AX2340S 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.1

Ver. 2.1 対応

AX23S-S001-20

■ 対象製品

このマニュアルは AX2340S を対象に記載しています。また，ソフトウェア OS-L2N Ver.2.1 の機能について記載しています。

■ 輸出時の注意

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

■ 商標一覧

Cisco は，米国 Cisco Systems, Inc. の米国および他の国々における登録商標です。
Ethernet は，富士フイルムビジネスイノベーション株式会社の登録商標です。
Microsoft は，米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
OpenSSL は，米国およびその他の国における米国 OpenSSL Software Foundation の登録商標です。
Python は，Python Software Foundation の登録商標です。
RSA および RC4 は，米国およびその他の国における米国 EMC Corporation の登録商標です。
sFlow は，米国およびその他の国における米国 InMon Corp. の登録商標です。
ssh は，SSH Communications Security,Inc.の登録商標です。
UNIX は，The Open Group の米国ならびに他の国における登録商標です。
Windows は，米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
イーサネットは，富士フイルムビジネスイノベーション株式会社の登録商標です。
そのほかの記載の会社名，製品名は，それぞれの会社の商標もしくは登録商標です。

■ マニュアルはよく読み，保管してください。

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

■ ご注意

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

■ 発行

２０２２年　５月 （第３版） ＡＸ２３Ｓ－Ｓ００１－２０

■ 著作権

変更内容

【Ver. 2.1 対応版】

表　変更内容

章・節・項・タイトル	追加・変更内容
1.1　本装置の特長	• モデルの追加に伴い，ファンレスおよび耐環境の記述を追加しました。
2.1　最大ポート数ごとの対応モデル	• AX2340S-24TH4X および AX2340S-24PH4X の記述を追加しました。
2.2　各モデルの特徴	• AX2340S-24TH4X および AX2340S-24PH4X の記述を追加しました。
2.4　実装メモリ量	• AX2340S-24TH4X および AX2340S-24PH4X の記述を追加しました。
2.5　ソフトウェア	• AX2340S-24TH4X および AX2340S-24PH4X の記述を追加しました。
3.4.2　VLAN	• AX2340S-24TH4X および AX2340S-24PH4X の記述を追加しました。
3.4.3　スパニングツリー	• マルチプルスパニングツリーの収容条件を変更しました。
3.4.5　IGMP snooping/MLD snooping	• マルチキャストルータ自動学習数の収容条件を追加しました。
3.5　IP インタフェース	• IPv6 に関連する記述を追加しました。
3.6　フィルタ・QoS	• IPv6 に関連する記述を追加しました。
3.7.2　Web 認証	• 本項を追加しました。
3.9.1　アップリンク・リダンダント	• AX2340S-24TH4X および AX2340S-24PH4X の記述を追加しました。
4.1.2　運用端末	• IPv6 に関連する記述を追加しました。
8　ログインセキュリティと RADIUS/TACACS+	• IPv6 に関連する記述を追加しました。
9　SSH（Secure Shell）	• IPv6 に関連する記述を追加しました。
11　ホスト名と DNS	• IPv6 に関連する記述を追加しました。
18　SNMP	• IPv6 に関連する記述を追加しました。
20.1.4　10GBASE-R	• 10GBASE-BR について記述を追加しました。
20.3　PoE の解説	• AX2340S-24PH4X の記述を追加しました。
29.3.3　マルチキャストルータとの接続	• マルチキャストルータポート自動学習についての記述を追加しました。
29.5　IGMP snooping/MLD snooping 使用時の注意事項	• 「(4) マルチキャストルータポートの自動学習」を追加しました。 • 「(9) IGMP Query メッセージの送信間隔」を追加しました。
30.1.4　マルチキャストルータポートの設定	• マルチキャストルータポート自動学習についての設定方法を追加しました。
32　IPv6 通信	• 本章を追加しました。
33　DHCP サーバ機能	• サポートに伴い，将来サポートとの記述を削除しました。

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 対応版】

表　変更内容

項目	追加・変更内容
本装置の特長	• マルチギガビットイーサネットの記述を追加しました。
最大ポート数ごとの対応モデル	• AX2340S-16P8MP2X の記述を追加しました。
各モデルの特徴	• AX2340S-16P8MP2X の記述を追加しました。
実装メモリ量	• AX2340S-16P8MP2X の記述を追加しました。
ソフトウェア	• オプションライセンス OP-ULTG の対応モデルを追加しました。
VLAN	• AX2340S-16P8MP2X の記述を追加しました。
アップリンク・リダンダント	• AX2340S-16P8MP2X の記述を追加しました。
ポートの種類とサポート機能	• 100BASE-TX/1000BASE-T/2.5GBASE-T ポートの記述を追加しました。
PoE の解説	• IEEE802.3bt 規格に準拠するモデルについて記述を追加しました。
PoE の設定	• Autoclass 機能によるポートへの供給電力割り当ての設定を追加しました。

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 AX2340S を対象に記載しています。また，ソフトウェア OS-L2N Ver.2.1 およびオプションライセンスによってサポートする機能について記載しています。

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。

https://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。

●ハードウェアの設備条件，取扱方法を調べる

ハードウェア取扱説明書
（AX23S-H001）

トランシーバ
ハードウェア取扱説明書
（AX-COM-H001）

●ソフトウェアの機能とコマンド，コンフィグレーションの設定を知りたい

コンフィグレーションガイド
Vol.1
（AX23S-S001）

Vol.2
（AX23S-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
（AX23S-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
（AX23S-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
（AX23S-S005）

●MIBについて調べる

MIBレファレンス
（AX23S-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
（AX23S-T001）

■ このマニュアルでの表記

AC	Alternating Current
ACK	ACKnowledge
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
ARP	Address Resolution Protocol
bit/s	bits per second　*bpsと表記する場合もあります。
BPDU	Bridge Protocol Data Unit
CA	Certificate Authority
CBC	Cipher Block Chaining
CC	Continuity Check
CFM	Connectivity Fault Management
CIST	Common and Internal Spanning Tree
CRC	Cyclic Redundancy Check
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CST	Common Spanning Tree
DA	Destination Address
DC	Direct Current
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DRR	Deficit Round Robin
DSA	Digital Signature Algorithm
DSAP	Destination Service Access Point

DSCP	Differentiated Services Code Point
DSS	Digital Signature Standard
E-Mail	Electronic Mail
EAP	Extensible Authentication Protocol
EAPOL	EAP Over LAN
ECDHE	Elliptic Curve Diffie-Hellman key exchange, Ephemeral
ECDSA	Elliptic Curve Digital Signature Algorithm
EEE	Energy Efficient Ethernet
FAN	Fan Unit
FCS	Frame Check Sequence
FDB	Filtering DataBase
FQDN	Fully Qualified Domain Name
GCM	Galois/Counter Mode
GSRP	Gigabit Switch Redundancy Protocol
HMAC	Keyed-Hashing for Message Authentication
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
ICMPv6	Internet Control Message Protocol version 6
ID	Identifier
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IETF	the Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISP	Internet Service Provider
IST	Internal Spanning Tree
L2LD	Layer 2 Loop Detection
LAN	Local Area Network
LED	Light Emitting Diode
LLC	Logical Link Control
LLDP	Link Layer Discovery Protocol
MA	Maintenance Association
MAC	Media Access Control
MC	Memory Card
MD5	Message Digest 5
MDI	Medium Dependent Interface
MDI-X	Medium Dependent Interface crossover
MEP	Maintenance association End Point
MIB	Management Information Base
MIP	Maintenance domain Intermediate Point
MLD	Multicast Listener Discovery
MSTI	Multiple Spanning Tree Instance
MSTP	Multiple Spanning Tree Protocol
MTU	Maximum Transmission Unit
NAK	Not AcKnowledge
NAS	Network Access Server
NDP	Neighbor Discovery Protocol
NTP	Network Time Protocol
OAM	Operations,Administration,and Maintenance
OUI	Organizationally Unique Identifier
packet/s	packets per second　　*ppsと表記する場合もあります。
PAD	PADding
PAE	Port Access Entity
PC	Personal Computer
PDU	Protocol Data Unit
PGP	Pretty Good Privacy
PID	Protocol IDentifier
PIM	Protocol Independent Multicast
PoE	Power over Ethernet
PQ	Priority Queueing
PS	Power Supply
QoS	Quality of Service
RA	Router Advertisement
RADIUS	Remote Authentication Dial In User Service
RDI	Remote Defect Indication
REJ	REJect
RFC	Request For Comments
RMON	Remote Network Monitoring MIB
RQ	ReQuest
RSA	Rivest, Shamir, Adleman
RSTP	Rapid Spanning Tree Protocol

SA	Source Address
SFD	Start Frame Delimiter
SFP	Small Form factor Pluggable
SFP+	enhanced Small Form-factor Pluggable
SHA	Secure Hash Algorithm
SMTP	Simple Mail Transfer Protocol
SNAP	Sub-Network Access Protocol
SNMP	Simple Network Management Protocol
SSAP	Source Service Access Point
SSH	Secure Shell
SSL	Secure Socket Layer
STP	Spanning Tree Protocol
TACACS+	Terminal Access Controller Access Control System Plus
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
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
USB	Universal Serial Bus
VLAN	Virtual LAN
WAN	Wide Area Network
WWW	World-Wide Web

■ KB（キロバイト）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　本装置の概要と収容条件

1 本装置の概要 1

1.1 本装置の特長 2

2 装置構成 5

2.1 最大ポート数ごとの対応モデル 6

2.2 各モデルの特徴 7

2.3 ハードウェア構成 10

2.4 実装メモリ量 12

2.5 ソフトウェア 13

3 収容条件 15

3.1 リモートアクセス 16

3.2 NTP 17

3.3 リンクアグリゲーション 18

3.4 レイヤ 2 スイッチ 19

3.4.1 MAC アドレステーブル 19

3.4.2 VLAN 19

3.4.3 スパニングツリー 20

3.4.4 Ring Protocol 22

3.4.5 IGMP snooping/MLD snooping 22

3.5 IP インタフェース 24

3.5.1 IP アドレスを設定できるインタフェース数 24

3.5.2 マルチホームの最大サブネット数 24

3.5.3 IP アドレス最大設定数 25

3.5.4 最大相手装置数 25

3.5.5 スタティックルーティング最大エントリ数 26

3.5.6 DHCP サーバ 26

3.6 フィルタ・QoS 27

3.6.1 フィルタエントリ数 27

3.6.2 QoS エントリ数 27

3.7 レイヤ 2 認証 29

3.7.1 IEEE802.1X 29

3.7.2 Web 認証 29

3.7.3 MAC 認証 30
3.8 DHCP snooping 31
3.9 冗長化構成による高信頼化 32
3.9.1 アップリンク・リダンダント 32
3.10 ネットワーク監視機能 33
3.10.1 L2 ループ検知 33
3.11 ネットワークの管理 34
3.11.1 IEEE802.3ah/UDLD 34
3.11.2 CFM 34
3.11.3 LLDP 35

第 2 編 運用管理

4 装置へのログイン 37
4.1 運用端末による管理 38
4.1.1 運用端末の接続形態 38
4.1.2 運用端末 38
4.1.3 運用管理機能の概要 40
4.2 装置起動 41
4.2.1 起動から停止までの概略 41
4.2.2 装置の起動 41
4.2.3 装置の停止 42
4.3 ログイン・ログアウト 43

5 コマンド操作 45
5.1 コマンド入力モード 46
5.1.1 コマンド一覧 46
5.1.2 コマンド入力モード 46
5.2 CLI での操作 48
5.2.1 補完機能 48
5.2.2 ヘルプ機能 48
5.2.3 入力エラー位置指摘機能 48
5.2.4 コマンド短縮実行 49
5.2.5 ヒストリ機能 49
5.2.6 パイプ機能 50
5.2.7 リダイレクト 51
5.2.8 ページング 51
5.2.9 CLI 設定のカスタマイズ 51

5.3 CLI の注意事項 53

6 コンフィグレーション 55

6.1 コンフィグレーション 56
6.1.1 起動時のコンフィグレーション 56
6.1.2 運用中のコンフィグレーション 56
6.2 ランニングコンフィグレーションの編集概要 57
6.3 コンフィグレーションコマンド入力におけるモード遷移 58
6.4 コンフィグレーションの編集方法 59
6.4.1 コマンド一覧 59
6.4.2 configure（configure terminal）コマンド 60
6.4.3 コンフィグレーションの表示・確認（show コマンド） 60
6.4.4 コンフィグレーションの追加・変更・削除 62
6.4.5 コンフィグレーションのファイルへの保存（save コマンド） 63
6.4.6 コンフィグレーションの編集終了（exit コマンド） 63
6.4.7 コンフィグレーションの編集時の注意事項 64
6.5 コンフィグレーションの操作 65
6.5.1 コンフィグレーションのバックアップ 65
6.5.2 バックアップコンフィグレーションファイルの本装置への反映 65
6.5.3 ftp コマンドを使用したファイル転送 66
6.5.4 MC を使用したファイル転送 67
6.5.5 バックアップコンフィグレーションファイル反映時の注意事項 68

7 リモート運用端末から本装置へのログイン 69

7.1 解説 70
7.1.1 通信用ポート接続 70
7.2 コマンドガイド 71
7.2.1 コマンド一覧 71
7.2.2 本装置への IP アドレスの設定 71
7.2.3 telnet によるログインを許可する 72
7.2.4 ftp によるログインを許可する 72

8 ログインセキュリティと RADIUS/TACACS+ 75

8.1 ログインセキュリティのコマンドガイド 76
8.1.1 コマンド一覧 76
8.1.2 ログイン制御の概要 77
8.1.3 ログインユーザの作成と削除 77
8.1.4 装置管理者モード変更のパスワードの設定 78
8.1.5 リモート運用端末からのログインの許可 78

8.1.6 同時にログインできるユーザ数の設定 79
8.1.7 リモート運用端末からのログインを許可する IP アドレスの設定 79
8.1.8 ログインバナーの設定 80
8.2 RADIUS/TACACS+の解説 82
8.2.1 RADIUS/TACACS+の概要 82
8.2.2 RADIUS/TACACS+の適用機能および範囲 82
8.2.3 RADIUS/TACACS+を使用した認証 88
8.2.4 RADIUS/TACACS+/ローカルを使用したコマンド承認 92
8.2.5 RADIUS/TACACS+を使用したアカウンティング 103
8.2.6 RADIUS/TACACS+との接続 106
8.3 RADIUS/TACACS+のコマンドガイド 107
8.3.1 コマンド一覧 107
8.3.2 RADIUS サーバによる認証の設定 107
8.3.3 TACACS+サーバによる認証の設定 108
8.3.4 RADIUS/TACACS+/ローカルによるコマンド承認の設定 109
8.3.5 RADIUS/TACACS+によるログイン・ログアウトアカウンティングの設定 111
8.3.6 TACACS+サーバによるコマンドアカウンティングの設定 111

9 SSH(Secure Shell) 113
9.1 解説 114
9.1.1 概要 114
9.1.2 SSH の基本機能 116
9.1.3 サポート機能 116
9.1.4 SSH のセキュリティ機能 119
9.1.5 SSH が使用する暗号技術 122
9.1.6 ログイン制御機能のサポート 125
9.1.7 RADIUS/TACACS+のサポート 126
9.1.8 SSH 使用時の注意事項 126
9.2 コマンドガイド 127
9.2.1 コマンド一覧 127
9.2.2 SSH サーバの基本設定（パスワード設定） 128
9.2.3 ユーザ認証に公開鍵認証を使用する設定 128
9.2.4 SSHv2 サーバの暗号アルゴリズムの設定変更 131
9.2.5 リモート運用端末からの SSH 接続を許可する IP アドレスの設定 131
9.2.6 RADIUS/TACACS+機能と連携した SSH サーバの設定 132
9.2.7 ホスト公開鍵の確認 132
9.2.8 ホスト鍵ペアの変更 133

10 時刻の設定と NTP 135
10.1 解説 136

10.1.1 NTP サポート仕様 136
10.1.2 クライアント機能 137
10.1.3 サーバ機能 139
10.1.4 シンメトリック接続 140
10.1.5 ローカルタイムサーバ 140
10.1.6 NTP 使用時の注意事項 140
10.1.7 時刻変更に関する注意事項 141
10.2 コマンドガイド 142
10.2.1 コマンド一覧 142
10.2.2 システムクロックの設定 143
10.2.3 クライアント機能の設定 143
10.2.4 サーバ機能の設定 144
10.2.5 シンメトリック接続の設定 144
10.2.6 認証の設定 145

11 ホスト名と DNS 147
11.1 解説 148
11.2 コマンドガイド 149
11.2.1 コマンド一覧 149
11.2.2 ホスト名の設定 149
11.2.3 DNS の設定 149

12 装置の管理 151
12.1 コマンドガイド 152
12.1.1 コマンド一覧 152
12.1.2 モデルに応じたコンフィグレーション 153
12.2 運用情報のバックアップ・リストア 154
12.2.1 コマンド一覧 154
12.2.2 backup/restore コマンドを用いる手順 154
12.3 障害時の復旧 156
12.3.1 障害部位と復旧内容 156
12.4 内蔵フラッシュメモリへ保存時の注意事項 157

13 MC 運用モード 159
13.1 解説 160
13.1.1 概要 160
13.1.2 MC に保存されるファイル 160
13.1.3 MC 運用モードを使用した運用手順 160
13.1.4 障害時の動作 161

13.1.5 MC 運用モード使用時の注意事項 162
13.2 コマンドガイド 163
13.2.1 コマンド一覧 163
14 ゼロタッチプロビジョニング 165
14.1 解説 166
14.1.1 概要 166
14.1.2 本装置と AX-Network-Manager との通信方法 166
14.1.3 ゼロタッチプロビジョニングの対象ファイル 167
14.1.4 ゼロタッチプロビジョニングを使用した運用手順 167
14.1.5 ゼロタッチプロビジョニング使用時の注意事項 168
14.2 コマンドガイド 169
14.2.1 コマンド一覧 169
14.2.2 ゼロタッチプロビジョニングの設定 169
15 ソフトウェアの管理 171
15.1 ソフトウェアアップデートの解説 172
15.1.1 概要 172
15.1.2 アップデートの準備 172
15.1.3 アップデートの注意事項 174
15.2 アップデートのコマンドガイド 175
15.2.1 コマンド一覧 175
15.2.2 アップデートファイルの準備 175
15.2.3 アップデートコマンドの実行 176
15.3 オプションライセンスの解説 178
15.3.1 概要 178
15.3.2 オプションライセンスに関する注意事項 178
15.4 オプションライセンスのコマンドガイド 179
15.4.1 コマンド一覧 179
15.4.2 オプションライセンスの設定方法 179
15.4.3 オプションライセンスの削除方法 180
16 省電力機能 183
16.1 省電力機能の解説 184
16.1.1 省電力機能の概要 184
16.1.2 省電力機能 184
16.2 省電力機能のコマンドガイド 185
16.2.1 コマンド一覧 185

17 ログ出力機能 187
17.1 解説 188
17.2 コマンドガイド 189
17.2.1 コマンド一覧 189
17.2.2 ログの syslog 出力の設定 189
17.2.3 運用メッセージの出力抑止 190
17.2.4 ログの E-Mail 出力の設定 190
18 SNMP 191
18.1 解説 192
18.1.1 SNMP 概説 192
18.1.2 MIB 概説 195
18.1.3 SNMPv1，SNMPv2C オペレーション 197
18.1.4 SNMPv3 オペレーション 202
18.1.5 トラップ 206
18.1.6 インフォーム 207
18.1.7 RMON MIB 208
18.1.8 SNMP マネージャとの接続時の注意事項 211
18.2 コマンドガイド 212
18.2.1 コマンド一覧 212
18.2.2 SNMPv1，SNMPv2C による MIB アクセス許可の設定 213
18.2.3 SNMPv3 による MIB アクセス許可の設定 213
18.2.4 SNMPv1，SNMPv2C によるトラップ送信の設定 214
18.2.5 SNMPv3 によるトラップ送信の設定 214
18.2.6 SNMPv2C によるインフォーム送信の設定 215
18.2.7 リンクトラップの抑止 215
18.2.8 RMON イーサネットヒストリグループの制御情報の設定 216
18.2.9 RMON による特定 MIB 値の閾値チェック 216
19 高機能スクリプト 219
19.1 解説 220
19.1.1 概要 220
19.1.2 高機能スクリプトの適用例 222
19.1.3 高機能スクリプトの仕様 223
19.1.4 スクリプト使用時の注意事項 224
19.2 スクリプトの作成と実行 226
19.2.1 コマンド一覧 226
19.2.2 スクリプトの実行の流れ 227
19.2.3 スクリプトファイルの作成 227

19.2.4　スクリプトファイルの正常性確認　227
19.2.5　スクリプトファイルのインストール　229
19.2.6　スクリプトの起動　230
19.3　本装置の Python サポート内容　233
19.3.1　標準 Python との差分および制限　233
19.3.2　標準ライブラリ　233
19.4　Python 拡張ライブラリの使用方法　236
19.4.1　指定コマンド実行の設定　236
19.4.2　運用メッセージ出力の設定　240
19.4.3　イベント監視機能の設定　241
19.4.4　スクリプト起動契機の取得　244

第 3 編　ネットワークインタフェース

20 イーサネット　247
20.1　接続インタフェースの解説　248
20.1.1　ポートの種類とサポート機能　248
20.1.2　10BASE-T/100BASE-TX/1000BASE-T/2.5GBASE-T　250
20.1.3　1000BASE-X　256
20.1.4　10GBASE-R　257
20.2　イーサネット共通の解説　259
20.2.1　フローコントロール　259
20.2.2　フレームフォーマット　263
20.2.3　ジャンボフレーム　265
20.3　PoE の解説　266
20.3.1　ポートへの供給電力の割り当て　266
20.3.2　電力供給の優先制御　267
20.3.3　装置の電力超過時の動作　268
20.3.4　PoE 給電分散機能　268
20.3.5　PoE 使用時の注意事項　269
20.4　コマンドガイド　271
20.4.1　コマンド一覧　271
20.4.2　イーサネットインタフェースの設定　272
20.4.3　複数インタフェースの一括設定　273
20.4.4　速度と全二重/半二重の設定　273
20.4.5　自動 MDI/MDIX 機能の設定　275
20.4.6　フローコントロールの設定　275
20.4.7　ジャンボフレームの設定　276
20.4.8　リンクダウン検出タイマの設定　277

20.4.9　リンクアップ検出タイマの設定　278
20.4.10　フレーム送受信エラー通知の設定　278
20.4.11　PoE の設定　279

21 リンクアグリゲーション　283
21.1　リンクアグリゲーション基本機能の解説　284
21.1.1　概要　284
21.1.2　リンクアグリゲーションの構成　284
21.1.3　サポート仕様　284
21.1.4　チャネルグループの MAC アドレス　284
21.1.5　フレーム送信時のポート振り分け　285
21.1.6　リンクアグリゲーション使用時の注意事項　285
21.2　リンクアグリゲーション基本機能のコマンドガイド　287
21.2.1　コマンド一覧　287
21.2.2　スタティックリンクアグリゲーションの設定　287
21.2.3　LACP リンクアグリゲーションの設定　288
21.2.4　ポートチャネルインタフェースの設定　289
21.2.5　チャネルグループの削除　291
21.3　リンクアグリゲーション拡張機能の解説　293
21.3.1　スタンバイリンク機能　293
21.3.2　離脱ポート制限機能　294
21.4　リンクアグリゲーション拡張機能のコマンドガイド　295
21.4.1　コマンド一覧　295
21.4.2　スタンバイリンク機能のコンフィグレーション　295
21.4.3　離脱ポート制限機能のコンフィグレーション　296

第 4 編　レイヤ 2 スイッチング

22 レイヤ 2 スイッチ概説　297
22.1　概要　298
22.1.1　MAC アドレス学習　298
22.1.2　VLAN　298
22.2　サポート機能　299
22.2.1　本装置の MAC アドレス　299
22.3　レイヤ 2 スイッチ機能と他機能の共存について　301

23 MAC アドレス学習　307
23.1　解説　308

23.1.1 送信元 MAC アドレス学習 308
23.1.2 MAC アドレス学習の移動検出 308
23.1.3 学習 MAC アドレスのエージング 308
23.1.4 MAC アドレスによるレイヤ 2 スイッチング 308
23.1.5 スタティックエントリの登録 309
23.1.6 MAC アドレス学習抑止 309
23.1.7 MAC アドレステーブルのクリア 309
23.1.8 注意事項 311
23.2 コマンドガイド 312
23.2.1 コマンド一覧 312
23.2.2 エージングタイムの設定 312
23.2.3 スタティックエントリの設定 312
23.2.4 MAC アドレス学習抑止の設定 313

24 VLAN 315
24.1 VLAN 基本機能の解説 316
24.1.1 VLAN の種類 316
24.1.2 ポートの種類 316
24.1.3 デフォルト VLAN 317
24.1.4 VLAN の優先順位 318
24.1.5 VLAN Tag 319
24.1.6 VLAN 使用時の注意事項 321
24.2 VLAN 基本機能のコマンドガイド 322
24.2.1 コマンド一覧 322
24.2.2 VLAN の設定 322
24.2.3 ポートの設定 323
24.2.4 トランクポートの設定 323
24.2.5 VLAN Tag の TPID の設定 324
24.3 ポート VLAN の解説 326
24.3.1 アクセスポートとトランクポート 326
24.3.2 ネイティブ VLAN 326
24.3.3 ポート VLAN 使用時の注意事項 327
24.4 ポート VLAN のコマンドガイド 328
24.4.1 コマンド一覧 328
24.4.2 ポート VLAN の設定 328
24.4.3 トランクポートのネイティブ VLAN の設定 329
24.5 プロトコル VLAN の解説 331
24.5.1 概要 331
24.5.2 プロトコルの識別 331
24.5.3 プロトコルポートとトランクポート 332

24.5.4 プロトコルポートのネイティブ VLAN 332
24.6 プロトコル VLAN のコマンドガイド 333
24.6.1 コマンド一覧 333
24.6.2 プロトコル VLAN の作成 333
24.6.3 プロトコルポートのネイティブ VLAN の設定 335
24.7 MAC VLAN の解説 337
24.7.1 概要 337
24.7.2 装置間の接続と MAC アドレス設定 337
24.7.3 レイヤ 2 認証機能との連携について 338
24.7.4 MAC ポートの VLAN 設定 338
24.8 MAC VLAN のコマンドガイド 340
24.8.1 コマンド一覧 340
24.8.2 MAC VLAN の設定 340
24.8.3 MAC ポートのネイティブ VLAN の設定 342
24.9 VLAN インタフェース 344
24.9.1 IP アドレスを設定するインタフェース 344
24.10 VLAN インタフェースのコマンドガイド 345
24.10.1 コマンド一覧 345
24.10.2 レイヤ 3 インタフェースとしての VLAN の設定 345

25 VLAN 拡張機能 347
25.1 VLAN トンネリングの解説 348
25.1.1 概要 348
25.1.2 VLAN トンネリングを使用するための必須条件 348
25.1.3 VLAN トンネリング使用時の注意事項 349
25.2 VLAN トンネリングのコマンドガイド 350
25.2.1 コマンド一覧 350
25.2.2 VLAN トンネリングの設定 350
25.3 Tag 変換の解説 351
25.3.1 概要 351
25.3.2 Tag 変換使用時の注意事項 351
25.4 Tag 変換のコマンドガイド 352
25.4.1 コマンド一覧 352
25.4.2 Tag 変換の設定 352
25.5 L2 プロトコルフレーム透過機能の解説 354
25.5.1 概要 354
25.5.2 L2 プロトコルフレーム透過機能の注意事項 354
25.6 L2 プロトコルフレーム透過機能のコマンドガイド 355
25.6.1 コマンド一覧 355
25.6.2 L2 プロトコルフレーム透過機能の設定 355

25.7 ポート間中継遮断機能の解説 356
25.7.1 概要 356
25.7.2 ポート間中継遮断機能使用時の注意事項 356
25.8 ポート間中継遮断機能のコマンドガイド 358
25.8.1 コマンド一覧 358
25.8.2 ポート間中継遮断機能の設定 358
25.8.3 遮断するポートの変更 359
25.9 VLAN debounce 機能の解説 360
25.9.1 概要 360
25.9.2 VLAN debounce 機能と他機能との関係 360
25.9.3 VLAN debounce 機能使用時の注意事項 360
25.10 VLAN debounce 機能のコマンドガイド 362
25.10.1 コマンド一覧 362
25.10.2 VLAN debounce 機能の設定 362

26 スパニングツリー 363
26.1 スパニングツリーの概説 364
26.1.1 概要 364
26.1.2 スパニングツリーの種類 364
26.1.3 スパニングツリーと高速スパニングツリー 365
26.1.4 スパニングツリートポロジーの構成要素 366
26.1.5 スパニングツリーのトポロジー設計 369
26.1.6 STP 互換モード 370
26.1.7 スパニングツリー共通の注意事項 371
26.2 スパニングツリーのコマンドガイド 372
26.2.1 コマンド一覧 372
26.2.2 動作モードの設定 372
26.3 PVST+解説 375
26.3.1 PVST+によるロードバランシング 375
26.3.2 アクセスポートの PVST+ 376
26.3.3 PVST+使用時の注意事項 377
26.4 PVST+のコマンドガイド 378
26.4.1 コマンド一覧 378
26.4.2 PVST+の設定 378
26.4.3 PVST+のトポロジー設定 379
26.4.4 PVST+のパラメータ設定 380
26.5 シングルスパニングツリー解説 382
26.5.1 概要 382
26.5.2 PVST+との併用 382
26.5.3 シングルスパニングツリー使用時の注意事項 383

26.6 シングルスパニングツリーのコマンドガイド 384
26.6.1 コマンド一覧 384
26.6.2 シングルスパニングツリーの設定 384
26.6.3 シングルスパニングツリーのトポロジー設定 385
26.6.4 シングルスパニングツリーのパラメータ設定 386
26.7 マルチプルスパニングツリー解説 388
26.7.1 概要 388
26.7.2 マルチプルスパニングツリーのネットワーク設計 391
26.7.3 ほかのスパニングツリーとの互換性 392
26.7.4 マルチプルスパニングツリー使用時の注意事項 393
26.8 マルチプルスパニングツリーのコマンドガイド 394
26.8.1 コマンド一覧 394
26.8.2 マルチプルスパニングツリーの設定 394
26.8.3 マルチプルスパニングツリーのトポロジー設定 395
26.8.4 マルチプルスパニングツリーのパラメータ設定 397
26.9 スパニングツリー共通機能解説 399
26.9.1 PortFast 399
26.9.2 BPDU フィルタ 399
26.9.3 ループガード 400
26.9.4 ルートガード 401
26.10 スパニングツリー共通機能のコマンドガイド 403
26.10.1 コマンド一覧 403
26.10.2 PortFast の設定 403
26.10.3 BPDU フィルタの設定 404
26.10.4 ループガードの設定 405
26.10.5 ルートガードの設定 405
26.10.6 リンクタイプの設定 406

27 Ring Protocol の解説 407
27.1 Ring Protocol の概要 408
27.1.1 概要 408
27.1.2 特長 409
27.1.3 サポート仕様 410
27.2 Ring Protocol の基本原理 412
27.2.1 ネットワーク構成 412
27.2.2 制御 VLAN 414
27.2.3 障害監視方法 414
27.2.4 通信経路の切り替え 414
27.3 シングルリングの動作概要 415
27.3.1 リング正常時の動作 415

27.3.2 障害検出時の動作 415
27.3.3 復旧検出時の動作 417
27.4 マルチリングの動作概要 419
27.4.1 リング正常時の動作 419
27.4.2 共有リンク障害・復旧時の動作 421
27.4.3 共有リンク非監視リングでの共有リンク以外の障害・復旧時の動作 423
27.4.4 共有リンク監視リングでの共有リンク以外の障害・復旧時の動作 425
27.5 Ring Protocol の多重障害監視機能 428
27.5.1 概要 428
27.5.2 多重障害監視機能の基本構成 429
27.5.3 多重障害監視の動作概要 429
27.5.4 多重障害発生時の動作 430
27.5.5 多重障害復旧時の動作 433
27.6 Ring Protocol のネットワーク設計 437
27.6.1 VLAN マッピングの使用方法 437
27.6.2 制御 VLAN の forwarding-delay-time の使用方法 437
27.6.3 Ring Protocol の禁止構成 438
27.6.4 多重障害監視機能の禁止構成 438
27.7 Ring Protocol 使用時の注意事項 439

28 Ring Protocol の設定と運用 443
28.1 コマンドガイド 444
28.1.1 コマンド一覧 444
28.1.2 Ring Protocol 設定の流れ 445
28.1.3 リング ID の設定 445
28.1.4 制御 VLAN の設定 446
28.1.5 VLAN マッピングの設定 446
28.1.6 VLAN グループの設定 447
28.1.7 モードとリングポートに関する設定（シングルリングと共有リンクなしマルチリング構成） 447
28.1.8 モードとリングポートに関する設定（共有リンクありマルチリング構成） 449
28.1.9 各種パラメータの設定 451
28.1.10 多重障害監視機能の設定 452

29 IGMP snooping/MLD snooping の解説 453
29.1 IGMP snooping/MLD snooping の概要 454
29.1.1 マルチキャスト概要 454
29.1.2 IGMP snooping および MLD snooping 概要 455
29.2 IGMP snooping/MLD snooping サポート機能 456
29.3 IGMP snooping 457

29.3.1 MAC アドレスの学習 457
29.3.2 IPv4 マルチキャストパケットのレイヤ 2 中継 458
29.3.3 マルチキャストルータとの接続 459
29.3.4 IGMP クエリア機能 462
29.3.5 IGMP 即時離脱機能 462
29.4 MLD snooping 464
29.4.1 MAC アドレスの学習 464
29.4.2 IPv6 マルチキャストパケットのレイヤ 2 中継 465
29.4.3 マルチキャストルータとの接続 465
29.4.4 MLD クエリア機能 466
29.5 IGMP snooping/MLD snooping 使用時の注意事項 468

30 IGMP snooping/MLD snooping の設定と運用 471
30.1 IGMP snooping のコマンドガイド 472
30.1.1 コマンド一覧 472
30.1.2 IGMP snooping の設定 473
30.1.3 IGMP クエリア機能の設定 473
30.1.4 マルチキャストルータポートの設定 473
30.2 MLD snooping のコマンドガイド 476
30.2.1 コマンド一覧 476
30.2.2 MLD snooping の設定 476
30.2.3 MLD クエリア機能の設定 476
30.2.4 マルチキャストルータポートの設定 477

第 5 編 IP インタフェース

31 IPv4 通信 479
31.1 解説 480
31.1.1 アドレッシング 480
31.1.2 インターネットプロトコル(IP) 481
31.1.3 ICMP 482
31.1.4 ARP 484
31.1.5 経路設定 485
31.1.6 IPv4 使用時の注意事項 486
31.2 コマンドガイド 487
31.2.1 コマンド一覧 487
31.2.2 インタフェースの設定 488
31.2.3 マルチホームの設定 488

31.2.4　ループバックインタフェースの設定　488
31.2.5　スタティック ARP の設定　488
31.2.6　デフォルト経路の設定　489
31.2.7　スタティック経路の設定　489

32 IPv6 通信　491
32.1　解説　492
32.1.1　IPv6 アドレス　492
32.1.2　本装置で使用する IPv6 アドレスの扱い　501
32.1.3　インターネットプロトコル　バージョン 6 (IPv6)　503
32.1.4　ICMPv6　505
32.1.5　NDP　506
32.1.6　RA　507
32.1.7　IPv6 使用時の注意事項　507
32.2　コマンドガイド　509
32.2.1　コマンド一覧　509
32.2.2　インタフェースの設定　510
32.2.3　リンクローカルアドレスの手動設定　510
32.2.4　ループバックインタフェースの設定　510
32.2.5　スタティック NDP の設定　511
32.2.6　RA の設定　511

33 DHCP サーバ機能　513
33.1　解説　514
33.1.1　サポート仕様　514
33.1.2　クライアントへの配布情報　514
33.1.3　ダイナミック DNS 連携　515
33.1.4　IP アドレスの二重配布防止　515
33.1.5　DHCP サーバ機能使用時の注意事項　516
33.2　コマンドガイド　517
33.2.1　コマンド一覧　517
33.2.2　クライアントに IP を配布する設定　518
33.2.3　クライアントに固定 IP を配布する設定　519
33.2.4　ダイナミック DNS 連携時の設定　521

付録　523
付録 A　準拠規格　524
付録 A.1　TELNET/FTP　524

付録 A.2　RADIUS/TACACS+ 524
付録 A.3　SSH 524
付録 A.4　NTP 525
付録 A.5　DNS 525
付録 A.6　EEE 525
付録 A.7　SYSLOG 525
付録 A.8　SNMP 526
付録 A.9　イーサネット 528
付録 A.10　リンクアグリゲーション 529
付録 A.11　VLAN 529
付録 A.12　スパニングツリー 529
付録 A.13　IGMP snooping/MLD snooping 530
付録 A.14　IPv4 通信 530
付録 A.15　IPv6 通信 530
付録 A.16　DHCP サーバ機能 531

索引 533

1 本装置の概要

この章では，本装置の特長について説明します。

1.1　本装置の特長

本装置は，充実した認証機能を含む各種機能を備えた，ギガビットイーサネット対応のレイヤ 2 スイッチです。AX シリーズとしての一貫した操作性を備え，ローエンドのイーサネットレイヤ 2 スイッチとしてエッジの部分をカバーします。

本装置は，次に示す特長を備えています。

(1)　AX シリーズとの接続性と相互運用性を保持

●レイヤ 2 の VLAN 機能

- ポート VLAN，プロトコル VLAN，MAC VLAN 機能を実装
- 用途に応じた VLAN 構築が可能

●スパニングツリープロトコル

- スパニングツリー（IEEE 802.1D），高速スパニングツリー（IEEE 802.1w），PVST+，マルチプルスパニングツリー（IEEE 802.1s）を実装

●VLAN トンネリングによる L2-VPN の実現

●QoS による通信品質保証

- ハードウェアによる高性能な QoS 処理
- きめ細かなパラメータ（L2/L3/L4 ヘッダ）指定で，高い精度の QoS 制御が可能
- 多様な QoS 制御機能

  L2-QoS（IEEE 802.1p，優先制御，廃棄制御など），IP-QoS（Diff-Serv，優先制御，廃棄制御など）
- 音声・データ統合ネットワークでさまざまなシェーパ機能

  VoIP パケットを優先し，クリアな音声を提供可能

●多様な冗長ネットワーク構築

- 高速な経路切り替え

  リンクアグリゲーション（IEEE 802.3AX），高速スパニングツリー（IEEE 802.1w，IEEE 802.1s）などの標準機能，GSRP aware や Autonomous Extensible Ring Protocol（以降，Ring Protocol と呼びます。）などの独自機能で，冗長化した高信頼ネットワークを構築可能。また，スパニングツリーを使用しない冗長構成が可能なアップリンク・リダンダントに対応。

(2)　優れたネットワーク管理，保守・運用

●ネットワーク管理

- IPv4/v6 デュアルスタックや IPv6 環境に対応したネットワーク管理（SNMP over IPv6）など充実した機能
- 基本的な MIB-II に加え，IPv6 MIB，RMON などの豊富な MIB をサポート

●USB メモリカード※採用

- コンフィグレーションのバックアップや障害情報採取が容易に実行可能
- 保守作業の簡略化が可能

注※　本シリーズのマニュアルでは，USB メモリカードの操作および表示説明で「MC」と表記しています。

●MC 運用モード

- MC へのソフトウェアと装置情報の一括保存，MC に保存したソフトウェアと装置情報からの起動が容易に実行可能

●ゼロタッチプロビジョニング

- AX-Network-Manager※と連携することで，障害時などの装置交換をコンソールや MC 不要で実施可能

  注※　AX-Network-Manager の操作や設定については，AX-Network-Manager のマニュアルを参照してください。

(3)　マルチギガビットイーサネット（mGig）対応

●100BASE-TX/1000BASE-T/2.5GBASE-T ポートに対応

- ツイストペアケーブル（UTP）を使用して既存のシステムを利用したまま，高速な無線 LAN 装置の収容が可能

(4)　10G アップリンク対応

●10G アップリンク対応

- 構内ネットワークで AX シリーズと組み合わせると，ハイパフォーマンスな 10G ネットワークを実現。
- 10G イーサネットのトランシーバとして 1G と 10G のイーサネットに対応可能な SFP+を採用。SFP+/SFP 共用ポートによって，1G イーサネットから 10G イーサネットへのスムーズな移行が可能。

(5)　強固なセキュリティ機能

●セキュアブート

- 本装置で動作するソフトウェアの改ざんを検知し，不正があった場合，装置の起動を抑止するセキュリティ機能を実装

●認証・検疫ソリューション

- レイヤ 2 認証機能（IEEE802.1X，Web 認証，MAC 認証）によって，エッジの物理構成の自由度を保ちつつ，PC1 台 1 台を認証し，VLAN に加入させることが可能
- 端末認証とユーザ認証の組み合わせで許可された場合にだけネットワークの使用を許可する，マルチステップ認証をサポート

●不正な DHCP サーバ／固定 IP アドレス端末の排除が可能

- DHCP snooping によって，不正な DHCP サーバや固定 IP アドレス端末の排除が可能

(6)　PoE 対応

●IP 電話機，無線 LAN AP などの PD（受電装置）を収容

- 電力線配線工事をなくし，ケーブル増による煩わしさを減らすと同時に電力線配線コストを削減し，工事期間の短縮を実現
- IEEE802.3af/IEEE802.3at/IEEE 802.3bt 準拠

●装置起動時の PoE 給電分散

- 装置起動から PoE 給電開始までの待機時間を設定して PoE 給電開始を分散させ，システム全体での電力使用量のピークを低減

(7)　コンパクト・環境負荷低減・省電力

●コンパクトな筐体

- 高さ 1U サイズのコンパクトな筐体
- 10BASE-T/100BASE-TX/1000BASE-T を最大 48 ポート収容可能な高ポート密度

●RoHS 対応の環境負荷低減を実現

●EEE（Energy Efficient Ethernet）

- イーサネット上の通信がない場合に，電力供給を低減することで省電力を実現
- IEEE 802.3az 準拠

(8)　ファンレス・耐環境

●ファンレスに対応

- 機器内に吸い込まれる埃によるトラブルの発生を軽減するとともに，騒音のない静かなオフィス環境を実現

●耐環境に対応

- ファンレスおよび PoE 対応でありながら，厳しい温度条件下での動作を実現

2 装置構成

この章では，本装置の各モデル構成要素など，各装置本体について説明します。

2.1　最大ポート数ごとの対応モデル

本装置はボックス型イーサネットスイッチです。

最大ポート数ごとの対応モデルを次の表に示します。

表 2-1　最大ポート数ごとの対応モデル

最大ポート数による分類	対応モデル
10BASE-T/100BASE-TX/1000BASE-T　24 ポート 1000BASE-T または 1000BASE-X　2 ポート 1000BASE-T，1000BASE-X，または 10GBASE-R　4 ポート	AX2340S-24T4X AX2340S-24TH4X
10BASE-T/100BASE-TX/1000BASE-T　48 ポート 1000BASE-T または 1000BASE-X　2 ポート 1000BASE-T，1000BASE-X，または 10GBASE-R　4 ポート	AX2340S-48T4X
10BASE-T/100BASE-TX/1000BASE-T（PoE）　24 ポート 1000BASE-T または 1000BASE-X　2 ポート 1000BASE-T，1000BASE-X，または 10GBASE-R　4 ポート	AX2340S-24P4X AX2340S-24PH4X
10BASE-T/100BASE-TX/1000BASE-T（PoE）　48 ポート 1000BASE-T または 1000BASE-X　2 ポート 1000BASE-T，1000BASE-X，または 10GBASE-R　4 ポート	AX2340S-48P4X
10BASE-T/100BASE-TX/1000BASE-T（PoE）　16 ポート 100BASE-TX/1000BASE-T/2.5GBASE-T（PoE）　8 ポート 1000BASE-T，1000BASE-X，または 10GBASE-R　2 ポート	AX2340S-16P8MP2X

2.2　各モデルの特徴

最大収容可能回線数をはじめとする各モデルの特徴を次に示します。

(1)　AX2340S-24T4X，AX2340S-24TH4X および AX2340S-48T4X

AX2340S-24T4X，AX2340S-24TH4X および AX2340S-48T4X には，次に示す種類のポートがあります。

- 10BASE-T/100BASE-TX/1000BASE-T ポート
  10BASE-T/100BASE-TX/1000BASE-T で使用できるポートです。
- SFP ポート
  1000BASE-X で使用できるポートです。また，1000BASE-T 用 SFP をサポートしており，1000BASE-T としても使用できるポートです。
- SFP+/SFP 共用ポート
  SFP+使用時は 10GBASE-R で，SFP 使用時は 1000BASE-X で使用できるポートです。また，1000BASE-T 用 SFP をサポートしており，1000BASE-T としても使用できるポートです。なお，10GBASE-R は，アップリンク 10G に対応するオプションライセンス使用時に利用できます。

ポートの種類と収容回線数を次の表に示します。

表 2–2　最大収容可能回線数

ポートの種類	AX2340S-24T4X AX2340S-24TH4X	AX2340S-48T4X
10BASE-T/100BASE-TX/1000BASE-T ポート	24	48
SFP ポート	2	2
SFP+/SFP 共用ポート※	4	4

注※
SFP+/SFP 共用ポートで SFP+を使用するには，オプションライセンス（アップリンク 10G）が必要です。

(2)　AX2340S-24P4X，AX2340S-24PH4X および AX2340S-48P4X

AX2340S-24P4X，AX2340S-24PH4X および AX2340S-48P4X には，次に示す種類のポートがあります。

- 10BASE-T/100BASE-TX/1000BASE-T ポート
  10BASE-T/100BASE-TX/1000BASE-T で使用できるポートであるほか，PoE に対応するポートです。
- SFP ポート
  1000BASE-X で使用できるポートです。また，1000BASE-T 用 SFP をサポートしており，1000BASE-T としても使用できるポートです。
- SFP+/SFP 共用ポート
  SFP+使用時は 10GBASE-R で，SFP 使用時は 1000BASE-X で使用できるポートです。また，1000BASE-T 用 SFP をサポートしており，1000BASE-T としても使用できるポートです。なお，10GBASE-R は，アップリンク 10G に対応するオプションライセンス使用時に利用できます。

ポートの種類と収容回線数を次の表に示します。

表 2-3 最大収容可能回線数

ポートの種類	AX2340S-24P4X AX2340S-24PH4X	AX2340S-48P4X
10BASE-T/100BASE-TX/1000BASE-T ポート	24	48
SFP ポート	2	2
SFP+/SFP 共用ポート※	4	4

注※
SFP+/SFP 共用ポートで SFP+を使用するには，オプションライセンス（アップリンク 10G）が必要です。

また，モデルごとの PoE 関連の仕様を次の表に示します。

表 2-4 PoE の仕様

PoE の仕様		AX2340S-24P4X	AX2340S-24PH4X	AX2340S-48P4X
PoE 対応ポート数		24	24	48
最大供給電力	装置全体	535 ワット	250 ワット	785 ワット
	ポート当たり	30 ワット	30 ワット	30 ワット

(3) AX2340S-16P8MP2X

AX2340S-16P8MP2X には，次に示す種類のポートがあります。

- 10BASE-T/100BASE-TX/1000BASE-T ポート
  10BASE-T/100BASE-TX/1000BASE-T で使用できるポートであるほか，PoE に対応するポートです。
- 100BASE-TX/1000BASE-T/2.5GBASE-T ポート
  100BASE-TX/1000BASE-T/2.5GBASE-T で使用できるポートであるほか, PoE に対応するポートです。
- SFP+/SFP 共用ポート
  SFP+使用時は 10GBASE-R で，SFP 使用時は 1000BASE-X で使用できるポートです。また，1000BASE-T 用 SFP をサポートしており，1000BASE-T としても使用できるポートです。

ポートの種類と収容回線数を次の表に示します。

表 2-5 最大収容可能回線数

ポートの種類	AX2340S-16P8MP2X
10BASE-T/100BASE-TX/1000BASE-T ポート	16
100BASE-TX/1000BASE-T/2.5GBASE-T ポート	8
SFP+/SFP 共用ポート	2

また，モデルごとの PoE 関連の仕様を次の表に示します。

表 2–6　PoE の仕様

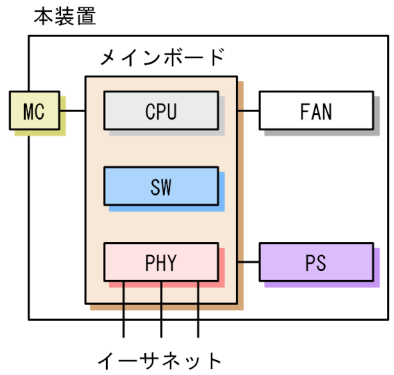
PoE の仕様			AX2340S-16P8MP2X
PoE 対応ポート数			24
最大供給電力	装置全体		815 ワット
	ポート当たり	10BASE-T/100BASE-TX/1000BASE-T ポート	30 ワット
		100BASE-TX/1000BASE-T/2.5GBASE-T ポート	60 ワット

2.3　ハードウェア構成

本装置の各モデルは，統一したアーキテクチャで設計しています。

ハードウェアの構成を次の図に示します。

図 2-1　ハードウェアの構成



（凡例）MC：Memory Card
SW：SWitch processor
PHY：Physical Interface
PS：Power Supply

(1)　装置筐体

装置筐体には，メインボード，PS，FAN が含まれています。

(2)　メインボード

メインボードは CPU 部，SW 部，PHY 部から構成されます。

- CPU（Central Processing Unit）
  CPU を実装し，装置全体の管理，SW 部/PHY 部の制御，各種プロトコル処理をソフトウェアで行います。
  ソフトウェアは CPU 部に実装される装置内メモリに格納されます。
- SW（Switch processor）
  L2 フレームのスイッチングを行います。SW 部はハードウェアによる MAC アドレス学習/エージング，リンクアグリゲーション，フィルタ/QoS テーブル検索，自宛/自発パケットの DMA 転送を行います。
- PHY（Physical Interface）
  各種メディア対応のインタフェース部です。

(3)　PS（Power Supply）

PS は外部供給電源から本装置内で使用する直流電源を生成します。

なお，PS には電源スイッチ（ブレーカ）がありません。電源ケーブルを接続／抜去（取り付け／取り外し）することで，電源が ON／OFF の状態となります。

(4)　FAN

FAN は装置内部を冷却するファンです。

ただし，AX2340S-24T4X，AX2340S-24TH4X，および AX2340S-24PH4X はファンレスモデルとなります。

(5)　MC（Memory Card）

MC を使用して，コンフィグレーションのバックアップ，およびダンプ情報の採取ができます。MC として USB メモリカードを使用できます。

2.4　実装メモリ量

実装メモリ量および内蔵フラッシュメモリ量を次の表に示します。本装置では実装メモリおよび内蔵フラッシュメモリの増設はできません。

表 2-7　実装メモリ量と内蔵フラッシュメモリ量

項目	AX2340S-24T4X AX2340S-24TH4X AX2340S-48T4X AX2340S-24P4X AX2340S-24PH4X AX2340S-48P4X	AX2340S-16P8MP2X
実装メモリ量	2GB	
内蔵フラッシュメモリ量	1GB	2GB

2.5　ソフトウェア

本装置のソフトウェアを次の表に示します。

表 2-8　本装置のソフトウェア一覧

ソフトウェア略称	内容
OS-L2N	L2 スイッチ中継，VLAN，スパニングツリー，SNMP，LLDP ほか

本装置でサポートしているオプションライセンスを次の表に示します。

表 2-9　本装置のオプションライセンス一覧

オプションライセンス略称	内容
OP-ULTG	アップリンク 10G 次の装置に本ライセンスを設定すると，SFP+/SFP 共用ポートを 10Gbit/s（SFP+）で使用できます。 • AX2340S-24T4X • AX2340S-24TH4X • AX2340S-48T4X • AX2340S-24P4X • AX2340S-24PH4X • AX2340S-48P4X

3 収容条件

この章では，収容条件について説明します。

3.1　リモートアクセス

本装置へのリモートアクセスでの収容条件を示します。

(1)　リモートログインできるユーザ数

telnet や ssh によって本装置へリモートログインできるユーザの最大数は，コンフィグレーションコマンド line vty で設定する，ログインできるユーザ数です。なお，line vty コマンドで設定できるログインできるユーザ数は，最大で 16 です。

(2)　本装置へのユーザ公開鍵の登録

SSH によって本装置へ接続するユーザが公開鍵認証を使用する場合は，ユーザ名と，該当ユーザのユーザ公開鍵を登録してください。公開鍵認証を使用する場合に登録できるユーザ数およびユーザ公開鍵数を次の表に示します。

表 3-1　登録できるユーザ数およびユーザ公開鍵数

項目	最大数
登録できる公開鍵認証ユーザ数	20 ユーザ／装置
登録できるユーザ公開鍵数	10 個／ユーザ

3.2　NTP

本装置での NTP サーバおよびクライアントの最大接続数を次の表に示します。

表 3-2　NTP サーバおよびクライアントの最大接続数

機能	最大接続数
ユニキャスト	50 クライアント※
ブロードキャスト	上限なし

注※

上位 NTP サーバ，シンメトリック接続サーバ，および下位クライアント数の合計です。

本装置での NTP コンフィグレーション設定数を次の表に示します。

表 3-3　コンフィグレーション設定数

機能	最大設定数
ユニキャストクライアント（ntp server）	10※
シンメトリック接続（ntp peer）	10※
ブロードキャストサーバ（ntp broadcast）	10※

注※

コンフィグレーションコマンド ntp server，ntp peer，および ntp broadcast で設定できるエントリ数の合計は最大 10 です。

3.3　リンクアグリゲーション

コンフィグレーションによって設定できるリンクアグリゲーションの収容条件を次の表に示します。

表 3-4　リンクアグリゲーションの収容条件

モデル	チャネルグループ当たりの 最大ポート数	装置当たりの 最大チャネルグループ
全モデル共通	8	54

3.4　レイヤ 2 スイッチ

3.4.1　MAC アドレステーブル

L2 スイッチ機能では，接続されたホストの MAC アドレスをダイナミックに学習して MAC アドレステーブルへ登録します。また，スタティックに MAC アドレステーブルへ登録することもできます。

MAC アドレステーブルに登録できる MAC アドレスのエントリの最大数を次の表に示します。

表 3-5　MAC アドレステーブルに登録できる MAC アドレスのエントリ数

モデル	装置当たり	
	最大エントリ数	スタティックエントリ数
全モデル共通	16384※	2048

注※

ハードウェアの制限によって，収容条件の最大数まで登録できないことがあります。

MAC アドレスが収容条件を超えた場合，学習済みエントリがエージングされるまで新たな MAC アドレス学習は行われません。したがって，未学習の MAC アドレス宛てのパケットは該当する VLAN ドメイン内でフラッディングされます。

また，本装置では，MAC アドレステーブルのエントリの数をコンフィグレーションによって変更することはできません。

3.4.2　VLAN

コンフィグレーションによって設定できる VLAN の数を次の表に示します。

表 3-6　VLAN のサポート数

モデル	ポート当たり VLAN	装置当たり VLAN	ポートごと VLAN 数の装置での合計
AX2340S-16P8MP2X	1024	1024	26624
AX2340S-24T4X AX2340S-24TH4X AX2340S-24P4X AX2340S-24PH4X			30720
AX2340S-48T4X AX2340S-48P4X			55296

ポートごと VLAN 数の装置での合計は，ポートに設定している VLAN の数を，装置の全ポートで合計した値です。例えば，24 ポートの装置で，ポート 1 からポート 10 では設定している VLAN 数が 1000，ポート 11 からポート 24 では設定している VLAN 数が 1 の場合，ポートごと VLAN 数の装置での合計は 10014 となります。なお，チャネルグループに所属するポートでも，チャネルグループでまとめるのではなく，ポートに設定している VLAN の数で計算されます。ポートごと VLAN 数の装置での合計が収容条件を超えた場合，CPU の利用率が高くなり，コンフィグレーションコマンドや運用コマンドのレスポンスが遅くなったり，実行できなくなったりすることがあります。

(1)　プロトコル VLAN

プロトコル VLAN では，イーサネットフレーム内の Ethernet-Type，LLC SAP，および SNAP type フィールドの値を基にプロトコルの識別を行います。コンフィグレーションによって設定できるプロトコル VLAN の収容条件を次の表に示します。

表 3-7　プロトコル VLAN のプロトコルの種類数

モデル	ポート当たり	装置当たり
全モデル共通	12	12

表 3-8　プロトコル VLAN 数

モデル	ポート当たり	装置当たり
全モデル共通	100※	100

注※　トランクポートに設定できるプロトコル VLAN 数。プロトコルポートに設定できるプロトコル VLAN 数は 12 です。

(2)　MAC VLAN

MAC VLAN の収容条件を次の表に示します。

表 3-9　MAC VLAN の登録 MAC アドレス数

モデル	コンフィグレーションによる最大登録 MAC アドレス数	L2 認証機能による最大登録 MAC アドレス数	同時登録最大 MAC アドレス数
全モデル共通	64	1024	1088

(3)　VLAN トンネリング

コンフィグレーションによって設定できる VLAN トンネリングの数を次の表に示します。

表 3-10　VLAN トンネリングの数

モデル	装置当たり
全モデル共通	実装ポート数－ 1

(4)　Tag 変換

コンフィグレーションによって設定できる Tag 変換情報エントリ数を次の表に示します。Tag 変換をチャネルグループに設定した場合は，チャネルグループに所属するポートごとにエントリを消費します。

表 3-11　Tag 変換情報エントリ数

モデル	装置当たり
全モデル共通	4096

3.4.3　スパニングツリー

スパニングツリーの収容条件を種類ごとに次の表に示します。

なお，スパニングツリーの VLAN ポート数は，スパニングツリーが動作する VLAN に所属するポート数の延べ数です。チャネルグループの場合，チャネルグループ当たりの物理ポート数を数えます。ただし，次の VLAN やポートは，VLAN ポート数に含めません。

- コンフィグレーションコマンド state で suspend パラメータが設定されている VLAN
- VLAN トンネリングを設定しているポート
- BPDU ガード機能を設定しているが，BPDU フィルタ機能を設定していないポート
- PortFast 機能と BPDU フィルタ機能を設定しているアクセスポート

表 3-12　PVST+の収容条件

モデル	対象 VLAN 数	VLAN ポート数※1
全モデル共通	250	256※2

注※1

スパニングツリー対象となる各 VLAN に設定するポート数の合計（VLAN 数とポート数の積）。

例えば，100 個の VLAN を設定し，それぞれの VLAN に 2 回線が所属している場合，ポート数は 100×2 ＝ 200 となります。

VLAN トンネリングとの併用時，アクセスポートはポート数に含みません。

注※2

PortFast 機能を設定したポート数は含めません。

表 3-13　シングルスパニングツリーの収容条件

モデル	対象 VLAN 数	VLAN ポート数※1	VLAN ポート数※1 (PVST+併用時※2)
全モデル共通	1024※3	5000	1000

注※1

スパニングツリー対象となる各 VLAN に設定するポート数の合計（VLAN 数とポート数の積）。

例えば，100 個の VLAN を設定し，それぞれの VLAN に 2 回線が所属している場合，ポート数は 100×2 ＝ 200 となります。

VLAN トンネリングとの併用時，アクセスポートはポート数に含みません。

注※2

PVST+の対象ポート含み合計の最大値が 1000 となります。

注※3

PVST+同時動作時は PVST+対象 VLAN 数を引いた値となります。

表 3-14　マルチプルスパニングツリーの収容条件

モデル	対象 VLAN 数	VLAN ポート数※1	MST インスタンス数	MST インスタンスごとの対象 VLAN 数※2
全モデル共通	1024	5000	16	200

注※1

スパニングツリー対象となる各 VLAN に設定するポート数の合計（VLAN 数とポート数の積）。

例えば，100 個の VLAN を設定し，それぞれの VLAN に 2 回線が所属している場合，ポート数は 100×2 ＝ 200 となります。

VLAN トンネリングとの併用時，アクセスポートはポート数に含みません。

注※2

MST インスタンス 0 は除きます。MST インスタンス 0 の対象 VLAN 数は 1024 となります。なお，運用中は運用コマンド show spanning-tree port-count で対象 VLAN 数と VLAN ポート数を確認できます。

3.4.4　Ring Protocol

(1)　Ring Protocol

Ring Protocol の収容条件を次の表に示します。

表 3-15　Ring Protocol の収容条件

項目	リング当たり	装置当たり
リング数	－	24
VLAN マッピング数	－	128
VLAN グループ数	2	48
VLAN グループの VLAN 数	1023※1※2	1023※1※2
リングポート数※3	2	48

（凡例）－：該当なし

注※1

装置として推奨する VLAN の最大数です。

リング当たりに制御 VLAN 用として VLAN を一つ消費するため，VLAN グループに使用できる VLAN の最大数は 1023 となります。ただし，リング数が増加するに従い，VLAN グループに使用できる VLAN の最大数は減少します。

注※2

多重障害監視機能は，多重障害監視 VLAN 用としてリング当たり VLAN を一つ消費するため，VLAN グループに使用できる VLAN の最大数は減少します。

注※3

チャネルグループの場合は，チャネルグループ単位で 1 ポートと数えます。

(2)　多重障害監視機能

多重障害監視機能の収容条件を次の表に示します。

表 3-16　多重障害監視機能の収容条件

項目	最大数
装置当たりの多重障害監視可能リング数	4
リング当たりの多重障害監視 VLAN 数	1
装置当たりの多重障害監視 VLAN 数	4

3.4.5　IGMP snooping/MLD snooping

IGMP snooping の収容条件を次の表に示します。

表 3-17　IGMP snooping の収容条件

項目	最大数
設定 VLAN 数	64
VLAN ポート数※1	512
登録エントリ数※2※3	1024
マルチキャストルータ自動学習数	32

注※1

IGMP snooping が動作するポート数（IGMP snooping を設定した VLAN に収容されるポートの総和）です。例えば，各々 10 ポート収容している 16 個の VLAN で IGMP snooping を動作させる場合，IGMP snooping 動作ポート数は 160 となります。

注※2

登録エントリ数の最大数には，ルーティングプロトコルなどで使用する制御パケットのマルチキャストアドレスも含みます。該当するエントリは，制御パケットに対するグループ参加要求を受信した場合に登録します。VLAN 内で複数のルーティングプロトコルを同時に使用する場合，該当するプロトコルの制御パケットが使用するマルチキャストアドレス分だけエントリを使用します。

注※3

各 VLAN で学習したマルチキャスト MAC アドレスの総和です。

MLD snooping の収容条件を次の表に示します。

表 3-18　MLD snooping の収容条件

項目	最大数
設定 VLAN 数	32
VLAN ポート数※1	512
登録エントリ数※2※3	500

注※1

MLD snooping が動作するポート数（MLD snooping を設定した VLAN に収容されるポートの総和）です。例えば，各々 10 ポート収容している 16 個の VLAN で MLD snooping を動作させる場合，MLD snooping 動作ポート数は 160 となります。

注※2

登録エントリ数の最大数には，ルーティングプロトコルなどで使用する制御パケットのマルチキャストアドレスも含みます。該当するエントリは，制御パケットに対するグループ参加要求を受信した場合に登録します。VLAN 内で複数のルーティングプロトコルを同時に使用する場合，該当するプロトコルの制御パケットが使用するマルチキャストアドレス分だけエントリを使用します。

注※3

各 VLAN で学習したマルチキャスト MAC アドレスの総和です。

3.5　IP インタフェース

本装置では VLAN に対して IP アドレスを設定します。ここでは，IP アドレスを設定できる VLAN インタフェースの最大数，設定できる IP アドレスの最大数，通信できる相手装置の最大数などについて説明します。また，DHCP サーバの収容条件についても説明します。

3.5.1　IP アドレスを設定できるインタフェース数

本装置でサポートする最大インタフェース数を次の表に示します。ここで示す値は，IPv4 と IPv6 の合計の値です。

なお，IPv4 と IPv6 を同一のインタフェースに設定することも，個別に設定することもできます。

表 3-19　最大インタフェース数

モデル	インタフェース数（装置当たり）
全モデル共通	128

3.5.2　マルチホームの最大サブネット数

LAN のマルチホーム接続では一つのインタフェースに対して，複数の IPv4 アドレスまたは IPv6 アドレスを設定します。

(1)　IPv4 の場合

IPv4 でのマルチホームの最大サブネット数を次の表に示します。

表 3-20　マルチホームの最大サブネット数（IPv4 の場合）

モデル	マルチホーム サブネット数 （インタフェース当たり）
全モデル共通	128

(2)　IPv6 の場合

IPv6 でのマルチホームの最大サブネット数を次の表に示します。なお，ここで示す値にはリンクローカルアドレスを含みます。一つのインタフェースには必ず一つのリンクローカルアドレスが設定されます。このため，すべてのインタフェースで IPv6 グローバルアドレスだけを設定した場合，実際に装置に設定される IPv6 アドレス数は，表の数値に，自動生成される IPv6 リンクローカルアドレス数の 1 を加算した，8 になります。

表 3-21　マルチホームの最大サブネット数（IPv6 の場合）

モデル	マルチホーム サブネット数 （インタフェース当たり）
全モデル共通	7

3.5.3　IP アドレス最大設定数

(1)　IPv4 アドレス

装置当たりのコンフィグレーションで設定できる IPv4 アドレスの最大数を次の表に示します。

表 3-22　コンフィグレーションで装置に設定できる IPv4 アドレス最大数

モデル	IPv4 アドレス数（装置当たり）
全モデル共通	128※

注※

VLAN インタフェースに設定できる IPv4 アドレス数です。ループバックインタフェースに設定したアドレス数は含みません。

(2)　IPv6 アドレス

装置当たりのコンフィグレーションで設定できる IPv6 アドレスの最大数を次の表に示します。

表 3-23　コンフィグレーションで装置に設定できる IPv6 アドレス最大数

モデル	IPv6 アドレス数（装置当たり）
全モデル共通	128※

注※

VLAN インタフェースに設定できる IPv6 アドレス数です。ループバックインタフェースに設定したアドレス数は含みません。

3.5.4　最大相手装置数

本装置が接続する最大相手装置数を示します。この場合の相手装置はルータに限らず，端末も含みます。

(1)　ARP エントリ数

IPv4 では，ARP によって，送信しようとするパケットの宛先アドレスに対応するハードウェアアドレスを決定します。したがって，ARP エントリ数によって最大相手装置数が決まります。

ARP エントリは動的に学習することも，コンフィグレーションによってスタティックに指定することもできます。

表 3-24　最大 ARP エントリ数

モデル	インタフェース当たり		装置当たり	
	最大エントリ数	最大スタティックエントリ数	最大エントリ数	最大スタティックエントリ数
全モデル共通	4096	256	4096	256

(2)　NDP エントリ数

IPv6 では，NDP によって，送信しようとするパケットの宛先アドレスに対応するハードウェアアドレスを決定します。したがって，NDP エントリ数によって最大相手装置数が決まります。

NDP エントリは動的に学習することも，コンフィグレーションによってスタティックに指定することもできます。

表 3-25　最大 NDP エントリ数

モデル	インタフェース当たり		装置当たり	
	最大エントリ数	最大スタティックエントリ数	最大エントリ数	最大スタティックエントリ数
全モデル共通	512	128	512	128

3.5.5　スタティックルーティング最大エントリ数

本装置発パケットの経路情報として利用できるスタティックルーティングの最大エントリ数を次の表に示します。なお，本装置ではスタティックルーティングだけが利用でき，RIP や OSPF などのルーティングプロトコルはサポートしていません。

(1)　IPv4 スタティックルーティングエントリ数

表 3-26　スタティックルーティングの最大エントリ数（IPv4 の場合）

モデル	項目	最大エントリ数
全モデル共通	IPv4 ユニキャスト経路エントリ	128※

注※　ダイレクト経路は含みません。

(2)　IPv6 スタティックルーティングエントリ数

表 3-27　スタティックルーティングの最大エントリ数（IPv6 の場合）

モデル	項目	最大エントリ数
全モデル共通	IPv6 ユニキャスト経路エントリ	64※

注※　ダイレクト経路は含みません。

3.5.6　DHCP サーバ

DHCP サーバで設定できるインタフェース数および配布可能 IP アドレス数などを次の表に示します。

表 3-28　DHCP サーバの最大数

項目	装置当たりの最大数
DHCP サーバインタフェース数	128
DHCP サーバ管理サブネット数	1024
配布可能 IP アドレス数※1	2000
配布可能固定 IP アドレス数	160
配布除外 IP アドレス範囲数※2	4096

注※1　配布可能固定 IP アドレス数を含みます。

注※2　サブネット当たり 1024 までです。

3.6　フィルタ・QoS

フィルタ・QoS の検出条件は，コンフィグレーションコマンド access-list および qos-flow-list で設定します。ここでは，設定したリストを装置内部で使用する形式（エントリ）に変換したエントリ数の上限をフィルタ・QoS の収容条件として示します。

フィルタ・QoS の検出条件によるリソース配分を決定するために，フィルタおよび QoS，かつ受信側および送信側の共通モードであるフロー検出モードを選択します。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 で設定します。選択するモードによって，エントリ数の上限値を決定する条件が異なります。なお，受信側はフィルタおよび QoS を，送信側はフィルタをサポートしています。

3.6.1　フィルタエントリ数

フロー検出モードごとの，装置当たりに設定できるフィルタ最大エントリ数を次の表に示します。

フィルタエントリは受信側と送信側に設定することができ，最大エントリ数は受信側と送信側の総和になります。

表 3-29　フィルタ最大エントリ数

フロー検出モード	最大エントリ数※		
	MAC 条件	IPv4 条件	IPv6 条件
layer2-1	256	－	－
layer2-2	－	256	－
layer2-3	－	128	64

（凡例）－：該当なし

注※

フィルタエントリ追加時，該当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フロー未検出時に動作するエントリ（廃棄動作）を自動的に付与します。このため，フィルタ最大エントリ数のすべてを使用できません。フィルタエントリの数え方の例を次に示します。

（例 1）

エントリ条件：イーサネットインタフェース 1/0/1 に 1 エントリ設定

エントリ数　：設定エントリ(1)とイーサネットインタフェース 1/0/1 の廃棄エントリ(1)の合計 2 エントリを使用する

残エントリ数：フィルタ最大エントリ数－使用したエントリ数

（例 2）

エントリ条件：イーサネットインタフェース 1/0/1 に 2 エントリ，VLAN10 のインタフェースに 3 エントリ設定

エントリ数　：設定エントリ(5)とイーサネットインタフェース 1/0/1 の廃棄エントリ(1)および VLAN10 のインタフェースの廃棄エントリ(1)の合計 7 エントリを使用する

残エントリ数：フィルタ最大エントリ数－使用したエントリ数

3.6.2　QoS エントリ数

フロー検出モードごとの，装置当たりに設定できる QoS 最大エントリ数を次の表に示します。

QoS エントリは受信側にだけ設定できます。

表 3-30　QoS 最大エントリ数

フロー検出モード	最大エントリ数		
	MAC 条件	IPv4 条件	IPv6 条件
layer2-1	128	－	－
layer2-2	－	128	－
layer2-3	－	64	32

（凡例）－：該当なし

3.7　レイヤ 2 認証

3.7.1　IEEE802.1X

IEEE802.1X の収容条件を次の表に示します。

表 3-31　IEEE802.1X の収容条件

項目		ポート単位の最大認証端末数	装置単位の最大認証端末数
最大認証数	固定 VLAN モード	64	1024※1
	ダイナミック VLAN モード	64	1024※2

注※1

IEEE802.1X（固定 VLAN モード），Web 認証（固定 VLAN モード）および MAC 認証（固定 VLAN モード）を同時に動作させた場合は，それぞれの認証端末数の合計で装置当たり 1024 までとなります。

注※2

IEEE802.1X（ダイナミック VLAN モード），Web 認証（ダイナミック VLAN モード）および MAC 認証（ダイナミック VLAN モード）を同時に動作させた場合は，それぞれの認証端末数の合計で装置当たり 1024 までとなります。

3.7.2　Web 認証

Web 認証の収容条件を次の表に示します。

表 3-32　Web 認証の装置当たりの収容条件

項目		最大数
最大認証数	固定 VLAN モード	1024※1
	ダイナミック VLAN モード	1024※2
内蔵 Web 認証 DB 登録ユーザ数		300※3
認証画面入れ替えで指定できるファイルの合計サイズ		1024KB
認証画面入れ替えで指定できるファイル数		100
認証前端末用に設定できる IPv4 アクセスリスト数		1
認証前端末用 IPv4 アクセスリストに指定できるフィルタ条件数		20

注※1

Web 認証（固定 VLAN モード），IEEE802.1X（固定 VLAN モード）および MAC 認証（固定 VLAN モード）を同時に動作させた場合は，それぞれの認証端末数の合計で装置当たり 1024 までとなります。

注※2

Web 認証（ダイナミック VLAN モード），MAC 認証（ダイナミック VLAN モード）および IEEE802.1X（ダイナミック VLAN モード）を同時に動作した場合は，それぞれの認証端末数の合計で装置当たり 1024 までとなります。

注※3

内蔵 Web 認証 DB に登録したユーザ ID を複数の端末で使用すると，最大認証端末数まで端末を認証できます。ただし，認証対象となるユーザ ID の数が内蔵 Web 認証 DB の最大登録数より多い場合は，RADIUS サーバを用いた RADIUS 認証方式を使用してください。

3.7.3　MAC 認証

MAC 認証の収容条件を次の表に示します。

表 3-33　MAC 認証の装置当たりの収容条件

項目		最大数
最大認証数	固定 VLAN モード	1024※1
	ダイナミック VLAN モード	1024※2
内蔵 MAC 認証 DB 登録ユーザ数		1024

注※1

MAC 認証（固定 VLAN モード），IEEE802.1X（固定 VLAN モード）および Web 認証（固定 VLAN モード）を同時に動作させた場合は，それぞれの認証端末数の合計で装置当たり 1024 までとなります。

注※2

MAC 認証（ダイナミック VLAN モード），IEEE802.1X（ダイナミック VLAN モード）および Web 認証（ダイナミック VLAN モード）を同時に動作させた場合は，それぞれの認証端末数の合計で装置当たり 1024 までとなります。

3.8　DHCP snooping

DHCP snooping の収容条件を次の表に示します。

表 3-34　DHCP snooping の最大エントリ数

モデル	バインディングデータベースエントリ数※		端末フィルタエントリ数
	ダイナミック／スタティックの合計	スタティック	
全モデル共通	3070	256	200

注※

untrust ポート配下の端末当たり 1 エントリを消費します。

表 3-35　DHCP snooping の最大 VLAN 数

モデル	最大 VLAN 数	
	DHCP snooping	ダイナミック ARP 検査
全モデル共通	1024	32

3.9　冗長化構成による高信頼化

3.9.1　アップリンク・リダンダント

アップリンク・リダンダントに関する収容条件を次の表に示します。

表 3-36　アップリンク・リダンダント収容条件

モデル	アップリンクポート数※	アップリンクポート当たりの収容インタフェース数
AX2340S-16P8MP2X	13	2
AX2340S-24T4X AX2340S-24TH4X AX2340S-24P4X AX2340S-24PH4X	15	2
AX2340S-48T4X AX2340S-48P4X	27	2

注※　チャネルグループの場合は，チャネルグループ単位で 1 ポートと数えます。

表 3-37　MAC アドレスアップデート機能の収容条件

モデル	最大送信 MAC アドレスエントリ数
全モデル共通	3000

3.10　ネットワーク監視機能

3.10.1　L2 ループ検知

L2 ループ検知の L2 ループ検知フレーム送信レートを次の表に示します。

表 3-38　L2 ループ検知フレーム送信レート

モデル	L2 ループ検知フレームの送信レート（装置当たり）※1	
	スパニングツリーを使用している場合	スパニングツリーを使用していない場合
全モデル共通	30pps（推奨値）※2	200pps（最大値）※3

- L2 ループ検知フレーム送信レート算出式
  L2 ループ検知フレーム送信対象の VLAN ポート数÷L2 ループ検知フレームの送信レート（pps）≦送信間隔（秒）
  なお，チャネルグループの場合，VLAN ポート数はチャネルグループ単位で 1 ポートと数えます。

注※1
送信レートは上記の条件式に従って，自動的に 200pps 以内で変動します。

注※2
スパニングツリーを使用している場合は，30pps 以下に設定してください。30pps より大きい場合，スパニングツリーの正常動作を保証できません。

注※3
200pps を超えるフレームは送信しません。送信できなかったフレームに該当するポートや VLAN ではループ障害を検知できなくなります。必ず 200pps 以下に設定してください。

3.11　ネットワークの管理

3.11.1　IEEE802.3ah/UDLD

全物理ポートでの運用を可能にします。1 ポート 1 対地を原則とするため，同一ポートから複数装置の情報を受信する場合（禁止構成）でも，保持する情報は 1 装置分だけです。IEEE802.3ah/UDLD の収容条件を次の表に示します。

表 3-39　最大リンク監視情報数

モデル	最大リンク監視情報数
全モデル共通	装置の最大物理ポート数

3.11.2　CFM

CFM の収容条件を次の表に示します。

表 3-40　CFM の収容条件

モデル	ドメイン数	MA 数	MEP 数	MIP 数	CFM ポート総数※1※2	リモート MEP 総数※2※3
全モデル共通	8／装置	32／装置	32／装置	32／装置	256／装置	2016／装置

注※1

CFM ポート総数とは，MA のプライマリ VLAN のうち，CFM のフレームを送信する VLAN ポートの総数です。

Down MEP だけの MA の場合

Down MEP の VLAN ポートの総数

Up MEP を含む MA の場合

プライマリ VLAN の全 VLAN ポートの総数

なお，CFM ポート総数は運用コマンド show cfm summary で確認できます。

注※2

CFM ポート総数およびリモート MEP 総数は，CCM 送信間隔がデフォルト値のときの収容条件です。CCM 送信間隔を変更すると，CFM ポート総数およびリモート MEP 総数の収容条件が変わります。CCM 送信間隔による CFM ポート総数およびリモート MEP 総数の収容条件を次の表に示します。

表 3-41　CCM 送信間隔による収容条件

モデル	CCM 送信間隔	CFM ポート総数	リモート MEP 総数
全モデル共通	1 分以上	256／装置	2016／装置
	10 秒	128／装置	2016／装置
	1 秒	50／装置	200／装置

注※3

リモート MEP 総数とは，自装置以外の MEP の総数です。MEP からの CCM 受信性能に影響します。
リモート MEP 総数は運用コマンド show cfm remote-mep で確認できます。

表 3-42　CFM の物理ポートおよびチャネルグループの収容条件

モデル	MEP・MIP を設定可能な物理ポートおよびチャネルグループの総数※
全モデル共通	8／装置

注※

MEP・MIP は同一ポートに対して複数設定できます。チャネルグループの場合は，チャネルグループ単位で 1 ポートと数えます。

表 3-43　CFM のデータベース収容条件

モデル	MEP CCM データベース エントリ数	MIP CCM データベース エントリ数	Linktrace データベース エントリ数※
全モデル共通	63／MEP	2048／装置	1024／装置

注※

1 ルート当たり 256 装置の情報を保持する場合は，最大で 4 ルート分を保持します（1024÷256 装置＝ 4 ルート）。

3.11.3　LLDP

LLDP の収容条件を次の表に示します。

表 3-44　LLDP の収容条件

項目		最大収容数
LLDP 隣接装置情報	IEEE 802.1AB Draft 6	108
	IEEE Std 802.1AB-2009	108
Port And Protocol VLAN ID TLV で送信できる VLAN 数		100※
VLAN Name TLV で送信できる VLAN 数		100※

注※

Port And Protocol VLAN ID TLV と VLAN Name TLV で合わせて 100 個となります。また，値の小さい順に 100 個となります。

4 装置へのログイン

この章では，装置の起動と停止，およびログイン・ログアウト，運用管理の概要，運用端末とその接続形態について説明します。

4.1　運用端末による管理

本装置の運用にはコンソールまたはリモート運用端末が必要です。コンソールは RS232C に接続する端末，リモート運用端末は IP ネットワーク経由で接続する端末です。また，本装置は IP ネットワーク経由で SNMP マネージャによるネットワーク管理にも対応しています。コンソールやリモート運用端末など本装置の運用管理を行う端末を運用端末と呼びます。

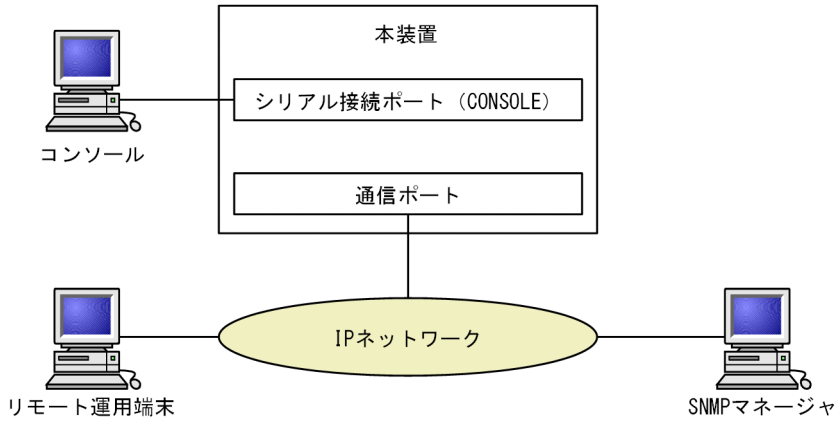
4.1.1　運用端末の接続形態

コンソールは本装置のシリアル接続ポート（CONSOLE）に接続します。また，リモート運用端末は次に示す接続形態がとれます。

- 通信ポートが接続する IP ネットワークから接続する形態

運用端末の接続形態を次の図に示します。

図 4-1　運用端末の接続形態



(1)　シリアル接続ポート（CONSOLE）

シリアル接続ポート（CONSOLE）にコンソールを接続します。コンフィグレーションを設定していなくても本ポートを経由してログインできるため，初期導入時には本ポートからログインして，初期設定ができます。

(2)　通信用ポート

通信用ポートを経由して，遠隔のリモート運用端末からの本装置に対するログインや SNMP マネージャによるネットワーク管理ができます。このポートを経由して telnet，ssh，ftp などによって本装置へログインするためには，本装置のコンフィグレーションで IP アドレスおよびリモートアクセスの設定をする必要があります。

4.1.2　運用端末

コンソールとリモート運用端末の運用管理での適用範囲の違いを次の表に示します。

表 4-1　コンソールとリモート運用端末の運用管理での適用範囲の違い

運用機能	コンソール	リモート運用端末
遠隔からのログイン	不可	可
本装置から運用端末へのログイン	不可	可
アクセス制御	なし	あり
コマンド入力	可	可
ファイル転送方式	なし	ftp
IP 通信	不可	IPv4 および IPv6
SNMP マネージャ接続	不可	可
コンフィグレーション設定	不要	必要

(1)　コンソール

コンソールは RS232C に接続する端末で，一般的な通信端末，通信ソフトウェアが使用できます。コンソールが本装置と通信できるように，次の標準 VT-100 設定値（本装置のデフォルト設定値）が通信ソフトウェアに設定されていることを確認してください。

- 通信速度：115200bit/s
- データ長：8 ビット
- パリティビット：なし
- ストップビット：1 ビット
- フローコントロール：なし

なお，通信速度を 115200bit/s 以外（2400／4800／9600／19200bit/s）で設定して使用したい場合は，コンフィグレーションコマンド speed で本装置側の通信速度設定を変更してください。ただし，実際に設定が反映されるのはコンソールからいったんログアウトしたあとになります。

図 4-2　コンソールの通信速度の設定例

```
(config)# line console 0
(config-line)# speed 19200
```

注意

コンソールを使用する場合は次の点に注意してください。

- 本装置ではコンソール端末からログインする際に，自動的に VT-100 の制御文字を使用して画面サイズを取得・設定します。VT-100 に対応していないコンソール端末では，不正な文字列が表示されたり，最初の CLI プロンプトがずれて表示されたりして，画面サイズが取得・設定できません。

  また，ログインと同時にキー入力した場合，VT-100 の制御文字の表示結果が正常に取得できないため同様の現象となりますのでご注意ください。この場合は，再度ログインし直してください。
- 通信速度の設定が反映されるのは，ログアウトしたあとになります。コンソールからいったんログアウトしたあとで，使用している通信端末や通信ソフトウェアの通信速度の設定を変更してください。変更するまでは文字列が不正な表示になります（「login」プロンプトなど）。
- 通信速度をデフォルト設定値以外に設定して運用している場合，装置を起動（再起動）するとコンフィグレーションが装置に反映されるまでの間，不正な文字列が表示されます。

(2)　リモート運用端末

本装置に IP ネットワーク経由で接続してコマンド操作を行う端末が，リモート運用端末です。telnet プロトコルまたは ssh プロトコルのクライアント機能がある端末はリモート運用端末として使用できます。

注意

本装置の telnet サーバは，改行コードとして[CR]を認識します。一部のクライアント端末では，改行コードとして[CR]および[LF]を送信します。これらの端末から接続した場合，空行が表示されたり，(y/n) 確認時にキー入力ができなかったりするなどの現象がおこります。このような場合は，各クライアント端末の設定を確認してください。

4.1.3　運用管理機能の概要

本装置はセットアップ作業が終了し，装置の電源 ON で運用に入ります。本装置と接続した運用端末では，運用コマンドやコンフィグレーションコマンドを実行し，装置の状態を調べたり，接続ネットワークの変更に伴うコンフィグレーションの変更を実施したりできます。本装置で実施する運用管理の種類を次の表に示します。

表 4-2　運用管理の種類

運用機能	概要
コマンド入力機能	コマンドラインによる入力を受け付けます。
ログイン制御機能	不正アクセス防止，パスワードチェックを行います。
コンフィグレーション編集機能	運用のためのコンフィグレーションを設定します。設定された情報はすぐ運用に反映されます。
ネットワークコマンド機能	リモート操作コマンドなどをサポートします。
ログ・統計情報	過去に発生した障害情報および回線使用率などの統計情報を表示します。
LED および障害部位の表示	LED によって本装置の状態を表示します。
MIB 情報収集	SNMP マネージャによるネットワーク管理を行います。
装置保守機能	装置を保守するための状態表示，装置とネットワークの障害を切り分けるための回線診断などのコマンドを持ちます。
MC 保守機能	MC のフォーマットなどを行います。

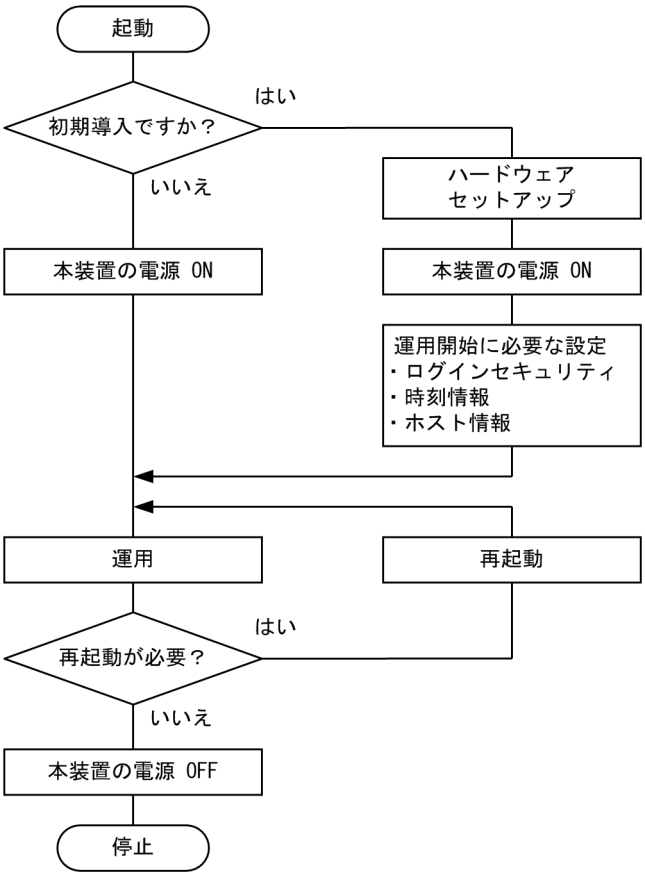
4.2　装置起動

この節では，装置の起動と停止について説明します。

4.2.1　起動から停止までの概略

本装置の起動から停止までの概略フローを次の図に示します。ハードウェアセットアップの内容については「ハードウェア取扱説明書」を参照してください。

図 4-3　起動から停止までの概略フロー



4.2.2　装置の起動

本装置の起動，再起動の方法を次の表に示します。

表 4-3　起動，再起動の方法

起動の種類	内容	操作方法
電源 ON による起動	本装置の電源 OFF からの立ち上げです。	本装置に取り付けた電源ケーブルをコンセントに差し込むことで電源を ON にします。
コマンドによる再起動	障害発生などにより，本装置をリセットしたい場合に行います。	reload コマンドを実行します。

本装置を起動，再起動したときに ST1 LED が橙点灯となった場合は，「トラブルシューティングガイド」を参照してください。また，LED ランプ表示内容の詳細は，「ハードウェア取扱説明書」を参照してください。

本装置は，ソフトウェアイメージを k.img という名称で書き込んだ MC をスロットに挿入して起動した場合，MC から起動します。MC から装置を起動した場合，アカウント，コンフィグレーションは工場出荷時の初期状態となり，設定しても保存することはできません。通常運用時は MC から起動しないでください。

4.2.3　装置の停止

本装置の電源を OFF にする場合は，アクセス中のファイルが壊れるおそれがあるので，本装置にログインしているユーザがいない状態で行ってください。運用コマンド reload stop で装置を停止させたあとに電源を OFF にすることを推奨します。本装置に取り付けた電源ケーブルをコンセントから抜くことで，電源を OFF にできます。

4.3　ログイン・ログアウト

この節では，ログインとログアウトについて説明します。

(1)　ログイン

装置が起動すると，ログイン画面を表示します。この画面でユーザ名とパスワードを入力してください。正しく認証された場合は，コマンドプロンプトを表示します。また，認証に失敗した場合は”Login incorrect”のメッセージを表示し，ログインできません。ログイン画面を次の図に示します。

なお，初期導入時には，ユーザ名 operator でパスワードなしでログインができます。

図 4-4　ログイン画面

```
login: operator
Password:                                                    …1
No password is set. Please set password!                     …2

Copyright (c) 20XX ALAXALA Networks Corporation. All rights reserved.

>                                                            …3
```

1. パスワードが設定されていない場合は改行だけでログインができます。
   また，パスワードの入力文字は表示しません。
2. 本装置に設定したパスワード未設定のログインユーザ（operator も含む）でログインした場合に表示されます。
3. コマンドプロンプトを表示します。

(2)　ログアウト

CLI での操作を終了してログアウトしたい場合は logout コマンドまたは exit コマンドを実行してください。ログアウト画面を次の図に示します。

図 4-5　ログアウト画面

```
> logout
login:
```

(3)　自動ログアウト

一定時間（デフォルト：60 分）内にキーの入力がなかった場合，自動的にログアウトします。なお，自動ログアウト時間はコンフィグレーションコマンド username，または運用コマンド set exec-timeout で変更できます。

5 コマンド操作

この章では，本装置でのコマンドの指定方法について説明します。

5.1　コマンド入力モード

5.1.1　コマンド一覧

コマンド入力モードの切り換えおよびユーティリティに関する運用コマンド一覧を次の表に示します。

表 5-1　運用コマンド一覧

コマンド名	説明
enable	コマンド入力モードを一般ユーザモードから装置管理者モードに変更します。
disable	コマンド入力モードを装置管理者モードから一般ユーザモードに変更します。
quit	現在のコマンド入力モードを終了します。
exit	現在のコマンド入力モードを終了します。
logout	装置からログアウトします。
configure (configure terminal)	コマンド入力モードを装置管理者モードからコンフィグレーションコマンドモードに変更して，コンフィグレーションの編集を開始します。
diff※	指定した二つのファイル同士を比較し，相違点を表示します。
grep※	指定したファイルを検索して，指定したパターンを含む行を出力します。
more※	指定したファイルの内容を一画面分だけ表示します。
less※	指定したファイルの内容を一画面分だけ表示します。
tail※	指定したファイルの指定された位置以降を出力します。
hexdump※	ヘキサダンプを表示します。

注※
「運用コマンドレファレンス」「8　ユーティリティ」を参照してください。

5.1.2　コマンド入力モード

本装置でコンフィグレーションの変更を実施したり，または装置の状態を参照したりする場合，適切なコマンド入力モードに遷移し，コンフィグレーションコマンドや運用コマンドを入力する必要があります。また，CLI プロンプトでコマンド入力モードを識別できます。

コマンド入力モードとプロンプトの対応を次の表に示します。

表 5-2　コマンド入力モードとプロンプトの対応

コマンド入力モード	実行可能なコマンド	プロンプト
一般ユーザモード	運用コマンド（configure，adduser コマンドなど，一部のコマンドは装置管理者モードでだけ実行可能です。）	>
装置管理者モード		#
コンフィグレーションコマンドモード	コンフィグレーションコマンド※	(config)#

注※

コンフィグレーションの編集中に運用コマンドを実行したい場合，quit コマンドや exit コマンドによってコマンド入力モードを装置管理者モードに切り替えなくても，運用コマンドの先頭に「$」を付けた形式で入力することで実行できます。

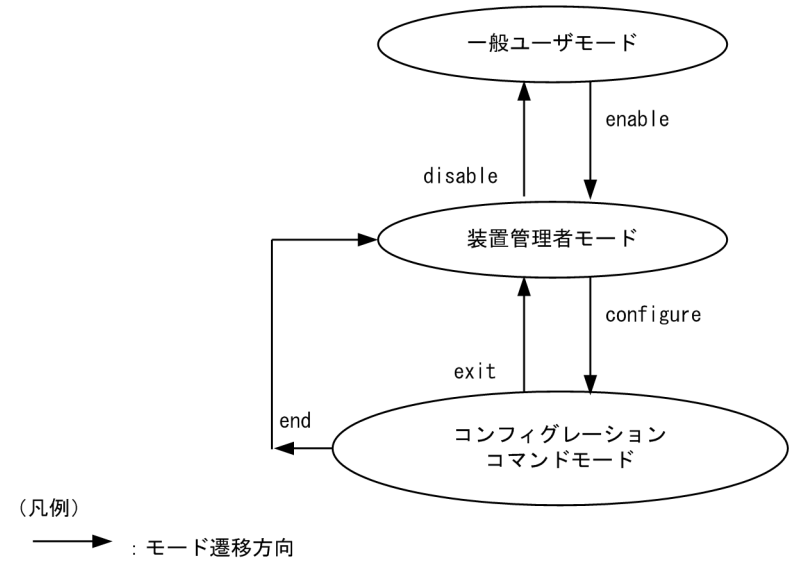
＜例＞

コンフィグレーションコマンドモードで運用コマンド show ip arp を実行する場合

```
(config)# $show ip arp
```

モード遷移の概要を次の図に示します。

図 5-1　モード遷移の概要



また，CLI プロンプトとして，次に示す場合でも，その状態を意味する文字がプロンプトの先頭に表示されます。

1. コンフィグレーションコマンド hostname でホスト名称を設定している場合，ホスト名称の先頭から 20 文字目までがプロンプトに反映されます。
2. ランニングコンフィグレーションを編集し，その内容をスタートアップコンフィグレーションに保存していない場合，プロンプトの先頭に「！」が付きます。

1.～2.のプロンプト表示例を次の図に示します。

図 5-2　プロンプト表示例

```
> enable
# configure
(config)# hostname ”OFFICE1”
!OFFICE1(config)# save
OFFICE1(config)# quit
OFFICE1# quit
OFFICE1>
```

5.2　CLI での操作

5.2.1　補完機能

コマンドライン上で［Tab］を入力することで，コマンド入力時のコマンド名称やファイル名の入力を少なくすることができ，コマンド入力が簡単になります。補完機能を使用したコマンド入力の簡略化を次の図に示します。

図 5-3　補完機能を使用したコマンド入力の簡略化

```
(config)# in[Tab]
(config)# interface
```

［Tab］押下で使用できるパラメータやファイル名の一覧が表示されます。

```
(config)# interface [Tab]
gigabitethernet     port-channel        tengigabitethernet
loopback            range               vlan
(config)# interface
```

5.2.2　ヘルプ機能

コマンドライン上で［?］を入力することで，指定できるコマンドまたはパラメータを検索できます。また，コマンドやパラメータの意味を知ることができます。次の図に［?］入力時の表示例を示します。

図 5-4　［?］入力時の表示例

```
> show vlan ?
  <vlan id list>        1 to 4094 ex. "5", "10-20" or "30,40"
  channel-group-number  Display the VLAN information specified by
                        channel-group-number
  detail                Display the detailed VLAN information
  list                  Display the list of VLAN information
  mac-vlan              Display the MAC VLAN information
  port                  Display the VLAN information specified by port number
  summary               Display the summary of VLAN information
  <cr>
> show vlan
```

なお，パラメータの入力途中でスペース文字を入れないで［?］を入力した場合は，補完機能が実行されます。また，コマンドパラメータで?文字を使用する場合は，［Ctrl］＋［V］を入力後，［?］を入力してください。

5.2.3　入力エラー位置指摘機能

コマンドまたはパラメータを不正に入力した際，エラー位置を「 ^ 」で指摘し，次行にエラーメッセージ（「運用コマンドレファレンス」「入力エラー位置指摘で表示するメッセージ」を参照）を表示します。［Tab］入力時と［?］入力時も同様となります。

「 ^ 」の指摘個所とエラーメッセージの説明によって，コマンドまたはパラメータを見直して再度入力してください。入力エラー位置指摘の表示例を「図 5-5　スペルミスをしたときの表示例」および「図 5-6　パラメータ入力途中の表示例」に示します。

図 5-5　スペルミスをしたときの表示例

```
(config)# interface gigabitehternet 1/0/1
interface gigabitehternet 1/0/1
                  ^
% illegal parameter at '^' marker
(config)# interface gigabitehternet 1/0/1
```

図 5-6　パラメータ入力途中の表示例

```
(config)# interface gigabitethernet 1/0/1
(config-if)# speed
speed
      ^
% Incomplete command at '^' marker
(config-if)#
```

5.2.4　コマンド短縮実行

コマンドまたはパラメータを短縮して入力し，入力された文字が一意のコマンドまたはパラメータとして認識できる場合，コマンドを実行します。短縮入力のコマンド実行例を次の図に示します。

図 5-7　短縮入力のコマンド実行例（show ip arp の短縮入力）

```
> sh ip ar
Date 20XX/11/15 19:37:02 UTC
Total: 1 entries
 IP Address       Linklayer Address  Netif            State      Type
 192.168.0.1      0012.e240.0a00     VLAN0100         STALE      arpa
```

なお，「表 6-1　コンフィグレーションコマンド一覧」にあるコンフィグレーションの編集および操作に関するコマンドは，コンフィグレーションモードの第一階層以外で短縮実行できません。

また，*を含むパラメータを指定した場合は，それ以降のパラメータについて短縮実行できません。

5.2.5　ヒストリ機能

ヒストリ機能を使用すると，過去に入力したコマンドを簡単な操作で再実行したり，過去に入力したコマンドの一部を変更して再実行したりできます。ヒストリ機能を使用した例を次の図に示します。

図 5-8　ヒストリ機能を使用したコマンド入力の簡略化

```
> ping 192.168.0.1 numeric count 1                          …1
PING 192.168.0.1 (192.168.0.1): 56(84) data bytes
64 bytes from 192.168.0.1: icmp_seq=0 ttl=31 time=1.329 ms

--- 192.168.0.1 PING Statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 1ms
rtt min/avg/max/mdev = 1.329/1.329/1.329/0.000 ms
>                                                           …2
> ping 192.168.0.1 numeric count 1                          …3
PING 192.168.0.1 (192.168.0.1): 56(84) data bytes
64 bytes from 192.168.0.1: icmp_seq=0 ttl=31 time=1.225 ms

--- 192.168.0.1 PING Statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 1ms
rtt min/avg/max/mdev = 1.225/1.225/1.225/0.000 ms
>                                                           …4
> ping 192.168.0.2 numeric count 1                          …5
PING 192.168.0.2 (192.168.0.2): 56(84) data bytes

--- 192.168.0.2 PING Statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms
>
```

1. 192.168.0.1 に対して ping コマンドを実行します。
2. [↑] キーを入力することで前に入力したコマンドを呼び出せます。
   この例の場合，[↑] キーを 1 回押すと「ping 192.168.0.1 numeric count 1」が表示されるので，[Enter] キーの入力だけで同じコマンドを再度実行できます。
3. 192.168.0.1 に対して ping コマンドを実行します。

4. [↑] キーを入力することで前に入力したコマンドを呼び出し，[←] キーおよび [Backspace] キーを使ってコマンド文字列を編集できます。

   この例の場合，[↑] キーを 1 回押すと「ping 192.168.0.1 numeric count 1」が表示されるので，IP アドレスの「1」の部分を「2」に変更して [Enter] キーを入力しています。

5. 192.168.0.2 に対して ping コマンドを実行します。

ヒストリ機能に次の表に示す文字列を使用した場合，コマンド実行前に過去に実行したコマンド文字列に変換したあとにコマンドを実行します。なお，コンフィグレーションコマンドでは，コマンド文字列変換はサポートしていません。

表 5-3　ヒストリのコマンド文字列変換で使用できる文字一覧

項番	指定	説明
1	!!	直前に実行したコマンドへ変換して実行します。
2	!n	ヒストリ番号 n※のコマンドへ変換して実行します。
3	!-n	n 回前のコマンドへ変換して実行します。
4	!str	文字列 str で始まる過去に実行した最新のコマンドへ変換して実行します。
5	^str1^str2	直前に実行したコマンドの文字列 str1 を str2 に置換して実行します。

注※

運用コマンド show history で表示される配列番号のこと。

また，過去に実行したコマンドを呼び出して，コマンド文字列を編集したり，[Backspace] キーや [Ctrl] ＋ [C] キーで消去したりしたあと，再度コマンドを呼び出すと，該当コマンドのヒストリを編集したり消去したりできます。

注意

通信ソフトウェアによって方向キー（[↑]，[↓]，[←]，[→]）を入力してもコマンドが呼び出されない場合があります。その場合は，通信ソフトウェアのマニュアルなどで設定を確認してください。

5.2.6　パイプ機能

パイプ機能を利用することによって，コマンドの実行結果を別のコマンドに引き継ぐことができます。実行結果を引き継ぐコマンドに grep コマンドを使うことによって，コマンドの実行結果をよりわかりやすくすることができます。ただし，コマンドが実行できなかった場合などに表示される応答メッセージは，引き継ぎをしないで，そのタイミングで画面に表示されます。「図 5-9　show sessions コマンド実行結果」に show sessions コマンドの実行結果を，「図 5-10　show sessions コマンド実行結果を grep コマンドでフィルタリング」に show sessions コマンドの実行結果を grep コマンドでフィルタリングした結果を示します。

図 5-9　show sessions コマンド実行結果

```
> show sessions
Date 20XX/01/07 12:00:00 UTC
operator console  -----  0   Jan  6 14:16
operator pts/0    -----  2   Jan  6 14:16 (192.168.3.7)
operator pts/1    -----  3   Jan  6 14:16 (192.168.3.7)
operator pts/2    admin  4   Jan  6 14:16 (192.168.3.7)
```

図 5-10　show sessions コマンド実行結果を grep コマンドでフィルタリング

```
> show sessions | grep admin
operator pts/2    admin  4   Jan  6 14:16 (192.168.3.7)
>
```

5.2.7　リダイレクト

リダイレクト機能を利用することによって，コマンドの実行結果をファイルに出力できます。ただし，コマンドが実行できなかった場合などに表示される応答メッセージは，ファイルに出力しないで，そのタイミングで画面に表示されます。show ip interface コマンドの実行結果をファイルに出力する例を次の図に示します。

図 5-11　show ip interface コマンド実行結果をファイルに出力

```
> show ip interface > show_interface.log
>
```

5.2.8　ページング

コマンドの実行により出力される結果について，表示すべき情報が一画面にすべて表示しきれない場合は，ユーザのキー入力を契機に一画面ごとに区切って表示します。ただし，リダイレクトがあるときにはページングを行いません。なお，ページングはコンフィグレーションコマンド username，または運用コマンド set terminal pager でその機能を有効にしたり無効にしたりできます。

5.2.9　CLI 設定のカスタマイズ

自動ログアウト機能や CLI 機能の一部は，CLI 環境情報としてユーザごとに動作をカスタマイズできます。カスタマイズ可能な CLI 機能と CLI 環境情報を次の表に示します。

表 5-4　カスタマイズ可能な CLI 機能と CLI 環境情報

機能	カスタマイズ内容と初期導入時のデフォルト設定
自動ログアウト	自動ログアウトするまでの時間を設定できます。 初期導入時のデフォルト設定は，60 分です。
ページング	ページングするかどうかを設定できます。 初期導入時のデフォルト設定は，ページングをします。
ヘルプ機能	ヘルプメッセージで表示するコマンドの一覧を設定できます。 初期導入時のデフォルト設定は，運用コマンドのヘルプメッセージを表示する際に，入力可能なすべての運用コマンドの一覧を表示します。

これらの CLI 環境情報は，ユーザごとに，コンフィグレーションコマンド username，または次に示す運用コマンドで設定できます。

- set exec-timeout
- set terminal pager
- set terminal help

コンフィグレーションコマンド username による設定は，運用コマンドによる設定よりも優先されます。三つの CLI 環境情報のうち，どれか一つでもコンフィグレーションコマンドで設定した場合，その対象ユーザには，運用コマンドによる設定値は使用されません。コンフィグレーションコマンドの設定値または省略時の初期値で動作します。

運用コマンドによる設定は，コンフィグレーションコマンドによる設定がない場合に使用されます。コンフィグレーションコマンドで一つも CLI 環境情報を設定していないユーザは，運用コマンドによる設定値が使用されます。なお，運用コマンドによる設定では，設定状態を表示できないため，各機能の動作状態で確認してください。

運用コマンドによる設定内容は，コマンドが実行されたセッションでは実行直後から動作に反映されます。同一ユーザでも別セッションの場合は，次回ログイン時に反映されます。また，コンフィグレーションコマンドによる設定で動作している場合でも，一時的に実行された該当セッションでの動作を変更できます。

なお，運用コマンドによる設定の場合，adduser コマンドで no-flash パラメータを指定して追加したアカウントのユーザは，装置を再起動したときに，CLI 環境情報が初期導入時のデフォルト設定に戻ります。

5.3　CLI の注意事項

(1)　ログイン後に運用端末がダウンした場合

ログイン後に運用端末がダウンした場合，本装置内ではログインしたままの状態になっていることがあります。この場合，自動ログアウトを待つか，再度ログインし直して，ログインしたままの状態になっているユーザを運用コマンド killuser で削除してください。

(2)　CLI の特殊キー操作に関する注意事項

［Ctrl］＋［C］キー，［Ctrl］＋［Z］キー，［Ctrl］＋［¥］キーのどれかを押した場合に，ごくまれにログアウトする場合があります。その場合は，再度ログインしてください。

6 コンフィグレーション

本装置には，ネットワークの運用環境に合わせて，構成および動作条件などのコンフィグレーションを設定しておく必要があります。この章では，コンフィグレーションを設定するのに必要なことについて説明します。

6.1　コンフィグレーション

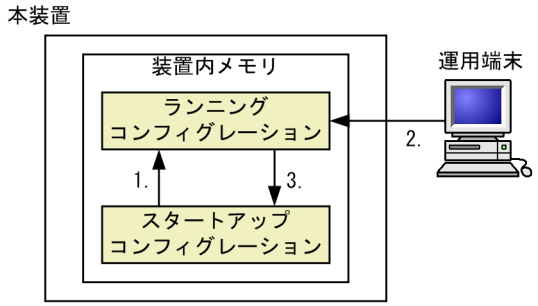
運用開始時または運用中，ネットワークの運用環境に合わせて，本装置に接続するネットワークの構成および動作条件などのコンフィグレーションを設定する必要があります。初期導入時，コンフィグレーションは設定されていません。

6.1.1　起動時のコンフィグレーション

本装置の電源を入れると，装置内メモリ上のスタートアップコンフィグレーションファイルが読み出され，設定されたコンフィグレーションに従って運用を開始します。運用に使用されているコンフィグレーションをランニングコンフィグレーションと呼びます。

なお，スタートアップコンフィグレーションは，直接編集できません。ランニングコンフィグレーションを編集したあとに save(write)コマンドを使用することで，スタートアップコンフィグレーションが更新されます。起動時，および運用中のコンフィグレーションの概要を次の図に示します。

図 6-1　起動時，および運用中のコンフィグレーションの概要



1. 本装置を起動すると，装置内メモリのスタートアップコンフィグレーションが読み出され，
   ランニングコンフィグレーションとしてロードされる。
   ランニングコンフィグレーションの内容で運用を開始する。
2. コンフィグレーションを変更した場合は，ランニングコンフィグレーションに反映される。
3. 変更されたランニングコンフィグレーションをスタートアップコンフィグレーションに
   保存する。

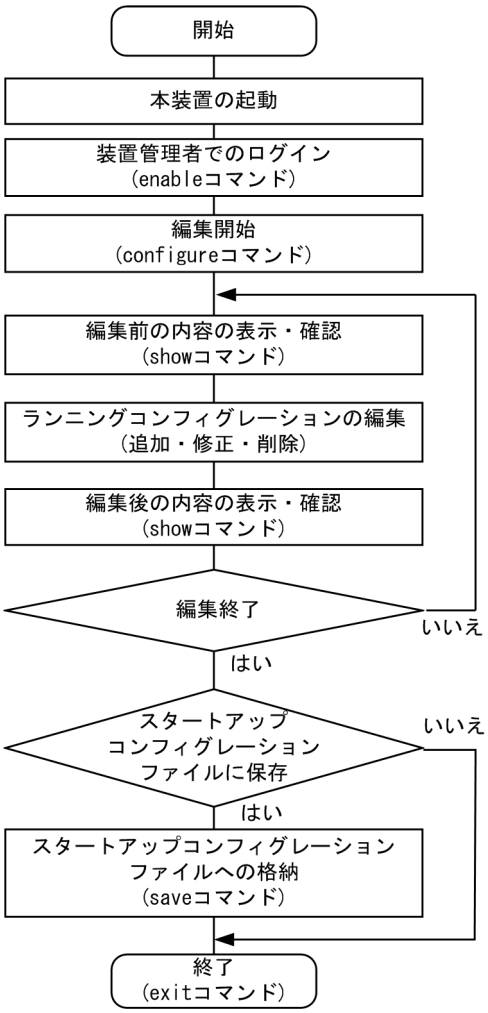
6.1.2　運用中のコンフィグレーション

運用中にコンフィグレーションを編集すると，編集した内容はランニングコンフィグレーションとしてすぐに運用に反映されます。save(write)コマンドを使用することで，ランニングコンフィグレーションが装置内メモリにあるスタートアップコンフィグレーションに保存されます。編集した内容を保存しないで装置を再起動すると，編集した内容が失われるので注意してください。

6.2　ランニングコンフィグレーションの編集概要

初期導入時やネットワーク構成を変更する場合は，ランニングコンフィグレーションを編集します。なお，初期導入時のランニングコンフィグレーションの編集はコンソールから行う必要があります。ランニングコンフィグレーションの編集の流れを次の図に示します。詳細については，「6.4　コンフィグレーションの編集方法」を参照してください。

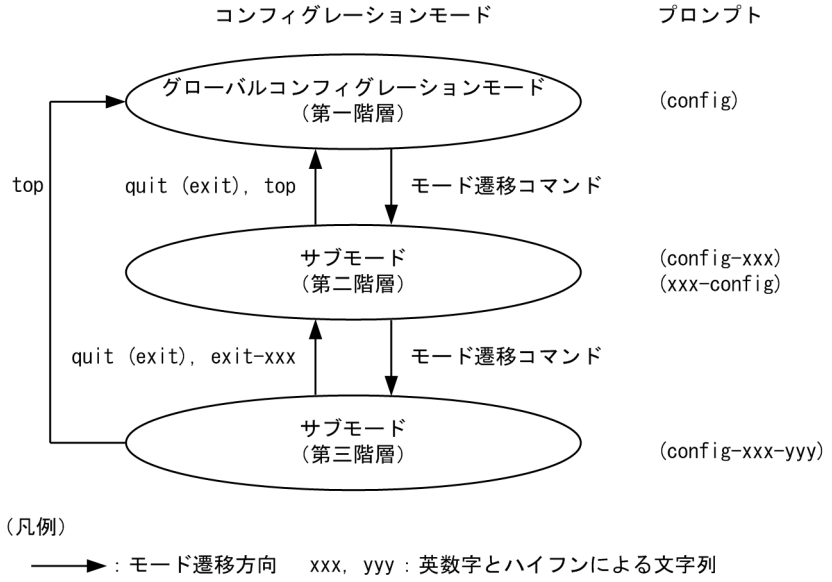
図 6-2　ランニングコンフィグレーションの編集の流れ



6.3　コンフィグレーションコマンド入力におけるモード遷移

コンフィグレーションは，実行可能なコンフィグレーションモードで編集します。第二階層のコンフィグレーションを編集する場合は，グローバルコンフィグレーションモードで第二階層のコンフィグレーションモードに移行するためのコマンドを実行してモードを移行した上で，コンフィグレーションコマンドを実行する必要があります。コンフィグレーションのモード遷移の概要を次の図に示します。

図 6-3　コンフィグレーションのモード遷移の概要



（凡例）

：モード遷移方向　xxx，yyy：英数字とハイフンによる文字列

6.4　コンフィグレーションの編集方法

6.4.1　コマンド一覧

コンフィグレーションの編集および操作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 6-1　コンフィグレーションコマンド一覧

コマンド名	説明
end	コンフィグレーションコマンドモードを終了して装置管理者モードに戻ります。
quit (exit)	モードを一つ戻ります。グローバルコンフィグレーションモードで編集中の場合は，コンフィグレーションコマンドモードを終了して装置管理者モードに戻ります。
save (write)	編集したコンフィグレーションをスタートアップコンフィグレーションに保存します。
show	編集中のコンフィグレーションを表示します。
status	編集中のコンフィグレーションの状態を表示します。
top	コンフィグレーションコマンドモードの第二階層以下からグローバルコンフィグレーションモード（第一階層）に戻ります。

コンフィグレーションの編集および操作に関する運用コマンド一覧を次の表に示します。

表 6-2　運用コマンド一覧

コマンド名	説明
show running-config	ランニングコンフィグレーションを表示します。
show startup-config	スタートアップコンフィグレーションを表示します。
copy	コンフィグレーションをコピーします。
erase configuration	ランニングコンフィグレーションの内容を初期導入時のものに戻します。
erase startup-config	スタートアップコンフィグレーションファイルの内容を初期導入時の状態に戻します。
show file	ローカルまたはリモートサーバ上のファイルの内容と行数を表示します。
cd	現在のディレクトリ位置を移動します。
pwd	カレントディレクトリのパス名を表示します。
ls	ファイルおよびディレクトリを表示します。
dir	復元可能な形式で削除された本装置用のファイルの一覧を表示します。
cat	指定されたファイルの内容を表示します。
cp	ファイルをコピーします。
mkdir	新しいディレクトリを作成します。
mv	ファイルの移動およびファイル名の変更をします。
rm	指定したファイルを削除します。

コマンド名	説明
rmdir	指定したディレクトリを削除します。
delete	本装置用のファイルを復元可能な形式で削除します。
undelete	復元可能な形式で削除された本装置用のファイルを復元します。
squeeze	復元可能な形式で削除された本装置用の deleted ファイルを完全に消去します。

6.4.2　configure（configure terminal）コマンド

コンフィグレーションを編集する場合は，enable コマンドを実行して装置管理者モードに移行してください。装置管理者モードで，configure コマンドまたは configure terminal コマンドを入力すると，プロンプトが「(config)#」になり，ランニングコンフィグレーションの編集が可能となります。ランニングコンフィグレーションの編集開始例を次の図に示します。

