AX260A ソフトウェアマニュアル

コンフィグレーションガイド Vol.2

Ver. 4.21 対応

AX26A-S002-60

AlaxalA

■対象製品

このマニュアルは AX260A モデルを対象に記載しています。
また，AX260A のソフトウェア Ver.4.21 の機能について記載しています。ソフトウェア機能は，ソフトウェア OS-L2F，およびオプションライセンスによってサポートする機能について記載します。

■輸出時の注意

本製品を輸出される場合には，外国為替及び外国貿易法の規制ならびに米国の輸出管理規則など外国の輸出関連法規をご確認のうえ，必要な手続きをお取りください。
なお，不明な場合は，弊社担当営業にお問い合わせください。

■商標一覧

Ethernet は，富士ゼロックス株式会社の登録商標です。
Internet Explorer は，米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
IPX は，Novell,Inc. の商標です。
Microsoft は，米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
Windows は，米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
sFlow は，米国およびその他の国における米国 InMon Corp. の登録商標です。
イーサネットは，富士ゼロックス株式会社の登録商標です。
そのほかの記載の会社名，製品名は，それぞれの会社の商標もしくは登録商標です。

■マニュアルはよく読み，保管してください。

製品を使用する前に，安全上の説明をよく読み，十分理解してください。
このマニュアルは，いつでも参照できるよう，手近な所に保管してください。

■ご注意

このマニュアルの内容については，改良のため，予告なく変更する場合があります。

■発行

２０２０年　１１月 （第７版） ＡＸ ２６ Ａ － Ｓ ００２－６０

■著作権

変更履歴

【Ver.4.21（第 7 版）】

表　変更履歴

章タイトル	追加・変更内容
1　フィルタ	・受信側フロー検出モードを変更しました。 ・送信側フロー検出モードを変更しました。
3　フロー制御	・受信側フロー検出モードを変更しました。
4　送信制御	・シェーパ使用時の注意事項を変更しました。
5　レイヤ2認証機能の概説	・レイヤ2認証機能と他機能の共存を変更しました。
13　DHCP snooping	・リレーエージェント情報オプション（DHCP Option82）を追加しました。
14　ホワイトリスト機能【OP-WL】	・ホワイトリスト機能使用時の注意事項の記述を変更しました。
15　特定端末へのWeb通信不可表示機能	・受信側フロー検出モードlayer2-3を追加しました。
17　アップリンク・リダンダント	・装置起動時のアクティブポート固定機能を変更しました。 ・スタックに対応しました。
20　L2ループ検知	・L2ループ検知使用時の注意事項を変更しました。
22　SNMPを使用したネットワーク管理	・SNMPv3の記述を変更しました。
23　ログ出力機能	・syslogサーバ出力形式の説明を変更しました。
25　LLDP	・LLDP標準2009を追加しました。

なお，単なる誤字・脱字などはお断りなく訂正しました。

【Ver.4.12（第 6 版）】

表　変更履歴

章タイトル	追加・変更内容
フロー制御	・下記の記述を変更しました。 フロー検出時の注意事項 帯域監視使用時の注意事項 CoS 値・キューイング優先度
IEEE802.1X の解説	・アカウント機能の記述を変更しました。
Web 認証の解説	・下記の記述を変更しました。 アカウント機能 認証エラーメッセージ
MAC 認証の解説	・アカウント機能の記述を変更しました。
ホワイトリスト機能【OP-WL】	・下記の記述を変更しました。 ホワイトリスト共通機能 他機能との共存
アップリンク・リダンダント	・アップリンク・リダンダント使用時の注意事項の記述を変更しました。
ログ出力機能	・ログ出力機能使用時の注意事項の記述を変更しました。
LLDP	・サポート仕様の記述を変更しました。

章タイトル	追加・変更内容
ポートミラーリング	・下記の記述を変更しました。 ポートミラーリングの概要 ポートミラーリング使用時の注意事項
ポリシーベースミラーリング	・下記の記述を変更しました。 概要 ポリシーベースミラーリング使用時の注意事項

【Ver.4.10（第 5 版）】

表　変更履歴

章タイトル	追加・変更内容
6　IEEE802.1X の解説	• 端末検出動作切り替えオプションに passive モードを追加しました。
10　MAC 認証の解説	• MAC 認証の認証契機について注意事項を追加しました。
14　ホワイトリスト機能【OP-WL】	• 下記の記述を変更しました。 ホワイトリスト機能の有効化と排他関係 他機能との共存 ホワイトアドレスリスト機能の注意事項 • ホワイトリスト機能と L2 ループ検知の併用を追加しました。
20　L2 ループ検知	• 他機能との共存の記述を変更しました。

【Ver.4.7（第 4 版）】

表　変更履歴

章タイトル	追加・変更内容
フィルタ	• 受信側フロー検出モードの記述を変更しました。
フロー制御	• 受信側フロー検出モードの記述を変更しました。
レイヤ 2 認証機能の概説	• レイヤ 2 認証機能と他機能の共存の記述を変更しました。
IEEE802.1X の解説	• 端末検出動作切り替えオプションの記述を変更しました。
ホワイトリスト機能【OP-WL】	• ホワイトリスト機能の有効化と排他関係を変更しました。 • 他機能との共存の記述を変更しました。
特定端末への Web 通信不可表示機能	• 本章を追加しました。
ポートミラーリング	• 802.1Q Tag 付与機能，ミラーポートのポートチャネル指定について追加しました。

【Ver.4.6（第 3 版）】

表　変更履歴

章タイトル	追加・変更内容
フィルタ	• 下記の記述を変更しました。 受信側フロー検出モード フロー検出条件 アクセスリスト
フロー制御	• フロー検出条件の記述を変更しました。
ポートミラーリング	•「(2) サポート範囲」の記述を変更しました。
ポリシーベースミラーリング	• 本章を追加しました。

【Ver.4.5（第 2 版）】

表　変更履歴

章タイトル	追加・変更内容
はじめに	• 「本バージョンでご使用時の注意事項」の記述を変更しました。
フロー制御	• 「CoS 値・キューイング優先度」の「優先度決定で変更できないフレーム一覧」の記述を変更しました。
Web 認証の解説	• 「URL リダイレクト機能」に HTTPS リクエストの URL リダイレクト抑止指定について記述を追加しました。 • 「HTTP サーバの初期タイムアウト時間の変更」の記述を変更しました。 • 「8.8.2　認証モード共通の注意事項」の「HTTP サーバの初期タイムアウト時間指定について」の記載内容を「8.2.2　認証機能」の「HTTP サーバの初期タイムアウト時間の変更」へ移動しました。
ホワイトリスト機能【OP-WL】	• ホワイトリスト機能の有効化と排他関係を変更しました。 • 他機能との共存の記述を変更しました。
ストームコントロール	• 「未認証パケットの流量制限」の注意事項を削除しました。

はじめに

■対象製品およびソフトウェアバージョン

このマニュアルは AX260A モデルを対象に記載しています。また，AX260A のソフトウェア Ver.4.21 の機能について記載しています。ソフトウェア機能は，ソフトウェア OS-L2F，およびオプションライセンスによってサポートする機能について記載します。

操作を行う前にこのマニュアルをよく読み，書かれている指示や注意を十分に理解してください。このマニュアルは必要なときにすぐ参照できるよう使いやすい場所に保管してください。

なお，このマニュアルでは特に断らないかぎり AX260A に共通の機能について記載しますが，モデル固有の機能については以下のマークで示します。

【08TF】:

AX260A-08TF についての記述です。

【08T】:

AX260A-08T についての記述です。

また，オプションライセンスの機能については以下のマークで示します。

【OP-WL】:

オプションライセンス OP-WL についての記述です。

【OP-WLE】:

オプションライセンス OP-WLE についての記述です。

また，当該マークの記述は，オプションライセンス OP-WL 登録済が前提です。

■本バージョンでご使用時の注意事項

本バージョンは，以下の機能に制限がありますので，当該機能に関するコマンドはご使用にならないでください。

本バージョンでの制限事項（未サポート項目）

対象機能	サポート項目	制限事項（未サポート）
OAN	－	全機能

■このマニュアルの訂正について

このマニュアルに記載の内容は，ソフトウェアと共に提供する「リリースノート」および「マニュアル訂正資料」で訂正する場合があります。

■対象読者

本装置を利用したネットワークシステムを構築し，運用するシステム管理者の方を対象としています。

また，次に示す知識を理解していることを前提としています。

- ネットワークシステム管理の基礎的な知識

■このマニュアルの URL

このマニュアルの内容は下記 URL に掲載しております。

http://www.alaxala.com

■マニュアルの読書手順

本装置の導入，セットアップ，日常運用までの作業フローに従って，それぞれの場合に参照するマニュアルを次に示します。

●初期導入時の基本的な設定について知りたい，ハードウェアの設備条件，取扱方法を調べる

AX260A
ハードウェア取扱説明書
(AX26A-H001)

●ラック搭載の手順について知りたい

MNTKIT-01
ハードウェア取扱説明書
(AXMK-H001)

●ソフトウェアの機能，コンフィグレーションの設定，運用コマンドについて知りたい

コンフィグレーションガイド
Vol.1
(AX26A-S001)

Vol.2
(AX26A-S002)

●コンフィグレーションコマンドの入力シンタックス，パラメータ詳細について知りたい

コンフィグレーション
コマンドレファレンス
(AX26A-S003)

●運用コマンドの入力シンタックス，パラメータ詳細について知りたい

運用コマンドレファレンス
(AX26A-S004)

●メッセージとログについて調べる

メッセージ・ログレファレンス
(AX26A-S005)

●MIBについて調べる

MIBレファレンス
(AX26A-S006)

●トラブル発生時の対処方法について知りたい

トラブルシューティングガイド
(AX26A-T001)

■このマニュアルでの表記

AC	Alternating Current
ACK	ACKnowledge
ADSL	Asymmetric Digital Subscriber Line
ALG	Application Level Gateway
ANSI	American National Standards Institute
ARP	Address Resolution Protocol
AS	Autonomous System
AUX	Auxiliary
BGP	Border Gateway Protocol
BGP4	Border Gateway Protocol - version 4

BGP4+	Multiprotocol Extensions for Border Gateway Protocol - version 4
bit/s	bits per second *bpsと表記する場合もあります。
BPDU	Bridge Protocol Data Unit
BRI	Basic Rate Interface
CC	Continuity Check
CDP	Cisco Discovery Protocol
CFM	Connectivity Fault Management
CIDR	Classless Inter-Domain Routing
CIR	Committed Information Rate
CIST	Common and Internal Spanning Tree
CLNP	ConnectionLess Network Protocol
CLNS	ConnectionLess Network System
CONS	Connection Oriented Network System
CRC	Cyclic Redundancy Check
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CSNP	Complete Sequence Numbers PDU
CST	Common Spanning Tree
DA	Destination Address
DC	Direct Current
DCE	Data Circuit terminating Equipment
DHCP	Dynamic Host Configuration Protocol
DIS	Draft International Standard/Designated Intermediate System
DNS	Domain Name System
DR	Designated Router
DSAP	Destination Service Access Point
DSCP	Differentiated Services Code Point
DTE	Data Terminal Equipment
DVMRP	Distance Vector Multicast Routing Protocol
E-Mail	Electronic Mail
EAP	Extensible Authentication Protocol
EAPOL	EAP Over LAN
EFM	Ethernet in the First Mile
EPU	External Power Unit
ES	End System
FAN	Fan Unit
FCS	Frame Check Sequence
FDB	Filtering DataBase
FQDN	Fully Qualified Domain Name
FTTH	Fiber To The Home
GBIC	GigaBit Interface Converter
GSRP	Gigabit Switch Redundancy Protocol
HMAC	Keyed-Hashing for Message Authentication
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
ICMPv6	Internet Control Message Protocol version 6
ID	Identifier
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IETF	the Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPCP	IP Control Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPV6CP	IP Version 6 Control Protocol
IPX	Internetwork Packet Exchange
ISO	International Organization for Standardization
ISP	Internet Service Provider
IST	Internal Spanning Tree
L2LD	Layer 2 Loop Detection
LAN	Local Area Network
LCP	Link Control Protocol
LED	Light Emitting Diode
LLC	Logical Link Control
LLDP	Link Layer Discovery Protocol
LLQ+3WFQ	Low Latency Queueing + 3 Weighted Fair Queueing
LSP	Label Switched Path
LSP	Link State PDU
LSR	Label Switched Router
MA	Maintenance Association
MAC	Media Access Control
MC	Memory Card
MD5	Message Digest 5
MDI	Medium Dependent Interface

MDI-X	Medium Dependent Interface crossover
MEP	Maintenance association End Point
MIB	Management Information Base
MIP	Maintenance domain Intermediate Point
MLD	Multicast Listener Discovery
MRU	Maximum Receive Unit
MSTI	Multiple Spanning Tree Instance
MSTP	Multiple Spanning Tree Protocol
MTU	Maximum Transfer Unit
NAK	Not AcKnowledge
NAS	Network Access Server
NAT	Network Address Translation
NCP	Network Control Protocol
NDP	Neighbor Discovery Protocol
NET	Network Entity Title
NLA ID	Next-Level Aggregation Identifier
NPDU	Network Protocol Data Unit
NSAP	Network Service Access Point
NSSA	Not So Stubby Area
NTP	Network Time Protocol
OADP	Octpower Auto Discovery Protocol
OAM	Operations,Administration,and Maintenance
OSPF	Open Shortest Path First
OUI	Organizationally Unique Identifier
packet/s	packets per second　　*ppsと表記する場合もあります。
PAD	PADding
PAE	Port Access Entity
PC	Personal Computer
PCI	Protocol Control Information
PDU	Protocol Data Unit
PICS	Protocol Implementation Conformance Statement
PID	Protocol IDentifier
PIM	Protocol Independent Multicast
PIM-DM	Protocol Independent Multicast-Dense Mode
PIM-SM	Protocol Independent Multicast-Sparse Mode
PIM-SSM	Protocol Independent Multicast-Source Specific Multicast
PoE	Power over Ethernet
PRI	Primary Rate Interface
PS	Power Supply
PSNP	Partial Sequence Numbers PDU
QoS	Quality of Service
RA	Router Advertisement
RADIUS	Remote Authentication Dial In User Service
RDI	Remote Defect Indication
REJ	REJect
RFC	Request For Comments
RIP	Routing Information Protocol
RIPng	Routing Information Protocol next generation
RMON	Remote Network Monitoring MIB
RPF	Reverse Path Forwarding
RQ	ReQuest
RSTP	Rapid Spanning Tree Protocol
SA	Source Address
SD	Secure Digital
SDH	Synchronous Digital Hierarchy
SDU	Service Data Unit
SEL	NSAP SELector
SFD	Start Frame Delimiter
SFP	Small Form factor Pluggable
SFP+	Enhanced Small Form factor Pluggable
SML	Split Multi Link
SMTP	Simple Mail Transfer Protocol
SNAP	Sub-Network Access Protocol
SNMP	Simple Network Management Protocol
SNP	Sequence Numbers PDU
SNPA	Subnetwork Point of Attachment
SPF	Shortest Path First
SSAP	Source Service Access Point
STP	Spanning Tree Protocol
TA	Terminal Adapter
TACACS+	Terminal Access Controller Access Control System Plus
TCP/IP	Transmission Control Protocol/Internet Protocol
TLA ID	Top-Level Aggregation Identifier
TLV	Type, Length, and Value

TOS	Type Of Service
TPID	Tag Protocol Identifier
TTL	Time To Live
UDLD	Uni-Directional Link Detection
UDP	User Datagram Protocol
ULR	Uplink Redundant
UPC	Usage Parameter Control
UPC-RED	Usage Parameter Control - Random Early Detection
VAA	VLAN Access Agent
VLAN	Virtual LAN
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network
WDM	Wavelength Division Multiplexing
WFQ	Weighted Fair Queueing
WRED	Weighted Random Early Detection
WS	Work Station
WWW	World-Wide Web
XFP	10 gigabit small Form factor Pluggable

■ kB(バイト) などの単位表記について

1kB(キロバイト), 1MB(メガバイト), 1GB(ギガバイト), 1TB(テラバイト) はそれぞれ 1024 バイト, 1024^2 バイト, 1024^3 バイト, 1024^4 バイトです。

目次

第 1 編　フィルタ

第 2 編　QoS

第 7 編　リモートネットワーク管理

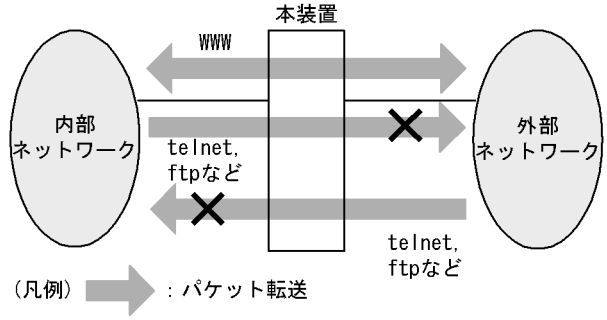
1 フィルタ

フィルタは，ある特定のフレームを中継したり，廃棄したりする機能です。
この章ではフィルタ機能の解説と操作方法について説明します。

1.1 解説

フィルタは，ある特定のフレームを中継または廃棄する機能です。フィルタはネットワークのセキュリティを確保するために使用します。フィルタを使用すれば，ユーザごとにネットワークへのアクセスを制限できます。例えば，内部ネットワークと外部ネットワーク間で WWW は中継しても，telnet や ftp は廃棄したいなどの運用ができます。外部ネットワークからの不正なアクセスを防ぎ，また，内部ネットワークから外部ネットワークへ不要な情報の漏洩を防ぐことができます。フィルタを使用したネットワーク構成例を次に示します。

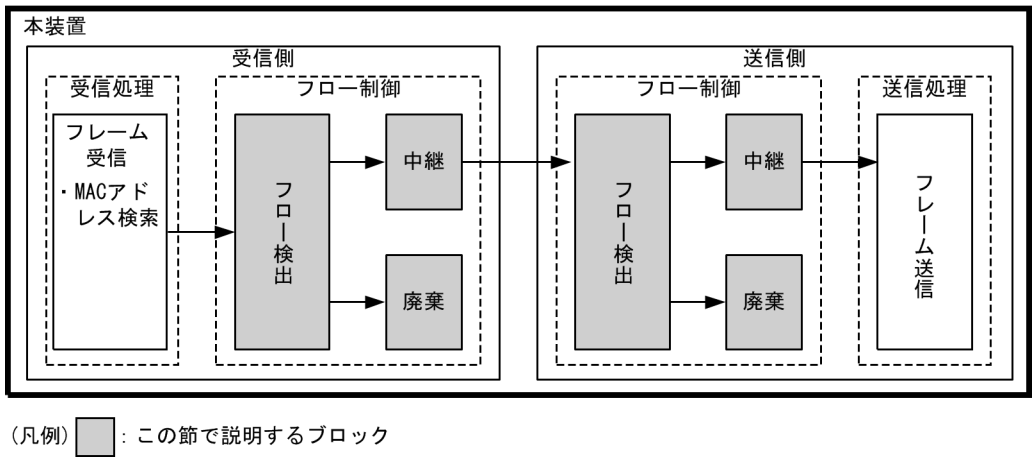
図 1-1 フィルタを使用したネットワーク構成例



1.1.1 フィルタの概要

本装置のフィルタの機能ブロックを次の図に示します。

図 1-2 本装置のフィルタの機能ブロック



この図に示したフィルタの各機能ブロックの概要を次の表に示します。

表 1-1 フィルタの各機能ブロックの概要

機能部位		機能概要
フロー制御部	フロー検出	MAC アドレスやプロトコル種別，IP アドレス，TCP/UDP のポート番号，ICMP ヘッダなどの条件に一致するフロー（特定フレーム）を検出します。
	中継・廃棄	フロー検出したフレームに対し，中継または廃棄します。

本装置では，MAC アドレス，プロトコル種別，IP アドレス，TCP/UDP のポート番号，ICMP ヘッダなどのフロー検出と，中継や廃棄という動作を組み合わせたフィルタエントリを作成し，フィルタを実施します。

本装置のフィルタの仕組みを次に示します。

1. 各インタフェースに設定したフィルタエントリをユーザが設定した優先順に検索します。
2. 一致したフィルタエントリが見つかった時点で検索を終了します。
3. 該当したフレームはフィルタエントリで設定した動作に従って，中継や廃棄が実行されます。
4. すべてのフィルタエントリに一致しなかった場合，そのフレームを廃棄します。廃棄動作の詳細は，「1.1.7　暗黙の廃棄」を参照してください。

注意事項

受信側インタフェースでフレームが廃棄された場合，送信側インタフェースではフロー検出しません。

1.1.2　フロー検出

フロー検出とは，フレームの一連の流れであるフローを MAC ヘッダ，IP ヘッダ，TCP ヘッダ，ICMP ヘッダなどの条件に基づいて検出する機能です。アクセスリストで設定します。アクセスリストの詳細は，「1.1.6　アクセスリスト」を参照してください。

本装置では，受信側イーサネットインタフェース・VLAN インタフェースで，イーサネット V2 形式および IEEE802.3 の SNAP/RFC1042 形式フレームのフロー検出ができます。設定可能なインタフェースは，受信側フロー検出モードによって変わります。

本装置では，送信側イーサネットインタフェース・VLAN インタフェースで，イーサネット V2 形式および IEEE802.3 の SNAP/RFC1042 形式フレームのフロー検出ができます。設定可能なインタフェースは，送信側フロー検出モードによって変わります。

なお，一部の制御フレームと snooping 対象フレームは，フィルタ（送信側）の対象外です。

1.1.3　受信側フロー検出モード

本装置では，ネットワーク構成や運用形態を想定して受信側フロー検出モードを用意しています。受信側フロー検出モードは，受信側インタフェースに対するフィルタ・QoS エントリの配分パターンを決めるモードです。また，ポリシーベースミラーリングで適用するフロー検出条件のエントリ配分パターンも受信側フロー検出モードで決定します。エントリの配分は「コンフィグレーションガイド Vol.1　3.2　収容条件」を参照し，使い方に合わせて選択してください。

受信側フロー検出モードはコンフィグレーションコマンド flow detection mode で指定します。なお，選択した受信側フロー検出モードはフィルタ・QoS・ポリシーベースミラーリングで共通です。受信側フロー検出モードを変更する場合，受信側インタフェースに設定された次のコマンドをすべて削除する必要があります。

- mac access-group
- ip access-group
- ipv6 traffic-filter
- mac qos-flow-group
- ip qos-flow-group
- ipv6 qos-flow-group

また，以下の機能を未サポートのモードに変更する場合も，各コマンドを削除する必要があります。

- ホワイトリスト機能：white-list enable
- 特定端末への Web 通信不可機能：access-redirect http port
- ポリシーベースミラーリング：monitor session filter

受信側フロー検出モードを指定しない場合，layer2-2（デフォルトコンフィグレーション）が設定されます。

受信側フロー検出モードとフロー動作の関係を次の表に示します。

表 1-2　受信側フロー検出モードとフロー動作の関係

受信側フロー検出モード名称	運用目的	フロー動作	検出対象インタフェース
layer2-1	IP パケットやそれ以外のフレームのフィルタを行いたい場合に使用します。	MAC アドレス，イーサネットタイプなどの MAC ヘッダでフレームを検出します。	イーサネット，VLAN
layer2-2	IPv4 パケットに特化し，きめ細かいフィルタを行いたい場合に使用します。	IPv4 パケットについて，IP ヘッダ，TCP/UDP ヘッダ，ICMP ヘッダでフレームを検出します。	イーサネット，VLAN
layer2-3	IPv4，IPv6 パケットに特化し，きめ細かいフィルタを行いたい場合に使用します。	IPv4 パケットは，IP ヘッダ，TCP/UDP ヘッダ，ICMP ヘッダでフレームを検出します。IPv6 パケットは，IP ヘッダ，TCP/UDP ヘッダ，ICMP ヘッダでフレームを検出します。	イーサネット，VLAN
layer2-1-mirror	IP パケットやそれ以外のフレームのフィルタとポリシーベースミラーリングを行いたい場合に使用します。	MAC アドレス，イーサネットタイプなどの MAC ヘッダでフレームを検出します。	イーサネット，VLAN，モニターセッション※
layer2-2-mirror	IPv4 パケットに特化し，きめ細かいフィルタとポリシーベースミラーリングを行いたい場合に使用します。	IPv4 パケットについて，IP ヘッダ，TCP/UDP ヘッダ，ICMP ヘッダでフレームを検出します。	イーサネット，VLAN，モニターセッション※

注※
ポリシーベースミラーリングの場合は，モニターセッションに設定されたモニターポート（イーサネット）が検出対象です。

1.1.4　送信側フロー検出モード

本装置では，ネットワーク構成や運用形態を想定して送信側フロー検出モードを用意しています。送信側フロー検出モードは，送信側インタフェースに対するフィルタエントリの配分パターンを決めるモードです。エントリの配分は「コンフィグレーションガイド Vol.1　3.2　収容条件」を参照し，使い方に合わせて選択してください。

送信側フロー検出モードはコンフィグレーションコマンド flow detection out mode で指定します。なお，選択した送信側フロー検出モードはフィルタで有効です。送信側フロー検出モードを変更する場合，送信側インタフェースに設定された次のコマンドをすべて削除する必要があります。

- mac access-group
- ip access-group
- ipv6 traffic-filter

送信側フロー検出モードを指定しない場合，layer2-2-out（デフォルトコンフィグレーション）が設定されます。

送信側フロー検出モードとフロー動作の関係を次の表に示します。

表 1-3 送信側フロー検出モードとフロー動作の関係

送信側フロー検出モード名称	運用目的	フロー動作	検出対象インタフェース
layer2-1-out	IP パケットやそれ以外のフレームのフィルタを行いたい場合に使用します。	MAC アドレス，イーサネットタイプなどの MAC ヘッダでフレームを検出します。	イーサネット，VLAN
layer2-2-out	IPv4 パケットに特化したフィルタを行いたい場合に使用します。	IPv4 パケットについて，IP ヘッダ，TCP/UDP ヘッダ，ICMP ヘッダでフレームを検出します。	イーサネット，VLAN
layer2-3-out	IPv4，IPv6 パケットに特化し，きめ細かいフィルタを行いたい場合に使用します。それ以外のフレームのフィルタも可能です。	IPv6 パケットやそれ以外のフレームで検出します。 IP パケットは IP ヘッダ，TCP/UDP ヘッダ，ICMP ヘッダでも検出します。 MAC アドレス，イーサネットタイプなどの MAC ヘッダでフレームを検出することも可能です。	イーサネット，VLAN

1.1.5 フロー検出条件

フロー検出するためには，コンフィグレーションでフローを識別するための条件を設定します。受信側および送信側インタフェースでのフロー検出条件を次に示します。

（1） 受信側フロー検出条件

受信側インタフェースのフロー検出条件を次の表に示します。

表 1-4 受信側インタフェースで指定可能なフロー検出条件

種別		設定項目	layer2-1 layer2-1-mirror		layer2-2 layer2-2-mirror		layer2-3	
			イーサネット	VLAN ※7	イーサネット	VLAN ※7	イーサネット	VLAN
MAC 条件	MAC ヘッダ	VLAN ID	○	−	−	−	−	−
		送信元 MAC アドレス	○	○	−	−	−	−
		宛先 MAC アドレス	○	○	−	−	−	−
		イーサネットタイプ	○	○	−	−	−	−
		ユーザ優先度 ※1	○	○	−	−	−	−
	クラス	ユーザクラス ※6	○	○	−	−	−	−
IPv4 条件	MAC ヘッダ	VLAN ID	−	−	○	−	○	−
		ユーザ優先度 ※1	−	−	○	○	○	○
	IPv4 ヘッダ ※2	上位プロトコル	−	−	○	○	○	○
		送信元 IP アドレス	−	−	○	○	○	○
		宛先 IP アドレス	−	−	○	○	○	○

種別		設定項目		layer2-1 layer2-1-mirror		layer2-2 layer2-2-mirror		layer2-3	
				イーサネット	VLAN ※7	イーサネット	VLAN ※7	イーサネット	VLAN
		TOS		−	−	○	○	○	○
		DSCP		−	−	○	○	○	○
		Precedence		−	−	○	○	○	○
	IPv4-TCP ヘッダ	送信元ポート番号	単一指定（eq）	−	−	○	○	○	○
			範囲指定（range）	−	−	○ ※4	○ ※4	○ ※4	○ ※4
		宛先ポート番号	単一指定（eq）	−	−	○	○	○	○
			範囲指定（range）	−	−	○ ※4	○ ※4	○ ※4	○ ※4
		TCP 制御フラグ ※3		−	−	○	○	○	○
	IPv4-UDP ヘッダ	送信元ポート番号	単一指定（eq）	−	−	○	○	○	○
			範囲指定（range）	−	−	○ ※4	○ ※4	○ ※4	○ ※4
		宛先ポート番号	単一指定（eq）	−	−	○	○	○	○
			範囲指定（range）	−	−	○ ※4	○ ※4	○ ※4	○ ※4
	IPv4-ICMP ヘッダ	ICMP タイプ値		−	−	○	○	○	○
		ICMP コード値		−	−	○	○	○	○
	クラス	ユーザクラス ※6		−	−	○	○	○	○
IPv6 条件	MAC ヘッダ	VLAN ID		−	−	−	−	○	−
		ユーザ優先度 ※1		−	−	−	−	○	○
	IPv6 ヘッダ ※5	上位プロトコル		−	−	−	−	○	○
		送信元 IP アドレス		−	−	−	−	○	○
		宛先 IP アドレス		−	−	−	−	○	○
		トラフィッククラス		−	−	−	−	○	○
		DSCP		−	−	−	−	○	○
	IPv6-TCP ヘッダ	送信元ポート番号	単一指定（eq）	−	−	−	−	○	○
			範囲指定（range）	−	−	−	−	○ ※4	○ ※4
		宛先ポート番号	単一指定（eq）	−	−	−	−	○	○
			範囲指定（range）	−	−	−	−	○ ※4	○ ※4
		TCP 制御フラグ ※3		−	−	−	−	○	○

種別		設定項目		layer2-1 layer2-1-mirror		layer2-2 layer2-2-mirror		layer2-3	
				イーサネット	VLAN ※7	イーサネット	VLAN ※7	イーサネット	VLAN
	IPv6-UDPヘッダ	送信元ポート番号	単一指定(eq)	－	－	－	－	○	○
			範囲指定(range)	－	－	－	－	○ ※4	○ ※4
		宛先ポート番号	単一指定(eq)	－	－	－	－	○	○
			範囲指定(range)	－	－	－	－	○ ※4	○ ※4
	IPv6-ICMPヘッダ	ICMP タイプ値		－	－	－	－	○	○
		ICMP コード値		－	－	－	－	○	○
	クラス	ユーザクラス ※6		－	－	－	－	○	○

（凡例）○：指定できる　　－：指定できない

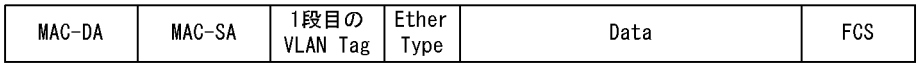
注 ※1

次に示すフレームについてはユーザ優先度を検出できません。常に，ユーザ優先度 3 として検出します。

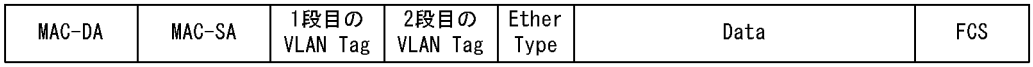
- VLAN Tag なしのフレーム
- VLAN トンネリングを設定したポートで受信したフレーム

また，VLAN Tag が複数あるフレームに対してユーザ優先度を検出する場合，MAC アドレス側から 1 段目の VLAN Tag にあるユーザ優先度が対象となります。次の図に VLAN Tag が複数あるフレームの例を示します。

(i) VLAN Tag 1段のフォーマット



(ii) VLAN Tag 2段のフォーマット

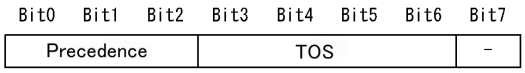


注 ※2

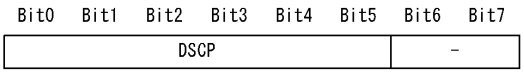
TOS フィールドの指定についての補足

TOS　　：TOS フィールドのビット 3 ～ 6 の値です。

Precedence：TOS フィールドの上位 3 ビットの値です。



DSCP　　：TOS フィールドの上位 6 ビットの値です。



注 ※3

ack/fin/psh/rst/syn/urg フラグが 1 のパケットを検出します。

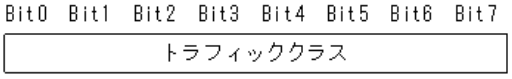
注 ※4

TCP/UDP ポート番号検出パターンの使用例については，「コンフィグレーションガイド Vol.1　3.2　収容条件」を参照してください。

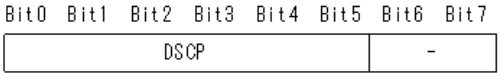
注 ※5

トラフィッククラスフィールドの指定についての補足

トラフィッククラス：トラフィッククラスフィールドの値です。



DSCP：トラフィッククラスフィールドの上位 6 ビットの値です。



注 ※6

ユーザクラスは認証機能で使用します。詳細は，「5　レイヤ 2 認証機能の概説　5.4.9　ダイナミック ACL/QoS 機能」を参照してください。

注 ※7

VLAN インタフェースは，フィルタ機能の検出対象です。ポリシーベースミラーリングは検出対象外です。

(2) 送信側フロー検出条件

送信側インタフェースのフロー検出条件を次の表に示します。

表 1-5　送信側インタフェースで指定可能なフロー検出条件

種別		設定項目		layer2-1-out		layer2-2-out		layer2-3-out	
				イーサネット	VLAN ※6	イーサネット	VLAN ※6	イーサネット	VLAN ※6
MAC 条件	MAC ヘッダ	VLAN ID※1		○	−	−	−	○	−
		送信元 MAC アドレス		○	○	−	−	○	○
		宛先 MAC アドレス		○	○	−	−	○	○
		イーサネットタイプ		○	○	−	−	○	○
		ユーザ優先度 ※2		○	○	−	−	○	○
	クラス	ユーザクラス ※7		○	○	−	−	−	−
IPv4 条件	MAC ヘッダ	VLAN ID※1		−	−	○	−	○	−
		ユーザ優先度 ※2		−	−	○	○	○	○
	IPv4 ヘッダ ※3	上位プロトコル		−	−	○	○	○	○
		送信元 IP アドレス		−	−	○	○	○	○
		宛先 IP アドレス		−	−	○	○	○	○
		TOS		−	−	○	○	○	○
		DSCP		−	−	○	○	○	○
		Precedence		−	−	○	○	○	○
	IPv4-TCP ヘッダ	送信元ポート番号	単一指定 (eq)	−	−	○	○	○	○
			範囲指定 (range)	−	−	−	−	−	−
		宛先ポート番号	単一指定 (eq)	−	−	○	○	○	○
			範囲指定 (range)	−	−	−	−	−	−
		TCP 制御フラグ ※4		−	−	○	○	○	○

種別		設定項目		layer2-1-out		layer2-2-out		layer2-3-out	
				イーサネット	VLAN ※6	イーサネット	VLAN ※6	イーサネット	VLAN ※6
	IPv4-UDPヘッダ	送信元ポート番号	単一指定（eq）	－	－	○	○	○	○
			範囲指定（range）	－	－	－	－	－	－
		宛先ポート番号	単一指定（eq）	－	－	○	○	○	○
			範囲指定（range）	－	－	－	－	－	－
	IPv4-ICMPヘッダ	ICMP タイプ値		－	－	○	○	○	○
		ICMP コード値		－	－	○	○	○	○
	クラス	ユーザクラス ※7		－	－	○	○	○	○
IPv6条件	MAC ヘッダ	VLAN ID※1		－	－	－	－	○	－
		ユーザ優先度 ※2		－	－	－	－	○	○
	IPv6 ヘッダ ※5	上位プロトコル		－	－	－	－	○	○
		送信元 IP アドレス		－	－	－	－	○	○
		宛先 IP アドレス		－	－	－	－	○	○
		トラフィッククラス		－	－	－	－	○	○
		DSCP		－	－	－	－	○	○
	IPv6-TCPヘッダ	送信元ポート番号	単一指定（eq）	－	－	－	－	○	○
			範囲指定（range）	－	－	－	－	－	－
		宛先ポート番号	単一指定（eq）	－	－	－	－	○	○
			範囲指定（range）	－	－	－	－	－	－
		TCP 制御フラグ ※4		－	－	－	－	○	○
	IPv6-UDPヘッダ	送信元ポート番号	単一指定（eq）	－	－	－	－	○	○
			範囲指定（range）	－	－	－	－	－	－
		宛先ポート番号	単一指定（eq）	－	－	－	－	○	○
			範囲指定（range）	－	－	－	－	－	－
	IPv6-ICMPヘッダ	ICMP タイプ値		－	－	－	－	○	○
		ICMP コード値		－	－	－	－	○	○
	クラス	ユーザクラス ※7		－	－	－	－	○	○

（凡例）○：指定できる　　－：指定できない

注 ※1

次に示す場合，VLAN ID を指定できません。

- Tag 変換を設定したイーサネットインタフェースに指定する場合
- VLAN トンネリングを設定したイーサネットインタフェースに指定する場合

注 ※2

送信フレームの VLAN Tag にあるユーザ優先度を検出します。VLAN Tag が複数あるフレームに対してユーザ優先度を検出する場合，MAC アドレス側から 1 段目の VLAN Tag にあるユーザ優先度が対象となります。次の図に VLAN Tag が複数あるフレームの例を示します。

(i) VLAN Tag 1段のフォーマット

MAC-DA	MAC-SA	1段目の VLAN Tag	Ether Type	Data	FCS

(ii) VLAN Tag 2段のフォーマット

MAC-DA	MAC-SA	1段目の VLAN Tag	2段目の VLAN Tag	Ether Type	Data	FCS

送信側インタフェースでは，VLAN Tag なしのフレームについてもユーザ優先度を検出します。ユーザ優先度検出の詳細を次の表に示します。

表 1-6　送信側インタフェースでのユーザ優先度検出

フレーム送信ポート	送信フレーム	ユーザ優先度のフロー検出動作
VLAN トンネリング設定なし	－	受信側でマーカー機能を使用した場合は，マーカー後のユーザ優先度を検出します。 受信側でマーカー機能を使用していない場合で，かつ受信フレームが VLAN Tag なしのときは，ユーザ優先度 3 として検出します。 受信側でマーカー機能を使用していない場合で，かつ受信フレームが VLAN Tag ありのときは，受信時のユーザ優先度を検出します。 ただし，次に示すフレームは優先度 3 として検出します。 • VLAN トンネリングを設定したポートで受信したフレーム
VLAN トンネリング設定あり	VLAN Tag なし	同上
	VLAN Tag あり	受信側のマーカー機能の使用有無に関係なく，送信フレームのユーザ優先度を検出します。送信フレームのユーザ優先度は次のようになります。 • VLAN トンネリングを設定したポートで受信したフレームは，受信時のユーザ優先度 • VLAN トンネリングを設定していないポートで受信したフレームは，受信フレームから VLAN Tag を外したあとのユーザ優先度

(凡例)

－：VLAN Tag の有無に影響しない

注 ※3

TOS フィールドの指定についての補足

TOS　　：TOS フィールドのビット 3 ～ 6 の値です。

Precedence：TOS フィールドの上位 3 ビットの値です。

Bit0	Bit1	Bit2	Bit3	Bit4	Bit5	Bit6	Bit7
Precedence			TOS				-

DSCP　　：TOS フィールドの上位 6 ビットの値です。

Bit0	Bit1	Bit2	Bit3	Bit4	Bit5	Bit6	Bit7
DSCP						-	

受信側インタフェースでマーカー機能の DSCP 書き換えを使用した場合，送信側インタフェースでの TOS，DSCP および Precedence の検出は，DSCP 書き換え後のフレームに対して実施します。

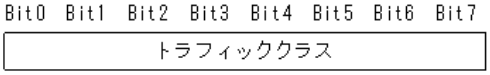
注 ※4

ack/fin/psh/rst/syn/urg フラグが 1 のパケットを検出します。

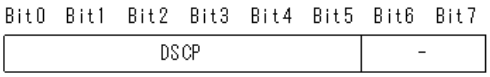
注 ※5

トラフィッククラスフィールドの指定についての補足

トラフィッククラス：トラフィッククラスフィールドの値です。



DSCP：トラフィッククラスフィールドの上位 6 ビットの値です。



注 ※6

次に示す VLAN インタフェースでは，フィルタエントリを適用できません。

- 該当 VLAN に属するすべてのイーサネットインタフェースに対し，どれか一つでも Tag 変換を設定している場合

注 ※7

ユーザクラスは認証機能で使用します。詳細は，「5　レイヤ 2 認証機能の概説　5.4.9　ダイナミック ACL/QoS 機能」を参照してください。

1.1.6　アクセスリスト

フィルタのフロー検出を実施するためにはコンフィグレーションでアクセスリストを設定します。フロー検出条件に応じて設定するアクセスリストが異なります。また，フロー検出条件ごとに検出可能なフレーム種別が異なります。フロー検出条件と対応するアクセスリスト，および検出可能なフレーム種別の関係を次の表に示します。

表 1-7　フロー検出条件と対応するアクセスリスト，検出可能なフレーム種別の関係

フロー検出条件	対応するアクセスリスト	対応する受信側フロー検出モード	対応する送信側フロー検出モード	検出可能なフレーム種別		
				非 IP	IPv4	IPv6
MAC 条件	mac access-list	layer2-1 layer2-1-mirror	layer2-1-out layer2-3-out	○	○ ※	○ ※
IPv4 条件	ip access-list	layer2-2 layer2-3 layer2-2-mirror	layer2-2-out layer2-3-out	－	○	－
IPv6 条件	ipv6 access-list	layer2-3	layer2-3-out	－	－	○

（凡例）○：検出できる　　－：検出できない

注 ※：イーサネットタイプで指定したときだけ検出可能です。

アクセスリストのインタフェースへの適用は，アクセスグループコマンドまたはトラフィックフィルタコマンドで実施します。適用順序は，アクセスリストのパラメータであるシーケンス番号によって決定します。

(1) 複数のフィルタが適用される場合の動作

(a) 受信フィルタと送信フィルタが適用される場合

1 つのフレームに対して，受信フィルタと送信フィルタが適用される場合，両方とも permit のときにフィルタとして permit となります。受信フィルタで deny となったフレームには送信フィルタが適用されません。（送信フィルタの統計情報にも計上しません。）

(b) 受信フィルタと QoS が同時に設定されている場合

受信フィルタと QoS が同時に設定されている場合，受信フィルタで deny となって廃棄される受信フレームも QoS の統計情報に計上します。

(c) 受信側フロー検出モード layer2-3 以外を設定時の受信フィルタ

受信側フロー検出モード layer2-1/layer2-1/layer2-1-mirror/layer2-2-mirror を設定時の受信フィルタは以下のようになります。

1つの受信フレームに対して，イーサネットインタフェースに設定された受信フィルタと，VLAN インタフェースに設定された受信フィルタが適用される場合，両方とも permit のときに受信フィルタとして permit となります。どちらかに deny（暗黙の deny を含む）がある場合は，deny が優先されます。

統計情報はイーサネットインタフェースおよび VLAN インタフェースで計上します。

受信フィルタで複数のフィルタエントリに一致した場合の動作を，次の表に示します。

表 1-8 複数フィルタエントリー致時の動作（layer2-1/layer2-2/layer2-1-mirror/layer2-2-mirror の場合）

複数フィルタエントリー致となる組み合わせ		有効になるフィルタエントリ		統計情報を計上するインタフェース
イーサネット	VLAN	インタフェース	動作	
permit	permit	イーサネット	permit（中継）	イーサネット VLAN
permit	deny	VLAN	deny（廃棄）	イーサネット VLAN
deny	permit	イーサネット	deny（廃棄）	イーサネット VLAN
deny	deny	イーサネット	deny（廃棄）	イーサネット VLAN

(d) 受信側フロー検出モード layer2-3 設定時の受信フィルタ

1 つのフレームに対して複数のフロー検出条件の受信フィルタを設定した場合，次の表に示す順序でフロー検出を実施します。複数のフィルタエントリには一致しません。

表 1-9 フロー検出順序（layer2-3 の場合）

フロー検出順序	フロー検出条件（アクセスリスト）	インタフェース
1	IPv4 条件（ip access-list ）または IPv6 条件（ipv6 access-list）	イーサネット
2		VLAN

例：

IPv6 条件の受信フィルタが設定されているイーサネットインタフェースで受信した IPv6 パケットには，VLAN インタフェースに設定されている IPv6 条件の受信フィルタが適用されません。

(e) 送信側フロー検出モード layer2-1-out または layer2-2-out 設定時の送信フィルタ

1つの送信フレームに対して，イーサネットインタフェースに設定された送信フィルタと，VLAN インタフェースに設定された送信フィルタが適用される場合，両方とも permit のときに送信フィルタとして permit となります。どちらかに deny（暗黙の deny を含む）がある場合は，deny が優先されます。

統計情報はどちらが有効になった場合でも，イーサネットインタフェースだけ計上します。

送信フィルタで複数のフィルタエントリに一致した場合の動作を，次の表に示します。

表 1-10 複数フィルタエントリー致時の動作（layer2-1-out または layer2-2-out の場合）

複数フィルタエントリー致となる組み合わせ		有効になるフィルタエントリ		統計情報を計上するインタフェース
イーサネット	VLAN	インタフェース	動作	
permit	permit	イーサネット	permit（中継）	イーサネット
permit	deny	VLAN	deny（廃棄）	イーサネット
deny	permit	イーサネット	deny（廃棄）	イーサネット
deny	deny	イーサネット	deny（廃棄）	イーサネット

(f) 送信側フロー検出モード layer2-3-out 設定時の送信フィルタ

1 つのフレームに対して複数のフロー検出条件の送信フィルタを設定した場合，次の表に示す順序でフレームを検出します。複数のフィルタエントリには一致しません。

表 1-11 フロー検出順序（layer2-3-out の場合）

フロー検出順序	フロー検出条件（アクセスリスト）	インタフェース
1	MAC 条件（mac access-list）	イーサネット
2		VLAN
3	IPv4 条件（ip access-list ）または IPv6 条件（ipv6 access-list）	イーサネット
4		VLAN

例 1：

送信イーサネットインタフェースに MAC 条件と IPv6 条件を設定した場合は，IPv6 条件の設定は意味を持たず，すべての送信フレームに対して MAC 条件だけが適用されます。

例 2：

送信フレームが属する VLAN インタフェースに MAC 条件を設定した場合は，送信イーサネットインタフェースに IPv4 条件を設定していても適用されません。

1.1.7 暗黙の廃棄

フィルタを設定したインタフェースでは，フロー検出条件に一致しないフレームは廃棄します。

暗黙の廃棄のフィルタエントリは，アクセスリストを生成すると自動生成されます。アクセスリストを一つも設定しない場合，すべてのフレームを中継します。

1.1.8 フィルタ使用時の注意事項

(1) フィルタの収容条件について

どのインタフェースからも参照されないアクセスリスト※が設定されている場合，収容条件（コンフィグレーションガイド Vol.1 3.2 収容条件」参照）に達する前に，アクセスリストが設定できなくなる場合があります。その場合は，未使用のアクセスリストの設定を削除してください。

注※ アクセスリスト：下記コマンドで設定するアクセスリスト

- ip access-list extended

- ip access-list standard
- ipv6 access-list
- mac access-list extended

（2） 複数フィルタエントリー致時の動作

「1.1.6　アクセスリスト（1）複数のフィルタが適用される場合の動作」を参照してください。

（3） VLAN Tag 付きフレームに対するフィルタ

3 段以上の VLAN Tag があるフレームに対して，MAC 条件のイーサネットタイプ，IPv4 条件，または IPv6 条件をフロー検出条件としたフィルタを実施できません。

2 段の VLAN Tag があるフレームに対して，MAC 条件のイーサネットタイプ，IPv4 条件，または IPv6 条件をフロー検出条件としたフィルタを受信側で実施するためには，次の条件のどちらかを満たす必要があります。

- 本装置で VLAN トンネリング機能が動作していない
- 本装置で VLAN トンネリング機能が動作していて，フレームを受信したポートがトランクポートである

（4） IPv4 フラグメントパケットに対するフィルタ

IPv4 フラグメントパケットに対して TCP/UDP ヘッダ・ICMP ヘッダをフロー検出条件としたフィルタを行った場合，2 番目以降のフラグメントパケットは TCP/UDP ヘッダ・ICMP ヘッダがパケット内にないため，検出できません。フラグメントパケットを含めたフィルタを実施する場合は，フロー検出条件に MAC ヘッダ，IP ヘッダを指定してください。

（5） 拡張ヘッダのある IPv6 パケットに対するフィルタ

IPv6 拡張ヘッダのある IPv6 パケットに対して TCP/UDP ヘッダ・ICMP ヘッダをフロー検出条件としたフィルタはできません。拡張ヘッダのあるパケットに対してフィルタを実施する場合は，フロー検出条件に MAC ヘッダ，IPv6 ヘッダを指定してください。

（6） フィルタエントリ適用時の動作

本装置では，インタフェースに対してフィルタを適用する※と，暗黙の廃棄エントリから適用します。そのため，ユーザが設定したフィルタエントリが適用されるまでの間，暗黙の廃棄に一致するフレームが一時的に廃棄されます。また，暗黙の廃棄エントリの統計情報が採られます。

注 ※

- 1 エントリ以上を設定したアクセスリストをアクセスグループコマンドによりインタフェースに適用する場合
- アクセスリストをアクセスグループコマンドにより適用し，ひとつ目のエントリを追加する場合

（7） フィルタエントリ変更時の動作

本装置では，インタフェースに適用済みのフィルタエントリを変更すると，変更が反映されるまでの間，検出の対象となるフレームが検出されなくなります。そのため，一時的にほかのフィルタエントリまたは暗黙の廃棄エントリで検出されます。

（8） コンフィグレーション変更時の統計情報について

アクセスリストに関連したコンフィグレーションを変更した際，変更したエントリ以外の統計カウンタが

瞬間的にカウントを停止しますが，それ以外のフィルタ機能は正常に動作しています。

（9） IPv4 プロトコル検出について

プロトコル名称 ah またはプロトコル番号 51 は，フィルタ条件として指定しても検出できません。

（10）本装置が送信するフレーム / パケットに対するフィルタ

本装置が自発的に送信するレイヤ 2 フレーム，および snooping 機能で自発的に送信または監視するレイヤ 3 パケットの一部は，フロー検出できないため廃棄できません。

また，フロー検出できないフレーム / パケットは，送信フィルタの統計情報に計上しません。

（11）他機能との同時使用

（a） 特定の条件により廃棄されたフレームの統計情報

以下の場合フレームは廃棄しますが，インタフェースに対してフィルタエントリを設定し一致した場合，一致したフィルタエントリの統計情報が採られます。

- VLAN のポートのデータ転送状態が Blocking（データ転送停止中）の状態で，該当ポートからフレームを受信した場合
- ポート間中継遮断機能で指定したポートからフレームを受信した場合
- ネイティブ VLAN をトランクポートで送受信する VLAN に設定しないで，VLAN Tag なしフレームを受信した場合
- トランクポートで送受信する VLAN に設定していない VLAN Tag 付きフレームを受信した場合
- プロトコルポートおよび MAC ポートで VLAN Tag 付きフレームを受信した場合
- MAC アドレス学習機能によってフレームが廃棄された場合
- レイヤ 2 認証によってフレームが廃棄された場合
- レイヤ 2 プロトコルが無効なためフレームが廃棄された場合
- IGMP snooping および MLD snooping によってフレームが廃棄された場合
- DHCP snooping によってフレームが廃棄された場合
- ストームコントロールによってフレームが廃棄された場合

（b） フィルタ使用時のストーム検出

フィルタ検出による廃棄とストーム検出による廃棄が同時に発生すると，本来，中継されるべきフレームを含め，より多くのフレーム廃棄が発生する場合があります。

1.2 コンフィグレーション

1.2.1 コンフィグレーションコマンド一覧

フィルタで使用するコンフィグレーションコマンド一覧を次の表に示します。

表 1-12 コンフィグレーションコマンド一覧

コマンド名	説明
deny	フィルタでのアクセスを廃棄する条件を指定します。
flow detection mode	フィルタ・QoS 制御の受信側フロー検出モードを設定します。
flow detection out mode	フィルタの送信側フロー検出モードを設定します。
ip access-group	イーサネットインタフェースまたは VLAN インタフェースに対して IPv4 フィルタを適用し，IPv4 フィルタ機能を有効にします。
ip access-list extended	IPv4 パケットフィルタとして動作するアクセスリストを設定します。
ip access-list resequence	IPv4 アドレスフィルタおよび IPv4 パケットフィルタのフィルタ条件適用順序のシーケンス番号を再設定します。
ip access-list standard	IPv4 アドレスフィルタとして動作するアクセスリストを設定します。
ipv6 access-list	IPv6 フィルタとして動作するアクセスリストを設定します。
ipv6 access-list resequence	IPv6 フィルタのフィルタ条件適用順序のシーケンス番号を再設定します。
ipv6 traffic-filter	イーサネットインタフェースまたは VLAN インタフェースに対して IPv6 フィルタを適用し，IPv6 フィルタ機能を有効にします。
mac access-group	イーサネットインタフェースまたは VLAN インタフェースに対して MAC フィルタを適用し，MAC フィルタ機能を有効にします。
mac access-list resequence	MAC フィルタのフィルタ条件適用順序のシーケンス番号を再設定します。
mac access-list extended	MAC フィルタとして動作するアクセスリストを設定します。
permit	フィルタでのアクセスを中継する条件を指定します。
remark	フィルタの補足説明を指定します。

1.2.2 MAC ヘッダで中継・廃棄をする設定

(1) 受信側フロー検出モードの設定

フィルタの受信側フロー検出モードを指定する例を次に示します。

[設定のポイント]

受信側フロー検出モードは，ハードウェアの基本的な動作条件を決定するため，最初に設定します。

[コマンドによる設定]

1. **(config)# flow detection mode layer2-1**

受信側フロー検出モード layer2-1 を有効にします。

(2) 送信側フロー検出モードの設定

フィルタの送信側フロー検出モードを指定する例を次に示します。

［設定のポイント］
送信側フロー検出モードは，ハードウェアの基本的な動作条件を決定するため，最初に設定します。

［コマンドによる設定］

1. **(config)# flow detection out mode layer2-1-out**
送信側フロー検出モード layer2-1-out を有効にします。

（3） MAC ヘッダをフロー検出条件とする例

MAC ヘッダをフロー検出条件として，フレームを中継・廃棄指定する例を次に示します。

［設定のポイント］
フレーム受信時に MAC ヘッダによってフロー検出を行い，フィルタエントリに一致したフレームを廃棄・中継します。

［コマンドによる設定］

1. **(config)# mac access-list extended IPX_DENY**
mac access-list（IPX_DENY）を作成します。本リストを作成することによって，MAC フィルタの動作モードに移行します。

2. **(config-ext-macl)# deny any any ipx**
イーサネットタイプが IPX のフレームを廃棄する MAC フィルタを設定します。

3. **(config-ext-macl)# permit any any**
すべてのフレームを中継する MAC フィルタを設定します。

4. **(config-ext-macl)# exit**
MAC フィルタの動作モードからグローバルコンフィグレーションモードに戻ります。

5. **(config)# interface gigabitethernet 0/1**
ポート 0/1 のインタフェースモードに移行します。

6. **(config-if)# mac access-group IPX_DENY in**
(config-if)# exit
受信側に MAC フィルタを有効にします。

1.2.3 IP ヘッダ・TCP/UDP ヘッダで中継・廃棄をする設定

（1） 受信側フロー検出モードの設定

フィルタの受信側フロー検出モードを指定する例を次に示します。

［設定のポイント］
受信側フロー検出モードは，ハードウェアの基本的な動作条件を決定するため，最初に設定します。

［コマンドによる設定］

1. **(config)# flow detection mode layer2-3**
受信側フロー検出モード layer2-3 を有効にします。

(2) 送信側フロー検出モードの設定

フィルタの送信側フロー検出モードを指定する例を次に示します。

[設定のポイント]

送信側フロー検出モードは，ハードウェアの基本的な動作条件を決定するため，最初に設定します。

[コマンドによる設定]

1. **(config)# flow detection out mode layer2-2-out**
   送信側フロー検出モード layer2-2-out を有効にします。

(3) IPv4 アドレスをフロー検出条件とする設定

IPv4 アドレスをフロー検出条件とし，フレームを中継・廃棄指定する例を次に示します。

[設定のポイント]

フレーム受信時に送信元 IPv4 アドレスによってフロー検出を行い，フィルタエントリに一致したフレームを中継します。フィルタエントリに一致しない IP パケットはすべて廃棄します。

[コマンドによる設定]

1. **(config)# ip access-list standard FLOOR_A_PERMIT**
   ip access-list（FLOOR_A_PERMIT）を作成します。本リストを作成することによって，IPv4 アドレスフィルタの動作モードに移行します。

2. **(config-std-nacl)# permit 192.168.0.0 0.0.0.255**
   送信元 IP アドレス 192.168.0.0/24　ネットワークからのフレームを中継する IPv4 アドレスフィルタを設定します。

3. **(config-std-nacl)# exit**
   IPv4 アドレスフィルタの動作モードからグローバルコンフィグレーションモードに戻ります。

4. **(config)# interface vlan 10**
   VLAN10 のインタフェースモードに移行します。

5. **(config-if)# ip access-group FLOOR_A_PERMIT in**
   (config-if)# exit
   受信側に IPv4 フィルタを有効にします。

(4) IPv4 パケットをフロー検出条件とする設定

IPv4 telnet パケットをフロー検出条件とし，フレームを中継・廃棄指定する例を次に示します。

[設定のポイント]

フレーム受信時に IP ヘッダ・TCP/UDP ヘッダによってフロー検出を行い，フィルタエントリに一致したフレームを廃棄します。

[コマンドによる設定]

1. **(config)# ip access-list extended TELNET_DENY**
   ip access-list（TELNET_DENY）を作成します。本リストを作成することによって，IPv4 パケット

フィルタの動作モードに移行します。

2. **(config-ext-nacl)# deny tcp any any eq telnet**
   telnet のパケットを廃棄する IPv4 パケットフィルタを設定します。

3. **(config-ext-nacl)# permit ip any any**
   すべてのフレームを中継する IPv4 パケットフィルタを設定します。

4. **(config-ext-nacl)# exit**
   IPv4 パケットフィルタの動作モードからグローバルコンフィグレーションモードに戻ります。

5. **(config)# interface vlan 10**
   VLAN10 のインタフェースモードに移行します。

6. **(config-if)# ip access-group TELNET_DENY in**
   (config-if)# exit
   受信側に IPv4 フィルタを有効にします。

（5） TCP/UDP ポート番号の範囲をフロー検出条件とする設定

UDP ポート番号の範囲をフロー検出条件とし，フレームを中継・廃棄指定する例を次に示します。

［設定のポイント］

フレーム受信時に UDP ヘッダの宛先ポート番号の範囲によってフロー検出を行い，フィルタエントリに一致したフレームを廃棄します。

［コマンドによる設定］

1. **(config)# ip access-list extended PORT_RANGE_DENY**
   ip access-list（PORT_RANGE_DENY）を作成します。本リストを作成することによって，IPv4 パケットフィルタの動作モードに移行します。

2. **(config-ext-nacl)# deny udp any any range 10 20**
   UDP ヘッダの宛先ポート番号が 10 ～ 20 のパケットを廃棄する IPv4 パケットフィルタを設定します。

3. **(config-ext-nacl)# permit ip any any**
   すべてのフレームを中継する IPv4 パケットフィルタを設定します。

4. **(config-ext-nacl)# exit**
   IPv4 パケットフィルタの動作モードからグローバルコンフィグレーションモードに戻ります。

5. **(config)# interface vlan 10**
   VLAN10 のインタフェースモードに移行します。

6. **(config-if)# ip access-group PORT_RANGE_DENY in**
   (config-if)# exit
   受信側に IPv4 フィルタを有効にします。

（6） IPv6 パケットをフロー検出条件とする設定

IPv6 パケットをフロー検出条件として，フレームを中継・廃棄指定する例を次に示します。

［設定のポイント］

フレーム受信時に IP アドレスによってフロー検出を行い，フィルタエントリに一致したフレームを中継します。フィルタエントリに一致しない IP パケットはすべて廃棄します。

［コマンドによる設定］

1. **(config)# ipv6 access-list FLOOR_B_PERMIT**
   ipv6 access-list(FLOOR_B_PERMIT) を作成します。本リストを作成することによって，IPv6 パケットフィルタの動作モードに移行します。

2. **(config-ipv6-acl)# permit ipv6 2001:100::1/64 any**
   送信元 IP アドレス 2001:100::1/64 からのフレームを中継する IPv6 パケットフィルタを設定します。

3. **(config-ipv6-acl)# exit**
   IPv6 パケットフィルタの動作モードからグローバルコンフィグレーションモードに戻ります。

4. **(config)# interface gigabitethernet 0/1**
   ポート 0/1 のインタフェースモードに移行します。

5. **(config-if)# ipv6 traffic-filter FLOOR_B_PERMIT in**
   (config-if)# exit
   受信側に IPv6 フィルタを有効にします。

1.2.4 複数インタフェースフィルタの設定

複数のイーサネットインタフェースにフィルタを指定する例を次に示します。

［設定のポイント］

config-if-range モードで複数のイーサネットインタフェースにフィルタを設定できます。

［コマンドによる設定］

1. **(config)# ip access-list standard HOST_IP**
   (config-std-nacl)# permit host 192.168.0.1
   (config-std-nacl)# exit
   ホスト 192.168.0.1 からだけフレームを中継する IPv4 アドレスフィルタを設定します。

2. **(config)# interface range gigabitethernet 0/1-4**
   ポート 0/1-4 のインタフェースモードに移行します。

3. **(config-if-range)# ip access-group HOST_IP in**
   (config-if-range)# exit
   受信側に IPv4 フィルタを有効にします。

1.3 オペレーション

運用コマンド show access-filter によって，設定した内容が反映されているかどうかを確認します。

1.3.1 運用コマンド一覧

フィルタで使用する運用コマンド一覧を次の表に示します。

表 1-13 運用コマンド一覧

コマンド名	説明
show access-filter	アクセスグループコマンド (mac access-group，ip access-group，ipv6 traffic-filter) で設定したアクセスリスト (mac access-list，ip access-list，ipv6 access-list) の統計情報を表示します。
clear access-filter	アクセスグループコマンド (mac access-group，ip access-group，ipv6 traffic-filter) で設定したアクセスリスト (mac access-list，ip access-list，ipv6 access-list) の統計情報をクリアします。

1.3.2 フィルタの確認

(1) イーサネットインタフェースに設定されたエントリの確認

イーサネットインタフェースにフィルタを設定した場合の動作確認の方法を次の図に示します。

図 1-3 イーサネットインタフェースにフィルタを設定した場合の動作確認

```
> show access-filter 0/3 only-appletalk

Date 20XX/11/24 16:28:03 UTC
Using Port:0/3 in
Extended MAC access-list:only-appletalk
  remark "permit only appletalk"
  10 permit any any appletalk
    Matched packets          :      23741
  20 permit any any 0x80f3
    Matched packets          :        363
  Implicitly denied packets :       2883

>
```

指定したポートのフィルタに「Extended MAC access-list」を表示することを確認します。

(2) VLAN インタフェースに設定されたエントリの確認

VLAN インタフェースにフィルタを設定した場合の動作確認の方法を次の図に示します。

図 1-4 VLAN インタフェースにフィルタを設定した場合の動作確認

```
> show access-filter interface vlan 1500

Date 20XX/11/24 17:33:23 UTC
Using Interface:vlan 1500 in
Standard IP access-list:pc-a1024
  remark "permit only pc-a1024"
  10 permit host 192.168.1.254
    Matched packets          :   50310935
  Implicitly denied packets :      31394
IPv6 access-list:only-ra
  remark "permit only Router-11"
  10 permit icmp host fe80::213:20ff:fea5:24ab any router-advertisement
    Matched packets          :          9
  Implicitly denied packets :        268
```

```
Using Interface:vlan 1500 out
Extended IP access-list:only-https
  remark "permit only https"
  10 permit tcp any any eq https
    Matched packets          :   52826479
  Implicitly denied packets :       6794

>
```

指定した VLAN のフィルタに「Standard IP access-list」「Extended IPv6 access-list」「Extended IP access-list」を表示することを確認します。

2 QoS 制御の概要

QoS 制御は，帯域監視・マーカー・優先度決定・帯域制御によって通信品質を制御し，回線の帯域やキューのバッファ容量などの限られたネットワーク資源を有効に利用するための機能です。この章では，本装置の QoS 制御について説明します。

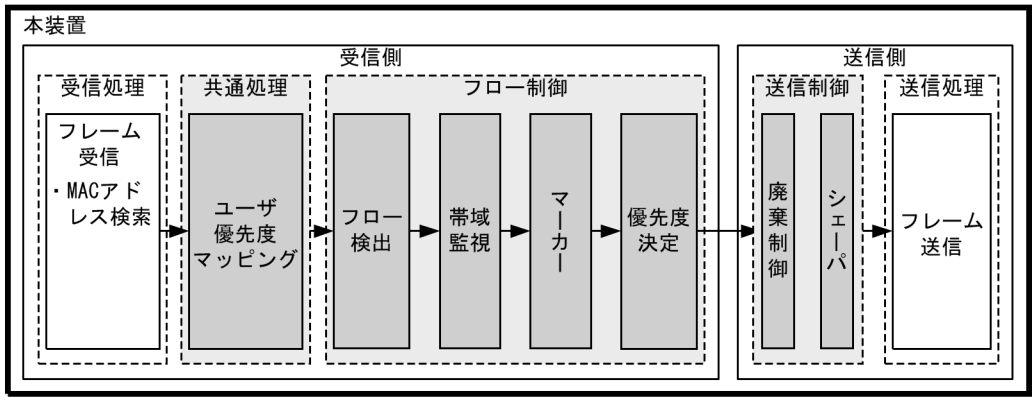
2.1 QoS 制御構造

ネットワークを利用したサービスの多様化に伴い，通信品質を保証しないベストエフォート型のトラフィックに加え，実時間型・帯域保証型のトラフィックが増加しています。本装置の QoS 制御を使用することによって，トラフィック種別に応じた通信品質を提供できます。

本装置の QoS 制御は，回線の帯域やキューのバッファ容量などの限られたネットワーク資源を有効に使用できます。アプリケーションごとに要求されるさまざまな通信品質を満たすために，QoS 制御を使用しネットワーク資源を適切に分配します。

本装置の QoS 制御の機能ブロックを次の図に示します。

図 2-1 本装置の QoS 制御の機能ブロック



（凡例） ：この節で説明するブロック

図に示した QoS 制御の各機能ブロックの概要を次の表に示します。

表 2-1 QoS 制御の各機能ブロックの概要

機能部位		機能概要
受信処理部	フレーム受信	フレームを受信し，MAC アドレステーブル検索を実施します。
共通処理部	ユーザ優先度マッピング	受信フレームの VLAN Tag のユーザ優先度に従い，優先度を決定します。
フロー制御部	フロー検出	MAC ヘッダやプロトコル種別，IP アドレス，TCP/UDP のポート番号，ICMP ヘッダなどの条件に一致するフローを検出します。
	帯域監視	フローごとに帯域を監視して，帯域を超えたフローに対してペナルティを与えます。
	マーカー	IP ヘッダ内の DSCP や VLAN Tag のユーザ優先度を書き換える機能です。
	優先度決定	フローに対する優先度や，廃棄されやすさを示すキューイング優先度を決定します。
送信制御部	廃棄制御	フレームの優先度とキューの状態に応じて，該当フレームをキューイングするか廃棄するかを制御します。
	シェーパ	各キューからのフレームの出力順序および出力帯域を制御します。
送信処理部	フレーム送信	シェーパによって制御されたフレームを送信します。

本装置の QoS 制御は，受信フレームの優先度をユーザ優先度マッピング，またはフロー制御によって決定します。ユーザ優先度マッピングは，受信フレームの VLAN Tag 内にあるユーザ優先度に基づいて優先度

を決定します。ユーザ優先度ではなく，MAC アドレスや IP アドレスなどの特定の条件に一致するフレームに対して優先度を決定したい場合は，フロー制御を使用します。

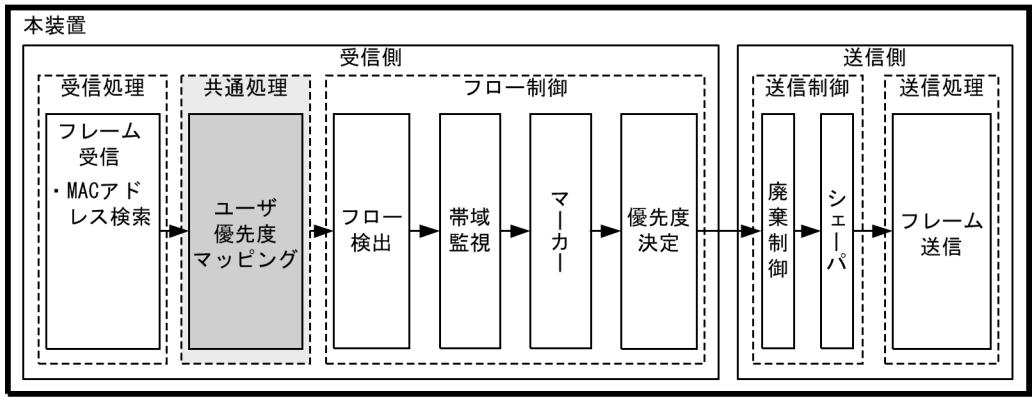
フロー制御による優先度の決定は，ユーザ優先度マッピングよりも優先されます。また，フロー制御は，優先度決定のほかに帯域監視やマーカーも実施することができます。フロー検出で検出したフローに対して，帯域監視，マーカー，優先度決定の各機能は同時に動作することができます。

送信制御は，ユーザ優先度マッピングやフロー制御によって決定した優先度に基づいて，廃棄制御やシェーパを実施します。

2.2　共通処理解説

この節で説明するユーザ優先度マッピングの位置づけを次の図に示します。

図 2-2　ユーザ優先度マッピングの位置づけ



（凡例）：この節で説明するブロック

2.2.1　ユーザ優先度マッピング

ユーザ優先度マッピングは，受信フレームの VLAN Tag 内にあるユーザ優先度に基づいて優先度を決定する機能です。本装置では，常にユーザ優先度マッピングが動作し，すべての受信フレームに対して優先度を決定します。

優先度の値には，装置内の優先度を表す CoS 値を用います。受信フレームのユーザ優先度の値から CoS 値にマッピングし，CoS 値によって送信キューを決定します。CoS 値と送信キューの対応については，「3.10.2　CoS マッピング機能」を参照してください。

ユーザ優先度は，Tag Control フィールド（VLAN Tag ヘッダ情報）の上位 3 ビットを示します。なお，VLAN Tag がないフレームは，常に CoS 値 3 を使用します。

フロー制御による優先度決定が動作する場合，ユーザ優先度マッピングよりも優先して動作します。

表 2-2　ユーザ優先度と CoS 値のマッピング

フレームの種類		マッピングされる CoS 値
VLAN Tag の有無	ユーザ優先度値	
VLAN Tag なし	−	3
VLAN Tag あり ※	0	0
	1	1
	2	2
	3	3
	4	4
	5	5
	6	6
	7	7

（凡例）

－：該当なし

注 ※

次の場合，受信時のユーザ優先度値に関係なく，常に CoS 値 3 でマッピングされます。

- VLAN トンネリングを設定したポートで受信したフレーム

2.3　QoS 制御共通のコンフィグレーション

2.3.1　コンフィグレーションコマンド一覧

QoS 制御共通のコンフィグレーションコマンド一覧を次の表に示します。

表 2-3　コンフィグレーションコマンド一覧

コマンド名	説明
flow detection mode	フィルタ・QoS 制御の受信側フロー検出モードを設定します。
ip qos-flow-group	イーサネットインタフェースまたは VLAN インタフェースに対して，IPv4 QoS フローリストを適用し，IPv4 QoS 制御を有効にします。
ip qos-flow-list	IPv4 QoS フロー検出として動作する QoS フローリストを設定します。
ip qos-flow-list resequence	IPv4 QoS フローリストの条件適用順序のシーケンス番号を再設定します。
ipv6 qos-flow-group	イーサネットインタフェースまたは VLAN インタフェースに対して，IPv6 QoS フローリストを適用し，IPv6 QoS 制御を有効にします。
ipv6 qos-flow-list	IPv6 QoS フロー検出として動作する QoS フローリストを設定します。
ipv6 qos-flow-list resequence	IPv6 QoS フローリストの条件適用順序のシーケンス番号を再設定します。
limit-queue-length	本装置の物理ポートの送信キュー長を設定します。
mac qos-flow-group	イーサネットインタフェースまたは VLAN インタフェースに対して，MAC QoS フローリストを適用し，MAC QoS 制御を有効にします。
mac qos-flow-list	MAC QoS フロー検出として動作する QoS フローリストを設定します。
mac qos-flow-list resequence	MAC QoS フローリストの条件適用順序のシーケンス番号を再設定します。
qos	QoS フローリストでのフロー検出条件および動作指定を設定します。
qos-queue-group	イーサネットインタフェースに対して，QoS キューリスト情報を適用し，レガシーシェーパを有効にします。
qos-queue-list	QoS キューリスト情報にスケジューリングモードを設定します。
remark	QoS の補足説明を記述します。
traffic-shape rate	イーサネットインタフェースにポート帯域制御を設定します。
control-packet user-priority	本装置が自発的に送信するフレームの VLAN Tag 内にあるユーザ優先度を設定します。

2.4 QoS 制御共通のオペレーション

2.4.1 運用コマンド一覧

QoS 制御共通の運用コマンド一覧を次の表に示します。

表 2-4 運用コマンド一覧

コマンド名	説明
show qos-flow	QoS フローグループコマンド (mac qos-flow-group，ip qos-flow-group，ipv6 qos-flow-group) で設定した QoS フローリスト (mac qos-flow-list，ip qos-flow-list，ipv6 qos-flow-list) の統計情報を表示します。
clear qos-flow	QoS フローグループコマンド (mac qos-flow-group，ip qos-flow-group，ipv6 qos-flow-group) で設定した QoS フローリスト (mac qos-flow-list，ip qos-flow-list，ipv6 qos-flow-list) の統計情報をクリアします。
show qos queueing	イーサネットインタフェースの送信キューの統計情報を表示します。
clear qos queueing	イーサネットインタフェースの送信キューの統計情報をクリアします。

3 フロー制御

この章では本装置のフロー制御（フロー検出，帯域監視，マーカー，優先度決定）について説明します。

3.1　フロー検出解説

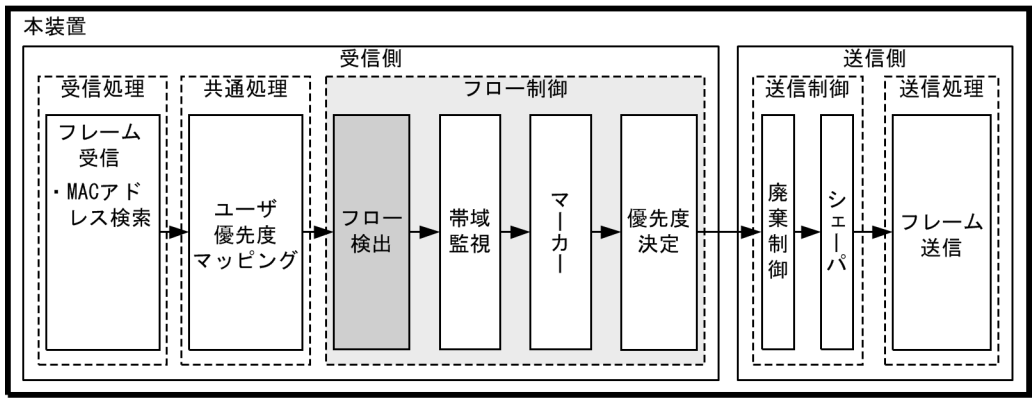
フロー検出とは，フレームの一連の流れであるフローを MAC ヘッダ，IP ヘッダ，TCP ヘッダ，ICMP ヘッダなどの条件に基づいてフレームを検出する機能です。QoS フローリストで設定します。QoS フローリストの詳細は，「3.1.3　QoS フローリスト」を参照してください。

本装置では，受信側イーサネットインタフェース・VLAN インタフェースで，イーサネット V2 形式および IEEE802.3 の SNAP/RFC1042 形式フレームのフロー検出ができます。設定可能なインタフェースは，受信側フロー検出モードによって変わります。

なお，一部の制御フレームと snooping 対象フレームは，QoS の対象外です。

この節で説明するフロー検出の位置づけを次の図に示します。

図 3-1　フロー検出の位置づけ



（凡例）：この節で説明するブロック

3.1.1　受信側フロー検出モード

本装置では，ネットワーク構成や運用形態を想定して受信側フロー検出モードを用意しています。受信側フロー検出モードは，受信側インタフェースに対するフィルタ・QoS エントリの配分パターンを決めるモードです。また，ポリシーベースミラーリングで適用するフロー検出条件のエントリ配分パターンも受信側フロー検出モードで決定します。エントリの配分は「コンフィグレーションガイド Vol.1　3.2　収容条件」を参照し，使い方に合わせて選択してください。

受信側フロー検出モードは flow detection mode コマンドで指定します。なお，選択した受信側フロー検出モードはフィルタ・QoS・ポリシーベースミラーリングで共通です。受信側フロー検出モードを変更する場合，受信側インタフェースに設定された次のコマンドをすべて削除する必要があります。

- mac access-group
- ip access-group
- ipv6 traffic-filter
- mac qos-flow-group
- ip qos-flow-group
- ipv6 qos-flow-group

また，以下の機能を未サポートのモードに変更する場合も，各コマンドを削除する必要があります。

- ホワイトリスト機能：white-list enable

- 特定端末への Web 通信不可機能：access-redirect http port
- ポリシーベースミラーリング：monitor session filter

受信側フロー検出モードを指定しない場合，layer2-2（デフォルトコンフィグレーション）が設定されます。

受信側フロー検出モードとフロー動作の関係を次の表に示します。

表 3-1　受信側フロー検出モードとフロー動作の関係

受信側フロー検出モード名称 ※	運用目的	フロー動作	検出対象インタフェース
layer2-1	IP パケットやそれ以外のフレームの QoS フロー検出を行いたい場合に使用します。	MAC アドレス，イーサネットタイプなどの MAC ヘッダでフレームを検出します。	イーサネット，VLAN
layer2-2	IPv4 パケットに特化し，きめ細かい QoS フロー検出を行いたい場合に使用します。	IPv4 パケットについて，IP ヘッダ，TCP/UDP ヘッダ，ICMP ヘッダでフレームを検出します。	イーサネット，VLAN
layer2-3	IPv4，IPv6 パケットに特化し，きめ細かい QoS フロー検出を行いたい場合に使用します。	IPv4 パケットは，IP ヘッダ，TCP/UDP ヘッダ，ICMP ヘッダでフレームを検出します。 IPv6 パケットは，IP ヘッダ，TCP/UDP ヘッダ，ICMP ヘッダでフレームを検出します。	イーサネット，VLAN

注 ※
layer2-1-mirror，layer2-2-mirror は，QoS フロー検出機能未サポートです。

3.1.2　フロー検出条件

フロー検出するためには，コンフィグレーションでフローを識別するための条件を設定します。受信側インタフェースでのフロー検出条件を次に示します。

(1) 受信側フロー検出条件

受信側インタフェースのフロー検出条件を次の表に示します。

表 3-2　受信側インタフェースで指定可能なフロー検出条件

種別		設定項目	layer2-1		layer2-2		layer2-3	
			イーサネット	VLAN	イーサネット	VLAN	イーサネット	VLAN
MAC 条件	MAC ヘッダ	VLAN ID	○	－	－	－	－	－
		送信元 MAC アドレス	○	○	－	－	－	－
		宛先 MAC アドレス	○	○	－	－	－	－
		イーサネットタイプ	○	○	－	－	－	－
		ユーザ優先度 ※1	○	○	－	－	－	－
	クラス	ユーザクラス ※6	○	○	－	－	－	－
IPv4 条件	MAC ヘッダ	VLAN ID	－	－	○	－	○	－
		ユーザ優先度 ※1	－	－	○	○	○	○

種別		設定項目		layer2-1		layer2-2		layer2-3	
				イーサネット	VLAN	イーサネット	VLAN	イーサネット	VLAN
	IPv4 ヘッダ※2	上位プロトコル		−	−	○	○	○	○
		送信元 IP アドレス		−	−	○	○	○	○
		宛先 IP アドレス		−	−	○	○	○	○
		TOS		−	−	○	○	○	○
		DSCP		−	−	○	○	○	○
		Precedence		−	−	○	○	○	○
	IPv4-TCP ヘッダ	送信元ポート番号	単一指定(eq)	−	−	○	○	○	○
			範囲指定(range)	−	−	○※4	○※4	○※4	○※4
		宛先ポート番号	単一指定(eq)	−	−	○	○	○	○
			範囲指定(range)	−	−	○※4	○※4	○※4	○※4
		TCP 制御フラグ※3		−	−	○	○	○	○
	IPv4-UDP ヘッダ	送信元ポート番号	単一指定(eq)	−	−	○	○	○	○
			範囲指定(range)	−	−	○※4	○※4	○※4	○※4
		宛先ポート番号	単一指定(eq)	−	−	○	○	○	○
			範囲指定(range)	−	−	○※4	○※4	○※4	○※4
	IPv4-ICMP ヘッダ	ICMP タイプ値		−	−	○	○	○	○
		ICMP コード値		−	−	○	○	○	○
	クラス	ユーザクラス※6		−	−	○	○	○	○
IPv6 条件	MAC ヘッダ	VLAN ID		−	−	−	−	○	−
		ユーザ優先度※1		−	−	−	−	○	○
	IPv6 ヘッダ※5	上位プロトコル		−	−	−	−	○	○
		送信元 IP アドレス		−	−	−	−	○	○
		宛先 IP アドレス		−	−	−	−	○	○
		トラフィッククラス		−	−	−	−	○	○
		DSCP		−	−	−	−	○	○
	IPv6-TCP ヘッダ	送信元ポート番号	単一指定(eq)	−	−	−	−	○	○
			範囲指定(range)	−	−	−	−	○※4	○※4
		宛先ポート番号	単一指定(eq)	−	−	−	−	○	○
			範囲指定(range)	−	−	−	−	○※4	○※4

種別		設定項目		layer2-1		layer2-2		layer2-3	
				イーサネット	VLAN	イーサネット	VLAN	イーサネット	VLAN
		TCP 制御フラグ※3		－	－	－	－	○	○
	IPv6-UDP ヘッダ	送信元ポート番号	単一指定（eq）	－	－	－	－	○	○
			範囲指定（range）	－	－	－	－	○※4	○※4
		宛先ポート番号	単一指定（eq）	－	－	－	－	○	○
			範囲指定（range）	－	－	－	－	○※4	○※4
	IPv6-ICMP ヘッダ	ICMP タイプ値		－	－	－	－	○	○
		ICMP コード値		－	－	－	－	○	○
	クラス	ユーザクラス※6		－	－	－	－	○	○

（凡例）○：指定できる　　－：指定できない

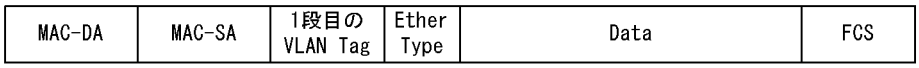
注 ※1

次に示すフレームについてはユーザ優先度を検出できません。常に，ユーザ優先度 3 として検出します。

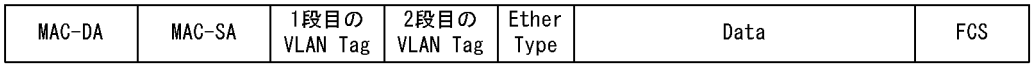
- VLAN Tag なしのフレーム
- VLAN トンネリングを設定したポートで受信したフレーム

また，VLAN Tag が複数あるフレームに対してユーザ優先度を検出する場合，MAC アドレス側から 1 段目の VLAN Tag にあるユーザ優先度が対象となります。次の図に VLAN Tag が複数あるフレームの例を示します。

（i）VLAN Tag 1段のフォーマット



（ii）VLAN Tag 2段のフォーマット

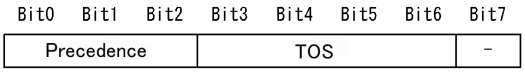


注 ※2

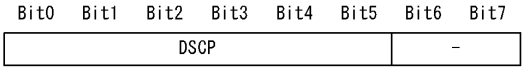
TOS フィールドの指定についての補足

TOS　　：TOS フィールドのビット 3 ～ 6 の値です。

Precedence：TOS フィールドの上位 3 ビットの値です。



DSCP　　：TOS フィールドの上位 6 ビットの値です。



注 ※3

ack/fin/psh/rst/syn/urg フラグが 1 のパケットを検出します。

注 ※4

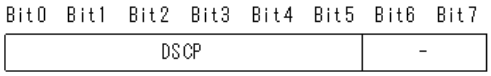
TCP/UDP ポート番号検出パターンの使用例については，「コンフィグレーションガイド Vol.1　3.2　収容条件」を参照してください。

注 ※5

トラフィッククラスフィールドの指定についての補足

トラフィッククラス：トラフィッククラスフィールドの値です。

DSCP：トラフィッククラスフィールドの上位 6 ビットの値です。



注 ※6

ユーザクラスは認証機能で使用します。詳細は，「5　レイヤ 2 認証機能の概説　5.4.9　ダイナミック ACL/QoS 機能」を参照してください。

3.1.3　QoS フローリスト

QoS のフロー検出を実施するためにはコンフィグレーションで QoS フローリストを設定します。フロー検出条件に応じて設定する QoS フローリストが異なります。また，フロー検出条件ごとに検出可能なフレーム種別が異なります。フロー検出条件と対応する QoS フローリスト，および検出可能なフレーム種別の関係を次の表に示します。

表 3-3　フロー検出条件と対応する QoS フローリスト，検出可能なフレーム種別の関係

フロー検出条件	対応する QoS フローリスト	対応する受信側フロー検出モード	検出可能なフレーム種別		
			非 IP	IPv4	IPv6
MAC 条件	mac qos-flow-list	layer2-1	○	○※	○※
IPv4 条件	ip qos-flow-list	layer2-2 layer2-3	－	○	－
IPv6 条件	ipv6 qos-flow-list	layer2-3	－	－	○

（凡例）○：検出できる　　－：検出できない
注 ※：イーサネットタイプで指定したときだけ検出可能です。

QoS フローリストのインタフェースへの適用は，QoS フローグループコマンドで実施します。適用順序は，QoS フローリストのパラメータであるシーケンス番号によって決定します。

（1）複数の QoS が適用される場合の動作

（a）受信フィルタと QoS が同時に設定されている場合

受信フィルタと QoS が同時に設定されている場合，受信フィルタで deny となって廃棄される受信フレームも QoS の統計情報に計上します。

（b）受信フロー検出モード layer2-1 または layer2-2 設定時の QoS フロー

フレームを受信したイーサネットインタフェースと，受信フレームが属する VLAN インタフェースの両方に QoS フローリスト※ が設定されている場合，action パラメータで指定された動作が競合しない（例：イーサネットで replace-dscp，VLAN で replace-user-priority）ときは，両方とも有効になります。

注 ※

コンフィグレーションコマンド mac qos-flow-group，または ip qos-flow-group を示します。

action パラメータで指定された動作が競合する場合は，イーサネットインタフェースの QoS フローリストで指定された動作が有効になります。

統計情報はイーサネットインタフェースと VLAN インタフェースの両方に計上します。

(c) 受信側フロー検出モード layer2-3 設定時の QoS フロー

フレームを受信したイーサネットインタフェースと，受信フレームが属する VLAN インタフェースの両方に QoS フローリスト※1 が設定されている場合，イーサネットインタフェースの QoS フローリスト条件※2 に該当したフレームには，VLAN インタフェースの QoS フローリストは適用されません。

注 ※1
コンフィグレーションコマンド ip qos-flow-group，または ipv6 qos-flow-group を示します。

注 ※2
コンフィグレーションコマンド ip qos-flow-list，または ipv6 qos-flow-list で指定された，IP アドレスや TCP ポート番号などを示します。

この場合，VLAN インタフェースに設定されている QoS フローリストの統計情報も計上しません。

(d) CoS 値とユーザ優先度の同時指定

CoS 値とユーザ優先度を同時に指定した場合のユーザ優先度は，CoS 指定した値に従い設定されます。

3.1.4 フロー検出使用時の注意事項

(1) QoS の収容条件について

どのインタフェースからも参照されない QoS フローリスト※ が設定されている場合，収容条件（コンフィグレーションガイド Vol.1 3.2 収容条件」参照）に達する前に，QoS フローリストが設定できなくなる場合があります。その場合は，未使用の QoS フローリストの設定を削除してください。

注 ※　QoS フローリスト：下記コマンドで設定する QoS フローリスト
- ip qos-flow-list
- ipv6 qos-flow-list
- mac qos-flow-list

(2) 複数 QoS エントリー致時の動作

「3.1.3　QoS フローリスト（1）複数の QoS が適用される場合の動作」を参照してください。

(3) VLAN Tag 付きフレームに対する QoS フロー検出

3 段以上の VLAN Tag があるフレームに対して，MAC 条件のイーサネットタイプ，IPv4 条件，または IPv6 条件をフロー検出条件とした QoS フロー検出を実施できません。

2 段の VLAN Tag があるフレームに対して，MAC 条件のイーサネットタイプ，IPv4 条件，または IPv6 条件をフロー検出条件とした QoS フロー検出を受信側で実施するためには，次の条件のどちらかを満たす必要があります。
- 本装置で VLAN トンネリング機能が動作していない
- 本装置で VLAN トンネリング機能が動作していて，フレームを受信したポートがトランクポートである

(4) IPv4 フラグメントパケットに対する QoS フロー検出

IPv4 フラグメントパケットに対して TCP/UDP ヘッダ・ICMP ヘッダをフロー検出条件とした QoS フロー検出を行った場合，2 番目以降のフラグメントパケットは TCP/UDP ヘッダ・ICMP ヘッダがフレーム内にないため検出できません。フラグメントパケットを含めた QoS フロー検出を実施する場合は，フ

ロー検出条件に MAC ヘッダ，IP ヘッダを指定してください。

（5） IPv6 アドレス使用時の自装置宛てユニキャストパケットの QoS フロー検出

IPv6 アドレスを使用時，コンフィグレーションコマンド qos で以下を設定していると，当該フレームを受信できません。

- フロー検出条件　自装置宛てユニキャストフレーム，動作パラメータ CoS 値を 0 に指定（action cos 0）

当該フレームの CoS 値を指定する場合は，1 以上を指定してください。

（6） 拡張ヘッダのある IPv6 パケットに対する QoS フロー検出

IPv6 拡張ヘッダのある IPv6 パケットに対して TCP/UDP ヘッダ・ICMP ヘッダをフロー検出条件とした QoS フロー検出はできません。拡張ヘッダのあるパケットに対して QoS フロー検出を実施する場合は，フロー検出条件に MAC ヘッダ，IPv6 ヘッダを指定してください。

（7） QoS エントリ変更時の動作

本装置では，インタフェースに適用済みの QoS エントリを変更すると，変更が反映されるまでの間，検出の対象となるフレームが検出されなくなります。そのため，一時的にほかの QoS エントリで検出される場合があります。

（8） コンフィグレーション変更時の統計情報について

QoS フローリストに関連したコンフィグレーションを変更した際，変更したエントリ以外の統計カウンタが瞬間的にカウントを停止しますが，それ以外の QoS 機能は正常に動作しています。

（9） IPv4 プロトコル検出について

プロトコル名称 ah またはプロトコル番号 51 は，フロー検出条件として指定しても検出できません。

（10） 他機能との同時使用

（a） 他機能と同時使用時の統計情報について

以下の場合フレームは廃棄しますが，インタフェースに対して QoS エントリを設定し一致した場合，一致した QoS エントリの統計情報が採られます。

- VLAN のポートのデータ転送状態が Blocking（データ転送停止中）の状態で，該当ポートからフレームを受信した場合
- ポート間中継遮断機能で指定したポートからフレームを受信した場合
- ネイティブ VLAN をトランクポートで送受信する VLAN に設定しないで，VLAN Tag なしフレームを受信した場合
- トランクポートで送受信する VLAN に設定していない VLAN Tag 付きフレームを受信した場合
- 廃棄動作を指定したフィルタエントリ（暗黙の廃棄のエントリを含む）に一致するフレームを受信した場合
- プロトコルポートおよび MAC ポートで VLAN Tag 付きフレームを受信した場合
- MAC アドレス学習機能によってフレームが廃棄された場合
- レイヤ 2 認証によってフレームが廃棄された場合
- レイヤ 2 プロトコルが無効なためフレームが廃棄された場合
- IGMP snooping および MLD snooping によってフレームが廃棄された場合
- DHCP snooping によってフレームが廃棄された場合
- ストームコントロールによってフレームが廃棄された場合

(b) ポートミラーリング機能との共存について

ポートミラーリング機能の ICMP 限定ミラーリングを使用する場合は制限があります。詳細は「26.1.2 ポートミラーリング使用時の注意事項」を参照してください。

(c) ポリシーベースミラーリング機能との共存について

ポリシーベースミラーリング機能を使用する場合は制限があります。詳細は「26.1.2　ポートミラーリング使用時の注意事項」を参照してください。

3.2 フロー検出のコンフィグレーション

3.2.1 受信側フロー検出モードの設定

QoS 制御の受信側フロー検出モードを指定する例を示します。

［設定のポイント］

受信側フロー検出モードは，ハードウェアの基本的な動作条件を決定するため，最初に設定します。

［コマンドによる設定］

1. **(config)# flow detection mode layer2-2**
   受信側フロー検出モード layer2-2 を有効にします。

3.2.2 複数インタフェースの QoS 制御の指定

複数のイーサネットインタフェースに QoS 制御を指定する例を示します。

［設定のポイント］

config-if-range モードで QoS 制御を有効に設定することで，複数のイーサネットインタフェースに QoS 制御を設定できます。

［コマンドによる設定］

1. **(config)# ip qos-flow-list QOS-LIST1**
   IPv4 QoS フローリスト（QOS-LIST1）を作成します。本リストを作成することによって，IPv4 QoS フローリストモードに移行します。

2. **(config-ip-qos)# qos ip any host 192.168.100.10 action cos 6**
   192.168.100.10 の IP アドレスを宛先とし，CoS 値＝ 6 の QoS フローリストを設定します。

3. **(config-ip-qos)# exit**
   IPv4 QoS フローリストモードからグローバルコンフィグレーションモードに戻ります。

4. **(config)# interface range gigabitethernet 0/1-4**
   ポート 0/1-4 のインタフェースモードに移行します。

5. **(config-if-range)# ip qos-flow-group QOS-LIST1 in**
   (config-if-range)# exit
   受信側に IPv4 QoS フローリストを有効にします。

3.2.3 TCP/UDP ポート番号の範囲で QoS 制御する設定

UDP ポート番号の範囲をフロー検出条件とし，QoS 制御を設定する例を示します。

［設定のポイント］

フレーム受信時に UDP ヘッダの宛先ポート番号の範囲によってフロー検出を行い，QoS 制御を実施します。

［コマンドによる設定］

1. **(config)# ip qos-flow-list QOS-LIST1**
   IPv4 QoS フローリスト（QOS-LIST1）を作成します。本リストを作成することによって，IPv4 QoS フローリストモードに移行します。

2. **(config-ip-qos)# qos udp any any range 10 20 action cos 6**
   UDP ヘッダの宛先ポート番号の範囲 10 ～ 20 をフロー検出条件とし，CoS 値＝ 6 の QoS フローリストを設定します。

3. **(config-ip-qos)# exit**
   IPv4 QoS フローリストモードからグローバルコンフィグレーションモードに戻ります。

4. **(config)# interface gigabitethernet 0/1**
   ポート 0/1 のインタフェースモードに移行します。

5. **(config-if)# ip qos-flow-group QOS-LIST1 in**
   (config-if)# exit
   受信側に IPv4 QoS フローリストを有効にします。

3.3　フロー検出のオペレーション

運用コマンド show qos-flow によって，設定した内容が反映されているかどうかを確認します。

3.3.1　IPv4 パケットをフロー検出条件とした QoS 制御の動作確認

IPv4 パケットをフロー検出条件とした QoS 制御の動作確認の方法を次の図に示します。

図 3-2　IPv4 パケットをフロー検出条件とした QoS 制御の動作確認

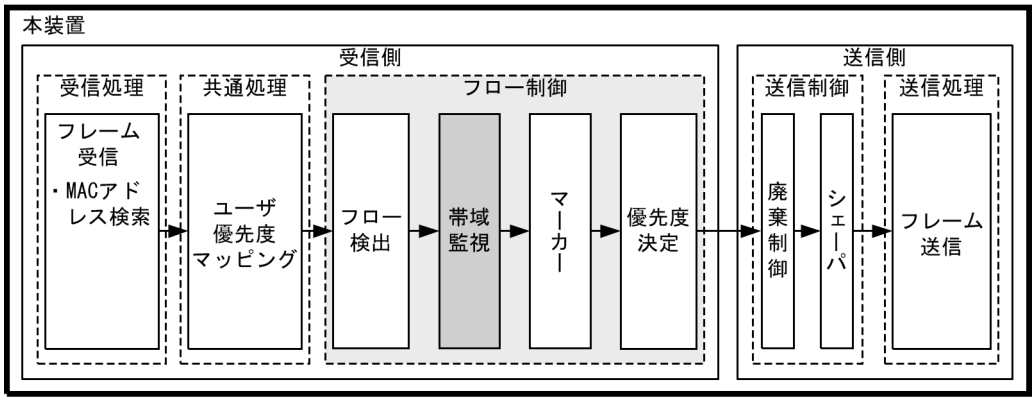
```
> show qos-flow 0/1 QOS_LIST_IP

Date 20XX/05/20 17:45:06 UTC
Using Port:0/1 in
IP qos-flow-list:QOS_LIST_IP
  remark "cos 1"
  10 qos udp any range 10000 65535 any action cos 1
    matched packets         :       2531

>
```

指定したポートの QoS 制御に「IP qos-flow-list」を表示することを確認します。

3.4 帯域監視解説

帯域監視は，フロー検出で検出したフローの帯域を監視する機能です。この節で説明する帯域監視の位置づけを次の図に示します。

図 3-3 帯域監視の位置づけ



（凡例）：この節で説明するブロック

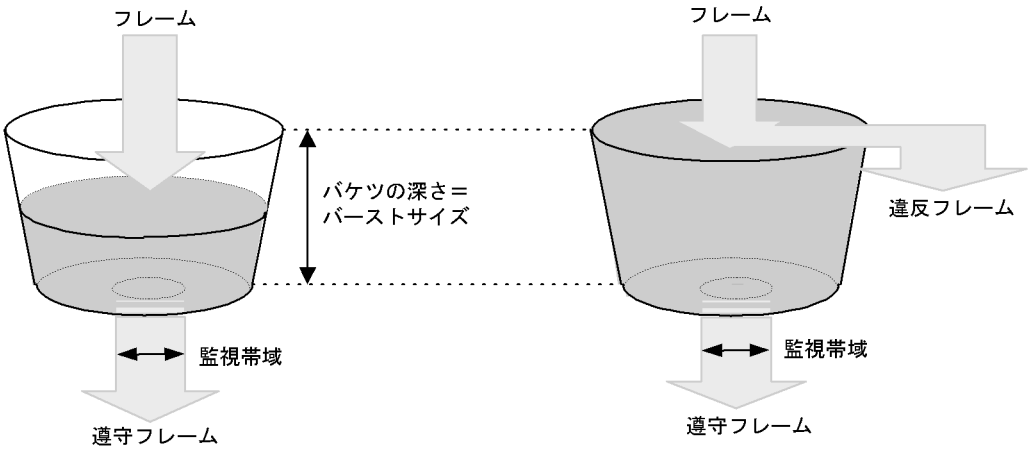
3.4.1 帯域監視

フロー検出で検出したフレームのフレーム長（MAC アドレスから FCS まで）を基に帯域を監視する機能です。指定した監視帯域内として中継するフレームを「遵守フレーム」，監視帯域以上としてペナルティを科すフレームを「違反フレーム」と呼びます。

フロー検出で検出したフレームが監視帯域を遵守しているかまたは違反しているかの判定には，水の入った穴の開いたバケツをモデルとする，Leaky Bucket アルゴリズムを用いています。

Leaky Bucket アルゴリズムのモデルを次の図に示します。

図 3-4 Leaky Bucket アルゴリズムのモデル



バケツからは監視帯域分の水が流れ，フレーム受信時には MAC アドレスから FCS までのサイズの水が注ぎ込まれます。水が注ぎ込まれる際にバケツがあふれていなければ，遵守フレームとして中継されます（上図の左側の例）。水が注ぎ込まれる際にバケツがあふれている場合は，フロー検出で検出したフレームを違反フレームとしてペナルティを科します（上図の右側の例）。水が一時的に大量に注ぎ込まれたときに

許容できる量，すなわちバケツの深さがバーストサイズに対応します。

デフォルトコンフィグレーションのバーストサイズは 32kbyte ですが，より帯域の揺らぎが大きいトラフィックの遵守フレームを中継する際には，バッファサイズを大きく設定し使用してください。

本機能は，最低帯域監視と最大帯域制御から成り，最低帯域監視と最大帯域制御で使用できるペナルティの種類を次の表に示します。

表 3-4　最低帯域監視と最大帯域制御で使用できるペナルティの種類

違反フレームに対するペナルティ	帯域監視種別	
	最低帯域監視	最大帯域制御
廃棄	－	○
キューイング優先度変更	○	－
DSCP 書き換え	○	－

（凡例）○：使用可能なペナルティ　－：使用不可能なペナルティ

3.4.2　帯域監視使用時に採取可能な統計情報

帯域監視ごとに採取可能な統計情報が異なります。帯域監視使用時に採取可能な統計情報を次の表に示します。

表 3-5　帯域監視使用時に採取可能な統計情報

帯域監視種別	採取可能な統計情報			
	最大帯域違反	最大帯域遵守	最低帯域違反	最低帯域遵守
最低帯域監視	－	－	○	○
最大帯域制御	○	○	－	－
最低帯域監視と最大帯域制御の組み合わせ	○	○	－	－

（凡例）○：採取可能　－：採取不可能

3.4.3　帯域監視使用時の注意事項

（1）帯域監視と送信イーサネットインタフェース・送信キューの関係

次のような場合に，送信イーサネットインタフェースまたは送信キューで遵守フレームを廃棄するおそれがあります。

- 帯域監視で指定する監視帯域値を，該当フローの送信イーサネットインタフェースまたは送信キューの帯域値より大きい値とした場合
- 帯域監視を使用しないフローと使用するフローを，同じ送信イーサネットインタフェースまたは送信キューに送信した場合

特に，複数のフローで複数の帯域監視を使用する場合は，各帯域監視の監視帯域値の合計に注意してください。

（2）プロトコル制御フレームとの帯域監視

本装置では，本装置宛のプロトコル制御フレームも帯域監視対象になります。従って，本装置宛のプロト

コル制御フレームも最大帯域制御違反として廃棄される場合があります。そのため，本装置宛のプロトコル制御フレームを考慮した最大帯域を確保する必要があります。

（3） TCP フレームに対する最大帯域制御の使用

最大帯域制御を使用した場合には，TCP のスロースタートが繰り返されデータ転送速度が極端に遅くなる場合があります。

上記動作を防ぐために，最低帯域監視を使用して，「フレームが廃棄されやすくなるようにキューイング優先度を下げる」の動作を実施するようにしてください。本設定によって，契約帯域を超えてもすぐに廃棄されないで，出力回線が混んできたときだけに廃棄されるようになります。

（4） 複数の QoS エントリに一致した場合の帯域監視

帯域監視機能を指定した QoS フローで複数エントリに一致した場合，帯域監視機能が正しく動作しません。

（5） ほかの機能との同時動作

- 廃棄動作を指定したフィルタエントリ（暗黙の廃棄のエントリを含む）に一致するフレームを受信した場合，フレームは廃棄しますが帯域監視対象になります。
- 帯域監視違反とストーム検出が同時に発生すると，本来，中継されるべきフレームを含め，より多くのフレーム廃棄が発生する場合があります。

3.5 帯域監視のコンフィグレーション

3.5.1 最大帯域制御の設定

［設定のポイント］

フレーム受信時に宛先 IP アドレスによってフロー検出を行い，最大帯域制御を行う帯域監視を設定します。

［コマンドによる設定］

1. **(config)# ip qos-flow-list QOS-LIST1**
   IPv4 QoS フローリスト (QOS-LIST1) を作成します。本リストを作成することによって，IPv4 QoS フローリストモードに移行します。

2. **(config-ip-qos)# qos ip any host 192.168.100.10 action max-rate 5M max-rate-burst 512**
   宛先 IP アドレスが 192.168.100.10 のフローに対し，最大帯域制御の監視帯域 =5Mbit/s，最大帯域制御のバーストサイズ =512kbyte の IPv4 QoS フローリストを設定します。

3. **(config-ip-qos)# exit**
   IPv4 QoS フローリストモードからグローバルコンフィグレーションモードに戻ります。

4. **(config)# interface gigabitethernet 0/1**
   ポート 0/1 のインタフェースモードに移行します。

5. **(config-if)# ip qos-flow-group QOS-LIST1 in**
   (config-if)# exit
   受信側に IPv4 QoS フローリスト (QOS-LIST1) を有効にします。

3.5.2 最低帯域監視違反時のキューイング優先度の設定

［設定のポイント］

フレーム受信時に宛先 IP アドレスによってフロー検出を行い，最低帯域監視を行うことを設定します。最低帯域監視を違反したフレームに対しては，キューイング優先度の変更を行う設定をします。

［コマンドによる設定］

1. **(config)# ip qos-flow-list QOS-LIST2**
   IPv4 QoS フローリスト (QOS-LIST2) を作成します。本リストを作成することによって，IPv4 QoS フローリストモードに移行します。

2. **(config-ip-qos)# qos ip any host 192.168.110.10 action min-rate 1M min-rate-burst 64 penalty-discard-class 1**
   宛先 IP アドレスが 192.168.110.10 のフローに対し，最低監視帯域 =1Mbit/s，最低監視帯域のバーストサイズ =64kbyte，最低帯域監視での違反フレームのキューイング優先度 =1 の IPv4 QoS フローリストを設定します。

3. **(config-ip-qos)# exit**

IPv4 QoS フローリストモードからグローバルコンフィグレーションモードに戻ります。

4. **(config)# interface gigabitethernet 0/3**
   ポート 0/3 のインタフェースモードに移行します。

5. **(config-if)# ip qos-flow-group QOS-LIST2 in**
   (config-if)# exit
   受信側に IPv4 QoS フローリスト (QOS-LIST2) を有効にします。

3.5.3 最低帯域監視違反時の DSCP 書き換えの設定

特定のフローに対して最低帯域監視 (違反フレームは DSCP の書き換え) を実施する場合に設定します。

［設定のポイント］

フレーム受信時に宛先 IP アドレスによってフロー検出を行い，最低帯域監視 (min-rate) を行う帯域監視を設定します。最低監視帯域を違反したフレームに対しては，DSCP 値の変更を行う設定をします。

［コマンドによる設定］

1. **(config)# ip qos-flow-list QOS-LIST3**
   IPv4 QoS フローリスト (QOS-LIST3) を作成します。本リストを作成することによって，IPv4 QoS フローリストモードに移行します。

2. **(config-ip-qos)# qos ip any host 192.168.120.10 action min-rate 1M min-rate-burst 64 penalty-dscp 8**
   宛先 IP アドレスが 192.168.120.10 のフローに対し，最低監視帯域 =1Mbit/s，最低監視帯域のバーストサイズ =64kbyte，最低帯域監視での違反フレームの DSCP 値 =8 の IPv4 QoS フローリストを設定します。

3. **(config-ip-qos)# exit**
   IPv4 QoS フローリストモードからグローバルコンフィグレーションモードに戻ります。

4. **(config)# interface gigabitethernet 0/5**
   ポート 0/5 のインタフェースモードに移行します。

5. **(config-if)# ip qos-flow-group QOS-LIST3 in**
   (config-if)# exit
   受信側に IPv4 QoS フローリスト (QOS-LIST3) を有効にします。

3.5.4 最大帯域制御と最低帯域監視の組み合わせの設定

特定のフローに対して最大帯域制御と最低帯域監視 (違反フレームは DSCP の書き換え) を実施したい場合に設定します。

［設定のポイント］

フレーム受信時に宛先 IP アドレスによってフロー検出を行い，最大帯域制御と最低帯域制御を行う帯域監視を設定します。最低帯域監視を違反したフレームに対しては，DSCP 値の変更を行う設定をします。

［コマンドによる設定］

1. **(config)# ip qos-flow-list QOS-LIST4**
   IPv4 QoS フローリスト (QOS-LIST4) を作成します。本リストを作成することによって，IPv4 QoS フローリストモードに移行します。

2. **(config-ip-qos)# qos ip any host 192.168.130.10 action max-rate 5M max-rate-burst 512 min-rate 1M min-rate-burst 64 penalty-dscp 8**
   宛先 IP アドレスが 192.168.130.10 のフローに対し，最大帯域制御の監視帯域 =5Mbit/s，最大帯域制御のバーストサイズ =512kbyte，最低監視帯域 =1Mbit/s，最低監視帯域のバーストサイズ =64kbyte，最低帯域監視での違反フレームの DSCP 値 =8 の IPv4 QoS フローリストを設定します。

3. **(config-ip-qos)# exit**
   IPv4 QoS フローリストモードからグローバルコンフィグレーションモードに戻ります。

4. **(config)# interface gigabitethernet 0/7**
   ポート 0/7 のインタフェースモードに移行します。

5. **(config-if)# ip qos-flow-group QOS-LIST4 in**
   (config-if)# exit
   受信側に IPv4 QoS フローリスト (QOS-LIST4) を有効にします。

3.6 帯域監視のオペレーション

運用コマンド show qos-flow によって，設定した内容が反映されているかどうかを確認します。

3.6.1 最大帯域制御の確認

最大帯域制御の確認方法を次の図に示します。

図 3-5 最大帯域制御の確認

```
> show qos-flow 0/1

Date 20XX/05/20 13:00:00 UTC
Using Port:0/1 in
IP qos-flow-list:QOS-LIST1
  10 qos ip any host 192.168.100.10 action max-rate 5000 max-rate-burst 512
    matched packets(max-rate over) :   1641076
    matched packets(max-rate under):   6084645

>
```

QOS-LIST1 のリスト情報に「最大帯域制御の監視帯域 (max-rate 5000)」,「最大帯域制御のバーストサイズ (max-rate-burst 512)」が表示されることを確認します。

3.6.2 最低帯域監視違反時のキューイング優先度の確認

最低帯域監視違反時のキューイング優先度の確認方法を次の図に示します。

図 3-6 最低帯域監視違反時のキューイング優先度の確認

```
> show qos-flow 0/3

Date 20XX/05/20 13:00:00 UTC
Using Port:0/3 in
IP qos-flow-list:QOS-LIST2
  10 qos ip any host 192.168.110.10 action min-rate 1000 min-rate-burst 64
penalty-discard-class 1
    matched packets(min-rate over) :2772803018
    matched packets(min-rate under):1687368447

>
```

QOS-LIST2 のリスト情報に「最低監視帯域 (min-rate 1000)」,「最低監視帯域のバーストサイズ (min-rate-burst 64)」,「違反フレームのキューイング優先度 (penalty-discard-class 1)」が表示されることを確認します。

3.6.3 最低監視帯域違反時の DSCP 書き換えの確認

最低監視帯域違反時の DSCP 書き換えの確認方法を次の図に示します。

図 3-7 最低監視帯域違反時の DSCP 書き換えの確認

```
> show qos-flow 0/5

Date 20XX/05/20 13:00:00 UTC
Using Port:0/5 in
IP qos-flow-list:QOS-LIST3
  10 qos ip any host 192.168.120.10 action min-rate 1000 min-rate-burst 64
```

```
penalty-dscp cs1
    matched packets(min-rate over) :2761106946
    matched packets(min-rate under):1644016892

>
```

QOS-LIST3 のリスト情報に「最低監視帯域 (min-rate 1000)」,「最低監視帯域のバーストサイズ (min-rate-burst 64)」,「違反フレームの DSCP 名称 (penalty-dscp cs1)」が表示されることを確認します。

3.6.4 最大帯域制御と最低帯域監視の組み合わせの確認

最大帯域制御と最低帯域監視の組み合わせの確認方法を次の図に示します。

図 3-8 最大帯域制御と最低帯域監視の組み合わせの確認

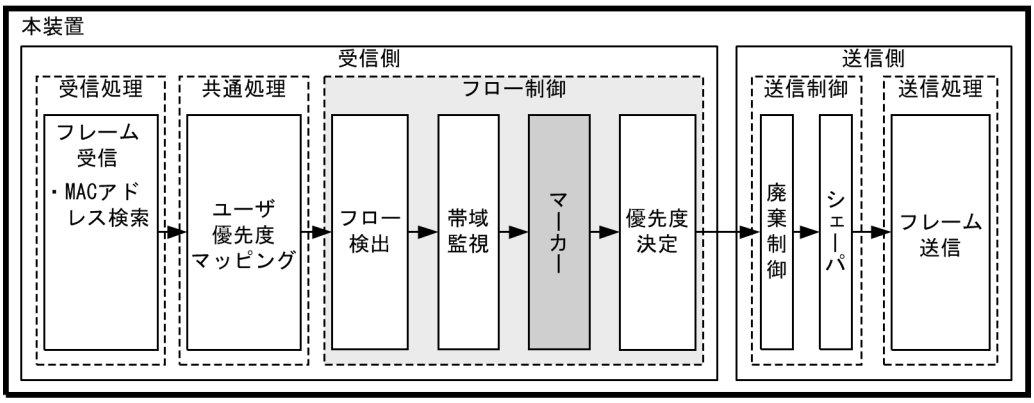
```
> show qos-flow

Date 20XX/05/20 02:22:41 UTC
Using Port:0/7 in
IP qos-flow-list: QOS-LIST4
  10 qos ip any host 192.168.130.10 action max-rate 5000 max-rate-burst 512
min-rate 1000 min-rate-burst 64 penalty-dscp cs1
    matched packets(max-rate over) :    531665
    matched packets(max-rate under):   1037839

>
```

QOS-LIST4 のリスト情報に「最大帯域制御の監視帯域 (max-rate 5000)」,「最大帯域制御のバーストサイズ (max-rate-burst 512)」,「最低監視帯域 (min-rate 1000)」,「最低監視帯域のバーストサイズ (min-rate-burst 64)」,「違反フレームの DSCP 名称 (penalty-dscp cs1)」が表示されることを確認します。

3.7　マーカー解説

マーカーは，フロー検出で検出したフレームの VLAN Tag 内のユーザ優先度および IP ヘッダ内の DSCP を書き換える機能です。この節で説明するマーカーの位置づけを次の図に示します。

図 3-9　マーカーの位置づけ

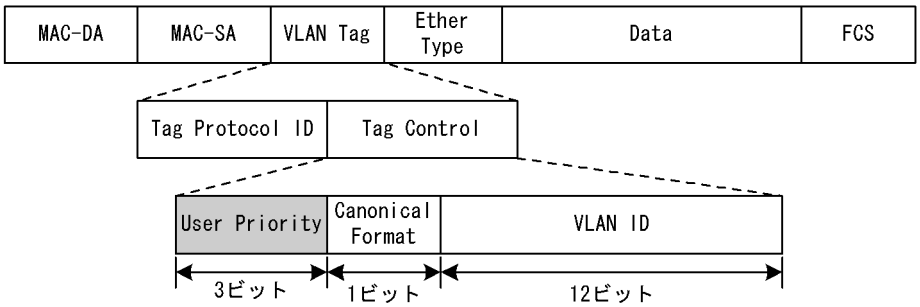


（凡例）：この節で説明するブロック

3.7.1　ユーザ優先度書き換え

フロー検出で検出したフレームの VLAN Tag 内にあるユーザ優先度（User Priority）を書き換える機能です。ユーザ優先度は，次の図に示す Tag Control フィールドの先頭 3 ビットを指します。

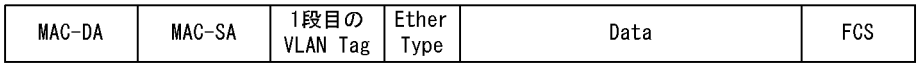
図 3-10　VLAN Tag のヘッダフォーマット



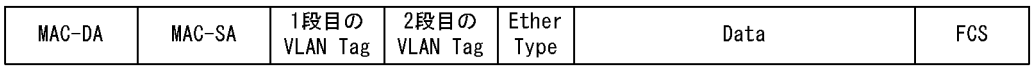
VLAN Tag が複数あるフレームに対してユーザ優先度書き換えを行う場合，MAC アドレス側から 1 段目の VLAN Tag にあるユーザ優先度を書き換えます。次の図に VLAN Tag が複数あるフレームフォーマットを示します。

図 3-11　VLAN Tag が複数あるフレームフォーマットの概略図

（i）VLAN Tag 1段のフォーマット



（ii）VLAN Tag 2段のフォーマット



次のフレームについてはユーザ優先度を書き換えることができません。

- VLAN トンネリングを設定したポートで送信するフレーム

ユーザ優先度書き換えを実施しない場合は，次の表に示すユーザ優先度となります。

表 3-6 フレーム送信時のユーザ優先度

フレーム送信時のユーザ優先度	対象となるフレーム
3	• VLAN Tag なしで受信し，VLAN Tag ありで送信するフレーム • VLAN トンネリング機能で，アクセス回線からバックボーン回線に中継するフレーム
受信フレームのユーザ優先度	• VLAN トンネリング機能で，アクセス回線からアクセス回線に中継する VLAN Tag ありフレーム • Tag 変換を設定してない，かつ VLAN トンネリングを設定していないポートで VLAN Tag ありフレームを受信し，VLAN Tag ありで送信するフレーム

優先度決定機能と同時に設定した場合，優先度決定機能で決定した CoS 値に応じて固定的にユーザ優先度を決定します。

優先度決定機能とユーザ優先度書き換え機能を同時に設定した場合のユーザ優先度を次の表に示します。

表 3-7 優先度決定機能とユーザ優先度書き換え機能を同時に設定した場合のユーザ優先度

優先度決定機能で決定した CoS 値	ユーザ優先度
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

3.7.2 DSCP 書き換え

IPv4 ヘッダの TOS フィールドまたは IPv6 ヘッダのトラフィッククラスフィールドの上位 6 ビットである DSCP 値を書き換える機能です。TOS フィールドのフォーマット，およびトラフィッククラスフィールドのフォーマットの図を次に示します。

図 3-12　TOS フィールドのフォーマット

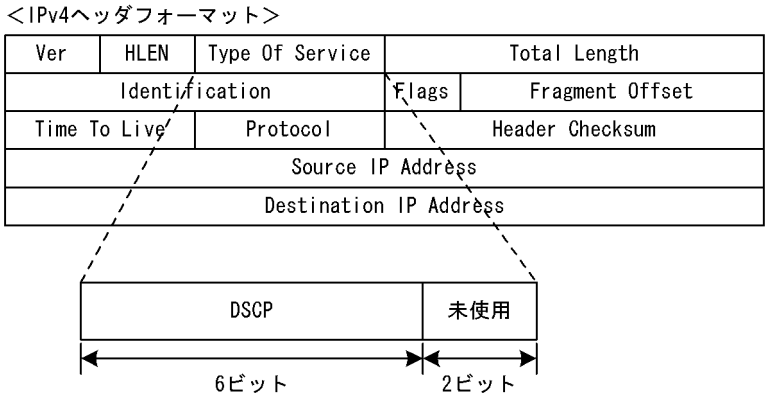
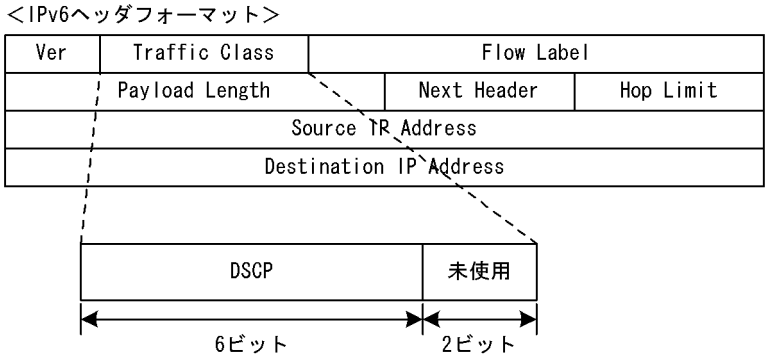


図 3-13　トラフィッククラスフィールドのフォーマット



検出したフローの TOS フィールドまたはトラフィッククラスフィールドの上位 6 ビットを書き換えます。

3.8 マーカーのコンフィグレーション

3.8.1 ユーザ優先度書き換えの設定

特定のフローに対してユーザ優先度を書き換える場合に設定します。

［設定のポイント］

フレーム受信時に宛先 IP アドレスによってフロー検出を行い，ユーザ優先度の書き換えを設定します。

［コマンドによる設定］

1. **(config)# ip qos-flow-list QOS-LIST1**
   IPv4 QoS フローリスト（QOS-LIST1）を作成します。本リストを作成することによって，IPv4 QoS フローリストモードに移行します。

2. **(config-ip-qos)# qos ip any host 192.168.100.10 action replace-user-priority 6**
   192.168.100.10 の IP アドレスを宛先とし，ユーザ優先度を 6 に書き換える IPv4 QoS フローリストを設定します。

3. **(config-ip-qos)# exit**
   IPv4 QoS フローリストモードからグローバルコンフィグレーションモードに戻ります。

4. **(config)# interface gigabitethernet 0/1**
   ポート 0/1 のインタフェースモードに移行します。

5. **(config-if)# ip qos-flow-group QOS-LIST1 in**
   (config-if)# exit
   受信側の IPv4 QoS フローリスト（QOS-LIST1）を有効にします。

3.8.2 DSCP 書き換えの設定

特定のフローに対して DSCP を書き換える場合に設定します。

［設定のポイント］

フレーム受信時に宛先 IP アドレスによってフロー検出を行い，DSCP 値の書き換えを設定します。

［コマンドによる設定］

1. **(config)# ip qos-flow-list QOS-LIST2**
   IPv4 QoS フローリスト（QOS-LIST2）を作成します。本リストを作成することによって，IPv4 QoS フローリストモードに移行します。

2. **(config-ip-qos)# qos ip any host 192.168.100.10 action replace-dscp 63**
   192.168.100.10 の IP アドレスを宛先とし，DSCP 値を 63 に書き換える IPv4 QoS フローリストを設定します。

3. **(config-ip-qos)# exit**
   IPv4 QoS フローリストモードからグローバルコンフィグレーションモードに戻ります。

4. **(config)# interface gigabitethernet 0/3**
   ポート 0/3 のインタフェースモードに移行します。

5. **(config-if)# ip qos-flow-group QOS-LIST2 in**
   (config-if)# exit
   受信側の IPv4 QoS フローリスト（QOS-LIST2）を有効にします。

3.9 マーカーのオペレーション

運用コマンド show qos-flow によって，設定した内容が反映されているかどうかを確認します。

3.9.1 ユーザ優先度書き換えの確認

ユーザ優先度書き換えの確認方法を次の図に示します。

図 3-14 ユーザ優先度書き換えの確認

```
> show qos-flow 0/2

Date 20XX/05/20 10:30:24 UTC
Using Port:0/2 in
IP qos-flow-list:QOS-LIST10
  remark "cos 4"
  10 qos ip any host 192.168.100.10 action replace-user-priority 6
    matched packets         :          0

>
```

QOS-LIST10 のリスト情報に「replace-user-priority 6」を表示することを確認します。

3.9.2 DSCP 書き換えの確認

DSCP 書き換えの確認方法を次の図に示します。

図 3-15 DSCP 書き換えの確認

```
> show qos-flow 0/3

Date 20XX/05/20 10:35:24 UTC
Using Port:0/3 in
IP qos-flow-list:QOS-LIST20
  remark "cos 4"
  10 qos ip any host 192.168.100.10 action replace-dscp 63
    matched packets         :          0

>
```

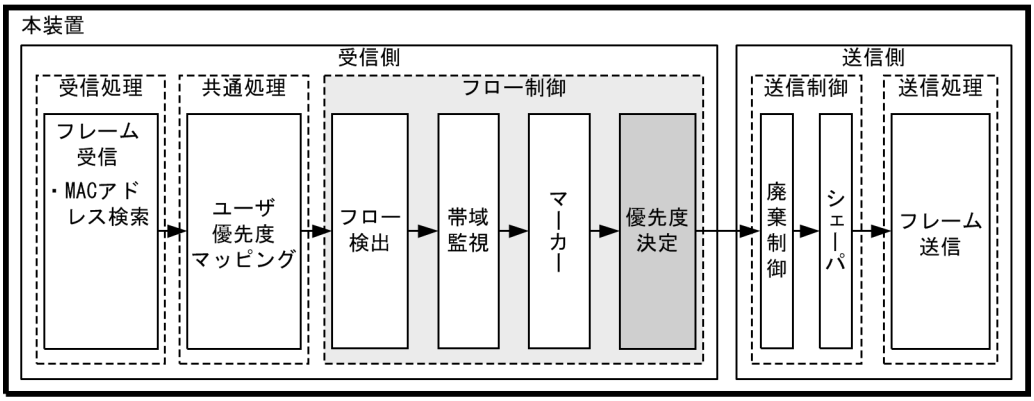
QOS-LIST20 のリスト情報に「replace-dscp 63」を表示することを確認します。

3.10　優先度決定の解説

優先度決定は，フロー検出で検出したフレームの優先度を CoS 値で指定して，送信キューを決定する機能です。

この節で説明する優先度決定の位置づけを次の図に示します。

図 3-16　優先度決定の位置づけ



（凡例）：この節で説明するブロック

3.10.1　CoS 値・キューイング優先度

CoS 値は，フレームの装置内における優先度を表すインデックスを示します。キューイング優先度は，キューイングする各キューに対して廃棄されやすさの度合いを示します。

CoS 値とキューイング優先度の指定範囲を次の表に示します。

表 3-8　CoS 値とキューイング優先度の指定範囲

項目	指定範囲
CoS 値	0 ～ 7
キューイング優先度	1 ～ 3

また，フロー制御の優先度決定が設定されていない場合は，次の表に示す CoS 値とキューイング優先度のデフォルトコンフィグレーションを使用します。

表 3-9　CoS 値とキューイング優先度のデフォルトコンフィグレーション

項目	デフォルトコンフィグレーション	対象となるフレーム
CoS 値	ユーザ優先度マッピングに従います	• フロー制御の優先度決定に一致しないフレーム • フロー制御の優先度決定に一致し，かつ優先度決定を設定しないフレーム
キューイング優先度	3	• フロー検出で検出しないフレーム • フロー検出で検出し，優先度決定（キューイング優先度値の指定）を実施しないフレーム

なお，次に示すフレームは，フロー制御の優先度決定の有無にかかわらず，固定的に CoS 値を決定します。

優先度決定で変更できないフレームを次の表に示します。

表 3-10 優先度決定で変更できないフレーム一覧

フレーム種別	CoS 値
本装置が自発的に送信するフレーム （IP パケット：Ping，Telnet，FTP など）	※1
本装置が自発的に送信するフレーム （IP パケット以外：BPDU，LLDP，LACP，Ring Protocol など）※2	7
本装置が受信するフレームのうち次のフレーム • スパニングツリー (BPDU) • リンクアグリゲーション • LLDP※3 • GSRP (GSRP aware) • CFM • L2 ループ検知フレーム • Ring Protocol	7
本装置が受信するフレームのうち次のフレーム • 本装置 MAC アドレス宛のフレーム • フラッシュ制御フレーム（アップリンク・リダンダント用）	6
本装置が受信するフレームのうち次のフレーム • IGMP/MLD snooping • EAPOL※3 • 回線テストに使用するフレーム	5
本装置が受信するフレームのうち次のフレーム • IPv4 マルチキャストフレーム ※3 • IPv6 マルチキャストフレーム ※3※4 • Web 認証 /MAC 認証対象フレーム ※3 • ブロードキャストフレーム ※3 • ARP フレーム ※5	4
上記にないマルチキャストフレーム ※3	0

注 ※1

フロー制御による優先度決定では変更できませんが，コンフィグレーションコマンド control-packet user-priority の設定によりマッピングされます。

なお，IGMP/MLD フレームは，コンフィグレーションコマンド control-packet user-priority を設定しても，マッピングされる CoS 値は固定です。

詳細は後述の「3.13 自発フレームのユーザ優先度の解説」を参照してください。

注 ※2

VLAN Tag ありの BPDU と L2 ループ検知，およびアップリンク・リダンダント用フラッシュ制御フレームはここに分類されます。

注 ※3

スタック動作時は，優先度決定で変更できます。

スタンドアロン動作時は，システム受信モードを受信条件重視モード（コンフィグレーションコマンド system control fine）設定時に，優先度決定で変更できます。システム受信モードについては，「コンフィグレーションガイド Vol.1 13 装置の管理」を参照してください。

注 ※4

アドレス 3333.0000.0001，3333.ff00.0000 ～ 3333.ffff.ffff のフレームが対象です。

注 ※5

ダイナミック ARP 検査有効時（コンフィグレーションコマンド ip arp inspection vlan 設定時）は，優先度決定で変更できません。

キューイング優先度は，フロー制御の優先度決定により変更できます。しかし，IP パケット以外の本装置が自発的に送信するフレームについては，変更できません（デフォルトコンフィグレーション固定です）。

3.10.2 CoS マッピング機能

CoS マッピング機能は，ユーザ優先度マッピングで決定した CoS 値，またはフロー制御の優先度決定で指定した CoS 値に基づいて，送信キューを決定する機能です。

CoS 値と送信キューのマッピングを次の表に示します。

表 3-11 CoS 値と送信キューのマッピング

CoS 値	送信時のキュー番号		
	送信キュー長：64	送信キュー長：128	送信キュー長：728
0	1	1	1
1	2	1	1
2	3	2	1
3	4	2	1
4	5	3	1
5	6	3	1
6	7	4	1
7	8	4	2

送信キュー長については，「4.1.2 送信キュー長指定」も参照してください。

3.10.3 優先度決定使用時の注意事項

（1） 本装置宛フレームの優先度決定

本装置では，中継するフレームだけでなく，本装置宛のフレームも QoS フロー検出対象になります。従って，「本装置宛フレームの優先度」を「表 3-10 優先度決定で変更できないフレーム一覧」に示す受信フレームの CoS 値と同等または高い優先度値を設定時，本装置宛の受信フレーム負荷が高くなると，プロトコル制御フレームを受信できなくなることがあります。

このような現象が発生した場合は，「本装置宛フレームの優先度を下げる」動作を実施してください。

3.11 優先度決定のコンフィグレーション

3.11.1 CoS 値の設定

特定のフローに対して CoS 値を設定します。

［設定のポイント］

フレーム受信時に宛先 IP アドレスによってフロー検出を行い，CoS 値を設定します。

［コマンドによる設定］

1. **(config)# ip qos-flow-list QOS-LIST1**
   IPv4 QoS フローリスト（QOS-LIST1）を作成します。本リストを作成することによって，IPv4 QoS フローリストモードに移行します。

2. **(config-ip-qos)# qos ip any host 192.168.100.10 action cos 6**
   192.168.100.10 の IP アドレスを宛先とし，CoS 値＝ 6 の IPv4 QoS フローリストを設定します。

3. **(config-ip-qos)# exit**
   IPv4 QoS フローリストモードからグローバルコンフィグレーションモードに戻ります。

4. **(config)# interface gigabitethernet 0/1**
   ポート 0/1 のインタフェースモードに移行します。

5. **(config-if)# ip qos-flow-group QOS-LIST1 in**
   (config-if)# exit
   IPv4 QoS フローリスト（QOS-LIST1）を有効にします。

3.12　優先度のオペレーション

3.12.1　優先度の確認

回線にトラフィック（宛先 IP アドレスが 192.168.100.10 のフレーム）を注入している状態で，運用コマンド show qos queueing によってキューイングされているキュー番号を確認します。対象のイーサネットインタフェースはポート 0/1 です。

図 3-17　優先度の確認

```
> show qos queueing 0/1

Date 20XX/05/20 10:17:32 UTC
Port 0/1 (outbound)
 Status : Active
 Max_Queue=8, Rate_limit=10000kbit/s, Qmode=pq
  Queue 1: Qlen=     0, Limit_Qlen=   64
  Queue 2: Qlen=     0, Limit_Qlen=   64
  Queue 3: Qlen=     0, Limit_Qlen=   64
  Queue 4: Qlen=     0, Limit_Qlen=   64
  Queue 5: Qlen=     0, Limit_Qlen=   64
  Queue 6: Qlen=     0, Limit_Qlen=   64
  Queue 7: Qlen=     1, Limit_Qlen=   64
  Queue 8: Qlen=     0, Limit_Qlen=   64
   discard packets
    HOL1=          0, HOL2=          0

>
```

Qlen の値がカウントされているのが，Queue7 であることを確認します。

3.13 自発フレームのユーザ優先度の解説

コンフィグレーションコマンド control-packet user-priority により，自発フレームのユーザ優先度を任意の値に変更できます。ユーザ優先度は自発フレームのレイヤ２，レイヤ３の単位で指定できます。指定したユーザ優先度のレイヤと同じレイヤのフレームはすべて同一ユーザ優先度値で動作します。

コンフィグレーション未設定の場合，自発フレームのユーザ優先度は 7 となります。

本設定は，設定値入力後反映されますので，装置の再起動は不要です。

各プロトコルの自発フレーム種別とユーザ優先度設定範囲を次の表に示します。

表 3-12 自発フレーム種別とユーザ優先度設定範囲

自発フレーム種別※	レイヤ	control-packet user-priority の設定範囲		
		ユーザ優先度（デフォルト）	ユーザ優先度指定レイヤ	ユーザ優先度設定範囲
BPDU L2 ループ検知 フラッシュ制御フレーム（アップリンク・リダンダント用） MAC アドレスアップデートフレーム（アップリンク・リダンダント用） CFM Ring Protocol 回線テストに使用するフレーム	2	7	layer-2	0 ～ 7
IP 上で動作するプロトコルフレーム	3	7	layer-3	0 ～ 7

注※

VLAN Tag なしの自発フレームは，ユーザ優先度設定の対象外です。

なお，自発フレームのユーザ優先度を設定した場合，自発フレームの CoS 値は下表のようにマッピングされます。下表に示すレイヤ 2 フレームおよび IGMP/MLD フレームは常に CoS 値 7 にマッピングされ，その他のフレームの CoS 値はユーザ優先度の設定値に従ってマッピングされます。

表 3-13 自発フレームのユーザ優先度設定値と CoS 値のマッピング

自発フレーム種別	control-packet user-priority の設定値		マッピングされる CoS 値
BPDU L2 ループ検知 フラッシュ制御フレーム（アップリンク・リダンダント用） MAC アドレスアップデートフレーム（アップリンク・リダンダント用） CFM Ring Protocol 回線テストに使用するフレーム	layer-2	0 ～ 7	7
IGMP MLD	layer-3		

自発フレーム種別	control-packet user-priority の設定値		マッピングされる CoS 値
IGMP/MLD 以外の IP 上で動作するプロトコルフレーム	layer-3	0	0
		1	1
		2	2
		3	3
		4	4
		5	5
		6	6
		7	7

3.14 自発フレームのユーザ優先度のコンフィグレーション

3.14.1 自発フレームのユーザ優先度の設定

［設定のポイント］

レイヤ単位に自発フレームのユーザ優先度値を設定します。

［コマンドによる設定］

1. **(config)# control-packet user-priority layer-2 5**

   レイヤ２の自発フレームのユーザ優先度を５に設定します。
   指定しなかったレイヤ３の自発フレームのユーザ優先度は７となります。

［設定のポイント］

レイヤ２とレイヤ３両方の自発フレームのユーザ優先度値を設定します。

［コマンドによる設定］

1. **(config)# control-packet user-priority layer-2 5 layer-3 2**

   レイヤ２の自発フレームのユーザ優先度を５，レイヤ３の自発フレームのユーザ優先度を２に設定します。

4 送信制御

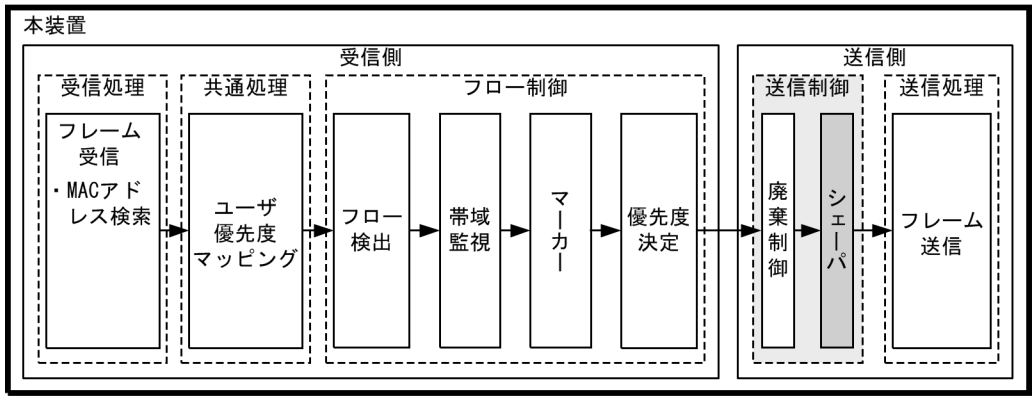
この章では本装置の送信制御（シェーパおよび廃棄制御）について説明します。

4.1　シェーパ解説

4.1.1　レガシーシェーパの概要

シェーパは，フレームの出力順序や出力帯域を制御する機能です。この節で説明するシェーパの位置づけを次の図に示します。

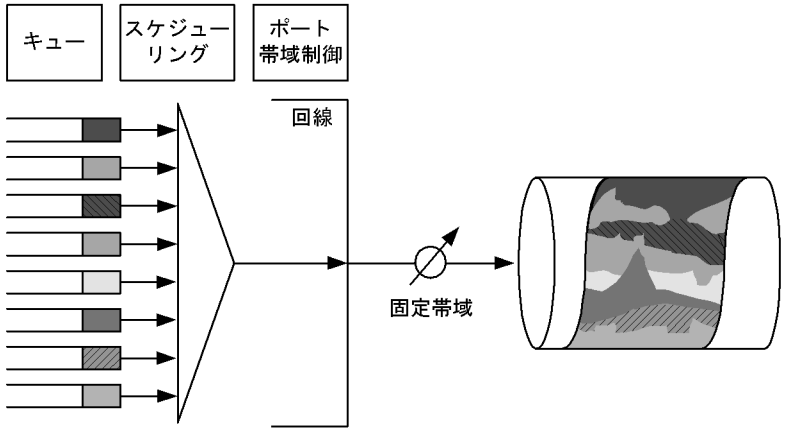
図 4-1　シェーパの位置づけ



（凡例）：この節で説明するブロック

レガシーシェーパは，次の図に示すように，どのキューにあるフレームを次に送信するかを決めるスケジューリングと，イーサネットインタフェースの帯域をシェーピングするポート帯域制御から構成されています。レガシーシェーパの概念を次の図に示します。

図 4-2　レガシーシェーパの概念



（凡例）：固定的に帯域をシェーピング

4.1.2 送信キュー長指定

本装置では，ネットワーク構成や運用形態に合わせて送信キュー長を変更できます。送信キュー長の変更はコンフィグレーションコマンド limit-queue-length で設定します。送信キュー長を拡大することによって，バーストトラフィックによるキューあふれを低減させることができます。なお，設定した送信キュー長は本装置のすべてのイーサネットインタフェースに対して有効になります。

送信キュー長を設定しない場合，キュー長 64 で動作します。

表 4-1 送信キュー長を指定したときの各送信キュー長の状態

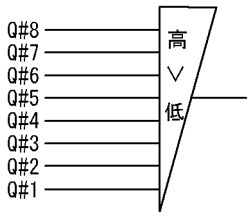
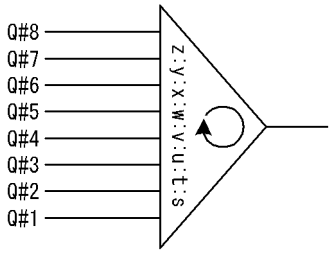
キュー番号	送信キュー長：64	送信キュー長：128	送信キュー長：728
1	64	128	728
2	64	128	64
3	64	128	0
4	64	128	0
5	64	0	0
6	64	0	0
7	64	0	0
8	64	0	0

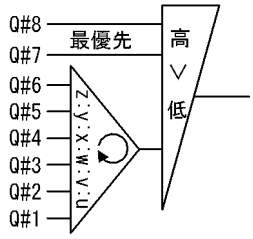
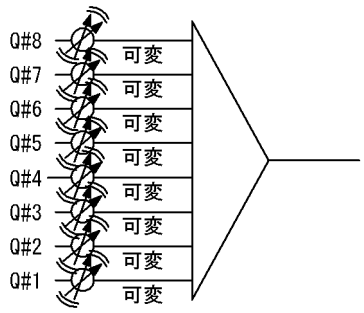
送信キュー長と CoS マッピングは，「表 3-11 CoS 値と送信キューのマッピング」を参照してください。

4.1.3 スケジューリング

スケジューリングは，各キューに積まれたフレームをどのような順序で送信するかを制御する機能です。本装置では，次に示す四つのスケジューリング機能があります。スケジューリングの動作説明を次の表に示します。

表 4-2 スケジューリングの動作説明

スケジューリング種別	概念図	動作説明	適用例
PQ		完全優先。複数のキューにフレームがキューイングされている場合，優先度の高いキュー 8（左図 Q#8）から常に送出します。	トラフィック優先順を完全に遵守する場合
WRR		重み（フレーム数）付きラウンドロビン。複数のキューにフレームが存在する場合，順番にキューを見ながら設定した z：y：x：w：v：u：t：s の重み（フレーム数）に応じて，キュー 8 ～ 1（左図 Q#8 ～ Q#1）からフレームを送出します。	すべてのトラフィックの送信が要求されかつ，優先すべきトラフィックと優先しないトラフィックが混在している場合

スケジューリング種別	概念図	動作説明	適用例
2PQ+6WRR		最優先キューと重み（フレーム数）付きラウンドロビン。最優先のキュー 8（左図 Q#8）は，常に最優先でフレームを送出します。キュー 7（左図 Q#7）は，キュー 8（左図 Q#8）の次に優先的にフレームを送出します。キュー 8,7 の送出がないときに，キュー 6 ～ 1（左図 Q#6 ～ Q#1）は各キュー設定したフレームの重み（z：y：x：w：v：u）に応じてフレームを送出します。	最優先キューに映像，音声，WRR キューにデータ系トラフィック
WFQ		重み付き均等保証。すべてのキューに対して重み（最低保証帯域）を設定し，はじめにキューごとに最低保証帯域分を送出します。	すべてのトラフィックに対し最低帯域保証が要求される場合

スケジューリングの仕様について次の表に示します。

表 4-3　スケジューリング仕様

項目		仕様
キュー数		8 キュー
2PQ+6WRR	キュー 1 ～ 6 の重みの設定範囲	1 ～ 15
WFQ	キュー 1 ～ 8 の重みの設定範囲	「表 4-4　WFQ の設定範囲」を参照してください。最低保証帯域の合計が回線帯域以下になるように設定してください。
	最低保証帯域の対象となるフレームの範囲	MAC ヘッダから FCS まで

WFQ の設定範囲を次の表に示します。回線状態が半二重モードの場合，WFQ は正常に動作しません。全二重モードで使用してください。

表 4-4　WFQ の設定範囲

設定単位 ※1	設定範囲	刻み値
Gbit/s	1G	1Gbit/s
Mbit/s	1M ～ 10000M	1Mbit/s
kbit/s	1000 ～ 10000000	100kbit/s※2
	64 ～ 960	64kbit/s※3

注 ※1

1G，1M，1k はそれぞれ 1000000000，1000000，1000 として扱います（運用コマンドによるコンフィグレーション表示時は，k 単位で表示します）。

注 ※2
設定値が 1000k 以上の場合 100k 刻みで指定します（1000，1100，1200，…，10000000）。

注 ※3
設定値が 1000k 未満の場合 64k 刻みで指定します（64，128，192，…，960）。

4.1.4 ポート帯域制御

ポート帯域制御は，スケジューリングを実施した後に，該当するポートに指定した送信帯域にシェーピングする機能です。この制御を使用して，広域イーサネットサービスへ接続できます。

例えば，回線帯域が 1Gbit/s で ISP との契約帯域が 400Mbit/s の場合，ポート帯域制御機能を使用してあらかじめ帯域を 400Mbit/s 以下に抑えてフレームを送信することができます。

ポート帯域制御の設定範囲を次の表に示します。設定帯域は回線速度以下になるように設定してください。回線状態が半二重モードの場合，ポート帯域制御は動作しません。

表 4-5 ポート帯域制御の設定範囲

設定単位 ※1	設定範囲	刻み値
Gbit/s	1G	1Gbit/s
Mbit/s	1M ～ 10000M	1Mbit/s
kbit/s	1000 ～ 10000000	100kbit/s※2
	64 ～ 960	64kbit/s※3

注 ※1
1G，1M，1k はそれぞれ 1000000000，1000000，1000 として扱います（運用コマンドによるコンフィグレーション表示時は，k 単位で表示します）。

注 ※2
設定値が 1000k 以上の場合 100k 刻みで指定します（1000，1100，1200，…，10000000）。

注 ※3
設定値が 1000k 未満の場合 64k 刻みで指定します（64，128，192，…，960）。

ポート帯域制御の対象となるフレームの範囲は MAC ヘッダから FCS までです。ポート帯域制御の対象範囲を次の図に示します。

図 4-3 ポート帯域制御の対象範囲

4.1.5 シェーパ使用時の注意事項

(1) 送信キュー長指定時の注意事項

- 送信キュー長の設定はハードウェアの基本的な動作条件を設定するため，設定変更後は本装置の再起動が必要になります。（スタック動作時については，「コンフィグレーションガイド Vol.1 7 スタックの解説【OP-WLE】」を参照してください。）
- 送信キュー長の設定前に，スケジューリングモード PQ を設定してください。他のスケジューリングモードでは設定できません。

- コンフィグレーションコマンド limit-queue-length 未設定時は，スケジューリングモードの制限はありません。

(2) パケットバッファ枯渇時のスケジューリングの注意事項

出力回線の帯域を上回るトラフィックを受信したとき，本装置のパケットバッファの枯渇が発生する場合があります。そのため，受信したフレームがキューにキューイングされず廃棄されるため，指定したスケジューリングどおりにフレームが送信されない場合があります。

パケットバッファの枯渇については，運用コマンド show qos queueing の HOL1 または HOL2 カウンタがインクリメントされていることで確認できます。

パケットバッファの枯渇が定常的に発生する場合，ネットワーク設計の見直しが必要です。

4.2 シェーパのコンフィグレーション

4.2.1 PQ の設定

［設定のポイント］

レガシーシェーパモードに PQ（完全優先）を設定した QoS キューリスト情報を作成し，該当するポートに設定します。

［コマンドによる設定］

1. **(config)# qos-queue-list QUEUE-PQ pq**
   QoS キューリスト名称（QUEUE-PQ）のレガシーシェーパモードを完全優先に設定します。

2. **(config)# interface gigabitethernet 0/1**
   ポート 0/1 のインタフェースモードに移行します。

3. **(config-if)# qos-queue-group QUEUE-PQ**
   (config-if)# exit
   QoS キューリスト（QUEUE-PQ）を有効にします。

4.2.2 WRR の設定

［設定のポイント］

レガシーシェーパモードに WRR（重み（フレーム数）付きラウンドロビン）を設定した QoS キューリスト情報を作成し，該当するポートに設定します。

［コマンドによる設定］

1. **(config)# qos-queue-list QUEUE-WRR wrr 1 2 3 4 6 8 10 12**
   QoS キューリスト名称（QUEUE-WRR）のレガシーシェーパモードを WRR に設定します。

2. **(config)# interface gigabitethernet 0/4**
   ポート 0/4 のインタフェースモードに移行します。

3. **(config-if)# qos-queue-group QUEUE-WRR**
   (config-if)# exit
   QoS キューリスト（QUEUE-WRR）を有効にします。

4.2.3 2PQ+6WRR の設定

［設定のポイント］

レガシーシェーパモードに 2PQ+6WRR（最優先キュー＋重み（フレーム数）付きラウンドロビン）を設定した QoS キューリスト情報を作成し，該当するポートに設定します。

［コマンドによる設定］

1. **(config)# qos-queue-list QUEUE-PQ-WRR 2pq+6wrr 1 2 4 4 8 12**
   QoS キューリスト名称（QUEUE-PQ-WRR）のレガシーシェーパモードを 2pq+6wrr に設定します。

2. **(config)# interface gigabitethernet 0/6**
   ポート 0/6 のインタフェースモードに移行します。

3. **(config-if)# qos-queue-group QUEUE-PQ-WRR**
   (config-if)# exit
   QoS キューリスト（QUEUE-PQ-WRR）を有効にします。

4.2.4 WFQ の設定

［設定のポイント］
レガシーシェーパモードに WFQ（重み付き均等保証）を設定した QoS キューリスト情報を作成し，該当するポートに設定します。

［コマンドによる設定］

1. **(config)# qos-queue-list QUEUE-WFQ wfq min-rate1 2M min-rate2 2M min-rate3 2M min-rate4 4M min-rate5 10M min-rate6 10M min-rate7 10M min-rate8 20M**
   QoS キューリスト名称（QUEUE-WFQ）のレガシーシェーパモードを wfq に設定します。

2. **(config)# interface gigabitethernet 0/6**
   ポート 0/6 のインタフェースモードに移行します。

3. **(config-if)# qos-queue-group QUEUE-WFQ**
   (config-if)# exit
   QoS キューリスト（QUEUE-WFQ）を有効にします。

4.2.5 ポート帯域制御の設定

該当するポートの出力帯域を実回線の帯域より低くする場合に設定します。

［設定のポイント］
該当するポート（100Mbit/s）に対し，ポート帯域制御による帯域の設定（20Mbit/s）を行います。

［コマンドによる設定］

1. **(config)# interface gigabitethernet 0/3**
   ポート 0/3 のインタフェースモードに移行します。

2. **(config-if)# traffic-shape rate 20M**
   (config-if)# exit
   ポート帯域を 20Mbit/s に設定します。

4.3 シェーパのオペレーション

運用コマンド show qos queueing によって，イーサネットインタフェースに設定したレガシーシェーパの内容を確認します。

4.3.1 スケジューリングの確認

スケジューリングの確認方法を次の図に示します。

図 4-4 スケジューリングの確認

```
> show qos queueing 0/1

Date 20XX/05/20 12:08:10 UTC
Port 0/1 (outbound)
 Status : Active
 Max_Queue=8, Rate_limit=100000kbit/s, Qmode=pq
  Queue 1: Qlen=    0, Limit_Qlen=   64
  Queue 2: Qlen=    0, Limit_Qlen=   64
  Queue 3: Qlen=    0, Limit_Qlen=   64
  Queue 4: Qlen=    0, Limit_Qlen=   64
  Queue 5: Qlen=    0, Limit_Qlen=   64
  Queue 6: Qlen=    0, Limit_Qlen=   64
  Queue 7: Qlen=    0, Limit_Qlen=   64
  Queue 8: Qlen=    0, Limit_Qlen=   64
   discard packets
    HOL1=         0, HOL2=         0

>
```

Qmode パラメータの内容が，「pq」になっていることを確認します。

4.3.2 ポート帯域制御の確認

ポート帯域制御の確認方法を次の図に示します。

図 4-5 ポート帯域制御の確認

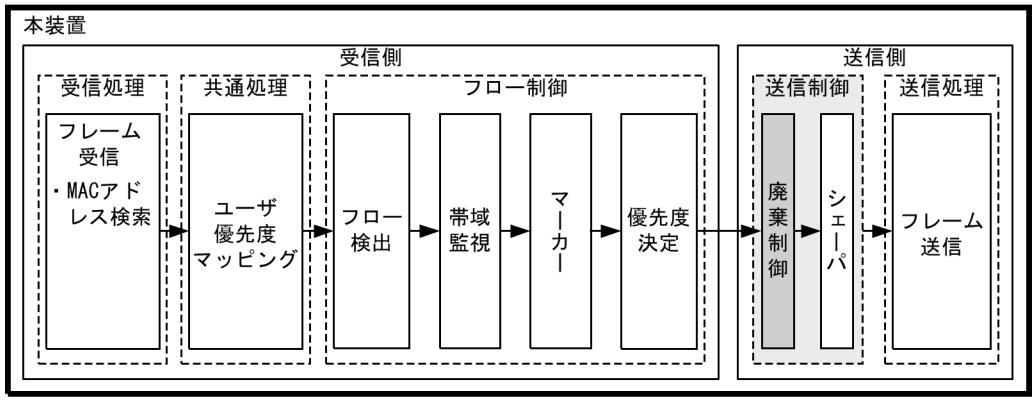
```
> show qos queueing 0/3

Date 20XX/05/20 12:15:23 UTC
Port 0/3 (outbound)
 Status : Active
 Max_Queue=8, Rate_limit=2000kbit/s, Qmode=pq
  Queue 1: Qlen=    0, Limit_Qlen=   64
  Queue 2: Qlen=    0, Limit_Qlen=   64
  Queue 3: Qlen=    0, Limit_Qlen=   64
  Queue 4: Qlen=    0, Limit_Qlen=   64
  Queue 5: Qlen=    0, Limit_Qlen=   64
  Queue 6: Qlen=    0, Limit_Qlen=   64
  Queue 7: Qlen=    0, Limit_Qlen=   64
  Queue 8: Qlen=    0, Limit_Qlen=   64
   discard packets
    HOL1=         0, HOL2=         0

>
```

Rate_limit パラメータの内容が，「2000kbit/s」になっていることを確認します。

4.4 廃棄制御解説

この節で説明する廃棄制御の位置づけを次の図に示します。

図 4-6 廃棄制御の位置づけ



（凡例）：この節で説明するブロック

4.4.1 廃棄制御

廃棄制御は，キューイングする各キューに対して廃棄されやすさの度合いを示すキューイング優先度と，キューにフレームが滞留している量に応じて，該当フレームをキューイングするか廃棄するかを制御する機能です。

キューにフレームが滞留している場合，キューイング優先度を変えることによって，さらにきめ細かいQoSを実現できます。

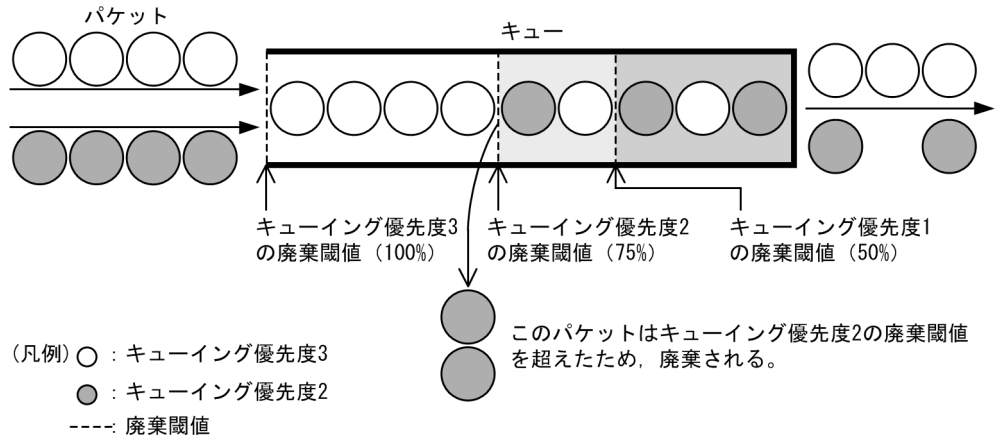
一つのキューにキューイングできるフレーム数を「キュー長」と呼びます。

本装置は，テールドロップ方式で廃棄制御を行います。

(1) テールドロップ

キュー長が廃棄閾値を超えると，フレームを廃棄する機能です。廃棄閾値は，キューイング優先度ごとに異なり，キューイング優先度値が高いほどフレームが廃棄されにくくなります。テールドロップの概念を次の図に示します。キューイング優先度２の廃棄閾値を超えると，キューイング優先度２のフレームをすべて廃棄します。

図 4-7　テールドロップの概念



次に，テールドロップ機能におけるキューイング優先度ごとの廃棄閾値を次の表に示します。廃棄閾値は，キュー長に対するキューの溜まり具合を百分率で表します。

表 4-6　テールドロップの廃棄閾値

キューイング優先度	廃棄閾値［%］
1	50
2	75
3	100

4.5 廃棄制御のコンフィグレーション

4.5.1 キューイング優先度の設定

特定のフローに対してキューイング優先度を設定します。

［設定のポイント］

フレーム受信時に宛先 IP アドレスによってフロー検出を行い，キューイング優先度を設定します。

［コマンドによる設定］

1. **(config)# ip qos-flow-list QOS-LIST2**
   IPv4 QoS フローリスト (QOS-LIST2) を作成します。本リストを作成することによって，IPv4 QoS フローリストモードに移行します。

2. **(config-ip-qos)# qos ip any host 192.168.100.10 action discard-class 2**
   192.168.100.10 の IP アドレスを宛先とし，キューイング優先度 =2 の QoS フローリストを設定します。

3. **(config-ip-qos)# exit**
   IPv4 QoS フローリストモードからグローバルコンフィグレーションモードに戻ります。

4. **(config)# interface gigabitethernet 0/1**
   ポート 0/1 のインタフェースモードに移行します。

5. **(config-if)# ip qos-flow-group QOS-LIST2 in**
   (config-if)# exit
   受信側に IPv4 QoS フローリスト (QOS-LIST2) を有効にします。

4.6 廃棄制御のオペレーション

回線にトラフィック (Queue4 の Qlen が 64 程度の滞留が発生するトラフィック) を注入している状態で，運用コマンド show qos queueing によってキューイングされているキュー番号および廃棄パケット数を確認します。対象のイーサネットインタフェースは，ポート 0/1 です。

4.6.1 キューイング優先度の確認

キューイング優先度の確認方法を次の図に示します。

図 4-8 キューイング優先度の確認

```
> show qos queueing 0/1

Date 20XX/05/20 11:15:31 UTC
Port 0/1 (outbound)
 Status : Active
 Max_Queue=8, Rate_limit=10000kbit/s, Qmode=pq/tail_drop
  Queue 1: Qlen=    0, Limit_Qlen=   64
  Queue 2: Qlen=    0, Limit_Qlen=   64
  Queue 3: Qlen=    0, Limit_Qlen=   64
  Queue 4: Qlen=   48, Limit_Qlen=   64                          … 1,2
  Queue 5: Qlen=    0, Limit_Qlen=   64
  Queue 6: Qlen=    0, Limit_Qlen=   64
  Queue 7: Qlen=    0, Limit_Qlen=   64
  Queue 8: Qlen=    0, Limit_Qlen=   64
   discard packets
    HOL1=   1878332, HOL2=         0, Tail_drop=   1878285     … 2
              :
```

1. Queue4 の Qlen の値がカウントされていることを確認します。
2. Qlen の値が Limit_Qlen の値の 75%であり，discard packets の Tail_drop の値がカウントされていることを確認します。

5 レイヤ 2 認証機能の概説

本装置では，IEEE802.1X，Web 認証，MAC 認証のレイヤ 2 認証機能をサポートしています。この章では本装置のレイヤ 2 認証機能のサポート種別，レイヤ 2 認証共通機能，レイヤ 2 認証の共存について説明します。

5.1　レイヤ２認証機能の概説

5.1.1　レイヤ２認証機能種別

本装置は次の表に示すレイヤ２認証機能をサポートしています。

表 5-1　本装置でサポートするレイヤ２認証機能

認証種別	認証機能	認証方式グループ	認証モード	認証サブモード
シングル認証	IEEE802.1X	装置デフォルト※ 認証方式リスト	ポート単位認証（静的） ポート単位認証（動的）	シングルモード 端末認証モード
	Web 認証	装置デフォルト 認証方式リスト	固定 VLAN モード ダイナミック VLAN モード	－
	MAC 認証	装置デフォルト 認証方式リスト	固定 VLAN モード ダイナミック VLAN モード	－
マルチステップ認証	MAC 認証＋ IEEE802.1X	装置デフォルト※ 認証方式リスト	固定 VLAN モード ダイナミック VLAN モード	IEEE802.1X は端末認証モードで使用
	MAC 認証＋ Web 認証		固定 VLAN モード ダイナミック VLAN モード	－
	IEEE802.1X ＋ Web 認証		固定 VLAN モード ダイナミック VLAN モード	IEEE802.1X は端末認証モードで使用

（凡例）
－：なし

注※
IEEE802.1X の装置デフォルトは，RADIUS 認証で動作します。

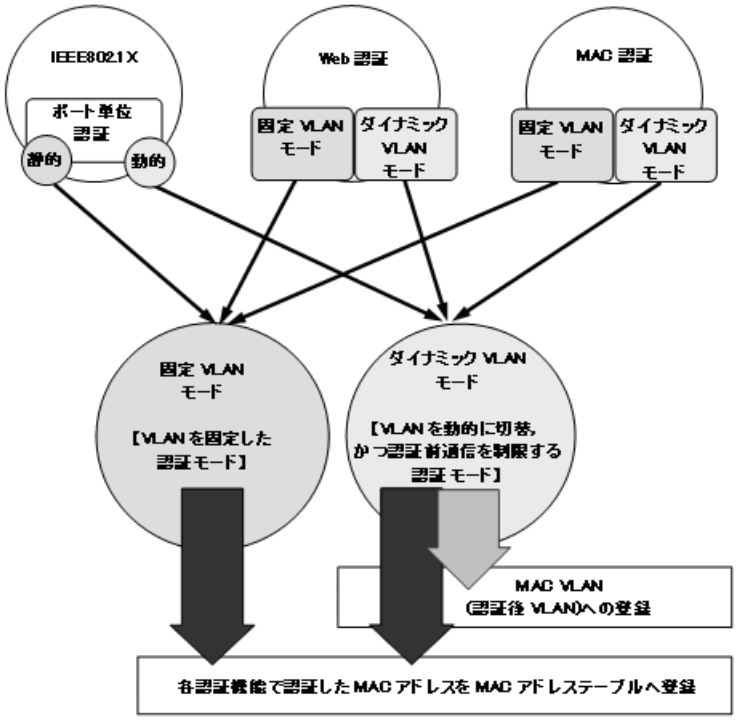
- シングル認証
  IEEE802.1X，Web 認証，MAC 認証がそれぞれ独立して認証を実施し完結します。
- マルチステップ認証
  認証を２段階で実施します。１段目の認証が完了後に，２段目の認証を実施し完結します。本装置では，MAC 認証完了後に，IEEE802.1X または Web 認証を実施します。端末認証 dot1x オプションにより，IEEE802.1X 認証完了後に Web 認証を実施することもできます。
  マルチステップ認証については，後述の「12　マルチステップ認証」を参照してください。
- IEEE802.1X
  IEEE802.1X に準拠したユーザ認証をする機能です。IEEE802.1X 認証に必要な EAPOL フレームを送信する端末を認証します。
  認証サーバとして一般の RADIUS サーバを使用することができ，比較的小規模から中規模のシステムに適しています。
  IEEE802.1X の Supplicant ソフトウェアを持つ端末を使用できます。
- Web 認証
  端末上の汎用 Web ブラウザから入力されたユーザ ID およびパスワードを用いて，内蔵認証データベース（内蔵 Web 認証 DB），または一般の RADIUS サーバを使用して認証を行い，MAC アドレス単位に指定された VLAN へのアクセス許可有無を行う機能です。
  Internet Explorer などの汎用 Web ブラウザを持つ端末を使用できます。

- MAC 認証
  各端末から受信したフレームの MAC アドレスを用いて，内蔵認証データベース（内蔵 MAC 認証 DB），または一般の RADIUS サーバを使用して認証を行い，MAC アドレス単位に指定された VLAN へのアクセス許可有無を行う機能です。これにより，端末側に特別なソフトウェアをインストールすることなく，認証を行うことが可能になります。
  プリンタや IP 電話などの IEEE802.1X の Supplicant ソフトウェアがない，またはユーザ ID およびパスワード入力のできない端末の認証が可能です。

5.1.2 各認証機能の認証モード

各認証機能は，「固定 VLAN モード」「ダイナミック VLAN モード」で動作します。各認証機能と認証モードの対応を次の図に示します。

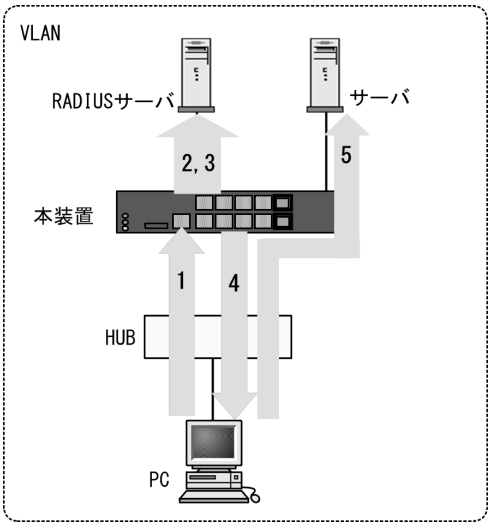
図 5-1 各認証機能と認証モードの対応図



(1) 固定 VLAN モード

固定 VLAN モードは，認証要求端末の VLAN は認証前と認証後で VLAN が変わりません。認証要求端末の所属する VLAN は，端末の接続ポートが所属する VLAN となります。

図 5-2 固定 VLAN モード概要図（RADIUS 認証の例）



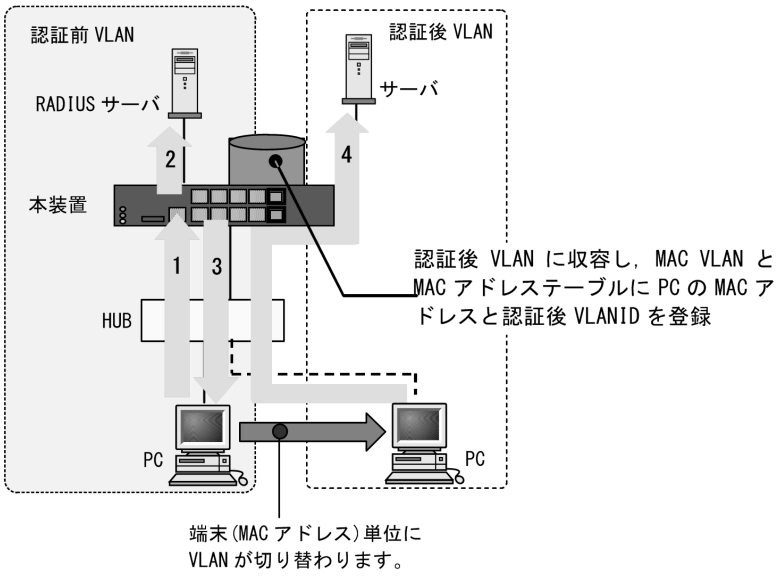
1. HUB などを経由して接続した認証対象端末（図内の PC）から本装置にアクセスします。
2. 認証対象端末の接続ポートまたは VLAN ID により，認証対象端末が所属する VLAN ID を特定します。
3. 端末情報に特定した VLAN ID 情報を加えて RADIUS サーバへ認証要求することで，収容可能な VLAN を制限することが可能となります。
4. 認証成功であれば，ログイン成功画面を端末に表示します。（Web 認証の場合）
5. 認証済み端末は，接続された VLAN のサーバに接続できるようになります。

（2） ダイナミック VLAN モード

ダイナミック VLAN モードは，認証後の VLAN 切り替えを MAC VLAN で実施し，認証に成功した端末の MAC アドレスと VLAN ID を MAC VLAN と MAC アドレステーブルに登録します。

認証前の端末が所属する VLAN を認証前 VLAN と呼びます。また，認証後の VLAN を認証後 VLAN と呼びます。

図 5-3 ダイナミック VLAN モード概要図（RADIUS 認証の例）



1. HUB 経由で接続された認証対象端末（図内の PC）から本装置にアクセスします。
2. 外部に設置された RADIUS サーバに従って認証を行います。
3. 認証成功であれば，ログイン成功画面を端末に表示します。（Web 認証の場合）
4. RADIUS サーバから送られる VLAN ID 情報に従って，認証済み端末を認証後の VLAN に収容して，サーバに接続できるようになります。

（3） 各認証機能の収容条件や混在使用について

各認証機能の収容条件については，「コンフィグレーションガイド Vol.1　3.2　収容条件」を参照してください。

認証機能は装置内および同一ポート内で混在使用できます。詳細は後述の「5.7　レイヤ 2 認証機能の共存使用」を参照してください。

各認証機能の詳細は，後述の各章を参照してください。

5.1.3　認証方式グループ

各認証機能ごとに，装置全体の標準である「装置デフォルト」か，特定条件に合致した際に任意の RADIUS サーバを適用する「認証方式リスト」を選択することができます。

表 5-2　本装置の認証方式グループ

認証方式グループ	選択範囲	認証要求先
装置デフォルト	ローカル認証	内蔵認証データベース
	RADIUS 認証	認証専用 RADIUS サーバ情報のホスト
		汎用 RADIUS サーバ情報のホスト
認証方式リスト	RADIUS サーバグループ	指定した RADIUS サーバグループ内のサーバホスト

（1） 装置デフォルト

各認証機能ごとに装置デフォルトとなる認証方式を設定します。認証方式は，ローカル認証方式と RADIUS 認証方式があります。また，コンフィグレーションにより，ローカル認証方式・RADIUS 認証方式を単独でも同時でも設定できます。詳細は後述の「5.3.3　装置デフォルトのローカル認証と RADIUS 認証の優先設定」を参照してください。

（a） ローカル認証方式

ユーザ ID とパスワードの入力または端末の MAC アドレスと，本装置の内蔵認証データベース（内蔵 Web 認証 DB，内蔵 MAC 認証 DB）を照合し，対象が一致していれば認証を許可する方式です。内蔵認証データベースは運用コマンドで本装置に登録します。

（b） RADIUS 認証方式

ユーザ ID とパスワードの入力または端末の MAC アドレスを RADIUS サーバに送信し，RADIUS サーバで対象が一致していれば認証を許可する方式です。

RADIUS サーバは一般の外部 RADIUS サーバを使用します。RADIUS サーバには認証対象ユーザ（または端末）の情報を登録します。RADIUS サーバのユーザ情報などの登録については，ご使用になる RADIUS サーバのマニュアルを参照してください。

また，本装置には認証要求先 RADIUS サーバの IP アドレスや RADIUS 鍵などの RADIUS サーバ情報を設定します。設定情報には，汎用 RADIUS サーバ情報と認証専用 RADIUS サーバ情報があります。詳細

は，後述の「5.3.1　レイヤ 2 認証機能で使用する RADIUS サーバ情報」を参照してください。

(2) 認証方式リスト

各認証機能ごとに特定の条件で任意の RADIUS サーバを適用する「認証方式リスト」を指定できます。

「認証方式リスト」には，RADIUS サーバグループだけを設定できます。

「認証方式リスト」は，各認証機能ごとに最大 4 エントリまで登録することができます。詳細は後述の「5.2　認証方式グループ」を参照してください。

RADIUS サーバグループは，最大 4 グループまで設定できます。詳細は，後述の「5.3.1　レイヤ 2 認証機能で使用する RADIUS サーバ情報」および「コンフィグレーションガイド Vol.1　10　ログインセキュリティと RADIUS」を参照してください。

5.2 認証方式グループ

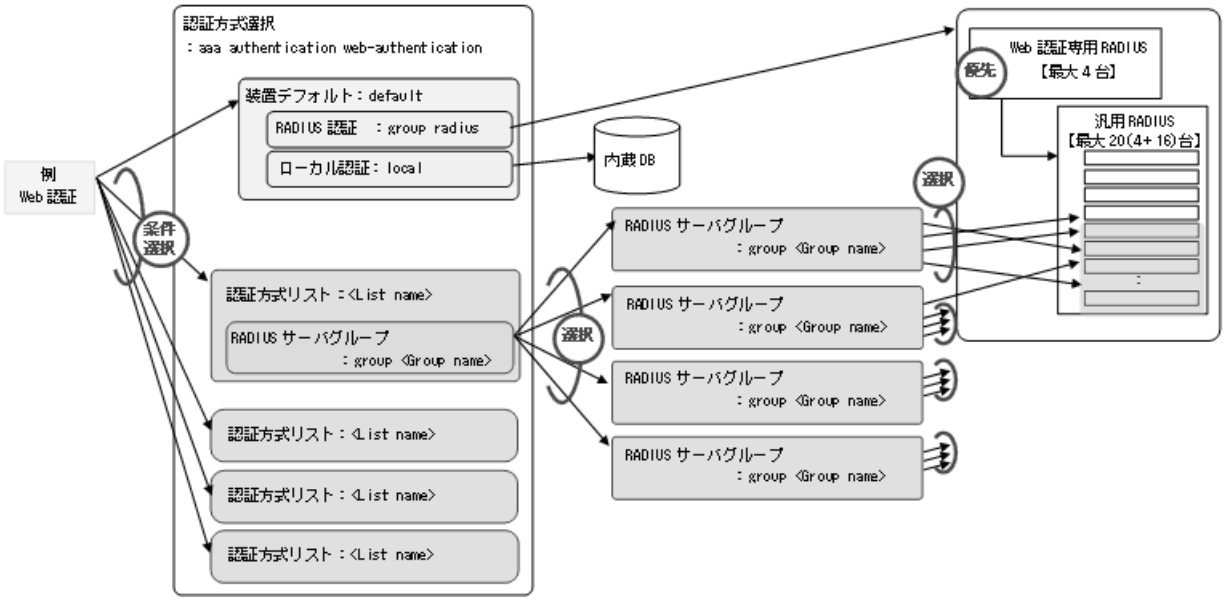
5.2.1 概要

装置標準である「装置デフォルト」の設定と，特定条件に合致した際に任意の RADIUS サーバを適用する「認証方式リスト」設定の相関図を Web 認証を例に説明します。

通常は「装置デフォルト」の設定に従い，ローカル認証，または RADIUS 認証を実施します。

- 装置デフォルト
  「装置デフォルト」で RADIUS 認証を実施する場合，汎用 RADIUS サーバのほかに認証専用 RADIUS サーバを使用することもできます。
  認証専用 RADIUS サーバは，各レイヤ 2 認証機能ごとに，それぞれ 4 台まで RADIUS サーバを設定することができます。
- 認証方式リスト
  「認証方式リスト」機能を使用する場合は，「特定条件」を設定します。
  「特定条件」に合致した際に，適用する「認証方式リスト」に登録されている RADIUS サーバグループ名を参照します。
  RADIUS サーバグループには，汎用 RADIUS サーバとして設定している RADIUS サーバの IP アドレスを指定して引用します。

図 5-4 認証方式リスト設定の相関図



5.2.2 認証方式リスト

認証方式リストは，以下の特定条件で使用します。

- ポート別認証方式
- ユーザ ID 別認証方式

本機能が動作可能な認証モードを次の表に示します。

表 5-3 認証方式リスト指定が動作可能な認証モード

認証機能	認証モード	ポート別認証方式	ユーザ ID 別認証方式
IEEE802.1X	ポート単位認証 (静的)	○	×
	ポート単位認証 (動的)	○	×
Web 認証	固定 VLAN モード	○	○
	ダイナミック VLAN モード	○	○
MAC 認証	固定 VLAN モード	○	×
	ダイナミック VLAN モード	○	×

(凡例)
○：動作可能
×：動作不可

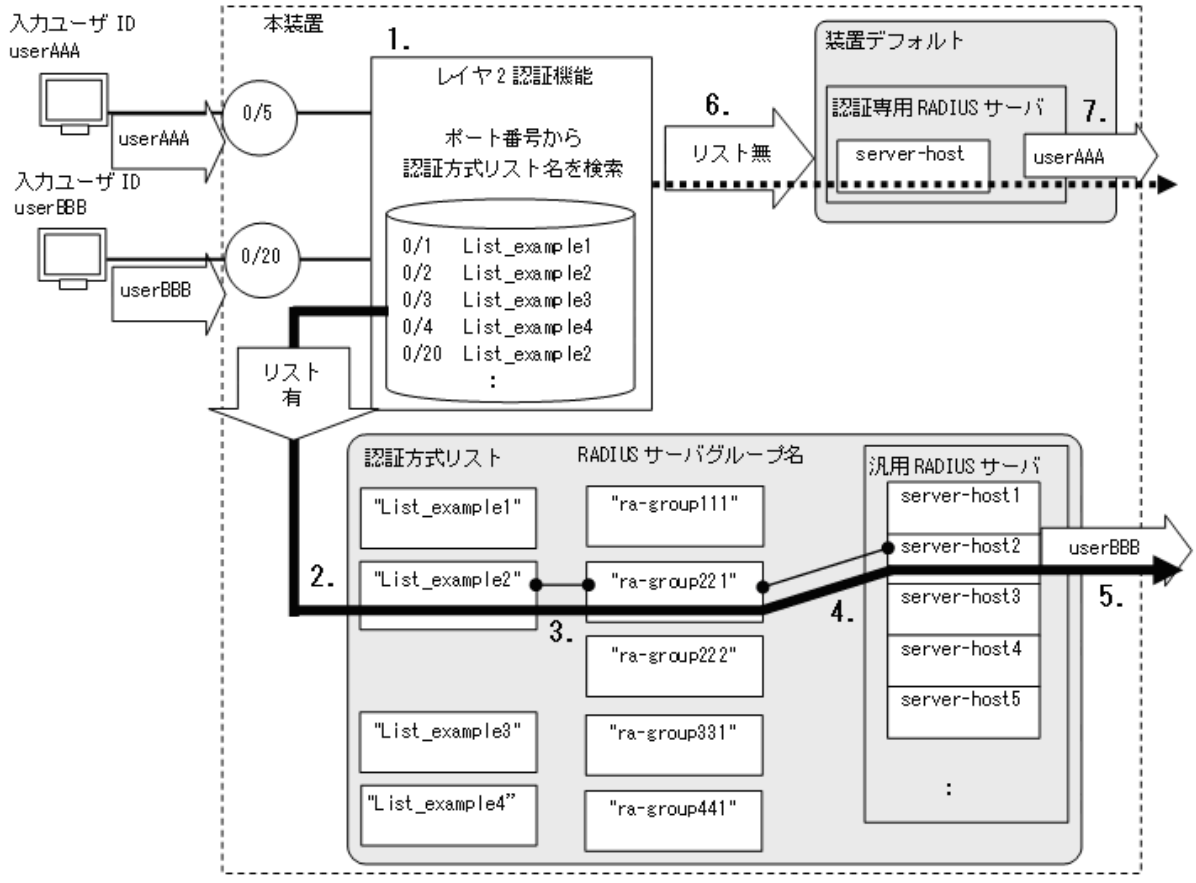
(1) ポート別認証方式

認証ポートごとに個別の RADIUS サーバで認証する機能です。

任意の認証ポートに認証方式リスト名を設定することで，当該認証方式リストに指定された RADIUS サーバグループで RADIUS 認証を実施できます。

ポート別認証方式の動作概要を次の図に示します。

図 5-5 ポート別認証方式の動作概要



【ポートに認証方式リスト名設定時】

1. 認証ポートで認証要求を受信すると，当該認証機能でポートに認証方式リスト名が設定されているか検索します。
2. 当該ポートの認証方式リスト名（図内 "List_example2"）が本装置の認証方式リストに登録されているか確認します。
3. 本装置に登録されている認証方式リストと一致すると，当該認証方式リストに指定された RADIUS サーバグループ（図内 "ra-group221"）を参照します。
4. 参照した RADIUS サーバグループに登録されている汎用 RADIUS サーバ情報の IP アドレス（図内 server-host2）を確認します。
5. 該当した RADIUS サーバへ認証要求を送信します。

【ポートに認証方式リスト名未設定時】

6. ポートに認証方式リスト名未設定時は，当該認証機能の認証専用 RADIUS サーバ情報の IP アドレスを参照します。（認証専用 RADIUS サーバ情報未設定のときは，汎用 RADIUS サーバ情報を参照します。）
7. 該当した RADIUS サーバへ認証要求を送信します。

ポート別認証方式で使用する RADIUS サーバグループは，汎用 RADIUS サーバ情報の任意のサーバ IP アドレスをグループ設定します。従って，認証方式リスト内の RADIUS サーバグループのサーバ IP アドレスが汎用 RADIUS サーバ情報と不一致の時は，認証失敗となります。

また，認証方式リスト内の RADIUS サーバグループに指定された RADIUS サーバがすべて無応答となったときは，強制認証設定に従って動作します。（強制認証設定無効のときは，認証失敗となります。）

なお，以下の場合は，装置デフォルトで認証します。

- ポートに認証方式リスト名未設定
- ポートに設定した認証方式リスト名が，認証方式グループの認証方式リストと不一致
- ポートに設定した認証方式リスト名が，認証方式グループに存在しない

設定については，下記を参照してください。

- ポート別認証方式設定例：「5.2.3　認証方式リストのコンフィグレーション（2）ポート別認証方式の設定例」
- IEEE802.1X：「7　IEEE802.1X の設定と運用」
- Web 認証：「9　Web 認証の設定と運用」
- MAC 認証：「11　MAC 認証の設定と運用」

（a） 認証済み端末のポート移動について

本機能を有効に設定した場合，以下の条件で認証解除が実施されます。

- IEEE802.1X：IEEE802.1X 認証設定ポートへポート移動検出時に，認証解除
  （IEEE802.1X 認証未設定ポートへ移動したときは，認証解除しません。）
- Web 認証　：Web 認証設定ポートへポート移動検出時，ポート移動の前後で認証方式リスト名が異なった場合，ローミング設定有無に関わらず認証解除
  （Web 認証未設定ポートへ移動したときは，認証解除しません。）
- MAC 認証　：MAC 認証設定ポートへポート移動検出時，ポート移動の前後で認証方式リスト名が異なった場合，ローミング設定有無に関わらず認証解除
  （MAC 認証未設定ポートへ移動したときは，認証解除しません。）

認証未設定ポートへ移動したときは，認証状態が解除されるまで通信できません。それぞれ運用コマンド

を使用して，端末の認証状態を解除してください。

- IEEE802.1X：運用コマンド clear dot1x auth-state
- Web 認証　：運用コマンド clear web-authentication auth-state
- MAC 認証　：運用コマンド clear mac-authentication auth-state

認証未設定ポートへ移動したときに認証状態を解除する場合は，コンフィグレーションコマンド authentication auto-logout strayer を設定してください。

（2） ユーザ ID 別認証方式

Web 認証でユーザ ID ごとに個別の RADIUS サーバで認証する機能です。

Web 認証のユーザ ID 別認証方式機能を有効時に，" ユーザ ID@ 認証方式リスト名 " でログインすると，"@" 以降の認証方式リストに指定された RADIUS サーバグループで RADIUS 認証を実施できます。

ユーザ ID と認証方式リスト名の分割条件を次の表に示します。（ユーザ ID"userID"，認証方式リスト名 "List1" を例とします。）

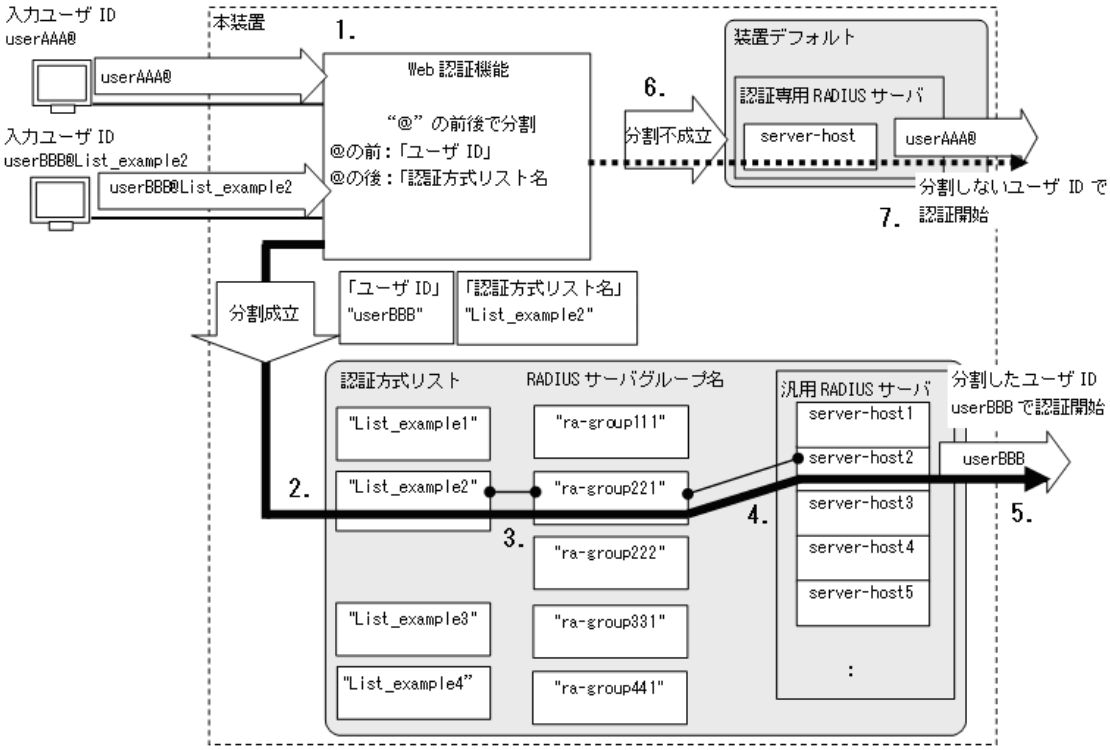
表 5-4　ユーザ ID と認証方式リスト名の分割条件

ユーザ ID と認証方式リスト名の入力文字列例 ※	分割成否	備考
userID@List1	分割成立	
userID@group1@List1	分割成立	複数の @ が含まれているが，最後の @ で分割成立
userID	分割不成立	@ 以降がないため不成立
userID@	分割不成立	@ 以降に文字がないため不成立
@ List1	分割不成立	@ の前に文字がないため不成立
userID@・・・33 文字以上	分割不成立	@ 以降が 33 文字以上のため不成立

注 ※
ユーザ ID の入力可能文字数は @ 以降も含めて最大 128 文字以内です。

ユーザ ID 別認証方式の動作概要を次の図に示します。

図 5-6 ユーザ ID 別認証方式の動作概要



【ユーザ ID 別認証方式有効で，分割成立時】

1. " ユーザ ID@ 認証方式リスト名 "（図内 "userBBB@List_example2"）で認証要求を受信すると，"@" より前の文字列をユーザ ID，"@" 以降を認証方式リスト名に分割します。
2. 分割に成功すると，分割した認証方式リスト名（図内 "List_example2"）が本装置に登録されているか確認します。
3. 本装置に登録されている認証方式リストと一致すると，当該認証方式リストに指定された RADIUS サーバグループ（図内 "ra-group221"）を参照します。
4. 参照した RADIUS サーバグループに登録されている汎用 RADIUS サーバ情報の IP アドレス（図内 server-host2）を確認します。
5. 該当した RADIUS サーバへ認証要求を送信します。（分割が成立しているので，ユーザ ID"userBBB" を送信します。）

【ユーザ ID 別認証方式無効，または分割不成立時】

6. 本機能無効時，または分割不成立時は，当該認証機能の認証専用 RADIUS サーバ情報の IP アドレスを参照します。（認証専用 RADIUS サーバ情報未設定のときは，汎用 RADIUS サーバ情報を参照します。）
7. 該当した RADIUS サーバへ認証要求を送信します。（分割が不成立だったので，ユーザ ID"userAAA@" を送信します。）

ユーザ ID 別認証方式で使用する RADIUS サーバグループは，汎用 RADIUS サーバ情報の任意のサーバ IP アドレスをグループ設定します。従って，認証方式リスト内の RADIUS サーバグループのサーバ IP アドレスが汎用 RADIUS サーバ情報と不一致の時は，認証失敗となります。

また，認証方式リスト内の RADIUS サーバグループに指定された RADIUS サーバがすべて無応答となったときは，強制認証設定に従って動作します。（強制認証設定無効のときは，認証失敗となります。）

なお，以下の場合は，装置デフォルトで認証します。

- ユーザ ID の " @ " 以降に指定した認証方式リスト名が，当該認証機能の認証方式グループの認証方式リストと不一致
- ユーザ ID と認証方式リスト名が " @ " で分割できない

設定については，下記を参照してください。

- ユーザ ID 別認証方式の設定例：「5.2.3　認証方式リストのコンフィグレーション（3）ユーザ ID 別認証方式の設定例」

（3） 認証方式リスト設定のコンフィグレーション排他関係

ポート別認証方式設定，ユーザ ID 別認証方式は装置内で共存できません。いずれか 1 種類を設定してください。

次の表に認証方式リスト設定の同時設定不可条件を示します。

表 5-5　認証方式リスト設定の同時設定不可条件

ポート別認証方式設定	ユーザ ID 別認証方式設定
dot1x authentication web-authentication authentication mac-authentication authentication	web-authentication user-group
上記のどれか 1 つでも設定済み	×
すべて未設定	○

（凡例）
　○：設定可
　×：設定不可

5.2.3　認証方式リストのコンフィグレーション

（1） コンフィグレーションコマンド一覧

本項では，認証方式リストによる認証方式設定のコンフィグレーションについて説明します。

表 5-6　コンフィグレーションコマンドと対象認証方式リスト

コマンド名	説明	認証方式リスト	
		ポート別認証方式	ユーザ ID 別認証方式
aaa authentication dot1x <List name>	IEEE802.1X 認証用の認証方式グループで「装置デフォルト」「認証方式リスト」を設定します。	○	×
dot1x authentication <List name>	IEEE802.1X 認証で使用する，ポート別認証方式の認証方式リスト名を設定します。	○	×
aaa authentication web-authentication <List name>	Web 認証用の認証方式グループで「装置デフォルト」「認証方式リスト」を設定します。	○	○
web-authentication authentication <List name>	Web 認証で使用する，ポート別認証方式の認証方式リスト名を設定します。	○	×
web-authentication user-group	Web 認証で，ユーザ ID 別認証方式を有効にします。	×	○

コマンド名	説明	認証方式リスト	
		ポート別認証方式	ユーザ ID 別認証方式
aaa authentication mac-authentication	MAC 認証用の認証方式グループで「装置デフォルト」「認証方式リスト」を設定します。	○	×
mac-authentication authentication <List name>	MAC 認証で使用する，ポート別認証方式の認証方式リスト名を設定します。	○	×
radius-server host	汎用 RADIUS サーバ情報を設定します。	○	○
aaa group server radius <Group name>	RADIUS サーバグループ名を設定します。	○	○
server	RADIUS サーバグループに汎用 RADIUS サーバ情報を登録します。	○	○

（凡例）
○：設定可
×：設定不可

（2） ポート別認証方式の設定例

本項では，ポート別認証方式を使用してトリプル認証を実施する構成例を説明します。対象ポート番号と RADIUS サーバグループ名は下記を使用します。

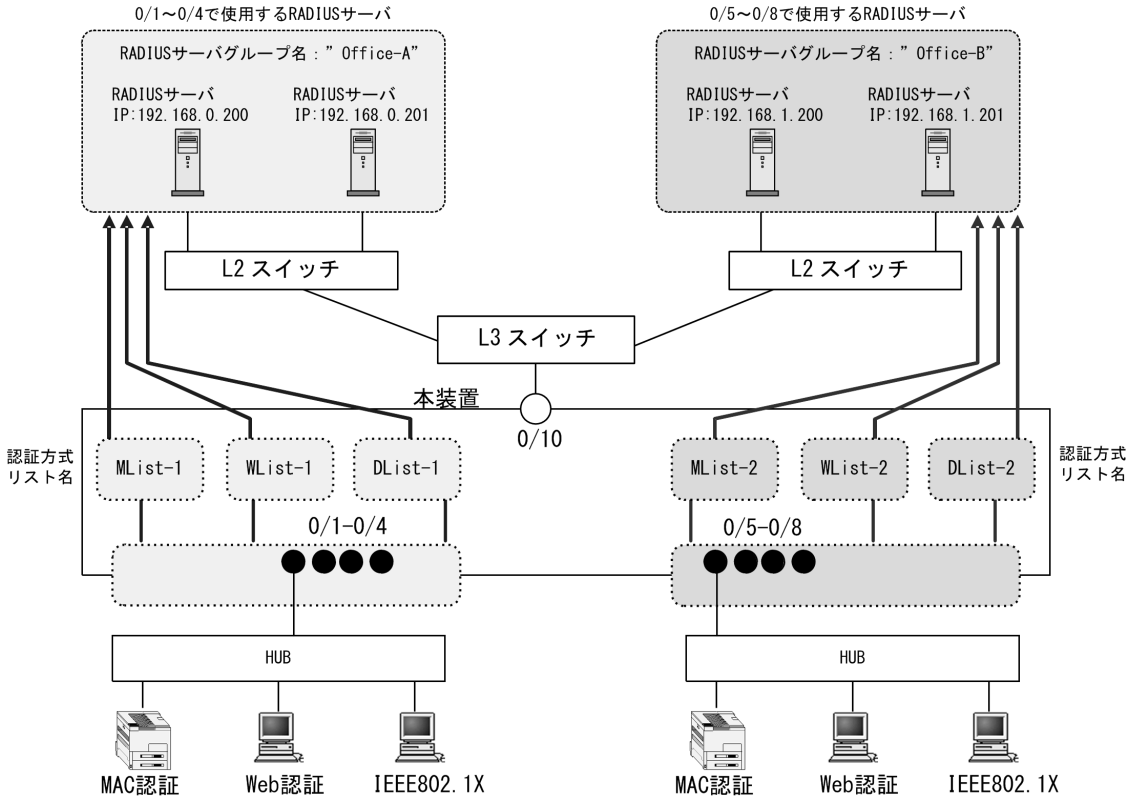
- ポート 0/1 ～ 0/4：RADIUS サーバグループ "Office-A" を使用して認証を実施
- ポート 0/5 ～ 0/8：RADIUS サーバグループ "Office-B" を使用して認証を実施

ポート別認証方式設定以外の各認証機能のコンフィグレーションについては，下記を参照してください。

- IEEE802.1X：「7　IEEE802.1X の設定と運用」
- Web 認証：「9　Web 認証の設定と運用」
- MAC 認証：「11　MAC 認証の設定と運用」

