AX1200S 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. 1.4 対応

AX12S-S002-90

AlaxalA

■対象製品

このマニュアルは AX1200S モデルを対象に記載しています。また，AX1200S のソフトウェア Ver. 1.4 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-LT 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，外国為替および外国貿易法ならびに米国の輸出管理関連法規などの規制をご確認の上，必要な手続きをお取りください。
なお，ご不明な場合は，弊社担当営業にお問い合わせください。

■商標一覧

Ethernet は，米国 Xerox Corp. の商品名称です。
Microsoft は，米国およびその他の国における米国 Microsoft Corp. の登録商標です。
Windows は，米国およびその他の国における米国 Microsoft Corp. の登録商標です。
イーサネットは，富士ゼロックス（株）の商品名称です。
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

２０１０年　3月 （第１０版） ＡＸ １２ Ｓ － Ｓ ００２－９０

■著作権

変更履歴

【Ver. 1.4（第 10 版）】

表　変更履歴

章・節・項・タイトル	追加・変更内容
1　フィルタ	• 他機能と同時使用時の注意事項を追加しました。
6　IEEE802.1X の解説	• アカウント機能の記述を変更しました。
8　Web 認証の解説	• Web 認証専用 IP アドレスの記述を変更しました。 • URL リダイレクトをプロキシ環境で使用時の注意事項について記述を変更しました。
16　L2 ループ検知	• L2 ループ検知使用時の注意事項を追加しました。
18　ログ出力機能	• 解説の記述を変更しました。

なお，単なる誤字・脱字などはお断りなく訂正しました。

【Ver. 1.4（第 9 版）】

表　変更履歴

章・節・項・タイトル	追加・変更内容
事前準備（IEEE802.1X の解説）	• RADIUS 認証で使用する RADIUS 属性に，ポート単位認証（動的）の収容 VLAN として VLAN 名称指定を追加しました。（VLAN 単位認証（動的）も対象です。）
事前準備（Web 認証の解説）	• RADIUS 認証で使用する RADIUS 属性に，ダイナミック VLAN モードの収容 VLAN として VLAN 名称指定を追加しました。（レガシーモードも対象です。）
事前準備（MAC 認証の解説）	• RADIUS 認証で使用する RADIUS 属性に，ダイナミック VLAN モードの収容 VLAN として VLAN 名称指定を追加しました。（レガシーモードも対象です。）
レイヤ 2 認証の共通機能と共存使用	• ダイナミック VLAN モード収容 VLAN の VLAN 名称管理と設定について記述を追加しました。（レガシーモードも対象です。）
ポートミラーリング	• 注意事項を追加しました。 • コンフィグレーションのモニタポートの設定例を変更しました。

なお，単なる誤字・脱字などはお断りなく訂正しました。

【Ver. 1.4（第 8 版）】

表　変更履歴

章・節・項・タイトル	追加・変更内容
送信制御	• 送信キュー長指定の記述を追加しました。
レイヤ 2 認証機能の概説	• 従来のダイナミック VLAN モードをレガシーモードに名称を変更しました。 • 新たにダイナミック VLAN モードの記述を追加しました。
IEEE802.1X の解説	• 新たにポート単位認証（動的）の記述を追加しました。
IEEE802.1X の設定と運用	• 新たにポート単位認証（動的）の記述を追加しました。 • 認証除外の設定方法の記述を追加しました。
Web 認証の解説	• 従来のダイナミック VLAN モードをレガシーモードに名称を変更しました。 • 新たにダイナミック VLAN モードの記述を追加しました。
Web 認証の設定と運用	• 従来のダイナミック VLAN モードをレガシーモードに名称を変更しました。 • 新たにダイナミック VLAN モードの記述を追加しました。 • 認証除外の設定方法の記述を追加しました。

章・節・項・タイトル	追加・変更内容
MAC 認証の解説	• 従来のダイナミック VLAN モードをレガシーモードに名称を変更しました。 • 新たにダイナミック VLAN モードの記述を追加しました。
MAC 認証の設定と運用	• 従来のダイナミック VLAN モードをレガシーモードに名称を変更しました。 • 新たにダイナミック VLAN モードの記述を追加しました。 • 認証除外の設定方法の記述を追加しました。
レイヤ 2 認証の共通機能と共存使用	• 従来のダイナミック VLAN モードをレガシーモードに名称を変更しました。 • 新たにダイナミック VLAN モードの記述を追加しました。

なお，単なる誤字・脱字などはお断りなく訂正しました。

【Ver. 1.3（第 7 版）】

表　変更履歴

章・節・項・タイトル	追加・変更内容
Web 認証画面入れ替え機能使用時の注意事項	• 本項を追加しました。
コンフィグレーションコマンド一覧	• web-authentication ip address の説明を変更しました。
Web 認証のパラメータ設定	•「(1)Web 認証専用 IP アドレスの設定」にドメイン名設定を追加しました。
Web 認証の設定状態表示	• show web-authentication の画面例を変更しました。

なお，単なる誤字・脱字などはお断りなく訂正しました。

【Ver. 1.3（第 6 版）】

表　変更履歴

章・節・項・タイトル	追加・変更内容
サポート機能	•「(4)VLAN との共存仕様」を削除しました。VLAN との動作については，6 章，8 章，10 章の各認証機能を参照してください。
IEEE802.1X の動作条件と他機能を併用時の動作について	• IEEE802.1X の動作条件にプロトコル VLAN，プロトコルポートを追加しました。
解説（Web 認証）	• 表 8-2　Web 認証の動作条件を追加しました。
固定 VLAN モード（Web 認証）	• 固定 VLAN モードの記述を変更しました。
固定 VLAN モード使用時の注意事項（Web 認証）	•「(9) 本装置の内蔵 DHCP サーバの使用について」を追加しました。
Web 認証固有タグ（Web 認証）	•「(2) 注意事項」に「(c) バージョンアップ時の注意事項」を追加しました。
解説（MAC 認証）	• 表 10-1　ダイナミック VLAN モードでの強制認証ポート指定を追加しました。 • 表 10-2　MAC 認証の動作条件を追加しました。
認証機能（MAC 認証）	• ダイナミック VLAN モードに「(6) 強制認証ポート指定」を追加しました。
固定 VLAN モード（MAC 認証）	• 固定 VLAN モードの記述を追加しました。
アカウント機能（MAC 認証）	• ダイナミック VLAN モードの強制認証時のトラップ発行条件を追加しました。
MAC 認証の注意事項（MAC 認証）	• ダイナミック VLAN モード / 固定 VLAN モード共通の注意事項に「(5) 強制認証ポートの使用について」を追加し，固定 VLAN モード使用時の注意事項の「(4) 強制認証ポートの使用について」を削除しました。
認証処理に関する設定（MAC 認証）	• ダイナミック VLAN モードに「(5) 強制認証ポートの設定」を追加しました。
L2 ループ検知	• 本章を追加しました。

なお，単なる誤字・脱字などはお断りなく訂正しました。

【Ver. 1.3（第 5 版）】

表　変更履歴

章・節・項・タイトル	追加・変更内容
適合装置	下記のモデルを追加しました。 • AX-1230-24T2CA (AX1230S-24T2CA) • AX-1230-24P2CA (AX1230S-24P2CA)
レイヤ 2 認証機能の概説	• 本章を追加しました。
Web 認証の解説	• 固定 VLAN モードのサポートに伴い，「解説」を分離しました。
Web 認証の設定と運用	• 固定 VLAN モードのサポートに伴い，「設定と運用」を分離しました。
MAC 認証の解説	• 固定 VLAN モードのサポートに伴い，「解説」を分離しました。
MAC 認証の設定と運用	• 固定 VLAN モードのサポートに伴い，「設定と運用」を分離しました。
レイヤ 2 認証機能の共存	• 本章を追加しました。

なお，単なる誤字・脱字などはお断りなく訂正しました。

【Ver. 1.2（第 4 版）】

表　変更履歴

章・節・項・タイトル	追加・変更内容
フィルタ使用時の注意事項	•「(6) IP フィルタ条件適用の制限」を削除しました。
自発フレームのユーザ優先度の解説	• 本項を追加しました。
自発フレームのユーザ優先度のコンフィグレーション	• 本項を追加しました。
アカウント機能	• 本項を追加しました。
端末検出動作切り替えオプション	• shortcut/disable オプションをサポートしました。
コンフィグレーションコマンド一覧	• dot1x supplicant-detection，dot1x vlan dynamic supplicant-detection コマンドを追加しました。
認証モードオプションの設定	• 本項を追加しました。
アカウント機能	• アカウントログ情報にポート番号を追加サポートしました。 • プライベート Trap をサポートしました。
認証手順	• ログイン・ログアウト URL を共通化しました。
事前準備	• RADIUS サーバのユーザ ID とパスワードの文字数を 1 ～ 16 に変更しました。
認証エラーメッセージ	• 認証エラーメッセージを追加しました。
Web 認証画面入れ替え機能	• 本項を追加しました。
内蔵 DHCP サーバ機能の解説	• DHCP サーバの配布情報にルータオプション（default-router）を追加しました。
Web 認証画面作成手引き	• 本項を追加しました。
RADIUS 認証による MAC 認証	•「RADIUS サーバ問い合わせ時の MAC アドレス形式とパスワード」を追加しました。
アカウント機能	• アカウントログ情報にポート番号を追加サポートしました。 • プライベート Trap をサポートしました。
事前準備	• RADIUS サーバへ問い合わせ時の MAC アドレス形式とパスワードをコンフィグレーションで指定可能に変更しました。

章・節・項・タイトル	追加・変更内容
MAC 認証のパラメータ設定	• 「(5) RADIUS サーバ問い合わせ時の MAC アドレス形式の設定」を追加しました。 • 「(6) RADIUS サーバ問い合わせ時のパスワードの設定」を追加しました。 • 「(7) 認証端末数制限の設定」を追加しました。
GSRP の切り替え制御	• GSRP Flush Request フレームのフラッディングを追加しました。 • 「GSRP aware 使用時の注意事項」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. 1.1（第 3 版）】

表　変更履歴

章・節・項・タイトル	追加・変更内容
解説	• MAC 認証の認証 DB について追記しました。
ポートミラーリング使用時の注意事項	• 注意事項を追加しました。

なお，単なる誤字・脱字などはお断りなく訂正しました。

【Ver. 1.1（第 2 版）】

表　変更履歴

章・節・項・タイトル	追加・変更内容
適合装置	下記のモデルを追加しました。 • AX-1230-24P2C (AX1230S-24P2C) • AX-1230-48T2C (AX1230S-48T2C)
フィルタ	• フロー制御モードの記述を追加しました。(Layer2-1/Layer2-2) • IP アクセスリストの記述を追加しました。
QoS 制御の概要	• 本章を追加しました。
フロー制御	• 本章を追加しました。
送信制御	• スケジューリングについての記述を追加しました。 • ポート帯域制御についての記述を追加しました。
Web 認証	• 本章を追加しました。
MAC 認証	• 本章を追加しました。
ストームコントロール	• (2) ストームの検出と回復の検出についての記述を追加しました。
SNMP を使用したネットワーク管理	• RMON についての記述を追加しました。 • プライベート MIB/ トラップについての記述を追加しました。

なお，単なる誤字・脱字などはお断りなく訂正しました。

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AX1200Sモデルを対象に記載しています。また，AX1200Sのソフトウェア Ver. 1.4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-LT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。また，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。

■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

AX1200S
ハードウェア取扱説明書
(AX12S-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の確認を知りたい

コンフィグレーションガイド
Vol.1
(AX12S-S001)
Vol.2
(AX12S-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
(AX12S-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
(AX12S-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
(AX12S-S005)

●MIBについて調べる

MIBレファレンス
(AX12S-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
(AX12S-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
CDP	Cisco Discovery Protocol
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
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
MAC	Media Access Control
MC	Memory Card
MD5	Message Digest 5
MDI	Medium Dependent Interface
MDI-X	Medium Dependent Interface crossover
MIB	Management Information Base
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
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
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
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
UPC	Usage Parameter Control
UPC-RED	Usage Parameter Control - Random Early Detection
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

■常用漢字以外の漢字の使用について

このマニュアルでは，常用漢字を使用することを基本としていますが，次に示す用語については，常用漢字以外

を使用しています。

- 宛て (あて)
- 宛先 (あてさき)
- 溢れ (あふれ)
- 迂回 (うかい)
- 鍵 (かぎ)
- 個所 (かしょ)
- 筐体 (きょうたい)
- 桁 （けた）
- 毎 （ごと）
- 閾値 (しきいち)
- 芯 (しん)
- 溜まる (たまる)
- 誰 (だれ)
- 必須 (ひっす)
- 輻輳 (ふくそう)
- 閉塞 (へいそく)
- 漏洩 (ろうえい)

■ 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 3 編 レイヤ 2 認証

第 4 編　冗長化構成による高信頼化機能

第 5 編　ネットワークの障害検出による高信頼化機能

第 7 編　隣接装置情報の管理

第 8 編　ポートミラーリング

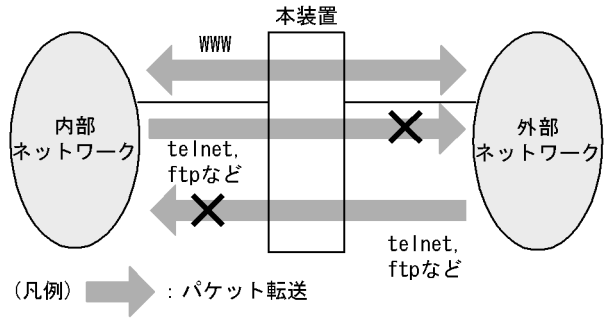
1 フィルタ

フィルタは，受信した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，受信した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。

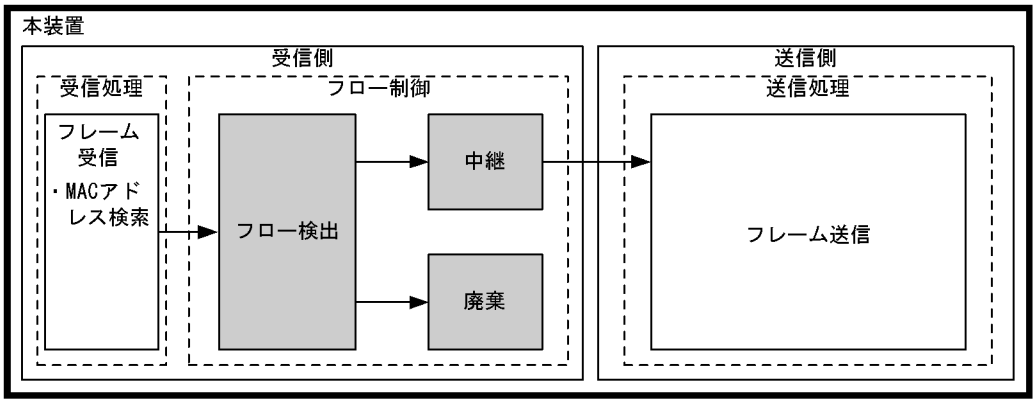
図 1-1 フィルタを使用したネットワーク構成例



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，「1.1.6　暗黙の廃棄」を参照してください。

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，「1.1.5　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，フロー検出モードによって変わります。なお，自発送信のフレームはフロー検出対象外です。

1.1.3　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二つのフロー検出モードを用意しています。使い方に合わせて選択してください。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，選択したフロー検出モードはフィルタ・QoS で共通です。

フロー検出モードを指定しない場合，layer2-2 がデフォルトのモードとして設定されます。

表 1-2　フロー検出モードとフロー動作の関係

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ロー制御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，きめ細かいフロー制御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 ヘッダでフレームを検出します。	イーサネット，VLAN

1.1.4　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指定します。フロー検出モードごとの指定可能なフロー検出条件を次の表に示します。

表 1-3　指定可能なフロー検出条件

種別		設定項目	layer2-1		layer2-2	
			イーサネット	VLAN	イーサネット	VLAN
MAC 条件	コンフィグレーション	VLAN ID ※1	○	－	－	－
	MAC ヘッダ	送信元 MAC アドレス	○	○	－	－
		宛先 MAC アドレス	○	○	－	－

種別		設定項目	layer2-1		layer2-2	
			イーサネット	VLAN	イーサネット	VLAN
		イーサネットタイプ	○	○	－	－
		ユーザ優先度※2	○	○	－	－
IPv4 条件	コンフィグレーション	VLAN ID※1	－	－	○	－
	MAC ヘッダ	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	－	－	○	○
		宛先ポート番号	－	－	○	○
		TCP 制御フラグ※4	－	－	○	○
	IPv4-UDP ヘッダ	送信元ポート番号	－	－	○	○
		宛先ポート番号	－	－	○	○

（凡例）○：指定できる　　－：指定できない

注※ 1

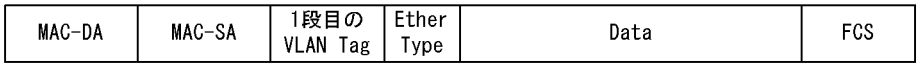
本装置のフロー検出で検出できる VLAN ID は，VLAN コンフィグレーションで入力した VLAN に対して付与する値です。入力フレームの属する VLAN ID を検出します。

注※ 2

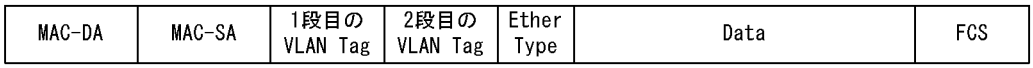
本装置では VLAN Tag なしのフレームについてはユーザ優先度を検出できません。常に，ユーザ優先度 3 として検出します。

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

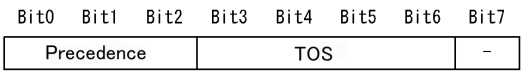


注※ 3

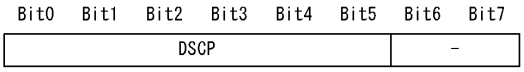
ToS フィールドの指定についての補足

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。



DSCP　　：ToS フィールドの上位 6 ビットの値です。



注※ 4
ack/fin/psh/rst/syn/urg フラグが 1 のパケットを検出します。

1.1.5 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 1-4 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	○	○※	○※
IPv4 条件	ip access-list	layer2-2	－	○	－

（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。また，アクセスリストごとに，フィルタエントリの検索は独立して実施します。そのため，フレームが複数のフィルタエントリに一致することがあります。複数のフィルタエントリに一致した場合，実際に動作するのは単一のフィルタエントリです。

（1）イーサネットインタフェースと VLAN インタフェース同時に一致した場合の動作

イーサネットインタフェースと，該当するイーサネットインタフェースが属している VLAN インタフェースに対してフィルタエントリを設定し，該当するイーサネットインタフェースからの受信フレームに対してフィルタを実施すると，複数のフィルタエントリに一致する場合があります。この場合，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）が優先となります。イーサネットインタフェース，および VLAN インタフェース共に中継動作を指定したフィルタエントリに一致する場合はイーサネットインタフェース上のフィルタエントリを優先します。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 1-5 複数のフィルタエントリに一致した場合の動作

複数フィルタエントリ一致となる組み合わせ		有効になるフィルタエントリ	
イーサネット	VLAN	インタフェース	動作
中継	中継	イーサネット	中継
中継	廃棄	VLAN	廃棄
廃棄	中継	イーサネット	廃棄
廃棄	廃棄	イーサネット	廃棄

この条件に該当するのは，フロー検出モード layer2-1，layer2-2 です。

1.1.6 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。

1.1.7 フィルタ使用時の注意事項

(1) 運用前のシステムファンクションリソース設定について

本機能は共用のシステムファンクションリソースを使用するため，他機能との同時動作には，システムファンクションリソースの設定が必要となります。システムファンクションリソース設定については，「コンフィグレーションガイド Vol.1 9.1.6 システムファンクションリソース配分の設定」を参照し，フィルタ機能以外の適切な機能も合わせて選択してください。

(2) 複数フィルタエントリー致時の動作

フレームが複数のフィルタエントリに一致した場合，一致したフィルタエントリの統計情報が採られます。

(3) 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。

(4) 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

(5) 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。

(6) 他機能との共存

(a) 他機能との同時使用について

フィルタ機能と下記に示す機能を同時に使用したときの動作を，次の表に示します。

表 1-6 フィルタ機能と他機能の同時使用について

機能	動作
DHCP snooping	フィルタ条件を設定したポートで DHCP snooping を運用すると，DHCP フレーム（ダイナミック ARP 検査有効時は ARP フレームも対象）に対してフィルタ機能が無効になり，中継してしまいます。
IGMP snooping	フィルタ条件を設定したポートで IGMP snooping を運用すると，IGMP フレームに対してフィルタ機能が無効になり，中継してしまいます。
MLD snooping	フィルタ条件を設定したポートで MLD snooping を運用すると，MLD フレームに対してフィルタ機能が無効になり，中継してしまいます。

(b) 他機能と同時運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
- プロトコル VLAN・MAC VLAN で，VLAN-Tag 付き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

(7) フィルタ条件適用の制限

チャネルグループで受信するフレームに対するフィルタ条件は，VLAN インタフェースに設定したアクセスグループのフィルタ条件だけを適用します。

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 1-7 コンフィグレーションコマンド一覧

コマンド名	説明
deny	MAC フィルタ・IPv4 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。
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	MAC フィルタ・IPv4 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) フロー検出モードの設定

フィルタの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]

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**
   フロー検出モード layer2-1 を有効にします。

(2) 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 src 0000.0000.0000 ffff.ffff.ffff dst 0000.0000.0000 ffff.ffff.ffff ethernet-type-string 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 src 0000.0000.0000 ffff.ffff.ffff dst 0000.0000.0000 ffff.ffff.ffff**
   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 fastethernet 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） フロー検出モードの設定

フィルタの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］

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**
   フロー検出モード layer2-2 を有効にします。

（2） 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 src 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。

(3) 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 src 0.0.0.0 255.255.255.255 dst 0.0.0.0 255.255.255.255 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 protocol ip src 0.0.0.0 255.255.255.255 dst 0.0.0.0 255.255.255.255**
   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 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。

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。

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 src 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 fastethernet 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 1-8 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) で設定したアクセスリスト (mac access-list，ip 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) で設定したアクセスリスト (mac access-list，ip 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 interface fastethernet 0/1

Date 2006/12/14 23:31:30 UTC
Using Port: interface fastethernet 0/1 in
Extended MAC access-list: only-appletalk
  remark "permit only appletalk"
  seq 1 permit src 0000.0000.0000 ffff.ffff.ffff dst 0000.0000.0000
ffff.ffff.ffff ethernet-type 0x814c vlan 1001 user-priority 1
    matched packets          :          256
  implicitly denied packets : 4294967295

>
```

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 1

Date 2007/03/09 15:55:48 UTC
Using Port: interface vlan 1 in
Extended IP access-list: telnet-server
  remark "permit only http server"
  seq 10 permit tcp src 0.0.0.0 255.255.255.255 dst 10.10.10.2 0.0.0.0 eq http
    matched packets          :           0
  implicitly denied packets :          14

>
```

指定した VLAN のフィルタに「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，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。

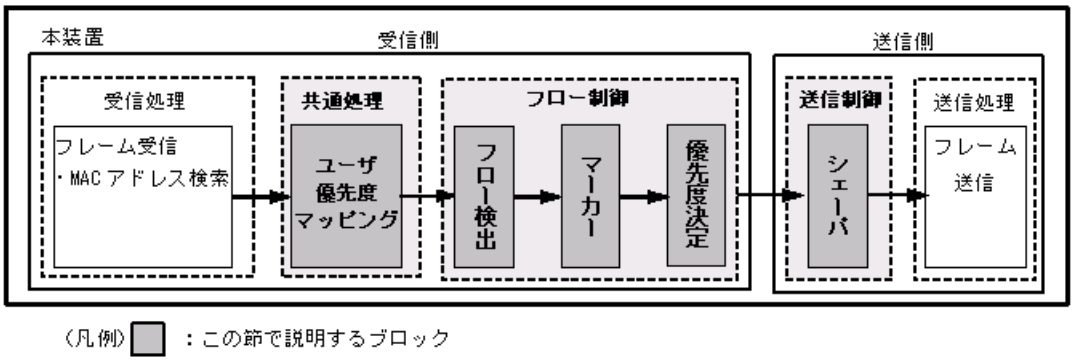
2.1　QoS 制御構造

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



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，ポート番号などの条件に一致するフローを検出します。
	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を決定します。
送信制御部	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，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，シェーパを実施します。

2.1.1 QoS 制御機能使用時の注意事項

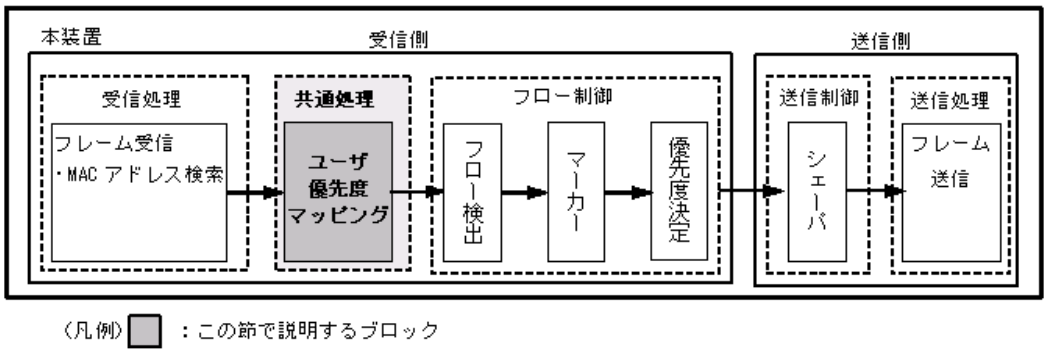
（1） 運用前のシステムファンクションリソース設定について

本機能は共用のシステムファンクションリソースを使用するため，他機能との同時動作には，システムファンクションリソースの設定が必要となります。システムファンクションリソース設定については，「コンフィグレーションガイド Vol.1 9.1.6 システムファンクションリソース配分の設定」を参照し，QoS 制御機能以外の適切な機能も合わせて選択してください。

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



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，「3.7.2　CoS マッピング機能」を参照してください。

ユーザ優先度は，VLAN Tag ヘッダ内タグ情報（Tag Control）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

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 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 extended	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。
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 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 extended	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-shaper 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) で設定した QoS フローリスト (mac qos-flow-list，ip 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) で設定した QoS フローリスト (mac qos-flow-list，ip 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，マーカー，優先度決定）について説明します。

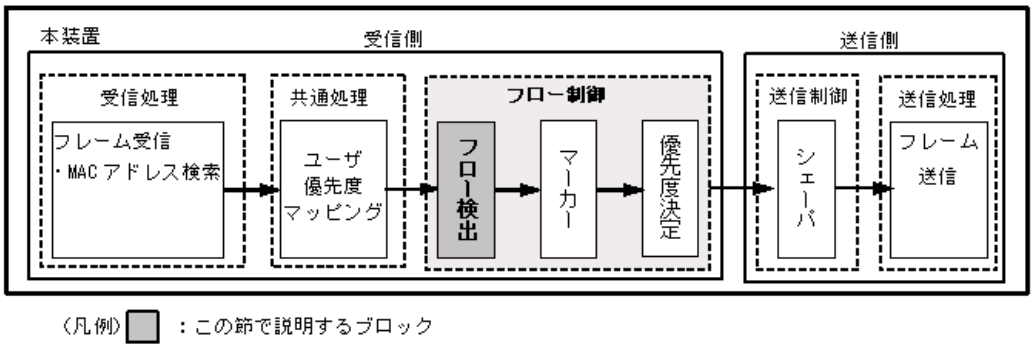
3.1 フロー検出解説

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，フロー検出モードによって変わります。なお，本装置が自発的に送信するフレームはフロー検出対象外です。

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



3.1.1 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二つのフロー検出モードを用意しています。使い方に合わせて選択してください。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，選択したフロー検出モードはフィルタ・QoS で共通です。

フロー検出モードを指定しない場合，layer2-2 がデフォルトのモードとして設定されます。

表 3-1 フロー検出モードとフロー動作の関係

フロー検出モード	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ロー制御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，きめ細かいフロー制御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 ヘッダでフレームを検出します。	イーサネット，VLAN

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指定します。フロー検出モードごとの指定可能なフロー検出条件を次の表に示します。

表 3-2 指定可能なフロー検出条件

種別		設定項目	layer2-1		layer2-2	
			イーサネット	VLAN	イーサネット	VLAN
MAC 条件	コンフィグレーション	VLAN ID※1	○	－	－	－
	MAC ヘッダ	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	○	○	－	－
IPv4 条件	コンフィグレーション	VLAN ID※1	－	－	○	－
	MAC ヘッダ	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	－	－	○	○
		宛先ポート番号	－	－	○	○
		TCP 制御フラグ※4	－	－	○	○
	IPv4-UDP ヘッダ	送信元ポート番号	－	－	○	○
		宛先ポート番号	－	－	○	○

（凡例）○：指定できる　　－：指定できない

注※ 1

本装置のフロー検出で検出できる VLAN ID は，VLAN コンフィグレーションで入力した VLAN に対して付与する値です。入力フレームの属する VLAN ID を検出します。

注※ 2

本装置では VLAN Tag なしの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。

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

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

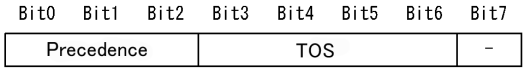
MAC-DA	MAC-SA	1段目の VLAN Tag	2段目の VLAN Tag	Ether Type	Data	FCS

注※ 3

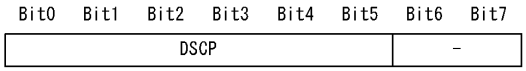
ToS フィールドの指定についての補足

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。



DSCP　：ToS フィールドの上位 6 ビットの値です。



注※ 4

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

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	－	○	－

（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。また，QoS フローリストごとに，QoS エントリの検索は独立して実施します。そのため，フレームが複数の QoS エントリに一致することがあります。複数の QoS エントリに一致した場合，実際に動作するのは単一の QoS エントリです。

（1）イーサネットインタフェースと VLAN インタフェース同時に一致した場合の動作

イーサネットインタフェースと，該当するイーサネットインタフェースが属する VLAN インタフェースに対して QoS エントリを設定し，該当するイーサネットインタフェースからの受信フレームに対して QoS フロー検出を実施すると，複数の QoS エントリに一致する場合があります。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 QoS エントリに一致する場合は，イーサネットインタフェース上の QoS エントリを優先します。複数の QoS エントリに一致した場合の動作を次の表に示します。

表 3-4　複数の QoS エントリに一致した場合の動作

複数フィルタエントリ一致となる組み合わせ		有効になる QoS エントリ
イーサネット	VLAN	
○	－	イーサネット
－	○	VLAN
○	○	イーサネット

（凡例）○：指定あり　　－：指定なし

この条件に該当するのは，フロー検出モード layer2-1，layer2-2 です。

3.1.4 フロー検出使用時の注意事項

（1） 複数 QoS エントリー致時の動作

フレームが複数の QoS エントリ一致した場合，一致した QoS エントリの統計情報が採られます。

（2） 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。

（3） 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。

（4） ほかの機能との同時動作

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
- プロトコル VLAN・MAC VLAN で，VLAN-Tag 付き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

（5） QoS フロー検出条件適用の制限

チャネルグループで受信するフレームに対する QoS フロー検出条件は，VLAN インタフェースに設定した QoS フローグループの QoS フロー検出条件だけを適用します。

3.2 フロー検出コンフィグレーション

3.2.1 フロー検出モードの設定

QoS 制御の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］

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**
   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 extended 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 protocol ip src 0.0.0.0 255.255.255.255 dst 192.168.100.10 0.0.0.0 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 fastethernet 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-ip-range)# 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

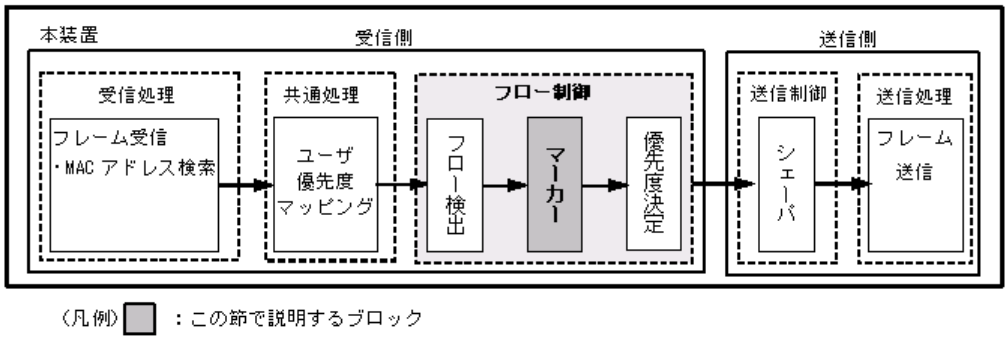
```
> show qos-flow interface fastethernet 0/1

Date 2007/03/09 12:12:05 UTC
Using Port: interface fastethernet 0/1 in
IP qos-flow-list:QOS-LIST1
  remark "cos 6"
  seq 10 qos protocol ip src 0.0.0.0 255.255.255.255 dst 192.168.100.10 0.0.0.0
action cos 6
    matched packets         :          0

>
```

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　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。

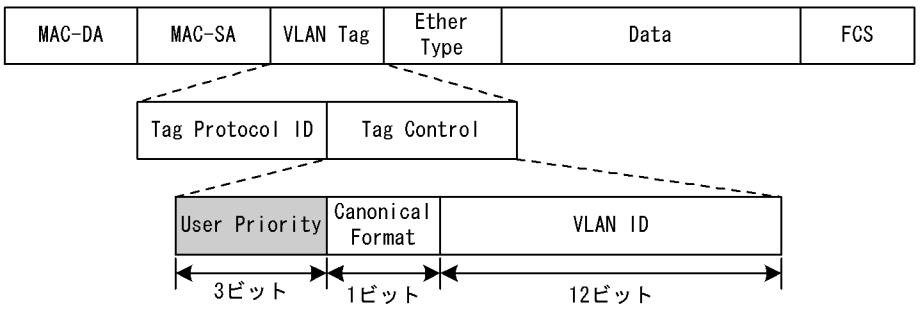
図 3-3　マーカーの位置づけ



3.4.1　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，次の図に示すタグ情報（Tag Control）フィールドの先頭 3 ビットを指します。

図 3-4　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 3-5　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

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

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。

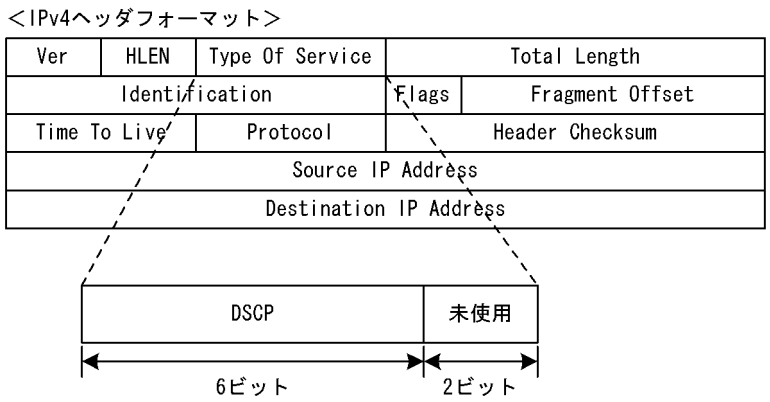
表 3-5　優先度決定機能とユーザ優先度書き換え機能を同時に設定した場合のユーザ優先度

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

3.4.2　DSCP 書き換え

IPv4 ヘッダの ToS 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のフォーマットの図を次に示します。

図 3-6　ToS フィールドのフォーマット



検出したフローの ToS フィールドの上位 6 ビットを書き換えます。

3.5 マーカーのコンフィグレーション

3.5.1 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 extended 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 protocol ip src 0.0.0.0 255.255.255.255 dst 192.168.100.10 0.0.0.0 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 fastethernet 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。

3.5.2 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 extended 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 protocol ip src 0.0.0.0 255.255.255.255 dst 192.168.100.10 0.0.0.0 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 fastethernet 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。

3.6 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。

3.6.1 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 3-7 ユーザ優先度書き換えの確認

```
> show qos-flow interface fastethernet 0/1

Date 2007/03/09 12:12:05 UTC
Using Port: interface fastethernet 0/1 in
IP qos-flow-list: QOS-LIST1
  remark "cos 4"
  seq 10 qos protocol ip src 0.0.0.0 255.255.255.255 dst 192.168.100.10 0.0.0.0
action replace-user-priority 6
    matched packets         :          0
>
```

QOS-LIST1 のリスト情報に「replace-user-priority 6」を表示することを確認します。

3.6.2 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 3-8 DSCP 書き換えの確認

```
> show qos-flow interface fastethernet 0/3

Date 2007/03/09 12:15:05 UTC
Using Port: interface fastethernet 0/3 in
IP qos-flow-list: QOS-LIST2
  remark "cos 4"
  seq 10 qos protocol ip src 0.0.0.0 255.255.255.255 dst dst 192.168.100.10
0.0.0.0 action replace-dscp 63
    matched packets         :          0
>
```

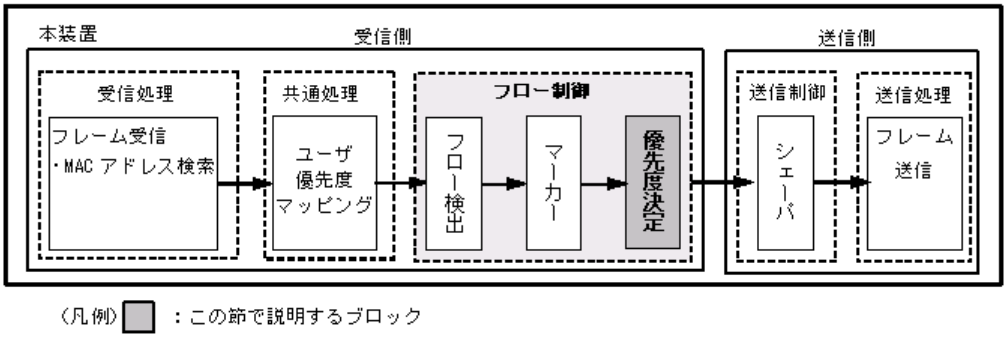
QOS-LIST2 のリスト情報に「replace-dscp 63」を表示することを確認します。

3.7　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 3-9　優先度決定の位置づけ



3.7.1　CoS 値

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。

CoS 値の指定範囲を次の表に示します。

表 3-6　CoS 値の指定範囲

項目	指定範囲
CoS 値	0 ～ 7

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，次の表に示すデフォルトの CoS 値を使用します。

表 3-7　デフォルトの CoS 値

フレーム種別	CoS 値
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	ユーザ優先度マッピングに従います

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 3-8 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） ※2	※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 など）※3	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 • GSRP (GSRP aware)	7
本装置が受信するフレームのうち次のフレーム • system • ポート MAC	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 • MAC 認証レガシーモードのポートから受信した MAC 認証契機のフレーム • EAPOL	5

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。詳細は後述の「3.10 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
IGMP/MLD は変更できません。

注※3
VLAN Tag あり BPDU と L2 ループ検知はここに分類されます。

3.7.2 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 3-9 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：32	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。

3.7.3　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 3-8　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。

3.8 優先度決定コンフィグレーション

3.8.1 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 extended 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 protocol ip src 0.0.0.0 255.255.255.255 dst 192.168.100.10 0.0.0.0 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 fastethernet 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。

3.9 優先度のオペレーション

3.9.1 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 3-10 優先度の確認

```
> show qos queueing interface fastethernet 0/1

Date 2007/03/12 12:07:46 UTC
Port 0/1 (outbound)
 Status : Active
 Max_Queue=8, Rate_limit=10Mbit/s, Qmode=wfq/tail_drop
  Queue 1: Qlen=     0, Limit_Qlen=   32
  Queue 2: Qlen=     0, Limit_Qlen=   32
  Queue 3: Qlen=     0, Limit_Qlen=   32
  Queue 4: Qlen=     0, Limit_Qlen=   32
  Queue 5: Qlen=     0, Limit_Qlen=   32
  Queue 6: Qlen=     1, Limit_Qlen=   32
  Queue 7: Qlen=     0, Limit_Qlen=   32
  Queue 8: Qlen=     0, Limit_Qlen=   32
   discard packets
    HOL1=          0, HOL2=          0, Tail_drop=          0

>
```

Qlen の値がカウントされているのが，Queue6 であることを確認します。

3.10 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 3-10 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※	2	7	layer-2	0 ～ 7
ICMP ARP Telnet FTP NTP SNMP syslog IGMP MLD	3	7	layer-3	0 ～ 7

注※

BPDU/L2 ループ検知以外のレイヤ２自発フレームは VLAN Tag なしのフレームであるため，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 値は下記のようにマッピングされます。BPDU/L2 ループ検知 /IGMP/MLD 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 3-11 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	layer-2	0 ～ 7	7
IGMP MLD	layer-3		
ICMP	layer-3	0	0
ARP		1	1
Telnet		2	2

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
FTP		3	3
NTP		4	4
SNMP		5	5
syslog		6	6
		7	7

3.11 自発フレームのユーザ優先度のコンフィグレーション

3.11.1 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

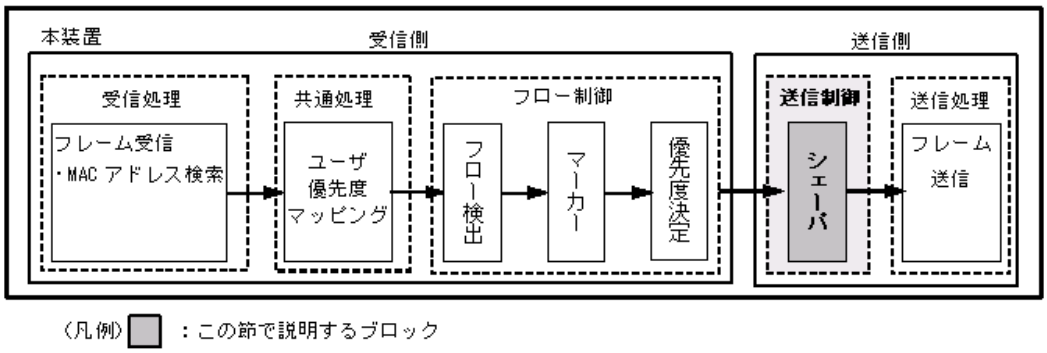
この章では本装置の送信制御（シェーパ）について説明します。

4.1　シェーパ解説

4.1.1　レガシーシェーパの概要

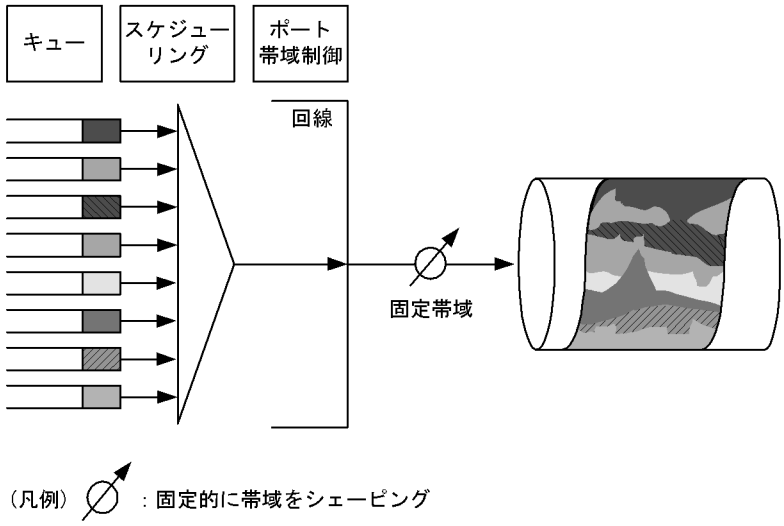
シェーパは，フレームの出力順序や出力帯域を制御する機能です。この節で説明するシェーパの位置づけを次の図に示します。

図 4-1　シェーパの位置づけ



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



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 32 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

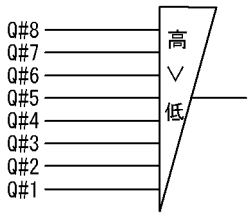
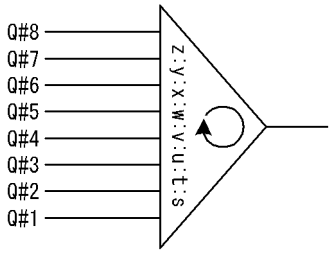
キュー番号	送信キュー長：32	送信キュー長：128	送信キュー長：728
1	32	128	728
2	32	128	32
3	32	128	0
4	32	128	0
5	32	0	0
6	32	0	0
7	32	0	0
8	32	0	0

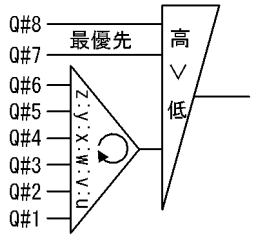
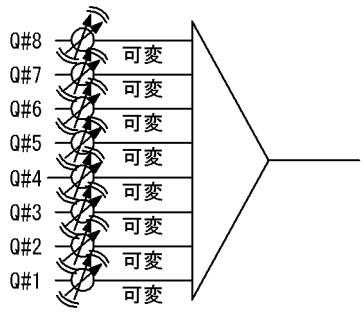
送信キュー長と CoS マッピングは，「表 3-9 CoS 値と送信キューのマッピング」を参照してください。

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。回線状態が半二重の場合，WFQ は動作しません。PQ で動作します。

表 4-4　WFQ の設定範囲

回線速度	帯域幅	設定範囲		刻み値
1Gbit/s	64kbit/s ～ 1Gbit/s	Mbit/s	1M ～ 1000M	1Mbit/s ※1
		kbit/s	1000 ～ 1000000	100kbit/s ※2
			64 ～ 960	64kbit/s ※3
100Mbit/s	64kbit/s ～ 100Mbit/s	Mbit/s	1M ～ 100M	1Mbit/s ※1
		kbit/s	1000 ～ 100000	100kbit/s ※2
			64 ～ 960	64kbit/s ※3

回線速度	帯域幅	設定範囲		刻み値
10Mbit/s	64kbit/s ～ 10Mbit/s	Mbit/s	1M ～ 10M	1Mbit/s※1
		kbit/s	1000 ～ 10000	100kbit/s※2
			64 ～ 960	64kbit/s※3
Auto Negotiation	64kbit/s ～ 1Gbit/s	Mbit/s	1M ～ 1000M	1Mbit/s※1
		kbit/s	1000 ～ 1000000	100kbit/s※2
			64 ～ 960	64kbit/s※3

注※1　1M は 1000k として扱います。
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回線全体の送信帯域を指定した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。イーサネットインタフェース帯域と契約帯域の差による輻輳を回避できます。

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。

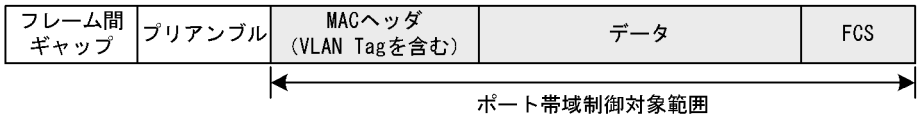
表 4-5　ポート帯域制御の設定値一覧

回線速度	帯域幅	設定範囲		刻み値
1Gbit/s	64kbit/s ～ 1Gbit/s	Mbit/s	1M ～ 1000M	1Mbit/s※1
		kbit/s	1000 ～ 1000000	100kbit/s※2
			64 ～ 960	64kbit/s※3
100Mbit/s	64kbit/s ～ 100Mbit/s	Mbit/s	1M ～ 100M	1Mbit/s※1
		kbit/s	1000 ～ 100000	100kbit/s※2
			64 ～ 960	64kbit/s※3
10Mbit/s	64kbit/s ～ 10Mbit/s	Mbit/s	1M ～ 10M	1Mbit/s※1
		kbit/s	1000 ～ 10000	100kbit/s※2
			64 ～ 960	64kbit/s※3
Auto Negotiation	64kbit/s ～ 1Gbit/s	Mbit/s	1M ～ 1000M	1Mbit/s※1
		kbit/s	1000 ～ 1000000	100kbit/s※2
			64 ～ 960	64kbit/s※3

注※1　1M は 1000k として扱います。
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。詳細は，「図 4-3　ポート帯域制御の対象範囲」を参照してください。

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。
- 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。
- 送信キュー長728を設定する場合は，コンフィグレーションコマンドflowcontrolで「ポーズパケットを送信する」設定をしてください。

（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，当該回線に設定します。

［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 fastethernet 0/11**
   ポート 0/11 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，当該回線に設定します。

［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 fastethernet 0/14**
   ポート 0/14 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，当該回線に設定します。

［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 fastethernet 0/16**
   ポート 0/16 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，当該回線に設定します。

［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 fastethernet 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

当該回線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］

当該回線（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 fastethernet 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 PQ の確認

PQ の確認方法を次の図に示します。

図 4-4 PQ の確認

```
> show qos queueing interface fastethernet 0/11

Date 2007/03/12 12:08:10 UTC
Port 0/11 (outbound)
 Status : Active
 Max_Queue=8, Rate_limit=100Mbit/s, Qmode=pq/tail_drop
  Queue 1: Qlen=    0, Limit_Qlen=   32
  Queue 2: Qlen=    0, Limit_Qlen=   32
  Queue 3: Qlen=    0, Limit_Qlen=   32
  Queue 4: Qlen=    0, Limit_Qlen=   32
  Queue 5: Qlen=    0, Limit_Qlen=   32
  Queue 6: Qlen=    0, Limit_Qlen=   32
  Queue 7: Qlen=    0, Limit_Qlen=   32
  Queue 8: Qlen=    0, Limit_Qlen=   32
   discard packets
    HOL1=         0, HOL2=         0, Tail_drop=         0

>
```

Qmode パラメータの内容が，「pq/tail_drop」になっていることを確認します。

4.3.2 WRR の確認

WRR の確認方法を次の図に示します。

図 4-5 WRR の確認

```
> show qos queueing interface fastethernet 0/14

Date 2007/03/12 12:09:55 UTC
Port 0/14 (outbound)
 Status : Active
 Max_Queue=8, Rate_limit=100Mbit/s, Qmode=wrr/tail_drop
  Queue 1: Qlen=    0, Limit_Qlen=   32
  Queue 2: Qlen=    0, Limit_Qlen=   32
  Queue 3: Qlen=    0, Limit_Qlen=   32
  Queue 4: Qlen=    0, Limit_Qlen=   32
  Queue 5: Qlen=    0, Limit_Qlen=   32
  Queue 6: Qlen=    0, Limit_Qlen=   32
  Queue 7: Qlen=    0, Limit_Qlen=   32
  Queue 8: Qlen=    0, Limit_Qlen=   32
   discard packets
    HOL1=         0, HOL2=         0, Tail_drop=         0

>
```

Qmode パラメータの内容が，「wrr/tail_drop」になっていることを確認します。

4.3.3 2PQ+6WRR の確認

2PQ+6WRR の確認方法を次の図に示します。

図 4-6 2PQ+6WRR の確認

```
> show qos queueing interface fastethernet 0/16

Date 2007/03/12 12:09:55 UTC
Port 0/16 (outbound)
 Status : Active
 Max_Queue=8, Rate_limit=100Mbit/s, Qmode=2pq+6wrr/tail_drop
  Queue 1: Qlen=    0, Limit_Qlen=   32
  Queue 2: Qlen=    0, Limit_Qlen=   32
  Queue 3: Qlen=    0, Limit_Qlen=   32
  Queue 4: Qlen=    0, Limit_Qlen=   32
  Queue 5: Qlen=    0, Limit_Qlen=   32
  Queue 6: Qlen=    0, Limit_Qlen=   32
  Queue 7: Qlen=    0, Limit_Qlen=   32
  Queue 8: Qlen=    0, Limit_Qlen=   32
   discard packets
    HOL1=         0, HOL2=         0, Tail_drop=         0

>
```

Qmode パラメータの内容が，「2pq+6wrr/tail_drop」になっていることを確認します。

4.3.4 WFQ の確認

WFQ の確認方法を次の図に示します。

図 4-7 WFQ の確認

```
> show qos queueing interface fastethernet 0/6

Date 2007/03/12 12:08:34 UTC
Port 0/6 (outbound)
 Status : Active
 Max_Queue=8, Rate_limit=100Mbit/s, Qmode=wfq/tail_drop
  Queue 1: Qlen=    0, Limit_Qlen=   32
  Queue 2: Qlen=    0, Limit_Qlen=   32
  Queue 3: Qlen=    0, Limit_Qlen=   32
  Queue 4: Qlen=    0, Limit_Qlen=   32
  Queue 5: Qlen=    0, Limit_Qlen=   32
  Queue 6: Qlen=    0, Limit_Qlen=   32
  Queue 7: Qlen=    0, Limit_Qlen=   32
  Queue 8: Qlen=    0, Limit_Qlen=   32
   discard packets
    HOL1=         0, HOL2=         0, Tail_drop=         0

>
```

Qmode パラメータの内容が，「wfq/tail_drop」になっていることを確認します。

4.3.5 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 4-8　ポート帯域制御の確認

```
> show qos queueing interface fastethernet 0/3

Date 2007/03/12 12:15:23 UTC
Port 0/3 (outbound)
 Status : Active
 Max_Queue=8, Rate_limit=20Mbit/s, Qmode=pq/tail_drop
  Queue 1: Qlen=    0, Limit_Qlen=   32
  Queue 2: Qlen=    0, Limit_Qlen=   32
  Queue 3: Qlen=    0, Limit_Qlen=   32
  Queue 4: Qlen=    0, Limit_Qlen=   32
  Queue 5: Qlen=    0, Limit_Qlen=   32
  Queue 6: Qlen=    0, Limit_Qlen=   32
  Queue 7: Qlen=    0, Limit_Qlen=   32
  Queue 8: Qlen=    0, Limit_Qlen=   32
   discard packets
    HOL1=         0, HOL2=         0, Tail_drop=         0

>
```

Rate_limit パラメータの内容が，「20Mbit/s」になっ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を説明します。

5.1　レイヤ 2 認証機能の概要

5.1　レイヤ２認証機能の概要

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

認証機能	認証方式	認証モード	認証サブモード
IEEE802.1X	RADIUS 認証	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
		VLAN 単位認証（動的）	－
Web 認証	ローカル認証 RADIUS 認証	固定 VLAN モード ダイナミック VLAN モード レガシーモード	－
MAC 認証	ローカル認証 RADIUS 認証	固定 VLAN モード ダイナミック VLAN モード レガシーモード	－

（凡例）
－：なし

- IEEE802.1X
  IEEE802.1X 準拠のポート単位に認証を行うポート単位認証，VLAN の MAC アドレス単位に認証を行う VLAN 単位認証（動的）があります。
  それぞれ，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　認証方式

前述の各認証機能は，ローカル認証方式または RADIUS 認証方式で認証を実施します。

（1） 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。

（2） 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。

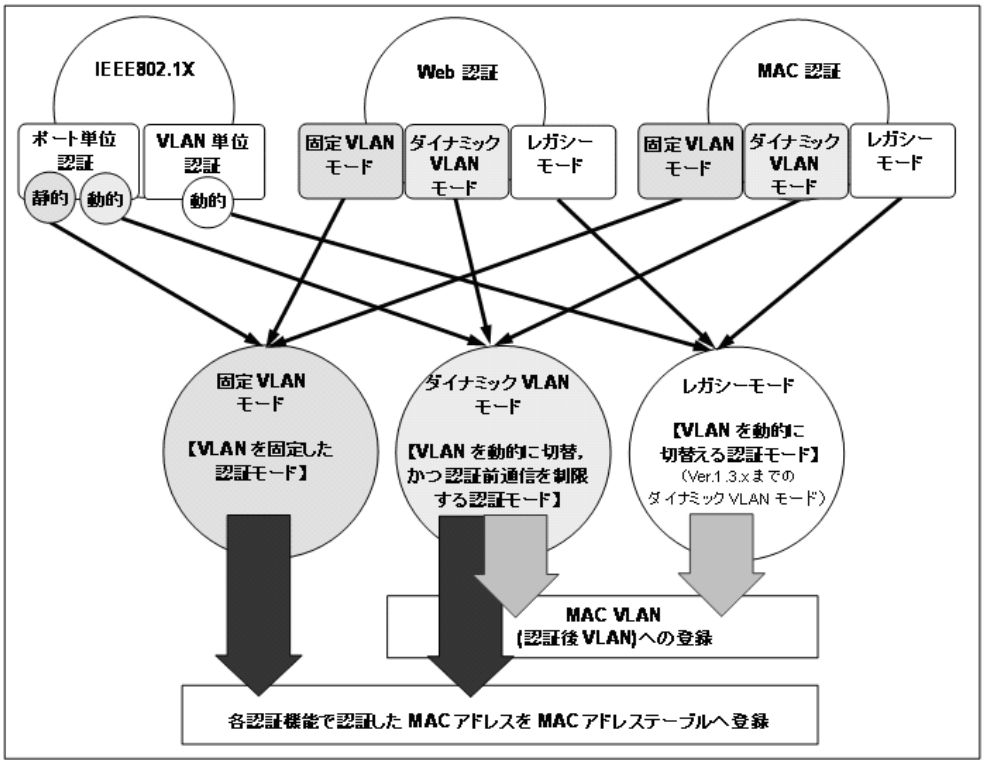
RADIUS サーバは一般の外部 RADIUS サーバを使用します。RADIUS サーバには認証対象ユーザ（または端末）の情報を登録します。RADIUS サーバのユーザ情報などの登録については，ご使用になる RADIUS サーバのマニュアルを参照してください。