図 6-4　ランニングコンフィグレーションの編集開始例

```
> enable                  …1
# configure               …2
(config)#
```

1. enable コマンドで装置管理者モードに移行します。
2. ランニングコンフィグレーションの編集を開始します。

6.4.3　コンフィグレーションの表示・確認（show コマンド）

(1)　スタートアップコンフィグレーション，ランニングコンフィグレーションの表示・確認

装置管理者モードで運用コマンド show running-config／show startup-config を使用することで，ランニングコンフィグレーションおよびスタートアップコンフィグレーションを表示･確認できます。ランニングコンフィグレーションの表示例を次の図に示します。

図 6-5　ランニングコンフィグレーションの表示例

```
OFFICE01# show running-config                    …1
#default configuration file for AX2340S-24T4X
!
hostname "OFFICE01"
switch 1 provision 2340-24t4x
!
vlan 1
  name "VLAN0001"
!
vlan 100
  state active
!
vlan 200
  state active
!
interface gigabitethernet 1/0/1
  switchport mode access
  switchport access vlan 100
!
interface gigabitethernet 1/0/2
  switchport mode access
  switchport access vlan 200
!
OFFICE01#
```

1. ランニングコンフィグレーションを表示します。

(2)　コンフィグレーションの表示・確認

コンフィグレーションモードで show コマンドを使用することで，編集前，編集後のコンフィグレーションを表示・確認できます。コンフィグレーションを表示した例を「図 6-6　コンフィグレーションの内容をすべて表示」～「図 6-9　インタフェースモードで指定のインタフェース情報を表示」に示します。

図 6-6　コンフィグレーションの内容をすべて表示

```
OFFICE01(config)# show                  …1
#default configuration file for AX2340S-24T4X
!
hostname "OFFICE01"
switch 1 provision 2340-24t4x
!
vlan 1
  name "VLAN0001"
!
vlan 100
  state active
!
vlan 200
  state active
!
interface gigabitethernet 1/0/1
  switchport mode access
  switchport access vlan 100
!
interface gigabitethernet 1/0/2
  switchport mode access
  switchport access vlan 200
!
OFFICE01(config)#
```

1.パラメータを指定しない場合はランニングコンフィグレーションを表示します。

図 6-7　設定済みのすべてのインタフェース情報を表示

```
OFFICE01(config)# show interface gigabitethernet        …1
interface gigabitethernet 1/0/1
  switchport mode access
  switchport access vlan 100
!
interface gigabitethernet 1/0/2
  switchport mode access
  switchport access vlan 200
!
OFFICE01(config)#
```

1.ランニングコンフィグレーションのうち，設定済みのすべてのインタフェースを表示します。

図 6-8　指定のインタフェース情報を表示

```
OFFICE01(config)# show interface gigabitethernet 1/0/1       …1
interface gigabitethernet 1/0/1
  switchport mode access
  switchport access vlan 100
!
OFFICE01(config)#
```

1.ランニングコンフィグレーションのうち，インタフェース 1/0/1 を表示します。

図 6-9　インタフェースモードで指定のインタフェース情報を表示

```
OFFICE01(config)# interface gigabitethernet 1/0/1
OFFICE01(config-if)# show                               …1
interface gigabitethernet 1/0/1
  switchport mode access
  switchport access vlan 100
!
OFFICE01(config-if)#
```

1. ランニングコンフィグレーションのうち，インタフェース 1/0/1 を表示します。

6.4.4 コンフィグレーションの追加・変更・削除

(1) コンフィグレーションコマンドの入力

コンフィグレーションコマンドを使用して，コンフィグレーションを編集します。また，コンフィグレーションのコマンド単位での削除は，コンフィグレーションコマンドの先頭に「no」を指定することで実現できます。

ただし，機能の抑止を設定するコマンドでは，コンフィグレーションコマンドの先頭に「no」を指定して設定し，機能の抑止を解除する場合は「no」を外したコンフィグレーションコマンドを入力します。

コンフィグレーションの編集例を「図 6-10　コンフィグレーションの編集例」に，機能の抑止および解除の編集例を「図 6-11　機能の抑止および解除の編集例」に示します。

図 6-10　コンフィグレーションの編集例

```
(config)# vlan 100                                  …1
(config-vlan)# state active                         …2
(config-vlan)# exit
(config)# interface gigabitethernet 1/0/1           …3
(config-if)# switchport mode access                 …4
(config-if)# switchport access vlan 100             …5
(config-if)# exit
(config)#
(config)# vlan 100                                  …6
(config-vlan)# state suspend                        …7
(config-vlan)# exit
(config)#
(config)# interface gigabitethernet 1/0/1           …8
(config-if)# no switchport access vlan              …9
```

1. VLAN 100 をポート VLAN として設定します。
2. VLAN 100 を有効にします。
3. イーサネットインタフェース 1/0/1 にモードを遷移します。
4. ポート 1/0/1 にアクセスモードを設定します。
5. アクセス VLAN に 100 を設定します。
6. VLAN 100 にモードを遷移します。
7. VLAN 100 を有効から無効に変更します。
8. イーサネットインタフェース 1/0/1 にモードを遷移します。
9. 設定されているアクセス VLAN の VLAN ID 100 を削除します。

図 6-11　機能の抑止および解除の編集例

```
(config)# no ip domain lookup                       …1
(config)# ip domain name router.example.com         …2
(config)# ip name-server 192.168.0.1                …3
(config)# ip domain lookup                          …4
```

1. DNS リゾルバ機能を無効にします。
2. ドメイン名を router.example.com に設定します。
3. ネームサーバを 192.168.0.1 に設定します。
4. DNS リゾルバ機能を有効にします。

(2)　入力コマンドのチェック

コンフィグレーションコマンドを入力すると，入力されたコンフィグレーションに誤りがないかすぐにチェックされます。エラーがない場合は「図 6-12　正常入力時の出力」に示すようにプロンプトが表示されて，コマンドの入力待ちになります。ランニングコンフィグレーションの編集中の場合は，変更した内容がすぐに運用に使用されます。

エラーがある場合は「図 6-13　異常入力時のエラーメッセージ出力」に示すように，入力したコマンドの行の下にエラーの内容を示したエラーメッセージが表示されます。この場合，入力したコンフィグレーションは反映されないので，入力の誤りを正してから再度入力してください。

図 6-12　正常入力時の出力

```
(config)# interface gigabitethernet 1/0/1
(config-if)# description TokyoOsaka
(config-if)#
```

図 6-13　異常入力時のエラーメッセージ出力

```
(config)# interface tengigabitethernet 1/0/1
(config-if)# description
description
            ^
% Incomplete command at '^' marker
(config-if)#
```

6.4.5　コンフィグレーションのファイルへの保存（save コマンド）

save(write)コマンドを使用することで，編集したランニングコンフィグレーションをスタートアップコンフィグレーションファイルに保存できます。コンフィグレーションの保存例を次の図に示します。

図 6-14　コンフィグレーションの保存例

```
# configure                    …1
(config)#
        :
        :                      …2
        :
!(config)# save                …3
(config)#
```

1. ランニングコンフィグレーションの編集を開始します。
2. コンフィグレーションを変更します。
3. スタートアップコンフィグレーションファイルに保存します。

6.4.6　コンフィグレーションの編集終了（exit コマンド）

ランニングコンフィグレーションの編集を終了する場合は，グローバルコンフィグレーションモードで exit コマンドを実行します。コンフィグレーションを編集したあと，save コマンドで変更後の内容をスタートアップコンフィグレーションファイルへ保存していない場合は，exit コマンドを実行すると確認のメッセージが表示されます。スタートアップコンフィグレーションファイルに保存しないでコンフィグレーションコマンドモードを終了する場合は「y」を入力してください。「y」以外が入力されるとコンフィグレーションコマンドモードを終了できません。コンフィグレーションの編集終了例を「図 6-15　コンフィグレーションの編集終了例」と「図 6-16　変更内容を保存しない場合のコンフィグレーションの編集終了例」に示します。

図 6-15　コンフィグレーションの編集終了例

```
!(config)# save
(config)# exit                 …1
```

1.編集を終了します。

図 6-16 変更内容を保存しない場合のコンフィグレーションの編集終了例

```
# configure                                                                    …1
(config)#
        :
        :                                                                      …2
        :
!(config)# exit
Unsaved changes found! Do you exit ”configure” without save ? (y/n): y …3
!#
```

1.コンフィグレーションの編集を開始します。

2.コンフィグレーションを変更します。

3.確認メッセージが表示されます。

6.4.7 コンフィグレーションの編集時の注意事項

(1) 設定できるコンフィグレーションのコマンド数に関する注意事項

設定されたコンフィグレーションはメモリに保持されるため,設定できるコンフィグレーションのコマンド数はメモリ量によって決まります。設定するコンフィグレーションに比べてメモリ量が少なかったり,制限を超えるようなコンフィグレーションを編集したりした場合は,「Maximum number of entries are already defined (config memory shortage). <IP>」または「Maximum number of entries are already defined.<IP>」のメッセージが表示されます。このような場合,むだなコンフィグレーションが設定されていないか確認してください。

(2) コンフィグレーションをコピー＆ペーストで入力する際の注意事項

コンフィグレーションをコピー＆ペーストで入力する場合,一行に入力できる文字数は 1000 文字,一度に入力できる文字数は 4000 文字未満（スペース,改行を含む）です。4000 文字以上を一度にペーストすると正しくコンフィグレーションを設定できない状態になるので注意してください。

4000 文字を超えるコンフィグレーションを設定する場合は,一行を 1000 文字,一度のペーストを 4000 文字未満で複数回にわけてコピー＆ペーストを行ってください。

6.5　コンフィグレーションの操作

この節では，コンフィグレーションのバックアップ，ファイル転送などの操作について説明します。

6.5.1　コンフィグレーションのバックアップ

運用コマンド copy を使用することで，コンフィグレーションをリモートサーバや本装置上にバックアップすることができます。ただし，本装置にバックアップ用のコンフィグレーションファイルを格納する場合，スタートアップコンフィグレーションファイルの格納ディレクトリ（/config）は指定できません。バックアップ用のコンフィグレーションファイルはログインユーザのホームディレクトリに作成してください。

バックアップできるコンフィグレーションは，スタートアップコンフィグレーションとランニングコンフィグレーションの 2 種類です。運用中にコンフィグレーションを変更し保存していない場合は，スタートアップコンフィグレーションをバックアップしても，バックアップしたコンフィグレーションファイルの内容は運用中のコンフィグレーションと異なります。それぞれのバックアップ例を次の図に示します。

図 6-17　スタートアップコンフィグレーションのバックアップ例

```
> enable
# copy startup-config ftp://staff@192.168.0.1/backup.cnf
Configuration file copy to ftp://staff@192.168.0.1/backup.cnf?
(y/n): y

Authentication for 192.168.0.1.
User: staff
Password: xxx                                …1
transferring…

Data transfer succeeded.
#
```

1. リモートサーバ上のユーザ staff のパスワードを入力します。

図 6-18　ランニングコンフィグレーションのバックアップ例

```
> enable
# copy running-config ftp://staff@192.168.0.1/backup.cnf
Configuration file copy to ftp://staff@192.168.0.1/backup.cnf?
(y/n): y

Authentication for 192.168.0.1.
User: staff
Password: xxx                                …1
transferring…

Data transfer succeeded.
#
```

1. リモートサーバ上のユーザ staff のパスワードを入力します。

6.5.2　バックアップコンフィグレーションファイルの本装置への反映

バックアップコンフィグレーションファイルをスタートアップコンフィグレーションまたはランニングコンフィグレーションに反映する場合は，運用コマンド copy を使用します。それぞれの反映例を次の図に示します。

図 6-19　スタートアップコンフィグレーションへの反映例

```
> enable
# copy ftp://staff@192.168.0.1/backup.cnf startup-config
Configuration file copy to startup-config?
(y/n): y
```

```
Authentication for 192.168.0.1.
User: staff
Password: xxx                                …1
transferring…

Data transfer succeeded.
#
```

1.リモートサーバ上のユーザ staff のパスワードを入力します。

図 6-20 ランニングコンフィグレーションへの反映例

```
> enable
# copy ftp://staff@192.168.0.1/backup.cnf running-config
Configuration file copy to running-config?
(y/n): y

Authentication for 192.168.0.1.
User: staff
Password: xxx                                …1
transferring…

Data transfer succeeded.
#
```

1.リモートサーバ上のユーザ staff のパスワードを入力します。

6.5.3 ftp コマンドを使用したファイル転送

リモート運用端末との間でファイル転送をするときは ftp コマンドを使用します。

(1) バックアップコンフィグレーションファイルを本装置に転送する場合

バックアップコンフィグレーションファイルを格納するディレクトリ（/usr/home/operator）にバックアップコンフィグレーションファイルを転送後，運用コマンド copy を使用してスタートアップコンフィグレーションにコピーします。ftp コマンドを使用してバックアップコンフィグレーションファイルを本装置に転送する例を次の図に示します。

図 6-21 バックアップコンフィグレーションファイルの本装置へのファイル転送例（ftp コマンド）

```
> cd /usr/home/operator
> ftp 192.168.0.1
Connect to 192.168.0.1.
220  FTP server (Version wn-2.4(4) Wed Jan 1 00:00:00 JST 1999) ready.
Name (192.168.0.1:operator): test
331 Password required for test.
Password:xxxxxx
230 User test logged in.
Remote system type UNIX.
Using binary mode to transfer files.
ftp> get backup.cnf                                    …1
local: backup.cnf remote: backup.cnf
200 PORT command successful.
150 Opening BINARY mode data connection for backup.cnf (12,345 bytes)
226 Transfer complete.
ftp> bye
221 Goodby
> enable
# copy /usr/home/operator/backup.cnf startup-config    …2
Configuration file copy to startup-config ? (y/n): y   …3
#
```

1.バックアップコンフィグレーションファイルを転送します。

2.backup.cnf のバックアップコンフィグレーションファイルをスタートアップコンフィグレーションに使用します。

3.入れ替えてよいかどうかの確認です。

(2)　バックアップコンフィグレーションファイルをリモート運用端末へ転送する場合

本装置に格納したバックアップコンフィグレーションファイルをリモート運用端末へ転送する例を次の図に示します。

図 6-22　バックアップコンフィグレーションファイルのリモート運用端末へのファイル転送例

```
> cd /usr/home/operator
> enable
# copy running-config backup.cnf                              …1
Configuration file copy to /usr/home/operator/backup.cnf? (y/n) : y
# exit
> ftp 192.168.0.1
Connect to 192.168.0.1.
220  FTP server (Version wn-2.4(4) Fri Jan 1 00:00:00 JST 1999) ready.
Name (192.168.0.1:operator): test
331 Password required for test.
Password:xxxxxx
230 User test logged in.
Remote system type UNIX.
Using binary mode to transfer files.
ftp> put backup.cnf                                           …2
local: backup.cnf remote: backup.cnf
200 PORT command successful.
150 Opening BINARY mode data connection for backup.cnf (12,345 bytes)
226 Transfer complete.
ftp> bye
221 Goodby
>
```

1. 運用しているコンフィグレーションファイルをバックアップコンフィグレーションファイルへコピーします。
2. バックアップコンフィグレーションファイルを転送します。

6.5.4　MC を使用したファイル転送

MC にファイル転送をするときは cp コマンドを使用します。

(1)　バックアップコンフィグレーションファイルを本装置に転送する場合

バックアップコンフィグレーションファイルを格納するディレクトリ（/usr/home/operator）にバックアップコンフィグレーションファイルを MC から転送後，運用コマンド copy を使用してスタートアップコンフィグレーションにコピーします。cp コマンドを使用してバックアップコンフィグレーションファイルを本装置に転送する例を次の図に示します。

図 6-23　バックアップコンフィグレーションファイルの MC から本装置へのファイル転送例（cp コマンド）

```
> cd /usr/home/operator
> cp mc-file backup.cnf backup.cnf                            …1
> enable
# copy /usr/home/operator/backup.cnf startup-config           …2
Configuration file copy to startup-config? (y/n): y           …3
#
```

1. バックアップコンフィグレーションファイルを MC から転送します。
2. backup.cnf のバックアップコンフィグレーションファイルを運用に使用します。
3. 入れ替えてよいかどうかの確認です。

(2)　バックアップコンフィグレーションファイルを MC に転送する場合

本装置に格納したバックアップコンフィグレーションファイルを MC に転送する例を次の図に示します。

図 6-24　バックアップコンフィグレーションファイルの MC へのファイル転送例

```
> cd /usr/home/operator
> enable
# copy running-config backup.cnf                              …1
Configuration file copy to /usr/home/operator/backup.cnf? (y/n) : y
# exit
> cp backup.cnf mc-file backup.cnf                             …2
>
```

1. 運用しているコンフィグレーションファイルをバックアップコンフィグレーションファイルへコピーします。
2. バックアップコンフィグレーションファイルを MC へ転送します。

6.5.5　バックアップコンフィグレーションファイル反映時の注意事項

運用コマンド copy を使用して，バックアップコンフィグレーションファイルをランニングコンフィグレーションにコピーする場合，運用中のポートが再起動しますので，ネットワーク経由でログインしている場合は注意してください。

バックアップコンフィグレーションファイルの内容が本装置の構成と一致していない場合は，バックアップコンフィグレーションファイルの内容を変更してから運用コマンド copy を使用してください。本装置の構成と一致していないバックアップコンフィグレーションファイルに copy コマンドを実行すると，copy コマンドがエラー終了するか，copy コマンドが正常終了しても運用には正常に反映されないことがあります。その際は，バックアップコンフィグレーションファイルの内容を変更してから，再度 copy コマンドを実行してください。

7 リモート運用端末から本装置へのログイン

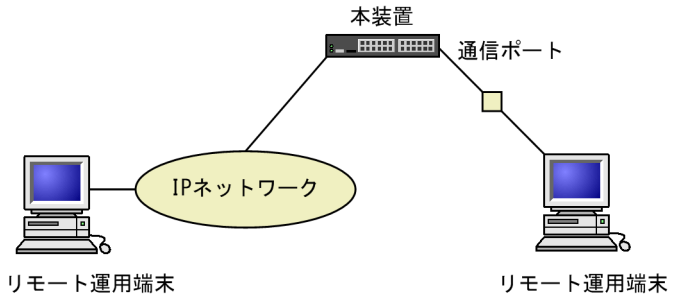
この章では, リモート運用端末から本装置へのリモートアクセスについて説明します。

7.1　解説

7.1.1　通信用ポート接続

通信用ポートを介して，リモート運用端末から本装置へログインするには，本装置で VLAN や IP アドレスなどの設定が必要です。ただし，初期導入時には，VLAN や IP アドレスなどの設定が行われていません。そのため，コンソールからログインして，コンフィグレーションを設定する必要があります。

図 7-1　リモート運用端末からの本装置へのログイン



7.2　コマンドガイド

7.2.1　コマンド一覧

運用端末の接続とリモート操作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 7-1　コンフィグレーションコマンド一覧

コマンド名	説明
ftp-server	リモート運用端末から ftp プロトコルを使用したアクセスを許可します。
line console	コンソール（RS232C）のパラメータを設定します。
line vty	装置へのリモートアクセスを許可します。
speed	コンソール（RS232C）の通信速度を設定します。
transport input	リモート運用端末から各種プロトコルを使用したアクセスを規制します。

運用端末の接続とリモート操作に関する運用コマンド一覧を次の表に示します。

表 7-2　運用コマンド一覧

コマンド名	説明
set exec-timeout	自動ログアウトが実行されるまでの時間を設定します。
set terminal help	ヘルプメッセージで表示するコマンドの一覧を設定します。
set terminal pager	ページングの実施／未実施を設定します。
show history	過去に実行した運用コマンドの履歴を表示します（コンフィグレーションコマンドの履歴は表示しません）。
telnet	指定された IP アドレスのリモート運用端末と仮想端末と接続します。
ftp	本装置と TCP/IP で接続されているリモート端末との間でファイル転送をします。
tftp	本装置と接続されているリモート端末との間で UDP でファイル転送をします。

SSH の設定については，「9　SSH(Secure Shell)」を参照してください。

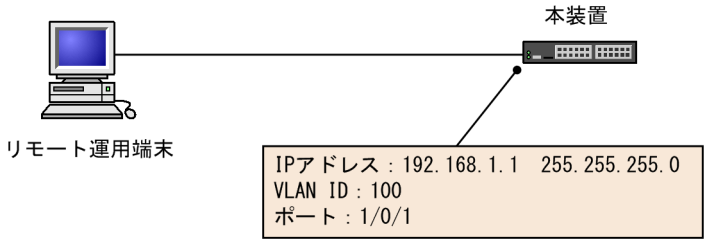
VLAN の設定，および IP インタフェースの設定に関するコンフィグレーションコマンドについては，「24　VLAN」，「31　IPv4 通信」，または「32　IPv6 通信」を参照してください。

7.2.2　本装置への IP アドレスの設定

［設定のポイント］

リモート運用端末から本装置へアクセスするためには，あらかじめ，接続するインタフェースに対して IP アドレスを設定しておく必要があります。

図 7-2　リモート運用端末との接続例



[コマンドによる設定]

1. **(config)# vlan 100**
   (config-vlan)# exit
   VLAN ID 100 のポート VLAN を作成し，VLAN 100 の VLAN コンフィグレーションモードに移行します。
2. **(config)# interface gigabitethernet 1/0/1**
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 100
   (config-if)# exit
   ポート 1/0/1 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。ポート 1/0/1 を VLAN 100 のアクセスポートに設定します。
3. **(config)# interface vlan 100**
   (config-if)# ip address 192.168.1.1 255.255.255.0
   (config-if)# exit
   (config)#
   VLAN ID 100 の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。VLAN ID 100 に IPv4 アドレス 192.168.1.1，サブネットマスク 255.255.255.0 を設定します。

7.2.3　telnet によるログインを許可する

[設定のポイント]

あらかじめ，IP アドレスを設定しておく必要があります。

リモート運用端末から本装置に telnet プロトコルによるリモートログインを許可するコンフィグレーションコマンド line vty を設定します。

このコンフィグレーションが設定されていない場合，コンソールからだけ本装置にログインできます。

[コマンドによる設定]

1. **(config)# line vty 0 2**
   (config-line)#
   リモート運用端末から本装置への telnet プロトコルによるリモートアクセスを許可します。また，装置に同時にリモートログインできるユーザ数を最大 3 に設定します。

7.2.4　ftp によるログインを許可する

[設定のポイント]

あらかじめ，IP アドレスを設定しておく必要があります。

リモート運用端末から本装置に ftp プロトコルによるリモートアクセスを許可するコンフィグレーションコマンド ftp-server を設定します。

このコンフィグレーションを実施していない場合，ftp プロトコルを用いた本装置へのアクセスはできません。

[コマンドによる設定]

1. (config)# ftp-server

リモート運用端末から本装置への ftp プロトコルによるリモートアクセスを許可します。

8 ログインセキュリティと RADIUS/TACACS+

この章では，本装置のログイン制御，ログインセキュリティ，アカウンティング，および RADIUS/TACACS+について説明します。

8.1　ログインセキュリティのコマンドガイド

8.1.1　コマンド一覧

ログインセキュリティ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 8-1　コンフィグレーションコマンド一覧

コマンド名	説明
aaa authentication enable	装置管理者モードへの変更（enable コマンド）時に使用する認証方式を指定します。
aaa authentication enable attribute-user-per-method	装置管理者モードへの変更（enable コマンド）時の認証に使用するユーザ名属性を変更します。
aaa authentication enable end-by-reject	装置管理者モードへの変更（enable コマンド）時の認証で，否認された場合に認証を終了します。
aaa authentication login	リモートログイン時に使用する認証方式を指定します。
aaa authentication login console	コンソール（RS232C）からのログイン時に aaa authentication login コマンドで指定した認証方式を使用します。
aaa authentication login end-by-reject	ログイン時の認証で，否認された場合に認証を終了します。
aaa authorization commands	RADIUS サーバまたは TACACS+サーバによるコマンド承認をする場合に指定します。
aaa authorization commands console	コンソール(RS232C)からのログインの場合に aaa authorization commands コマンドで指定したコマンド承認を行います。
banner	ユーザのログイン前およびログイン後に表示するメッセージを設定します。
commands exec	ローカル（コンフィグレーション）によるコマンド承認で使用するコマンドリストに，コマンド文字列を追加します。
ip access-group	本装置へリモートログインを許可または拒否するリモート運用端末の IPv4 アドレスを指定したアクセスリストを設定します。
ipv6 access-class	本装置へリモートログインを許可または拒否するリモート運用端末の IPv6 アドレスを指定したアクセスリストを設定します。
parser view	ローカル（コンフィグレーション）によるコマンド承認で使用するコマンドリストを生成します。
username	指定ユーザに，ローカル（コンフィグレーション）によるコマンド承認で使用するコマンドリストまたはコマンドクラスを設定します。

ログインセキュリティに関する運用コマンド一覧を次の表に示します。

表 8-2　運用コマンド一覧

コマンド名	説明
adduser	新規ログインユーザ用のアカウントを追加します。
rmuser	adduser コマンドで登録されているログインユーザのアカウントを削除します。

コマンド名	説明
password	ログインユーザのパスワードを変更します。
clear password	ログインユーザのパスワードを削除します。
show sessions	本装置にログインしているユーザを表示します。
show whoami	本装置にログインしているユーザの中で，このコマンドを実行したログインユーザだけを表示します。
killuser	ログイン中のユーザを強制的にログアウトさせます。

8.1.2　ログイン制御の概要

本装置にはローカルログイン（シリアル接続）と IPv4 および IPv6 ネットワーク経由のリモートログイン機能（telnet）があります。

本装置ではログイン時およびログイン中に次に示す制御を行っています。

1. ログイン時に不正アクセスを防止するため，ユーザ ID によるコマンドの使用範囲の制限やパスワードによるチェックを設けています。
2. 複数の運用端末から同時にログインできます。
3. 本装置にログインできるリモートユーザ数は最大 16 ユーザです。なお，コンフィグレーションコマンド line vty でログインできるユーザ数を制限できます。
4. 本装置にアクセスできる IPv4 および IPv6 アドレスをコンフィグレーションコマンド ip access-list standard，ipv6 access-list，access-list，ip access-group，ipv6 access-class で制限できます。
5. 本装置にアクセスできるプロトコル（telnet，ftp）をコンフィグレーションコマンド transport input や ftp-server で制限できます。
6. コマンド実行結果はログインした端末だけに表示します。運用メッセージはログインしているすべての運用端末に表示されます。
7. 入力したコマンドとその応答メッセージおよび運用メッセージを運用ログとして収集します。運用ログは運用コマンド show logging で参照できます。
8. キー入力が最大 60 分間ない場合は自動的にログアウトします。
9. 運用コマンド killuser を使用してユーザを強制ログアウトできます。

8.1.3　ログインユーザの作成と削除

adduser コマンドを用いて本装置にログインできるユーザを作成してください。ログインユーザの作成例を次の図に示します。

図 8-1　ユーザ newuser を作成

```
> enable
# adduser newuser
User(empty password) add done. Please setting password.

Changing local password for newuser.
New password:********                                   … 1
Retype new password:********                            … 2
# quit
>
```

1. パスワードを入力します（実際には入力文字は表示されません）。

2. 確認のため再度パスワードを入力します（実際には入力文字は表示されません）。

また，使用しなくなったユーザは rmuser コマンドを用いて削除できます。

特に，初期導入時に設定されているログインユーザ”operator”を運用中のログインユーザとして使用しない場合，セキュリティの低下を防ぐため，新しいログインユーザを作成したあとに rmuser コマンドで削除することをお勧めします。また，コンフィグレーションコマンド aaa authentication login で，RADIUS/TACACS+を使用したログイン認証ができます。コンフィグレーションの設定例については，「8.3.2　RADIUS サーバによる認証の設定」および「8.3.3　TACACS+サーバによる認証の設定」を参照してください。

なお，作成したログインユーザ名とパスワードは忘れないように管理してください。ログインユーザ名とパスワードが分からなくなると，本装置へログインできなくなるので注意してください。

8.1.4　装置管理者モード変更のパスワードの設定

コンフィグレーションコマンドを実行するためには enable コマンドで装置管理者モードに変更する必要があります。初期導入時に enable コマンドを実行した場合，パスワードは設定されていませんので認証なしで装置管理者モードに変更します。ただし，通常運用中にすべてのユーザがパスワード認証なしで装置管理者モードに変更できるのはセキュリティ上危険ですので，初期導入時にパスワードを設定しておいてください。なお，設定したパスワードは忘れないように管理してください。パスワードが分からなくなると，コンフィグレーションコマンドを実行できなくなります。

パスワード設定の実行例を次の図に示します。

図 8-2　初期導入直後の装置管理者モード変更のパスワード設定

```
> enable
# password enable-mode
Changing local password for admin.
New password:
Retype new password:
#
```

また，コンフィグレーションコマンド aaa authentication enable で，RADIUS/TACACS+を使用した認証ができます。コンフィグレーションの設定例については，「8.3.2　RADIUS サーバによる認証の設定」および「8.3.3　TACACS+サーバによる認証の設定」を参照してください。

8.1.5　リモート運用端末からのログインの許可

コンフィグレーションコマンド line vty を設定することで，リモート運用端末から本装置へログインできるようになります。このコンフィグレーションが設定されていない場合，コンソールからだけ本装置にログインできます。リモート運用端末からのログインを許可する設定例を次の図に示します。

図 8-3　リモート運用端末からのログインを許可する設定例

```
(config)# line vty 0 2
(config-line)#
```

また，リモート運用端末から ftp プロトコルを用いて，本装置にアクセスする場合には，コンフィグレーションコマンド ftp-server を設定する必要があります。本設定を実施しない場合，ftp プロトコルを用いた本装置へのアクセスはできません。

図 8-4　ftp プロトコルによるアクセス許可の設定例

```
(config)# ftp-server
(config)#
```

8.1.6　同時にログインできるユーザ数の設定

コンフィグレーションコマンド line vty を設定することで，リモート運用端末から本装置へログインできるようになります。line vty コマンドの<num>パラメータで，リモートログインできるユーザ数が制限されます。なお，この設定にかかわらず，コンソールからは常にログインできます。2 人まで同時にログインを許可する設定例を次の図に示します。

図 8-5　同時にログインできるユーザ数の設定例

```
(config)# line vty 0 1
(config-line)#
```

同時ログインに関する動作概要を次に示します。

- 複数ユーザが同時にログインすると，ログインしているユーザ数が制限数以下でもログインできない場合があります。
- 同時にログインできるユーザ数を変更しても，すでにログインしているユーザのセッションが切れることはありません。

8.1.7　リモート運用端末からのログインを許可する IP アドレスの設定

リモート運用端末から本装置へのログインを許可する IP アドレスを設定することで，ログインを制限できます。なお，設定後はリモート運用端末から本装置へのログインの可否を確認してください。

[設定のポイント]

特定のリモート運用端末からだけ，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，ipv6 access-list，access-list，ip access-group，ipv6 access-class 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。アクセスを許可する IPv4 アドレスとサブネットマスク，または IPv6 アドレスとプレフィックスは，合わせて最大 128 個の登録ができます。このコンフィグレーションを実施していない場合，すべてのリモート運用端末から本装置へのアクセスが可能となります。

[コマンドによる設定]（IPv4 の場合）

1. **(config)# ip access-list standard REMOTE**
   (config-std-nacl)# permit 192.168.0.0 0.0.0.255
   (config-std-nacl)# exit
   ネットワーク（192.168.0.0/24）からだけログインを許可するアクセスリスト情報 REMOTE を設定します。
2. **(config)# line vty 0 2**
   (config-line)# ip access-group REMOTE in
   (config-line)#
   line モードに遷移し，アクセスリスト情報 REMOTE を適用し，ネットワーク（192.168.0.0/24）にあるリモート運用端末からだけログインを許可します。

[コマンドによる設定]（IPv6 の場合）

1. **(config)# ipv6 access-list REMOTE6**
   (config-ipv6-nacl)# permit ipv6 2001:db8:1::/64 any
   (config-ipv6-nacl)# exit

ネットワーク（2001:db8:1::/64）からだけログインを許可するアクセスリスト情報 REMOTE6 を設定します。

2. **(config)# line vty 0 2**
   (config-line)# ipv6 access-class REMOTE6 in
   (config-line)#
   line モードに遷移し，アクセスリスト情報 REMOTE6 を適用し，ネットワーク（2001:db8:1::/64）にあるリモート運用端末からだけログインを許可します。

8.1.8　ログインバナーの設定

コンフィグレーションコマンド banner でログインバナーの設定を行うと，console から，またはリモート運用端末の telnet や ftp クライアントなどから本装置に接続したとき，ログインする前やログインしたあとにメッセージを表示できます。

[設定のポイント]

リモート運用端末の telnet や ftp クライアントからネットワークを介して本装置の telnet や ftp サーバへ接続するとき，ログインする前に次のメッセージを表示させます。

```
##########################################
Warning!!! Warning!!! Warning!!!
This is our system. You should not login.
Please close connection.
##########################################
```

[コマンドによる設定]

1. **(config)# banner login plain-text**
   --- Press CTRL+D or only '.' line to end ---
   ##
   Warning!!! Warning!!! Warning!!!
   This is our system. You should not login.
   Please close connection.
   ##
   .
   ログイン前メッセージのスクリーンイメージを入力します。
   入力が終わったら，"."（ピリオド）だけの行（または CTRL+D）を入力します。
2. **(config)# show banner**
   banner login encode
   "IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjCldhcm5pbmchISEgV2FybmluZyEhISBXYX
   JuaW5nISEhClRoaXMgaXMgb3VyIHN5c3RlbS4gW91IHNob3VsZCBub3QgbG9naW4uClBsZWFzZSBjbG9zZSBjb25uZ
   WN0aW9uLgojIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMK"
   入力されたメッセージは自動的にエンコードされて設定されます。
3. **(config)# show banner login plain-text**
   ##
   Warning!!! Warning!!! Warning!!!
   This is our system. You should not login.
   Please close connection.
   ##

(config)#

show の際に plain- text パラメータを指定すると，テキスト形式で確認できます。

設定が完了したら，リモート運用端末の telnet または ftp クライアントから本装置へ接続します。接続後，クライアントにメッセージが表示されます。

図 8-6　リモート運用端末から本装置へ接続した例（telnet で接続した場合）

```
> telnet 10.10.10.10
Trying 10.10.10.10...
Connected to 10.10.10.10.
Escape character is '^]'.

##########################################
Warning!!! Warning!!! Warning!!!
This is our system. You should not login.
Please close connection.
##########################################
login:
```

図 8-7　リモート運用端末から本装置へ接続した例（ftp で接続した場合）

```
> ftp 10.10.10.10
Connected to 10.10.10.10.
220-
##########################################
Warning!!! Warning!!! Warning!!!
This is our system. You should not login.
Please close connection.
##########################################
220 10.10.10.10 FTP server ready.
Name (10.10.10.10:staff):
```

8.2　RADIUS/TACACS+の解説

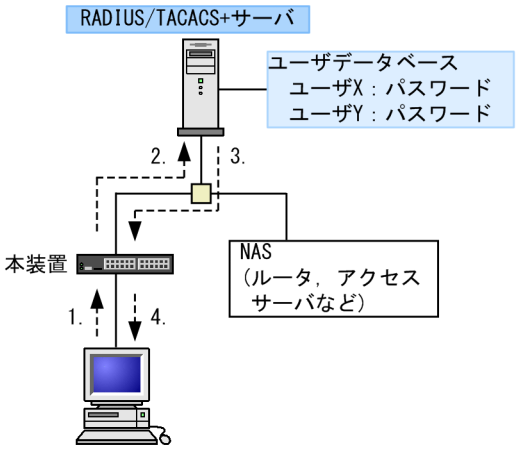
8.2.1　RADIUS/TACACS+の概要

RADIUS（Remote Authentication Dial In User Service），TACACS+（Terminal Access Controller Access Control System Plus）とは，NAS（Network Access Server）に対して認証，承認，およびアカウンティングを提供するプロトコルです。NAS は RADIUS/TACACS+のクライアントとして動作するリモートアクセスサーバ，ルータなどの装置のことです。NAS は構築されている RADIUS/TACACS+サーバに対してユーザ認証，コマンド承認，およびアカウンティングなどのサービスを要求します。RADIUS/TACACS+サーバはその要求に対して，サーバ上に構築された管理情報データベースに基づいて要求に対する応答を返します。本装置は NAS の機能をサポートします。

RADIUS/TACACS+を使用すると一つの RADIUS/TACACS+サーバだけで，複数 NAS でのユーザパスワードなどの認証情報や，コマンド承認情報やアカウンティング情報を一元管理できるようになります。本装置では，RADIUS/TACACS+サーバに対してユーザ認証，コマンド承認，およびアカウンティングを要求できます。

RADIUS/TACACS+認証の流れを次の図に示します。

図 8-8　RADIUS/TACACS+認証の流れ



1. リモート運用端末からユーザXが本装置にtelnetを実行する。
2. 本装置はコンフィグレーションで指定したRADIUS/TACACS+サーバに対して認証を要求する。
3. RADIUS/TACACS+サーバはユーザデータベースに基づいてユーザXを認証し，本装置にユーザXを認証したことを通知する。
4. 本装置はRADIUS/TACACS+認証に基づいて，ユーザXのリモート運用端末からのtelnet許可する。
5. 本装置はコンフィグレーションでコマンド承認を設定した場合，RADIUS/TACACS+サーバに設定してあるコマンドリストに従って，ユーザが投入する運用コマンドを許可／制限する。

8.2.2　RADIUS/TACACS+の適用機能および範囲

本装置では RADIUS/TACACS+を，運用端末からのログイン認証と装置管理者モードへの変更（enable コマンド）時の認証，コマンド承認，およびアカウンティングに使用します。また，RADIUS は IEEE802.1X および Web 認証の端末認証にも使用します。RADIUS/TACACS+機能のサポート範囲を次に示します。

(1)　RADIUS/TACACS+の適用範囲

RADIUS/TACACS+認証を適用できる操作を次に示します。

- 本装置への telnet
- 本装置への ssh
- 本装置への ftp
- 本装置への sftp
- 本装置への scp
- コンソール（RS232C)からのログイン
- 装置管理者モードへの変更（enable コマンド）

RADIUS/TACACS+コマンド承認を適用できる操作を次に示します。

- 本装置への telnet
- 本装置への ssh
- コンソール（RS232C）からのログイン

RADIUS/TACACS+アカウンティングを適用できる操作を次に示します。

- 本装置への telnet によるログイン・ログアウト
- 本装置への ssh によるログイン・ログアウト
- 本装置への ftp によるログイン・ログアウト
- 本装置への sftp によるログイン・ログアウト
- 本装置への scp によるログイン・ログアウト
- コンソール（RS232C）からのログイン・ログアウト
- CLI でのコマンド入力（TACACS+だけサポート）

(2)　RADIUS のサポート範囲

RADIUS サーバに対して，本装置がサポートする NAS 機能を次の表に示します。

表 8-3　RADIUS のサポート範囲

分類	内容
文書全体	NAS に関する記述だけを対象にします。
パケットタイプ	ログイン認証，装置管理者モードへの変更（enable コマンド）時の認証，コマンド承認で使用する次のタイプ • Access-Request (送信) • Access-Accept (受信) • Access-Reject (受信) アカウンティングで使用する次のタイプ • Accounting-Request (送信) • Accounting-Response (受信)

分類	内容
属性	ログイン認証と装置管理者モードへの変更（enable コマンド）時の認証で使用する次の属性 • User-Name • User-Password • Service-Type • NAS-IP-Address • NAS-IPv6-Address • NAS-Identifier • Reply-Message コマンド承認で使用する次の属性 • Class • Vendor-Specific(Vendor-ID=21839) アカウンティングで使用する次の属性 • User-Name • NAS-IP-Address • NAS-IPv6-Address • NAS-Port • NAS-Port-Type • Service-Type • Calling-Station-Id • Acct-Status-Type • Acct-Delay-Time • Acct-Session-Id • Acct-Authentic • Acct-Session-Time

(a)　使用する RADIUS 属性の内容

使用する RADIUS 属性の内容を次の表に示します。

RADIUS サーバを利用してコマンド承認する場合は，認証時に下の表に示すような Class や Vendor-Specific を返すようにあらかじめ RADIUS サーバを設定しておく必要があります。RADIUS サーバには，ベンダー固有属性を登録(dictionary ファイルなどに設定)してください。コマンド承認の属性詳細については「8.2.4　RADIUS/TACACS+/ローカルを使用したコマンド承認」を参照してください。

表 8-4　使用する RADIUS 属性の内容

属性名	属性値	パケットタイプ	内容
User-Name	1	Access-Request Accounting-Request	認証するユーザの名前。 ログイン認証の場合は，ログインユーザ名を送信します。 装置管理者モードへの変更（enable コマンド）時の認証の場合は，「表 8-9　設定するユーザ名属性」に従ってユーザ名を送信します。

属性名	属性値	パケットタイプ	内容
User-Password	2	Access-Request	認証ユーザのパスワード。送信時には暗号化されます。
Service-Type	6	Access-Request Accounting-Request	Login(値=1)。Administrative(値=6，ただしパケットタイプが Access-Request の場合だけ使用)。Access-Accept および Access-Reject に添付された場合は無視します。
NAS-IP-Address	4	Access-Request Accounting-Request	本装置の IP アドレス。ローカルアドレスが設定されている場合はローカルアドレス，ローカルアドレスが設定されていない場合は送信インタフェースの IP アドレスになります。
NAS-IPv6-Address	95	Access-Request Accounting-Request	本装置の IPv6 アドレス。ローカルアドレスが設定されている場合はローカルアドレス，ローカルアドレスが設定されていない場合は送信インタフェースの IPv6 アドレスになります。ただし，IPv6 リンクローカルアドレスで通信する場合は，ローカルアドレス設定の有無にかかわらず送信インタフェースの IPv6 リンクローカルアドレスになります。
NAS-Identifier	32	Access-Request Accounting-Request	本装置の装置名。装置名が設定されていない場合は添付されません。
Reply-Message	18	Access-Accept Access-Reject Accounting-Response	サーバからのメッセージ。添付されている場合は，運用ログとして出力されます。
Class	25	Access-Accept	ログインクラス。コマンド承認で適用します。
Vendor-Specific	26	Access-Accept	ログインリスト。コマンド承認で適用します。
NAS-Port	5	Accounting-Request	ユーザが接続されている NAS のポート番号を指します。本装置では，tty ポート番号を格納します。ただし，ftp の場合は 100 を格納します。
NAS-Port-Type	61	Accounting-Request	NAS に接続した方法を指します。本装置では，telnet/ftp は Virtual(5), コンソールは Async(0)を格納します。
Calling-Station-Id	31	Accounting-Request	利用者の識別 ID を指します。本装置では，telnet/ftp はクライアントの IP アドレス，コンソールは“console”を格納します。
Acct-Status-Type	40	Accounting-Request	Accounting-Request がどのタイミングで送信されたかを指します。本装置では，ユーザのログイン時に Start(1)，ログアウト時に Stop(2)を格納します。
Acct-Delay-Time	41	Accounting-Request	送信する必要のあるイベント発生から Accounting-Request を送信するまでにかかった時間(秒)を格納します。
Acct-Session-Id	44	Accounting-Request	セッションを識別するための文字列を指します。本装置では，セッションのプロセス ID を格納します。

属性名	属性値	パケットタイプ	内容
Acct-Authentic	45	Accounting-Request	ユーザがどのように認証されたかを指します。本装置では，RADIUS(1)，Local(2)，Remote(3)の 3 種類を格納します。
Acct-Session-Time	46	Accounting-Request（Acct-Status-Type が Stop の場合だけ）	ユーザがサービスを利用した時間(秒)を指します。本装置では，ユーザがログイン後ログアウトするまでの時間(秒)を格納します。

- Access-Request パケット
  本装置が送信するパケットには，この表で示す以外の属性は添付しません。
- Access-Accept，Access-Reject，Accounting-Response パケット
  この表で示す以外の属性が添付されていた場合，本装置ではそれらの属性を無視します。

(3)　TACACS+のサポート範囲

TACACS+サーバに対して，本装置がサポートする NAS 機能を次の表に示します。

表 8-5　TACACS+のサポート範囲

分類		内容
パケットタイプ		ログイン認証と装置管理者モードへの変更（enable コマンド）時の認証で使用する次のタイプ • Authentication Start (送信) • Authentication Reply(受信) • Authentication Continue (送信) コマンド承認で使用する次のタイプ • Authorization Request (送信) • Authorization Response (受信) アカウンティングで使用する次のタイプ • Accounting Request (送信) • Accounting Reply (受信)
ログイン認証 装置管理者モードへの変更（enable コマンド）時の認証	属性	• User • Password • priv-lvl
コマンド承認	service	• taclogin
	属性	• class • allow-commands • deny-commands
アカウンティング	flag	• TAC_PLUS_ACCT_FLAG_START • TAC_PLUS_ACCT_FLAG_STOP
	属性	• task_id • start_time

分類		内容
		• stop_time • elapsed_time • timezone • service • priv-lvl • cmd

(a)　使用する TACACS+属性の内容

使用する TACACS+属性の内容を次の表に示します。

TACACS+サーバを利用してコマンド承認する場合は，認証時に class または allow-commands や deny-commands 属性とサービスを返すように TACACS+サーバ側で設定します。コマンド承認の属性詳細については「8.2.4　RADIUS/TACACS+/ローカルを使用したコマンド承認」に示します。

表 8-6　使用する TACACS+属性の内容

service	属性	説明
-	User	認証するユーザの名前。 ログイン認証の場合は，ログインユーザ名を送信します。 装置管理者モードへの変更（enable コマンド）時の認証の場合は，「表 8-9　設定するユーザ名属性」に従ってユーザ名を送信します。
	Password	認証ユーザのパスワード。送信時には暗号化されます。
	priv-lvl	認証するユーザの特権レベル。 ログイン認証の場合，1 を使用します。装置管理者モードへの変更（enable コマンド）時の認証の場合，15 を使用します。
taclogin	class	コマンドクラス
	allow-commands	許可コマンドリスト
	deny-commands	制限コマンドリスト

（凡例）－：該当なし

アカウンティング時に使用する TACACS+ flag を次の表に示します。

表 8-7　TACACS+アカウンティング flag 一覧

flag	内容
TAC_PLUS_ACCT_FLAG_START	アカウンティング START パケットを示します。ただし，aaa コンフィグレーションで送信契機に stop-only を指定している場合は，アカウンティング START パケットは送信しません。
TAC_PLUS_ACCT_FLAG_STOP	アカウンティング STOP パケットを示します。ただし，aaa コンフィグレーションで送信契機に stop-only を指定している場合は，このアカウンティング STOP パケットだけを送信します。

アカウンティング時に使用する TACACS+属性(Attribute-Value)の内容を次の表に示します。

表 8-8　TACACS+アカウンティング Attribute-Value 一覧

Attribute	Value
task_id	イベントごとに割り当てられる ID です。本装置ではアカウンティングイベントのプロセス ID を格納します。
start_time	イベントを開始した時刻です。本装置ではアカウンティングイベントが開始された時刻を格納します。この属性は次のイベントで格納されます。 • 送信契機 start-stop 指定時のログイン時，コマンド実行前 • 送信契機 stop-only 指定時のコマンド実行前
stop_time	イベントを終了した時刻です。本装置ではアカウンティングイベントが終了した時刻を格納します。この属性は次のイベントで格納されます。 • 送信契機 start-stop 指定時のログアウト時，コマンド実行後 • 送信契機 stop-only 指定時のログアウト時
elapsed_time	イベント開始からの経過時間(秒)です。本装置ではアカウンティングイベントの開始から終了までの時間(秒)を格納します。この属性は次のイベントで格納されます。 • 送信契機 start-stop 指定時のログアウト時，コマンド実行後 • 送信契機 stop-only 指定時のログアウト時
timezone	タイムゾーン文字列を格納します。
service	文字列“shell”を格納します。
priv-lvl	コマンドアカウンティング設定時に，入力されたコマンドが運用コマンドの場合は 1，コンフィグレーションコマンドの場合は 15 を格納します。
cmd	コマンドアカウンティング設定時に，入力されたコマンド文字列（最大 250 文字）を格納します。

8.2.3　RADIUS/TACACS+を使用した認証

RADIUS/TACACS+を使用した認証方法について説明します。

(1)　認証サービスの選択

ログイン認証および装置管理者モードへの変更（enable コマンド）時の認証に使用するサービスは複数指定できます。指定できるサービスは RADIUS，TACACS+および adduser/password コマンドによる本装置単体でのログインセキュリティ機能です。

これらの認証方式は単独でも同時でも指定できます。同時に指定された場合に先に指定された方式で認証に失敗したときの認証サービスの選択動作を，次に示す end-by-reject を設定するコンフィグレーションコマンドで変更できます。

ログイン認証の場合

　aaa authentication login end-by-reject

装置管理者モードへの変更（enable コマンド）時の認証の場合

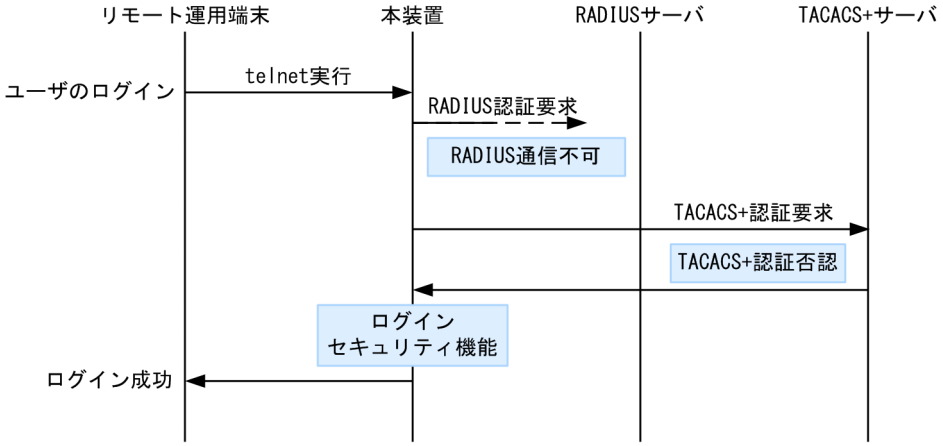
　aaa authentication enable end-by-reject

(a)　end-by-reject 未設定時

end-by-reject 未設定時の認証サービスの選択について説明します。end-by-reject 未設定時は，先に指定された方式で認証に失敗した場合に，その失敗の理由に関係なく，次に指定された方式で認証できます。

例として，コンフィグレーションで認証方式に RADIUS，TACACS+，単体でのログインセキュリティの順番で指定し，それぞれの認証結果が RADIUS サーバ通信不可，TACACS+サーバ認証否認，ログインセキュリティ機能認証成功となる場合の認証方式シーケンスを次の図に示します。

図 8-9　認証方式シーケンス（end-by-reject 未設定時）



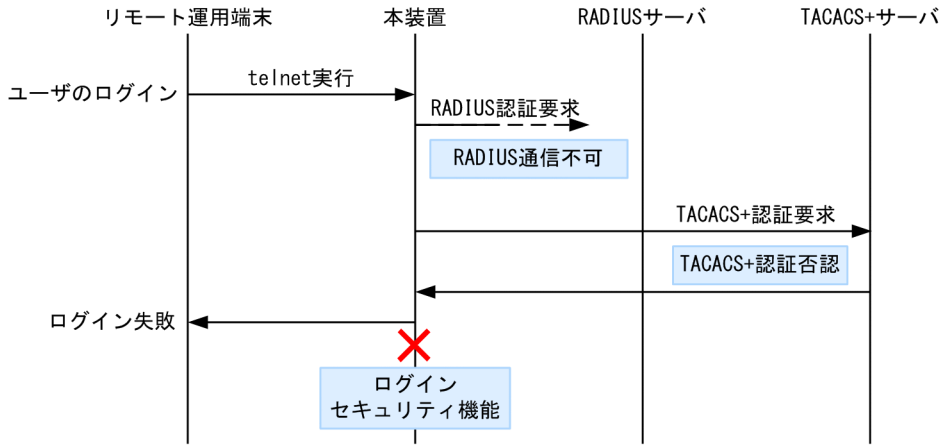
この図で端末からユーザが本装置に telnet を実行すると，RADIUS サーバに対し本装置から RADIUS 認証を要求します。RADIUS サーバとの通信不可によって RADIUS サーバでの認証に失敗すると，次に TACACS+サーバに対し本装置から TACACS+認証を要求します。TACACS+認証否認によって TACACS+サーバでの認証に失敗すると，次に本装置のログインセキュリティ機能での認証を実行します。ここで認証に成功し，ユーザは本装置へのログインに成功します。

(b)　end-by-reject 設定時

end-by-reject 設定時の認証サービスの選択について説明します。end-by-reject 設定時は，先に指定された方式で認証否認された場合に，次に指定された方式で認証を行いません。否認された時点で認証を終了し，一連の認証が失敗となります。通信不可などの異常によって認証が失敗した場合だけ，次に指定された方式で認証できます。

例として，コンフィグレーションで認証方式に RADIUS，TACACS+，単体でのログインセキュリティの順番で指定し，それぞれの認証結果が RADIUS サーバ通信不可，TACACS+サーバ認証否認となる場合の認証方式シーケンスを次の図に示します。

図 8-10　認証方式シーケンス（end-by-reject 設定時）



この図で端末からユーザが本装置に telnet を実行すると，RADIUS サーバに対し本装置から RADIUS 認証を要求します。RADIUS サーバとの通信不可によって RADIUS サーバでの認証に失敗すると，次に TACACS+サーバに対し本装置から TACACS+認証を要求します。TACACS+認証否認によって TACACS+サーバでの認証に失敗すると，この時点で一連の認証が失敗となり，認証を終了します。次に指定されている本装置のログインセキュリティ機能での認証を実行しません。その結果，ユーザは本装置へのログインに失敗します。

(2)　RADIUS/TACACS+サーバの選択

RADIUS サーバ，TACACS+サーバはそれぞれ最大四つまで指定できます。一つのサーバと通信できず，認証サービスが受けられない場合は，順次これらのサーバへの接続を試行します。

また，RADIUS サーバ，TACACS+サーバをホスト名で指定したときに，複数のアドレスが解決できた場合は，優先順序に従い，アドレスを一つだけ決定し，RADIUS サーバ，TACACS+サーバと通信します。

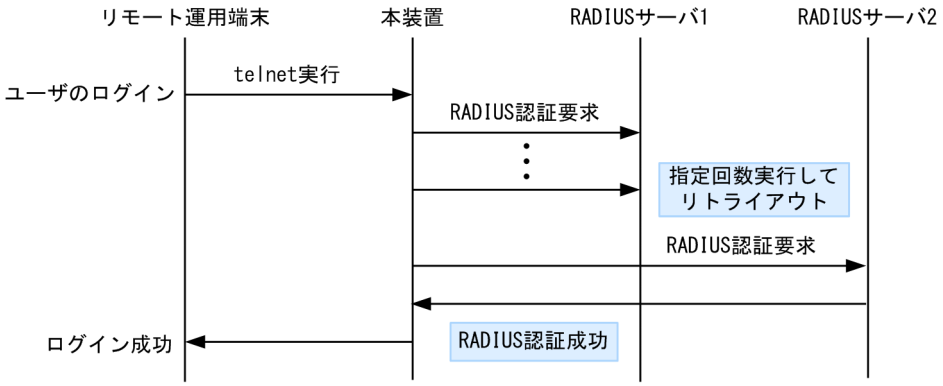
優先順序についての詳細は，「11　ホスト名と DNS　11.1　解説」を参照してください。

注意

DNS サーバを使用してホスト名を解決する場合，DNS サーバとの通信に時間が掛かることがあります。このため，RADIUS サーバ，TACACS+サーバは IP アドレスで指定することをお勧めします。

RADIUS/TACACS+サーバと通信不可を判断するタイムアウト時間を設定できます。デフォルト値は 5 秒です。また，各 RADIUS サーバでタイムアウトした場合は，再接続を試行します。この再試行回数も設定でき，デフォルト値は 3 回です。このため，ログイン方式として RADIUS が使用できないと判断するまでの最大時間は，タイムアウト時間×リトライ回数×RADIUS サーバ設定数になります。なお，各 TACACS+サーバでタイムアウトした場合は，再接続を試行しません。このため，ログイン方式として TACACS+が使用できないと判断するまでの最大時間は，タイムアウト時間×TACACS+サーバ設定数になります。RADIUS サーバ選択のシーケンスを次の図に示します。

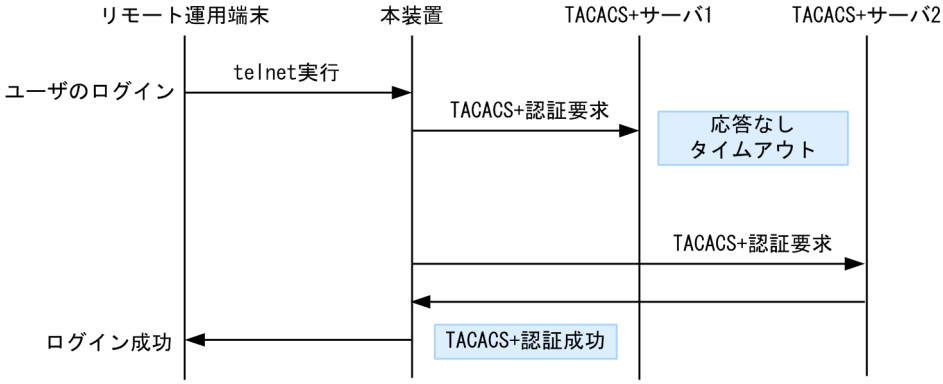
図 8-11　RADIUS サーバ選択のシーケンス



この図でリモート運用端末からユーザが本装置に telnet を実行すると，RADIUS サーバ 1 に対し本装置から RADIUS 認証を要求します。RADIUS サーバ 1 と通信できなかった場合は，続いて RADIUS サーバ 2 に対して RADIUS 認証を実行します。ここで認証に成功し，ユーザは本装置へのログインに成功します。

TACACS+サーバ選択のシーケンスを次の図に示します。

図 8-12　TACACS+サーバ選択のシーケンス



この図でリモート運用端末からユーザが本装置に telnet を実行すると，TACACS+サーバ 1 に対し本装置から TACACS+認証を要求します。TACACS+サーバ 1 と通信できなかった場合は，続いて TACACS+サーバ 2 に対して TACACS+認証を実行します。ここで認証に成功し，ユーザは本装置へのログインに成功します。

(3)　RADIUS/TACACS+サーバへの登録情報

(a)　ログイン認証を使用する場合

RADIUS/TACACS+サーバにユーザ名およびパスワードを登録します。RADIUS/TACACS+サーバへ登録するユーザ名には次に示す 2 種類があります。

- 本装置に adduser コマンドを使用して登録済みのユーザ名
  本装置に登録されたユーザ情報を使用してログイン処理を行います。
- 本装置に未登録のユーザ名
  次に示す共通のユーザ情報でログイン処理を行います。
  - ユーザ ID：remote_user
  - ホームディレクトリ：/usr/home/remote_user

本装置に未登録のユーザでログインした場合の注意点を示します。

- ファイルの管理
  ファイルを作成した場合，すべて remote_user 管理となって，別のユーザでも，作成したファイルの読み込みおよび書き込みができます。重要なファイルは ftp などで外部に保管するなど，ファイルの管理に注意してください。

(b)　装置管理者モードへの変更（enable コマンド）時の認証を使用する場合

装置管理者モードへの変更（enable コマンド）用に，次のユーザ情報を登録してください。

- ユーザ名
  本装置ではユーザ名属性として，次の表に示すユーザ名をサーバに送信します。送信するユーザ名はコンフィグレーションコマンドで変更できます。対応するユーザ名をサーバに登録してください。

  表 8-9　設定するユーザ名属性

コマンド名	ユーザ名	
	RADIUS 認証	TACACS+認証
設定なし	admin	admin
aaa authentication enable attribute-user-per-method	$enab15$	ログインユーザ名

- 特権レベル
  特権レベルは 15 で固定です。

ただし，サーバによっては，送信したユーザ名属性に関係なく特定のユーザ名（例えば$enab15$）を使用する場合や，特権レベルの登録が不要な場合などがあります。詳細は，使用するサーバのマニュアルを確認してください。

8.2.4　RADIUS/TACACS+/ローカルを使用したコマンド承認

RADIUS/TACACS+/ローカル（コンフィグレーション）を使用したコマンド承認方法について説明します。

(1)　コマンド承認の概要

RADIUS サーバ，TACACS+サーバ，またはローカルパスワードによる認証の上ログインしたユーザに対し，使用できる運用コマンドの種類を制限することができます。これをコマンド承認と呼びます。使用できる運用コマンドは，RADIUS サーバまたは TACACS+サーバから取得する，コマンドクラスおよびコマンドリスト，またはコンフィグレーションで設定したコマンドクラスおよびコマンドリストに従い制御を行います。また，制限した運用コマンドは，CLI の補完機能で補完候補として表示しません。なお，<option>や<Host Name>などの，<>で囲まれたパラメータ部分の値や文字列を含んだ運用コマンドを，許可するコマンドリストに指定した場合は，<>部分は補完候補として表示しません。

図 8-13　RADIUS/TACACS+サーバによるログイン認証，コマンド承認

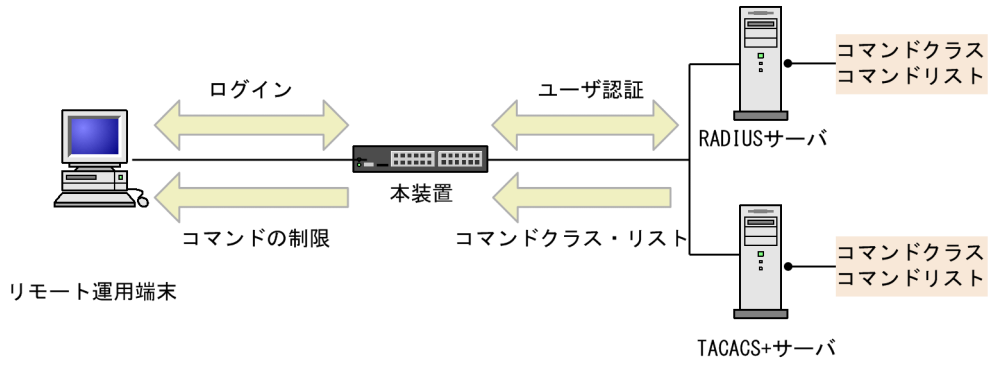
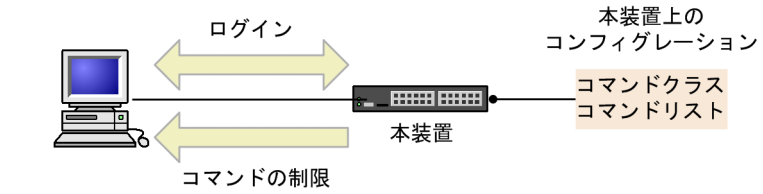


図 8-14　ローカルによるログイン認証，コマンド承認



本装置の aaa コンフィグレーションでコマンド承認を設定すると，RADIUS/TACACS+指定時は，ログイン認証と同時に，サーバからコマンドリストを取得します。ローカル指定時は，ログイン認証と同時に，コンフィグレーションで設定されたコマンドリストを使用します。本装置ではこれらのコマンドリストに従ってログイン後の運用コマンドを許可／制限します。

図 8-15　RADIUS/TACACS+サーバによるコマンド承認のシーケンス

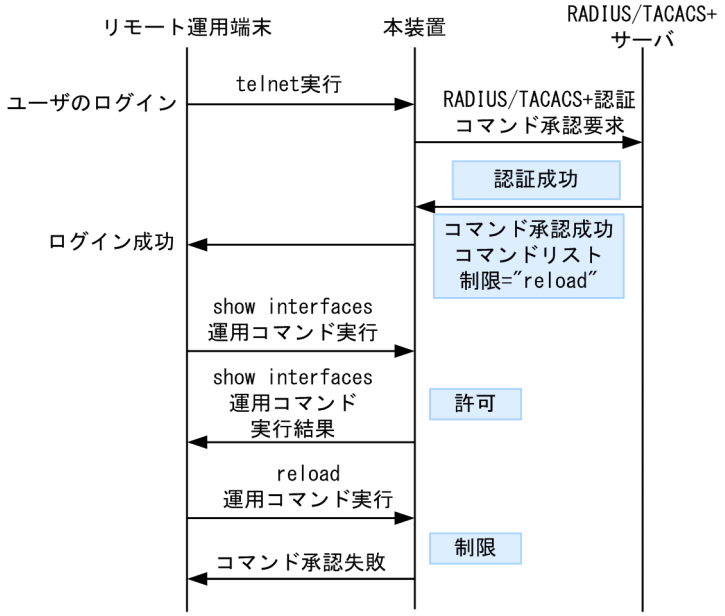
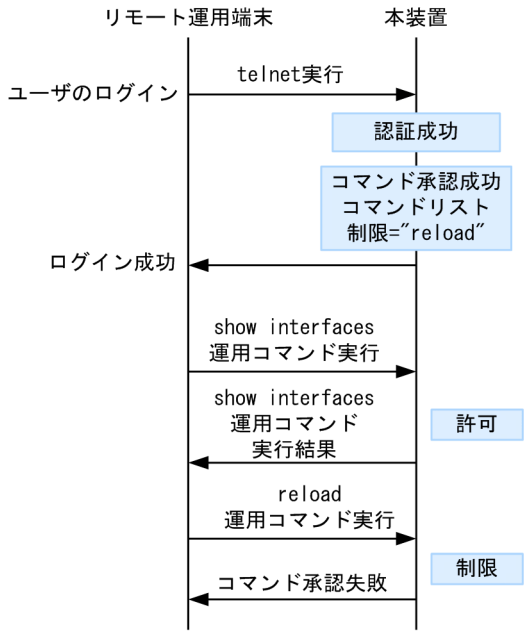


図 8-16　ローカルコマンド承認のシーケンス



「図 8-15　RADIUS/TACACS+サーバによるコマンド承認のシーケンス」で端末からユーザが本装置に telnet を実行すると，RADIUS/TACACS+サーバに対し本装置から認証，コマンド承認を要求します。認証成功時に RADIUS/TACACS+サーバからコマンドリストを取得し，ユーザは本装置にログインします。

「図 8-16　ローカルコマンド承認のシーケンス」で端末からユーザが本装置に telnet を実行すると，ローカル認証を行います。認証成功時にコンフィグレーションからコマンドリストを取得し，ユーザは本装置にログインします。

ログイン後，ユーザは本装置で運用コマンド show interfaces などを実行できますが，運用コマンド reload はコマンドリストによって制限されているために実行できません。

注意

RADIUS/TACACS+サーバのコマンドリストの設定を変更した場合またはコンフィグレーションのコマンドリストを変更した場合は，次回のログイン認証後から反映されます。

(2)　RADIUS/TACACS+/ローカルコマンド承認設定手順

RADIUS/TACACS+によるコマンド承認を使用するためには，次の手順で RADIUS/TACACS+サーバや本装置を設定します。

1. コマンド制限のポリシーを決める。
   各ユーザに対し，運用コマンドの中で，制限・許可するコマンドのポリシーを決めます。
2. コマンドリストを指定する。
   コマンドクラス以外に，許可／制限コマンドリストとして，許可コマンドと制限コマンドをそれぞれ指定できます。
3. RADIUS/TACACS+サーバを設定する。
   決定したコマンド制限ポリシーを基に，RADIUS または TACACS+のリモート認証サーバに，コマンド制限のための設定を行います。
4. 本装置のリモート認証を設定する。

本装置で RADIUS または TACACS+サーバのコンフィグレーション設定と aaa コンフィグレーション設定を行います。

5. コマンド承認の動作を確認する。
   RADIUS/TACACS+を使用したリモート運用端末から本装置へログインし，確認を行います。

ローカルコマンド承認を使用するためには，次の手順で本装置を設定します。

1. コマンド制限のポリシーを決める。
   各ユーザに対し，運用コマンドの中で，制限・許可するコマンドのポリシーを決めます。
2. コマンドリストを作成する。
   コマンドクラス以外に，コマンドリストとして許可コマンドと制限コマンドをそれぞれ指定できます。決定したコマンド制限ポリシーを基に，コマンドリストのコンフィグレーション設定を行います。
   なお，コマンドクラスだけを使用する場合は作成不要です。
3. ユーザにコマンドクラスまたはコマンドリストを割り当てる。
   各ユーザに対し，コマンドクラスまたはコマンドリストを割り当てる username コンフィグレーション設定を行います。
   その後に，aaa コンフィグレーション設定を行います。
4. コマンド承認の動作を確認する。
   本装置へローカル認証でログインし確認を行います。

(3)　コマンド制限のポリシー決定

各ユーザに対し，運用コマンドの中で，制限・許可するコマンドのポリシーを決めます。ここでは，各ユーザがログインしたときに，あるコマンド群は許可し，それ以外のコマンドは制限するなどを決めます。ポリシーは「(5)　RADIUS/TACACS+/ローカルコマンド承認の設定」で設定します。

コマンド制限・許可の対象となるのは，運用コマンドです。マニュアル未掲載のデバッグコマンド（ps コマンドなど）は対象外で，常に制限されます（許可が必要な場合は，次に説明するコマンドクラスで root を指定してコマンド無制限クラスとしてください）。なお，logout，exit，quit，disable，end，set terminal，show whoami，who am i コマンドに関しては常に許可されます。

本装置には，あらかじめ「コマンドクラス」として，以下のポリシーが定義されています。規定のコマンドクラスを選択することで，そのクラスの応じたコマンド制限を行うことができます。

表 8-10　コマンドクラス一覧

コマンドクラス	許可コマンド	制限コマンド
root 全コマンド無制限クラス	従来どおりすべてのコマンド（マニュアル未掲載のデバッグコマンドを含む）	なし
allcommand 運用コマンド無制限クラス	すべての運用コマンド"all"	なし（マニュアル未掲載のデバッグコマンドは不可）
noconfig コンフィグレーション変更制限クラス（コンフィグレーションコマンド指定も制限します）	制限以外の運用コマンド	"config, copy, erase configuration, erase startup-config"
nomanage ユーザ管理コマンド制限クラス	制限以外の運用コマンド	"adduser, rmuser, clear password, password, killuser"

コマンドクラス	許可コマンド	制限コマンド
noenable 装置管理者モードコマンド制限クラス	制限以外の運用コマンド	"enable"

また，コマンドクラス以外に，許可コマンドリストと制限コマンドリストをそれぞれ指定することもできます。

(4)　コマンドリストの指定方法について

コマンドクラス以外に，許可／制限コマンドリストとして，許可コマンドと制限コマンドをそれぞれ指定できます。コマンドを指定する場合は，各コマンドリストに設定対象のコマンド文字列をスペースも意識して指定します。複数指定する場合はコンマ(,)で区切って並べます。なお，ローカルコマンド承認では，コマンド文字列をコンフィグレーションコマンド commands exec で一つずつ設定します。本装置では，その設定されたコマンド文字列をコンマ(,)で連結したものをコマンドリストとして使用します。

コマンドリストで指定されたコマンド文字列と，ユーザが入力したコマンドの先頭部分とが，合致するかどうかを判定します(前方一致)。なお，特別な文字列として，all を指定できます。all は運用コマンドすべてを意味します。

判定時に，許可コマンドリストと制限コマンドリストの両方に合致した場合は，合致したコマンド文字数が多い方の動作を採用します（ただし，all 指定は文字数を 1 とします)。その際，許可コマンドリストと制限コマンドリストに同じコマンド文字列が指定されていた場合は，許可として判定されます。

また，コマンドクラスと許可／制限コマンドリストを同時に指定した場合は，コマンドクラスごとに規定されているコマンドリスト（「表 8-10　コマンドクラス一覧」中の" "で囲まれているコマンドリストに対応）と許可／制限コマンドリストを合わせて判定を行います。なお，コマンドクラスに root を指定した場合，許可／制限コマンドクラスの設定は無効となり，マニュアル未掲載のデバッグコマンド（ps コマンドなど）を含むすべてのコマンドが実行できるようになります。

例 1～7 にある各コマンドリストを設定した場合，本装置でどのようなコマンドが許可／制限されるかを示します。

(例 1)

許可コマンドリストだけを設定した場合，設定されたコマンドだけが実行を許可されます。

表 8-11　コマンドリスト例 1

コマンドリスト	指定コマンド	判定
許可コマンドリスト="show ,ping" 制限コマンドリスト 設定なし	show ip arp	許可
	ping 10.10.10.10	許可
	reload	制限

(例 2)

許可コマンドリストと制限コマンドリストの両方に合致した場合は，合致したコマンド文字数が多い方の動作とします(ただし，all 指定は文字数 1 とします)。

表 8-12　コマンドリスト例 2

コマンドリスト	指定コマンド	判定
許可コマンドリスト="show"	show system	許可

コマンドリスト	指定コマンド	判定
制限コマンドリスト="show ip"	show ip arp	制限

(例 3)

許可コマンドリストと制限コマンドリストの両方を設定し，両方に合致しない場合は，許可として判定されます。

表 8-13　コマンドリスト例 3

コマンドリスト	指定コマンド	判定
許可コマンドリスト="show" 制限コマンドリスト="reload"	ping 10.10.10.10	許可
	reload	制限

(例 4)

許可コマンドリストと制限コマンドリストに同じコマンド文字列が指定されている場合は，許可として判定されます。

表 8-14　コマンドリスト例 4

コマンドリスト	指定コマンド	判定
許可コマンドリスト="show" 制限コマンドリスト="show,ping"	show system	許可
	ping 10.10.10.10	制限

(例 5)

コマンドリストをまったく設定しなかった場合は，logout などのコマンド以外はすべて制限されます。

表 8-15　コマンドリスト例 5

コマンドリスト	指定コマンド	判定
許可コマンドリスト 設定なし 制限コマンドリスト 設定なし	すべて	制限
	logout，exit，quit，disable，end，set terminal，show whoami，who am i	許可

(例 6)

クラスとして root を指定した場合は，従来どおりすべてのコマンドが実行可能となります。なお，コマンドクラスに root を指定した場合，許可／制限コマンドクラスの制限は無効となり，マニュアル未掲載のデバッグコマンド（ps コマンドなど）を含むすべてのコマンドが実行可能となります。

表 8-16　コマンドリスト例 6

コマンドリスト	指定コマンド	判定
コマンドクラス="root"	すべて（マニュアル未掲載のデバッグコマンドを含む）	許可

(例 7)

制限コマンドリストだけを設定した場合は，リストに合致しない運用コマンドはすべて許可となります。

表 8-17　コマンドリスト例 7

コマンドリスト	指定コマンド	判定
許可コマンドリスト 設定なし 制限コマンドリスト= "reload"	reload 以外の運用コマンドすべて	許可
	reload	制限

本マニュアルでは，例として次表のようなポリシーでコマンド制限を行います。

表 8-18　コマンド制限のポリシー例

ユーザ名	コマンドクラス	許可コマンド	制限コマンド
staff	allcommand	運用コマンドすべて	なし
guest	なし	制限以外の運用コマンドすべて許可	reload …※ inactivate …※ enable …※
test	なし	show ip …※ （show ipv6 …は制限）	許可以外，すべて制限

注※　…は任意のパラメータを意味します（show ip …は show ip arp など）。

(5)　RADIUS/TACACS+/ローカルコマンド承認の設定

「表 8-18　コマンド制限のポリシー例」で決定したコマンド制限ポリシーを基に，RADIUS または TACACS+のリモート認証サーバでは，通常のログイン認証の設定以外に，以下の属性値を使用したコマンド制限のための設定を行います。

なお，サーバ側でコマンド承認の設定を行っていない場合，ユーザが認証されログインできても logout，exit，quit，disable，end，set terminal，show whoami，who am i 以外のすべてのコマンドが制限され，コマンドを実行できなくなりますのでご注意ください。その場合は，コンソールからログインしてください。

ただし，コンフィグレーションコマンド aaa authorization commands console によってコンソールもコマンド承認の対象となっている場合は，コンソールでもコマンドが制限されるので注意してください。

- RADIUS サーバを使用する場合

RADIUS サーバを利用してコマンド制限する場合は，認証時に以下のような属性を返すようにサーバで設定します。

表 8-19　RADIUS 設定属性一覧

属性	ベンダー固有属性	値
25 Class	－	クラス 次の文字列のどれか一つを指定します。 root，allcommand，noconfig，nomanage，noenable
26 Vendor-Specific Vendor-Id: 21839	ALAXALA-Allow-Commands Vendor type: 101	許可コマンドリスト 許可するコマンドの前方一致文字列をコンマ(,)で区切って指定します。空白も区別します。 運用コマンドすべては"all"を指定します。

属性	ベンダー固有属性	値
		許可コマンドリストだけ設定した場合は，許可コマンドリスト以外のコマンドはすべて制限となります。 （例：ALAXALA-Allow-Commands="show ,ping ,telnet ")
	ALAXALA-Deny-Commands Vendor type: 102	制限コマンドリスト 制限するコマンドの前方一致文字列をコンマ(,)で区切って指定します。空白も区別します。 運用コマンドすべては"all"を指定します。 制限コマンドリストだけ設定した場合は，制限コマンドリスト以外はすべて許可となります。 （例：ALAXALA-Deny-Commands="enable,reload, inactivate"）

（凡例）－：該当なし

RADIUS サーバには，上記のベンダー固有属性を登録（dictionary ファイルなどに設定）してください。

図 8-17　RADIUS サーバでのベンダー固有属性の dictionary ファイル登録例

```
VENDOR          ALAXALA                 21839
ATTRIBUTE       ALAXALA-Allow-Commands  101     string  ALAXALA
ATTRIBUTE       ALAXALA-Deny-Commands   102     string  ALAXALA
```

「表 8-18　コマンド制限のポリシー例」で決定したポリシーを一般的な RADIUS サーバに設定する場合，以下のような設定例になります。

図 8-18　RADIUS サーバ設定例

```
staff  Password = ”******”
       Class = ”allcommand”                                  … 1


guest  Password = ”******”
       Alaxala-Deny-Commands = ”enable,reload,inactivate”    … 2


test  Password = ”******”
      Alaxala-Allow-Commands = ”show ip ”                    … 3
```

注 ******の部分には各ユーザのパスワードを設定します。

1. クラス"allcommand"で運用コマンドすべてを許可します。
2. enable，reload，および inactivate で始まるコマンドを制限します。
   allow-commands が指定されていないため，ほかのコマンドは許可となります。
3. 空白の有無が意味を持ちます。
   "show ip "の後ろに空白があるため，show ip arp などのコマンドは許可されますが，show ipv6 neighbors などのコマンドは許可されません。
   ほかのコマンドはすべて制限となります。

注意

- 本装置では Class エントリを複数受信した場合，1 個目の Class を認識し 2 個目以降の Class エントリは無効となります。

図 8-19　複数 Class エントリ設定例

```
Class = ”noenable”                                    … 1
Class = ”allcommand”
```

1. 本装置では一つ目の noenable だけ有効となります。

- 本装置では Class エントリに複数のクラス名を記述した場合，1 個目のクラス名を認識し 2 個目以降のクラス名は無効となります。例えば，class="nomanage,noenable"と記述した場合，nomanage だけが有効になります。
- ALAXALA-Deny-Commands, ALAXALA-Allow-Commands のそれぞれにおいて，同一属性のエントリを複数受信した場合，一つの属性につきコンマ(,)と空白も含み 1024 文字までを認識し，1025 文字以降は受信しても無効となります。なお，下記の例のように同一属性を複数エントリ記述し，本装置で 2 個目以降のエントリを受信した場合にはエントリの先頭に自動的にコンマ(,)を設定します。

図 8-20　複数 Deny-Commands エントリ設定例

```
ALAXALA-Deny-Commands = ”inactivate,reload”                … 1
ALAXALA-Deny-Commands = ”activate,test,.....”              … 1
```

1. 本装置では下線の部分を合計 1024 文字まで認識します。

上記の Deny-Commands を受信した場合は，下記のように 2 個目のエントリの先頭である activate コマンドの前にコンマ(,)が自動的に設定されます。

```
Deny-Commands = ”inactivate,reload,activate,test,.....”
```

- TACACS+サーバを使用する場合

TACACS+サーバを使用してコマンド制限をする場合は，TACACS+サーバで承認の設定として以下のような属性－値のペアを設定します。

表 8-20　TACACS+設定属性一覧

service	属性	値
taclogin	class	コマンドクラス 次の文字列のどれかを指定 root，allcommand，noconfig，nomanage，noenable
	allow-commands	許可コマンドリスト 許可するコマンドの前方一致文字列をコンマ(,)で区切って指定します。空白も区別します。 運用コマンドすべては"all"を指定します。 許可コマンドリストだけ設定した場合は，許可コマンドリスト以外のコマンドはすべて制限となります。 （例：allow-commands="show ,ping ,telnet "）
	deny-commands	制限コマンドリスト 制限するコマンドの前方一致文字列をコンマ(,)で区切って指定します。空白も区別します。 運用コマンドすべては"all"を指定します。制限コマンドリストだけ設定した場合は，制限コマンドリスト以外はすべて許可となります。 （例：deny-commands="enable,reload,inactivate"）

「表 8-18　コマンド制限のポリシー例」で決定したポリシーを一般的な TACACS+サーバに設定する場合，以下のような設定ファイルイメージになります。

図 8-21　TACACS+サーバの設定例

```
user=staff {
    login = cleartext ”******”
    service = taclogin {                                    … 1
        class = ”allcommand”
    }
}


user=guest {
    login = cleartext ”******”
    service = taclogin {
        deny-commands = ”enable,reload,inactivate”          … 2
    }
}


user=test {
    login = cleartext ”******”
    service = taclogin {
        allow-commands = ”show ip ”                         … 3
    }
}
```

注 ******の部分には各ユーザのパスワードを設定します。

1. service 名は taclogin と設定します。
   クラス"allcommand"で運用コマンドすべてを許可します。
2. enable，reload，および inactivate で始まるコマンドを制限します。
   allow-commands が指定されていないため，ほかのコマンドは許可となります。
3. 空白の有無が意味を持ちます。
   "show ip "の後ろに空白があるため，show ip arp などのコマンドは許可されますが，show ipv6 neighbors などのコマンドは許可されません。
   ほかのコマンドはすべて制限となります。

注意

- 本装置では class エントリに複数のクラス名を記述した場合, 1 個目のクラス名を認識し 2 個目以降のクラス名は無効となります。例えば class="nomanage,noenable"と記述した場合，nomanage だけが有効になります。
- deny-commands，allow-commands のそれぞれにおいて，一つの属性につきコンマ(,)と空白も含み 1024 文字までを認識し，1025 文字以降は受信しても無効となります。

- **ローカルコマンド承認を使用する場合**

「表 8-18　コマンド制限のポリシー例」で決定したポリシーをローカルコマンド承認で設定する場合，次のようなコンフィグレーションの設定になります。

図 8-22　コンフィグレーションの設定例

```
username guest view guest_view
username staff view-class allcommand                        … 1
username test view test_view
!
parser view guest_view
  commands exec exclude all ”enable”                        … 2
  commands exec exclude all ”inactivate”                    … 2
  commands exec exclude all ”reload”                        … 2
!
parser view test_view
  commands exec include all ”show ip ”                      … 3
!
```

```
aaa authentication login default local
aaa authorization commands default local
```

1. ユーザ"staff"に対し，クラス"allcommand"で運用コマンドすべてを許可します。
2. enable，inactivate，および reload で始まるコマンドを制限します。
   commands exec include が指定されていないため，ほかのコマンドは許可となります。
3. 空白の有無が意味を持ちます。
   "show ip "の後ろに空白があるため，show ip arp などのコマンドは許可されますが，show ipv6 neighbors などのコマンドは許可されません。
   ほかのコマンドはすべて制限となります。

(a) ログインしての確認

設定が完了した後，RADIUS/TACACS+/ローカルを使用したリモート運用端末から本装置へのログインを行います。ログイン後，show whoami コマンドでコマンドリストが設定されていること，コマンドを実行して制限・許可していることを確認してください。

図 8-23 staff がログイン後の確認例

```
> show whoami
Date 20XX/01/07 12:00:00 UTC
staff ttyp0    -----  2   Jan  6 14:17 (10.10.10.10)

Home-directory: /usr/home/staff
Authentication: TACACS+ (Server 192.168.10.1)
Class: allcommand
      Allow: ”all”
      Deny : -----
Command-list: -----
>
> show clock
Wed Jan 7 12:00:10 UTC 20XX
> /bin/date
% Command not authorized.
>
```

図 8-24 guest がログイン後の確認例

```
>show whoami
Date 20XX/01/07 12:00:00 UTC
guest ttyp0    -----  2   Jan  6 14:17 (10.10.10.20)

Home-directory: /usr/home/guest
Authentication: RADIUS (Server 192.168.10.1)
Class: -----
Command-list:
      Allow: -----
      Deny : ”enable,reload,inactivate”
>
> show clock
Wed Jan 7 12:00:10 UTC 20XX
> reload
% Command not authorized.
>
```

図 8-25 test がログイン後の確認例

```
>show whoami
Date 20XX/01/07 12:00:00 UTC
test ttyp0    -----  2   Jan  6 14:17 (10.10.10.30)

Home-directory: /usr/home/test
Authentication: LOCAL
Class: -----
Command-list:
      Allow: ”show ip ”
      Deny : -----
```

```
>
> show ip arp
***コマンド実行されます***
> show ipv6 neighbors
% Command not authorized.
>
```

8.2.5　RADIUS/TACACS+を使用したアカウンティング

RADIUS/TACACS+を使用したアカウンティング方法について説明します。

(1)　アカウンティングの指定

本装置の RADIUS/TACACS+コンフィグレーションと aaa accounting コンフィグレーションのアカウンティングを設定すると，運用端末から本装置へのログイン・ログアウト時に RADIUS または TACACS+サーバへアカウンティング情報を送信します。また，本装置へのコマンド入力時に TACACS+サーバへアカウンティング情報を送信します。

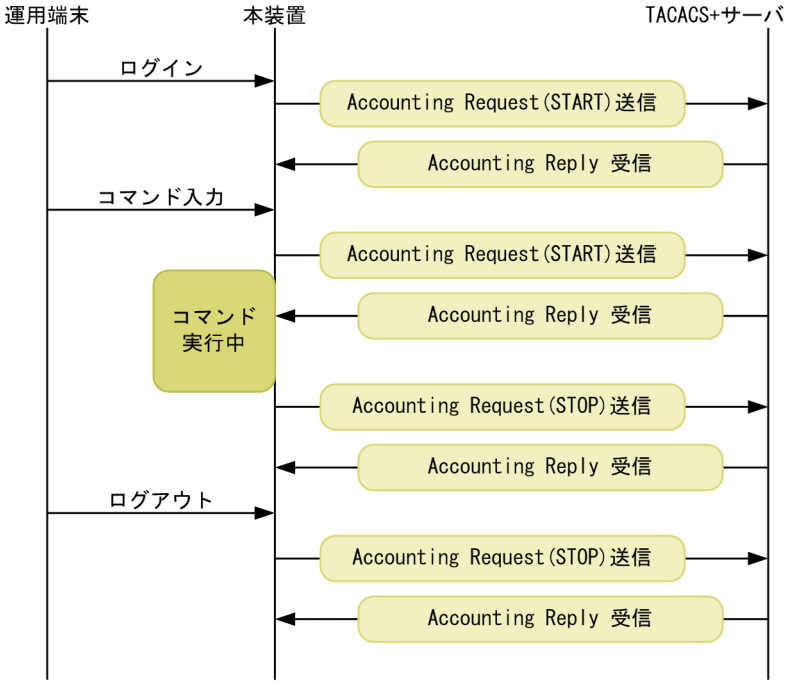
アカウンティングの設定は，ログインとログアウトのイベントを送信するログインアカウンティング指定と, コマンド入力のイベントを送信するコマンドアカウンティング指定があります。コマンドアカウンティングは TACACS+だけでサポートしています。

それぞれのアカウンティングに対して，アカウンティング START と STOP を両方送信するモード（start-stop）と STOP だけを送信するモード（stop-only）を選択できます。さらに，コマンドアカウンティングに対しては, 入力したコマンドをすべて送信するモードとコンフィグレーションだけを送信するモードを選択できます。また，設定された各 RADIUS/TACACS+サーバに対して，通常はどこかのサーバでアカウンティングが成功するまで順に送信しますが, 成功したかどうかにかかわらずすべてのサーバへ順に送信するモード（broadcast）も選択できます。

(2)　アカウンティングの流れ

ログインアカウンティングとコマンドアカウンティングの両方を START-STOP 送信モードで TACACS+サーバへ送信する設定をした場合のシーケンスを次の図に示します。

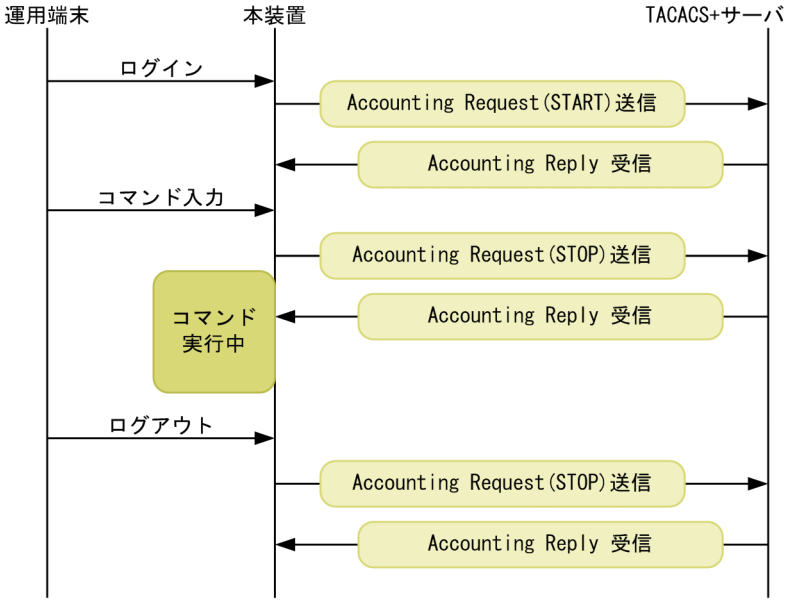
図 8-26　TACACS+アカウンティングのシーケンス（ログイン・コマンドアカウンティングの START-STOP 送信モード時）



この図で運用端末から本装置にログインが成功すると，本装置から TACACS+サーバに対しユーザ情報や時刻などのアカウンティング情報を送信します。また，コマンドの入力前後にも本装置から TACACS+サーバに対し入力したコマンド情報などのアカウンティング情報を送信します。最後に，ログアウト時には，ログインしていた時間などの情報を送信します。

ログインアカウンティングは START-STOP 送信モードのままで，コマンドアカウンティングだけを STOP-ONLY 送信モードして TACACS+サーバへ送信する設定をした場合のシーケンスを次の図に示します。

図 8-27　TACACS+アカウンティングのシーケンス（ログインアカウンティング START-STOP，コマンドアカウンティング STOP-ONLY 送信モード時）



「図 8-26　TACACS+アカウンティングのシーケンス（ログイン・コマンドアカウンティングの START-STOP 送信モード時）」の例と比べると，ログイン・ログアウトでのアカウンティング動作は同じですが，コマンドアカウンティングで STOP-ONLY を指定している場合，コマンドの入力前にだけ本装置から TACACS+サーバに対し入力したコマンド情報などのアカウンティング情報を送信します。

(3)　アカウンティングの注意事項

RADIUS/TACACS+コンフィグレーション，aaa accounting コンフィグレーションのアカウンティングの設定や interface loopback コンフィグレーションで IPv4 装置アドレスを変更した場合は，送受信途中や未送信のアカウンティングイベントと統計情報はクリアされ，新しい設定で動作します。

多数のユーザが，コマンドを連続して入力したり，ログイン・ログアウトを繰り返したりした場合，アカウンティングイベントが大量に発生するため，一部のイベントでアカウンティングできないことがあります。

アカウンティングイベントの大量な発生による本装置・サーバ・ネットワークへの負担を避けるためにも，コマンドアカウンティングは STOP-ONLY で設定することをお勧めします。また，正常に通信できない RADIUS/TACACS+サーバは指定しないでください。

運用コマンド clear accounting でアカウンティング統計情報をクリアする場合，clear accounting コマンドの入力時点で各サーバへの送受信途中のアカウンティングイベントがあるときは，そのイベントの送受信終了後に，各サーバへの送受信統計のカウントを開始します。

DNS サーバを使用してホスト名を解決する場合，DNS サーバとの通信に時間が掛かることがあります。このため，RADIUS サーバおよび TACACS+サーバは IP アドレスで指定することをお勧めします。

8.2.6　RADIUS/TACACS+との接続

(1)　RADIUS サーバとの接続

(a)　RADIUS サーバでの本装置の識別

RADIUS プロトコルでは NAS を識別するキーとして，要求パケットの発信元 IP アドレスを使用するよう規定されています。本装置では要求パケットの発信元 IP アドレスに次に示すアドレスを使用します。

- コンフィグレーションコマンド interface loopback 0 のローカルアドレスが設定されている場合は，ローカルアドレスを発信元 IP アドレスとして使用します。
- ローカルアドレスが設定されていない場合は，送信インタフェースの IP アドレスを使用します。

このため，ローカルアドレスが設定されている場合は，RADIUS サーバに本装置を登録するためにローカルアドレスで指定した IP アドレスを使用する必要があります。これによって，RADIUS サーバと通信するインタフェースが特定できない場合は，ローカルアドレスを設定することで RADIUS サーバを確実に識別できる本装置の情報を登録できるようになります。

(b)　RADIUS サーバのメッセージ

RADIUS サーバは応答に Reply-Message 属性を添付して要求元にメッセージを送付する場合があります。本装置では，RADIUS サーバからの Reply-Message 属性の内容を運用ログに出力します。RADIUS サーバとの認証に失敗する場合は，運用ログを参照してください。

(c)　RADIUS サーバのポート番号

RADIUS の認証サービスのポート番号は，RFC2865 で 1812 と規定されています。本装置では特に指定しないかぎり，RADIUS サーバへの要求に 1812 のポート番号を使用します。しかし，一部の RADIUS サーバで 1812 ではなく初期の実装時に使用されていた 1645 のポート番号を使用している場合があります。このときはコンフィグレーション radius-server host の auth-port パラメータで 1645 を指定してください。なお，auth-port パラメータでは 1～65535 の任意の値が指定できますので，RADIUS サーバが任意のポート番号で待ち受けできる場合にも対応できます。

(2)　TACACS+サーバとの接続

(a)　TACACS+サーバの設定

- 本装置と TACACS+サーバを接続する場合は，Service と属性名などに注意してください。TACACS+サーバの属性については，「8.2.4　RADIUS/TACACS+/ローカルを使用したコマンド承認」を参照してください。
- コンフィグレーションコマンド interface loopback 0 のローカルアドレスが設定されている場合は，ローカルアドレスを発信元 IP アドレスとして使用します。

8.3　RADIUS/TACACS+のコマンドガイド

8.3.1　コマンド一覧

RADIUS/TACACS+，アカウンティング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 8-21　コンフィグレーションコマンド一覧（RADIUS）

コマンド名	説明
radius-server host	認証，承認，アカウンティングに使用する RADIUS サーバを設定します。
radius-server key	認証，承認，アカウンティングに使用する RADIUS サーバ鍵を設定します。
radius-server retransmit	認証，承認，アカウンティングに使用する RADIUS サーバへの再送回数を設定します。
radius-server timeout	認証，承認，アカウンティングに使用する RADIUS サーバの応答タイムアウト値を設定します。

表 8-22　コンフィグレーションコマンド一覧（TACACS+）

コマンド名	説明
tacacs-server host	認証，承認，アカウンティングに使用する TACACS+サーバを設定します。
tacacs-server key	認証，承認，アカウンティングに使用する TACACS+サーバの共有秘密鍵を設定します。
tacacs-server timeout	認証，承認，アカウンティングに使用する TACACS+サーバの応答タイムアウト値を設定します。

表 8-23　コンフィグレーションコマンド一覧（アカウンティング）

コマンド名	説明
aaa accounting commands	コマンドアカウンティングを行うときに設定します。
aaa accounting exec	ログイン・ログアウトアカウンティングを行うときに設定します。

8.3.2　RADIUS サーバによる認証の設定

(1)　ログイン認証の設定例

[設定のポイント]

RADIUS サーバ，およびローカル認証を行う設定例を示します。RADIUS サーバとの通信不可などの異常によって認証に失敗した場合だけローカル認証を行うように設定します。なお，否認によって認証に失敗した場合には，その時点で一連の認証を終了し，ローカル認証を行いません。

あらかじめ，通常のリモートアクセスに必要な設定を行っておく必要があります。

[コマンドによる設定]

1. **(config)# aaa authentication login default group radius local**

ログイン時に使用する認証方式を RADIUS 認証，ローカル認証の順に設定します。

2. **(config)# aaa authentication login end-by-reject**

   RADIUS 認証で否認された場合には，その時点で一連の認証を終了し，ローカル認証を行わないように設定します。

3. **(config)# radius-server host 192.168.10.1 key "039fkllf84kxm3"**

   RADIUS 認証に使用するサーバ 192.168.10.1 の IP アドレスと共有鍵を設定します。

(2)　装置管理者モードへの変更（enable コマンド）時の認証の設定例

[設定のポイント]

RADIUS サーバ，およびローカル認証を行う設定例を示します。RADIUS サーバとの通信不可などの異常によって認証に失敗した場合だけローカル認証を行うように設定します。なお，否認によって認証に失敗した場合には，その時点で一連の認証を終了し，ローカル認証を行いません。

また，RADIUS 認証時のユーザ名属性として$enab15$を送信するように設定します。

[コマンドによる設定]

1. **(config)# aaa authentication enable default group radius enable**

   装置管理者モードへの変更（enable コマンド）時に使用する認証方式を RADIUS 認証，ローカル認証の順に設定します。

2. **(config)# aaa authentication enable end-by-reject**

   RADIUS 認証で否認された場合には，その時点で一連の認証を終了し，ローカル認証を行わないように設定します。

3. **(config)# aaa authentication enable attribute-user-per-method**

   RADIUS 認証時のユーザ名属性として$enab15$を送信するように設定します。

4. **(config)# radius-server host 192.168.10.1 key "039fkllf84kxm3"**

   RADIUS 認証に使用するサーバ 192.168.10.1 の IP アドレスと共有鍵を設定します。

8.3.3　TACACS+サーバによる認証の設定

(1)　ログイン認証の設定例

[設定のポイント]

TACACS+サーバおよびローカル認証を行う設定例を示します。TACACS+サーバとの通信不可などの異常によって認証に失敗した場合だけローカル認証を行うように設定します。なお，否認によって認証に失敗した場合には，その時点で一連の認証を終了し，ローカル認証を行いません。

あらかじめ，通常のリモートアクセスに必要な設定を行っておく必要があります。

[コマンドによる設定]

1. **(config)# aaa authentication login default group tacacs+ local**

   ログイン時に使用する認証方式を TACACS+認証，ローカル認証の順に設定します。

2. **(config)# aaa authentication login end-by-reject**

   TACACS+認証で否認された場合には，その時点で一連の認証を終了し，ローカル認証を行わないように設定します。

3. **(config)# tacacs-server host 192.168.10.1 key "4h8dlir9r-w2"**

   TACACS+認証に使用するサーバ 192.168.10.1 の IP アドレスと共有鍵を設定します。

(2)　装置管理者モードへの変更（enable コマンド）時の認証の設定例

[設定のポイント]

TACACS+サーバおよびローカル認証を行う設定例を示します。TACACS+サーバとの通信不可などの異常によって認証に失敗した場合だけローカル認証を行うように設定します。なお，否認によって認証に失敗した場合には，その時点で一連の認証を終了し，ローカル認証を行いません。

また，TACACS+認証時のユーザ名属性としてログインユーザ名を送信するように設定します。

[コマンドによる設定]

1. **(config)# aaa authentication enable default group tacacs+ enable**
   装置管理者モードへの変更（enable コマンド）時に使用する認証方式を TACACS+認証，ローカル認証の順に設定します。
2. **(config)# aaa authentication enable end-by-reject**
   TACACS+認証で否認された場合には，その時点で一連の認証を終了し，ローカル認証を行わないように設定します。
3. **(config)# aaa authentication enable attribute-user-per-method**
   TACACS+認証時のユーザ名属性としてログインユーザ名を送信するように設定します。
4. **(config)# tacacs-server host 192.168.10.1 key "4h8dlir9r-w2"**
   TACACS+認証に使用するサーバ 192.168.10.1 の IP アドレスと共有鍵を設定します。

8.3.4　RADIUS/TACACS+/ローカルによるコマンド承認の設定

(1)　RADIUS サーバによるコマンド承認の設定例

[設定のポイント]

RADIUS サーバによるコマンド承認を行う設定例を示します。

あらかじめ，RADIUS 認証を使用する設定を行ってください。

[コマンドによる設定]

1. **(config)# aaa authentication login default group radius local**
   (config)# radius-server host 192.168.10.1 key "RaD#001"
   あらかじめ，RADIUS サーバによる認証の設定を行います。
2. **(config)# aaa authorization commands default group radius**
   RADIUS サーバを使用して，コマンド承認を行います。

[注意事項]

本設定後にユーザが RADIUS 認証されてログインしたとき，RADIUS サーバ側でコマンド承認の設定がされていなかった場合は，コマンドがすべて制限されて実行できなくなります。設定ミスなどでコマンドの実行ができない場合は，コンソールからログインして修正してください。ただし，コンフィグレーションコマンド aaa authorization commands console によってコンソールもコマンド承認の対象となっている場合は，コンソールでもコマンドが制限されるので注意してください。

(2)　TACACS+サーバによるコマンド承認の設定例

[設定のポイント]

TACACS+サーバによるコマンド承認を行う設定例を示します。

あらかじめ，TACACS+認証を使用する設定を行ってください。

[コマンドによる設定]

1. **(config)# aaa authentication login default group tacacs+ local**
   (config)# tacacs-server host 192.168.10.1 key "TaC#001"
   あらかじめ，TACACS+サーバによる認証の設定を行います。
2. **(config)# aaa authorization commands default group tacacs+**
   TACACS+サーバを使用して，コマンド承認を行います。

[注意事項]

本設定後にユーザが TACACS+認証されてログインしたとき，TACACS+サーバ側でコマンド承認の設定がされていなかった場合は，コマンドがすべて制限されて実行できなくなります。設定ミスなどでコマンドの実行ができない場合は，コンソールからログインして修正してください。ただし，コンフィグレーションコマンド aaa authorization commands console によってコンソールもコマンド承認の対象となっている場合は，コンソールでもコマンドが制限されるので注意してください。

(3) ローカルコマンド承認の設定例

[設定のポイント]

ローカルコマンド承認を行う設定例を示します。

あらかじめ，ユーザ名とそれに対応したコマンドクラス（username view-class）またはコマンドリスト（username view・parser view・commands exec）の設定を行ってください。

また，ローカルパスワード認証を使用する設定を行ってください。

[コマンドによる設定]

1. **(config)# parser view Local_001**
   (config-view)# commands exec include all "show"
   (config-view)# commands exec exclude all "reload"
   コマンドリストを使用する場合は，あらかじめコマンドリストの設定を行います。
   なお，コマンドクラスだけを使用する場合は，コマンドリストの設定は必要ありません。
2. **(config)# username user001 view Local_001**
   (config)# username user001 view-class noenable
   指定ユーザにコマンドクラスまたはコマンドリストの設定を行います。
   なお，コマンドクラスとコマンドリストを同時に設定することもできます。
3. **(config)# aaa authentication login default local**
   ローカルパスワードによる認証の設定を行います。
4. **(config)# aaa authorization commands default local**
   ローカル認証を使用して，コマンド承認を行います。

[注意事項]

ローカルコマンド承認を設定すると，ローカル認証でログインしたすべてのユーザに適用されますので，設定に漏れがないようご注意ください。

コマンドクラスまたはコマンドリストの設定がされていないユーザは，コマンドがすべて制限されて実行できなくなります。

設定ミスなどでコマンドの実行ができない場合は，コンソールからログインして修正してください。ただし，コンフィグレーションコマンド aaa authorization commands console によってコンソールもコマンド承認の対象となっている場合は，コンソールでもコマンドが制限されるので注意してください。

8.3.5　RADIUS/TACACS+によるログイン・ログアウトアカウンティングの設定

(1)　RADIUS サーバによるログイン・ログアウトアカウンティングの設定例

[設定のポイント]

RADIUS サーバによるログイン・ログアウトアカウンティングを行う設定例を示します。あらかじめ，アカウンティング送信先となる RADIUS サーバホスト側の設定を行ってください。

[コマンドによる設定]

1. **(config)# radius-server host 192.168.10.1 key "RaD#001"**
   あらかじめ，RADIUS サーバの設定を行います。
2. **(config)# aaa accounting exec default start-stop group radius**
   ログイン・ログアウトアカウンティングの設定を行います。

[注意事項]

radius-server コンフィグレーションの設定がされていない状態で aaa accounting exec を設定した場合，ユーザがログイン・ログアウトしたときに System accounting failed という運用ログが表示されます。使用する radius-server コンフィグレーションを設定してください。

(2)　TACACS+サーバによるログイン・ログアウトアカウンティングの設定例

[設定のポイント]

TACACS+サーバによるログイン・ログアウトアカウンティングを行う設定例を示します。あらかじめ，アカウンティング送信先となる TACACS+サーバホスト側の設定を行ってください。

[コマンドによる設定]

1. **(config)# tacacs-server host 192.168.10.1 key "TaC#001"**
   あらかじめ，TACACS+サーバの設定を行います。
2. **(config)# aaa accounting exec default start-stop group tacacs+**
   ログイン・ログアウトアカウンティングの設定を行います。

[注意事項]

tacacs-server コンフィグレーションの設定がされていない状態で aaa accounting exec を設定した場合，ユーザがログイン・ログアウトしたときに System accounting failed という運用ログが表示されます。使用する tacacs-server コンフィグレーションを設定してください。

8.3.6　TACACS+サーバによるコマンドアカウンティングの設定

(1)　TACACS+サーバによるコマンドアカウンティングの設定例

[設定のポイント]

TACACS+サーバによるコマンドアカウンティングを行う設定例を示します。

あらかじめ，アカウンティング送信先となる TACACS+サーバホスト側の設定を行ってください。

[コマンドによる設定]

1. **(config)# tacacs-server host 192.168.10.1 key "TaC#001"**
   TACACS+サーバの設定を行います。
2. **(config)# aaa accounting commands 0-15 default start-stop group tacacs+**
   コマンドアカウンティングを設定します。

[注意事項]

tacacs-server コンフィグレーションの設定がされていない状態で aaa accounting commands を設定した場合，ユーザがコマンドを入力したときに System accounting failed という運用ログが表示されます。使用する tacacs-server コンフィグレーションを設定してください。

9 SSH(Secure Shell)

この章では，SSH の解説と操作方法について説明します。

9.1　解説

9.1.1　概要

SSH は，クライアントからサーバへ，安全ではないネットワーク上で，セキュアに接続する機能です。

SSH を使用すると，クライアントとサーバは相互に認証し，通信内容を暗号化し，メッセージ認証によって通信内容が変更されていないことを確認します。このため，ネットワーク上の悪意ある第三者によるなりすまし，盗聴，改ざんから通信を保護できます。SSH を使用することで，telnet 接続の脅威（不正なりすましサーバへの誤接続，運用情報の流出，データの改ざんなど）から保護された，セキュアな運用管理を実現できます。telnet 接続による脅威および SSH 接続によるセキュアな運用管理を次の図に示します。

図 9-1　telnet 接続による脅威

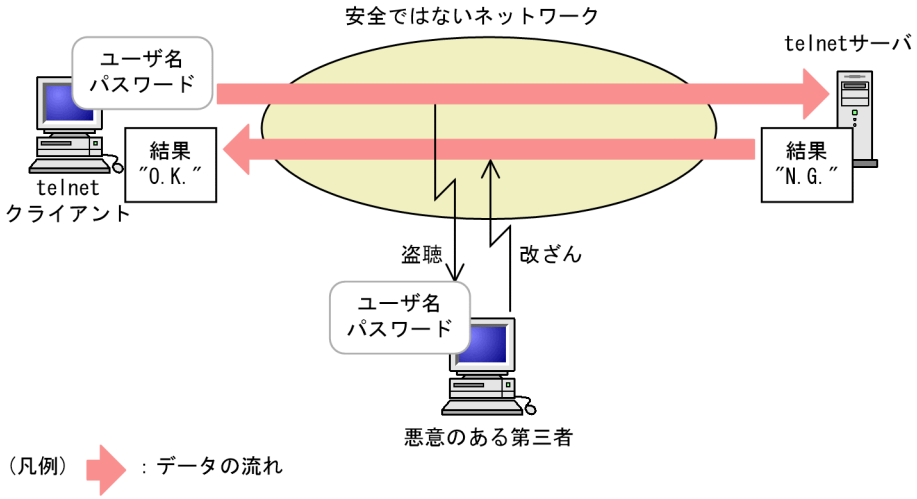
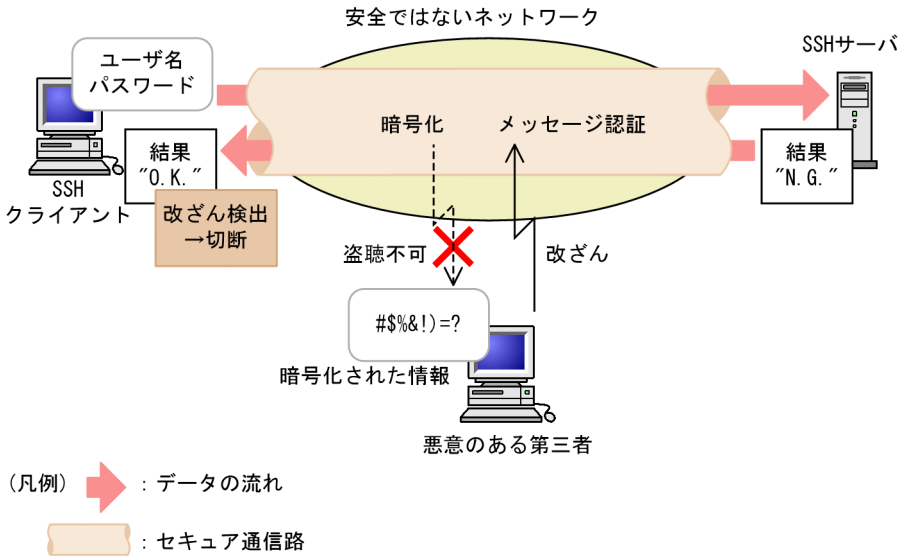


図 9-2　SSH 接続によるセキュアな運用管理



SSH サーバへ接続するユーザの認証方法として，telnet や FTP で使用されていたパスワード認証のほかに，より安全な公開鍵認証を使用できます。公開鍵認証を使用することで，パスワードが漏洩して他者に利用されることを防ぎます。

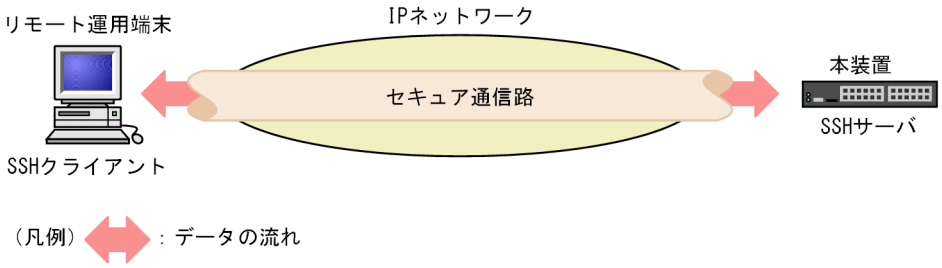
SSH には，バージョン 1（SSHv1）とバージョン 2（SSHv2）があります。本装置は SSHv1 と SSHv2 の両方をサポートしています。

しかし，できるだけ SSHv2 に限定して運用することを推奨します。理由は，SSHv2 は SSHv1 に比べてセキュリティが向上しているためです。SSHv2 では，メッセージ認証によって通信の改ざんを防ぎます。また，SSHv2 は SSHv1 よりも進歩した暗号技術を採用しています。

本装置の SSH 機能は，IP ネットワークで使用できます。本装置は SSH サーバ機能と SSH クライアント機能の両方をサポートしています。

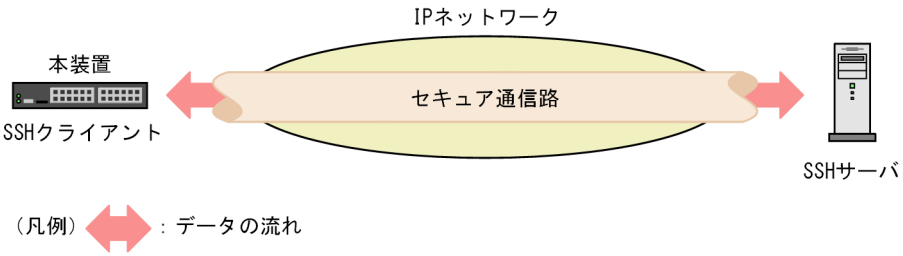
本装置の SSH サーバ機能によって，セキュア通信路上でリモート運用端末から本装置へのログインやファイル転送を実現できます。リモート運用端末から本装置への SSH の接続例を次の図に示します。

図 9-3　リモート運用端末から SSH クライアントを使用して本装置へ接続する例



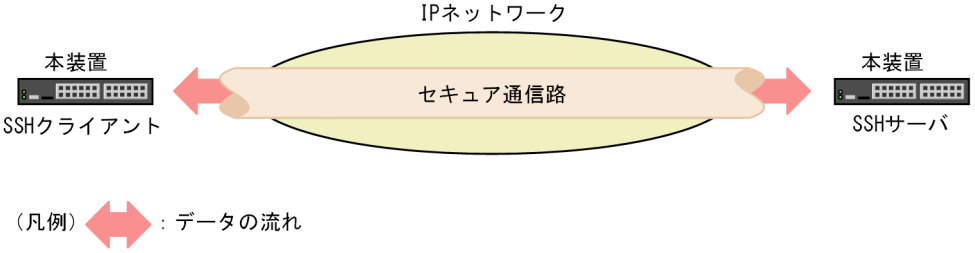
本装置の SSH クライアント機能によって，セキュア通信路を使用して本装置から SSH サーバへのログインやファイル転送を実現できます。本装置から SSH サーバへの接続例を次の図に示します。

図 9-4　本装置の SSH クライアントからリモートにある SSH サーバへ接続する例



また，本装置は SSH サーバと SSH クライアントの両方をサポートしているため，セキュア通信路を使用し，本装置から別の本装置へのログインやファイル転送を実現できます。本装置から別の本装置への接続例を次の図に示します。

図 9-5　本装置から別の本装置へ SSH を使用して接続する例



9.1.2 SSH の基本機能

(1) セキュアリモートログイン

SSH が提供するセキュア通信路をリモートログインに使用する機能です。セキュアリモートログインを使用すると，インターネット経由でも安全に，運用端末から SSH サーバへログインできます。また，通信内容を他者に見られないため，安全な運用管理を実現できます。

本装置の運用にセキュアリモートログインを使用することで, インターネット経由でも運用端末から本装置へ安全にログインし運用できます。

(2) セキュアコマンド実行

SSH が提供するセキュア通信路を使用して，サーバ上でコマンドを実行する機能です。ユーザ認証に公開鍵認証を使用した環境でセキュアコマンド実行を使用すると, リモート運用端末からログインやパスワード入力をしないで安全にコマンドを実行できます。

本装置の運用にセキュアコマンド実行を使用することで，ARP テーブルの確認や ping による疎通確認など，単純な，運用コマンドによる運用が容易になります。

なお，SSH クライアントからセキュアコマンド実行を使用して本装置上でコマンドを実行する場合，次に示す二つの注意点があります。

- SSH クライアント側で仮想端末を割り当てるように指定する必要があります。一般的な SSH クライアントの実装では，ssh コマンドの-t パラメータを指定することで仮想端末を割り当てます。本装置の運用コマンド ssh でも，-t パラメータによって仮想端末を割り当てます。
- 実行できるコマンドは，一般ユーザモードで実行できる運用コマンドだけです。装置管理者モードの運用コマンドや，コンフィグレーションコマンドは実行できません。