ポート別認証方式の構成例を次の図に示します。

図 5-7 ポート別認証方式構成図例



［設定のポイント］

1. RADIUS サーバの設定
   - 「認証方式リスト」で使用する汎用 RADIUS サーバ情報を設定
   - 汎用 RADIUS サーバ情報をグループ化
2. 各認証機能の設定
   - 各認証機能ごとに，認証方式リストと RADIUS サーバグループを関連付け
   - ポートごとに，各認証機能で使用する認証方式リストを設定

［コマンドによる設定］

1. **(config)# radius-server host 192.168.0.200 key AuthKey**
   (config)# radius-server host 192.168.0.201 key AuthKey
   (config)# radius-server host 192.168.1.200 key AuthKey
   (config)# radius-server host 192.168.1.201 key AuthKey
   4 台分の汎用 RADIUS サーバ情報を設定します。
2. **(config)# aaa group server radius Office-A**
   (config-group)# server 192.168.0.200
   (config-group)# server 192.168.0.201
   (config-group)# exit
   RADIUS サーバグループ名 "Office-A" と，このグループで使用する汎用 RADIUS サーバの IP アドレスを登録します。
3. **(config)# aaa group server radius Office-B**
   (config-group)# server 192.168.1.200
   (config-group)# server 192.168.1.201
   (config-group)# exit

RADIUS サーバグループ名 "Office-B" と，このグループで使用する汎用 RADIUS サーバの IP アドレスを登録します。

4. **(config)# aaa authentication dot1x DList-1 group Office-A**
   (config)# aaa authentication dot1x DList-2 group Office-B
   (config)# aaa authentication web-authentication WList-1 group Office-A
   (config)# aaa authentication web-authentication WList-2 group Office-B
   (config)# aaa authentication mac-authentication MList-1 group Office-A
   (config)# aaa authentication mac-authentication MList-2 group Office-B
   各認証機能ごとに認証方式リスト名と，RADIUS サーバグループ名を関連付けします。
5. **(config)# interface range gigabitethernet 0/1-4**
   (config-if-range)# dot1x authentication DList-1
   (config-if-range)# web-authentication authentication WList-1
   (config-if-range)# mac-authentication authentication Mlist-1
   (config-if-range)# exit
   ポート 0/1 から 0/4 に対して，各認証機能で使用する認証方式リスト名 DList-1，WList-1，MList-1 を設定します。
6. **(config)# interface range gigabitethernet 0/5-8**
   (config-if-range)# dot1x authentication DList-2
   (config-if-range)# web-authentication authentication WList-2
   (config-if-range)# mac-authentication authentication Mlist-2
   (config-if-range)# exit
   ポート 0/5 から 0/8 に対して，各認証機能で使用する認証方式リスト名 DList-2，WList-2，MList-2 を設定します。

[注意事項]

1. ポート別認証方式未設定時は，装置デフォルトに従って認証します。
2. ポートに設定した認証方式リスト名と，認証方式グループの認証方式リスト名が不一致，または認証方式グループに存在しないときは，装置デフォルトに従って認証します。
3. Web 認証のユーザ ID 別認証方式は併用設定できません。詳細は「5.2.2　認証方式リスト」を参照してください。

(3) ユーザ ID 別認証方式の設定例

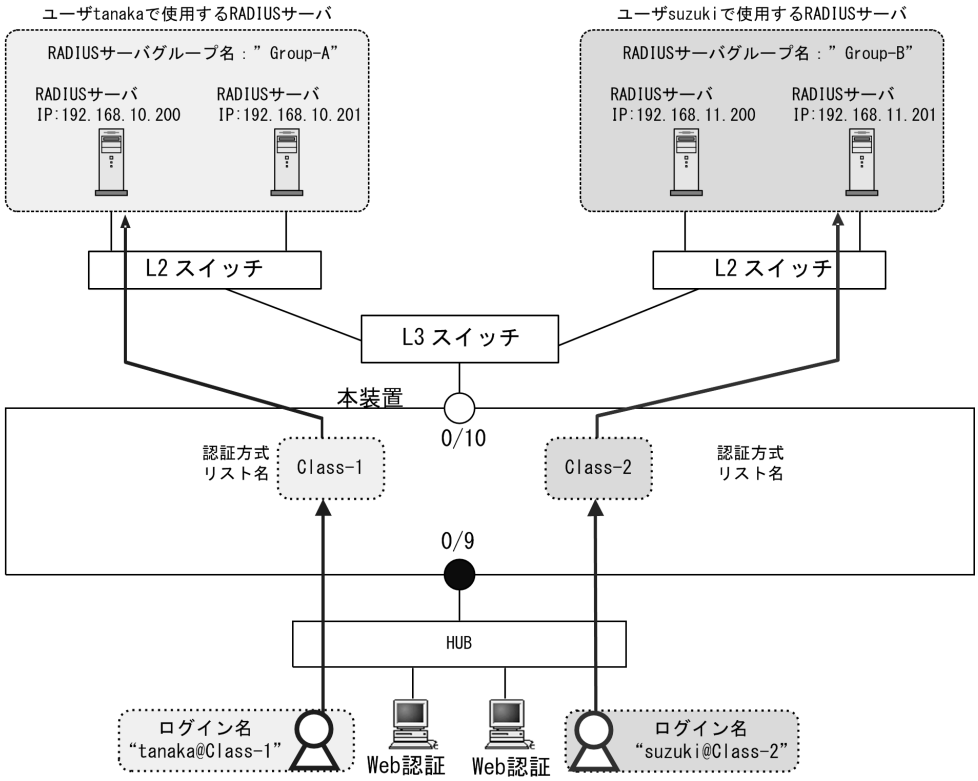
本項では，ユーザ ID 別認証方式を使用して Web 認証を実施する構成例を説明します。Web 認証対象ユーザ ID と RADIUS サーバグループ名は下記を使用します。

- ユーザ "tanaka"：ポート 0/9 で RADIUS サーバグループ "Group-A" を使用して認証
- ユーザ "suzuki"：ポート 0/9 で RADIUS サーバグループ "Group-B" を使用して認証

上記以外の Web 認証機能のコンフィグレーションについては，「9　Web 認証の設定と運用」を参照してください。

ユーザ ID 別認証方式の構成例を次の図に示します。

図 5-8 ユーザ ID 別認証方式構成図例



[設定のポイント]

1. RADIUS サーバの設定
   - 「認証方式リスト」で使用する汎用 RADIUS サーバ情報を設定
   - 汎用 RADIUS サーバ情報をグループ化
2. Web 認証機能の設定
   - Web 認証の認証方式リストと RADIUS サーバグループを関連付け
   - Web 認証にユーザ ID 別認証方式リストを設定

[コマンドによる設定]

1. **(config)# radius-server host 192.168.10.200 key AuthKey**
   (config)# radius-server host 192.168.10.201 key AuthKey
   (config)# radius-server host 192.168.11.200 key AuthKey
   (config)# radius-server host 192.168.11.201 key AuthKey
   4 台分の汎用 RADIUS サーバ情報を設定します。
2. **(config)# aaa group server radius Group-A**
   (config-group)# server 192.168.10.200
   (config-group)# server 192.168.10.201
   (config-group)# exit
   RADIUS サーバグループ名 "Group-A" と，このグループで使用する汎用 RADIUS サーバの IP アドレスを登録します。
3. **(config)# aaa group server radius Group-B**
   (config-group)# server 192.168.11.200

```
(config-group)# server 192.168.11.201
(config-group)# exit
```

RADIUS サーバグループ名 "Group-B" と，このグループで使用する汎用 RADIUS サーバの IP アドレスを登録します。

4. **(config)# aaa authentication web-authentication Class-1 group Group-A**
   (config)# aaa authentication web-authentication Class-2 group Group-B
   Web 認証の認証方式リスト名と，RADIUS サーバグループ名を関連付けします。
5. **(config)# web-authentication user-group**
   Web 認証機能にユーザ ID 別認証方式を設定します。

[注意事項]

1. ユーザ ID 別認証方式未設定時は，装置デフォルトに従って認証します。
2. ユーザ ID 別認証方式の設定を変更した場合は，全 Web 認証端末を認証解除します。
3. ユーザ ID の@以降に指定された認証方式リスト名と，認証方式グループの認証方式リスト名が不一致，または認証方式グループに存在しないときは，装置デフォルトに従って認証します。
4. ポート別認証方式は併用設定できません。詳細は「5.2.2　認証方式リスト」を参照してください。

5.3 RADIUS 認証

レイヤ 2 認証機能の RADIUS 認証で使用する，以下の項目について説明します。

- レイヤ 2 認証機能で使用する RADIUS サーバ情報
- RADIUS サーバ通信の dead-interval 機能
- 装置デフォルトのローカル認証と RADIUS 認証の優先設定
- RADIUS サーバのアカウント機能

5.3.1 レイヤ 2 認証機能で使用する RADIUS サーバ情報

(1) 本装置で設定できる RADIUS サーバ情報

本装置では，下記の RADIUS サーバ情報を設定できます。

表 5-7 本装置で設定する RADIUS サーバ情報

RADIUS サーバ情報種別	設定情報	使用する機能
汎用 RADIUS サーバ情報	RADIUS サーバホスト情報 自動復旧時間（dead-interval 時間）	ログイン認証 IEEE802.1X Web 認証 MAC 認証
IEEE802.1X 認証専用 RADIUS サーバ情報	RADIUS サーバホスト情報 自動復旧時間（dead-interval 時間）	IEEE802.1X
Web 認証専用 RADIUS サーバ情報	RADIUS サーバホスト情報 自動復旧時間（dead-interval 時間）	Web 認証
MAC 認証専用 RADIUS サーバ情報	RADIUS サーバホスト情報 自動復旧時間（dead-interval 時間）	MAC 認証
RADIUS サーバグループ情報	RADIUS サーバホスト情報 ※	ログイン認証 IEEE802.1X Web 認証 MAC 認証

注 ※

設定した汎用 RADIUS サーバ情報（radius-server host）のなかから，RADIUS サーバグループに割り当てます。汎用 RADIUS サーバ情報と同一の IP アドレス，サーバの認証用ポート番号，サーバのアカウンティング用ポート番号を設定してください。なお，自動復旧時間は汎用 RADIUS サーバ情報の自動復旧時間（radius-server dead-interval）設定に従います。

各 RADIUS サーバ情報では，サーバの IP アドレス，サーバの認証用ポート番号，サーバのアカウンティング用ポート番号，RADIUS 鍵，再送回数，応答タイムアウト時間を設定できます。RADIUS 鍵，再送回数，応答タイムアウト時間の指定を省略したときは，下記のコンフィグレーションコマンドの設定に従います。

- RADIUS 鍵：radius-server key
- 再送回数：radius-server retransmit
- 応答タイムアウト時間：radius-server timeout

サーバの認証用ポート番号指定を省略したときは 1812 で，アカウンティング用ポート番号指定を省略したときは，1813 で動作します。

各 RADIUS サーバ情報の設定については，下記を参照してください。

- 汎用 RADIUS サーバ情報の設定：「コンフィグレーションガイド Vol.1　10　ログインセキュリティと RADIUS」
- 認証専用 RADIUS サーバ情報の設定
  - IEEE802.1X：「7.2.1　認証方式グループと RADIUS サーバ情報の設定」
  - Web 認証：「9.2.1　認証方式グループと RADIUS サーバ情報の設定」
  - MAC 認証：「11.2.1　認証方式グループと RADIUS サーバ情報の設定」
- RADIUS サーバグループ情報の設定：「コンフィグレーションガイド Vol.1　10　ログインセキュリティと RADIUS」

(a) 自動復旧時間（dead-interval 時間）

自動復旧時間の設定は，それぞれの RADIUS サーバ情報に対して動作します。他の認証専用 RADIUS サーバ情報には影響しません。

自動復旧時間の動作については，後述の「5.3.2　RADIUS サーバ通信の dead-interval 機能」を参照してください。

(2) 各 RADIUS サーバ情報間の同一アドレス設定の扱い

各 RADIUS サーバ情報は同時設定可能ですが，同じ IP アドレスを設定したときは，「同一 RADIUS サーバ」として扱います。

従って，同一 RADIUS サーバとの通信には，同一 RADIUS 鍵，同一再送回数，同一応答タイムアウト時間を適用します。

このため，コンフィグレーションコマンドの入力時に下記処理を実施します。

1. 汎用 RADIUS サーバ情報間の同一 IP アドレス指定
   IP アドレスが既存の RADIUS サーバ設定と一致するときは，すべてのパラメータを新しく入力したコマンド内容に置き換えます。
   新しいコマンドの入力で省略したパラメータはデフォルトコンフィグレーションに戻ります。
2. 同じ種類の認証専用 RADIUS サーバ情報間の同一 IP アドレス指定
   汎用 RADIUS サーバ情報間と同様です。
3. 汎用 RADIUS サーバ情報と認証専用 RADIUS サーバ情報で同一 IP アドレス指定
   汎用 RADIUS サーバ情報間と同様です。
4. 異なる種類の RADIUS サーバ間で同一 IP アドレス指定
   汎用 RADIUS サーバ情報間と同様です。

- 【異なる種類の RADIUS サーバ間で同一 IP アドレスを設定した例】
  汎用 RADIUS サーバを設定後，同じ IP アドレスで MAC 認証専用 RADIUS サーバを設定します。
  - `(config)# radius-server host 192.168.7.7 retransmit 10 key aaaaa`
    汎用 RADIUS サーバの設定 【初期状態】
  - `(config)# mac-authentication radius-server host 192.168.7.7 key bbbbb`
    MAC 認証専用 RADIUS サーバの設定

  上記の順で入力したとき，汎用 RADIUS サーバの再送回数 (retransmit) は，自動的にデフォルトコンフィグレーション (3 回) に戻り，RADIUS 鍵も MAC 認証専用 RADIUS サーバで入力した "bbbbb" に変更されます。
  自動変更された結果は，運用コマンド show running-config にも反映されます。
- 【運用コマンド show running-config の表示結果】

- `radius-server host 192.168.7.7 key bbbbb`　【自動変更適用後の内容】
- `mac-authentication radius-server host 192.168.7.7 key bbbbb`

その後，MAC 認証専用 RADIUS サーバ情報を削除しても，汎用 RADIUS サーバ情報は【初期状態】のコンフィグレーションに戻りません。

（3） 各 RADIUS サーバ情報併用設定での運用

ポート別認証方式または Web 認証のユーザ ID 別認証方式が有効のときは，認証方式リストに登録された RADIUS サーバグループ情報で運用します。

ポート別認証方式または Web 認証のユーザ ID 別認証方式が無効のときは，装置デフォルトに従います。装置デフォルトでは，汎用 RADIUS サーバ情報または認証専用 RADIUS サーバ情報で運用しますが，汎用 RADIUS サーバ情報と認証専用 RADIUS サーバ情報を両方設定したときは，各認証機能の認証専用 RADIUS サーバ情報で運用します。

汎用 RADIUS サーバと認証専用 RADIUS サーバの運用関係を次の表に示します。

表 5-8　汎用 RADIUS サーバ情報と認証専用 RADIUS サーバ情報の運用関係

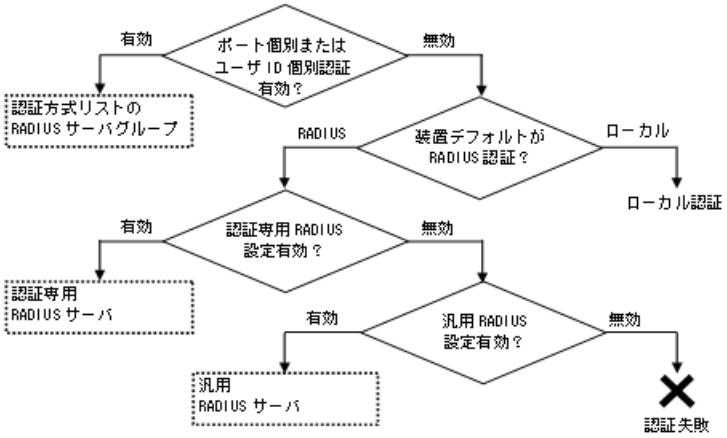
認証専用 RADIUS サーバ情報	汎用 RADIUS サーバ情報	動作
1 件以上設定有	1 件以上設定有	認証専用 RADIUS サーバ情報で運用
	1 件も設定無	認証専用 RADIUS サーバ情報で運用
1 件も設定無	1 件以上設定有	汎用 RADIUS サーバ情報で運用
	1 件も設定無	RADIUS 認証実行不可

汎用 RADIUS サーバと認証専用 RADIUS サーバの運用関係を，MAC 認証を例に説明します。

1. MAC 認証専用 RADIUS サーバ情報で運用する場合
   コンフィグレーションコマンド mac-authentication radius-server host を 1 件でも設定しているときは，mac-authentication radius-server host で設定した MAC 認証専用 RADIUS サーバだけを使用します。
   このとき，認証要求先 RADIUS サーバの選択や自動復旧（dead-interval）処理は，他の認証機能に影響しません。
2. 汎用 RADIUS サーバ情報で運用する場合
   コンフィグレーションコマンド mac-authentication radius-server host を 1 件も設定していないときは，コンフィグレーションコマンド radius-server host で設定した汎用 RADIUS サーバを使用します。
   このとき，認証要求先 RADIUS サーバの選択や自動復旧（dead-interval）処理は，汎用 RADIUS サーバを使用しているすべての認証機能で共通となります。

RADIUS サーバ情報併用設定時の運用を次の図に示します。

図 5-9　RADIUS サーバ情報併用設定時の運用

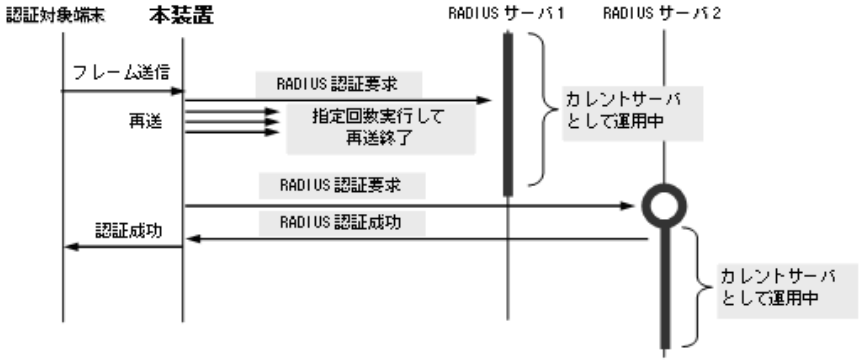


（4） 認証要求先 RADIUS サーバの選択

汎用 RADIUS サーバ情報，各認証専用 RADIUS サーバ情報，RADIUS サーバグループでは，それぞれ複数の RADIUS サーバホストを設定できます。（最大設定数は，「コンフィグレーションガイド Vol.1 3.2 収容条件」を参照してください。）

一つのサーバと通信できず，認証サービスが受けられない場合は，順次それぞれで設定したサーバへの接続を試行します。RADIUS サーバ選択のシーケンスを次の図に示します。

図 5-10　RADIUS サーバ選択のシーケンス



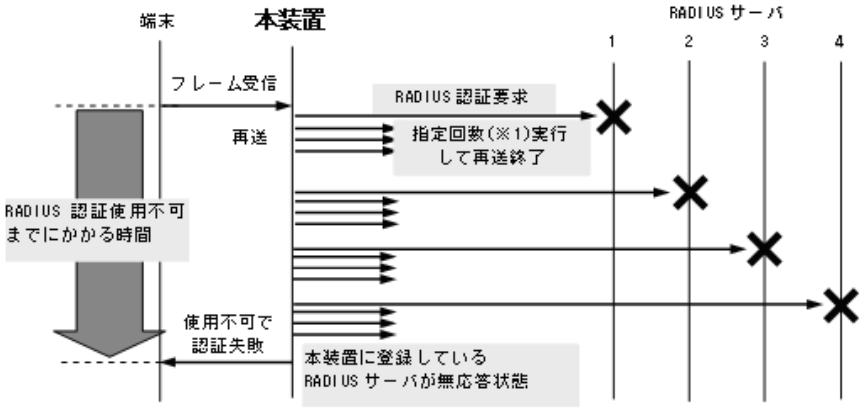
この図で認証対象端末から本装置に新規にフレームを受信すると，RADIUS サーバ 1 に対し本装置から RADIUS 認証を要求します。RADIUS サーバ 1 と通信できなかった場合は，続いて RADIUS サーバ 2 に対して RADIUS 認証を実行します。ここで認証に成功すると，認証済みネットワークへ通信可能となります。

また，認証要求先として運用中の RADIUS サーバをカレントサーバと呼びます。

（5） RADIUS 認証使用不可までの最大時間

RADIUS サーバと通信不可を判断する応答タイムアウト時間を設定できます。デフォルトコンフィグレーションは 5 秒です。また，各 RADIUS サーバでタイムアウトした場合は，再接続を試行します。この再送回数も設定でき，デフォルトコンフィグレーションは 3 回です。このため，認証方式として RADIUS が使用できないと判断するまでの最大時間は，応答タイムアウト時間 ×（最初の 1 回＋再送回数）×RADIUS サーバ設定数になります。

図 5-11　RADIUS 認証使用不可までのシーケンス（RADIUS サーバ最大数設定時）



指定回数※1：RADIUS サーバへの再送回数（デフォルト 3 回：コンフィグレーションで変更可）

設定した RADIUS サーバが使用不可のときは，強制認証機能により認証許可することもできます。後述の「5.4.6　認証共通の強制認証」を参照してください。

5.3.2　RADIUS サーバ通信の dead-interval 機能

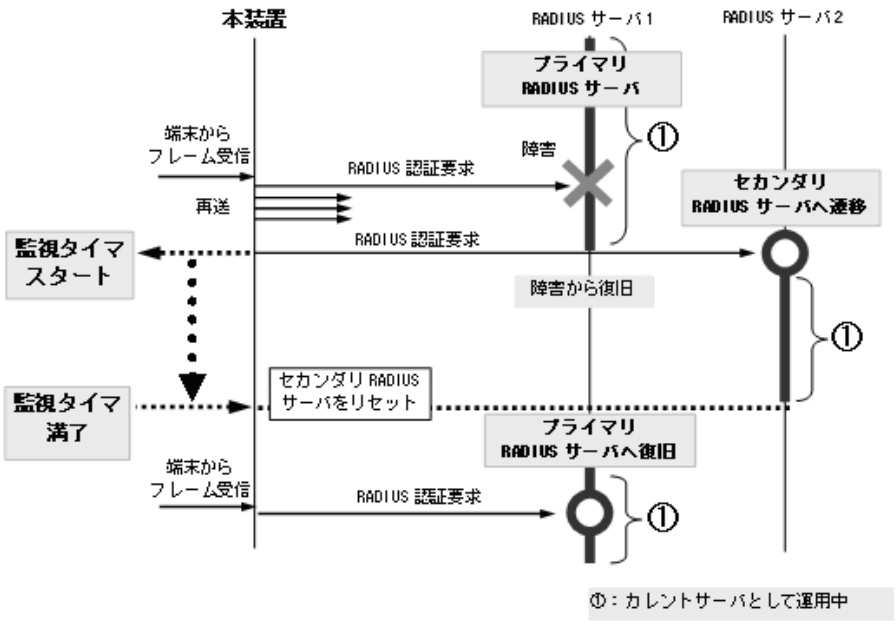
本装置の RADIUS 認証では，認証対象端末からのフレーム受信による RADIUS 認証要求を契機に有効な RADIUS サーバを検出し，以降の端末は常に有効な RADIUS サーバを使用します。この方式では，認証されるまでの時間は軽減されますが，RADIUS サーバを負荷分散構成などで使用時，RADIUS サーバに障害が発生すると負荷分散状態に自動的に復旧できません。

本装置では，最初の RADIUS サーバへの自動復旧手段として，監視タイマによる dead-interval 機能をサポートしています。本機能での RADIUS サーバを下記で表記します。

- プライマリ RADIUS サーバ：最初の有効な RADIUS サーバ
- セカンダリ RADIUS サーバ：次に有効な RADIUS サーバ
- カレントサーバ：認証要求先として運用中の RADIUS サーバ

プライマリ RADIUS サーバへの復旧シーケンスを次の図に示します。また，説明文中は MAC 認証専用 RADIUS サーバ用のコマンド名で記述しています。

図 5-12　プライマリ RADIUS サーバへの復旧シーケンス (1)



1. プライマリ RADIUS サーバ（※ 1）をカレントサーバとして RADIUS 認証要求を開始します。
2. プライマリ RADIUS サーバに障害が発生して，次に有効な RADIUS サーバ（セカンダリ RADIUS サーバ）へ遷移します。
3. カレントサーバがセカンダリ RADIUS サーバに遷移した時点で監視タイマをスタートします。
4. 最後の有効な RADIUS サーバへ認証要求ができなかったときは認証失敗（※ 2）とし，この状態をカレントサーバ（※ 3）として監視タイマをスタート（※ 4）します。（監視タイマをスタート済みのときは継続します。）
5. 監視タイマが満了すると，カレントサーバはプライマリ RADIUS サーバへ復旧します。
6. 監視タイマ満了後にプライマリ RADIUS サーバへ復旧してもプライマリ RADIUS サーバが障害から復旧していない場合，再度有効な RADIUS サーバ選択処理を実行します。カレントサーバが有効なセカンダリ RADIUS サーバへ遷移した時点で，再度監視タイマをスタートします。

注 ※ 1

コンフィグレーションコマンド mac-authentication radius-server host で設定した RADIUS サーバは，以下のいずれかの条件を満たしている設定が有効です。

- mac-authentication radius-server host の key パラメータの設定有
- mac-authentication radius-server host の key パラメータの設定無だが，radius-server key 設定有

上記の条件を満たしていない RADIUS サーバ設定は無効となり，最初に設定されていてもプライマリ RADIUS サーバとなりません。

注 ※2

ログイン認証の場合は，認証失敗となります。

レイヤ２認証機能の場合は，強制認証または認証失敗となります。レイヤ２認証機能の強制認証については，「5.4.6　認証共通の強制認証」を参照してください。

注 ※3

運用コマンド show radius-server では，「* hold down」を表示します。

注 ※4

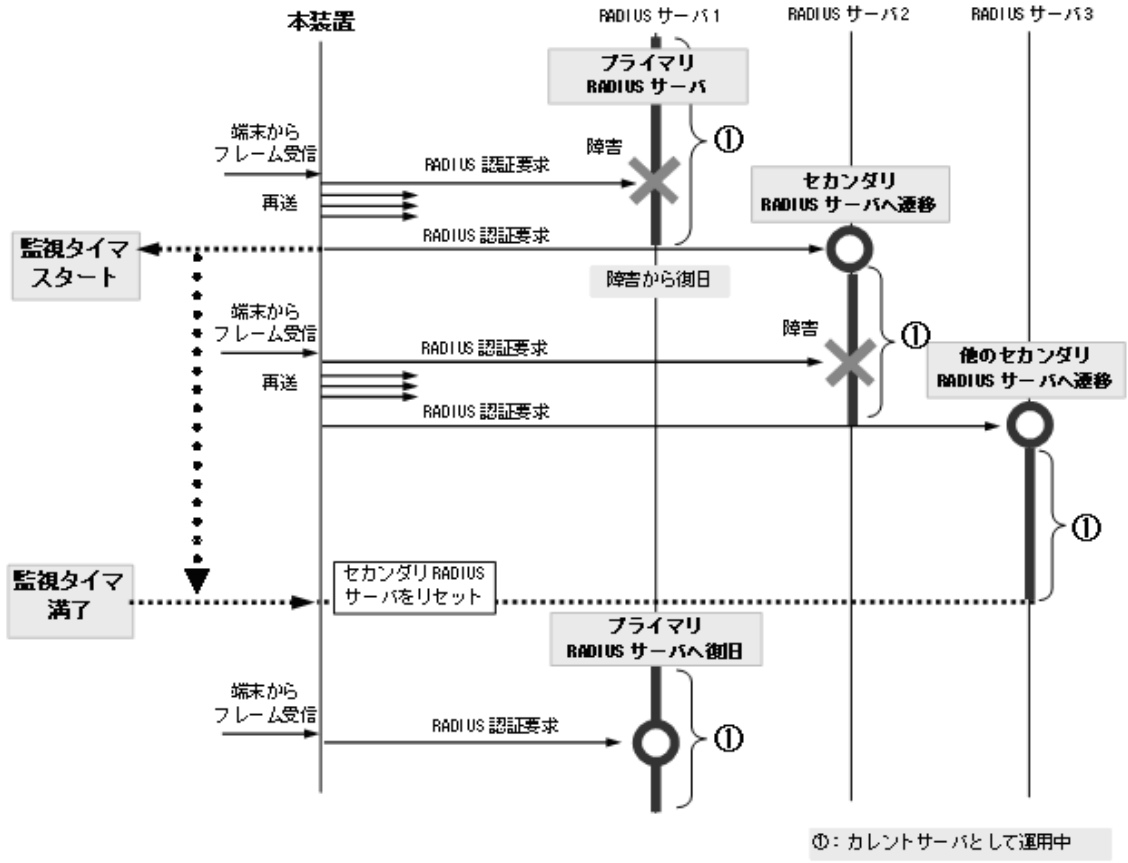
このときの監視タイマが満了するまでは，RADIUS サーバへ認証要求を送信しないで，認証失敗（レイヤ 2 認証機能は強制認証または認証失敗）として扱います。（コンフィグレーションコマンド mac-authentication radius-server dead-interval 0 設定のときは，監視タイマをスタートしないで，プライマリ RADIUS サーバへ復旧します。）

また，監視タイマはいったんスタートすると基本的には満了するまでリセットしません。

下記のように 3 台以上の RADIUS サーバを設定した環境で監視タイマをスタート後に，別の RADIUS サーバにカレントサーバが遷移した場合でも，監視タイマはリセットせずに満了するまで継続します。

3 台以上の RADIUS サーバを設定した場合のシーケンスを次の図に示します。

図 5-13　プライマリ RADIUS サーバへの復旧シーケンス (2)



なお，下記の契機では例外として監視タイマを満了せずにリセットします。

- コンフィグレーションコマンドで mac-authentication dead-interval 0 を設定したとき
- カレントサーバとして運用中の RADIUS サーバ情報を，コンフィグレーションコマンド mac-authentication radius-server host で削除したとき
- 運用コマンド clear radius-server を実行したとき

5.3.3 装置デフォルトのローカル認証と RADIUS 認証の優先設定

「5.2 認証方式グループ」で設定する装置デフォルトは，コンフィグレーションによりローカル認証方式・RADIUS 認証方式を単独でも同時でも設定できます。同時に設定したときは，先に指定した方式で認証に失敗したときに，次に指定した方式で認証できます。

ローカル認証方式と RADIUS 認証方式の優先設定のサポート範囲を次の表に示します。

表 5-9 ローカル認証方式と RADIUS 認証方式の優先設定サポート範囲

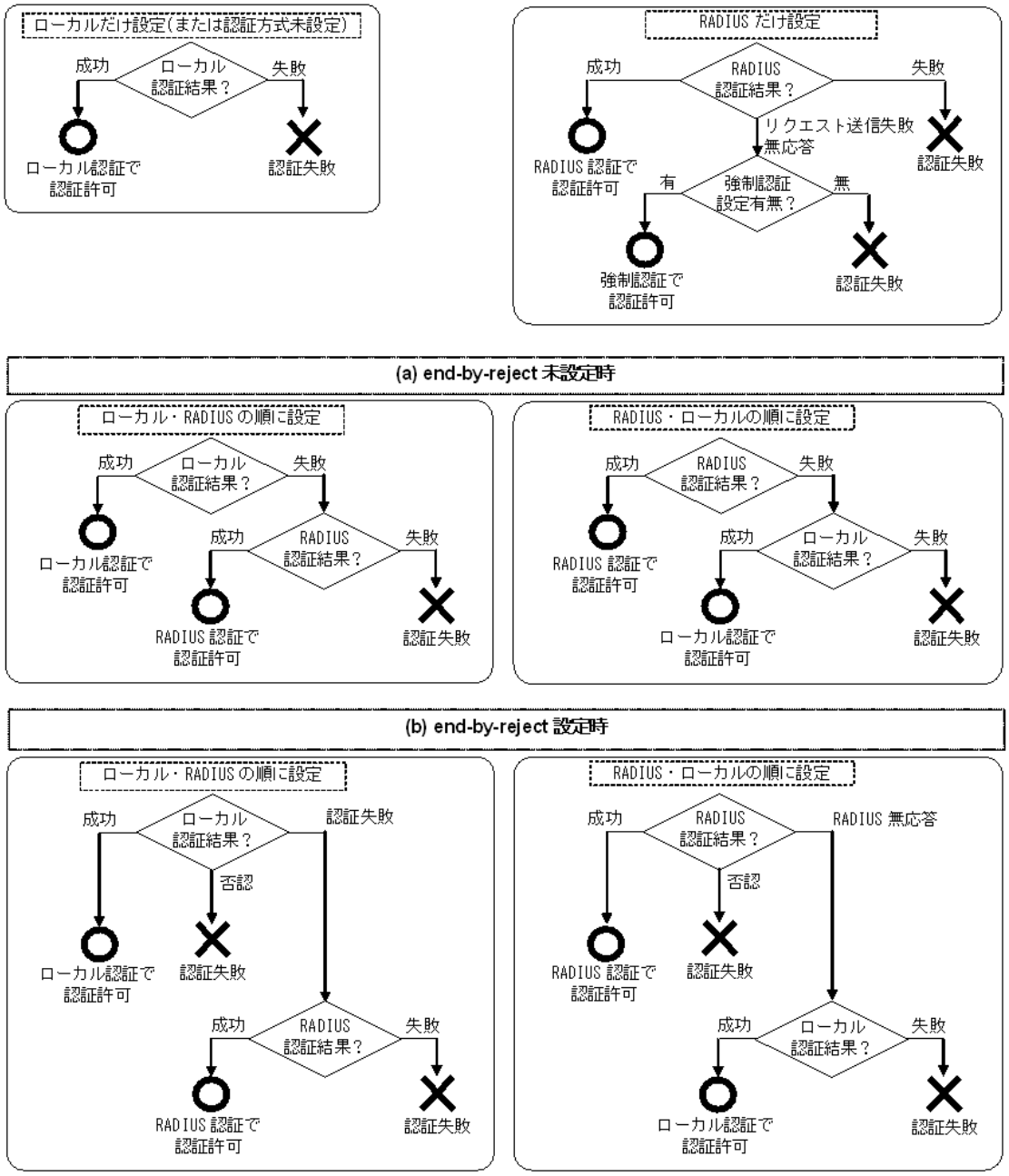
認証機能	認証モード	認証方式		
		ローカル	RADIUS	優先設定
IEEE802.1X	ポート単位認証（静的）	×	○	×
	ポート単位認証（動的）	×	○	×
Web 認証	固定 VLAN モード	○	○	○
	ダイナミック VLAN モード	○	○	○
MAC 認証	固定 VLAN モード	○	○	○
	ダイナミック VLAN モード	○	○	○

（凡例）
○：サポート
×：未サポート

また，同時に指定された場合に，先に指定された方式で認証に失敗したときの認証方式の選択動作を，コンフィグレーションコマンド aaa authentication web-authentication end-by-reject（MAC 認証は aaa authentication mac-authentication end-by-reject）で変更できます。

認証方式の設定種別と認証結果の関連を次の図に示します。

図 5-14 認証方式の設定種別と認証結果の関連



（a） end-by-reject 未設定時

end-by-reject 未設定時は，先に指定された方式で認証に失敗した場合に，その失敗の理由に関係なく，次に指定された方式で認証できます。

例えば，認証前端末からの受信により，RADIUS サーバに対し本装置から RADIUS 認証を要求します。RADIUS 認証否認によって RADIUS サーバでの認証に失敗すると，次にローカル認証を実行します。ここで認証に成功すると認証済み端末として管理します。

（b） end-by-reject 設定時

end-by-reject 設定時は，先に指定された方式で認証否認された場合に，次に指定された方式で認証を行いません。否認された時点で認証を終了し，一連の認証が失敗となります。通信不可 （RADIUS サーバ無

応答など）によって認証が失敗した場合だけ，次に指定された方式で認証できます。

例えば，認証前端末からの受信により，RADIUS サーバに対し本装置から RADIUS 認証を要求します。RADIUS 認証否認によって RADIUS サーバでの認証に失敗すると，この時点で一連の認証が失敗となり，認証を終了します。次に指定されているローカル認証は行いません。その結果，該当端末は認証失敗端末として管理します。

認証方式のコンフィグレーションについては，下記を参照してください。

- IEEE802.1X :「7.2.1　認証方式グループと RADIUS サーバ情報の設定」
- Web 認証 :「9.2.1　認証方式グループと RADIUS サーバ情報の設定」
- MAC 認証 :「11.2.1　認証方式グループと RADIUS サーバ情報の設定」

5.3.4　RADIUS サーバを使用したアカウント機能

（1） 概要

本装置では RADIUS サーバを使用したアカウント機能（以下，RADIUS アカウント機能）をサポートしています。

本装置の RADIUS アカウント機能は，レイヤ 2 認証機能だけで使用します。RADIUS アカウント機能のサポート範囲を次の表に示します。

表 5-10　RADIUS アカウント機能のサポート範囲

対象機能	アカウント方式グループ		発行契機		アカウンティングサーバ種別
	装置デフォルト	アカウント方式リスト	start-stop	stop-only	group radius
ログイン	×	×	×	×	×
IEEE802.1X	○	×	○	×	○
Web 認証	○	×	○	×	○
MAC 認証	○	×	○	×	○

（凡例）
　○：サポート
　×：未サポート

（2） アカウンティング情報の送信先

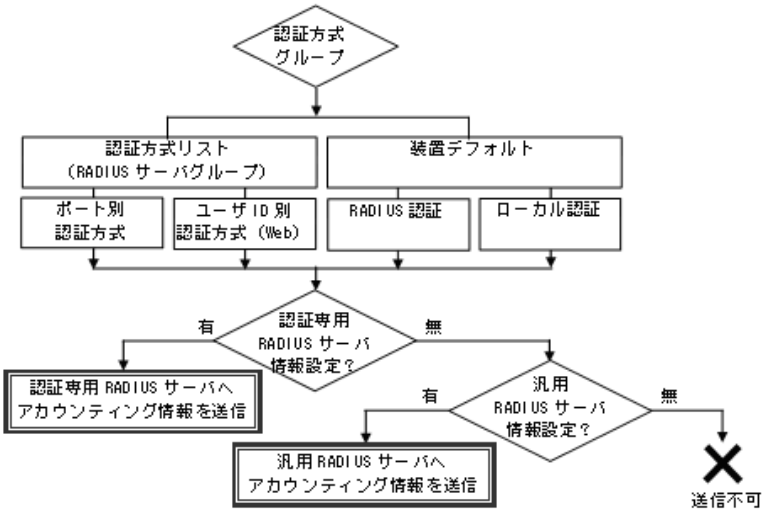
アカウンティング情報は，当該認証機能の装置デフォルトとして運用される RADIUS サーバ宛（認証専用 RADIUS サーバ，または汎用 RADIUS サーバ）に送信します。RADIUS サーバグループは適用しません。

従って，ポート別認証方式または Web 認証のユーザ ID 別認証方式で RADIUS サーバグループで認証しても，アカウンティング情報は認証専用 RADIUS サーバまたは汎用 RADIUS サーバへ送信します。

また，ローカル認証で認証したときも，当該認証機能の認証専用 RADIUS サーバまたは汎用 RADIUS サーバへ送信します 。

アカウンティング情報の送信先 RADIUS サーバの選択を次の図に示します。

図 5-15 アカウンティング情報の送信先 RADIUS サーバの選択



当該認証専用 RADIUS サーバと汎用 RADIUS サーバが両方設定されているときは，当該認証専用 RADIUS サーバ宛に送信します。

(3) RADIUS サーバの選択と復旧

RADIUS サーバへアカウンティング情報の送達が確認できないときは，RADIUS 認証のときと同様に送信先 RADIUS サーバを順次選択します。

送達が確認できた時点で，「カレントサーバ」情報が遷移し，自動復旧時間（dead-interval タイマ）が起動します。

dead-interval タイマ値は，RADIUS 認証の設定値と同一の値が適用されますが，RADIUS 認証用の dead-interval タイマと，RADIUS アカウント機能用の dead-interval タイマは，それぞれ個別に起動し本装置内で管理します。dead-interval タイマのカウントや復旧などのシーケンスは，RADIUS 認証用と同一です。

運用コマンド clear radius-server で，起動中の dead-interval タイマをリセット（カレントサーバを初期値に戻す）した場合，RADIUS 認証用の dead-interval タイマと，RADIUS アカウント機能用の dead-interval タイマを同時にクリアします。

(4) RADIUS 属性

本機能で使用する RADIUS 属性の詳細は，各認証機能を参照してください。

- IEEE802.1X :「6.6 事前準備」
- Web 認証 :「8.5 事前準備 8.5.2 RADIUS 認証の場合」
- MAC 認証 :「10.5 事前準備 10.5.2 RADIUS 認証の場合」

5.4　レイヤ 2 認証の共通機能

レイヤ 2 認証共通で使用する，以下の機能について説明します。

- 認証前端末の通信許可（認証専用 IPv4 アクセスリスト）
- VLAN 名称による収容 VLAN 指定
- MAC VLAN の自動 VLAN 割当
- 同一 MAC ポートでの自動認証モード収容
- MAC ポートでの Tagged フレームの認証
- 認証共通の強制認証
- 認証共通の端末数制限
- ダイナミック ACL/QoS 機能
- ポートリンクダウン時の認証解除抑止

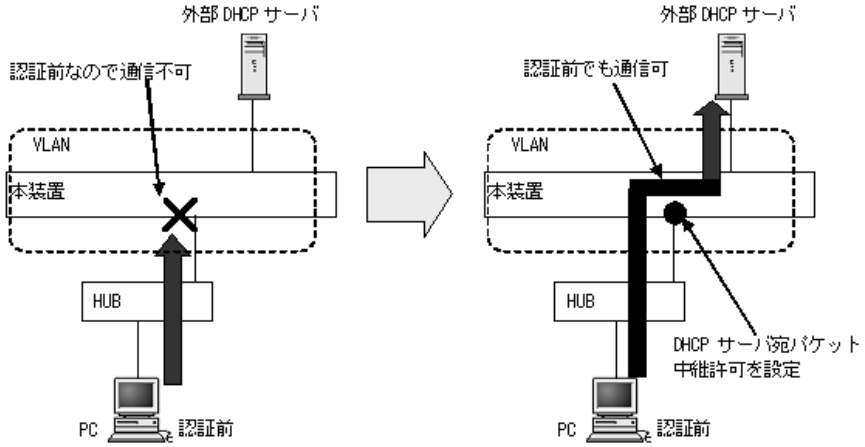
5.4.1　認証前端末の通信許可（認証専用 IPv4 アクセスリスト）

下記の機能および認証モードで，外部 DHCP サーバやドメインサーバを使用するときは，認証前にフレームを中継させる必要があります。

- IEEE802.1X：ポート単位認証（静的），ポート単位認証（動的）
- Web 認証：固定 VLAN モード，ダイナミック VLAN モード
- MAC 認証：固定 VLAN モード，ダイナミック VLAN モード

上記の各認証を実施する認証対象ポートに対して，認証専用の IPv4 アクセスリストをコンフィグレーションコマンド authentication ip access-group で設定して，認証前の端末から本装置外へ特定のフレームを送信できます。

図 5-16　認証専用 IPv4 アクセスリストの使用前と使用後



通常のアクセスリスト（コンフィグレーションコマンド ip access-group など）とは異なり，認証後は認証専用 IPv4 アクセスリストで設定されたフィルタ条件が適用されません。

認証対象ポートに通常のアクセスリストと認証専用 IPv4 アクセスリストを設定した場合，通常のアクセスリストのフィルタ条件が，認証前にも認証後にも適用されますので，認証専用 IPv4 アクセスリストに設定したフィルタ条件を通常のアクセスリストにも設定してください。

また，認証前の端末に本装置内蔵の DHCP サーバ機能から IP アドレスを配布する場合，および外部

DHCP サーバから IP アドレスを配布する場合，認証専用 IPv4 アクセスリストのフィルタ条件に，対象となる DHCP サーバ向けの DHCP パケットを通信させる設定が必要になります。この場合は，次に示すようにフィルタ条件を必ず設定してください。

［必要なフィルタ条件設定例］

DHCP サーバの IP アドレスが 10.10.10.254，認証対象端末のネットワークが 10.10.10.0/24 の場合

```
permit udp 10.10.10.0 0.0.0.255 host 10.10.10.254 eq bootps
permit udp host 0.0.0.0 host 10.10.10.254 eq bootps
permit udp host 0.0.0.0 host 255.255.255.255 eq bootps
```

［認証専用 IPv4 アクセスリスト設定時の注意］

コンフィグレーションコマンド authentication ip access-group を設定する場合，次の点に注意してください。

1. 認証専用 IPv4 アクセスリストの収容条件については，「コンフィグレーションガイド Vol.1 3.2 収容条件」を参照してください。
2. コンフィグレーションコマンド permit または deny によって次のフィルタ条件が指定されても，適用されません。
   - tcp ポートの range 指定
   - udp ポートの range 指定
   - class 指定（ダイナミック ACL/QoS 機能）
3. 設定した条件以外のフレーム廃棄設定は，本設定の収容条件数には含まれません。各認証機能で条件以外のフレーム廃棄設定が暗黙に設定されます。
4. 認証前の端末から送信される ARP フレームを中継させるため，コンフィグレーションコマンド authentication arp-relay を設定してください。
5. Web 認証専用 IP アドレス宛てパケットは，認証専用 IPv4 アクセスリストの結果に関わらず中継されません。

5.4.2 VLAN 名称による収容 VLAN 指定

各認証機能のダイナミック VLAN モードで収容する VLAN を，VLAN 名称で指定できます。VLAN 名称は，VLAN インタフェースのコンフィグレーションコマンド name で設定します。設定した VLAN 名称を RADIUS サーバに設定することで，ダイナミック VLAN モードの収容 VLAN を VLAN 名称で管理できます。

本機能が動作可能な認証モードを次の表に示します。

表 5-11 VLAN 名称指定が動作可能な認証モード

認証機能	認証モード	本機能の動作可否	備考
IEEE802.1X	ポート単位認証 (静的)	×	固定 VLAN モード
	ポート単位認証 (動的)	○	ダイナミック VLAN モード
Web 認証	固定 VLAN モード	×	
	ダイナミック VLAN モード	○	
MAC 認証	固定 VLAN モード	×	
	ダイナミック VLAN モード	○	

（凡例）

○：動作可能

×：動作不可

RADIUS サーバの設定については，各認証機能の解説編「事前準備」の「RADIUS サーバの準備」を参照してください。

5.4.3 MAC VLAN の自動 VLAN 割当

本装置では認証済み端末を収容する認証後 VLAN を，認証対象ポートに自動で割り当てることができます。自動割当は下記の認証結果で実施します。

- ローカル認証で認証成功時に，内蔵認証データベースから認証後 VLAN を指定されたとき
- RADIUS 認証で認証成功時に，RADIUS 属性で認証後 VLAN を指定されたとき
- 強制認証時に，認証後 VLAN を設定済みのとき

MAC VLAN の自動 VLAN 割当と解除は，上記の認証後 VLAN のコンフィグレーション設定有無とポートの認証済み端末の状態に従います。

また，コンフィグレーションコマンド no switchport mac auto-vlan を設定することで，ポートごとに自動 VLAN 割当を抑止することもできます。

自動 VLAN 割当と解除の条件と次の表に示します。

表 5-12 自動 VLAN 割当と解除の条件（自動 VLAN 割当抑止コマンド未設定）

認証後 VLAN のコンフィグレーション ポートの MAC VLAN 設定	ポートの認証済み端末の存在	自動 VLAN 割当と解除	備考
無	無 → 有	▲	※1
	有 → 無	▽	※2
無 → 有	有	▽	※3
有 → 無		▲	※1

（凡例）

▲ : VLAN を割り当てる

▽ : 割り当てた VLAN を解除

注 ※1

自動 VLAN 割当抑止コマンド no switchport mac auto-vlan が設定されている場合は，自動で VLAN は割り当てられません。端末は認証失敗（当該ポートに存在する認証済み端末は認証解除）となります。

注 ※2

下記の条件で認証済み端末がすべて認証解除された場合は，自動で割り当てた VLAN を当該ポートから解除します。

- 当該ポートの VLAN 内に認証済み端末が 1 台も存在しなくたったとき
- 当該ポートのリンクダウンにより，当該ポートのすべての認証済み端末が解除されたとき
- VLAN コンフィグレーション削除により，すべての認証済み端末が解除されたとき

注 ※3

コンフィグレーションコマンド switchport mac vlan で VLAN をポートに設定したときは，自動割当 VLAN は解除しますが，認証済みの端末は設定したコンフィグレーションに従いますので，認証は解除しません。

本機能が動作可能な認証モードを，次の表に示します。

表 5-13 自動 VLAN 割当が動作可能な認証モード

認証機能	認証モード	本機能の動作可否	備考
IEEE802.1X	ポート単位認証 (静的)	×	固定 VLAN モード
	ポート単位認証 (動的)	○	ダイナミック VLAN モード
Web 認証	固定 VLAN モード	×	
	ダイナミック VLAN モード	○	
MAC 認証	固定 VLAN モード	×	
	ダイナミック VLAN モード	○	

(凡例)
○：動作可能
×：動作不可

(1) 自動で割り当てた VLAN の扱いについて

本装置で自動で割り当てた VLAN は次のように扱います。

下記の機能と共存するときは，自動で割り当てた VLAN はそれぞれの機能に従い動作します。

- スパニングツリー
- アップリンク・リダンダント
- L2 ループ検知機能
- DHCP snooping（ダイナミック ARP 検査機能を含む）

5.4.4 同一 MAC ポートでの自動認証モード収容

本装置では，同一 MAC ポートで固定 VLAN モードとダイナミック VLAN モードを使用できます。

認証対象端末から Untagged フレームで受信したときに，認証結果で決定した収容 VLAN により，自動で認証対象端末を固定 VLAN モード，またはダイナミック VLAN モードの認証端末として管理します。

本機能が動作可能な認証モードを，次の表に示します。

表 5-14 同一 MAC ポートでの自動認証モード収容が動作可能な認証モード

認証機能	認証モード	本機能の動作可否	備考
IEEE802.1X	ポート単位認証 (静的)	○	固定 VLAN モード
	ポート単位認証 (動的)	○	ダイナミック VLAN モード
Web 認証	固定 VLAN モード	○	
	ダイナミック VLAN モード	○	
MAC 認証	固定 VLAN モード	○	
	ダイナミック VLAN モード	○	

(凡例)
○：動作可能
×：動作不可

（1） RADIUS 認証での自動認証モード収容

RADIUS 認証では，RADIUS サーバから受信した Access-Accept の RADIUS 属性の内容により，端末の認証モードを決定します。

対象となる RADIUS 属性は，RADIUS サーバから Access-Accept 受信時の「Tunnel-Type」「Tunnel-Medium-Type」「Tunnel-Private-Group-ID」です。

Access-Accept 受信時の RADIUS 属性の組み合わせによる動作を次の表に示します。

表 5-15　Access-Accept 受信時の RADIUS 属性の組合せによる動作

Tunnel-Type	Tunnel-Medium-Type	Tunnel-Private-Group-ID	認証動作	端末の認証モード状態
無	無	無	認証後 VLAN として，ネイティブ VLAN に収容	固定 VLAN モード
VLAN(13)	IEEE-802(6)	表 5-16 に従います	表 5-16 に従います	
上記以外の組み合わせ			認証失敗	認証失敗

表 5-16　RADIUS 認証時の Tunnel-Private-Group-ID に対応した処理

Tunnel-Private-Group-ID の内容	認証ポートのネイティブ VLAN と比較	認証動作	端末の認証モード状態	FDB※1 登録	MAC VLAN 登録
無または空の場合	－	ネイティブ VLAN に収容	固定 VLAN モード	登録	未登録
• 数値 • 文字列 VLAN 後に数値 • VLAN 名称	ネイティブ VLAN 以外 ※2	Tunnel-Private-Group-ID に指定された VLAN に収容 ※3	ダイナミック VLAN モード	登録	登録
	ネイティブ VLAN と同一	認証失敗	認証失敗によりモード未決定	未登録	未登録
	VLAN 名称無	認証失敗	認証失敗によりモード未決定	未登録	未登録
上記以外	－	認証失敗	認証失敗によりモード未決定	未登録	未登録

（凡例）

－：内容には依存しない

注 ※1

FDB：MAC アドレステーブルを示します。

- 固定 VLAN モードに収容した端末の MAC アドレスは，MAC アドレステーブルに認証エントリとして登録します。
- ダイナミック VLAN モードに収容した端末の MAC アドレスは，MAC アドレステーブルと MAC VLAN テーブルに認証エントリとして登録します。

注 ※2

当該認証ポートの switchport mac dot1q vlan の VLAN と一致した場合は，認証失敗となります。

注 ※3

Tunnel-Private-Group-ID で指定する VLAN は，コンフィグレーションコマンド vlan mac-based で本装置に設定しておいてください。

(2) ローカル認証での自動認証モード収容

ローカル認証では，内蔵認証データベースの VLAN 結果により，端末の認証モードを決定します。

表 5-17 ローカル認証時の VLAN 結果に対応した処理

内蔵認証データベースの認証結果 VLAN 有無	認証ポートのネイティブ VLAN と比較	認証動作	端末の認証モード状態	FDB※1 登録	MAC VLAN 登録
無または空の場合	ー	ネイティブ VLAN に収容	固定 VLAN モード	登録	未登録
有	ネイティブ VLAN 以外 ※2	内蔵認証データベースに指定された VLAN に収容 ※3	ダイナミック VLAN モード	登録	登録
	ネイティブ VLAN と同一	認証失敗	認証失敗によりモード未決定	未登録	未登録

(凡例)

ー：内容には依存しない

注 ※1

FDB：MAC アドレステーブルを示します。

- 固定 VLAN モードに収容した端末の MAC アドレスは，MAC アドレステーブルに認証エントリとして登録します。
- ダイナミック VLAN モードに収容した端末の MAC アドレスは，MAC アドレステーブルと MAC VLAN テーブルに認証エントリとして登録します。

注 ※2

当該認証ポートの switchport mac dot1q vlan の VLAN と一致した場合は，認証失敗となります。

注 ※3

内蔵認証データベースで指定する VLAN は，コンフィグレーションコマンド vlan mac-based で本装置に設定しておいてください。

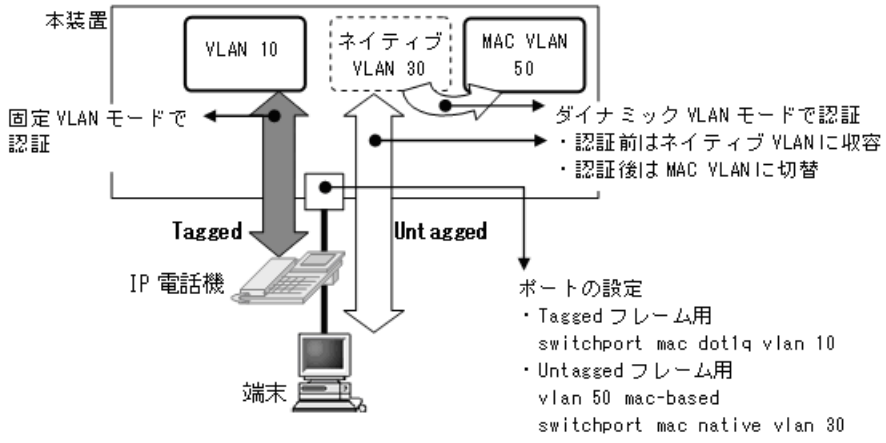
5.4.5 MAC ポートの Tagged フレームの認証（dot1q vlan 設定）

MAC ポートにコンフィグレーションコマンド switchport mac dot1q vlan を設定することにより，認証対象端末から Tagged フレームを受信したときに固定 VLAN モードの動作に従って認証します。

Untagged フレームはダイナミック VLAN モードの動作に従って認証します。Untagged フレームは認証前はネイティブ VLAN に収容し，認証成功後に認証後 VLAN に切り替えます。

MAC ポートに dot1q vlan を設定したときの動作を次の図に示します。

図 5-17 MAC ポートに dot1q vlan を設定したときの動作



各認証機能のポート内動作については，後述「5.7.2 同一ポート内で共存 (3) 同一ポートでダイナミック VLAN モードと固定 VLAN モードの共存」を参照してください。

5.4.6 認証共通の強制認証

コンフィグレーションコマンド authentication force-authorized enable を設定することで，認証共通で強制認証機能が有効になります。

本機能が動作する条件は下記のとおりです。

- 各認証機能の認証方式に「RADIUS 認証」だけを設定していること（RADIUS 認証とローカル認証の優先順を設定している場合は無効です。）
- 設定されている RADIUS サーバが無応答状態になったとき

本機能が動作する認証モードを次の表に示します。

表 5-18 認証共通の強制認証が動作する認証モード

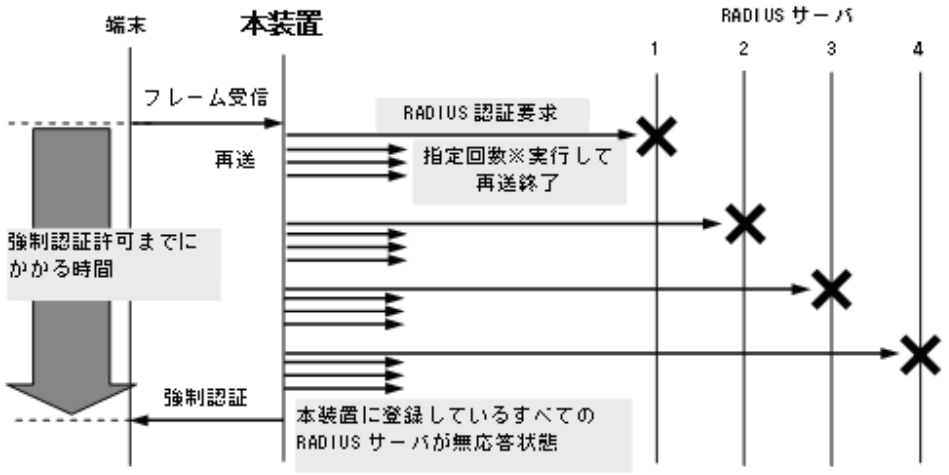
認証機能	認証モード	強制認証の動作
IEEE802.1X	ポート単位認証 (静的)	○
	ポート単位認証 (動的)	○
Web 認証	固定 VLAN モード	○
	ダイナミック VLAN モード	○
MAC 認証	固定 VLAN モード	○
	ダイナミック VLAN モード	○

（凡例）
○：動作可能
×：動作不可

(1) RADIUS 認証要求開始から強制認証許可までの動作

強制認証許可までの時間は，認証要求開始後から本装置に登録されているすべての RADIUS サーバのタイムアウトまでとなります。

図 5-18　強制認証許可までのシーケンス（RADIUS サーバ最大数設定時）



指定回数※：RADIUS サーバへの再送回数（デフォルト 3 回：コンフィグレーションで変更可）

認証要求端末ごとに，上記のシーケンスで強制認証許可までの時間を要します。

RADIUS サーバのリトライ回数は，汎用 RADIUS サーバ情報および認証専用 RADIUS サーバ情報それぞれのコンフィグレーションコマンドで，IP アドレスとともに設定できます。前述の「5.3.1　レイヤ 2 認証機能で使用する RADIUS サーバ情報」を参照してください。

また，RADIUS サーバ無応答状態となったとき，各認証機能で次の表に示すアカウントログを採取します。

表 5-19　各認証機能で採取するアカウントログ

認証機能	アカウントログメッセージ
IEEE802.1X	• No=82 WARNING:SYSTEM: (付加情報) Failed to connect to RADIUS server. 付加情報：IP アカウントログは運用コマンド show dot1x logging で確認できます。
Web 認証	• No=21 NOTICE:LOGIN:(付加情報) Login failed ; Failed to connection to RADIUS server. 付加情報：MAC，USER，IP，PORT，CHGR，VLAN アカウントログは運用コマンド show web-authentication logging で確認できます。
MAC 認証	• No=21 NOTICE:LOGIN: (付加情報) Login failed ; Failed to connection to RADIUS server 付加情報：MAC，PORT，CHGR，VLAN アカウントログは運用コマンド show mac-authentication logging で確認できます。

（2） 強制認証が動作するためのコンフィグレーション

認証共通の強制認証設定を動作するために，強制認証機能を有効にするとともに，下記に示す各認証機能のコンフィグレーション設定が必要です。

また，各認証で使用する RADIUS サーバ（RADIUS サーバグループ含む）は，通常状態で認証要求を送信できる有効な情報を設定してください。

表 5-20 強制認証が動作するためのコンフィグレーション

認証機能	認証モード	各認証機能のコンフィグレーション
IEEE802.1X	IEEE802.1X 共通	• dot1x system-auth-control 装置デフォルト • aaa authentication dot1x default group radius • dot1x radius-server host または radius-server host 認証方式リスト，ポート別認証方式 • aaa authentication dot1x <List name> group <Group name>※1 • aaa group server radius <Group name> • server • radius-server host
	ポート単位認証 (静的)	• dot1x port-control auto • switchport mode access • dot1x authentication※2
	ポート単位認証 (動的)	• vlan <VLAN ID> mac-based • dot1x port-control auto • switchport mode mac-vlan • dot1x authentication※2
Web 認証	Web 認証共通	• web-authentication system-auth-control 装置デフォルト • aaa authentication web-authentication default group radius※1 • web-authentication radius-server host または radius-server host 認証方式リスト，ポート別認証方式，ユーザ ID 別認証方式 • aaa authenticationweb-authentication <List name> group <Group name>※1 • aaa group server radius <Group name> • server • radius-server host • web-authentication user-group※3
	固定 VLAN モード	• web-authentication port • switchport mode access • web-authentication authentication※2
	ダイナミック VLAN モード	• vlan <VLAN ID> mac-based • web-authentication port • switchport mode mac-vlan • web-authentication authentication※2
MAC 認証	MAC 認証共通	• mac-authentication system-auth-control 装置デフォルト • aaa authentication mac-authentication default group radius※1 • mac-authentication radius-server host または radius-server host 認証方式リスト，ポート別認証方式 • aaa authentication mac-authentication <List name> group <Group name>※1 • aaa group server radius <Group name> • server • radius-server host

認証機能	認証モード	各認証機能のコンフィグレーション
	固定 VLAN モード	• mac-authentication port • switchport mode access • mac-authentication authentication※2
	ダイナミック VLAN モード	• vlan <VLAN ID> mac-based • mac-authentication port • switchport mode mac-vlan • mac-authentication authentication※2

注 ※1

装置デフォルトで強制認証使用時は，「default group radius」だけ設定してください。

ポート別認証方式またはユーザ ID 別認証方式使用時は，「<List name> group <Group name>」を設定してください。

注 ※2

ポート別認証方式使用時に設定してください。

注 ※3

ユーザ ID 別認証方式使用時に設定してください。

（3） 強制認証での収容 VLAN について

ダイナミック VLAN モードの収容 VLAN はコンフィグレーションコマンド authentication force-authorized vlan で設定します。

本コマンド設定を省略したときは，該当端末をネイティブ VLAN に収容します。このとき該当端末を固定 VLAN モードの端末として扱います。

また，本コマンドの設定変更前に強制認証で VLAN に収容した端末は，設定変更後も次の認証契機まで収容 VLAN を変更しません。

（4） 強制認証でのプライベート Trap

認証共通の強制認証では，各認証機能で特定のアカウントログ（SYSTEM）採取を契機に，「表 5-18　認証共通の強制認証が動作する認証モード」に該当する認証モードで強制認証用のプライベート Trap が発行可能となります。

表 5-21　アカウントログ (SYSTEM) とプライベート Trap 発行条件

認証機能	認証モード	Trap 発行に必要なコンフィグレーション設定	
		コマンド	パラメータ
IEEE802.1X	ポート単位認証 (静的)	snmp-server host	dot1x
		authentication force-authorized	enable
	ポート単位認証 (動的)	snmp-server host	dot1x
		authentication force-authorized	enable
		authentication force-authorized	vlan※

認証機能	認証モード	Trap 発行に必要なコンフィグレーション設定	
		コマンド	パラメータ
Web 認証	固定 VLAN モード	snmp-server host	web-authentication
		authentication force-authorized	enable
	ダイナミック VLAN モード	snmp-server host	web-authentication
		authentication force-authorized	enable
		authentication force-authorized	vlan※
MAC 認証	固定 VLAN モード	snmp-server host	mac-authentication
		authentication force-authorized	enable
	ダイナミック VLAN モード	snmp-server host	mac-authentication
		authentication force-authorized	enable
		authentication force-authorized	vlan※

注※

authentication force-authorized vlan 未設定時は固定 VLAN モード管理となります。前述の「(3) 強制認証での収容 VLAN について」を参照してください。

5.4.7 認証失敗時の端末管理

本装置では，レイヤ 2 認証機能で認証に失敗した端末情報を，失敗端末リストとして MAC アドレス単位で最大 256 端末まで管理します。失敗端末リストは，運用コマンド show authentication fail-list で表示できます。

各認証機能では，端末の認証失敗が確定したときに，失敗端末リストに登録します。認証失敗時の処理は，ローカル認証・RADIUS 認証ともに共通です。

認証失敗時の端末情報の処理を次の表に示します。

表 5-22 認証失敗時の端末情報の処理

認証機能	項目	新規認証契機での認証結果		再認証契機での認証結果	
		Reject	Reject 以外での失敗	Reject	Reject 以外での失敗
IEEE802.1X	認証管理テーブルの該当端末ステータス	"HELD" (quiet-period 時間保持)	"Connecting" (次の認証待ち)	"HELD" (quiet-period 時間保持)	"Connecting" (次の認証待ち)
	MAC アドレステーブルの該当端末エントリ状態	－	－	削除	削除
	失敗端末リスト (fail-list) への登録契機	失敗時に即時登録	失敗時に即時登録	失敗時に即時登録	失敗時に即時登録
Web 認証	認証管理テーブルの該当端末ステータス	該当エントリ削除	該当エントリ削除	" 認証済 " (既存エントリを残し，時間更新無)	" 認証済 " (既存エントリを残し，時間更新無)
	MAC アドレステーブルの該当端末エントリ状態	－	－	登録状態のまま	登録状態のまま
	失敗端末リスト (fail-list) への登録契機	失敗時に即時登録	失敗時に即時登録	失敗時に即時登録	失敗時に即時登録

認証機能	項目	新規認証契機での認証結果		再認証契機での認証結果	
		Reject	Reject 以外での失敗	Reject	Reject 以外での失敗
MAC 認証	認証管理テーブルの該当端末ステータス	" 保留 " (quiet-period 時間保持)	" 保留 " (quiet-period 時間保持)	" 保留 " (quiet-period 時間保持)	" 保留 " (quiet-period 時間保持)
	MAC アドレステーブルの該当端末エントリ状態	－	－	削除	削除
	失敗端末リスト (fail-list) への登録契機	quiet-period 満了後に登録	quiet-period 満了後に登録	quiet-period 満了後に登録	quiet-period 満了後に登録

（凡例）
－：新規認証で失敗したので，MAC アドレステーブルには該当端末のエントリ無

5.4.8 認証共通の端末数制限

レイヤ 2 認証共通で認証数の制限を設定できます。設定する単位を次に示します。

- ポート単位
- 装置単位

(1) ポート単位の認証数制限

コンフィグレーションコマンド authentication max-user で，ポート単位に認証数の制限を設定できます。
各レイヤ 2 認証で認証された数がポート単位に設定された制限値を超えた場合，認証エラーとなります。

(2) 装置単位の認証数制限

コンフィグレーションコマンド authentication max-user で，装置単位に認証数の制限を設定できます。
各レイヤ 2 認証で認証された合計数が装置単位に設定された制限値を超えた場合，認証エラーとなります。

(3) 認証数制限を適用できるレイヤ 2 認証

ポート単位の認証数制限，および装置単位の認証数制限を適用できるレイヤ 2 認証を次の表に示します。

表 5-23 認証数制限を適用できるレイヤ 2 認証

認証機能	認証モード	ポート単位の認証数制限	装置単位の認証数制限
IEEE802.1X	ポート単位認証 (静的)	○	○
	ポート単位認証 (動的)	○	○
Web 認証	固定 VLAN モード	○	○
	ダイナミック VLAN モード	○	○
MAC 認証	固定 VLAN モード	○	○
	ダイナミック VLAN モード	○	○

（凡例）
○：適用可能

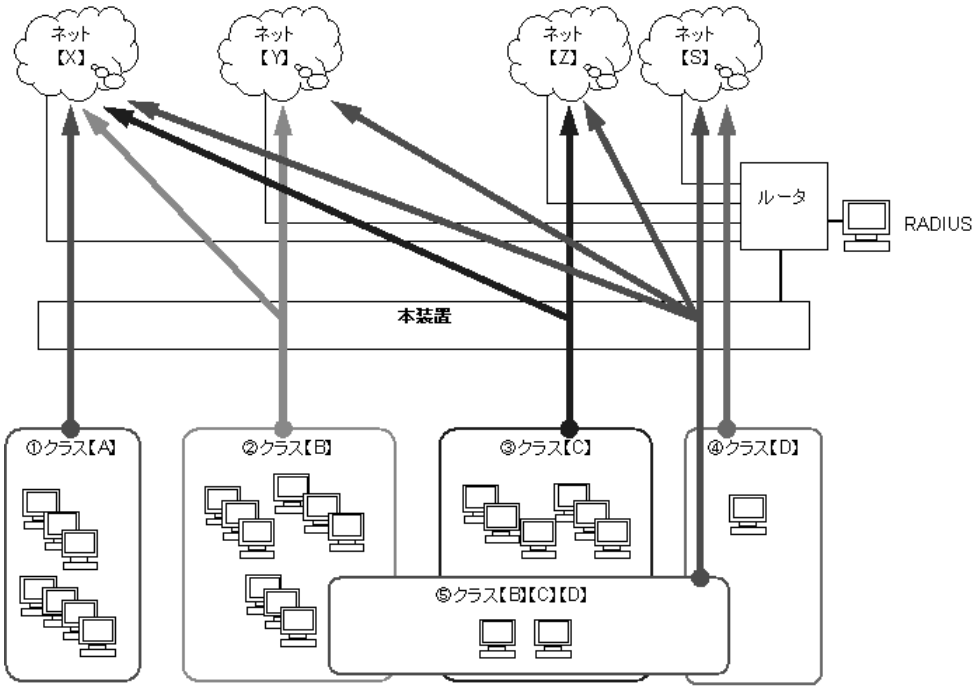
5.4.9 ダイナミック ACL/QoS 機能

（1） 概要

本機能は，各種レイヤ 2 認証機能で認証済みとなった端末（またはユーザ）を，一律に通信許可とせず，認証済み端末に付与されたクラスでネットワークのアクセス制御を行います。

本機能は，RADIUS サーバ，および本装置の認証機能とフィルタ /QoS 機能を併用します。RADIUS サーバと本装置の認証機能により，認証済み端末ごとに所属クラスを付与します。付与された所属クラスのネットワークアクセス制御を，フィルタ /QoS 機能で実現します。

図 5-19 ダイナミック ACL/QoS 機能の概要



図内の各クラスに所属する端末とアクセス可能なネットワーク

①クラス【A】に所属する端末：ネット【X】だけにアクセス可能
②クラス【B】に所属する端末：ネット【X】【Y】にアクセス可能
③クラス【C】に所属する端末：ネット【X】【Z】にアクセス可能
④クラス【D】に所属する端末：ネット【S】にのみアクセス可能
⑤クラス【B】【C】【D】に所属する端末：全ネットワークにアクセス可能

（a） 本機能の動作契機

本機能を有効にするコンフィグレーションはありません。レイヤ 2 認証を実施した際に，RADIUS サーバから端末に付与された RADIUS 属性を識別して動作します。

（b） RADIUS サーバの事前設定

端末に付与する所属クラスは，RADIUS サーバにあらかじめ設定します。端末を認証する RADIUS サーバで，端末ごとに RADIUS 属性に所属クラスを設定します。RADIUS サーバの事前設定内容と条件を次の表に示します。

表 5-24 RADIUS サーバの事前設定内容と条件

項目	内容	条件など
RADIUS 属性	"Filter-Id"	複数の情報は，スラッシュ（/）で区切ること
記述ルール	区切り文字	スラッシュ（/）
	クラス情報	"/Class= 整数 " のフォーマットで記述する • "Class" は語頭だけ大文字 • "=" は必須 • 0 から 63 までの 10 進整数 • すべてスペース無で記述

上記フォーマット以外の場合，当該クラス情報は無効です。

なお，マルチステップ認証と併用する場合は，"/MultiStep/Class=37"（マルチステップ認証対象，端末の所属クラス 37）のように設定してください。

(c) 認証機能サポート範囲

ダイナミック ACL/QoS 機能が動作する認証機能を次の表に示します。

表 5-25 ダイナミック ACL/QoS 機能が動作する認証機能

認証機能	固定 VLAN モード	ダイナミック VLAN モード	認証方式	
			ローカル	RADIUS
IEEE802.1X	○	○	−	○
Web 認証	○	○	×	○
MAC 認証	○	○	×	○
マルチステップ認証	○	○	×	○

（凡例）
○：動作可
×：動作不可
−：ローカル認証なし

ダイナミック ACL/QoS 機能で認証する端末数は，「コンフィグレーションガイド Vol.1 3.2 収容条件」に示す認証の収容条件に含みます。また，認証機能と DHCP snooping 併用時の認証端末数の制限も同様です。

(d) フィルタ /QoS 機能

RADIUS サーバから付与された所属クラスごとのネットワークアクセス制御は，フィルタ /QoS 機能で行うため，既存のフィルタ /QoS 機能にクラスおよびクラスマスク指定を追加します。クラス指定は受信側だけが有効です。送信側には指定できません。

フィルタ /QoS 機能のサポート有無を次の表に示します。

表 5-26 フィルタ /QoS 機能のサポート有無

機能	アクセスリスト /QoS フローリスト		サポート有無
フィルタ	IPv4 アクセスリスト	standard(permit/deny)	×
		extended(permit/deny)	○
	IPv6 アクセスリスト	extended(permit/deny)	○

機能	アクセスリスト /QoS フローリスト		サポート有無
	MAC アクセスリスト	extended(permit/deny)	○
QoS	IPv4QoS フローリスト		○
	IPv6QoS フローリスト		○
	MACQoS フローリスト		○

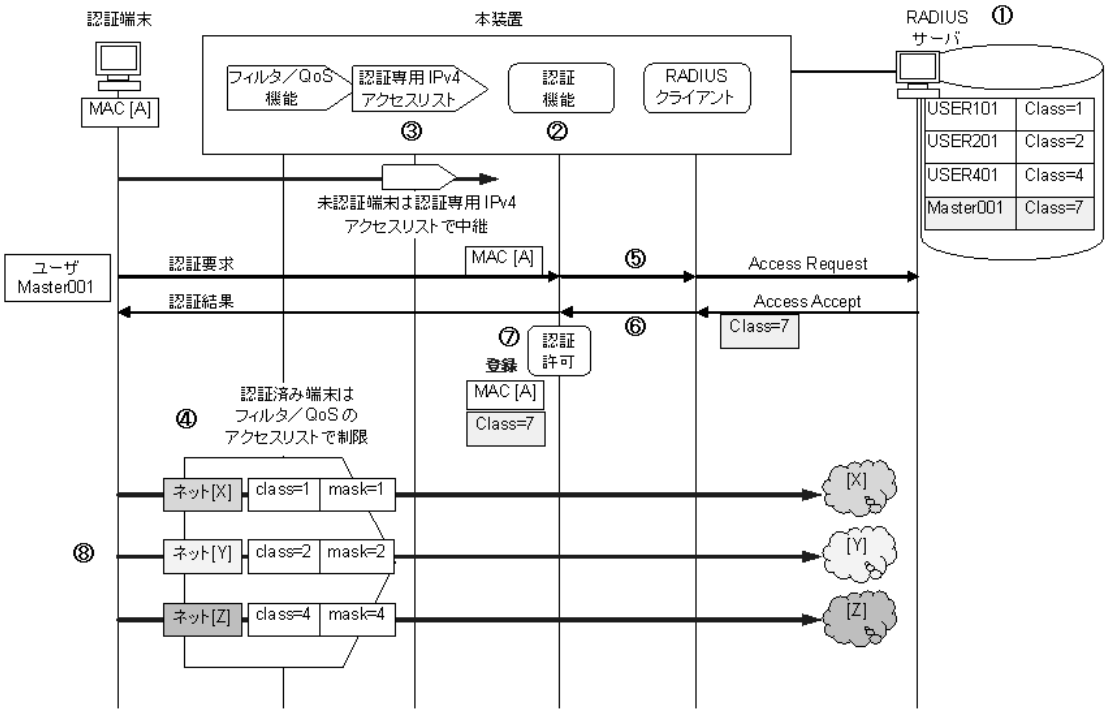
（凡例）
○：サポート
×：未サポート

ダイナミック ACL/QoS 機能で使用するフィルタエントリおよび QoS エントリは，「コンフィグレーションガイド Vol.1 3.2　収容条件」に示すフィルタ /QoS 機能の収容条件に含みます。

（2） 動作概要

本機能を使用するための事前設定と動作概要を次の図に示します。

図 5-20　ダイナミック ACL/QoS 機能の動作概要



【事前設定】（①～④は上記図内の①～④に該当します）

① RADIUS サーバ

各レイヤ 2 認証に対応するユーザ名と所属クラス（Class）を設定します。

②本装置：認証機能

使用するレイヤ 2 認証機能を設定します。

③本装置：認証専用 IPv4 アクセスリスト（ARP リレー含む）

未認証端末がアクセス可能なネットワーク条件などを設定します。

④本装置：フィルタ /QoS 機能

認証済み端末の所属クラスのアクセス条件として，クラス (class) とネットワークなどを設定しま

す。クラスはマスク (mask) 指定することも可能です。

【動作概要】(⑤～⑧は上記図内の⑤～⑧に該当します)

⑤未認証端末からの認証要求

未認証端末（MAC[A]）の「MASTER001」ユーザから認証要求されると，本装置は RADIUS サーバに対して Access Request を発行し，認証を実施します。

⑥ RADIUS サーバからの応答

RADIUS サーバは，「MASTER001」ユーザを検出し Access Accept を本装置に応答します。この際，クラス情報（本例では Class=7）を RADIUS 属性に付与して応答します。

⑦本装置に認証結果の登録と「MASTER001」ユーザへ認証結果通知

本装置の認証機能では，端末 MAC[A] とクラス情報（この例では Class=7）を登録して認証許可状態とし，「MASTER001」ユーザへ認証結果（認証許可）を通知します。

⑧認証済み端末からのアクセス制限

認証済み端末（MAC[A]）からのアクセスは，フィルタ /QoS 機能によりアクセス可能なネットワークが制限されます。

本装置で，認証済み端末（MAC[A]）の所属クラスとフィルタ /QoS 機能に設定したクラスマスクの論理積を，フィルタ /QoS 機能に設定したクラス値と比較して，ネットワークのアクセスを制限します。

上記例では，端末 MAC[A] の所属クラスが Class=7 であるため，ネット [X]，ネット [Y]，ネット [Z] の各クラスとクラスマスク条件と一致します。従って，端末 MAC[A] は，全ネットワークへのアクセスが可能な端末となります。

(3) 端末の所属クラスとフィルタ /QoS エントリの関係

認証済み端末の所属クラスと，フィルタ /QoS エントリの関係を次の表に示します。

表 5-27　認証済み端末の所属クラス

RADIUS 認証後のクラス情報付与の有無	端末の所属クラス
クラス情報　付与有	当該クラスに所属
クラス情報　付与無	クラス ＝ 0 に所属 ※

注 ※

RADIUS 認証で強制認証となった場合も，クラス＝ 0 として扱います。

表 5-28　フィルタ /QoS エントリの検索動作

クラス指定有無	クラスマスク指定有無	検索動作
－	－	クラス = any として検索
○	－	クラスマスク = 63（フルマスク）で検索
○	○	該当クラスと該当マスクで検索

(凡例)

○：指定有

－：指定無

認証済み端末の所属クラスと，フィルタ /QoS エントリの検索条件を下記に示します。なお，クラスマスクは，ワイルドカードではなく，マスクで扱います。

【検索条件】

① < 認証済み端末の所属クラス > と < フィルタ /QoS エントリのクラスマスク > の論理積を算出
（クラスマスクを 2 進数としたときに，"1" となったビットが比較対象です。）
② ①の算出結果と < フィルタ /QoS エントリのクラス > を比較
③ ②で一致した場合：
- 当該エントリの他のフィルタ /QoS 条件に一致すれば当該エントリの条件を適用
- 当該エントリの他のフィルタ /QoS 条件に一致しない場合は，次のエントリを検索

④ ②で一致しなければ，次のエントリを検索
⑤ どのエントリにも一致しなければ，フィルタの場合は暗黙の deny となりアクセス拒否とする

フィルタエントリの設定例，端末の所属クラスと端末から受信する宛先アドレス，およびフィルタエントリの検索例を以下に示します。

［フィルタ（アクセスリスト）エントリの設定例］

```
10 permit ip any 192.168.40.0 0.0.0.255 class 4
20 permit ip any 192.168.40.0 0.0.0.255 class 4 mask 4
30 permit ip any 192.168.40.0 0.0.0.255
（暗黙の deny）
```

表 5-29　フィルタエントリの検索例

端末の所属クラスと端末から受信する宛先アドレスの例		フィルタエントリの検索結果（数字はフィルタエントリのシーケンス番号）			
所属クラス	宛先アドレス	10	20	30	暗黙の deny
0	192.168.40.1	×	×	○	－
3	192.168.40.20	×	×	○	－
4	192.168.40.30	○	－	－	－
5	192.168.40.100	×	○	－	－
17	192.168.50.1	×	×	×	○

（凡例）
○：フィルタエントリに一致
×：フィルタエントリに不一致
－：先のシーケンス番号のエントリに一致したので検索しない

上記の表では，端末の所属クラスが 5（000101）の場合は，下記のように検索します。

1. エントリ 10 は mask 未指定のため，クラスマスク 63（111111）として扱います。所属クラスとクラスマスクの論理積は 5（000101）となり，class 4（000100）と不一致のため次のエントリを検索します。
2. エントリ 20 の mask 4（000100）と所属クラス 5 の論理積は 4（000100）となり，class 4（000100）と一致します。その他のフィルタ /QoS 条件も一致するため，端末はエントリ 20 の条件でアクセス許可となります。

（4）クラスごとのアクセス制御の定義について

クラスごとのアクセス制御は，「表 5-26　フィルタ /QoS 機能のサポート有無」に示すコンフィグレーションで，ネットワークアクセス条件に加えて，クラス（class），クラスマスク（mask）を指定します。

- クラス（class）：端末が所属するクラスを指定します。
- クラスマスク（mask）：複数クラスに所属する端末をマスク管理します。

ここでは，クラスごとのアクセス制御の定義例として，１端末が１つのクラスにだけ所属するケース１と，１端末が複数クラスに所属するケース２を説明します。

(a) ケース 1

１端末が１クラスにだけ所属するケースです。

このケースでは，クラスマスクを使用しません。以下のような端末のクラスとフィルタ設定で，アクセス制御ができます。

【端末のクラス】

クラス 10：端末 A001，A002，A003・・・
クラス 20：端末 B001，B002，B003・・・
クラス 30：端末 C001，C002，C003・・・
クラス 40：端末 D001，D002，D003・・・

【フィルタ設定】

アクセス先ネットワーク [X][Y][Z][Q] に対して，各クラスのアクセス条件とフィルタ設定例を次の表に示します。

表 5-30 ケース 1 のフィルタ設定例

アクセス先ネットワーク	アクセス条件	フィルタ設定例	備考
ネット [X]	クラス 20 だけをアクセス拒否	deny ネット [X] class 20	
ネット [Y]	クラス 10 だけをアクセス許可	permit ネット [Y] class 10	
ネット [Z]	クラス 30 とクラス 40 をアクセス許可	permit ネット [Z] class 30 permit ネット [Z] class 40	
ネット [Q]	全クラスのアクセス許可	permit ネット [Q]	クラス指定しない

(b) ケース 2

クラスとネットワークを関連付けし，１端末が複数クラスに所属するケースです。

このケースでは，クラスとネットワークを関連付けし，クラスマスクを併用してクラスをビットで意味づけすることで，端末を複数クラスに所属できます。これにより，以下のような端末グループのクラスとフィルタ設定で，端末の複数クラスのアクセス制御ができます。

【クラスとネットワークの関連付け】

各ネットワークのアクセスを許可するクラスを下記のように関連付けします。

クラス 4　ネット [X]　：役員専用ネットワーク
クラス 8　ネット [Y]　：総務系ネットワーク
クラス 16　ネット [Z]　：共有ネットワーク
クラス 32　ネット [Q]　：各部門を個別管理

【端末グループのクラス】

アクセスするネットワークのクラスを加算した値を，各グループのクラス値とします。

クラス 28（クラス 4 ＋クラス 8 ＋クラス 16）　：役員グループ
クラス 24（クラス 8 ＋クラス 16）　：総務グループ
クラス 48（クラス 16 ＋クラス 32）　：各部門グループ

RADIUS サーバには，加算したクラス値を各グループの端末に付与するクラス値として設定してくだ

さい。

【フィルタ設定】

各端末グループのアクセス条件とフィルタ設定例を次の表に示します。

表 5-31 ケース 2 のフィルタ設定例

端末グループ	アクセス条件	フィルタ設定例
役員	役員専用ネットワーク 総務系ネットワーク 共有ネットワーク にアクセス許可	permit ネット [X] class 4 mask 4 permit ネット [Y] class 8 mask 8 permit ネット [Z] class 16 mask 16 permit ネット [Q] class 32 mask 32
総務	総務系ネットワーク 共有ネットワーク にアクセス許可	
各部門	部門ネットワーク 共有ネットワーク にアクセス許可	

5.4.10 ポートリンクダウン時の認証解除抑止

認証済み端末の所属ポートでリンクダウンが発生したときは端末を認証解除しますが，コンフィグレーションの設定（no authentication logout linkdown）により，認証解除を抑止できます。

本機能が動作可能な認証モードを次の表に示します。

表 5-32 ポートリンクダウン時の認証解除抑止が動作可能な認証モード

認証機能	認証モード	本機能の動作可否	備考
IEEE802.1X	ポート単位認証 (静的)	○	固定 VLAN モード
	ポート単位認証 (動的)	○	ダイナミック VLAN モード
Web 認証	固定 VLAN モード	○	
	ダイナミック VLAN モード	○	
MAC 認証	固定 VLAN モード	○	
	ダイナミック VLAN モード	○	

（凡例）

○：動作可能

本機能はポート単位（物理ポート / ポートチャネルインタフェース）で設定可能です。

本機能を設定したポートは，リンクダウン条件での認証解除だけを抑止します。リンクダウン検出時は，マルチステップ認証の 1 段目完了済み端末や，MAC 認証の保留中端末などを含めた，全認証端末情報を保持します。

従って，無通信監視など，その他の認証解除条件で解除するか，移動先ポートでのローミング成立まで認証端末情報を保持します。

5.5　レイヤ 2 認証共通のコンフィグレーション

5.5.1　コンフィグレーションコマンド一覧

本項では，レイヤ 2 認証で共通で使用するコンフィグレーションについて説明します。

表 5-33　レイヤ 2 認証共通のコンフィグレーションコマンドと認証モード一覧

コマンド名	説明	認証モード	
		固	ダ
authentication arp-relay	認証前端末から受信する ARP パケットを他ポートに中継します。	○	○
authentication ip access-group	認証前端末から受信した IP パケットに本コマンドで指定した IPv4 アクセスリストを適用し，合致 (permit) したパケットだけを他ポートに中継します。	○	○
authentication auto-logout strayer	Web 認証 /MAC 認証の認証済み端末が，Web 認証 /MAC 認証未設定ポートに移動したことを検出したときに，認証を解除します。	○	○
authentication force-authorized enable	認証共通の強制認証を有効にします。	○	○
authentication force-authorized vlan	該当ポートのダイナミック VLAN モード共通で収容する，認証後 VLAN を設定します。	○	○
authentication logout linkdown	no authentication logout linkdown 設定時，認証済み端末の所属ポートがリンクダウンしても認証解除しません。	○	○
authentication max-user (global)	装置単位の認証数制限値を設定します。	○	○
authentication max-user (interface)	ポート単位の認証数制限値を設定します。	○	○
name	VLAN に VLAN 名称を設定します。	－	○
switchport mac auto-vlan	no switchport mac auto-vlan 設定時，認証機能による認証後 VLAN が switchport mac vlan で指定された VLAN と一致するときだけ通信できます。 (MAC VLAN の自動 VLAN 割当を抑止)	－	○

(凡例)

固：固定 VLAN モード

ダ：ダイナミック VLAN モード

○：設定内容に従って動作します

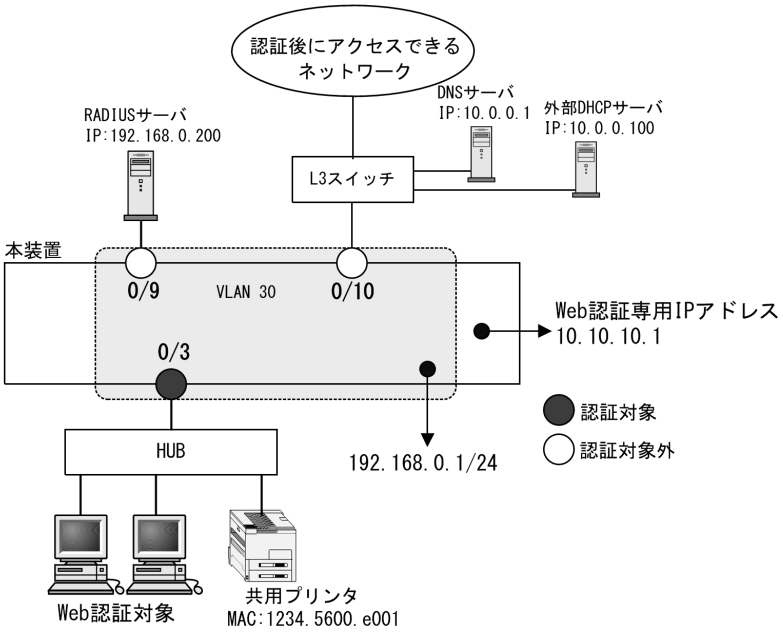
×：コマンドを入力できません

－：「5.4.2　VLAN 名称による収容 VLAN 指定」の対象外です

5.5.2　認証専用 IPv4 アクセスリストの設定

本例では，Web 認証固定 VLAN モードで外部 DHCP サーバを使用する構成とします。Web 認証固定 VLAN モードのコンフィグレーションは「9.3　固定 VLAN モードのコンフィグレーション」を参照してください。

図 5-21 認証専用 IPv4 アクセスリストの使用例



[設定のポイント]

認証前の端末から本装置の外部への通信を許可する，認証専用 IPv4 アクセスリストと ARP フレームの中継を設定します。

（その他の認証に必要なコンフィグレーションは設定済みとし，本例では認証前中継用の設定だけを記載しています。）

[コマンドによる設定]

1. **(config)# ip access-list extended L2-auth**
   (config-ext-nacl)# permit udp any any eq bootps
   (config-ext-nacl)# permit ip any host 10.0.0.1
   (config-ext-nacl)# exit
   (config)# interface gigabitethernet 0/3
   (config-if)# web-authentication port
   (config-if)# authentication ip access-group L2-auth
   (config-if)# authentication arp-relay
   (config-if)# exit

   認証前の端末から DHCP フレーム（bootp）と IP アドレス 10.0.0.1（DNS サーバ）へのアクセスを許可する認証専用 IPv4 アクセスリストを設定します。

   ポート 0/3 に，認証モード設定（web-authentication port）と認証前アクセス条件のアクセスリスト名（L2-auth）を設定します。

   さらに，ARP フレームを本装置の外部に中継させるように設定します。

[注意事項]

1. ポートに認証専用 IPv4 アクセスリストおよび ARP フレーム中継の設定を実施する前に，下記のいずれかを設定してください。
   - dot1x port-control auto
   - web-authentication port
   - mac-authentication port
2. 認証専用 IPv4 アクセスリストおよび ARP フレーム中継を設定しているポートの認証モード設定

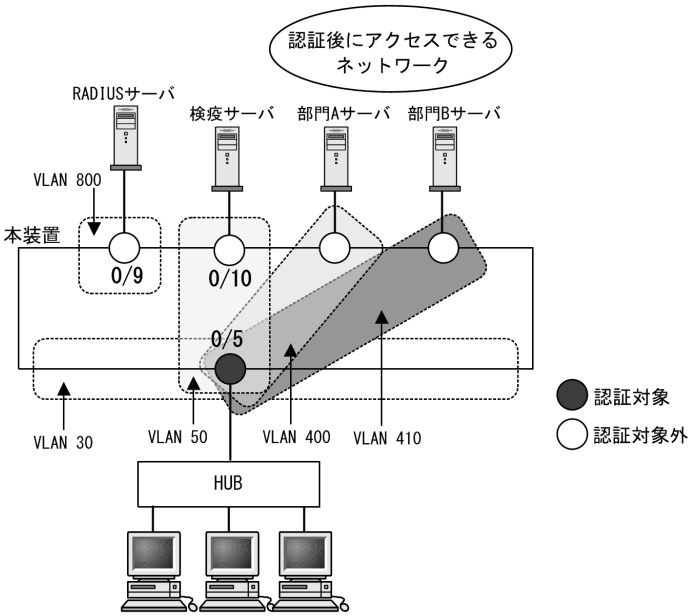
を削除する場合は，先に下記コマンドを両方とも該当ポートから削除してください。

- authentication arp-relay
- authentication ip access-group

5.5.3　VLAN 名称による収容 VLAN 指定

本例では，Web 認証ダイナミック VLAN モードを使用する構成とします。

図 5-22　ダイナミック VLAN モードの VLAN 名称指定の使用例



［設定のポイント］

ダイナミック VLAN モードを設定し，収容する VLAN に管理名称を設定します。また，RADIUS サーバに認証後に収容する VLAN を管理名称で設定します。

- VLAN 30：認証前 VLAN
- VLAN 50：検疫 VLAN
- VLAN400：認証後の部門 A ネットワーク
- VLAN410：認証後の部門 B ネットワーク

その他の Web 認証に必要な設定は，「9　Web 認証の設定と運用」を参照してください。

［コマンドによる設定］

1. **(config)# vlan 30,800**
   (config-vlan)# exit
   VLAN ID 30，800 を設定します。

2. **(config)# vlan 50 mac-based**
   (config-vlan)# name Keneki-Network
   (config-vlan)# exit
   VLAN ID 50 に MAC VLAN と検疫 VLAN 名称を設定します。

3. **(config)# vlan 400 mac-based**

```
(config-vlan)# name GroupA-Network
(config-vlan)# exit
```
VLAN ID 400 に MAC VLAN と認証後の部門 A ネットワーク VLAN 名称を設定します。

4.
```
(config)# vlan 410 mac-based
(config-vlan)# name GroupB-Network
(config-vlan)# exit
```
VLAN ID 410 に MAC VLAN と認証後の部門 B ネットワーク VLAN 名称を設定します。

5.
```
(config)# interface gigabitethernet 0/5
(config-if)# switchport mode mac-vlan
(config-if)# switchport mac native vlan 30
```
ポート 0/5 を MAC ポートとして設定します。また，MAC ポートのネイティブ VLAN30（認証前 VLAN）を設定します。（認証後 VLAN は「5.4.3　MAC VLAN の自動 VLAN 割当」により割り当てられます。）

6.
```
(config-if)# web-authentication port
(config-if)# exit
```
ポート 0/5 に認証モード（web-authentication port）を設定します。

7.
```
(config)# interface gigabitethernet 0/9
(config-if)# switchport mode access
(config-if)# switchport access vlan 800
(config-if)# exit
```
ポート 0/9 を VLAN800 のアクセスポートとして設定します。認証は除外するので認証モードは設定しません。図内の RADIUS サーバ用ポートに設定します。

8.
```
(config)# interface gigabitethernet 0/10
(config-if)# switchport mode access
(config-if)# switchport access vlan 50
(config-if)# exit
```
ポート 0/10 を VLAN50 のアクセスポートとして設定します。認証は除外するので認証モードは設定しません。図内の検疫サーバ用ポートに設定します。

RADIUS サーバには，下記を設定してください。

- 検疫 NG のとき：Tunnel-Group-ID に "Keneki-Network"
- 検疫 OK のとき
  - 部門 A の認証後 VLAN へ切り替え：Tunnel-Group-ID に "GroupA-Network"
  - 部門 B の認証後 VLAN へ切り替え：Tunnel-Group-ID に "GroupB-Network"

［注意事項］

1. コンフィグレーションコマンド name で設定する VLAN 名称を，RADIUS 認証の認証後 VLAN として使用するときは下記に注意してください。
   - VLAN 名称が，複数の VLAN で重複しないように設定してください。VLAN 名称が重複していると，重複しているうちで最も小さい VLAN ID が RADIUS 認証の認証後 VLAN として割り当てられます。
   - VLAN 名称の先頭に数字を指定しないでください。先頭の数字を VLAN ID として認識し，認

証に失敗する場合があります。

2. RADIUS サーバから認証成功（Accept）受信で，RADIUS 属性に認証後 VLAN 情報がないときは，該当 MAC ポートのネイティブ VLAN に端末を収容します。このとき端末は固定 VLAN モードの認証済み端末として扱います。
3. 認証後 VLAN を「5.4.3　MAC VLAN の自動 VLAN 割当」で割り当てるときは，下記を設定してください。
   - コンフィグレーションコマンド vlan mac-based
     RADIUS サーバから通知される VLAN を設定してください。（この場合は，MAC ポートにコンフィグレーションコマンド switchport mac vlan による設定は不要です。）
4. MAC VLAN の自動 VLAN 割当を抑止する場合は，下記を設定してください。
   - コンフィグレーションコマンド no switchport mac auto-vlan
   - コンフィグレーションコマンド switchport mac vlan
     RADIUS サーバから通知される VLAN を設定してください。

5.5.4　認証共通の強制認証設定

認証共通で使用する強制認証機能を設定します。

［設定のポイント］

本例では , マルチステップ認証使用時の強制認証を設定します。

- 各認証機能の認証方式は，RADIUS 認証方式を設定します。
- ポート 0/1 にマルチステップ認証を設定します。
- 強制認証時に収容する VLAN を設定します。

なお，認証ポートの認証後 VLAN は，「5.4.3　MAC VLAN の自動 VLAN 割当」により割り当てられるものとします。
その他のマルチステップ認証に必要な設定は，「12　マルチステップ認証」を参照してください。

［コマンドによる設定］

1. **(config)# vlan 40,600 mac-based**
   (config-vlan)# exit
   VLAN ID 40，600 に MAC VLAN を設定します。

2. **(config)# vlan 20**
   (config-vlan)# exit
   VLAN ID 20 を設定します。

3. **(config)# aaa authentication web-authentication default group radius**
   (config)# aaa authentication mac-authentication default group radius
   各認証機能の認証方式に RADIUS 認証を設定します。

4. **(config)# authentication force-authorized enable**
   認証共通の強制認証を有効にします。

5. **(config)# interface gigabitethernet 0/1**
   (config-if)# switchport mode mac-vlan
   (config-if)# switchport mac native vlan 20
   (config-if)# mac-authentication port

(config-if)# web-authentication port
(config-if)# authentication multi-step
ポート 0/1 に MAC ポート，Web 認証モード，MAC 認証モード，マルチステップ認証モードを設定します。また，MAC ポートのネイティブ VLAN20（認証前 VLAN）を設定します。（認証後 VLAN は「5.4.3　MAC VLAN の自動 VLAN 割当」により割り当てられます。）

6. **(config-if)# authentication force-authorized vlan 600**
   (config-if)# exit
   強制認証時の収容 VLAN に 600 を設定します。

［注意事項］

1. 各認証機能の認証方式は，RADIUS 認証だけ設定してください。RADIUS 認証とローカル認証の優先順を設定していると，強制認証機能は無効となります。
2. 本例のマルチステップ認証のときは，RADIUS サーバ側の RADIUS 属性 Filter-Id に下記を設定してください。
   - MAC 認証で認証する RADIUS サーバ："@@Web-Auth@@"
3. RADIUS サーバから認証成功（Accept）受信で，RADIUS 属性に認証後 VLAN 情報がないときは，該当 MAC ポートのネイティブ VLAN に端末を収容します。このとき端末は固定 VLAN モードの認証済み端末として扱います。
4. 認証後 VLAN を「5.4.3　MAC VLAN の自動 VLAN 割当」で割り当てるときは，下記を設定してください。
   - コンフィグレーションコマンド vlan mac-based
     RADIUS サーバから通知される VLAN を設定してください。（この場合は，MAC ポートにコンフィグレーションコマンド switchport mac vlan による設定は不要です。）
5. MAC VLAN の自動 VLAN 割当を抑止する場合は，下記を設定してください。
   - コンフィグレーションコマンド no switchport mac auto-vlan
   - コンフィグレーションコマンド switchport mac vlan
     RADIUS サーバから通知される VLAN を設定してください。

5.5.5　認証共通の認証数制限の設定

（1） 装置単位の認証数制限値の設定

［設定のポイント］
レイヤ 2 認証の装置単位の認証数制限を設定します。

［コマンドによる設定］

1. **(config)# authentication max-user 512**
   レイヤ 2 認証の装置単位の認証数制限を 512 に設定します。

（2） ポート単位の認証数制限値の設定

［設定のポイント］
レイヤ 2 認証のポート単位の認証数制限を設定します。

［コマンドによる設定］

1. **(config)# interface gigabitethernet 0/1**

```
(config-if)# switchport mode mac-vlan
(config-if)# switchport mac native vlan 20
(config-if)# mac-authentication port
(config-if)# web-authentication port
(config-if)# authentication max-user 64
(config-if)# exit
```

認証対象ポート 0/1 の認証数制限を 64 に設定します。

5.5.6 ダイナミック ACL/QoS 機能のアクセス制御の設定

ダイナミック ACL/QoS 機能自体を有効にするコンフィグレーションはありませんが，RADIUS サーバから付与されたクラス情報に対するネットワークのアクセス制御はフィルタ /QoS 機能で設定します。

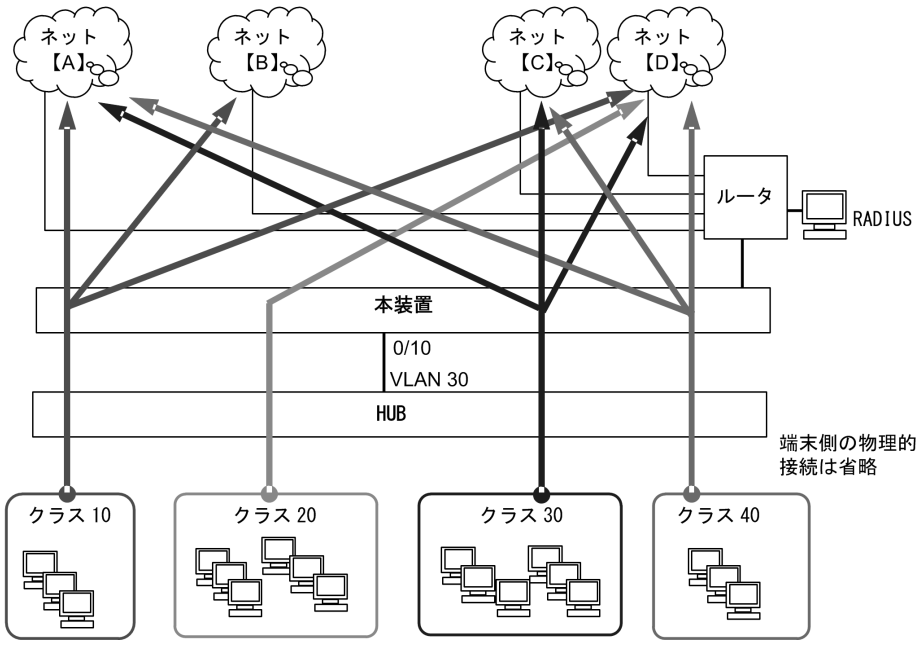
フィルタ /QoS 機能は，受信側フロー検出モード flow detection mode layer2-2 を設定済みとします。

レイヤ 2 認証機能として必要な条件は設定済みとし，ここではダイナミック ACL/QoS 機能のアクセス制御に必要な設定について説明します。

(1) ケース 1：端末が 1 クラスに所属する場合の設定

本例では，端末が 1 クラスに所属する場合のネットワークアクセス条件を設定します。

図 5-23 端末が 1 クラスに所属する場合の構成例



［設定のポイント］

本装置の認証ポートは Web 認証，MAC 認証混在で，固定 VLAN モードを使用します。

端末はクラス 10，20，30，40 のいずれかに所属するよう RADIUS サーバに設定します。

アクセス先ネットワークと各クラスのアクセス条件を次の表に示します。

本例では，端末側の送信元ネットワークは限定しないものとします。

表 5-34 アクセス先ネットワークとアクセス条件

アクセス先ネットワーク		アクセス条件	備考
ネット [A]	100.10.10.0/24	クラス 20 だけをアクセス拒否	
ネット [B]	100.20.20.0/24	クラス 10 だけをアクセス許可	
ネット [C]	100.30.30.0/24	クラス 30 とクラス 40 をアクセス許可	
ネット [D]	200.10.10.0/24	全クラスのアクセス許可	クラス指定しない

［コマンドによる設定］

1. **(config)# ip access-list extended authen-classes**
   (config-ext-nacl)# deny ip any 100.10.10.0 0.0.0.255 class 20
   (config-ext-nacl)# permit ip any 100.20.20.0 0.0.0.255 class 10
   (config-ext-nacl)# permit ip any 100.30.30.0 0.0.0.255 class 30
   (config-ext-nacl)# permit ip any 100.30.30.0 0.0.0.255 class 40
   (config-ext-nacl)# permit ip any 200.10.10.0 0.0.0.255
   (config-ext-nacl)# exit
   アクセスリスト authen-classes に，アクセス条件，ネットワーク条件，およびクラスを設定します。

2. **(config)# vlan 30**
   (config-vlan)# exit
   VLAN30 を設定します。

3. **(config)# aaa authentication web-authentication default group radius**
   (config)# aaa authentication mac-authentication default group radius
   Web 認証の RADIUS 認証方式，MAC 認証の RADIUS 認証方式を設定します。

4. **(config)# interface gigabitethernet 0/10**
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 30
   (config-if)# web-authentication port
   (config-if)# mac-authentication port
   認証を行う端末が接続されているポート 0/10 をアクセスポートとして設定し，認証用 VLAN30，Web 認証モード，MAC 認証モードを設定します。

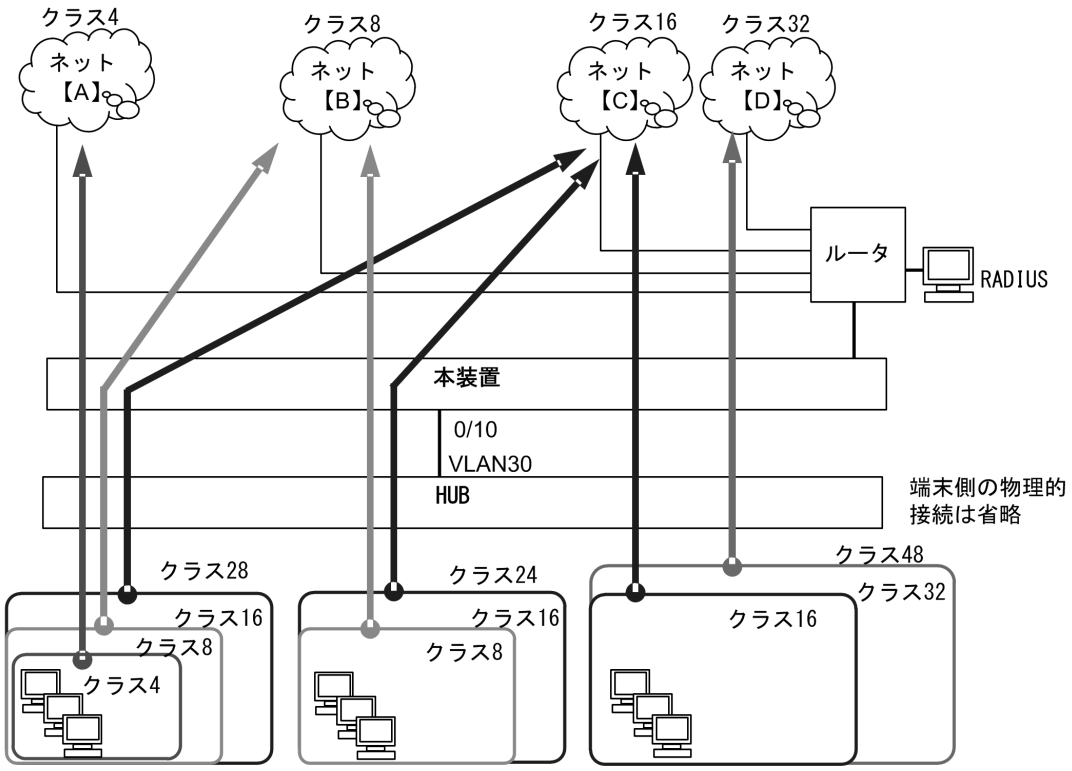
5. **(config-if)# ip access-group authen-classes in**
   (config-if)# exit
   ポート 0/10 に，受信側フィルタとして authen-classes を設定します。

6. **(config)# web-authentication system-auth-control**
   (config)# mac-authentication system-auth-control
   Web 認証，MAC 認証を有効にします。

(2) ケース 2：端末が複数クラスに所属する場合の設定

本例では，クラスとネットワークを関連付けし，端末が複数クラスに所属する場合のネットワークアクセス条件を設定します。

図 5-24 端末が複数クラスに所属する場合の構成例



［設定のポイント］

本装置の認証ポートは Web 認証，MAC 認証混在で，固定 VLAN モードを使用します。
クラスとネットワークを関連付けし，端末のグループとクラスを以下のように設定します。

【クラスとネットワークの関連付け】

各ネットワークのアクセスを許可するクラスを下記のように関連付けします。

クラス 4　ネット [A]　：役員専用ネットワーク
クラス 8　ネット [B]　：総務系ネットワーク
クラス 16　ネット [C]　：共有ネットワーク
クラス 32　ネット [D]　：各部門を個別管理

【端末グループのクラス】

アクセスするネットワークのクラスを加算した値を，各グループのクラス値とします。

クラス 28（クラス 4 ＋クラス 8 ＋クラス 16）　：役員グループ
クラス 24（クラス 8 ＋クラス 16）　：総務グループ
クラス 48（クラス 16 ＋クラス 32）　：各部門グループ

RADIUS サーバには，加算したクラス値を各グループの端末に付与するクラス値として設定してください。

表 5-35 端末グループとアクセス条件

端末グループ	アクセス条件	アクセス先ネットワーク
役員	役員専用ネットワーク 総務系ネットワーク 共有ネットワーク にアクセス許可	役員専用ネットワーク：ネット [A] 192.10.10.0/24 総務系ネットワーク　：ネット [B] 192.20.20.0/24 共有ネットワーク　　：ネット [C] 192.30.30.0/24 各部門ネットワーク　：ネット [D] 192.200.20.0/24
総務	総務系ネットワーク 共有ネットワーク にアクセス許可	
各部門	部門ネットワーク 共有ネットワーク にアクセス許可	

［コマンドによる設定］

1. **(config)# ip access-list extended authen-class-group**
   (config-ext-nacl)# permit ip any 192.10.10.0 0.0.0.255 class 4 mask 4
   (config-ext-nacl)# permit ip any 192.20.20.0 0.0.0.255 class 8 mask 8
   (config-ext-nacl)# permit ip any 192.30.30.0 0.0.0.255 class 16 mask 16
   (config-ext-nacl)# permit ip any 192.200.20.0 0.0.0.255 class 32 mask 32
   (config-ext-nacl)# exit
   アクセスリスト authen-class-group に，アクセス条件，ネットワーク条件，クラス，およびクラスマスクを設定します。

2. **(config)# vlan 30**
   (config-vlan)# exit
   VLAN30 を設定します。

3. **(config)# aaa authentication web-authentication default group radius**
   (config)# aaa authentication mac-authentication default group radius
   Web 認証の RADIUS 認証方式，MAC 認証の RADIUS 認証方式を設定します。

4. **(config)# interface gigabitethernet 0/10**
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 30
   (config-if)# web-authentication port
   (config-if)# mac-authentication port
   認証を行う端末が接続されているポート 0/10 をアクセスポートとして設定し，認証用 VLAN30，Web 認証モード，MAC 認証モードを設定します。

5. **(config-if)# ip access-group authen-class-group in**
   (config-if)# exit
   ポート 0/10 に，受信側フィルタとして authen-class-group を設定します。

6. **(config)# web-authentication system-auth-control**
   (config)# mac-authentication system-auth-control
   Web 認証，MAC 認証を有効にします。

5.5.7 ポートリンクダウン時の認証解除抑止設定

［設定のポイント］

認証済み端末の所属ポートがリンクダウンしても，端末を認証解除しないように設定します。

［コマンドによる設定］

1. **(config)# interface gigabitethernet 0/1**
   (config-if)# no authentication logout linkdown
   (config-if)# exit
   ポート 0/1 がリンクダウンしても，当該ポートの認証済み端末がリンクダウンしないように設定します。

5.6　レイヤ 2 認証共通のオペレーション

5.6.1　運用コマンド一覧

本節では，レイヤ 2 認証共通で使用する運用コマンドについて説明します。

表 5-36　レイヤ 2 認証共通の運用コマンド一覧

コマンド名	説明
show authentication fail-list	レイヤ 2 認証に失敗した端末情報を MAC アドレス昇順で表示します。
clear authentication fail-list	レイヤ 2 認証に失敗した端末情報をクリアします。
show authentication logging	各レイヤ 2 認証が採取している動作ログメッセージを採取順に表示します。
clear authentication logging	採取順に表示した動作ログメッセージをクリアします。

5.7　レイヤ 2 認証機能の共存使用

本節では，認証モードを「固定 VLAN モード」「ダイナミック VLAN モード」で表記します。
IEEE802.1X の認証モードは下記が相当します。

- ポート単位認証（静的）：固定 VLAN モード
- ポート単位認証（動的）：ダイナミック VLAN モード

5.7.1　装置内で共存

装置内で，ポートの種類により認証機能の共存，固定 VLAN モードとダイナミック VLAN モードの共存が可能です。

共存使用例と動作可否を下記に示します。

図 5-25　共存使用例と動作可否

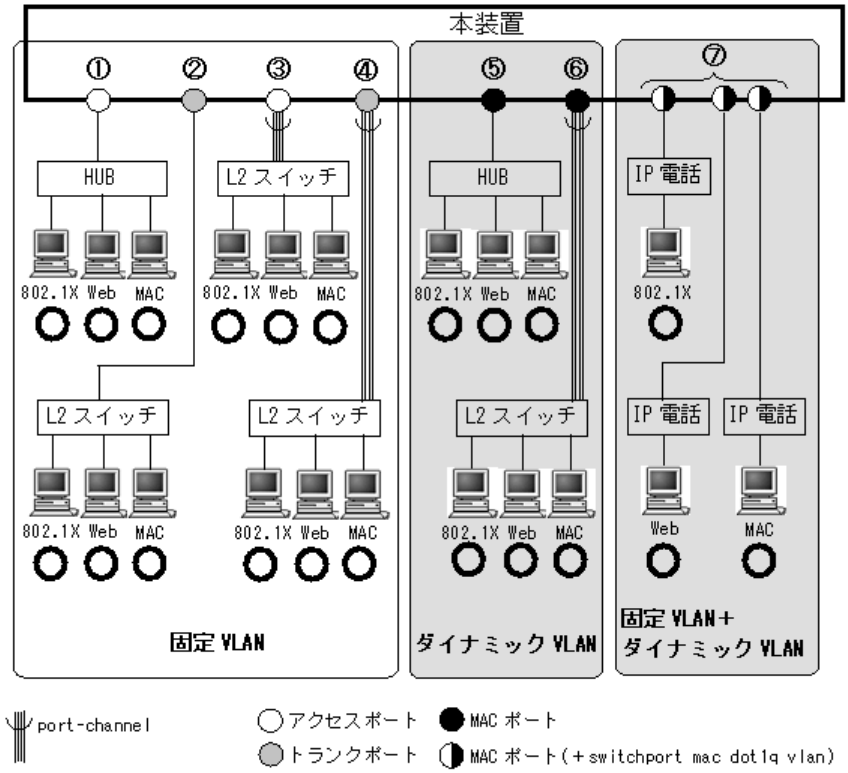


表 5-37　認証モードとポートの種類の組み合わせと認証機能の動作可否

認証モード	図内	ポートの種類	各認証機能の動作可否と該当する認証モード		
分類	番号		IEEE802.1X	Web 認証	MAC 認証
固定 VLAN	①	アクセス	○ ポート単位認証 （静的）	○ 固定 VLAN モード	○ 固定 VLAN モード
	②	トランク	○ ポート単位認証 （静的）	○ 固定 VLAN モード	○ 固定 VLAN モード

認証モード分類	図内番号	ポートの種類	各認証機能の動作可否と該当する認証モード		
			IEEE802.1X	Web 認証	MAC 認証
	③	アクセス（port-channel）	○ ポート単位認証（静的）	○ 固定 VLAN モード	○ 固定 VLAN モード
	④	トランク（port-channel）	○ ポート単位認証（静的）	○ 固定 VLAN モード	○ 固定 VLAN モード
ダイナミック VLAN	⑤	MAC	○ ポート単位認証（動的）	○ ダイナミック VLAN モード	○ ダイナミック VLAN モード
	⑥	MAC（port-channel）	○ ポート単位認証（動的）	○ ダイナミック VLAN モード	○ ダイナミック VLAN モード
固定 VLAN ＋ ダイナミック VLAN	⑦	MAC※（Tagged）	○ ポート単位認証（静的）	○ 固定 VLAN モード	○ 固定 VLAN モード
		MAC※（Untagged）	○ ポート単位認証（動的）	○ ダイナミック VLAN モード	○ ダイナミック VLAN モード

（凡例）
○：動作可
×：動作不可
－：該当外

注 ※
本例は，MAC ポートに Tagged フレーム中継許可設定（コンフィグレーションコマンド switchport mac dot1q vlan）している場合です。この場合，IP 電話からは Tagged フレームを受信して固定 VLAN モードで認証し，端末からは Untagged フレームを受信してダイナミック VLAN モードで動作します。
また，MAC ポートで Untagged フレームだけを対象にしている場合でも，固定 VLAN モードとダイナミック VLAN モードを共存できます。詳細は，「5.4.4　同一 MAC ポートでの自動認証モード収容」を参照してください。

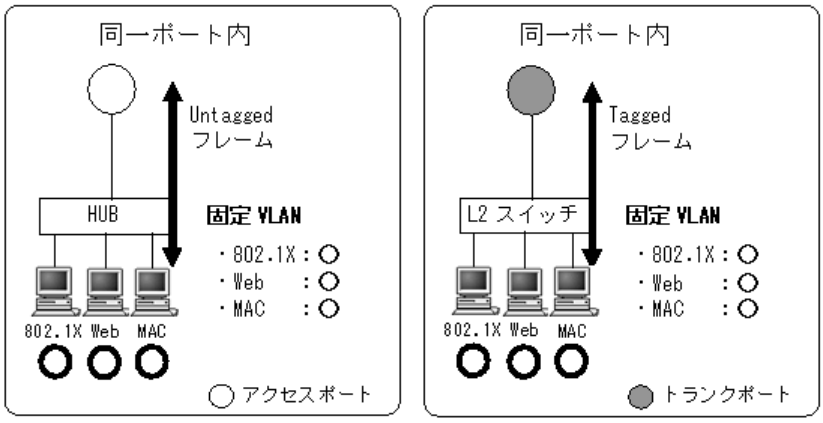
5.7.2　同一ポート内で共存

同一ポート内でも，下記の共存が可能です。

- 固定 VLAN モードの共存
- ダイナミック VLAN モードの共存
- ダイナミック VLAN モードと固定 VLAN モードの共存

（1） 同一ポートで固定 VLAN モードの共存

図 5-26 同一ポート内固定 VLAN モードの共存例



同一ポートで固定 VLAN モードの共存を使用するときには，「図 5-26 同一ポート内固定 VLAN モードの共存例」に示すように本装置に接続するポートの種類をアクセスポートまたはトランクポートにすることで，IEEE802.1X，Web 認証，MAC 認証の全認証機能で対応が可能です。ただし，コンフィグレーションの設定内容によっては，動作不可となる認証機能があります。

「表 5-38 アクセスポートでの設定内容における認証機能の動作可否」にアクセスポートでの固定 VLAN モードの共存を行うときに，コンフィグレーションの設定内容によって認証機能の動作可否を示します。

表 5-38 アクセスポートでの設定内容における認証機能の動作可否

コンフィグレーションの設定内容		認証機能		
共通の設定	認証機能の設定	IEEE802.1X	Web 認証	MAC 認証
switchport mode access switchport access	dot1x port-control auto dot1x multiple-authentication ※ web-authentication port mac-authentication port	○	○	○
	web-authentication port mac-authentication port	×	○	○
	dot1x port-control auto dot1x multiple-authentication ※ mac-authentication port	○	×	○
	dot1x port-control auto dot1x multiple-authentication ※ web-authentication port	○	○	×

（凡例）
○：動作可
×：動作不可

注 ※
Web 認証または MAC 認証を設定したポートに IEEE802.1X のポート単位認証を設定するときは，端末認証モード（dot1x multiple-authentication）を設定してください。

「表 5-39 トランクポートでの設定内容における認証機能の動作可否」にトランクポートでの固定 VLAN モードの共存を行うときに，コンフィグレーションの設定内容によって認証機能の動作可否を示します。

表 5-39 トランクポートでの設定内容における認証機能の動作可否

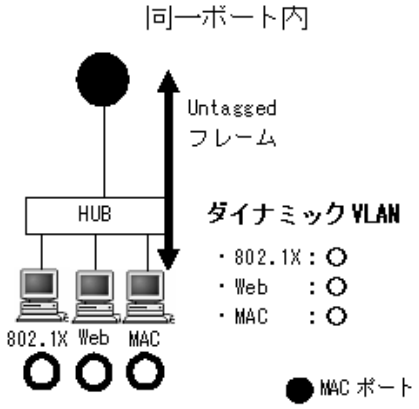
コンフィグレーションの設定内容		認証機能		
共通の設定	認証機能の設定	IEEE802.1X	Web 認証	MAC 認証
switchport mode trunk switchport trunk	dot1x port-control auto dot1x multiple-authentication ※ web-authentication port mac-authentication port	○	○	○
	web-authentication port mac-authentication port	×	○	○
	dot1x port-control auto dot1x multiple-authentication ※ mac-authentication port	○	×	○
	dot1x port-control auto dot1x multiple-authentication ※ web-authentication port	○	○	×

（凡例）
○：動作可
×：動作不可

注 ※
Web 認証または MAC 認証を設定したポートに IEEE802.1X のポート単位認証を設定するときは，端末認証モード（dot1x multiple-authentication）を設定してください。

（2） 同一ポートでダイナミック VLAN モードの共存

図 5-27 同一ポート内ダイナミック VLAN モードの共存例



同一ポートでダイナミック VLAN モードの共存を使用するときには，「図 5-27 同一ポート内ダイナミック VLAN モードの共存例」に示すように本装置に接続するポートの種類を MAC ポートにすることで，IEEE802.1X，Web 認証，MAC 認証の全認証機能で対応が可能です。ただし，コンフィグレーションの設定内容によっては，動作不可となる認証機能があります。

詳細は「表 5-40 MAC ポートでの設定内容における認証機能の動作可否」に示します。

表 5-40 MAC ポートでの設定内容における認証機能の動作可否

コンフィグレーションの設定内容		認証機能		
共通の設定	認証機能の設定	IEEE802.1X	Web 認証	MAC 認証
vlan xx mac-based ※1 switchport mode mac-vlan ※2	dot1x port-control auto dot1x multiple-authentication ※3 web-authentication port mac-authentication port	○	○	○
no switchport mac auto-vlan※4 switchport mac vlan xx※4	web-authentication port mac-authentication port	×	○	○
	dot1x port-control auto dot1x multiple-authentication ※3 mac-authentication port	○	×	○
	dot1x port-control auto dot1x multiple-authentication ※3 web-authentication port	○	○	×

（凡例）

○：動作可

×：動作不可

注 ※1

MAC ポートの認証後 VLAN は「5.4.3 MAC VLAN の自動 VLAN 割当」により割り当てられます。

注 ※2

RADIUS サーバから Accept 受信で，RADIUS 属性に自動 VLAN 割当情報がないときは，該当 MAC ポートのネイティブ VLAN に端末を収容します。このとき端末は固定 VLAN モードの認証済み端末として扱います。

注 ※3

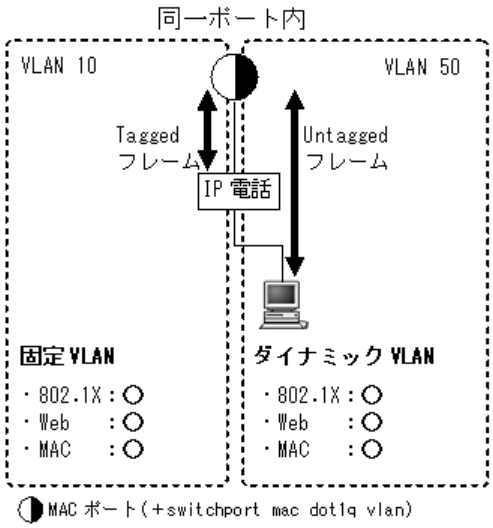
Web 認証または MAC 認証を設定したポートに IEEE802.1X のポート単位認証を設定するときは，端末認証モード（dot1x multiple-authentication）を設定してください。

注 ※4

MAC VLAN の自動 VLAN 割当を抑止する場合に設定してください。

（3）同一ポートでダイナミック VLAN モードと固定 VLAN モードの共存

図 5-28　同一ポート内ダイナミック VLAN モードと固定 VLAN モードの共存例



同一ポートで固定 VLAN モードとダイナミック VLAN モードの共存を使用するときには，「図 5-28　同一ポート内ダイナミック VLAN モードと固定 VLAN モードの共存例」に示すように本装置に接続するポートの種類を MAC ポートにすることで，実現することができます。ただし，コンフィグレーションの設定内容によっては，動作不可となる認証機能があります。

詳細は「表 5-41　MAC ポートでの設定内容における固定 VLAN モードとダイナミック VLAN モードの共存での認証機能の動作可否」に示します。

表 5-41　MAC ポートでの設定内容における固定 VLAN モードとダイナミック VLAN モードの共存での認証機能の動作可否

コンフィグレーションの設定内容	フレーム種別	認証機能		
		IEEE802.1X	Web 認証	MAC 認証
・vlan 50 mac-based ※1※4 ・switchport mode mac-vlan ・switchport mac dot1q vlan 10 ※1 ・no switchport mac auto-vlan※6 ・switchport mac vlan 50 ※6	Tagged	○ ※2	○ ※2	○ ※2
	Untagged	● ※3	● ※3	● ※3
		○ ※5	○ ※5	○ ※5

（凡例）

○：固定 VLAN モードで動作可

●：ダイナミック VLAN モードで動作可

注 ※1

「図 5-28　同一ポート内ダイナミック VLAN モードと固定 VLAN モードの共存例」を参考にして VLAN 番号を記載しています。各認証モード（dot1x port-control auto，web-authentication port，mac-authentication port）は設定済みとします。

注 ※2

Tagged フレームを受信して，固定 VLAN モードで認証します。（「図 5-28　同一ポート内ダイナミック VLAN モードと固定 VLAN モードの共存例」の例では，IP 電話の認証動作となります。）

注 ※3

Untagged フレームを受信して，ダイナミック VLAN モードで認証します。(「図 5-28　同一ポート内ダイナミック VLAN モードと固定 VLAN モードの共存例」の例では，端末の認証動作となります。)

注 ※4

MAC ポートの認証後 VLAN は，「5.4.3　MAC VLAN の自動 VLAN 割当」により割り当てられます。

注 ※5

RADIUS サーバから Accept 受信で，RADIUS 属性に自動 VLAN 割当情報がないときは，該当 MAC ポートのネイティブ VLAN に端末を収容します。このとき端末は固定 VLAN モードの認証済み端末として扱います。

注 ※6

MAC VLAN の自動 VLAN 割当を抑止する場合に設定してください。

5.8　レイヤ２認証共存のコンフィグレーション

レイヤ２認証の共存のコンフィグレーション例として，次の例を示します。

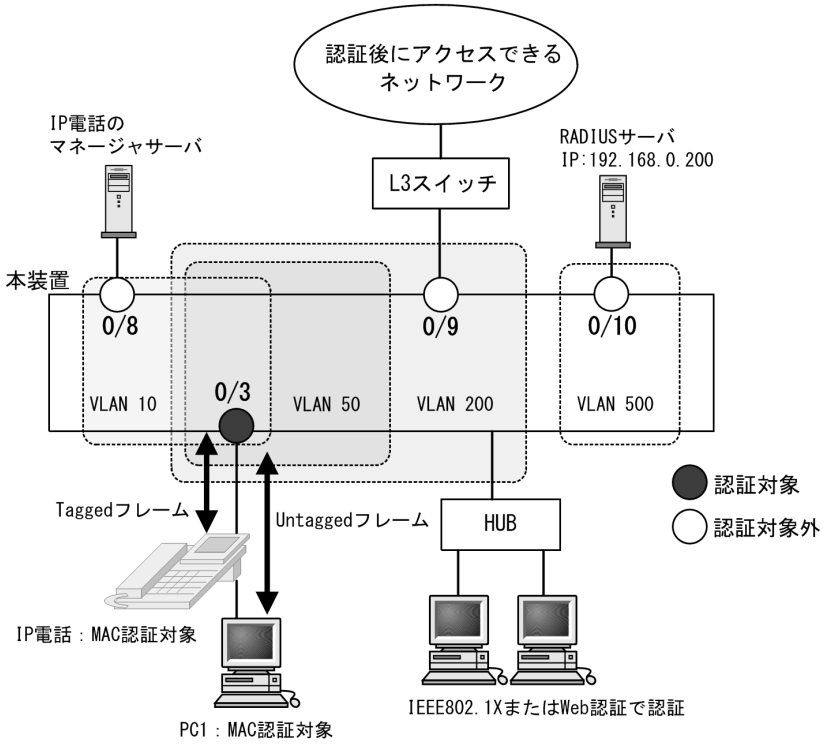
- 同一ポートで固定 VLAN モードとダイナミック VLAN モードを共存
  「5.8.1　MAC ポートで Tagged フレームを認証する設定」を参照してください。

5.8.1　MAC ポートで Tagged フレームを認証する設定

MAC ポートでは，コンフィグレーションコマンド switchport mac dot1q vlan を設定することで Tagged フレームを中継します。

本例では MAC 認証を使用し，同一ポートで Tagged フレームを固定 VLAN モードで認証し，Untagged フレームをダイナミック VLAN モードで認証します。

図 5-29　MAC ポートで Tagged フレームを認証する構成例



［設定のポイント］

MAC 認証対象ポートに MAC ポートを設定し，同一 MAC ポートで Tagged フレームと Untagged フレームを扱うポートとして設定します。認証方式は RADIUS 認証の例とします。

- VLAN 10：Tagged フレームを扱い，固定 VLAN モードで認証
- VLAN 50，200：Untagged フレームを扱い，ダイナミック VLAN モードで認証（認証前 VLAN：50，認証後 VLAN：200）

なお，認証ポートの認証後 VLAN は，「5.4.3　MAC VLAN の自動 VLAN 割当」により割り当てられるものとします。
その他の MAC 認証に必要な設定は，「11　MAC 認証の設定と運用」を参照してください。

［コマンドによる設定］

1. **(config)# vlan 200 mac-based**
   (config-vlan)# exit
   VLAN ID 200 に MAC VLAN を設定します。

2. **(config)# vlan 10,50,500**
   (config-vlan)# exit
   VLAN ID 10，50，500 を設定します。

3. **(config)# interface gigabitethernet 0/3**
   (config-if)# switchport mode mac-vlan
   ポート 0/3 を MAC ポートとして設定します。

4. **(config-if)# switchport mac dot1q vlan 10**
   MAC ポートで Tagged フレームを扱う VLAN として，VLAN 10 を設定します。

5. **(config-if)# switchport mac native vlan 50**
   MAC ポートのネイティブ VLAN50（認証前 VLAN）を設定します。（認証後 VLAN は「5.4.3　MAC VLAN の自動 VLAN 割当」により割り当てられます。）

6. **(config-if)# mac-authentication port**
   (config-if)# exit
   ポート 0/3 に認証モード（mac-authentication port）を設定します。

7. **(config)# interface gigabitethernet 0/8**
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 10
   (config-if)# exit
   ポート 0/8 を VLAN10 のアクセスポートとして設定します。認証は除外するので認証モードは設定しません。図内の IP 電話が認証後に通信可能になります。

8. **(config)# interface gigabitethernet 0/9**
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 200
   (config-if)# exit
   ポート 0/9 を VLAN200 のアクセスポートとして設定します。認証は除外するので認証モードは設定しません。図内の端末 PC1 が認証後に通信可能になります。

9. **(config)# interface gigabitethernet 0/10**
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 500
   (config-if)# exit
   ポート 0/10 を VLAN500 のアクセスポートとして設定します。認証は除外するので認証モードは設定しません。図内の RADIUS サーバ用ポートに設定します。

［注意事項］

1. MAC ポートの Tagged フレーム中継については，「コンフィグレーションガイド Vol.1　21.7 MAC VLAN の解説」も参照してください。
2. RADIUS サーバから認証成功（Accept）受信で，RADIUS 属性に認証後 VLAN 情報がないときは，該当 MAC ポートのネイティブ VLAN に端末を収容します。このとき端末は固定 VLAN モードの認証済み端末として扱います。
3. 認証後 VLAN を「5.4.3　MAC VLAN の自動 VLAN 割当」で割り当てるときは，下記を設定してください。
   - コンフィグレーションコマンド vlan mac-based
     RADIUS サーバから通知される VLAN を設定してください。（この場合は，MAC ポートにコンフィグレーションコマンド switchport mac vlan による設定は不要です。）
4. MAC VLAN の自動 VLAN 割当を抑止する場合は，下記を設定してください。
   - コンフィグレーションコマンド no switchport mac auto-vlan
   - コンフィグレーションコマンド switchport mac vlan
     RADIUS サーバから通知される VLAN を設定してください。

5.9　レイヤ 2 認証機能使用時の注意事項

5.9.1　レイヤ 2 認証の共通機能使用時の注意事項

（1） 認証方式リストの設定

ポート別認証方式と Web 認証のユーザ ID 別認証方式設定は，装置内で共存できません。「5.2.2　認証方式リスト （3）認証方式リスト設定のコンフィグレーション排他関係」を参照してご使用ください。

（2） 認証前端末の通信許可

コンフィグレーションコマンド authentication ip access-group を設定する前に，認証対象ポートに下記の認証モード用コンフィグレーションを設定してください。あらかじめ下記コンフィグレーションを設定していないと，authentication ip access-group を設定できません。

- IEEE802.1X：dot1x port-control auto
- Web 認証：web-authentication port
- MAC 認証：mac-authentication port

（3） MAC VLAN の自動 VLAN 割当

RADIUS サーバから通知する認証後 VLAN を，コンフィグレーションコマンド vlan mac-based で本装置に設定してください。また，認証対象ポートには MAC ポートを設定してください。

なお，MAC VLAN の自動 VLAN 割当を抑止する場合は，認証対象ポートに下記コンフィグレーションコマンドを設定してください。

- no switchport mac auto-vlan
- switchport mac vlan （RADIUS サーバから通知する認証後 VLAN を設定）

（4） 同一 MAC ポートでの自動認証モード収容

認証対象端末から Untagged フレームを受信したとき，RADIUS 認証から受信した Access-Accept の RADIUS 属性 Tunnel-Private-Group-ID で取得した VLAN ID で認証モードを決定します。このとき取得した VLAN ID が，当該ポートにコンフィグレーションコマンド switchport mac dot1q vlan で設定されていた場合，不正な VLAN と判定し「認証失敗」扱いとします。

（5） ダイナミック ACL/QoS 機能

（a） 認証許可保留状態の端末について

下記の端末は，認証前の端末と同一の動作となり，フィルタ /QoS 機能によるクラスごとのアクセス制御が適用されず，認証専用 IPv4 アクセスリスト，ARP リレーだけが適用されます。

- マルチステップ認証の 1 段目の認証済み状態
- 認証完了済みで MAC アドレステーブルの登録が未完了状態（認証許可保留状態）

（b） クラス指定の対象

アクセスリスト，および QoS フローリストで指定するクラスパラメータは，フィルタ /QoS の受信側だけが有効となります。

アクセスリスト，および QoS フローリストを使用する機能で，クラス指定の対象を次の表に示します。

表 5-42 クラス指定の対象

機能	方向	アクセスリスト	QoS フローリスト
リモートログイン (ip access-group, ipv6 access-class)	in	IPv4 拡張アクセスリストは設定エラー。 IPv6 アクセスリストは，クラス設定を含むリスト設定は許容するが，クラス動作は無効。（送信元 IPv4/IPv6 アドレス以外の条件はすべて無効。）	コマンドなし。
フィルタ (ip access-group, ipv6 traffic-filter, mac access-group)	in	クラス設定，動作ともに有効。	コマンドなし。
	out	クラス設定を含むリストは設定エラー。	コマンドなし。
QoS (ip qos-flow-list, ipv6 qos-flow-list, mac qos-flow-list)	in	コマンドなし。	クラス設定，動作ともに有効。
認証専用 IPv4 アクセスリスト (authentication ip access-group)	－	クラス設定を含むリスト設定は許容するが，クラス動作は無効。	コマンドなし。
認証対象 MAC アドレスの制限 (mac-authentication access-group)	－	クラス設定を含むリスト設定は許容するが，クラス動作は無効。（送信元 MAC アドレス以外の条件はすべて無効。）	コマンドなし。
SNMP MIB アクセス許可 (snmp-server community)	－	クラス設定を含むリスト設定は許容するが，クラス動作は無効。（送信元 IPv4/IPv6 アドレス以外の条件はすべて無効。）	コマンドなし。

（凡例）
－：該当なし

(c) ユーザ切替オプション

Web 認証のユーザ切替オプションで運用中，クラスが付与された認証済み端末から，別ユーザ名でログインした場合は，下記の動作となります。

- 新ユーザのログインが拒否された場合
  旧ユーザの認証状態を保持します。
- 新ユーザのログインが許可された場合
  旧ユーザのクラス情報ありの認証許可状態を解除し，クラス情報を含め新ユーザの認証許可状態を適用します。
  新ユーザの認証要求に対して，RADIUS サーバから所属クラスが付与されない場合は，class=0 の認証許可端末として本装置に登録します。

(6) ポートリンクダウン時の認証解除抑止について

(a) コンフィグレーションの有効・無効の設定変更による影響

認証済み端末が存在するポートで，コンフィグレーションコマンド no authentication logout linkdown の有効・無効が設定変更された場合でも，認証済み端末情報に影響を与えません。

(b) ポートチャネルインタフェースについて

本機能が有効の場合でも，下記のようにポートチャネルインタフェースに関わるコンフィグレーションが変更されると，認証状態を解除します。

- 認証済み端末が物理ポートに所属している状態
  コンフィグレーションの変更により，当該物理ポートをポートチャネルインタフェースに収容され

た場合は，認証状態を解除します。
- 認証済み端末がポートチャネルインタフェースに所属している状態
  コンフィグレーションの変更により，当該ポートチャネルインタフェースが削除された場合，認証状態を解除します。

5.9.2 レイヤ 2 認証機能同士の共存

(1) 同一端末で複数の認証機能の使用について

1 台の端末を使用して IEEE802.1X，Web 認証および MAC 認証を実施した場合，最初に許可された認証機能が優先されます。

MAC 認証は認証対象端末から送信されるフレームが認証契機となるので，通常は MAC 認証が最初に動作しますが，RADIUS サーバに MAC 認証用の許可情報が登録されていない，または内蔵 MAC 認証 DB と照合できない場合は，MAC 認証は保留状態（猶予タイマ "mac-authentication timeout quiet-period" の間）となり，この間に IEEE802.1X か Web 認証が行われるのを待ちます。

この間に IEEE802.1X か Web 認証が許可されれば，最初に許可された認証機能が有効となり，以降に認証状態が解除されるまで，他の認証機能は上書きできません。

このとき，上書きに失敗した他の認証機能のアカウントログには認証失敗が記録されます。

なお，MAC 認証の保留状態時間内に，IEEE802.1X か Web 認証が完了しない場合，MAC 認証のアカウントログに失敗ログが記録されます。

(2) 複数の認証機能を共存時に最大収容数を超えた場合

複数の認証機能を共存した際に最大収容数を超えた場合，処理中の認証機能のアカウントログ情報には認証失敗と記録されます。

5.9.3 レイヤ 2 認証機能と他機能の共存

レイヤ 2 認証機能と他機能の共存について，次の表に示します。

表 5-43 レイヤ 2 認証機能と他機能の共存仕様

レイヤ 2 認証機能	機能名		共存仕様
IEEE802.1X	スタック		「コンフィグレーションガイド Vol.1 7. スタックの解説【OP-WLE】」を参照してください。
	リンクアグリゲーション		端末認証モードで，スタティック／LACP リンクアグリゲーションのチャネルグループと同時に使用できます。
	MAC アドレス学習の抑止		装置内で共存できますが，同一 VLAN は使用できません。
	VLAN	ポート VLAN	ポート単位認証 (静的) で使用できます。
		プロトコル VLAN	装置で同時に使用できません。
		MAC VLAN	ポート単位認証 (静的) ／ポート単位認証 (動的) で使用できます。
	デフォルト VLAN		ポート単位認証 (静的) で使用できます。 ポート単位認証 (動的) では認証前 VLAN に使用できます。
	VLAN 拡張機能	VLAN トンネリング	装置で同時に使用できません。
		EAPOL フォワーディング	装置で同時に使用できません。

レイヤ 2 認証機能	機能名		共存仕様
	スパニングツリー		IEEE802.1X 認証ポートではスパニングツリーを使用できません。
	Ring Protocol		IEEE802.1X 認証ポートでは Ring Protocol を使用できません。
	IGMP snooping		一部制限があります。※1
	MLD snooping		一部制限があります。※1
	DHCP snooping		同時に使用できます。※2
	ホワイトリスト機能		「14.1.5　他機能との共存」を参照してください。
	L2 ループ検知		同時に使用できます。
	GSRP aware		IEEE802.1X 認証ポートでは GSRP aware を使用できません。
	アップリンク・リダンダント		アップリンクポートで使用できません。
	CFM		「21.1.9　CFM 使用時の注意事項」を参照してください。
	IEEE802.3ah/UDLD		IEEE802.1X 認証ポートでは UDLD を使用できません。
	LLDP		IEEE802.1X 認証ポートでは LLDP を使用できません。
Web 認証	スタック		「コンフィグレーションガイド Vol.1　7. スタックの解説【OP-WLE】」を参照してください。
	リンクアグリゲーション		スタティック／ LACP リンクアグリゲーションのチャネルグループと同時に使用できます。
	MAC アドレス学習の抑止		装置内で共存できますが，同一 VLAN は使用できません。
	VLAN	ポート VLAN	固定 VLAN モードで使用できます。
		プロトコル VLAN	装置で同時に使用できません。
		MAC VLAN	固定 VLAN モード／ダイナミック VLAN モードで使用できます。
	デフォルト VLAN		固定 VLAN モードで使用できます。 ダイナミック VLAN モードでは認証前 VLAN に使用できます。
	VLAN 拡張機能	VLAN トンネリング	装置で同時に使用できません。
		EAPOL フォワーディング	共存できます。
	スパニングツリー		Web 認証ポートではスパニングツリーを使用できません。
	Ring Protocol		Web 認証ポートでは Ring Protocol を使用できません。
	IGMP snooping		一部制限があります。※1
	MLD snooping		一部制限があります。※1
	DHCP snooping		同時に使用できます。※2
	ホワイトリスト機能		「14.1.5　他機能との共存」を参照してください。
	L2 ループ検知		同時に使用できます。
	GSRP aware		Web 認証ポートでは GSRP aware を使用できません。
	アップリンク・リダンダント		アップリンクポートで使用できません。
	CFM		「21.1.9　CFM 使用時の注意事項」を参照してください。
	IEEE802.3ah/UDLD		Web 認証を設定したポートでは使用しないでください。
	ログ出力機能		「23.1.3　ログ出力機能使用時の注意事項」を参照してください。
	LLDP		Web 認証ポートでは LLDP を使用できません。

レイヤ 2 認証機能	機能名		共存仕様
MAC 認証	スタック		「コンフィグレーションガイド Vol.1　7. スタックの解説【OP-WLE】」を参照してください。
	リンクアグリゲーション		スタティック／LACP リンクアグリゲーションのチャネルグループと同時に使用できます。
	MAC アドレス学習の抑止		装置内で共存できますが，同一 VLAN は使用できません。
	VLAN	ポート VLAN	固定 VLAN モードで使用できます。
		プロトコル VLAN	装置で同時に使用できません。
		MAC VLAN	固定 VLAN モード／ダイナミック VLAN モードで使用できます。
	デフォルト VLAN		固定 VLAN モードで使用できます。 ダイナミック VLAN モードでは認証前 VLAN に使用できます。
	VLAN 拡張機能	VLAN トンネリング	装置で同時に使用できません。
		EAPOL フォワーディング	共存できます。
	スパニングツリー		MAC 認証ポートではスパニングツリーを使用できません。
	Ring Protocol		MAC 認証ポートでは Ring Protocol を使用できません。
	IGMP snooping		一部制限があります。※1
	MLD snooping		一部制限があります。※1
	DHCP snooping		同時に使用できます。※2
	ホワイトリスト機能		「14.1.5　他機能との共存」を参照してください。
	L2 ループ検知		同時に使用できます。
	GSRP aware		MAC 認証ポートでは GSRP aware を使用できません。
	アップリンク・リダンダント		アップリンクポートで使用できません。
	CFM		「21.1.9　CFM 使用時の注意事項」を参照してください。
	IEEE802.3ah/UDLD		MAC 認証を設定したポートでは使用しないでください。
	LLDP		MAC 認証ポートでは LLDP を使用できません。

注 ※1

認証ポートでは，IGMP/MLD snooping を使用できません。
認証ポートに設定されている VLAN，および MAC VLAN の自動割当機能で使用する VLAN には，IGMP/MLD snooping を設定しないでください。

注 ※2

レイヤ 2 認証機能と DHCP snooping を併用した場合，通信可能な最大端末数は DHCP snooping の管理端末数（最大 500 台）となります。

5.9.4　認証解除の注意事項

clear コマンドや認証ポートのリンクダウンなどによって多数の端末の認証を一度に解除するとき，本装置に対する ping などへの応答が秒単位で遅延する場合があります。

特にコンフィグレーション変更（no mac-authentication port など）によって多数の端末の認証を解除する場合は，LACP(short) のタイムアウトが発生する可能性があるため，事前に clear コマンドで認証を解除してから実行してください。

6 IEEE802.1X の解説

IEEE802.1X は OSI 階層モデルの第 2 レイヤで認証を行う機能です。この章では IEEE802.1X の概要について説明します。

6.1 IEEE802.1X の概要

IEEE802.1X は，不正な LAN 接続を規制する機能です。バックエンドに認証サーバ（一般的には RADIUS サーバ）を設置し，認証サーバによる端末の認証が通過した上で，本装置の提供するサービスを利用できるようにします。

IEEE802.1X の構成要素と動作概略を次の表に示します。

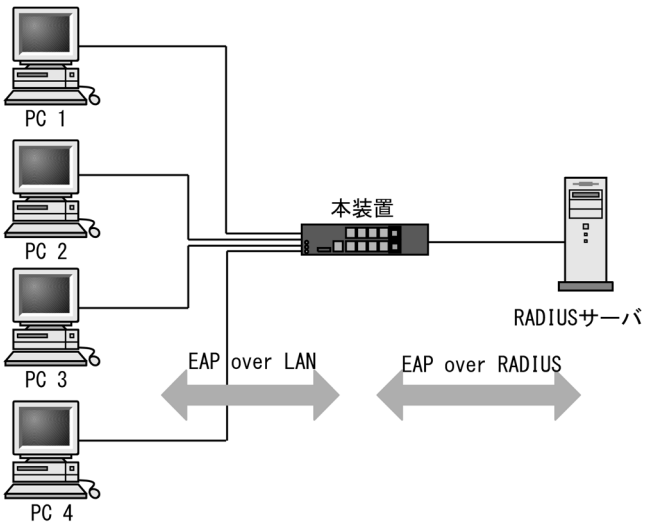
表 6-1 構成要素と動作概略

構成要素	動作概略
本装置（Authenticator）	端末の LAN へのアクセスを制御します。また，端末と認証サーバ間で認証情報のリレーを行います。端末と本装置間の認証処理にかかわる通信は EAP Over LAN(EAPOL) で行います。本装置と認証サーバ間は EAP Over RADIUS を使って認証情報を交換します。なお，本章では，「本装置」または「Authenticator」と表記されている場合，本装置自身と本装置に搭載されている Authenticator ソフトウェアの両方を意味します。
端末（Supplicant）	EAPOL を使用して端末の認証情報を本装置とやりとりします。なお，本章では，「端末」または「Supplicant」と表記されている場合，端末自身と端末に搭載されている Supplicant ソフトウェアの両方を意味します。「Supplicant ソフトウェア」と表記されている場合，Supplicant 機能を持つソフトウェアだけを意味します。
認証サーバ（Authentication Server）	端末の認証を行います。認証サーバは端末の認証情報を確認し，本装置の提供するサービスへのアクセスを要求元の端末に許可すべきかどうかを本装置に通知します。

標準的な IEEE802.1X の構成では，本装置のポートに直接端末を接続して運用します。

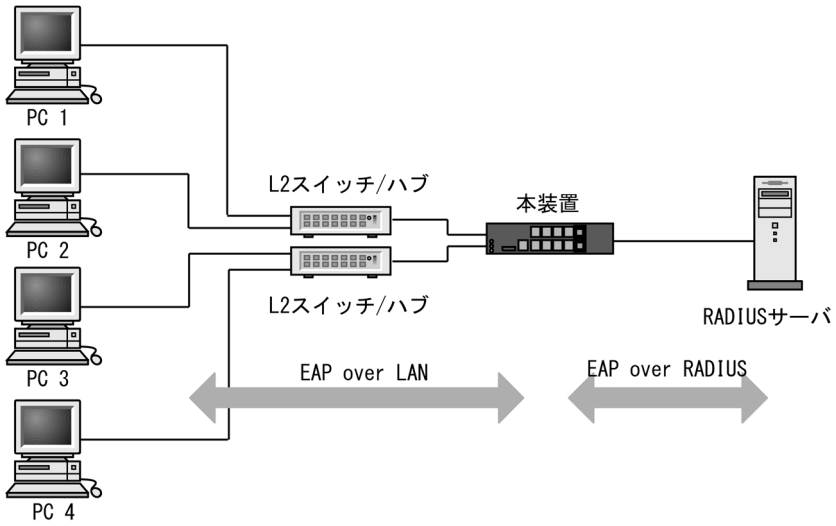
本装置を使った IEEE802.1X 基本構成を次の図に示します。

図 6-1 IEEE802.1X 基本構成



また，本装置では一つのポートで複数の端末の認証を行う拡張機能をサポートしています（端末認証モード）。本拡張機能を使用した場合，端末と本装置間に L2 スイッチやハブを配置することで，ポート数によって端末数が制限を受けない構成にできます。本構成を行う場合，端末と本装置間に配置する L2 スイッチは EAPOL を透過する必要があります。その場合の構成を次の図に示します。

図 6-2 端末との間に L2 スイッチを配置した IEEE802.1X 構成



6.1.1 基本機能

本装置でサポートする IEEE802.1X の基本機能を以下に示します。

(1) 本装置の認証動作モード

本装置でサポートする認証動作モード（PAE モード）は Authenticator です。本装置が Supplicant として動作することはありません。

(2) 認証方式グループ

本装置は RADIUS サーバで認証します。端末から受信した EAPOL フレームを EAPoverRADIUS に変換し，認証処理は RADIUS サーバで行います。RADIUS サーバは EAP 対応されている必要があります。

本装置の IEEE802.1X では，次に示す認証方式グループを設定できます。（設定した認証方式グループは，IEEE802.1X の全認証モードで使用できます。）

- 装置デフォルト：RADIUS 認証方式
  ネットワーク内に設置した RADIUS サーバを用いて認証する方式です。
- 認証方式リスト
  特定条件に合致した際に，認証方式リストに登録した任意の RADIUS サーバグループを用いて認証する方式です。

下記も合わせて参照してください。

- 「5.1.3 認証方式グループ」
- 「5.2.2 認証方式リスト」
- 「5.3.1 レイヤ 2 認証機能で使用する RADIUS サーバ情報」
- 「7.2.1 認証方式グループと RADIUS サーバ情報の設定」

(3) 認証アルゴリズム

本装置でサポートする認証アルゴリズムを次の表に示します。

表 6-2 サポートする認証アルゴリズム

認証アルゴリズム	概要
EAP-MD5-Challenge	UserPassword とチャレンジ値の比較を行う。
EAP-TLS	証明書発行機構を使用した認証方式。
EAP-PEAP	EAP-TLS トンネル上で，ほかの EAP 認証アルゴリズムを用いて認証する。 2 種類の認証方式に対応 (1)PEAP-MS-CHAP V2：パスワードベースの資格情報を使用した認証方式 (2)PEAP-TLS　　：証明書発行機構を使用した認証方式
EAP-TTLS	EAP-TLS トンネル上で，他方式 (EAP，PAP，CHAP など) の認証アルゴリズムを用いて認証する。

6.1.2 拡張機能の概要

本装置では，標準的な IEEE802.1X に対して機能拡張を行っています。拡張機能の概要を以下に示します。

(1) 認証モード

本装置の IEEE802.1X では，二つの基本認証モードとその下に認証サブモードを設けています。基本認証モードは，認証制御を行う単位を示し，認証サブモードは認証単位内の端末接続モードを指定します。

本装置の基本認証モード（以降は，認証モードと表記）は下記をサポートしています。

- ポート単位認証（静的）
  認証が成功した端末の MAC アドレスを MAC アドレステーブルに登録し，コンフィグレーションで指定された VLAN への通信を可能とします。
- ポート単位認証（動的）
  認証が成功した端末の MAC アドレスを，MAC VLAN と MAC アドレステーブルに登録して，認証前のネットワークと認証後のネットワークを分離します。

(2) 各認証モードのサポート機能

各認証モードのサポート機能を下記に示します。

表 6-3 各認証モードのサポート機能一覧

機能		ポート単位認証（静的）	ポート単位認証（動的）
装置デフォルト： ローカル認証		×	×
装置デフォルト： RADIUS 認証	外部サーバ • IEEE802.1X 認証専用 RADIUS サーバ情報 • 汎用 RADIUS サーバ情報	○ 「5.3.1」参照 「6.6」参照 「7.2.1」参照	○ 「5.3.1」参照 「6.6」参照 「7.2.1」参照
	VLAN（認証後の VLAN）	×	○
	検疫によるアクセス制限 （RADIUS 属性の Filter-Id 使用）	○ 「6.2.3」参照	×

機能		ポート単位認証（静的）	ポート単位認証（動的）
	強制認証	○ 「5.4.6」参照	○ 「5.4.6」参照
	認証許可ポート設定	○ 「5.5.4」参照	○ 「5.5.4」参照
	プライベートトラップ	○ 「5.4.6」参照	○ 「5.4.6」参照
認証方式リスト	外部サーバ • RADIUS サーバグループ	○ 「5.3.1」参照 「6.6」参照 「7.2.1」参照	○ 「5.3.1」参照 「6.6」参照 「7.2.1」参照
	ポート別認証方式	○ 「5.2.2」参照 「5.2.3」参照	○ 「5.2.2」参照 「5.2.3」参照
認証サブモード	シングルモード	○ 「6.2.1」参照	○ 「6.3.1」参照
	端末認証モード	○ 「6.2.1」参照	○ 「6.3.1」参照
認証モードオプション	認証除外端末オプション	○ 「6.2.1」参照 「7.3.2」参照	○ 「6.3.1」参照 「7.4.2」参照
	認証デフォルト VLAN	×	×
認証数制限	ポート単位	1024 「5.4.8」参照 「5.5.5」参照	1000 「5.4.8」参照 「5.5.5」参照
	装置単位	1024 「5.4.8」参照 「5.5.5」参照	1000 「5.4.8」参照 「5.5.5」参照
認証	端末検出動作切り替え	○ 「6.2.2」参照	○ 「6.3.2」参照
	マルチキャストで EAP- Request フレーム送信	○ 「7.3.2」参照	○ 「7.4.2」参照
	ユニキャストで EAP- Request フレーム送信	○ 「7.3.2」参照	○ 「7.4.2」参照
	EAP-Request フレーム送信停止	○ 「7.3.2」参照	○ 「7.4.2」参照
	端末へ EAP-Request/Identity フレーム送信	○ 「6.2.2」参照 「7.3.3」参照	○ 「6.3.2」参照 「7.4.3」参照
	端末へ EAP-Request フレーム再送	○ 「6.2.2」参照 「7.3.3」参照	○ 「6.3.2」参照 「7.4.3」参照
	端末からの再認証要求の抑止	○ 「6.2.2」参照 「7.3.3」参照	○ 「6.3.2」参照 「7.4.3」参照
	複数端末からの認証要求時の通信遮断状態保持時間	○ ※1 「6.2.1」参照 「7.3.3」参照	○ ※1 「6.3.1」参照 「7.4.3」参照

機能		ポート単位認証 （静的）	ポート単位認証 （動的）
	認証失敗時の認証再開までの待機時間	○ 「6.2.2」参照 「7.3.3」参照	○ 「6.3.2」参照 「7.4.3」参照
	認証サーバ応答待ち時間	○ 「6.2.2」参照 「7.3.3」参照	○ 「6.3.2」参照 「7.4.3」参照
	認証前通過（認証専用 IPv4 アクセスリスト）	○ 「5.4.1」参照 「5.5.2」参照	○ 「5.4.1」参照 「5.5.2」参照
認証解除	再認証要求時の無応答端末の認証解除	○ 「6.2.2」参照 「7.3.3」参照	○ 「6.3.2」参照 「7.4.3」参照
	認証済み端末の無通信監視	○※2 「6.2.2」参照 「7.3.3」参照	○ 「6.3.2」参照 「7.4.3」参照
	MAC アドレステーブルエージング監視	○※3 「6.2.2」参照 「7.3.3」参照	×※4
	認証端末接続ポートのリンクダウン	○ 「6.2.2」参照	○ 「6.3.2」参照
	VLAN 設定変更	○ 「6.2.2」参照	○ 「6.3.2」参照
	運用コマンド	○ 「6.2.2」参照	○ 「6.3.2」参照
EAPOL フォワーディング		全モード共通　「6.4」参照	
アカウントログ	本装置内蔵アカウントログ	「6.5」参照	
	RADIUS サーバのアカウント機能	全モード共通 「5.3.4」参照 「6.5」参照 「7.2.2」参照	

（凡例）

○：サポート

×：未サポート

「5.x.x」参照：「5　レイヤ 2 認証機能の概説」の参照先番号

「6.x.x」参照：本章の参照先番号

「7.x.x」参照：「7　IEEE802.1X の設定と運用」の参照先番号

注 ※1

本機能は，シングルモードのポートにだけ適用します。

注 ※2

フルアクセス許可（認証および検疫済み状態）の端末が対象です。

注 ※3

制限付アクセス許可（検疫状態）の端末が対象です。

注 ※4

マルチステップ認証で 1 段目の端末認証を IEEE802.1X で認証成功したときは，MAC アドレステーブルエージング監視で認証エントリを監視します。詳細は「12　マルチステップ認証」を参照してください。

表 6-4 IEEE802.1X の動作条件

種別		ポートの設定	設定可能な VLAN 種別	フレーム種別	ポート単位認証（静的）	ポート単位認証（動的）
ポートの種類	アクセスポート	native	ポート VLAN MAC VLAN	Untagged	○	×
	トランクポート	native	ポート VLAN MAC VLAN	Untagged	○	×
		allowed	ポート VLAN MAC VLAN	Tagged	○	×
	プロトコルポート	－	－	－	×	×
	MAC ポート	native	ポート VLAN	Untagged	○※	×
		mac	MAC VLAN	Untagged	×	○
		dot1q	ポート VLAN MAC VLAN	Tagged	○	×
デフォルト VLAN					○	×
インタフェース種別	gigabitethernet				○	○
	port channel				○	○

（凡例）
○：動作可
×：動作不可
－：認証ポートでは，設定対象外

注 ※
詳細は「5.4.4 同一 MAC ポートでの自動認証モード収容」を参照してください。

本装置の IEEE802.1X では，チャネルグループについても一つの束ねられたポートとして扱います。この機能での「ポート」の表現には通常のポートとチャネルグループを含むものとします。

次項からは，「ポート単位認証（静的）」「ポート単位認証（動的）」の順に各認証モードの概要を説明します。各認証モードで同じ機能，同一動作については，「～を参照してください。」としていますので，該当箇所を参照してください。

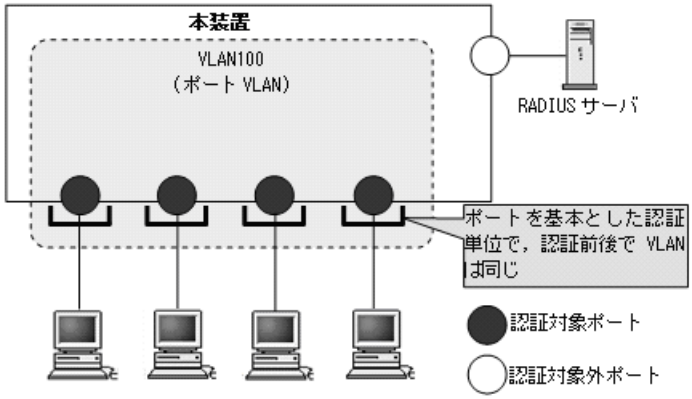
6.2 ポート単位認証（静的）

認証の制御を物理ポートまたはチャネルグループに対して行います。IEEE802.1X の標準的な認証単位です。この認証モードでは，IEEE802.1Q VLAN Tag の付与された EAPOL フレームを下記のように扱います。

- アクセスポート
  IEEE802.1Q VLAN Tag の付与された EAPOL フレームを扱うことはできません。IEEE802.1Q VLAN Tag の付与された EAPOL フレームを受信すると廃棄します。
- トランクポートまたは MAC ポートの switchport mac dot1q vlan
  IEEE802.1Q VLAN Tag の付与された EAPOL フレームを扱うことができます。

ポート単位認証（静的）の構成例を次の図に示します。

図 6-3 ポート単位認証（静的）の構成例



認証前の端末は，認証が成功するまで通信できません。ポート単位認証（静的）で認証が成功すると，認証が成功した端末の MAC アドレスと VLAN ID を MAC アドレステーブルに IEEE802.1X ポート単位認証エントリとして登録して通信可能になります。（MAC アドレステーブルの登録状態は，運用コマンド show mac-address-table で確認できます。）

6.2.1 認証サブモードと認証モードオプション

本装置の IEEE802.1X では，認証モードとその下に認証サブモードを設けています。認証モードは，認証制御を行う単位を示し，認証サブモードは認証単位内の端末接続モードを指定します。また，各モードで設定可能な認証モードオプションがあります。

認証モードとサブモード，および認証モードオプションの関係を次の表に示します。

表 6-5 認証サブモードと認証モードオプションの関係

認証モード	認証サブモード	認証モードオプション
ポート単位認証（静的）	シングルモード	－
	端末認証モード	認証除外端末オプション

（1） 認証サブモード

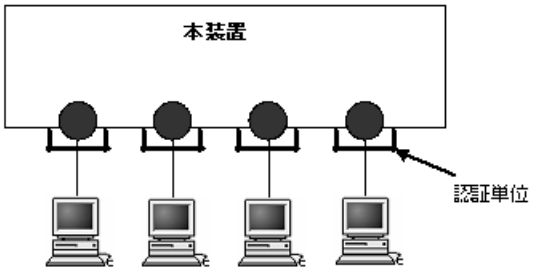
ポート単位認証（静的）の認証サブモードは，シングルモードと端末認証モードがあります。デフォルト

コンフィグレーションはシングルモードで動作し，コンフィグレーションコマンド dot1x multiple-authentication を設定すると，端末認証モードで動作します。

(a) シングルモード

一つの認証単位内に一つの端末だけ認証して接続するモードです。IEEE802.1X の標準的な認証モードです。最初の端末が認証している状態でほかの端末からの EAP を受信すると，そのポートの認証状態は未認証状態に戻り，コンフィグレーションコマンド dot1x timeout keep-unauth で指定された時間が経過したあとに認証処理を再開します。

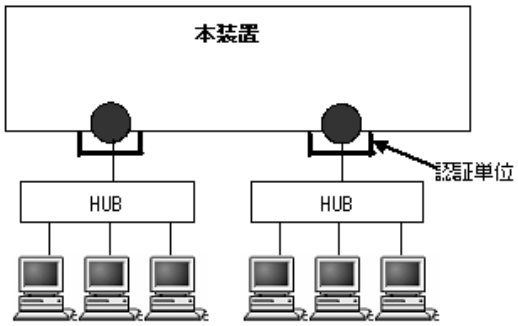
図 6-4 シングルモードの構成



(b) 端末認証モード

一つの認証単位内に複数端末の接続を許容し，端末ごと（送信元 MAC アドレスで識別）に認証を行うモードです。端末が認証されている状態でほかの端末の EAP を受信すると，EAP を送信した端末との間で個別の認証処理を開始します。

図 6-5 端末認証モードの構成



(2) 認証モードオプション

(a) 認証除外端末オプション

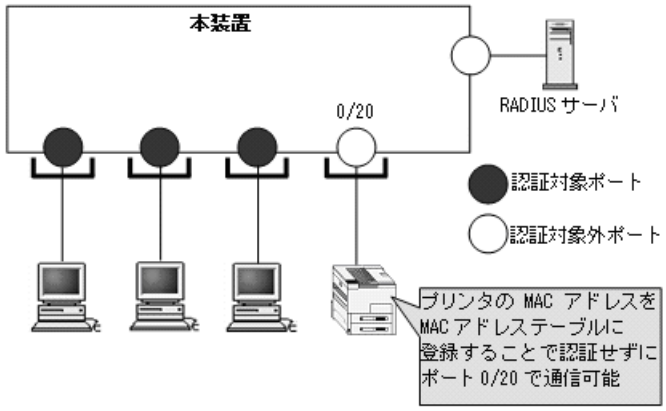
スタティック MAC アドレス学習機能※によって MAC アドレスが設定された端末については認証を不要とし，通信を許可するオプション設定です。Supplicant 機能を持たないプリンタなどの装置やサーバなど認証が不要な端末を，端末単位で認証対象から除外したいときに使用します。端末認証モードの場合だけ使用可能なオプションです。

注※

コンフィグレーションコマンド mac-address-table static で，MAC アドレステーブルに MAC アドレスを設定

ポート単位認証（静的）での認証除外端末構成例を次の図に示します。

図 6-6 ポート単位認証（静的）での認証除外端末構成例



6.2.2 認証機能

（1） 認証契機

ポート単位認証（静的）の対象ポートに接続されている端末から，EAPOL-Start を受信したときに認証契機となります。

（2） EAP-Request/Identity フレーム送信

自発的に認証を開始しない端末に対して，認証開始を誘発するために本装置から定期的に EAP-Request/Identity を送信する時間間隔を，コンフィグレーションコマンド dot1x timeout tx-period で設定できます。

（3） 端末検出動作切り替えオプション

本装置では認証済み端末が存在しない場合，認証前端末を検出するためにコンフィグレーションコマンド dot1x timeout tx-period で指定した間隔で EAP-Request/Identity をマルチキャスト送信します。認証サブモードが端末認証モードの場合，認証済み端末と認証前端末が混在するため，認証済み端末が存在する場合でも端末検出が必要です。しかし，EAP-Request/Identity をマルチキャスト送信すると認証済み端末も受信するため，認証済み端末の再認証が発生するなどの問題があります。

本装置では，端末認証モードの場合だけ，認証済み端末が存在する場合の端末検出動作を 4 方式から選択できます。各方式の特徴をご理解の上，適切な方式を選択してください。なお，端末検出動作の方式はコンフィグレーションコマンド dot1x supplicant-detection で指定できます。指定しない場合は shortcut で動作します。

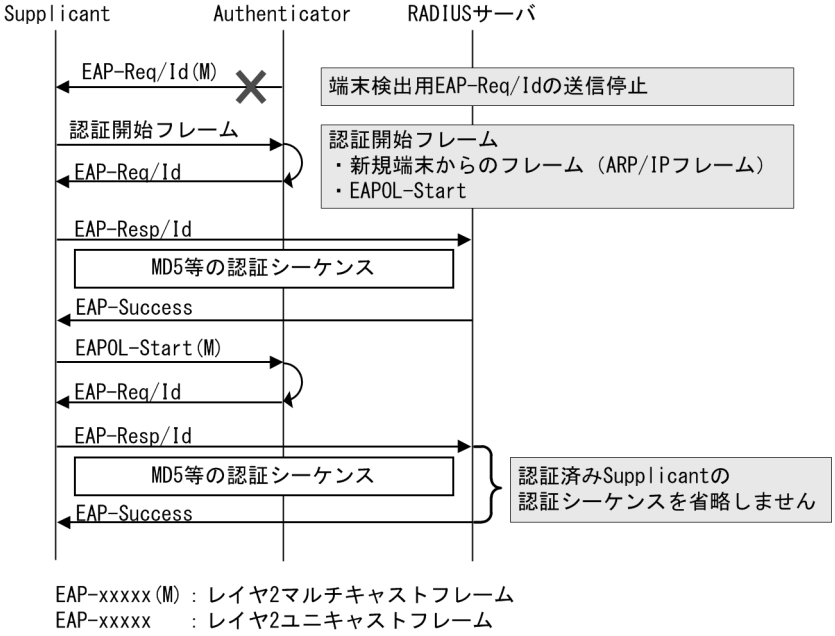
以下に各方式を説明します。

（a） auto

認証済み端末が存在する場合は，EAP-Request/Identity をマルチキャスト送信しません。その代わり，認証前端末が送信した ARP/IP フレームを受信することで認証前端末を検出し，認証を開始します。認証済み端末に EAP-Request/Identity が到達しないので認証済み端末の再認証による負荷はありません。検出にも負荷にも問題がないため、本方式での運用をお勧めします。

auto 指定時の EAP-Request/Identity のシーケンスを次の図に示します。

図 6-7 auto の EAP-Request/Identity のシーケンス



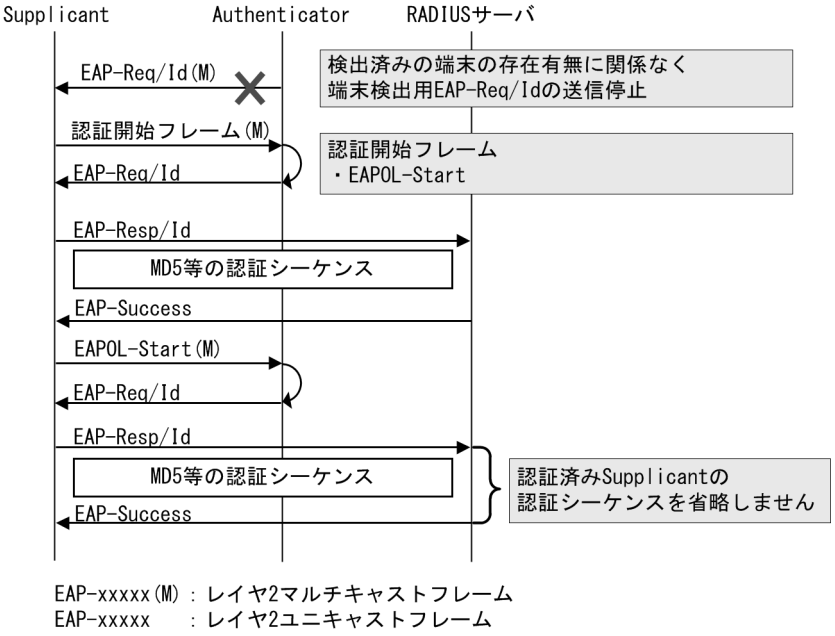
(b) passive

当該ポートの検出済み端末の存在有無に関係なく，本装置から EAP-Request/Identity をマルチキャスト送信しません。本装置からの EAP-Request/Identity マルチキャスト送信を完全停止する場合は，disable ではなく，passive を指定してください。認証前端末が送信した EAPOL-Start を受信することで認証を開始します。

このため，自発的に EAPOL-Start を送信しない Supplicant ソフトウェアを使用すると，認証前端末を検出できません。この方式では，認証済み端末に EAP-Request/Identity が到達しないため，認証済み端末の再認証による負荷はありません。

passive 指定時の EAP-Request/Identity のシーケンスを次の図に示します。

図 6-8 passive の EAP-Request/Identity のシーケンス



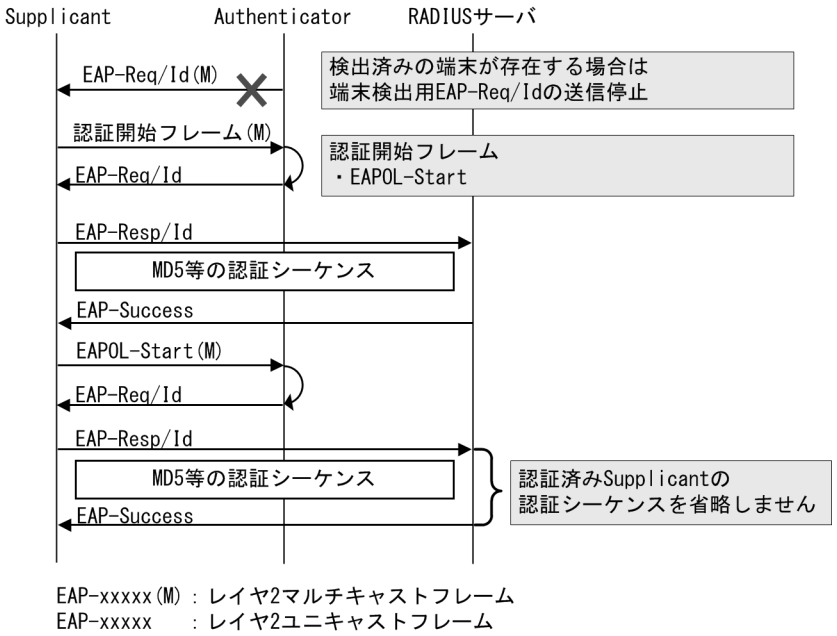
（c） disable

当該ポートで検出済みの端末が存在する場合は，EAP-Request/Identity をマルチキャスト送信しません。認証前端末が EAPOL-Start を送信することで認証を開始します。

このため，自発的に EAPOL-Start を送信しない Supplicant ソフトウェアを使用する場合，認証前端末を検出できません。このような場合には Supplicant に EAPOL-Start を送信するよう設定するか，本装置の端末検出動作に auto を指定してください。この方式では，認証済み端末に EAP-Request/Identity が到達しないため，認証済み端末の再認証による負荷はありません。

disable 指定時の EAP-Request/Identity のシーケンスを次の図に示します。

図 6-9 disable の EAP-Request/Identity のシーケンス



（d） shortcut

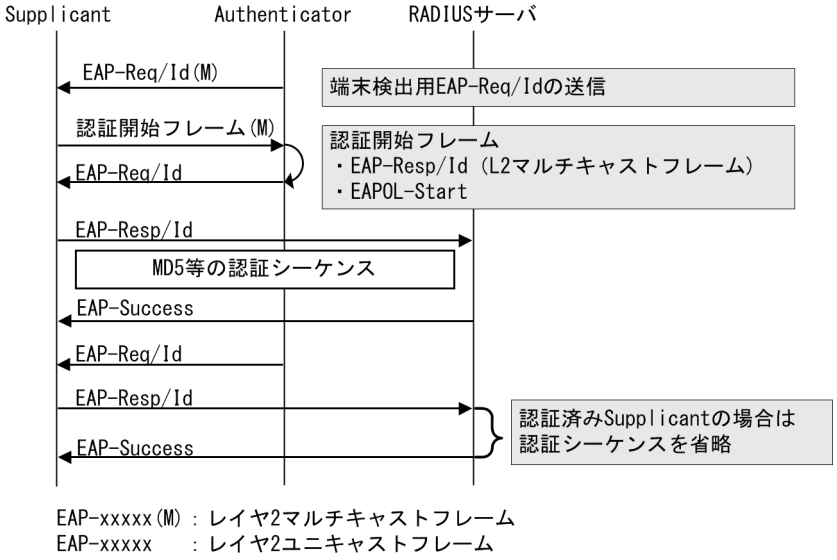
認証済み端末が存在する場合も，EAP-Request/Identity をマルチキャスト送信します。認証前端末がこのフレームを受信し応答することで認証を開始します。

認証済み端末もこのフレームを受信することで再認証を開始します。shortcut では認証済み端末が再認証を開始した場合に認証シーケンスを省略して EAP-Success を即時返すことで負荷を軽減します。

しかし，一部の Supplicant ソフトウェアでは，EAP-Success を即時返す動作を認証失敗とみなします。この結果，認証後すぐに通信が途切れたり，認証後数分から数十分で通信が途切れたり，再認証を繰り返して負荷が上がったりする場合があります。

shortcut 指定時の EAP-Request/Identity のシーケンスを次の図に示します。

図 6-10 shortcut の EAP-Request/Identity のシーケンス



(4) 端末への EAP-Request フレーム再送

端末の認証中に，本装置から送信する EAP-Request（認証サーバからの要求メッセージ）に対して，端末から応答がない場合の再送時間と再送回数を設定します。

再送時間はコンフィグレーションコマンド dot1x timeout supp-timeout，再送回数はコンフィグレーションコマンド dot1x max-req で設定できます。

(5) 端末からの認証要求に対する抑止機能

(a) 端末からの再認証要求の抑止

端末から送信される EAPOL-Start を契機とする認証処理を抑止する機能です。多数の端末から短い間隔で再認証要求を受信したときに，EAP-Request/Identity を送信しないようにすることで，認証処理による本装置の負荷の上昇を防ぎます。

端末からの再認証要求の抑止は，コンフィグレーションコマンド dot1x reauthentication とコンフィグレーションコマンド dot1x ignore-eapol-start で設定できます。

なお，本機能の設定後は，下記のコンフィグレーションで指定した間隔で定期的に本装置から EAP-Request/Identity を送信することで端末の再認証を行います。

- コンフィグレーションコマンド dot1x timeout tx-period
- コンフィグレーションコマンド dot1x timeout reauth-period

(b) 複数端末からの認証要求時の通信遮断

ポート単位認証のシングルモードが動作しているポートで，複数の端末からの認証要求を検出した場合に，該当ポートの通信を遮断する時間をコンフィグレーションで設定できます。

通信遮断時間はコンフィグレーションコマンド dot1x timeout keep-unauth で設定できます。

(6) 認証失敗時の認証再開までの待機時間

認証に失敗した端末に対する認証再開までの待機時間を，コンフィグレーションコマンド dot1x timeout quiet-period で設定できます。

（7） 認証サーバ応答待ち時間

認証サーバへの要求に対する応答がない場合の待ち時間を，コンフィグレーションコマンド dot1x timeout server-timeout で設定できます。設定した時間が経過すると，Supplicant へ認証失敗を通知します。コンフィグレーションコマンド radius-server で設定している再送を含めた総時間と比較して，短い方の時間で Supplicant へ認証失敗を通知します。

（8） 強制認証ポート指定

強制認証については，「5.4.6　認証共通の強制認証」を参照してください。

また，強制認証で認証許可した端末は，通常の認証済み端末と同様に後述の「6.2.2　認証機能　（10）認証解除」により認証状態が解除されます。

強制認証した端末から送信される EAPOL フレームは，次の再認証時間になるまですべて廃棄します。

（9） 認証数制限

装置単位およびポート単位に認証数の制限が設定できます。詳細は，「5.4.8　認証共通の端末数制限」を参照してください。

（10）認証解除

ポート単位認証（静的）では，認証解除の手段として下記があります。

- 再認証要求時の無応答端末の認証解除
- 認証済み端末の無通信監視による認証解除
- 検疫状態端末の MAC アドレステーブルエージング監視による認証解除
- 認証端末接続ポートのリンクダウンによる認証解除
- VLAN 設定変更による認証解除
- 運用コマンドによる認証解除

（a） 再認証要求時の無応答端末の認証解除

認証後にネットワークから外れた端末は本装置から認証を解除できないため，認証済みの端末に対して再認証を促し，応答のない端末の認証を解除します。

該当ポートに，再認証を促すコンフィグレーションコマンド dot1x reauthentication と，再認証の時間間隔をコンフィグレーションコマンド dot1x timeout reauth-period を設定します。

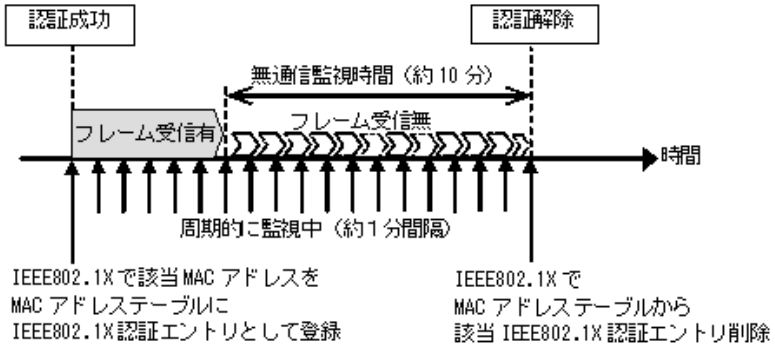
（b） 認証済み端末の無通信監視による認証解除

検疫および認証済み状態の端末が対象となります。

本機能は，認証済み端末が一定時間無通信だった場合に自動的に認証を解除します。

MAC アドレステーブルの IEEE802.1X 認証エントリを周期的（約 1 分間隔）に監視し，IEEE802.1X で登録した認証済み端末からのフレーム受信有無を確認します。該当端末からのフレーム受信を一定時間（約 10 分）検出しなかったときに，MAC アドレステーブルから該当 IEEE802.1X 認証エントリを削除し，認証を解除します。

図 6-11 認証済み端末の無通信監視概要



認証済み端末の無通信監視は，下記の条件で動作が有効となります。

• IEEE802.1X ポート単位認証（静的）またはポート単位認証（動的）有効で，dot1x auto-logout 有効

コンフィグレーションコマンドで no dot1x auto-logout を設定すると，自動で認証を解除しません。

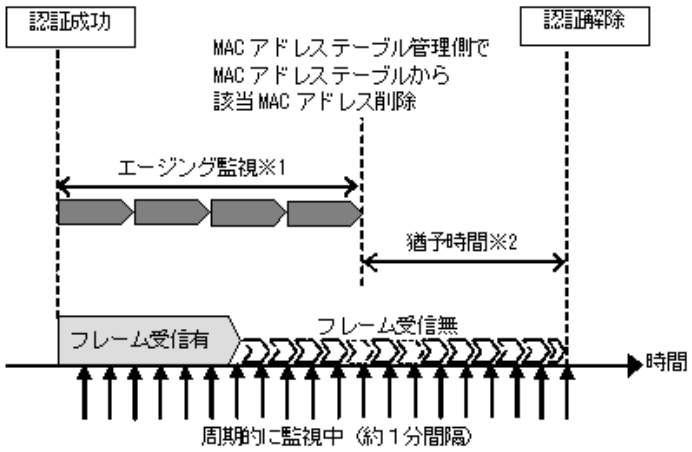
(c) 検疫状態端末の MAC アドレステーブルエージング監視による認証解除

ポート単位認証（静的）で認証したときは，検疫状態で登録されている端末が対象となります。（検疫状態については，後述の「6.2.3 NAP 検疫システムとの連携について」を参照してください。）

本機能は MAC アドレステーブルのダイナミックエントリを周期的（約 1 分間隔）に監視し，該当する端末の MAC アドレスがエージングされているか確認します。そのため，該当する端末の MAC アドレスがエージングタイムアウトにより MAC アドレステーブルから削除されている場合は，自動的に端末の検疫状態を解除します。

ただし，回線の瞬断などの影響で解除されてしまうことを防ぐために，MAC アドレステーブルから MAC アドレスが削除されてから約 10 分間（解除までの猶予時間）で，該当する端末の MAC アドレスが，MAC アドレステーブルに登録されていない場合に，検疫状態を解除します。

図 6-12 MAC アドレステーブルエージング監視による解除概要



※1 エージング監視：mac-address-table aging-time で設定した間隔で監視

※2 猶予時間：約１０分（コンフィグレーション変更不可）

MAC アドレステーブルエージング監視は，下記の条件で動作が有効となります。

- IEEE802.1X　ポート単位認証（静的）有効で，dot1x auto-logout 有効
- 該当端末が検疫状態

コンフィグレーションコマンドで no dot1x auto-logout を設定すると，エージングタイムアウト時でも自動で認証を解除しません。

(d) 認証端末接続ポートのリンクダウンによる認証解除

認証済み端末の接続ポートでリンクダウンを検出した際に，当該ポートの IEEE802.1X 認証端末を自動的に認証解除します。

なお，当該ポートにコンフィグレーションコマンド no authentication logout linkdown が設定されている場合は，リンクダウンを検出しても認証端末を認証解除しません。詳細は「5.4.10　ポートリンクダウン時の認証解除抑止」「5.5.7　ポートリンクダウン時の認証解除抑止設定」を参照してください。

(e) VLAN 設定変更による認証解除

コンフィグレーションコマンドで認証端末が含まれる VLAN の設定を変更した場合，変更された VLAN に含まれる端末の認証を解除します。

[コンフィグレーションの変更内容]
- VLAN を削除した場合
- VLAN を停止（suspend）した場合

(f) 運用コマンドによる認証解除

運用コマンド clear dot1x auth-state で，IEEE802.1X 認証端末を手動で認証解除します。

6.2.3 NAP 検疫システムとの連携について

Network Access Protection（以下，NAP）検疫システムでは，ネットワークに接続する前の端末に対しシステム正常性を検証し，セキュリティポリシーに準拠していない端末をアクセス制限付きネットワークに隔離できます。

NAP 検疫システムでは端末のセキュリティ状態を監視する機器をネットワークポリシーサーバ（以下，NPS），監視される端末を NAP クライアントと呼びます。本装置は，NPS と NAP クライアントの間に位置します。

(1) 動作概要

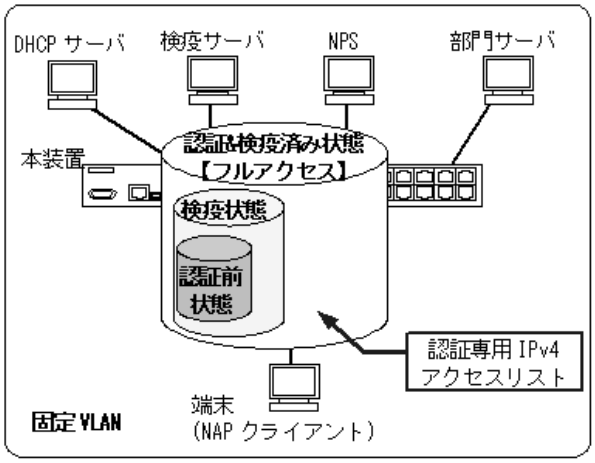
本装置では，ポート単位認証（静的）で NAP 検疫システムと連携した運用が可能です。ポート単位認証（静的）では VLAN を動的に切替えないので，NPS は以下の「状態」で NAP クライアントを監視し，NAP クライアントの「状態」を本装置に通知します。

- 認証前状態
- 検疫状態
- 認証および検疫済み状態

本装置は NPS から受信した情報により，セキュリティポリシーに合致した NAP クライアント（認証および検疫済み状態の端末）だけに，フルアクセス通信を許可します。

ポート単位認証（静的）での NAP 検疫システム連携の概要を次の図に示します。

図 6-13 ポート単位認証（静的）での NAP 検疫システム連携概要図



本装置は，RADIUS サーバ（図内 NPS が相当）からの応答結果である Access-Accept 属性に含まれる「Filter-Id」により，対象端末のアクセス制限を実施します。「Filter-Id」には認証専用 IPv4 アクセスリストが設定されています。

RADIUS サーバからの応答による本装置の動作を次の表に示します。

表 6-6 RADIUS サーバ（NPS）からの応答による本装置の動作

RADIUS サーバ側				本装置の動作		アクセス動作
認証結果	検疫結果	RADIUS 応答	属性 Filter-Id の内容	MAC アドレステーブルへの登録処理	端末への送信	
NG	－	Reject	－	未実施	EAPoL-Failure	通常の認証失敗と同様
OK	NG	Accept	Filter-Id = 認証用 ACL	未実施	EAPoL-Success	検疫状態で制限付アクセス（認証用 ACL の範囲）
OK	OK	Accept	Filter-Id = 0 または Filter-Id なし	実施	EAPoL-Success	認証および検疫済み状態でフルアクセス許可（制限解除）

（凡例）
認証用 ACL：認証専用 IPv4 アクセスリスト
－：通常の失敗と同様のため該当外

本装置には，認証専用 IPv4 アクセスリストで検疫サーバ宛のアクセス許可を設定し，RADIUS サーバの Access-Accept 属性の「Filter-Id」に認証専用 IPv4 アクセスリスト名を設定してご使用ください。
RADIUS サーバの属性については，後述の「6.6 事前準備」も参照してください。

（2） 端末の「検疫状態」「認証および検疫済み状態」の表示

NAP 検疫システム連携では，「検疫状態」（制限付アクセス許可）状態，「認証および検疫済み状態」（フルアクセス許可）が発生します。この状態は，運用コマンド show dot1x の認証サブ状態で確認できます。
表示内容の詳細は運用コマンドレファレンスを参照してください。

表 6-7 IEEE802.1X の状態表示

認証結果	検疫結果	運用コマンド show dot1x の表示		備考
		AuthState 端末の認証処理状態	SubState 認証サブ状態	
NG	－	認証完了以外	認証が完了していないため， 認証サブ状態なし	認証前状態
OK	NG	認証完了	制限付アクセス許可	検疫状態
OK	OK	認証完了	フルアクセス許可	認証および検疫済み状態

（凡例）
－：通常の失敗と同様のため該当外

（3） 本機能を有効にするコンフィグレーション

NAP 検疫システム連携を有効にするためのコンフィグレーションは特にありません。IEEE802.1X のポート単位認証（静的）に必要なコンフィグレーションを設定してください。また，認証専用 IPv4 アクセスリストに検疫サーバ宛のアクセス許可を設定してください。

- ポート単位認証（静的）の設定：「7.3　ポート単位認証（静的）のコンフィグレーション」を参照してください。
- 認証専用 IPv4 アクセスリストの設定：「5.5.2　認証専用 IPv4 アクセスリストの設定」を参照してください。

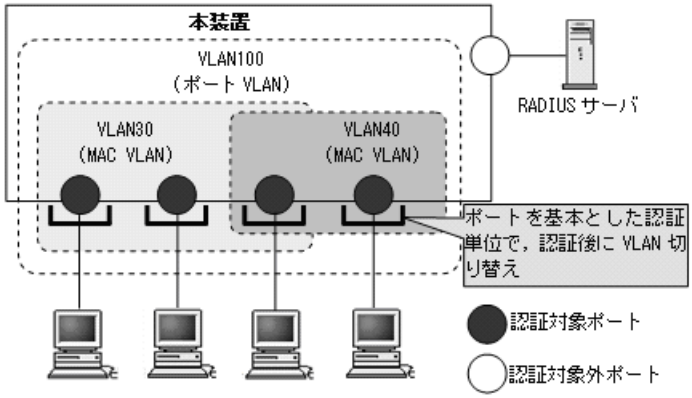
6.3 ポート単位認証（動的）

認証の制御を MAC VLAN に所属する物理ポートまたはチャネルグループに接続している端末に対して行います。この認証モードでは IEEE802.1Q VLAN Tag の付与された EAPOL フレームを扱うことはできません。IEEE802.1Q VLAN Tag の付与された EAPOL フレームを受信すると廃棄します。

認証に成功した端末は，認証サーバである RADIUS サーバからの VLAN 情報（MAC VLAN の VLAN ID）に従い，動的に VLAN の切り替えを行います。

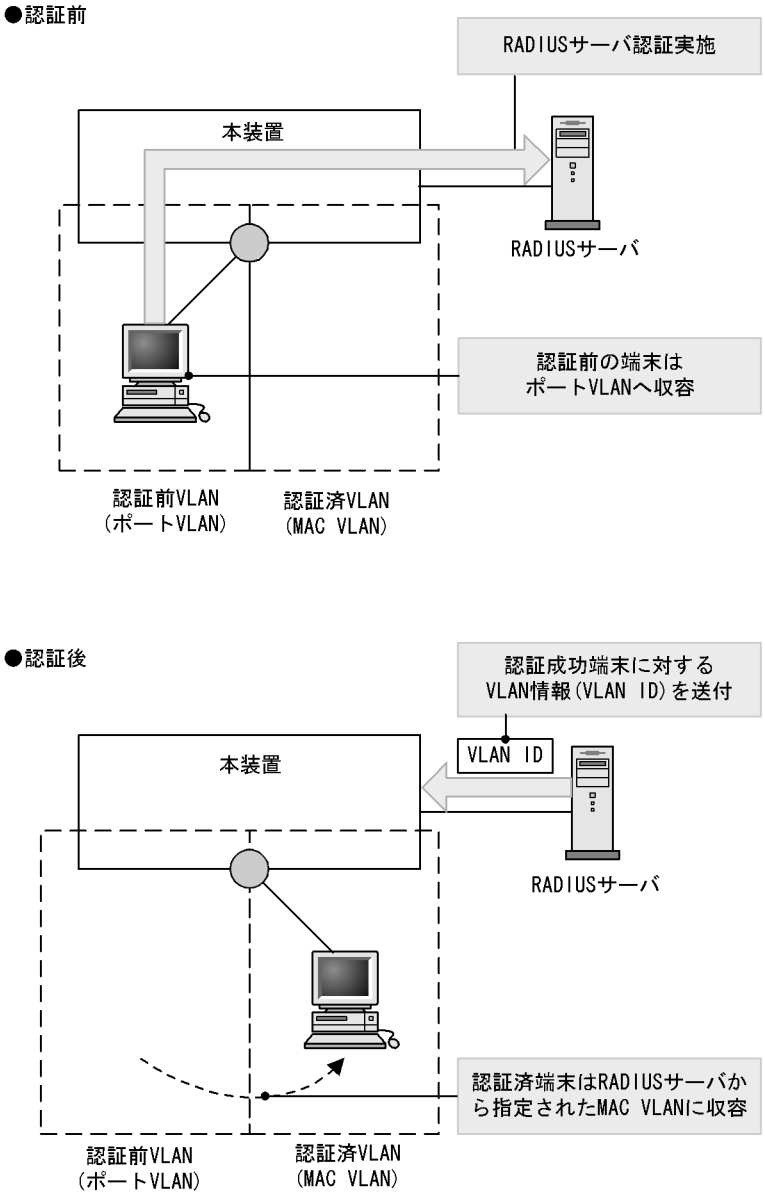
ポート単位認証（動的）の構成例を次の図に示します。

図 6-14 ポート単位認証（動的）の構成例



認証前の端末は，認証が成功するまで通信できません。ポート単位認証（動的）で認証が成功すると，認証が成功した端末の MAC アドレスと認証後 VLAN ID を MAC VLAN と MAC アドレステーブルに IEEE802.1X ポート単位認証エントリとして登録して通信可能になります。（MAC アドレステーブルの登録状態は，運用コマンド show mac-address-table で確認できます。）