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。RADIUS サーバ情報については，「コンフィグレーションガイド Vol.1　8　ログインセキュリティと RADIUS」を参照してください。

5.1.3　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」「レガシーモード」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。

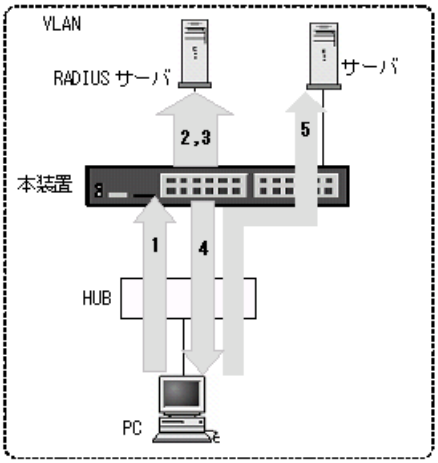
図 5-1　各認証機能と認証モードの対応図



（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）

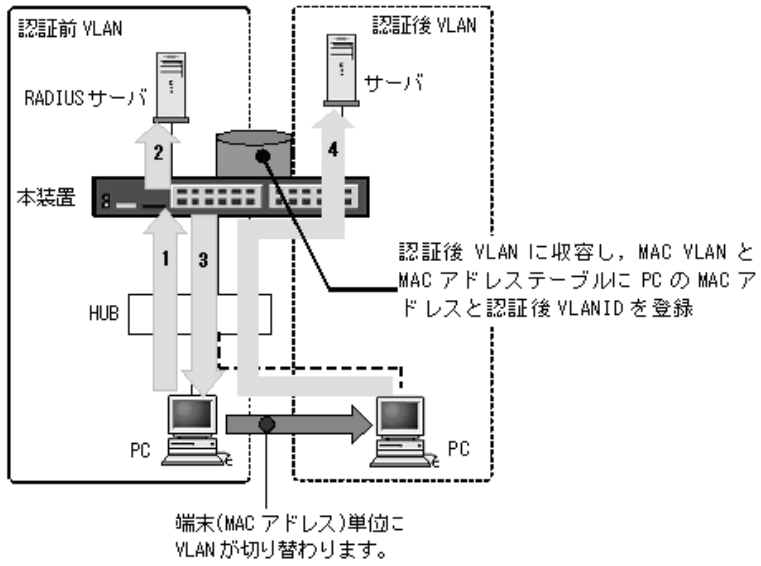


1. HUB などを経由して接続した認証対象端末（図内の PC）から本装置にアクセスします。
2. 認証対象端末の接続ポートまたは VLAN ID により，認証対象端末が所属する VLAN ID を特定します。
3. 端末情報に特定した VLAN ID 情報を加えて RADIUS サーバへ認証要求することで，収容可能な VLAN を制限することが可能となります。
4. 認証成功であれば，認証成功画面を端末に表示します。（Web 認証の場合）
5. 認証済み端末は，接続された VLAN のサーバに接続できるようになります。

（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。

図 5-3 ダイナミック VLAN モード概要図（RADIUS 認証の例）



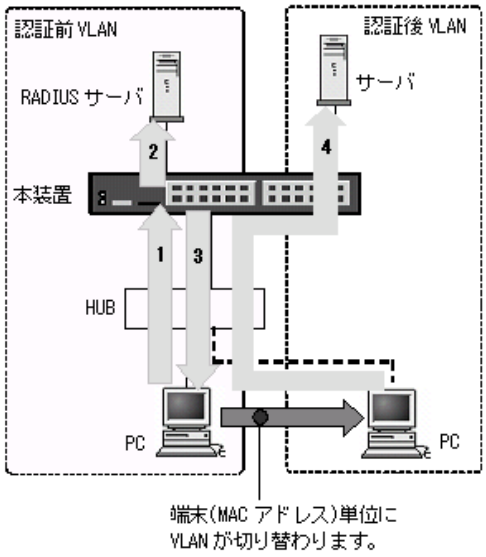
1. HUB などを経由して接続した認証対象端末（図内の PC）から本装置にアクセスします。
2. 外部に設置された RADIUS サーバに従って認証を行います。
3. 認証成功であれば，認証成功画面を端末に表示します。（Web 認証の場合）
4. RADIUS サーバから送られる VLAN ID 情報に従って，認証済み端末を認証後の VLAN に収容して，

サーバに接続できるようになります。

(3) レガシーモード

レガシーモードは，MAC VLAN 機能を使用して認証要求端末ごとに認証・検疫し，動的に VLAN を割り当てることにより，認証前のネットワークと認証後のネットワークを分離できます。(Ver.1.3. x までのダイナミック VLAN モードが該当します。)

図 5-4 レガシーモード概要図（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. 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，認証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 情報とコンフィグレーションで設定した認証後 VLAN 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。

(4) 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「12　レイヤ 2 認証の共通機能と共存使用」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。

5.1.4 レイヤ 2 認証機能使用時の注意事項

(1) 運用前のシステムファンクションリソースの設定について

下記の認証機能および認証モードを使用する場合，システムファンクションリソースの設定が必要となります。

- 認証機能共通：認証専用 IPv4 アクセスリスト
- IEEE802.1X：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，Web 認証専用 IP アドレス

- MAC 認証：固定 VLAN モード，ダイナミック VLAN モード

システムファンクションリソース設定については，「コンフィグレーションガイド Vol.1　9.1.6　システムファンクションリソース配分の設定」を参照し，上記以外の適切な機能も合わせて選択してください。

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。

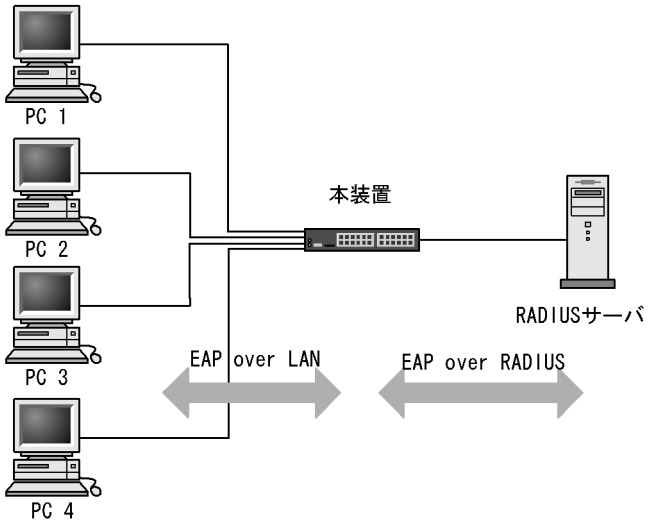
表 6-1 構成要素と動作概略

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。

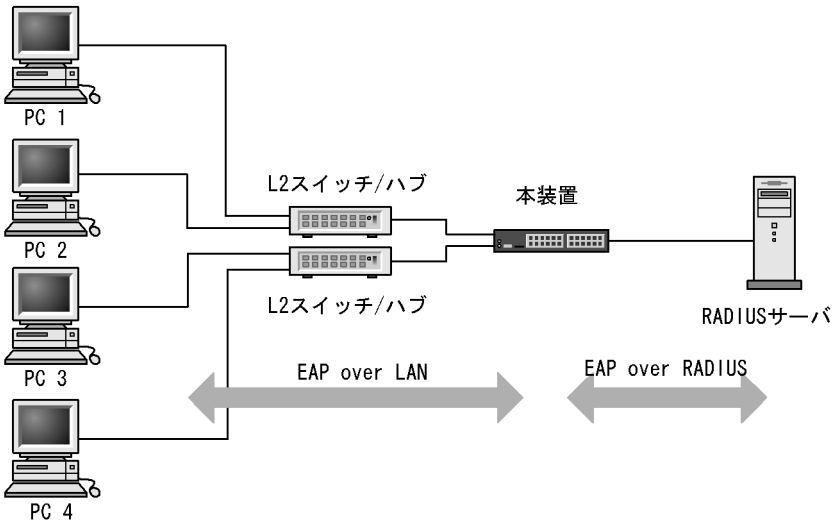
本装置を使った IEEE802.1X 基本構成を次の図に示します。

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

本装置でサポートする認証方式は RADIUS サーバ認証です。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。

(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。
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。

本装置の IEEE802.1X では，三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。
- VLAN 単位認証（動的）
  MAC VLAN による VLAN 切り替えにより，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。

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一覧

機能			ポート単位認証（静的）	ポート単位認証（動的）	VLAN 単位認証（動的）
ローカル認証			×	×	×
RADIUS 認証	RADIUS サーバ		外部サーバ 「6.7」参照	外部サーバ 「6.7」参照	外部サーバ 「6.7」参照
	VLAN （認証後の VLAN）		×	○	○
	強制認証		○ 「6.2.2」参照	○ 「6.3.2」参照	○ 「6.4.2」参照
		認証許可ポート設定	○ 「7.3.3」参照	○ 「7.4.3」参照	○ 「7.5.3」参照
		プライベートトラップ	×	×	×
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	○ 「6.4.1」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	○ 「6.4.1」参照 「7.5.2」参照
	認証デフォルト VLAN		×	×	○ 「7.5.2」参照
認証	端末検出動作切り替え		○ 「6.2.2」参照 「7.3.2」参照	○ 「6.3.2」参照 「7.4.2」参照	○ 「6.4.2」参照 「7.5.2」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	○ 「6.4.2」参照 「7.5.3」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	○ 「6.4.2」参照 「7.5.3」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	○ 「6.4.2」参照 「7.5.3」参照

機能		ポート単位認証（静的）	ポート単位認証（動的）	VLAN 単位認証（動的）
	複数端末からの認証要求時の通信遮断状態保持時間	○※ 「6.2.1」参照 「7.3.3」参照	○※ 「6.3.1」参照 「7.4.3」参照	×
	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	○ 「6.4.2」参照 「7.5.3」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	○ 「6.4.2」参照 「7.5.3」参照
	認証前通過（認証専用 IPv4 アクセスリスト）	○ 「12」参照	○ 「12」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	○ 「6.4.2」参照 「7.5.3」参照
	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	○ 「6.4.2」参照
	運用コマンド	○ 「6.2.2」参照	○ 「6.3.2」参照	○ 「6.4.2」参照
EAPOL フォワーディング		全モード共通　「6.5」参照		
アカウントログ	本装置内蔵アカウントログ	全モード合わせて 2100 行　「6.6」参照		

（凡例）

○：サポート

×：未サポート

「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※

本機能は，ポート単位認証（静的）およびポート単位認証（動的）のシングルモードだけ適用します。

表 6-4　IEEE802.1X の動作条件

種別			ポート単位認証（静的）	ポート単位認証（動的）	VLAN 単位認証（動的）
VLAN 種別	ポート VLAN		○	×	×
	プロトコル VLAN		×	×	×
	MAC VLAN		×	○	○
デフォルト VLAN			○	×	×
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		×	×	×
	MAC ポート	Untagged	×	○	○
		Tagged	×	×	×
インタフェース種別	fastethernet		○	○	○
	gigabitethernet		○	○	○
	port channel		○	×	○

（凡例）
○：動作可　　×：動作不可

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。

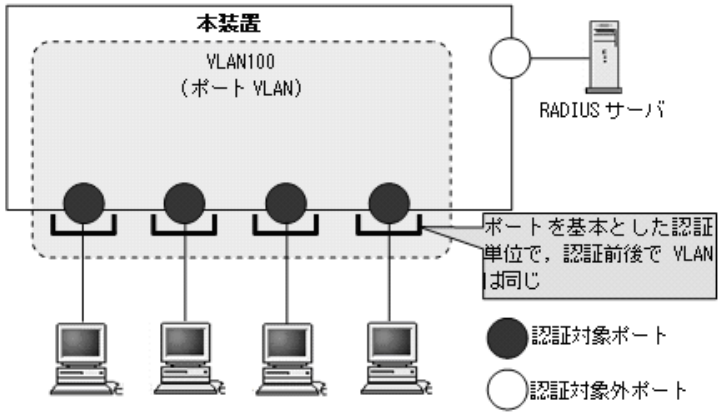
次項からは，「ポート単位認証（静的）」「ポート単位認証（動的）」「VLAN 単位認証（動的）」の順に各認証モードの概要を説明します。各認証モードで同じ機能，同一動作については，「～を参照してください。」としていますので，該当箇所を参照してください。

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。

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

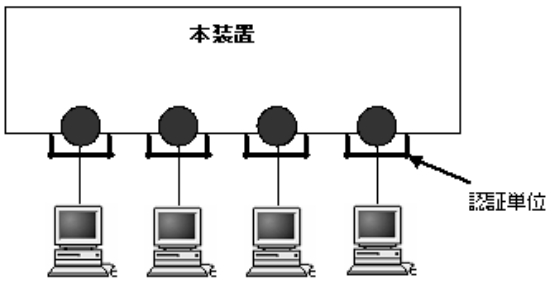
ポート単位認証（静的）の認証サブモードは，シングルモードと端末認証モードがあります。デフォルトはシングルモードで動作し，コンフィグレーションコマンド dot1x multiple-authentication を設定すると，端末認証モードで動作します。

（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。

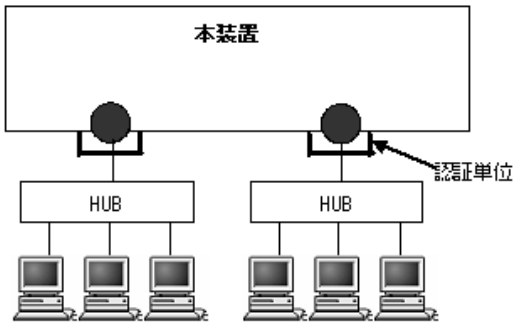
図 6-4 シングルモードの構成



(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

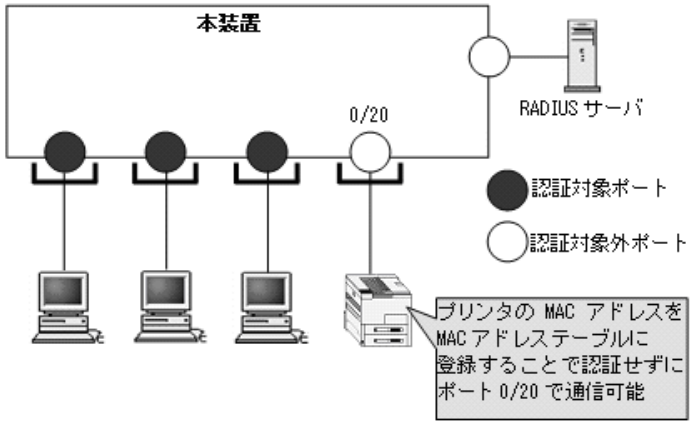
スタティック MAC アドレス学習機能※によって MAC アドレスが設定された端末については認証を不要とし，通信を許可するオプション設定です。Supplicant 機能を持たないプリンタなどの装置やサーバなど認証が不要な端末を，端末単位で認証対象から除外したいときに使用します。端末認証モードの場合だけ使用可能なオプションです。

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

端末の認証開始を誘発するために，本装置はコンフィグレーションで設定した間隔で 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，認証単位に複数の端末が存在する可能性があります。そのため，本装置ではすべての端末の認証が完了するまで EAP-Request/Identity の送信を継続することをデフォルトの動作としています。

このとき，認証単位当たりの端末数が増えると EAP-Request/Identity に応答した端末の認証処理で装置に負荷を掛けるおそれがあるため，認証済み端末からの応答には認証シーケンスを一部省略することで，装置の負荷を低減しています。

ただし，使用する Supplicant ソフトウェアの種類によっては，認証シーケンスの省略によって認証済み端末の通信が途切れる問題が発生することがあります。そのため，認証済み端末に対する動作を切り替えるオプションを用意しています。本オプションはコンフィグレーションコマンド dot1x supplicant-detection で選択を行い，次に示す二種類の動作を指定できます。

（a） shortcut

装置の負荷を低減するため，認証済み端末に対する EAP-Request/Identity 契機の認証シーケンスを一部省略します。一部の Supplicant ソフトウェアを本モードで使用すると，EAP-Request/Identity による認証時に認証済み端末との通信が途切れる場合があります。そのときに，使用する Supplicant ソフトウェアが EAPOL-Start を自発的に送信できる場合は disable を指定してください。

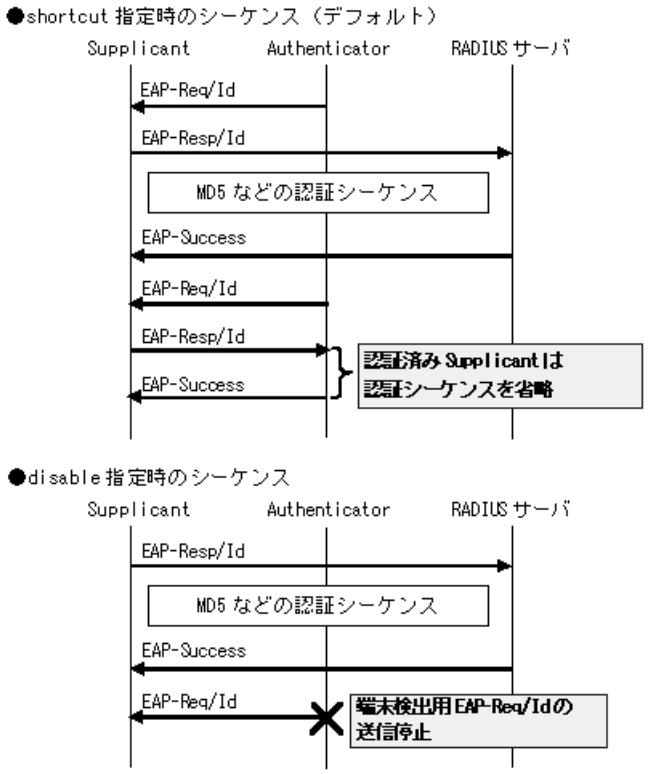
（b） disable

端末の認証開始を誘発するための EAP-Request/Identity の送信を停止します。自発的に EAPOL-Start を

送信しない Supplicant ソフトウェアで本モードを使用すると，認証開始の契機がなくなるため認証を開始できません。Windows 標準の Supplicant ソフトウェアはデフォルトでは自発的に EAP-Start を送信しませんが，レジストリ SupplicantMode の値を変更することによってこの動作を変更できます。レジストリの詳細については，Microsoft 社の WWW サイトまたは公開技術文書を参照してください。レジストリの設定を失敗すると Windows が起動しなくなるおそれがありますので注意してください。また，レジストリを変更する場合は必ずレジストリのバックアップを取ることをお勧めします。

本オプションは端末認証モードだけで有効です。それぞれの動作シーケンスを次の図に示します。

図 6-7　shortcut，disable 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

強制認証指定したポートに接続された端末の RADIUS 認証が，経路障害などで RADIUS サーバへリクエスト送信失敗または無応答となったときは，認証対象端末を認証許可状態にします。

強制認証を許可するポートにコンフィグレーションコマンド dot1x force-authorized を設定します。また，強制認証を許可した端末へ EAP-Success 応答を送信するためにコンフィグレーションコマンド dot1x force-authorized eapol を設定します。

なお，強制認証は下記の条件を満たしたときに許可となります。

表 6-6 強制認証許可条件

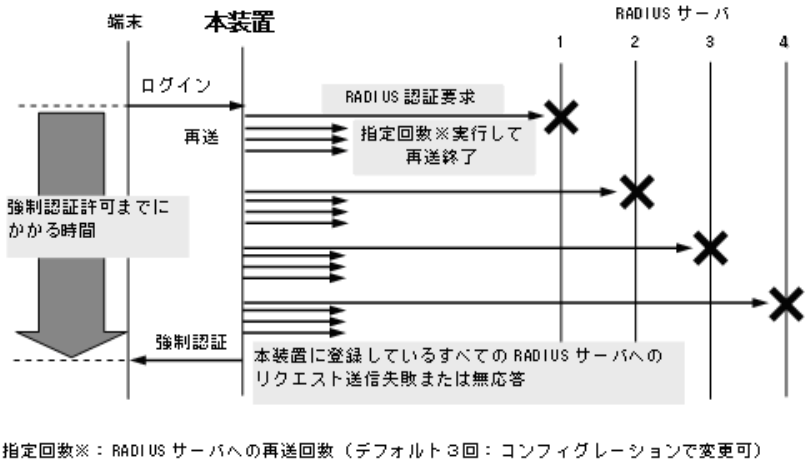
項目	条件
コンフィグレーション	下記のコンフィグレーションがすべて設定されていること • aaa authentication dot1x default group radius • radius-server • dot1x system-auth-control • dot1x port-control auto ※ • dot1x force-authorized ※ • switchport mode access ※
アカウントログ	RADIUS サーバへの認証要求送信で，下記のアカウントログが採取された場合 • Failed to connect to RADIUS server. (IP=xxx.xxx.xxx.xxx) アカウントログは運用コマンド show dot1x logging で確認できます。

注※
同じポートに設定してください。

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 (9) 認証解除」のいずれかの解除機能により認証状態が解除されます。

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しているすべての RADIUS サーバのタイムアウト（リクエスト送信失敗または無応答）までとなります。

図 6-8　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 サーバの接続については，「コンフィグレーションガイド Vol.1　8　ログインセキュリティと RADIUS」を参照してください。

なお，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。

(c) 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。

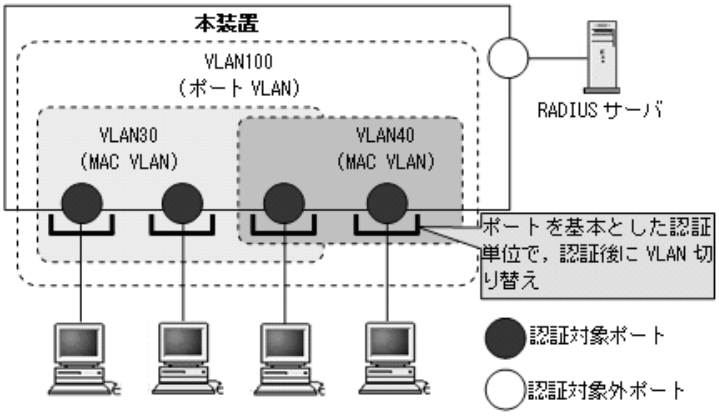
6.3 ポート単位認証（動的）

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。

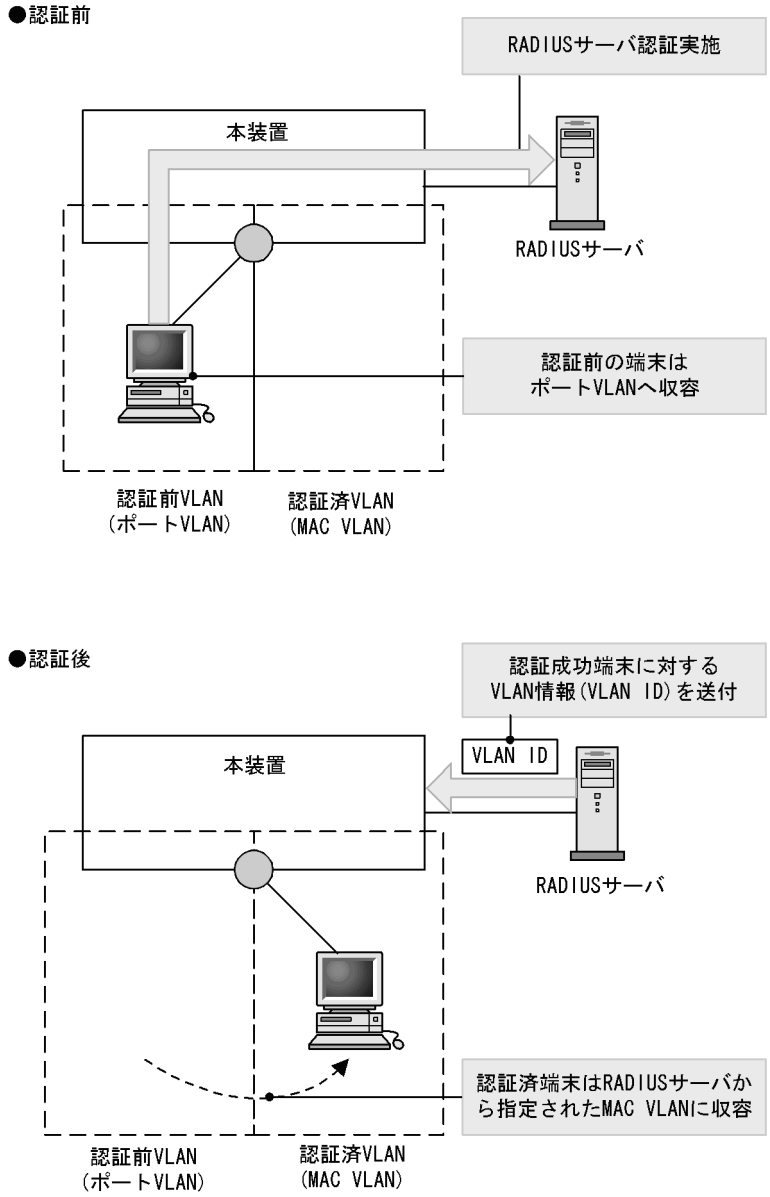
ポート単位認証（動的）の構成例を次の図に示します。

図 6-9 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 6-10 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 6-7 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

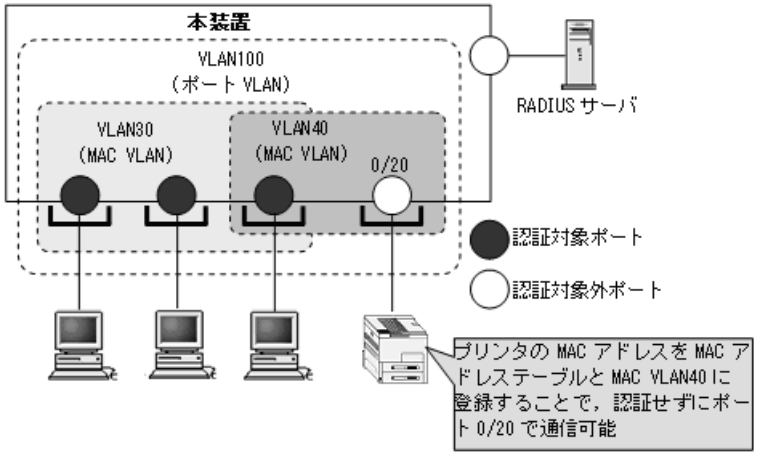
コンフィグレーションコマンド mac-address-table static で，MAC アドレステーブルに MAC アドレスを設定

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 6-11 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

強制認証指定したポートに接続された端末の RADIUS 認証が，経路障害などで RADIUS サーバへリクエスト送信失敗または無応答となったときは，認証対象端末を認証許可状態にします。

強制認証を許可するポートにコンフィグレーションコマンド dot1x force-authorized vlan を設定します。また，強制認証を許可した端末へ EAP-Success 応答を送信するためにコンフィグレーションコマンド dot1x force-authorized eapol を設定します。

なお，強制認証は下記の条件を満たしたときに許可となります。

表 6-8 強制認証許可条件

項目	条件
コンフィグレーション	下記のコンフィグレーションがすべて設定されていること • aaa authentication dot1x default group radius • radius-server • dot1x system-auth-control • dot1x force-authorized vlan ※1 • dot1x port-control auto ※2 • vlan <VLAN ID> mac-based ※1 • switchport mac ※1※2 • switchport mode mac-vlan ※2
アカウントログ	RADIUS サーバへの認証要求送信で，下記のアカウントログが採取された場合 • Failed to connect to RADIUS server. (IP=xxx.xxx.xxx.xxx) アカウントログは運用コマンド show dot1x logging で確認できます。

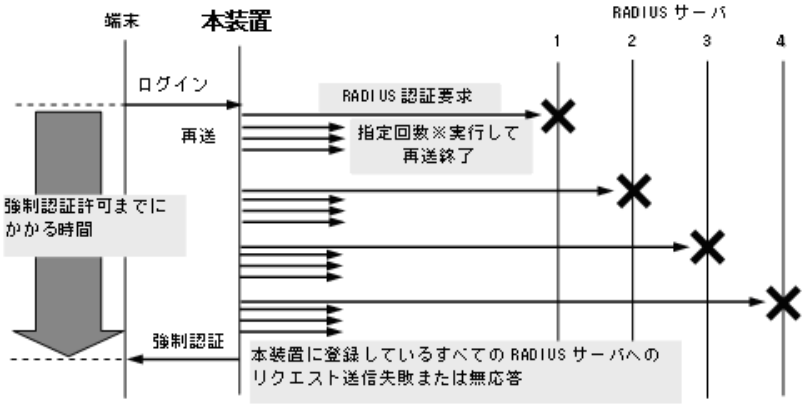
注※ 1
同じ VLAN ID を設定してください。

注※ 2
同じポートに設定してください。

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 (9) 認証解除」のいずれかの解除機能により認証状態が解除されます。

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しているすべての RADIUS サーバのタイムアウト（リクエスト送信失敗または無応答）までとなります。

図 6-12 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 サーバの接続については，「コンフィグレーションガイド Vol.1 8 ログインセキュリティと RADIUS」を参照してください。

なお，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) 認証解除

ポート単位認証（静的）と同様です。「6.2.2 認証機能 (9) 認証解除」を参照してください。

6.4 VLAN 単位認証（動的）

認証の制御を MAC VLAN に所属する端末に対して行います。IEEE802.1Q VLAN-Tag の付与された EAPOL フレームを扱うことができません。このフレームを受信した場合には廃棄します。

指定された MAC VLAN のトランクポートおよびアクセスポートは認証除外ポートとして扱われます。

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。ただし，RADIUS サーバから受信した VLAN 情報が，VLAN 単位認証（動的）の認証後 VLAN 設定（コンフィグレーションコマンド dot1x vlan dynamic radius-vlan）に含まれない場合は，認証失敗となります。

VLAN 単位認証（動的）の構成例と動作イメージを次の図に示します。

図 6-13 VLAN 単位認証（動的）の構成例

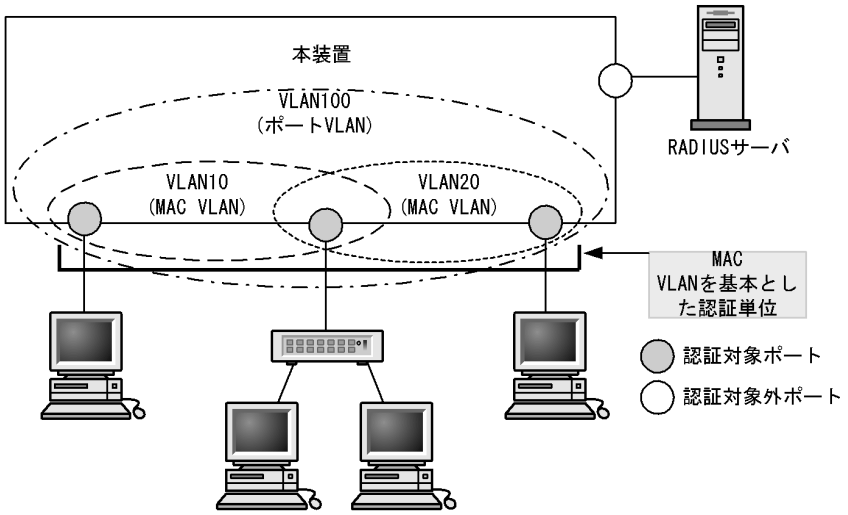
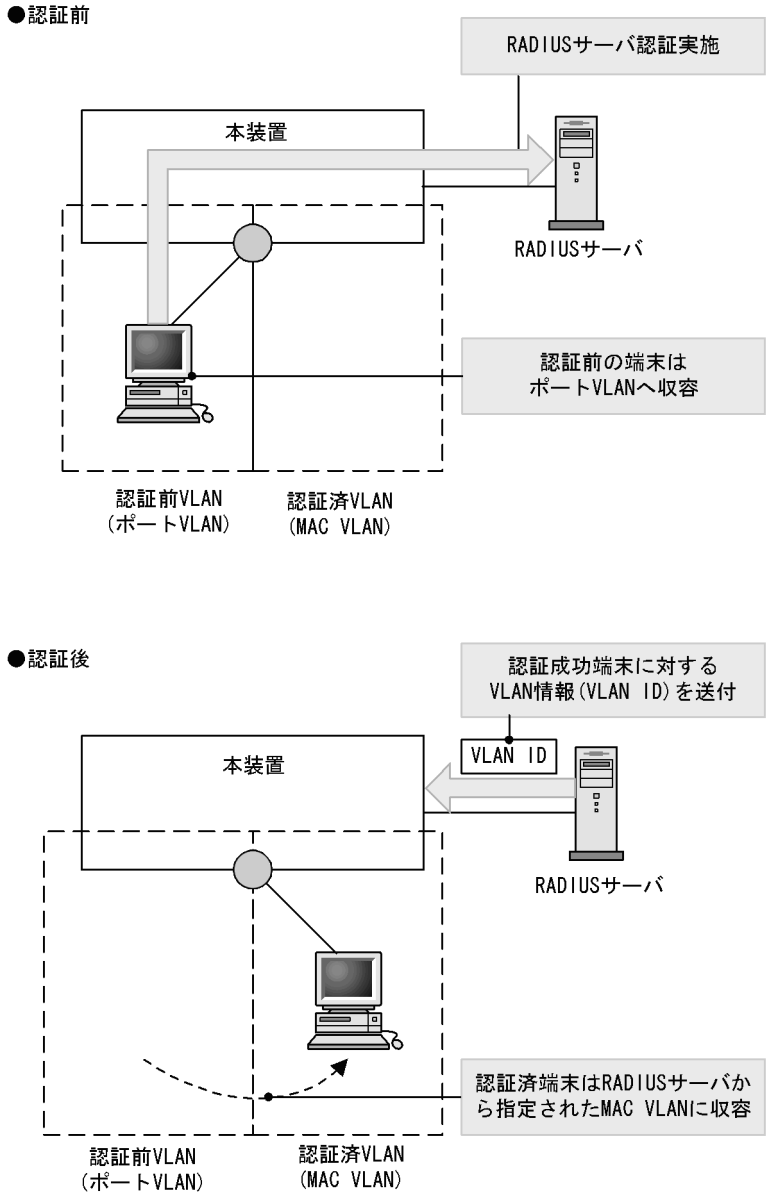


図 6-14 VLAN 単位認証（動的）の動作イメージ



6.4.1 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 6-9 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
VLAN 単位認証（動的）	端末認証モード	認証除外端末オプション
		認証デフォルト VLAN

(1) 認証サブモード

VLAN 単位認証（動的）の認証サブモードは，端末認証モードだけです。

(a) 端末認証モード

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　(b) 端末認証モード」を参照してください。

(2) 認証モードオプション

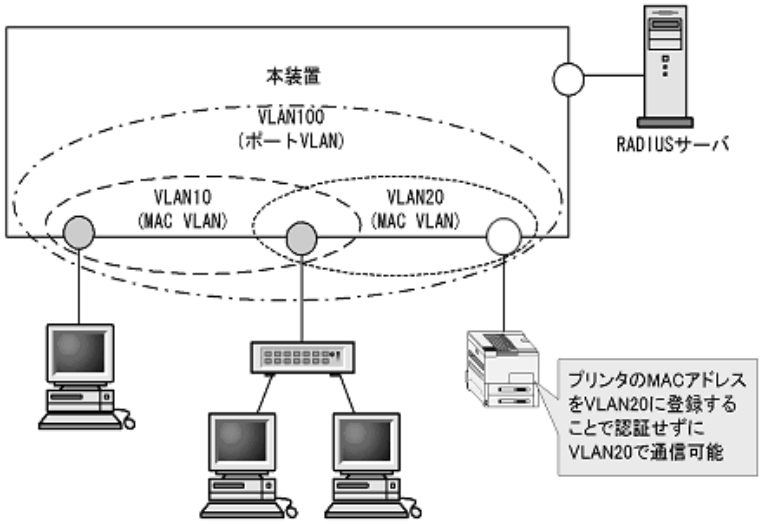
(a) 認証除外端末オプション

MAC VLAN 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 で MAC VLAN に MAC アドレスを設定

VLAN 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 6-15　VLAN 単位認証（動的）での認証除外端末構成例



(b) 認証デフォルト VLAN 機能

認証デフォルト VLAN 機能は，IEEE802.1X に未対応などの理由によって MAC VLAN に収容できない端末をポート VLAN に収容する機能です。VLAN 単位認証 (動的) に設定したポートに対してポート VLAN またはデフォルト VLAN が設定されている場合，その VLAN は認証デフォルト VLAN として動作します。次に示すような場合，端末は認証デフォルト VLAN に収容します。

- IEEE802.1X 未対応の端末
- 認証前の IEEE802.1X 対応の端末
- 認証または再認証に失敗した端末
- RADIUS サーバから指定された VLAN ID が MAC VLAN でない場合
- RADIUS サーバから指定された VLAN ID がポートに設定されていない場合

6.4.2 認証機能

（1） 認証契機

VLAN 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

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 vlan dynamic 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

端末の認証開始を誘発するために，本装置はコンフィグレーションで設定した間隔で 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，認証単位に複数の端末が存在する可能性があります。そのため，本装置ではすべての端末の認証が完了するまで EAP-Request/Identity の送信を継続することをデフォルトの動作としています。

このとき，認証単位当たりの端末数が増えると EAP-Request/Identity に応答した端末の認証処理で装置に負荷を掛けるおそれがあるため，認証済み端末からの応答には認証シーケンスを一部省略することで，装置の負荷を低減しています。

ただし，使用する Supplicant ソフトウェアの種類によっては，認証シーケンスの省略によって認証済み端末の通信が途切れる問題が発生することがあります。そのため，認証済み端末に対する動作を切り替えるオプションを用意しています。本オプションはコンフィグレーションコマンド dot1x vlan dynamic supplicant-detection で選択を行い，次に示す二種類の動作を指定できます。

（a） shortcut

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（a） shortcut」を参照してください。

（b） disable

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 （b） disable」を参照してください。

（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 vlan dynamic timeout supp-timeout，再送回数はコンフィグレーションコマンド dot1x vlan dynamic 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 vlan dynamic reauthentication とコンフィグレーションコマンド dot1x vlan dynamic 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 vlan dynamic timeout tx-period
- コンフィグレーションコマンド dot1x vlan dynamic timeout reauth-period

(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 vlan dynamic 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 vlan dynamic 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

強制認証指定したポートに接続された端末の RADIUS 認証が，経路障害などで RADIUS サーバへリクエスト送信失敗または無応答となったときは，認証対象端末を認証許可状態にします。

強制認証を許可するポートにコンフィグレーションコマンド dot1x force-authorized vlan を設定します。また，強制認証を許可した端末へ EAP-Success 応答を送信するためにコンフィグレーションコマンド dot1x force-authorized eapol を設定します。

なお，強制認証は下記の条件を満たしたときに許可となります。

表 6-10 強制認証許可条件

項目	条件
コンフィグレーション	下記のコンフィグレーションがすべて設定されていること • aaa authentication dot1x default group radius • radius-server • dot1x system-auth-control • aaa authorized network default group radius • dot1x vlan dynamic enable • dot1x vlan dynamic radius-vlan ※1 • dot1x force-authorized vlan ※1 • vlan <VLAN ID> mac-based ※1 • switchport mac ※1※2 • switchport mode mac-vlan ※2
アカウントログ	RADIUS サーバへの認証要求送信で，下記のアカウントログが採取された場合 • Failed to connect to RADIUS server. (IP=xxx.xxx.xxx.xxx) アカウントログは運用コマンド show dot1x logging で確認できます。

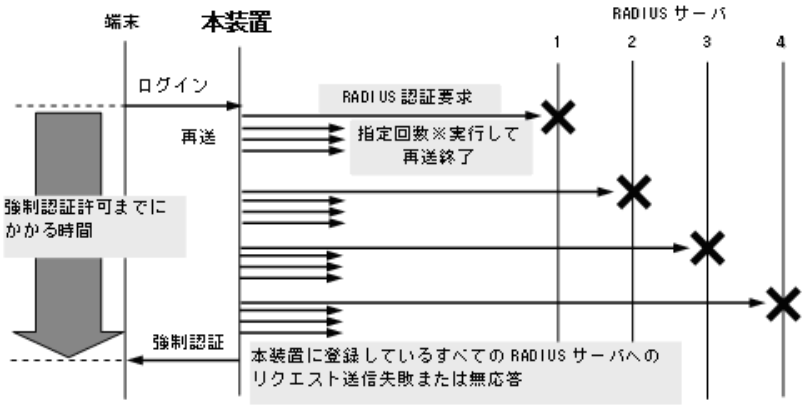
注※1
同じ VLAN ID を設定してください。

注※2
同じポートに設定してください。

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「6.4.2 認証機能 (9) 認証解除」のいずれかの解除機能により認証状態が解除されます。

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しているすべての RADIUS サーバのタイムアウト（リクエスト送信失敗または無応答）までとなります。

図 6-16 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 サーバの接続については，「コンフィグレーションガイド Vol.1 8 ログインセキュリティと RADIUS」を参照してください。

なお，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 vlan dynamic 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 vlan dynamic timeout reauth-period を設定します。

(b) 認証端末接続ポートのリンクダウンによる認証解除

ポート単位認証（静的）と同様です。「6.2.2 認証機能 (9) 認証解除 (b) 認証端末接続ポートのリンクダウンによる認証解除」を参照してください。

(c) 運用コマンドによる認証解除

ポート単位認証（静的）と同様です。「6.2.2 認証機能 (9) 認証解除 (c) 運用コマンドによる認証解除」を参照してください。

6.5 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　16.2　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。

6.6 アカウント機能

IEEE802.1X の認証結果は，本装置に内蔵のアカウントログ機能で記録されます。RADIUS サーバのアカウント機能はサポートしておりません。

なお，本装置の内蔵アカウントログには，IEEE802.1X の全認証モードの合計で最大 2100 行まで記録されます。2100 行を超えた場合，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 6-11 アカウントログ種別

アカウントログ種別	内容
LOGIN	認証操作に関する内容（成功・失敗）
LOGOUT	認証操作に関する内容（理由等）
SYSTEM	IEEE802.1X の動作に関する内容（強制認証許可も含む）

表 6-12 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 21 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. イベントごとのコンソール表示
   運用コマンド trace-monitor enable を実施済みの環境においても，アカウントログはイベント発生ごとにコンソールに表示しません。
2. 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。
3. syslog サーバへ出力
   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，装置全体のイベントトレース情報と合わせてアカウントログ情報を出力します。IEEE802.1X 認証の内蔵アカウントログ情報だけ

を syslog サーバへ出力または抑止指定することはできません。

4. 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 6-13 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

6.7 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 の情報を設定するコンフィグレーションコマンドの作成を行って設定します。(「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 6-14 認証で使用する属性名（その 1 Access-Request）

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。
User-Name	1	認証されるユーザ ID。
User-Password	2	ユーザパスワード。
NAS-IP-Address	4	認証を要求している，本装置の IP アドレス。 IP 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 IP アドレスを使用します。
NAS-Port	5	Supplicant を認証している認証単位の IfIndex。
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	本装置の MAC アドレス（大文字 ASCII，"-" 区切り)。
Calling-Station-Id	31	Supplicant の MAC アドレス（大文字 ASCII，"-" 区切り)。
NAS-Identifier	32	Authenticator を識別する文字列（ホスト名の文字列)。
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。
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 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。
Reply-Message	18	ユーザに表示されるメッセージ※1。

属性名	Type 値	解説
Tunnel-Type	64	トンネル・タイプ。 ポート単位認証（動的），VLAN 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。 ポート単位認証（動的），VLAN 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※2。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），VLAN 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）※3 （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

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※ 2

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 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※ 3

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，「12.2.3　ダイナミック VLAN モード収容 VLAN の VLAN 名称指定」を参照してください。

表 6-16 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。

注※
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。

表 6-17 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。

注※
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。

(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），VLAN 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 6-18 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），VLAN 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

6.8 IEEE802.1X の注意事項

6.8.1 IEEE802.1X と他機能を併用時の動作について

IEEE802.1X と他機能を併用時の動作について次の表に示します。

表 6-19 IEEE802.1X と他機能を併用時の動作

機能名	併用時の動作
スパニングツリー	常に Forwarding であるポートで認証が可能です。それ以外のポートでは認証を行わないように設定してください。 常に Forwarding であるポートは次のとおりです。 • PortFast ポート • ルートブリッジのポート
	BPDU の送受信およびスパニングツリーのトポロジー計算は，IEEE802.1X の認証状態に関係なく行われます。

6.8.2 IEEE802.1X 使用時の注意事項

(1) VLAN 単位認証（動的）での MAC アドレス学習のエージング時間設定について

VLAN 単位認証（動的）を使用する場合，MAC アドレスエントリのエージング時間に 0（無限）を指定しないでください。0（無限）を指定すると，端末の所属する VLAN が切り替わったときに，切り替わる前の VLAN の MAC アドレスエントリがエージングで消去されないで残り続けるため，不要な MAC アドレスエントリが蓄積することになります。切り替わる前の VLAN に不要な MAC アドレスエントリが蓄積した場合は，運用コマンド clear mac-address-table で消去してください。

(2) 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。VLAN 単位認証（動的）で認証した端末は，Dynamic を表示します。

(3) 認証済み端末のポート移動について

認証済み端末が同一 VLAN 内の認証をしないポートへ移動した場合，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。

(4) 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。

(5) 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 6-17　禁止構成例

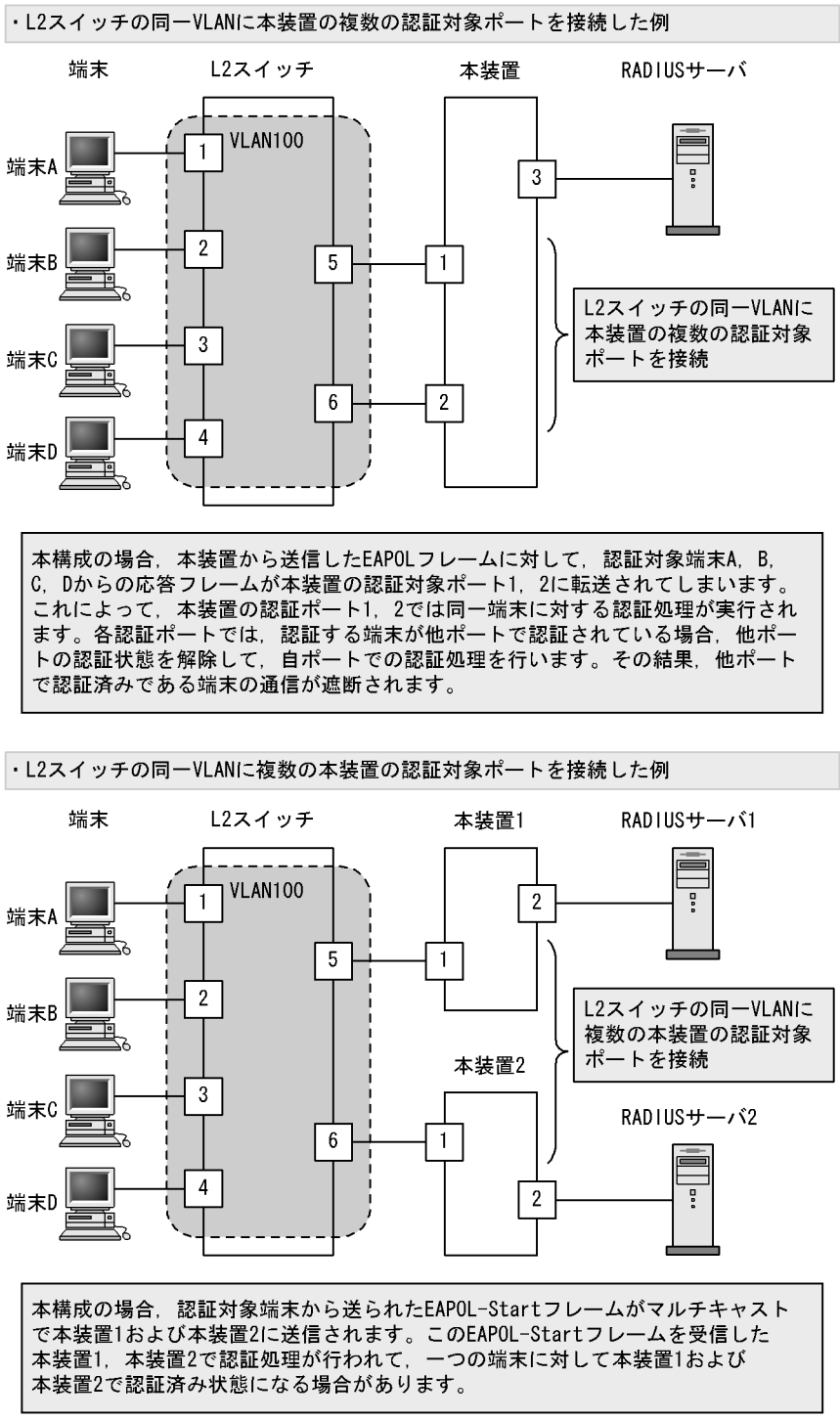
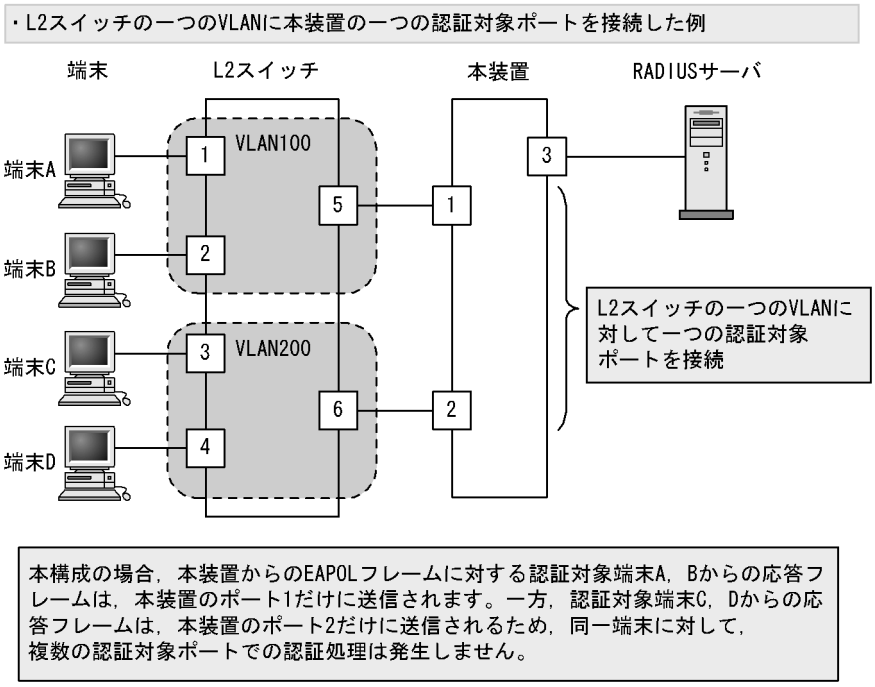


図 6-18　正しい構成例



(6) MAC VLAN をアクセスポートとして指定した場合の注意事項

- VLAN 単位認証（動的）の MAC VLAN をアクセスポートとして指定した場合，本装置の指定したポートから EAPOL フレームが送信されます。ただし，ユーザ側で EAPOL フレームに対する認証応答を行っても，指定ポートは認証除外ポートとして扱われます。これにより認証成功または失敗に関わらず，指定ポートでの疎通が可能となります。
- 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「12　レイヤ 2 認証の共通機能と共存使用」を参照してください。）

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		VLAN 単位
		静的	動的	動的
aaa authentication dot1x default	IEEE802.1X のユーザ認証を RADIUS サーバで行うことを設定します。	○	○	○
aaa authorization network default	RADIUS サーバから指定された VLAN 情報に従って，VLAN 単位認証（動的）を行う場合に設定します。	－	－	○
authentication arp-relay ※1	認証前状態の端末から送信される他機器宛て ARP フレームを，認証対象外のポートへ出力させます。	○	○	×
authentication ip access-group ※1	認証前状態の端末から送信される他機器宛ての IP フレームを，IPv4 アクセスリストを適用して設定されたフレームだけを認証対象外のポートへ出力させます。	○	○	×
dot1x force-authorized	RADIUS 認証方式を使用時，経路障害などで RADIUS サーバへのリクエスト失敗時に，当該ポートで認証要求した認証対象端末を強制的に認証許可状態とします。	○	×	×
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 force-authorized vlan	RADIUS 認証方式を使用時，経路障害などで RADIUS サーバへのリクエスト失敗時に当該ポートで認証要求した認証対象端末を強制的に認証許可状態とし，認証後 VLAN を割り当てます。	×	○	○
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 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 ※2	ポート単位認証を有効にします。	○	○	－
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。	○	○	○

コマンド名	説明	認証モード		
		ポート単位		VLAN 単位
		静的	動的	動的
dot1x timeout keep-unauth ※3	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。	○	○	－
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。	○	○	－
dot1x vlan dynamic enable	VLAN 単位認証（動的）を有効にします。	－	－	○
dot1x vlan dynamic 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 vlan dynamic 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 vlan dynamic radius-vlan	VLAN 単位認証（動的）で，RADIUS サーバからの VLAN 情報により動的な VLAN 割り当てを許可する VLAN を設定します。	－	－	○
dot1x vlan dynamic reauthentication	認証済み端末の再認証の有効／無効を設定します。	－	－	○
dot1x vlan dynamic 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 vlan dynamic 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 vlan dynamic timeout reauth-period	認証済み端末の再認証を行う間隔を設定します。	－	－	○
dot1x vlan dynamic timeout server-timeout	認証サーバからの応答待ち時間を設定します。	－	－	○
dot1x vlan dynamic 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 vlan dynamic 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）
VLAN 単位　動的：VLAN 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
設定の詳細については，「12　レイヤ 2 認証の共通機能と共存使用」を参照してください。

注※ 2
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※ 3
本コマンドの設定は，ポート単位認証（静的）およびポート単位認証（動的）のシングルモードだけ適用します。

7.1.2　IEEE802.1X のコンフィグレーションを設定する前に

IEEE802.1X で認証モードを設定する場合は，コンフィグレーションを設定する前に，下記を設定してください。

［設定のポイント］

下記の認証モードまたは機能を使用する場合，設定の最初の段階でシステムファンクションリソースの割り当てをコンフィグレーションで設定する必要があります。

- ポート単位認証（動的）
- 認証専用 IPv4 アクセスリスト

システムファンクションリソースの割り当て設定は装置の再起動が必要です。システムファンクションリソースの割り当てについての詳細は「コンフィグレーションガイド Vol.1　9.1.6 システムファンクションリソース配分の設定」を参照してください。
本例ではフィルタと拡張認証機能を割り当てます。

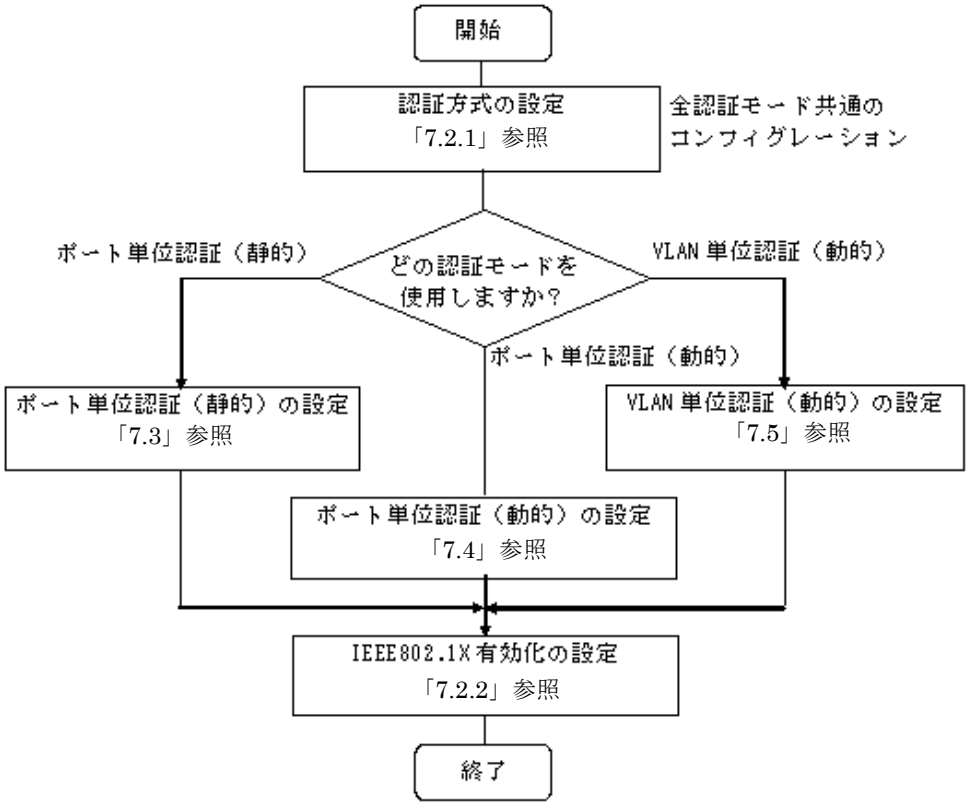
［コマンドによる設定］

1. **(config)# system function filter extended-authentication**
   ```
   Please execute the reload command after save,
   because this command becomes effective after reboot.
   ```
   システムリファンクションソースとしてフィルタと拡張認証機能を割り当てます。設定の保存と装置再起動を促すメッセージを表示します。
2. **(config)# end**
   # copy running-config startup-config
   ```
   Do you wish to copy from running-config to startup-config? (y/n): y
   ```
   @# reload
   ```
   Restart OK? (y/n): y
   ```
   コンフィグレーションの設定を保存すると，プロンプトに " @ " を表示しますので，装置を再起動してください。