(3) セキュアコピー（SCP）

SSH が提供するセキュア通信路を使用して，コピー元ファイル名とコピー先ファイル名を指定し，クライアントとサーバ間でファイルを転送する機能です。コピー元にサーバ上のファイルを指定すると, サーバからクライアントへファイルをコピーします。コピー先にサーバ上のファイルを指定すると, クライアントからサーバへファイルをコピーします。

本装置の運用にセキュアコピーを使用することで, コンフィグレーションのバックアップなどを安全に実行できます。

(4) セキュア FTP（SFTP）

SSH が提供するセキュア通信路を使用して，FTP と同様の会話型インタフェースを使用し，クライアントとサーバ間でファイルを転送する機能です。ファイル転送のほかに, ファイル名を確認したりファイルを削除したりできます。

本装置の運用にセキュア FTP を使用することで，アップデート実施時のアップデートファイル取得などを安全に実行できます。

9.1.3 サポート機能

本装置がサポートする SSH サーバおよび SSH クライアントの役割，SSH プロトコルバージョン，SSH 接続に使用できるプロトコルを次の表に示します。

表 9-1　SSH サーバ／クライアント・プロトコルバージョン・接続プロトコルサポート一覧

機能名		サポート有無
SSH サーバ		○
SSH クライアント		○
SSH プロトコルバージョン	バージョン 1（SSHv1）	○
	バージョン 2（SSHv2）	○
SSH 接続に使用できるプロトコル	IPv4	○
	IPv6	○

（凡例）　○：サポート

SSH の基本機能とサポート状況を次の表に示します。

表 9-2　SSH 基本機能サポート一覧

機能名	説明	サポート有無
セキュアリモートログイン	SSH を使用したリモートログイン	○
セキュアコマンド実行	SSH を使用したコマンド実行	○
セキュアコピー（SCP）	SSH を使用したファイルコピー	○
セキュア FTP（SFTP）	SSH を使用したファイル転送	SSHv1：× SSHv2：○
認証エージェント	認証エージェント機能	×
ポート転送	TCP 転送機能	×
X11 プロトコル自動転送	X11 を自動転送する機能	×
データ圧縮	通信のデータを圧縮する機能	×

（凡例）　○：サポート　×：未サポート

SSHv1 のセキュリティ機能の方式別サポート状況を次の表に示します。

表 9-3　SSHv1 セキュリティ機能の方式別サポート一覧

機能名	方式		サポート有無
ホスト認証	公開鍵認証	RSA	○
ユーザ認証	公開鍵認証	RSA	サーバ：○ クライアント：×
	パスワード認証		○
	RHOSTS 認証		×
	RHOSTS + RSA 認証		×
暗号化	共通鍵暗号	3des-cbc，blowfish-cbc	○

機能名	方式	サポート有無
	その他の方式	×

（凡例） ○：サポート　×：未サポート

SSHv2 のセキュリティ機能の方式別サポート状況を次の表に示します。

表 9-4　SSHv2 セキュリティ機能の方式別サポート一覧

機能名	方式		サポート有無
ホスト認証	公開鍵認証	ECDSA，RSA，DSA	○
	証明局証明書による公開鍵認証		×
	PGP 証明書による公開鍵認証		×
ユーザ認証	公開鍵認証	ECDSA，RSA，DSA	サーバ：○ クライアント：×
	証明局証明書による公開鍵認証		×
	PGP 証明書による公開鍵認証		×
	ホストベース認証		×
	パスワード認証		○
鍵交換	ecdh-sha2-nistp256，ecdh-sha2-nistp384，ecdh-sha2-nistp521，dh-group16-sha512，dh-group14-sha256，dh-group-ex-sha1，dh-group14-sha1，dh-group1-sha1		○
	その他の方式		×
共通鍵暗号	aes128-ctr，aes192-ctr，aes256-ctr，aes128-cbc，aes192-cbc，aes256-cbc，3des-cbc，blowfish，arcfour256，arcfour128，arcfour		○
	その他の方式		×
メッセージ認証コード	hmac-sha2-256，hmac-sha2-512，hmac-sha1，hmac-md5，hmac-sha1-96，hmac-md5-96		○
	その他の方式		×
認証付き暗号	aes128-gcm@openssh.com aes256-gcm@openssh.com		○
	その他の方式		×

（凡例） ○：サポート　×：未サポート

SSH サーバのログインセキュリティと RADIUS/TACACS+対応のサポート状況を次の表に示します。

表 9-5　SSH サーバのログインセキュリティ機能サポート一覧

機能名	サポート有無
同時にログインできるユーザ数の設定	○

機能名		サポート有無
リモート運用端末の IP アドレスによる制限		○
ログインメッセージ	ログイン前	SSHv1：× SSHv2：○
	ログイン後	○
RADIUS/TACACS+	認証	○
	コマンド承認	○
	アカウンティング	○

（凡例）　○：サポート　×：未サポート

9.1.4　SSH のセキュリティ機能

SSH には，セキュリティを確保するために暗号技術を使用する機能が五つあります。

1. ホスト認証
2. ユーザ認証
3. セッション鍵の共有
4. 暗号化
5. メッセージ認証（SSHv2 だけ）

以降，各機能について説明します。

(1)　ホスト認証

ホスト認証は，SSH クライアントが SSH サーバを認証する機能です。

各 SSH サーバは，それぞれ異なるホスト鍵ペアを保持しています。SSHv1 では，ホスト公開鍵を使用してクライアントからサーバへ公開鍵暗号で通信することによって，サーバを認証します。SSHv2 では，サーバがホスト秘密鍵でデジタル署名を作成し，クライアントがホスト公開鍵で署名を確認することによって，サーバを認証します。本装置がサポートするホスト鍵ペアの公開鍵アルゴリズムとサイズを次の表に示します。

表 9-6　本装置がサポートするホスト鍵ペアの公開鍵アルゴリズムとサイズ

SSH バージョン	公開鍵 アルゴリズム	鍵のサイズ	
		SSH サーバ	SSH クライアント
SSHv1	RSA	1024bit	1024bit～2048bit
SSHv2	ECDSA	521bit（nistp521）， 384bit（nistp384）， 256bit（nistp256）	521bit（nistp521）， 384bit（nistp384）， 256bit（nistp256）
	RSA	1024bit，2048bit，3072bit，4096bit	512bit～5120bit
	DSA	1024bit	512bit～1536bit

本装置の SSH サーバ機能では，デフォルトで SSHv1 用 RSA 1024bit と SSHv2 用 RSA 2048bit のホスト鍵ペアを生成します。デフォルト以外の鍵ペアを使用する場合や鍵ペアを生成し直す場合は，運用コマンド set ssh hostkey を使用してください。SSHv2 の不要なアルゴリズムの鍵ペアを削除する場合は，運用コマンド erase ssh hostkey を使用してください。なお，SSHv1 の RSA ホスト鍵ペアは削除できません。

SSH クライアントでは，過去に接続したサーバのホスト公開鍵を保持しています。SSH クライアントでは，SSH サーバへ初めて接続するときやサーバのホスト公開鍵が変更されたときに，公開鍵のフィンガープリント（ハッシュ値）を表示して，ユーザに正しい公開鍵かどうか確認を要求します。事前にユーザへ告知したサーバのホスト公開鍵のフィンガープリントと，ユーザが接続したときに表示されたフィンガープリントを比較することで，サーバのなりすましを防げます。

本装置の SSH サーバ機能のホスト公開鍵およびホスト公開鍵のフィンガープリントを確認するには，運用コマンド show ssh hostkey を使用してください。表示内容と表示形式を次の表に示します。

表 9-7　SSH サーバ機能のホスト公開鍵およびフィンガープリント表示形式

SSH バージョン	表示内容	表示形式
SSHv1	公開鍵	SSHv1 形式
	フィンガープリント	SECSH（MD5）形式（RFC4716）
	フィンガープリント	SHA256 形式
SSHv2	公開鍵	OpenSSH 形式
	フィンガープリント	SECSH（MD5）形式（RFC4716）
	フィンガープリント	SHA256 形式

本装置の SSH クライアント機能がサーバ初回接続時に表示する，フィンガープリントの表示形式を次の表に示します。

表 9-8　SSH クライアント機能の未知ホストフィンガープリント表示形式

SSH バージョン	表示内容	表示形式
SSHv1	フィンガープリント	SECSH（MD5）形式（RFC4716）
	フィンガープリント	SHA256 形式
SSHv2	フィンガープリント	SECSH（MD5）形式（RFC4716）
	フィンガープリント	SHA256 形式

(2) ユーザ認証

ユーザ認証は，SSH サーバが SSH クライアントを認証する機能です。本装置では，ユーザ認証方式として次に示す二つの方式をサポートしています。

- 公開鍵認証
- パスワード認証

本装置の SSH サーバが使用するユーザ認証方式は，コンフィグレーションコマンド ip ssh authentication で設定できます。なお，本装置の SSH クライアントは，パスワード認証だけをサポートしています。

(a)　公開鍵認証

公開鍵アルゴリズムを使用してユーザを認証する機能です。各ユーザは，それぞれ鍵ペアを用意します。SSH サーバには，ユーザの公開鍵を設定しておきます。SSHv1 では，サーバから公開鍵暗号で通信することによってユーザを認証します。SSHv2 では，クライアントがユーザの秘密鍵でデジタル署名を作成し，サーバが署名を確認することでユーザを認証します。

本装置では，SSH サーバ機能だけが公開鍵認証をサポートして，SSH クライアント機能は公開鍵認証をサポートしません。本装置から別の本装置へ SSH で接続する場合，ユーザ認証方式に公開鍵認証を使用できない点に注意してください。

本装置の SSH サーバがユーザ認証でサポートする，公開鍵アルゴリズムと公開鍵のサイズを次の表に示します。

表 9-9　本装置の SSH サーバがサポートするユーザ公開鍵のアルゴリズムとサイズ

SSH バージョン	公開鍵アルゴリズム	ユーザ公開鍵のサイズ
SSHv1	RSA	512bit～2560bit
SSHv2	ECDSA	521bit（nistp521），384bit（nistp384），256bit（nistp256）
	RSA	512bit～5120bit
	DSA	512bit～1536bit

本装置の SSH サーバでは，ユーザ公開鍵の登録にコンフィグレーションコマンド ip ssh authkey を使用します。登録できる公開鍵の形式を次の表に示します。

表 9-10　登録できる公開鍵の形式

SSH バージョン	表示形式
SSHv1	SSHv1 形式の公開鍵ファイル
	SSHv1 形式の公開鍵を示す数字列
SSHv2	SECSH（RFC4716）形式の公開鍵ファイル
	OpenSSH 形式の公開鍵ファイル
	SECSH 形式または OpenSSH 形式の公開鍵を示す文字列

(b)　パスワード認証

SSH クライアントがユーザ名とパスワードを送信し，SSH サーバがサーバ内のユーザアカウント情報と照合するか，または RADIUS/TACACS+などによって認証サーバへユーザ名とパスワードが正しいかどうか問い合わせることで，ユーザ名とパスワードを確認します。SSH では，ユーザ認証情報は暗号化されるため，盗聴によってパスワードが漏洩する危険はありません。

本装置では，SSH サーバ機能および SSH クライアント機能のどちらもパスワード認証をサポートしています。ただし，本装置の SSH サーバでは，パスワードを設定していないユーザはパスワード認証ができません。本装置への SSH 接続のユーザ認証方式としてパスワード認証を使用する場合は，ユーザアカウントにパスワードを設定してください。

(3) セッション鍵の共有

セキュア通信路の暗号化やメッセージ認証に共通鍵として使用するセッション鍵を，サーバとクライアントで共有する機能です。SSHv1 では，クライアントがセッション鍵を作成し，ホスト認証時の RSA 公開鍵暗号によってクライアントからサーバへセッション鍵を送付します。SSHv2 では，鍵交換方式によってサーバとクライアントの両方に同じセッション鍵を生成します。

本装置では，SSHv2 サーバが使用する鍵交換方式を選択できます。鍵交換方式を選択するには，コンフィグレーションコマンド ip ssh key-exchange を使用してください。

(4) 暗号化

セキュア通信路を暗号化する機能です。暗号化には共通鍵暗号を使用しますが，SSHv2 では認証付き暗号も使用できます。

本装置では，コンフィグレーションコマンド ip ssh ciphers を設定することで，SSHv2 サーバの暗号化方式を制限できます。また，SSH クライアント機能の運用コマンドに-c パラメータを使用すると，SSH クライアント機能で使用する暗号化方式を指定できます。

(5) メッセージ認証

セキュア通信路のデータを認証する機能で，SSHv2 だけに存在します。メッセージ認証では，メッセージ認証コードを使用します。また，暗号化方式に認証付き暗号を使用した場合は，認証付き暗号でデータを認証します。

本装置では，コンフィグレーションコマンド ip ssh macs を設定することで，SSHv2 サーバのメッセージ認証コードを制限できます。また，SSHv2 クライアント機能の運用コマンドに-m パラメータを使用すると，SSHv2 クライアント機能が使用するメッセージ認証方式を指定できます。

9.1.5 SSH が使用する暗号技術

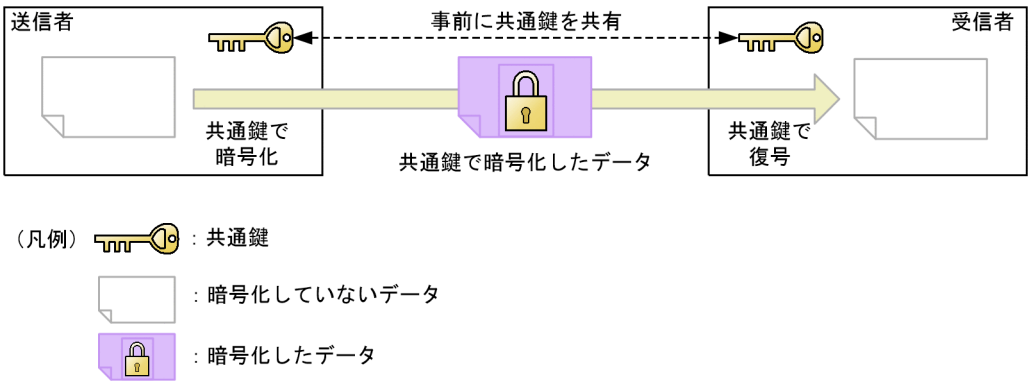
SSH では，次に示す暗号技術を使用して，セキュアな通信を実現します。

- 共通鍵暗号
- メッセージ認証コード
- 認証付き暗号
- 公開鍵アルゴリズム
- 鍵交換

(1) 共通鍵暗号

送信者と受信者で同じ鍵（共通鍵と呼ぶ）を使用します。共通鍵暗号は，送信者と受信者とで共通鍵を共有し，送信者はその鍵で暗号化し，受信者はその鍵で復号する技術です。共通鍵暗号による暗号化通信の例を次の図に示します。

図 9-6　共通鍵暗号による暗号化通信の例

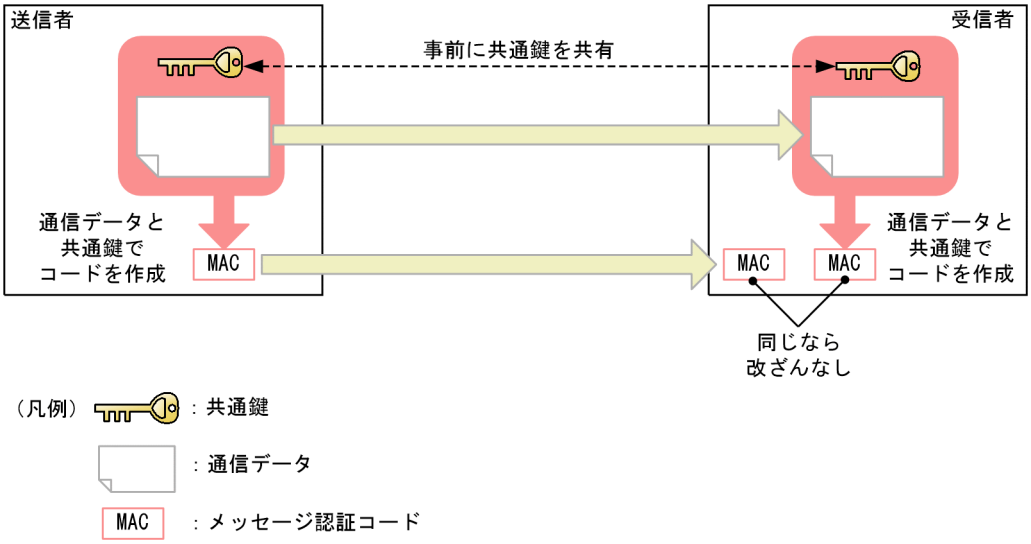


(2)　メッセージ認証コード

メッセージ認証コードは，共通鍵を使用して，送信者が送信した通信データが改ざんされていないことを確認する技術です。また，改ざんされていないことを確認するために使用する固定長のデータのことも，メッセージ認証コードと呼びます。

送信者は通信データと共通鍵を組み合わせてメッセージ認証コードを作成し，通信データと同時に送信します。受信者でも通信データと共通鍵を組み合わせてメッセージ認証コードを作成し，受信したメッセージ認証コードと比較します。比較した結果同じであれば，通信データが改ざんされてないことが確認できます。メッセージ認証コードによる改ざん確認の例を次の図に示します。

図 9-7　メッセージ認証コードによる改ざん確認の例



(3)　認証付き暗号

認証付き暗号は，共通鍵暗号とメッセージ認証コードを組み合わせた方式です。共通鍵を使用し，暗号とメッセージ認証を同時に実現します。

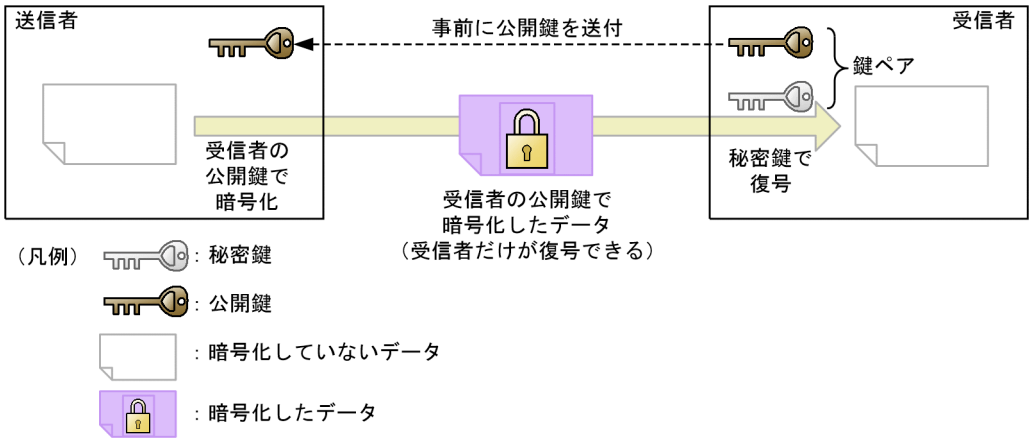
(4)　公開鍵アルゴリズム

公開鍵アルゴリズムは，二種類の鍵である公開鍵と秘密鍵を，ペアで使用するアルゴリズムです。ペアになる公開鍵と秘密鍵の組み合わせを鍵ペアと呼びます。

(a)　公開鍵暗号

公開鍵暗号は，公開鍵で暗号化し，秘密鍵で復号する暗号化技術です。受信者は鍵ペアを作成して，公開鍵だけを送信者へ送付します。送信者は，受信者の公開鍵でデータを暗号化して送信します。このように，秘密鍵を保持する受信者しか復号できない暗号化通信を実現します。公開鍵暗号による暗号化通信の例を次の図に示します。

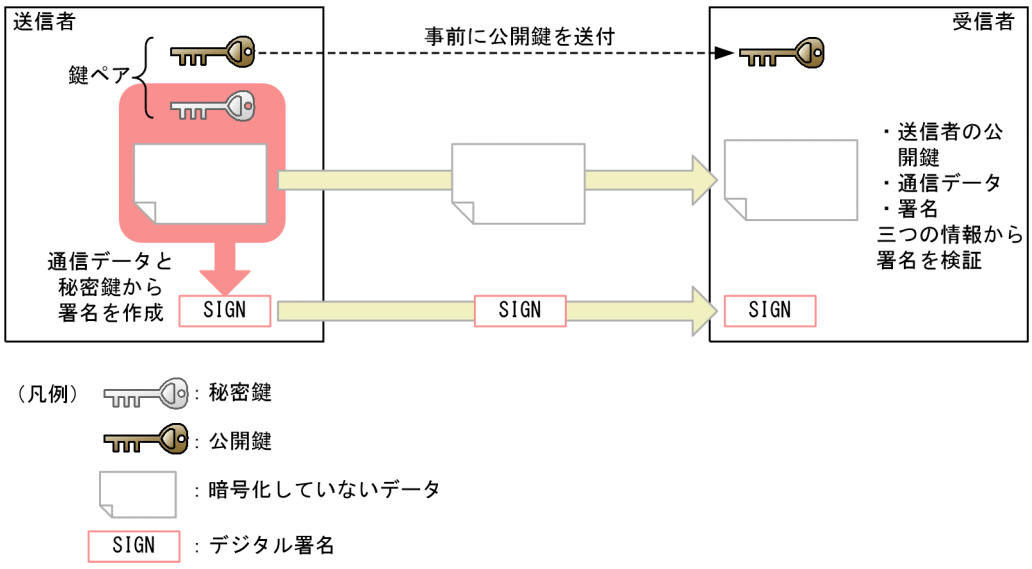
図 9-8　公開鍵暗号による暗号化通信の例



(b)　デジタル署名

デジタル署名は，通信データが改ざんされていないか，送信者が正しいかを確認する技術です。送信者は，あらかじめ公開鍵を受信者へ公開しておき，通信データと秘密鍵から署名を作成します。受信者は，通信データと署名と公開鍵から，署名が正しいことを確認します。署名が正しければ，通信データが改ざんされていないこと（通信データの認証），および送信者が秘密鍵の保有者であること（送信者の認証）が確認できます。デジタル署名の例を次の図に示します。

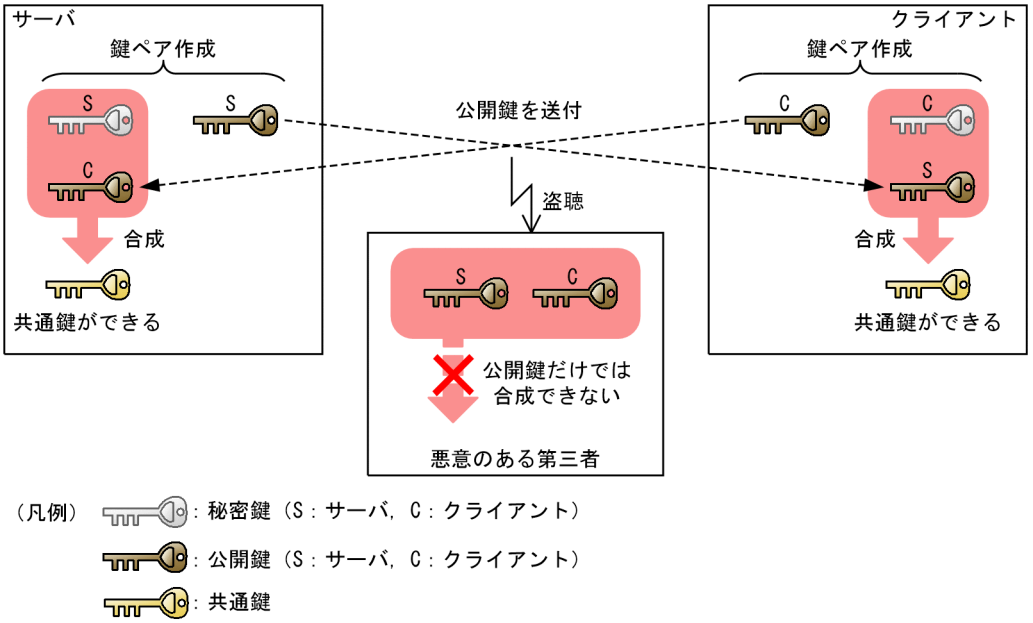
図 9-9　デジタル署名の例



(5)　鍵交換

鍵交換は，通信の両端が交換した情報を基に共通鍵を作成する方式です。サーバとクライアントは，それぞれ鍵ペアを生成し，互いに公開鍵を送付します。自装置の秘密鍵と対向装置の公開鍵を合成すると，サーバとクライアントで同じ共通鍵が生成されます。悪意ある第三者が盗聴してサーバとクライアントの公開鍵を入手しても，公開鍵だけでは共通鍵を作成できません。このため，サーバとクライアントの間で安全に共通鍵を共有できます。鍵交換の例を次の図に示します。

図 9-10　鍵交換の例



9.1.6　ログイン制御機能のサポート

(1)　リモート運用端末からのログインの許可および同時にログインできるユーザ数

本装置に対してセキュアリモートログインする場合やセキュアコマンド実行をする場合は，コンフィグレーションコマンド line vty を設定する必要があります。また，セキュアリモートログインとセキュアコマンド実行は，リモートログインのユーザ数としてカウントされ，ユーザ数の制限対象となります。

(2)　リモート運用端末の IP アドレスによる制限

リモート運用端末から本装置の SSH サーバへのアクセスは，リモート運用端末の IP アドレスによる制限対象となります。

(3)　ログインメッセージ表示

ログインバナーを設定すると，リモート運用端末から本装置へ SSH で接続した場合にも，ログイン前後にログインメッセージを表示します。

ログイン前のメッセージは，SSHv2 だけでサポートします。どの SSH 基本機能を利用する場合でも表示します。

ログイン後のメッセージは，SSHv1 と SSHv2 の両方でサポートします。なお，セキュアリモートログインの場合だけ表示し，セキュアコマンド実行，SCP，および SFTP の場合には表示しません。

9.1.7 RADIUS/TACACS+のサポート

本装置の SSH サーバは，RADIUS/TACACS+による認証，コマンド承認，およびアカウンティングをサポートしています。ただし，RADIUS/TACACS+によるログイン認証を使用できるのはパスワード認証だけです。詳細は，「8.2.2 RADIUS/TACACS+の適用機能および範囲」を参照してください。

9.1.8 SSH 使用時の注意事項

(1) 多国語 SSH クライアントの制限

日本語などの一部の多国語クライアントでは，ASCII 文字以外の文字（日本語など）でサーバへエラーメッセージを送付することがあります。

本装置の SSH サーバでログを表示する際，クライアントからのエラーメッセージを表示する部分では，送付された文字が ASCII 文字以外の場合に，ASCII 表示できる文字にエンコード変換されて表示します。

できるだけ，ASCII 文字でエラーメッセージを送付するクライアントを使用してください。

9.2　コマンドガイド

ここでは，SSH サーバ機能について説明します。なお，SSH クライアント機能はコンフィグレーションを設定する必要はありません。

9.2.1　コマンド一覧

SSH 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 9-11　コンフィグレーションコマンド一覧

コマンド名	説明
ip ssh	SSH サーバを動作させます。
ip ssh authentication	SSH サーバのユーザ認証方式を制限します。
ip ssh authkey	SSH サーバで公開鍵認証に使用するユーザ公開鍵を登録します。
ip ssh ciphers	SSHv2 サーバで使用する暗号方式を制限します。
ip ssh key-exchange	SSHv2 サーバで使用する鍵交換方式を制限します。
ip ssh macs	SSHv2 サーバで使用するメッセージ認証コード方式を制限します。
ip ssh version	SSH サーバの SSH プロトコルバージョンを制限します。
transport input※1	リモート運用端末から本装置へのアクセスに使用できるプロトコルを制限するために使用します。
ip access-group※2	リモート運用端末から本装置へのアクセスを，端末の IPv4 アドレスによって制限するために使用します。
ipv6 access-class※2	リモート運用端末から本装置へのアクセスを，端末の IPv6 アドレスによって制限するために使用します。

注※1

「コンフィグレーションコマンドレファレンス」「2　運用端末接続」を参照してください。

注※2

「コンフィグレーションコマンドレファレンス」「4　ログインセキュリティと RADIUS/TACACS+」を参照してください。

SSH サーバ機能の運用コマンド一覧を次に示します。

表 9-12　運用コマンド一覧

コマンド名	説明
show ssh hostkey	ホスト公開鍵とフィンガープリントを表示します。
set ssh hostkey	ホスト鍵ペアを変更します。
erase ssh hostkey	SSH ホスト鍵ペアを削除します。
show ssh logging	SSH サーバのトレースログを表示します。
clear ssh logging	SSH サーバのトレースログを消去します。

SSH クライアント機能の運用コマンド一覧を次に示します。

表 9-13 運用コマンド一覧

コマンド名	説明
ssh	セキュアリモートログイン機能およびセキュアコマンド実行機能を提供します。
sftp	セキュア FTP によってファイルを転送します。
scp	セキュアコピーによってファイルを転送します。

9.2.2 SSH サーバの基本設定（パスワード設定）

本装置の SSH サーバ機能を利用するために必要な設定を示します。ユーザ認証方式は，telnet と同じパスワード認証を使用します。

[設定のポイント]

SSH 接続に使用するユーザアカウントへのパスワードの設定例と，SSHv2 サーバを動作させる設定例を示します。セキュリティのため SSHv1 が不要な場合は，動作させる SSH のバージョンを SSHv2 に制限してください。

ログインユーザの作成時にパスワードを設定するように注意してください。パスワードを設定していないユーザは，SSH のパスワード認証でログインできないためです。ログインユーザの作成については，「8.1.3 ログインユーザの作成と削除」を参照してください。

SSH クライアントが本装置へ初めて接続するとき，SSH クライアントはホスト公開鍵のフィンガープリントを表示して正しいかどうか確認を要求します。本装置のホスト公開鍵とフィンガープリントの表示方法については，「9.2.7 ホスト公開鍵の確認」を参照してください。

[コマンドによる設定]

1. **# configure**
   (config)# ip ssh version 2
   SSH サーバが動作するバージョンを SSHv2 に制限します。
2. **(config)# ip ssh**
   SSH サーバの動作を開始させます。
3. **(config)# line vty 0 2**
   本装置へのリモートログインを許可します。この設定例では，ログインできるユーザ数を 3 に設定しています。

9.2.3 ユーザ認証に公開鍵認証を使用する設定

(1) ユーザ公開鍵を転送する場合

クライアントで作成したユーザ鍵ペアのうち，ユーザ公開鍵を本装置の SSH サーバへ登録し，公開鍵認証をする設定例を示します。

[設定のポイント]

あらかじめ，クライアントでユーザ公開鍵ファイルを作成し，本装置へ転送しておいてください。ユーザ公開鍵の転送には ftp を使用できますが，よりセキュリティを確保できる SCP または SFTP を使用することをお勧めします。

ここでは SECSH 形式の SSHv2 DSA のユーザ公開鍵で説明していますが，SSHv2 RSA や ECDSA のユーザ公開鍵，OpenSSH 形式や SSHv1 形式のユーザ公開鍵も同様の方法で登録できます。

[コマンドによる設定]

1. **(config)# ip ssh authentication publickey**
   ユーザ認証方式として公開鍵認証だけを許可します。
2. **(config)# ip ssh authkey staff client-v2 load-key-file /usr/home/staff/id_dsa_1024_a.pub**
   ユーザ（staff）の SSHv2 のユーザ公開鍵を，あらかじめ転送したファイル（/usr/home/staff/id_dsa_1024_a.pub）から読み込みます。このとき，この鍵の名前（インデックス名）を client-v2 とします。コンフィグレーションには，ユーザ公開鍵の内容が設定されます。

[注意事項]

各ユーザのホームディレクトリ配下に，「.ssh」という名前のディレクトリを作成しないでください。さらに，「.ssh」ディレクトリ配下にファイルを転送，コピー，および生成しないでください。

「.ssh」ディレクトリは，本装置の SSH サーバ機能が自動的に生成し，使用します。ユーザがファイルを置いた場合，削除されたり上書きされたりします。

(2)　SSHv2 ユーザ公開鍵（SECSH 形式）を直接入力する場合

公開鍵認証をするために，クライアントで作成したユーザ鍵ペアのうち，ユーザ公開鍵を本装置の SSH サーバへ登録します。

クライアントで，あらかじめ SECSH 形式のユーザ公開鍵を作成します。ip ssh authkey コマンドで SECSH 形式のユーザ公開鍵の内容を直接入力する場合は，ヘッダ（Comment:コメントなど），開始マーカ，終了マーカ，および改行コードを除いた，鍵の部分だけを入力してください。ユーザ公開鍵（SECSH 形式）の入力部分を次の図に示します。

図 9-11　SSHv2 ユーザ公開鍵（SECSH 形式）の入力部分

```
---- BEGIN SSH2 PUBLIC KEY ----
Subject: staff
Comment: "1024-bit dsa, staff@client1-pc, Tue Oct 22 20XX 16:21:35 +09¥
00"
AAAAB3NzaC1kc3MAAACBAPQX4hUjicV2cuSbb0eYug3Zwe1wdveLixNAcRX15dh8XDDIv1
drKW6LnxTDiM8wfsEPDoOCOZwae9VOLgpBFXqdNAHIBSPeKVEUvSBah+romEWRuPgBHIkJ
Wg3FbzkHV8cYiQxzAZT87RunikN9j2kq+ftoJIs7IWR4gHXby/JTAAAAFQDTI3fYwEZaZE
F1ZATkUeLsaBnn/wAAAIEAhy3mVaF87Pjjbaq+XY+I2mjIOptqGb7KcTKvbfb2JZVscidx
zOaKnNWRMJtsZSyMXkpdEjaWNmQvbV6MDGn3PYX63CLomIsWUPxdo7bcOJFyx1GvZ4bef7
JTP9xO48/IFSwQTL7bKeXZ9cidgGXMmch8Tz15WSu8rP+t3m/yS7gAAACAZ/yWFB1rI8Be
NkvcsmiIupce2hb2uaef/4I7ymPT9irDQsfRY3RxiG5KOUh7g84j9WFtx/y9KtFk46hUiz
NYnkkVcEwjo1uTbhtRpehFObUYPyQu+ZxFDHZ3vB1oONOfaOU4xME18RC4CHax+Fm/OUMd
PzpzAD6FZHS+9zkdi7k=
---- END SSH2 PUBLIC KEY ----
```

入力する部分

[設定のポイント]

この例では，ユーザ公開鍵ファイルの内容を ip ssh authkey コマンドで直接入力して，ユーザ公開鍵を登録します。

ここでは SECSH 形式の SSHv2 DSA のユーザ公開鍵で説明していますが，SSHv2 RSA や ECDSA のユーザ公開鍵も同様の方法で登録できます。

[コマンドによる設定]

1. **(config)# ip ssh authkey staff client-v2 "AAAAB3NzaC…S+9zkdi7k="**

SSHv2 クライアントであらかじめ作成したユーザ（staff）のユーザ公開鍵（SECSH 形式）の内容を，途中で改行しないようにダブルクォート（"）で囲んで入力します。このとき，このユーザ公開鍵の名前（インデックス名）を client-v2 とします。

[注意事項]

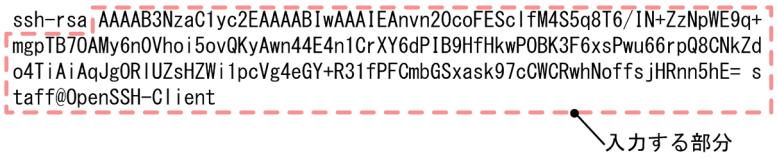
SECSH 形式のユーザ公開鍵には改行コードが含まれているため，すべての改行を取り除いて 1 行の形式にしてください。また，変換後のユーザ公開鍵の部分に空白を含めないでください。空白のあとは，コメントと見なされます。

(3)　SSHv2 ユーザ公開鍵（OpenSSH 鍵）を直接入力する場合

公開鍵認証をするために，クライアントで作成したユーザ鍵ペアのうち，ユーザ公開鍵を本装置の SSH サーバへ登録します。

クライアントで，あらかじめ OpenSSH 形式のユーザ公開鍵を作成します。ip ssh authkey コマンドで SECSH 形式のユーザ公開鍵の内容を直接入力する場合は，先頭にある「ssh-rsa」，「ecdsa-sha2-nistpXXX」，または「ssh-dss」を取り除いた部分を，改行コードを含めないでそのまま 1 行で入力してください。ユーザ公開鍵（OpenSSH 鍵）の入力部分を次の図に示します。

図 9-12　SSHv2 ユーザ公開鍵（OpenSSH 鍵）の入力部分



[設定のポイント]

この例では，ユーザ公開鍵ファイルの内容を ip ssh authkey コマンドで直接入力して，ユーザ公開鍵を登録します。

ここでは OpenSSH の SSHv2 RSA ユーザ公開鍵で説明していますが，SSHv2 DSA や ECDSA のユーザ公開鍵も同様の方法で登録できます。

[コマンドによる設定]

1. **(config)# ip ssh authkey staff client-O "AAAAB…n5hE= staff@OpenSSH-Client"**

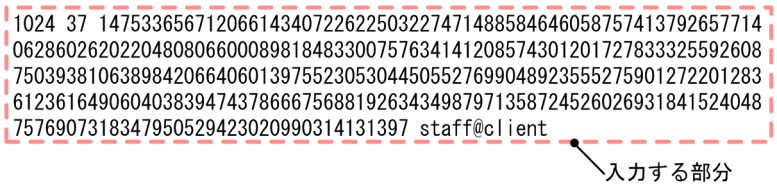
   あらかじめ作成したユーザ（staff）の SSHv2 のユーザ公開鍵（OpenSSH 形式）を，途中で改行しないようにダブルクォート（"）で囲んで入力します。このとき，このユーザ公開鍵の名前（インデックス名）を client-O とします。

(4)　SSHv1 ユーザ公開鍵を直接入力する場合

公開鍵認証をするために，クライアントで作成したユーザ鍵ペアのうち，ユーザ公開鍵を本装置の SSH サーバへ登録します。

クライアントで，あらかじめ SSHv1 ユーザ公開鍵を作成します。ユーザ公開鍵の入力部分を次の図に示します。

図 9-13　SSHv1 ユーザ公開鍵の入力部分



[設定のポイント]

この例では，ユーザ公開鍵ファイルの内容を ip ssh authkey コマンドで直接入力して，ユーザ公開鍵を登録します。

[コマンドによる設定]

1. **(config)# ip ssh authkey staff client-v1 ”1024 37 14753…31397 staff@client”**

   あらかじめ作成したユーザ (staff) の SSHv1 のユーザ公開鍵を，途中で改行しないようにダブルクォート（"）で囲んで入力します。このとき，このユーザ公開鍵の名前（インデックス名）を client-v1 とします。

9.2.4　SSHv2 サーバの暗号アルゴリズムの設定変更

SSHv2 のセキュリティ機能では，ホスト認証とユーザ認証のほかに，鍵交換，暗号化，メッセージ認証を使用します。本装置の SSHv2 サーバ機能では，鍵交換，暗号化，メッセージ認証についても，複数の種類のアルゴリズムをサポートしています。

[設定のポイント]

サポートしている複数のアルゴリズムのうちから，使用するアルゴリズムを設定します。

[コマンドによる設定]

1. **(config)# ip ssh key-exchange ecdh-sha2-nistp256 diffie-hellman-group14-sha256**

   SSHv2 サーバの鍵交換アルゴリズムとして，ecdh-sha2-nistp256 と diffie-hellman-group14-sha256 だけを使用するように設定します。

2. **(config)# ip ssh ciphers aes128-gcm@openssh.com aes128-ctr**

   SSHv2 サーバの暗号化アルゴリズムとして，認証付き暗号の aes128-gcm@openssh.com と，共通鍵暗号の aes128-ctr だけを使用するように設定します。

3. **(config)# ip ssh macs hmac-sha2-256 hmac-sha1**

   SSHv2 サーバのメッセージ認証コードアルゴリズムとして，hmac-sha2-256 と hmac-sha1 だけを使用するように設定します。

9.2.5　リモート運用端末からの SSH 接続を許可する IP アドレスの設定

リモート運用端末からのアクセスを許可する IP アドレスを制限すると，SSH による接続も制限されます。アクセスを許可する IP アドレスの設定例については，「8.1.7　リモート運用端末からのログインを許可する IP アドレスの設定」を参照してください。

9.2.6 RADIUS/TACACS+機能と連携した SSH サーバの設定

RADIUS/TACACS+を設定すると，SSH サーバも RADIUS/TACACS+と連携して動作します。RADIUS/TACACS+のコンフィグレーションについては，「8.3 RADIUS/TACACS+のコマンドガイド」を参照してください。

9.2.7 ホスト公開鍵の確認

SSH クライアントが SSH サーバを確認できるように，各 SSH サーバは異なるホスト鍵ペアを保持しています。SSH クライアント側では，SSH サーバに初めて接続する場合や，ホスト公開鍵が変更された場合に，そのサーバのフィンガープリントを確認するようにメッセージが表示されます。このとき，あらかじめ接続先サーバのフィンガープリント（またはホスト公開鍵）を入手しておき，接続時に目視確認することでより安全に接続できます。

show ssh hostkey コマンドで，SSHv1/SSHv2 のホスト公開鍵およびそのフィンガープリントが確認できます。

図 9-14 ホスト公開鍵の表示

```
> show ssh hostkey
Date 20XX/01/20 12:00:00 UTC
******* SSHv1 Hostkey *******
1024 65537 14698797177375959661209963212352629087681324221885617869300690227975249964150563327374294515778228277627736937005824220192838922145093952246943786354524785835232009819519418410439056570668557966909117970589675621692841311987886107483073232336049430761156956847716463382453597556633690675063768429754776320874 9 1024-bit rsa1 hostkey

Fingerprint for key:
SHA256:gblxC3SCNJsZfjaV5BC6rcckTR+B/hYYTEcBEQO00m8
MD5:c9:d5:c0:4f:1b:2e:ff:b7:2e:9d:c3:66:ed:93:d3:4e

******* SSHv2 DSA Hostkey *******
ssh-dss AAAAB3NzaC1kc3MAAACBAJenC0V9Xr8ahylD8fqpiAIYGwpjoRqDosb9udd/bDkxicU5YAhwsKktXvh5lPI+GDL0JVB5hHOVmVCH45PAcoAx+xrEvL2wjoghhLVzDbTfyCCtehxvfcsVxoJSBhGggtWTmllytogGvE3us2vCgEybau8qIpUy+BiA7ONunIDpAAAAFQDz1v9c2U8Eh5xNCApzCFL2ez48gwAAAIAOeAgtPewuIHY1Q3z00SawBa2xWrLxly4WcFrzfAja9GIRp/+s3iJLu/6UZ5nyMyjSF10KAZUzFSG+HteGE/pLB1c+r4B2okzZVH1R7tnst/LAoDg3fQObTF74+j7cGMIwgE0i1E8hciHq9NmQ9RBe2uBxsej8crzXDTpljfP/gQAAAIB3IWnKpTSvI4Rs49ItzGY+SS5DfkSy+BKB1VFB1xoUr/DYFpT4Q4kA3RTuPFxpjElEIIUP5/+WET/iJSBizyfpwM/lairBhWtSNyOcjeWLD9eYVhw1HqexjQLl8BvTFQtICWWvsviYgNGUGfwTH0RZ6B5HKKO5IVs6bh2VVHoq2A== 1024-bit dsa hostkey

Fingerprint for key:
SHA256:EH9axeEZO+hj5qzBRqx4fgyncb/J5BN4DffD/my9tN8
MD5:21:b9:aa:78:66:df:02:67:01:48:86:88:cb:31:c4:da

******* SSHv2 RSA Hostkey *******
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDQ0re6puJtq2gqvyZwzWVqlJgxPuXo7EphTgysp4av+LaGYdiU2jYoQ66Eo4759z4fZQ/yHtXJicaDMvIz3iNbBQTr01x4F/5m1oR5UJS7XHfhqc5pGNLKglEaIZo8dJkKOo72xI1HERY11ICobKshhWHpGP95WmrRIdxBGUDZKBIk8iW0CeS5duMksrL9O0LMLf1+NXkELmJBT/npMkHiZHBPJcKn1kPRiq5X8igO3THLKeYcPUzOPOkUAUrIDT42s8oJG2FkwO6CIewQcGK9zkCcqKPyFyZahDI8OvwZ05o7VOQb3/sLNiFZfQlRqoGxpiGvNZae76Hb6kS3+cOJ+Yyu/Tbz5kKK0Bz70dxb+4DqClV7yYfquiTdues6hOO8+KAUttNf/w3PNSyjFUFyRxcEDENvxDDq11/gA78VXWitre1ZMin9ybsSEZGzIS7OzDd0I5/AosKcYNWGkLRrBdGFcB5mJ/9haTALMOWsyxbF3RjXMvcCWVUpxbGKuqs= 3072-bit rsa host key

Fingerprint for key:
SHA256:lnaICZdvjFnmZoRCum+XblmhEmcilZhq15w4W8R3vOg
MD5:81:48:0e:52:a6:7f:64:d8:29:57:e8:fb:4b:34:bb:a0

******* SSHv2 ECDSA Hostkey *******
ecdsa-sha2-nistp384 AAAAE2VjZHNhLXNoYTItbmlzdHAzODQAAAAIbmlzdHAzODQAAABhBNLBG8RhJwOBU8Z/e+c1wz6qwZP+IHXM6iUINja2EMOi947VPI8/CA7ZK2INnUW7lXaqkeu6LihUN68wwz8Gisgx9sAPthB3VkNqBEsvKjxk2aSC1/neygmD5H/5Wo9Q6A== 384-bit ecdsa hostkey

Fingerprint for key:
SHA256:rnuan5fOrHpNP8IVbZgKNt+t+x/EVTxWKF3tF2CMRA0
MD5:69:5f:70:c3:a0:09:91:e8:70:12:fe:c5:52:21:fe:19

>
```

9.2.8　ホスト鍵ペアの変更

本装置ではホスト鍵ペアは初回の装置起動時に自動生成されるため，SSH サーバとして運用するに当たり，意図してホスト鍵ペアを生成する必要はありません。

本装置を別の用途へ転用する場合は，SSH のホスト鍵ペアを変更することをお勧めします。SSH のホスト鍵ペアを変更する場合は，set ssh hostkey コマンドを実行します。

また，SSHv2 のホスト鍵としてデフォルトの RSA 2048bit 以外のホスト鍵ペアを使用する場合にも，set ssh hostkey コマンドを実行します。デフォルトの RSA ホスト鍵ペアを使用しない場合には，erase ssh hostkey コマンドを実行して RSA ホスト鍵ペアを削除してください。

図 9-15　ホスト鍵ペア（SSHv1 RSA と SSHv2 RSA）の変更

```
> enable
# set ssh hostkey

WARNING!!
Would you wish to generate SSHv1 RSA and SSHv2 RSA hostkeys? (y/n): y
Generating public/private rsa1 key pair.
The key fingerprint is:
SHA256:nxeQpjv+aQOQXo6Wqg0Q9BklwosYJ7K3kkUCXgXwwBg
MD5:a6:7e:c8:3c:0a:d7:ae:e8:78:58:66:8e:9e:be:e8:3a

Generating public/private rsa key pair.
The key fingerprint is:
SHA256:fDIqAY5v/ybGewFybchsJ1r3gMCnYkGTdKJr0TwAtkc
MD5:42:06:3d:06:50:3a:29:4a:2a:79:2f:3c:d4:cc:ea:48

The hostkey generation is completed.
#
```

図 9-16　SSHv2 ECDSA ホスト鍵ペアの作成および SSHv2 DSA ホスト鍵ペアの削除

```
> enable
# set ssh hostkey ecdsa 521

WARNING!!
Would you wish to generate the SSHv2 ECDSA hostkey? (y/n): y
Generating public/private ecdsa key pair.
The key fingerprint is:
SHA256:jTz5rFJlA6oIrYrWKb6EueKvHcyCQXA1jYU1N+orgqg
MD5:0c:c1:c4:8a:38:b0:46:66:2e:ff:f2:44:3c:57:88:4e

The hostkey generation is completed.
# erase ssh hostkey dsa

WARNING!!
Would you wish to erase the SSHv2 DSA hostkey? (y/n): y

The hostkey was erased successfully.
#
```

10 時刻の設定と NTP

この章では，時刻の設定と NTP について説明します。

10.1　解説

時刻は，本装置の初期導入時に設定してください。時刻は，本装置のログ情報や各種ファイルの作成時刻などに付与される情報です。運用開始時には正確な時刻を本装置に設定してください。運用コマンド set clock で時刻を設定できます。

また，このほかに，NTP プロトコルを使用して，ネットワーク上の NTP サーバと時刻の同期ができます。本装置は RFC5905 NTP バージョン 3 および 4 に準拠しています。なお，本装置は NTP モード 6 およびモード 7 のパケットには応答しません。

10.1.1　NTP サポート仕様

本装置でサポートしている NTP の機能を次の表に示します。

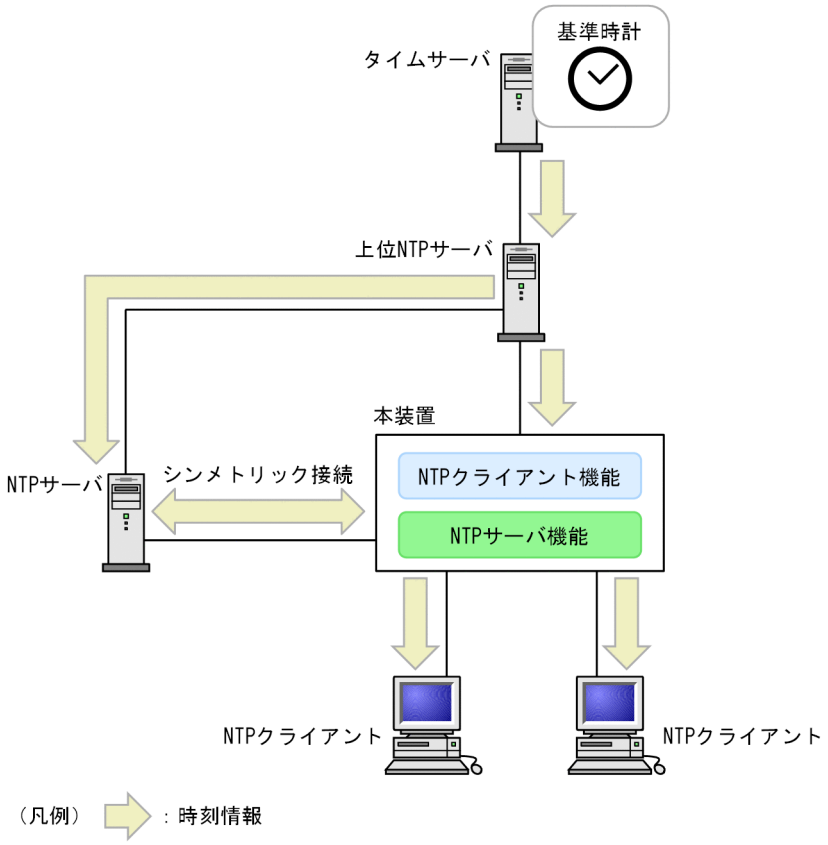
表 10-1　本装置でサポートする NTP の機能

機能		内容	サポート
クライアント機能	ユニキャストクライアント	本装置の時刻を上位 NTP サーバの時刻に同期します。	○
	ブロードキャストクライアント		○
	マルチキャストクライアント		×
サーバ機能	ユニキャストサーバ	NTP クライアント，または下位 NTP サーバに，本装置から時刻を提供します。	○
	ブロードキャストサーバ		○
	マルチキャストサーバ		×
シンメトリック接続		双方向で時刻を同期します。	○
ローカルタイムサーバ		上位 NTP サーバと通信できなくなった場合に，本装置がローカルタイムサーバとして機能し，本装置の時刻を NTP クライアントに提供します。	○
認証		ほかの装置と時刻を同期する場合に，セキュリティを目的とした認証をします。これによって，不正な NTP サーバによる時刻の改変を防止します。	○

（凡例）○：サポート　×：未サポート

本装置と上位 NTP サーバとの接続，および本装置と NTP クライアントの接続を次の図に示します。

図 10-1　NTP での接続構成



10.1.2　クライアント機能

(1)　接続形態

(a)　ユニキャストクライアント

上位 NTP サーバがユニキャストサーバの場合，コンフィグレーションコマンド ntp server で上位 NTP サーバを設定することで，本装置はユニキャストクライアントとして動作し，サーバの時刻と同期します。

(b)　ブロードキャストクライアント

上位 NTP サーバがブロードキャストサーバの場合，コンフィグレーションコマンド ntp broadcast client を設定することで，本装置はブロードキャストクライアントとして動作し，サーバの時刻と同期します。

(2)　認証

本装置が NTP クライアントとして送受信する NTP メッセージに付ける認証鍵を次の表に示します。

表 10-2　本装置が NTP クライアントとして動作時に付ける認証鍵

本装置の接続形態	本装置からの送信	本装置での受信
ユニキャストクライアント	コンフィグレーションコマンド ntp server の key パラメータで指定した認証鍵	任意の認証鍵 (本装置のコンフィグレーションに設定されている認証鍵)
ブロードキャストクライアント	送信はありません	

(3)　上位 NTP サーバの選択

システム内に上位 NTP サーバが複数存在する場合，次に示す手順「(a)　同期不適合の判定」～「(c)　クラスターアルゴリズム」に従って，最適な NTP サーバを選択します。接続している各 NTP サーバの動作状態は，運用コマンド show ntp associations で確認できます。

(a)　同期不適合の判定

次に示す条件のどれかに該当する NTP サーバを，同期先選択の対象 NTP サーバから除外します。

表 10-3　同期不適合条件

不適合条件	詳細
NTP サーバが同期できない	NTP サーバが非同期状態 受信した NTP メッセージの LI フラグ＝ 3
	NTP サーバの stratum 値が不適合 受信した NTP メッセージの stratum 値≧16
NTP サーバの距離限界	NTP サーバのルート距離※＞ 1 秒＋ポーリング間隔で発生する遅れ時間
ループ状態（NTP サーバの同期先が本装置）	NTP サーバの Reference ID（ref id）が本装置の IP アドレス
無通信状態	NTP サーバの reach ＝ 0（過去 8 回の送信で一度も受信がない）

注※

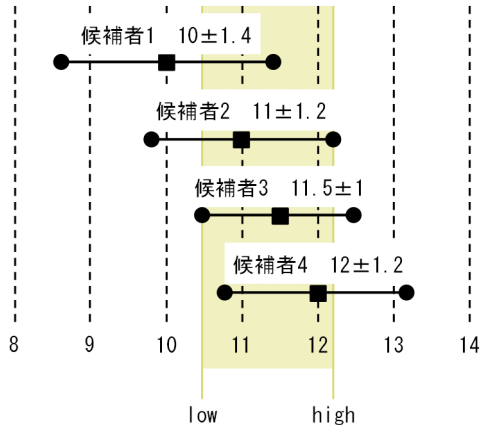
prefer パラメータが指定された NTP サーバから受信したメッセージの Root Dispersion は，上限 500 ミリ秒に制限されます。

(b)　インターセクションアルゴリズム

各候補者の「offset±ルート距離」が，最も多くの候補者で重なる下限（low）と上限（high）を求めます。このうち，offset が low～high の範囲内の候補者を truechimer（適切な候補者），範囲外の候補者を falseticker（不適切な候補者）とし，falseticker を候補者から除外します。ただし，prefer パラメータが指定された NTP サーバは，常に truechimer となります。

インターセクションアルゴリズムの選択例を次の図に示します。この例では，最も多くの候補者が重なる区間は 10.5～12.2 で，候補者 1 が falseticker となり除外されます。

図 10-2　インターセクションアルゴリズムの選択例



(c)　クラスターアルゴリズム

候補者の中で，offset の標準偏差（jitter）を見ることで，さらに多くの offset が集まっている範囲に絞り込み，集まりから外れている候補者（outlier）を除外していきます。

現在の同期先 NTP サーバが，残った候補者の中にある場合は，現在の同期先 NTP サーバを同期先として選択します。それ以外の場合，残った候補者の中から，stratum 値が最小（stratum 値が同じ場合はルート距離が小さい方）の候補者を同期先として選択します。

なお，prefer パラメータを指定された候補者がいる場合は，絞り込みは無効で，その候補者を無条件で同期先とします。

10.1.3　サーバ機能

本装置は NTP サーバとして動作できます。本装置から時刻を提供するためには，他の NTP サーバと時刻同期している，またはローカルタイムサーバとして動作している必要があります。

(1)　接続形態

(a)　ユニキャストサーバ

本装置はユニキャストサーバとして，NTP クライアントおよび下位 NTP サーバにクライアント／サーバモードで接続し，時刻を提供します。

(b)　ブロードキャストサーバ

本装置をブロードキャストサーバとする場合，コンフィグレーションコマンド ntp broadcast を設定することで，NTP クライアントおよび下位 NTP サーバに時刻を提供します。

(2)　認証

本装置が NTP サーバとして送受信する NTP メッセージに付ける認証鍵を次の表に示します。

表 10–4　本装置が NTP サーバとして動作時に付ける認証鍵

本装置の接続形態	本装置からの送信	本装置での受信
ユニキャストサーバ	ユニキャストクライアントから受信した NTP メッセージの認証鍵※	任意の認証鍵 （本装置のコンフィグレーションに設定されている認証鍵）
ブロードキャストサーバ	コンフィグレーションコマンド ntp broadcast の key パラメータで指定した認証鍵	受信はありません

注※

ユニキャストクライアントから認証情報がない NTP メッセージを受信した場合は，認証情報なしの応答メッセージを送信します。

10.1.4　シンメトリック接続

(1)　接続形態

本装置は，コンフィグレーションコマンド ntp peer で設定された IP アドレスの装置と，アクティブ／パッシブモードでシンメトリック接続します。また，設定されていない IP アドレスから受信したシンメトリック要求の時刻には同期しません。

上位 NTP サーバとの接続が切断した場合でも，シンメトリック接続した NTP サーバを経由することでシステムの時刻を同期します。

(2)　認証

シンメトリック接続する装置に対して，本装置が送受信する NTP メッセージに付ける認証鍵を次の表に示します。

表 10-5　本装置が NTP クライアントとして動作時に付ける認証鍵

本装置の接続形態	本装置からの送信	本装置での受信
シンメトリック接続	コンフィグレーションコマンド ntp peer の key パラメータで指定した認証鍵※	任意の認証鍵 (本装置のコンフィグレーションに設定されている認証鍵)

注※

ユニキャストクライアントから認証情報がない NTP メッセージを受信した場合は，認証情報なしの応答メッセージを送信します。

10.1.5　ローカルタイムサーバ

コンフィグレーションコマンド ntp master を設定すると，上位 NTP サーバと通信できなくなった場合に，本装置はローカルタイムサーバとして動作します。

システム内に複数のローカルタイムサーバが存在する場合は，システム内の時刻が同期されないおそれがあるため，シンメトリック接続の構成にしてください。

10.1.6　NTP 使用時の注意事項

- NTP は，各装置が誤差の範囲内で正しい時刻を保持していることを前提としています。このため，関係する装置間の時刻の差が想定外に大きい場合は，時刻が同期されません。
- 本装置と同期先 NTP サーバの時刻の差が 128 ミリ秒以上になった場合は，同期する前に 900 秒の確認期間が必要です。
- 次に示すときは，上位サーバとの時刻の差が 1000 秒（約 17 分）以上でも時刻を同期します。
  - 装置起動時
  - NTP に関するコンフィグレーション設定時
  - 運用コマンド restart ntp および set clock の実行時
- 装置が再起動されると 1 秒程度の誤差が発生します。このため，停電や運用コマンド reload などによって再起動したあと，上位 NTP サーバに再同期して下位 NTP クライアントへ時刻を提供できるようになるまでに 10 分程度を必要とします。

- 本装置の NTP クライアントは，dispersion が 1 秒を超える上位 NTP サーバには同期しません。ただし，コンフィグレーションコマンド ntp server で prefer パラメータが指定された場合は，過大な dispersion を無視して同期します。dispersion が 1 秒を超える上位 NTP サーバに同期させたい場合は，prefer パラメータを指定してください。
- ループバックインタフェースで装置の IP アドレスが設定されている場合，NTP パケット送信時の送信元 IP アドレスとして，ループバックインタフェースの IP アドレスを使用します。そのため，本装置を同期元または同期先とする場合は，IP アドレスとしてループバックインタフェースの IP アドレスを指定してください。ループバックインタフェースの IP アドレスの追加，変更，および削除時には，運用コマンド restart ntp で NTP プログラムを再初期化してください。
- NTP によるうるう秒挿入の瞬間には，本装置は“23:59:60”を“23:59:59”と表示します。次に示す表の項番 3 の状態です。

表 10-6　うるう秒挿入時の UTC と本装置の時刻表示

項番	UTC	本装置
1	12/31　23:59:58	12/31　23:59:58
2	12/31　23:59:59	12/31　23:59:59
3	12/31　23:59:60	12/31　23:59:59
4	01/01　00:00:00	01/01　00:00:00
5	01/01　00:00:01	01/01　00:00:01

10.1.7　時刻変更に関する注意事項

本装置で収集している統計情報の CPU 使用率は，時刻が変更された時点で 0 にクリアされます。

10.2　コマンドガイド

10.2.1　コマンド一覧

時刻設定および NTP 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 10-7　コンフィグレーションコマンド一覧

コマンド名	説明
clock timezone	タイムゾーンを設定します。
ntp access-group	アクセスグループを作成し，IPv4 アドレスフィルタによって，NTP サービスへのアクセスを許可または制限できます。
ntp authenticate	NTP 認証機能を有効化します。
ntp authentication-key	認証鍵を設定します。
ntp broadcast	インタフェースごとにブロードキャストで NTP パケットを送信し，ほかの装置が本装置に同期するように設定します。
ntp broadcast client	接続したサブネット上の装置からの NTP ブロードキャストメッセージを受け付けるための設定をします。
ntp broadcastdelay	NTP ブロードキャストサーバと本装置間で予測される遅延時間を指定します。
ntp master	ローカルタイムサーバを設定します。 上位 NTP サーバが存在しない場合に，本装置がローカルタイムサーバとして機能し，本装置の時刻を NTP クライアントに提供します。
ntp peer	NTP サーバと本装置でシンメトリック接続し，アクティブ/パッシブモードを構成します。
ntp server	本装置をクライアントモードに設定し，クライアントサーバモードを構成します。
ntp trusted-key	ほかの装置と同期する場合に，セキュリティ目的の認証をするように鍵番号を設定します。

時刻設定および NTP に関する運用コマンド一覧を次の表に示します。

表 10-8　運用コマンド一覧

コマンド名	説明
set clock	日付，時刻を表示，設定します。
show clock	現在設定されている日付，時刻を表示します。
show ntp associations	接続されている NTP サーバの動作状態を表示します。
restart ntp	ローカル NTP サーバを再起動します。

10.2.2　システムクロックの設定

[設定のポイント]

日本時間として時刻を設定する場合は，あらかじめコンフィグレーションコマンド clock timezone でタイムゾーンに JST，UTC からのオフセットを+9 に設定する必要があります。

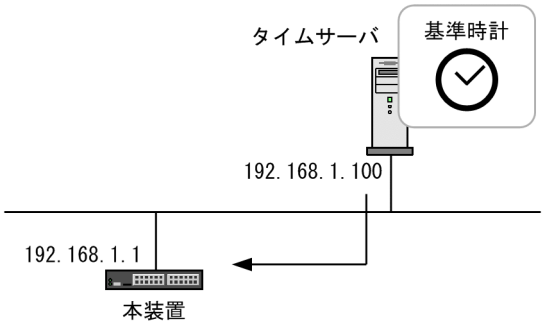
[コマンドによる設定]

1. **(config)# clock timezone JST +9**
   日本時間として，タイムゾーンに JST，UTC からのオフセットを+9 に設定します。
2. **(config)# save**
   (config)# exit
   保存し，コンフィグレーションモードから装置管理者モードに移行します。
3. **# set clock 2109011530**
   Wed Sep 1 15:30:00 JST 2021
   2021 年 9 月 1 日 15 時 30 分に時刻を設定します。

10.2.3　クライアント機能の設定

NTP 機能を使用して，本装置の時刻をタイムサーバの時刻に同期させます。

図 10-3　NTP 構成図（タイムサーバへの時刻の同期）



(1)　ユニキャストクライアント

本装置をユニキャストクライアントとして，上位 NTP サーバと時刻の同期をします。

[設定のポイント]

コンフィグレーションコマンド ntp server で，同期先タイムサーバの IP アドレスを設定します。

[コマンドによる設定]

1. **(config)# ntp server 192.168.1.100**
   IP アドレス 192.168.1.100 のタイムサーバに本装置を同期させます。

(2)　ブロードキャストクライアント

本装置をブロードキャストクライアントとして，上位 NTP サーバと時刻の同期をします。

[設定のポイント]

コンフィグレーションコマンド ntp broadcast client で，サブネット上の装置からの NTP ブロードキャストメッセージを受け付ける設定をします。

[コマンドによる設定]

1. **(config)# ntp broadcast client**

ほかの装置からの NTP ブロードキャストを受信して本装置を同期させます。

10.2.4　サーバ機能の設定

本装置をブロードキャストサーバとして，NTP クライアントまたは下位 NTP サーバに時刻を提供します。

[設定のポイント]

コンフィグレーションコマンド ntp broadcast で，インタフェースごとにブロードキャストで NTP パケットを送信する設定をします。

[コマンドによる設定]

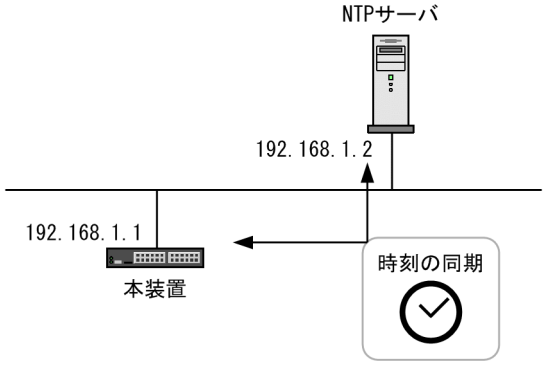
1. **(config)# interface vlan 300**
   (config-if)# ip address 192.168.1.1 255.255.255.0
   (config-if)# ntp broadcast

指定されたインタフェースに対して，NTP ブロードキャストの設定をします。本装置の時刻が NTP サーバに同期すると，IPv4 アドレス 192.168.1.0，サブネット 255.255.255.0 のネットワークに NTP ブロードキャストパケットを送信します。

10.2.5　シンメトリック接続の設定

NTP 機能を使用して，本装置の時刻とシンメトリック接続する NTP サーバの時刻をお互いに調整しながら，同期させます。

図 10-4　NTP 構成図（NTP サーバとの時刻の同期）



[設定のポイント]

コンフィグレーションコマンド ntp peer で，シンメトリック接続先 NTP サーバの IP アドレスを設定します。

[コマンドによる設定]

1. **(config)# ntp peer 192.168.1.2**

IP アドレス 192.168.1.2 の NTP サーバとの間をシンメトリック接続として設定します。

10.2.6　認証の設定

本装置が NTP クライアント，NTP サーバ，およびシンメトリック接続のどの接続形態で認証する場合にも，まず認証鍵を設定します。その後，使用する接続形態に応じた設定をする際に鍵番号を指定します。

(1)　認証鍵の設定

[設定のポイント]

NTP 認証で使用する鍵番号と認証鍵を設定します。

[コマンドによる設定]

1. **(config)# ntp authenticate**
   NTP 認証機能を有効にします。
2. **(config)# ntp authentication-key 1 md5 NtP001**
   NTP 認証鍵として，鍵番号 1 に「NtP001」を設定します。
3. **(config)# ntp trusted-key 1**
   NTP 認証に使用する鍵番号 1 を指定します。

(2)　クライアント機能

クライアント機能で認証を使用する場合は，次に示す設定をします。

[設定のポイント]

クライアント機能を設定するコマンドの key パラメータで，認証鍵として設定した鍵番号を指定します。ここでは，ユニキャストクライアントを設定する例を示します。

[コマンドによる設定]

1. **(config)# ntp server 192.168.1.100 key 1**
   本装置の時刻を上位 NTP サーバ（192.168.1.100）に同期させます。その際，鍵番号 1 を使用した認証をするため，本装置が送信する認証鍵の鍵番号を 1 とします（上位 NTP サーバはクライアントが送信した鍵番号で応答します）。
   上位 NTP サーバ側も同様に NTP 認証を設定してください。

(3)　サーバ機能

サーバ機能で認証を使用する場合は，次に示す設定をします。

[設定のポイント]

ブロードキャストサーバ機能を設定するコマンドの key パラメータで，認証鍵として設定した鍵番号を指定します。

[コマンドによる設定]

1. **(config)# interface vlan 300**
   (config-if)# ip address 192.168.100.1 255.255.255.0
   (config-if)# ntp broadcast key 1

ブロードキャストの NTP メッセージを送信する VLAN インタフェースを指定します。本装置から送信する鍵番号は 1 です。

(4)　シンメトリック接続

[設定のポイント]

シンメトリック接続を設定するコマンドの key パラメータで，認証鍵として設定した鍵番号を指定します。

[コマンドによる設定]

1. **(config)# ntp peer 192.168.1.200 key 1**

本装置の時刻をシンメトリック接続先 NTP サーバ（192.168.1.200）に同期させます。その際，鍵番号 1 を使用した認証をするため，本装置が送信する認証鍵の鍵番号を 1 とします。本装置はシンメトリック接続した NTP サーバが送信する鍵番号で認証をします。

シンメトリック接続先 NTP サーバ側も同様に NTP 認証を設定してください。

本装置が送信する鍵番号と，シンメトリック接続先 NTP サーバが送信する鍵番号を，異なる鍵番号にもできます。その場合は，認証鍵の設定時に，シンメトリック接続先 NTP サーバが送信する鍵番号の設定を追加してください。

11 ホスト名と DNS

この章では，ホスト名と DNS の解説と操作方法について説明します。

11.1　解説

本装置では, ネットワーク上の装置を識別するためにホスト名情報を設定できます。設定したホスト名情報は, 本装置のログ情報などのコンフィグレーションを設定するときにネットワーク上のほかの装置を指定する名称として使用できます。本装置で使用するホスト名情報は次に示す方法で設定できます。

- コンフィグレーションコマンド ip host／ipv6 host で個別に指定する方法
- DNS リゾルバ機能を使用してネットワーク上の DNS サーバに問い合わせる方法

コンフィグレーションコマンド ip host／ipv6 host を使用して設定する場合は，使用するホスト名ごとに IP アドレスとの対応を明示的に設定する必要があります。DNS リゾルバを使用する場合は，ネットワーク上の DNS サーバで管理されている名称を問い合わせて参照するため，本装置で参照するホスト名ごとに IP アドレスを設定する必要がなくなります。

コンフィグレーションコマンド ip host／ipv6 host と DNS リゾルバ機能の両方が設定されている場合, ip host／ipv6 host で設定されているホスト名が優先されます。

本装置の DNS リゾルバ機能は RFC1034 および RFC1035 に準拠しています。

11.2　コマンドガイド

11.2.1　コマンド一覧

ホスト名・DNS 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 11-1　コンフィグレーションコマンド一覧

コマンド名	説明
ip domain lookup	DNS リゾルバ機能を無効化または有効化します。
ip domain name	DNS リゾルバで使用するドメイン名を設定します。
ip host	IPv4 アドレスに付与するホスト名情報を設定します。
ip name-server	DNS リゾルバが参照するネームサーバを設定します。
ipv6 host	IPv6 アドレスに付与するホスト名情報を設定します。

11.2.2　ホスト名の設定

(1)　IPv4 アドレスに付与するホスト名の設定

[設定のポイント]

IPv4 アドレスに付与するホスト名を設定します。

[コマンドによる設定]

1. **(config)# ip host WORKPC1 192.168.0.1**

   IPv4 アドレス 192.168.0.1 の装置にホスト名 WORKPC1 を設定します。

(2)　IPv6 アドレスに付与するホスト名の設定

[設定のポイント]

IPv6 アドレスに付与するホスト名を設定します。

[コマンドによる設定]

1. **(config)# ipv6 host WORKPC2 2001:db8:3::1234**

   IPv6 アドレス 2001:db8:3::1234 の装置にホスト名 WORKPC2 を設定します。

11.2.3　DNS の設定

(1)　DNS リゾルバの設定

[設定のポイント]

DNS リゾルバで使用するドメイン名および DNS リゾルバが参照するネームサーバを設定します。
DNS リゾルバ機能はデフォルトで有効なため，ネームサーバが設定された時点から機能します。

[コマンドによる設定]

1. **(config)# ip domain name router.example.com**

ドメイン名を router.example.com に設定します。

2.**(config)# ip name-server 192.168.0.1**

ネームサーバを 192.168.0.1 に設定します。

(2)　DNS リゾルバ機能の無効化

[設定のポイント]

DNS リゾルバ機能を無効にします。

[コマンドによる設定]

1.**(config)# no ip domain lookup**

DNS リゾルバ機能を無効にします。

12 装置の管理

この章では，本装置を導入した際，および本装置を管理する上で必要な作業について説明します。

12.1　コマンドガイド

12.1.1　コマンド一覧

装置を管理する上で必要なコンフィグレーションコマンド, および運用コマンド一覧の一覧を次の表に示します。

表 12-1　コンフィグレーションコマンド一覧

コマンド名	説明
system fan mode	ファンの運転モードを設定します。
system l2-table mode	レイヤ 2 ハードウェアテーブルの検索方式を設定します。
system recovery	no system recovery コマンドを設定すると，装置の障害が発生した際に，障害部位の復旧処理を行わないようにし，障害発生以降に障害部位を停止したままにします。
system temperature-warning-level	装置内温度が指定温度以上になった場合に運用メッセージを出力します。
switch provision	本装置のモデルを設定します。

表 12-2　運用コマンド一覧（ソフトウェアバージョンと装置状態の確認）

コマンド名	説明
show version	本装置に組み込まれているソフトウェアや実装されているボードの情報を表示します。
show system	本装置の運用状態を表示します。
clear control-counter	障害による装置再起動回数および部分再起動回数を 0 クリアします。
show environment	筐体のファン，電源，温度の状態と累積稼働時間を表示します。
reload	装置を再起動します。
show tech-support	テクニカルサポートで必要となるハードウェアおよびソフトウェアの状態に関する情報を表示します。

表 12-3　運用コマンド一覧（装置内メモリと MC の確認）

コマンド名	説明
show flash	装置内メモリの使用状態を表示します。
show mc	MC の形式と使用状態を表示します。
format mc	MC を本装置用のフォーマットで初期化します。

表 12-4　運用コマンド一覧（リソース情報とダンプ情報の確認）

コマンド名	説明
show cpu	CPU 使用率を表示します。
show processes	装置の現在実行中のプロセスの情報を表示します。

コマンド名	説明
show memory	装置の現在使用中のメモリの情報を表示します。
df	ディスクの空き領域を表示します。
du	ディレクトリ内のファイル容量を表示します。
erase dumpfile	ダンプファイルを消去します。
show dumpfile	ダンプファイル格納ディレクトリに格納されているダンプファイルの一覧を表示します。

12.1.2　モデルに応じたコンフィグレーション

本装置には，装置のモデルを設定するコンフィグレーションコマンド switch provision があります。

自装置のモデルは自動で設定されます。変更および削除できません。

なお，switch provision の設定情報は，運用コマンド show running-config で確認できます。

図 12–1　switch provision の設定情報の確認

```
# show running-config
#default configuration file for AX2340S-24T4X
!
switch 1 provision 2340-24t4x
!
   ⋮
   ⋮
#
```

12.2　運用情報のバックアップ・リストア

装置障害または交換時の運用情報の復旧手順を示します。

次に示す「12.2.2　backup/restore コマンドを用いる手順」を実施してください。すべてを手作業で復旧することもできますが，取り扱う情報が複数にわたるため管理が複雑になり，また，完全に復旧できないため，お勧めしません。

12.2.1　コマンド一覧

バックアップ・リストアに使用する運用コマンド一覧を次の表に示します。

表 12-5　運用コマンド一覧

コマンド名	説明
backup	稼働中のソフトウェアおよび装置の情報を内蔵フラッシュメモリ，MC，またはリモートの ftp サーバに保存します。
restore	内蔵フラッシュメモリ，MC，またはリモートの ftp サーバに保存している装置情報を本装置に復旧します。

12.2.2　backup/restore コマンドを用いる手順

(1)　情報のバックアップ

装置が正常に稼働しているときに，backup コマンドを用いてバックアップを作成しておきます。backup コマンドは，装置の稼働に必要な次の情報を一つのファイルにまとめて，内蔵フラッシュメモリ，MC，または外部の FTP サーバに保存します。

これらの情報に変更があった場合，backup コマンドによるバックアップの作成をお勧めします。

- 稼働中のソフトウェア
- オプションライセンス
- スタートアップコンフィグレーション
- ユーザアカウント／パスワード
- SSH サーバのホスト鍵ペア
- 内蔵 Web 認証 DB
- Web 認証画面
- Web 認証のサーバ証明書・秘密鍵・中間 CA 証明書
- 内蔵 MAC 認証 DB
- MC 運用モード
- インストール済みのスクリプトファイル

backup コマンドでは次に示す情報は保存されないので注意してください。

- show logging コマンドで表示される運用ログ情報など
- 装置内に保存されているダンプファイルなどの障害情報

- ユーザアカウントごとに設けられるホームディレクトリにユーザが作成および保存したファイル

(2)　情報のリストア

backup コマンドで作成されたバックアップファイルから情報を復旧する場合，restore コマンドを使用します。

restore コマンドを実行すると，バックアップファイル内に保存されているソフトウェアアップデート用ファイルを使用して装置のソフトウェアをアップデートします。このアップデート作業後, 装置は自動的に再起動します。再起動後，復旧された環境になります。

なお，restore コマンドを実行するときは，次の点に注意してください。

- restore コマンドで情報を復旧する場合は，リストア対象の装置と同じモデル名称の装置で作成したバックアップファイルを使用してください。

  装置のモデル名称は，show version コマンドで表示される Model で確認してください。
- バックアップファイル作成時のソフトウェアバージョンが，リストア対象の装置に適していることを確認してください。
- 装置に設定されたユーザアカウントと，バックアップファイルに含まれるユーザアカウントが同じ（ユーザ名およびユーザの追加／削除順序が同じ）になるようにしてください。ユーザアカウントが異なる場合，リストア後にファイルが操作できなくなります。

12.3　障害時の復旧

本装置では運用中に障害が発生した場合は自動的に復旧処理を行います。障害部位に応じて復旧処理を局所化して行い，復旧処理による影響範囲を狭めることによって，正常運用部分が中断しないようにします。

12.3.1　障害部位と復旧内容

障害発生時，障害の内容によって復旧内容が異なります。障害部位と復旧内容を次の表に示します。

表 12-6　障害部位と復旧内容

障害部位	装置の対応	復旧内容	影響範囲
ポートで検出した障害	該当するポートの自動復旧を 6 回／1 時間行います。自動復旧の回数が 6 回のときに障害が発生すると停止します。ただし，初回の障害発生から 1 時間以上運用すると，自動復旧の回数を初期化します。	該当するポートの再初期化を行います。	該当するポートを介する通信が中断されます。
メインボード障害（CPU および SW※1)	自動復旧を行います。復旧後 1 時間以上運用すると，自動復旧の回数を初期化します。※2	該当するメインボードの再初期化を行います。 6 回目以降の自動復旧の場合は，ランニングコンフィグレーションを初期化かつポートの状態を disable に設定して起動します。	装置内の全ポートを介する通信が中断されます。
メインボード障害（SW※1)	自動復旧を 6 回／1 時間行います。自動復旧の回数が 6 回のときに障害が発生すると停止します。※2 ただし，初回の障害発生から 1 時間以上運用すると，自動復旧の回数を初期化します。	該当するスイッチングプロセッサの再初期化を行います。	装置内の全ポートを介する通信が中断されます。
電源障害（PS）	装置の運用に必要な電力が供給されなくなると停止します。	装置を停止します。	装置内全ポートを介する通信が中断されます。
ファン障害	残りのファンを高速にします。	自動復旧はありません。	ファンが高速回転しますが通信に影響はありません。

注※1　SW は障害内容によって復旧内容が異なります。

注※2　コンフィグレーションコマンド no system recovery で復旧処理を行わない設定をしている場合には，自動復旧を行いません。

12.4　内蔵フラッシュメモリへ保存時の注意事項

本装置はソフトウェア，コンフィグレーション，ログ情報など，装置情報の保存先として，内蔵フラッシュメモリを使用しています。

内蔵フラッシュメモリはデバイスの一般的な特性上，書き換えられる回数に上限があります。その回数を超えて書き換えた場合，内蔵フラッシュメモリは故障するおそれがあります。

本装置の内蔵フラッシュメモリへの書き込み契機は，コンフィグレーションを保存したとき，および装置に対して一部の運用コマンドを実行したときです。これらの操作を 100 分周期で継続した場合，10 年程度で書き込み上限値に達することがあります。

(1)　コンフィグレーションコマンド

内蔵フラッシュメモリへの書き込み契機になる主なコンフィグレーションコマンドを，次に示します。

- save（write）
- ip ssh authkey
- ip dhcp snooping database url flash

(2)　運用コマンド

内蔵フラッシュメモリへの書き込み契機になる主な運用コマンドを，次の表に示します。なお，各プログラムのダンプコマンド実行時も該当します。

表 12–7　内蔵フラッシュメモリへの書き込み契機になる主な運用コマンド

分類	運用コマンド
コンフィグレーションとファイルの操作	copy，cp，rm，delete，undelete，squeeze，erase configuration，erase startup-config
ログインセキュリティと RADIUS/TACACS+	adduser，rmuser，password，clear password
SSH	set ssh hostkey，erase ssh hostkey
装置の管理	reload，backup，restore
ソフトウェアの管理	ppupdate，set license，erase license
ログ	clear logging
高機能スクリプト	install script，uninstall script
IPv4 通信，IPv6 通信	show tcpdump（writefile パラメータ指定時）
Web 認証	commit web-authentication, set web-authentication html-files，clear web-authentication html-files
MAC 認証	commit mac-authentication

13 MC 運用モード

この章では，MC 運用モードについて説明します。

13.1　解説

13.1.1　概要

本装置は通常，内蔵フラッシュメモリのソフトウェアと装置情報で起動しますが，MC 運用モードを使用すると次に示す動作ができます。

装置起動時

ソフトウェアと装置情報をあらかじめ格納した MC を挿入し，本装置を起動すると，MC 内のソフトウェアと装置情報で起動します。内蔵フラッシュメモリと MC 内の情報に差分がある場合は，内蔵フラッシュメモリが更新されます。

運用中の MC 挿入時

運用中に MC を挿入すると，自動でソフトウェアと装置情報が一括で MC に保存されます。

MC 出力コマンド実行時

運用コマンド update mc-configuration を実行すると，ソフトウェアと装置情報が一括で MC に保存されます。

MC 運用モードが有効な場合は，次に示すコマンドの実行時に，該当コマンドの動作に加えて運用コマンド update mc-configuration の処理も自動で実行されます。

- コンフィグレーションコマンド save でコンフィグレーションを保存時
- 運用コマンド copy でコピー先にスタートアップコンフィグレーションファイルを指定時
- 運用コマンド ppupdate の実行時

13.1.2　MC に保存されるファイル

MC 運用モード使用時に MC に保存されるファイルを次に示します。

表 13–1　MC に保存されるファイル

項目	内容	MC に保存される名称
ソフトウェア	稼働中のソフトウェア	axsroot/k.img
装置情報	運用コマンド backup 相当の装置情報※	/axsroot/mc-configuration.dat

注※

対象の装置情報については「12.2　運用情報のバックアップ・リストア」を参照してください。

13.1.3　MC 運用モードを使用した運用手順

MC 運用モードは，システム導入，構成変更，装置交換などの装置メンテナンス作業で利用できます。その際は，次に示す手順で実施してください。

(1)　システム導入時

1. MC をフォーマットします。

本装置に MC を挿入し，運用コマンド format mc を実行してください。

2. MC 運用モードを設定します。

運用コマンド set mc-configuration を実行してください。

3. システム構築後，各装置のソフトウェアと装置情報を MC に保存します。
   運用コマンド update mc-configuration を実行してください。
4. MC を挿入したまま運用します。

(2)　システム構成変更時

1. システム再構築後，各装置のソフトウェアと装置情報を MC に保存します。
   運用コマンド update mc-configuration を実行してください。

(3)　装置交換時

1. 新しい装置を用意します。
2. 新しい装置に MC 運用モードを設定します。
   運用コマンド set mc-configuration を実行してください。
3. 新しい装置の電源を OFF にします。
4. 新しい装置に，交換前の装置のソフトウェアと装置情報を保存した MC を挿入します。
5. 新しい装置の電源を ON にします。

(4)　予備の MC 作成時

1. 新しい MC を用意します。
2. MC がアクセス中でないことを確認して，運用中の MC を抜去します。
3. 該当装置に新しい MC を挿入します。
   装置のソフトウェアと装置情報が一括で MC に保存されます。

13.1.4　障害時の動作

MC 運用モード有効時に MC 障害を検出した場合の動作を次の表に示します。

表 13-2　MC 運用モードで MC 障害検出時の動作

イベント契機	障害要因	動作
装置起動時	MC 未搭載	内蔵フラッシュメモリのソフトウェアおよび装置情報で，装置が起動します。 また，MC 内の情報の読み込みに失敗したことを示す運用ログが採取されます。
	MC 読み込み失敗	
MC 挿入時	MC 書き込み失敗	MC 出力失敗を示す運用ログが採取されます。 また，ST2 LED が橙点灯※1 します。
	MC 空き容量不足	
MC 出力コマンド※2 実行時	MC 未搭載	コマンド実行エラーを示す応答メッセージが表示されます。
	MC 書き込み失敗	
	MC 空き容量不足	
上記以外のコマンド※3 実行時	MC 未搭載	MC 出力失敗を示す運用ログが採取されます。
	MC 書き込み失敗	
	MC 空き容量不足	

注※1

ST2 LED が橙点灯しているときは，MC を取り出して運用ログを確認してください。

注※2

運用コマンド update mc-configuration が対象です。

注※3

次に示すコマンドが対象です。

・コンフィグレーションコマンド save でコンフィグレーションを保存時

・運用コマンド copy でコピー先にスタートアップコンフィグレーションファイルを指定時

・運用コマンド ppupdate の実行時

13.1.5　MC 運用モード使用時の注意事項

(1)　他機能との共存

装置起動時に MC 運用モードとゼロタッチプロビジョニングの両方が有効な場合は，本機能が有効，ゼロタッチプロビジョニングが無効となります。

(2)　MC に保存されたディレクトリおよびファイルについて

運用コマンド update mc-configuration の実行，または MC の挿入によって，「表 13-1　MC に保存されるファイル」に示す名称で MC 内に保存されたソフトウェアや装置情報は，追加，変更，および削除をしないでください。また，名称も変更しないでください。

(3)　MC の抜き挿しについて

- 装置起動時は，MC 内のソフトウェアと装置情報で起動するため，MC にアクセスしています。装置の起動が完了するまで MC を抜かないでください。
- MC を挿入した場合は，内蔵フラッシュメモリのソフトウェアと装置情報を MC に書き込んでいます。ST2 LED が緑点灯している間は MC を抜かないでください。
- MC にアクセスする運用コマンドの実行中に，MC の抜き挿しをしないでください。MC の抜き挿しを正しく検出できないことがあります。

13.2　コマンドガイド

13.2.1　コマンド一覧

MC 運用モードのコンフィグレーションコマンド一覧を次の表に示します。

表 13-3　コンフィグレーションコマンド一覧

コマンド名	説明
save (write)※	編集したコンフィグレーションの内容を，スタートアップコンフィグレーションファイルへ保存します。MC 運用モードが有効な場合は，運用コマンド update mc-configuration の処理も自動で実行されます。

注※
「コンフィグレーションコマンドレファレンス」「3　コンフィグレーションの編集と操作」を参照してください。

MC 運用モードの運用コマンド一覧を次の表に示します。

表 13-4　運用コマンド一覧

コマンド名	説明
set mc-configuration	MC 運用モードを設定します。
update mc-configuration	稼働中のソフトウェアおよび装置の情報を，MC に出力します。
copy※1	指定したファイルまたはディレクトリをコピーします。MC 運用モードが有効な場合は，コピー先がスタートアップコンフィグレーションファイルのときに，運用コマンド update mc-configuration の処理も自動で実行されます。
show system※2	運用状態を表示します。 MC 運用モードの動作状態は，本コマンドの「MC Configuration mode」で確認できます。
ppupdate※3	指定したソフトウェアにアップデートします。MC 運用モードが有効な場合は，運用コマンド update mc-configuration の処理も自動で実行されます。

注※1
「運用コマンドレファレンス」「4　コンフィグレーションとファイルの操作」を参照してください。

注※2
「運用コマンドレファレンス」「9　装置の管理」を参照してください。

注※3
「運用コマンドレファレンス」「14　ソフトウェアの管理」を参照してください。

14 ゼロタッチプロビジョニング

この章では，ゼロタッチプロビジョニングについて説明します。

14.1　解説

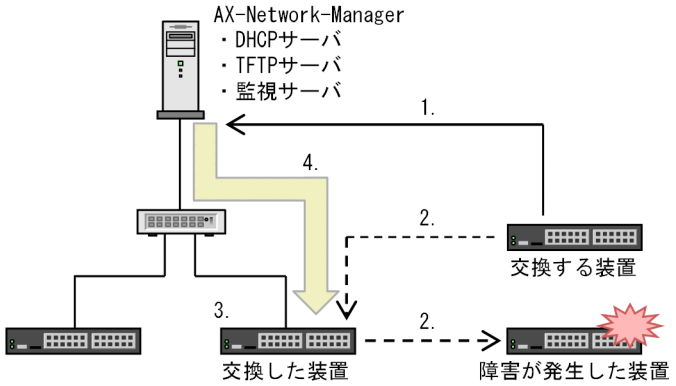
14.1.1　概要

ゼロタッチプロビジョニングは，DHCP サーバ，TFTP サーバ，監視サーバなどを含む AX-Network-Manager と連動し，ソフトウェアを含む装置情報を自動で該当装置に設定します。

障害などによって交換した装置の電源を ON にすると，自動で AX-Network-Manager から装置情報が取得されて装置に反映されます。これによって，コンソールや MC を使用しなくても，装置交換と装置情報のリストアができます。

ゼロタッチプロビジョニングの動作概要を次の図に示します。

図 14-1　ゼロタッチプロビジョニングの動作概要



1. 交換する装置の情報を登録する
2. 障害が発生した装置と交換する
3. 交換した装置の電源を ON にする
4. 交換した装置に装置情報をリストアする

なお，システム内の各装置の装置情報は，AX-Network-Manager でバックアップを実行しファイルとして管理されています。

ゼロタッチプロビジョニングは，コンフィグレーションコマンド system zero-touch-provisioning を設定および保存した状態で，装置を起動したときに動作します。system zero-touch-provisioning コマンドは，初期状態で有効です。本機能を使用しない場合は，コンフィグレーションコマンド no system zero-touch-provisioning で削除してください。

14.1.2　本装置と AX-Network-Manager との通信方法

ゼロタッチプロビジョニングで AX-Network-Manager と通信するには，装置 IP アドレスやサーバからのファイル取得処理が必要です。これらの処理は，本機能によって自動で実行されます。

(1)　装置 IP アドレスの取得

1. 装置起動時に，ゼロタッチプロビジョニング専用の VLAN だけが通信できます。それ以外の VLAN ではすべての通信を廃棄します。なお，初期状態では VLAN 1（デフォルト VLAN）が本機能専用です。

2. 本装置のゼロタッチプロビジョニングによって，AX-Network-Manager（DHCP サーバ）から本機能専用で使用する装置 IP アドレスを取得します。
3. バックアップファイルを取得する TFTP サーバの IP アドレス，およびファイル名を取得します。

(2)　バックアップファイルの取得とリストア

1. 本装置の TFTP クライアント機能によって，取得した TFTP サーバの IP アドレスで AX-Network-Manager（TFTP サーバ）へ接続し，バックアップファイルを取得します。
2. バックアップファイルを保存し，取得した装置情報と本装置の装置情報に差分があった場合に，装置を再起動して反映します。

14.1.3　ゼロタッチプロビジョニングの対象ファイル

ゼロタッチプロビジョニングの使用時に AX-Network-Manager からリストアされる装置情報を次の表に示します。

表 14–1　AX-Network-Manager からリストアされる装置情報

バックアップファイル種別	内容
一括情報	本装置のソフトウェア，コンフィグレーション，各認証データベース，ライセンス情報などを一つにまとめた装置情報。 AX-Network-Manager が運用コマンド backup で採取したもの※。

注※
　対象の装置情報については「12.2　運用情報のバックアップ・リストア」を参照してください。

ゼロタッチプロビジョニングは，AX-Network-Manager に一括情報のバックアップファイルが存在することが必須です。

14.1.4　ゼロタッチプロビジョニングを使用した運用手順

ゼロタッチプロビジョニングは装置の交換作業で利用できます。その際は，次に示す手順で実施してください。

(1)　交換手順

1. **交換する新しい装置を用意します。**
   AX-Network-Manager との通信に使用する VLAN を設定し，ゼロタッチプロビジョニングを有効にした装置を用意してください。
2. **新しい装置の MAC アドレスを AX-Network-Manager 側へ登録します。**
   AX-Network-Manager 側で管理しているバックアップファイルの MAC アドレス情報が，新しい装置の MAC アドレスに変更されます。
3. **障害が発生した装置と新しい装置を交換し，LAN ケーブルなどを交換前と同様に配線します。**
4. **新しい装置の電源を ON にします。**
5. **自動で装置情報のリストアを開始します。**
   このとき，AX-Network-Manager との通信に使用する VLAN だけが通信でき，それ以外の VLAN ではすべての通信を廃棄します。
   リストアが完了して装置の再起動が完了すると，すべての VLAN が通信できるようになります。

(2)　起動後の確認方法

装置起動後の結果は，運用コマンド show system および運用ログで確認できます。

- ゼロタッチプロビジョニング動作モード起動
  自動リストアが実行されて，装置が起動したことを示します。
- 通常モード起動
  自動リストアが実行されないで，該当装置の装置情報で起動したことを示します。
  通常モードで起動した要因には，AX-Network-Manager との接続失敗や，リストア用ファイルの読み込み失敗などがあります。

14.1.5　ゼロタッチプロビジョニング使用時の注意事項

(1)　他機能との共存

ゼロタッチプロビジョニングは，次に示す機能と同時に使用できません。

- MC 運用モード
  装置起動時にゼロタッチプロビジョニングと MC 運用モードの両方が有効な場合は，MC 運用モードが有効，本機能が無効となります。
- IP インタフェース
  ゼロタッチプロビジョニングが有効な場合は，VLAN インタフェースに IP 情報を設定できません。また，IP 情報の設定された VLAN インタフェースが存在する場合は，本機能を有効にできません。

(2)　ゼロタッチプロビジョニングで使用する VLAN について

ゼロタッチプロビジョニング用の VLAN は，本機能専用の VLAN として設定してください。本機能で使用する VLAN は，初期状態では VLAN 1（デフォルト VLAN）が設定されています。他機能と重複しないように，本機能専用の VLAN を割り当ててください。

ゼロタッチプロビジョニングを使用しない場合は，コンフィグレーションコマンド no system zero-touch-provisioning で削除してください。

14.2　コマンドガイド

14.2.1　コマンド一覧

ゼロタッチプロビジョニ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 14-2　コンフィグレーションコマンド一覧

コマンド名	説明
system zero-touch-provisioning	ゼロタッチプロビジョニングを有効にします。
system zero-touch-provisioning vlan	ゼロタッチプロビジョニングで使用する VLAN を設定します。

ゼロタッチプロビジョニングの運用コマンド一覧を次の表に示します。

表 14-3　運用コマンド一覧

コマンド名	説明
show system※	運用状態を表示します。 ゼロタッチプロビジョニング動作モードの起動状態は，本コマンドの「Zero-touch-provisioning status」で確認できます。

注※
「運用コマンドレファレンス」「9　装置の管理」を参照してください。

14.2.2　ゼロタッチプロビジョニングの設定

ゼロタッチプロビジョニングは初期状態で有効です。この場合，使用する VLAN は 1 となります。

(1)　使用する VLAN を変更する場合

ゼロタッチプロビジョニングで使用する VLAN を設定し，ゼロタッチプロビジョニングを有効にします。

[設定のポイント]
ゼロタッチプロビジョニングで使用する VLAN に 4094 を設定します。

[コマンドによる設定]

1. **(config)# vlan 4094**
   (config-vlan)# exit
   VLAN 4094 を設定します。
2. **(config)# interface gigabitethernet 1/0/1**
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 4094
   (config-if)# exit
   ポート 1/0/1 に VLAN 4094 を設定します。
3. **(config)# system zero-touch-provisioning vlan 4094**
   ゼロタッチプロビジョニングで使用する VLAN に 4094 を設定します。
4. **(config)# system zero-touch-provisioning**

ゼロタッチプロビジョニングを有効にします。

5. (config)# save
   設定内容を保存します。

[注意事項]

- 設定内容は次の装置起動時から適用されます。
- 本装置の VLAN インタフェースに IP 情報を設定している場合，ゼロタッチプロビジョニングを有効にできません。本機能を有効にする場合は，VLAN インタフェースから IP 情報を削除してください。

(2)　ゼロタッチプロビジョニングを無効にする場合

ゼロタッチプロビジョニングを使用しない場合は，コンフィグレーションを削除して無効にします。

[設定のポイント]

ゼロタッチプロビジョニングを削除します。本機能は初期状態で有効なため，使用しない場合は削除してください。

[コマンドによる設定]

1. (config)# no system zero-touch-provisioning
   ゼロタッチプロビジョニングを無効にします。
2. (config)# save
   設定内容を保存します。

15 ソフトウェアの管理

この章では，ソフトウェアの管理について説明します。

15.1　ソフトウェアアップデートの解説

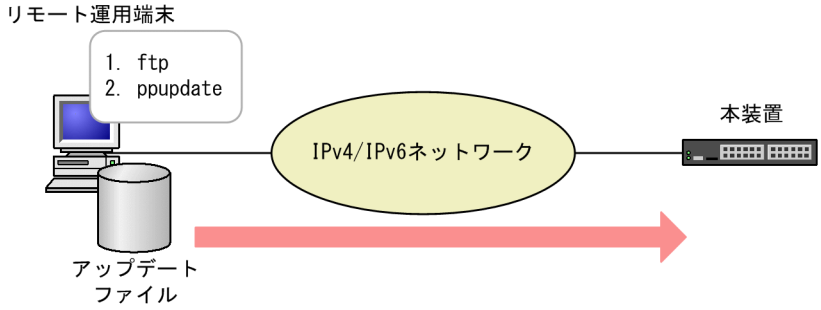
15.1.1　概要

ソフトウェアのアップデートとは，旧バージョンのソフトウェアから新バージョンのソフトウェアにバージョンアップすることを指します。ソフトウェアをアップデートするには，リモート運用端末や MC からアップデートファイルを本装置に転送し，運用コマンド ppupdate を実行します。アップデート時，装置管理のコンフィグレーションおよびユーザ情報（ユーザアカウント，パスワードなど）はそのまま引き継がれます。

(1)　リモート運用端末からのアップデート

PC などのリモート運用端末からアップデートする流れを次の図に示します。

図 15-1　リモート運用端末からアップデートする流れ

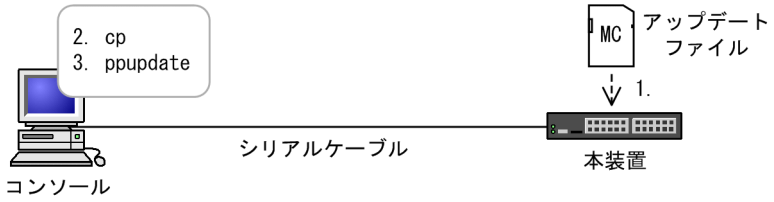


1. アップデートファイルを ftp でリモート運用端末から本装置に転送します。
2. 本装置にログイン後，アップデートコマンド（ppupdate）を実行します。

(2)　MC によるアップデート

MC を使用してアップデートする流れを次の図に示します。

図 15-2　MC を使用してアップデートする流れ



1. アップデートファイルが格納されている MC を本装置に挿入します。
2. アップデートファイルを MC から本装置にコピー（cp）します。
3. 本装置にログイン後，アップデートコマンド（ppupdate）を実行します。

15.1.2　アップデートの準備

アップデート作業をする前に次の内容を確認してください。

(1)　アップデートに必要な条件

本装置へアップデートファイルを転送し，アップデートコマンドを実行するためには，いくつかの条件を満たす必要があります。アップデートに必要な条件を次の表に示します。

表 15-1　アップデートに必要な条件

操作	条件	対処方法
共通	内蔵フラッシュメモリに，アップデートファイルを転送できる未使用容量が確保されていること。※	容量不足のためアップデートファイルが転送できない場合は，「(2)　内蔵フラッシュメモリ容量を確保する方法」を参照して，必要な未使用容量を確保してください。
	運用コマンド enable で装置管理者モードへ変更するための権限があること。	アップデートコマンドを実行するには enable コマンドで装置管理者モードへ変更する必要があるため，装置管理者モードの権限を設定してください。
リモート運用端末からのアップデート	リモート運用端末から本装置に対してネットワーク経由で到達できる状態であること。	リモート運用端末を用意して，本装置と IP 通信ができるようネットワークに接続してください。
	リモート運用端末で ftp クライアントソフトウェアが動作し，本装置に対してファイルの書き込み（put）ができること。	ftp クライアントソフトウェアを用意して，リモート運用端末にインストールしてください。なお，Windows では，OS に付属している ftp を使用できます。
	リモート運用端末からの ftp プロトコルによるリモートアクセスを本装置で許可していること。	コンフィグレーションコマンド ftp-server を設定してください。また，config-line モード（line vty）でアクセスリストを指定している場合には，リモート運用端末からのアクセスを許可する設定としてください。
	リモート運用端末から本装置へログインできること。	リモート運用端末から telnet でログインする場合には，コンフィグレーションコマンド line vty で telnet プロトコルによるリモートアクセスを許可する設定をしてください。
MC によるアップデート	コンソールから本装置へログインできること。	コンソールと本装置を接続してください。
		コンソールで通信ソフトウェアが使用できるようにしてください。

注※

運用コマンド show system で，内蔵フラッシュメモリのユーザ領域（user area）に，次に示す値以上の未使用容量（free）があることを確認してください。

アップデートファイルのサイズ＋ 10MB

(2)　内蔵フラッシュメモリ容量を確保する方法

内蔵フラッシュメモリ容量が不足している場合は，次に示す方法で未使用容量を確保してください。

- /usr/var/core/配下のファイルを運用コマンド rm で削除する。
- 運用コマンド erase protocol-dump を実行する。
- 運用コマンド squeeze を実行する。
- ユーザ領域に保存しているユーザファイルを削減する。

15.1.3　アップデートの注意事項

(1)　ファイル転送時の注意事項

アップデートファイルは，本装置上の/usr/var/update ディレクトリ配下に k.img というファイル名で転送してください。すでにファイルが存在している場合は，既存のファイルに上書きします。なお，ファイルのアクセス権によっては，ほかのユーザ※が作成した k.img ファイルに上書きできない場合があります。その場合は，いったん k.img ファイルを運用コマンド rm で削除してから転送してください。また，転送先およびファイル名を誤った場合は，誤ったファイルを削除してから再度転送してください。

注※　運用コマンド rmuser で削除済みのユーザが作成したファイルの場合，運用コマンド ls で詳細情報を表示したときに，ファイル所有者を数字で表示します。

(2)　MC からファイルをコピーするときの注意事項

- MC は，弊社製品を使用してください。
- 事前に PC などを使用して，アップデートファイルを MC に格納しておいてください。

(3)　アップデートコマンド実行時の注意事項

- アップデートコマンドが異常終了した場合は，次のコマンドを実行して，ppupdate.exec ファイルの有無を確認してください。

  ```
  ls /tmp/ppupdate.exec
  ```

  該当するファイルが存在するときは，運用コマンド rm で対象ファイルを削除してください。
- アップデートコマンドは，複数のユーザで同時に実行できません。実行した場合，メッセージ「another user is executing now」を表示し，異常終了します。
- コンフィグレーションコマンドモードでは，アップデートコマンドを実行できません。
- k.img ファイルは削除しないでください。異常終了時にファイルを復旧できなくなります。
- アップデート実行中は，電源を OFF にしないでください。電源が OFF になった場合は，再起動後，最初からアップデートを再実行してください。
- 内蔵フラッシュメモリに保存されているコンフィグレーションは，アップデート後のバージョンにも内容が引き継がれます。保存されているコンフィグレーションの設定数が多い状態でアップデートすると，コンフィグレーションの引き継ぎに時間が掛かることがあります。

  なお，バージョンダウンする場合，未サポートになるコンフィグレーションはあらかじめ削除してください。本装置では，未サポートになるコンフィグレーションは削除して運用するため，意図しないネットワークを構築するおそれがあります。

15.2　アップデートのコマンドガイド

15.2.1　コマンド一覧

アップデートに関する運用コマンド一覧を次の表に示します。

表 15-2　運用コマンド一覧

コマンド名	説明
ppupdate	指定したソフトウェアにアップデートします。

15.2.2　アップデートファイルの準備

アップデートに使用するアップデートファイルを準備します。

1. コンフィグレーションをオンラインで編集したあと保存していない場合は，アップデートの前にコンフィグレーションコマンド save を実行して，コンフィグレーションを保存します。

   コンフィグレーションを保存しないと，アップデート終了後の再起動によって編集前のコンフィグレーションに戻ります。

2. show flash コマンドを実行します。

   内蔵フラッシュメモリのユーザ領域（user area）に，次に示す値以上の未使用容量（free）があることを確認してください。

   アップデートファイルのサイズ－「/usr/var/update/k.img」のサイズ＋ 10MB

3. アップデートファイルを本装置に転送して，k.img という名前でディレクトリ（/usr/var/update）に置きます。

   ファイルの転送には，FTP を使用する方法と MC を使用する方法があります。FTP を使用する場合は，バイナリモードで転送してください。MC を使用してアップデートファイルを転送する例を次の図に示します。

   図 15-3　MC を使用したアップデートファイルの転送例

```
>ls mc-dir
 Volume in drive C has no label
 Volume Serial Number is 0000-000D
Directory for C:/

k         img  87436856 YYYY-MM-DD  HH:MM
       XX files          XXX XXX XXX bytes
                     XX XXX XXX XXX bytes free
>cp mc-file k.img /usr/var/update/k.img
>
>ls -l /usr/var/update
total 28952
-rw-r--r--    1 operator users     87436856 Jun 18 17:57 k.img
>
```

   下線の部分でファイルサイズを確認できます。

4. ls -l /usr/var/update コマンドを実行します。

   k.img のファイルサイズが，取得元のファイルサイズと等しいことを確認してください。確認が終了したら，「15.2.3　アップデートコマンドの実行」に進んでください。

15.2.3　アップデートコマンドの実行

ソフトウェアのバージョンを次の手順で旧バージョンから新バージョンにアップデートします。アップデートが完了すると，装置が自動で再起動します。再起動時には通信が一時的に中断されるため，注意してください。また，事前にアップデートファイルを本装置へ転送しておいてください。

1. enable コマンドを実行します。
   コマンドプロンプトが“#”に変更されます。
2. cd /usr/var/update コマンドを実行します。
3. ppupdate k.img コマンドを実行します。
   インストールされるソフトウェアのバージョンと，アップデート対象が表示されます。アップデートが完了すると，自動で装置が再起動します。
4. 再起動後，再度装置にログインします。
5. show version コマンドを実行して，アップデート後のバージョンで動作していることを確認します。

アップデートの実行例を次の図に示します。

図 15-4　アップデートの実行例

```
> enable
#
# cd /usr/var/update/
#
# ls -l
total 28952
-rw-r--r--  1 operator  users  29603328 Nov  3 00:42 k.img
#
# ppupdate k.img

Software update start

Broadcast message from operator@ (somewhere) (Wed Jul 14 15:32:20 20XX):

**********************************************
** UPDATE IS STARTED.                        **
**********************************************

Current version is 1.0
New version is 1.1
Automatic reboot process will be run after installation process.
Do you wish to continue? (y/n) y

100% |************************| 28909 KiB    1.72 MiB/s    00:00 ETA

Update done.

Broadcast Message from operator@
        (??) at 10:25 JST...

**********************************************
** UPDATE IS FINISHED SUCCESSFULLY.          **
**********************************************

#

         :

login: operator
Password:

Copyright (c) 20XX ALAXALA Networks Corporation. All rights reserved.


> show version software
Date 20XX/11/03 18:07:46 UTC
```

```
S/W: OS-L2N Ver. 1.0
>
```

15.3　オプションライセンスの解説

15.3.1　概要

本装置には，オプションライセンスを設定できます。オプションライセンスとは，装置に含まれる付加機能を使用するために必要となるライセンスで，付加機能ごとに提供します。

15.3.2　オプションライセンスに関する注意事項

- オプションライセンスは，装置に対応したものを設定してください。
- オプションライセンスの設定情報は，装置に保存されます。
  装置の交換やソフトウェアの新規インストール時には，オプションライセンスの再設定が必要です。ソフトウェアのバージョンアップ時には，オプションライセンスの再設定は不要です。
- オプションライセンスを設定した場合，設定を反映するには装置を再起動する必要があります。
- ある機能のオプションライセンスが設定された状態で，別機能のオプションライセンスを追加で設定できます。

15.4　オプションライセンスのコマンドガイド

15.4.1　コマンド一覧

オプションライセンスに関する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
set license	オプションライセンスを設定します。
show license	設定されているオプションライセンスを表示します。
erase license	指定したオプションライセンスを削除します。

15.4.2　オプションライセンスの設定方法

オプションライセンスは，ライセンスキーを使用して次の手順で設定します。なお，ライセンスキーは「オプションライセンス使用許諾契約書兼ライセンスシート」に記述されています。

1. enable コマンドを実行します。
2. show license コマンドを実行して，現在のオプションライセンスの設定状況を確認します。
3. set license key-code <license key>コマンドを実行して，オプションライセンスを設定します。
   <license key>には，設定するライセンスキーを指定してください。
4. show license コマンドを実行して，設定したオプションライセンスが表示されることを確認します。
   設定したライセンスキーの先頭 16 桁が表示されます。
5. reload -f no-dump-image コマンドを実行して，装置を再起動します。
   設定したライセンスキーは，装置が再起動したあとで有効になります。
6. 再起動後，再度装置にログインします。
7. show license コマンドを実行して，設定したオプションライセンスが有効になっていることを確認します。

オプションライセンス設定の実行例を次の図に示します。

図 15-5　オプションライセンス設定の実行例

```
> enable
#
# show license
Date 20XX/11/03 10:35:39 UTC
  Available:
    ----------------
#
# set license key-code 1f00-1234-8000-0000-1234-5678-abcd-ef00
#
# show license
Date 20XX/11/03 10:36:07 UTC
  Available:
    Serial Number        Licensed software
    1f00-1234-8000-0000  OP-ULTG(AX-P2340-F21)
#
# reload -f no-dump-image
#

         :
```

```
login: operator
Password:

Copyright (c) 20XX ALAXALA Networks Corporation. All rights reserved.


>
> show license
Date 20XX/11/03 00:27:05 UTC
  Available: OP-ULTG
    Serial Number        Licensed software
    1f00-1234-8000-0000  OP-ULTG(AX-P2340-F21)
>
```

15.4.3　オプションライセンスの削除方法

オプションライセンスは次の手順で削除します。

1. enable コマンドを実行します。
2. show license コマンドを実行して，現在のオプションライセンスの設定状況を確認します。
   削除するオプションライセンスのシリアル番号を確認してください。シリアル番号は 16 桁の英数字です。
3. erase license <serial no.>コマンドを実行して，オプションライセンスを削除します。
   <serial no.>には，削除するオプションライセンスのシリアル番号を指定してください。
4. 確認メッセージが表示されたら，“y”を入力します。
5. show license コマンドを実行して，指定したオプションライセンスが削除されていることを確認します。
6. reload -f no-dump-image コマンドを実行して，装置を再起動します。
   削除したライセンスキーは，装置が再起動したあとで無効になります。
7. 再起動後，再度装置にログインします。
8. show license コマンドを実行して，オプションライセンスが無効になっていることを確認します。

オプションライセンス削除の実行例を次の図に示します。

図 15-6　オプションライセンス削除の実行例

```
> enable
#
# show license
Date 20XX/11/03 00:27:53 UTC
  Available: OP-ULTG
    Serial Number        Licensed software
    1f00-1234-8000-0000  OP-ULTG(AX-P2340-F21)
#
# erase license 1f00-1234-8000-0000
This serial number enable OP-ULTG
Erase OK? (y/n): y
#
# show license
Date 20XX/11/03 00:28:12 UTC
  Available: OP-ULTG
    ----------------
#
# reload -f no-dump-image
#

         :

login: operator
Password:
```

```
Copyright (c) 20XX ALAXALA Networks Corporation. All rights reserved.

>
> show license
Date 20XX/11/03 00:30:06 UTC
  Available:
    ----------------
>
```

16 省電力機能

この章では，本装置の省電力機能について説明します。

16.1　省電力機能の解説

16.1.1　省電力機能の概要

ネットワークの使用量の増加に備え，収容ポートの帯域を増やしているケースでは，増やしたポート帯域分の電力も消費しています。本装置では，省電力機能によって，不要に消費される電力を抑えられます。

(1)　サポートする省電力機能

本装置では，省電力機能として次に示す機能をサポートします。

- EEE 機能
- ポートの電力供給 OFF

16.1.2　省電力機能

(1)　EEE 機能

EEE（Energy Efficient Ethernet）とは，IEEE802.3az で標準化されている省電力機能です。データ送受信がないときに LPI（Low Power Idle）モードになり，イーサネットの消費電力を低減させます。

本装置と相手装置の双方が EEE 機能に対応している必要があり，オートネゴシエーションのリンク確立プロセスで，双方が EEE 機能のサポート状態を広告することで有効になります。

本装置は，次の接続インタフェースで EEE 機能をサポートします。

- オートネゴシエーションによる 100BASE-TX 全二重
- オートネゴシエーションによる 1000BASE-T 全二重

ただし，SFP ポートおよび SFP+/SFP 共用ポートを 1000BASE-T で使用する場合は含みません。

(2)　ポートの電力供給 OFF

使用していないポートの電力供給を OFF にすると，消費電力を削減できます。次の方法でポートの電力供給を OFF にできます。

- コンフィグレーションコマンドでポートをシャットダウン状態にする

16.2　省電力機能のコマンドガイド

16.2.1　コマンド一覧

省電力機能のコンフィグレーションコマンド一覧を次の表に示します。

表 16-1　コンフィグレーションコマンド一覧

コマンド名	説明
eee enable	ポートの EEE 機能を有効に設定します。
shutdown※	ポートへの電力供給を OFF に設定します。

注※
「コンフィグレーションコマンドレファレンス」「14　イーサネット」を参照してください。

省電力機能の運用コマンド一覧を次の表に示します。

表 16-2　運用コマンド一覧

コマンド名	説明
show power	装置の最大消費電力情報を表示します。
show port eee※	ポートの EEE 情報を表示します。

注※
「運用コマンドレファレンス」「20　イーサネット」を参照してください。

17 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。

17.1　解説

本装置では動作情報や障害情報などを運用メッセージとして通知します。同メッセージは運用端末に出力するほか，運用ログとして装置内に保存します。この情報で装置の運用状態や障害の発生を管理できます。

運用ログは装置運用中に発生した事象（イベント）を発生順に記録したログ情報で，運用メッセージと同様の内容が格納されます。運用ログとして格納する情報には次に示すものがあります。

- オペレータの操作および応答メッセージ
- 運用メッセージ

種別ログは装置内で発生した障害や警告についての運用ログ情報をメッセージ ID ごとに分類した上で，同事象が最初に発生した日時および最後に発生した日時と累積回数をまとめた情報です。