図 6-15 ポート単位認証（動的）の動作イメージ



なお，認証前 VLAN に通信する場合は，認証専用 IPv4 アクセスリストを設定してください。

6.3.1 認証サブモードと認証モードオプション

本装置の IEEE802.1X では，認証モードとその下に認証サブモードを設けています。認証モードは，認証制御を行う単位を示し，認証サブモードは認証単位内の端末接続モードを指定します。また，各モードで設定可能な認証モードオプションがあります。

認証モードとサブモード，および認証モードオプションの関係を次の表に示します。

表 6-8 認証サブモードと認証モードオプションの関係

認証モード	認証サブモード	認証モードオプション
ポート単位認証（動的）	シングルモード	－
	端末認証モード	認証除外端末オプション

（1） 認証サブモード

ポート単位認証（静的）と同様です。「6.2.1 認証サブモードと認証モードオプション （1）認証サブモード」を参照してください。

（2） 認証モードオプション

(a) 認証除外端末オプション

スタティック MAC アドレス学習機能 ※1 および MAC VLAN 機能 ※2 によって MAC アドレスが設定された端末については認証を不要とし，通信を許可するオプション設定です。Supplicant 機能を持たないプリンタなどの装置やサーバなど認証が不要な端末を，端末単位で認証対象から除外したいときに使用します。端末認証モードの場合だけ使用可能なオプションです。

注 ※1

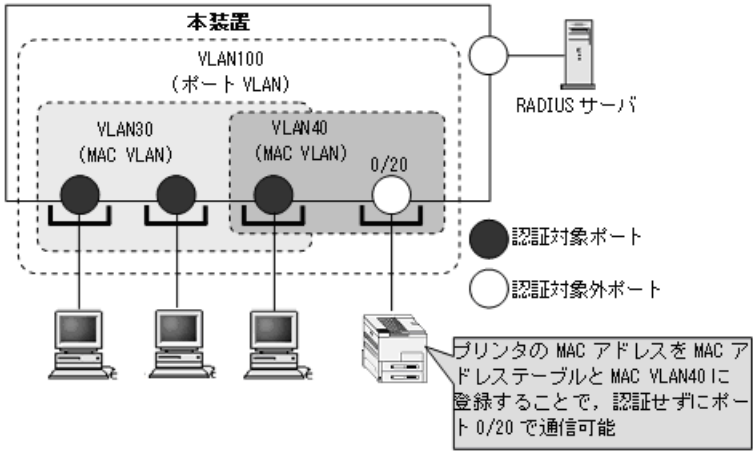
コンフィグレーションコマンド mac-address-table static で，MAC アドレステーブルに MAC アドレスを設定

注 ※2

コンフィグレーションコマンド mac-address で MAC VLAN に MAC アドレスを設定

ポート単位認証（動的）での認証除外端末構成例を次の図に示します。

図 6-16 ポート単位認証（動的）での認証除外端末構成例



6.3.2 認証機能

（1） 認証契機

ポート単位認証（動的）の対象ポートに接続されている端末から，EAPOL-Start を受信したときに認証契機となります。

（2） EAP-Request/Identity フレーム送信

ポート単位認証（静的）と同様です。「6.2.2　認証機能　（2）EAP-Request/Identity フレーム送信」を参照してください。

（3） 端末検出動作切り替えオプション

ポート単位認証（静的）と同様です。「6.2.2　認証機能　（3）端末検出動作切り替えオプション」を参照してください。

（4） 端末への EAP-Request フレーム再送

ポート単位認証（静的）と同様です。「6.2.2　認証機能　（4）端末への EAP-Request フレーム再送」を参照してください。

（5） 端末からの認証要求に対する抑止機能

ポート単位認証（静的）と同様です。「6.2.2　認証機能　（5）端末からの認証要求に対する抑止機能」を参照してください。

（6） 認証失敗時の認証再開までの待機時間

ポート単位認証（静的）と同様です。「6.2.2　認証機能　（6）認証失敗時の認証再開までの待機時間」を参照してください。

（7） 認証サーバ応答待ち時間

ポート単位認証（静的）と同様です。「6.2.2　認証機能　（7）認証サーバ応答待ち時間」を参照してください。

（8） 強制認証ポート指定

強制認証については，「5.4.6　認証共通の強制認証」を参照してください。

また，強制認証で認証許可した端末は，通常の認証済み端末と同様に後述の「6.3.2　認証機能　（10）認証解除」により認証状態が解除されます。

強制認証した端末から送信される EAPOL フレームは，次の再認証時間になるまですべて廃棄します。

（9） 認証数制限

装置単位およびポート単位に認証数の制限が設定できます。詳細は，「5.4.8　認証共通の端末数制限」を参照してください。

（10）認証解除

ポート単位認証（動的）では，認証解除の手段として下記があります。

- 再認証要求時の無応答端末の認証解除
- 認証済み端末の無通信監視による認証解除
- 認証端末接続ポートのリンクダウンによる認証解除
- VLAN 設定変更による認証解除
- 運用コマンドによる認証解除

各認証解除手段は，ポート単位認証（静的）と同様です。「6.2.2　認証機能　（10）認証解除」を参照してください。

6.4 EAPOL フォワーディング機能

本装置で IEEE802.1X を動作させない場合に，EAPOL フレームを中継する機能です。EAPOL フレームは宛先 MAC アドレスが IEEE802.1D で予約されているアドレスであるため通常は中継を行いませんが，IEEE802.1X を使用していない場合はこの機能によって中継が可能です。ほかの Authenticator と端末の間の L2 スイッチとして本装置を使用する場合に設定します。

本機能の設定例は，「コンフィグレーションガイド Vol.1 22.6 L2 プロトコルフレーム透過機能のコンフィグレーション」を参照してください。

6.5 アカウント機能

IEEE802.1X の認証結果は，次のアカウント機能で記録されます。

- 本装置内蔵のアカウントログ
- RADIUS サーバのアカウント機能への記録
- RADIUS サーバへの認証情報の記録
- syslog サーバへのアカウントログ出力

(1) 本装置内蔵のアカウントログ

IEEE802.1X の認証結果や動作情報などの動作ログは，本装置内蔵のアカウントログに記録されます。

本装置内蔵のアカウントログは以下の最大数まで記録できます。

- スタック動作時：全認証機能の合計で最大 4096 行
- スタンドアロン動作時：IEEE802.1X 全体で最大 2100 行

最大数を超えた場合，古い順に記録が削除され，最新のアカウントログ情報が追加記録されていきます。

記録されるアカウントログ情報は次の情報です。

表 6-9 本装置内蔵のアカウントログへの出力情報

アカウントログ種別		時刻	IP	MAC	VLAN	Port	メッセージ
LOGIN	成功	○	×	○	○ ※1	○	認証成功メッセージ
	失敗	○	×	○	○ ※1	○	認証失敗要因メッセージ
LOGOUT		○	×	○	○ ※1	○	認証解除メッセージ
SYSTEM		○	○ ※1※2	○ ※1	×	○ ※1	IEEE802.1X の動作に関するメッセージ

(凡例)
○：出力します
×：出力しません

注 ※1
メッセージによっては出力しない場合があります。

注 ※2
フレーム送信元 IP アドレスまたは接続先 RADIUS サーバ IP アドレス

メッセージの詳細については，「運用コマンドレファレンス 28 IEEE802.1X show dot1x logging」を参照してください。

また，記録されたアカウントログの出力機能については下記のとおりです。

1. 運用コマンド表示
   運用コマンド show dot1x logging で，採取されているアカウントログを最新の情報から表示します。
2. syslog サーバへ出力
   後述「(4) syslog サーバへのアカウントログ出力」を参照してください。
3. プライベート Trap
   IEEE802.1X 認証の特定イベントのアカウントログ採取を契機にプライベート Trap を発行する機能をサポートしています。プライベート Trap 発行可否および発行種別はコンフィグレーションコマンドで

設定してください。

表 6-10 アカウントログ（LOGIN/LOGOUT）とプライベート Trap 発行条件

アカウントログ種別		プライベート Trap 発行に必要なコンフィグレーション設定	
		コマンド	パラメータ
LOGIN	成功	snmp-server host	dot1x
		snmp-server traps	dot1x-trap all
	失敗	snmp-server host	dot1x
		未設定，または下記のどちらかを設定	
		snmp-server traps	dot1x-trap all
		snmp-server traps	dot1x-trap failure
LOGOUT		snmp-server host	dot1x
		snmp-server traps	dot1x-trap all

強制認証のプライベート Trap 発行条件については，「5.4.6 認証共通の強制認証（4）強制認証でのプライベート Trap」を参照してください。

（2） RADIUS サーバのアカウント機能への記録

コンフィグレーションコマンド aaa accounting dot1x で，RADIUS サーバのアカウント機能を使用できます。

なお，RADIUS サーバへアカウンティング情報を送信するときに使用する RADIUS 属性については，「6.6 事前準備」を参照してください。

（3） RADIUS サーバへの認証情報の記録

RADIUS 認証方式の場合は，RADIUS サーバが持っている機能によって，認証成功／認証失敗が記録されます。ただし，使用する RADIUS サーバによって記録される情報が異なることがありますので，詳細は RADIUS サーバの説明書を参照してください。

（4） syslog サーバへのアカウントログ出力

コンフィグレーションで syslog 設定されているすべての syslog サーバへ，装置全体の運用ログ情報と合わせて IEEE802.1X のアカウントログ情報を出力します。

図 6-17 syslog サーバ出力形式

```
 Fac 月 日 時刻 hostname [番号]:AUT 月/日 時刻 1X  ログメッセージ本文
|(1)|---(2) ---|--(3)---|--(4)-|(5)|----(6)---|(7)|-----------(8)-------------|

  (1)ファシリティ
  (2)TIMESTAMP：メッセージ生成時刻
  (3)HOSTNAME:本装置の識別名称
  (4)機能番号
  (5)認証機能を示すログ種別
  (6)事象発生時刻
  (7)IEEE802.1X を示す認証機能種別
  (8)メッセージ本文
```

syslog サーバへのログ出力について詳細は，後述の「23 ログ出力機能」を参照してください。なお，コ

ンフィグレーションコマンド dot1x logging enable および logging event-kind aut によって，
IEEE802.1X のアカウントログ出力を開始および停止できます。

6.6 事前準備

RADIUS 認証方式を使用するにあたっては，次の準備が必要です。

- コンフィグレーションの設定
- RADIUS サーバの準備

(1) コンフィグレーションの設定

IEEE802.1X を使用するために，本装置に VLAN 情報や IEEE802.1X の情報をコンフィグレーションコマンドで設定します。(「7 IEEE802.1X の設定と運用」を参照してください。)

(2) RADIUS サーバの準備

(a) 使用する RADIUS 属性

本装置が使用する RADIUS の属性名を次の表に示します。

表 6-11 認証で使用する属性名（その 1 Access-Request）

属性名	Type 値	解説
User-Name	1	認証されるユーザ ID。
NAS-IP-Address	4	認証を要求している，本装置の IPv4 アドレス。 IPv4 アドレスが登録されている VLAN インタフェースのうち，最も小さい VLAN ID の IPv4 アドレスを使用します。
NAS-Port	5	• ポート単位認証（静的）：認証している認証単位の IfIndex • ポート単位認証（動的）：認証している認証単位の IfIndex
Service-Type	6	提供するサービスタイプ。 Framed(2) 固定。
Framed-MTU	12	Supplicant ～ Authenticator 間の最大フレームサイズ。 (1466) 固定。
State	24	Authenticator と RADIUS サーバ間の State 情報の保持を可能にする。
Called-Station-Id	30	認証ポートの MAC アドレス（小文字 ASCII※，ハイフン（－）区切り）。
Calling-Station-Id	31	Supplicant の MAC アドレス（小文字 ASCII※，ハイフン（－）区切り）。
NAS-Identifier	32	＜ IEEE802.1Q VLAN Tag 付き EAPOL フレーム受信＞ 認証端末を収容している VLAN ID。 ＜ IEEE802.1Q VLAN Tag なし EAPOL フレーム受信＞ コンフィグレーションコマンド hostname で設定された文字列。
NAS-Port-Type	61	Authenticator がユーザ認証に使用している，物理ポートのタイプ。 Ethernet(15) 固定。
Connect-Info	77	Supplicant のコネクションの特徴を示す文字列。 • ポート単位認証（静的）： 物理ポート ("CONNECT Ethernet") チャネルグループポート ("CONNECT Port-Channel ") • ポート単位認証（動的）： 物理ポート ("CONNECT Ethernet") チャネルグループポート ("CONNECT Port-Channel ")
EAP-Message	79	EAP フレームをカプセル化する。
Message-Authenticator	80	RADIUS/EAP フレームを保護するために使用する。

属性名	Type 値	解説
NAS-Port-Id	87	Supplicant を認証する Authenticator のポートを識別するための文字列（x，y には数字が入ります）。 • ポート単位認証（静的）："Port x/y"，"ChGr x" • ポート単位認証（動的）："Port x/y"，"ChGr x"
NAS-IPv6-Address	95	認証を要求している，本装置の IPv6 アドレス。 IPv6 アドレスが登録されている VLAN インタフェースのうち，最も小さい VLAN ID の IPv6 アドレスを使用します。

注 ※

本装置では，「Called-Station-Id」「Calling-Station-Id」の MAC アドレスを小文字で使用しますが，コンフィグレーションコマンド radius-server attribute station-id capitalize により，MAC アドレス内の "a" ～ "f" の文字を大文字形式にできます。

表 6-12　認証で使用する属性名（その 2 Access-Accept）

属性名	Type 値	解説
Service-Type	6	提供するサービスタイプ。 Framed(2) 固定。
Filter-Id	11	テキスト文字列。 • Authenticator に認証前フレームのフィルタを実施させる認証専用 IPv4 アクセスリスト名 • マルチステップ認証で使用 ※1
Reply-Message	18	ユーザに表示されるメッセージ。
Tunnel-Type	64	トンネル・タイプ ※2。 ポート単位認証（動的）で意味を持つ。 VLAN(13) 固定。
Tunnel-Medium-Type	65	トンネルを作成する際のプロトコル ※2。 ポート単位認証（動的）で意味を持つ。 IEEE802(6) 固定。
EAP-Message	79	EAP フレームをカプセル化する。
Message-Authenticator	80	RADIUS/EAP フレームを保護するために使用する。
Tunnel-Private-Group-ID	81	VLAN を識別する文字列 ※3。Accept 時は，認証済みの Supplicant に割り当てる VLAN を意味する。 ポート単位認証（動的）で意味を持つ。 次に示す文字列が対応する。 (1)VLAN ID を示す文字列 (2)"VLAN"+VLAN ID を示す文字列 文字列にスペースを含んではいけない（含めた場合 VLAN 割り当ては失敗する）。 (3) コンフィグレーションコマンド name で VLAN インタフェースに設定された VLAN 名称を示す文字列（VLAN ID の小さいほうを優先）※4 （設定例） VLAN ID：10 コンフィグレーションコマンド name：Authen_VLAN (1) の場合　"10" (2) の場合　"VLAN10" (3) の場合　"Authen_VLAN"

注 ※1

マルチステップ認証で使用する文字列については，「12　マルチステップ認証」を参照してください。

注 ※2

Tag 領域は無視します。

注 ※3

本装置では文字列形式の選択および VLAN ID の識別を下記条件で実施します。

1. Tunnel-Private-Group-ID の文字列形式 (1)(2)(3) 選択条件
   - 先頭が 0 ～ 9 の数字文字で始まる文字列は，(1) の形式
   - 先頭が "VLAN" ＋ 0 ～ 9 の数字文字で始まる文字列は，(2) の形式
   - 上記以外の文字列は，(3) の形式

   なお，先頭 1 バイトが 0x00 ～ 0x1f のときは Tag 付きですが Tag 領域は無視します。
2. (1)(2) 形式の文字列から VLAN ID を識別する条件
   - 数字文字 "0" ～ "9" だけを 10 進数に変換し，先頭 4 文字だけ有効範囲とします。（5 文字目以降は無視します。）

     例) "0010" は "010" や "10" と同じで，VLAN ID = 10　となります。

     "01234" は，VLAN ID =123　となります。
   - 文字列の途中に "0" ～ "9" 以外が入っていると，文字列の終端とします。

     例)"12+3" は，VLAN ID =12　となります。

注 ※4

コンフィグレーションコマンド name による VLAN 名称指定については，「5.4.2　VLAN 名称による収容 VLAN 指定」を参照してください。

表 6-13　認証で使用する属性名（その 3 Access-Challenge）

属性名	Type 値	解説
Reply-Message	18	ユーザに表示されるメッセージ。
State	24	Authenticator と RADIUS サーバ間の State 情報の保持を可能にする。
EAP-Message	79	EAP フレームをカプセル化する。
Message-Authenticator	80	RADIUS/EAP フレームを保護するために使用する。

表 6-14　認証で使用する属性名（その 4 Access-Reject）

属性名	Type 値	解説
Reply-Message	18	ユーザに表示されるメッセージ。
EAP-Message	79	EAP フレームをカプセル化する。
Message-Authenticator	80	RADIUS/EAP フレームを保護するために使用する。

表 6-15　RADIUS アカウント機能で使用する属性名

属性名	Type 値	解説
User-Name	1	認証されるユーザ ID。
NAS-IP-Address	4	認証を要求している，本装置の IPv4 アドレス。 IPv4 アドレスが登録されている VLAN インタフェースのうち，最も小さい VLAN ID の IPv4 アドレスを使用します。
NAS-Port	5	• ポート単位認証（静的）：認証している認証単位の IfIndex • ポート単位認証（動的）：認証している認証単位の IfIndex
Service-Type	6	提供するサービスタイプ。 Framed(2) 固定。
Calling-Station-Id	31	Supplicant の MAC アドレス（小文字 ASCII※，ハイフン（－）区切り）。

属性名	Type 値	解説
NAS-Identifier	32	＜ IEEE802.1Q VLAN Tag 付き EAPOL フレーム受信＞ 認証端末を収容している VLAN ID。 ＜ IEEE802.1Q VLAN Tag なし EAPOL フレーム受信＞ コンフィグレーションコマンド hostname で設定された文字列。
Acct-Status-Type	40	アカウンティング要求種別。 Start(1)，Stop(2)。
Acct-Delay-Time	41	アカウンティング情報（送信遅延時間）。（秒）
Acct-Input-Octets	42	アカウンティング情報（受信オクテット数）。 (0) 固定。
Acct-Output-Octets	43	アカウンティング情報（送信オクテット数）。 (0) 固定。
Acct-Session-Id	44	アカウンティング情報を識別する ID。
Acct-Authentic	45	認証方式。 RADIUS(1)。
Acct-Session-Time	46	アカウンティング情報（セッション持続時間）。 (0) 固定。
Acct-Input-Packets	47	アカウンティング情報（受信パケット数）。 (0) 固定。
Acct-Output-Packets	48	アカウンティング情報（送信パケット数）。 (0) 固定。
Acct-Terminate-Cause	49	アカウンティング情報セッション終了要因。 「表 6-16　Acct-Terminate-Cause での切断要因」を参照。
NAS-Port-Type	61	Authenticator がユーザ認証に使用している，物理ポートのタイプ。 Ethernet(15) 固定。
NAS-Port-Id	87	Supplicant を認証する Authenticator のポートを識別するための文字列（x，y には数字が入ります）。 • ポート単位認証（静的）："Port x/y"，"ChGr x" • ポート単位認証（動的）："Port x/y"，"ChGr x"
NAS-IPv6-Address	95	認証を要求している，本装置の IPv6 アドレス。 IPv6 アドレスが登録されている VLAN インタフェースのうち，最も小さい VLAN ID の IPv6 アドレスを使用します。

注 ※

本装置では，「Calling-Station-Id」の MAC アドレスを小文字で使用しますが，コンフィグレーションコマンド radius-server attribute station-id capitalize により，MAC アドレス内の "a" ～ "f" の文字を大文字形式にできます。

表 6-16　Acct-Terminate-Cause での切断要因

属性名	Type 値	解説
User Request	1	Supplicant からの要求で切断した。 • 認証端末から logoff を受信した場合 端末移動を検出したため切断した。
Idle Timeout	4	無通信時間が一定時間続いたため切断した。

属性名	Type 値	解説
Admin Reset	6	管理者の意思で切断した。 • 認証単位でコンフィグレーションを削除した場合 • コンフィグレーションで dot1x port-control force-authorized を設定した場合 • コンフィグレーションで dot1x port-control force-unauthorized を設定した場合 • コンフィグレーションで dot1x port-control を削除した場合 • 運用コマンドで clear dot1x auth-state を実行した場合 その他認証用コンフィグレーションの変更や運用コマンドによる切断要因を含む。
NAS Request	10	マルチステップ認証で２段目が成功したため，１段目の IEEE802.1X 認証を切断した。（コンフィグレーションコマンド authentication multi-step dot1x 設定時）
Reauthentication Failure	20	再認証に失敗した。
Port Reinitialized	21	ポートの MAC が再初期化された。 • ポートがリンクダウンした場合 • コンフィグレーションでポートから vlan を削除した場合 • コンフィグレーションで shutdown を設定した場合 • 運用コマンド inactivate を実行した場合
Port Administratively Disabled	22	ポートが管理的に無効にされた。 • 認証サブモードがシングルモードのポートで２台目の端末を検出した場合

（b） RADIUS サーバに設定する情報

RADIUS 認証方式を使用するに当たっては，RADIUS サーバでユーザごとにユーザ ID，パスワード，VLAN ID の設定が必要です。

なお，RADIUS サーバの詳細な設定方法については，使用する RADIUS サーバの説明書を参照してください。

認証対象ユーザごとの VLAN 情報の RADIUS サーバ設定例を示します。

- ポート単位認証（静的）の場合：設定不要
- ポート単位認証（動的）の場合：認証後 VLAN「40」
- コンフィグレーションコマンド name の設定：「dot1x-authen-vlan」

表 6-17　RADIUS サーバ設定例

設定項目	設定内容
User-Name	認証対象端末のユーザ ID。
Auth-Type	Local
User-Password	認証対象端末のパスワード。
NAS-Identifier	本装置のホスト名。 （コンフィグレーションコマンド hostname の設定文字列）
Tunnel-Type	Virtual VLAN（値 13）
Tunnel-Medium-Type	IEEE-802（値 6）

設定項目	設定内容
Tunnel-Private-Group-ID	ポート単位認証（動的）の場合 下記のいずれかの形式 • "40" 認証後 VLAN ID を数字文字で設定。 • "VLAN40" 文字列 "VLAN" に続いて，認証後 VLAN ID を数字文字で設定。 • "dot1x-authen-vlan" コンフィグレーションコマンド name で設定された VLAN 名称を示す文字列。
認証方式	EAP

6.7 IEEE802.1X の注意事項

6.7.1 IEEE802.1X と他機能の共存について

IEEE802.1X と他機能の共存については，「5.9.3 レイヤ 2 認証機能と他機能の共存」を参照してください。

6.7.2 IEEE802.1X 使用時の注意事項

(1) 認証済み端末の MAC アドレステーブル表示について

ポート単位認証で認証した端末は，運用コマンド show mac-address-table でタイプに Dot1x を表示します。ただし，ポート単位認証（静的）で検疫状態の端末は，Dynamic を表示します。

(2) 認証済み端末のポート移動について

認証済み端末を IEEE802.1X 認証設定ポートへポート移動したときは，認証解除します。

なお，認証済み端末を同一 VLAN 内の IEEE802.1X 認証未設定ポートへ移動したときは，認証状態が解除されるまで通信できません。運用コマンド clear dot1x auth-state を使用して，端末の認証状態を解除してください。

(3) タイマ値の変更について

タイマ値（tx-period，reauth-period，supp-timeout，quiet-period，keep-unauth）を変更した場合，変更した値が反映されるのは，各認証単位で現在動作中のタイマがタイムアウトして 0 になったときです。すぐに変更を反映させたい場合には，運用コマンド clear dot1x auth-state を使用して認証状態をいったん解除してください。

(4) 端末と本装置の間に L2 スイッチを配置する場合の注意事項

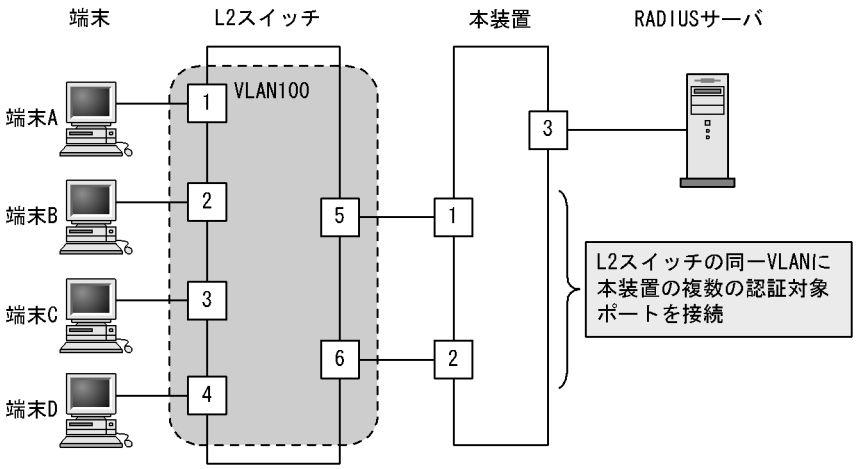
端末からの応答は一般的にマルチキャストとなるため，端末と本装置の間に L2 スイッチを配置する場合，端末からの応答による EAPOL フレームは L2 スイッチの同一 VLAN の全ポートへ転送されます。従って，L2 スイッチの VLAN を次のように設定すると，同一端末からの EAPOL フレームが本装置の複数のポートへ届き，複数のポートで同一端末に対する認証処理が行われるようになります。そのため，認証動作が不安定になり，通信が切断されたり，認証ができなくなったりします。

- L2 スイッチの同一 VLAN に設定されているポートを，本装置の認証対象となっている複数のポートに接続した場合
- L2 スイッチの同一 VLAN に設定されているポートを，複数の本装置の認証対象となっているポートに接続した場合

端末と本装置の間に L2 スイッチを配置する場合の禁止構成例と正しい構成例を次の図に示します。

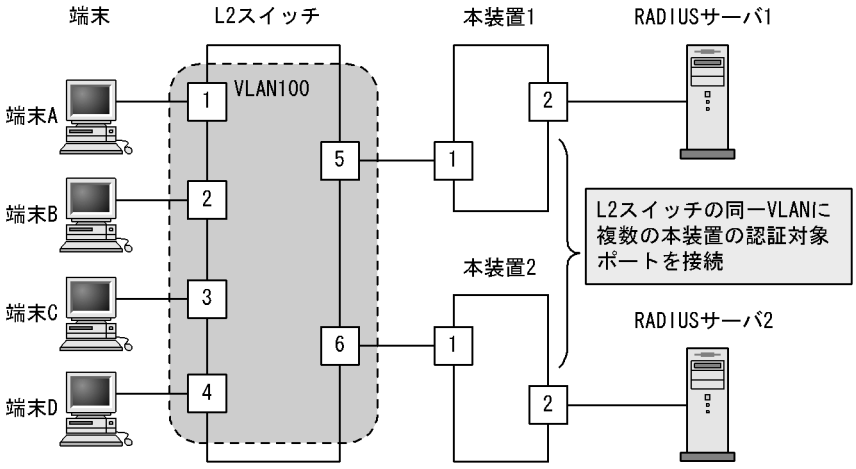
図 6-18 禁止構成例

・L2スイッチの同一VLANに本装置の複数の認証対象ポートを接続した例



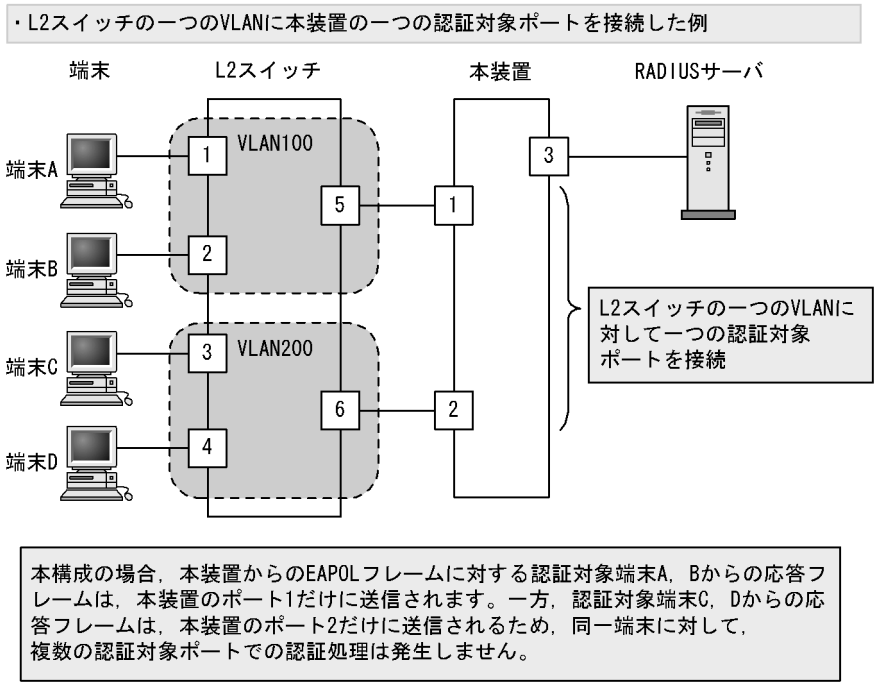
本構成の場合，本装置から送信したEAPOLフレームに対して，認証対象端末A，B，C，Dからの応答フレームが本装置の認証対象ポート1，2に転送されてしまいます。これによって，本装置の認証ポート1，2では同一端末に対する認証処理が実行されます。各認証ポートでは，認証する端末が他ポートで認証されている場合，他ポートの認証状態を解除して，自ポートでの認証処理を行います。その結果，他ポートで認証済みである端末の通信が遮断されます。

・L2スイッチの同一VLANに複数の本装置の認証対象ポートを接続した例



本構成の場合，認証対象端末から送られたEAPOL-Startフレームがマルチキャストで本装置1および本装置2に送信されます。このEAPOL-Startフレームを受信した本装置1，本装置2で認証処理が行われて，一つの端末に対して本装置1および本装置2で認証済み状態になる場合があります。

図 6-19 正しい構成例



(5) MAC VLAN をアクセスポートとして指定した場合の注意事項

MAC VLAN をアクセスポートとして指定したインタフェースにポート単位認証（静的）を設定できますが，ポート単位認証（動的）とポート内共存はできません。（装置内での共存は可能です。詳細は「5 レイヤ 2 認証機能の概説」を参照してください。）

(6) 強制認証ポートの使用について

本機能はセキュリティ上の問題となる可能性がありますので，十分検討の上ご使用ください。

7 IEEE802.1X の設定と運用

IEEE802.1X は OSI 階層モデルの第 2 レイヤで認証を行う機能です。この章では，IEEE802.1X のオペレーションについて説明します。

7.1　IEEE802.1X のコンフィグレーション

7.1.1　コンフィグレーションコマンド一覧

IEEE802.1X のコンフィグレーションコマンドと認証モード一覧を次の表に示します。

表 7-1　IEEE802.1X のコンフィグレーションコマンドと認証モード一覧

コマンド名	説明	認証モード	
		ポート単位	
		静的	動的
aaa accounting dot1x	IEEE802.1X のアカウンティング情報をアカウンティングサーバへ送信します。	○	○
aaa authentication dot1x	IEEE802.1X の認証方式グループを設定します。	○	○
authentication arp-relay	コマンドおよび設定の詳細などについては，「5　レイヤ 2 認証機能の概説」を参照。	○	○
authentication ip access-group	コマンドおよび設定の詳細などについては，「5　レイヤ 2 認証機能の概説」を参照。	○	○
dot1x authentication	ポート別認証方式の認証方式リスト名を設定します。	○	○
dot1x auto-logout	no dot1x auto-logout コマンドで，IEEE802.1X で認証された端末から一定時間フレームを受信しなかった状態を検出したときに認証を自動解除する設定を無効にします。	○	○
dot1x force-authorized eapol	認証対象端末を強制的に認証許可状態としたとき，端末に対して本装置から EAPoL-Success 応答フレームを送信します。	○	○
dot1x ignore-eapol-start	Supplicant からの EAPOL-Start 受信時に，EAP-Request/Identity を送信しない設定をします。	○	○
dot1x logging enable	IEEE802.1X の動作ログに出力する情報を syslog サーバへ出力します。	○	○
dot1x max-req	Supplicant からの応答がない場合に EAP-Request/Identity を再送する最大回数を設定します。	○	○
dot1x multiple-authentication	ポート単位認証の認証サブモードを設定します。	○	○
dot1x port-control※1	ポート単位認証を有効にします。	○	○
dot1x radius-server host	IEEE802.1X 認証専用 RADIUS サーバ情報を設定します。	○	○
dot1x radius-server dead-interval	IEEE802.1X 認証専用 RADIUS サーバ使用時，プライマリ RADIUS サーバへ自動復旧するまでの監視タイマを設定します。	○	○
dot1x reauthentication	認証済み端末の再認証の有効／無効を設定します。	○	○
dot1x supplicant-detection	認証サブモードに端末認証モードを指定したときの端末検出動作のオプションを設定します。	○	○
dot1x system-auth-control	IEEE802.1X を有効にします。	○	○
dot1x timeout keep-unauth※2	ポート単位認証のシングルモードで，複数の端末からの認証要求を検出したときに，そのポートでの通信遮断状態を保持する時間を設定します。	○	○
dot1x timeout quiet-period	認証（再認証を含む）に失敗した Supplicant の認証処理再開を許可するまでの待機時間を設定します。	○	○
dot1x timeout reauth-period	認証済み端末の再認証を行う間隔を設定します。	○	○

コマンド名	説明	認証モード	
		ポート単位	
		静的	動的
dot1x timeout server-timeout	認証サーバからの応答待ち時間を設定します。	○	○
dot1x timeout supp-timeout	Supplicant へ送信した EAP-Request/Identity に対して，Supplicant からの応答待ち時間を設定します。	○	○
dot1x timeout tx-period	定期的な EAP-Request/Identity の送信間隔を設定します。	○	○

（凡例）

ポート単位　静的：ポート単位認証（静的）

ポート単位　動的：ポート単位認証（動的）

○：設定内容に従って動作します

－：コマンドは入力できますが，動作しません

×：コマンドを入力できません

注 ※1

本コマンドの設定は，認証モードの切り替えに影響します。

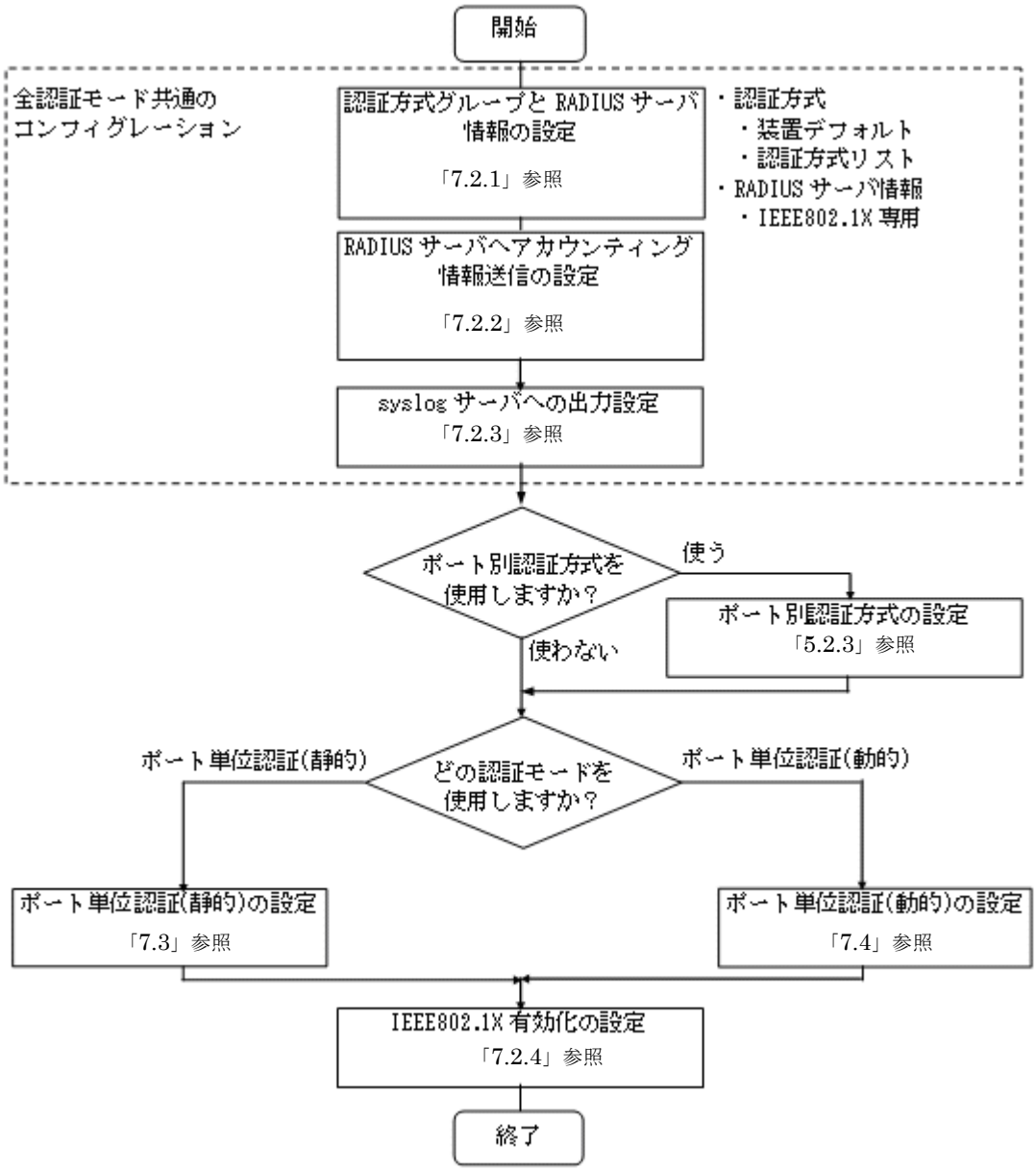
注 ※2

本コマンドの設定は，シングルモードのポートにだけ適用します。

7.1.2 IEEE802.1X の設定手順

IEEE802.1X は，下記の手順で設定してください。

図 7-1 IEEE802.1X の設定手順



各設定の詳細は，下記を参照してください。

1. 全認証モード共通のコンフィグレーション
   全認証モード共通のコンフィグレーションを設定します。
   - 認証方式グループと RADIUS サーバ情報の設定：「7.2.1　認証方式グループと RADIUS サーバ情報の設定」
   - RADIUS サーバへアカウンティング情報送信の設定：「7.2.2　アカウンティング情報送信の設定」
   - syslog サーバへの出力設定：「7.2.3　syslog サーバへの出力設定」
   - ポート別認証方式の設定：「5.2.3　認証方式リストのコンフィグレーション（2）ポート別認証方式の設定例」

2. 各認証モードの設定
   各認証モードのコンフィグレーションを設定します。
   設定項目によっては，他の認証モードと共通になる場合があります。これについては「～を参照してく

ださい。」と記載していますので，該当箇所を参照してください。
- ポート単位認証（静的）の設定：「7.3　ポート単位認証（静的）のコンフィグレーション」
- ポート単位認証（動的）の設定：「7.4　ポート単位認証（動的）のコンフィグレーション」

3. IEEE802.1X の有効化
   最後に IEEE802.1X を有効設定して，IEEE802.1X の設定は終了です。
   - 「7.2.4　IEEE802.1X の有効化」

各認証モードは下記のコンフィグレーション設定で有効となります。

表 7-2　各認証モード有効条件

認証モード	コンフィグレーション設定
共通	• aaa authentication dot1x • dot1x radius-server host または radius-server • dot1x system-auth-control
ポート単位認証（静的）	アクセスポートで使用する場合 • vlan <VLAN ID list> • dot1x port-control auto • switchport mode access • switchport access vlan トランクポートで使用する場合 • vlan <VLAN ID list> • dot1x port-control auto • switchport mode trunk • switchport trunk allowed vlan • switchport trunk native vlan MAC ポートで使用する場合 • vlan <VLAN ID list> または vlan <VLAN ID list> mac-based • dot1x port-control auto • switchport mode mac-vlan • switchport mac dot1q vlan
ポート単位認証（動的）	• vlan <VLAN ID list> mac-based • dot1x port-control auto • switchport mode mac-vlan

7.2　全認証モード共通のコンフィグレーション

7.2.1　認証方式グループと RADIUS サーバ情報の設定

（1） 認証方式グループの設定

［設定のポイント］

IEEE802.1X の認証方式グループを設定します。

IEEE802.1X 共通で使用する装置デフォルトを 1 エントリ，認証ポートで使用する認証方式リストを 2 エントリ設定します。

1. 装置デフォルト
   本例では，装置デフォルトに RADIUS 認証を設定します。
2. 認証方式リスト
   認証方式リストに指定する RADIUS サーバグループ情報は，"Keneki-group1" と "Keneki-group2" を設定済みとします。
   認証方式リストについては「5.2.2　認証方式リスト」を参照してください。
   RADIUS サーバグループ情報については，「5.3.1　レイヤ 2 認証機能で使用する RADIUS サーバ情報」「コンフィグレーションガイド Vol.1 10 ログインセキュリティと RADIUS」を参照してください。

［コマンドによる設定］

1. **(config)# aaa authentication dot1x default group radius**
   装置デフォルトの認証方式は，RADIUS 認証を設定します。
2. **(config)# aaa authentication dot1x DOT1X-list1 group Keneki-group1**
   認証方式リスト "DOT1X-list1" に，RADIUS サーバグループ名 "Keneki-group1" を設定します。
3. **(config)# aaa authentication dot1x DOT1X-list2 group Keneki-group2**
   認証方式リスト "DOT1X-list2" に，RADIUS サーバグループ名 "Keneki-group2" を設定します。

［注意事項］

認証方式グループの設定を変更したときは，影響を受ける端末の認証を解除します。

- 装置デフォルトを追加したときは，認証を解除しません。
- 装置デフォルトを変更，または削除したときは，装置デフォルトで認証した端末を認証解除します。
- 認証方式リストを追加したときは，当該認証方式リスト名を設定したポートの端末を認証解除します。（ポートに設定されている認証方式リストがコンフィグレーションコマンド aaa authentication dot1x で未設定の場合，装置デフォルトで認証されます。）
- 認証方式リストを変更，または削除したときは，当該認証方式リストで認証した端末を認証解除します。

（2） RADIUS サーバ情報の設定

（a） IEEE802.1X 専用 RADIUS サーバを使用する場合

［設定のポイント］

IEEE802.1X だけで使用する認証専用 RADIUS サーバ情報を設定します。

RADIUS サーバ設定を有効にするためには，IP アドレスと RADIUS 鍵の設定が必要です。コンフィグレーションコマンド dot1x radius-server host では IP アドレスだけの設定も可能ですが，RADIUS 鍵を設定するまでは認証に使用されません。

また，本例では使用不可状態になった IEEE802.1X 認証専用 RADIUS サーバを，自動復旧する監視タイマ（dead-interval 時間）も設定します。

［コマンドによる設定］

1. **(config)# dot1x radius-server host 192.168.10.200 key "dot1x-auth"**
   IEEE802.1X だけで使用する RADIUS サーバの IP アドレスおよび RADIUS 鍵を設定します。この場合，auth-port，acct-port，timeout，retransmit は省略時の初期値が適用されます。
2. **(config)# dot1x radius-server dead-interval 15**
   設定した IEEE802.1X 認証専用 RADIUS サーバが使用不可状態になったときに，自動復旧までの監視タイマ（dead-interval 時間）を 15 分に設定します。

［注意事項］

- 本情報未設定時は，汎用 RADIUS サーバ情報の設定に従います。IEEE802.1X 認証専用 RADIUS サーバ情報と汎用 RADIUS サーバ情報の両方未設定のときは，RADIUS 認証を実施できません。
- IEEE802.1X 認証専用 RADIUS サーバ情報は，最大 4 エントリまで設定できます。
- RADIUS 鍵，再送回数，応答タイムアウト時間を省略したときは，それぞれコンフィグレーションコマンド radius-server key，radius-server retransmit，radius-server timeout の設定に従います。

（b） 汎用 RADIUS サーバを使用する場合

汎用 RADIUS サーバの設定については，「コンフィグレーションガイド Vol.1 10 ログインセキュリティと RADIUS」を参照してください。

7.2.2 アカウンティング情報送信の設定

［設定のポイント］
IEEE802.1X のアカウンティング情報を RADIUS サーバへ送信するよう設定します。

［コマンドによる設定］

1. **(config)# aaa accounting dot1x default start-stop group radius**
   RADIUS サーバへアカウンティング情報を送信するよう設定します。

7.2.3 syslog サーバへの出力設定

IEEE802.1X のアカウントログを syslog サーバへ出力するよう設定します。

［設定のポイント］
IEEE802.1X の認証情報および動作情報を記録したアカウントログを，syslog サーバへ出力する設定をします。

［コマンドによる設定］

1. **(config)# dot1x logging enable**
   syslog サーバへの出力を有効にします。

［注意事項］
syslog サーバへの送信対象イベント種別として，コンフィグレーションコマンド logging event-kind aut も合わせて設定してください。

7.2.4 IEEE802.1X の有効化

［設定のポイント］

グローバルコンフィグレーションモードで IEEE802.1X を有効にします。このコマンドを実行しないと，IEEE802.1X のほかのコマンドが有効になりません。

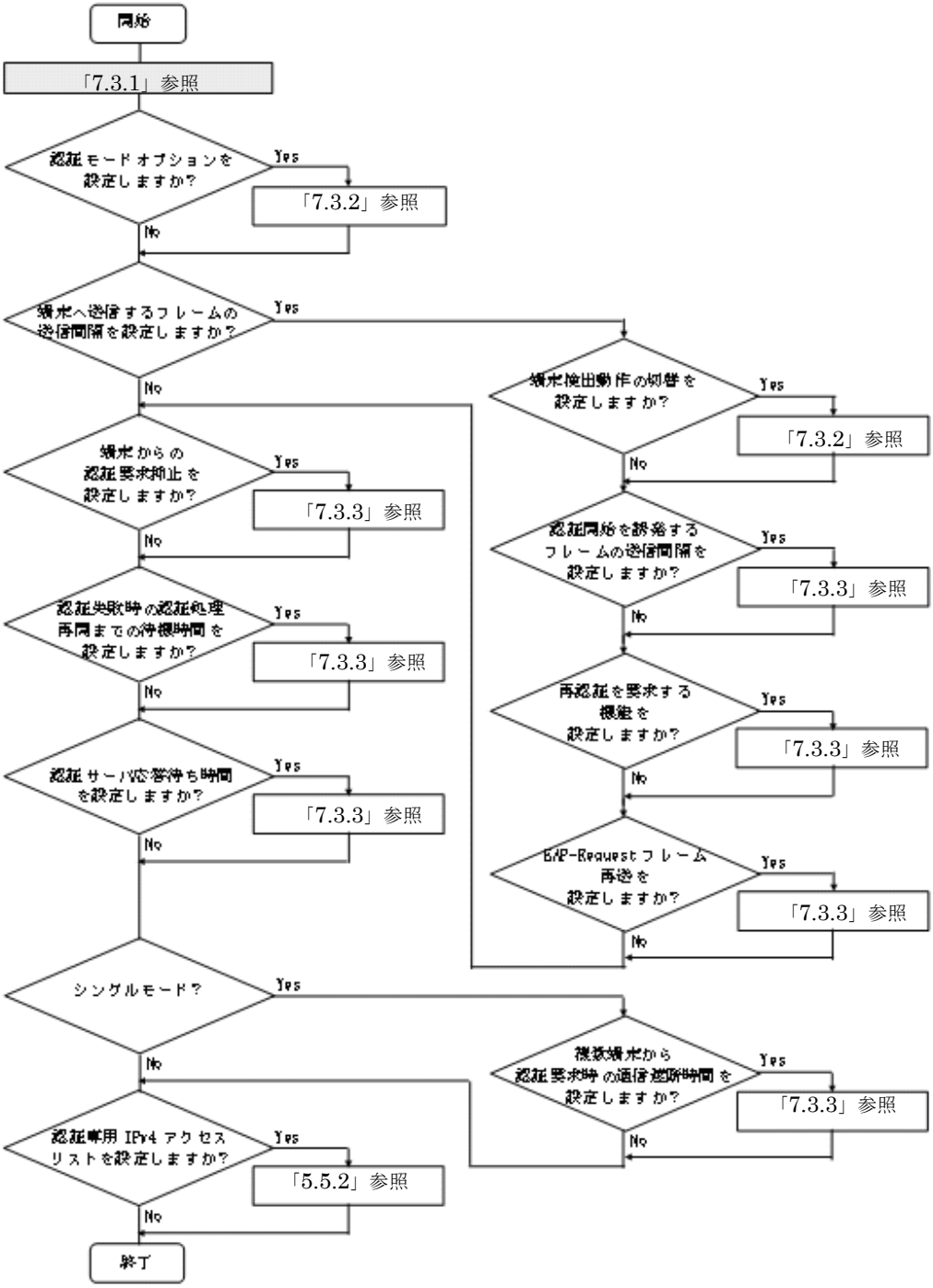
［コマンドによる設定］

1. **(config)# dot1x system-auth-control**
   IEEE802.1X を有効にします。

7.3　ポート単位認証（静的）のコンフィグレーション

「7.1　IEEE802.1X のコンフィグレーション」および「7.2　全認証モード共通のコンフィグレーション」に記載の設定をしたうえで，次の図の手順に従ってポート単位認証（静的）のコンフィグレーションを設定してください。

図 7-2　ポート単位認証（静的）の設定手順



各設定の詳細は，下記を参照してください。

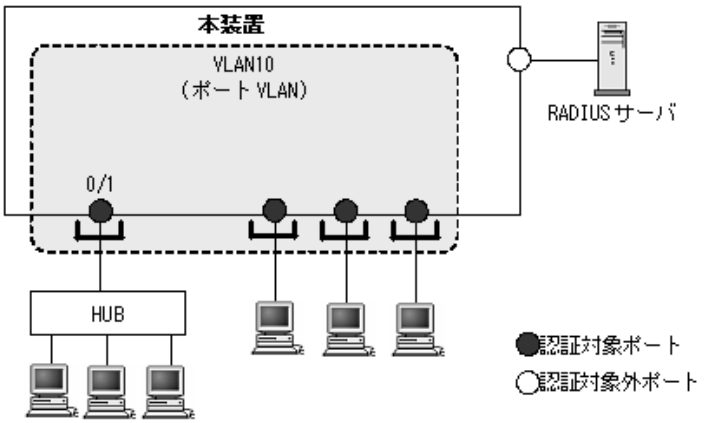
1. ポート単位認証（静的）の設定：「7.3.1　ポート単位認証（静的）の設定」
2. 認証モードオプションの設定：「7.3.2　認証モードオプションの設定」
3. 端末へ送信するフレームの送信間隔の設定
   - 端末検出動作切り替えの設定：「7.3.2　認証モードオプションの設定　(2) 端末検出動作の切替設定」
   - 認証開始を誘発するフレームの送信制御：「7.3.3　認証処理に関する設定　(1) 端末へ認証開始を誘発するフレームの送信間隔の設定」
   - 再認証を要求する機能：「7.3.3　認証処理に関する設定　(2) 端末へ再認証を要求する機能の設定
   - EAP-Request フレーム再送：「7.3.3　認証処理に関する設定　(3) 端末へ EAP-Request フレーム再送の設定」
4. 端末からの認証抑止の設定：「7.3.3　認証処理に関する設定　(4) 端末からの認証要求を抑止する機能の設定」
5. 認証失敗時の認証処理再開までの待機時間設定：「7.3.3　認証処理に関する設定　(5) 認証失敗時の認証処理再開までの待機時間設定」
6. 認証サーバ応答待ち時間の設定：「7.3.3　認証処理に関する設定　(6) 認証サーバ応答待ち時間のタイマ設定」
7. 複数端末からの認証要求時の通信遮断時間の設定：「7.3.3　認証処理に関する設定　(7) 複数端末から認証要求時の通信遮断時間の設定」
8. 認証専用 IPv4 アクセスリストの設定：「5.5.2　認証専用 IPv4 アクセスリストの設定」

7.3.1　ポート単位認証（静的）の設定

(1) 認証ポートと認証用 VLAN 情報の設定

物理ポートまたはチャネルグループを認証の対象に設定します。

図 7-3　ポート単位認証（静的）の構成例



[設定のポイント]

アクセスポートを設定し，そのポートでポート単位認証（静的）を有効にします。認証サブモードを設定します。認証サブモードの設定を省略するとシングルモードになります。

[コマンドによる設定]

1. **(config)# vlan 10**

```
(config-vlan)# exit
```
VLAN ID 10 を設定します。

2.
```
(config)# interface gigabitethernet 0/1
(config-if)# switchport mode access
(config-if)# switchport access vlan 10
```
ポート 0/1 をアクセスポートとして設定し，VLAN ID 10 を設定します。

3.
```
(config-if)# dot1x multiple-authentication
```
認証サブモードを端末認証モードに設定します。

4.
```
(config-if)# dot1x port-control auto
(config-if)# exit
```
ポート単位認証を有効にします。

（2） ポート別認証方式の認証方式リスト名の設定

［設定のポイント］

ポート別認証方式の認証方式リスト名を設定します。
認証方式リストの設定は前述の「7.2.1　認証方式グループと RADIUS サーバ情報の設定（1）認証方式グループの設定」を参照してください。

［コマンドによる設定］

1.
```
(config)# interface gigabitethernet 0/1
(config-if)# dot1x authentication DOT1X-list1
(config-if)# exit
```
ポート 0/1 に認証方式リスト名 "DOT1X-list1" を設定します。

［注意事項］

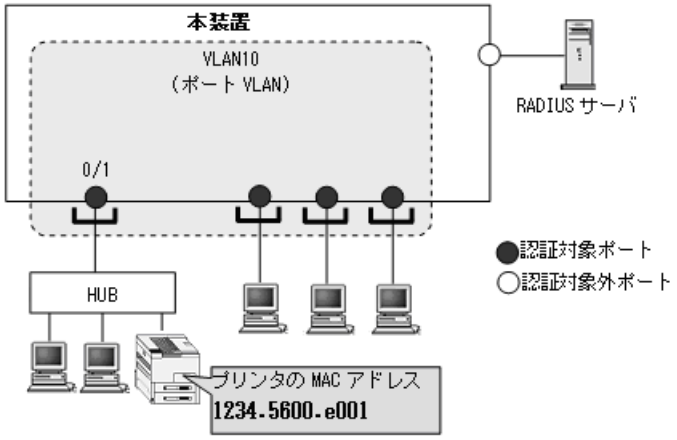
- 本情報未設定時は，「7.2.1　認証方式グループと RADIUS サーバ情報の設定（1）認証方式グループの設定」の装置デフォルトに従って認証します。
- ポートに設定した認証方式リスト名と，認証方式グループの認証方式リスト名が不一致，または認証方式グループに存在しないときは，装置デフォルトに従って認証します。
- Web 認証のユーザ ID 別認証方式は併用設定できません。詳細は「5.2.2　認証方式リスト」を参照してください。

7.3.2　認証モードオプションの設定

（1） 認証除外オプションの設定

IEEE802.1X を持たない端末など，認証を行わないで通信を許可する端末の MAC アドレスを設定します。本例では，「7.3.1　ポート単位認証（静的）の設定」で設定したポート 0/1 に，認証しないで通信するプリンタ（MAC アドレス：1234.5600.e001）を接続します。

図 7-4 ポート単位認証（静的）の認証除外の構成例



［設定のポイント］

ポート単位認証（静的）では，MAC アドレステーブルにスタティックエントリを登録します。

［コマンドによる設定］

1. **(config)# mac-address-table static 1234.5600.e001 vlan 10 interface gigabitethernet 0/1**

   ポート 0/1 の VLAN ID 10 に認証しないで通信させたい MAC アドレス (1234.5600.e001) を MAC アドレステーブルに設定します。

(2) 端末検出動作の切替設定

端末の認証開始を誘発するために，本装置は tx-period コマンドで指定した間隔で EAP-Request/Identity をマルチキャスト送信します。このとき，EAP-Request/Identity に応答した認証済み端末に対する認証シーケンス動作を設定します。デフォルトコンフィグレーションは，認証処理を省略します。

［設定のポイント］

- shortcut は，認証処理を省略して本装置の負荷を軽減します。
- disable は，当該ポートで検出済みの端末が存在する場合，定期的な EAP-Request/Identity の送信を行いません。
- auto は，新規端末からの ARP/IP フレーム受信時に，EAP-Request/Identify を当該端末にだけ送信します。

［コマンドによる設定］（shortcut の例）

1. **(config)# interface gigabitethernet 0/1**
   (config-if)# dot1x multiple-authentication
   (config-if)# dot1x port-control auto
   (config-if)# dot1x supplicant-detection shortcut
   (config-if)# exit

   ポート 0/1 に認証済み端末からの EAP-Response/Identity 受信では，再認証処理を省略して認証成功とするように設定します。

［コマンドによる設定］（auto の例）

1. **(config)# interface gigabitethernet 0/1**

```
(config-if)# dot1x multiple-authentication
(config-if)# dot1x port-control auto
(config-if)# dot1x supplicant-detection auto
(config-if)# exit
```

ポート 0/1 では，新規端末からの ARP/IP フレーム受信時に，該当端末にだけ EAP-Request/Identity を送信するように設定します。

7.3.3 認証処理に関する設定

(1) 端末へ認証開始を誘発するフレームの送信間隔の設定

自発的に認証を開始しない端末に対して，認証開始を誘発するために本装置から定期的に EAP-Request/Identity を送信する時間間隔を設定します。

[設定のポイント]

本機能は，tx-period タイマに設定してある時間間隔で EAP-Request/Identity をマルチキャスト送信します。認証済みの端末からも EAP-Response/Identity の応答を受信し，装置の負荷を高くする可能性がありますので，以下の計算式で決定される値を設定してください。

reauth-period ＞ tx-period ≧ (装置で認証を行う総端末数÷20)×2

tx-period のデフォルトコンフィグレーションが 30 秒であるため，300 台以上の端末で認証を行う場合は，tx-period タイマ値を変更してください。

[コマンドによる設定]

1.
```
(config)# interface gigabitethernet 0/1
(config-if)# dot1x timeout tx-period 300
(config-if)# exit
```

ポート単位認証を設定しているポート 0/1 に EAP-Request/Identity 送信の時間間隔を 300 秒に設定します。

(2) 端末へ再認証を要求する機能の設定

認証後にネットワークから外れた端末は本装置から認証を解除できないため，認証済みの端末に対して再認証を促し，応答のない端末の認証を解除します。

[設定のポイント]

認証済みの端末ごとに，reauth-period タイマに設定している時間間隔で EAP-Request/Identity を送信します。reauth-period タイマの設定値は，tx-period タイマの設定値よりも大きい値を設定してください。

[コマンドによる設定]

1.
```
(config)# interface gigabitethernet 0/1
(config-if)# dot1x reauthentication
(config-if)# dot1x timeout reauth-period 360
(config-if)# exit
```

ポート 0/1 での再認証要求機能を有効に設定し，再認証の時間間隔を 360 秒に設定します。

(3) 端末へ EAP-Request フレーム再送の設定

端末の認証中に，本装置から送信する EAP-Request（認証サーバからの要求メッセージ）に対して，端末から応答がない場合の再送時間と再送回数を設定します。

[設定のポイント]

再送時間間隔と再送回数の総時間が，reauth-period タイマに設定している時間より短い時間になるように設定してください。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 0/1**
   (config-if)# dot1x timeout supp-timeout 60
   ポート 0/1 での EAP-Request フレームの再送時間を 60 秒に設定します。

2. **(config-if)# dot1x max-req 3**
   (config-if)# exit
   ポート 0/1 での EAP-Request フレームの再送回数を 3 回に設定します。

(4) 端末からの認証要求を抑止する機能の設定

端末からの EAPOL-Start フレーム受信による認証処理を抑止します。本機能を設定した場合，新規認証および再認証は，それぞれ tx-period タイマ，reauth-period タイマの時間間隔で行われます。

[設定のポイント]

多数の端末から短い時間間隔で再認証要求が行われ，装置の負荷が高い場合に設定を行い，負荷を低減します。本コマンドの設定前に dot1x reauthentication コマンドの設定が必要です。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 0/1**
   (config-if)# dot1x reauthentication
   (config-if)# dot1x ignore-eapol-start
   (config-if)# exit
   ポート 0/1 で EAPOL-Start フレーム受信による認証処理を抑止します。

(5) 認証失敗時の認証処理再開までの待機時間設定

認証に失敗した端末に対する認証再開までの待機時間を設定します。

[設定のポイント]

認証に失敗した端末から，短い時間に認証の要求が行われることで装置の負荷が高くなることを抑止します。

ユーザが ID やパスワードの入力誤りによって認証が失敗した場合でも，設定した時間を経過しないと認証処理を再開しないので，設定時間には注意してください。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 0/1**
   (config-if)# dot1x timeout quiet-period 300
   (config-if)# exit
   ポート単位認証を設定しているポート 0/1 に認証処理再開までの待機時間を 300 秒に設定します。

(6) 認証サーバ応答待ち時間のタイマ設定

認証サーバへの要求に対する応答がない場合の待ち時間を設定します。設定した時間が経過すると，Supplicant へ認証失敗を通知します。コンフィグレーションコマンド radius-server で設定している再送を含めた総時間と比較して短い方の時間で Supplicant へ認証失敗を通知します。

[設定のポイント]

コンフィグレーションコマンド radius-server で複数のサーバを設定している場合，各サーバの再送回数を含めた総応答待ち時間よりも短い時間を設定すると，認証サーバへ要求している途中で Supplicant へ認証失敗を通知します。設定したすべての認証サーバから応答がないときに認証失敗を通知したい場合は，本コマンドの設定時間を長く設定してください。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 0/1**
   (config-if)# dot1x timeout server-timeout 300
   (config-if)# exit
   ポート単位認証を設定しているポート 0/1 に認証サーバからの応答待ち時間を 300 秒に設定します。

(7) 複数端末から認証要求時の通信遮断時間の設定

ポート単位認証のシングルモードが動作しているポートで，複数の端末からの認証要求を検出した場合に，そのポートでの通信を遮断する時間を設定します。

[設定のポイント]

該当ポートで複数の端末から認証要求を検出したときに，ポートの通信を遮断する時間を設定してください。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 0/1**
   (config-if)# dot1x timeout keep-unauth 1800
   (config-if)# exit
   ポート単位認証を設定しているポート 0/1 に通信遮断状態の時間を 1800 秒に設定します。

(8) 自動認証解除条件の設定

(a) 認証済み端末の無通信監視機能の設定

ポート単位認証（静的）またはポート単位認証（動的）が有効なとき，コンフィグレーションコマンド dot1x auto-logout を設定しなくても本機能は有効となります。ポート単位認証（静的）では，検疫および認証済み端末に対して無通信監視を実施します。

なお，コンフィグレーションコマンドで no dot1x auto-logout を設定すると，自動で認証解除しません。

(b) MAC アドレステーブルエージング監視の設定

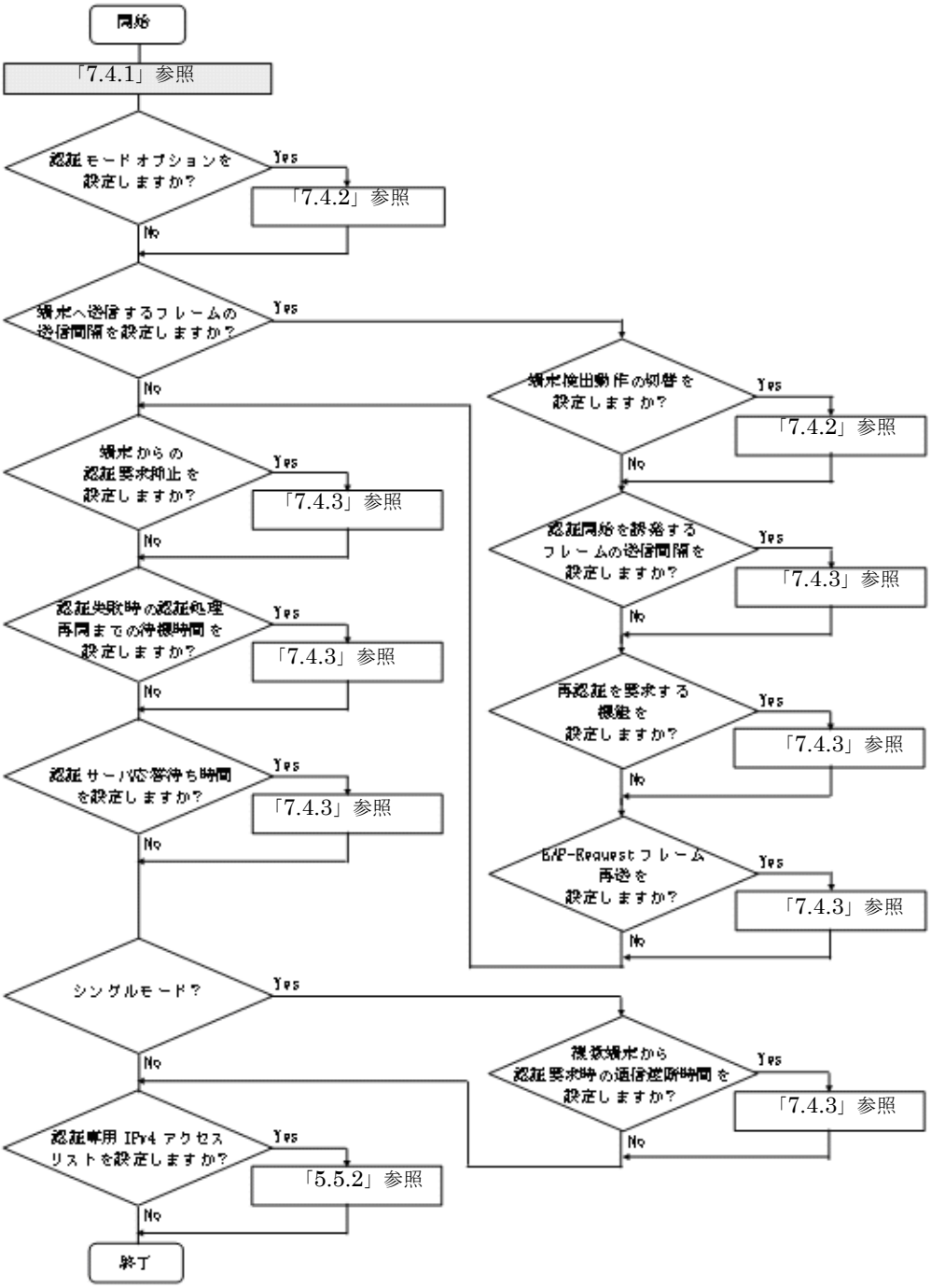
ポート単位認証（静的）が有効なとき，コンフィグレーションコマンド dot1x auto-logout を設定しなくても本機能は有効となります。ポート単位認証（静的）では，検疫状態端末に対して MAC アドレステーブルエージング監視を実施します。

なお，コンフィグレーションコマンドで no dot1x auto-logout を設定すると，自動で認証解除しません。

7.4　ポート単位認証（動的）のコンフィグレーション

「7.1　IEEE802.1X のコンフィグレーション」および「7.2　全認証モード共通のコンフィグレーション」に記載の設定をしたうえで，次の図の手順に従ってポート単位認証（動的）のコンフィグレーションを設定してください。

図 7-5　ポート単位認証（動的）の設定手順



各設定の詳細は，下記を参照してください。

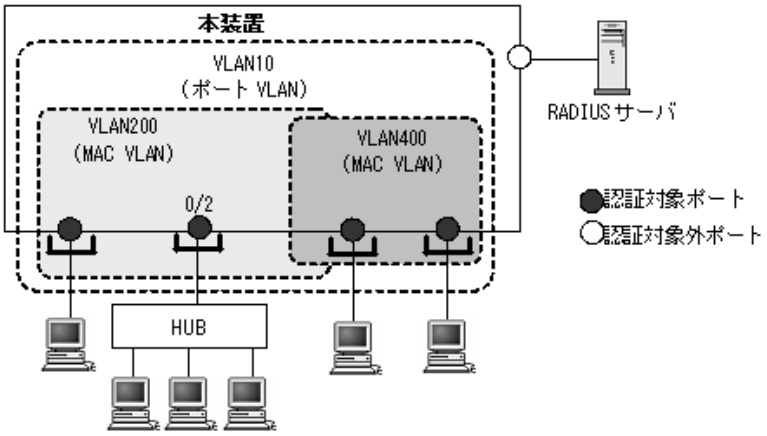
1. ポート単位認証（動的）の設定：「7.4.1　ポート単位認証（動的）の設定」
2. 認証モードオプションの設定：「7.4.2　認証モードオプションの設定」
3. 端末へ送信するフレームの送信間隔の設定
   - 端末検出動作切り替えの設定：「7.4.2　認証モードオプションの設定（2）端末検出動作の切替設定」
   - 認証開始を誘発するフレームの送信制御：「7.4.3　認証処理に関する設定（1）端末へ認証開始を誘発するフレームの送信間隔の設定」
   - 再認証を要求する機能：「7.4.3　認証処理に関する設定（2）端末へ再認証を要求する機能の設定」
   - EAP-Request フレーム再送：「7.4.3　認証処理に関する設定（3）端末へ EAP-Request フレーム再送の設定」
4. 端末からの認証抑止の設定：「7.4.3　認証処理に関する設定（4）端末からの認証要求を抑止する機能の設定」
5. 認証失敗時の認証処理再開までの待機時間設定：「7.4.3　認証処理に関する設定（5）認証失敗時の認証処理再開までの待機時間設定」
6. 認証サーバ応答待ち時間の設定：「7.4.3　認証処理に関する設定（6）認証サーバ応答待ち時間のタイマ設定」
7. 複数端末からの認証要求時の通信遮断時間の設定：「7.4.3　認証処理に関する設定（7）複数端末から認証要求時の通信遮断時間の設定」
8. 認証専用 IPv4 アクセスリストの設定：「5.5.2　認証専用 IPv4 アクセスリストの設定」

7.4.1　ポート単位認証（動的）の設定

（1） 認証ポートと認証用 VLAN 情報の設定

物理ポートまたはチャネルグループを認証の対象に設定します。

図 7-6　ポート単位認証（動的）の構成例



［設定のポイント］

MAC VLAN と MAC ポートを設定し，そのポートでポート単位認証（動的）を有効にします。認証サブモードを設定します。認証サブモードの設定を省略するとシングルモードになります。
なお，認証ポートの認証後 VLAN は，「5.4.3　MAC VLAN の自動 VLAN 割当」により割り当てられるものとします。

［コマンドによる設定］

1. **(config)# vlan 200,400 mac-based**
   (config-vlan)# exit

VLAN ID 200，400 に MAC VLAN を設定します。

2. **(config)# vlan 10**
   (config-vlan)# exit
   VLAN ID 10 を設定します。

3. **(config)# interface gigabitethernet 0/2**
   (config-if)# switchport mode mac-vlan
   (config-if)# switchport mac native vlan 10
   認証を行う端末が接続されているポート 0/2 を MAC ポートとして設定し，認証前 VLAN10 を設定します。（認証後 VLAN は「5.4.3　MAC VLAN の自動 VLAN 割当」により割り当てられます。）

4. **(config-if)# dot1x multiple-authentication**
   認証サブモードを端末認証モードに設定します。

5. **(config-if)# dot1x port-control auto**
   (config-if)# exit
   ポート単位認証（動的）を有効にします。

（2） ポート別認証方式の認証方式リスト名の設定

［設定のポイント］

ポート別認証方式の認証方式リスト名を設定します。
認証方式リストの設定は前述の「7.2.1　認証方式グループと RADIUS サーバ情報の設定（1）認証方式グループの設定」を参照してください。

［コマンドによる設定］

1. **(config)# interface gigabitethernet 0/2**
   (config-if)# dot1x authentication DOT1X-list1
   (config-if)# exit
   ポート 0/2 に認証方式リスト名 "DOT1X-list1" を設定します。

［注意事項］

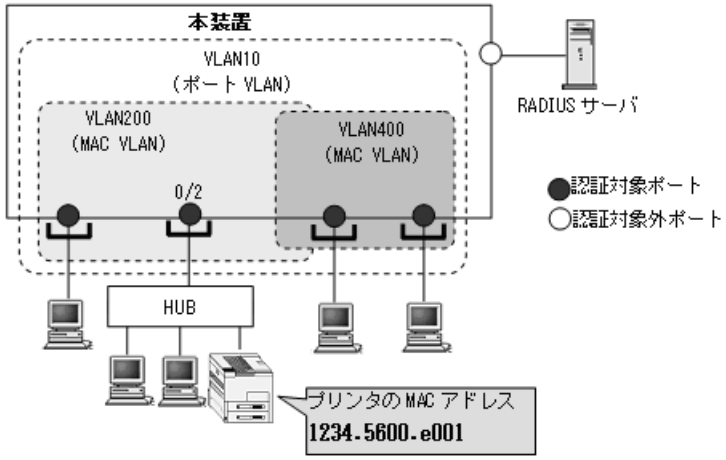
- 本情報未設定時は，「7.2.1　認証方式グループと RADIUS サーバ情報の設定（1）認証方式グループの設定」の装置デフォルトに従って認証します。
- ポートに設定した認証方式リスト名と，認証方式グループの認証方式リスト名が不一致，または認証方式グループに存在しないときは，装置デフォルトに従って認証します。
- Web 認証のユーザ ID 別認証方式は併用設定できません。詳細は「5.2.2　認証方式リスト」を参照してください。

7.4.2　認証モードオプションの設定

（1） 認証除外オプションの設定

IEEE802.1X を持たない端末など，認証を行わないで通信を許可する端末の MAC アドレスを設定します。本例では，「7.4.1　ポート単位認証（動的）の設定」で設定したポート 0/2 に，認証しないで通信するプリンタ（MAC アドレス：1234.5600.e001）を接続します。

図 7-7 ポート単位認証（動的）の認証除外の構成例



[設定のポイント]

ポート単位認証（動的）では，MAC アドレステーブルと MAC VLAN にスタティックエントリを登録します。

[コマンドによる設定]

1. **(config)# vlan 200 mac-based**
   (config-vlan)# mac-address 1234.5600.e001
   (config-vlan)# exit
   VLAN ID 200 に通信可能とする MAC アドレス (1234.5600.e001) を設定します。プリンタは，IEEE802.1X の認証を行わないで VLAN ID 200 で通信できます。

2. **(config)# interface gigabitethernet 0/2**
   (config-if)# switchport mode mac-vlan
   (config-if)# switchport mac vlan 200
   (config-if)# exit
   認証ポートに除外端末が属する MAC VLAN ID 200 を設定します。

3. **(config)# mac-address-table static 1234.5600.e001 vlan 200 interface gigabitethernet 0/2**
   ポート 0/2 の VLAN ID 200 に認証しないで通信させたい MAC アドレス (1234.5600.e001) を MAC アドレステーブルに設定します。

[注意事項]

MAC アドレステーブルに認証除外端末の MAC アドレスを設定する前に，除外端末が所属するポートに MAC VLAN の VLAN ID を設定してください。

(2) 端末検出動作の切替設定

ポート単位認証（静的）と同様です。「7.3.2 認証モードオプションの設定（2）端末検出動作の切替設定」を参照してください。

7.4.3　認証処理に関する設定

（1） 端末へ認証開始を誘発するフレームの送信間隔の設定

ポート単位認証（静的）と同様です。「7.3.3　認証処理に関する設定（1）端末へ認証開始を誘発するフレームの送信間隔の設定」を参照してください。

（2） 端末へ再認証を要求する機能の設定

ポート単位認証（静的）と同様です。「7.3.3　認証処理に関する設定（2）端末へ再認証を要求する機能の設定」を参照してください。

（3） 端末へ EAP-Request フレーム再送の設定

ポート単位認証（静的）と同様です。「7.3.3　認証処理に関する設定（3）端末へ EAP-Request フレーム再送の設定」を参照してください。

（4） 端末からの認証要求を抑止する機能の設定

ポート単位認証（静的）と同様です。「7.3.3　認証処理に関する設定（4）端末からの認証要求を抑止する機能の設定」を参照してください。

（5） 認証失敗時の認証処理再開までの待機時間設定

ポート単位認証（静的）と同様です。「7.3.3　認証処理に関する設定（5）認証失敗時の認証処理再開までの待機時間設定」を参照してください。

（6） 認証サーバ応答待ち時間のタイマ設定

ポート単位認証（静的）と同様です。「7.3.3　認証処理に関する設定（6）認証サーバ応答待ち時間のタイマ設定」を参照してください。

（7） 複数端末から認証要求時の通信遮断時間の設定

ポート単位認証（静的）と同様です。「7.3.3　認証処理に関する設定（7）複数端末から認証要求時の通信遮断時間の設定」を参照してください。

（8） 自動認証解除条件の設定

(a) 認証済み端末の無通信監視機能の設定

認証済み端末が解除対象で，無通信監視設定ポート単位認証（静的）と同様です。「7.3.3　認証処理に関する設定（8）自動認証解除条件の設定（a）認証済み端末の無通信監視機能の設定」を参照してください。

7.5　IEEE802.1X のオペレーション

7.5.1　運用コマンド一覧

IEEE802.1X の運用コマンド一覧を次の表に示します。

表 7-3　運用コマンド一覧

コマンド名	説明
show dot1x	認証単位ごとの状態や認証済みの Supplicant 情報を表示します。
show dot1x logging	IEEE802.1X 認証で採取している動作ログメッセージを表示します。
show dot1x statistics	IEEE802.1X 認証にかかわる統計情報を表示します。
clear dot1x auth-state	認証済みの端末情報をクリアします。
clear dot1x logging	IEEE802.1X 認証で採取している動作ログメッセージをクリアします。
clear dot1x statistics	IEEE802.1X 認証にかかわる統計情報を 0 にクリアします。
reauthenticate dot1x	IEEE802.1X 認証状態を再認証します。

7.5.2　IEEE802.1X 状態の表示

（1） 認証状態の表示

IEEE802.1X の状態は運用コマンド show dot1x で確認してください。

（a） 装置全体の状態表示

IEEE802.1X の装置全体表示は，運用コマンド show dot1x を実行して確認してください。

図 7-8　show dot1x の実行結果

```
> show dot1x

Date 20XX/05/20 17:05:03 UTC
System 802.1X : Enable
   AAA Authentication Dot1x   : Enable
       Accounting Dot1x       : Enable
                  Auto-logout  : Enable

Authentication Default     : RADIUS
Authentication dot1x_auth1 : RADIUS dot1x_auth1
Accounting Default         : RADIUS

Port/ChGr          AccessControl  PortControl        Status        Supplicants
Port 0/4           Multiple-Auth  Auto               ---           1
Port 0/5           Multiple-Auth  Auto               ---           0
Port 0/6(Dynamic)  Multiple-Auth  Auto               ---           0
ChGr 64            Multiple-Auth  Auto               ---           0

>
```

（b） ポート単位認証（静的）の状態表示

ポート単位認証（静的）におけるポートごとの状態情報は，運用コマンド show dot1x port を実行して確認してください。チャネルグループごとの状態は運用コマンド show dot1x channel-group-number を実行して確認してください。

- ポート番号を指定すると，指定したポートの情報を表示します。

- detail パラメータを指定すると，認証対象端末の情報を表示します。

ポート番号と detail パラメータを指定時の表示例を次の図に示します。

図 7-9 show dot1x port（detail パラメータ指定時）の実行結果

```
> show dot1x port 0/4 detail

Date 20XX/05/20 17:10:21 UTC
Port 0/4
AccessControl  : Multiple-Auth             PortControl    : Auto
Status         : ---                       Last EAPOL     : 000a.e460.af39
Supplicants    : 1 / 1 / 1024              ReAuthMode     : Enable
TxTimer        : 300                       ReAuthTimer    : 300
ReAuthSuccess  : 1                         ReAuthFail     : 0
SuppDetection  : Auto
VLAN(s): 200

 Supplicants MAC  F  Status         AuthState      BackEndState   ReAuthSuccess
                     SessionTime(s) Date/Time                     SubState
Class
 [VLAN 200]          Port(Static)  Supplicants : 1
 000a.e460.af39      Authorized     Authenticated  Idle           1
                     192            20XX/05/20 17:03:36           Full
30

>
```

(c) ポート単位認証（動的）の状態表示

ポート単位認証におけるポートごとの状態情報は，運用コマンド show dot1x port を実行して確認してください。チャネルグループごとの状態は運用コマンド show dot1x channel-group-number を実行して確認してください。

- ポート番号を指定すると，指定したポートの情報を表示します。
- detail パラメータを指定すると，認証対象端末の所属 VLAN および端末情報を表示します。

チャネルグループ番号と detail パラメータを指定時の表示例を次の図に示します。

図 7-10 show dot1x channel-group-number（detail パラメータ指定時）の実行結果

```
> show dot1x channel-group-number 64 detail

Date 20XX/05/20 17:15:21 UTC
ChGr 64 (Dynamic)
AccessControl  : Multiple-Auth             PortControl    : Auto
Status         : ---                       Last EAPOL     : 0013.20a5.3e50
Supplicants    : 1 / 1 / 1024              ReAuthMode     : Disable
TxTimer        : 30                        ReAuthTimer    : 3600
ReAuthSuccess  : 1                         ReAuthFail     : 0
SuppDetection  : Auto
Authentication : port-list-DDD
VLAN(s): 40

 Supplicants MAC  F  Status         AuthState      BackEndState   ReAuthSuccess
                     SessionTime(s) Date/Time                     SubState
Class
 [VLAN 40]           Port(Dynamic)  Supplicants : 1
 0013.20a5.3e50      Authorized     Authenticated  Idle           1
                     435            20XX/05/20 17:03:45           Full
30

>
```

7.5.3 IEEE802.1X 認証状態の変更

（1） 認証状態の初期化

認証状態の初期化を行うには，運用コマンド clear dot1x auth-state を使用します。ポート番号，VLAN ID，端末の MAC アドレスのどれかを指定できます。何も指定しなかった場合は，すべての認証状態を初期化します。

コマンドを実行した場合，再認証を行うまで通信ができなくなるので注意してください。

図 7-11 装置内すべての IEEE802.1X 認証状態を初期化する実行例

```
> clear dot1x auth-state
Do you wish to initialize all 802.1X authentication information? (y/n):y
```

（2） 強制的な再認証

強制的に再認証を行うには，運用コマンド reauthenticate dot1x を使用します。ポート番号，VLAN ID，端末の MAC アドレスのどれかを指定できます。指定がない場合は，すべての認証済み端末に対して再認証を行います。

コマンドを実行しても，再認証に成功した Supplicant の通信に影響はありません。

図 7-12 装置内すべての IEEE802.1X 認証ポート，VLAN で再認証する実行例

```
> reauthenticate dot1x
Do you wish to reauthenticate all 802.1X ports and VLANs? (y/n):y
```

8 Web 認証の解説

Web 認証は，汎用 Web ブラウザを用いて認証されたユーザ単位に VLAN へのアクセス制御を行う機能です。この章では Web 認証の概要について説明します。

8.1 概要

Web 認証は，Internet Explorer などの汎用の Web ブラウザ（以降，単に Web ブラウザと表記）を利用しユーザ ID およびパスワードを使った認証によってユーザを認証し，このユーザが使用する端末の MAC アドレスを使用して認証状態に移行させて，認証後のネットワークへのアクセスを可能にします。

本機能によって，端末側に特別なソフトウェアをインストールすることなく，Web ブラウザだけで認証ができます。

(1) 認証モード

Web 認証には次に示す認証モードがあります。

- 固定 VLAN モード
  認証が成功した端末の MAC アドレスを MAC アドレステーブルに登録し，コンフィグレーションで指定された VLAN への通信を可能とします。
- ダイナミック VLAN モード
  認証が成功した端末の MAC アドレスを，MAC VLAN と MAC アドレステーブルに登録して，認証前のネットワークと認証後のネットワークを分離します。

(2) 認証方式グループ

Web 認証では，次に示す認証方式グループを設定できます。（設定した認証方式グループは，Web 認証の全認証モードで使用できます。）

- 装置デフォルト：ローカル認証方式
  本装置に内蔵した認証用 DB（内蔵 Web 認証 DB と呼びます）で認証する方式です。
- 装置デフォルト：RADIUS 認証方式
  ネットワーク内に設置した RADIUS サーバを用いて認証する方式です。
- 認証方式リスト
  特定条件に合致した際に，認証方式リストに登録した任意の RADIUS サーバグループを用いて認証する方式です。

(3) 認証ネットワーク

本装置の Web 認証は IPv4 アドレスだけに対応しています。認証の対象となる端末を収容する VLAN インタフェースには，IPv4 アドレスを設定してください。ただし，RADIUS サーバの設定では，IPv4 アドレスまたは IPv6 アドレスのどちらでも指定できます。

(4) 各認証モードのサポート機能

各認証モードのサポート機能を下記に示します。

表 8-1 各認証モードのサポート機能一覧

機能		固定 VLAN	ダイナミック VLAN
装置デフォルト： ローカル認証	内蔵 Web 認証 DB	○ 「8.2.1」参照 「8.5.1」参照	○ 「8.3.1」参照 「8.5.1」参照
	ユーザ ID	1 ～ 128 文字 「9.5.2」参照	1 ～ 128 文字 「9.5.2」参照
	パスワード	1 ～ 32 文字 「9.5.2」参照	1 ～ 32 文字 「9.5.2」参照
	VLAN（認証後の VLAN）	○ 「9.5.2」参照	○ 「9.5.2」参照
装置デフォルト： RADIUS 認証	外部サーバ • Web 認証専用 RADIUS サーバ情報 • 汎用 RADIUS サーバ情報	○ 「5.3.1」参照 「8.2.1」参照 「8.5.2」参照 「9.2.1」参照	○ 「5.3.1」参照 「8.3.1」参照 「8.5.2」参照 「9.2.1」参照
	ユーザ ID	1 ～ 128 文字 「8.2.1」参照 「8.5.2」参照	1 ～ 128 文字 「8.3.1」参照 「8.5.2」参照
	パスワード	1 ～ 32 文字 「8.2.1」参照 「8.5.2」参照	1 ～ 32 文字 「8.3.1」参照 「8.5.2」参照
	VLAN （認証後の VLAN）	○ 「8.2.1」参照 「8.5.2」参照	○ 「8.3.1」参照 「8.5.2」参照
	強制認証	○ 「5.4.6」参照	○ 「5.4.6」参照
	認証許可ポート設定	○ 「5.5.4」参照	○ 「5.5.4」参照
	プライベートトラップ	○ 「5.4.6」参照	○ 「5.4.6」参照
認証方式リスト	外部サーバ • RADIUS サーバグループ情報	○ 「5.3.1」参照 「8.2.1」参照 「8.5.2」参照 「9.2.1」参照	○ 「5.3.1」参照 「8.3.1」参照 「8.5.2」参照 「9.2.1」参照
	ポート別認証方式	○ 「5.2.2」参照 「5.2.3」参照	○ 「5.2.2」参照 「5.2.3」参照
	ユーザ ID 別認証方式	○ 「5.2.2」参照 「5.2.3」参照	○ 「5.2.2」参照 「5.2.3」参照
端末 IP アドレス配布	内蔵 DHCP サーバ※	○	○
認証数制限	ポート単位	1024 「5.4.8」参照 「5.5.5」参照	1000 「5.4.8」参照 「5.5.5」参照
	装置単位	1024 「5.4.8」参照 「5.5.5」参照	1000 「5.4.8」参照 「5.5.5」参照

機能		固定 VLAN	ダイナミック VLAN
ログイン	Web 認証専用 IP アドレス	○ 「8.2.2」参照 「9.2.2」参照	○ 「8.3.2」参照 「9.2.2」参照
	認証前通過（認証専用 IPv4 アクセスリスト）	○ 「5.4.1」参照 「5.5.2」参照	○ 「5.4.1」参照 「5.5.2」参照
	URL リダイレクト機能	○ 「8.2.2」参照 「9.3.2」参照	○ 「8.3.2」参照 「9.4.2」参照
	URL リダイレクトトリガパケットの TCP ポート指定	○ 「8.2.2」参照 「9.3.2」参照	○ 「8.3.2」参照 「9.4.2」参照
	ログイン画面プロトコル指定	○ 「8.2.2」参照 「9.3.2」参照	○ 「8.3.2」参照 「9.4.2」参照
	HTTPS リクエストの URL リダイレクト抑止指定	○ 「8.2.2」参照 「9.3.2」参照	○ 「8.3.2」参照 「9.4.2」参照
	外部 Web サーバリダイレクト機能	○ 「8.2.2」参照 「9.3.2」参照	○ 「8.3.2」参照 「9.4.2」参照
	認証成功後の URL 自動表示	○ 「8.2.2」参照 「9.3.2」参照	○ 「8.3.2」参照 「9.4.2」参照
	ユーザ切替オプション	○ 「8.2.2」参照 「9.2.6」参照	○ 「8.3.2」参照 「9.2.6」参照
	Web 認証プレフィルタ	○ 「8.2.2」参照	○ 「8.3.2」参照
	HTTP サーバの初期タイムアウト時間の変更	○ 「8.2.2」参照	○ 「8.3.2」参照
ログアウト	最大接続時間超過	○ 「8.2.2」参照 「9.2.3」参照	○ 「8.3.2」参照 「9.2.3」参照
	認証済み端末の無通信監視	○ 「8.2.2」参照 「9.3.2」参照	○ 「8.3.2」参照 「9.4.2」参照
	認証済み端末の接続監視機能	○ 「8.2.2」参照 「9.3.2」参照	×
	認証済み端末からの特殊フレーム受信	○ 「8.2.2」参照 「9.2.3」参照	○ 「8.3.2」参照 「9.2.3」参照
	認証端末接続ポートのリンクダウン	○ 「8.2.2」参照	○ 「8.3.2」参照
	VLAN 設定変更	○ 「8.2.2」参照	○ 「8.3.2」参照
	Web 画面操作	○ 「9.5.12」参照	○ 「9.5.12」参照

機能		固定 VLAN	ダイナミック VLAN
	運用コマンド	○ 「8.2.2」参照	○ 「8.3.2」参照
ローミング（認証済み端末のポート移動）	ポート移動許可設定	○ 「8.2.2」参照 「9.3.2」参照	○ 「8.3.2」参照 「9.4.2」参照
	プライベートトラップ	○ 「8.4」参照	○ 「8.4」参照
アカウントログ	本装置内蔵アカウントログ	「8.4」参照	
	RADIUS サーバのアカウント機能	全モード共通 「5.3.4」参照 「8.4」参照 「9.2.4」参照	
Web 認証画面	Web 認証画面入れ替え	全モード共通 「8.8」参照 「9.5.8」参照	
	ポートごとの個別 Web 認証画面指定	○ 「8.2.2」参照 「9.3.2」参照	○ 「8.3.2」参照 「9.4.2」参照

（凡例）

○：サポート

×：未サポート

「5. x . x 」参照：「5　レイヤ 2 認証機能の概説」の参照先番号

「8. x . x 」参照：本章の参照先番号

「9. x . x 」参照：「9　Web 認証の設定と運用」の参照先番号

注 ※

本装置の内蔵 DHCP サーバについては，「コンフィグレーションガイド Vol.1 31　DHCP サーバ機能」を参照してください。

Web 認証の動作条件を次の表に示します。

表 8-2　Web 認証の動作条件

種別		ポートの設定	設定可能な VLAN 種別	フレーム種別	固定 VLAN モード	ダイナミック VLAN モード
ポートの種類	アクセスポート	native	ポート VLAN MAC VLAN	Untagged	○	×
	トランクポート	native	ポート VLAN MAC VLAN	Untagged	○	×
		allowed	ポート VLAN MAC VLAN	Tagged	○	×
	プロトコルポート	－	－	－	×	×
	MAC ポート	native	ポート VLAN	Untagged	○※	×
		mac	MAC VLAN	Untagged	×	○
		dot1q	ポート VLAN MAC VLAN	Tagged	○	×
デフォルト VLAN					○	×

種別		ポートの設定	設定可能な VLAN 種別	フレーム種別	固定 VLAN モード	ダイナミック VLAN モード
インタフェース種別	gigabitethernet				○	○
	port channel				○	○

（凡例）
○：動作可
×：動作不可
－：認証ポートでは，設定対象外

注 ※
詳細は「5.4.4　同一 MAC ポートでの自動認証モード収容」を参照してください。

本装置の Web 認証では，チャネルグループについても一つの束ねられたポートとして扱います。この機能での「ポート」の表現には通常のポートとチャネルグループを含むものとします。

次項からは，「固定 VLAN モード」「ダイナミック VLAN モード」の順に各認証モードの概要を説明します。各認証モードで同じ機能で同一動作については，「～を参照してください。」としていますので，該当箇所を参照してください。

8.2 固定 VLAN モード

認証前の端末は，認証が成功するまで通信できません。固定 VLAN モードで認証が成功すると，MAC アドレステーブルに端末の MAC アドレスと VLAN ID が Web 認証エントリとして登録されて通信可能になります。(MAC アドレステーブルの登録状態は，運用コマンド show mac-address-table で確認できます。)

ログイン操作にあたっては，Web 認証専用の IP アドレスを使用する方法と，URL リダイレクト機能を使用する方法があります。どちらの場合も，「8.2.1　認証方式グループ」の認証方式で認証できます。このため，Web 認証専用 IP アドレスと URL リダイレクトの両方，またはどちらかを必ず設定してください。

8.2.1 認証方式グループ

Web 認証の認証方式グループは，装置デフォルトと認証方式リストを Web 認証の全認証モード共通で使用します。下記も合わせて参照してください。

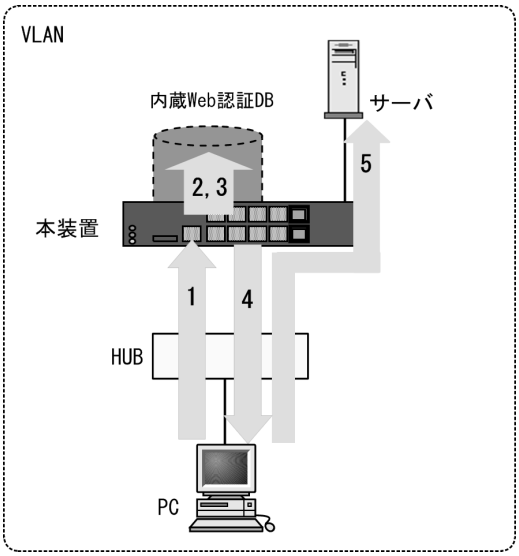
- 「5.1.3　認証方式グループ」
- 「5.3.3　装置デフォルトのローカル認証と RADIUS 認証の優先設定」
- 「5.2.2　認証方式リスト」
- 「5.3.1　レイヤ 2 認証機能で使用する RADIUS サーバ情報」
- 「9.2.1　認証方式グループと RADIUS サーバ情報の設定」

(1) 装置デフォルト：ローカル認証

認証対象ユーザからのユーザ ID およびパスワードで内蔵 Web 認証 DB を検索し，認証可否を判定します。

ローカル認証方式の認証動作を次の図に示します。

図 8-1　固定 VLAN モード概要図（ローカル認証方式）



1. HUB 経由で接続された PC から Web ブラウザを起動し，Web 認証専用 IP アドレスで本装置にアクセスします。
2. 内蔵 Web 認証 DB 検索時に，認証対象ユーザ（図内の PC）の接続ポートまたは VLAN ID により，認証対象ユーザが所属する VLAN ID を特定します。

3. ユーザ ID およびパスワードに VLAN ID 情報を加えて内蔵 Web 認証 DB を検索することで，収容可能な VLAN を制限することが可能となります。
4. 認証成功であれば，ログイン成功画面を PC に表示します。
5. 認証済み PC は，接続された VLAN のサーバに接続できるようになります。

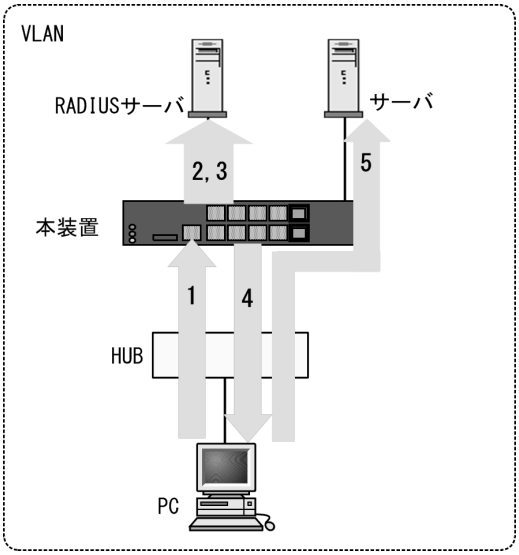
(a) VLAN 制限

認証対象ユーザの接続ポートから VLAN ID を抽出し，この VLAN ID を合わせて内蔵 Web 認証 DB を検索することで特定 VLAN での認証を制限可能としています。

(2) 装置デフォルト：RADIUS 認証

RADIUS 認証方式の動作を次の図に示します。

図 8-2 固定 VLAN モード概要図（RADIUS 認証方式）



1. HUB 経由で接続された PC から Web ブラウザを起動し，指定された URL で本装置にアクセスします。
2. 外部に設置された RADIUS サーバへ認証要求する際に，認証対象ユーザ（図内の PC）の接続ポートまたは VLAN ID により，認証対象ユーザが所属する VLAN ID を特定します。
3. ユーザ ID およびパスワードに VLAN ID 情報を加えて RADIUS サーバへ認証要求することで，収容可能な VLAN を制限することが可能となります。
4. 認証成功であれば，ログイン成功画面を PC に表示します。
5. 認証済み PC は，接続された VLAN のサーバに接続できるようになります。

(a) VLAN 制限

RADIUS 認証においても，ローカル認証と同様の方式を用いて VLAN 情報を取得し，RADIUS サーバへ認証要求する際の RADIUS 属性 "NAS-Identifier" に，取得した VLAN ID 情報 (認証要求時の端末が所属する VLAN ID) を設定して実施します。

RADIUS サーバ設定として，ユーザ ID およびパスワードと共に，認証許可する VLAN 情報 (認証要求時の端末が所属する VLAN ID) を "NAS-Identifier" に設定することで，収容可能な VLAN を制限することができます。

（3） 認証方式リスト

Web 認証では，ポート別認証方式またはユーザ ID 別認証方式を使用できます。ポート別認証方式およびユーザ ID 別認証方式の動作については，「5.2.2　認証方式リスト」を参照してください。

8.2.2　認証機能

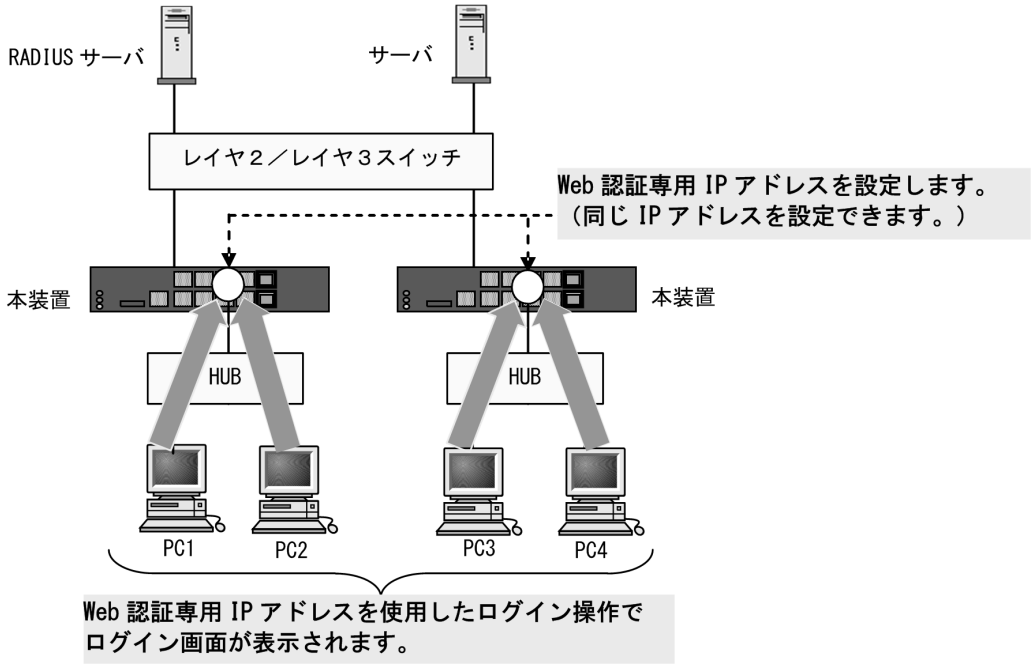
（1） Web 認証専用 IP アドレス

本装置に設定された Web 認証専用の IP アドレスを使用してログイン操作，およびログアウト操作ができます。

Web 認証専用に設定された IP アドレスは，各インタフェースに設定された IP アドレスとは異なり，Web 認証のログイン操作およびログアウト操作だけで使用されます。

Web 認証専用 IP アドレスは，コンフィグレーションコマンド web-authentication ip address で設定できます。

図 8-3　Web 認証専用 IP アドレスによるログイン操作



注意

- Web 認証専用 IP アドレスを使用する場合は，Web 認証の認証前 VLAN に必ず IP アドレスを設定してください。
- Web 認証専用 IP アドレスは，本装置に設定された VLAN インタフェースと重複しないサブネットの IP アドレスを設定してください。

（2） URL リダイレクト機能

認証前の端末から本装置外への HTTP および HTTPS アクセスを検出し，端末の画面に強制的にログイン画面を表示してログイン操作をさせることができます。

また，システム受信モードにより，以下の動作となります。

＜収容条件重視モード＞
認証専用 IPv4 アクセスリストの permit に該当する HTTP/HTTPS パケットは，URL リダイレクト機能の対象外となります。

＜受信条件重視モード＞
認証専用 IPv4 アクセスリストの permit/deny に該当する HTTP/HTTPS パケットは，URL リダイレクト機能の対象外となります。

システム受信モードについては，「コンフィグレーションガイド Vol.1　13　装置の管理」を参照してください。

なお，URL リダイレクトを設定する場合は，認証要求端末が所属する VLAN に IP アドレスを必ず設定してください。

(a) URL リダイレクトトリガパケット TCP ポート番号の追加

URL リダイレクトを実施するトリガパケットは，TCP の宛先ポート番号 =80 と 443 で，コンフィグレーションコマンドで TCP 宛先ポート番号を 1 件だけ追加可能です。設定後も基本の TCP 宛先ポート番号 =80 と 443 は有効です。

追加ポート番号は，コンフィグレーションコマンド web-authentication web-port で設定できます。

(b) ログイン画面プロトコル指定

Web 認証の URL リダイレクト機能使用時に，Web 認証ログイン画面を表示する際のプロトコル (URL) を，"http" または "https" のいずれかをコンフィグレーションで選択できます。未指定の場合は，"https" で表示します。

ログイン画面プロトコルは，コンフィグレーションコマンド web-authentication redirect-mode で設定できます。

(c) HTTPS リクエストの URL リダイレクト抑止指定

認証前の端末から，アプリケーションなどで自動送信される HTTPS リクエストを廃棄し，URL リダイレクトを抑止する機能です。これにより，本装置内に不要なリクエスト処理が滞留されなくなります。また，各認証前端末からの URL リダイレクト対象を HTTP リクエストに限定して，応答することができます。

本機能はコンフィグレーショコマンド web-authentication redirect ignore-https で設定できます。本コマンドによって URL リダイレクトが抑止される HTTPS リクエストは，CPU 受信後に廃棄します。

(3) 外部 Web サーバリダイレクト機能

Web 認証の URL リダイレクト機能使用時に，コンフィグレーションで指定された外部 Web サーバにリダイレクト先を変更します。また，外部 Web サーバへのリダイレクト時に，本装置が保有するクエリ（変数）を外部 Web サーバへ受け渡します。

(a) 自動付加するクエリ

コンフィグレーション設定に従って，リダイレクト先 URL の末尾に次の表に示すクエリを付加することができます。

表 8-3 自動付加するクエリとコマンドパラメータ

クエリ	コマンドパラメータ	備考
本装置のホスト名（hostname コマンド）	switch-hostname	
本装置の装置 MAC アドレス	switch-mac	
本装置の実 IP アドレス	switch-ip	端末の認証前 VLAN の IP アドレス
認証端末の MAC アドレス	client-mac	
認証端末の VLAN 番号	client-vlan	
認証端末の IP アドレス	client-ip	
認証端末が接続されているポート	port	物理ポートに接続されている場合は "port=" チャネルグループのポートに接続されている場合は "channel=" として付与します
リダイレクト前の URL	original-url	[:port] は復元できません

（b） URL リダイレクト先 Web サーバの切り替え機能 (生死監視)

外部 Web サーバの障害と復旧を監視し，障害時は本装置の Web サーバに，復旧時は外部 Web サーバに自動的に切り替え可能です。

監視パケットの送信間隔・障害判定条件・正常回復条件などは，コンフィグレーションで設定可能です。本コンフィグレーション設定状態で起動した直後は，" 正常 " ステータスで動作します。

障害・正常検出条件：

- 障害検出：コンフィグレーションコマンドで指定した回数で連続して「無応答」だった場合に，" 障害 " ステータスに遷移します。
- 正常検出：コンフィグレーションコマンドで指定した回数で連続して「応答」だった場合に，" 正常 " ステータスに遷移します。

なお，" 障害 " ステータス中は，本装置の Web サーバにリダイレクトします。

（4） 認証成功後の自動表示 URL 指定

ログイン成功画面表示後に，端末がアクセスする URL を自動表示するようコンフィグレーションで設定できます。表示する URL を指定，またはリダイレクト前の URL へジャンプする指定が可能です。

ログイン成功画面表示後に自動表示する URL は，コンフィグレーションコマンド web-authentication jump-url で，設定できます。

（a） 表示する URL を指定

コンフィグレーションコマンド web-authentication jump-url <url> で，あらかじめ URL を指定することで，ログイン成功画面表示後に，指定した URL の画面が表示されます。

Web 認証入れ替え画面機能で，ログイン成功画面ファイル（loginOK.html）を入れ替える場合は，<form> 内に Web 認証固有タグ <!--Redirect_URL--> を記載してください。

（b） リダイレクト前の URL の画面を表示する指定

Web 認証の URL リダイレクト機能使用時に，コンフィグレーションコマンド web-authentication jump-url original と設定することで，ログイン成功画面表示後に，リダイレクト前の URL の画面を表示

することができます。

この場合，端末から当初のアクセス時にリダイレクト前の URL を抽出し，以降は URL を引き継ぎながら認証を完了させます。

1. 本装置の Web サーバを使用する場合

   Web 認証入れ替え画面機能で，下記の画面を入れ替える場合は，<form> 内に Web 認証固有タグ "<!-- Original_URL -->" を記載してください。

   - ログイン画面ファイル（login.html）

   本装置にはデフォルトで当該タグが埋め込まれています。

2. 外部 Web サーバを使用する場合

   下記に示す例のように，認証端末から本装置への POST データに original_url=xxx※ が含まれるようにしてください。

   - POST データに original_url=xxx※ を含むための設定例
     外部 Web サーバの PHP などを使用して，外部 Web サーバが認証端末に送信するログイン画面の <form> 内に，<input type=hidded name="original_url" value=xxx※> と記述します。

   注 ※　xxx の値は，自動付加クエリの original-url から取得してください。

なお，Web 認証専用 IP アドレスや本装置の IP アドレスを直接指定して認証を開始した場合は，認証成功後にログイン成功画面だけ表示します。

(5) 強制認証ポート指定

強制認証については，「5.4.6　認証共通の強制認証」を参照してください。

また，強制認証で認証許可した端末は，通常の認証済み端末と同様に後述の「8.2.2　認証機能　(7) 認証状態からのログアウト」により認証状態が解除されます。

(6) 認証数制限

装置単位およびポート単位に認証数の制限が設定できます。詳細は，「5.4.8　認証共通の端末数制限」を参照してください。

(7) 認証状態からのログアウト

固定 VLAN モードでは，ログアウトの手段として下記があります。

- 最大接続時間超過時のログアウト
- 認証済み端末の無通信監視によるログアウト
- 認証済み端末の接続監視機能によるログアウト
- 認証済み端末からの特殊フレーム受信によるログアウト
- 認証端末接続ポートのリンクダウンによるログアウト
- VLAN 設定変更によるログアウト
- Web 画面によるログアウト
- 運用コマンドによるログアウト

(a) 最大接続時間超過時のログアウト

コンフィグレーションコマンドで設定された最大接続時間を超えた場合に，自動的に Web 認証の認証状態をログアウトします。この場合は，端末にログアウト完了画面を表示しません。

認証済みの状態で再ログインを行った場合，ローカル認証（RADIUS 認証使用時は RADIUS 認証）で認

証に成功すると認証時間を延長できます。認証に失敗すると認証時間は延長できません。

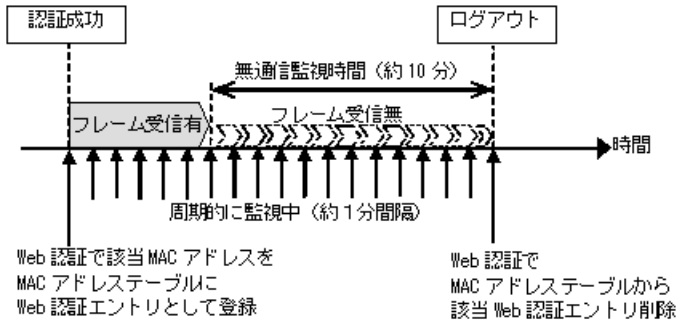
最大接続時間はコンフィグレーションコマンド web-authentication max-timer で設定できます。

(b) 認証済み端末の無通信監視によるログアウト

本機能は，認証済み端末が一定時間無通信だった場合に自動的にログアウトします。

MAC アドレステーブルの Web 認証エントリを周期的（約 1 分間隔）に監視し，Web 認証で登録した認証済み端末からのフレーム受信有無を確認します。該当端末からのフレーム受信を一定時間（約 10 分）検出しなかったときに，MAC アドレステーブルから該当 Web 認証エントリを削除し，認証をログアウトします。

図 8-4 認証済み端末の無通信監視概要



認証済み端末の無通信監視は，下記の条件で動作が有効となります。

- Web 認証固定 VLAN モードまたはダイナミック VLAN モード有効で，web-authentication auto-logout 有効

コンフィグレーションコマンドで no web-authentication auto-logout を設定すると，自動ログアウトしません。

(c) 認証済み端末の接続監視機能によるログアウト

認証済み端末に対し，コンフィグレーションコマンド web-authentication logout polling interval で指定された時間間隔で，ARP リクエストを送信し ARP リプライを受信することによって端末の接続監視を行います。コンフィグレーションコマンド web-authentication logout polling retry-interval と web-authentication logout polling count で設定された時間を超えても ARP リプライが受信できない場合，タイムアウトしていると判断し，自動的に Web 認証の認証状態をログアウトします。この場合には，端末にログアウト完了画面を表示しません。

なお，この機能はコンフィグレーションコマンド no web-authentication logout polling enable で無効にできます。

(d) 認証済み端末からの特殊フレーム受信によるログアウト

認証済み端末から送信された特殊フレームを受信した場合，該当端末の認証をログアウトします。この場合には，端末にログアウト完了画面を表示しません。特殊フレームの条件を次に示します。下記の条件をすべて満たした場合にログアウトします。

- 認証済み端末から Web 認証専用 IP アドレス宛に送信された ping フレームであること
- ping フレームの TTL 値がコンフィグレーションコマンド web-authentication logout ping ttl で設定した TTL 値と一致していること

- ping フレームの TOS 値がコンフィグレーションコマンド web-authentication logout ping tos-windows で設定した TOS 値と一致していること

(e) 認証端末接続ポートのリンクダウンによるログアウト

Web 認証固定 VLAN モード（コンフィグレーションコマンド web-authentication port）が設定されたポートでリンクダウンを検出した際に，当該ポートの Web 認証固定 VLAN モードによる認証済み端末をログアウトします。この場合には，端末にログアウト完了画面を表示しません。

なお，当該ポートにコンフィグレーションコマンド no authentication logout linkdown が設定されている場合は，リンクダウンを検出しても認証済み端末をログアウトしません。詳細は「5.4.10　ポートリンクダウン時の認証解除抑止」「5.5.7　ポートリンクダウン時の認証解除抑止設定」を参照してください。

(f) VLAN 設定変更によるログアウト

コンフィグレーションコマンドで認証端末が含まれる VLAN の設定を変更した場合，変更された VLAN に含まれる端末の認証状態をログアウトします。

[コンフィグレーションの変更内容]
- VLAN を削除した場合
- VLAN を停止（suspend）した場合

(g) Web 画面によるログアウト

端末から Web 認証に成功した URL にアクセスして，端末にログアウト画面を表示させます。画面上の Logout ボタンを押すと，Web 認証の認証状態をログアウトします。

後述の「9.5.12　端末からの認証手順」を参照してください。

(h) 運用コマンドによるログアウト

運用コマンド clear web-authentication auth-state 実行で，Web 認証済みユーザの一部，もしくは全 Web 認証済みユーザを強制的にログアウトします。

(8) ローミング（認証済み端末のポート移動）

HUB などを経由して接続した認証済み端末を，Web 認証設定ポートへリンクダウンしないでポート移動した場合でも，認証済み状態のまま継続して通信可能にします。

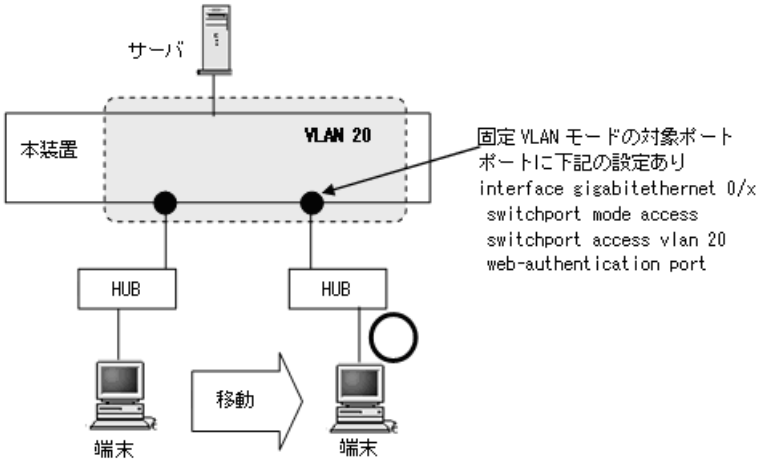
ローミングの動作可能な条件は下記のとおりです。

- コンフィグレーションコマンド web-authentication static-vlan roaming 設定有
- 移動前および移動後が，固定 VLAN モード対象ポート
- 移動前および移動後が，同一 VLAN

上記以外の条件でポート移動を検出したときは，該当端末の認証を強制的にログアウトします。

なお，HUB などを経由して認証済み端末を Web 認証未設定ポートへ移動したときは，該当端末の認証をログアウトしません。Web 認証未設定ポートへ移動したときに認証をログアウトする場合は，コンフィグレーションコマンド authentication auto-logout strayer を設定してください。

図 8-5 固定 VLAN モード ローミング概要図



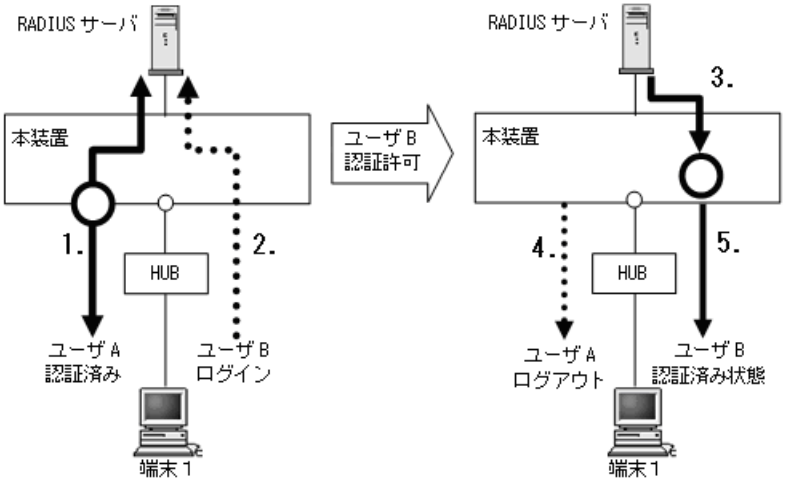
(9) ユーザ切替オプション

本オプションは，特定の端末でユーザが Web 認証でログイン済みのときに，いったんログアウト操作をしなくても，別ユーザ ID によるログインを可能にします。本オプションはコンフィグレーションコマンド web-authentication user replacement の設定で有効になります。

なお，本オプションは，1 台の端末（MAC アドレス）でログアウト操作無しでユーザ ID を切り替える機能であり，同時に複数ユーザでログインできる機能ではありません。

ユーザ切替オプションを設定しているときの動作例を次の図に示します。

図 8-6 ユーザ切替オプション概要図 (RADIUS 認証の例)



1. 特定の端末（図内の端末 1 ）からユーザ A がログインされると，本装置の設定に従った認証方式（RADIUS 認証，ローカル認証）で認証を実施します。（この例ではユーザ A は認証許可となり，認証済みユーザとして管理します。）
2. 認証済み端末（図内の端末 1 ）から別ユーザ ID（図内のユーザ B）でログインされると，本装置の設定に従った認証方式（RADIUS 認証，ローカル認証）で認証を実施します。
3. 認証の結果，新ユーザ（図内のユーザ B）が許可されます。
4. 本装置は旧ユーザ（図内のユーザ A）をログアウトします。

5. 新ユーザを認証済みユーザおよび認証済みとして装置内の管理情報を更新し，新ユーザにログイン成功を通知します。このとき，ログイン日時，残時間は旧ユーザの管理情報から新ユーザの情報に更新されます。

- 新ユーザの収容 VLAN，認証モードについて
  新ユーザの認証許可によって収容される VLAN，認証モードなどは，新ユーザの認証結果に依存します。
- 複数端末で同時にユーザ切り替え実行時
  複数の端末で同時にユーザ切り替えを実施した場合，最大管理ユーザ数は Web 認証の収容条件まで許容します。Web 認証の収容条件については，「コンフィグレーションガイド Vol.1 3.2 収容条件」を参照してください。
- 新ユーザの失敗について
  ユーザ切替に伴う認証中に，当該ポートのリンクダウンなどによるログアウト条件が成立した場合，従来の認証更新中の動作と同様にログアウト条件が成立した全認証端末をログアウトし，新ユーザの認証は失敗します。
  新ユーザの認証が失敗（拒否された）した場合，旧ユーザの認証状態は維持されます。

(a) ユーザ ID 別認証方式設定とユーザ ID 識別について

ユーザ ID 別認証方式設定有無により，ユーザ ID 識別範囲が異なります。ユーザ ID 別認証方式設定時は，入力されたユーザ ID 文字列すべてではなく，RADIUS サーバへ認証要求する「ユーザ ID」が識別範囲となります。（ユーザ ID 別認証方式については，「5.2.2 認証方式リスト」を参照してください。）

ユーザ ID 別認証方式設定有無とユーザ ID 識別範囲例を次の表に示します。

表 8-4 ユーザ ID 別認証方式設定有無とユーザ ID 識別範囲例

ユーザ ID 別認証方式	認証回数	ユーザの入力文字列	ユーザ ID 識別範囲	ユーザ識別結果	ユーザ切り替え動作
設定無	1	userAAA@list111	userAAA@list111	新規ユーザ	―
	2	userAAA@list111	userAAA@list111	同一ユーザ	―
	3	userBBB@list111	userBBB@list111	別ユーザ	○
	4	userBBB@list222	userBBB@list222	別ユーザ	○
設定有	1	userAAA@list111	userAAA	新規ユーザ	―
	2	userAAA@list111	userAAA	同一ユーザ	―
	3	userBBB@list111	userBBB	別ユーザ	○
	4	userBBB@list222	userBBB	同一ユーザ	―

（凡例）
○：動作する
―：動作しない

(b) マルチステップ認証ポートのユーザ切り替え動作

マルチステップ認証ポートの場合は，新ユーザの Web 認証結果（Filter-Id）と，当該端末の旧ユーザで実施した端末認証の認証結果を照合して認証登録可否を判定します。（マルチステップ認証については，後述の「12 マルチステップ認証」を参照してください。）

マルチステップ認証ポートのユーザ切り替え動作を次の表に示します。

表 8-5 マルチステップ認証ポートのユーザ切り替え

マルチステップ認証ポートの設定	旧ユーザの認証				新ユーザの認証	
	端末認証		ユーザ認証		ユーザ認証	
	端末認証種別	認証結果	認証結果	端末の認証管理状態	認証結果	端末の認証管理状態
オプション無	MAC 認証	成功	成功	マルチステップ認証	失敗	旧ユーザのログイン状態
					成功	新ユーザのマルチステップ認証状態
ユーザ許可オプション有	MAC 認証	失敗	成功	シングル認証	失敗	旧ユーザのログイン状態
					成功	旧ユーザのログイン状態 ※1
						新ユーザのシングル認証状態 ※2
		成功	成功	マルチステップ認証	失敗	旧ユーザのログイン状態
					成功	新ユーザのマルチステップ認証状態
端末認証 dot1x オプション有	MAC 認証	成功	成功	マルチステップ認証	失敗	旧ユーザのログイン状態
					成功	新ユーザのマルチステップ認証状態
	IEEE802.1X	成功	成功	マルチステップ認証	失敗	旧ユーザのログイン状態
					成功	新ユーザのマルチステップ認証状態

注 ※1

新ユーザが認証成功でも，端末認証必須ユーザのときは，新ユーザは認証失敗扱いとなり，旧ユーザのログイン状態となります。

注 ※2

新ユーザが認証成功で，端末認証不要ユーザのときは，シングル認証となります。

(10) Web 認証プレフィルタ

本機能は，ファイアウォール回避などを目的として TCP ポート 80（HTTP）を使用するアプリケーションが使われている場合に，Web 認証機能の性能劣化を軽減します。

本機能は初期状態で有効になっています。

Web 認証対象端末によっては，Web 認証プレフィルタとの相性問題が発生する可能性があります。この場合は，コンフィグレーションコマンド no web-authentication prefilter を設定して，本機能を無効にしてください。

(11) HTTP サーバの初期タイムアウト時間の変更

コンフィグレーションコマンド http-server initial-timeout により，HTTP サーバの初期タイムアウト時間を設定します。初期タイムアウトの条件は，HTTP レイヤで 1 オクテットも受信していない状態です。

なお，負荷が高い場合，実際のタイムアウト時間は本コマンドで指定した値より大きくなる可能性があります。

また，初期タイムアウト時間が短すぎる場合，端末の性能によっては，Web 認証が失敗する可能性があります。初期タイムアウト時間の変更後，Web 認証画面が表示されない事象が発生する場合は，初期タイムアウト時間を見直してください。

本機能により指定した初期タイムアウト時間は，OAN を含む全 HTTP/HTTPS リクエストに適用されます。

（12）ポートごとの個別 Web 認証画面

本機能は，登録したカスタムファイルセット (ディレクトリ名) を当該ポートの個別 Web 認証画面として扱い，当該ポートから Web 認証にアクセスされた際に，関連付けされた個別 Web 認証画面を表示する機能です。個別 Web 認証画面をポートに関連付けするときは，コンフィグレーションコマンド web-authentication html-fileset で設定します。

- 未認証端末から「他宛」アクセスがあったとき
  URL リダイレクト機能を用いて，当該ポートに関連付けされた個別 Web 認証画面へリダイレクトさせることができます。
- 当該ポートで URL リダイレクト機能が動作した場合のリダイレクト先 URL
  基本 Web 認証画面も個別 Web 認証画面も共通で http://IP アドレス /login.html となりますが，表示される画面はポートごとに設定したファイルセットとなります。
- 関連付けされていない認証画面ファイルにアクセスしたとき
  個別 Web 認証画面を関連付けされたポートから，関連付けされていない存在する URL，HTML ファイルにアクセスすることはできません。

例えば，特定ポートに検疫サーバへリダイレクトする個別 Web 認証画面ファイルセットを設定しておくと，該当認証ポートから認証画面にアクセスしたユーザに対して検疫サーバで検疫処理後にログインさせ，その他のポートのユーザに対しては通常の Web 認証を実施させるような運用が可能です。

本機能で使用する個別 Web 認証画面は，Web 認証入れ替え画面機能で本装置に登録します。また，本装置に登録するファイルセットをカスタムファイルセットと呼びます。詳細は，「8.8　Web 認証画面入れ替え機能」を参照してください。

8.2.3　認証動作

固定 VLAN モードは以下のシーケンスで認証動作を行います。

図 8-7 認証動作（Web 認証専用 IP アドレス使用時）

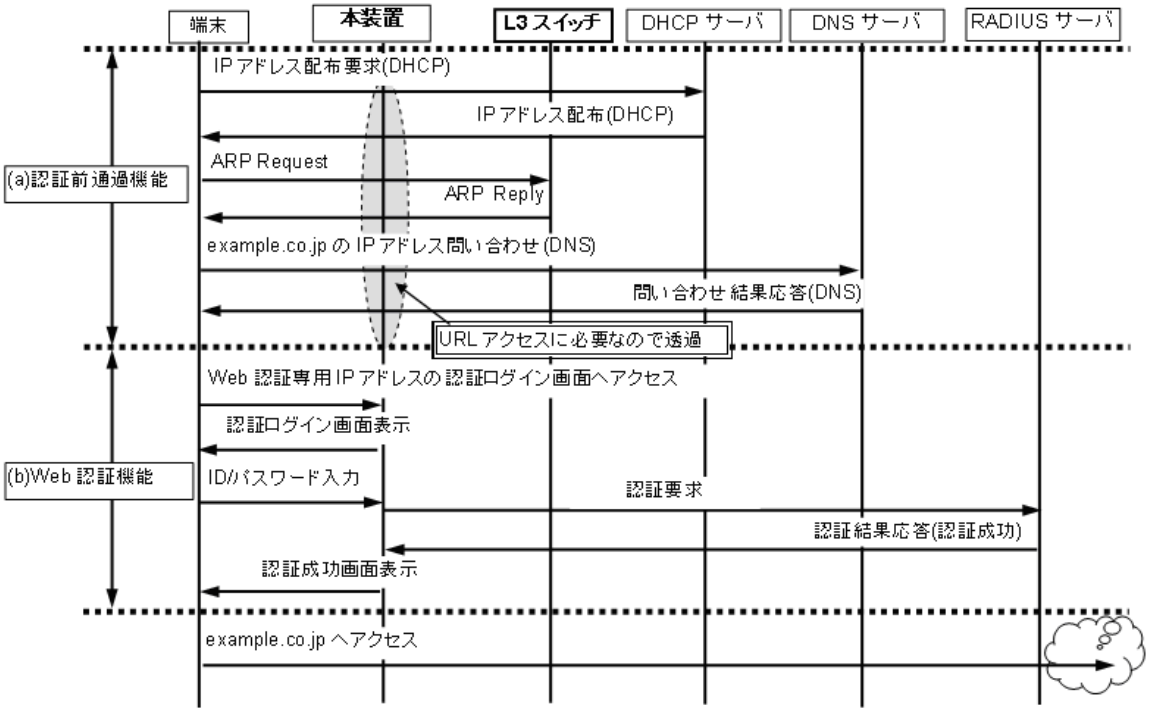
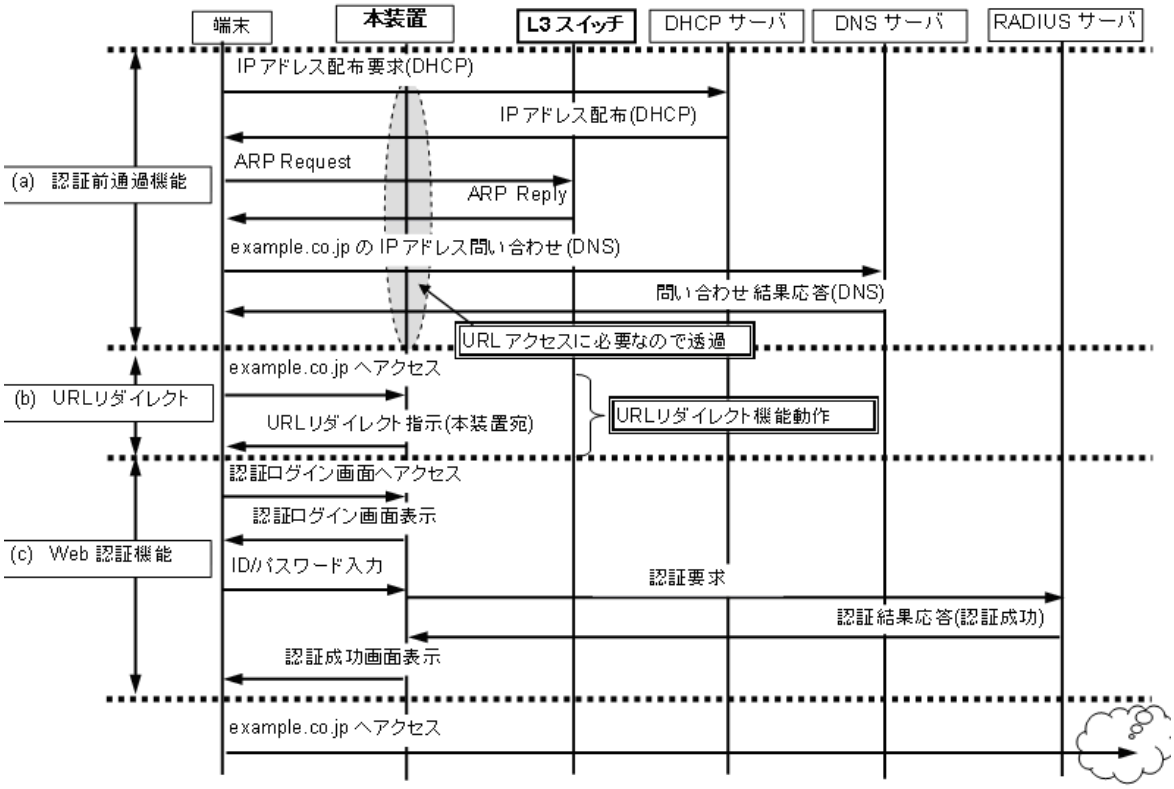


図 8-8 認証動作（URL リダイレクト機能使用時）



8.3 ダイナミック VLAN モード

認証前の端末は，認証が成功するまで通信できません。ダイナミック VLAN モードで認証が成功すると，MAC VLAN と MAC アドレステーブルに端末の MAC アドレスと認証後 VLAN ID が Web 認証エントリとして登録されて，認証後 VLAN 内で通信可能になります。（MAC アドレステーブルの登録状態は , 運用コマンド show mac-address-table で確認できます。）

ダイナミック VLAN モードは，MAC VLAN を設定した物理ポートに設定することで動作します。なお，ダイナミック VLAN モードで認証前 VLAN 内で通信する場合には，認証専用 IPv4 アクセスリストを設定してください。

ログイン操作に当たっては，URL リダイレクト機能を使用する方法と，Web 認証専用 IP アドレスを使用する方法があります。どちらの場合も，「8.3.1　認証方式グループ」の認証方式で認証できます。

8.3.1 認証方式グループ

Web 認証の認証方式グループは，装置デフォルトと認証方式リストを Web 認証の全認証モード共通で使用します。下記も合わせて参照してください。

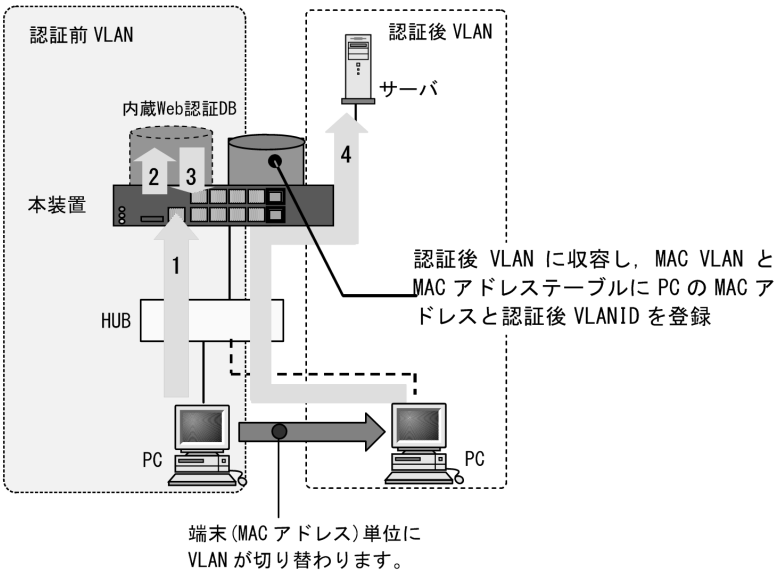
- 「5.1.3　認証方式グループ」
- 「5.3.3　装置デフォルトのローカル認証と RADIUS 認証の優先設定」
- 「5.2.2　認証方式リスト」
- 「5.3.1　レイヤ 2 認証機能で使用する RADIUS サーバ情報」
- 「9.2.1　認証方式グループと RADIUS サーバ情報の設定」

(1) 装置デフォルト：ローカル認証

認証対象ユーザからのユーザ ID およびパスワードで内蔵 Web 認証 DB を検索し，登録内容との照合で認証可否を判定します。一致した場合は，内蔵 Web 認証 DB に登録されている VLAN に収容し通信を許可します。

ローカル認証方式の認証動作を次の図に示します。

図 8-9　ダイナミック VLAN モード概要図（ローカル認証方式）



1. HUB 経由で接続された PC から Web ブラウザを起動し，指定された URL で本装置にアクセスします。
2. 内蔵 Web 認証 DB に従ってユーザ ID およびパスワードによる認証を行います。
3. 認証成功であれば，ログイン成功画面を PC に表示します。
4. 認証済み PC は認証後の VLAN に収容され，サーバに接続できるようになります。また，認証済み PC の MAC アドレスと VLAN ID を，MAC VLAN と MAC アドレステーブルに登録します。

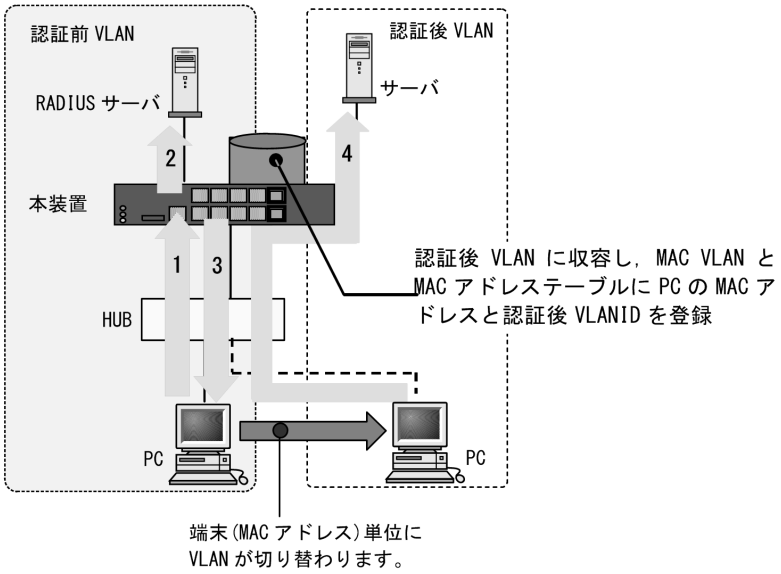
(a) 認証後 VLAN への収容条件

「5.4.3　MAC VLAN の自動 VLAN 割当」「5.4.4　同一 MAC ポートでの自動認証モード収容」を参照してください。

(2) 装置デフォルト：RADIUS 認証

RADIUS 認証方式の動作を次の図に示します。

図 8-10　ダイナミック VLAN モード概要図（RADIUS 認証方式）



1. HUB 経由で接続された PC から Web ブラウザを起動し，指定された URL で本装置にアクセスします。
2. 外部に設置された RADIUS サーバに従って，ユーザ ID およびパスワードによる認証を行います。
3. 認証成功であれば，ログイン成功画面を PC に表示します。
4. RADIUS サーバから送られる VLAN ID 情報に従って，認証済み PC は認証後の VLAN に収容され，サーバに接続できるようになります。また，認証済み PC の MAC アドレスと VLAN ID を，MAC VLAN と MAC アドレステーブルに登録します。

(a) 認証後 VLAN への収容条件

「5.4.3　MAC VLAN の自動 VLAN 割当」「5.4.4　同一 MAC ポートでの自動認証モード収容」を参照してください。

(3) 認証方式リスト

Web 認証では，ポート別認証方式またはユーザ ID 別認証方式を使用できます。ポート別認証方式およびユーザ ID 別認証方式の動作については，「5.2.2　認証方式リスト」を参照してください。

8.3.2 認証機能

(1) Web 認証専用 IP アドレス

固定 VLAN モードと同様です。「8.2.2 認証機能 (1) Web 認証専用 IP アドレス」を参照してください。

(2) URL リダイレクト機能

固定 VLAN モードと同様です。「8.2.2 認証機能 (2) URL リダイレクト機能」を参照してください。

(3) 外部 Web サーバリダイレクト機能

固定 VLAN モードと同様です。「8.2.2 認証機能 (3) 外部 Web サーバリダイレクト機能」を参照してください。

(4) 認証成功後の自動表示 URL 指定

自動表示する URL の指定については，固定 VLAN モードと同様です。「8.2.2 認証機能 (4) 認証成功後の自動表示 URL 指定」を参照してください。

また，ダイナミック VLAN モードの場合は，認証前 VLAN から認証後 VLAN への切り替えで，認証端末の IP アドレス変更が必要となるため，URL 移動までの時間を約 20 ～ 30 秒程度で設定してください。

装置内蔵 DHCP サーバで認証前の端末に IP アドレス配布している場合 (デフォルトリース時間 1 日) は，認証後 VLAN で正規 DHCP サーバから IP アドレスを取得します。このため，認証完了時点から，認証後 VLAN 通信が可能になるまで，約 20 ～ 30 秒程度かかる場合があります。

ログイン成功画面表示後に自動表示する URL と URL 移動までの時間は，コンフィグレーションコマンド web-authentication jump-url で設定できます。

(5) 強制認証ポート指定

強制認証については，「5.4.6 認証共通の強制認証」を参照してください。

また，強制認証で認証許可した端末は，通常の認証済み端末と同様に後述の「8.3.2 認証機能 (7) 認証状態からのログアウト」により認証状態が解除されます。

(6) 認証数制限

装置単位およびポート単位に認証数の制限が設定できます。詳細は，「5.4.8 認証共通の端末数制限」を参照してください。

(7) 認証状態からのログアウト

ダイナミック VLAN モードでは，ログアウトの手段として下記があります。

- 最大接続時間超過時のログアウト
- 認証済み端末の無通信監視によるログアウト
- 認証済み端末からの特殊フレーム受信によるログアウト
- 認証端末接続ポートのリンクダウンによるログアウト
- VLAN 設定変更によるログアウト
- Web 画面によるログアウト
- 運用コマンドによるログアウト

各ログアウト手段は，固定 VLAN モードと同様です。「8.2.2 認証機能 (7) 認証状態からのログアウ

ト」を参照してください。

（8） ローミング（認証済み端末のポート移動）

HUB などを経由して接続した認証済み端末を，Web 認証設定ポートへリンクダウンしないでポート移動した場合でも，認証済み状態のまま継続して通信可能にします。

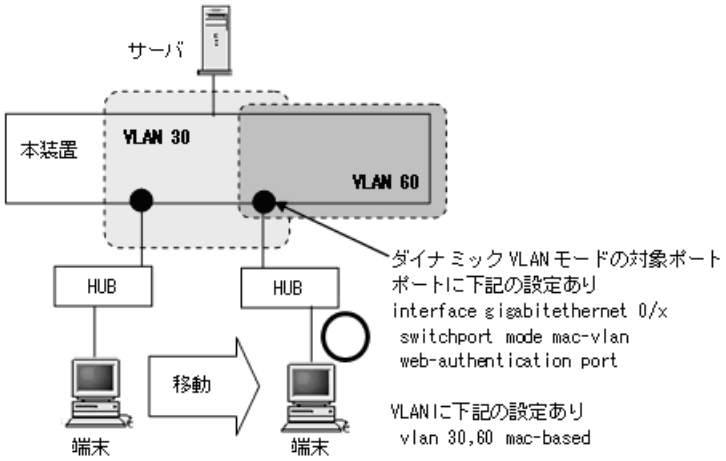
ローミングの動作可能な条件は下記のとおりです。

- コンフィグレーションコマンド web-authentication roaming 設定有
- 移動前および移動後が，ダイナミック VLAN モード対象ポート

上記以外の条件でポート移動を検出したときは，該当端末の認証を強制的にログアウトします。

なお，HUB などを経由して認証済み端末を Web 認証未設定ポートへ移動したときは，該当端末の認証をログアウトしません。Web 認証未設定ポートへ移動したときに認証をログアウトする場合は，コンフィグレーションコマンド authentication auto-logout strayer を設定してください。

図 8-11　ダイナミック VLAN モード　ローミング概要図



（9） ユーザ切替オプション

固定 VLAN モードと同様です。「8.2.2　認証機能（9）ユーザ切替オプション」を参照してください。

（10） Web 認証プレフィルタ

固定 VLAN モードと同様です。「8.2.2　認証機能（10）Web 認証プレフィルタ」を参照してください。

（11） HTTP サーバの初期タイムアウト時間の変更

固定 VLAN モードと同様です。「8.2.2　認証機能（11）HTTP サーバの初期タイムアウト時間の変更」を参照してください。

（12） ポートごとの個別 Web 認証画面

固定 VLAN モードと同様です。「8.2.2　認証機能（12）ポートごとの個別 Web 認証画面」を参照してください。

8.3.3 認証動作

ダイナミック VLAN モードは以下のシーケンスで認証動作を行います。

図 8-12 認証動作（Web 認証専用 IP アドレス使用時）

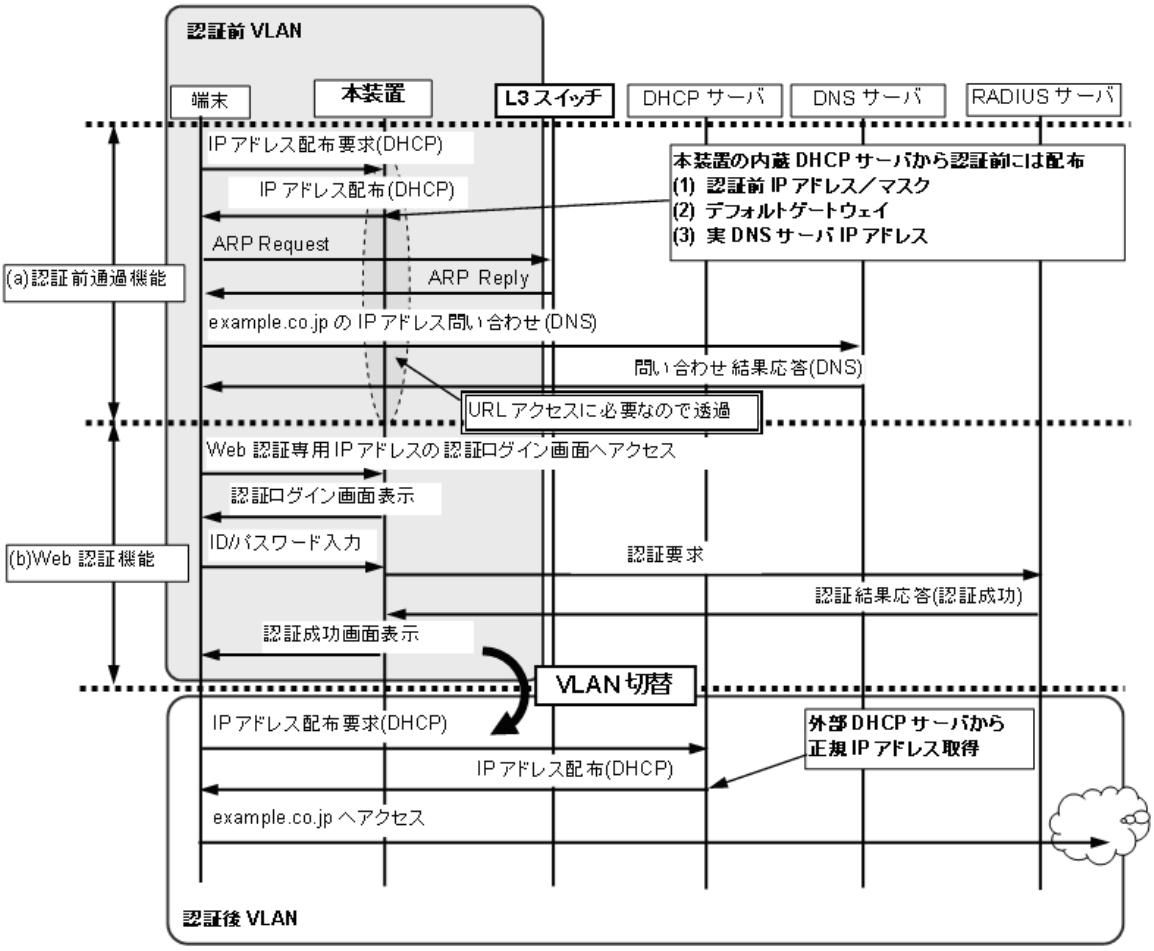
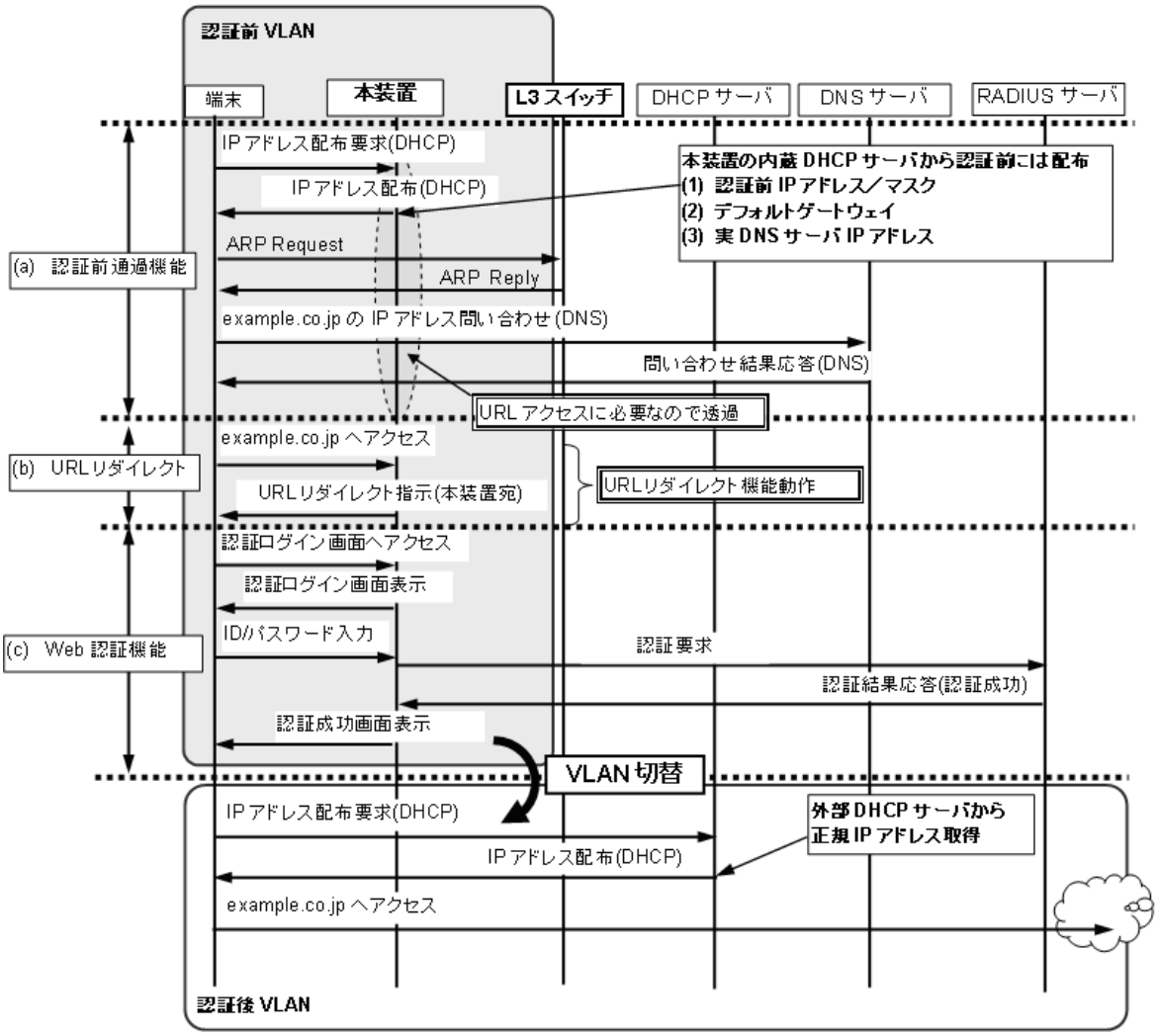


図 8-13　認証動作（URL リダイレクト機能使用時）



8.4 アカウント機能

Web 認証の認証結果は，次のアカウント機能で記録されます。

- 本装置内蔵のアカウントログ
- RADIUS サーバのアカウント機能への記録
- RADIUS サーバへの認証情報の記録
- syslog サーバへのアカウントログ出力

(1) 本装置内蔵のアカウントログ

Web 認証の認証結果や動作情報などの動作ログは，本装置内蔵のアカウントログに記録されます。

本装置内蔵のアカウントログは以下の最大数まで記録できます。

- スタック動作時：全認証機能の合計で最大 4096 行
- スタンドアロン動作時：Web 認証全体で最大 2100 行

最大数を超えた場合，古い順に記録が削除され，最新のアカウントログ情報が追加記録されていきます。

記録されるアカウントログ情報は次の情報です。

表 8-6 本装置内蔵のアカウントログへの出力情報

アカウントログ種別		時刻	ユーザ	IP	MAC	VLAN	Port※1	メッセージ
LOGIN	成功	○	○	○ ※2	○	○ ※2	○	ログイン成功メッセージ
	失敗	○	○	○ ※3	○ ※3	○ ※3	○ ※3	ログイン失敗要因メッセージ
LOGOUT		○	○ ※3	○ ※3	○ ※3	○ ※3	○ ※3	ログアウトメッセージ
SYSTEM		○	○ ※3	○ ※3	○ ※3	×	○ ※3	Web 認証機能の動作に関するメッセージ（ローミング検出，強制認証許可も含む）

（凡例）
○：出力します
×：出力しません

注 ※1
インタフェースポート番号またはチャネルグループ番号を出力します。

注 ※2
ダイナミック VLAN モードのログイン成功時に表示される IP アドレスには，認証前の IP アドレスが表示されます。また，VLAN ID には認証後の VLAN ID が表示されます。

注 ※3
メッセージによっては出力されない場合があります。
メッセージの詳細については，「運用コマンドレファレンス 29 Web 認証 show web-authentication logging」を参照してください。

また，記録されたアカウントログの出力機能については下記のとおりです。

1. 運用コマンド表示
運用コマンド show web-authentication logging で，採取されているアカウントログを最新の情報から

表示します。

2. syslog サーバへ出力
   後述「(4) syslog サーバへのアカウントログ出力」を参照してください。
3. プライベート Trap
   Web 認証の特定イベントのアカウントログ採取を契機にプライベート Trap を発行する機能をサポートしています。プライベート Trap 発行可否および発行種別はコンフィグレーションコマンドで設定してください。

表 8-7 アカウントログ（LOGIN/LOGOUT）とプライベート Trap 発行条件 (1)

アカウントログ種別		プライベート Trap 発行に必要なコンフィグレーション設定	
		コマンド	パラメータ
LOGIN	成功	snmp-server host	web-authentication
		snmp-server traps	web-authentication-trap all
	失敗	snmp-server host	web-authentication
		未設定，または下記のどちらかを設定	
		snmp-server traps	web-authentication-trap all
		snmp-server traps	web-authentication-trap failure
LOGOUT		snmp-server host	web-authentication
		snmp-server traps	web-authentication-trap all

表 8-8 アカウントログ (SYSTEM) とプライベート Trap 発行条件 (2)

アカウントログ種別 SYSTEM	認証モード	プライベート Trap 発行に必要なコンフィグレーション設定	
		コマンド	パラメータ
ローミング	固定 VLAN	snmp-server host	web-authentication
		web-authentication static-vlan roaming	action trap
	ダイナミック VLAN	snmp-server host	web-authentication
		web-authentication roaming	action trap

強制認証のプライベート Trap については，「5.4.6 認証共通の強制認証（4）強制認証でのプライベート Trap」を参照してください。

（2）RADIUS サーバのアカウント機能への記録

コンフィグレーションコマンド aaa accounting web-authentication で，RADIUS サーバのアカウント機能を使用できます。

なお，RADIUS サーバへアカウンティング情報を送信するときに使用する RADIUS 属性については，「8.5 事前準備」を参照してください。

（3）RADIUS サーバへの認証情報の記録

RADIUS 認証方式の場合は，RADIUS サーバが持っている機能によって，認証成功／認証失敗が記録されます。ただし，使用する RADIUS サーバによって記録される情報が異なることがありますので，詳細は RADIUS サーバの説明書を参照してください。

（4） syslog サーバへのアカウントログ出力

コンフィグレーションで syslog 設定されているすべての syslog サーバへ，装置全体の運用ログ情報と合わせて Web 認証のアカウントログ情報を出力します。

図 8-14　syslog サーバ出力形式

```
 Fac 月 日 時刻 hostname [番号]:AUT 月/日 時刻 WEB  ログメッセージ本文
|(1)|---(2) ---|--(3)---|--(4)-|(5)|----(6)---|(7)|------------(8)-------------|

  (1)ファシリティ
  (2)TIMESTAMP：メッセージ生成時刻
  (3)HOSTNAME:本装置の識別名称
  (4)機能番号
  (5)認証機能を示すログ種別
  (6)事象発生時刻
  (7)Web 認証を示す認証機能種別
  (8)メッセージ本文
```

syslog サーバへのログ出力について詳細は，後述の「23　ログ出力機能」を参照してください。

なお，コンフィグレーションコマンド web-authentication logging enable および logging event-kind aut によって，Web 認証のアカウントログ出力を開始および停止できます。

8.5　事前準備

8.5.1　ローカル認証の場合

ローカル認証方式を使用するにあたっては，次の準備が必要です。

- コンフィグレーションの設定
- 内蔵 Web 認証 DB の登録
- 内蔵 Web 認証 DB のバックアップ
- 内蔵 Web 認証 DB の復元

（1）コンフィグレーションの設定

Web 認証を使用するために，本装置に VLAN 情報や Web 認証の情報をコンフィグレーションコマンドで設定します。（「9　Web 認証の設定と運用」を参照してください。）

（2）内蔵 Web 認証 DB の登録

ローカル認証方式を使用する前に，運用コマンドで事前にユーザ情報（認証対象端末のユーザ ID，パスワードおよび認証後 VLAN ID）を内蔵 Web 認証 DB に登録しておく必要があります。

内蔵 Web 認証 DB へ登録手順として，ユーザ情報の編集（追加・変更・削除）と内蔵 Web 認証 DB への反映があります。手順を以下に示します。

なお，ユーザ情報の追加を行う前に，Web 認証システムの環境設定およびコンフィグレーションの設定を完了している必要があります。

- 運用コマンド set web-authentication user で，ユーザ情報（認証対象端末のユーザ ID，パスワードおよび認証後 VLAN ID）を追加します。
- 登録済みのパスワードを変更する場合は，運用コマンド set web-authentication passwd で行います。
- 登録済みの認証後 VLAN ID を変更する場合は，運用コマンド set web-authentication vlan で行います。
- 登録済みのユーザ情報を削除する場合は，運用コマンド remove web-authentication user で行います。
- 編集したユーザ情報は，運用コマンド commit web-authentication 実行により，内蔵 Web 認証 DB へ反映されます。

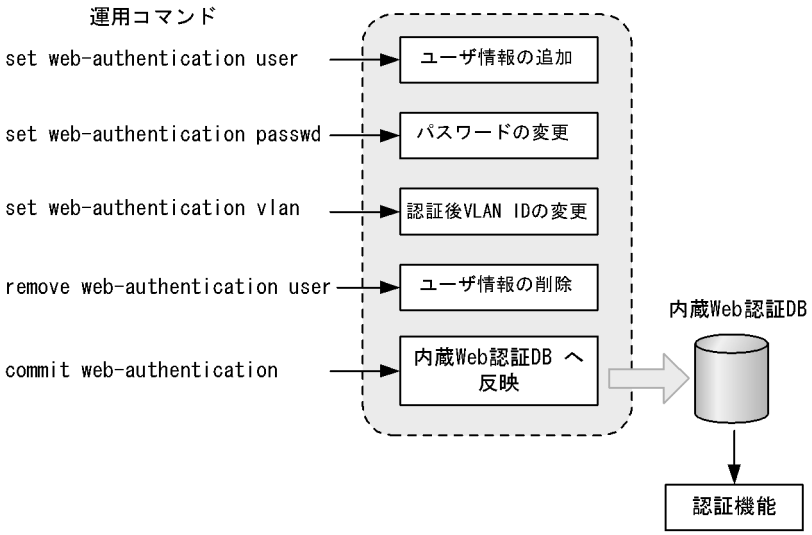
また，運用コマンド show web-authentication user で，運用コマンド commit web-authentication を実行するまでに編集したユーザアドレス情報をみることができます。

ユーザ ID とパスワードで文字数範囲と使用可能文字を次の表に示します。

表 8-9　文字数範囲と使用可能文字

ユーザ ID 文字数範囲	パスワード文字数範囲	使用可能文字
1 ～ 128 文字	1 ～ 32 文字	0 ～ 9 A ～ Z a ～ z アットマーク（@） ハイフン（-） アンダースコア（_） ドット（.）

図 8-15　ユーザ情報の編集と内蔵 Web 認証 DB への反映



（3） 内蔵 Web 認証 DB のバックアップ

運用コマンド store web-authentication で，内蔵 Web 認証 DB のバックアップを取ることができます。

（4） 内蔵 Web 認証 DB の復元

運用コマンド load web-authentication で，バックアップファイルから内蔵 Web 認証 DB の復元ができます。

ただし，直前までに運用コマンド set web-authentication user などで編集および登録した内容は廃棄され，復元された内容に置き換わりますので，復元の実行には注意が必要です。

8.5.2　RADIUS 認証の場合

RADIUS 認証方式を使用するにあたっては，次の準備が必要です。

- コンフィグレーションの設定
- RADIUS サーバの準備

（1） コンフィグレーションの設定

Web 認証を使用するために，本装置に VLAN 情報や Web 認証の情報をコンフィグレーションコマンドで設定します。（「9　Web 認証の設定と運用」を参照してください。）

（2） RADIUS サーバの準備

（a） 使用する RADIUS 属性

本装置が使用する RADIUS の属性名を次の表に示します。

表 8-10　認証で使用する属性名（その 1 Access-Request）

属性名	Type 値	解説
User-Name	1	認証されるユーザ ID。
User-Password	2	ユーザパスワード。

属性名	Type 値	解説
NAS-IP-Address	4	認証を要求している，本装置の IPv4 アドレス。 IPv4 アドレスが登録されている VLAN インタフェースのうち，最も小さい VLAN ID の IPv4 アドレスを使用します。
NAS-Port	5	• 固定 VLAN モード：認証している認証単位の IfIndex • ダイナミック VLAN モード：認証している認証単位の IfIndex
Service-Type	6	提供するサービスタイプ。 Framed(2) 固定。
State	24	テキスト文字列。 Access-Challenge に対応する Access-Request のときに，Access-Challenge が State 有の場合，本装置で保持していた State 情報を付加します。
Called-Station-Id	30	認証ポートの MAC アドレス（小文字 ASCII※，ハイフン（－）区切り）
Calling-Station-Id	31	端末の MAC アドレス（小文字 ASCII※，ハイフン（－）区切り）。
NAS-Identifier	32	• 固定 VLAN モード 認証要求端末が所属する VLAN の VLAN ID。 VLAN10 の場合 "10" • ダイナミック VLAN モード コンフィグレーションコマンド hostname で設定された文字列。
NAS-Port-Type	61	端末がユーザ認証に使用している物理ポートのタイプ。 Virtual(5)
Connect-Info	77	コネクションの特徴を示す文字列。 • 固定 VLAN モード： 物理ポート ("CONNECT Ethernet") チャネルグループポート ("CONNECT Port-Channel ") • ダイナミック VLAN モード： 物理ポート ("CONNECT Ethernet") チャネルグループポート ("CONNECT Port-Channel ")
NAS-Port-Id	87	ポートを識別するための文字列（x，y には数字が入ります）。 • 固定 VLAN モード："Port x/y"，"ChGr x" • ダイナミック VLAN モード："Port x/y"，"ChGr x"
NAS-IPv6-Address	95	認証を要求している，本装置の IPv6 アドレス。 IPv6 アドレスが登録されている VLAN インタフェースのうち，最も小さい VLAN ID の IPv6 アドレスを使用します。

注 ※

本装置では，「Called-Station-Id」「Calling-Station-Id」の MAC アドレスを小文字で使用しますが，コンフィグレーションコマンド radius-server attribute station-id capitalize により，MAC アドレス内の "a" ～ "f" の文字を大文字形式にできます。

表 8-11　認証で使用する属性名（その 3　Access-Accept）

属性名	Type 値	解説
Service-Type	6	提供するサービスタイプ。 Framed(2) 固定。
Filter-Id	11	テキスト文字列。 マルチステップ認証で使用 ※1。
Reply-Message	18	未使用 ※2
Tunnel-Type	64	トンネル・タイプ ※3。 VLAN(13) 固定。

属性名	Type 値	解説
Tunnel-Medium-Type	65	トンネルを作成する際のプロトコル※3。 IEEE802(6) 固定。
Tunnel-Private-Group-ID	81	VLAN を識別する文字列※4。 次に示す文字列が対応する。 (1)VLAN ID を示す文字列 (2)"VLAN"+VLAN ID を示す文字列 文字列にスペースを含んではいけない（含めた場合 VLAN 割り当ては失敗する）。 (3) コンフィグレーションコマンド name で VLAN インタフェースに設定された VLAN 名称を示す文字列（VLAN ID の小さいほうを優先）※5 （設定例） VLAN ID：10 コンフィグレーションコマンド name：Authen_VLAN (1) の場合　"10" (2) の場合　"VLAN10" (3) の場合　"Authen_VLAN"

注 ※1

マルチステップ認証で使用する文字列については，「12　マルチステップ認証」を参照してください。

注 ※2

Reply-Message の文字列はアカウントログとして本装置で採取しています。

注 ※3

Tag 領域は無視します。

注 ※4

本装置では文字列形式の選択および VLAN ID の識別を下記条件で実施します。

1. Tunnel-Private-Group-ID の文字列形式 (1)(2)(3) 選択条件
   - 先頭が 0 ～ 9 の数字文字で始まる文字列は，(1) の形式
   - 先頭が "VLAN" ＋ 0 ～ 9 の数字文字で始まる文字列は，(2) の形式
   - 上記以外の文字列は，(3) の形式

   なお，先頭 1 バイトが 0x00 ～ 0x1f のときは Tag 付きですが Tag 領域は無視します。
2. (1)(2) 形式の文字列から VLAN ID を識別する条件
   - 数字文字 "0" ～ "9" だけを 10 進数に変換し，先頭 4 文字だけ有効範囲とします。（5 文字目以降は無視します。）

     例) "0010" は "010" や "10" と同じで，VLAN ID = 10　となります。

     "01234" は，VLAN ID =123　となります。
   - 文字列の途中に "0" ～ "9" 以外が入っていると，文字列の終端とします。

     例)"12+3" は，VLAN ID =12　となります。

注 ※5

コンフィグレーションコマンド name による VLAN 名称指定については，「5.4.2　VLAN 名称による収容 VLAN 指定」を参照してください。

表 8-12　RADIUS アカウント機能で使用する属性名

属性名	Type 値	解説
User-Name	1	認証されるユーザ ID。
NAS-IP-Address	4	認証を要求している，本装置の IPv4 アドレス。 IPv4 アドレスが登録されている VLAN インタフェースのうち，最も小さい VLAN ID の IPv4 アドレスを使用します。

属性名	Type 値	解説
NAS-Port	5	• 固定 VLAN モード：認証している認証単位の IfIndex • ダイナミック VLAN モード：認証している認証単位の IfIndex
Service-Type	6	提供するサービスタイプ。 Framed(2) 固定。
Calling-Station-Id	31	認証端末の MAC アドレス（小文字 ASCII※，ハイフン（－）区切り）。
NAS-Identifier	32	• 固定 VLAN モード 認証要求端末が所属する VLAN の VLAN ID。 VLAN10 の場合 "10" • ダイナミック VLAN モード コンフィグレーションコマンド hostname で設定された文字列。
Acct-Status-Type	40	アカウンティング要求種別。 Start(1)，Stop(2)
Acct-Delay-Time	41	アカウンティング情報（送信遅延時間）。（秒）
Acct-Input-Octets	42	アカウンティング情報（受信オクテット数）。 (0) 固定。
Acct-Output-Octets	43	アカウンティング情報（送信オクテット数）。 (0) 固定。
Acct-Session-Id	44	アカウンティング情報を識別する ID。
Acct-Authentic	45	認証方式。 RADIUS(1)，Local(2)
Acct-Session-Time	46	アカウンティング情報（セッション持続時間）。 (0) 固定。
Acct-Input-Packets	47	アカウンティング情報（受信パケット数）。 (0) 固定。
Acct-Output-Packets	48	アカウンティング情報（送信パケット数）。 (0) 固定。
Acct-Terminate-Cause	49	アカウンティング情報（セッション終了要因）。 「表 8-13　Acct-Terminate-Cause での切断要因」を参照。
NAS-Port-Type	61	端末が認証に使用している物理ポートのタイプ。 Virtual(5) 固定。
NAS-Port-Id	87	ポートを識別するための文字列（x，y には数字が入ります）。 • 固定 VLAN モード："Port x/y"，"ChGr x" • ダイナミック VLAN モード："Port x/y"，"ChGr x"
NAS-IPv6-Address	95	認証を要求している，本装置の IPv6 アドレス。 IPv6 アドレスが登録されている VLAN インタフェースのうち，最も小さい VLAN ID の IPv6 アドレスを使用します。

注 ※

本装置では，「Calling-Station-Id」の MAC アドレスを小文字で使用しますが，コンフィグレーションコマンド radius-server attribute station-id capitalize により，MAC アドレス内の "a" ～ "f" の文字を大文字形式にできます。

表 8-13　Acct-Terminate-Cause での切断要因

属性名	Type 値	解説
User Request	1	Web 認証画面でログアウトを要求されたため切断した。 端末移動を検出したため切断した。
Idle Timeout	4	無通信時間が一定時間続いたため切断した。

属性名	Type 値	解説
Session Timeout	5	セッション期限が満了したため切断した。
Admin Reset	6	管理者の意思で切断した。 • コンフィグレーションで web-authentication port を削除した場合 その他認証用コンフィグレーションの変更や運用コマンドによる切断要因を含む。
Port Preempt	13	より優先度の高い利用者にサービスを提供するためにセッションを終了した。 ユーザを切り替えるために前のユーザをログアウトした。（コンフィグレーションコマンド web-authentication user replacement 設定時）
Service Unavailable	15	サービスを提供できなくなった。 • 認証済み端末のポート移動（ローミング）時に，移動先ポートで authentication max-user の設定数超過を検出したためログアウトした場合
Port Reinitialized	21	ポートの MAC が再初期化された。 • ポートがリンクダウンした場合 • コンフィグレーションでポートから vlan を削除した場合 • コンフィグレーションで shutdown を設定した場合 • 運用コマンド inactivate を実行した場合

(b) RADIUS サーバに設定する情報

RADIUS 認証方式を使用するに当たっては，RADIUS サーバでユーザごとにユーザ ID，パスワード，VLAN ID の設定が必要です。

なお，RADIUS サーバの詳細な設定方法については，使用する RADIUS サーバの説明書を参照してください。

ユーザごとの VLAN 情報の RADIUS サーバ設定例を示します。

- 固定 VLAN モードの場合：認証要求端末が所属する VLAN の VLAN ID「20」
- ダイナミック VLAN モードの場合：認証後 VLAN「400」
- コンフィグレーションコマンド name の設定：「GroupA-Network」

表 8-14 RADIUS サーバ設定例

設定項目	設定内容
User-Name	認証対象のユーザ ID。 文字数範囲： 1 ～ 128 文字 使用可能文字：文字コード範囲 0x21 ～ 0x7E※
Auth-Type	Local
User-Password	認証対象ユーザのパスワード。 文字数範囲： 1 ～ 32 文字 使用可能文字：文字コード範囲 0x21 ～ 0x7E※
NAS-Identifier	固定 VLAN モードの場合 "20" 認証要求端末が所属する VLAN の VLAN ID を数字文字で設定。
Tunnel-Type	Virtual VLAN（値 13）
Tunnel-Medium-Type	IEEE-802（値 6）

設定項目	設定内容
Tunnel-Private-Group-ID	ダイナミック VLAN モードの場合 下記のいずれかの形式 • "400" 認証後 VLAN ID を数字文字で設定。 • "VLAN0400" 文字列 "VLAN" に続いて，認証後 VLAN ID を数字文字で設定。 • "GroupA-Network" コンフィグレーションコマンド name で設定された VLAN 名称を示す文字列。
認証方式	PAP

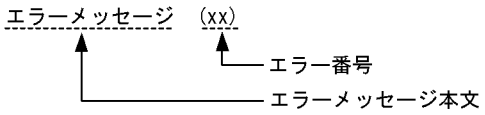
注 ※

文字コード範囲に対応する文字については，「コンフィグレーションコマンドレファレンス　文字コード一覧」を参照してください。

8.6 認証エラーメッセージ

認証エラー画面に表示する認証エラーメッセージ表示の形式を次の図に示します。

図 8-16 認証エラーメッセージ形式



認証エラーの発生理由を次の表に示します。

表 8-15 認証エラーメッセージとエラー発生理由対応表

エラーメッセージ内容	エラー番号	エラー発生理由
User ID or password is wrong. Please enter correct user ID and password.	11	ログインユーザ ID が指定されていません。
	12	ログインユーザ ID が最大文字数を超えています。
	13	パスワードが指定されていません。
	14	ログインユーザ ID が内蔵 Web 認証 DB に登録されていません。
	15	パスワードが最大文字数を超えているか，または登録されていません。
	22	ローカル認証方式で，認証済みの端末から再ログインを行った際に，パスワードが一致していませんでした。
RADIUS: Authentication reject.	31	RADIUS サーバから認証許可以外 (アクセス拒否またはアクセスチャレンジ) を受信しました。
RADIUS: No authentication response.	32	RADIUS サーバから認証許可を受信できませんでした（受信タイムアウト，または RADIUS サーバの設定がされていない状態です)。
You cannot login by this machine.	33	下記の要因が考えられます。 • RADIUS サーバに設定された認証後 VLAN が，Web 認証で定義された VLAN ではありません。 • ダイナミック VLAN モードの認証後 VLAN が，MAC VLAN ではありません。 • RADIUS サーバの RADIUS 属性で設定された VLAN と，認証対象ポートのネイティブ VLAN が衝突しました。 • RADIUS サーバの RADIUS 属性で設定された VLAN とコンフィグレーションコマンド switchport mac dot1q vlan で設定した VLAN が衝突しました。 • コンフィグレーションコマンド no switchport mac auto-vlan 設定有ですが，認証対象ポートに MAC VLAN が設定されていません。
	35	下記の要因が考えられます。 • 対象ポートが固定 VLAN モードまたはダイナミック VLAN モードとして設定されていません。 • 端末が接続されている認証対象ポートがリンクダウンの状態です。
	36	認証した端末を収容する VLAN が suspend 状態になっています。
	37	RADIUS 認証方式で，ログイン数が最大収容条件を超えたために認証できませんでした。
	41	同一 MAC アドレスの端末から，異なるユーザでのログイン要求がありました。

エラーメッセージ内容	エラー番号	エラー発生理由
	42	下記の要因が考えられます。 • 内蔵 Web 認証 DB に設定された VLAN ID が，Web 認証で定義された VLAN ではありません。 • ダイナミック VLAN モードの認証後 VLAN が，MAC VLAN ではありません。 • 内蔵 Web 認証 DB に設定された VLAN と，認証対象ポートのネイティブ VLAN が衝突しました。 • 内蔵 Web 認証 DB に設定された VLAN と，コンフィグレーションコマンド switchport mac dot1q vlan で設定した VLAN が衝突しました。 • コンフィグレーションコマンド no switchport mac auto-vlan 設定有ですが，認証対象ポートに MAC VLAN が設定されていません。
	44	下記の要因が考えられます。 • 別の認証機能で同一端末を認証済みのため認証できません。 • コンフィグレーションコマンド mac-address-table static で端末の MAC アドレスを MAC アドレステーブルに登録済みのため認証できません。 • コンフィグレーションコマンド mac-address で端末の MAC アドレスを MAC VLAN に登録済みのため認証できません。
	45	下記の要因が考えられます。 • 対象ポートが固定 VLAN モードまたはダイナミック VLAN モードとして設定されていません。 • 端末が接続されている認証対象ポートがリンクダウンの状態です。
	46	認証した端末を収容する VLAN が suspend 状態になっています。
	47	ログイン数が最大収容条件を超えたために認証できませんでした。
	78	MAC アドレスを MAC アドレステーブルに登録する際，ログイン数が最大収容条件を超えています。 または，ハードウェアの制約で，端末の MAC アドレスが MAC アドレステーブルに登録できなかった可能性があります。
	101	Web 認証の設定が無効です。
	103	認証中 (AUTHENTICATING) に同一 MAC アドレスの端末から新たにログイン要求がありました。
Sorry, you cannot login just now. Please try again after a while.	51	ログイン端末の IP アドレスから MAC アドレスを解決できませんでした。
	52	下記の要因が考えられます。 ・ ログイン端末のMAC認証またはIEEE802.1Xが認証解除されているため，マルチステップ認証※2ができません。（スタック動作時※1） ・ 既に他の認証が完了しているため，マルチステップ認証※2ができません。
	105	スタック構成が変化したので，認証処理を中断しました。（スタック動作時※1）
The system error occurred. Please contact the system administrator.	64	RADIUS サーバへアクセスできませんでした。
A fatal error occurred. Please inform the system administrator.	71	Web 認証の内部エラー (同時に最大収容数を超えた RADIUS サーバへの認証要求が起きました。)
	72	MAC VLAN に認証した MAC アドレスを登録できませんでした。

エラーメッセージ内容	エラー番号	エラー発生理由
Sorry, you cannot logout just now. Please try again after a while.	81	ログアウト要求された端末の IP アドレスから MAC アドレスを解決できませんでした。
The client PC is not authenticated.	82	ログインされていない端末からのログアウト要求です。

エラー番号ごとの対処方法

- 1x：正しいユーザ ID とパスワードで再度ログイン操作を行ってください。
- 3x：RADIUS サーバと本装置の Web 認証情報の設定を見直してください。
- 4x：Web 認証のコンフィグレーション，および内蔵 Web 認証 DB の設定を見直してください。
- 5x：しばらく経ってから，再度ログイン操作を行ってください。
- 6x：本装置の RADIUS サーバ情報の設定を見直してください。
- 7x：システム構成を確認してください。
- 8x：URL を確認して，再度ログアウト操作を行ってください。
- 101：RADIUS サーバと本装置の Web 認証情報の設定を見直してください。
- 103：他の Web ブラウザウィンドウでログインが完了していることを確認してください。

注 ※1

スタック機能については，「コンフィグレーションガイド Vol.1　7　スタックの解説【OP-WLE】」を参照してください。

注 ※2

マルチステップ認証については，後述の「12　マルチステップ認証」を参照してください。

8.7 Web 認証の注意事項

8.7.1 Web 認証と他機能の共存について

Web 認証と他機能の共存については，「5.9.3 レイヤ 2 認証機能と他機能の共存」を参照してください。

8.7.2 認証モード共通の注意事項

(1) Web 認証専用 IP アドレスと URL リダイレクト機能の使用について

ログイン操作では，Web 認証専用 IP アドレスを使用する方法と，URL リダイレクト機能を使用する方法があります。どちらの場合でもローカル認証方式および RADIUS 認証方式で認証できます。

このため，Web 認証専用 IP アドレスと URL リダイレクトの両方，またはどちらかを必ず設定してください。

(2) URL リダイレクト機能の使用について

(a) IP アドレスの設定

URL リダイレクトを使用する場合は，必ず対象 VLAN に IP アドレスを設定してください。

(b) プロキシ環境で使用時の制限

下記の条件すべてに該当する環境で使用時，認証対象端末に Web 認証ログイン画面が表示されず，端末を認証できません。

- ネットワークがプロキシ設定環境
- URL リダイレクト有効
  (コンフィグレーションコマンド web-authentication redirect enable のデフォルトコンフィグレーション)
- URL リダイレクトでの Web 認証ログイン画面プロトコル https 指定
  (コンフィグレーションコマンド web-authentication redirect-mode のデフォルトコンフィグレーション)

この場合は，本装置および認証対象端末に下記を設定してご使用ください。

- 本装置側：Web 認証専用 IP アドレスを設定
- 認証対象端末側：Web 認証専用 IP アドレスを「プロキシ例外アドレス」として設定

(c) 認証前の端末から https による本装置外の URL アクセスについて

認証前の端末から https で URL へアクセスしたとき，本装置に登録されている証明書のドメイン名と一致しなかった場合は，証明書不一致の警告メッセージが端末の Web ブラウザ上に表示されます。警告メッセージが表示されても「続行」操作を選択すると，Web 認証のログイン画面が表示されログイン操作が可能になります。

(d) Web 認証用のアクセスポート（TCP 待ち受けポート）番号について

本装置では，Web 認証用のアクセスポートの指定はサポートしておりません。

コンフィグレーションコマンド web-authentication web-port は，URL リダイレクト機能で使用するための指定です。

(e) 外部 Web サーバリダイレクト機能について

外部 Web サーバリダイレクト機能使用時，パスワード入力ミスなどによりログイン失敗画面が表示され，「login page」ボタンがクリックされた場合は，内蔵 Web サーバのログイン画面を表示します。

(f) URL リダイレクト先 Web サーバの切り替え機能について

本機能をご使用の場合は，下記にご注意ください。

- host が FQDN の場合は，監視ごとに DNS 解決します。DNS 失敗（DNS リゾルバ再送後）は「無応答」扱いとします。
- 本装置の IP レイヤ以下に問題があった場合は，監視パケットが送信されないまま「無応答」と判定する可能性があります。
- 監視パケットの送信間隔は，1 回の監視処理修了から，次の監視処理開始までの間隔です。（DNS や TCP の再送が発生する場合は，指定した監視間隔が延びます。）
- プロキシ経由の監視は未サポートです。

(g) リダイレクト先 URL に付加するクエリについて

コンフィグレーションコマンド web-authentication redirect queries で original-url を設定時，下記に該当する場合は，リダイレクト前の URL を付加することができません。

- リダイレクト前の URL が URL エンコード後 ※ に 1024 文字を超える場合
- リダイレクト前の URL にパーセント (%) が含まれる場合

注 ※

アンパーサンド (&) が "%26" になります。詳細は RFC3986 を参照してください。

(h) 認証成功後の自動表示 URL 指定について

コンフィグレーションコマンド web-authentication jump-url original を設定時，下記に該当する場合はリダイレクト前の URL の画面を表示することができないため，認証成功後にログイン成功画面を表示したままになります。

- リダイレクト前の URL が URL エンコード後 ※1 に 1024 文字を超える場合
- リダイレクト前の URL が HTML エンコード後 ※2 に 1024 文字を超える場合
- リダイレクト前の URL にパーセント (%) が含まれる場合
- パスワード入力ミスなどによりログイン失敗画面が表示され，「login page」ボタンでログイン画面に戻ってから，再度ログインして認証成功となった場合

注 ※1

アンパーサンド (&) が "%26" になります。詳細は RFC3986 を参照してください。

注 ※2

アンパーサンド (&) が "&" になります。詳細は RFC1866 を参照してください。

(3) DHCP サーバの IP アドレスリース時間設定について

認証対象端末に認証前 IP アドレスを DHCP サーバから配布する場合，DHCP サーバの IP アドレスリース時間をできるだけ短く設定してください。

なお，内蔵 DHCP サーバに関しては，10 秒から指定できますが，小さい値を設定し，しかも，認証ユーザ数が多い場合には装置に負荷が掛かりますので，必要に応じてリース時間の設定を変更してください。

(4) 内蔵 Web 認証 DB の変更時

運用コマンドで内蔵 Web 認証 DB への追加，変更を行った場合，現在認証中のユーザには適用されず，次

回ログイン時から有効となります。

(5) 装置再起動により Web 認証を再起動した場合

装置を再起動した場合，認証中のユーザすべての認証が解除されます。この場合，再起動後に端末から手動で再度認証を行ってください。

(6) 最大接続時間の設定について

コンフィグレーションコマンド web-authentication max-timer で最大接続時間の短縮，延長を行った場合，現在認証中のユーザには適用されず，次回ログイン時から設定が有効となります。

(7) 認証接続時間を延長する際の注意

認証済みの状態で再ログインを行った場合，ローカル認証（RADIUS 認証使用時は RADIUS 認証）で認証に成功すると認証時間を延長できます。認証に失敗すると認証時間は延長できません。

(8) 強制認証ポートの使用について

1. 本機能はセキュリティ上の問題となる可能性がありますので，十分検討の上ご使用ください。
2. 本機能は RADIUS 認証方式だけサポートしています。
   強制認証をご使用になるときは，認証方式に RADIUS 認証だけを設定してください。以下のようにローカル認証・RADIUS 認証の両方を設定したときは，強制認証を設定しても動作しません。
   - aaa authentication web-authentication default group radius local
   - aaa authentication web-authentication default local group radius

(9) 認証済み端末のポート移動について

認証済み端末を Web 認証設定ポートへポート移動したときは，「8.2　固定 VLAN モード　8.2.2　認証機能　(8) ローミング（認証済み端末のポート移動)」「8.3　ダイナミック VLAN モード　8.3.2　認証機能　(8) ローミング（認証済み端末のポート移動)」により，継続通信または認証ログアウトとなります。

なお，認証済み端末を同一 VLAN 内の Web 認証未設定ポートへポート移動したときは，認証状態が解除されるまで通信できません。運用コマンド clear web-authentication auth-state を使用して，端末の認証状態を解除してください。

コンフィグレーションコマンド authentication auto-logout strayer を設定しておくと，Web 認証未設定ポートへ移動したときに，認証状態を解除できます。

(10) ローミング設定と DHCP snooping 併用時の制限

コンフィグレーションコマンド web-authentication static-vlan roaming，web-authentication roaming 設定状態で DHCP snooping 機能併用時，認証済み端末のポートを移動すると，認証状態は移動後のポートに遷移しますが，バインディングデータベースは更新されないため通信できません。

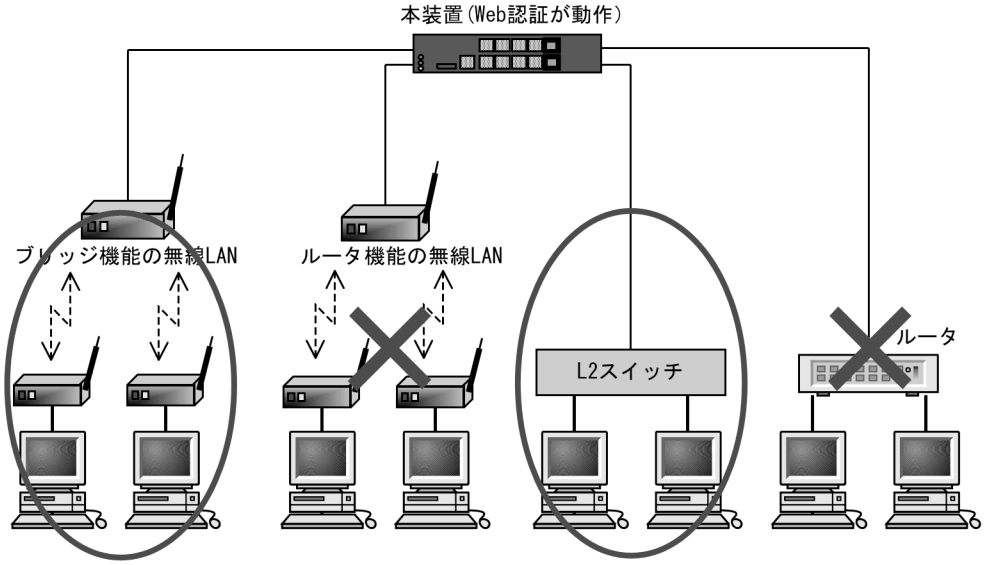
(11) 本装置と認証対象の端末間に接続する装置について

本装置の配下にはプロキシサーバやルータを接続しないでください。

本装置と認証端末との間の経路上に，クライアント端末の MAC アドレスを書き換えるもの（プロキシサーバやルータなど）が存在した場合，Web 認証が書き換えられた MAC アドレスを認証対処端末と認識してしまうために端末ごとの認証ができません。

また，本装置の配下にポート間遮断機能のない HUB や無線 LAN を接続し，それに複数の PC が接続されている場合，認証済みでなくても PC 同士で通信ができてしまいますので注意が必要です。

図 8-17 本装置と端末間の接続



8.7.3 固定 VLAN モード使用時の注意事項

(1) 固定 VLAN モードのポートについて

固定 VLAN モードはアクセスポート / トランクポート，および MAC ポートで Tagged フレーム中継可（コンフィグレーションコマンド switchport mac dot1q vlan）が設定されているポートでの Tagged フレームによる Web 認証が動作可能です。

(2) 接続監視機能について

固定 VLAN モードはデフォルトコンフィグレーションで認証済み端末の接続監視機能が有効になっています。装置の負荷が高い場合は，監視フレームである ARP パケットを送受信できずにポーリングタイムアウトを誤検出する可能性があります。その場合はコンフィグレーションコマンド web-authentication logout polling retry-interval の設定値を大きくしてください。

認証端末の台数が多い場合 (100 台以上) はコンフィグレーションコマンド web-authentication logout polling retry-interval を 10 秒に設定することを推奨します。

8.7.4 ダイナミック VLAN モード使用時の注意事項

(1) MAC アドレス学習エージング時間設定上の注意

MAC アドレステーブルのエージング時間を短く設定した状態で端末が使用されていない時間が続くと，強制的にログアウトしてしまうので注意が必要です。なお，強制的にログアウトさせたくない場合は，コンフィグレーションコマンド no web-authentication auto-logout を設定してください。

(2) 認証後 VLAN へ切り替え後に端末からの通信がない場合

認証後 VLAN へ切り替え後に端末からの通信がまったくないと，MAC アドレス学習が行われません。この場合，認証済みであっても MAC アドレステーブルに MAC アドレスが登録されていないので，強制的にログアウトします。認証後は必ず通信を行ってください。なお，強制的にログアウトさせたくない場合は，コンフィグレーションコマンド no web-authentication auto-logout を設定してください。

(3) ログアウト後の端末 IP アドレスについて

ログアウト後（Web 画面によるログアウト，最大接続時間を超えての強制ログアウト）は，端末の IP アドレスを認証前の IP アドレスに変更してください。

- 手動設定の場合は，手動で端末の IP アドレスを認証前の IP アドレスに設定してください。
- DHCP サーバを使用している場合，端末の IP アドレスをいったん削除してから，あらためて DHCP サーバへ IP アドレスの配布指示を行ってください。（例：Windows の場合，コマンドプロンプトから ipconfig /release を実行した後に，ipconfig /renew を実行してください。）

8.8 Web 認証画面入れ替え機能

本装置の Web 認証画面入れ替え機能で使用する，ファイルセット種別および認証画面種別について以下の用語を使用します。

表 8-16 Web 認証画面入れ替え機能で使用する用語

用語		説明
ファイルセット		Web 認証を実施するために必要な HTML ファイル (login.html, logout.html など) が格納されたディレクトリの総称。
	デフォルトファイルセット	装置にあらかじめ初期状態で格納されており，すべての HTML ファイルが初期状態のディレクトリ。
	カスタムファイルセット	ユーザが独自に生成した Web 認証用の HTML ファイルが格納されているディレクトリ。
認証画面	基本 Web 認証画面	通常の Web 認証を実施した際に表示する標準の Web 認証画面。 基本 Web 認証画面は，本装置内にデフォルトファイルセットがあり，カスタムファイルセットで入れ替え可能。 （本装置の Web 認証共通で通常使用する認証画面）
	個別 Web 認証画面	条件とカスタムファイルセットを関連付けし，特定条件成立時に表示する Web 認証画面。 個別 Web 認証画面は，本装置にデフォルトファイルセットはなく，カスタムファイルセットで追加可能。 （本装置のポートごとの個別 Web 認証画面指定で使用する認証画面）

8.8.1 Web 認証画面入れ替え機能

Web 認証で使用するログイン画面やログアウト画面など，Web ブラウザに表示する画面情報（以降，Web 認証画面と呼びます）は，外部装置（PC など）で作成し，カスタムファイルセットとして運用コマンド set web-authentication html-files で本装置に入れ替えることができます。

入れ替え可能な画面を次に示します。

表 8-17 入れ替え可能な画面ファイル

ファイル種別	HTML ファイル名	備考
ログイン画面	login.html	入れ替え時のカスタムファイルセットに必須
ログアウト画面	logout.html	
ログイン成功画面	loginOK.html	
ログイン失敗画面	loginNG.html	
ログアウト完了画面	logoutOK.html	
ログアウト失敗画面	logoutNG.html	
アイコン	favicon.ico	

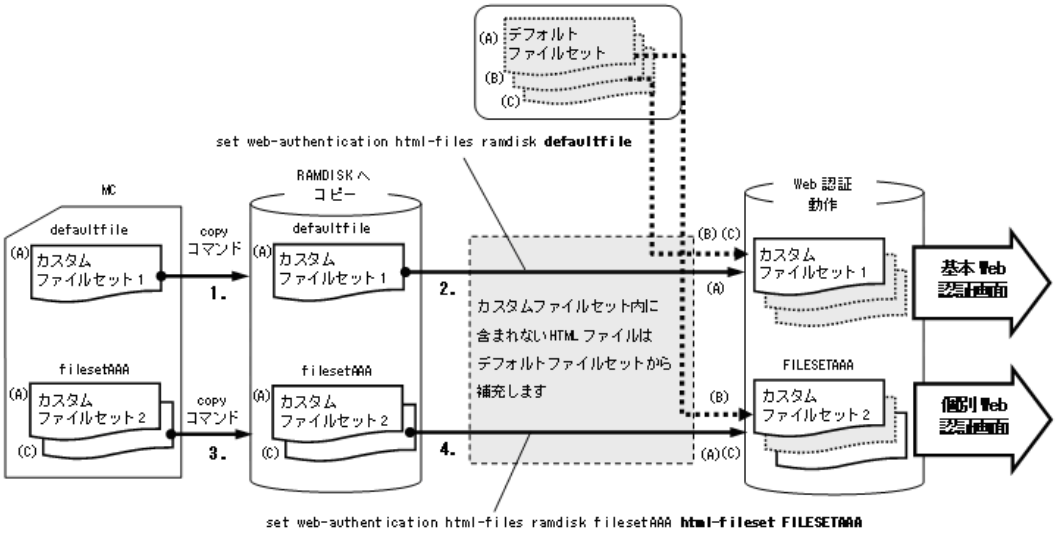
本装置には，「表 8-16 Web 認証画面入れ替え機能で使用する用語」に示す基本 Web 認証画面と個別 Web 認証画面をカスタムファイルセットとして登録できます。

- 基本 Web 認証画面のカスタムファイルセット
  運用コマンド set web-authentication html-files で指定した RAMDISK のファイルセットを本装置に登録し，現在動作中の基本 Web 認証画面をファイルセットの画面ファイルに置き換えます。また，画面ファイル以外に gif ファイルなどの画像ファイルも同時に登録できます。

- 個別 Web 認証画面のカスタムファイルセット
  基本 Web 認証画面と同様に運用コマンド set web-authentication html-files で本装置に登録しますが，html-fileset パラメータで指定したファイルセット名で本装置に個別に登録します。

MC に保存したカスタムファイルセットを個別 Web 認証画面として登録する手順について次の図に示します。個別 Web 認証画面は，基本 Web 認証画面のほかに最大 4 種類のファイルセットを登録することができます。

図 8-18　カスタムファイルセット登録手順



1. MC のカスタムファイルセット 1 （defaultfile）を，運用コマンド copy で本装置の RAMDISK へコピーします。
2. defaultfile は基本 Web 認証画面として使用するので，RAMDISK へコピーしておいたファイルセット名 defaultfile を指定します。（set web-authentication html-files ramdisk defaultfile）
   カスタムファイルセット内に含まれないファイル（上図の場合は (B)(C)）は，デフォルトファイルセットから補充します。
3. カスタムファイルセット 2 （filesetAAA）を，運用コマンド copy で本装置の RAMDISK へコピーします。
4. filesetAAA は個別 Web 認証画面として使用するので，RAMDISK へコピーしておいたファイルセット名 filesetAAA を本装置へ登録するファイルセット名（図では FILESETAAA）で指定します。（set web-authentication html-files ramdisk filesetAAA html-fileset FILESETAAA）
   カスタムファイルセット内に含まれないファイル（上図の場合は (B)）は，デフォルトファイルセットから補充します。

ただし，登録時には各ファイルのサイズチェックだけを行い，ファイルの内容はチェックしませんので，必ず動作確認を行ってから HTML ファイルや画像ファイルを登録してください。

登録できるカスタムファイルセットの合計サイズとファイル数については，「コンフィグレーションガイド Vol.1 3.2 収容条件」を参照してください。

なお，登録したカスタムファイルセットは運用コマンド clear web-authentication html-files で削除できます。削除したあとは，デフォルトファイルセットに戻ります。

また，「表 8-15　認証エラーメッセージとエラー発生理由対応表」に示す認証エラーメッセージや，Web ブラウザのお気に入りに表示するアイコン（favicon.ico）も入れ替えることができます。

運用コマンド set web-authentication html-files で登録した画面，メッセージ，およびアイコンは，装置再起動時にも保持されます。

各ファイルの詳細は，「8.9　Web 認証画面作成手引き」を参照してください。

8.8.2　Web 認証画面入れ替え機能使用時の注意事項

（1） 作成した Web 認証画面ファイルの保管と変更について

PC などで作成した Web 認証画面ファイルは，外部媒体などで保管しておいてください。Web 認証画面ファイルの変更は，あらかじめ保管しておいた Web 認証画面ファイルを編集し，本装置に登録してください。

なお，運用コマンド store web-authentication html-files により，本装置で動作中の Web 認証画面ファイルを取り出すことができます。取り出した Web 認証画面ファイルは，RAMDISK に一時的に格納されますので，ftp で PC へファイル転送するか，または運用コマンド copy で MC に格納してください。（本装置を再起動すると，RAMDISK 上のファイルは削除されます。）

（2） 作成した Web 認証画面ファイルの転送について

作成した Web 認証画面ファイルは，本装置の RAMDISK に転送します。転送方法は，ftp でファイル転送するか，または MC から運用コマンド copy でコピーしてください。

運用コマンド set web-authentication html-files で本装置に登録後，RAMDISK に転送した Web 認証画面ファイルは不要となりますので，運用コマンド del で削除してください。（本装置を再起動した場合も，RAMDISK 上のファイルは削除されます。）

8.9 Web 認証画面作成手引き

Web 認証画面入れ替え機能で入れ替えができる画面と対応するファイル名を次に示します。

- ログイン画面（ファイル名：login.html）
- ログアウト画面（ファイル名：logout.html）
- ログイン成功画面（ファイル名：loginOK.html）
- ログイン失敗画面（ファイル名：loginNG.html）
- ログアウト完了画面（ファイル名：logoutOK.html）
- ログアウト失敗画面（ファイル名：logoutNG.html）

各 Web 認証画面ファイルは HTML 形式で作成してください。

HTML 上には，JavaScript のようにクライアント端末上だけで動作する言語は使用可能ですが，サーバへアクセスするような言語は使用できません。また，perl などの CGI も指定しないでください。

ただし，ログイン画面，ログアウト画面では，Web 認証とのインタフェース用の記述が必要です。ログイン画面，ログアウト画面については，「8.9.1　ログイン画面（login.html）」，「8.9.2　ログアウト画面（logout.html）」を参照してください。

また，「表 8-15　認証エラーメッセージとエラー発生理由対応表」に示した認証エラーメッセージも置き換えることができます。使用できるファイル名は次のとおりです。ファイルの作成方法については，「8.9.3　認証エラーメッセージファイル（webauth.msg）」を参照してください。

- 認証エラーメッセージ（ファイル名：webauth.msg）

さらに，Web ブラウザのお気に入りに表示するアイコンも入れ替えることができます。

- Web ブラウザのお気に入りに表示するアイコン（ファイル名：favicon.ico）

注意

入れ替え可能な画面および認証エラーメッセージのファイル名は，必ず上記に示したファイル名と一致させてください。

8.9.1 ログイン画面（login.html）

Web 認証にログインする際，ユーザ ID とパスワードの入力をクライアントに対し要求する画面です。

（1） 設定条件

ログイン画面の HTML ファイルを作成する際は，次の表に示す記述を必ず入れてください。

表 8-18　ログイン画面に必要な設定

記述内容	意味
<form name="Login" method="post" action="/cgi-bin/Login.cgi"></form>	ログイン操作を Web 認証に指示するための記述です。この記述は変更しないでください。
<input name="uid" size="40" maxlength="128" autocomplete="OFF" type="text">	ユーザ ID を指定するための記述です。size と maxlength 以外の記述は変更しないでください。上記 <form></form> の内部に設定してください。また，maxlength は必ず 6 以上の数字を設定してください。

記述内容	意味
<input name="pwd" size="40" maxlength="32" autocomplete="OFF" type="password">	パスワードを指定するための記述です。size と maxlength 以外の記述は変更しないでください。上記 <form></form> の内部に設定してください。また，maxlength は必ず 6 以上の数字を設定してください。
<input value="Login" type="submit">	Web 認証にログイン要求を行うために記述です。この記述は変更しないでください。上記 <form></form> の内部に設定してください。

ログイン・ログアウト共通画面で作成する際は，「表 8-19　ログアウト画面に必要な設定」も参照してください。

注意

login.html ファイルに，ほかのファイルを関連付ける場合は，関連付けするファイル名の先頭に ”/” （スラッシュ）を記述してください。

（例）　< img src="/image_file.gif" >

（2） 設定例

ログイン画面（login.html）のソース例を次の図に示します。

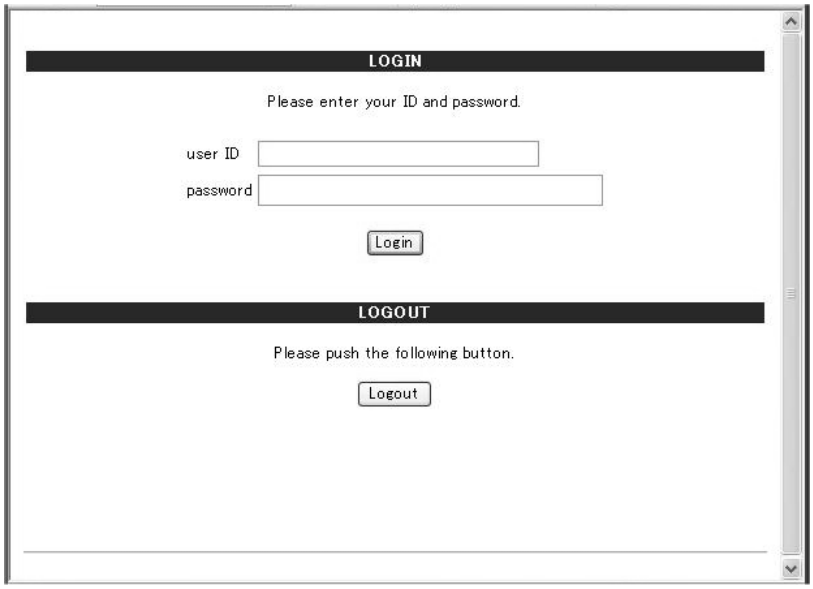
図 8-19　ログイン画面（login.html）のソース例

```
<?xml version="1.0" encoding="euc-jp"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="ja" lang="ja">
<head>

 <meta http-equiv="Pragma" content="no-cache">
 <meta http-equiv="Cache-Control" content="no-cache">
 <meta http-equiv="Expires" content="Thu, 01 Dec 1994 16:00:00 GMT">
 <title> </title>
</head>

<body oncontextmenu="return false;">
<!-- === Body === -->
<center>
<br>
<table width="100%">
 <tbody><tr><td align="center" bgcolor="#2b1872">
 <font color="#ffffff"><b>LOGIN</b></font>
 </td></tr></tbody>
</table>
<br>
Please enter your ID and password.<br>
<br>

<form name="Login" method="post" action="/cgi-bin/Login.cgi">
<table><tbody><tr>                          ログイン操作を Web 認証に指示するための記述
 <td>user ID</td>
 <td><input name="uid" size="40" maxlength="128" autocomplete="OFF" type="text"></td></tr>
<tr>                                        ユーザ ID 指定のための記述
 <td>password</td>
 <td><input name="pwd" size="40" maxlength="32" autocomplete="OFF" type="password"></td></tr>
</tbody></table>                            パスワード指定のための記述
<br>
<input value="Login" type="submit">         Web 認証にログイン要求を行うための記述
</form>
<br>
<form name="Logout" action="/cgi-bin/Logout.cgi" method="post">
<table width="100%">                        ログアウト操作を Web 認証に指示するための記述
 <tbody>
  <tr>
    <td align="center" bgcolor="#2b1872"><font color="#ffffff"><b>LOGOUT</b></font>
   </td></tr>
 </tbody>
</table>
 <br>Please push the following button.<br><br>
   <input value="Logout" type="submit">     Web 認証にログアウト要求を行うための記述
</form>
<br>
<br>
<br>
<br>
<br>
<br>
</center>
<!-- === Footer === -->
<hr>
<div align="right"></div>
</body>
</html>
```

(3) ログイン画面表示例

ログイン画面の表示例を次の図に示します。(ログインとログアウト共通画面の例です。)

図 8-20 ログイン画面の表示例



8.9.2 ログアウト画面(logout.html)

Web 認証機能でログインしているクライアントがログアウトを要求するための画面です。

(1) 設定条件

ログアウト画面の HTML ファイルを作成する際は,次の表に示す記述を必ず入れてください。

表 8-19 ログアウト画面に必要な設定

記述内容	意味
<form name="Logout" action="/cgi-bin/Logout.cgi" method="post" ></form>	ログアウト操作を Web 認証に指示するための記述です。この記述は変更しないでください。
<input value="Logout" type="submit">	Web 認証にログアウト要求を行うために記述です。この記述は変更しないでください。上記 <form></form> の内部に設定してください。

注意

logout.html ファイルに,ほかのファイルを関連付ける場合は,関連付けするファイル名の先頭に "/" (スラッシュ)を記述してください。

(例) < img src="/image_file.gif" >

（2） 設定例

ログアウト画面（logout.html）のソース例を次の図に示します。

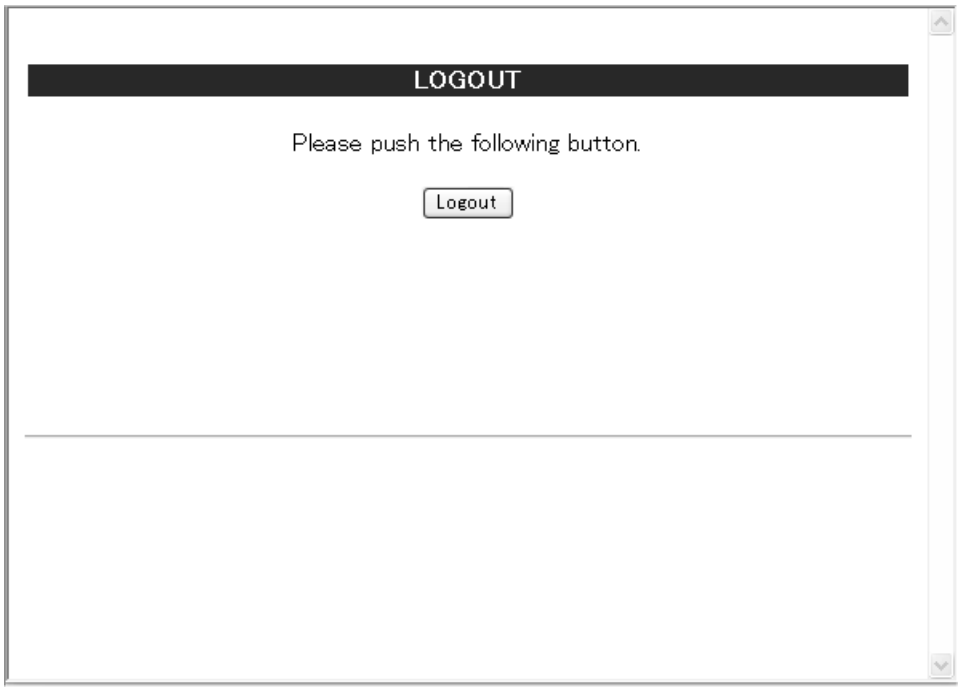
図 8-21　ログアウト画面（logout.html）のソース例

```
<?xml version="1.0" encoding="euc-jp"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="ja" lang="ja">
<head>

 <meta http-equiv="Pragma" content="no-cache">
 <meta http-equiv="Cache-Control" content="no-cache">
 <meta http-equiv="Expires" content="Thu, 01 Dec 1994 16:00:00 GMT">
 <title> </title>
</head>

<body oncontextmenu="return false;">
<!-- ===== Body ===== -->
<center>
<br>
<form name="Logout" action="/cgi-bin/Logout.cgi" method="post">
<table width="100%">          ログアウト操作を Web 認証に指示するための記述
  <tbody>
  <tr>
    <td align="center" bgColor="#2b1872"><font color="#ffffff"><b>LOGOUT</b></font>
    </td>
  </tr>
 </tbody>
</table>
 <br>Please push the following button.<br><br>
   <input value="Logout" type="submit">
</form>                       Web 認証にログアウト要求を行うための記述
<br><br><br><br><br><br>
</center>
<!-- ===== Footer ===== -->
<hr>

<div align="right"></div>
</body>
</html>
```

(3) ログアウト画面表示例

ログアウト画面の表示例を次の図に示します。

図 8-22 ログアウト画面の表示例



8.9.3 認証エラーメッセージファイル（webauth.msg）

認証エラーメッセージファイル（webauth.msg）は，Web 認証ログインまたは Web 認証ログアウトの失敗時に応答画面で表示するメッセージ群を格納したファイルです。

デフォルト設定の認証エラーメッセージを入れ替える際は，次の表に示す 9 行のメッセージを格納した認証エラーメッセージファイルを作成してください。

表 8-20 認証エラーメッセージファイルの各行の内容

行番号	内容
1 行目	ログイン時，ユーザ ID またはパスワード記述を誤った場合，もしくは Web 認証 DB による認証エラーとなった場合に出力するメッセージ。 [デフォルトメッセージ] “User ID or password is wrong. Please enter correct user ID and password.”
2 行目	Radius による認証エラーとなった場合に出力するメッセージ。 [デフォルトメッセージ] “RADIUS: Authentication reject.”
3 行目	コンフィグレーション上，Radius 認証の設定となっているが，Radius サーバと本装置との接続が確立していない場合に出力するメッセージ。 [デフォルトメッセージ] “RADIUS: No authentication response.”
4 行目	本装置のコンフィグレーションの設定誤り，または他機能との競合のためにログインできない場合に出力するメッセージ。 [デフォルトメッセージ] “You cannot login by this machine.”