7.1.3 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。
   - 認証方式の設定：「7.2.1　認証方式の設定」

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」
   - VLAN 単位認証（動的）の設定：「7.5　VLAN 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。
   - 「7.2.2　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 default group radius • radius-server • dot1x system-auth-control
ポート単位認証（静的）	• vlan <VLAN ID list> • dot1x port-control auto • switchport mode access • switchport access vlan
ポート単位認証（動的）	• vlan <VLAN ID list> mac-based • dot1x port-control auto • switchport mode mac-vlan • switchport mac vlan
VLAN 単位認証（動的）	• vlan <VLAN ID list> mac-based • aaa authorization network default • dot1x vlan dynamic enable • dot1x vlan dynamic radius-vlan • switchport mode mac-vlan • switchport 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 認証方式の設定

(1) 認証方式の設定

[設定のポイント]

IEEE802.1X の認証を RADIUS サーバで行うことを設定します。

[コマンドによる設定]

1. **(config)# aaa authentication dot1x default group radius**
   RADIUS サーバで IEEE802.1X の認証を行うように設定します。

(2) RADIUS サーバの設定

IEEE802.1X の認証に使用する RADIUS サーバを設定します。

[設定のポイント]

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 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。

[コマンドによる設定]

1. **radius-server host 192.168.10.200 key "L2auth"**
   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，timeout，retransmit は省略時の初期値が適用されます。

[注意事項]

1. 本設定省略時は，IEEE802.1X で認証できません。
2. RADIUS サーバ情報は，本装置全体で最大 4 エントリまで設定できます。ログインセキュリティ機能やほかのレイヤ 2 認証機能と共用となることを考慮して，RADIUS サーバ情報を設定してください。

7.2.2 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。

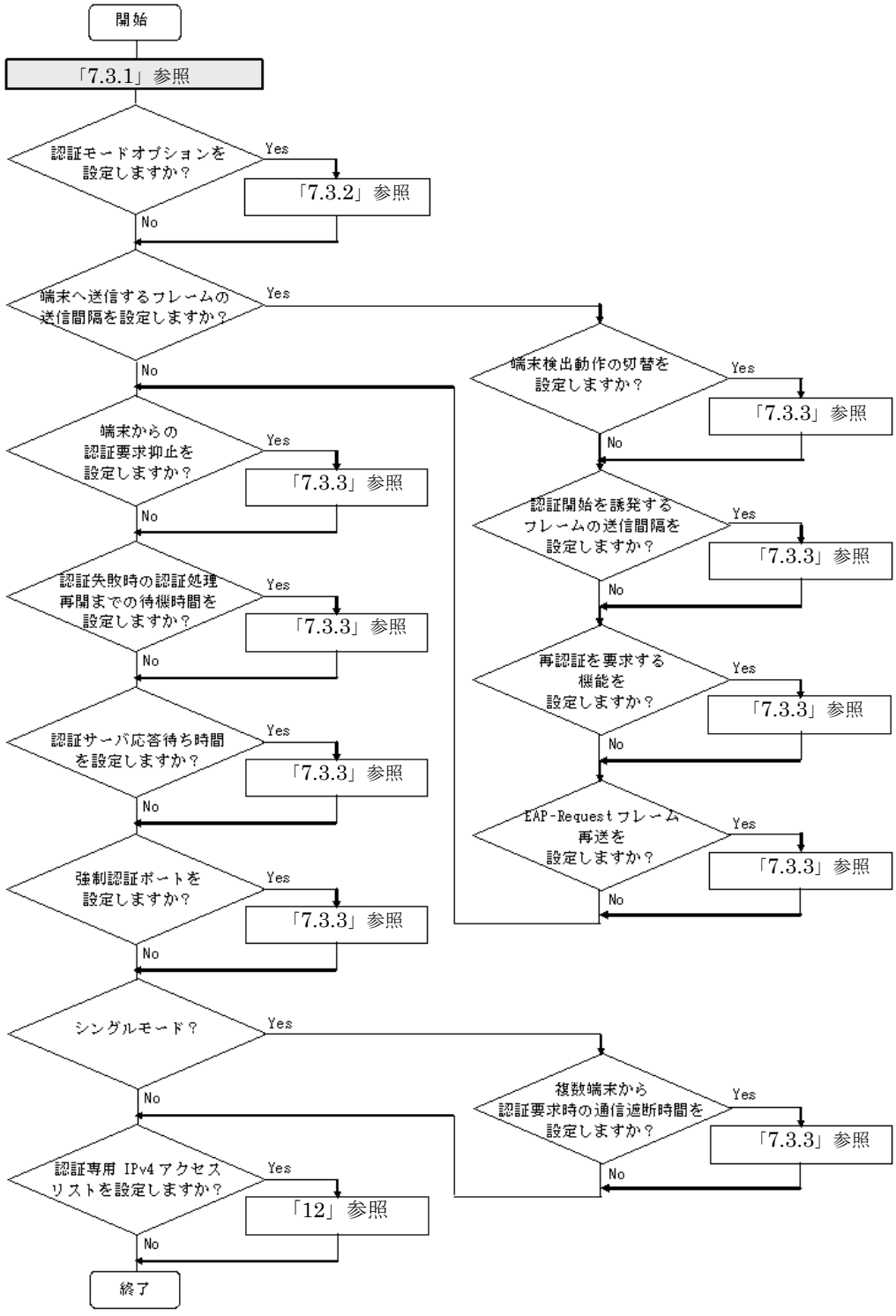
[コマンドによる設定]

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



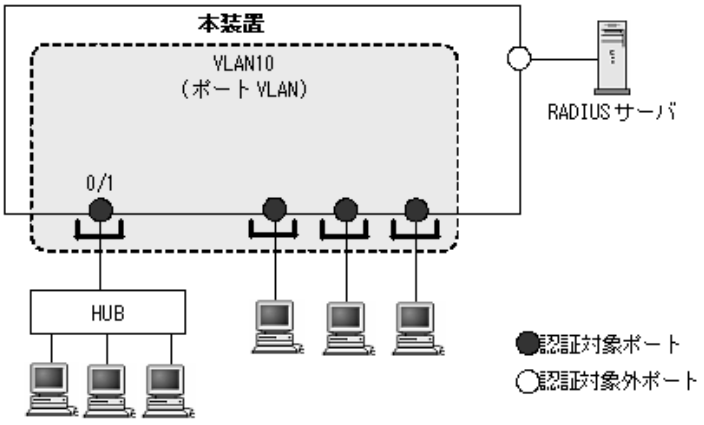
各設定の詳細は，下記を参照してください。

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. 強制認証ポートの設定：「7.3.3　認証処理に関する設定　(8) 強制認証ポートの設定」
8. 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」
9. 認証専用 IPv4 アクセスリストの設定：「12　レイヤ 2 認証の共通機能と共存使用」

7.3.1　ポート単位認証（静的）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 fastethernet 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。

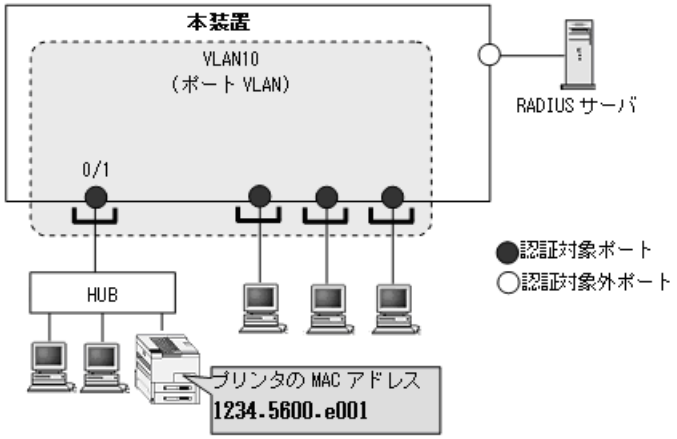
4. **(config-if)# dot1x port-control auto**
   (config-if)# exit
   ポート単位認証を有効にします。

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 fastethernet 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，定期的な EAP-Request/Identity の送信を行いません。

[コマンドによる設定]

1. **(config)# interface fastethernet 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。

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 のデフォルト値が 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 fastethernet 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 fastethernet 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 fastethernet 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 fastethernet 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 fastethernet 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 fastethernet 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 fastethernet 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） 強制認証ポートの設定

［設定のポイント］

ポート単位認証（静的）の対象ポートで，強制認証を許可するポートに設定します。

［コマンドによる設定］

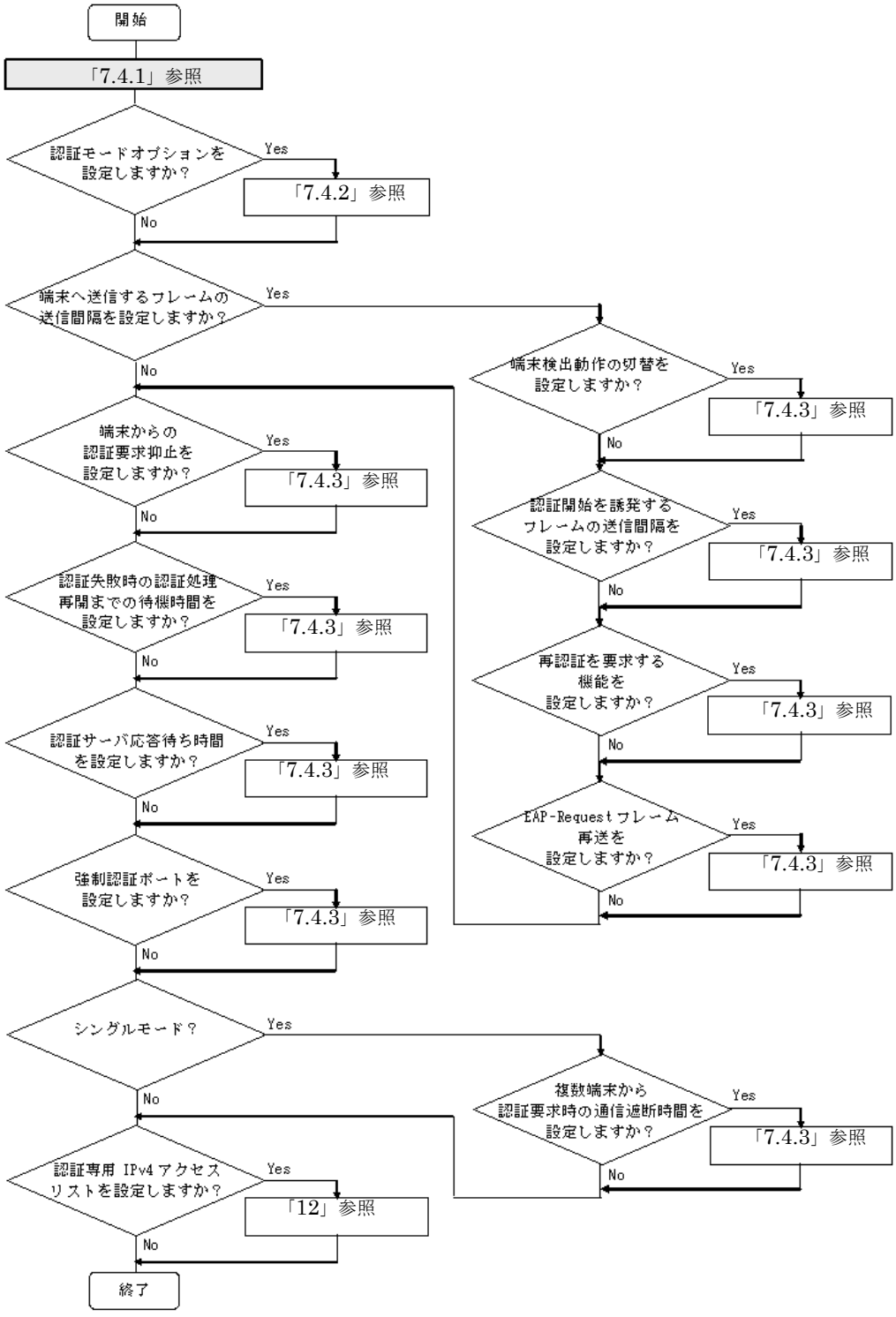
1. **(config)# interface fastethernet 0/1**
   (config-if)# dot1x force-authorized
   (config-if)# exit
   ポート 0/1 を強制認証対象ポートに設定します。

2. **(config)# 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。

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



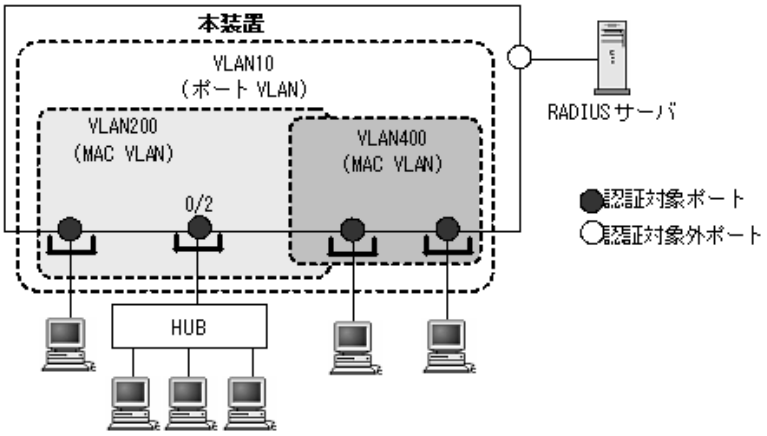
各設定の詳細は，下記を参照してください。

1. ポート単位認証（静的）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. 強制認証ポートの設定：「7.4.3 認証処理に関する設定（8）強制認証ポートの設定」
8. 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」
9. 認証専用 IPv4 アクセスリストの設定：「12 レイヤ 2 認証の共通機能と共存使用」

7.4.1 ポート単位認証（動的）の設定

物理ポート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。

［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 fastethernet 0/2**
   (config-if)# switchport mode mac-vlan
   (config-if)# switchport mac vlan 200
   (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 と認証後 VLAN200 を設定します。

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。

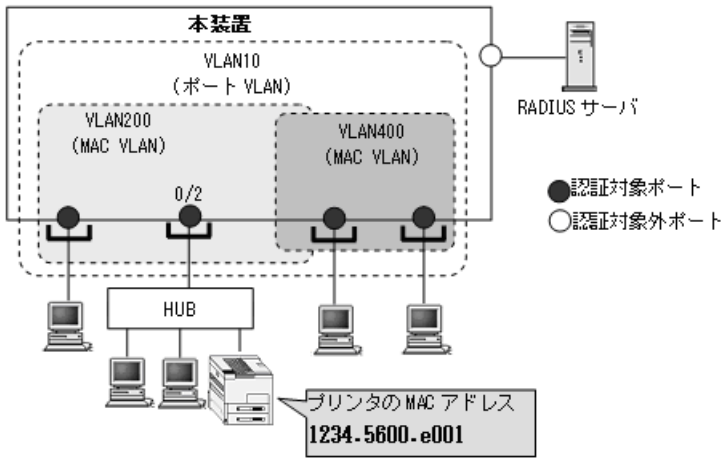
5. **(config-if)# dot1x port-control auto**
   (config-if)# exit
   ポート単位認証（動的）を有効にします。

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)# mac-address-table static 1234.5600.e001 vlan 200 interface**

fastethernet 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。

2. **(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) 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） 強制認証ポートの設定

［設定のポイント］

ポート単位認証（動的）の対象ポートで，強制認証を許可して割り当てる認証後 VLAN を設定します。

［コマンドによる設定］

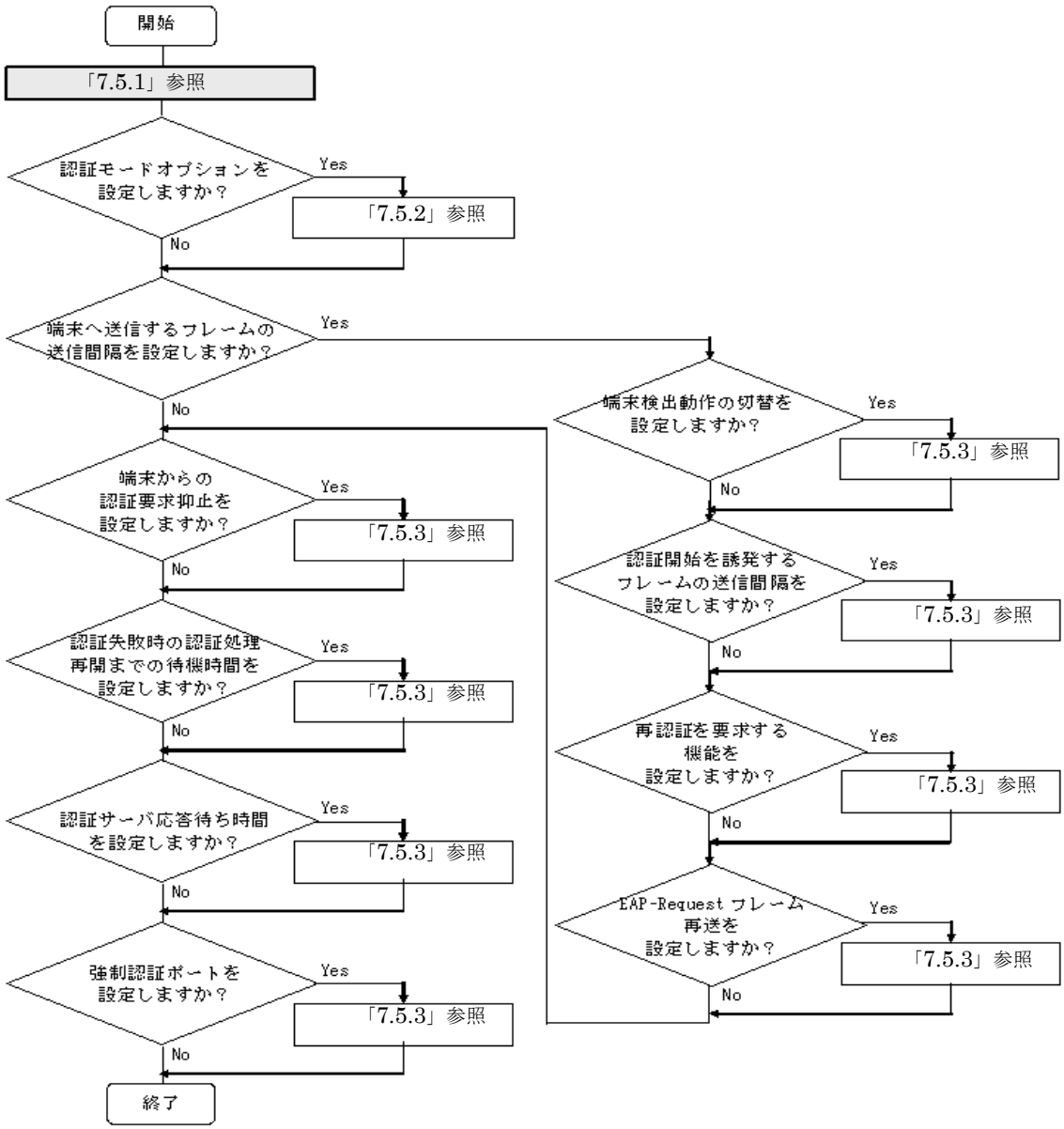
1. **(config)# interface fastethernet 0/2**
   (config-if)# dot1x force-authorized vlan 200
   (config-if)# exit
   ポート 0/2 で，強制認証を許可して割り当てる認証後 VLAN の VLAN ID を設定します。

2. **(config)# 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。

7.5 VLAN 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 VLAN 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 7-8 VLAN 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（静的）の設定：「7.5.1 VLAN 単位認証（動的）の設定」
2. 認証モードオプションの設定：「7.5.2 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：「7.5.2 認証モードオプションの設定」
   - 認証開始を誘発するフレームの送信制御：「7.5.3 認証処理に関する設定（1）端末へ認証開始を誘

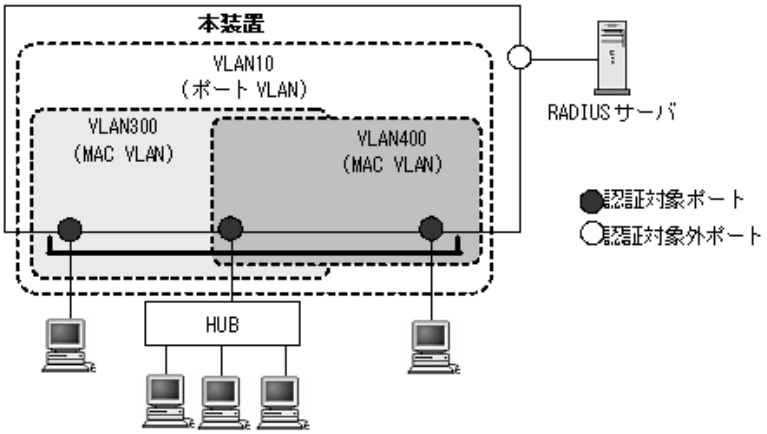
発するフレームの送信間隔の設定」
- 再認証を要求する機能：「7.5.3　認証処理に関する設定（2）端末へ再認証を要求する機能の設定」
- EAP-Request フレーム再送：「7.5.3　認証処理に関する設定（3）端末へ EAP-Request フレーム再送の設定」

4. 端末からの認証抑止の設定：「7.5.3　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：「7.5.3　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：「7.5.3　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. 強制認証ポートの設定：「7.5.3　認証処理に関する設定（7）強制認証ポートの設定」

7.5.1 VLAN 単位認証（動的）の設定

MAC VLAN に所属する端末を認証の対象とします。

図 7-9　VLAN 単位認証（動的）の構成例



［設定のポイント］

MAC VLAN を設定し，その VLAN で VLAN 単位認証（動的）を有効にします。
認証した端末を RADIUS サーバから指定された VLAN に従って登録します。また，コンフィグレーションコマンド dot1x vlan dynamic radius-vlan により RADIUS サーバから指定される VLAN のリストを登録します。

［コマンドによる設定］

1. **(config)# vlan 300,400 mac-based**
   (config-vlan)# exit
   VLAN ID 300，400 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)# dot1x vlan dynamic radius-vlan 300,400**
   VLAN ID 300，400 を VLAN 単位認証（動的）の対象に設定します。

4. **(config)# aaa authorization network default group radius**
   RADIUS サーバから指定された VLAN に従って登録します。

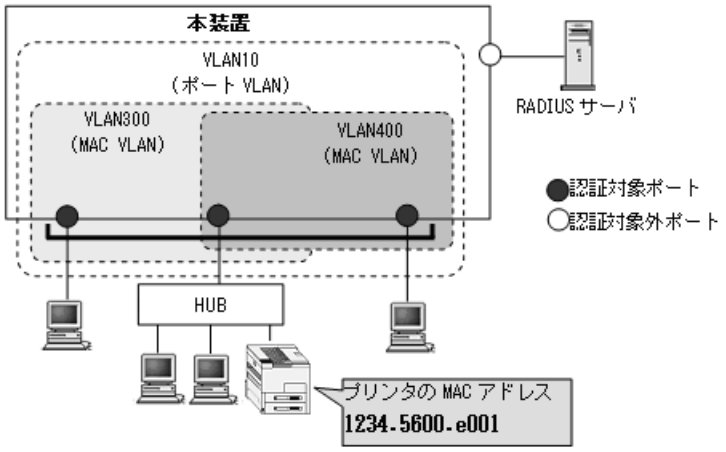
5. **(config)# dot1x vlan dynamic enable**
   VLAN 単位認証（動的）を有効にします。

7.5.2 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，「7.5.1 VLAN 単位認証（動的）の設定」で設定した VLAN ID 300 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 7-10 VLAN 単位認証（動的）の認証除外の構成例



[設定のポイント]
VLAN 単位認証（動的）では，MAC VLAN に MAC アドレスを登録します。

[コマンドによる設定]

1. **(config)# vlan 300 mac-based**
   (config-vlan)# mac-address 1234.5600.e001
   (config-vlan)# exit
   VLAN ID 300 の MAC VLAN で通信可能とする 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 300 で通信できます。

(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，定期的な EAP-Request/

Identity の送信を行いません。

［コマンドによる設定］

1. **(config)# dot1x vlan dynamic supplicant-detection shortcut**
   VLAN 単位認証（動的）で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。

7.5.3 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 のデフォルト値が 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)# dot1x vlan dynamic timeout tx-period 300**
   VLAN 単位認証（動的）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)# dot1x vlan dynamic reauthentication**
   (config)# dot1x vlan dynamic timeout reauth-period 360
   VLAN 単位認証（動的）での再認証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)# dot1x vlan dynamic timeout supp-timeout 60**
   VLAN 単位認証（動的）での EAP-Request フレームの再送時間を 60 秒に設定します。

2. **(config)# dot1x vlan dynamic max-req 3**
   VLAN 単位認証（動的）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)# dot1x vlan dynamic reauthentication**
   (config)# dot1x vlan dynamic ignore-eapol-start
   VLAN 単位認証（動的）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)# dot1x vlan dynamic timeout quiet-period 300**
   VLAN 単位認証（動的）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)# dot1x vlan dynamic timeout server-timeout 300**
   VLAN 単位認証（動的）の対象ポートで，強制認証を許可するポートに設定します。

（7） 強制認証ポートの設定

［設定のポイント］

VLAN 単位認証（動的）の対象ポートで，強制認証を許可して割り当てる認証後 VLAN を設定します。

［コマンドによる設定］

1. **(config)# interface fastethernet 0/3**
   (config-if)# switchport mode mac-vlan
   (config-if)# switchport mac vlan 300
   (config-if)# dot1x force-authorized vlan 300
   (config-if)# exit
   ポート 0/3 で，強制認証を許可して割り当てる認証後 VLAN の VLAN ID を設定します。

2. **(config)# 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。

7.6　IEEE802.1X のオペレーション

7.6.1　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 の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 の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。

7.6.2　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 の設定一覧は，運用コマンド show dot1x で確認してください。

図 7-11　show dot1x の実行結果

```
> show dot1x

Date 2008/06/23 21:24:20 UTC
System 802.1X : Enable
   AAA Authentication Dot1x    : Enable
       Authorization Network   : Enable

Port/ChGr/VLAN     AccessControl  PortControl        Status        Supplicants
Port 0/1           ---            Auto               Authorized    1
Port 0/26(Dynamic) Multiple-Auth  Auto               ---           1
ChGr 1             ---            Auto               Authorized    1
VLAN(Dynamic)      Multiple-Auth  Auto               ---           4

>
```

(b) ポート単位認証の状態表示

ポート単位認証におけるポートごとの状態情報を運用コマンド show dot1x port で確認してください。
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 で確認してください。

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，認証している端末の情報を表示します。

図 7-12 show dot1x port（detail パラメータ指定時）の実行結果

```
> show dot1x port 0/1 detail

Date 2008/06/23 21:27:16 UTC

Port 0/1
AccessControl  : ---                          PortControl    : Auto
Status         : Authorized                   Last EAPOL     : 0013.20a5.3e4f
Supplicants    : 1 / 1                        ReAuthMode     : Enable
TxTimer        : 3                            ReAuthTimer    : 5
ReAuthSuccess  : 972                          ReAuthFail     : 1
KeepUnauth     : 5

 Supplicants MAC  F  Status         AuthState      BackEndState   ReAuthSuccess
                     SessionTime(s) Date/Time
 0013.20a5.3e4f   *  Authorized     Authenticated  Idle           878
                     4430           2008/06/23 20:13:26

>
```

(c) VLAN 単位認証（動的）の状態表示

VLAN 単位認証（動的）における VLAN ごとの状態は，運用コマンド show dot1x vlan dynamic で確認してください。VLAN ID を指定すると，指定した VLAN の情報を表示します。detail パラメータを指定すると，認証している端末の情報を表示します。

図 7-13 show dot1x vlan dynamic（detail パラメータ指定時）の実行結果

```
> show dot1x vlan dynamic detail

Date 2008/06/23 21:27:49 UTC

VLAN(Dynamic)
AccessControl  : Multiple-Auth                PortControl    : Auto
Status         : ---                          Last EAPOL     : 0006.0003.0001
Supplicants    : 4 / 4 / 256                  ReAuthMode     : Enable
TxTimer        : 30                           ReAuthTimer    : 60
ReAuthSuccess  : 5070                         ReAuthFail     : 1
SuppDetection  : Shortcut
VLAN(s): 4,40,400,4000

 Supplicants MAC  F  Status         AuthState      BackEndState   ReAuthSuccess
                     SessionTime(s) Date/Time
 [VLAN 4]            VLAN(Dynamic) Supplicants : 1
 0006.0003.0001      Authorized     Authenticated  Idle           0
                     337            2008/06/23 21:22:12
 [VLAN 40]           VLAN(Dynamic) Supplicants : 1
 0006.0003.0002   *  Authorized     Authenticated  Idle           5
                     336            2008/06/23 21:22:12
 [VLAN 400]          VLAN(Dynamic) Supplicants : 1
 0006.0003.0003      Authorized     Authenticated  Idle           5
                     336            2008/06/23 21:22:12
 [VLAN 4000]         VLAN(Dynamic) Supplicants : 1
 0006.0003.0004      Authorized     Authenticated  Idle           5
                     336            2008/06/23 21:22:12

>
```

7.6.3 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 7-14 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 7-15 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 解説

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。（本装置では Internet Explorer 6 でのご使用を推奨します。）

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。
- レガシーモード
  MAC VLAN による VLAN 切り替えにより，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。（Ver.1.3.x までのダイナミック VLAN モードが該当します。）

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。

認証には，本装置に内蔵した認証用 DB（内蔵 Web 認証 DB と呼びます）によるローカル認証方式と，外部に設置した RADIUS サーバに認証要求する RADIUS 認証方式があり，どちらかの方式を選択できます。

なお，Web 認証では IPv4 アドレスだけに対応しています。

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一覧

機能		固定 VLAN	ダイナミック VLAN	レガシー
ローカル認証	内蔵 Web 認証 DB	○ 「8.2.1」参照 「8.6.1」参照	○ 「8.3.1」参照 「8.6.1」参照	○ 「8.4.1」参照 「8.6.1」参照
	ユーザ ID	1 ～ 16 文字 「9.7.2」参照	1 ～ 16 文字 「9.7.2」参照	1 ～ 16 文字 「9.7.2」参照
	パスワード	1 ～ 16 文字 「9.7.2」参照	1 ～ 16 文字 「9.7.2」参照	1 ～ 16 文字 「9.7.2」参照
	VLAN （認証後の VLAN）	○ 「9.7.2」参照	○ 「9.7.2」参照	○ 「9.7.2」参照
RADIUS 認証	RADIUS サーバ	外部サーバ 「8.2.1」参照 「8.6.2」参照 「9.2.1」参照	外部サーバ 「8.3.1」参照 「8.6.2」参照 「9.2.1」参照	外部サーバ 「8.4.1」参照 「8.6.2」参照 「9.2.1」参照
	ユーザ ID	1 ～ 32 文字 「8.2.1」参照 「8.6.2」参照	1 ～ 32 文字 「8.3.1」参照 「8.6.2」参照	1 ～ 32 文字 「8.4.1」参照 「8.6.2」参照

機能		固定 VLAN	ダイナミック VLAN	レガシー
	パスワード	1 ～ 32 文字 「8.2.1」参照 「8.6.2」参照	1 ～ 32 文字 「8.3.1」参照 「8.6.2」参照	1 ～ 32 文字 「8.4.1」参照 「8.6.2」参照
	VLAN (認証後の VLAN)	○ 「8.2.1」参照 「8.6.2」参照	○ 「8.3.1」参照 「8.6.2」参照	○ 「8.4.1」参照 「8.6.2」参照 「9.5.1」参照
	強制認証	○ 「8.2.2」参照	○ 「8.3.2」参照	○ 「8.4.2」参照
	認証許可ポート設定	○ 「9.3.2」参照	○ 「9.4.2」参照	○ 「9.5.2」参照
	プライベートトラップ	○ 「8.5」参照	○ 「8.5」参照	○ 「8.5」参照
端末 IP アドレス配布	内蔵 DHCP サーバ	×	○ 「8.11」参照 「9.6」参照	○ 「8.11」参照 「9.6」参照
最大認証ユーザ数	ポート単位	1024 「8.2.2」参照 「9.3.2」参照	256 「8.3.2」参照 「9.4.2」参照	256 「8.4.2」参照 「9.5.2」参照
	装置単位	1024 「8.2.2」参照 「9.3.2」参照	256 「8.3.2」参照 「9.4.2」参照	256 「8.4.2」参照 「9.5.2」参照
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	○ 「8.4.2」参照 「9.2.2」参照
	認証前通過（認証専用 IPv4 アクセスリスト)	○ 「12」参照	○ 「12」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	×
	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	○ 「8.4.2」参照 「9.5.2」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	○ 「8.4.2」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	×
	MAC アドレステーブルエージング監視	×	×	○ 「8.4.2」参照 「9.5.2」参照

機能		固定 VLAN	ダイナミック VLAN	レガシー
	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	○ 「8.4.2」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	○ 「8.4.2」参照
	Web 画面操作	○ 「9.7.12」参照	○ 「9.7.12」参照	○ 「9.7.12」参照
	運用コマンド	○ 「8.2.2」参照	○ 「8.3.2」参照	○ 「8.4.2」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	○ 「8.5」参照	○ 「8.5」参照	×
アカウントログ	本装置内蔵アカウントログ	全モード合わせて 2100 行 「8.5」参照		

（凡例） ○：サポート　×：未サポート
「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

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			固定 VLAN	ダイナミック VLAN	レガシー
VLAN 種別	ポート VLAN		○	×	×
	プロトコル VLAN		×	×	×
	MAC VLAN		△	○	○
デフォルト VLAN			○	×	×
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		×	×	×
	MAC ポート	Untagged	×	○	○
		Tagged	△	×	×
インタフェース種別	fastethernet		○	○	○
	gigabitethernet		○	○	○
	port channel		×	×	○

（凡例）
○：動作可
×：動作不可

△：switchport mac dot1q vlan 設定有のとき，動作可

次項からは，「固定 VLAN モード」「ダイナミック VLAN モード」「レガシーモード」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，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。

8.2.1 認証方式

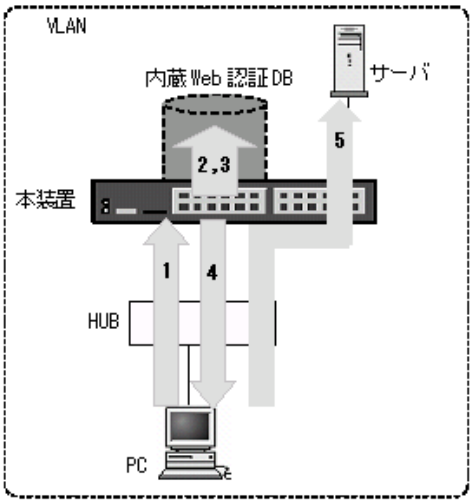
本装置では，ローカル認証方式と RADIUS 認証方式をサポートしています。認証方式は，Web 認証全認証モード共通で使用します。

（1） 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，認証成功画面を 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。

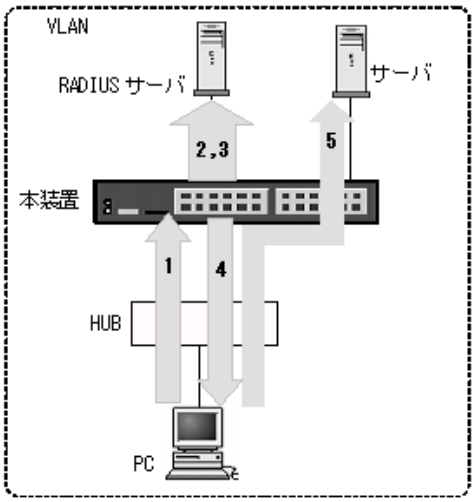
（a） VLAN 制限

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） 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，認証成功画面を 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。

8.2.2　認証機能

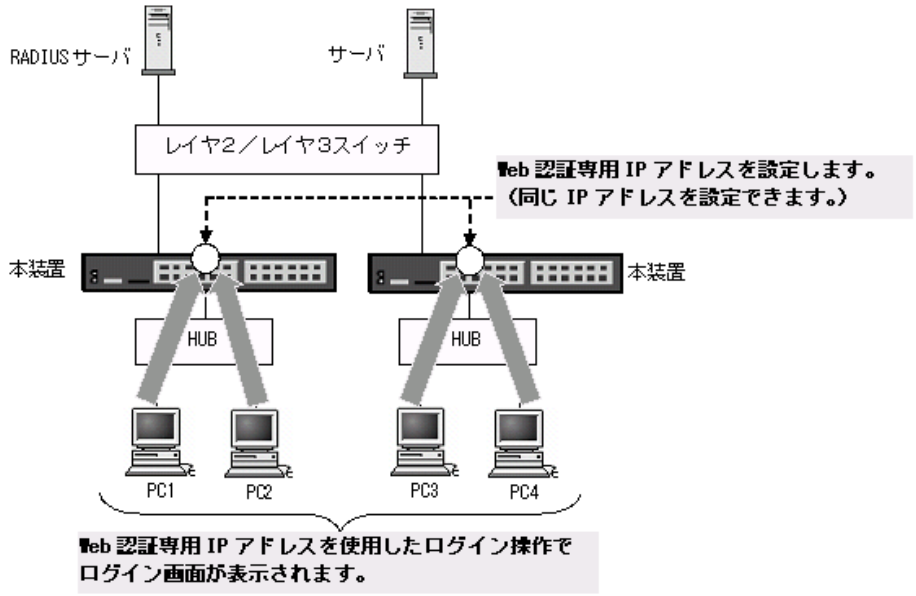
（1） Web 認証専用 IP アドレス

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 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。

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 で，コンフィグレーションで 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 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 redirect tcp-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。

(3) 認証成功後の自動表示 URL 指定

認証成功画面表示後に自動的に表示する URL をコンフィグレーションで指定できます。

認証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。

(4) 強制認証ポート指定

強制認証指定したポートに接続された端末の RADIUS 認証が，経路障害などで RADIUS サーバへリクエスト送信失敗または無応答となったときは，認証対象端末を認証許可状態にします。

強制認証を許可するポートにコンフィグレーションコマンド web-authentication static-vlan force-authorized を設定します。

なお，強制認証は下記の条件を満たしたときに許可となります。

表 8-3 強制認証許可条件

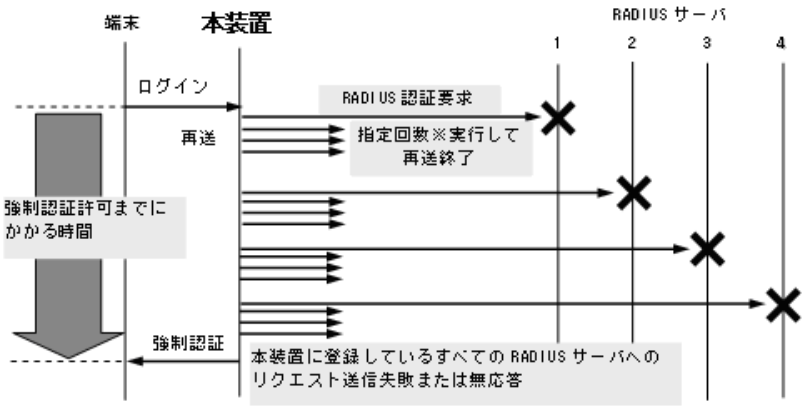
項目	条件
コンフィグレーション	下記のコンフィグレーションがすべて設定されていること • aaa authentication web-authentication default group radius • radius-server • web-authentication system-auth-control • web-authentication port ※ • web-authentication static-vlan force-authorized ※
アカウントログ	RADIUS サーバへの認証要求送信で，下記のアカウントログが採取された場合 No=21 NOTICE:LOGIN:(付加情報) Login failed ; Failed to connection to RADIUS server. 付加情報：MAC，USER，IP，PORT，VLAN No=258 NOTICE:LOGIN:(付加情報) Login failed ; RADIUS request send error. 付加情報：MAC，USER，PORT 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。

注※
同じイーサネットポートに設定してください。

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 (6) 認証状態からのログアウト」のいずれかの解除機能により認証状態が解除されます。

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（リクエスト送信失敗または無応答）までとなります。

図 8-4　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 サーバの接続については，「コンフィグレーションガイド Vol.1　8　ログインセキュリティと RADIUS」を参照してください。

（5） 最大認証ユーザ数

最大認証ユーザ数の設定は，装置単位とポート単位の両方で指定することができます。最大認証ユーザ数はコンフィグレーションコマンド web-authentication static-vlan max-user で最大 1024 台まで設定できます。

装置単位とポート単位を同時に設定することは可能ですが，どちらかが最大数に達した場合，それ以降の新規ユーザの認証はできません。

また，運用中に認証済みユーザ数より最大認証ユーザ数を少なく変更した場合，認証済みのユーザは継続通信できますが，新規ユーザの認証はできません。

（6） 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。

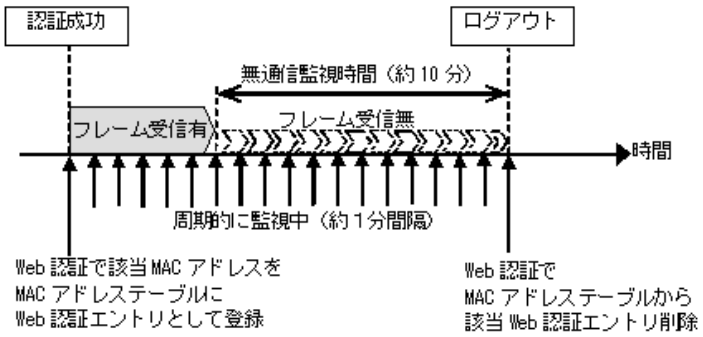
最大接続時間はコンフィグレーションコマンド web-authentication max-timer で設定できます。

(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 8-5 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。

- 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。

(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「9.7.12　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。

(7) ローミング（認証済み端末のポート移動）

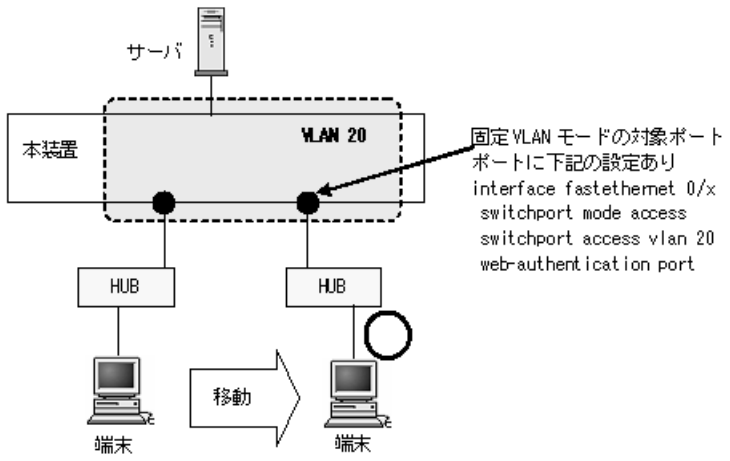
HUB などを経由して接続した認証済み端末を，リンクダウンしないでポート移動した場合でも，認証済み状態のまま継続して通信可能にします。

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。

図 8-6　固定 VLAN モード　ローミング概要図



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）

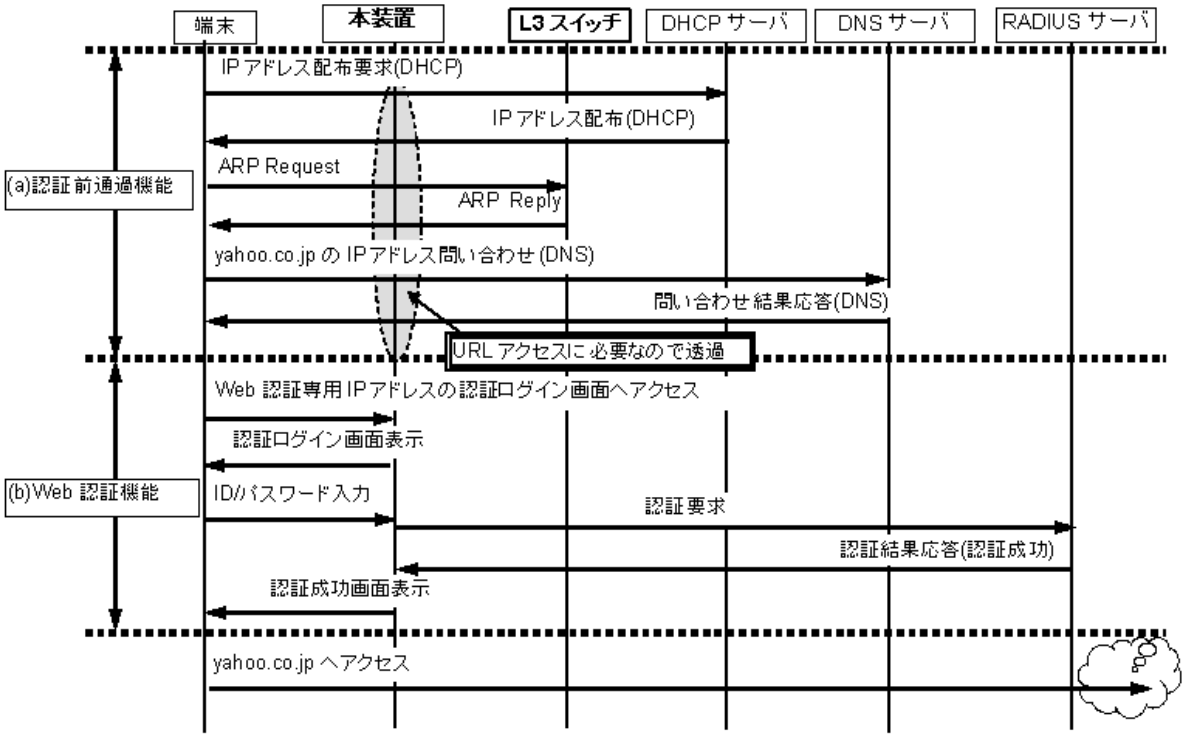
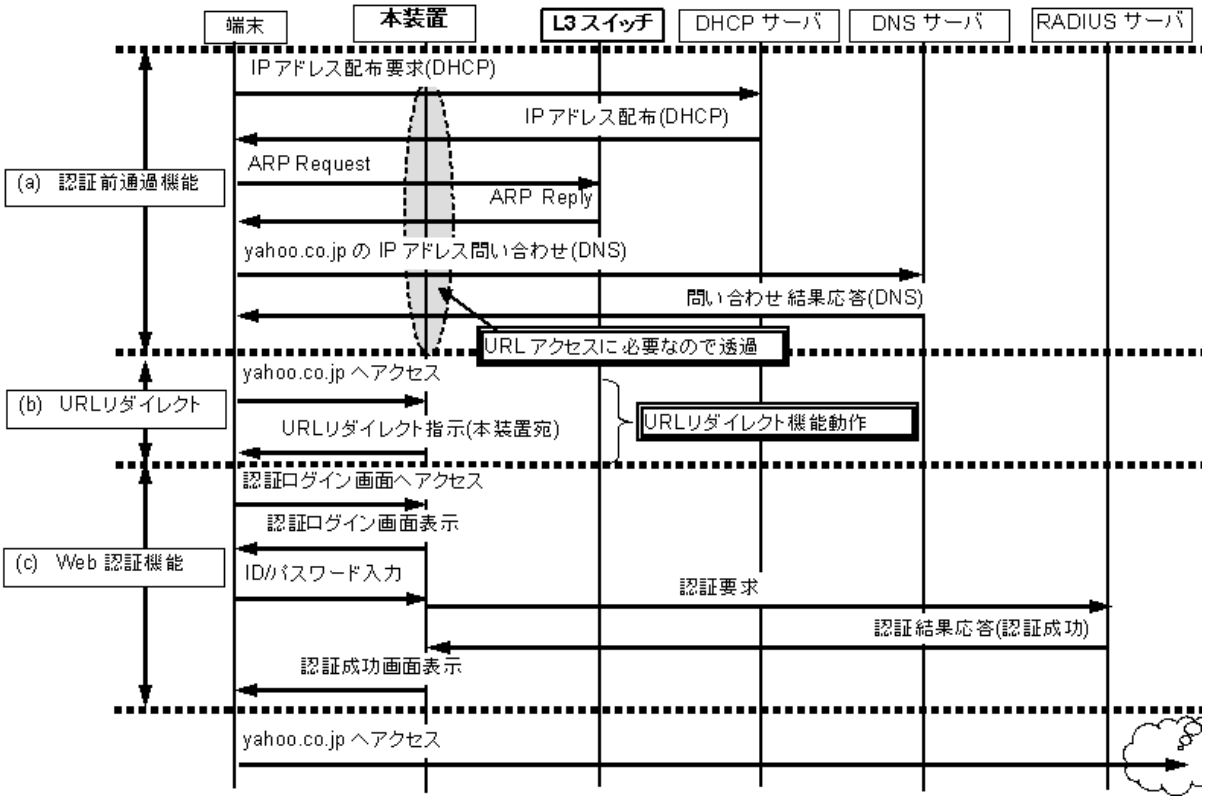


図 8-8 認証動作（URL リダイレクト機能使用時）



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。）

レガシーモードは，認証後 VLAN を設定することで動作しますが，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，ローカル認証方式および RADIUS 認証方式で認証できます。

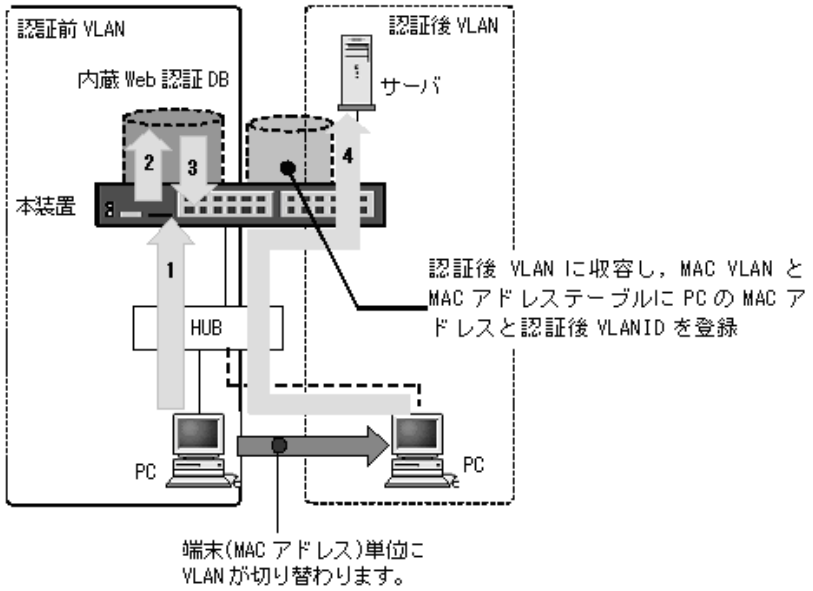
8.3.1 認証方式

（1） 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 Web 認証用内蔵 DB 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，認証成功画面を 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。

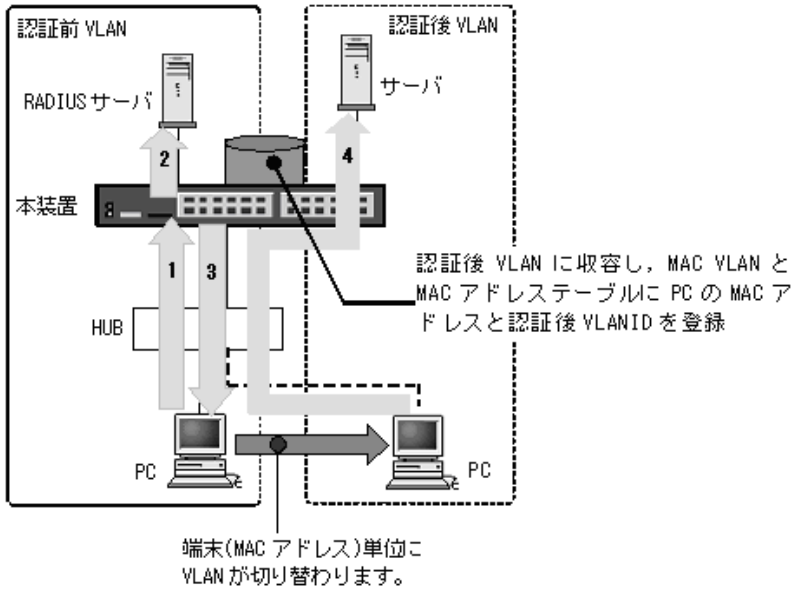
(a) 認証後 VLAN への収容条件

内蔵 Web 認証 DB の該当ユーザのエントリに登録されている VLAN ID により認証後 VLAN へ収容します。ただし，VLAN ID がダイナミック VLAN モード対象ポートの VLAN 設定（コンフィグレーションコマンド switchport mac vlan）に含まれない場合は，認証失敗となります。

(2) 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，認証成功画面を 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

RADIUS サーバの当該ユーザのエントリに登録されている VLAN ID により認証後 VLAN へ収容します。ただし，VLAN ID がダイナミック VLAN モード対象ポートの VLAN 設定（コンフィグレーションコマンド switchport mac vlan）に含まれない場合は，認証失敗となります。

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) 認証成功後の自動表示 URL 指定

認証成功画面表示後に自動的に表示する URL をコンフィグレーションで指定できます。また，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 10 秒) 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。

認証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。

(4) 強制認証ポート指定

強制認証指定したポートに接続された端末の RADIUS 認証が，経路障害などで RADIUS サーバへリクエスト送信失敗または無応答となったときは，認証対象端末を認証許可状態にします。

強制認証を許可するポートにコンフィグレーションコマンド web-authentication force-authorized vlan を設定します。

なお，強制認証は下記の条件を満たしたときに許可となります。

表 8-4　強制認証許可条件

項目	条件
コンフィグレーション	下記のコンフィグレーションがすべて設定されていること • aaa authentication web-authentication default group radius • radius-server • web-authentication system-auth-control • vlan <VLAN ID list> mac-based ※1 • web-authentication port ※2 • web-authentication force-authorized vlan ※1※2 • switchport mac vlan ※1※2 • switchport mode mac-vlan ※2
アカウントログ	RADIUS サーバへの認証要求送信で，下記のアカウントログが採取された場合 No=21 NOTICE:LOGIN:(付加情報) Login failed ; Failed to connection to RADIUS server. 付加情報：MAC，USER，IP，PORT，VLAN No=258 NOTICE:LOGIN:(付加情報) Login failed ; RADIUS request send error. 付加情報：MAC，USER，PORT 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。

注※ 1
同じ VLAN ID を設定してください。

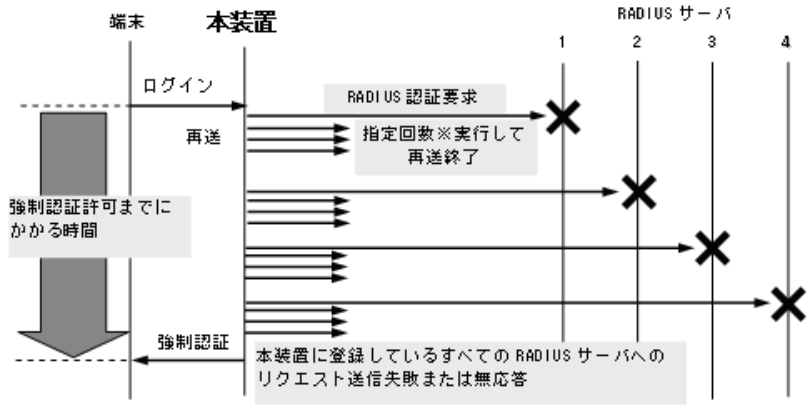
注※ 2
同じイーサネットポートに設定してください。

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　(6) 認証

状態からのログアウト」のいずれかの解除機能により認証状態が解除されます。

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（リクエスト送信失敗または無応答）までとなります。

図 8-11　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 サーバの接続については，「コンフィグレーションガイド Vol.1　8　ログインセキュリティと RADIUS」を参照してください。

（5） 最大認証ユーザ数

最大認証ユーザ数の設定は，装置単位とポート単位の両方で指定することができます。最大認証ユーザ数はコンフィグレーションコマンド web-authentication max-user で最大 256 台まで設定できます。

装置単位とポート単位を同時に設定することは可能ですが，どちらかが最大数に達した場合，それ以降の新規ユーザの認証はできません。

また，運用中に認証済みユーザ数より最大認証ユーザ数を少なく変更した場合，認証済みのユーザは継続通信できますが，新規ユーザの認証はできません。

（6） 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　(6) 認証状態からのログアウト」を参照してください。

（7） 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，リンクダウンしないでポート移動した場合でも，認証済

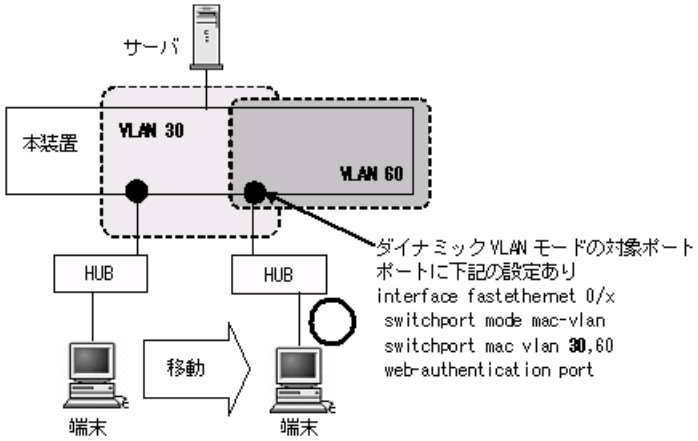
み状態のまま継続して通信可能にします。

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
- 移動前の認証後 VLAN が，移動後ポートのコンフィグレーションコマンド switchport mac vlan に設定されていること