これらのログは装置内にテキスト形式で格納されています。装置管理者は，表示コマンドでこれらの情報を参照できます。

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管理装置に送ることができます※1，※2。また，同様に，ログ情報を E-Mail を使用してネットワーク上の管理装置に送ることもできます。これらのログ出力機能を使用することで，多数の装置を管理する場合にログの一元管理ができるようになります。また，ログ情報を E-Mail で送信することもできます。

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，RFC5424 で定義されている HEADER 部の HOSTNAME 欄は未設定です。

17.2　コマンドガイド

17.2.1　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 17-1　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メッセージ種別を設定します。
logging facility	ログ情報を syslog インタフェースで出力するためのファシリティを設定します。
logging host	ログ情報の出力先を設定します。
logging syslog-dump	本装置で発生したログを内蔵フラッシュメモリに格納しません。
logging syslog-version	syslog サーバに送信する syslog メッセージのフォーマットバージョンを指定します。
logging trap	syslog サーバに送信対象とするログ情報の重要度を設定します。

表 17-2　コンフィグレーションコマンド一覧（E-Mail 出力に関する設定）

コマンド名	説明
logging email	ログ情報を E-Mail で出力するための E-Mail アドレスを設定します。
logging email-event-kind	E-Mail で出力対象とするログ情報のメッセージ種別を設定します。
logging email-from	ログ情報を E-Mail で出力する E-Mail の送信元を設定します。
logging email-interval	ログ情報を E-Mail で出力するための送信間隔を設定します。
logging email-server	ログ情報を E-Mail で出力するため SMTP サーバの情報を設定します。

ログ出力機能に関する運用コマンド一覧を次の表に示します。

表 17-3　運用コマンド一覧

コマンド名	説明
show logging	本装置で収集しているログを表示します。
clear logging	本装置で収集しているログを消去します。
show logging console	set logging console コマンドで設定された内容を表示します。
set logging console	運用メッセージの画面表示をイベントレベル単位で制御します。

17.2.2　ログの syslog 出力の設定

本装置では，syslog 送信データのヘッダ部に付ける facility や severity を送信先単位で設定したり，装置単位で設定したりできます。送信先単位の設定と装置単位の設定を同時に設定した場合は，送信先単位の設定が使用されます。

[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 LOG_HOST facility local3 severity 4**

   ログをホスト名 LOG_HOST 宛て，facility を local3，severity を 4 で出力するように設定します。

17.2.3　運用メッセージの出力抑止

装置の状態が変化した場合，本装置は動作情報や障害情報などを運用メッセージとしてコンソールやリモート運用端末に表示します。例えば，回線が障害状態から回復した場合は回線が回復したメッセージを，回線が障害になって運用を停止した場合は回線が障害になったメッセージを表示します。運用メッセージの詳細は，「メッセージ・ログレファレンス」「1　運用メッセージ」を参照してください。

運用端末に出力される運用メッセージは，運用コマンド set logging console を使用することでイベントレベル単位で出力を抑止できます。また，その抑止内容については，運用コマンド show logging console で確認できます。イベントレベルが E5 以下の運用メッセージの運用端末への出力抑止の設定例を次に示します。

図 17-1　運用メッセージの出力抑止の設定例

```
> set logging console disable E5
> show logging console
  System message mode : E5
>
```

注意

多数の運用メッセージが連続して発生した際は，コンソールやリモート運用端末上には一部しか表示しませんので，運用コマンド show logging で確認してください。

17.2.4　ログの E-Mail 出力の設定

[設定のポイント]

E-Mail 送信機能を使用して，採取したログ情報をリモートホスト，PC など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 email system@loghost**

   送信先のメールアドレスとして system@loghost を設定します。

18 SNMP

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。

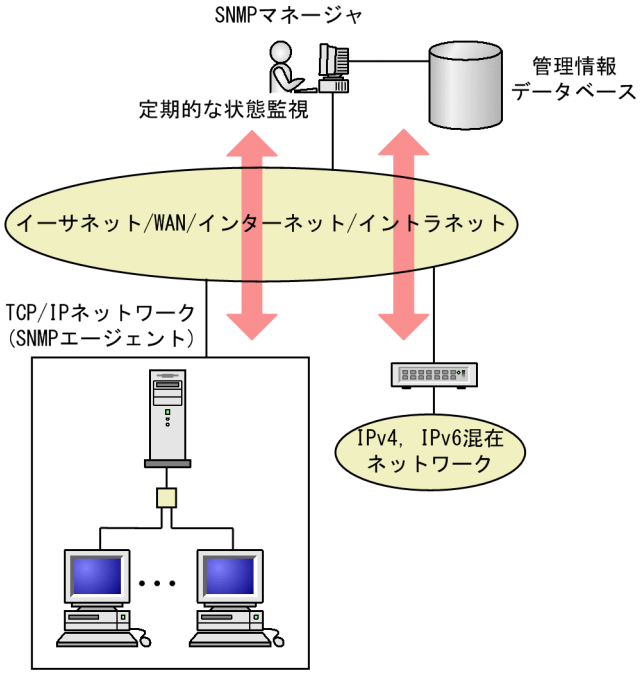
18.1　解説

18.1.1　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。

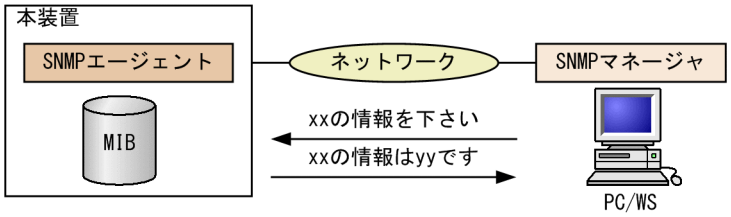
図 18-1　ネットワーク管理の概要



(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 18-2　MIB 取得の例

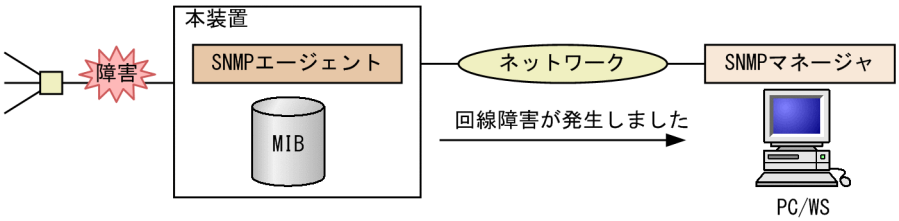


本装置の運用コマンドには MIB 情報を表示するための SNMP コマンドがあります。このコマンドは，自装置およびリモート装置の SNMP エージェントの MIB を表示します。

本装置では，SNMPv1（RFC1157），SNMPv2C（RFC1901），および SNMPv3（RFC3410）をサポートしています。SNMP マネージャを使用してネットワーク管理を行う場合は，SNMPv1，SNMPv2C，または SNMPv3 プロトコルで使用してください。なお，SNMPv1，SNMPv2C，SNMPv3 をそれぞれ同時に使用することもできます。

また，SNMP エージェントは**トラップ**（Trap）や**インフォーム**（Inform）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。以降，トラップおよびインフォームを SNMP 通知と呼びます。SNMP マネージャは，SNMP 通知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 18-3　トラップの例



インフォームもトラップと同じ UDP によるイベント通知ですが，トラップとは異なって SNMP マネージャからの応答を要求します。そのため，応答の有無でインフォームの到達を確認できます。これによって，ネットワークの輻輳などに対してもインフォームの再送で対応できます。

なお，本装置の SNMP プロトコルは IPv4 および IPv6 に対応しています。

(3)　SNMPv3

SNMPv3 は SNMPv2C までの全機能に加えて，管理セキュリティ機能が大幅に強化されています。ネットワーク上を流れる SNMP パケットを認証・暗号化することによって，SNMPv2C でのコミュニティ名と SNMP マネージャの IP アドレスの組み合わせによるセキュリティ機能では実現できなかった，盗聴，なりすまし，改ざん，再送などのネットワーク上の危険から SNMP パケットを守ることができます。

(a)　SNMP エンティティ

SNMPv3 では，SNMP マネージャおよび SNMP エージェントを「SNMP エンティティ」と総称します。本装置の SNMPv3 は，SNMP エージェントに相当する SNMP エンティティをサポートしています。

(b)　SNMP エンジン

SNMP エンジンは認証，および暗号化したメッセージ送受信と管理オブジェクトへのアクセス制御のためのサービスを提供します。SNMP エンティティとは 1 対 1 の関係です。SNMP エンジンは，同一管理ドメイン内でユニークな SNMP エンジン ID により識別されます。

(c)　ユーザ認証と暗号化機能

SNMPv1，SNMPv2C でのコミュニティ名による認証に対して，SNMPv3 ではユーザ認証を行います。また，SNMPv1，SNMPv2C にはなかった暗号化機能も SNMPv3 でサポートされています。ユーザ認証と暗号化機能は，ユーザ単位に設定できます。

本装置では，ユーザ認証に使用する認証プロトコルとして次のプロトコルをサポートしています。

HMAC-MD5-96

MD5 アルゴリズムを使用した認証プロトコルです。128 ビットのダイジェストのうち，先頭の 96 ビットを使用します。

HMAC-SHA-96

SHA-1 アルゴリズムを使用した認証プロトコルです。160 ビットのダイジェストのうち，先頭の 96 ビットを使用します。

HMAC-SHA-256

SHA-256 アルゴリズムを使用した認証プロトコルです。256 ビットのダイジェストのうち，先頭の 192 ビットを使用します。

HMAC-SHA-512

SHA-512 アルゴリズムを使用した認証プロトコルです。512 ビットのダイジェストのうち，先頭の 384 ビットを使用します。

暗号化機能に使用するプライバシープロトコルとして次のプロトコルをサポートしています。

CBC-DES

DES アルゴリズムと，暗号利用モード CBC を組み合わせて暗号化するプライバシープロトコルです。

CFB128-AES-128

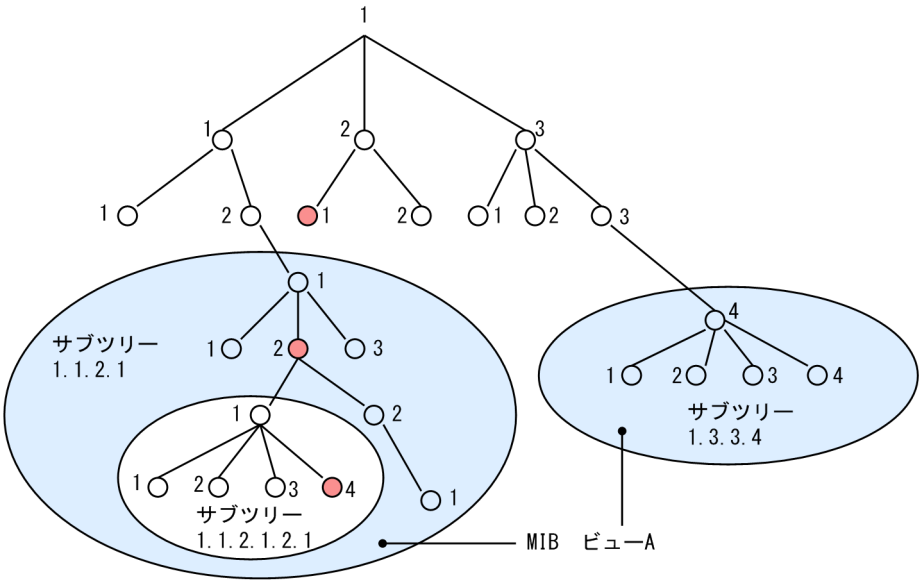
AES アルゴリズムと，暗号利用モード CFB を組み合わせて暗号化するプライバシープロトコルです。

(d) MIB ビューによるアクセス制御

SNMPv3 では，ユーザ単位に，アクセスできる MIB オブジェクトの集合を設定できます。この MIB オブジェクトの集合を MIB ビューと呼びます。MIB ビューは，MIB のオブジェクト ID のツリーを表すビューサブツリーを集約することによって表現されます。集約する際には，ビューサブツリーごとに included（MIB ビューに含む），または excluded（MIB ビューから除外する）を選択できます。MIB ビューは，ユーザ単位に，Read ビュー，Write ビュー，Notify ビューとして設定できます。

次に，MIB ビューの例を示します。MIB ビューは，「図 18–4　MIB ビューの例」に示すような MIB ツリーの一部である MIB サブツリーをまとめて設定します。オブジェクト ID 1.1.2.1.2 は，サブツリー 1.1.2.1 に含まれるので，MIB ビュー A でアクセスできます。しかし，オブジェクト ID 1.2.1 は，どちらのサブツリーにも含まれないので，アクセスできません。また，オブジェクト ID 1.1.2.1.2.1.4 は，サブツリー 1.1.2.1.2.1 がビュー A から除外されているためアクセスできません。

図 18-4 MIB ビューの例



コンフィグレーションの内容

```
ViewA  1.1.2.1       included
       1.3.3.4       included
       1.1.2.1.2.1 excluded
```

18.1.2 MIB 概説

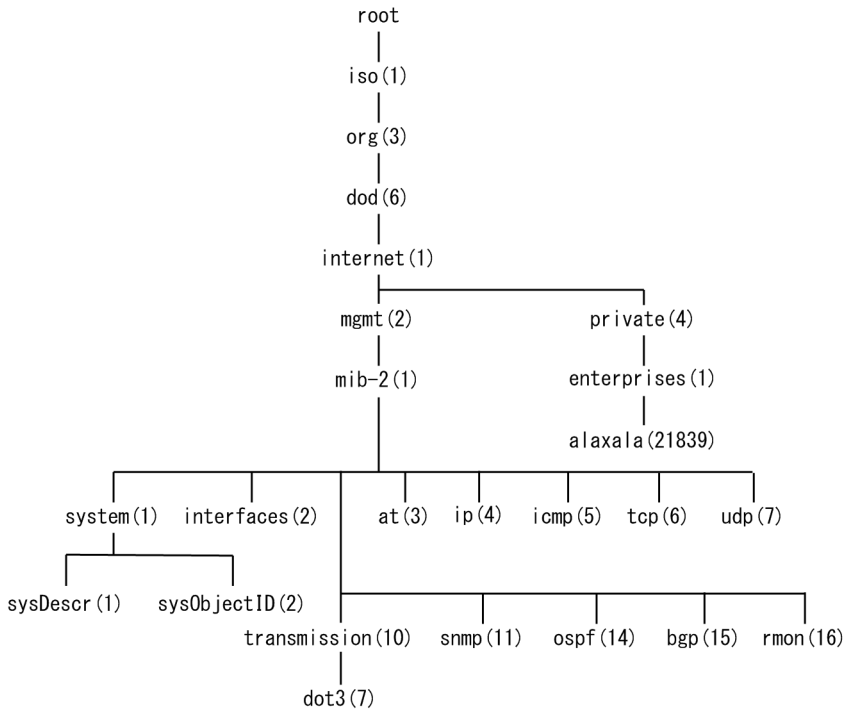
装置が管理し，SNMP マネージャに提供する MIB は，RFC で規定されたものと，装置の開発ベンダーが独自に用意する情報の 2 種類があります。

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 18-5 MIB ツリーの構造例



(2) MIB オブジェクトの表し方

オブジェクト ID は数字と.（ドット）（例：1.3.6.1.2.1.1.1）で表現します。しかし，数字の羅列ではわかりにくいため，マネージャによっては，sysDescr というニーモニックで指定できるものもあります。ニーモニックで指定する場合，SNMP マネージャがどの MIB のニーモニックを使えるか確認してから使用してください。また，本装置の SNMP コマンドで使用できるニーモニックについては，snmp lookup コマンドを実行することで確認できます。

(3) インデックス

MIB を指定するときのオブジェクト ID を使用しますが，一つの MIB に一つの意味だけある場合と一つの MIB に複数の情報がある場合があります。MIB を特定するためにはインデックス（INDEX）を使用します。インデックスは，オブジェクト ID の後ろに数字を付加して表し，何番目の情報かなどを示すために使用します。

一つの MIB に一つの意味だけがある場合，MIB のオブジェクト ID に".0"を付加して表します。一つの MIB に複数の情報がある場合，MIB のオブジェクト ID の後ろに数字を付加して何番目の情報であるか表します。例えば，インタフェースのタイプを示す MIB に ifType（1.3.6.1.2.1.2.2.1.2）があります。本装置には複数のインタフェースがあります。特定のインタフェースのタイプを調べるには，"2 番目のインタフェースのタイプ"というように具体的に指定する必要があります。MIB で指定するときは，2 番目を示すインデックス.2 を MIB の最後に付加して ifType.2（1.3.6.1.2.1.2.2.1.2.2）と表します。

インデックスの表し方は，各 MIB によって異なります。RFC などの MIB の定義で，
INDEX{ xxxxx,yyyyy,zzzzzz }となっている MIB のエントリは，xxxxx と yyyyy と zzzzzz をインデックスに持ちます。それぞれの MIB について，どのようなインデックスを取るか確認して MIB のオペレーションを行ってください。

(4)　本装置のサポート MIB

本装置では，装置の状態，インタフェースの統計情報，装置の機器情報など，管理に必要な MIB を提供しています。なお，プライベート MIB の定義（ASN.1）ファイルは，ソフトウェアとともに提供します。

各 MIB の詳細については，「MIB レファレンス」を参照してください。

18.1.3　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。

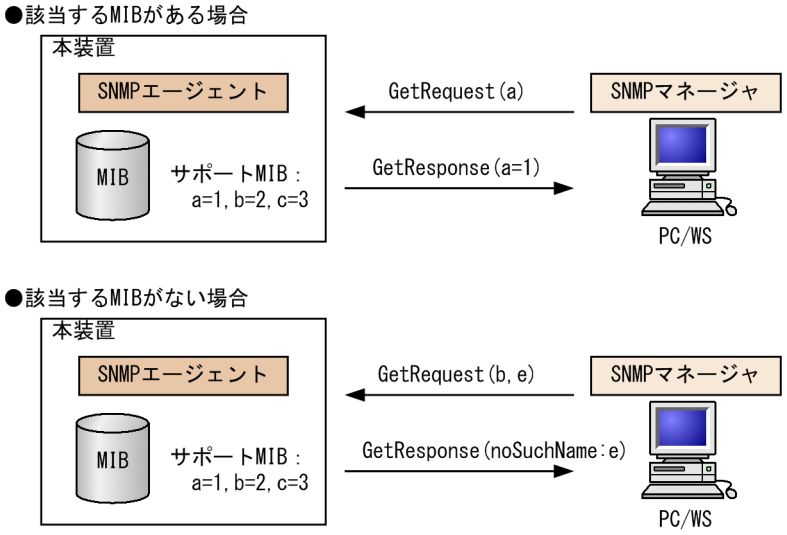
各オペレーションは SNMP マネージャから装置（SNMP エージェント）に対して行われます。各オペレーションについて説明します。

(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。

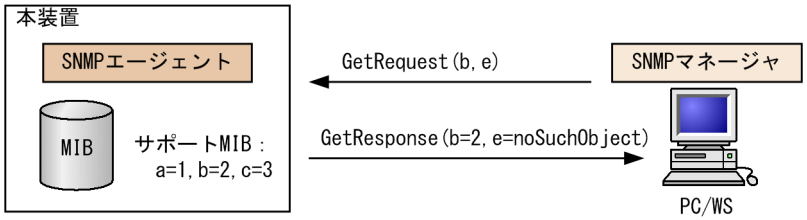
装置が該当する MIB を保持している場合，GetResponse オペレーションで MIB 情報を応答します。該当する MIB を保持していない場合は，GetResponse オペレーションで noSuchName を応答します。
GetRequest オペレーションを次の図に示します。

図 18-6　GetRequest オペレーション



SNMPv2C では，装置が該当する MIB を保持していない場合は，GetResponse オペレーションで MIB 値に noSuchObject を応答します。SNMPv2C の場合の GetRequest オペレーションを次の図に示します。

図 18-7　GetRequest オペレーション（SNMPv2C）

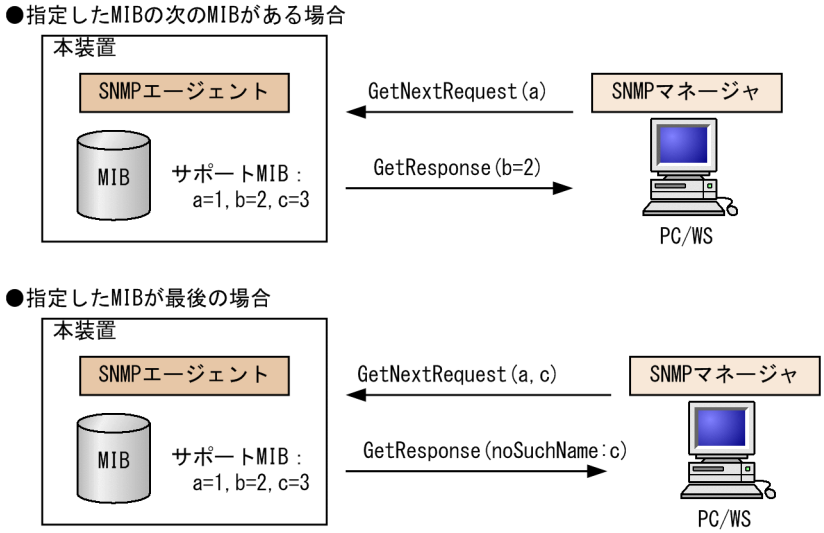


(2)　GetNextRequest オペレーション

GetNextRequest オペレーションは，GetRequest オペレーションに似たオペレーションです。GetRequest オペレーションは，指定した MIB の読み出しに使用しますが，GetNextRequest オペレーションは，指定した MIB の次の MIB を取り出すときに使用します。このオペレーションも一つまたは複数の MIB を指定できます。

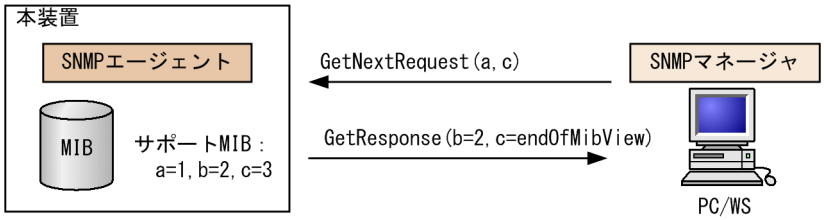
装置が指定した次の MIB を保持している場合は，GetResponse オペレーションで MIB を応答します。指定した MIB が最後の場合は，GetResponse で noSuchName を応答します。GetNextRequest オペレーションを次の図に示します。

図 18-8　GetNextRequest オペレーション



SNMPv2C の場合，指定した MIB が最後の場合は GetResponse で MIB 値に endOfMibView を応答します。SNMPv2C の場合の GetNextRequest オペレーションを次の図に示します。

図 18-9　GetNextRequest オペレーション（SNMPv2C）

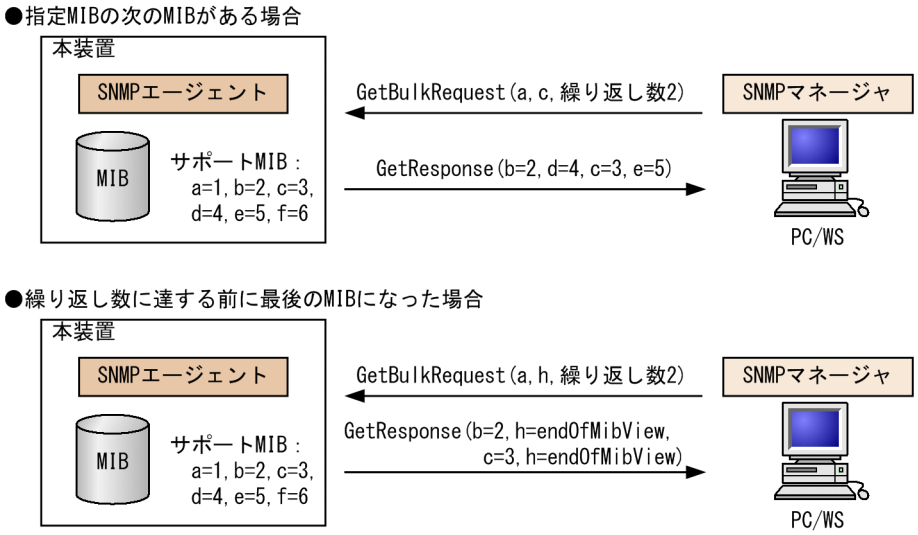


(3)　GetBulkRequest オペレーション

GetBulkRequest オペレーションは，GetNextRequest オペレーションを拡張したオペレーションです。このオペレーションでは繰り返し回数を設定し，指定した MIB の次の項目から指定した繰り返し回数個分の MIB を取得できます。このオペレーションも，一つまたは複数の MIB を指定できます。

装置が，指定した MIB の次の項目から指定した繰り返し回数個分の MIB を保持している場合は，GetResponse オペレーションで MIB を応答します。指定した MIB が最後の場合，または繰り返し数に達する前に最後の MIB になった場合，GetResponse オペレーションで MIB 値に endOfMibView を応答します。GetBulkRequest オペレーションを次の図に示します。

図 18-10　GetBulkRequest オペレーション

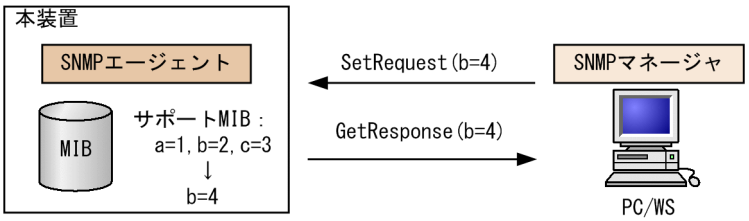


(4)　SetRequest オペレーション

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 18-11　SetRequest オペレーション



(a)　MIB を設定できない場合の応答

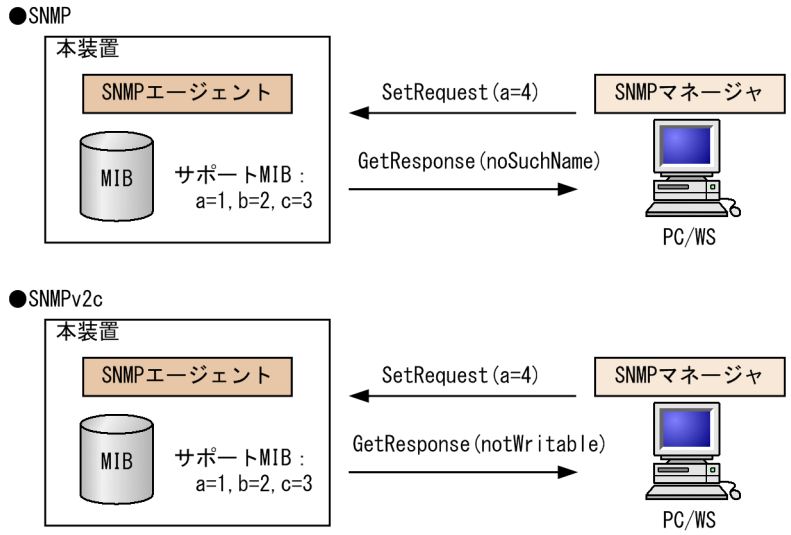
MIB を設定できないケースは，次に示す 3 とおりです。

- MIB が読み出し専用の場合（読み出し専用コミュニティに属するマネージャの場合も含む）

- 設定値が正しくない場合
- 装置の状態によって設定できない場合

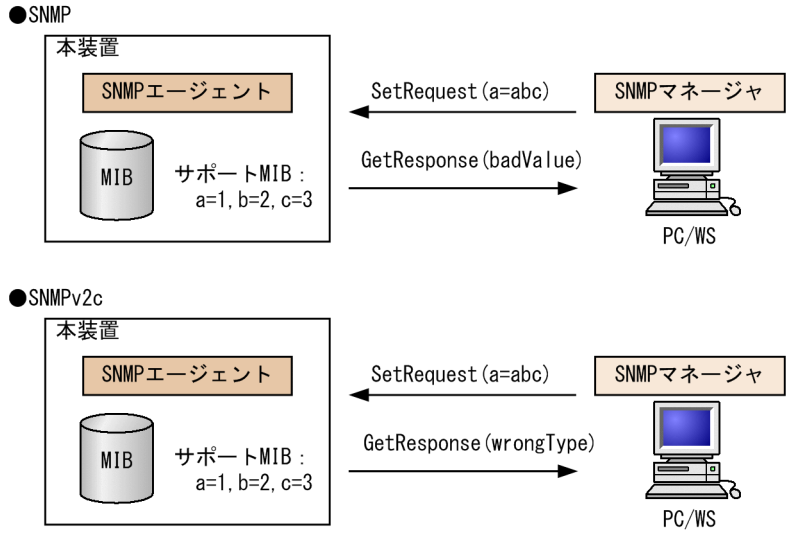
各ケースによって，応答が異なります。MIB が読み出し専用の場合，noSuchName の GetResponse 応答をします。SNMPv2C の場合，MIB が読み出し専用のときは notWritable の GetResponse 応答をします。MIB が読み出し専用の場合の SetRequest オペレーションを次の図に示します。

図 18-12　MIB 変数が読み出し専用の場合の SetRequest オペレーション



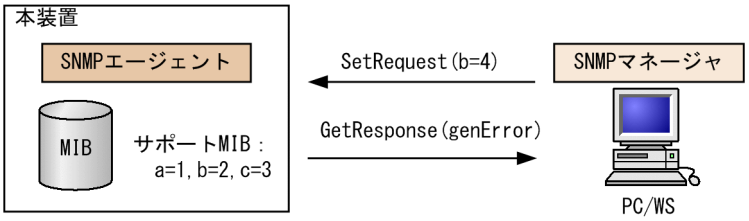
設定値のタイプが正しくない場合，badValue の GetResponse 応答をします。SNMPv2C の場合，設定値のタイプが正しくないときは wrongType の GetResponse 応答をします。設定値のタイプが正しくない場合の SetRequest オペレーションを次の図に示します。

図 18-13　設定値のタイプが正しくない場合の SetRequest オペレーション例



装置の状態によって設定できない場合，genError を応答します。例えば，装置内で値を設定しようとしたときに，装置内部で設定タイムアウトを検出した場合などがこれに当てはまります。装置の状態によって設定できない場合の SetRequest オペレーションを次の図に示します。

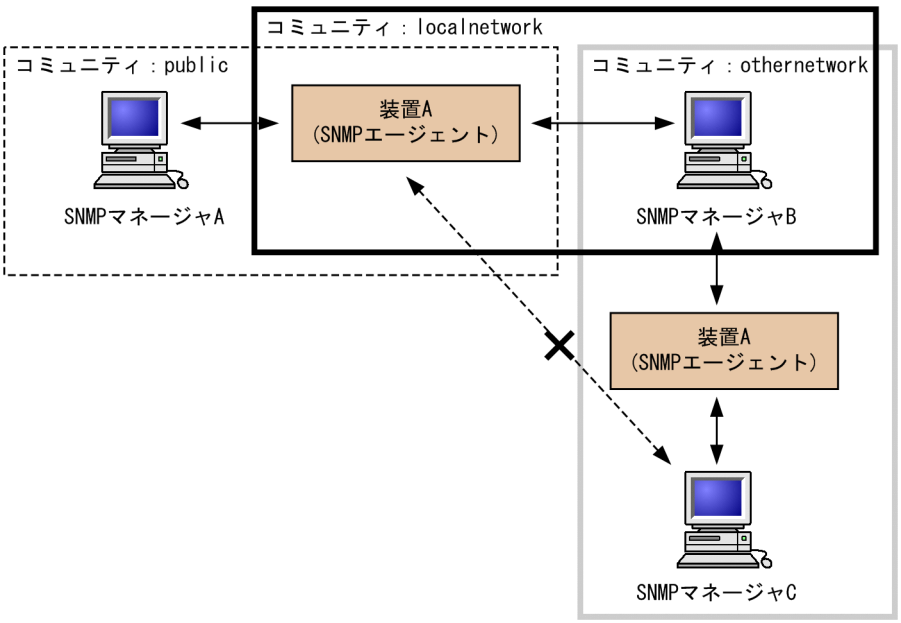
図 18-14　装置の状態によって設定できない場合の SetRequest オペレーション



(5)　コミュニティによるオペレーション制限

SNMPv1 および SNMPv2C では，オペレーションを実行する SNMP マネージャを限定するため，コミュニティという概念があります。コミュニティはオペレーションを実行する SNMP マネージャと SNMP エージェントを一つのグループとして割り当てる名称です。MIB に対してオペレーションする場合は，SNMP マネージャと SNMP エージェントは，同一のグループ（コミュニティ）に属する必要があります。コミュニティによるオペレーションを次の図に示します。

図 18-15　コミュニティによるオペレーション



装置 A はコミュニティ（public）およびコミュニティ（localnetwork）に属しています。コミュニティ（othernetwork）には属していません。この場合，装置 A はコミュニティ（public）およびコミュニティ（localnetwork）の SNMP マネージャ A，B から MIB のオペレーションを受け付けますが，コミュニティ（othernetwork）の SNMP マネージャ C からのオペレーションは受け付けません。

(6)　IP アドレスによるオペレーション制限

本装置では，セキュリティを考慮し，アクセスリストを使用することでコミュニティと SNMP マネージャの IP アドレスの組み合わせが合わないときは MIB のオペレーションを受け付けないようにできます。本装置で SNMPv1 および SNMPv2C を使用するときは，コミュニティをコンフィグレーションコマンドで登録する必要があります。なお，コミュニティは文字列で設定します。また，一般的にコミュニティ名称は，public を使用している場合が多いです。

(7) SNMP オペレーションのエラーステータスコード

オペレーションでエラーが発生した場合，SNMP エージェントはエラーステータスにエラーコードを設定し，何番目の MIB 情報でエラーが発生したかをエラー位置番号に設定した GetResponse オペレーションの応答を返します。オペレーションの結果が正常なら，エラーステータスにエラーなしのコードを設定し，MIB 情報内にオペレーションした MIB 情報を設定した GetResponse オペレーションの応答を返します。エラーステータスコードを次の表に示します。

表 18-1 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。
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。

18.1.4 SNMPv3 オペレーション

管理データ（MIB:management information base）の収集や設定を行うため，SNMP では次に示す四種類のオペレーションがあります。

- GetRequest ：指定した MIB の情報を取り出します。
- GetNextRequest：指定した次の MIB の情報を取り出します。
- GetBulkRequest：GetNextRequest の拡張版です。
- SetRequest ：指定した MIB に値を設定します。

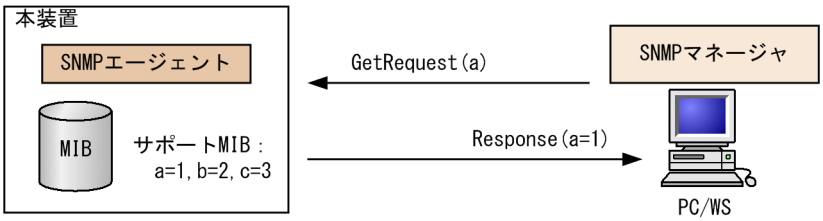
各オペレーションは SNMP マネージャから装置（SNMP エージェント）に対して行われます。各オペレーションについて説明します。

(1)　GetRequest オペレーション

GetRequest オペレーションは，SNMP マネージャから装置（エージェント機能）に対して MIB の情報を取り出すときに使用します。このオペレーションでは，一つまたは複数の MIB を指定できます。装置が該当する MIB を保持している場合，Response オペレーションで MIB 情報を応答します。

GetRequest オペレーションを次の図に示します。

図 18-16　GetRequest オペレーション

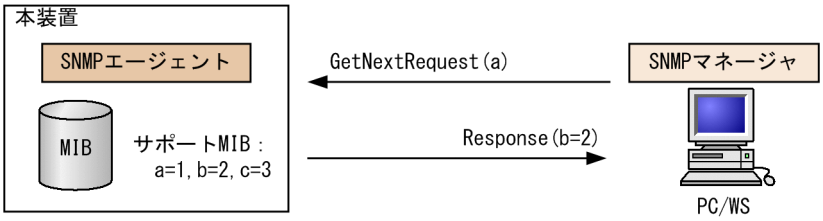


(2)　GetNextRequest オペレーション

GetNextRequest オペレーションは，GetRequest オペレーションに似たオペレーションです。GetRequest オペレーションが指定した MIB の読み出しに使用するのに対し，GetNextRequest オペレーションは指定した MIB の次の MIB を取り出すときに使用します。このオペレーションも一つまたは複数の MIB を指定できます。

GetNextRequest オペレーションを次の図に示します。

図 18-17　GetNextRequest オペレーション

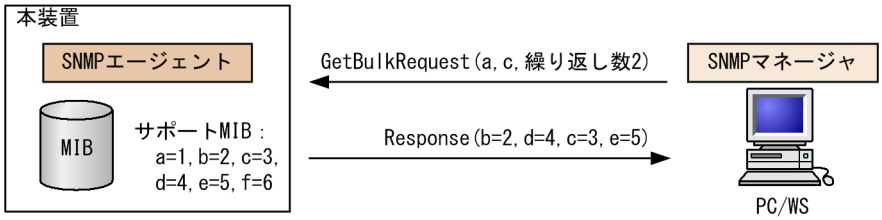


(3)　GetBulkRequest オペレーション

GetBulkRequest オペレーションは，GetNextRequest オペレーションを拡張したオペレーションです。このオペレーションでは繰り返し回数を設定し，指定した MIB の次の項目から指定した繰り返し回数個分の MIB を取得できます。このオペレーションも，一つまたは複数の MIB を指定できます。

GetBulkRequest オペレーションを次の図に示します。

図 18-18　GetBulkRequest オペレーション



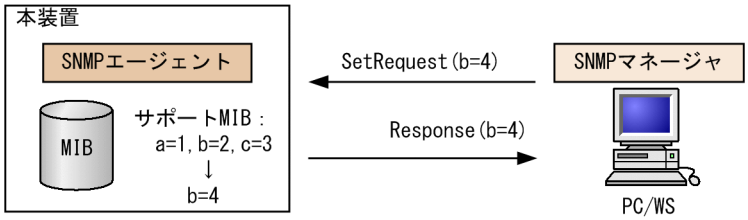
(4)　SetRequest オペレーション

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，Response オペレーションで MIB と設定値を応答します。

SetRequest オペレーションを次の図に示します。

図 18-19　SetRequest オペレーション



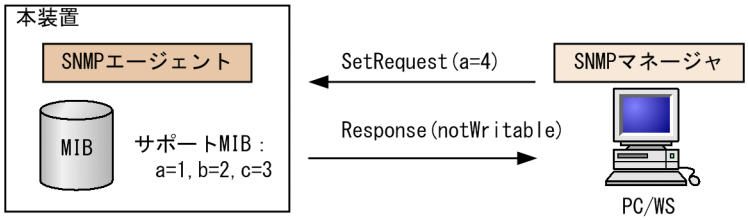
(a)　MIB を設定できない場合の応答

MIB を設定できないケースは，次に示す 3 とおりです。

- MIB が読み出し専用の場合
- 設定値が正しくない場合
- 装置の状態によって設定できない場合

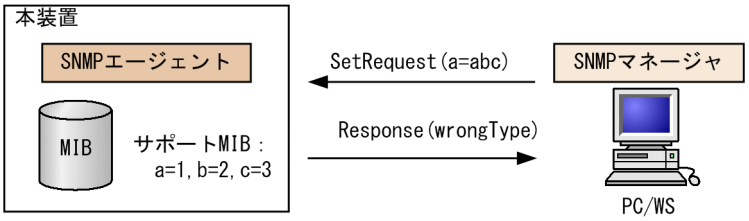
各ケースによって，応答が異なります。MIB が読み出し専用のときは notWritable の Response 応答をします。MIB が読み出し専用の場合の SetRequest オペレーションを次の図に示します。

図 18-20　MIB 変数が読み出し専用の場合の SetRequest オペレーション



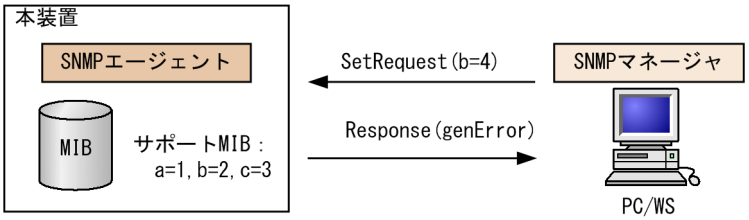
設定値のタイプが正しくないときは wrongType の Response 応答をします。設定値のタイプが正しくない場合の SetRequest オペレーションを次の図に示します。

図 18-21　設定値のタイプが正しくない場合の SetRequest オペレーション例



装置の状態によって設定できない場合，genError を応答します。例えば，装置内で値を設定しようとしたときに，装置内部で設定タイムアウトを検出した場合などがこれに当てはまります。装置の状態によって設定できない場合の SetRequest オペレーションを次の図に示します。

図 18-22　装置の状態によって設定できない場合の SetRequest オペレーション



(5)　SNMPv3 でのオペレーション制限

SNMPv1 および SNMPv2C ではコミュニティと SNMP マネージャの IP アドレスの組み合わせによって確認が行われるのに対し，SNMPv3 ではユーザ認証と MIB ビューによって MIB のオペレーションを制限します。本装置で SNMPv3 を使用するときは，SNMP セキュリティユーザ，MIB ビューおよびセキュリティグループをコンフィグレーションコマンドで登録する必要があります。また，トラップを送信するには，SNMP セキュリティユーザ，MIB ビュー，セキュリティグループ，およびトラップ送信 SNMP マネージャをコンフィグレーションコマンドで登録する必要があります。

(6)　SNMPv3 オペレーションのエラーステータスコード

オペレーションの結果エラーが発生した場合，SNMP エージェントはエラーステータスにエラーコードを設定し，何番目の MIB 情報でエラーが発生したかをエラー位置番号に設定した Response オペレーションの応答を返します。オペレーションの結果が正常であれば，エラーステータスにエラーなしのコードを設定し，MIB 情報内にオペレーションした MIB 情報を設定した Response オペレーションの応答を返します。エラーステータスコードを次の表に示します。

表 18-2　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。
authorizationError	16	認証に失敗しました。
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。

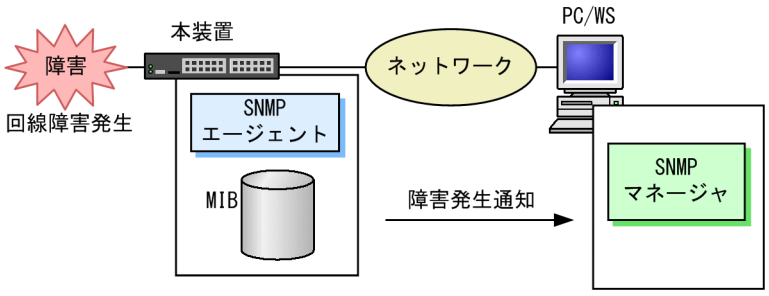
18.1.5　トラップ

(1)　トラップ概説

SNMP エージェントは**トラップ**（Trap）と呼ばれるイベント通知（主に障害発生の情報やログ情報など）機能があります。トラップは重要なイベントを SNMP エージェントから SNMP マネージャに非同期に通知する機能です。SNMP マネージャは，トラップを受信することで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。

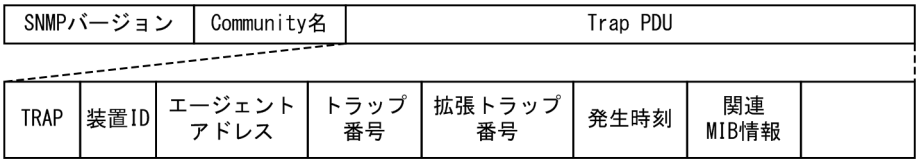
図 18-23　トラップの例



(2)　トラップフォーマット（SNMPv1）

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（SNMPv1）を次の図に示します。

図 18-24 トラップフォーマット（SNMPv1）

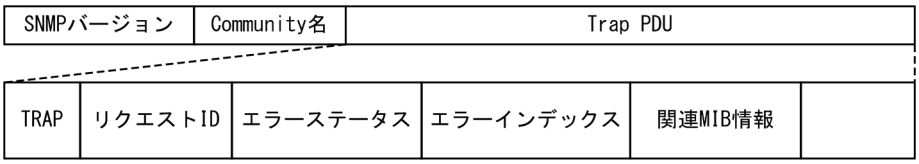


装置ID　：装置の識別ID（通常MIB-IIのsysObjectIDの値が設定される）
エージェントアドレス：トラップが発生した装置のIPアドレス
トラップ番号　：トラップの種別を示す識別番号
拡張トラップ番号　：トラップ番号の補足をするための番号
発生時刻　：トラップが発生した時間（装置が起動してからの経過時間）
関連MIB情報　：このトラップに関連するMIB情報

(3) トラップフォーマット（SNMPv2C，SNMPv3）

トラップフレームには，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（SNMPv2C，SNMPv3）を次の図に示します。

図 18-25 トラップフォーマット（SNMPv2C，SNMPv3）



リクエストID　：メッセージ識別子。リクエストごとに異なる。
エラーステータス　：発生したエラーを示す値
エラーインデックス　：関連MIB情報でのエラー位置
関連MIB情報　：このトラップに関連するMIB情報

18.1.6 インフォーム

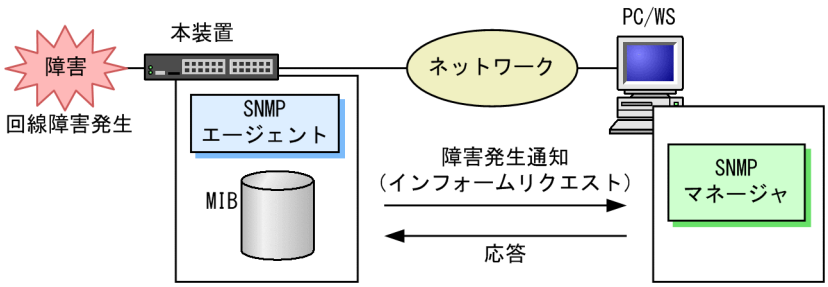
(1) インフォーム概説

SNMP エージェントは**インフォーム**（Inform）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。インフォームはインフォームリクエストを送信して，重要なイベントを SNMP エージェントから SNMP マネージャに通知する機能です。SNMP マネージャは，インフォームリクエストを受信することで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。

インフォームは SNMPv2C だけのサポートとなります。また，SNMP マネージャもインフォームに対応している必要があります。

なお，インフォームもトラップと同じ UDP によるイベント通知ですが，トラップとは異なって SNMP マネージャからの応答を要求します。そのため，応答の有無でインフォームリクエストの到達を確認できます。これによって，ネットワークの輻輳などに対してもインフォームリクエストの再送で対応できます。インフォームの例を次の図に示します。

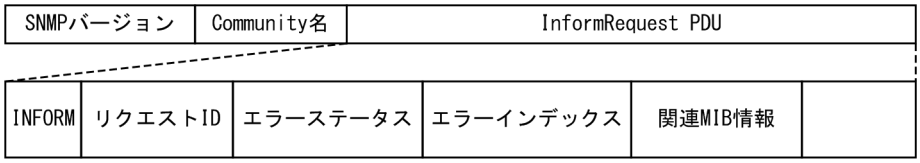
図 18-26　インフォームの例



(2)　インフォームリクエストフォーマット

インフォームリクエストフレームには，いつ，何が発生したかを示す情報を含みます。インフォームリクエストフォーマットを次の図に示します。

図 18-27　インフォームリクエストフォーマット



リクエストID　　：メッセージ識別子。リクエストごとに異なる。
エラーステータス　：発生したエラーを示す値
エラーインデックス　：関連MIB情報でのエラー位置
関連MIB情報　　：このインフォームリクエストに関連するMIB情報

18.1.7　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 SNMP 通知を送信したりすることを指定する MIB です。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。

alarm グループによる MIB 監視には，MIB 値の差分（変動）と閾値を比較する **delta 方式**と，MIB 値と閾値を直接比較する **absolute 方式**があります。

delta 方式による閾値チェックでは，例えば，CPU 使用率の変動が 50%以上あったときに，ログを収集したり，SNMP マネージャに SNMP 通知を送信したりできます。absolute 方式による閾値チェックでは，例えば，CPU の使用率が 80%に達したときに，ログを収集したり，SNMP マネージャに SNMP 通知を送信したりできます。

本装置では，閾値をチェックするタイミングによる検出漏れをできるだけ防止するために，alarmInterval（MIB 値を監視する時間間隔（秒）を表す MIB）の間に複数回チェックします。alarmInterval ごとの閾値チェック回数を次の表に示します。

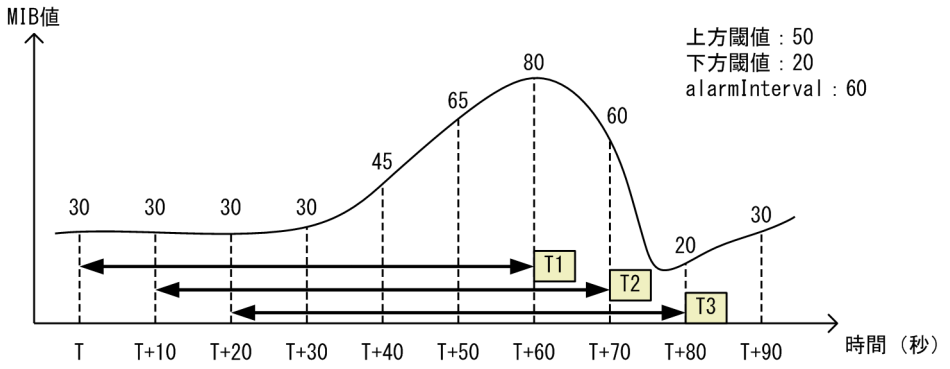
表 18-3 alarmInterval ごとの閾値チェック回数

alarmInterval（秒）	閾値チェック回数
1	1
2～5	2
6～10	3
11～20	4
21～50	5
51～100	6
101～200	7
201～400	8
401～800	9
801～1300	10
1301～2000	11
2001～4294967295	12

閾値のチェックは，およそ alarmInterval を閾値チェック回数で割った秒数ごとに行います。例えば，alarmInterval が 60（秒）の場合，閾値チェック回数は 6 回になるため，10 秒に 1 回のタイミングで閾値をチェックします。

上方閾値を 50，下方閾値を 20，alarmInterval を 60 として，CPU 使用率の MIB 値を delta 方式で監視した場合の例を次の図に示します。

図 18-28　delta 方式による MIB 監視例



T1

閾値と比較する値が 50（T+60（秒）の MIB 値 80－T（秒）の MIB 値 30）のため，上方閾値以上を検出

T2

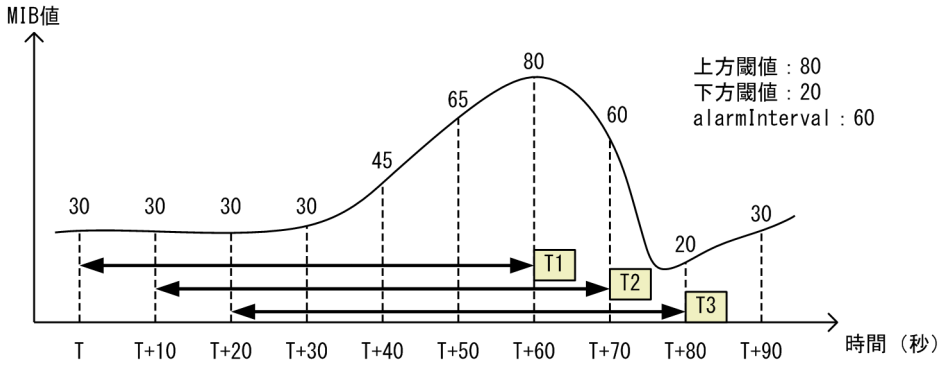
閾値と比較する値が 30（T+70（秒）の MIB 値 60－T+10（秒）の MIB 値 30）のため，閾値検出なし

T3

閾値と比較する値が-10（T+80（秒）の MIB 値 20－T+20（秒）の MIB 値 30）のため，下方閾値以下を検出

上方閾値を 80，下方閾値を 20，alarmInterval を 60 として，CPU 使用率の MIB 値を absolute 方式で監視した場合の例を次の図に示します。

図 18-29　absolute 方式による MIB 監視例



T1

閾値と比較する値が 80（T+60（秒）の MIB 値）のため，上方閾値以上を検出

T2

閾値と比較する値が 60（T+70（秒）の MIB 値）のため，閾値検出なし

T3

閾値と比較する値が 20（T+80（秒）の MIB 値）のため，下方閾値以下を検出

(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 SNMP 通知を送信するのか，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。

18.1.8 SNMP マネージャとの接続時の注意事項

(1) MIB 情報収集周期のチューニング

SNMP マネージャは，ネットワーク上の新しい装置を検出したり，トラフィック状況を監視したりするため，SNMP エージェントサポート機器から定期的に MIB を取得します。この定期的な MIB 取得の間隔が短いと，ネットワーク機器やネットワークに負荷が掛かります。また，装置の状態や構成などによって，MIB 取得時にマネージャ側でタイムアウトが発生するおそれがあります。特に，次に示すケースでは応答タイムアウトの発生するおそれが高まります。

- 接続 SNMP マネージャ数が多い場合
  本装置に SNMP マネージャが多数接続され，MIB 情報の収集が集中した場合。
- SNMP イベントが同時に多数発生している場合
  本装置から大量に SNMP 通知が送信されるような状態のときに，MIB を取得した場合や，本装置から送信された SNMP 通知に基づいて，並行して MIB を取得した場合。

応答タイムアウトが頻発する場合は，SNMP マネージャのポーリング周期や応答監視タイマ値をチューニングしてください。代表的な SNMP マネージャのチューニングパラメータには，次の三つがあります。

- ポーリング周期
- 応答監視タイマ
- 応答監視タイムアウト時のリトライ回数

18.2 コマンドガイド

18.2.1 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 18-4 コンフィグレーションコマンド一覧

コマンド名	説明
hostname	本装置のホスト名称を設定します。本設定は RFC1213 の sysName に対応します。
rmon alarm	RMON（RFC1757)アラームグループの制御情報を設定します。
rmon collection history	RMON（RFC1757)イーサネットの統計来歴の制御情報を設定します。
rmon event	RMON（RFC1757)イベントグループの制御情報を設定します。
snmp-server community	SNMP コミュニティに対するアクセスリストを設定します。
snmp-server contact	本装置の連絡先などを設定します。本設定は RFC1213 の sysContact に対応します。
snmp-server engineID local	SNMP エンジン ID 情報を設定します。
snmp-server group	SNMP セキュリティグループ情報を設定します。
snmp-server host	SNMP 通知を送信する宛先のネットワーク管理装置（SNMP マネージャ）を登録します。
snmp-server informs	インフォームの再送条件を設定します。
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	SNMP 通知の送信契機を設定します。
snmp-server user	SNMP セキュリティユーザ情報を設定します。
snmp-server view	MIB ビュー情報を設定します。
snmp trap link-status	回線がリンクアップまたはダウンした場合に，SNMP 通知（linkUp または LinkDown）の送信を抑止します。

SNMP/RMON に関する運用コマンド一覧を次の表に示します。

表 18-5 運用コマンド一覧

コマンド名	説明
show snmp	SNMP 情報を表示します。
show snmp pending	送信を保留中のインフォームリクエストを表示します。
snmp lookup	サポート MIB オブジェクト名称およびオブジェクト ID を表示します。
snmp get	指定した MIB の値を表示します。
snmp getnext	指定した次の MIB の値を表示します。

コマンド名	説明
snmp walk	指定した MIB ツリーを表示します。
snmp rget	指定したリモート装置の MIB の値を表示します。
snmp rgetnext	指定したリモート装置の次の MIB の値を表示します。
snmp rwalk	指定したリモート装置の MIB ツリーを表示します。

18.2.2 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。

[コマンドによる設定]

1. **(config)# access-list 1 permit 10.1.1.1 0.0.0.0**

   IP アドレス 10.1.1.1 からのアクセスを許可するアクセスリストの設定を行います。

2. **(config)# snmp-server community "NETWORK" ro 1**

   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：1
   - アクセスモード：read only

18.2.3 SNMPv3 による MIB アクセス許可の設定

[設定のポイント]

SNMPv3 で MIB にアクセスするために，アクセスを許可する MIB オブジェクトの集合を MIB ビューとして設定し，ユーザ認証と暗号化機能の情報を SNMP セキュリティユーザとして設定します。また，MIB ビューと SNMP セキュリティユーザを関連づけるために，SNMP セキュリティグループを設定します。

[コマンドによる設定]

1. **(config)# snmp-server view "READ_VIEW" 1.3.6.1 included**

   (config)# snmp-server view "READ_VIEW" 1.3.6.1.6.3 excluded

   (config)# snmp-server view "WRITE_VIEW" 1.3.6.1.2.1.1 included

   MIB ビューを設定します。

   - ビュー名 READ_VIEW に internet グループ MIB（サブツリー：1.3.6.1）を登録します。
   - ビュー名 READ_VIEW から snmpModules グループ MIB（サブツリー：1.3.6.1.6.3）を対象外にします。
   - ビュー名 WRITE_VIEW に system グループ MIB（サブツリー：1.3.6.1.2.1.1）を登録します。

2. **(config)# snmp-server user "ADMIN" "ADMIN_GROUP" v3 auth md5 "ABC*_1234" priv des "XYZ/+6789"**

   SNMP セキュリティユーザを設定します。

   - SNMP セキュリティユーザ名：ADMIN

- SNMP セキュリティグループ名：ADMIN_GROUP
- 認証プロトコル：HMAC-MD5
- 認証パスワード：ABC*_1234
- プライバシープロトコル：CBC-DES
- プライバシーパスワード：XYZ/+6789

3. **(config)# snmp-server group "ADMIN_GROUP" v3 priv read "READ_VIEW" write "WRITE_VIEW"**
   SNMP セキュリティグループを設定します。
   - SNMP セキュリティグループ名：ADMIN_GROUP
   - セキュリティレベル：認証あり，暗号化あり
   - Read ビュー名：READ_VIEW
   - Write ビュー名：WRITE_VIEW

18.2.4 SNMPv1，SNMPv2C によるトラップ送信の設定

[設定のポイント]

トラップを送信する宛先の 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 10.1.1.1 traps "NETWORK" version 1 snmp**
   SNMP マネージャに標準トラップを送信する設定をします。
   - コミュニティ名：NETWORK
   - SNMP マネージャの IP アドレス：10.1.1.1
   - 送信するトラップ：coldStart，warmStart，linkDown，linkUp，authenticationFailure

18.2.5 SNMPv3 によるトラップ送信の設定

[設定のポイント]

MIB ビューと SNMP セキュリティユーザを設定の上，SNMP セキュリティグループを設定し，さらに SNMP トラップモードを設定します。

[コマンドによる設定]

1. **(config)# snmp-server view "ALL_TRAP_VIEW" * included**
   MIB ビューを設定します。
   - ビュー名 ALL_TRAP_VIEW に全サブツリーを登録します。
2. **(config)# snmp-server user "ADMIN" "ADMIN_GROUP" v3 auth md5 "ABC*_1234" priv des "XYZ/+6789"**
   SNMP セキュリティユーザを設定します。
   - SNMP セキュリティユーザ名：ADMIN
   - SNMP セキュリティグループ名：ADMIN_GROUP
   - 認証プロトコル：HMAC-MD5
   - 認証パスワード：ABC*_1234

- プライバシープロトコル：CBC-DES
- プライバシーパスワード：XYZ/+6789

3. **(config)# snmp-server group "ADMIN_GROUP" v3 priv notify "ALL_TRAP_VIEW"**
   SNMP セキュリティグループを設定します。
   - SNMP セキュリティグループ名：ADMIN_GROUP
   - セキュリティレベル：認証あり，暗号化あり
   - Notify ビュー名：ALL_TRAP_VIEW
4. **(config)# snmp-server host 10.1.1.1 traps "ADMIN" version 3 priv snmp**
   SNMPv3 によって SNMP マネージャに標準トラップを送信する設定をします。
   - SNMP マネージャの IP アドレス：10.1.1.1
   - SNMP セキュリティユーザ名：ADMIN
   - セキュリティレベル：認証あり，暗号化あり
   - 送信するトラップ：coldStart，warmStart，linkDown，linkUp，authenticationFailure

18.2.6 SNMPv2C によるインフォーム送信の設定

[設定のポイント]

インフォームを送信する宛先の 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 10.1.1.1 informs "NETWORK" version 2c snmp**
   SNMP マネージャに標準のインフォームを送信する設定をします。
   - コミュニティ名：NETWORK
   - SNMP マネージャの IP アドレス：10.1.1.1
   - 送信するインフォーム：coldStart，warmStart，linkDown，linkUp，authenticationFailure

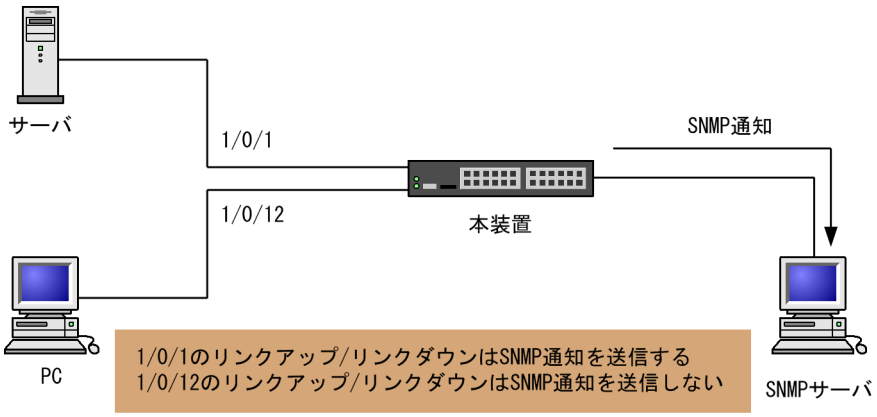
18.2.7 リンクトラップの抑止

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 通知（linkUp または linkDown）を送信します。これをリンクトラップと呼びます。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 SNMP 通知を送信し，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 18-30 リンクトラップの構成図



ここでは，ポート 1/0/1 については，SNMP 通知を送信するので，コンフィグレーションの設定は必要ありません。ポート 1/0/12 については，SNMP 通知を送信しないように設定します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/0/12**
   (config-if)# no snmp trap link-status
   リンクアップ／リンクダウン時に SNMP 通知を送信しません。
2. **(config-if)# exit**

18.2.8 RMON イーサネットヒストリグループの制御情報の設定

[設定のポイント]

RMON（RFC1757）イーサネットの統計来歴の制御情報を設定します。本コマンドでは最大 32 エントリの設定ができます。あらかじめ SNMP マネージャを登録しておく必要があります。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/0/5**
   ギガビット・イーサネットインタフェース 1/0/5 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**
   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”

18.2.9 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
   - SNMP 通知先コミュニティ名：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

19 高機能スクリプト

この章では，高機能スクリプトの使用方法について説明します。

19.1　解説

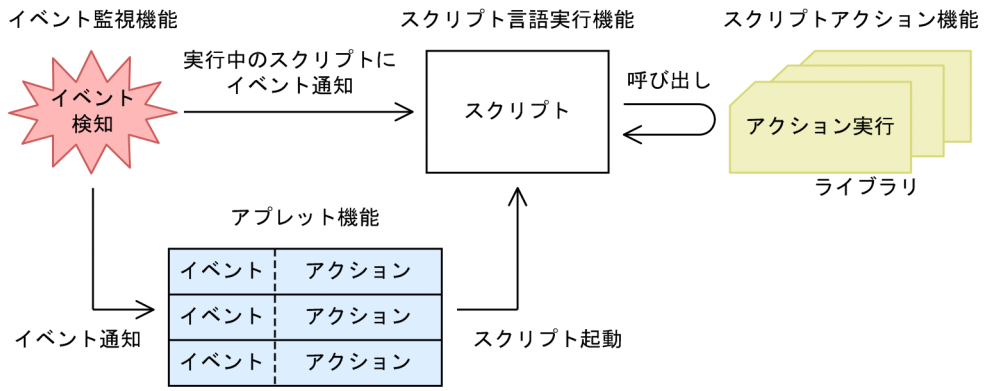
19.1.1　概要

高機能スクリプトとは，本装置のコンフィグレーションやオペレーションを，装置内でプログラミングできるようにする機能です。本機能は，次のような用途に適用できます。

- オペレーションの自動化
  例えば，運用メッセージの出力を契機として，コマンドを自動で実行できます。
- 運用機能のカスタマイズ
  例えば，ユーザが作成した運用メッセージを出力できます。

高機能スクリプトを構成する主要機能，およびそれぞれの関連性を次の図に示します。

図 19-1　高機能スクリプトを構成する主要機能



(1)　スクリプト言語実行機能

スクリプトは，本装置のコンフィグレーションやオペレーションの手順をプログラミングしたものです。スクリプト言語実行機能とは，作成したスクリプトを実行する機能です。

なお，本装置では，スクリプト言語に Python を使用します。Python は次に示す特徴を持つ言語です。

- 可読性が高い
  コードブロックをインデントでそろえるなど，記述方法を統一することで，高い可読性を持ちます。
- デバッグやプロトタイピングが容易
  Python で作成したスクリプトはインタプリタ方式で 1 行ずつ実行できるため，デバッグやプロトタイピングが容易です。
- ライブラリ提供機能の再利用が容易
  Python では，メール送信や本装置の管理機能など，よく使用する機能をまとめてライブラリという形で提供します。ライブラリで提供される機能は，スクリプトからライブラリを参照するだけで実行できます。これを利用することで，手軽にオペレーションをカスタマイズできます。

(2)　スクリプトアクション機能

スクリプトアクション機能とは，本装置へのコマンド実行などのアクションをスクリプトから実行する機能です。次に示すようなアクションがあります。

- Python 本体とともに配布される標準ライブラリを使用した，メール送信やファイルアクセスなど利便性の高い多数のアクション
- 本装置固有の拡張ライブラリを使用した，コマンド実行や運用メッセージ出力などのアクション
- ユーザが作成したライブラリを使用した，独自のアクション

このうち，本装置固有の拡張ライブラリで実行できるスクリプトアクションを次の表に示します。

表 19-1　本装置固有の拡張ライブラリのスクリプトアクション一覧

アクション	説明
コマンド実行	スクリプトで指定したコマンドを実行します。
運用メッセージ出力	指定した任意の文字列を運用メッセージとして出力します。

(3)　イベント監視機能

イベント監視機能とは，装置やネットワークの状態などを監視する機能です。監視対象の状態変化（イベント）を契機として，次に示すスクリプトやアプレットに通知します。通知先は，監視イベントの登録方法によって異なります。

- 実行中のスクリプトにイベントを通知
  監視イベントの登録と検出には，本装置が提供する拡張ライブラリを使用します。
- アプレットにイベントを通知
  監視イベントの登録には，アプレット機能が提供するコンフィグレーションを使用します。

監視イベントの一覧を次の表に示します。

表 19-2　監視イベントの一覧

監視イベント	説明
運用メッセージ監視	出力された運用メッセージを監視します。
タイマ監視	タイマを使用して，決められた時間を監視します。 タイマでは，次の 2 種類の形式で時間を指定できます。 • 時間間隔を指定（interval タイマ） • 時刻を指定（cron タイマ）

(4)　アプレット機能

アプレット機能とは，イベント監視機能と連携して，イベント発生を契機として事前に登録したアクションを実行する機能です。

監視イベントおよびアクションは，コンフィグレーションで登録します。なお，サポートしているアクションは，スクリプトファイルの起動（イベント起動スクリプト）だけです。

(5)　高機能スクリプトの使用方法

高機能スクリプトを使用する場合，まず本装置のコンフィグレーションやオペレーションをスクリプトとして作成します。このとき，スクリプトアクション機能，イベント監視機能，およびアプレット機能を自由に組み合わせて作成できます。

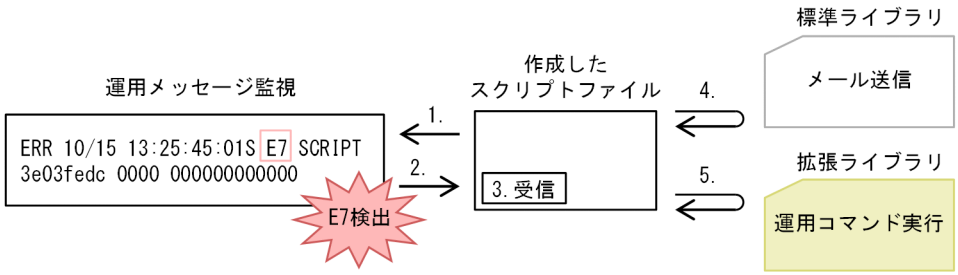
作成したスクリプトをスクリプト言語実行機能で実行すると，スクリプトに記載した各処理が実行されます。このように，高機能スクリプトを使用すると，本装置のコンフィグレーションやオペレーションをプログラミングして実行できるようになります。

19.1.2　高機能スクリプトの適用例

(1)　異常検出

スクリプトを使用して，異常（警告）検出時にオペレータへの通知と解析情報の自動収集をする例を次の図に示します。この図では運用メッセージを監視して，レベル E7 の運用メッセージ出力を検出したら，スクリプトからメール送信と運用コマンドを実行します。

図 19-2　運用メッセージ監視によるメール送信および運用コマンド実行

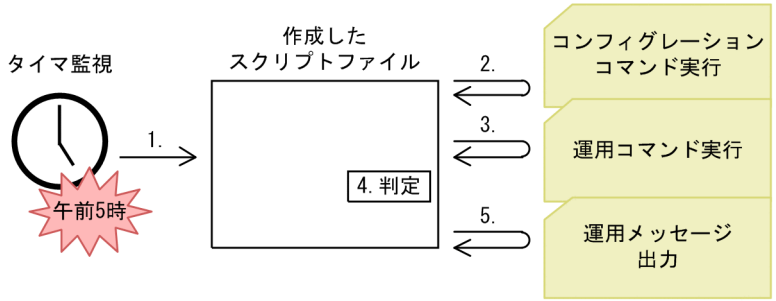


1. 運用メッセージ監視イベントを登録して，イベントの発生を待ちます。
2. レベル E7 の運用メッセージ出力を検出したら，イベントを通知します。
3. イベントを受信します。
4. イベントを受信したスクリプトは，Python の標準ライブラリを使用してオペレータにメールを送信します。
5. 関連する運用コマンドを実行して，事象発生時の解析情報を収集します。

(2)　定期的なコマンド実行

スクリプトを使用して，定期的にコマンドを実行する例を次の図に示します。この図ではタイマ監視をして，コンフィグレーションコマンドおよび運用コマンドを実行したあと，運用メッセージを出力します。

図 19-3　タイマ監視によるコマンド実行および運用メッセージ出力



事前に，午前 5 時に発生するタイマ監視イベントと，イベント発生時に起動するスクリプトファイルを，コンフィグレーションで登録しておきます。

1. 午前 5 時になるとイベントが発生して，スクリプトが起動します。

2. コンフィグレーションコマンドを実行します。

3. コンフィグレーションの反映結果が確認できる運用コマンドを実行します。

4. 3.の運用コマンドの出力結果を文字列解析して，正常性を確認します。

5. コンフィグレーションの反映結果を格納した運用メッセージを出力して，オペレータへ通知します。

19.1.3　高機能スクリプトの仕様

(1)　スクリプトの分類

スクリプトは起動方法によって次の 3 種類に分けられます。

表 19-3　起動方法によるスクリプト種別

スクリプト種別	説明
コマンドスクリプト	運用コマンド python を実行して，スクリプトを起動します。
常駐スクリプト	常駐プログラムとしてスクリプトを起動します。 運用コマンド install script でインストールしたファイルを，コンフィグレーションコマンド resident-script で指定することで起動します。
イベント起動スクリプト	監視イベントの検出を契機としてスクリプトを起動します。 運用コマンド install script でファイルをインストールしたあと，監視イベントと起動対象のファイルの関連づけをアプレット機能のコンフィグレーションコマンドで指定します。

(2)　スクリプトの標準入出力

スクリプトの標準入出力に対するサポートを次の表に示します。

表 19-4　スクリプトの標準入出力に対するサポート

スクリプト種別	標準入力	標準出力	標準エラー出力
コマンドスクリプト	○	○	○
常駐スクリプト	×	×	○※
イベント起動スクリプト	×	×	○※

（凡例）　○：サポートする　×：サポートしない

注※

運用コマンド dump script-user-program で確認できます。

(3)　スクリプト専用ユーザ

常駐スクリプトおよびイベント起動スクリプトは，スクリプト専用ユーザの権限で動作します。スクリプト専用ユーザについて次の表に示します。

表 19-5　スクリプト専用ユーザ

項目	ユーザ情報
ユーザ名	script

項目	ユーザ情報
ホームディレクトリ	/opt/script

(4)　アクセス権限

本装置で実行するスクリプトでは，本装置上のディレクトリおよびファイルへアクセスできます。スクリプトでアクセスできるディレクトリおよびファイルの範囲を次の表に示します。

表 19-6　アクセスできるディレクトリおよびファイルの範囲

アクセス種別	説明
コマンドスクリプト	コマンドスクリプトを起動したユーザ権限に従います。
常駐スクリプト	スクリプト専用ユーザの権限に従います。
イベント起動スクリプト	

(5)　同時に実行できるスクリプト数

本装置では複数回スクリプトを起動させることで，同時に複数のスクリプトを実行できます。同時に実行できるスクリプト数を次の表に示します。

表 19-7　同時に実行できるスクリプト数

スクリプト種別	同時に実行できる上限数
コマンドスクリプト	4
常駐スクリプト	4
イベント起動スクリプト	4

19.1.4　スクリプト使用時の注意事項

(1)　使用する作業ディレクトリについて

頻繁にファイルへアクセスする場合は，RAM ディスク（メモリ）上にある次の作業ディレクトリを使用してください。

表 19-8　作業ディレクトリ

ディレクトリ名	容量
/opt/script※	16MB

注※

装置を再起動すると，配下のファイルは削除されます。

(2)　動作検証について

スクリプトを使用した運用に当たっては，実環境での使用を想定して，事前に CPU やメモリなど装置のリソースの利用状況に留意した動作検証をしてください。

(3)　運用コマンド show logging での表示について

スクリプトが実行するコマンドのログを運用コマンド show logging で非表示とした場合，ログを確認するときに運用上重要なコマンドのエラーを見逃すおそれがあります。そのため，次に示す対応を推奨します。

- 重要なコマンドを実行するときは一時的に表示対象とする。
- コマンドの実行結果がエラーになったときにメッセージを出力するスクリプトを作成する。

(4)　運用コマンド set clock 使用時の注意事項

タイマ監視（cron タイマ）は装置の時刻を使って管理しています。そのため，運用コマンド set clock で時刻を変更した場合，変更した直後は，変更した時間によってイベント発生の周期が変わったり，短い時間に複数回のイベントが発生したりすることがあります。なお，それ以降はタイマ監視の周期に従って，正常にイベントが発生するようになります。

19.2　スクリプトの作成と実行

19.2.1　コマンド一覧

高機能スクリプトのコンフィグレーションコマンド一覧を次の表に示します。

表 19-9　コンフィグレーションコマンド一覧

コマンド名	説明
aaa authorization commands script	スクリプトによるコマンド実行時のコマンド承認動作を設定します。
action	アプレット機能による監視イベント検出時のアクション（イベント起動スクリプト）を指定します。
disable	アプレット機能の動作を抑止します。
event manager applet	アプレット機能に関する動作情報を指定します。
event sysmsg	アプレット機能による運用メッセージ監視の監視条件を指定します。
event timer	アプレット機能によるタイマ監視の監視条件を指定します。
priority	アプレットの実行優先度を指定します。
resident-script	常駐スクリプトの起動情報を指定します。

高機能スクリプトの運用コマンド一覧を次の表に示します。

表 19-10　運用コマンド一覧

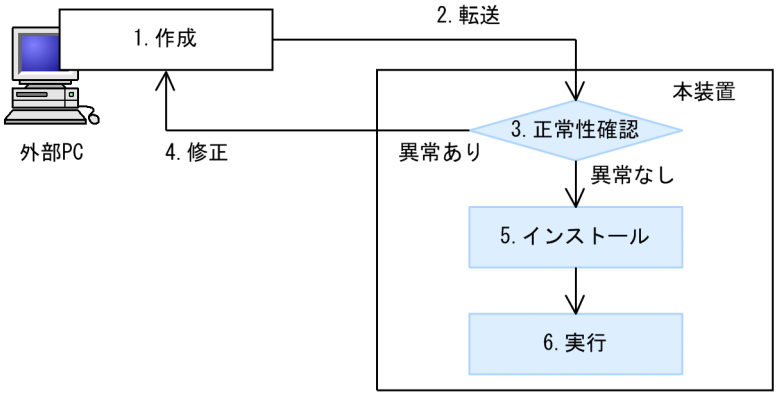
コマンド名	説明
python	Python を実行します。
stop python	起動中のスクリプトを停止します。
pyflakes	スクリプトファイルの文法チェックをします。
install script	作成したスクリプトファイルを本装置にインストールします。
uninstall script	本装置にインストールされているスクリプトファイルを削除します。
show script installed-file	本装置にインストールされているスクリプトファイルの情報を表示します。
show script running-state	スクリプトの起動情報を表示します。
show event manager history	監視イベントの発生履歴を表示します。
show event manager monitor	監視イベント情報を表示します。
clear event manager	イベント管理に関連する統計情報と発生履歴をクリアします。
restart script-manager	スクリプト管理プログラムを再起動します。 スクリプト管理プログラムは, コマンドスクリプトおよび常駐スクリプトの起動情報を管理します。
restart event-manager	イベント管理プログラムを再起動します。 イベント管理プログラムは, スクリプトから登録されたイベントを監視および検出します。

コマンド名	説明
dump script-user-program	常駐スクリプトおよびイベント起動スクリプトで出力される標準エラーを取得します。
dump script-manager	スクリプト管理プログラムで採取している制御情報をファイルへ出力します。
dump event-manager	イベント管理プログラムで採取している制御情報をファイルへ出力します。

19.2.2　スクリプトの実行の流れ

本装置でスクリプトを実行する流れについて次の図に示します。

図 19-4　スクリプト実行の流れ



1. 外部 PC でスクリプトを作成します。
2. 作成したスクリプトを，本装置に転送します。
3. 本装置内の機能を使用して，スクリプトの正常性を確認します。
4. スクリプトに異常がある場合，外部 PC でスクリプトを修正します。
5. スクリプトに異常がない場合，スクリプトを本装置にインストールします。
6. インストールしたスクリプトを実行します。

19.2.3　スクリプトファイルの作成

スクリプトファイルは，PC などの外部装置で作成してから，ftp などを使用して本装置に転送してください。作成および転送時の注意事項を次に示します。

- 文字コードは UTF-8（BOM なし）を使用してください。
- 本装置へ ftp で転送するときは，スクリプトファイルの形式に合わせたモードを使用してください。

  テキストのスクリプトファイル（拡張子が.py）の場合

  　アスキーモードで転送してください。

  コンパイル済みのスクリプトファイル（拡張子が.pyc または.pyo）の場合

  　バイナリモードで転送してください。

19.2.4　スクリプトファイルの正常性確認

作成したスクリプトファイルの正常性を確認する方法を次の表に示します。

表 19-11　スクリプトファイルの正常性を確認する方法

確認方法	説明
運用コマンド pyflakes	PyPI（Python ライブラリの公開サイト）に公開されている，「pyflakes（pyflakes3k）」と呼ばれる文法チェッカーを利用して確認します。
pdb モジュール	Python の標準ライブラリとして提供されているデバッガを利用して確認します。ブレークポイントの設定や，ステップ実行ができます。
運用コマンド dump script-user-program	常駐スクリプトで出力される標準エラーを取得して確認します。

(1)　運用コマンド pyflakes による確認

運用コマンド pyflakes を実行すると，指定したファイルに対して pyflakes（pyflakes3k）による文法チェックをします。pyflakes コマンドを使用して，sample.py ファイルの文法チェックをする例を次の図に示します。

図 19-5　pyflakes コマンドの実行例

```
> pyflakes sample.py
sample.py:4: invalid syntax
for cnt in range(10)
                   ^                                    …1
>
```

1. for 文の末尾に異常があることを示しています。

(2)　pdb モジュールを使用した確認

運用コマンド python で pdb モジュールを使用すると，指定したファイルをデバッグするためのデバッガコマンドが使用できます。pdb モジュールを使用して，sample.py ファイルの正常性を確認する例を次の図に示します。

図 19-6　pdb モジュールの使用例

```
# python -m pdb sample.py                              …1
> /usr/home/share/sample.py(1)<module>()
-> import os
(Pdb) b 4                                              …2
Breakpoint 1 at /usr/home/share/sample.py:4
(Pdb) r                                                …3
> /usr/home/share/sample.py(4)<module>()
-> for cnt in range(10):
(Pdb) s                                                …4
> /usr/home/share/sample.py(5)<module>()
-> if(cnt == 9):
(Pdb) cl                                               …5
Clear all breaks? y
Deleted breakpoint 1 at /usr/home/share/sample.py:4
(Pdb) r
--Return--
> /usr/home/share/sample.py(7)<module>()->None
-> sys.exit()
(Pdb) q                                                …6
#
```

1. -m オプションで pdb モジュールを使用して，sample.py スクリプトを実行します。
2. デバッガコマンド b(reak)で，sample.py の 4 行目にブレークポイントを作成します。
3. デバッガコマンド r(un)で，スクリプトを実行します。

4. ブレークポイントで処理が停止したため，デバッガコマンド s(tep)でスクリプトをステップ実行します。
5. デバッガコマンド cl(ear)で，ブレークポイントを削除します。
6. デバッガコマンド q(uit)で，デバッガを終了します。

(3)　運用コマンド dump script-user-program による確認

運用コマンド dump script-user-program を実行すると，常駐スクリプトで出力される標準エラーを取得できます。ただし，標準出力は取得できません。常駐スクリプトの標準エラー出力を確認する例を次の図に示します。

図 19-7　常駐スクリプトの標準エラー出力例

```
# dump script-user-program                          …1
# cd /usr/var/scriptManager                         …2
# gzip -d smd_script_user.gz                        …3
# cat smd_script_user                               …4
[resident tag 1 info]
**** 20XX/03/19 17:52:36 UTC ****
Script start filename=/usr/var/script/script.file/sample1.py pid=128

**** 20XX/03/19 17:52:36 UTC ****
  File "/usr/var/script/script.file/sample1.py", line 1
    print a
          ^
SyntaxError: invalid syntax

**** 20XX/03/19 17:52:36 UTC ****
Script end filename=/usr/var/script/script.file/sample1.py pid=128
        :
        :
        :
#
```

1. 標準エラーをファイル（smd_script_user.gz）へ出力します。このファイルは，/usr/var/scriptManager/の配下に作成されます。
2. /usr/var/scriptManager/の配下に移動します。
3. smd_script_user.gz を解凍します。
4. 解凍したファイルを表示します。

19.2.5　スクリプトファイルのインストール

スクリプトファイルをインストールします。常駐スクリプトおよびイベント起動スクリプトは，インストールしたスクリプトファイルを起動します。また，インストールしたスクリプトファイルは，Python モジュールとしてインポートできます。

インストールできるスクリプトファイルには，次の条件があります。

- インストールできるスクリプトファイルの拡張子は，次のどれかです。
  - .py
  - .pyc
  - .pyo
- インストール済みのスクリプトファイルと，拡張子だけが異なるスクリプトファイルは，インストールできません。

スクリプトファイルのインストールでの上限値を次の表に示します。

表 19-12　スクリプトファイルのインストールでの上限値

項目	上限値
インストールできるファイル数	100
合計ファイルサイズ	4MB
1 ファイルのサイズ	512KB

スクリプトファイルのインストールには，運用コマンド install script を使用します。install script コマンドを使用して sample.py ファイルをインストールする例を次の図に示します。

図 19-8　スクリプトファイルのインストール

```
# install script sample.py                          …1
# show script installed-file                        …2
Date 20XX/01/15 20:32:35 UTC
Total: 1 files, 100 bytes

name: sample.py
size: 100 bytes
MD5: 12f58123c2b0f4286cf6d607656207c3
#
```

1. sample.py ファイルを本装置にインストールします。
2. 本装置にインストールされているスクリプトファイルを確認します。

19.2.6　スクリプトの起動

作成したスクリプトを，コマンドスクリプト，常駐スクリプト，またはイベント起動スクリプトとして起動します。

(1)　コマンドスクリプトの起動

スクリプトファイル名を指定して運用コマンド python を実行すると，コマンドスクリプトが起動します。

図 19-9　python コマンドの実行例（スクリプトの起動）

```
# python sample.py                                  …1
```

1. sample.py ファイルを起動します。

また，次の図に示すように，インストールしたスクリプトをモジュールとして起動できます。

図 19-10　python コマンドの実行例（モジュールの起動）

```
# install script sample.py                          …1
# python -m sample                                  …2
```

1. sample.py ファイルを本装置にインストールします。
2. sample.py ファイルをモジュールとして起動します。モジュールとして起動する場合は，拡張子を省略します。

(2)　常駐スクリプトの起動

常駐スクリプトを起動するには，次の二つの設定が必要です。

- 本装置へのスクリプトファイルのインストール
- スクリプトファイルの常駐スクリプト登録

両登録の完了を契機として，常駐スクリプトが起動します。常駐スクリプトの設定例を次の図に示します。

図 19-11　常駐スクリプトの設定例

```
# install script sample.py                          …1
# configure
(config)# resident-script 1 python sample.py        …2
(config)#
```

1. sample.py ファイルを本装置にインストールします。
2. sample.py ファイルを常駐スクリプトのスクリプト ID 1 に登録します。登録を契機として，sample.py が起動します。

(3)　イベント起動スクリプトの起動

イベント起動スクリプトを起動するには，次の三つの設定が必要です。

- 本装置へのスクリプトファイルのインストール
- 監視イベントの登録
- イベント検出時に起動するスクリプトファイル名の登録

これらの登録後，監視イベントの検出を契機として，イベント起動スクリプトが起動します。

監視イベントをタイマ監視とする場合の，イベント起動スクリプトの設定例を次の図に示します。

図 19-12　イベント起動スクリプトの設定例（タイマ監視）

```
# install script sample.py                          …1
# configure
(config)# event manager applet INTERVAL100s         …2
(config-applet)# event timer interval 100           …3
(config-applet)# action 1 python sample.py          …4
(config-applet)#
```

1. sample.py ファイルを本装置にインストールします。
2. アプレット名が INTERVAL100s のアプレットを作成して，アプレットのコンフィグレーションモードに移行します。
3. 100 秒周期でイベントを発生させる，タイマ監視を登録します。
4. sample.py ファイルをアクションのシーケンス番号 1 に登録します。登録を契機として，100 秒周期で sample.py が起動します。

監視イベントを運用メッセージ監視とする場合の，イベント起動スクリプトの設定例を次の図に示します。

図 19-13　イベント起動スクリプトの設定例（運用メッセージ監視）

```
# install script sample.py                          …1
# configure
(config)# event manager applet PORT_UP              …2
(config-applet)# event sysmsg message-id 25011001 …3
(config-applet)# action 1 python sample.py          …4
(config-applet)#
07/07 12:00:00 01S E4 PORT GigabitEthernet1/0/1 25011001 1350:000000000000 Port up.
                                                    …5
(config-applet)#
```

1. sample.py ファイルを本装置にインストールします。
2. アプレット名が PORT_UP のアプレットを作成して，アプレットのコンフィグレーションモードに移行します。
3. メッセージ識別子が 25011001 の運用メッセージ出力を監視する，運用メッセージ監視を登録します。

4. sample.py ファイルをアクションのシーケンス番号 1 に登録します。
5. 監視条件（メッセージ識別子 25011001）に該当する運用メッセージの出力を契機として，sample.py が起動します。

(4)　起動スクリプトの PID 確認

起動したスクリプトには，OS によって PID（Process ID）と呼ばれる識別子が割り当てられます。同じスクリプトを複数起動した場合でも，それぞれを区別するために異なる PID が割り当てられます。

各スクリプトに割り当てられた PID は，運用コマンド show script running-state で確認できます。複数の端末から同じスクリプトを起動した場合の PID 表示例を次の図に示します。

図 19-14　起動スクリプトの PID 確認

```
# show script running-state                          …1
Date 20XX/02/05 18:17:40 UTC

[operation command]                                  …2
  command line args: python sample.py
  PID: 2213
  start time: 20XX/02/05 18:17:24 UTC

  command line args: python sample.py
  PID: 1968
  start time: 20XX/02/05 18:17:26 UTC

[applet]                                             …3
  applet name: INTERVAL100s
  action sequence: 1
  command line args: python sample.py
  PID: 11700
  start time: 20XX/02/05 18:17:38 UTC

[resident]                                           …4
  script id: 1
  command line args: python sample.py
  state: Running
  PID: 1977
  start time: 20XX/02/05 18:17:29 UTC
#
```

1. 現在起動中のスクリプトを表示します。
2. コマンドスクリプトとして起動しているスクリプトが確認できます。
   この例では，PID が 2213 と 1968 のスクリプトが起動中であることを確認できます。
3. イベント起動スクリプトとして起動しているスクリプトが確認できます。
   この例では，PID が 11700 のスクリプトが起動中であることを確認できます。
4. 常駐スクリプトとして起動しているスクリプトが確認できます。
   この例では，PID が 1977 のスクリプトが起動中であることを確認できます。

19.3　本装置の Python サポート内容

本装置に実装する Python は，バージョン 3.2.3 です。オリジナルの Python 言語や標準ライブラリの仕様については，Python Software Foundation が公開しているドキュメントや一般書籍などを参照してください。この節では，本装置がサポートする内容について説明します。

19.3.1　標準 Python との差分および制限

本装置の Python サポート内容と，標準 Python との差分および制限を次に示します。

(1)　python コマンド

本装置の運用コマンド python のコマンドラインオプションについて，標準 Python 3.2.3 との差異を次に示します。

- -B オプションは未サポートです。
- -O(OO)オプションは未サポートです。
- -u オプションは未サポートです。
- スクリプトファイルの起動時に適用できるパラメータ数は，最大 32 です。
- スクリプトファイルの起動時に適用できる一つのパラメータの文字数は，最大 63 文字です。
- 指定できる総文字数は，空白文字を含めて最大 1000 文字です。
- スクリプトファイルの起動時に適用できるパラメータには，次の表に示す特殊文字を設定できません。

表 19-13　設定できない特殊文字

文字の名称	文字
ダブルクォート	"
シングルクォート	'
セミコロン	;
バックスラッシュ	¥
逆シングルクォート	`

(2)　__pycache__制限

本装置では，Python からスクリプトをインポートしても，ディレクトリ__pycache__を作成しません。

(3)　ポートの使用制限

Python を使用して特定のポートをバインドする場合は，IPv4 または IPv6 に関係なく，TCP，UDP のどちらもポート番号 49155～49166 を使用してください。

19.3.2　標準ライブラリ

標準ライブラリのサポート内容を次に示します。

(1)　サポートライブラリー覧

本装置が提供する Python の標準ライブラリー覧を次の表に示します。

表 19-14　標準ライブラリー覧

モジュール名				
__future__	_dummy_thread	_thread	abc	aifc
argparse	array	ast	asynchat	asyncore
atexit	audioop	base64	bdb	binascii
binhex	bisect	builtins	cProfile	calendar
cgi	cmath	cmd	code	codecs
collections	colorsys	compileall	concurrent	configparser
contextlib	copy	copyreg	csv	datetime
dbm	decimal	difflib	dis	distutils
doctest	dummy_threading	email	encodings	errno
fcntl	filecmp	fnmatch	fractions	ftplib
functools	gc	getopt	getpass	gettext
glob	hashlib	heapq	hmac	html
http	imaplib	imghdr	imp	importlib
inspect	io	itertools	json	keyword
lib2to3	linecache	locale	logging	macpath
mailbox	marshal	math	mimetypes	mmap
modulefinder	netrc	nntplib	numbers	operator
optparse	os	parser	pdb	pickle
pickletools	pipes	pkgutil	platform	plistlib
poplib	posixpath	pprint	profile	pstats
pty	pwd	py_compile	pyclbr	pydoc
queue	quopri	random	re	rlcompleter
runpy	sched	select	shelve	shlex
shutil	signal	site	smtpd	smtplib
sndhdr	socket	socketserver	stat	string
stringprep	struct	sunau	symtable	sys
sysconfig	tabnanny	tarfile	telnetlib	tempfile
test	textwrap	threading	time	timeit

モジュール名				
token	tokenize	trace	traceback	tty
types	unicodedata	unittest	urllib	uu
uuid	warnings	wave	weakref	webbrowser
wsgiref	xdrlib	xml	xmlrpc	zipfile
zipimport	zlib	-	-	-

（凡例）　-：該当なし

(2)　os モジュール制限

os モジュールが提供する一部の関数には，次に示す制限があります。

- os.kill 制限
  本装置では，Python の os.kill()および os.killpg()を使用して，スクリプト以外にシグナルを送信できません。
- os.fork 制限
  本装置では，Python の os.fork()および os.forkpty()によって，サブプロセスを作成できません。
- os.system 制限
  本装置では，Python の os.system()によるプログラムの実行について，動作を保証しません。プログラムを実行する場合は commandline モジュールを使用してください。

(3)　socketserver モジュール制限

socketserver モジュールが提供する次のクラスは，サポート対象外です。

- ForkingMixIn
- ForkingUDPServer
- ForkingTCPServer

(4)　http.server モジュール制限

http.server モジュールが提供する次のクラスは，サポート対象外です。

- CGIHTTPRequestHandler

(5)　ユーザ制限

標準ライブラリにはスーパーユーザでだけ実行できるライブラリがありますが，本装置ではスーパーユーザでの実行をサポートしません。

19.4　Python 拡張ライブラリの使用方法

本装置は実装する Python に加えて，本装置へのオペレーションを制御するための拡張ライブラリを提供します。この節では，拡張ライブラリの使用方法について説明します。提供するモジュールのメソッドや関数の詳細は，「運用コマンドレファレンス」「19　Python 拡張ライブラリ」を参照してください。

19.4.1　指定コマンド実行の設定

ここでは，commandline モジュールを使用して，指定したコマンドを実行する方法を説明します。

commandline モジュールには，コンフィグレーションコマンドおよび運用コマンドをスクリプトから実行する CommandLine クラスがあります。CommandLine クラスのメソッド一覧を次の表に示します。

表 19-15　CommandLine クラスのメソッド一覧

メソッド名	説明
exec	引数に指定したコマンドを実行します。
exit	該当インスタンスによるコマンド実行を終了します。
set_default_timeout	該当インスタンスによるコマンド実行時のデフォルトタイムアウト時間を設定します。
set_default_logging	該当インスタンスから実行するコマンドのログを，運用コマンド show logging の表示対象とするかどうかのデフォルト値を設定します。

(1)　スクリプトファイルおよび実行結果の例

(a)　さまざまなコマンドを実行する例

さまざまなコマンドを実行するスクリプトファイルの例を次に示します。

図 19-15　スクリプトファイル（sample1.py）記載例

```
# sample1.py
# -*- coding: utf-8 -*-
import extlib.commandline                                          …1
obj = extlib.commandline.CommandLine()                             …2

# デフォルトタイムアウトの指定
obj.set_default_timeout(180)                                       …3

# コマンドログのshow loggingデフォルト非表示指定
obj.set_default_logging(extlib.commandline.DISABLE)                …4

# ユーザ応答なしコマンド（ls）
print("ls start")
dict_ret = obj.exec("ls")                                          …5
if dict_ret['result'] == extlib.commandline.OK:
    print(dict_ret['strings'])                                     …6
else:
    print("timeout.")

# ユーザ応答ありコマンド（file1, file2の削除）
print("rm start")
dict_ret = obj.exec("rm -i file1 file2", ("?","y"), ("?", "y"),
                    logging=extlib.commandline.ENABLE)             …7
if dict_ret['result'] == extlib.commandline.OK:
    print(dict_ret['strings'])                                     …8
else:
    print("timeout.")

# コマンド応答タイムアウト時間指定（pingを3秒間実行）
```

```
print("ping start")
dict_ret = obj.exec("ping 192.0.2.1", 3)                              …9
if dict_ret['result'] == extlib.commandline.TIMEOUT:
    print(dict_ret['strings'])                                        …10
obj.exit()                                                            …11
```

1. モジュールをインポートします。
2. CommandLine クラスのインスタンスを生成します。
3. コマンド応答のデフォルトタイムアウト時間を指定します。
4. コマンドログのデフォルトの show logging 表示設定を非表示にします。
5. exec メソッドで，実行するコマンド（ユーザ応答なし）を指定します。
6. コマンドの実行結果を出力します。
7. exec メソッドで，実行するコマンド（ユーザ応答あり）とコマンドログの show logging 表示設定（表示する）を指定します。
8. コマンドの実行結果を出力します。
9. exec メソッドで，実行するコマンドとコマンド応答のタイムアウト時間を指定します。
10. コマンドの実行結果を出力します。
11. コマンド実行状態を終了します。

スクリプトファイル sample1.py の実行結果を次に示します。exec メソッドで指定した運用コマンド ls, rm，および ping が，正しく実行されています。

図 19-16　スクリプト（sample1.py）実行結果

```
# python sample1.py
ls start
file1 file2

rm start
remove 'file1'? remove 'file2'?
ping start
PING 192.0.2.1 (192.0.2.1): 56 data bytes
64 bytes from 192.0.2.1: icmp_seq=0 ttl=63 time=0.377 ms
64 bytes from 192.0.2.1: icmp_seq=1 ttl=63 time=0.545 ms
64 bytes from 192.0.2.1: icmp_seq=2 ttl=63 time=1.349 ms
64 bytes from 192.0.2.1: icmp_seq=3 ttl=63 time=0.578 ms

----192.0.2.1 PING Statistics----
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.377/0.858/1.385/0.445 ms

#
```

(b)　スクリプト実行中にエラーが発生する例

コマンド応答のタイムアウト時間に，不正な値を指定した例を次に示します。

図 19-17　スクリプトファイル（sample2.py）記載例

```
# sample2.py
# -*- coding: utf-8 -*-
import extlib.commandline                                             …1
obj = extlib.commandline.CommandLine()                                …2

# コマンド応答タイムアウト時間指定（時間に負数を指定）
print("ping start")
dict_ret = obj.exec("ping 192.0.2.1", -3)                             …3
print(dict_ret['strings'])                                            …4

obj.exit()                                                            …5
```

1.モジュールをインポートします。

2.CommandLine クラスのインスタンスを生成します。

3.exec メソッドで，実行するコマンドとコマンド応答のタイムアウト時間（負数）を指定します。

4.コマンドの実行結果を出力します。

5.コマンド実行状態を終了します。

スクリプトファイル sample2.py の実行結果を次に示します。タイムアウト時間に指定した値が正しくないため，エラーになります。

図 19-18　スクリプト（sample2.py）実行結果

```
# python sample2.py
ping start
Traceback (most recent call last):
  File "sample2.py", line 7, in <module>
    dict_ret = obj.exec("ping 192.0.2.1", -3)
  File "/usr/local/lib/python3.2/site-packages/extlib/commandline.py", line 741, in exec
    CNST.ERR_TIMER_INVALID))
ValueError: The timer value is invalid.
#
```

(c)　コマンド実行失敗の例外が発生する例

exec メソッドでコマンド実行失敗の例外が発生したときに，インスタンスを再生成する例を次に示します。

図 19-19　スクリプトファイル（sample3.py）記載例

```
# sample3.py
# -*- coding: utf-8 -*-
import extlib.commandline                                          …1
obj = extlib.commandline.CommandLine()                             …2

retry_cnt = 0

# ユーザ応答なしコマンド（ls）
print("ls start")
while retry_cnt < 3:
    try:
        dict_ret = obj.exec("ls")                                  …3
        if dict_ret['result'] == extlib.commandline.OK:
            print(dict_ret['strings'])                             …4
            print("success!!")
        else:
            print("timeout.")
        break
    except extlib.commandline.ExecuteCommandError:                 …5
        obj.exit()                                                 …6
        obj = extlib.commandline.CommandLine()                     …7
        print("Regenerate the instance")
        retry_cnt = retry_cnt + 1

obj.exit()                                                         …8
```

1.モジュールをインポートします。

2.CommandLine クラスのインスタンスを生成します。

3.exec メソッドで，実行するコマンド（ユーザ応答なし）を指定します。

4.コマンドの実行結果を出力します。

5.exec メソッドでのコマンド実行失敗の例外を捕捉します。

6.コマンド実行状態をいったん終了します。

7.CommandLine クラスのインスタンスを再生成します。

8. コマンド実行状態を終了します。

スクリプトファイル sample3.py の実行結果を次に示します。例外が発生しても，インスタンスを再生成したため，運用コマンド ls が正しく実行されています。

図 19-20　スクリプト（sample3.py）実行結果

```
# python sample3.py
ls start
Regenerate the instance
file1 file2

success!!
#
```

(2)　インスタンス生成

CommandLine クラスのインスタンスは，一つのプロセスに対して複数生成できません。インスタンスを再生成するときは，先に，既存のインスタンスに対して exit メソッドを呼び出してください。

(3)　exec メソッドでのコマンド実行

commandline モジュールの exec メソッドを使用してコマンドを実行する場合，スクリプト専用ユーザ（ユーザ名 script）によって該当コマンドが実行されます。exec メソッドを使用したコマンド実行について次の表に示します。

表 19-16　exec メソッドを使用したコマンド実行

項目	説明
初期コマンド入力モード	一般ユーザモード
無効コマンド	スクリプト専用ユーザでは，次に示す運用コマンドの実行による設定変更は無効となります。 • set exec-timeout • set terminal pager また，スクリプト専用ユーザに対する次のコンフィグレーションコマンドは無効となります。 • username コマンドの logging-console パラメータ • username コマンドの exec-timeout パラメータ • username コマンドの terminal-pager パラメータ

(4)　コマンド承認

本装置にコマンド承認を設定している場合，スクリプトから実行するコマンドにもコマンド承認が適用されます。

スクリプトから実行するコマンドは，コンフィグレーションコマンド aaa authorization commands script の username パラメータで指定したユーザ名の権限で承認されます。なお，bypass パラメータを指定すると，コマンド承認をしないで無条件にコマンドを実行できます。

コマンド承認についての特記事項を次に示します。

- aaa authorization commands script コマンドだけを設定しても，コマンド承認はしません。aaa authorization commands コマンドをあわせて設定してください。ただし，RADIUS サーバによるコ

マンド承認はサポートしないため，TACACS+サーバまたはローカルによるコマンド承認の設定が必要です。

- コンソール（RS232C）で接続した運用端末からスクリプトを起動してコマンドを実行した場合のコマンド承認は，aaa authorization commands console コマンドの設定に従います。

  aaa authorization commands console コマンドの設定がある場合

  コマンド承認の対象となります。ただし，bypass パラメータが設定されている場合は，コマンド承認をしないですべてのコマンドが実行できます。

  aaa authorization commands console コマンドの設定がない場合

  コマンド承認をしません。すべてのコマンドが実行できます。

- aaa authorization commands コマンドの設定があり，コマンド承認情報（コマンドクラスまたはコマンドリスト）を取得できなかった場合は，すべてのコマンドが実行できません。コマンド承認情報を取得できない例を次に示します。
  - aaa authorization commands script コマンドの設定がない
  - 指定したユーザ名が，TACACS+サーバまたはローカルに存在しない
  - TACACS+サーバにアクセスできない
- コマンド承認情報（コマンドクラスまたはコマンドリスト）は，CommandLine クラスのインスタンス生成時に取得します。
- コマンド承認を設定している場合，Python 標準ライブラリの os.system()などによるプログラムの起動についても，起動制限の対象となります。プログラムを起動できるのは，次に示す場合だけです。
  - aaa authorization commands コマンドの設定がない場合
  - aaa authorization commands コマンドの設定があり，aaa authorization commands script コマンドの bypass パラメータの設定がある場合
  - aaa authorization commands コマンドの設定があり，aaa authorization commands console コマンドの設定がなく，コンソール（RS232C）で接続した運用端末から起動したスクリプトでプログラムを起動する場合

19.4.2　運用メッセージ出力の設定

ここでは，sysmsg モジュールを使用して，指定した文字列を運用メッセージとして出力する方法を説明します。

sysmsg モジュールの関数一覧を次の表に示します。

表 19-17　sysmsg モジュールの関数一覧

関数名	説明
send	運用メッセージを出力します。

(1)　スクリプトファイルおよび実行結果の例

運用メッセージを出力するスクリプトファイルの例を次に示します。

図 19-21　スクリプトファイル（test1.py）記載例

```
# test1.py
# -*- coding: utf-8 -*-
import sys
import extlib.sysmsg                                                    …1
```

```
try:
    extlib.sysmsg.send(”E3”, 0xfedc, 0xba9876543210,”Script Start!!”) …2
    print(”send success.”)
except extlib.sysmsg.MsgSendError:                                    …3
    print(”send failed.”)
    sys.exit()
```

1. モジュールをインポートします。
2. 出力する運用メッセージを，次のように指定します。
   - イベントレベル E3
   - メッセージ識別子 3e03fedc
   - 付加情報 ba9876543210
   - メッセージテキスト“Script Start!!”
3. 運用メッセージ出力失敗の例外を捕捉します。

スクリプトファイル test1.py の実行結果および運用メッセージの出力例を次に示します。

図 19-22　スクリプト（test1.py）実行結果

```
# python test1.py
send success.
#
```

図 19-23　運用メッセージ出力例

```
EVT 07/07 12:00:00 01S E3 SCRIPT 3e03fedc 2600:ba9876543210 Script Start!!
```

19.4.3　イベント監視機能の設定

ここでは，eventmonitor モジュールを使用して，イベントを登録，削除，および受信する方法を説明します。

eventmonitor モジュールは，装置やネットワークの状態などの監視と連携して，監視対象の状態変化（イベント）を起動中のスクリプトに通知する機能をサポートします。イベント監視機能に関連する関数一覧を次の表に示します。

表 19-18　イベント監視機能に関連する関数一覧

機能種別	関数名	説明
イベント登録	regist_sysmsg	監視する運用メッセージを登録します。
	regist_cron_timer	cron タイマを登録します。
	regist_interval_timer	interval タイマを登録します。
イベント削除	event_delete	登録したイベントを削除します。
イベント受信	event_receive	イベントが発生したときにイベントを受信します。

(1)　スクリプトファイルの例

(a)　運用メッセージをイベントとして監視する例

運用メッセージをイベントとして監視する，イベントの登録例を次に示します。

図 19-24　スクリプト記載例 1

```
import sys
import extlib.eventmonitor                                                    …1

try:
    event_sysmsg=extlib.eventmonitor.regist_sysmsg(event_level="E7",
    message_id=0xabcd1234,message_text="(Error|error)")                       …2
except Exception as e:                                                        …3
    print('ERROR!! regist_sysmsg()',e)
    sys.exit()

while 1:
    dict = extlib.eventmonitor.event_receive(extlib.eventmonitor.BLOCK_ON, 0)  …4

    if dict['event_id']== event_sysmsg:                                       …5
        print('EVENT OCCURRED!!')
```

1.モジュールをインポートします。

2.イベントを登録します。次の条件を満たす運用メッセージの出力を監視します。

- イベントレベル E7
- メッセージ識別子 abcd1234
- メッセージテキストに文字列“Error”または“error”を含む

3.イベントが登録されたかどうか確認します。登録に失敗した場合，ログを出力して終了します。

4.イベント受信関数を呼び出します。

5.戻り値を参照して，意図した値かどうか確認します。

(b)　cron タイマによってイベントを監視する例

cron タイマによってイベントを監視する，イベントの登録例を次に示します。

図 19-25　スクリプト記載例 2

```
import sys
import extlib.eventmonitor                                                    …1

try:
    event_cron_timer = extlib.eventmonitor.regist_cron_timer('0 23 * * *')    …2
except Exception as e:                                                        …3
    print('ERROR!! regist_cron_timer ()',e)
    sys.exit()

while 1:
    dict = extlib.eventmonitor.event_receive(extlib.eventmonitor.BLOCK_ON, 0)  …4

    if dict['event_id']== event_cron_timer:                                   …5
        print('EVENT OCCURRED!!')
```

1.モジュールをインポートします。

2.毎日 23 時に発生するイベントを登録します。

3.イベントが登録されたかどうか確認します。登録に失敗した場合，ログを出力して終了します。

4.イベント受信関数を呼び出します。

5.戻り値を参照して，意図した値かどうか確認します。

(c)　interval タイマによってイベントを監視する例

interval タイマによってイベントを監視する，イベントの登録例を次に示します。

図 19-26　スクリプト記載例 3

```
import sys
import extlib.eventmonitor                                                    …1

try:
    event_interval_timer = extlib.eventmonitor.regist_interval_timer(1800)    …2
except Exception as e:                                                        …3
    print('ERROR!! regist_interval_timer()',e)
    sys.exit()

while 1:
    dict = extlib.eventmonitor.event_receive(extlib.eventmonitor.BLOCK_ON, 0)  …4

    if dict['event_id']== event_interval_timer:                               …5
        print('EVENT OCCURRED!!')
```

1.モジュールをインポートします。

2.1800 秒ごとに発生するイベントを登録します。

3.イベントが登録されたかどうか確認します。登録に失敗した場合，ログを出力して終了します。

4.イベント受信関数を呼び出します。

5.戻り値を参照して，意図した値かどうか確認します。

(d)　登録したイベントを削除する例

登録したイベントを削除する例を次に示します。

図 19-27　スクリプト記載例 4

```
import sys
import extlib.eventmonitor                                                    …1

try:
    event_cron_timer = extlib.eventmonitor.regist_cron_timer('0 23 * * *')    …2
except Exception as e:                                                        …3
    print('ERROR!! regist_cron_timer ()',e)
    sys.exit()

try:
    result_dict = extlib.eventmonitor.event_delete(event_cron_timer)          …4
    print('EVENT DELETE!!')
except:                                                                       …5
    print('ERROR!! event_delete()')
```

1.モジュールをインポートします。

2.イベントを登録します。

3.イベントが登録されたかどうか確認します。登録に失敗した場合，ログを出力して終了します。

4.登録したイベントの監視イベント ID を指定して，監視を停止します。

5.停止に失敗した場合，ログを出力します。

(e)　イベントを受信する例

イベントを受信する例を次に示します。

図 19-28　スクリプト記載例 5

```
import sys
import extlib.eventmonitor                                                    …1

try:
    event_cron_timer = extlib.eventmonitor.regist_cron_timer('0 23 * * *')    …2
except Exception as e:                                                        …3
    print('ERROR!!  event_cron_timer()',e)
```

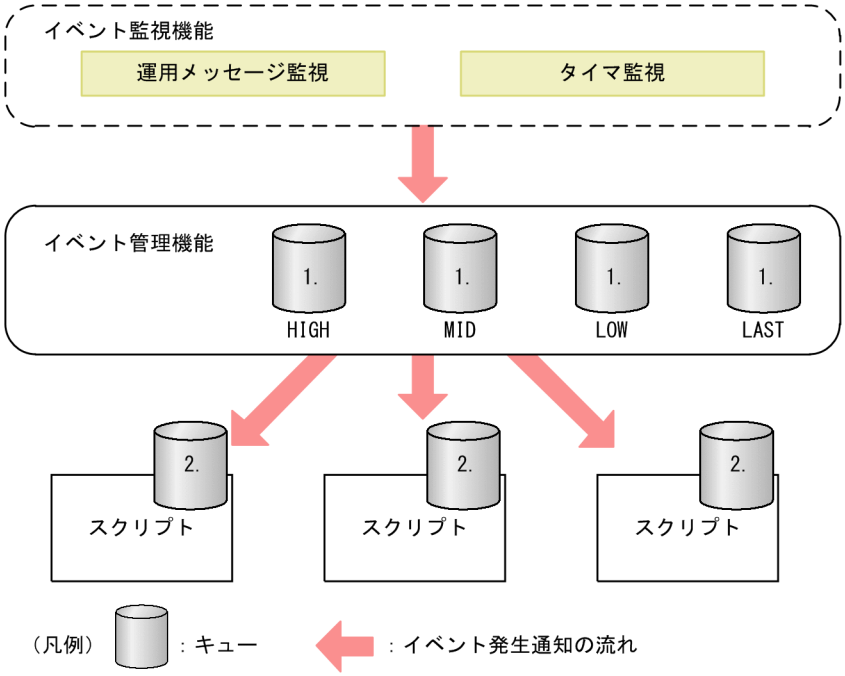
```
    sys.exit()
dict = extlib.eventmonitor.event_receive(extlib.eventmonitor.BLOCK_ON , 0)       …4
if dict['event_id']== event_cron_timer:                                          …5
    print('EVENT OCCURRED!!')
```

1. モジュールをインポートします。
2. イベントを登録します。
3. イベントが登録されたかどうか確認します。登録に失敗した場合，ログを出力して終了します。
4. イベント受信関数を呼び出します。受信タイムアウトなしのブロッキングモードで受信します。
5. 戻り値を参照して，意図した値かどうか確認します。

(2)　通知情報の廃棄

監視イベントの発生頻度が高い場合，イベント発生通知がスクリプトに通知される前に廃棄されることがあります。イベント発生通知の流れを次の図に示します。図中の 1.および 2.の通知受信キューが満杯になると，廃棄が発生します。

図 19-29　イベント発生通知の流れ



1. キューあふれ閾値は，優先度ごとに 1024 メッセージ
2. キューあふれ閾値は，スクリプトごとに 1024 メッセージ

なお，廃棄の発生有無は，運用コマンド show event manager monitor で表示されるイベント廃棄回数（discard）で確認できます。

19.4.4　スクリプト起動契機の取得

ここでは，eventmonitor モジュールの get_exec_trigger()関数を使用して，動作中のスクリプトから，自身が起動した要因（イベント起動スクリプトの場合は発生イベント）を取得する方法を説明します。

(1)　スクリプトファイルの例

イベント起動スクリプトの起動要因（発生イベント）を取得するスクリプトファイルの例を次に示します。

図 19-30　スクリプトファイル記載例

```
import sys
import extlib.eventmonitor                                          …1
dict = extlib.eventmonitor.get_exec_trigger ()                      …2

if dict['type'] == extlib.eventmonitor.APPLET :                     …3
# アプレット
    if dict['applet']['type'] == extlib.eventmonitor.TIMER_EVT :    …4
    # タイマイベント

        if dict['applet']['condition'][extlib.eventmonitor.TIMER_TYPE] == ¥
            extlib.eventmonitor.CRON :
        # cronタイマ

            # cron監視条件の文字列を表示
            print("[condition]",file=sys.stderr)
            print(dict['applet']['condition'][extlib.eventmonitor.CRON],file=sys.stderr)

        elif dict['applet']['condition'][extlib.eventmonitor.TIMER_TYPE] == ¥
            extlib.eventmonitor.INTERVAL :
        # intervalタイマ

            # interval監視条件の文字列を表示
            print("[condition]",file=sys.stderr)
            print(dict['applet']['condition'][extlib.eventmonitor.INTERVAL],
                file=sys.stderr)

    elif dict['applet']['type'] == extlib.eventmonitor.SYSMSG_EVT :  …5
    # 運用メッセージイベント

        ## 運用メッセージ監視条件の表示
        print("[condition]",file=sys.stderr)
        ## イベントレベル
        print("SYSMSG_EVENT_LEVEL:" + str(dict['applet']['condition']
            [extlib.eventmonitor.SYSMSG_EVENT_LEVEL]),file=sys.stderr)

        ## イベント発生要因の運用メッセージを表示
        print("[trigger system message]",file=sys.stderr)
        ## 発生時刻
        print("SYSMSG_TIME:" + dict['applet']['trigger']
            [extlib.eventmonitor.SYSMSG_TIME],file=sys.stderr)
        ## メッセージ識別子
        print("SYSMSG_MSG_ID:" + str(hex(dict['applet']['trigger']
            [extlib.eventmonitor.SYSMSG_MSG_ID])),file=sys.stderr)

sys.exit()
```