行番号	内容
5 行目	プログラムの軽度の障害が発生した場合に出力するメッセージ。 ［デフォルトメッセージ］ “Sorry, you cannot login just now. Please try again after a while.”
6 行目	プログラムの中度の障害が発生した場合に出力するメッセージ。 ［デフォルトメッセージ］ “The system error occurred. Please contact the system administrator.”
7 行目	プログラムの重度の障害が発生した場合に出力するメッセージ。 ［デフォルトメッセージ］ “A fatal error occurred. Please inform the system administrator.”
8 行目	ログアウト処理で CPU 高負荷などによって，ログアウトが失敗した場合に出力するメッセージ。 ［デフォルトメッセージ］ “Sorry, you cannot logout just now. Please try again after a while.”
9 行目	ログインしていないユーザがログアウトした場合に出力するメッセージ。 ［デフォルトメッセージ］ “The client PC is not authenticated.”

(1) 設定条件

- 改行だけの行があった場合は，デフォルトのエラーメッセージを表示します。
- ファイル保存時は，改行コードを ”CR+LF” または ”LF” のどちらかで保存してください。
- 1 行に書き込めるメッセージ長は，半角 512 文字（全角 256 文字）までです。ここで示している文字数には html タグ，改行タグ ”
” も含みます。なお，半角 512 文字を超えた文字については無視します。
- 認証エラーメッセージファイルが 10 行以上あった場合は，10 行目以降の内容は無視します。

(2) 認証エラーメッセージファイル作成のポイント

- 認証エラーメッセージファイル上に記述したテキストは，そのまま HTML テキストとして使用します。従って，認証エラーメッセージ上に HTML のタグを記述すると，そのタグの動作を行います。
- 1 メッセージは 1 行で記述する必要があるため，エラーメッセージの表示イメージに改行を入れたい場合は，改行したい個所に HTML の改行タグ ”
” を挿入してください。

(3) 設定例

認証エラーメッセージファイル（webauth.msg）のソース例を次の図に示します。

図 8-23 認証エラーメッセージファイル（webauth.msg）のソース例

```
ユーザID又はパスワードが不正です
パスワードが不正です
認証サーバが見つかりません<BR>システム管理者に問い合わせてください。
システムの設定に誤りがあります<BR>システム管理者に問い合わせてください。
システム障害発生（minor）<BR>しばらくしてから再度ログインをしてください。
システム障害発生（major）<BR>システム管理者に問い合わせてください。
システム障害発生（critical）<BR>システム管理者に問い合わせてください。
システムが高負荷状態です<BR>しばらくしてからログアウトしてください。
ログインしていません
```

(4) 表示例

上記の認証エラーメッセージファイルを使用し，パスワード長不正により，ログインに失敗したときのログイン失敗画面の表示例を次の図に示します。

図 8-24 ログイン失敗画面の表示例（パスワード長不正）

8.9.4 Web 認証固有タグ

（1） Web 認証固有タグの種類

Web 認証画面の HTML ファイルに Web 認証固有タグを書き込むことで，Web 認証固有タグ部分を当該情報に変換します。

HTML ファイルの記述内容によって，認証画面上にログイン時刻やエラーメッセージを表示したり，Web ブラウザ上で動作する任意アプリケーションにて当該情報を認識することが可能です。

表 8-21 Web 認証固有タグ種別と変換情報

Web 認証固有タグ	変換後文字列の例	変換情報
<!-- Login_Time -->	"2010/08/20 19:56:01 UTC"	ログインが成功した時刻
<!-- Logout_Time -->	"2010/08/20 20:56:01 UTC"	ログアウト時刻 ※1
<!-- After_Vlan -->	"100"	ログイン成功後の VLAN ID
<!-- Error_Message -->	" ユーザ ID 又はパスワードが不正です "	エラーメッセージ ※2
<!-- Redirect_URL -->	"http://www.example.com"	認証成功後の自動表示 URL
<!-- Original_URL -->	"http://www.original.com"	リダイレクト前 URL

注 ※1

表示画面によって意味が異なります。
ログイン成功画面　：最大接続時間が満了しログアウトする予定の時刻。
ログアウト完了画面：ログアウト動作が完了した時刻。

注 ※2

ログインまたはログアウトが失敗した場合のエラー要因。

設定例については，「8.9.5　その他の画面サンプル」を参照してください。

各 Web 認証固有タグと当該情報の変換処理が有効となる画面の組み合わせを次の表に示します。

表 8-22 Web 認証固有タグと変更が有効となる画面の組み合わせ

Web 認証固有タグ	変換が有効となる画面（変換対象画面）					
	ログイン画面	ログアウト画面	ログイン成功画面	ログイン失敗画面	ログアウト完了画面	ログアウト失敗画面
<!-- Login_Time -->	－	－	○	－	－	－
<!-- Logout_Time -->	－	－	○	－	○	－
<!-- After_Vlan -->	－	－	○	－	－	－
<!-- Error_Message -->	－	－	－	○	－	○
<!-- Redirect_URL -->	－	－	○	－	－	－
<!-- Original_URL -->	○	－	－	－	－	－

（凡例）

○：HTML ファイル内に Web 認証固有タグが含まれている場合に，当該情報に変換する。

－：HTML ファイル内に Web 認証固有タグが含まれていても，当該情報に変換しない。

（2） 注意事項

（a） Web 認証のデフォルト HTML ファイルについて

Web 認証のデフォルト HTML ファイルには，あらかじめ Web 認証固有タグが含まれており，当該情報を Web ブラウザ上に表示しています。

例外として，ログイン成功後の VLAN ID に変換する固有タグ（"<!-- After_Vlan -->"）は，デフォルト HTML ファイルに下記の記述で埋め込まれているため，Web ブラウザ上には表示しません。

【ログイン成功画面にデフォルトで記述されている HTML(loginOK.html)】

<meta name="vlan-id" content="<!-- After_Vlan -->" />

※：メタタグは付加情報の位置づけのため一般的な Web ブラウザには表示しません。

Web ブラウザ上にログイン成功後 VLAN ID を表示したい場合は，ログイン成功後画面ファイル（loginOK.html ファイル）を任意に作成し，「8.8.1 Web 認証画面入れ替え機能」にてログイン成功後画面に表示することができます。

（b） スペース（空白文字）の扱いについて

各 Web 認証固有タグに含まれるスペースは，キーワード間のセパレータとして認識されます。キーワードはスペースを含まず連続していなければいけませんが，それぞれのキーワード間のスペースは 1 文字以上であれば正常にセパレータとして処理されます。

ただし，Web 認証固有タグを認識可能な最大文字数は，"<" から ">" までの文字列で（"<" および ">" を含め）80 文字以内です。

【キーワード】

1. "<!--"
2. "Login_Time"，"Logout_Time"，"After_Vlan"，"Error_Message"
3. "-->"

8.9.5 その他の画面サンプル

Web 認証画面（loginOK.html，logoutOK.html，loginNG.html，logoutNG.html）のサンプルソースを示します。

（1） ログイン成功画面（loginOK.html）

ログイン成功画面のソース例および表示例を次の図に示します。

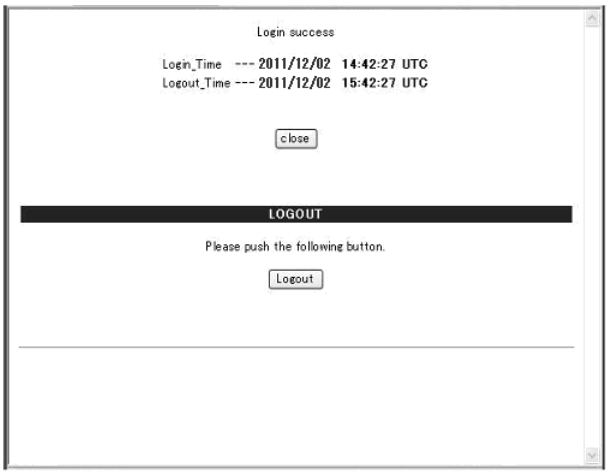
図 8-25 ログイン成功画面のソース例（loginOK.html）

```
<?xml version="1.0" encoding="euc-jp"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="ja" lang="ja">
<head>
  <title> </title>
  <meta name="vlan-id" content="<!-- After_Vlan -->" />
</head>                                  ログイン成功後の VLAN ID タグ

<body oncontextmenu="return false;">
<!-- === Body === -->
<center>
Login success
<br>
<br>
<table border="0">
<tbody>
 <tr>
  <td align="left">Login_Time</td>
  <td align="left"> -- </td>
  <td align="left"><b><!-- Login_Time --></b></td>
 </tr>                       ログイン時刻表示タグ
 <tr>
  <td align="left">Logout_Time</td>
  <td align="left"> -- </td>
  <td align="left"><b><!-- Logout_Time --></b></td>
 </tr>                       ログアウト時刻表示タグ
</tboby>
</table>
<b><!-- Redirect_URL --></b>
<br>
        認証成功後の自動表示 URL タグ
<br>
<form>
 <input value="close" onclick="window.close()" type="button">
</form><br>
<br>
<form name="Logout" action="/cgi-bin/Logout.cgi" method="post">
 <table width="100%">
  <tbody>
  <tr>
    <td align="center" bgcolor="#2b1872"><font color="#ffffff"><b>LOGOUT</b></font>
    </td>
  </tr>
  </tbody>
 </table>
 <br>Please push the following button.<br><br>
    <input value="Logout" type="submit">
</form>
<br>
</center>
<br>

<!-- === Footer === -->
<hr>
<div align="right"></div>

</body>
</html>
```

注意

- loginOK.html ファイルに，ほかのファイルを関連付ける場合は，関連付けするファイル名の先頭に”/”（スラッシュ）を記述してください。
  （例） < img src="/image_file.gif" >
- ダイナミック VLAN モードにおいて，loginOK.html ファイルに，ほかのファイルを関連付けしたとき，ログイン成功画面が正常に表示されない場合があります。

図 8-26 ログイン成功画面の表示例



（2） ログアウト完了画面（logoutOK.html）

ログアウト完了画面のソース例および表示例を次の図に示します。

図 8-27 ログアウト完了画面のソース例（logoutOK.html）

```
<?xml version="1.0" encoding="euc-jp"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="ja" lang="ja">
<head>
 <title> </title>
</head>
<body oncontextmenu="return false;">
<!-- ===== Body ===== -->
<center>
Logout success
<br>
<br>
Logout Time --- <b><!-- Logout_Time --></b>
<br>
<br>
<br>

<form>
 <input value="close" onclick="window.close()" type="button">
</form>

<br>
<br>
</center>

<!-- ===== Footer ===== -->
<hr>
<div align="right"></div>
</body></html>
```

ログアウト時刻表示タグ

注意

logoutOK.html ファイルに，ほかのファイルを関連付ける場合は，関連付けするファイル名の先頭に”/”（スラッシュ）を記述してください。

（例） ＜ img src="/image_file.gif" ＞

図 8-28 ログアウト完了画面の表示例

（3） ログイン／ログアウト失敗画面（loginNG.html / logoutNG.html）

ログイン／ログアウト失敗画面のソース例および表示例を次の図に示します。

図 8-29 ログイン失敗画面のソース例（loginNG.html ）

```
<?xml version="1.0" encoding="euc-jp"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="ja" lang="ja">
<head>
<title> </title>
</head>

<body oncontextmenu="return false;">
<!-- ===== Body ===== -->
<center>
<br>
 <i style="color: red;"><b><!-- Error_Message --></b></i>
<br>
<br>
<br>
<br>

<form>
 <input value="login page" onclick="window.location.href='/login.html'" type="button">
 <input value="close" onclick="window.close()" type="button">
</form>

<br>
</center>
<!-- ===== Footer ===== -->
<hr>
<div align="right"></div>
</body>
</html>
```

エラーメッセージ表示タグ

図 8-30　ログアウト失敗画面のソース例（logoutNG.html）

```
<?xml version="1.0" encoding="euc-jp"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="ja" lang="ja">
<head>
<title> </title>
</head>

<body oncontextmenu="return false;">
<!-- ===== Body ===== -->
<center>
<br>
 <i style="color: red;"><b><!-- Error_Message --></b></i>
<br>
<br>
<br>
<br>

<form>
 <input value="back" onclick="history.back()" type="button">
 <input value="close" onclick="window.close()" type="button">
</form>

<br>
</center>
<!-- ===== Footer ===== -->
<hr>
<div align="right"></div>
</body>
</html>
```

エラーメッセージ表示タグ

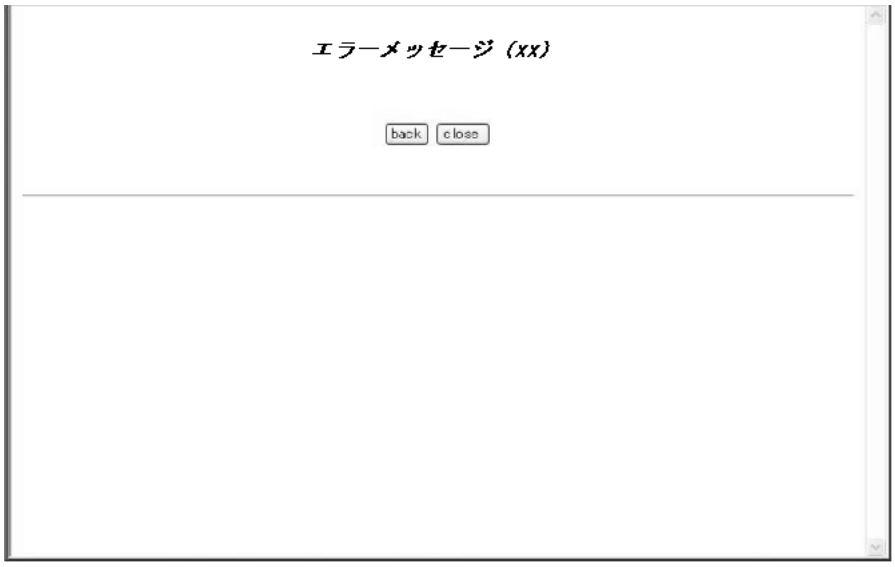
注意

loginNG.html，logoutNG.html ファイルに，ほかのファイルを関連付ける場合は，関連付けするファイル名の先頭に ”/”（スラッシュ）を記述してください。

（例）　< img src="/image_file.gif" >

図 8-31　ログイン失敗画面の表示例

図 8-32　ログアウト失敗画面の表示例



9 Web 認証の設定と運用

Web 認証は，汎用 Web ブラウザを用いて認証されたユーザ単位に VLAN へのアクセス制御を行う機能です。この章では Web 認証の設定と運用について説明します。

9.1 Web 認証のコンフィグレーション

9.1.1 コンフィグレーションコマンド一覧

Web 認証のコンフィグレーションコマンドと認証モード一覧を次の表に示します。

表 9-1 コンフィグレーションコマンドと認証モード一覧

コマンド名	説明	認証モード	
		固	ダ
aaa accounting web-authentication	Web 認証 のアカウンティング情報をアカウンティングサーバへ送信します。	○	○
aaa authentication web-authentication	Web 認証の認証方式グループを設定します。	○	○
aaa authentication web-authentication end-by-reject	ログイン時の認証で否認された場合に，認証を終了します。通信不可（RADIUS サーバ無応答など）による認証失敗時は，コンフィグレーションコマンド aaa authentication web-authentication で次に指定されている認証方式で認証します。	○	○
authentication arp-relay	コマンドおよび設定の詳細などについては，「5　レイヤ 2 認証機能の概説」を参照。	○	○
authentication ip access-group	コマンドおよび設定の詳細などについては，「5　レイヤ 2 認証機能の概説」を参照。	○	○
http-server initial-timeout	HTTP サーバの初期タイムアウト時間を設定します。	○	○
web-authentication authentication	ポート別認証方式の認証方式リスト名を設定します。	○	○
web-authentication auto-logout	no web-authentication auto-logout コマンドで，Web 認証で認証された端末から一定時間フレームを受信しなかった状態を検出したときに認証を自動ログアウトする設定を無効にします。	○	○
web-authentication html-fileset	ポートごとに表示する個別 Web 認証画面のカスタムファイルセット名を設定します。	○	○
web-authentication ip address	Web 認証専用 IP アドレスとドメイン名を設定します。	○	○
web-authentication jump-url	ログイン成功画面表示後，自動的に表示する URL と URL 移動までの時間を指定します。	○	○
web-authentication logging enable	Web 認証の動作ログに出力する情報を syslog サーバへ出力します。	○	○
web-authentication logout ping tos-windows	認証済み端末から特殊フレーム（ping）を受信した場合，該当する MAC アドレスの認証状態を解除する特殊フレームの TOS 値を設定します。	○	○
web-authentication logout ping ttl	認証済み端末から特殊フレーム（ping）を受信した場合，該当する MAC アドレスの認証状態を解除する特殊フレームの TTL 値を設定します。	○	○
web-authentication logout polling count	認証済み端末の接続状態を周期的に監視する監視用フレームの応答で，無応答を検出時に再送する送信回数を設定します。	○	－
web-authentication logout polling enable	no web-authentication logout polling enable コマンドで，一定周期による接続監視で認証済み端末の未接続を検出したときの自動ログアウトを無効に設定します。	○	－
web-authentication logout polling interval	認証済み端末の接続状態を周期的に監視する，監視用フレームのポーリング間隔を設定します。	○	－
web-authentication logout polling retry-interval	認証済み端末の接続状態を周期的に監視する監視用フレームの応答で，無応答を検出時に再送する送信間隔を設定します。	○	－

コマンド名	説明	認証モード	
		固	ダ
web-authentication max-timer	最大接続時間を設定します。	○	○
web-authentication port※	ポートに認証モードを設定します。	○	○
web-authentication prefilter	no web-authentication prefilter を設定時，Web 認証プレフィルタを無効にします。	○	○
web-authentication radius-server host	Web 認証専用の RADIUS サーバ情報を設定します。	○	○
web-authentication radius-server dead-interval	Web 認証専用の RADIUS サーバ使用時，プライマリ RADIUS サーバへ自動復旧するまでの監視タイマを設定します。	○	○
web-authentication redirect-mode	URL リダイレクト機能有効時，Web 認証のログイン画面を表示させるプロトコルを設定します。	○	○
web-authentication redirect enable	no web-authentication redirect enable コマンドで，URL リダイレクト機能を無効に設定します。	○	○
web-authentication redirect ignore-https	HTTPS リクエストに対する URL リダイレクトを抑止します。	○	○
web-authentication redirect polling	外部 Web サーバの生死監視を実施し，障害時には本装置の Web サーバにリダイレクトします。	○	○
web-authentication redirect queries	本装置や認証端末に関するパラメータをリダイレクト先（外部 Web サーバ）の URL にクエリとして付加します。	○	○
web-authentication redirect target	URL リダイレクト機能におけるリダイレクト先を，指定された外部 Web サーバに変更します。	○	○
web-authentication roaming	HUB などを経由して接続した認証済み端末を，リンクダウンしないでポート移動した場合の通信許可（ローミング）を設定します。	－	○
web-authentication static-vlan roaming	HUB などを経由して接続した認証済み端末を，リンクダウンしないでポート移動した場合の通信許可（ローミング）を設定します。	○	－
web-authentication system-auth-control	Web 認証を有効にします。	○	○
web-authentication user-group	ユーザ ID 別認証方式を有効にします。	○	○
web-authentication user replacement	ユーザ切替オプションを有効にします。 1 台の端末を複数のユーザ ID で使用する場合，最初のユーザ ID で認証成功後に別のユーザ ID で認証が可能となります。	○	○
web-authentication web-port	URL リダイレクト機能有効時，本装置で URL リダイレクト対象とするフレームの TCP 宛先ポート番号を追加設定します。	○	○

（凡例）

固：固定 VLAN モード

ダ：ダイナミック VLAN モード

○：設定内容に従って動作します

－：コマンドは入力できますが，動作しません

×：コマンドを入力できません

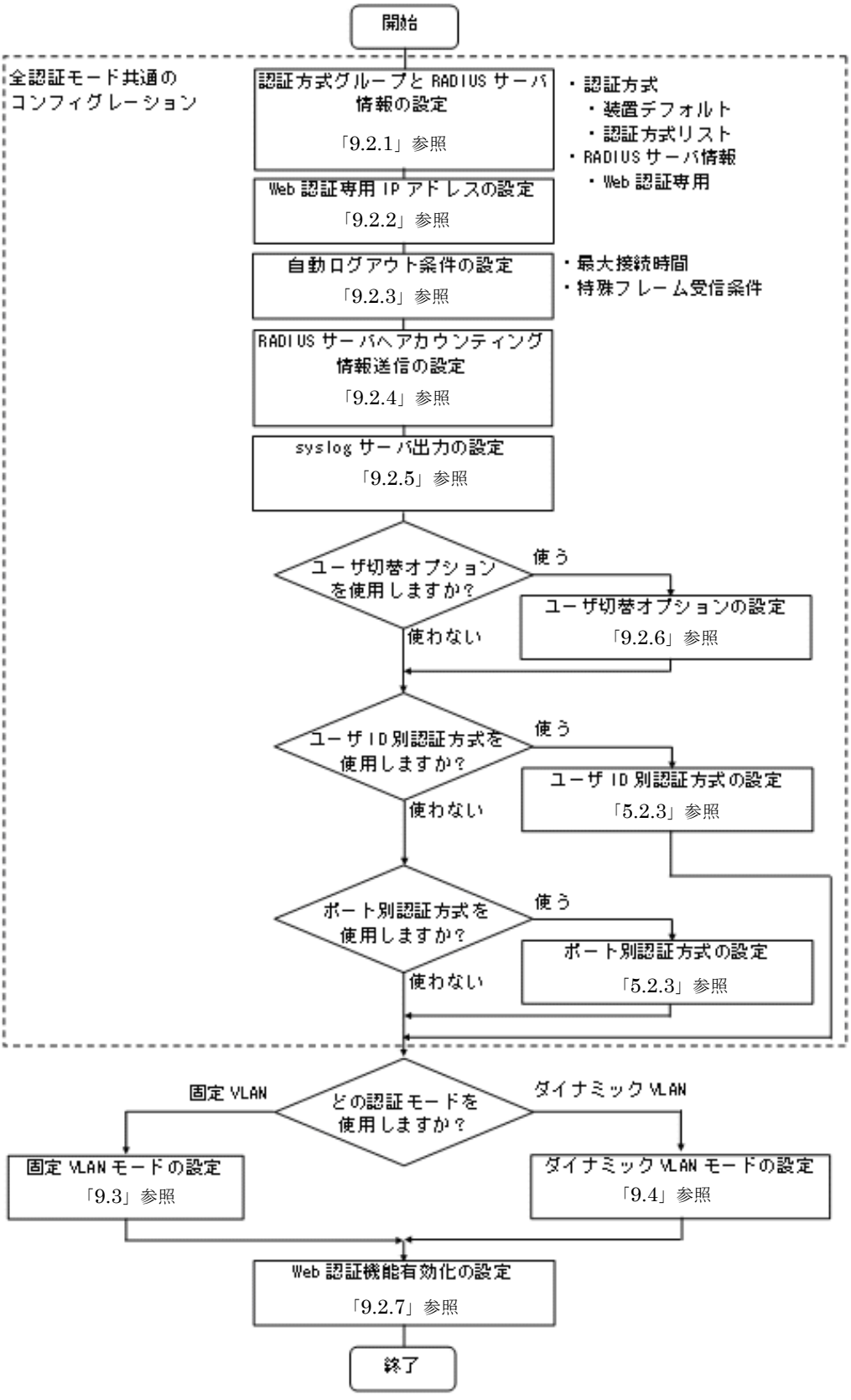
注 ※

本コマンドの設定は，認証モードの切り替えに影響します。

9.1.2 Web 認証の設定手順

Web 認証は，下記の手順で設定してください。

図 9-1 Web 認証の設定手順



各設定の詳細は，下記を参照してください。

1. 全認証モード共通のコンフィグレーション
   全認証モード共通のコンフィグレーションを設定します。
   - 認証方式グループと RADIUS サーバ情報の設定：「9.2.1　認証方式グループと RADIUS サーバ情報の設定」
   - Web 認証専用 IP アドレスの設定：「9.2.2　Web 認証専用 IP アドレスの設定」
   - 認証モード共通の自動ログアウト条件の設定：「9.2.3　認証モード共通の自動ログアウト条件の設定」
   - RADIUS サーバへアカウンティング情報送信の設定：「9.2.4　アカウンティング情報送信の設定」
   - syslog サーバへの出力設定：「9.2.5　syslog サーバ出力設定」
   - ユーザ切替オプションの設定：「9.2.6　ユーザ切替オプションの設定」
   - ユーザ ID 別認証方式の設定：「5.2.3　認証方式リストのコンフィグレーション（3）ユーザ ID 別認証方式の設定例」
   - ポート別認証方式の設定：「5.2.3　認証方式リストのコンフィグレーション（2）ポート別認証方式の設定例」
2. 各認証モードの設定
   各認証モードのコンフィグレーションを設定します。
   設定項目によっては，他の認証モードと共通になる場合があります。これについては「～を参照してください。」と記載していますので，該当箇所を参照してください。
   - 固定 VLAN モードの設定：「9.3　固定 VLAN モードのコンフィグレーション」
   - ダイナミック VLAN モードの設定：「9.4　ダイナミック VLAN モードのコンフィグレーション」
3. Web 認証機能の有効化
   最後に Web 認証機能を有効設定して，Web 認証の設定は終了です。
   - 「9.2.7　Web 認証機能の有効化」

各認証モードは下記のコンフィグレーション設定で有効となります。

表 9-2　各認証モード有効条件

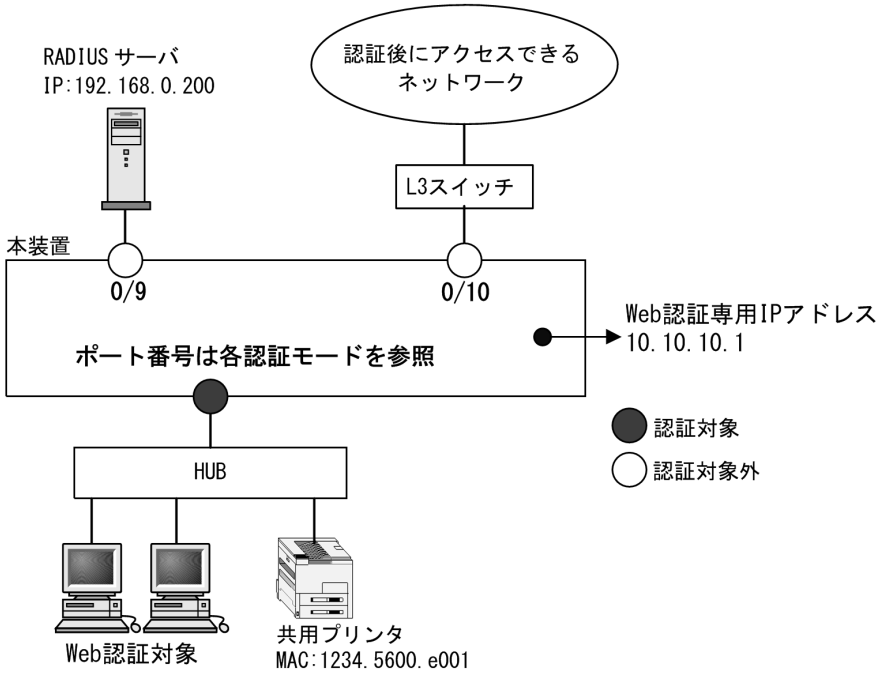
認証モード	コンフィグレーション設定
共通	• aaa authentication web-authentication • web-authentication radius-server host または radius-server • web-authentication system-auth-control
固定 VLAN モード	アクセスポートで使用する場合 • vlan <VLAN ID list> • web-authentication port • switchport mode access • switchport access vlan トランクポートで使用する場合 • vlan <VLAN ID list> • web-authentication port • switchport mode trunk • switchport trunk allowed vlan • switchport trunk native vlan

認証モード	コンフィグレーション設定
	MAC ポートで使用する場合 • vlan <VLAN ID list> または vlan <VLAN ID list> mac-based • web-authentication port • switchport mode mac-vlan • switchport mac dot1q vlan
ダイナミック VLAN モード	• vlan <VLAN ID list> mac-based • web-authentication port • switchport mode mac-vlan

9.2　全認証モード共通のコンフィグレーション

本章では，下記の基本構成を基に各認証モードの設定を説明します。RADIUS サーバと認証後ネットワーク用のポート番号は 0/9，0/10 を例として使用します。認証対象端末を接続するポート番号は，各認証モードの設定例を参照してください。

図 9-2　基本構成



9.2.1　認証方式グループと RADIUS サーバ情報の設定

(1) 認証方式グループの設定

[設定のポイント]

Web 認証の認証方式グループを設定します。

Web 認証共通で使用する装置デフォルトを 1 エントリ，認証ポートで使用する認証方式リストを 2 エントリ設定します。

1. 装置デフォルト

   本例では，装置デフォルトの認証方式を RADIUS 認証とローカル認証とし，通信不可（RADIUS サーバ無応答など）により RADIUS 認証に失敗したときは，ローカル認証を実行するよう設定します。

   なお，RADIUS 認証否認によって認証に失敗した場合には，その時点で認証を終了し，ローカル認証を行いません。

   - ローカル認証方式は内蔵 Web 認証 DB を使用します。「9.5.2　内蔵 Web 認証 DB の登録」を参照して，本装置に内蔵 Web 認証 DB を登録してください。

2. 認証方式リスト

   認証方式リストに指定する RADIUS サーバグループ情報は，"Keneki-group1" と "Keneki-group2" を設定済みとします。

   認証方式リストについては「5.2.2　認証方式リスト」を参照してください。

RADIUS サーバグループ情報については，「5.3.1　レイヤ 2 認証機能で使用する RADIUS サーバ情報」「コンフィグレーションガイド Vol.1 10 ログインセキュリティと RADIUS」を参照してください。

［コマンドによる設定］

1. **(config)# aaa authentication web-authentication default group radius local**
   装置デフォルトの認証方式は，RADIUS 認証方式，ローカル認証方式の順番に設定します。
2. **(config)# aaa authentication web-authentication end-by-reject**
   RADIUS 認証で否認された場合には，その時点で認証を終了し，ローカル認証を行わないように設定します。
3. **(config)# aaa authentication web-authentication WEB-list1 group Keneki-group1**
   認証方式リスト "WEB-list1" に，RADIUS サーバグループ名 "Keneki-group1" を設定します。
4. **(config)# aaa authentication web-authentication WEB-list2 group Keneki-group2**
   認証方式リスト "WEB-list2" に，RADIUS サーバグループ名 "Keneki-group2" を設定します。

［注意事項］

- 装置デフォルトを設定変更したときは，装置デフォルトの認証方式で認証した端末を認証解除します。
- 認証方式リストを設定変更したときは，当該認証方式リストで認証した端末を認証解除します。
- aaa authentication web-authentication 設定省略時はローカル認証方式となります。
- 強制認証機能を使用するときは，上記コマンドで「default group radius」だけ設定してください。ローカル認証だけ，または RADIUS 認証とローカル認証の優先順を設定（上記のような設定）したときは使用できません。
- aaa authentication web-authentication end-by-reject を設定変更したときは，Web 認証の認証済み端末を認証解除します。

（2） RADIUS サーバ情報の設定

（a） Web 認証専用 RADIUS サーバを使用する場合

［設定のポイント］

Web 認証だけで使用する認証専用 RADIUS サーバ情報を設定します。
RADIUS サーバ設定を有効にするためには，IP アドレスと RADIUS 鍵の設定が必要です。コンフィグレーションコマンド web-authentication radius-server host では IP アドレスだけの設定も可能ですが，RADIUS 鍵を設定するまでは認証に使用されません。
また，本例では使用不可状態になった Web 認証専用 RADIUS サーバを，自動復旧する監視タイマ（dead-interval 時間）も設定します。

［コマンドによる設定］

1. **(config)# web-authentication radius-server host 192.168.10.201 key "web-auth"**
   Web 認証だけで使用する RADIUS サーバの IP アドレスおよび RADIUS 鍵を設定します。この場合，auth-port，acct-port，timeout，retransmit は省略時の初期値が適用されます。

2. **(config)# web-authentication radius-server dead-interval 15**
   設定した Web 認証専用 RADIUS サーバが使用不可状態になったときに，自動復旧までの監視タイマ（dead-interval 時間）を 15 分に設定します。

［注意事項］

- 本情報未設定時は，汎用 RADIUS サーバ情報の設定に従います。Web 認証専用 RADIUS サーバ情

報と汎用 RADIUS サーバ情報の両方未設定のときは，RADIUS 認証を実施できません。
- Web 認証専用 RADIUS サーバ情報は，最大４エントリまで設定できます。
- RADIUS 鍵，再送回数，応答タイムアウト時間を省略したときは，それぞれコンフィグレーションコマンド radius-server key，radius-server retransmit，radius-server timeout の設定に従います。

(b) 汎用 RADIUS サーバを使用する場合

汎用 RADIUS サーバの設定については，「コンフィグレーションガイド Vol.1 10 ログインセキュリティと RADIUS」を参照してください。

9.2.2 Web 認証専用 IP アドレスの設定

[設定のポイント]

Web 認証専用の IP アドレスとドメイン名を設定します。

[コマンドによる設定]

1. **(config)# web-authentication ip address 10.10.10.1 fqdn ax260a.example.com**
   Web 認証専用の IP アドレス（10.10.10.1）とドメイン名を設定します。

9.2.3 認証モード共通の自動ログアウト条件の設定

(1) 最大接続時間の設定

[設定のポイント]

認証済みユーザの最大接続時間を設定します。最大接続時間を超過すると，自動的にログアウトします。

[コマンドによる設定]

1. **(config)# web-authentication max-timer 60**
   認証済みユーザの最大接続時間を 60 分に設定します。

(2) 特殊フレーム受信によるログアウト条件の設定

[設定のポイント]

認証済みの端末からの特殊フレーム受信によるログアウト条件を設定します。

[コマンドによる設定]

1. **(config)# web-authentication logout ping tos-windows 2**
   (config)# web-authentication logout ping ttl 2
   設定した TOS 値および TTL 値の両条件に一致した場合だけ，当該 MAC アドレスの端末を自動ログアウトします。

9.2.4 アカウンティング情報送信の設定

[設定のポイント]

Web 認証のアカウンティング情報を RADIUS サーバへ送信するよう設定します。

［コマンドによる設定］

1. **(config)# aaa accounting web-authentication default start-stop group radius**
RADIUS サーバへアカウンティング情報を送信するよう設定します。

9.2.5 syslog サーバ出力設定

動作ログの syslog サーバへの出力を設定します。

［設定のポイント］
Web 認証の認証情報および動作情報を記録した動作ログを，syslog サーバへ出力する設定をします。

［コマンドによる設定］

1. **(config)# web-authentication logging enable**
syslog サーバへの出力を有効にします。

［注意事項］
- syslog サーバへの送信対象イベント種別として，コンフィグレーションコマンド logging event-kind aut も合わせて設定してください。

9.2.6 ユーザ切替オプションの設定

［設定のポイント］
1 台の端末で最初のユーザ ID で認証成功後に，別のユーザ ID で認証可能となるユーザ切替オプションを設定します。

［コマンドによる設定］

1. **(config)# web-authentication user replacement**
ユーザ切替オプションを設定します。

［注意事項］
- ユーザ切替で認証成功したユーザ ID を認証解除しても，最初のユーザ ID に戻りません。

9.2.7 Web 認証機能の有効化

［設定のポイント］
Web 認証用のコンフィグレーションを設定後，Web 認証を有効にします。

［コマンドによる設定］

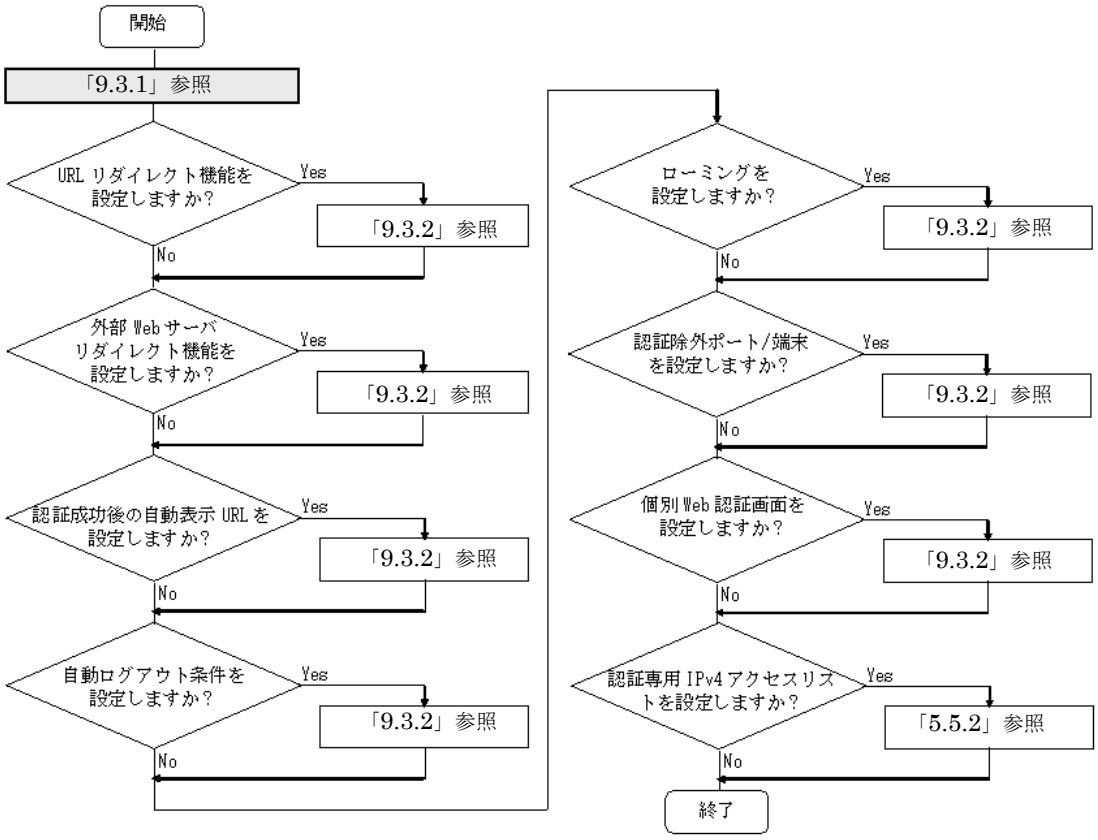
1. **(config)# web-authentication system-auth-control**
Web 認証を有効にします。

［注意事項］
Web 認証の設定をすべて終了してから，本コマンドを設定してください。途中の状態で認証を有効化すると，認証失敗のアカウントログが採取される場合があります。

9.3 固定 VLAN モードのコンフィグレーション

「9.1 Web 認証のコンフィグレーション」および「9.2 全認証モード共通のコンフィグレーション」に記載の設定をしたうえで，次の図の手順に従って固定 VLAN モードのコンフィグレーションを設定してください。

図 9-3 固定 VLAN モードの設定手順



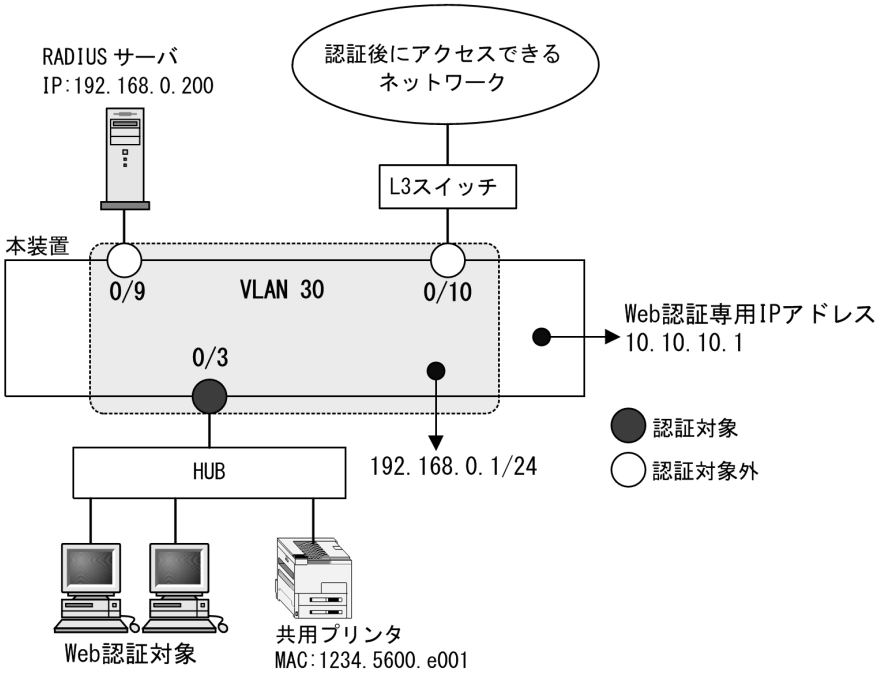
各設定の詳細は，下記を参照してください。

1. 固定 VLAN モードの設定：「9.3.1 固定 VLAN モードの設定」
2. URL リダイレクト機能の設定：「9.3.2 認証処理に関する設定（1）URL リダイレクト機能の設定」
3. 外部 Web サーバリダイレクト機能の設定：「9.3.2 認証処理に関する設定 （2）外部 Web サーバリダイレクト機能の設定」
4. 認証成功後の自動表示 URL の設定：「9.3.2 認証処理に関する設定（3）認証成功後の自動表示 URL の設定」
5. 自動ログアウト条件の設定：「9.3.2 認証処理に関する設定（4）自動ログアウト条件の設定」
6. ローミングの設定：「9.3.2 認証処理に関する設定（5）ローミング（認証済み端末のポート移動通信許可）の設定」
7. 認証除外の設定：「9.3.2 認証処理に関する設定（6）認証除外の設定」
8. 個別 Web 認証画面の設定：「9.3.2 認証処理に関する設定（7）ポートごとの個別 Web 認証画面の設定」
9. 認証専用 IPv4 アクセスリストの設定：「5.5.2 認証専用 IPv4 アクセスリストの設定」
   認証前端末に本装置内蔵の DHCP サーバまたは外部 DHCP サーバから IP アドレスを配布する場合は，認証前に対象となる DHCP サーバと通信できるよう認証専用 IPv4 アクセスリストの設定が必要です。

詳細は「5.5.2 認証専用 IPv4 アクセスリストの設定」を参照してください。

9.3.1 固定 VLAN モードの設定

図 9-4 固定 VLAN モードの構成例



(1) 認証ポートと認証用 VLAN 情報の設定

[設定のポイント]

固定 VLAN モードで使用するポートに，固定 VLAN モードと認証用 VLAN 情報を設定します。

[コマンドによる設定]

1. **(config)# vlan 30**
   (config-vlan)# exit
   VLAN ID 30 を設定します。

2. **(config)# interface gigabitethernet 0/3**
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 30
   認証を行う端末が接続されているポート 0/3 をアクセスポートして設定し，認証用 VLAN30 を設定します。

3. **(config-if)# web-authentication port**
   (config-if)# exit
   ポート 0/3 に固定 VLAN モードを指定します。

（2） VLAN インタフェースに IP アドレスを設定

[設定のポイント]

Web 認証で使用する VLAN に IP アドレスを設定します。

[コマンドによる設定]

1. **(config)# interface vlan 30**
   (config-if)# ip address 192.168.0.1 255.255.255.0
   (config-if)# exit
   Web 認証で使用する VLAN 30 に IP アドレスを設定します。

（3） ポート別認証方式の認証方式リスト名の設定

[設定のポイント]

ポート別認証方式の認証方式リスト名を設定します。
認証方式リストの設定は前述の「9.2.1　認証方式グループと RADIUS サーバ情報の設定（1）認証方式グループの設定」を参照してください。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 0/3**
   (config-if)# web-authentication authentication WEB-list1
   (config-if)# exit
   ポート 0/3 に認証方式リスト名 "WEB-list1" を設定します。

[注意事項]

- 本情報未設定時は，「9.2.1　認証方式グループと RADIUS サーバ情報の設定（1）認証方式グループの設定」の装置デフォルトに従って認証します。
- ポートに設定した認証方式リスト名と，認証方式グループの認証方式リスト名が不一致，または認証方式グループに存在しないときは，装置デフォルトに従って認証します。
- Web 認証のユーザ ID 別認証方式は併用設定できません。詳細は「5.2.2　認証方式リスト」を参照してください。

9.3.2　認証処理に関する設定

固定 VLAN モードの認証処理に関する設定を説明します。

（1） URL リダイレクト機能の設定

(a) トリガパケットの TCP ポート設定

[設定のポイント]

リダイレクトのトリガパケット対象とする宛先 TCP ポート番号を設定します。デフォルトコンフィグレーションの TCP ＝ 80，443 と本設定の TCP ポート番号のパケットが対象となります。
コンフィグレーションコマンド web-authentication web-port で http および https の TCP ポート番号を各 1 個ずつ追加設定することができます。

[コマンドによる設定]

1. **(config)# web-authentication web-port http 8080**
   TCP ポート番号 http の 8080 を追加設定します。
   (config)# web-authentication web-port https 24000

TCP ポート番号 https の 24000 を追加設定します。

(b) ログイン操作プロトコル設定

[設定のポイント]

Web 認証の URL リダイレクト機能時にログインを操作させるプロトコルを設定します。

[コマンドによる設定]

1. **(config)# web-authentication redirect-mode http**
   Web 認証の URL リダイレクト機能で http を用います。

(2) 外部 Web サーバリダイレクト機能の設定

(a) 外部 Web サーバの設定

[設定のポイント]

URL リダイレクトのリダイレクト先として，外部 Web サーバの URL を設定します。

[コマンドによる設定]

1. **(config)# web-authentication redirect target "http://**
   www.example.gaibuserver.co.jp"
   外部 Web サーバの URL を設定します。

[注意事項]

外部 Web サーバでリダイレクトする場合は，コンフィグレーションコマンド web-authentication redirect-mode が無効となります。外部 Web サーバ障害時に本装置の Web サーバでリダイレクトする場合は，コンフィグレーションコマンド web-authentication redirect-mode が有効となります。

(b) URL リダイレクト先 Web サーバの切り替え (生死監視) の設定

[設定のポイント]

外部 Web サーバの生死監視の監視方式，監視間隔，障害検出条件，および正常検出条件を設定します。
障害検出条件は，指定回数連続して「無応答」を検出したときに障害と判断します。
正常検出条件は，指定回数連続して「応答」を検出したときに正常と判断します。
外部 Web サーバの障害時は本装置の Web サーバに，復旧時は外部 Web サーバに自動的に切り替わります。

[コマンドによる設定]

1. **(config)# web-authentication redirect polling tcp interval 30 dead-count 3**
   alive-count 5
   外部 Web サーバの生死監視の監視方式 TCP，監視間隔 30 秒，障害検出条件 3 回，正常検出条件 5 回を設定します。

[注意事項]

1. host が FQDN の場合は監視ごとに DNS 解決します。DNS 失敗（DNS リゾルバ再送後）は「無応答」扱いとします。
2. 本装置の IP レイヤ以下に問題があった場合は，監視パケットが送信されないまま「無応答」と判定する可能性があります。

3. 監視間隔は，1回の監視処理終了から，次の監視処理開始までの間隔とします。（DNS や TCP の再送が発生する場合は監視間隔が延びる方向とします。）
4. プロキシ経由の監視は未サポートです。

(c) リダイレクト先 URL に付加するクエリの設定

[設定のポイント]

リダイレクト先として外部 Web サーバを設定時，リダイレクト先の URL に付加する，本装置や認証端末に関するパラメータを設定します。

[コマンドによる設定]

1. **(config)# web-authentication redirect queries switch-hostname switch-mac client-mac client-ip original-url**
   付加するクエリとして，本装置のホスト名，本装置の装置 MAC アドレス，認証端末の MAC アドレス，認証端末の IP アドレス，リダイレクト前の URL を設定します。

(3) 認証成功後の自動表示 URL の設定

(a) 指定した URL を表示する設定

[設定のポイント]

認証成功後に表示する URL を設定します。

[コマンドによる設定]

1. **(config)# web-authentication jump-url "http://www.example.com/"**
   認証成功後に http://www.example.com/ の画面を表示させます。

[注意事項]

コンフィグレーションコマンドでは指定 URL へ移動するまでの時間（デフォルトコンフィグレーションは 5 秒）も変更できますが，固定 VLAN モードでは設定不要です。デフォルトコンフィグレーションより短い時間で指定 URL を表示させたいときは変更してください。

(b) リダイレクト前の URL の画面を表示する設定

[設定のポイント]

URL リダイレクト機能使用時，認証成功後に，リダイレクト前の URL の画面を表示するよう設定します。

[コマンドによる設定]

1. **(config)# web-authentication jump-url original**
   認証成功後，リダイレクト前の URL の画面を表示するよう設定します。

[注意事項]

「(a) 指定した URL を表示する設定」と同様です。

(4) 自動ログアウト条件の設定

(a) 最大接続時間の設定

本設定は，Web 認証の全認証モードで共通です。「9.2　全認証モード共通のコンフィグレーション 9.2.3　認証モード共通の自動ログアウト条件の設定」を参照してください。

(b) 認証済み端末の無通信監視機能の設定

Web 認証の固定 VLAN モードまたはダイナミック VLAN モードが有効となったとき，コンフィグレーションコマンド web-authentication auto-logout を設定しなくても本機能は有効となります。

なお，コンフィグレーションコマンドで no web-authentication auto-logout を設定すると，自動ログアウトしません。

(c) 認証済み端末の接続監視機能の設定

[設定のポイント]

認証済み端末の接続を監視する接続監視機能を設定します。

[コマンドによる設定]

1. **(config)# web-authentication logout polling enable**
   接続監視機能を有効に設定します。
2. **(config)# web-authentication logout polling interval 300**
   接続監視フレームのポーリング間隔を 300 秒に設定します。
3. **(config)# web-authentication logout polling retry-interval 10**
   接続監視フレームの再送間隔を 10 秒に設定します。
4. **(config)# web-authentication logout polling count 5**
   接続監視フレームの再送回数を 5 回に設定します。

(d) 特殊フレーム受信条件の設定

本設定は，Web 認証の全認証モードで共通です。「9.2　全認証モード共通のコンフィグレーション 9.2.3　認証モード共通の自動ログアウト条件の設定」を参照してください。

(5) ローミング（認証済み端末のポート移動通信許可）の設定

[設定のポイント]

固定 VLAN モードで認証済みの端末を，ポートリンクダウンしないで他のポートへ移動しても通信可能に設定します。

[コマンドによる設定]

1. **(config)# web-authentication static-vlan roaming**
   認証済み端末をポート移動した場合は，通信を継続します。

[注意事項]

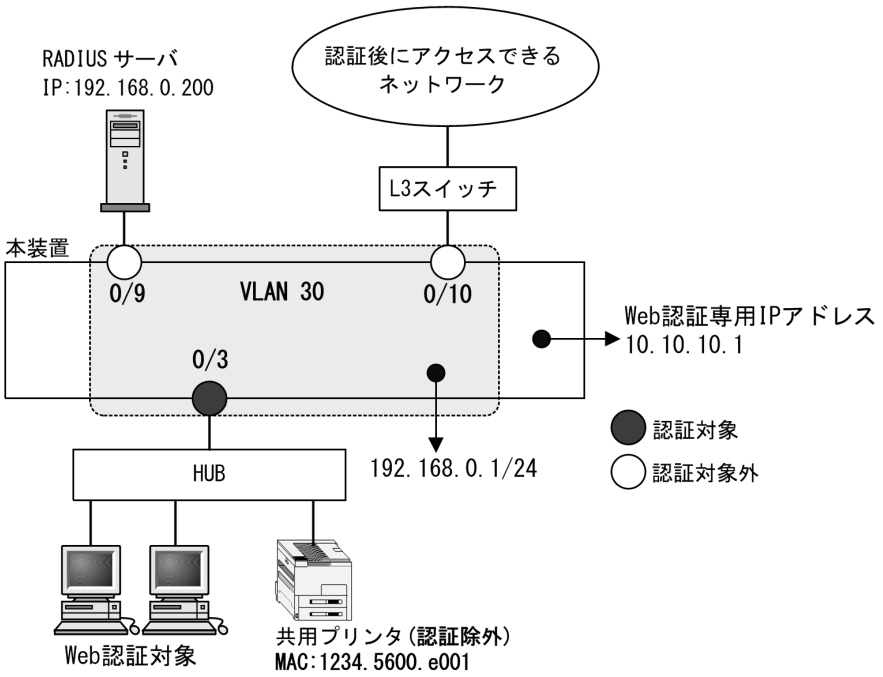
ローミングの動作可能な条件は下記のとおりです。

- 移動前および移動後が，固定 VLAN モード対象ポート
- 移動前および移動後が，同一 VLAN

(6) 認証除外の設定

固定 VLAN モードで認証対象外とするポートや端末を設定します。本例では，次の図に示すポート 0/9，0/10，および共用プリンタを認証除外として設定します。

図 9-5 固定 VLAN モードの認証除外の構成例



(a) 認証除外ポートの設定

[設定のポイント]

固定 VLAN モードで認証を除外するポートに対しては，認証モードを設定しません。

[コマンドによる設定]

1. **(config)# interface range gigabitethernet 0/9-10**
   (config-if-range)# switchport mode access
   (config-if-range)# switchport access vlan 30
   (config-if-range)# exit
   VLAN ID 30 のポート 0/9 と 0/10 を，アクセスポートとして設定します。認証モード（web-authentication port）は設定しません。

(b) 認証除外端末の設定

[設定のポイント]

固定 VLAN モードで認証を除外する端末の MAC アドレスを，MAC アドレステーブルに登録します。

[コマンドによる設定]

1. **(config)# mac-address-table static 1234.5600.e001 vlan 30 interface gigabitethernet 0/3**
   VLAN ID 30 のポート 0/3 で認証を除外して通信を許可する端末の MAC アドレス（図内の共用プリンタの MAC アドレス：1234.5600.e001）を，MAC アドレステーブルに設定します。

(7) ポートごとの個別 Web 認証画面の設定

[設定のポイント]

固定 VLAN モードの認証対象ポートで使用する個別 Web 認証画面のカスタムファイルセット名を設

定します。

［コマンドによる設定］

1. **(config)# interface gigabitethernet 0/3**
   (config-if)# web-authentication port
   (config-if)# web-authentication html-fileset FILESETAAA
   (config-if)# exit
   ポート 0/3 で使用する個別 Web 認証画面のカスタムファイルセット名 "FILESETAAA" を設定します。（カスタムファイルセット名は，運用コマンド set web-authentication html-files で本装置に登録した名称を設定します。）

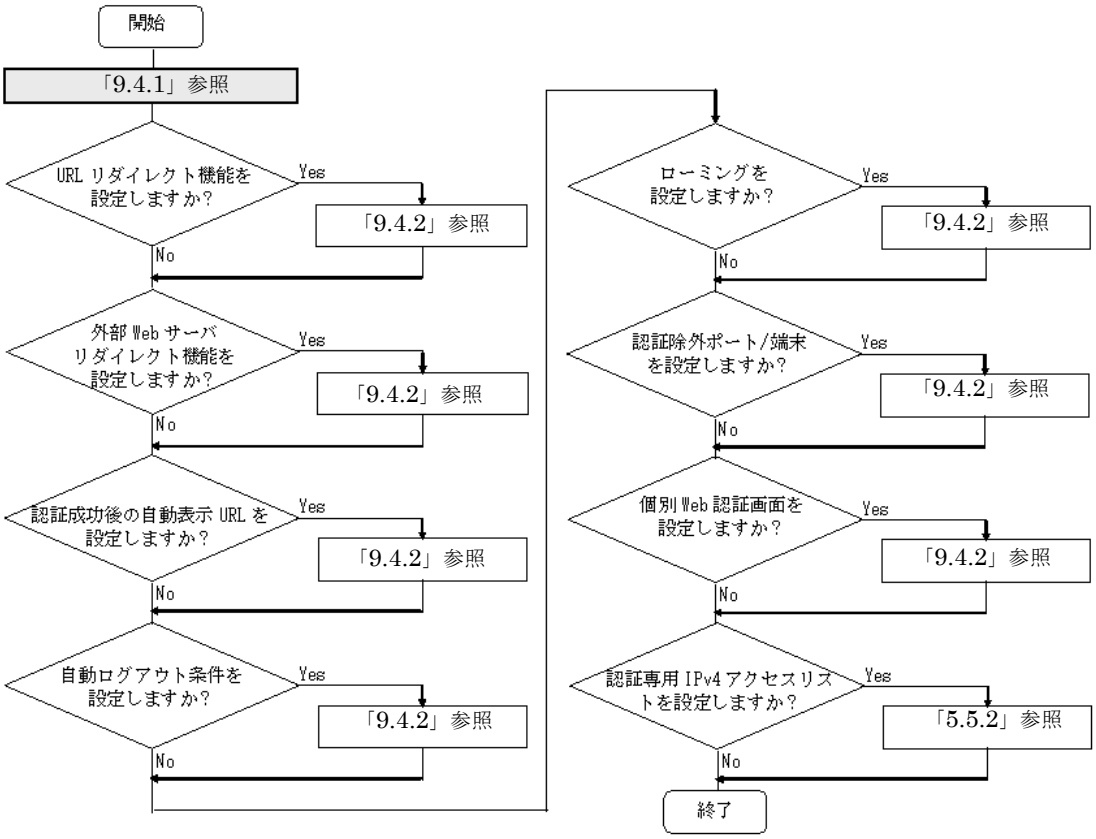
［注意事項］

1. 本コマンドを設定するポートに，あらかじめコンフィグレーションコマンド web-authentication port を設定してください。
2. 個別 Web 認証画面のカスタムファイルセットは，運用コマンド set web-authentication html-files で本装置に登録してください。

9.4　ダイナミック VLAN モードのコンフィグレーション

「9.1　Web 認証のコンフィグレーション」および「9.2　全認証モード共通のコンフィグレーション」に記載の設定をしたうえで，次の図の手順に従ってダイナミック VLAN モードのコンフィグレーションを設定してください。

図 9-6　ダイナミック VLAN モードの設定手順



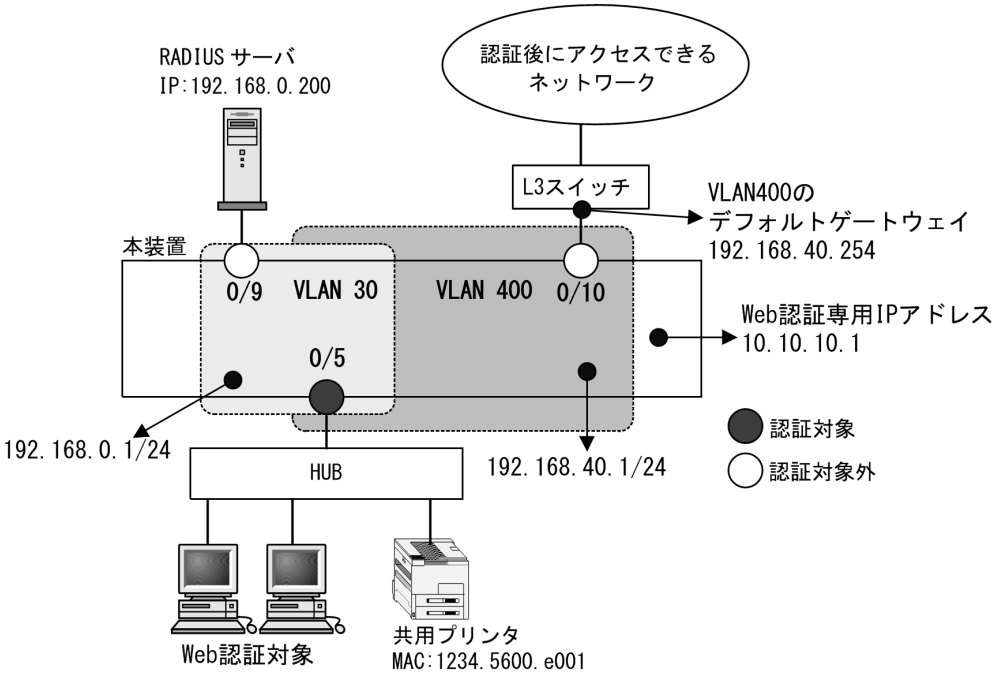
各設定の詳細は，下記を参照してください。

1. ダイナミック VLAN モードの設定：「9.4.1　ダイナミック VLAN モードの設定」
2. URL リダイレクト機能の設定：「9.4.2　認証処理に関する設定（1）URL リダイレクト機能の設定」
3. 外部 Web サーバリダイレクト機能の設定：「9.4.2　認証処理に関する設定　（2）外部 Web サーバリダイレクト機能の設定」
4. 認証成功後の自動表示 URL の設定：「9.4.2　認証処理に関する設定（3）認証成功後の自動表示 URL と URL 移動までの時間の設定」
5. 自動ログアウト条件の設定：「9.4.2　認証処理に関する設定（4）自動ログアウト条件の設定」
6. ローミングの設定：「9.4.2　認証処理に関する設定（5）ローミング（認証済み端末のポート移動通信許可）の設定」
7. 認証除外の設定：「9.4.2　認証処理に関する設定（6）認証除外の設定」
8. 個別 Web 認証画面の設定：「9.4.2　認証処理に関する設定（7）ポートごとの個別 Web 認証画面の設定」
9. 認証専用 IPv4 アクセスリストの設定：「5.5.2　認証専用 IPv4 アクセスリストの設定」

認証前端末に本装置内蔵の DHCP サーバまたは外部 DHCP サーバから IP アドレスを配布する場合は，認証前に対象となる DHCP サーバと通信できるよう認証専用 IPv4 アクセスリストの設定が必要です。詳細は「5.5.2　認証専用 IPv4 アクセスリストの設定」を参照してください。

9.4.1　ダイナミック VLAN モードの設定

図 9-7　ダイナミック VLAN モードの構成例



(1) 認証ポートと認証用 VLAN 情報の設定

[設定のポイント]

ダイナミック VLAN モードで使用するポートに，ダイナミック VLAN モードと認証用 VLAN 情報を設定します。

なお，認証ポートの認証後 VLAN は，「5.4.3　MAC VLAN の自動 VLAN 割当」により割り当てられるものとします。

[コマンドによる設定]

1. **(config)# vlan 400 mac-based**
   (config-vlan)# exit
   VLAN ID 400 に MAC VLAN を設定します。

2. **(config)# vlan 30**
   (config-vlan)# exit
   VLAN ID 30 を設定します。

3. **(config)# interface gigabitethernet 0/5**
   (config-if)# switchport mode mac-vlan
   (config-if)# switchport mac native vlan 30

認証を行う端末が接続されているポート 0/5 を MAC ポートとして設定し，認証前 VLAN30 を指定します。（認証後 VLAN は「5.4.3　MAC VLAN の自動 VLAN 割当」により割り当てられます。）

4. **(config-if)# web-authentication port**
   (config-if)# exit
   ポート 0/5 にダイナミック VLAN モードを設定します。

（2） VLAN インタフェースに IP アドレスを設定

［設定のポイント］

Web 認証で使用する認証前 VLAN と認証後 VLAN に IP アドレスを設定します。

［コマンドによる設定］

1. **(config)# interface vlan 30**
   (config-if)# ip address 192.168.0.1 255.255.255.0
   (config-if)# exit
   Web 認証で使用する認証前 VLAN 30 に IP アドレスを設定します。

2. **(config)# interface vlan 400**
   (config-if)# ip address 192.168.40.1 255.255.255.0
   (config-if)# exit
   Web 認証で使用する認証後 VLAN 400 に IP アドレスを設定します。

（3） ポート別認証方式の認証方式リスト名の設定

［設定のポイント］

ポート別認証方式の認証方式リスト名を設定します。
認証方式リストの設定は前述の「9.2.1　認証方式グループと RADIUS サーバ情報の設定（1）認証方式グループの設定」を参照してください。

［コマンドによる設定］

1. **(config)# interface gigabitethernet 0/5**
   (config-if)# web-authentication authentication WEB-list1
   (config-if)# exit
   ポート 0/5 に認証方式リスト名 "WEB-list1" を設定します。

［注意事項］

- 本情報未設定時は，「9.2.1　認証方式グループと RADIUS サーバ情報の設定（1）認証方式グループの設定」の装置デフォルトに従って認証します。
- ポートに設定した認証方式リスト名と，認証方式グループの認証方式リスト名が不一致，または認証方式グループに存在しないときは，装置デフォルトに従って認証します。
- Web 認証のユーザ ID 別認証方式は併用設定できません。詳細は「5.2.2　認証方式リスト」を参照してください。

9.4.2 認証処理に関する設定

ダイナミック VLAN モードの認証処理に関する設定を説明します。

(1) URL リダイレクト機能の設定

固定 VLAN モードと同様です。「9.3.2 認証処理に関する設定（1）URL リダイレクト機能の設定」を参照してください。

(2) 外部 Web サーバリダイレクト機能の設定

固定 VLAN モードと同様です。「9.3.2 認証処理に関する設定 （2）外部 Web サーバリダイレクト機能の設定」を参照してください。

(3) 認証成功後の自動表示 URL と URL 移動までの時間の設定

(a) 指定した URL を表示する設定

[設定のポイント]

認証成功後に表示する URL と URL に移動するまでの時間を設定します。

[コマンドによる設定]

1. **(config)# web-authentication jump-url "http://www.example.com/" delay 30**
   認証成功後，30 秒経過してから http://www.example.com/ の画面を表示させます。

[注意事項]

認証前 VLAN から認証後 VLAN への切り替えで，認証端末の IP アドレス変更が必要となるため，URL 移動までの時間を約 20 ～ 30 秒程度で設定してください。
装置内蔵 DHCP サーバで認証前の端末に IP アドレス配布している場合 (デフォルトリース時間：1 日) は，認証後 VLAN で正規 DHCP サーバから IP アドレスを取得します。このため，認証完了時点から，認証後 VLAN 通信が可能になるまで，約 20 ～ 30 秒程度かかる場合があります。

(b) リダイレクト前の URL の画面を表示する設定

[設定のポイント]

URL リダイレクト機能使用時，認証成功後に，リダイレクト前の URL の画面を表示するよう設定します。

1. **(config)# web-authentication jump-url original delay 30**
   認証成功後，30 秒経過してからリダイレクト前の URL の画面を表示するよう設定します。

[注意事項]

「(a) 指定した URL を表示する設定」と同様です。

(4) 自動ログアウト条件の設定

(a) 最大接続時間の設定

本設定は，Web 認証の全認証モードで共通です。「9.2 全認証モード共通のコンフィグレーション 9.2.3 認証モード共通の自動ログアウト条件の設定」を参照してください。

(b) 認証済み端末の無通信監視機能の設定

固定 VLAN モードと同様です。「9.3.2 認証処理に関する設定（4）自動ログアウト条件の設定（b）認証済み端末の無通信監視機能の設定」を参照してください。

(c) 特殊フレーム受信条件の設定

本設定は，Web 認証の全認証モードで共通です。「9.2　全認証モード共通のコンフィグレーション 9.2.3　認証モード共通の自動ログアウト条件の設定」を参照してください。

(5) ローミング（認証済み端末のポート移動通信許可）の設定

[設定のポイント]

ダイナミック VLAN モードで認証済みの端末を，ポートリンクダウンしないで他のポートへ移動しても通信可能に設定します。

[コマンドによる設定]

1. **(config)# web-authentication roaming**

認証済み端末をポート移動した場合は，通信を継続します。

[注意事項]

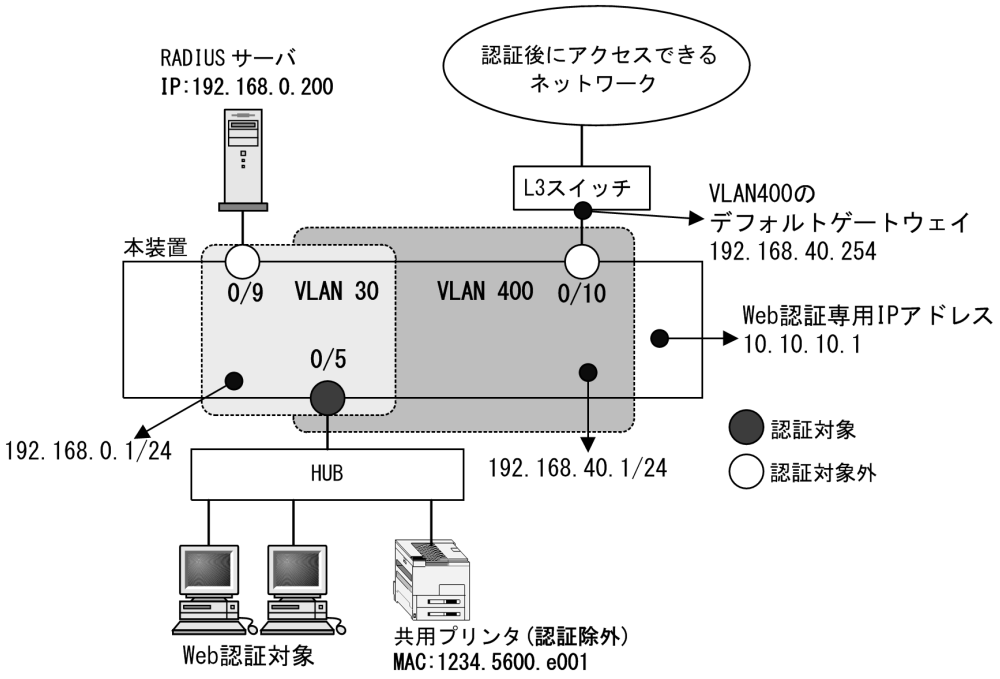
ローミングの動作可能な条件は下記のとおりです。

- 移動前および移動後が，ダイナミック VLAN モード対象ポート

(6) 認証除外の設定

ダイナミック VLAN モードで認証対象外とするポートや端末を設定します。本例では，次の図に示すポート 0/9，0/10，および共用プリンタを認証除外として設定します。

図 9-8　ダイナミック VLAN モードの認証除外の構成例



(a) 認証除外ポートの設定

[設定のポイント]

認証を除外するポートをアクセスポートとして設定し，認証モードを設定しません。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 0/9**

```
(config-if)# switchport mode access
(config-if)# switchport access vlan 30
(config-if)# exit
```

VLAN ID 30 のポート 0/9 をアクセスポートとして設定します。認証モード（web-authentication port）は設定しません。

2.
```
(config)# interface gigabitethernet 0/10
(config-if)# switchport mode access
(config-if)# switchport access vlan 400
(config-if)# exit
```

MAC VLAN ID 400 のポート 0/10 をアクセスポートとして設定します。認証モード（web-authentication port）は設定しません。

(b) 認証除外端末の設定

[設定のポイント]

認証を除外する端末の MAC アドレスを，MAC VLAN と MAC アドレステーブルに登録します。

[コマンドによる設定]

1.
```
(config)# vlan 400 mac-based
(config-vlan)# mac-address 1234.5600.e001
(config-vlan)# exit
```

認証を除外する MAC アドレス（図内の共用プリンタの MAC アドレス：1234.5600.e001）を，MAC VLAN ID 400 に設定します。

2.
```
(config)# interface gigabitethernet 0/5
(config-if)# switchport mode mac-vlan
(config-if)# switchport mac vlan 400
(config-if)# exit
```

認証ポートに除外端末が属する MAC VLAN ID 400 を設定します。

3.
```
(config)# mac-address-table static 1234.5600.e001 vlan 400 interface
gigabitethernet 0/5
```

MAC VLAN ID 400 のポート 0/5 で認証を除外して通信を許可する端末の MAC アドレス（図内の共用プリンタの MAC アドレス：1234.5600.e001）を，MAC アドレステーブルに設定します。

[注意事項]

MAC アドレステーブルに認証除外端末の MAC アドレスを設定する前に，除外端末が所属するポートに MAC VLAN の VLAN ID を設定してください。

(7) ポートごとの個別 Web 認証画面の設定

[設定のポイント]

ダイナミック VLAN モードの認証対象ポートで使用する個別 Web 認証画面のカスタムファイルセット名を設定します。

[コマンドによる設定]

1.
```
(config)# interface gigabitethernet 0/5
```

```
(config-if)# web-authentication port
(config-if)# web-authentication html-fileset FILESETBBB
(config-if)# exit
```

ポート 0/5 で使用する個別 Web 認証画面のカスタムファイルセット名 "FILESETBBB" を設定します。（カスタムファイルセット名は，運用コマンド set web-authentication html-files で本装置に登録した名称を設定します。）

［注意事項］

1. 本コマンドを設定するポートに，あらかじめコンフィグレーションコマンド web-authentication port を設定してください。
2. 個別 Web 認証画面のカスタムファイルセットは，運用コマンド set web-authentication html-files で本装置に登録してください。

9.5 Web 認証のオペレーション

9.5.1 運用コマンド一覧

Web 認証の運用コマンド一覧を次の表に示します。

表 9-3 運用コマンド一覧

コマンド名	説明
set web-authentication user	内蔵 Web 認証 DB に Web 認証用のユーザ情報（ユーザ ID・パスワード・認証後 VLAN ID）を追加します。（ユーザ情報の編集）
set web-authentication passwd	内蔵 Web 認証 DB のユーザ ID のパスワードを変更します。（ユーザ情報の編集）
set web-authentication vlan	内蔵 Web 認証 DB のユーザ ID の認証後 VLAN ID を変更します。（ユーザ情報の編集）
remove web-authentication user	内蔵 Web 認証 DB からユーザ情報を削除します。（ユーザ情報の編集）
commit web-authentication	編集したユーザ情報を内蔵 Web 認証 DB に反映します。
store web-authentication	内蔵 Web 認証 DB のバックアップファイルを作成します。
load web-authentication	バックアップファイルから内蔵 Web 認証 DB を復元します。
show web-authentication user	内蔵 Web 認証 DB の登録内容，または編集中のユーザ情報を表示します。
clear web-authentication auth-state	認証済みユーザの強制ログアウトを行います。
show web-authentication	Web 認証の設定状態を表示します。
show web-authentication login	Web 認証の認証状態を表示します。
show web-authentication login select-option	Web 認証の認証状態を表示オプションを選択して表示します。
show web-authentication login summary	認証済みユーザ数を表示します。
show web-authentication statistics	Web 認証の統計情報を表示します。
clear web-authentication statistics	統計情報をクリアします。
show web-authentication logging	Web 認証で採取している動作ログメッセージを表示します。
clear web-authentication logging	Web 認証で採取している動作ログメッセージをクリアします。
set web-authentication html-files	指定された Web 認証画面のカスタムファイルセットを本装置に登録します。
clear web-authentication html-files	本装置に登録した Web 認証画面のカスタムファイルセットを削除します。
show web-authentication html-files	本装置に登録した Web 認証画面カスタムファイルセットのファイル名，ファイルサイズと登録日時を表示します。
store web-authentication html-files	本装置で動作中の Web 認証画面ファイルセットを取り出し，RAMDISK の任意のディレクトリに格納します。
show web-authentication redirect target	URL リダイレクト機能において，リダイレクト先を外部 Web サーバに変更したときの状態を表示します。

9.5.2 内蔵 Web 認証 DB の登録

ローカル認証方式で使用する，認証対象端末のユーザ情報（ユーザ ID，パスワード，認証後 VLAN ID）

を内蔵 Web 認証 DB に登録します。手順として，ユーザ情報の編集（追加・変更・削除）と内蔵 Web 認証 DB への反映があります。以下に登録例を示します。

なお，ユーザ情報の追加を行う前に，Web 認証システムの環境設定およびコンフィグレーションの設定を完了している必要があります。

（1） ユーザ情報の追加

認証対象のユーザごとに，運用コマンド set web-authentication user で，ユーザ ID，パスワード，認証後 VLAN ID を追加します。

- 固定 VLAN モードの場合：認証対象ユーザ（端末）の接続ポートが所属する VLAN ID を指定
- ダイナミック VLAN モードの場合：認証対象ユーザ（端末）を認証後に収容する VLAN ID を指定

次の例では，USER01 ～ USER05 の 5 ユーザ分を登録します。

［コマンド入力］

```
# set web-authentication user USER01 PAS0101 100
# set web-authentication user USER02 PAS0200 100
# set web-authentication user USER03 PAS0300 100
# set web-authentication user USER04 PAS0320 100
# set web-authentication user USER05 PAS0400 100
```

（2） ユーザ情報変更と削除

登録済みユーザのパスワード，認証後 VLAN ID の変更およびユーザの削除は次の手順で行います。

（a） パスワードの変更

登録済みユーザのパスワードの変更は，運用コマンド set web-authentication passwd で行います。次の例では，ユーザ ID（USER01）のパスワードを変更します。

［コマンド入力］

```
# set web-authentication passwd USER01 PAS0101 PPP4321
```

ユーザ ID（USER01）のパスワードを PAS0101 から PPP4321 に変更します。

（b） 認証後 VLAN ID 変更

登録済みユーザの認証後 VLAN ID の変更は，運用コマンド set web-authentication vlan で行います。

- 固定 VLAN モードの場合：認証対象ユーザ（端末）の接続ポートが所属する VLAN ID を指定
- ダイナミック VLAN モードモードの場合：認証対象ユーザ（端末）を認証後に収容する VLAN ID を指定

次の例では，ユーザ ID（USER01）の認証後 VLAN ID を変更します。

［コマンド入力］

```
# set web-authentication vlan USER01 200
```

ユーザ ID（USER01）の認証後 VLAN ID を 200 に変更します。

（c） ユーザ情報の削除

登録済みユーザ情報の削除は，運用コマンド remove web-authentication user で行います。次の例では，ユーザ ID（USER01）のユーザ情報を削除します。

［コマンド入力］

```
# remove web-authentication user USER01
```

```
Remove web-authentication user  Are you sure? (y/n): y

#
```

ユーザ ID（USER01）を削除します。

（3） 内蔵 Web 認証 DB へ反映

編集したユーザ情報を，運用コマンド commit web-authentication で内蔵 Web 認証 DB へ反映します。

[コマンド入力]

```
# commit web-authentication
Commitment web-authentication user data. Are you sure? (y/n): y

Commit complete.
#
```

9.5.3 内蔵 Web 認証 DB のバックアップと復元

内蔵 Web 認証 DB のバックアップおよびバックアップファイルからの復元を示します。

（1） 内蔵 Web 認証 DB のバックアップ

内蔵 Web 認証 DB から運用コマンド store web-authentication でバックアップファイル（次の例では backupfile）を作成します。

[コマンド入力]

```
# store web-authentication ramdisk backupfile
Backup web-authentication user data.  Are you sure? (y/n): y

Backup complete.
#
```

（2） 内蔵 Web 認証 DB の復元

バックアップファイル（次の例では backupfile）から運用コマンド load web-authentication で内蔵 Web 認証 DB を復元します。

[コマンド入力]

```
# load web-authentication ramdisk backupfile
Restore web-authentication user data.  Are you sure? (y/n): y

Restore complete.
#
```

9.5.4 Web 認証の設定状態表示

運用コマンド show web-authentication で，Web 認証の設定状態を表示します。

図 9-9 Web 認証の設定状態表示

```
# show web-authentication

Date 20XX/05/20 07:54:33 UTC
<<<Web-Authentication mode status>>>
  Dynamic-VLAN     : Enable
  Static-VLAN      : Enable

<<<System configuration>>>
 * Authentication parameter
  Authentic-mode   : Dynamic-VLAN
  ip address       : 1.1.1.1
  max-user         : 1024
```

```
  user-group       : Disable
  user replacement : Disable
  roaming          : Disable
  html-files       : Default

 * AAA methods
  Authentication Default       : RADIUS
  Authentication port-list-AAA : RADIUS web-group-1
  Authentication End-by-reject : Disable
  Accounting Default           : RADIUS

 * Logout parameter
  max-timer        : 60(min)
  auto-logout      : Enable
  logout ping      : tos-windows:   1  ttl:   1
  logout polling   : -

 * Redirect parameter
  redirect         : Enable
  redirect target  : http://10.0.0.209
  redirect queries :
  redirect polling : tcp, interval=60, dead-count=1, alive-count=1
  redirect-mode    : HTTP
  web-port         : HTTP : 80(Fixed)  HTTPS : 443(Fixed)
  jump-url         : original

 * Logging status
  [Syslog send]    : Disable
  [Traps]          : Disable

 * Internal DHCP sever status
  service dhcp vlan: Disable

<Port configuration>
  Port Count            : 1

  Port                  : 0/3
  VLAN ID               : 1000
  Forceauth VLAN        : Disable
  Access-list-No        : L2-auth
  ARP relay             : Enable
  Max-user              : 1024
  Authentication method : port-list-AAA
  HTML fileset          : FILESETXYZ

<<<System configuration>>>
 * Authentication parameter
  Authentic-mode   : Static-VLAN
  ip address       : 1.1.1.1
  max-user         : 1024
  user-group       : Disable
  user replacement : Disable
  roaming          : Disable
  html-files       : Default

 * AAA methods
  Authentication Default       : RADIUS
  Authentication port-list-AAA : RADIUS web-group-1
  Authentication End-by-reject : Disable
  Accounting Default           : RADIUS

 * Logout parameter
  max-timer        : 60(min)
  auto-logout      : Enable
  logout ping      : tos-windows:   1  ttl:   1
  logout polling   : Enable  [ interval: 300, count: 3, retry-interval: 1 ]

 * Redirect parameter
  redirect         : Enable
  redirect target  : http://10.0.0.209
  redirect queries :
  redirect polling : tcp, interval=60, dead-count=1, alive-count=1
  redirect-mode    : HTTP
  web-port         : HTTP : 80(Fixed)  HTTPS : 443(Fixed)
```

```
  jump-url         : original

 * Logging status
  [Syslog send]    : Disable
  [Traps]          : Disable

 * Internal DHCP sever status
  service dhcp vlan: -

<Port configuration>
  Port Count            : 1

  Port                  : 0/9
  VLAN ID               : 200
  Forceauth VLAN        : Disable
  Access-list-No        : L2-auth
  ARP relay             : Enable
  Max-user              : 1024
  Authentication method : port-list-AAA
  HTML fileset          : FILESETXYZ

#
```

9.5.5 Web 認証の状態表示

運用コマンド show web-authentication statistics で，Web 認証の状態および RADIUS サーバとの通信状況を表示します。

図 9-10 Web 認証の表示

```
# show web-authentication statistics

Date 20XX/05/20 11:40:35 UTC
Web-Authentication Information:
  Authentication Request Total :         17
  Authentication Current Count :          2
  Authentication Error Total   :          1

RADIUS Web-Authentication Information:
[RADIUS frames]
  TxTotal   :        17  TxAccReq  :        17  TxError   :         0
  RxTotal   :        12  RxAccAccpt:        11  RxAccRejct:         1
                         RxAccChllg:         0  RxInvalid :         0
Account Web-Authentication Information:
[Account frames]
  TxTotal   :        24  TxAccReq  :        24  TxError   :         0
  RxTotal   :        19  RxAccResp :        19  RxInvalid :         0

#
```

9.5.6 Web 認証の認証状態表示

(1) 表示オプション指定なしで表示

運用コマンド show web-authentication login で，Web 認証の認証状態を表示します。

図 9-11 Web 認証の認証状態表示

```
# show web-authentication login

Date 20XX/05/20 20:44:01 UTC
 Dynamic VLAN mode total login counts(Login/Max):   1 / 1000
  Authenticating client counts :    0
  Port roaming : Disable
   No F User name                Port  VLAN Class Login time          Limit
    1   web1000                  0/3   1000     0 20XX/05/20 20:42:29 00:58:27

 Static VLAN mode total login counts(Login/Max):    1 / 1024
```

```
  Authenticating client counts :    0
  Port roaming : Disable
   No F User name                 Port   VLAN Class Login time          Limit
    1 * web024                    0/9    200     0 20XX/05/20 20:43:22 00:59:21

#
```

（2） 表示オプション指定ありで表示 (select-option 指定)

運用コマンド show web-authentication login select-option で，Web 認証の認証状態を指定した表示オプションで表示します。下記にインタフェースポート番号指定時の実行例を示します。

図 9-12 ポート指定時の情報表示

```
# show web-authentication login select-option port 0/3

Date 20XX/05/20 20:47:43 UTC
 Dynamic VLAN mode total login counts(Login/Max):   1 / 1000
  Authenticating client counts :    0
  Port roaming : Disable
   No F User name                 Port  VLAN Class Login time          Limit
    1   web1000                   0/3   1000     0 20XX/05/20 20:42:29 00:54:45

#
```

（3） 認証済み端末数だけで表示 (summary 表示)

運用コマンド show web-authentication login summary で Web 認証の認証済みユーザ数を表示します。

図 9-13 認証済みユーザ数だけの表示

```
# show web-authentication login summary port

Date 20XX/05/20 09:42:51 UTC
 Dynamic VLAN mode total login counts(Login/Max):   1 / 1000
  Port roaming : Enable
   No  Port  Login /  Max
    1  0/3       1 / 1000

 Static VLAN mode total login counts(Login/Max):    1 / 1024
  Port roaming : Enable
   No  Port  Login /  Max
    1  0/9       1 / 1024

#
```

9.5.7 URL リダイレクト先を外部 Web サーバに変更したときの状態表示

運用コマンド show web-authentication redirect target で，URL リダイレクト先を Web サーバに変更したときの状態を表示します。

図 9-14 URL リダイレクト先を Web サーバに変更したときの状態表示

```
# show web-authentication redirect target

Date 20XX/05/20 08:13:34 UTC
<Web-server information>
 target               : http://10.0.0.209
   status             : alive
   last change time   : 20XX/05/20 08:12:39 UTC
   total change count : 2

#
```

9.5.8　Web 認証画面ファイルの登録

（1） 基本 Web 認証画面カスタムファイルセットの登録

基本 Web 認証画面カスタムファイルセットの登録は次の手順で行います。

1. 各 Web 認証画面のファイルを外部装置（PC など）で作成します。（このファイル群のディレクトリを基本 Web 認証画面のカスタムファイルセットと称す。）
2. 基本 Web 認証画面のカスタムファイルセットを MC から RAMDISK にコピーします。
3. 運用コマンド set web-authentication html-files で基本 Web 認証画面のカスタムファイルセットを登録します。

図 9-15　基本 Web 認証画面のカスタムファイルセットの登録

```
# copy mc webfileset ramdisk webfileset

# set web-authentication html-files ramdisk webfileset
Do you wish to install new html-files ? (y/n):y
executing...
Install complete.
#
```

（2） 個別 Web 認証画面カスタムファイルセットの登録

ポートごとに使用する個別 Web 認証画面カスタムファイルセットの登録は次の手順で行います。

1. 各 Web 認証画面のファイルを外部装置（PC など）で作成します。（このファイル群のディレクトリを個別 Web 認証画面のカスタムファイルセットと称す。）
2. 個別 Web 認証画面のカスタムファイルセットを MC から RAMDISK にコピーします。
3. 運用コマンド set web-authentication html-files で個別 Web 認証画面のカスタムファイルセットを登録します。

図 9-16　個別 Web 認証画面ファイルの登録

```
# copy mc filesetAAA ramdisk filesetAAA

# set web-authentication html-files ramdisk filesetAAA html-fileset FILESETAAA
Do you wish to install new html-files ? (y/n):y
executing...
Install complete.
#
```

［注意事項］

- 個別 Web 認証画面のカスタムファイルセットを登録するときは，運用コマンド set web-authentication html-files で html-fileset パラメータとカスタムファイルセット名を必ず指定してください。未指定のときは基本 Web 認証画面のカスタムファイルセットとして登録します。
- 本装置に登録する個別 Web 認証画面のカスタムファイルセット名は，英数字大文字で指定してください。
- ポートごとに個別 Web 認証画面を指定するときは，本コマンドで登録したカスタムファイルセット名（上記の例では "FILESETAAA"）を指定してください。（ポートごとの個別 Web 認証画面の設定は，「9.3.2　認証処理に関する設定（7）ポートごとの個別 Web 認証画面の設定」を参照してください。）

9.5.9 登録した Web 認証画面ファイルの情報表示

運用コマンド show web-authentication html-files で，登録した Web 認証画面ファイルの情報を表示します。

図 9-17 登録した Web 認証画面ファイルの情報表示

```
# show web-authentication html-files

    File Date               Size Name
    20XX/05/29 02:12       1,507 login.html           •••1
    20XX/05/29 02:12       1,260 loginOK.html
    20XX/05/29 02:12         666 loginNG.html
    20XX/05/29 02:12         937 logout.html
    20XX/05/29 02:12         586 logoutOK.html
    20XX/05/29 02:12         640 logoutNG.html
    20XX/05/29 02:12         545 webauth.msg
    default now                0 favicon.ico           •••2
    20XX/05/29 02:12      17,730 the other files
    < FILESETXYZ >                                  •••3
    20XX/05/29 02:14       1,507 login.html
    20XX/05/29 02:14       1,260 loginOK.html
    20XX/05/29 02:14         666 loginNG.html
    20XX/05/29 02:14         937 logout.html
    20XX/05/29 02:14         586 logoutOK.html
    20XX/05/29 02:14         640 logoutNG.html
    20XX/05/29 02:14         545 webauth.msg
    default now                0 favicon.ico
    20XX/05/29 02:14      17,730 the other files


#
```

1. 基本 Web 認証画面のカスタムファイルセットを登録した時間を表示します。
2. デフォルト状態の場合，" default now" を表示します。
3. 個別 Web 認証画面のカスタムファイルセットを登録しているときに表示します。

9.5.10 登録した Web 認証画面カスタムファイルセットの削除

運用コマンド set web-authentication html-files で登録した Web 認証画面のカスタムファイルセットを，運用コマンド clear web-authentication html-files で削除します。

図 9-18 基本 Web 認証画面のカスタムファイルセットの削除

```
# clear web-authentication html-files
Do you wish to clear registered html-files and initialize? (y/n):y
executing...
Clear complete.

#
```

図 9-19 個別 Web 認証画面のカスタムファイルセットの削除

```
# clear web-authentication html-files html-fileset FILESETAAA
Do you wish to clear registered html-files and initialize? (y/n):y
executing...
Clear complete.

#
```

図 9-20 登録したすべてのカスタムファイルセットの削除

```
# clear web-authentication html-files -all
Do you wish to clear registered html-files and initialize? (y/n):y
executing...
```

```
Clear complete.

#
```

9.5.11 動作中の Web 認証画面ファイルセットの取り出し

動作中の Web 認証画面ファイルセットを，運用コマンド store web-authentication html-files で RAMDISK の任意のディレクトリに格納します。RAMDISK に格納した Web 認証画面ファイルは，運用コマンド copy で MC にコピーしてください。（装置を再起動すると，RAMDISK のファイルは削除されます。）

Web 認証画面ファイルセットは一括で取り出されますので，ファイルの個別指定はできません。

図 9-21 基本 Web 認証画面のファイルセットの取り出し

```
# store web-authentication html-files ramdisk webfileset
Do you wish to store html-files? (y/n): y
executing...
Store complete.

#
```

図 9-22 個別 Web 認証画面のカスタムファイルセットの取り出し

```
# store web-authentication html-files ramdisk filesetAAA html-fileset FILESETAAA
Do you wish to store html-files? (y/n): y
executing...
Store complete.

#
```

[注意事項]

個別 Web 認証画面のカスタムファイルセットを取り出すときは，運用コマンド set web-authentication html-files で html-fileset パラメータで指定したカスタムファイルセット名を指定してください。未指定のときは基本 Web 認証画面のファイルセットとして取り出します。

9.5.12 端末からの認証手順

本項では，Web 認証端末からのログイン・ログアウト手順を説明します。Web 認証に必要なコンフィグレーションの設定が終了したあと，下記の手順で行ってください。

（1） 認証前の端末の IP アドレス設定

端末の IP アドレス設定に DHCP サーバを使用したときは，認証対象端末を認証前 VLAN に接続すると，端末から DHCP サーバへ IP アドレス要求が出されます。DHCP サーバは，端末に対して認証前 IP アドレスを配布します。これによって，端末は Web 認証へのアクセスが可能となります。

DHCP サーバを使用しないときは，手動で端末に認証用の IP アドレス（本装置にアクセスするための IP アドレス）を設定してください。

（2） Web 認証のログイン画面表示

Web 認証専用 IP アドレスを設定していない場合は，Web 認証専用の URL（http:// 認証前 VLAN のインタフェース IP アドレス /login.html）にアクセスします。

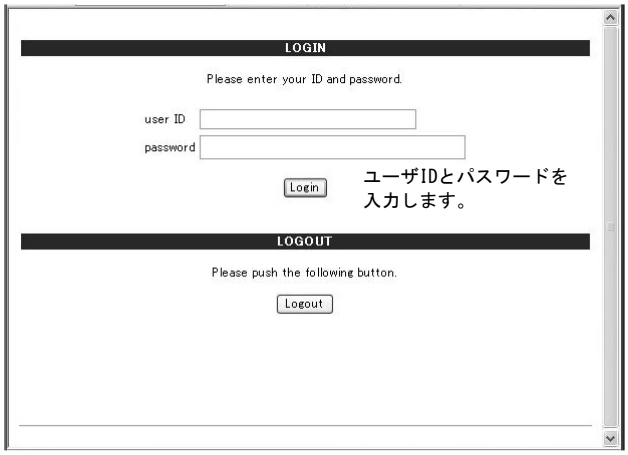
Web 認証専用 IP アドレスを設定している場合は，Web 認証専用 IP アドレスの URL（http://Web 認証専

用 IP アドレス /login.html）にアクセスします。

Web 認証のログイン画面を表示しますので，ログイン画面からユーザ ID とパスワードを入力します。

この画面はログイン・ログアウト共通画面となっています。詳細は，「9.5.12　端末からの認証手順（7）ログイン・ログアウト共通 URL 指定」および「(8) ログイン成功画面でのログアウト操作」を参照してください。

図 9-23　ログイン画面



(3) ログイン画面に入力されたユーザ ID，パスワードの認証

入力されたユーザ ID とパスワードを基に，ローカル認証方式の場合は内蔵 Web 認証 DB に登録されているユーザ情報と一致しているかチェックします。また，RADIUS 認証方式の場合は RADIUS サーバに認証要求を行い，認証可否のチェックをします。

(4) 認証成功時のログイン成功画面表示

内蔵 Web 認証 DB または RADIUS サーバに登録されているユーザ情報と一致した場合，ログイン成功画面を表示し，VLAN 内へ通信できます。さらに，ユーザごとに登録されている VLAN ID に従って VLAN の収容を変更します。

図 9-24　ログイン成功画面

この画面を閉じないで，使用後に画面上の Logout ボタンを押して認証解除することも可能です。ログイン成功画面の Logout ボタン操作については，「9.5.12　端末からの認証手順（8）ログイン成功画面でのログアウト操作」を参照してください。

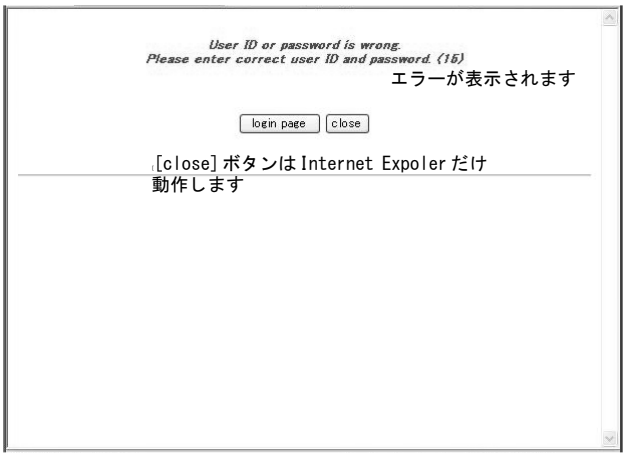
また，コンフィグレーションコマンド web-authentication jump-url で認証成功後にアクセスする URL が指定されている場合は，端末にログイン成功画面が表示されたあとに指定された URL へのアクセスが行われます。

（5） 認証失敗時の画面表示

認証失敗となった場合は，認証エラー画面を表示します。

なお，認証エラー画面に表示するエラーの発生理由を，「8.6　認証エラーメッセージ」に示します。

図 9-25　ログイン失敗画面



（6） ログアウト

端末のログアウトは，次のいずれかで行います。（本装置の認証モードによって，ログアウトのサポート内容が異なります。詳細は，「8　Web 認証の解説」を参照してください。

- 最大接続時間超過時のログアウト
- 認証済み端末の無通信監視によるログアウト
- 認証済み端末の接続監視機能によるログアウト
- 認証済み端末からの特殊フレーム受信によるログアウト
- 認証端末接続ポートのリンクダウンによるログアウト
- VLAN 設定変更によるログアウト
- Web 画面によるログアウト
- 運用コマンドによるログアウト

なお，Web 画面によるログアウト後，および Web 認証から強制的にログアウトされた場合，端末の IP アドレスを認証前の IP アドレスに変更してください。また，DHCP サーバを使用している場合は，端末から IP アドレスの再配布指示を行ってください。

（a） Web 画面によるログアウト

端末から Web 認証に成功した URL（http:// 認証後 VLAN のインタフェース IP アドレス /login.html）にアクセスして，端末にログアウト画面を表示させます。画面上の Logout ボタンを押すと，Web 認証の認証状態をログアウトします。

認証が解除されると，VLAN ID を元の VLAN に収容を変更して，ログアウト完了画面を表示します。

図 9-26 ログアウト画面

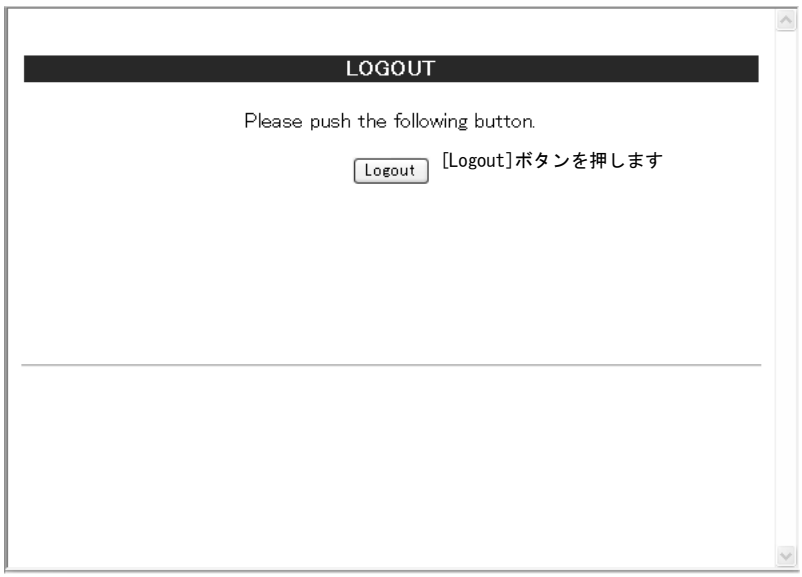
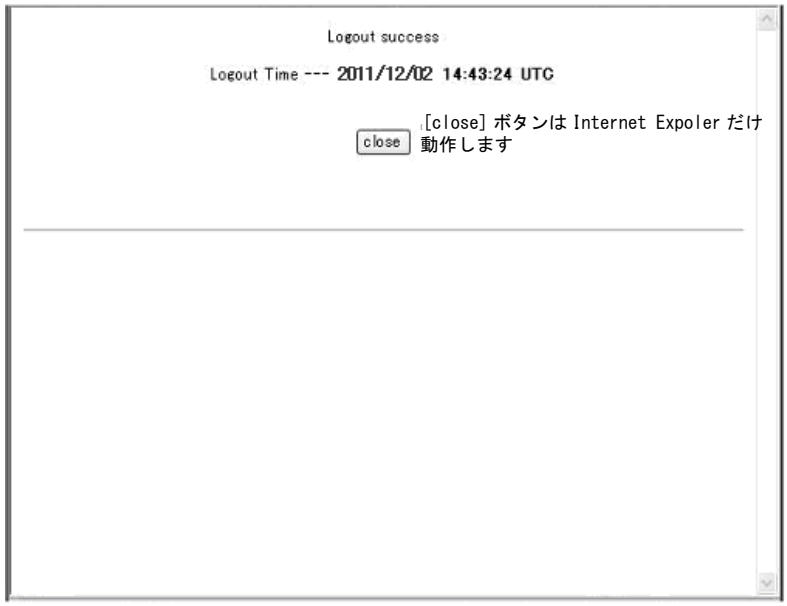


図 9-27 ログアウト完了画面

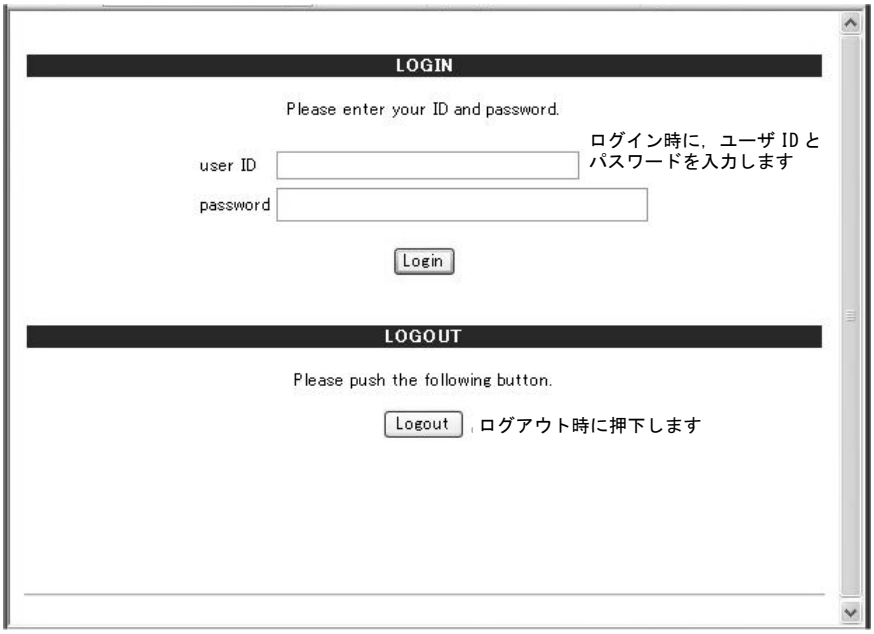


(7) ログイン・ログアウト共通 URL 指定

ログインおよびログアウト時ともに共通の URL（http:// 認証前または認証後 VLAN のインタフェース IP アドレス /）を指定することが可能です。（IP アドレスの次の login.html や logout.html 指定は不要です。）

Logout ボタン操作については，デフォルトゲートウェイの設定が必要です。詳細は「9.5.12 端末からの認証手順（8）ログイン成功画面でのログアウト操作」を参照してください。

図 9-28 ログイン・ログアウト共通画面



(8) ログイン成功画面でのログアウト操作

認証対象ユーザの端末に認証後 VLAN インタフェースの IP アドレスをデフォルトゲートウェイとして設定することにより，ログイン成功画面の Logout ボタン押下でログアウトすることが可能です。(ログイン・ログアウト共通画面での Logout 操作も同様です。)

- 端末の IP アドレス設定に DHCP サーバを使用する場合，配布アドレス情報にデフォルトルータオプションとして認証後 VLAN インタフェースの IP アドレスを設定してください。
- DHCP サーバを使用しない場合は，手動で端末にデフォルトゲートウェイとして認証後 VLAN インタフェースの IP アドレスを設定してください。

Web 認証ログイン時の URL（http:// 認証後 VLAN インタフェースの IP アドレス /）を指定してください。

ログイン成功画面 (図 9-24 ログイン成功画面を参照) を表示したら，この画面を閉じないで使用します。使用後に画面上の Logout ボタンを押して認証解除することが可能です。

(9) 認証済み端末の IP アドレスについて

端末の IP アドレス設定に DHCP サーバを使用したときは，端末の VLAN 収容が変更された後，DHCP サーバから認証後の IP アドレスが配布され，認証後のネットワークにアクセスできます。

DHCP サーバを使用しないときは，ログイン成功画面を表示後に，手動で端末の IP アドレス設定を認証後のネットワークアドレスに変更してください。デフォルトゲートウェイを使用する場合は，デフォルトゲートウェイアドレスの設定も変更してください。

10 MAC 認証の解説

MAC 認証は，MAC アドレスを用いて認証された端末単位に VLAN へのアクセス制御を行う機能です。この章では MAC 認証の概要について説明します。

10.1 概要

MAC 認証は，端末から送信されるフレームの送信元 MAC アドレスを使って端末を認証し，認証済み端末からのフレームだけ通信を許可します。

(1) 認証モード

MAC 認証には次に示す認証モードがあります。

- 固定 VLAN モード
  認証が成功した端末の MAC アドレスを MAC アドレステーブルに登録し，コンフィグレーションで指定された VLAN への通信を可能とします。
- ダイナミック VLAN モード
  認証が成功した端末の MAC アドレスを，MAC VLAN と MAC アドレステーブルに登録して，認証前のネットワークと認証後のネットワークを分離します。

(2) 認証方式グループ

MAC 認証では，次に示す認証方式グループを設定できます。(設定した認証方式グループは，MAC 認証の全認証モードで使用できます。)

- 装置デフォルト：ローカル認証方式
  本装置に内蔵した認証用 DB（内蔵 MAC 認証 DB と呼びます）で認証する方式です。
- 装置デフォルト：RADIUS 認証方式
  ネットワーク内に設置した RADIUS サーバを用いて認証する方式です。
- 認証方式リスト
  特定条件に合致した際に，認証方式リストに登録した任意の RADIUS サーバグループを用いて認証する方式です。

(3) 各認証モードのサポート機能

各認証モードのサポート機能を下記に示します。

表 10-1 各認証モードのサポート機能一覧

機能			固定 VLAN	ダイナミック VLAN
装置デフォルト： ローカル認証	内蔵 MAC 認証 DB		○ 「10.2.1」参照 「10.5.1」参照	○ 「10.3.1」参照 「10.5.1」参照
		MAC アドレス	○ 「11.5.2」参照	○ 「11.5.2」参照
		VLAN	○ 「11.5.2」参照	○ 「11.5.2」参照
		パスワード	×	×
	VLAN（認証後の VLAN）		○ 「10.2.1」参照 「11.3.2」参照	○ 「10.3.1」参照 「11.4.1」参照
装置デフォルト： RADIUS 認証	外部サーバ • MAC 認証専用 RADIUS サーバ情報 • 汎用 RADIUS サーバ情報		○ 「5.3.1」参照 「10.2.1」参照 「10.5.2」参照 「11.2.1」参照	○ 「5.3.1」参照 「10.3.1」参照 「10.5.2」参照 「11.2.1」参照

機能			固定 VLAN	ダイナミック VLAN
		ユーザ ID（MAC アドレス）	1 ～ 32 文字 「10.2.1」参照 「10.5.2」参照 「11.2.4」参照	1 ～ 32 文字 「10.3.1」参照 「10.5.2」参照 「11.2.4」参照
		VLAN	○ 「10.5.2」参照	○ 「10.5.2」参照
		パスワード	1 ～ 32 文字 「10.5.2」参照 「11.2.4」参照	1 ～ 32 文字 「10.5.2」参照 「11.2.4」参照
	VLAN （認証後の VLAN）		○ 「10.2.1」参照 「10.5.2」参照 「11.3.2」参照	○ 「10.3.1」参照 「10.5.2」参照 「11.4.1」参照
	強制認証		○ 「5.4.6」参照	○ 「5.4.6」参照
		認証許可ポート設定	○ 「5.5.4」参照	○ 「5.5.4」参照
		プライベートトラップ	○ 「5.4.6」参照	○ 「5.4.6」参照
	認証要求時の MAC アドレス形式・パスワード指定		○ 「10.5.2」参照 「11.2.4」参照	○ 「10.5.2」参照 「11.2.4」参照
認証方式リスト	外部サーバ • RADIUS サーバグループ情報		○ 「5.3.1」参照 「10.2.1」参照 「10.5.2」参照 「11.2.1」参照	○ 「5.3.1」参照 「10.3.1」参照 「10.5.2」参照 「11.2.1」参照
	ポート別認証方式		○ 「5.2.2」参照 「5.2.3」参照	○ 「5.2.2」参照 「5.2.3」参照
認証制限数	ポート単位		1024 「5.4.8」参照 「5.5.5」参照	1000 「5.4.8」参照 「5.5.5」参照
	装置単位		1024 「5.4.8」参照 「5.5.5」参照	1000 「5.4.8」参照 「5.5.5」参照
認証・再認証	認証再開猶予タイマ		○ 「10.2.2」参照 「11.2.4」参照	○ 「10.3.2」参照 「11.2.4」参照
	定期的再認証要求		○ 「10.2.2」参照 「11.2.4」参照	○ 「10.3.2」参照 「11.2.4」参照
	認証対象 MAC アドレスの制限（MAC アクセスリスト）		○ 「10.2.2」参照 「11.2.2」参照	○ 「10.3.2」参照 「11.2.2」参照
	認証専用 IPv4 アクセスリスト		○ 「5.4.1」参照 「5.5.2」参照	○ 「5.4.1」参照 「5.5.2」参照
認証解除	最大接続時間超過		○ 「10.2.2」参照 「11.2.3」参照	○ 「10.3.2」参照 「11.2.3」参照

機能		固定 VLAN	ダイナミック VLAN
	認証済み端末の無通信監視	○ 「10.2.2」参照 「11.3.2」参照	○ 「10.3.2」参照 「11.4.2」参照
	認証端末接続ポートのリンクダウン	○ 「10.2.2」参照	○ 「10.3.2」参照
	VLAN 設定変更	○ 「10.2.2」参照	○ 「10.3.2」参照
	運用コマンド	○ 「10.2.2」参照	○ 「10.3.2」参照
ローミング（認証済み端末のポート移動）	ポート移動許可設定	○ 「10.2.2」参照 「11.3.2」参照	○ 「10.3.2」参照 「11.4.2」参照
	プライベートトラップ	○ 「10.4」参照	○ 「10.4」参照
アカウントログ	本装置内蔵アカウントログ	「10.4」参照	
	RADIUS サーバのアカウント機能	全モード共通 「5.3.4」参照 「10.4」参照 「11.2.5」参照	

（凡例）

○：サポート

×：未サポート

「5.x.x」参照：「5　レイヤ 2 認証機能の概説」の参照先番号

「10 x . x」参照：本章の参照先番号

「11.x.x」参照：「11　MAC 認証の設定と運用」の参照先番号

MAC 認証の動作条件を次の表に示します。

表 10-2　MAC 認証の動作条件

種別		ポートの設定	設定可能な VLAN 種別	フレーム種別	固定 VLAN モード	ダイナミック VLAN モード
ポートの種類	アクセスポート	native	ポート VLAN MAC VLAN	Untagged	○	×
	トランクポート	native	ポート VLAN MAC VLAN	Untagged	○	×
		allowed	ポート VLAN MAC VLAN	Tagged	○	×
	プロトコルポート	−	−	−	×	×
	MAC ポート	native	ポート VLAN	Untagged	○※	×
		mac	MAC VLAN	Untagged	×	○
		dot1q	ポート VLAN MAC VLAN	Tagged	○	×
デフォルト VLAN					○	×
インタフェース種別	gigabitethernet				○	○
	port channel				○	○

（凡例）
○：動作可
×：動作不可
－：認証ポートでは，設定対象外

注 ※
詳細は「5.4.4　同一 MAC ポートでの自動認証モード収容」を参照してください。

本装置の MAC 認証では，チャネルグループについても一つの束ねられたポートとして扱います。この機能での「ポート」の表現には通常のポートとチャネルグループを含むものとします。

次項からは，「固定 VLAN モード」「ダイナミック VLAN モード」の順に各認証モードの概要を説明します。各認証モードで同じ機能で同一動作については，「～を参照してください。」としていますので，該当箇所を参照してください。

10.2 固定 VLAN モード

認証前の端末は，認証が成功するまで通信できません。固定 VLAN モードで認証が成功すると，MAC アドレステーブルに端末の MAC アドレスと VLAN ID が MAC 認証エントリとして登録されて通信可能になります。(MAC アドレステーブルの登録状態は，運用コマンド show mac-address-table で確認できます。)

10.2.1 認証方式グループ

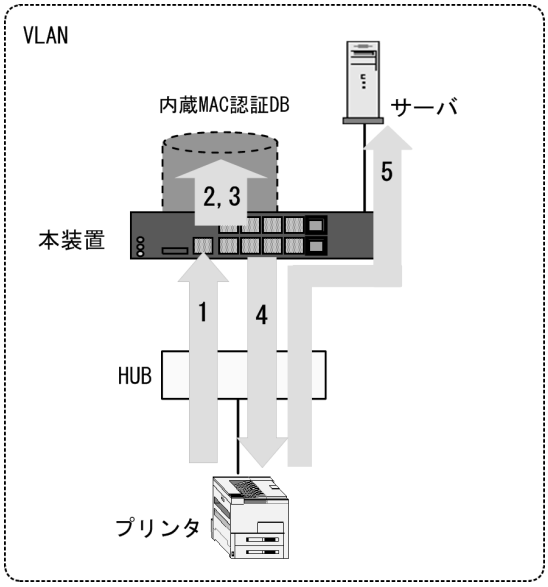
MAC 認証の認証方式グループは，装置デフォルトと認証方式リストを MAC 認証の全認証モード共通で使用します。下記も合わせて参照してください。

- 「5.1.3 認証方式グループ」
- 「5.3.3 装置デフォルトのローカル認証と RADIUS 認証の優先設定」
- 「5.2.2 認証方式リスト」
- 「5.3.1 レイヤ 2 認証機能で使用する RADIUS サーバ情報」
- 「11.2.1 認証方式グループと RADIUS サーバ情報の設定」

(1) 装置デフォルト：ローカル認証

端末から送信されるフレームの送信元 MAC アドレスと，内蔵 MAC 認証 DB の MAC アドレスを照合し，一致した場合は認証成功として通信を許可します。

図 10-1 固定 VLAN モード概要図（ローカル認証方式）



1. HUB 経由で接続された端末（図内のプリンタ）からのフレームを本装置で受信します。
2. . 認証対象端末（図内のプリンタ）の接続ポートまたは VLAN ID により，認証対象端末（図内のプリンタ）が所属する VLAN ID を特定します。
3. 本装置の内蔵 MAC 認証 DB で受信フレームの MAC アドレスを照合します。
   (VLAN ID の照合については，「表 10-3 ローカル認証方式の VLAN ID 照合」を参照してください。)
4. MAC アドレスが登録されていた場合，認証許可となります。
5. 当該端末（図内のプリンタ）は接続されている VLAN に所属するサーバなどと通信が可能になります。

なお，ローカル認証方式には，MAC アドレスだけで照合する方法と，MAC アドレスと VLAN ID との組み合わせで照合する方法があります。これらの方法は，コンフィグレーションコマンド mac-authentication vlan-check で選択できます。

内蔵 MAC 認証 DB には MAC アドレスと MAC マスクの組み合わせでも登録できます。このときの照合の優先順は下記のとおりです。また，MAC アドレスだけのエントリと混在登録可能です。

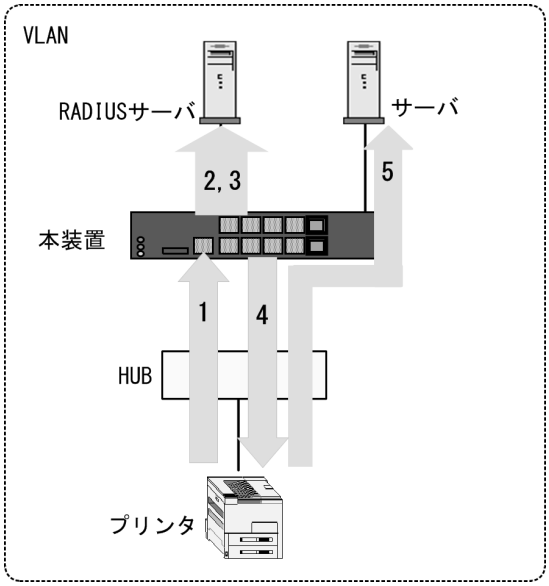
表 10-3　ローカル認証方式の VLAN ID 照合

コンフィグレーション mac-authentication vlan-check	内蔵 MAC 認証 DB の VLAN ID 設定（①②は照合の優先順）	
	あり	なし
設定有	① MAC アドレスと VLAN ID で照合 ② MAC アドレス，MAC マスク，および VLAN ID で照合	① MAC アドレスだけで照合 ② MAC アドレスと MAC マスクで照合
設定無	① MAC アドレスだけで照合 ② MAC アドレスと MAC マスクで照合	① MAC アドレスだけで照合 ② MAC アドレスと MAC マスクで照合

（2） 装置デフォルト：RADIUS 認証

端末から送信されるフレームの送信元 MAC アドレスを使って，外部に設置した RADIUS サーバに認証要求し，認証成功であれば通信を許可します。

図 10-2　固定 VLAN モード概要図（RADIUS 認証方式）



1. HUB 経由で接続された端末（図内のプリンタ）からのフレームを本装置で受信します。
2. 認証対象端末（図内のプリンタ）の接続ポートまたは VLAN ID により，認証対象端末（図内のプリンタ）が所属する VLAN ID を特定します。
3. 外部に設置された RADIUS サーバへ，ユーザ ID（端末の MAC アドレス），パスワード（端末の MAC アドレス，または任意のパスワード），VLAN ID による認証要求を行います。
4. 認証成功であれば，RADIUS サーバから認証成功を受信します。
5. 当該端末（図内のプリンタ）は接続されている VLAN に所属するサーバなどと通信が可能になります。

なお，RADIUS 認証方式には，MAC アドレスだけで照合する方法と，MAC アドレスと VLAN ID との組み合わせで照合する方法があります。これらの方法は，コンフィグレーションコマンド mac-authentication vlan-check で選択できます。

MAC アドレスと VLAN ID による照合時の設定条件を次の表に示します。

表 10-4　RADIUS 認証方式の VLAN ID 照合

コンフィグレーション mac-authentication vlan-check	動作
設定有	MAC アドレスと VLAN ID で照合
設定無	MAC アドレスだけで照合

RADIUS 認証要求に用いる MAC アドレスの形式は，コンフィグレーションコマンド mac-authentication id-format で設定できます。

また，RADIUS サーバへの認証要求に用いるパスワードは，コンフィグレーションコマンド mac-authentication password で設定できます。なお，コンフィグレーションコマンド mac-authentication password が設定されていない場合は，認証を行う端末の MAC アドレスをパスワードとして用います。

詳細は，後述の「10.5　事前準備（2）RADIUS サーバの準備（c）固定 VLAN モードで認証要求時の MAC アドレス形式とパスワード」を参照してください。

（3） 認証方式リスト

MAC 認証では，ポート別認証方式を使用できます。ポート別認証方式の動作については，「5.2.2　認証方式リスト」を参照してください。

10.2.2　認証機能

（1） 認証契機

固定 VLAN モードは，MAC 認証固定 VLAN モードの対象として指定したポートから，本装置が受信した全フレームが認証開始契機となります。

MAC 認証固定 VLAN モードの対象ポートは，コンフィグレーションコマンド mac-authentication port を該当イーサネットポートに設定します。

（2） 認証対象 MAC アドレスの制限

MAC 認証では，MAC アクセスリストを使用して，特定範囲の MAC アドレスを MAC 認証の対象に指定することができます。

- MAC アクセスリストの有効なパラメータ
  送信元 MAC アドレス，送信元マスクの指定内容（宛先 MAC アドレスなどのオプション情報の指定内容は無効です。）
- MAC アクセスリストの許可条件（permit）に一致した MAC アドレスの扱い
  認証対象として認証処理を実施します。
- MAC アクセスリストの廃棄条件（deny）に一致した MAC アドレスの扱い
  認証対象外として認証処理を実施しません。

また，コンフィグレーションコマンド mac-authentication access-group で指定した MAC アクセスリスト

ID が存在しない場合は，MAC アドレス制限なしとしてすべての MAC アドレスが認証対象になります。

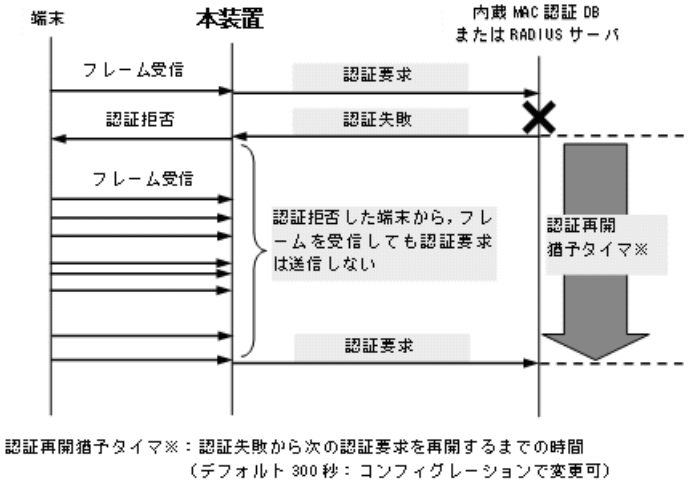
（3） 認証再開猶予タイマ

MAC 認証は，認証再開猶予タイマを設定可能です。

本機能は，認証処理で認証を拒否された端末から，連続してフレームを受信した場合に発生する再認証要求処理を軽減する機能です。

一度 MAC 認証での認証要求で認証拒否された端末から，認証再開猶予タイマ（デフォルトコンフィグレーションは 300 秒）の時間内にフレームを受信しても，認証処理を実施しません。

図 10-3　認証再開猶予タイマ概要



また，本機能は MAC 認証と IEEE802.1X や Web 認証を同一ポートで共存した場合に，不要な MAC 認証失敗ログが採取されることを防止します。

複数の認証機能を同一ポートで共存した構成では，IEEE802.1X や Web 認証を実施予定の端末も，MAC 認証の対象となってしまうため，不要な認証要求処理と MAC 認証失敗ログが採取されてしまいます。

このため，認証再開猶予タイマ期間中に他の認証機能で認証許可された端末は，MAC 認証失敗ログが採取されません。MAC 認証の失敗ログは，認証再開猶予タイマが満了した時点で，他の認証機能で認証許可されていない場合に採取されます。

認証対象 MAC アドレス制限と認証再開猶予タイマを併用することで，不要な認証要求や MAC 認証失敗ログの採取を軽減することができます。

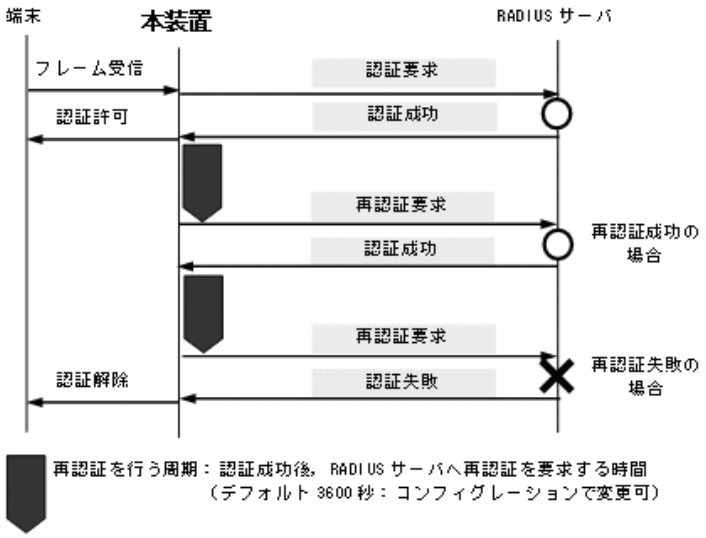
なお，認証再開猶予タイマは，コンフィグレーションコマンド mac-authentication timeout quiet-period で無効に設定，および猶予タイマ値を変更することができます。

（4） 定期的再認証要求

認証成功後，RADIUS サーバの設定情報を反映させるために，認証成功から一定周期（デフォルトコンフィグレーションは 3600 秒）で RADIUS サーバへ再認証要求処理を実施します。

定期的再認証要求の結果，認証成功となれば MAC 認証状態は継続されますが，認証失敗となった場合は強制的に該当端末の MAC 認証状態を解除します。

図 10-4　RADIUS サーバへの定期的再認証要求概要



再認証を行う周期はコンフィグレーションコマンド mac-authentication timeout reauth-period で設定できます。

(5) 強制認証ポート指定

強制認証については，「5.4.6　認証共通の強制認証」を参照してください。

また，強制認証で認証許可した端末は，通常の認証済み端末と同様に後述の「10.2.2　認証機能（7）認証解除」により認証状態が解除されます。

(6) 認証数制限

装置単位およびポート単位に認証数の制限が設定できます。詳細は，「5.4.8　認証共通の端末数制限」を参照してください。

(7) 認証解除

固定 VLAN モードでは，認証解除の手段として下記があります。

- 最大接続時間超過時の認証解除
- 認証済み端末の無通信監視による認証解除
- 認証端末接続ポートのリンクダウンによる認証解除
- VLAN 設定変更による認証解除
- 運用コマンドによる認証解除

(a) 最大接続時間超過時の認証解除

認証済み端末（MAC アドレス）ごとに，認証許可時点からの最大接続時間超過を監視し，超過した端末を自動的に認証解除します。

最大接続時間は，コンフィグレーションコマンド mac-authentication max-timer で設定できます。

(b) 認証済み端末の無通信監視による認証解除

本機能は，認証済み端末が一定時間無通信だった場合に自動的に認証を解除します。

MAC アドレステーブルの MAC 認証エントリを周期的（約 1 分間隔）に監視し，MAC 認証で登録した認

証済み端末からのフレーム受信有無を確認します。該当端末からのフレーム受信を一定時間※検出しなかったときに，MAC アドレステーブルから該当 MAC 認証エントリを削除し，認証を解除します。

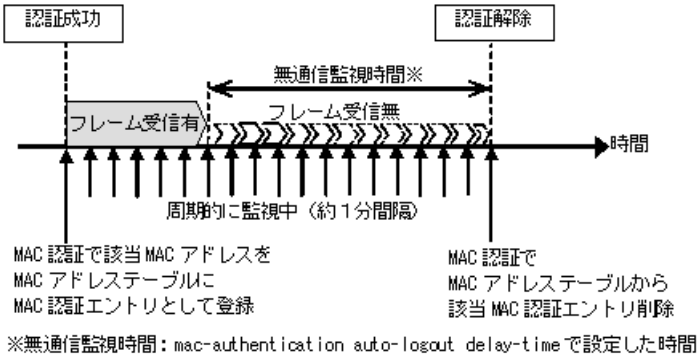
注 ※

コンフィグレーションコマンド mac-authentication auto-logout の設定時間
（delay-time：デフォルトコンフィグレーションは 3600 秒）

無通信監視時間はコンフィグレーションコマンド mac-authentication auto-logout で無通信監視時間を変更，または無効に設定することができます。

なお，無通信監視時間（delay-time）に 0 秒を設定すると，デフォルトコンフィグレーションと同様に 3600 秒で動作します。

図 10-5　認証済み端末の無通信監視概要



認証済み端末の無通信監視は，下記の条件で動作が有効となります。

- MAC 認証固定 VLAN モードまたはダイナミック VLAN モード有効で，mac-authentication auto-logout 有効

コンフィグレーションコマンドで no mac-authentication auto-logout を設定すると，認証を解除しません。

(c) 認証端末接続ポートのリンクダウンによる認証解除

コンフィグレーションコマンド mac-authentication port が設定されたポートでリンクダウンを検出した際に，当該ポートの MAC 認証固定 VLAN モードによる認証済み端末を自動的に認証解除します。

なお，当該ポートにコンフィグレーションコマンド no authentication logout linkdown が設定されている場合は，リンクダウンを検出しても認証済み端末を認証解除しません。詳細は「5.4.10　ポートリンクダウン時の認証解除抑止」「5.5.7　ポートリンクダウン時の認証解除抑止設定」を参照してください。

(d) VLAN 設定変更による認証解除

コンフィグレーションコマンドで認証端末が含まれる VLAN の設定を変更した場合，変更された VLAN に含まれる端末の認証を解除します。

［コンフィグレーションの変更内容］

- VLAN を削除した場合
- VLAN を停止（suspend）した場合

(e) 運用コマンドによる認証解除

運用コマンド clear mac-authentication auth-state 実行で，MAC 認証許可状態の端末の一部，または全

MAC 認証端末を手動で認証解除します。

（8） ローミング（認証済み端末のポート移動）

HUB などを経由して接続した認証済み端末（下図ではプリンタ）を，MAC 認証設定ポートへリンクダウンしないでポート移動した場合でも，認証済み状態のまま継続して通信可能にします。

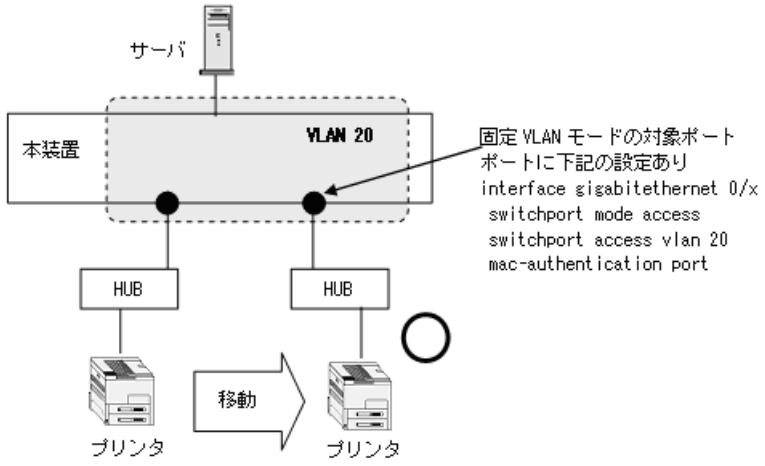
ローミングの動作可能な条件は下記のとおりです。

- コンフィグレーションコマンド mac-authentication static-vlan roaming 設定有
- 移動前および移動後が，固定 VLAN モード対象ポート
- 移動前および移動後が，同一 VLAN

上記以外の条件でポート移動を検出したときは，該当端末の認証を強制的に解除します。

なお，HUB などを経由して認証済み端末を MAC 認証未設定ポートへ移動したときは，該当端末の認証を解除しません。MAC 認証未設定ポートへ移動したときに認証を解除する場合は，コンフィグレーションコマンド authentication auto-logout strayer を設定してください。

図 10-6　固定 VLAN モード　ローミング概要図



10.3　ダイナミック VLAN モード

認証前の端末は，認証が成功するまで通信できません。ダイナミック VLAN モードで認証が成功すると，MAC VLAN と MAC アドレステーブルに端末の MAC アドレスと認証後 VLAN ID が MAC 認証エントリとして登録されて通信可能になります。（MAC アドレステーブルの登録状態は , 運用コマンド show mac-address-table で確認できます。）

10.3.1　認証方式グループ

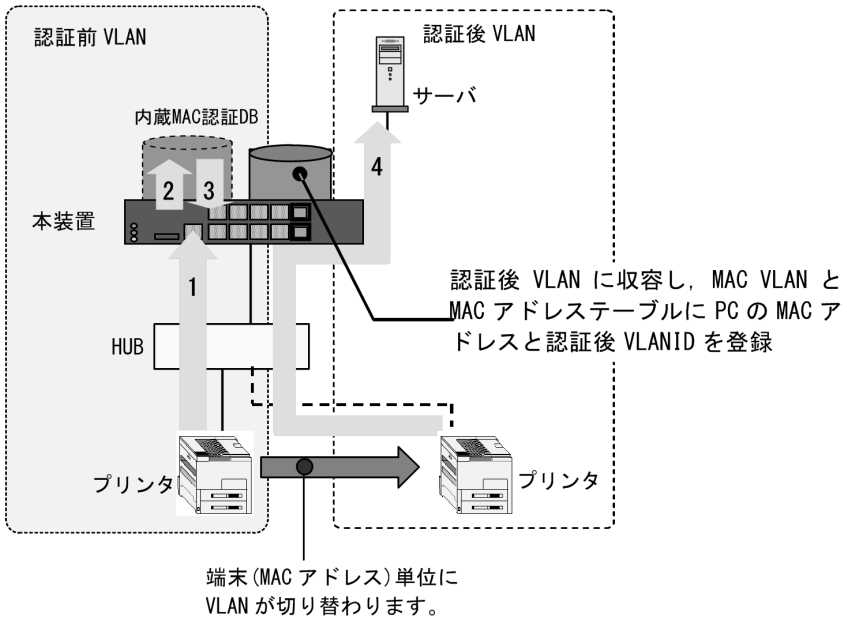
MAC 認証の認証方式グループは，装置デフォルトと認証方式リストを MAC 認証の全認証モード共通で使用します。下記も合わせて参照してください。

- 「5.1.3　認証方式グループ」
- 「5.3.3　装置デフォルトのローカル認証と RADIUS 認証の優先設定」
- 「5.2.2　認証方式リスト」
- 「5.3.1　レイヤ 2 認証機能で使用する RADIUS サーバ情報」
- 「11.2.1　認証方式グループと RADIUS サーバ情報の設定」

（1）装置デフォルト：ローカル認証

端末から送信されるフレームの送信元 MAC アドレスと内蔵 MAC 認証 DB の MAC アドレスを照合し，一致した場合は認証成功として内蔵 MAC 認証 DB に登録されている VLAN に収容し，通信を許可します。

図 10-7　ダイナミック VLAN モード概要図（ローカル認証方式）



1. HUB 経由で接続された端末（図内のプリンタ）からのフレームを本装置で受信します。
2. 本装置の内蔵 MAC 認証 DB で受信フレームの MAC アドレスを照合します。
3. MAC アドレスが登録されていた場合，内蔵 MAC 認証 DB に登録されている VLAN に従い収容 VLAN が決定します。
4. 当該端末（図内のプリンタ）は内蔵 MAC 認証 DB に登録されている VLAN に収容され（認証後 VLAN），認証後 VLAN に所属するサーバなどと通信が可能になります。また，認証した端末の MAC

アドレスと VLAN ID を，MAC VLAN と MAC アドレステーブルに登録します。

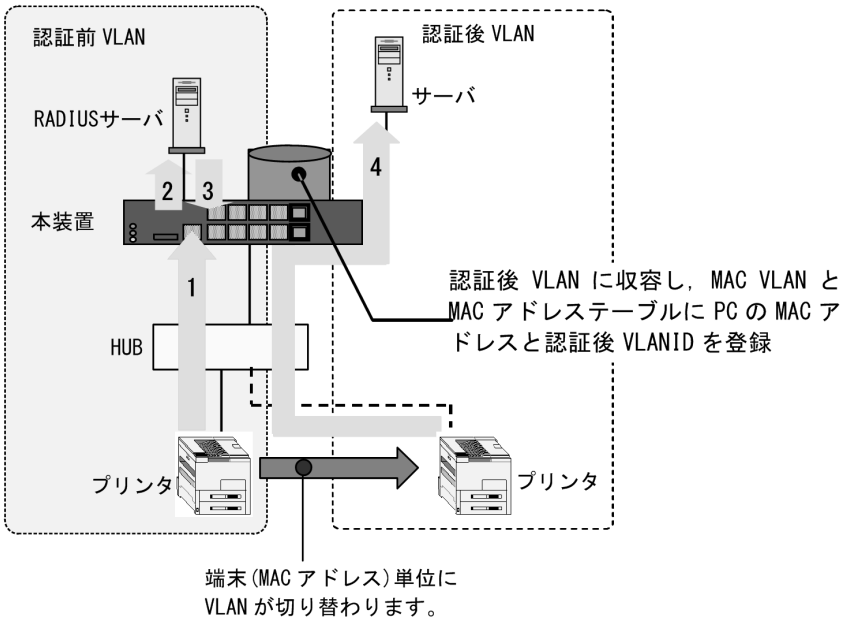
(a) 収容 VLAN の切り替えについて

「5.4.3　MAC VLAN の自動 VLAN 割当」「5.4.4　同一 MAC ポートでの自動認証モード収容」を参照してください。

(2) 装置デフォルト：RADIUS 認証

端末から送信されるフレームの送信元 MAC アドレスを使って外部に設置した RADIUS サーバに認証要求し，認証成功であれば指定された認証後 VLAN に収容し通信を許可します。

図 10-8　ダイナミック VLAN モード概要図（RADIUS 認証方式）



1. HUB 経由で接続された端末（図内のプリンタ）からのフレームを本装置で受信します。
2. 外部に設置された RADIUS サーバへ，ユーザ ID（端末の MAC アドレス），パスワード（端末の MAC アドレス，または任意のパスワード）による認証要求を行います。
3. 認証成功であれば，RADIUS サーバから VLAN 情報を受信します。
4. 当該端末（図内のプリンタ）は RADIUS サーバから受信した VLAN に収容され（認証後 VLAN），認証後 VLAN に所属するサーバなどと通信が可能になります。また，認証した端末の MAC アドレスと VLAN ID を，MAC VLAN と MAC アドレステーブルに登録します。

(a) 収容 VLAN の切り替えについて

「5.4.3　MAC VLAN の自動 VLAN 割当」「5.4.4　同一 MAC ポートでの自動認証モード収容」を参照してください。

(3) 認証方式リスト

MAC 認証では，ポート別認証方式を使用できます。ポート別認証方式の動作については，「5.2.2　認証方式リスト」を参照してください。

10.3.2 認証機能

(1) 認証契機

ダイナミック VLAN モードは，MAC 認証ダイナミック VLAN モードの対象として指定したポートから，本装置が受信した全フレームが認証開始契機となります。

MAC 認証ダイナミック VLAN モードの対象ポートは，コンフィグレーションコマンド mac-authentication port を該当イーサネットポートに設定します。該当イーサネットポートのポート種別（コンフィグレーションコマンド switchport mode）には，MAC ポートを設定しておいてください。

(2) 認証対象 MAC アドレスの制限

固定 VLAN モードと同様です。「10.2.2 認証機能 (2) 認証対象 MAC アドレスの制限」を参照してください。

(3) 認証再開猶予タイマ

固定 VLAN モードと同様です。「10.2.2 認証機能 (3) 認証再開猶予タイマ」を参照してください。

(4) 定期的再認証要求

固定 VLAN モードと同様です。「10.2.2 認証機能（4）定期的再認証要求」を参照してください。

(5) 強制認証ポート指定

強制認証については，「5.4.6 認証共通の強制認証」を参照してください。

また，強制認証で認証許可した端末は，通常の認証済み端末と同様に後述の「10.3.2 認証機能（7）認証解除」により認証状態が解除されます。

(6) 認証数制限

装置単位およびポート単位に認証数の制限が設定できます。詳細は，「5.4.8 認証共通の端末数制限」を参照してください。

(7) 認証解除

ダイナミック VLAN モードでは，認証解除の手段として下記があります。

- 最大接続時間超過時の認証解除
- 認証済み端末の無通信監視による認証解除
- 認証端末接続ポートのリンクダウンによる認証解除
- VLAN 設定変更による認証解除
- 運用コマンドによる認証解除

各認証解除手段は，固定 VLAN モードと同様です。「10.2.2 認証機能 (7) 認証解除」を参照してください。

(8) ローミング（認証済み端末のポート移動）

HUB などを経由して接続した認証済み端末（下図ではプリンタ）を，MAC 認証設定ポートへリンクダウンしないでポート移動した場合でも，認証済み状態のまま継続して通信可能にします。

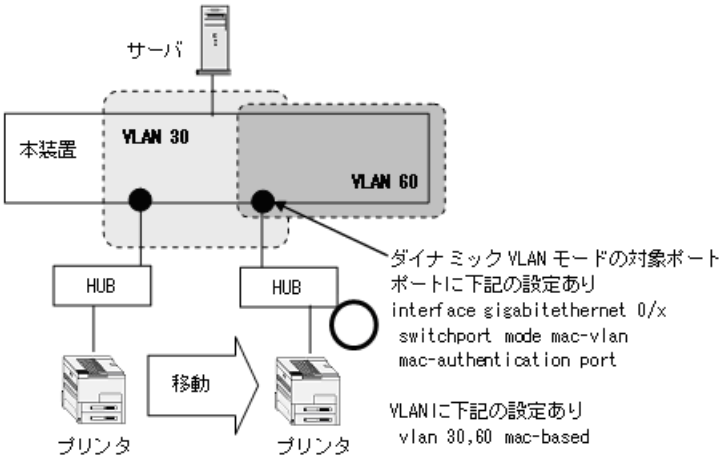
ローミングの動作可能な条件は下記のとおりです。

- コンフィグレーションコマンド mac-authentication roaming 設定有
- 移動前および移動後が，ダイナミック VLAN モード対象ポート

上記以外の条件でポート移動を検出したときは，該当端末の認証を強制的に解除します。

なお，HUB などを経由して認証済み端末を MAC 認証未設定ポートへ移動したときは，該当端末の認証を解除しません。MAC 認証未設定ポートへ移動したときに認証を解除する場合は，コンフィグレーションコマンド authentication auto-logout strayer を設定してください。

図 10-9　ダイナミック VLAN モード　ローミング概要図



10.4　アカウント機能

MAC 認証の認証結果は，次のアカウント機能で記録されます。

- 本装置内蔵のアカウントログ
- RADIUS サーバのアカウント機能への記録
- RADIUS サーバへの認証情報の記録
- syslog サーバへのアカウントログ出力

（1） 本装置内蔵のアカウントログ

MAC 認証の認証結果や動作情報などの動作ログは，本装置内蔵のアカウントログに記録されます。

本装置内蔵のアカウントログは以下の最大数まで記録できます。

- スタック動作時：全認証機能の合計で最大 4096 行
- スタンドアロン動作時：MAC 認証全体で最大 2100 行

最大数を超えた場合，古い順に記録が削除され，最新のアカウントログ情報が追加記録されていきます。

記録されるアカウントログ情報は次の情報です。

表 10-5　本装置内蔵のアカウントログへの出力情報

アカウントログ種別		時刻	MAC	VLAN	PORT	メッセージ
LOGIN	成功	○	○	○	○	認証成功メッセージ
	失敗	○	○	○※	○※	認証失敗要因メッセージ
LOGOUT		○	○	○※	○	認証解除メッセージ
SYSTEM		○	○	○※	○※	MAC 認証機能の動作に関するメッセージ（ローミング検出，強制認証許可も含む）

（凡例）
　○：出力します。
　×：出力しません。

注 ※
　メッセージによっては出力しない場合があります。

メッセージの詳細については，「運用コマンドレファレンス　30　MAC 認証　show mac-authentication logging」を参照してください。

また，記録されたアカウントログの出力機能については下記のとおりです。

1. 運用コマンド表示
   運用コマンド show mac-authentication logging で，採取されているアカウントログを最新の情報から表示します。
2. syslog サーバへ出力
   後述「(4) syslog サーバへのアカウントログ出力」を参照してください。
3. プライベート Trap
   MAC 認証の特定イベントのアカウントログ採取を契機にプライベート Trap を発行する機能をサポートしています。プライベート Trap 発行可否および発行種別はコンフィグレーションコマンドで設定してください。

表 10-6 アカウントログ（LOGIN/LOGOUT）とプライベート Trap 発行条件 (1)

アカウントログ種別		プライベート Trap 発行に必要なコンフィグレーション設定	
		コマンド	パラメータ
LOGIN	成功	snmp-server host	mac-authentication
		snmp-server traps	mac-authentication-trap all
	失敗	snmp-server host	mac-authentication
		未設定，または下記のどちらかを設定	
		snmp-server traps	mac-authentication-trap all
		snmp-server traps	mac-authentication-trap failure
LOGOUT		snmp-server host	mac-authentication
		snmp-server traps	mac-authentication-trap all

表 10-7 アカウントログ (SYSTEM) とプライベート Trap 発行条件 (2)

アカウントログ種別 SYSTEM	認証モード	プライベート Trap 発行に必要なコンフィグレーション設定	
		コマンド	パラメータ
ローミング	固定 VLAN	snmp-server host	mac-authentication
		mac-authentication static-vlan roaming	action trap
	ダイナミック VLAN	snmp-server host	mac-authentication
		mac-authentication roaming	action trap

強制認証のプライベート Trap については，「5.4.6 認証共通の強制認証（4）強制認証でのプライベート Trap」を参照してください。

（2） RADIUS サーバのアカウント機能への記録

コンフィグレーションコマンド aaa accounting mac-authentication で，RADIUS サーバのアカウント機能を使用できます。

なお，RADIUS サーバへアカウンティング情報を送信するときに使用する RADIUS 属性については，「10.5 事前準備」を参照してください。

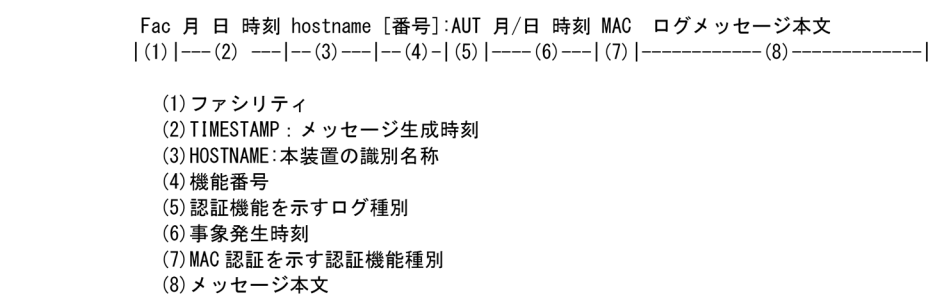
（3） RADIUS サーバへの認証情報の記録

RADIUS 認証方式の場合は，RADIUS サーバが持っている機能によって，認証成功／認証失敗が記録されます。ただし，使用する RADIUS サーバによって記録される情報が異なることがありますので，詳細は RADIUS サーバの説明書を参照してください。

（4） syslog サーバへのアカウントログ出力

コンフィグレーションで syslog 設定されているすべての syslog サーバへ，装置全体の運用ログ情報と合わせて MAC 認証のアカウントログ情報を出力します。

図 10-10 syslog サーバ出力形式



syslog サーバへのログ出力について詳細は，後述の「23 ログ出力機能」を参照してください。

なお，コンフィグレーションコマンド mac-authentication logging enable および logging event-kind aut によって，MAC 認証のアカウントログ出力を開始および停止できます。

10.5　事前準備

10.5.1　ローカル認証の場合

ローカル認証方式を使用するにあたっては，次の準備が必要です。

- コンフィグレーションの設定
- 内蔵 MAC 認証 DB の登録
- 内蔵 MAC 認証 DB のバックアップ
- 内蔵 MAC 認証 DB の復元

（1） コンフィグレーションの設定

MAC 認証を使用するために，本装置に VLAN 情報や MAC 認証の情報をコンフィグレーションコマンドで設定します。（「11.1　MAC 認証のコンフィグレーション」を参照してください。）

（2） 内蔵 MAC 認証 DB の登録

ローカル認証方式を使用する前に，運用コマンドで事前に MAC アドレス情報（認証対象端末の MAC アドレスや認証後 VLAN ID）を内蔵 MAC 認証 DB に登録しておく必要があります。

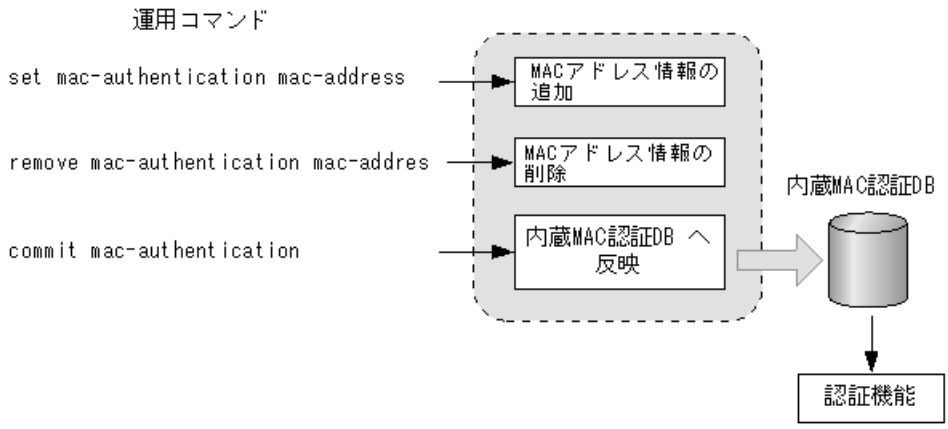
内蔵 MAC 認証 DB へ登録手順として，MAC アドレス情報の編集（追加・削除）と内蔵 MAC 認証 DB への反映があります。手順を以下に示します。

なお，MAC アドレス情報の追加を行う前に，MAC 認証システムの環境設定およびコンフィグレーションの設定を完了している必要があります。

- 運用コマンド set mac-authentication mac-address で，MAC アドレス情報（認証対象端末の MAC アドレスや認証後 VLAN ID）を追加します。
- 登録済みの MAC アドレス情報を削除する場合は，運用コマンド remove mac-authentication mac-address で行います。
- 編集した MAC アドレス情報は，運用コマンド commit mac-authentication 実行により，内蔵 MAC 認証 DB へ反映されます。

また，運用コマンド show mac-authentication mac-address で，運用コマンド commit mac-authentication を実行するまでに編集した MAC アドレス情報をみることができます。

図 10-11　MAC アドレス情報の編集と内蔵 MAC 認証 DB への反映



ローカル認証方式では，運用コマンド show mac-authentication mac-address の表示順で MAC アドレスを検索します。

(a) 同一 MAC アドレスの登録について

内蔵 MAC 認証 DB には異なる VLAN ID（VLAN 設定無も含む）で同一の MAC アドレスを複数設定できます。

(b) MAC マスク情報の登録について

内蔵 MAC 認証 DB には，MAC アドレスと MAC マスクのエントリを登録できます。

MAC マスク付きのエントリは，ほかの MAC マスク付きエントリに包含される条件でも登録できます。（エントリの数値が完全一致する場合だけ登録できません。）

any 条件は 1 エントリだけ登録できます。（すでに登録済みの場合は , 上書されます。）

運用コマンド show mac-authentication mac-address では MAC アドレスの昇順で表示しますが，MAC アドレスだけの登録エントリ，MAC マスク付きの登録エントリ，any 条件のエントリの順となります。

(3) 内蔵 MAC 認証 DB のバックアップ

運用コマンド store mac-authentication で，内蔵 MAC 認証 DB のバックアップを取ることができます。

バックアップファイルは，MAC アドレスエントリだけのファイルと，MAC マスク付きエントリを含むファイルの 2 種類が自動で生成されます。

- < ファイル名 >　　: MAC マスク付きエントリを含まないファイル
- < ファイル名 >.msk : MAC マスク付きエントリを含むファイル

(4) 内蔵 MAC 認証 DB の復元

運用コマンド load mac-authentication で，バックアップファイルから内蔵 MAC 認証 DB の復元ができます。

ただし，直前までに運用コマンド set mac-authentication mac-address などで編集および登録した内容は廃棄され，復元された内容に置き換わりますので，復元の実行には注意が必要です。

バックアップファイルは，MAC アドレスエントリだけのファイルと，MAC マスク付きエントリを含むファイルが自動生成されます。（前述の「(3) 内蔵 MAC 認証 DB のバックアップ」を参照してください。）

- MAC アドレスエントリだけで使用するときは，MAC マスク付きエントリを含まないバックアップファイルから復元してください。
- MAC アドレスと MAC マスク付きエントリで使用するときは，MAC マスク付きエントリを含むバックアップファイルから復元してください。

10.5.2 RADIUS 認証の場合

RADIUS 認証方式を使用するにあたっては，次の準備が必要です。

- コンフィグレーションの設定
- RADIUS サーバの準備

(1) コンフィグレーションの設定

MAC 認証を使用するために，本装置に VLAN 情報や MAC 認証の情報をコンフィグレーションコマンドで設定します。(「11.1 MAC 認証のコンフィグレーション」を参照してください。)

(2) RADIUS サーバの準備

(a) 使用する RADIUS 属性

本装置が使用する RADIUS の属性名を次の表に示します。

表 10-8 認証で使用する属性名（その 1 Access-Request）

属性名	Type 値	解説
User-Name	1	端末の MAC アドレス。 端末の MAC アドレスを 1 バイトごとにハイフン（−）で区切った形式※1
User-Password	2	ユーザパスワード。 端末の MAC アドレスを 1 バイトごとにハイフン（−）で区切った形式※1
NAS-IP-Address	4	認証を要求している，本装置の IPv4 アドレス。 IPv4 アドレスが登録されている VLAN インタフェースのうち，最も小さい VLAN ID の IPv4 アドレスを使用します。
NAS-Port	5	• 固定 VLAN モード：認証している認証単位の IfIndex • ダイナミック VLAN モード：認証している認証単位の IfIndex
Service-Type	6	提供するサービスタイプ。 Framed(2) 固定。
Called-Station-Id	30	認証ポートの MAC アドレス (小文字 ASCII※2，ハイフン（−）区切り)。
Calling-Station-Id	31	端末の MAC アドレス（小文字 ASCII※2，ハイフン（−）区切り)。
NAS-Identifier	32	• 固定 VLAN モード 認証要求端末が所属する VLAN の VLAN ID。 VLAN10 の場合 "10" • ダイナミック VLAN モード コンフィグレーションコマンド hostname で設定された文字列。
NAS-Port-Type	61	端末が認証に使用している物理ポートのタイプ。 Virtual(5)
Connect-Info	77	コネクションの特徴を示す文字列。 • 固定 VLAN モード： 物理ポート ("CONNECT Ethernet") チャネルグループポート ("CONNECT Port-Channel ") • ダイナミック VLAN モード： 物理ポート ("CONNECT Ethernet") チャネルグループポート ("CONNECT Port-Channel ")
NAS-Port-Id	87	ポートを識別するための文字列（x，y には数字が入ります)。 • 固定 VLAN モード："Port x/y"，"ChGr x" • ダイナミック VLAN モード："Port x/y"，"ChGr x"

属性名	Type 値	解説
NAS-IPv6-Address	95	認証を要求している，本装置の IPv6 アドレス。 IPv6 アドレスが登録されている VLAN インタフェースのうち，最も小さい VLAN ID の IPv6 アドレスを使用します。

注 ※1

後述の「(b) RADIUS サーバに設定する情報」を参照してください。

注 ※2

本装置では，「Called-Station-Id」「Calling-Station-Id」の MAC アドレスを小文字で使用しますが，コンフィグレーションコマンド radius-server attribute station-id capitalize により，MAC アドレス内の "a" ～ "f" の文字を大文字形式にできます。

表 10-9 認証で使用する属性名（その２ Access-Accept）

属性名	Type 値	解説
Service-Type	6	提供するサービスタイプ。 Framed(2) 固定。
Filter-Id	11	テキスト文字列。 マルチステップ認証で使用 ※1。
Reply-Message	18	未使用 ※2
Tunnel-Type	64	トンネル・タイプ ※3。 VLAN(13) 固定。
Tunnel-Medium-Type	65	トンネルを作成する際のプロトコル ※3。 IEEE802(6) 固定。
Tunnel-Private-Group-ID	81	VLAN を識別する文字列 ※4。 次に示す文字列が対応する。 (1)VLAN ID を示す文字列 (2)"VLAN"+VLAN ID を示す文字列 文字列にスペースを含んではいけない（含めた場合 VLAN 割り当ては失敗する）。 (3) コンフィグレーションコマンド name で VLAN インタフェースに設定された VLAN 名称を示す文字列（VLAN ID の小さいほうを優先）※5 （設定例） VLAN ID ：10 コンフィグレーションコマンド name：Authen_VLAN (1) の場合 "10" (2) の場合 "VLAN10" (3) の場合 "Authen_VLAN"

注 ※1

マルチステップ認証で使用する文字列については，「12 マルチステップ認証」を参照してください。

注 ※2

Reply-Message の文字列はアカウントログとして本装置で採取しています。

注 ※3

Tag 領域は無視します。

注 ※4

本装置では文字列形式の選択および VLAN ID の識別を下記条件で実施します。

1. Tunnel-Private-Group-ID の文字列形式 (1)(2)(3) 選択条件
   - 先頭が 0 ～ 9 の数字文字で始まる文字列は，(1) の形式
   - 先頭が "VLAN" ＋ 0 ～ 9 の数字文字で始まる文字列は，(2) の形式

- 上記以外の文字列は，(3) の形式

なお，先頭 1 バイトが 0x00 ～ 0x1f のときは Tag 付きですが Tag 領域は無視します。

2. (1)(2) 形式の文字列から VLAN ID を識別する条件
   - 数字文字 "0" ～ "9" だけを 10 進数に変換し，先頭 4 文字だけ有効範囲とします。（5 文字目以降は無視します。）
     例) "0010" は "010" や "10" と同じで，VLAN ID = 10　となります。
     "01234" は，VLAN ID =123　となります。
   - 文字列の途中に "0" ～ "9" 以外が入っていると，文字列の終端とします。
     例)"12+3" は，VLAN ID =12　となります。

注 ※5

コンフィグレーションコマンド name による VLAN 名称指定については，「5.4.2　VLAN 名称による収容 VLAN 指定」を参照してください。

表 10-10　RADIUS アカウント機能で使用する属性名

属性名	Type 値	解説
User-Name	1	端末の MAC アドレス。 端末の MAC アドレスを 1 バイトごとにハイフン（－）で区切った形式 ※1
NAS-IP-Address	4	認証を要求している，本装置の IPv4 アドレス。 IPv4 アドレスが登録されている VLAN インタフェースのうち，最も小さい VLAN ID の IPv4 アドレスを使用します。
NAS-Port	5	• 固定 VLAN モード：認証している認証単位の IfIndex • ダイナミック VLAN モード：認証している認証単位の IfIndex
Service-Type	6	提供するサービスタイプ。 Framed(2) 固定。
Calling-Station-Id	31	認証端末の MAC アドレス（小文字 ASCII※2，ハイフン（－）区切り）。
NAS-Identifier	32	• 固定 VLAN モード 認証要求端末が所属する VLAN の VLAN ID。 VLAN10 の場合 "10" • ダイナミック VLAN モード コンフィグレーションコマンド hostname で設定された文字列。
Acct-Status-Type	40	アカウンティング要求種別。 Start(1)，Stop(2)
Acct-Delay-Time	41	アカウンティング情報（送信遅延時間）。(秒)
Acct-Input-Octets	42	アカウンティング情報（受信オクテット数）。 (0) 固定。
Acct-Output-Octets	43	アカウンティング情報（送信オクテット数）。 (0) 固定。
Acct-Session-Id	44	アカウンティング情報を識別する ID。
Acct-Authentic	45	認証方式。 RADIUS(1)，Local(2)
Acct-Session-Time	46	アカウンティング情報（セッション持続時間）。 (0) 固定。
Acct-Input-Packets	47	アカウンティング情報（受信フレーム数）。 (0) 固定。
Acct-Output-Packets	48	アカウンティング情報（送信フレーム数）。 (0) 固定。
Acct-Terminate-Cause	49	アカウンティング情報（セッション終了要因）。 「表 10-11　Acct-Terminate-Cause での切断要因」を参照。

属性名	Type 値	解説
NAS-Port-Type	61	端末が認証に使用している物理ポートのタイプ。 Virtual(5) 固定。
NAS-Port-Id	87	ポートを識別するための文字列（x，y には数字が入ります）。 • 固定 VLAN モード："Port x/y"，"ChGr x" • ダイナミック VLAN モード："Port x/y"，"ChGr x"
NAS-IPv6-Address	95	認証を要求している，本装置の IPv6 アドレス。 IPv6 アドレスが登録されている VLAN インタフェースのうち，最も小さい VLAN ID の IPv6 アドレスを使用します。

注 ※1

後述の「(b) RADIUS サーバに設定する情報」を参照してください。

注 ※2

本装置では，「Calling-Station-Id」の MAC アドレスを小文字で使用しますが，コンフィグレーションコマンド radius-server attribute station-id capitalize により，MAC アドレス内の "a" ～ "f" の文字を大文字形式にできます。

表 10-11 Acct-Terminate-Cause での切断要因

属性名	Type 値	解説
User Request	1	端末移動を検出したため切断した。
Idle Timeout	4	無通信時間が一定時間続いたため切断した。
Session Timeout	5	セッション期限が満了したため切断した。
Admin Reset	6	管理者の意思で切断した。 • コンフィグレーションで mac-authentication port を削除した場合 その他認証用コンフィグレーションの変更や運用コマンドによる切断要因を含む。
NAS Request	10	マルチステップ認証で２段目が成功したため，１段目の MAC 認証を切断した。
Service Unavailable	15	サービスを提供できなくなった。 • 認証済み端末のポート移動（ローミング）時に，移動先ポートで authentication max-user の設定数超過を検出したため認証解除した場合
Reauthentication Failure	20	再認証に失敗した。
Port Reinitialized	21	ポートの MAC が再初期化された。 • ポートがリンクダウンした場合 • コンフィグレーションでポートから vlan を削除した場合 • コンフィグレーションで shutdown を設定した場合 • 運用コマンド inactivate を実行した場合

(b) RADIUS サーバに設定する情報

MAC 認証機能が RADIUS サーバへ認証要求する際のユーザ ID，パスワードはいずれも端末の MAC アドレスとなります。RADIUS サーバに MAC 認証端末情報を設定する際は，ユーザ ID 部，パスワード部ともに端末の MAC アドレスを１バイトごとにハイフン（－）で区切った形で設定してください。

ユーザ ID の MAC アドレス形式，パスワードはコンフィグレーションによる指定も可能です。コンフィグレーションで指定したときの形式については，後述の「(c) 固定 VLAN モードで認証要求時の MAC アドレス形式とパスワード」「(d) ダイナミック VLAN モードで認証要求時の MAC アドレス形式とパスワード」を参照してください。

なお，RADIUS サーバの詳細な設定方法については，使用する RADIUS サーバの説明書を参照してください。

下記の認証端末情報を例に，RADIUS サーバ設定例を示します。

- 端末の MAC アドレス「12-34-56-00-ff-e1」
- 固定 VLAN モードの場合：認証要求端末が所属する VLAN の VLAN ID「10」
- ダイナミック VLAN モードの場合：認証後 VLAN「311」
- コンフィグレーションコマンド name の設定：「mac-authen-vlan」

表 10-12　RADIUS サーバ設定例

設定項目	設定内容
User-Name	12-34-56-00-ff-e1 端末の MAC アドレスを 1 バイトごとにハイフン（−）で区切った形式※1
Auth-Type	Local
User-Password	12-34-56-00-ff-e1 端末の MAC アドレスを 1 バイトごとにハイフン（−）で区切った形式※2
NAS-Identifier	固定 VLAN モードの場合 "10" 認証要求端末が所属する VLAN の VLAN ID を数字文字で設定。
Tunnel-Type	Virtual VLAN（値 13）
Tunnel-Medium-Type	IEEE-802（値 6）
Tunnel-Private-Group-ID	ダイナミック VLAN モードの場合 下記のいずれかの形式 • "311" 認証後 VLAN ID を数字文字で設定。 • "VLAN0311" 文字列 "VLAN" に続いて，認証後 VLAN ID を数字文字で設定。 • "mac-authen-vlan" コンフィグレーションコマンド name で設定された VLAN 名称を示す文字列。
認証方式	PAP

注 ※1

MAC アドレスに "A ～ F" が含まれる場合は，必ず "a ～ f"（小文字）で RADIUS サーバに設定してください。
コンフィグレーションで MAC アドレス形式を設定している場合は，コンフィグレーションの形式で設定してください。

注 ※2

コンフィグレーションで MAC アドレス形式を設定している場合は，コンフィグレーションの形式で設定してください。
コンフィグレーションでパスワードを設定している場合は，コンフィグレーションの文字列で設定してください。

(c) 固定 VLAN モードで認証要求時の MAC アドレス形式とパスワード

固定 VLAN モードでは，VLAN が移動しないため RADIUS サーバへの認証要求結果に含まれている VLAN ID は意識しません。よって意図しない VLAN からでも認証許可される弊害を防止するため，以下の 2 種類の VLAN 制限機能をサポートしています。

- User-Name 使用による VLAN 制限
- NAS-Identifier 使用による VLAN 制限

1. User-Name 使用による VLAN 制限
   RADIUS サーバへ認証要求時に，MAC アドレスに区切り文字列（デフォルトコンフィグレーションは "%VLAN"）と付加情報（VLAN ID）を含めたユーザ ID を生成して実施します。区切り文字列はコンフィグレーションコマンド mac-authentication vlan-check で指定できます。
   MAC アドレス =12-34-56-00-ff-e1，VLAN ID=100 の場合の例を下表に示します。

表 10-13　コンフィグレーションの設定と RADIUS サーバへの認証要求形式

コンフィグレーションの設定			RADIUS サーバへの認証要求形式	
id-format	vlan-check	password	ユーザ ID	パスワード
無	無	無	12-34-56-00-ff-e1	12-34-56-00-ff-e1
	vlan-check		12-34-56-00-ff-e1%VLAN100	
	vlan-check key @VLAN		12-34-56-00-ff-e1@VLAN100	
id-format 0	無		12-34-56-00-ff-e1	12-34-56-00-ff-e1
	vlan-check		12-34-56-00-ff-e1%VLAN100	
	vlan-check key @VLAN		12-34-56-00-ff-e1@VLAN100	
id-format 0 capitals	無		12-34-56-00-FF-E1	12-34-56-00-FF-E1
	vlan-check		12-34-56-00-FF-E1%VLAN100	
	vlan-check key @VLAN		12-34-56-00-FF-E1@VLAN100	
id-format 1	無		12345600ffe1	12345600ffe1
	vlan-check		12345600ffe1%VLAN100	
	vlan-check key @VLAN		12345600ffe1@VLAN100	
id-format 1 capitals	無		12345600FFE1	12345600FFE1
	vlan-check		12345600FFE1%VLAN100	
	vlan-check key @VLAN		12345600FFE1@VLAN100	
id-format 2	無		1234.5600.ffe1	1234.5600.ffe1
	vlan-check		1234.5600.ffe1%VLAN100	
	vlan-check key @VLAN		1234.5600.ffe1@VLAN100	
id-format 2 capitals	無		1234.5600.FFE1	1234.5600.FFE1
	vlan-check		1234.5600.FFE1%VLAN100	
	vlan-check key @VLAN		1234.5600.FFE1@VLAN100	
id-format 3	無		12:34:56:00:ff:e1	12:34:56:00:ff:e1
	vlan-check		12:34:56:00:ff:e1%VLAN100	
	vlan-check key @VLAN		12:34:56:00:ff:e1@VLAN100	
id-format 3 capitals	無		12:34:56:00:FF:E1	12:34:56:00:FF:E1
	vlan-check		12:34:56:00:FF:E1%VLAN100	
	vlan-check key @VLAN		12:34:56:00:FF:E1@VLAN100	

コンフィグレーションの設定			RADIUS サーバへの認証要求形式	
id-format	vlan-check	password	ユーザ ID	パスワード
無	無	有 (任意文字列)	12-34-56-00-ff-e1	指定文字列
	vlan-check		12-34-56-00-ff-e1%VLAN100	
	vlan-check key @VLAN		12-34-56-00-ff-e1@VLAN100	
id-format 0	無		12-34-56-00-ff-e1	
	vlan-check		12-34-56-00-ff-e1%VLAN100	
	vlan-check key @VLAN		12-34-56-00-ff-e1@VLAN100	
id-format 0 capitals	無		12-34-56-00-FF-E1	
	vlan-check		12-34-56-00-FF-E1%VLAN100	
	vlan-check key @VLAN		12-34-56-00-FF-E1@VLAN100	
id-format 1	無		12345600ffe1	
	vlan-check		12345600ffe1%VLAN100	
	vlan-check key @VLAN		12345600ffe1@VLAN100	
id-format 1 capitals	無		12345600FFE1	
	vlan-check		12345600FFE1%VLAN100	
	vlan-check key @VLAN		12345600FFE1@VLAN100	
id-format 2	無		1234.5600.ffe1	
	vlan-check		1234.5600.ffe1%VLAN100	
	vlan-check key @VLAN		1234.5600.ffe1@VLAN100	
id-format 2 capitals	無		1234.5600.FFE1	
	vlan-check		1234.5600.FFE1%VLAN100	
	vlan-check key @VLAN		1234.5600.FFE1@VLAN100	
id-format 3	無		12:34:56:00:ff:e1	
	vlan-check		12:34:56:00:ff:e1%VLAN100	
	vlan-check key @VLAN		12:34:56:00:ff:e1@VLAN100	
id-format 3 capitals	無		12:34:56:00:FF:E1	
	vlan-check		12:34:56:00:FF:E1%VLAN100	
	vlan-check key @VLAN		12:34:56:00:FF:E1@VLAN100	

2. NAS-Identifier 使用による VLAN 制限
   固定 VLAN モードで，RADIUS サーバへ認証要求時の RADIUS 属性 "NAS-Identifier" に，取得した VLAN ID 情報 (認証要求時の端末が所属する VLAN ID) を設定して実施します。
   RADIUS サーバには，ユーザ ID・パスワードと共に，認証許可する VLAN 情報 (認証要求時の端末が所属する VLAN ID) を "NAS-Identifier" に設定することで，収容可能な VLAN を制限できます。

(d) ダイナミック VLAN モードで認証要求時の MAC アドレス形式とパスワード

本装置の MAC 認証では，RADIUS サーバへ認証要求時のユーザ ID およびパスワードは端末の MAC アドレスを使用しますが，MAC アドレス形式やパスワード文字列はコンフィグレーションで変更可能です。

また「capitals」指定により MAC アドレス内の "a" ～ "f" の文字を大文字形式にできます。

端末 MAC アドレスを「12-34-56-00-ff-e1」とした場合，コンフィグレーションの設定による RADIUS サーバへ認証要求時の例を下表に示します。

表 10-14　コンフィグレーションの設定と RADIUS サーバへの認証要求形式

コンフィグレーションの設定		RADIUS サーバへの認証要求形式	
id-format	password	ユーザ ID	パスワード
無	無	12-34-56-00-ff-e1	12-34-56-00-ff-e1
id-format 0		12-34-56-00-ff-e1	12-34-56-00-ff-e1
id-format 0 capitals		12-34-56-00-FF-E1	12-34-56-00-FF-E1
id-format 1		12345600ffe1	12345600ffe1
id-format 1 capitals		12345600FFE1	12345600FFE1
id-format 2		1234.5600.ffe1	1234.5600.ffe1
id-format 2 capitals		1234.5600.FFE1	1234.5600.FFE1
id-format 3		12:34:56:00:ff:e1	12:34:56:00:ff:e1
id-format 3 capitals		12:34:56:00:FF:E1	12:34:56:00:FF:E1
無	有 (任意文字列)	12-34-56-00-ff-e1	指定文字列
id-format 0		12-34-56-00-ff-e1	
id-format 0 capitals		12-34-56-00-FF-E1	
id-format 1		12345600ffe1	
id-format 1 capitals		12345600FFE1	
id-format 2		1234.5600.ffe1	
id-format 2 capitals		1234.5600.FFE1	
id-format 3		12:34:56:00:ff:e1	
id-format 3 capitals		12:34:56:00:FF:E1	

10.6　MAC 認証の注意事項

10.6.1　MAC 認証と他機能の共存について

MAC 認証と他機能の共存については，「5.9.3　レイヤ 2 認証機能と他機能の共存」を参照してください。

10.6.2　認証モード共通の注意事項

（1） 他装置宛て ARP フレームの MAC 認証契機について

システム受信モードのサポートに伴い，収容条件重視モード（装置デフォルト）使用時は，他装置宛て ARP フレームは MAC 認証契機の対象外となります。

（2） 認証契機のフレームについて

認証契機となった最初のフレームは，認証前フレームのため中継されません。

（3） 最大接続時間の設定について

コンフィグレーションコマンド mac-authentication max-timer で最大接続時間の短縮，延長を行った場合，現在認証済みの端末には適用されず，次回認証時から設定が有効となります。

（4） 内蔵 MAC 認証 DB について

（a） 内蔵 MAC 認証 DB の変更時

運用コマンドで内蔵 MAC 認証 DB への追加，変更を行った場合，現在認証済みの端末には適用されず，次回認証時から有効となります。

（b） 内蔵 MAC 認証 DB への同一 MAC アドレス複数設定について

内蔵 MAC 認証 DB には異なる VLAN ID（VLAN 設定無も含む）で同一の MAC アドレスを複数設定できます。この場合は，最初に一致した MAC アドレスで動作しますが，認証モードと設定内容により下記の動作となります。

表 10-15　固定 VLAN モードの場合

最初に一致した MAC アドレスの内蔵 MAC 認証 DB の VLAN ID 設定	コンフィグレーション mac-authentication vlan-check	動作
有	設定有	内蔵 MAC 認証 DB と，認証要求端末の MAC アドレスおよび所属する VLAN の，両方が一致した時点で認証許可（VLAN も照合）※
	設定無	最初に MAC アドレスが一致した時点で，認証対象端末が所属する VLAN で認証許可（VLAN は照合しない）
無	設定有	最初に MAC アドレスが一致した時点で，認証対象端末が所属する VLAN で認証許可（VLAN は照合しない）
	設定無	

注 ※
両方一致しなければ，認証失敗です。（この条件では，最初に一致した MAC アドレスとは限りません。）

表 10-16 ダイナミック VLAN モードの場合

最初に一致した MAC アドレスの内蔵 MAC 認証 DB の VLAN ID 設定	動作
有	最初に一致した MAC アドレスの VLAN に収容し，認証許可
無	認証後 VLAN としてネイティブ VLAN に収容 ※。（固定 VLAN モードの認証済み端末として管理）

注 ※
「5.4.4 同一 MAC ポートでの自動認証モード収容」を参照してください。

(c) MAC マスク付きエントリの検索について

MAC マスクなしのエントリで該当しなかった場合は，MAC マスク付きのエントリで一致するエントリを検索します。検索で一致したときの動作は，MAC マスクなしのエントリの場合と同様です。

MAC マスク付きエントリは，MAC アドレスの昇順（運用コマンド show mac-authentication mac-address の表示順）で検索します。MAC マスクの指定によっては ,MAC アドレスを包含しているエントリが前後する場合があります。運用コマンド show mac-authentication mac-address で，意図した順序で登録されているか確認してください。

(5) 強制認証ポートの使用について

1. 本機能はセキュリティ上の問題となる可能性がありますので，十分検討の上ご使用ください。
2. 本機能は RADIUS 認証方式だけサポートしています。
   強制認証をご使用になるときは，認証方式に RADIUS 認証だけを設定してください。以下のようにローカル認証・RADIUS 認証の両方を設定したときは，強制認証を設定しても動作しません。
   - aaa authentication mac-authentication default group radius local
   - aaa authentication mac-authentication default local group radius

(6) 認証済み端末のポート移動について

認証済み端末を MAC 認証設定ポートへポート移動したときは，「10.2 固定 VLAN モード 10.2.2 認証機能 (8) ローミング（認証済み端末のポート移動)」「10.3 ダイナミック VLAN モード 10.3.2 認証機能 (8) ローミング（認証済み端末のポート移動)」により，継続通信または認証解除となります。

なお，認証済み端末を同一 VLAN 内の MAC 認証未設定ポートへポート移動したときは，認証状態が解除されるまで通信できません。運用コマンド clear mac-authentication auth-state を使用して，端末の認証状態を解除してください。

コンフィグレーションコマンド authentication auto-logout strayer を設定しておくと，MAC 認証未設定ポートへ移動したときに，認証状態を解除できます。

(7) ローミング設定と DHCP snooping 併用時の制限

コンフィグレーションコマンド mac-authentication static-vlan roaming，mac-authentication roaming 設定状態で DHCP snooping 機能併用時，認証済み端末のポートを移動すると，認証状態は移動後のポートに遷移しますが，バインディングデータベースは更新されないため通信できません。

10.6.3 固定 VLAN モード使用時の注意事項

（1） 固定 VLAN モードのポートについて

固定 VLAN モードはアクセスポート / トランクポート，および MAC ポートで Tagged フレーム中継可（コンフィグレーションコマンド switchport mac dot1q vlan）が設定されているポートでの Tagged フレームによる MAC 認証が動作可能です。

11 MAC 認証の設定と運用

MAC 認証は，MAC アドレスを用いて認証されたユーザ単位に VLAN へのアクセス制御を行う機能です。この章では MAC 認証の設定と運用について説明します。

11.1　MAC 認証のコンフィグレーション

11.1.1　コンフィグレーションコマンド一覧

MAC 認証のコンフィグレーションコマンドと認証モード一覧を次の表に示します。

表 11-1　コンフィグレーションコマンドと認証モード一覧

コマンド名	説明	認証モード	
		固	ダ
aaa accounting mac-authentication	MAC 認証 のアカウンティング情報をアカウンティングサーバへ送信します。	○	○
aaa authentication mac-authentication	MAC 認証の認証方式グループを設定します。	○	○
aaa authentication mac-authentication end-by-reject	認証で否認された場合に，認証を終了します。通信不可（RADIUS サーバ無応答など）による認証失敗時は，コンフィグレーションコマンド aaa authentication mac-authentication で次に指定されている認証方式で認証します。	○	○
authentication arp-relay	コマンドおよび設定の詳細などについては，「5　レイヤ 2 認証機能の概説」を参照。	○	○
authentication ip access-group	コマンドおよび設定の詳細などについては，「5　レイヤ 2 認証機能の概説」を参照。	○	○
mac-authentication access-group	MAC 認証用ポートに MAC アクセスリストを適用し，認証対象端末・非対象端末を MAC アドレスで設定します。	○	○
mac-authentication authentication	ポート別認証方式の認証方式リスト名を設定します。	○	○
mac-authentication auto-logout	no mac-authentication auto-logout コマンドで，MAC 認証で認証された端末から一定時間フレームを受信しなかった状態を検出したときに認証を自動解除する設定を無効にします。	○	○
mac-authentication id-format	RADIUS 認証方式を使用時，RADIUS サーバへ認証要求する際の MAC アドレス形式を設定します。	○	○
mac-authentication logging enable	MAC 認証の動作ログに出力する情報を syslog サーバへ出力します。	○	○
mac-authentication max-timer	最大接続時間を設定します。	○	○
mac-authentication password	RADIUS 認証方式を使用時，RADIUS サーバへ認証要求する際のパスワードを設定します。	○	○
mac-authentication port※	ポートに認証モードを設定します。	○	○
mac-authentication radius-server host	MAC 認証専用 RADIUS サーバ情報を設定します。	○	○
mac-authentication radius-server dead-interval	MAC 認証専用 RADIUS サーバ使用時，プライマリ RADIUS サーバへ自動復旧するまでの監視タイマを設定します。	○	○
mac-authentication roaming	HUB などを経由して接続した認証済み端末を，リンクダウンしないでポート移動した場合の通信許可（ローミング）を設定します。	－	○
mac-authentication static-vlan roaming	HUB などを経由して接続した認証済み端末を，リンクダウンしないでポート移動した場合の通信許可（ローミング）を設定します。	○	－
mac-authentication system-auth-control	MAC 認証を有効にします。	○	○

コマンド名	説明	認証モード	
		固	ダ
mac-authentication timeout quiet-period	認証失敗時に，同一端末（MAC アドレス）の認証を再開しない時間（認証再開猶予タイマ）を設定します。	○	○
mac-authentication timeout reauth-period	認証成功後，端末の再認証を行う周期を設定します。	○	○
mac-authentication vlan-check	認証処理で MAC アドレスを照合する際に，VLAN ID も照合します。	○	－