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。

図 8-12　ダイナミック VLAN モード　ローミング概要図



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 8-13 認証動作（Web 認証専用 IP アドレス使用時）

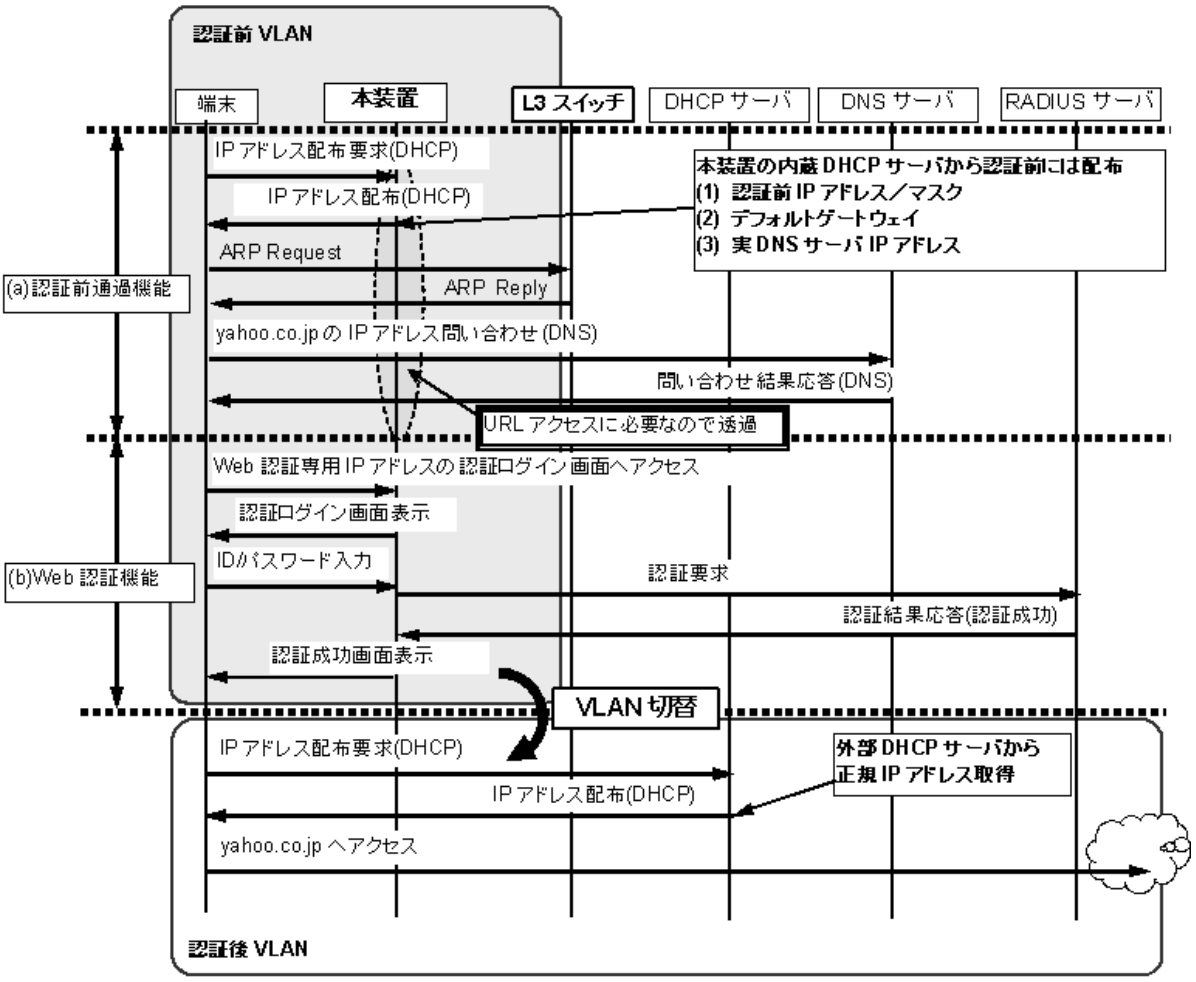
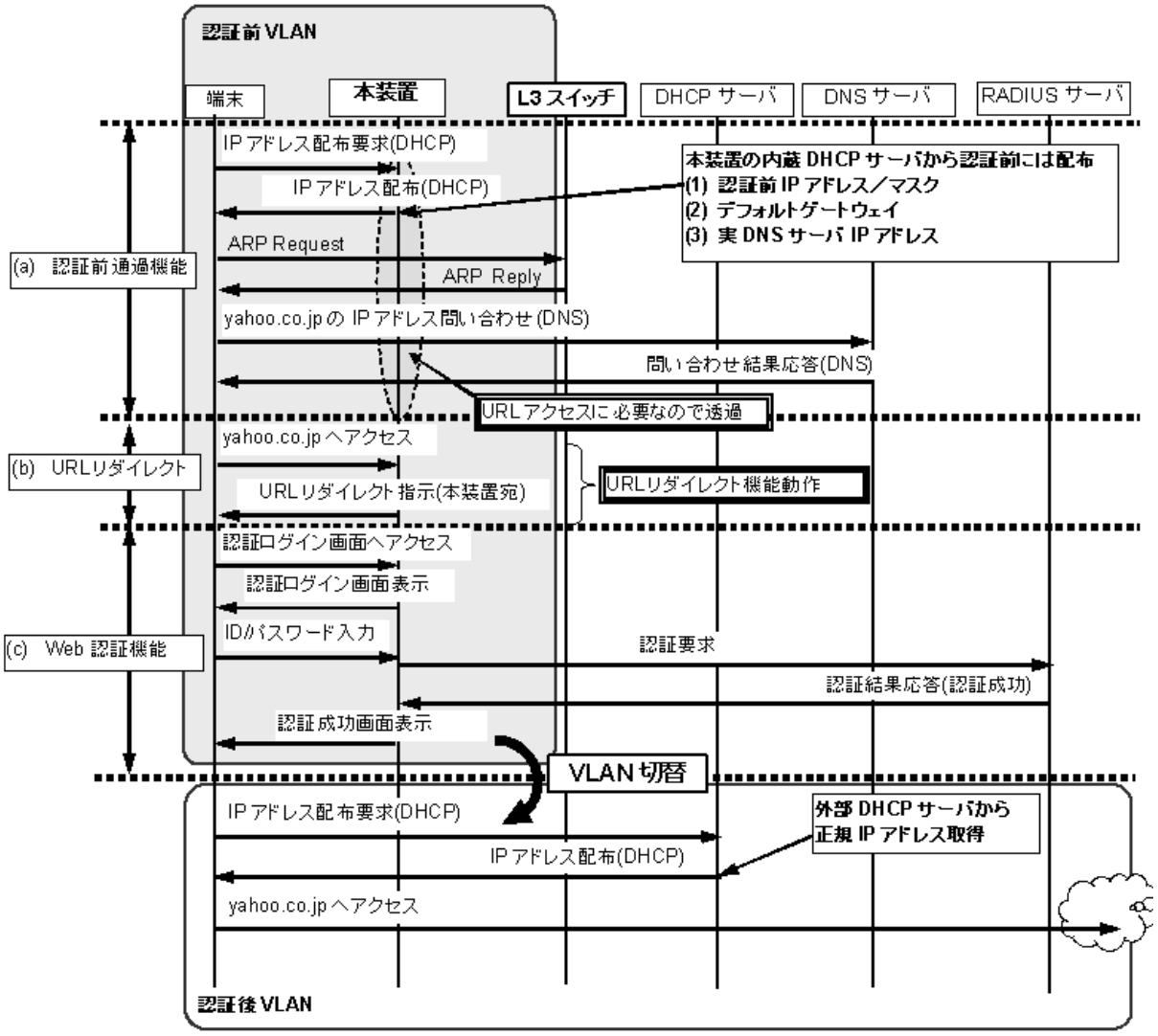


図 8-14　認証動作（URL リダイレクト機能使用時）



8.4 レガシーモード

認証前 VLAN の端末は，フレーム受信により MAC アドレステーブルにダイナミックエントリとして MAC アドレスと認証前 VLAN ID が登録され，認証前 VLAN 内の通信が可能です。レガシーモードで認証が成功すると，MAC VLAN に MAC アドレスと認証後 VLAN ID が登録され，認証後 VLAN 内の通信が可能になります。

ログイン操作は，Web 認証専用 IP アドレスまたは認証前 VLAN の IP アドレスでログインできます。どちらもローカル認証方式および RADIUS 認証方式で認証できます。

8.4.1 認証方式

本装置では，ローカル認証方式と RADIUS 認証方式をサポートしています。認証方式は，Web 認証全認証モード共通で使用します。

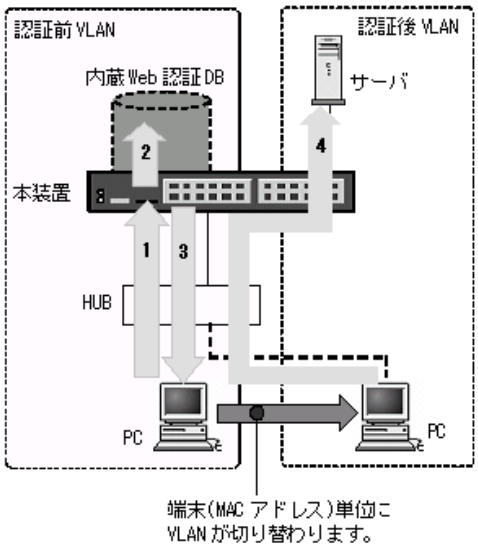
(1) ローカル認証

小規模ネットワークで安価に構築したい場合は，内蔵 Web 認証 DB を使用したローカル認証が適しています。

認証対象ユーザからのユーザ ID およびパスワードで Web 認証用内蔵 DB 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 8-15 レガシーモード概要図（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，認証成功画面を 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。

(a) 認証後 VLAN への収容条件

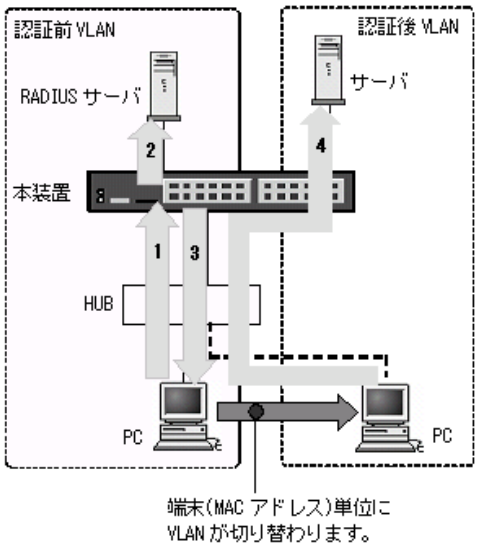
内蔵 Web 認証 DB の該当ユーザのエントリに登録されている VLAN ID が，レガシーモードの認証後 VLAN 設定 (コンフィグレーションコマンド web-authentication vlan) に含まれない場合は，認証失敗となります。

(2) RADIUS 認証

比較的規模の大きな構成での認証には，外部に設置した RADIUS サーバを使った認証が適しています。

RADIUS 認証方式の動作を次の図に示します。

図 8-16 レガシーモード概要図（RADIUS 認証の例）



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，認証成功画面を 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。

(a) 認証後 VLAN への収容条件

RADIUS サーバの当該ユーザのエントリに登録されている VLAN ID が，レガシーモードの認証後 VLAN 設定 (コンフィグレーションコマンド web-authentication vlan) に含まれない場合は，認証失敗となります。

8.4.2 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) 認証成功後の自動表示 URL 指定

ダイナミック VLAN モードと同様です。「8.3.2 認証機能 (3) 認証成功後の自動表示 URL 指定」を参照してください。

(3) 強制認証ポート指定

強制認証指定したポートに接続された端末の RADIUS 認証が，経路障害などで RADIUS サーバへリクエスト送信失敗または無応答となったときは，認証対象端末を認証許可状態にします。

強制認証を許可するポートにコンフィグレーションコマンド web-authentication force-authorized vlan を設定します。

なお，強制認証は下記の条件を満たしたときに許可となります。

表 8-5 強制認証許可条件

項目	条件
コンフィグレーション	下記のコンフィグレーションがすべて設定されていること • aaa authentication web-authentication default group radius • radius-server • web-authentication system-auth-control • vlan <VLAN ID list> mac-based ※1 • web-authentication vlan ※1 • web-authentication force-authorized vlan ※1※2 • switchport mac vlan ※1※2 • switchport mode mac-vlan ※2
アカウントログ	RADIUS サーバへの認証要求送信で，下記のアカウントログが採取された場合 No=21 NOTICE:LOGIN:(付加情報) Login failed ; Failed to connection to RADIUS server. 付加情報：MAC，USER，IP，PORT または CHGR，VLAN No=258 NOTICE:LOGIN:(付加情報) Login failed ; RADIUS request send error. 付加情報：MAC，USER，PORT または CHGR 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。

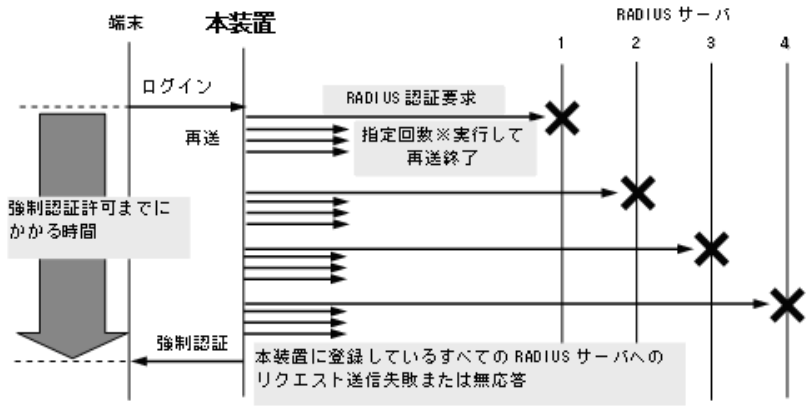
注※ 1
同じ VLAN ID を設定してください。

注※ 2
同じイーサネットポートに設定してください。

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「8.4.2 認証機能 (5) 認証状態からのログアウト」のいずれかの解除機能により認証状態が解除されます。

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（リクエスト送信失敗または無応答）までとなります。

図 8-17　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 サーバの接続については，「コンフィグレーションガイド Vol.1　8　ログインセキュリティと RADIUS」を参照してください。

（4） 最大認証ユーザ数

ダイナミック VLAN モードと同様です。「8.3.2　認証機能　（5）最大認証ユーザ数」を参照してください。

（5） 認証状態からのログアウト

レガシーモードでは，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
- MAC アドレステーブルエージング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
- 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

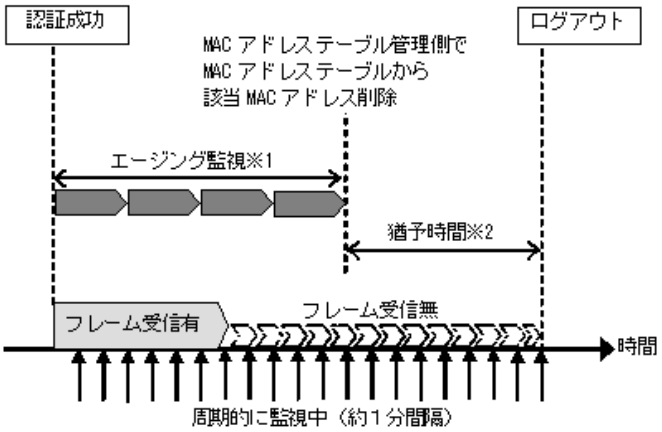
「MAC アドレステーブルエージング監視によるログアウト」以外のログアウト手段は，固定 VLAN モードと同様です。「8.2.2　認証機能　（6）認証状態からのログアウト」を参照してください。

（a） MAC アドレステーブルエージング監視によるログアウト

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，レガシーモードの認証後 VLAN ID で登録されている端末の 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 Web 認証の認証状態をログアウトし，認証前の VLAN ID に収容を変更します。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。

ただし，回線の瞬断などの影響で認証がログアウト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（ログアウトまでの猶予時間）で，該当する 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，認証状態をログアウトします。

図 8-18 MAC アドレステーブルエージング監視によるログアウト概要



※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）

なお，この機能はコンフィグレーションコマンド no web-authentication auto-logout で無効にできます。（エージングタイムアウト時でも強制的にログアウトしない設定が可能。）

（6） 認証済み端末のポート移動と認証ユーザ数の表示について

レガシーモードでは，ローミング用のコンフィグレーションはありません。認証済みの端末をポート移動した際は下記の動作となります。

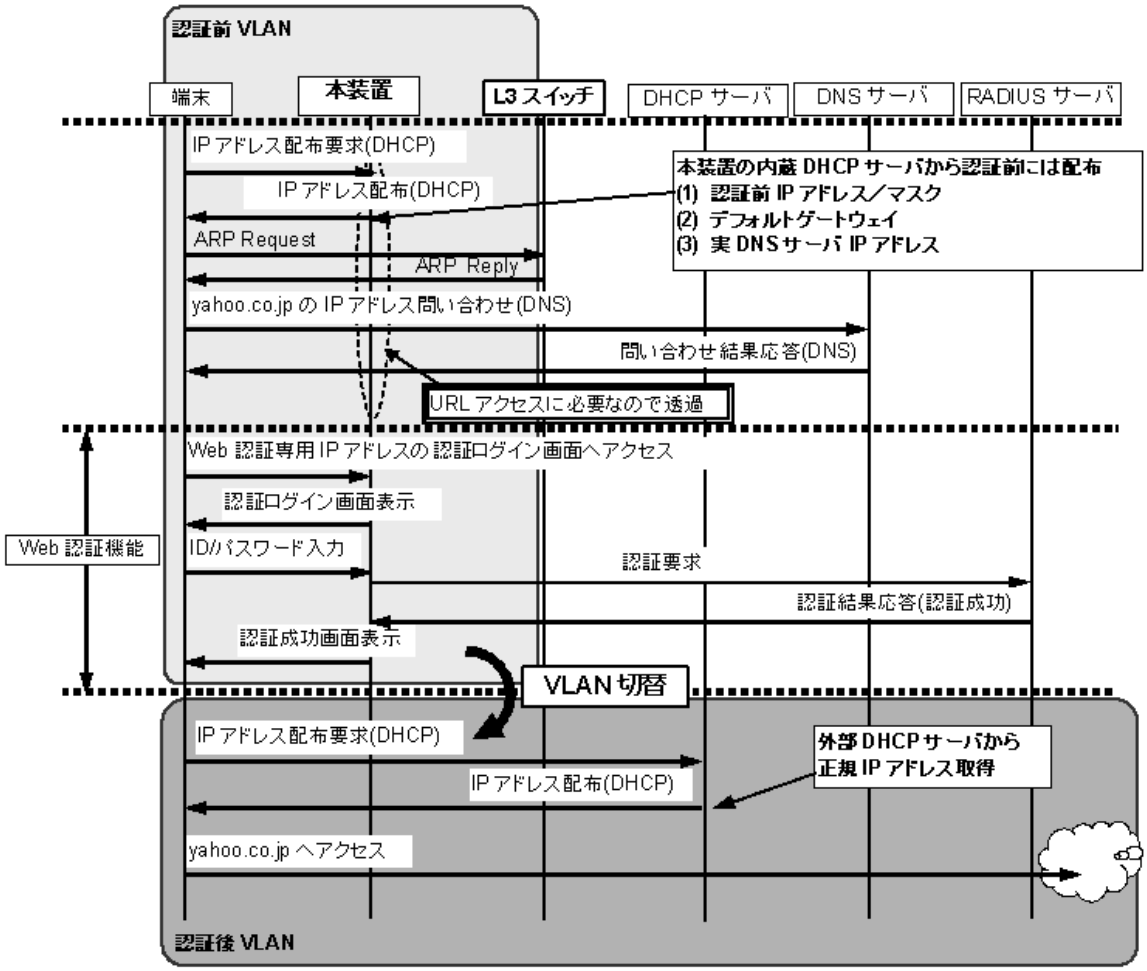
1. 一度認証が完了した端末は，認証した時点のポートで認証ユーザ数に計上されます。
2. レガシーモードで認証済みの端末をほかのポートに移動した場合，下記の条件すべてに該当する場合は継続して通信可能です。
   - 移動前および移動後が，レガシーモード対象ポート
   - 移動前の認証後 VLAN が，移動後ポートのコンフィグレーションコマンド switchport mac vlan に設定されていること

   移動後の端末は MAC アドレステーブルエージング監視で検出されるまでの間，通信可能となります。ただし，移動後ポートで DHCP snooping やフィルタなどを併用している場合は，その条件に依存します。
   上記以外の移動は認証をログアウトしますが，レガシーモードで認証済みの端末を認証対象外ポートに移動したときはログアウトしない場合があります。
3. 次の認証時間となった時点でポートの移動を検出します。
4. 移動後のポートがレガシーモードの対象ポートの場合，認証ユーザ数の計上は下記のとおりです。
   - 最大認証ユーザ数制限以内であれば，移動前ポートの認証ユーザ数減算と，移動後ポートでの認証登録が実施されます。
   - 最大認証ユーザ数制限以上となった場合，移動前ポートの認証ユーザ数減算と，認証ログアウトが実施されます。
5. 次の認証時間がくる前に MAC アドレステーブルエージング監視で，移動前ポートでの MAC アドレス消失が検出された場合，移動後ポートで新規端末として認証処理が実施されます。

8.4.3 認証動作

レガシーモードは以下のシーケンスで認証動作を行います。

図 8-19 認証動作（Web 認証専用 IP アドレス使用時）



8.5 アカウント機能

Web 認証の認証結果は，本装置に内蔵のアカウントログ機能で記録されます。RADIUS サーバのアカウント機能はサポートしておりません。

なお，本装置の内蔵アカウントログには，Web 認証の全認証モードの合計で最大 2100 行まで記録されます。2100 行を超えた場合，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 アカウントログ種別

アカウントログ種別	内容
LOGIN	ログイン操作に関する内容（成功・失敗）
LOGOUT	ログアウト操作に関する内容（理由等）
SYSTEM	Web 認証機能の動作に関する内容 （ローミング検出，強制認証許可も含む）

表 8-7 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

（凡例）
○：出力します
×：出力しません

注※ 1
固定 VLAN モード，ダイナミック VLAN モード：インタフェースポート番号を出力します。
レガシーモード：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 22 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. イベントごとのコンソール表示
   運用コマンド trace-monitor enable を実施済みの環境においても，アカウントログはイベント発生ごとにコンソールに表示しません。
2. 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。

3. syslog サーバへ出力
   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，装置全体のイベントトレース情報と合わせてアカウントログ情報を出力します。Web 認証の内蔵アカウントログ情報だけを syslog サーバへ出力または抑止指定することはできません。
4. 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 8-8　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 8-9　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
強制認証	固定 VLAN	snmp-server host	web-authentication
		web-authentication static-vlan force-authorized	action trap
	ダイナミック VLAN	snmp-server host	web-authentication
		web-authentication force-authorized vlan	action trap
	レガシー	snmp-server host	web-authentication
		web-authentication force-authorized vlan	action trap
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 force-authorized vlan	action trap
	レガシー	－（対象外のため，該当設定なし）	

8.6　事前準備

8.6.1　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。

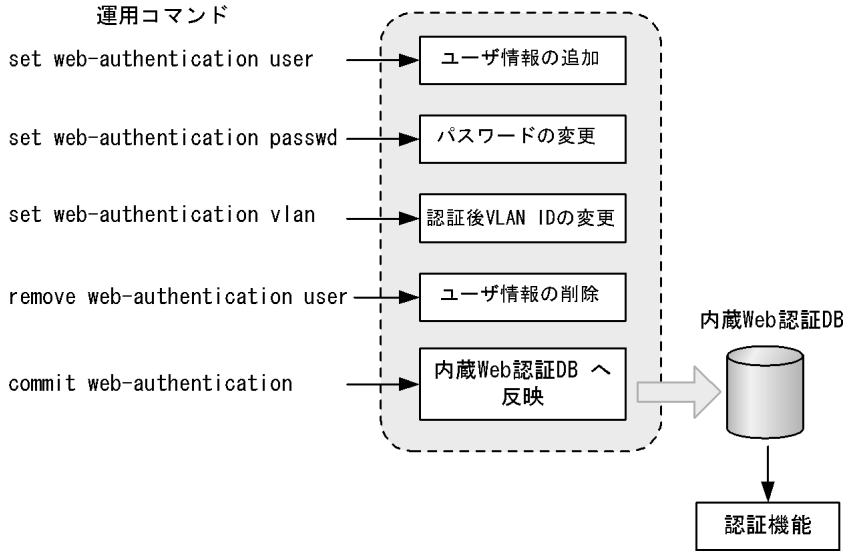
- 運用コマンド set web-authentication user で，ユーザ情報（認証対象端末のユーザ ID，パスワードおよび認証後 VLAN ID）を追加します。
- 登録済みのパスワードを変更する場合は，運用コマンド set web-authentication passwd で行います。
- 登録済みの認証後 VLAN ID を変更する場合は，運用コマンド set web-authentication vlan で行います。
- 登録済みのユーザ情報を削除する場合は，運用コマンド remove web-authentication user で行います。
- 編集したユーザ情報は，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 とパスワードは，文字数１～１６文字で次の文字が使用できます。

- ユーザ ID：０～９　Ａ～Ｚ　ａ～ ｚ
- パスワード：０～９　Ａ～Ｚ　ａ～ ｚ

図 8-20　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。

8.6.2　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
Service-Type	6	提供するサービスタイプ。 Framed(2) 固定。
User-Name	1	認証されるユーザ ID。
User-Password	2	ユーザパスワード。
NAS-IP-Address	4	認証を要求している，本装置の IP アドレス。IP 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 IP アドレスを使用します。
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，レガシーモード： 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)

表 8-11 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。
Reply-Message	18	未使用※ 1
Tunnel-Type	64	トンネル・タイプ。 VLAN(13) 固定。
Tunnel-Medium-Type	65	トンネルを作成する際のプロトコル。 IEEE802(6) 固定。
Tunnel-Private-Group-ID	81	VLAN を識別する文字列※ 2。 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）※ 3 （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

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※ 2

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 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※ 3

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，「12.2.3　ダイナミック VLAN モード収容 VLAN の VLAN 名称指定」を参照してください。

(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，レガシーモードの場合：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 8-12　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 ～ 32 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 ※
Tunnel-Type	Virtual VLAN（値 13）
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-Medium-Type	IEEE-802（値 6）
Tunnel-Private-Group-ID	ダイナミック VLAN モード，レガシーモードの場合 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

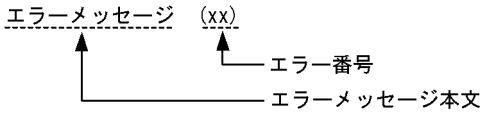
注※

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。

8.7 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 8-21 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 8-13 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 サーバに設定されている認証後 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 モードまたはレガシーモードの認証後 VLAN が，対象ポートの MAC VLAN ではありません。 • VLAN がインタフェースに設定されていません。
	34	RADIUS 認証方式で，認証済み端末から再ログインを行った際に 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。
	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。 • 同一ポートに IEEE802.1X/Web 認証 /MAC 認証のダイナミック VLAN モードとレガシーモードが混在しているため，レガシーモードで認証できません。 • 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。

エラーメッセージ内容	エラー番号	エラー発生理由
	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。
	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 モードまたはレガシーモードの認証後 VLAN が，対象ポートの MAC VLAN ではありません。 • VLAN がインタフェースに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。 • 同一ポートに IEEE802.1X/Web 認証 /MAC 認証のダイナミック VLAN モードとレガシーモードが混在しているため，レガシーモードで認証できません。 • 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。
	77	MAC アドレスを MAC アドレステーブルに登録する際，収容する VLAN が suspend 状態になっています。 または，VLAN がインタフェースに設定されていません。
	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。
	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。
The system error occurred. Please contact the system administrator.	64	RADIUS サーバへの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 256 件を超えた 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。
	74	MAC アドレスを MAC アドレステーブルに登録する際にエラーが発生しました。
	75	MAC アドレステーブルから MAC アドレスを削除する際にエラーが発生しました。
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：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。
- 102：IEEE802.1X，MAC 認証，MAC VLAN の MAC アドレス（VLAN のコンフィグレーションコマンド mac-address）の設定，およびシステム構成を確認してください。
- 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。

8.8　Web 認証の注意事項

8.8.1　認証モード共通の注意事項

（1） Web 認証のコンフィグレーションを設定する前に

固定 VLAN モード，ダイナミック VLAN モード，Web 認証専用 IP アドレスを使用する場合，システムファンクションリソースの設定が必要となります。システムファンクションリソース設定については，「コンフィグレーションガイド Vol.1　9.1.6　システムファンクションリソース配分の設定」を参照し，ほかの適切な機能も合わせて選択してください。

（2） 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

【固定 VLAN モード】【ダイナミック VLAN モード】

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。

（3） URL リダイレクト機能の使用について

【固定 VLAN モード】【ダイナミック VLAN モード】

（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 デフォルト状態）
- 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 デフォルト状態）

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） 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 redirect tcp-port は，URL リダイレクト機能で使用するための指定です。

（4） 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。

（5） 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。

（6） 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。

（7） 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。

（8） 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。

（9） ログアウト後の端末 IP アドレスについて

【ダイナミック VLAN モード】【レガシーモード】

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，および MAC アドレステーブルエージングタイムアウトでの強制ログアウト）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。）

（10） RADIUS サーバとの通信が切れた場合の注意事項

Web 認証で使用する RADIUS サーバとの通信が切れた場合，またはコンフィグレーションコマンド radius-server host で設定した RADIUS サーバが存在しない場合，ログイン要求ごとにタイムアウト（コンフィグレーションコマンド radius-server timeout で設定した時間）を待ち，RADIUS サーバへ再送（コンフィグレーションコマンド radius-server retransmit で設定した再送回数）を行うため，認証処理に時間が掛かります。

また，複数の RADIUS サーバが設定された場合でも，コンフィグレーションコマンド radius-server host の順にログインごとに毎回アクセスするため，先に設定された RADIUS サーバで障害などによって通信ができなくなると，認証処理に時間が掛かります。

このようなときは，Web 認証のログイン操作をいったん止め，コンフィグレーションコマンド radius-server host で正常な RADIUS サーバを設定し直した後に，ログイン操作を行ってください。

（11） 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。

- 本機能は RADIUS 認証方式だけサポートしています。

（12）ローミングと DHCP snooping 併用時の制限

【固定 VLAN モード】【ダイナミック VLAN モード】

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。

（13）ポート移動と最大認証ユーザ数について

【固定 VLAN モード】【ダイナミック VLAN モード】

最大認証ユーザ数チェックは，新規認証のユーザに対してだけ実施します。

従って，認証済みユーザのポート移動では，移動後のポートで最大認証ユーザ数チェックを行いません。

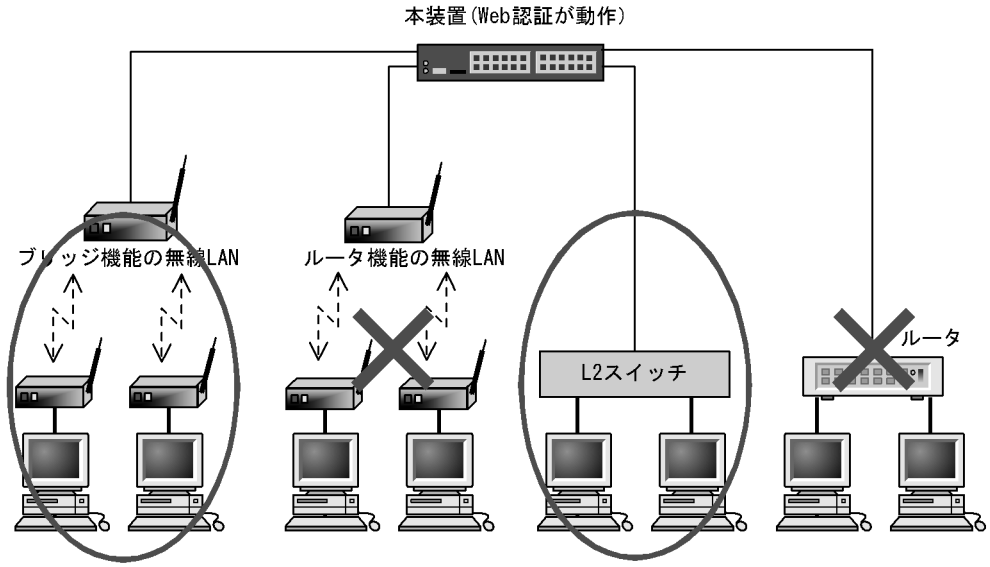
（14）本装置と認証対象の端末間に接続する装置について

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 8-22　本装置と端末間の接続



8.8.2　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 モードが動作可能なポートはイーサネットインタフェースだけです。

また，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） 本装置の内蔵 DHCP サーバの使用について

固定 VLAN モードでは，本装置の内蔵 DHCP サーバを使用できません。

外部 DHCP サーバをご用意ください。

8.8.3 ダイナミック VLAN ／レガシー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。

8.8.4 バージョンアップ（またはダウン）時の注意事項

（1） MAC ポートの認証モードの動作について

Ver.1.4 以降では，レガシーモードを使用できないケースがあります。MAC ポートに下記のコンフィグレーション設定がある場合，レガシーモードは使用できなくなり，かわってダイナミック VLAN モードとして動作します。

表 8-14 MAC ポートと認証モードのバージョンアップ別動作

MAC ポートのコンフィグレーション設定	対象バージョン	固定 VLAN	ダイナミック VLAN	レガシー
web-authentication port あり	Ver.1.1 ～ 1.3.x	○※1	未サポート	○
switchport mac dot1q vlan あり	Ver.1.4 ～	○※1	○	×※2

（凡例）
○：動作可
×：動作不可

注※ 1
Tagged フレームだけ対象

注※ 2
ダイナミック VLAN モードへ移行

8.9　Web 認証画面入れ替え機能

8.9.1　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，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。

運用コマンド set web-authentication html-files で指定したディレクトリ配下に，次に示す画面のファイルがあった場合，該当する Web 認証画面と置き換えます。また，次に示すファイル以外に gif ファイルなどの画像ファイルも同時に登録できます。

入れ替えることができる画面を次に示します。

［入れ替え可能な画面］
- 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

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。

登録できるファイル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 Web 認証画面は運用コマンド clear web-authentication html-files で削除できます。削除したあとは，デフォルトの Web 認証画面に戻ります。

また，「表 8-13　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，「8.10　Web 認証画面作成手引き」を参照してください。

8.9.2　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。登録した Web 認証画面ファイルを，本装置からアップロードすることはできません。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。

また，デフォルト画面も本装置からアップロードすることはできません。

なお，Ver.1.4 以降は運用コマンド 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。）

（3） バージョンアップについて

バージョンアップ後も登録済みの Web 認証画面ファイルを継続して使用できます。

ただし，Ver.1.2 ～ Ver.1.2.B の Web 認証画面入れ替え機能で登録済みの Web 認証画面では，Ver.1.3 以降でサポートした Web 認証自動 URL 表示機能を使用できません。詳細は，「8.10.4　Web 認証固有タグ（2）注意事項（c）バージョンアップ時の注意事項」を参照してください。

8.10 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，「8.10.1　ログイン画面（login.html）」，「8.10.2　ログアウト画面（logout.html）」を参照してください。

また，「表 8-13　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，「8.10.3　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。

8.10.1 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 8-15　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 type="text" name="uid" size="40" maxlength="32" autocomplete="OFF" />	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 type="password" name="pwd" size="40" maxlength="32" autocomplete="OFF" />	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 type="submit" value="Login" />	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。

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。

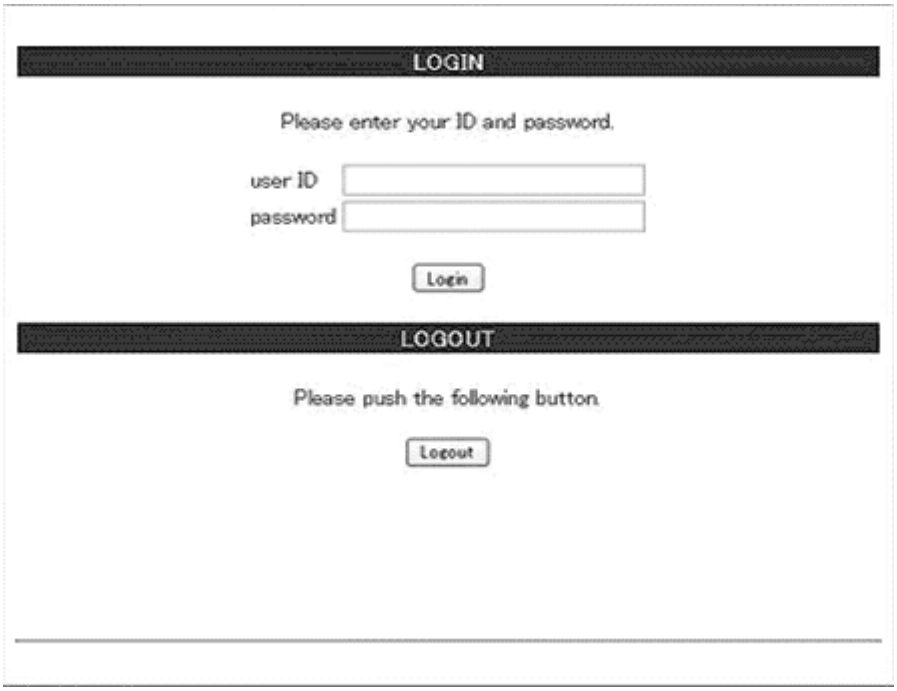
図 8-23 ログイン画面（login.html）のソース例

```
<?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>
<title> </title>
</head>
<body>
<!-- ===== Body ===== -->
<center>
<br />
<table width="100%">
<tr><td align="center" bgcolor="#2b1872">
<font color="#ffffff"><b>LOGIN</b></font>
</td></tr></table>
<br />
Please enter your ID and password.<br />
<br />

<form name="Login" method="post" action="/cgi-bin/Login.cgi">
<table><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 type="text" name="uid" size="40" maxlength="32" autocomplete="OFF" />
                                                        ユーザID指定のための記述
</td>
</tr><tr>
 <td>password</td>
 <td>

<input type="password" name="pwd" size="40" maxlength="32"
autocomplete="OFF" />
                                                        パスワード指定のための記述
</td></tr>
</table>
<br />
<input type="submit" value="Login" />
                                        Web認証にログイン要求を行うための記述
</form>
<br /><br /><br /><br /><br />
</center>
<!-- ===== Footer ===== -->
<hr>
</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。

図 8-24　ログイン画面の表示例



8.10.2　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 8-16　ログアウト画面に必要な設定

記述内容	意味
<form name="Logout" method="post" action="/cgi-bin/Logout.cgi"></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 type="submit" value="Logout" />	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。

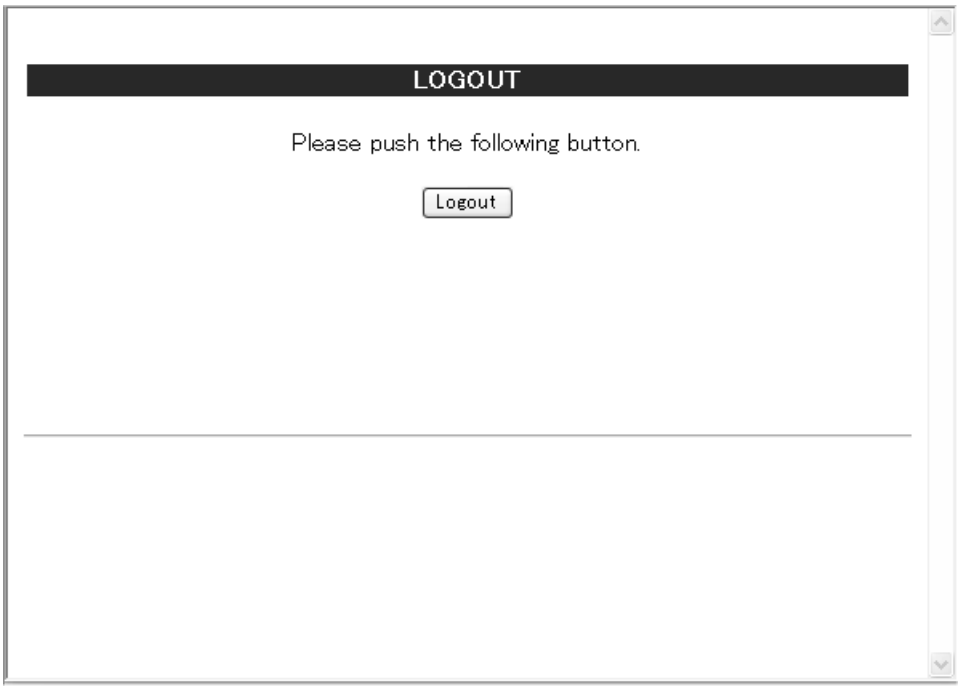
図 8-25 ログアウト画面（logout.html）のソース例

```
<?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>
<title> </title>
</head>
<body>
<!-- ===== Body ===== -->                    ログアウト操作をWeb認証に指示するための記述
<center>
<br />
<form name="Logout" method="post" action="/cgi-bin/Logout.cgi">
<table width="100%">
<tr><td align="center" bgcolor="#2b1872">
<font color="#ffffff"><b>LOGOUT</b></font>
</td></tr></table>
<br />
Please push the following button.<br />
<br />
<input type="submit" value="Logout" />
</form>
<br /><br /><br /><br /><br />
</center>
<!-- ===== Footer ===== -->                  Web認証にログアウト要求を行うための記述
<hr>
</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 8-26 ログアウト画面の表示例



8.10.3 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 8-17 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”のどちから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。

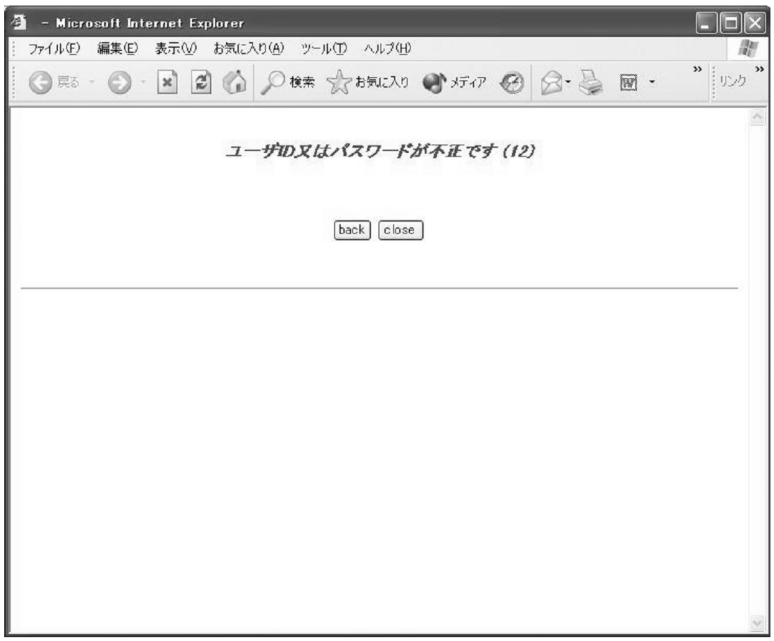
図 8-27　認証エラーメッセージファイル（webauth.msg）のソース例

```
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 8-28 ログイン失敗画面の表示例（パスワード長不正）



8.10.4 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 8-18 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 -->	"2007/08/02 19:56:01 UTC"	ログインが成功した時刻
<!-- Logout_Time -->	"2007/08/02 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

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，「8.10.5 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 8-19 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 -->	－	－	○	－	－	－

（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，「8.9.1 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. "-->"

（c） バージョンアップ時の注意事項

本装置の Ver.1.2 ～ 1.2.B の Web 認証画面入れ替え機能で登録した Web 認証画面では，Ver.1.3 以降でサ

ポートした Web 認証自動 URL 表示機能を使用できません。下記の手順で Web 認証画面を再度作成してください。

1. 保管してあるログイン成功画面ファイルを準備します。保管していない場合は，ログイン成功画面ファイルを作成します。
2. ログイン成功画面ファイルに，自動 URL 表示用の Web 認証固有タグ（"<!-- Redirect_URL -->"）と，ログイン成功後に表示する URL（コンフィグレーションコマンド web-authentication jump-url の設定内容）を記述します。
   また，Ver.1.4 以降は指定 URL へ移動するまでの時間を記述してください。時間はコンフィグレーションコマンド web-authentication jump-url のパラメータ delay に合わせてください。
3. 入れ替え実行時には，ログイン画面ファイルが必要ですので，保管してあるログイン画面ファイルを準備します。保管していない場合は，ログイン画面ファイルを作成します。
4. Web 認証画面入れ替え機能により，ログイン画面およびログイン成功画面ファイルを本装置に登録します。

なお，本装置から Web 認証画面ファイルをアップロードすることはできません。

8.10.5 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 8-29　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>
</head>
<body oncontextmenu=¥"return false;¥">
<!-- ===== Body ===== -->
<center>
Login success
<br /><br />
<Table Border="0">
<Tr>
<Td Align="left">
Login Time
</Td>
<Td Align="left">
 ---
</Td>
<Td Align="left">
<b><!-- Login_Time --></b>
</Td>
</Tr>
<Tr>
<Td Align="left">
Logout Time
</Td>
<Td Align="left">
 ---
</Td>
<Td Align="left">
<b><!-- Logout_Time --></b>
</Td>
</Tr>
</Table>
<br /><br />

<form>
<input type="button" value="close" onClick="window.close()" />
</form>
<br /><br />
</center>
<br /><br />
<!-- ===== Footer ===== -->
<hr>
</body>
</html>
```