1. モジュールをインポートします。
2. 起動要因（発生イベント）を取得する関数を呼び出します。
3. スクリプトの起動要因がアプレット機能（イベント起動スクリプト）かどうか判定します。
4. 起動要因がタイマ監視の場合の監視条件を取得します。
5. 起動要因が運用メッセージ監視の場合の監視条件，および起動要因となった運用メッセージの情報を取得します。

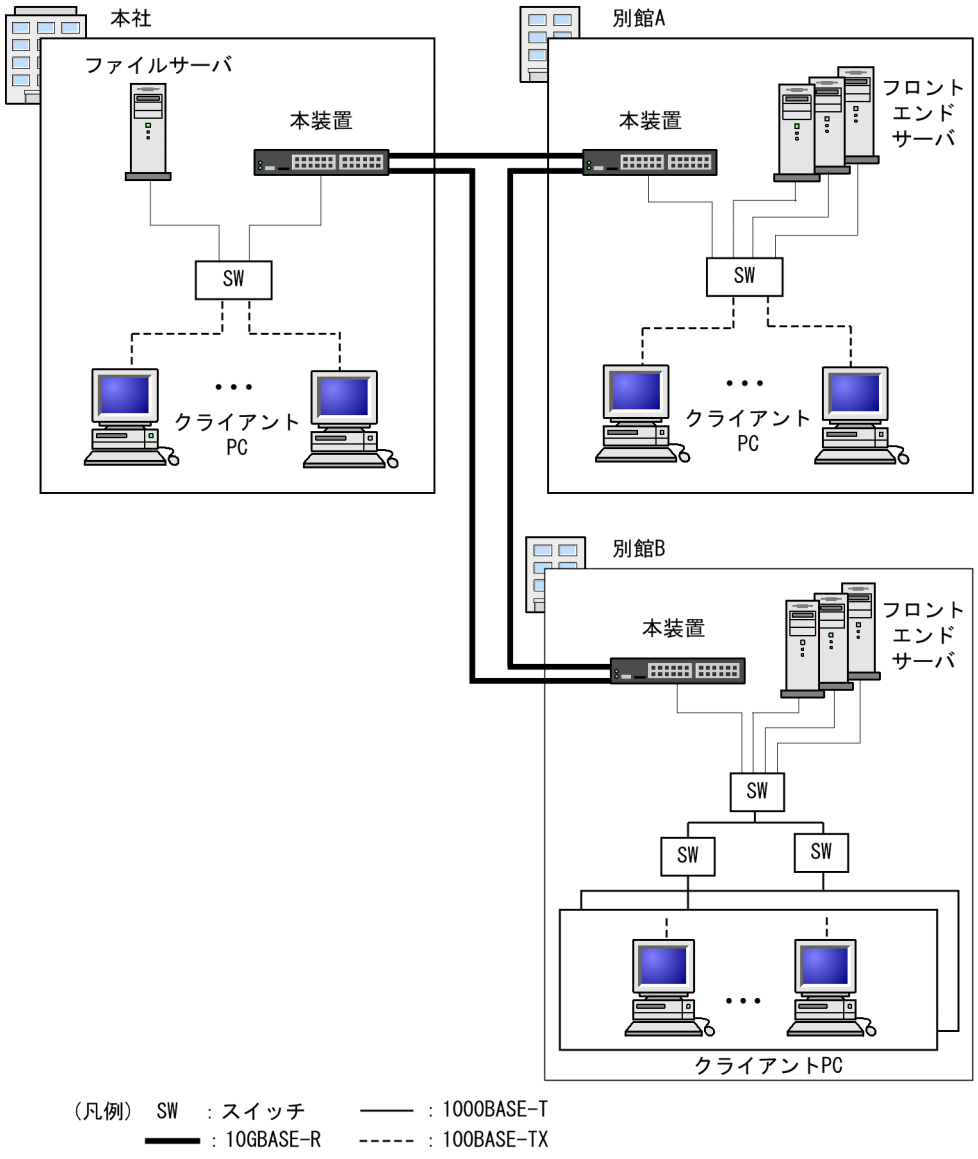
20 イーサネット

この章では，本装置のイーサネットについて説明します。

20.1　接続インタフェースの解説

本装置を使用した代表的なイーサネットの構成例を次の図に示します。各ビル間，サーバ間を 10GBASE-R で接続することによって，10BASE-T/100BASE-TX/1000BASE-T および 1000BASE-X よりもサーバ間のパフォーマンスが向上します。

図 20-1　イーサネットの構成例



20.1.1　ポートの種類とサポート機能

(1)　ポートの種類

ポートの種類と，ポートごとにサポートするイーサネット規格を次の表に示します。

表 20-1　ポートの種類とサポートするイーサネット規格

ポートの種類	イーサネット規格
10BASE-T/100BASE-TX/1000BASE-T ポート	10BASE-T，100BASE-TX，1000BASE-T
100BASE-TX/1000BASE-T/2.5GBASE-T ポート	100BASE-TX，1000BASE-T，2.5GBASE-T
SFP ポート	1000BASE-T，1000BASE-X
SFP+/SFP 共用ポート	1000BASE-T，1000BASE-X，10GBASE-R

(a)　10BASE-T/100BASE-TX/1000BASE-T ポート

10BASE-T／100BASE-TX／1000BASE-T のツイストペアケーブル（UTP）を使用します。

(b)　100BASE-TX/1000BASE-T/2.5GBASE-T ポート

100BASE-TX／1000BASE-T／2.5GBASE-T のツイストペアケーブル（UTP）を使用します。

(c)　SFP ポート

1000BASE-SX，1000BASE-LX，1000BASE-LH，および 1000BASE-BX の SFP をサポートしています。

1000BASE-T で接続する場合，SFP-T を使用します。

(d)　SFP+/SFP 共用ポート

1000BASE-T で接続する場合，SFP-T を使用します。

1000BASE-X で接続する場合，1000BASE-SX，1000BASE-LX，1000BASE-LH，および 1000BASE-BX の SFP をサポートしています。

10GBASE-R で接続する場合，10GBASE-SR，10GBASE-LR，10GBASE-ER，および 10GBASE-BR の SFP+をサポートしています。本製品では，10GBASE-CU のダイレクトアタッチケーブルは将来サポートする予定です。

(2)　接続モードとサポート機能

接続インタフェースごとの接続モードとサポート機能を次の表に示します。

表 20-2　接続インタフェースごとの接続モードとサポート機能

接続インタフェース	接続モード	サポート機能
10BASE-T	• 半二重固定 • 全二重固定 • 半二重または全二重のオートネゴシエーション	• 自動 MDI/MDIX 機能 • フローコントロール
100BASE-TX	• 半二重固定 • 全二重固定 • 半二重または全二重のオートネゴシエーション	• 自動 MDI/MDIX 機能 • フローコントロール • ジャンボフレーム
1000BASE-T	• 全二重のオートネゴシエーション	• 自動 MDI/MDIX 機能 • フローコントロール • ジャンボフレーム

接続インタフェース	接続モード	サポート機能
2.5GBASE-T	• 全二重のオートネゴシエーション	• 自動 MDI/MDIX 機能 • フローコントロール • ジャンボフレーム
1000BASE-X	• 全二重固定 • 全二重のオートネゴシエーション	• フローコントロール • ジャンボフレーム
10GBASE-R	• 全二重固定	• フローコントロール • ジャンボフレーム

20.1.2　10BASE-T/100BASE-TX/1000BASE-T/2.5GBASE-T

10BASE-T／100BASE-TX／1000BASE-T／2.5GBASE-T のツイストペアケーブル（UTP）を使用したインタフェースについて説明します。

(1)　接続インタフェース

10BASE-T，100BASE-TX，1000BASE-T，および 2.5GBASE-T では，オートネゴシエーションをサポートしています。オートネゴシエーションは，伝送速度，全二重／半二重，およびフローコントロールについて，相手装置とやりとりをして装置間で最適な接続動作を決定する機能です。本装置では，オートネゴシエーションで解決できなかった場合，リンク接続されるまで接続動作を繰り返します。

1000BASE-T および 2.5GBASE-T では，オートネゴシエーションによる全二重接続だけをサポートしています。

10BASE-T および 100BASE-TX では，オートネゴシエーションのほかに全二重／半二重固定接続をサポートしています。

コンフィグレーションでは次のモードを指定できます。接続するネットワークに合わせて設定してください。本装置のデフォルト値は，オートネゴシエーションとなります。

- オートネゴシエーション
- 100BASE-TX 全二重固定
- 100BASE-TX 半二重固定
- 10BASE-T 全二重固定
- 10BASE-T 半二重固定

(2)　接続仕様

本装置のコンフィグレーションでの指定値と相手装置の伝送速度および，全二重および半二重モードの接続仕様を次に示します。

10BASE-T および 100BASE-TX は，相手装置によってオートネゴシエーションでは接続できない場合があるため，できるだけ相手装置のインタフェースに合わせた固定設定にしてください。

10BASE-T/100BASE-TX/1000BASE-T ポートの接続仕様を次の表に示します。

表 20–3　接続仕様（10BASE-T/100BASE-TX/1000BASE-T）

相手装置		本装置の設定				
設定	インタフェース	固定				オート ネゴシエーション
		10BASE-T 半二重	10BASE-T 全二重	100BASE-TX 半二重	100BASE-TX 全二重	
固定	10BASE-T 半二重	10BASE-T 半二重	×	×	×	10BASE-T 半二重
	10BASE-T 全二重	×	10BASE-T 全二重	×	×	×
	100BASE-TX 半二重	×	×	100BASE-TX 半二重	×	100BASE-TX 半二重
	100BASE-TX 全二重	×	×	×	100BASE-TX 全二重	×
	1000BASE-T 半二重	×	×	×	×	×
	1000BASE-T 全二重	×	×	×	×	×
オート ネゴシエーション	10BASE-T 半二重	10BASE-T 半二重	×	×	×	10BASE-T 半二重
	10BASE-T 全二重	×	×	×	×	10BASE-T 全二重
	10BASE-T 全二重および半二重	10BASE-T 半二重	×	×	×	10BASE-T 全二重
	100BASE-TX 半二重	×	×	100BASE-TX 半二重	×	100BASE-TX 半二重
	100BASE-TX 全二重	×	×	×	×	100BASE-TX 全二重
	100BASE-TX 全二重および半二重	×	×	100BASE-TX 半二重	×	100BASE-TX 全二重
	10BASE-T/ 100BASE-TX 全二重および半二重	10BASE-T 半二重	×	100BASE-TX 半二重	×	100BASE-TX 全二重
	1000BASE-T 半二重	×	×	×	×	×
	1000BASE-T	×	×	×	×	1000BASE-T

相手装置		本装置の設定				
設定	インタフェース	固定				オート ネゴシエーション
		10BASE-T 半二重	10BASE-T 全二重	100BASE-TX 半二重	100BASE-TX 全二重	
	全二重					全二重
	1000BASE-T 全二重および半二重	×	×	×	×	1000BASE-T 全二重
	10BASE-T/ 100BASE-TX/ 1000BASE-T 全二重および半二重	10BASE-T 半二重	×	100BASE-TX 半二重	×	1000BASE-T 全二重

（凡例） ×：接続できない

100BASE-TX/1000BASE-T/2.5GBASE-T ポートの接続仕様を次の表に示します。

表 20–4 接続仕様（100BASE-TX/1000BASE-T/2.5GBASE-T）

相手装置		本装置の設定		
設定	インタフェース	固定		オート ネゴシエーション
		100BASE-TX 半二重	100BASE-TX 全二重	
固定	100BASE-TX 半二重	100BASE-TX 半二重	×	100BASE-TX 半二重
	100BASE-TX 全二重	×	100BASE-TX 全二重	×
	1000BASE-T 半二重	×	×	×
	1000BASE-T 全二重	×	×	×
	2.5GBASE-T 半二重	×	×	×
	2.5GBASE-T 全二重	×	×	×
オート ネゴシ エーション	100BASE-TX 半二重	100BASE-TX 半二重	×	100BASE-TX 半二重
	100BASE-TX 全二重	×	×	100BASE-TX 全二重
	100BASE-TX 全二重および半二重	100BASE-TX 半二重	×	100BASE-TX 全二重

相手装置		本装置の設定		
設定	インタフェース	固定		オート ネゴシエーション
		100BASE-TX 半二重	100BASE-TX 全二重	
	1000BASE-T 半二重	×	×	×
	1000BASE-T 全二重	×	×	1000BASE-T 全二重
	1000BASE-T 全二重および半二重	×	×	1000BASE-T 全二重
	10BASE-T/ 100BASE-TX/ 1000BASE-T 全二 重および半二重	100BASE-TX 半二重	×	1000BASE-T 全二重
	100BASE-TX/ 1000BASE-T 全二重および半二重	100BASE-TX 半二重	×	1000BASE-T 全二重
	2.5GBASE-T 半二重	×	×	×
	2.5GBASE-T 全二重	×	×	2.5GBASE-T 全二重
	2.5GBASE-T 全二重および半二重	×	×	2.5GBASE-T 全二重
	1000BASE-T/ 2.5GBASE-T 全二重および半二重	×	×	2.5GBASE-T 全二重
	100BASE-TX/ 1000BASE-T/ 2.5GBASE-T 全二重および半二重	100BASE-TX 半二重	×	2.5GBASE-T 全二重

（凡例）　×：接続できない

SFP ポートおよび SFP+/SFP 共用ポートで SFP-T を使用した場合の接続仕様を次の表に示します。

表 20-5　接続仕様（SFP ポートおよび SFP+/SFP 共用ポートで SFP-T を使用）

相手装置		本装置の設定
設定	インタフェース	オートネゴシエーション
固定	10BASE-T 半二重	×
	10BASE-T 全二重	×
	100BASE-TX 半二重	×

相手装置		本装置の設定
設定	インタフェース	オートネゴシエーション
	100BASE-TX 全二重	×
	1000BASE-T 半二重	×
	1000BASE-T 全二重	×
オートネゴシエーション	10BASE-T 半二重	×
	10BASE-T 全二重	×
	10BASE-T 全二重および半二重	×
	100BASE-TX 半二重	×
	100BASE-TX 全二重	×
	100BASE-TX 全二重および半二重	×
	10BASE-T/100BASE-TX 全二重および半二重	×
	1000BASE-T 半二重	×
	1000BASE-T 全二重	1000BASE-T 全二重
	1000BASE-T 全二重および半二重	1000BASE-T 全二重
	10BASE-T/100BASE-TX/1000BASE-T 全二重および半二重	1000BASE-T 全二重

（凡例）　×：接続できない

(3)　自動 MDI/MDIX 機能

自動 MDI/MDIX 機能は，MDI と MDI-X を自動的に切り替える機能です。これによって，クロスケーブルまたはストレートケーブルどちらでも通信できるようになります。オートネゴシエーション時だけサポートします。全二重固定時は MDI-X となります。MDI／MDI-X のピンマッピングを次の表に示します。

表 20-6　MDI／MDI-X のピンマッピング

RJ45 Pin No.	MDI			MDI-X		
	1000BASE-T 2.5GBASE-T ※1	100BASE-TX※2	10BASE-T ※2	1000BASE-T 2.5GBASE-T ※1	100BASE-TX※2	10BASE-T ※2
1	BI_DA ＋	TD ＋	TD ＋	BI_DB ＋	RD ＋	RD ＋
2	BI_DA−	TD−	TD−	BI_DB−	RD−	RD−
3	BI_DB ＋	RD ＋	RD ＋	BI_DA ＋	TD ＋	TD ＋
4	BI_DC ＋	Unused	Unused	BI_DD ＋	Unused	Unused
5	BI_DC−	Unused	Unused	BI_DD−	Unused	Unused

RJ45 Pin No.	MDI			MDI-X		
	1000BASE-T 2.5GBASE-T ※1	100BASE-TX※2	10BASE-T ※2	1000BASE-T 2.5GBASE-T ※1	100BASE-TX※2	10BASE-T ※2
6	BI_DB−	RD−	RD−	BI_DA−	TD−	TD−
7	BI_DD ＋	Unused	Unused	BI_DC ＋	Unused	Unused
8	BI_DD−	Unused	Unused	BI_DC−	Unused	Unused

注※1

1000BASE-T および 2.5GBASE-T では，8 ピンすべてを送信と受信が同時双方向（bi-direction）通信するため，信号名表記が異なります（BI_Dx：双方向データ信号）。

注※2

10BASE-T と 100BASE-TX では，送信（TD）と受信（RD）信号は別々の信号線を使用しています。

(4)　ダウンシフト機能

ダウンシフト機能は，オートネゴシエーション設定時に機能し，オートネゴシエーションで決定された最適な接続動作（最も速い回線速度）でリンク接続ができなかった場合（例えば，オートネゴシエーションでは 1000BASE-T が最適な接続動作と決定したが，伝送品質の劣化などによって 1000Mbit/s でリンク接続できないなど）に，オートネゴシエーションで広告する最も速い速度を無効に設定し，次に速い速度でリンク接続を試みる機能です。

(a)　回線速度の変更順序

オートネゴシエーション完了後にリンク接続できない場合，オートネゴシエーションで広告する回線速度を，フェーズ 1，フェーズ 2，…の順に下げていきます。回線速度が最低になってもリンク接続できない場合は，フェーズ 1 に戻ってダウンシフトを繰り返します。回線速度の変更順序を，ポートの種類ごとに次の表に示します。

表 20–7　回線速度の変更順序（10BASE-T/100BASE-TX/1000BASE-T ポート）

フェーズ	コンフィグレーションコマンド speed のパラメータ設定内容※1			
	auto	auto 10 100 1000	auto 10 100	auto 1000※2 or auto 100※2 or auto 10※2
1	10 100 1000	10 100 1000	10 100	−
2	10 100	10 100	10	−
3	10	10	−	−

（凡例）　−：ダウンシフト動作をしない

注※1　数値は回線速度を示します。単位は Mbit/s です。

注※2　ダウンシフト動作をさせたくない場合は，この設定をしてください。

表 20-8　回線速度の変更順序（100BASE-TX/1000BASE-T/2.5GBASE-T ポート）

フェーズ	コンフィグレーションコマンド speed のパラメータ設定内容※1			
	auto or auto 100 1000 2500※2	auto 100 1000※2	auto 1000 2500	auto 2500※3 or auto 1000※3 or auto 100※3
1	1000 2500	1000	1000 2500	－
2	1000	－	1000	－

（凡例）　－：ダウンシフト動作をしない

注※1　数値は回線速度を示します。単位は Mbit/s です。

注※2　100Mbit/s へのダウンシフトは未サポートです。

注※3　ダウンシフト動作をさせたくない場合は，この設定をしてください。

(5)　接続時の注意事項

- 伝送速度，および全二重および半二重モードが相手装置と不一致の場合，接続できないので注意してください。

  不一致の状態で通信を行うと，以降の通信が停止することがあります。この場合，当該ポートに対して inactivate コマンド，activate コマンドを実行してください。
- 使用するケーブルについては，「ハードウェア取扱説明書」を参照してください。
- 全二重インタフェースはコリジョン検出とループバック機能を行わないことによって実現しています。このため，10BASE-T または 100BASE-TX を全二重インタフェース設定で使用する場合，相手接続ポートは必ず全二重インタフェースに設定して接続してください。

20.1.3　1000BASE-X

1000BASE-X の光ファイバを使用したインタフェースについて説明します。

(1)　接続インタフェース

1000BASE-SX，1000BASE-LX，1000BASE-LH，および 1000BASE-BX をサポートしています。回線速度は 1000Mbit/s 全二重固定です。

1000BASE-SX

短距離間を接続するために使用します（マルチモード，最大 550m）。

1000BASE-LX

中距離間を接続するために使用します（シングルモード，最大 5km／マルチモード，最大 550m）。

1000BASE-LH

長距離間を接続するために使用します（シングルモード，最大 70km）。

1000BASE-BX

送受信で波長の異なる光を使用することで，1 芯の光ファイバを使い，光ファイバのコストを抑えることができます。

送受信で異なる波長の光を使用するため，アップ側とダウン側で 1 対となるトランシーバを使用します。

本装置では，IEEE802.3ah で規定されている 1000BASE-BX10-D/1000BASE-BX10-U と，独自規格の 1000BASE-BX40-D/1000BASE-BX40-U をサポートします。

1000BASE-BX10-D/1000BASE-BX10-U

中距離間を接続するために使用します（シングルモード，最大 10km）。

1000BASE-BX40-D/1000BASE-BX40-U

長距離間を接続するために使用します（シングルモード，最大 40km）。

コンフィグレーションでは次のモードを指定できます。接続するネットワークに合わせて設定してください。本装置のデフォルト値は，オートネゴシエーションになります。

- オートネゴシエーション
- 1000BASE-X 全二重固定

オートネゴシエーションは，全二重およびフローコントロールについて，相手装置とやりとりをして装置間で最適な接続動作を決定する機能です。本装置では，オートネゴシエーションで解決できなかった場合，リンク接続されるまで接続動作を繰り返します。

(2)　接続仕様

本装置のコンフィグレーションでの指定値と相手装置の伝送速度および，全二重および半二重モードの接続仕様を次の表に示します。なお，1000BASE-X の物理仕様については，「ハードウェア取扱説明書」を参照してください。

表 20-9　接続仕様

相手装置		本装置の設定	
設定	インタフェース	固定	オートネゴシエーション
		1000BASE 全二重	1000BASE 全二重
固定	1000BASE 半二重	×	×
	1000BASE 全二重	1000BASE 全二重	×
オート ネゴシエーション	1000BASE 半二重	×	×
	1000BASE 全二重	×	1000BASE 全二重

（凡例）　×：接続できない

(3)　接続時の注意事項

- 相手装置（スイッチングハブなど）をオートネゴシエーションまたは全二重固定に設定してください。
- 「ハードウェア取扱説明書」に示すトランシーバ以外を使用した場合の動作は保証できません。

20.1.4　10GBASE-R

10GBASE-R の光ファイバを使用したインタフェースについて説明します。

(1)　接続インタフェース

10GBASE-SR，10GBASE-LR，10GBASE-ER および 10GBASE-BR をサポートしています。回線速度は 10Gbit/s 全二重固定です。

10GBASE-SR

短距離間を接続するために使用します（マルチモード，伝送距離：最大 300m※）。

注※

伝送距離は使用するケーブルによって異なります。ケーブルごとの伝送距離は，「ハードウェア取扱説明書」を参照してください。

10GBASE-LR

中距離間を接続するために使用します（シングルモード，伝送距離：最大 10km）。

10GBASE-ER

長距離間を接続するために使用します（シングルモード，伝送距離：最大 40km）。

10GBASE-BR

1000BASE-BX と同様に送受信で波長の異なる光を使用することで，1 芯の光ファイバで双方向の通信ができます。そのため，光ファイバのコストを抑えられます。

送受信で異なる波長の光を使用するため，アップ側とダウン側で 1 対となるトランシーバを使用します。

10GBASE-BR10-D/10GBASE-BR10-U

中距離間を接続するために使用します（シングルモード，最大 10km）。

10GBASE-BR40-D/10GBASE-BR40-U

長距離間を接続するために使用します（シングルモード，最大 40km）。

(2) 接続仕様

本装置の物理仕様については，「ハードウェア取扱説明書」を参照してください。

(3) 接続時の注意事項

- 「ハードウェア取扱説明書」に示すトランシーバ以外を使用した場合の動作は保証できません。
- 10GBASE-BR および 10GBASE-ZR はベンダー独自仕様のため，他ベンダーの装置と接続した場合の動作は保証できません。
- ダイレクトアタッチケーブル使用時は，リンクアップまでに 5～8 秒掛かります。

20.2　イーサネット共通の解説

20.2.1　フローコントロール

フローコントロールは，装置内の受信バッファ枯渇でフレームを廃棄しないように，相手装置にフレームの送信をポーズパケットによって，一時的に停止指示する機能です。自装置がポーズパケット受信時は，送信規制を行います。この機能は全二重だけサポートします。

(1)　フローコントロールの設定と動作

本装置内の受信バッファが枯渇して受信フレームを廃棄することがないようにするためには，ポーズパケットを送信して相手装置に送信規制を要求します。また，相手装置はポーズパケットを受信して送信規制できる必要があります。

相手装置からのポーズパケットを受信したとき，本装置が送信規制するかどうかは設定に従います。

また，48 ポートモデルの場合，ポート 1～24 および 49～50 と，ポート 25～48 および 51～54 の間の通信では，送信側のポートの輻輳による受信側のポートからのポーズパケットの送信はしません。

フローコントロールのコンフィグレーションは，送信と受信でそれぞれ，有効，無効，またはネゴシエーション結果によって動作を決定するモードを選択できます。本装置と相手装置の設定を，送信と受信で一致させてください。

本装置のポーズパケット送信の設定と相手装置の設定を組み合わせたときのフローコントロール動作を，次の表に示します。

表 20-10　フローコントロールの送信動作

本装置の ポーズパケット送信 (send パラメータ)	相手装置の ポーズパケット受信	フローコントロール動作
on	有効	相手装置が送信規制を行う
off	無効	相手装置が送信規制を行わない
desired	Desired	相手装置が送信規制を行う

（凡例）Desired：ネゴシエーション結果によって動作を決定するモード

本装置のポーズパケット受信の設定と相手装置の設定を組み合わせたときのフローコントロール動作を，次の表に示します。

表 20-11　フローコントロールの受信動作

本装置の ポーズパケット受信 (receive パラメータ)	相手装置の ポーズパケット送信	フローコントロール動作
on	有効	本装置が送信規制を行う
off	無効	本装置が送信規制を行わない
desired	Desired	本装置が送信規制を行う

（凡例）Desired：ネゴシエーション結果によって動作を決定するモード

オートネゴシエーション時，本装置の設定が off で相手装置が Desired の場合および本装置の設定が desired の場合，フローコントロール動作はネゴシエーション結果に従います。

(2) オートネゴシエーション使用時のフローコントロール動作

本装置では，オートネゴシエーションに対応したインタフェースでオートネゴシエーションの使用時に，相手装置とポーズパケットを送受信するかどうかを折衝できます。

オートネゴシエーション使用時のフローコントロール動作を次の表に示します。

表 20-12 オートネゴシエーション使用時のフローコントロール動作

本装置 (パラメータ)		相手装置		本装置のオートネゴシエーション結果		フローコントロール動作	
ポーズパケット送信	ポーズパケット受信	ポーズパケット送信	ポーズパケット受信	ポーズパケット送信	ポーズパケット受信	本装置の送信規制	相手装置の送信規制
on	desired	有効	有効	on	on	行う	行う
			無効	on	off	行わない	行わない
			Desired	on	on	行う	行う
		無効	有効	on	on	行わない	行う
			無効	on	off	行わない	行わない
			Desired	on	on	行う	行う
		Desired	有効	on	on	行う	行う
			無効	on	off	行わない	行わない
			Desired	on	on	行う	行う
off		有効	有効	on	on	行う	行う
			無効	off	on	行う	行わない
			Desired	on	on	行う	行う
		無効	有効	on	on	行わない	行う
			無効	off	off	行わない	行わない
			Desired	on	on	行う	行う
		Desired	有効	on	on	行う	行う
			無効	off	on	行う	行わない
			Desired	on	on	行う	行う
desired	on	有効	有効	on	on	行う	行う
			無効	off	on	行う	行わない
			Desired	on	on	行う	行う
		無効	有効	on	on	行わない	行う

本装置 (パラメータ)		相手装置		本装置のオートネゴシエーション結果		フローコントロール動作	
ポーズパケット送信	ポーズパケット受信	ポーズパケット送信	ポーズパケット受信	ポーズパケット送信	ポーズパケット受信	本装置の送信規制	相手装置の送信規制
			無効	off	on	行わない	行わない
			Desired	on	on	行う	行う
		Desired	有効	on	on	行う	行う
			無効	off	on	行わない	行わない
			Desired	on	on	行う	行う
	off	有効	有効	off	off	行わない	行わない
			無効	off	off	行わない	行わない
			Desired	off	off	行わない	行わない
		無効	有効	on	off	行わない	行う
			無効	off	off	行わない	行わない
			Desired	on	off	行わない	行う
		Desired	有効	off	off	行わない	行わない
			無効	off	off	行わない	行わない
			Desired	off	off	行わない	行わない
	desired	有効	有効	on	on	行う	行う
			無効	off	off	行わない	行わない
			Desired	on	on	行う	行う
		無効	有効	on	on	行わない	行う
			無効	off	off	行わない	行わない
			Desired	on	on	行う	行う
		Desired	有効	on	on	行う	行う
			無効	off	off	行わない	行わない
			Desired	on	on	行う	行う

（凡例）Desired：ネゴシエーション結果によって動作を決定するモード

次のポートでオートネゴシエーションを使用する場合，ポーズパケット受信の設定が desired，ポーズパケット送信の設定が on の組み合わせの場合にだけ，フローコントロールが利用できます。フローコントロールの動作が異なるポートを次の表に示します。

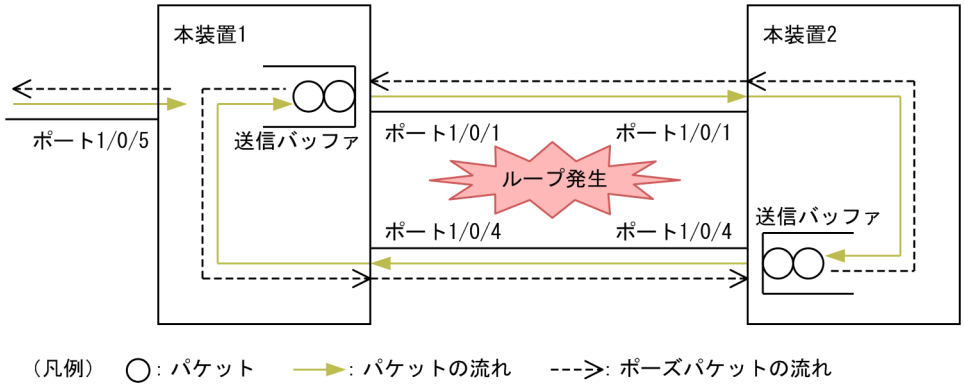
表 20-13　フローコントロールの動作が異なるポート

モデル	ポート番号
AX2340S-24T4X	ポート 25～30
AX2340S-24TH4X	ポート 25～30
AX2340S-48T4X	ポート 53～54
AX2340S-24P4X	ポート 25～30
AX2340S-24PH4X	ポート 25～30
AX2340S-48P4X	ポート 53～54
AX2340S-16P8MP2X	ポート 25～26

(3)　ルーズモード

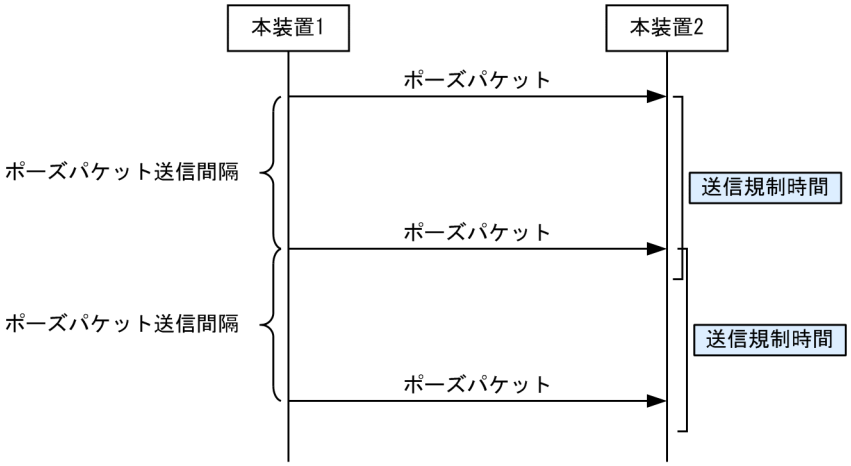
サーバへの接続などで，パケットの損失をできるだけ防ぎたい場合は，厳密なフローコントロールが求められます。しかし，相互に厳密なフローコントロールを行うと，瞬間的なループ状態を契機として次の図に示すようにお互いが送信規制されたままの状態となるおそれがあります。フローコントロールのルーズモードは，このようなネットワークでフローコントロールを行う場合に適したモードです。

図 20-2　相互に送信規制する例



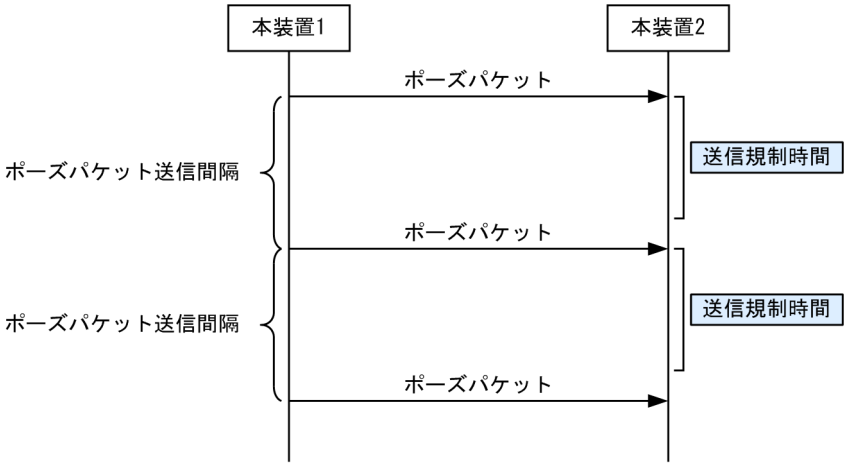
デフォルト動作の場合，“ポーズパケット送信間隔≦送信規制時間”となるため，ポーズパケットの受信側では送信が完全に停止します。デフォルトでの動作シーケンスを次の図に示します。

図 20-3　デフォルトでの動作シーケンス



ルーズモードの場合，“ポーズパケット送信間隔＞送信規制時間”となるため，本装置同士の接続でも送信が完全に停止し続けることがありません。ルーズモードでの動作シーケンスを次の図に示します。

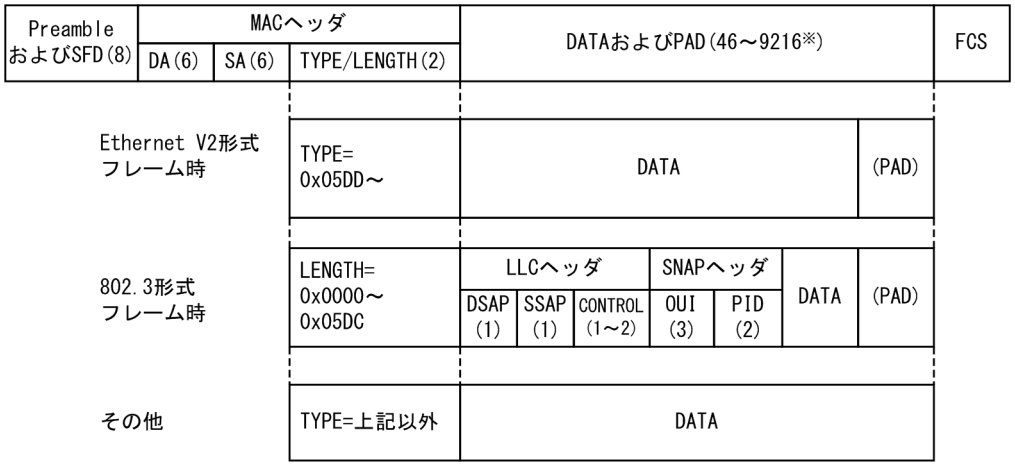
図 20-4　ルーズモードでの動作シーケンス



20.2.2　フレームフォーマット

フレームフォーマットを次の図に示します。

図 20-5　フレームフォーマット



（ ）内の数字はフィールド長を示す。（単位：オクテット）

注※　DATAおよびPADの最大長はEthernetV2形式フレーム時だけ9216。
802.3形式フレームおよびその他の形式のフレームは1500。

本装置では，Ethernet V2 形式フレームだけをサポートします。IEEE802.3 形式フレームはサポートしていません。ただし，本装置でサポートしている L2 プロトコルで使用する制御フレームは受信および転送します。

(1)　MAC 副層フレームフォーマット

(a)　Preamble および SFD

64 ビット長の 2 進数で「1010...1011(最初の 62 ビットは 10 繰り返し，最後の 2 ビットは 11)」のデータです。送信時にフレームの先頭に付加します。この 64 ビットパターンのないフレームは受信できません。

(b)　DA および SA

48 ビット形式をサポートします。16 ビット形式およびローカルアドレスはサポートしていません。

(c)　TYPE/LENGTH

TYPE／LENGTH フィールドの扱いを次の表に示します。

表 20-14　TYPE／LENGTH フィールドの扱い

TYPE／LENGTH 値	本装置での扱い
0x0000～0x05DC	IEEE802.3 CSMA/CD のフレーム長
0x05DD～	Ethernet V2.0 のフレームタイプ

(d)　FCS

32 ビットの CRC 演算を使用します。

(2)　LLC の扱い

Ethernet V2 と同様に扱います。

(3)　受信フレームの廃棄条件

次に示すどれかの条件によって受信したフレームを廃棄します。

- 受信フレーム長（DA～FCS）が 64 オクテット未満，または 1523 オクテット以上
  ただし，ジャンボフレーム選択時は，指定したフレームサイズを超えた場合
- FCS エラー
- 接続インタフェースが半二重の場合に，受信中に衝突が発生したフレーム

(4)　パッドの扱い

送信フレーム長が 64 オクテット未満の場合, MAC 副層で FCS の直前にパッドを付加します。パッドの値は不定です。

20.2.3　ジャンボフレーム

ジャンボフレームは，MAC ヘッダの DA～データが 1518 オクテットを超えるフレームを中継するための機能です。コンフィグレーションコマンド ip mtu の MTU 長を合わせて変更することで, IP パケットをフラグメント化するサイズを大きくすることもできます。

Tagged フレームについては,「24.1.5　VLAN Tag」の Tagged フレームのフォーマットを参照してください。ジャンボフレームのサポート機能を次の表に示します。

表 20-15　ジャンボフレームサポート機能

項目	フレーム形式		内容
	Ethernet V2	IEEE802.3	
フレーム長（オクテット）	1519～9234	×	MAC ヘッダの DA～データの長さ。FCS は含みません。
受信機能	○	×	LENGTH フィールド値が 0x05DD（1501 オクテット）以上の場合，Ethernet V2.0 のフレームタイプとして扱います。
送信機能	○	×	IEEE802.3 フレームは送信しません。

（凡例）　○：サポート　×：未サポート

なお，10BASE-T／100BASE-TX／1000BASE-T では，100BASE-TX（全二重）および 1000BASE-T（全二重）だけをサポートします。

20.3　PoE の解説

PoE（Power over Ethernet）とは，データ通信用の UTP ケーブルを使ってネットワーク機器に電力を供給する機能です。PoE は，電源を取りにくい場所に設置するネットワーク機器で使用します。電力の供給側を給電装置，需要側を受電装置と呼びます。

本装置は IEEE802.3af/IEEE802.3at 規格，または IEEE802.3bt 規格に準拠する給電装置です。なお，Pre.STD の受電装置の接続はサポートしていません。

本装置の準拠規格と対応する電力クラスを次の表に示します。

表 20-16　本装置の準拠規格と対応する電力クラス

モデル	準拠規格	ポート	電力クラス
AX2340S-24P4X	IEEE802.3af IEEE802.3at	1～24	Class0～Class4
AX2340S-24PH4X			
AX2340S-48P4X		1～48	
AX2340S-16P8MP2X	IEEE802.3bt	1～16	Class1～Class4
		17～24	Class1～Class6

20.3.1　ポートへの供給電力の割り当て

(1)　IEEE802.3af/IEEE802.3at 規格準拠のモデル

本装置は，自動的に受電装置を検出し，受電装置が要求する電力クラスを分類して，電力を供給します。本装置が受電装置を分類するときの電力クラスと最大出力電力を次の表に示します。

なお，電力クラスの分類は，IEEE802.3af 規格ではオプションとなっています。受電装置が次の電力クラス分類に対応していない場合は，Class0 に分類します。

表 20-17　本装置の電力クラスと最大出力電力

電力クラス	最大出力電力
Class0	15.4 ワット
Class1	4.0 ワット
Class2	7.0 ワット
Class3	15.4 ワット
Class4	30.0 ワット

また，コンフィグレーションコマンド power inline allocation の limit パラメータで，ポートへの供給電力を設定できます。実消費電力が電力クラスごとの割り当てよりも大幅に小さい場合，この設定で無駄を省けます。

(2)　IEEE802.3bt 規格準拠のモデル

本装置は，自動的に受電装置を検出し，受電装置が要求する電力クラスを分類して，電力を供給します。本装置が受電装置を分類するときの電力クラスと最大出力電力を次の表に示します。

なお，受電装置が次の電力クラス分類に対応していない場合は，Class3 に分類します。

表 20-18　本装置の電力クラスと最大出力電力

電力クラス※	最大出力電力
Class1	4.0 ワット
Class2	7.0 ワット
Class3	15.4 ワット
Class4	30.0 ワット
Class5	45.0 ワット
Class6	60.0 ワット

注※　Class7 および Class8 は未サポートです。

また，本装置は IEEE802.3bt 規格でオプションとなっている Autoclass 機能をサポートしています。本機能は，コンフィグレーションコマンド power inline allocation の autoclass パラメータで有効になります。

本機能が有効で，受電装置が本機能に対応している場合，本装置は，受電装置への給電開始時に，受電装置が実際に消費する最大電力を測定します。測定した結果を基に，ポートへの供給電力の割り当てを自動的に設定します。

20.3.2　電力供給の優先制御

コンフィグレーションコマンド power inline で，ポートごとに電力供給の優先度を設定できます。供給する電力が不足する場合，この機能によって，電力供給を保証するポートと停止させるポートを指定できます。コンフィグレーションの設定がない場合，デフォルトの優先度は「高」です。また，同じ設定が複数あった場合は，ポート番号の小さいポートを優先します。

本装置は，装置全体でポートごとに設定した優先度に従って，優先度の高いポートを優先して電力を供給します。一方，コンフィグレーションコマンド power inline priority-control disable を設定した場合は，ポートごとの優先度に関係なく，すでに接続されているポートへの給電を優先します。この設定では，先に接続された受電装置に優先して電力を供給するため，総消費電力が本装置の最大供給電力を超えた状態で優先度の高いポートに受電装置が接続された場合，その受電装置には電力を供給しません。

power inline priority-control disable コマンドと power inline コマンドの設定とポートの優先度の関係を次の表に示します。

表 20-19　power inline priority-control disable コマンドと power inline コマンドの設定とポートの優先度の関係

power inline priority-control disable コマンドの設定	power inline コマンドによる優先度パラメータの設定	ポートの動作
設定なし	critical	最重要ポートとして電力を供給します。
	high	優先度「高」で電力を供給します。
	low	優先度「低」で電力を供給します。
	never	電力の供給を停止します。
設定あり	critical	ポートごとの優先度を無視します。
	high	
	low	
	never	電力の供給を停止します。

20.3.3　装置の電力超過時の動作

コンフィグレーションコマンド power inline allocation の limit パラメータでポートの電力量割り当てを手動で設定する場合，ポートに割り当てる電力の総和は，本装置の最大供給電力以下になるように，次の関係式を満たすように設定してください。

装置の最大供給電力（ワット）≧

Class0 のポート数×出力電力（15.4 ワット）＋

Class1 のポート数×出力電力（4.0 ワット）＋

Class2 のポート数×出力電力（7.0 ワット）＋

Class3 のポート数×出力電力（15.4 ワット）＋

Class4 のポート数×出力電力（30.0 ワット）＋

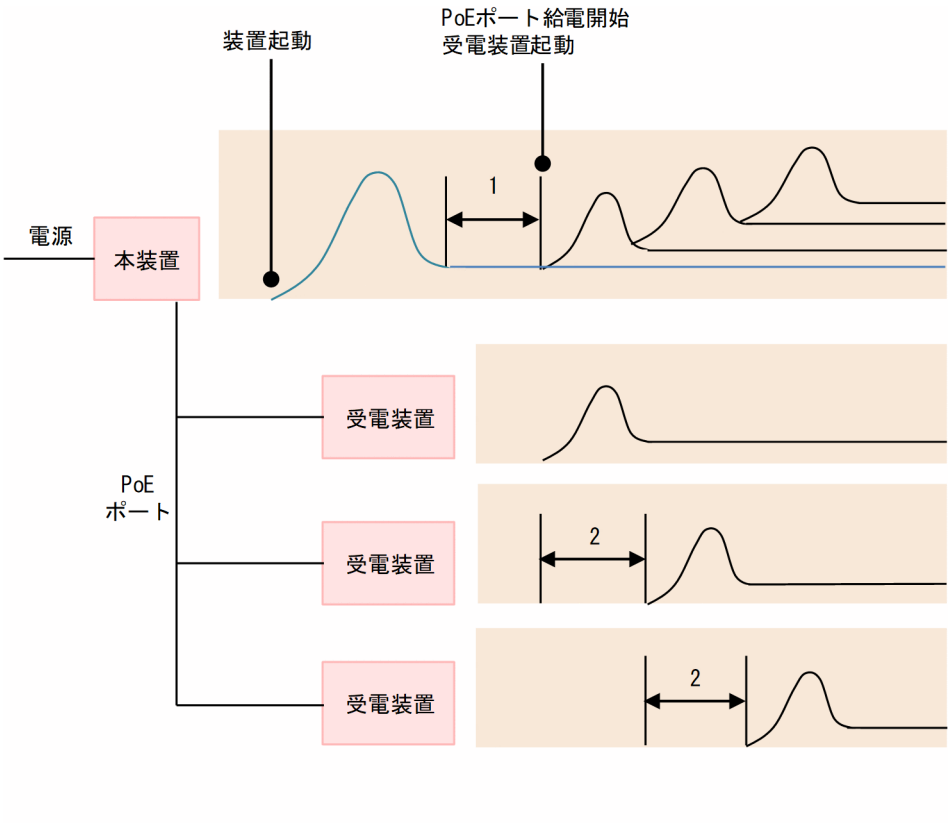
手動電力割り当て設定ポートの合計電力

受電装置への供給電力の総和が装置の最大供給電力をオーバーする場合，ポートに設定した優先度に従って電力の供給を停止します。また，装置の供給電力量が残り少なくなったとき，SNMP 通知を送信します。

20.3.4　PoE 給電分散機能

本装置の PoE 給電分散機能は，起動時の PoE 給電開始時間を分散させることで，システム内の電力使用量のピークを低減する機能です。PoE 給電分散機能の概要を次の図に示します。

図 20-6　PoE 給電分散機能の概要



1：装置のPoE給電開始待機時間

2：PoEポートの給電開始間隔

1. 装置の PoE 給電開始待機時間

   装置起動後，コンフィグレーションで設定された PoE 給電開始待機時間が経過するまで，給電開始を抑止します。

2. PoE ポートの給電開始間隔

   コンフィグレーションで設定された給電開始間隔に従って，ポートの給電を開始します。

上記は，コンフィグレーションコマンド power inline delay で設定できます。

20.3.5　PoE 使用時の注意事項

(1)　power inline allocation limit による電力割り当てについて

コンフィグレーションコマンド power inline allocation の limit パラメータで，ポートごとの電力量割り当てを手動で設定する場合は，受電装置のマニュアルを参照して，お客様の責任で実施してください。

受電装置の最大消費電力には，少し余裕を持たせた値を設定してください。受電装置が必要とする最低消費電力よりも小さな値を手動で設定すると，オーバーロードを検出して，受電装置への電力供給を停止することがあります。回復するときは，運用コマンド activate power inline を実行してください。

(2)　回線テストを実行した場合

PoE ポートで回線テスト（internal 指定）を実行した場合，給電を継続します。

(3) ポート状態による給電について

- シャットダウン状態になった場合，給電を停止します。
- inactive 状態になった場合，給電を継続します。

(4) 電力クラスの分類および Autoclass 機能による電力割り当てについて

受電装置の電力クラスがポートの最大電力クラスを超える場合，ポートの最大電力クラスに分類します。また，Autoclass 機能で測定した受電装置の最大電力がポートの最大供給電力を超える場合，ポートの最大供給電力を割り当てます。

このような場合，オーバーロードを検出して，受電装置への電力供給を停止することがあります。回復するときは，運用コマンド activate power inline を実行してください。

20.4　コマンドガイド

20.4.1　コマンド一覧

イーサネットのコンフィグレーションコマンド一覧を次の表に示します。

表 20-20　コンフィグレーションコマンド一覧

コマンド名	説明
bandwidth	帯域幅を設定します。
description	補足説明を設定します。
duplex	duplex を設定します。
flowcontrol	フローコントロールを設定します。
frame-error-notice	フレーム受信エラーおよびフレーム送信エラー発生時のエラーの通知条件を設定します。
interface gigabitethernet	回線速度が最大 1000Mbit/s のイーサネットインタフェースのコンフィグレーションを指定します。
interface tengigabitethernet	回線速度が最大 10Gbit/s のイーサネットインタフェースのコンフィグレーションを指定します。
link debounce	リンクダウン検出時間を設定します。
link up-debounce	リンクアップ検出時間を設定します。
mdix auto	自動 MDI/MDIX 機能を設定します。
mtu	イーサネットの MTU を設定します。
power inline	ポートごとに電力供給の優先度を設定します。
power inline allocation	ポートごとに割り当てる電力を設定します。
power inline delay	装置の PoE 給電開始待機時間と PoE ポートの給電開始間隔を設定します。
power inline priority-control disable	すでに給電しているポートを優先します。
shutdown	イーサネットをシャットダウンします。
speed	速度を設定します。
system flowcontrol off	装置内の全ポートでフローコントロールを無効にします。
system mtu	イーサネットの MTU の装置としての値を設定します。

イーサネットの運用コマンド一覧を次の表に示します。

表 20-21　運用コマンド一覧

コマンド名	説明
show interfaces	イーサネットの情報を表示します。

コマンド名	説明
clear counters	イーサネットの統計情報カウンタをクリアします。
show port	イーサネットの情報を一覧で表示します。
activate	inactive 状態のイーサネットを active 状態にします。
inactivate	active 状態のイーサネットを inactive 状態にします。
test interfaces	回線テストを実行します。
no test interfaces	回線テストを停止し，結果を表示します。
show power inline	装置およびポートごとの PoE 情報を表示します。
activate power inline	電力供給を手動で再開します。
inactivate power inline	電力供給を手動で停止します。

20.4.2　イーサネットインタフェースの設定

イーサネットインタフェースは，接続するインタフェースに対応するコマンドで該当するモードに移行してから，コンフィグレーションを設定します。ポートの種類と対応するモード移行コマンドを次の表に示します。

表 20-22　ポートの種類と対応するモード移行コマンド

ポートの種類	モード移行コマンド
10BASE-T/100BASE-TX/1000BASE-T ポート	interface gigabitethernet
100BASE-TX/1000BASE-T/2.5GBASE-T ポート	interface gigabitethernet
SFP ポート	interface gigabitethernet
SFP+/SFP 共用ポート	interface tengigabitethernet

(1)　インタフェースに対するコンフィグレーションの設定

[設定のポイント]

イーサネットのコンフィグレーションでは，複数のコマンドでコンフィグレーションを設定することがあります。そのとき，コンフィグレーションの設定が完了していない状態でイーサネットがリンクアップ状態になると期待した通信ができません。したがって，最初にイーサネットをシャットダウンしてから，コンフィグレーションの設定が完了したあとにイーサネットのシャットダウンを解除することを推奨します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/0/10**
   イーサネットインタフェース 1/0/10 のコンフィグレーションモードに移行します。
2. **(config-if)# shutdown**
   イーサネットインタフェースをシャットダウンします。
3. **(config-if)# ＊＊＊＊＊**
   イーサネットインタフェースに対するコンフィグレーションを設定します。

4. **(config-if)# no shutdown**

   イーサネットインタフェースのシャットダウンを解除します。

(2)　インタフェースのシャットダウン

イーサネットをシャットダウンするには，該当するイーサネットインタフェースのコンフィグレーションモードに移行して，shutdown コマンドを実行します。使用しないイーサネットはシャットダウンしておいてください。

なお，運用コマンド inactivate でイーサネットの運用を停止することもできます。ただし，inactivate コマンドで inactive 状態とした場合は，装置を再起動するとイーサネットが active 状態になります。イーサネットをシャットダウンした場合は，装置を再起動してもイーサネットは disable 状態のままとなり，active 状態にするためにはコンフィグレーションで no shutdown を設定してシャットダウンを解除する必要があります。

20.4.3　複数インタフェースの一括設定

[設定のポイント]

イーサネットのコンフィグレーションでは，複数のインタフェースに同じ情報を設定することがあります。このような場合，複数のインタフェースを range 指定すると，情報を一括して設定できます。

[コマンドによる設定]

1. **(config)# interface range gigabitethernet 1/0/1-10, gigabitethernet 1/0/15-20, tengigabitethernet 1/0/27**

   ギガビットイーサネットインタフェース 1/0/1 から 1/0/10，1/0/15 から 1/0/20，および 10 ギガビットイーサネットインタフェース 1/0/27 のコンフィグレーションモードに移行します。

2. **(config-if-range)# ＊＊＊＊＊**

   複数のインタフェースに同じコンフィグレーションを一括して設定します。

20.4.4　速度と全二重/半二重の設定

次に示す場合は，必要に応じて各ポートに回線速度と全二重／半二重を設定します。

- 10BASE-T/100BASE-TX/1000BASE-T ポート
- 100BASE-TX/1000BASE-T/2.5GBASE-T ポート
- SFP ポートで SFP-T または SFP（1000BASE-X）を使用
- SFP+/SFP 共用ポートで SFP-T または SFP を使用

デフォルトではオートネゴシエーションを使用します。オートネゴシエーションを使用しないで固定設定で接続する場合は，回線速度と全二重／半二重を設定します。固定設定で接続する場合は，speed コマンドと duplex コマンドの両方に固定設定をする必要があります。正しい組み合わせが設定されていない場合は，デフォルトで動作します。

なお，次に示す場合はインタフェース固有の回線速度および全二重固定のため，設定は不要です。

- SFP+/SFP 共用ポートで SFP+を使用

(1) 回線速度と全二重／半二重を固定して相手装置と接続する場合

[設定のポイント]

オートネゴシエーションを使用しない場合は，回線速度と全二重／半二重を指定して，固定設定で接続します。ここでは，1000BASE-X ポートで，1000Mbit/s 全二重固定で相手装置と接続する場合の設定例を示します。

なお，回線速度を 1000Mbit/s に設定する場合は，必ず全二重に設定してください。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/0/1**
   (config-if)# shutdown
   (config-if)# speed 1000
   (config-if)# duplex full
   イーサネットインタフェースをシャットダウンして，相手装置と 1000Mbit/s 全二重固定で接続する設定をします。
2. **(config-if)# no shutdown**
   イーサネットインタフェースのシャットダウンを解除します。

(2) オートネゴシエーションに対応していない相手装置と接続する場合

[設定のポイント]

10BASE-T および 100BASE-TX では，相手装置によってはオートネゴシエーションで接続できない場合があります。その場合は，相手装置に合わせて回線速度と全二重／半二重を指定して，固定設定で接続します。

ここでは，10BASE-T 半二重固定で相手装置と接続する場合の設定例を示します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/0/10**
   (config-if)# shutdown
   (config-if)# speed 10
   (config-if)# duplex half
   イーサネットインタフェースをシャットダウンして，相手装置と 10BASE-T 半二重固定で接続する設定をします。
2. **(config-if)# no shutdown**
   イーサネットインタフェースのシャットダウンを解除します。

(3) オートネゴシエーションでも特定の速度を使用して相手装置と接続する場合

[設定のポイント]

本装置は，オートネゴシエーションで接続する場合でも，回線速度を設定できます。オートネゴシエーションに加えて回線速度を設定した場合，相手装置とオートネゴシエーションで接続しても，設定された回線速度にならないときはリンクがアップしません。そのため，意図しない回線速度で接続されることを防止できます。

ここでは，オートネゴシエーションを使用しても，回線速度は 1000Mbit/s だけで相手装置と接続する場合の設定例を示します。

[コマンドによる設定]

1. (config)# interface gigabitethernet 1/0/10
   (config-if)# shutdown
   (config-if)# speed auto 1000
   イーサネットインタフェースをシャットダウンして，相手装置との接続にオートネゴシエーションを使用しても，回線速度は 1000Mbit/s だけで接続する設定をします。
2. (config-if)# no shutdown
   イーサネットインタフェースのシャットダウンを解除します。

20.4.5　自動 MDI/MDIX 機能の設定

本装置はツイストペアケーブルを使用するポートで，自動 MDI/MDIX 機能をサポートしています。そのため，オートネゴシエーション時に，ケーブルのストレートまたはクロスに合わせて自動的に MDI 設定が切り替わり通信できます。また，本装置は MDI の固定機能を持っており，MDI 固定時は MDI-X（HUB 仕様）となります。

[設定のポイント]

自動 MDI/MDIX 機能を MDI-X に固定する場合に，固定したいインタフェースに設定します。

[コマンドによる設定]

1. (config)# interface gigabitethernet 1/0/24
   イーサネットインタフェース 1/0/24 のコンフィグレーションモードに移行します。
2. (config-if)# no mdix auto
   (config-if)# exit
   自動 MDI/MDIX 機能を無効にし，MDI-X 固定にします。

20.4.6　フローコントロールの設定

本装置では，フローコントロールをポート単位に設定したり，装置内の全ポートでフローコントロールを無効にしたりできます。装置内の全ポートでフローコントロールを無効にすると，ポート単位のフローコントロールの設定はコンフィグレーションファイルに残りますが，動作しません。

(1)　ポート単位のフローコントロールの設定

[設定のポイント]

フローコントロールの設定内容は，相手装置と矛盾しないように決定してください。

[コマンドによる設定]

1. (config)# interface tengigabitethernet 1/0/27
   (config-if)# shutdown
   イーサネットインタフェースをシャットダウンします。
2. (config-if)# flowcontrol send off
   (config-if)# flowcontrol receive off
   相手装置とのポーズパケット送受信を停止します。
3. (config-if)# no shutdown
   イーサネットインタフェースのシャットダウンを解除します。

(2) 全ポート共通のフローコントロールの設定

[設定のポイント]

装置内の全ポートでフローコントロールを無効にします。

[コマンドによる設定]

1. **(config)# system flowcontrol off**
   全ポートで相手装置とのポーズパケット送受信の停止を設定します。
2. **(config)# save**
   (config)# exit
   保存して，コンフィグレーションモードから装置管理者モードに移行します。
3. **# restart vlan**
   VLAN プログラムを再起動します。全ポートで相手装置とのポーズパケット送受信を停止します。すべてのイーサネットインタフェースが再初期化され，VLAN を構成しているポートは一時的にデータの送受信ができなくなります。

(3) フローコントロールのルーズモード設定

[設定のポイント]

フローコントロールのルーズモードを設定します。

[コマンドによる設定]

1. **(config)# interface tengigabitethernet 1/0/25**
   (config-if)# shutdown
   イーサネットインタフェースをシャットダウンします。
2. **(config-if)# flowcontrol send on loose**
   相手装置とのポーズパケット送信をルーズモードにします。
3. **(config-if)# no shutdown**
   イーサネットインタフェースのシャットダウンを解除します。

20.4.7 ジャンボフレームの設定

イーサネットインタフェースの MTU は規格上 1500 オクテットです。本装置は，ジャンボフレームを使用して MTU を拡張し，一度に転送するデータ量を大きくすることでスループットを向上できます。

ジャンボフレームを使用するポートでは MTU を設定します。本装置は，設定された MTU に VLAN Tag が一つ付いているフレームを送受信できるようになります。

ポートの MTU の設定値は，ネットワークおよび相手装置と合わせて決定します。VLAN トンネリングなどで，VLAN Tag が二つ付く場合は，そのフレームを送受信できるように，MTU の値に 4 を加えた値を設定します。

(1) ポート単位の MTU の設定

[設定のポイント]

ポート 1/0/10 のポートの MTU を 8192 オクテットに設定します。この設定によって，8210 オクテットまでのジャンボフレームを送受信できるようになります。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/0/10**
   (config-if)# shutdown
   (config-if)# mtu 8192
   イーサネットインタフェースをシャットダウンして，ポートの MTU を 8192 オクテットに設定します。
2. **(config-if)# no shutdown**
   イーサネットインタフェースのシャットダウンを解除します。

[注意事項]

コンフィグレーションでポートの MTU を設定していても，10BASE-T で接続する場合（オートネゴシエーションの結果が 10BASE-T になった場合も含みます）は，ポートの MTU は 1500 オクテットになります。

(2)　全ポート共通の MTU の設定

[設定のポイント]

本装置の全イーサネットインタフェースでポートの MTU を 4096 オクテットに設定します。この設定によって，4114 オクテットまでのジャンボフレームを送受信できるようになります。

[コマンドによる設定]

1. **(config)# system mtu 4096**
   装置の全ポートで，ポートの MTU を 4096 オクテットに設定します。

[注意事項]

コンフィグレーションでポートの MTU を設定していても，10BASE-T で接続する場合（オートネゴシエーションの結果が 10BASE-T になった場合も含みます）は，ポートの MTU は 1500 オクテットになります。

20.4.8　リンクダウン検出タイマの設定

リンク障害を検出してからリンクダウンするまでのリンクダウン検出時間が短い場合，相手装置によってはリンクが不安定になることがあります。このような場合，リンクダウン検出タイマを設定することで，リンクが不安定になることを防ぐことができます。

[設定のポイント]

リンクダウン検出時間は，リンクが不安定とならない範囲でできるだけ短い値にします。リンクダウン検出時間を設定しなくてもリンクが不安定とならない場合は，リンクダウン検出時間を設定しないでください。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/0/10**
   イーサネットインタフェース 1/0/10 のコンフィグレーションモードに移行します。
2. **(config-if)# link debounce time 5000**
   リンクダウン検出タイマを 5000 ミリ秒に設定します。

[注意事項]

リンクダウン検出時間を設定すると，リンクが不安定になることを防ぐことができますが，障害が発生した場合にリンクダウンするまでの時間が長くなります。リンク障害を検出してからリンクダウンするまでの時間を短くしたい場合は，リンクダウン検出タイマを設定しないでください。

20.4.9　リンクアップ検出タイマの設定

リンク障害回復を検出してからリンクアップするまでのリンクアップ検出時間が短い場合，相手装置によってはネットワーク状態が不安定になることがあります。このような場合，リンクアップ検出タイマを設定することで，ネットワーク状態が不安定になることを防ぐことができます。

[設定のポイント]

リンクアップ検出時間は，ネットワーク状態が不安定とならない範囲でできるだけ短い値にします。リンクアップ検出時間を設定しなくてもネットワーク状態が不安定とならない場合は，リンクアップ検出時間を設定しないでください。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/0/10**
   イーサネットインタフェース 1/0/10 のコンフィグレーションモードに移行します。
2. **(config-if)# link up-debounce time 5000**
   リンクアップ検出タイマを 5000 ミリ秒に設定します。

[注意事項]

リンクアップ検出タイマを長く設定すると，リンク障害回復から通信できるまでの時間が長くなります。リンク障害回復から通信できるまでの時間を短くしたい場合は，リンクアップ検出タイマを設定しないでください。

20.4.10　フレーム送受信エラー通知の設定

軽度のエラーが発生してフレームの受信または送信に失敗した場合，本装置はフレームが廃棄された原因を統計情報として採取します。30 秒間に発生したエラーの回数とエラーの発生する割合が閾値を超えた場合は，エラーの発生について，ログで通知し，プライベートの SNMP 通知を送信します。

本装置では，閾値とエラーが発生した場合の通知について設定ができます。設定がない場合，30 秒間に 15 回エラーが発生したときに最初の 1 回だけログを表示します。

(1)　エラーフレーム数を閾値にしての通知

[設定のポイント]

エラーの通知条件のうち，エラーの発生回数（エラーフレーム数）の閾値を本装置に設定する場合は，frame-error-notice コマンドで error-frames を設定します。

[コマンドによる設定]

1. **(config)# frame-error-notice error-frames 50**
   エラーの発生回数（エラーフレーム数）の閾値を 50 回に設定します。

(2)　エラーレートを閾値にしての通知

[設定のポイント]

エラーの通知条件のうち，エラーの発生割合（エラーレート）の閾値を本装置に設定する場合は，frame-error-notice コマンドで error-rate を設定します。

[コマンドによる設定]

1. **(config)# frame-error-notice error-rate 20**
   エラーの発生割合の閾値を 20%に設定します。

(3)　通知時のログ表示設定

[設定のポイント]

エラーの通知条件のうち，エラーが発生したときのログの表示を設定する場合は，frame-error-notice コマンドで onetime-display，または everytime-display を設定します。ログを表示しないようにする場合は，off を設定します。この設定は，プライベートの SNMP 通知には関係しません。

[コマンドによる設定]

1. **(config)# frame-error-notice everytime-display**
   エラーが発生するたびにログを表示します。

(4)　条件の組み合わせ設定

[設定のポイント]

エラーの通知条件を複数組み合わせて設定する場合は，frame-error-notice コマンドで，複数の条件を同時に設定します。frame-error-notice コマンド入力前に設定していた通知条件は無効となりますので，引き続き同じ通知条件を設定する場合は，frame-error-notice コマンドで再度設定し直してください。

[コマンドによる設定]

すでにエラーが発生するたびにログを表示することを設定していて，さらにエラーの発生割合（エラーレート）の閾値を設定する場合の設定例を示します。

1. **(config)# frame-error-notice error-frames 50 everytime-display**
   エラーの発生回数（エラーフレーム数）の閾値を 50 回に設定し，エラーが発生するたびにログを表示します。

[注意事項]

プライベートの SNMP 通知を使用する場合は，snmp-server host コマンドでフレーム受信エラー発生時の SNMP 通知とフレーム送信エラー発生時の SNMP 通知を送信するように設定してください。

20.4.11　PoE の設定

(1)　ポート優先度の設定

[設定のポイント]

接続する装置が PoE 受電装置で，本装置から電力を供給しない場合，または接続する相手装置も PoE 給電装置の場合に，電力供給の停止を設定します。ここでは，ポート 1/0/1 で電力を供給しないように設定します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/0/1**
   (config-if)# power inline never
   PoE 機能で電力を供給しないように設定します。
2. **(config-if)# exit**

[注意事項]

PoE ポートで接続する相手装置が給電装置の場合は，本装置で該当するポートに電力供給の停止を設定してください。相手装置が給電装置で，電力供給の停止を設定しない場合は，オーバーロードを検出してメッセージを出力することがあります。相手装置で電力供給を停止できる場合は，相手装置でも電力供給を停止することを推奨します。

(2) 既給電ポート優先の設定

ポート優先度を無効にして，すでに給電しているポートを優先した場合，先に接続された受電装置を優先して電力を供給します。

[設定のポイント]

本装置でコンフィグレーションコマンド power inline によるポート優先度設定を無効にして，すでに給電しているポートを優先します。

[コマンドによる設定]

1. **(config)# power inline priority-control disable**
   ポート優先度設定を無効にして，すでに給電しているポートを優先するように設定します。
2. **(config)# save**
   (config)# exit
   コンフィグレーションを保存して，コンフィグレーションコマンドモードから装置管理者モードに戻ります。
3. **# reload**
   本装置を再起動します。

[注意事項]

本コマンドを設定および削除した場合は，装置再起動後に変更内容が反映されます。

(3) Autoclass 機能によるポートへの供給電力割り当ての設定

Autoclass 機能を使って，ポートの供給電力割り当てを自動的に設定し，受電装置に電力を供給します。

[設定のポイント]

すでに給電しているポートの割り当て電力を，Autoclass 機能を使った割り当て電力に変更する場合は，給電をいったん停止してから再開します。そうすることで，実際の割り当て電力が変更されます。

ここでは，ポート 1/0/1 で Autoclass 機能を使って，供給電力を割り当てるように設定します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/0/1**
   (config-if)# power inline allocation autoclass
   Autoclass 機能を使って，ポートへの供給電力を割り当てるように設定します。

2. **(config-if)# save**

   (config-if)# end

   コンフィグレーションを保存して，コンフィグレーションコマンドモードから装置管理者モードに戻ります。

3. **# inactivate power inline gigabitethernet 1/0/1**

   # activate power inline gigabitethernet 1/0/1

   すでに該当のポートが給電中であった場合は，給電をいったん停止してから再開することで，実際の割り当て電力が変更されます。

[注意事項]

power inline allocation コマンドの autoclass パラメータの設定を変更または削除した場合も，すでに該当のポートが給電中であったときは，同様にポートの給電をいったん停止してから再開します。そうすることで，実際の割り当て電力が変更されます。

21 リンクアグリゲーション

この章では，リンクアグリゲーションの解説と操作方法について説明します。

21.1　リンクアグリゲーション基本機能の解説

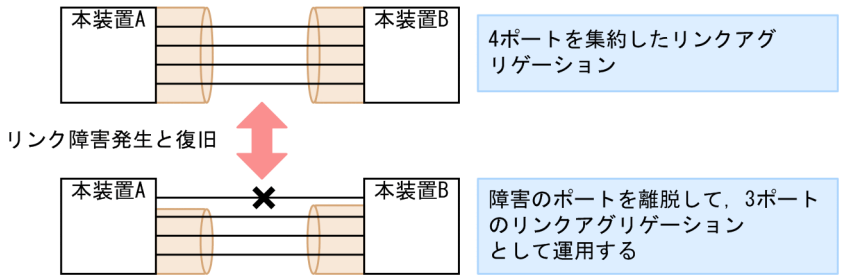
21.1.1　概要

リンクアグリゲーションは，隣接装置との間を複数のイーサネットポートで接続し，それらを束ねて一つの仮想リンクとして扱う機能です。この仮想リンクをチャネルグループと呼びます。リンクアグリゲーションによって接続装置間の帯域の拡大や冗長性を確保できます。

21.1.2　リンクアグリゲーションの構成

リンクアグリゲーションの構成例を次の図に示します。この例では四つのポートを集約しています。集約しているポートのうちの 1 本が障害となった場合には，チャネルグループから離脱し，残りのポートでチャネルグループとして通信を継続します。

図 21-1　リンクアグリゲーションの構成例



21.1.3　サポート仕様

(1)　リンクアグリゲーションのモード

本装置のリンクアグリゲーションは，モードとして LACP およびスタティックの 2 種類をサポートします。

- LACP リンクアグリゲーション
  IEEE802.1AX 準拠の LACP を利用したリンクアグリゲーションです。LACP によるネゴシエーションが成功した場合にチャネルグループとしての運用を開始します。LACP によって，隣接装置との整合性確認やリンクの正常性確認ができます。
- スタティックリンクアグリゲーション
  コンフィグレーションによるスタティックなリンクアグリゲーションです。LACP は動作させません。チャネルグループとして設定したポートがリンクアップした時点で運用を開始します。

(2)　回線速度

チャネルグループを構成するポートのうち，最速かつ同一速度のポートを集約します。

21.1.4　チャネルグループの MAC アドレス

スパニングツリーなどのプロトコルを運用する際に，チャネルグループの MAC アドレスを使用します。本装置は，チャネルグループの MAC アドレスとして，グループに所属するポートのうちどれかの MAC アドレスを使用します。

チャネルグループに所属するポートから MAC アドレスを使用しているポートを削除すると，チャネルグループの MAC アドレスが変更されます。

21.1.5　フレーム送信時のポート振り分け

リンクアグリゲーションへフレームを送信するとき，送信するフレームごとにポートを選択しトラフィックを各ポートへ分散させることで複数のポートを効率的に利用します。本装置は，送信するフレーム内の次に示す情報を基に，自動で送信するポートを選択して振り分けます。

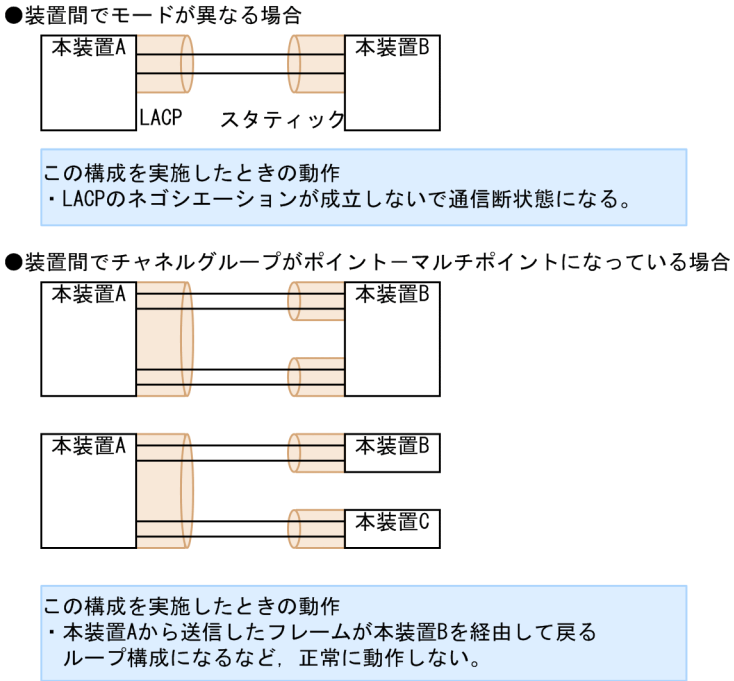
- 宛先 MAC アドレス
- 送信元 MAC アドレス
- 宛先 IP アドレス
- 送信元 IP アドレス
- 宛先 TCP/UDP ポート番号
- 送信元 TCP/UDP ポート番号

21.1.6　リンクアグリゲーション使用時の注意事項

(1)　リンクアグリゲーションが不可能な構成

リンクアグリゲーション構成時には，装置間での設定が一致している必要があります。リンクアグリゲーションが不可能な構成例を次に示します。

図 21-2　リンクアグリゲーションが不可能な構成例



(2)　リンクアグリゲーションの設定手順

リンクアグリゲーション構成時には，装置間での設定が一致している必要があります。一致していない状態で通信を開始しようとするとループ構成となるおそれがあります。設定はリンクダウン状態で行い，「(1)

リンクアグリゲーションが不可能な構成」のような構成になっていないことを確認したあとで，ポートをリンクアップさせることをお勧めします。

(3)　CPU 過負荷時

LACP リンクアグリゲーションモード使用時に CPU が過負荷な状態になった場合，本装置が送受信する LACPDU の廃棄または処理遅延が発生して，タイムアウトのメッセージ出力，一時的な通信断になることがあります。過負荷状態が頻発する場合は，LACPDU の送信間隔を長くするか，スタティックリンクアグリゲーションを使用してください。

21.2　リンクアグリゲーション基本機能のコマンドガイド

21.2.1　コマンド一覧

リンクアグリゲーション基本機能のコンフィグレーションコマンド一覧を次の表に示します。

表 21-1　コンフィグレーションコマンド一覧

コマンド名	説明
channel-group lacp system-priority	チャネルグループごとに LACP システム優先度を設定します。
channel-group mode	ポートをチャネルグループに登録します。
channel-group periodic-timer	LACPDU の送信間隔を設定します。
description	チャネルグループの補足説明を設定します。
interface port-channel	ポートチャネルインタフェースを設定します。 チャネルグループのパラメータもポートチャネルインタフェースコンフィグレーションモードで設定します。
lacp port-priority	LACP のポート優先度を設定します。
lacp system-priority	LACP システム優先度のデフォルト値を設定します。
shutdown	チャネルグループの通信を停止します。

リンクアグリゲーションの運用コマンド一覧を次の表に示します。

表 21-2　運用コマンド一覧

コマンド名	説明
show channel-group	リンクアグリゲーションの情報を表示します。
show channel-group statistics	リンクアグリゲーションの統計情報を表示します。
clear channel-group statistics lacp	LACPDU の送受信統計情報をクリアします。
restart link-aggregation	リンクアグリゲーションプログラムを再起動します。
dump protocols link-aggregation	リンクアグリゲーションの詳細イベントトレース情報および制御テーブル情報をファイルへ出力します。

21.2.2　スタティックリンクアグリゲーションの設定

[設定のポイント]

スタティックリンクアグリゲーションは，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で channel-group mode コマンドを使用してチャネルグループ番号と「on」のモードを設定します。スタティックリンクアグリゲーションは channel-group mode コマンドを設定することによって動作を開始します。

[コマンドによる設定]

1. **(config)# interface range gigabitethernet 1/0/1-2**
   ポート 1/0/1，1/0/2 のイーサネットインタフェースモードに移行します。
2. **(config-if-range)# channel-group 10 mode on**
   ポート 1/0/1，1/0/2 を，スタティックモードのチャネルグループ 10 に登録します。

21.2.3　LACP リンクアグリゲーションの設定

(1)　チャネルグループの設定

[設定のポイント]

LACP リンクアグリゲーションは，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で channel-group mode コマンドを使用してチャネルグループ番号と「active」または「passive」のモードを設定します。

[コマンドによる設定]

1. **(config)# interface range gigabitethernet 1/0/1-2**
   ポート 1/0/1，1/0/2 のイーサネットインタフェースモードに移行します。
2. **(config-if-range)# channel-group 10 mode active**
   ポート 1/0/1，1/0/2 を LACP モードのチャネルグループ 10 に登録します。LACP は active モードとして対向装置に関係なく LACPDU の送信を開始します。passive を指定した場合は，対向装置からの LACPDU を受信したときだけ LACPDU の送信を開始します。

(2)　システム優先度の設定

LACP のシステム優先度を設定します。本装置では，システム優先度は拡張機能の離脱ポート制限機能で使用します。通常，本パラメータを変更する必要はありません。

[設定のポイント]

LACP システム優先度は値が小さいほど高い優先度となります。

[コマンドによる設定]

1. **(config)# lacp system-priority 100**
   本装置の LACP システム優先度を 100 に設定します。
2. **(config)# interface port-channel 10**
   (config-if)# channel-group lacp system-priority 50
   チャネルグループ 10 の LACP システム優先度を 50 に設定します。本設定を行わない場合は装置のシステム優先度である 100 を使用します。

(3)　ポート優先度の設定

LACP のポート優先度を設定します。本装置では，ポート優先度は拡張機能のスタンバイリンク機能で使用します。通常，本パラメータを変更する必要はありません。

[設定のポイント]

LACP ポート優先度は値が小さいほど高い優先度となります。

[コマンドによる設定]

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

(config-if)# lacp port-priority 100

ポート 1/0/1 の LACP ポート優先度を 100 に設定します。

(4)　LACPDU 送信間隔の設定

[設定のポイント]

対向装置が本装置に向けて送信する LACPDU の間隔を設定します。本装置は本パラメータで設定した間隔で LACPDU を受信します。

LACPDU の送信間隔は long（30 秒），short（1 秒）のどちらかを選択します。デフォルトは long（30 秒）で動作します。送信間隔を short（1 秒）に変更した場合，リンクの障害によるタイムアウトを検知しやすくなり，障害時に通信が途絶える時間を短く抑えることができます。

[コマンドによる設定]

1. **(config)# interface port-channel 10**

   (config-if)# channel-group periodic-timer short

   チャネルグループ 10 の LACPDU 送信間隔を short（1 秒）に設定します。

[注意事項]

LACPDU 送信間隔を short（1 秒）に設定すると，障害を検知しやすくなる一方で，LACPDU トラフィックが増加することによってリンクアグリゲーションプログラムの負荷が増加します。本パラメータを short（1 秒）にすることでタイムアウトのメッセージや一時的な通信断が頻発する場合は，デフォルトの long（30 秒）に戻すかスタティックモードを使用してください。

21.2.4　ポートチャネルインタフェースの設定

ポートチャネルインタフェースでは，チャネルグループ上で動作する機能を設定します。

ポートチャネルインタフェースは，コンフィグレーションコマンドで設定するか，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で channel-group mode コマンドを設定することによって自動的に生成されます。

(1)　ポートチャネルインタフェースとイーサネットインタフェースの関係

ポートチャネルインタフェースは，チャネルグループ上で動作する機能を設定します。それらは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でも設定することができます。このような機能を設定するコマンドはポートチャネルインタフェースとイーサネットインタフェースで関連性があり，設定する際に次のように動作します。

- ポートチャネルインタフェースとイーサネットインタフェースで関連コマンドの設定が一致している必要があります。
- ポートチャネルインタフェースを未設定の状態でイーサネットインタフェースに channel-group mode コマンドを設定すると，自動的にポートチャネルインタフェースを生成します。このとき，channel-group mode コマンドを設定するイーサネットインタフェースに関連コマンドが設定されていてはいけません。
- ポートチャネルインタフェースがすでに設定済みの状態でイーサネットインタフェースに channel-group mode コマンドを設定する場合，関連コマンドが一致している必要があります。
- ポートチャネルインタフェースで関連コマンドを設定すると，channel-group mode コマンドで登録されているイーサネットインタフェースの設定にも同じ設定が反映されます。

ポートチャネルインタフェースとイーサネットインタフェースで一致している必要のあるポートチャネル関連コマンドを次の表に示します。

表 21-3　ポートチャネルインタフェースの関連コマンド

機能	コマンド
VLAN	switchport mode
	switchport access
	switchport trunk
	switchport protocol
	switchport mac
	switchport vlan mapping
	switchport vlan mapping enable
スパニングツリー	spanning-tree portfast
	spanning-tree bpdufilter
	spanning-tree bpduguard
	spanning-tree guard
	spanning-tree link-type
	spanning-tree port-priority
	spanning-tree cost
	spanning-tree vlan port-priority
	spanning-tree vlan cost
	spanning-tree single port-priority
	spanning-tree single cost
	spanning-tree mst port-priority
	spanning-tree mst cost
DHCP snooping	ip dhcp snooping trust
	ip arp inspection trust
	ip verify source
L2 ループ検知	loop-detection

(2)　チャネルグループ上で動作する機能の設定

[設定のポイント]

ポートチャネルインタフェースでは，VLAN やスパニングツリーなど，チャネルグループ上で動作する機能を設定します。ここでは，トランクポートを設定する例を示します。

[コマンドによる設定]

1. (config)# interface range gigabitethernet 1/0/1-2
   (config-if-range)# channel-group 10 mode on
   (config-if-range)# exit
   ポート 1/0/1，1/0/2 をスタティックモードのチャネルグループ 10 に登録します。また，チャネルグループ 10 のポートチャネルインタフェースが自動生成されます。
2. (config)# interface port-channel 10
   チャネルグループ 10 のポートチャネル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)# switchport mode trunk
   チャネルグループ 10 をトランクポートに設定します。

(3)　ポートチャネルインタフェースの shutdown

[設定のポイント]

ポートチャネルインタフェースを shutdown に設定すると，チャネルグループに登録されているすべてのポートの通信を停止します。リンクアップしているポートはアップ状態のまま通信停止状態になります。

[コマンドによる設定]

1. (config)# interface range gigabitethernet 1/0/1-2
   (config-if-range)# channel-group 10 mode on
   (config-if-range)# exit
   ポート 1/0/1，1/0/2 をスタティックモードのチャネルグループ 10 として登録します。
2. (config)# interface port-channel 10
   (config-if)# shutdown
   ポートチャネルインタフェースコンフィグレーションモードに移行して shutdown を設定します。
   ポート 1/0/1，1/0/2 の通信が停止し，チャネルグループ 10 は停止状態になります。

21.2.5　チャネルグループの削除

チャネルグループのポートやチャネルグループ全体を削除する場合は，削除する対象のポートをあらかじめ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で shutdown に設定しておく必要があります。shutdown に設定することで，削除する際にループが発生することを防ぎます。

(1)　チャネルグループ内のポートの削除

[設定のポイント]

ポートをチャネルグループから削除します。削除したポートはチャネルグループとは別のポートとして動作するため，削除時のループを回避するために事前に shutdown に設定します。

削除したポートには，削除前に interface port-channel で設定した関連コマンド（表 21-3　ポートチャネルインタフェースの関連コマンド）は残るため，別の用途に使用する際には注意してください。

チャネルグループ内のすべてのポートを削除しても，interface port-channel の設定は自動的には削除されません。チャネルグループ全体の削除は「(2)　チャネルグループ全体の削除」を参照してください。

[コマンドによる設定]

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

(config-if)# shutdown

ポート 1/0/1 をチャネルグループから削除するために，事前に shutdown にしてリンクダウンさせます。

2. **(config-if)# no channel-group**

ポート 1/0/1 からチャネルグループの設定を削除します。

(2)　チャネルグループ全体の削除

[設定のポイント]

チャネルグループ全体を削除します。削除したチャネルグループに登録していたポートはそれぞれ個別のポートとして動作するため，削除時のループを回避するために事前に shutdown に設定します。

チャネルグループは interface port-channel を削除することによって，全体が削除されます。この削除によって，登録していた各ポートから channel-group mode コマンドが自動的に削除されます。ただし，各ポートには削除前に interface port-channel で設定した関連コマンド（表 21-3　ポートチャネルインタフェースの関連コマンド）は残るため，別の用途に使用する際には注意してください。

[コマンドによる設定]

1. **(config)# interface range gigabitethernet 1/0/1-2**

(config-if-range)# shutdown

(config-if-range)# exit

チャネルグループ全体を削除するために，削除したいチャネルグループに登録されているポートをすべて shutdown に設定しリンクダウンさせます。

2. **(config)# no interface port-channel 10**

チャネルグループ 10 を削除します。ポート 1/0/1，1/0/2 に設定されている channel-group mode コマンドも自動的に削除されます。

21.3　リンクアグリゲーション拡張機能の解説

21.3.1　スタンバイリンク機能

(1)　解説

チャネルグループ内にあらかじめ待機用のポートを用意しておき，運用中のポートで障害が発生したときに待機用のポートに切り替えることによって，グループとして運用するポート数を維持する機能です。この機能を使用すると，障害時に帯域の減少を防ぐことができます。

この機能は，スタティックリンクアグリゲーションだけ使用できます。

(2)　スタンバイリンクの選択方法

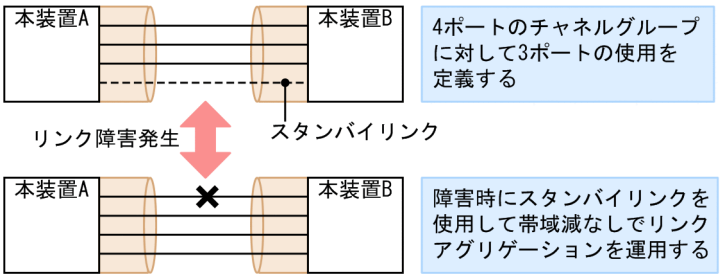
コンフィグレーションでチャネルグループとして運用する最大ポート数を設定します。グループに属するポート数が指定された最大ポート数を超えた分のポートが待機用ポートになります。

待機用ポートは，まずコンフィグレーションで設定するポート優先度，次にポート番号の順で，選択優先度の高い順に決定されます。つまり，ポート優先度が同じ場合は，ポート番号で判断します。待機用ポートの決定基準を，選択優先度の高い順に次に示します。

1. ポート優先度
   優先度の値の大きいポートから待機用ポートとして選択されます。
2. ポート番号
   ポート番号の大きい順に待機用ポートとして選択されます。

スタンバイリンク機能の例を次の図に示します。この例では，グループに属するポート数を 4，運用する最大ポート数を 3 としています。

図 21–3　スタンバイリンク機能の構成例



(3)　スタンバイリンクのモード

スタンバイリンク機能には，次に示す二つのモードがあります。

- リンクダウンモード
  スタンバイリンクをリンクダウン状態にします。スタンバイリンク機能をサポートしていない対向装置も待機用ポートにすることができます。
- 非リンクダウンモード
  スタンバイリンクをリンクダウン状態にしないで，送信だけを停止します。リンクアップ状態のため，待機中のポートでも障害を監視できます。また，待機中のポートは送信だけを停止して，受信は行いま

す。スタンバイリンク機能をサポートしていない対向装置は，リンクダウンが伝わらないためスタンバイリンク上で送信を継続しますが，そのような対向装置とも接続できます。

リンクダウンモードを使用している場合，運用中のポートが一つのとき，そのポートで障害が発生すると，待機用のポートに切り替わる際にチャネルグループがいったんダウンします。非リンクダウンモードの場合，ダウンせずに待機用ポートを使用します。

運用中のポートが一つの状態とは，次に示す状態です。

- コンフィグレーションコマンド max-active-port で 1 を設定している状態。

21.3.2　離脱ポート制限機能

離脱ポート制限機能は，リンクに障害が発生したポートを離脱して残りのポートで運用を継続する機能を抑止します。チャネルグループのどれかのポートに障害が発生するとグループ全体を障害とみなして，該当チャネルグループの運用を停止します。グループ内の全ポートが復旧するとグループの運用を再開します。

アップリンク・リダンダントなどの冗長化機能と合わせて運用することで，チャネルグループ内に 1 ポートだけ障害が発生した場合でも，グループ単位で経路を切り替えることができます。

この機能は LACP リンクアグリゲーションだけ使用できます。

離脱ポート制限機能の集約動作は，チャネルグループで接続する装置間で，優先度の高い装置が，自装置および対向装置のチャネルグループ内の全ポートで集約可能な状態と判断できた場合に集約します。そうすることで，一部のポートだけが集約することがないようにしており，帯域保証しています。

優先度は，まずコンフィグレーションで設定する LACP システム優先度，次にチャネルグループの MAC アドレスの順で判断されます。つまり，LACP システム優先度が同じ場合は，チャネルグループの MAC アドレスで判断します。

チャネルグループ内の全ポートが集約可能か判定する装置の決定基準を，選択優先度の高い順に次に示します。

1. LACP システム優先度
   LACP システム優先度の値が小さい装置が優先されます。
2. チャネルグループの MAC アドレス
   MAC アドレスの小さい装置が優先されます。

21.4　リンクアグリゲーション拡張機能のコマンドガイド

21.4.1　コマンド一覧

リンクアグリゲーション拡張機能のコンフィグレーションコマンド一覧を次の表に示します。

表 21-4　コンフィグレーションコマンド一覧

コマンド名	説明
channel-group lacp system-priority	システム優先度をチャネルグループごとに設定します。離脱ポート制限機能で集約条件を判定する装置を決定します。
channel-group max-active-port	スタンバイリンク機能を設定し，最大ポート数を指定します。
channel-group max-detach-port	離脱ポート制限機能を設定します。
lacp port-priority	ポート優先度を設定します。スタンバイリンクを選択するために使用します。
lacp system-priority	システム優先度のデフォルト値を設定します。離脱ポート制限機能で集約条件を判定する装置を決定します。

21.4.2　スタンバイリンク機能のコンフィグレーション

[設定のポイント]

チャネルグループにスタンバイリンク機能を設定して，同時に最大ポート数を設定します。また，リンクダウンモード，非リンクダウンモードのどちらかを設定します。スタンバイリンク機能は，スタティックリンクアグリゲーションだけで使用できます。

待機用ポートはポート優先度によって設定し，優先度が低いポートからスタンバイリンクに選択します。ポート優先度は値が小さいほど高い優先度になります。

[コマンドによる設定]

1. **(config)# interface port-channel 10**

   チャネルグループ 10 のポートチャネル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)# channel-group max-active-port 3**

   チャネルグループ 10 にスタンバイリンク機能を設定して，最大ポート数を 3 に設定します。チャネルグループ 10 はリンクダウンモードで動作します。

3. **(config-if)# exit**

   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 port-channel 20**

   (config-if)# channel-group max-active-port 1 no-link-down

   (config-if)# exit

   チャネルグループ 20 のポートチャネルインタフェースコンフィグレーションモードに移行して，スタンバイリンク機能を設定します。最大ポート数を 1 とし，非リンクダウンモードを設定します。

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

   (config-if)# channel-group 20 mode on

   (config-if)# lacp port-priority 300

チャネルグループ 20 にポート 1/0/1 を登録して，ポート優先度を 300 に設定します。ポート優先度は値が小さいほど優先度が高く，ポート優先度のデフォルト値の 128 よりもスタンバイリンクに選択されやすくなります。

21.4.3　離脱ポート制限機能のコンフィグレーション

[設定のポイント]

チャネルグループに離脱ポート制限機能を設定します。本コマンドではチャネルグループから離脱することを許容する最大ポート数に 0 と 7 のどちらかを指定します。7 を指定した場合は離脱ポート制限機能を設定しない場合と同じです。

離脱ポート制限機能をサポートしている装置と接続する場合，接続先の装置と本設定を合わせてください。離脱ポート制限機能をサポートしていない装置と接続する場合，本装置の LACP システム優先度を高くしてください。LACP システム優先度は値が小さいほど優先度が高くなります。

離脱ポート制限機能は，LACP リンクアグリゲーションだけで使用できます。

[コマンドによる設定]

1. **(config)# interface port-channel 10**

   チャネルグループ 10 のポートチャネル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)# channel-group max-detach-port 0**

   チャネルグループ 10 に離脱ポート制限機能を設定します。離脱を許容する最大ポート数を 0 とし，障害などによって 1 ポートでも離脱した場合にチャネルグループ全体を障害とみなします。

3. **(config-if)# channel-group lacp system-priority 100**

   チャネルグループ 10 のシステム優先度を 100 に設定します。

22 レイヤ２スイッチ概説

この章では，本装置の機能のうち，OSI 階層モデルの第 2 レイヤでデータを中継するレイヤ 2 スイッチ機能の概要について説明します。

22.1　概要

22.1.1　MAC アドレス学習

レイヤ 2 スイッチはフレームを受信すると送信元 MAC アドレスを MAC アドレステーブルに登録します。MAC アドレステーブルの各エントリには，MAC アドレスとフレームを受信したポートおよびエージングタイマを記録します。フレームを受信するごとに送信元 MAC アドレスに対応するエントリを更新します。

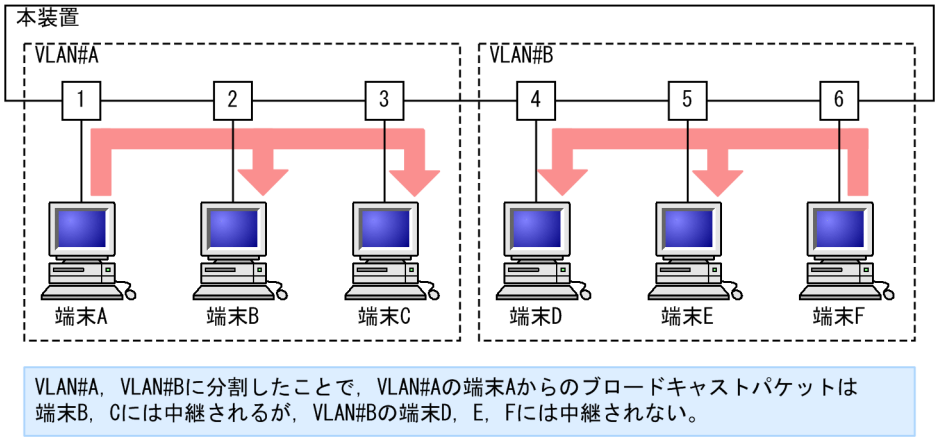
レイヤ 2 スイッチは，MAC アドレステーブルのエントリに従ってフレームを中継します。フレームの宛先 MAC アドレスに一致するエントリがあると，そのエントリのポートに中継します（エントリのポートが受信したポートである場合は中継しません）。一致するエントリがない場合，受信したポート以外のすべてのポートにフレームを中継します。この中継をフラッディングと呼びます。

22.1.2　VLAN

VLAN は，スイッチ内を仮想的なグループに分ける機能のことです。スイッチ内を複数の VLAN にグループ分けすることによってブロードキャストドメインを分割します。これによって，ブロードキャストフレームの抑制や，セキュリティの強化を図ることができます。

VLAN の概要を次の図に示します。VLAN#A と VLAN#B の間ではブロードキャストドメインが分割されるため，フレームが届くことはありません。

図 22-1　VLAN の概要



22.2　サポート機能

レイヤ 2 スイッチ機能として，本装置がサポートする機能を次の表に示します。

これらの機能は，組み合わせて利用できる機能とできない機能があります。機能の組み合わせ制限については，次項で説明します。

表 22-1　レイヤ 2 スイッチサポート機能

サポート機能		機能概要
MAC アドレス学習		MAC アドレステーブルに登録する MAC アドレスの学習機能
VLAN	ポート VLAN	ポート単位にスイッチ内を仮想的なグループに分ける機能
	プロトコル VLAN	プロトコル単位にスイッチ内を仮想的なグループに分ける機能
	MAC VLAN	送信元の MAC アドレス単位にスイッチ内を仮想的なグループに分ける機能
	デフォルト VLAN	コンフィグレーションが未設定のときにデフォルトで所属する VLAN
	ネイティブ VLAN	トランクポート，プロトコルポート，MAC ポートでの Untagged フレームを扱うポート VLAN の呼称
	トンネリング	複数ユーザの VLAN をほかの VLAN に集約して「トンネル」する機能
	Tag 変換	VLAN Tag を変換して別の VLAN に中継する機能
	L2 プロトコルフレーム透過機能	レイヤ 2 のプロトコルのフレームを中継する機能 スパニングツリー（BPDU），IEEE802.1X（EAP）を透過します。
スパニングツリー	PVST+	VLAN 単位のスイッチ間のループ防止機能
	シングルスパニングツリー	装置単位のスイッチ間のループ防止機能
	マルチプルスパニングツリー	MST インスタンス単位のスイッチ間のループ防止機能
Ring Protocol		リングトポロジーでのレイヤ 2 ネットワークの冗長化機能
IGMP snooping/MLD snooping		レイヤ 2 スイッチで VLAN 内のマルチキャストトラフィック制御機能
ポート間中継遮断機能		指定したポート間ですべての通信を遮断する機能

22.2.1　本装置の MAC アドレス

(1)　装置 MAC アドレス

本装置は，装置を識別するための MAC アドレスを一つ持ちます。この MAC アドレスのことを装置 MAC アドレスと呼びます。装置 MAC アドレスは，レイヤ 3 インタフェースの MAC アドレスやスパニングツリーなどのプロトコルの装置識別子として使用します。

(2)　装置 MAC アドレスを使用する機能

装置 MAC アドレスを使用する機能を次の表に示します。

表 22-2　装置 MAC アドレスを使用する機能

機能	用途
リンクアグリゲーションの LACP	装置識別子
VLAN	VLAN インタフェースの MAC アドレス
スパニングツリー	装置識別子
アップリンク・リダンダント（フラッシュ制御フレーム送信）	装置識別子
L2 ループ検知	装置識別子
IEEE802.3ah/UDLD	装置識別子
CFM	装置識別子
LLDP	装置識別子

22.3　レイヤ 2 スイッチ機能と他機能の共存について

レイヤ 2 スイッチ機能と併用する際，共存不可または制限事項がある機能があります。機能間の共存についての制限事項を次の表に示します。

なお，これらの表では各機能間の共存関係で，制限のある項目だけを示しています。

表 22–3　MAC アドレス学習での制限事項

使用したい機能	制限のある機能	制限の内容
MAC アドレス学習	アップリンク・リダンダント	一部制限あり※

注※

スタティックエントリの設定は，アップリンクポートで使用できません。

表 22–4　VLAN での制限事項

使用したい機能		制限のある機能	制限の内容
VLAN 種別	ポート VLAN	VLAN トンネリング	一部制限あり※1
		レイヤ 2 認証	一部制限あり※2
		ポートミラーリング（ミラーポート）	一部制限あり※3
	プロトコル VLAN	デフォルト VLAN	共存不可
		VLAN トンネリング	
		PVST+	
		レイヤ 2 認証	一部制限あり※2
		ポートミラーリング（ミラーポート）	共存不可
	MAC VLAN	デフォルト VLAN	共存不可
		VLAN トンネリング	
		PVST+	
		レイヤ 2 認証	一部制限あり※2
		ポートミラーリング（ミラーポート）	共存不可
デフォルト VLAN		プロトコル VLAN	共存不可
		MAC VLAN	
		IGMP snooping	
		MLD snooping	
		レイヤ 2 認証	一部制限あり※2
		ポートミラーリング（ミラーポート）	一部制限あり※3
VLAN 拡張機能	Tag 変換	PVST+	共存不可
		IGMP snooping	

使用したい機能		制限のある機能	制限の内容
		MLD snooping	
		アップリンク・リダンダント	一部制限あり※4
	VLAN トンネリング	ポート VLAN	一部制限あり※1
		プロトコル VLAN	共存不可
		MAC VLAN	
		PVST+	
		シングルスパニングツリー	
		マルチプルスパニングツリー	
		IGMP snooping	
		MLD snooping	
		レイヤ 2 認証	一部制限あり※2
		DHCP snooping	共存不可
		アップリンク・リダンダント	一部制限あり※4
	L2 プロトコルフレーム透過機能（BPDU）	PVST+	共存不可
		シングルスパニングツリー	
		MSTP	
	L2 プロトコルフレーム透過機能（EAP）	レイヤ 2 認証	一部制限あり※2
	ポート間中継遮断機能	IGMP snooping	一部制限あり※5
		MLD snooping	一部制限あり※5
		レイヤ 2 認証	一部制限あり※6
		DHCP snooping	一部制限あり※7
		GSRP aware	一部制限あり※8
		CFM	一部制限あり※9

注※1

VLAN トンネリング機能を使用する場合は，トランクポートでネイティブ VLAN を使用しないでください。

注※2

「コンフィグレーションガイド Vol.2」「5.2.1　レイヤ 2 認証と他機能との共存」を参照してください。

注※3

802.1Q Tag 付与機能を使用している場合だけ，使用できます。

注※4

アップリンクポートでは使用できません。

注※5

IGMP snooping/MLD snooping を有効にした場合，ポート間中継遮断機能を設定しても本装置が受信した IGMP メッセージおよび MLD メッセージや，ルーティングプロトコルなどの制御パケットは遮断の対象になりません。IGMP snooping/MLD snooping が転送するルーティングプロトコルなどの制御パケットについては，「29.5 IGMP snooping/MLD snooping 使用時の注意事項」の「(2)　制御パケットのフラッディング」を参照してください。

注※6

認証前端末からの ARP パケットのリレー機能を有効にした場合，ポート間中継遮断機能を設定しても認証前状態の端末から送信される ARP パケットの転送は遮断の対象になりません。

注※7

DHCP snooping を有効にした場合，ポート間中継遮断機能を設定しても本装置が受信したすべての DHCP パケットは遮断の対象になりません。また，ダイナミック ARP 検査も有効にした場合，本装置が受信したすべての ARP パケットも遮断の対象になりません。

注※8

通信を遮断したポートで GSRP スイッチと接続した場合，GSRP Flush request フレームは遮断の対象になりません。

注※9

CFM を有効にした場合，ポート間中継遮断機能を設定しても本装置が受信したリンクトレースメッセージは遮断の対象になりません。

表 22-5　スパニングツリーでの制限事項

使用したい機能	制限のある機能	制限の内容
PVST+	プロトコル VLAN	共存不可
	MAC VLAN	
	VLAN トンネリング	
	Tag 変換	
	L2 プロトコルフレーム透過機能(BPDU)	
	マルチプルスパニングツリー	
	Ring Protocol	
	レイヤ 2 認証	一部制限あり※
	アップリンク・リダンダント	共存不可
シングルスパニングツリー	VLAN トンネリング	共存不可
	L2 プロトコルフレーム透過機能(BPDU)	
	マルチプルスパニングツリー	
	Ring Protocol	
	レイヤ 2 認証	一部制限あり※
	アップリンク・リダンダント	共存不可
マルチプルスパニングツリー	VLAN トンネリング	共存不可
	L2 プロトコルフレーム透過機能(BPDU)	

使用したい機能	制限のある機能	制限の内容
	シングルスパニングツリー	
	PVST+	
	ループガード	
	Ring Protocol	
	レイヤ 2 認証	一部制限あり※
	アップリンク・リダンダント	共存不可

注※

「コンフィグレーションガイド Vol.2」「5.2.1　レイヤ 2 認証と他機能との共存」を参照してください。

表 22-6　Ring Protocol での制限事項

使用したい機能	制限のある機能	制限の内容
Ring Protocol	PVST+	共存不可
	シングルスパニングツリー	
	マルチプルスパニングツリー	
	レイヤ 2 認証	一部制限あり※1
	アップリンク・リダンダント	一部制限あり※2

注※1

「コンフィグレーションガイド Vol.2」「5.2.1　レイヤ 2 認証と他機能との共存」を参照してください。

注※2

リングポートでは使用できません。

表 22-7　IGMP/MLD snooping での制限事項

使用したい機能	制限のある機能	制限の内容
IGMP snooping	デフォルト VLAN	共存不可
	Tag 変換	
	VLAN トンネリング	
	ポート間中継遮断機能	一部制限あり※1
	レイヤ 2 認証	一部制限あり※2
MLD snooping	デフォルト VLAN	共存不可
	Tag 変換	
	VLAN トンネリング	
	ポート間中継遮断機能	一部制限あり※1

注※1

IGMP snooping/MLD snooping を有効にした場合，ポート間中継遮断機能を設定しても本装置が受信したルーティングプロトコルなどの制御パケットは遮断の対象になりません。IGMP snooping/MLD snooping が転送する

ルーティングプロトコルなどの制御パケットについては,「29.5　IGMP snooping/MLD snooping 使用時の注意事項」の「(2)　制御パケットのフラッディング」を参照してください。

注※2

「コンフィグレーションガイド Vol.2」「5.2.1　レイヤ 2 認証と他機能との共存」を参照してください。

23 MAC アドレス学習

この章では，MAC アドレス学習機能の解説と操作方法について説明します。

23.1　解説

本装置は，フレームを宛先 MAC アドレスによって目的のポートへ中継するレイヤ 2 スイッチングを行います。宛先 MAC アドレスによって特定のポートだけに中継することで，ユニキャストフレームのフラッディングによるむだなトラフィックを抑止します。

MAC アドレス学習では，チャネルグループを一つのポートとして扱います。

23.1.1　送信元 MAC アドレス学習

すべての受信フレームを MAC アドレス学習の対象とし，送信元 MAC アドレスを学習して MAC アドレステーブルに登録します。登録した MAC アドレスはエージングタイムアウトまで保持します。

MAC アドレス学習は VLAN 単位に行い，MAC アドレステーブルは MAC アドレスと VLAN のペアによって管理します。異なる VLAN であれば，同一の MAC アドレスを学習することもできます。

23.1.2　MAC アドレス学習の移動検出

(1)　VLAN で MAC アドレスを学習した場合

学習済みの送信元 MAC アドレスと VLAN の組み合わせを持つフレームを学習時と異なるポートから受信した場合，その MAC アドレスが移動したものと見なして MAC アドレステーブルのエントリを再登録（移動先ポートに関する上書き）します。

(2)　チャネルグループで学習した場合

チャネルグループで学習した MAC アドレスについては, そのチャネルグループに含まれないポートからフレームを受信した場合に MAC アドレスが移動したものと見なします。

23.1.3　学習 MAC アドレスのエージング

学習したエントリは, エージングタイム内に同じ送信元 MAC アドレスからフレームを受信しなかった場合はエントリを削除します。これによって，不要なエントリの蓄積を防止します。エージングタイム内にフレームを受信した場合は, エージングタイマを更新しエントリを保持します。エージングタイムを設定できる範囲を次に示します。

- エージングタイムの範囲：0，10～1000000（秒）
  0 は無限を意味し，エージングしません。
- デフォルト値：300（秒）

学習したエントリを削除するまでに最大でエージング時間の 2 倍掛かることがあります。

また, ポートがダウンした場合には該当ポートから学習したエントリをすべて削除します。チャネルグループで学習したエントリは，そのチャネルグループがダウンした場合に削除します。

23.1.4　MAC アドレスによるレイヤ 2 スイッチング

MAC アドレス学習の結果に基づいてレイヤ 2 スイッチングを行います。宛先 MAC アドレスに対応するエントリを保持している場合，学習したポートだけに中継します。

レイヤ 2 スイッチングの動作仕様を次の表に示します。

表 23-1　レイヤ 2 スイッチングの動作仕様

宛先 MAC アドレスの種類	動作概要
学習済みのユニキャスト	学習したポートへ中継します。
未学習のユニキャスト	受信した VLAN に所属する全ポートへ中継します。
ブロードキャスト	受信した VLAN に所属する全ポートへ中継します。
マルチキャスト	受信した VLAN に所属する全ポートへ中継します。ただし，IGMP snooping，MLD snooping 動作時は snooping 機能の学習結果に従って中継します。

23.1.5　スタティックエントリの登録

受信フレームによるダイナミックな学習のほかに，ユーザ指定によってスタティックに MAC アドレスを登録できます。ユニキャスト MAC アドレスに対して一つのポートまたはチャネルグループを指定できます。また，ポートを指定するのではなく「廃棄」を指定することもできます。その場合，指定の宛先 MAC アドレスまたは送信元 MAC アドレスのフレームはどのポートにも中継されないで廃棄されます。

ユニキャスト MAC アドレスに対してスタティックに登録を行うと，そのアドレスについてダイナミックな学習は行いません。すでに学習済みのエントリは MAC アドレステーブルから削除してスタティックエントリを登録します。また，指定された MAC アドレスが送信元のフレームをポートまたはチャネルグループ以外から受信した場合は，そのフレームを廃棄します。スタティックエントリの指定パラメータを次の表に示します。

表 23-2　スタティックエントリの指定パラメータ

項番	指定パラメータ	説明
1	MAC アドレス	ユニキャスト MAC アドレスが指定できます。
2	VLAN	このエントリを登録する VLAN を指定します。
3	送信先ポート／廃棄指定	一つのポートまたはチャネルグループを指定できます。また，項番 1，2 に該当するフレームを廃棄する指定ができます。

23.1.6　MAC アドレス学習抑止

受信フレームによるダイナミックな MAC アドレス学習に制限を設けて，使用する MAC アドレステーブルのエントリを管理できます。

VLAN ごとに，ダイナミックな MAC アドレス学習を抑止できます。ダイナミックな MAC アドレス学習を抑止すると，学習抑止の対象となる VLAN で受信したフレームはフラッディングします。

すでに MAC アドレスを学習しているときに MAC アドレス学習を抑止すると，MAC アドレス学習を抑止した VLAN で学習していた MAC アドレステーブルのエントリは削除します。

23.1.7　MAC アドレステーブルのクリア

本装置は運用コマンドやプロトコルの動作などによって MAC アドレステーブルをクリアします。

VLAN 単位で MAC アドレス学習したエントリをクリアする契機を次の表に示します。

表 23-3　MAC アドレステーブルをクリアする契機

契機	説明
ポートダウン※1	該当ポートから学習したエントリを削除します。
チャネルグループダウン※2	該当チャネルグループから学習したエントリを削除します。
運用コマンド clear mac-address-table の実行	パラメータに従って MAC アドレステーブルをクリアします。
MAC アドレステーブル Clear 用 MIB (プライベート MIB)	セット時に MAC アドレステーブルをクリアします。
スパニングツリーのトポロジー変更	[本装置でスパニングツリーを構成] トポロジー変更を検出した時に MAC アドレステーブルをクリアします。
	[スパニングツリーと Ring Protocol を併用しているネットワーク構成で本装置がリングノードとして動作] Ring Protocol と併用している装置がトポロジー変更を検出した時に送信するフラッシュ制御フレームを受信した場合，MAC アドレステーブルをクリアします。
GSRP のマスタ／バックアップ切り替え	GSRP スイッチがマスタ状態になった時に送信される GSRP Flush request フレームを受信した場合，MAC アドレステーブルをクリアします。
Ring Protocol による経路の切り替え	経路切り替え時にマスタノードから送信されるフラッシュ制御フレームを受信した場合，MAC アドレステーブルをクリアします。 フラッシュ制御フレーム受信待ち保護時間のタイムアウト時に MAC アドレステーブルをクリアします。
	多重障害監視機能適用時，バックアップリングの切り替え／切り戻しに伴い共有ノードから送信されるフラッシュ制御フレームを受信した場合，MAC アドレステーブルをクリアします。
	経路切り替え時にマスタノードから送信される隣接リング用フラッシュ制御フレームを受信した場合，MAC アドレステーブルをクリアします。
アップリンク・リダンダント機能によるプライマリポートとセカンダリポートの切り替え	プライマリポートからセカンダリポートへの切り替え時，およびセカンダリポートからプライマリポートへの切り戻し時に送信されるフラッシュ制御フレームを受信した場合，MAC アドレステーブルをクリアします。
MAC アドレス学習抑止のコンフィグレーションの設定	コンフィグレーションコマンド no mac-address-table learning で MAC アドレス学習抑止を設定した場合，該当 VLAN で学習したエントリを削除します。

注※1

回線障害，運用コマンド inactivate の実行，コンフィグレーションコマンド shutdown の設定などによるポートダウン。

注※2

LACP，回線障害，コンフィグレーションコマンド shutdown の設定などによるチャネルグループダウン。

23.1.8　注意事項

(1)　他機能との共存

(a)　レイヤ 2 スイッチ機能との共存

「22.3　レイヤ 2 スイッチ機能と他機能の共存について」を参照してください。

(b)　レイヤ 2 認証との共存

「コンフィグレーションガイド Vol.2」「5.2.1　レイヤ 2 認証と他機能との共存」を参照してください。

23.2　コマンドガイド

23.2.1　コマンド一覧

MAC アドレス学習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 23-4　コンフィグレーションコマンド一覧

コマンド名	説明
mac-address-table aging-time	MAC アドレス学習のエージングタイムを設定します。
mac-address-table learning	ダイナミックな MAC アドレス学習の可否を設定します。
mac-address-table static	スタティックエントリを設定します。

MAC アドレス学習の運用コマンド一覧を次の表に示します。

表 23-5　運用コマンド一覧

コマンド名	説明
show mac-address-table	MAC アドレステーブルの情報を表示します。 learning-counter パラメータを指定すると，ポート単位に MAC アドレス学習の学習アドレス数と MAC アドレス学習の移動回数を表示します。
clear mac-address-table	MAC アドレステーブルをクリアします。
show vlan※	VLAN の MAC アドレス学習状態を表示します。

注※

「運用コマンドレファレンス」「23　VLAN」を参照してください。

23.2.2　エージングタイムの設定

[設定のポイント]

MAC アドレス学習のエージングタイムを変更できます。設定は装置単位です。設定しない場合，エージングタイムは 300 秒で動作します。

[コマンドによる設定]

1. **(config)# mac-address-table aging-time 600**

   エージングタイムを 600 秒に設定します。

23.2.3　スタティックエントリの設定

スタティックエントリを登録すると，指定した MAC アドレスについて MAC アドレス学習をしないで，常に登録したエントリに従ってフレームを中継するため，MAC アドレスのエージングによるフラッディングを回避できます。本装置に直接接続したサーバなどのように，ポートの移動がなく，かつトラフィック量の多い端末などに有効な機能です。

スタティックエントリには，MAC アドレス，VLAN および出力先を指定します。出力先はポート，チャネルグループ，廃棄のどれかを指定します。

(1)　出力先にポートを指定するスタティックエントリ

[設定のポイント]

出力先にポートを指定した例を示します。

[コマンドによる設定]

1. **(config)# mac-address-table static 0012.e200.1122 vlan 10 interface gigabitethernet 1/0/1**

   VLAN 10 で，宛先 MAC アドレス 0012.e200.1122 のフレームの出力先をポート 1/0/1 に設定します。

[注意事項]

VLAN 10 で，送信元 MAC アドレス 0012.e200.1122 のフレームをポート 1/0/1 以外から受信した場合は廃棄します。

(2)　出力先にリンクアグリゲーションを指定するスタティックエントリ

[設定のポイント]

出力先にリンクアグリゲーションを指定した例を示します。

[コマンドによる設定]

1. **(config)# mac-address-table static 0012.e200.1122 vlan 10 interface port-channel 5**

   VLAN 10 で, 宛先 MAC アドレス 0012.e200.1122 のフレームの出力先をチャネルグループ 5 に設定します。

[注意事項]

VLAN 10 で, 送信元 MAC アドレス 0012.e200.1122 のフレームをチャネルグループ 5 以外から受信した場合は廃棄します。

(3)　廃棄を指定するスタティックエントリ

[設定のポイント]

指定した MAC アドレス宛および指定した MAC アドレスからのフレームを廃棄に設定します。

[コマンドによる設定]

1. **(config)# mac-address-table static 0012.e200.1122 vlan 10 drop**

   VLAN 10 で，宛先および送信元 MAC アドレス 0012.e200.1122 のフレームを廃棄に設定します。

23.2.4　MAC アドレス学習抑止の設定

[設定のポイント]