（凡例）

固：固定 VLAN モード

ダ：ダイナミック VLAN モード

○：設定内容に従って動作します

－：コマンドは入力できますが，動作しません

×：コマンドを入力できません

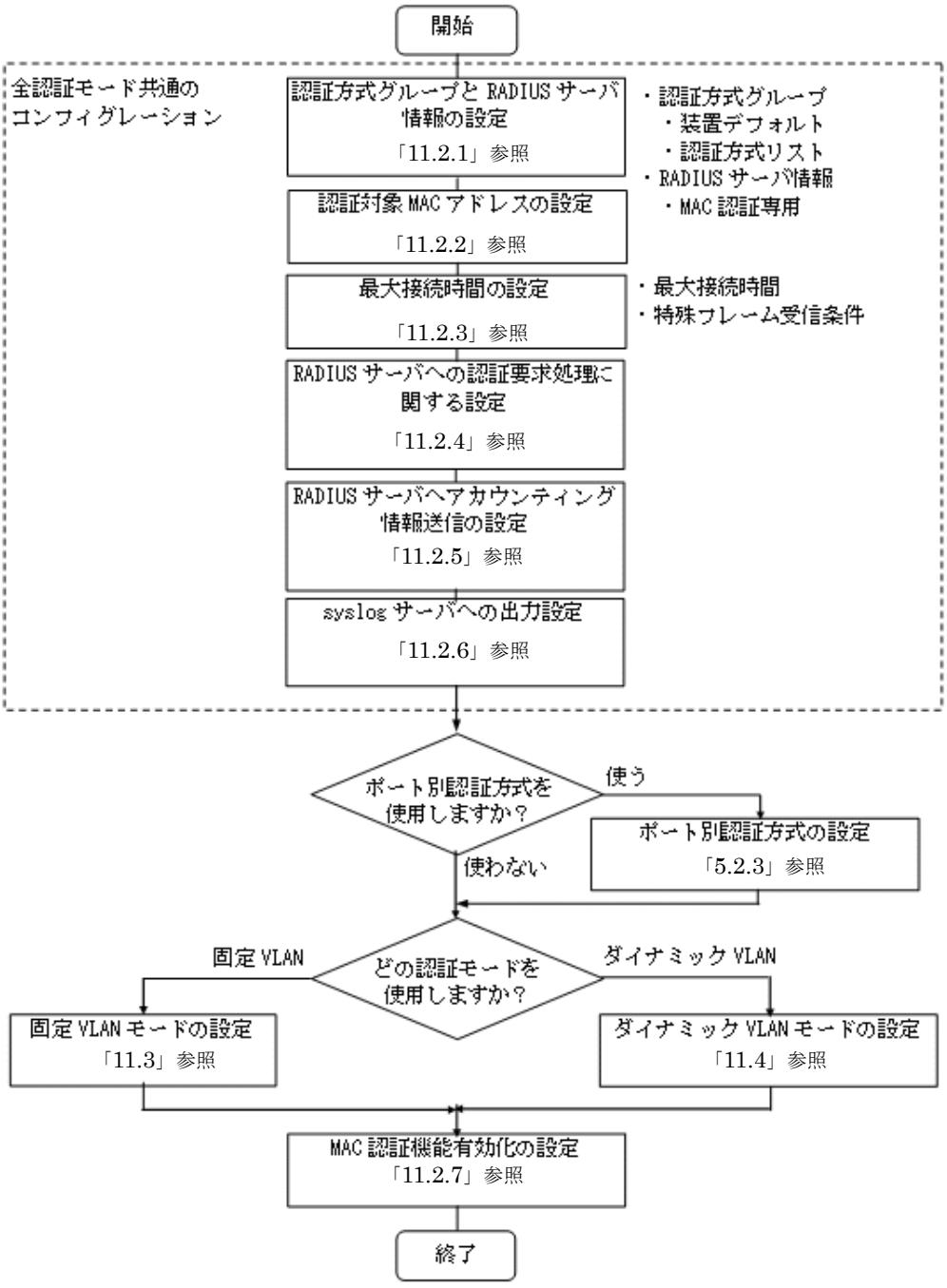
注 ※

本コマンドの設定は，認証モードの切り替えに影響します。

11.1.2　MAC 認証の設定手順

MAC 認証は，下記の手順で設定してください。

図 11-1　MAC 認証の設定手順



各設定の詳細は，下記を参照してください。

1. 全認証モード共通のコンフィグレーション
   全認証モード共通のコンフィグレーションを設定します。
   - 認証方式グループと RADIUS サーバ情報の設定：「11.2.1　認証方式グループと RADIUS サーバ情

報の設定」
- 認証対象 MAC アドレスの設定：「11.2.2　認証対象 MAC アドレスの制限」
- 最大接続時間の設定：「11.2.3　最大接続時間の設定」
- RADIUS サーバへの認証要求処理に関する設定：「11.2.4　RADIUS サーバへの認証要求処理に関する設定」
- RADIUS サーバへアカウンティング情報送信の設定：「11.2.5　アカウンティング情報送信の設定」
- syslog サーバへの出力設定：「11.2.6　syslog サーバ出力設定」
- ポート別認証方式の設定：「5.2.3　認証方式リストのコンフィグレーション（2）ポート別認証方式の設定例」

2. 各認証モードの設定
   各認証モードのコンフィグレーションを設定します。
   設定項目によっては，他の認証モードと共通になる場合があります。これについては「～を参照してください。」と記載していますので，該当箇所を参照してください。
   - 固定 VLAN モードの設定：「11.3　固定 VLAN モードのコンフィグレーション」
   - ダイナミック VLAN モードの設定：「11.4　ダイナミック VLAN モードのコンフィグレーション」

3. MAC 認証機能の有効化
   最後に MAC 認証機能を有効設定して，MAC 認証の設定は終了です。
   - 「11.2.7　MAC 認証機能の有効化」

各認証モードは下記のコンフィグレーション設定で有効となります。

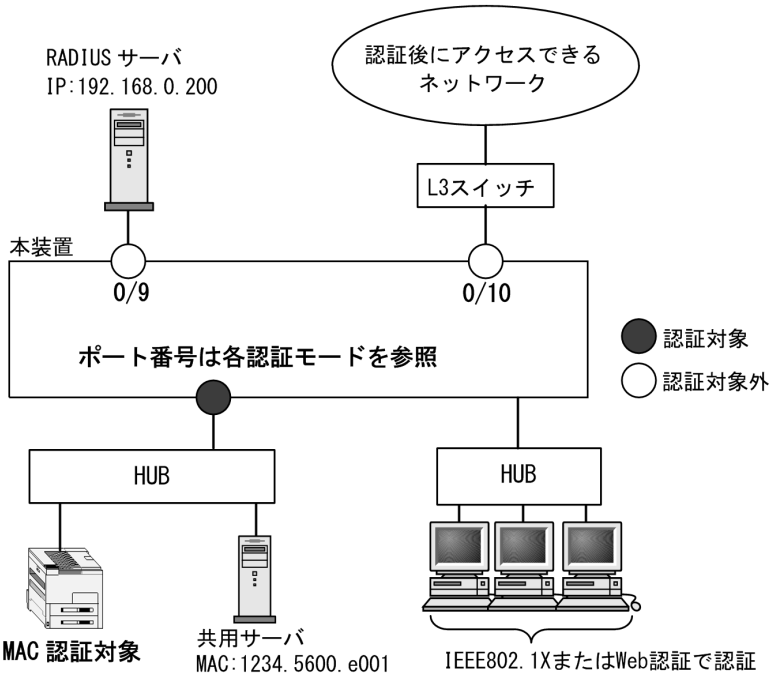
表 11-2　各認証モード有効条件

認証モード	コンフィグレーション設定
共通	• aaa authentication mac-authentication • mac-authentication radius-server host または radius-server • mac-authentication system-auth-control
固定 VLAN モード	アクセスポートで使用する場合 • vlan <VLAN ID list> • mac-authentication port • switchport mode access • switchport access vlan トランクポートで使用する場合 • vlan <VLAN ID list> • mac-authentication port • switchport mode trunk • switchport trunk allowed vlan • switchport trunk native vlan MAC ポートで使用する場合 • vlan <VLAN ID list> または vlan <VLAN ID list> mac-based • mac-authentication port • switchport mode mac-vlan • switchport mac dot1q vlan
ダイナミック VLAN モード	• vlan <VLAN ID list> mac-based • mac-authentication port • switchport mode mac-vlan

11.2　全認証モード共通のコンフィグレーション

本章では，下記の基本構成を基に各認証モードの設定を説明します。RADIUS サーバと認証後ネットワーク用のポート番号は 0/9，0/10 を例として使用します。認証対象端末を接続するポート番号は，各認証モードの設定例を参照してください。

図 11-2　基本構成



11.2.1　認証方式グループと RADIUS サーバ情報の設定

(1) 認証方式グループの設定

[設定のポイント]

MAC 認証の認証方式グループを設定します。

MAC 認証共通で使用する装置デフォルトを１エントリ，認証ポートで使用する認証方式リストを２エントリ設定します。

1. 装置デフォルト

   本例では，装置デフォルトの認証方式を RADIUS 認証とローカル認証とし，通信不可（RADIUS サーバ無応答など）により RADIUS 認証に失敗したときは，ローカル認証を実行するよう設定します。

   なお，RADIUS 認証否認によって認証に失敗した場合には，その時点で認証を終了し，ローカル認証を行いません。

   - RADIUS 認証方式では，認証要求時の MAC アドレス形式の設定やパスワードなども設定できます。設定については，「11.2.4　RADIUS サーバへの認証要求処理に関する設定」を参照してください。
   - ローカル認証方式は内蔵 MAC 認証 DB を使用します。「11.5.2　内蔵 MAC 認証 DB の登録」を参照して，本装置に内蔵 MAC 認証 DB を登録してください。

2. 認証方式リスト

認証方式リストに指定する RADIUS サーバグループ情報は，"Keneki-group1" と "Keneki-group2" を設定済みとします。
認証方式リストについては「5.2.2　認証方式リスト」を参照してください。
RADIUS サーバグループ情報については，「5.3.1　レイヤ 2 認証機能で使用する RADIUS サーバ情報」「コンフィグレーションガイド Vol. 10 ログインセキュリティと RADIUS」を参照してください。

［コマンドによる設定］

1. **(config)# aaa authentication mac-authentication default group radius local**
装置デフォルトの認証方式は，RADIUS 認証方式，ローカル認証方式の順番に設定します。
2. **(config)# aaa authentication mac-authentication end-by-reject**
RADIUS 認証で否認された場合には，その時点で認証を終了し，ローカル認証を行わないように設定します。
3. **(config)# aaa authentication mac-authentication MAC-list1 group Keneki-group1**
認証方式リスト "MAC-list1" に，RADIUS サーバグループ名 "Keneki-group1" を設定します。
4. **(config)# aaa authentication mac-authentication MAC-list2 group Keneki-group2**
認証方式リスト "MAC-list2" に，RADIUS サーバグループ名 "Keneki-group2" を設定します。

［注意事項］

- 装置デフォルトを設定変更したときは，装置デフォルトの認証方式で認証した端末を認証解除します。
- 認証方式リストを設定変更したときは，当該認証方式リストで認証した端末を認証解除します。
- aaa authentication mac-authentication 設定省略時はローカル認証方式となります。
- 強制認証機能を使用するときは，上記コマンドで「default group radius」だけ設定してください。ローカル認証だけ，または RADIUS 認証とローカル認証の優先順を設定（上記のような設定）したときは使用できません。
- aaa authentication mac-authentication end-by-reject を設定変更したときは，MAC 認証の認証済み端末を認証解除します。

（2） RADIUS サーバ情報の設定

（a） MAC 認証専用 RADIUS サーバを使用する場合

［設定のポイント］

MAC 認証だけで使用する認証専用 RADIUS サーバ情報を設定します。
RADIUS サーバ設定を有効にするためには，IP アドレスと RADIUS 鍵の設定が必要です。コンフィグレーションコマンド mac-authentication radius-server host では IP アドレスだけの設定も可能ですが，RADIUS 鍵を設定するまでは認証に使用されません。
また，本例では使用不可状態になった MAC 認証専用 RADIUS サーバを，自動復旧する監視タイマ（dead-interval 時間）も設定します。

［コマンドによる設定］

1. **(config)# mac-authentication radius-server host 192.168.10.202 key "mac-auth"**
MAC 認証だけで使用する RADIUS サーバの IP アドレスおよび RADIUS 鍵を設定します。この場合，auth-port，acct-port，timeout，retransmit は省略時の初期値が適用されます。
2. **(config)# mac-authentication radius-server dead-interval 15**
設定した MAC 認証専用 RADIUS サーバが使用不可状態になったときに，自動復旧までの監視タイマ（dead-interval 時間）を 15 分に設定します。

［注意事項］

- 本情報未設定時は，汎用 RADIUS サーバ情報の設定に従います。MAC 認証専用 RADIUS サーバ情報と汎用 RADIUS サーバ情報の両方未設定のときは，RADIUS 認証を実施できません。
- MAC 認証専用 RADIUS サーバ情報は，最大 4 エントリまで設定できます。
- RADIUS 鍵，再送回数，応答タイムアウト時間を省略したときは，それぞれコンフィグレーションコマンド radius-server key，radius-server retransmit，radius-server timeout の設定に従います。

（b） 汎用 RADIUS サーバを使用する場合

汎用 RADIUS サーバの設定については，「コンフィグレーションガイド Vol.1 10 ログインセキュリティと RADIUS」を参照してください。

11.2.2 認証対象 MAC アドレスの制限

［設定のポイント］

MAC 認証で認証要求する端末（MAC アドレス）範囲と，MAC 認証で認証要求しない端末範囲を設定します。

［コマンドによる設定］

1. **(config)# mac-authentication access-group MacAuthFilter**
   (config)# mac access-list extended MacAuthFilter
   (config-ext-macl)# permit 1234.5600.e000 0000.0000.ffff any
   (config-ext-macl)# exit
   MAC アドレスが "1234.5600.e000" ～ "1234.5600.efff" の範囲の端末を，MAC 認証で認証要求する範囲に設定します。

［注意事項］

- 本機能で使用するアクセスリストは，フロー検出モードの設定に依存しません。
- MAC アクセスリストは拡張（extended）だけサポートしているため，有効な MAC アドレス範囲は送信元 MAC アドレス（src 指定）部分に記述してください。
- MAC アクセスリストのコンフィグレーションコマンドは，宛先 MAC アドレス（dst 以降）の指定も必要ですが，MAC 認証の認証対象フィルタとしては無視されますので，入力時は任意の値を指定してください。
- permit 条件に一致した MAC アドレスは，MAC 認証処理の対象となります。
  deny 条件に一致した MAC アドレスは，MAC 認証処理の対象外となり RADIUS サーバへの認証要求は発生しません。
  MAC アクセスリスト最終行には，全 MAC アドレスを対象とした暗黙の deny 条件が存在します。本設定例では permit 条件を 1 行だけ設定していますが，この permit 条件に一致しなかった場合は，暗黙の deny 条件に一致したものとみなすため，MAC 認証処理の対象外となり RADIUS サーバへの認証要求は発生しません。

11.2.3 最大接続時間の設定

［設定のポイント］

認証済み端末の最大接続時間を設定します。最大接続時間を超過すると，自動的に認証を解除します。

［コマンドによる設定］

1. **(config)# mac-authentication max-timer 60**
   認証済み端末を自動的に認証解除する時間を 60 分に設定します。

11.2.4 RADIUS サーバへの認証要求処理に関する設定

（1） RADIUS サーバへ認証要求時の MAC アドレス形式の設定

［設定のポイント］

認証を許可する端末の MAC アドレスを RADIUS サーバへ認証要求する際に使用する，端末の MAC アドレス形式を設定します。設定の組み合わせについては「10.5.2 RADIUS 認証の場合（2） RADIUS サーバの準備」を参照してください。

［コマンドによる設定］

1. **(config)# mac-authentication id-format 3 capitals**

RADIUS サーバへ認証要求する MAC アドレス形式を「xx:xx:xx:xx:xx:xx」形式で，A ～ F を大文字に設定します。（capitals を指定しない場合は，小文字です。）

［注意事項］

本コマンド未設定の場合は「xx-xx-xx-xx-xx-xx」形式で，A ～ F は小文字となります。

（2） RADIUS サーバへ認証要求時のパスワードの設定

［設定のポイント］

認証を許可する端末を RADIUS サーバへ認証要求する際に使用する，パスワードを設定します。設定の組み合わせについては「10.5.2 RADIUS 認証の場合（2）RADIUS サーバの準備」を参照してください。

［コマンドによる設定］

1. **(config)# mac-authentication password system1-pc0001**

RADIUS サーバへ認証要求するパスワードを任意の文字列で設定します。 1 ～ 32 文字以内で設定できます。

［注意事項］

- 本コマンド未設定の場合は，認証を許可する端末の MAC アドレスがパスワードとなります。MAC アドレスの形式は，コンフィグレーションコマンド mac-authentication id-format の設定に依存します。
- 本コマンドで設定したパスワードは，すべての MAC 認証端末で共通となります。

（3） RADIUS 認証再開猶予タイマの設定

［設定のポイント］

RADIUS サーバへの認証要求で認証拒否され，一時的に認証処理保留扱いとなった端末（MAC アドレス）を，認証処理保留状態から解除するまでの時間を設定します。

［コマンドによる設定］

1. **(config)# mac-authentication timeout quiet-period 60**

認証処理保留状態から解除するまでの時間を 60 秒に設定します。
なお，認証処理保留状態は，MAC 認証にだけ適用されるので，保留状態中も IEEE802.1X や，Web 認証の処理には影響しません。

［注意事項］

- 本機能は MAC 認証機能を有効にすると 300 秒（デフォルトコンフィグレーション）で動作します。タイマ値に 0 を設定した場合，認証保留状態の時間がなくなり，認証拒否された端末から送信され

るパケットを契機に即 RADIUS サーバへ認証要求が実施されますので注意してください。

- 本設定は MAC 認証で認証拒否された時点のコンフィグレーションが適用されます。このため，既に MAC 認証で認証拒否され保留状態となった端末が存在する状態で再開猶予タイマを変更した場合，変更値が保留状態と端末に適用されるのは，以前の保留状態が解除されたあと，再度認証を拒否された時点からとなります。

（4） RADIUS サーバへの定期的再認証要求時間の設定

［設定のポイント］

認証済み端末の認証情報有無を RADIUS サーバに要求する周期を設定します。

［コマンドによる設定］

1. **(config)# mac-authentication timeout reauth-period 600**
   RADIUS サーバへの定期的再認証要求周期を 600 秒に設定します。
   本機能は MAC 認証で認証された端末だけに対して，端末が認証された時点から設定時間経過後に定期的に RADIUS サーバへ再認証要求を行います。

［注意事項］

1. 定期的再認証要求周期で 0 を設定した場合，RADIUS サーバへの定期的再認証要求を停止します。この場合，RADIUS サーバの認証情報が変更されても反映されないため，認証許可された端末は認証後 VLAN に移動したままの状態となります。
2. 認証状態を解除する場合は，下記を参照して解除してください。
   - 固定 VLAN モード：「10.2.2　認証機能（7）認証解除」
   - ダイナミック VLAN モード：「10.3.2　認証機能（7）認証解除」
3. 本設定は MAC 認証で認証された時点のコンフィグレーションが端末単位に適用されます。このため，既に MAC 認証で認証済みの端末がある状態で，RADIUS サーバへの再認証要求時間を変更した場合，変更値が認証済みの端末に適用されるのは次に再認証要求を行い，認証許可された時点からとなります。

11.2.5　アカウンティング情報送信の設定

［設定のポイント］

MAC 認証のアカウンティング情報を RADIUS サーバへ送信するよう設定します。

［コマンドによる設定］

1. **(config)# aaa accounting mac-authentication default start-stop group radius**
   RADIUS サーバへアカウンティング情報を送信するよう設定します。

11.2.6　syslog サーバ出力設定

動作ログの syslog サーバへの出力を設定します。

［設定のポイント］

MAC 認証の認証情報および動作情報を記録した動作ログを，syslog サーバへ出力する設定をします。

［コマンドによる設定］

1. **(config)# mac-authentication logging enable**
   syslog サーバへの出力を有効にします。

［注意事項］

syslog サーバへの送信対象イベント種別として，コンフィグレーションコマンド logging event-kind aut も合わせて設定してください。

11.2.7 MAC 認証機能の有効化

［設定のポイント］

MAC 認証用のコンフィグレーションを設定後，MAC 認証を有効にします。

［コマンドによる設定］

1. **(config)# mac-authentication system-auth-control**

MAC 認証を有効にします。

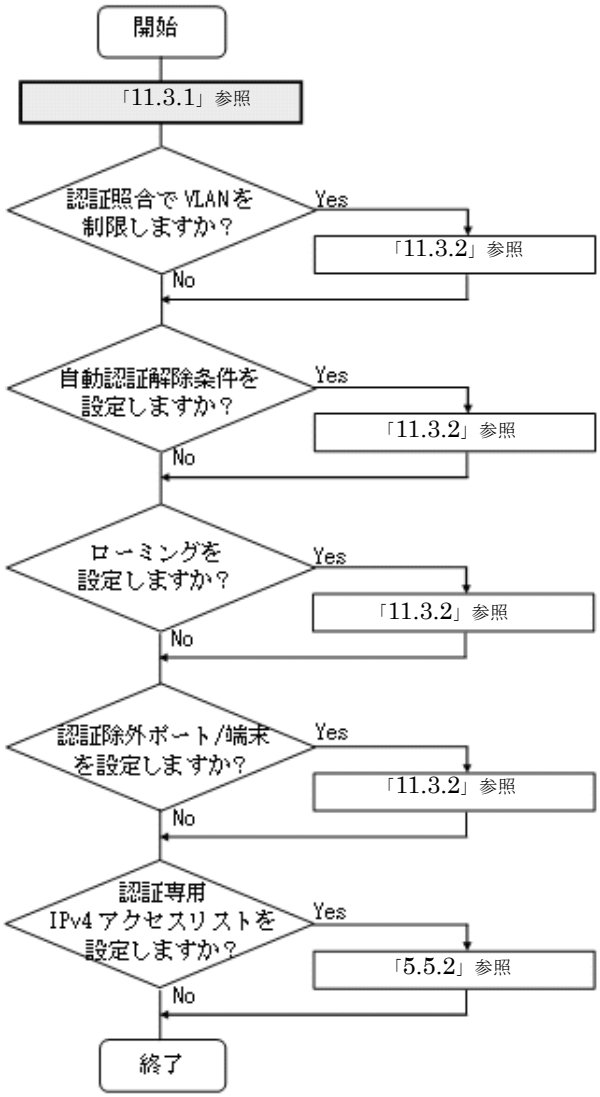
［注意事項］

MAC 認証の設定をすべて終了してから，本コマンドを設定してください。途中の状態で認証を有効化すると，認証失敗のアカウントログが採取される場合があります。

11.3 固定 VLAN モードのコンフィグレーション

「11.1 MAC 認証のコンフィグレーション」および「11.2 全認証モード共通のコンフィグレーション」に記載の設定をしたうえで，次の図の手順に従って固定 VLAN モードのコンフィグレーションを設定してください。

図 11-3 固定 VLAN モードの設定手順

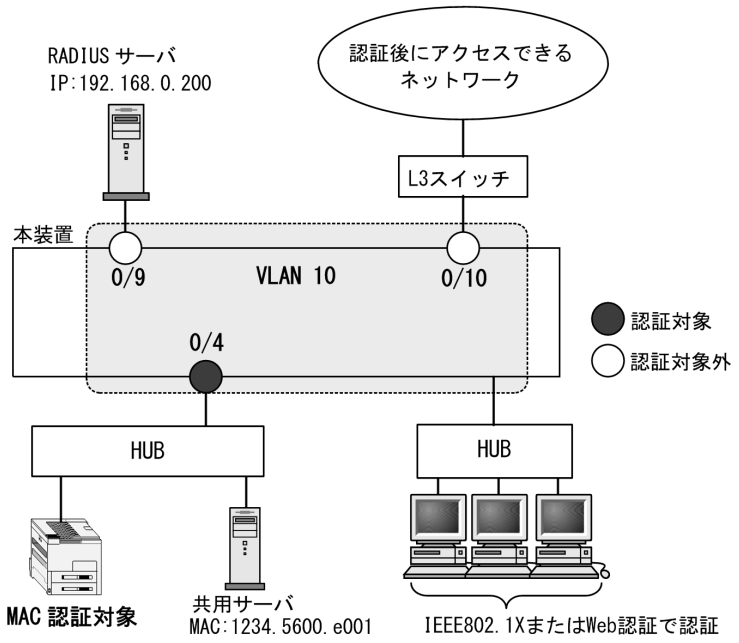


各設定の詳細は，下記を参照してください。

1. 固定 VLAN モードの設定：「11.3.1 固定 VLAN モードの設定」
2. 認証照合での VLAN 制限の設定：「11.3.2 認証処理に関する設定（1）認証情報照合時の VLAN 制限の設定」
3. 自動認証解除の設定：「11.3.2 認証処理に関する設定（2）自動認証解除条件の設定」
4. ローミングの設定：「11.3.2 認証処理に関する設定（3）ローミング（認証済み端末のポート移動通信許可）の設定」
5. 認証除外ポート / 端末の設定：「11.3.2 認証処理に関する設定（4）認証除外の設定」
6. 認証専用 IPv4 アクセスリストの設定：「5.5.2 認証専用 IPv4 アクセスリストの設定」

11.3.1 固定 VLAN モードの設定

図 11-4 固定 VLAN モードの構成例



(1) 認証ポートと認証用 VLAN 情報の設定

[設定のポイント]

固定 VLAN モードで使用するポートに，固定 VLAN モードと認証用 VLAN 情報を設定します。

[コマンドによる設定]

1. **(config)# vlan 10**
   (config-vlan)# exit
   VLAN ID 10 を設定します。

2. **(config)# interface gigabitethernet 0/4**
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 10
   認証を行う端末が接続されているポート 0/4 をアクセスポートして設定し，認証用 VLAN10 を設定します。

3. **(config-if)# mac-authentication port**
   (config-if)# exit
   ポート 0/4 に固定 VLAN モードを設定します。

(2) ポート別認証方式の認証方式リスト名の設定

[設定のポイント]

ポート別認証方式の認証方式リスト名を設定します。
認証方式リストの設定は前述の「11.2.1 認証方式グループと RADIUS サーバ情報の設定（1）認証方式グループの設定」を参照してください。

［コマンドによる設定］

1. **(config)# interface gigabitethernet 0/4**
   (config-if)# mac-authentication authentication MAC-list1
   (config-if)# exit
   ポート 0/4 に認証方式リスト名 "MAC-list1" を設定します。

［注意事項］

- 本情報未設定時は，「11.2.1　認証方式グループと RADIUS サーバ情報の設定（1）認証方式グループの設定」の装置デフォルトに従って認証します。
- ポートに設定した認証方式リスト名と，認証方式グループの認証方式リスト名が不一致，または認証方式グループに存在しないときは，装置デフォルトに従って認証します。
- Web 認証のユーザ ID 別認証方式は併用設定できません。詳細は「5.2.2　認証方式リスト」を参照してください。

11.3.2　認証処理に関する設定

固定 VLAN モードの認証処理に関する設定を説明します。

（1） 認証情報照合時の VLAN 制限の設定

［設定のポイント］

固定 VLAN モードでローカル認証または RADIUS 認証による認証対象端末の照合時，VLAN ID も照合対象に設定します。

［コマンドによる設定］

1. **(config)# mac-authentication vlan-check key @VLAN**
   ローカル認証の場合は "MAC アドレスと当該ポートの VLAN ID"，RADIUS 認証の場合は "MAC アドレスと区切り文字列@と当該ポートの VLAN ID" で，認証対象端末の照合を実施します。
   RADIUS 認証の場合は，「11.2.4　RADIUS サーバへの認証要求処理に関する設定（1）RADIUS サーバへ認証要求時の MAC アドレス形式の設定」「11.2.4　RADIUS サーバへの認証要求処理に関する設定（2）RADIUS サーバへ認証要求時のパスワードの設定」も参照のうえ，必要に応じて設定してください。

（2） 自動認証解除条件の設定

(a) 最大接続時間の設定

本設定は，MAC 認証の全認証モードで共通です。「11.2　全認証モード共通のコンフィグレーション 11.2.3　最大接続時間の設定」を参照してください。

(b) 認証済み端末の無通信監視時間の設定

［設定のポイント］

認証済み端末の無通信監視時間を設定します。設定時間を経過しても該当端末からフレームを受信していない状態を検出した場合は，自動的に認証を解除します。
なお，無通信監視時間は MAC 認証機能を有効にすると 3600 秒（デフォルトコンフィグレーション）で動作します。no mac-authentication auto-logout を設定した場合は，認証を解除しません。

［コマンドによる設定］

1. **(config)# mac-authentication auto-logout delay-time 600**
   認証済み端末の無通信監視時間を 600 秒（＝ 10 分）に設定します。

［注意事項］

- 自動認証解除の適用時間と，RADIUS サーバ定期的再認証要求（mac-authentication timeout reauth-period）機能の適用時間が重複した場合は，自動認証解除が優先されます。
- 本設定は即時に適用されますが，無通信監視は 60 秒周期のため，実際に適用されるまで最大 60 秒の誤差が生じます。なお，mac-authentication auto-logout delay-time の値を現時点の設定値から短い値に変更した場合，既に変更後の無通信監視時間を経過していた端末を検出した時点で自動的に認証解除を実施しますが，本検出でも同様に最大 60 秒の誤差が生じます。

（3） ローミング（認証済み端末のポート移動通信許可）の設定

［設定のポイント］

固定 VLAN モードで認証済みの端末を，ポートリンクダウンしないで他のポートへ移動しても通信可能に設定します。

［コマンドによる設定］

1. **(config)# mac-authentication static-vlan roaming**

固定 VLAN モードでの認証済み端末のポート移動後の通信許可に設定します。

［注意事項］

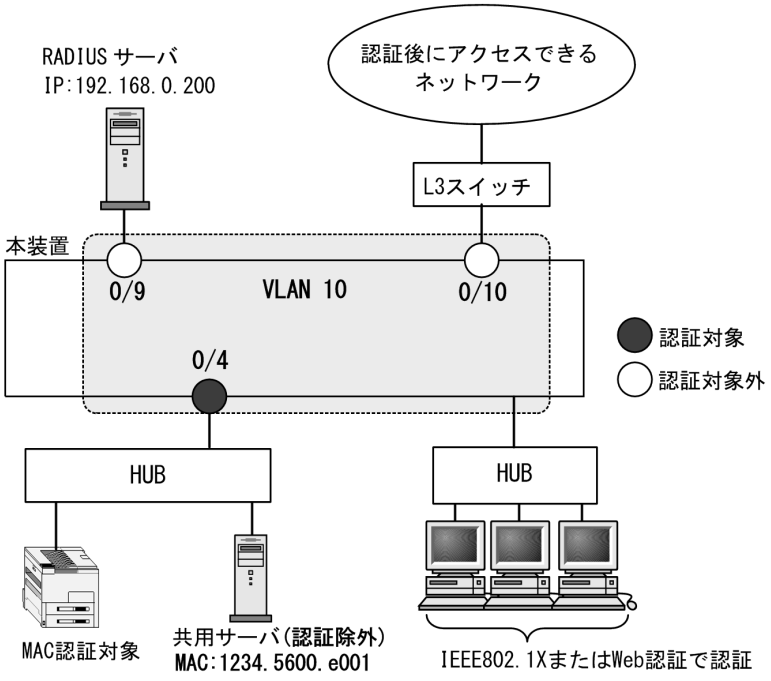
ローミングの動作可能な条件は下記のとおりです。

- 移動前および移動後が，固定 VLAN モード対象ポート
- 移動前および移動後が，同一 VLAN

（4） 認証除外の設定

固定 VLAN モードで認証対象外とするポートや端末を設定します。本例では，次の図に示すポート 0/9，0/10，および共用サーバを認証除外として設定します。

図 11-5　固定 VLAN モードの認証除外の構成例



(a) 認証除外ポートの設定

[設定のポイント]

固定 VLAN モードで認証を除外するポートに対しては，認証モードを設定しません。

[コマンドによる設定]

1. **(config)# interface range gigabitethernet 0/9-10**
   (config-if-range)# switchport mode access
   (config-if-range)# switchport access vlan 10
   (config-if-range)# exit
   VLAN ID 10 のポート 0/9 と 0/10 を，アクセスポートとして設定します。認証モード（mac-authentication port）は設定しません。

(b) 認証除外端末の設定

[設定のポイント]

固定 VLAN モードで認証を除外する端末の MAC アドレスを，MAC アドレステーブルに登録します。

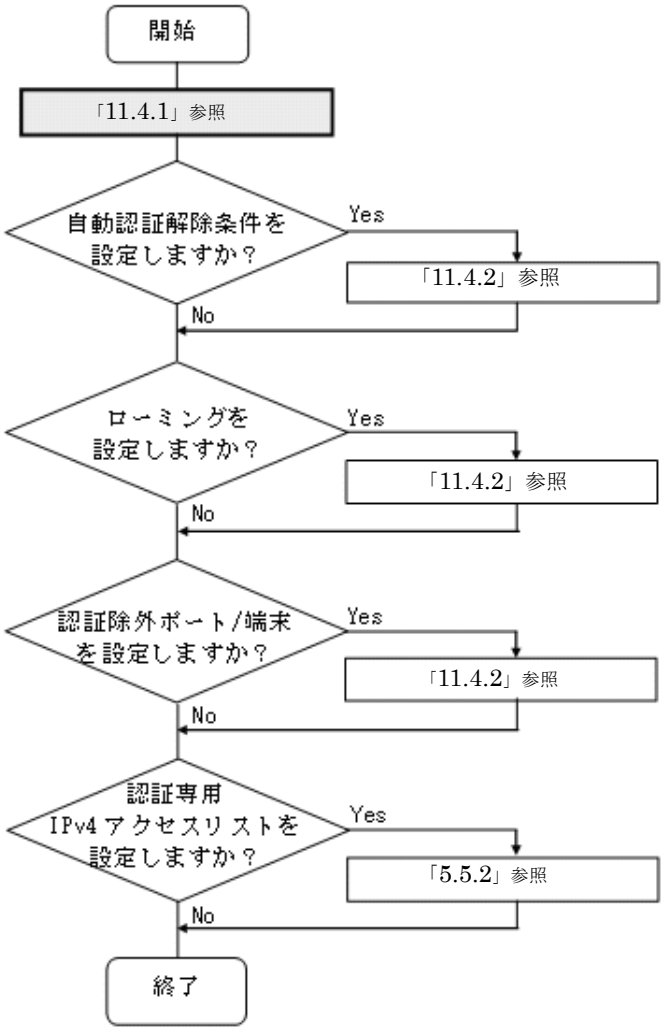
[コマンドによる設定]

1. **(config)# mac-address-table static 1234.5600.e001 vlan 10 interface gigabitethernet 0/4**
   VLAN ID 10 のポート 0/4 で認証を除外して通信を許可する端末の MAC アドレス（図内の共用サーバの MAC アドレス：1234.5600.e001）を，MAC アドレステーブルに設定します。

11.4　ダイナミック VLAN モードのコンフィグレーション

「11.1　MAC 認証のコンフィグレーション」および「11.2　全認証モード共通のコンフィグレーション」に記載の設定をしたうえで，次の図の手順に従ってダイナミック VLAN モードのコンフィグレーションを設定してください。

図 11-6　ダイナミック VLAN モードの設定手順

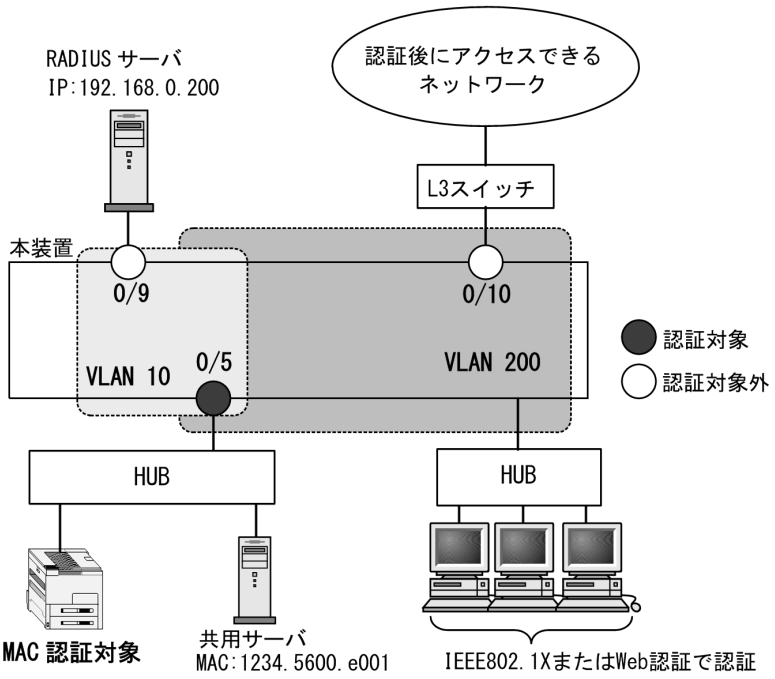


各設定の詳細は，下記を参照してください。

1. ダイナミック VLAN モードの設定：「11.4.1　ダイナミック VLAN モードの設定」
2. 自動認証解除の設定：「11.4.2　認証処理に関する設定（1）自動認証解除条件の設定」
3. ローミングの設定：「11.4.2　認証処理に関する設定（2）ローミング（認証済み端末のポート移動通信許可）の設定」
4. 認証除外ポート / 端末の設定：「11.4.2　認証処理に関する設定（3）認証除外の設定」
5. 認証専用 IPv4 アクセスリストの設定：「5.5.2　認証専用 IPv4 アクセスリストの設定」

11.4.1 ダイナミック VLAN モードの設定

図 11-7 ダイナミック VLAN モードの構成例



(1) 認証ポートと認証用 VLAN 情報の設定

[設定のポイント]

ダイナミック VLAN モードで使用するポートに，ダイナミック VLAN モードと認証用 VLAN 情報を設定します。

なお，認証ポートの認証後 VLAN は，「5.4.3 MAC VLAN の自動 VLAN 割当」により割り当てられるものとします。

[コマンドによる設定]

1. **(config)# vlan 200 mac-based**
   (config-vlan)# exit
   VLAN ID 200 に MAC VLAN を設定します。

2. **(config)# vlan 10**
   (config-vlan)# exit
   VLAN ID 10 を設定します。

3. **(config)# interface gigabitethernet 0/5**
   (config-if)# switchport mode mac-vlan
   (config-if)# switchport mac native vlan 10
   認証を行う端末が接続されているポート 0/5 を MAC ポートとして設定し，認証前 VLAN10 を設定します。(認証後 VLAN は「5.4.3 MAC VLAN の自動 VLAN 割当」により割り当てられます。)

4. **(config-if)# mac-authentication port**

```
(config-if)# exit
```
ポート 0/5 にダイナミック VLAN モードを設定します。

(2) ポート別認証方式の認証方式リスト名の設定

[設定のポイント]

ポート別認証方式の認証方式リスト名を設定します。
認証方式リストの設定は前述の「11.2.1 認証方式グループと RADIUS サーバ情報の設定（1）認証方式グループの設定」を参照してください。

[コマンドによる設定]

1.
```
(config)# interface gigabitethernet 0/5
(config-if)# mac-authentication authentication MAC-list1
(config-if)# exit
```
ポート 0/5 に認証方式リスト名 "MAC-list1" を設定します。

[注意事項]

- 本情報未設定時は，「11.2.1 認証方式グループと RADIUS サーバ情報の設定（1）認証方式グループの設定」の装置デフォルトに従って認証します。
- ポートに設定した認証方式リスト名と，認証方式グループの認証方式リスト名が不一致，または認証方式グループに存在しないときは，装置デフォルトに従って認証します。
- Web 認証のユーザ ID 別認証方式は併用設定できません。詳細は「5.2.2 認証方式リスト」を参照してください。

11.4.2 認証処理に関する設定

ダイナミック VLAN モードの認証処理に関する設定を説明します。

(1) 自動認証解除条件の設定

(a) 最大接続時間の設定

本設定は，MAC 認証の全認証モードで共通です。「11.2 全認証モード共通のコンフィグレーション 11.2.3 最大接続時間の設定」を参照してください。

(b) 認証済み端末の無通信監視時間の設定

固定 VLAN モードと同様です。「11.3.2 認証処理に関する設定（2）自動認証解除条件の設定（b）認証済み端末の無通信監視時間の設定」を参照してください。

(2) ローミング（認証済み端末のポート移動通信許可）の設定

[設定のポイント]

ダイナミック VLAN モードで認証済みの端末を，ポートリンクダウンしないで他のポートへ移動しても通信可能に設定します。

[コマンドによる設定]

1.
```
(config)# mac-authentication roaming
```
ダイナミック VLAN モードで認証済み端末のポート移動後の通信許可を設定します。

[注意事項]

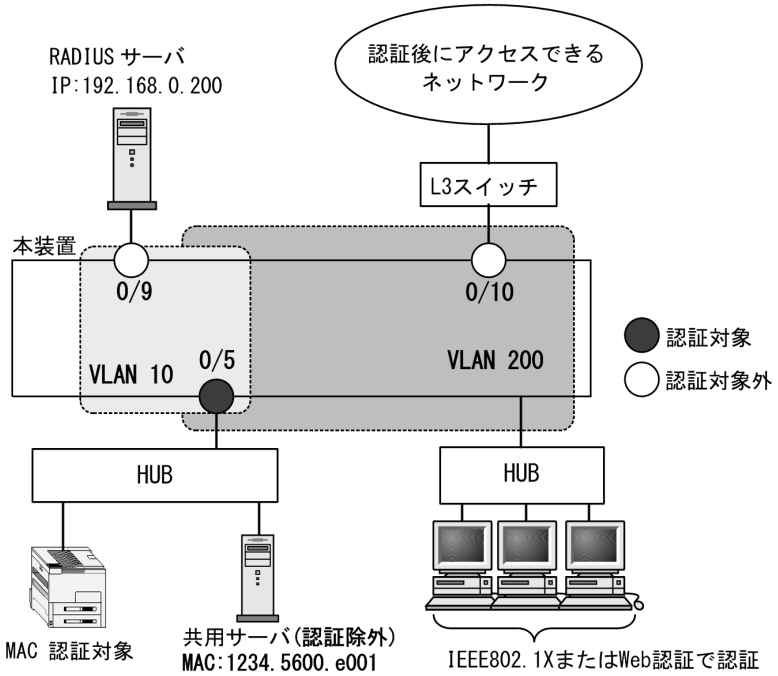
ローミングの動作可能な条件は下記のとおりです。

- 移動前および移動後が，ダイナミック VLAN モード対象ポート

(3) 認証除外の設定

ダイナミック VLAN モードで認証対象外とするポートや端末を設定します。本例では，次の図に示すポート 0/9，0/10，および共用サーバを認証除外として設定します。

図 11-8 ダイナミック VLAN モードの認証除外の構成例



(a) 認証除外ポートの設定

[設定のポイント]

認証を除外するポートをアクセスポートとして設定し，認証モードを設定しません。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 0/9**
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 10
   (config-if)# exit
   VLAN ID 10 のポート 0/9 をアクセスポートとして設定します。認証モード（mac-authentication port）は設定しません。
2. **(config)# interface gigabitethernet 0/10**
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 200
   (config-if)# exit
   MAC VLAN ID 200 のポート 0/10 をアクセスポートとして設定します。認証モード（mac-authentication port）は設定しません。

(b) 認証除外端末の設定

[設定のポイント]

認証を除外する端末の MAC アドレスを，MAC VLAN と MAC アドレステーブルに登録します。

[コマンドによる設定]

1. **(config)# vlan 200 mac-based**
   (config-vlan)# mac-address 1234.5600.e001
   (config-vlan)# exit
   認証を除外する MAC アドレス（図内の共用サーバの MAC アドレス：1234.5600.e001）を，MAC VLAN ID 200 に設定します。
2. **(config)# interface gigabitethernet 0/5**
   (config-if)# switchport mode mac-vlan
   (config-if)# switchport mac vlan 200
   (config-if)# exit
   認証ポートに除外端末が属する MAC VLAN ID 200 を設定します。
3. **(config)# mac-address-table static 1234.5600.e001 vlan 200 interface gigabitethernet 0/5**
   MAC VLAN ID 200 のポート 0/5 で認証を除外して通信を許可する端末の MAC アドレス（図内の共用サーバの MAC アドレス：1234.5600.e001）を，MAC アドレステーブルに設定します。

[注意事項]

MAC アドレステーブルに認証除外端末の MAC アドレスを設定する前に，除外端末が所属するポートに MAC VLAN の VLAN ID を設定してください。

11.5　MAC 認証のオペレーション

11.5.1　運用コマンド一覧

MAC 認証の運用コマンド一覧を次の表に示します。

表 11-3　運用コマンド一覧

コマンド名	説明
set mac-authentication mac-address	内蔵 MAC 認証 DB に MAC 認証用の MAC アドレス・認証後 VLAN ID 情報を追加します。（MAC アドレス情報の編集）
remove mac-authentication mac-address	内蔵 MAC 認証 DB から MAC アドレス情報を削除します。（MAC アドレス情報の編集）
commit mac-authentication	編集した MAC アドレス情報を内蔵 MAC 認証 DB に反映します。
store mac-authentication	内蔵 MAC 認証 DB のバックアップファイルを作成します。
load mac-authentication	バックアップファイルから内蔵 MAC 認証 DB を復元します。
show mac-authentication mac-address	内蔵 MAC 認証 DB の登録内容，または編集中の MAC アドレス情報を表示します。
show mac-authentication	MAC 認証の設定状態を表示します。
clear mac-authentication auth-state	認証済み MAC アドレスの強制認証解除を行います。
show mac-authentication login	MAC 認証の認証状態を表示します。
show mac-authentication login select-option	MAC 認証の認証状態を，表示オプションを選択して表示します。
show mac-authentication login summary	認証済み端末数を表示します。
show mac-authentication logging	MAC 認証で採取している動作ログメッセージを表示します。
clear mac-authentication logging	MAC 認証で採取している動作ログメッセージをクリアします。
show mac-authentication statistics	MAC 認証の統計情報を表示します。
clear mac-authentication statistics	MAC 認証の統計情報をクリアします。

11.5.2　内蔵 MAC 認証 DB の登録

ローカル認証方式で使用する，認証対象端末の MAC アドレス情報（MAC アドレス，認証後 VLAN ID）を内蔵 MAC 認証 DB に登録します。手順として，MAC アドレス情報の編集（追加・削除）と内蔵 MAC 認証 DB への反映があります。以下に登録例を示します。

なお，MAC アドレス情報の追加を行う前に，MAC 認証システムの環境設定およびコンフィグレーションの設定を完了している必要があります。

（1）MAC アドレス情報の追加

認証対象の端末ごとに，運用コマンド set mac-authentication mac-address で，MAC アドレス，認証後 VLAN ID を追加します。次の例では，MAC アドレスだけの登録例，MAC アドレスと MAC マスクの登録例を示します。

［コマンド入力］（MAC アドレスで指定）

```
# set mac-authentication mac-address 0012.e201.fff1 20
# set mac-authentication mac-address 0012.e202.fff1 30
```

［コマンド入力］（MAC アドレスと MAC マスクで指定）

```
# set mac-authentication mac-address 0012.e201.0000 0000.0000.ffff 40
# set mac-authentication mac-address 0012.e202.0000 0000.0000.ffff 60
```

［コマンド入力］（any 条件の指定）

```
# set mac-authentication mac-address 0000.0000.0000 ffff.ffff.ffff 1
```

上記の登録内容は，運用コマンド show mac-authentication mac-address で下記のように表示します。MAC アドレスの昇順で表示しますが，MAC アドレスだけの登録エントリ，MAC マスク有の登録エントリの順となります。

また，ローカル認証時の MAC アドレス検索は，下記の表示順で実行します。

図 11-9　内蔵 MAC 認証 DB の設定状態表示

```
# show mac-authentication mac-address edit

Date 20XX/05/20 17:40:02 UTC
 Total mac-address counts: 5
 mac-address     mac-mask          VLAN
 0012.e201.fff1  -                   20
 0012.e202.fff1  -                   30
 0012.e201.0000  0000.0000.ffff      40
 0012.e202.0000  0000.0000.ffff      60
 (any)           ffff.ffff.ffff       1

#
```

（2） MAC アドレス情報の削除

登録済み MAC アドレス情報の削除は，運用コマンド remove mac-authentication mac-address で行います。次の例では，１ユーザ分を削除します。

［コマンド入力］

```
# remove mac-authentication mac-address 0012.e202.fff1 30
Remove mac-authentication mac-address.  Are you sure? (y/n): y

#
```

MAC アドレス =0012.e202.fff1 VLAN ID=30 を削除します。

（3） 内蔵 MAC 認証 DB へ反映

編集した MAC アドレス情報を，運用コマンド commit mac-authentication で内蔵 MAC 認証 DB へ反映します。

［コマンド入力］

```
# commit mac-authentication
Commitment mac-authentication mac-address data.  Are you sure? (y/n): y

Commit complete.
#
```

11.5.3　内蔵 MAC 認証 DB のバックアップと復元

内蔵 MAC 認証 DB のバックアップおよびバックアップファイルからの復元を示します。

（1） 内蔵 MAC 認証 DB のバックアップ

内蔵 MAC 認証 DB から運用コマンド store mac-authentication でバックアップファイル（次の例では backupfile）を作成します。

［コマンド入力］

```
# store mac-authentication ramdisk backupfile
Backup mac-authentication MAC address data.  Are you sure? (y/n): y

Backup complete.
#
```

このとき，自動で 2 ファイル生成されます。（ファイル名 backupfile の例）

- backupfile　　：MAC マスク情報を含まないファイル
- backupfile.msk：MAC マスク情報を含むファイル

（2） 内蔵 MAC 認証 DB の復元

バックアップファイル（次の例では backupfile）から運用コマンド load mac-authentication で内蔵 MAC 認証 DB を復元します。

［コマンド入力］（MAC マスク情報を含まない内蔵 MAC 認証 DB を復元）

```
# load mac-authentication ramdisk backupfile
Restore mac-authentication MAC address data.  Are you sure? (y/n): y

Restore complete.
#
```

［コマンド入力］（MAC マスク情報を含む内蔵 MAC 認証 DB を復元）

```
# load mac-authentication ramdisk backupfile.msk
Restore mac-authentication MAC address data.  Are you sure? (y/n): y

Restore complete.
#
```

11.5.4 MAC 認証の設定状態表示

運用コマンド show mac-authentication で，MAC 認証の設定状態を表示します。

図 11-10 MAC 認証の設定状態表示

```
# show mac-authentication

Date 20XX/05/20 14:30:47 UTC
<<<MAC-Authentication mode status>>>
  Dynamic-VLAN     : Enable
  Static-VLAN      : Enable

<<<System configuration>>>
 * Authentication parameter
  Authentic-mode   : Dynamic-VLAN
  max-user         : 1024
  id-format type   : xx-xx-xx-xx-xx-xx
  password         : Disable
  vlan-check       : -
  roaming          : Disable

 * AAA methods
  Authentication Default       : RADIUS
  Authentication port-list-BBB : RADIUS ra-group-2
  Authentication End-by-reject : Disable
  Accounting Default           : RADIUS
```

```
 * Logout parameter
  max-timer         : infinity
  auto-logout       : 3600
  quiet-period      : 300
  reauth-period     : 3600

 * Logging status
  [Syslog send]     : Disable
  [Traps]           : Disable

<Port configuration>
  Port Count            : 1

  Port                  : 0/5
  VLAN ID               : 1000
  Forceauth VLAN        : Disable
  Access-list-No        : L2-auth
  ARP relay             : Enable
  Max-user              : 1024

<<<System configuration>>>
 * Authentication parameter
  Authentic-mode    : Static-VLAN
  max-user          : 1024
  id-format type    : xx-xx-xx-xx-xx-xx
  password          : Disable
  vlan-check        : Disable
  roaming           : Disable

 * AAA methods
  Authentication Default       : RADIUS
  Authentication port-list-BBB : RADIUS ra-group-2
  Authentication End-by-reject : Disable
  Accounting Default           : RADIUS

 * Logout parameter
  max-timer         : infinity
  auto-logout       : 3600
  quiet-period      : 300
  reauth-period     : 3600

 * Logging status
  [Syslog send]     : Disable
  [Traps]           : Disable

<Port configuration>
  Port Count            : 1

  Port                  : 0/4
  VLAN ID               : 200
  Forceauth VLAN        : Disable
  Access-list-No        : L2-auth
  ARP relay             : Enable
  Max-user              : 1024

#
```

11.5.5 MAC 認証の状態表示

運用コマンド show mac-authentication statistics で MAC 認証の状態および RADIUS サーバとの通信状況を表示します。

図 11-11 MAC 認証の表示

```
# show mac-authentication statistics

Date 20XX/05/20 13:23:41 UTC
MAC-Authentication Information:
  Authentication Request Total :         56
  Authentication Success Total :         32
  Authentication Fail Total    :         24
```

```
  Authentication Refuse Total  :         21
  Authentication Current Count :          1
  Authentication Current Fail  :          1

RADIUS MAC-Authentication Information:
[RADIUS frames]
  TxTotal   :        52  TxAccReq  :        52  TxError   :         0
  RxTotal   :        38  RxAccAccpt:        16  RxAccRejct:        22
                         RxAccChllg:         0  RxInvalid :         0
Account MAC-Authentication Information:
[Account frames]
  TxTotal   :        22  TxAccReq  :        22  TxError   :         0
  RxTotal   :        20  RxAccResp :        20  RxInvalid :         0

#
```

11.5.6 MAC 認証の認証状態表示

(1) 表示オプション指定なしで表示

運用コマンド show mac-authentication login で MAC 認証の認証状態を表示します。

図 11-12 MAC 認証の認証状態表示

```
# show mac-authentication login

Date 20XX/05/20 20:10:47 UTC
 Dynamic VLAN mode total client counts(Login/Max):  1 / 1000
  Authenticating client counts :    1
  Hold down client counts      :    1
  Port roaming : Enable
   No F MAC address     Port  VLAN Class  Login time           Limit     Reauth
    1   009f.eafb.003d  0/5   1000    62  20XX/05/20 20:10:46   23:59:58   86398

 Static VLAN mode total client counts(Login/Max):    1 / 1024
  Authenticating client counts :    1
  Hold down client counts      :    1
  Port roaming : Enable
   No F MAC address     Port  VLAN Class  Login time           Limit     Reauth
    1   0025.64c2.4725  0/4    200    24  20XX/05/20 20:10:46   23:59:59   86399

#
```

(2) 表示オプション指定ありで表示 (select-option 指定)

運用コマンド show mac-authentication login select-option で，MAC 認証の認証状態を指定した表示オプションで表示します。下記にインタフェースポート番号指定時の実行例を示します。

図 11-13 ポート指定時の情報表示

```
# show mac-authentication login select-option port 0/4

Date 20XX/05/20 20:23:21 UTC
 Static VLAN mode total client counts(Login/Max):    1 / 1024
  Authenticating client counts :    1
  Hold down client counts      :    1
  Port roaming : Enable
   No F MAC address     Port  VLAN Class  Login time           Limit     Reauth
    1   0025.64c2.4725  0/4    200    24  20XX/05/20 20:10:46   23:59:59   86399

#
```

(3) 認証済み端末数だけで表示 (summary 表示)

運用コマンド show mac-authentication login summary で MAC 認証の認証済み端末数を表示します。

図 11-14 認証済み端末数の表示

```
# show mac-authentication login summary port

Date 20XX/05/20 20:28:21 UTC
 Dynamic VLAN mode total client counts(Login/Max):   1 / 1000
  Authenticating client counts :    1
  Hold down client counts      :    1
  Port roaming : Disable
   No  Port  Login /  Max
    1  0/5       1 / 1000

 Static VLAN mode total client counts(Login/Max):    1 / 1024
  Authenticating client counts :    1
  Hold down client counts      :    1
  Port roaming : Disable
   No  Port  Login /  Max
    1  0/4       1 / 1024

#
```

12 マルチステップ認証

本装置では，端末認証とユーザ認証を 2 段階で実施するマルチステップ認証機能をサポートしています。この章では，マルチステップ認証について解説します。

12.1 解説

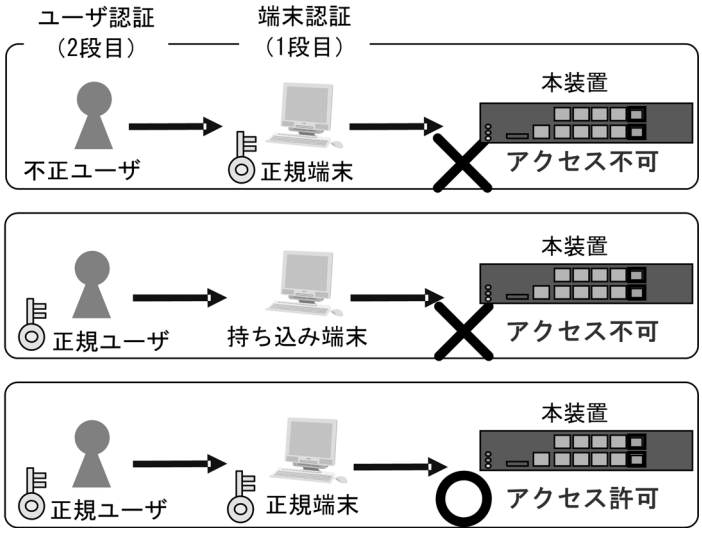
本機能は，下記の２段階認証により，正規端末を使用する正規ユーザだけにアクセスを許可します。

- １段目の端末認証が完了した正規端末の使用者だけに，２段目のユーザ認証を許可
- ２段目のユーザ認証まで認証完了した使用者を，正規ユーザとしてアクセスを許可

これにより，不正ユーザや持ち込み端末によるアクセスを排除できます。

マルチステップ認証の概要を次の図に示します。

図 12-1 マルチステップ認証概要図



本装置では，１段目の端末認証（以降，端末認証）と２段目のユーザ認証（以降，ユーザ認証）に下記のレイヤ 2 認証を使用します。

- 端末認証：MAC 認証，IEEE802.1X
- ユーザ認証：IEEE802.1X，Web 認証

また，マルチステップ認証独自で設定する機能はありませんが，認証対象端末に対して下記の機能も対応しています。

- 強制認証：「12.1.2　認証動作（8）強制認証」参照
- 認証済み端末のポート移動：「12.1.2　認証動作（10）ローミング（認証済み端末のポート移動）」参照
- 認証状態表示，アカウントログ，Trap：「12.1.2　認証動作（11）状態表示・アカウントログ・Trap など」参照

12.1.1 サポート範囲

(1) 対応する認証モード

マルチステップ認証は RADIUS 認証方式だけで使用できます。マルチステップ認証が動作する認証モードを次の表に示します。

表 12-1　マルチステップ認証が動作する認証モード

認証機能	認証方式グループ※	認証モード
MAC 認証＋ IEEE802.1X	装置デフォルト 認証方式リスト	固定 VLAN モード ダイナミック VLAN モード
MAC 認証＋ Web 認証	装置デフォルト 認証方式リスト	固定 VLAN モード ダイナミック VLAN モード
IEEE802.1X ＋ Web 認証	装置デフォルト 認証方式リスト	固定 VLAN モード ダイナミック VLAN モード

注※
　どちらの認証方式グループを設定しても，RADIUS 認証で動作します。

（2） 想定されるユーザまたは端末

本マニュアルでは，マルチステップ認証ポートへの接続が想定されるユーザまたは端末を以下のように定義します。

表 12-2　想定されるユーザまたは端末の定義

想定されるユーザまたは端末	通信許可に必要な認証	認証の種別
プリンタなど	端末認証のみ	シングル認証
社員ユーザ	端末認証＋ユーザ認証	マルチステップ認証
ゲストユーザ	ユーザ認証のみ	シングル認証

（3） マルチステップ認証のオプション

マルチステップ認証には，基本マルチステップ認証と，次の表に示すオプション種別があります。

表 12-3　マルチステップ認証のオプション種別

端末認証	ユーザ認証	マルチステップ認証のオプション種別	コンフィグレーション	備考
MAC 認証	IEEE802.1X Web 認証	基本マルチステップ認証	authentication multi-step	端末認証成功時だけ， ユーザ認証実施可能です。
MAC 認証	IEEE802.1X Web 認証	ユーザ認証許可オプション	authentication multi-step permissive	端末認証が失敗しても， ユーザ認証実施可能です。
IEEE802.1X MAC 認証	Web 認証	端末認証 dot1x オプション	authentication multi-step dot1x	端末認証成功時だけ， ユーザ認証実施可能です。 端末認証に IEEE802.1X を追加します。

（a） ユーザ認証許可オプション

本装置のマルチステップ認証設定には，ユーザ認証許可オプションがあります。基本的には端末認証成功後にだけユーザ認証の機会が与えられますが，本オプションの設定によって，同一マルチステップ認証ポートで，社員ユーザとゲストユーザを混在させることが可能です。

マルチステップ認証のコンフィグレーションと端末やユーザの認証可否を次の表に示します。

表 12-4 マルチステップ認証のコンフィグレーションと端末やユーザの認証可否

マルチステップ認証設定	ユーザ認証許可オプション設定	プリンタ	社員ユーザ	ゲストユーザ
設定有	設定無	○	●	×
	設定有	○	●※	○※
設定無	－	○	○	○

（凡例）
●：マルチステップ認証
○：シングル認証
×：ユーザ認証実施不可
－：対象外

注※
端末認証が失敗の場合でもユーザ認証を実施できるマルチステップ認証ポートになりますが，RADIUS 属性 Filter-Id の内容により，特定のユーザ ID(社員ユーザ) に対しては端末認証成功が必須とし，特定のユーザ (ゲストユーザ) に対しては，端末認証不要で認証完了とさせることができます。

(b) 端末認証 dot1x オプション

端末認証に，IEEE802.1X を追加するオプションです。基本的には MAC 認証成功後にユーザ認証を許可しますが，本オプションの設定によって端末認証の IEEE802.1X が認証成功時に，ユーザ認証（この場合は Web 認証だけが対象）の機会を与えられます。

- 本オプションを設定したポートは，端末認証として MAC 認証と IEEE802.1X が同時に動作します。
- 本オプションを設定したポートは，端末認証成功時だけ，ユーザ認証の機会が与えられます。
- 本オプションとユーザ認証許可オプションは，同一ポートに設定できません。

(4) 同一ポートでの各認証機能の動作

同一マルチステップ認証設定ポートでの，各認証機能の動作を次の表に示します。

表 12-5 同一マルチステップ認証設定ポートでの各認証機能の動作

マルチステップ認証ポート設定とオプション種別	端末認証			ユーザ認証			想定されるユーザまたは端末
	RADIUS 属性 Filter-Id 有無	MAC 認証許可の扱い	IEEE802.1X 許可の扱い※	RADIUS 属性 Filter-Id 有無	IEEE802.1X 許可の扱い	Web 認証許可の扱い	
基本マルチステップ認証ポート	無	○	－	－	－	－	プリンタなど
	有	△	－	無	●	●	社員ユーザ
				有	●	●	社員ユーザ
ユーザ認証許可オプションポート	無	○	－	－	－	－	プリンタなど
	有	△	－	無	○	○	ゲストユーザ
				有	●	●	社員ユーザ
端末認証 dot1x オプションポート	無	○	○	－	－	－	プリンタなど
	有	△	△	無	－	●	社員ユーザ
				有	－	●	社員ユーザ
未設定ポート（シングル認証）	－	○	－	－	○	○	－

（凡例）

●：マルチステップ認証
○：シングル認証
△：ユーザ認証結果待ち（認証許可保留中）
－：対象外

注※
IEEE802.1X コンピュータ認証など

12.1.2　認証動作

（1）MAC 認証契機

マルチステップ認証ポートとシングル認証ポートでは，MAC 認証の認証契機となるフレームに差異があります。

次の表に示すように，マルチステップ認証ポートでは，IEEE802.1X 設定有無および Web 認証の設定有無に関わらず，EAPOL フレームや http/https フレームを含むすべてのフレームが MAC 認証の認証契機となります。

シングル認証ポートでは，IEEE802.1X 未設定の場合に EAPOL フレームが MAC 認証契機となり，Web 認証未設定の場合に http/https フレームが MAC 認証契機となります。

MAC 認証の認証契機となる対象フレームを次の表に示します。

表 12-6　マルチステップ認証設定と MAC 認証契機の対象フレーム

フレーム種別	EAPOL		http/https	
ポートの設定	IEEE802.1X 設定有	IEEE802.1X 設定無	Web 認証 設定有	Web 認証 設定無
マルチステップ認証設定有	○	○	○	○
マルチステップ認証設定無（シングル認証ポート）	－	○	－	○

（凡例）
○：MAC 認証の対象
－：MAC 認証の対象外

（2）RADIUS 属性 Filter-Id による認証動作の判定

マルチステップ認証では，RADIUS サーバから認証成功（Accept）を受信したときに RADIUS 属性 Filter-Id の文字列で次段階の認証動作を判定します。

マルチステップ認証で使用する RADIUS 属性 Filter-Id の文字列を次の表に示します。

表 12-7　マルチステップ認証で使用する RADIUS 属性 Filter-Id 文字列

RADIUS 属性 Filter-Id の文字列	意味	RADIUS 属性 Filter-Id の文字列を判定する認証機能
@@1X-Auth@@	IEEE802.1X の認証動作を許可	MAC 認証
/1X-Auth		
@@Web-Auth@@	Web 認証の認証動作を許可	IEEE802.1X※1，MAC 認証
/Web-Auth		

RADIUS 属性 Filter-Id の文字列	意味	RADIUS 属性 Filter-Id の文字列を判定する認証機能
@@MultiStep@@	IEEE802.1X と Web 認証の認証動作を許可（ユーザ認証はどちらを実施してもよい）	IEEE802.1X※1※2，MAC 認証
/MultiStep		
@@MAC-Auth@@	MAC 認証が必須	IEEE802.1X，Web 認証
/MAC-Auth		

注 ※1

端末認証 dot1x オプションが設定されているとき

注 ※2

端末認証が IEEE802.1X のときは，Filter-Id が "@@MultiStep@@"（または，"/MultiStep"）でもユーザ認証は Web 認証だけを許可します。

"@@ MAC-Auth@@" などの代わりに "/MAC-Auth" の形式も使用可能です。

（3） 基本マルチステップ認証ポートの動作

基本マルチステップ認証ポートでは，端末認証とユーザ認証は下記の認証動作を行います。

1. 端末認証では，端末認証成功時に RADIUS 属性 Filter-Id の下記文字列に従って次のユーザ認証待ちとなります。このとき，MAC アドレステーブルには該当端末の MAC アドレスを認証エントリとして登録しません。（下記文字列以外はシングル認証扱いとなり，MAC アドレステーブルに該当端末の MAC アドレスを認証エントリとして登録します。）
   - @@1X-Auth@@（または，/1X-Auth）
   - @@Web-Auth@@（または，/Web-Auth）
   - @@MultiStep@@（または，/MutliStep）
2. ユーザ認証は，端末認証成功後に許可されるので，ユーザ認証時は RADIUS 属性 Filter-Id の結果に依存せずにユーザ認証成功で認証完了となります。MAC アドレステーブルに該当端末の MAC アドレスを認証エントリとして登録し，端末の通信が可能になります。
   なお，MAC アドレステーブルに認証機能が MAC アドレスを認証エントリとして登録したときは，運用コマンド show mac-address table で MAC アドレスエントリに各認証機能名が表示されます。
   - IEEE802.1X（Dot1x）
   - Web 認証（WebAuth）
   - MAC 認証（MacAuth）

   （Static）と表示される MAC アドレスエントリは，コンフィグレーションコマンド mac-address-table static で登録されているエントリです。
   認証が完全に完了していない端末は，（Dynamic）と表示されます。
3. このポートで実施できる認証
   基本マルチステップ認証ポートで実施できる認証を次の表に示します。

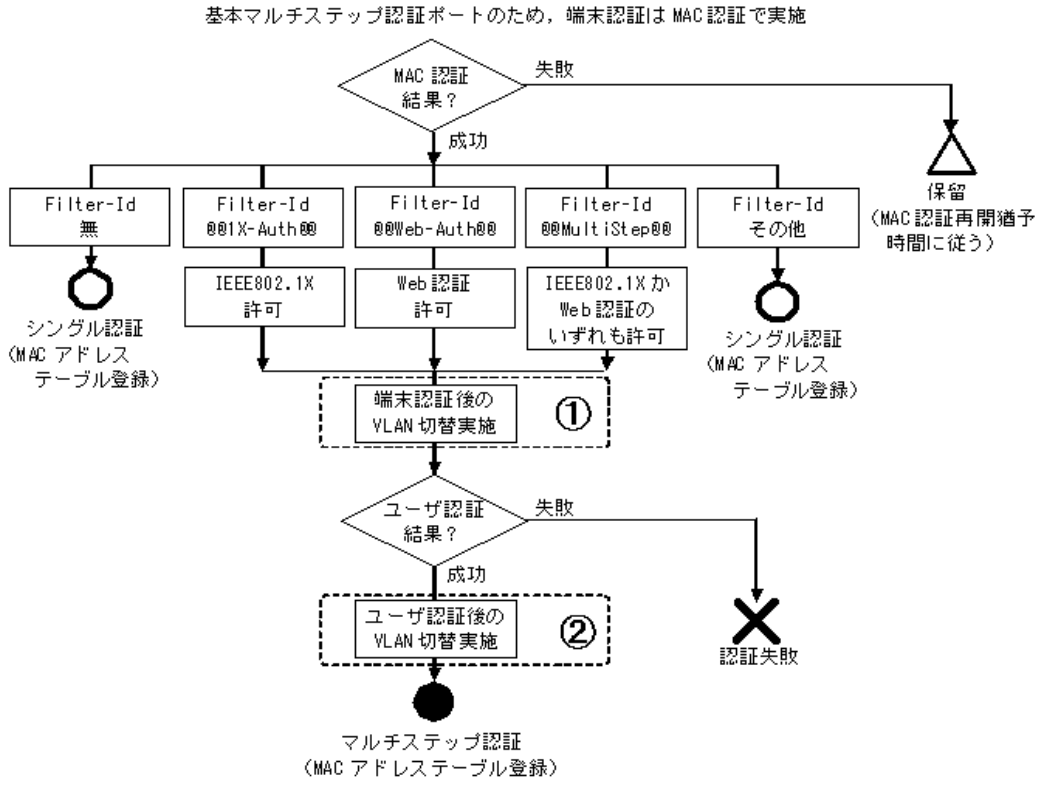
表 12-8 基本マルチステップ認証ポートで実施できる認証

端末認証	ユーザ認証	端末の管理
MAC 認証：成功	ユーザ認証無	シングル認証
MAC 認証：成功	IEEE802.1X：成功	マルチステップ認証
MAC 認証：成功	Web 認証：成功	マルチステップ認証

上記以外の組み合わせでは認証できません。

基本マルチステップ認証ポートの動作を次の図に示します。（図内の Filter-Id は，"@@ ～ @@" の例です。）

図 12-2　基本マルチステップ認証ポートの認証動作



ダイナミック VLAN モードのときは，端末認証とユーザ認証でそれぞれ認証成功時に VLAN 切替を実施（図内①および②）します。

ユーザ認証が失敗したときも，端末認証で実施した VLAN 切替（図内①）状態は維持されます。

なお，認証済み端末は無通信監視などの認証解除条件が成立すると認証を解除し，切り替えた VLAN を認証前の状態（ネイティブ VLAN）に戻します。

（4） ユーザ認証許可オプションポートの認証動作

同一マルチステップ認証ポートで社員ユーザとゲストユーザを混在するときは，コンフィグレーションコマンド authentication multi-step で，ユーザ認証許可オプション permissive を指定します。

ユーザ認証許可オプションを指定したポートでは，１段目の端末認証（MAC 認証）が失敗しても，ユーザ認証（IEEE802.1X または Web 認証）の認証動作を許可します。

このときのユーザ認証は，端末認証（MAC 認証）の失敗状態（保留エントリ）が存在する時間内だけ実施できます。従って，MAC 認証の認証再開猶予タイマ（mac-authentication timeout quiet-period）は，0 秒以外を設定してください。（デフォルトコンフィグレーションは 300 秒です。）

ユーザ認証許可オプションポートで実施できる認証を次の表に示します。

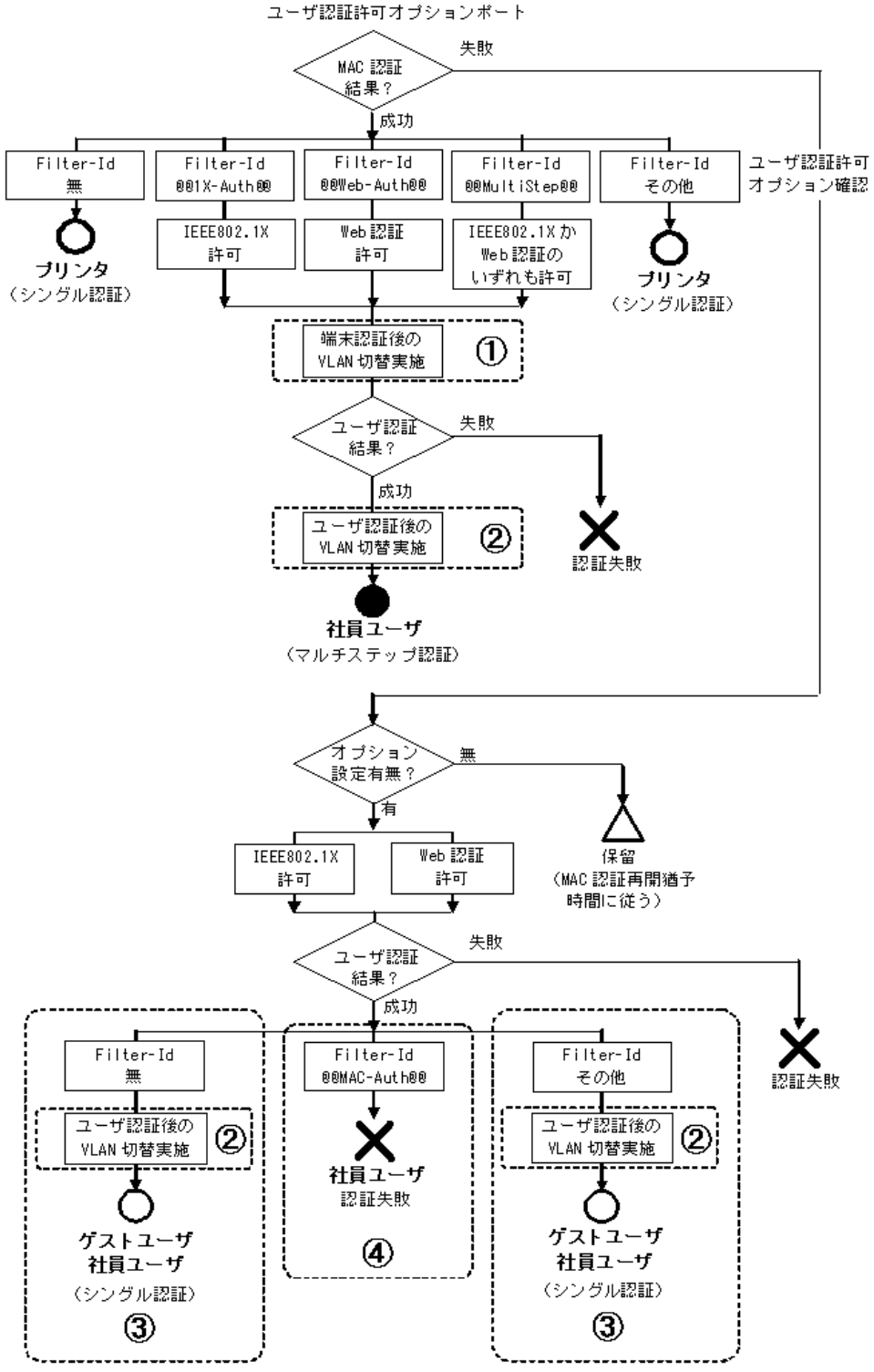
表 12-9 ユーザ認証許可オプションポートで実施できる認証

端末認証	ユーザ認証	端末の管理
MAC 認証：成功	ユーザ認証無	シングル認証
MAC 認証：成功	IEEE802.1X：成功	マルチステップ認証
MAC 認証：成功	Web 認証：成功	マルチステップ認証
MAC 認証：失敗	IEEE802.1X：成功	シングル認証
MAC 認証：失敗	Web 認証：成功	シングル認証

上記以外の組み合わせでは認証できません。

ユーザ認証許可オプションポートの認証動作を次の図に示します。（図内の Filter-Id は，"@@ ～ @@" の例です。）

図 12-3　マルチステップ認証設定ポートでユーザ認証許可オプション有の認証動作



ダイナミック VLAN モードのときは，端末認証とユーザ認証でそれぞれ認証成功時に VLAN 切替を実施（図内①および②）します。

ユーザ認証が失敗したときも，端末認証で実施した VLAN 切替（図内①）状態は維持されます。

なお，認証済み端末は無通信監視などの認証解除条件が成立すると認証を解除し，切り替えた VLAN を認証前の状態（ネイティブ VLAN）に戻します。

ユーザ認証許可オプションポートで同時に社員ユーザも認証すると，社員ユーザもシングル認証扱い（図内③）となります。この場合は，ユーザ認証用の RADIUS サーバで，RADIUS 属性 Filter-Id に "@@MAC-Auth@@"（または，"/MAC-Auth"）を設定してください。Filter-Id の "@@MAC-Auth@@"（または，"/MAC-Auth"）により，ユーザ認証許可オプションポートでも，端末認証失敗時は社員ユーザを認証失敗（図内④）にすることが可能です。

ユーザ認証許可オプションポートで受信した RADIUS 属性 Filter-Id とユーザ認証の認証動作を次の表に示します。

表 12-10　ユーザ認証許可オプションポートの認証動作

ユーザ認証で受信した RADIUS 属性 Filter-Id 内容	端末認証結果	ユーザ認証の認証動作	想定ユーザ
無	－	MAC 認証不要ユーザと判断し，認証成功	ゲストユーザ
@@MAC-Auth@@（または，/MAC-Auth）	成功	MAC 認証必須ユーザと判断。 MAC 認証結果が成功しているので，認証成功	社員ユーザ
	失敗	MAC 認証必須ユーザと判断。 MAC 認証結果が失敗しているため，認証失敗	不正ユーザ
上記以外	－	MAC 認証不要ユーザと判断し，認証成功	ゲストユーザ

（凡例）
－：端末認証結果には依存しない

（5） 端末認証 dot1x オプションポートの認証動作

端末認証 dot1x オプションポートでは，端末認証とユーザ認証は下記の認証動作を行います。

1. 端末認証では，端末認証成功時に RADIUS 属性 Filter-Id の下記文字列に従って次のユーザ認証待ちとなります。このとき，MAC アドレステーブルには該当端末の MAC アドレスを認証エントリとして登録しません。（下記文字列以外はシングル認証扱いとなり，MAC アドレステーブルに該当端末の MAC アドレスを認証エントリとして登録します。）
   - @@Web-Auth@@（または，/Web-Auth）
   - @@MultiStep@@（または，/MultiStep）
2. ユーザ認証は，端末認証成功後に許可されるので，ユーザ認証時は RADIUS 属性 Filter-Id の結果に依存せずにユーザ認証成功で認証完了となります。MAC アドレステーブルに該当端末の MAC アドレスを認証エントリとして登録し，端末の通信が可能になります。
   なお，MAC アドレステーブルに認証機能が MAC アドレスを認証エントリとして登録したときは，運用コマンド show mac-address table で MAC アドレスエントリに各認証機能名が表示されます。
   - IEEE802.1X（Dot1x）
   - Web 認証（WebAuth）
   - MAC 認証（MacAuth）

   （Static）と表示される MAC アドレスエントリは，コンフィグレーションコマンド mac-address-table static で登録されているエントリです。
   認証が完全に完了していない端末は，（Dynamic）と表示されます。
3. このポートで実施できる認証

端末認証 dot1x オプションポートで実施できる認証を次の表に示します。

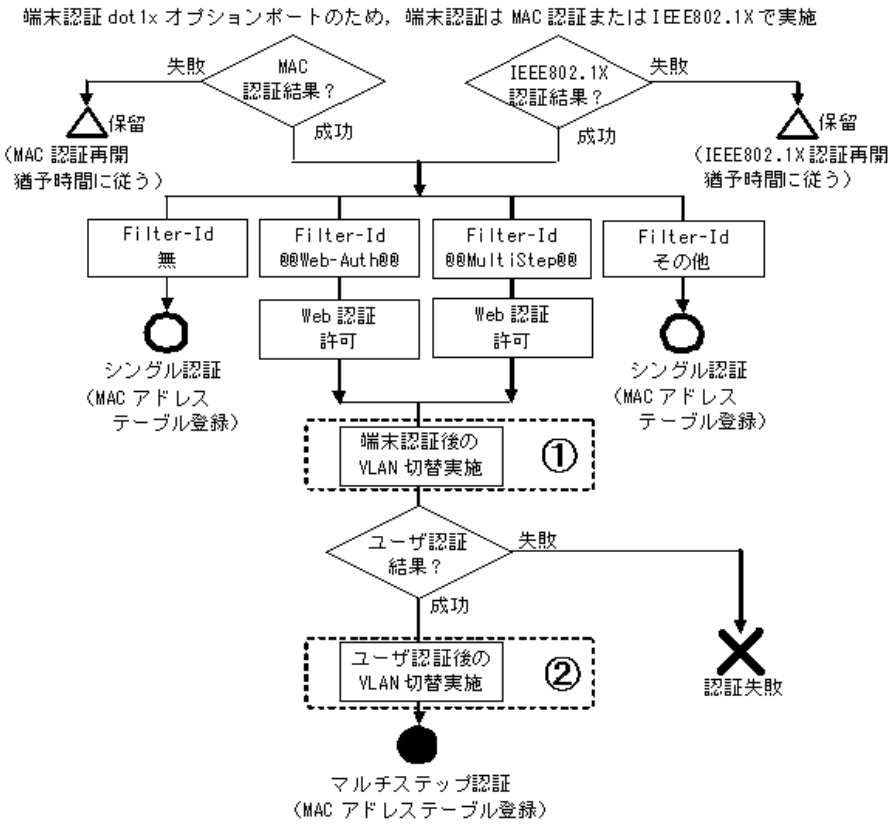
表 12-11　端末認証 dot1x オプションポートで実施できる認証

端末認証	ユーザ認証	端末の管理
MAC 認証：成功	ユーザ認証無	シングル認証
IEEE802.1X：成功	ユーザ認証無	シングル認証
MAC 認証：成功	Web 認証：成功	マルチステップ認証
IEEE802.1X：成功	Web 認証：成功	マルチステップ認証

上記以外の組み合わせでは認証できません。

端末認証 dot1x オプションポートの認証動作を次の図に示します。（図内の Filter-Id は，"@@ 〜 @@" の例です。）

図 12-4　端末認証 dot1x オプションポートの認証動作



ダイナミック VLAN モードのときは，端末認証とユーザ認証でそれぞれ認証成功時に VLAN 切替を実施（図内①および②）します。

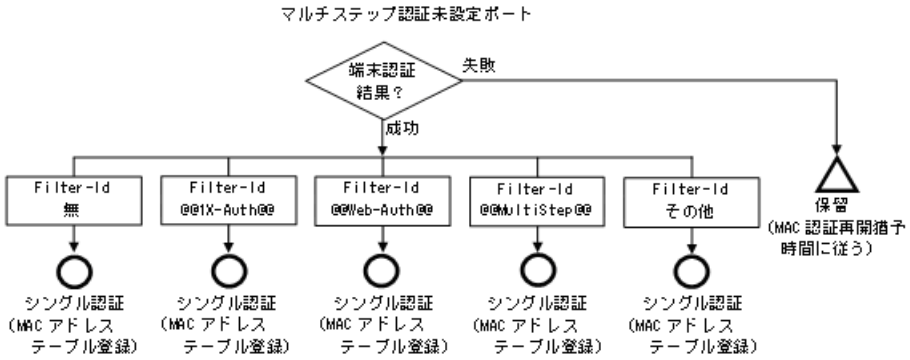
ユーザ認証が失敗したときも，端末認証で実施した VLAN 切替（図内①）状態は維持されます。

なお，認証済み端末は無通信監視などの認証解除条件が成立すると認証を解除し，切り替えた VLAN を認証前の状態（ネイティブ VLAN）に戻します。

(6) マルチステップ認証未設定ポート（シングル認証ポート）の認証動作

マルチステップ認証未設定ポートの認証動作を次の図に示します。(図内の Filter-Id は，"@@ ～ @@" の例です。)

図 12-5 マルチステップ認証未設定ポートの認証動作



Filter-Id に下記の文字列が指定されていても，シングル認証扱いとなります。

- @@1X-Auth@@（または，/1X-Auth）
- @@Web-Auth@@（または，/Web-Auth）
- @@MultiStep@@（または，/MultiStep）

(7) 認証後 VLAN について

ダイナミック VLAN モードを使用しているときは，認証成功時に端末認証・ユーザ認証それぞれの RADIUS サーバから通知された VLAN に切り替わります。RADIUS サーバに設定する VLAN 情報については，後述の「12.1.3 事前準備」を参照してください。

(8) 強制認証

強制認証有効時の該当端末は，以下の認証扱いとなります。

表 12-12 強制認証有効時の該当端末の扱い

マルチステップ認証ポートオプション種別	端末認証で強制認証時	ユーザ認証で強制認証時
基本マルチステップ認証	シングル認証	マルチステップ認証
ユーザ認証許可オプション	シングル認証	シングル認証
端末認証 dot1x オプション	シングル認証	マルチステップ認証

強制認証時に端末を収容する VLAN は，下記のとおりです。

表 12-13 強制認証時の該当端末の収容 VLAN

ポートの種類	コンフィグレーション 強制認証用の VLAN 設定	収容 VLAN
アクセスポート	対象外	VLAN 固定
トランクポート	対象外	VLAN 固定

ポートの種類	コンフィグレーション 強制認証用の VLAN 設定	収容 VLAN
MAC ポート	設定有	コンフィグレーションで設定された VLAN に依存
	設定無	ネイティブ VLAN
MAC ポート （dot1q vlan 設定時）	対象外	VLAN 固定

（9） 認証端末の管理と認証解除

（a） マルチステップ認証端末の管理

マルチステップ認証端末の管理は，最終認証機能で管理します。端末認証で認証許可となった端末が，ユーザ認証で許可されたときはユーザ認証の管理下とします。マルチステップ認証ポートでもシングル認証で認証完了したときは，当該認証機能で端末を管理します。

（b） マルチステップ認証端末の認証解除

マルチステップ認証端末の認証解除は，ユーザ認証の解除条件に従って解除します。マルチステップ認証ポートでもシングル認証で認証完了したときは，当該認証機能の解除条件に従って解除します。認証解除については，各認証機能の解説編を参照してください。

なお，端末認証 dot1x オプションポートで EAPOL-Start フレームを受信すると，Web 認証で認証済みの端末を認証解除します。（同ポートで，MAC 認証＋ Web 認証で認証済みの端末が EAPOL-Start フレームを受信したときも同様に認証解除します。）

（c） マルチステップ認証端末の無通信監視

マルチステップ認証ポートの認証端末は，端末の状態に応じて以下の無通信監視手段を適用します。

- 認証完了している端末は，無通信監視を適用します。
- 保留状態の端末は，MAC アドレステーブルエージング監視を適用します。
- 認証失敗状態の端末は，端末のエントリを一定時間保持します。

端末の状態と無通信監視手段を次の表に示します。

表 12-14　端末の状態と無通信監視手段

端末の状態	認証状態	MAC 認証	IEEE802.1X	Web 認証
認証完了	マルチステップ認証 （ユーザ認証完了）	－	無通信監視時間	無通信監視時間
	シングル認証	無通信監視時間	無通信監視時間	無通信監視時間
保留	端末認証成功 ※1 （ユーザ認証完了待ち）	MAC アドレステーブル エージング監視時間	MAC アドレステーブル エージング監視時間	－
	検疫状態 ※1※2	－	MAC アドレステーブル エージング監視時間	－
認証失敗	認証失敗	MAC 認証再開 猶予タイマ満了まで保持	IEEE802.1X 認証再開 猶予タイマ満了まで保持	即エントリ消去

（凡例） －：対象外

注 ※1

該当端末の MAC アドレスは，Dynamic エントリとして MAC アドレステーブルで管理されています。
該当端末の MAC アドレスが MAC アドレステーブルからエージングで消去されてから，無通信監視時間経過後に認証解除されます。

注 ※2
ポート単位認証（静的）のときだけです。

（10）ローミング（認証済み端末のポート移動）

認証済み端末のポート移動は，最終認証した機能により下記の動作となります。マルチステップ認証独自のローミング設定はありません。

1. 最終認証：IEEE802.1X
認証済み端末をマルチステップ認証または IEEE802.1X 認証の設定ポートへポート移動したときは，認証解除します。
なお，認証済み端末をマルチステップ認証および IEEE802.1X 認証未設定ポートへ移動したときは，認証解除しません。

2. 最終認証：Web 認証
認証ポリシーと Web 認証のローミング設定に従います。
移動前後の認証ポリシーが同一のポートは移動可能です。
移動前後のポートがシングル認証同士の場合は，Web 認証のポート移動条件に従います。

【認証ポリシー】
以下のコンフィグレーションの組み合わせが，移動前後のポートで完全一致していることを条件とします。

表 12-15　移動前後のポートのコンフィグレーション組み合わせ条件

条件		備考
移動前後に authentication multi-step 設定有		移動前後で authentication multi-step 設定無は，シングル認証同士として処理
	ユーザ認証許可オプション有無が同一	authentication multi-step 設定時に比較
	端末認証 dot1x オプション有無が同一	authentication multi-step 設定時に比較
以下の組み合わせが同一		authentication multi-step 設定時に比較
	dot1x port-control	aaa authentication dot1x default 設定時に比較
	web-authentication port	web-authentication system-auth-control 設定時に比較
	mac-authentication port	mac-authentication system-auth-control 設定時に比較

上記に該当しないときは認証解除となります。
なお，認証済み端末をマルチステップ認証および Web 認証未設定ポートへ移動したときは，認証解除しません。認証未設定ポートへ移動したときに認証を解除する場合は，コンフィグレーションコマンド authentication auto-logout strayer を設定してください。

3. 最終認証：MAC 認証
MAC 認証のローミング設定に従います。
移動前後のポートでマルチステップ認証設定が同一のときに移動可能です。
移動前後のポートがシングル認証同士の場合は，MAC 認証のポート移動条件に従います。

表 12-16　移動前後のポートのマルチステップ認証設定条件

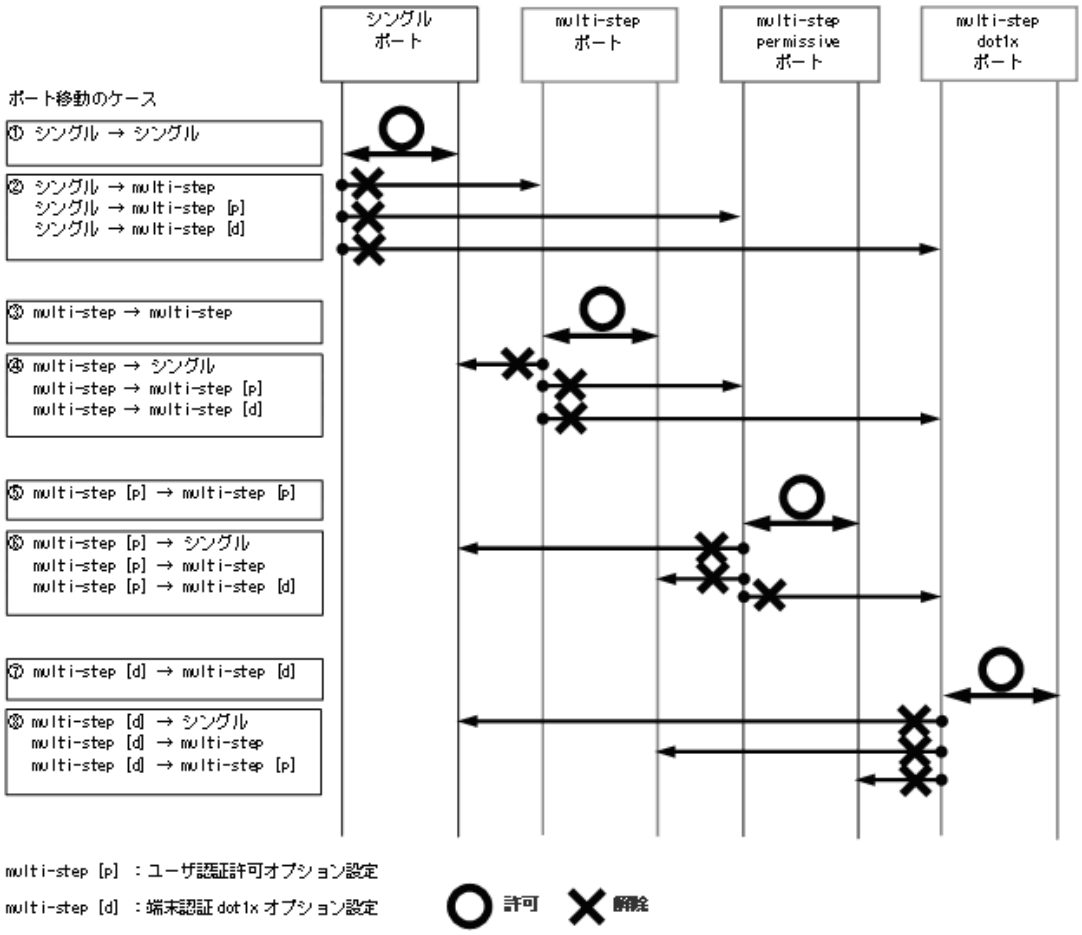
条件		備考
移動前後に authentication multi-step 設定有		移動前後で authentication multi-step 設定無は，シングル認証同士として処理
	ユーザ認証許可オプション有無が同一	authentication multi-step 設定時に比較
	端末認証 dot1x オプション有無が同一	authentication multi-step 設定時に比較

上記に該当しないときは認証解除となります。
なお，認証済み端末をマルチステップ認証および MAC 認証未設定ポートへ移動したときは，認証解除しません。認証未設定ポートへ移動したときに認証を解除する場合は，コンフィグレーションコマンド authentication auto-logout strayer を設定してください。

Web 認証や MAC 認証のローミング設定については，「8　Web 認証の解説」および「10　MAC 認証の解説」で各認証モードの「ローミング（認証済み端末のポート移動)」を参照してください。

マルチステップ認証端末のポート移動のケースと移動可否を次の図に示します。移動前後のポートは，マルチステップ認証またはシングル認証を設定済みとします。

図 12-6　マルチステップ認証端末のポート移動のケースと移動可否



図内①はシングル認証同士のため，Web 認証や MAC 認証のポート移動条件に従います。

図内③⑤⑦は移動前後のポートで「表 12-15　移動前後のポートのコンフィグレーション組み合わせ条件」や「表 12-16　移動前後のポートのマルチステップ認証設定条件」に一致しているときに，ポート移動可能となります。

その他は，マルチステップ認証ポート設定が移動前後で不一致のため，認証解除となります。

ポート移動検出時の動作は，該当端末を最終認証した認証機能に従います。「図 12-6　マルチステップ認証端末のポート移動のケースと移動可否」を例に，各認証機能のポート移動検出時の動作を以下に示します。

1. 最終認証：IEEE802.1X
   フレーム受信により，IEEE802.1X 端末のポート移動を検出した際は，ローミング設定がありませんので，全ケースで認証解除となります。
2. 最終認証：Web 認証
   フレーム受信により，Web 認証端末のポート移動を検出した際の動作を次の表に示します。認証ポリシーは，「表 12-15　移動前後のポートのコンフィグレーション組み合わせ条件」を参照してください。

表 12-17　Web 認証端末のポート移動検出時の動作

「図 12-6」ポート移動のケース	Web 認証のローミング設定		
	disable	enable	
		認証ポリシー一致	認証ポリシー不一致
①，③，⑤，⑦	認証解除	認証情報更新 (ポート移動)	認証解除
上記以外	認証解除	認証解除	認証解除

3. 最終認証：MAC 認証
   フレーム受信により，MAC 認証端末のポート移動を検出した際の動作を次の表に示します。

表 12-18　MAC 認証端末のポート移動検出時の動作

「図 12-6」番号ポート移動のケース	MAC 認証のローミング設定	
	disable	enable
①，③，⑤，⑦	認証解除	認証情報更新 (ポート移動)
上記以外	認証解除	認証解除

(11) 状態表示・アカウントログ・Trap など

- マルチステップ認証状態
  運用コマンド show authentication multi-step でマルチステップ認証の認証経過を MAC アドレス単位で表示します。
- アカウントログ表示
  運用コマンド show authentication logging で，各認証機能のアカウントログを採取時刻順に統合表示します。
- プライベート Trap
  プライベート Trap は各認証機能の設定に従います。マルチステップ認証独自のプライベート Trap はありません。

12.1.3　事前準備

マルチステップ認証では RADIUS 認証だけサポートしています。端末認証とユーザ認証は，RADIUS サーバから Accept 受信時に RADIUS 属性 Filter-Id の文字列で認証動作を決定します。

表 12-19　マルチステップ認証で使用する属性名（Access-Accept）

属性名	Type 値	解説
Filter-Id	11	テキスト文字列。 本装置でマルチステップ認証運用時に認証動作を判定します※。 • @@1X-Auth@@（または，/1X-Auth） • @@Web-Auth@@（または，/Web-Auth） • @@MultiStep@@（または，/MultiStep） • @@MAC-Auth@@（または，/MAC-Auth）
Tunnel-Private-Group-ID	81	VLAN を識別する文字列。 1.　端末認証用 RADIUS サーバの場合 • ユーザ認証が IEEE802.1X IEEE802.1X の認証前 VLAN • ユーザ認証が Web 認証 Web 認証ログイン画面にアクセスする IP アドレスが所属する VLAN 2.　ユーザ認証用 RADIUS サーバの場合 • 認証後 VLAN

注 ※
Filter-Id 文字列を判定する認証機能および認証動作については，「12.1.2　認証動作」を参照してください。

その他の RADIUS 属性は各認証機能に従います。各認証機能解説編の事前準備を参照してください。

12.1.4　マルチステップ認証使用時の注意事項

（1）ユーザ認証許可オプション有と MAC 認証の設定について

ユーザ認証許可オプション（permissive）は，端末認証（MAC 認証）が失敗したときもユーザ認証を許可するための設定です。ユーザ認証許可オプションを設定したときも端末認証とユーザ認証を実行するために，MAC 認証で下記の設定を確認してください。

1. 認証対象 MAC アドレスの制限
   認証対象 MAC アドレスの制限（mac-authentication access-group）で，ユーザ認証（IEEE802.1X または Web 認証）で使用する端末の MAC アドレスは，認証対象 MAC アドレスとして設定してください。
   認証対象外 MAC アドレスに設定していると MAC 認証が開始されないため，ユーザ認証も実行できなくなります。
   認証対象 MAC アドレス制限については，「10　MAC 認証の解説　10.2.2　認証機能　（2）認証対象 MAC アドレスの制限」を参照してください。
2. 認証再開猶予タイマ
   認証再開猶予タイマ（mac-authentication timeout quiet-period）は，0 秒以外を設定してください。（デフォルトコンフィグレーションは 300 秒です。）
   0 秒を設定すると MAC 認証で認証失敗時に失敗情報が保持されず，ユーザ認証許可オプション設定有でもユーザ認証を実行できなくなります。
   認証再開猶予タイマについては，「10　MAC 認証の解説　10.2.2　認証機能　（3）認証再開猶予タイマ」を参照してください。

（2） IEEE802.1X を使用する場合

マルチステップ認証対象ポートで，IEEE802.1X を使用するときは，下記設定を確認してご使用ください。

- 認証サブモード：端末認証モード設定（dot1x multiple-authentication）
- 端末検出動作切り替えオプション：auto 設定（dot1x supplicant-detection auto）

（3） 端末認証 dot1x オプションについて

端末認証 dot1x オプションを設定すると，端末認証として MAC 認証と IEEE802.1X が同時に動作します。認証対象端末を IEEE802.1X ＋ Web 認証でご使用になるときは，システム条件として MAC 認証が成功する設定をしないでください。（RADIUS サーバに当該端末を MAC 認証対象として登録しないなど。）

（4） 認証済み端末のポート移動について

認証済み端末をマルチステップ認証またはシングル認証の設定ポートへ移動したときは，「12.1.2　認証動作　（10）ローミング（認証済み端末のポート移動）」により，継続通信または認証解除となります。

なお，認証済み端末を同一 VLAN 内のマルチステップ認証およびシングル認証未設定ポートへ移動したときは，認証状態が解除されるまで通信できません。認証済み端末が最終認証された機能の運用コマンドを使用して，端末の認証状態を解除してください。

- IEEE802.1X：運用コマンド clear dot1x auth-state
- Web 認証　：運用コマンド clear web-authentication auth-state
- MAC 認証　：運用コマンド clear mac-authentication auth-state

認証未設定ポートへ移動したときに認証状態を解除する場合は，コンフィグレーションコマンド authentication auto-logout strayer を設定してください。

（5） RADIUS 属性の Filter-id の設定について

"@@ MAC-Auth@@" などの代わりに "/MAC-Auth" の形式も使用可能ですが，マルチステップ認証と併用する機能によって下記の制限があります。

- 本機能とダイナミック ACL/QoS 機能を併用する場合
  "/MAC-Auth/Class=37" などとしてください。（"@" で始まる形式は使用できません。）
- 本機能と IEEE802.1X の NAP 連携を併用する場合
  "123@@MAC-Auth@@" などとしてください。（"/" で始まる形式は使用できません。）

12.2　コンフィグレーション

12.2.1　コンフィグレーションコマンド一覧

マルチステップ認証のコンフィグレーションコマンド一覧を次の表に示します。

表 12-20　マルチステップ認証のコンフィグレーションコマンド一覧

コマンド名	説明
authentication multi-step	マルチステップ認証を実行するポートに設定します。

12.2.2　マルチステップ認証の構築形態

以降のコンフィグレーション説明では，マルチステップ認証の構築形態ごとに，構成例と設定例，および設定のポイントについて説明します。

本項で説明するマルチステップ認証の構築形態を次の表に示します。なお，どのケースも，端末の IP アドレスは DHCP サーバから取得とします。

表 12-21　マルチステップ認証の構築形態

マルチステップポートの種別	認証モード種別	ポート種別	認証対象種別	認証機能種別		設定ポイント参照先	設定例参照先
				端末	ユーザ		
基本マルチステップ認証ポート	ダイナミック VLAN	MAC	社員ユーザ	MAC	Web	12.2.3 (1)(b) ケース①	12.2.3 (1)(d)
			プリンタ	MAC	―	12.2.3 (1)(c) ケース②	
	固定 VLAN	アクセス トランク MAC（ネイティブ）	社員ユーザ	MAC	Web	12.2.3 (2)(b) ケース③	12.2.3 (2)(d)
			プリンタ	MAC	―	12.2.3 (2)(c) ケース④	
ユーザ認証許可オプションポート	ダイナミック VLAN	MAC	ゲストユーザ	―	Web	12.2.4 (1)(b) ケース⑤	12.2.4 (1)(d)
			社員ユーザ	MAC	Web	12.2.4 (1)(c) ケース⑥	
	固定 VLAN	アクセス トランク MAC（ネイティブ）	ゲストユーザ	―	Web	12.2.4 (2)(b) ケース⑦	12.2.4 (2)(d)
			社員ユーザ	MAC	Web	12.2.4 (2)(c) ケース⑧	
端末認証 dot1x オプションポート	ダイナミック VLAN	MAC	社員ユーザ	IEEE802.1X	Web	12.2.5 (1)(b) ケース⑨	12.2.5 (1)(c)
	固定 VLAN	アクセス トランク	社員ユーザ	IEEE802.1X	Web	12.2.5 (2)(b) ケース⑩	12.2.5 (2)(c)

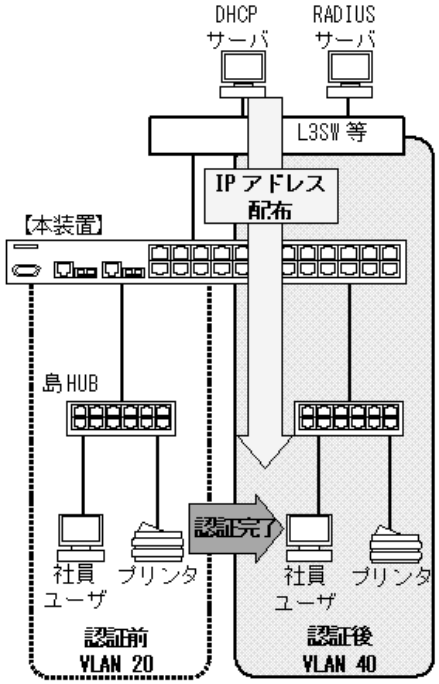
12.2.3　基本マルチステップ認証ポートのコンフィグレーション

（1）ダイナミック VLAN モード

（a）全体構成

基本マルチステップ認証ポートのダイナミック VLAN モードは，社員ユーザとプリンタを同一ポートに接続し，両方とも認証後に IP アドレスの取得を行う構成で説明します。

図 12-7　基本マルチステップ認証の構成例（ダイナミック VLAN モード）

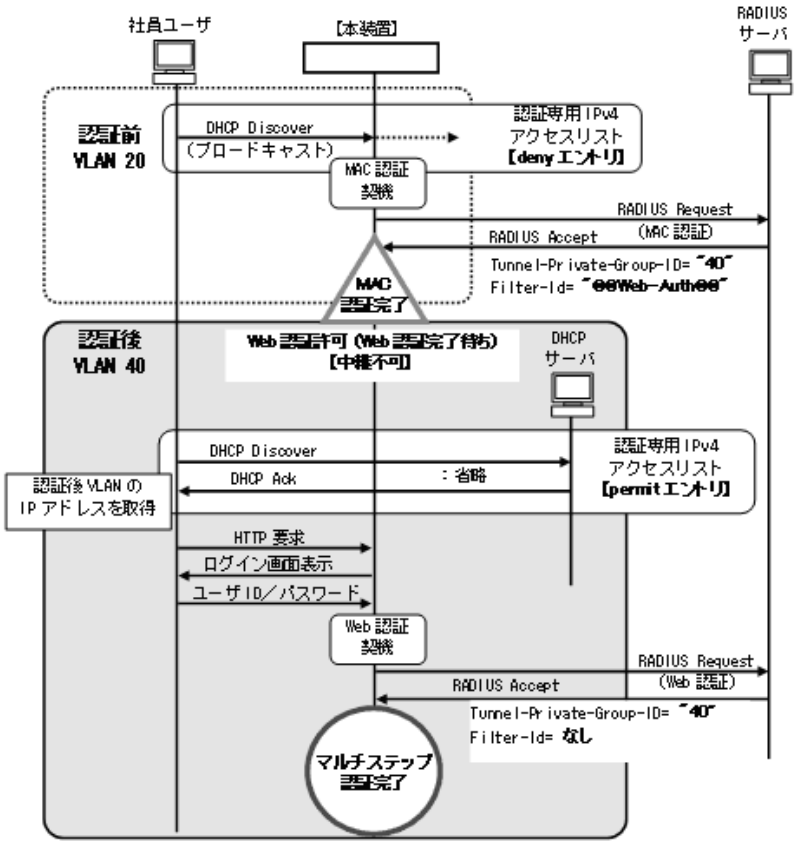


（b）ケース①：社員ユーザの認証と設定のポイント

［認証動作］

基本マルチステップ認証を使用すると，端末認証（MAC 認証）完了時に端末を認証後 VLAN に移動し，VLAN 移動後に認証専用 IPv4 アクセスリストで IP アドレスを取得させます。その後にユーザ認証（Web 認証）を実施することで，ダイナミック VLAN モードでも Web 認証の前後で端末の IP アドレスが変わらない運用が可能です。

図 12-8　社員ユーザの認証動作（ダイナミック VLAN モード）



［設定のポイント］

表 12-22　社員ユーザ認証の設定ポイント（ダイナミック VLAN モード）

設定項目	用途	設定内容		備考
認証専用 IPv4 アクセスリスト	必要	deny	eq bootps vlan 20	認証前 VLAN は DHCP フレームを廃棄※
		permit	eq bootps	全 VLAN で DHCP フレームを中継
本装置内蔵 DHCP サーバ	不要	－		
外部 DHCP サーバ	必要	VLAN 40		認証後 VLAN に配置
RADIUS サーバ	MAC 認証用（社員ユーザ用端末 MAC アドレスの認証）	Tunnel-Private-Group-ID	"40"	認証後 VLAN を応答する設定
		Filter-Id	"@@Web-Auth@@"（または，"/Web-Auth"）	"@@Web-Auth@@"（または，"/Web-Auth"）を応答する設定 端末認証（MAC 認証）が完了しても，VLAN 移動だけで通信不可状態のまま，ユーザ認証（Web 認証）待ちとなります。
	Web 認証用（社員ユーザ ID の認証）	Tunnel-Private-Group-ID	"40"	認証後 VLAN を応答する設定
		Filter-Id	未設定	Filter-Id 無で応答する設定

（凡例）

－：設定不要のためなし

注※

認証前 VLAN では DHCP フレームを認証専用 IPv4 アクセスリストで中継させると，内蔵 DHCP サーバが未設定の場合，認証専用 IPv4 アクセスリストに該当するフレームでは MAC 認証開始契機となりません。このため，IP アドレスを取得し，ARP フレームが送信されるまで MAC 認証が開始されません。

本ケースでは，認証前 VLAN に DHCP サーバを配置しないため，永久に MAC 認証開始契機がなくなってしまいます。

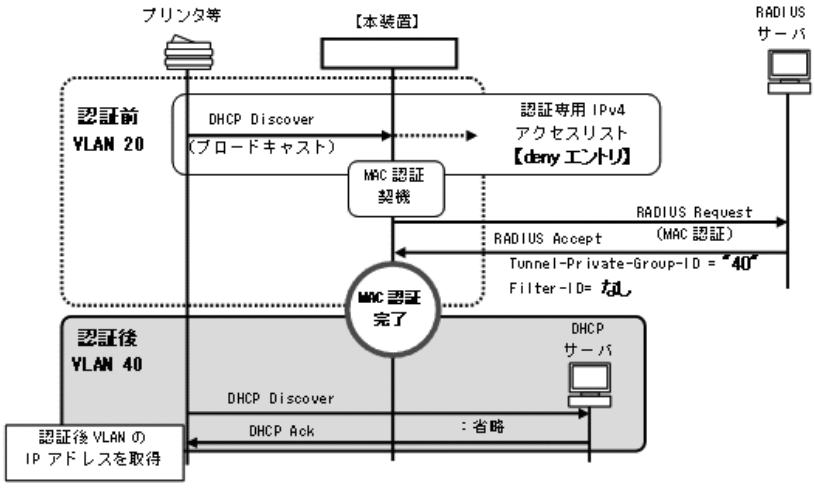
従って，認証前 VLAN でだけ DHCP フレーム廃棄を設定することで，DHCP フレームを MAC 認証開始契機とし，１段目の端末認証を完了します。

(c) ケース②：プリンタの認証と設定のポイント

［認証動作］

社員ユーザと同一ポートにダイナミック VLAN モードで接続されるプリンタがあるときは，以下のシーケンスで認証します。

図 12-9 プリンタの認証動作（ダイナミック VLAN モード）



［設定のポイント］

表 12-23 プリンタ認証の設定ポイント（ダイナミック VLAN モード）

設定項目	用途	設定内容	備考
認証専用 IPv4 アクセスリスト	不要	－	MAC 認証だけの端末としては不要ですが，「社員ユーザ」と同一ポートで運用するケースでは同一の認証専用 IPv4 アクセスリストが適用されます。
本装置内蔵 DHCP サーバ	不要	－	
外部 DHCP サーバ	必要	VLAN 40	認証後 VLAN に配置

設定項目	用途	設定内容		備考
RADIUS サーバ	MAC 認証用（プリンタの MAC アドレスの認証）	Tunnel-Private-Group-ID	"40"	認証後 VLAN を応答する設定
		Filter-Id	未設定	Filter-Id 無で応答する設定 端末認証（MAC 認証）完了時点で通信可能状態となります。
	Web 認証用	－		設定不要

（凡例）
－：設定不要のためなし

（d） ダイナミック VLAN モードでのコンフィグレーション

基本マルチステップ認証ポートで使用するダイナミック VLAN モードのコンフィグレーションについて，以下に説明します。

［設定の項目］

認証対象ポートに以下の項目を設定します。

- 各 VLAN の設定
- 認証方式の設定
- MAC ポートとネイティブ VLAN の設定
- 端末認証（MAC 認証）の設定
- ユーザ認証（Web 認証）の設定
- マルチステップ認証ポートの設定
- 認証専用 IPv4 アクセスリストの設定

なお，認証ポートの認証後 VLAN は，「5.4.3　MAC VLAN の自動 VLAN 割当」により割り当てられるものとします。
その他，Web 認証に必要な設定は「9　Web 認証の設定と運用」，MAC 認証に必要な設定は「11 MAC 認証の設定と運用」を参照してください。

［コマンドによる設定］

1. **(config)# vlan 40 mac-based**
   (config-vlan)# exit
   VLAN ID 40 に MAC VLAN を設定します。（RADIUS サーバから通知される認証後 VLAN と同じ VLAN ID を設定します。）

2. **(config)# vlan 20**
   (config-vlan)# exit
   VLAN ID 20 を設定します。

3. **(config)# aaa authentication mac-authentication default group radius**
   (config)# aaa authentication web-authentication default group radius
   MAC 認証と Web 認証の認証方式に RADIUS 認証を設定します。

4. **(config)# interface gigabitethernet 0/1**
   (config-if)# switchport mode mac-vlan
   (config-if)# switchport mac native vlan 20
   ポート 0/1 を MAC ポートとして設定します。また，MAC ポートのネイティブ VLAN20（認証前

VLAN）を設定します。（認証後 VLAN は「5.4.3　MAC VLAN の自動 VLAN 割当」により割り当てられます。）

5. **(config-if)# web-authentication port**
   (config-if)# mac-authentication port
   (config-if)# authentication multi-step
   ポート 0/1 に Web 認証，MAC 認証，マルチステップ認証（ユーザ認証許可オプション無）を設定します。

6. **(config-if)# authentication ip access-group L2-AUTH**
   (config-if)# authentication arp-relay
   (config-if)# exit
   ポート 0/1 に認証前端末からのフレームに対する認証専用 IPv4 アクセスリストを設定します。また，認証前端末からの ARP フレーム中継を設定します。

7. **(config)# ip access-list extended L2-AUTH**
   (config-ext-nacl)# deny udp any any eq bootps vlan 20
   (config-ext-nacl)# permit udp any any eq bootps
   (config-ext-nacl)# exit
   認証前 VLAN で DHCP フレーム（bootps）を廃棄とし，それ以外の VLAN では DHCP フレームの中継を許可する認証専用 IPv4 アクセスリストを設定します。

[注意事項]

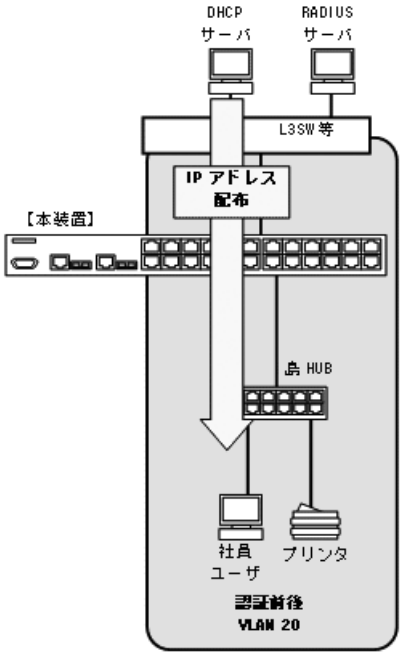
1. 上記設定例のマルチステップ認証のときは，RADIUS サーバ側の RADIUS 属性 Filter-Id に下記を設定してください。
   - MAC 認証で認証する RADIUS サーバ：@@Web-Auth@@（または，/Web-Auth）
2. RADIUS サーバから認証成功（Accept）受信で，RADIUS 属性に認証後 VLAN 情報がないときは，該当 MAC ポートのネイティブ VLAN に端末を収容します。このとき端末は固定 VLAN モードの認証済み端末として扱います。
3. 認証後 VLAN を「5.4.3　MAC VLAN の自動 VLAN 割当」で割り当てるときは，下記を設定してください。
   - コンフィグレーションコマンド vlan mac-based
     RADIUS サーバから通知される VLAN を設定してください。（この場合は，MAC ポートにコンフィグレーションコマンド switchport mac vlan による設定は不要です。）
4. MAC VLAN の自動 VLAN 割当を抑止する場合は，下記を設定してください。
   - コンフィグレーションコマンド no switchport mac auto-vlan
   - コンフィグレーションコマンド switchport mac vlan
     RADIUS サーバから通知される VLAN を設定してください。

（2） 固定 VLAN モード

（a） 全体構成

基本マルチステップ認証ポートの固定 VLAN モードは，社員ユーザとプリンタを同一ポートに接続し，両方とも認証後に IP アドレスの取得を行う構成で説明します。

図 12-10　基本マルチステップ認証の構成例（固定 VLAN モード）



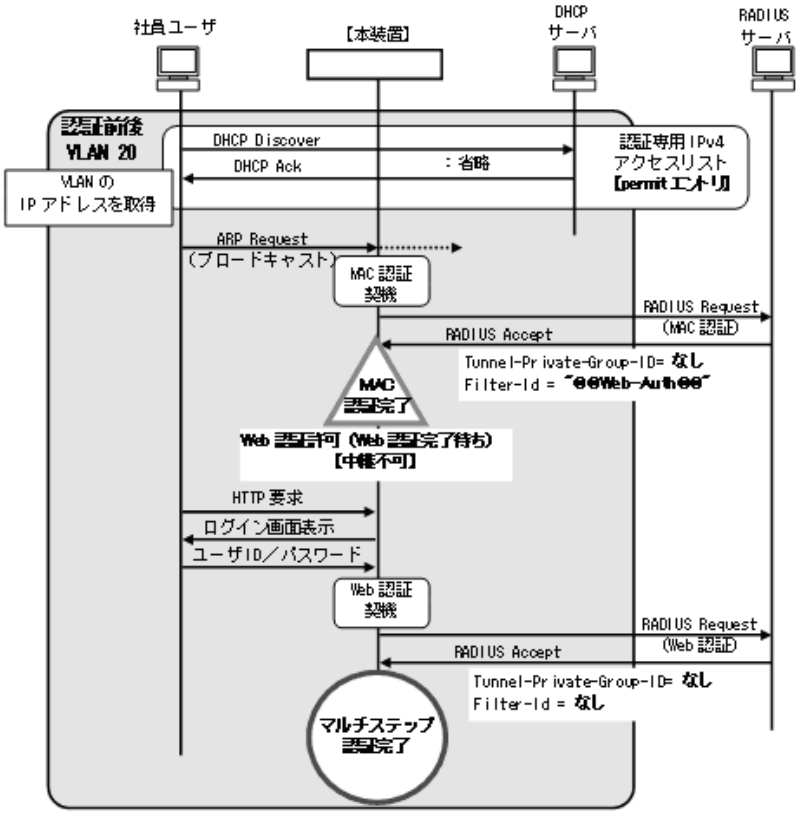
(b) ケース③：社員ユーザの認証と設定のポイント

[認証動作]

基本マルチステップ認証の社員ユーザは，最初に認証専用 IPv4 アクセスリストを通して IP アドレスを取得し，ARP などのフレームで端末認証（MAC 認証）を開始します。

これによりユーザ認証（Web 認証）が可能となり，Web 認証完了後にフルアクセス可能となります。

図 12-11 社員ユーザの認証動作（固定 VLAN モード）



［設定のポイント］

表 12-24 社員ユーザ認証の設定ポイント（固定 VLAN モード）

設定項目	用途	設定内容		備考
認証専用 IPv4 アクセスリスト	必要	permit	eq bootps	全 VLAN で DHCP フレームを中継
本装置内蔵 DHCP サーバ	不要	－		
外部 DHCP サーバ	必要	VLAN 20		認証後 VLAN に配置
RADIUS サーバ	MAC 認証用（社員ユーザ用端末 MAC アドレスの認証）	Tunnel-Private-Group-ID	未設定	Tunnel-Private-Group-ID 無で応答する設定
		Filter-Id	"@@Web-Auth@@"（または，"/Web-Auth"）	"@@Web-Auth@@"（または，"/Web-Auth"）を応答する設定
	Web 認証用（社員ユーザ ID の認証）	Tunnel-Private-Group-ID	未設定	Tunnel-Private-Group-ID 無で応答する設定
		Filter-Id	未設定	Filter-Id 無で応答する設定

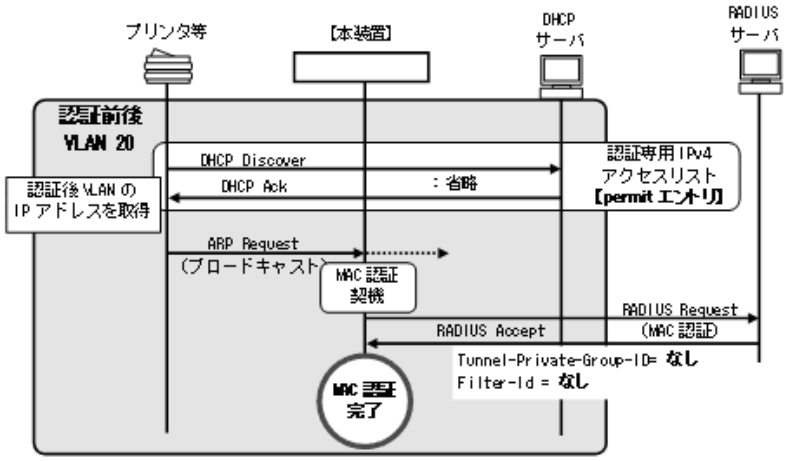
（凡例）
－：設定不要のためなし

(c) ケース④：プリンタの認証と設定のポイント

［認証動作］

社員ユーザと同一ポートに固定 VLAN モードで接続されるプリンタがある場合には，以下のシーケンスで認証されます。

図 12-12　プリンタの認証動作（固定 VLAN モード）



［設定のポイント］

表 12-25　プリンタ認証の設定ポイント（固定 VLAN モード）

設定項目	用途	設定内容		備考
認証専用 IPv4 アクセスリスト	不要	－		MAC 認証だけの端末としては不要ですが，「社員ユーザ」と同一ポートで運用するケースでは同一の認証専用 IPv4 アクセスリストが適用されます。
本装置内蔵 DHCP サーバ	不要	－		
外部 DHCP サーバ	必要	VLAN 20		認証後 VLAN に配置
RADIUS サーバ	MAC 認証用（プリンタの MAC アドレスの認証）	Tunnel-Private-Group-ID	未設定	Tunnel-Private-Group-ID 無で応答する設定
		Filter-Id	未設定	Filter-Id 無で応答する設定 端末認証（MAC 認証）完了時点で通信可能状態となります。
	Web 認証用	－		設定不要

（凡例）

－：設定不要のためなし

(d) 固定 VLAN モードでのコンフィグレーション

基本マルチステップ認証ポートで使用する固定 VLAN モードのコンフィグレーションについて，以下に説明します。

[設定の項目]

認証対象ポートに以下の項目を設定します。

- VLAN の設定
- 認証方式の設定
- アクセスポートと VLAN の設定
- 端末認証（MAC 認証）の設定
- ユーザ認証（Web 認証）の設定
- マルチステップ認証ポートの設定
- 認証専用 IPv4 アクセスリストの設定

その他，Web 認証に必要な設定は「9　Web 認証の設定と運用」，MAC 認証に必要な設定は「11 MAC 認証の設定と運用」を参照してください。

[コマンドによる設定]

1. **(config)# vlan 20**
   (config-vlan)# exit
   認証の前後で通信する VLAN ID 20 を設定します。

2. **(config)# aaa authentication mac-authentication default group radius**
   (config)# aaa authentication web-authentication default group radius
   MAC 認証と Web 認証の認証方式に RADIUS 認証を設定します。

3. **(config)# interface gigabitethernet 0/1**
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 20
   ポート 0/1 をアクセスポートとして設定します。また，アクセスポートに VLAN20 を設定します。

4. **(config-if)# web-authentication port**
   (config-if)# mac-authentication port
   (config-if)# authentication multi-step
   ポート 0/1 に Web 認証，MAC 認証，マルチステップ認証（ユーザ認証許可オプション無）を設定します。

5. **(config-if)# authentication ip access-group L2-AUTH**
   (config-if)# authentication arp-relay
   (config-if)# exit
   ポート 0/1 に認証前端末からのフレームに対する認証専用 IPv4 アクセスリストを設定します。また，認証前端末からの ARP フレーム中継を設定します。

6. **(config)# ip access-list extended L2-AUTH**
   (config-ext-nacl)# permit udp any any eq bootps
   (config-ext-nacl)# exit
   当該ポートでは DHCP フレーム（bootps）の中継を許可する認証専用 IPv4 アクセスリストを設定し

ます。

［注意事項］

1. 上記設定例のマルチステップ認証のときは，RADIUS サーバ側の RADIUS 属性 Filter-Id に下記を設定してください。
   - MAC 認証で認証する RADIUS サーバ：＂@@Web-Auth@@＂（または，＂/Web-Auth＂）

12.2.4　ユーザ認証許可オプションポートのコンフィグレーション

（1） ダイナミック VLAN モード

（a） 全体構成

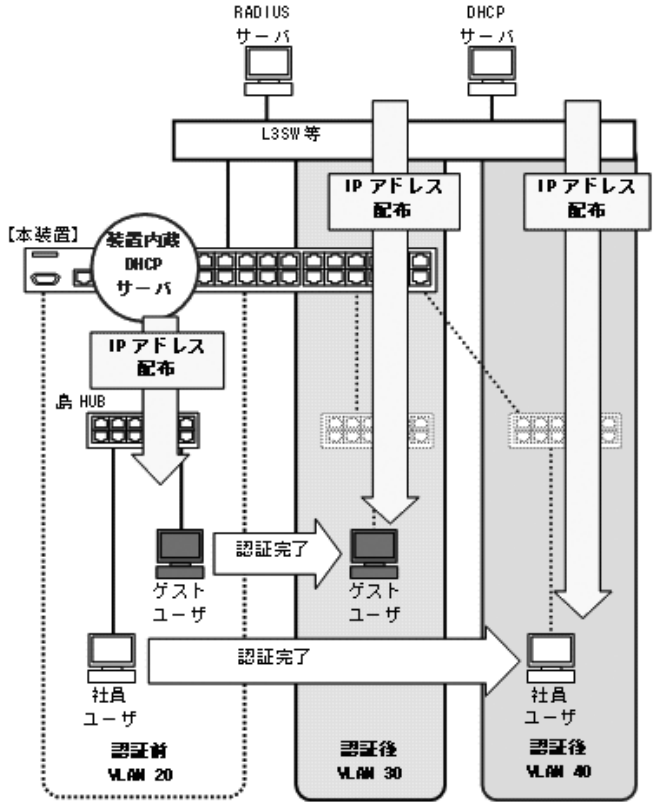
ユーザ認証許可オプションポートのダイナミック VLAN モードでは，ゲストユーザと社員ユーザを同一ポートに接続することができます。

ゲストユーザに対しては，持ち込み端末による Web 認証を許可し，ゲストユーザがアクセス可能な VLAN に収容します。

社員ユーザに対しては，持ち込み端末を許可せず，指定端末を使用した登録ユーザだけがアクセス可能な VLAN に収容します。

両方とも認証前と認証後に別 VLAN で IP アドレスを取得する構成で説明します。

図 12-13　ユーザ認証許可オプションの構成例（ダイナミック VLAN モード）



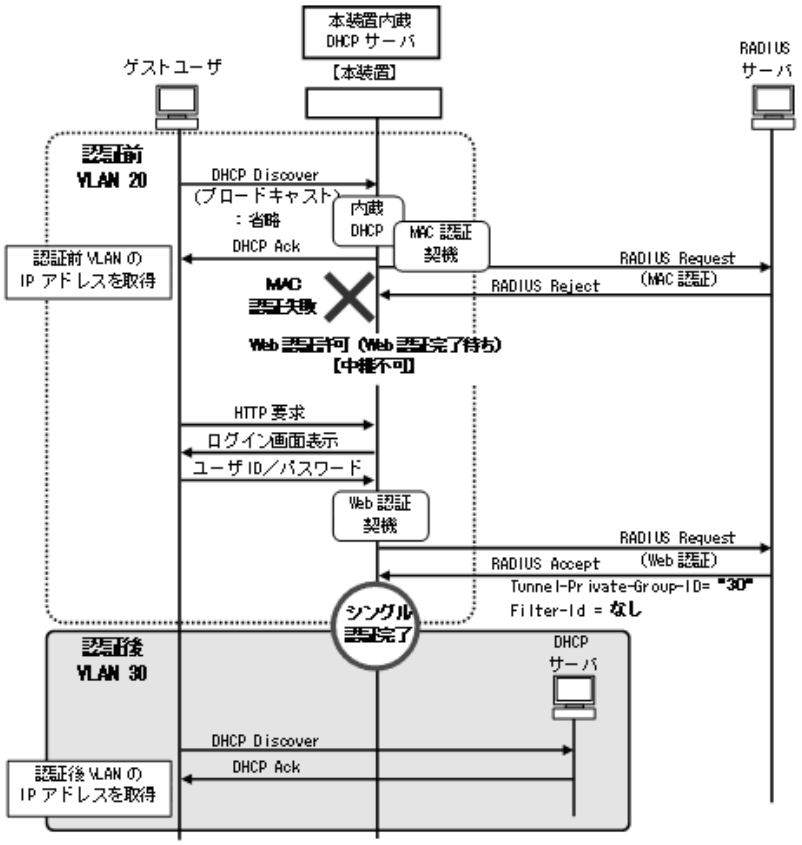
（b） ケース⑤：ゲストユーザの認証と設定のポイント

［認証動作］

ユーザ認証許可オプションは，ゲストユーザと社員ユーザが混在することを想定した機能です。

ゲストユーザは端末認証が失敗するため，ダイナミック VLAN モードのときは端末認証で VLAN を移動できません。従って，認証前 VLAN で IP アドレスを取得する必要があります。認証前 VLAN で IP アドレスを取得させるために，本装置内蔵 DHCP サーバを使用します。
本装置内蔵 DHCP サーバを認証前 VLAN で動作させることで，認証専用 IPv4 アクセスリストで DHCP フレームを中継設定しても，DHCP フレームが MAC 認証開始契機となります。

図 12-14　ゲストユーザの認証動作（ダイナミック VLAN モード）



［設定のポイント］

表 12-26　ゲストユーザ認証の設定ポイント（ダイナミック VLAN モード）

設定項目	用途	設定内容		備考
認証専用 IPv4 アクセスリスト	必要	permit	eq bootps	全 VLAN で DHCP フレームを中継
本装置内蔵 DHCP サーバ	必要	VLAN 20		認証前 VLAN で有効に設定
外部 DHCP サーバ	必要	VLAN 30，40		認証後 VLAN に配置
RADIUS サーバ	MAC 認証用（持ち込み端末の MAC アドレスの認証）	－		拒否：Access-Reject を応答するため設定不要
	Web 認証用（ゲストユーザ ID の認証）	Tunnel-Private-Group-ID	"30"	認証後 VLAN を応答する設定
		Filter-Id	未設定	Filter-Id 無で応答する設定

（凡例）

－：設定不要のためなし

(c) ケース⑥：社員ユーザの認証と設定のポイント

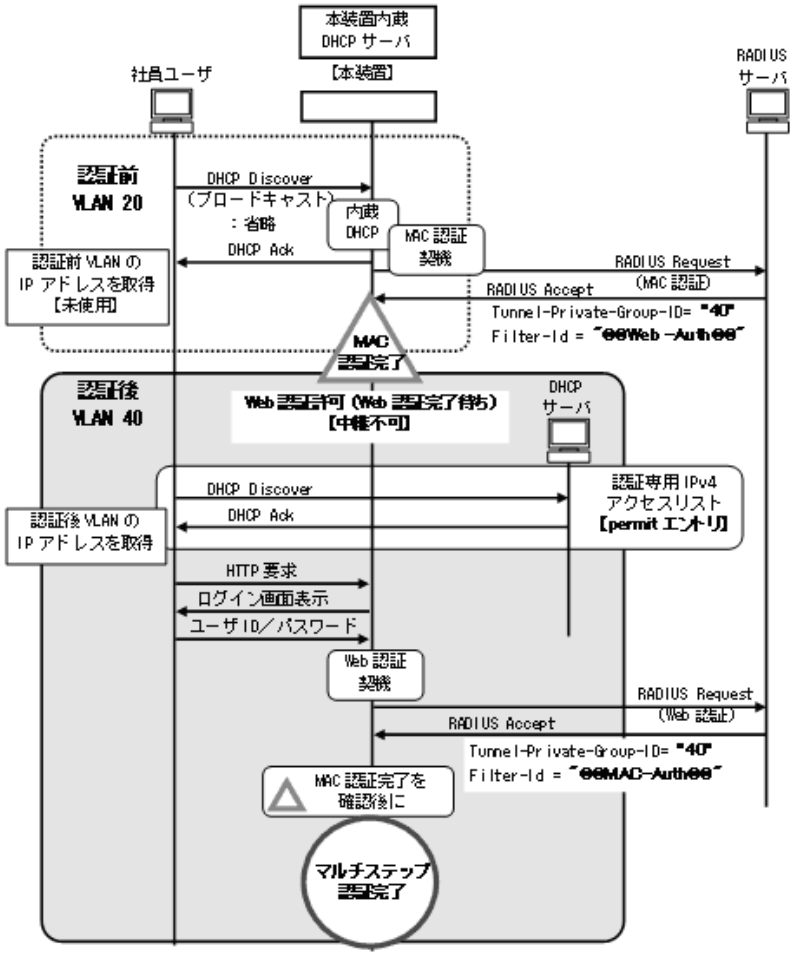
［認証動作］

社員ユーザの認証で端末認証（MAC 認証）が成功したときに VLAN を移動する動作については，基本マルチステップ認証と同様です。本ポートではゲストユーザのために認証前 VLAN で本装置内蔵 DHCP サーバが有効になっています。従って，本ケースでは実際に使用しない認証前 VLAN の IP アドレスを一時的に取得します。

なお，端末認証（MAC 認証）完了時点では VLAN 移動だけが完了しており，認証後 VLAN で外部 DHCP サーバから IP アドレスを取得するため，認証専用 IPv4 アクセスリスト設定が必要となります。

また，社員ユーザに対しては持ち込み端末を不可とするため，Web 認証用の RADIUS サーバに端末認証（MAC 認証）完了が必須であることを設定しおきます。これにより，Web 認証完了後に MAC 認証の成否と合わせて認証完了とします。

図 12-15　社員ユーザの認証動作（ダイナミック VLAN モード）



［設定のポイント］

表 12-27 社員ユーザの設定ポイント（ダイナミック VLAN モード）

設定項目	用途	設定内容		備考
認証専用 IPv4 アクセスリスト	必要	permit	eq bootps	全 VLAN で DHCP フレームを中継
本装置内蔵 DHCP サーバ	不要	－		社員ユーザとしては不要ですが，「ゲストユーザ」のために認証前 VLAN で適用されます。
外部 DHCP サーバ	必要	VLAN 40		認証後 VLAN に配置
RADIUS サーバ	MAC 認証用（社員ユーザ用端末 MAC アドレスの認証）	Tunnel-Private-Group-ID	"40"	認証後 VLAN を応答する設定
		Filter-Id	"@@Web-Auth@@"（または，"/Web-Auth"）	"@@Web-Auth@@"（または，"/Web-Auth"）を応答する設定 端末認証（MAC 認証）が完了しても，VLAN 移動だけで通信不可状態のまま，ユーザ認証（Web 認証）待ちとなります。
	Web 認証用（社員ユーザ ID の認証）	Tunnel-Private-Group-ID	"40"	認証後 VLAN を応答する設定
		Filter-Id	"@@MAC-Auth@@"（または，"/MAC-Auth"）	"@@MAC-Auth@@"（または，"/MAC-Auth"）を応答する設定 端末認証（MAC 認証）が成功しているユーザだけを認証完了とします。

（凡例）
－：設定不要のためなし

（d） ダイナミック VLAN モードでのコンフィグレーション

ユーザ認証許可オプションポートで使用するダイナミック VLAN モードのコンフィグレーションについて，以下に説明します。

［設定の項目］

認証対象ポートに以下の項目を設定します。

- 各 VLAN の設定
- 認証方式の設定
- MAC ポートとネイティブ VLAN の設定
- 端末認証（MAC 認証）の設定
- ユーザ認証（Web 認証）の設定
- マルチステップ認証ポートの設定（ユーザ認証許可オプション有）
- 認証専用 IPv4 アクセスリストの設定
- 本装置内蔵 DHCP サーバの設定

なお，認証ポートの認証後 VLAN は，「5.4.3 MAC VLAN の自動 VLAN 割当」により割り当てられるものとします
その他，Web 認証に必要な設定は「9 Web 認証の設定と運用」，MAC 認証に必要な設定は「11 MAC 認証の設定と運用」を参照してください。

［コマンドによる設定］

1. **(config)# vlan 30 mac-based**
   (config-vlan)# exit
   (config)# vlan 40 mac-based
   (config-vlan)# exit
   VLAN ID 30 と 40 に MAC VLAN を設定します。（RADIUS サーバから通知される認証後 VLAN と同じ VLAN ID を設定します。）

2. **(config)# vlan 20**
   (config-vlan)# exit
   VLAN ID 20 を設定します。

3. **(config)# aaa authentication mac-authentication default group radius**
   (config)# aaa authentication web-authentication default group radius
   MAC 認証と Web 認証の認証方式に RADIUS 認証を設定します。

4. **(config)# interface gigabitethernet 0/1**
   (config-if)# switchport mode mac-vlan
   (config-if)# switchport mac native vlan 20
   ポート 0/1 を MAC ポートとして設定します。また，MAC ポートのネイティブ VLAN20（認証前 VLAN）を設定します。（認証後 VLAN は「5.4.3　MAC VLAN の自動 VLAN 割当」により割り当てられます。）

5. **(config-if)# web-authentication port**
   (config-if)# mac-authentication port
   (config-if)# authentication multi-step permissive
   ポート 0/1 に Web 認証，MAC 認証，マルチステップ認証（ユーザ認証許可オプション有）を設定します。

6. **(config-if)# authentication ip access-group L2-AUTH**
   (config-if)# authentication arp-relay
   (config-if)# exit
   ポート 0/1 に認証前端末からのフレームに対する認証専用 IPv4 アクセスリストを設定します。また，認証前端末からの ARP フレーム中継を設定します。

7. **(config)# ip access-list extended L2-AUTH**
   (config-ext-nacl)# permit udp any any eq bootps
   (config-ext-nacl)# exit
   認証前端末からの DHCP フレーム（bootps）の中継を許可する認証専用 IPv4 アクセスリストを設定します。

8. **(config)# interface vlan 20**
   (config-if)# ip address 192.168.20.254 255.255.255.0
   (config-if)# exit
   (config)# service dhcp vlan 20
   (config)# ip dhcp pool NativeVLAN

```
(dhcp-config)# network 192.168.20.0/24
(dhcp-config)# exit
```

認証前 VLAN に IP アドレスを設定します。さらに認証前 VLAN20 で本装置内蔵 DHCP サーバを有効します。

［注意事項］

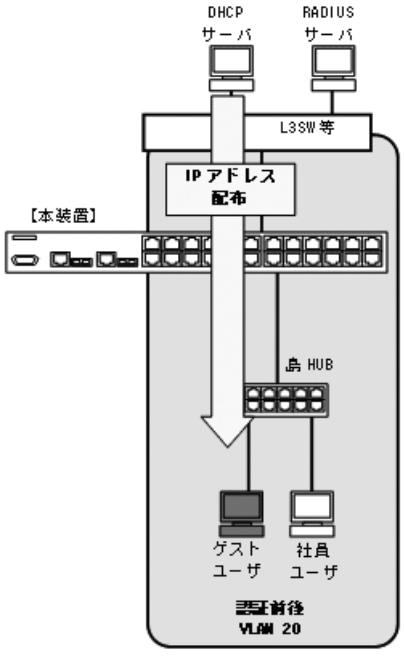
1. 上記設定例のマルチステップ認証のときは，RADIUS サーバ側の RADIUS 属性 Filter-Id に下記を設定してください。
   - MAC 認証で認証する RADIUS サーバ："@@Web-Auth@@"（または，"/Web-Auth"）
   - Web 認証で認証する RADIUS サーバ："@@MAC-Auth@@"（または，"/MAC-Auth"）
2. RADIUS サーバから認証成功（Accept）受信で，RADIUS 属性に認証後 VLAN 情報がないときは，該当 MAC ポートのネイティブ VLAN に端末を収容します。このとき端末は固定 VLAN モードの認証済み端末として扱います。
3. 認証後 VLAN を「5.4.3　MAC VLAN の自動 VLAN 割当」で割り当てるときは，下記を設定してください。
   - コンフィグレーションコマンド vlan mac-based
     RADIUS サーバから通知される VLAN を設定してください。（この場合は，MAC ポートにコンフィグレーションコマンド switchport mac vlan による設定は不要です。）
4. MAC VLAN の自動 VLAN 割当を抑止する場合は，下記を設定してください。
   - コンフィグレーションコマンド no switchport mac auto-vlan
   - コンフィグレーションコマンド switchport mac vlan
     RADIUS サーバから通知される VLAN を設定してください。

（2） 固定 VLAN モード

（a） 全体構成

ユーザ認証許可オプションポートの固定 VLAN モードでは，ゲストユーザと社員ユーザを同一ポートに接続し，両方とも認証前に IP アドレスを取得する構成で説明します。

図 12-16　ユーザ認証許可オプションの構成例（固定 VLAN モード）



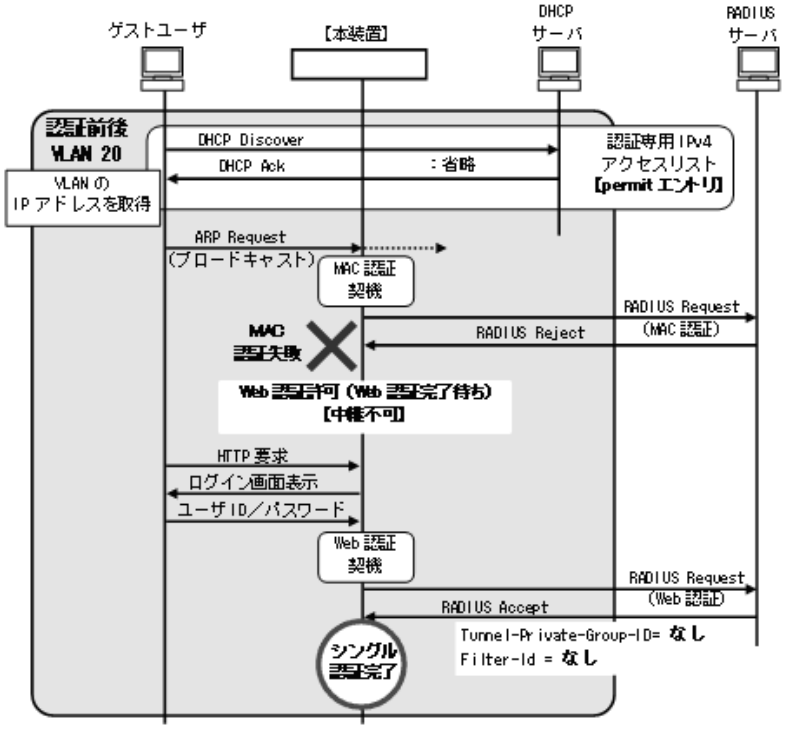
(b) ケース⑦：ゲストユーザの認証と設定のポイント

［認証動作］

ユーザ認証許可オプションポートのゲストユーザは，最初に認証専用 IPv4 アクセスリストを通して IP アドレスを取得し，ARP などのフレームで端末認証（MAC 認証）を開始します。ただし，持ち込み端末で未登録の MAC アドレスのため，MAC 認証は失敗します。

ユーザ認証許可オプションポートでは，端末認証（MAC 認証）が失敗してもユーザ認証（Web 認証）の実行を許可する機能のため，Web 認証が可能となります。Web 認証完了後にゲストユーザはフルアクセス可能となります。

図 12-17　ゲストユーザの認証動作（固定 VLAN モード）



［設定のポイント］

表 12-28　ゲストユーザ認証の設定ポイント（固定 VLAN モード）

設定項目	用途	設定内容		備考
認証専用 IPv4 アクセスリスト	必要	permit	eq bootps	全 VLAN で DHCP フレームを中継
本装置内蔵 DHCP サーバ	不要	－		
外部 DHCP サーバ	必要	VLAN 20		認証後 VLAN に配置

設定項目	用途	設定内容		備考
RADIUS サーバ	MAC 認証用（持ち込み端末の MAC アドレスの認証）	－		拒否：Access-Reject を応答するため設定不要
	Web 認証用（ゲストユーザ ID の認証）	Tunnel-Private-Group-ID	未設定	Tunnel-Private-Group-ID 無で応答する設定
		Filter-Id	未設定	Filter-Id 無で応答する設定 端末認証（MAC 認証）結果に依存せずに認証が完了します。

（凡例）

－：設定不要のためなし

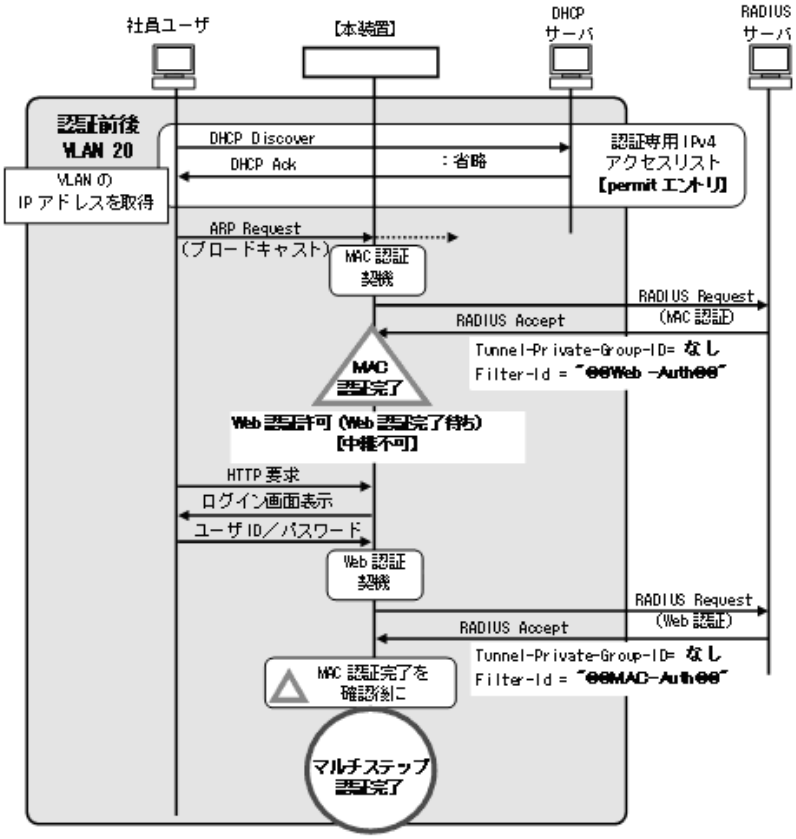
(c) ケース⑧：社員ユーザの認証と設定のポイント

［認証動作］

ユーザ認証許可オプションポートの社員ユーザは，最初に認証専用 IPv4 アクセスリストを通して IP アドレスを取得し，ARP などのフレームで端末認証（MAC 認証）を開始します。

これにより Web 認証が可能となり，Web 認証完了後にフルアクセス可能となります。

図 12-18　社員ユーザの認証動作（固定 VLAN モード）



［設定のポイント］

表 12-29　社員ユーザ認証の設定ポイント（固定 VLAN モード）

設定項目	用途	設定内容		備考
認証専用 IPv4 アクセスリスト	必要	permit	eq bootps	全 VLAN で DHCP フレームを中継
本装置内蔵 DHCP サーバ	不要	－		
外部 DHCP サーバ	必要	VLAN 20		認証後 VLAN に配置
RADIUS サーバ	MAC 認証用（社員ユーザ用端末 MAC アドレスの認証）	Tunnel-Private-Group-ID	未設定	Tunnel-Private-Group-ID 無で応答する設定
		Filter-Id	"@@Web-Auth@@"（または，"/Web-Auth"）	"@@Web-Auth@@"（または，"/Web-Auth"）を応答する設定 端末認証（MAC 認証）が完了しても通信不可状態のまま，ユーザ認証待ちとなります。
	Web 認証用（社員ユーザ ID の認証）	Tunnel-Private-Group-ID	未設定	Tunnel-Private-Group-ID 無で応答する設定
		Filter-Id	"@@MAC-Auth@@"（または，"/MAC-Auth"）	"@@MAC-Auth@@"（または，"/MAC-Auth"）を応答する設定 端末認証（MAC 認証）が成功しているユーザだけを認証完了とします。

（凡例）
－：設定不要のためなし

（d）固定 VLAN モードでのコンフィグレーション

ユーザ認証許可オプションポートで使用する固定 VLAN モードのコンフィグレーションについて，以下に説明します。

［設定の項目］

認証対象ポートに以下の項目を設定します。

- VLAN の設定
- 認証方式の設定
- アクセスポートと VLAN の設定
- 端末認証（MAC 認証）の設定
- ユーザ認証（Web 認証）の設定
- マルチステップ認証ポートの設定（ユーザ認証許可オプション有）
- 認証専用 IPv4 アクセスリストの設定

その他，Web 認証に必要な設定は「9　Web 認証の設定と運用」，MAC 認証に必要な設定は「11　MAC 認証の設定と運用」を参照してください。

［コマンドによる設定］

1. **(config)# vlan 20**
   (config-vlan)# exit
   認証の前後で通信する VLAN ID 20 を設定します。

2. **(config)# aaa authentication mac-authentication default group radius**
   (config)# aaa authentication web-authentication default group radius

MAC 認証と Web 認証の認証方式に RADIUS 認証を設定します。

3. **(config)# interface gigabitethernet 0/1**
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 20
   ポート 0/1 をアクセスポートとして設定します。また，アクセスポートに VLAN20 を設定します。

4. **(config-if)# web-authentication port**
   (config-if)# mac-authentication port
   (config-if)# authentication multi-step permissive
   ポート 0/1 に Web 認証，MAC 認証，マルチステップ認証（ユーザ認証許可オプション有）を設定します。

5. **(config-if)# authentication ip access-group L2-AUTH**
   (config-if)# authentication arp-relay
   (config-if)# exit
   ポート 0/1 に認証前端末からのフレームに対する認証専用 IPv4 アクセスリストを設定します。また，認証前端末からの ARP フレーム中継を設定します。

6. **(config)# ip access-list extended L2-AUTH**
   (config-ext-nacl)# permit udp any any eq bootps
   (config-ext-nacl)# exit
   認証前端末からの DHCP フレーム（bootps）の中継を許可する認証専用 IPv4 アクセスリストを設定します。

[注意事項]

1. 上記設定例のマルチステップ認証のときは，RADIUS サーバ側の RADIUS 属性 Filter-Id に下記を設定してください。
   - MAC 認証で認証する RADIUS サーバ："@@Web-Auth@@"（または，"/Web-Auth"）
   - Web 認証で認証する RADIUS サーバ："@@MAC-Auth@@"（または，"/MAC-Auth"）

12.2.5 端末認証 dot1x オプションポートのコンフィグレーション

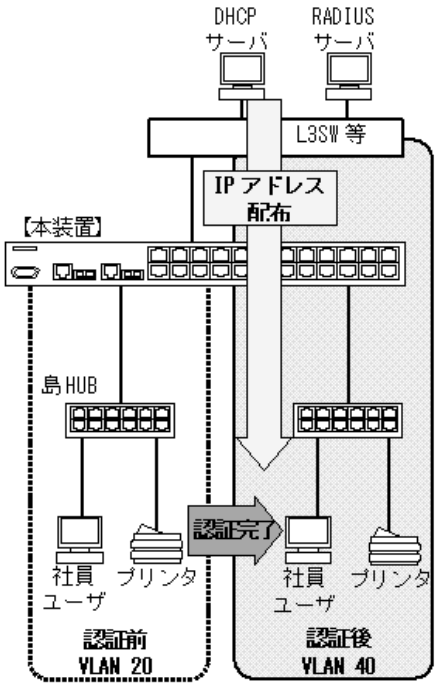
(1) ダイナミック VLAN モード

(a) 全体構成

端末認証 dot1x オプションポートのダイナミック VLAN モードは，社員ユーザとプリンタを同一ポートに接続し，両方とも認証後に IP アドレスの取得を行う構成で説明します。

プリンタの認証動作については，基本マルチステップ認証ポートと同様です。「12.2.3 基本マルチステップ認証ポートのコンフィグレーション」を参照してください。

図 12-19 端末認証 dot1x オプションの構成例（ダイナミック VLAN モード）

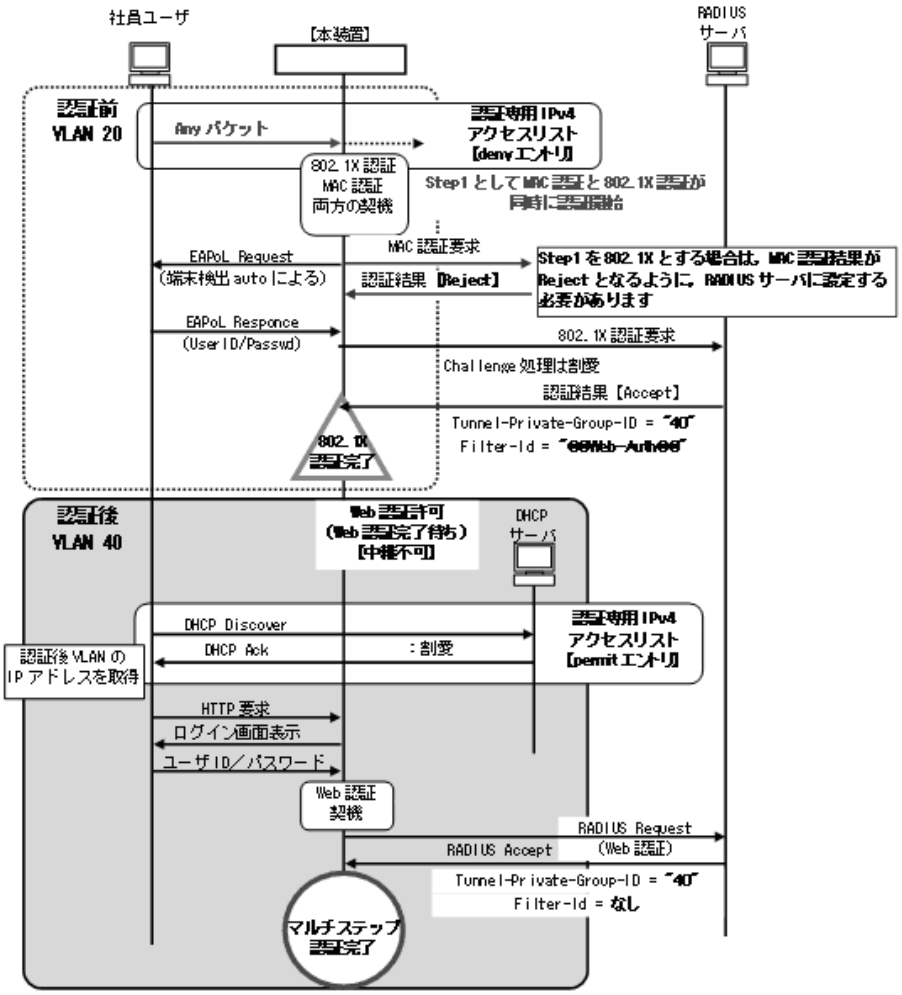


(b) ケース⑨：社員ユーザの認証と設定のポイント

[認証動作]

端末認証 dot1x オプションを使用すると，端末認証（IEEE802.1X）完了時に端末を認証後 VLAN に移動し，VLAN 移動後に認証専用 IPv4 アクセスリストで IP アドレスを取得させます。その後にユーザ認証（Web 認証）を実施することで，ダイナミック VLAN モードでも Web 認証の前後で端末の IP アドレスが変わらない運用が可能です。

図 12-20 社員ユーザの認証動作（ダイナミック VLAN モード）



［設定のポイント］

表 12-30 社員ユーザ認証の設定ポイント（ダイナミック VLAN モード）

設定項目	用途	設定内容		備考
認証専用 IPv4 アクセスリスト	必要	deny	eq bootps vlan 20	認証前 VLAN は DHCP フレームを廃棄※
		permit	eq bootps	全 VLAN で DHCP フレームを中継
本装置内蔵 DHCP サーバ	不要	－		
外部 DHCP サーバ	必要	VLAN 40		認証後 VLAN に配置
RADIUS サーバ	IEEE802.1X 用（社員ユーザ用端末 MAC アドレスの認証）	Tunnel-Private-Group-ID	"40"	認証後 VLAN を応答する設定
		Filter-Id	"@@Web-Auth@@"（または，"/Web-Auth"）	"@@Web-Auth@@"（または，"/Web-Auth"）を応答する設定 端末認証（IEEE802.1X）が完了しても，VLAN 移動だけで通信不可状態のまま，ユーザ認証（Web 認証）待ちとなります。

設定項目	用途	設定内容		備考
	Web 認証用（社員ユーザ ID の認証）	Tunnel-Private-Group-ID	"40"	認証後 VLAN を応答する設定
		Filter-Id	未設定	Filter-Id 無で応答する設定

（凡例）

－：設定不要のためなし

注 ※

認証前 VLAN では DHCP フレームを認証専用 IPv4 アクセスリストで中継させると，内蔵 DHCP サーバが未設定の場合，認証専用 IPv4 アクセスリストに該当するフレームでは MAC 認証開始契機となりません。このため，IP アドレスを取得し，ARP フレームが送信されるまで MAC 認証が開始されません。

本ケースでは，認証前 VLAN に DHCP サーバを配置しないため，永久に MAC 認証開始契機がなくなってしまいます。

従って，認証前 VLAN でだけ DHCP フレーム廃棄を設定することで，DHCP フレームを MAC 認証開始契機とし，１段目の端末認証を完了します。

(c) ダイナミック VLAN モードでのコンフィグレーション

端末認証 dot1x オプションポートで使用するダイナミック VLAN モードのコンフィグレーションについて，以下に説明します。

IEEE802.1X と Web 認証は社員ユーザ認証用，MAC 認証はプリンタ認証用に設定します。

[設定の項目]

認証対象ポートに以下の項目を設定します。

- 各 VLAN の設定
- 認証方式の設定
- MAC ポートとネイティブ VLAN の設定
- 端末認証（IEEE802.1X）の設定
- ユーザ認証（Web 認証）の設定
- 端末認証（MAC 認証）の設定
- マルチステップ認証ポートの設定（端末認証 dot1x オプション有）
- 認証専用 IPv4 アクセスリストの設定

なお，認証ポートの認証後 VLAN は，「5.4.3　MAC VLAN の自動 VLAN 割当」により割り当てられるものとします。

その他，IEEE802.1X に必要な設定は「7　IEEE802.1X の設定と運用」，Web 認証に必要な設定は「9　Web 認証の設定と運用」，MAC 認証に必要な設定は「11　MAC 認証の設定と運用」を参照してください。

[コマンドによる設定]

1. **(config)# vlan 40 mac-based**
   (config-vlan)# exit
   VLAN ID 40 に MAC VLAN を設定します。（RADIUS サーバから通知される認証後 VLAN と同じ VLAN ID を設定します。）

2. **(config)# vlan 20**
   (config-vlan)# exit
   VLAN ID 20 を設定します。

3. **(config)# aaa authentication dot1x default group radius**
   (config)# aaa authentication web-authentication default group radius
   (config)# aaa authentication mac-authentication default group radius
   IEEE802.1X と Web 認証，および MAC 認証の認証方式に RADIUS 認証を設定します。

4. **(config)# interface gigabitethernet 0/1**
   (config-if)# switchport mode mac-vlan
   (config-if)# switchport mac native vlan 20
   ポート 0/1 を MAC ポートとして設定します。また，MAC ポートのネイティブ VLAN20（認証前 VLAN）を設定します。（認証後 VLAN は「5.4.3　MAC VLAN の自動 VLAN 割当」により割り当てられます。）

5. **(config-if)# dot1x port-control auto**
   (config-if)# dot1x multiple-authentication
   (config-if)# dot1x supplicant-detection auto
   (config-if)# web-authentication port
   (config-if)# mac-authentication port
   (config-if)# authentication multi-step dot1x
   ポート 0/1 に IEEE802.1X，Web 認証，MAC 認証，マルチステップ認証（端末認証 dot1x オプション有）を設定します。

6. **(config-if)# authentication ip access-group L2-AUTH**
   (config-if)# authentication arp-relay
   (config-if)# exit
   ポート 0/1 に認証前端末からのフレームに対する認証専用 IPv4 アクセスリストを設定します。また，認証前端末からの ARP フレーム中継を設定します。

7. **(config)# ip access-list extended L2-AUTH**
   (config-ext-nacl)# deny udp any any eq bootps vlan 20
   (config-ext-nacl)# permit udp any any eq bootps
   (config-ext-nacl)# exit
   認証前 VLAN で DHCP フレーム（bootps）を廃棄とし，それ以外の VLAN では DHCP フレームの中継を許可する認証専用 IPv4 アクセスリストを設定します。

[注意事項]

1. 上記設定例のマルチステップ認証のときは，RADIUS サーバ側の RADIUS 属性 Filter-Id に下記を設定してください。
   - IEEE802.1X で認証する RADIUS サーバ："@@Web-Auth@@"（または，"/Web-Auth"）

   また，上記設定例の場合は，端末認証として MAC 認証と IEEE802.1X が同時に動作します。社員ユーザを IEEE802.1X で認証する場合は，RADIUS サーバに当該端末を MAC 認証対象として登録しないなど，MAC 認証が失敗するようにしてください。
2. RADIUS サーバから認証成功（Accept）受信で，RADIUS 属性に認証後 VLAN 情報がないときは，該当 MAC ポートのネイティブ VLAN に端末を収容します。このとき端末は固定 VLAN モードの認証済み端末として扱います。
3. 認証後 VLAN を「5.4.3　MAC VLAN の自動 VLAN 割当」で割り当てるときは，下記を設定してください。

- コンフィグレーションコマンド vlan mac-based
  RADIUS サーバから通知される VLAN を設定してください。（この場合は，MAC ポートにコンフィグレーションコマンド switchport mac vlan による設定は不要です。）

4. MAC VLAN の自動 VLAN 割当を抑止する場合は，下記を設定してください。
   - コンフィグレーションコマンド no switchport mac auto-vlan
   - コンフィグレーションコマンド switchport mac vlan
     RADIUS サーバから通知される VLAN を設定してください。

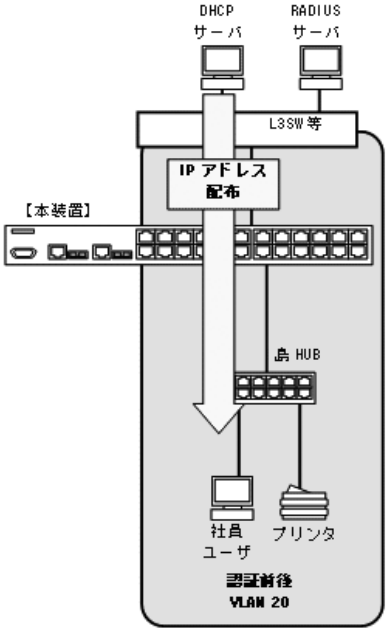
（2） 固定 VLAN モード

（a） 全体構成

端末認証 dot1x オプションポートの固定 VLAN モードは，社員ユーザとプリンタを同一ポートに接続し，両方とも認証後に IP アドレスの取得を行う構成で説明します。

プリンタの認証動作については，基本マルチステップ認証ポートと同様です。「12.2.3　基本マルチステップ認証ポートのコンフィグレーション」を参照してください。

図 12-21　端末認証 dot1x オプションの構成例（固定 VLAN モード）

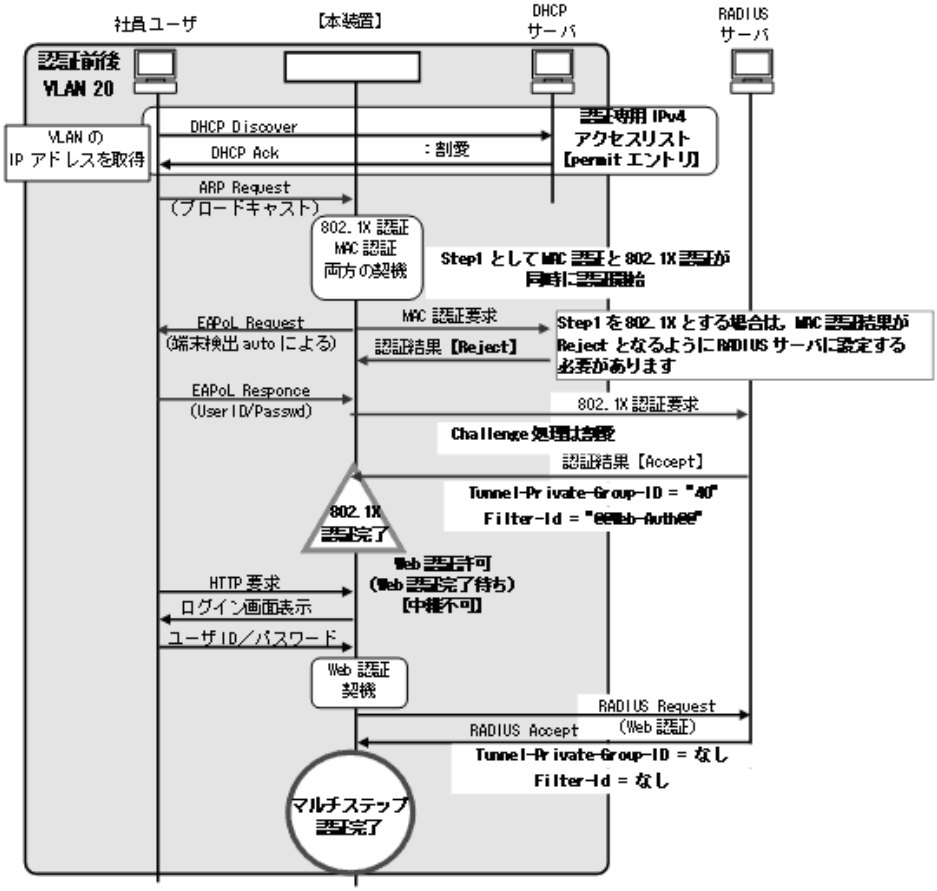


（b） ケース⑩：社員ユーザの認証と設定のポイント

［認証動作］

端末認証 dot1x オプションの社員ユーザは，最初に認証専用 IPv4 アクセスリストを通して IP アドレスを取得し，ARP などのフレームで端末認証（IEEE802.1X）を開始します。これによりユーザ認証（Web 認証）が可能となり，Web 認証完了後にフルアクセス可能となります。

図 12-22 社員ユーザの認証動作（固定 VLAN モード）



［設定のポイント］

表 12-31 社員ユーザ認証の設定ポイント（固定 VLAN モード）

設定項目	用途	設定内容		備考
認証専用 IPv4 アクセスリスト	必要	permit	eq bootps	全 VLAN で DHCP フレームを中継
本装置内蔵 DHCP サーバ	不要	－		
外部 DHCP サーバ	必要	VLAN 20		認証後 VLAN に配置
RADIUS サーバ	IEEE802.1X 用（社員ユーザ用端末 MAC アドレスの認証）	Tunnel-Private-Group-ID	未設定	Tunnel-Private-Group-ID 無で応答する設定
		Filter-Id	"@@Web-Auth@@"（または，"/Web-Auth"）	"@@Web-Auth@@"（または，"/Web-Auth"）を応答する設定
	Web 認証用（社員ユーザ ID の認証）	Tunnel-Private-Group-ID	未設定	Tunnel-Private-Group-ID 無で応答する設定
		Filter-Id	未設定	Filter-Id 無で応答する設定

（凡例）

－：設定不要のためなし

(c) 固定 VLAN モードでのコンフィグレーション

端末認証 dot1x オプションポートで使用する固定 VLAN モードのコンフィグレーションについて，以下に説明します。

IEEE802.1X と Web 認証は社員ユーザ認証用，MAC 認証はプリンタ認証用に設定します。

[設定の項目]

認証対象ポートに以下の項目を設定します。

- VLAN の設定
- 認証方式の設定
- アクセスポートと VLAN の設定
- 端末認証（IEEE802.1X）の設定
- ユーザ認証（Web 認証）の設定
- 端末認証（MAC 認証）の設定
- マルチステップ認証ポートの設定（端末認証 dot1x オプション有）
- 認証専用 IPv4 アクセスリストの設定

その他，IEEE802.1X に必要な設定は「7　IEEE802.1X の設定と運用」，Web 認証に必要な設定は「9　Web 認証の設定と運用」，MAC 認証に必要な設定は「11　MAC 認証の設定と運用」を参照してください。

[コマンドによる設定]

1. **(config)# vlan 20**
   (config-vlan)# exit
   認証の前後で通信する VLAN ID 20 を設定します。

2. **(config)# aaa authentication dot1x default group radius**
   (config)# aaa authentication web-authentication default group radius
   (config)# aaa authentication mac-authentication default group radius
   IEEE802.1X と Web 認証，および MAC 認証の認証方式に RADIUS 認証を設定します。

3. **(config)# interface gigabitethernet 0/1**
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 20
   ポート 0/1 をアクセスポートとして設定します。また，アクセスポートに VLAN20 を設定します。

4. **(config-if)# dot1x port-control auto**
   (config-if)# dot1x multiple-authentication
   (config-if)# dot1x supplicant-detection auto
   (config-if)# web-authentication port
   (config-if)# mac-authentication port
   (config-if)# authentication multi-step dot1x
   ポート 0/1 に IEEE802.1X，Web 認証，MAC 認証，マルチステップ認証（端末認証 dot1x オプション有）を設定します。

5. **(config-if)# authentication ip access-group L2-AUTH**
   (config-if)# authentication arp-relay
   (config-if)# exit

ポート 0/1 に認証前端末からのフレームに対する認証専用 IPv4 アクセスリストを設定します。また，認証前端末からの ARP フレーム中継を設定します。

6. **(config)# ip access-list extended L2-AUTH**
   (config-ext-nacl)# permit udp any any eq bootps
   (config-ext-nacl)# exit
   当該ポートでは DHCP フレーム（bootps）の中継を許可する認証専用 IPv4 アクセスリストを設定します。

［注意事項］

1. 上記設定例のマルチステップ認証のときは，RADIUS サーバ側の RADIUS 属性 Filter-Id に下記を設定してください。
   • IEEE802.1X で認証する RADIUS サーバ："@@Web-Auth@@"（または，"/Web-Auth"）
   また，上記設定例の場合は，端末認証として MAC 認証と IEEE802.1X が同時に動作します。社員ユーザを IEEE802.1X で認証する場合は，RADIUS サーバに当該端末を MAC 認証対象として登録しないなど，MAC 認証が失敗するようにしてください。

12.3　オペレーション

12.3.1　運用コマンド一覧

マルチステップ認証の運用コマンド一覧を次の表に示します。

表 12-32　マルチステップ認証の運用コマンド一覧

コマンド名	説明
show authentication multi-step	マルチステップ認証ポートの認証端末情報を，インタフェースごとに表示します。
show authentication logging	各レイヤ 2 認証が採取している動作ログメッセージを，最新の採取時刻から表示します。

12.3.2　マルチステップ認証の認証状態の表示

本装置ではマルチステップ認証ポートの認証端末情報を，運用コマンド show authentication multi-step で表示します。

図 12-23　show authentication multi-step の実行例

```
# show authentication multi-step

Date 20XX/05/20 11:36:36 UTC
Port 0/8  : multi-step permissive
     <     Supplicant information     >  <Authentic method>
  No MAC address    State VLAN F Type   class  Last  (first step)
   1 0025.64c2.4725 pass   200   multi     60  web   (mac)

Port 0/10 : multi-step permissive
     <     Supplicant information     >  <Authentic method>
  No MAC address    State VLAN F Type   class  Last  (first step)
   1 000a.e460.af52 pass   200   single    24  mac   (-)

#
```

13 DHCP snooping

この章では，DHCP snooping の解説と操作方法について説明します。

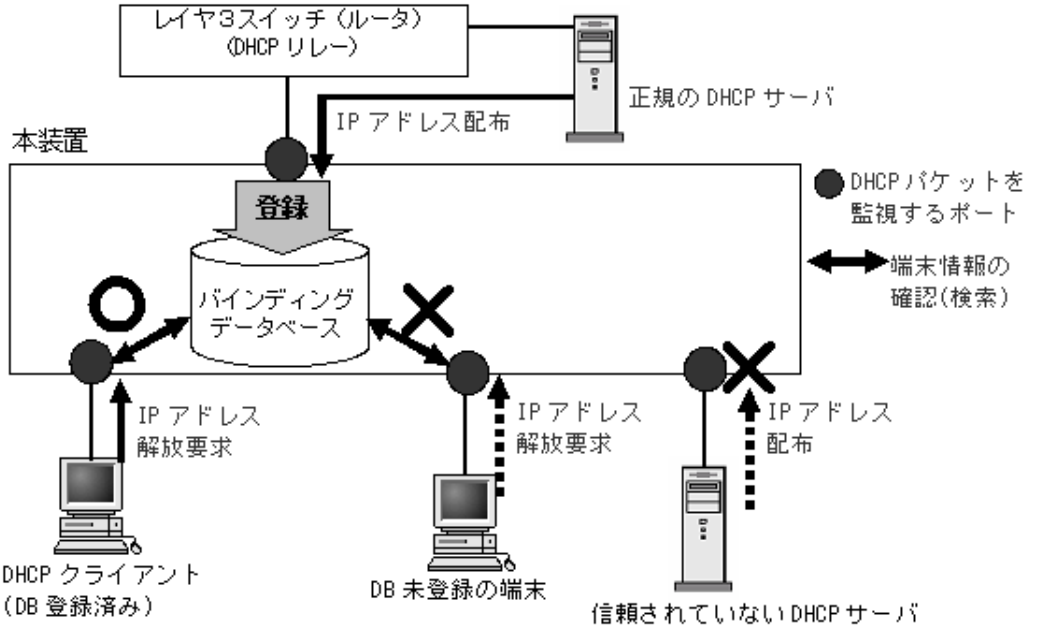
13.1　DHCP snooping 機能の解説

DHCP snooping は，本装置を通過する DHCP パケットを監視して，信頼されていない端末からのアクセスを制限する機能です。

- DHCP サーバから IP アドレスを配布されたクライアントと固定 IP アドレス端末を，バインディングデータベースに登録して管理します。
- 信頼されていない端末（バインディングデータベース未登録の端末のこと。以下，DB 未登録の端末と表記）からの，IP アドレス解放要求を抑止します。
- 信頼されていない DHCP サーバからの IP アドレス配布を抑止します。

DHCP snooping は，次の図に示すように DHCP サーバと DHCP クライアントの間に本装置を接続して使用します。

図 13-1　DHCP snooping 概要



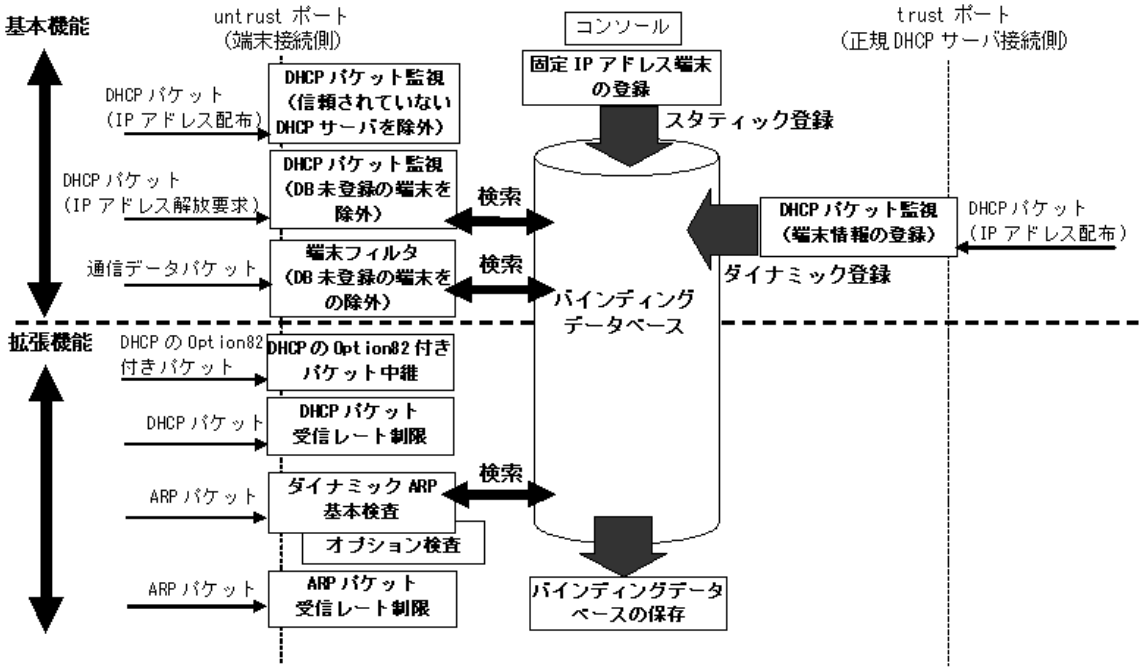
また，DB 未登録の端末からの IPv4 パケットをすべて廃棄する，端末フィルタ機能をサポートしています。

DHCP snooping は，上記のほかに拡張機能として下記をサポートしています。

- DHCP の Option82 付きパケットの中継
- DHCP パケットの受信レート制限
- ダイナミック ARP 検査機能
- バインディングデータベースの保存

各機能とバインディングデータベースの動作関係を次の図に示します。

図 13-2　各機能とバインディングデータベースの動作関係図



各機能の詳細説明や設定説明は下記を参照してください。

表 13-1　DHCP snooping のサポート機能

機能	項目	機能説明参照先	設定説明参照先
基本	DHCP パケットの監視	「13.1.1」参照	「13.2.3」参照
	端末フィルタ	「13.1.2」参照	「13.2.3」参照
	固定 IP アドレス端末の通信許可	「13.1.2」参照	「13.2.3」参照
拡張	DHCP の Option82 付きパケットの中継	「13.1.3」参照	「13.2.4」参照
	DHCP パケットの受信レート制限	「13.1.5」参照	「13.2.5」参照
	ダイナミック ARP 検査機能		
	基本検査	「13.1.6」参照	「13.2.6」参照
	オプション検査	「13.1.6」参照	「13.2.6」参照
	ARP パケットの受信レート制限	「13.1.6」参照	「13.2.6」参照
	バインディングデータベースの保存		
	書き込み指定時間満了時の保存	「13.1.7」参照	「13.2.7」参照
	特定オペレーションによる保存	「13.1.7」参照	－

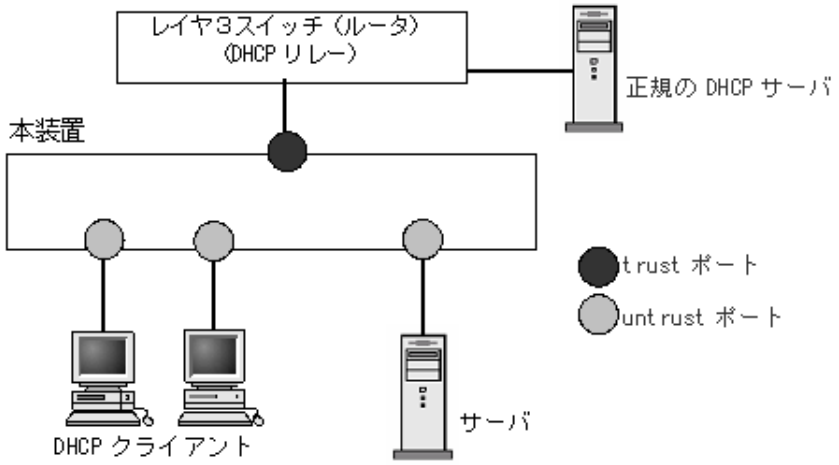
13.1.1 DHCP パケットの監視

（1） ポートの種別と DHCP パケット監視動作

DHCP snooping では，ポートを下記の種別に分類して，DHCP パケットを監視します。

1. trust ポート
   正規の DHCP サーバを接続するポートです。
   trust ポートで受信した DHCP サーバからのパケットを監視し，バインディングデータベースに端末情報をダイナミック登録します。
   DHCP クライアントを接続した場合，監視・学習・検査の対象外となります。
2. untrust ポート
   DHCP クライアントや部門サーバなど，不特定の端末を接続するポートであり，DHCP サーバは接続しません。

図 13-3 DHCP snooping のポート種別

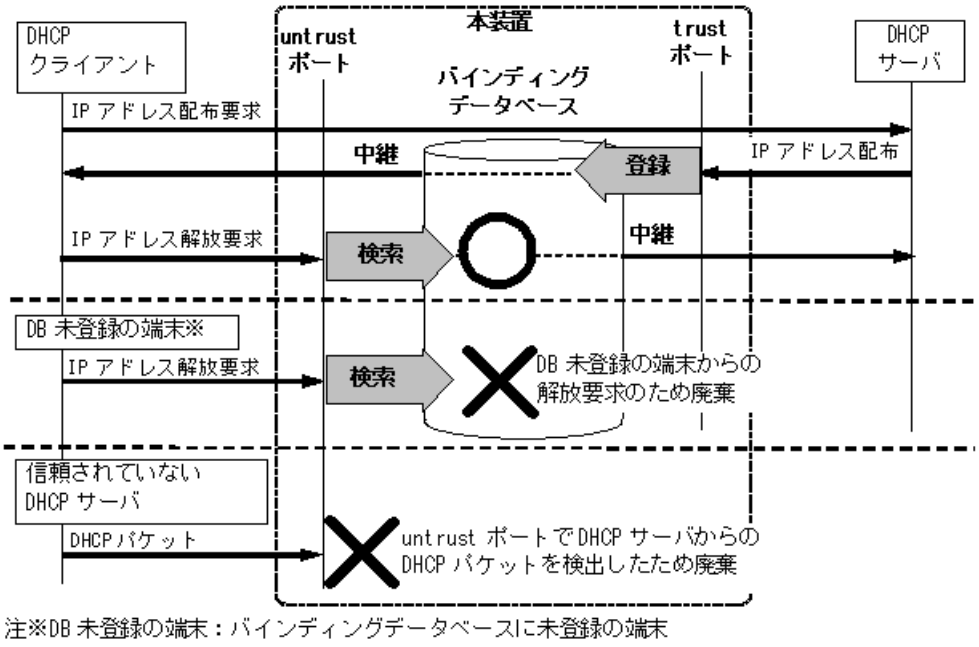


untrust ポートに接続された端末を対象に DHCP パケットを監視し，下記のアクセスを除外します。

- DB 未登録の端末からの IP アドレス解放要求を抑止
  untrust ポートで，DB 未登録の端末から IP アドレス解放要求を受信したときは廃棄します。これにより，正規の DHCP サーバから IP アドレスを配布された形跡のない端末からの IP アドレス解放要求を抑止することができます。
- DHCP サーバからの DHCP パケットを廃棄
  untrust ポートで，受信した DHCP パケットを監視し，DHCP サーバからのパケットを検出したときは廃棄します。これにより，信頼されていない DHCP サーバからの IP アドレス配布を抑止することができます。

DHCP パケット監視の動作概要を次の図に示します。

図 13-4　DHCP パケット監視の動作概要



注※DB 未登録の端末：バインディングデータベースに未登録の端末

コンフィグレーションコマンド ip dhcp snooping で DHCP snooping を有効にすると，デフォルトコンフィグレーションでは全ポートが untrust ポートになります。正規の DHCP サーバへ接続するポートを trust ポートとして設定してください。trust ポートはコンフィグレーションコマンド ip dhcp snooping trust で設定できます。

(2) バインディングデータベースの登録

バインディングデータベースの登録には，ダイナミック登録とスタティック登録があります。

- ダイナミック登録：DHCP サーバから IP アドレスが配布されたときに登録
- スタティック登録：コンフィグレーションコマンド ip source binding で登録

バインディングデータベースの登録内容は，下記のとおりです。

表 13-2　バインディングデータベースの登録内容

項 目		ダイナミック登録	スタティック登録
エントリ数	500 エントリ	ダイナミック・スタティックの合計登録値です。 （うち，スタティック登録は最大 128 エントリまで登録可能）	
登録内容	端末の MAC アドレス	DHCP クライアントの MAC アドレス	固定 IP アドレス端末の MAC アドレス
	端末の IP アドレス	DHCP サーバから配布された IP アドレス	固定 IP アドレス端末の IP アドレス
		ダイナミック・スタティックともに，下記の範囲が有効 • 1.0.0.0 ～ 126.255.255.255 • 128.0.0.0 ～ 223.255.255.255	
	端末の VLAN ID	端末を接続するポートまたはチャネルグループの所属する VLAN ID	

項目		ダイナミック登録	スタティック登録
	端末のポート番号	端末を接続するポート番号またはチャネルグループ番号	
エージングタイマ	リース時間	ダイナミック登録してからエントリをエージングするまでの時間です。DHCP サーバから配布された IP アドレスのリース時間を適用します。	エージング対象外

13.1.2 端末フィルタ

(1) 端末フィルタの概要

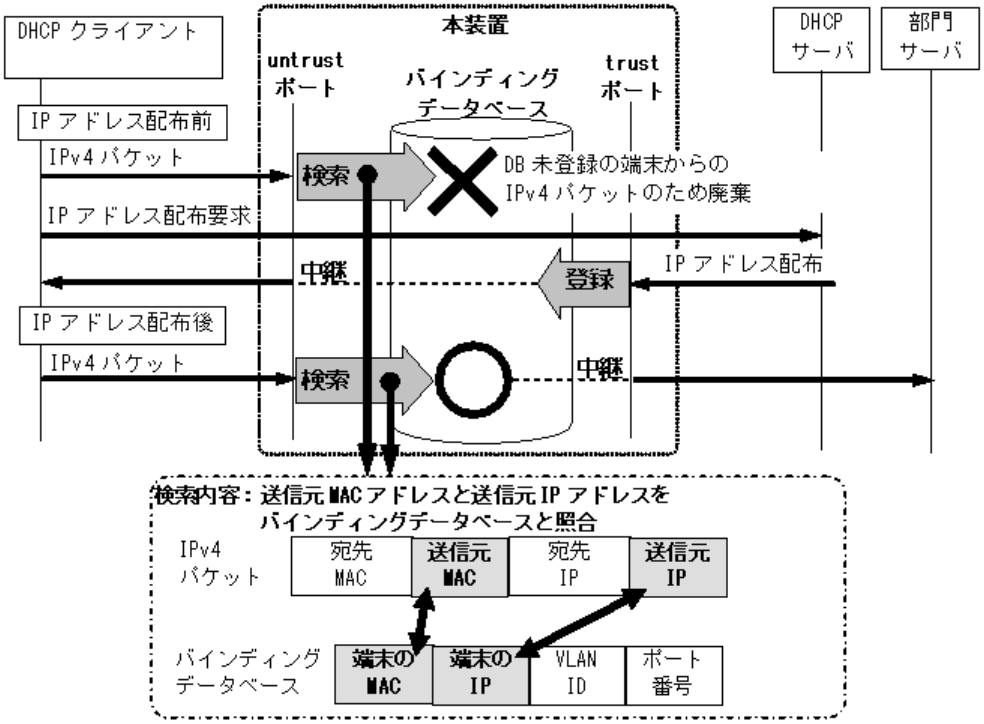
端末フィルタは，DB 未登録の端末からの IPv4 パケットをすべて廃棄します。端末フィルタの対象は，untrust ポートに接続された端末からの IPv4 パケットです。ただし，DHCP snooping 対象 VLAN の DHCP パケットは除きます。

端末フィルタを有効にする際，フィルタ条件を設定します。フィルタ条件は下記の 3 種類がありますので，セキュリティポリシーに従って設定してください。

- 送信元 IP アドレス（Source IP Address）だけの端末フィルタ
- 送信元 IP アドレス（Source IP Address）と送信元 MAC アドレス（Source MAC Address）の端末フィルタ
- 送信元 MAC アドレス（Source MAC Address）だけの端末フィルタ

端末フィルタは，コンフィグレーションコマンド ip verify source でポート単位に設定してください。

図 13-5 端末フィルタの動作概要（送信元 IP アドレスと送信元 MAC アドレスの端末フィルタ例）



これにより，バインディングデータベースに未登録の送信元 IP ドレスと送信元 MAC アドレスの IPv4 パケットを廃棄します。

（2） 固定 IP アドレス端末の通信許可

untrust ポートに接続された固定 IP アドレスを持つ部門サーバなどの通信を許可する場合，バインディングデータベースに端末情報をスタティック登録することで通信を許可できます。

固定 IP アドレス端末の通信許可は，コンフィグレーションコマンド ip source binding で，下記の情報を登録してください。

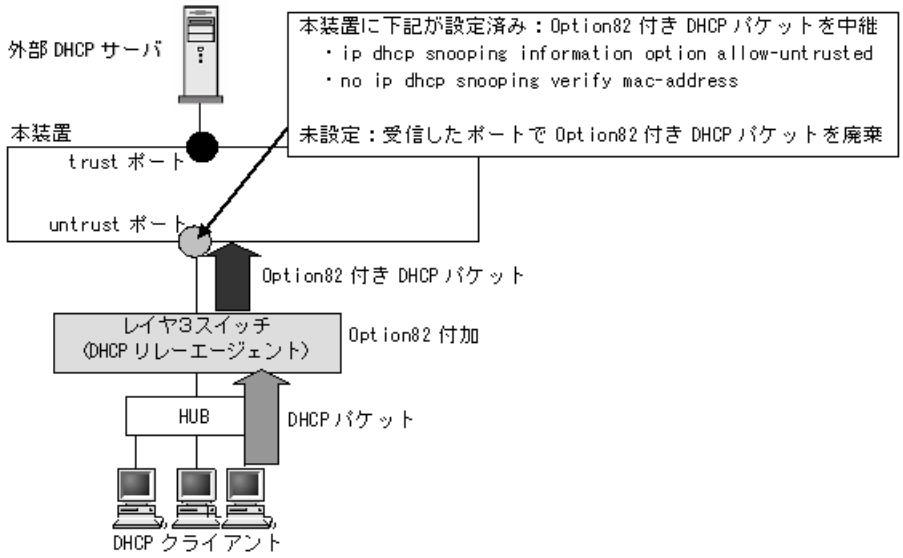
- 端末の IP アドレス
- 端末の MAC アドレス
- 端末を接続するポート番号またはチャネルグループ番号
- 端末を接続するポートまたはチャネルグループの所属する VLAN ID

本コマンドでの設定可能エントリ数については，「表 13-2　バインディングデータベースの登録内容」を参照してください。

13.1.3　DHCP の Option82 付きパケットの中継

本装置と DHCP クライアントの間に，レイヤ 3 スイッチなど DHCP リレーエージェントを配置した構成の場合，DHCP リレーエージェントが DHCP クライアントからの DHCP パケットに Option82 情報を付加する場合があります。

図 13-6　Option82 付きパケットが付加される構成例



Option82 付きパケットは，DHCP リレーエージェントが DHCP クライアントの拡張情報を伝達するための情報で，端末 MAC アドレス，接続ポート番号，ホスト名などが含まれます。

DHCP snooping を有効にした場合，untrust ポートで受信した Option82 付きパケットは廃棄します。従って，本装置が DHCP サーバと DHCP リレーエージェントの中間に配置され，DHCP リレーエージェントが Option82 情報を付加する構成の場合，本装置の DHCP snooping が正しく動作できません。

この場合，コンフィグレーションコマンド ip dhcp snooping information option allow-untrusted で，Option82 付きパケットの通信許可を設定します。

また，DHCP snooping は，untrust ポートから受信した DHCP パケットの送信元 MAC アドレスと

DHCP パケット内のクライアントハードウェアアドレスの一致（MAC アドレスの整合性）を確認しています。untrust ポートに DHCP リレーエージェントが存在した場合，パケットの送信元 MAC アドレスが書き換えられるため，本装置は DHCP パケットを不正と判断し廃棄します。

このため，Option82 付きパケット通信許可設定と共に，コンフィグレーションコマンド no ip dhcp snooping verify mac-address で，MAC アドレス整合性チェックの解除が必要です。

13.1.4 リレーエージェント情報オプション（DHCP Option82）

本装置では DHCP snooping でリレーエージェント情報オプション（DHCP Option82）を付けることが可能です。リレーエージェント情報オプション（DHCP Option82）は，DHCP snooping でパケットを中継するときに，リレーエージェント固有の情報を付けてからサーバに転送するためのオプションです。

コンフィグレーションコマンド ip dhcp snooping information option-insert を設定すると，DHCP/BOOTP パケットのオプションの最後に，次の二つのサブオプションを含む情報を付けます。

- サーキット ID
- リモート ID

サーバに DHCP/BOOTP パケットを転送する場合（DHCP Request）に，前述のサブオプションを必ず付加し，クライアントに DHCP/BOOTP パケットを転送する場合（DHCP Reply）は，リレーエージェント情報オプションを削除してから転送します。

このとき，DHCP Option82 のリモート ID 情報が装置情報と不一致の場合は，転送せずに装置で廃棄します（デフォルトコンフィグレーションの動作）。廃棄動作については，コンフィグレーションによりチェック処理をせずに転送することも可能です。

DHCP Option82 の付加・削除，および転送動作を次の表に示します。

表 13-3 DHCP Option82 の付加・削除および転送動作

受信パケット（DHCP）					DHCP snooping の設定	パケット処理内容	
DHCP 基本		Option					
オペコード	DHCP リレーエージェントの IP アドレス	Option82			information no-check	Option82	転送
		有無	リモート ID	サーキット ID			
1 (Request)	すべて 0	無	－	－	－	付加する	転送する
		有	－	－	－	変更しない	転送する
	いずれか 0 以外	無	－	－	－	付加する	転送する
		有	－	－	－	変更しない	転送する
2 (Reply)	－	無	－	－	check	－	廃棄する
					no-check	－	転送する
		有	装置と不一致	－	check	－	廃棄する
					no-check	削除する	転送する
			装置と一致	－	check	削除する	転送する
					no-check	削除する	転送する