ログイン時刻表示タグ

ログアウト時刻表示タグ

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" >

図 8-30　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 8-31　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 type="button" value="close" onClick="window.close()" />
</form>
<br /><br />
</center>
<!-- ===== Footer ===== -->
<hr>
</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 8-32　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 8-33　ログイン／ログアウト失敗画面のソース例（loginNG.html / 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>                                    エラーメッセージ表示タグ
<br>
<i style="color:red"><b><!-- Error_Message --></b></i>
<br /><br /><br /><br />
<form>
<input type="button" value="back" onClick="history.back()" />
<input type="button" value="close" onClick="window.close()" />
</form>
<br />
</center>
<!-- ===== Footer ===== -->
<hr>
</body>
</html>
```

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 8-34　ログイン／ログアウト失敗画面の表示例

8.11 内蔵 DHCP サーバ機能の解説

本装置の内蔵 DHCP サーバ機能は，DHCP クライアントに対して，IP アドレスやオプション情報などを動的に割り当てるための機能です。

8.11.1 サポート仕様

本装置の内蔵 DHCP サーバ機能のサポート仕様を次の表に示します。DHCP サーバとクライアント接続は，同一ネットワーク内の直結で行います。

表 8-20 内蔵 DHCP サーバ機能のサポート仕様

項目	仕様
接続構成	DHCP クライアントを直接収容 DHCP リレーエージェント経由では収容不可
BOOTP サーバ機能	未サポート
ダイナミック DNS 連携	未サポート
動的 IP アドレス配布機能	サポート
固定 IP アドレス配布機能	未サポート

8.11.2 クライアントへの配布情報

本装置でクライアントへ配布可能な情報の一覧を次の表に示します。配布可能な情報の中でオプション扱いの情報については，本装置で配布するオプションを指定した場合でも，クライアント側からオプション要求リストによって要求しない場合は配布データに含めません。

表 8-21 本装置でクライアントに配布する情報の一覧

項目	仕様
IP アドレス	クライアントが使用可能な IP アドレスを設定します。
IP アドレスリース時間	配布する IP アドレスのリース時間を設定します。本装置では default-lease-time/max-lease-time パラメータとクライアントからの要求によって値が決定されます。(Option No.51)
サブネットマスク	本オプションはコンフィグレーションで指定したネットワーク情報のサブネットマスク長が使用されます。(Option No.1)
ルータオプション	クライアントのサブネット上にあるルータの IP アドレスを指定します。この IP アドレスがクライアントのゲートウェイアドレスとして使用されます。(Option No.3)
DNS オプション	クライアントが利用できるドメインネームサーバのIPアドレスを指定します。(Option No：6)

8.11.3 IP アドレスの二重配布防止

本装置の DHCP サーバは，ICMP エコーによる IP アドレスの二重配布防止をサポートしていません。本装置が運用コマンド show ip dhcp conflict で表示する情報は，"decline" メッセージを受信した端末情報です。

8.11.4 DHCP サーバ使用時の注意事項

DHCP サーバ機能使用時の注意事項について説明します。

（1） 本装置のデフォルトリース時間

本装置のデフォルトリース時間は 10 秒で，これ以上短く設定することはできません。リース時間の設定範囲は 10 秒～ 365 日です。

また，配布可能な最大 IP アドレス数は 512 までです。

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	レ
aaa authentication web-authentication default group radius	Web 認証での RADIUS サーバの使用有無を設定します。	○	○	○
authentication arp-relay ※1	認証前状態の端末から送信される他機器宛て ARP フレームを，認証対象外のポートへ出力させます。	○	○	×
authentication ip access-group ※1	認証前状態の端末から送信される他機器宛ての IP フレームを，IPv4 アクセスリストを適用して設定されたフレームだけを認証対象外のポートへ出力させます。	○	○	×
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 force-authorized vlan	RADIUS 認証方式を使用時，経路障害などで RADIUS サーバへのリクエスト失敗時に，当該ポートで認証要求した認証対象端末を強制的に認証許可状態とし，認証後 VLAN を割り当てます。	－	○	○
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	認証成功画面表示後，自動的に表示する URL と URL 移動までの時間を設定します。	○	○	○
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。	○	－	－
web-authentication max-timer	最大接続時間を指定します。	○	○	○
web-authentication max-user	装置単位で認証可能な最大認証ユーザ数を設定します。	－	○	○
web-authentication max-user (interface)	当該ポートで認証可能な最大認証ユーザ数を設定します。	－	○	○
web-authentication port ※2	ポートに認証モードを設定します。	○	○	－

コマンド名	説明	認証モード		
		固	ダ	レ
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 tcp-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。	○	○	－
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 force-authorized	RADIUS 認証方式を使用時，経路障害などで RADIUS サーバへのリクエスト失敗時に，該当ポートに接続された認証対象端末を強制的に認証許可状態とします。	○	－	－
web-authentication static-vlan max-user	装置単位で認証可能な最大認証ユーザ数を設定します。	○	－	－
web-authentication static-vlan max-user (interface)	当該ポートで認証可能な最大認証ユーザ数を設定します。	○	－	－
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 vlan	ユーザ認証後，動的に切り替える VLAN ID を設定します。	－	－	○

（凡例）

固：固定 VLAN モード

ダ：ダイナミック VLAN モード

レ：レガシーモード

○：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※ 1

設定の詳細については，「12　レイヤ 2 認証の共通機能と共存使用」を参照してください。

注※ 2

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。

内蔵 DHCP サーバ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 9-2　内蔵 DHCP サーバコンフィグレーションコマンド一覧

コマンド名	説明	認証モード		
		固	ダ	レ
default-router	クライアントに配布するルータオプションを指定します。ルータオプションは，クライアントがサブネット上のルータ IP アドレス（デフォルトルータ）として使用可能な IP アドレスです。「クライアントに IP を配布する設定」のようにクライアントが使用するルータの IP アドレスを設定します。	－	○	○
dns-server	クライアントに配布するドメインネームサーバオプションを設定します。	－	○	○

コマンド名	説明	認証モード		
		固	ダ	レ
ip dhcp excluded-address	network コマンドで指定した IP アドレスプールのうち，配布対象から除外する IP アドレスの範囲を指定します。「クライアントに IP を配布する設定」のようにネットワークの IP アドレス範囲のうち，クライアントへの配布から除外する IP アドレスを設定します。	－	○	○
ip dhcp pool	DHCP アドレスプール情報を設定します。	－	○	○
lease	クライアントに配布する IP アドレスのデフォルトリース時間を指定します。「クライアントに IP を配布する設定」のようにクライアントが使用する IP アドレスのリース時間を設定します。	－	○	○
max-lease	クライアントがリース時間を指定して IP アドレスを要求した際に，許容する最大リース時間を指定します。	－	○	○
network	DHCP によって動的に IP アドレスを配布するネットワークのサブネットを指定します。実際に DHCP アドレスプールとして登録されるものは，サブネットのうち，IP アドレスホスト部のビットがすべて 0 およびすべて 1 のアドレスを除いたものです。「クライアントに IP を配布する設定」のように DHCP によって IP アドレスを配布するネットワークを設定します。	－	○	○
service dhcp	DHCP サーバを有効にするインタフェースを指定します。 本設定を行ったインタフェースでだけ DHCP パケットを受信します。 「クライアントに IP を配布する設定」のように DHCP クライアントが接続されている VLAN インタフェースを設定します。	－	○	○

（凡例）

固：固定 VLAN モード

ダ：ダイナミック VLAN モード

レ：レガシーモード

○：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

9.1.2 Web 認証のコンフィグレーションを設定する前に

Web 認証で認証モードを設定する場合は，コンフィグレーションを設定する前に，下記を設定してください。

［設定のポイント］

下記の認証モードまたは機能を使用する場合，設定の最初の段階でシステムファンクションリソースの割り当てをコンフィグレーションで設定する必要があります。

- Web 認証専用 IP アドレス（全認証モード共通）
- 固定 VLAN モード
- ダイナミック VLAN モード

システムファンクションリソースの割り当て設定は装置の再起動が必要です。システムファンクションリソースの割り当てについての詳細は「コンフィグレーションガイド Vol.1 9.1.6 システムファンクションリソース配分の設定」を参照してください。
本例ではフィルタと拡張認証機能を割り当てます。

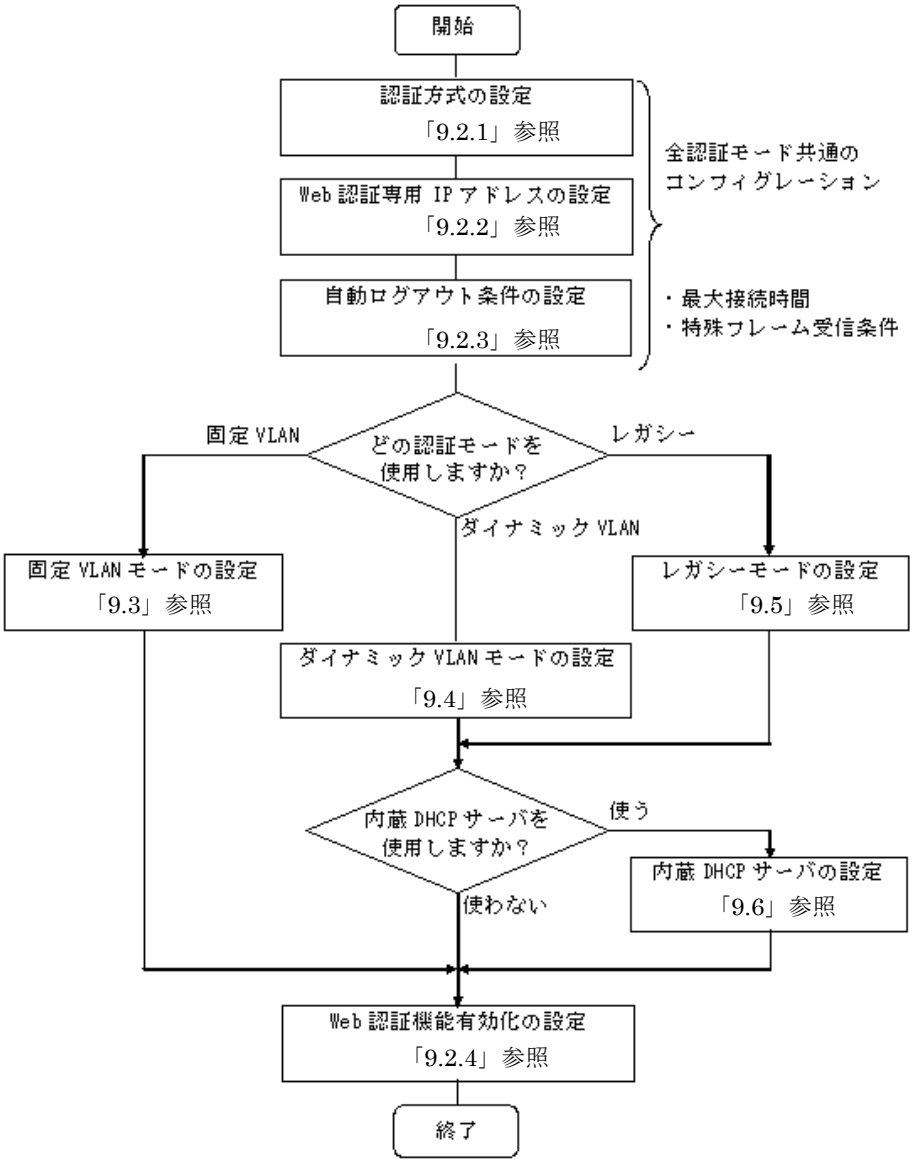
［コマンドによる設定］

1. **(config)# system function filter extended-authentication**
   ```
   Please execute the reload command after save,
   because this command becomes effective after reboot.
   ```
   システムリソースとしてフィルタと拡張認証機能を割り当てます。設定の保存と装置再起動を促すメッセージを表示します。
2. **(config)# end**
   # copy running-config startup-config
   ```
   Do you wish to copy from running-config to startup-config? (y/n): y
   ```
   @# reload
   ```
   Restart OK? (y/n): y
   ```
   コンフィグレーションの設定を保存すると，プロンプトに " @ " を表示しますので，装置を再起動してください。

9.1.3 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。
   - 認証方式の設定：「9.2.1　認証方式の設定」
   - 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」
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」

- レガシーモードの設定：「9.5　レガシーモードのコンフィグレーション」

3. 内蔵 DHCP サーバの設定
   ダイナミック VLAN モード，レガシーモードの場合は，本装置の内蔵 DHCP サーバを使用できます。
   - 内蔵 DHCP サーバの設定：「9.6　内蔵 DHCP サーバの設定」

4. 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。
   - 「9.2.4　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。

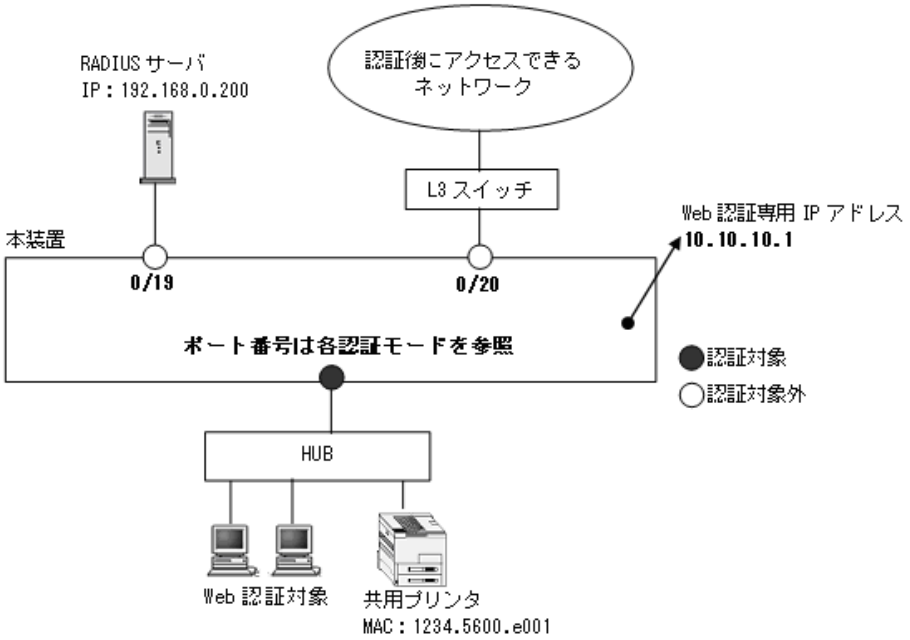
表 9-3　各認証モード有効条件

認証モード	コンフィグレーション設定
共通	• 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 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 • switchport mac vlan
レガシーモード	• vlan <VLAN ID list> mac-based • web-authentication vlan • switchport mode mac-vlan • switchport 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 0/19，0/20 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 認証方式の設定

［設定のポイント］

Web 認証共通で使用する認証方式として，RADIUS 認証方式と 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 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。

［コマンドによる設定］

1. **(config)# aaa authentication web-authentication default group radius**
   RADIUS 認証方式を設定します。

2. **(config)# radius-server host 192.168.0.200 key "L2auth"**
   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，timeout，retransmit は省略時の初期値が適用されます。

［注意事項］

1. 本設定省略時はローカル認証方式となります。ローカル認証方式では，内蔵 Web 認証 DB の登録が必要です。登録については「9.7.2 内蔵 Web 認証 DB の登録」を参照してください。
2. RADIUS サーバ情報は，本装置全体で最大４エントリまで設定できます。ログインセキュリティ機能やほかのレイヤ２認証機能と共用となることを考慮して，RADIUS サーバ情報を設定してく

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 ax1230s.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 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。

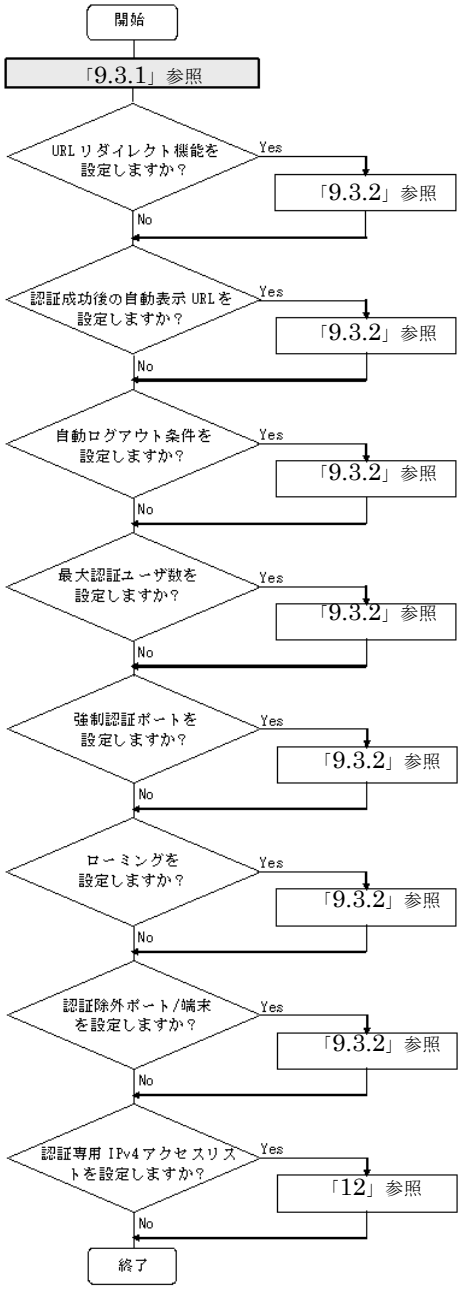
［注意事項］

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。

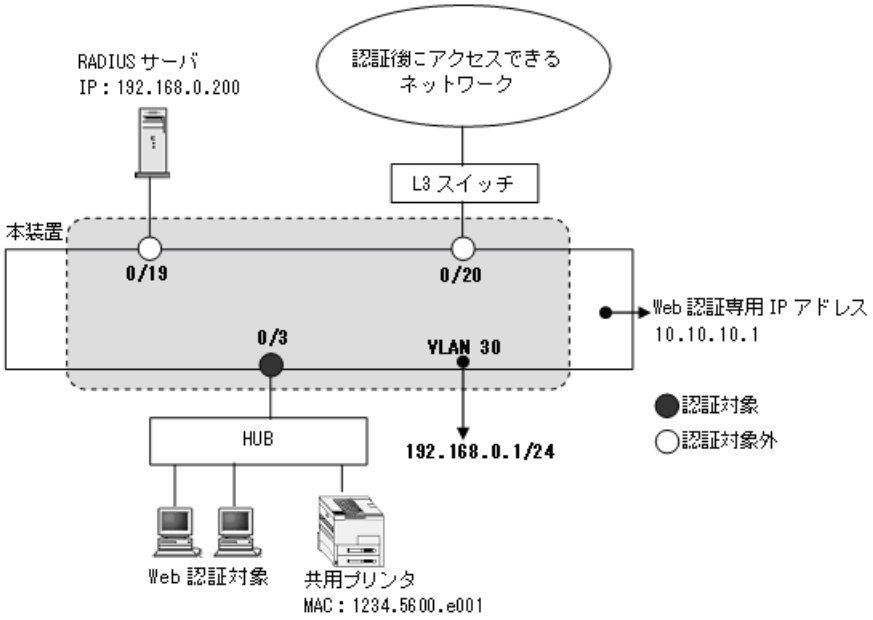
1. 認証ポートの設定：「9.3.1 認証ポートの設定」
2. URL リダイレクト機能の設定：「9.3.2 認証処理に関する設定（1）URL リダイレクト機能の設定」

3. 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（2）認証成功後の自動表示 URL の設定」
4. 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（3）自動ログアウト条件の設定」
5. 最大認証ユーザ数の設定：「9.3.2　認証処理に関する設定（4）最大認証ユーザ数の設定」
6. 強制認証ポートの設定：「9.3.2　認証処理に関する設定（5）強制認証ポートの設定」
7. ローミングの設定：「9.3.2　認証処理に関する設定（6）ローミング（認証済み端末のポート移動通信許可）の設定」
8. 認証除外の設定：「9.3.2　認証処理に関する設定（7）認証除外の設定」
9. 認証専用 IPv4 アクセスリストの設定：「12　レイヤ 2 認証の共通機能と共存使用」

固定 VLAN モードでは，本装置内蔵 DHCP サーバを使用できません。外部 DHCP サーバを使用しますが，認証前に外部 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「12　レイヤ 2 認証の共通機能と共存使用」を参照してください。

9.3.1　認証ポートの設定

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 fastethernet 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。

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 TCP = 80 と本設定の TCP ポート番号のパケットが対象となります。

[コマンドによる設定]

1. **(config)# web-authentication redirect tcp-port 8080**
TCP ポート番号 8080 を追加設定します。

[注意事項]
SSL ポート番号は未サポートです。

(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) 認証成功後の自動表示 URL の設定

[設定のポイント]

認証成功後に端末がアクセスする 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 5 秒）も変更できますが，固定 VLAN モードでは設定不要です。デフォルト時間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。

(3) 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，コマンドを設定しなくても本機能は有効となります。

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。

(4) 最大認証ユーザ数の設定

[設定のポイント]

固定 VLAN モードで認証可能な最大ユーザ数を設定します。

装置単位で設定する場合はグローバルコンフィグレーションモードで設定し，ポート単位で設定する場合は当該ポートのコンフィグレーションモードで設定します。

［コマンドによる設定］

1. **(config)# web-authentication static-vlan max-user 30**
   Web 認証で認証可能な最大ユーザ数を装置最大で 30 ユーザに設定します。

(5) 強制認証ポートの設定

［設定のポイント］

固定 VLAN モードの対象ポートで，強制認証を許可するポートに設定します。

［コマンドによる設定］

1. **(config)# interface fastethernet 0/3**
   (config-if)# web-authentication static-vlan force-authorized
   (config-if)# exit
   ポート 0/3 を強制認証ポートに設定します。

(6) 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］

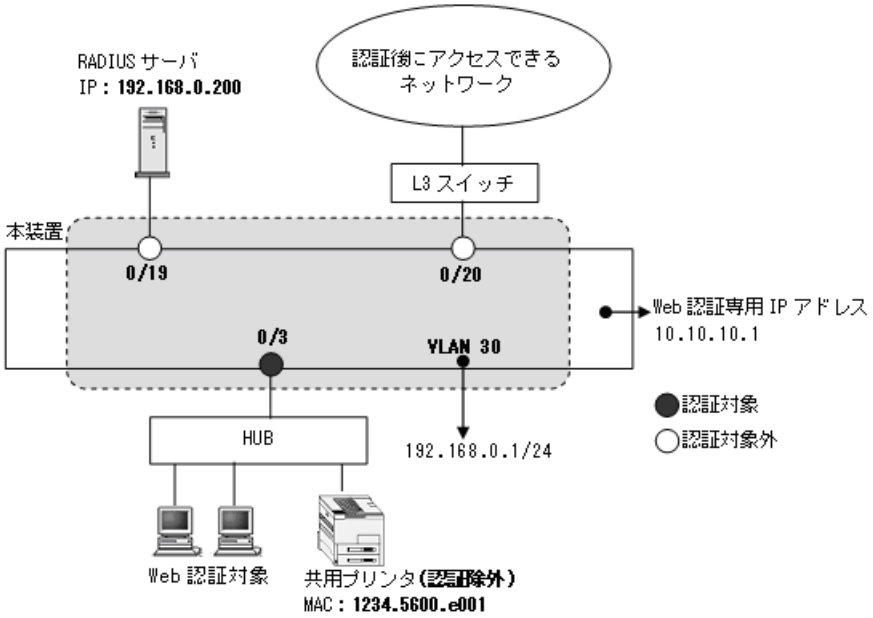
ローミングの動作可能な条件は下記のとおりです。

- 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

(7) 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 0/19，0/20，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 fastethernet 0/19-0/20**
   (config-if-range)# switchport mode access
   (config-if-range)# switchport access vlan 30
   (config-if-range)# exit
   VLAN ID 30 のポート 0/19 と 0/20 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。

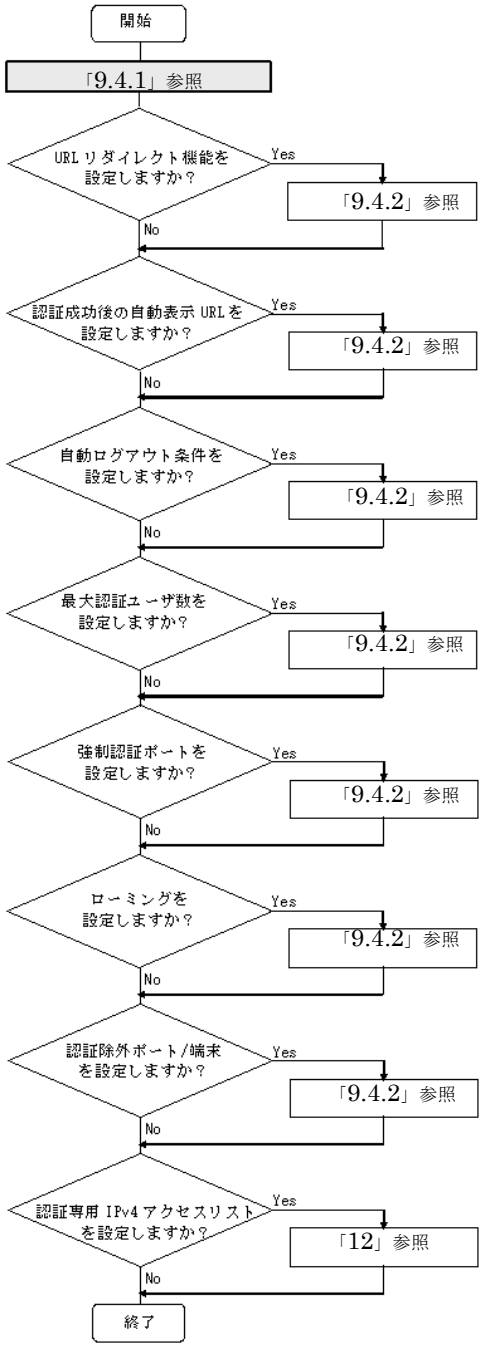
[コマンドによる設定]

1. **(config)# mac-address-table static 1234.5600.e0001 vlan 30 interface fastethernet 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。

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

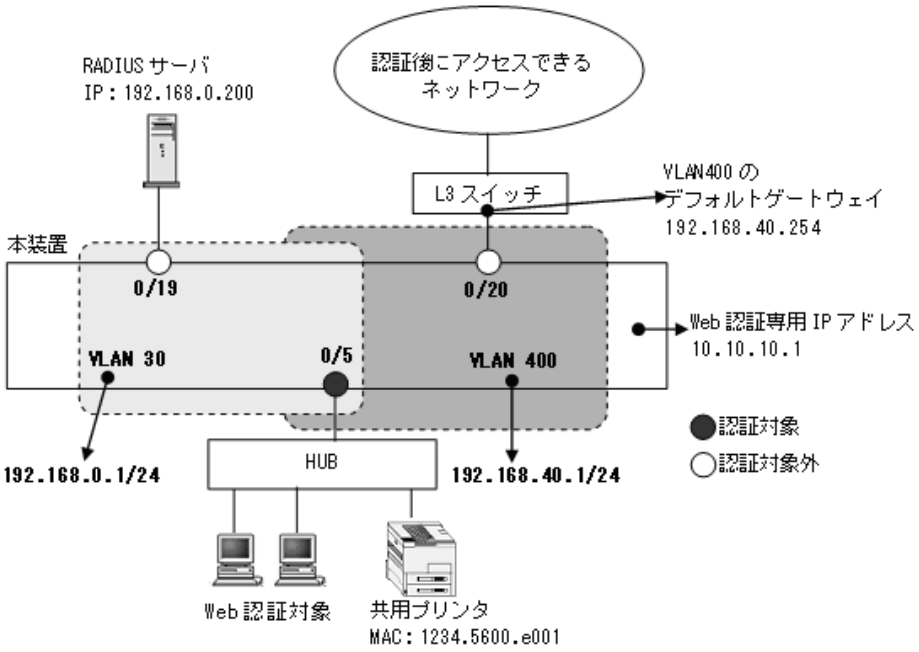


各設定の詳細は，下記を参照してください。

1. 認証ポートの設定：「9.4.1　認証ポートの設定」
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. 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（2）認証成功後の自動表示 URL と URL 移動までの時間の設定」
4. 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（3）自動ログアウト条件の設定」
5. 最大認証ユーザ数の設定：「9.4.2　認証処理に関する設定（4）最大認証ユーザ数の設定」
6. 強制認証ポートの設定：「9.4.2　認証処理に関する設定（5）強制認証ポートの設定」
7. ローミングの設定：「9.4.2　認証処理に関する設定（6）ローミング（認証済み端末のポート移動通信許可）の設定」
8. 認証除外の設定：「9.4.2　認証処理に関する設定（7）認証除外の設定」
9. 認証専用 IPv4 アクセスリストの設定：12　レイヤ 2 認証の共通機能と共存使用」

9.4.1　認証ポートの設定

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。

［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 fastethernet 0/5**
   (config-if)# switchport mode mac-vlan
   (config-if)# switchport mac vlan 400
   (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 と認証後 VLAN400 を指定します。

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。

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) 認証成功後の自動表示 URL と URL 移動までの時間の設定

[設定のポイント]

認証成功後に端末がアクセスする 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：10 秒）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。

（3） 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（3）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。

（4） 最大認証ユーザ数の設定

[設定のポイント]

ダイナミック VLAN モードで認証可能な最大ユーザ数を設定します。

装置単位で設定する場合はグローバルコンフィグレーションモードで設定し，ポート単位で設定する場合は当該ポートのコンフィグレーションモードで設定します。

[コマンドによる設定]

1. **(config)# web-authentication max-user 5**

   Web 認証で認証可能な最大ユーザ数を 5 ユーザに設定します。

（5） 強制認証ポートの設定

[設定のポイント]

ダイナミック VLAN モードの対象ポートで，強制認証を許可して割り当てる認証後 VLAN を設定します。

[コマンドによる設定]

1. **(config)# interface fastethernet 0/5**
   (config-if)# web-authentication force-authorized vlan 400
   (config-if)# exit

   ポート 0/5 で，強制認証を許可して割り当てる認証後 VLAN の VLAN ID を設定します。

（6） 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］

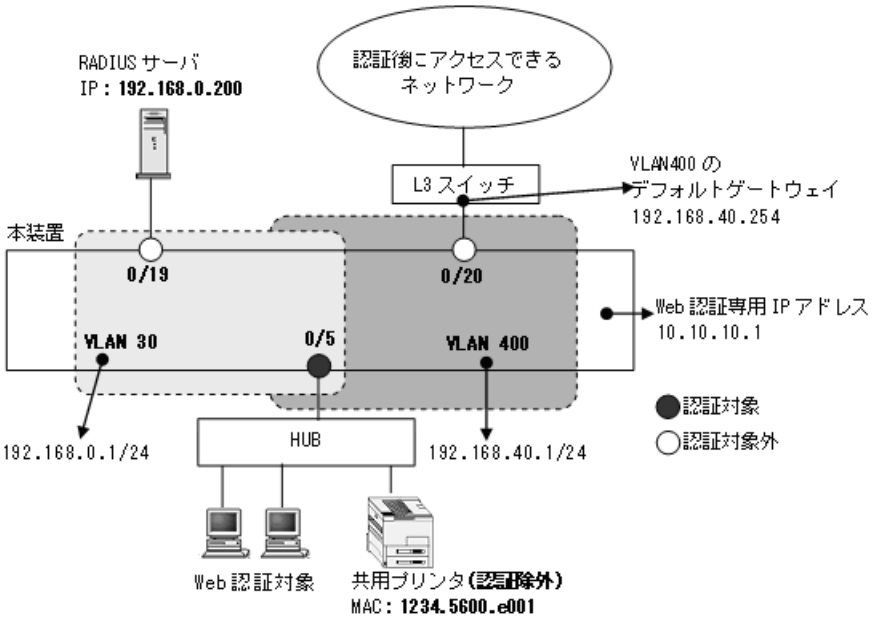
ローミングの動作可能な条件は下記のとおりです。

- 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
- 移動前の認証後 VLAN が，移動後ポートのコンフィグレーションコマンド switchport mac vlan に設定されていること

(7) 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 0/19，0/20，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 fastethernet 0/19**
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 30
   (config-if)# exit
   VLAN ID 30 のポート 0/19 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 fastethernet 0/20**
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 400
   (config-if)# exit
   MAC VLAN ID 400 のポート 0/20 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]

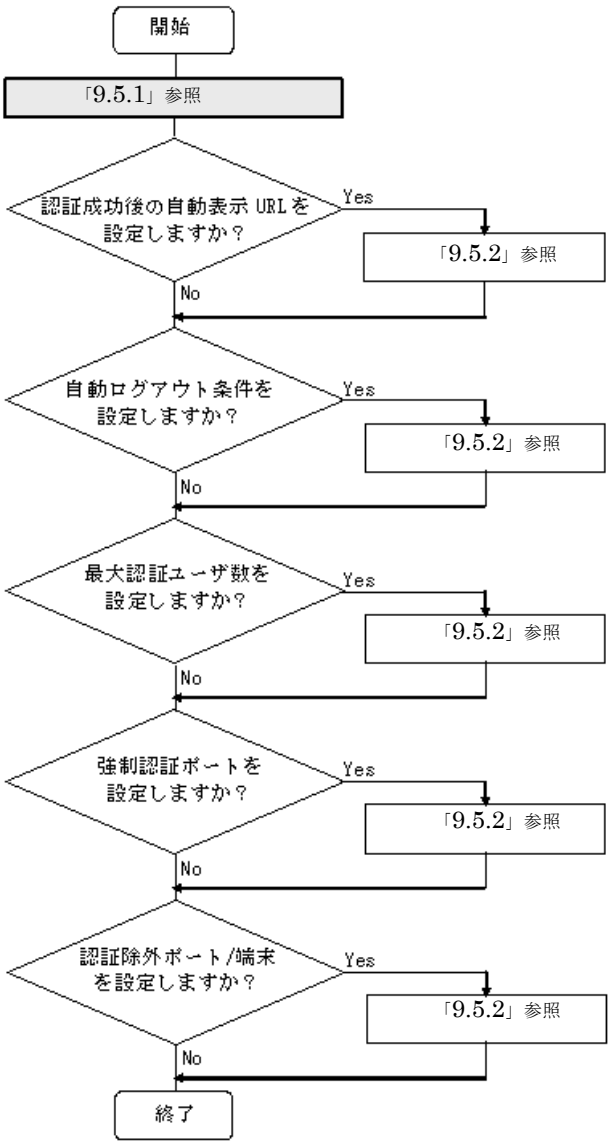
1. **(config)# vlan 400 mac-based**
   (config-vlan)# mac-address 1234.5600.e001
   (config-vlan)# exit
   認証を除外する MAC アドレス（図内の共用プリンタの MAC アドレス：1234.5600.e001）を，MAC VLAN ID 400 に設定します。

2. **(config)# mac-address-table static 1234.5600.e001 vlan 400 interface fastethernet 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。

9.5 レガシー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レガシーモードのコンフィグレーションを設定してください。

図 9-9 レガシーモードの設定手順

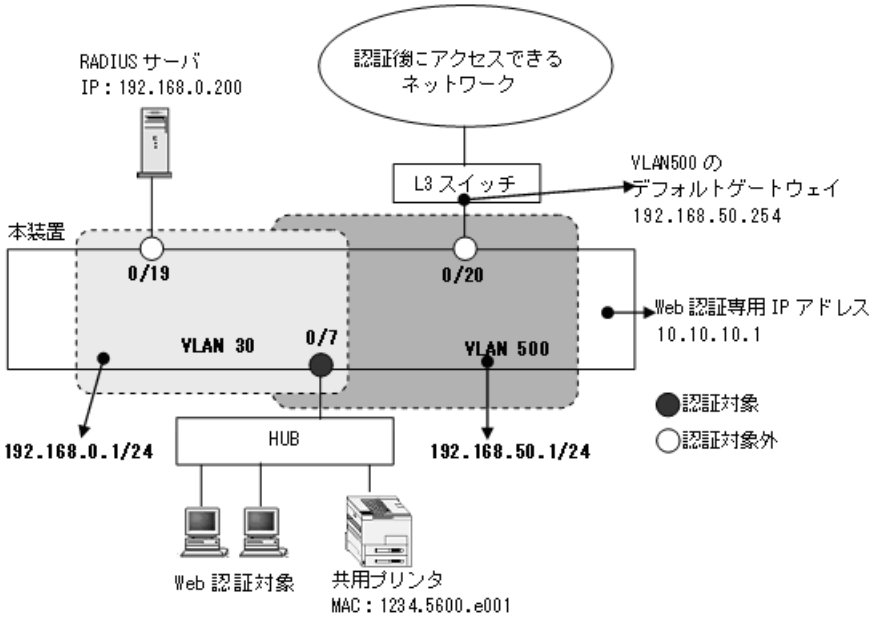


各設定の詳細は，下記を参照してください。

1. 認証ポートの設定：「9.5.1 認証ポートの設定」
2. 認証成功後の自動表示 URL の設定：「9.5.2 認証処理に関する設定（1）認証成功後の自動表示 URL と URL 移動までの時間の設定」
3. 自動ログアウト条件の設定：「9.5.2 認証処理に関する設定（2）自動ログアウト条件の設定」
4. 最大認証ユーザ数の設定：「9.5.2 認証処理に関する設定（3）最大認証ユーザ数の設定」
5. 強制認証ポートの設定：「9.5.2 認証処理に関する設定（4）強制認証ポートの設定」
6. 認証除外の設定：「9.5.2 認証処理に関する設定（5）認証除外の設定」

9.5.1　認証ポートの設定

図 9-10　レガシーモードの構成例



（1） 認証ポートと認証用 VLAN 情報の設定

［設定のポイント］

レガシーモードで使用するポートに，認証用 VLAN 情報を設定します。

［コマンドによる設定］

1. **(config)# vlan 500 mac-based**
   (config-vlan)# exit
   VLAN ID 500 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 fastethernet 0/7**
   (config-if)# switchport mode mac-vlan
   (config-if)# switchport mac vlan 500
   (config-if)# switchport mac native vlan 30
   (config-if)# exit
   認証を行う端末が接続されているポート 0/7 を MAC ポートとして設定し，認証前 VLAN ID 30 と認証後 VLAN ID 500 を指定します。

（2） 認証後 VLAN の設定

［設定のポイント］

レガシーモードで使用する，認証後 VLAN ID を設定します。レガシーモードで認証成功後，本コマンドで設定した VLAN に動的に切り替わります。

［コマンドによる設定］

1. **(config)# web-authentication vlan 500**
   レガシーモードの認証後 VLAN の VLAN ID 500 を設定します。

［注意事項］

本情報未設定のとき，レガシーモードで認証失敗となりますので，該当 VLAN ID を設定してください。

（3） 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 500**
   (config-if)# ip address 192.168.50.1 255.255.255.0
   (config-if)# exit
   Web 認証で使用する認証後 VLAN 500 に IP アドレスを設定します。

9.5.2 認証処理に関する設定

レガシーモードの認証処理に関する設定を説明します。

（1） 認証成功後の自動表示 URL と URL 移動までの時間の設定

ダイナミック VLAN モードと同様です。「9.4.2 認証処理に関する設定 （2）認証成功後の自動表示 URL と URL 移動までの時間の設定」を参照してください。

（2） 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） MAC アドレスエージングタイムアウト後の自動ログアウトの設定

Web 認証のレガシーモードが有効となったとき，コマンドを設定しなくても本機能は有効となります。

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） 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。

(3) 最大認証ユーザ数の設定

ダイナミック VLAN モードと同様です。「9.4.2 認証処理に関する設定（4）最大認証ユーザ数の設定」を参照してください。

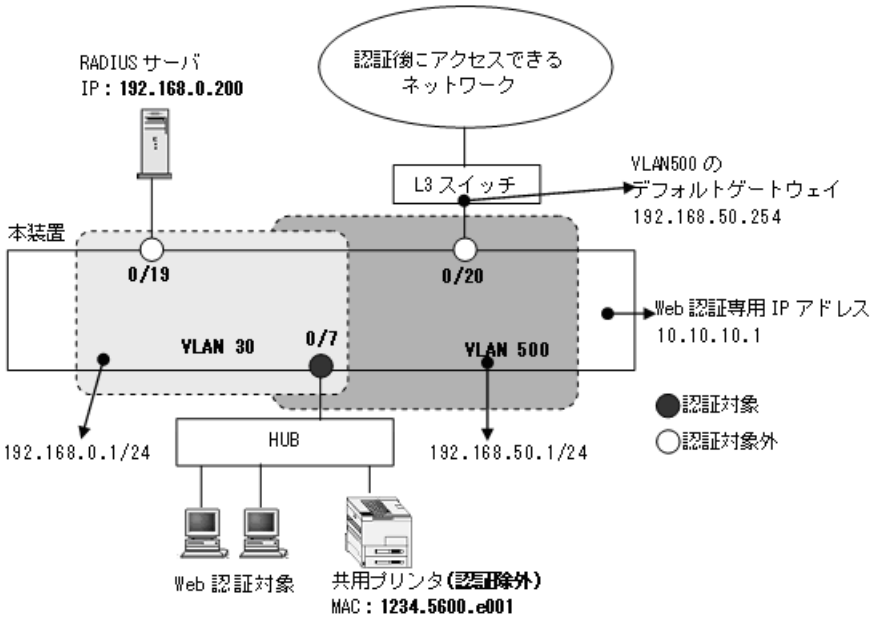
(4) 強制認証ポートの設定

ダイナミック VLAN モードと同様です。「9.4.2 認証処理に関する設定（5）強制認証ポートの設定」を参照してください。

(5) 認証除外の設定

レガシー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 0/19，0/20，および共用プリンタを認証除外として設定します。

図 9-11 レガシー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ます。

[コマンドによる設定]

1. **(config)# interface fastethernet 0/19**
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 30
   (config-if)# exit
   VLAN ID 30 のポート 0/19 をアクセスポートとして設定します。

2. **(config)# interface fastethernet 0/20**
   (config-if)# switchport mode access

```
(config-if)# switchport access vlan 500
(config-if)# exit
```

MAC VLAN ID 500 のポート 0/20 をアクセスポートとして設定します。

(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 に登録します。

[コマンドによる設定]

1.
```
(config)# vlan 500 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 500 に設定します。

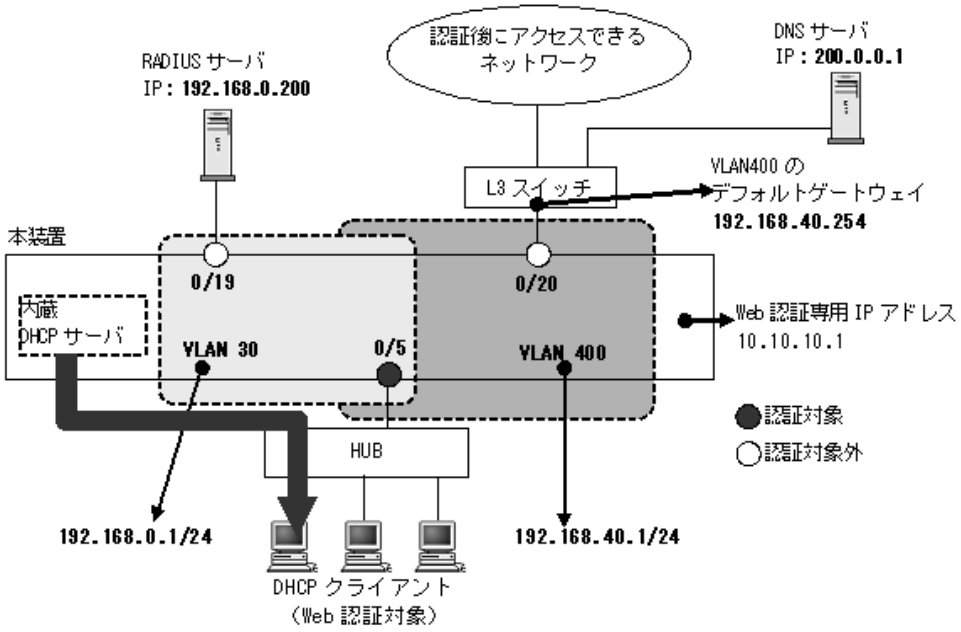
9.6 内蔵 DHCP サーバの設定

Web 認証で DHCP クライアント（認証対象端末）に IP アドレスを配布する設定です。本例は，「9.4 ダイナミック VLAN モードのコンフィグレーション」を基本構成として，内蔵 DHCP サーバの設定例を追加しています。

［設定のポイント］

DHCP クライアントへ割り当てをしたくない IP アドレスを割り当て除外アドレスに設定します。また，DHCP クライアントに対して IP アドレスを動的に配布するための DHCP アドレスプールを設定します。

図 9-12 内蔵 DHCP サーバ構成例（ダイナミック VLAN モードの例）



［コマンドによる設定］

1. **(config)# service dhcp vlan 30**
   認証前 VLAN30 で DHCP サーバを有効にします。

2. **(config)# ip dhcp excluded-address 192.168.0.1**
   (config)# ip dhcp excluded-address 192.168.0.200
   本装置の VLAN 30 の IP アドレスと RADIUS サーバの IP アドレスを除外設定します。

3. **(config)# ip dhcp pool POOL30**
   (dhcp-config)# network 192.168.0.0/24
   アドレスプール名 POOL30 を設定し，アドレスプールのネットワークアドレスを設定します。（認証前 VLAN30 と同じネットワークアドレスを設定してください。）

4. **(dhcp-config)# lease 0 0 1**
   アドレスのリース時間（1 分）を設定します。

5. **(dhcp-config)# default-router 192.168.0.1**
   認証前 VLAN30 の IP アドレスをデフォルトルータとして設定します。

6. **(dhcp-config)# dns-server 200.0.0.1**
   (dhcp-config)# exit
   DNS サーバの IP アドレスを設定します。

認証後 VLAN でも内蔵 DHCP サーバを使用する場合は，以下も設定します。

［コマンドによる設定］

1. **(config)# service dhcp vlan 400**
   認証後 VLAN400 で DHCP サーバを有効にします。

2. **(config)# ip dhcp excluded-address 192.168.40.1**
   (config)# ip dhcp excluded-address 192.168.40.254
   本装置の VLAN 400 の IP アドレスと L3 スイッチのデフォルトゲートウェイアドレスを除外設定します。

3. **(config)# ip dhcp pool POOL400**
   (dhcp-config)# network 192.168.40.0/24
   アドレスプール名 POOL400 を設定し，アドレスプールのネットワークアドレスを設定します。（認証後 VLAN400 と同じネットワークアドレスを設定してください。）

4. **(dhcp-config)# lease 1**
   アドレスのリース時間（1 日）を設定します。

5. **(dhcp-config)# default-router 192.168.40.1**
   認証後 VLAN400 の IP アドレスをデフォルトルータとして設定します。

6. **(dhcp-config)# dns-server 200.0.0.1**
   (dhcp-config)# exit
   DNS サーバの IP アドレスを設定します。

9.7 Web 認証のオペレーション

9.7.1 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 9-4 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	認証済みのアカウントログを表示します。
clear web-authentication logging	認証済みのアカウントログをクリアします。
set web-authentication html-files	指定された Web 認証画面ファイルを登録します。
clear web-authentication html-files	登録した Web 認証画面ファイルを削除します。
show web-authentication html-files	登録した Web 認証画面ファイルのファイル名，ファイルサイズと登録日時を表示します。
store web-authentication html-files	動作中の Web 認証画面ファイルを取り出し，RAMDISK の任意のディレクトリに格納します。

内蔵 DHCP サーバの運用コマンド一覧を次の表に示します。

表 9-5 内蔵 DHCP サーバの運用コマンド一覧

コマンド名	説明
show ip dhcp binding	DHCP サーバ上の結合情報を表示します。
clear ip dhcp binding	DHCP サーバのデータベースから結合情報を削除します。

コマンド名	説明
show ip dhcp conflict	DHCP サーバによって検出した衝突 IP アドレス情報を表示します。衝突 IP アドレスとは，DHCP サーバのプール IP アドレスでは空きとなっていますが，すでにネットワーク上の端末に割り当てられている IP アドレスを指します。
clear ip dhcp conflict	DHCP サーバから衝突 IP アドレス情報を取り除きます。
show ip dhcp server statistics	DHCP サーバの統計情報を表示します。
clear ip dhcp server statistics	DHCP サーバの統計情報をリセットします。

9.7.2 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，レガシーモードの場合：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，レガシーモードの場合：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.
#
```

9.7.3 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.
#
```

9.7.4 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 9-13 Web 認証の設定状態表示

```
# show web-authentication

Date 2008/06/16 16:53:33 UTC
<<<Web-Authentication mode status>>>
  Dynamic-VLAN     : Enable
  Static-VLAN      : Enable

<<<System configuration>>>
 * Authentication parameter
  Authentic-mode   : Dynamic-VLAN
  Authentic-method : RADIUS
  ip address       : 10.10.10.10
  web-port         : HTTP : 80(Fixed)  HTTPS : 443(Fixed)
  max-user         : 256
  roaming          : Disable
  html-files       : Default
  web-authentication vlan : 4

 * Logout parameter
  max-timer        : 60(min)
  auto-logout      : Enable
  logout ping      : tos-windows:   1  ttl:   1
  logout polling   : -

 * Redirect parameter
  redirect         : Enable
  redirect-mode    : HTTPS
  tcp-port         : 80(Fixed)
  jump-url         : Disable

 * Logging status
  [Radius account] : -
  [Syslog send]    : Disable
  [Traps]          : All

 * Internal DHCP sever status
  service dhcp vlan: 4094

<Port configuration>
  Port Count       : 3
  Function per port:
    Port  max-user  force-auth    arp-relay  ip access-group
  L 0/1        256  Disable       -          -
  L 0/3        256  Disable       -          -
    0/5        256  Disable       Disable    Disable
  VLANs per port   :
    Port  VLAN ID
    0/1   4
    0/3   4
    0/5   4000

<<<System configuration>>>
 * Authentication parameter
  Authentic-mode   : Static-VLAN
  Authentic-method : RADIUS
   ip address       : 10.10.10.10
  web-port         : HTTP : 80(Fixed)  HTTPS : 443(Fixed)
  max-user         : 1024
  roaming          : Disable
  html-files       : Default
  web-authentication vlan : -

 * 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-mode     : HTTPS
  tcp-port          : 80(Fixed)
  jump-url          : Disable

 * Logging status
  [Radius account] : -
  [Syslog send]     : Disable
  [Traps]           : All

 * Internal DHCP sever status
  service dhcp vlan: -

<Port configuration>
  Port Count        : 5
  Function per port:
    Port  max-user  force-auth    arp-relay  ip access-group
    0/9       1024  Enable        Enable     Before-Auth
    0/10      1024  Enable        Enable     Before-Auth
    0/11      1024  Enable        Enable     Before-Auth
    0/12      1024  Enable        Enable     Before-Auth
    0/13      1024  Enable        Enable     Before-Auth
  VLANs per port   :
    Port  VLAN ID
    0/9   40
    0/10  40
    0/11   40
    0/12  40
    0/13  40

#
```

9.7.5 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 9-14 Web 認証の表示

```
# show web-authentication statistics

Date 2007/03/11 13:53:34 UTC
Web-authentication Information:
  Authentication Request Total :         16
  Authentication Current Count :          1
  Authentication Error Total   :         14

RADIUS Web-Authentication Information:
[RADIUS frames]
  TxTotal   :        14  TxAccReq  :        14  TxError   :         0
  RxTotal   :        14  RxAccAccpt:        14  RxAccRejct:         0
                         RxAccChllg:         0  RxInvalid :         0

#
```

9.7.6 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 9-15 Web 認証の認証状態表示

```
# show web-authentication login

Date 2008/06/16 16:53:46 UTC
 Dynamic VLAN mode total login counts(Login/Max):   2 / 256
  Port roaming : Disable
   No F User name                      Port VLAN Login time          Limit
L   1   web0004                        0/2     4 2008/06/16 16:51:48 00:58:02
    2   web4000                        0/5  4000 2008/06/16 16:53:20 00:59:34

 Static VLAN mode total login counts(Login/Max):    1 / 1024
  Port roaming : Disable
   No F User name                      Port VLAN Login time          Limit
    1   web0040                        0/16   40 2008/06/16 16:52:03 00:58:17

#
```

（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 9-16 ポート指定時の情報表示

```
# show web-authentication login select-option port 0/1-16

Date 2008/06/17 13:02:27 UTC
 Dynamic VLAN mode total login counts(Login/Max):   2 / 256
  Port roaming : Disable
   No F User name                       Port VLAN Login time          Limit
L   1   web0004                         0/2     4 2008/06/17 13:01:23 00:58:55
    2   web4000                        0/5  4000 2008/06/17 13:01:59 00:59:31

 Static VLAN mode total login counts(Login/Max):    1 / 1024
  Port roaming : Disable
   No F User name                      Port VLAN Login time          Limit
    1   web0040                        0/16   40 2008/06/17 13:01:52 00:59:24

#
```

（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 9-17 認証済みユーザ数だけの表示

```
# show web-authentication login summary port

Date 2008/06/16 16:53:59 UTC
 Dynamic VLAN mode total login counts(Login/Max):   2 / 256
  Port roaming : Disable
   No  Port  Login /  Max
 L  1  0/2       1 /  256
    2  0/5       1 /  256

 Static VLAN mode total login counts(Login/Max):    1 / 1024
  Port roaming : Disable
   No  Port  Login /  Max
    1  0/16      1 / 1024

#
```

9.7.7 Web 認証画面ファイルの登録

Web 認証画面ファイル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。
2. 本装置へログインし，RAMDISK に Web 認証画面ファイルを格納するディレクトリを作成します。
3. Web 認証画面ファイルを 2. で作成したディレクトリ配下に，ファイル転送または MC 経由で格納します。
4. 運用コマンド set web-authentication html-files で Web 認証画面を登録します。

図 9-18 Web 認証画面ファイルの登録

```
# mkdir ramdisk docs                                    …1

# set web-authentication html-files ramdisk docs
Do you wish to install new html-files ? (y/n):y
executing...
Install complete.
#
```

1. RAMDISK にディレクトリ docs を作成し，配下に，登録するファイルを置きます。

9.7.8 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 9-19 登録した Web 認証画面ファイルの情報表示

```
# show web-authentication html-files

Date 2007/08/06 09:36:41 UTC

    Total Size :          56,851
    File Date               Size Name
    2007/08/06 09:36       2,642 login.htmls      …1
    default now            1,160 loginOK.html     …2
    default now              600 loginNG.html
    default now              897 logout.html
    default now              547 logoutOK.html
    default now              600 logoutNG.html
    default now              502 webauth.msg
    default now                0 favicon.ico
    2007/08/06 09:36       9,903 the other files

#
```

1. 登録した Web 認証画面ファイルの時間を表示します。
2. デフォルト状態の場合，" default now" を表示します。

9.7.9 登録した Web 認証画面ファイルの削除

運用コマンド set web-authentication html-files で登録した Web 認証画面ファイルを，運用コマンド clear web-authentication html-files で削除します。

図 9-20 Web 認証画面ファイルの削除

```
# clear web-authentication html-files
Do you wish to clear registered html-files and initialize? (y/n):y
Clear complete.

#
```

9.7.10 動作中の Web 認証画面ファイルの取り出し

動作中の Web 認証画面ファイルを，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 Web 認証画面ファイルの取り出し

```
# store web-authentication html-files ramdisk "web-file"
Do you wish to store html-files? (y/n): y
executing...
Store complete.

#
```

9.7.11 DHCP サーバの確認

（1）割り当て可能な IP アドレス数の確認

クライアントに割り当て可能な IP アドレスの個数は，運用コマンド show ip dhcp server statistics の実行結果「address pools」で表示します。この数がクライアントに割り当てたい数よりも多いことを確認してください。

図 9-22 show ip dhcp server statistics の実行結果

```
# show ip dhcp server statistics

Date 2007/03/07 05:24:12 UTC
   < DHCP Server use statistics >
     address pools          : 333
     automatic bindings     : 4
     expired bindings       : 28
     over pools request     : 0
     discard packets        : 0
   < Receive Packets >
     DHCPDISCOVER           : 35
     DHCPREQUEST            : 5974
     DHCPDECLINE            : 0
     DHCPRELEASE            : 0
   < Send Packets >
     DHCPOFFER              : 35
     DHCPACK                : 5937
     DHCPNAK                : 34

#
```

（2） 配布した IP アドレスの確認

実際に DHCP クライアントへ割り当てられた IP アドレスについては，運用コマンド show ip dhcp binding で確認してください。リースを満了していない IP アドレスを表示します。

図 9-23　show ip dhcp binding の実行結果

```
> show ip dhcp binding

Date 2007/03/07 05:22:26 UTC
 No  IP Address        MAC Address      Lease Expiration       Type
 1   192.168.20.3      0080.9880.1ad6   2007/03/07 05:22:27    Automatic
 2   192.168.20.2      0013.20a5.24ab   2007/03/07 05:22:35    Automatic

>
```

9.7.12　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

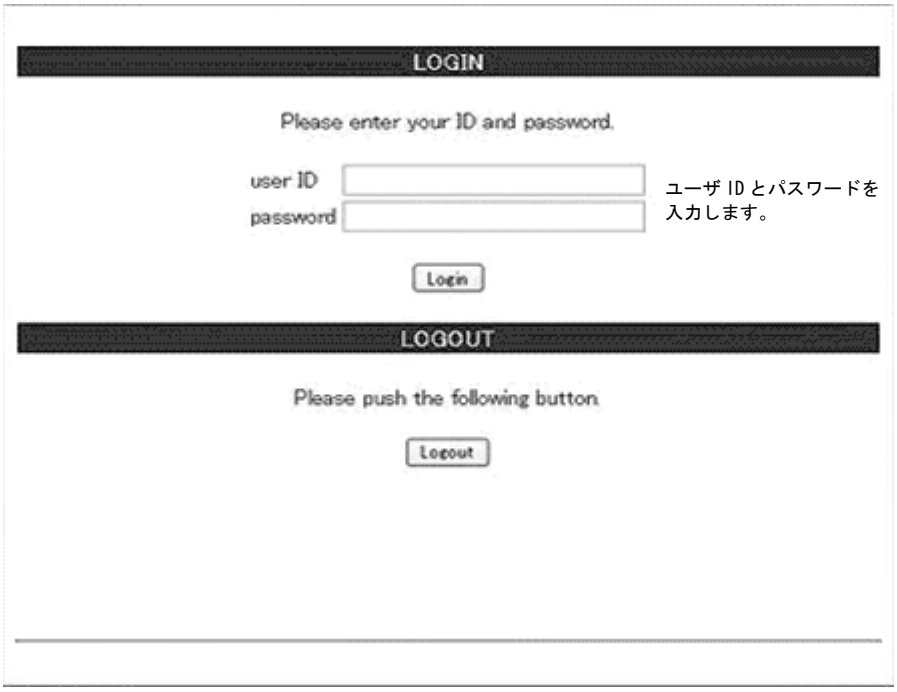
Web 認証専用 IP アドレスを設定していない場合は，Web 認証専用の URL（http:// 認証前 VLAN のインタフェース IP アドレス /login.html）にアクセスします。

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 IP 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，「9.7.12　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 9-24 ログイン画面



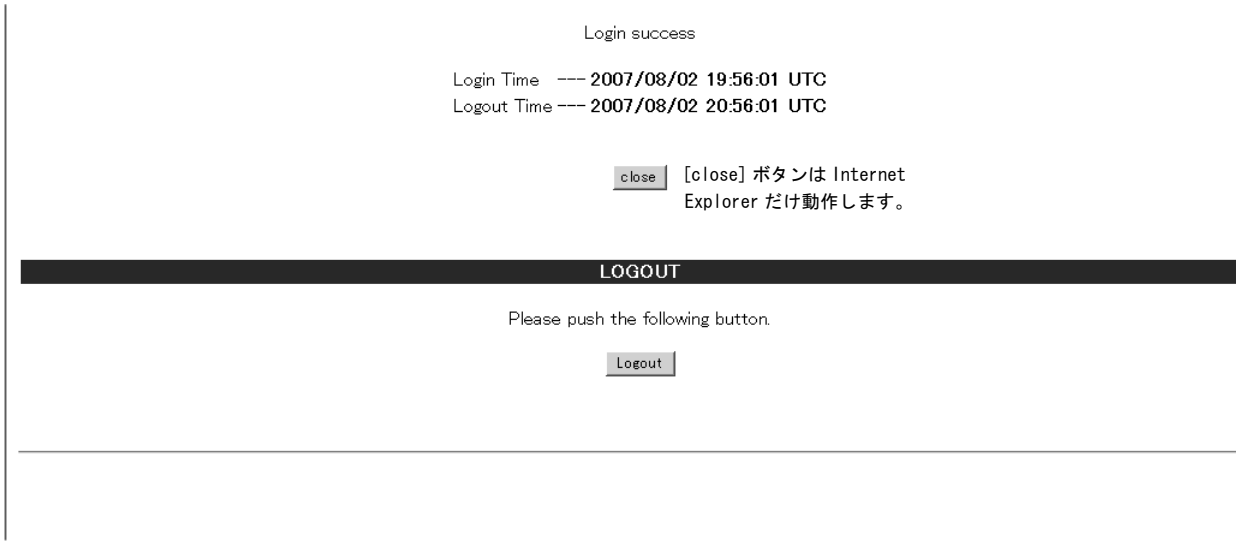
(3) ログイン画面に入力されたユーザ ID，パスワードの認証

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) 認証成功時の認証成功画面表示

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 9-25　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，「9.7.12　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，「8.7　認証エラーメッセージ」に示します。

図 9-26 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，自動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（レガシーモードの場合は，MAC アドレステーブルエージング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 9-27　ログアウト画面

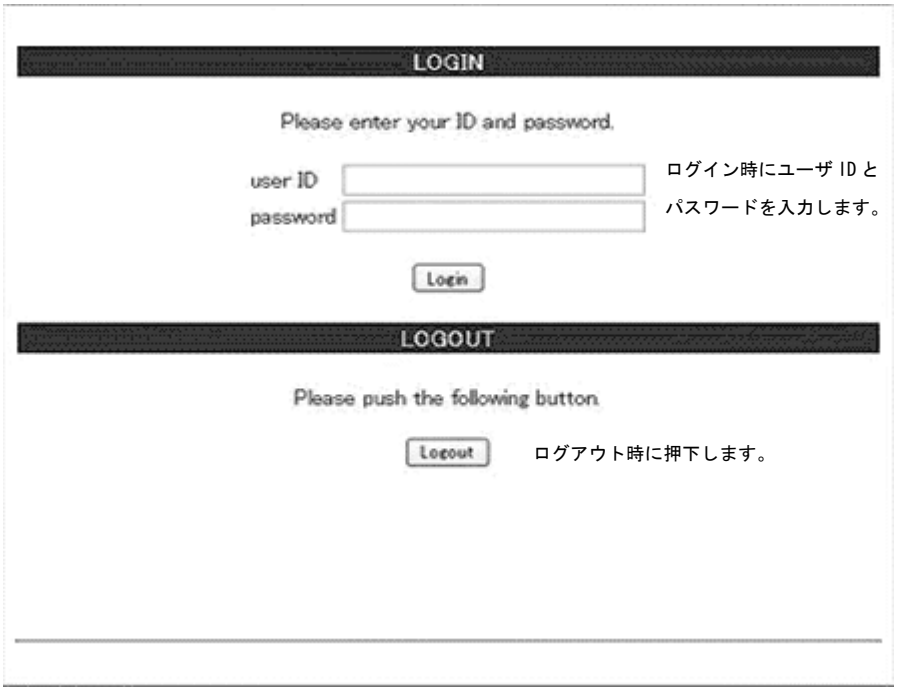
図 9-28　ログアウト完了画面

(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「9.7.12　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 9-29 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 9-25　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 解説

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。

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。
- レガシーモード
  MAC VLAN による VLAN 切り替えにより，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。（Ver.1.3.x までのダイナミック VLAN モードが該当します。）

認証には，本装置に内蔵した DB（内蔵 MAC 認証 DB と呼びます）によるローカル認証方式と，外部に設置した RADIUS サーバに認証要求する RADIUS 認証方式があり，どちらかの方式を選択できます。

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一覧

機能			固定 VLAN	ダイナミック VLAN	レガシー
ローカル認証	内蔵 MAC 認証 DB		○ 「10.2.1」参照 「10.6.1」参照	○ 「10.3.1」参照 「10.6.1」参照	○ 「10.4.1」参照 「10.6.1」参照
		MAC アドレス	○ 「11.6.2」参照	○ 「11.6.2」参照	○ 「11.6.2」参照
		VLAN	○ 「11.6.2」参照	○ 「11.6.2」参照	○ 「11.6.2」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	○ 「10.4.1」参照 「11.5.1」参照
RADIUS 認証	RADIUS サーバ		外部サーバ 「10.2.1」参照 「10.6.2」参照 「11.2.1」参照	外部サーバ 「10.3.1」参照 「10.6.2」参照 「11.2.1」参照	外部サーバ 「10.4.1」参照 「10.6.2」参照 「11.2.1」参照
		ユーザ ID （MAC アドレス）	1 ～ 32 文字 「10.2.1」参照 「10.6.2」参照 「11.2.4」参照	1 ～ 32 文字 「10.3.1」参照 「10.6.2」参照 「11.2.4」参照	1 ～ 32 文字 「10.4.1」参照 「10.6.2」参照 「11.2.4」参照
		VLAN	○ 「10.6.2」参照	○ 「10.6.2」参照	○ 「10.6.2」参照
		パスワード	1 ～ 32 文字 「10.6.2」参照 「11.2.4」参照	1 ～ 32 文字 「10.6.2」参照 「11.2.4」参照	1 ～ 32 文字 「10.6.2」参照 「11.2.4」参照

機能		固定 VLAN	ダイナミック VLAN	レガシー
	VLAN （認証後の VLAN）	○ 「10.2.1」参照 「10.6.2」参照 「11.3.2」参照	○ 「10.3.1」参照 「10.6.2」参照 「11.4.1」参照	○ 「10.4.1」参照 「10.6.2」参照 「11.5.1」参照
	強制認証	○ 「10.2.2」参照	○ 「10.3.2」参照	○ 「10.4.2」参照
	認証許可ポート設定	○ 「11.3.2」参照	○ 「11.4.2」参照	○ 「11.5.2」参照
	プライベートトラップ	○ 「10.5」参照	○ 「10.5」参照	○ 「10.5」参照
	RADIUS サーバ定期的再認証要求	×	○ 「10.3.2」参照 「11.2.4」参照	○ 「10.4.2」参照 「11.2.4」参照
	認証要求時の MAC アドレス形式・パスワード指定	○ 「10.6.2」参照 「11.2.4」参照	○ 「10.6.2」参照 「11.2.4」参照	○ 「10.6.2」参照 「11.2.4」参照
最大認証ユーザ数	ポート単位	1024 「10.2.2」参照 「11.3.2」参照	256 「10.3.2」参照 「11.4.2」参照	256 「10.4.2」参照 「11.5.2」参照
	装置単位	1024 「10.2.2」参照 「11.3.2」参照	256 「10.3.2」参照 「11.4.2」参照	256 「10.4.2」参照 「11.5.2」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	○ 「10.4.2」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	○ 「10.4.2」参照 「11.2.2」参照
	認証専用 IPv4 アクセスリスト	○ 「12」参照	○ 「12」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	○ 「10.4.2」参照 「11.2.3」参照
	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	×
	MAC アドレステーブルエージング監視	×	×	○ 「10.4.2」参照 「11.5.2」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	○ 「10.4.2」参照
	運用コマンド	○ 「10.2.2」参照	○ 「10.3.2」参照	○ 「10.4.2」参照

機能		固定 VLAN	ダイナミック VLAN	レガシー
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	○ 「10.5」参照	○ 「10.5」参照	×
アカウントログ	本装置内蔵アカウントログ	全モード合わせて 2100 行 「10.5」参照		

（凡例） ○：サポート　×：未サポート
「10ｘ.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			固定 VLAN	ダイナミック VLAN	レガシー
VLAN 種別	ポート VLAN		○	×	×
	プロトコル VLAN		×	×	×
	MAC VLAN		△	○	○
デフォルト VLAN			○	×	×
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		×	×	×
	MAC ポート	Untagged	×	○	○
		Tagged	△	×	×
インタフェース種別	fastethernet		○	○	○
	gigabitethernet		○	○	○
	port channel		×	×	×

（凡例）
○：動作可
×：動作不可
△：switchport mac dot1q vlan 設定有のとき，動作可

次項からは，「固定 VLAN モード」「ダイナミック VLAN モード」「レガシーモード」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。）