MAC アドレス学習をする場合はコンフィグレーションの設定は不要です。例えば, 特定の VLAN に対しての MAC アドレス学習を抑止したい場合に，MAC アドレス学習をしない VLAN に対してだけ MAC アドレス学習抑止を設定します。

[コマンドによる設定]

1. **(config)# no mac-address-table learning vlan 100**

   VLAN100 では MAC アドレス学習を抑止します。

24 VLAN

VLAN はスイッチ内を仮想的なグループに分ける機能です。この章では，VLAN の解説と操作方法について説明します。

24.1 VLAN 基本機能の解説

この節では，VLAN の概要を説明します。

24.1.1 VLAN の種類

本装置がサポートする VLAN の種類を次の表に示します。

表 24-1 サポートする VLAN の種類

項目	概要
ポート VLAN	ポート単位に VLAN のグループを分けます。
プロトコル VLAN	プロトコル単位に VLAN のグループを分けます。
MAC VLAN	送信元の MAC アドレス単位に VLAN のグループを分けます。

24.1.2 ポートの種類

(1) 解説

本装置は，ポートの設定によって使用できる VLAN が異なります。使用したい VLAN の種類に応じて各ポートの種類を設定する必要があります。ポートの種類を次の表に示します。

表 24-2 ポートの種類

ポートの種類	概要	使用する VLAN
アクセスポート	ポート VLAN として Untagged フレームを扱います。 このポートでは，すべての Untagged フレームを一つのポート VLAN で扱います。	ポート VLAN MAC VLAN
プロトコルポート	プロトコル VLAN として Untagged フレームを扱います。 このポートでは，フレームのプロトコルによって VLAN を決定します。	プロトコル VLAN ポート VLAN
MAC ポート	MAC VLAN として Untagged フレームを扱います。 このポートでは，フレームの送信元 MAC アドレスによって VLAN を決定します。	MAC VLAN ポート VLAN
トランクポート	すべての種類の VLAN で Tagged フレームを扱います。 このポートでは，VLAN Tag によって VLAN を決定します。	すべての種類の VLAN
トンネリングポート	VLAN トンネリングのポート VLAN として，フレームの Untagged と Tagged を区別しないで扱います。このポートでは，すべてのフレームを一つのポート VLAN で扱います。	ポート VLAN

アクセスポート，プロトコルポート，MAC ポートは Untagged フレームを扱うポートです。これらのポートで Tagged フレームを扱うことはできません。Tagged フレームを受信したときは廃棄し，また送信することもありません。

Tagged フレームはトランクポートでだけ扱うことができます。トランクポートの Untagged フレームはネイティブ VLAN が扱います。

トンネリングポートは，VLAN トンネリングをするポートで，フレームが Untagged か，Tagged かを区別しないで扱います。

ポートの種類ごとの，使用できる VLAN の種類を次の表に示します。プロトコル VLAN と MAC VLAN は同じポートで使用できません。VLAN Tag を扱うトランクポートはすべての VLAN で同じポートを使用できます。

表 24-3　ポート上で使用できる VLAN

ポートの種類	VLAN の種類		
	ポート VLAN	プロトコル VLAN	MAC VLAN
アクセスポート	○	×	○
プロトコルポート	○	○	×
MAC ポート	○	×	○
トランクポート	○	○	○
トンネリングポート	○	×	×

(凡例)　○：使用できる　×：使用できない

(2)　ポートのネイティブ VLAN

アクセスポート，トンネリングポート以外のポート（プロトコルポート，MAC ポート，トランクポート）では, それぞれの設定と一致しないフレームを受信する場合があります。例えば, プロトコルポートで IPv4 プロトコルだけ設定していたときに IPv6 のフレームを受信した場合です。アクセスポート，トンネリングポート以外ではこのようなフレームを扱うためにポート VLAN を一つ設定することができます。この VLAN のことを，各ポートでのネイティブ VLAN と呼びます。

アクセスポート，トンネリングポート以外の各ポートでは，ポートごとに作成済みのポート VLAN をネイティブ VLAN に設定できます。コンフィグレーションで指定がないポートは，VLAN 1（デフォルト VLAN）がネイティブ VLAN になります。

24.1.3　デフォルト VLAN

(1)　概要

本装置では，コンフィグレーションが未設定の状態であっても，装置の起動後すぐにレイヤ 2 中継ができます。このとき，すべてのポートはアクセスポートとなり，デフォルト VLAN と呼ぶ VLAN ID 1 の VLAN に属します。デフォルト VLAN は常に存在し，VLAN ID「1」は変更できません。

(2)　デフォルト VLAN から除外するポート

アクセスポートは，コンフィグレーションが未設定の場合は VLAN 1（デフォルト VLAN）に属します。しかし，コンフィグレーションによってデフォルト VLAN の自動的な所属から除外する場合があります。次に示すポートはデフォルト VLAN に自動的に所属しなくなります。

- アクセスポートで VLAN 1 以外を指定したポート
- VLAN トンネリング機能を設定した場合の全ポート
- ポートミラーリングのミラーポート（802.1Q Tag 付与機能を使用していない場合）

アクセスポート以外のポート（プロトコルポート，MAC ポート，トランクポート，トンネリングポート）は自動的に VLAN に所属することはありません。

24.1.4 VLAN の優先順位

(1) フレーム受信時の VLAN 判定の優先順位

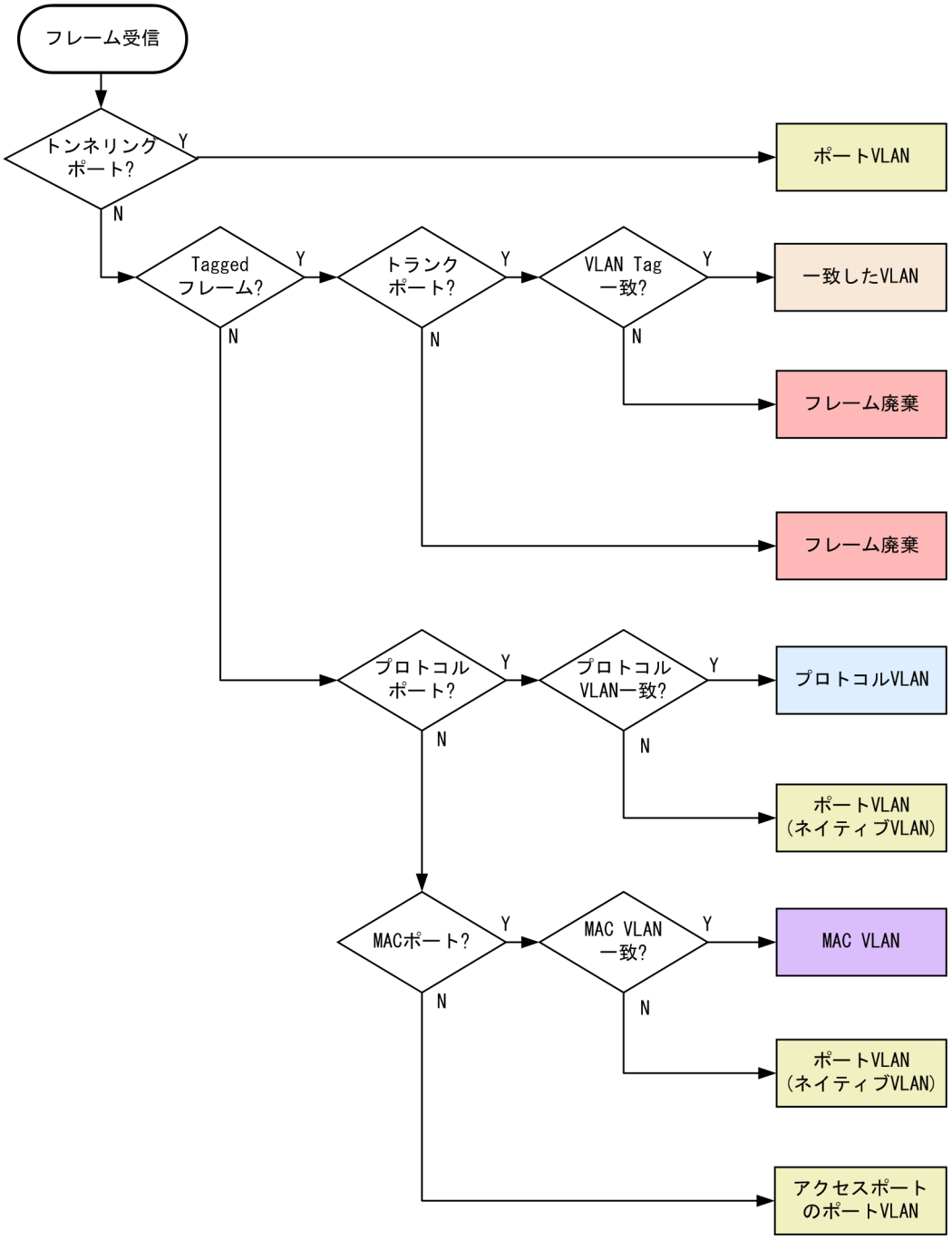
フレームを受信したとき，受信したフレームの VLAN を判定します。VLAN 判定の優先順位を次の表に示します。

表 24-4 VLAN 判定の優先順位

ポートの種類	VLAN 判定の優先順位
アクセスポート	ポート VLAN
プロトコルポート	プロトコル VLAN ＞ポート VLAN（ネイティブ VLAN）
MAC ポート	MAC VLAN ＞ポート VLAN（ネイティブ VLAN）
トランクポート	VLAN Tag ＞ポート VLAN（ネイティブ VLAN）
トンネリングポート	ポート VLAN

VLAN 判定のアルゴリズムを次の図に示します。

図 24-1　VLAN 判定のアルゴリズム



24.1.5　VLAN Tag

(1)　概要

IEEE 802.1Q 規定による VLAN Tag(イーサネットフレーム中に Tag と呼ばれる識別子を挿入する方法)を使用して，一つのポートに複数の VLAN を構築できます。

VLAN Tag はトランクポートで使用します。トランクポートはその対向装置も VLAN Tag を認識できなければなりません。

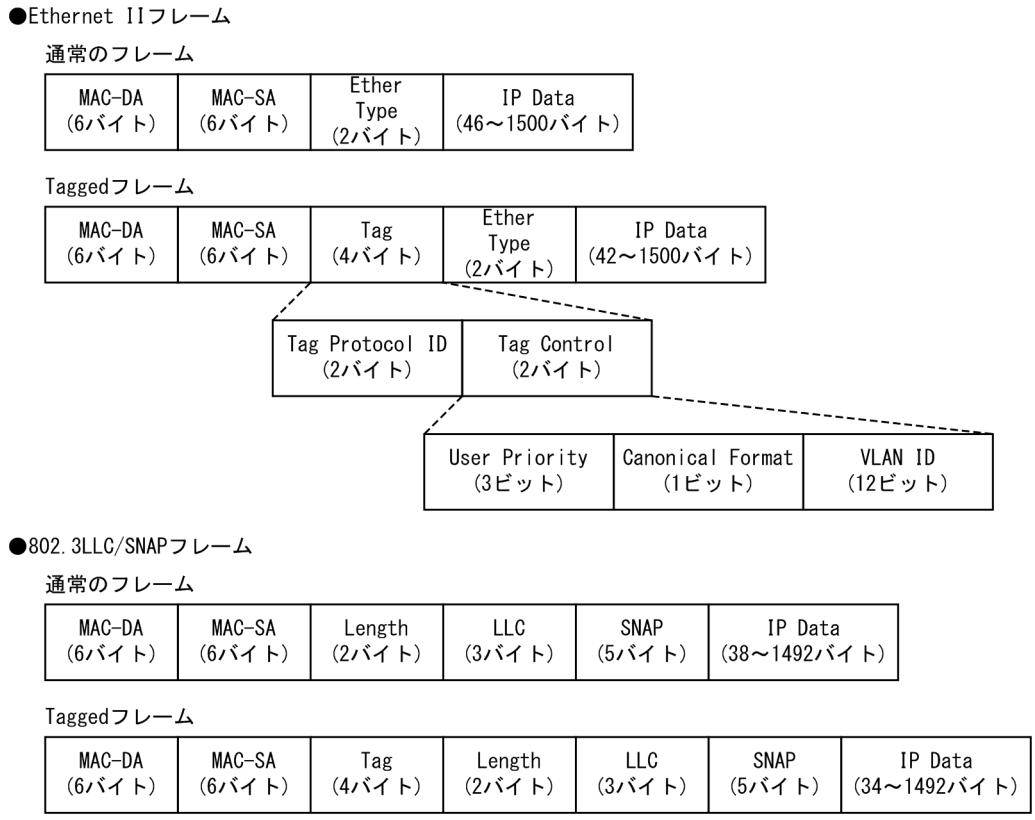
また，本装置では，VLAN Tag は 2 段までのフレームがサポート対象です。3 段以上の場合は，フレームを正しく中継できないことがあります。

(2) プロトコル仕様

VLAN Tag はイーサネットフレームに Tag と呼ばれる識別子を埋め込むことで，VLAN 情報（=VLAN ID）を離れたセグメントへと伝えることができます。

Tagged フレームのフォーマットを次の図に示します。VLAN Tag を挿入するイーサネットフレームのフォーマットは，Ethernet V2 フォーマットと 802.3 フォーマットの 2 種類があります。

図 24-2 Tagged フレームのフォーマット



VLAN Tag のフィールドの説明を次の表に示します。

表 24-5 VLAN Tag のフィールド

フィールド	説明	本装置の条件
TPID (Tag Protocol ID)	IEEE802.1Q VLAN Tag が続くことを示す Ether Type 値を示します。	ポートごとに任意の値を設定できます。
User Priority	IEEE802.1D のプライオリティを示します。	コンフィグレーションで 8 段階のプライオリティレベルを選択できます。
CF (Canonical Format)	MAC ヘッダ内の MAC アドレスが標準フォーマットに従っているかどうかを示します。	本装置では標準(0)だけをサポートします。

フィールド	説明	本装置の条件
VLAN ID	VLAN ID を示します。※	ユーザが使用できる VLAN ID は 1～4094 です。

注※

Tag 変換を使用している場合，Tag 変換で設定した VLAN ID を使用します。詳細は「25.3　Tag 変換の解説」を参照してください。VLAN ID=0 を受信した場合は，Untagged フレームと同様の扱いになります。VLAN ID=0 を送信することはありません。

本装置が新たに VLAN Tag を付与する場合は，User Priority がデフォルト値の 3 になります。

24.1.6　VLAN 使用時の注意事項

(1)　他機能との共存

「22.3　レイヤ 2 スイッチ機能と他機能の共存について」を参照してください。

24.2 VLAN 基本機能のコマンドガイド

24.2.1 コマンド一覧

VLAN 基本機能のコンフィグレーションコマンド一覧を次の表に示します。

表 24-6 コンフィグレーションコマンド一覧

コマンド名	説明
name	VLAN の名称を設定します。
state	VLAN の状態（停止／開始）を設定します。
switchport access	アクセスポートの VLAN を設定します。
switchport dot1q ethertype	ポートごとに VLAN Tag の TPID を設定します。
switchport mode	ポートの種類（アクセス，プロトコル，MAC，トランク，トンネリング）を設定します。
switchport trunk	トランクポートの VLAN を設定します。
vlan	VLAN を作成します。また，VLAN コンフィグレーションモードで VLAN に関する項目を設定します。
vlan-dot1q-ethertype	VLAN Tag の TPID のデフォルト値を設定します。
vlan-up-message	no vlan-up-message コマンドで，VLAN の Up および Down 時の運用メッセージならびに LinkUp／LinkDown トラップの送信を抑止します。

VLAN の運用コマンド一覧を次の表に示します。

表 24-7 運用コマンド一覧

コマンド名	説明
show vlan	VLAN の各種情報を表示します。
show vlan mac-vlan	MAC VLAN に登録されている MAC アドレスを表示します。
restart vlan	VLAN プログラムを再起動します。
dump protocols vlan	VLAN プログラムで採取している詳細イベントトレース情報および制御テーブルをファイルへ出力します。

24.2.2 VLAN の設定

[設定のポイント]

VLAN を作成します。新規に VLAN を作成するためには，VLAN ID と VLAN の種類を指定します。VLAN の種類を省略した場合はポート VLAN を作成します。VLAN ID リストによって複数の VLAN を一括して設定することもできます。

vlan コマンドによって，VLAN コンフィグレーションモードに移行します。作成済みの VLAN を指定した場合は，モードの移行だけとなります。VLAN コンフィグレーションモードでは VLAN のパラメータを設定できます。

なお，ここでは VLAN の種類によらない共通した設定について説明します。ポート VLAN，プロトコル VLAN，MAC VLAN のそれぞれについては次節以降を参照してください。

[コマンドによる設定]

1. **(config)# vlan 10**

   VLAN ID 10 のポート VLAN を作成し，VLAN 10 の VLAN コンフィグレーションモードに移行します。

2. **(config-vlan)# name "PORT BASED VLAN 10"**

   (config-vlan)# exit

   作成したポート VLAN 10 の名称を”PORT BASED VLAN 10”に設定します。

3. **(config)# vlan 100-200**

   VLAN ID 100～200 のポート VLAN を一括して作成します。また，VLAN 100～200 の VLAN コンフィグレーションモードに移行します。

4. **(config-vlan)# state suspend**

   作成した VLAN ID 100～200 のポート VLAN を一括して停止状態にします。

24.2.3 ポートの設定

[設定のポイント]

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，ポートチャネルインタフェースコンフィグレーションモードでポートの種類を設定します。ポートの種類は使用したい VLAN の種類に合わせて設定します。

なお，ポート VLAN，プロトコル VLAN，MAC VLAN それぞれの詳細な設定方法については次節以降を参照してください。

[コマンドによる設定]

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

   ポート 1/0/1 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)# switchport mode access**

   (config-if)# exit

   ポート 1/0/1 をアクセスポートに設定します。ポート 1/0/1 はポート VLAN で Untagged フレームを扱うポートになります。

3. **(config)# interface port-channel 10**

   チャネルグループ 10 のポートチャネルインタフェースコンフィグレーションモードに移行します。

4. **(config-if)# switchport mode trunk**

   チャネルグループ 10 をトランクポートに設定します。ポートチャネル 10 は Tagged フレームを扱うポートになります。

24.2.4 トランクポートの設定

[設定のポイント]

トランクポートは VLAN の種類に関係なく，すべての VLAN で使用でき，Tagged フレームを扱います。また，イーサネットインタフェースおよびポートチャネルインタフェースで使用できます。

トランクポートは，switchport mode コマンドを設定しただけではどの VLAN にも所属していません。このポートで扱う VLAN は switchport trunk allowed vlan コマンドによって設定します。

VLAN の追加と削除は，switchport trunk allowed vlan add コマンドおよび switchport trunk allowed vlan remove コマンドによって行います。すでに switchport trunk allowed vlan コマンドを設定した状態でもう一度 switchport trunk allowed vlan コマンドを実行すると，指定した VLAN ID リストに置き換わります。

[コマンドによる設定]

1. **(config)# vlan 10-20,100,200-300**
   (config-vlan)# exit
   (config)# interface gigabitethernet 1/0/1
   (config-if)# switchport mode trunk
   VLAN 10～20，100，200～300 を作成します。また，ポート 1/0/1 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，トランクポートに設定します。この状態では，ポート 1/0/1 はどの VLAN にも所属していません。
2. **(config-if)# switchport trunk allowed vlan 10-20**
   ポート 1/0/1 に VLAN 10～20 を設定します。ポート 1/0/1 は VLAN 10～20 の Tagged フレームを扱います。
3. **(config-if)# switchport trunk allowed vlan add 100**
   ポート 1/0/1 で扱う VLAN に VLAN 100 を追加します。
4. **(config-if)# switchport trunk allowed vlan remove 15,16**
   ポート 1/0/1 で扱う VLAN から VLAN 15 および VLAN 16 を削除します。この状態で，ポート 1/0/1 は VLAN 10～14，17～20，VLAN 100 の Tagged フレームを扱います。
5. **(config-if)# switchport trunk allowed vlan 200-300**
   ポート 1/0/1 で扱う VLAN を VLAN 200～300 に設定します。以前の設定はすべて上書きされ，VLAN 200～300 の Tagged フレームを扱います。

[注意事項]

トランクポートで Untagged フレームを扱うためには，ネイティブ VLAN を設定します。詳しくは，「24.4.3　トランクポートのネイティブ VLAN の設定」を参照してください。

トランクポートで，一度に削除する VLAN 数が 30 以上の場合，および所属している VLAN 数が 30 以上のときにモードをトランクポート以外に変更する場合は，該当ポートの MAC アドレステーブル，ARP および NDP 情報を削除します。そのため，L3 中継を行っている場合は，いったん ARP/NDP を再学習して通信が中断するので注意してください。

24.2.5　VLAN Tag の TPID の設定

[設定のポイント]

本装置は，VLAN Tag の TPID を任意の値に設定することができます。vlan-dot1q-ethertype コマンドで装置のデフォルト値を，switchport dot1q ethertype コマンドでポートごとの値を設定します。ポートごとの値を設定していないポートは装置のデフォルト値で動作します。

ポートごとの TPID の設定は，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で設定します。

[コマンドによる設定]

1. **(config)# vlan-dot1q-ethertype 9100**

装置のデフォルト値を 0x9100 に設定します。すべてのポートにおいて VLAN Tag を TPID 9100 として動作します。

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

   ポート 1/0/1 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)# switchport dot1q ethertype 8100**

   ポート 1/0/1 の TPID を 0x8100 に設定します。ポート 1/0/1 は 0x8100 を VLAN Tag として認識します。そのほかのポートは装置のデフォルト値である 0x9100 で動作します。

[注意事項]

TPID は，フレーム上では Untagged フレームの EtherType と同じ位置を使用します。そのため，IPv4 の EtherType である 0x0800 など，EtherType として使用している値を設定するとネットワークが正しく構築できないおそれがあります。EtherType 値として未使用の値を設定してください。

24.3　ポート VLAN の解説

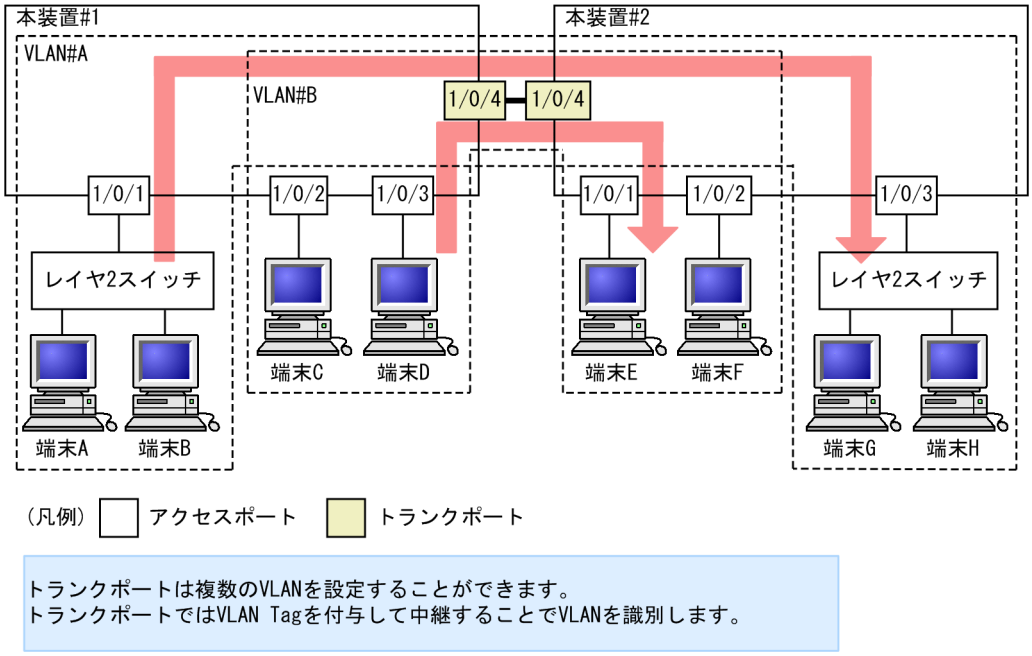
ポート単位に VLAN のグループ分けを行います。

24.3.1　アクセスポートとトランクポート

ポート VLAN は一つのポートに一つの VLAN を割り当てます。ポート VLAN として使用するポートはアクセスポートとして設定します。複数のポート VLAN をほかの LAN スイッチなどに接続するためにはトランクポートを使用します。トランクポートは VLAN Tag によって VLAN を識別するため，一つのポートに複数の VLAN を設定できます。

ポート VLAN の構成例を次の図に示します。ポート 1/0/1～1/0/3 はアクセスポートとしてポート VLAN を設定します。2 台の本装置の間はトランクポート(ポート 1/0/4)で接続します。そのとき，VLAN Tag を使います。

図 24-3　ポート VLAN の構成例



24.3.2　ネイティブ VLAN

プロトコルポート，MAC ポート，トランクポートにはコンフィグレーションに一致しないフレームを扱うネイティブ VLAN があります。各ポートのネイティブ VLAN はコンフィグレーションで指定しない場合は VLAN 1（デフォルト VLAN）です。また，ほかのポート VLAN にコンフィグレーションで変更することもできます。

例えば，「図 24-3　ポート VLAN の構成例」のトランクポートにおいて VLAN#B をネイティブ VLAN に設定すると，VLAN#B はトランクポートでも Untagged フレームで中継します。

24.3.3 ポート VLAN 使用時の注意事項

(1) アクセスポートでの Tagged フレームに関する注意事項

アクセスポートは Untagged フレームを扱うポートです。Tagged フレームを受信した場合は廃棄します。また，送信することもできません。なお，VLAN Tag 値が 0 の場合は，受信時に Untagged フレームと同じ扱いになります。

(2) トランクポートでのネイティブ VLAN に関する注意事項

トランクポートでネイティブ VLAN だけを設定した場合，アクセスポートと同じ動作になります。

24.4　ポート VLAN のコマンドガイド

24.4.1　コマンド一覧

ポート VLAN 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 24-8　コンフィグレーションコマンド一覧

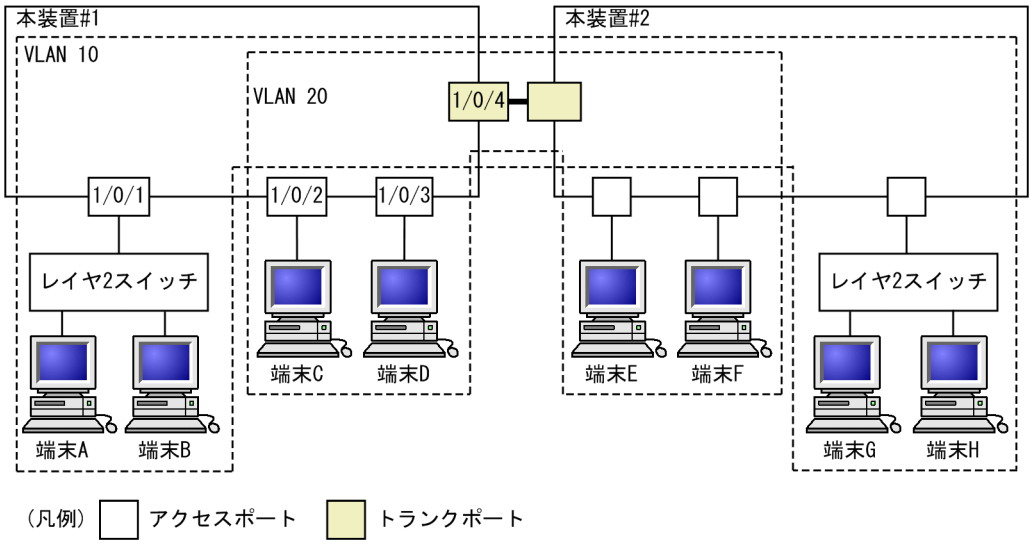
コマンド名	説明
switchport access	アクセスポートの VLAN を設定します。
switchport mode	ポートの種類（アクセス，トランク）を設定します。
switchport trunk	トランクポートの VLAN を設定します。
vlan	ポート VLAN を作成します。また，VLAN コンフィグレーションモードで VLAN に関する項目を設定します。

24.4.2　ポート VLAN の設定

ポート VLAN を設定する手順を以下に示します。ここでは，次の図に示す本装置#1 の設定例を示します。

ポート 1/0/1 はポート VLAN 10 を設定します。ポート 1/0/2，1/0/3 はポート VLAN 20 を設定します。ポート 1/0/4 はトランクポートでありすべての VLAN を設定します。

図 24-4　ポート VLAN の設定例



(1)　ポート VLAN の作成

[設定のポイント]

ポート VLAN を作成します。VLAN を作成する際に VLAN ID だけを指定して VLAN の種類を指定しないで作成するとポート VLAN となります。

[コマンドによる設定]

1. **(config)# vlan 10,20**

VLAN ID 10，VLAN ID 20 をポート VLAN として作成します。本コマンドで VLAN コンフィグレーションモードに移行します。

(2) アクセスポートの設定

一つのポートに一つの VLAN を設定して Untagged フレームを扱う場合，アクセスポートとして設定します。

[設定のポイント]

ポートをアクセスポートに設定して，そのアクセスポートで扱う VLAN を設定します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/0/1**
   ポート 1/0/1 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)# switchport mode access**
   (config-if)# switchport access vlan 10
   (config-if)# exit
   ポート 1/0/1 をアクセスポートに設定します。また，VLAN 10 を設定します。
3. **(config)# interface range gigabitethernet 1/0/2-3**
   ポート 1/0/2，1/0/3 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。ポート 1/0/2，1/0/3 は同じコンフィグレーションとなるため，一括して設定します。
4. **(config-if-range)# switchport mode access**
   (config-if-range)# switchport access vlan 20
   ポート 1/0/2，1/0/3 をアクセスポートに設定します。また，VLAN 20 を設定します。

(3) トランクポートの設定

[設定のポイント]

Tagged フレームを扱うポートはトランクポートとして設定し，そのトランクポートに VLAN を設定します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/0/4**
   ポート 1/0/4 のイーサネットインタフェースコンフィグレーションモードに移行します。
2. **(config-if)# switchport mode trunk**
   (config-if)# switchport trunk allowed vlan 10,20
   ポート 1/0/4 をトランクポートに設定します。また，VLAN 10，20 を設定します。

24.4.3 トランクポートのネイティブ VLAN の設定

[設定のポイント]

トランクポートで Untagged フレームを扱いたい場合，ネイティブ VLAN を設定します。ネイティブ VLAN はポート VLAN だけを設定できます。

ネイティブ VLAN の VLAN ID を switchport trunk allowed vlan コマンドで指定すると，トランクポートで Untagged フレームを扱う VLAN となります。ネイティブ VLAN は，コンフィグレーションで明示して指定しない場合は VLAN 1（デフォルト VLAN）です。

トランクポート上で，デフォルト VLAN で Tagged フレーム（VLAN ID 1 の VLAN Tag）を扱いたい場合は，ネイティブ VLAN をほかの VLAN に変更してください。

[コマンドによる設定]

1. **(config)# vlan 10,20**
   (config-vlan)# exit
   VLAN ID 10，VLAN ID 20 をポート VLAN として作成します。
2. **(config)# interface gigabitethernet 1/0/1**
   (config-if)# switchport mode trunk
   ポート 1/0/1 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。また，トランクポートとして設定します。この状態で，トランクポート 1/0/1 のネイティブ VLAN はデフォルト VLAN です。
3. **(config-if)# switchport trunk native vlan 10**
   (config-if)# switchport trunk allowed vlan 1,10,20
   トランクポート 1/0/1 のネイティブ VLAN を VLAN 10 に設定します。また，VLAN 1，10，20 を設定します。ネイティブ VLAN である VLAN 10 が Untagged フレームを扱い，VLAN 1（デフォルト VLAN），VLAN 20 は Tagged フレームを扱います。

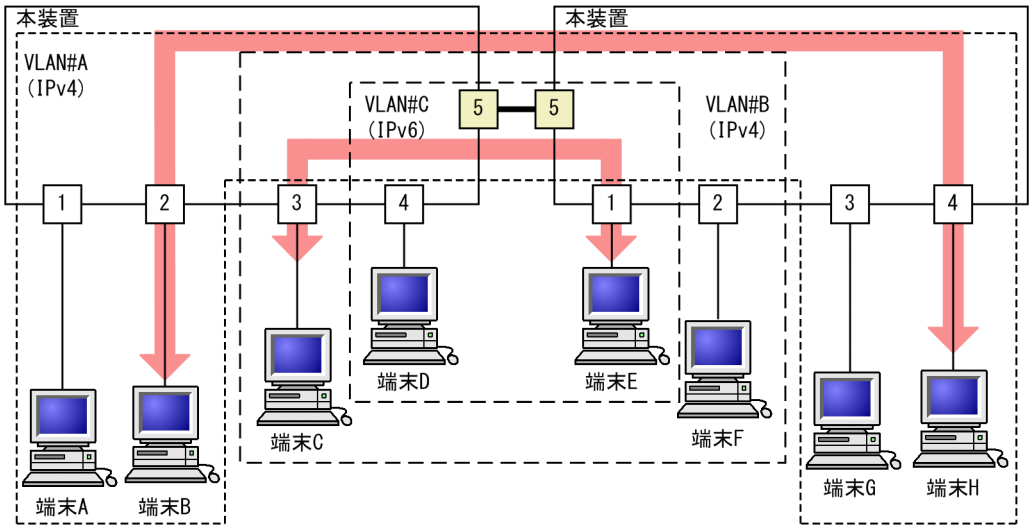
24.5　プロトコル VLAN の解説

24.5.1　概要

プロトコル単位で VLAN のグループ分けを行います。IPv4 や IPv6 といったプロトコルごとに異なる VLAN を構成できます。複数のプロトコルを同一のプロトコル VLAN に設定することもできます。

プロトコル VLAN の構成例を次の図に示します。VLAN#A，#B を IPv4 プロトコルで構成し，VLAN#C を IPv6 プロトコルで構成した例を示しています。

図 24-5　プロトコル VLAN の構成例



（凡例）：プロトコルポート　：トランクポート

・VLAN#A，#BはIPv4プロトコルのVLANです。
・VLAN#CはIPv6プロトコルのVLANです。
・端末D，EはVLAN#B，#Cの両方に属しています。
・矢印は端末Bと端末H間，端末Cと端末E間で同じVLANで通信している例です。

24.5.2　プロトコルの識別

プロトコルの識別には次の 3 種類の値を使用します。

表 24-9　プロトコルを識別する値

識別する値	概要
Ether-type 値	EthernetV2 形式フレームの Ether-type 値によってプロトコルを識別します。
LLC 値	802.3 形式フレームの LLC 値(DSAP,SSAP)によってプロトコルを識別します。
SNAP Ether-type 値	802.3 形式フレームの Ether-type 値によってプロトコルを識別します。フレームの LLC 値が AA AA 03 であるフレームだけが対象となります。

プロトコルは，コンフィグレーションによってプロトコルを作成し VLAN に対応付けます。一つのプロトコル VLAN に複数のプロトコルを対応付けることもできます。

24.5.3　プロトコルポートとトランクポート

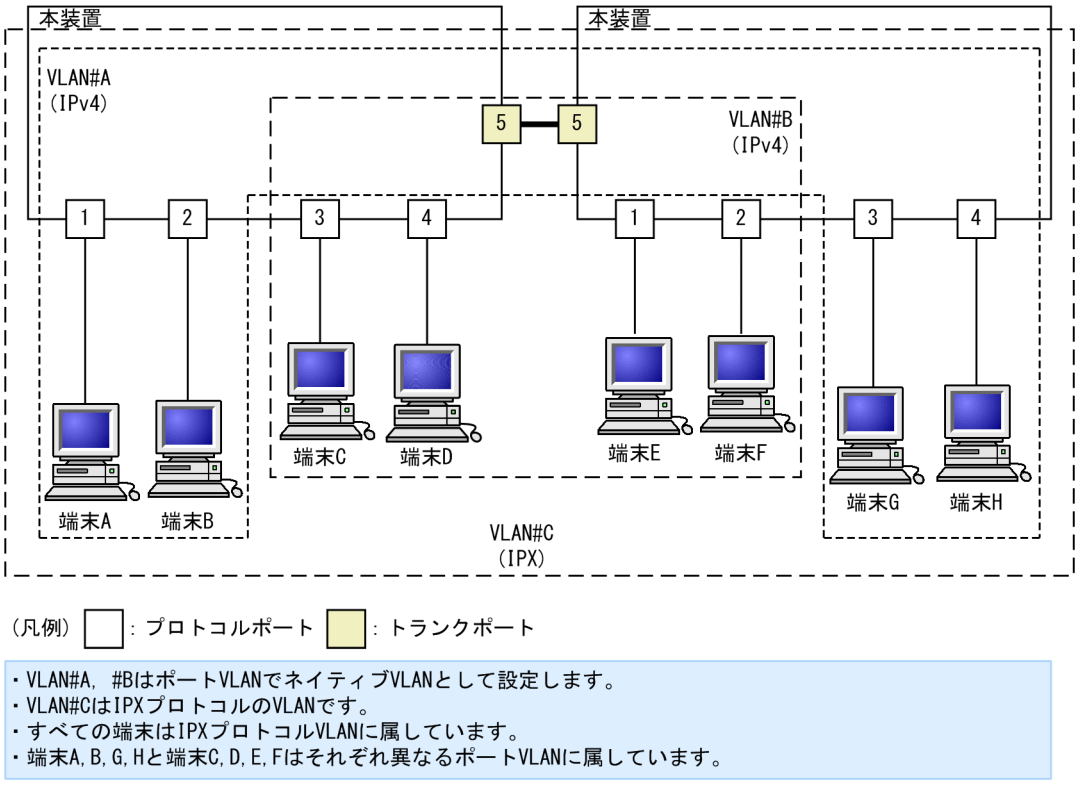
プロトコルポートは Untagged フレームのプロトコルを識別します。プロトコル VLAN として使用するポートはプロトコルポートを設定します。プロトコルポートには複数のプロトコルで異なる VLAN を割り当てることもできます。複数のプロトコル VLAN をほかの LAN スイッチなどに接続するためにはトランクポートを使用します。なお，トランクポートは VLAN Tag によって VLAN を識別するため，プロトコルによる識別は行いません。

24.5.4　プロトコルポートのネイティブ VLAN

プロトコルポートでコンフィグレーションに一致しないプロトコルのフレームを受信した場合はネイティブ VLAN で扱います。ネイティブ VLAN は，コンフィグレーションで指定しない場合は VLAN 1（デフォルト VLAN）です。また，ほかのポート VLAN にコンフィグレーションで変更することもできます。

次の図に，プロトコルポートでネイティブ VLAN を使用する構成例を示します。図の構成は，IPX プロトコルをネットワーク全体で一つの VLAN とし，そのほか（IPv4 など）のプロトコルについてはポート VLAN で VLAN を分ける例です。VLAN#A，VLAN#B を各ポートのネイティブ VLAN として設定します。なお，この構成例では，VLAN#A，VLAN#B も IPv4 のプロトコル VLAN として設定することもできます。

図 24-6　プロトコルポートでネイティブ VLAN を使用する構成例



・VLAN#A，#Bはポート VLAN でネイティブ VLAN として設定します。
・VLAN#C は IPX プロトコルの VLAN です。
・すべての端末は IPX プロトコル VLAN に属しています。
・端末 A，B，G，H と端末 C，D，E，F はそれぞれ異なるポート VLAN に属しています。

24.6　プロトコル VLAN のコマンドガイド

24.6.1　コマンド一覧

プロトコル VLAN 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 24-10　コンフィグレーションコマンド一覧

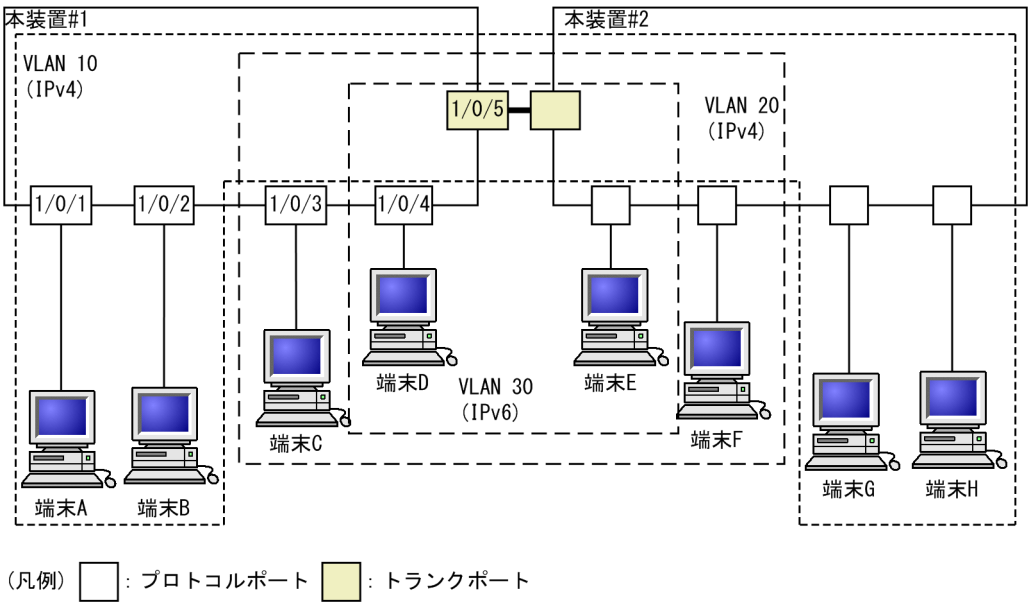
コマンド名	説明
protocol	プロトコル VLAN で VLAN を識別するプロトコルを設定します。
switchport mode	ポートの種類（プロトコル，トランク）を設定します。
switchport protocol	プロトコルポートの VLAN を設定します。
switchport trunk	トランクポートの VLAN を設定します。
vlan	protocol-based パラメータを指定してプロトコル VLAN を作成します。
vlan-protocol	プロトコル VLAN 用のプロトコル名称とプロトコル値を設定します。

24.6.2　プロトコル VLAN の作成

プロトコル VLAN を設定する手順を以下に示します。ここでは，次の図に示す本装置#1 の設定例を示します。

ポート 1/0/1，1/0/2 は IPv4 プロトコル VLAN 10 を設定します。ポート 1/0/3，1/0/4 は IPv4 プロトコル VLAN 20 を設定します。ポート 1/0/4 は VLAN 20 と同時に IPv6 プロトコル VLAN 30 にも所属します。ポート 1/0/5 はトランクポートであり，すべての VLAN を設定します。

図 24-7　プロトコル VLAN の設定例



(1) VLAN を識別するプロトコルの作成

[設定のポイント]

プロトコル VLAN は，VLAN を作成する前に識別するプロトコルを vlan-protocol コマンドで設定します。プロトコルは，プロトコル名称とプロトコル値を設定します。一つの名称に複数のプロトコル値を関連づけることもできます。

IPv4 プロトコルは, IPv4 の Ether-type と同時に ARP の Ether-type も指定する必要があるため, IPv4 には二つのプロトコル値を関連づけます。

[コマンドによる設定]

1. **(config)# vlan-protocol IPV4 ethertype 0800 ethertype 0806**

   名称 IPV4 のプロトコルを作成します。プロトコル値として，IPv4 の Ether-type 値 0800 と ARP の Ether-type 値 0806 を関連づけます。

   なお，この設定でのプロトコル判定は EthernetV2 形式のフレームだけとなります。

2. **(config)# vlan-protocol IPV6 ethertype 86dd**

   名称 IPV6 のプロトコルを作成します。プロトコル値として IPv6 の Ether-type 値 86DD を関連づけます。

(2) プロトコル VLAN の作成

[設定のポイント]

プロトコル VLAN を作成します。VLAN を作成する際に VLAN ID と protocol-based パラメータを指定します。また，VLAN を識別するプロトコルとして，作成したプロトコルを指定します。

[コマンドによる設定]

1. **(config)# vlan 10,20 protocol-based**

   VLAN 10, 20 をプロトコル VLAN として作成します。VLAN 10, 20 は同じ IPv4 プロトコル VLAN とするため一括して設定します。本コマンドで VLAN コンフィグレーションモードに移行します。

2. **(config-vlan)# protocol IPV4**

   (config-vlan)# exit

   VLAN 10，20 を識別するプロトコルとして，作成した IPv4 プロトコルを指定します。

3. **(config)# vlan 30 protocol-based**

   (config-vlan)# protocol IPV6

   VLAN 30 をプロトコル VLAN として作成します。また，VLAN 30 を識別するプロトコルとして，作成した IPv6 プロトコルを指定します。

(3) プロトコルポートの設定

[設定のポイント]

プロトコル VLAN でプロトコルによって VLAN を識別するポートは，プロトコルポートを設定します。このポートでは Untagged フレームを扱います。

[コマンドによる設定]

1. **(config)# interface range gigabitethernet 1/0/1-2**

   ポート 1/0/1，1/0/2 のイーサネットインタフェースコンフィグレーションモードに移行します。ポート 1/0/1，1/0/2 は同じコンフィグレーションとなるため一括して指定します。

2. **(config-if-range)# switchport mode protocol-vlan**
   (config-if-range)# switchport protocol vlan 10
   (config-if-range)# exit
   ポート 1/0/1，1/0/2 をプロトコルポートに設定します。また，VLAN 10 を設定します。
3. **(config)# interface range gigabitethernet 1/0/3-4**
   (config-if-range)# switchport mode protocol-vlan
   (config-if-range)# switchport protocol vlan 20
   (config-if-range)# exit
   ポート 1/0/3，1/0/4 をプロトコルポートに設定します。また，VLAN 20 を設定します。
4. **(config)# interface gigabitethernet 1/0/4**
   (config-if)# switchport protocol vlan add 30
   ポート 1/0/4 に VLAN 30 を追加します。ポート 1/0/4 は IPv4，IPv6 の 2 種類のプロトコル VLAN を設定しています。

[注意事項]

switchport protocol vlan コマンドは，それ以前のコンフィグレーションに追加するコマンドではなく指定した<vlan id list>に設定を置き換えます。すでにプロトコル VLAN を運用中のポートで VLAN の追加や削除を行う場合は，switchport protocol vlan add コマンドおよび switchport protocol vlan remove コマンドを使用してください。

(4) トランクポートの設定

[設定のポイント]

プロトコル VLAN においても，Tagged フレームを扱うポートはトランクポートとして設定し，そのトランクポートに VLAN を設定します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/0/5**
   ポート 1/0/5 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)# switchport mode trunk**
   (config-if)# switchport trunk allowed vlan 10,20,30
   ポート 1/0/5 をトランクポートに設定します。また，VLAN 10，20，30 を設定します。

24.6.3 プロトコルポートのネイティブ VLAN の設定

[設定のポイント]

プロトコルポートで設定したプロトコルに一致しない Untagged フレームを扱いたい場合，そのフレームを扱う VLAN としてネイティブ VLAN を設定します。ネイティブ VLAN はポート VLAN だけを設定できます。

ネイティブ VLAN の VLAN ID を switchport protocol native vlan コマンドで指定すると，プロトコルポート上で設定したプロトコルに一致しない Untagged フレームを扱う VLAN となります。ネイティブ VLAN は，コンフィグレーションで明示して指定しない場合は VLAN 1（デフォルト VLAN）です。

ネイティブ VLAN に state suspend コマンドが設定されている場合は，設定したプロトコルと一致しないフレームが中継されません。

[コマンドによる設定]

1. **(config)# vlan 10,20 protocol-based**
   (config-vlan)# exit
   (config)# vlan 30
   (config-vlan)# exit
   VLAN 10，20 をプロトコル VLAN として作成します。また，VLAN 30 をポート VLAN として作成します。
2. **(config)# interface gigabitethernet 1/0/1**
   (config-if)# switchport mode protocol-vlan
   ポート 1/0/1 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。また，プロトコルポートとして設定します。
3. **(config-if)# switchport protocol native vlan 30**
   (config-if)# switchport protocol vlan 10,20
   プロトコルポート 1/0/1 のネイティブ VLAN をポート VLAN 30 に設定し，設定したプロトコルに一致しない Untagged フレームを扱う VLAN とします。また，プロトコル VLAN 10，20 を設定します。

24.7　MAC VLAN の解説

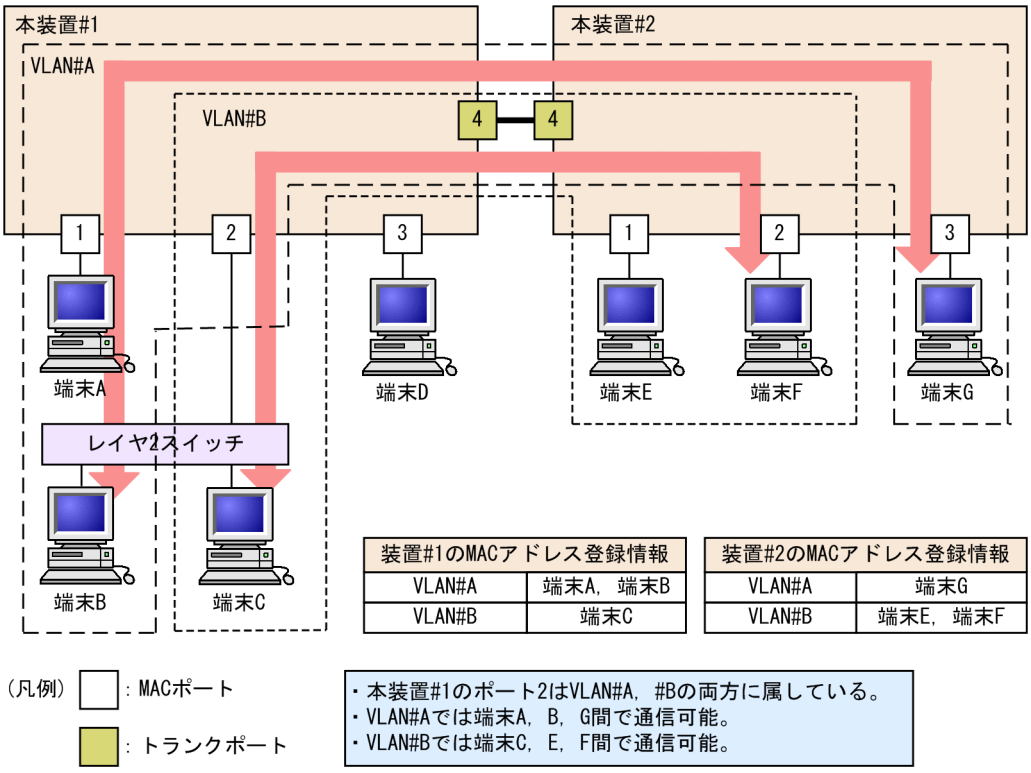
24.7.1　概要

送信元の MAC アドレス単位に VLAN のグループ分けを行います。VLAN への MAC アドレスの登録は，コンフィグレーションによる登録と，レイヤ 2 認証機能による動的な登録ができます。

MAC VLAN は，許可した端末の MAC アドレスをコンフィグレーションで登録するか，レイヤ 2 認証機能で認証された MAC アドレスを登録することによって，接続を許可された端末とだけ通信できるように設定できます。

MAC VLAN の構成例を次の図に示します。VLAN を構成する装置間にトランクポートを設定している場合は，送信元 MAC アドレスに関係なく VLAN Tag によって VLAN を決定します。そのため，すべての装置に同じ MAC アドレスの設定をする必要はありません。装置ごとに MAC ポートに接続した端末の MAC アドレスを設定します。

図 24-8　MAC VLAN の構成例



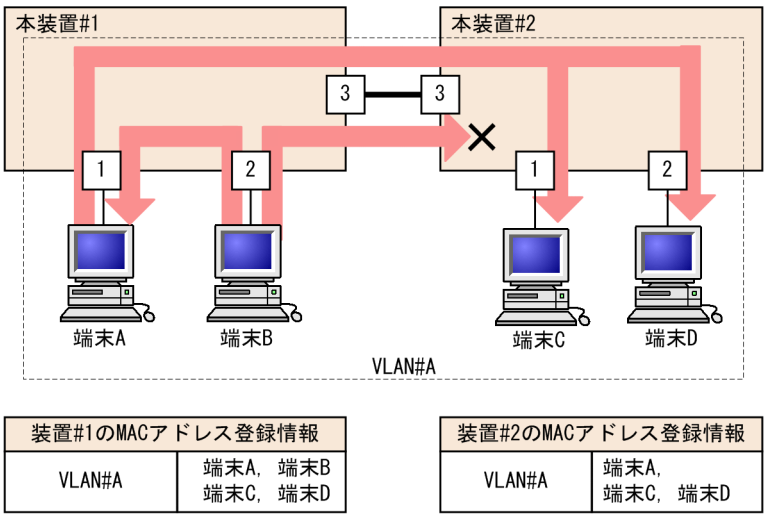
24.7.2　装置間の接続と MAC アドレス設定

複数の装置で MAC VLAN を構成する場合，装置間の接続はトランクポートをお勧めします。トランクポートで受信したフレームの VLAN 判定は VLAN Tag で行います。そのため，送信元 MAC アドレスが VLAN に設定されていなくても，MAC VLAN で通信できます。トランクポートで装置間を接続した場合については，「図 24-8　MAC VLAN の構成例」を参照してください。

MAC ポートで装置間を接続する場合は，その VLAN に属するすべての MAC アドレスをすべての装置に設定する必要があります。ルータが存在する場合は，ルータの MAC アドレスも登録してください。

MAC ポートで装置間を接続した場合の図を次に示します。

図 24-9　装置間を MAC ポートで接続した場合



装置#1のMACアドレス登録情報	
VLAN#A	端末A，端末B 端末C，端末D

装置#2のMACアドレス登録情報	
VLAN#A	端末A， 端末C，端末D

（凡例）　：MACポート

・端末Aは，本装置#1，#2の両方に設定があるため，端末C，端末Dと通信可能。
・端末Bは，本装置#2に設定がないため，端末C，端末Dと通信不可。
　端末Aとは通信可能。

24.7.3　レイヤ 2 認証機能との連携について

MAC VLAN は，レイヤ 2 認証機能と連携して，VLAN への MAC アドレスを動的に登録できます。連携するレイヤ 2 認証機能を次に示します。

- Web 認証
- MAC 認証

プリンタやサーバなど，レイヤ 2 認証機能を動作させないで MAC ポートと接続する端末は，その MAC アドレスをコンフィグレーションで VLAN に登録します。

コンフィグレーションとレイヤ 2 認証機能で同じ MAC アドレスを設定した場合，コンフィグレーションの MAC アドレスを登録します。

24.7.4　MAC ポートの VLAN 設定

MAC ポートに VLAN を設定する場合，コンフィグレーションコマンド switchport mac vlan による設定と，レイヤ 2 認証機能による動的な設定ができます。

なお，同じ MAC ポートに，コンフィグレーションによる VLAN の設定と，レイヤ 2 認証機能による動的な VLAN の設定とを共存させることはできません。認証対象ポートとして設定されている MAC ポートに対し，レイヤ 2 認証機能で VLAN が動的に設定されている状態のときにコンフィグレーションコマンド switchport mac vlan が設定された場合，該当ポートに動的に設定されていた VLAN はすべて削除されます。

動的に VLAN が設定できるレイヤ 2 認証機能と認証モードを次の表に示します。

表 24–11 動的に VLAN が設定できるレイヤ 2 認証機能と認証モード

レイヤ 2 認証機能	認証モード
Web 認証	ダイナミック VLAN モード
MAC 認証	ダイナミック VLAN モード

24.8 MAC VLAN のコマンドガイド

24.8.1 コマンド一覧

MAC VLAN 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 24-12 コンフィグレーションコマンド一覧

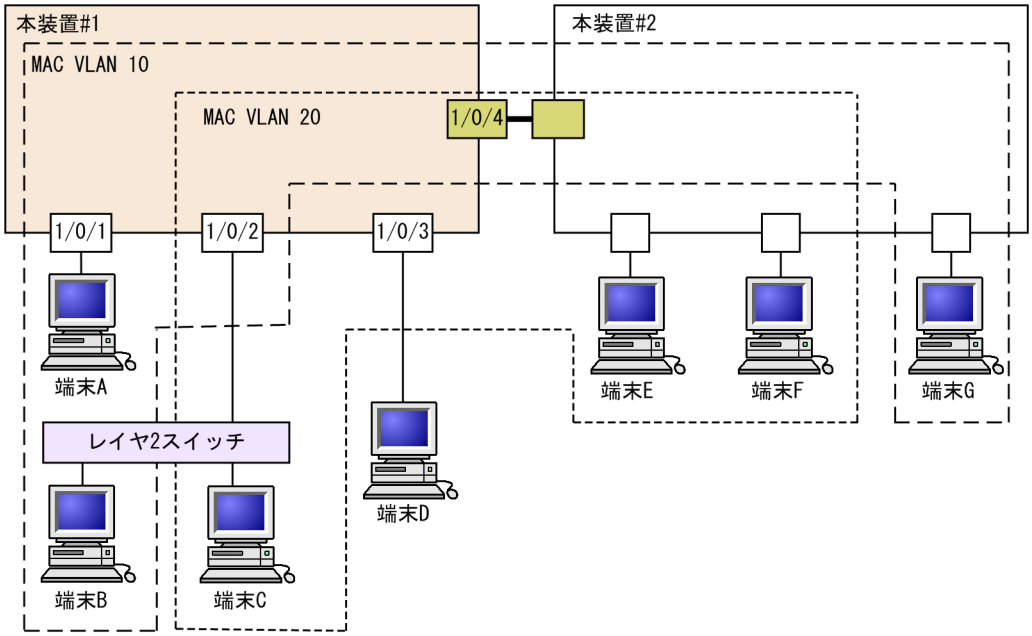
コマンド名	説明
mac-address	MAC VLAN で VLAN に所属する端末の MAC アドレスをコンフィグレーションによって設定します。
switchport mac	MAC ポートの VLAN を設定します。
switchport mode	ポートの種類（MAC，トランク）を設定します。
switchport trunk	トランクポートの VLAN を設定します。
vlan	mac-based パラメータを指定して MAC VLAN を作成します。

24.8.2 MAC VLAN の設定

MAC VLAN を設定する手順を以下に示します。ここでは，MAC VLAN と VLAN に所属する MAC アドレスをコンフィグレーションで設定する場合の例を示します。IEEE802.1X との連携については，「コンフィグレーションガイド Vol.2」「7 IEEE802.1X の設定と運用」を参照してください。

次の図に示す本装置#1 の設定例を示します。ポート 1/0/1 は MAC VLAN 10 を設定します。ポート 1/0/2 は MAC VLAN 10 および 20，1/0/3 は MAC VLAN 20 を設定します。ただし，ポート 1/0/3 には MAC アドレスを登録していない端末 D を接続しています。

図 24-10　MAC VLAN の設定例



装置#1のMACアドレス登録情報		
VLAN 10	端末A	0012.e200.0001
	端末B	0012.e200.0002
VLAN 20	端末C	0012.e200.0003

(1)　MAC VLAN の作成と MAC アドレスの登録

[設定のポイント]

MAC VLAN を作成します。VLAN を作成する際に VLAN ID と mac-based パラメータを指定します。

また，VLAN に所属する MAC アドレスを設定します。構成例の端末 A～C をそれぞれの VLAN に登録します。端末 D は MAC VLAN での通信を許可しない端末にするので登録しません。

[コマンドによる設定]

1. **(config)# vlan 10 mac-based**
   (config-vlan)# name MACVLAN10
   VLAN 10 を MAC VLAN として作成します。本コマンドで VLAN コンフィグレーションモードに移行します。
2. **(config-vlan)# mac-address 0012.e200.0001**
   (config-vlan)# mac-address 0012.e200.0002
   (config-vlan)# exit
   端末 A（0012.e200.0001），端末 B（0012.e200.0002）を MAC VLAN 10 に登録します。
3. **(config)# vlan 20 mac-based**
   (config-vlan)# name MACVLAN20
   (config-vlan)# mac-address 0012.e200.0003
   VLAN 20 を MAC VLAN として作成し，端末 C（0012.e200.0003）を MAC VLAN 20 に登録します。

[注意事項]

MAC VLAN に登録する MAC アドレスでは，同じ MAC アドレスを複数の VLAN に登録できません。

(2) MAC ポートの設定

[設定のポイント]

MAC VLAN で送信元 MAC アドレスによって VLAN を識別するポートは，MAC ポートを設定します。このポートでは Untagged フレームを扱います。

[コマンドによる設定]

1. **(config)# interface range gigabitethernet 1/0/1-2**

   ポート 1/0/1，1/0/2 のイーサネットインタフェースコンフィグレーションモードに移行します。

2. **(config-if-range)# switchport mode mac-vlan**

   (config-if-range)# exit

   ポート 1/0/1，1/0/2 を MAC ポートに設定します。ポート 1/0/1，1/0/2 はレイヤ 2 認証機能によって動的に VLAN が登録されます。

3. **(config)# interface gigabitethernet 1/0/3**

   (config-if)# switchport mode mac-vlan

   (config-if)# switchport mac vlan 20

   ポート 1/0/3 を MAC ポートに設定します。また，VLAN 20 を設定します。

[注意事項]

switchport mac vlan コマンドは，それ以前のコンフィグレーションに追加するコマンドではなく指定した<vlan id list>に設定を置き換えます。すでに MAC VLAN を運用中のポートで VLAN の追加や削除を行う場合は，switchport mac vlan add コマンドおよび switchport mac vlan remove コマンドを使用してください。

(3) トランクポートの設定

[設定のポイント]

MAC VLAN においても，Tagged フレームを扱うポートはトランクポートとして設定し，そのトランクポートに VLAN を設定します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/0/4**

   ポート 1/0/4 のイーサネットインタフェースコンフィグレーションモードに移行します。

2. **(config-if)# switchport mode trunk**

   (config-if)# switchport trunk allowed vlan 10,20

   ポート 1/0/4 をトランクポートに設定します。また，VLAN 10，20 を設定します。

24.8.3 MAC ポートのネイティブ VLAN の設定

[設定のポイント]

MAC ポートで MAC VLAN に登録した MAC アドレスに一致しない Untagged フレームを扱いたい場合，そのフレームを扱う VLAN としてネイティブ VLAN を設定します。ネイティブ VLAN はポート VLAN だけが設定できます。

ネイティブ VLAN の VLAN ID を switchport mac native vlan コマンドで指定すると，MAC ポート上で登録した MAC アドレスに一致しない Untagged フレームを扱う VLAN となります。ネイティブ VLAN は，コンフィグレーションで明示して指定しない場合は VLAN 1（デフォルト VLAN）です。

ネイティブ VLAN に state suspend コマンドが設定されていた場合は，登録した MAC アドレスに一致しないフレームが中継されません。

[コマンドによる設定]

1. **(config)# vlan 10,20 mac-based**
   (config-vlan)# exit
   (config)# vlan 30
   (config-vlan)# exit
   VLAN 10,20 を MAC VLAN として作成します。また，VLAN 30 をポート VLAN として作成します。
2. **(config)# interface gigabitethernet 1/0/1**
   (config-if)# switchport mode mac-vlan
   ポート 1/0/1 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。また，MAC ポートとして設定します。
3. **(config-if)# switchport mac native vlan 30**
   ポート 1/0/1 のネイティブ VLAN をポート VLAN 30 に設定します。VLAN 30 はポート 1/0/1 で登録されていない MAC アドレスからの Untagged フレームを扱う VLAN となります。

24.9 VLAN インタフェース

24.9.1 IP アドレスを設定するインタフェース

VLAN に IP アドレスを設定することで，レイヤ 3 インタフェースとして使用できます。VLAN インタフェースの MAC アドレスは，装置 MAC アドレスを使用します。

IP アドレスはコンフィグレーションコマンド interface vlan によって設定します。このインタフェースのことを VLAN インタフェースと呼びます。

24.10　VLAN インタフェースのコマンドガイド

24.10.1　コマンド一覧

VLAN インタフェース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 24-13　コンフィグレーションコマンド一覧

コマンド名	説明
interface vlan	VLAN インタフェースを設定します。また，インタフェースモードへ移行します。
ip address※	インタフェースの IPv4 アドレスを設定します。

注※

「コンフィグレーションコマンドレファレンス」「22　IPv4 通信」を参照してください。

24.10.2　レイヤ 3 インタフェースとしての VLAN の設定

[設定のポイント]

VLAN は IP アドレスを設定してレイヤ 3 インタフェースとして使用できます。interface vlan コマンドおよび VLAN インタフェースコンフィグレーションモードでさまざまなレイヤ 3 機能を設定できます。

ここでは, VLAN インタフェースに IPv4 アドレスを設定する例を示します。VLAN インタフェースで設定できるレイヤ 3 機能については，使用する各機能の章を参照してください。

[コマンドによる設定]

1. **(config)# interface vlan 10**

   VLAN 10 の VLAN 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。interface vlan コマンドで指定した VLAN ID が未設定の VLAN ID の場合, 自動的にポート VLAN を作成して vlan コマンドが設定されます。

2. **(config-if)# ip address 192.168.1.1 255.255.255.0**

   VLAN 10 に IPv4 アドレス 192.168.1.1，サブネットマスク 255.255.255.0 を設定します。

25 VLAN 拡張機能

この章では，VLAN に適用する拡張機能の解説と操作方法について説明します。

25.1　VLAN トンネリングの解説

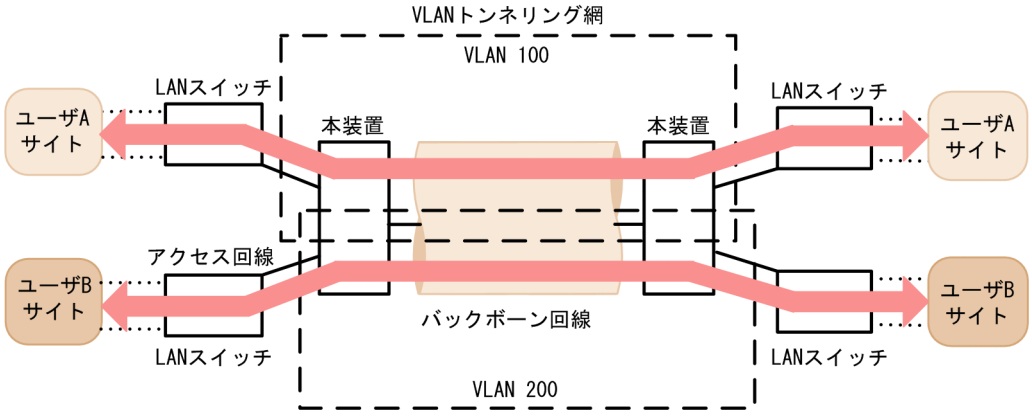
25.1.1　概要

VLAN トンネリング機能とは，複数ユーザの VLAN をほかの VLAN の中に集約して「トンネル」する機能です。IEEE802.1Q VLAN Tag をスタックすることで一つの VLAN 内にほかの VLAN に属するフレームをトランスペアレントに通すことができます。トンネルは 3 か所以上のサイトを接続するマルチポイント接続ができます。

VLAN トンネリング概要（広域イーサネットサービス適用例）を次の図に示します。VLAN トンネリングでは，VLAN Tag をスタックすることで VLAN トンネリング網内の VLAN を識別します。

この適用例は，レイヤ 2 VPN サービスである広域イーサネットサービスに適用する場合の例です。本装置に VLAN トンネリング機能を適用します。VLAN トンネリングでは，VLAN Tag をスタックすることで VLAN トンネリング網内の VLAN を識別します。ユーザサイトを収容するポートをアクセス回線，VLAN トンネリング網内に接続するポートをバックボーン回線と呼びます。アクセス回線からのフレームに VLAN Tag を追加してバックボーン回線に中継します。バックボーン回線からのフレームは VLAN Tag を外しアクセス回線へ中継します。

図 25–1　VLAN トンネリング概要（広域イーサネットサービス適用例）



25.1.2　VLAN トンネリングを使用するための必須条件

VLAN トンネリング機能を使用する場合は，次の条件に合わせてネットワークを構築する必要があります。

- ポート VLAN を使用します。
- VLAN トンネリング機能を実現する VLAN では，アクセス回線側はトンネリングポートとし，バックボーン回線側をトランクポートとします。
- VLAN トンネリング網内のバックボーン回線では VLAN Tag をスタックするため，通常より 4 バイト大きいサイズのフレームを扱える必要があります。
- 装置内で，アクセスポートとトンネリングポートは共存できません。一つでもトンネリングポートを設定すると，アクセスポートとして設定していたポートもトンネリングポートとして動作します。

25.1.3　VLAN トンネリング使用時の注意事項

(1)　他機能との共存

「22.3　レイヤ 2 スイッチ機能と他機能の共存について」を参照してください。

(2)　デフォルト VLAN について

デフォルト VLAN の自動加入を行いません。すべての VLAN を明示的に設定してください。

(3)　トランクポートのネイティブ VLAN について

VLAN トンネリングのトランクポートは VLAN Tag をスタックするポートとなりますが，ネイティブ VLAN では VLAN Tag をスタックしません。ほかの VLAN と異なる動作となるので, VLAN トンネリング網のバックボーン回線の VLAN としては使用できません。VLAN トンネリングを使用する場合，トランクポートのネイティブ VLAN は suspend 状態にしてください。

トランクポートのネイティブ VLAN は，コンフィグレーションコマンド switchport trunk native vlan で設定しない場合デフォルト VLAN です。デフォルト VLAN で VLAN トンネリング機能を使用する場合は，switchport trunk native vlan でネイティブ VLAN にデフォルト VLAN 以外の VLAN を設定してください。ただし，トランクポートにネイティブ VLAN だけを設定した場合，トンネリングポートとして動作します。

(4)　フレームの User Priority について

VLAN トンネリングを使用する場合の User Priority については,「コンフィグレーションガイド Vol.2」「3.3　マーカー解説」を参照してください。

25.2　VLAN トンネリングのコマンドガイド

25.2.1　コマンド一覧

VLAN トンネ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 25-1　コンフィグレーションコマンド一覧

コマンド名	説明
switchport access	アクセス回線をトンネリングポートで設定します。
switchport mode	アクセス回線，バックボーン回線を設定するためにポートの種類を設定します。
switchport trunk	バックボーン回線を設定します。
mtu※	バックボーン回線でジャンボフレームを設定します。

注※
「コンフィグレーションコマンドレファレンス」「14　イーサネット」を参照してください。

25.2.2　VLAN トンネリングの設定

(1)　アクセス回線，バックボーン回線の設定

[設定のポイント]

VLAN トンネリング機能はポート VLAN を使用し，アクセス回線をトンネリングポート，バックボーン回線をトランクポートで設定します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/0/1**
   ポート 1/0/1 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)# switchport mode dot1q-tunnel**
   (config-if)# switchport access vlan 10
   ポート 1/0/1 をトンネリングポートに設定します。また，VLAN 10 を設定します。
   トランクポートのコンフィグレーションについては，「24.4　ポート VLAN のコマンドガイド」を参照してください。

(2)　バックボーン回線のジャンボフレームの設定

[設定のポイント]

バックボーン回線は VLAN Tag をスタックするため通常より 4 バイト以上大きいサイズのフレームを扱います。そのため，ジャンボフレームを設定する必要があります。

[コマンドによる設定]

ジャンボフレームのコンフィグレーションについては，「20.4.7　ジャンボフレームの設定」を参照してください。

25.3　Tag 変換の解説

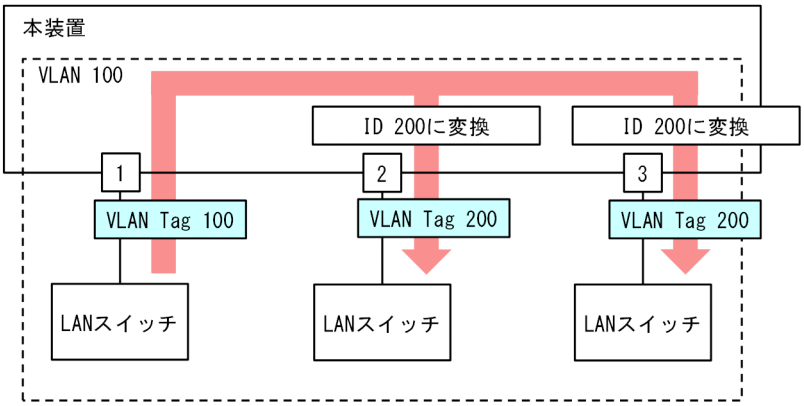
25.3.1　概要

Tag 変換は，Tagged フレームをレイヤ 2 スイッチ中継する際に，フレームの VLAN Tag の VLAN ID フィールドを別の値に変換する機能です。この機能によって，異なる VLAN ID で設定した既設の VLAN を一つの VLAN として接続できるようになります。

Tag 変換は，トランクポートで指定します。Tag 変換を使用しない場合は，VLAN Tag の VLAN ID フィールドにその VLAN の VLAN ID を使用します。Tag 変換を指定した場合はその ID を使用します。

Tag 変換の構成例を次の図に示します。図では，ポート 1 で Tag 変換が未指定であり，ポート 2 およびポート 3 にそれぞれ Tag 変換を設定し，VLAN Tag の VLAN ID フィールドを変換して中継します。また，フレームを受信する際にも，各ポートで設定した ID の VLAN Tag のフレームを VLAN 100 で扱います。

図 25-2　Tag 変換の構成例



25.3.2　Tag 変換使用時の注意事項

(1)　他機能との共存

「22.3　レイヤ 2 スイッチ機能と他機能の共存について」を参照してください。

25.4　Tag 変換のコマンドガイド

25.4.1　コマンド一覧

Tag 変換のコンフィグレーションコマンド一覧を次の表に示します。

表 25-2　コンフィグレーションコマンド一覧

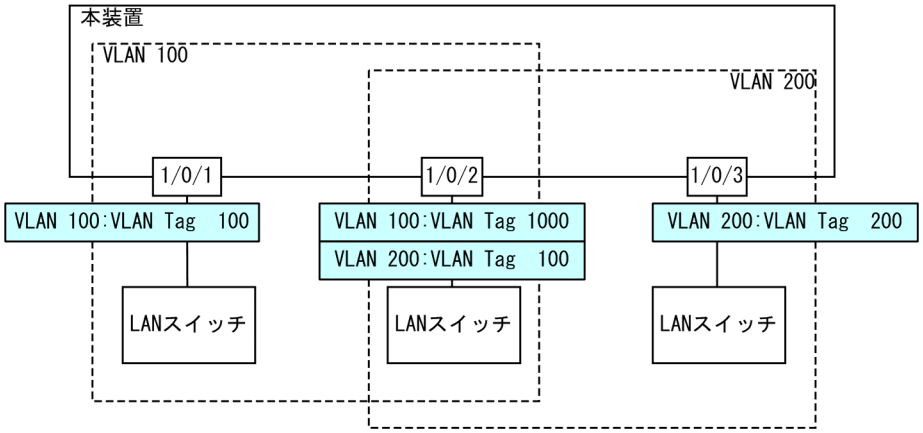
コマンド名	説明
switchport vlan mapping	変換する ID を設定します。
switchport vlan mapping enable	指定したポートで Tag 変換を有効にします。

25.4.2　Tag 変換の設定

Tag 変換を設定する手順を次の図に示します。ここでは，図に示す構成のポート 1/0/2 の設定例を示します。

構成例では，ポート 1/0/2 に Tag 変換を適用します。ポート 1/0/2 では，VLAN 100 のフレームの送受信は VLAN Tag 1000 で行い，VLAN 200 のフレームの送受信は VLAN Tag 100 で行います。このように，VLAN 100 で Tag 変換を行った場合，ほかの VLAN で VLAN Tag 100 を使用することもできます。また，ポート 1/0/2 では VLAN Tag 200 のフレームを VLAN 200 として扱わないで，未設定の VLAN Tag として廃棄します。

図 25-3　Tag 変換の設定例



[設定のポイント]

Tag 変換は，Tag 変換を有効にする設定と，変換する ID を設定することによって動作します。Tag 変換の設定はトランクポートだけ有効です。

Tag 変換は switchport vlan mapping コマンドで設定します。設定した変換を有効にするためには，switchport vlan mapping enable コマンドを設定します。Tag 変換を有効にすると，そのポートで変換を設定していない VLAN はフレームの送受信を停止します。

[コマンドによる設定]

1.
```
(config)# interface gigabitethernet 1/0/2
(config-if)# switchport mode trunk
```

(config-if)# switchport trunk allowed vlan 100,200

ポート 1/0/2 をトランクポートに設定して，VLAN 100，200 を設定します。

2. **(config-if)# switchport vlan mapping 1000 100**

   (config-if)# switchport vlan mapping 100 200

   ポート 1/0/2 で VLAN 100, 200 に Tag 変換を設定します。VLAN 100 では VLAN Tag 1000 でフレームを送受信して，VLAN 200 では VLAN Tag 100 でフレームを送受信するように設定します。

3. **(config-if)# switchport vlan mapping enable**

   ポート 1/0/2 で Tag 変換を有効にします。本コマンドを設定するまでは Tag 変換は動作しません。

[注意事項]

Tag 変換を使用するポートは，そのポートのすべての VLAN で Tag 変換の設定をする必要があります。変換しない VLAN の場合は，同じ値に変換する設定を行ってください。

Tag 変換で変換する VLAN と VLAN Tag の VLAN ID の組み合わせは装置で共通のため，ポートが異なっていても同じ VLAN の場合は同じ VLAN Tag の VLAN ID を設定してください。

25.5　L2 プロトコルフレーム透過機能の解説

25.5.1　概要

この機能は，レイヤ 2 のプロトコルフレームを中継する機能です。中継するフレームにはスパニングツリーの BPDU，IEEE802.1X の EAPOL があります。通常，これらレイヤ 2 のプロトコルフレームは中継しません。

中継するフレームは本装置では単なるマルチキャストフレームとして扱い，本装置のプロトコルには使用しません。

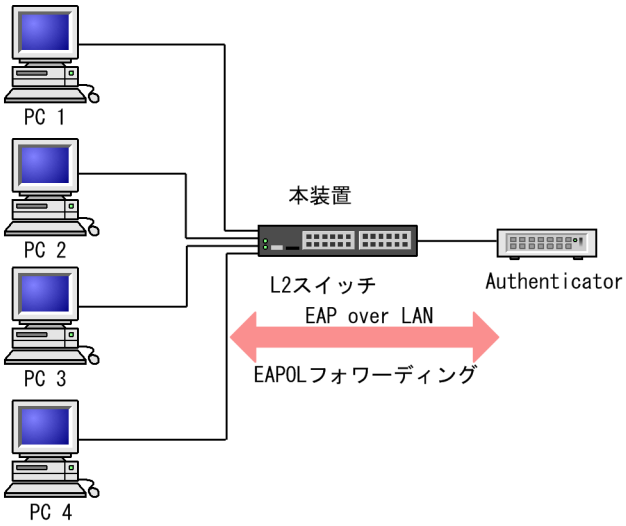
(1)　BPDU フォワーディング機能

本装置でスパニングツリーを使用しない場合に BPDU を中継できます。VLAN トンネリングでこの機能を使用すると，ユーザの BPDU を通過させることができます。その際，VLAN トンネリング網のすべてのエッジ装置，コア装置で BPDU フォワーディング機能を設定する必要があります。

(2)　EAPOL フォワーディング機能

本装置で IEEE802.1X を使用しない場合に EAPOL を中継できます。本装置を，Authenticator と端末（Supplicant）の間の L2 スイッチとして用いるときにこの機能を使用します。

図 25-4　EAPOL フォワーディング機能の適用例



25.5.2　L2 プロトコルフレーム透過機能の注意事項

(1)　他機能との共存

「22.3　レイヤ 2 スイッチ機能と他機能の共存について」を参照してください。

25.6　L2 プロトコルフレーム透過機能のコマンドガイド

25.6.1　コマンド一覧

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コマンド一覧を次の表に示します。

表 25-3　コンフィグレーションコマンド一覧

コマンド名	説明
l2protocol-tunnel eap	IEEE802.1X の EAPOL を中継します。
l2protocol-tunnel stp	スパニングツリーの BPDU を中継します。

25.6.2　L2 プロトコルフレーム透過機能の設定

(1)　BPDU フォワーディング機能の設定

[設定のポイント]

本機能の設定は装置単位で有効になります。設定すると，BPDU をすべての VLAN で中継します。

BPDU フォワーディング機能は，本装置のスパニングツリーを停止してから設定する必要があります。

[コマンドによる設定]

1. **(config)# spanning-tree disable**
   (config)# l2protocol-tunnel stp

   BPDU フォワーディング機能を設定します。事前にスパニングツリーを停止し，BPDU フォワーディング機能を設定します。本装置は BPDU をプロトコルフレームとして扱わないで中継します。

(2)　EAPOL フォワーディング機能の設定

[設定のポイント]

本機能の設定は装置単位で有効になります。設定すると，EAPOL をすべての VLAN で中継します。

EAPOL フォワーディング機能と IEEE802.1X は同時に使用することはできません。

[コマンドによる設定]

1. **(config)# l2protocol-tunnel eap**

   EAPOL フォワーディング機能を設定します。本装置は EAPOL をプロトコルフレームとして扱わないで中継します。

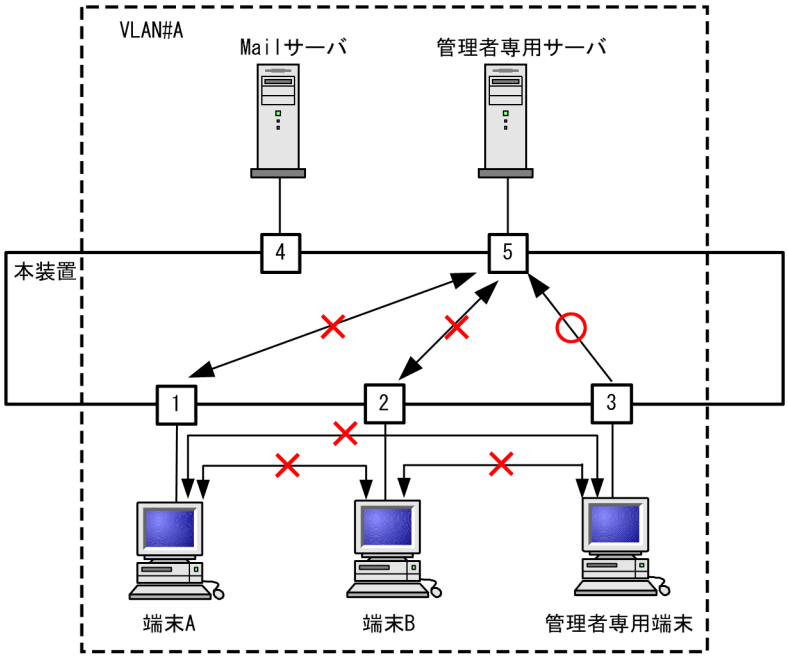
25.7　ポート間中継遮断機能の解説

25.7.1　概要

ポート間中継遮断機能は，指定したポートですべての通信を遮断する機能です。特定のポートからのアクセスだけを許可するサーバの接続や，直接の通信を遮断したい端末の接続などに適用することによってセキュリティを確保できます。

次の図に適用例を示します。この例では，管理者専用サーバは通常の端末からのアクセスを遮断して，管理者専用端末からだけアクセスできます。また，端末間は直接の通信を遮断し，各端末のセキュリティを確保します。

図 25-5　ポート間中継遮断機能の適用例



・管理者用サーバへは管理者専用端末からだけ通信を許可し，
　ほかの端末からの通信を遮断します
・端末間は直接の通信を遮断します
・Mailサーバはすべての端末から通信を可能とします

25.7.2　ポート間中継遮断機能使用時の注意事項

(1)　他機能との共存

「22.3　レイヤ 2 スイッチ機能と他機能の共存について」を参照してください。

(2)　一つのポートに複数の VLAN を設定したポート間の遮断について

ポート間中継遮断機能は，VLAN 内のレイヤ 2 中継のすべての通信を遮断します。

(3)　スパニングツリーを同時に使用するときの注意事項

通信を遮断したポートでスパニングツリーを運用するとトポロジーによって通信できなくなる場合があります。

(4)　ポート間中継遮断機能で遮断されないフレームについて

ポート間中継遮断機能は，ハードウェアで中継するフレームだけを遮断します。ソフトウェアで中継するフレームは遮断しません。ソフトウェアで中継するフレームについては，「22.3　レイヤ 2 スイッチ機能と他機能の共存について」を参照してください。

(5)　中継を遮断するポートにチャネルグループに所属するポートを指定した場合

指定したポートが所属するチャネルグループと同じグループに所属するすべてのポートからの中継を遮断します。

25.8　ポート間中継遮断機能のコマンドガイド

25.8.1　コマンド一覧

ポート間中継遮断機能のコンフィグレーションコマンド一覧を次の表に示します。

表 25-4　コンフィグレーションコマンド一覧

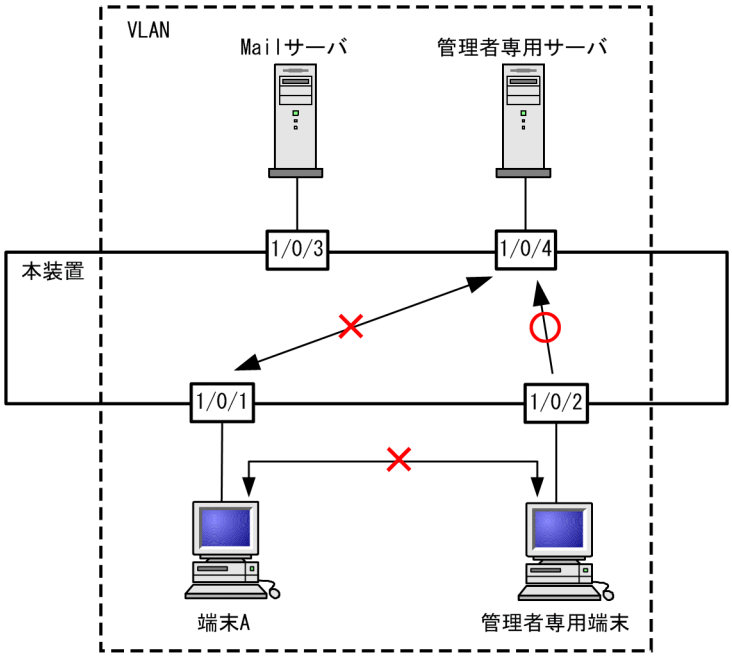
コマンド名	説明
switchport isolation	指定したポートへの中継を遮断します。

25.8.2　ポート間中継遮断機能の設定

ポート間中継遮断機能を設定する手順を次に示します。ここでは，図に示す構成の設定例を示します。

構成例では，ポート 1/0/1 からポート 1/0/4 への通信を遮断します。また，ポート 1/0/1，1/0/2 間の通信を遮断します。ポート 1/0/3 はどのポートとも通信が可能です。

図 25-6　ポート間中継遮断機能の設定例



・管理者用サーバへは管理者専用端末からだけ通信を許可し，
　ほかの端末からの通信を遮断します
・端末間は直接の通信を遮断します
・Mailサーバはすべての端末から通信を可能とします

[設定のポイント]

ポート間中継遮断機能は，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で，そのポートからの通信を許可しないポートを指定することで設定します。通信を双方向で遮断するためには，遮断したい各ポートで設定する必要があります。

[コマンドによる設定]

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

   ポート 1/0/1 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)# switchport isolation interface gigabitethernet 1/0/2, gigabitethernet 1/0/4**

   (config-if)# exit

   ポート 1/0/1 でポート 1/0/2，1/0/4 からの中継を遮断します。

3. **(config)# interface gigabitethernet 1/0/2**

   (config-if)# switchport isolation interface gigabitethernet 1/0/1

   (config-if)# exit

   ポート 1/0/2 のイーサネットインタフェースコンフィグレーションモードに移行し，ポート 1/0/2 でポート 1/0/1 からの中継を遮断します。この設定によって，ポート 1/0/1，1/0/2 間は双方向で通信を遮断します。

4. **(config)# interface gigabitethernet 1/0/4**

   (config-if)# switchport isolation interface gigabitethernet 1/0/1

   ポート 1/0/4 のイーサネットインタフェースコンフィグレーションモードに移行し，ポート 1/0/4 でポート 1/0/1 からの中継を遮断します。この設定によって，ポート 1/0/1，1/0/4 間は双方向で通信を遮断します。

25.8.3　遮断するポートの変更

[設定のポイント]

switchport isolation add コマンドおよび switchport isolation remove コマンドでポート間中継遮断機能で遮断するポートを変更します。すでに設定したポートで switchport isolation <interface id list>によって一括して指定した場合，指定した設定に置き換わります。

[コマンドによる設定]

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

   (config-if)# switchport isolation interface gigabitethernet 1/0/2-10

   ポート 1/0/1 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，ポート 1/0/2～1/0/10 からポート 1/0/1 への中継を遮断します。

2. **(config-if)# switchport isolation interface add gigabitethernet 1/0/11**

   (config-if)# switchport isolation interface remove gigabitethernet 1/0/5

   ポート 1/0/1 への遮断にポート 1/0/11 を追加します。また，ポート 1/0/5 の設定を解除します。この状態で，ポート 1/0/2～1/0/4，1/0/6～1/0/11 からポート 1/0/1 への通信を遮断します。

3. **(config-if)# switchport isolation interface gigabitethernet 1/0/3-4**

   ポート 1/0/1 への中継を遮断するポートを 1/0/3～1/0/4 に設定します。以前の設定はすべて上書きされ，ポート 1/0/3～1/0/4 からの中継だけを遮断しそのほかのポートは通信を可能とします。

25.9　VLAN debounce 機能の解説

25.9.1　概要

VLAN インタフェースは VLAN が通信可能な状態になったときにアップし，VLAN のポートがダウンした場合や，スパニングツリーなどの機能でブロッキング状態になり通信できなくなった場合にダウンします。

VLAN debounce 機能は，VLAN インタフェースのアップやダウンを遅延させて，ネットワークトポロジーの変更や，運用メッセージ，SNMP 通知などを削減する機能です。

スパニングツリーや Ring Protocol などレイヤ 2 での冗長構成を使用したときに障害が発生した場合，通常レイヤ 3 のトポロジー変更と比べて短い時間で代替経路へ切り替わります。VLAN debounce 機能によってレイヤ 2 での代替経路への切替時間まで VLAN インタフェースのダウンを遅延させると，レイヤ 3 のトポロジーを変化させずにすみ，通信の可用性を確保できます。

レイヤ 3 での冗長構成を使用する場合，マスター側に障害が発生したあとの回復時に，両系がマスターとして動作することを防ぐために VLAN インタフェースのアップを遅延させたいとき, VLAN debounce 機能で VLAN インタフェースのアップを遅延できます。

25.9.2　VLAN debounce 機能と他機能との関係

(1)　スパニングツリー

スパニングツリーでは，ポートに障害が発生して代替経路へ変更されるまでに，スパニングツリーのトポロジーの変更に必要な時間が掛かります。この間に VLAN インタフェースをダウンさせたくない場合は，VLAN インタフェースのダウン遅延時間をトポロジーの変更に必要な時間以上に設定してください。

(2)　Ring Protocol

Ring Protocol を使用する場合，マスタノードではプライマリポートがフォワーディング，セカンダリポートがブロッキングとなっています。VLAN debounce 機能を使わない場合，プライマリポートで障害が発生するといったん VLAN インタフェースがダウンし，セカンダリポートのブロッキングが解除されると再び VLAN インタフェースがアップします。

このようなときに VLAN がいったんダウンすることを防ぐためには, VLAN インタフェースのダウン遅延時間を設定してください。

(3)　その他の冗長化機能

スパニングツリーや Ring Protocol 以外の冗長化を使用する場合でも，VLAN が短時間にアップやダウンを繰り返すときには，VLAN debounce 機能を使用するとアップやダウンを抑止できます。

25.9.3　VLAN debounce 機能使用時の注意事項

(1)　ダウン遅延時間の注意事項

ダウン遅延時間を設定すると，回復しない障害が発生した場合でも VLAN のダウンが遅延します。VLAN debounce 機能でダウンが遅延している間は，通信できない状態です。ダウン遅延時間は，ネットワークの構成や運用に応じて必要な値を設定してください。

VLAN に status コマンドで suspend を設定した場合や VLAN のポートをすべて削除した場合など，コンフィグレーションを変更しないとその VLAN が通信可能とならない場合には，ダウン遅延時間を設定していても VLAN のダウンは遅延しません。

(2)　アップ遅延時間の注意事項

アップ遅延時間を設定すると，いったんアップした VLAN がダウンしたあと，再度アップするときにアップが遅延します。装置を再起動したり，restart vlan コマンドで VLAN プログラムを再起動したりすると，VLAN は初期状態になるため，アップ遅延時間を設定していても VLAN のアップは遅延しません。

(3)　遅延時間の誤差に関する注意事項

アップまたはダウン遅延時間は，ソフトウェアのタイマを使用しているため，CPU 利用率が高い場合には設定した時間より大きくなることがあります。

25.10　VLAN debounce 機能のコマンドガイド

25.10.1　コマンド一覧

VLAN debounce 機能のコンフィグレーションコマンド一覧を次の表に示します。

表 25-5　コンフィグレーションコマンド一覧

コマンド名	説明
down-debounce	VLAN インタフェースのダウン遅延時間を指定します。
up-debounce	VLAN インタフェースのアップ遅延時間を指定します。

25.10.2　VLAN debounce 機能の設定

VLAN debounce 機能を設定する手順を次に示します。

[設定のポイント]

VLAN debounce 機能の遅延時間は，ネットワーク構成および運用に合わせて最適な値を設定します。

[コマンドによる設定]

1. **(config)# interface vlan 100**
   VLAN 100 の VLAN インタフェースモードに移行します。
2. **(config-if)# down-debounce 2**
   (config-if)# exit
   VLAN 100 のダウン遅延時間を 2 秒に設定します。
3. **(config)# interface range vlan 201-300**
   VLAN 201-300 の複数 VLAN インタフェースモードに移行します。
4. **(config-if-range)# down-debounce 3**
   (config-if-range)# exit
   VLAN 201-300 のダウン遅延時間を 3 秒に設定します。

26 スパニングツリー

この章では，スパニングツリー機能の解説と操作方法について説明します。

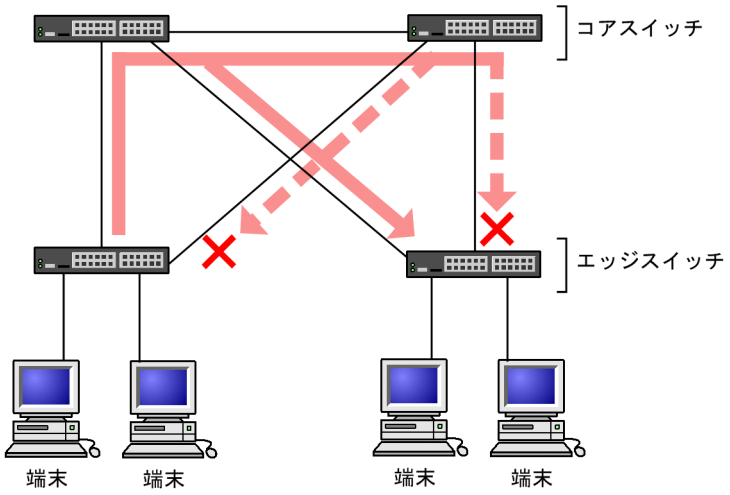
26.1　スパニングツリーの概説

26.1.1　概要

スパニングツリープロトコルは，レイヤ２のループ防止プロトコルです。スパニングツリープロトコルを使用することで，レイヤ２ネットワークを冗長化し，ループを防止できます。

スパニングツリーを適用したネットワークの概要を次の図に示します。

図 26-1　スパニングツリーを適用したネットワークの概要



（凡例）×：Blocking状態

図の構成は，ネットワークのコアを担うスイッチを冗長化し，また，端末を収容するエッジスイッチからの通信経路を冗長化しています。装置および通信経路を冗長化することで，通常の通信経路に障害が発生しても代替の経路で通信を継続できます。

レイヤ２ネットワークを冗長化するとレイヤ２ループの構成になります。レイヤ２のループはブロードキャストストームの発生や MAC アドレス学習が安定しないなどの問題を引き起こします。スパニングツリーは，冗長化してループ構成になったレイヤ２ネットワークで，通信を止める場所を選択して Blocking 状態とすることでループを防止するプロトコルです。

26.1.2　スパニングツリーの種類

本装置では，PVST+，シングルスパニングツリーおよびマルチプルスパニングツリーの３種類のスパニングツリーをサポートします。各スパニングツリーは構築の単位が異なります。スパニングツリーの種類と概要について次の表に示します。

表 26-1　スパニングツリーの種類

名称	構築単位	概要
PVST+	VLAN 単位	VLAN 単位にツリーを構築します。一つのポートに複数の VLAN が所属している場合，VLAN ごとに異なるツリー構築結果を適用します。

名称	構築単位	概要
シングルスパニングツリー	装置単位	装置全体のポートを対象としツリーを構築します。 VLAN 構成とは無関係に装置のすべてのポートにツリー構築結果を適用します。
マルチプルスパニングツリー	MST インスタンス単位	複数の VLAN をまとめた MST インスタンスというグループごとにスパニングツリーを構築します。一つのポートに複数の VLAN が所属している場合，MST インスタンス単位に異なるツリー構築結果を適用します。

本装置では，上記で記述したスパニングツリーを単独または組み合わせて使用できます。スパニングツリーの組み合わせと適用範囲を次の表に示します。

表 26-2　スパニングツリーの組み合わせと適用範囲

ツリー構築条件	トポロジー計算結果の適用範囲
PVST+単独	PVST+が動作している VLAN には VLAN ごとのスパニングツリーを適用します。そのほかの VLAN はスパニングツリーを適用しません。 本装置では，デフォルトでポート VLAN 上で PVST+が動作します。
シングルスパニングツリー単独	全 VLAN にシングルスパニングツリーを適用します。 PVST+をすべて停止した構成です。
PVST+とシングルスパニングツリーの組み合わせ	PVST+が動作している VLAN には VLAN ごとのスパニングツリーを適用します。そのほかの VLAN にはシングルスパニングツリーを適用します。
マルチプルスパニングツリー単独	全 VLAN にマルチプルスパニングツリーを適用します。

注　マルチプルスパニングツリーはほかのツリーと組み合わせて使用できません。

26.1.3　スパニングツリーと高速スパニングツリー

PVST+，シングルスパニングツリーには IEEE802.1D のスパニングツリーと IEEE802.1w の高速スパニングツリーの 2 種類があります。それぞれ，PVST+と Rapid PVST+，STP と Rapid STP と呼びます。

スパニングツリープロトコルのトポロジー計算は，通信経路を変更する際にいったんポートを通信不可状態（Blocking 状態）にしてから複数の状態を遷移して通信可能状態（Forwarding 状態）になります。IEEE 802.1D のスパニングツリーはこの状態遷移においてタイマによる状態遷移を行うため，通信可能となるまでに一定の時間が掛かります。IEEE 802.1w の高速スパニングツリーはこの状態遷移でタイマによる待ち時間を省略して高速な状態遷移を行うことで，トポロジー変更によって通信が途絶える時間を最小限にします。

なお，マルチプルスパニングツリーは IEEE802.1s として規格化されたもので，状態遷移の時間は IEEE802.1w と同等です。それぞれのプロトコルの状態遷移とそれに必要な時間を以下に示します。

表 26-3　PVST+，STP(シングルスパニングツリー)の状態遷移

状態	状態の概要	次の状態への遷移
Disable	ポートが使用できない状態です。使用可能となるとすぐに Blocking に遷移します。	−

状態	状態の概要	次の状態への遷移
Blocking	通信不可の状態で，MAC アドレス学習も行いません。リンクアップ直後またはトポロジーが安定して Blocking になるポートもこの状態になります。	20 秒(変更可能)または BPDU を受信
Listening	通信不可の状態で，MAC アドレス学習も行いません。該当ポートが Learning になる前に，トポロジーが安定するまで待つ期間です。	15 秒(変更可能)
Learning	通信不可の状態です。しかし，MAC アドレス学習は行います。該当ポートが Forwarding になる前に，事前に MAC アドレス学習を行う期間です。	15 秒(変更可能)
Forwarding	通信可能の状態です。トポロジーが安定した状態です。	－

（凡例）－：該当なし

表 26–4　Rapid PVST+，Rapid STP(シングルスパニングツリー)の状態遷移

状態	状態の概要	次の状態への遷移
Disable	ポートが使用できない状態です。使用可能となるとすぐに Discarding に遷移します。	－
Discarding	通信不可の状態で，MAC アドレス学習も行いません。該当ポートが Learning になる前に，トポロジーが安定するまで待つ期間です。	省略または 15 秒(変更可能)
Learning	通信不可の状態です。しかし，MAC アドレス学習は行います。該当ポートが Forwarding になる前に，事前に MAC アドレス学習を行う期間です。	省略または 15 秒(変更可能)
Forwarding	通信可能の状態です。トポロジーが安定した状態です。	－

（凡例）－：該当なし

Rapid PVST+，Rapid STP では，対向装置からの BPDU 受信によって Discarding と Learning 状態を省略します。この省略により，高速なトポロジー変更を行います。

高速スパニングツリーを使用する際は，以下の条件に従って設定してください。条件を満たさない場合，Discarding，Learning を省略しないで高速な状態遷移を行わない場合があります。

- トポロジーの全体を同じプロトコル（Rapid PVST+または Rapid STP）で構築する（Rapid PVST+と Rapid STP の相互接続は「26.3.2　アクセスポートの PVST+」を参照してください)。
- スパニングツリーが動作する装置間は Point-to-Point 接続する。
- スパニングツリーが動作する装置を接続しないポートでは PortFast を設定する。

26.1.4　スパニングツリートポロジーの構成要素

スパニングツリーのトポロジーを設計するためには，ブリッジやポートの役割およびそれらの役割を決定するために用いる識別子などのパラメータがあります。これらの構成要素とトポロジー設計における利用方法を以下に示します。

(1)　ブリッジの役割

ブリッジの役割を次の表に示します。スパニングツリーのトポロジー設計はルートブリッジを決定することから始まります。

表 26-5　ブリッジの役割

ブリッジの役割	概要
ルートブリッジ	トポロジーを構築する上で論理的な中心となるスイッチです。トポロジー内に一つだけ存在します。
指定ブリッジ	ルートブリッジ以外のスイッチです。ルートブリッジの方向からのフレームを転送する役割を担います。

(2)　ポートの役割

ポートの役割を次の表に示します。指定ブリッジは 3 種類のポートの役割を持ちます。ルートブリッジは，以下の役割のうち，すべてのポートが指定ポートとなります。

表 26-6　ポートの役割

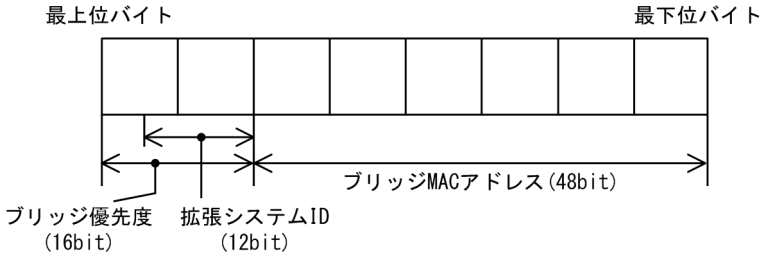
ポートの役割	概要
ルートポート	指定ブリッジからルートブリッジへ向かう通信経路のポートです。通信可能なポートとなります。
指定ポート	ルートポート以外の通信可能なポートです。ルートブリッジからの通信経路でトポロジーの下流へ接続するポートです。
非指定ポート	ルートポート，指定ポート以外のポートで，通信不可の状態のポートです。障害が発生した際に通信可能になり代替経路として使用します。

(3)　ブリッジ識別子

トポロジー内の装置を識別するパラメータをブリッジ識別子と呼びます。ブリッジ識別子が最も小さい装置が優先度が高く，ルートブリッジとして選択されます。

ブリッジ識別子はブリッジ優先度（16bit）とブリッジ MAC アドレス（48bit）で構成されます。ブリッジ優先度の下位 12bit は拡張システム ID です。拡張システム ID には，シングルスパニングツリー，マルチプルスパニングツリーの場合は 0 が設定され，PVST+の場合は VLAN ID が設定されます。ブリッジ識別子を次の図に示します。

図 26-2　ブリッジ識別子



(4) パスコスト

スイッチ上の各ポートの通信速度に対応するコスト値をパスコストと呼びます。指定ブリッジからルートブリッジへ到達するために経由するすべてのポートのコストを累積した値をルートパスコストと呼びます。ルートブリッジへ到達するための経路が 2 種類以上ある場合，ルートパスコストが最も小さい経路を使用します。

PVST+およびシングルスパニングツリーのパスコスト値には short（16bit 値），long（32bit 値）の 2 種類があり，トポロジーの全体で合わせる必要があります。速度が 10Gbit/s 以上のポートを使用する場合は long（32bit 値）を使用することをお勧めします。本装置のデフォルトでは short（16bit 値）で動作します。マルチプルスパニングツリーは long（32bit 値）だけです。イーサネットインタフェースの速度による自動的な設定は，short（16bit 値）か long（32bit 値）かで設定内容が異なります。

速度が速いポートほどパスコストを低くすることをお勧めしています。パスコストはデフォルト値がポートの速度に応じた値となっていて，コンフィグレーションで変更することもできます。速度に応じたデフォルト値については，「コンフィグレーションコマンドレファレンス」で，次に示すコンフィグレーションコマンドの説明を参照してください。

PVST+の場合

- spanning-tree pathcost method
- spanning-tree vlan pathcost method

シングルスパニングツリーの場合

- spanning-tree pathcost method
- spanning-tree single pathcost method

マルチプルスパニングツリーの場合

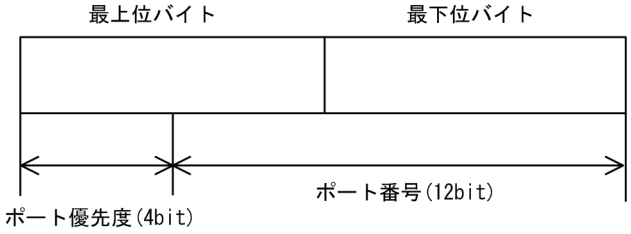
- spanning-tree pathcost method の long

(5) ポート識別子

スイッチ内の各ポートを識別するパラメータをポート識別子と呼びます。ポート識別子は 2 台のスイッチ間で 2 本以上の冗長接続をし，かつ各ポートでパスコストを変更できない場合に通信経路の選択に使用します。ただし，2 台のスイッチ間の冗長接続はリンクアグリゲーションを使用することをお勧めします。リンクアグリゲーションをサポートしていない装置と冗長接続するためにはスパニングツリーを使用してください。

ポート識別子はポート優先度（4bit）とポート番号（12bit）によって構成されます。ポート識別子を次の図に示します。

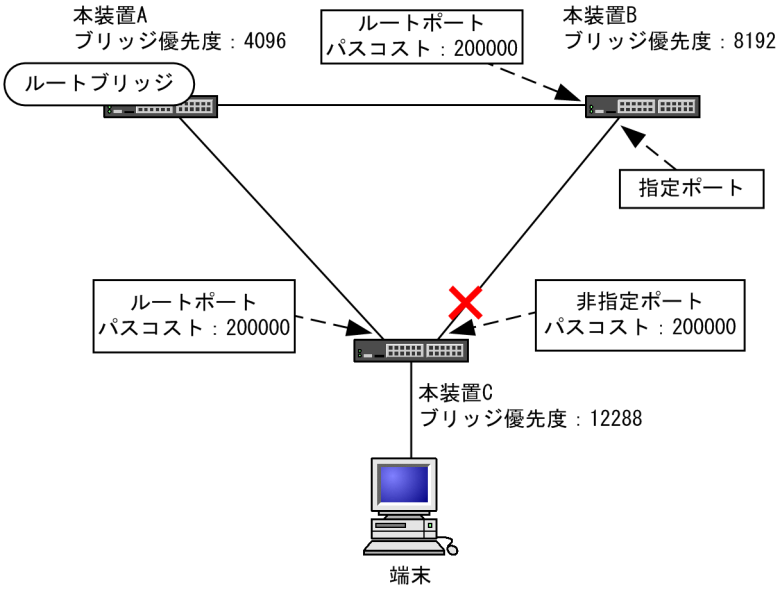
図 26-3 ポート識別子



26.1.5　スパニングツリーのトポロジー設計

スパニングツリーは，ブリッジ識別子，パスコストによってトポロジーを構築します。次の図に，トポロジー設計の基本的な手順を示します。図の構成は，コアスイッチとして 2 台を冗長化して，エッジスイッチとして端末を収容するスイッチを配置する例です。

図 26-4　スパニングツリーのトポロジー設計



（凡例）×　：Blocking状態

(1)　ブリッジ識別子によるルートブリッジの選出

ルートブリッジは，ブリッジ識別子の最も小さい装置を選出します。通常，ルートブリッジにしたい装置のブリッジ優先度を最も小さい値（最高優先度）に設定します。図の例では，本装置 A がルートブリッジになるように設定します。本装置 B，本装置 C は指定ブリッジとなります。

また，ルートブリッジに障害が発生した場合に代替のルートブリッジとして動作するスイッチを本装置 B になるように設定します。本装置 C は最も低い優先度として設定します。

スパニングツリーのトポロジー設計では，図の例のようにネットワークのコアを担う装置をルートブリッジとし，代替のルートブリッジとしてコアを冗長化する構成をお勧めします。

(2)　通信経路の設計

ルートブリッジを選出した後，各指定ブリッジからルートブリッジに到達するための通信経路を決定します。

(a)　パスコストによるルートポートの選出

本装置 B，本装置 C では，ルートブリッジに到達するための経路を最も小さいルートパスコスト値になるよう決定します。図の例は，すべてのポートがパスコスト 200000 としています。それぞれ直接接続したポートが最もルートパスコストが小さく，ルートポートとして選出します。

ルートパスコストの計算は，指定ブリッジからルートブリッジへ向かう経路で，各装置がルートブリッジの方向で送信するポートのパスコストの総和で比較します。例えば，本装置 C の本装置 B を経由する経路はパスコストが 400000 となりルートポートには選択されません。

パスコストは，ポートの速度が速いほど小さい値をデフォルト値に持ちます。また，ルートポートの選択にはルートブリッジまでのコストの総和で比較します。そのため，速度の速いポートや経由する装置の段数が少ない経路を優先して使用したい場合，通常はパスコスト値を変更する必要はありません。速度の遅いポートを速いポートより優先して経路として使用したい場合はコンフィグレーションで変更することによって通信したい経路を設計します。

(b) 指定ポート，非指定ポートの選出

本装置 B，本装置 C 間の接続はルートポート以外のポートでの接続になります。このようなポートではどれかのポートが非指定ポートとなって Blocking 状態になります。スパニングツリーは，このように片側が Blocking 状態となることでループを防止します。

指定ポート，非指定ポートは次のように選出します。

- 装置間でルートパスコストが小さい装置が指定ポート，大きい装置が非指定ポートになります。
- ルートパスコストが同一の場合，ブリッジ識別子の小さい装置が指定ポート，大きい装置が非指定ポートになります。

図の例では，ルートパスコストは同一です。ブリッジ優先度によって本装置 B が指定ポート，本装置 C が非指定ポートとなり，本装置 C が Blocking 状態となります。Blocking 状態になるポートを本装置 B にしたい場合は，パスコストを調整して本装置 B のルートパスコストが大きくなるように設定します。

26.1.6 STP 互換モード

(1) 概要

Rapid PVST+，Rapid STP，およびマルチプルスパニングツリーで，対向装置が PVST+または STP の場合，該当するポートは STP 互換モードで動作します。

STP 互換モードで動作すると，該当するポートで高速遷移が行われなくなり，通信復旧に時間が掛かるようになります。

対向装置が Rapid PVST+，Rapid STP，およびマルチプルスパニングツリーに変わった場合，STP 互換モードから復旧し，再び高速遷移が行われるようになりますが，タイミングによって該当するポートと対向装置が STP 互換モードで動作し続けることがあります。

STP 互換モード復旧機能は，STP 互換モードで動作しているポートを強制的に復旧させ，正常に高速遷移ができるようにします。

(2) 復旧機能

運用コマンド clear spanning-tree detected-protocol を実行することで，STP 互換モードから強制的に復旧します。該当するポートのリンクタイプが point-to-point，shared のどちらの場合でも動作します。

(3) 自動復旧機能

該当するポートのリンクタイプが point-to-point の場合，STP 互換モード復旧機能が自動で動作します。

該当するポートが非指定ポートで STP 互換モードで動作した場合，該当するポートから RST BPDU または MST BPDU を送信することで，STP 互換モードを解除します。

該当するポートのリンクタイプが shared の場合，自動復旧モードが正しく動作できないため，自動復旧モードは動作しません。

26.1.7　スパニングツリー共通の注意事項

(1)　CPU の過負荷について

CPU が過負荷な状態になった場合，本装置が送受信する BPDU の廃棄が発生して，タイムアウトのメッセージ出力，トポロジー変更，一時的な通信断となることがあります。

(2)　VLAN のダウンを伴うコンフィグレーションコマンドの設定について

コンフィグレーションコマンド no spanning-tree disable で本装置にスパニングツリー機能を適用すると，全 VLAN が一時的にダウンします。

26.2　スパニングツリーのコマンドガイド

スパニングツリーの動作モードを設定します。

コンフィグレーションを設定しない状態で本装置を起動すると，動作モードは pvst で動作します。

26.2.1　コマンド一覧

スパニングツリーのコンフィグレーションコマンド一覧を次の表に示します。

表 26–7　コンフィグレーションコマンド一覧

コマンド名	説明
spanning-tree disable	スパニングツリー機能の停止を設定します。
spanning-tree mode	スパニングツリー機能の動作モードを設定します。
spanning-tree single mode	シングルスパニングツリーの STP と Rapid STP を選択します。
spanning-tree vlan mode	VLAN ごとに PVST+と Rapid PVST+を選択します。

スパニングツリーの運用コマンド一覧を次の表に示します。

表 26–8　運用コマンド一覧

コマンド名	説明
show spanning-tree	スパニングツリー情報を表示します。
show spanning-tree statistics	スパニングツリーの統計情報を表示します。
clear spanning-tree statistics	スパニングツリーの統計情報をクリアします。
clear spanning-tree detected-protocol	スパニングツリーの STP 互換モードを強制回復します。
show spanning-tree port-count	スパニングツリーの収容数を表示します。
restart spanning-tree	スパニングツリープログラムを再起動します。
dump protocols spanning-tree	スパニングツリーで採取している詳細イベントトレース情報および制御テーブル情報をファイルへ出力します。

26.2.2　動作モードの設定

スパニングツリーは装置の動作モードを設定することで各種スパニングツリーを使用することができます。装置の動作モードを次の表に示します。動作モードを設定しない場合，pvst モードで動作します。

動作モードに rapid-pvst を指定しても，シングルスパニングツリーのデフォルトは STP であることに注意してください。

表 26–9　スパニングツリー動作モード

コマンド名	説明
spanning-tree disable	スパニングツリーを停止します。

コマンド名	説明
spanning-tree mode pvst	PVST+とシングルスパニングツリーを使用できます。デフォルトでPVST+が動作します。シングルスパニングツリーはデフォルトでは動作しません。
spanning-tree mode rapid-pvst	PVST+とシングルスパニングツリーを使用できます。デフォルトで高速スパニングツリーの Rapid PVST+が動作します。シングルスパニングツリーはデフォルトでは動作しません。
spanning-tree mode mst	マルチプルスパニングツリーが動作します。

(1)　動作モード pvst の設定

[設定のポイント]

装置の動作モードを pvst に設定します。ポート VLAN を作成すると，その VLAN で自動的にPVST+が動作します。VLAN ごとに Rapid PVST+に変更することもできます。

シングルスパニングツリーはデフォルトでは動作しないで，設定することで動作します。その際，デフォルトでは STP で動作し，Rapid STP に変更することもできます。

[コマンドによる設定]

1. **(config)# spanning-tree mode pvst**

   スパニングツリーの動作モードを pvst に設定します。ポート VLAN で自動的に PVST+が動作します。

2. **(config)# spanning-tree vlan 10 mode rapid-pvst**

   VLAN 10 の動作モードを Rapid PVST+に変更します。ほかのポート VLAN は PVST+で動作し，VLAN 10 は Rapid PVST+で動作します。