（凡例）－：処理なし

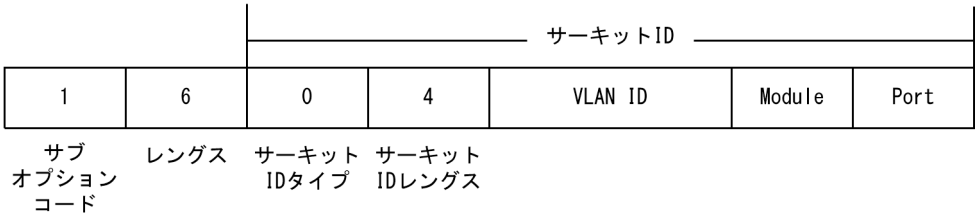
（1） サーキット ID（サブオプションコード 1）

サーキット ID は，クライアントが接続されているポートを識別するための ID です。サーキット ID には，VLAN ID およびポート情報（スイッチ番号とポート番号，またはチャネルグループ番号）が設定されます。サーキット ID の形式は，コンフィグレーションで設定できます。

（a） サーキット ID タイプ 0（circuit-type 0 指定時）

コンフィグレーションコマンド ip dhcp snooping vlan information option format-type circuit-id のパラメータ circuit-id-type 0 指定時の形式です。

図 13-7　サーキット ID タイプ 0 の形式



＜イーサネットインタフェースの場合＞

以下が設定されます。

Module：スイッチ番号（< switch no.>：スタック動作時 1 ～ 2，スタンドアロン動作時 0）

Port：ポート番号（<IF#> のポート番号 1 ～ 10）

＜ポートチャネルインタフェースの場合＞

以下が設定されます。

Module：ポートチャネルを表す固定値（0xc）

Port：チャネルグループ番号（<channel group>：スタック動作時 1 ～ 120，スタンドアロン動作時 1 ～ 64）

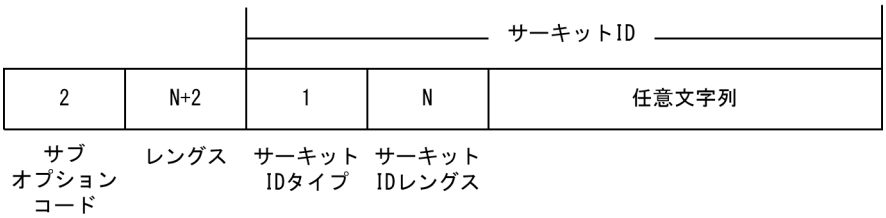
＜ VLAN ID ＞

VLAN Tag の VLAN ID が設定されます。VLAN Tag を使用しない場合は，0 が設定されます。

（b） サーキット ID タイプ 1（circuit-id string 指定時）

コンフィグレーションコマンド ip dhcp snooping vlan information option format-type circuit-id のパラメータ str <circuit-id-string> 指定時の形式です。

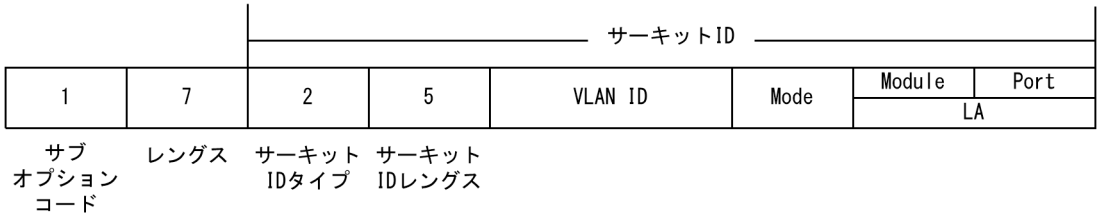
図 13-8　サーキット ID タイプ 1 の形式（任意文字列）



（c） サーキット ID タイプ 2（circuit-type 2 指定時，コマンド省略時）

コンフィグレーションコマンド ip dhcp snooping vlan information option format-type circuit-id のパラメータ circuit-id-type 2 指定時，またはコマンド省略時の形式です。

図 13-9 サーキット ID タイプ 2 の形式



＜イーサネットインタフェースの場合＞

以下が設定されます。

Mode：イーサネットを表す固定値（0）

Module：スイッチ番号（< switch no.>：スタック動作時 1 ～ 2，スタンドアロン動作時 0）

Port：ポート番号（<IF#> のポート番号 1 ～ 10）

＜ポートチャネルインタフェースの場合＞

以下が設定されます。

Mode：ポートチャネルを表す固定値（1）

LA：チャネルグループ番号（<channel group>：スタック動作時 1 ～ 120，スタンドアロン動作時 1 ～ 64）

＜ VLAN ID ＞

VLAN Tag の VLAN ID が設定されます。VLAN Tag を使用しない場合は，0 が設定されます。

(2) リモート ID（サブオプションコード 2）

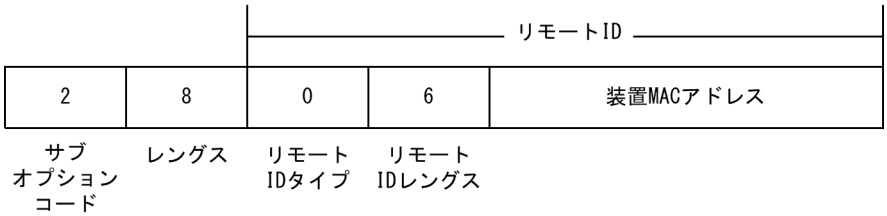
リモート ID は，装置を識別するための ID です。リモート ID の形式は，コンフィグレーションで指定できます。

(a) リモート ID タイプ 0（コマンド省略時）

コンフィグレーションコマンド ip dhcp snooping information option format remote-id 省略時の形式です。

リモート ID の MAC アドレス（6 バイト）には，本装置の装置 MAC アドレスが設定されます。

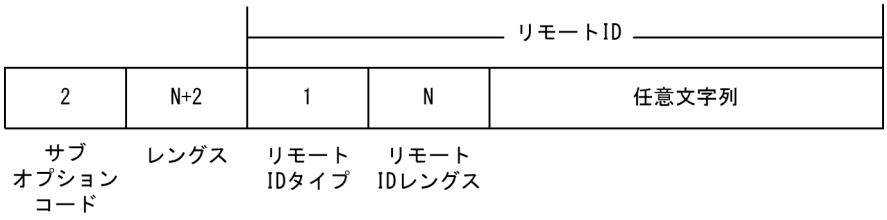
図 13-10 リモート ID タイプ 0 の形式



(b) リモート ID タイプ 1（string 指定時）

コンフィグレーションコマンド ip dhcp snooping information option format remote-id のパラメータ str <string> 設定時の形式です。

図 13-11 リモート ID タイプ 1 の形式



13.1.5 DHCP パケットの受信レート制限

DHCP snooping 有効時に，受信する DHCP パケットの監視を実施する際，設定した受信レートを超えた DHCP パケットを廃棄する機能です。

受信レートはコンフィグレーションコマンド ip dhcp snooping limit rate で設定できます。本コマンド未設定の場合は，受信レートは無制限となります。

DHCP パケットの受信レート制限は，untrust ポートだけを対象とし，trust ポートは対象外です。

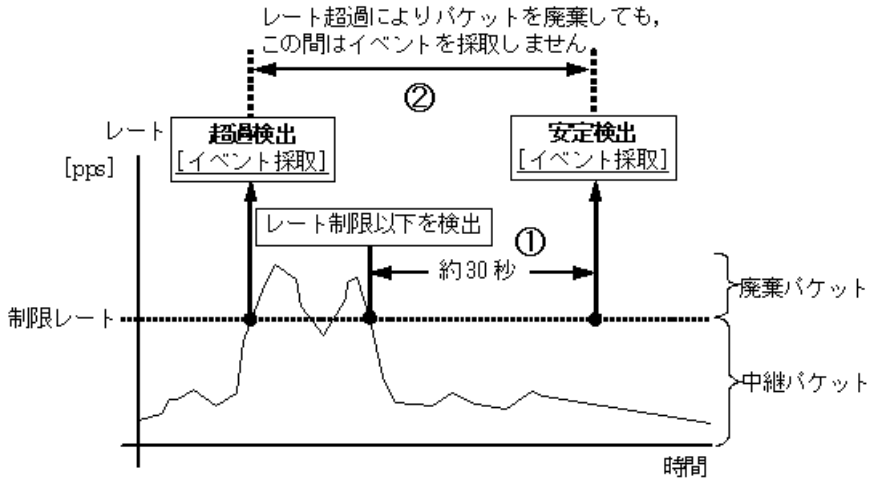
受信レートを超えた DHCP パケットは廃棄し，運用ログ情報を採取します。ただし，Trap は発行しません。なお，運用ログ情報は運用コマンド show logging で，廃棄パケット数については運用コマンド show ip dhcp snooping statistics で確認してください。

運用ログ情報は下記の契機で採取します。

- コンフィグレーションで設定した受信レートを超過したときに，「超過検出」イベントを採取します。
- 「超過検出」イベントを採取後，設定レート制限以下の状態が約 30 秒間継続（図内①）したときに，「安定検出」イベントを採取します。
  「超過検出」イベントを採取後から「安定検出」イベント採取までの間（図内②）は，レート超過によりパケットを廃棄してもイベントを採取しません。

運用ログ情報の採取契機を次の図に示します。

図 13-12 DHCP パケット受信レートの運用ログ情報採取契機



13.1.6 ダイナミック ARP 検査機能

DHCP snooping 有効時に，本装置が untrust ポートで受信した ARP パケット内の発信者 IP アドレス（Sender IP Address）および発信者 MAC アドレス（Sender MAC Address）が，バインディングデータベースに登録されている正規端末のアドレスであるか検査する機能です。本機能により，DB 未登録の端末から送信された詐称 ARP パケットによる，正規端末の通信の乗っ取りを防止します。

(1) ダイナミック ARP 検査対象

ダイナミック ARP 検査の対象は，下記の条件にすべて一致する ARP パケットです。

- ARP 検査対象 VLAN に所属するポートで受信した ARP パケット
  （ARP 検査対象 VLAN は，コンフィグレーションコマンド ip arp inspection vlan で設定します。）
- untrust ポート（コンフィグレーションコマンド ip arp inspection trust を設定していないポート）で受信した ARP パケット

(2) ダイナミック ARP 検査の基本検査

基本検査では，untrust ポートで受信した ARP パケットとバインディングデータベースのエントリの整合性を検査します。

ダイナミック ARP 検査の基本検査を下記に示します。

図 13-13 ダイナミック ARP 検査の基本検査概要

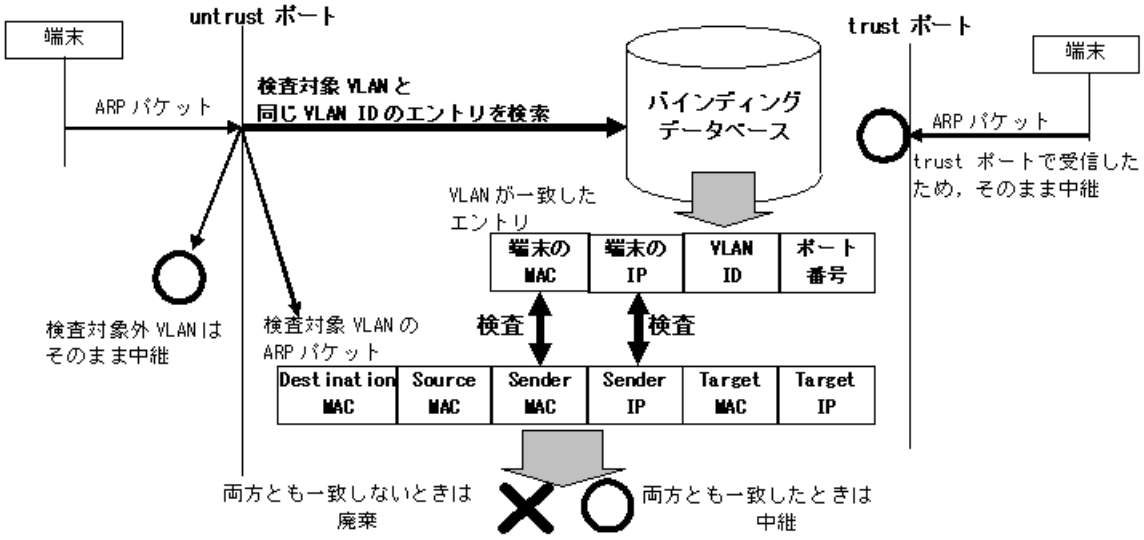


表 13-4 ARP パケットのフィールド別基本検査対象

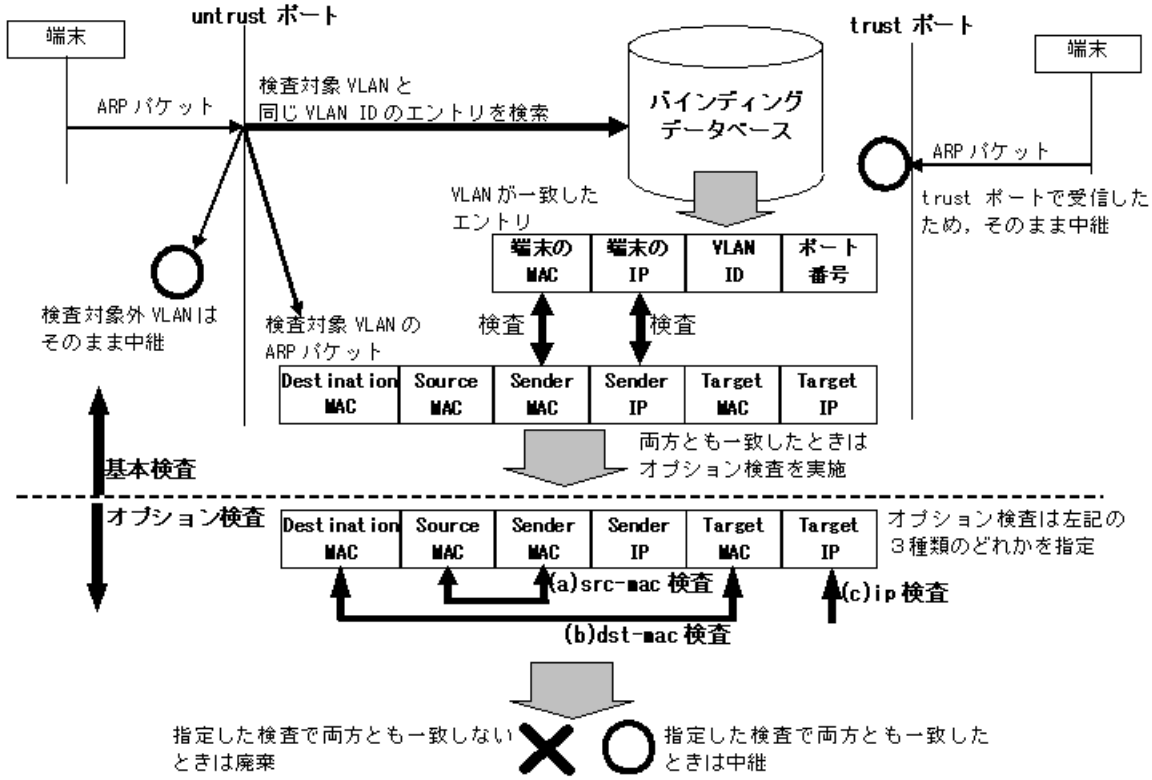
ARP パケットのフィールド			Request	Reply	備考
Ethernet ヘッダ	Destination	MAC	—	—	—
	Source	MAC	—	—	—
ARP ヘッダ	Sender	MAC	○	○	バインディングデータベースと比較
		IP	○	○	バインディングデータベースと比較
	Target	MAC	—	—	—
		IP	—	—	—

（凡例）
○：検査対象
－：検査対象外

（3） ダイナミック ARP 検査のオプション検査

ダイナミック ARP 検査機能は，バインディングデータベースとの整合性を検査しますが，オプションとして ARP パケット内データの整合性の検査もサポートします。

図 13-14　ダイナミック ARP 検査の基本検査とオプション検査の関係



（a） 送信元 MAC アドレス指定 (src-mac 検査）

受信 ARP パケットの送信元 MAC アドレス（Source MAC Address）と，発信者 MAC アドレス（Sender MAC Address）が同一であることを検査します。

ARP Request，ARP Reply の双方に対して実施します。

（b） 宛先 MAC アドレス指定（dst-mac 検査）

受信 ARP パケットの宛先 MAC アドレス（Destination MAC Address）と，対象者 MAC アドレス（Target MAC Address）が同一であることを検査します。

ARP Reply に対してだけ実施します。

（c） IP アドレス指定（ip 検査）

受信 ARP パケットの対象者 IP アドレス（Target IP Address）が，下記の範囲内であることを検査します。

- 1.0.0.0 ～ 126.255.255.255

- 128.0.0.0 ～ 223.255.255.255

ARP Reply に対してだけ実施します。

表 13-5 ARP パケットのフィールド別オプション検査対象

ARP パケットのフィールド			src-mac 検査		dst-mac 検査		ip 検査	
			Request	Reply	Request	Reply	Request	Reply
Ethernet ヘッダ	Destination	MAC	－	－	－	○	－	－
	Source	MAC	○	○	－	－	－	－
ARP ヘッダ	Sender	MAC	○	○	－	－	－	－
		IP	－	－	－	－	－	－
	Target	MAC	－	－	－	○	－	－
		IP	－	－	－	－	－	○

（凡例）
○：検査対象
－：検査対象外

（4） ARP パケットの受信レート制限

ダイナミック ARP 検査機能有効時に，ダイナミック ARP 検査対象 VLAN に所属するポートで，設定した受信レートを超えた ARP パケットを廃棄する機能です。

受信レートはコンフィグレーションコマンド ip arp inspection limit rate で設定できます。本コマンド未設定の場合は，受信レートは無制限となります。

受信レートを超えた ARP パケットは廃棄し，運用ログ情報を採取します。ただし，Trap は発行しません。なお，運用ログ情報は運用コマンド show logging で，廃棄パケット数については運用コマンド show ip arp inspection statistics で確認してください。

ARP パケット受信レート超過時の運用ログ情報の採取契機は，DHCP パケットの受信レート制限と同様です。「13.1.5 DHCP パケットの受信レート制限 図 13-12 DHCP パケット受信レートの運用ログ情報採取契機」を参照してください。

13.1.7 バインディングデータベースの保存

コンフィグレーションで指定することにより，バインディングデータベースの保存，および装置再起動時の復元が可能です。

（1） バインディングデータベースの保存の動作条件

バインディングデータベースの保存は，下記のコンフィグレーションコマンドの設定により動作可能です。

- ip dhcp snooping：DHCP snooping の有効設定
- ip dhcp snooping vlan：DHCP snooping を実施する VLAN の設定
- ip dhcp snooping database url：バインディングデータベース保存先

本装置では，書き込み指定時間満了時または特定オペレーションにより保存を実施します。

（2） 書き込み指定時間満了時の保存

書き込み指定時間は下記のいずれかを保存契機としてタイマをスタートし，タイマが満了した場合に指定

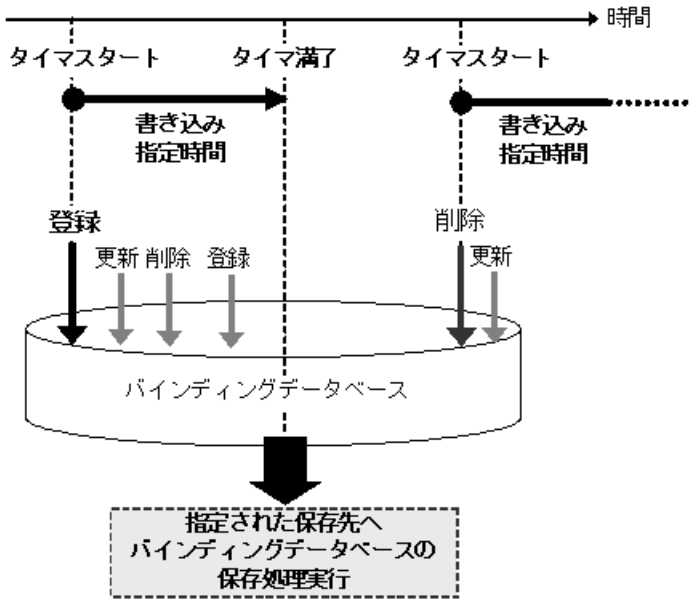
した保存先へ保存します。

- ダイナミックのバインディングデータベースの登録・更新・削除時
- コンフィグレーションコマンド ip dhcp snooping database url 設定時（保存先の変更を含む）
- 運用コマンド clear ip dhcp snooping binding 実行時

書き込み指定時間は，コンフィグレーションコマンド ip dhcp snooping database write-delay で設定します。

書き込み指定時間のタイマは，上記の保存契機でスタートすると，タイマ満了となるまではタイマを停止しません。この間にバインディングデータベースの登録・更新・削除が発生してもタイマの再スタートはありません。

図 13-15　保存契機と書き込み指定時間の動作概要（バインディングデータベース登録を契機とした例）



（3） 特定オペレーションによる保存

装置再起動を促す下記のオペレーションを実行した場合は，その時点でのバインディングデータベースをコンフィグレーションで指定した保存先へ保存します。

なお，コンフィグレーションで保存先が指定されていない場合は，下記のオペレーションを実行しても，バインディングデータベースを保存しません。

表 13-6　特定オペレーションによる保存

オペレーション	保存先	動作契機
reload	コンフィグレーションで指定した保存先	運用端末から運用コマンド入力
ppupdate		運用端末から運用コマンド入力
backup		運用端末から運用コマンド入力
copy-config		OAN から実行

（4） バインディングデータベースの保存先

コンフィグレーションで指定するバインディングデータベースの保存先は，内蔵フラッシュメモリと MC

があります。どちらの場合も書き込み実施時の全エントリが保存され，次の書き込み実施時に上書きされます。

保存先は，コンフィグレーションコマンド ip dhcp snooping database url で設定します。

(5) 保存したバインディングデータベースの復元

保存したバインディングデータベースは，装置起動時に復元します。装置起動前に下記を確認してください。

- コンフィグレーションコマンド ip dhcp snooping database url で保存先が設定されている
- 保存先が MC の場合，保存したファイルの MC が挿入されている

13.1.8 DHCP snooping 使用時の注意事項

(1) 他機能との共存について

(a) レイヤ 2 スイッチ機能との共存

「コンフィグレーションガイド Vol.1　19.3　レイヤ 2 スイッチ機能と他機能の共存について」を参照してください。

(b) フィルタ機能との共存

「1.1.8　フィルタ使用時の注意事項」を参照してください。

(c) レイヤ 2 認証機能との共存

DHCP snooping および端末フィルタと，各認証機能（IEEE802.1X 認証，Web 認証，MAC 認証）は，同一ポート内での共存が可能です。

この場合，端末フィルタよりも各認証の結果が優先されるため，端末フィルタで通信許可された端末においても，各認証機能で許可されなければ通信できません。

また，trust ポート，untrust ポートに依存せず各認証機能は混在可能です。

DHCP snooping とレイヤ 2 認証機能を併用した場合，通信可能な最大端末数は DHCP snooping の管理端末数（最大 500 台）となります。

(d) ホワイトリスト機能との共存

「14.1.5　他機能との共存」を参照してください。

(e) CFM との共存

「21.1.9　CFM 使用時の注意事項」を参照してください。

(f) 省電力機能との共存

「コンフィグレーションガイド Vol.1　15.1.7　省電力機能使用時の注意事項」を参照してください。

(g) スタックとの共存

「コンフィグレーションガイド Vol.1　7. スタックの解説【OP-WLE】」を参照してください。

(2) ダイナミック ARP 検査機能の使用について

ダイナミック ARP 検査機能は，DHCP snooping 機能が有効の場合だけ動作する機能です。DHCP

snooping 機能が無効の状態で，ダイナミック ARP 検査機能だけを有効にした場合，ARP パケットが中継されなくなります。ダイナミック ARP 検査機能を使用する場合は，DHCP snooping 機能と合わせて設定し，バインディングデータベースが生成されることが必要です。

- コンフィグレーションコマンド ip dhcp snooping：DHCP snooping の有効設定
- コンフィグレーションコマンド ip dhcp snooping vlan：DHCP snooping を実施する VLAN の設定

また，コンフィグレーションコマンド ip source binding でバインディングデータベースにスタティック登録されたエントリもダイナミック ARP 検査の対象となります。

（3）バインディングデータベースの保存と復元について

- コンフィグレーションコマンド ip dhcp snooping database url 未設定（初期状態）の場合，バインディングデータベースは保存されません。装置を再起動すると登録済のバインディングデータベースが消去されるため，DHCP クライアントからの通信ができなくなります。この場合は，DHCP クライアント側で IP アドレスの解放と更新を実施してください。（例：Windows の場合，コマンドプロンプトから ipconfig /release を実行した後に，ipconfig /renew を実行してください。）
  これにより，バインディングデータベースに端末情報が再登録され，DHCP クライアントの通信が可能になります。
- 復元するエントリのうち，DHCP サーバのリース時間を満了したエントリは復元されません。バインディングデータベースが保存された後，本装置の電源 OFF 前に時計設定を変更すると，電源 ON 後のバインディングデータベース復元処理が正しく実施されない場合があります。
- コンフィグレーションコマンド ip source binding によりスタティック登録されたエントリの復元は，起動時のスタートアップコンフィグレーションファイルに従います。
- バインディングデータベースの保存先を MC にした場合は，装置再起動後の画面にプロンプトが表示されるまで MC を抜かないでください。
- 運用コマンド backup で保存して運用コマンド restore で復元する場合，復元先の装置にコンフィグレーションコマンド ip dhcp snooping database url が設定されていないことを確認してから実行してください。設定されたまま運用コマンド restore を実行すると，バインディングデータベース復元処理が正しく実施されない場合があります。

13.2 DHCP snooping のコンフィグレーション

13.2.1 コンフィグレーションコマンド一覧

DHCP snooping のコンフィグレーションコマンド一覧を次の表に示します。

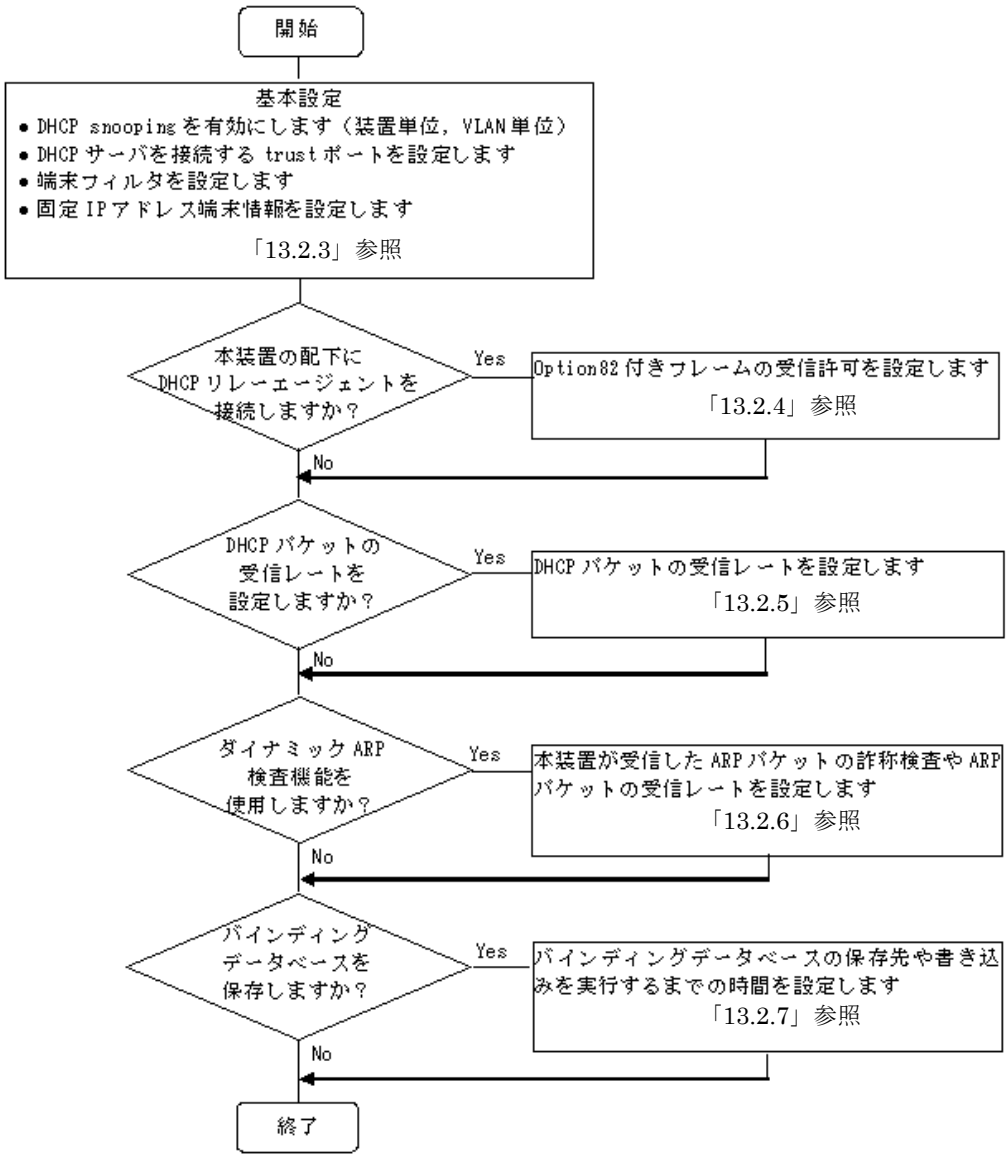
表 13-7 コンフィグレーションコマンド一覧

コマンド名	説明
ip arp inspection limit rate	当該ポートでの ARP パケットの受信レート（1 秒あたりに受信可能な ARP パケット数）を設定します。
ip arp inspection trust	ダイナミック ARP 検査を実施しないポートに対して設定します。
ip arp inspection validate	ダイナミック ARP 検査機能有効時に，ダイナミック ARP 検査の精度を高めるために追加する検査項目を設定します。
ip arp inspection vlan	ダイナミック ARP 検査機能の検査対象 VLAN を設定します。
ip dhcp snooping	DHCP snooping の有効／無効を設定します。
ip dhcp snooping database url	バインディングデータベースの保存先を設定します。
ip dhcp snooping information no-check	DHCP Replyパケットからリレーエージェント情報オプション（DHCP Option82）を削除する際に，DHCP Option82をチェックせずに転送します。
ip dhcp snooping database write-delay	バインディングデータベース保存時の書き込み指定時間を設定します。
ip dhcp snooping information option allow-untrusted	untrust ポートでの Option82 付きの DHCP パケットの受信可否を設定します。
ip dhcp snooping information option format remote-id	DHCP Option82サブオプションのリモートIDを設定します。
ip dhcp snooping information option-insert	リレーエージェント情報オプション（DHCP Option82） の付加を有効にします。
ip dhcp snooping limit rate	当該ポートでの DHCP パケットの受信レート（1 秒あたりに受信可能な DHCP パケット数）を設定します。
ip dhcp snooping trust	インタフェースを trust ポートとして設定します。
no ip dhcp snooping verify mac-address	untrust ポートから受信した DHCP パケットの送信元 MAC アドレスと，クライアントのハードウェアアドレスの一致をチェックするか否かを設定します。
ip dhcp snooping vlan	VLAN での DHCP snooping を有効にします。
ip dhcp snooping vlan information option format-type circuit-id	DHCP Option82サブオプションのサーキットIDを設定します。
ip source binding	固定 IP アドレス端末用のバインディングデータベースを設定します。
ip verify source	DHCP snooping バインディングデータベースを基に，端末フィルタを実施する場合に設定します。

13.2.2 DHCP snooping の設定手順

本節の設定例は，レイヤ 3 スイッチを経由した構成例を基本設定とし，DHCP snooping の各機能を設定する形態で記載しています。次の図に示す手順に沿って設定してください。

図 13-16　DHCP snooping の設定手順

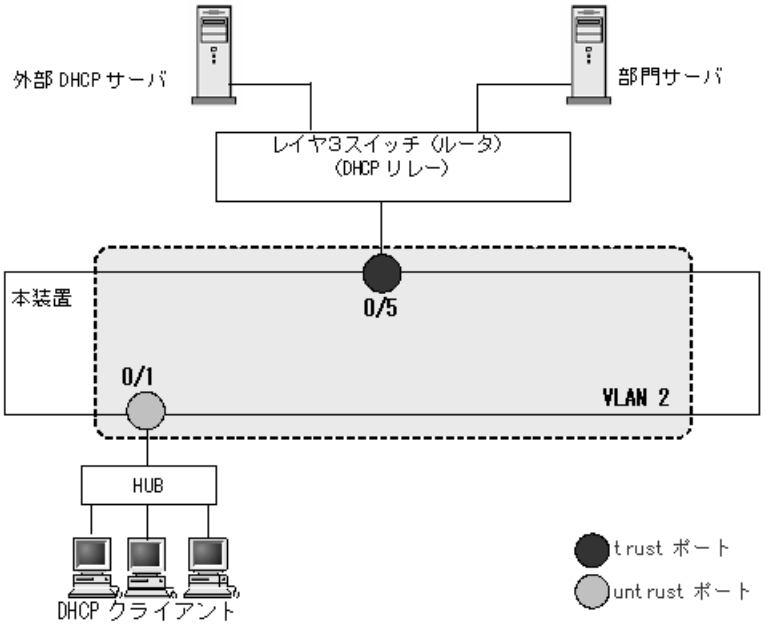


13.2.3　基本設定（レイヤ３スイッチを経由した場合）

DHCP snooping を使用するための基本的な設定について説明します。

DHCP サーバと部門サーバをレイヤ３スイッチを経由する構成で，レイヤ３スイッチに接続するポートを trust ポートとして設定します。

図 13-17　レイヤ３スイッチ経由の構成例



（1） DHCP snooping の有効設定

［設定のポイント］

装置としての DHCP snooping を有効にし，下記を設定します。

- DHCP snooping を有効にする VLAN を設定
- DHCP サーバを接続するポートを trust ポートとして設定
- untrust ポートに，DB 未登録の端末からのパケットを廃棄する端末フィルタを設定

［コマンドによる設定］

1. **(config)# ip dhcp snooping**
   装置としての DHCP snooping 機能を有効にします。
2. **(config)# vlan 2**
   (config-vlan)# exit
   (config)# ip dhcp snooping vlan 2
   VLAN ID 2 で DHCP snooping を有効にします。本コマンドを指定しない VLAN では DHCP snooping は動作しません。
3. **(config)# interface gigabitethernet 0/1**
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 2
   (config-if)# exit
   ポート 0/1 をアクセスポートとし，ポート 0/1 が所属する VLAN として VLAN ID 2 を設定します。

（2） trust ポートの設定

［設定のポイント］

DHCP サーバに接続するポート（構成図ではレイヤ３スイッチと接続するポート）を trust ポートとして使用するインタフェースを設定します。

［コマンドによる設定］

1. **(config)# interface gigabitethernet 0/5**
   (config-if)# ip dhcp snooping trust
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 2
   (config-if)# exit
   ポート 0/5 を trust ポートとして設定します。その他のポートは untrust ポートとなります。またポート 0/5 をアクセスポートとし，ポート 0/5 が所属する VLAN として VLAN ID 2 を設定します。

（3） 端末フィルタの設定

［設定のポイント］

バインディングデータベースを基にパケットを廃棄するポートに端末フィルタを設定します。

［コマンドによる設定］

1. **(config)# interface gigabitethernet 0/1**
   (config-if)# ip verify source port-security
   (config-if)# exit
   ポート 0/1 に送信元 IP アドレスと送信元 MAC アドレスの端末フィルタを設定します。

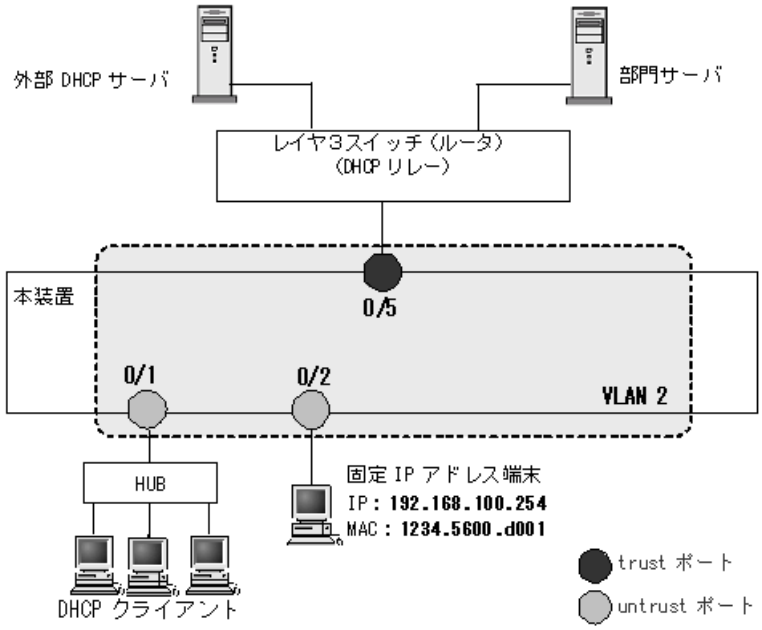
［注意事項］

trust ポートで本コマンドを設定しても，端末フィルタは無効です。また，DHCP snooping 有効時は，ip dhcp snooping vlan で設定されていない VLAN でも端末フィルタが有効となりますのでご注意ください。

（4） 固定 IP アドレス端末を接続した場合

固定 IP アドレスを持つ端末を接続する場合の設定について説明します。

図 13-18　固定 IP アドレス端末を接続した場合の構成例



DHCP snooping の設定は「13.2.3　基本設定（レイヤ 3 スイッチを経由した場合)」と同様です。本例で

は，固定 IP アドレスを持つ端末を untrust ポートに接続するため，バインディングデータベースに固定 IP アドレス端末の登録が必要です。

上記の設定は，コンフィグレーションコマンドで設定します。

［設定のポイント］

固定 IP アドレスを持つ端末用にバインディングデータベースを設定します。

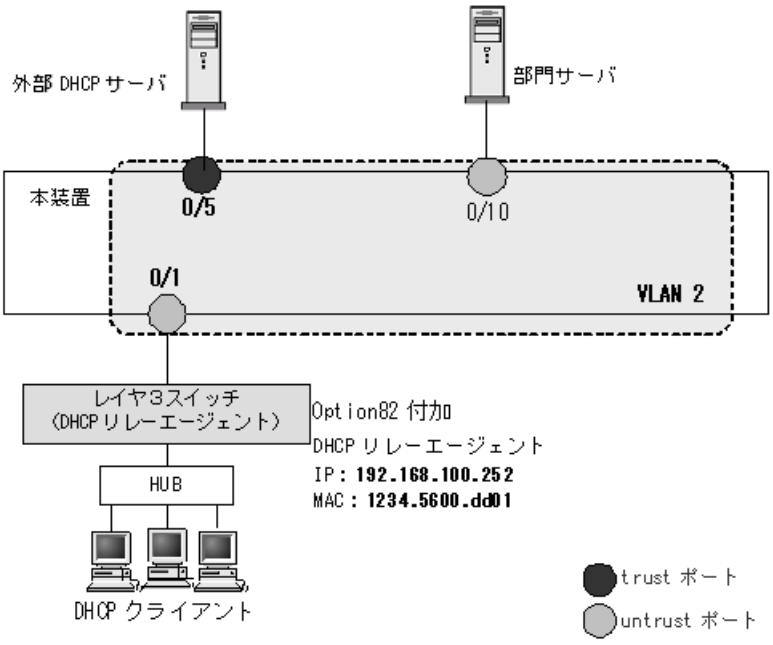
［コマンドによる設定］

1. **(config)# interface gigabitethernet 0/2**
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 2
   (config-if)# exit
   固定 IP アドレス端末を接続するポート 0/2 に VLAN ID 2 を設定します。
2. **(config)# ip source binding 1234.5600.d001 vlan 2 192.168.100.254 interface gigabitethernet 0/2**
   端末の MAC アドレス，端末が接続されている VLAN ID，端末の IP アドレス，端末が接続されているポート番号を，バインディングデータベースに設定します。

13.2.4 本装置の配下に DHCP リレーエージェントが接続された場合

本装置の配下に Option82 を付加した DHCP パケットを送信する DHCP リレーエージェントを接続した場合，本装置で Option82 付きパケットを中継できるように設定します。

図 13-19 本装置の配下に DHCP リレーエージェントを接続した場合の構成例



本装置の DHCP snooping 設定は「13.2.3 基本設定（レイヤ 3 スイッチを経由した場合）」同様です。本例では，DHCP リレーエージェントが Option82 付き DHCP パケットを送信するため，本装置で DHCP リレーエージェントを接続する untrust ポートで Option82 付きパケットの中継を許可する設定が必要です。その他，同じ untrust ポートで DHCP パケットの送信元アドレスをチェックしない設定，ARP パケットの中継を許可する設定，端末フィルタを IP アドレスだけでフィルタする設定も必要です。

上記の設定は，コンフィグレーションコマンドで設定します。

（1） Option82 付き DHCP パケットを untrust ポートで受信許可する設定

［設定のポイント］

untrust ポートでの Option82 付き DHCP パケットを受信可能に設定します。

［コマンドによる設定］

1. **(config)# ip dhcp snooping information option allow-untrusted**
   untrust ポートで Option82 付きの DHCP パケットの受信を許可します。

（2） untrust ポートで DHCP パケットの送信元アドレスチェックを解除する設定

［設定のポイント］

untrust ポートで DHCP パケットの送信元 MAC アドレスをチェックしないで中継するため，アドレスチェック機能の解除を設定します。

［コマンドによる設定］

1. **(config)# no ip dhcp snooping verify mac-address**
   untrust ポートで受信した DHCP パケットの送信元 MAC アドレスのチェック無を設定します。

［注意事項］

本コマンド未設定の場合，送信元 MAC アドレスをチェックするため，untrust ポートに DHCP リレーエージェントを接続できなくなります。

（3） untrust ポートで ARP パケットの中継を許可するバインディングデータベースの設定

［設定のポイント］

untrust ポートに接続した DHCP リレーエージェントからの ARP パケットを中継するために，DHCP リレーエージェントのアドレスをバインディングデータベースに設定します。

［コマンドによる設定］

1. **(config)# ip source binding 1234.5600.dd01 vlan 2 192.168.100.252 interface gigabitethernet 0/1**
   DHCP リレーエージェントの MAC アドレス，接続されている VLAN ID，IP アドレス，接続されているポート番号を，バインディングデータベースとして設定します。

（4） untrust ポートで IP アドレスだけの端末フィルタの設定

［設定のポイント］

DHCP クライアントからのパケットは，レイヤ 3 スイッチ経由により送信元 MAC アドレスが書き換えられているため，untrust ポートに IP アドレスだけの端末フィルタを設定します。

［コマンドによる設定］

1. **(config)# interface gigabitethernet 0/1**
   (config-if)# ip verify source
   (config-if)# exit
   ポート 0/1 に IP アドレスだけの端末フィルタを設定します。

13.2.5 DHCP パケットの受信レートの設定

DHCP パケットを受信するポートの受信レート制限をコンフィグレーションで設定します。

DHCP snooping の設定は「13.2.3 基本設定（レイヤ 3 スイッチを経由した場合)」と同様です。

(1) 受信レートの設定

[設定のポイント]

端末から DHCP パケットを受信するポート 0/1 に受信レートを設定します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 0/1**
   (config-if)# ip dhcp snooping limit rate 50
   (config-if)# exit
   ポート 0/1 の受信レートを 50 パケット / 秒に設定します。

13.2.6 ダイナミック ARP 検査機能の設定

ダイナミック ARP 検査機能を使用するための基本的な設定について説明します。

DHCP snooping の設定は「13.2.3 基本設定（レイヤ 3 スイッチを経由した場合)」と同様です。

(1) ダイナミック ARP 検査機能の検査対象 VLAN の設定（基本検査対象）

[設定のポイント]

DHCP snooping を有効にした VLAN のうちで，ダイナミック ARP 検査機能の検査対象 VLAN ID を設定します。設定した VLAN で受信した ARP パケットが基本検査対象となります。

[コマンドによる設定]

1. **(config)# ip arp inspection vlan 2**
   VLAN ID 2 をダイナミック ARP 検査対象に設定します。本コマンドを指定しない VLAN ではダイナミック ARP 検査機能は動作しません。

[注意事項]

1. コンフィグレーションコマンド ip dhcp snooping vlan で設定している VLAN ID を指定してください。
2. 本コマンドを設定した場合は，コンフィグレーションコマンド ip source binding で登録したバインディングデータベースエントリも，ダイナミック ARP 検査の対象となります。
3. 本コマンドを設定した VLAN に所属しているポートに対して，コンフィグレーションコマンド ip arp inspection trust を設定した場合は，そのポートでダイナミック ARP 検査を実施しません。

(2) ダイナミック ARP 検査を実施しないポートの設定

[設定のポイント]

ダイナミック ARP 検査を実施しないポートに対して設定します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 0/5**
   (config-if)# ip arp inspection trust
   (config-if)# exit

ポート 0/5 はダイナミック ARP 検査を実施しないポートとなります。その他のポートはダイナミック ARP 検査を実施するポートとなります。

[注意事項]

1. 本コマンドを設定したポートでは，ダイナミック ARP 検査機能の検査対象 VLAN に所属していても，ダイナミック ARP 検査を実施しません。
2. 本コマンドを設定したポートの ARP パケット受信レートは無制限となります。

(3) ダイナミック ARP 検査機能のオプション検査の設定

[設定のポイント]

基本検査した ARP パケットに対するオプション検査を設定します。本例では，受信 ARP パケットの送信元 MAC アドレス（Source MAC Address）と，発信者 MAC アドレス（Sender MAC Address）が同一であることを検査するよう設定します。

[コマンドによる設定]

1. **(config)# ip arp inspection validate src-mac**

受信 ARP パケットの送信元 MAC アドレス（Source MAC Address）と，発信者 MAC アドレス（Sender MAC Address）が同一であることを検査する src-mac 検査を設定します。

(4) ARP パケットの受信レートの設定

[設定のポイント]

端末から ARP パケットを受信するポート 0/1 に受信レートを設定します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 0/1**
   (config-if)# ip arp inspection limit rate 100
   (config-if)# exit

ポート 0/1 の受信レートを 100 パケット / 秒に設定します。

13.2.7 バインディングデータベース保存の設定

(1) 保存先の設定

(a) 内蔵フラッシュメモリに保存する場合

[設定のポイント]

バインディングデータベースの保存先に内蔵フラッシュメモリを設定します。

[コマンドによる設定]

1. **(config)# ip dhcp snooping database url flash**

保存先として内蔵フラッシュメモリを設定します。

[注意事項]

運用コマンド backup を実行した場合，内蔵フラッシュメモリに保存されたバインディングデータベースもバックアップ対象となります。運用コマンド restore で復元できます。

(b) MC に保存する場合

[設定のポイント]

バインディングデータベースの保存先に MC を設定します。MC の場合は保存するファイル名を設定できます。

[コマンドによる設定]

1. **(config)# ip dhcp snooping database url mc dhcpsn-db**

保存先として MC，および保存時のファイル名 dhcpsn-db を設定します。

[注意事項]

保存先を MC にする場合は，本装置のメモリカードスロットに MC を挿入しておいてください。また，MC はアラクサラ製品をご使用ください。

(2) 書き込み指定時間の設定

[設定のポイント]

バインディングデータベースの保存先への書き込み指定時間を設定します。

[コマンドによる設定]

1. **(config)# ip dhcp snooping database write-delay 3600**

下記のいずれかを保存契機とし，保存処理を実行するまでの時間を 3600 秒に設定します。

- ダイナミックのバインディングデータベースの登録・更新・削除時
- コンフィグレーションコマンド ip dhcp snooping database url 設定時（保存先の変更を含む）
- 運用コマンド clear ip dhcp snooping binding 実行時

[注意事項]

次回の保存契機から本コマンドで設定した時間が運用に反映されます。

13.3 DHCP snooping のオペレーション

13.3.1 運用コマンド一覧

DHCP snooping の運用コマンド一覧を次の表に示します。

表 13-8 運用コマンド一覧

コマンド名	説明
show ip arp inspection statistics	ダイナミック ARP 検査の統計情報を表示します。
clear ip arp inspection statistics	ダイナミック ARP 検査の統計情報をクリアします。
show ip dhcp snooping	DHCP snooping 情報を表示します。
show ip dhcp snooping binding	DHCP snooping バインディングデータベース情報を表示します。
clear ip dhcp snooping binding	DHCP snooping バインディングデータベース情報をクリアします。
show ip dhcp snooping statistics	DHCP snooping 統計情報を表示します。
clear ip dhcp snooping statistics	DHCP snooping 統計情報をクリアします。

13.3.2 DHCP snooping の確認

(1) DHCP snooping 情報の確認

DHCP snooping 情報を運用コマンド show ip dhcp snooping で表示します。Option82 付きパケットの許可状態，DHCP パケット送信元 MAC アドレスのチェック可否，DHCP snooping が動作している VLAN リスト情報などを表示します。

運用コマンド show ip dhcp snooping の実行結果を次の図に示します。

図 13-20 show ip dhcp snooping の実行結果（スタック動作時）

```
> show ip dhcp snooping

Date 20XX/12/10 20:45:04 UTC
Switch DHCP snooping is Enable
Option allow untrusted: off,  Verify mac-address: on
DHCP snooping is configured on the following VLANs:
  1-8,2048,4090-4094
Port      Trusted Verify source Rate limit(pps)
1/0/1     no      off           unlimited
1/0/2     no      off           unlimited
1/0/3     no      off           unlimited
     :                :
ChGr:32   no      off           unlimited
ChGr:64   yes     off           unlimited

>
```

(2) バインディングデータベースの確認

バインディングデータベース情報を運用コマンド show ip dhcp snooping binding で表示します。端末の MAC アドレス，IP アドレス，バインディングデータベースのエージング時間などを表示します。

運用コマンド show ip dhcp snooping binding の実行結果を次の図に示します。

図 13-21 show ip dhcp snooping binding の実行結果（スタック動作時）

```
> show ip dhcp snooping binding

Date 20XX/12/10 20:45:08 UTC

Agent URL: -
Last succeeded time: -

Total Bindings: 10
MAC Address     IP Address       Expire(min)  Type      VLAN  Port
0012.e294.86b2  192.168.254.201  1437         dynamic   4094  1/0/1
0012.e294.88b2  192.168.254.202  1438         dynamic   4094  1/0/1
0012.e294.8ab2  192.168.254.203  1439         dynamic   4094  1/0/1
     :                :
0012.e2a5.4241  192.168.254.154  -            static    4094  2/0/3
0012.e2a5.4251  192.168.254.155  -            static    4094  2/0/3

>
```

（3） DHCP snooping 統計情報の確認

DHCP snooping 統計情報を運用コマンド show ip dhcp snooping statistics で表示します。untrust ポートで受信した DHCP 総パケット数，インタフェースごとの受信した DHCP パケット数，フィルタした DHCP パケット数，受信レート制限超過で廃棄した DHCP パケット数を表示します。

運用コマンド show ip dhcp snooping statistics の実行結果を次の図に示します。

図 13-22 show ip dhcp snooping statistics の実行結果（スタック動作時）

```
> show ip dhcp snooping statistics

Date 20XX/12/10 20:45:14 UTC
Database Exceeded: 0
Total DHCP Packets: 78
Port            Recv      Filter   Rate over
1/0/1             35           0           0
1/0/2              0           0           0
1/0/3             23           3           0
     :               :
ChGr:32            0           0           0
ChGr:64            0           0           0
Transmission rate over :          0

>
```

13.3.3 ダイナミック ARP 検査の確認

（1） ダイナミック ARP 検査統計情報の確認

ダイナミック ARP 検査の統計情報を運用コマンド show ip arp inspection statistics で表示します。中継した ARP パケット数，廃棄した ARP パケット数，廃棄 ARP パケット数の内訳を表示します。

運用コマンド show ip arp inspection statistics の実行結果を次の図に示します。

図 13-23　show ip arp inspection statistics の実行結果（スタック動作時）

```
# show ip arp inspection statistics

Date 20XX/12/10 13:09:52 UTC
Port      VLAN   Forwarded      Dropped (  Rate over  DB unmatch     Invalid )
1/0/1       11           0           15 (         0          15           0 )
1/0/2       11         584          883 (         0         883           0 )
1/0/3       11           0            0 (         0           0           0 )

   :                  :

ChGr:64     11         170           53 (         0          53           0 )
Transmission rate over :          0

#
```

14 ホワイトリスト機能【OP-WL】

ホワイトリスト機能は，運用中のネットワーク内で許可されていない端末からの通信の抽出・遮断を行い，ネットワークのセキュリティ性向上を目的とした機能です。この章では，ホワイトリスト機能について説明します。
本機能の使用では，モデルによりオプションライセンス対応が異なります。
【08TF】オプションライセンス必要
【08T】オプションライセンス不要

14.1 解説

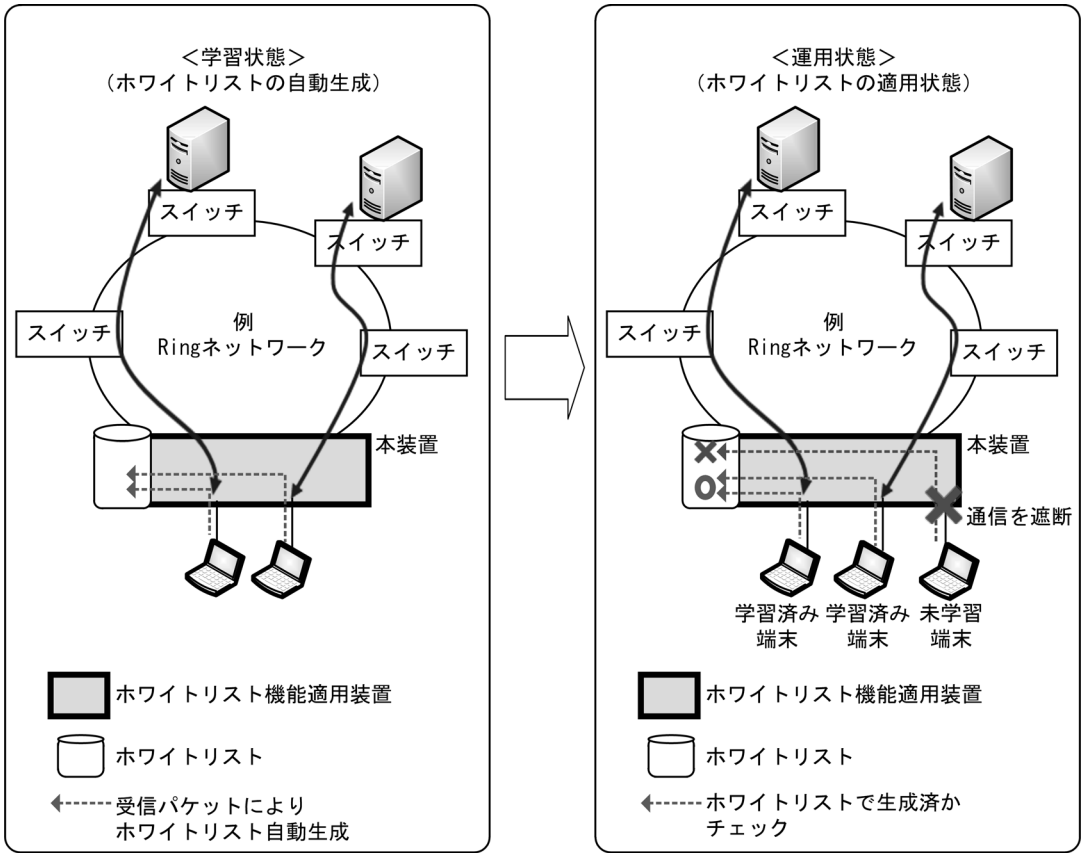
14.1.1 概要

ホワイトリスト機能は，以下の「学習状態」と「運用状態」を切り替えて使用することで，お客様のネットワークのセキュリティの向上を目的とした機能です。

- 学習状態：通信を許可したい端末からの受信パケットでホワイトリストを自動生成
- 運用状態：ホワイトリストに自動生成されていない未学習端末からの通信の抽出・遮断

ホワイトリスト機能の概要を次の図に示します。

図 14-1 ホワイトリスト機能の概要



ホワイトリスト機能は，次に示す手順で運用することで，お客様ネットワークで未学習端末の通信だけを抽出・遮断できます。このとき，学習済み端末の通信への影響はありません。

＜手順＞

1. ホワイトリストの動作対象から除外する trust ポート，または trust モードの情報を設定します。
   - ホワイトリスト機能を有効にしたとき，初期状態では全ポートがホワイトリスト対象ポートとなります。冗長構成の切り替えポートなど，対象から除外するポートをあらかじめ trust ポートとして設定してください。
   - ホワイトリスト対象ポートで，特定のプロトコルをホワイトパケットリストの対象外とする場合は，trust モードを設定してください。
2. ホワイトリストに学習されなかった未学習端末通信の扱いを設定します。以下の項目を設定できます。

- 未学習端末からの受信パケットの廃棄
- 未学習端末から受信した未学習パケット情報を syslog サーバへ出力
- 未学習端末からの受信パケットをミラーリング出力

3. ホワイトリスト機能を学習状態に設定します。
4. ホワイトリスト機能を有効化します。(学習状態開始)
   - 学習状態では，本装置のホワイトリスト対象ポート・対象プロトコルに一致した受信パケットを，ホワイトリストとして学習します。
5. 期待される端末通信が実施され，ホワイトリストの新規学習が落ち着いたら，学習状態を終了し，ホワイトリスト機能を運用状態にします。
   - No.3 および No.4 でホワイトリストに学習された端末の通信は中継します。
   - No.3 および No.4 でホワイトリストに学習されなかった端末通信は，前述の No.2 の設定に従い，「中継」または「廃棄」,「syslog サーバへ出力」,「ミラーリング出力」処理します。

(1) サポート機能

本装置でサポートするホワイトリスト機能を次の表に示します。

表 14-1 本装置でサポートするホワイトリスト機能

機能項目		機能概要
ホワイトリスト共通機能		ホワイトアドレスリスト・ホワイトパケットリスト共通の機能。
	ホワイトリスト機能の有効化	ホワイトリスト機能停止状態からの有効化。
	ホワイトリスト機能の状態変更	ホワイトリスト機能の学習状態と運用状態を切り替える設定。
	trust ポート	特定のポートを trust ポートとして設定し，ホワイトリスト機能の学習・運用から除外。
	未学習パケットの廃棄	運用状態で，未学習パケットを受信したとき廃棄。
	未学習パケット情報の採取	運用状態で，未学習パケットを受信したときに採取
	未学習パケット情報の syslog サーバへの出力と抑止	運用状態で，未学習パケットを受信したときに採取した未学習パケット情報を syslog サーバへ出力およびパケット種別ごとの出力抑止。
	未学習パケットのミラーリング	運用状態で，未学習パケットを受信したときに，当該パケットをミラーリング出力。
	ホワイトリスト情報の表示	ホワイトリスト情報・統計情報を表示。
	ホワイトリストの削除	学習したホワイトリストの一括削除。
ホワイトアドレスリスト機能		通信を許可する端末 MAC アドレスの学習と，当該端末 MAC アドレスの別ポートへの移動を抑止する機能。
	ホワイトアドレスリスト機能停止	ホワイトアドレスリスト機能の学習および運用を停止する機能。
ホワイトパケットリスト機能		通信を許可するフローのフィルタリストの学習と，フィルタリストに非該当のフローを抽出，または廃棄する機能。
	ホワイトパケットリスト動作モード	ホワイトパケットリスト動作モードを以下のパターンから選択可能。 • 動作モード 1（受信パケット種別モード） • 動作モード 2（送信元抽出モード）
	trust モード	特定のプロトコルを trust モードとし，ホワイトパケットリストの学習と運用から除外。 以下のパターンから選択可能。 • trust モード 1(IPv6) • trust モード 2(IPv4・ARP 以外) • trust モード 3(すべて除外し，ホワイトアドレスリスト機能だけを動作させます。) • trust モード 4(IPv4 以外)

機能項目		機能概要
	L4 プロトコル	TCP/UDP のポート番号をフロー条件に含めるか含めないかを選択可能。
	エントリタイマ機能	ホワイトパケットリストエントリを一時的に無効化，および一定時間経過後に当該エントリを自動復旧させる機能。

(2) 用語の定義

本機能で使用する用語の説明を次の表に示します。

表 14-2 本機能で使用する用語の説明

用語	説明
ホワイトリスト機能	通信を許可する端末フィルタの学習・運用の総称。 「ホワイトリスト」の総称で記載している場合は，「ホワイトアドレスリスト」「ホワイトパケットリスト」両方の機能を包含。 「ホワイトアドレスリスト」「ホワイトパケットリスト」機能については，「表 14-1 本装置でサポートするホワイトリスト機能」参照。
学習済み端末	学習状態でホワイトリストに学習された通信許可端末。
未学習端末	ホワイトリストに学習されていない通信不可端末。この端末からの受信パケットは，未学習パケットとして処理。
停止状態	ホワイトリスト機能を有効化するコンフィグレーションが未設定で，ホワイトリスト機能が停止している状態。
学習状態	ホワイトリスト機能により，通信端末 MAC アドレス，フロー条件を学習する状態。
運用状態	学習したホワイトリストを適用し，ポート移動抑止，抽出，廃棄などの通信制御を行う状態。
対象ポート	ホワイトリスト機能の動作対象ポート。 ホワイトリスト機能が有効化された初期状態では，全ポートが対象ポート。
trust ポート	ホワイトリスト機能の動作対象外ポート。
リストエントリ	ホワイトリストで学習した 1 つの通信許可条件。
未学習パケット	ホワイトリストで学習されていない通信条件のパケット。

14.1.2 ホワイトリスト共通機能

(1) ホワイトリスト機能の有効化と排他関係

ホワイトリスト機能は，コンフィグレーションコマンド white-list enable を設定することで有効となります。(スタックと異なり，装置再起動は不要です。)

上記コマンドが未設定の場合も，その他のホワイトリスト機能に関するコンフィグレーションは設定可能ですが，動作は無効です。また，運用コマンドも実行できません。

なお，後述の「コンフィグレーションコマンドとの排他」に該当する場合は，上記コマンドの設定に失敗します。排他のコンフィグレーションコマンドをすべて削除してから，再度設定してください。

(a) コンフィグレーションコマンドとの排他

ホワイトリスト機能の有効化と排他関係となるコンフィグレーションコマンドを次の表に示します。

＜排他条件その 1 ＞

次の表に示すコマンドは設定必須です。

両方未設定の場合，コンフィグレーションコマンド white-list enable を設定できません。表に示すコ

マンドを両方とも設定してから，再度 white-list enable を設定してください。
また，white-list enable を設定済みの場合，表に示すコマンドは削除できません。
なお，IGMP snooping を併用する場合は，システム受信モードを受信条件重視モード（system receive control fine）に設定してください。この場合，"no ip igmp snooping" 設定は不要です。システム受信モードについては，「コンフィグレーションガイド Vol.1　13　装置の管理」を参照してください。

表 14-3　コンフィグレーションの排他条件（その 1）

機能	入力モード	設定必須コマンド
IGMP snooping	(config)#	no ip igmp snooping※
MLD snooping	(config)#	no ipv6 mld snooping

注 ※
IGMP snooping を併用する場合は，コンフィグレーションコマンド system receive control fine を設定してください。no ip igmp snooping は設定不要です。

＜排他条件その 2 ＞
次の表に示すコマンドは排他対象です。
表に示すコマンドが設定済みの場合，コンフィグレーションコマンド white-list enable を設定できません。すべて削除してから再度 white-list enable を設定してください。
また，white-list enable を設定済みの場合，表に示すコマンドは設定できません。

表 14-4　コンフィグレーションの排他条件（その 2）

機能	入力モード	排他コマンド
MAC アドレス学習の抑止	(config)#	no mac-address-table learning
受信側フロー検出モード	(config)#	flow detection mode layer2-3
IEEE802.1X	(config)#	dot1x system-auth-control
Web 認証	(config)#	web-authentication system-auth-control
MAC 認証	(config)#	mac-authentication system-auth-control
DHCP snooping	(config)#	ip dhcp snooping
特定端末への Web 通信不可表示機能	(config)#	access-redirect http port
CFM	(config)#	ethernet cfm enable

また，コンフィグレーションコマンド white-list monitor destination interface で設定したミラーポートは，コンフィグレーションコマンド monitor session source の destination interface に指定できません。

(2) ホワイトリスト機能の状態変更

ホワイトリスト機能の学習状態・運用状態は，コンフィグレーションコマンド white-list learning により変更します。

- 学習状態：white-list learning 設定時
- 運用状態：white-list learning 削除時

未学習状態で white-list learning 未設定のまま本機能を有効化すると，すべての受信パケットが未学習パケットとして処理されます。本機能を有効化する前に，white-list learning を設定してください。

期待される端末通信が実施され，ホワイトリストの学習が落ち着いたら，white-list learning 設定を削除

し，運用状態へ変更してください。

（3） trust ポート

ホワイトリスト機能が有効化されたときの初期状態では，全ポートがホワイトリスト機能の対象ポートとなります。ホワイトリスト機能の対象外にしたいポートは，コンフィグレーションコマンド white-list trust を設定することで，通常ポートとして使用できます。

本設定は，物理ポート単位で設定できます。チャネルグループに設定する場合は，チャネルグループに含まれるすべての物理ポートに white-list trust を設定してください。

ホワイトリスト機能を適用したポートでは，MAC アドレステーブルが学習抑止状態となります。従って，冗長経路構成で経路切り替えが発生した場合，MAC アドレステーブルが新しい経路に追従できずに通信不可となります。経路切り替えを実行するポートは，trust ポートに設定してください。（詳細は，後述の「14.1.5　他機能との共存　（2）冗長機能との併用」を参照してください。）

（4） 未学習パケットの廃棄

運用状態で，ホワイトリスト未学習パケットを受信したとき，コンフィグレーションコマンド white-list action discard の設定により，廃棄できます。

本コマンドを設定しない場合，ホワイトリスト未学習パケットは他機能によって廃棄されない限り，中継または自宛受信として処理されます。詳細は，後述の「14.1.5　他機能との共存　（4）ホワイトリストとアクセスリストとの併用」を参照してください。ただし，未学習パケットの自宛受信の CoS 値は 0 になります。

本設定は，物理ポート単位です。チャネルグループに対して使用したい場合は，チャネルグループに含まれるすべての物理ポートに white-list action discard を設定してください。

なお，「廃棄」を設定した場合でも，以下のパケットは「廃棄」対象外として中継されます。

- trust ポートで受信したパケット
- trust モードに設定したプロトコルのパケット

（5） 未学習パケット情報の採取

運用状態で，ホワイトリスト未学習パケットを受信したとき，装置全体の運用ログとは別に，ホワイトリスト専用ログ情報として未学習パケット情報を採取します。未学習パケット情報は，運用コマンド show white-list miss-hit で確認できます。

表 14-5　未学習パケット情報の項目

項目	内容	備考
未学習パケット採取の判定条件	ホワイトアドレスリストで未学習	どちらかのパケット種別内容を採取
	ホワイトパケットリストで未学習	
	ホワイトアドレスリスト，ホワイトパケットリスト両方で未学習	両方のパケット種別内容を 1 件の未学習パケット情報として採取
未学習パケット情報 1 件あたりの内容	• 受信ポート番号 • VLAN ID • 最初に未学習パケットを受信した日時 • 最後に未学習パケットを受信した日時 • パケット種別内容 • 当該パケット種別内容の受信数	パケット種別内容が同一の場合は 1 件のエントリに集約し，当該パケット種別内容の受信数を計上
収容条件	「コンフィグレーションガイド Vol.1　3　収容条件」参照	※

注 ※
収容条件を超えた場合は，未学習パケットを最後に受信した時間が最も古い時間のエントリを削除し，新規に受信した未学習パケット情報を採取します。

(6) 未学習パケット情報の syslog サーバへの出力と抑止

(a) syslog サーバへの出力

本装置内の未学習パケット情報は装置再起動により消失しますが，コンフィグレーションコマンド white-list action log により，syslog サーバへ出力できます。

syslog サーバへは以下の形式で出力します。

図 14-2 syslog サーバへの出力形式

```
Fac 月 日 時刻 hostname [番号]:    月/日   時刻   ログメッセージ本文
--------------(1)-------------:WHT MM/DD HH:MM:SS Port 0/x VLAN <vlan id> unlisted address <mac>; packet <packet>.
                                                                                    (2)
```

＜図内の表記について＞
(1) syslog サーバへ出力時に付加される情報
(2) ホワイトアドレスリストとホワイトパケットリストの両方で未学習だった場合の形式
ホワイトアドレスリストだけで未学習の場合は address <mac>
ホワイトパケットリストだけで未学習の場合は packet <packet>
図内 (1) 部分の詳細は，後述の「23 ログ出力機能」を参照してください。
図内 (2) の <packet> のメッセージ形式は運用コマンド show white-list miss-hit と同様です。詳細は，「運用コマンドレファレンス 33 ホワイトリスト機能【OP-WL】 show white-list miss-hit」を参照してください。

(b) syslog サーバへの出力抑止

コンフィグレーションコマンド white-list logging filter の指定により，未学習パケット情報の syslog サーバへの出力を抑止することが可能です。

- "address" : ホワイトアドレスリストの未学習パケットを syslog サーバへ出力しません。
- "packet" : ホワイトパケットリストの未学習パケットのうち，指定されたパケット種別の未学習パケットを syslog サーバへ出力しません。

ARP パケットを受信時に，syslog サーバへの出力を抑止する設定を次の表に示します。

表 14-6 syslog サーバへの出力を抑止する設定例

受信パケット	ホワイトリスト		未学習ログ	white-list logging filter 設定		syslog 出力結果
	アドレス	パケット		address	packet	
ARP パケット	学習済	学習済	無	−	−	×
（例）	学習済	未学習	[p] type=arp	−	packet arp	×
	未学習	学習済	[a] mac	address	−	×
	未学習	未学習	[a] mac [p] type=arp	address	packet arp	×

（凡例）
−：未設定
×：出力しない
[a]：ホワイトアドレスリスト未学習パケット情報のログ

[p]：ホワイトパケットリスト未学習パケット情報のログ

(c) ホワイトリスト未学習パケット受信時の syslog 情報追加

コンフィグレーションコマンド white-list logging format-add により，未学習パケット情報を syslog サーバへ出力する際に情報を追加することが可能です。

ホワイトリスト未学習パケット受信時の syslog サーバへの出力情報を次の表に示します。

表 14-7　ホワイトリスト未学習パケット受信時の syslog サーバ出力情報

条件		syslog サーバ出力情報				
white-list logging format-add	未学習パケット種別	ポート	VLAN	区分	送信元 MAC アドレス	送信元 IP アドレス
		Port	VLAN	[a]	mac	sip
address src-ip 未設定時	ARP	○	○	○	○	×
	IPv4	○	○	○	○	×
	その他	○	○	○	○	×
address src-ip 設定時	ARP	○	○	○	○	○※
	IPv4	○	○	○	○	○
	その他	○	○	○	○	×

（凡例）
○：出力する
×：出力しない
※：ARP ヘッダ内の送信元プロトコルアドレス（Sender Protocol Address）
[a]：「表 14-6　syslog サーバへの出力を抑止する設定例」を参照

図 14-3　syslog サーバへの出力形式（syslog 情報追加時）

```
Fac 月 日 時刻 hostname [番号]:     月/日    時刻    ログメッセージ本文
-------------(1)-------------:WHT MM/DD HH:MM:SS Port 0/x VLAN <vlan id> unlisted address <mac> sip=s.s.s.s ; packet <packet>.
                                                                                              (2)          (3)
```

＜図内の表記について＞
(1) syslog サーバへ出力時に付加される情報
(2) コンフィグレーションコマンド white-list logging format-add address src-ip 設定時に追加
図内 (1) 部分の詳細は，後述の「23　ログ出力機能」を参照してください。
図内 (3) の <packet> のメッセージ形式は運用コマンド show white-list miss-hit と同様です。詳細は，「運用コマンドレファレンス　33　ホワイトリスト機能【OP-WL】 show white-list miss-hit」を参照してください。

コンフィグレーションコマンド white-list logging format-add により追加される情報は，syslog サーバへの出力情報にだけ適用されます。運用コマンド show white-list miss-hit の表示内容には適用されません。

(7) 未学習パケットのミラーリング

運用状態で未学習パケットを受信したとき，受信した未学習パケットをミラーリングすることができます。

本機能は，次に示すコンフィグレーションを設定することで動作します。

表 14-8　未学習パケットのミラーリング設定

コマンド	設定項目	備考
white-list action monitor	未学習パケットを受信したときミラーリング対象とする設定	
white-list monitor destination interface	未学習パケットのミラーポートを設定	最大 2 ポート設定可※

注※
ミラーポート数はポートミラーリング機能と合わせて装置全体で最大 4 ポートです。詳細は「26　ポートミラーリング」を参照してください。

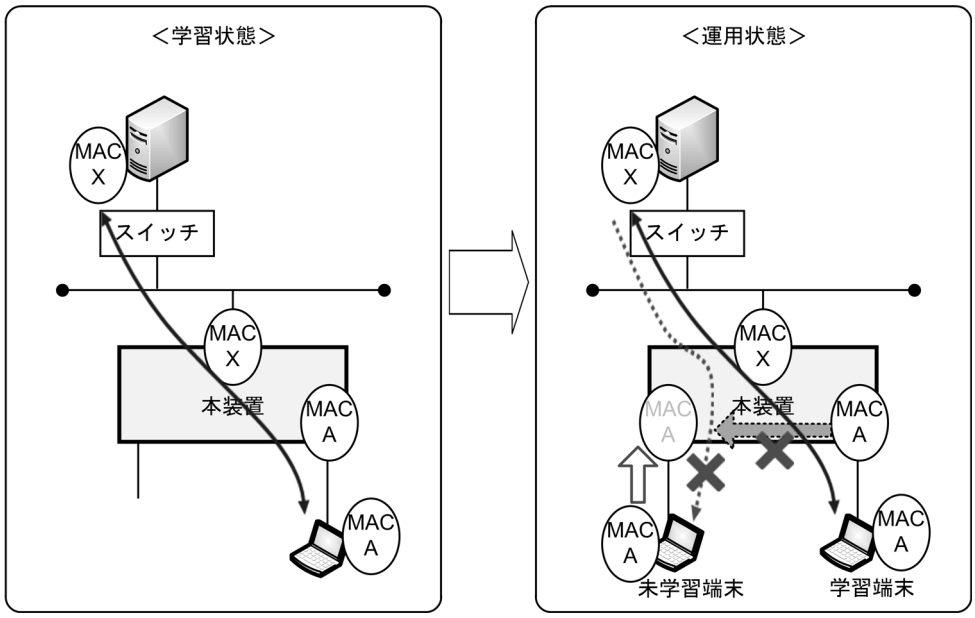
14.1.3　ホワイトアドレスリスト機能

（1）概要

本機能は，学習状態で学習した端末 MAC アドレスとポート番号の組み合わせを保持し，運用状態で端末 MAC アドレスのポート移動を抑止することで，通信妨害・傍受を抑止するための機能です。

本機能は，ホワイトリスト機能を有効化することで動作します。

図 14-4　ホワイトアドレスリスト機能の概要



＜学習状態＞
MAC(A) と MAC(X) の端末間通信により，MAC(A)，および MAC(X) とポート番号の組み合わせを，本装置のホワイトアドレスリストに学習します。

＜運用状態＞
別ポートに MAC(A) を詐称した未学習端末が接続された場合，MAC アドレスのポート移動を抑止しているため，未学習端末の MAC(A) は本装置でポート移動しません。これにより，未許可端末による通信妨害・傍受が抑止されます。

(2) 学習状態

(a) ホワイトアドレスリストの学習の契機

ホワイトアドレスリストは，コンフィグレーションコマンド white-list learning の設定後に学習を開始します。

表 14-9 学習状態の動作

ポート種別	ホワイトアドレスリスト	MAC アドレステーブル	パケット処置
trust ポート	未学習	ダイナミックエントリ登録	中継
対象ポート	学習	スタティックエントリ登録	中継

(b) 学習対象外の MAC アドレス

対象ポートで受信した送信元 MAC アドレスが以下に該当する場合は学習対象外のため，ホワイトアドレスリスト未学習となります。MAC アドレステーブルにも登録しません。

- 非ユニキャスト（先頭バイトの最下位ビットが 1）
- すべてのビットが 0
- 自装置 MAC アドレス

(c) コンフィグレーションとの関係

学習したホワイトアドレスリストとコンフィグレーションとの関係を次の表に示します。

表 14-10 コンフィグレーションとの関係

コンフィグレーション	登録・保存
ランニングコンフィグレーション	登録 ※
スタートアップコンフィグレーションファイル	save コマンド（または copy コマンド）で保存可能

注 ※
ホワイトアドレスリストに学習すると，通常のコンフィグレーションと同様に，コンソールのプロンプトに「！」が表示されます。

コンフィグレーションコマンド mac-address-table static とホワイトアドレスリストの関係を次の表に示します。

表 14-11 コンフィグレーションコマンド mac-address-table static との関係

コマンド設定状態	条件	ホワイトアドレスリスト
設定済み	受信パケットの MAC アドレスと VLAN	同一の場合は学習しない
		異なる場合は学習する
未設定	ホワイトアドレスリストに学習後に mac-address-table static で MAC アドレスと VLAN を追加	一致したホワイトアドレスリストエントリは無効にする ※（mac-address-table static の設定が有効となる）
	同一 MAC アドレスと VLAN の mac-address-table static を削除	一致したホワイトアドレスリストエントリを有効にする

注 ※
運用コマンド show white-list address では，競合したホワイトアドレスリストエントリに「コンフィグレーション優先状態」を示すマークを付加して表示します。

(d) ホワイトアドレスリストの収容条件

ホワイトアドレスリストは「コンフィグレーションガイド Vol.1　3　収容条件」に示すエントリ数まで学習します。収容条件を超過した場合は，運用ログを出力します。

なお，収容条件超過の運用ログをいったん出力後は，以下のいずれかの事象が発生するまで，出力を抑止します。

- 装置再起動
- 学習状態のコンフィグレーション設定
- ホワイトアドレスリストの手動削除
- ホワイトリストエントリの一括削除

(e) ポート移動

MAC アドレスをホワイトアドレスリストで学習した後，同一 MAC アドレスを別ポートで受信した場合を「移動」とします。

学習状態ではエントリの更新処理となり，更新完了までの間は通信不可となります。

詳細は「14.1.6　ホワイトリスト機能使用時の注意事項　(1) ホワイトアドレスリスト機能の注意事項 (a) ホワイトアドレスリスト学習済みの端末 MAC アドレスが別ポートへ移動した場合」を参照してください。

(3) 運用状態

(a) 運用中の動作

ホワイトアドレスリストは，コンフィグレーションコマンド white-list learning の削除後に運用を開始します。

表 14-12　運用状態の動作

ポート種別	ホワイトアドレスリスト	MAC アドレステーブル	パケット処置
trust ポート	チェックしない	既存：登録維持	中継 ※1
		新規：ダイナミックエントリ登録	中継 ※1
対象ポート	学習済み	登録維持	中継
	未学習	未登録（抑止状態）	廃棄 ※2

注 ※1
　通常のフィルタ機能（アクセスリスト）が設定されている場合は，その条件に従います。

注 ※2
　未学習パケットの処理は，コンフィグレーションの設定（white-list action discard）に従います。

(b) コンフィグレーションとの関係

コンフィグレーションコマンド mac-address-table static とホワイトアドレスリストの関係を次の表に示します。

表 14-13 コンフィグレーションコマンド mac-address-table static との関係

条件	ホワイトアドレスリスト
運用中に mac-address-table static で同一 MAC アドレス・VLAN を追加	一致したリストエントリは無効※ （mac-address-table static の設定が有効となる）
同一 MAC アドレス・VLAN の mac-address-table static を削除	一致したリストエントリを復活

注※
運用コマンド show white-list address では，競合したホワイトアドレスリストエントリに「コンフィグレーション優先状態」を示すマークを付加して表示します。

(c) ポート移動

MAC アドレスをホワイトアドレスリストで学習した後，同一 MAC アドレスを別ポートで受信した場合を「移動」とします。

運用状態では，ポート移動した場合は通信不可となります。

詳細は「14.1.6 ホワイトリスト機能使用時の注意事項 (1) ホワイトアドレスリスト機能の注意事項 (a) ホワイトアドレスリスト学習済みの端末 MAC アドレスが別ポートへ移動した場合」を参照してください。

(4) ホワイトアドレスリスト機能の停止

ホワイトアドレスリスト機能は，コンフィグレーションコマンド white-list address trust により停止することが可能です。本機能の停止は装置単位となります。

なお，コンフィグレーションにより本機能を停止した場合，すでに学習済のホワイトアドレスリストは自動的に消去されず，残っています。手動で削除する場合は，運用コマンド erase white-list で削除してください。

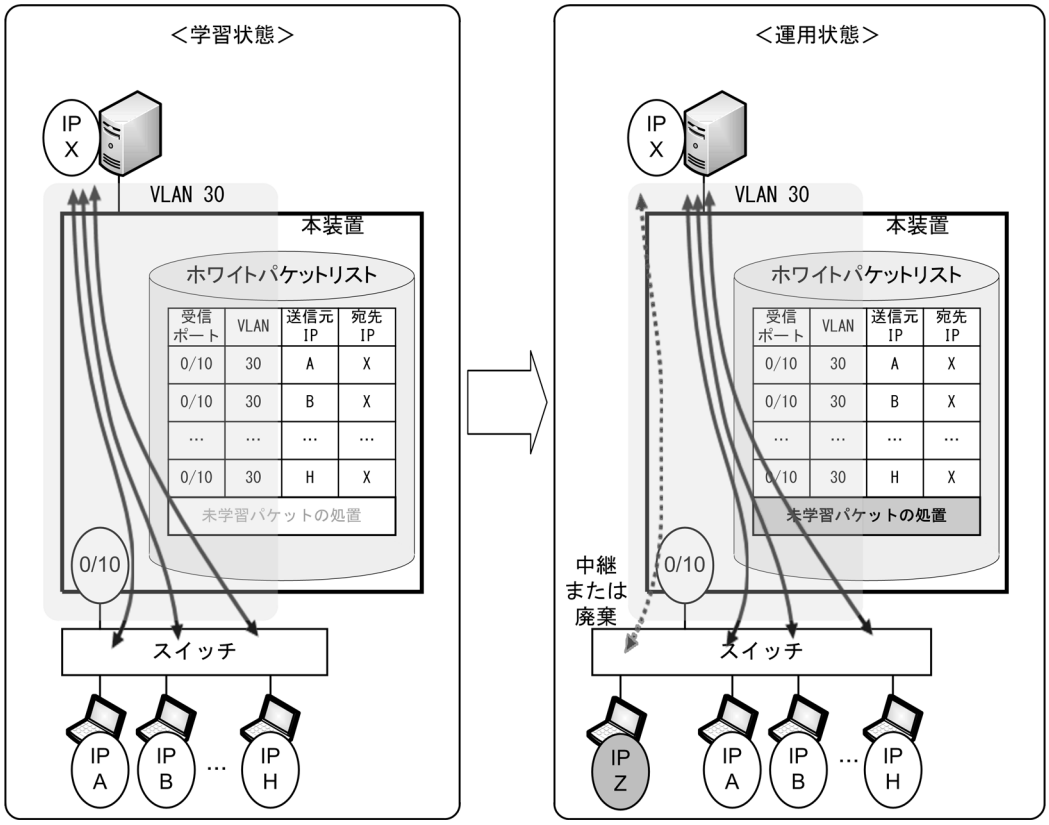
14.1.4 ホワイトパケットリスト機能

(1) 概要

本機能は，コンフィグレーションの設定により学習状態で端末間通信フローを抽出し，フローのフィルタ条件を学習します。運用状態では学習したフローのフィルタ条件に一致しないフローを「14.1.2 ホワイトリスト共通機能 (4) 未学習パケットの廃棄」設定に従って，中継または廃棄します。これにより，不正端末の通信を抑止し，ネットワークセキュリティを向上します。

なお，trust ポートに設定されたポート，trust モードが指定されたプロトコルのパケットを受信した場合は，本機能の適用から除外します。

図 14-5　ホワイトパケットリスト機能の概要



＜学習状態＞

IP(A) ～ IP(H) と IP(X) の端末間の通信フローにより，IP(A) ～ IP(H) のフローフィルタ条件を，本装置のホワイトパケットリストに学習します。

＜運用状態＞

IP(Z) から受信したパケットは，ホワイトパケットリストのフローフィルタ条件に一致しないため，IP(X) との通信は抑止されます。(「未学習パケットの「廃棄」を設定している場合は廃棄しますので，通信は抑止されます。)

(2) 学習状態

(a) ホワイトパケットリスト動作モード

ホワイトパケットリスト動作モードは，受信パケット種別モードと送信元抽出モードがあり，コンフィグレーションコマンド white-list packet mode で選択可能です。

動作モード 1：受信パケット種別モード

受信パケット種別に従いエントリを生成するモードです。ホワイトリスト機能が有効化された初期状態での動作モードです。

受信したパケット種別に従い，「表 14-14　ホワイトパケットリストの学習情報（動作モード 1：受信パケット種別モード)」に示す情報でリストエントリを生成します。

動作モード 2：送信元抽出モード

送信元情報に特化してエントリを生成するモードです。

「表 14-15　ホワイトパケットリストの学習情報（動作モード 2：送信元抽出モード)」に示すように送信元情報に特化したリストエントリを生成します。

表 14-14 ホワイトパケットリストの学習情報（動作モード 1：受信パケット種別モード）

受信パケット	受信ポート	VLAN	MAC アドレス		IP アドレス		プロトコル種別	L4 プロトコル（ポート番号）				その他
								TCP		UDP		
			送信元	宛先	送信元	宛先		送信元	宛先	送信元	宛先	
IPv4	○	○	×	×	○	○	●	●	●	●	●	×
ARP	○	○	○※	×	○※	×	×	×	×	×	×	×
その他	○	○	○	○	×	×	×	×	×	×	×	×

表 14-15 ホワイトパケットリストの学習情報（動作モード 2：送信元抽出モード）

受信パケット	受信ポート	VLAN	MAC アドレス		IP アドレス		プロトコル種別	L4 プロトコル（ポート番号）				その他
								TCP		UDP		
			送信元	宛先	送信元	宛先		送信元	宛先	送信元	宛先	
IPv4	○	○	○	×	○	×	×	×	×	×	×	×
ARP	○	○	○※	×	○※	×	×	×	×	×	×	×
その他	○	○	○	×	×	×	×	×	×	×	×	×

（凡例）

○：ホワイトパケットリストとして学習可能の情報

●：コンフィグレーションコマンド white-list packet tcp/white-list packet udp により学習可能になる情報

×：ホワイトパケットリストとして学習不可の情報

注 ※

ARP ヘッダ内の送信元 MAC アドレス / 送信元プロトコルアドレス（Sender Hardware/Protocol Address）

動作モードを送信元抽出モードで運用する場合は「(g) L4 プロトコル」を併用できません。後述の「14.1.6 ホワイトリスト機能使用時の注意事項 (2) ホワイトパケットリスト機能の注意事項」を参照して動作モードを変更してください。

(b) ホワイトパケットリストの学習の契機

ホワイトパケットリストは，コンフィグレーションコマンド white-list learning の設定後に学習を開始します。

(c) パケット形式

ホワイトパケットリスト機能では，次の表に示す VLAN 識別とフォーマットをサポートします。なお，VLAN トンネリングパケットはホワイトパケットリストで判定しますが，VLAN トンネリング機能を本装置内で併用することはできません。（後述「14.1.5 他機能との共存」を参照してください。）

表 14-16 ホワイトパケットリストでの VLAN 識別

VLAN Tag	識別
Untag	受信した VLAN で識別 • アクセスポートのポート VLAN • トランクポートのネイティブ VLAN
1 段の VLAN Tag	Tag を識別
2 段の VLAN Tag	2 段の Tag の外側 Tag だけを識別

表 14-17 ホワイトパケットリストでのサポートフォーマット

形式	識別
Ethernet V2	
IEEE802.2(LLC/SNAP)	"aa-aa-03-00-00-00" で識別

(d) 学習対象外の MAC アドレス

対象ポートで受信した送信元 MAC アドレスが以下に該当する場合は学習対象外のため，ホワイトパケットリスト未学習となります。

- 非ユニキャスト（先頭バイトの最下位ビットが 1）
- すべてのビットが 0
- 自装置 MAC アドレス

(e) IPv4 パケット

IPv4 パケットについては，以下のとおりホワイトパケットリストで学習するもの，学習せず廃棄するものがあります。

表 14-18 IPv4 パケットの扱い

種類	動作	ホワイトパケットリスト
IP ヘッダ	不正な IP ヘッダを持つパケットを受信した場合は無効扱いとする	学習しない 受信パケットを廃棄
IP フラグメントパケット	非先頭フラグメントパケットのプロトコル情報は認識しない	コンフィグレーションコマンド white-list packet tcp/white-list packet udp を設定したポートは学習しない その他のポートは学習する
IP オプション	IP ヘッダのオプションフィールドの有無を考慮し，L4 プロトコルポート番号を識別	学習する
未指定 IP アドレス	以下を識別 • 送信元 IPv4 アドレスが 0.0.0.0 の IPv4 パケット（DHCP） • ARP パケット（IP アドレス重複確認用）	学習する

(f) trust モードパケット

本機能では，trust モードを設定することで，当該プロトコルの通信をホワイトパケットリストの対象外にすることができます。

trust モードの対象範囲を「図 14-6 trust モードの対象範囲」に，設定可能な trust モードを「表 14-19 設定可能な trust モード」に示します。trust モードは択一指定です。

図 14-6 trust モードの対象範囲

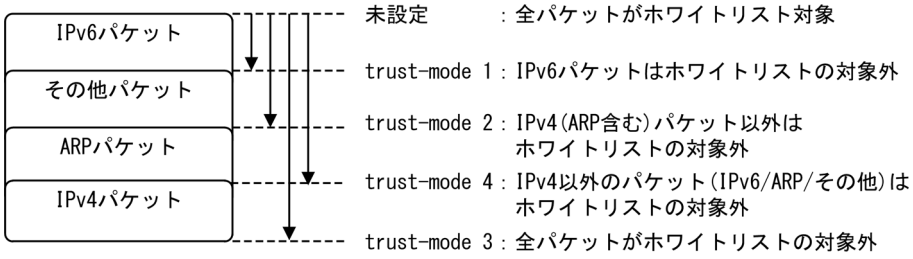


表 14-19 設定可能な trust モード

モード	Ether Type	動作概要
trust モード 1	0x86dd	IPv6 パケットを除外対象とします。
trust モード 2	0x0800	IPv4 パケット・ARP パケット以外のパケットを除外対象とします。
	0x0806	
trust モード 3	すべて	すべてのパケットを除外対象とします。 本モード設定時，ホワイトアドレスリスト機能だけの動作となります。
trust モード 4	0x0800 以外	IPv4 パケット以外のすべてのパケットを除外対象とします。

本コマンドは物理ポート単位で設定できます。チャネルグループに対して設定したい場合は，チャネルグループに含まれるすべての物理ポートに本コマンドを設定してください。

(g) L4 プロトコル

受信した IPv4 の TCP パケットまたは UDP パケットからフロー条件に加えるホワイトパケットリストのポート番号は，コンフィグレーションコマンドによって，次の表に示す種類を設定できます。

表 14-20 L4 プロトコルのフロー条件

種別	コンフィグレーション コマンド	フロー条件	内容
TCP	white-list packet tcp	送信元ポート番号	TCP パケットの送信元ポート番号だけをフロー条件に加えます
		宛先ポート番号	TCP パケットの宛先ポート番号だけをフロー条件に加えます
		送信元・宛先両方のポート番号	TCP パケットの送信元・宛先ポート番号の両方をフロー条件に加えます
		サーバ側ポート番号	TCP パケットのサーバ側ポート番号だけをフロー条件に加えます
UDP	white-list packet udp	送信元ポート番号	UDP パケットの送信元ポート番号だけをフロー条件に加えます
		宛先ポート番号	UDP パケットの宛先ポート番号だけをフロー条件に加えます
		送信元・宛先両方のポート番号	UDP パケットの送信元・宛先ポート番号の両方をフロー条件に加えます

上記コマンドは物理ポート単位で設定できます。チャネルグループに対して設定したい場合は，チャネルグループに含まれるすべての物理ポートに上記コマンドを設定してください。

また，TCP の場合，サーバ側ポート番号を設定することで，送信元 / 宛先といった固定的な指定ではなく，サーバ側のポート番号を動的にホワイトパケットリストのフロー条件に加えることができます。

なお，FTP の場合はプロトコル（RFC959）が特殊であるため，サーバ側ポート番号を指定しても，FTP 動作に効果的ではありません。

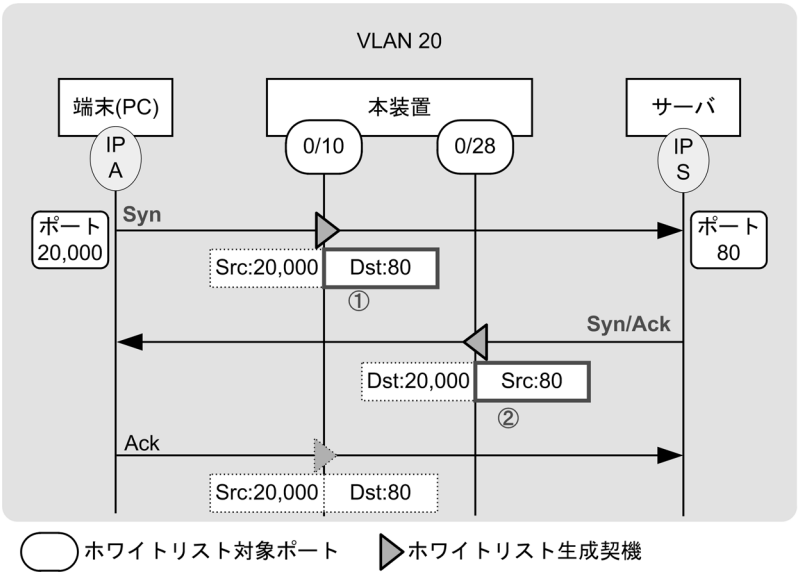
サーバ側ポート番号をフロー条件に指定した例を次に示します。

＜サーバ側ポート番号指定時のフロー条件＞

受信パケットで，かつ TCP の Syn フラグ付きパケット

- Ack フラグ無：宛先ポート番号を登録・・・①
- Ack フラグ有：送信元ポート番号を登録・・②

図 14-7　サーバ側ポート番号指定時の例



ホワイトパケットリスト						
物理ポート	VLAN	送信元IP	宛先IP	送信元ポート	宛先ポート	
0/10	20	A	S	any	80	①の条件で生成
0/28	20	S	A	80	any	②の条件で生成

いったん生成されたホワイトパケットリストエントリは，途中で本コマンドを設定しても影響されません。本コマンド設定の変更後に，新規受信パケットのホワイトパケットリストエントリが，既存のホワイトパケットリストエントリを包含していても，既存のホワイトパケットリストエントリは削除されません。

ただし，新規受信パケットのホワイトパケットリストエントリが，既存のリストエントリに包含される場合は，新規ホワイトパケットリストエントリは生成されません。

(h) コンフィグレーションとの関係

学習したホワイトパケットリストとコンフィグレーションとの関係を次の表に示します。

表 14-21　コンフィグレーションとの関係

コンフィグレーション	登録・保存
ランニングコンフィグレーション	登録※
スタートアップコンフィグレーションファイル	save コマンド（または copy コマンド）で保存可能

注※

ホワイトパケットリストに学習すると，通常のコンフィグレーションと同様に，コンソールのプロンプトに「！」

が表示されます。

(i) ホワイトパケットリストの収容条件

ホワイトパケットリストは「コンフィグレーションガイド Vol.1　3　収容条件」に示すエントリ数まで学習します。収容条件を超過した場合は，運用ログを出力します。

なお，収容条件超過の運用ログをいったん出力後は，以下のいずれかの事象が発生するまで，出力を抑止します。

- 装置再起動
- 学習状態のコンフィグレーション設定
- ホワイトパケットリストの手動削除
- ホワイトリストエントリの一括削除

(j) ポート移動

すでに登録済みのホワイトパケットリストと同一条件のパケットを別ポートで受信した場合を「移動」とします。

移動前後のポートのフロー条件が同一の場合は，ホワイトパケットリストエントリを更新します。フロー条件が異なる場合は，移動前の情報は残存し，新規にホワイトパケットリストエントリを登録します。

学習状態で「移動」を検出した場合の動作を次の表に示します。

表 14-22　学習状態でのポート移動

移動前	移動後		
ポート種別	ポート種別	ホワイトパケットリスト	パケット処置
対象ポート	trust ポート	学習結果維持	中継 ※1
	別対象ポート	更新 ※2	中継 ※1

注 ※1

ホワイトパケットリスト以外の機能で廃棄する場合は中継しません。

注 ※2

移動後ポートのフロー条件（コンフィグレーションコマンド white-list packet tcp/white-list packet udp の設定）が異なる場合は，新規リストエントリ登録となります。

(3) 運用状態

(a) 運用中の動作

ホワイトパケットリストは，コンフィグレーションコマンド white-list learning の削除後に運用を開始します。

表 14-23　運用状態の動作

ポート種別	ホワイトパケットリスト	パケット処置
trust ポート	チェックしない	中継 ※1
対象ポート	学習済み	中継
	未学習	廃棄 ※2

注 ※1

通常のフィルタ機能（アクセスリスト）が設定されている場合は，その条件に従います。

注 ※2
未学習パケットの処理は，コンフィグレーションの設定（white-list action discard）に従います。

(b) ポート移動

すでに学習済みのリストエントリと同一条件となるパケットを，別ポートで受信した場合は「移動」とします。

運用状態で「移動」を検出した場合の動作を次の表に示します。

表 14-24 運用状態でのポート移動

移動前	移動後		
ポート種別	ポート種別	ホワイトパケットリスト	パケット処置
対象ポート	trust ポート	学習結果維持	中継 ※1
	別対象ポート	学習結果維持	廃棄 ※2

注 ※1
ホワイトパケットリスト以外の機能で廃棄する場合は中継しません。

注 ※2
未学習パケットの処理は，コンフィグレーションの設定（white-list action discard）に従います。

(4) エントリタイマ機能

本機能は，サーバ側が不審端末を検出した際，本装置に対して不審端末に関するホワイトパケットリストエントリを一時的に無効化，および一定時間経過後に当該エントリを自動復旧させる機能です。

サーバ側からは，該当端末の送信元 IP アドレス，無効化しているエントリタイマ残時間，タイマ削除を指定可能です。

本装置は全ホワイトパケットリストを検索し，指定された送信元 IP アドレスに該当するエントリをすべて無効化します。なお，無効化しているエントリに該当するパケットは未学習パケットとして処理されます。

(a) 適用範囲

本機能は，ホワイトパケットリストを対象とします。また，「送信元 IP アドレス」は IPv4 アドレスを対象とするため，パケット種別「IPv4」と「ARP」の送信元 IP アドレスが対象となります。

IPv6 を含むその他のパケット種別のエントリは対象となりません。

(b) エントリタイマ機能の指定範囲

サーバからは，プライベート MIB のホワイトリスト情報グループに対して，SNMP Set Request により指定します。（プライベート MIB の詳細は「MIB レファレンス」を参照してください。）

また，運用コマンド (CLI) でも指定可能です。

表 14-25 エントリタイマ指定可能項目

項目	範囲	単位	SNMP	CLI	備考
送信元 IP アドレス	制限なし	−	○	○	
	0	[秒]	×	○	強制的にエントリを復旧

項目	範囲	単位	SNMP	CLI	備考
	1 ～ 2147483647	[秒]	○	○	指定時間から減算していき，0 でエントリ復旧
エントリタイマ削除	MIB ステータスを削除※	－	○	×	

（凡例）○：指定可，×：指定不可

注※：axsWhitelistSrouceBlockRowStatus を "destroy" に設定

(c) サーバインタフェース

サーバからの指定方法は，SNMP マネージャおよび SNMP プロトコルに従ってください。

サーバからの Set Request に対して，本装置は以下を応答します。

表 14-26　Set Request に対するエントリタイマ機能のエラー応答内容

エントリタイマ機能で生じるエラー内容	エラーステータスコード		SNMP Version		
	値	ステータス	v1	v2C	v3
ホワイトリストエントリの一時削除に成功	0	noError	○	○	○
要求された残時間が範囲外のため，実行不可	3	badVaule	○	－	－
	10	wrongValue	－	○	○
エントリタイマ残時間管理領域不足により実行不可	5	genError	○	－	－
	13	resourceUnavailable	－	○	○
その他のエラー※	各種	各種	○	○	○

（凡例）○：応答する　－：対象外

注※：その他の SNMP 関連の各種エラーコードは，「22　SNMP を使用したネットワーク管理」を参照してください。

また，本装置には，対応する SNMP バージョン（v1/v2C/v3）に合わせて，SNMP コンフィグレーション（snmp-server host など）を設定してください。

(d) エントリタイマの動作

エントリタイマ残時間中に，同一送信元 IP アドレスに対するエントリタイマが複数回指定された場合は，指定内容を上書きします。（現在の残時間よりも大きい値で指定された場合は残時間を延長，小さい値で指定された場合は，残時間を短縮します。）

エントリタイマ経過時間（エントリ無効状態）中に，無効指示された IP アドレスを含むホワイトパケットリストが追加された場合は，エントリタイマの対象となります。従って，この場合の追加エントリは自動的に無効状態となり，エントリタイマ残時間 0 になってから有効となります。

エントリタイマが指定された時点で，無効化された IP アドレスを含むホワイトリストエントリが存在しない場合も，エントリタイマの管理対象となります。従って，無効状態のエントリが存在しなくても，エントリタイマが残時間 0 になるまで，エントリタイマの収容条件を消費します。（エントリタイマの収容条件は，「コンフィグレーションガイド Vol.1　3　収容条件」を参照してください。）

14.1.5 他機能との共存

(1) 他機能との併用

ホワイトリスト機能と他機能との併用可否について次の表に示します。

表 14-27 ホワイトリストと他機能との併用可否

項目		併用可否	備考
運用管理	コンソールからのログイン	○	
	リモート運用端末からのログイン	○	
	コンフィグレーションの操作と編集	○	
	ログインセキュリティと RADIUS	○	
	時刻の設定と NTP	○	
	ホスト名と DNS	○	
	省電力機能	○	
	OAN(Open Autonomic Networking)	―	
スタック	スタック	○	※7
ネットワークインタフェース	イーサネット	○	
	リンクアグリゲーション	○	
レイヤ 2 スイッチ	MAC アドレス学習	△	※2
	ポート VLAN	○	
	プロトコル VLAN	×	
	MAC VLAN	×	
	Tag 変換	×	
	VLAN トンネリング	×	
	VLAN Tag の TPID の設定	×	
	L2 プロトコルフレーム透過機能	○	
	ポート間中継遮断	○	
	スパニングツリー	△	※3
	Ring Protocol	△	※3
	IGMP snooping	△	※5
	MLD snooping	×	※1
IP インタフェース	IPv4・ARP・ICMP	○	
	IPv6・NDP・ICMPv6	○	
	DHCP サーバ機能	×	
フィルタ	フロー検出モード	△	※1
	アクセスリスト	△	※4
QoS	フロー検出	△	※4
	帯域監視	○	
	マーカー	○	
	優先度決定	○	
	シェーパ	○	

項目		併用可否	備考
	廃棄制御	○	
レイヤ 2 認証	IEEE802.1X	×	※1
	Web 認証	×	※1
	MAC 認証	×	※1
	マルチステップ認証	×	※4
セキュリティ	DHCP snooping	×	※1
	特定端末への Web 通信不可表示機能	×	※1
冗長化構成による高信頼化機能	GSRP aware	○	
	アップリンク・リダンダント	△	※3
ネットワークの障害検出による高信頼化機能	ストームコントロール	○	
	IEEE802.3ah/UDLD	○	
	L2 ループ検知	○	※6
	CFM	×	
リモートネットワーク管理	SNMP	○	
	ログ出力機能	○	
	sFlow 統計	×	
隣接装置情報の管理	LLDP	○	
ポートミラーリング	ポートミラーリング	○	
	ポリシーベースミラーリング	○	

（凡例）
○：併用可能，×：併用不可，△：一部制限あり　－：未サポート

注 ※1
コンフィグレーションで排他されます。詳細は前述の「14.1.2　ホワイトリスト共通機能　(1) ホワイトリスト機能の有効化と排他関係」を参照してください。

注 ※2
MAC アドレス学習の抑止はコンフィグレーションで排他されます。詳細は前述の「14.1.2　ホワイトリスト共通機能　(1) ホワイトリスト機能の有効化と排他関係」を参照してください。

注 ※3
冗長経路切り替えポートを trust ポートに設定してください。詳細は「(2) 冗長機能との併用」を参照してください。

注 ※4
コンフィグレーションで排他される機能に関連するため，併用が制限されます。

注 ※5
コンフィグレーションコマンド system receive control fine 設定時は併用可能です。

注 ※6
コンフィグレーションコマンド white-list address permit loop-detection 設定時は併用可能です。

注 ※7
AX260A-08TF が対象です。スタックとホワイトリスト機能の併用については，「コンフィグレーションガイド Vol.1　7　スタックの解説【OP-WLE】」を参照してください。

(2) 冗長機能との併用

ホワイトリスト機能は，本装置でサポートするプロトコルの制御フレームに対しても機能します。

ホワイトリスト機能は，本装置を中継するパケットのポート番号，パケット種別などを限定・制限する機能であるため，経路切り替え後 ※1 のポートで受信した未学習パケットは廃棄 ※2 されます。

注 ※1　以下の機能

- スパニングツリー
- Ring Protocol
- GSRP aware
- アップリンク・リダンダント

注 ※2　未学習パケットを「廃棄する」設定の場合

未学習パケットを「中継する」設定の場合でも，切り替え後の受信パケットをすべて「未学習パケット」として CPU 受信するため，装置に対する過度なトラフィックの要因となります。

Ring Protocol などでブロッキング状態のポートで受信したパケットは，ホワイトアドレスリスト，ホワイトパケットリストの既存エントリに一致しない限り，未学習パケットとして扱います。

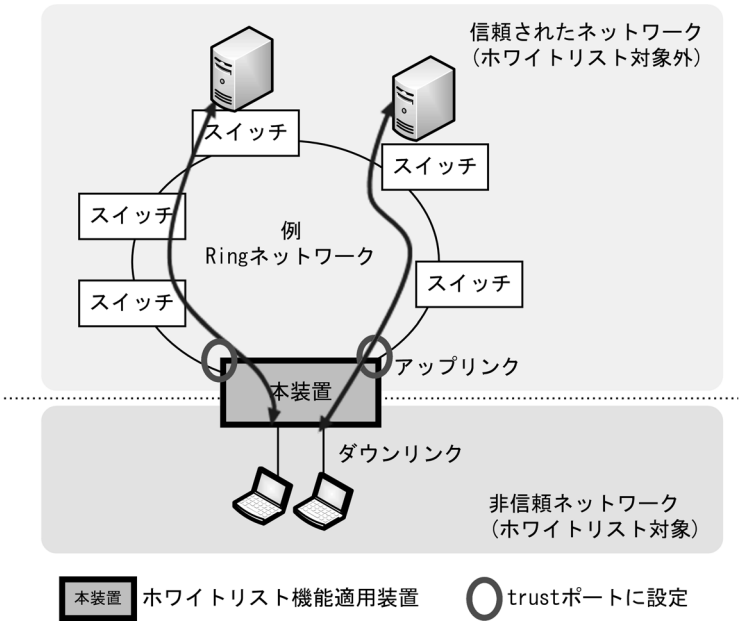
この場合，学習状態ではホワイトリストに学習し，運用状態ではミラーリング・未学習パケット情報の採取の対象となります。

このため，冗長経路を持つ機能と併用する際は，経路が冗長化されるアップリンク側を信頼されたネットワーク，端末接続のダウンリンク側を非信頼ネットワークとする概念でホワイトリスト機能を設定してください。

具体的には，経路切り替えが発生するポートからの受信パケットに対して，ホワイトリスト機能を適用せず，正常に通信できます。

冗長構成の例として，ホワイトリスト機能と Ring ネットワークの併用を次の図に示します。アップリンク側の経路切り替えが発生するポートを trust ポートに設定しています。

図 14-8　ホワイトリスト機能と Ring ネットワークの併用例



（3）L2 ループ検知との併用について

ホワイトリスト機能と L2 ループ検知を併用する場合は，コンフィグレーションコマンド white-list address permit で loop-detection を指定し，MAC アクセスリストで L2 ループ検知フレームを許可する設

定をしてください。設定する L2 ループ検知フレームは「表 14-28　L2 ループ検知で使用するフレーム」を，設定手順については後述の「14.2.5　ホワイトリスト機能と L2 ループ検知の併用」を参照してください。

表 14-28　L2 ループ検知で使用するフレーム

L2 ループ検知で使用するフレーム		MAC アクセスリスト設定例
宛先 MAC アドレス	イーサネットタイプ	
0012.E2E0.0F10 ～ 0012.E2E0.0F50	88F3	permit any 0012.e2e0.0f10 0000.0000.000f 0x88f3
		permit any 0012.e2e0.0f20 0000.0000.000f 0x88f3
		permit any 0012.e2e0.0f30 0000.0000.000f 0x88f3
		permit any 0012.e2e0.0f40 0000.0000.000f 0x88f3
		permit any host 0012.e2e0.0f50 0x88f3
0112.E2E0.0F10		permit any host 0112.e2e0.0f10 0x88f3

(4) ホワイトリストとアクセスリストとの併用

ポートにホワイトパケットリストとアクセスリストを設定して併用した場合，明示的に設定したアクセスリストの条件が優先されます。

＜学習状態＞

アクセスリストで明示的に permit/deny 条件に一致したパケットは，ホワイトパケットリストに学習しません。

＜運用状態＞

アクセスリストで明示的に設定した permit/deny 条件に一致したパケットは，ホワイトパケットリストの有無に依存せず，アクセスリストに従います。

アクセスリストの暗黙の deny となったパケットが，ホワイトリストの対象となります。

なお，VLAN のアクセスリストは，ホワイトリスト機能の動作に影響しません。

(a) 学習状態

ホワイトリストの対象ポートにアクセスリストが設定されている場合，次の表に示すようにアクセスリストの暗黙の deny となったパケットが，ホワイトパケットリストに学習します。

なお，ホワイトアドレスリストは，アクセスリストの条件によらず，ホワイトアドレスリストに学習します。

表 14-29　学習状態でホワイトリストとアクセスリストを併用した場合

アクセスリスト条件	ホワイトリスト				パケット処置
	受信ポート	trust モード ※3	ホワイトパケットリスト	ホワイトアドレスリスト	
permit	trust ポート	－	未学習	未学習	中継
	対象ポート	－	未学習	学習	中継
deny	trust ポート	－	未学習	未学習	廃棄 ※1
	対象ポート	－	未学習	学習	廃棄 ※1

アクセスリスト条件	ホワイトリスト				パケット処置
	受信ポート	trust モード ※3	ホワイトパケットリスト	ホワイトアドレスリスト	
暗黙の deny	trust ポート	－	未学習	未学習	廃棄 ※2
	対象ポート	非該当	学習	学習	中継
		該当	未学習	学習	中継

（凡例）－：条件に依存しない

注 ※1

アクセスリストの deny 条件に一致したため廃棄されます。

注 ※2

trust ポートはホワイトリスト機能の対象外ポートのため，アクセスリストの暗黙の deny と同様に廃棄されます。

注 ※3

該当　：コンフィグレーションコマンド white-list packet trust-mode で指定した，除外対象パケット
非該当：上記に該当しないパケット
trust モードの詳細については，「表 14-19　設定可能な trust モード」を参照してください。

(b) 運用状態

ホワイトリストの対象ポートにアクセスリストが設定されている場合，次の表に示すようにアクセスリストの暗黙の deny となったパケットが，ホワイトリストによって中継・廃棄が決定されます。この場合，アクセスリストの廃棄カウンタは計上されません。

ホワイトパケットリスト・ホワイトアドレスリストで未学習のため廃棄されたパケットは，QoS の帯域計算に反映されます。

表 14-30　運用状態でホワイトリストとアクセスリストを併用した場合

アクセスリスト条件	ホワイトリスト				未学習パケットの処置 ※1				
	受信ポート	trust モード ※2	ホワイトパケットリスト	ホワイトアドレスリスト	パケット処置	ホワイトパケットリスト		ホワイトアドレスリスト	
						未学習情報	ミラーリング	未学習情報	ミラーリング
permit	trust	－	－	－	中継	×	×	×	×
	対象	－	－	未学習	※	×	×	○	○
		－	－	学習済	中継	×	×	×	×
deny	trust	－	－	－	廃棄	×	×	×	×
	対象	－	－	未学習	廃棄	×	×	○	○
				学習済	廃棄	×	×	×	×
暗黙の deny	trust	－	－	－	廃棄	×	×	×	×
	対象	非該当	未学習	未学習	※	○	○	○	○
				学習済	※	○	○	×	×
			学習済	未学習	※	×	×	○	○
				学習済	中継	×	×	×	×
		該当	－	未学習	※	×	×	○	○
				学習済	中継	×	×	×	×

（凡例）－：条件に依存しない　○出力する　×：出力しない

注 ※1

パケット中継・廃棄，未学習情報・ミラーリングの出力有無は，コンフィグレーションの設定に依存します。
詳細は「14.1.2　ホワイトリスト共通機能」を参照してください。

注 ※2

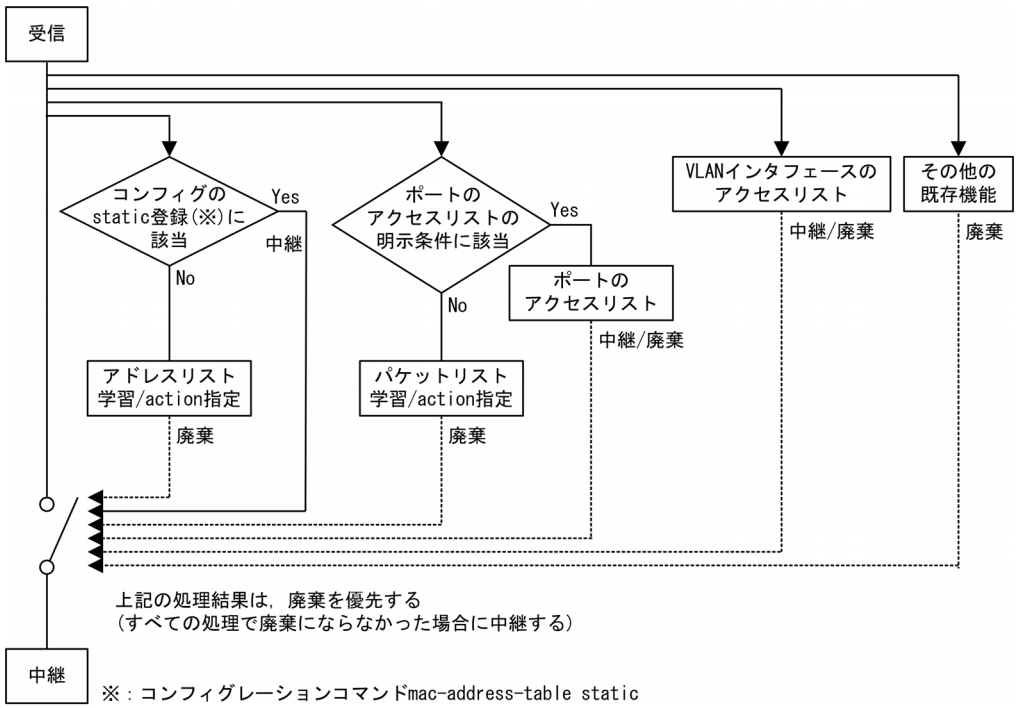
該当　：コンフィグレーションコマンド white-list packet trust-mode で指定した，除外対象パケット
非該当：上記に該当しないパケット
trust モードの詳細については，「表 14-19　設定可能な trust モード」を参照してください。

また，次に示す機能を併用した場合，すべての機能が並列で判定された結果，廃棄が優先されます。このとき，それぞれの統計情報に計上されます。

- ホワイトアドレスリストによる廃棄
- ホワイトパケットリストによる廃棄
- VLAN インタフェースのアクセスリストによる廃棄
- その他（ポート移動による廃棄，QoS 最大帯域監視による廃棄など）

次の図に機能併用時の判定イメージと廃棄優先を示します。

図 14-9　機能併用時の判定イメージと廃棄優先



14.1.6　ホワイトリスト機能使用時の注意事項

（1）ホワイトアドレスリスト機能の注意事項

ホワイトアドレスリスト機能には以下の注意事項があります。

(a) ホワイトアドレスリスト学習済みの端末 MAC アドレスが別ポートへ移動した場合

ホワイトリスト機能と L2 ループ検知を併用しない設定（white-list address permit loop-detection 設定無）で，ホワイトアドレスリスト学習済みの端末 MAC アドレスを送信元とするパケットを別ポートから受信した場合は，受信ポートにコンフィグレーションコマンド white-list action discard 未設定でも廃棄

します。また，trust ポートから受信した場合も廃棄します。

表 14-31 ホワイトアドレスリスト学習済みの端末 MAC アドレスが別ポートへ移動した場合

white-list address permit loop-detection 設定有無	装置状態	受信ポート種別	動作
設定無	学習状態	trust ポート	学習対象外ポートのためホワイトアドレスリストは更新しません。 受信パケットは廃棄します。
		対象ポート	学習状態のエントリが更新完了するまで廃棄します。
	運用状態	trust ポート	廃棄します。
		対象ポート	廃棄します。white-list action discard の設定有無には依存しません。
設定有	学習状態	trust ポート	廃棄しません。
		対象ポート	廃棄しません。
	運用状態	trust ポート	廃棄しません。
		対象ポート	white-list action discard 設定有：廃棄します。 white-list action discard 設定無：廃棄しません。

(b) コンフィグレーションとの関係

コンフィグレーションコマンド mac-address-table static と同一 VLAN・MAC アドレスのパケットを受信した場合は，コンフィグレーションを優先し，ホワイトアドレスリストには学習しません。

(c) ポート移動と MAC アドレステーブルの更新について

ホワイトアドレスリスト機能動作時に該当端末をポート移動した場合，MAC アドレステーブルの更新は以下の動作となります。

＜学習状態＞

当該 MAC アドレスが既に trust ポートで登録済の場合は，対象ポートで当該 MAC アドレスのパケットを受信したときに，新たに学習して MAC アドレステーブルに登録します。
当該 MAC アドレスが既に他の対象ポートで登録済の場合も同様です。
ただし，対象ポートで登録済 MAC アドレスの端末が，trust ポートに移動した場合は，当該 MAC アドレスは "White" エントリとして登録されているため削除されません。コンフィグレーションコマンド white-list data を使用して削除できます。

＜運用状態＞

① MAC アドレステーブル未登録の端末から受信した場合
MAC アドレステーブルに登録しません。従って，この MAC アドレス宛の通信はフラッディング転送となります。

② MAC アドレステーブル登録済の端末から受信した場合
当該 MAC アドレスが既に trust ポートで登録済の場合，"Dynamic" エントリのためエージングタイムアウトするまで通信不可ですが，その後は通信可能となります（ただし，フラッディング転送です)。
当該 MAC アドレスが既に他の対象ポートで登録済の場合，"White" エントリとして登録されているため削除されません。コンフィグレーションコマンド white-list data を使用して削除できます。

(2) ホワイトパケットリスト機能の注意事項

ホワイトパケットリスト機能の注意事項を次の表に示します。

表 14-32 ホワイトパケットリスト機能の注意事項

項目	制限内容
ホワイトパケットリスト動作モード	動作モードの変更は，ハードウェアの動作条件を設定するものであるため，変更する場合はホワイトリスト機能を停止し，学習されているホワイトパケットリスト情報をすべて削除する必要があります。 ホワイトパケットリスト動作モードを設定または削除する前に，必ずコンフィグレーションコマンド white-list enable を削除し，運用コマンド erase white-list packet all を実行してください。
	動作モードを変更する前に，コンフィグレーションコマンド white-list packet tcp/ white-list packet udp を設定しているポートがある場合はすべて削除してください。
L4 無効パケット	コンフィグレーションコマンド white-list packet tcp/white-list packet udp を設定時，非先頭フラグメントパケットは，L4 プロトコルのポート番号が「無効」扱いとなり，ホワイトパケットリストエントリを生成せず，未学習となります。
認証ヘッダ	protocol=51 が付与されているパケットは未サポートです。
IP トンネリング	protocol=4 が付与されているパケットは，外側の IP ヘッダを用いてホワイトパケットリストエントリを生成します。内側の IP ヘッダ，および内側の IP ヘッダに記載されている L4 プロトコル情報は認識しません。
不正 VLAN パケット	受信ポートに属していない VLAN のパケットを受信した場合，ホワイトアドレスリスト，ホワイトパケットリストの既存エントリに一致しないかぎり，未学習パケットとして扱います。 学習状態：ホワイトリストエントリを生成し，廃棄 運用状態：廃棄
ポート閉塞	Ring Protocol などによるブロッキング状態のポートで受信したパケットは，ホワイトアドレスリスト，ホワイトパケットリストの既存エントリに一致しないかぎり，未学習パケットとして扱います。 学習状態：ホワイトリストエントリを生成し，廃棄 運用状態：廃棄

(a) 運用コマンドの表示について

運用コマンド show white-list packet とその他の運用コマンドのホワイトパケットリスト表示順序は一致しない場合があります。

- 運用コマンド show running-config，show startup-config
  ホワイトリスト自動学習順，またはコンフィグレーションコマンド white-list data 登録順に表示されます。
- 運用コマンド show white-list packet
  ホワイトリストエントリの昇順に表示されます。

(b) IP アドレスマスクを指定したエントリについて

IP アドレスマスクのエントリに包含される IP アドレスが複数存在したときは，表示順と異なるエントリにパケット数が計上される場合があります。

コンフィグレーションコマンド white-list data で包含される IP アドレスエントリを削除して運用することを推奨します。

(3) コンフィグレーション変更時

(a) コンフィグレーションの変更・削除した場合

いったん学習したホワイトアドレスリスト，ホワイトパケットリストは，ホワイトリストのコンフィグレーションを変更または削除しても，自動的に削除または更新されません。

また，インタフェース・IP アドレス・VLAN などホワイトリスト機能以外のコンフィグレーション変更に

伴い，無意味な条件となった場合でも，自動的に削除または更新されません。

他のコンフィグレーションを変更した場合は，それに合わせたホワイトアドレスリスト，ホワイトパケットリストを更新してください。

(b) 物理ポートで学習後にチャネルグループに所属させた場合

物理ポートで学習したホワイトパケットリストエントリは，当該ポートをチャネルグループに所属させた後も有効です。

(4) 未学習パケットを廃棄しない場合

未学習パケットを廃棄しない場合，ホワイトアドレスリスト未学習・ホワイトパケットリスト学習済みのAXRP パケットは，未学習パケット扱いになりません。ホワイトパケットリストに一致したものとして処理されます。

(5) 未学習パケット情報の syslog サーバ出力について

未学習パケット情報の syslog サーバ出力は，装置全体で 200 ミリ秒ごとに 1 個に制限されます。

本制限は固定値で変更できません。

(6) 未学習パケットのミラーリングについて 【08TF】

未学習の Untagged パケットをミラーリングした場合，ミラーポートからは Tagged パケットが送信されます。

(7) ホワイトリスト学習状態中の装置スリープについて

ホワイトリスト機能の学習状態中に，省電力機能の装置スリープのスケジュール実行時間帯になった場合，スリープ状態から復帰したとき，save コマンドで保存していないホワイトリストは消失します。

14.2 コンフィグレーション

14.2.1 コンフィグレーションコマンド一覧

ホワイトリストのコンフィグレーションコマンド一覧を次の表に示します。

表 14-33 コンフィグレーションコマンド一覧

コマンド名	説明
white-list action discard	ホワイトリストの運用状態で，当該ポートで受信したホワイトリスト未学習パケットを廃棄します。
white-list action log	ホワイトリストの運用状態で，当該ポートで受信したホワイトリスト未学習パケット情報を syslog サーバへ出力します。
white-list action monitor	ホワイトリストの運用状態で，当該ポートで受信したホワイトリスト未学習パケットをミラーリング対象に設定します。
white-list address permit	指定機能の制御フレームを，ホワイトアドレスリスト対象外にします。
white-list address trust	ホワイトアドレスリスト機能を無効に設定します。
white-list data	ホワイトリスト機能のパケット条件付きコマンドです。
white-list enable	本装置でホワイトリスト機能を有効にします。
white-list learning	本装置でホワイトリスト機能の学習（ホワイトリスト生成）を開始します。
white-list logging filter	white-list action log コマンドを設定時に，ホワイトリスト未学習パケットを syslog サーバへ出力する際のパケット種別を制限します。
white-list logging format-add	ホワイトリスト未学習パケットを syslog サーバへ出力する際の情報を追加します。
white-list monitor destination interface	white-list action monitor コマンドを設定したポートで受信した，ホワイトリスト未学習パケットのミラーポートを設定します。
white-list packet mode	ホワイトパケットリスト機能の動作モードを設定します。
white-list packet tcp	ホワイトパケットリストのフロー条件に TCP ポート番号を含めます。
white-list packet trust-mode	ホワイトパケットリスト機能の trust モードを設定します。
white-list packet udp	ホワイトパケットリストのフロー条件に UDP ポート番号を含めます。
white-list trust	ホワイトリスト機能の trust ポートを設定します。

14.2.2 ホワイトリストの条件の設定と学習の開始

ホワイトアドレスリストの場合，trust ポートの設定以外に条件の指定はありません。以降はホワイトパケットリストのフロー条件の設定となります。フロー条件を設定後，ホワイトリスト機能を有効にして，学習を開始します。

＜設定手順＞

1. trust ポートの設定
2. trust モードパケットの設定
3. ホワイトパケットリストのフロー条件の設定
4. ホワイトリストの学習状態を設定
5. ホワイトリスト機能を有効にして，ホワイトリストの学習を開始する

（1） trust ポートの設定

ホワイトリストの学習・運用から除外する trust ポートを設定します。本設定のポートはホワイトアドレ

スリスト・ホワイトパケットリストの有無に関わりなく，受信パケットを中継します。

［設定のポイント］
冗長機能の切り替えポートなど，ホワイトリストの有無に関わりなく中継するポートに設定します。

［コマンドによる設定］

1. **(config)# interface gigabitethernet 0/10**
   (config-if)# white-list trust
   (config-if)# exit
   ポート 0/10 を trust ポートに設定します。本設定により，当該ポートはホワイトアドレスリスト・ホワイトパケットリストの学習状態・運用状態から除外されます。

(2) ホワイトパケットリストのフロー条件の設定

ホワイトパケットリストから除外する trust モードパケット，ホワイトパケットリストに含める TCP ポート番号や UDP ポート番号のフロー条件を設定します。

(a) trust モードパケットの設定

本設定はホワイトパケットリストの学習状態・運用状態に対して有効になります。

［設定のポイント］
ホワイトパケットリストの学習状態・運用状態で，trust モードパケットを設定します。

［コマンドによる設定］

1. **(config)# interface gigabitethernet 0/1**
   (config-if)# white-list packet trust-mode 2
   (config-if)# exit
   ポート 0/1 の受信パケットのうち，IPv4 パケットおよび ARP パケット以外を，ホワイトパケットリストの判定対象から除外します。

(b) TCP ポート番号を含める設定

本設定はホワイトパケットリストの学習状態に対して有効になります。

［設定のポイント］
ホワイトパケットリストのフロー条件に TCP ポート番号を含める設定をします。
TCP ポート番号は，送信元，宛先，送信元・宛先，サーバ側ポート番号の 4 種類から 1 種類を選択します

［コマンドによる設定］

1. **(config)# interface gigabitethernet 0/2**
   (config-if)# white-list packet tcp both
   (config-if)# exit
   ポート 0/2 のフロー条件に TCP 送信元ポート番号・宛先ポート番号の両方を含めるよう設定します。

(c) UDP ポート番号を含める設定

本設定はホワイトパケットリストの学習状態に対して有効になります。

［設定のポイント］

ホワイトパケットリストのフロー条件に UDP ポート番号を含める設定をします。

TCP ポート番号は，送信元，宛先，送信元・宛先ポート番号の 3 種類から 1 種類を選択します

［コマンドによる設定］

1. **(config)# interface gigabitethernet 0/3**
   (config-if)# white-list packet udp source
   (config-if)# exit
   ポート 0/3 のフロー条件に UDP 送信元ポート番号を含めるよう設定します。

(3) ホワイトリストの学習状態を設定する

［設定のポイント］

ホワイトリスト機能を有効化する前に，ホワイトリストの学習状態を設定します。

［コマンドによる設定］

1. **(config)# white-list learning**
   ホワイトリストの学習状態を設定します。本コマンドを削除するまで，本装置は受信パケットによるホワイトリストの学習状態となります。

(4) ホワイトリスト機能を有効にする

［設定のポイント］

ホワイトリストの条件と学習状態を設定後，ホワイトリスト機能を有効にします。

［コマンドによる設定］

1. **(config)# white-list enable**
   ホワイトリスト機能を有効にします。本コマンド設定後，ホワイトリストの学習を開始します。

   ［注意事項］

   「14.1.2　ホワイトリスト共通機能　(a) コンフィグレーションコマンドとの排他」を参照し，排他条件に該当するコンフィグレーションコマンドの設定有無を確認してください。排他条件に該当すると，white-list enable を設定できません。

14.2.3　学習したホワイトリストの運用

ホワイトリストを運用状態に切り替える前に，ホワイトリスト未学習パケットを受信したときの処理を設定します。未学習パケットに対して，廃棄・syslog サーバへの出力・ミラーリングを設定できます。この設定は，運用状態で有効になりますので，学習中に設定しておくことをお奨めします。

未学習パケットの処理を設定後，学習を停止し運用状態に切り替えます。

(1) 未学習パケットの処理を設定する

運用中に未学習パケットを受信した場合の処理を各ポートに設定します。

(a) 未学習パケットを廃棄

［設定のポイント］

未学習パケットを受信したときに廃棄するよう設定します。本処理を未設定のポートで未学習パケッ

トを受信した場合は中継します。

［コマンドによる設定］

1. **(config)# interface gigabitethernet 0/2**
   (config-if)# white-list action discard
   (config-if)# exit
   ポート 0/2 で未学習パケットを受信した場合は廃棄するよう設定します。

［注意事項］

ホワイトリスト学習状態では，本設定は無効です。

(b) 未学習パケットを syslog サーバへ出力

［設定のポイント］

1. 未学習パケット情報を syslog サーバへ出力するよう設定します。
2. コンフィグレーションコマンド logging event-kind で "wht" 以外が指定されている場合は，"wht" を設定します。(logging event-kind 未設定の場合は，設定不要です。)
3. 送信先 syslog サーバは設定済みとします。

［コマンドによる設定］

1. **(config)# interface gigabitethernet 0/2**
   (config-if)# white-list action log
   (config-if)# exit
   ポート 0/2 で受信した未学習パケットを syslog サーバへ送信するよう設定します。

2. **(config)# logging event-kind wht**
   コンフィグレーションコマンド logging event-kind で "wht" 以外が指定されている場合は，上記のように "wht" を設定してください。logging event-kind 未設定の場合は，デフォルトコンフィグレーションで "wht" が有効になっているため，設定不要です。

［注意事項］

1. ホワイトリスト学習状態では，white-list action log 設定は無効です。
2. 未学習パケットに関する syslog サーバへの出力は，装置全体で 200 ミリ秒ごとに 1 個です。

(c) 未学習パケットの syslog サーバへの出力を抑止するパケット種別を指定

前述の「(b) 未学習パケットを syslog サーバへ出力」に，出力を抑止するパケット種別の設定を追加します。

［設定のポイント］

［コマンドによる設定］

ホワイトアドレスリストと，ARP パケットの未学習パケットは syslog サーバへの出力を抑止します。

1. **(config)# interface gigabitethernet 0/2**
   (config-if)# white-list logging filter address
   (config-if)# white-list logging filter packet arp
   (config-if)# exit
   ポート 0/2 で受信した未学習パケットのうち，ホワイトアドレスリストと ARP パケットは syslog サーバへの出力を抑止するよう設定します。

(d) 未学習パケットの syslog サーバへの出力時の情報を追加

前述の「(b) 未学習パケットを syslog サーバへ出力」の出力情報に，ホワイトリスト未学習パケットの送信元情報を追加します。

[設定のポイント]

ホワイトアドレスリスト未学習パケットの送信元 IP アドレスを追加します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 0/2**
   (config-if)# white-list logging format-add address src-ip
   (config-if)# exit
   ポート 0/2 で受信したホワイトアドレスリスト未学習パケットに送信元 IP アドレス情報を追加して syslog サーバへの出力するよう設定します。

(e) 未学習パケットをミラーリング

[設定のポイント]

1. 未学習パケットをミラーリング対象とするポートに，コンフィグレーションコマンド white-list action monitor を設定します。
2. 未学習パケットのミラーポートを，コンフィグレーションコマンド white-list monitor destination interface で設定します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 0/2**
   (config-if)# white-list action monitor
   (config-if)# exit
   ポート 0/2 で受信した未学習パケットのミラーリングを設定します。

2. **(config)# white-list monitor destination interface gigabitethernet 0/10**
   ポート 0/2 で受信するホワイトリスト未学習パケットのミラーポートとして，ポート 0/10 を設定します。

[注意事項]

1. ホワイトリスト学習状態では，white-list action monitor 設定は無効です。
2. ミラーポートの制限については，「26　ポートミラーリング」を参照してください。

(2) ホワイトリストの学習を停止し，運用を開始する

[設定のポイント]

ホワイトリストの学習を停止することで，本装置はホワイトリストの運用状態に切り替わります。

[コマンドによる設定]

1. **(config)# no white-list learning**
   ホワイトリストの学習を停止し，ホワイトリストによる運用を開始します。運用開始後は，ホワイトリスト未学習パケットを受信したとき，前述の action 設定に従って処理されます。

（3） ホワイトアドレスリスト機能を停止する

［設定のポイント］

ホワイトアドレスリスト機能だけを停止します。これに伴い，ホワイトアドレスリスト機能の学習・運用が停止します。

［コマンドによる設定］

1. **(config)# white-list address trust**
   ホワイトアドレスリスト機能を停止します。

［注意事項］

1. すでに学習済のホワイトアドレスリストは自動的に消去されず，残っています。手動で削除する場合は，運用コマンド erase white-list で削除してください。
2. 本コマンドを削除して，ホワイトアドレスリスト機能を有効に戻した場合，MAC アドレステーブルのダイナミックエントリはすべて削除されます。

14.2.4 学習済みホワイトリストの追加と保存

（1） 学習済みのホワイトリストに新規リストを追加学習させる

運用開始後に，ホワイトリストを追加する場合は，いったん学習状態に戻してください。

［設定のポイント］

運用を停止し，学習状態に戻します。このとき，ホワイトリストのフロー条件を追加するポートがある場合は，設定を追加してください。

［コマンドによる設定］

1. **(config)# white-list learning**
   ホワイトリストの学習を開始します。
   学習終了後，「(2) ホワイトリストの学習を停止し，運用を開始する」を参照し，運用状態に戻してください。

（2） 学習済みのホワイトリストに新規リストを手動で追加または削除する

運用中に通信端末故障で端末の入れ替えが発生した場合など，リストエントリの編集が必要な際にご利用いただけます。

学習済みのホワイトリストは，コンフィグレーションコマンド white-list data として自動設定されており，運用コマンド show running-config で，以下のいずれかの形式で表示されます。下線部はリストエントリ部分を示しています。

なお，ホワイトパケットリスト動作モードにより「IPv4 パケット」と「IPv4/ARP 以外のパケット」は表示項目が異なります。

図 14-10 show running-config の表示形式

```
＜ホワイトアドレスリスト＞
white-list data "a <mac> v <vlan id> p <IF#>"
white-list data "a <mac> v <vlan id> c <channel group>"

＜ホワイトパケットリスト（IPv4）＞［動作モード1：受信パケット種別モード］
white-list data "p <IF#> v <vlan id> ip {<src ip> | <src ip>/<masklen>} {<dest
ip> | <dest ip>/<masklen>} [<protocol> [s <src port>] [d <dst port>]]"
white-list data "p c <channel group> v <vlan id> ip {<src ip> | <src ip>/
<masklen>} {<dest ip> | <dest ip>/<masklen>} [<protocol> [s <src port>] [d <dst
```

port>ll"

＜ホワイトパケットリスト（IPv4）＞［動作モード2：送信元抽出モード］
white-list data "p <IF#> v <vlan id> ip <src mac> <src ip>"
white-list data "p c <channel group> v <vlan id> ip <src mac> <src ip>"

＜ホワイトパケットリスト（ARP）＞
white-list data "p <IF#> v <vlan id> arp <src mac> <src ip>"
white-list data "p c <channel group> v <vlan id> arp <src mac> <src ip>"

＜ホワイトパケットリスト（IPv4/ARP以外）＞［動作モード1：受信パケット種別モード］
white-list data "p <IF#> v <vlan id> <src mac> <dst mac>"
white-list data "p c <channel group> v <vlan id> <src mac> <dst mac>"

＜ホワイトパケットリスト（IPv4/ARP以外）＞［動作モード2：送信元抽出モード］
white-list data "p <IF#> v <vlan id> <src mac>"
white-list data "p c <channel group> v <vlan id> <src mac>"

キーワード：a，p，c，v，ip，s，d，arp
設定値　　：< >で表示しているパラメータ名

［設定のポイント］

運用コマンド show running-config で学習されているホワイトリスト (white-list data) を確認してください。
コンフィグレーションコマンド white-list data で設定を変更します。リストエントリ部分は，上図に示すリストの形式に従って，ダブルクォートで囲んで入力してください。
本コマンドは手動設定を意図したコマンドではないため，パラメータの書式を誤らないように慎重に操作してください。

［コマンドによる設定］（追加）

1. **(config)# white-list data "a 0012.e200.ff00 v 4094 p 0/1"**
   ポート 0/1 にホワイトアドレスリストを追加します。

［コマンドによる設定］（追加したエントリを削除）

1. **(config)# no white-list data "a 0012.e200.ff00 v 4094 p 0/1"**
   追加した内容を削除する場合は，［↑］で入力した内容を表示させ，先頭に "no" を追加して削除してください。

［コマンドによる設定］（学習済みのエントリを削除）

1. **# show running-config**
   （省略）
   white-list data "p 0/3 v 1000 arp 0012.e234.0006 192.168.254.106"
   運用コマンド show running-config でエントリを表示させます。

2. **# configure**
   (config)#
   コンフィグレーションモードへ遷移します。

3. **(config)# no white-list data "p 0/3 v 1000 arp 0012.e234.0006 192.168.254.106"**
   該当行をコピー＆ペーストし，先頭に "no" を追加して削除してください。

［注意事項］

1. ポート番号またはチャネルグループ番号が異なる場合は，当該エントリが上書きされます。

2. 下線部のシンタックスチェック，補完機能，ヘルプ機能は実施されません。
3. ダブルクォート内の書式は，上記のいずれかの形式で入力されることを前提とします。
4. キーワードや設定値の入力順が不正な場合は，装置に正しく反映されない場合があります。
5. キーワードを含む設定値はすべて小文字で入力してください。
6. キーワードと設定値の間はスペース 1 文字を入力してください。

(3) 学習したホワイトリストを保存する

学習したホワイトリストはランニングコンフィグレーションに自動設定されています。通常のコンフィグレーションと同様に save コマンドでスタートアップコンフィグレーションファイルに保存できます。

14.2.5 ホワイトリスト機能と L2 ループ検知の併用

ホワイトリスト機能使用時に，L2 ループ検知フレームを透過させる場合の設定例です。

[設定のポイント]

L2 ループ検知を併用する場合は，MAC アクセスリストも使用しますので，本設定の最初に受信側フロー検出モードを設定してください。

＜設定項目＞

- 受信側フロー検出モード layer2-1
- MAC アクセスリストで中継を許可する L2 ループ検知フレームを指定
  本例では 1 リストの設定例を示します。L2 ループ検知フレームの設定範囲は，前述の「表 14-28　L2 ループ検知で使用するフレーム」を参照してください。
- ホワイトリスト機能と L2 ループ検知併用の設定
- L2 ループ検知の有効化
  （その他の L2 ループ検知に必要なコンフィグレーションは設定済とします。）
- ホワイトリスト機能の有効化

[コマンドによる設定]

1. **(config)# flow detection mode layer2-1**
   受信側フロー検出モードを layer2-1 に設定します。

2. **(config)# mac access-list extended PERMIT_L2LD**
   (config-ext-macl)# permit any host 0012.e2e0.0f10 0x88f3
   (config-ext-macl)# exit
   MAC アクセスリストに，許可する L2 ループ検知フレームを設定します。

3. **(config)# interface gigabitethernet 0/1**
   (config-if)# mac access-group PERMIT_L2LD in
   (config-if)# exit
   ポート 0/1 に MAC アクセスリスト PERMIT_L2LD を割り当てます。

4. **(config)# white-list address permit loop-detection**
   L2 ループ検知フレームを，ホワイトアドレスリスト対象外にします。（ホワイトリスト機能と L2 ループ検知の併用）

5. **(config)# loop-detection enable**
   L2 ループ検知を有効にします。

6. **(config)# white-list enable**
   ホワイトリスト機能を有効にします。

14.2.6 ホワイトパケットリスト動作モードの変更

ホワイトパケットリスト動作モードを，受信パケット種別モードから送信元抽出モードに変更する場合の設定例です。

［設定のポイント］

ホワイトリスト機能を無効化し，学習している全ホワイトパケットリストを削除します。

＜設定項目＞

- ホワイトリスト機能の無効化
- コンフィグレーションコマンド white-list packet tcp/white-list packet udp の設定がある場合は，全ポートから削除
- 運用コマンドで全ホワイトパケットリストを削除
- ホワイトパケットリスト動作モードを変更
- ホワイトリスト機能の有効化

［コマンドによる設定］

1. **(config)# no white-list enable**
   ホワイトリスト機能を無効にします。

2. **(config)# interface range gigabitethernet 0/1-10**
   (config-if-range)# no white-list packet tcp
   (config-if-range)# no white-list packet udp
   (config-if-range)# exit
   コンフィグレーションコマンド white-list packet tcp/white-list packet udp を設定したポートがある場合はすべて削除します。（未設定の場合，この部分は不要です。）

3. **(config)# exit**
   # erase white-list packet all
   Do you wish to erase white-list (packet)? (y/n): y
   #
   コンフィグレーションモードから装置管理者モードへ移行し，本装置で学習している全ホワイトパケットリストを削除します。

4. **# configure**
   (config)# white-list packet mode 2
   再度，コンフィグレーションモードへ移行し，ホワイトパケットリスト動作モードを送信元抽出モードに変更します。

5. **(config)# white-list enable**
   ホワイトリスト機能を有効にします。

14.3　オペレーション

14.3.1　運用コマンド一覧

ホワイトリストの運用コマンド一覧を次の表に示します。

表 14-34　運用コマンド一覧

コマンド名	説明
show white-list address	ホワイトアドレスリスト情報を表示します。また，全ポート合計の統計情報を表示します。
show white-list packet	ホワイトパケットリスト情報を表示します。また，全ポート合計の統計情報を表示します。
clear white-list statistics	ホワイトリストの統計情報をクリアします。
set white-list packet entry-timer	ホワイトパケットリストのエントリタイマ機能で，一時的に無効化するエントリを設定します。
show white-list packet entry-timer	ホワイトパケットリストのエントリタイマ機能の設定状態を表示します。
show white-list miss-hit	ホワイトリストの運用状態で受信した未学習パケット情報を表示します。
clear white-list miss-hit	ホワイトリストの運用状態で受信した未学習パケット情報をクリアします。
erase white-list	ホワイトリスト（ホワイトアドレスリスト，ホワイトパケットリスト）を一括削除します。

14.3.2　ホワイトアドレスリスト情報の確認

運用コマンド show white-list address で，学習したホワイトアドレスリスト，全ポート合計の未学習パケット数などを確認できます。

図 14-11　ホワイトアドレスリスト情報の表示例

```
> show white-list address

Date 20XX/06/06 20:56:18 UTC
White-list status       : Applying
Total learning count    :          4    …1.
Port change count       :          0    …1.
Invalid mac address     :       7536    …1.
Address list overflow   :          0    …1.
Total inspected packets :     217027    …1.

Total entry / Max entry :         14 / 2000    …2.
  Port     VLAN  MAC address
  0/5      4000  0012.e2aa.0000
  0/5      4000  0012.e2cc.0000
  0/5      4000  0012.e2dd.0000
  0/9      2048  0012.e2aa.0000
  0/9      2048  0012.e2aa.0001
  0/9      2048  0012.e2aa.0002
  0/9      2048  0012.e2aa.0003
  0/9      2048  0012.e2aa.0004
  ChGr:64     1  0012.e202.0251
  ChGr:64     1  0012.e202.0252
  ChGr:64  4000  0012.e211.0000
  ChGr:64  4000  0012.e222.0000
  ChGr:64  4000  0012.e233.0000
  ChGr:64  4000  0012.e244.0000
```

```
Total miss-hit packets  :     304623    …3.

>
```

1. ホワイトアドレスリストの各種統計情報（全ポート合計）
2. 現在学習済みのホワイトアドレスリストエントリ数（全ポート合計）/最大エントリ数（収容条件）
3. ホワイトアドレスリストの未学習パケット受信数（全ポート合計）

14.3.3 ホワイトパケットリスト情報の確認

運用コマンド show white-list packet で，学習したホワイトパケットリスト，全ポート合計の未学習パケット数などを確認できます。

図 14-12 ホワイトパケットリスト情報の表示例

```
> show white-list packet

Date 20XX/02/06 20:55:59 UTC
White-list status       : Applying
Packet list mode        : 1
Total learning count    :          9    …1.
Port change count       :          0    …1.
Invalid mac address     :       7536    …1.
Invalid ip packets      :       5889    …1.
Invalid arp packets     :       7810    …1.
Unsupported packets     :          0    …1.
Packet list overflow    :          0    …1.
Total inspected packets :     205994    …1.

Total entry / Max entry :         19 / 32000    …2.
  Port     VLAN  Type                                                    …3.
                                                                         Matched packets
  0/5      4000  ipv4 sip=192.168.254.100 dip=192.168.254.254                        0
x 0/5      4000  arp smac=0012.e2aa.0000 sip=192.168.100.100                        0
  0/5      4000  other smac=0012.e2bb.0000 dmac=0000.ffff.0000                       0
  0/5      4000  other smac=0012.e2cc.0000 dmac=0000.ffff.0000                       0
  0/5      4000  other smac=0012.e2dd.0000 dmac=0000.ffff.0000                       0
  0/9      2048  ipv4 sip=192.168.254.101 dip=192.168.254.254                      156
  0/9      2048  ipv4 sip=192.168.254.102 dip=192.168.254.254                      156
  0/9      2048  ipv4 sip=192.168.254.103 dip=192.168.254.254                      156
  0/9      2048  ipv4 sip=192.168.254.104 dip=192.168.254.254                      155
x 0/9      2048  arp smac=0012.e2aa.0000 sip=192.168.100.100                        0
x 0/9      2048  arp smac=0012.e2aa.0000 sip=192.168.100.101                        0
x 0/9      2048  arp smac=0012.e2aa.0000 sip=192.168.100.102                        0
x 0/9      2048  arp smac=0012.e2aa.0000 sip=192.168.100.103                        0
x 0/9      2048  arp smac=0012.e2aa.0000 sip=192.168.100.104                        0
  0/9      2048  other smac=0012.e2aa.0000 dmac=0000.ffff.0000                     597
  ChGr:64     1  other smac=0012.e202.0251 dmac=0180.c200.0002                      0
  ChGr:64     1  other smac=0012.e202.0251 dmac=0180.c200.000e                     0
  ChGr:64     1  other smac=0012.e202.0252 dmac=0180.c200.0002                     0
  ChGr:64     1  other smac=0012.e202.0252 dmac=0180.c200.000e                     0
```

```
Total miss-hit packets  :     281885    …4.

>
```

1. ホワイトパケットリストの各種統計情報（全ポート合計）
2. 現在学習済みのホワイトパケットリストエントリ数（全ポート合計）/最大エントリ数（収容条件）
3. Matched packets：ホワイトパケットリストに一致したパケット数（リスト単位）
4. ホワイトパケットリストの未学習パケット受信数（全ポート合計）

14.3.4 エントリタイマ機能の設定状態の確認

ホワイトパケットリストのエントリタイマ機能の設定状態は，運用コマンド show white-list packet entry-timer で確認できます。

図 14-13 エントリタイマ機能設定状態の表示例

```
> show white-list packet entry-timer

Date 20XX/02/06 20:56:07 UTC
Total entry / Max entry :          22 / 2000
Source IP address   Expire(s)     Entries
192.168.100.100           257           2
192.168.100.101           257           1
192.168.100.102           257           1
192.168.100.103           257           1
192.168.100.104           258           1
192.168.100.105           258           0
192.168.100.106           258           0
192.168.100.107           258           0
192.168.100.108           258           0
       :

>
```

また，このとき運用コマンド show white-list packet でエントリタイマ指定有のホワイトパケットリストエントリは，先頭に "x" が表示されます。（「図 14-12 ホワイトパケットリスト情報の表示例」参照。）

14.3.5 ホワイトリスト未学習パケット情報の確認

未学習パケットのパケット種別内容は，運用コマンド show white-list miss-hit で確認できます。

図 14-14 未学習パケット情報の表示例

```
> show white-list miss-hit

Date 20XX/06/08 17:25:28 UTC
White-list status       : Applying

Total entry / Max entry :        404 / 2000
  Port     VLAN  Last detection time  First detection time       Count
  0/1      2000  20XX/06/08 17:25:28  20XX/06/08 16:57:00         8308
    [a] mac=0012.e278.0007
    [p] type=ipv4 sip=110.110.110.116 dip=120.120.120.126 proto=tcp sp=56803 dp
=61172
  0/1      1000  20XX/06/08 17:25:28  20XX/06/08 16:57:03         8274
    [a] mac=0012.e234.0008
    [p] type=arp smac=0012.e234.0008 sip=192.168.254.108
  0/1      1000  20XX/06/08 17:25:28  20XX/06/08 16:57:04         8326
    [a] mac=0012.e234.0007
    [p] type=arp smac=0012.e234.0007 sip=192.168.254.107
  0/9      2000  20XX/06/08 17:25:28  20XX/06/08 16:57:01         8824
    [a] mac=0012.e278.000a
    [p] type=ipv4 sip=110.110.110.119 dip=120.120.120.129 proto=tcp sp=56806 dp
=61175
  0/10      400  20XX/06/08 17:25:28  20XX/06/08 16:57:00         9679
    [p] type=ipv4 sip=110.110.110.112 dip=120.120.120.122 proto=51 Unsupported
           :
           :
```

```
            :
  ChGr:33  2048  20XX/06/08 16:15:22  20XX/06/08 16:15:20            3
    [p] type=arp smac=0012.e295.78d3 sip=0.0.0.0
  0/3         1  20XX/06/08 16:15:20  20XX/06/08 16:15:18            3
    [a] mac=00eb.f009.0001
  0/5         1  20XX/06/08 16:15:19  20XX/06/08 16:15:19            1
    [a] mac=0012.e272.12ac
    [p] type=other smac=0012.e272.12ac dmac=0180.c200.0000

>
```

[a]だけ表示：ホワイトアドレスリスト未学習パケット情報
[p]だけ表示：ホワイトパケットリスト未学習パケット情報
[a][p]両方表示：ホワイトアドレスリスト・ホワイトパケットリスト両方での未学習パケット情報

14.3.6 ホワイトリストの削除

ランニングコンフィグレーションに登録されているホワイトリスト（ホワイトアドレスリスト，ホワイトパケットリスト）を削除します。

図 14-15 ホワイトリストの削除

```
# erase white-list all
Do you wish to erase white-list of all? (y/n): y
# copy running-config startup-config
Do you wish to copy from running-config to startup-config? (y/n): y
>
```

[注意事項]

運用コマンド erase white-list はランニングコンフィグレーションのホワイトリストを削除します。削除後は copy コマンドでスタートアップコンフィグレーションファイルに保存してください。保存しないで装置を再起動した場合，削除結果がランニングコンフィグレーションに反映されません。

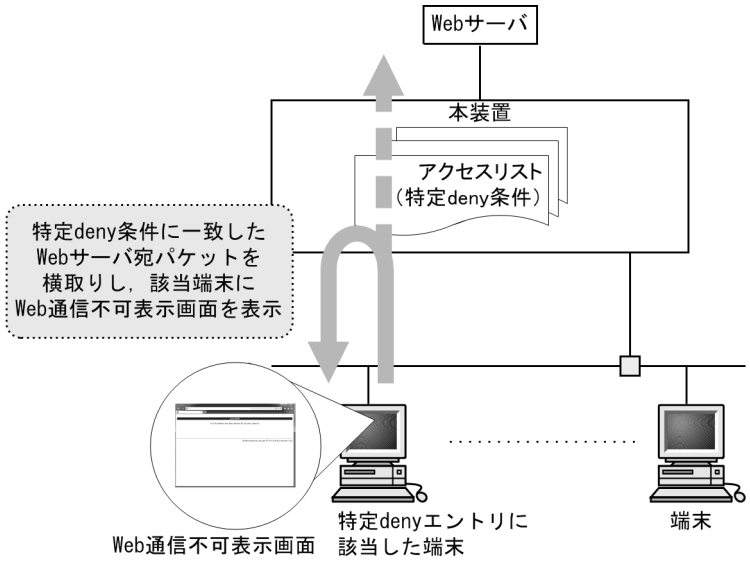
15 特定端末への Web 通信不可表示機能

本機能は，アクセスリストの deny エントリに該当する端末からの HTTP リクエストに対して，送信元ユーザ端末のブラウザに通信不可画面を表示させる機能です。
この章では，特定端末への Web 通信不可表示機能について説明します。

15.1　概要

本装置では，アクセスリストの deny エントリに指定された特定の宛先 TCP ポート番号に該当するパケットを受信した場合，当該端末からの他 Web サーバ宛 HTTP リクエストに対して，Web 通信不可表示画面を当該端末のブラウザに表示させます。

図 15-1　特定端末への Web 通信不可表示機能概要図

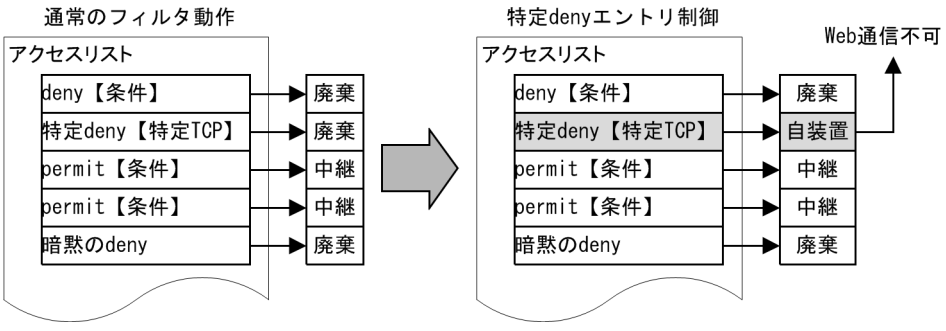


15.1.1　特定 deny エントリの制御

通常のアクセスリストは deny エントリに一致したパケットは廃棄します。

本機能では，コンフィグレーションコマンド access-redirect http port で設定した TCP ポート番号が，アクセスリストの deny 条件の宛先 TCP ポート番号に設定されたエントリを「特定 deny エントリ」と定義します。この「特定 deny エントリ」に一致したパケットは廃棄せずに，Web 通信不可対象として処理します。

図 15-2　特定 deny エントリ制御



15.1.2　特定端末への Web 通信不可表示（リダイレクト）

前述の特定 deny エントリ制御により，他宛の TCP パケットを本装置で Web 通信不可対象として処理し，TCP コネクションを開設します。TCP パケットの送信元端末から他 Web サーバ宛の HTTP リクエストを

受信した場合，コンフィグレーションの設定によって，以下のいずれかの動作を行います。

（1） Web 通信不可表示画面の直接応答

本装置内に格納されたデフォルトの Web 通信不可表示画面，または運用コマンドによって入れ替えた Web 通信不可表示画面を，HTTP リダイレクトしないで直接応答します。入れ替え画面ファイルの詳細については，後述の「15.1.4　Web 通信不可表示画面の入れ替え」を参照してください。

図 15-3　Web 通信不可表示画面例

（2） 外部 Web サーバへリダイレクト

コンフィグレーションコマンド access-redirect http target で指定された URL へのリダイレクト指示を当該端末に応答します。

（3） 本機能の動作条件

本機能を使用する場合は，本装置に次の設定をしてください。

- システム受信モード：受信条件重視モード
- 受信側フロー検出モード：layer-2-2，layer2-3，layer2-2-mirror のどれかを設定
  （受信側フロー検出モード未設定の場合は，layer2-2 となります。）

本機能は，本装置で IPv4 アドレスを設定されている VLAN の IPv4 パケットに対して動作します。

また，フィルタと併用する場合は，コンフィグレーションコマンド access-redirect http port を設定してから，イーサネットインタフェース・VLAN インタフェースに ip access-group を設定してください。

なお，受信側フロー検出モード layer2-3 で IPv4 アクセスリストと IPv6 アクセスリストを両方設定した場合は，IPv4 アクセスリストは本機能とフィルタ機能，IPv6 アクセスリストはフィルタ機能が動作します。

15.1.3 他機能との共存

(1) フィルタ

本機能とフィルタ（イーサネット・VLAN インタフェース）を併用した場合の動作は以下となります。

受信側フロー検出モード layer2-3 の場合は IPv4 アクセスリストと IPv6 アクセスリストを併用可能ですが，特定 deny に一致した場合は，IPv4 アクセスリストは特定 deny，IPv6 アクセスリストは deny（フィルタ動作）となります。

表 15-1 本機能とフィルタを併用時の動作

イーサネットのフィルタ	VLAN インタフェースのフィルタ				
	未設定	permit に一致	deny に一致	特定 deny に一致	暗黙 deny に一致
未設定	permit	permit	deny	IPv4：特定 deny IPv6：deny	deny
permit に一致	permit	permit	deny	IPv4：特定 deny IPv6：deny	deny
deny に一致	deny	deny	deny	IPv4：deny IPv6：deny	deny
特定 deny に一致	IPv4：特定 deny IPv6：deny	IPv4：特定 deny IPv6：deny	IPv4：deny IPv6：deny	IPv4：特定 deny IPv6：deny	IPv4：deny IPv6：deny
暗黙 deny に一致	deny	deny	deny	IPv4：deny IPv6：deny	deny

(2) 装置内共存不可機能

次に示す機能は装置内で共存できません。コンフィグレーションで排他されます。

- システム受信モード：収容条件重視モード
- スタック
- ホワイトリスト機能

(3) ポート閉塞時

スパニングツリーなどによる閉塞ポートの特定 deny エントリに一致したパケットは，本装置の CPU 受信後に廃棄されます。

(4) ストームコントロール

特定 deny エントリに一致したパケットはストームコントロールによる流量制限を無視して本装置で CPU 受信します。

15.1.4 Web 通信不可表示画面の入れ替え

本機能では，Web 通信不可表示画面ファイルを使用します。

Web 通信不可表示画面ファイルは，本装置が受信した HTTP パケットがアクセスリストの deny エントリに該当した場合，ユーザ端末のブラウザに Web 通信不可の警告画面を表示させるための HTML ファイルです。

特定端末への Web 通信不可表示画面ファイルは本装置にデフォルト画面が登録されていますが，外部装置

（PCなど）で作成し，運用コマンドset access-redirect html-fileで本装置に入れ替えることができます。

入れ替えに指定できるファイルは，HTMLファイル1個，ファイルサイズは10,240バイト以下です。画像などを使用する場合は，HTMLファイルへ埋め込んで（src=data:image/gifなど）ください。なお，外部参照へのファイルパスは使用しないことを推奨します。

入れ替えの手順は，後述の「15.3.4　Web通信不可表示画面ファイルの入れ替え」を参照してください。入れ替えたHTMLファイルは運用コマンドclear access-redirect html-fileで削除できます。削除後は，デフォルト画面に戻ります。

Web通信不可表示画面ファイルについては，後述の「(1) Web通信不可表示画面ファイル」を参照してください。

(1) Web通信不可表示画面ファイル

(a) 設定条件

Web通信不可表示画面のHTMLファイルを作成する際は，次の表に示す記述を必ず入れてください。

表15-2　Web通信不可表示画面に必要な設定

記述内容	内容
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">	文字コードを指定するための記述です。 Content-Typeはtext/htmlを指定してください。 charsetは文字コード種別を指定してください。（例：UTF-8）

注意

BOM（Byte Order Mark）が付加されていても，本装置から端末へそのまま送信します。

(b) 設定例

Web通信不可表示画面のソース例を次の図に示します。

図 15-4　Web 通信不可表示画面のソース例

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
    "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8"> 文字コード指定用の記述
<meta http-equiv="Pragma" content="no-cache">
<meta http-equiv="Cache-Control" content="no-cache">
<meta http-equiv="Expires" content="Thu, 01 Dec 1994 16:00:00 GMT">
<title> </title>
</head>
<body oncontextmenu="return false;">
<!-- ===== Body ===== -->
<center>
<br />
<table width="100%">
<tr><td align="center" bgcolor="#2b1872">
<font color="#ffffff"><b>CAUTION!</b></font>
</td></tr></table>
<br />
Your IP address has been banned for security reasons.<br /> 警告メッセージの記述
<br />
<br />
<br />
<br />
<br />
<br />
</center>
<!-- ===== Footer ===== -->
<hr>
<div align="right"></div>
</body>
</html>
```

(c) Web 通信不可画面表示例

Web 通信不可画面の表示例を次の図に示します。

図 15-5　Web 通信不可画面の表示例

15.1.5　特定端末への Web 通信不可表示機能使用時の注意事項

外部 Web サーバへリダイレクトする場合，リダイレクト先の外部 Web サーバへの通信が，アクセスリストの特定 deny 条件に該当すると，永久にリダイレクトを繰り返す可能性があります。

15.2　コンフィグレーション

15.2.1　コンフィグレーションコマンド一覧

特定端末への Web 通信不可表示機能のコンフィグレーションコマンド一覧を次の表に示します。

表 15-3　コンフィグレーションコマンド一覧

コマンド名	説明
access-redirect http port	特定端末への Web 通信不可表示機能で使用する TCP ポート番号を指定します。
access-redirect http target	特定端末への Web 通信不可表示機能エントリに該当した HTTP パケットに対してのリダイレクト先を指定します。
access-redirect timeout	TCP 接続後，指定時間以内に HTTP 要求ヘッダの受信が完了しない場合に，TCP コネクションを切断する時間を変更します。

15.2.2　特定端末への Web 通信不可表示機能を設定

［設定のポイント］

＜前提条件＞

- システム受信モード：受信条件重視モード
- 受信側フロー検出モード：layer2-2，layer2-3，layer2-2-mirror のどれかを設定
- イーサネットインタフェース，VLAN インタフェースに ip access-group コマンドが設定されていないこと

1. アクセスリストの deny エントリに，抽出する端末の IP アドレスと宛先 TCP ポート番号を設定します。
2. 特定端末への Web 通信表示不可機能を有効にします。

［コマンドによる設定］

1. **(config)# ip access-list extended AAAAA**
   (config-ext-nacl)# deny tcp host 192.168.1.254 any eq 80
   (config-ext-nacl)# permit tcp any any
   (config-ext-nacl)# exit
   deny エントリに抽出する端末の IP アドレス（例 192.168.1.254）と，宛先 TCP ポート番号 80 を設定します。

2. **(config)# access-redirect http port 80**
   特定端末への Web 通信不可表示機能で使用する TCP ポート番号 80 を指定し，本機能を有効にします。

［注意事項］

イーサネットインタフェースおよび VLAN インタフェースの ip access-group 設定は上記の設定後に実行してください。

15.2.3　外部 Web サーバへのリダイレクト処理の設定

［設定のポイント］

「15.2.2　特定端末への Web 通信不可表示機能を設定」後，リダイレクト先を外部 Web サーバに設定

します。

［コマンドによる設定］

1. **access-redirect http target "http://www.example.gaibuserver/sample.html"**
   リダイレクト先の外部Webサーバの URL を設定します。

15.3　オペレーション

15.3.1　運用コマンド一覧

特定端末への Web 通信不可表示機能の運用コマンド一覧を次の表に示します。

表 15-4　運用コマンド一覧

コマンド名	説明
show access-redirect statistics	特定端末への Web 通信不可表示機能の統計情報を表示します。
clear access-redirect statistics	特定端末への Web 通信不可表示機能の統計情報を 0 クリアします。
show access-redirect logging	特定端末への Web 通信不可表示機能のアクセスログ情報を表示します。
clear access-redirect logging	特定端末への Web 通信不可表示機能のアクセスログ情報をクリアします。
set access-redirect html-file	特定端末への Web 通信不可表示画面ファイルを入れ替えます。
clear access-redirect html-file	入れ替えた特定端末への Web 通信不可表示画面ファイルを削除し，装置デフォルトの特定端末への Web 通信不可表示画面ファイルに戻します。

15.3.2　特定端末への Web 通信不可表示機能の統計情報の確認

運用コマンド show access-redirect statistics により，特定端末への Web 通信不可表示機能の TCP ポート番号，リダイレクト先，統計情報を確認できます。

図 15-6　特定端末への Web 通信不可表示機能の統計情報の確認

```
> show access-redirect statistics

Date 20XX/05/25 10:46:18 UTC
Redirect port                : 80
Redirect target              : Local (default)
Redirect timeout             : 1000 (msec)

Connection requests          :         21
Unsupported method           :          0
Receive timeout              :          0
URL too long                 :          0
Invalid requests             :          0
Translation table overflows  :          0
Outbound translation errors  :          0
Inbound translation errors   :          0
Invalid VLAN packets         :          0

>
```

15.3.3　特定端末への Web 通信不可表示機能のアクセスログ情報の確認

運用コマンド show access-redirect logging により，特定端末への Web 通信不可表示機能に該当した端末情報と HTTP リクエストのアクセスログ情報を確認できます。

図 15-7　特定端末への Web 通信不可表示機能のアクセスログ情報の確認

```
> show access-redirect logging

Date 20XX/05/25 10:23:30 UTC
20XX/05/25 10:23:25 192.168.10.101:60102 HTTP/1.1 www.example.com /index.html
20XX/05/25 10:23:04 192.168.10.101:60101 HTTP/1.1 /index.html
    :

>
```

15.3.4　Web 通信不可表示画面ファイルの入れ替え

Web 通信不可表示画面ファイルの入れ替えは次の手順で行います。

1. Web 通信不可画面ファイルを外部装置（PC など）で作成します。
2. Web 通信不可画面ファイルを MC から RAMDISK にコピーします。
3. 運用コマンド set access-redirect html-file で Web 通信不可表示画面ファイルを登録します。

図 15-8　Web 通信不可表示画面ファイルの登録

```
# copy mc custom-caution.html ramdisk custom-caution.html

# set access-redirect html-file ramdisk custom-caution.html
Do you wish to continue? (y/n): y
executing...
Install complete.
#
```

[注意事項]

入れ替えできるファイルは 1 ファイルです。また，ファイルサイズは 10,240 バイト以下としてください。

15.3.5　装置デフォルトの Web 通信不可表示画面ファイルに戻す

運用コマンド set access-redirect html-file で入れ替えた Web 通信不可表示画面ファイルを運用コマンド clear access-redirect html-file で装置デフォルトの Web 通信不可表示画面ファイルに戻します。

図 15-9　装置デフォルトの Web 通信不可表示画面ファイルに戻す

```
# clear access-redirect html-file
Erase OK ? (y/n): y
executing...
Clear complete.
#
```

16 GSRP aware 機能

GSRP aware は，GSRP スイッチからフレームを受信することにより自装置の MAC アドレステーブルをクリアする機能です。この章では，GSRP aware 機能について説明します。

16.1　GSRP の概要

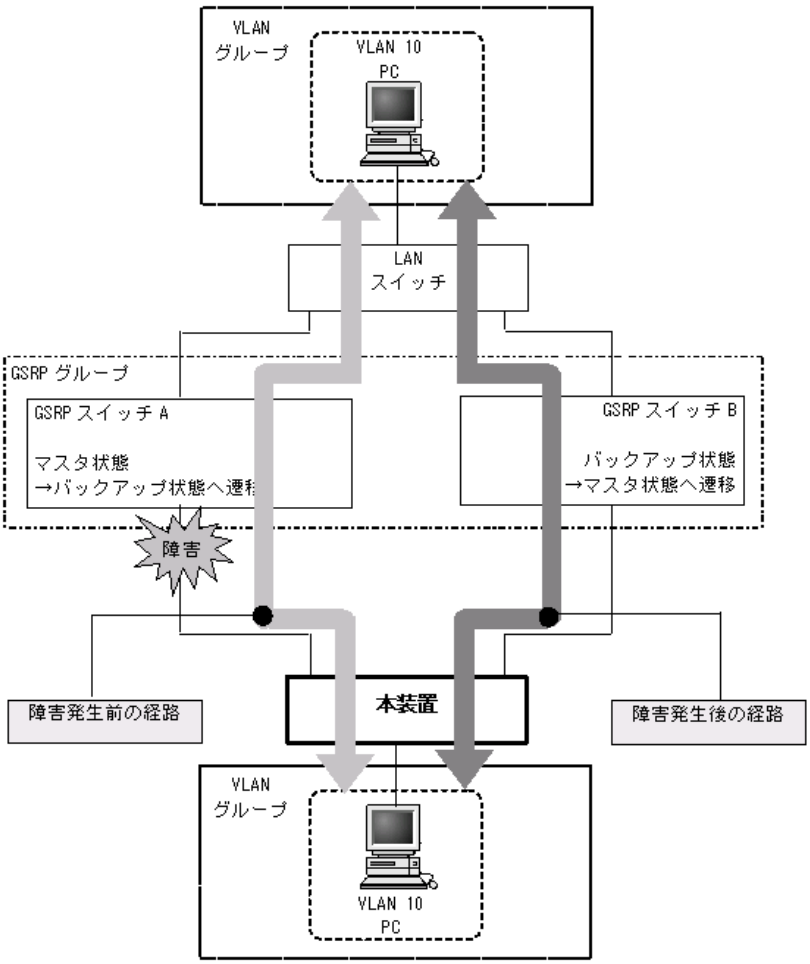
16.1.1　概要

GSRP（Gigabit Switch Redundancy Protocol）は，スイッチに障害が発生した場合でも，同一ネットワーク上の別スイッチを経由して通信経路を確保することを目的とした装置の冗長化を実現する機能です。

ネットワークの冗長化を行う機能としてスパニングツリーがありますが，GSRP では 2 台のスイッチ間で制御するため，スパニングツリーよりも装置間の切り替えが高速です。また，ネットワークのコアスイッチを多段にするような大規模な構成にも適しています。一方で，スパニングツリーは標準プロトコルであり，マルチベンダーによるネットワーク構築に適しています。

GSRP によるレイヤ 2 の冗長化の概要を次の図に示します。

図 16-1　GSRP の概要



16.1.2　サポート仕様

本装置では，GSRP aware だけサポートします。次項の「16.2　GSRP の切り替え制御」を参照してください。

（1） 他機能との共存について

（a） レイヤ 2 スイッチ機能との共存

「コンフィグレーションガイド Vol.1　19.3　レイヤ 2 スイッチ機能と他機能の共存について」を参照してください。

（b） レイヤ 2 認証機能との共存

「5.9.3　レイヤ 2 認証機能と他機能の共存」を参照してください。

（c） スタック動作時の GSRP aware について

スタック動作時の GSRP aware については，「コンフィグレーションガイド Vol.1　7. スタックの解説【OP-WLE】」を参照してください。

16.2　GSRP の切り替え制御

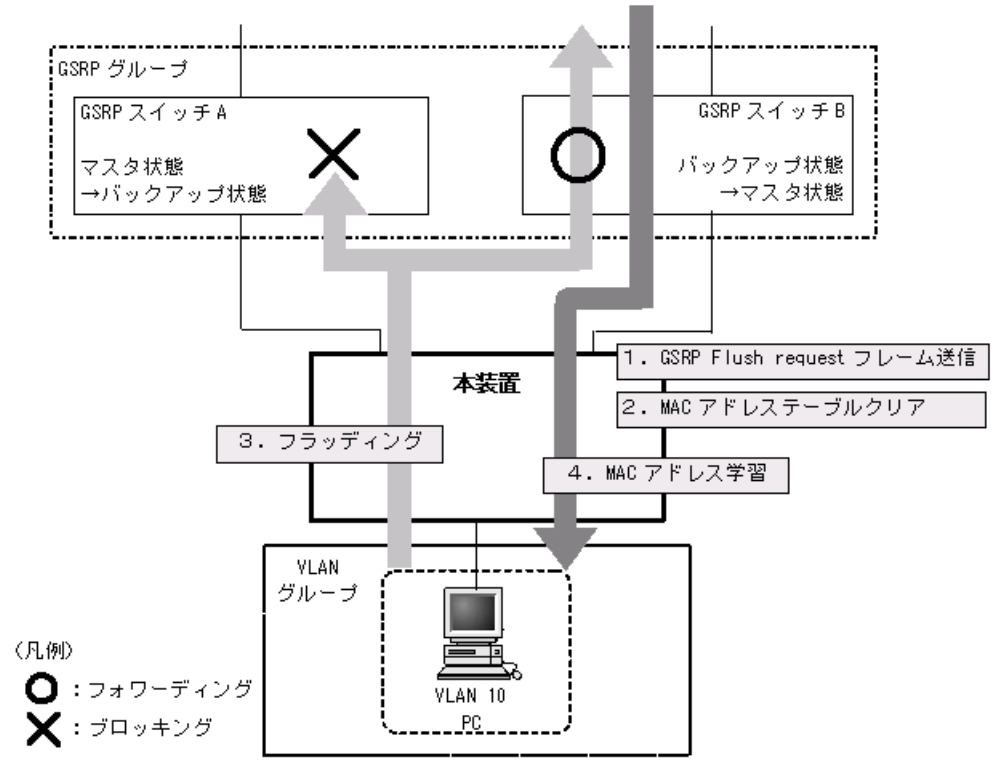
GSRP スイッチで切り替えを行う際，フレームに対するフォワーディングおよびブロッキングの切り替え制御を行うだけでは，エンドーエンド間の通信を即時に再開できません。これは，周囲のスイッチの MAC アドレステーブルにおいて，MAC アドレスエントリが切り替え前にマスタ状態であった GSRP スイッチ向けに登録されたままであるためです。通信を即時に再開するためには，GSRP スイッチの切り替えと同時に，周囲のスイッチの MAC アドレステーブルエントリをクリアする必要があります。

GSRP では，周囲のスイッチの MAC アドレステーブルエントリをクリアする方法として下記をサポートしています。

（1） GSRP Flush request フレームの送信

GSRP では切り替えを行うとき，周囲のスイッチに対して MAC アドレステーブルエントリのクリアを要求するため GSRP Flush request フレームと呼ぶ制御フレームを送信します。この GSRP Flush request フレームを受信して，自装置内の MAC アドレステーブルをクリアできるスイッチを GSRP aware と呼びます。GSRP aware は GSRP Flush request フレームをフラッディングします。本装置は常に GSRP aware として動作します。GSRP Flush request フレームによる切り替え制御の概要を次の図に示します。

図 16-2　GSRP Flush request フレームによる切り替え制御の概要



1. GSRP スイッチ A と GSRP スイッチ B との間で切り替えが行われ，GSRP スイッチ B は GSRP Flush request フレームを本装置へ向けて送信します。
2. 本装置は GSRP Flush request フレームを受けて，自装置内の MAC アドレステーブルをクリアします。

3. この結果，本装置上は PC の送信するフレームに対して，MAC アドレスの学習が行われるまでフラッディングを行います。
   当該フレームは，マスタ状態である GSRP スイッチ B を経由して宛先へフォワーディングされます。
4. 応答として PC 宛のフレームが戻ってくると，本装置は MAC アドレスの学習を行います。
   以後，本装置は PC からのフレームを GSRP スイッチ B へ向けてだけフォワーディングするようになります。

16.3　コンフィグレーション

本装置は，GSRP aware だけサポートしていますので，コンフィグレーションはありません。

16.4　オペレーション

16.4.1　運用コマンド一覧

GSRP の運用コマンド一覧を次の表に示します。

表 16-1　運用コマンド一覧

コマンド名	説明
show gsrp aware	GSRP の aware 情報を表示します。

16.4.2　GSRP aware 情報の確認

本装置では GSRP aware 情報を運用コマンド show gsrp aware で表示します。

図 16-3　show gsrp aware の実行例

```
> show gsrp aware

Date 20XX/05/20 14:34:40 UTC
Last mac_address_table Flush Time : 20XX/05/20 14:34:35
GSRP Flush Request Parameters :
 GSRP ID : 10      VLAN Group ID : 6   Port : 0/1
 Source MAC Address : 0012.e208.2096