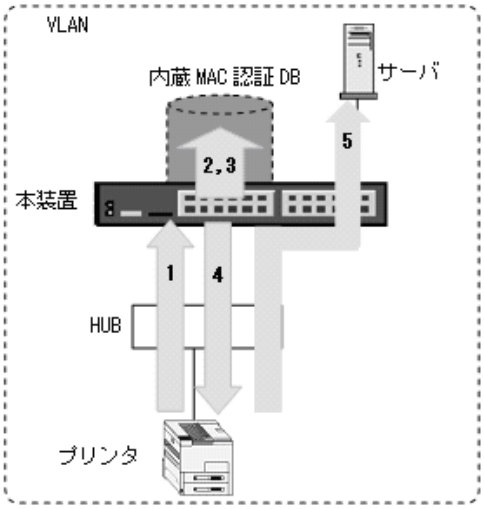
10.2.1　認証方式

本装置では，ローカル認証方式と RADIUS 認証方式をサポートしています。認証方式は，MAC 認証の全認証モード共通で使用します。

（1） 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。

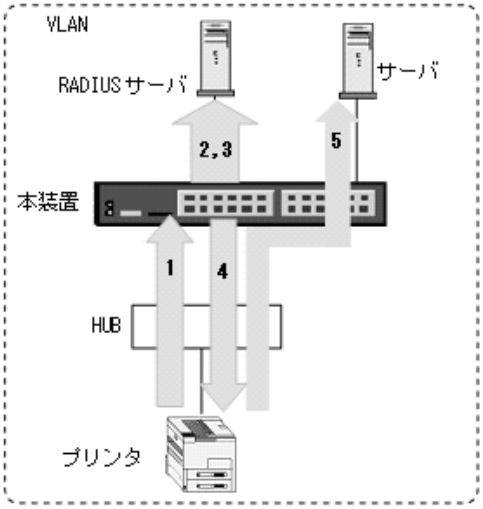
表 10-3 ローカル認証方式の VLAN ID 照合

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
設定あり	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
設定なし	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） 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
設定あり	MAC アドレスと VLAN ID で照合
設定なし	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「10.6 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。

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。

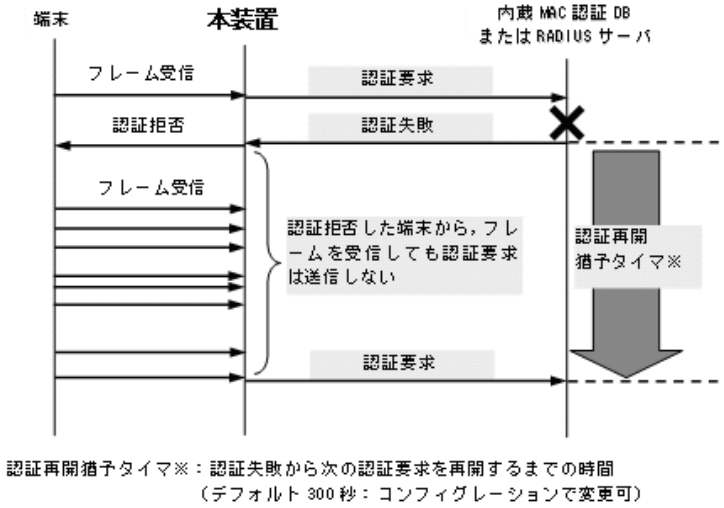
（3） 認証再開猶予タイマ

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 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） 強制認証ポート指定

強制認証指定したポートに接続された端末の RADIUS 認証が，経路障害などで RADIUS サーバへリクエスト送信失敗または無応答となったときは，認証対象端末を認証許可状態にします。

強制認証を許可するポートにコンフィグレーションコマンド mac-authentication static-vlan force-authorized を設定します。

なお，強制認証は下記の条件を満たしたときに許可となります。

表 10-5　強制認証許可条件

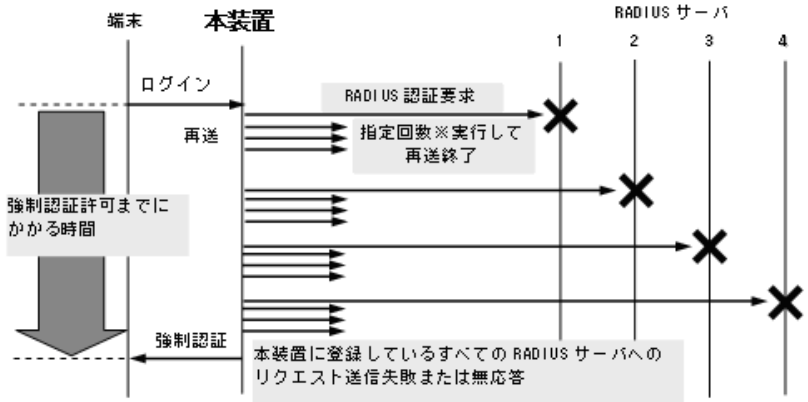
項目	条件
コンフィグレーション	下記のコンフィグレーションがすべて設定されていること • aaa authentication mac-authentication default group radius • radius-server • mac-authentication system-auth-control • mac-authentication port ※ • mac-authentication static-vlan force-authorized ※
アカウントログ	RADIUS サーバへの認証要求送信で，下記のアカウントログが採取された場合 No=21 NOTICE:LOGIN: (付加情報) Login failed ; Failed to connection to RADIUS server. 付加情報：MAC，PORT，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。

注※
同じイーサネットポートに設定してください。

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（6）認証解除」のいずれかの解除機能により認証状態が解除されます。

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 10-4　強制認証許可までのシーケンス（RADIUS サーバ最大数設定時）



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 サーバの接続については，「コンフィグレーションガイド Vol.1　8　ログインセキュリティと RADIUS」を参照してください。

（5）最大認証端末数

最大認証端末数は，装置単位とポート単位の両方で指定することができます。最大認証端末数はコンフィグレーションコマンド mac-authentication static-vlan max-user で最大 1024 台まで設定できます。

装置単位とポート単位を同時に設定することは可能ですが，どちらかが最大数に達した場合，それ以降の新規端末の認証はできません。

また，運用中に認証済み端末数より最大認証端末数を少なく変更した場合，認証済みの端末は継続通信で

きますが，新規端末の認証はできません。

(6) 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。

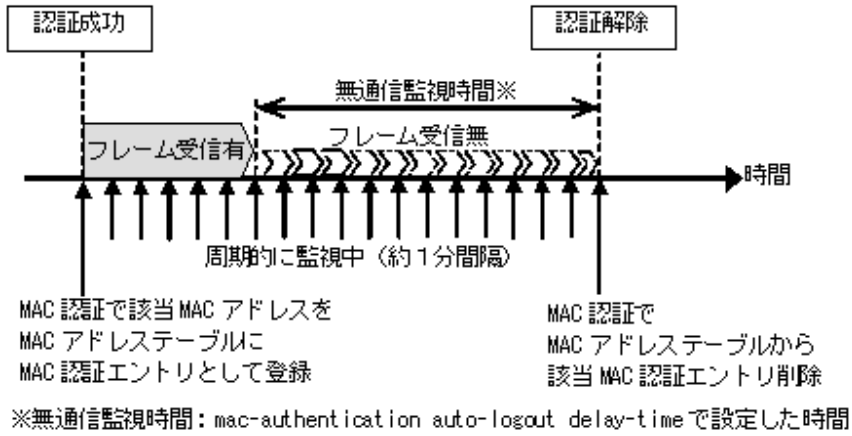
MAC アドレステーブルの MAC 認証エントリを周期的（約 1 分間隔）に監視し，MAC 認証で登録した認証済み端末からのフレーム受信有無を確認します。該当端末からのフレーム受信を一定時間※検出しなかったときに，MAC アドレステーブルから該当 MAC 認証エントリを削除し，認証を解除します。

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 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，デフォルト値と同様に 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。

(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。

(7) ローミング（認証済み端末のポート移動）

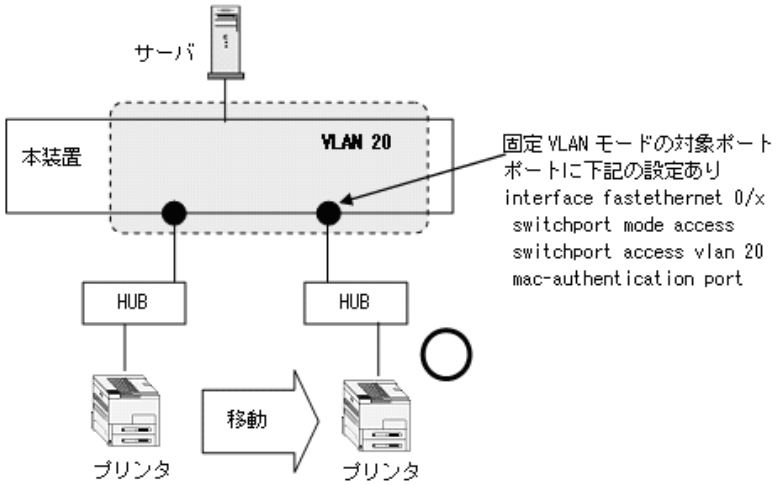
HUB などを経由して接続した認証済み端末（下図ではプリンタ）を，リンクダウンしないでポート移動した場合でも，認証済み状態のまま継続して通信可能にします。

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。

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。）

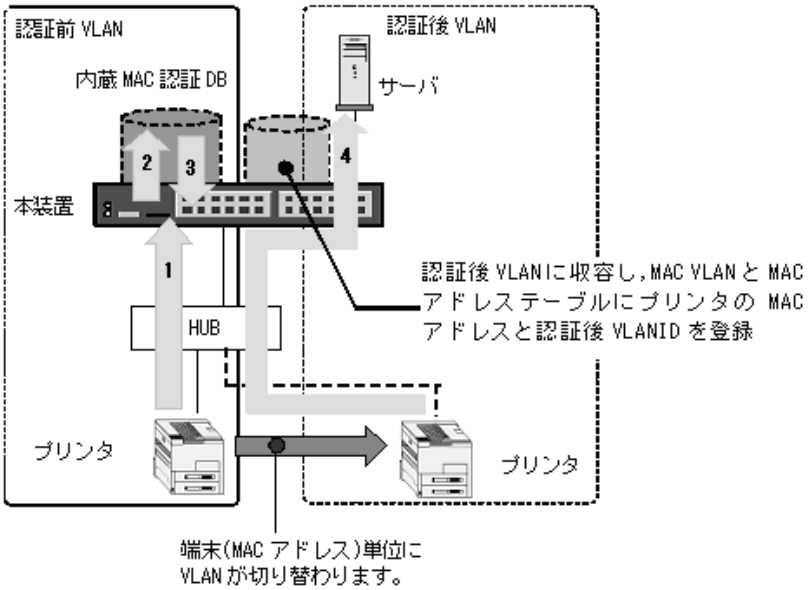
10.3.1 認証方式

本装置では，ローカル認証方式と RADIUS 認証方式をサポートしています。認証方式は，MAC 認証の全認証モード共通で使用します。

（1） 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

内蔵 MAC 認証 DB の該当 MAC アドレスのエントリ情報に従います。

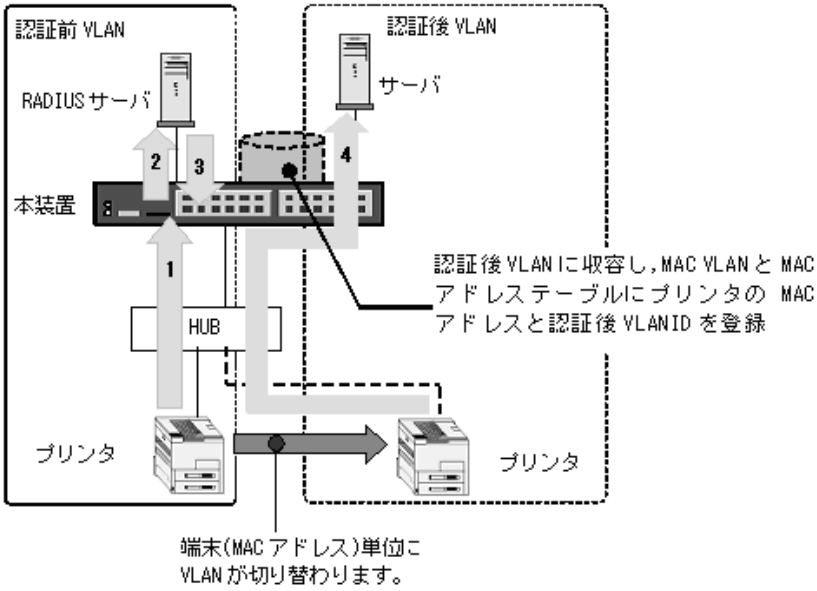
- VLAN ID が登録されている場合：登録されている VLAN に収容します。ただし，VLAN ID がダイナミック VLAN モード対象ポートの VLAN 設定（コンフィグレーションコマンド switchport mac vlan）

に含まれない場合は，認証失敗となります。
- VLAN ID が登録されていない場合：認証失敗となります。

（2） 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

RADIUS サーバの該当 MAC アドレスのエントリに登録されている VLAN ID により認証後 VLAN へ収容します。ただし，VLAN ID がダイナミック VLAN モード対象ポートの VLAN 設定（コンフィグレーションコマンド switchport mac vlan）に含まれない場合は，認証失敗となります。

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

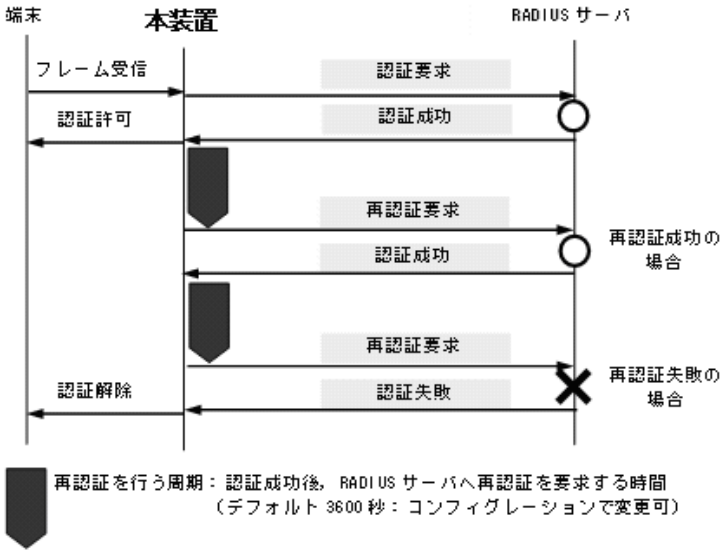
固定 VLAN モードと同様です。「10.2.2　認証機能　（3）認証再開猶予タイマ」を参照してください。

（4） RADIUS サーバへの定期的再認証要求

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 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 10-9　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

強制認証指定したポートに接続された端末の RADIUS 認証が，経路障害などで RADIUS サーバへリクエスト送信失敗または無応答となったときは，認証対象端末を認証許可状態にします。

強制認証を許可するポートにコンフィグレーションコマンド mac-authentication force-authorized vlan を設定します。

なお，強制認証は下記の条件を満たしたときに許可となります。

表 10-6　強制認証許可条件

項目	条件
コンフィグレーション	下記のコンフィグレーションがすべて設定されていること • aaa authentication mac-authentication default group radius • radius-server • mac-authentication system-auth-control • vlan <VLAN ID list> mac-based ※1 • mac-authentication force-authorized vlan ※1※2 • mac-authentication port ※2 • switchport mac vlan ※1※2 • switchport mode mac-vlan ※2
アカウントログ	RADIUS サーバへの認証要求送信で，下記のアカウントログが採取された場合 No=21 NOTICE:LOGIN: (付加情報) Login failed ; Failed to connection to RADIUS server. 付加情報：MAC，PORT，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。

注※ 1

同じ VLAN ID を設定してください。

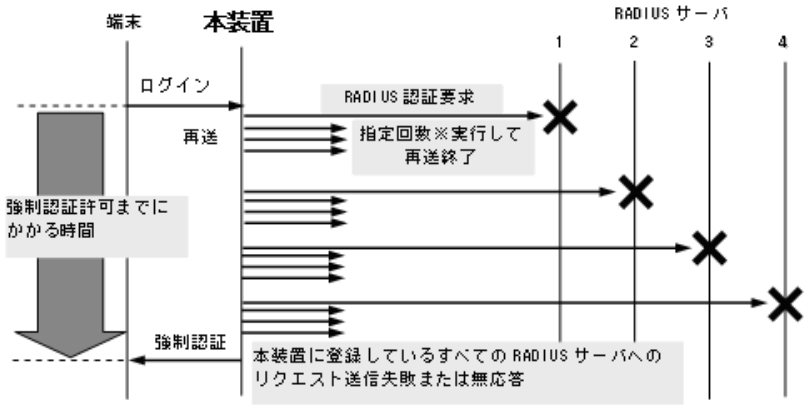
注※ 2

同じイーサネットポートに設定してください。

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」のいずれかの解除機能により認証状態が解除されます。

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 10-10　強制認証許可までのシーケンス（RADIUS サーバ最大数設定時）



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 サーバの接続については，「コンフィグレーションガイド Vol.1　8　ログインセキュリティと RADIUS」を参照してください。

（6）最大認証端末数

最大認証端末数は，装置単位とポート単位の両方で指定することができます。最大認証端末数はコンフィ

グレーションコマンド mac-authentication max-user で最大 256 台まで設定できます。

装置単位とポート単位を同時に設定することは可能ですが，どちらかが最大数に達した場合，それ以降の新規端末の認証はできません。

また，運用中に認証済み端末数より最大認証端末数を少なく変更した場合，認証済みの端末は継続通信できますが，新規端末の認証はできません。

(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　(6) 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）

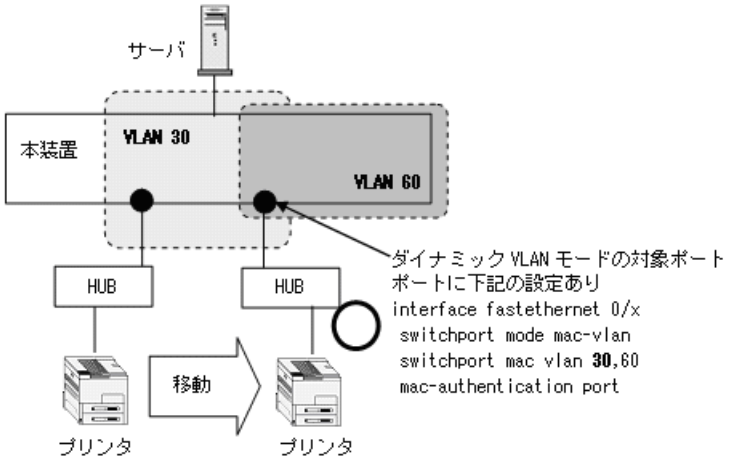
HUB などを経由して接続した認証済み端末（下図ではプリンタ）を，リンクダウンしないでポート移動した場合でも，認証済み状態のまま継続して通信可能にします。

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
- 移動前の認証後 VLAN が，移動後ポートのコンフィグレーションコマンド switchport mac vlan に設定されていること

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。

図 10-11　ダイナミック VLAN モード　ローミング概要図



10.4　レガシーモード

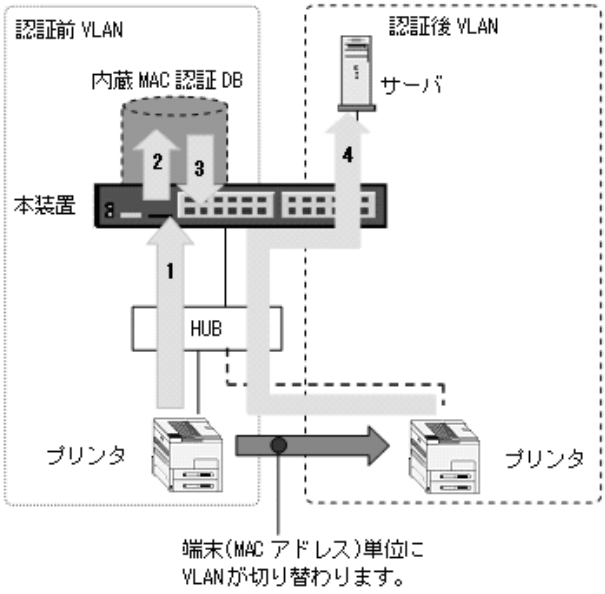
10.4.1　認証方式

本装置では，ローカル認証方式と RADIUS 認証方式をサポートしています。認証方式は，MAC 認証の全認証モード共通で使用します。

(1) 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 10-12　レガシーモード概要図（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。

(a) 収容 VLAN の切り替えについて

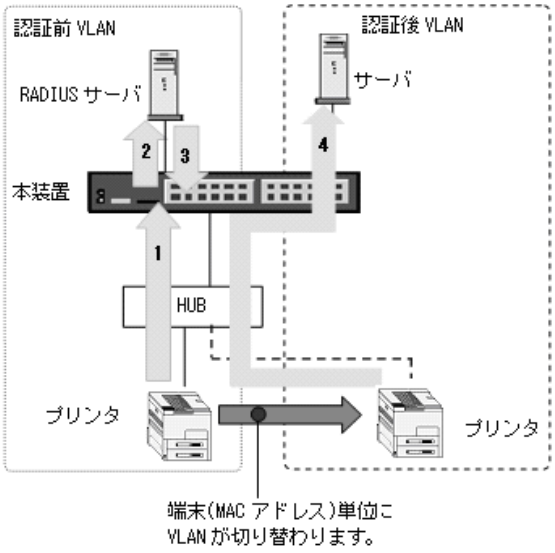
内蔵 MAC 認証 DB の該当 MAC アドレスのエントリに登録されている VLAN ID が，レガシーモードの認証後 VLAN 設定 (コンフィグレーションコマンド mac-authentication vlan) に含まれない場合は，認証失敗となります。

また，内蔵 MAC 認証 DB の該当 MAC アドレスのエントリに VLAN 情報が登録されていない場合も，認証失敗となります。

（2） 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 10-13 レガシーモード概要図（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。

(a) 収容 VLAN の切り替えについて

RADIUS サーバの該当 MAC アドレスのエントリに登録されている VLAN ID が，レガシーモードの認証後 VLAN 設定 (コンフィグレーションコマンド mac-authentication vlan) に含まれない場合は，認証失敗となります。

10.4.2 認証機能

（1） 認証契機

レガシーモードは，MAC VLAN に収容されているポートでかつ MAC 認証レガシーモードの対象として指定したポートのネイティブ VLAN 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 ユニキャスト，MAC ブロードキャスト，MAC マルチキャストフレームを問わず，すべてのフレームが対象となります。

このため，MAC VLAN のネイティブ VLAN に収容された端末間が通信を行うと，端末間の通信データすべてが MAC 認証対象フレームとなり，MAC 認証処理が動作しますので，認証対象 MAC アドレス制限機能などを用いて適切な設定と運用が必要です。

また，MAC 認証は対象端末を本装置に直接またはスイッチなどを経由し接続するだけで，認証対象端末側には特別な認証設定や認証手順は必要ありません。ただし，MAC 認証対象端末からなんらかのフレー

ムが送信されなければ，MAC 認証処理が開始されませんのでご注意ください。

レガシーモードの認証ポートは，固定 VLAN モードやダイナミック VLAN モードと異なり，ポート単位ではなく装置単位でレガシーモードを動作させるイーサネットポート番号を設定します。

コンフィグレーションコマンド mac-authentication interface で，レガシーモードを動作させるポート番号を設定できます。

(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) RADIUS サーバへの定期的再認証要求

ダイナミック VLAN モードと同様です。「10.3.2　認証機能　(4) RADIUS サーバへの定期的再認証要求」を参照してください。

(5) 強制認証ポート指定

強制認証指定したポートに接続された端末の RADIUS 認証が，経路障害などで RADIUS サーバへリクエスト送信失敗または無応答となったときは，認証対象端末を認証許可状態にします。

強制認証を許可するポートにコンフィグレーションコマンド mac-authentication force-authorized vlan を設定します。

なお，強制認証は下記の条件を満たしたときに許可となります。

表 10-7　強制認証許可条件

項目	条件
コンフィグレーション	下記のコンフィグレーションがすべて設定されていること • aaa authentication mac-authentication default group radius • radius-server • mac-authentication system-auth-control • mac-authentication vlan ※1 • vlan <VLAN ID list> mac-based ※1 • mac-authentication force-authorized vlan ※1※2 • switchport mac vlan ※1※2 • switchport mode mac-vlan ※2 • mac-authentication interface ※3
アカウントログ	RADIUS サーバへの認証要求送信で，下記のアカウントログが採取された場合 No=21 NOTICE:LOGIN: (付加情報) Login failed ; Failed to connection to RADIUS server. 付加情報：MAC，PORT，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。

注※ 1
同じ VLAN ID を設定してください。

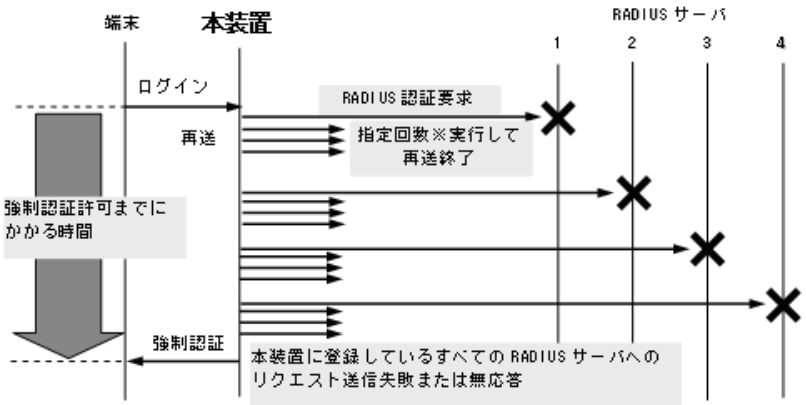
注※ 2
同じイーサネットポートに設定してください。

注※ 3
※ 2 のコマンドを設定したイーサネットポート番号を設定してください。

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「10.4.2　認証機能（7）認証解除」のいずれかの解除機能により認証状態が解除されます。

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 10-14　強制認証許可までのシーケンス（RADIUS サーバ最大数設定時）



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 サーバの接続については，「コンフィグレーションガイド Vol.1　8　ログインセキュリティと RADIUS」を参照してください。

（6） 最大認証端末数

最大認証端末数は，装置単位とポート単位の両方で指定することができます。最大認証端末数はコンフィグレーションコマンド mac-authentication max-user で最大 256 台まで設定できます。

装置単位とポート単位を同時に設定することは可能ですが，どちらかが最大数に達した場合，それ以降の新規端末の認証はできません。

また，運用中に認証済み端末数より最大認証端末数を少なく変更した場合，認証済みの端末は継続通信できますが，新規端末の認証はできません。

（7） 認証解除

レガシーモードでは，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
- MAC アドレステーブルエージング監視による認証解除
- 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

「MAC アドレステーブルエージング監視による認証解除」以外の認証解除手段は，固定 VLAN モードと同様です。「10.2.2　認証機能　（6）認証解除」を参照してください。

（a）MAC アドレステーブルエージング監視による認証解除

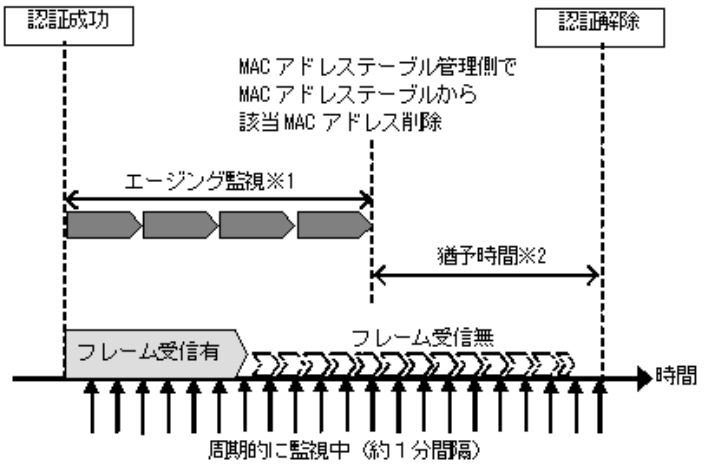
MAC アドレステーブルのダイナミックエントリを周期的（約 1 分間隔）に監視し，レガシーモードの認証後 VLAN ID で登録されている端末の MAC アドレスがエージングされているか確認します。

レガシーモードの MAC アドレスエージング時間は，固定 VLAN モードやダイナミック VLAN モードと異なり，コンフィグレーションコマンド mac-address-table aging-time の設定に従います。
mac-address-table aging-time のエージングタイムアウトで該当 MAC アドレスが削除されてから，コンフィグレーションコマンド mac-authentication auto-logout で指定した猶予時間（delay-time：デフォルト 3600 秒）まで削除状態が継続した場合に，自動で認証を解除します。

エージングタイムアウト後の猶予時間はコンフィグレーションコマンド mac-authentication auto-logout で猶予時間を変更，または無効に設定することができます。

なお，猶予時間（delay-time）に 0 秒を設定すると，エージングタイムアウトで該当 MAC アドレス削除を検出後，即時に認証を解除します。

図 10-15　レガシーモードで認証済み端末の MAC アドレステーブルエージング概要



※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：mac-authentication auto-logout delay-time で設定した時間

（8）認証済み端末のポート移動と認証端末数の表示について

レガシーモードでは，ローミング用のコンフィグレーションはありません。認証済みの端末をポート移動した際は下記の動作となります。

1. 一度 MAC 認証が完了した端末は，認証した時点のポートで認証端末数に計上されます。
2. レガシーモードで認証済みの端末をほかのポートに移動した場合，下記の条件すべてに該当する場合は継続して通信可能です。
   - 移動前および移動後が，レガシーモード対象ポート
   - 移動前の認証後 VLAN が，移動後ポートのコンフィグレーションコマンド switchport mac vlan に設定されていること

   移動後の端末は MAC アドレステーブルエージング監視で検出されるまでの間，通信可能となります。ただし，移動後ポートで DHCP snooping やフィルタなどを併用している場合は，その条件に依存します。
   上記以外の移動は認証を解除しますが，レガシーモードで認証済みの端末を認証対象外ポートに移動したときは認証解除しない場合があります。

3. 次の再認証時間となった時点でポートの移動を検出します。
4. 移動後のポートがレガシーモードの対象ポートの場合，認証端末数の計上は下記のとおりです。
   - 最大認証端末数制限以内であれば，移動前ポートの認証端末数減算と，移動後ポートでの認証登録が実施されます。
   - 最大認証端末数制限以上となった場合，移動前ポートの認証端末数減算と，認証解除が実施されます。
5. 次の認証時間がくる前に MAC アドレステーブルエージング監視で，移動前ポートでの MAC アドレス消失が検出された場合，移動後ポートで新規端末として認証処理が実施されます。

10.5 アカウント機能

MAC 認証の認証結果は，本装置に内蔵のアカウントログ機能で記録されます。RADIUS サーバのアカウント機能はサポートしておりません。

なお，本装置の内蔵アカウントログには，MAC 認証の全認証モードの合計で最大 2100 行まで記録されます。2100 行を超えた場合，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 10-8 アカウントログ種別

アカウントログ種別	内容
LOGIN	認証操作に関する内容（成功・失敗）
LOGOUT	認証解除操作に関する内容（理由等）
SYSTEM	MAC 認証機能の動作に関する内容 （ローミング検出，強制認証許可も含む）

表 10-9 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	MAC	VLANI	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

（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 23 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. イベントごとのコンソール表示
   運用コマンド trace-monitor enable を実施済みの環境においても，アカウントログはイベント発生ごとにコンソールに表示しません。
2. 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。
3. syslog サーバへ出力
   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，装置全体のイベントトレース情報と合わせてアカウントログ情報を出力します。MAC 認証の内蔵アカウントログ情報だけを syslog サーバへ出力または抑止指定することはできません。
4. 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 10-10 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 10-11 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
強制認証	固定 VLAN	snmp-server host	mac-authentication
		mac-authentication static-vlan force-authorized	action trap
	ダイナミック VLAN	snmp-server host	mac-authentication
		mac-authentication force-authorized vlan	action trap
	レガシー	snmp-server host	mac-authentication
		mac-authentication force-authorized vlan	action trap
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
	レガシー	－（対象外のため，該当設定なし）	

10.6　事前準備

10.6.1　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。

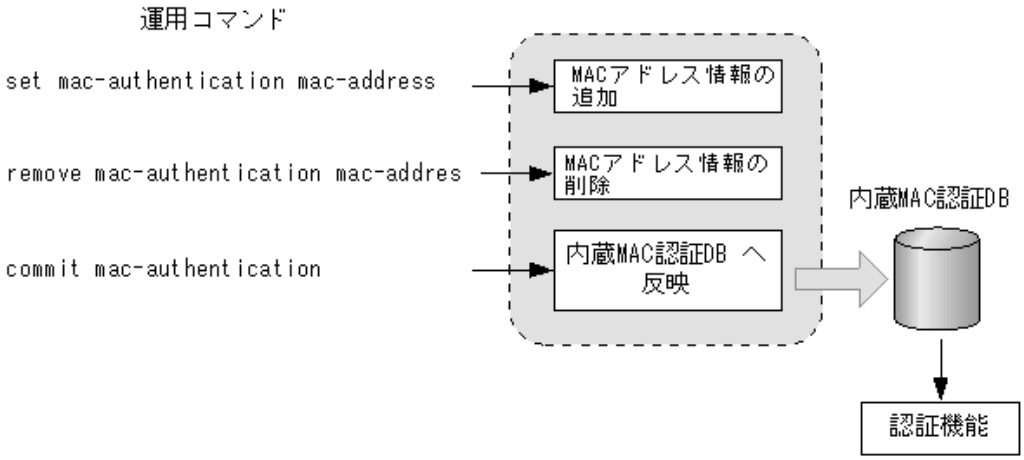
内蔵 MAC 認証 DB へ登録手順として，MAC アドレス情報の編集（追加・削除）と内蔵 MAC 認証 DB への反映があります。手順を以下に示します。

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 10-16　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 設定なしも含む）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。

Ver.1.4 以降では，内蔵 MAC 認証 DB に MAC アドレスと MAC マスク付きのエントリも登録できます。このため，Ver.1.4 以降の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。MAC アドレスエントリだけのファイルは，Ver.1.3 ～ 1.3.x の MAC マスク情報未サポートの装置でも復元するときに使用できます。

- < 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。

また，Ver.1.4 以降で作成した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。

バージョンアップまたはダウン時の内蔵 MAC 認証 DB の復元状態については，後述の「10.7.4　バージョンアップ（またはダウン）時の注意事項　(2) 内蔵 MAC 認証 DB について」を参照してください。

10.6.2 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 10-12 認証で使用する属性名（その 1 Access-Request）

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。
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※
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※
NAS-IP-Address	4	認証を要求している，本装置の IP アドレス。IP 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 IP アドレスを使用します。
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，レガシーモード： 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)

注※
後述の「(b) RADIUS サーバに設定する情報」を参照してください。

表 10-13 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。
Reply-Message	18	未使用※1
Tunnel-Type	64	トンネル・タイプ。 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。 IEEE802(6) 固定。
Tunnel-Private-Group-ID	81	VLAN を識別する文字列※2。 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）※3 （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

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※ 2

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 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※ 3

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，「12.2.3　ダイナミック VLAN モード収容 VLAN の VLAN 名称指定」を参照してください。

(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 モードまたはレガシー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，レガシーモードの場合：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 10-14 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
Tunnel-Type	Virtual VLAN（値 13）
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-Medium-Type	IEEE-802（値 6）
Tunnel-Private-Group-ID	ダイナミック VLAN モード，レガシーモードの場合 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 10-15　コンフィグレーションの設定と RADIUS サーバへ認証要求形式

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		12345600fffe1	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	
無	無	有	12-34-56-00-ff-e1	指定文字列
	vlan-check	（任意文字列）	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	

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
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 モードまたはレガシー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 10-16 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	12-34-56-00-ff-e1	指定文字列
id-format 0	（任意文字列）	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	

10.7　MAC 認証の注意事項

10.7.1　認証モード共通の注意事項

（1） MAC 認証のコンフィグレーションを設定する前に

【固定 VLAN モード】【ダイナミック VLAN モード】

固定 VLAN モード，ダイナミック VLAN モードを使用する場合，システムファンクションリソースの設定が必要となります。システムファンクションリソース設定については，「コンフィグレーションガイド Vol.1　9.1.6　システムファンクションリソース配分の設定」を参照し，その他の適切な機能も合わせて選択してください。

（2） 認証契機のフレームについて

【固定 VLAN モード】【ダイナミック VLAN モード】

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 設定なしも含む）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 10-17　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
あり	設定あり	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）※
	設定なし	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）
なし	設定あり	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）
	設定なし	

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 10-18 ダイナミック VLAN モード，レガシーモードの場合

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
あり	最初に一致した MAC アドレスの VLAN に収容し，認証許可
なし	認証後 VLAN に収容できないので，認証失敗

(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

- 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。
- 本機能は RADIUS 認証方式だけサポートしています。

(6) ローミング設定と DHCP snooping 併用時の制限

【固定 VLAN モード】【ダイナミック VLAN モード】

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。

(7) ポート移動と最大認証端末数について

【固定 VLAN モード】【ダイナミック VLAN モード】

最大認証端末数チェックは，新規認証の端末に対してだけ実施します。

従って，認証済み端末のポート移動では，移動後のポートで最大認証端末数チェックを行いません。

10.7.2 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 モードが動作可能なポートはイーサネットインタフェースだけです。また，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。

10.7.3　レガシー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 アドレステーブルエージング時間（コンフィグレーションコマンド mac-address-table aging-time）を短く設定すると，MAC アドレスエージング監視機能で，自動的に認証解除される時間が短くなります。なお，自動的に認証解除させたくない場合は，コンフィグレーションコマンド no mac-authentication auto-logout を設定してください。

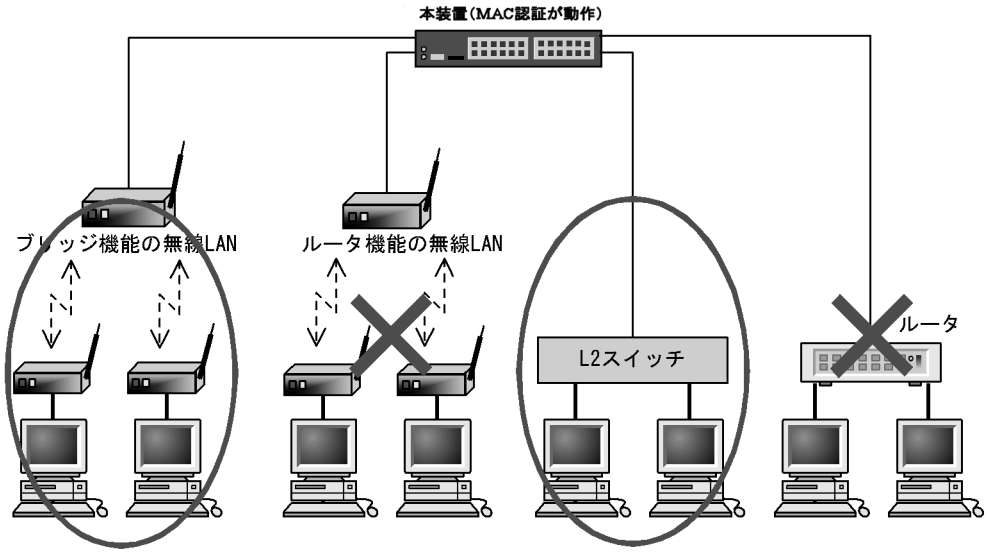
（2） 本装置と認証対象の端末間に接続する装置について

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）が存在した場合，MAC 認証が書き換えられた MAC アドレスを認証対象端末と認識できないため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無い 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 10-17　本装置と端末間の接続



（3） アカウントログ情報のポート番号情報について

ポート番号情報は，認証時および再認証時の情報となります。

認証済み端末の接続ポートを移動した際は，即時に情報は採取されず，再認証時間の経過時に検出したポート番号情報が採取されます。

10.7.4　バージョンアップ（またはダウン）時の注意事項

（1） MAC ポートの認証モードの動作について

Ver.1.4 以降では，レガシーモードを使用できないケースがあります。MAC ポートに下記のコンフィグレーション設定がある場合，レガシーモードは使用できなくなり，かわってダイナミック VLAN モードとして動作します。

表 10-19 MAC ポートと認証モードのバージョンアップ別動作

MAC ポートのコンフィグレーション設定	対象バージョン	固定 VLAN	ダイナミック VLAN	レガシー
mac-authentication port あり	Ver.1.1 ～ 1.3.x	○※1	未サポート	○
switchport mac dot1q vlan あり	Ver.1.4 ～	○※1	○	×※2

（凡例）
○：動作可
×：動作不可

注※ 1
Tagged フレームだけ対象

注※ 2
ダイナミック VLAN モードへ移行

（2） 内蔵 MAC 認証 DB について

Ver.1.4 以降で登録した MAC マスクを含む内蔵 MAC 認証 DB のバックアップファイルを，Ver.1.4 より古いバージョンの装置に復元すると，MAC マスクなしのエントリだけが復元されます。

表 10-20 バージョンアップまたはダウン時のデータ保障と互換性

本装置のバージョン	実施前の内蔵 MAC 認証 DB	バージョンアップ・ダウン	データ保障	実施後の内蔵 MAC 認証 DB
1.3 ～ 1.3.x	MAC アドレスだけ	アップ	○	MAC アドレスだけ
		ダウン	○	MAC アドレスだけ
1.4 ～	MAC アドレスだけ	アップ	○	MAC アドレスだけ
		ダウン	○	MAC アドレスだけ
	MAC アドレス＋ MAC マスク	アップ	○	MAC アドレス＋ MAC マスク
		ダウン	○	MAC アドレスだけ

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	レ
aaa authentication mac-authentication default group radius	MAC 認証機能での RADIUS サーバの使用有無を設定します。	○	○	○
authentication arp-relay ※1	認証前状態の端末から送信される他機器宛て ARP フレームを，認証対象外のポートへ出力させます。	○	○	×
authentication ip access-group ※1	認証前状態の端末から送信される他機器宛ての IP フレームを，IPv4 アクセスリストを適用して設定されたフレームだけを認証対象外のポートへ出力させます。	○	○	×
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 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 force-authorized vlan	RADIUS 認証方式を使用時，経路障害などで RADIUS サーバへのリクエスト失敗時に，該当ポートに接続された認証対象端末を強制的に認証許可状態にします。	－	○	○
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 interface	MAC 認証の対象イーサネットポートを設定します。	－	－	○
mac-authentication max-timer	最大接続時間を設定します。	○	○	○
mac-authentication max-user	装置単位の最大認証端末数を設定します。	－	○	○
mac-authentication max-user (interface)	当該ポートの最大認証端末数を設定します。	－	○	○
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 ※2	ポートに認証モードを設定します。	○	○	－
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 force-authorized	RADIUS 認証方式を使用時，経路障害などで RADIUS サーバへのリクエスト失敗時に，該当ポートに接続された認証対象端末を強制的に認証許可状態にします。	○	－	－
mac-authentication static-vlan max-user	装置単位の最大認証端末数を設定します。	○	－	－
mac-authentication static-vlan max-user (interface)	当該ポートの最大認証端末数を設定します。	○	－	－
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。	○	－	－

コマンド名	説明	認証モード		
		固	ダ	レ
mac-authentication system-auth-control	MAC 認証を有効にします。	○	○	○
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	端末認証後，動的に切り替える VLAN ID 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
レ：レガシーモード
○：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※ 1
設定の詳細については，「12　レイヤ 2 認証の共通機能と共存使用」を参照してください。

注※ 2
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 認証のコンフィグレーションを設定する前に

MAC 認証で認証モードを設定する場合は，コンフィグレーションを設定する前に，下記を設定してください。

［設定のポイント］
下記の認証モードの場合，設定の最初の段階でシステムファンクションリソースの割り当てをコンフィグレーションで設定する必要があります。
- 固定 VLAN モード
- ダイナミック VLAN モード

システムファンクションリソースの割り当て設定は装置の再起動が必要です。システムファンクションリソースの割り当てについての詳細は「コンフィグレーションガイド Vol.1 9.1.6 システムファンクションリソース配分の設定」を参照してください。
本例ではフィルタと拡張認証機能を割り当てます。

［コマンドによる設定］

1. **(config)# system function filter extended-authentication**
```
Please execute the reload command after save,
because this command becomes effective after reboot.
```
システムリソースとしてフィルタと拡張認証機能を割り当てます。設定の保存と装置再起動を促すメッセージを表示します。
2. **(config)# end**
```
# copy running-config startup-config
Do you wish to copy from running-config to startup-config? (y/n): y
@# reload
```

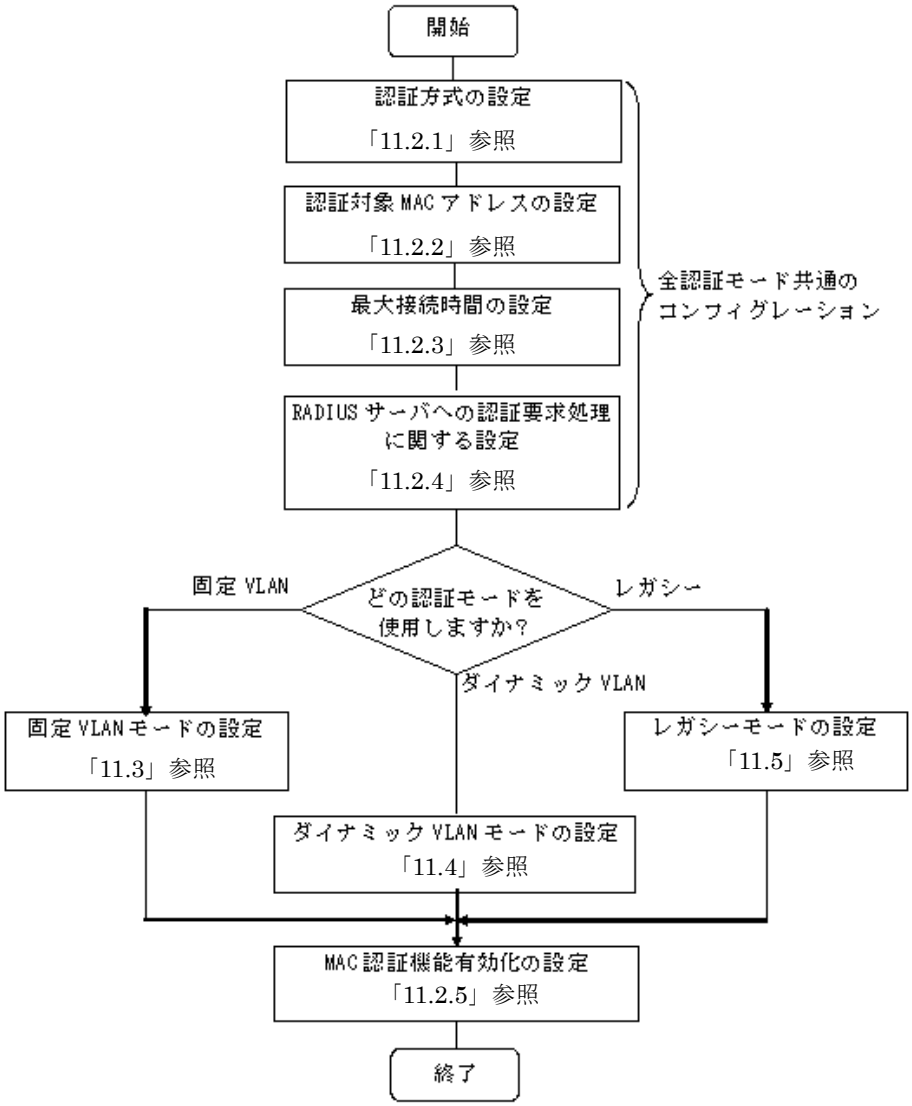
```
Restart OK? (y/n): y
```

コンフィグレーションの設定を保存すると，プロンプトに " @ " を表示しますので，装置を再起動してください。

11.1.3 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。
   - 認証方式の設定：「11.2.1　認証方式の設定」
   - 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」

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」
   - レガシーモードの設定：「11.5　レガシー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。
   - 「11.2.5　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。

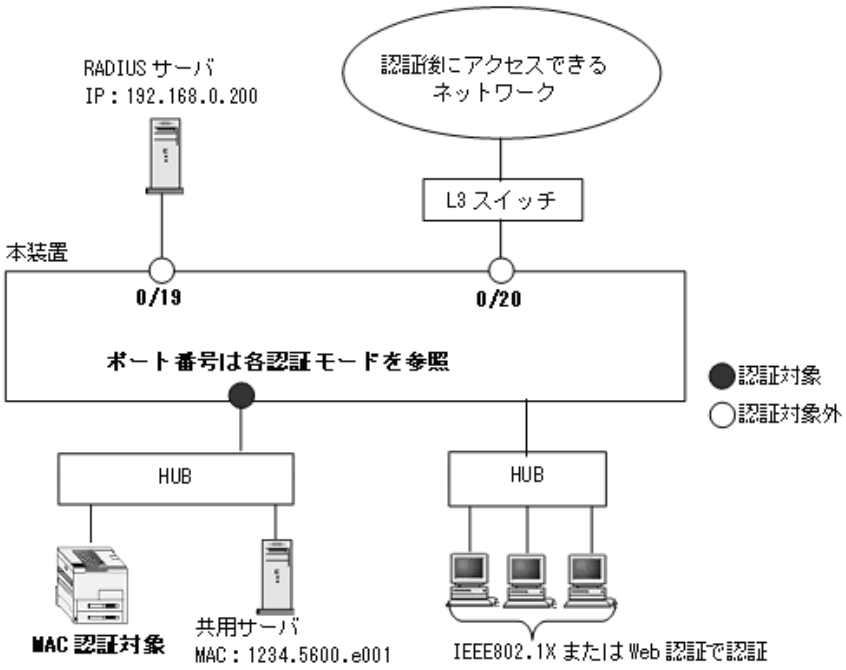
表 11-2　各認証モード有効条件

認証モード	コンフィグレーション設定
共通	• 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 • switchport mac vlan
レガシーモード	• vlan <VLAN ID list> mac-based • mac-authentication interface • mac-authentication vlan • switchport mode mac-vlan • switchport 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 0/19，0/20 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　認証方式の設定

［設定のポイント］

MAC 認証共通で使用する認証方式として，RADIUS 認証方式と 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 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。

［コマンドによる設定］

1. **(config)# aaa authentication mac-authentication default group radius**
   RADIUS 認証方式を設定します。

2. **(config)# radius-server host 192.168.0.200 key "L2auth"**
   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，timeout，retransmit は省略時の初期値が適用されます。

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。

［注意事項］

1. 本設定省略時はローカル認証方式となります。ローカル認証方式では，内蔵 MAC 認証 DB の登録が必要です。登録については「11.6.2　内蔵 MAC 認証 DB の登録」を参照してください。
2. RADIUS サーバ情報は，本装置全体で最大４エントリまで設定できます。ログインセキュリティ機能やほかのレイヤ２認証機能と共用となることを考慮して，RADIUS サーバ情報を設定してください。

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 src 1234.5600.e000 0000.0000.ffff dst 0000.0000.0000 ffff.ffff.ffff
   (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］

1. 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。
2. 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。
3. 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。
4. 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「10.6.2　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，パスワードをを設定します。設定の組み合わせについては「10.6.2　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］

1. 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。
2. 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］

1. 本機能は MAC 認証機能を有効にするとデフォルト 300 秒で動作します。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。

2. 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]

MAC 認証ダイナミック VLAN モードまたはレガシーモードで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。
なお，固定 VLAN モードは本設定の対象外です。

[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。
   - ダイナミック VLAN モード :「10.3.2　認証機能（7）認証解除」
   - レガシーモード :「10.4.2　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　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。

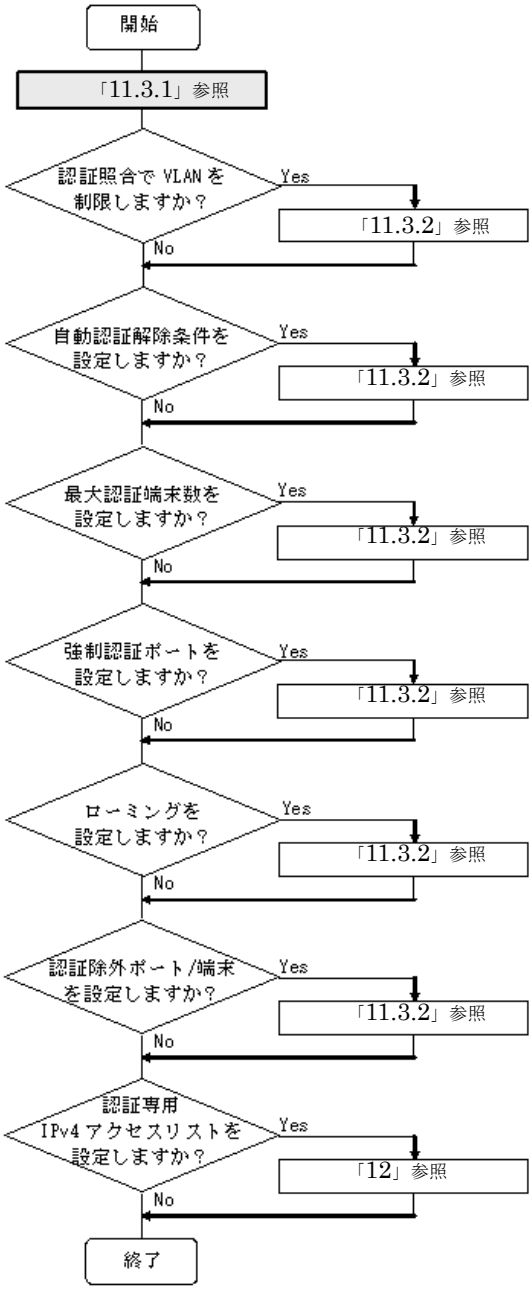
[注意事項]

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



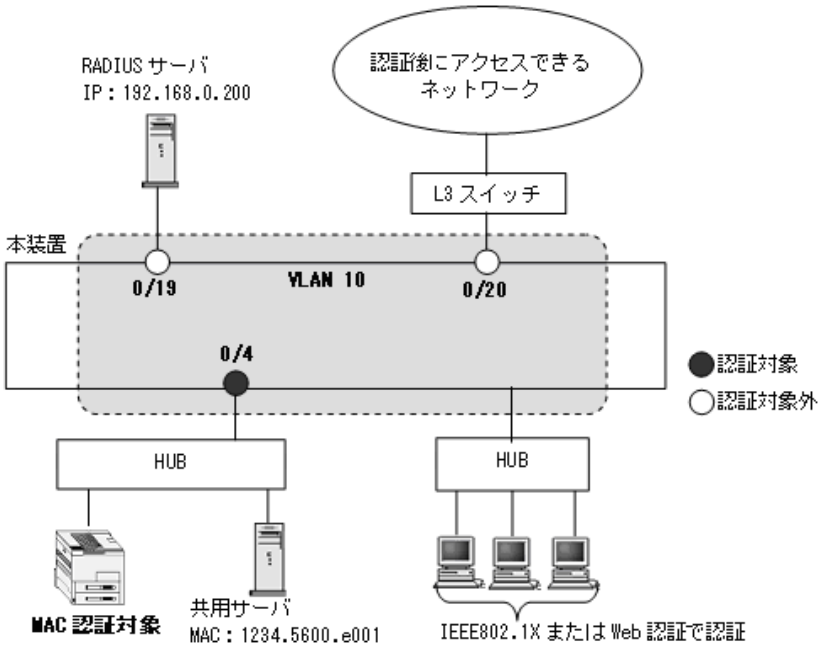
各設定の詳細は，下記を参照してください。

1. 認証ポートの設定：「11.3.1 認証ポートの設定」
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. 最大認証端末数の設定：「11.3.2　認証処理に関する設定（3）最大認証端末数の設定」
5. 強制認証ポートの設定：「11.3.2　認証処理に関する設定（4）強制認証ポートの設定」
6. ローミングの設定：「11.3.2　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. 認証除外ポート / 端末の設定：「11.3.2　認証処理に関する設定（6）認証除外の設定」
8. 認証専用 IPv4 アクセスリストの設定：「12　レイヤ 2 認証の共通機能と共存使用」

11.3.1　認証ポートの設定

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 fastethernet 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。

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 モード認証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。

[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。
本機能は MAC 認証機能を有効にするとデフォルト（delay-time：3600 秒）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。

[注意事項]

1. 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。
2. 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） 最大認証端末数の設定

［設定のポイント］

固定 VLAN モードで認証可能な最大認証端末数を設定します。
装置単位で設定する場合はグローバルコンフィグレーションモードで設定し，ポート単位で設定する場合は当該ポートのコンフィグレーションモードで設定します。

［コマンドによる設定］

1. **(config)# interface fastethernet 0/4**
   (config-if)# mac-authentication static-vlan max-user 2
   (config-if)# exit
   ポート 0/4 での認証最大端末数を 2 に設定します。

（4） 強制認証ポートの設定

［設定のポイント］

固定 VLAN モードの対象ポートで，強制認証を許可するポートに設定します。

［コマンドによる設定］

1. **(config)# interface fastethernet 0/4**
   (config-if)# mac-authentication static-vlan force-authorized
   (config-if)# exit
   ポート 0/4 を強制認証ポートに設定します。

（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)# 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］