3. **(config)# spanning-tree single**

   シングルスパニングツリーを動作させます。PVST+を使用していない VLAN に適用します。デフォルトでは STP で動作します。

4. **(config)# spanning-tree single mode rapid-stp**

   シングルスパニングツリーを Rapid STP に変更します。

(2)　動作モード rapid-pvst の設定

[設定のポイント]

装置の動作モードを rapid-pvst に設定します。ポート VLAN を作成すると，その VLAN で自動的にRapid PVST+が動作します。VLAN ごとに PVST+に変更することもできます。

シングルスパニングツリーはデフォルトでは動作しないで，設定することで動作します。動作モードにrapid-pvst を指定しても，シングルスパニングツリーのデフォルトは STP であることに注意してください。

[コマンドによる設定]

1. **(config)# spanning-tree mode rapid-pvst**

   スパニングツリーの動作モードを rapid-pvst に設定します。ポート VLAN で自動的に Rapid PVST+が動作します。

2. **(config)# spanning-tree vlan 10 mode pvst**

VLAN 10 の動作モードを PVST+に変更します。ほかのポート VLAN は Rapid PVST+で動作し，VLAN 10 は PVST+で動作します。

3. **(config)# spanning-tree single**
   シングルスパニングツリーを動作させます。PVST+を使用していない VLAN に適用します。デフォルトでは STP で動作します。
4. **(config)# spanning-tree single mode rapid-stp**
   シングルスパニングツリーを Rapid STP に変更します。

(3) 動作モード mst の設定

[設定のポイント]

マルチプルスパニングツリーを使用する場合，装置の動作モードを mst に設定します。マルチプルスパニングツリーはすべての VLAN に適用します。PVST+やシングルスパニングツリーとは併用できません。

[コマンドによる設定]

1. **(config)# spanning-tree mode mst**
   マルチプルスパニングツリーを動作させます。

(4) スパニングツリーを停止する設定

[設定のポイント]

スパニングツリーを使用しない場合，disable を設定することで本装置のスパニングツリーをすべて停止します。

[コマンドによる設定]

1. **(config)# spanning-tree disable**
   スパニングツリーの動作を停止します。

26.3　PVST+解説

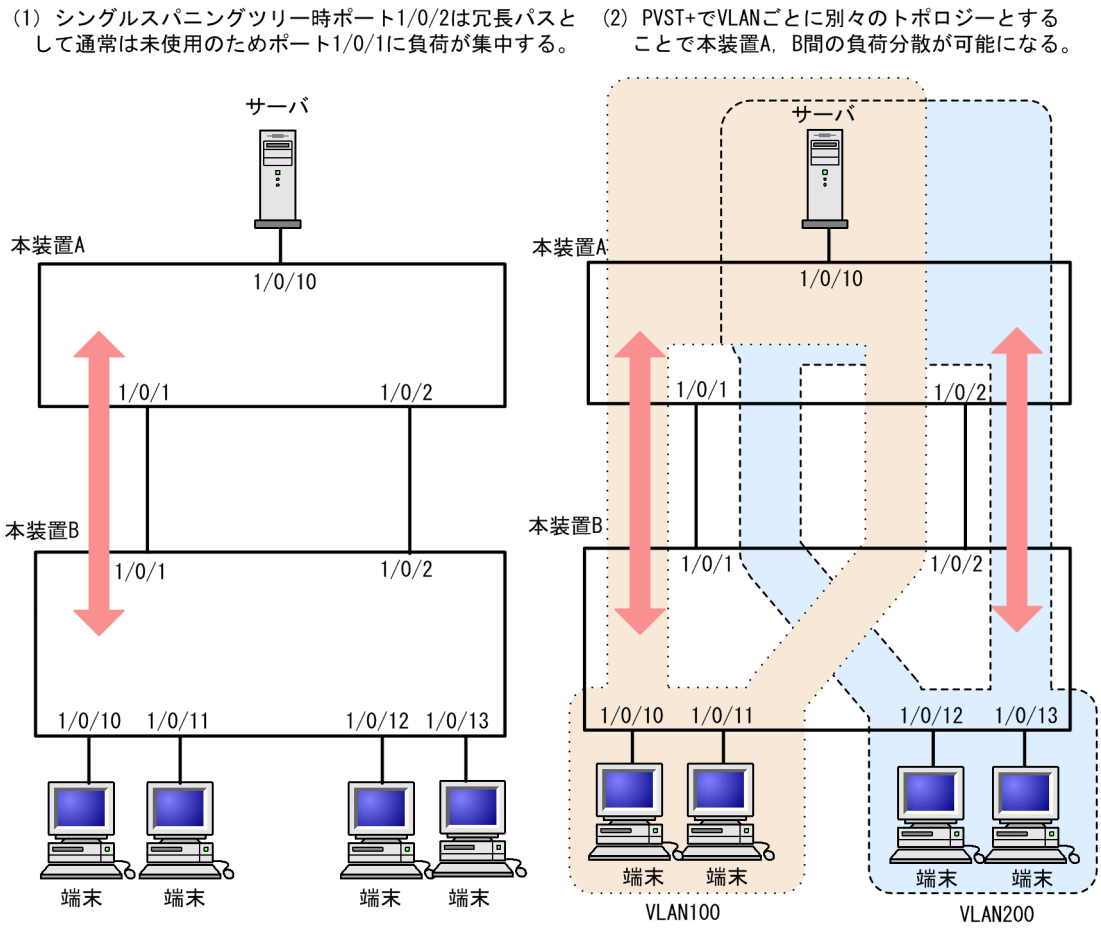
PVST+は，VLAN 単位にツリーを構築します。VLAN 単位にツリーを構築できるため，ロードバランシングが可能です。また，アクセスポートでは，シングルスパニングツリーで動作しているスイッチと接続できます。

26.3.1　PVST+によるロードバランシング

次の図に示すような本装置 A, B 間で冗長パスを組んだネットワークにおいてシングルスパニングツリーを組んだ場合，各端末からサーバへのアクセスは本装置 A，B 間のポート 1 に集中します。そこで，複数の VLAN を組み，PVST+によって VLAN ごとに別々のトポロジーとなるように設定することで冗長パスとして使用できるようになり, さらに負荷分散を図れます。ポート優先度によるロードバランシングの例を次の図に示します。

この例では，VLAN100 に対してはポート 1/0/1 のポート優先度をポート 1/0/2 より高く設定し，逆に VLAN200 に対しては 1/0/2 のポート優先度をポート 1/0/1 より高く設定することで，各端末からサーバに対するアクセスを VLAN ごとに負荷分散を行っています。

図 26-5　PVST+によるロードバランシング



26.3.2　アクセスポートの PVST+

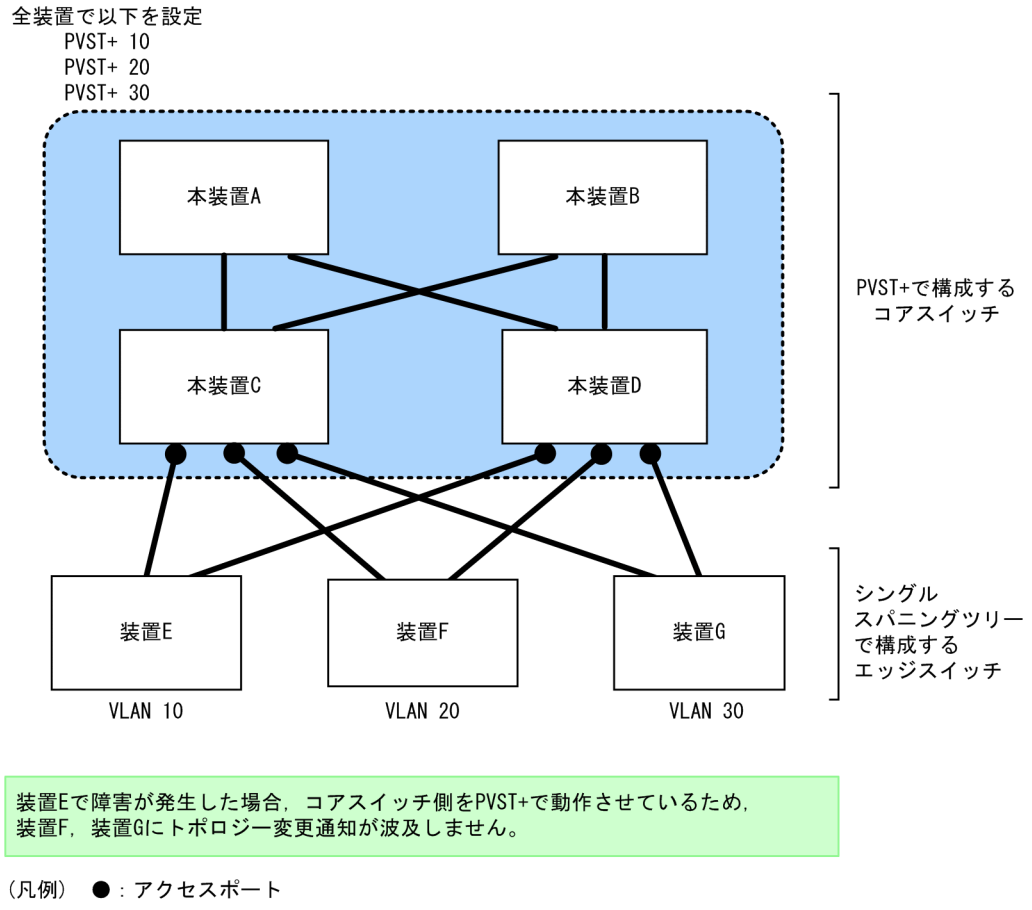
(1)　解説

シングルスパニングツリーを使用している装置，または装置で一つのツリーを持つシングルスパニングツリーに相当する機能をサポートしている装置（以降，単にシングルスパニングツリーと表記します）とPVST+を用いてネットワークを構築できます。シングルスパニングツリーで運用している装置をエッジスイッチ，本装置をコアスイッチに配置して使います。このようなネットワークを構築することで，次のメリットがあります。

- エッジスイッチに障害が発生しても，ほかのエッジスイッチにトポロジー変更の影響が及ばない。
- コアスイッチ間でロードバランスができる。

シングルスパニングツリーとは，アクセスポートで接続できます。構成例を次の図に示します。この例では，エッジスイッチでシングルスパニングツリーを動作させ，コアスイッチで PVST+を動作させています。コアスイッチではエッジスイッチと接続するポートをアクセスポートとしています。各エッジスイッチはそれぞれ単一の VLAN を設定しています。

図 26-6　シングルスパニングツリーとの接続



（凡例）　●：アクセスポート

(2)　アクセスポートでシングルスパニングツリーを混在させた場合

PVST+とシングルスパニングツリーを混在して設定している場合，アクセスポートでは，シングルスパニングツリーは停止状態（Disable）になります。

(3)　構成不一致検出機能

同一 VLAN で接続しているポートについて，本装置でアクセスポート，プロトコルポート，MAC ポートのどれかを設定（Untagged フレームを使用）し，対向装置ではトランクポートを設定（Tagged フレームを使用）した場合，該当 VLAN では通信できないポートとなります。このようなポートを構成不一致として検出します。検出する条件は，本装置がアクセスポートで，対向装置でトランクポートを設定（Tagged フレームを使用）した場合です。この場合，該当するポートを停止状態（Disable）にします。対向装置でトランクポートの設定（Tagged フレームを使用）を削除すれば，hello-time 値×3 秒（デフォルトは 6 秒）後に，自動的に停止状態を解除します。

26.3.3　PVST+使用時の注意事項

(1)　他機能との共存

「22.3　レイヤ 2 スイッチ機能と他機能の共存について」を参照してください。

(2)　VLAN 1（デフォルト VLAN）の PVST+とシングルスパニングツリーについて

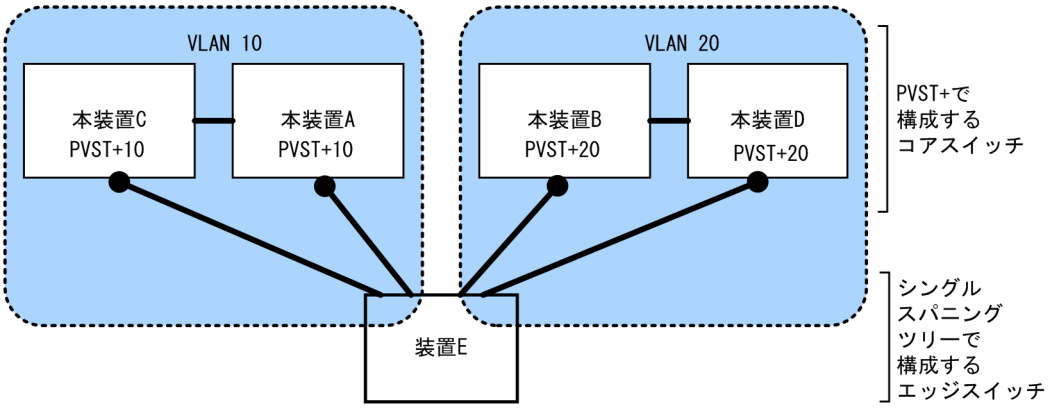
シングルスパニングツリーと VLAN 1 の PVST+を同時に動作させることはできません。シングルスパニングツリーを動作させると VLAN 1 の PVST+は停止します。

(3)　禁止構成

本装置とシングルスパニングツリーで動作する装置は，単一のスパニングツリーで構成してください。複数のスパニングツリーで構成すると正しいトポロジーになりません。

禁止構成の例を次の図に示します。この例では，装置 E のシングルスパニングツリーが複数の PVST+スパニングツリーとトポロジーを構成しているため，正しいトポロジーになりません。

図 26-7　シングルスパニングツリーとの禁止構成例



（凡例）　●：アクセスポート

装置Eは単一のスパニングツリーで構成されていないため，正しいトポロジーになりません。

26.4　PVST+のコマンドガイド

26.4.1　コマンド一覧

PVST+のコンフィグレーションコマンド一覧を次の表に示します。

表 26-10　コンフィグレーションコマンド一覧

コマンド名	説明
spanning-tree cost	ポートごとにパスコストのデフォルト値を設定します。
spanning-tree pathcost method	ポートごとにパスコストに使用する値の幅のデフォルト値を設定します。
spanning-tree port-priority	ポートごとにポート優先度のデフォルト値を設定します。
spanning-tree vlan	PVST+の動作，停止を設定します。
spanning-tree vlan cost	VLAN ごとにパスコスト値を設定します。
spanning-tree vlan forward-time	ポートの状態遷移に必要な時間を設定します。
spanning-tree vlan hello-time	BPDU の送信間隔を設定します。
spanning-tree vlan max-age	送信 BPDU の最大有効時間を設定します。
spanning-tree vlan pathcost method	VLAN ごとにパスコストに使用する値の幅を設定します。
spanning-tree vlan port-priority	VLAN ごとにポート優先度を設定します。
spanning-tree vlan priority	ブリッジ優先度を設定します。
spanning-tree vlan transmission-limit	hello-time 当たりに送信できる最大 BPDU 数を設定します。

26.4.2　PVST+の設定

[設定のポイント]

動作モード pvst，rapid-pvst を設定するとポート VLAN で自動的に PVST+が動作しますが，VLAN ごとにモードの変更や PVST+の動作，停止を設定できます。停止する場合は，no spanning-tree vlan コマンドを使用します。

VLAN を作成するときにその VLAN で PVST+を動作させたくない場合，no spanning-tree vlan コマンドを VLAN 作成前にあらかじめ設定しておくことができます。

[コマンドによる設定]

1. **(config)# no spanning-tree vlan 20**
   VLAN 20 の PVST+の動作を停止します。
2. **(config)# spanning-tree vlan 20**
   停止した VLAN 20 の PVST+を動作させます。

[注意事項]

- PVST+はコンフィグレーションに表示がないときは自動的に動作しています。no spanning-tree vlan コマンドで停止すると，停止状態であることがコンフィグレーションで確認できます。

- PVST+は最大 250 個のポート VLAN まで動作します。それ以上のポート VLAN を作成しても自動的には動作しません。

26.4.3　PVST+のトポロジー設定

(1)　ブリッジ優先度の設定

ブリッジ優先度は，ルートブリッジを決定するためのパラメータです。トポロジーを設計する際に，ルートブリッジにしたい装置を最高の優先度に設定し，ルートブリッジに障害が発生したときのために，次にルートブリッジにしたい装置を 2 番目の優先度に設定します。

[設定のポイント]

ブリッジ優先度は値が小さいほど高い優先度となり，最も小さい値を設定した装置がルートブリッジになります。ルートブリッジはブリッジ優先度と装置の MAC アドレスから成るブリッジ識別子で判定するため，本パラメータを設定しない場合は装置の MAC アドレスが最も小さい装置がルートブリッジになります。

[コマンドによる設定]

1. **(config)# spanning-tree vlan 10 priority 4096**

   VLAN 10 の PVST+のブリッジ優先度を 4096 に設定します。

(2)　パスコストの設定

パスコストは通信経路を決定するためのパラメータです。スパニングツリーのトポロジー設計において，ブリッジ優先度決定後に，指定ブリッジのルートポート（指定ブリッジからルートブリッジへの通信経路）を本パラメータで設計します。

[設定のポイント]

パスコスト値は指定ブリッジの各ポートに設定します。小さい値で設定することによってルートポートに選択されやすくなります。設定しない場合，ポートの速度ごとに異なるデフォルト値になり，高速なポートほどルートポートに選択されやすくなります。

パスコストは，速度の遅いポートを速いポートより優先して経路として使用したい場合に設定します。速いポートを優先したトポロジーとする場合は設定する必要はありません。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/0/1**
   (config-if)# spanning-tree cost 100
   (config-if)# exit

   ポート 1/0/1 のパスコストを 100 に設定します。

2. **(config)# spanning-tree pathcost method long**
   (config)# interface gigabitethernet 1/0/1
   (config-if)# spanning-tree vlan 10 cost 200000

   long（32bit 値）のパスコストを使用するように設定した後に，ポート 1/0/1 の VLAN 10 をコスト値 200000 に変更します。ポート 1/0/1 では VLAN 10 だけパスコスト 200000 となり，そのほかの VLAN は 100 で動作します。

[注意事項]

リンクアグリゲーションを使用する場合，チャネルグループのパスコストのデフォルト値は，チャネルグループ内の全ポートの合計ではなく一つのポートの速度の値となります。

(3)　ポート優先度の設定

ポート優先度は 2 台の装置間での接続をスパニングツリーで冗長化し，パスコストも同じ値とする場合に，どちらのポートを使用するかを決定するために設定します。

2 台の装置間の接続を冗長化する機能にはリンクアグリゲーションがあり，通常はリンクアグリゲーションを使用することをお勧めします。接続する対向の装置がリンクアグリゲーションをサポートしていなくスパニングツリーで冗長化する必要がある場合に本機能を使用してください。

[設定のポイント]

ポート優先度は値が小さいほど高い優先度となります。2 台の装置間で冗長化している場合に，ルートブリッジに近い側の装置でポート優先度の高いポートが通信経路として使われます。本パラメータを設定しない場合はポート番号の小さいポートが優先されます。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/0/1**
   (config-if)# spanning-tree port-priority 64
   (config-if)# exit
   ポート 1/0/1 のポート優先度を 64 に設定します。
2. **(config)# interface gigabitethernet 1/0/1**
   (config-if)# spanning-tree vlan 10 port-priority 144
   ポート 1/0/1 の VLAN 10 をポート優先度 144 に変更します。ポート 1/0/1 では VLAN 10 だけポート優先度 144 となり，そのほかの VLAN は 64 で動作します。

26.4.4　PVST+のパラメータ設定

各パラメータは「2×(forward-time－1) ≧ max-age ≧ 2×(hello-time ＋ 1)」という関係を満たすように設定する必要があります。パラメータを変える場合は，スパニングツリーを構築するすべての装置でパラメータを合わせる必要があります。

(1)　BPDU の送信間隔の設定

BPDU の送信間隔は，短くした場合はトポロジー変更を検知しやすくなります。長くした場合はトポロジー変更の検知までに時間が掛かるようになる一方で，BPDU トラフィックや本装置のスパニングツリープログラムの負荷を軽減できます。

[設定のポイント]

設定しない場合，2 秒間隔で BPDU を送信します。通常は設定する必要はありません。

[コマンドによる設定]

1. **(config)# spanning-tree vlan 10 hello-time 3**
   VLAN 10 の PVST+の BPDU 送信間隔を 3 秒に設定します。

[注意事項]

BPDU の送信間隔を短くすると，トポロジー変更を検知しやすくなる一方で BPDU トラフィックが増加することによりスパニングツリープログラムの負荷が増加します。本パラメータをデフォルト値（2 秒）より短くすることでタイムアウトのメッセージ出力やトポロジー変更が頻発する場合は，デフォルト値に戻して使用してください。

(2)　送信する最大 BPDU 数の設定

スパニングツリーでは，CPU 負荷の増大を抑えるために，hello-time（BPDU 送信間隔）当たりに送信する最大 BPDU 数を決めることができます。トポロジー変更が連続的に発生すると，トポロジー変更を通知，収束するために大量の BPDU が送信され，BPDU トラフィックの増加，CPU 負荷の増大につながります。送信する BPDU の最大数を制限することでこれらを抑えます。

[設定のポイント]

設定しない場合，hello-time（BPDU 送信間隔）当たりの最大 BPDU 数は 3 で動作します。本パラメータのコンフィグレーションは Rapid PVST+だけ有効であり，PVST+は 3（固定）で動作します。通常は設定する必要はありません。

[コマンドによる設定]

1. **(config)# spanning-tree vlan 10 transmission-limit 5**
   VLAN 10 の Rapid PVST+の hello-time 当たりの最大送信 BPDU 数を 5 に設定します。

(3)　BPDU の最大有効時間の設定

ルートブリッジから送信する BPDU の最大有効時間を設定します。BPDU のカウンタは装置を経由するたびに増加し，最大有効時間を超えた BPDU は無効な BPDU となって無視されます。

[設定のポイント]

最大有効時間を大きく設定することで，多くの装置に BPDU が届くようになります。設定しない場合，最大有効時間は 20 で動作します。

[コマンドによる設定]

1. **(config)# spanning-tree vlan 10 max-age 25**
   VLAN 10 の PVST+の BPDU の最大有効時間を 25 に設定します。

(4)　状態遷移時間の設定

PVST+モードまたは Rapid PVST+モードでタイマによる動作となる場合，ポートの状態が一定時間ごとに遷移します。PVST+モードの場合は Blocking から Listening, Learning, Forwarding と遷移し，Rapid PVST+モードの場合は Discarding から Learning，Forwarding と遷移します。この状態遷移に必要な時間を設定できます。小さい値を設定すると，より早く Forwarding 状態に遷移できます。

[設定のポイント]

設定しない場合，状態遷移時間は 15 秒で動作します。本パラメータを短い時間に変更する場合，BPDU の最大有効時間（max-age），送信間隔（hello-time）との関係が「2×(forward-time－1) ≧ max-age ≧ 2×(hello-time ＋ 1)」を満たすように設定してください。

[コマンドによる設定]

1. **(config)# spanning-tree vlan 10 forward-time 10**
   VLAN 10 の PVST+の状態遷移時間を 10 に設定します。

26.5　シングルスパニングツリー解説

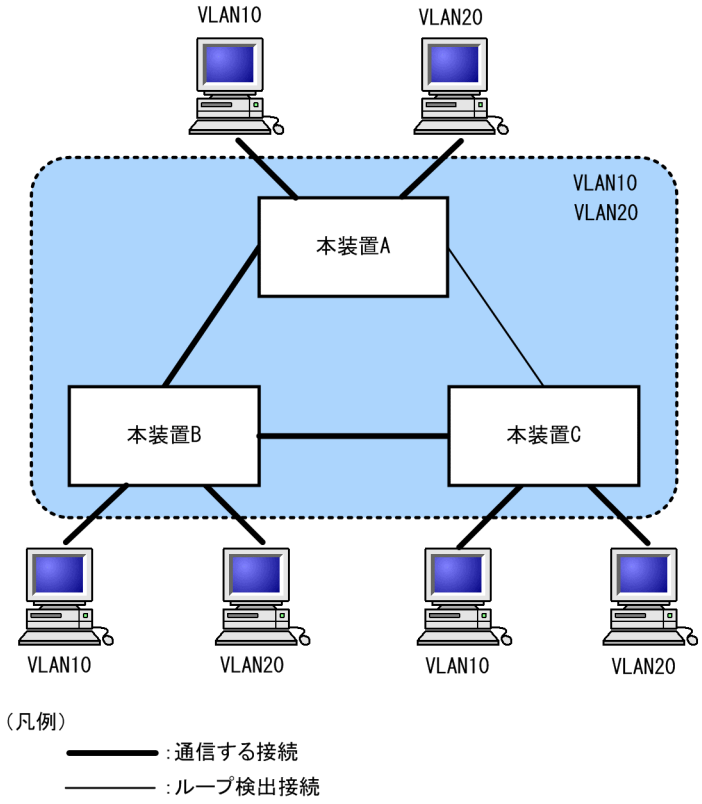
シングルスパニングツリーは装置全体を対象としトポロジーを構築します。

26.5.1　概要

シングルスパニングツリーは，一つのスパニングツリーですべての VLAN のループを回避できます。VLAN ごとに制御する PVST+よりも多くの VLAN を扱えます。

シングルスパニングツリーによるネットワーク構成を次の図に示します。この図では，本装置 A，B，C に対して，VLAN 10 および VLAN 20 を設定し，すべての VLAN で PVST+を停止しシングルスパニングツリーを適用しています。すべての VLAN で一つのトポロジーを使用して通信します。

図 26-8　シングルスパニングツリーによるネットワーク構成



26.5.2　PVST+との併用

プロトコル VLAN，MAC VLAN では PVST+を使用できません。また，PVST+が動作可能な VLAN 数は 250 個であり，それ以上の VLAN で使用することはできません。シングルスパニングツリーを使用することで，PVST+を使用しながらこれらの VLAN にもスパニングツリーを適用できます。

シングルスパニングツリーは，PVST+が動作していないすべての VLAN に対し適用します。次の表に，シングルスパニングツリーを PVST+と併用したときにシングルスパニングツリーの対象になる VLAN を示します。

表 26-11　シングルスパニングツリー対象の VLAN

項目	VLAN
PVST+対象の VLAN	PVST+が動作している VLAN。 最大 250 個のポート VLAN は自動的に PVST+が動作します。
シングルスパニングツリー対象の VLAN	251 個目以上のポート VLAN。
	PVST+を停止（no spanning-tree vlan コマンドで指定）している VLAN。
	デフォルト VLAN（VLAN ID 1 のポート VLAN）。
	プロトコル VLAN。
	MAC VLAN。

26.5.3　シングルスパニングツリー使用時の注意事項

(1)　他機能との共存

「22.3　レイヤ 2 スイッチ機能と他機能の共存について」を参照してください。

(2)　VLAN 1（デフォルト VLAN）の PVST+とシングルスパニングツリーについて

シングルスパニングツリーと VLAN 1 の PVST+を同時に動作させることはできません。シングルスパニングツリーを動作させると VLAN 1 の PVST+は停止します。

26.6　シングルスパニングツリーのコマンドガイド

26.6.1　コマンド一覧

シングルスパニングツリーのコンフィグレーションコマンド一覧を次の表に示します。

表 26-12　コンフィグレーションコマンド一覧

コマンド名	説明
spanning-tree cost	ポートごとにパスコストのデフォルト値を設定します。
spanning-tree pathcost method	ポートごとにパスコストに使用する値の幅のデフォルト値を設定します。
spanning-tree port-priority	ポートごとにポート優先度のデフォルト値を設定します。
spanning-tree single	シングルスパニングツリーの動作，停止を設定します。
spanning-tree single cost	シングルスパニングツリーのパスコストを設定します。
spanning-tree single forward-time	ポートの状態遷移に必要な時間を設定します。
spanning-tree single hello-time	BPDU の送信間隔を設定します。
spanning-tree single max-age	送信 BPDU の最大有効時間を設定します。
spanning-tree single pathcost method	シングルスパニングツリーのパスコストに使用する値の幅を設定します。
spanning-tree single port-priority	シングルスパニングツリーのポート優先度を設定します。
spanning-tree single priority	ブリッジ優先度を設定します。
spanning-tree single transmission-limit	hello-time 当たりに送信できる最大 BPDU 数を設定します。

26.6.2　シングルスパニングツリーの設定

[設定のポイント]

シングルスパニングツリーの動作，停止を設定します。シングルスパニングツリーは，動作モード pvst，rapid-pvst を設定しただけでは動作しません。設定することによって動作を開始します。

VLAN 1（デフォルト VLAN）とシングルスパニングツリーは同時に使用できません。シングルスパニングツリーを設定すると VLAN 1 の PVST+は停止します。

[コマンドによる設定]

1. **(config)# spanning-tree single**

   シングルスパニングツリーを動作させます。この設定によって，VLAN 1 の PVST+が停止し，VLAN 1 はシングルスパニングツリーの対象となります。

2. **(config)# no spanning-tree single**

   シングルスパニングツリーを停止します。VLAN 1 の PVST+を停止に設定していないで，かつすでに 250 個の PVST+が動作している状態でない場合，VLAN 1 の PVST+が自動的に動作を開始します。

26.6.3　シングルスパニングツリーのトポロジー設定

(1)　ブリッジ優先度の設定

ブリッジ優先度は，ルートブリッジを決定するためのパラメータです。トポロジーを設計する際に，ルートブリッジにしたい装置を最高の優先度に設定し，ルートブリッジに障害が発生したときのために，次にルートブリッジにしたい装置を 2 番目の優先度に設定します。

[設定のポイント]

ブリッジ優先度は値が小さいほど高い優先度となり，最も小さい値を設定した装置がルートブリッジになります。ルートブリッジはブリッジ優先度と装置の MAC アドレスから成るブリッジ識別子で判定するため，本パラメータを設定しない場合は装置の MAC アドレスが最も小さい装置がルートブリッジになります。

[コマンドによる設定]

1. **(config)# spanning-tree single priority 4096**

   シングルスパニングツリーのブリッジ優先度を 4096 に設定します。

(2)　パスコストの設定

パスコストは通信経路を決定するためのパラメータです。スパニングツリーのトポロジー設計において，ブリッジ優先度決定後に，指定ブリッジのルートポート（指定ブリッジからルートブリッジへの通信経路）を本パラメータで設計します。

[設定のポイント]

パスコスト値は指定ブリッジの各ポートに設定します。小さい値で設定することによりルートポートに選択されやすくなります。設定しない場合，ポートの速度ごとに異なるデフォルト値になり，高速なポートほどルートポートに選択されやすくなります。

パスコストは，速度の遅いポートを速いポートより優先して経路として使用したい場合に設定します。速いポートを優先したトポロジーとする場合は設定する必要はありません。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/0/1**
   (config-if)# spanning-tree cost 100
   (config-if)# exit

   ポート 1/0/1 のパスコストを 100 に設定します。

2. **(config)# spanning-tree pathcost method long**
   (config)# interface gigabitethernet 1/0/1
   (config-if)# spanning-tree single cost 200000

   long（32bit 値）のパスコストを使用するように設定した後に，シングルスパニングツリーのポート 1/0/1 のパスコストを 200000 に変更します。ポート 1/0/1 ではシングルスパニングツリーだけパスコスト 200000 となり，同じポートで使用している PVST+は 100 で動作します。

[注意事項]

リンクアグリゲーションを使用する場合，チャネルグループのパスコストのデフォルト値は，チャネルグループ内の全ポートの合計ではなく一つのポートの速度の値になります。

(3)　ポート優先度の設定

ポート優先度は 2 台の装置間での接続をスパニングツリーで冗長化し，パスコストも同じ値とする場合に，どちらのポートを使用するかを決定するために設定します。

2 台の装置間の接続を冗長化する機能にはリンクアグリゲーションがあり，通常はリンクアグリゲーションを使用することをお勧めします。接続する対向の装置がリンクアグリゲーションをサポートしていないで，スパニングツリーで冗長化する必要がある場合に本機能を使用してください。

[設定のポイント]

ポート優先度は値が小さいほど高い優先度となります。2 台の装置間で冗長化している場合に，ルートブリッジに近い側の装置でポート優先度の高いポートが通信経路として使われます。本パラメータを設定しない場合はポート番号の小さいポートが優先されます。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/0/1**
   (config-if)# spanning-tree port-priority 64
   (config-if)# exit
   ポート 1/0/1 のポート優先度を 64 に設定します。
2. **(config)# interface gigabitethernet 1/0/1**
   (config-if)# spanning-tree single port-priority 144
   シングルスパニングツリーのポート 1/0/1 のポート優先度を 144 に変更します。ポート 1/0/1 ではシングルスパニングツリーだけポート優先度 144 となり，同じポートで使用している PVST+は 64 で動作します。

26.6.4　シングルスパニングツリーのパラメータ設定

各パラメータは「2×(forward-time－1) ≧ max-age ≧ 2×(hello-time ＋ 1)」という関係が成立するように設定する必要があります。パラメータを変える場合はトポロジー全体でパラメータを合わせる必要があります。

(1)　BPDU の送信間隔の設定

BPDU の送信間隔は，短くした場合はトポロジー変更を検知しやすくなります。長くした場合はトポロジー変更の検知までに時間が掛かるようになる一方で，BPDU トラフィックや本装置のスパニングツリープログラムの負荷を軽減できます。

[設定のポイント]

設定しない場合，2 秒間隔で BPDU を送信します。通常は設定する必要はありません。

[コマンドによる設定]

1. **(config)# spanning-tree single hello-time 3**
   シングルスパニングツリーの BPDU 送信間隔を 3 秒に設定します。

[注意事項]

BPDU の送信間隔を短くすると，トポロジー変更を検知しやすくなる一方で BPDU トラフィックが増加することによりスパニングツリープログラムの負荷が増加します。本パラメータをデフォルト値（2 秒）より短くすることによってタイムアウトのメッセージ出力やトポロジー変更が頻発する場合は，デフォルト値に戻して使用してください。

(2)　送信する最大 BPDU 数の設定

スパニングツリーでは，CPU 負荷の増大を抑えるために，hello-time（BPDU 送信間隔）当たりに送信する最大 BPDU 数を決めることができます。トポロジー変更が連続的に発生すると，トポロジー変更を通知，収束するために大量の BPDU が送信され，BPDU トラフィックの増加，CPU 負荷の増大につながります。送信する BPDU の最大数を制限することでこれらを抑えます。

[設定のポイント]

設定しない場合，hello-time（BPDU 送信間隔）当たりの最大 BPDU 数は 3 で動作します。本パラメータのコンフィグレーションは Rapid STP だけ有効であり，STP は 3（固定）で動作します。通常は設定する必要はありません。

[コマンドによる設定]

1. **(config)# spanning-tree single transmission-limit 5**
   シングルスパニングツリーの hello-time 当たりの最大送信 BPDU 数を 5 に設定します。

(3)　BPDU の最大有効時間

ルートブリッジから送信する BPDU の最大有効時間を設定します。BPDU のカウンタは装置を経由するたびに増加し，最大有効時間を超えた BPDU は無効な BPDU となって無視されます。

[設定のポイント]

最大有効時間を大きく設定することで，多くの装置に BPDU が届くようになります。設定しない場合，最大有効時間は 20 で動作します。

[コマンドによる設定]

1. **(config)# spanning-tree single max-age 25**
   シングルスパニングツリーの BPDU の最大有効時間を 25 に設定します。

(4)　状態遷移時間の設定

STP モードまたは Rapid STP モードでタイマによる動作となる場合，ポートの状態が一定時間ごとに遷移します。STP モードの場合は Blocking から Listening，Learning，Forwarding と遷移し，Rapid STP モードの場合は Discarding から Learning，Forwarding と遷移します。この状態遷移に必要な時間を設定できます。小さい値を設定すると，より早く Forwarding 状態に遷移できます。

[設定のポイント]

設定しない場合，状態遷移時間は 15 秒で動作します。本パラメータを短い時間に変更する場合，BPDU の最大有効時間（max-age），送信間隔（hello-time）との関係が「2×(forward-time－1) ≧ max-age ≧ 2×(hello-time ＋ 1)」を満たすように設定してください。

[コマンドによる設定]

1. **(config)# spanning-tree single forward-time 10**
   シングルスパニングツリーの状態遷移時間を 10 に設定します。

26.7　マルチプルスパニングツリー解説

26.7.1　概要

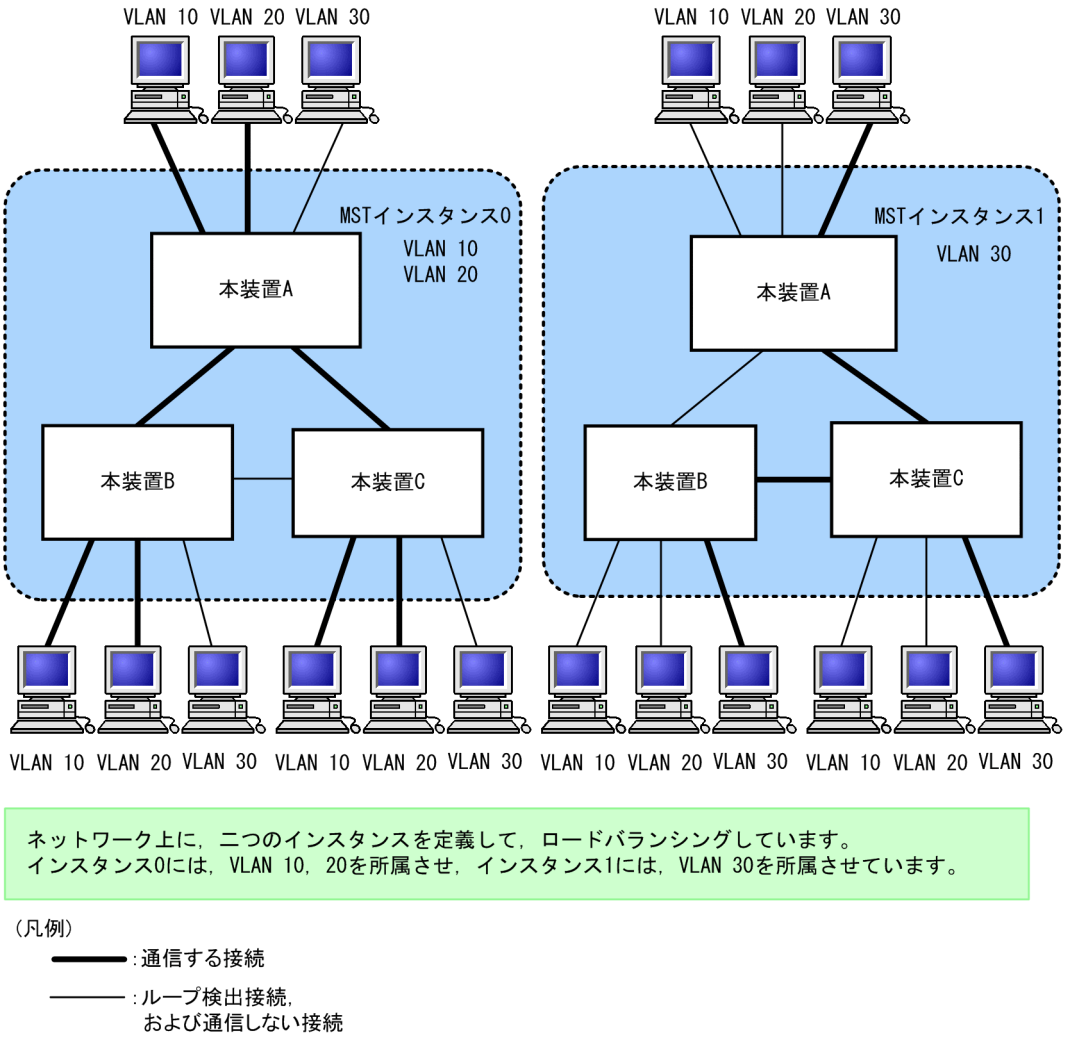
マルチプルスパニングツリーには，次の特長があります。MST インスタンスによってロードバランシングを可能にしています。また，MST リージョンによって，大規模なネットワーク構成を中小構成に分割することでネットワーク設計が容易になります。以降, これらを実現するためのマルチプルスパニングツリーの機能概要を説明します。

(1)　MST インスタンス

マルチプルスパニングツリーは, 複数の VLAN をまとめた MST インスタンス（MSTI：Multiple Spanning Tree Instance）というグループごとにスパニングツリーを構築でき，MST インスタンスごとにロードバランシングが可能です。PVST+によるロードバランシングでは，VLAN 数分のツリーが必要でしたが，マルチプルスパニングツリーでは MST インスタンスによって，計画したロードバランシングに従ったツリーだけで済みます。その結果, PVST+とは異なり VLAN 数の増加に比例した CPU 負荷およびネットワーク負荷の増加を抑えられます。本装置では最大 16 個の MST インスタンスが設定できます。

MST インスタンスイメージを次の図に示します。

図 26-9　MST インスタンスイメージ



(2)　MST リージョン

マルチプルスパニングツリーでは，複数の装置をグルーピングして MST リージョンとして扱えます。同一の MST リージョンに所属させるには，リージョン名，リビジョン番号，MST インスタンス ID と VLAN の対応を同じにする必要があります。これらはコンフィグレーションで設定します。ツリーの構築は MST リージョン間と MST リージョン内で別々に行い，MST リージョン内のトポロジーは MST インスタンス単位に構築できます。

次に，MST リージョン間や MST リージョン内で動作するスパニングツリーについて説明します。

- CST

  CST（Common Spanning Tree）は，MST リージョン間や，シングルスパニングツリーを使用しているブリッジ間の接続を制御するスパニングツリーです。このトポロジーはシングルスパニングツリーと同様で物理ポートごとに計算するのでロードバランシングすることはできません。

- IST

  IST（Internal Spanning Tree）は，MST リージョン外と接続するために，MST リージョン内で Default 動作するトポロジーのことを指し，MST インスタンス ID0 が割り当てられます。MST リージョン外と接続しているポートを境界ポートと呼びます。また，リージョン内，リージョン間で MST

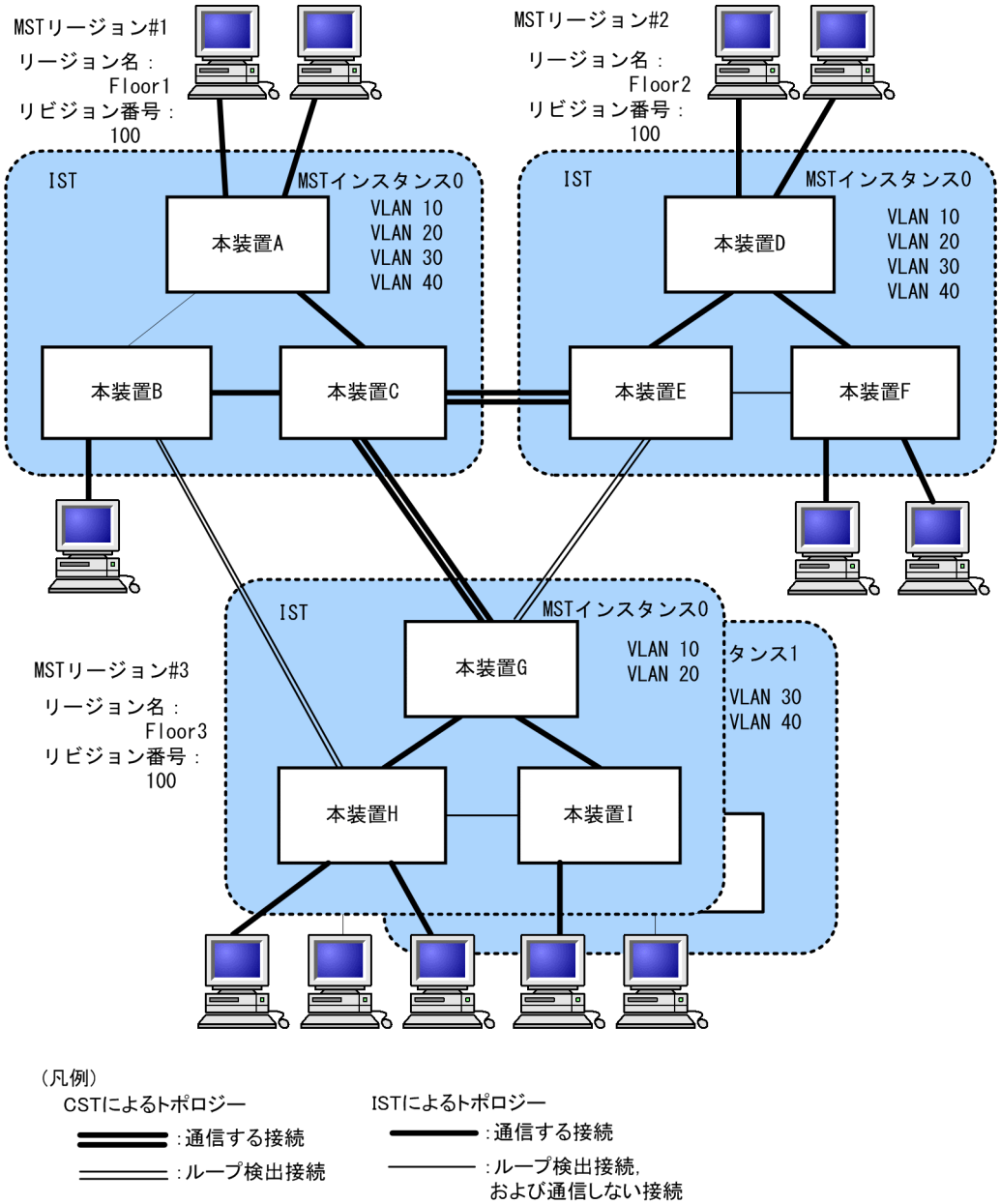
BPDU を送受信する唯一の MST インスタンスとなります。全 MST インスタンスのトポロジー情報は，MST BPDU にカプセル化し通知します。

- CIST

  CIST（Common and Internal Spanning Tree）は，IST と CST とを合わせたトポロジーを指します。

マルチプルスパニングツリー概要を次の図に示します。

図 26-10　マルチプルスパニングツリー概要

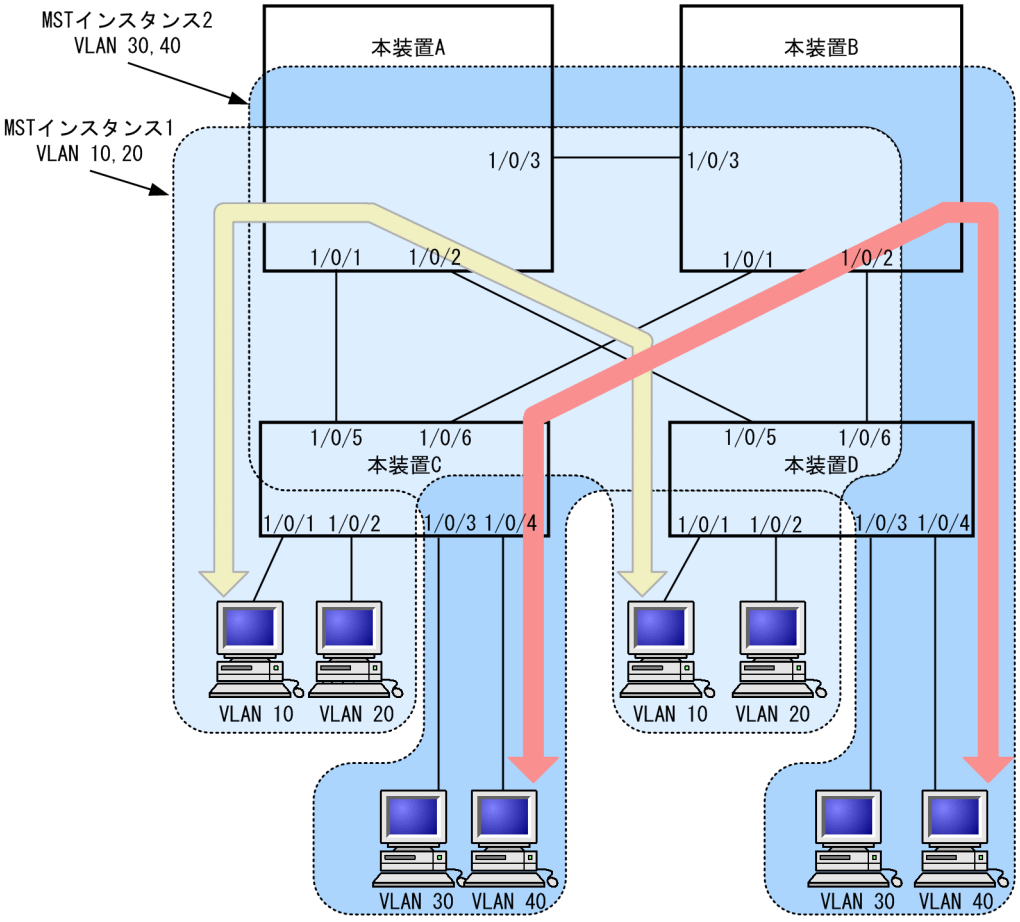


26.7.2　マルチプルスパニングツリーのネットワーク設計

(1)　MST インスタンス単位のロードバランシング構成

マルチプルスパニングツリーでは，MST インスタンス単位にロードバランシングができます。ロードバランシング構成の例を次の図に示します。この例では，VLAN 10，20 を MST インスタンス 1 に，VLAN 30，40 を MST インスタンス 2 に設定して，二つのロードバランシングを行っています。マルチプルスパニングツリーでは，この例のように四つの VLAN であっても二つのツリーだけを管理することでロードバランシングができます。

図 26-11　マルチプルスパニングツリーのロードバランシング構成



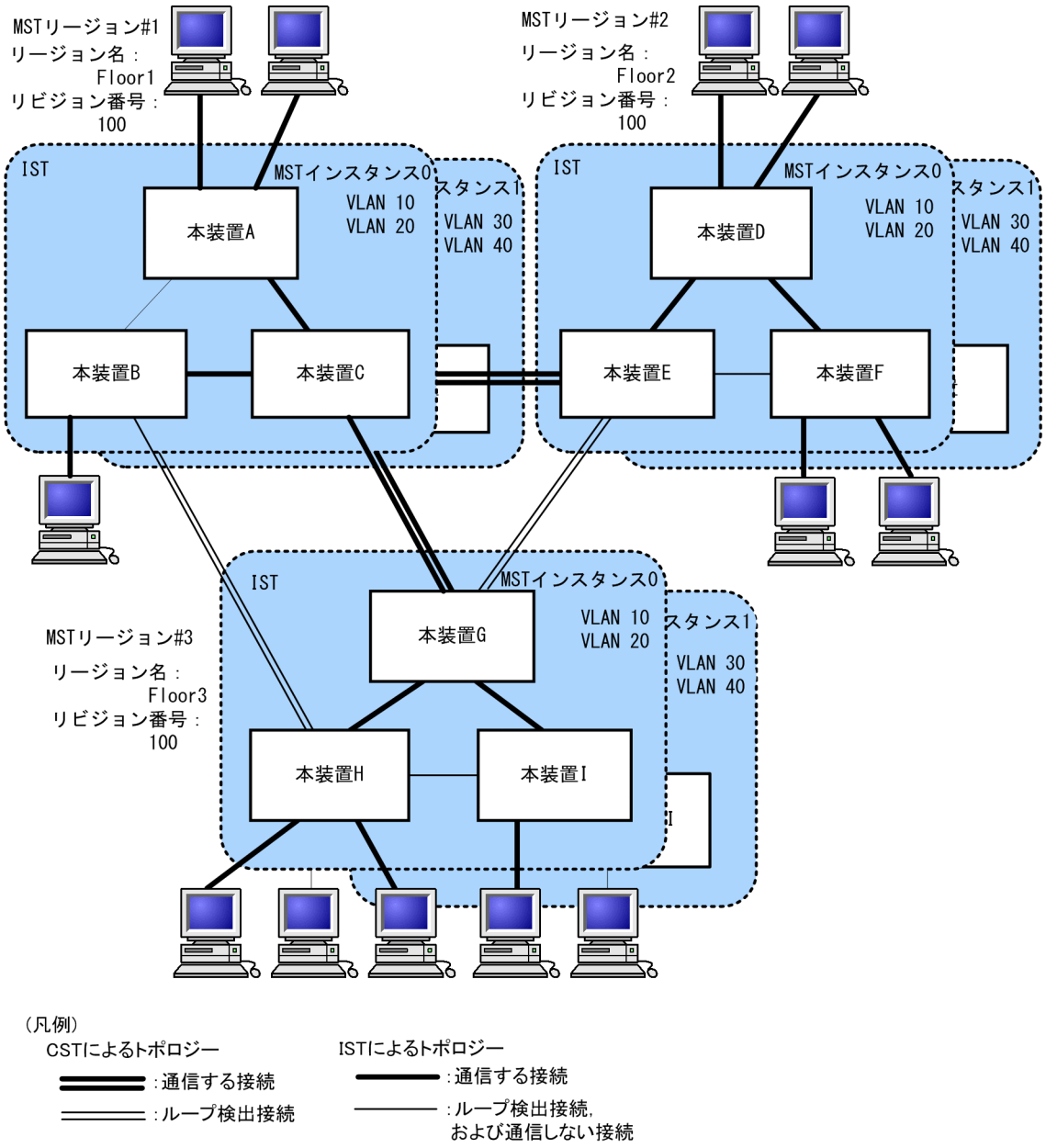
本装置Cと本装置Dに接続しているVLAN10の端末の通信経路と，本装置Cと本装置Dに接続しているVLAN40の端末で通信経路をロードバランシングしています。

(2)　MST リージョンによるネットワーク設計

ネットワーク構成が大規模になるに従ってネットワーク設計は複雑になりますが，MST リージョンによって中小規模構成に分割することで，例えば，ロードバランシングを MST リージョン単位に実施できるため，ネットワーク設計が容易になります。

MST リージョンによるネットワーク設計例を次の図に示します。この例では，装置 A，B，C を MST リージョン#1，装置 D，E，F を MST リージョン#2，本装置 G，H，I を MST リージョン#3 に設定して，ネットワークを三つの MST リージョンに分割しています。

図 26-12　MST リージョンによるネットワーク構成



26.7.3　ほかのスパニングツリーとの互換性

(1)　シングルスパニングツリーとの互換性

マルチプルスパニングツリーは，シングルスパニングツリーで動作する STP，Rapid STP と互換性があります。これらと接続した場合，別の MST リージョンと判断し接続します。Rapid STP と接続した場合は高速な状態遷移を行います。

(2)　PVST+との互換性

マルチプルスパニングツリーは，PVST+と互換性はありません。ただし，PVST+が動作している装置のアクセスポートはシングルスパニングツリーと同等の動作をするため，マルチプルスパニングツリーと接続できます。

26.7.4　マルチプルスパニングツリー使用時の注意事項

(1)　他機能との共存

「22.3　レイヤ 2 スイッチ機能と他機能の共存について」を参照してください。

(2)　MST リージョンについて

本装置と他装置で扱える VLAN の範囲が異なることがあります。そのような装置を同じ MST リージョンとして扱いたい場合は，該当 VLAN を MST インスタンス 0 に所属させてください。

(3)　トポロジーの収束に時間が掛かる場合について

CIST のルートブリッジまたは MST インスタンスのルートブリッジで，次の表に示すイベントが発生すると，トポロジーが落ち着くまでに時間が掛かる場合があります。その間，通信が途絶えたり，MAC アドレステーブルのクリアが発生したりします。

表 26-13　ルートブリッジでのイベント発生

イベント	内容	イベントの発生したルートブリッジ種別	影響トポロジー
コンフィグレーション変更	リージョン名(1)，リビジョン番号(2)，またはインスタンス番号と VLAN の対応(3)をコンフィグレーションで変更し，リージョンを分割または同じにする場合 (1) MST コンフィグレーションモードの name コマンド (2) MST コンフィグレーションモードの revision コマンド (3) MST コンフィグレーションモードの instance コマンド	CIST のルートブリッジ	CIST
		MST インスタンス 0 (IST) でのルートブリッジ	CIST
		MST インスタンス 1 以降でのルートブリッジ	当該 MST インスタンス
	ブリッジ優先度を spanning-tree mst root priority コマンドで下げた（現状より大きな値を設定した）場合	CIST のルートブリッジ	CIST
		MST インスタンス 1 以降でのルートブリッジ	当該 MST インスタンス
その他	本装置が停止した場合	CIST のルートブリッジ	CIST
		MST インスタンス 0 (IST) でのルートブリッジ	CIST
		MST インスタンス 1 以降でのルートブリッジ	当該 MST インスタンス
	本装置と接続している対向装置で，ループ構成となっている本装置の全ポートがダウンした場合（本装置が当該ループ構成上ルートブリッジではなくなった場合）	CIST のルートブリッジ	CIST
		MST インスタンス 0 (IST) でのルートブリッジ	CIST
		MST インスタンス 1 以降でのルートブリッジ	当該 MST インスタンス

26.8　マルチプルスパニングツリーのコマンドガイド

26.8.1　コマンド一覧

マルチプルスパニングツリーのコンフィグレーションコマンド一覧を次の表に示します。

表 26-14　コンフィグレーションコマンド一覧

コマンド名	説明
instance	マルチプルスパニングツリーの MST インスタンスに所属する VLAN を設定します。
name	マルチプルスパニングツリーのリージョンを識別するための文字列を設定します。
revision	マルチプルスパニングツリーのリージョンを識別するためのリビジョン番号を設定します。
spanning-tree cost	ポートごとにパスコストのデフォルト値を設定します。
spanning-tree mode	スパニングツリー機能の動作モードを設定します。
spanning-tree mst configuration	マルチプルスパニングツリーの MST リージョンの形成に必要な情報を設定します。
spanning-tree mst cost	マルチプルスパニングツリーの MST インスタンスごとのパスコストを設定します。
spanning-tree mst forward-time	ポートの状態遷移に必要な時間を設定します。
spanning-tree mst hello-time	BPDU の送信間隔を設定します。
spanning-tree mst max-age	送信 BPDU の最大有効時間を設定します。
spanning-tree mst max-hops	MST リージョン内での最大ホップ数を設定します。
spanning-tree mst port-priority	マルチプルスパニングツリーの MST インスタンスごとのポート優先度を設定します。
spanning-tree mst root priority	MST インスタンスごとのブリッジ優先度を設定します。
spanning-tree mst transmission-limit	hello-time 当たりに送信できる最大 BPDU 数を設定します。
spanning-tree port-priority	ポートごとにポート優先度のデフォルト値を設定します。

26.8.2　マルチプルスパニングツリーの設定

(1)　マルチプルスパニングツリーの設定

[設定のポイント]

スパニングツリーの動作モードをマルチプルスパニングツリーに設定すると，PVST+，シングルスパニングツリーはすべて停止し，マルチプルスパニングツリーの動作を開始します。

[コマンドによる設定]

1.**(config)# spanning-tree mode mst**

マルチプルスパニングツリーを使用するように設定し，CIST が動作を開始します。

[注意事項]

no spanning-tree mode コマンドでマルチプルスパニングツリーの動作モード設定を削除すると，デフォルトの動作モードである pvst になります。その際，ポート VLAN で自動的に PVST+が動作を開始します。

(2)　リージョン，インスタンスの設定

[設定のポイント]

MST リージョンは，同じリージョンに所属させたい装置はリージョン名，リビジョン番号，MST インスタンスのすべてを同じ設定にする必要があります。

MST インスタンスは，インスタンス番号と所属する VLAN を同時に設定します。リージョンを一致させるために，本装置に未設定の VLAN ID もインスタンスに所属させることができます。インスタンスに所属することを指定しない VLAN は自動的に CIST（インスタンス 0）に所属します。

MST インスタンスは，CIST（インスタンス 0）を含め 16 個まで設定できます。

[コマンドによる設定]

1. **(config)# spanning-tree mst configuration**
   (config-mst)# name "REGION TOKYO"
   (config-mst)# revision 1
   マルチプルスパニングツリーコンフィグレーションモードに移り，name（リージョン名），revision（リビジョン番号）の設定を行います。
2. **(config-mst)# instance 10 vlans 100-150**
   (config-mst)# instance 20 vlans 200-250
   (config-mst)# instance 30 vlans 300-350
   インスタンス 10，20，30 を設定し，各インスタンスに所属する VLAN を設定します。インスタンス 10 に VLAN 100～150, インスタンス 20 に VLAN 200～250, インスタンス 30 に VLAN 300～350 を設定します。指定していないそのほかの VLAN は CIST（インスタンス 0）に所属します。

26.8.3　マルチプルスパニングツリーのトポロジー設定

(1)　インスタンスごとのブリッジ優先度の設定

ブリッジ優先度は，ルートブリッジを決定するためのパラメータです。トポロジーを設計する際に，ルートブリッジにしたい装置を最高の優先度に設定し，ルートブリッジに障害が発生したときのために，次にルートブリッジにしたい装置を 2 番目の優先度に設定します。

[設定のポイント]

ブリッジ優先度は値が小さいほど高い優先度になり，最も小さい値を設定した装置がルートブリッジになります。ルートブリッジはブリッジ優先度と装置の MAC アドレスから成るブリッジ識別子で判定するため，本パラメータを設定しない場合は装置の MAC アドレスが最も小さい装置がルートブリッジになります。

マルチプルスパニングツリーのブリッジ優先度はインスタンスごとに設定します。インスタンスごとに値を変えた場合，インスタンスごとのロードバランシング（異なるトポロジーの構築）ができます。

[コマンドによる設定]

1. **(config)# spanning-tree mst 0 root priority 4096**

(config)# spanning-tree mst 20 root priority 61440

CIST（インスタンス 0）のブリッジ優先度を 4096 に，インスタンス 20 のブリッジ優先度を 61440 に設定します。

(2) インスタンスごとのパスコストの設定

パスコストは通信経路を決定するためのパラメータです。スパニングツリーのトポロジー設計において，ブリッジ優先度決定後に，指定ブリッジのルートポート（指定ブリッジからルートブリッジへの通信経路）を本パラメータで設計します。

[設定のポイント]

パスコスト値は指定ブリッジの各ポートに設定します。小さい値で設定することによってルートポートに選択されやすくなります。設定しない場合，ポートの速度ごとに異なるデフォルト値になり，高速なポートほどルートポートに選択されやすくなります。

パスコストは，速度の遅いポートを速いポートより優先して経路として使用したい場合に設定します。速いポートを優先したトポロジーとする場合は設定する必要はありません。

[コマンドによる設定]

1. **(config)# spanning-tree mst configuration**
   (config-mst)# instance 10 vlans 100-150
   (config-mst)# instance 20 vlans 200-250
   (config-mst)# instance 30 vlans 300-350
   (config-mst)# exit
   (config)# interface gigabitethernet 1/0/1
   (config-if)# spanning-tree cost 2000
   MST インスタンス 10，20，30 を設定し，ポート 1/0/1 のパスコストを 2000 に設定します。CIST（インスタンス 0），MST インスタンス 10，20，30 のポート 1/0/1 のパスコストは 2000 になります。
2. **(config-if)# spanning-tree mst 20 cost 500**
   MST インスタンス 20 のポート 1/0/1 のパスコストを 500 に変更します。インスタンス 20 以外は 2000 で動作します。

[注意事項]

リンクアグリゲーションを使用する場合，チャネルグループのパスコストのデフォルト値は，チャネルグループ内の全ポートの合計ではなく，一つのポートの速度の値となります。

(3) インスタンスごとのポート優先度の設定

ポート優先度は 2 台の装置間での接続をスパニングツリーで冗長化し，パスコストも同じ値とする場合に，どちらのポートを使用するかを決定するために設定します。

2 台の装置間の接続を冗長化する機能にはリンクアグリゲーションがあり，通常はリンクアグリゲーションを使用することをお勧めします。接続する対向の装置がリンクアグリゲーションをサポートしていなくスパニングツリーで冗長化する必要がある場合に本機能を使用してください。

[設定のポイント]

ポート優先度は値が小さいほど高い優先度となります。2 台の装置間で冗長化している場合に，ルートブリッジに近い側の装置でポート優先度の高いポートが通信経路として使われます。本パラメータを設定しない場合はポート番号の小さいポートが優先されます。

[コマンドによる設定]

1. (config)# interface gigabitethernet 1/0/1
   (config-if)# spanning-tree port-priority 64
   (config-if)# exit
   ポート 1/0/1 のポート優先度を 64 に設定します。
2. (config)# interface gigabitethernet 1/0/1
   (config-if)# spanning-tree mst 20 port-priority 144
   インスタンス 20 のポート 1/0/1 にポート優先度 144 を設定します。ポート 1/0/1 ではインスタンス 20 だけポート優先度 144 となり，そのほかのインスタンスは 64 で動作します。

26.8.4　マルチプルスパニングツリーのパラメータ設定

各パラメータは「2×(forward-time－1) ≧ max-age ≧ 2×(hello-time ＋ 1)」という関係が成立するように設定する必要があります。パラメータを変える場合はトポロジー全体でパラメータを合わせる必要があります。

(1)　BPDU の送信間隔の設定

BPDU の送信間隔は，短くした場合はトポロジー変更を検知しやすくなります。長くした場合はトポロジー変更の検知までに時間が掛かるようになる一方で，BPDU トラフィックや本装置のスパニングツリープログラムの負荷を軽減できます。

[設定のポイント]

設定しない場合，2 秒間隔で BPDU を送信します。通常は設定する必要はありません。

[コマンドによる設定]

1. (config)# spanning-tree mst hello-time 3
   マルチプルスパニングツリーの BPDU 送信間隔を 3 秒に設定します。

[注意事項]

BPDU の送信間隔を短くすると，トポロジー変更を検知しやすくなる一方で BPDU トラフィックが増加することによりスパニングツリープログラムの負荷が増加します。本パラメータをデフォルト値（2 秒）より短くすることによってタイムアウトのメッセージ出力やトポロジー変更が頻発する場合は，デフォルト値に戻して使用してください。

(2)　送信する最大 BPDU 数の設定

スパニングツリーでは，CPU 負荷の増大を抑えるために，hello-time（BPDU 送信間隔）当たりに送信する最大 BPDU 数を決めることができます。トポロジー変更が連続的に発生すると，トポロジー変更を通知，収束するために大量の BPDU が送信され，BPDU トラフィックの増加，CPU 負荷の増大につながります。送信する BPDU の最大数を制限することによりこれらを抑えます。

[設定のポイント]

設定しない場合，hello-time（BPDU 送信間隔）当たりの最大 BPDU 数は 3 で動作します。通常は設定する必要はありません。

[コマンドによる設定]

1. (config)# spanning-tree mst transmission-limit 5

マルチプルスパニングツリーの hello-time 当たりの最大送信 BPDU 数を 5 に設定します。

(3) 最大ホップ数の設定

ルートブリッジから送信する BPDU の最大ホップ数を設定します。BPDU のカウンタは装置を経由するたびに増加し，最大ホップ数を超えた BPDU は無効な BPDU となって無視されます。

シングルスパニングツリーの装置と接続しているポートは，最大ホップ数（max-hops）ではなく最大有効時間（max-age）のパラメータを使用します。ホップ数のカウントはマルチプルスパニングツリーの装置間で有効なパラメータです。

[設定のポイント]

最大ホップ数を大きく設定することによって，多くの装置に BPDU が届くようになります。設定しない場合，最大ホップ数は 20 で動作します。

[コマンドによる設定]

1. **(config)# spanning-tree mst max-hops 10**
   マルチプルスパニングツリーの BPDU の最大ホップ数を 10 に設定します。

(4) BPDU の最大有効時間の設定

マルチプルスパニングツリーでは，最大有効時間（max-age）はシングルスパニングツリーの装置と接続しているポートでだけ有効なパラメータです。トポロジー全体をマルチプルスパニングツリーが動作している装置で構成する場合は設定する必要はありません。

最大有効時間は，ルートブリッジから送信する BPDU の最大有効時間を設定します。BPDU のカウンタは装置を経由するたびに増加して，最大有効時間を超えた BPDU は無効な BPDU となって無視されます。

[設定のポイント]

最大有効時間を大きく設定することで，多くの装置に BPDU が届くようになります。設定しない場合，最大有効時間は 20 で動作します。

[コマンドによる設定]

1. **(config)# spanning-tree mst max-age 25**
   マルチプルスパニングツリーの BPDU の最大有効時間を 25 に設定します。

(5) 状態遷移時間の設定

タイマによる動作となる場合，ポートの状態が Discarding から Learning，Forwarding へ一定時間ごとに遷移します。この状態遷移に必要な時間を設定できます。小さい値を設定すると，より早く Forwarding 状態に遷移できます。

[設定のポイント]

設定しない場合，状態遷移時間は 15 秒で動作します。本パラメータを短い時間に変更する場合，BPDU の最大有効時間（max-age），送信間隔（hello-time）との関係が「2×(forward-time－1) ≧ max-age ≧ 2×(hello-time ＋ 1)」を満たすように設定してください。

[コマンドによる設定]

1. **(config)# spanning-tree mst forward-time 10**
   マルチプルスパニングツリーの状態遷移時間を 10 に設定します。

26.9　スパニングツリー共通機能解説

26.9.1　PortFast

(1)　概要

PortFast は，端末が接続されループが発生しないことがあらかじめわかっているポートのための機能です。PortFast はスパニングツリーのトポロジー計算対象外となり，リンクアップ後すぐに通信できる状態になります。

(2)　PortFast 適用時の BPDU 受信

PortFast を設定したポートは BPDU を受信しないことを想定したポートですが，もし，PortFast を設定したポートで BPDU を受信した場合は，その先にスイッチが存在しループの可能性があることになります。そのため，PortFast 機能を停止し，トポロジー計算や BPDU の送受信など，通常のスパニングツリー対象のポートとしての動作を開始します。

いったんスパニングツリー対象のポートとして動作を開始した後，リンクのダウン／アップによって再び PortFast 機能が有効になります。

なお，BPDU を受信したときに PortFast 機能を停止しないようにする場合は，BPDU フィルタ機能を併用してください。

(3)　PortFast 適用時の BPDU 送信

PortFast を設定したポートではスパニングツリーを動作させないため，BPDU の送信は行いません。

ただし，PortFast を設定したポート同士を誤って接続した状態を検出するために，PortFast 機能によって即時に通信可状態になった時点から 10 フレームだけ BPDU の送信を行います。

(4)　BPDU ガード

PortFast に適用する機能として，BPDU ガード機能があります。BPDU ガード機能を適用したポートでは，BPDU 受信時に，スパニングツリー対象のポートとして動作するのではなくポートを inactive 状態にします。

inactive 状態にしたポートを activate コマンドで解放することによって，再び BPDU ガード機能を適用した PortFast としてリンクアップして通信を開始します。

26.9.2　BPDU フィルタ

(1)　概要

BPDU フィルタ機能を適用したポートでは，BPDU の送受信を停止します。BPDU フィルタ機能は，端末が接続されループが発生しないことがあらかじめわかっている，PortFast を設定したポートに適用します。

(2)　BPDU フィルタに関する注意事項

PortFast を適用したポート以外に BPDU フィルタ機能を設定した場合，BPDU の送受信を停止するため，タイマによるポートの状態遷移が終了するまで通信断になります。

26.9.3　ループガード

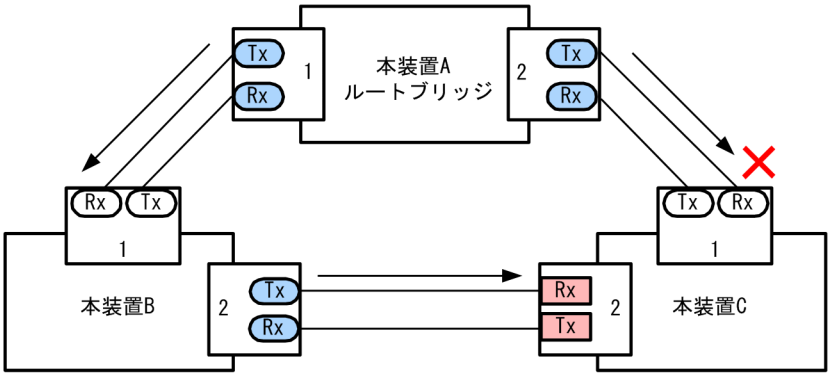
(1)　概要

片線切れなどの単一方向のリンク障害が発生し，BPDU の受信が途絶えた場合，ループが発生することがあります。ループガード機能は，このような場合にループの発生を防止する機能です。

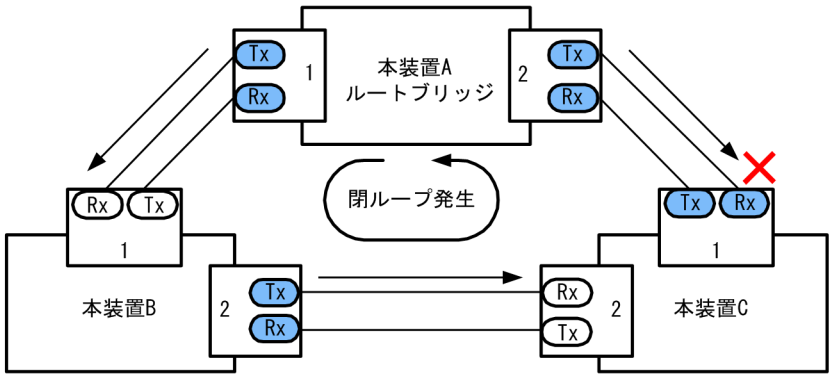
次の図に単一方向のリンク障害時の問題点を示します。

図 26-13　単一方向のリンク障害時の問題点

（1）本装置Cのポート1の片リンク故障で，BPDUの受信が途絶えるとルートポートがポート2に切り替わります。



（2）本装置Cのポート1は指定ポートとなって，通信可状態を維持するため閉ループが発生します。



（凡例）：ルートポート　：指定ポート　：非指定ポート

ループガード機能とは BPDU の受信が途絶えたポートの状態を，再度 BPDU を受信するまで転送不可状態に遷移させる機能です。BPDU 受信を開始した場合は通常のスパニングツリー対象のポートとしての動作を開始します。

ループガード機能は，端末を接続するポートを指定する機能である PortFast を設定したポート，またはルートガード機能を設定したポートには設定できません。

(2)　ループガードに関する注意事項

ループガードはマルチプルスパニングツリーでは使用できません。

ループガード機能を設定したあと，次に示すイベントが発生すると，ループガードが動作してポートをブロックします。その後，BPDU を受信するまで，ループガードは解除されません。

- 装置起動
- ポートのアップ（リンクアグリゲーションのアップも含む）
- スパニングツリープログラムの再起動
- スパニングツリープロトコルの種別変更（STP/高速 STP，PVST+/高速 PVST+）

なお，ループガード機能は，指定ポートだけでなく対向装置にも設定してください。指定ポートだけに設定すると，上記のイベントが発生しても，指定ポートは BPDU を受信しないことがあります。このような場合，ループガードの解除に時間が掛かります。ループガードを解除するには，対向装置のポートで BPDU 受信タイムアウトを検出したあとの BPDU の送信を待つ必要があるためです。

また，両ポートにループガードを設定した場合でも，指定ポートで BPDU を一度も受信せずに，ループガードの解除に時間が掛かることがあります。具体的には，対向ポートが指定ポートとなるようにブリッジやポートの優先度，パスコストを変更した場合です。対向ポートで BPDU タイムアウトを検出し，ループガードが動作します。このポートが指定ポートになった場合，BPDU を受信しないことがあり，ループガードの解除に時間が掛かることがあります。

運用中にループガード機能を設定した場合，その時点では，ループガードは動作しません。運用中に設定したループガードは，BPDU の受信タイムアウトが発生した時に動作します。

本装置と対向装置のポート間に BPDU を中継しない装置が存在し，かつポートの両端にループガード機能を設定した状態でポートがリンクアップした場合，両端のポートはループガードが動作したままになります。復旧するには，ポート間に存在する装置の BPDU 中継機能を有効にし，再度ポートをリンクアップさせる必要があります。

26.9.4　ルートガード

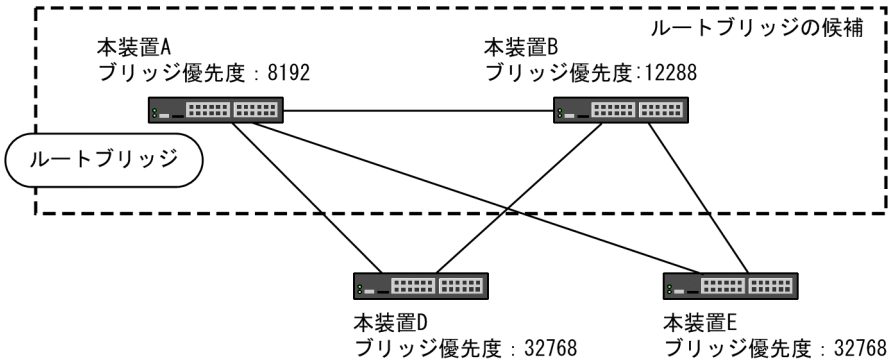
(1)　概要

ネットワークの管理の届かない個所で誤って装置が接続された場合や設定が変更された場合，意図しないトポロジーになることがあります。意図しないトポロジーのルートブリッジの性能が低い場合，トラフィックが集中するとネットワーク障害のおそれがあります。ルートガード機能は，このようなときのためにルートブリッジの候補を特定しておくことによって，ネットワーク障害を回避する機能です。

誤って装置が接続されたときの問題点を次の図に示します。

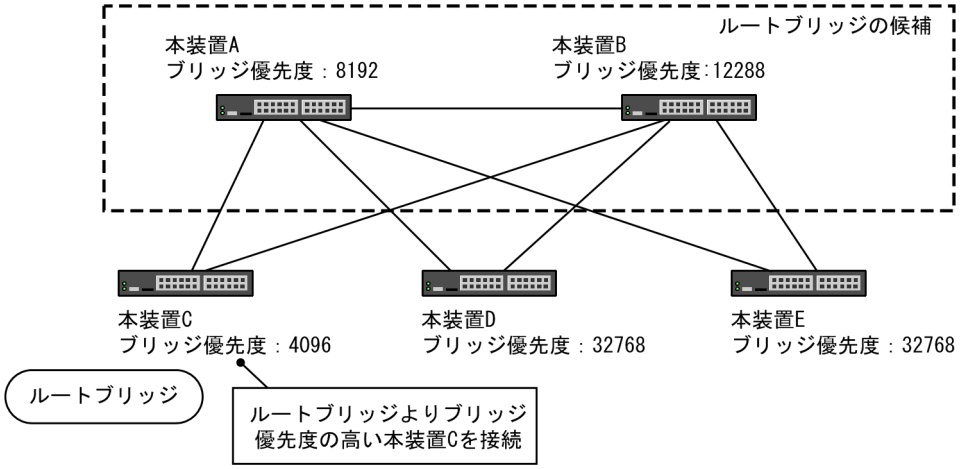
- 本装置 A，本装置 B をルートブリッジの候補として運用

図 26-14　本装置 A，本装置 B をルートブリッジの候補として運用



- 本装置 A，本装置 B よりブリッジ優先度の高い本装置 C を接続すると，本装置 C がルートブリッジになり，本装置 C にトラフィックが集中するようになる

図 26-15　本装置 A，本装置 B よりブリッジ優先度の高い本装置 C を接続



ルートガード機能は，現在のルートブリッジよりも優先度の高いブリッジを検出し，BPDU を廃棄することによってトポロジーを保護します。また，該当するポートをブロック状態に設定することでループを回避します。ルートガード機能は，ループガード機能を設定したポートには設定できません。

26.10　スパニングツリー共通機能のコマンドガイド

26.10.1　コマンド一覧

スパニングツリー共通機能のコンフィグレーションコマンド一覧を次の表に示します。

表 26-15　コンフィグレーションコマンド一覧

コマンド名	説明
spanning-tree bpdufilter	ポートごとに BPDU フィルタ機能を設定します。
spanning-tree bpduguard	ポートごとに BPDU ガード機能を設定します。
spanning-tree guard	ポートごとにループガード機能，ルートガード機能を設定します。
spanning-tree link-type	ポートのリンクタイプを設定します。
spanning-tree loopguard default	ループガード機能をデフォルトで使用するように設定します。
spanning-tree portfast	ポートごとに PortFast 機能を設定します。
spanning-tree portfast bpduguard default	BPDU ガード機能をデフォルトで使用するように設定します。
spanning-tree portfast default	PortFast 機能をデフォルトで使用するように設定します。

26.10.2　PortFast の設定

(1)　PortFast の設定

PortFast は，端末を接続するポートなど，ループが発生しないことがあらかじめわかっているポートを直ちに通信できる状態にしたい場合に適用します。

[設定のポイント]

spanning-tree portfast default コマンドを設定すると，アクセスポート，プロトコルポート，MAC ポートにデフォルトで PortFast 機能を適用します。デフォルトで適用してポートごとに無効にしたい場合は，spanning-tree portfast disable コマンドを設定します。

トランクポートでは，ポートごとの指定で適用できます。

[コマンドによる設定]

1. **(config)# spanning-tree portfast default**

   すべてのアクセスポート，プロトコルポート，MAC ポートに対して PortFast 機能を適用するように設定します。

2. **(config)# interface gigabitethernet 1/0/1**
   (config-if)# switchport mode access
   (config-if)# spanning-tree portfast disable
   (config-if)# exit

   ポート 1/0/1（アクセスポート）で PortFast 機能を使用しないように設定します。

3. **(config)# interface gigabitethernet 1/0/3**
   (config-if)# switchport mode trunk

```
(config-if)# spanning-tree portfast trunk
```

ポート 1/0/3 をトランクポートに指定し，PortFast 機能を適用します。トランクポートはデフォルトでは適用されません。ポートごとに指定するためには trunk パラメータを指定する必要があります。

(2) BPDU ガードの設定

BPDU ガード機能は，PortFast を適用したポートで BPDU を受信した場合にそのポートを inactive 状態にします。通常，PortFast 機能は冗長経路ではないポートを指定し，ポートの先にはスパニングツリー装置がないことを前提とします。BPDU を受信したことによる意図しないトポロジー変更を回避したい場合に設定します。

[設定のポイント]

BPDU ガード機能を設定するためには，PortFast 機能を同時に設定する必要があります。spanning-tree portfast bpduguard default コマンドは PortFast 機能を適用しているすべてのポートにデフォルトで BPDU ガードを適用します。デフォルトで適用するときに BPDU ガード機能を無効にしたい場合は，spanning-tree bpduguard disable コマンドを設定します。

[コマンドによる設定]

1.
```
(config)# spanning-tree portfast default
(config)# spanning-tree portfast bpduguard default
```
すべてのアクセスポート，プロトコルポート，MAC ポートに対して PortFast 機能を設定します。また，PortFast 機能を適用したすべてのポートに対し BPDU ガード機能を設定します。

2.
```
(config)# interface gigabitethernet 1/0/1
(config-if)# spanning-tree bpduguard disable
(config-if)# exit
```
ポート 1/0/1(アクセスポート) で BPDU ガード機能を使用しないように設定します。ポート 1/0/1 は通常の PortFast 機能を適用します。

3.
```
(config)# interface gigabitethernet 1/0/2
(config-if)# switchport mode trunk
(config-if)# spanning-tree portfast trunk
```
ポート 1/0/2（トランクポート）に PortFast 機能を設定します。また，BPDU ガード機能を設定します。トランクポートはデフォルトでは PortFast 機能を適用しないためポートごとに設定します。デフォルトで BPDU ガード機能を設定している場合は, PortFast 機能を設定すると自動的に BPDU ガードも適用します。デフォルトで設定していない場合は，spanning-tree bpduguard enable コマンドで設定します。

26.10.3 BPDU フィルタの設定

BPDU フィルタ機能は，BPDU を受信した場合にその BPDU を廃棄します。また，BPDU を一切送信しなくなります。通常は冗長経路ではないポートを指定することを前提とします。

[設定のポイント]

インタフェース単位に BPDU フィルタ機能を設定できます。

[コマンドによる設定]

1.
```
(config)# interface gigabitethernet 1/0/1
(config-if)# spanning-tree bpdufilter enable
```

ポート 1/0/1 で BPDU フィルタ機能を設定します。

26.10.4　ループガードの設定

片線切れなどの単一方向のリンク障害が発生し，BPDU の受信が途絶えた場合，ループが発生することがあります。ループガードは，このようにループの発生を防止したい場合に設定します。

[設定のポイント]

ループガードは，PortFast 機能を設定していないポートで動作します。

spanning-tree loopguard default コマンドを設定すると，PortFast を設定したポート以外のすべてのポートにループガードを適用します。デフォルトで適用する場合に，ループガードを無効にしたい場合は spanning-tree guard none コマンドを設定します。

[コマンドによる設定]

1. **(config)# spanning-tree loopguard default**

   PortFast を設定したポート以外のすべてのポートに対してループガード機能を適用するように設定します。

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

   (config-if)# spanning-tree guard none

   (config-if)# exit

   デフォルトでループガードを適用するように設定した状態で，ポート 1/0/1 はループガードを無効にするように設定します。

3. **(config)# no spanning-tree loopguard default**

   (config)# interface gigabitethernet 1/0/2

   (config-if)# spanning-tree guard loop

   デフォルトでループガードを適用する設定を削除します。また，ポート 1/0/2 に対してポートごとの設定でループガードを適用します。

26.10.5　ルートガードの設定

ネットワークに誤って装置が接続された場合や設定が変更された場合，ルートブリッジが替わり，意図しないトポロジーになることがあります。ルートガードは，このような意図しないトポロジー変更を防止したい場合に設定します。

[設定のポイント]

ルートガードは指定ポートに対して設定します。ルートブリッジの候補となる装置以外の装置と接続する個所すべてに適用します。

ルートガード動作時，PVST+が動作している場合は，該当する VLAN のポートだけブロック状態に設定します。マルチプルスパニングツリーが動作している場合，該当するインスタンスのポートだけブロック状態に設定しますが，該当するポートが境界ポートの場合は，全インスタンスのポートをブロック状態に設定します。

[コマンドによる設定]

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

   (config-if)# spanning-tree guard root

   ポート 1/0/1 でルートガード機能を設定します。

26.10.6　リンクタイプの設定

リンクタイプはポートの接続状態を表します。Rapid PVST+，シングルスパニングツリーの Rapid STP，マルチプルスパニングツリーで高速な状態遷移を行うためには，スイッチ間の接続が point-to-point である必要があります。shared の場合は高速な状態遷移はしないで，PVST+，シングルスパニングツリーの STP と同様にタイマによる状態遷移となります。

[設定のポイント]

ポートごとに接続状態を設定できます。設定しない場合，ポートが全二重の接続のときは point-to-point，半二重の接続の場合は shared となります。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/0/1**
   (config-if)# spanning-tree link-type point-to-point
   ポート 1/0/1 を point-to-point 接続とみなして動作させます。

[注意事項]

実際のネットワークの接続形態が 1 対 1 接続ではない構成では，本コマンドで point-to-point を指定しないでください。1 対 1 接続ではない構成とは，一つのポートに隣接するスパニングツリー装置が 2 台以上存在する構成です。

27 Ring Protocol の解説

この章は，Autonomous Extensible Ring Protocol について説明します。
Autonomous Extensible Ring Protocol は，リングトポロジーでのレイヤ 2 ネットワークの冗長化プロトコルで，以降，Ring Protocol と呼びます。

27.1　Ring Protocol の概要

27.1.1　概要

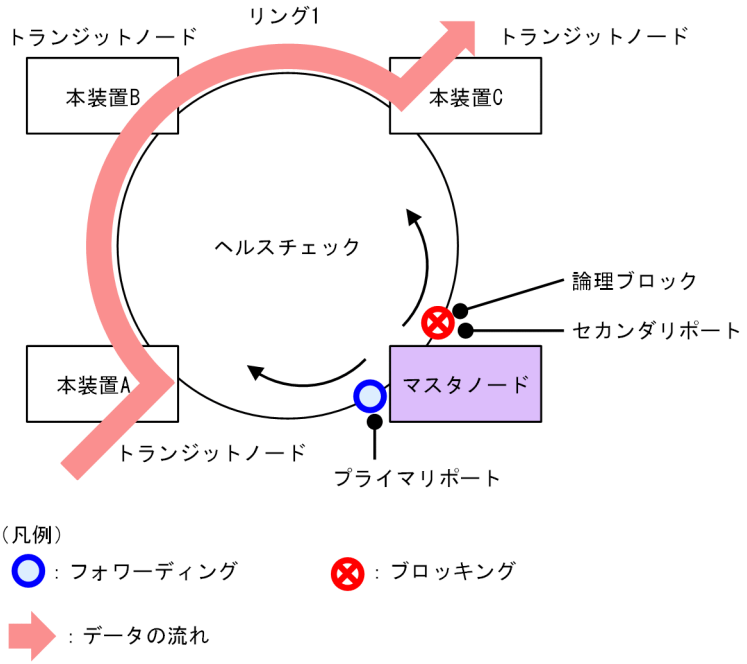
Ring Protocol とは，スイッチをリング状に接続したネットワークでの障害の検出と，それに伴う経路切り替えを高速に行うレイヤ 2 ネットワークの冗長化プロトコルです。

レイヤ 2 ネットワークの冗長化プロトコルとして，スパニングツリーが利用されますが，障害発生に伴う切り替えの収束時間が遅いなどの欠点があります。Ring Protocol を使用すると，障害発生に伴う経路切り替えを高速にできるようになります。また，リングトポロジーを利用することで，メッシュトポロジーよりも伝送路やインタフェースの必要量が少なくて済むという利点もあります。

Ring Protocol を構成するスイッチにはマスタノードとトランジットノードがありますが，本装置はトランジットノードだけをサポートしています。本マニュアルでは，本装置のトランジットノードについて説明します。マスタノードについては，マスタノードをサポートしている AX シリーズのマニュアルを参照してください。

Ring Protocol によるリングネットワークの概要を次の図に示します。

図 27-1　Ring Protocol の概要



リングを構成するノードのうち一つをマスタノードとして，ほかのリング構成ノードをトランジットノードとします。各ノード間を接続する二つのポートをリングポートと呼び，マスタノードのリングポートにはプライマリポートとセカンダリポートがあります。マスタノードはセカンダリポートを論理ブロックすることでリング構成を分断します。これによって，データフレームのループを防止しています。マスタノードはリング内の状態監視を目的とした制御フレーム（ヘルスチェックフレーム）を定期的に送信します。マスタノードは，巡回したヘルスチェックフレームの受信，未受信によって，リング内で障害が発生していないかどうかを判断します。障害または障害復旧を検出したマスタノードは，セカンダリポートの論理ブロックを設定または解除することで経路を切り替え，通信を復旧させます。

27.1.2　特長

(1)　イーサネットベースのリングネットワーク

Ring Protocol はイーサネットベースのネットワーク冗長化プロトコルです。従来のリングネットワークでは FDDI のように二重リンクの光ファイバを用いたネットワークが主流でしたが, Ring Protocol を用いることでイーサネットを用いたリングネットワークが構築できます。

Ring Protocol の適用例を次の図に示します。

図 27-2　Ring Protocol の適用例（その 1）

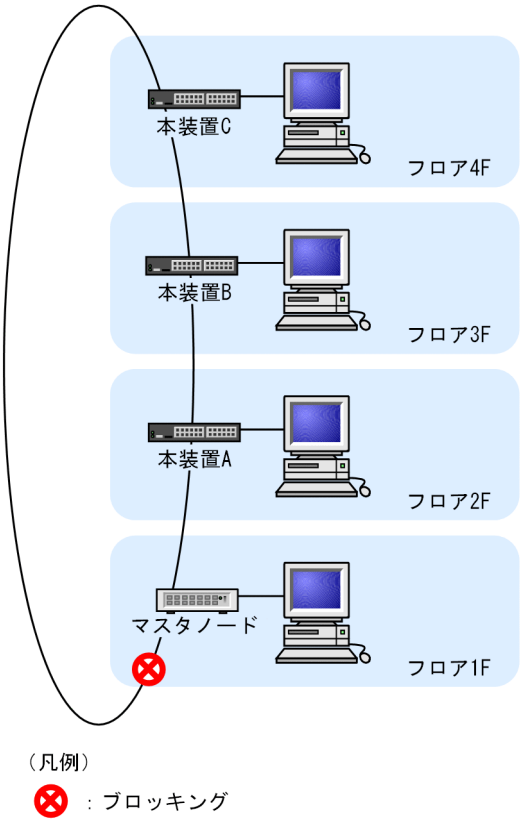
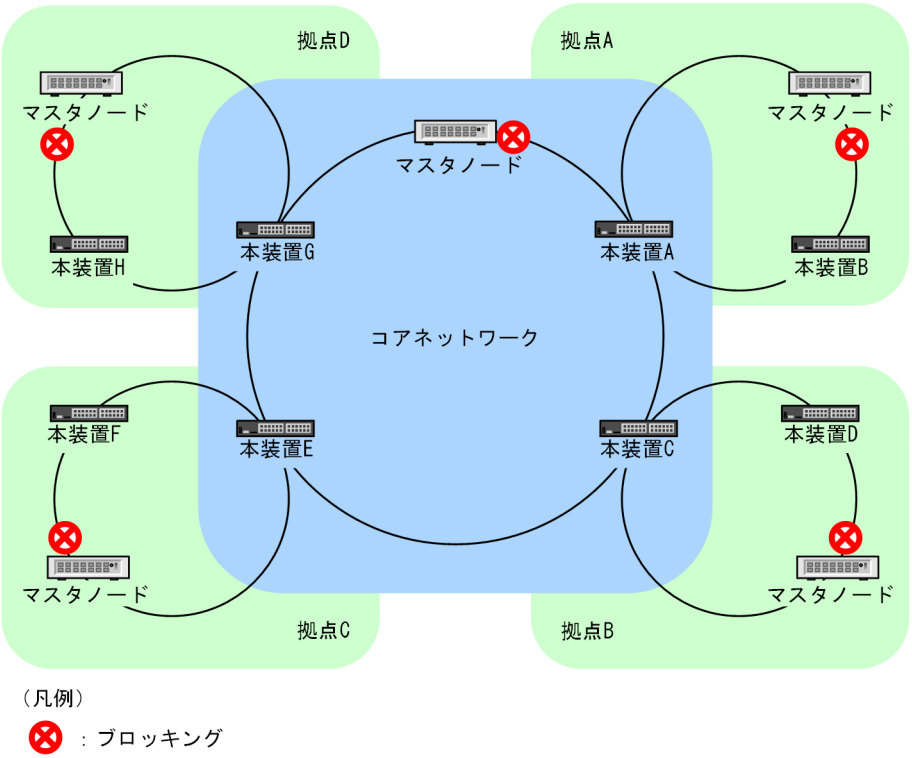


図 27-3　Ring Protocol の適用例（その 2）



(2)　シンプルな動作方式

Ring Protocol を使用したネットワークは，マスタノード 1 台とそのほかのトランジットノードで構成したシンプルな構成となります。リング状態（障害や障害復旧）の監視や経路の切り替え動作は，主にマスタノードが行い，そのほかのトランジットノードはマスタノードからの指示によって経路の切り替え動作を行います。

(3)　制御フレーム

Ring Protocol では，本プロトコル独自の制御フレームを使用します。制御フレームは，マスタノードによるリング状態の監視やマスタノードからトランジットノードへの経路の切り替え指示に使われます。制御フレームの送受信は，専用の VLAN 上で行われるため，通常のスパニングツリーのようにデータフレームと制御フレームが同じ VLAN 内に流れることはありません。また，制御フレームは優先的に処理されるため，データトラフィックが増大しても制御フレームに影響を与えません。

(4)　負荷分散方式

リング内で使用する複数の VLAN を論理的なグループ単位にまとめ，マスタノードを基点としてデータの流れを右回りと左回りに分散させる設定ができます。負荷分散や VLAN ごとに経路を分けたい場合に有効です。

27.1.3　サポート仕様

Ring Protocol でサポートする項目と仕様を次の表に示します。

表 27-1　Ring Protocol でサポートする項目・仕様

項目		内容
適用レイヤ	レイヤ 2	○
	レイヤ 3	×
リング構成	シングルリング	○
	マルチリング	○（共有リンクありマルチリング構成含む）
ノード	マスタノード	×
	トランジットノード	○
	共有ノード	×
装置当たりのリング ID 最大数		24
リングポート（1 リング ID 当たりのポート数）		2（物理ポートまたはリンクアグリゲーション）
VLAN 数	1 リング ID 当たりの制御 VLAN 数	1（デフォルト VLAN の設定は不可）
	1 リング ID 当たりのデータ転送用 VLAN グループ最大数	2
	1 データ転送用 VLAN グループ当たりの VLAN マッピング最大数	128
	1VLAN マッピング当たりの VLAN 最大数	1023
ヘルスチェックフレーム送信間隔		マスタノードに依存
障害監視時間		マスタノードに依存
負荷分散方式		マスタノードに依存
多重障害監視機能	装置当たりの多重障害監視可能リング数	4
	1 リング ID 当たりの多重障害監視 VLAN 数	1（デフォルト VLAN の設定は不可）
	多重障害監視フレーム送信間隔	共有ノードに依存
	多重障害監視時間	共有ノードに依存

（凡例）　○：サポート　×：未サポート

27.2　Ring Protocol の基本原理

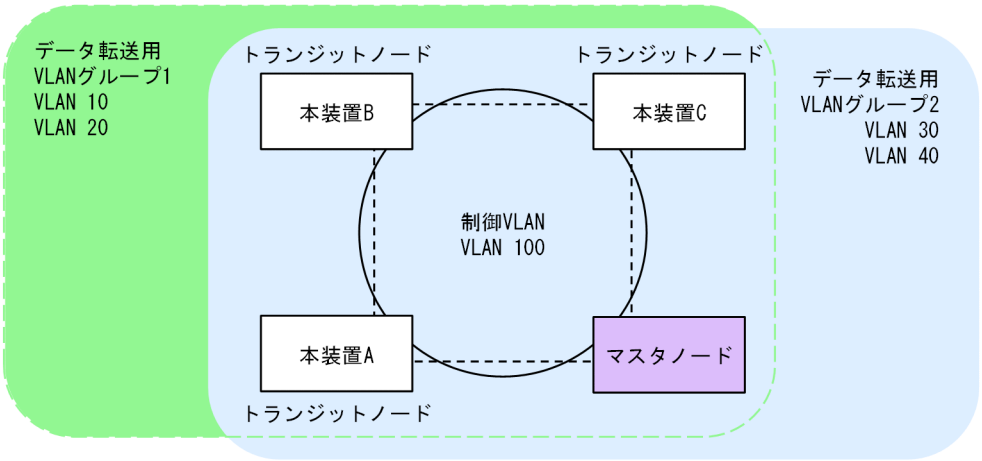
27.2.1　ネットワーク構成

Ring Protocol を使用する場合の基本的なネットワーク構成を次に示します。

(1)　シングルリング構成

シングルリング構成について，次の図に示します。

図 27-4　シングルリング構成

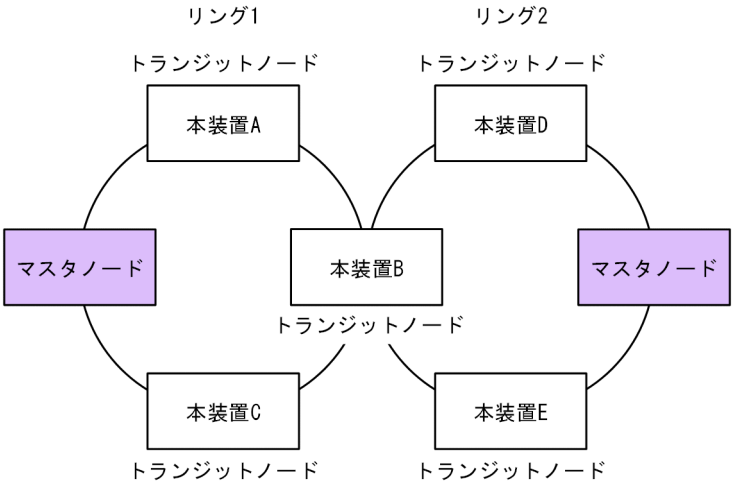


マスタノード 1 台とトランジットノード数台から成る一つのリング構成をシングルリング構成と呼びます。リングを構成するノード間は，リングポートとして，物理ポートまたはリンクアグリゲーションで接続されます。また，リングを構成するすべてのノードに，制御 VLAN として同一の VLAN，およびデータフレームの転送用として共通の VLAN を使用する必要があります。マスタノードから送信した制御フレームは，制御 VLAN 内を巡回します。データフレームの送受信に使用する VLAN は，VLAN グループと呼ばれる一つの論理的なグループに束ねて使用します。VLAN グループは複数の VLAN をまとめることができ，一つのリングにマスタノードを基点とした右回り用と左回り用の最大 2 グループを設定できます。

(2)　マルチリング構成

マルチリング構成のうち，隣接するリングの接点となるノードが一つの場合の構成について次の図に示します。

図 27-5　マルチリング構成

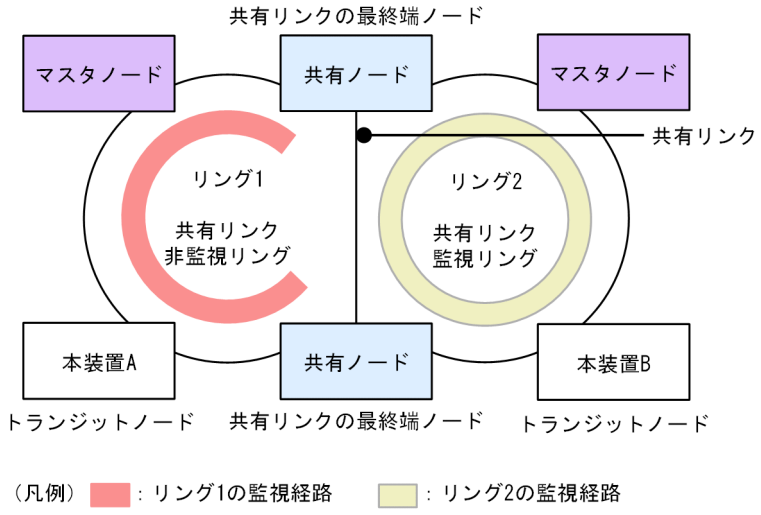


それぞれのリングを構成しているノードは独立したシングルリングとして動作します。このため，リング障害の検出および復旧の検出はそれぞれのリングで独立して行われます。

(3)　共有リンクありのマルチリング構成

マルチリング構成のうち，隣接するリングの接点となるノードが二つ以上の場合の構成について次の図に示します。

図 27-6　共有リンクありのマルチリング構成



複数のシングルリングが，二つ以上のノードで接続されている場合，複数のリングでリンクを共有することになります。このリンクを共有リンクと呼び，共有リンクのあるマルチリング構成を，共有リンクありのマルチリング構成と呼びます。これに対し，（2）のように，複数のシングルリングが一つのノードで接続されている場合には，共有リンクがありませんので，共有リンクなしのマルチリング構成と呼びます。

(4)　仮想リンク

Ring Protocol とスパニングツリーを併用できる装置では，二つの機能が共存しているリングネットワーク上の 2 装置間を，仮想的な回線で接続して運用します。この仮想的な回線を仮想リンクと呼びます。仮想

リンクには，仮想リンク間で制御フレームを送受信するための仮想リンク VLAN があります。仮想リンク VLAN にはデータ転送 VLAN のうち一つが割り当てられ，この VLAN 上で仮想リンク制御フレームとフラッシュ制御フレームを通信します。本装置は仮想リンクをサポートしていませんが，本装置をトランジットノードとして使用するリングネットワーク上で，Ring Protocol とスパニングツリーを併用している装置がある場合は，仮想リンク制御フレームの中継，およびフラッシュ制御フレームの受信だけをします。

27.2.2　制御 VLAN

Ring Protocol を利用するネットワークでは，制御フレームの送信範囲を限定するために，制御フレームの送受信に専用の VLAN を使用します。この VLAN を制御 VLAN と呼び，リングを構成するすべてのノードで同一の VLAN を使用します。制御 VLAN は，リングごとに共通な一つの VLAN を使用しますので，マルチリング構成時には，隣接するリングで異なる VLAN を使用する必要があります。

27.2.3　障害監視方法

Ring Protocol のリング障害の監視は，マスタノードがヘルスチェックフレームと呼ぶ制御フレームを定期的に送信し，マスタノードがこのヘルスチェックフレームの受信可否を監視することで実現します。

詳細は，マスタノードの装置のマニュアルを参照してください。

27.2.4　通信経路の切り替え

(1)　トランジットノードの経路切り替え

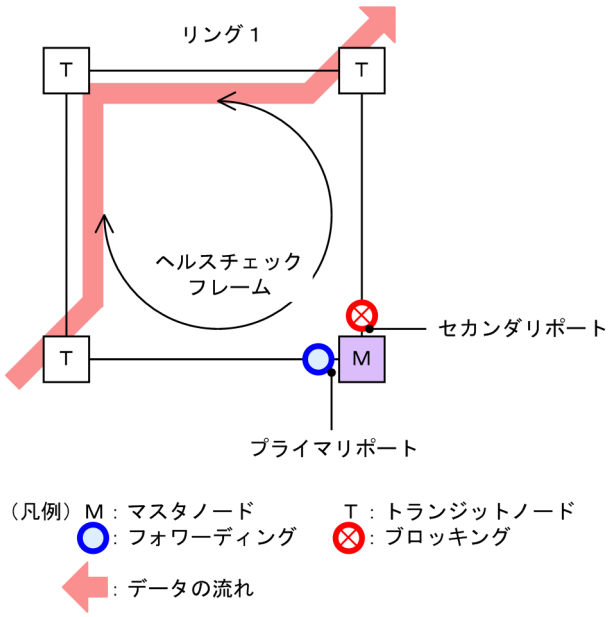
マスタノードがリングの障害を検出すると，同一の制御 VLAN を持つリング内の，そのほかのトランジットノードに対して MAC アドレステーブルエントリのクリアを要求するために，フラッシュ制御フレームと呼ぶ制御フレームを送信します。トランジットノードでは，このフラッシュ制御フレームを受信すると，MAC アドレステーブルエントリのクリアを行います。これによって，MAC アドレスの学習が行われるまでフラッディングを行います。新しい経路でのフレームの送受信によって MAC アドレス学習が行われ，通信経路の切り替えが完了します。

27.3　シングルリングの動作概要

27.3.1　リング正常時の動作

シングルリングでのリング正常時の動作について次の図に示します。

図 27–7　リング正常時の動作



(1)　マスタノード動作

片方向リンク障害による障害誤検出を防止するために，二つのリングポートからヘルスチェックフレームを送信します。あらかじめ設定された時間内に，両方向のヘルスチェックフレームを受信するか監視します。データフレームの転送は，プライマリポートで行います。セカンダリポートは論理ブロックされているため，データフレームの転送および MAC アドレス学習は行いません。

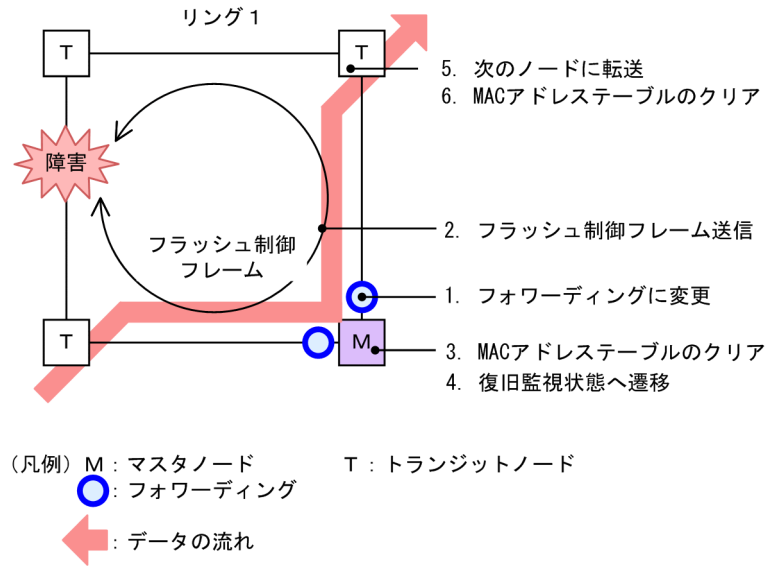
(2)　トランジットノード動作

トランジットノードでは，マスタノードが送信するヘルスチェックフレームの監視は行いません。ヘルスチェックフレームを受信すると，リング内の次ノードに転送します。データフレームの転送は，両リングポートで行います。

27.3.2　障害検出時の動作

シングルリングでのリング障害検出時の動作について次の図に示します。

図 27-8　リング障害時の動作



(1)　マスタノード動作

あらかじめ設定された時間内に，両方向のヘルスチェックフレームを受信しなければ障害と判断します。障害を検出したマスタノードは，次に示す手順で切り替え動作を行います。

1.　データ転送用リング VLAN 状態の変更

セカンダリポートのリング VLAN 状態をブロッキングからフォワーディングに変更します。障害検出時のリング VLAN 状態は次の表のように変更します。

表 27-2　障害検出時のデータ転送用リング VLAN 状態

リングポート	変更前（正常時）	変更後（障害時）
プライマリポート	フォワーディング	フォワーディング
セカンダリポート	ブロッキング	フォワーディング

2.　フラッシュ制御フレームの送信

マスタノードのプライマリポートおよびセカンダリポートからフラッシュ制御フレームを送信します。

3.　MAC アドレステーブルのクリア

MAC アドレステーブルエントリのクリアを行います。MAC アドレステーブルエントリをクリアすることで，迂回経路へ切り替えられます。

4.　監視状態の変更

リング障害を検出すると，マスタノードは障害監視状態から復旧監視状態に遷移します。

(2)　トランジットノード動作

障害を検出したマスタノードから送信されるフラッシュ制御フレームを受信すると，トランジットノードでは次に示す動作を行います。

5.　フラッシュ制御フレームの転送

受信したフラッシュ制御フレームを次のノードに転送します。

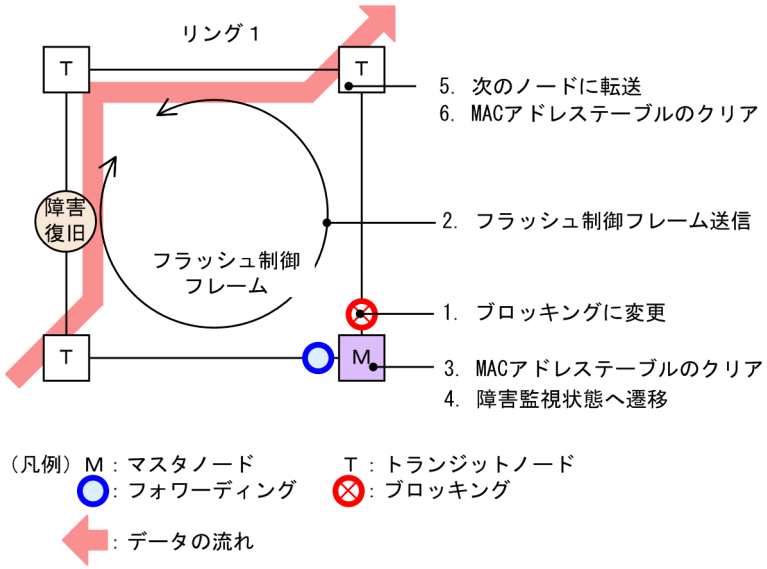
6. MAC アドレステーブルのクリア

MAC アドレステーブルエントリのクリアを行います。MAC アドレステーブルエントリをクリアすることで，迂回経路へ切り替えられます。

27.3.3　復旧検出時の動作

シングルリングでのリング障害復旧時の動作について次の図に示します。

図 27-9　障害復旧時の動作



(1)　マスタノード動作

リング障害を検出している状態で，自身が送出したヘルスチェックフレームを受信すると，リング障害が復旧したと判断し，次に示す復旧動作を行います。

1. データ転送用リング VLAN 状態の変更

セカンダリポートのリング VLAN 状態をフォワーディングからブロッキングに変更します。復旧検出時のリング VLAN 状態は次の表のように変更します。

表 27-3　復旧検出時のデータ転送用リング VLAN 状態

リングポート	変更前（障害時）	変更後（復旧時）
プライマリポート	フォワーディング	フォワーディング
セカンダリポート	フォワーディング	ブロッキング

2. フラッシュ制御フレームの送信

マスタノードのプライマリポートおよびセカンダリポートからフラッシュ制御フレームを送信します。なお，リング障害復旧時は，各トランジットノードが転送したフラッシュ制御フレームがマスタノードへ戻ってきますが，マスタノードでは受信しても廃棄します。

3. MAC アドレステーブルのクリア

MAC アドレステーブルエントリのクリアを行います。

MAC アドレステーブルエントリをクリアすることで，迂回経路へ切り替えられます。

4. 監視状態の変更

リング障害の復旧を検出すると，マスタノードは復旧監視状態から障害監視状態に遷移します。

(2) トランジットノード動作

マスタノードから送信されるフラッシュ制御フレームを受信すると，次に示す動作を行います。

5. フラッシュ制御フレームの転送

受信したフラッシュ制御フレームを次のノードに転送します。

6. MAC アドレステーブルのクリア

MAC アドレステーブルエントリのクリアを行います。

MAC アドレステーブルエントリをクリアすることで，迂回経路へ切り替えられます。

また，リンク障害が発生したトランジットノードでは，リンク障害が復旧した際のループの発生を防ぐため，リングポートのリング VLAN 状態はブロッキング状態となります。ブロッキング状態を解除する契機は，マスタノードが送信するフラッシュ制御フレームを受信したとき，またはトランジットノードでリングポートのフラッシュ制御フレーム受信待ち保護時間（forwarding-shift-time）がタイムアウトしたときとなります。フラッシュ制御フレーム受信待ち保護時間（forwarding-shift-time）は，リングポートのリンク障害復旧時に設定されます。

27.4　マルチリングの動作概要

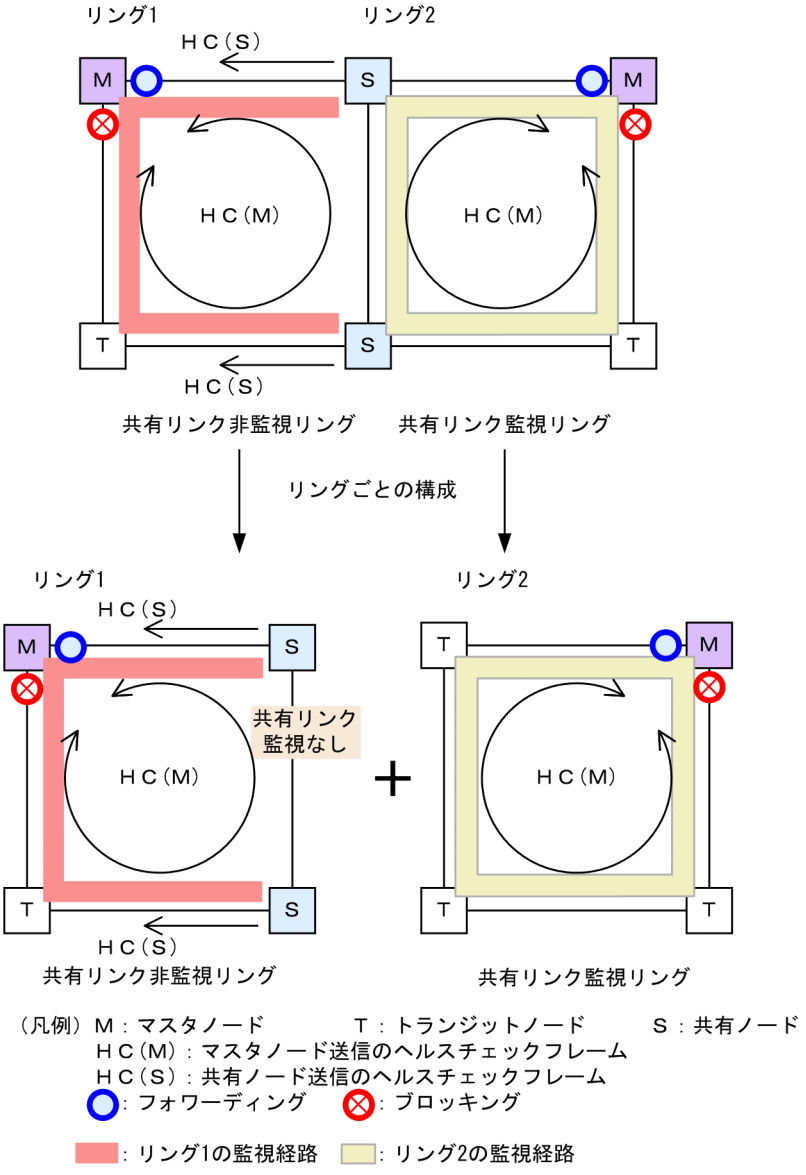
マルチリング構成のうち，共有リンクありのマルチリング構成について説明します。共有リンクなしのマルチリング構成については，シングルリング時の動作と同様ですので，「27.3　シングルリングの動作概要」を参照してください。