>
```

17 アップリンク・リダンダント

アップリンク・リダンダントは，スパニングツリーを使用しないで冗長構成を構築できます。
この章では，アップリンク・リダンダントの解説と操作方法について説明します。

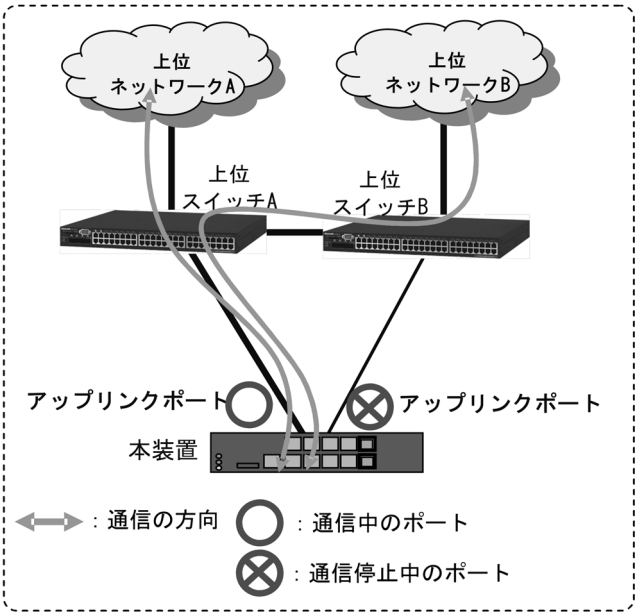
17.1　解説

アップリンク・リダンダントは，本装置でアップリンクに用いるポートを二重化し，障害時にバックアップ用ポートに切り替えて上位スイッチとの通信を継続する機能です。本機能を使用すると，スパニングツリーなどのプロトコルを使わないでアップリンクに用いるポートを冗長化できます。冗長化するための二つのポートをあわせて，アップリンクポートと呼びます。

- レイヤ２スイッチを逆三角形構成で接続し，下位スイッチが切り替えを実施します。
- 下位スイッチは，レイヤ２インタフェース（イーサネットまたはポートチャネル）のペア設定により，アップリンクポートを二重化します。

アップリンク・リダンダントの基本構成を次の図に示します。

図 17-1　アップリンク・リダンダント概要



この図の構成でアップリンク・リダンダントを使用した場合，本装置と上位スイッチ A との間のリンクに障害が発生しても，本装置と上位スイッチ B との間のリンクに切り替えることで通信を継続できます。

各機能の詳細や設定説明については下記を参照してください。

表 17-1　アップリンク・リダンダントのサポート機能

機能	項目	機能説明参照先	設定説明参照先
基本	アップリンク・リダンダント動作	「17.1.1」参照	－
	アップリンクポートの適用インタフェース	「17.1.1」参照	「17.2.2」参照
	アップリンクポート数	「17.1.1」参照	－
	プライマリ・セカンダリ切り替え切り戻し	「17.1.2」参照	－
	障害復旧時の切り戻し	「17.1.2」参照	「17.2.2」参照
	ポート制御	「17.1.2」参照	－
拡張	フラッシュ制御フレーム送受信機能	「17.1.3」参照	「17.2.3」参照
	MAC アドレスアップデート機能	「17.1.4」参照	「17.2.4」参照
	装置起動時のアクティブポート固定機能	「17.1.5」参照	－

17.1.1　アップリンク・リダンダント動作

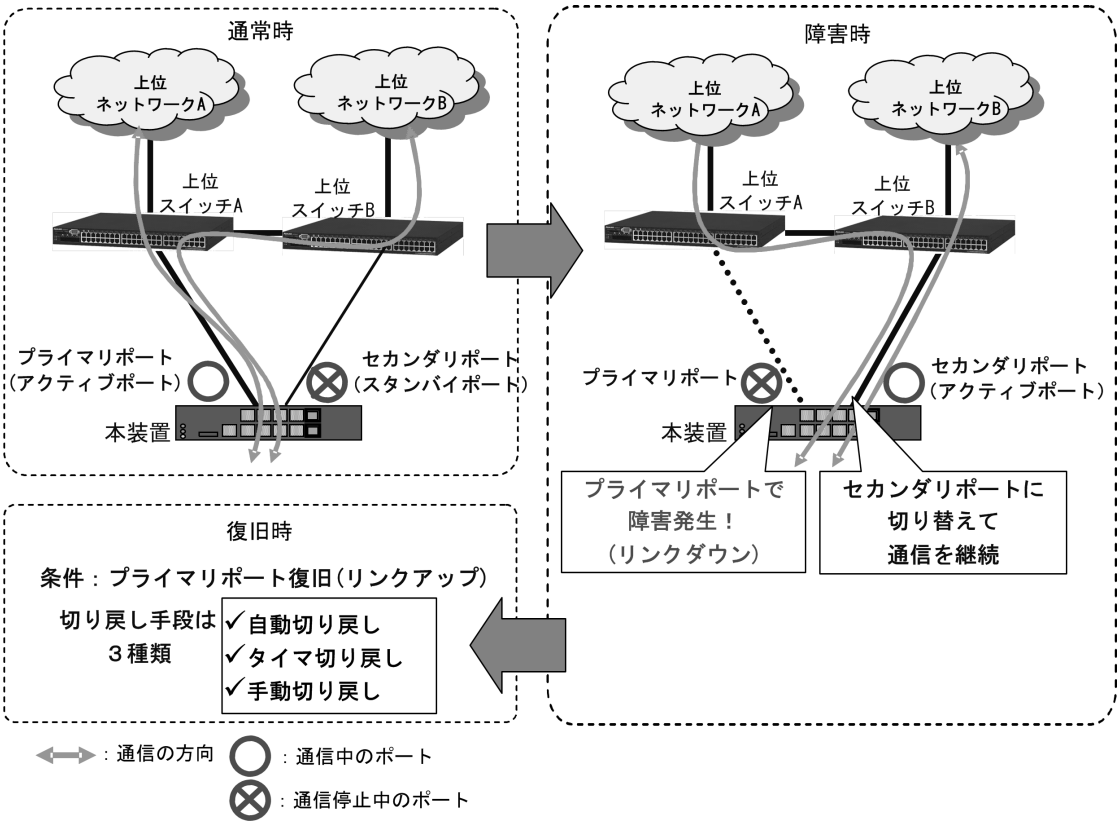
アップリンク・リダンダントでは，1 対のポートまたはリンクアグリゲーションを用いて冗長性を確保します。このポート対がアップリンクポートです。アップリンクポートには，通常，通信を行うプライマリポートと，プライマリポートの障害時に通信を行うセカンダリポートの二つがあります。これらのポートは，コンフィグレーションで設定します。

アップリンクポートのうち，現在通信を行っているポートをアクティブポートと呼びます。また，アクティブポートに障害が発生した場合に，通信継続のため，すぐに通信を開始できるような準備ができているポートをスタンバイポートと呼びます。

アップリンクポートを構成する 1 対のポートは，VLAN などの構成を同一設定にする必要があります。また，アップリンクポートに設定しているポートは，ほかのアップリンクポートでは設定できません。

アップリンク・リダンダントの動作概要を次の図に示します。

図 17-2　アップリンク・リダンダント動作概要



通常時：

本装置のプライマリポートと上位スイッチ A が通信可能で，本装置のセカンダリポートは通信不可状態となっています。

障害時：

プライマリポートのリンクダウンを契機に，本装置でアクティブポートをセカンダリポートに変更し，セカンダリポートを経由して上位スイッチへの通信を継続します。この動作を切り替えと呼びます。

復旧時：

プライマリポートがリンクアップしてスタンバイポートになっていれば，本装置で「自動 (タイマ) 切戻し」「手動切戻し」などの手段でアクティブポートをプライマリポートに変更できます。この動作

を切り戻しと呼びます。

また，アクティブポートを変更したとき，コンフィグレーションにより上位スイッチへMACアドレステーブルクリアを要求するフラッシュ制御フレームを，アクティブポートに変更したポートから送信することもできます。

(1) アップリンクポートの適用インタフェース

アップリンクポートは，イーサネットインタフェースまたはポートチャネルインタフェースを指定できます。プライマリ・セカンダリの組み合わせには，イーサネットインタフェース・ポートチャネルインタフェースの組み合わせ指定も可能です。

表 17-2　プライマリポート・セカンダリポートの範囲と組み合わせ

モデル	インタフェース種別	ポート番号範囲	プライマリ・セカンダリの組み合わせ
AX260A-08TF AX260A-08T	イーサネット	gigabitethernet 0/1 ～ 0/10	いずれのインタフェースでも組み合わせ可能
	ポートチャネル	port-channel 1 ～ 64	

(2) アップリンクポート数

本機能ではアップリンクポートとして，プライマリポートを1ポートとセカンダリポートを1ポートの組み合わせを設定します。装置内で設定可能なアップリンクポート数を次の表に示します。

表 17-3　アップリンクポートの最大設定数

モデル	最大設定数
AX260A-08TF AX260A-08T	5

17.1.2　プライマリ・セカンダリ切り替えと切り戻し

切り替え・切り戻しとは，通信を行っているポートの障害によって自動的にアクティブポートを変更する動作，または運用コマンドによって手動でアクティブポートを変更する動作です。切り替え・切り戻しを行う場合には，アクティブポートの変更先ポートがスタンバイポートとなっている必要があります。

(1) 障害時の切り替え

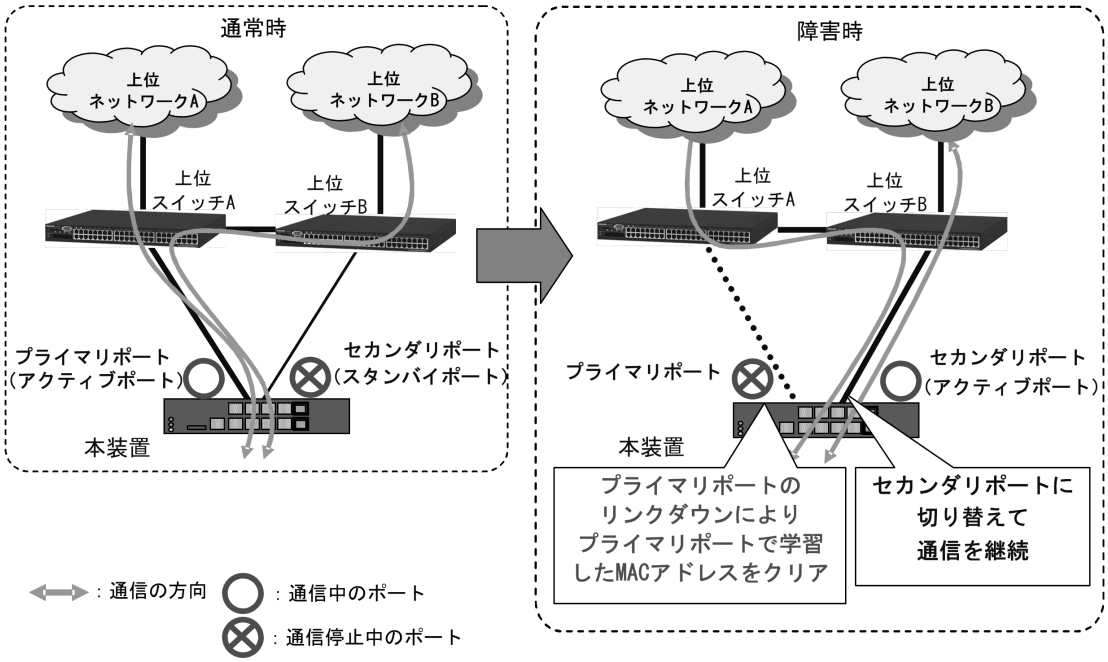
本装置にあらかじめプライマリポートとセカンダリポートをコンフィグレーションで設定しておきます。

通常時はプライマリポート（アクティブポート）で通信し，プライマリポートのリンクダウンを検知すると，アクティブポートをセカンダリポートに変更します。

切り替え・切り戻し動作と同時に，通信を行っていたポートで学習していたMACアドレスをすべてクリアして，新しくアクティブポートになったポートで通信を行います。

フラッシュ制御フレームまたはMACアドレスアップデートフレームを送信する設定をしている場合は，切り替え・切り戻しと同時に新しくアクティブポートになったポートから上位スイッチに，フラッシュ制御フレームまたはMACアドレスアップデートフレームを送信します。

図 17-3　プライマリ・セカンダリ切り替え概要



(2) 障害復旧時の切り戻し

障害復旧時の切り戻しには，自動切り戻し，タイマ切り戻し，および手動切り戻しがあります。

(a) 自動切り戻し

アップリンク・リダンダント動作時，コンフィグレーションの切り戻し時間（0 秒）設定により，自動切り戻しを実行します。

プライマリポートがリンクアップ後，即時に自動で切り戻します。タイマによる自動切り戻しは，次の「(b) タイマ切り戻し」を参照してください。

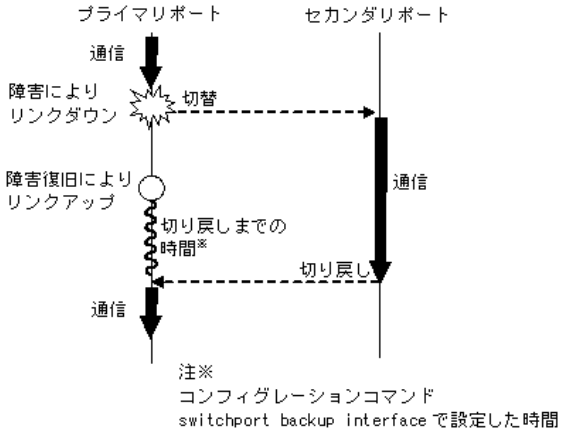
(b) タイマ切り戻し

アップリンク・リダンダント動作時，コンフィグレーションの切り戻し時間（1 ～ 300 秒）設定により，自動でタイマ切り戻しを実行します。

プライマリポートのリンクアップ状態が，コンフィグレーションコマンド switchport backup interface で設定されたタイマ切り戻し時間を超えて継続した場合に切り戻します。

タイマ切り戻し時間満了前にプライマリポートがリンクダウンした場合は，時間計測をリセットします。タイマ切り戻しの概要を次の図に示します。

図 17-4 タイマ切り戻し概要



(c) 手動切り戻し

アップリンク・リダンダント動作時，プライマリポートのインタフェースが障害復旧により，リンクアップ後もアクティブポートはセカンダリポートで動作を続けます。プライマリポート回復後，アクティブポートをプライマリポートへの切り戻すときは運用コマンド set switchport-backup active で実行します。

運用コマンドは指定する切り戻し先がリンクアップしているときに実行可能です。

(3) ポート制御

アップリンク・リダンダントのポート制御は，Blocking（通信不可状態）/Forwarding（通信可能状態）制御です。次の表に示すポート制御を実施します。

表 17-4 アップリンク・リダンダントのポート制御

ポートの状態（プライマリ・セカンダリ設定，物理状態）			アップリンク・リダンダントのポート制御		
状態	設定	物理状態	動作	フレーム受信	フレーム送信
通常状態	プライマリ	リンクアップ	Forwarding	○	○
	セカンダリ	リンクアップ	Blocking	×	×※
プライマリポートリンクダウン検出時	プライマリ	リンクダウン	Blocking	×	×
	セカンダリ	リンクアップ	Forwarding	○	○
プライマリポートリンク回復時で下記のいずれかの状態 • 自動切り戻し実行前 • タイマ切り戻し実行前 • 手動切り戻し待ち	プライマリ	リンクアップ	Blocking	×	×※
	セカンダリ	リンクアップ	Forwarding	○	○
セカンダリポートリンクダウン検出時	プライマリ	リンクアップ	Forwarding	○	○
	セカンダリ	リンクダウン	Blocking	×	×
プライマリ，セカンダリ両ポートリンクダウン検出時	プライマリ	リンクダウン	Blocking	×	×
	セカンダリ	リンクダウン	Blocking	×	×

（凡例）
○：送信する　×：送信しない

注 ※
Blocking 時でも LACP などのフレームは送受信可能です。

17.1.3　フラッシュ制御フレーム送受信機能

フラッシュ制御フレームを送信することで，上位スイッチの MAC アドレステーブルをクリアします。上位スイッチは，フラッシュ制御フレームによる MAC アドレステーブルのクリアをサポートしている必要があります。

（1） 送信動作

コンフィグレーションにより，MAC アドレステーブルクリアを要求するフラッシュ制御フレーム送信が設定されている場合，アクティブポートの変更時にフラッシュ制御フレームを送信します。

送信契機は，プライマリポート・セカンダリポートの切り替え後のポートがアップ直後に，アクティブポートに変更したポートから送信します。

送信はアクティブポートの変更時に 1 秒間隔で同一フレームを 3 回送信します。送信する VLAN は次の表のとおりです。

表 17-5　フラッシュ制御フレームを送信する VLAN

コンフィグレーションの フラッシュ制御フレーム送信設定	送信ポートのポート種別	送信する VLAN
送信 VLAN 指定なし	アクセスポート	アクセス VLAN に送信
	トランクポート	ネイティブ VLAN に送信
	MAC ポート	ネイティブ VLAN に送信
	プロトコルポート	ネイティブ VLAN に送信
送信 VLAN 指定あり	アクセスポート	アクセス VLAN に送信
	トランクポート	指定 VLAN に送信
	MAC ポート	ネイティブ VLAN に送信
	プロトコルポート	ネイティブ VLAN に送信

（2） 受信動作

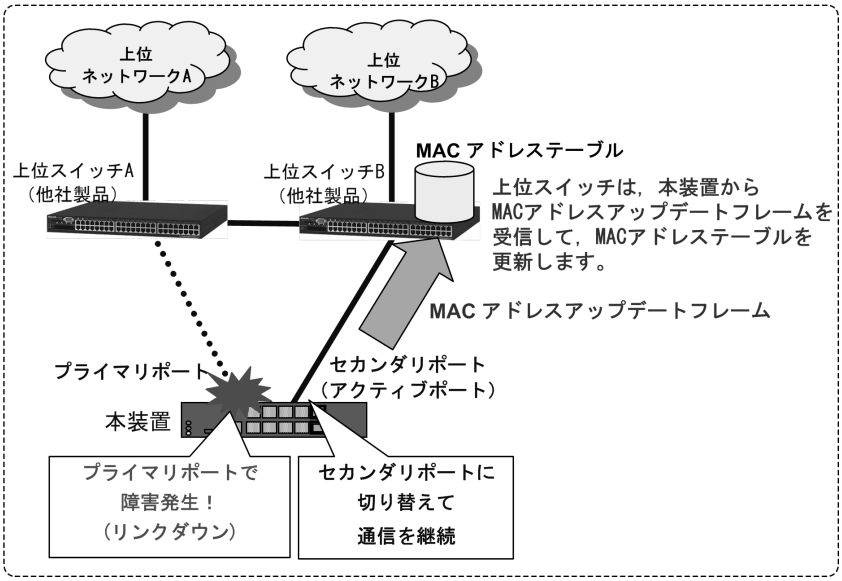
フラッシュ制御フレームを受信することで，MAC アドレステーブルをクリアします。クリア範囲は 1 フレーム受信につき全エントリが対象です。

受信用のコンフィグレーションはありません。

17.1.4　MAC アドレスアップデート機能

上位スイッチが AX シリーズ以外（他社製品）などフラッシュ制御フレームを受信できない装置のときに，フラッシュ制御フレームのかわりに上位スイッチの MAC アドレステーブルを更新させる機能です。

図 17-5 MAC アドレスアップデート機能概要



（1） 送信動作

コンフィグレーションにより，MAC アドレステーブル更新を要求する MAC アドレスアップデート機能が設定されている場合，アクティブポートの変更時に MAC アドレスアップデートフレームを送信します。

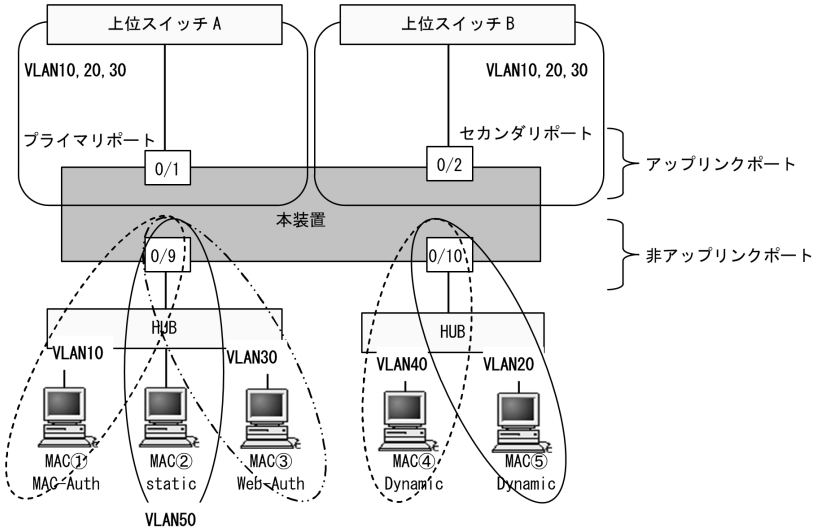
送信契機は，プライマリポート・セカンダリポートの切り替え後のポートがアップ直後に，アクティブポートに変更したポートから送信します。切り替えができないときは送信しません。

送信はアクティブポートの変更時に MAC アドレステーブルから取得した最大 1024 件分の MAC アドレスを送信します。対象となる MAC アドレスが 1024 件を超える場合，1025 件目以降は送信せず，運用ログを採取します。登録されている MAC アドレステーブルのうちで，送信対象となる MAC アドレスは以下の条件です。

- 非アップリンクポートで学習していること
- 学習した MAC アドレスの VLAN がアップリンクポートに含まれていること
- スタティック，ダイナミック，認証（Dot1x，WebAuth，MacAuth）で登録されていること（Snoop は，MAC アドレスアップデートフレーム送信対象外です。）
- 本装置の装置 MAC アドレスであること
- コンフィグレーションで指定した対象外 VLAN に含まれていないこと
  （後述の「(b) MAC アドレスアップデート機能の対象 VLAN と対象外 VLAN」を参照してください。）

MAC アドレス送信対象例を次の図に示します。

図 17-6　MAC アドレス送信対象例



〔VLAN 設定〕
1. 非アップリンクポートの VLAN：10, 20, 30, 40, 50
2. 学習した VLAN のうち，アップリンクポートに含まれている VLAN：10, 20, 30
3. MAC アドレスアップデート機能の対象外に指定した VLAN：30

表 17-6　MAC アドレス送信対象結果

MAC アドレス	VLAN	学習状態	ポート	送信対象
MAC ①	10	MacAuth	0/9	○
MAC ②	50	Static	0/9	×
MAC ③	30	WebAuth	0/9	×
MAC ④	40	Dynamic	0/10	×
MAC ⑤	20	Dynamic	0/10	○

（凡例）
　○：送信する　×：送信しない

(a) フレーム再送回数

コンフィグレーションにより最大 3 回まで再送回数を設定できます。再送時は，MAC アドレステーブルの再取得は行わず，1 度目と同一フレームを送信します。

(b) MAC アドレスアップデート機能の対象 VLAN と対象外 VLAN

- 対象 VLAN
  非アップリンクポートで学習した VLAN のうち，アップリンクポートに含まれる全 VLAN が対象 VLAN です。
  MAC アドレスアップデート機能は，上記 VLAN に含まれる MAC アドレスをすべて送信します。
- 対象外 VLAN
  MAC アドレスを MAC アドレスアップデート機能の送信対象から除外するときは，VLAN 単位で除外することができます。コンフィグレーションで，上記の対象 VLAN に対して対象外 VLAN を設定します。指定した VLAN で学習した MAC アドレスは，MAC アドレスアップデートフレームで送信しません。

(c) フラッシュ制御フレーム送受信機能との混在について

フラッシュ制御フレーム送信機能と本機能は同一ポートに設定できません。別のプライマリポートに設定して装置内の混在使用は可能です。フラッシュ制御フレームの受信機能は同一ポートで混在動作します。

(2) 受信動作

MAC アドレスアップデートフレームの受信により，通常の MAC アドレス学習を行い MAC アドレステーブルを更新します。

受信用のコンフィグレーションはありません。

17.1.5 装置起動時のアクティブポート固定機能

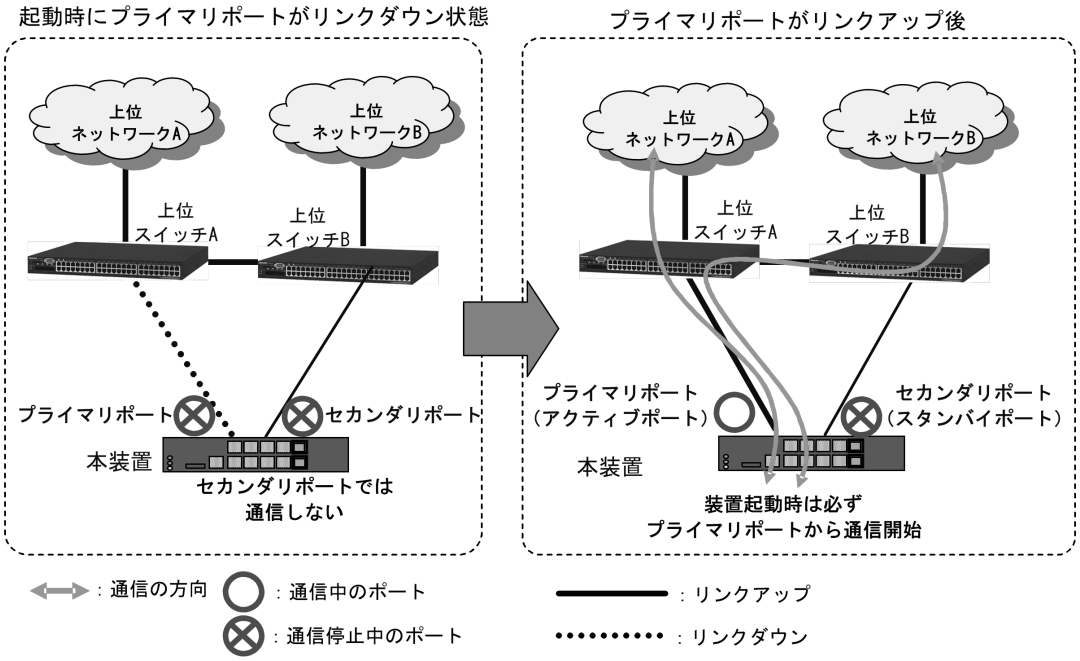
装置起動時のアクティブポート固定機能は，本装置の起動時に，必ずプライマリポートから通信を開始したい場合に利用します。この機能を有効にした装置は，起動時にセカンダリポートがリンクアップしていても，プライマリポートがリンクアップするまではアップリンクポートでの通信をしません。

アクティブポート固定機能は次に示す条件のどれかを満たすと解除されて，アクティブポートを決定します。アクティブポートが決定したあとは，通常と同じ動作となり，アクティブポートでの障害発生，または運用コマンド実行によってアクティブポートを切り替えます。

- プライマリポートがリンクアップした場合
- 運用コマンド set switchport-backup active の実行によって，セカンダリポートがアクティブポートに遷移した場合
- スタック動作時，マスタスイッチの切り替えが発生した場合

装置起動時のアクティブポート固定機能有効時の動作を次の図に示します。

図 17-7 装置起動時のアクティブポート固定機能有効時の動作



17.1.6 運用ログ，MIB・トラップについて

（1） 運用ログの採取について

本機能で実施したプライマリポート・セカンダリポートの切り替え・切り戻しのポート動作や，フラッシュ制御フレーム受信による MAC アドレステーブルクリア動作や，MAC アドレスアップデートフレーム送信時の MAC アドレス超過検出を装置イベントとして運用ログに採取します。運用ログは運用コマンド show logging で確認できます。

また，syslog サーバへのログ出力機能が設定されていると，採取した運用ログを syslog サーバへ送信します。

（2） プライベート MIB/Trap について

本機能はプライベート MIB およびプライベート Trap をサポートしています。プライベート MIB については，マニュアル「MIB レファレンス」を参照してください。

プライベート Trap の発行可否はコンフィグレーションコマンド snmp-server host で設定してください。

17.1.7 他機能との共存

他機能との共存については，次の表に示す動作となります。

表 17-7 他機能と共存時の動作

共存機能	共存可否	共存時の動作
スタック	可能	「コンフィグレーションガイドVol.1 7 スタックの解説【OP-WLE】」を参照してください。
リンクアグリゲーション	可能	リンクアグリゲーションでも動作します。
VLAN トンネリング	不可 （ポート共存不可）	アップリンクポートでは使用できません。
Tag 変換	不可 （ポート共存不可）	アップリンクポートでは使用できません。
スパニングツリー	不可 （ポート共存不可）	アップリンクポートではスパニングツリー強制 Disable（ポート単位）。
Ring Protocol	可能 （一部制限あり）	リングポートではアップリンク・リダンダントを使用できません。
L2 ループ検知	可能	コンフィグレーションで設定されたとおり動作します。 ただし，アップリンク・リダンダントによる Blocking ポートでは，L2 ループ検知フレームを送受信しません。
GSRP aware	可能	通常どおり動作します。 ただし，アップリンク・リダンダントによる Blocking ポートでは GSRP Flush request フレームを受信しません。
OAN	可能	コンフィグレーションで設定されたとおり動作します。
認証機能	不可 （ポート共存不可）	本機能と下記の機能は装置内共存でご使用ください。 • IEEE802.1X • Web 認証 • MAC 認証 アップリンクポート内で上記機能との共存運用は推奨しておりません。
DHCP snooping	不可 （ポート共存不可）	本機能と DHCP snooping 機能は装置内共存でご使用ください。 アップリンクポート内での共存運用は推奨しておりません。

共存機能	共存可否	共存時の動作
MACアドレステーブルスタティック定義	不可 (ポート共存不可)	コンフィグレーションは設定可能です。 ただし，プライマリ・セカンダリ切り替えにより，MACアドレステーブルスタティック定義のポートが無効になるため，実際の共存はできません。
ホワイトリスト機能	可能 (一部制限あり)	「14.1.5　他機能との共存」を参照してください。

共存機能	共存可否	共存時の動作
その他機能	可能	プライマリ，セカンダリのいずれかが Forwarding 状態のポートだけ動作可能です。 共存機能の動作についてはプライマリ，セカンダリの各ポートの設定状態に従います。 よってプライマリおよびセカンダリポートにそれぞれ別々の機能が設定されていた場合，そのとき動作しているポートの設定に従い機能が動作します。 なお，プライマリ，セカンダリポートのコンフィグレーション設定の同一性チェックなどは行いません。

17.1.8 アップリンク・リダンダント使用時の注意事項

(1) L2 ループ検知と併用時について

L2 ループ検知ポートを send だけ設定した場合，ループは検知しますがプライマリ・セカンダリの切り替えは発生しません。

セカンダリポートへ切り替え後，セカンダリポートでも L2 ループ検知を実施した場合，システム的にループ要因が解消されていないときは，再度ループを検出します。

プライマリまたはセカンダリポートと L2 ループ検知（send-inact）ポートを兼用したときは，他のポートから自発の L2 ループ検知フレームを受信するとプライマリまたはセカンダリポートに設定した send-inact ポートを閉塞します。

(2) アップリンクポートのペアについて

プライマリ・セカンダリのペアになるポートの VLAN は，同一設定にしてください。

(3) 上位スイッチでスパニングツリー使用時のタイマ切り戻し時間設定について

上位スイッチでスパニングツリーを使用しているときは，リンクダウンから復帰すると「Listening」または「Learning」状態となり，すぐには通信することができません。このような時はタイマ切り戻し時間を 30 秒以上で設定することをお勧めします。

(4) フラッシュ制御フレーム送受信機能の使用について

- 上位スイッチで，アップリンク・リダンダントのフラッシュ制御フレーム受信機能をサポートしていることをご確認ください。
  未サポートのスイッチでは，フラッシュ制御フレームを本装置から送信しても，MAC アドレステーブルはクリアされません。この場合，MAC アドレスアップデート機能をご使用ください。
- フラッシュ制御フレーム送信設定で VLAN Tag 値を指定したときは，該当ポートがアクセスポートのときも Tagged フレームでフラッシュ制御フレームを送信します。
- フラッシュ制御フレーム送信設定は，プライマリポートに設定してください。

(5) MAC アドレスアップデート機能の使用について

- MAC アドレスアップデート機能は，プライマリポートに設定してください。
- フラッシュ制御フレーム送信機能と本機能は同一ポートに設定できません。別のプライマリポートに設定して装置内の混在使用は可能です。フラッシュ制御フレームの受信機能は同一ポートで混在動作します。

(6) ループ構成での設定変更について

アップリンク・リダンダントは，基本的にループ構成のネットワークで使用します。

アップリンク・リダンダントの設定変更時は，あらかじめアップリンク・リダンダント対象ポートを shutdown し，設定変更後に shutdown を解除してください。shutdown しないで設定変更すると，ループが発生する場合があります。

(7) プライマリ・セカンダリポートの切り替え・切り戻し時間について

本機能とログ出力機能 (syslog) を併用時に，プライマリ・セカンダリポートに多数の VLAN が設定されている場合や，多数の MAC アドレスエントリを学習している場合，プライマリ・セカンダリの切り替え・切り戻しに時間がかかることがあります。

17.2　コンフィグレーション

17.2.1　コンフィグレーションコマンド一覧

アップリンク・リダンダントのコンフィグレーションコマンド一覧を次の表に示します。

表 17-8　コンフィグレーションコマンド一覧

コマンド名	説明
switchport backup interface	プライマリ・セカンダリポートと自動切り戻し，またはタイマ切り戻し時間を設定します。
switchport backup flush-request transmit	上位スイッチへ MAC アドレステーブルクリアを要求するフラッシュ制御フレーム送信を設定します。
switchport backup mac-address-table update transmit	上位スイッチへ MAC アドレステーブルを更新させる MAC アドレスアップデートフレーム送信を設定します。
switchport backup mac-address-table update exclude-vlan	MAC アドレスアップデートフレーム送信時に対象から除外する VLAN を設定します。
switchport backup mac-address-table update retransmit	MAC アドレスアップデートフレームの再送回数を設定します。
switchport-backup startup-active-port-selection	装置起動時のアクティブポート固定機能を有効にします。

17.2.2　プライマリ・セカンダリポートのペアとタイマ切り戻し時間の設定

［設定のポイント］

イーサネットポート 0/1 をプライマリポート，イーサネットポート 0/8 をセカンダリポートとして設定します。また，プライマリポートが復旧したときのタイマ切り戻し時間を設定します。

［コマンドによる設定］

1. **(config)# interface gigabitethernet 0/1**
   (config-if)# switchport backup interface gigabitethernet 0/8 preemption-delay 10
   (config-if)# exit
   プライマリポートとなるポート 0/1 のコンフィグレーションモードへ移行します。セカンダリポートとしてポート 0/8 とタイマ切り戻し時間 10 秒を設定します。セカンダリポートへ切り替え後，プライマリポートが復旧して 10 秒以上継続したときに，プライマリポートへ切り戻します。

［注意事項］

上位スイッチでスパニングツリーを使用しているときは，リンクダウンから復帰すると「Listening」または「Learning」状態となり，すぐには通信することができません。このような時はタイマ切り戻し時間を 30 秒以上で設定することをお勧めします。

17.2.3 上位スイッチに対するフラッシュ制御フレーム送受信機能の設定

［設定のポイント］

イーサネットポート 0/1 をプライマリポートとし，フラッシュ制御フレームの送信を設定します。また，フラッシュ制御フレームに付加する VLAN Tag 値を設定します。受信用の設定はありません。

［コマンドによる設定］

1. **(config)# vlan 10,50**
   (config-vlan)# exit
   VLAN 10,50 を設定します。

2. **(config)# interface gigabitethernet 0/1**
   (config-if)# switchport mode trunk
   (config-if)# switchport trunk allowed vlan 10,50
   (config-if)# switchport trunk native vlan 10
   ポート 0/1 をトランクポートとし，VLAN 10 と 50 を設定します。また，ネイティブ VLAN に 10 を設定します。

3. **(config-if)# switchport backup flush-request transmit vlan 50**
   (config-if)# exit
   フラッシュ制御フレームに付加する VLAN Tag 値として 50 を設定します。

［注意事項］

1. 本設定で VLAN Tag 値を指定したときは，該当ポートがアクセスポートのときも Tagged フレームでフラッシュ制御フレームを送信します。
2. 本設定は，プライマリポートに設定してください。

17.2.4 上位スイッチに対する MAC アドレスアップデート機能の設定

［設定のポイント］

イーサネットポート 0/1 をプライマリポートとし，以下を設定します。

- トランクポートと VLAN 10，20，30，50，ネイティブ VLAN10 を設定
- MAC アドレスアップデート機能を有効にする
- MAC アドレスアップデート機能の対象外 VLAN
- アップデートフレームの再送回数

イーサネットポート 0/2 をセカンダリポートとし，プライマリポートと同じ VLAN を設定します。受信用の設定はありません。

［コマンドによる設定］

1. **(config)# vlan 10,20,30,50**
   (config-vlan)# exit
   VLAN 10,20,30,50 を設定します。

2. **(config)# interface gigabitethernet 0/1**
   (config-if)# switchport mode trunk

(config-if)# switchport trunk allowed vlan 10,20,30,50
(config-if)# switchport trunk native vlan 10
ポート 0/1 をトランクポートとし，VLAN 10，20，30，50 を設定します。また，ネイティブ VLAN に 10 を設定します。

3. **(config-if)# switchport backup mac-address-table update transmit**
MAC アドレスアップデート機能を有効にします。
4. **(config-if)# switchport backup mac-address-table update exclude-vlan 20**
対象外 VLAN として VLAN20 を設定します。
5. **(config-if)# switchport backup mac-address-table update retransmit 3**
(config-if)# exit
アップデートフレームの再送回数を 3 回に設定します。
6. **(config)# interface gigabitethernet 0/2**
(config-if)# switchport mode trunk
(config-if)# switchport trunk allowed vlan 10,20,30,50
(config-if)# switchport trunk native vlan 10
(config-if)# exit
ポート 0/2 をトランクポートとし，VLAN 10，20，30，50 を設定します。また，ネイティブ VLAN に 10 を設定します。

[注意事項]

1. 本設定は，プライマリポートに設定してください。

17.3 オペレーション

17.3.1 運用コマンド一覧

アップリンク・リダンダントの運用コマンド一覧を次の表に示します。

表 17-9 運用コマンド一覧

コマンド名	説明
show switchport-backup	アップリンク・リダンダント情報を表示します。
show switchport-backup statistics	フラッシュ制御フレームの統計情報を表示します。
clear switchport-backup statistics	フラッシュ制御フレームの統計情報をクリアします。
set switchport-backup active	アクティブポートを変更する場合に，新しくアクティブポートになるポートを指定します。
show switchport-backup mac-address-table update	MAC アドレスアップデートフレームの情報を表示します。
show switchport-backup mac-address-table update statistics	MAC アドレスアップデートフレームの統計情報を表示します。
clear switchport-backup mac-address-table update statistics	MAC アドレスアップデートフレームの統計情報をクリアします。

17.3.2 アップリンク・リダンダント状態の表示

(1) 切り替え状態とフレッシュ制御フレーム送信 VLAN の表示

プライマリポート・セカンダリポートの切り替え状態や，自動切り戻しまたはタイマ切り戻しの残時間や，送信 VLAN を表示します。

運用コマンド show switchport-backup の実行結果を次の図に示します。

図 17-8 show switchport-backup の実行結果

```
> show switchport-backup

Date 20XX/05/20 02:27:19 UTC
Startup active port selection: primary only
Switchport backup pairs                                 Preemption    Flush
 Primary    Status      Secondary  Status      Delay Limit   VLAN
 Port 0/1   Blocking    Port 0/8   Forwarding      -     -   4094
 Port 0/3   Blocking    ChGr 4     Forwarding    100    94     10
*Port 0/4   Down        Port 0/5   Down            -     -      -
 Port 0/6   Blocking    ChGr 1     Forwarding     30     2   untag
 ChGr 64    Blocking    Port 0/2   Forwarding    300   298    100

>
```

[注意事項]

下記のケースはプライマリ / セカンダリペアの情報を表示しません。

- セカンダリポートで指定したポートチャネルインタフェースのコンフィグレーションがない場合

(2) フラッシュ制御フレーム統計情報の表示

フラッシュ制御フレームの送受信数や，MAC アドレステーブルクリアを実行したフレーム受信数などの統計情報を表示します。

運用コマンド show switchport-backup statistics の実行結果を次の図に示します。

図 17-9 show switchport-backup statistics の実行結果

```
> show switchport-backup statistics

Date 20XX/05/20 17:34:51 UTC
System ID : 00ed.f009.0001
Port 0/1  Transmit : on
          Transmit Total packets      :          3
          Receive  Total packets      :          0
                   Valid packets      :          0
                   Unknown version    :          0
                   Self-transmitted   :          0
                   Duplicate sequence :          0
  Last change time   : 20XX/05/20 16:52:21 UTC (00:42:30 ago)
  Last transmit time : 20XX/05/20 16:52:22 UTC (00:42:29 ago)
  Last receive time  : -
   Sender system ID  : 0000.0000.0000
              :
              :

>
```

（3） 切り替え状態と MAC アドレスアップデートフレーム対象 VLAN の表示

プライマリポート・セカンダリポートの切り替え状態や，自動切り戻しまたはタイマ切り戻しの残時間や，対象 VLAN リストと対象外 VLAN を表示します。

運用コマンド show switchport-backup mac-address-table update の実行結果を次の図に示します。

図 17-10 show switchport-backup mac-address-table update の実行結果

```
> show switchport-backup mac-address-table update

Date 20XX/05/20 18:02:40 UTC
Startup active port selection: primary only
Switchport backup pairs                          Preemption    Retransmit
 Primary    Status      Secondary  Status       Delay Limit
 Port 0/1   Down        Port 0/8   Forwarding      0     -            -
  VLAN            : 1,101-149,151-200,2001-2049,2051-2100,4040-4049,4051-4094
  Exclude-VLAN    : 50,150,1050,2050,3050,4050

Switchport backup pairs                          Preemption    Retransmit
 Primary    Status      Secondary  Status       Delay Limit
 Port 0/3   Down        Port 0/6   Forwarding      0     -            3
  VLAN            : 1,101-149,151-200,2001-2049,2051-2100,4040-4049,4051-4094
  Exclude-VLAN    : 50,150,1050,2050,3050,4050

Switchport backup pairs                          Preemption    Retransmit
 Primary    Status      Secondary  Status       Delay Limit
 ChGr 1     Down        ChGr 2     Forwarding      0     -            3
  VLAN            : 1,101-149,151-200,2001-2049,2051-2100,4040-4049,4051-4094
  Exclude-VLAN    : 50,150,1050,2050,3050,4050

>
```

[注意事項]

下記のケースはプライマリ / セカンダリペアの情報を表示しません。

- セカンダリポートで指定したポートチャネルインタフェースのコンフィグレーションがない場合

（4） MAC アドレスアップデートフレーム統計情報の表示

MAC アドレスアップデートフレームの再送信回数や，切り替え発生回数などの統計情報を表示します。

運用コマンド show switchport-backup mac-address-table update statistics の実行結果を次の図に示します。

図 17-11 show switchport-backup mac-address-table update statistics の実行結果

```
> show switchport-backup mac-address-table update statistics

Date 20XX/05/20 18:04:33 UTC
System ID : 0012.e244.0000
Port 0/1  Transition count                 :      20094
          Update transmit total packets    :          0
          Transmission over flows          :          0
  Last change time   : 20XX/05/20 16:25:55 UTC (01:38:38 ago)
  Last transmit time : -

Port 0/3  Transition count                 :      20094
          Update transmit total packets    :        294
          Transmission over flows          :          0
  Last change time   : 20XX/05/20 16:25:59 UTC (01:38:34 ago)
  Last transmit time : 20XX/05/20 16:26:07 UTC (01:38:26 ago)

Port 0/4  Transition count                 :      18743
          Update transmit total packets    :     325020
          Transmission over flows          :       9224
  Last change time   : 20XX/05/20 18:01:31 UTC (00:03:02 ago)
  Last transmit time : 20XX/05/20 18:01:36 UTC (00:02:57 ago)

Port 0/6  Transition count                 :      18743
          Update transmit total packets    :    4098830
          Transmission over flows          :      10569
  Last change time   : 20XX/05/20 18:01:37 UTC (00:02:56 ago)
  Last transmit time : 20XX/05/20 18:04:22 UTC (00:00:11 ago)

ChGr 1    Transition count                 :        511
          Update transmit total packets    :      30553
          Transmission over flows          :        480
  Last change time   : 20XX/05/20 18:01:29 UTC (00:03:04 ago)
  Last transmit time : 20XX/05/20 18:01:19 UTC (00:03:14 ago)

ChGr 2    Transition count                 :        512
          Update transmit total packets    :     128844
          Transmission over flows          :        480
  Last change time   : 20XX/05/20 18:01:33 UTC (00:03:00 ago)
  Last transmit time : 20XX/05/20 18:04:32 UTC (00:00:01 ago)

>
```

[注意事項]

下記のケースはプライマリ / セカンダリペアの情報を表示しません。

- セカンダリポートで指定したポートチャネルインタフェースのコンフィグレーションがない場合

17.3.3 アクティブポートの手動変更

運用コマンド set switchport-backup active で，アクティブポートを変更できます。

このコマンドは，指定したポートがスタンバイポートの場合だけ動作します。

図 17-12 set switchport-backup active の実行結果

```
# set switchport-backup active port 0/1
Are you sure to change the forwarding port to specified port? (y/n): y

#
```

18 ストームコントロール

ストームコントロールはフラッディング対象フレーム中継の量を制限する機能です。この章では，ストームコントロールの解説と操作方法について説明します。

18.1 解説

18.1.1 ストームコントロールの概要

レイヤ2ネットワークでは，ネットワーク内にループが存在すると，ブロードキャストフレームなどがスイッチ間で無制限に中継されて，ネットワークおよび接続された機器に異常な負荷を掛けることになります。このような現象はブロードキャストストームと呼ばれ，レイヤ2ネットワークでは避けなければならない問題です。マルチキャストフレームが無制限に中継されるマルチキャストストーム，ユニキャストフレームが無制限に中継されるユニキャストストームも防止する必要があります。

ネットワークおよび接続された機器への影響を抑えるために，スイッチでフラッディング対象フレーム中継の量を制限する機能がストームコントロールです。

本装置では，イーサネットインタフェースごとに，ストーム検出閾値（上限閾値）として1秒間で受信する最大フレーム数を設定でき，その値を超えたフレームを廃棄します。閾値の設定は，ブロードキャストフレーム，マルチキャストフレーム，ユニキャストフレームの3種類のフレームで個別に設定します。

さらに，受信したフレーム数が閾値を超えた場合，そのポートを閉塞したり，プライベートトラップやログメッセージを出力できます。

18.1.2 流量制限機能

ストーム検出時，本装置が自動でトラフィック停止または流量制限／再開を行うことができます。

本装置ではブロードキャストフレーム，マルチキャストフレーム，ユニキャストフレームの種別毎にストーム検出閾値を超えたフレームを停止または指定した流量に制限します。指定した種別の1秒間の受信フレーム数がストーム検出閾値（上限閾値）を超えた場合，流量制限値（下限閾値）に流量を制限します。流量制限値を0指定することによりストーム検出後のトラフィックを停止することができます。

流量制限機能はストーム回復閾値以下の値を指定した時間以上継続した場合，自動的に解除します（流量制限解除監視時間）。流量制限解除後は，ストーム回復閾値でストームを監視します。

流量制限動作を次の図に示します。

図 18-1 流量制限動作

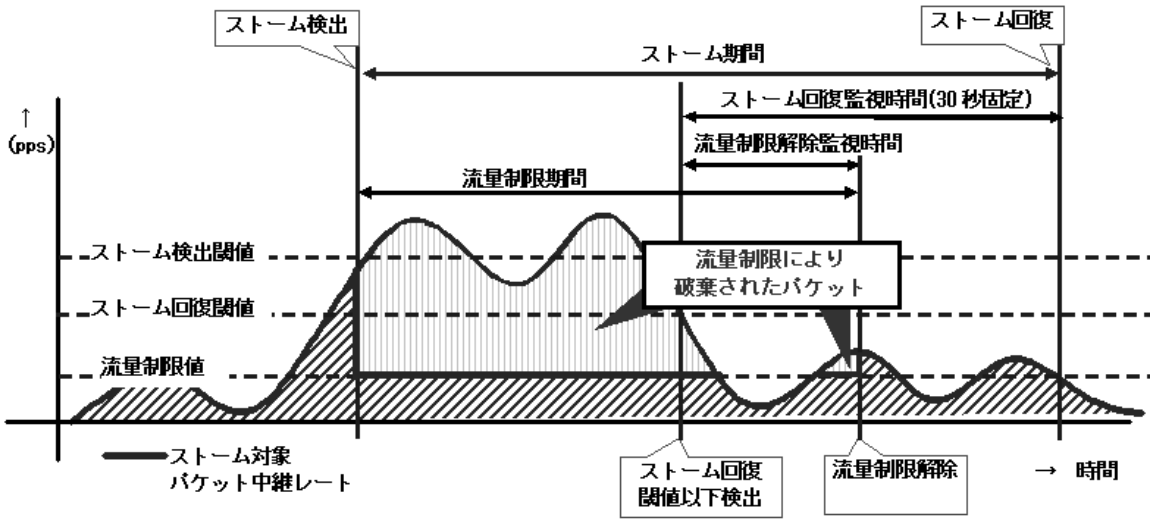


表 18-1 図内の動作および時間の説明

動作	説明
ストーム検出	ストームコントロールを検出する位置です。 action コマンドで設定した動作を開始します。
ストーム回復	ストームコントロールの回復を検出する位置です。 action log コマンドおよび action trap コマンドの回復が動作します。
ストーム期間	ストームコントロールが発生している期間です。 action log コマンドおよび action trap コマンドではこの間がストーム中となります。
ストーム検出閾値	ストームを検出する閾値です。コンフィグレーションで指定した値 (pps) を超えたときストームを検出し，ハードウェアでの超過分を廃棄します（上限閾値）。 ストーム回復閾値の指定がない場合は，「ストーム検出閾値 = ストーム回復閾値」として動作します。
ストーム回復閾値	ストーム回復を判断する閾値です。コンフィグレーションで指定した値 (pps) を一定時間下回ったとき，ストーム回復と判断します。
流量制限値	コンフィグレーションによりストーム検出後，流量値 (pps) を制限します。（下限閾値）
流量制限期間	流量制限を行う期間です。
ストーム回復監視時間	ストーム回復閾値以下の値 (pps) が 30 秒以上継続したとき，回復と判断します。
流量制限解除監視時間	ストーム回復閾値以下の値 (pps) がコンフィグレーションで指定した時間以上継続したとき，流量制限を解除します。

18.1.3 ストームコントロール使用時の注意事項

(1) ユニキャストフレームの扱い

本装置では，ユニキャストストームの検出と，フレームの廃棄で対象フレームが異なります。ユニキャストストームの検出は，受信するすべてのユニキャストフレームの数で行います。フレームの廃棄は，MAC アドレステーブルに宛先 MAC アドレスが登録されていないためにフラッディングされるユニキャストフレームだけが対象です。

(2) ストームの検出閾値と中継動作について

ストーム検出閾値を小さい値で指定した場合，ストーム検出後の数秒間は閾値以上のフレームを中継することがあります。その後は閾値を超えたフレームを廃棄します。

＜例：閾値を 100pps で指定した場合＞

- 閾値に対して 200%のフレームを受信時：最大約 1 秒間，100pps×200%中継
- 閾値に対して 110%のフレームを受信時：最大約 10 秒間，100pps×110% 中継

(3) ストームの検出と回復の検出

本装置は，1 秒間に受信したフレーム数が，コンフィグレーションで設定された閾値を超えたときに，ストームが発生したと判定します。ストームが発生したあと，1 秒間に受信したフレーム数が閾値以下の状態が 30 秒続いたときに，ストームが回復したと判定します。(図 18-1 流量制限動作参照)

(4) ポート閉塞時のストーム回復の確認について

ストーム発生時にポートを閉塞する場合は，そのポートではフレームを受信しなくなるため，ストームの回復も検出できなくなります。ストーム発生時にポートの閉塞を設定した場合は，ネットワーク監視装置などの本装置とは別の手段でストームが回復したことを確認してください。

(5) 閾値の設定について

各フレーム種別の閾値は，次の表に示す刻み値で設定してください。

表 18-2 閾値の設定範囲と刻み値

閾値の設定範囲（単位：pps）	刻み値 （単位：pps）
0 ～ 1,500,000	10
1,500,000 ～ 10,000,000	100

(6) ポートチャネルインタフェースのストーム検出について

ポートチャネルインタフェースにストームコントロールを設定し，ストームを検出した場合，以下に示す動作となります。

- ポートチャネルインタフェース内でストーム未検出の物理ポートは，検出日時が表示されません。

(7) スタック動作時のストームコントロールについて

スタック動作時のストームコントロールについては，「コンフィグレーションガイド Vol.1　7. スタックの解説【OP-WLE】」を参照してください。

(8) フィルタ使用時のストーム検出

フィルタ廃棄とストーム検出が同時に発生すると，本来，中継されるべきフレームを含め，より多くのフレーム廃棄が発生する場合があります。

(9) 帯域監視使用時のストーム検出

帯域監視違反とストーム検出が同時に発生すると，本来，中継されるべきフレームを含め，より多くのフレーム廃棄が発生する場合があります。

18.2 コンフィグレーション

18.2.1 コンフィグレーションコマンド一覧

ストームコントロールのコンフィグレーションコマンド一覧を次の表に示します。

表 18-3 コンフィグレーションコマンド一覧

コマンド名	説明
storm-control	ストームコントロールの閾値を設定します。また，ストームを検出した場合の動作や回復時間を設定できます。

18.2.2 基本設定

● ブロードキャストフレームの抑制

ブロードキャストストームを防止するためには，イーサネットインタフェースで受信するブロードキャストフレーム数を閾値として設定します。ブロードキャストフレームには，ARP パケットなど通信に必要なフレームも含まれるので，閾値には通常使用するフレーム数を考慮して余裕のある値を設定します。

● マルチキャストフレームの抑制

マルチキャストストームを防止するためには，イーサネットインタフェースで受信するマルチキャストフレーム数を閾値として設定します。マルチキャストフレームには，BPDU などの制御マルチキャストや IPv4 マルチキャストパケットの制御パケットなど通信に必要なフレームも含まれるので，閾値には通常使用するフレーム数を考慮して余裕のある値を設定します。

● ユニキャストストームの抑制

ユニキャストストームを防止するためには，イーサネットインタフェースで受信するユニキャストフレーム数を閾値として設定します。閾値には通常使用するフレーム数を考慮して余裕のある値を設定します。

なお，本装置では，ユニキャストフレームの検出には，受信する全ユニキャストフレーム数を使用しますが，中継せずに廃棄するフレームは，MAC アドレステーブルに宛先 MAC アドレスが登録されていないためにフラッディングされるユニキャストフレームだけが対象です。特にストーム検出時の動作にポートの閉塞を指定する場合は，通常使用するフレームでストーム検出とならないよう，閾値の設定には十分余裕のある値としてください。

● ストーム検出時の動作

ストームを検出したときの本装置の動作を設定します。ポートの閉塞，プライベートトラップの送信，運用ログの出力を，ポートごとに組み合わせて選択できます。

- ポートの閉塞
  ストームを検出したとき，そのポートを inactive 状態にします。ストームが回復したあと，再びそのポートを active 状態に戻すには，運用コマンド activate を使用します。
- プライベートトラップの送信
  ストームを検出したときおよびストームの回復を検出したとき，プライベートトラップを送信して通知します。
- 運用ログの出力
  ストームを検出したときおよびストームの回復を検出したとき，運用ログを出力して通知します。ただし，ポートの閉塞時の運用ログは必ず出力します。

［設定のポイント］

設定できるインタフェースはイーサネットインタフェースです。
ストームが発生したとき，ポートを閉塞します。

［コマンドによる設定］

1. **(config)# interface gigabitethernet 0/10**
   (config-if)# storm-control broadcast level pps 50
   ブロードキャストフレームのストーム検出閾値を 50pps に設定します。

2. **(config-if)# storm-control multicast level pps 500**
   マルチキャストフレームのストーム検出閾値を 500pps に設定します。

3. **(config-if)# storm-control unicast level pps 1000**
   ユニキャストフレームのストーム検出閾値を 1000pps に設定します。

4. **(config-if)# storm-control action inactivate**
   (config-if)# exit
   ストームを検出したときに，ポートを inactive 状態にします。

18.2.3 拡張設定：流量制限

ストーム検出閾値は基本設定と同じですが，検出時はポートを閉塞しないで各フレーム種別ごとに指定した流量に制限します。

［設定のポイント］

ストームが発生したとき，受信フレームのストーム検出閾値を超えた場合，流量を制限します。
ストーム回復閾値以内に戻ったとき，自動的に流量制限を解除する流量制限解除監視時間を設定します。
また，ストーム検出時とストーム回復時に運用ログを出力するよう設定します。

［コマンドによる設定］

1. **(config)# interface gigabitethernet 0/10**
   (config-if)# storm-control broadcast level pps 50 40
   ポート 0/10 では，基本設定に追加して，ブロードキャストフレームのストーム回復閾値を 40pps に設定します。

2. **(config-if)# storm-control multicast level pps 500 400**
   基本設定に追加して，マルチキャストフレームのストーム回復閾値を 400pps に設定します。

3. **(config-if)# storm-control unicast level pps 1000 800**
   基本設定に追加して，ユニキャストフレームのストーム回復閾値を 800pps に設定します。

4. **(config-if)# storm-control action filter**
   流量制限設定を有効にします。

5. **(config-if)# storm-control filter-broadcast 30**
   ブロードキャストフレームの流量制限値を 30pps に設定します。

6. **(config-if)# storm-control filter-multicast 300**
   マルチキャストフレームの流量制限値を 300pps に設定します。

7. **(config-if)# storm-control filter-unicast 700**
   ユニキャストフレームの流量制限値を 700pps に設定します。

8. **(config-if)# storm-control filter-recovery-time 15**
   流量制限解除監視時間を 15 秒に設定します。

9. **(config-if)# storm-control action log**
   (config-if)# exit
   ストーム検出時とストーム回復時に運用ログを出力するよう設定します。

18.3 オペレーション

18.3.1 運用コマンド一覧

ストームコントロールの運用コマンド一覧を次の表に示します。

表 18-4 運用コマンド一覧

コマンド名	説明
show storm-control	ストームコントロールの状態表示

18.3.2 ストームコントロール状態の確認

運用コマンド show storm-control でストームコントロールの設定と運用状態を確認できます。

ストーム検出閾値とストーム回復閾値，流量制限値（下限閾値），ストームの検出状態が確認できます。また，ストーム検出時の検出回数や，最後に検出した時刻も確認できます。

detail パラメータを指定すると，ストームを検出時の動作や，流量制限監視時間やその残り時間なども表示します。

運用コマンド show storm-control の実行結果を次の図に示します。

図 18-2 show storm-control の実行結果

```
> show storm-control

Date 20XX/05/24 10:46:35 UTC
<Broadcast>
 Port    Detect Recovery   Filter  State            Count Last detect
 0/1        200      100      100  Filtering            1 20XX/05/24 10:46:25
 0/2        200      100        -  Forwarding           0 ----/--/-- --:--:--

<Unicast>
 Port    Detect Recovery   Filter  State            Count Last detect
 0/1      10000     5000     5000  Filtering            1 20XX/05/24 10:45:52
 0/2      10000     5000        -  Forwarding           0 ----/--/-- --:--:--

>
```

図 18-3 show storm-control detail の実行結果（ポート 0/1 ブロードキャストの詳細表示）

```
> show storm-control port 0/1 broadcast detail

Date 20XX/05/24 10:48:20 UTC
<Broadcast>
 Port 0/1
  Detect rate : 200         Recover rate : 100         Filter rate : 100
  Action : Filter,Trap,Log
  Filter recovery time : 30
  <Status>
  State : Filtering          Filter recovery remaining time : 30
  Current rate :        189  Current filter rate     :        100
  Detect count :          1  Last detect             : 20XX/05/24 10:46:25

>
```

19 IEEE802.3ah/UDLD

IEEE802.3ah/UDLD 機能は，片方向リンク障害を検出し，それに伴うネットワーク障害の発生を事前に防止する機能です。
この章では，IEEE802.3ah/UDLD 機能の解説と操作方法について説明します。

19.1 解説

19.1.1 概要

UDLD（Uni-Directional Link Detection）とは，片方向リンク障害を検出する機能です。

片方向リンク障害が発生すると，一方の装置では送信はできるが受信ができず，もう一方の装置では受信はできるが送信ができない状態になり，上位プロトコルで誤動作が発生し，ネットワーク上でさまざまな障害が発生します。よく知られている例として，スパニングツリーでのループ発生や，リンクアグリゲーションでのフレーム紛失が挙げられます。これらの障害は，片方向リンク障害を検出した場合に該当するポートを inactivate することによって未然に防ぐことができます。

IEEE802.3ah（Ethernet in the First Mile）で slow プロトコルの一部として位置づけられた OAM（Operations, Administration, and Maintenance）プロトコル（以下，IEEE802.3ah/OAM と示す）では，双方向リンク状態の監視を行うために，制御フレームを用いて定常的に対向装置と自装置の OAM 状態情報の交換を行い，相手装置とのフレームの到達性を確認する方式が述べられています。本装置では IEEE802.3ah/OAM 機能を用いて双方向リンク状態の監視を行い，その確認がとれない場合に片方向リンク障害を検出する方式で UDLD 機能を実現しています。

また，IEEE802.3ah/OAM プロトコルでは，Active モードと Passive モードの概念があり，Active モード側から制御フレームの送信が開始され，Passive モード側では，制御フレームを受信するまで制御フレームの送信は行いません。本装置のデフォルトコンフィグレーションは IEEE802.3ah/OAM 機能が有効になっていて，全ポートが Passive モードで動作します。

Ethernet ケーブルで接続された双方の装置のポートにコンフィグレーションコマンド efmoam active udld を設定することで，片方向リンク障害の検出動作を行います。コンフィグレーションコマンド efmoam active udld を設定したポートで片方向リンク障害を検出した場合，該当するポートを inactivate することで対向装置側のポートでもリンクダウンが検出され，接続された双方の装置で該当ポートの運用を停止します。

19.1.2 サポート仕様

IEEE802.3ah/UDLD 機能では，次の表に示すとおり IEEE802.3ah/OAM 機能をサポートしています。

表 19-1 IEEE802.3ah/UDLD でサポートする IEEE802.3ah OAMPDU

名称	説明	サポート
Information	相手装置に OAM 状態情報を送信する。	○
Event Notification	相手装置に Link Event の警告を送信する。	×
Variable Request	相手装置に MIB 変数を要求する。	×
Variable Response	要求された MIB 変数を送信する。	×
Loopback Control	相手装置の Loopback 状態を制御する。	×
Organization Specific	機能拡張用。	×

（凡例）○：サポート　×：未サポート

19.1.3 IEEE802.3ah/UDLD 使用時の注意事項

（1） IEEE802.3ah/UDLD 機能を設定した装置間に IEEE802.3ah/OAM 機能をサポートしない装置を接続した場合

一般的なスイッチでは，IEEE802.3ah/OAM 機能で使用する制御フレームは中継しません。このため，装置間で情報の交換ができず，コンフィグレーションコマンド efmoam active udld を設定したポートで片方向リンク障害を検出してしまいます。IEEE802.3ah/UDLD 機能の運用はできません。

（2） IEEE802.3ah/UDLD 機能を設定した装置間にメディアコンバータなどの中継装置を接続した場合

片方のリンク状態が切断された場合に，もう片方のリンク状態を自動的に切断しないメディアコンバータを装置間に設置した場合，装置間でリンク状態の認識にずれが生じます。このため，コンフィグレーションコマンド efmoam active udld を設定したポートで相手装置が動作していない状態でも片方向リンク障害を検出してしまいます。復旧する際にも，双方の装置で同期をとる必要があり，運用が困難になります。片方のリンク状態が切断された場合に，もう片方のリンク状態を自動的に切断する機能のあるメディアコンバータを使用してください。

（3） 他社の UDLD 機能との接続について

UDLD 機能はそれぞれ各社の独自仕様で機能を実装しているため，本装置の IEEE802.3ah/UDLD 機能と他社装置の UDLD 機能の相互接続はできません。

（4） 他機能との共存について

（a） レイヤ 2 認証との共存

「5.9.3　レイヤ 2 認証機能と他機能の共存」を参照してください。

19.2 コンフィグレーション

19.2.1 コンフィグレーションコマンド一覧

IEEE802.3ah/UDLD のコンフィグレーションコマンド一覧を次の表に示します。

表 19-2 コンフィグレーションコマンド一覧

コマンド名	説明
efmoam active	物理ポートで IEEE802.3ah/OAM 機能を Active モードにします。
efmoam disable	IEEE802.3ah/OAM 機能を無効にします。
efmoam udld-detection-count	片方向リンク障害とするためのカウンタ値を指定します。

19.2.2 IEEE802.3ah/UDLD の設定

(1) IEEE802.3ah/UDLD 機能の設定

[設定のポイント]

IEEE802.3ah/UDLD 機能を運用するには，先ず装置全体で IEEE802.3ah/OAM 機能を有効にしておくことが必要です。本装置のデフォルトコンフィグレーションは IEEE802.3ah/OAM 機能が有効となっている状態（全ポート Passive モード）です。次に，実際に片方向リンク障害検出機能を動作させたいポートに対し，UDLD パラメータを付加した Active モードの設定をします。

ここでは，gigabitethernet 0/1 で IEEE802.3ah/UDLD 機能を運用させます。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 0/1**

ポート 0/1 のイーサネットインタフェースコンフィグレーションモードに移行します。

2. **(config-if)# efmoam active udld**
(config-if)# exit

ポート 0/1 で IEEE802.3ah/OAM 機能の Active モード動作を行い，片方向リンク障害検出動作を開始します。

(2) 片方向リンク障害検出カウントの設定

[設定のポイント]

片方向リンク障害は，相手からの情報がタイムアウトして双方向リンク状態の確認ができない状態が，決められた数だけ連続して発生した場合に検出します。この数が片方向リンク障害検出カウントです。双方向リンク状態は，1 秒に 1 回確認しています。

片方向リンク障害検出カウントを変更すると，実際に片方向リンク障害が発生してから検出するまでの時間を調整できます。片方向リンク障害検出カウントを少なくすると障害を早く検出する一方で，誤検出のおそれがあります。通常，本設定は変更する必要はありません。

片方向リンク障害発生から検出までのおよその時間を次に示します。なお，最大 10% の誤差が生じます。

5+（片方向リンク障害検出カウント）[秒]

［コマンドによる設定］

1. **(config)# efmoam udld-detection-count 60**
   片方向リンク障害検出とするための相手からの情報タイムアウト発生連続回数を 60 回に設定します。

19.3 オペレーション

19.3.1 運用コマンド一覧

IEEE802.3ah/OAM 機能の運用コマンド一覧を次の表に示します。

表 19-3 運用コマンド一覧

コマンド名	説明
show efmoam	IEEE802.3ah/OAM の設定情報およびポートの設定情報を表示します。
show efmoam statistics	IEEE802.3ah/OAM に関する統計情報を表示します。
clear efmoam statistics	IEEE802.3ah/OAM に関する統計情報をクリアします。

19.3.2 IEEE802.3ah/OAM 情報の表示

IEEE802.3ah/OAM 情報の表示は，運用コマンド show efmoam で行います。運用コマンド show efmoam は，IEEE802.3ah/OAM の設定情報と Active モードに設定されたポートの情報を表示します。また，運用コマンド show efmoam statistics では，IEEE802.3ah/OAM プロトコルの統計情報に加え，IEEE802.3ah/UDLD 機能で検出した障害状況を表示します。

図 19-1 show efmoam の実行結果

```
> show efmoam

Date 20XX/05/20 17:36:11 UTC
Port    Status              Dest MAC
0/1     Forced Down (UDLD)  0012.e214.ffae
0/2     Mutually Seen       0012.e214.ffaf
0/3     Partner Seen        0012.e214.ffb0
0/4     Down                unknown
0/5     Down                unknown

>
```

図 19-2 show efmoam statistics の実行結果

```
> show efmoam statistics

Date 20XX/05/20 17:35:25 UTC
Port 0/1 [Forced Down (UDLD)]
  OAMPDUs:Tx     :        133  Rx         :         57
          Invalid:          0  Unrecogn. :          0
  Expirings      :          1  Thrashings:          0  Blockings:          1
Port 0/2 [Mutually Seen]
  OAMPDUs:Tx     :        771  Rx         :        750
          Invalid:          0  Unrecogn. :          0
  Expirings      :          0  Thrashings:          0  Blockings:          0
Port 0/3 [Partner Seen]
  OAMPDUs:Tx     :        631  Rx         :        593
          Invalid:          0  Unrecogn. :          0
  Expirings      :          0  Thrashings:          0  Blockings:          0

>
```

20 L2 ループ検知

L2 ループ検知は，レイヤ 2 ネットワークでループ障害を検知し，ループの原因となるポートを閉塞状態にすることでループ障害を解消する機能です。
この章では，L2 ループ検知機能の解説と操作方法について説明します。

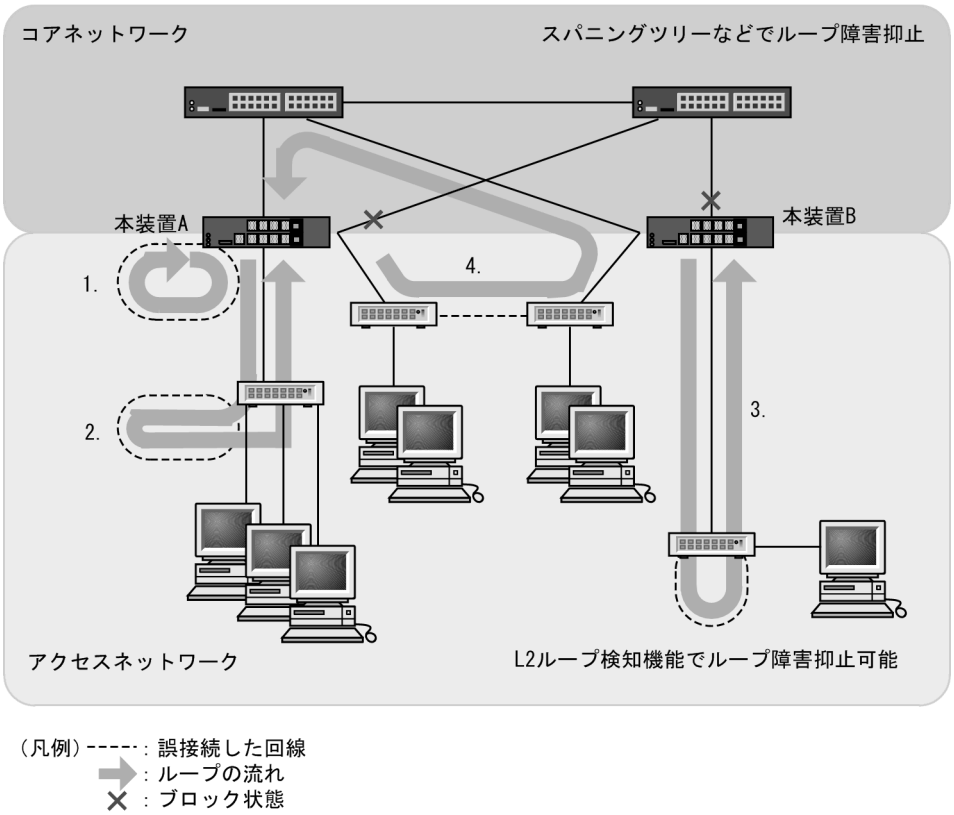
20.1　解説

20.1.1　概要

レイヤ 2 ネットワークでは，ネットワーク内にループ障害が発生すると，MAC アドレス学習が安定しなくなったり，装置に負荷が掛かったりして正常な通信ができない状態になります。このような状態を回避するためのプロトコルとして，スパニングツリーなどがありますが，L2 ループ検知機能は，一般的にそれらプロトコルを動作させているコアネットワークではなく，冗長化をしていないアクセスネットワークでのループ障害を解消する機能です。

L2 ループ検知機能は，本装置配下で発生した L2 ループ障害を検知したときに，検知したポートを閉塞（inactive）することで原因となっている個所をネットワークから切り離し，ネットワーク全体にループ障害が波及しないようにします。

図 20-1　ループ障害の発生例



図内 1.

本装置 A で回線を誤接続し，ループ障害が発生しています。

図内 2，3.

本装置 A または本装置 B から下位の装置または L2 スイッチで回線を誤接続し，ループ障害が発生しています。

図内 4.

下位の装置で回線を誤接続し，コアネットワークにわたるループ障害が発生しています。

L2 ループ検知機能は，このような本装置での誤接続や他装置での誤接続など，さまざまな場所でのループ

障害を検知できます。

20.1.2 動作概要

L2 ループ検知機能では，コンフィグレーションで設定したポート（物理ポートまたはチャネルグループ）から L2 ループ検知用の制御フレーム（L2 ループ検知フレーム）を定期的に送信します。L2 ループ検知機能が有効なポートで，本装置から送信した L2 ループ検知フレームを受信した場合にループ障害と判断し，受信したポートまたは送信元ポートを閉塞状態（inactive 状態）にします。

閉塞したポートは，ループ障害の原因を解決後に運用コマンドで active 状態にします。また，自動復旧機能を設定しておくと，自動的に active 状態にできます。

（1）L2 ループ検知機能のポート種別と動作

L2 ループ検知機能のポート種別は下記の種類があります。ポート種別はコンフィグレーションコマンド loop-detection で設定します。

- 検知ポート
  L2 ループ検知機能有効時のポート初期状態（コンフィグレーションコマンド loop-detection 未設定時の状態）です。
- 検知送信閉塞ポート（send-inact-port）
  L2 ループ検知機能が有効で，自装置からの L2 ループ検知フレームを受信時にポートを閉塞します。
- 検知送信ポート（send-port）
  L2 ループ検知機能が有効で，自装置からの L2 ループ検知フレームを受信してもポート閉塞はしません。
- アップリンクポート（uplink-port）
  上位ネットワークに接続しているポート，または基幹となるポートで，L2 ループ検知機能を有効にしているポートです。
- 検知対象外ポート（exception-port）
  L2 ループ検知機能が無効のポートです。

各ポートの動作は下記のとおりです。

表 20-1　ポート種別と動作

ポート種別	L2 ループ検知機能	L2 ループ検知フレーム送信	自装置からの L2 ループ検知フレームを受信時の動作		
			ポート閉塞の実施	動作ログの採取	トラップ発行
検知ポート	有効	×	×	○	○
send-inact-port	有効	○	○	○	○
send-port	有効	○	×	○	○
uplink-port	有効	×	※	○	○
exception-port	無効	×	×	×	×

（凡例）
　○：する　×：しない

注 ※
　アップリンクポートでのループ検知時は下記の動作となります。
- uplink-port は閉塞しません。
- L2 ループ検知フレームの送信元が send-inact-port の場合は，送信元ポートを閉塞します。
- L2 ループ検知フレームの送信元が send-port の場合は，送信元ポートを閉塞しません。

（2） L2 ループ検知フレームの送信について

（a） Tagged フレーム

トランクポートの "switchport trunk allowed vlan"，および MAC ポートの "switchport mac dot1q vlan" に対する L2 ループ検知フレームは，該当する VLAN 数分を Tagged フレームで送信します。

トランクポートの " switchport trunk native vlan" に対する L2 ループ検知フレームは，Untagged フレームで送信します。

（b） Untagged フレーム

- アクセスポート
  当該ポートに属する VLAN の L2 ループ検知フレームは，Untagged フレームで送信します。
- プロトコルポート，MAC ポート
  VLAN を多重させている場合，L2 ループ検知フレームを集約して，Untagged フレームで送信します。（多重 VLAN 分は送信しません。）

（c） 送信対象ポート

- interface gigabitethernet
- interface port-channel（物理ポート単位ではなく，チャネルグループ単位で送信します。）

各ポートの L2 ループ検知フレーム送信数は，ポートの種類（アクセス，トランク，プロトコル，MAC）と，収容 VLAN 数により異なります。

（d） 送信間隔

L2 ループ検知フレームは，検知送信閉塞ポートと検知送信ポートに所属しているすべての VLAN から，コンフィグレーションで設定した送信間隔で送信します。

L2 ループ検知フレームの送信間隔は，コンフィグレーションコマンド loop-detection interval で設定できます。

（e） 送信レートおよび送信フレーム数

L2 ループ検知フレームは，収容条件の範囲内で送信可能なポートおよび VLAN から送信します。それを超えるフレームは送信しません。フレームを送信できなかったポートや VLAN では，ループ障害が検知できなくなります。

収容条件については，マニュアル「コンフィグレーションガイド Vol.1 3.2 収容条件」を参照してください。

（3） L2 ループ検知フレームの受信とポート閉塞

（a） ポート閉塞までの L2 ループ検知回数の設定

ポートを閉塞するまでの L2 ループ検知回数は，コンフィグレーションコマンド loop-detection threshold で設定します。

本コマンドを省略した場合は，１回の L2 ループ検知でポートを閉塞します。本コマンドの設定は，一時的な L2 ループ障害検知で，検知送信閉塞ポートの閉塞を回避する場合に有効です。

（b） L2 ループ検知回数の保持について

自装置からの L2 ループ検知フレームを受信し，L2 ループ検知回数を計上します。計上した L2 ループ検知回数は，ポートを閉塞するまで保持し，ポート閉塞実施後にクリアします。

また，L2 ループ検知回数の保持時間をコンフィグレーションコマンド loop-detection hold-time で設定できます。L2 ループ検知フレームを受信してから，本コマンドで設定した時間内は検知回数を保持します。設定した保持時間内に再度 L2 ループ検知フレームを受信しなかった場合は，検知回数をクリアします。

(c) ポート閉塞

ポート閉塞は物理ポート単位に実施します。

チャネルグループに所属するポートは，所属する全物理ポートに対して inactivate を発行し閉塞します。スタンバイリンク機能（リンクダウン／非リンクダウン）で待機中のポートに対しても同様です。

(4) 閉塞したポートの復旧

L2 ループ検知機能で閉塞したポートを復旧させる手段として，手動復旧と自動復旧があります。

(a) 手動復旧

L2 ループ検知機能により閉塞したポートは，運用コマンド activate で物理ポート単位で復旧できます。チャネルグループのポートの場合も復旧手段は物理ポート単位とし，チャネルグループに所属する物理ポートのうち，1 ポートでもリンクアップした時点で，L2 ループ検知機能によるチャネルグループの閉塞状態が解除されます。

(b) 自動復旧

L2 ループ検知機能により閉塞したポートを，指定時間経過後に自動的に復旧する機能です。本機能は，コンフィグレーションコマンド loop-detection auto-restore-time で設定します。

チャネルグループのポートが閉塞した場合の復旧は，所属する全物理ポートに対して自動で activate を発行します。スタンバイリンク機能（リンクダウン／非リンクダウン）で待機中のポートに対しても，同様に自動で activate を発行します。

20.1.3 他機能との共存について

L2 ループ検知機能と他機能の共存については下記のようになります。

表 20-2 L2 ループ検知機能と他機能の共存

機能	項目	装置内共存	ポート共存	共存時の動作
リンクアグリゲーション	IEEE802.3ad	共存可	共存可	L2 ループ検知機能によりポート閉塞したチャネルグループに属する物理ポートが，リンクアップした場合に閉塞解除
MAC アドレステーブル	MAC アドレス学習	共存可	共存可	
ポート VLAN	port-based VLAN	共存可	共存可	Untagged フレームで送信
プロトコル VLAN	protocol-based VLAN	共存可	共存可	VLAN を多重させている場合，L2 ループ検知フレームを集約して送信
MAC VLAN	mac-based VLAN	共存可	共存可	
スパニングツリー	IEEE802.1d IEEE802.1w IEEE802.1s PVST+	共存可	共存可 ※1	Forwarding 時だけ L2 ループ検知フレームの送受信可能
DHCP snooping	端末フィルタ	共存可	共存可	L2 ループ検知フレームは DHCP snooping の対象外
フィルタ	permit/deny	共存可	共存可	

機能	項目	装置内共存	ポート共存	共存時の動作
QoS	優先度変更	共存可	共存可	L2 ループ検知フレームは QoS フローの対象外
自発フレームの優先度	user-priority 設定	共存可	共存可	L2 ループ検知フレームは自発フレームの優先度設定の対象外
レイヤ 2 認証	IEEE802.1X Web 認証 MAC 認証	共存可	共存可	認証前でも L2 ループ検知フレームは送受信可能
ホワイトリスト機能	学習状態 運用状態	共存可 ※2	共存可 ※2	「14.1.5　他機能との共存」を参照してください。

注 ※1

ポート共存の場合，L2 ループ検知機能で閉塞するポートは inactive にしますので，スパニングツリーはトポロジー変更が発生します。

注 ※2

コンフィグレーションコマンド white-list address permit loop-detection 設定時に共存可能です。

20.1.4　動作ログ・トラップについて

（1） 動作ログの採取

本機能では，受信フレームログとループ検知・閉塞イベントログの 2 種類を採取します。

（a） 受信フレームログ

本装置が送信した L2 ループ検知フレームの受信フレームを 1000 フレーム分を採取します。採取内容は，送信ポート・受信ポート・VLAN 番号・ポート動作などです。受信フレームログは運用コマンド show loop-detection logging で確認できます。

なお，受信フレームログは，syslog サーバへは送信されません。

（b） ループ検知・閉塞イベントログ

L2 ループ検知機能が検知したループ障害，および実施した閉塞・復旧のポート動作を装置イベントとして，運用ログに採取します。運用ログは運用コマンド show logging で確認できます。

なお，ループ検知・閉塞イベントログは syslog サーバへ送信されます。

（2） プライベート MIB/Trap について

本機能はプライベート MIB およびプライベート Trap をサポートしています。

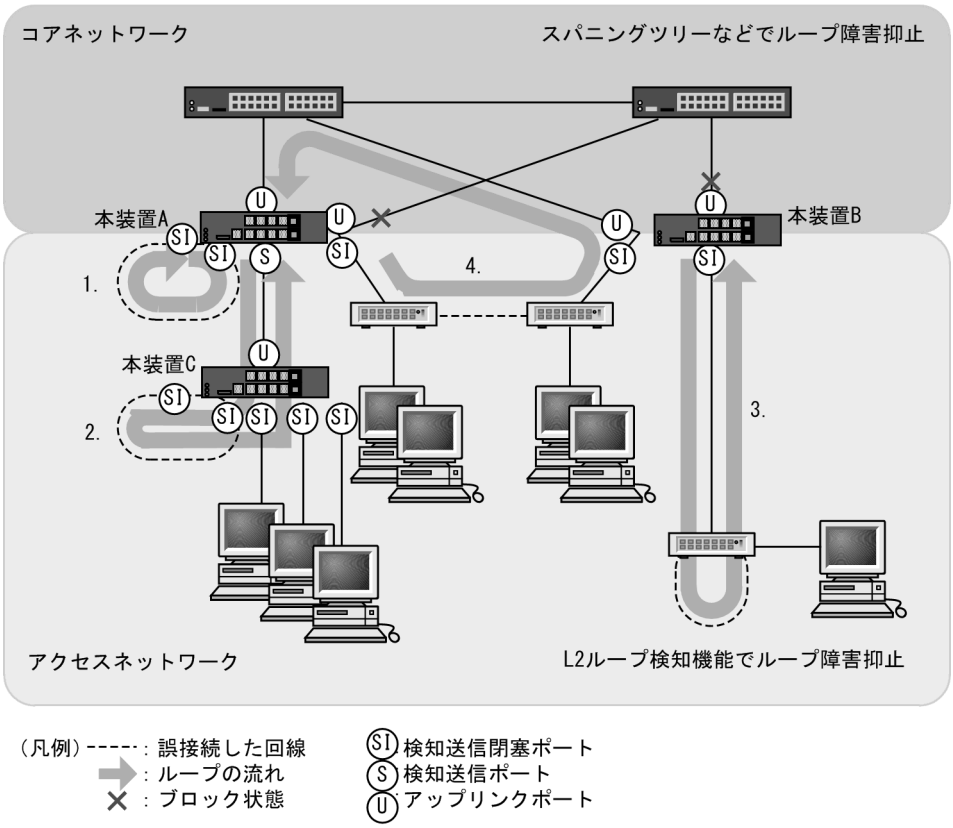
プライベート MIB については，マニュアル「MIB レファレンス」を参照してください。

プライベート Trap の発行可否はコンフィグレーションコマンド snmp-server host で設定してください。

20.1.5　適用例

L2 ループ検知機能を適用したネットワーク構成例を示します。

図 20-2 L2 ループ検知機能を適用したネットワーク構成例



（1） 検知送信閉塞ポートの適用

L2 ループ検知機能で一般的に設定するポート種別です。本装置 A，B で示すように，検知送信閉塞ポートを下位側のポートに設定しておくことで，図内 1，2，3 のような下位側の誤接続によるループ障害に対応します。

（2） 検知送信ポートの適用

ループ障害の波及範囲を局所化するためには，できるだけ下位の装置で本機能を動作させるほうが有効です。本装置 A と本装置 C のように多段で接続している場合に，図内 2. のような誤接続で本装置 A 側のポートを閉塞すると，本装置 C のループ障害と関係しないすべての端末で上位ネットワークへの接続ができなくなります。そのため，より下流となる本装置 C で L2 ループ検知機能を動作させることを推奨します。

なお，その場合は，本装置 A 側のポートには検知送信ポートを設定しておきます。この設定によって，正常運用時は本装置 C でループ障害を検知しますが，本装置 C で L2 ループ検知機能の設定誤りなどでループ障害を検知できないときには，本装置 A でループ障害を検知できます。（この場合，本装置 A はポートを閉塞しません。）

（3） アップリンクポートの適用

上位ネットワークに繋がっているポートまたはコアネットワークに接続するポートで設定します。この設定によって，図内 4. のような誤接続となった場合，本装置 A の送信元ポートが閉塞状態になるため，コアネットワークへの接続を確保できます。

20.1.6 L2 ループ検知使用時の注意事項

（1） プロトコル VLAN や MAC VLAN での動作について

L2 ループ検知フレームは，独自フォーマットの Untagged フレームです。プロトコルポートや MAC ポートではネイティブ VLAN として転送されるため，次に示す条件をどちらも満たしている場合，装置間にわたるループ障害が検知できないおそれがあります。

- コアネットワーク側のポートをアップリンクポートとして設定している
- コアネットワーク側にネイティブ VLAN を設定していない

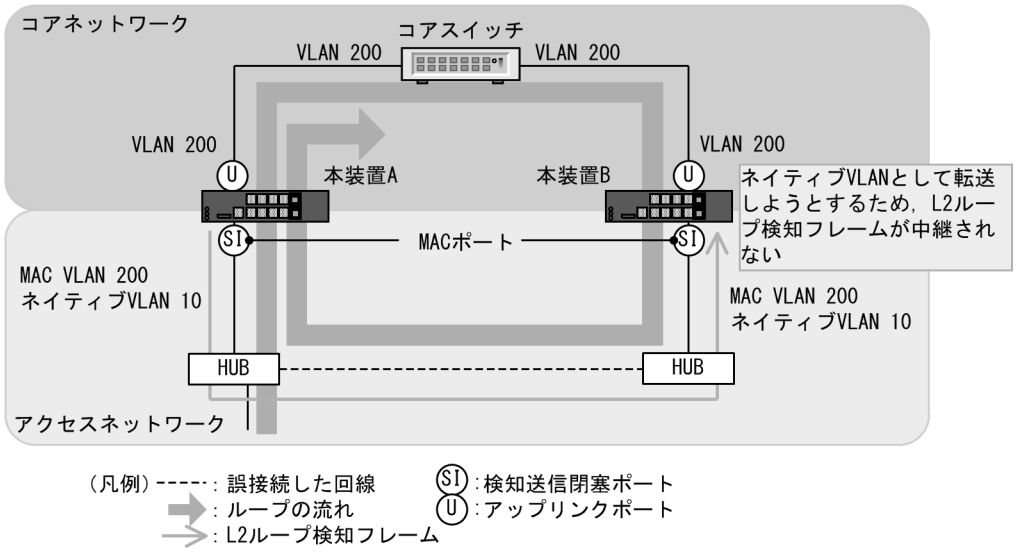
  この場合は，アップリンクポートとして設定しているコアネットワーク側のポートを検知送信ポートに設定すると，ループ障害を検知できます。具体的な構成例を次に示します。

（a） ループ検知の制限となる構成例

次の図に示す構成で本装置の配下の HUB 間を誤接続すると，装置間にわたるループが発生します。

本装置 A は HUB 側の検知送信閉塞ポートから L2 ループ検知フレームを送信し，コアスイッチ側のアップリンクポートからは送信しません。本装置 B は MAC ポートで受信した L2 ループ検知フレームをネイティブ VLAN として転送しようとするため，L2 ループ検知フレームはコアスイッチ側へ中継されません。この場合，L2 ループ検知フレームは本装置 A へ戻ってこないため，ループ障害を検知できません。

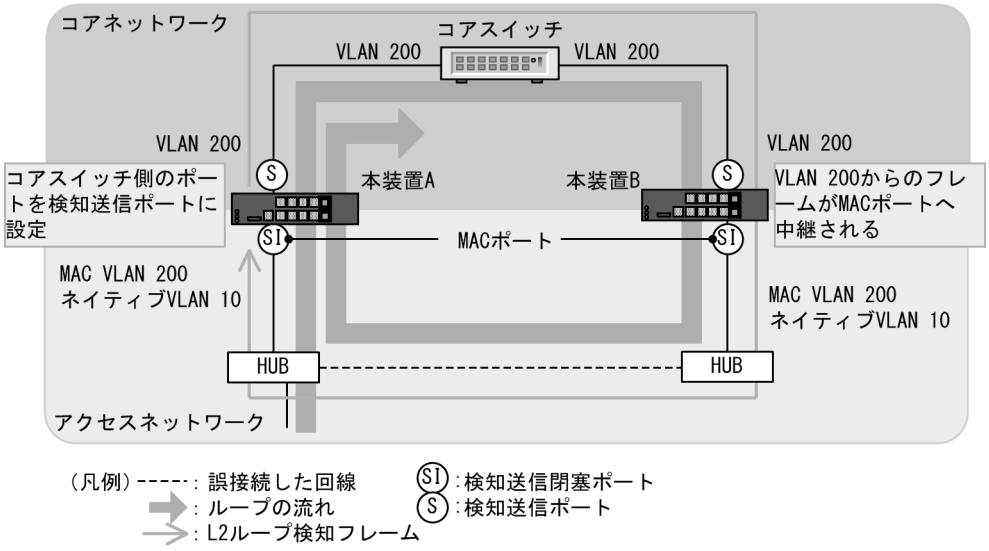
図 20-3 ループ検知の制限となる構成



（b） ループ検知可能な構成例

本装置 A のコアスイッチ側のポートを検知送信ポートに設定した場合，本装置 B はコアスイッチ側のポートから受信した L2 ループ検知フレームを MAC ポートへ中継するため，本装置 A でループ障害が検知できます。

図 20-4 ループ検知可能な構成



（2） Tag 変換使用時の動作について

次のような場合に，ループ障害を検知します。

- 自装置の Tag 変換ポートから送信した Tag 変換された L2 ループ検知フレームが，ネットワーク内で折り返り，自装置で受信した場合
- 他装置で Tag 変換された L2 ループ検知フレームを自装置で受信した場合

意図的に自装置に折り返すようなネットワーク構成にする場合は，対象ポートを検知対象外ポートに設定して，ループ障害を回避してください。

（3） L2 ループ検知機能の動作環境について

本機能を使用する場合に，同一ネットワーク内に L2 ループ検知未サポートの装置を配置したとき，その装置でループ検知フレームを受信するとフレームを廃棄します。そのため，その装置を含む経路でループ障害が発生しても検知できません。

（4） inactive 状態にしたポートを自動的に active 状態にする機能（自動復旧機能）について

スタティックリンクアグリゲーション上で自動復旧機能を使用する場合は，次の点に注意してください。

- オートネゴシエーションで接続する場合は回線速度を指定してください。指定しないと，回線品質の劣化などによって一時的に回線速度が異なる状態になり，低速回線が該当チャネルグループから離脱することがあります。この状態でループを検知した場合，該当チャネルグループで自動復旧機能が動作しないおそれがあります。

自動復旧機能が動作しない場合は，ループ原因を解消したあと，運用コマンド activate でポートを active 状態にしてください。

（5） スタック動作時の L2 ループ検知について

スタック動作時の L2 ループ検知については，「コンフィグレーションガイド Vol.1　7. スタックの解説【OP-WLE】」を参照してください。

20.2 コンフィグレーション

20.2.1 コンフィグレーションコマンド一覧

L2 ループ検知のコンフィグレーションコマンド一覧を次の表に示します。

表 20-3 コンフィグレーションコマンド一覧

コマンド名	説明
loop-detection	L2 ループ検知のポート種別を設定します。
loop-detection auto-restore-time	閉塞したポートを自動的に active 状態にする時間を設定します。
loop-detection enable	L2 ループ検知を有効にします。
loop-detection hold-time	ポート閉塞までの L2 ループ検知回数の保持時間を設定します。
loop-detection interval-time	L2 ループ検知フレームの送信間隔を設定します。
loop-detection threshold	ポート閉塞までの L2 ループ検知回数を設定します。

20.2.2 L2 ループ検知の設定

(1) L2 ループ検知有効設定と L2 ループ検知ポート種別の設定

[設定のポイント]

L2 ループ検知のコンフィグレーションでは，装置全体で機能を有効にする設定と，実際に L2 ループ障害を検知するポート，L2 ループ検知の対象外ポートなどを設定します。

[コマンドによる設定]

1. **(config)# loop-detection enable**
   L2 ループ検知を有効にします。

2. **(config)# interface gigabitethernet 0/2**
   (config-if)# loop-detection send-inact-port
   (config-if)# exit
   ポート 0/2 を検知送信閉塞ポートに設定します。

3. **(config)# interface gigabitethernet 0/4**
   (config-if)# loop-detection send-port
   (config-if)# exit
   ポート 0/4 を検知送信ポートに設定します。

4. **(config)# interface gigabitethernet 0/5**
   (config-if)# loop-detection uplink-port
   (config-if)# exit
   ポート 0/5 をアップリンクポートに設定します。

5. **(config)# interface gigabitethernet 0/1**
   (config-if)# loop-detection exception-port
   (config-if)# exit
   ポート 0/1 を L2 ループ検知対象外ポートに設定します。

(2) L2 ループ検知フレーム送信間隔の設定

[設定のポイント]

L2 ループ検知フレームの送信レートを超えたフレームは送信しません。フレームを送信できなかったポートや VLAN では，ループ障害を検知できなくなります。L2 ループ検知フレームの最大送信レートを超える場合は，送信間隔を長く設定し送信レートに収まるように設定します。

[コマンドによる設定]

1. **(config)# loop-detection interval-time 60**
   L2 ループ検知フレームの送信間隔を 60 秒に設定します。

(3) ポート閉塞条件の設定

[設定のポイント]

コマンド未設定の場合，1 回（初期値）のループ障害の検知でポートを閉塞します。瞬間的なループで閉塞したくない場合には，ポート閉塞までの L2 ループ検知回数を設定します。

[コマンドによる設定]

1. **(config)# loop-detection threshold 100**
   ポート閉塞までの L2 ループ検知回数 100 とし，100 以上となった場合にポートを閉塞するように設定します。

2. **(config)# loop-detection hold-time 60**
   最後の L2 ループ検知フレームを受信してから，L2 ループ検知回数を 60 秒間保持するように設定します。再度 L2 ループ検知フレームを受信しないで 60 秒を超えると，L2 ループ検知回数をクリアします。

(4) ポート閉塞からの自動復旧時間の設定

[設定のポイント]

L2 ループ検知機能によって閉塞したポートを，自動的に active にする時間を設定します。

[コマンドによる設定]

1. **(config)# loop-detection auto-restore-time 360**
   L2 ループ検知機能によって閉塞したポートを，自動的に active にする時間を 360 秒に設定します。

20.3 オペレーション

20.3.1 運用コマンド一覧

L2 ループ検知の運用コマンド一覧を次の表に示します。

表 20-4 運用コマンド一覧

コマンド名	説明
show loop-detection	L2 ループ検知情報を表示します。
show loop-detection statistics	L2 ループ検知の統計情報を表示します。
clear loop-detection statistics	L2 ループ検知の統計情報をクリアします。
show loop-detection logging	L2 ループ検知受信フレームログ情報を表示します。
clear loop-detection logging	L2 ループ検知受信フレームログ情報をクリアします。

20.3.2 L2 ループ検知状態の確認

運用コマンド show loop-detection で L2 ループ検知の設定と運用状態を確認できます。

L2 ループ検知フレームの送信レートが最大値を超えて，フレームを送信できないポートがないかを確認できます。VLAN Port Counts の Configuration が Capacity を超えていない場合は問題ありません。

ループ障害によって閉塞しているポートは Port Information の Status で確認できます。

図 20-5 運用コマンド show loop-detection の実行結果

```
> show loop-detection

Date 20XX/05/20 10:44:11 UTC
Interval Time           :10
Output Rate             :20pps
Threshold               :1
Hold Time               :60
Auto Restore Time       :300
VLAN Port Counts
    Configuration       :4          Capacity       :200
Port Information
  Port      Status     Type         DetectCnt RestoringTimer  SourcePort   Vlan
  0/1       Down(loop) send-inact           1            206  0/4 (U)         1
  0/2       Up         send                 3              -  0/4 (U)         2
  0/3       Down       exception            0              -  -
  0/4       Up         uplink               -              -  0/2             2
  0/8       Down(loop) send-inact           1            206  ChGr:37         5
    :

>
```

21 CFM

CFM（Connectivity Fault Management）は，レイヤ 2 レベルでのブリッジ間の接続性の検証とルート確認を行う，広域イーサネット網の保守管理機能です。
この章では，CFM の解説と操作方法について説明します。

21.1 解説

21.1.1 概要

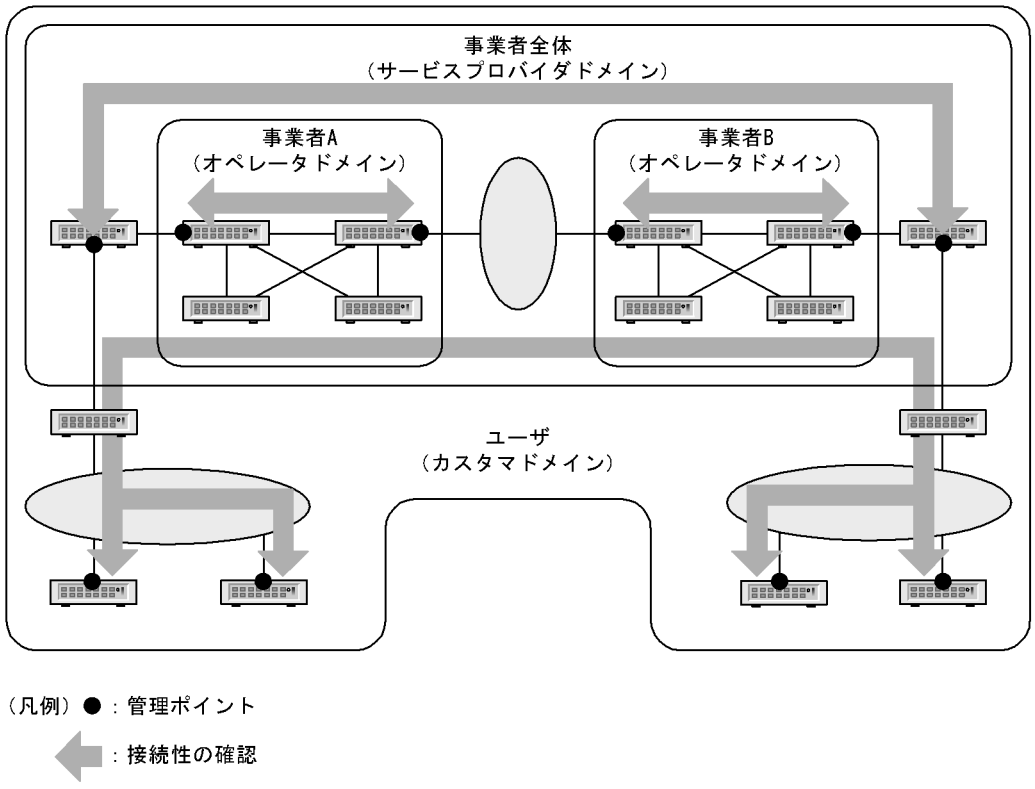
イーサネットは企業内 LAN だけでなく広域網でも使われるようになってきました。これに伴い，イーサネットに SONET や ATM と同等の保守管理機能が求められています。

CFM では，次の三つの機能を使って，レイヤ 2 ネットワークの保守管理を行います。

1. Continuity Check
   管理ポイント間で，情報が正しく相手に届くか（到達性・接続性）を常時監視します。
2. Loopback
   障害を検出したあと，Loopback でルート上のどこまで到達するのかを特定します（ループバック試験）。
3. Linktrace
   障害を検出したあと，Linktrace で管理ポイントまでのルートを確認します（レイヤ 2 ネットワーク内のルート探索）。

CFM の構成例を次の図に示します。

図 21-1 CFM の構成例



（1） CFM の機能

CFM は IEEE802.1ag で規定されていて，次の表に示す機能があります。本装置は，これらの機能をサポートしています。

表 21-1 CFM の機能

名称	説明
Continuity Check（CC）	管理ポイント間の到達性の常時監視
Loopback	ループバック試験 ping 相当の機能をレイヤ 2 で実行します。
Linktrace	ルート探索 traceroute 相当の機能をレイヤ 2 で実行します。

（2） CFM の構成

CFM を構成する要素を次の表に示します。CFM はドメイン，MA，MEP および MIP から構成された保守管理範囲内で動作します。

表 21-2 CFM を構成する要素

名称	説明
ドメイン （Maintenance Domain）	CFM を適用するネットワーク上の管理用のグループのこと。
MA （Maintenance Association）	ドメインを細分化して管理する VLAN のグループのこと。
MEP （Maintenance association End Point）	管理終端ポイントのこと。 ドメインの境界上のポートで，MA 単位に設定します。 また，CFM の各機能を実行するポートです。
MIP （Maintenance domain Intermediate Point）	管理中間ポイントのこと。 ドメインの内部に位置する管理ポイントです。
MP （Maintenance Point）	管理ポイントのことで，MEP と MIP の総称です。

21.1.2 CFM の構成要素

（1） ドメイン

CFM ではドメインという単位でネットワークを階層的に管理し，ドメイン内で CFM PDU を送受信することで保守管理を行います。ドメインには 0 ～ 7 のレベル（ドメインレベル）があり，レベルの値が大きいほうが高いレベルとなります。

高いドメインレベルでは，低いドメインレベルの CFM PDU を廃棄します。低いドメインレベルでは，高いドメインレベルの CFM PDU を処理しないで転送します。従って，低いドメインレベルの CFM PDU が高いドメインレベルのドメインに渡ることはなく，ドメインで独立した保守管理ができます。

ドメインレベルは区分に応じて使用するように，規格で規定されています。区分に割り当てられたドメインレベルを次の表に示します。

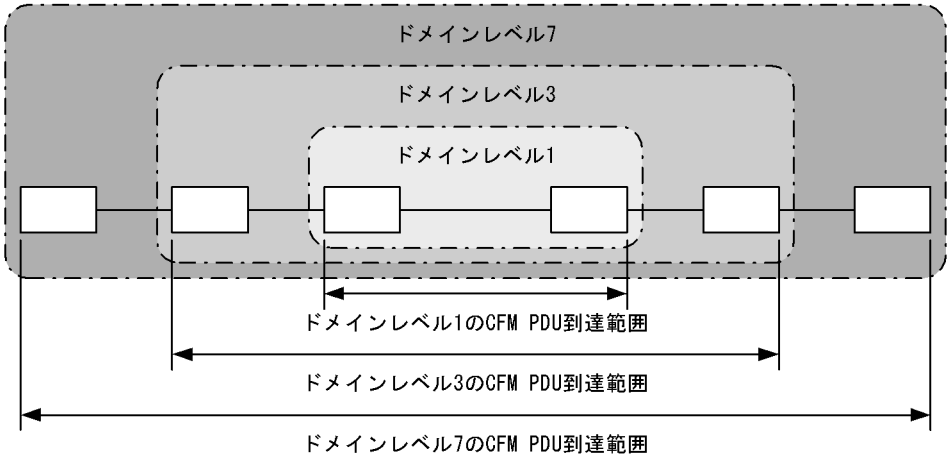
表 21-3 区分に割り当てられたドメインレベル

ドメインレベル	区分
7	カスタマ（ユーザ）
6	
5	

ドメインレベル	区分
4	サービスプロバイダ（事業者全体）
3	
2	オペレータ（事業者）
1	
0	

ドメインは階層的に設定できます。ドメインを階層構造にする場合は低いドメインレベルを内側に，高いドメインレベルを外側に設定します。階層的なドメインの構成例を次の図に示します。

図 21-2　階層的なドメインの構成例



（2） MA

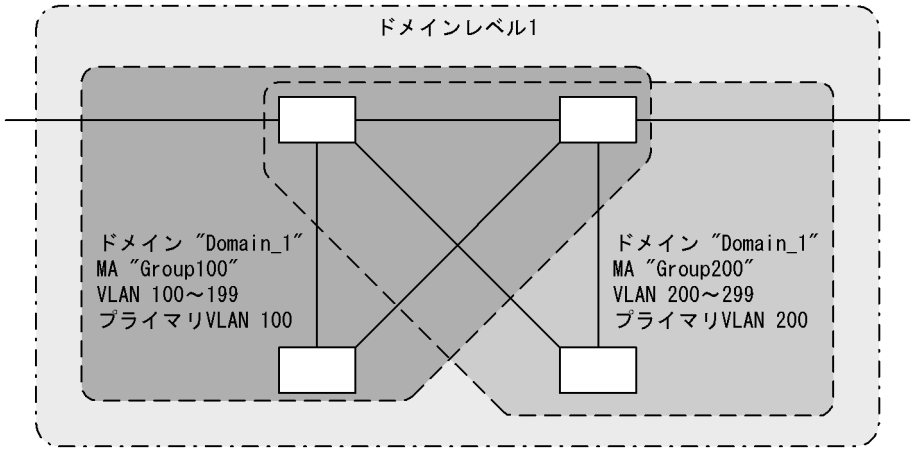
MA はドメイン内を VLAN グループで分割して管理する場合に使います。ドメインには最低一つの MA が必要です。

CFM は MA 内で動作するため，MA を設定することで管理範囲を細かく制御できます。

MA はドメイン名称および MA 名称で識別されます。そのため，同じ MA 内で運用する各装置では，設定時にドメインと MA の名称を合わせておく必要があります。

MA の管理範囲の例を次の図に示します。

図 21-3 MA の管理範囲の例



また，CFM PDU を送受信する VLAN（プライマリ VLAN）を同一 MA 内で合わせておく必要があります。

初期状態では，MA 内で VLAN ID の値がいちばん小さい VLAN がプライマリ VLAN になります。コンフィグレーションコマンド ma vlan-group を使えば，任意の VLAN を明示的にプライマリ VLAN に設定できます。

プライマリ VLAN をデータ転送用の VLAN と同じ VLAN に設定することで，実際の到達性を監視できます。

（3） MEP

MEP はドメインの境界上の管理ポイントで，MA に対して設定します。MEP には MEP ID という MA 内でユニークな ID を設定して各 MEP を識別します。

CFM の機能は MEP で実行されます。CFM は MEP 間（ドメインの境界から境界までの間）で CFM PDU を送受信することで，該当ネットワークの接続性を確認します。

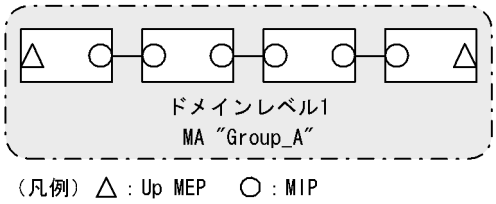
MEP には次の二つの種類があります。

● Up MEP

リレー側に設定する MEP です。Up MEP 自身は CFM PDU を送受信しないで，同一 MA 内の MIP またはポートを介して送受信します。

Up MEP の設定例を次の図に示します。

図 21-4 Up MEP の設定例

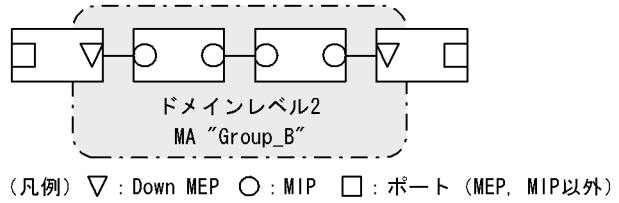


● Down MEP

回線側に設定する MEP です。Down MEP 自身が CFM PDU を送受信します。

Down MEP の設定例を次の図に示します。

図 21-5 Down MEP の設定例



Down MEP，Up MEP からの送信例，および Down MEP，Up MEP での受信例を次の図に示します。

図 21-6 Down MEP，Up MEP からの送信

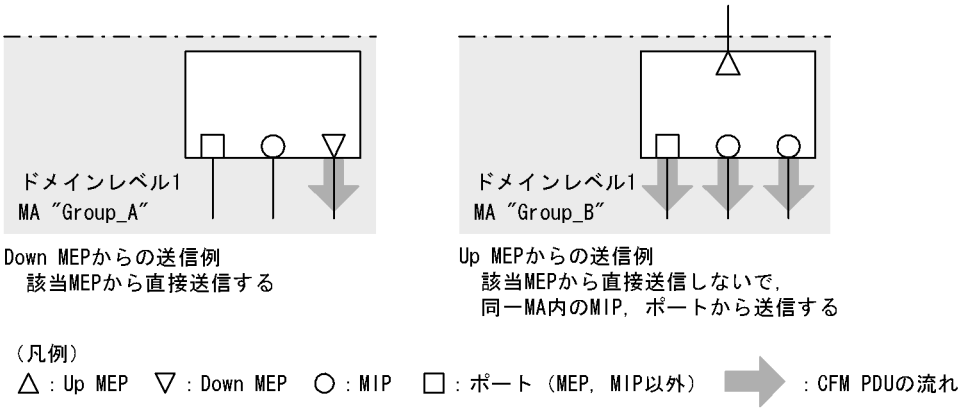
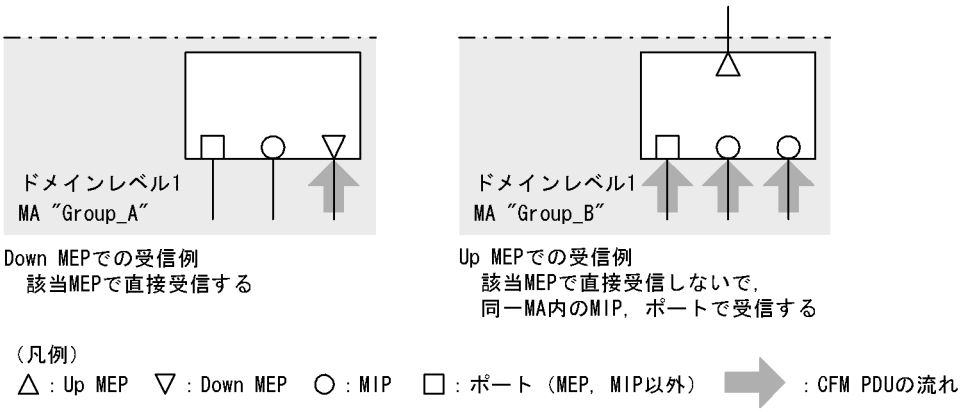
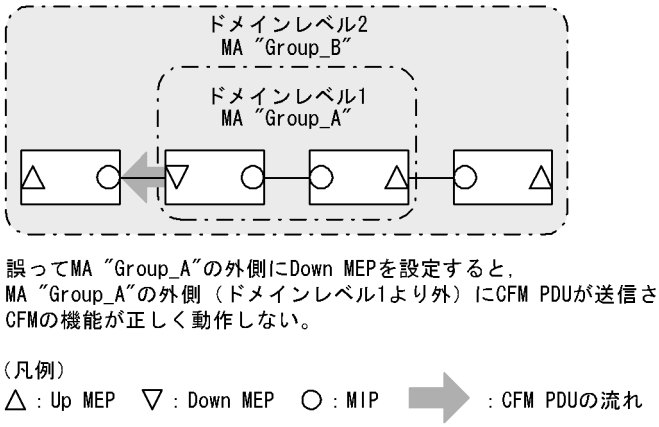


図 21-7 Down MEP，Up MEP での受信



Down MEP および Up MEP は正しい位置に設定してください。例えば，Down MEP は回線側（MA の内側）に設定する必要があります。リレー側（MA の外側）に対して設定した場合，CFM PDU が MA の外側に送信されるため，CFM の機能が正しく動作しません。誤って Down MEP を設定した例を次の図に示します。

図 21-8　誤って Down MEP を設定した例



（4） MIP

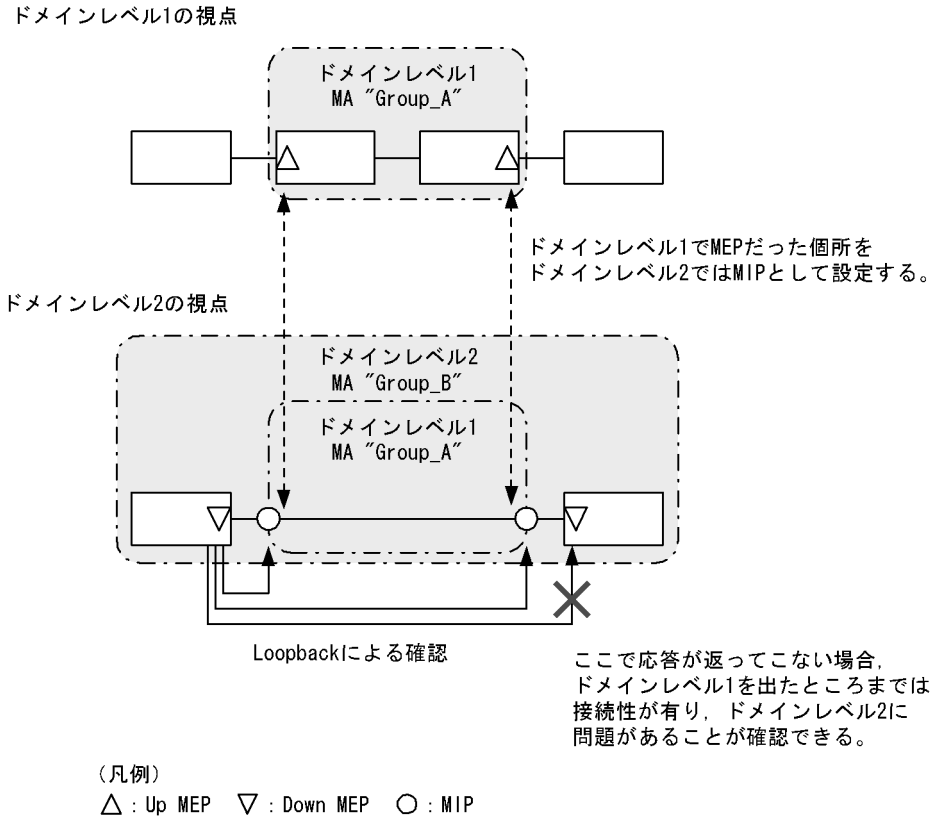
MIP はドメインの内部に設定する管理ポイントで，ドメインに対して設定します（同一ドメイン内の全 MA で共通）。階層構造の場合，MIP は高いドメインレベルのドメインが低いドメインレベルのドメインと重なる個所に設定します。また，MIP は Loopback および Linktrace に応答するので，ドメイン内の保守管理したい個所に設定します。

(a) ドメインが重なる個所に設定する場合

ドメインが重なる個所に MIP を設定すると，上位ドメインでは，低いドメインを認識しながらも，低いドメインの構成を意識しない状態で管理できます。

ドメインレベル 1 とドメインレベル 2 を使った階層構造の例を次の図に示します。

図 21-9　ドメインレベル 1 とドメインレベル 2 の階層構造の例



ドメインレベル 2 を設計する際，ドメインレベル 1 の MA で MEP に設定しているポートをドメインレベル 2 の MIP として設定します。これによって，ドメインレベル 2 ではドメインレベル 1 の範囲を認識しながらも，運用上は意識しない状態で管理できます。

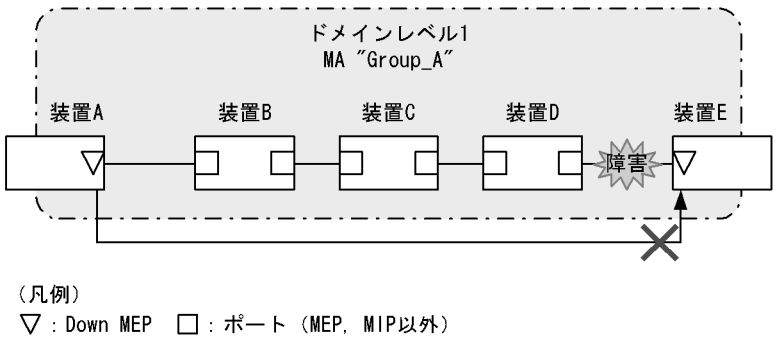
障害発生時は，ドメインレベル 2 の問題か，ドメインレベル 1 のどこかの問題かを切り分けられるため，調査範囲を特定できます。

(b) 保守管理したい個所に設定する場合

ドメイン内で細かく MIP を設定すれば，より細かな保守管理ができるようになります。

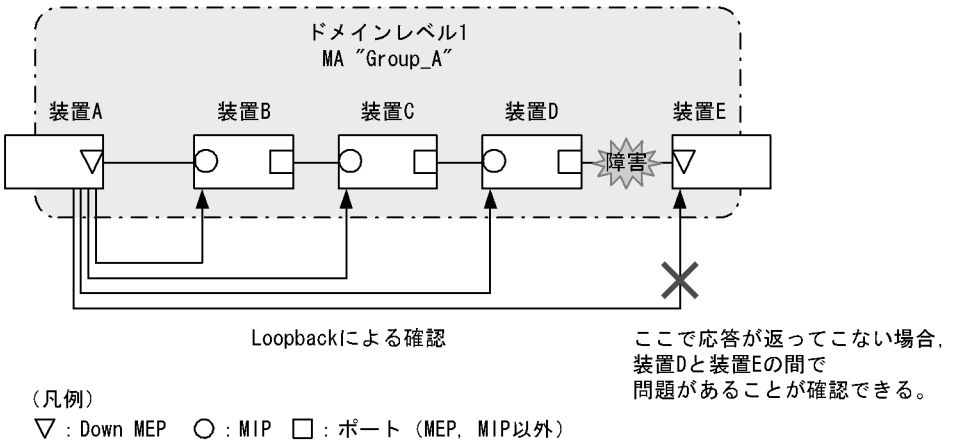
ドメイン内に MIP が設定されていない構成の例を次の図に示します。この例では，ネットワークに障害が発生した場合，装置 A，装置 E の MEP 間で通信できないことは確認できますが，どこで障害が発生したのか特定できません。

図 21-10　ドメイン内に MIP が設定されていない構成の例



ドメイン内に MIP を設定した構成の例を次の図に示します。この例では，ドメイン内に MIP を設定することで，Loopback や Linktrace の応答が各装置から返ってくるため，障害発生個所を特定できるようになります。

図 21-11　ドメイン内に MIP を設定した構成の例



21.1.3　ドメインの設計

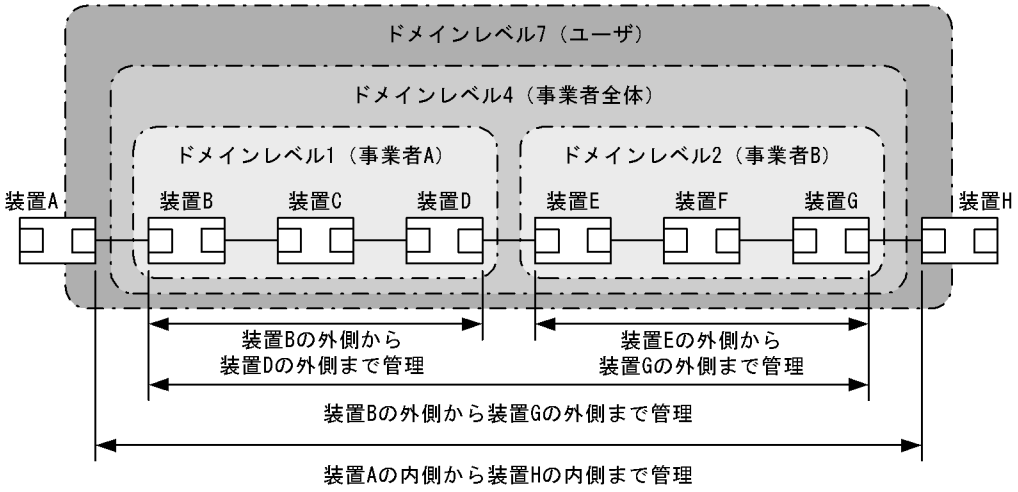
CFM を使用する際には，まずドメインを設計します。ドメインの構成と階層構造を設計し，次に個々のドメインの詳細設計をします。

ドメインの設計には，ドメインレベル，MA，MEP および MIP の設定が必要です。

（1） ドメインの構成と階層構造の設計

ドメインの境界となる MA のポートを MEP に設定し，低いドメインと重なるポートを MIP に設定します。次に示す図の構成例を基に，ドメインの構成および階層構造の設計手順を示します。

図 21-12 構成例



（凡例）□：ポート

事業者 A，事業者 B，事業者全体，ユーザという単位でドメインを設計し，区分に応じたドメインレベルを設定します。また，次の項目を想定しています。

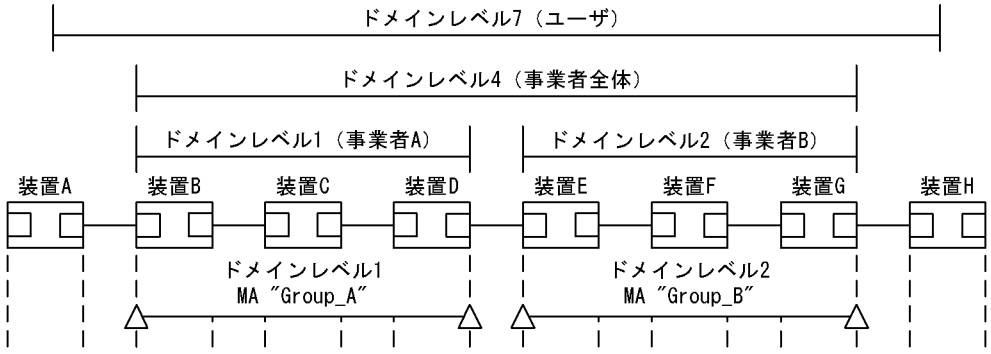
- 事業者 A，事業者 B，事業者全体は，ユーザに提供する回線が利用できることを保証するために，ユーザに提供するポートを含めた接続性を管理
- ユーザは，事業者の提供する回線が使用できるかどうかを監視するために，事業者から提供される回線の接続性を管理

ドメインの設計は，次に示すように低いレベルから順に設定します。

- **ドメインレベル 1，2 の設定**

1. ドメインレベル 1 で MA“Group_A” を設定します。
   この例では，一つのドメインを一つの MA で管理していますが，ドメイン内を VLAN グループ単位に分けて詳細に管理したい場合は，管理する単位で MA を設定します。
2. ドメインの境界に当たる装置 B，D で，MA のポートに MEP を設定します。
   事業者はユーザに提供するポートを含めた接続性を管理するため，Up MEP を設定します。
3. ドメインレベル 2 も同様に，MA を設定し，装置 E，G に Up MEP を設定します。

図 21-13 ドメインレベル 1，2 の設定

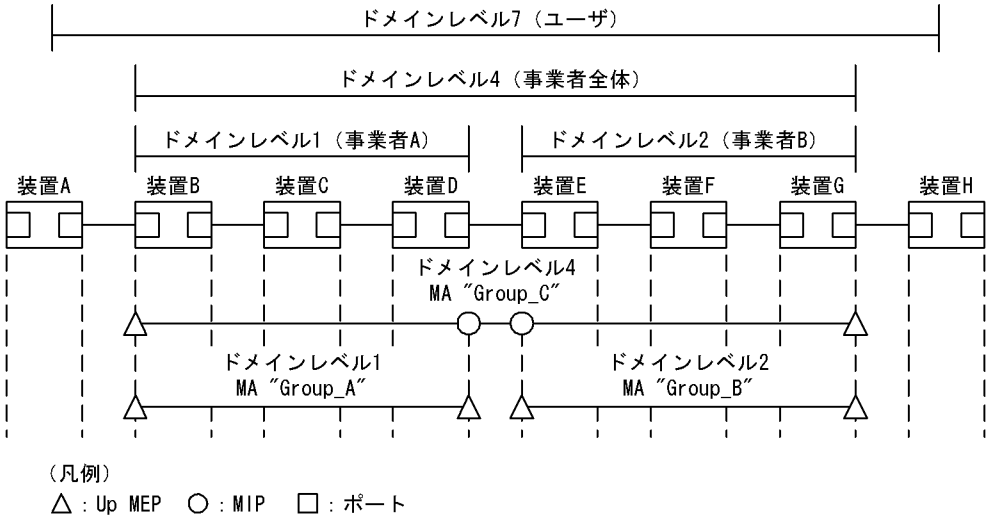


（凡例）
△：Up MEP　□：ポート

- ドメインレベル 4 の設定

1. ドメインレベル 4 で MA“Group_C” を設定します。
2. ドメインレベル 4 の境界に当たる装置 B，G で，MA のポートに MEP を設定します。
   事業者はユーザに提供するポートを含めた接続性を管理するため，Up MEP を設定します。
3. ドメインレベル 4 はドメインレベル 1 と 2 を包含しているため，それぞれの中継点である装置 D，E に MIP を設定します。
   低いドメインの MEP を高いドメインで MIP に設定すると，Loopback や Linktrace を使って自分で管理するドメインでの問題か，低いレベルで管理するドメインでの問題かを切り分けられるため，調査範囲を特定しやすくなります。

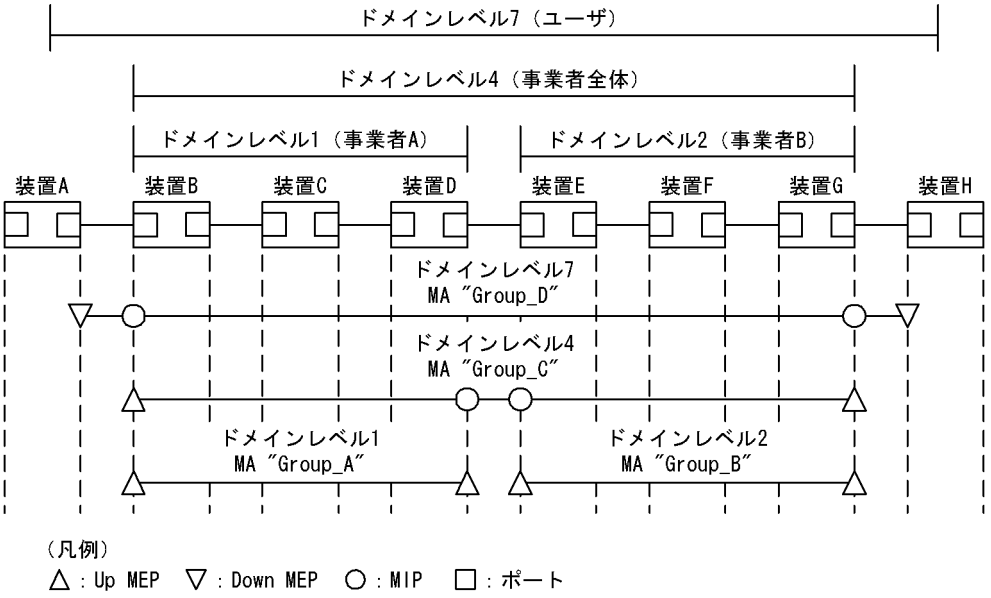
図 21-14　ドメインレベル 4 の設定



- ドメインレベル 7 の設定

1. ドメインレベル 7 で MA“Group_D” を設定します。
2. ドメインレベル 7 の境界に当たる A，H で，MA のポートに MEP を設定します。
   ユーザは事業者から提供される回線の接続性を管理するため，Down MEP を設定します。
3. ドメインレベル 7 はドメインレベル 4 を包含しているため，中継点である装置 B，G に MIP を設定します。
   ドメインレベル 1 と 2 は，ドメインレベル 4 の中継点として設定しているため，ドメインレベル 7 では設定する必要はありません。

図 21-15 ドメインレベル 7 の設定



（2） 個々のドメインの詳細設計

個々の詳細設計では，Loopback，Linktrace を適用したい個所に MIP を設定します。

MIP 設定前の構成および MIP 設定後の構成の例を次の図に示します。

図 21-16 MIP 設定前の構成例

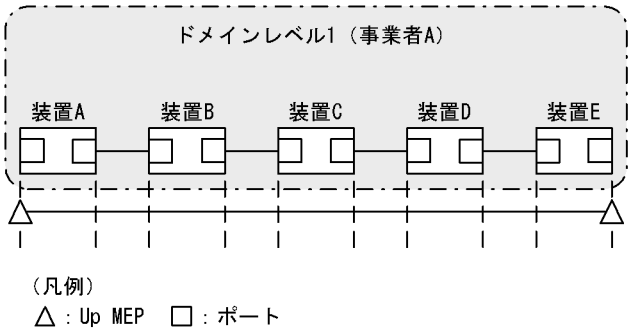
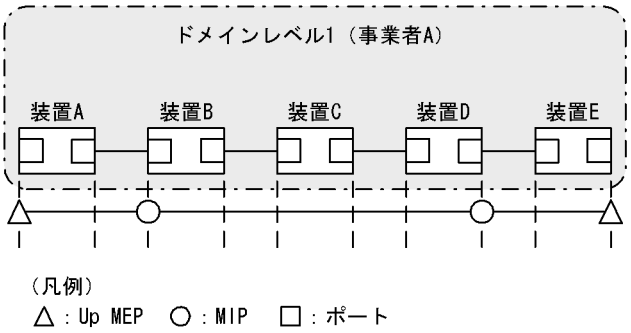


図 21-17 MIP 設定後の構成例



ドメインの内側で Loopback，Linktrace の宛先にしたいポートを MIP に設定します。この例では，装置

B，D に MIP を設定しています。この設定によって装置 B，D の MIP に対し，Loopback，Linktrace を実行できます。また，Linktrace のルート情報として応答を返すようになります。

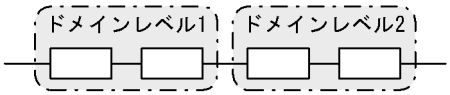
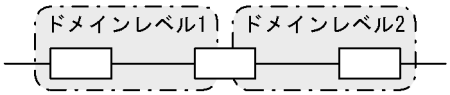
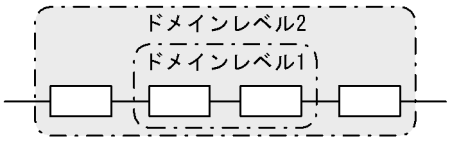
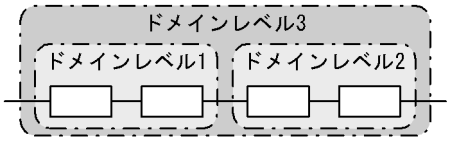
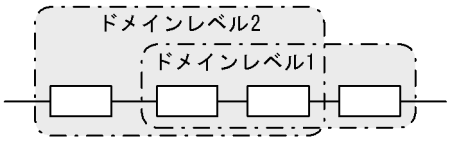
MIP を設定していない装置 C は Loopback，Linktrace の宛先として指定できません。また，Linktrace に応答しないためルート情報に装置 C の情報は含まれません。

（3） ドメインの構成例

ドメインは階層的に設定できますが，階層構造の内側が低いレベル，外側が高いレベルとなるように設定する必要があります。

ドメインの構成例と構成の可否を次の表に示します。

表 21-4　ドメインの構成例と構成の可否

構成状態	構成例	構成の可否
ドメインの隣接		可
ドメインの接触		可
ドメインのネスト		可
ドメインの隣接とネストの組み合わせ		可
ドメインの交差		不可

21.1.4　Continuity Check

Continuity Check（CC）は MEP 間の接続性を常時監視する機能です。MA 内の全 MEP が CCM（Continuity Check Message。CFM PDU の一種）を送受信し合い，MA 内の MEP を学習します。MEP の学習内容は Loopback，Linktrace でも使用します。

CC を動作させている装置で CCM を受信しなくなったり，該当装置の MA 内のポートが通信できない状態になったりした場合に，障害が発生したと見なします。この際，障害検出フラグを立てた CCM を送信し，MA 内の MEP に通知します。

CC で検出する障害を次の表に示します。検出する障害には障害レベルがあります。本装置では検出する障害レベルをコンフィグレーションで変更できます。初期値は障害レベル 2 以上を検出します。

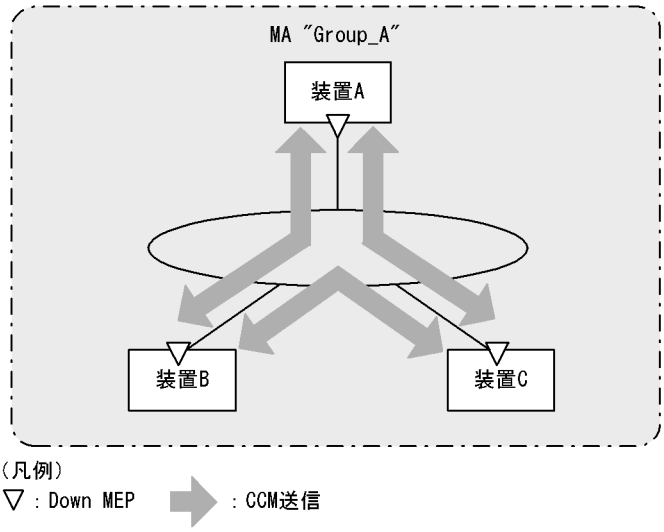
表 21-5　CC で検出する障害レベルと障害内容

障害レベル	障害内容	初期状態
5	ドメイン，MA が異なる CCM を受信した。	検出する
4	MEP ID または送信間隔が誤っている CCM を受信した。	
3	CCM を受信しなくなった。	
2	該当装置のポートが通信できない状態になった。	
1	障害検出通知の CCM を受信した。 Remote Defect Indication	検出しない
0	障害を検出しない。	

次の図の装置 B に着目して CC の動作例を示します。

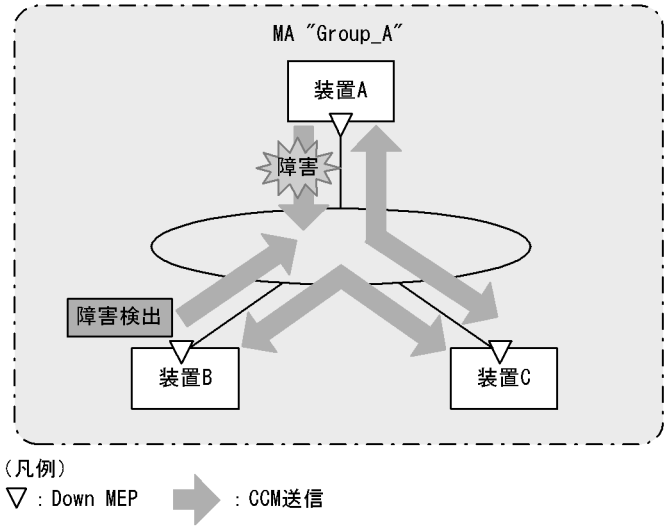
各 MEP はマルチキャストで MA 内に CCM を 1 分間隔で定期的に送信します。各 MEP の CCM を定期的に受信することで常時接続性を監視します。なお，本装置ではコンフィグレーションにより CCM の送信間隔を変更できます。

図 21-18　CC での常時接続性の監視



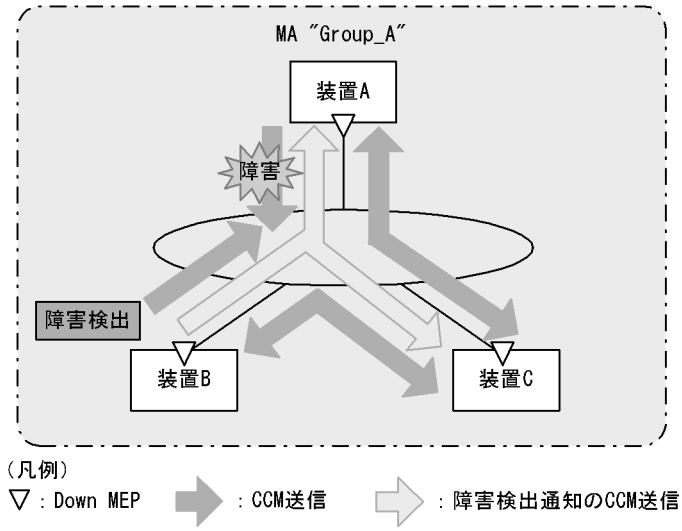
装置 A の CCM が装置の故障またはネットワーク上の障害によって，装置 B に届かなくなると，装置 B は装置 A とのネットワーク上の障害として検出します。

図 21-19　CC で障害を検出



障害を検出した装置 B は，MA 内の全 MEP に対して，障害を検出したことを通知します。

図 21-20　障害を全 MEP に通知



障害検出通知の CCM を受信した各 MEP は，MA 内のどこかで障害が発生したことを認識します。各装置で Loopback，Linktrace を実行することによって，MA 内のどのルートで障害が発生したのかを確認できます。

（1） 障害の検出とトラップ通知について

CC で障害を検出したときはトラップを通知しますが，コンフィグレーションにより障害を検出したときに一定時間はトラップ通知を抑止することができます。コンフィグレーションにより設定できる時間種別を次の表に示します。

表 21-6　CC 障害検出時のトラップ通知時間

時間種別	内容	設定範囲
障害検出開始時間 （障害検出後のトラップ通知時間）	障害検出からトラップ通知するまでの時間。 障害検出後，コンフィグレーションで設定した時間を経過してからトラップを通知します。	2500ms ～ 10000ms
障害再検出時間 （連続トラップ通知抑止時間）	連続した障害検出を再検出とみなす時間。 障害検出後，コンフィグレーションで設定した時間内に障害を検出しても再検知とみなし，トラップを通知しません。 （ただし，再検出時間中に現在よりも高いレベルの障害を検出したときは，トラップを通知します。）	2500ms ～ 10000ms

21.1.5　Loopback

Loopback はレイヤ 2 レベルで動作する，ping 相当の機能です。同一 MA 内の MEP-MEP 間または MEP-MIP 間の接続性を確認します。

CC が MEP-MEP 間の接続性の確認であるのに対し，Loopback では MEP-MIP 間の確認もできるため，MA 内の接続性を詳細に確認できます。

MEP から宛先へループバックメッセージ（CFM PDU の一種）を送信し，宛先から応答が返ってくることを確認することで接続性を確認します。

Loopback には MIP または MEP が直接応答するため，例えば，装置内に複数の MIP を設定した場合，MIP ごとに接続性を確認できます。

MIP および MEP に対する Loopback の実行例を次の図に示します。

図 21-21　MIP に対して Loopback を実行

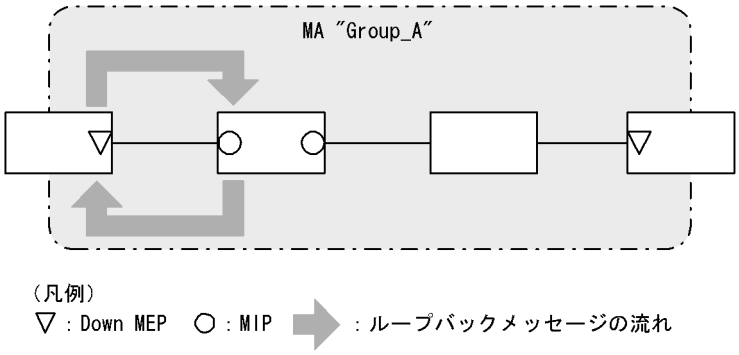
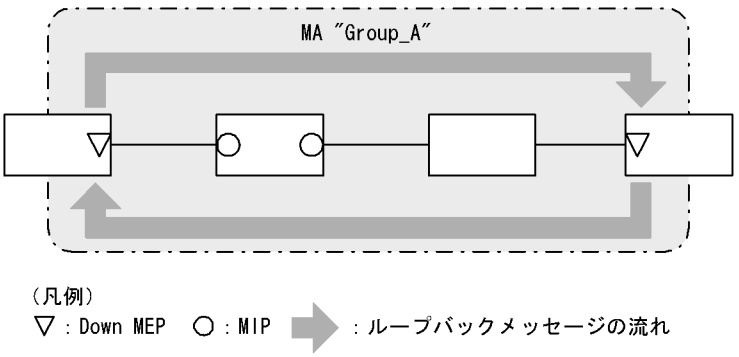


図 21-22　MEP に対して Loopback を実行



Loopback は CC の学習内容を使用するため，事前に CC を動作させておく必要があります。また，宛先に MIP を指定する場合は，事前に MIP のポートの MAC アドレスを調べておく必要があります。

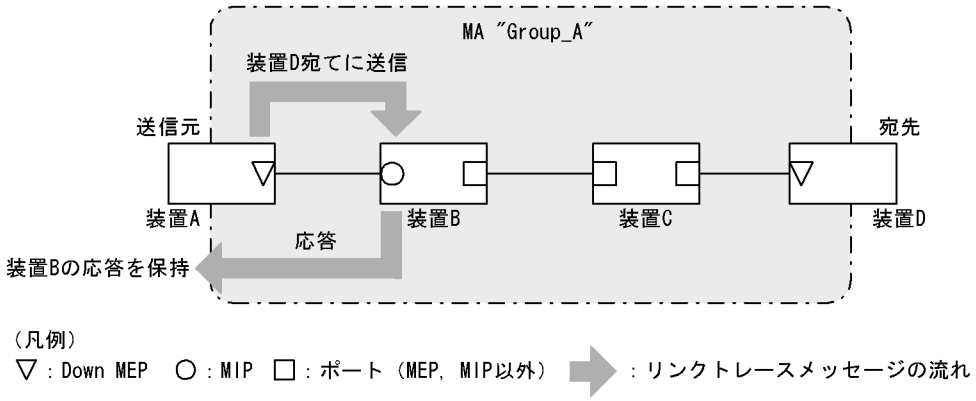
21.1.6 Linktrace

Linktrace はレイヤ 2 レベルで動作する traceroute 相当の機能です。同一 MA 内の MEP-MEP 間または MEP-MIP 間を経由する装置の情報を収集し，ルート情報を出力します。

リンクトレースメッセージ（CFM PDU の一種）を送信し，返ってきた応答をルート情報として収集します。

宛先にリンクトレースメッセージを送信した例を次の図に示します。

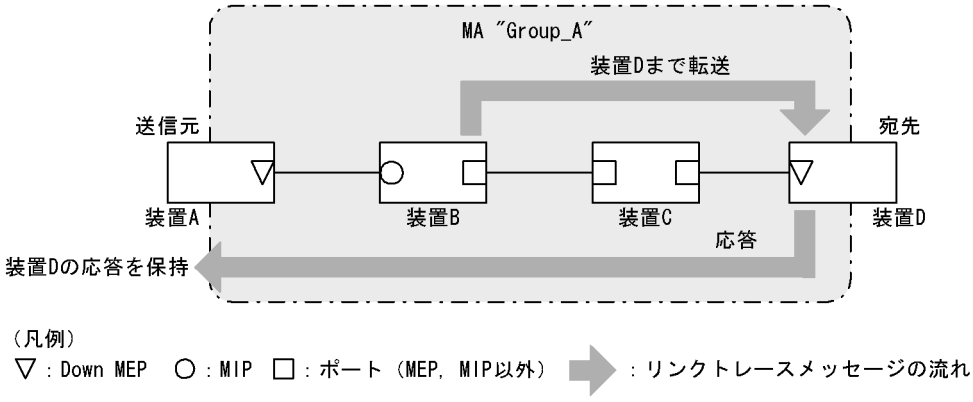
図 21-23　宛先にリンクトレースメッセージを送信



リンクトレースメッセージは宛先まで MIP を介して転送されます。MIP は転送する際に，自装置のどのポートで受信し，どのポートで転送したのかを応答します。送信元装置はルート情報として応答メッセージを保持します。

宛先にリンクトレースメッセージを転送した例を次の図に示します。

図 21-24　宛先にリンクトレースメッセージを転送



応答を返した MIP は宛先までリンクトレースメッセージを転送します。装置 C のように，MEP または MIP が設定されていない装置は応答を返しません（応答を返すには一つ以上の MIP が設定されている必要があります）。

宛先の MEP または MIP までリンクトレースメッセージが到達すると，宛先の MEP または MIP は到達

したことと，どのポートで受信したのかを送信元に応答します。

送信元では，保持した応答をルート情報として出力し，宛先までのルートを確認します。

Linktrace は装置単位に応答します。例えば，装置内に設定された MIP が一つでも複数でも，どちらの場合も同じように，受信ポートと転送ポートの情報を応答します。

Linktrace は CC の学習内容を使用するため，事前に CC を動作させておく必要があります。また，宛先に MIP を指定する場合は，事前に MIP のポートの MAC アドレスを調べておく必要があります。

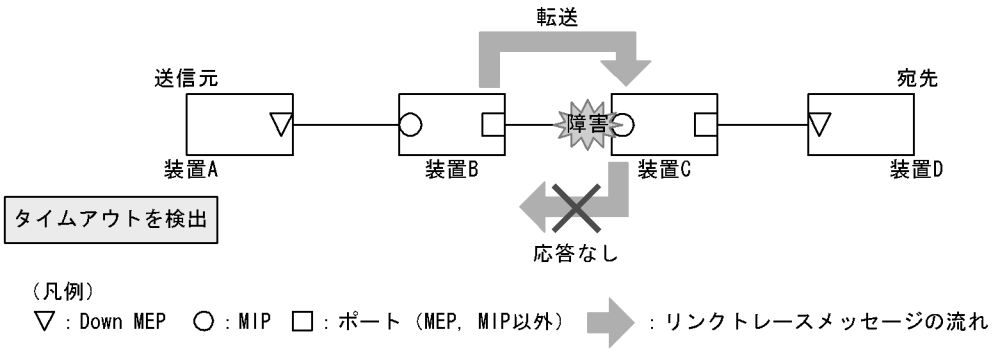
(a) Linktrace による障害の切り分け

Linktrace の実行結果によって，障害が発生した装置やポートなどを絞り込めます。

- **タイムアウトを検出した場合**

Linktrace でタイムアウトを検出した例を次の図に示します。

図 21-25 Linktrace でタイムアウトを検出した例

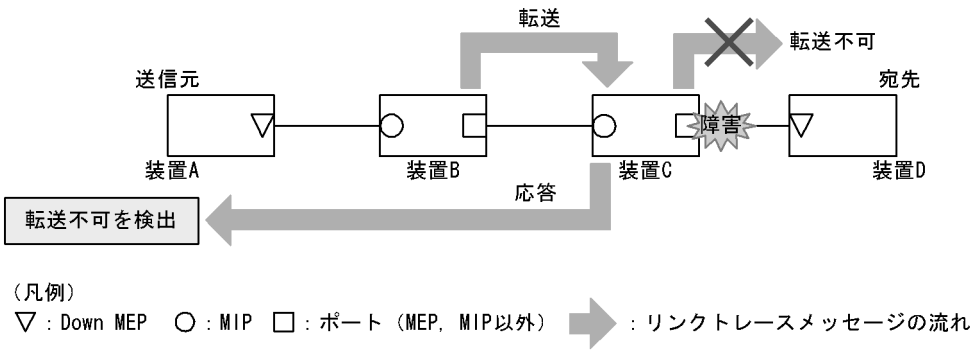


この例では，装置 A が Linktrace でタイムアウトを検出した場合，ネットワーク上の受信側のポートが通信できない状態が考えられます。リンクトレースメッセージが装置 B から装置 C に転送されていますが，装置 C が通信できない状態になっていて，応答を返さないため，タイムアウトになります。

- **転送不可を検出した場合**

Linktrace で通信不可を検出した例を次の図に示します。

図 21-26 Linktrace で通信不可を検出した例



装置 A が Linktrace での転送不可を検出した場合，ネットワーク上の送信側のポートが通信できない状態が考えられます。これは，装置 C が装置 D（宛先）にリンクトレースメッセージを転送できなかった場合，装置 A に送信側ポートが通信できない旨の応答を返すためです。

（b） Linktrace の応答について

リンクトレースメッセージはマルチキャストフレームです。

CFM が動作している装置でリンクトレースメッセージを転送する際には，MIP CCM データベースと MAC アドレステーブルを参照して，どのポートで転送するか決定します。

CFM が動作していない装置ではリンクトレースメッセージをフラッディングします。このため，CFM が動作していない装置がネットワーク上にある場合，宛先のルート以外の装置からも応答が返ります。

21.1.7 共通動作仕様

（1） ブロック状態のポートでの動作

CFM の各機能について，ブロック状態のポートでの動作を次の表に示します。

表 21-7 Up MEP がブロック状態の場合

機能	動作
CC	• CCM を送受信する。送信する CCM のポート状態には Blocked を設定する
Loopback	• 運用コマンド l2ping を実行できる • 自宛のループバックメッセージに応答する
Linktrace	• 運用コマンド l2traceroute を実行できる • リンクトレースメッセージに応答する。応答するリンクトレースメッセージの Egress Port の状態には Blocked を設定する

表 21-8 Down MEP がブロック状態の場合

機能	動作
CC	• CCM を送受信しない
Loopback	• 運用コマンド l2ping は実行できない • 自宛のループバックメッセージに応答しない
Linktrace	• 運用コマンド l2traceroute は実行できない • リンクトレースメッセージに応答しない

表 21-9 MIP がブロック状態の場合

機能	動作
CC	• CCM を透過しない
Loopback	• 回線側から受信した自宛のループバックメッセージに応答しない • リレー側から受信した自宛のループバックメッセージに応答する • ループバックメッセージを透過しない
Linktrace	• 回線側から受信したリンクトレースメッセージに応答しない • リレー側から受信したリンクトレースメッセージに応答する。応答するリンクトレースメッセージの Egress Port の状態には Blocked を設定する • リンクトレースメッセージを透過しない

表 21-10 MEP，MIP 以外のポートがブロック状態の場合

機能	動作
CC	• CCM を透過しない
Loopback	• ループバックメッセージを透過しない

機能	動作
Linktrace	• リンクトレースメッセージを透過しない

（2） VLAN トンネル構成での設定について

VLAN トンネリング網で CFM を使用する場合，VLAN トンネリング網内と VLAN トンネリング網外でドメインを分け，それぞれで管理します。なお，ドメインの設定個所によっては，CFM の機能の使用に一部制限があります。ドメインの設定個所別の機能の使用制限について次の表に示します。

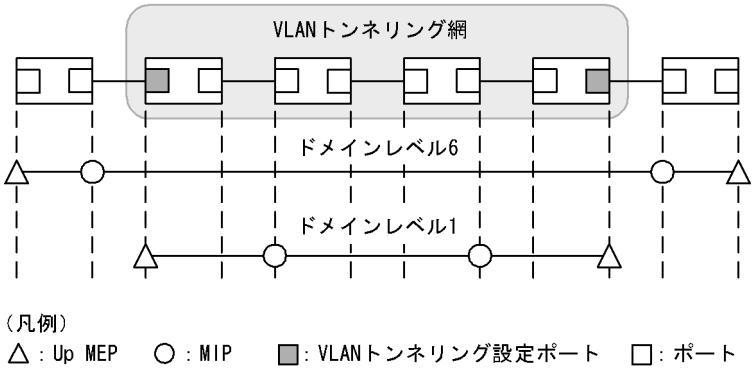
表 21-11　ドメインの設定個所別の機能の使用制限

ドメインの設定個所	機能		
	CC	Loopback	Linktrace
VLAN トンネリング網内と VLAN トンネリング網外	使用可	使用可	使用可
VLAN トンネリング網内だけ	使用可	使用可	使用可
VLAN トンネリング網外だけ	使用可	使用可	使用可

（a） VLAN トンネリング網内と VLAN トンネリング網外で CFM を使用する場合

VLAN トンネリング網内と VLAN トンネリング網外で CFM を使用する例を次の図に示します。

図 21-27　VLAN トンネリング網内と VLAN トンネリング網外で CFM を使用する例

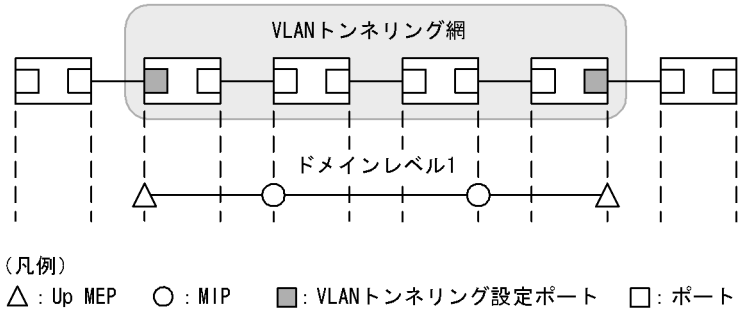


VLAN トンネリング網内のドメインレベル 1 は，VLAN トンネリング網内で任意の個所に管理ポイントを設定できます。VLAN トンネリング網外のドメインレベル 6 は，VLAN トンネリング網外の装置だけに管理ポイントを設定できます。VLAN トンネリング網内にはドメインレベル 6 の管理ポイントは設定できません。該当ドメインでは CFM の各機能が使用できます。

（b） VLAN トンネリング網内だけで CFM を使用する場合

VLAN トンネリング網内だけで CFM を使用する例を次の図に示します。

図 21-28　VLAN トンネリング網内だけで CFM を使用する例

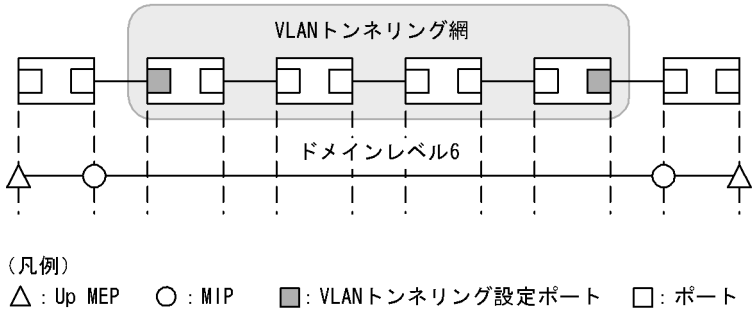


VLAN トンネリング網内のドメインレベル 1 は，VLAN トンネリング網内で任意の個所に管理ポイントを設定できます。該当ドメインでは CFM の各機能が使用できます。

（c） VLAN トンネリング網外だけで CFM を使用する場合

VLAN トンネリング網外だけで CFM を使用する例を次の図に示します。

図 21-29　VLAN トンネリング網外だけで CFM を使用する例



VLAN トンネリング網外のドメインレベル 6 は，VLAN トンネリング網外の装置だけに管理ポイントを設定できます。VLAN トンネリング網内にはドメインレベル 6 の管理ポイントは設定できません。該当ドメインでは CFM の各機能が使用できます。

21.1.8　CFM で使用するデータベース

CFM で使用するデータベースを次の表に示します。

表 21-12　CFM で使用するデータベース

データベース	内容	内容確認コマンド
MEP CCM データベース	各 MEP が保持しているデータベース。 同一 MA 内の MEP の情報。 CC で常時接続性の監視をする際に使用。 保持する内容は次のとおりです。 • MEP ID • MEP ID に対応する MAC アドレス • 該当 MEP で発生した障害情報	show cfm remote-mep

データベース	内容	内容確認コマンド
MIP CCM データベース	装置で保持しているデータベース。 同一ドメイン内の MEP の情報。 リンクトレースメッセージを転送する際，どのポートで転送するかを決定する際に使用。 保持する内容は次のとおりです。 • MEP の MAC アドレス • 該当 MEP の CCM を受信した VLAN とポート	無
リンクトレースデータベース	Linktrace の実行結果を保持しているデータベース。 保持する内容は次のとおりです。 • Linktrace を実行した MEP と宛先 • TTL • 応答を返した装置の情報 • リンクトレースメッセージを受信したポートの情報 • リンクトレースメッセージを転送したポートの情報	show cfm l2traceroute-db

(1) MEP CCM データベース

MEP CCM データベースは，同一 MA 内にどのような MEP があるかを保持しています。また，該当する MEP で発生した障害情報も保持しています。

Loopback，Linktrace では宛先を MEP ID で指定できますが，MEP CCM データベースに登録されていない MEP ID は指定できません。MEP ID がデータベース内に登録されているかどうかは運用コマンド show cfm remote-mep で確認できます。

本データベースのエントリは CC 実行時に MEP が CCM を受信したときに作成します。

(2) MIP CCM データベース

MIP CCM データベースは，リンクトレースメッセージを転送する際にどのポートから転送すればよいかを決定する際に使用します。

転送時，MIP CCM データベースに宛先 MEP の MAC アドレスが登録されていない場合は，MAC アドレステーブルを参照して転送するポートを決定します。

MAC アドレステーブルにもない場合はリンクトレースメッセージは転送しないで，転送できなかった旨の応答を転送元に返します。

本データベースのエントリは CC 実行時に MIP が CCM を転送したときに作成します。

(3) リンクトレースデータベース

リンクトレースデータベースは，Linktrace の実行結果を保持しています。

運用コマンド show cfm l2traceroute-db で，過去に実行した Linktrace の結果を参照できます。

(a) 保持できるルート数について

1 ルート当たり最大で 256 装置分の応答を保持します。装置全体では 1024 装置分の応答を保持します。

1 ルート当たり何装置分の応答を保持するかで何ルート分保持できるかが決ります。1 ルート当たり 256 装置分の応答を保持した場合は 4 ルート，1 ルート当たり 16 装置分の応答を保持している場合は 64 ルート保持できます。

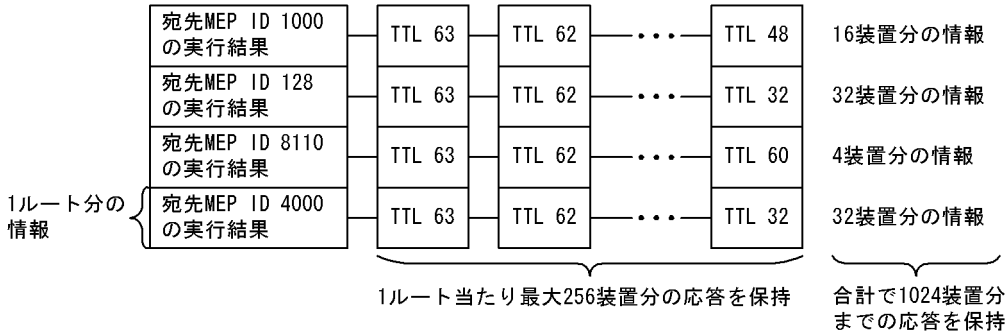
応答が 1024 装置分を超えた場合，古いルートの情報が消去され，新しいルートの情報を保持します。

リンクトレースデータベースに登録されている宛先に対して Linktrace を実行した場合，リンクトレース

データベース上から該当宛先までのルート情報を削除したあとに新しい Linktrace の応答を保持します。

リンクトレースデータベースを次の図に示します。

図 21-30　リンクトレースデータベース



本データベースのエントリは Linktrace 実行時に MEP が応答を受信したときに作成します。

21.1.9　CFM 使用時の注意事項

（1） CFM を動作させない装置について

CFM を適用する際，ドメイン内の全装置で CFM を動作させる必要はありませんが，CFM を動作させない装置では CFM PDU を透過させる必要があります。

本装置を除き，CFM を動作させない装置は，次の表に示すフレームを透過するように設定してください。

表 21-13　透過させるフレーム

フレーム種別	宛先 MAC アドレス
マルチキャスト	0180.c200.0030 ～ 0180.c200.003f

本装置は，CFM が動作していない場合はすべての CFM PDU を透過します。

（2） 他機能との共存について

他機能との共存については，次の表に示す動作となります。

表 21-14　本装置の他機能との動作可否

機能		動作可否	備考
ポートの種類	アクセスポート	○	
	トランクポート	○	
	プロトコルポート	×	CFM フレームは左記ポートへの収容不可（VLAN 内中継できません）。
	MAC ポート	×	CFM フレームは左記ポートへの収容不可（VLAN 内中継できません）。
スタック		×	
VLAN	ポート間中継遮断	×	CFM フレームに対しポート間中継遮断機能は無効です。
リンクアグリゲーション		○	CFM はチャネル単位に動作します。

機能		動作可否	備考
スパニングツリー		○	
GSRP aware		○	
Ring Protocol		○	
IGMP/MLD snooping		○	
DHCP Snooping		○	
	端末フィルタ	×	CFM フレームを受信できません。
	ダイナミック ARP 検査	○	
L2 ループ検知機能		○	
LLDP		×	
UDLD		○	
フィルタ		×	MAC アクセスリスト指定の場合は暗黙の廃棄対象になります。
QoS		×	中継動作に影響しません。 自発フレーム優先度は変更可能です。
IEEE802.1X 認証		×	CFM フレームを受信できない 可能性があるため，認証ポートは CFM の中継経路にしないでください。
Web 認証		×	
MAC 認証		×	
マルチステップ認証		×	
ホワイトリスト機能		×	
アップリンク・リダンダント		○	
ストームコントロール		○	マルチキャスト指定すると，CFM も廃棄対象となります。
ポートミラーリング		×	モニターポート設定は無効です。 また，自発フレーム，ソフトウェア中継フレームはミラーできません。

（凡例）
○：動作可
×：動作不可

（3） CFM PDU のバースト受信について

CC で常時監視するリモート MEP 数が 48 以上あると，リモート MEP からの CFM PDU 送信タイミングが偶然一致した場合に，本装置で CFM PDU をバースト受信することがあります。その場合，本装置で CFM PDU を廃棄することがあり，障害を誤検出するおそれがあります。

本現象が頻発する場合は，各装置での CFM PDU の送信タイミングが重ならないように調整してください。

（4） 同一ドメインで同一プライマリ VLAN を設定している MA での MEP 設定について

同一ドメインで同一プライマリ VLAN を設定している MA（同一 MA も含む）で，同一ポートに対して 2 個以上の MEP を設定しないでください。設定した場合は，該当する MEP で CFM が正常に動作しません。

（5） Linktrace でのルート情報の収集について

Linktrace ではリンクトレースメッセージの転送先ポートは，MIP CCM データベースまたは MAC アドレステーブルを参照して決定します。そのため，リンクアップ時（リンクダウン後の再アップ含む）やスパニングツリーなどによる経路変更後は，CC で CCM を送受信するまで転送先ポートが決定できないため，正しいルート情報の収集ができません。

（6） ブロック状態のポートで MIP が Loopback，Linktrace に応答しない場合について

ブロック状態のポートに MIP を設定し，該当ポートで次に示す運用をした場合，MIP は Loopback，Linktrace に応答しないことがあります。

- スパニングツリー（PVST+，シングル）でループガード機能を運用
- スパニングツリー（MSTP）の運用時に，アクセス VLAN またはネイティブ VLAN をプライマリ VLAN として設定
- Ring Protocol を運用
- アップリンク・リダンダントを運用

（7） 冗長構成での CC の動作について

スパニングツリーなどの冗長構成を組んだネットワーク上で CC を運用している場合，通信経路の切り替えが発生したときに，まれに自装置の MEP が送信した CCM を受信して ErrorCCM を検出することがあります。本障害は通信経路が安定すると回復します。

（8） Tag 変換使用時の CFM の動作について

Tag 変換を設定したポートで，変換後の VLAN の CFM フレームを受信した場合，廃棄せずに動作します。

21.2 コンフィグレーション

21.2.1 コンフィグレーションコマンド一覧

CFM のコンフィグレーションコマンド一覧を次の表に示します。

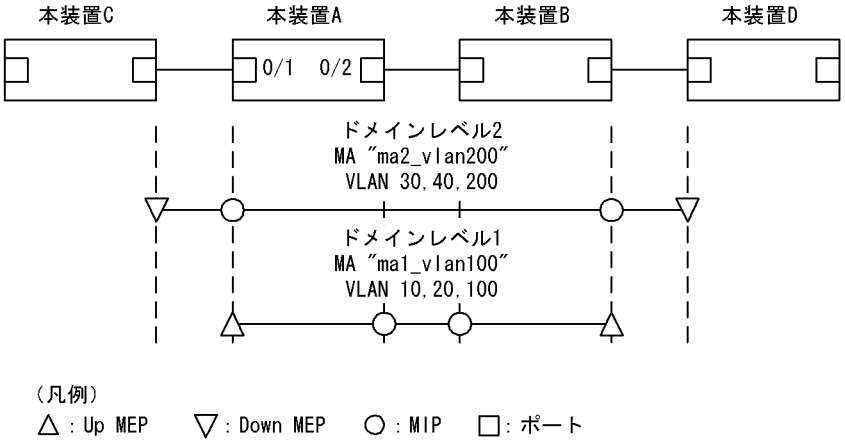
表 21-15 コンフィグレーションコマンド一覧

コマンド名	説明
domain name	該当ドメインで使用する名称を設定します。
ethernet cfm cc alarm-priority	CC で検出する障害レベルを設定します。
ethernet cfm cc alarm-reset-time	CC で連続して障害を検出する場合に，再検出とみなす時間を設定します。
ethernet cfm cc alarm-start-time	CC で障害を検出してからトラップを通知するまでの時間を設定します。
ethernet cfm cc interval	該当 MA の CCM 送信間隔を設定します。
ethernet cfm cc enable	ドメインで CC を使用する MA を設定します。
ethernet cfm domain	ドメインを設定します。
ethernet cfm enable (global)	CFM を開始します。
ethernet cfm enable (interface)	no ethernet cfm enable 設定時に CFM を停止します。
ethernet cfm mep	CFM で使用する MEP を設定します。
ethernet cfm mip	CFM で使用する MIP を設定します。
ma name	該当ドメインで使用する MA の名称を設定します。
ma vlan-group	該当ドメインで使用する MA に所属する VLAN を設定します。

21.2.2 CFM の設定（複数ドメイン）

複数ドメインを設定する手順を説明します。ここでは，次の図に示す本装置 A の設定例を示します。

図 21-31 CFM の設定例（複数ドメイン）



（1）複数ドメインおよびドメインごとの MA の設定

[設定のポイント]

複数のドメインがある場合，低いドメインレベルのドメインから設定します。MA の設定はドメイン

レベルと MA 識別番号，ドメイン名称，および MA 名称を対向装置と一致させる必要があります。設定が異なる場合，本装置と対向装置は同一 MA と判断されません。
MA のプライマリ VLAN には，本装置の MEP から CFM PDU を送信する VLAN を設定します。
primary-vlan パラメータが設定されていない場合は，vlan-group パラメータで設定された VLAN の中から，最も小さな VLAN ID を持つ VLAN がプライマリ VLAN になります。

［コマンドによる設定］

1. **(config)# ethernet cfm domain level 1 direction-up**
   (config-ether-cfm)# domain name str operator_1
   ドメインレベル 1 と MEP の初期状態を Up MEP にすることを設定します。コンフィグレーション イーサネット CFM モードに移行し，ドメイン名称を設定します。

2. **(config-ether-cfm)# ma 1 name str ma1_vlan100**
   (config-ether-cfm)# ma 1 vlan-group 10,20,100 primary-vlan 100
   (config-ether-cfm)# exit
   MA1 で MA 名称，MA に所属する VLAN，プライマリ VLAN を設定します。

3. **(config)# ethernet cfm domain level 2**
   (config-ether-cfm)# domain name str operator_2
   (config-ether-cfm)# ma 2 name str ma2_vlan200
   (config-ether-cfm)# ma 2 vlan-group 30,40,200 primary-vlan 200
   (config-ether-cfm)# exit
   ドメインレベル 2 と MEP の初期状態を Down MEP にすることを設定します。
   MA2 で MA 名称，MA に所属する VLAN，プライマリ VLAN を設定します。

（2） MEP および MIP の設定

［設定のポイント］

MEP および MIP の設定数は，収容条件数以内に収まるように設定してください。
設定した MEP および MIP の運用を開始するには，装置の CFM を有効にする設定が必要になります。

［コマンドによる設定］

1. **(config)# interface gigabitethernet 0/1**
   (config-if)# ethernet cfm mep level 1 ma 1 mep-id 101
   (config-if)# ethernet cfm mip level 2
   (config-if)# exit
   (config)# interface gigabitethernet 0/2
   (config-if)# ethernet cfm mip level 1
   (config-if)# exit
   ポート 0/1 に，ドメインレベル 1，MA1 に所属する MEP を設定します。また，ドメインレベル 2 の MIP を設定します。ポート 0/2 にドメインレベル 1 の MIP を設定します。

2. **(config)# ethernet cfm enable**
   本装置の CFM の運用を開始します。

(3) ポートの CFM の停止

[設定のポイント]

一時的にポートの CFM を停止したい場合に設定します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 0/1**
   (config-if)# no ethernet cfm enable
   (config-if)# exit
   ポート 0/1 の CFM を停止します。

(4) CC の設定

[設定のポイント]

コンフィグレーションコマンド ethernet cfm cc enable の設定直後から，CC が動作します。

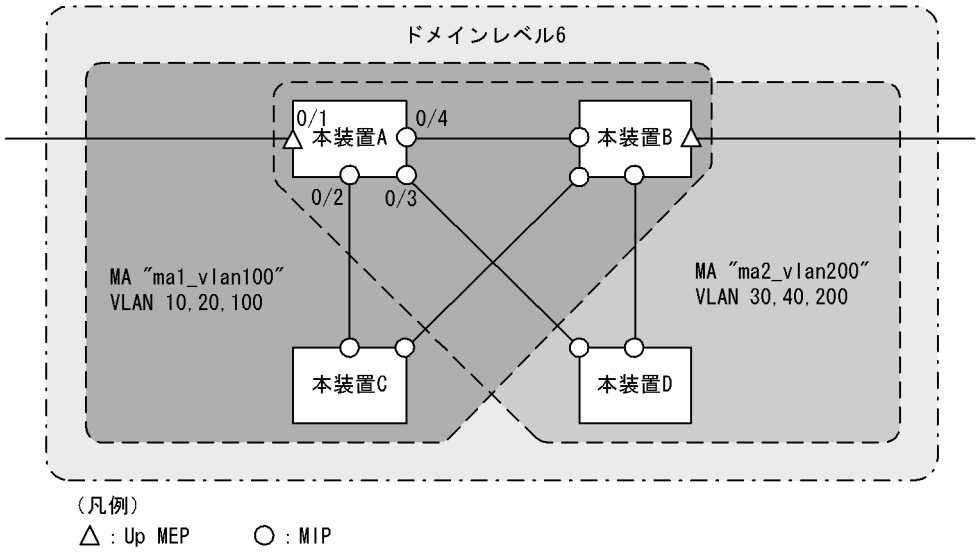
[コマンドによる設定]

1. **(config)# ethernet cfm cc level 1 ma 1 enable**
   ドメインレベル 1，MA1 で，CC の動作を開始します。

21.2.3 CFM の設定（同一ドメイン，複数 MA）

同一ドメインで複数の MA を設定する手順を説明します。ここでは，次の図に示す本装置 A の設定例を示します。

図 21-32 CFM の設定例（同一ドメイン，複数 MA）



(1) 同一ドメインでの複数 MA の設定

[設定のポイント]

同一ドメインで複数の MA を設定する場合は，MA 識別番号および MA 名称が重複しないように設定します。ドメインおよび MA の基本的な設定のポイントは，「21.2.2 CFM の設定（複数ドメイン）」を参照してください。

［コマンドによる設定］

1. **(config)# ethernet cfm domain level 6 direction-up**
   (config-ether-cfm)# domain name str customer_6
   ドメインレベルと MEP の初期状態を Up MEP にすることを設定します。コンフィグレーションイーサネット CFM モードに移行し，ドメイン名称を設定します。

2. **(config-ether-cfm)# ma 1 name str ma1_vlan100**
   (config-ether-cfm)# ma 1 vlan-group 10,20,100 primary-vlan 100
   (config-ether-cfm)# ma 2 name str ma2_vlan200
   (config-ether-cfm)# ma 2 vlan-group 30,40,200 primary-vlan 200
   (config-ether-cfm)# exit
   MA 識別番号と MA 名称，MA に所属する VLAN，プライマリ VLAN を設定します。

（2） MEP および MIP の設定

［設定のポイント］

MEP は MA ごとに設定する必要があります。MIP は複数の MA で共通で，ポート単位に一つ設定します。MEP および MIP の基本的な設定のポイントは，「21.2.2　CFM の設定（複数ドメイン）」を参照してください。

［コマンドによる設定］

1. **(config)# interface gigabitethernet 0/1**
   (config-if)# ethernet cfm mep level 6 ma 1 mep-id 101
   (config-if)# ethernet cfm mep level 6 ma 2 mep-id 201
   (config-if)# exit
   (config)# interface range gigabitethernet 0/2-4
   (config-if-range)# ethernet cfm mip level 6
   (config-if-range)# exit
   ポート 0/1 に，ドメインレベル 6，MA1 に所属する MEP を設定します。また，MA2 に所属する MEP を設定します。ポート 0/2 ～ 0/4 にドメインレベル 6 の MIP を設定します。

2. **(config)# ethernet cfm enable**
   本装置の CFM の運用を開始します。

21.3 オペレーション

21.3.1 運用コマンド一覧

CFM の運用コマンド一覧を次の表に示します。

表 21-16 運用コマンド一覧

コマンド名	説明
l2ping	CFM の Loopback 機能を実行します。指定 MP 間の接続を確認します。
l2traceroute	CFM の Linktrace 機能を実行します。指定 MP 間のルートを確認します。
show cfm	CFM のドメイン情報を表示します。
show cfm remote-mep	CFM のリモート MEP の情報を表示します。
show cfm fault	CFM の障害情報を表示します。
show cfm l2traceroute-db	運用コマンド l2traceroute で取得したルート情報を表示します。
show cfm statistics	CFM の統計情報を表示します。
clear cfm remote-mep	CFM のリモート MEP 情報をクリアします。
clear cfm fault	CFM の障害情報をクリアします。
clear cfm l2traceroute-db	運用コマンド l2traceroute で取得したルート情報をクリアします。
clear cfm statistics	CFM の統計情報をクリアします。

21.3.2 MP 間の接続確認

運用コマンド l2ping で，指定した MP 間の疎通を確認して，結果を表示します。コマンドには確認回数および応答待ち時間を指定できます。指定しない場合，確認回数は 5 回，応答待ち時間は 5 秒です。疎通確認の応答受信または応答待ち時間経過を契機に，次の確認を繰り返します。

図 21-33 l2ping の実行結果

```
> l2ping remote-mep 1010 domain-level 7 ma 1000 mep 1020 count 3
L2ping to MP:1010(0012.e254.dc01) on Level:7  MA:1000  MEP:1020  VLAN:20
Time:20XX/05/28 06:59:50
1: L2ping Reply from 0012.e254.dc01  64bytes  Time=   20 ms
2: L2ping Reply from 0012.e254.dc01  64bytes  Time=   10 ms
3: L2ping Reply from 0012.e254.dc01  64bytes  Time=   10 ms

--- L2ping Statistics ---
  Tx L2ping Request :    3  Rx L2ping Reply :    3  Lost Frame  :   0%
  Round-trip Min/Avg/Max : 10/13/20 ms
>
```

21.3.3 MP 間のルート確認

運用コマンド l2traceroute で，指定した MP 間のルート情報を収集し，結果を表示します。コマンドには応答待ち時間と TTL 値を指定できます。指定しない場合，応答待ち時間は 5 秒，TTL 値は 64 です。

宛先に指定した MP から応答を受信したことを「Hit」で確認できます。

図 21-34　l2traceroute の実行結果

```
> l2traceroute remote-mep 1010 domain-level 7 ma 1000 mep 1020 ttl 64
L2traceroute to MP:1010(0012.e254.dc01) on Level:7  MA:1000  MEP:1020  VLAN:20
Time:20XX/05/28 08:27:44
 63  00ed.f205.0115  Forwarded
 62  0012.e2a8.f8d0  Forwarded
 61  0012.e254.dc01  NotForwarded  Hit
>
```

21.3.4　ルート上の MP の状態確認

運用コマンド show cfm l2traceroute-db detail で，宛先の MP までのルートとルート上の MP の詳細情報を確認できます。「NotForwarded」が表示された場合，Ingress Port および Egress Port の「Action」で，リンクトレースメッセージが中継されなかった理由を確認できます。

図 21-35　show cfm l2traceroute-db detail の実行結果

```
> show cfm l2traceroute-db detail

Date 20XX/05/29 08:45:32 UTC
L2traceroute to MP:302(0012.e254.dc09) on Level:3  MA:300   MEP:300  VLAN:300
Time:20XX/05/29 08:35:02
63   00ed.f205.0111  Forwarded
  Last Egress : 00ed.f205.0001  Next Egress : 00ed.f205.0001
  Relay Action: MacAdrTbl
  Chassis ID    Type: MAC       Info: 00ed.f205.0001
  Ingress Port  Type: LOCAL      Info: Port 0/1
    MP Address: 00ed.f205.0101  Action: OK
  Egress Port   Type: LOCAL      Info: Port 0/7
    MP Address: 00ed.f205.0111  Action: OK
62   0012.e254.dc09  NotForwarded  Hit
  Last Egress : 00ed.f205.0001  Next Egress : 0012.e254.dbf0
  Relay Action: RlyHit
  Chassis ID    Type: MAC       Info: 0012.e254.dbf0
  Ingress Port  Type: LOCAL      Info: Port 0/7
    MP Address: 0012.e254.dc01  Action: OK
  Egress Port   Type: LOCAL      Info: Port 0/5
    MP Address: 0012.e254.dc09  Action: OK

>
```

21.3.5　CFM の状態の確認

運用コマンド show cfm で，CFM の設定状態と障害検知状態を表示します。CC で障害を検知した場合，検知した障害の中で，最も障害レベルの高い障害種別を「Status」で確認できます。

図 21-36 show cfm の実行結果

```
> show cfm

Date 20XX/05/28 09:31:33 UTC
Domain Level 3 Name(str): ProviderDomain_3
  MA 300   Name(str) : Tokyo_to_Osaka
    Primary VLAN:300   VLAN:10-20,300
    CC:Enable   Interval:1min
    Alarm Priority:2  Start Time: 2500ms  Reset Time:10000ms
    MEP Information
      ID:8012  UpMEP    CH1 (Up)    Enable   MAC:00ed.f205.0101  Status:-
  MA 400   Name(str) : Tokyo_to_Nagoya
    Primary VLAN:400   VLAN:30-40,400
    CC:Enable   Interval:10min
    Alarm Priority:0  Start Time: 7500ms  Reset Time: 5000ms
    MEP Information
      ID:8014  DownMEP  0/5(Up)     Disable  MAC:00ed.f205.0105  Status:-
  MIP Information
      0/2(Up)     Enable   MAC:00ed.f205.0102
      0/4(Down)   Enable   MAC:-
Domain Level 4 Name(str): ProviderDomain_4
  MIP Information
      CH8 (Up)    Enable   MAC:00ed.f205.0108

>
```

21.3.6 障害の詳細情報の確認

運用コマンド show cfm fault detail で，障害種別ごとに，障害検知状態と障害検知のきっかけとなった CCM 情報を表示します。CCM を送信したリモート MEP は「RMEP」，「MAC」および「VLAN」で確認できます。

図 21-37 show cfm fault detail の実行結果

```
> show cfm fault domain-level 7 detail

Date 20XX/05/29 07:28:32 UTC
MD:7  MA:1000  MEP:1000  Fault
  OtherCCM : -  RMEP:1001 MAC:0012.e254.dbff VLAN:1000 Time:20XX/05/29 07:18:44
  ErrorCCM : On RMEP:1001 MAC:0012.e254.dbff VLAN:1000 Time:20XX/05/29 07:27:45
  Timeout  : On RMEP:1001 MAC:0012.e254.dbff VLAN:1000 Time:20XX/05/29 07:27:20
  PortState: -
  RDI      : -  RMEP:1001 MAC:0012.e254.dbff VLAN:1000 Time:20XX/05/29 07:23:45

>
```

22 SNMP を使用したネットワーク管理

この章では本装置の SNMP エージェント機能についてサポート仕様を中心に説明します。

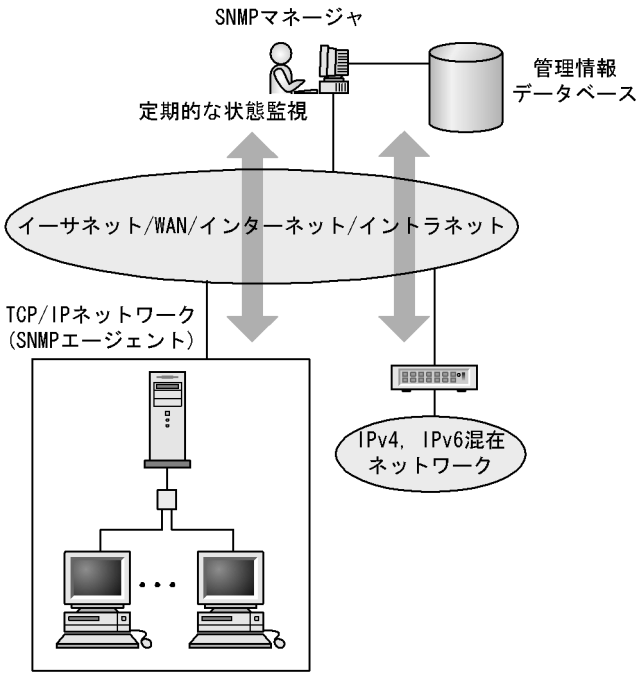
22.1　解説

22.1.1　SNMP 概説

（1） ネットワーク管理

ネットワークシステムの稼働環境や性能を維持するためには，高度なネットワーク管理が必要です。SNMP（simple network management protocol）は業界標準のネットワーク管理プロトコルです。SNMP をサポートしているネットワーク機器で構成されたマルチベンダーネットワークを管理できます。管理情報を収集して管理するサーバを **SNMP マネージャ**，管理される側のネットワーク機器を **SNMP エージェント**といいます。ネットワーク管理の概要を次の図に示します。

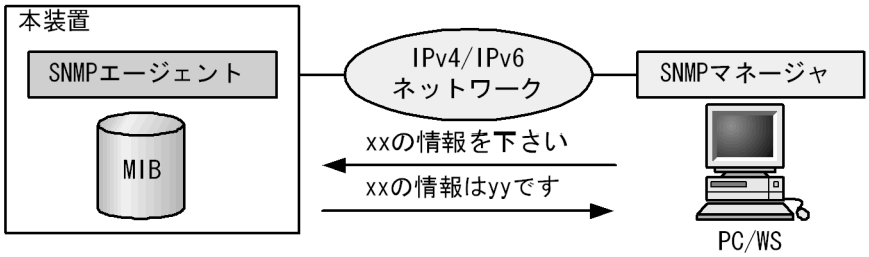
図 22-1　ネットワーク管理の概要



（2） SNMP エージェント機能

本装置の SNMP エージェントは，ネットワーク上の装置内部に組み込まれたプログラムです。装置内の情報を SNMP マネージャに提供する機能があります。装置内にある各種情報を MIB（Management Information Base）と呼びます。SNMP マネージャは，装置の情報を取り出して編集・加工し，ネットワーク管理を行うための各種情報をネットワーク管理者に提供するソフトウェアです。MIB 取得の例を次の図に示します。

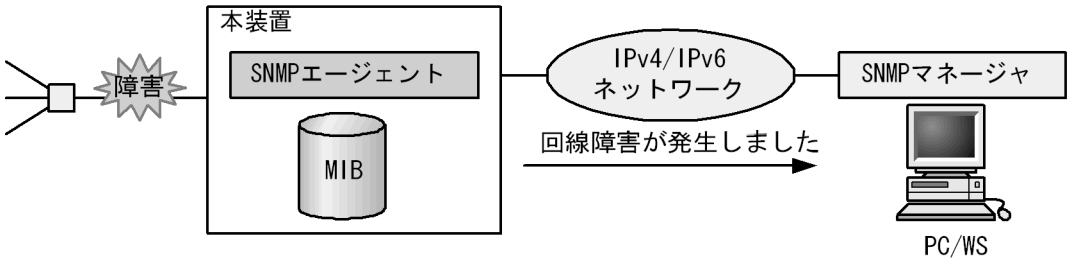
図 22-2　MIB 取得の例



本装置では，SNMPv1（RFC1157），SNMPv2C（RFC1901），および SNMPv3（RFC3410）をサポートしています。SNMP マネージャを使用してネットワーク管理を行う場合は，SNMPv1，SNMPv2C，または SNMPv3 プロトコルで使用してください。なお，SNMPv1，SNMPv2C，SNMPv3 をそれぞれ同時に使用することもできます。

また，SNMP エージェントは**トラップ**（Trap）と呼ばれるイベント通知（主に障害発生の情報など）機能があります。SNMP マネージャは，トラップを受信することで定期的に装置の状態変化を監視しなくても変化を知ることができます。ただし，トラップは UDP を使用しているため，装置から SNMP マネージャに対するトラップの到達確認ができません。そのため，ネットワークの輻輳などによって，トラップがマネージャに到達しない場合があります。通信経路を冗長化している場合であっても，障害発生から通信経路の切替が完了するまでの間に発生したトラップはマネージャに到達しない可能性があります。トラップの例を次の図に示します。

図 22-3　トラップの例



（3） SNMPv3

SNMPv3 は SNMPv2C までの全機能に加えて，管理セキュリティ機能が大幅に強化されています。ネットワーク上を流れる SNMP パケットを認証・暗号化することによって，SNMPv2C でのコミュニティ名と SNMP マネージャの IP アドレスの組み合わせによるセキュリティ機能では実現できなかった，盗聴，なりすまし，改ざん，再送などのネットワーク上の危険から SNMP パケットを守ることができます。

（a） SNMP エンティティ

SNMPv3 では，SNMP マネージャおよび SNMP エージェントを「SNMP エンティティ」と総称します。本装置の SNMPv3 は，SNMP エージェントに相当する SNMP エンティティをサポートしています。

（b） SNMP エンジン

SNMP エンジンは認証，および暗号化したメッセージ送受信と管理オブジェクトへのアクセス制御のためのサービスを提供します。SNMP エンティティとは 1 対 1 の関係です。SNMP エンジンは，同一管理ドメイン内でユニークな SNMP エンジン ID により識別されます。

(c) ユーザ認証と暗号化機能

SNMPv1，SNMPv2C でのコミュニティ名による認証に対して，SNMPv3 ではユーザ認証を行います。また，SNMPv1，SNMPv2C にはなかった暗号化機能も SNMPv3 でサポートされています。ユーザ認証と暗号化機能は，ユーザ単位に設定できます。

本装置では，ユーザ認証に使う認証プロトコルとして次のプロトコルをサポートしています。

- HMAC-MD5-96
  MD5 アルゴリズムを使用した認証プロトコルです。128 ビットのダイジェストのうち，先頭の 96 ビットを使用します。
- HMAC-SHA-96
  SHA-1 アルゴリズムを使用した認証プロトコルです。160 ビットのダイジェストのうち，先頭の 96 ビットを使用します。
- HMAC-SHA-256
  SHA-256 アルゴリズムを使用した認証プロトコルです。256 ビットのダイジェストのうち，先頭の 192 ビットを使用します。
- HMAC-SHA-512
  SHA-512 アルゴリズムを使用した認証プロトコルです。512 ビットのダイジェストのうち，先頭の 384 ビットを使用します。

暗号化機能に使うプライバシープロトコルとして次のプロトコルをサポートしています。

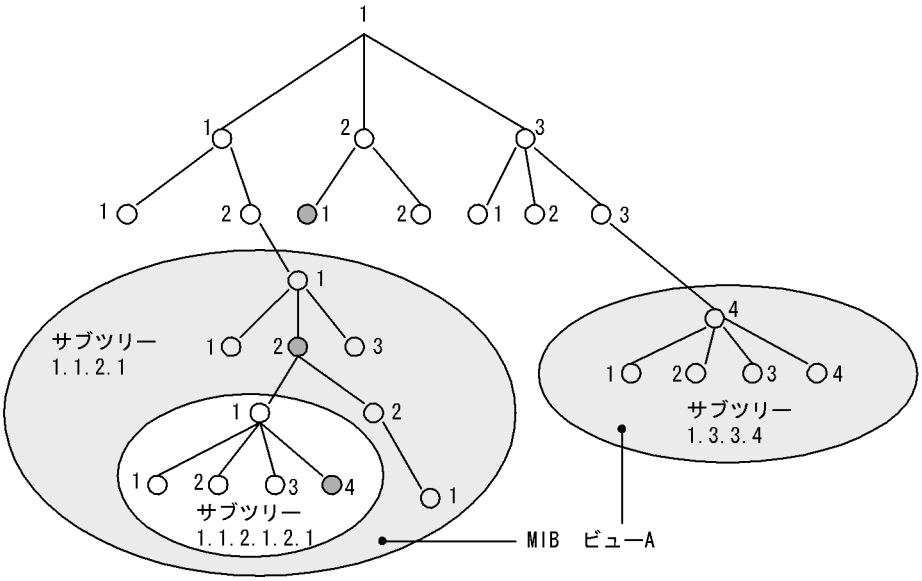
- CBC-DES
  DES アルゴリズムと，暗号利用モード CBC を組み合わせて暗号化するプライバシープロトコルです。
- CFB128-AES-128
  AES アルゴリズムと，暗号利用モード CFB を組み合わせて暗号化するプライバシープロトコルです。

(d) MIB ビューによるアクセス制御

SNMPv3 では，ユーザ単位に，アクセスできる MIB オブジェクトの集合を設定できます。この MIB オブジェクトの集合を MIB ビューと呼びます。MIB ビューは，MIB のオブジェクト ID のツリーを表すビューサブツリーを集約することによって表現されます。集約する際には，ビューサブツリーごとに included（MIB ビューに含む），または excluded（MIB ビューから除外する）を選択できます。MIB ビューは，ユーザ単位に，Read ビュー，Write ビュー，Notify ビューとして設定できます。

次に，MIB ビューの例を示します。MIB ビューは，「図 22-4　MIB ビューの例」に示すような MIB ツリーの一部である MIB サブツリーをまとめて設定します。オブジェクト ID 1.1.2.1.2 は，サブツリー 1.1.2.1 に含まれるので，MIB ビュー A でアクセスできます。しかし，オブジェクト ID 1.2.1 は，どちらのサブツリーにも含まれないので，アクセスできません。また，オブジェクト ID 1.1.2.1.2.1.4 は，サブツリー 1.1.2.1.2.1 がビュー A から除外されているためアクセスできません。

図 22-4　MIB ビューの例