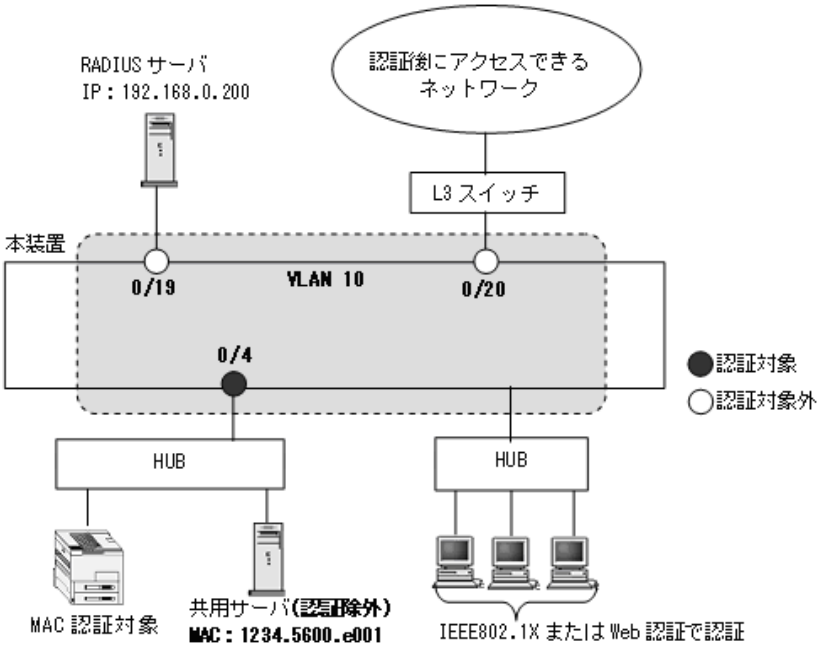
ローミングの動作可能な条件は下記のとおりです。

- 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

（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 0/19，0/20，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 fastethernet 0/19-0/20**
   (config-if-range)# switchport mode access
   (config-if-range)# switchport access vlan 10
   (config-if-range)# exit
   VLAN ID 10 のポート 0/19 と 0/20 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。

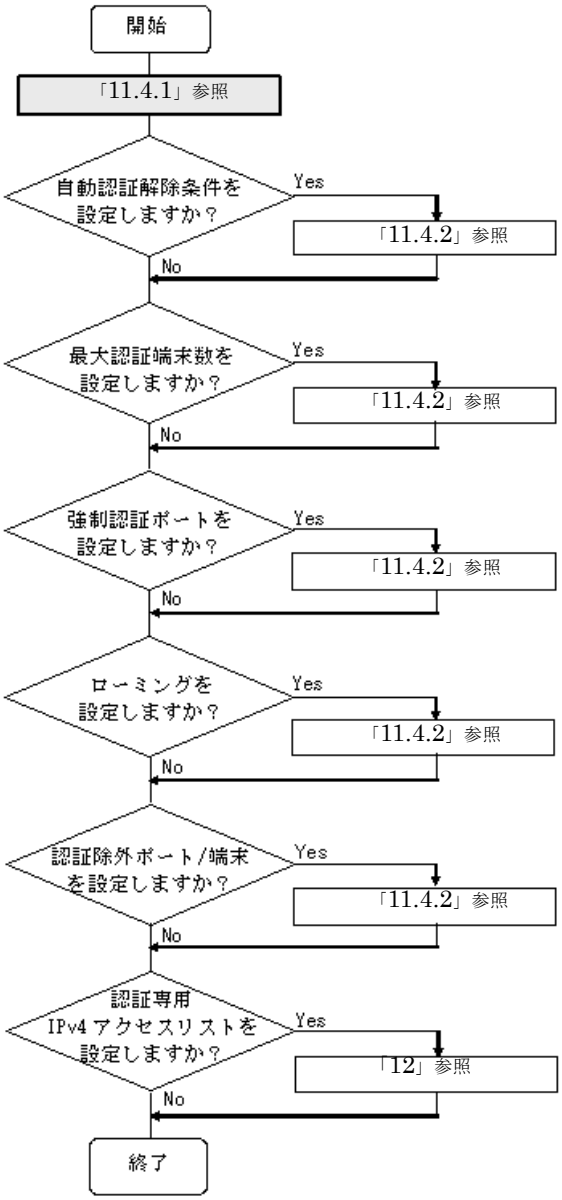
[コマンドによる設定]

1. **(config)# mac-address-table static 1234.5600.e001 vlan 10 interface fastethernet 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



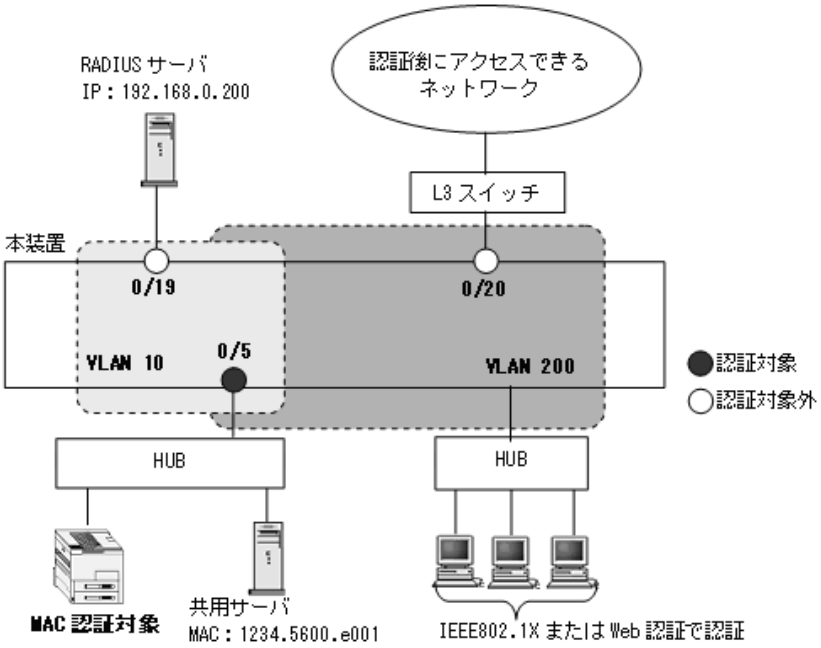
各設定の詳細は，下記を参照してください。

1. 認証ポートの設定：「11.4.1　認証ポートの設定」
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. 最大認証端末数の設定：「11.4.2　認証処理に関する設定（2）最大認証端末数の設定」

4. 強制認証ポートの設定：「11.4.2　認証処理に関する設定（3）強制認証ポートの設定」
5. ローミングの設定：「11.4.2　認証処理に関する設定（4）ローミング（認証済み端末のポート移動通信許可）の設定」
6. 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（5）認証除外の設定」
7. 認証専用 IPv4 アクセスリストの設定：「12　レイヤ 2 認証の共通機能と共存使用」

11.4.1　認証ポートの設定

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。

[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 fastethernet 0/5**
   (config-if)# switchport mode mac-vlan
   (config-if)# switchport mac vlan 200
   (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 と認証後 VLAN200 を設定します。

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。

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) 最大認証端末数の設定

[設定のポイント]

ダイナミック VLAN モードで認証可能な最大認証端末数を設定します。
装置単位で設定する場合はグローバルコンフィグレーションモードで設定し，ポート単位で設定する場合は当該ポートのコンフィグレーションモードで設定します。

[コマンドによる設定]

1. **(config)# interface fastethernet 0/5**
   (config-if)# mac-authentication max-user 2
   (config-if)# exit
   ポート 0/5 での最大認証端末数を 2 に設定します。

(3) 強制認証ポートの設定

[設定のポイント]

ダイナミック VLAN モードの対象ポートで，強制認証を許可して割り当てる認証後 VLAN を設定します。

[コマンドによる設定]

1. **(config)# interface fastethernet 0/5**
   (config-if)# mac-authentication force-authorized vlan 200
   (config-if)# exit
   ポート 0/5 で，強制認証を許可して割り当てる認証後 VLAN の VLAN ID を設定します。

[注意事項]

コンフィグレーションコマンド vlan で mac-based 設定（MAC VLAN 設定）している VLAN ID を設定してください。

(4) 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]

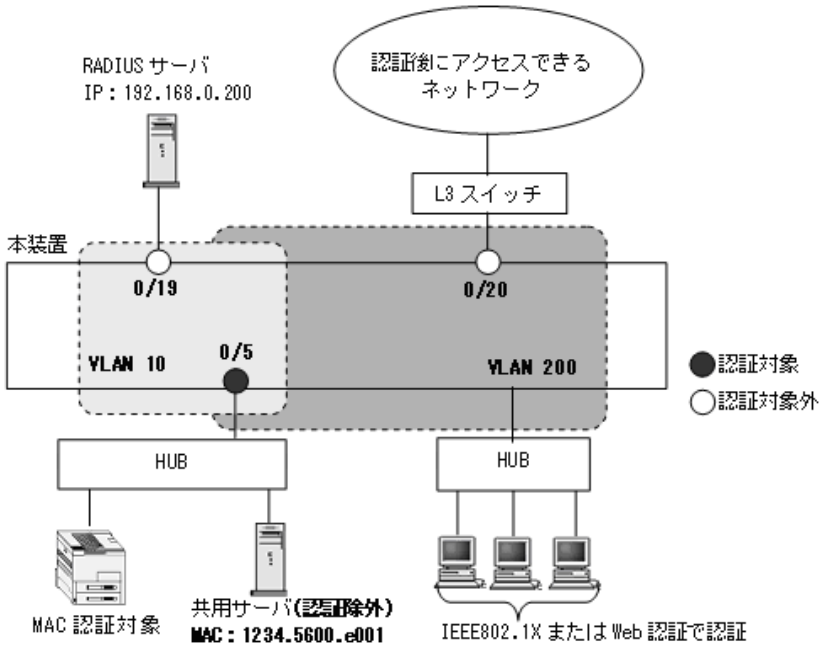
ローミングの動作可能な条件は下記のとおりです。

- 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
- 移動前の認証後 VLAN が，移動後ポートのコンフィグレーションコマンド switchport mac vlan に設定されていること

(5) 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 0/19，0/20，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 fastethernet 0/19**
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 10

(config-if)# exit

VLAN ID 10 のポート 0/19 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 fastethernet 0/20**
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 200
   (config-if)# exit
   MAC VLAN ID 200 のポート 0/20 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。

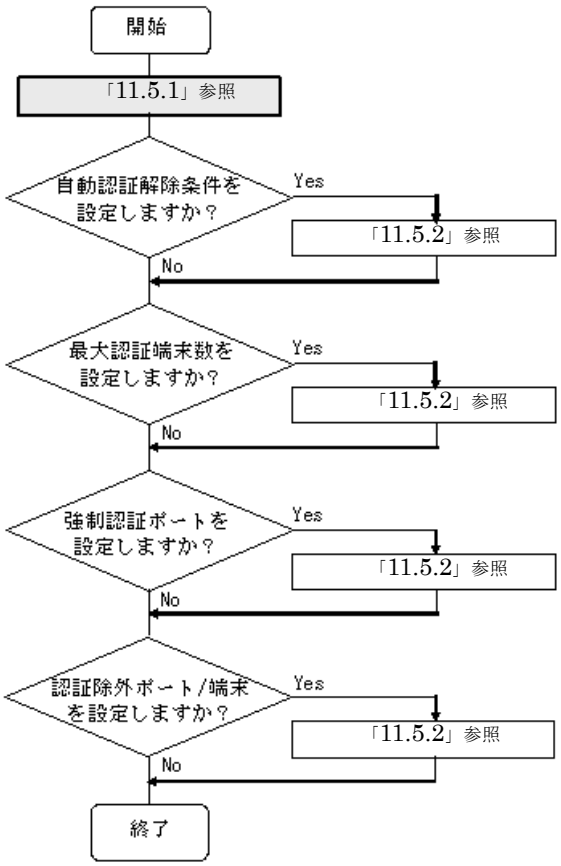
[コマンドによる設定]

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)# mac-address-table static 1234.5600.e001 vlan 200 interface fastethernet 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。

11.5 レガシー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レガシーモードのコンフィグレーションを設定してください。

図 11-9 レガシーモードの設定手順

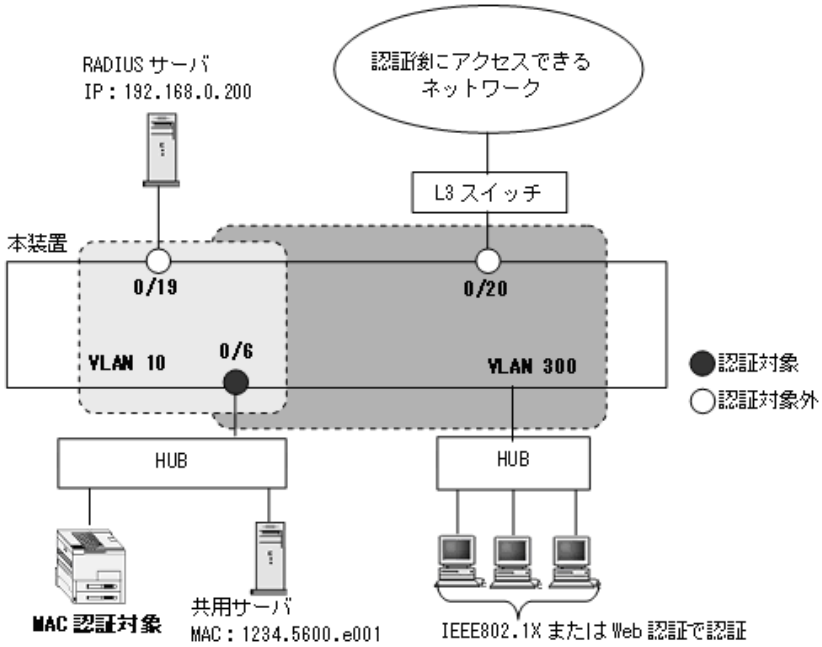


各設定の詳細は，下記を参照してください。

1. 認証ポートの設定：「11.5.1 認証ポートの設定」
2. 自動認証解除の設定：「11.5.2 認証処理に関する設定（1）自動認証解除条件の設定」
3. 最大認証端末数の設定：「11.5.2 認証処理に関する設定（2）最大認証端末数の設定」
4. 強制認証ポートの設定：「11.5.2 認証処理に関する設定（3）強制認証ポートの設定」
5. 認証除外ポート / 端末の設定：「11.5.2 認証処理に関する設定（4）認証除外の設定」

11.5.1 認証ポートの設定

図 11-10 レガシーモードの構成例



(1) レガシーモード対象ポートの設定

[設定のポイント]

レガシーモードで使用するポートを設定します。

[コマンドによる設定]

1. **(config)# mac-authentication interface fastethernet 0/6**

   ポート 0/6 をレガシーモードの対象ポートに設定します。

(2) 対象ポートの認証用 VLAN 情報の設定

[設定のポイント]

レガシーモードで使用するポートに認証用 VLAN 情報を設定します。

[コマンドによる設定]

1. **(config)# vlan 300 mac-based**
   (config-vlan)# exit

   VLAN ID 300 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 fastethernet 0/6**
   (config-if)# switchport mode mac-vlan

```
(config-if)# switchport mac vlan 300
(config-if)# switchport mac native vlan 10
(config-if)# exit
```

認証を行う端末が接続されているポート 0/6 を MAC ポートとして設定し，認証前 VLAN10 と認証後 VLAN300 を設定します。

(3) 認証後 VLAN の設定

[設定のポイント]

レガシーモードで使用する，認証後 VLAN ID を設定します。レガシーモードで認証成功後，本コマンドで設定した VLAN に動的に切り替わります。

[コマンドによる設定]

1. **(config)# mac-authentication vlan 300**
   レガシーモードの認証後 VLAN の VLAN ID を設定します。

[注意事項]

本情報未設定のとき，レガシーモードで認証失敗となりますので，該当 VLAN ID を設定してください。

11.5.2 認証処理に関する設定

レガシー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) MAC アドレスエージングタイムアウト後から自動解除までの猶予時間の設定

[設定のポイント]

レガシーモードで認証済みの端末を，MAC アドレステーブルエージングタイムアウトしてから，自動的に認証解除するまでの猶予時間を設定します。MAC アドレスエージング時間はコンフィグレーションコマンド mac-address-table aging-time の設定時間です。

[コマンドによる設定]

1. **(config)# mac-authentication auto-logout delay-time 60**
   MAC アドレスエージングタイムアウトしてから，自動的に認証解除するまでの猶予時間を 60 秒に設定します。
   本機能は MAC 認証機能を有効にするとデフォルト（delay-time：3600 秒）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。

[注意事項]

1. 自動認証解除の適用時間と，RADIUS サーバ定期問い合わせ（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。
2. 本設定は即時に適用されますが，MAC アドレスエージング監視は 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，既に変更後の猶予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。

(2) 最大認証端末数の設定

ダイナミック VLAN モードと同様です。「11.4.2　認証処理に関する設定（2）最大認証端末数の設定」を参照してください。

(3) 強制認証ポートの設定

[設定のポイント]

レガシーモードの対象ポートで，強制認証を許可して割り当てる認証後 VLAN を設定します。

[コマンドによる設定]

1. **(config)# interface fastethernet 0/6**
   (config-if)# mac-authentication force-authorized vlan 300
   (config-if)# exit
   ポート 0/6 で，強制認証を許可して割り当てる認証後 VLAN の VLAN ID を設定します。

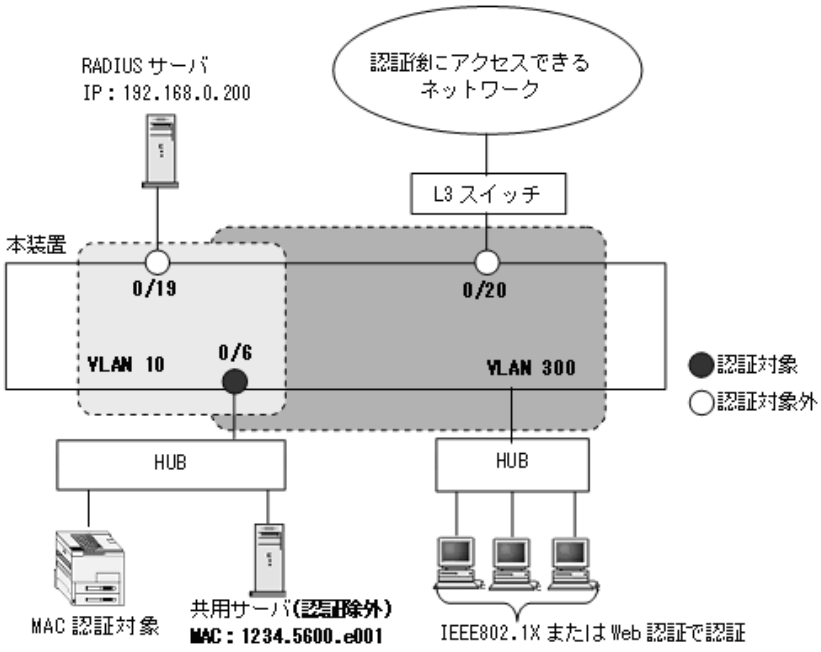
[注意事項]

コンフィグレーションコマンド vlan で mac-based 設定（MAC VLAN 設定）している VLAN ID を設定してください。

(4) 認証除外の設定

レガシー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 0/19，0/20，および共用サーバを認証除外として設定します。

図 11-11　レガシー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ます。

［コマンドによる設定］

1. **(config)# interface fastethernet 0/19**
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 10
   (config-if)# exit
   VLAN ID 10 のポート 0/19 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 fastethernet 0/20**
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 300
   (config-if)# exit
   MAC VLAN ID 300 のポート 0/20 を，アクセスポートとして設定します。

(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 に登録します。

［コマンドによる設定］

1. **(config)# vlan 300 mac-based**
   (config-vlan)# mac-address 1234.5600.e001
   (config-vlan)# exit
   認証を除外する端末の MAC アドレス（図内の共用サーバの MAC アドレス：1234.5600.e001）を，MAC VLAN ID 300 に設定します。

11.6　MAC 認証のオペレーション

11.6.1　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。
show mac-authentication auth-state	MAC 認証の認証状態を表示します。
show mac-authentication auth-state 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 auth-state summary	認証済み端末数を表示します。
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。 （運用コマンド show mac-authentication auth-state と表示内容は同一です。）
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。 （運用コマンド show mac-authentication auth-state select-option と表示内容は同一です。）
show mac-authentication login summary	認証済み端末数を表示します。 （運用コマンド show mac-authentication auth-state summary と表示内容は同一です。）
show mac-authentication logging	認証済のアカウントログを表示します。
clear mac-authentication logging	認証済のアカウントログをクリアします。
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。

11.6.2 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 11-12　内蔵 MAC 認証 DB の設定状態表示

```
# show mac-authentication mac-address edit

Date 2008/06/19 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.
#
```

11.6.3 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

内蔵 MAC 認証 DB から運用コマンド load mac-authentication でバックアップファイル（次の例では backupfile）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.
#
```

11.6.4 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 11-13 MAC 認証の設定状態表示

```
# show mac-authentication

Date 2008/06/19 16:15:39 UTC
<<<MAC-Authentication mode status>>>
  Dynamic-VLAN     : Enable
  Static-VLAN      : Enable

<<<System configuration>>>
 * Authentication parameter
  Authentic-mode   : Dynamic-VLAN
  Authentic-method : RADIUS
  max-user         : 256
  id-format type   : xx-xx-xx-xx-xx-xx
  password         : Disable
  vlan-check       : -
  roaming          : Disable
  mac-authentication vlan : 4,40

 * Logout parameter
  max-timer        : infinity
  auto-logout      : 3600
  quiet-period     : 300
  reauth-period    : 3600

 * Logging status
  [Radius account] : -
  [Syslog send]    : Disable
  [Traps]          : Disable

<Port configuration>
  Port Count       : 2
  Function per port:
    Port  max-user  force-auth    arp-relay  ip access-group
  L 0/2        256  Enable(   4)  -          -
    0/4        256  Disable       Enable     mac-auth
  VLANs per port   :
    Port  VLAN ID
    0/2   4
    0/4   40

<<<System configuration>>>
 * Authentication parameter
  Authentic-mode   : Static-VLAN
  Authentic-method : RADIUS
  max-user         : 1024
  id-format type   : xx-xx-xx-xx-xx-xx
  password         : Disable
  vlan-check       : Disable
  roaming          : Disable
  mac-authentication vlan : -

 * Logout parameter
  max-timer        : infinity
  auto-logout      : 3600
  quiet-period     : 300
  reauth-period    : -

 * Logging status
  [Radius account] : -
  [Syslog send]    : Disable
  [Traps]          : Disable

<Port configuration>
  Port Count       : 1
  Function per port:
    Port  max-user  force-auth    arp-relay  ip access-group
    0/8       1024  Enable        Enable     mac-auth
  VLANs per port   :
    Port  VLAN ID
    0/8   4000

#
```

11.6.5 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 11-14 MAC 認証の表示

```
# show mac-authentication statistics

Date 2007/03/09 12:11:13 UTC
MAC-Authentication Information:
  Authentication Request Total :         39
  Authentication Success Total :          2
  Authentication Fail Total    :         37
  Authentication Refuse Total  :          0
  Authentication Current Count :          2
  Authentication Current Fail  :          0

RADIUS MAC-Authentication Information:
[RADIUS frames]
  TxTotal   :        48  TxAccReq  :        13  TxError   :        35
  RxTotal   :         2  RxAccAccpt:         2  RxAccRejct:         0
                         RxAccchllg:         0  RxInvalid :         0

#
```

11.6.6 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 auth-state で MAC 認証の認証状態を表示します。

また，運用コマンド show mac-authentication login でも同じ内容を表示します。

図 11-15 MAC 認証の認証状態表示

```
# show mac-authentication auth-state

Date 2008/06/19 16:19:03 UTC
 Dynamic VLAN mode total client counts(Login/Max):   3 / 256
  Authenticating client counts :    1
  Hold down client counts      :    1
  Port roaming : Disable
   No F MAC address     Port VLAN  Login time            Limit     Reauth
    1   0000.0000.0004  0/4    40  2008/06/19 16:18:48   infinity    3585
    2   0000.0000.0001  0/4    40  2008/06/19 16:18:48   infinity    3585
L   3 * 0000.e227.8bf8  0/2     4  2008/06/19 16:18:48   infinity    3585

 Static VLAN mode total client counts(Login/Max):    1 / 1024
  Authenticating client counts :    1
  Hold down client counts      :    1
  Port roaming : Disable
   No F MAC address     Port VLAN  Login time            Limit
    1 * 0000.e28c.4add  0/8  4000  2008/06/19 16:18:48   infinity

#
```

(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 auth-state 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。

また，運用コマンド show mac-authentication login select-option でも同じ内容を表示します。

図 11-16 ポート指定時の情報表示

```
# show mac-authentication auth-state select-option port 0/4,0/8

Date 2008/06/19 16:24:22 UTC
 Dynamic VLAN mode total client counts(Login/Max):   3 / 256
  Authenticating client counts :    1
  Hold down client counts      :    1
  Port roaming : Disable
   No F MAC address     Port VLAN  Login time            Limit     Reauth
    1   0000.0000.0004  0/4    40  2008/06/19 16:18:48   infinity    3265
    2   0000.0000.0001  0/4    40  2008/06/19 16:18:48   infinity    3265

 Static VLAN mode total client counts(Login/Max):    1 / 1024
  Authenticating client counts :    1
  Hold down client counts      :    1
  Port roaming : Disable
   No F MAC address     Port VLAN  Login time            Limit
    1 * 0000.e28c.4add  0/8  4000  2008/06/19 16:18:48   infinity

#
```

(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 auth-state summary で MAC 認証の認証済み端末数を表示します。

また，運用コマンド show mac-authentication login summary でも同じ内容を表示します。

図 11-17 認証済み端末数の表示

```
# show mac-authentication auth-state summary port

Date 2008/06/19 16:31:35 UTC
 Dynamic VLAN mode total client counts(Login/Max):   3 / 256
  Authenticating client counts :    1
  Hold down client counts      :    1
  Port roaming : Disable
   No  Port  Login /  Max
 L  1  0/2       1 /  256
    2  0/4       2 /  256

 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  0/8       1 / 1024

#
```

12 レイヤ2認証の共通機能と共存使用

本装置では，IEEE802.1X，Web 認証，MAC 認証で共通で使用する機能があります。また，レイヤ 2 認証機能を，装置内および同一ポート内での共存が可能です。この章では本装置のレイヤ 2 認証の共通機能と，共存使用および使用上の注意について説明します。

12.1　レイヤ 2 認証共通の機能

本節では，レイヤ 2 認証共通で使用する機能について説明します。

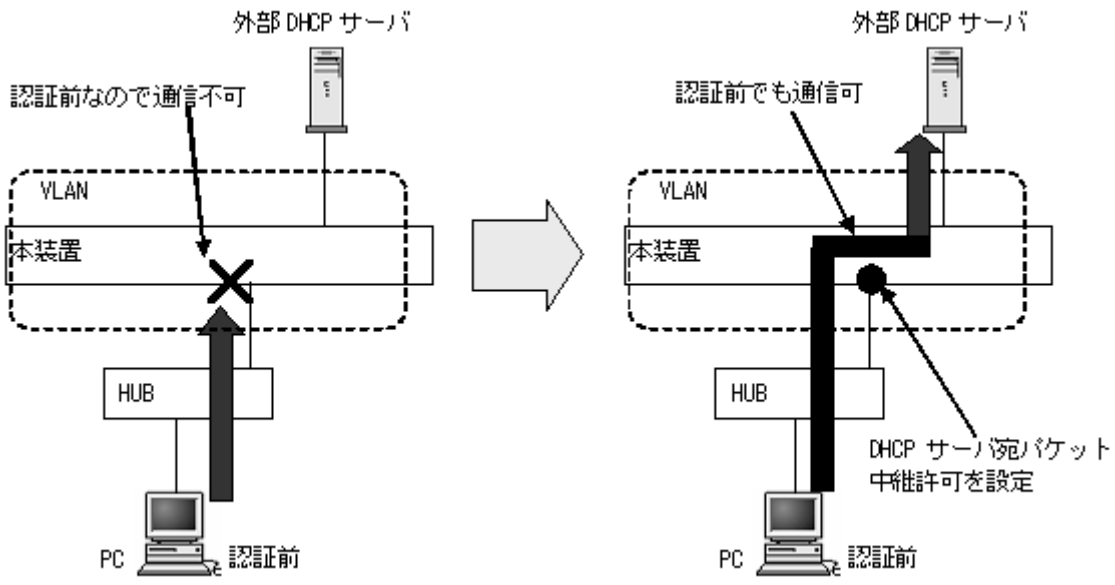
12.1.1　認証専用 IPv4 アクセスリスト

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通過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 12-1　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。

ただし，通常のアクセスリストで設定されたフィルタ条件は，認証専用 IPv4 アクセスリストで設定されたフィルタ条件よりも優先します。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。

なお，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。

- 指定できる IPv4 アクセスリスト名は 1 個だけです。認証対象となるすべてのポートに，コンフィグ

レーションコマンド authentication ip access-group で同一の設定をしてください。
- 設定した条件以外のフレーム廃棄設定は，暗黙に設定されます。
- 認証前の端末から送信される ARP フレームを通過させるため，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。

12.1.2　ダイナミック VLAN モード収容 VLAN の VLAN 名称管理

各認証機能のダイナミック VLAN モードで収容する VLAN の指定を，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。

本機能が利用可能な認証モードを次の表に示します。

表 12-1　VLAN 名称指定が利用可能な認証モード

認証機能	認証モード	本機能の利用可否	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
	VLAN 単位認証 (動的)	○	レガシーモード
Web 認証	固定 VLAN モード	×	
	ダイナミック VLAN モード	○	
	レガシーモード	○	
MAC 認証	固定 VLAN モード	×	
	ダイナミック VLAN モード	○	
	レガシーモード	○	

（凡例）
○：利用可能
×：利用不可

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。

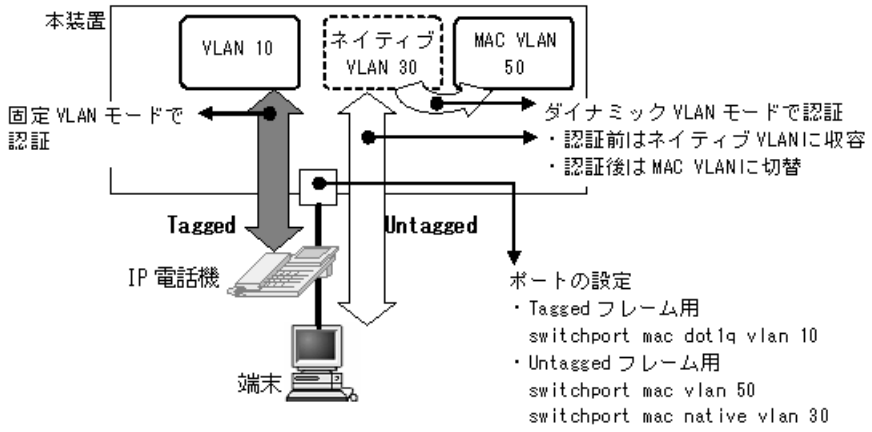
12.1.3　MAC ポートの Tagged フレームの認証（dot1q vlan 設定）

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 12-2　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「12.3.2　同一ポート内で共存　(4) 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。

12.2　レイヤ 2 認証共通の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

本節では，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 12-2　コンフィグレーションコマンドと認証モード一覧

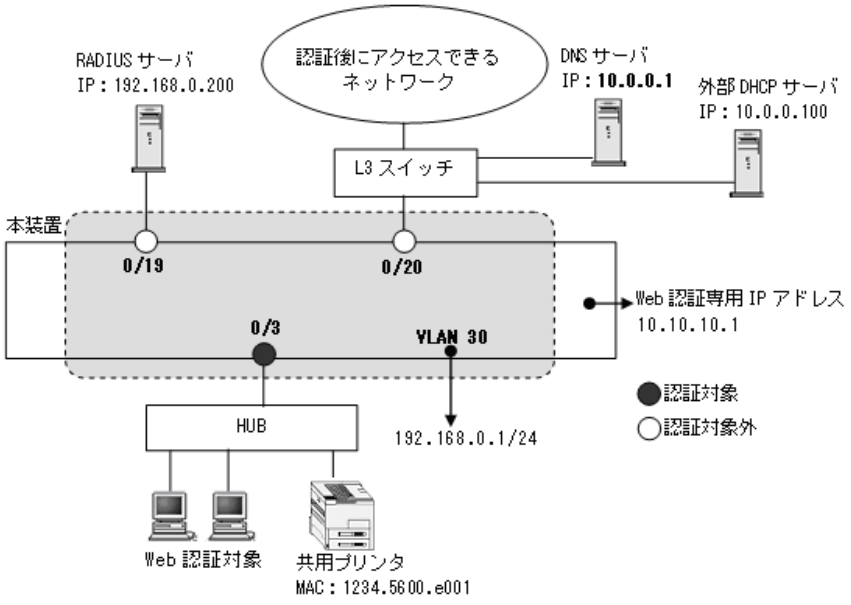
コマンド名	説明	認証モード		
		固	ダ	レ
authentication arp-relay	認証前状態の端末から送信される他機器宛て ARP フレームを，認証対象外のポートへ出力させます。	○	○	×
authentication ip access-group	認証前状態の端末から送信される他機器宛ての IP フレームを，IPv4 アクセスリストを適用して設定されたフレームだけを認証対象外のポートへ出力させます。	○	○	×
name	VLAN に VLAN 名称を設定します。	－	○	○

（凡例）
固：固定 VLAN モード
ダ：ダイナミック VLAN モード
レ：レガシーモード
○：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
－：「12.1.2　ダイナミック VLAN モード収容 VLAN の VLAN 名称管理」の対象外です

12.2.2　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 12-3　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 フレームの通過を設定します。
（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，本例では認証前通過用の設定だけを記載しています。）
本例ではフィルタと拡張認証機能を割り当てます。

［コマンドによる設定］

1. **(config)# ip access-list extended L2-auth**
   (config-ext-nacl)# permit udp src 0.0.0.0 255.255.255.255 dst 0.0.0.0 255.255.255.255 eq bootps
   (config-ext-nacl)# permit protocol ip src 0.0.0.0 255.255.255.255 dst 10.0.0.1 0.0.0.0
   (config-ext-nacl)# exit
   (config)# interface fastethernet 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通過させるように設定します。

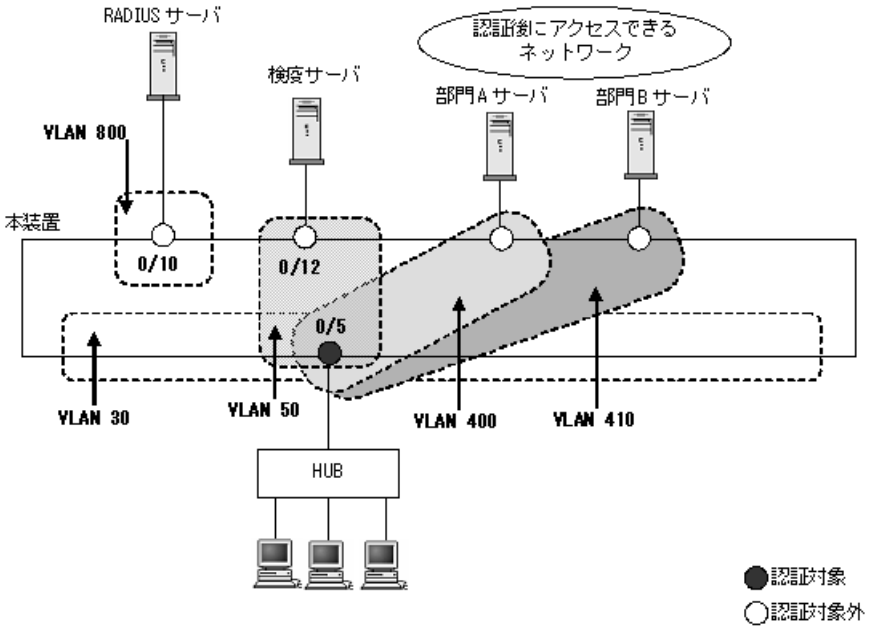
［注意事項］

1. 認証専用 IPv4 アクセスリストの使用には，システムファンクションリソースの設定が必要です。「5.1.4　レイヤ 2 認証機能使用時の注意事項」を参照してください。
2. ポートに認証専用 IPv4 アクセスリストおよび ARP フレーム通過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
3. 認証専用 IPv4 アクセスリストおよび ARP フレーム通過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

12.2.3　ダイナミック VLAN モード収容 VLAN の VLAN 名称指定

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 12-4　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 fastethernet 0/5**
   (config-if)# switchport mode mac-vlan
   ポート 0/5 を MAC ポートとして設定します。

6. **(config-if)# switchport mac vlan 50,400,410**
   (config-if)# switchport mac native vlan 30
   MAC ポートで認証対象端末の認証後 VLAN として，VLAN 50，400，410 を設定します。
   また，認証対象端末の認証前 VLAN30 を設定します。

7. **(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。

8. **(config)# interface fastethernet 0/10**
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 800
   (config-if)# exit
   ポート 0/10 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。

9. **(config)# interface fastethernet 0/12**
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 50
   (config-if)# exit
   ポート 0/12 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"

また，レガシーモードの場合は，[コマンドによる設定] 項 7 の認証モードの設定のかわりに下記を設定してください。

- **(config)# web-authentication vlan 50**
  (config)# web-authentication vlan 400
  (config)# web-authentication vlan 410
  レガシーモードの認証後 VLAN の VLAN ID 50，400，410 を設定します。

［注意事項］

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。

1. 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。
2. 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。

12.3　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」「レガシーモード」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
- VLAN 単位認証（動的）：レガシーモード

12.3.1　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，およびレガシー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 12-5　共存使用例と動作可否

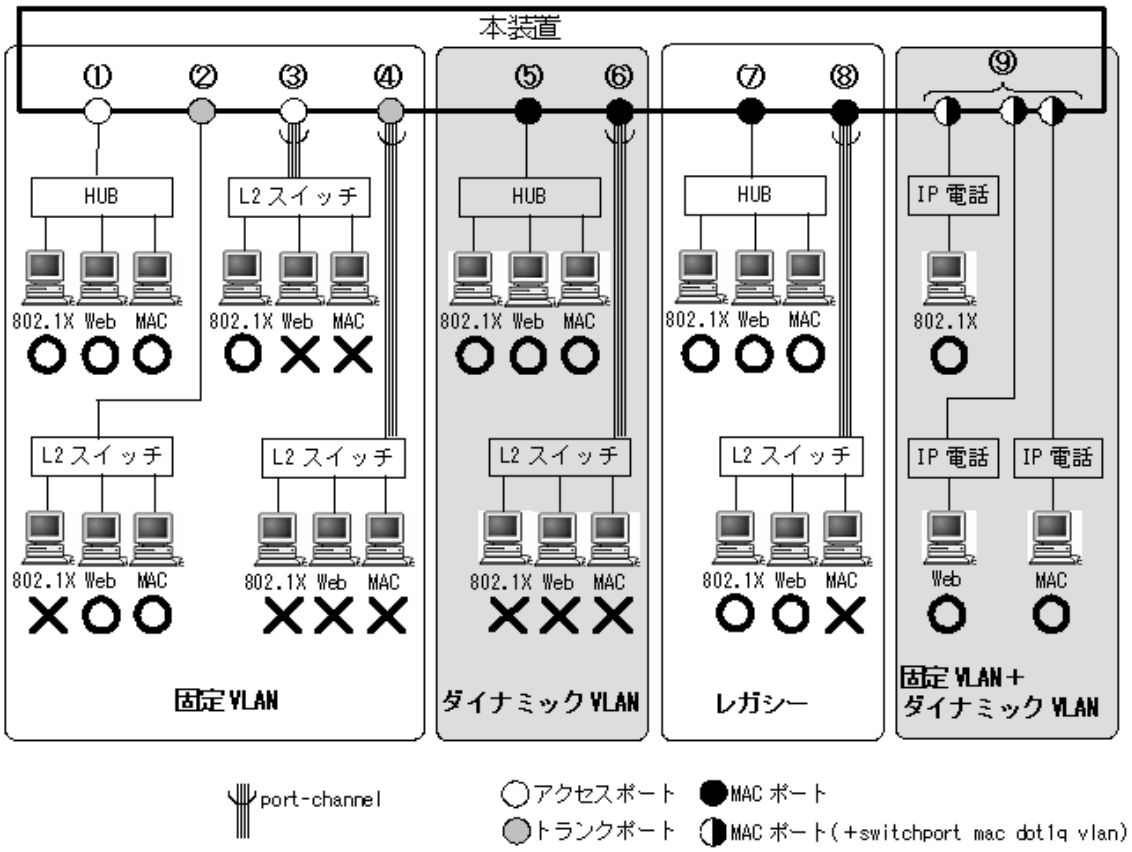


表 12-3　認証モードとポートの種類の組み合わせと認証機能の動作可否

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
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	×	○ 固定 VLAN モード	○ 固定 VLAN モード
	③	アクセス （port-channel）	○ ポート単位認証 （静的）	×	×
	④	トランク （port-channel）	×	×	×
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）	×	×	×
レガシー	⑦	MAC	○ VLAN 単位認証 （動的）	○ レガシーモード	○ レガシーモード
	⑧	MAC （port-channel）	○ VLAN 単位認証 （動的）	○ レガシーモード	×
固定 VLAN ＋ ダイナミック VLAN	⑨	MAC※ （Tagged）	×	○ 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※
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。
この設定の MAC ポートでは，レガシーモードは動作しません。

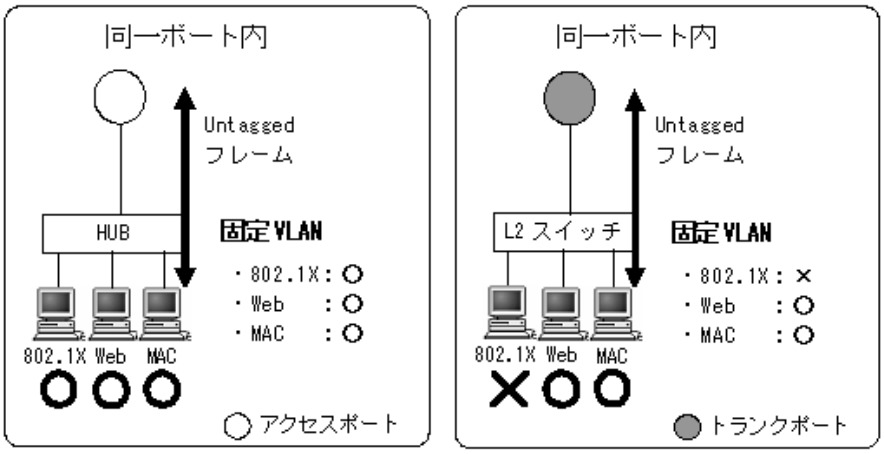
12.3.2　同一ポート内で共存

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
- レガシーモードの共存
- 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 12-6　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 12-6　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（アクセスポート，トランクポート）によって，動作可能な認証機能が異なります。またコンフィグレーションの設定内容によっても動作可能な認証機能が異なります。

「表 12-4　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 12-4　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 12-5　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。

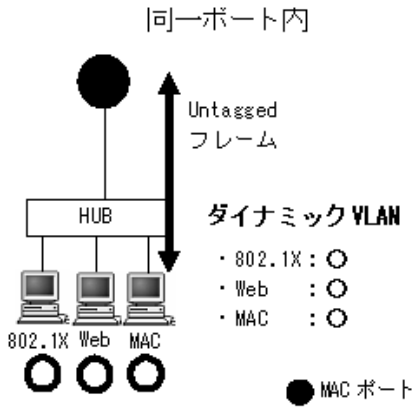
表 12-5　トランクポートでの設定内容における認証機能の動作可否

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 web-authentication port mac-authentication port	×	○	○
	web-authentication port mac-authentication port	×	○	○
	dot1x port-control auto mac-authentication port	×	×	○
	dot1x port-control auto web-authentication port	×	○	×

（凡例）
　○：動作可
　×：動作不可

（2）同一ポートでダイナミック VLAN モードの共存

図 12-7　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 12-7　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は可能です。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 12-6　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 12-6　MAC ポートでの設定内容における認証機能の動作可否

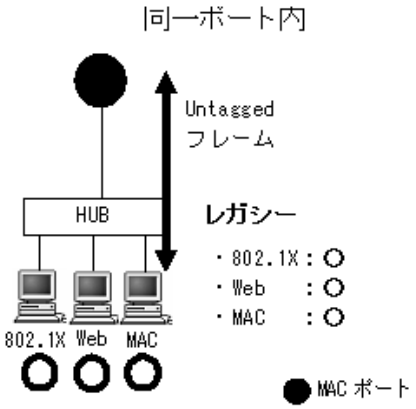
コンフィグレーションの設定内容		認証機能		
共通の設定	認証機能の設定	IEEE802.1X	Web 認証	MAC 認証
switchport mode mac-vlan switchport mac vlan	dot1x port-control auto dot1x multiple-authentication ※ web-authentication port mac-authentication port	○	○	○
	web-authentication port mac-authentication port	×	○	○
	dot1x port-control auto dot1x 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。

（3） 同一ポートでレガシーモードの共存

図 12-8　同一ポート内レガシーモードの共存例



同一ポートでレガシーモードの共存を使用するときには，「図 12-8　同一ポート内レガシーモードの共存例」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は可能です。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 12-7　MAC ポートでの設定内容におけるレガシーモードでの認証機能の動作可否」に示します。

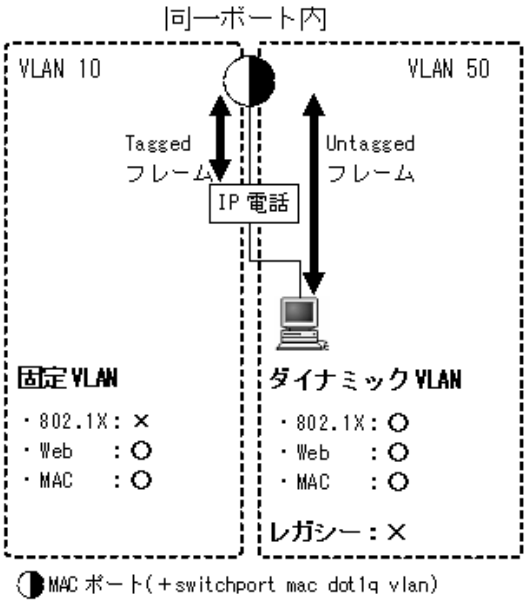
表 12-7　MAC ポートでの設定内容におけるレガシーモードでの認証機能の動作可否

コンフィグレーションの設定内容		認証機能		
インタフェースでの設定	グローバルコンフィグレーションモードでの設定	IEEE802.1X	Web 認証	MAC 認証
switchport mode mac-vlan switchport mac vlan	aaa authorization network default dot1x vlan dynamic enable dot1x vlan dynamic vlan web-authentication vlan mac-authentication vlan	○	○	○
switchport mode mac-vlan switchport mac vlan dot1x port-control auto	aaa authorization network default dot1x vlan dynamic enable dot1x vlan dynamic vlan web-authentication vlan mac-authentication vlan	△	×	×
switchport mode mac-vlan switchport mac vlan web-authentication port	aaa authorization network default dot1x vlan dynamic enable dot1x vlan dynamic vlan web-authentication vlan mac-authentication vlan	×	△	×
switchport mode mac-vlan switchport mac vlan mac-authentication port	aaa authorization network default dot1x vlan dynamic enable dot1x vlan dynamic vlan web-authentication vlan mac-authentication vlan	×	×	△

（凡例）
○：動作可
×：動作不可
△：ダイナミック VLAN モードで動作

（4） 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 12-9　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 12-9　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，IEEE802.1X は固定 VLAN モードでは使用することはできません。またコンフィグレーションの設定内容によっても動作可能な認証機能が異なります。

詳細は「表 12-8　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 12-8　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
・switchport mode mac-vlan ・switchport mac vlan 50 ※1 ・switchport mac dot1q vlan 10 ※1	Tagged	×	○※2	○※2
	Untagged	●※3	●※3	●※3

（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

×：動作不可

注※ 1

「図 12-9　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 12-9　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 12-9　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。）

12.4　認証機能共存で使用時の注意事項

12.4.1　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 VLAN 単位（動的），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全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。

12.4.2　他機能との併用

（1） DHCP snooping と併用時

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 246 台）となります。

（2） スパニングツリーを使用する上での注意

（a） IEEE802.1X と使用する場合

IEEE802.1X とスパニングツリーとの共存仕様について次の表に示します。

表 12-9　IEEE802.1X とスパニングツリーの共存仕様

機能名	共存仕様
スパニングツリー	常に Forwarding であるポートで認証が可能です。それ以外のポートでは認証を行わないように設定してください。 常に Forwarding であるポートは次のとおりです。 • PortFast ポート • ルートブリッジのポート
	BPDU の送受信およびスパニングツリーのトポロジー計算は，IEEE802.1X の認証状態に関係なく行われます。

12.5　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。

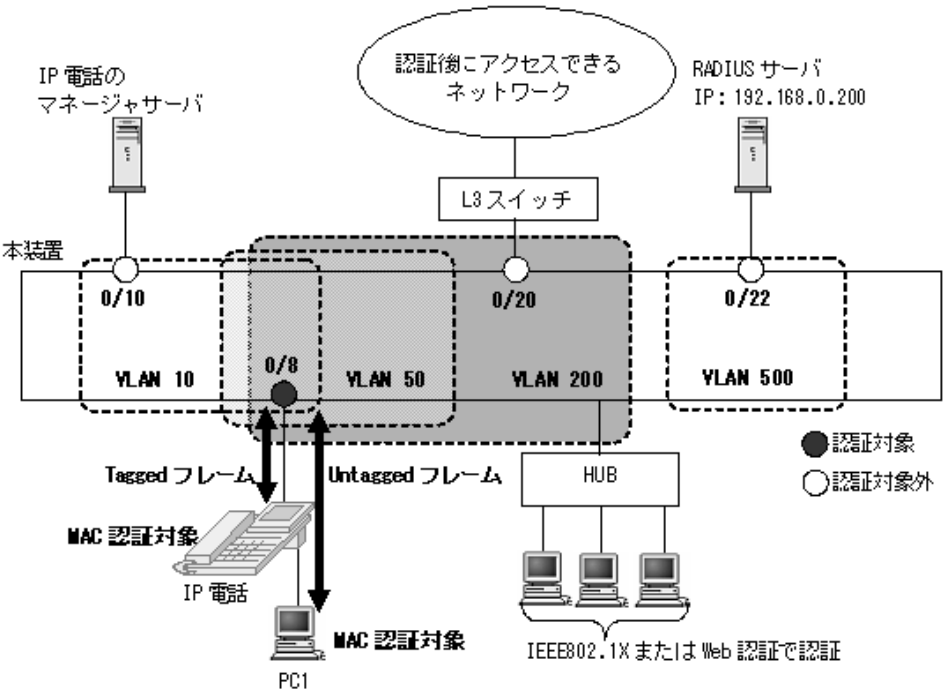
- 同一ポートで固定 VLAN モードとダイナミック VLAN モードを共存
  「12.5.1　MAC ポートで Tagged フレームを認証する設定」を参照してください。

12.5.1　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 12-10　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）

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 fastethernet 0/8**
   (config-if)# switchport mode mac-vlan
   ポート 0/8 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 vlan 200**
   (config-if)# switchport mac native vlan 50
   MAC ポートで Untagged フレームを扱う VLAN および認証対象端末の認証後 VLAN として，VLAN 200 を設定します。
   また，認証対象端末の認証前 VLAN50 を設定します。

6. **(config-if)# mac-authentication port**
   (config-if)# exit
   ポート 0/8 に認証モード（mac-authentication port）を設定します。

7. **(config)# interface fastethernet 0/10**
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 10
   (config-if)# exit
   ポート 0/10 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 fastethernet 0/20**
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 200
   (config-if)# exit
   ポート 0/20 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 fastethernet 0/22**
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 500
   (config-if)# exit
   ポート 0/22 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。

13 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。

13.1　GSRP の概要

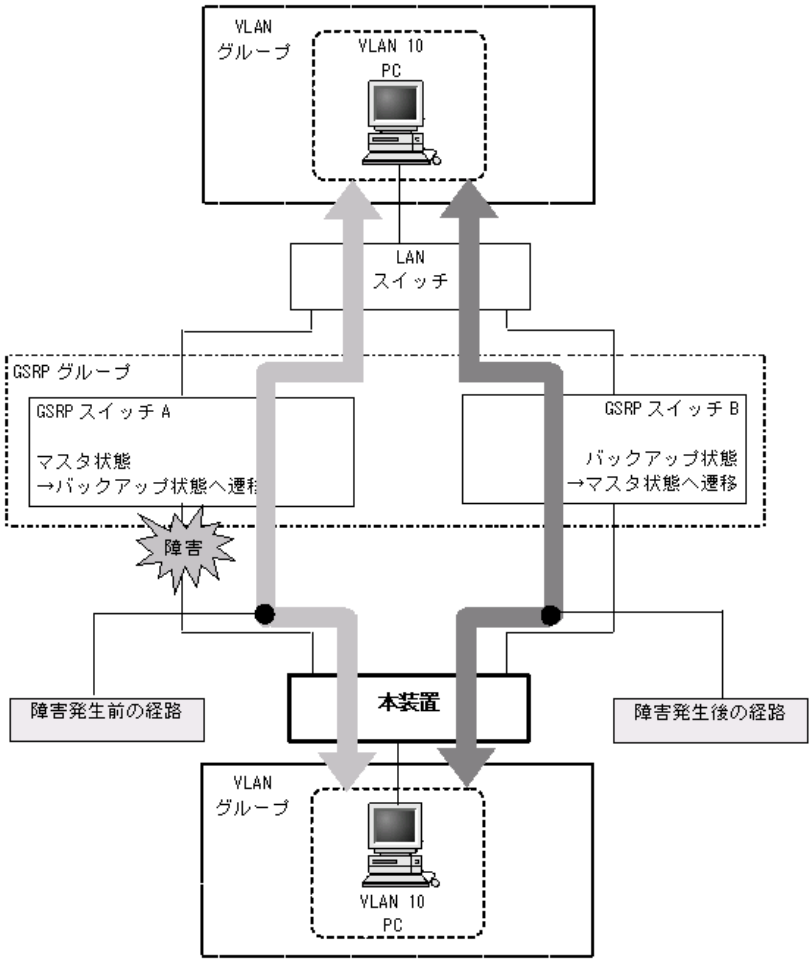
13.1.1　概要

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 13-1　GSRP の概要



13.1.2　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「13.2　GSRP の切り替え制御」を参照してください。

13.2　GSRP の切り替え制御

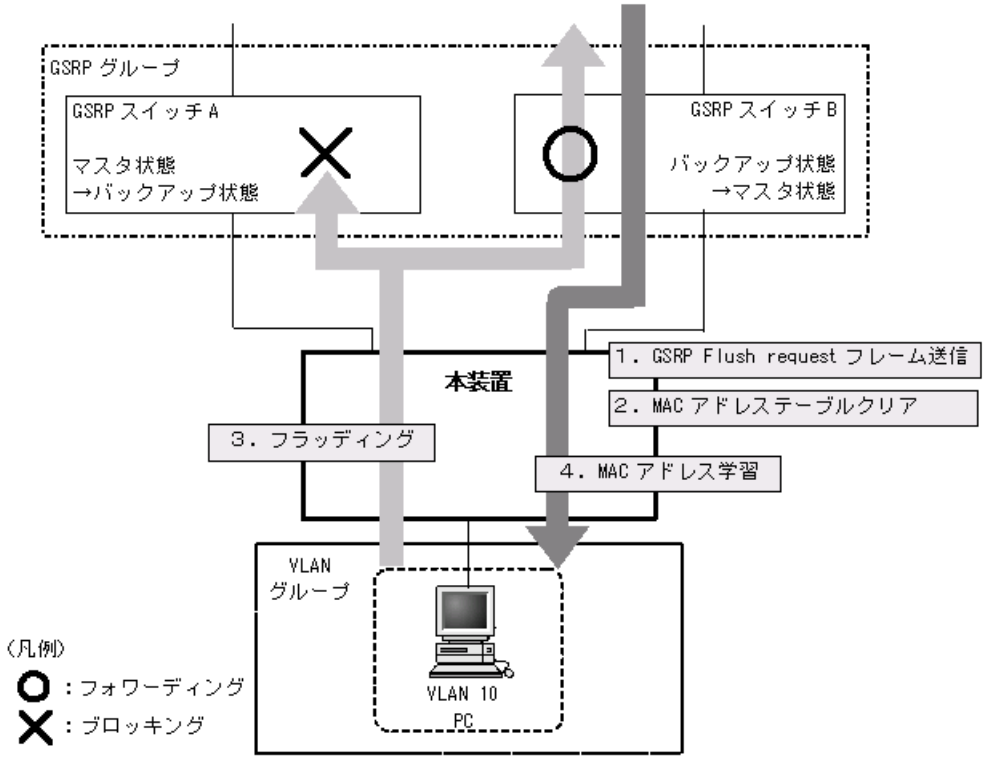
GSRP スイッチで切り替えを行う際，フレームに対するフォワーディングおよびブロッキングの切り替え制御を行うだけでは，エンドーエンド間の通信を即時に再開できません。これは，周囲のスイッチの MAC アドレステーブルにおいて，MAC アドレスエントリが切り替え前にマスタ状態であった GSRP スイッチ向けに登録されたままであるためです。通信を即時に再開するためには，GSRP スイッチの切り替えと同時に，周囲のスイッチの MAC アドレステーブルエントリをクリアする必要があります。

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 13-2　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。

13.2.1 GSRP aware 使用時の注意事項

（1） GSRP Flush request フレームの中継について

GSRP aware は GSRP Flush request フレームをフラッディングします。GSRP aware で GSRP Flush request フレームを中継させるネットワーク構成では，GSRP aware のソフトウェアバージョンを Ver.1.2 以降にする必要があります。

13.3　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。

13.4　オペレーション

13.4.1　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 13-1　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。

13.4.2　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 13-3　show gsrp aware の実行例