```
コンフィグレーションの内容
 ViewA  1.1.2.1      included
        1.3.3.4      included
        1.1.2.1.2.1 excluded
```

22.1.2　MIB 概説

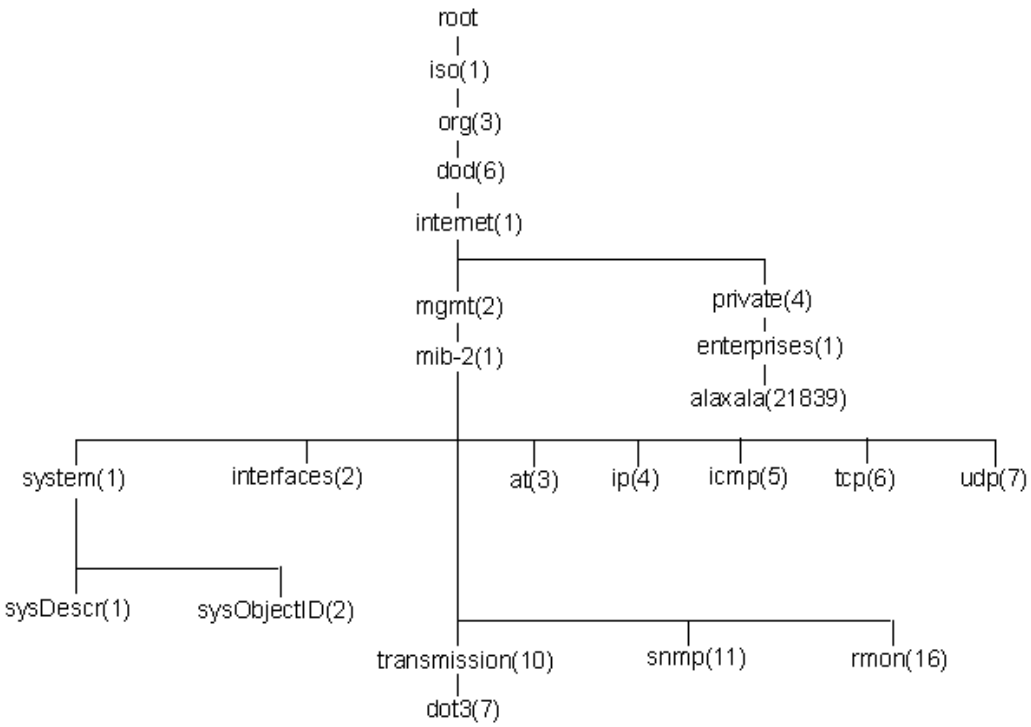
装置が管理し，SNMP マネージャに提供する MIB は，RFC で規定されたものと，装置の開発ベンダーが独自に用意する情報の 2 種類があります。

RFC で規定された MIB を**標準 MIB** と呼びます。標準 MIB は規格化されているため提供情報の内容の差はあまりありません。装置の開発ベンダーが独自に用意する MIB を**プライベート MIB** と呼び，装置によって内容が異なります。ただし，MIB のオペレーション（情報の採取・設定など）は，標準 MIB，プライベート MIB で共通です。オペレーションは，装置と目的の MIB 情報を指定するだけです。装置は IP アドレスで，MIB 情報はオブジェクト ID で指定します。

（1）MIB 構造

MIB の構造はツリー構造になっています。MIB はツリー構造のため，各ノードを識別するために番号を付けて表す決まりになっています。root から各ノードの数字を順番にたどって番号を付けることで個々の MIB 情報を一意に識別できます。この番号列をオブジェクト ID と呼びます。オブジェクト ID は root から下位のオブジェクトグループ番号をドットで区切って表現します。例えば，sysDescr という MIB をオブジェクト ID で示すと 1.3.6.1.2.1.1.1 になります。MIB ツリーの構造例を次の図に示します。

図 22-5 MIB ツリーの構造例



(2) MIB オブジェクトの表し方

オブジェクト ID は数字と.（ドット）（例：1.3.6.1.2.1.1.1）で表現します。しかし，数字の羅列ではわかりにくいため，マネージャによっては，sysDescr というニーモニックで指定できるものもあります。ニーモニックで指定する場合，SNMP マネージャがどの MIB のニーモニックを使えるか確認してから使用してください。

(3) インデックス

MIB を指定するときのオブジェクト ID を使用しますが，一つの MIB に一つの意味だけある場合と一つの MIB に複数の情報がある場合があります。MIB を特定するためにはインデックス（INDEX）を使用します。インデックスは，オブジェクト ID の後ろに数字を付加して表し，何番目の情報かなどを示すために使用します。

一つの MIB に一つの意味だけがある場合，MIB のオブジェクト ID に ".0" を付加して表します。一つの MIB に複数の情報がある場合，MIB のオブジェクト ID の後ろに数字を付加して何番目の情報であるか表します。例えば，インタフェースのタイプを示す MIB に ifType（1.3.6.1.2.1.2.2.1.2）があります。本装置には複数のインタフェースがあります。特定のインタフェースのタイプを調べるには，"2 番目のインタフェースのタイプ " というように具体的に指定する必要があります。MIB で指定するときは，2 番目を示すインデックス .2 を MIB の最後に付加して ifType.2（1.3.6.1.2.1.2.2.1.2.2）と表します。

インデックスの表し方は，各 MIB によって異なります。RFC などの MIB の定義で，INDEX{ xxxxx,yyyyy,zzzzzz } となっている MIB のエントリは，xxxxx と yyyyy と zzzzzz をインデックスに持ちます。それぞれの MIB について，どのようなインデックスを取るか確認して MIB のオペレーションを行ってください。

（4） 本装置のサポート MIB

本装置では，装置の状態，インタフェースの統計情報，装置の機器情報など，管理に必要な MIB を提供しています。なお，プライベート MIB の定義（ASN.1）ファイルは，ソフトウェアとともに提供します。

各 MIB の詳細については，マニュアル「MIB レファレンス」を参照してください。

22.1.3　SNMPv1，SNMPv2C オペレーション

管理データ（MIB:management information base）の収集や設定を行うため，SNMP では次に示す 4 種類のオペレーションがあります。

- GetRequest　　：指定した MIB の情報を取り出します。
- GetNextRequest：指定した次の MIB の情報を取り出します。
- GetBulkRequest：GetNextRequest の拡張版です。
- SetRequest　　：指定した MIB に値を設定します。

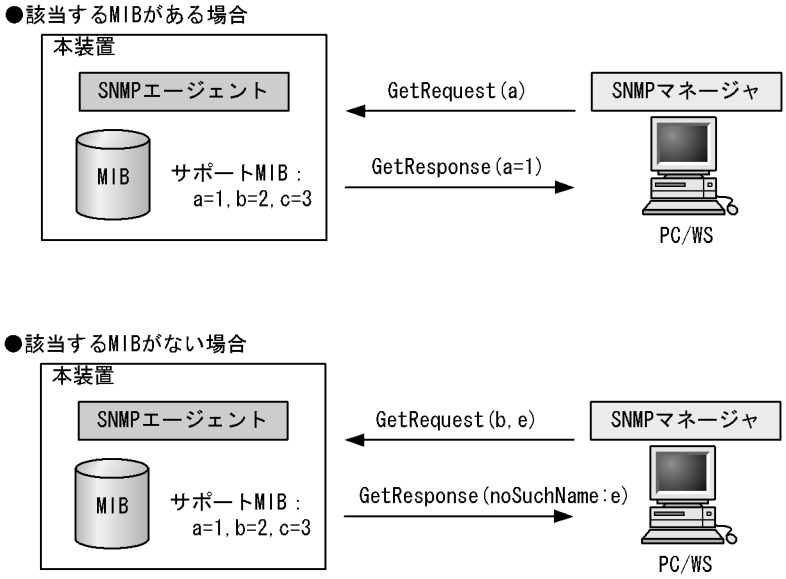
各オペレーションは SNMP マネージャから装置（SNMP エージェント）に対して行われます。各オペレーションについて説明します。

（1） GetRequest オペレーション

GetRequest オペレーションは，SNMP マネージャから装置（エージェント機能）に対して MIB の情報を取り出すときに使用します。このオペレーションでは，一つまたは複数 MIB を指定できます。

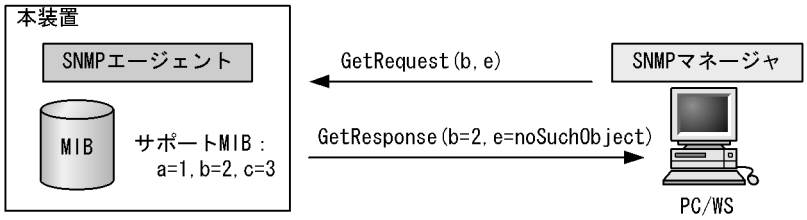
装置が該当する MIB を保持している場合，GetResponse オペレーションで MIB 情報を応答します。該当する MIB を保持していない場合は，GetResponse オペレーションで noSuchName を応答します。GetRequest オペレーションを次の図に示します。

図 22-6　GetRequest オペレーション



SNMPv2C では，装置が該当する MIB を保持していない場合は，GetResponse オペレーションで MIB 値に noSuchObject を応答します。SNMPv2C の場合の GetRequest オペレーションを次の図に示します。

図 22-7　GetRequest オペレーション（SNMPv2C）

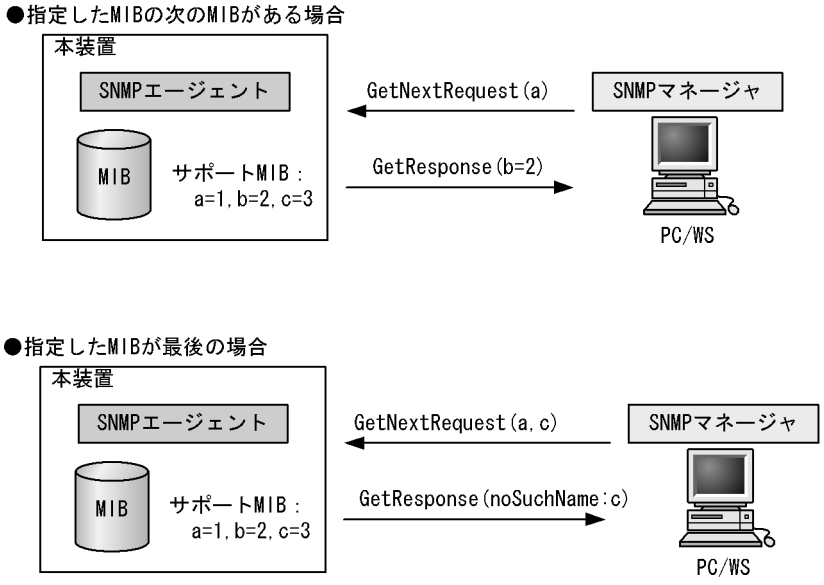


（2） GetNextRequest オペレーション

GetNextRequest オペレーションは，GetRequest オペレーションに似たオペレーションです。GetRequest オペレーションは，指定した MIB の読み出しに使用しますが，GetNextRequest オペレーションは，指定した MIB の次の MIB を取り出すときに使用します。このオペレーションも一つまたは複数の MIB を指定できます。

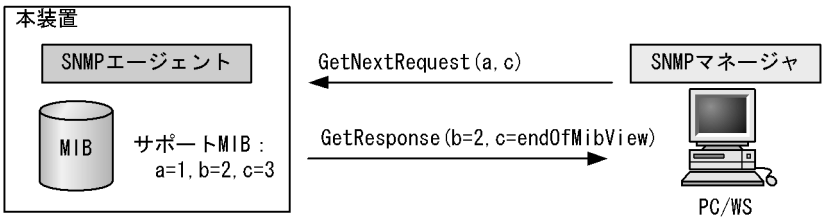
装置が指定した次の MIB を保持している場合は，GetResponse オペレーションで MIB を応答します。指定した MIB が最後の場合は，GetResponse で noSuchName を応答します。GetNextRequest オペレーションを次の図に示します。

図 22-8　GetNextRequest オペレーション



SNMPv2C の場合，指定した MIB が最後の場合は GetResponse で MIB 値に endOfMibView を応答します。SNMPv2C の場合の GetNextRequest オペレーションを次の図に示します。

図 22-9　GetNextRequest オペレーション（SNMPv2C）

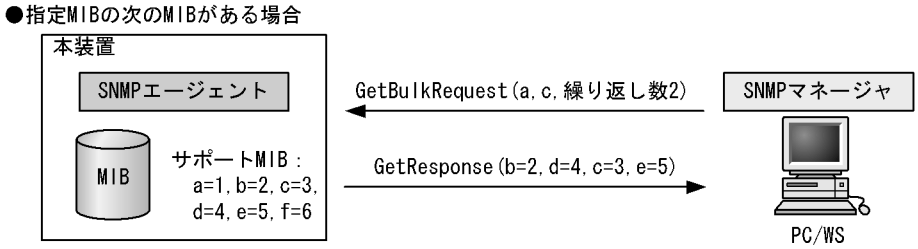


（3） GetBulkRequest オペレーション

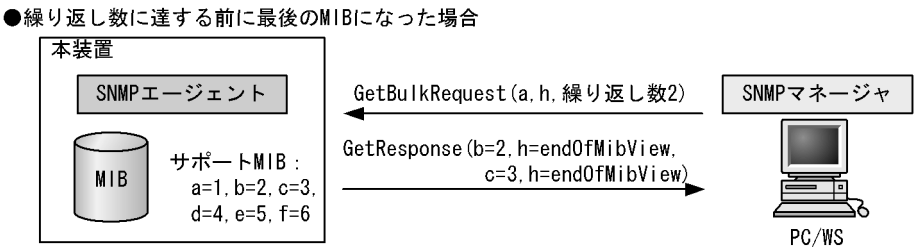
GetBulkRequest オペレーションは，GetNextRequest オペレーションを拡張したオペレーションです。このオペレーションでは繰り返し回数を設定し，指定した MIB の次の項目から指定した繰り返し回数個分の MIB を取得できます。このオペレーションも，一つまたは複数の MIB を指定できます。

装置が，指定した MIB の次の項目から指定した繰り返し回数個分の MIB を保持している場合は，GetResponse オペレーションで MIB を応答します。指定した MIB が最後の場合，または繰り返し数に達する前に最後の MIB になった場合，GetResponse オペレーションで MIB 値に endOfMibView を応答します。GetBulkRequest オペレーションを次の図に示します。

図 22-10　GetBulkRequest オペレーション



上記の図では，MIB：a，c，繰り返し数 2 を指定したので，a の次の MIB=b，c の次の MIB= d，再度繰り返して b の次の MIB=c，d の次の MIB=e までを取得できます。



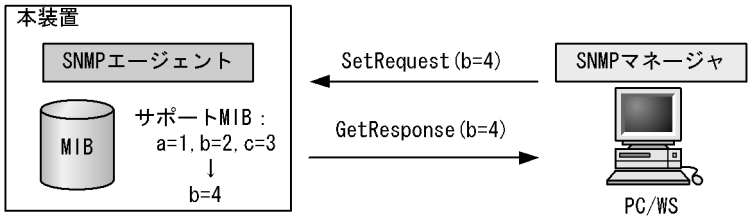
上記の図では，MIB：a，h，繰り返し数 2 を指定しましたが，h は最後の MIB なので endOfMibView を応答しています。

（4） SetRequest オペレーション

SetRequest オペレーションは，SNMP マネージャから装置（エージェント機能）に対して行うオペレーションという点で GetRequest，GetNextRequest，GetBulkRequest オペレーションと似ていますが，値の設定方法が異なります。

SetRequest オペレーションでは，設定する値と MIB を指定します。値を設定すると，GetResponse オペレーションで MIB と設定値を応答します。SetRequest オペレーションを次の図に示します。

図 22-11　SetRequest オペレーション



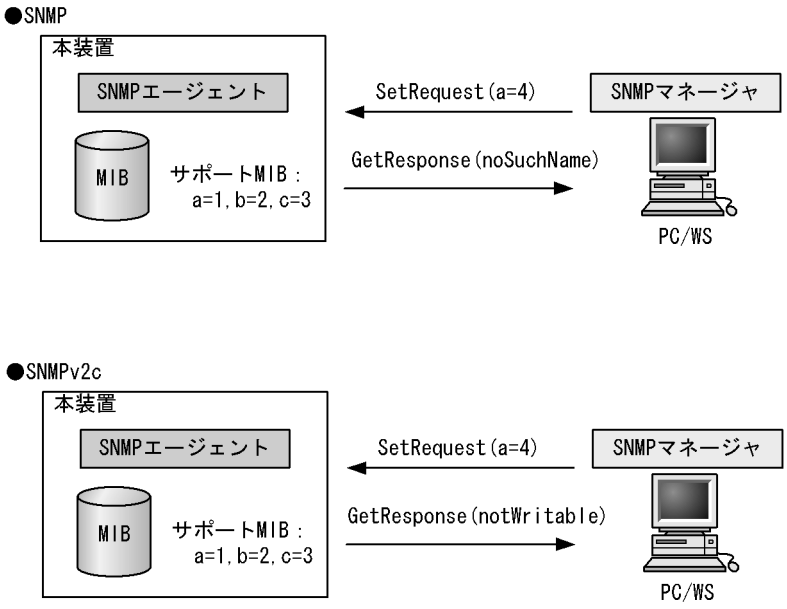
(a) MIB を設定できない場合の応答

MIB を設定できないケースは，次に示す 3 とおりです。

- MIB が読み出し専用の場合（読み出し専用コミュニティに属するマネージャの場合も含む）
- 設定値が正しくない場合
- 装置の状態によって設定できない場合

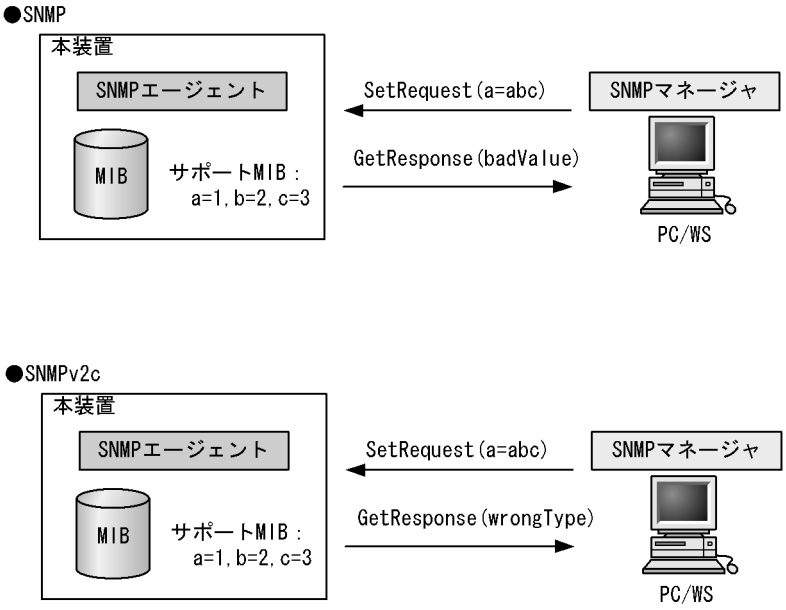
各ケースによって，応答が異なります。MIB が読み出し専用の場合，noSuchName の GetResponse 応答をします。SNMPv2C の場合，MIB が読み出し専用のときは notWritable の GetResponse 応答をします。MIB が読み出し専用の場合の SetRequest オペレーションを次の図に示します。

図 22-12　MIB 変数が読み出し専用の場合の SetRequest オペレーション



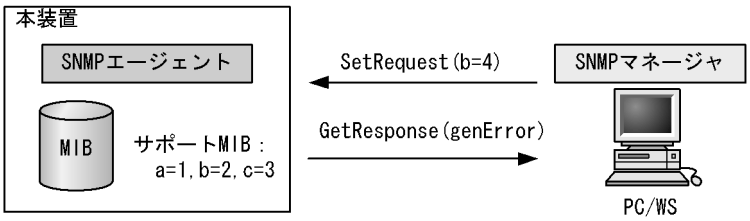
設定値のタイプが正しくない場合，badValue の GetResponse 応答をします。SNMPv2C の場合，設定値のタイプが正しくないときは wrongType の GetResponse 応答をします。設定値のタイプが正しくない場合の SetRequest オペレーションを次の図に示します。

図 22-13　設定値のタイプが正しくない場合の SetRequest オペレーション例



装置の状態によって設定できない場合，genError を応答します。例えば，装置内で値を設定しようとしたときに，装置内部で設定タイムアウトを検出した場合などがこれに当てはまります。装置の状態によって設定できない場合の SetRequest オペレーションを次の図に示します。

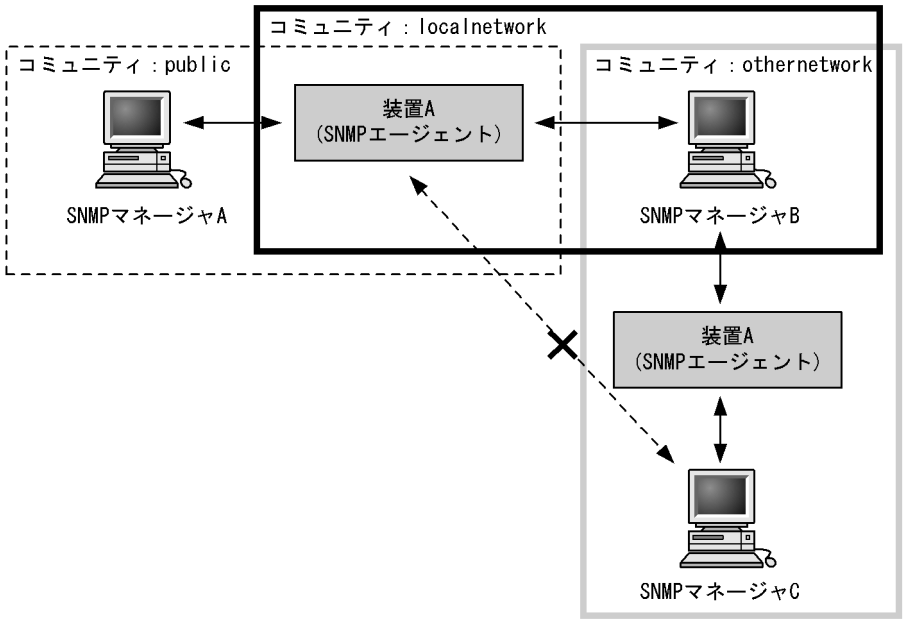
図 22-14　装置の状態によって設定できない場合の SetRequest オペレーション



（5）コミュニティによるオペレーション制限

SNMPv1 および SNMPv2C では，オペレーションを実行する SNMP マネージャを限定するため，コミュニティという概念があります。コミュニティはオペレーションを実行する SNMP マネージャと SNMP エージェントを一つのグループとして割り当てる名称です。MIB に対してオペレーションする場合は，SNMP マネージャと SNMP エージェントは，同一のグループ（コミュニティ）に属する必要があります。コミュニティによるオペレーションを次の図に示します。

図 22-15　コミュニティによるオペレーション



装置 A はコミュニティ（public）およびコミュニティ（localnetwork）に属しています。コミュニティ（othernetwork）には属していません。この場合，装置 A はコミュニティ（public）およびコミュニティ（localnetwork）の SNMP マネージャ A，B から MIB のオペレーションを受け付けますが，コミュニティ（othernetwork）の SNMP マネージャ C からのオペレーションは受け付けません。

（6） IP アドレスによるオペレーション制限

本装置では，セキュリティを考慮し，アクセスリストを使用することでコミュニティと SNMP マネージャの IP アドレスの組み合わせが合わないときは MIB のオペレーションを受け付けないようにできます。本装置で SNMPv1 および SNMPv2C を使用するときは，コミュニティをコンフィグレーションコマンドで登録する必要があります。なお，コミュニティは文字列で設定します。また，一般的にコミュニティ名称は，public を使用している場合が多いです。

（7） SNMP オペレーションのエラーステータスコード

オペレーションでエラーが発生した場合，SNMP エージェントはエラーステータスにエラーコードを設定し，何番目の MIB 情報でエラーが発生したかをエラー位置番号に設定した GetResponse オペレーションの応答を返します。オペレーションの結果が正常なら，エラーステータスにエラーなしのコードを設定し，MIB 情報内にオペレーションした MIB 情報を設定した GetResponse オペレーションの応答を返します。エラーステータスコードを次の表に示します。

表 22-1　SNMPv1 のエラーステータスコード

エラーステータス	値	発生条件
noError	0	正常。
tooBig	1	応答メッセージ長が 2048 バイトを超えました。
noSuchName	2	• Get/Set で指定されたオブジェクトが存在しません。 • Set で指定されたオブジェクトが read-only 実装になっています。 • Set のコミュニティが ro 定義されています。 • GetNext で最後に到達しました。(snmpwalk が完了しました。)

エラーステータス	値	発生条件
badValue	3	Set で不正な値が指定されました。（型などが不正な場合を含みます）
readOnly	4	未使用。
genError	5	Set で最大エントリ数を超えました。 （ホワイトリスト機能無効で axsWhitelistSourceBlockGroup を Set したとき，およびリソース不足状態も含みます）

コミュニティ名が未設定の場合は，応答を返しません。（エラーコードもありません。）

表 22-2　SNMPv2C のエラーステータスコード

エラーステータス	値	発生条件
noError	0	正常。
tooBig	1	応答メッセージ長が 2048 バイトを超えました。
noSuchName	2	未使用。
badValue	3	未使用。
readOnly	4	未使用。
genError	5	他に該当しないエラーです。
noAccess	6	Set のコミュニティが ro 定義されています。
wrongType	7	Set で不正な値が指定されました。（型が不一致）
wrongLength	8	Set で不正な値が指定されました。（文字列長などが範囲外）
wrongEncoding	9	Set で指定された値の符号化が不正です。（本装置では未使用）
wrongValue	10	Set で不正な値が指定されました。
noCreation	11	• Set で指定された ifTable の列（ifIndex）が存在しません。 • Set で指定されたテーブル型オブジェクトの列番号が範囲外です。
inconsistentValue	12	エントリへのアクセス手順が合っていないため，Set で指定された値を設定できません。
resourceUnavailable	13	Set で最大エントリ数を超えました。 （ホワイトリスト機能無効で axsWhitelistSourceBlockGroup を Set したとき，およびリソース不足状態も含みます）
commitFailed	14	設定処理で失敗しました。
undoFailed	15	復元処理で失敗しました。（本装置では未使用）
authorizationError	16	未使用。
notWritable	17	• Set で指定されたオブジェクトが実装されていません。 • Set で指定されたオブジェクトが read-only 実装になっています。
inconsistentName	18	エントリへのアクセス手順が合っていないため，Set で指定されたテーブル型オブジェクトの列を生成できません。

コミュニティ名が未設定の場合は，応答を返しません。（エラーコードもありません。）

表 22-3　SNMPv2C のオブジェクトごとのステータス

ステータス	値	発生条件
noSuchObject	[0]	Get で指定されたオブジェクトが存在しません。
noSuchInstance	[1]	Get で指定されたテーブル型オブジェクトの列が存在しません。
endOfMibView	[2]	GetNext で最後に到達しました。（snmpwalk が完了しました。）

22.1.4　SNMPv3 オペレーション

管理データ（MIB:management information base）の収集や設定を行うため，SNMP では次に示す四種類のオペレーションがあります。

- GetRequest　　：指定した MIB の情報を取り出します。
- GetNextRequest：指定した次の MIB の情報を取り出します。
- GetBulkRequest：GetNextRequest の拡張版です。
- SetRequest　　：指定した MIB に値を設定します。

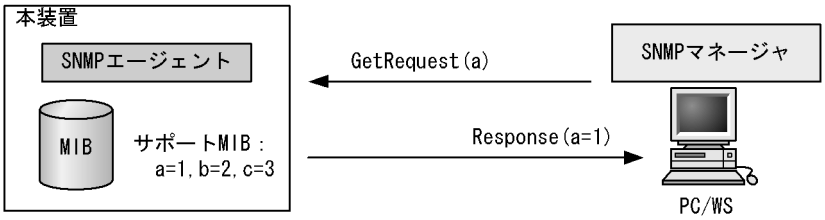
各オペレーションは SNMP マネージャから装置（SNMP エージェント）に対して行われます。各オペレーションについて説明します。

（1） GetRequest オペレーション

GetRequest オペレーションは，SNMP マネージャから装置（エージェント機能）に対して MIB の情報を取り出すときに使用します。このオペレーションでは，一つまたは複数の MIB を指定できます。装置が該当する MIB を保持している場合，Response オペレーションで MIB 情報を応答します。

GetRequest オペレーションを次の図に示します。

図 22-16　GetRequest オペレーション

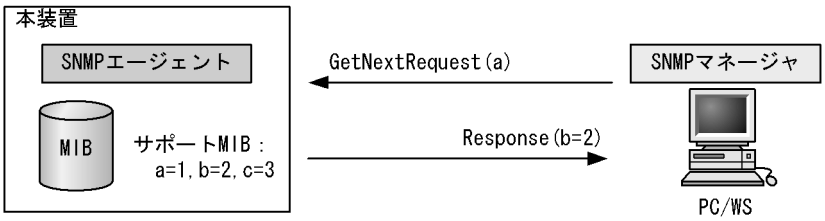


（2） GetNextRequest オペレーション

GetNextRequest オペレーションは，GetRequest オペレーションに似たオペレーションです。GetRequest オペレーションが指定した MIB の読み出しに使用するのに対し，GetNextRequest オペレーションは指定した MIB の次の MIB を取り出すときに使用します。このオペレーションも一つまたは複数の MIB を指定できます。

GetNextRequest オペレーションを次の図に示します。

図 22-17　GetNextRequest オペレーション



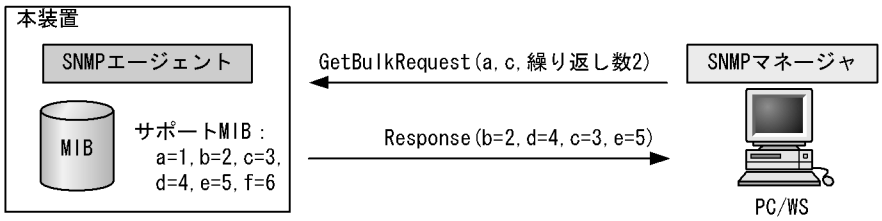
（3） GetBulkRequest オペレーション

GetBulkRequest オペレーションは，GetNextRequest オペレーションを拡張したオペレーションです。このオペレーションでは繰り返し回数を設定し，指定した MIB の次の項目から指定した繰り返し回数個

分の MIB を取得できます。このオペレーションも，一つまたは複数の MIB を指定できます。

GetBulkRequest オペレーションを次の図に示します。

図 22-18　GetBulkRequest オペレーション



上記の図では，MIB：a，c，繰り返し数 2 を指定したので，a の次の MIB=b，c の次の MIB= d，再度繰り返して b の次の MIB=c，d の次の MIB=e までを取得できます。

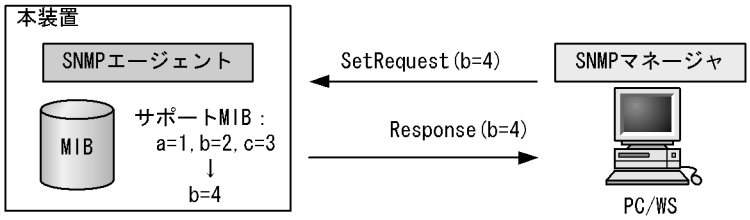
（4） SetRequest オペレーション

SetRequest オペレーションは，SNMP マネージャから装置（エージェント機能）に対して行うオペレーションという点で GetRequest，GetNextRequest，GetBulkRequest オペレーションと似ていますが，値の設定方法が異なります。

SetRequest オペレーションでは，設定する値と MIB を指定します。値を設定すると，Response オペレーションで MIB と設定値を応答します。

SetRequest オペレーションを次の図に示します。

図 22-19　SetRequest オペレーション



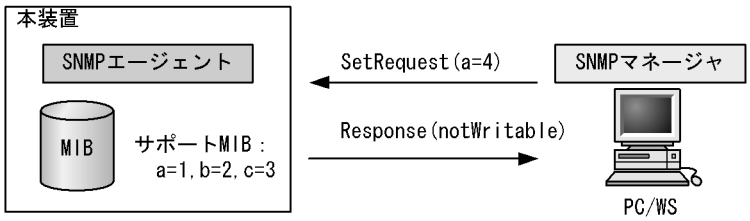
(a) MIB を設定できない場合の応答

MIB を設定できないケースは，次に示す 3 とおりです。

- MIB が読み出し専用の場合
- 設定値が正しくない場合
- 装置の状態によって設定できない場合

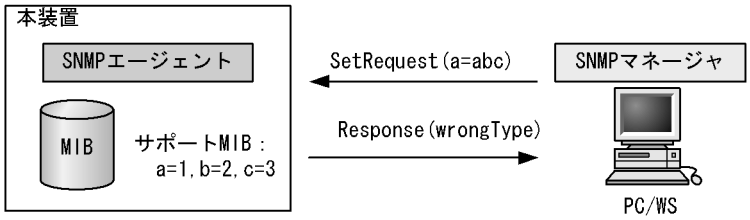
各ケースによって，応答が異なります。MIB が読み出し専用のときは notWritable の Response 応答をします。MIB が読み出し専用の場合の SetRequest オペレーションを次の図に示します。

図 22-20 MIB 変数が読み出し専用の場合の SetRequest オペレーション



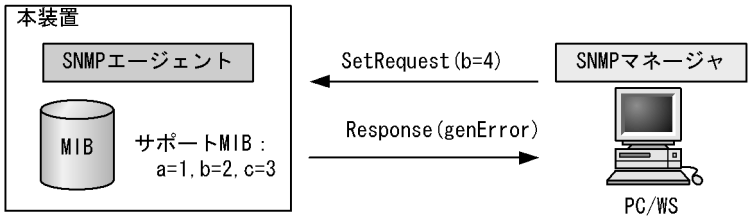
設定値のタイプが正しくないときは wrongType の Response 応答をします。設定値のタイプが正しくない場合の SetRequest オペレーションを次の図に示します。

図 22-21 設定値のタイプが正しくない場合の SetRequest オペレーション例



装置の状態によって設定できない場合，genError を応答します。例えば，装置内で値を設定しようとしたときに，装置内部で設定タイムアウトを検出した場合などがこれに当てはまります。装置の状態によって設定できない場合の SetRequest オペレーションを次の図に示します。

図 22-22 装置の状態によって設定できない場合の SetRequest オペレーション



(5) SNMPv3 でのオペレーション制限

SNMPv1 および SNMPv2C ではコミュニティと SNMP マネージャの IP アドレスの組み合わせによって確認が行われるのに対し，SNMPv3 ではユーザ認証と MIB ビューによって MIB のオペレーションを制限します。本装置で SNMPv3 を使用するときは，SNMP セキュリティユーザ，MIB ビューおよびセキュリティグループをコンフィグレーションコマンドで登録する必要があります。また，トラップを送信するには，SNMP セキュリティユーザ，MIB ビュー，セキュリティグループ，およびトラップ送信 SNMP マネージャをコンフィグレーションコマンドで登録する必要があります。

(6) SNMPv3 オペレーションのエラーステータスコード

オペレーションの結果エラーが発生した場合，SNMP エージェントはエラーステータスにエラーコードを設定し，何番目の MIB 情報でエラーが発生したかをエラー位置番号に設定した Response オペレーションの応答を返します。オペレーションの結果が正常であれば，エラーステータスにエラーなしのコードを設定し，MIB 情報内にオペレーションした MIB 情報を設定した Response オペレーションの応答を返します。エラーステータスコードを次の表に示します。

表 22-4 SNMPv3 のレポート

値	オブジェクト ID	発生条件
snmpInASNParseErrs	1.3.6.1.2.1.11.6	セキュリティパラメータの ASN.1 符号化が正しくありません。
snmpUnknoenSecurityModels	1.3.6.1.6.3.11.2.1.1	セキュリティモデルが正しくありません。
snmpInvalidMsgs	1.3.6.1.6.3.11.2.1.2	暗号メッセージが認証されていません。
snmpUnknownPDUHandlers	1.3.6.1.6.3.11.2.1.3	コンテキストエンジン ID が正しくありません。
usmStatsUnknownEngineIDs	1.3.6.1.6.3.15.1.1.4	エンジン ID が正しくありません。
usmStatsUnknownUserNames	1.3.6.1.6.3.15.1.1.3	ユーザ名が定義されていません。
usmStatsUnsupportedSecLevels	1.3.6.1.6.3.15.1.1.1	認証鍵が未設定のユーザから認証メッセージを受信しました。 または，暗号鍵が未設定のユーザから暗号メッセージを受信しました。
usmStatsNotInTimeWindows	1.3.6.1.6.3.15.1.1.2	再起動回数，または再起動後の経過時間が合っていません。
usmStatsDecryptionErrors	1.3.6.1.6.3.15.1.1.6	本装置では未使用。
snmpUnknownContexts	1.3.6.1.6.3.12.1.5	コンテキスト名が正しくありません。

表 22-5 SNMPv3 のエラーステータスコード

エラーステータス	値	発生条件
noError	0	正常。
tooBig	1	応答メッセージが 2048 バイトを超えました。 または，応答メッセージ長が要求元の限界を超えています。ただし，GetBulk 応答は自動的に調整されます。
noSuchName	2	未使用。
badValue	3	未使用。
readOnly	4	未使用。
genError	5	他に該当しないエラーです。
noAccess	6	Set のコミュニティ名が ro 定義されています。
wrongType	7	Set で不正な値が指定されました。（型が不一致）
wrongLength	8	Set で不正な値が指定されました。（文字列長などが範囲外）
wrongEncoding	9	Set で指定された値の符号化が不正です。（本装置では未使用）
wrongValue	10	Set で不正な値が指定されました。
noCreation	11	• Set で指定された ifTable の列（ifIndex）が存在しません。 • Set で指定されたテーブル型オブジェクトの列番号が範囲外です。
inconsistentValue	12	エントリへのアクセス手順が合っていないため，Set で指定された値を設定できません。
resourceUnavailable	13	Set で最大エントリ数を超えました。 （ホワイトリスト機能無効で axsWhitelistSourceBlockGroup を Set したとき，およびリソース不足状態も含みます）
commitFailed	14	設定処理で失敗しました。
undoFailed	15	復元処理で失敗しました。（本装置では未使用）

エラーステータス	値	発生条件
authorizationError	16	• Get/GetNext/GetBulk 要求のユーザのグループに read ビューが設定されていません。または read ビューが空です。 • Set 要求のユーザのグループに write ビューが設定されていません。または write ビューが空です。
notWritable	17	• Set で指定されたオブジェクトが実装されていません。 • Set で指定されたオブジェクトが read-only 実装になっています。
inconsistentName	18	エントリへのアクセス手順が合っていないため，Set で指定されたテーブル型オブジェクトの列を生成できません。

表 22-6　SNMPv3 のオブジェクトごとのステータス

ステータス	値	発生条件
noSuchObject	[0]	Get で指定されたオブジェクトが存在しません。
noSuchInstance	[1]	Get で指定されたテーブル型オブジェクトの列が存在しません。
endOfMibView	[2]	GetNext で最後に到達しました。（snmpwalk が完了しました。）

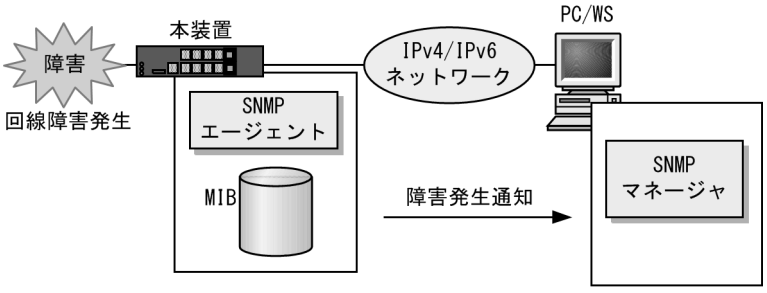
22.1.5　トラップ

（1）トラップ概説

SNMP エージェントは**トラップ**（Trap）と呼ばれるイベント通知（主に障害発生の情報やログ情報など）機能があります。トラップは重要なイベントを SNMP エージェントから SNMP マネージャに非同期に通知する機能です。SNMP マネージャは，トラップを受信することで定期的に装置の状態変化を検知できます。この通知を基に，装置内の MIB を取得して，さらに詳細な情報を得ることができます。

なお，トラップは UDP を使用しているため，装置から SNMP マネージャに対するトラップの到達が確認できません。そのため，ネットワークの輻輳などによってトラップがマネージャに到達しない場合があります。通信経路を冗長化している場合であっても，障害発生から通信経路の切替が完了するまでの間に発生したトラップはマネージャに到達しない可能性があります。トラップの例を次の図に示します。

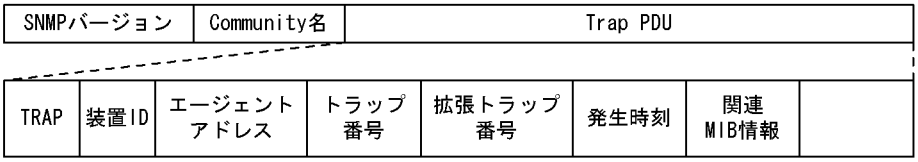
図 22-23　トラップの例



（2）トラップフォーマット

トラップフレームには，どの IP アドレスの装置で，いつ，何が発生したかを示す情報を含みます。トラップフォーマットを次の図に示します。

図 22-24　トラップフォーマット



装置ID　　：装置の識別ID（通常MIB-IIのsysObjectIDの値が設定される）
エージェントアドレス：トラップが発生した装置のIPアドレス
トラップ番号　　：トラップの種別を示す識別番号
拡張トラップ番号　：トラップ番号の補足をするための番号
発生時刻　　：トラップが発生した時間（装置が起動してからの経過時間）
関連MIB情報　　：このトラップに関連するMIB情報

22.1.6　RMON MIB

RMON（Remote Network Monitoring）とは，イーサネット統計情報を提供する機能，収集した統計情報の閾値チェックを行ってイベントを発生させる機能，パケットをキャプチャする機能などを持ちます。この RMON は RFC1757 で規定されています。

RMON MIB のうち，statistics，history，alarm，event の各グループについて概要を説明します。

（1） statistics グループ

監視対象のサブネットワークについての，基本的な統計情報を収集します。例えば，サブネットワーク中の総パケット数，ブロードキャストパケットのような各種類ごとのパケット数，CRC エラー，コリジョンエラーなどのエラー数などです。statistics グループを使うと，サブネットワークのトラフィック状況や回線状態などの統計情報を取得できます。

（2） history グループ

statistics グループで収集する情報とほぼ同じ統計情報をサンプリングし，来歴情報として保持できます。

history グループには historyControlTable という制御テーブルと，etherHistoryTable というデータテーブルがあります。historyControlTable はサンプリング間隔や来歴記録数の設定を行うための MIB です。

etherHistoryTable は，サンプリングした統計情報の来歴記録の MIB です。history グループは，一定期間の統計情報を装置内で保持しています。このため，SNMP マネージャなどが定期的にポーリングして統計情報を収集するのと比較して，ネットワークに負荷をかけることが少なく，連続した一定期間の統計情報を取得できます。

（3） alarm グループ

監視対象とする MIB のチェック間隔，閾値などを設定して，その MIB が閾値に達したときにログを記録したり，SNMP マネージャにトラップを発行したりすることを指定する MIB です。

この alarm グループは，例えば，サンプルタイムとして設定した 5 分間のうちに，パケットを取りこぼすという状態が 10 回以上検出したときにログを収集したり，SNMP マネージャにトラップを発行したりできます。この alarm グループを使用するときは，event グループも設定する必要があります。

（4） event グループ

event グループには alarm グループで設定した MIB の閾値を超えたときの動作を指定する eventTable グループ MIB と閾値を超えたときにログを記録する logTable グループ MIB があります。

eventTable グループ MIB は，閾値に達したときにログを記録するのか，SNMP マネージャにトラップを発行するのか，またはその両方するか何もしないかを設定するための MIB です。

logTable グループ MIB は，eventTable グループ MIB でログの記録を指定したときに，装置内にログを記録します。装置内のログのエントリ数は決まっているので，エントリをオーバーした場合，新しいログ情報の追加によって，古いログ情報が消去されていきます。定期的に SNMP マネージャに記録を退避しないと，前のログが消されてしまう可能性がありますので注意してください。

22.1.7　SNMP マネージャとの接続時の注意事項

（1） MIB 情報収集周期のチューニング

SNMP マネージャは，ネットワーク上の新しい装置を検出したり，トラフィック状況を監視したりするため，SNMP エージェントサポート機器から定期的に MIB を取得します。この定期的な MIB 取得の間隔が短いと，ネットワーク機器やネットワークに負荷が掛かります。また，装置の状態や構成などによって，MIB 取得時にマネージャ側でタイムアウトが発生するおそれがあります。特に，次に示すケースでは応答タイムアウトの発生するおそれが高まります。

- 接続 SNMP マネージャ数が多い場合
  本装置に SNMP マネージャが多数接続され，MIB 情報の収集が集中した場合。
- SNMP イベントが同時に多数発生している場合
  本装置から大量にトラップが発行されるような状態のときに，MIB を取得した場合や，本装置から発行されたトラップに基づいて，並行して MIB を取得した場合。

応答タイムアウトが頻発する場合は，SNMP マネージャのポーリング周期や応答監視タイマ値をチューニングしてください。代表的な SNMP マネージャのチューニングパラメータには，次の三つがあります。

- ポーリング周期
- 応答監視タイマ
- 応答監視タイムアウト時のリトライ回数

22.2　コンフィグレーション

22.2.1　コンフィグレーションコマンド一覧

SNMP/RMON に関するコンフィグレーションコマンド一覧を次の表に示します。

表 22-7　コンフィグレーションコマンド一覧

コマンド名	説明
hostname	本装置のホスト名称を設定します。本設定は RFC1213 の sysName に対応します。
rmon alarm	RMON（RFC1757）アラームグループの制御情報を設定します。
rmon collection history	RMON（RFC1757）イーサネットの統計来歴の制御情報を設定します。
rmon event	RMON（RFC1757）イベントグループの制御情報を設定します。
snmp-server community	SNMP コミュニティに対するアクセスリストを設定します。
snmp-server contact	本装置の連絡先などを設定します。本設定は RFC1213 の sysContact に対応します。
snmp-server engineID local	SNMP エンジン ID 情報を設定します。
snmp-server group	SNMPv3 のセキュリティグループ情報を設定します。
snmp-server host	トラップを送信するネットワーク管理装置（SNMP マネージャ）を登録します。
snmp-server location	本装置を設置する場所の名称を設定します。本設定は RFC1213 の sysLocation に対応します。
snmp-server traps	トラップの発行契機を設定します。
snmp-server user	SNMPv3 のセキュリティユーザ情報を設定します。
snmp-server view	SNMPv3 の MIB ビュー情報を設定します。
snmp trap link-status	no snmp trap link-status 設定時，回線がリンクアップまたはダウンした場合に，トラップ（SNMP link down および up Trap）の送信を抑止します。

22.2.2　SNMPv1，SNMPv2C による MIB アクセス許可の設定

［設定のポイント］

SNMP マネージャから本装置の MIB へのアクセスを許可するための設定をします。

特定の SNMP マネージャからだけ，本装置へのアクセスを許可する場合は，コンフィグレーションコマンド ip access-list standard であらかじめアクセスを許可する端末の IP アドレスを登録しておく必要があります。1 コミュニティに 1 アクセスリストを指定できます。

［コマンドによる設定］

1. **(config)# ip access-list standard SNMPMNG**
   (config-std-nacl)# permit host 128.1.1.2
   (config-std-nacl)# exit
   IP アドレス 128.1.1.2 からのアクセスを許可するアクセスリストを設定します。
2. **(config)# snmp-server community "NETWORK" ro SNMPMNG**
   SNMP マネージャのコミュニティに対する MIB アクセスモードおよび適用するアクセスリストを設定します。
   - コミュニティ名：NETWORK

- アクセスリスト：SNMPMNG
- アクセスモード：read only

［注意事項］

- 本機能で使用するアクセスリストは，フロー検出モードの設定に依存しません。
- permit 条件に一致した IP アドレスは，アクセス許可の対象となります。
  deny 条件に一致した IP アドレスは，アクセス拒否の対象となります。
  IP アクセスリスト最終行には，全 IP アドレスを対象とした暗黙の deny 条件が存在します。
  本設定例では permit 条件を 1 行だけ設定していますが，この permit 条件に一致しなかった場合は，暗黙の deny 条件に一致したものとみなすため，アクセスを拒否します。

22.2.3 SNMPv3 による MIB アクセス許可の設定

［設定のポイント］

SNMPv3 で MIB にアクセスするために，アクセスを許可する MIB オブジェクトの集合を MIB ビューとして設定し，ユーザ認証とプライバシー機能の情報を SNMPv3 セキュリティユーザとして設定します。また，MIB ビューと SNMPv3 セキュリティユーザを関連づけるために，SNMPv3 セキュリティグループを設定します。

［コマンドによる設定］

1. **(config)# snmp-server view "READ_VIEW" 1.3.6.1 included**
   (config)# snmp-server view "READ_VIEW" 1.3.6.1.6.3 excluded
   (config)# snmp-server view "WRITE_VIEW" 1.3.6.1.2.1.1 included
   MIB ビューを設定します。
   - ビュー名 READ_VIEW に internet グループ MIB（サブツリー：1.3.6.1）を登録します。
   - ビュー名 READ_VIEW から snmpModules グループ MIB（サブツリー：1.3.6.1.6.3）を対象外にします。
   - ビュー名 WRITE_VIEW に system グループ MIB（サブツリー：1.3.6.1.2.1.1）を登録します。
2. **(config)# snmp-server user "ADMIN" "ADMIN_GROUP" v3 auth md5 "ABC*_1234" priv des "XYZ/+6789"**
   SNMPv3 セキュリティユーザを設定します。
   - SNMPv3 セキュリティユーザ名：ADMIN
   - SNMPv3 セキュリティグループ名：ADMIN_GROUP
   - 認証プロトコル：HMAC-MD5
   - 認証パスワード：ABC*_1234
   - 暗号化プロトコル：CBC-DES
   - 暗号化パスワード：XYZ/+6789
3. **(config)# snmp-server group "ADMIN_GROUP" v3 priv read "READ_VIEW" write "WRITE_VIEW"**
   SNMPv3 セキュリティグループを設定します。
   - SNMPv3 セキュリティグループ名：ADMIN_GROUP
   - セキュリティレベル：認証あり，暗号化あり
   - Read ビュー名：READ_VIEW
   - Write ビュー名：WRITE_VIEW

22.2.4 SNMPv1，SNMPv2C によるトラップ送信の設定

［設定のポイント］

トラップを発行する SNMP マネージャを登録します。

［コマンドによる設定］

1. **(config)# snmp-server host 128.1.1.2 traps "NETWORK" version 1 snmp**
   SNMP マネージャに標準トラップを発行する設定をします。
   - コミュニティ名：NETWORK
   - SNMP マネージャの IP アドレス：128.1.1.2
   - 発行するトラップ：標準トラップ

22.2.5 SNMPv3 によるトラップ送信の設定

［設定のポイント］

MIB ビューと SNMPv3 セキュリティユーザを設定の上，SNMPv3 セキュリティグループを設定し，さらに SNMP トラップモードを設定します。

［コマンドによる設定］

1. **(config)# snmp-server view "ALL_TRAP_VIEW" * included**
   MIB ビューを設定します。
   - ビュー名 ALL_TRAP_VIEW に全サブツリーを登録します。

2. **(config)# snmp-server user "ADMIN" "ADMIN_GROUP" v3 auth md5 "ABC*_1234" priv des "XYZ/+6789"**
   SNMPv3 セキュリティユーザを設定します。
   - SNMPv3 セキュリティユーザ名：ADMIN
   - SNMPv3 セキュリティグループ名：ADMIN_GROUP
   - 認証プロトコル：HMAC-MD5
   - 認証パスワード：ABC*_1234
   - 暗号化プロトコル：CBC-DES
   - 暗号化パスワード：XYZ/+6789

3. **(config)# snmp-server group "ADMIN_GROUP" v3 priv notify "ALL_TRAP_VIEW"**
   SNMPv3 セキュリティグループを設定します。
   - SNMPv3 セキュリティグループ名：ADMIN_GROUP
   - セキュリティレベル：認証あり，暗号化あり
   - Notify ビュー名：ALL_TRAP_VIEW

4. **(config)# snmp-server host 128.1.1.2 traps "ADMIN" version 3 priv snmp**
   SNMPv3 によって SNMP マネージャに標準トラップを発行する設定をします。
   - SNMPv3 マネージャの IP アドレス：128.1.1.2
   - SNMPv3 セキュリティユーザ名：ADMIN
   - セキュリティレベル：認証あり，暗号化あり
   - 発行するトラップ：標準トラップ

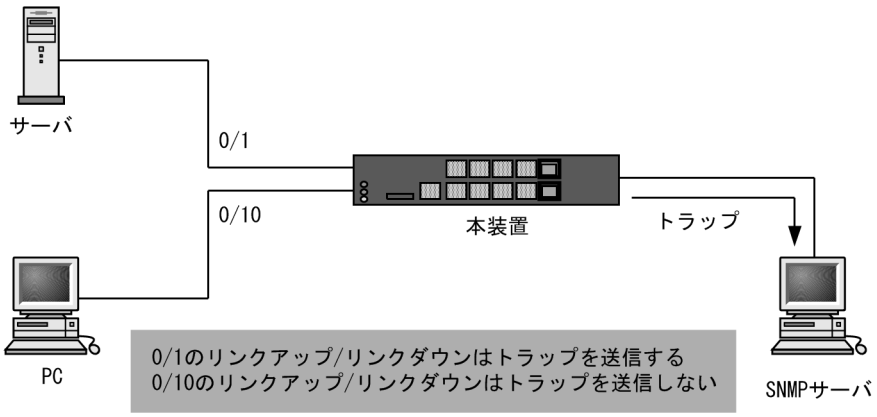
22.2.6　リンクトラップの抑止

本装置は，デフォルト動作としてイーサネットインタフェースがリンクアップまたはリンクダウンしたときに，SNMP トラップを発行します。また，コンフィグレーションによって，イーサネットインタフェースごとに，リンクトラップの送信抑止を設定できます。例えば，サーバと接続する回線のように重要度の高い回線だけトラップを送信し，そのほかの回線のリンクトラップの送信を抑止することで，本装置，ネットワーク，および SNMP マネージャの不要な処理を削減できます。

［設定のポイント］

リンクトラップの設定内容はネットワーク全体の運用方針に従って決定します。

図 22-25　リンクトラップの構成図



ここでは，ポート 0/1 については，トラップを送信するので，コンフィグレーションの設定は必要ありません。ポート 0/10 については，トラップを送信しないように設定します。

［コマンドによる設定］

1. **(config)# interface gigabitethernet 0/10**
   (config-if)# no snmp trap link-status
   (config-if)# exit
   リンクアップ／リンクダウン時にトラップを送信しません。

22.2.7　RMON イーサネットヒストリグループの制御情報の設定

［設定のポイント］

RMON（RFC1757）イーサネットの統計来歴の制御情報を設定します。本コマンドでは最大 32 エントリの設定ができます。あらかじめ SNMP マネージャを登録しておく必要があります。

［コマンドによる設定］

1. **(config)# interface gigabitethernet 0/5**
   ポート 0/5 のインタフェースモードに遷移します。
2. **(config-if)# rmon collection history controlEntry 33 owner "NET-MANAGER" buckets 10**
   (config-if)# exit
   統計来歴の制御情報の情報識別番号，設定者の識別情報，および統計情報を格納する来歴エントリ数を設定します。
   - 情報識別番号：33

- 来歴情報の取得エントリ：10 エントリ
- 設定者の識別情報："NET-MANAGER"

22.2.8 RMON による特定 MIB 値の閾値チェック

［設定のポイント］

特定の MIB の値に対して定期的に閾値チェックを行い，閾値を超えたら SNMP マネージャにイベントを通知するように設定します。
イベント実行方法に trap を指定する場合は，あらかじめ SNMP トラップモードの設定が必要です。

［コマンドによる設定］

1. **(config)# rmon event 3 log trap public**
   アラームが発生したときに実行するイベントを設定します。
   - 情報識別番号：3
   - イベント実行方法：log，trap
   - Trap 送信コミュニティ名：public

2. **(config)# rmon alarm 12 "ifOutDiscards.13" 256111 delta rising-threshold 400000 rising-event-index 3 falling-threshold 100 falling-event-index 3 owner "NET-MANAGER"**
   RMON アラームグループの制御情報を次の条件で設定します。
   - RMON アラームグループの制御情報識別番号：12
   - 閾値チェックを行う MIB のオブジェクト識別子：ifOutDiscards.13
   - 閾値チェックを行う時間間隔：256111 秒
   - 閾値チェック方式：差分値チェック（delta）
   - 上方閾値の値：400000
   - 上方閾値を超えたときのイベント方法の識別番号：3
   - 下方閾値の値：100
   - 下方閾値を超えたときのイベント方法の識別番号：3

   コンフィグレーション設定者の識別情報：NET-MANAGER

22.2.9 SNMP マネージャとの通信の確認

本装置に SNMP エージェント機能を設定して SNMP プロトコルによるネットワーク管理を行う場合，次のことを確認してください。

● ネットワーク上の SNMP マネージャから本装置に対して MIB を取得できること

● 本装置からネットワーク上の SNMP マネージャへ SNMP のトラップが送信されていること

確認手順を次に示します。なお，本装置から取得できる MIB についてはマニュアル「MIB レファレンス 1. サポート MIB の概要」を，本装置から送信されるトラップについてはマニュアル「MIB レファレンス 4.2 サポートトラップ -PDU 内パラメータ」を，それぞれ参照してください。

1. 運用コマンド ping を SNMP マネージャの IP アドレスを指定して実行し，本装置から SNMP マネージャに対して IP 通信ができることを確認してください。通信ができない場合はマニュアル「トラブルシューティングガイド」を参照してください。
2. SNMP マネージャから本装置に対して MIB の取得ができることを確認してください。取得できない場合の対応はマニュアル「トラブルシューティングガイド」を参照してください。

22.3　オペレーション

22.3.1　運用コマンド一覧

SNMP に関する運用コマンド一覧を次の表に示します。

表 22-8　運用コマンド一覧

コマンド名	説明
show snmp engineID local	SNMP エージェントのエンジン ID を表示します。
set snmp-server engineID local	SNMPv3 のエンジン ID やエンジン ID 変更後の起動回数を修復します。

22.3.2　SNMP エージェントのエンジン ID の確認

運用コマンド show snmp engineID local の実行で，SNMP エージェントのエンジン ID を表示します。

図 22-26　show snmp engineID local の実行結果

```
> show snmp engineID local

Date 20XX/05/20 09:18:56 UTC
Local SNMP engineID              : 8000554F043235333073203031323343536373839
Boot count since engineID change : 12

>
```

22.3.3　SNMP エンジン ID の修復手順

コンフィグレーションコマンド snmp-server engineID local が入力された直後，または装置起動時に不慮のリブート（停電など）が発生すると，内蔵フラッシュメモリに記録しているエンジン ID やエンジン ID 変更後の起動回数を壊す可能性があります。

起動時，内蔵フラッシュメモリに記録しているエンジン ID やエンジン ID 変更後の起動回数が壊れていることを検出した場合は次のログを出力します。

- E3 SNMP 04100002 The recorded engineID is damaged.

起動回数の壊れ方によっては認証エラーを多発して，SNMPv3 を使用できなくなる場合があります。

SNMPv3 を使用できなくなった場合は，以下の手順で修復してください。

1. 省電力スケジュールで装置スリープが設定されている場合は，解除します。
2. 本装置と SNMP マネージャとの間の通信経路を，下記のいずれかの手段で遮断します。
   - 本装置と SNMP マネージャ間のケーブルを抜く
   - 運用コマンド inactivate で，該当ポートを停止する
   - 該当 VLAN インタフェースの IP アドレスを削除する
   - 可能なら SNMP マネージャを停止する
3. 運用コマンド show running-config で SNMP 関係の設定を確認し，意図と違うところがあれば訂正して save コマンドで保存します。特にコンフィグレーションコマンド snmp-server engineID local の有無と設定値に注意して確認してください。
4. 本コマンドでエンジン ID と起動回数を設定します。
5. 運用コマンド reload で本装置を再起動した後，SNMP マネージャとの間の通信経路を復旧させます。

（a）運用コマンド set snmp-server engineID local の指定例

コマンド入力形式：set snmp-server engineID local <engineid octet-string> <count>

- エンジン ID を明示的に設定している場合
  <engineid octet-string> 運用コマンド show snmp engineID local で表示したエンジン ID（16 進数表記）
  <count>　　SNMP マネージャが期待している起動回数
- 以前のデフォルトエンジン ID を継承する場合
  <engineid octet-string> SNMP マネージャが期待しているエンジン ID(16 進数表記）
  <count>　　SNMP マネージャが期待している起動回数
- 新規のデフォルトエンジン ID を生成する場合
  <engineid octet-string> ハイフン
  <count>　　0

［注意事項］

1. 本コマンドは不慮に発生した停電などによる悪影響を除去するためのものです。本コマンドを不必要に使用しないでください。本コマンドを不正に使用すると SNMPv3 の動作に支障を来たす可能性があります。
2. 起動回数が上限値 2147483647 に到達すると，SNMP メッセージの認証がすべて失敗するようになります。その場合はコンフィグレーションコマンド snmp-server engineID local で，エンジン ID を変更して起動回数を初期化してください。

23 ログ出力機能

この章では，本装置のログ出力機能について説明します。

23.1 解説

本装置では動作情報や障害情報などを運用メッセージとして通知します。運用メッセージは運用端末に出力するほか，運用ログとして装置内に保存します。この情報で装置の運用状態や障害の発生を管理できます。

運用ログは装置運用中に発生した事象（イベント）を発生順に記録したログ情報です。運用ログとして格納する情報には次に示すものがあります。

- ユーザのコマンド操作と応答メッセージ
- 運用メッセージ

種別ログは装置内で発生した障害や警告についての運用ログ情報をメッセージ ID ごとに分類した上で，同事象が最初に発生した日時および最後に発生した日時と累積回数をまとめた情報です。

これらのログは装置内にテキスト形式で格納されており，運用コマンド show logging で確認できます。

採取した本装置のログ情報は，syslog インタフェースを使用して syslog 機能を持つネットワーク上の他装置（UNIX ワークステーションなど）に送ることができます※1※2。

注 ※1

他装置からの syslog メッセージを受信する機能はサポートしていません。

注 ※2

本装置で生成した syslog メッセージは，HEADER 部を付加して syslog サーバへ出力します。syslog サーバへの出力形式を次の図に示します。

図 23-1 syslog サーバ出力形式

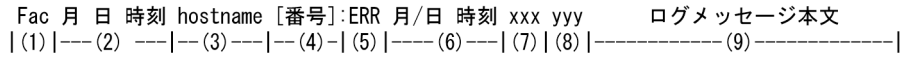


表 23-1 ログ種別ごとの表示有無

番号	項目	ログ種別ごとの表示有無					
		KEY	RSP	EVT	ERR	AUT	WHT
(1)	ファシリティ	○	○	○	○	○	○
(2)	TIMESTAMP （メッセージ生成時刻）	○	○	○	○	○	○
(3)	HOSTNAME （本装置の識別名称）	○	○	○	○	○	○
(4)	機能番号（[1] 固定）	○	○	○	○	○	○
(5)	ログ種別	○	○	○	○	○	○
(6)	事象発生時刻	○	○	○	○	○	○
(7)	イベントレベル	×	×	○	○	×	×
(8)	イベント発生部位	×	×	○	○	○	×
(9)	メッセージ本文	○	○	○	○	○	○

（凡例）○：表示あり　×：表示なし

(1) ファシリティは，コンフィグレーションコマンド logging facility で変更できます。

(2)TIMESTAMP 欄は，RFC3164 規定のフォーマットで付加します。
(3)HOSTNAME 欄は，コンフィグレーションコマンド hostname の設定により下記の文字列を付加します。

- コンフィグレーションコマンド hostname 設定無："AX2500S"
- コンフィグレーションコマンド hostname 設定有：" 設定文字列 "
  ただし，設定文字列に空白文字が含まれていると，"AX2500S" となります。

図内 (5) ～ (8) の詳細については，「メッセージ・ログレファレンス」を参照してください。ただし，図内 (5) で "AUT" を表示するログメッセージはレイヤ 2 認証機能のアカウントログを示し，"WHT" を表示するログメッセージはホワイトリスト機能の未学習パケット情報を示しますので，次の表に示す「運用コマンドレファレンス」の各コマンドを参照してください。

表 23-2　ログ種別 AUT/WHT のログメッセージ本文参照先

ログ種別	該当機能	メッセージ本文参照先
AUT	IEEE802.1X	運用コマンドレファレンス　show dot1x logging
	Web 認証	運用コマンドレファレンス　show web-authentication logging
	MAC 認証	運用コマンドレファレンス　show mac-authentication logging
WHT	ホワイトリスト	運用コマンドレファレンス　show white-list miss-hit

23.1.1　送信遅延処理

syslog 送信は毎秒 30 個ずつのメッセージ送信に制限するため，最大 512 個の送信遅延キューを用意しています。送信遅延キューが溢れた場合は，新しく発生したメッセージを廃棄します。

1. syslog メッセージの TIMESTAMP
   syslog メッセージの TIMESTAMP は，メッセージ生成時の日付と時刻を設定します。
2. 送信遅延中のコンフィグレーション変更
   送信遅延中にコンフィグレーションを変更した場合，syslog メッセージへの適用について次の表に示します。

表 23-3　送信遅延中のコンフィグレーション変更時のメッセージへの適用

コンフィグレーションコマンド	メッセージへの適用時期
logging event-kind logging facility logging trap clock timezone	各メッセージに対して，送信遅延の前に適用します。 コンフィグレーション変更時，遅延キューに滞留しているメッセージには適用しません。 コンフィグレーション変更の結果は，送信遅延時間が経過した後に反映されます。
logging host 設定	設定時に遅延キューに滞留しているメッセージは，新しく登録された syslog サーバへ送信しません。
logging host 削除	削除時に遅延キューに滞留しているメッセージは，削除された syslog サーバへ送信しません。
logging host no-date-info 変更 (UDP 指定)	削除後の再設定と同様です。
logging host no-date-info 変更 (TCP 指定)	送信遅延の後に適用します。 遅延キューに滞留している各メッセージは，過去に遡って変更が適用されたように見えます。

コンフィグレーションコマンド	メッセージへの適用時期
logging tcp trailer	送信遅延の後に適用します。 遅延キューに滞留している各メッセージは，過去に遡って変更が適用されたように見えます。
logging tcp connect delay logging tcp reconnect delay logging tcp notify open logging tcp notify resume	メッセージごとには適用しません。

23.1.2 送信オプション

本装置からの syslog メッセージ送信には次に示すオプション機能があります。

- TCP プロトコルで送信（デフォルトコンフィグレーションは UDP プロトコルで送信）
- 宛先ポート番号を指定（TCP，UDP どちらも指定可能）

本装置は syslog 送信先アドレスを IPv4，IPv6 で指定できますが，TCP 指定は IPv4 アドレスだけ指定できます。

(1) TCP プロトコル送信

syslog メッセージの送信プロトコルに TCP を指定した場合，TCP コネクションはメッセージ送信契機ごとに開設せず，常時接続状態を維持します。

(a) TCP コネクションの接続と切断

- TCP コネクションの開設契機
  装置起動時，コンフィグレーション設定時に TCP コネクション開設要求を行います。
- TCP コネクションの切断契機
  運用コマンド ppupdate，reload の実行による装置再起動時，TCP を選択した syslog サーバのコンフィグレーション削除時を TCP コネクションの切断契機とします。

TCP コネクション開設後に，上記切断契機以外の要因でコネクションが切断された場合は，コネクション開設を要求し接続されるまでリトライします。

TCP コネクションは常時接続状態とし，TCP コネクションが確立していない状態で生じた syslog メッセージは廃棄します。

(b) TCP 送信のメッセージ形式

TCP プロトコルの送信は，メッセージ長を前に格納しておく方式と，区切り文字を付加する方式があり，コンフィグレーションコマンド logging tcp trailer で選択できます。区切り文字は任意の 1 バイト，または CR+LF の 2 バイトを選択できます。

(c) TCP 送信の付加機能

TCP で送信時，次の表に示すコンフィグレーションの設定により syslog メッセージが消失した可能性を宛先 syslog サーバへ通知することができます。

表 23-4　TCP 送信の付加機能

コンフィグレーション コマンド	内容
logging tcp notify open	TCP 接続時に開始メッセージを送信します。 この開始メッセージが予定外のときに表示された場合は，それまで切断されていたことを示しますので，メッセージが消失した可能性があります。
logging tcp notify resume	送信バッファ溢れが解消したときに再開メッセージを送信します。 この再開メッセージが表示された場合は，それまでにメッセージが消失した可能性があります。

コンフィグレーションは装置単位で設定しますが，開始メッセージと再開メッセージは宛先 syslog サーバごとに送信します。
開始メッセージと再開メッセージの形式を次の表に示します。

表 23-5　開始メッセージと再開メッセージの形式

項目	説明
Facility	syslog(5) 変更不可（logging facility コマンドの対象外）
Serverity	notice(5) 変更不可（logging trap コマンドの対象外）
TIMESTAMP	「図 23-1　syslog サーバ出力形式」と同様。（RFC 準拠） 開始メッセージと再開メッセージは他のメッセージを追い越して送信されるため，宛先 syslog サーバで TIMESTAMP が前後して表示されます。
HOSTNAME	「図 23-1　syslog サーバ出力形式」と同様。
機能番号	「図 23-1　syslog サーバ出力形式」と同様。
ログ種別を示す文字列	LOG
メッセージ	開始メッセージ：Connection established. 再開メッセージ：Socket buffer been full.

23.1.3　ログ出力機能使用時の注意事項

（1）syslog メッセージの送信頻度

syslog メッセージの送信頻度は，syslog サーバごとに毎秒 30 パケットです。また，syslog メッセージの送信遅延時間（約 1000 ミリ秒）の誤差は最大 50 ミリ秒です。

（2）スタック構成でのマスタ交代時

スタック構成でメンバスイッチがマスタスイッチに遷移した直後，syslog サーバへ IP パケットの送信が一時的にできない状態となるため，syslog サーバへのメッセージは syslog サーバに届きません。

スイッチ状態遷移時のログ情報は，運用コマンド show logging で確認してください。

（3）TCP 送信オプション

（a）TCP 送信の使用について

TCP は全メッセージの到達を保証するものではありません。送信バッファ溢れや送信タイムアウトが発生した場合は，syslog メッセージを廃棄します。また，送信遅延キュー溢れが発生した場合も，syslog メッセージを廃棄します。

(b) TCP コネクションの接続

TCP コネクションの接続処理は VLAN のアップと同期しません。本装置に複数の IP アドレスが設定されている場合，宛先 syslog サーバへの通信経路が存在する VLAN がダウンしている間に TCP 接続処理を開始し，TCP 接続の再送信中に目的の VLAN がアップした場合は，TCP パケットの送信元 IP アドレスが意図しない IP アドレスになる可能性があります。

また，TCP 未接続の間に発生した syslog メッセージは廃棄しますので，装置起動直後や宛先 syslog サーバへの通信経路のアップ直後に発生した syslog メッセージは廃棄する可能性が高くなります。

(c) TCP コネクションの切断

TCP プロトコルを指定した syslog サーバを設定している場合，装置再起動処理（運用コマンド reload など）は，syslog 送信キューが空になって TCP コネクションが切断されるまで待機します。この間はコンソールや Telnet からのコマンド入力は完了待ち状態となります。

(d) TCP コネクション管理の運用ログ

syslog サーバ宛の TCP コネクションの状態変化（接続，切断）は運用ログに出力します。ただし，通信状態が不安定になった場合，TCP コネクション管理のログが連続して発生し，他の重要な運用ログが消失する可能があります。

(e) 他機能との併用について

本機能で TCP 送信を使用する場合，HTTP サーバを使用する以下の機能は併用できません。

- Web 認証
- OAN

23.2　コンフィグレーション

23.2.1　コンフィグレーションコマンド一覧

ログ出力機能に関するコンフィグレーションコマンド一覧を次の表に示します。

表 23-6　コンフィグレーションコマンド一覧（syslog 出力に関する設定）

コマンド名	説明
logging event-kind	syslog サーバに送信対象とするログ情報のイベント種別を設定します。
logging facility	ログ情報を syslog インタフェースで出力するためのファシリティを設定します。
logging host	ログ情報の出力先を設定します。
logging syslog-dump	no logging syslog-dump 設定時，装置で発生したログを内蔵フラッシュメモリに格納しません。
logging tcp connect delay	装置起動時，コンフィグレーション展開から TCP で接続開始するまでの時間を指定します。
logging tcp notify open	TCP 接続したとき，開始メッセージを送信します。
logging tcp notify resume	TCP 送信バッファ溢れが解消したときに再開メッセージを送信します。
logging tcp reconnect delay	TCP の接続開始までの時間を指定します。
logging tcp trailer	TCP 送信の syslog メッセージの区切り文字を指定します。
logging trap	syslog サーバに送信対象とするログ情報の重要度を設定します。

23.2.2　ログの syslog 出力の設定

［設定のポイント］

syslog 出力機能を使用して，採取したログ情報を syslog サーバに送信するための設定をします。

［コマンドによる設定］

1. **(config)# logging host 192.168.101.254**
   ログを IP アドレス 192.168.101.254 宛てに出力するように設定します。

23.2.3　TCP 送信の設定

［設定のポイント］

syslog 出力機能を使用して，採取したログ情報を syslog サーバへ TCP で送信するための設定をします。

- syslog メッセージの区切り文字に CR+LF を設定
- TCP の付加機能（開始メッセージ・再開メッセージ送信）を設定

［コマンドによる設定］

1. **(config)# logging host 192.168.101.254 tcp**
   ログを IP アドレス 192.168.101.254 宛て TCP に出力するように設定します。（ポート番号未指定の場合は "514" で動作します。）

2. **(config)# logging tcp trailer crlf**

TCP で送信する syslog メッセージの区切り文字に CR+LF を設定します。

3. **(config)# logging tcp notfity open**
   TCP 接続時に開始メッセージを送信するよう設定します。

4. **(config)# logging tcp notify resume**
   TCP の送信バッファ溢れが解消したときに再開メッセージを送信するよう設定します。

23.3　オペレーション

23.3.1　運用コマンド一覧

ログ出力機能に関する運用コマンドコマンド一覧を次の表に示します。

表 23-7　運用コマンド一覧（syslog 出力に関するオペレーション）

コマンド名	説明
show logging host	syslog 機能の統計情報を表示します。
clear logging host statistics	syslog 機能の統計情報を 0 クリアします。

23.3.2　syslog 機能の統計情報の確認

本装置の syslog 機能の統計情報は運用コマンド show logging host により確認できます。
送信遅延キュー溢れによって廃棄したメッセージ数，送信遅延キューに滞留しているメッセージ数，送信メッセージ数を確認できます。
また，TCP 送信オプションを指定時は，TCP 未接続のために廃棄したメッセージ数などを確認できます。

図 23-2　syslog 機能の統計情報表示例

```
> show logging host

Date 20XX/06/06 20:42:17 UTC
Discard message :          0
Queued message  :          1
Send message    :        525
Host : 172.22.200.1  TCP  Port 65535
  Discard message (not connect) :        156
  Discard message (overflow)    :          0
  Connection status             : Connect (Since 20XX/06/06 20:42:05)
  Connection cycles             :         19
Host : 172.22.200.2  TCP  Port 1
  Discard message (not connect) :        357
  Discard message (overflow)    :          0
  Connection status             : Connect (Since 20XX/06/06 20:42:05)
  Connection cycles             :         41
Host : 172.22.200.3  TCP  Port 514
  Discard message (not connect) :        357
  Discard message (overflow)    :          0
  Connection status             : Connect (Since 20XX/06/06 20:42:05)
  Connection cycles             :         41
Host : 172.22.200.5  TCP  Port 514
  Discard message (not connect) :        357
  Discard message (overflow)    :          0
  Connection status             : Connect (Since 20XX/06/06 20:42:05)
  Connection cycles             :         41

>
```

24 sFlow 統計（フロー統計）機能

この章では，本装置を中継するパケットのトラフィック特性を分析する機能である sFlow 統計の解説と操作方法について説明します。

24.1　解説

24.1.1　sFlow 統計の概要

sFlow 統計はエンドーエンドのトラフィック（フロー）特性や隣接するネットワーク単位のトラフィック特性を分析するため，ネットワーク上を流れるトラフィックを中継装置（ルータやスイッチ）でモニタする機能です。sFlow 統計は国際的に公開されているフロー統計プロトコル（RFC3176）で，レイヤ 2 からレイヤ 7 までの統計情報をサポートしています。sFlow 統計情報（以降，sFlow パケット）を受け取って表示する装置を sFlow コレクタ（以降，コレクタ）と呼び，コレクタに sFlow パケットを送付する装置を sFlow エージェント（以降，エージェント）と呼びます。sFlow 統計を使ったネットワーク構成例を次の図に示します。

図 24-1　sFlow 統計のネットワーク構成例

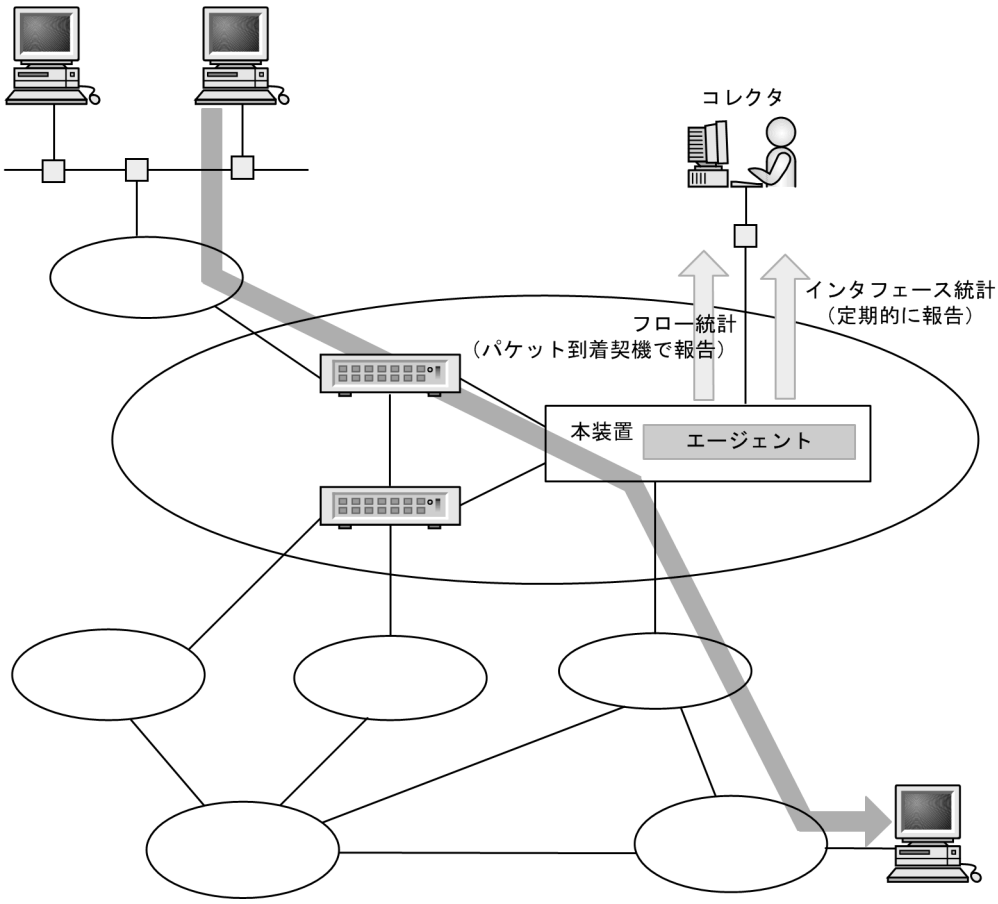
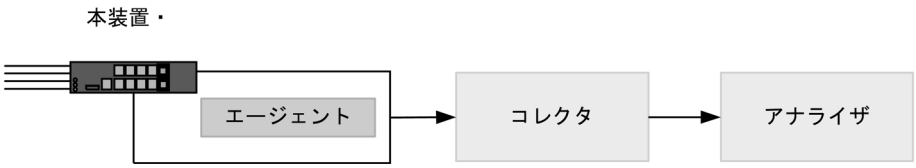


図 24-2　システム構成



本装置のエージェントでモニタされた情報はコレクタに集められ，統計結果をアナライザによってグラフィカルに表示できます。従って，sFlow 統計機能を利用するにはコレクタとアナライザが必要です。

表 24-1　システム構成要素

構成要素	役割
エージェント（本装置）	統計情報を収集してコレクタに送付します。
コレクタ※	エージェントから送付される統計情報を集計・編集・表示します。さらに，編集データをアナライザに送付します。
アナライザ	コレクタから送付されるデータをグラフィカルに表示します。

注※
　アナライザと一緒になっている場合もあります。

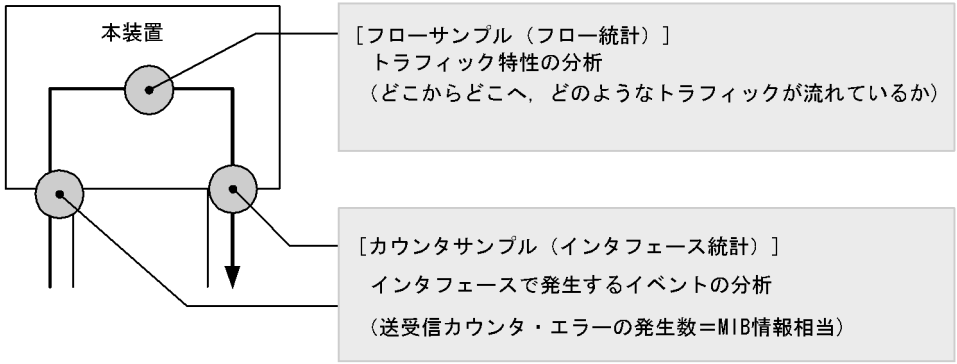
24.1.2　sFlow 統計エージェント機能

本装置のエージェントには，次の二つの機能があります。

- フロー統計（sFlow 統計ではフローサンプルと呼びます。以降，この名称で表記します。）作成機能
- インタフェース統計（sFlow 統計ではカウンタサンプルと呼びます。以降，この名称で表記します。）作成機能

フローサンプル作成機能は送受信パケット（フレーム）をユーザ指定の割合でサンプリングし，パケット情報を加工してフローサンプル形式でコレクタに送信する機能です。カウンタサンプル作成機能はインタフェース統計をカウンタサンプル形式でコレクタに送信する機能です。それぞれの収集箇所と収集内容を次の図に示します。

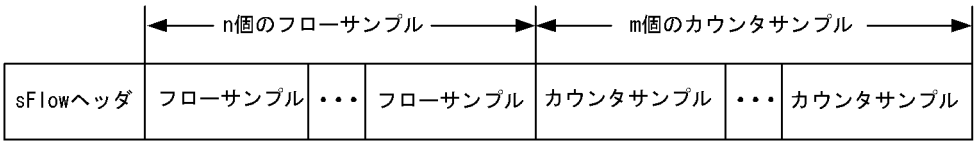
図 24-3　フローサンプルとカウンタサンプル



24.1.3　sFlow パケットフォーマット

本装置がコレクタに送信する sFlow パケット（フローサンプルとカウンタサンプル）について説明します。コレクタに送信するフォーマットは RFC3176 で規定されています。sFlow パケットのフォーマットを次の図に示します。

図 24-4　sFlow パケットフォーマット



（1） sFlow ヘッダ

sFlow ヘッダへ設定される内容を次の表に示します。

表 24-2　sFlow ヘッダのフォーマット

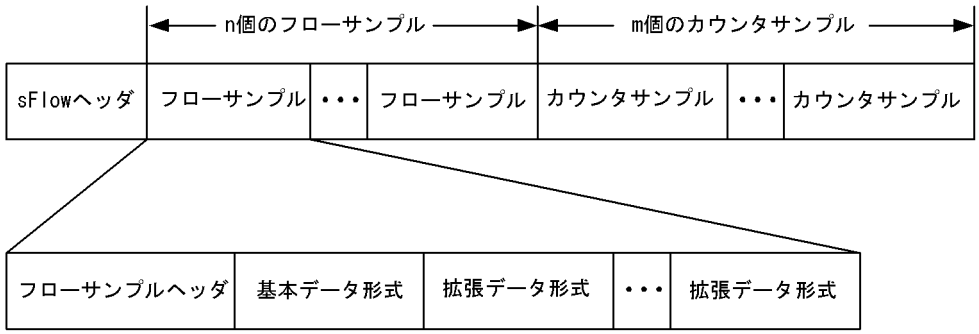
設定項目	説明	サポート
バージョン番号	sFlow パケットのバージョン（バージョン 2，4 をサポート）	○
アドレスタイプ	エージェントの IP タイプ（IPv4=1，IPv6=2）	○
エージェント IP アドレス	エージェントの IP アドレス	○
シーケンス番号	sFlow パケットの生成ごとに増加する番号	○
生成時刻	現在の時間（装置の起動時からのミリセカンド）	○
サンプル数	この信号に含まれるサンプリング（フロー・カウンタ）したパケット数 （「図 24-4　sFlow パケットフォーマット」の例では n+m が設定されます。）	○

（凡例）
　○：サポートする

（2） フローサンプル

フローサンプルとは，本装置が送受信（中継）したパケットの中から一定のサンプリング間隔でパケットを抽出し，コレクタに送信するためのフォーマットです。フローサンプルにはモニタしたパケットに加えて，パケットには含まれていない情報（受信インタフェースなど）も収集するため，詳細なネットワーク監視ができます。フローサンプルのフォーマットを次の図に示します。

図 24-5　フローサンプルのフォーマット



（a） フローサンプルヘッダ

フローサンプルヘッダへ設定する内容を次の表に示します。

表 24-3　フローサンプルヘッダのフォーマット

設定項目	説明	サポート
sequence_number	フローサンプルの生成ごとに増加する番号	○
source_id	フローサンプルの装置内の発生源（受信インタフェース）を表す SNMP Interface Index	○
sampling_rate	フローサンプルのサンプリング間隔	○
sample_pool	インタフェースに到着したパケットの総数	○ ※1
drops	廃棄したフローサンプルの総数	○

設定項目	説明	サポート
input	受信インタフェースの SNMP Interface Index 受信インタフェースが不明な場合は 0 を設定	○
output	送信インタフェースの SNMP Interface Index※2 送信インタフェースが不明な場合は 0 を設定	×

（凡例）
○：サポートする，×：サポートしない

注 ※1
概数です。

注 ※2
本装置では output をサポートしていないため 0 固定です。

（b） 基本データ形式

基本データ形式はヘッダ型，IPv4 型および IPv6 型の 3 種類があり，このうち一つだけ設定できます。基本データ形式のデフォルトコンフィグレーションはヘッダ型です。IPv4 型，IPv6 型を使用したい場合はコンフィグレーションコマンドで設定してください。各形式のフォーマットを以降の表に示します。

表 24-4　ヘッダ型のフォーマット

設定項目	説明	サポート
packet_information_type	基本データ形式のタイプ（ヘッダ型＝ 1）	○
header_protocol	ヘッダプロトコル番号（ETHERNET=1）	○
frame_length	オリジナルのパケット長	○
header_length	オリジナルからサンプリングした分のパケット長（デフォルトコンフィグレーションは 128）	○
header<>	サンプリングしたパケットの内容	○

（凡例）
○：サポートする

注　IP パケットとして解析できない場合には，本フォーマットになります。

表 24-5　IPv4 型のフォーマット

設定項目	説明	サポート
packet_information_type	基本データ形式のタイプ（IPv4 型＝ 2）	○
length	IPv4 パケットの長さ	○
protocol	IP プロトコルタイプ（例：TCP=6，UDP=17）	○
src_ip	送信元 IP アドレス	○
dst_ip	宛先 IP アドレス	○
src_port	送信元ポート番号	○
dst_port	宛先ポート番号	○
tcp_flags	TCP フラグ	○
TOS	IP のタイプオブサービス	○

（凡例）
○：サポートする

表 24-6 IPv6 型のフォーマット

設定項目	説明	サポート
packet_information_type	基本データ形式のタイプ（IPv6 型＝ 3）	○
length	低レイヤを除いた IPv6 パケットの長さ	○
protocol	IP プロトコルタイプ（例：TCP=6，UDP=17）	○
src_ip	送信元 IP アドレス	○
dst_ip	宛先 IP アドレス	○
src_port	送信元ポート番号	○
dst_port	宛先ポート番号	○
tcp_flags	TCP フラグ	○
priority	優先度	○

（凡例）
○：サポートする

(c) 拡張データ形式

拡張データ形式はスイッチ型・ルータ型・ゲートウェイ型・ユーザ型・URL 型の 5 種類があります。拡張データ形式のデフォルトコンフィグレーションではすべての拡張形式を収集し，コレクタに送信します。本形式はコンフィグレーションにより変更可能です。各形式のフォーマットを以降の表に示します。

表 24-7 拡張データ形式の種別一覧

設定項目	説明	サポート
スイッチ型	スイッチ情報（VLAN 情報など）を収集する	○
ルータ型	ルータ情報を収集する	×
ゲートウェイ型	ゲートウェイ情報を収集する	×
ユーザ型	ユーザ情報を収集する	○※1
URL 型	URL 情報を収集する	○※2

（凡例）
○：サポートする　×：サポートしない

注 ※1
本装置では RADIUS 認証要求パケットのユーザ名だけを収集します。

注 ※2
本装置では HTTP 要求パケットの URI だけを収集します。

表 24-8 スイッチ型のフォーマット

設定項目	説明	サポート
extended_information_type	拡張データ形式のタイプ（スイッチ型 =1）	○
src_vlan	受信パケットの 802.1Q VLAN ID	○
src_priority	受信パケットの 802.1p 優先度	○
dst_vlan	送信パケットの 802.1Q VLAN ID	×※
dst_priority	送信パケットの 802.1p 優先度	×※

（凡例）
○：サポートする　×：サポートしない

注 ※　未サポートのため 0 固定です。

表 24-9　ルータ型のフォーマット

設定項目	説明	サポート
extended_information_type	拡張データ形式のタイプ（ルータ型 =2）	×
nexthop_address_type	次の転送先ルータの IP アドレスタイプ	×
nexthop	次の転送先ルータの IP アドレス	×
src_mask	送信元アドレスのプレフィックスマスクビット	×
dst_mask	宛先アドレスのプレフィックスマスクビット	×

（凡例）
×：サポートしない

表 24-10　ゲートウェイ型のフォーマット

設定項目	説明	サポート
extended_information_type	拡張データ形式のタイプ（ゲートウェイ型 =3）	×
as	本装置の AS 番号	×
src_as	送信元の AS 番号	×
src_peer_as	送信元への隣接 AS 番号	×
dst_as_path_len	AS 情報数（1 固定）	×
dst_as_type	AS 経路種別（2：AS_SEQUENCE）	×
dst_as_len	AS 数（2 固定）	×
dst_peer_as	宛先への隣接 AS 番号	×
dst_as	宛先の AS 番号	×
communities<>	本経路に関するコミュニティ	×
localpref	本経路に関するローカル優先	×

（凡例）
×：サポートしない

表 24-11　ユーザ型のフォーマット

設定項目	説明	サポート
extended_information_type	拡張データ形式のタイプ（ユーザ型 =4）	○
src_user_len	送信元のユーザ名の長さ	○
src_user<>	送信元のユーザ名	○
dst_user_len	宛先のユーザ名の長さ ※	×
dst_user<>	宛先のユーザ名 ※	×

（凡例）
○：サポートする　×：サポートしない

注 ※　未サポートのため 0 固定です。

表 24-12 URL 型のフォーマット

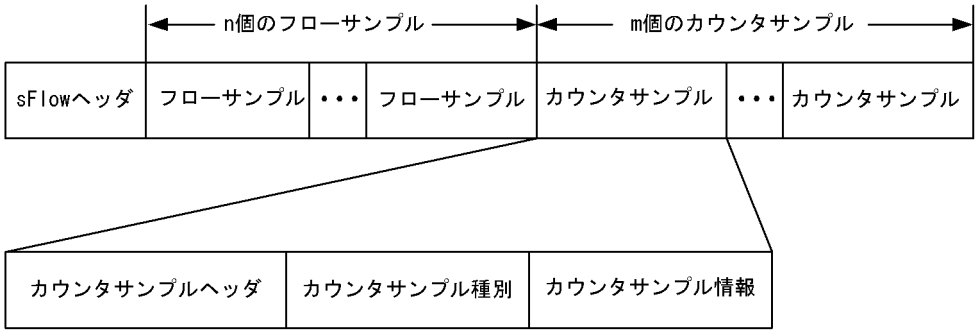
設定項目	説明	サポート
extended_information_type	拡張データ形式のタイプ（URL 型 =5）	○
url_direction	URL 情報源（source address=1，destination address=2）	○
url_len	URL 長	○
url<>	URL 内容	○

（凡例）
○：サポートする

(3) カウンタサンプル

カウンタサンプルは，インタフェース統計情報（到着したパケット数や，エラーの数など）を送信します。また，インタフェースの種別によりコレクタに送信するフォーマットが決定されます。カウンタサンプルのフォーマットを次の図に示します。

図 24-6 カウンタサンプルのフォーマット



(a) カウンタサンプルヘッダ

カウンタサンプルヘッダへ設定される内容を次の表に示します。

表 24-13 カウンタサンプルヘッダのフォーマット

設定項目	説明	サポート
sequence_number	カウンタサンプルの生成ごとに増加する番号	○
source_id	カウンタサンプルの装置内の発生源（特定のポート）を表す SNMP Interface Index	○
sampling_interval	コレクタへのカウンタサンプルの送信間隔	○

（凡例）
○：サポートする

(b) カウンタサンプル種別

カウンタサンプル種別はインタフェースの種別ごとに分類され収集されます。カウンタサンプル種別として設定される内容を次の表に示します。

表 24-14 カウンタサンプル種別一覧

設定項目	説明	サポート
GENERIC	一般的な統計（counters_type=1）	×※1
ETHERNET	イーサネット統計（counters_type=2）	○
TOKENRING	トークンリング統計（counters_type=3）	×※1
FDDI	FDDI 統計（counters_type=4）	×※1
100BaseVG	VG 統計（counters_type=5）	×※1
WAN	WAN 統計（counters_type=6）	×※1
VLAN	VLAN 統計（counters_type=7）	×※2

（凡例）
○：サポートする　×：サポートしない

注 ※1　本装置で未サポートのインタフェースタイプです。

注 ※2　本装置では VLAN 統計はサポートしていません。

(c) カウンタサンプル情報

カウンタサンプル情報はカウンタサンプル種別により収集される内容が変わります。カウンタサンプル情報として設定される内容を次の表に示します。

表 24-15 カウンタサンプル情報

設定項目	説明	サポート
GENERIC	一般的な統計	×
ETHERNET	イーサネット統計 [RFC2233，2358，3176 参照]	○※
TOKENRING	トークンリング統計	×
FDDI	FDDI 統計	×
100BaseVG	VG 統計	×
WAN	WAN 統計	×
VLAN	VLAN 統計	×

（凡例）
○：サポートする　×：サポートしない

注 ※
項目ごとのサポートは「MIB レファレンス」を参照してください。ifDirection，dot3StatsSymbolErrors は収集できません。

24.1.4 本装置でのフロー統計の動作について

(1) フロー統計収集の対象パケットに関する注意点

1. 本装置でのフロー統計は，受信パケットと送信パケットを対象パケットとして扱います。なお，装置としては受信パケット（sflow forward ingress），送信パケット（sflow forward egress）のどちらかしか指定できません。
2. ソフトウェア中継パケットや自発パケット，自宛パケットはフロー統計収集の対象外パケットとして扱います。（サンプリング間隔の計算には反映されます。）
   以下のパケットは自宛扱いとなりません。

- ARP 要求パケット（宛先 MAC アドレスがブロードキャストのパケット）
- NDP 要求パケット（宛先 MAC アドレスがマルチキャストのパケット）
- URL リダイレクト対象パケット

3. ポートミラーリングのミラーポートからの送信パケットは，フロー統計収集の対象外パケットとして扱います。
4. 2 段以上の VLAN Tag があるパケットは，フロー統計収集の対象外パケットとして扱います。
5. VLAN トンネリング機能と sFlow 統計機能を併用したとき，トンネリングポートの VLAN Tag があるパケット（トランクポートで 2 段以上の VLAN Tag があるパケット）は，フロー統計収集の対象パケットにならない場合があります。

（2） データ収集位置による注意点

1. ingress 指定および egress 指定のどちらで検出されても，フローサンプルの内容は本装置に入ってきた時点のパケット内容が収集されます。（本装置内でパケット内容の変換などが行なわれても，フローサンプルには反映されません。）
2. フィルタ機能と併用するときは，パケットが廃棄される条件を確認して運用してください。パケット廃棄位置とフロー統計データ収集位置によるフロー統計収集動作を次の表に示します。

表 24-16　パケット廃棄位置とフロー統計データ収集位置によるフロー統計収集動作

パケット廃棄位置	フロー統計データ収集位置とフロー統計収集動作	
	sflow forward ingress	sflow forward egress
フィルタ機能：受信側 • ip access-group in • ipv6 traffic-filter in • mac access-group in	廃棄対象でも収集される	廃棄対象は収集されない
フィルタ機能：送信側 • ip access-group out • ipv6 traffic-filter out • mac access-group out	廃棄対象でも収集される	廃棄対象でも収集される

24.2 コンフィグレーション

24.2.1 コンフィグレーションコマンド一覧

sFlow 統計で使用するコンフィグレーションコマンド一覧を次の表に示します。

表 24-17 コンフィグレーションコマンド一覧

コマンド名	説明
sflow destination	sFlow パケットの宛先であるコレクタの IP アドレスを指定します。
sflow extended-information-type	フローサンプルの各拡張データ形式の送信有無を指定します。
sflow forward egress	指定したポートの送信トラフィックを sFlow 統計の監視対象にします。
sflow forward ingress	指定したポートの受信トラフィックを sFlow 統計の監視対象にします。
sflow max-header-size	基本データ形式（sflow packet-information-type コマンド参照）にヘッダ型を使用している場合，サンプルパケットの先頭からコピーされる最大サイズを指定します。
sflow max-packet-size	sFlow パケットのサイズを指定します。
sflow packet-information-type	フローサンプルの基本データ形式を指定します。
sflow polling-interval	カウンタサンプルをコレクタへ送信する間隔を指定します。
sflow sample	装置全体に適用するサンプリング間隔を指定します。
sflow source	sFlow パケットの送信元（エージェント）に設定される IP アドレスを指定します。
sflow url-port-add	拡張データ形式で URL 情報を使用する場合に，HTTP パケットと判断するポート番号を 80 以外に追加指定します。
sflow version	送信する sFlow パケットのバージョンを設定します。

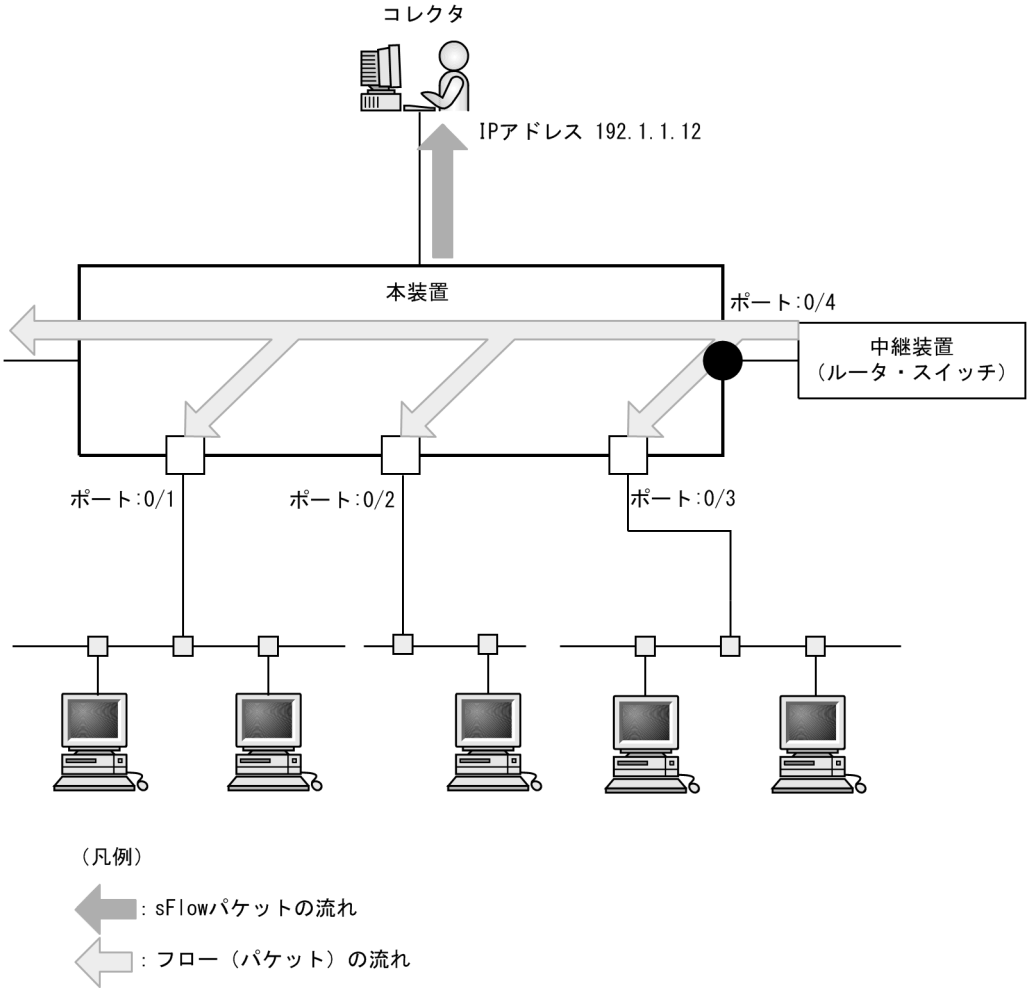
24.2.2 sFlow 統計の基本的な設定

(1) 受信パケットをモニタする設定

[設定のポイント]

sFlow 統計のコンフィグレーションは装置全体で有効な設定と，実際に運用するポートを指定する設定の二つが必要です。ここでは，ポート 0/4 に対して入ってくるパケットをモニタする設定を示します。

図 24-7　ポート 0/4 の受信パケットをモニタする設定例



［コマンドによる設定］

1. **(config)# sflow destination 192.1.1.12**
   コレクタとして IP アドレス 192.1.1.12 を設定します。

2. **(config)# sflow sample 512**
   512 パケットごとにトラフィックをモニタします。

3. **(config)# interface gigabitethernet 0/4**
   ポート 0/4 のイーサネットインタフェースコンフィグレーションモードに移行します。

4. **(config-if)# sflow forward ingress**
   (config-if)# exit
   ポート 0/4 の受信パケットに対して sFlow 統計機能を有効にします。

［注意事項］

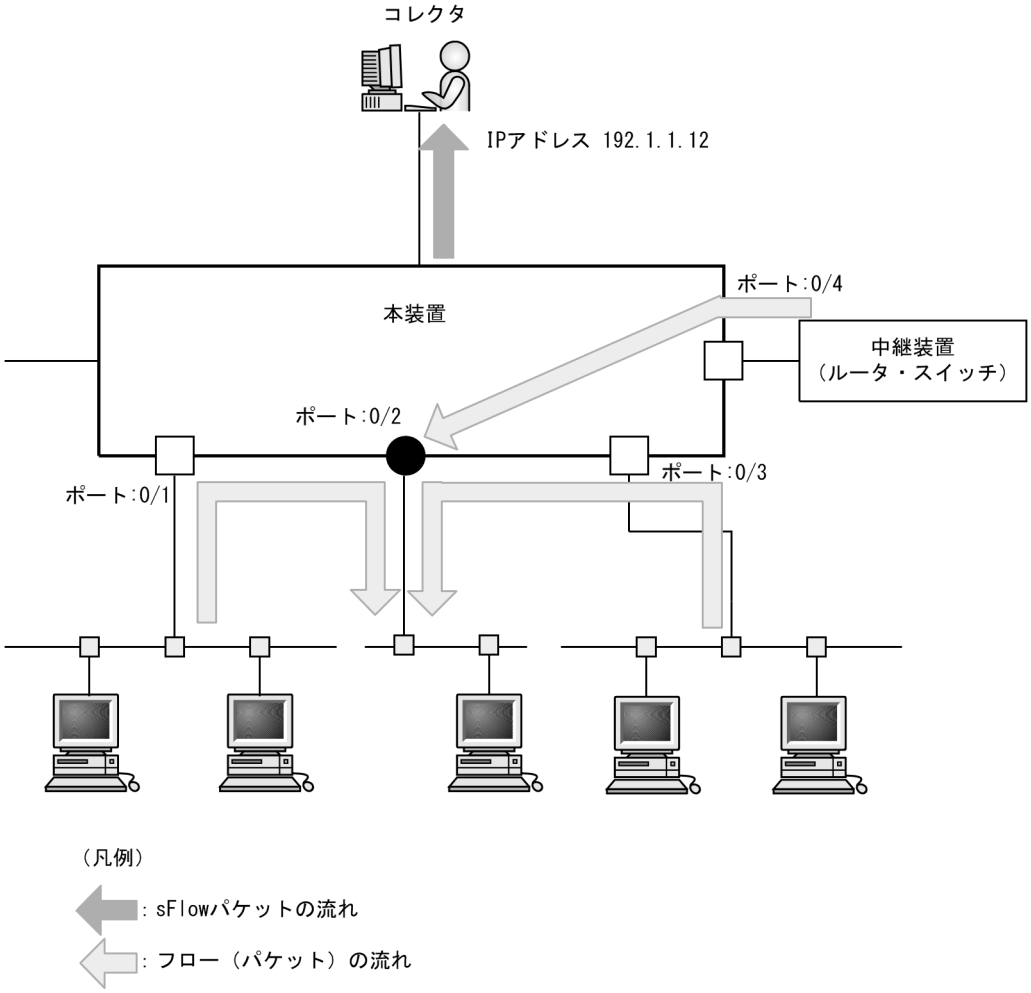
コンフィグレーションコマンド sflow sample で設定するサンプリング間隔については，インタフェースの回線速度を考慮して決める必要があります。詳細は「コンフィグレーションコマンドレファレンス　sflow sample」を参照してください。

(2) 送信パケットをモニタする設定

［設定のポイント］

sFlow 統計機能を，受信パケットまたは送信パケットのどちらに対して有効にするかは，インタフェースコンフィグレーションモードで設定するときに，コンフィグレーションコマンド sflow forward ingress または sflow forward egress のどちらを指定するかによって決まります。ここでは，ポート 0/2 から出て行くパケットをモニタする設定を示します。

図 24-8 ポート 0/2 の送信パケットをモニタする設定例



［コマンドによる設定］

1. **(config)# sflow destination 192.1.1.12**
   コレクタとして IP アドレス 192.1.1.12 を設定します。

2. **(config)# sflow sample 512**
   512 パケットごとにトラフィックをモニタします。

3. **(config)# interface gigabitethernet 0/2**
   ポート 0/2 のイーサネットインタフェースコンフィグレーションモードに移行します。

4. **(config-if)# sflow forward egress**

(config-if)# exit
ポート 0/2 の送信パケットに対して sFlow 統計機能を有効にします。

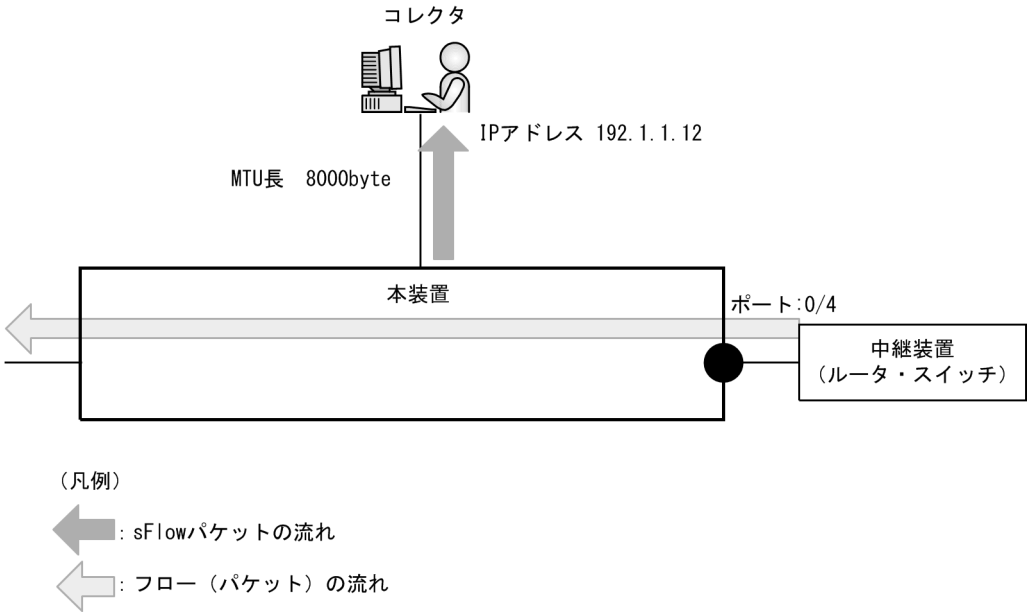
24.2.3 sFlow 統計コンフィグレーションパラメータの設定例

（1） MTU 長と sFlow パケットサイズの調整

［設定のポイント］

sFlow パケットはデフォルトコンフィグレーションでは 1400byte 以下のサイズでコレクタに送信されます。コレクタへの回線の MTU 値が大きい場合，同じ値に調整することでコレクタに対して効率よく送信できます。ここでは MTU 長が 8000byte の回線とコレクタが繋がっている設定を記述します。

図 24-9 コレクタへの送信を MTU=8000byte に設定する例



［コマンドによる設定］

1. **(config)# sflow destination 192.1.1.12**
コレクタとして IP アドレス 192.1.1.12 を設定します。

2. **(config)# sflow sample 32**
32 パケットごとにトラフィックをモニタします。

3. **(config)# sflow max-packet-size 8000**
sflow パケットサイズの最大値を 8000byte に設定します。

4. **(config)# interface gigabitethernet 0/4**
ポート 0/4 のイーサネットインタフェースコンフィグレーションモードに移行します。

5. **(config-if)# sflow forward ingress**
(config-if)# exit

ポート 0/4 の受信パケットに対して sFlow 統計機能を有効にします。

（2） 収集したい情報を絞る

［設定のポイント］

sFlow パケットの情報はコンフィグレーションを指定しないとすべて収集する条件になっています。しかし，不要な情報がある場合に，その情報を取らない設定をすることで CPU 使用率を下げることができます。ここではスイッチ情報だけが必要な場合の設定を記述します。

［コマンドによる設定］

1. **(config)# sflow destination 192.1.1.12**
   コレクタとして IP アドレス 192.1.1.12 を設定します。

2. **(config)# sflow sample 512**
   512 パケットごとにトラフィックをモニタします。

3. **(config)# sflow extended-information-type switch**
   フローサンプルの拡張データ形式に「スイッチ」を設定します。（スイッチ情報だけが取得できます。）

4. **(config)# interface gigabitethernet 0/4**
   ポート 0/4 のイーサネットインタフェースコンフィグレーションモードに移行します。

5. **(config-if)# sflow forward ingress**
   (config-if)# exit
   ポート 0/4 の受信パケットに対して sFlow 統計機能を有効にします。

（3） sFlow パケットのエージェント IP アドレスを固定化する

［設定のポイント］

一般的なコレクタは，sFlow パケットに含まれるエージェント IP アドレスの値を基にして同一の装置かどうかを判断しています。この理由から，コンフィグレーションコマンド sflow source でエージェント IP アドレスを設定していない場合，コレクタ側で複数装置から届いているように表示されるおそれがあります。長期的に情報を見る場合はエージェント IP アドレスを固定化してください。

［コマンドによる設定］

1. **(config)# sflow source 192.168.1.254**
   エージェントアドレスに IPv4 用として 192.168.1.254 を設定します。

2. **(config)# sflow source 2001:200::fffe**
   エージェントアドレスに IPv6 用として 2001:200::fffe を設定します。

3. **(config)# sflow sample 512**
   512 パケットごとにトラフィックをモニタします。

4. **(config)# interface gigabitethernet 0/4**
   ポート 0/4 のイーサネットインタフェースコンフィグレーションモードに移行します。

5. **(config-if)# sflow forward ingress**
   (config-if)# exit
   ポート 0/4 の受信パケットに対して sFlow 統計機能を有効にします。

(4) ローカルネットワーク環境での URL 情報収集

[設定のポイント]

本装置では sFlow 統計で URL 情報（HTTP パケット）を収集する場合，デフォルトコンフィグレーションでは宛先のポート番号として 80 番を利用しているネットワーク環境になっています。しかし，ローカルネットワーク環境ではポート番号が異なる場合があります。ローカルネットワーク環境で HTTP パケットのポート番号として 8080 番を利用している場合の設定を示します。

[コマンドによる設定]

1. **(config)# sflow destination 192.1.1.12**
   コレクタとして IP アドレス 192.1.1.12 を設定します。

2. **(config)# sflow sample 512**
   512 パケットごとにトラフィックをモニタします。

3. **(config)# sflow url-port-add 8080**
   拡張データ形式で URL 情報を使用する場合に，HTTP パケットと判断する宛先ポート番号 8080 を追加で設定します。

4. **(config)# interface gigabitethernet 0/4**
   ポート 0/4 のイーサネットインタフェースコンフィグレーションモードに移行します。

5. **(config-if)# sflow forward ingress**
   (config-if)# exit
   ポート 0/4 の受信パケットに対して sFlow 統計機能を有効にします。

[注意事項]

本パラメータを設定した後でも，HTTP パケットの対象として宛先ポート番号 80 番は有効です。

24.3 オペレーション

24.3.1 運用コマンド一覧

sFlow 統計で使用する運用コマンド一覧を次の表に示します。

表 24-18 運用コマンド一覧

コマンド名	説明
show sflow	sFlow 統計機能についての設定条件と動作状況を表示します。
clear sflow statistics	sFlow 統計で管理している統計情報をクリアします。

24.3.2 コレクタとの通信の確認

本装置で sFlow 統計機能を設定してコレクタに送信する場合，次のことを確認してください。

（1） コレクタとの疎通確認

運用コマンド ping をコレクタの IP アドレスを指定して実行し，本装置からコレクタに対して IP 通信ができることを確認してください。通信ができない場合は，「トラブルシューティングガイド」を参照してください。

（2） sFlow パケット通信確認

コレクタ側で sFlow パケットを受信していることを確認してください。受信していない場合の対応は，「トラブルシューティングガイド」を参照してください。

24.3.3 sFlow 統計機能の運用中の確認

本装置で sFlow 統計機能を使用した場合，運用中の確認内容には次のものがあります。

（1） sFlow パケット廃棄数の確認

運用コマンド show sflow を実行して sFlow 統計情報を表示し，sFlow 統計機能で Dropped sFlow samples（廃棄しているパケット数）や Overflow Time of sFlow Queue（廃棄パケット時間）を確認してください。どちらかの値が増加する場合は，増加しないサンプリング間隔を設定してください。

図 24-10 運用コマンド show sflow の実行結果

```
> show sflow

Date 20XX/05/26 01:37:12 UTC
sFlow service status: enable
Progress time from sFlow statistics cleared: 17:13:01
sFlow agent data :
 sFlow service version: 4
 CounterSample interval rate: 60 seconds
 Default configured rate: 1 per 2048 packets
 Default actual rate    : 1 per 2048 packets
 Configured sFlow ingress ports: 0/2-4
 Configured sFlow egress ports : ----
 Received sFlow samples:       1043  Dropped sFlow samples        :          0
 Exported sFlow samples:       1043  Couldn't export sFlow samples:          0
 Overflow time of sFlow queue: 0 seconds                                  …1
sFlow collector data :
 Collector IP address: 192.168.1.100  UDP: 6343  Source IP address: 192.168.1.25
3
```

```
  Send FlowSample UDP packets   :       1043  Send failed packets:          0
  Send CounterSample UDP packets:        372  Send failed packets:          0
 Collector IP address: 192.168.1.101  UDP: 6343  Source IP address: 192.168.1.25
3
  Send FlowSample UDP packets   :       1043  Send failed packets:          0
  Send CounterSample UDP packets:        372  Send failed packets:          0

>
```

1. 廃棄パケット時間が増加している場合，サンプリング間隔の設定を見直してください。

（2） CPU 使用率の確認

運用コマンド show cpu を実行して CPU 使用率を表示し，負荷を確認してください。CPU 使用率が高い場合は，コンフィグレーションコマンド sflow sample でサンプリング間隔を再設定してください。

図 24-11　運用コマンド show cpu の実行結果

```
> show cpu minutes

Date 20XX/05/27 10:04:33 UTC
*** Minutes ***
                                          0   25   50   75  100[%]
Date  Time              CPU average CPU peak +----+----+----+----+
05/27 09:04:00-09:04:59           9       26  **   P
05/27 09:05:00-09:05:59           9       31  **    P
05/27 09:06:00-09:06:59          10       31  **    P
05/27 09:07:00-09:07:59           8       38  **     P
05/27 09:08:00-09:08:59           7       26  **   P
05/27 09:09:00-09:09:59          10       31  **    P
05/27 09:10:00-09:10:59          10       38  **     P
05/27 09:11:00-09:11:59           7       33  **    P
05/27 09:12:00-09:12:59           8       26  **   P
05/27 09:13:00-09:13:59           9       33  **    P
05/27 09:14:00-09:14:59           8       21  **  P
05/27 09:15:00-09:15:59           8       31  **    P       …1
Date  Time              CPU average CPU peak +----+----+----+----+

>
```

1. CPU 使用率が高くなっている場合，サンプリング間隔の設定を見直してください。

24.3.4　sFlow 統計のサンプリング間隔の調整方法

本装置で sFlow 統計機能を使用した場合，サンプリング間隔の調整方法として次のものがあります。

（1） 回線速度から調整する

sFlow 統計機能を有効にしている全ポートの pps を運用コマンド show interfaces で確認し，受信パケットを対象にしている場合は「Input rate」を合計してください。もし，送信パケットを対象にしている場合は，「Output rate」も合計してください。その合計値を 100 で割った値が，目安となるサンプリング間隔となります。この値でサンプリング間隔を設定後，運用コマンド show sflow で廃棄数が増えないかどうかを確認してください。

ポート 0/5 とポート 0/6 に対して受信パケットをとる場合の目安となるサンプリング間隔の例を次に示します。

図 24-12　運用コマンド show interfaces の実行結果

```
> show interfaces gigabitethernet 0/5

Date 20XX/05/28 09:57:14 UTC
Port 0/5 : active up  1000BASE-T full(auto)  00eb.f507.0105
        Time-since-last-status-change: 3days 00:05:15
        Bandwidth: 1000000kbps  Average out: 1Mbps  Average in: 1Mbps
```

```
        Peak out: 1Mbps at 09:57:13  Peak in: 1Mbps at 09:57:13
        Output rate:         0.0bps         0.0pps
        Input  rate:     4063.5kbps       10.3kpps
        Flow control send   : off
        Flow control receive: off
        TPID: 8100
                :

>
> show interfaces gigabitethernet 0/6

Date 20XX/05/28 09:57:14 UTC
Port 0/6 : active up  1000BASE-T full(auto)  00eb.f507.0106
        Time-since-last-status-change: 3days 00:05:12
        Bandwidth: 1000000kbps  Average out: 1Mbps  Average in: 1Mbps
        Peak out: 1Mbps at 09:57:13  Peak in: 1Mbps at 09:57:13
        Output rate:     4893.5kbps       16.8kpps
        Input  rate:     4893.5kbps       16.8kpps
        Flow control send   : off
        Flow control receive: off
        TPID: 8100
                :

>
```

目安となるサンプリング間隔

＝ sFlow 統計機能を有効にしているポートの PPS 合計値 /100

＝ （10.3kpps+16.8kpps）/100

＝ 271※

注 ※

サンプリング間隔を 271 で設定すると実際は 512 で動作します。サンプリング間隔の詳細はコンフィグレーションコマンド sflow sample を参照してください。

（2） 詳細情報から調整する

運用コマンド show sflow detail を実行して表示される Sampling rate to collector（廃棄が発生しない推奨するサンプリング間隔）の値をサンプリング間隔として設定します。設定後は運用コマンド clear sflow statistics を実行し，しばらく様子を見てまだ Sampling rate to collector の値が設定より大きい場合は同じ手順でサンプリング間隔を設定してください。

図 24-13　運用コマンド show sflow detail の実行結果

```
> show sflow detail

Date 20XX/05/28 01:37:15 UTC
sFlow service status: enable
Progress time from sFlow statistics cleared: 17:13:05
sFlow agent data :
 sFlow service version: 4
 CounterSample interval rate: 60 seconds
 Default configured rate: 1 per 2048 packets
 Default actual rate    : 1 per 2048 packets
 Configured sFlow ingress ports: 0/2-4
 Configured sFlow egress ports : ----
 Received sFlow samples:       1043  Dropped sFlow samples        :          0
 Exported sFlow samples:       1043  Couldn't export sFlow samples:          0
 Overflow time of sFlow queue: 0 seconds
sFlow collector data :
 Collector IP address: 192.168.1.100  UDP: 6343  Source IP address: 192.168.1.25
3
  Send FlowSample UDP packets   :       1043  Send failed packets:          0
  Send CounterSample UDP packets:        372  Send failed packets:          0
 Collector IP address: 192.168.1.101  UDP: 6343  Source IP address: 192.168.1.25
3
  Send FlowSample UDP packets   :       1043  Send failed packets:          0
  Send CounterSample UDP packets:        372  Send failed packets:          0
```

```
Detail data :
 Max packet size: 1400 bytes
 Packet information type: header
 Max header size: 128 bytes
 Extended information type: switch,router,gateway,user,url
 Url port number: 80,8080
 Sampling mode: random-number
 Sampling rate to collector: 1 per 2048 packets
 Target ports for CounterSample: 0/2-4

>
```

25 LLDP

この章では，本装置に隣接する装置の情報を検出，管理する機能である LLDP の解説と操作方法について説明します。

25.1 解説

25.1.1 概要

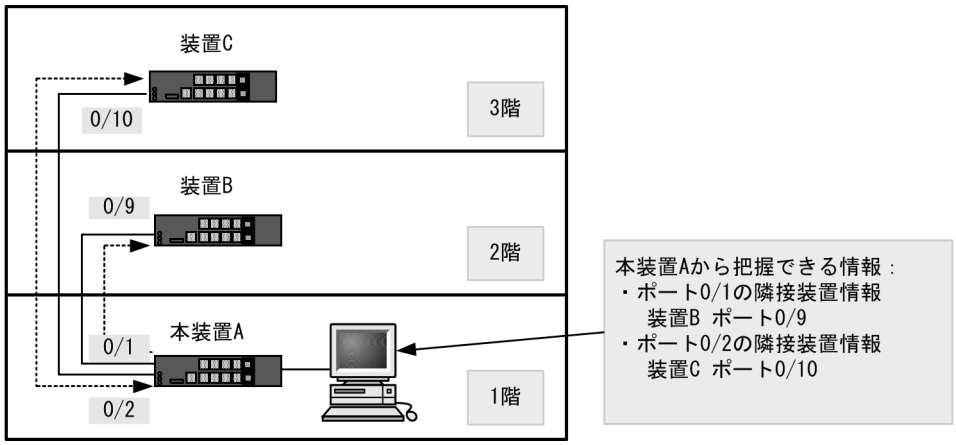
LLDP（Link Layer Discovery Protocol）は，データリンク層の接続を検出，管理するプロトコルです。LLDP フレーム（LLDPDU）の送受信により，隣接装置の情報を自動で検出します。

（1） LLDP の適用例

LLDP 機能は，本装置が収容するすべてのイーサネットポートで使用することができます。LLDP 機能を使用したポートでは，接続装置から受信する情報を隣接装置情報として管理します。

LLDP の適用例を次の図に示します。この例では，同一ビル内の各階に設置された装置との接続状態を，１階に設置した本装置 A から把握できるようになります。

図 25-1 LLDP の適用例



25.1.2 サポート仕様

（1） 接続可能な LLDP 規格

本装置では次に 3 つの規格をサポートします。

- IEEE Std 802.1AB-2009
- IEEE Std 802.1AB-2005
  本装置では，宛先 MAC アドレスが "01:80:C2:00:00:0E" だけ LLDPDU として受信できます。
- IEEE 802.1AB Draft 6

デフォルトでは IEEE Std 802.1AB-2009 で動作して，IEEE 802.1AB Draft 6 の LLDPDU だけを受信したポートからは IEEE 802.1AB Draft 6 の LLDPDU を送信します。なお，IEEE Std 802.1AB-2005 とも接続できます。

また，本装置には LLDP バージョンを設定するコンフィグレーションがあります。コンフィグレーションと規格別の受信 LLDPDU と送信 LLDPDU の関係を次の表に示します。

表 25-1 コンフィグレーションと規格別の受信 LLDPDU と送信 LLDPDU の関係

コンフィグレーションコマンド lldp version の設定	受信 LLDPDU の規格		送信 LLDPDU の規格
	IEEE Std 802.1AB-2009 IEEE Std 802.1AB-2005	IEEE802.1AB Draft 6	
2005	有 / 無	無（受信抑止）	IEEE Std 802.1AB-2005
draft	無（受信抑止）	有 / 無	IEEE802.1AB Draft 6
auto	有	有	IEEE Std 802.1AB-2009※
		無	IEEE Std 802.1AB-2009※
	無	有	IEEE802.1AB Draft 6
		無	IEEE Std 802.1AB-2009※

注 ※

System Capabilities TLV だけは IEEE Std 802.1AB-2005 の規格で送信します。

（2） サポート TLV

本装置のサポート TLV を次の表に示します。

表 25-2 サポート TLV

TLV name	コンフィグレーションコマンド lldp version の設定								説明
	draft		2005		auto				
	LLDPDU								
	Draft 6		2005		Draft 6		2009 2005		
	受信	送信	受信	送信	受信	送信	受信	送信 ※2	
End Of LLDPDU	○	○	○	○	○	○	○	○	LLDPDU の終端識別子です。
Chassis ID	○	○	○	○	○	○	○	○	本装置は装置の MAC アドレスを送信します。
Port ID	○	○	○	○	○	○	○	○	本装置はポートの MAC アドレスを送信します。
Time-to-Live	○	○	○	○	○	○	○	○	本装置が送信する情報の保持時間はコンフィグレーションで変更できます。
Port Description	○	○	○	○	○	○	○	○	本装置は interface グループ MIB の ifDescr と同じ値を送信します。
System Name	○	○	○	○	○	○	○	○	本装置は system グループ MIB の sysName と同じ値を送信します。
System Description	○	○	○	○	○	○	○	○	本装置は system グループ MIB の sysDescr と同じ値 ※1 を送信します。
System Capabilities	×	×	○	×	×	×	○	○	利用できる機能と有効な機能の情報を送信します。

TLV name		コンフィグレーションコマンド lldp version の設定								説明
		draft		2005		auto				
		LLDPDU								
		Draft 6		2005		Draft 6		2009 2005		
		受信	送信	受信	送信	受信	送信	受信	送信 ※2	
Management Address		×	×	○	×	×	×	○	○	管理アドレスを送信します。利用できる機能と有効な機能の情報を送信します。
Organizationally-defined TLV extensions	VLAN ID	○	○	○	○	○	○	×	×	設定されている VLAN ID や VLAN に関連づけられた IP アドレスを送信します。
	VLAN Address	○	○	○	○	○	○	×	×	
	他	×	×	×	×	×	×	×	×	
IEEE802.1 Organizationally TLV	Port VLAN ID	×	×	×	×	×	×	○	○	設定されているポート VLAN の VLAN ID 情報を送信します。
	Port And Protocol VLAN ID	×	×	×	×	×	×	○	○	設定されているプロトコル VLAN の VLAN ID 情報を送信します。
	VLAN Name	×	×	×	×	×	×	○	△ ※3	設定されているポート VLAN の VLAN ID，および VLAN の名前を送信します。
	他	×	×	×	×	×	×	×	×	

（凡例）

○：サポート　×：未サポート　△：一部サポート

Draft 6：IEEE 802.1AB Draft 6

2009　：IEEE Std 802.1AB-2009

2005　：IEEE Std 802.1AB-2005

注 ※1

スタック動作時にメンバスイッチから送信される LLDPDU の "System Description" には，マスタスイッチのモデル名が設定されます。

注 ※2

IEEE Std 802.1AB-2009 の規格で LLDPDU を送信します。ただし，System Capabilities は IEEE Std 802.1AB-2005 の規格で送信します。

注 ※3

VLAN Name Length の情報を 0 で送信し，VLAN の名前は送信しません。

LLDP でサポートする情報の詳細を以下に示します。

なお，MIB については「MIB レファレンス」を参照してください。

（a） Chassis ID（装置の識別子）

装置を識別する情報です。この情報には subtype が定義され，subtype によって送信内容が異なります。

subtype と送信内容を次の表に示します。

表 25-3 Chassis ID の subtype 一覧（IEEE Std 802.1AB-2009）

subtype	種別	送信内容
1	Chassis component	Entity MIB の entPhysicalAlias と同じ値
2	Chassis interface	interface MIB の ifAlias と同じ値
3	Port component	Entity MIB の portEntPhysicalAlias と同じ値，または Entity MIB の backplaneEntPhysicalAlias と同じ値
4	MAC address	LLDP MIB の macAddress と同じ値
5	Network address	LLDP MIB の networkAddress と同じ値
6	Interface name	interface MIB の ifName と同じ値
7	Locally assigned	LLDP MIB の local と同じ値

表 25-4 Chassis ID の subtype 一覧（IEEE 802.1AB Draft 6）

subtype	種別	送信内容
1	Chassis component	Entity MIB の entPhysicalAlias と同じ値
2	Chassis interface	interface MIB の ifAlias と同じ値
3	Port	Entity MIB の portEntPhysicalAlias と同じ値
4	Backplane component	Entity MIB の backplaneEntPhysicalAlias と同じ値
5	Network address	LLDP MIB の macAddress と同じ値
6	Interface name	LLDP MIB の networkAddress と同じ値
7	Locally assigned	LLDP MIB の local と同じ値

Chassis ID についての送受信条件は次のとおりです。

- 送信：送信する subtype の種別は MAC address だけです。送信する MAC アドレスは装置 MAC アドレスを使用します。また，スタック構成時はスタックの装置 MAC アドレスを使用します。
- 受信：上記に示した全 subtype について受信できます。
- 受信データ最大長：255 オクテット

（b） Port ID（ポート識別子）

ポートを識別する情報です。この情報には subtype が定義され，subtype によって送信内容が異なります。

subtype と送信内容を次の表に示します。

表 25-5 Port ID の subtype 一覧（IEEE Std 802.1AB-2009）

subtype	種別	送信内容
1	Interface alias	Interface MIB の ifAlias と同じ値
2	Port component	Entity MIB の portEntPhysicalAlias と同じ値，または Entity MIB の backplaneEntPhysicalAlias と同じ値
3	MAC address	LLDP MIB の macAddress と同じ値
4	Network address	LLDP MIB の networkAddress と同じ値
5	Interface name	interface MIB の ifName と同じ値

subtype	種別	送信内容
6	Agent circuit ID	RFC3046 の Circuit ID
7	Locally assigned	LLDP MIB の local と同じ値

表 25-6　Port ID の subtype 一覧（IEEE 802.1AB Draft 6）

subtype	種別	送信内容
1	Port	Interface MIB の ifAlias と同じ値
2	Port component	Entity MIB の portEntPhysicalAlias と同じ値
3	Backplane component	Entity MIB の backplaneEntPhysicalAlias と同じ値
4	MAC address	LLDP MIB の macAddress と同じ値
5	Network address	LLDP MIB の networkAddress と同じ値
6	Locally assigned	LLDP MIB の local と同じ値

Port ID についての送受信条件は次のとおりです。

- 送信：送信する subtype の種別は MAC address だけです。送信する MAC アドレスは該当 Port の MAC アドレスを使用します。
- 受信：上記に示した全 subtype について受信できます。
- 受信データ最大長：255 オクテット

（c） Time-to-Live（情報の保持時間）

配布する情報を受信装置側で保持する時間を示します。

保持時間はコンフィグレーションで変更できますが，初期状態で使用することをお勧めします。

（d） Port description/ System name/System description

Port description，System name，Sstem description には subtype はありません。送信内容および受信条件（受信データ長）を次の表に示します。

表 25-7　Port description/ System name/System description の送信内容および受信条件

TLV name	説明	subtype	送信内容	受信データ最大長
Port description	ポート識別子	なし	Interface MIB の ifDescr と同じ値	255 オクテット
System name	装置名称	なし	systemMIB の sysName と同じ値	255 オクテット
System description	装置種別	なし	systemMIB の sysDescr と同じ値	255 オクテット

（e） System Capabilities（装置の機能）

利用できる機能と有効な機能を識別する情報です。この情報は規格によって subtype の有無が異なります。

IEEE Std 802.1AB-2009

subtype が定義され，subtype には chassis ID subtype を使用します。

IEEE Std 802.1AB-2005

subtype はありません。

System Capabilities についての送信内容および受信条件は次のとおりです。

- 送信
  IEEE Std 802.1AB-2005 の規格で送信します。System Capabilities TLV の送信内容を次の表に示します。

表 25-8 System Capabilities TLV の送信内容

データ名	説明	送信内容
system capabilities	機能識別子（装置が有する機能）	MAC Bridge（1）有
enabled capabilities	機能識別子のうち，有効になっている機能	MAC Bridge（1）有

- 受信
  IEEE Std 802.1AB-2009，および IEEE Std 802.1AB-2005 の規格で受信できます。IEEE Std 802.1AB-2009 の規格では，すべての subtype について受信できます。

(f) Management Address（管理アドレス）

装置の IP アドレスや MAC アドレスを識別する情報です。この情報には subtype が定義され，subtype によって送信内容が異なります。

Management Address についての送信内容および受信条件は次のとおりです。

- 送信
  Management Address TLV の送信内容を次の表に示します。

表 25-9 Management Address TLV の送信内容

データ名	説明	設定値
management address subtype	管理アドレス種別	1：IP（IPv4 アドレス）または 2：IP6（IPv6 アドレス）
management address	管理アドレス	コンフィグレーションコマンド lldp management-address で設定した アドレスを使用します
interface numbering subtype	インタフェース番号サブタイプ	1：Unknown
OID string length	OID 情報長	0

- 受信
  すべての subtype について受信できます。LLDPDU 上に複数の Management Address TLV が付く場合は，最後の情報だけを保持します。
- 受信データ最大長
  167 オクテット

(g) Organizationally-defined TLV extensions

本装置独自に次の情報をサポートしています。

- VLAN ID
  該当ポートが使用する VLAN Tag の VLAN ID を示します。Tag 変換を使用している場合は，変換後の VLAN ID を示します。この情報はトランクポートだけ有効な情報です。
- VLAN Address
  この情報は，該当ポートで IP アドレスが設定されている VLAN のうち，最も小さい VLAN ID とその IP アドレスを 1 つ示します。

（h） IEEE802.1 Organizationally Specific TLVs

本装置では次の情報をサポートしています。

- Port VLAN ID
  該当ポートのポート VLAN の情報です。
  アクセスポートの場合，該当するポート VLAN の VLAN ID を送信します。アクセスポート以外の場合，ネイティブ VLAN が有効なときはネイティブ VLAN の VLAN ID を送信します。受信データ最大長は，6 オクテットです。
- Port And Protocol VLAN ID
  該当ポートのプロトコル VLAN の情報です。
  プロトコルポートの場合，該当するプロトコル VLAN の VLAN ID を送信します。送信する VLAN ID の情報は，最新の状態です。プロトコル VLAN の設定がないときは，プロトコル VLAN の情報を送信しません。受信データ最大長は，7 オクテットです。
- VLAN Name
  該当ポートのポート VLAN の情報です。
  アクセスポートの場合，該当するポート VLAN の VLAN ID を送信します。トランクポートの場合，VLAN Tag の VLAN ID を送信します。また，ネイティブ VLAN が有効なときは，ネイティブ VLAN の VLAN ID も同様に送信します。アクセスポートおよびトランクポート以外の場合，各種ポートの VLAN ID を送信します。また，ネイティブ VLAN が有効なときは，ネイティブ VLAN の VLAN ID も同様に送信します。
  送信する VLAN ID の情報は，最新の状態です。また，Tag 変換を使用している場合は，変換後の VLAN ID を送信し，VLAN トンネリング機能を使用している場合は，VLAN トンネリング機能で付けた VLAN Tag の VLAN ID を送信します。受信データ最大長は，39 オクテットです。

25.1.3 LLDP 使用時の注意事項

（1） 本機能を設定した装置間に本機能をサポートしない別装置を接続した場合

次に示す構成とした場合，隣接装置との接続状態を正確に把握しにくい状態になります。

- スイッチを経由して接続した場合，スイッチは LLDP の配布情報を中継します。そのため，直接接続していない装置間で，隣接情報として配布情報を受信できるので，直接接続されている装置間の情報と区別が付かなくなります。
- ルータを経由して接続した場合，LLDP の配布情報はルータで廃棄されるため LLDP 機能を設定した装置間では受信できません。

（2） 他社接続について

他社が独自にサポートしている Link Layer Discovery Protocol※ との相互接続はできません。

注 ※
Cisco Systems 社：CDP（Cisco Discovery Protocol）
Extreme Networks 社：EDP（Extreme Discovery Protocol）
Foundry Networks 社：FDP（Foundry Discovery Protocol）

（3） 隣接装置の最大数について

装置当たり「コンフィグレーションガイド Vol.1 3.2 収容条件」に示す隣接装置情報を収容できます。最大数を超えた場合，受信した配布情報は廃棄します。受信済みの隣接装置情報がタイムアウトで削除される時間を確保するために，廃棄状態は一定時間継続されます。時間は，最大収容数の閾値以上になった隣

接装置情報の保持時間と同一です。

（4） 他機能との共存について

(a) レイヤ 2 認証機能との共存

「5.9.3　レイヤ 2 認証機能と他機能の共存」を参照してください。

(b) CFM との共存

「21.1.9　CFM 使用時の注意事項」を参照してください。

25.2 コンフィグレーション

25.2.1 コンフィグレーションコマンド一覧

LLDP のコンフィグレーションコマンド一覧を次の表に示します。

表 25-10 コンフィグレーションコマンド一覧

コマンド名	説明
lldp enable	ポートで LLDP の運用を開始します。
lldp hold-count	本装置が送信する LLDP フレームに対して隣接装置が保持する時間を指定します。
lldp interval-time	本装置が送信する LLDP フレームの送信間隔を指定します。
lldp management-address	送信するManagement Address TLVの管理アドレスを設定します。
lldp run	装置全体で LLDP 機能を有効にします。
lldp version	本装置の LLDP のバージョンを設定します。

25.2.2 LLDP の設定

(1) LLDP 機能の設定

[設定のポイント]

LLDP 機能のコンフィグレーションは装置全体で機能を有効にする設定と，実際に運用するポートで有効にする設定が必要です。

ここでは，ポート 0/1 において LLDP 機能を運用させます。

[コマンドによる設定]

1. **(config)# lldp run**
   装置全体で LLDP 機能を有効にします。
2. **(config)# interface gigabitethernet 0/1**
   ポート 0/1 のイーサネットインタフェースコンフィグレーションモードに移行します。
3. **(config-if)# lldp enable**
   (config-if)# exit
   ポート 0/1 で LLDP 機能の動作を開始します。

(2) LLDP フレームの送信間隔，保持時間の設定

[設定のポイント]

LLDP フレームの保持時間は，送信間隔の倍率で指定します。

[コマンドによる設定]

1. **(config)# lldp interval-time 60**
   LLDP フレームの送信間隔を 60 秒に設定します。
2. **(config)# lldp hold-count 3**
   本装置が送信した情報を隣接装置が保持する時間を interval-time 時間の回数で設定します。この場合，60 秒 ×3 で 180 秒になります。

（3） LLDP フレームのバージョン設定

［設定のポイント］

任意のポートで IEEE802.1AB/D6.0 の LLDP フレームで運用するよう設定します。その他のポートでは，LLDP のバージョンを自動判別して運用します。

ここでは，ポート 0/10 に IEEE802.1AB/D6.0 の LLDP フレームで運用するよう設定します。

［コマンドによる設定］

1. **(config)# interface gigabitethernet 0/10**

   ポート 0/10 のイーサネットインタフェースコンフィグレーションモードに移行します。

2. **(config-if)# lldp version draft**

   (config-if)# lldp enable

   (config-if)# exit

   ポート 0/10 は IEEE802.1AB/D6.0 の LLDP フレームで運用します。

（4） 送信する管理アドレスの設定

［設定のポイント］

管理アドレスを設定すると，設定した IP アドレスが隣接装置に通知されます。設定できる IP アドレスは，インタフェースに設定されている IP アドレスに限りません。

［コマンドによる設定］

1. **(config)# lldp management-address ip 192.168.1.254**

   送信する Management Address TLV の管理アドレスを 192.168.1.254 に設定します。

25.3 オペレーション

25.3.1 運用コマンド一覧

LLDP の運用コマンド一覧を次の表に示します。

表 25-11 運用コマンド一覧

コマンド名	説明
show lldp	LLDP の設定情報および隣接装置情報を表示します。
show lldp statistics	LLDP の統計情報を表示します。
clear lldp	LLDP の隣接情報をクリアします。
clear lldp statistics	LLDP の統計情報をクリアします。

25.3.2 LLDP 情報の表示

LLDP 情報の表示は，運用コマンド show lldp で行います。

- 運用コマンド show lldp は，LLDP の設定情報とポートごとの隣接装置数を表示します。
- 運用コマンド show lldp detail は，隣接装置の詳細な情報を表示します。
- 運用コマンド show lldp neighbors は，隣接装置のサマリ情報を表示します。

図 25-2 show lldp の実行結果

```
> show lldp

Date 20XX/06/07 15:50:37 UTC
Status: Enabled  Chassis ID: Type=MAC       Info=0012.e201.0001
Interval Time: 30   Hold Count: 4  TTL: 120
Port Counts=4
  0/5         Link: Up    Neighbor Counts:   0  Draft Neighbor Counts:   1
  0/6         Link: Up    Neighbor Counts:   1  Draft Neighbor Counts:   0
  0/7         Link: Up    Neighbor Counts:   1  Draft Neighbor Counts:   0
  0/8(CH:64)  Link: Up    Neighbor Counts:   0  Draft Neighbor Counts:   0

>
```

図 25-3 show lldp detail の実行結果

```
> show lldp detail

Date 20XX/06/07 15:50:41 UTC
Status: Enabled  Chassis ID: Type=MAC     Info=0012.e201.0001
Interval Time: 30  Hold Count: 4  TTL: 120
System Name: AX260A-08T#1
System Description: ALAXALA AX260A AX-0260-A08T [AX260A-08T] Appliance software
Ver. 4.4 [OS-L2F]
Neighbor Counts=3
Draft Neighbor Counts=1
Port Counts=4
Port 0/5
  Link: Up    PortEnabled: TRUE   AdminStatus: enabledRxTx
  Neighbor Counts:   0  Draft Neighbor Counts:   1
  Port ID: Type=MAC       Info=00eb.fc01.0105
  Port Description: GigabitEther 0/5 (GE Port0/5)
  Tag ID: Untagged
  IPv4 Address: Untagged: 4000  40.0.26.1
  IPv6 Address: Untagged: 4000  2001:40::26:1
  LLDPDU Destination Address: 0100.8758.1310
  Draft Neighbor 1    TTL: 103
    Chassis ID: Type=MAC       Info=0012.e200.0033
    System Description: ALAXALA AX2530 AX-2530-24T-B [AX2530S-24T] Switching
```

```
software Ver. 4.2 [OS-L2A]
     Port ID: Type=MAC       Info=0012.e210.010e
     Port Description: GigabitEther 0/14
     Tag ID: Untagged
Port 0/6
  Link: Up    PortEnabled: TRUE   AdminStatus: enabledRxTx
  Neighbor Counts:   1  Draft Neighbor Counts:   0
  Port ID: Type=MAC       Info=0012.e201.0106
  Port Description: GigabitEther 0/6 (GE Port0/6)
  Tag ID: Untagged
  IPv4 Address: Untagged: 4000  40.0.26.1
  IPv6 Address: Untagged: 4000  2001:40::26:1
  LLDPDU Destination Address: 0180.c200.000e
  Neighbor 1    TTL: 88
    Chassis ID: Type=MAC       Info=0012.e2d2.af7b
    System Name: AX2530S-48T#1
    System Description: ALAXALA AX2530 AX-2530-48T-B [AX2530S-48T] Switching
software Ver. 4.4 [OS-L2A]
     Port ID: Type=MAC       Info=0012.e2d2.af8d
     Port Description: GigabitEther 0/18
     Tag ID: Untagged
Port 0/7
  Link: Up    PortEnabled: TRUE   AdminStatus: enabledRxTx
  Neighbor Counts:   1  Draft Neighbor Counts:   0
  Port ID: Type=MAC       Info=0012.e201.0107
  Port Description: GigabitEther 0/7 (GE Port0/7)
  Tag ID: Untagged
  LLDPDU Destination Address: 0180.c200.000e
  Neighbor 1    TTL: 111
    Chassis ID: Type=MAC       Info=0012.e207.0001
    System Name: AX260A-08TF#2
    System Description: ALAXALA AX260A AX-0260-A08TF [AX260A-08TF] Appliance
software Ver. 4.4 [OS-L2F]
     Port ID: Type=MAC       Info=0012.e207.0107
     Port Description: GigabitEther 0/7 (GE Port0/7)
     Tag ID: Untagged
Port 0/8(CH:64)
  Link: Up    PortEnabled: TRUE   AdminStatus: enabledRxTx
  Neighbor Counts:   0  Draft Neighbor Counts:   0
  Port ID: Type=MAC       Info=0012.e201.0108
  Port Description: GigabitEther 0/8 (GE Port0/8)
  Tag ID: Tagged=3333
  LLDPDU Destination Address: 0180.c200.000e

>
```

図 25-4　show lldp neighbors の実行結果

```
> show lldp neighbors

Date 20XX/06/07 15:51:31 UTC
Neighbor Counts:   3
Neighbor Information
                Chassis                       Port
0/5             0012.e200.0033                GigabitEther 0/14
0/6             0012.e2d2.af7b                GigabitEther 0/18
0/7             0012.e207.0001                GigabitEther 0/7 (GE Por...

>
```

26 ポートミラーリング

ポートミラーリングは，送受信するフレームのコピーを指定した物理ポートへ送信する機能です。この章では，ポートミラーリングの解説と操作方法について説明します。

26.1 解説

26.1.1 ポートミラーリングの概要

ポートミラーリングは，送受信するフレームのコピーを指定した物理ポートへ送信する機能です。フレームをコピーすることを**ミラーリング**と呼びます。この機能を利用して，ミラーリングしたフレームをアナライザなどで受信することによって，トラフィックの監視や解析を行えます。

受信フレームおよび送信フレームに対するミラーリングのそれぞれの動作を次の図に示します。

図 26-1 受信フレームのミラーリング

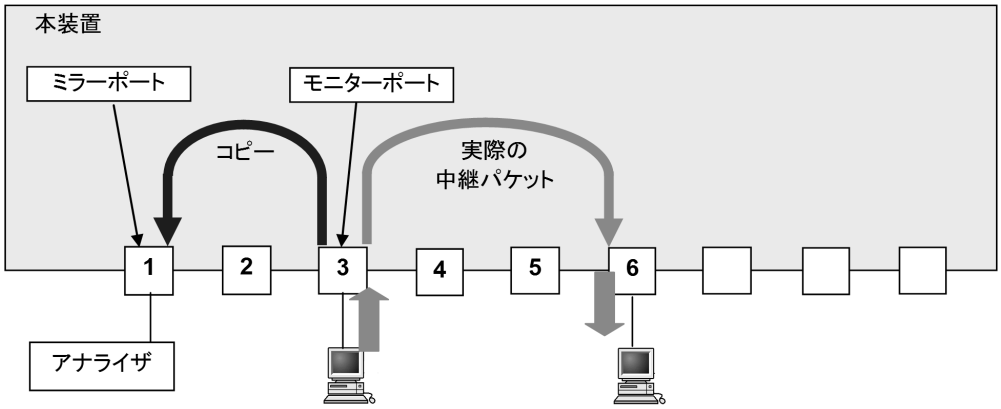
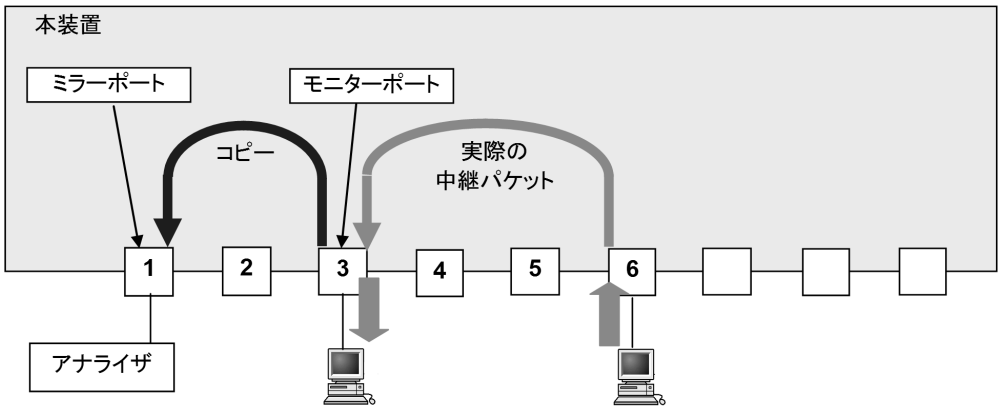


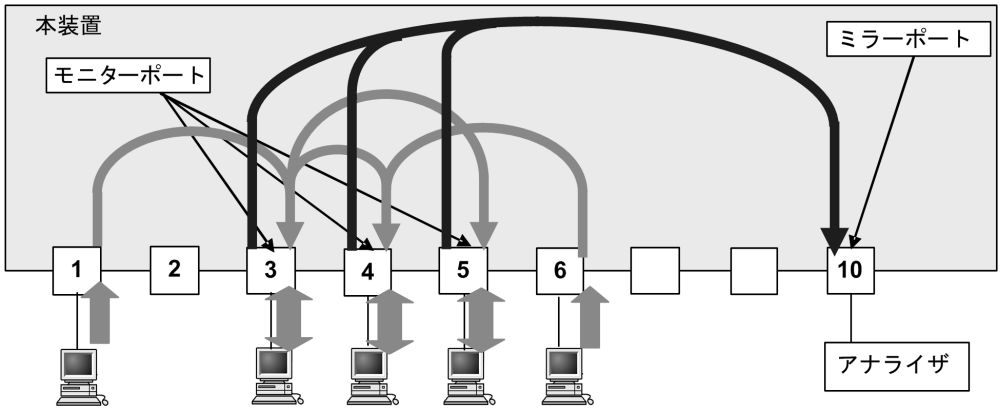
図 26-2 送信フレームのミラーリング



これらの図で示すとおり，トラフィックを監視する物理ポートを**モニターポート**と呼び，ミラーリングしたフレームの送信先となる物理ポートを**ミラーポート**と呼びます。

モニターポートとミラーポートは「多対１」の設定ができ，複数のモニターポートから受信したフレームのコピーを，１つのミラーポートへ送信できます。

図 26-3　複数ポートのフレームのミラーリング（多対 1）



また，下記のように「１対２」や「多対２」の設定ができ，１つまたは複数のモニターポートから受信したフレームのコピーを，最大２つのミラーポートへ送信できます。

図 26-4　1 対 2 のミラーリング

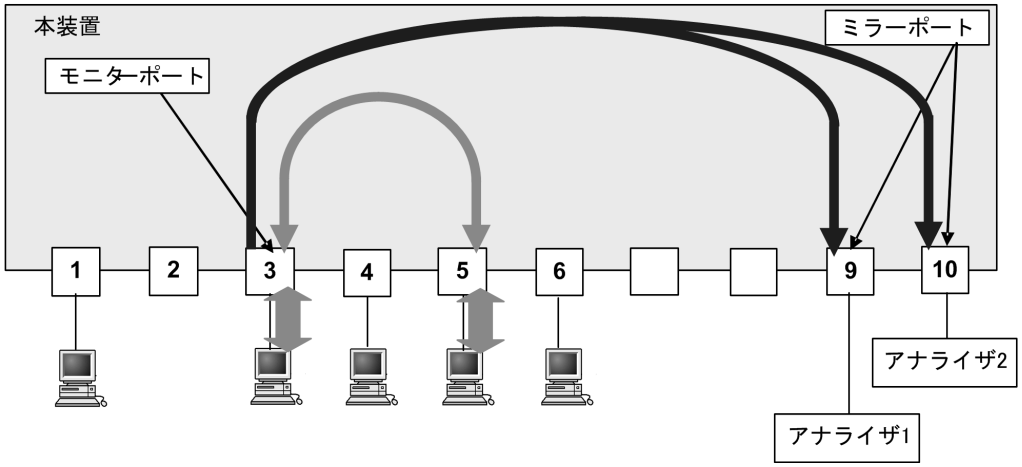
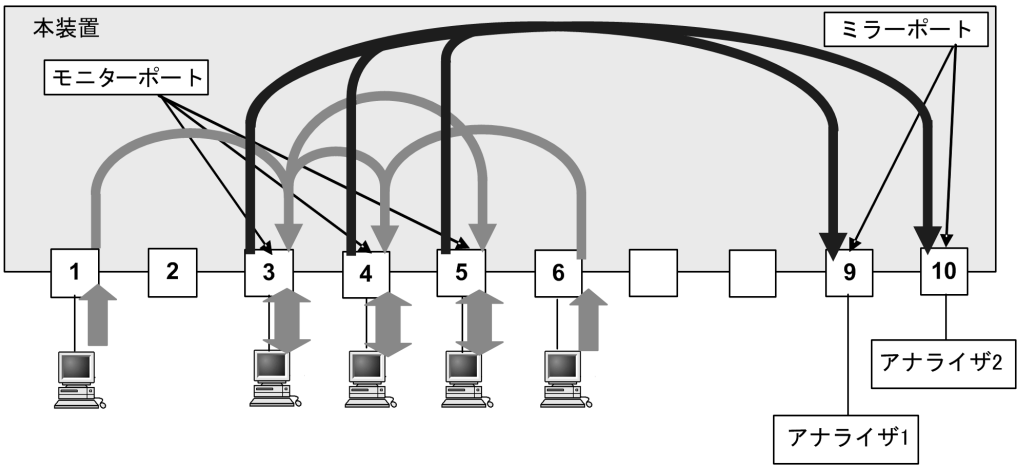


図 26-5　多対２のミラーリング



ミラーポートの受信，送信，送受信種別はモニターポートの設定に従います。ミラーポートを２ポート設定した場合も，モニターポートの設定に従い２ポートとも同じ種別のデータをミラーリングします。ミ

ラーポートごとに送信，受信，送受信を分けることはできません。

ポートミラーリングに関する運用コマンドはありません。ミラーポートに接続したアナライザで，フレームがミラーリングされていることを確認してください。

（1） ICMP 限定ミラーリング機能

本機能はポートミラーリング機能を利用し，当該ポートで受信したフレームのうち，ICMP フレームだけを抽出して任意のポートにミラーリングします。

本機能でミラーリングするフレームは，ホワイトリスト機能の学習・未学習に関係なく，モニターポートから受信した ICMP フレームを無条件でコピーしてミラーポートに送信します。

なお，本機能を使用する場合は，受信側フロー検出モードをデフォルトコンフィグレーション（flow detection mode 未設定）でご使用ください。

本機能はスタンドアロンで動作します。（スタックでは動作しません。）

（2） 802.1Q Tag 付与機能

802.1Q Tag 付与機能は，ポートミラーリングでミラーリングされたフレームに，VLAN Tag を付ける機能です。この機能を利用して，ミラーリングしたフレームをレイヤ 2 中継し，中継先にあるアナライザなどでフレームを受信することで，離れた場所にあるスイッチのトラフィックを監視したり解析したりできます。

この機能を使用する場合は，レイヤ 2 中継に使用しているトランクポートをミラーポートとして指定することも可能です。

802.1Q Tag 付与機能がフレームに付ける VLAN Tag のフィールドについて次の表に示します。

表 26-1　802.1Q Tag 付与機能がフレームに付ける VLAN Tag のフィールド

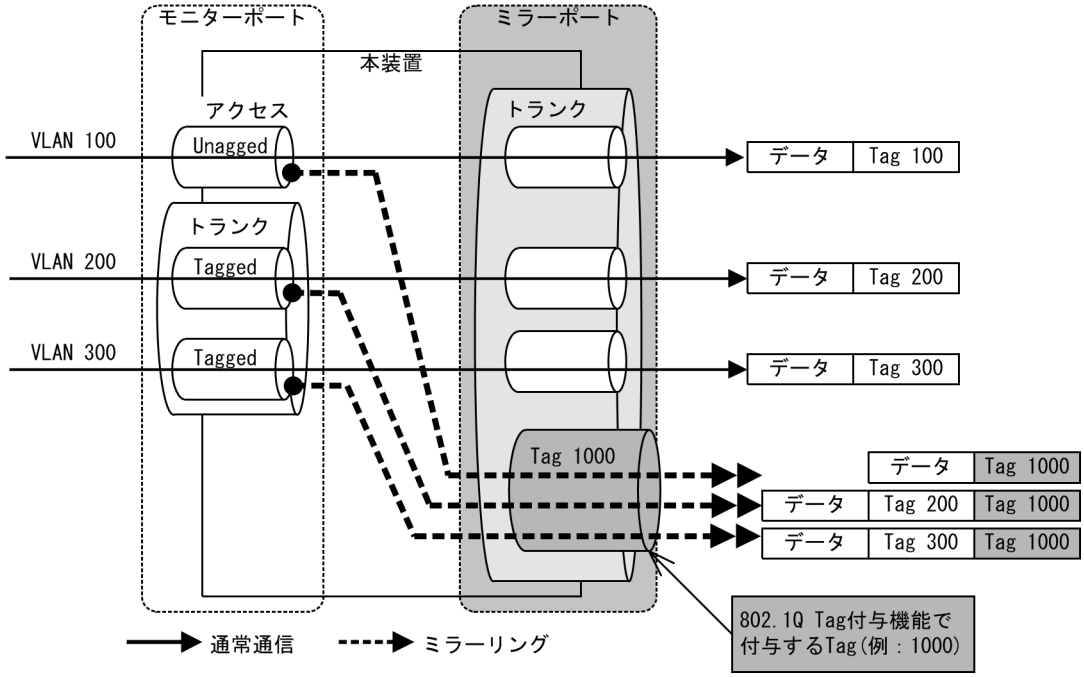
フィールド	説明	サポート内容
TPID	IEEE802.1Q VLAN Tag が続くことを示す Ether Type 値を示します。	ミラーポートとして使用するポートの TPID に従います。
User Priority	IEEE802.1D のプライオリティを示します。	コンフィグレーションで指定可能です。※
CF	MAC ヘッダ内の MAC アドレスが標準フォーマットに従っているかどうかを示します。	本装置では標準 (0) だけをサポートします。
VLAN ID	VLAN ID を示します。	コンフィグレーションで指定可能です。ただし，レイヤ 2 中継で未使用の VLAN ID に限ります。

注 ※

802.1Q Tag 付与機能で指定するユーザ優先度は 802.1Q Tag 内だけに記録されるものであり，本装置の送信キュー選択には影響しません。

802.1Q Tag 付与機能の概要を次の図に示します。

図 26-6 802.1Q Tag 付与機能の概要



上図に示すようにミラーリング対象フレームが Tagged フレームの場合は，本機能によって 802.1Q Tag を追加で付与するため，二重 Tagged フレームとしてミラーポートから送信します。

本機能は ICMP 限定ミラーリング機能やホワイトリスト機能，およびポリシーベースミラーリングで使用するミラーポートにも適用します。

本機能を使用する場合は，次の設定をしてください。

- ミラーポート：トランクポートに設定
  上図に示すようにレイヤ 2 中継に使用するポートをミラーポートとしても使用する場合はトランクポートに設定してください。
  802.1Q Tag 付与機能だけで使用する場合は，アクセスポートで使用可能です。
- 本機能で付与する Tag：コンフィグレーションコマンド vlan，interface vlan で設定していない VLAN ID（最大 1 つ）

本機能はスタンドアロンで動作します。（スタックでは動作しません。）

(3) サポート範囲

ポートミラーリング機能のサポート範囲を次の表に示します。

表 26-2 ポートミラーリング機能のサポート範囲

項目		スタック 動作時	スタンドアロン 動作時
最大セッション数※1		1	4
	ポリシーベースミラーリング	1	2
モニターポート	設定可能ポート	※2	※2

項目			スタック動作時	スタンドアロン動作時
ミラーポート※4	ミラーポート数／セッション単位		2	2
	受信フレームのミラーポート数／装置全体 （ホワイトリスト機能，ICMP 限定ミラーリング機能のミラーポートを含む）		2	4
	送信フレームのミラーポート数／装置全体		2	2
	受信フレームのミラーポート数／１つのモニターポート （ホワイトリスト機能，ICMP 限定ミラーリング機能のミラーポートを含む）		2	2
	802.1Q Tag 付与		×	○
	ミラーポート種別※3	イーサネット	○	○
		ポートチャネル	×	○
設定	受信フレーム／セッション単位		○	○
	送信フレーム／セッション単位		○	○
	送受信フレーム／セッション単位		○	○
	セッション情報の全項目設定		○	○
	セッション情報の全項目一括変更		○	○
	モニターポートの変更（追加・削除）		×	○
	セッション情報の全項目一括削除		○	○

（凡例）
○：サポート　×：未サポート

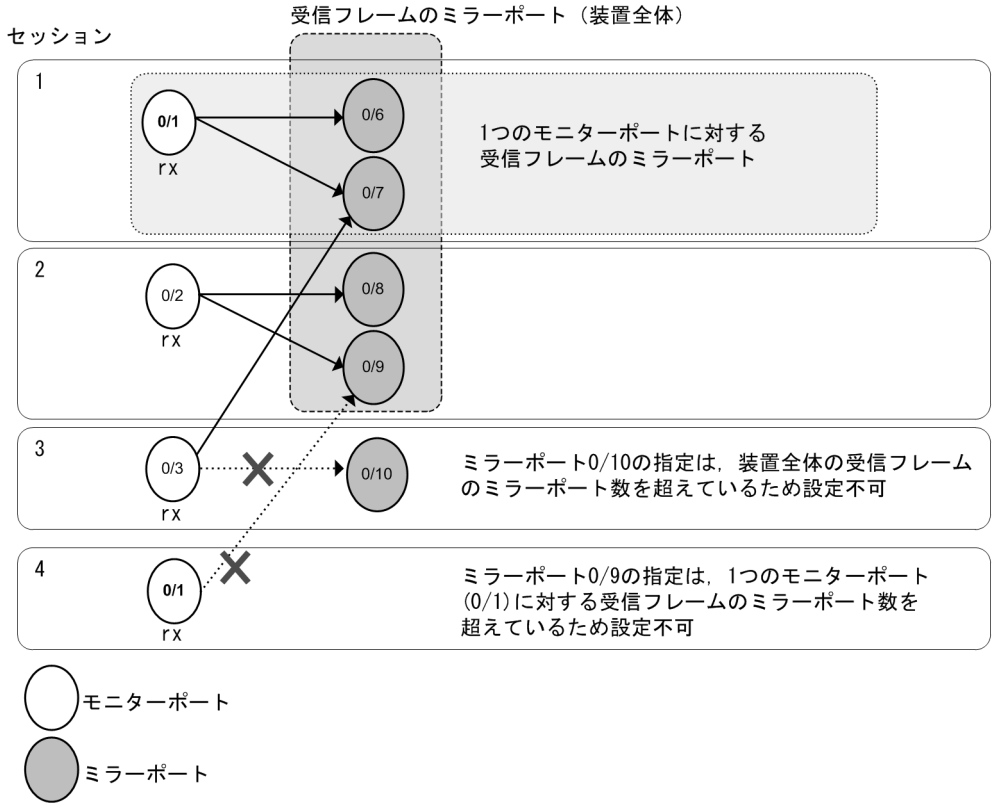
注 ※1
モニターセッションはポリシーベースミラーリングでも使用します。ポリシーベースミラーリングで 2 セッション使用する場合は，ポートミラーリングで使用可能なセッション数は 2 となります。スタック動作時は 1 セッションのため，ポートミラーリングかポリシーベースミラーリングのどちらかの使用となります。

注 ※2
スタック動作時のスタックポートは，モニターポートおよびミラーポートに指定できません。

注 ※3
ミラーポートは最大 2 件のイーサネットインタフェース，または最大 1 件のポートチャネルインタフェースのどちらか一方を選択してください。なお，ポートチャネルインタフェースに属するイーサネットインタフェースは，ミラーポートの収容条件に影響しません。

注 ※4
モニターポート，ミラーポートはセッション間で重複設定可能です。ただし，すべてのミラー機能に対して，同一ポートをモニターポートとミラーポートに混在する設定はできません。
ミラーポート数の数え方を，スタンドアロン動作時を例として次の図に示します。

図 26-7　受信フレームのミラーポート数（ホワイトリスト機能，ICMP 限定ミラーリング機能のミラー設定無）



受信フレーム（rx/both）に対するミラーポートの合計は，装置全体で最大 4 ポートです。
1 つのモニターポートの受信フレーム（rx/both）に対するミラーポートは，最大 2 ポートです。

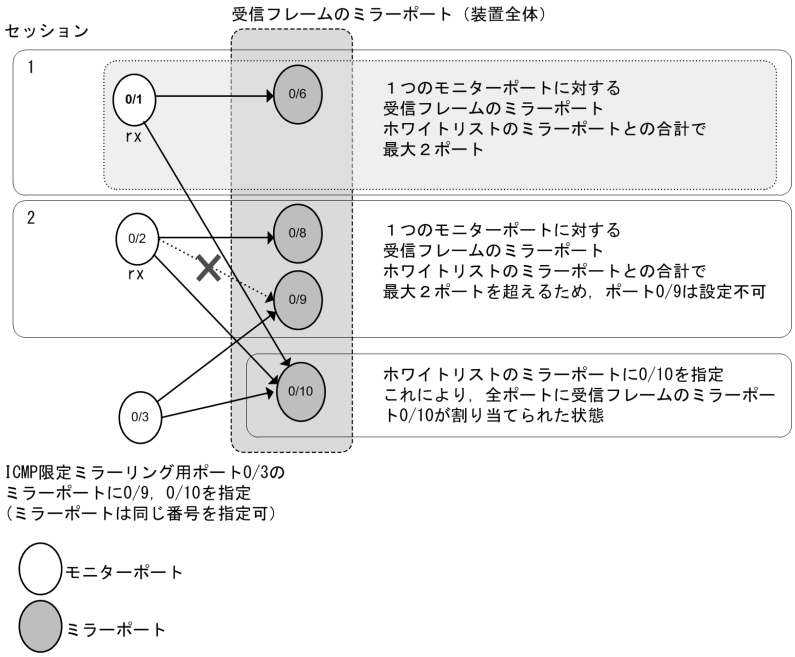
＜図内のセッション 3 について＞

ミラーポートはセッション間で重複設定可能です。ただし，装置全体の受信フレームのミラーポートは最大 4 ポートまでのため，モニターポート 0/3 にミラーポート 0/7 は設定できますが，ミラーポート 0/10 は設定できません。

＜図内のセッション 4 について＞

モニターポートはセッション間で重複設定可能です。ただし，1 つのモニターポートに対する受信フレームのミラーポートは最大 2 ポートまでのため，セッション 4 でモニターポート 0/1 にミラーポート 0/9 は設定できません。

図 26-8 （ホワイトリスト機能，ICMP 限定ミラーリング機能のミラー設定有）



受信フレーム（rx/both）に対するミラーポートの合計は，ホワイトリスト機能，ICMP 限定ミラーリング機能と合わせて装置全体で最大 4 ポートです。
また，ホワイトリスト機能でミラーポートを設定した場合，全ポートに対して受信フレームのミラーポートが割り当てられた状態となります。従って，1 つのモニターポートの受信フレーム（rx/both）に対するミラーポートは，ホワイトリスト機能，ICMP 限定ミラーリング機能と合わせて最大 2 ポートとなります。

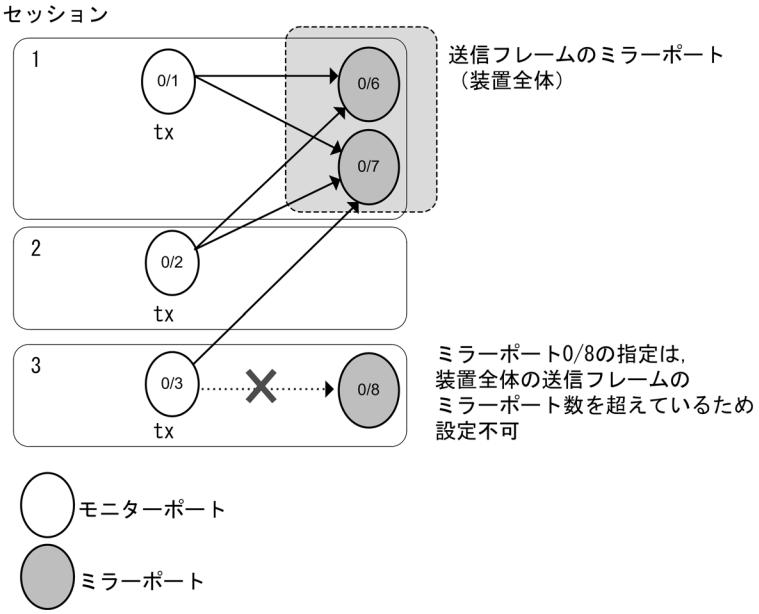
＜図内のセッション 2 について＞

ホワイトリスト機能のミラーポート 0/10 が設定されているため，全ポートにミラーポート 0/10 が割り当てられた状態となっています。
従って，ホワイトリスト機能のミラーポート 0/10 が設定されているため，ポート 0/2 に対する受信フレームのミラーポートは，ポート 0/8 を設定できますが，ポート 0/9 は最大 2 ポートを超えるため設定できません。

＜図内のポート 0/3 について＞

ポート 0/3 に ICMP 限定ミラーリングを設定します。
ホワイトリスト機能のミラーポート 0/10 が設定されているため，全ポートにミラーポート 0/10 が割り当てられた状態となっています。
従って，ICMP 限定ミラーリングのミラーポートは，ポート 0/6，0/8 ～ 0/9 のいずれか 1 つと，0/10 を設定できます。（図の例は，ポート 0/9 と 0/10 を設定しています。）
その他のポートは最大 2 ポートを超えるためミラーポートとして設定できません。

図 26-9 送信フレームのミラーポート数



送信フレーム（tx/both）に対するミラーポートの合計は，装置全体で最大 2 ポートです。

＜図内のセッション 3 について＞

ミラーポートはセッション間で重複設定可能です。ただし，装置全体の送信フレームのミラーポートは最大 2 ポートのため，ミラーポート 0/7 は設定できますが，ミラーポート 0/8 は設定できません。

26.1.2 ポートミラーリング使用時の注意事項

（1） 他機能との共存

1. スタック動作時のポートミラーリングについては，「コンフィグレーションガイド Vol.1　7. スタックの解説【OP-WLE】」を参照してください。
2. 以下のコンフィグレーションコマンドはミラーポートに設定できません。また，以下のコンフィグレーションコマンドを必要とする機能は，ミラーポートで使用できません。
   - switchport mode ※1※2
   - switchport access vlan
   - switchport trunk ※3
   - switchport mac
   - switchport protocol
   - no switchport mac auto-vlan
   - switchport vlan mapping enable
   - channel-group mode
   - dot1x port control
   - mac-authentication port
   - web-authentication port

   ※1 switchport mode access は設定可能ですが，ミラーポートはアクセスポートとして動作しません。

   ※2 switchport monitor dot1q tag が設定されているミラーポートでは，switchport mode trunk が設定可能です。

   ※3 switchport monitor dot1q tag が設定されているミラーポートでは設定可能です。
3. モニターポートでは，他の機能は制限なく動作します。
4. ICMP 限定ミラーリング機能を使用する場合は，以下に注意してください。
   - 受信側フロー検出モード

本機能を使用する場合は，受信側フロー検出モードをデフォルトコンフィグレーション（flow detection mode 未設定）のままにしてください。また，本機能を使用中は，受信側フロー検出モードを変更しないでください。
本機能を使用後に受信側フロー検出モードを変更する場合は，本機能のコンフィグレーションを削除した後，装置再起動が必要です。

- QoS フローリスト
本機能と QoS フローリストは併用できません。QoS フローリスト使用後に本機能を使用する場合は，QoS フローリストのコンフィグレーションを削除した後に，装置再起動が必要です。また，本機能を使用した後に QoS フローリストを使用する場合は，本機能のコンフィグレーションを削除した後，装置再起動が必要です。
- スタック
本機能はスタンドアロンでだけ使用可能です。スタックでは使用できません。

5. 802.1Q Tag 付与機能を使用する場合は，以下に注意してください。
   - Tag
   本機能で使用する Tag は，通常のコンフィグレーションコマンド vlan，interface vlan で設定していない VLAN ID を使用してください。
   また，VLAN 1 は装置デフォルトで存在するため，本機能で VLAN 1 は設定できません。
   - 送信フィルタ
   送信フィルタで VLAN 番号を抽出する条件は，1 段目の VLAN Tag に適用します。本機能で付与した Tag も 1 段目の VLAN Tag となりますが，本機能で付与した Tag は通常のレイヤ 2 機能として本装置に設定できません。
   従って，アクセスリストの VLAN 条件として指定できませんので，本機能で付与した Tag は，送信フィルタの VLAN 番号の抽出対象外となります。
   - スタック
   本機能はスタンドアロンでだけ使用可能です。スタックでは使用できません。

（2） ポートミラーリング使用時の注意事項

1. ポートミラーリングによりコピーしたフレームは，ミラーポートの回線帯域を超えて出力することはできません。
2. モニターポートとミラーポートはセッション間で重複設定可能です。ただし，すべてのミラーリング機能に対して，同一ポートをモニターポートとミラーポートに混在する設定はできません。
3. 受信したフレームの FCS が不正な場合，該当フレームをミラーリングしません。
4. 受信フレームのミラーリングでは，受信フィルタなどにより廃棄されるフレームもミラーリングされます。送信フレームのミラーリングでは，送信フィルタにより廃棄されるフレームもミラーリングされます。
5. ミラーポートに対して送信側フィルタを設定すると，ミラーリングされたフレームにも有効となります。フィルタで廃棄を設定した場合，ミラーリングされたフレームが廃棄されて，ミラーリングされません。
6. VLAN インタフェースに送信側フィルタを設定すると，ミラーリングされたフレームの VLAN ID が一致したときにも有効となります。フィルタで廃棄を設定した場合，ミラーリングされたフレームが廃棄されて，ミラーリングされません。
7. 送信フレームのミラーリングでは，自発フレームおよびハードウェアで中継するフレームをミラーリングします。ただし，一部の送信フレームはミラーリングしません。詳細は「表 26-3　ミラーリングできない送信フレーム」を参照してください。
   受信フレームのミラーリングでは，自宛フレームなどすべての受信フレームをミラーリングします。
8. 送信フレームのミラーリングで複数モニターポートを設定し，そのすべてまたは一部のポートにフレームをフラッディングする場合，1 個のフレームをミラーリングします。

スタック動作時は，「コンフィグレーションガイド Vol.1 7. スタックの解説【OP-WLE】」を参照してください。

9. 送信フレームのミラーリングでは，Untagged フレームを送信する場合でも，送信フレームの VLAN の Tag を持つ Tagged フレームをミラーリングします。
10. 送信フレームのミラーリングでは，送信ポートに Tag 変換が設定されていても，LAN 上で使用する VLAN Tag ではなく，送信フレームの VLAN の Tag を持つ Tagged フレームがミラーリングされます。
11. 送信フレームのミラーリングでは，モニターポートから送信されるフレームの順序と異なる順序で送信されることがあります。
12. ミラーリングのセッション数とミラーポート数には制限があります。
詳細は，前述の「26.1.1　ポートミラーリングの概要 （3）サポート範囲」を参照してください。
13. ミラーポートで下記機能が有効時，ミラーポートから制御フレームを送信します。
    - LLDP：LLDP フレーム
    - IEEE802.3ah/UDLD：UDLD フレーム
    - スパニングツリー：BPDU フレーム
      なお，スパニングツリーはデフォルトコンフィグレーションで有効です。BPDU フレーム送信を停止したいときは，コンフィグレーションコマンド spanning-tree disable を設定するか，またはミラーポートに BPDU フィルタ機能（コンフィグレーションコマンド spanning-tree bpdufilter）を設定してください。
14. 送信フレームのミラーリングでは，次に示す状態でモニターポートが通信できない場合でも，フレームによってはミラーリングされます。
    - スパニングツリーによる Blocking，Discarding，Listening，および Learning 状態
    - Ring Protocol によるブロッキング状態
    - アップリンク・リダンダントでのスタンバイポート

    ミラーリングされるフレームを次に示します。
    - フラッディングされるフレーム
    - モニターポートの状態を送信禁止にする際に実施する MAC アドレステーブルのクリア処理中に，MAC アドレステーブルエントリに一致したフレーム
15. 送信フレームのミラーリングでは，モニターポートの MTU 超過により廃棄されるフレームもミラーリングされます。
16. ミラーリングされたフレームは，ミラーポートの MTU に影響されません。ミラーポートの MTU を超えるフレームもミラーリングされます。
17. 送信フレームのミラーリングは，モニターポートのポート帯域制御に影響されません。しかし，ポート帯域制御による送信キュー溢れで廃棄される送信フレームはミラーリングされません。
18. ホワイトリスト機能使用時に未学習の Untagged パケットをミラーリングする場合，ミラーポートからは Tagged パケットが送信されます。【08TF】
19. VLAN Tag の TPID の設定を使用している場合，送信フレームをミラーリングしたフレームの TPID はミラーポートの TPID になります。
20. 802.1Q Tag 付与機能を使用しているミラーポートにミラーリングされるフレームが，同じポートにレイヤ 2 中継される場合，中継先ポートの MTU を超過していても廃棄されない場合があります。

表 26-3　ミラーリングできない送信フレーム

フレームの種類		条件
IGMP	本装置からの IGMP クエリー送信	IGMP snooping 機能有効時
	IGMP フレーム中継	

フレームの種類		条件
MLD	本装置からの MLD フレーム送信	MLD snooping 機能有効時
	本装置からの MLD クエリー送信	
	MLD フレーム中継	
DHCP	DHCP フレームの中継	DHCP snooping 機能有効時
ARP	ARP フレームの中継	ダイナミック ARP 検査機能有効時
LLDP	本装置からの LLDP フレーム送信	－
UDLD	本装置からの UDLD フレーム送信	－
LACP	本装置からの LACP フレーム送信	－
EAPOL	本装置からの EAPOL フレーム送信	－
BPDU	本装置からの BPDU フレーム送信	－
L2 ループ検知	本装置からの L2 ループ検知フレーム送信	－
アップリンク・リダンダント	本装置からのフラッシュ制御フレーム送信	－
	本装置からの MAC アドレスアップデートフレーム送信	－
GSRP aware	GSRP aware フレーム中継	－
CFM	本装置からの CFM フレーム送信	－
	CFM フレーム中継	CFM 機能有効時
Ring Protocol	本装置からのヘルスチェックフレーム送信など	－

26.2 コンフィグレーション

26.2.1 コンフィグレーションコマンド一覧

ポートミラーリングのコンフィグレーションコマンド一覧を次の表に示します。

表 26-4 コンフィグレーションコマンド一覧

コマンド名	説明
ip icmp monitor destination interface	ICMP フレームに限定したポートミラーリング機能を設定します。
monitor session source	ポートミラーリングを設定します。
switchport monitor dot1q tag	ミラーリング機能で該当ポートがミラーポートに指定された場合，ミラーリング対象フレームに指定した 802.1Q Tag を付与して送信します。

26.2.2 ポートミラーリングの設定

ポートミラーリングのコンフィグレーションでは，モニターポートとミラーポートの組み合わせをモニターセッションとして設定します。本装置でのモニターセッション数とセッション番号は次のとおりです。

- スタック動作時　　：最大 1 組，セッション番号は 1 固定
- スタンドアロン動作時：最大 4 組，組み合わせごとに 1 から 4 のセッション番号を使用可能

設定したモニターセッションを削除する場合は，設定時のセッション番号を指定して削除します。設定済みのセッション番号を指定すると，モニターセッションの設定内容は変更されて，以前のモニターセッションの情報は無効になります。

また，スタンドアロン動作時は，add/remove 指定によりモニターポートの一部を追加または削除することもできます。

モニターポートには，通信で使用するポートを指定します。ミラーポートには，トラフィックの監視や解析などのために，アナライザなどを接続するポートを指定します。

なお，ミラーポートの 802.1Q Tag 付与機能を使用することで，レイヤ 2 中継に使用しているトランクポートをミラーポートとして指定することも可能です。

(1) 受信フレームのミラーリング

[設定のポイント]

設定できるインタフェースはイーサネットインタフェース，またはポートチャネルインタフェースです。また，ミラーポートは VLAN などを設定していないポートに設定します。

[コマンドによる設定]

1. **(config)# monitor session 1 source interface gigabitethernet 0/1 rx destination interface gigabitethernet 0/5**
   アナライザをポート 0/5 に接続し，ポート 0/1 で受信するフレームをミラーリングすることを設定します。

(2) 送信フレームのミラーリング

[設定のポイント]

設定できるインタフェースはイーサネットインタフェース，またはポートチャネルインタフェースで

す。また，ミラーポートはVLANなどを設定していないポートに設定します。

[コマンドによる設定]

1. **(config)# monitor session 1 source interface gigabitethernet 0/2 tx destination interface gigabitethernet 0/6**
   アナライザをポート0/6に接続し，ポート0/2で送信するフレームをミラーリングすることを設定します。

(3) 送受信フレームのミラーリング

[設定のポイント]
設定できるインタフェースはイーサネットインタフェース，またはポートチャネルインタフェースです。また，ミラーポートはVLANなどを設定していないポートに設定します。

[コマンドによる設定]

1. **(config)# monitor session 1 source interface gigabitethernet 0/3 both destination interface gigabitethernet 0/10**
   アナライザをポート0/10に接続し，ポート0/3で送受信するフレームをミラーリングすることを設定します。

(4) 複数モニターポートのフレームのミラーリング（多対1）

[設定のポイント]
複数のモニターポートをリスト形式で設定できます。ミラーポートは1ポート（多対1）で設定します。

[コマンドによる設定]

1. **(config)# monitor session 1 source interface gigabitethernet 0/3-5 both destination interface gigabitethernet 0/10**
   アナライザをポート0/10に接続し，ポート0/3～0/5で送受信するフレームをミラーリングすることを設定します。

(5) 複数モニターポートのフレームのミラーリング（多対2）

[設定のポイント]
複数のモニターポートをリスト形式で設定できます。ミラーポートは2ポート（多対2）で設定します。

[コマンドによる設定]

1. **(config)# monitor session 1 source interface gigabitethernet 0/3-5 both destination interface gigabitethernet 0/9-10**
   アナライザをポート0/9と0/10に接続し，ポート0/3～0/5で送受信するフレームをミラーリングすることを設定します。

[注意事項]
ミラーポートを2ポート設定した場合も，モニターポートの設定に従い2ポートとも同じ種別のデータをミラーリングします。ミラーポートごとに送信，受信，送受信を分けることはできません。

(6) モニターポートの変更

スタンドアロン動作時は，設定済みのモニターポートを変更できます。

[設定のポイント]

任意のセッションに，複数のモニターポートを設定します。
monitor session <session no.> source interface add コマンドおよび monitor session <session no.> source interface remove コマンドで，設定済みのモニターポートを変更します。

[コマンドによる設定]

1. **(config)# monitor session 2 source interface gigabitethernet 0/3-5 both destination interface gigabitethernet 0/10**
   セッション 2 にアナライザをポート 0/10 に接続し，ポート 0/3 ～ 0/5 で送受信するフレームをミラーリングするよう設定します。

2. **(config)# monitor session 2 source interface add gigabitethernet 0/8**
   セッション 2 のモニターポートに，ポート 0/8 を追加します。

3. **(config)# monitor session 2 source interface remove gigabitethernet 0/3**
   セッション 2 のモニターポートから，ポート 0/3 を削除します。

26.2.3 ICMP 限定ミラーリング機能の設定

[設定のポイント]

前提条件として以下の状態とします。

- 受信側フロー検出モード layer2-2（flow detection mode 未設定）
- QoS フローリスト未使用
- monitor session source コマンドで受信フレーム（rx/both）のミラーポート 0/7 ～ 0/10 が設定されている

任意のポートに，ICMP 限定ミラーリングを設定します。ミラーポートは 0/7 ～ 0/10 のいずれかを設定します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 0/3**
   (config-if)# ip icmp monitor destination interface gigabitethernet 0/9-10
   (config-if)# exit
   ポート 0/3 で受信した ICMP フレームを，ポート 0/9 ～ 0/10 へミラーリングします。

26.2.4 802.1Q Tag 付与機能の設定

[設定のポイント]

設定できるインタフェースはイーサネットインタフェース，またはポートチャネルインタフェースです。また，本機能で使用する Tag は，通常のコンフィグレーションコマンド vlan，interface vlan で設定していない VLAN ID を最大 1 つ設定します。本例では，ミラーポートはレイヤ 2 中継に使用するポートを指定するものとし，トランクポートに設定します。
なお，レイヤ 2 中継に使用する VLAN100，200，300 は vlan コマンドで設定済とします。

［コマンドによる設定］

1. **(config)# monitor session 1 source interface gigabitethernet 0/3 both**
   destination interface gigabitethernet 0/10
   ポートミラーリングを設定します。

2. **(config)# interface gigabitethernet 0/10**
   (config-if)# switchport monitor dot1q tag 1000
   ミラーリング対象フレームに付与する Tag 1000 を指定します。

3. **(config-if)# switchport mode trunk**
   (config-if)# switchport trunk allowed vlan 100,200,300
   (config-if)# exit
   ミラーポートをトランクポートに設定します。また，VLAN 100，200，300 を設定します。（VLAN 100，200，300 はレイヤ 2 中継用の例です。）

27 ポリシーベースミラーリング

ポリシーベースミラーリングは，受信するフレームをフロー単位でコピーし，指定したポートへ送信する機能です。この章では，ポリシーベースミラーリングの解説と操作方法について説明します。

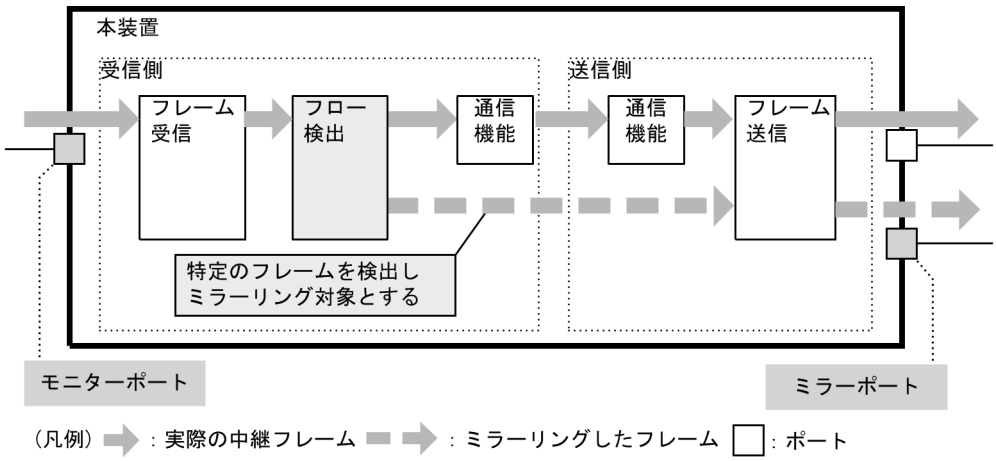
27.1 解説

27.1.1 概要

ポリシーベースミラーリングは，受信するフレームから特定のフローをコピーし，指定した物理ポートへ送信する機能です。フレームをコピーすることを**ミラーリング**と呼びます。この機能を利用して，フロー単位でミラーリングしたフレームをアナライザなどで受信することによって，トラフィックの監視や解析ができます。

受信フレームに対するポリシーベースミラーリングの動作を次の図に示します。

図 27-1 受信フレームに対するポリシーベースミラーリングの動作



上記の図で示すとおり，トラフィックを監視する物理ポートを**モニターポート**と呼び，ミラーリングしたフレームの送信先となる物理ポートを**ミラーポート**と呼びます。

本装置のポリシーベースミラーリングは，フロー検出によりきめ細やかなフレーム特定を行うことができます。また，最大 2 つのミラーポートに同時にコピーすることができます。

(1) 基本仕様

トラフィックの監視や解析などのために，アナライザなどを接続するポートをミラーポートに設定します。ミラーポートはミラーリング専用のポートになります。

モニターポートとミラーポートの組み合わせをモニターセッションと呼びます。本装置では，最大 2 つのモニターセッションを設定できます。（スタック動作時は 1 セッションです。）

モニターポートとミラーポートは，次に示す組み合わせで使用できます。

- 1 モニターポート対 1 ミラーポート
- 1 モニターポート対複数ミラーポート（最大 2 ミラーポート）
- 複数モニターポート対 1 ミラーポート
- 複数モニターポート対複数ミラーポート（最大 2 ミラーポート）

なお，モニターポートおよびミラーポートにはそれぞれ異なる速度のポートを設定できます。ただし，ミラーリングしたフレームは，ミラーポートの回線帯域内で送信するため，回線帯域を超えたフレームは廃棄します。

(2) モニターポート

ポリシーベースミラーリングのモニターポートは，ポートミラーリングの monitor session source で設定します。対象フローを特定するアクセスリストを同じモニターセッション番号に指定することで，当該モニターポートの受信フレームに対してフロー検出条件を適用します。設定する場合は，受信側フロー検出モードをポリシーベースミラーリング対応（layer2-1-mirror または layer2-2-mirror）に設定してください。

詳細なフロー検出条件などについては，「1　フィルタ」を参照してください。

(3) ミラーポート

ポリシーベースミラーリングのミラーポートは，ポートミラーリングの monitor session source で設定します。ただし，装置全体で使用可能なミラーポート数には制限があります。詳細は「26　ポートミラーリング　(3) サポート範囲」を参照してください。

(4) 受信フレームのミラーリング

モニターポートで受信するすべてのフレームに対してフロー条件を適用し，フロー条件に一致したフレームが，ミラーリングの対象となります。ただし，受信したフレームに異常があるときはミラーリングしません。

27.1.2 ポリシーベースミラーリング使用時の注意事項

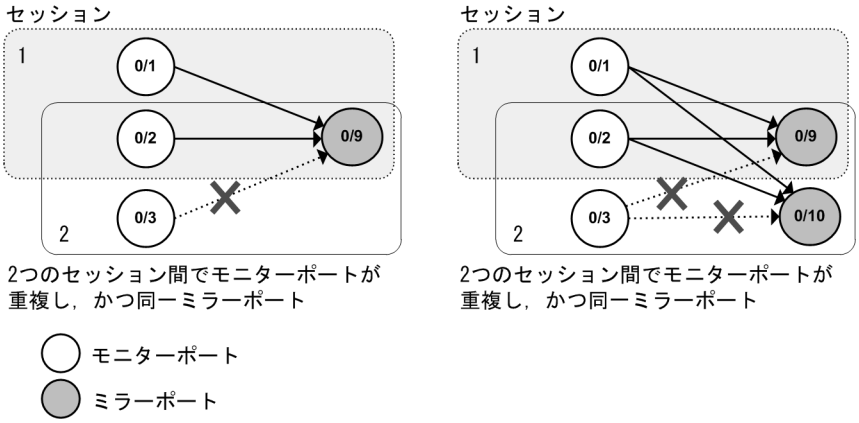
(1) 他機能との共存

1. 本機能使用時は，QoS フロー検出機能，ICMP 限定ミラーリング機能を使用できません。
2. スタック動作時のポートミラーリングについては，「コンフィグレーションガイド Vol.1　7. スタックの解説【OP-WLE】」を参照してください。
3. 本機能とホワイトリスト未学習パケットのミラーリング機能と併用可能です。本機能とホワイトリスト未学習パケットのミラーリング機能の両方の条件に該当したとき，双方のミラーポートが異なる場合はそれぞれのミラーポートに出力します。ミラーポートが同一の場合でも，受信パケット分だけを出力します。パケットの重複出力はありません。

(2) ポリシーベースミラーリング使用時の注意事項

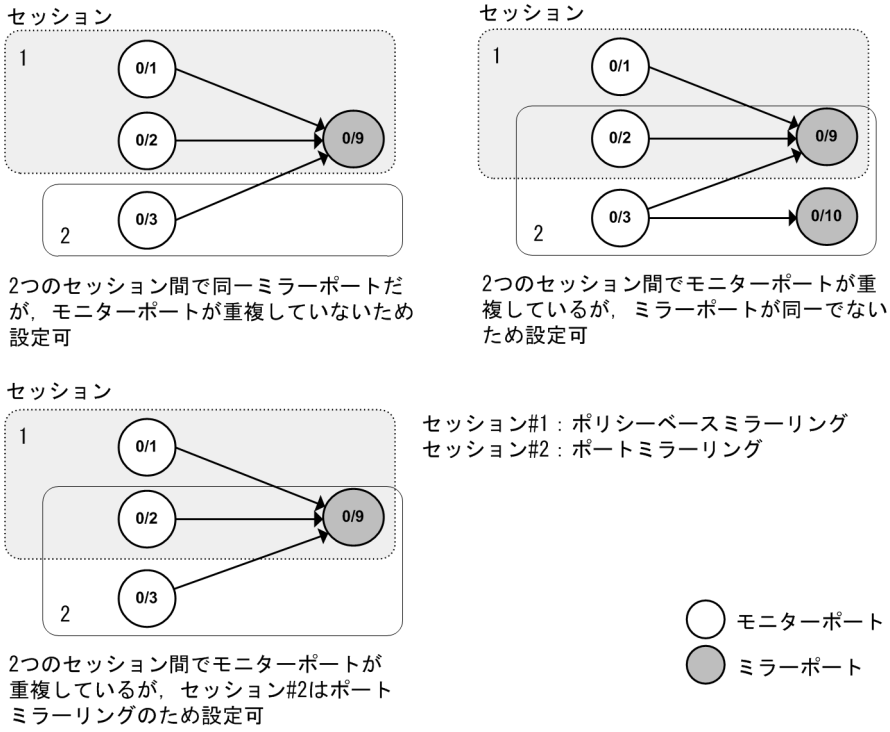
1. ポリシーベースミラーリングのモニターポートおよびミラーポートは，ポートミラーリングの同じセッション番号の monitor session source 設定を適用します。monitor session source 設定では，トラフィック方向を "rx"（受信フレームのミラー）で設定してください。"tx" や "both" の場合は，本機能を使用できません。
2. ポリシーベースミラーリングによりコピーしたフレームは，ミラーポートの回線帯域を超えて出力することはできません。
3. ポリシーベースミラーリングを複数セッション設定する場合，セッション間でモニターポートが重複し，かつ同一ミラーポートとなる設定はできません。
   設定不可の組み合わせを次の図に示します。

図 27-2 設定不可の組み合わせ



複数セッションを設定する場合は，モニターポートとミラーポートを次の図に示すような組み合わせで設定してください。

図 27-3 設定可能な組み合わせ



上記以外のモニターポート，ミラーポート，受信フレームのミラーリングに関する注意事項は，ポートミラーリングと同様です。「26 ポートミラーリング 26.1.2 ポートミラーリング使用時の注意事項」を参照してください。

4. ミラーリングのセッション数とミラーポート数には制限があります。詳細は，前述の「26 ポートミラーリング (3) サポート範囲」を参照してください。

27.2　コンフィグレーション

27.2.1　コンフィグレーションコマンド一覧

ポリシーベースミラーリングのコンフィグレーションコマンド一覧を次の表に示します。

表 27-1　コンフィグレーションコマンド一覧

コマンド名	説明
flow detection mode※1	受信側フロー検出モードを設定します。
ip access-list extended ※2	ポリシーベースミラーリングの対象フレームを IPv4 パケットフィルタで検出するアクセスリストを設定します。
ip access-list standard※2	ポリシーベースミラーリングの対象フレームを IPv4 アドレスフィルタで検出するアクセスリストを設定します。
mac access-list extended ※2	ポリシーベースミラーリングの対象フレームを MAC フィルタで検出するアクセスリストを設定します。
monitor session filter	モニターポートに適用するポリシーベースミラーリングのフロー検出条件（アクセスリスト）を設定します。
monitor session source	ポートミラーリングを設定します。
permit※2	対象フレームを検出するフロー検出条件をアクセスリストに指定します。

注 ※1

「コンフィグレーションコマンドレファレンス　21. フロー検出モード」を参照してください。

注 ※2

「コンフィグレーションコマンドレファレンス　22. アクセスリスト」を参照してください。

27.2.2　ポリシーベースミラーリングの設定

複数モニターポート対 1 ミラーポート，複数モニターポート対複数ミラーポートで使用する例を示します。複数モニターポート，複数ミラーポートなどモニターセッションの設定は，「26.1.2　ポートミラーリング使用時の注意事項」も合わせて参照してください。

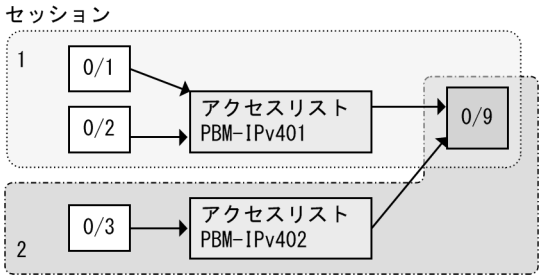
なお，ポリシーベースミラーリングでのモニターセッション数とセッション番号は次のとおりです。

- スタック動作時　　：最大 1 組，セッション番号は 1 固定
- スタンドアロン動作時：最大 2 組，1 から 4 のセッション番号を最大 2 つ使用可能

（1）複数モニターポート対 1 ミラーポートの設定

複数のモニターポートで別々のフロー検出条件に一致したフレームを，1 つのミラーポートへミラーリングする例です。

図 27-4 複数モニターポート対 1 ミラーポートの設定例



［設定のポイント］

IPv4 条件で検出する場合を例とし，以下の順で設定します。

1. 受信側フロー検出モード：layer2-2-mirror
2. セッション番号 1 のフロー検出条件：アクセスリスト PBM-IPv401，宛先 IP アドレス 10.0.0.1 のフレーム（permit で指定）
3. セッション番号 2 のフロー検出条件：アクセスリスト PBM-IPv402，宛先 IP アドレス 20.0.0.1 のフレーム（permit で指定）
4. セッション番号 1 にポリシーベースミラーリングのフロー検出条件として PBM-IPv401 を割り当て
5. セッション番号 2 にポリシーベースミラーリングのフロー検出条件として PBM-IPv402 を割り当て
6. セッション番号 1 にモニターポートとミラーポートを設定（同じセッション番号で rx を指定）
7. セッション番号 2 にセッション番号 1 と同じミラーポートを設定します。モニターポートはセッション番号 1 と重複しないポートを設定

［コマンドによる設定］

1. **(config)# flow detection mode layer2-2-mirror**
   受信側フロー検出モードを layer2-2-mirror に設定します。

2. **(config)# ip access-list extended PBM-IPv401**
   (config-ext-nacl)# permit ip any host 10.0.0.1
   (config-ext-nacl)# exit
   宛先 IP アドレス 10.0.0.1 のフレームを検出条件とします。

3. **(config)# ip access-list extended PBM-IPv402**
   (config-ext-nacl)# permit ip any host 20.0.0.1
   (config-ext-nacl)# exit
   宛先 IP アドレス 20.0.0.1 のフレームを検出条件とします。

4. **(config)# monitor session 1 filter ip access-group PBM-IPv401**
   セッション番号 1 にポリシーベースミラーリングのフロー検出条件として，アクセスリスト PBM-IPv401 を割り当てます。

5. **(config)# monitor session 2 filter ip access-group PBM-IPv402**
   セッション番号 2 にポリシーベースミラーリングのフロー検出条件として，アクセスリスト PBM-IPv402 を割り当てます。

6. **(config)# monitor session 1 source interface gigabitethernet 0/1-2 rx destination interface gigabitethernet 0/9**
   セッション番号 1 にモニターポート 0/1 ～ 0/2 とミラーポート 0/9 を設定します。トラフィック方向は "rx" を指定してください。

7. **(config)# monitor session 2 source interface gigabitethernet 0/3 rx destination interface gigabitethernet 0/9**
   セッション番号 2 にモニターポート 0/3 とミラーポート 0/9 を設定します。トラフィック方向は "rx" を指定してください。

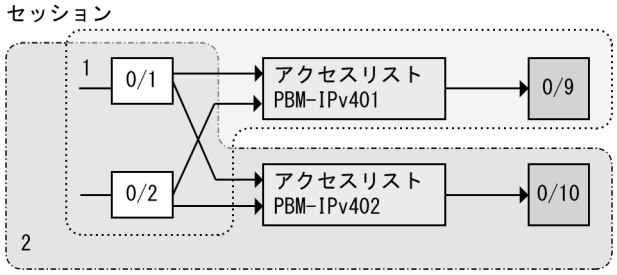
［注意事項］

1. 受信側フロー検出モードは layer2-1-mirror，または layer2-2-mirror を設定してください。
2. ポリシーベースミラーリングだけで使用する場合は，ポリシーベースミラーリングのフロー条件（monitor session filter）とポートミラーリング（monitor session source）で，同じセッション番号を使用してください。
3. ポートミラーリングのトラフィック方向は，"rx" で指定してください。"tx" や "both"（デフォルトコンフィグレーション含む）の場合は，ポリシーベースミラーリングを使用できません。
4. モニターポートとミラーポートの組み合わせについては，「(2) ポリシーベースミラーリング使用時の注意事項」も参照してください。

(2) 複数モニターポート対複数ミラーポートの設定

同じモニターポートから受信したフレームに対して，別々のフロー検出条件を適用し，それぞれ別のミラーポートへミラーリングする例です。

図 27-5 複数モニターポート対複数ミラーポートの設定例



［設定のポイント］

IPv4 条件で検出する場合を例とし，以下の順で設定します。

1. 受信側フロー検出モード：layer2-2-mirror
2. セッション番号 1 のフロー検出条件：アクセスリスト PBM-IPv401，宛先 IP アドレス 10.0.0.1 のフレーム（permit で指定）
3. セッション番号 2 のフロー検出条件：アクセスリスト PBM-IPv402，宛先 IP アドレス 20.0.0.1 のフレーム（permit で指定）
4. セッション番号 1 にポリシーベースミラーリングのフロー検出条件として PBM-IPv401 を割り当て
5. セッション番号 2 にポリシーベースミラーリングのフロー検出条件として PBM-IPv402 を割り当て
6. セッション番号 1 にモニターポートとミラーポートを設定（同じセッション番号で rx を指定）
7. セッション番号 2 にセッション番号 1 と同じモニターポートを設定します。ミラーポートはセッション番号 1 と重複しないポートを設定

［コマンドによる設定］

1. **(config)# flow detection mode layer2-2-mirror**
   受信側フロー検出モードを layer2-2-mirror に設定します。

2. **(config)# ip access-list extended PBM-IPv401**
   (config-ext-nacl)# permit ip any host 10.0.0.1
   (config-ext-nacl)# exit
   宛先 IP アドレス 10.0.0.1 のフレームを検出条件とします。

3. **(config)# ip access-list extended PBM-IPv402**
   (config-ext-nacl)# permit ip any host 20.0.0.1
   (config-ext-nacl)# exit
   宛先 IP アドレス 20.0.0.1 のフレームを検出条件とします。

4. **(config)# monitor session 1 filter ip access-group PBM-IPv401**
   セッション番号 1 にポリシーベースミラーリングのフロー検出条件として，アクセスリスト PBM-IPv401 を割り当てます。

5. **(config)# monitor session 2 filter ip access-group PBM-IPv402**
   セッション番号 2 にポリシーベースミラーリングのフロー検出条件として，アクセスリスト PBM-IPv402 を割り当てます。

6. **(config)# monitor session 1 source interface gigabitethernet 0/1-2 rx**
   destination interface gigabitethernet 0/9
   セッション番号 1 にモニターポート 0/1 ～ 0/2 とミラーポート 0/9 を設定します。トラフィック方向は "rx" を指定してください。

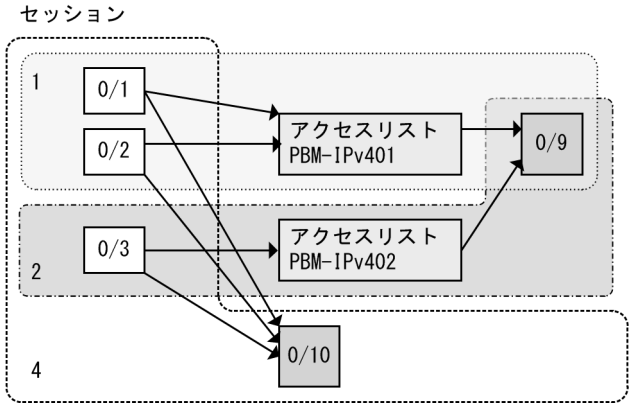
7. **(config)# monitor session 2 source interface gigabitethernet 0/1-2 rx**
   destination interface gigabitethernet 0/10
   セッション番号 2 にモニターポート 0/1 ～ 0/2 とミラーポート 0/10 を設定します。トラフィック方向は "rx" を指定してください。

［注意事項］
「(1) 複数モニターポート対 1 ミラーポートの設定」の注意事項を参照してください。

27.2.3 ポートミラーリングと併用

セッション番号を別々に指定することで，装置内でポリシーベースミラーリングとポートミラーリングを併用できます。

図 27-6 ポートミラーリングと併用



［設定のポイント］

1. セッション 1 と 2 でポリシーベースミラーリングにより，フロー検出条件に一致したフレームだけをミラーリングします。ポリシーベースミラーリングの設定については，「27.2.2 ポリシーベースミラーリングの設定 (1) 複数モニターポート対 1 ミラーポートの設定」を参照してください。
2. セッション 4 にポートミラーリングを設定し，セッション 1 ～ 2 で受信したフレームを，ミラーリングするよう設定します。

［コマンドによる設定］

1. **(config)# flow detection mode layer2-2-mirror**
   受信側フロー検出モードを layer2-2-mirror に設定します。以下，ポリシーベースミラーリングの設定は，「27.2.2 ポリシーベースミラーリングの設定 (1) 複数モニターポート対 1 ミラーポートの設定」と同じとします。

2. **(config)# monitor session 4 source interface gigabitethernet 0/1-3 both destination interface gigabitethernet 0/10**
   セッション番号 4 にモニターポート 0/1 ～ 0/3 とミラーポート 0/10 を設定します。

［注意事項］

1. スタック動作時は 1 セッションだけとなりますので，ポリシーベースミラーリングかポートミラーリングのどちらかで運用してください。

27.3 オペレーション

27.3.1 運用コマンド一覧

ポリシーベースミラーリングの運用コマンド一覧を次の表に示します。

表 27-2

コマンド名	説明
show monitor session	ポリシーベースミラーリングでフロー検出条件に適用した内容および一致したパケット数を表示します。
clear monitor session statistics	show monitor session で表示するパケット数を 0 クリアします。

27.3.2 ポリシーベースミラーリング情報の表示

本装置のポリシーベースミラーリングの統計情報は運用コマンド show monitor session により確認できます。ポリシーベースミラーリングのフロー条件に適用した内容，および一致したパケット数を表示します。

図 27-7 ポリシーベースミラーリングの統計情報表示例（スタック動作時）

```
> show monitor session

Date 20XX/12/09 17:57:33 UTC
Session no            : 1
Source interface      : 1/0/1-9,2/0/1-9
Destination interface : 1/0/10,2/0/10
Extended MAC access-list : ACL_MAC-P
  10 permit any any
    Matched packets
      Total    :  997542427
      Switch 1 : 3181028606
      Switch 2 :      42707

>
```

付録

付録 A　準拠規格

付録 A　準拠規格

付録 A.1　IEEE802.1X

表 A-1　IEEE802.1X の準拠規格および勧告

規格番号 (発行年月)	規格名
IEEE802.1X(2001 年 6 月)	Port-Based Network Access Control
RFC2865(2000 年 6 月)	Remote Authentication Dial In User Service (RADIUS)
RFC2866(2000 年 6 月)	RADIUS Accounting
RFC2868(2000 年 6 月)	RADIUS Attributes for Tunnel Protocol Support
RFC2869(2000 年 6 月)	RADIUS Extensions
RFC3162(2001 年 8 月)	RADIUS and IPv6
RFC3579(2003 年 9 月)	RADIUS Support For Extensible Authentication Protocol (EAP)
RFC3580(2003 年 9 月)	IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines
RFC3748(2004 年 6 月)	Extensible Authentication Protocol (EAP)

付録 A.2　Web 認証

表 A-2　Web 認証の準拠規格および勧告

規格番号 (発行年月)	規格名
RFC2865(2000 年 6 月)	Remote Authentication Dial In User Service (RADIUS)
RFC2866(2000 年 6 月)	RADIUS Accounting
RFC3162(2001 年 8 月)	RADIUS and IPv6

付録 A.3　MAC 認証

表 A-3　MAC 認証の準拠規格および勧告

規格番号 (発行年月)	規格名
RFC2865(2000 年 6 月)	Remote Authentication Dial In User Service (RADIUS)
RFC2866(2000 年 6 月)	RADIUS Accounting
RFC3162(2001 年 8 月)	RADIUS and IPv6

付録 A.4　IEEE802.3ah/UDLD

表 A-4　IEEE802.3ah/UDLD の準拠する規格および勧告

規格番号 (発行年月)	規格名
IEEE802.3ah(2004 年 9 月)	Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications Amendment: Media Access Control Parameters, Physical Layers, and Management Parameters for Subscriber Access Networks

付録 A.5　CFM

表 A-5　CFM の準拠規格および勧告

規格番号 (発行年月)	規格名
IEEE802.1ag-2007(2007 年 12 月)	Virtual Bridged Local Area Networks Amendment 5: Connectivity Fault Management

付録 A.6　SNMP

表 A-6　SNMP の準拠規格および勧告

規格番号 (発行年月)	規格名
RFC1155(1990 年 5 月)	Structure and Identification of Management Information for TCP/IP-based Internets
RFC1157(1990 年 5 月)	A Simple Network Management Protocol (SNMP)
RFC1901(1996 年 1 月)	Introduction to Community-based SNMPv2
RFC1902(1996 年 1 月)	Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC1903(1996 年 1 月)	Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC1904(1996 年 1 月)	Conformance Statements for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC1905(1996 年 1 月)	Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC1906(1996 年 1 月)	Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC1908(1996 年 1 月)	Coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework
RFC2578(1999 年 4 月)	Structure of Management Information Version 2 (SMIv2)
RFC2579(1999 年 4 月)	Textual Conventions for SMIv2
RFC2580(1999 年 4 月)	Conformance Statements for SMIv2
RFC3410(2002 年 12 月)	Introduction and Applicability Statements for Internet Standard Management Framework
RFC3411(2002 年 12 月)	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
RFC3412(2002 年 12 月)	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
RFC3413(2002 年 12 月)	Simple Network Management Protocol (SNMP) Applications
RFC3414(2002 年 12 月)	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
RFC3415(2002 年 12 月)	View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
RFC3416(2002 年 12 月)	Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)
RFC3417(2002 年 12 月)	Transport Mappings for the Simple Network Management Protocol (SNMP)
RFC3584(2003 年 8 月)	Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework

規格番号 (発行年月)	規格名
RFC3826(2004年 6月)	The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model
RFC7860(2016年 4月)	HMAC-SHA-2 Authentication Protocols in User-Based Security Model (USM) for SNMPv3

表 A-7　MIB の準拠規格および勧告 ※

規格番号 (発行年月)	規格名
IEEE8023-LAG-MIB (2000 年 3 月)	Aggregation of Multiple Link Segments
IEEE8021-PAE-MIB (2001 年 6 月)	Port-Based Network Access Control
IEEE8021-CFM-MIB (2007 年 12 月)	Virtual Bridged Local Area Networks Amendment 5: Connectivity Fault Management
RFC1158(1990 年 5 月)	Management Information Base for Network Management of TCP/IP-based internets: MIB-II
RFC1213(1991 年 3 月)	Management Information Base for Network Management of TCP/IP-based internets: MIB-II
RFC1493(1993 年 7 月)	Definitions of Managed Objects for Bridges
RFC1643(1994 年 7 月)	Definitions of Managed Objects for the Ethernet-like Interface Types
RFC1757(1995 年 2 月)	Remote Network Monitoring Management Information Base
RFC1907(1996 年 1 月)	Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC2011(1996 年 11 月)	SNMPv2 Management Information Base for the Internet Protocol using SMIv2
RFC2012(1996 年 11 月)	SNMPv2 Management Information Base for the Transmission Control Protocol using SMIv2
RFC2013(1996 年 11 月)	SNMPv2 Management Information Base for the User Datagram Protocol using SMIv2
RFC2233(1997 年 11 月)	The Interfaces Group MIB using SMIv2
RFC2674(1999 年 8 月)	Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions
RFC2863(2000 年 6 月)	The Interfaces Group MIB
RFC3411(2002年 12月)	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
RFC3412(2002年 12月)	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
RFC3413(2002年 12月)	Simple Network Management Protocol (SNMP) Applications
RFC3414(2002年 12月)	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
RFC3415(2002年 12月)	View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
RFC3418(2002 年 12 月)	Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)
RFC4022(2005 年 3 月)	Management Information Base for the Transmission Control Protocol (TCP)
RFC4113(2005 年 6 月)	Management Information Base for the User Datagram Protocol (UDP)
RFC4293(2006 年 4 月)	Management Information Base for the Internet Protocol (IP)

規格番号 (発行年月)	規格名
RFC4363(2006 年 1 月)	Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering, and Virtual LAN Extensions
LLDP-V2-MIB(2009年 6月)	Management Information Base module for LLDP configuration, statistics, local system data and remote systems data components.
LLDP-EXT-DOT1-V2-MIB (2009年 6月)	The LLDP Management Information Base extension module for IEEE 802.1 organizationally defined discovery information.

注 ※

一部の MIB だけ対象です。詳細は「MIB レファレンス」を参照してください。

付録 A.7　SYSLOG

表 A-8　SYSLOG の準拠する規格および勧告

規格番号 (発行年月)	規格名
RFC3164(2001 年 8 月)	The BSD syslog Protocol
RFC6587(2012 年 4 月)	Transmission of Syslog Messages over TCP

付録 A.8　sFlow

表 A-9　sFlow の準拠する規格および勧告

規格番号 (発行年月)	規格名
RFC3176(2001 年 9 月)	InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks

付録 A.9　LLDP

表 A-10　LLDP の準拠する規格および勧告

規格番号 (発行年月)	規格名
IEEE802.1AB/D6.0(2003 年 10 月)	Draft Standard for Local and Metropolitan Networks: Station and Media Access Control - Connectivity Discovery
IEEE Std 802.1AB-2005 (2005 年 5 月)	IEEE Standard for Local and metropolitan area networks: Station and Media Access Control Connectivity Discovery
IEEE Std 802.1AB-2009 (2009 年 9 月)	IEEE Standard for Local and Metropolitan Area Networks: Station and Media Access Control Connectivity Discovery

索引

数字

A

C

D

E

G

H

I

L

M

Q

R

S

T

U

V

W

あ

い

か

き

け

こ

さ

し

す

せ

そ

た

て

と

に

ね

は

ひ

ふ

ほ

ま

み

も

ゆ

り

れ

ろ