```
> show gsrp aware

Date 2006/12/14 11:12:39 UTC
Last mac_address_table Flush Time : 2006/12/14 11:12:26
GSRP Flush Request Parameters :
 GSRP ID : 10      VLAN Group ID : 1   Port : 0/25
 Source MAC Address : 0012.e208.0eea

>
```

14 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。

14.1 解説

14.1.1 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，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。

ストームコントロールの運用コマンドはありません。

14.1.2 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。

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。

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

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 14-1 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を設定できます。

14.2.2 ストームコントロールの設定

● 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，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，ログメッセージの出力を，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。
- ログメッセージの出力

  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，ログメッセージを出力して通知します。ただし，ポートの閉塞時のメッセージは必ず出力します。

［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 fastethernet 0/10**
   (config-if)# storm-control broadcast level pps 50
   ブロードキャストフレームの閾値を 50 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閾値を 500 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閾値を 1000 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。

15 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。

15.1 解説

15.1.1 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。本装置では工場出荷時の設定で 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片方の装置側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。正しく片方向リンク障害を検出させるためには，もう一方の装置側のポートで IEEE802.3ah/OAM 機能が有効である必要があります。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での運用を停止します。

15.1.2 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 15-1 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

15.1.3 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。

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

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 15-2 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。

15.2.2 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。本装置では工場出荷時の設定で 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，fastethernet 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 fastethernet 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。

15.3 オペレーション

15.3.1 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 15-3 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。

15.3.2 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 15-1 show efmoam の実行結果

```
> show efmoam

Date 2006/12/13 23:59:59 UTC
Port   Status              Dest MAC
0/1    Forced Down (UDLD)  0012.e298.dc20
0/2    Mutually Seen       unknown
0/3    Partner Seen        unknown
     :
     :
>
```

図 15-2 show efmoam statistics の実行結果

```
> show efmoam statistics

Date 2006/12/13 23:59:59 UTC
Port 0/1 [Forced Down (UDLD)]
  OAMPDUs:Tx     :        295  Rx         :        295
          Invalid:          0  Unrecogn   :          0
  Expirings      :          0  Thrashings:          0  Blockings:          0
Port 0/2 [Mutually Seen]
  OAMPDUs:Tx     :        100  Rx         :        100
          Invalid:          0  Unrecogn   :          0
  Expirings      :          0  Thrashings:          0  Blockings:          0
Port 0/3 [Partner Seen]
  OAMPDUs:Tx     :        100  Rx         :        100
          Invalid:          0  Unrecogn   :          0
  Expirings      :          0  Thrashings:          0  Blockings:          0
     :
     :
>
```

16 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。

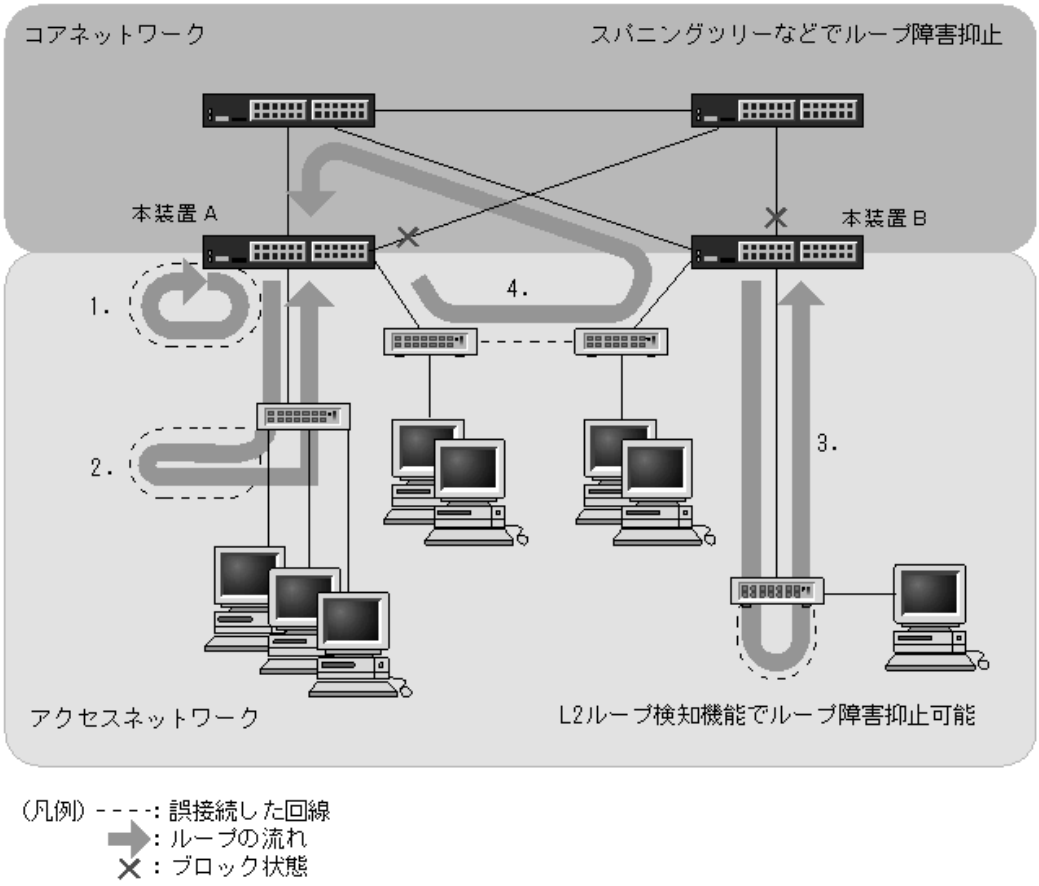
16.1　解説

16.1.1　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 16-1　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。

16.1.2 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 16-1　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 fastethernet
- interface gigabitethernet
- interface port-channel（物理ポート単位ではなく，論理ポート単位で送信します。）

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。

16.1.3 レイヤ 2 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 16-2 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	L2 ループ検知フレームは学習の対象外
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	

機能	項目	装置内共存	ポート共存	共存時の動作
スパニングツリー	IEEE802.1d IEEE802.1w IEEE802.1s PVST+	共存可	共存可※	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	L2 ループ検知フレームはフィルタの対象外
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

注※

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。

16.1.4 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，イベントトレースに採取します。イベントトレースは運用コマンド show even-trace 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。

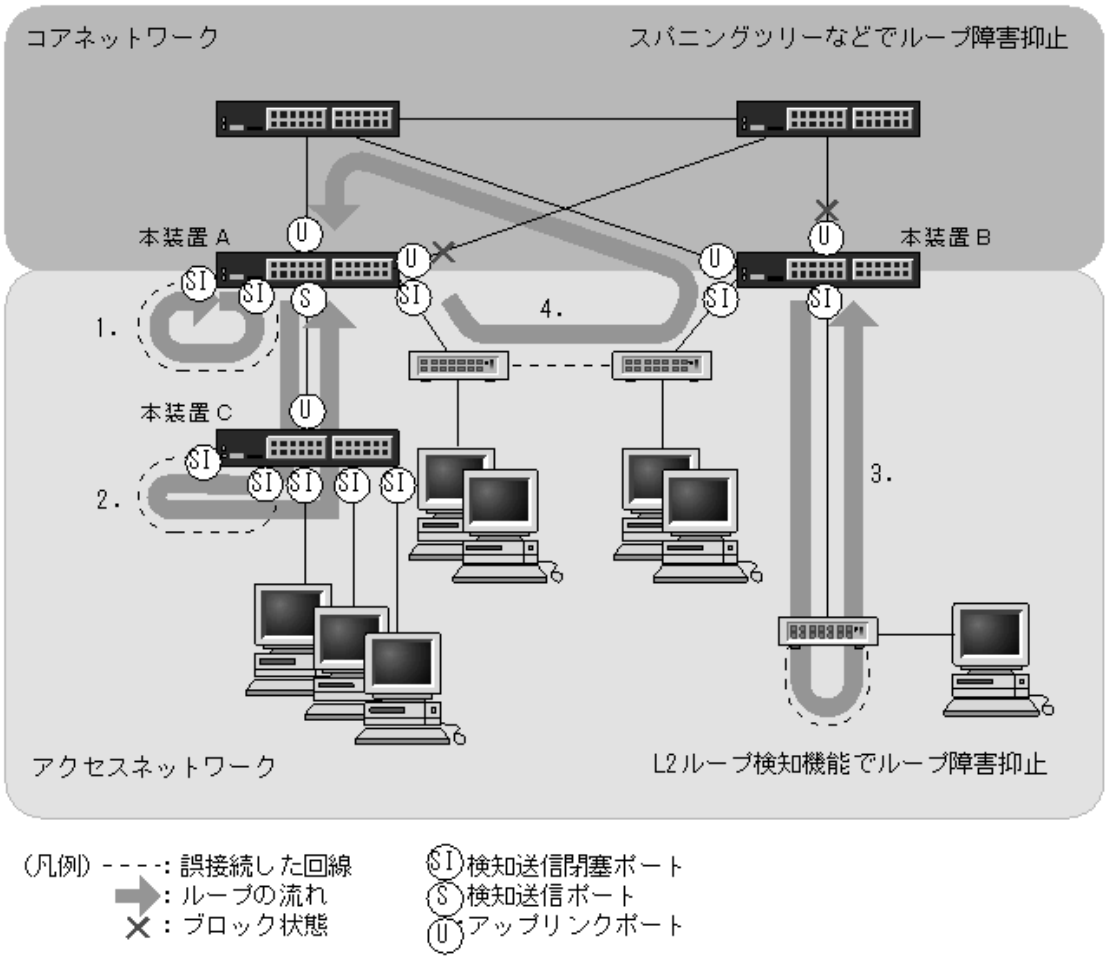
プライベート MIB については，マニュアル「MIB レファレンス」を参照してください。

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。

16.1.5 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 16-2　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。

16.1.6 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

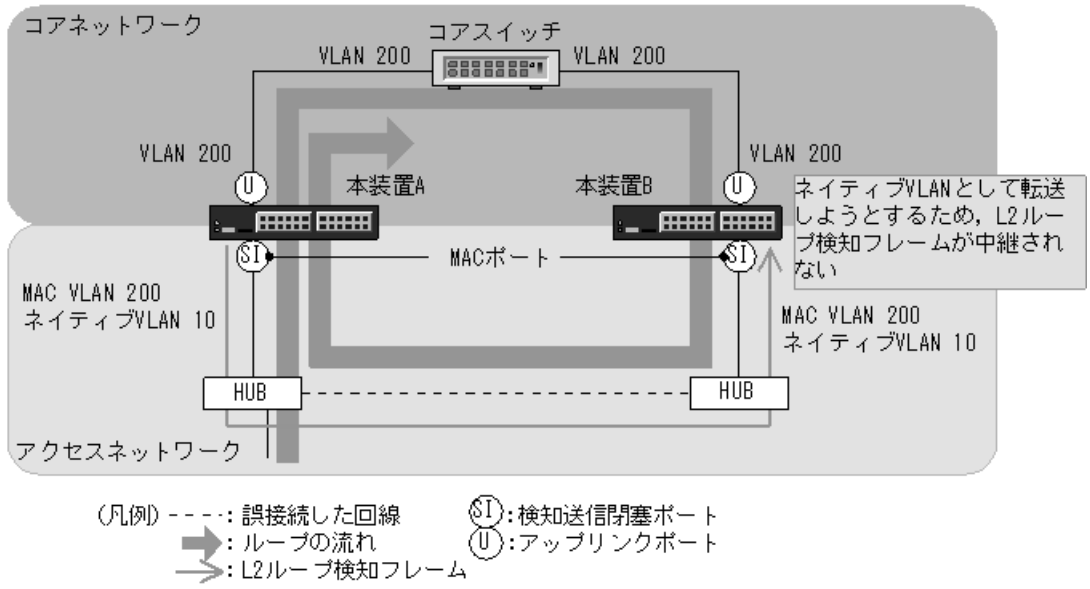
この場合は，アップリンクポートとして設定しているコアネットワーク側のポートを検知送信ポートに設定すると，ループ障害を検知できます。具体的な構成例を次に示します。

(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。

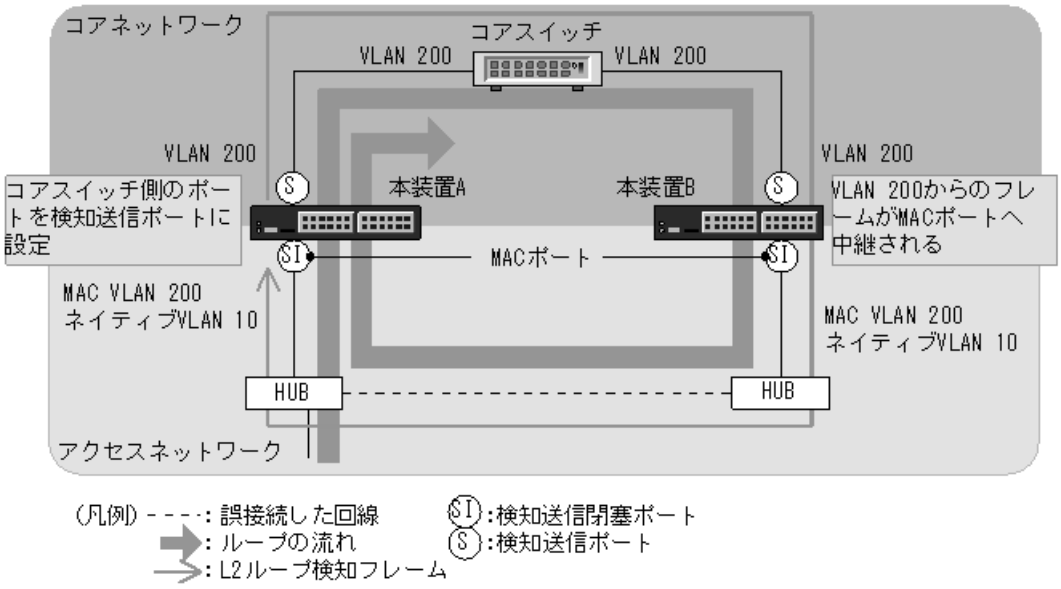
図 16-3 ループ検知の制限となる構成



(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 16-4　ループ検知可能な構成



（2） 他装置で Tag 変換機能使用時の動作について

本装置から送信した L2 ループ検知フレームを，他装置で Tag 変換されて本装置の別の VLAN として受信した場合もループ障害と判断します。

（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。

16.2 コンフィグレーション

16.2.1 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 16-3 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。

16.2.2 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 fastethernet 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 fastethernet 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 0/25**
   (config-if)# loop-detection uplink-port
   (config-if)# exit
   ポート 0/25 をアップリンクポートに設定します。

5. **(config)# interface fastethernet 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。

16.3 オペレーション

16.3.1 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 16-4 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。

16.3.2 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 16-5 運用コマンド show loop-detection の実行結果

```
> show loop-detection

Date 2008/03/21 19:22:37 UTC
Interval Time           :10
Output Rate             :20pps
Threshold               :200
Hold Time               :300
Auto Restore Time       :3600
VLAN Port Counts
    Configuration       :10         Capacity       :200
Port Information
  Port     Status      Type         DetectCnt RestoringTimer  SourcePort  Vlan
  0/1      Up          trap                 0              -  -
  0/2      Up          trap                 0              -  -
  0/3      Up          trap                 0              -  -
  0/4      Down(loop)  send-inact         200           3598  0/6           1
  0/5      Up          exception            0              -  0/7           1
  0/6      Down        send               200              -  0/4           1
  0/7      Up          send-inact           0              -  -
  0/8      Down(loop)  send-inact         200           3598  ChGr:8(U)     1
                   :
                   :
  ChGr:1   Down(loop)  send-inact         200           3598  ChGr:2        1
  ChGr:2   Down(loop)  send-inact         200           3598  ChGr:1        1
  ChGr:8   Down        uplink               -              -  0/8           1

>
```

17 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。

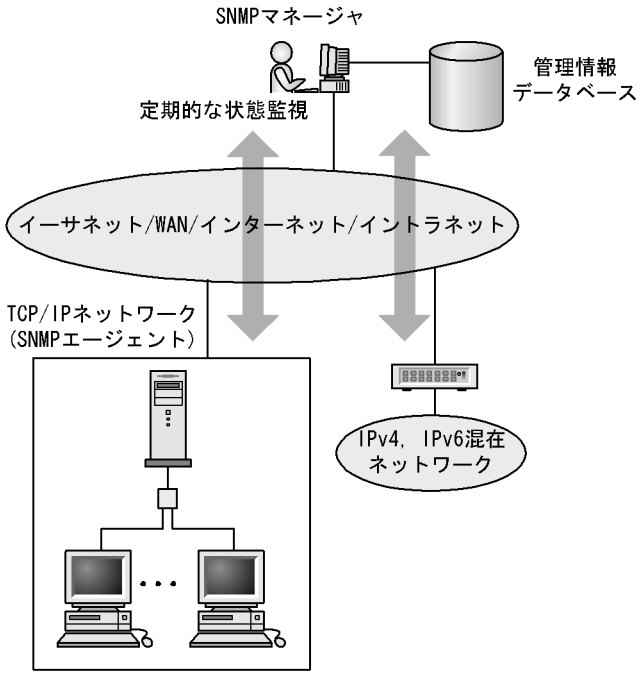
17.1　解説

17.1.1　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。

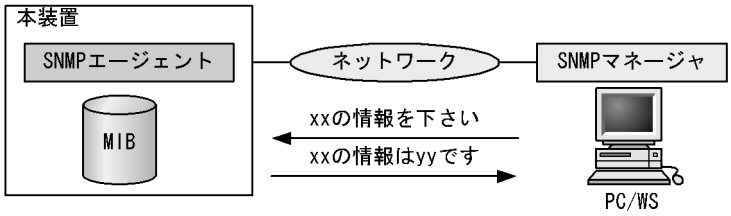
図 17-1　ネットワーク管理の概要



（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。

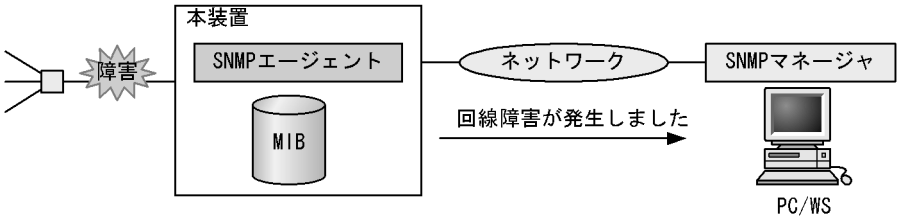
図 17-2　MIB 取得の例



本装置では，SNMPv1（RFC1157），SNMPv2c（RFC1901）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 プロトコルで使用してください。なお，SNMPv1，SNMPv2c 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。トラップの例を次の図に示します。

図 17-3　トラップの例



17.1.2　MIB 概説

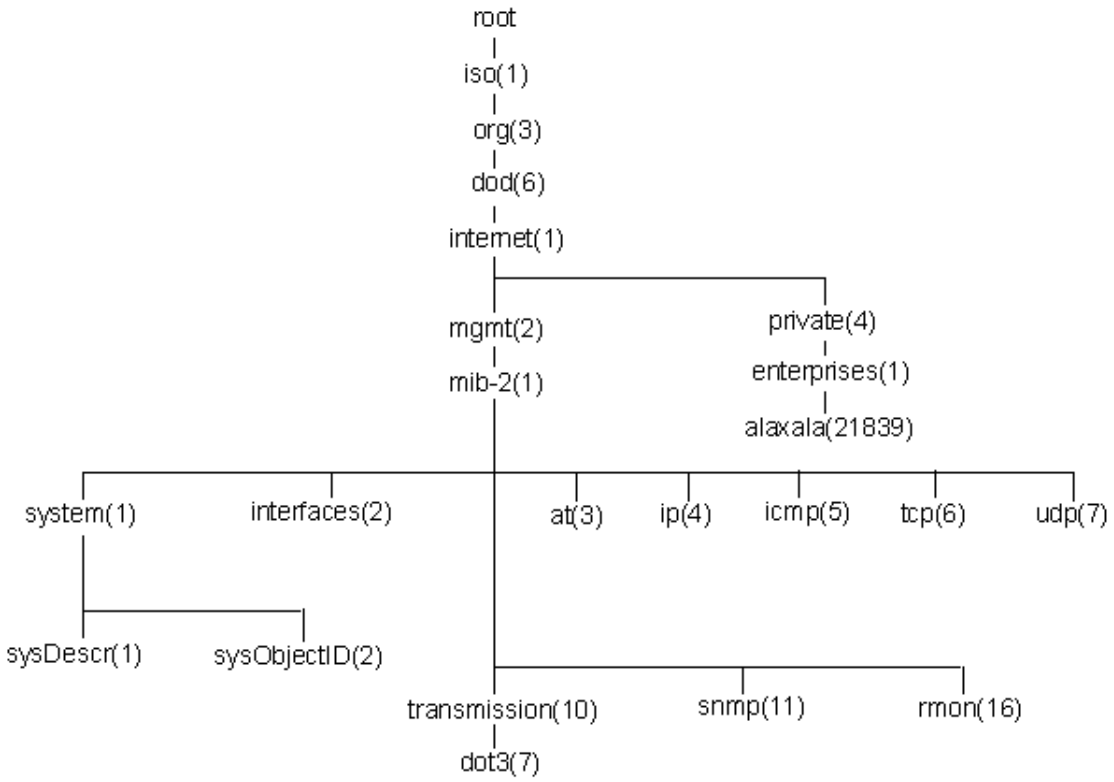
装置が管理し，SNMP マネージャに提供する MIB は，RFC で規定されたものと，装置の開発ベンダーが独自に用意する情報の 2 種類があります。

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 17-4 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。

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。

17.1.3　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。

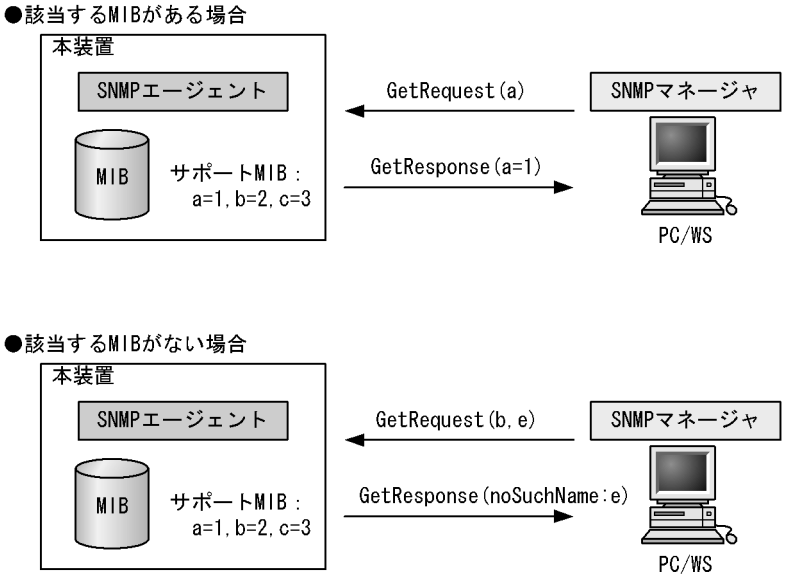
各オペレーションは SNMP マネージャから装置（SNMP エージェント）に対して行われます。各オペレーションについて説明します。

（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。

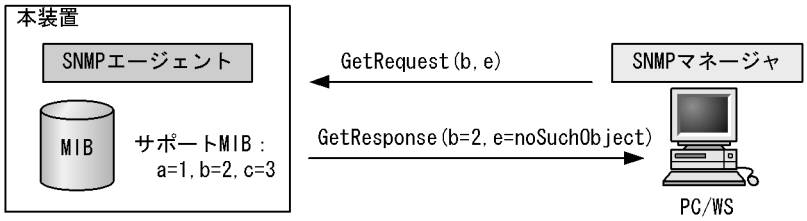
図 17-5　GetRequest オペレーション



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 17-6　GetRequest オペレーション（SNMPv2c）

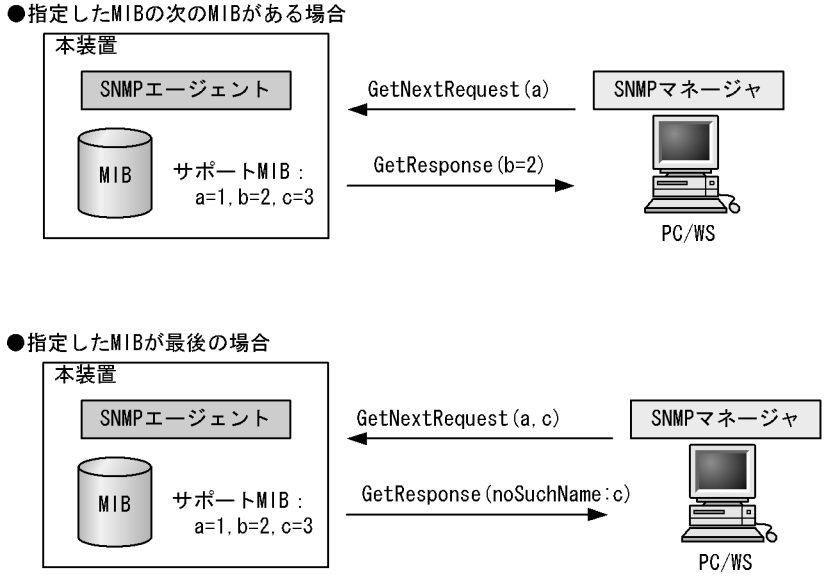


（2） GetNextRequest オペレーション

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。

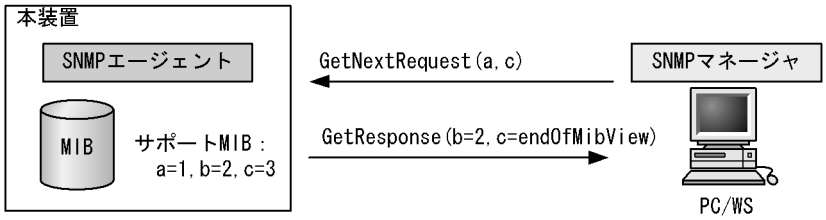
装置が指定した次の MIB を保持している場合は，GetResponse オペレーションで MIB を応答します。指定した MIB が最後の場合は，GetResponse で noSuchName を応答します。GetNextRequest オペレーションを次の図に示します。

図 17-7　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 17-8　GetNextRequest オペレーション（SNMPv2c）

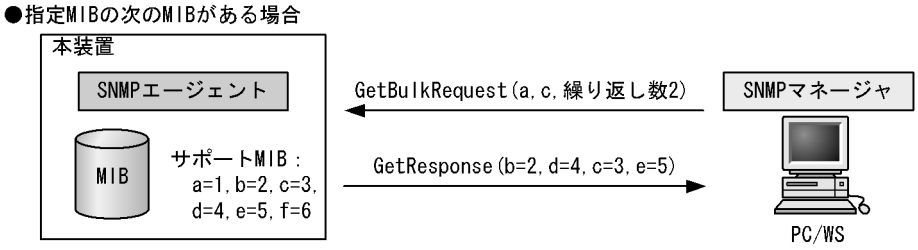


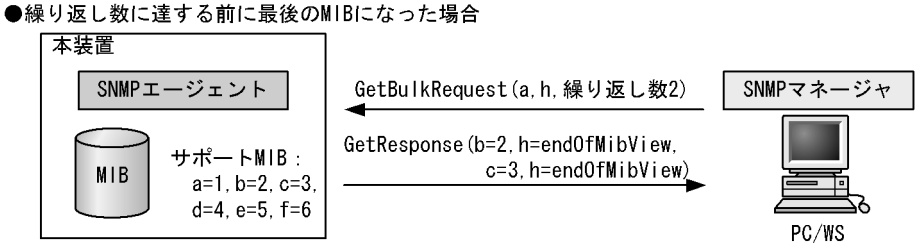
（3） GetBulkRequest オペレーション

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 17-9　GetBulkRequest オペレーション



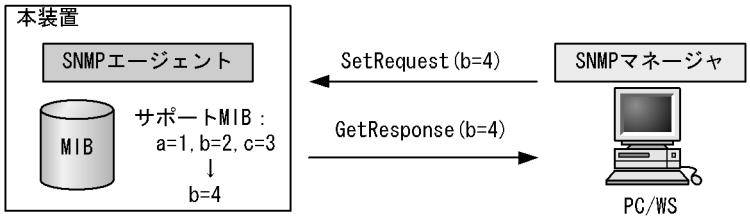


（4） SetRequest オペレーション

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 17-10　SetRequest オペレーション



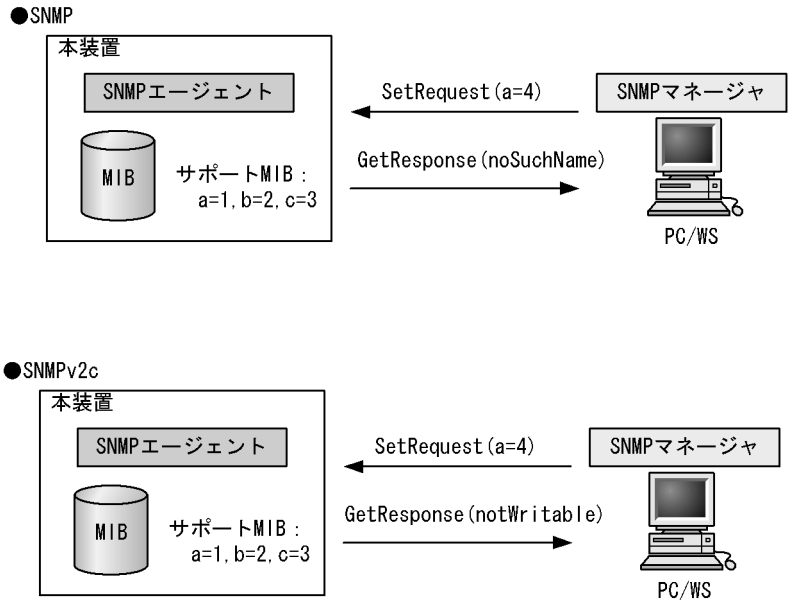
(a) MIB を設定できない場合の応答

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

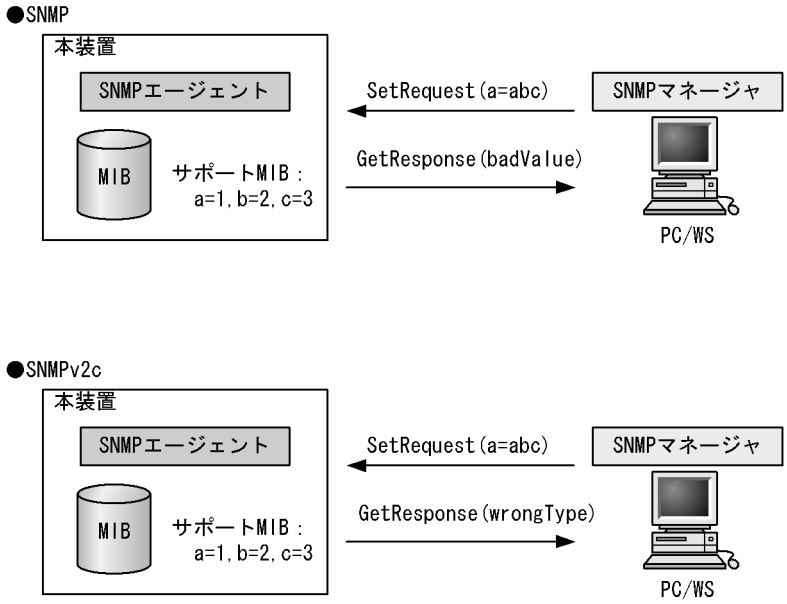
各ケースによって，応答が異なります。MIB が読み出し専用の場合，noSuchName の GetResponse 応答をします。SNMPv2c の場合，MIB が読み出し専用のときは notWritable の GetResponse 応答をします。MIB が読み出し専用の場合の SetRequest オペレーションを次の図に示します。

図 17-11　MIB 変数が読み出し専用の場合の SetRequest オペレーション



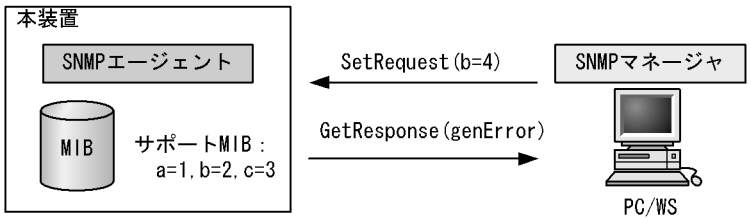
設定値のタイプが正しくない場合，badValue の GetResponse 応答をします。SNMPv2c の場合，設定値のタイプが正しくないときは wrongType の GetResponse 応答をします。設定値のタイプが正しくない場合の SetRequest オペレーションを次の図に示します。

図 17-12　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。

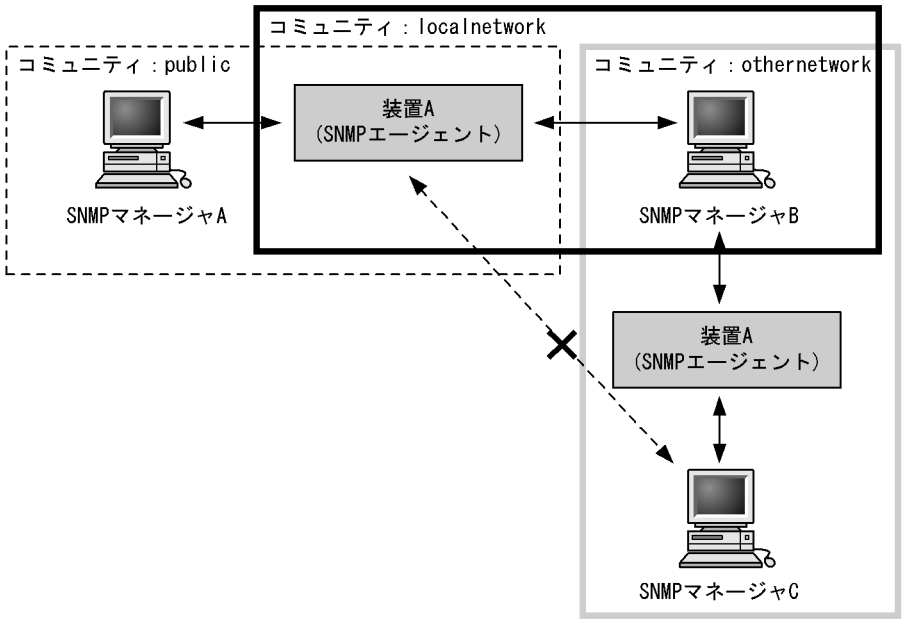
図 17-13　装置の状態によって設定できない場合の SetRequest オペレーション



(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 17-14 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 17-1 エラーステータスコード

エラーステータス	コード	内容
noError	0	エラーはありません。
tooBig	1	データサイズが大きく PDU に値を設定できません。
noSuchName	2	指定 MIB がない，または書き込みできませんでした。
badValue	3	設定値が不正です。
readOnly	4	書き込みできませんでした（本装置では応答することはありません）。
genError	5	その他のエラーが発生しました。

エラーステータス	コード	内容
noAccess	6	アクセスできない MIB に対して set を行おうとしました。
wrongType	7	MIB で必要なタイプと異なるタイプが指定されました。
wrongLength	8	MIB で必要なデータ長と異なる長さが指定されました。
wrongEncoding	9	ASN.1 符号が不正でした。
wrongValue	10	MIB 値が不正でした。
noCreation	11	該当する MIB が存在しません。
inconsistentValue	12	現在何か理由があって値が設定できません。
resourceUnavailable	13	値の設定のためにリソースが必要ですが，リソースが利用できません。
commitFailed	14	値の更新に失敗しました。
undoFailed	15	値の更新に失敗したときに，更新された値を元に戻すのに失敗しました。
notWritable	17	セットできません。
inconsistentName	18	該当する MIB が存在しないため，現在は作成できません。

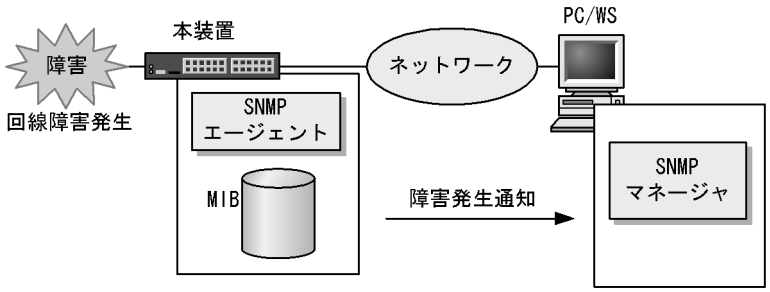
17.1.4　トラップ

（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。トラップの例を次の図に示します。

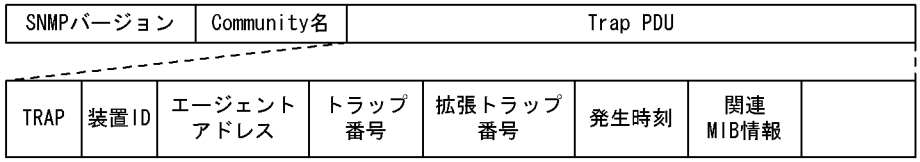
図 17-15　トラップの例



（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 17-16 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

17.1.5 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。

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

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 17-2 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 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 trap link-status	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。

17.2.2 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 src 128.1.1.2 0.0.0.0
   (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。

17.2.3　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

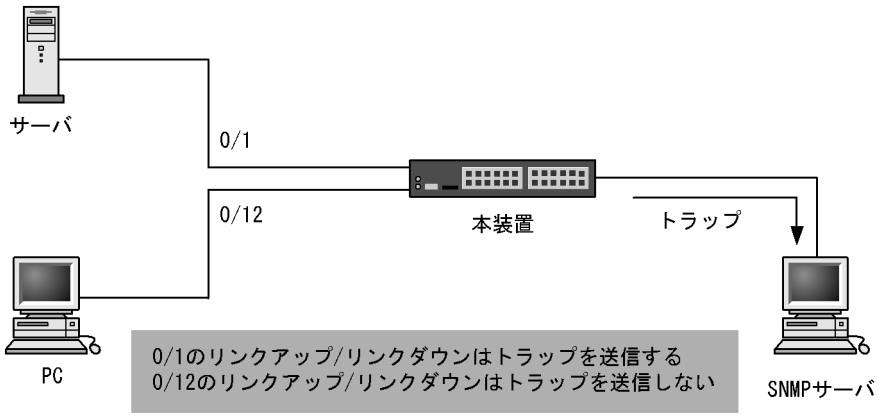
17.2.4　リンクトラップの抑止

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 17-17　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 0/12 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 fastethernet 0/12**
   (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。

17.2.5 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 fastethernet 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"

17.2.6 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.3" 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.3
   - 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

17.2.7　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。

18 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。

18.1 解説

本装置では動作情報や障害情報などをイベントメッセージとして通知します。イベントメッセージは装置内に保存し，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。

イベントメッセージ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。イベントメッセージ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
- 装置が出力する動作情報
- 装置障害ログ情報

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 event-trace で確認できます。また，装置障害ログ情報は，運用コマンド show log 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。

また，運用コマンド trace-monitor で運用端末（コンソール）にイベントトメッセージをモニタ表示することも可能です。モニタ表示については，「コンフィグレーションガイド Vol.1 9　装置の管理」を参照してください。

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 メッセージでは，RFC3164 で定義されている HEADER 部の HOSTNAME および TIMESTAMP 欄は未設定です。

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

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 18-1　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 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。

18.2.2　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。

19 LLDP

この章では，本装置に隣接する装置の情報を収集する機能である LLDP の解説と操作方法について説明します。

19.1 解説

19.1.1 概要

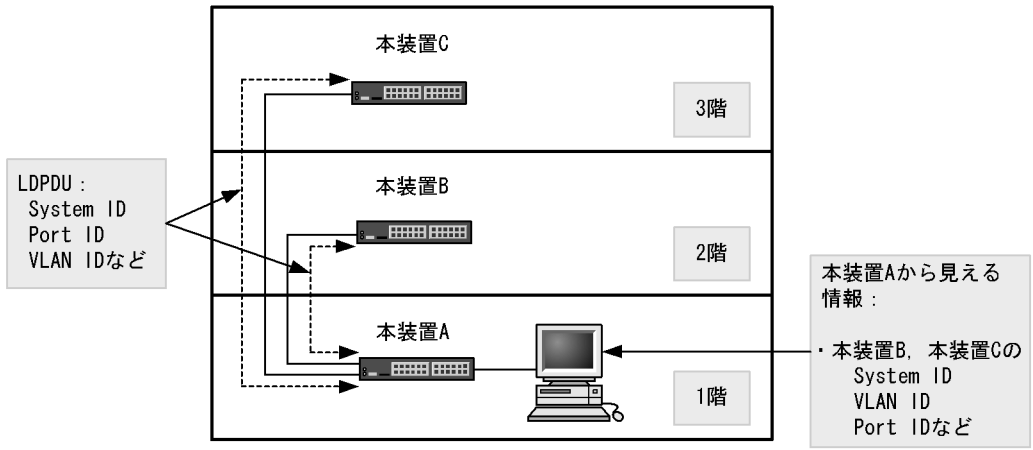
LLDP（Link Layer Discovery Protocol）は隣接する装置情報を収集するプロトコルです。運用・保守時に接続装置の情報を簡単に調査できることを目的とした機能です。

（1） LLDP の適用例

LLDP 機能を使用することで隣接装置と接続している各ポートに対して，本装置に関する情報および該当ポートに関する情報を送信します。該当ポートで受信した隣接装置の情報を管理することで本装置と隣接装置間の接続状態を把握できるようになります。

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本装置間の接続状態を，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 19-1 LLDP の適用例



19.1.2 サポート仕様

この機能を用いて隣接装置に配布する情報は，IEEE 802.1AB Draft 6 をベースに拡張機能として本装置独自の情報をサポートしています。サポートする情報を次の表に示します。

表 19-1 LLDP でサポートする情報

項番		名称	説明
1		End Of LDPDU	LDPDU の終端識別子
2		Time-to-Live	情報の保持時間
3		Chassis ID	装置の識別子
4		Port ID	ポート識別子
5		Port description	ポート種別
6		System name	装置名称
7		System description	装置種別
8	—	Organizationally-defined TLV extensions	ベンダー・組織が独自に定めた TLV

項番		名称	説明
	a	VLAN ID	設定されている VLAN ID
	b	VLAN Address	VLAN に関連づけられた IP アドレス

（凡例） －：該当なし

LLDP でサポートする情報の詳細を以下に示します。

なお，MIB についてはマニュアル「MIB レファレンス」を参照してください。

（1） 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。

（2） 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 19-2 Chassis Id の subtype 一覧

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	MAC address	LLDP MIB の macAddress と同じ値
6	Network address	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：subtype ＝ 5 だけ送信します。送信する MAC アドレスは装置 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：255byte

（3） 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 19-3 Port ID の subtype 一覧

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 macAddr と同じ値

subtype	種別	送信内容
5	Network address	LLDP MIB の networkAddr 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：subtype ＝ 4 だけ送信します。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：255Byte

（4） Port description（ポート種別）

ポートの種別を示す情報です。この情報には subtype はありません。

送信内容および受信条件は次のとおりです。

- 送信内容：「Interface MIB の ifDescr と同じ値」
- 受信データ最大長：255Byte

（5） System name（装置名称）

装置名称を示す情報です。この情報には subtype はありません。

送信内容および受信条件は次のとおりです。

- 送信内容：「systemMIB の sysName と同じ値」
- 受信データ最大長：255Byte

（6） System description（装置種別）

装置の種別を示す情報です。この情報には subtype はありません。

送信内容および受信条件は次のとおりです。

- 送信内容：「systemMIB の sysDescr と同じ値」
- 受信データ最大長：255Byte

（7） Organizationally-defined TLV extensions

本装置独自に以下の情報をサポートしています。

（a） VLAN ID

該当ポートが使用する VLAN Tag 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。

（b） VLAN Address

この情報は，IP アドレスが設定されている VLAN があれば，その VLAN ID とその IP アドレスを一つ示します。

19.1.3 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） IEEE 802.1AB 規格との接続について

本装置の LLDP は IEEE 802.1AB Draft 6 をベースにサポートした独自機能です。IEEE 802.1AB 規格との接続性はありません。

（4） 隣接装置の最大数について

装置当たり最大 50 の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。

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

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 19-4 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 run	装置全体で LLDP 機能を有効にします。

19.2.2 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，fastethernet 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 fastethernet 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 フレームの送信間隔を変更すると，装置の情報の変更が反映される時間を調整できます。送信間隔を短くすると変更が早く反映され，送信間隔を長くすると変更の反映が遅くなります。

[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。

19.3 オペレーション

19.3.1 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 19-5 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。

19.3.2 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。

図 19-2 show lldp の実行結果

```
>show lldp

Date 2006/12/13 11:31:31 UTC
Status: Enabled  Chassis ID: Type=MAC       Info=00ee.f209.0001
Interval Time: 30   Hold Count: 4  TTL: 120
Port Counts=3
  0/1         Link: Up    Neighbor Counts: 1
  0/2         Link: Up    Neighbor Counts: 0
  0/3(CH:1)   Link: Down  Neighbor Counts: 0

>
```

図 19-3 show lldp detail の実行結果

```
> show lldp detail

Date 2006/12/13 11:34:21 UTC
Status: Enabled  Chassis ID: Type=MAC     Info=00ee.f209.0001
Interval Time: 30  Hold Count: 4  TTL: 120
System Name: AX1200S-1
System Description: ALAXALA AX1230 AX-1230-24T2C [AX1230S-24T2C] Switching soft
ware Ver. 1.0 [OS-LT]
Total Neighbor Counts=3
Port Counts=3
Port 0/1           Link: Up   Neighbor Counts: 1
  Port ID: Type=MAC     Info=00ee.f209.0101
  Port Description:
  Tag ID: Untagged=1
          Tagged=
  1  TTL:98 Chassis ID: Type=MAC     Info=00ee.f210.0001
     System Name: No2.L1
     System Description: ALAXALA AX1230 AX-1230-24T2C [AX1230S-24T2C] Switching
 software Ver. 1.0 [OS-LT]
     Port ID: Type=MAC     Info=00ee.f210.0101
     Port Description:
     Tag ID: Untagged=1
Port 0/2           Link: Up   Neighbor Counts: 0
  Port ID: Type=MAC     Info=00ee.f209.0102
  Port Description:
  Tag ID: Untagged=1
          Tagged=
Port 0/3(CH:1)     Link: Down Neighbor Counts: 0

>
```

20 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。

20.1　解説

20.1.1　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 20-1　受信フレームのミラーリング

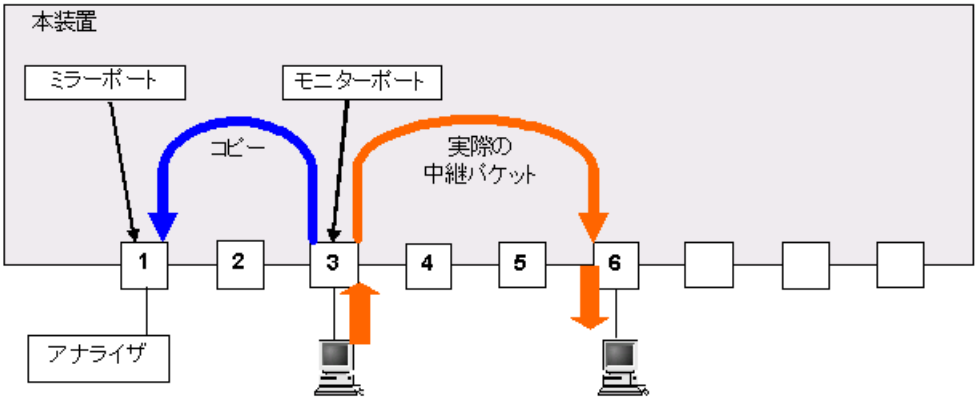
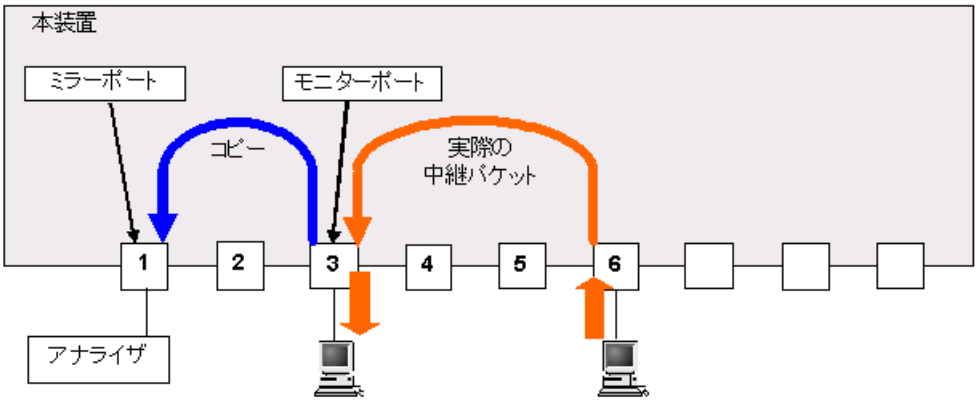


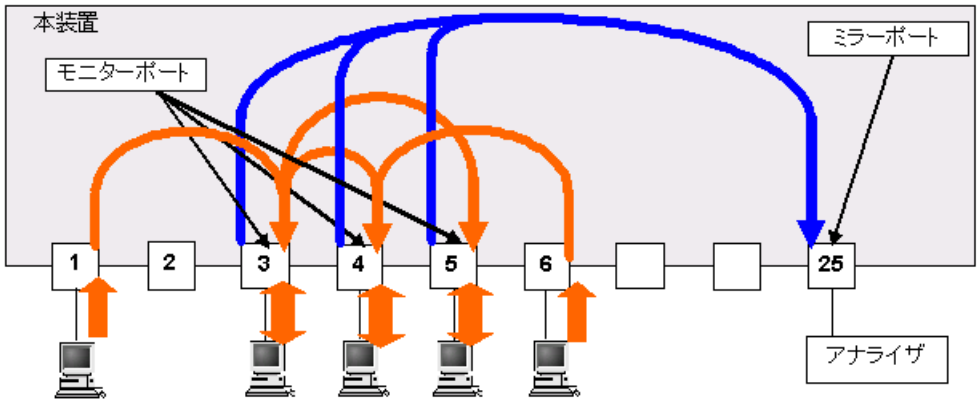
図 20-2　送信フレームのミラーリング



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。

また，モニターポートとミラーポートは「多対一」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，一つのミラーポートへ送信できます。ただし，モニターポートでコピーしたフレームを複数のミラーポートへ送信することはできません。

図 20-3　複数ポートのフレームのミラーリング



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。

20.1.2　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

- モニターポートでは，他の機能は制限なく動作します。
- ミラーポートでは，VLAN 機能が使用できません。VLAN 機能を前提とするスパニングツリー，IGMP snooping/MLD snooping などの機能も使用できません。

（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. 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。
3. モニターポートに対して，フィルタ制御を設定できますが，ポートミラーリング機能には影響しません。
4. 送信フレームのミラーリングでは，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。自発フレームはミラーリングしますが，下記の送信フレームはミラーリングしません。（「表 20-1　送信フレームのミラーリング可否」も参照してください。）
   - 自発の L2 フレーム（LLDP，UDLD など）
   - DHCP フレーム（DHCP snooping 機能有効時）
   - ARP フレーム（ダイナミック ARP 検査機能有効時）
   - IGMP フレーム（IGMP snooping 機能有効時）
   - MLD フレーム（MLD snooping 機能有効時）
   - 認証前フレーム（レイヤ 2 認証機能有効時）
   - 認証前通過フレーム（認証専用 IPv4 アクセスリスト設定時）
   - GSRP aware フレーム（中継時の送信だけ）
   - 自発の L2 ループ検知フレーム（L2 ループ検知有効時）

   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。
5. 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，ミラーリングするフレームは次のようになります。
   - 該当するポートが 0/1 ～ 0/24 および 0/49，0/50 と，0/25 ～ 0/48 にわたっている場合，2 個のフレームをミラーリングします。

- 上記以外の場合，1個のフレームをミラーリングします。

6. 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。
7. ミラーリングでは，1セッションだけ設定できます。
8. 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。

表20-1　送信フレームのミラーリング可否

フレームの種類	ミラーリング可否	種類	備考
ICMP	可	自発	
FTP	可	自発	
telnet	可	自発	
SNMP	可	自発	
SNMP TRAP	可	自発	
syslog	可	自発	
RADIUS	可	自発	
NTP	可	自発	
IGMP	可／不可	中継	IGMP snooping有効時だけ不可
MLD	可／不可	中継	MLD snooping有効時だけ不可
DHCP	可／不可	中継	DHCP snooping有効時だけ不可
ARP	可／不可	中継	ダイナミックARP検査機能有効時だけ不可
認証前	不可	中継	レイヤ2認証機能有効時 認証専用IPv4アクセスリスト設定時
LLDP	不可	自発	
UDLD	不可	自発	
LACP	不可	自発	
EAPOL	不可	自発	
BPDU	不可	自発	
L2ループ検知	不可	自発	
GSRP aware	不可	中継	中継時の送信だけ不可

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

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 20-2 コンフィグレーションコマンド一覧

コマンド名	説明
monitor session	ポートミラーリングを設定します。

20.2.2 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。本装置では最大 1 組のモニターセッションを設定できます。

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。

注※

Ver.1.4.B 以降は，モニタポートに FastEthernet と GigabitEthernet の混在指定が可能です。

(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です。リンクアグリゲーションで使用している場合も，単独のイーサネットインタフェースを指定します。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 0/1 rx destination interface fastethernet 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。セッション番号は 1 固定です。

(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です。リンクアグリゲーションで使用している場合も，単独のイーサネットインタフェースを指定します。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。セッション番号は 1 固定です。

[コマンドによる設定]

1. **(config)# monitor session 1 source interface 0/2 tx destination interface fastethernet 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。セッション番号は 1 固定です。

(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です。リンクアグリゲーションで使用している場合も，単独のイーサネットインタフェースを指定します。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。セッション番号は1固定です。

[コマンドによる設定]

1. **(config)# monitor session 1 source interface 0/3 both destination interface fastethernet 0/11**
   アナライザをポート0/11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。セッション番号は1固定です。

(4) 複数ポートの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です。リンクアグリゲーションで使用している場合も，単独のイーサネットインタフェースを指定します。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。セッション番号は1固定です。

[コマンドによる設定]

1. **(config)# monitor session 1 source interface 0/3-5 both destination interface gigabitethernet 0/25**
   アナライザをポート0/25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。セッション番号は1固定です。

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
RFC2284(1998 年 3 月)	PPP Extensible Authentication Protocol (EAP)
RFC2865(2000 年 6 月)	Remote Authentication Dial In User Service (RADIUS)
RFC2869(2000 年 6 月)	RADIUS Extensions
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

付録 A.2　DHCP サーバ機能

表 A-2　DHCP サーバ機能の準拠規格

規格番号 (発行年月)	規格名
RFC 2131(1997 年 3 月)	Dynamic Host Configuration Protocol
RFC 2132(1997 年 3 月)	DHCP Options and BOOTP Vendor Extensions

付録 A.3　IEEE802.3ah/UDLD

表 A-3　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.4　SNMP

表 A-4　SNMP の準拠規格および勧告

規格番号 (発行年月)	規格名
RFC 1155(1990 年 5 月)	Structure and Identification of Management Information for TCP/IP-based Internets
RFC 1157(1990 年 5 月)	A Simple Network Management Protocol (SNMP)
RFC 1213(1991 年 3 月)	Management Information Base for Network Management of TCP/IP-based internets: MIB-II
RFC 1493(1993 年 6 月)	Definitions of Managed Objects for Bridges ※
RFC 1643(1994 年 7 月)	Definitions of Managed Objects for the Ethernet-like Interface Types ※
RFC 1757(1995 年 2 月)	Remote Network Monitoring Management Information Base

規格番号 (発行年月)	規格名
RFC 1901(1996 年 1 月)	Introduction to Community-based SNMPv2
RFC 1902(1996 年 1 月)	Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC 1903(1996 年 1 月)	Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC 1904(1996 年 1 月)	Conformance Statements for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC 1905(1996 年 1 月)	Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC 1906(1996 年 1 月)	Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC 1907(1996 年 1 月)	Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC 1908(1996 年 1 月)	Coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework
RFC 2233(1997 年 11 月)	The Interfaces Group MIB using SMIv2
RFC 3621(2003 年 12 月)	Power Ethernet MIB

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.5　SYSLOG

表 A-5　SYSLOG の準拠する規格および勧告

規格番号 (発行年月)	規格名
RFC 3164(2001 年 8 月)	The BSD syslog Protocol

付録 A.6　LLDP

表 A-6　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

索引

T

V

W

あ

い

え

か

き

こ

さ

し

す

そ

た

と

な

に

ね

ひ

ふ

ほ

ま

み

も

ゆ

れ

ろ