なお，この節以降，HC はヘルスチェックフレームを意味し，HC(M)はマスタノードが送信するヘルスチェックフレーム，HC(S)は共有ノードが送信するヘルスチェックフレームを表します。

27.4.1　リング正常時の動作

共有リンクありのマルチリング構成でのリング正常時の状態について次の図に示します。

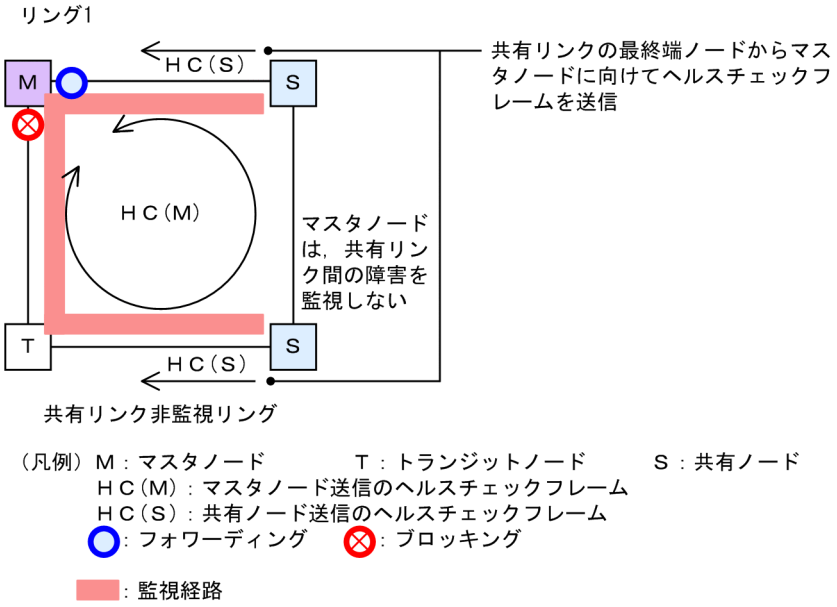
図 27-10　リング正常時の状態



(1)　共有リンク非監視リング

共有リンク非監視リングは，マスタノード 1 台とトランジットノード数台で構成します。しかし，共有リンクの障害を監視しないため，補助的な役割として，共有リンクの両端に位置する共有リンク非監視リングの最終端ノード（共有ノード）から，ヘルスチェックフレームをマスタノードに向けて送信します。このヘルスチェックフレームは，二つのリングポートのうち，共有リンクではない方のリングポートから送信します。これによって，共有リンク非監視リングのマスタノードは，共有リンクで障害が発生した場合に，自身が送信したヘルスチェックフレームが受信できなくなっても，共有リンク非監視リングの最終端ノード（共有ノード）からのヘルスチェックフレームが受信できている間は障害を検出しないようにできます。

図 27-11　共有リンク非監視リングでの正常時の動作



(a)　マスタノード動作

片方向リンク障害による障害誤検出を防止するために，二つのリングポートからヘルスチェックフレーム（HC(M)）を送信します。あらかじめ設定した時間内に，両方向の HC(M)を受信するか監視します。マスタノードが送信した HC(M)とは別に，共有リンクの両端に位置する共有リンク非監視リングの最終端ノード（共有ノード）から送信したヘルスチェックフレーム（HC(S)）についても合わせて受信を監視します。データフレームの転送は，プライマリポートで行います。セカンダリポートは論理ブロックされているため，データフレームの転送および MAC アドレス学習は行いません。

(b)　トランジットノード動作

トランジットノードの動作は，シングルリング時と同様です。トランジットノードは，HC(M)および HC(S)を監視しません。HC(M)や HC(S)を受信すると，リング内の次ノードに転送します。データフレームの転送は，両リングポートで行います。

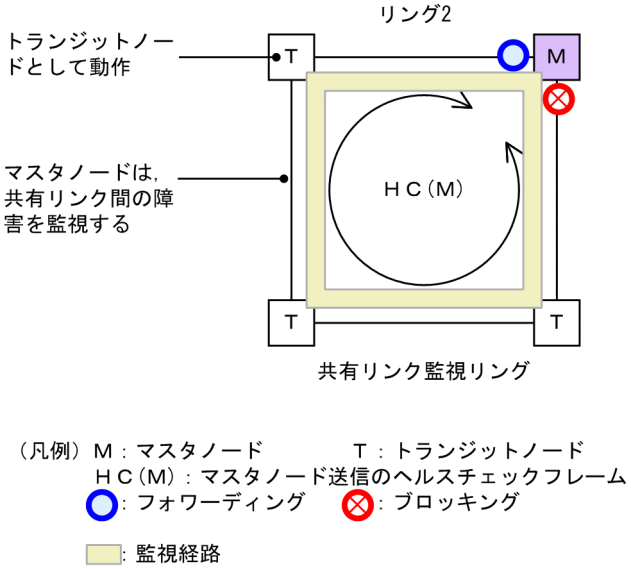
(c)　共有リンク非監視リングの最終端ノード動作

共有リンク非監視リングの最終端ノード（共有ノード）は，共有リンク非監視リングのマスタノードに向けて HC(S)の送信を行います。HC(S)の送信は，二つのリングポートのうち，共有リンクではない方のリングポートから送信します。マスタノードが送信する HC(M)や，データフレームの転送については，トランジットノードの場合と同様となります。

(2)　共有リンク監視リング

共有リンク監視リングは，シングルリング時と同様に，マスタノード 1 台と，そのほか数台のトランジットノードとの構成となります。共有リンクの両端に位置するノードは，シングルリング時と同様にマスタノードまたはトランジットノードとして動作します。

図 27-12　共有リンク監視リングでの正常時の動作



（凡例）Ｍ：マスタノード　　Ｔ：トランジットノード
ＨＣ（M）：マスタノード送信のヘルスチェックフレーム
：フォワーディング　：ブロッキング
：監視経路

(a)　マスタノード動作

片方向リンク障害による障害誤検出を防止するために，二つのリングポートからヘルスチェックフレーム（HC(M)）を送信します。あらかじめ設定された時間内に，両方向の HC(M)を受信するかを監視します。データフレームの転送は，プライマリポートで行います。セカンダリポートは論理ブロックされているため，データフレームの転送および MAC アドレス学習は行いません。

(b)　トランジットノード動作

トランジットノードの動作は，シングルリング時と同様です。トランジットノードは，マスタノードが送信した HC(M)を監視しません。HC(M)を受信すると，リング内の次ノードに転送します。データフレームの転送は，両リングポートで行います。

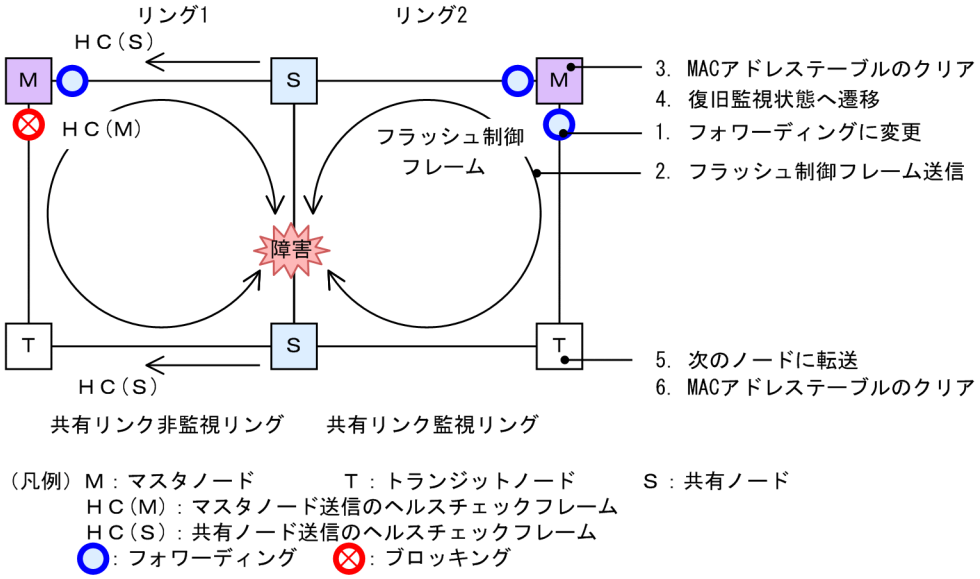
27.4.2　共有リンク障害・復旧時の動作

共有リンクありのマルチリング構成時に，共有リンク間で障害が発生した際の障害および復旧動作について説明します。

(1)　障害検出時の動作

共有リンクの障害を検出した際の動作について次の図に示します。

図 27-13　共有リンク障害時の動作



(a)　共有リンク監視リングのマスタノード動作

共有リンクで障害が発生すると，マスタノードは両方向の HC(M)を受信できなくなり，リング障害を検出します。障害を検出したマスタノードはシングルリング時と同様に，次に示す手順で障害動作を行います。

1. データ転送用リング VLAN 状態の変更
2. フラッシュ制御フレームの送信
3. MAC アドレステーブルのクリア
4. 監視状態の変更

(b)　共有リンク監視リングのトランジットノード動作

シングルリング時と同様に，マスタノードから送信されるフラッシュ制御フレームを受信すると次に示す動作を行います。

5. フラッシュ制御フレームの転送
6. MAC アドレステーブルのクリア

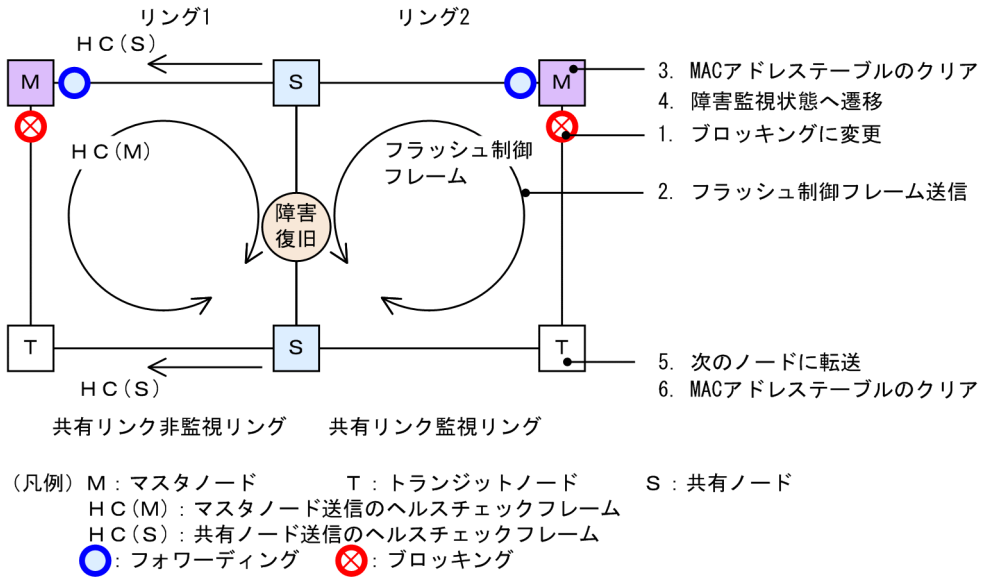
(c)　共有リンク非監視リングのマスタノードおよびトランジットノード動作

共有リンク非監視リングのマスタノードは，共有リンクでのリング障害を検出しないため，障害動作は行いません。このため，トランジットノードについても経路の切り替えは発生しません。

(2)　復旧検出時の動作

共有リンクの障害復旧を検出した際の動作について次の図に示します。

図 27-14　共有リング復旧時の動作



(a)　共有リンク監視リングのマスタノード動作

リング障害を検出している状態で，自身が送信した HC(M)を受信すると，リング障害が復旧したと判断し，シングルリング時と同様に，次に示す手順で復旧動作を行います。

1. データ転送用リング VLAN 状態の変更
2. フラッシュ制御フレームの送信
3. MAC アドレステーブルのクリア
4. 監視状態の変更

(b)　共有リンク監視リングのトランジットノード動作

シングルリング時と同様に，マスタノードから送信されるフラッシュ制御フレームを受信すると次に示す動作を行います。

5. フラッシュ制御フレームの転送
6. MAC アドレステーブルのクリア

(c)　共有リンク非監視リングのマスタノードおよびトランジットノード動作

共有リンク非監視リングのマスタノードは，リング障害を検出していないため，トランジットノードを含め，復旧動作は行いません。

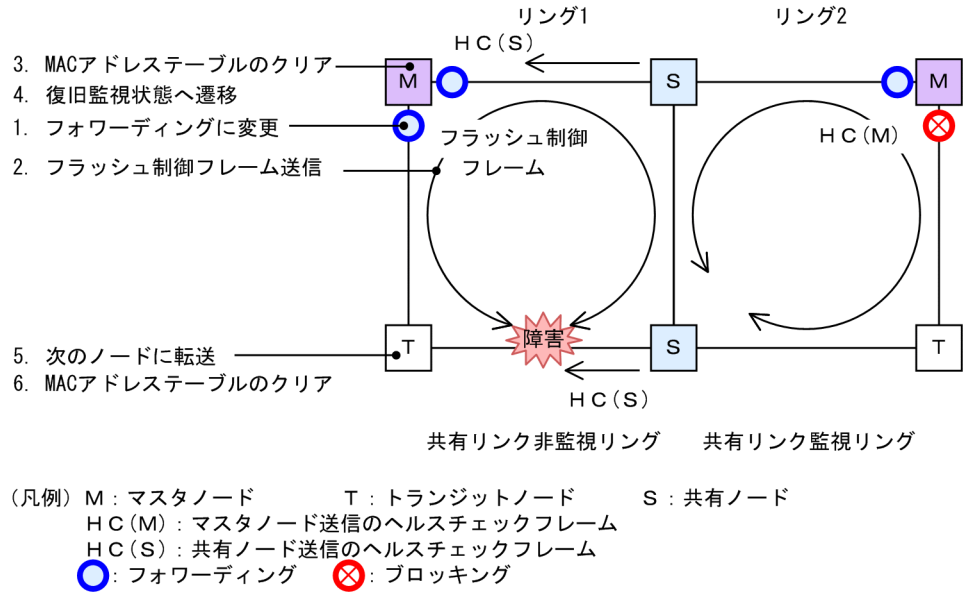
27.4.3　共有リンク非監視リングでの共有リンク以外の障害・復旧時の動作

共有リンク非監視リングでの，共有リンク以外のリング障害および復旧時の動作について説明します。

(1)　障害検出時の動作

共有リンク非監視リングでの共有リンク以外の障害を検出した際の動作について次の図に示します。

図 27-15　共有リンク非監視リングにおける共有リンク以外のリング障害時の動作



（凡例）Ｍ：マスタノード　　Ｔ：トランジットノード　　Ｓ：共有ノード
ＨＣ（Ｍ）：マスタノード送信のヘルスチェックフレーム
ＨＣ（Ｓ）：共有ノード送信のヘルスチェックフレーム
：フォワーディング　：ブロッキング

(a)　共有リンク非監視リングのマスタノード動作

共有リンク非監視リングのマスタノードは，自身が送信した両方向の HC(M)と共有ノードが送信した HC(S)が共に未受信となりリング障害を検出します。障害を検出したマスタノードの動作はシングルリング時と同様に，次に示す手順で障害動作を行います。

1. データ転送用リング VLAN 状態の変更
2. フラッシュ制御フレームの送信
3. MAC アドレステーブルのクリア
4. 監視状態の変更

(b)　共有リンク非監視リングのトランジットノードおよび共有ノード動作

シングルリング時と同様に，マスタノードから送信されるフラッシュ制御フレームを受信すると次に示す動作を行います。

5. フラッシュ制御フレームの転送
6. MAC アドレステーブルのクリア

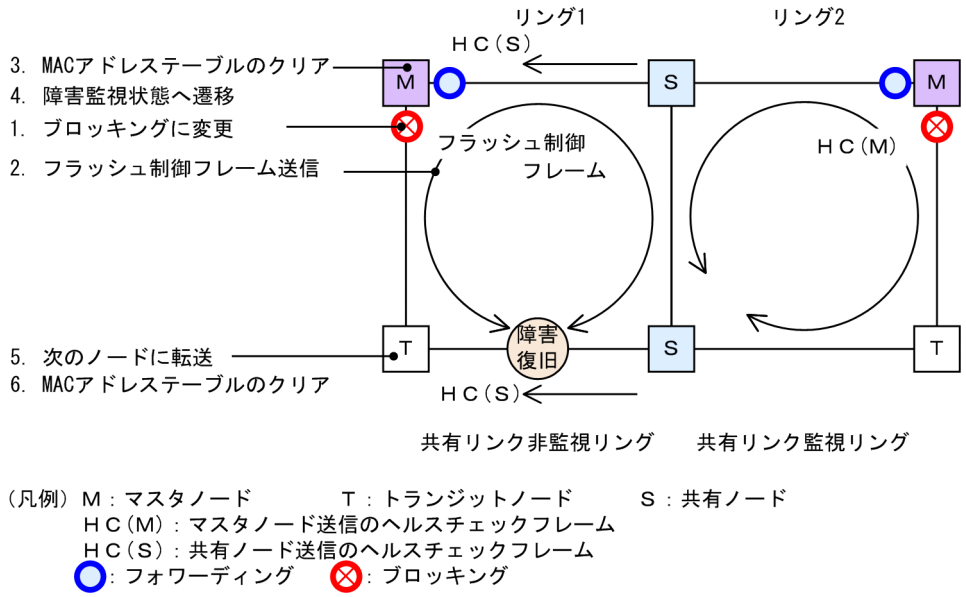
(c)　共有リンク監視リングのマスタノードおよびトランジットノード動作

共有リンク監視リング内では障害が発生していないため，障害動作は行いません。

(2)　復旧検出時の動作

共有リンク非監視リングでの共有リンク以外の障害が復旧した際の動作について次の図に示します。

図 27-16　共有リンク非監視リングでの共有リンク以外のリング障害復旧時の動作



（凡例）Ｍ：マスタノード　　Ｔ：トランジットノード　　Ｓ：共有ノード
ＨＣ（M）：マスタノード送信のヘルスチェックフレーム
ＨＣ（S）：共有ノード送信のヘルスチェックフレーム
：フォワーディング　：ブロッキング

(a)　共有リンク非監視リングのマスタノード動作

リング障害を検出している状態で，自身が送信した HC(M)を受信するか，または共有ノードが送信した HC(S)を両方向から受信すると，リング障害が復旧したと判断し，シングルリング時と同様に，次に示す手順で復旧動作を行います。

1. データ転送用リング VLAN 状態の変更
2. フラッシュ制御フレームの送信
3. MAC アドレステーブルのクリア
4. 監視状態の変更

(b)　共有リンク非監視リングのトランジットノードおよび共有ノード動作

シングルリング時と同様に，マスタノードから送信されるフラッシュ制御フレームを受信すると次に示す動作を行います。

5. フラッシュ制御フレームの転送
6. MAC アドレステーブルのクリア

(c)　共有リンク監視リングのマスタノードおよびトランジットノード動作

共有リンク監視リング内では障害が発生していないため，復旧動作は行いません。

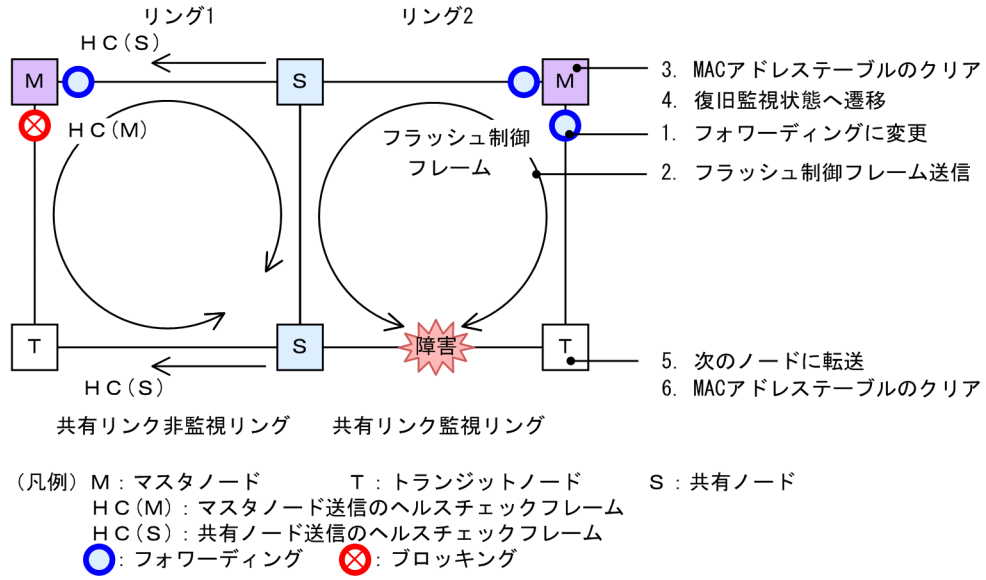
27.4.4　共有リンク監視リングでの共有リンク以外の障害・復旧時の動作

共有リンク監視リングでの共有リンク以外のリング障害および復旧時の動作について説明します。

(1)　障害検出時の動作

共有リンク監視リングでの共有リンク以外の障害を検出した際の動作について次の図に示します。

図 27-17　共有リンク監視リングでの共有リンク以外のリング障害時の動作



(a)　共有リンク監視リングのマスタノード動作

共有リンク監視リング内で障害が発生すると，マスタノードは両方向の HC(M)を受信できなくなり，リング障害を検出します。障害を検出したマスタノードはシングルリング時と同様に，次に示す手順で障害動作を行います。

1. データ転送用リング VLAN 状態の変更
2. フラッシュ制御フレームの送信
3. MAC アドレステーブルのクリア
4. 監視状態の変更

(b)　共有リンク監視リングのトランジットノード動作

シングルリング時と同様に，マスタノードから送信されるフラッシュ制御フレームを受信すると次に示す動作を行います。

5. フラッシュ制御フレームの転送
6. MAC アドレステーブルのクリア

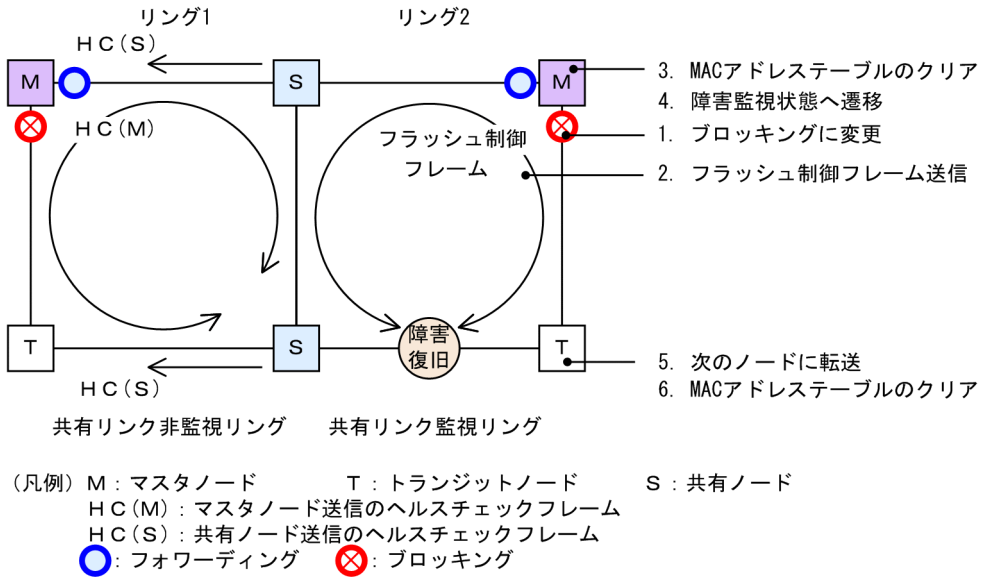
(c)　共有リンク非監視リングのマスタノードおよびトランジットノード（共有ノード）動作

共有リンク非監視リング内では障害が発生していないため，障害動作は行いません。

(2)　復旧検出時の動作

共有リンク監視リングでの共有リンク以外の障害が復旧した際の動作について次の図に示します。

図 27-18　共有リンク監視リングでの共有リンク以外のリング障害復旧時の動作



(a)　共有リンク監視リングのマスタノード動作

リング障害を検出している状態で，自身が送信した HC(M)を受信すると，リング障害が復旧したと判断し，シングルリング時と同様に，次に示す手順で復旧動作を行います。

1. データ転送用リング VLAN 状態の変更
2. フラッシュ制御フレームの送信
3. MAC アドレステーブルのクリア
4. 監視状態の変更

(b)　共有リンク監視リングのトランジットノード動作

シングルリング時と同様に，マスタノードから送信されるフラッシュ制御フレームを受信すると次に示す動作を行います。

5. フラッシュ制御フレームの転送
6. MAC アドレステーブルのクリア

(c)　共有リンク非監視リングのマスタノードおよびトランジットノード（共有ノード）動作

共有リンク非監視リング内では障害が発生していないため，復旧動作は行いません。

27.5　Ring Protocol の多重障害監視機能

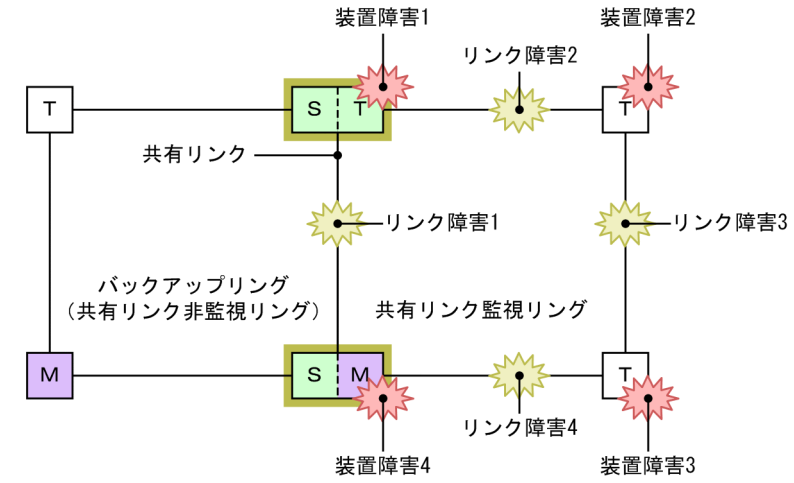
27.5.1　概要

多重障害監視機能は，共有リンクありのマルチリング構成での共有リンク監視リングの多重障害を監視して，多重障害を検出した場合に共有リンク非監視リングに経路を切り替える機能です。このとき，経路の切り替えに使用する共有リンク非監視リングを**バックアップリング**と呼びます。

多重障害監視機能で検出の対象となるのは，共有リンク障害と，共有リンク監視リング内のその他のリンク障害およびリンク障害を伴う装置障害です。

共有リンク監視リングでの障害発生例と，多重障害監視機能で検出できる障害の組み合わせを次に示します。

図 27-19　共有リンク監視リングでの障害発生例



（凡例）M：マスタノード　　T：トランジットノード
　　S：共有リンクの最終端ノード（トランジットノード）　　：共有ノード

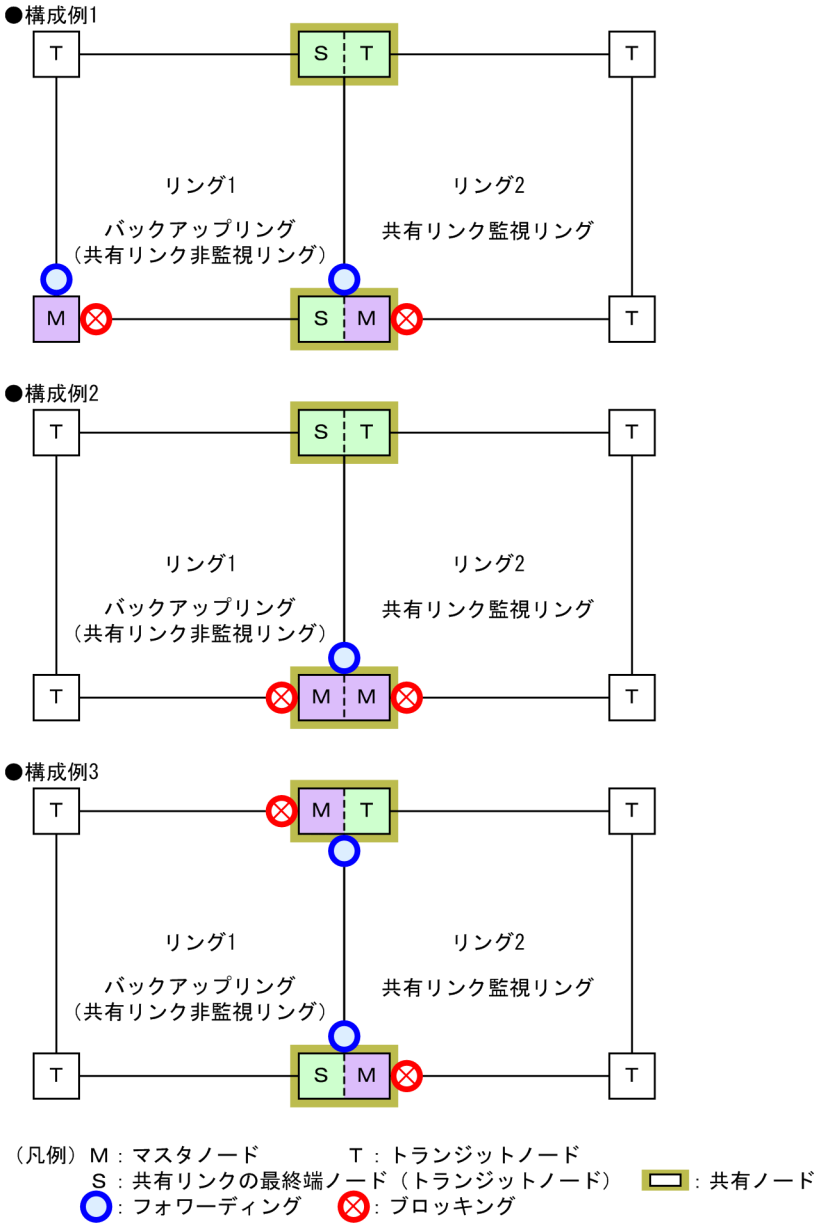
表 27-4　多重障害監視機能で検出できる障害の組み合わせ

障害種別	検出可能な組み合わせ	
リンク障害	リンク障害 1（共有リンク障害）	リンク障害 2（その他のリンク障害）
	リンク障害 1（共有リンク障害）	リンク障害 3（その他のリンク障害）
	リンク障害 1（共有リンク障害）	リンク障害 4（その他のリンク障害）
装置障害	装置障害 1（共有ノード障害）だけ	
	装置障害 4（共有ノード障害）だけ	
	装置障害 2（トランジットノード障害）	リンク障害 1（共有リンク障害）
	装置障害 3（トランジットノード障害）	リンク障害 1（共有リンク障害）

27.5.2　多重障害監視機能の基本構成

多重障害監視機能を適用できる共有リンクありのマルチリング構成は，共有リンク監視リングとバックアップリングとなる共有リンク非監視リングをそれぞれ 1 リングずつ対応づけた構成です。このとき，共有ノードを共有リンク監視リングのマスタノードとして設定します。多重障害監視機能の基本構成例を次の図に示します。

図 27-20　多重障害監視機能の基本構成例

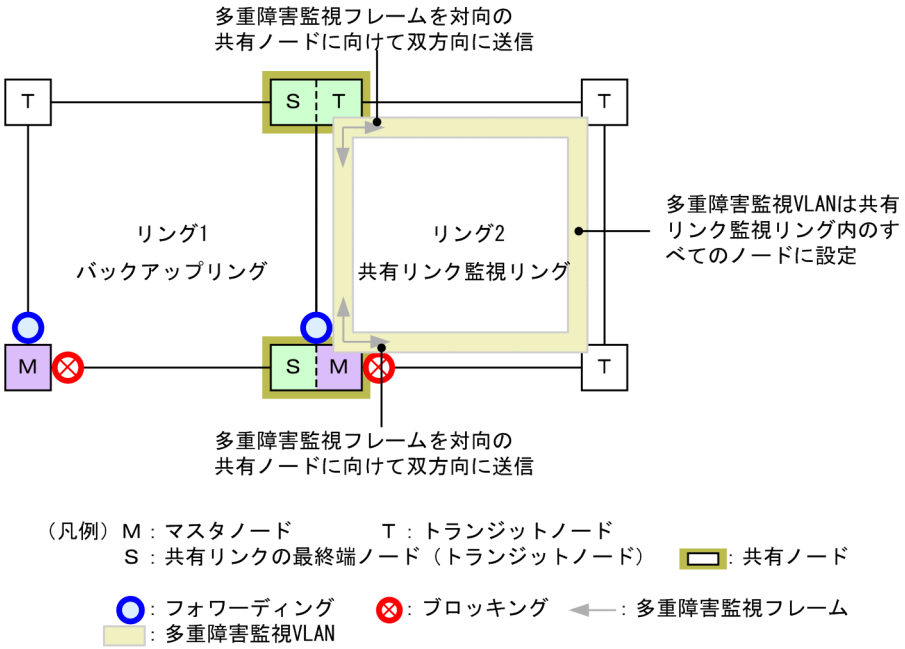


27.5.3　多重障害監視の動作概要

多重障害は，共有リンクありのマルチリング構成で共有リンクの両端に位置する共有ノードで監視します。共有ノードは，共有リンク監視リングの多重障害を監視するための制御フレーム（**多重障害監視フレーム**と呼びます）を送信します。対向の共有ノードでは，多重障害監視フレームの受信を監視します。なお，多重障害監視フレームは専用の VLAN（**多重障害監視 VLAN** と呼びます）上に送信します。

多重障害監視の動作概要を次の図に示します。

図 27-21　多重障害監視の動作概要



(1)　共有リンク監視リングの各ノードの動作

共有リンク監視リングのマスタノードおよびトランジットノードの動作は，マルチリング時の動作と同様ですので，「27.4.1　リング正常時の動作　(2)　共有リンク監視リング」を参照してください。

共有ノードでは，共有リンク監視リングの多重障害を監視します。共有ノードは，多重障害監視フレームを両リングポートから送信するとともに，対向の共有ノードが両リングポートから送信した多重障害監視フレームをあらかじめ設定した時間内に受信するかを監視します。

(2)　バックアップリングの各ノードの動作

バックアップリングのマスタノードおよびトランジットノードの動作は，マルチリング時の動作と同様ですので，「27.4.1　リング正常時の動作　(1)　共有リンク非監視リング」を参照してください。

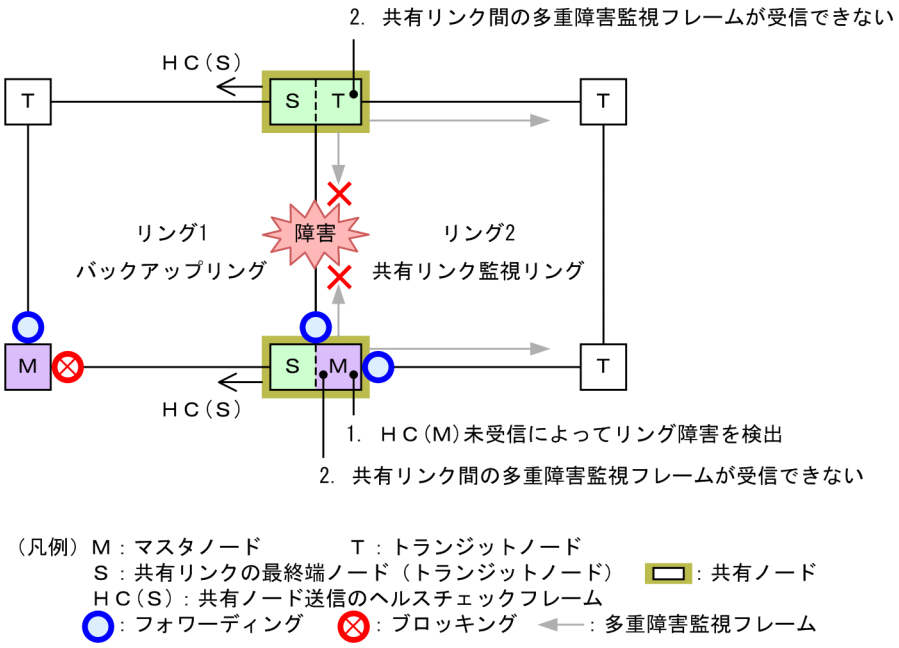
27.5.4　多重障害発生時の動作

共有リンク監視リングで，共有リンク障害とその他のリンク障害による多重障害が発生した場合の動作について説明します。

(1)　共有リンク障害時の動作

共有リンク監視リングでの共有リンク障害時の動作について，次の図に示します。

図 27-22　共有リンク障害時の動作



(a)　共有リンク監視リングの各ノードの動作

1.　HC(M)未受信によってリング障害を検出

マスタノードは両方向の HC(M)を受信できなくなり，リング障害を検出します。リング障害検出時のマスタノードおよびトランジットノードの動作は，マルチリング時の動作と同様ですので，「27.4.2 共有リンク障害・復旧時の動作　(1)　障害検出時の動作」を参照してください。

2.　共有リンク間の多重障害監視フレームが受信できない

共有ノードは共有リンク間での多重障害監視フレームの受信ができなくなりますが，もう一方のリングポートでは受信できているため，多重障害の監視を継続します。

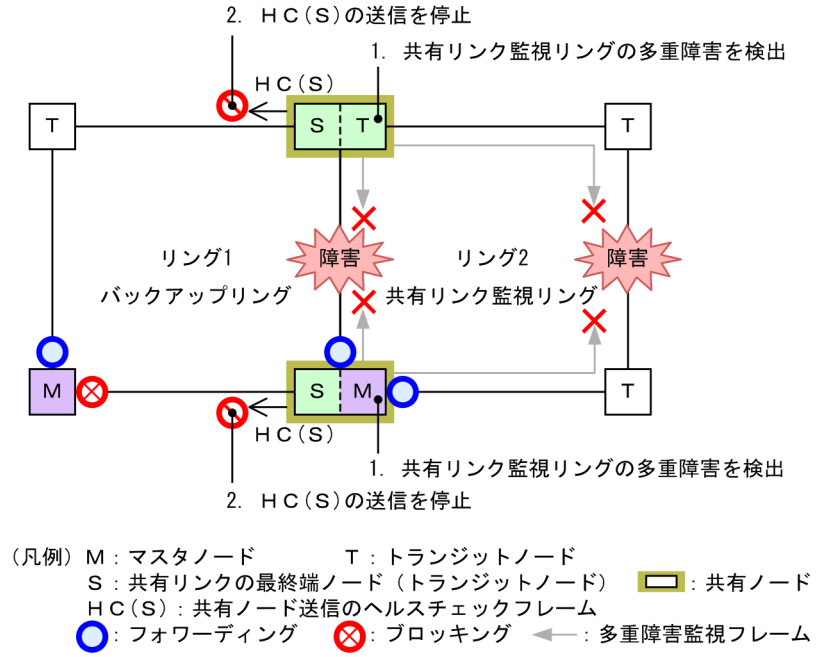
(b)　バックアップリングの各ノードの動作

バックアップリングではマスタノードが送信した HC(M)の受信はできなくなりますが，共有ノードが送信した HC(S)は受信できているため，障害検出時の動作は行いません。

(2)　多重障害発生時の動作

共有リンク障害と共有リンク監視リング内のその他のリンク障害による多重障害発生時の動作について，次の図に示します。

図 27-23　多重障害発生時の動作



(a)　共有リンク監視リングの各ノードの動作

1.　共有リンク監視リングの多重障害を検出

共有ノードは両リングポートで多重障害監視フレームを受信できなくなり，多重障害を検出します。

(b)　バックアップリングの各ノードの動作

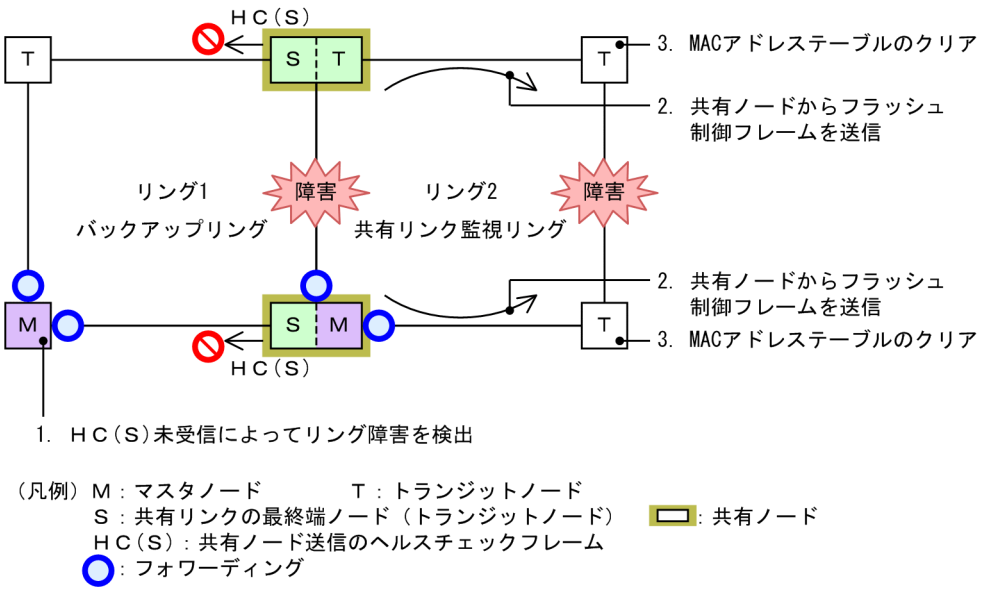
2.　HC(S)の送信を停止

多重障害を検出した共有ノードは，バックアップリングの HC(S)の送信を停止します。

(3)　バックアップリングへの切り替え動作

多重障害検出によるバックアップリングへの切り替え動作について，次の図に示します。

図 27-24　バックアップリングへの切り替え動作



(a)　バックアップリングの各ノードの動作

1.　HC(S)未受信によってリング障害を検出

マスタノードは自身が送信した両方向の HC(M)と共有ノードが送信した HC(S)がどちらも未受信となり，リング障害を検出します。リング障害検出時のマスタノードおよびトランジットノードの動作は，マルチリング時の動作と同様ですので，「27.4.3　共有リンク非監視リングでの共有リンク以外の障害・復旧時の動作　(1)　障害検出時の動作」を参照してください。

(b)　共有リンク監視リングの各ノードの動作

2.　共有ノードからフラッシュ制御フレームを送信

バックアップリングのマスタノードから送信されたフラッシュ制御フレームを受信すると，共有ノードは共有リンク監視リングに向けて，MAC アドレステーブルのクリアだけをするフラッシュ制御フレームを送信します。

3.　MAC アドレステーブルのクリア

トランジットノードは共有ノードから送信されたフラッシュ制御フレームを受信して，MAC アドレステーブルをクリアします。

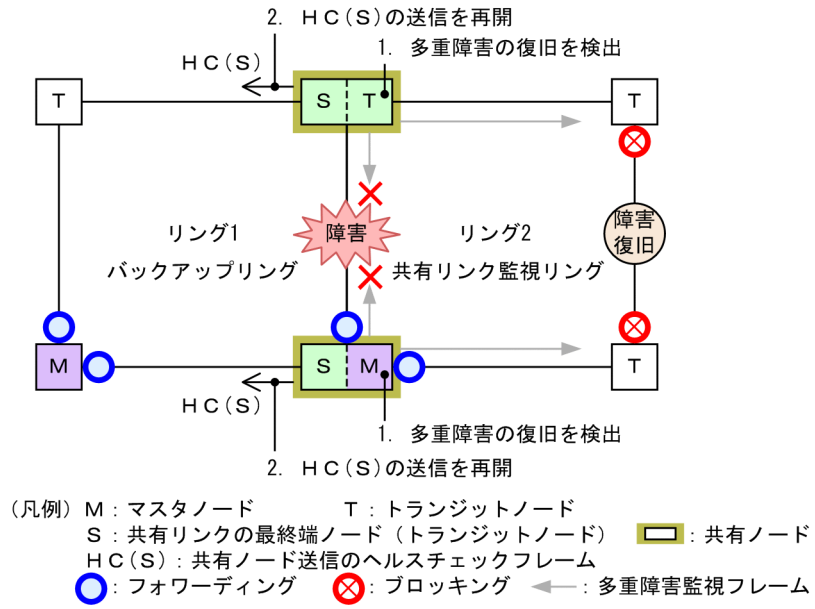
27.5.5　多重障害復旧時の動作

共有リンク監視リングでの多重障害が復旧した場合の動作について説明します。

(1)　多重障害からの一部復旧時の動作

共有リンク監視リングで多重障害からの一部復旧時の動作について，次の図に示します。

図 27-25　多重障害からの一部復旧時の動作



(a)　共有リンク監視リングの各ノードの動作

1.　多重障害の復旧を検出

共有ノードは対向の共有ノードが送信した多重障害監視フレームを受信して，多重障害の復旧を検出します。

(b)　バックアップリングの各ノードの動作

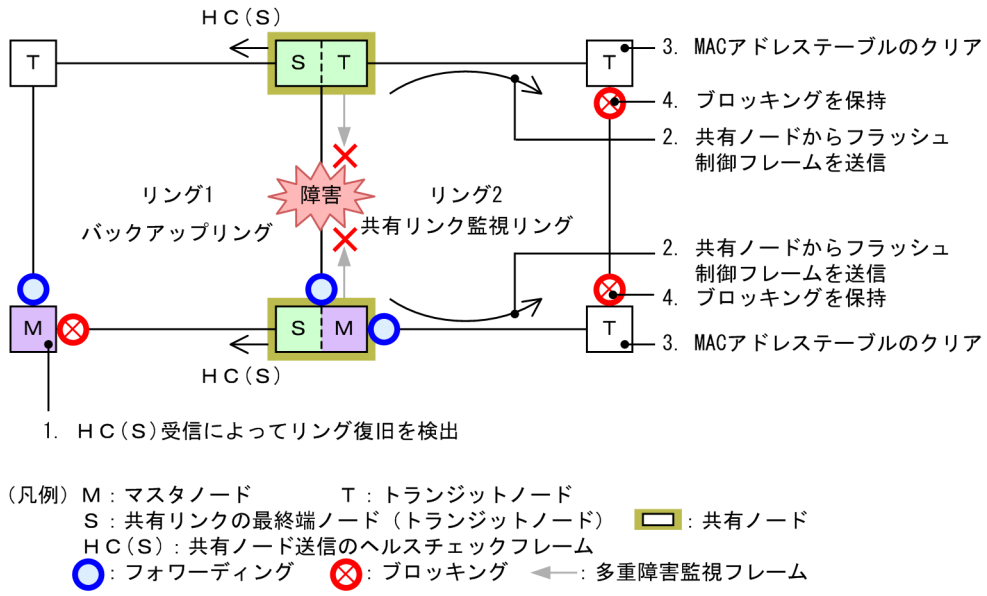
2.　HC(S)の送信を再開

多重障害の復旧を検出した共有ノードは，バックアップリングの HC(S)の送信を再開します。

(2)　バックアップリングからの切り戻し動作

バックアップリングからの切り戻し動作について，次の図に示します。

図 27-26　バックアップリングからの切り戻し動作



(a)　バックアップリングの各ノードの動作

1.　HC(S)受信によってリング復旧を検出

マスタノードは共有ノードが送信した HC(S)を両方向から受信すると，リング障害が復旧したと判断して復旧動作を行います。復旧検出時のマスタノードおよびトランジットノードの動作は，マルチリング時の動作と同様ですので，「27.4.3　共有リンク非監視リングでの共有リンク以外の障害・復旧時の動作　(2)　復旧検出時の動作」を参照してください。

(b)　共有リンク監視リングの各ノードの動作

2.　共有ノードからフラッシュ制御フレームを送信

バックアップリングのマスタノードから送信されたフラッシュ制御フレームを受信すると，共有ノードは共有リンク監視リングに向けて，MAC アドレステーブルのクリアだけをするフラッシュ制御フレームを送信します。

3.　MAC アドレステーブルのクリア

トランジットノードは共有ノードから送信されたフラッシュ制御フレームを受信して，MAC アドレステーブルをクリアします。

4.　ブロッキングを保持

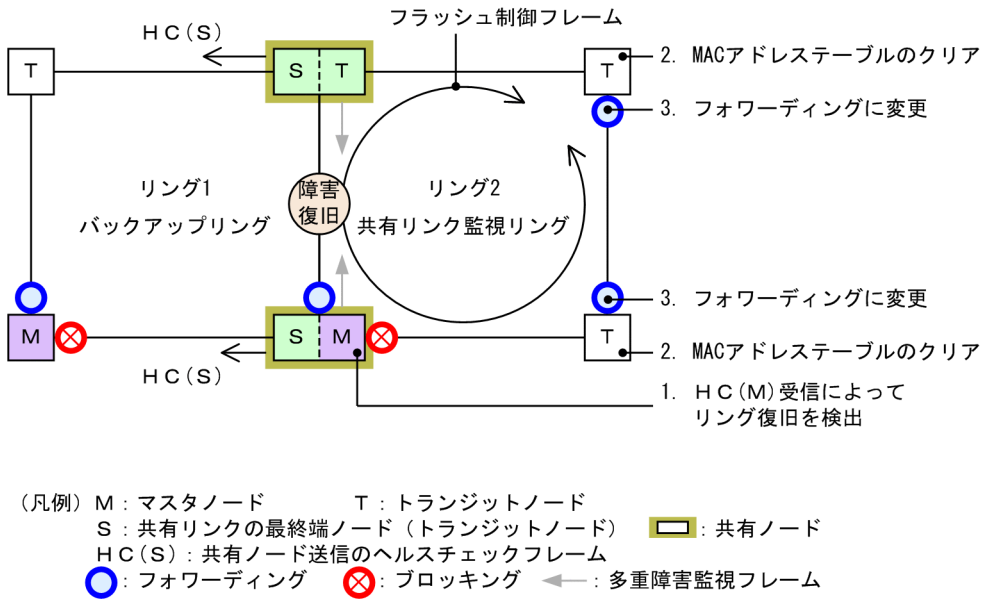
リンク障害から復旧したリングポートのリング VLAN 状態は，マスタノードがリング復旧を検出していないため，ブロッキングを保持します。

なお，ブロッキングの解除については「27.7　Ring Protocol 使用時の注意事項　(11)　多重障害の一部復旧時の通信について」を参照してください。

(3)　共有リンク障害復旧時の動作

共有リンク障害復旧時の動作について，次の図に示します。

図 27-27　共有リンク障害復旧時の動作



（凡例）Ｍ：マスタノード　　Ｔ：トランジットノード
Ｓ：共有リンクの最終端ノード（トランジットノード）　：共有ノード
ＨＣ（Ｓ）：共有ノード送信のヘルスチェックフレーム
：フォワーディング　：ブロッキング　：多重障害監視フレーム

(a)　共有リンク監視リングの各ノードの動作

1. HC(M)受信によってリング復旧を検出

マスタノードは自身が送信した HC(M)を受信すると，リング障害が復旧したと判断して復旧動作を行います。復旧検出時のマスタノードおよびトランジットノードの動作は，マルチリング時の動作と同様ですので，「27.4.2　共有リンク障害・復旧時の動作　(2)　復旧検出時の動作」を参照してください。

2. MAC アドレステーブルのクリア

トランジットノードはマスタノードから送信されたフラッシュ制御フレームを受信して，MAC アドレステーブルをクリアします。

3. フォワーディングに変更

トランジットノードはマスタノードが送信したフラッシュ制御フレームの受信によって，リンク障害から復旧したリングポートのリング VLAN 状態をフォワーディングに変更します。

27.6　Ring Protocol のネットワーク設計

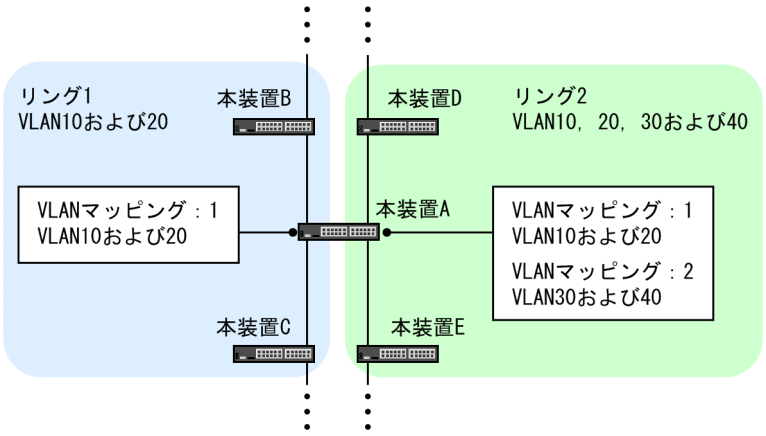
27.6.1　VLAN マッピングの使用方法

(1)　VLAN マッピングとデータ転送用 VLAN

マルチリング構成などで，一つの装置に複数のリング ID を設定するような場合，それぞれのリング ID に複数の同一 VLAN を設定する必要があります。このとき，データ転送用 VLAN として使用する VLAN のリスト（これを **VLAN マッピング**と呼びます）をあらかじめ設定しておくと，マルチリング構成時のデータ転送用 VLAN の設定を簡略できたり，コンフィグレーションの設定誤りによるループなどを防止できたりします。

VLAN マッピングは，データ転送用に使用する VLAN を VLAN マッピング ID に割り当てて使用します。この VLAN マッピング ID を VLAN グループに設定して，データ転送用 VLAN として管理します。

図 27-28　リングごとの VLAN マッピングの割り当て例



27.6.2　制御 VLAN の forwarding-delay-time の使用方法

トランジットノードの装置起動やプログラム再起動（運用コマンド restart axrp）など，Ring Protocol が初期状態から動作する場合，データ転送用 VLAN は論理ブロックされています。トランジットノードは，マスタノードが送信するフラッシュ制御フレームを受信することでこの論理ブロックを解除します。しかし，プログラム再起動時などは，マスタノードの障害監視時間が長いと，リングネットワークの状態変化を認識できないおそれがあります。この場合，フラッシュ制御フレーム受信待ち保護時間（forwarding-shift-time）がタイムアウトするまで論理ブロックは解除されないため，トランジットノードのデータ VLAN は通信できない状態になります。制御 VLAN のフォワーディング遷移時間（forwarding-delay-time）を設定すると次に示す手順で動作するため，このようなケースを回避できます。

1. トランジットノードは，装置起動やプログラム再起動直後に，制御 VLAN をいったん論理ブロックします。
2. トランジットノードの制御 VLAN が論理ブロックされたので，マスタノードで障害を検出します（ただし，装置起動時はこれ以前に障害を検出しています）。このため，通信は迂回経路に切り替わります。
3. トランジットノードは，制御 VLAN のフォワーディング遷移時間（forwarding-delay-time）のタイムアウトによって制御 VLAN のブロッキングを解除します。
4. マスタノードはヘルスチェックフレームを受信することで復旧を検出し，フラッシュ制御フレームを送信します。

5. トランジットノードは，このフラッシュ制御フレームを受信することでデータ転送用 VLAN の論理ブロックを解除します。これによってデータ転送用 VLAN での通信が再開され，リングネットワーク全体でも通常の通信経路に復旧します。

(1)　制御 VLAN のフォワーディング遷移時間（forwarding-delay-time）とフラッシュ制御フレーム受信待ち保護時間（forwarding-shift-time）の関係について

制御 VLAN のフォワーディング遷移時間（forwarding-delay-time）は，データ転送用 VLAN のフラッシュ制御フレーム受信待ち保護時間（forwarding-shift-time）より小さな値を設定してください。フラッシュ制御フレーム受信待ち保護時間（forwarding-shift-time）より大きな値を設定した場合，マスタノードで障害を検出するよりも早くデータ転送用 VLAN がフォワーディングとなるため，ループするおそれがあります。

27.6.3　Ring Protocol の禁止構成

禁止構成については，マスタノードの装置のマニュアルを参照してください。

27.6.4　多重障害監視機能の禁止構成

禁止構成については，共有ノードの装置のマニュアルを参照してください。

27.7　Ring Protocol 使用時の注意事項

(1)　運用中のコンフィグレーション変更について

運用中に Ring Protocol のコンフィグレーションを変更する際には，ループが発生しないように注意する必要があります。対象となるコンフィグレーションの対応方法を次に示します。

制御 VLAN（コンフィグレーションコマンド control-vlan）およびデータ転送用 VLAN（コンフィグレーションコマンド axrp vlan-mapping，vlan-group）の変更

リング内で使用する制御 VLAN やデータ転送用 VLAN を変更する場合は，ネットワークの構成上ループが発生するため，あらかじめ変更する VLAN を停止するか，リングポートを shutdown コマンドなどでダウン状態にしてから，変更してください。

(2)　他機能との共存

「22.3　レイヤ 2 スイッチ機能と他機能の共存について」を参照してください。

(3)　制御フレームを送受信する VLAN について

- Ring Protocol の制御フレームは Tagged フレームになります。このため，Ring Protocol の制御フレームを送受信する次の VLAN は，トランクポートの allowed vlan（ネイティブ VLAN は不可）に設定してください。なお，デフォルト VLAN（VLAN ID ＝ 1）は設定できません。
  - 制御 VLAN
  - 共有ノードが多重障害監視に使用する VLAN
  - 隣接リング用フラッシュ制御フレームを送受信する VLAN
- Ring Protocol の制御フレームを送受信する VLAN を Tag 変換によって異なる VLAN ID に変換すると，正常に障害・復旧検出ができなくなります。Ring Protocol の制御フレームを送受信する VLAN に対して，Tag 変換は設定しないでください。

(4)　トランジットノードのリング VLAN 状態について

トランジットノードでは，装置またはリングポートが障害となり，その障害が復旧した際，ループの発生を防ぐために，リングポートのリング VLAN 状態はブロッキング状態となります。このブロッキング状態解除の契機の一つとして，フラッシュ制御フレーム受信待ち保護時間（forwarding-shift-time）のタイムアウトがあります。このとき，フラッシュ制御フレーム受信待ち保護時間（forwarding-shift-time）がマスタノードのヘルスチェック送信間隔よりも短い場合，マスタノードがリング障害の復旧を検出して，セカンダリポートをブロッキング状態に変更するよりも先に，トランジットノードのリングポートがフォワーディング状態となることがあり，ループが発生するおそれがあります。したがって，フラッシュ制御フレーム受信待ち保護時間（forwarding-shift-time）はマスタノードのヘルスチェック送信間隔より大きい値を設定してください。

(5)　Ring Protocol 使用時のネットワーク構築について

Ring Protocol を利用するネットワークはループ構成となります。したがって，次の手順でネットワークを構築し，ループを防止してください。

1. 事前に，リング構成ノードのリングポート（物理ポートまたはチャネルグループ）を shutdown コマンドなどでダウン状態にしてください。
2. Ring Protocol のコンフィグレーションを設定するか，Ring Protocol の設定を含むコンフィグレーションファイルのコピー（copy コマンド）をして，Ring Protocol を有効にしてください。

3. ネットワーク内のすべての装置に Ring Protocol の設定が完了した時点でリングポートをアップ（shutdown コマンドなどの解除）してください。

(6)　相互運用

Ring Protocol は，弊社独自仕様の機能です。他社スイッチとは相互運用できません。

(7)　ネットワーク内の多重障害時について

同一リング内の異なるノード間で 2 個所以上の障害が起きた場合（多重障害），マスタノードは既に 1 個所目の障害で障害検出を行っているため，2 個所目以降の障害を検出しません。また，多重障害での復旧検出についても，最後の障害が復旧するまでマスタノードが送信しているヘルスチェックフレームを受信できないため，復旧を検出できません。その結果，多重障害のうち，一部の障害が復旧した（リングとして障害が残っている状態）ときには一時的に通信できないことがあります。

なお，多重障害監視機能を適用すると，障害の組み合わせによっては多重障害を検出できる場合があります。多重障害監視機能については，「27.5　Ring Protocol の多重障害監視機能」を参照してください。

(8)　VLAN のダウンを伴うコンフィグレーションコマンドの設定について

Ring Protocol に関するコンフィグレーションコマンドが設定されていない状態で，一つ目の Ring Protocol に関するコンフィグレーションコマンド（次に示すどれかのコマンド）を設定した場合に，すべての VLAN が一時的にダウンします。そのため，Ring Protocol を用いたリングネットワークを構築する場合には，あらかじめ次に示すコンフィグレーションコマンドを設定しておくことを推奨します。

- axrp
- axrp vlan-mapping
- axrp-ring-port

なお，VLAN マッピング（axrp vlan-mapping コマンド）については，新たに追加設定した場合でも，その VLAN マッピングに関連づけられる VLAN が一時的にダウンします。すでに設定されている VLAN マッピング，およびその VLAN マッピングに関連づけられているその他の VLAN には影響ありません。

(9)　マスタノードの装置起動時のフラッシュ制御フレーム送受信について

マスタノードの装置起動時に，トランジットノードがマスタノードと接続されているリングポートのリンクアップをマスタノードよりも遅く検出すると，マスタノードが初期動作時に送信するフラッシュ制御フレームを受信できない場合があります。このとき，フラッシュ制御フレームを受信できなかったトランジットノードのリングポートはブロッキング状態となります。該当するリングポートはフラッシュ制御フレーム受信待ち保護時間（forwarding-shift-time）が経過するとフォワーディング状態となり，通信が復旧します。

隣接するトランジットノードでフラッシュ制御フレームが受信できない場合には，マスタノードのフラッシュ制御フレームの送信回数を調節すると，受信できることがあります。また，フラッシュ制御フレーム未受信による通信断の時間を短縮したい場合は，トランジットノードのフラッシュ制御フレーム受信待ち保護時間（初期値：10 秒）を短くしてください。

なお，マスタノードで次の操作をした場合も同様です。

- VLAN プログラムの再起動（運用コマンド restart vlan の実行）
- コンフィグレーションファイルの運用への反映（運用コマンド copy の実行）

(10)　多重障害監視機能の監視開始タイミングについて

共有ノードでは，多重障害監視機能を適用したあと，対向の共有ノードが送信する多重障害監視フレームを最初に受信したときに多重障害の監視を開始します。このため，多重障害監視機能を設定するときにリングネットワークに障害が発生していると，多重障害の監視を開始できません。多重障害監視機能は，リングネットワークが正常な状態で設定してください。

(11)　多重障害の一部復旧時の通信について

多重障害の一部復旧時はマスタノードがリング復旧を検出しないため，トランジットノードのリングポートはフラッシュ制御フレームの受信待ち保護時間（forwarding-shift-time）が経過するまでの間，論理ブロック状態となります。論理ブロック状態を解除したい場合は，フラッシュ制御フレーム受信待ち保護時間（初期値：10 秒）を短くするか，残りのリンク障害を復旧してマスタノードにリング復旧を検出させてください。なお，フラッシュ制御フレームの受信待ち保護時間を設定するときは，共有ノードの多重障害監視フレームの送信間隔よりも大きい値を設定してください。小さい値を設定すると，一時的にループが発生するおそれがあります。

(12)　リングポートに指定したリンクアグリゲーションのダウンについて

リングネットワークを構成するノード間をリンクアグリゲーション（スタティックモードまたは LACP モード）で接続していた場合，リンクアグリゲーションの該当チャネルグループを shutdown コマンドでダウン状態にするときは，あらかじめチャネルグループに属するすべての物理ポートを shutdown コマンドでダウン状態に設定してください。

なお，該当チャネルグループを no shutdown コマンドでアップ状態にするときは，あらかじめチャネルグループに属するすべての物理ポートを shutdown コマンドでダウン状態に設定してください。

(13)　restart コマンドの実行について

トランジットノードで次に示す運用コマンドを実行すると，リングポートの VLAN がダウン状態になるため，マスタノードがリング障害を誤検出してセカンダリポートをフォワーディングにします。トランジットノードのリングポートは一時的なダウン状態であるため，マスタノードがリング障害の復旧を検出するまでループが発生します。

- restart uplink-redundant（アップリンク・リダンダント併用時）

トランジットノードでこれらのコマンドを実行する場合，ループを防止するため次に示す手順を実施してください。

1. リングポートを shutdown コマンドなどでダウン状態にします。
2. 上記の restart コマンドを実行します。
3. 手順 1 でダウン状態としたリングポートをアップ状態（shutdown コマンドなどの解除）にします。

28 Ring Protocol の設定と運用

この章では，Ring Protocol の設定例について説明します。

28.1　コマンドガイド

Ring Protocol 機能が動作するためには，axrp，axrp vlan-mapping，mode，control-vlan，vlan-group，axrp-ring-port の設定が必要です。すべてのノードについて，構成に即したコンフィグレーションを設定してください。

28.1.1　コマンド一覧

Ring Protocol 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 28–1　コンフィグレーションコマンド一覧

コマンド名	説明
axrp	リング ID を設定します。
axrp vlan-mapping	VLAN マッピング，およびそのマッピングに参加する VLAN を設定します。
axrp-ring-port	リングポートを設定します。
control-vlan	制御 VLAN として使用する VLAN を設定します。
disable	Ring Protocol 機能を無効にします。
forwarding-shift-time	フラッシュ制御フレームの受信待ちを行う保護時間を設定します。
mac-clear-mode	Ring Protocol 機能でクリアする MAC アドレステーブルのエントリ対象を設定します。
mode	リングでの動作モードを設定します。
multi-fault-detection mode	多重障害監視の監視モードを設定します。
multi-fault-detection vlan	多重障害監視 VLAN として使用する VLAN を設定します。
name	リングを識別するための名称を設定します。
vlan-group	Ring Protocol 機能で運用する VLAN グループ，および VLAN マッピング ID を設定します。

Ring Protocol の運用コマンド一覧を次の表に示します。

表 28–2　運用コマンド一覧

コマンド名	説明
show axrp	Ring Protocol 情報を表示します。
restart axrp	Ring Protocol プログラムを再起動します。
dump protocols axrp	Ring Protocol プログラムで採取している詳細イベントトレース情報および制御テーブル情報をファイルへ出力します。
show port※1	ポートの Ring Protocol 使用状態を表示します。
show vlan※2	VLAN の Ring Protocol 使用状態を表示します。

注※1
「運用コマンドレファレンス」「20　イーサネット」を参照してください。

注※2
「運用コマンドレファレンス」「23　VLAN」を参照してください。

28.1.2　Ring Protocol 設定の流れ

Ring Protocol 機能を正常に動作させるには，構成に合った設定が必要です。設定の流れを次に示します。

(1)　スパニングツリーの停止

Ring Protocol を使用する場合には，事前にスパニングツリーを停止することを推奨します。スパニングツリーの停止については，「26　スパニングツリー」を参照してください。

(2)　Ring Protocol 共通の設定

リングの構成，またはリングでの本装置の位置づけに依存しない共通の設定を行います。

- リング ID
- 制御 VLAN
- VLAN マッピング
- VLAN グループ

(3)　モードとポートの設定

リングの構成，またはリングでの本装置の位置づけに応じた設定を行います。設定の組み合わせに矛盾がある場合，Ring Protocol 機能は正常に動作しません。

- モード
- リングポート

(4)　各種パラメータ設定

Ring Protocol 機能は，次に示すコンフィグレーションの設定がない場合，初期値で動作します。値を変更したい場合はコマンドで設定してください。

- 機能の無効化
- フラッシュ制御フレーム受信待ち保護時間
- Ring Protocol でクリアする MAC アドレステーブルのエントリ対象

28.1.3　リング ID の設定

[設定のポイント]

リング ID を設定します。同じリングに属する装置にはすべて同じリング ID を設定する必要があります。

[コマンドによる設定]

1. **(config)# axrp 1**
リング ID 1 を設定します。

28.1.4　制御 VLAN の設定

(1)　制御 VLAN の設定

[設定のポイント]

制御 VLAN として使用する VLAN を指定します。なお，次に示す VLAN は設定できません。

- データ転送用 VLAN に使用されている VLAN
- 異なるリングで使用されている VLAN ID と同じ値の VLAN ID
- デフォルト VLAN（VLAN ＝ 1）

[コマンドによる設定]

1. **(config)# axrp 1**
   リング ID 1 の axrp コンフィグレーションモードに移行します。
2. **(config-axrp)# control-vlan 2**
   制御 VLAN として VLAN2 を指定します。

(2)　制御 VLAN のフォワーディング遷移時間の設定

[設定のポイント]

Ring Protocol が初期状態の場合に，トランジットノードでの制御 VLAN のフォワーディング遷移時間を設定します。トランジットノードでの制御 VLAN のフォワーディング遷移時間（forwarding-delay-time パラメータでの設定値）は，マスタノードでのヘルスチェックフレームの保護時間よりも大きな値を設定してください。また，フラッシュ制御フレーム受信待ち保護時間（コンフィグレーションコマンド forwarding-shift-time での設定値）よりも小さな値を設定してください。設定誤りからマスタノードが復旧を検出するよりも先にトランジットノードのリングポートがフォワーディング状態となった場合，一時的にループが発生するおそれがあります。

[コマンドによる設定]

1. **(config)# axrp 1**
   (config-axrp)# control-vlan 2 forwarding-delay-time 10
   制御 VLAN のフォワーディング遷移時間を 10 秒に設定します。

28.1.5　VLAN マッピングの設定

(1)　VLAN 新規設定

[設定のポイント]

データ転送用に使用する VLAN を VLAN マッピングに括り付けます。一つの VLAN マッピングを共通定義として複数のリングで使用できます。設定できる VLAN マッピングの最大数は 128 個です。VLAN マッピングに設定する VLAN はリストで複数指定できます。

リングネットワーク内で使用するデータ転送用 VLAN は，すべてのノードで同じにする必要があります。ただし，VLAN グループに指定した VLAN マッピングの VLAN が一致していればよいため，リングネットワーク内のすべてのノードで VLAN マッピング ID を一致させる必要はありません。

[コマンドによる設定]

1. **(config)# axrp vlan-mapping 1 vlan 5-7**

VLAN マッピング ID 1 に，VLAN ID 5，6，7 を設定します。

(2)　VLAN 追加

[設定のポイント]

設定済みの VLAN マッピングに対して，VLAN ID を追加します。追加した VLAN マッピングを適用したリングが動作中の場合には，すぐに反映されます。また，複数のリングで適用されている場合には，同時に反映されます。リング運用中に VLAN マッピングを変更すると，ループが発生することがあります。

[コマンドによる設定]

1. **(config)# axrp vlan-mapping 1 vlan add 8-10**

   VLAN マッピング ID 1 に VLAN ID 8，9，10 を追加します。

(3)　VLAN 削除

[設定のポイント]

設定済みの VLAN マッピングから，VLAN ID を削除します。削除した VLAN マッピングを適用したリングが動作中の場合には，すぐに反映されます。また，複数のリングで適用されている場合には，同時に反映されます。リング運用中に VLAN マッピングを変更すると，ループが発生することがあります。

[コマンドによる設定]

1. **(config)# axrp vlan-mapping 1 vlan remove 8-9**

   VLAN マッピング ID 1 から VLAN ID 8，9 を削除します。

28.1.6　VLAN グループの設定

[設定のポイント]

VLAN グループに VLAN マッピングを割り当てることによって，VLAN ID を Ring Protocol で使用する VLAN グループに所属させます。VLAN グループは一つのリングに最大二つ設定できます。
VLAN グループには，リスト指定によって最大 128 個の VLAN マッピング ID を設定できます。

[コマンドによる設定]

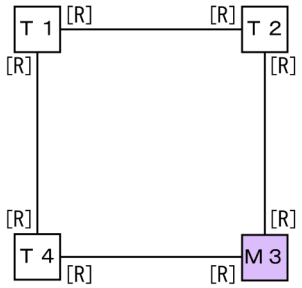
1. **(config)# axrp 1**
   (config-axrp)# vlan-group 1 vlan-mapping 1

   VLAN グループ 1 に，VLAN マッピング ID 1 を設定します。

28.1.7　モードとリングポートに関する設定（シングルリングと共有リンクなしマルチリング構成）

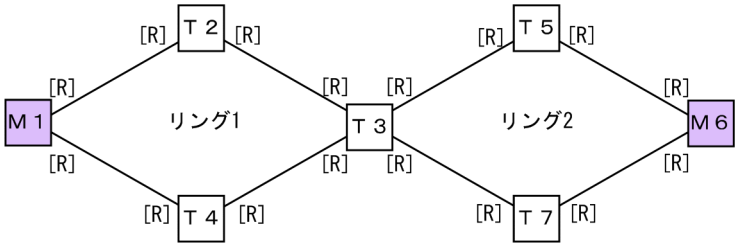
シングルリング構成を「図 28-1　シングルリング構成」に，共有リンクなしマルチリング構成を「図 28-2　共有リンクなしマルチリング構成」に示します。

図 28-1　シングルリング構成



（凡例）　M：マスタノード　　T：トランジットノード
　　[R]：リングポート

図 28-2　共有リンクなしマルチリング構成



（凡例）　M：マスタノード　　T：トランジットノード
　　[R]：リングポート

本装置はトランジットノードだけをサポートしています。本マニュアルでは，本装置のトランジットノードについて説明します。マスタノードについては，マスタノードの装置のマニュアルを参照してください。

(1)　トランジットノード

[設定のポイント]

リングでの本装置の動作モードをトランジットモードに設定します。イーサネットインタフェースまたはポートチャネルインタフェースをリングポートとして指定します。リングポートは一つのリングに対して二つ設定してください。「図 28-1　シングルリング構成」では T1，T2 および T4 ノード，「図 28-2　共有リンクなしマルチリング構成」では T2，T3，T4，T5 および T7 ノードがこれに該当します。

[コマンドによる設定]

1. **(config)# axrp 2**
   (config-axrp)# mode transit
   リング ID 2 の動作モードをトランジットモードに設定します。
2. **(config)# interface gigabitethernet 1/0/1**
   (config-if)# axrp-ring-port 2
   (config-if)# exit
   (config)# interface gigabitethernet 1/0/2
   (config-if)# axrp-ring-port 2

ポート 1/0/1 および 1/0/2 のインタフェースモードに移行し，該当するインタフェースをリング ID 2 のリングポートとして設定します。

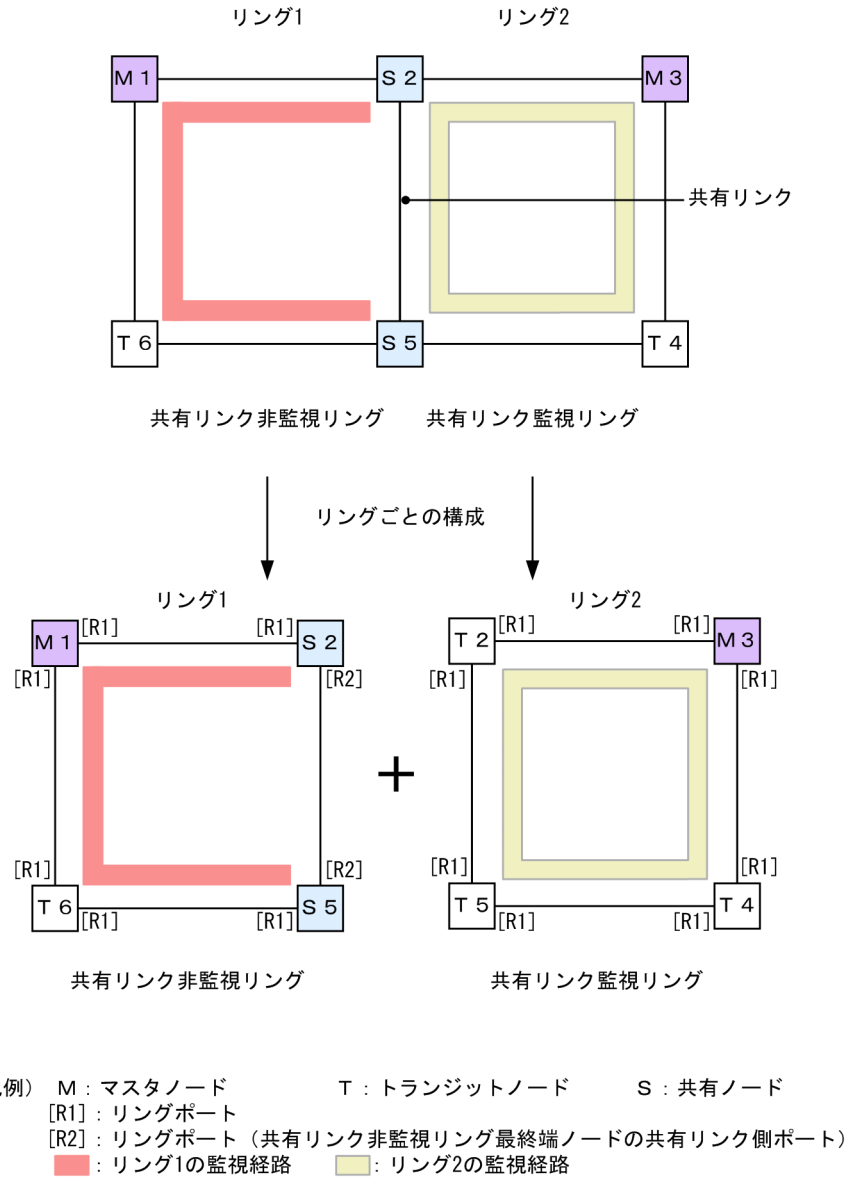
28.1.8　モードとリングポートに関する設定（共有リンクありマルチリング構成）

共有リンクありマルチリング構成について，モードとリングポートのパラメータ設定パターンを示します。

(1)　共有リンクありマルチリング構成（基本構成）

共有リンクありマルチリング構成（基本構成）を次の図に示します。

図 28-3　共有リンクありマルチリング構成（基本構成）



（凡例）　M：マスタノード　　T：トランジットノード　　S：共有ノード
[R1]：リングポート
[R2]：リングポート（共有リンク非監視リング最終端ノードの共有リンク側ポート）
：リング1の監視経路　　：リング2の監視経路

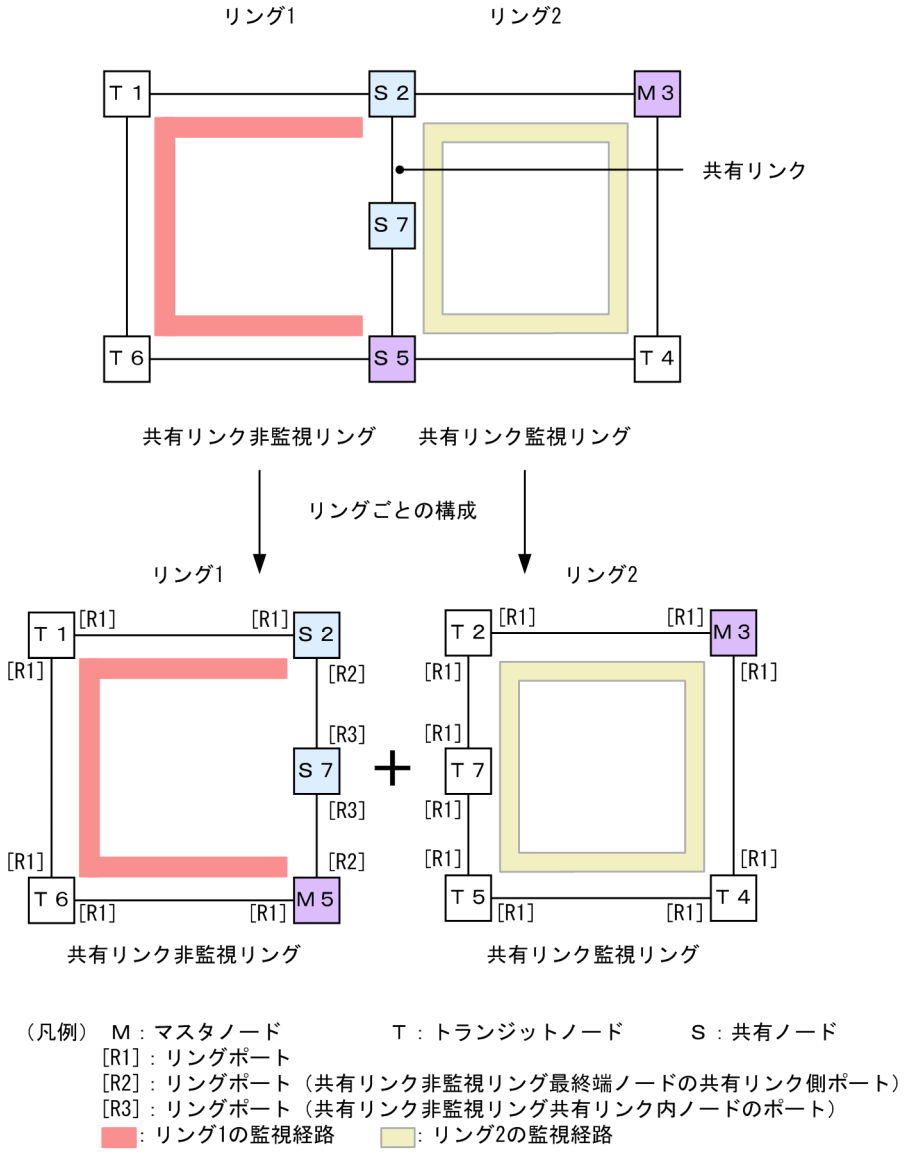
(a)　共有リンク監視リングのトランジットノード

シングルリングのトランジットノード設定と同様です。「28.1.7　モードとリングポートに関する設定（シングルリングと共有リンクなしマルチリング構成）(1)　トランジットノード」を参照してください。「図 28-3　共有リンクありマルチリング構成（基本構成）」では T2，T4 および T5 ノードがこれに該当します。

(2)　共有リンクありのマルチリング構成（拡張構成）

共有リンクありマルチリング構成（拡張構成）を次の図に示します。共有リンク非監視リングの最終端ノード（マスタノード）および共有リンク非監視リングの共有リンク内ノード（トランジット）以外の設定については，「(1)　共有リンクありマルチリング構成（基本構成）」を参照してください。

図 28-4　共有リンクありのマルチリング構成（拡張構成）



（凡例）　M：マスタノード　　T：トランジットノード　　S：共有ノード
[R1]：リングポート
[R2]：リングポート（共有リンク非監視リング最終端ノードの共有リンク側ポート）
[R3]：リングポート（共有リンク非監視リング共有リンク内ノードのポート）
：リング1の監視経路　　：リング2の監視経路

(a)　共有リンク非監視リングの共有リンク内ノード（トランジット）

[設定のポイント]

リングでの本装置の動作モードをトランジットモードに設定します。「図 28-4　共有リンクありのマルチリング構成（拡張構成）」では S7 ノードがこれに該当します。リングポートは両ポート共に shared パラメータを指定し，共有ポートとして設定します。「図 28-4　共有リンクありのマルチリング構成（拡張構成）」では S7 ノードのリングポート[R3]がこれに該当します。

[コマンドによる設定]

1. **(config)# axrp 1**
   (config-axrp)# mode transit
   リング ID 1 の動作モードをトランジットモードに設定します。
2. **(config)# interface gigabitethernet 1/0/1**
   (config-if)# axrp-ring-port 1 shared
   (config-if)# exit
   (config)# interface gigabitethernet 1/0/2
   (config-if)# axrp-ring-port 1 shared
   ポート 1/0/1 および 1/0/2 のインタフェースモードに移行し，該当するインタフェースをリング ID 1 の共有リンクポートに設定します。

28.1.9　各種パラメータの設定

(1)　Ring Protocol 機能の無効

[設定のポイント]

コマンドを指定して Ring Protocol 機能を無効にします。ただし，運用中に Ring Protocol 機能を無効にすると，ネットワークの構成上，ループが発生するおそれがあります。このため，先に Ring Protocol 機能を動作させているインタフェースを shutdown コマンドなどで停止させてから，Ring Protocol 機能を無効にしてください。

[コマンドによる設定]

1. **(config)# axrp 1**
   (config-axrp)# disable
   該当するリング ID 1 の axrp コンフィグレーションモードに移行します。disable コマンドを実行することで，Ring Protocol 機能が無効となります。

(2)　フラッシュ制御フレーム受信待ち保護時間

[設定のポイント]

トランジットノードでのフラッシュ制御フレームの受信待ち保護時間を設定します。それ以外のノードでは，本設定を実施しても，無効となります。トランジットノードでのフラッシュ制御フレームの受信待ちの保護時間（forwarding-shift-time コマンドでの設定値）は，マスタノードでのヘルスチェックフレームの送信間隔（health-check interval コマンドでの設定値）よりも大きい値を設定してください。設定誤りからマスタノードが復旧を検出するよりも先にトランジットノードのリングポートがフォワーディング状態になってしまった場合，一時的にループが発生するおそれがあります。

[コマンドによる設定]

1. (config)# axrp 1
   (config-axrp)# forwarding-shift-time 100
   フラッシュ制御フレームの受信待ちの保護時間を 100 秒に設定します。

28.1.10　多重障害監視機能の設定

(1)　多重障害監視 VLAN の設定

[設定のポイント]

共有リンク監視リングの各ノードに多重障害監視 VLAN として使用する VLAN を設定します。なお，制御 VLAN とデータ転送用 VLAN に使われている VLAN は使用できません。また，異なるリングで使用されている多重障害監視 VLAN の VLAN ID と同じ値の VLAN ID は使用できません。

[コマンドによる設定]

1. (config)# axrp 1
   リング ID 1 の axrp コンフィグレーションモードに移行します。
2. (config-axrp)# multi-fault-detection vlan 20
   多重障害監視 VLAN として VLAN 20 を設定します。

[注意事項]

多重障害監視 VLAN は多重障害監視機能を適用する共有リンク監視リングのすべてのノードに設定してください。

(2)　多重障害監視機能の監視モードの設定

[設定のポイント]

本装置の監視モードに transport-only を設定します（本装置は transport-only だけをサポートしています）。

[コマンドによる設定]

1. (config)# axrp 1
   リング ID 1 の axrp コンフィグレーションモードに移行します。
2. (config-axrp)# multi-fault-detection mode transport-only
   多重障害監視の監視モードを transport-only に設定します。

29 IGMP snooping/MLD snooping の解説

IGMP snooping/MLD snooping はレイヤ 2 スイッチで VLAN 内のマルチキャストトラフィックを制御する機能です。この章では，IGMP snooping/MLD snooping について説明します。

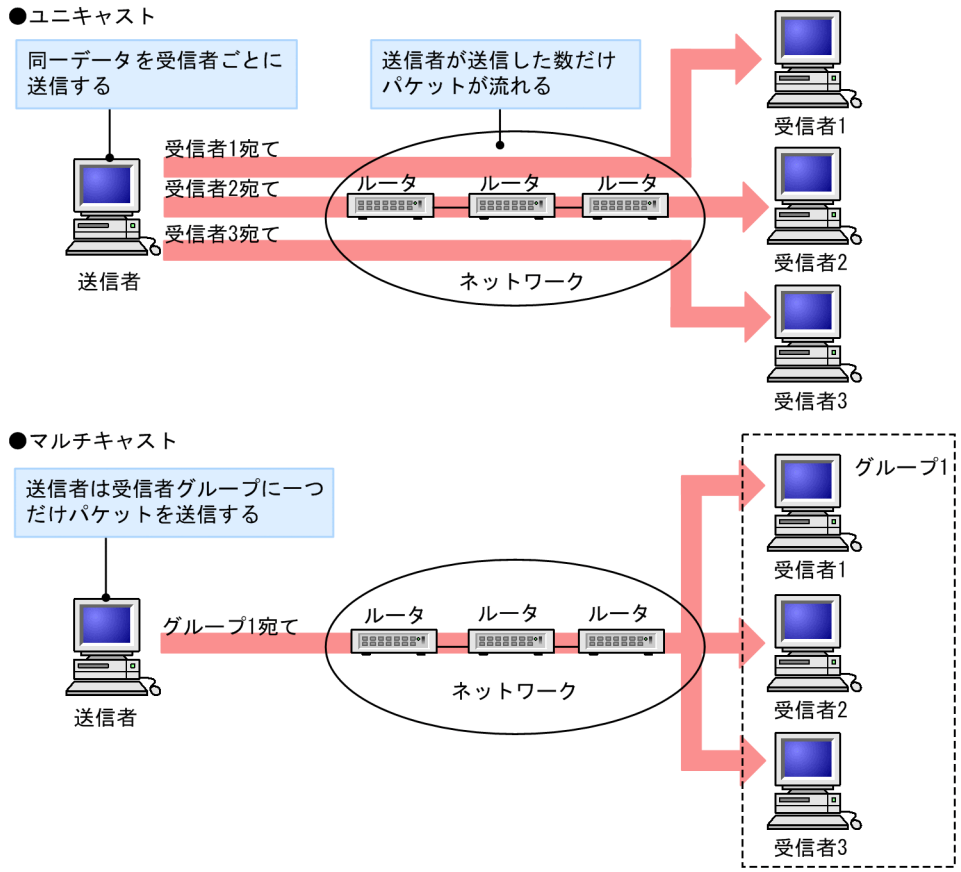
29.1　IGMP snooping/MLD snooping の概要

この節では，マルチキャスト，IGMP snooping および MLD snooping の概要について説明します。

29.1.1　マルチキャスト概要

同一の情報を複数の受信者に送信する場合，ユニキャストでは送信者が受信者の数だけデータを複製して送信するため，送信者とネットワークの負荷が高くなります。マルチキャストでは送信者がネットワーク内で選択されたグループに対してデータを送信します。送信者は受信者ごとにデータを複製する必要がないため，受信者の数に関係なくネットワークの負荷を軽減できます。マルチキャスト概要を次の図に示します。

図 29-1　マルチキャスト概要



マルチキャストで送信する場合に，宛先アドレスにはマルチキャストグループアドレスを使用します。マルチキャストグループアドレスを次の表に示します。

表 29-1　マルチキャストグループアドレス

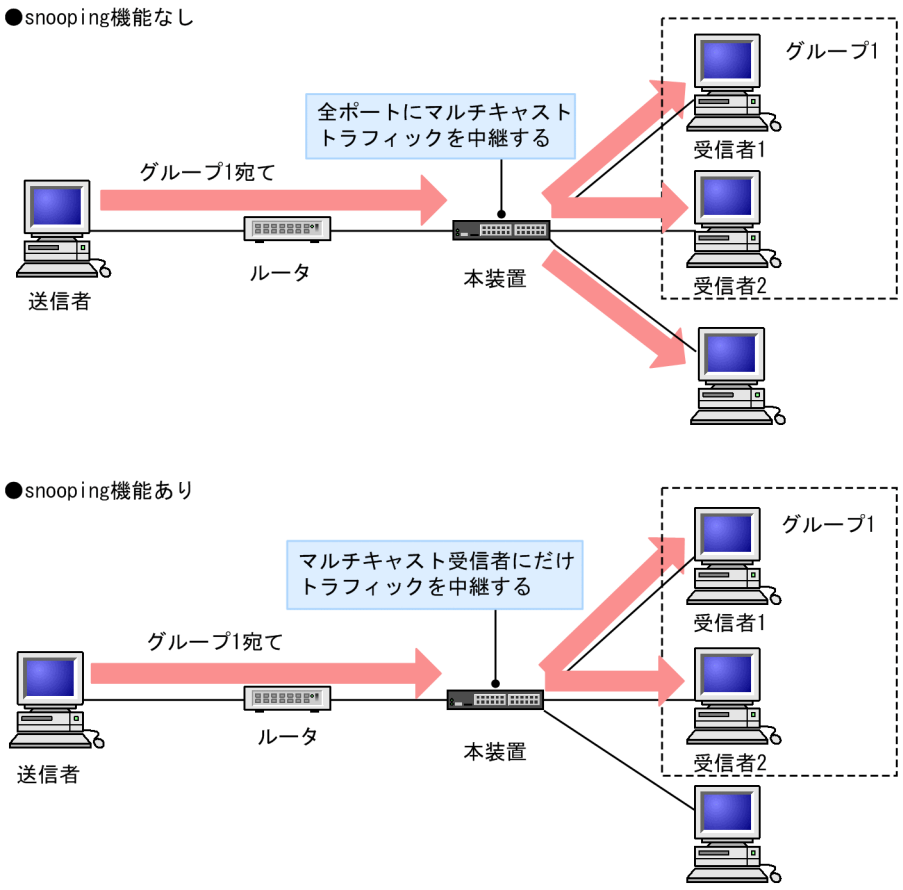
プロトコル	アドレス範囲
IPv4	224.0.0.0～239.255.255.255
IPv6	上位 8 ビットが ff(16 進数)となる IPv6 アドレス

29.1.2　IGMP snooping および MLD snooping 概要

レイヤ 2 スイッチはマルチキャストトラフィックを VLAN 内の全ポートに中継します。そのため，レイヤ 2 スイッチが接続されているネットワークでマルチキャストを使用すると，マルチキャストトラフィックの受信者がいないポートに不要なマルチキャストトラフィックが流れることになります。

IGMP snooping および MLD snooping は，IGMP あるいは MLD メッセージを監視して，受信者が接続しているポートに対してマルチキャストトラフィックを中継します。この機能を利用することで，不要なマルチキャストトラフィックの中継を抑止し，ネットワークを効率的に利用することができます。IGMP snooping/MLD snooping 概要を次の図に示します。

図 29-2　IGMP snooping/MLD snooping 概要



マルチキャストトラフィックの受信者が接続するポートを検出するため，本装置はグループ管理プロトコルのパケットを監視します。グループ管理プロトコルは，ルータホスト間でグループメンバーシップ情報を送受信するプロトコルで，IPv4 ネットワークでは IGMP が使用され，IPv6 ネットワークでは MLD が使用されます。ホストから送信されるグループ参加・離脱報告を示すパケットを検出することで，どの接続ポートへマルチキャストトラフィックを中継すべきかを学習します。

29.2　IGMP snooping/MLD snooping サポート機能

本装置がサポートする IGMP snooping/MLD snooping 機能を次の表に示します。

表 29-2　サポート機能

項 目		サポート内容	備考
インタフェース種別		全イーサネットをサポート フレーム形式は Ethernet V2 だけ	－
IGMP サポートバージョン MLD サポートバージョン		IGMP: Version 1，2，3 MLD: Version 1，2	－
この機能による学習 MAC アドレス範囲	IPv4	0100.5e00.0000 ～ 0100.5e7f.ffff	RFC1112 を参照
	IPv6	3333.0000.0000 ～ 3333.ffff.ffff	RFC2464 を参照
IGMP クエリア MLD クエリア		クエリア動作は IGMPv2/IGMPv3，MLDv1/MLDv2 の仕様に従う	－
マルチキャストルータ接続ポートの設定		コンフィグレーションによる static 設定	－
		マルチキャストルータ検知による自動設定	IGMP snooping だけ
IGMP 即時離脱機能		IGMPv2 Leave メッセージ，またはマルチキャストアドレスレコードタイプが CHANGE_TO_INCLUDE_MODE の IGMPv3 Report（離脱要求）メッセージの受信による即時離脱	－

（凡例）　－：該当なし

29.3　IGMP snooping

ここでは，IGMP snooping の機能と動作について説明します。本装置が送受信する IGMP メッセージのフォーマットおよびタイマは RFC2236 に従います。また，IGMP バージョン 3（以降，IGMPv3）メッセージのフォーマットおよび設定値は RFC3376 に従います。

29.3.1　MAC アドレスの学習

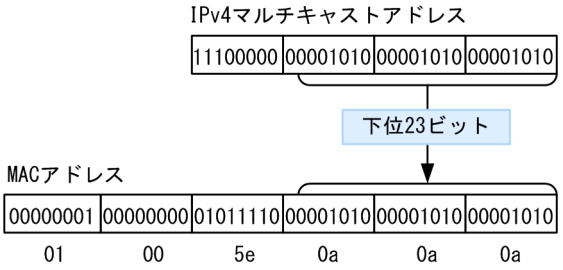
IGMP snooping が設定された VLAN で IGMP メッセージを受信することによってマルチキャスト MAC アドレスをダイナミックに学習します。学習したマルチキャスト MAC アドレスは MAC アドレステーブルに登録します。

(1)　エントリの登録

IGMPv1/IGMPv2 Report メッセージおよび，IGMPv3 Report（加入要求）メッセージを受信すると，メッセージに含まれるマルチキャストグループアドレスからマルチキャスト MAC アドレスを学習し，IGMPv1/IGMPv2/IGMPv3 Report メッセージを受信したポートにだけマルチキャストグループ宛てのトラフィックを転送するエントリを作成します。

IPv4 マルチキャストデータの宛先 MAC アドレスは IP アドレスの下位 23 ビットを MAC アドレスにコピーして生成します。そのため，下位 23 ビットが同じ IP アドレスは MAC アドレスが重複します。例えば，224.10.10.10 と 225.10.10.10 はどちらもマルチキャスト MAC アドレスは 0100.5E0A.0A0A となります。これらのアドレスについては，レイヤ 2 中継で同一 MAC アドレス宛てのパケットとして取り扱います。IPv4 マルチキャストアドレスと MAC アドレスの対応を次の図に示します。

図 29-3　IPv4 マルチキャストアドレスと MAC アドレスの対応



(2)　エントリの削除

学習したマルチキャスト MAC アドレスは次のどちらかの場合に，すべてのポートにグループメンバーが存在しなくなった時点で削除されます。

- IGMPv2 Leave メッセージを受信した場合

  IGMPv2 Leave メッセージを受信したポートに対して，本装置から Group-Specific Query メッセージを 1 秒間隔で 2 回送信します（Group-Specific Query メッセージの送信は，クエリア設定時だけです。未設定時は代表クエリアから送信されます）。応答がない場合にエントリからこのポートだけを削除します（このポートへのマルチキャストトラフィックの中継を抑止します）。VLAN 内のすべてのポートにグループメンバーが存在しなくなった場合にエントリ自体を削除します。

  IGMP 即時離脱機能を使用している場合は，IGMPv2 Leave メッセージを受信すると，エントリから該当ポートをすぐに削除します。クエリアを設定していても，Group-Specific Query メッセージは送信しません。

- IGMPv3 Report（離脱要求）メッセージを受信した場合

IGMPv3 Report（離脱要求）メッセージを受信したポートに対して，本装置から Group-Specific Query メッセージを 1 秒間隔で 2 回送信します（Group-Specific Query メッセージの送信は，クエリア設定時だけです。未設定時は代表クエリアから送信されます）。応答がない場合にエントリからこのポートだけを削除します（このポートへのマルチキャストトラフィックの中継を抑止します）。VLAN 内のすべてのポートにグループメンバーが存在しなくなった場合にエントリ自体を削除します。ただし，マルチキャストアドレスレコードタイプが BLOCK_OLD_SOURCES の IGMPv3 Report メッセージを受信した場合は，自装置へのクエリア設定を行っている場合だけ Group-Specific Query メッセージの送信および，エントリ削除処理を実行します。

IGMP 即時離脱機能を使用している場合は，マルチキャストアドレスレコードタイプが CHANGE_TO_INCLUDE_MODE の IGMPv3 Report（離脱要求）メッセージを受信すると，エントリから該当ポートをすぐに削除します。クエリアを設定していても，Group-Specific Query メッセージは送信しません。

- IGMPv1/IGMPv2/IGMPv3 Report（加入要求）メッセージを受信してから一定時間経過した場合

  マルチキャストルータは直接接続するインタフェース上にグループメンバーが存在するかを確認するため，定期的に Query メッセージを送信します。本装置はルータからの IGMP Query メッセージを受信した場合，VLAN 内の全ポートに中継します。IGMP Query メッセージに対する応答がない場合，エントリからこのポートだけを削除します。すべてのポートから応答がない場合は，エントリ自体を削除します。

  本装置では Group Membership Interval 時間，IGMPv1/IGMPv2/IGMPv3 Report（加入要求）メッセージを受信しない場合，対応するエントリを削除します。

  注

  Group Membership Interval は，Robustness Variable（RV）×Query Interval（QI）＋ Query Response Interval（QRI）で算出します。

  RV，QI，QRI の値を次に示します。

  ・他装置が代表クエリアで IGMPv3 で運用している場合

  RV，QI=受信した Query メッセージから取得

  QRI=10 秒

  ・自装置が代表クエリアで IGMPv3 で運用している場合，または IGMPv2 で運用している場合

  RV=2

  QI=コンフィグレーションコマンド ip igmp snooping query-interval で指定した時間

  QRI=10 秒

29.3.2　IPv4 マルチキャストパケットのレイヤ 2 中継

IPv4 マルチキャストパケットの受信 VLAN 内のレイヤ 2 中継は MAC アドレスベースで処理します。IGMP snooping の結果によるレイヤ 2 中継は，同一 MAC アドレスにマッピングされる IP マルチキャストアドレスの IGMP Report（加入要求）メッセージを受信したポートすべてに中継します。

「29.3.1　MAC アドレスの学習　(1)　エントリの登録」の例で述べた 224.10.10.10 と 225.10.10.10 のマルチキャスト MAC アドレスはどちらも 0100.5E0A.0A0A となるので，224.10.10.10 宛てのマルチキャストデータをレイヤ 2 中継する際に，225.10.10.10 への IGMP Report（加入要求）メッセージを受信したポートへも中継します。

29.3.3　マルチキャストルータとの接続

(1)　マルチキャストルータポートの設定

マルチキャストパケットは受信者だけでなく隣接するマルチキャストルータにも中継する必要があります。そのため，本装置とマルチキャストルータを接続して IGMP snooping を使用する場合，マルチキャストパケットをマルチキャストルータに中継するために，マルチキャストルータと接続するポート（以降，マルチキャストルータポートとします）を設定します。

本装置のマルチキャストルータポートの設定方法には，次に示す二つがあります。

- コンフィグレーションでマルチキャストルータポートを設定
- マルチキャストルータを検知したポートをマルチキャストルータポートに自動設定

どちらで設定した場合も，マルチキャストルータポートとしての動作は同じです。また，同一のポートまたはチャネルグループに対して，コンフィグレーションでの設定および自動設定を併用できます。

(2)　マルチキャストルータポートの自動学習

コンフィグレーションコマンド ip igmp snooping mrouter discovery を設定した VLAN で，監視対象のパケット受信によりマルチキャストルータを検知します。マルチキャストルータを検知したポートまたはチャネルグループは，マルチキャストルータポートに自動設定します。

(a)　監視対象パケット

マルチキャストルータを検知するための監視対象パケットを次の表に示します。

表 29-3　監視対象パケット

監視対象パケット※	検知対象マルチキャストルータ
IGMPv1 Membership Query メッセージ	IGMPv1 対応マルチキャストルータ
IGMPv2 General Query メッセージ	IGMPv2 対応マルチキャストルータ
IGMPv3 General Query メッセージ	IGMPv3 対応マルチキャストルータ
IPv4 PIM-Hello メッセージ	PIM 対応マルチキャストルータ

注※
フラグメント化されたメッセージは監視対象外です。

(b)　マルチキャストルータポートの保持時間

自動設定したマルチキャストルータポートの保持時間は，監視対象により異なります。

マルチキャストルータポートの保持時間を次の表に示します。

表 29-4　マルチキャストルータの保持時間

監視対象パケット	保持時間
IGMPv1 Membership Query	Robustness Variable※1×Query Interval※2＋

監視対象パケット	保持時間
メッセージ	Query Response Interval※3 /2+X※4
IGMPv2 General Query メッセージ	
IGMPv3 General Query メッセージ※5	Robustness Variable×Query Interval+ Query Response Interval/2+X※4
IPv4 PIM-Hello メッセージ	受信した PIM-Hello メッセージの Holdtime オプションの値。 Holdtime オプションが存在しない場合は 105 秒。

注※1

Robustness Variable は 2 固定。

注※2

デフォルト値は 125 秒。コンフィグレーションコマンド ip igmp snooping query-interval を設定した場合は，該当コマンドで指定した値。

注※3

デフォルト値は 10 秒。Query Interval が 10 秒以下の場合は，Query Interval の値。

注※4

コンフィグレーションコマンド ip igmp snooping mrouter discovery extension で指定した時間。

注※5

IGMPv3 Query メッセージの場合，Robustness Variable，Query Interval は，受信した Query メッセージから取得。Query Response Interval は 10 秒固定。

(c) マルチキャストルータポートの削除

自動設定したマルチキャスルータルータポートは，保持時間中に該当ポートまたはチャネルグループで再度マルチキャストルータを検知しなければ，保持時間満了となり，自動的に削除します。

保持時間満了以外で自動設定したマルチキャストルータポートを削除する条件と削除対象を次に示します。

- 運用コマンド clear igmp-snooping all を実行した場合
  すべての VLAN の自動設定したすべてのマルチキャストルータポートを削除します。
- 運用コマンド clear igmp-snooping mrouter を実行した場合
  該当 VLAN の自動設定したすべてのマルチキャストルータポートを削除します。
- VLAN で IGMP snooping を無効にした場合
  該当 VLAN の自動設定したすべてのマルチキャストルータポートを削除します。
- コンフィグレーションコマンド ip igmp snooping mrouter discovery igmp を削除した場合
  該当 VLAN の IGMP 監視で自動設定したすべてのマルチキャストルータポートを削除します。
- コンフィグレーションコマンド ip igmp snooping mrouter discovery pim を削除した場合
  該当 VLAN の PIM 監視で自動設定したすべてのマルチキャストルータポートを削除します。
- ポートまたはチャネルグループを VLAN から削除した場合
  すべての VLAN の該当ポートまたは該当チャネルグループで自動設定したマルチキャストルータポートを削除します。
- ポートをチャネルグループに追加した際に，該当ポートをマルチキャストルータポートに自動設定している場合
  すべての VLAN の該当ポートで自動設定したマルチキャストルータポートを削除します。

また，次に示す場合は削除しません。

- 該当ポートまたはチャネルグループがリンクダウンした場合
- 該当ポートまたはチャネルグループがスパニングツリーなどで Blocking 状態になった場合

(d)　運用メッセージの出力と抑止

本機能ではマルチキャストルータの検知に関する運用メッセージを出力します。運用メッセージの出力を抑止する場合は，コンフィグレーションコマンド no ip igmp snooping mrouter logging を設定してください。

(3)　IGMP メッセージの中継

IGMP はマルチキャストルータと受信者間で送受信するプロトコルであるため，IGMP メッセージはマルチキャストルータおよび受信者が受け取ります。本装置は IGMP メッセージを次の表に示すように中継します。

表 29-5　IGMPv1/IGMPv2 メッセージごとの動作

IGMP メッセージの種類	VLAN 内転送ポート	備考
Membership Query	全ポートへ中継します。	
Version 2 Membership Report	マルチキャストルータポートにだけ中継します。	
Leave Group	ほかのポートにまだグループメンバーが存在する場合はどのポートにも中継しません。 ほかのポートにグループメンバーが存在しない場合はマルチキャストルータポートに中継します。	※
Version 1 Membership Report	マルチキャストルータポートにだけ中継します。	

注※

自装置にクエリアを設定し，他装置が代表クエリアの場合の中継動作です。自装置が代表クエリアの場合は，IGMPv2 Leave メッセージは中継しません。クエリアを設定していない場合は，常にマルチキャストルータポートに中継します。ただし，IGMPv1/IGMPv2/IGMPv3 Report（加入要求）メッセージを受信していないポートで IGMPv2 Leave メッセージを受信した場合，クエリアの設定にかかわらず IGMPv2 Leave メッセージは中継しません。

表 29-6　IGMPv3 メッセージごとの動作

IGMPv3 メッセージの種類		VLAN 内転送ポート	備考
Version3 Membership Query		全ポートへ中継します。	
Version 3 Membership Report	加入要求の Report	マルチキャストルータポートにだけ中継します。	
	離脱要求の Report	ほかのポートにまだグループメンバーが存在する場合はどのポートにも中継しません。ほかのポートにグループメンバーが存在しない場合はマルチキャストルータポートに中継します。	※

注※

自装置にクエリアを設定し，他装置が代表クエリアの場合の中継動作です。自装置が代表クエリアの場合は，IGMPv3 Report（離脱要求）メッセージは中継しません。クエリアを設定していない場合は，常にマルチキャストルータポートに中継します。ただし，IGMPv1/IGMPv2/IGMPv3 Report（加入要求）メッセージを受信していな

いポートで離脱要求の IGMPv3 Report メッセージを受信した場合，クエリアの設定にかかわらず IGMPv3 Report（離脱要求）メッセージは中継しません。

29.3.4　IGMP クエリア機能

IGMP クエリア機能は，VLAN 内にマルチキャストルータが存在せず，マルチキャストパケットの送信ホストと受信ホストだけが存在する環境で，本装置が IGMP Query メッセージを代理で受信ホストに対して送信する機能です。マルチキャストルータは定期的に IGMP Query メッセージを送信し，ホストからの応答を受け取ることでグループメンバーの存在有無を確認します。マルチキャストルータが存在しない場合，受信ホストからの応答がなくなるためにグループメンバーを監視することができなくなります。この機能によって，VLAN 内にマルチキャストルータが存在しない場合でも，IGMP snooping 機能を使用可能とします。本装置では，コンフィグレーションコマンド ip igmp snooping query-interval で指定した送信間隔で，IGMP Query メッセージを送信します。

注

IGMPv2 で運用する場合，該当する VLAN では Query Interval を統一してください。

IGMP クエリア機能を利用するためには，IGMP snooping 機能を利用する VLAN に IP アドレスを設定する必要があります。

VLAN 内に IGMP Query メッセージを送信する装置が存在する場合，IGMP Query メッセージの送信元 IP アドレスの小さい方が代表クエリアとなって IGMP Query メッセージを送信します。VLAN 内のほかの装置が代表クエリアの場合，本装置は IGMP クエリア機能による Query メッセージの送信を停止します。

代表クエリアが障害などで停止すると新たに代表クエリアを選定します。VLAN 内の他装置が障害などで本装置が代表クエリアに決定すると Query メッセージの送信を開始します。本装置では代表クエリアの監視時間は，Other Querier Present Interval に従います。

注

Other Querier Present Interval は，Robustness Variable（RV）×Query Interval（QI）＋ Query Response Interval（QRI）/2 で算出します。

RV，QI，QRI の値を次に示します。

・他装置が代表クエリアで IGMPv3 で運用している場合

RV，QI=受信した Query メッセージから取得

QRI=10 秒

・本装置が代表クエリアで IGMPv3 で運用している場合，または IGMPv2 で運用している場合

RV=2

QI=コンフィグレーションコマンド ip igmp snooping query-interval で指定した時間

QRI=10 秒

本装置で送信する IGMP Query のバージョンは，IGMPv2 をデフォルト値としています。装置起動以降，IGMP Query のバージョンは，代表クエリアの IGMP バージョンに従います。

29.3.5　IGMP 即時離脱機能

IGMP 即時離脱機能は，IGMPv2 Leave および IGMPv3 Report（離脱要求）メッセージを受信した場合に，該当ポートへのマルチキャスト通信をすぐに停止する機能です。

IGMPv3 Report（離脱要求）メッセージでは，マルチキャストアドレスレコードタイプが CHANGE_TO_INCLUDE_MODE の IGMPv3 Report（離脱要求）メッセージだけを，本機能のサポート対象とします。

29.4　MLD snooping

ここでは，MLD snooping の機能と動作について説明します。本装置が送受信する MLD メッセージのフォーマットおよび既定値は RFC2710 に従います。また，MLD バージョン 2（以降，MLDv2）メッセージのフォーマットおよび設定値は RFC3810 に従います。

29.4.1　MAC アドレスの学習

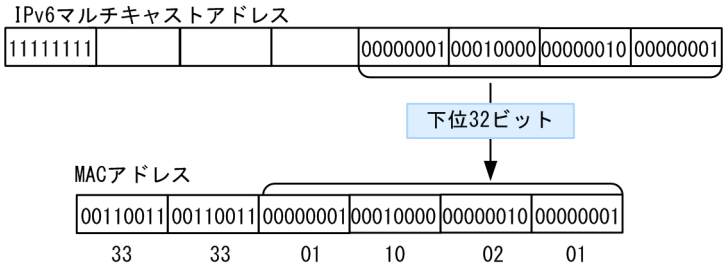
MLD snooping が設定された VLAN で MLD メッセージを受信することによってマルチキャスト MAC アドレスをダイナミックに学習します。学習したマルチキャスト MAC アドレスは MAC アドレステーブルに登録します。

(1)　エントリの登録

MLDv1 Report メッセージおよび，MLDv2 Report（加入要求）メッセージを受信すると，メッセージに含まれるマルチキャストグループアドレスからマルチキャスト MAC アドレスを学習し，MLDv1/MLDv2 Report メッセージを受信したポートにだけマルチキャストグループ宛てのトラフィックを転送するエントリを作成します。IPv6 マルチキャストデータの宛先 MAC アドレスは IP アドレスの下位 32 ビットを MAC アドレスにコピーして生成します。

IPv6 マルチキャストアドレスはマルチキャストグループを識別するグループ ID フィールドが 112 ビット長のフォーマットと 32 ビット長のフォーマットの 2 種類が規定されています。グループ ID フィールドが 112 ビット長のアドレスフォーマットを使用する場合は，IPv4 マルチキャストアドレスと同様に MAC アドレスの重複が発生します。IPv6 マルチキャストアドレスと MAC アドレスの対応を次の図に示します。

図 29–4　IPv6 マルチキャストアドレスと MAC アドレスの対応



(2)　エントリの削除

学習したマルチキャスト MAC アドレスは次のどちらかの場合に，すべてのポートにグループメンバーが存在しなくなった時点で削除されます。

- MLDv1 Done メッセージを受信した場合

  MLDv1 Done メッセージを受信したポートに対して，本装置から Group-Specific Query メッセージを 1 秒間隔で 2 回送信します（Group-Specific Query メッセージの送信は，クエリア設定時だけです。未設定時は代表クエリアから送信されます）。応答がない場合にエントリからこのポートだけを削除します（このポートへのマルチキャストトラフィックの中継を抑止します）。VLAN 内のすべてのポートにグループメンバーが存在しなくなった場合にエントリ自体を削除します。

- MLDv2 Report（離脱要求）メッセージを受信した場合

  MLDv2 Report（離脱要求）メッセージを受信したポートに対して，本装置から Group-Specific Query メッセージを 1 秒間隔で 2 回送信します（Group-Specific Query メッセージの送信は，クエリア設定時だけです。未設定時は代表クエリアから送信されます）。応答がない場合にエントリからこのポート

だけを削除します（このポートへのマルチキャストトラフィックの中継を抑止します）。VLAN 内のすべてのポートにグループメンバーが存在しなくなった場合にエントリ自体を削除します。ただし，マルチキャストアドレスレコードタイプが BLOCK_OLD_SOURCES の MLDv2 Report メッセージを受信した場合は，自装置へのクエリア設定を行っている場合だけ Group-Specific Query メッセージの送信および，エントリ削除処理を実行します。

- MLDv1/MLDv2 Report（加入要求）メッセージを受信してから一定時間経過した場合

  マルチキャストルータは直接接続するインタフェース上にグループメンバーが存在するかを確認するために，定期的に MLD Query メッセージを送信します。本装置はルータからの MLD Query メッセージを受信した場合，VLAN 内の全ポートに中継します。MLD Query メッセージに対する応答がない場合，エントリからこのポートだけを削除します。すべてのポートから応答がない場合は，エントリ自体を削除します。

  本装置では Multicast Listener Interval 時間，MLDv1/MLDv2 Report（加入要求）メッセージを受信しない場合，対応するエントリを削除します。

  注

  Multicast Listener Interval は，Robustness Variable（RV）×Query Interval（QI）＋ Query Response Interval（QRI）で算出します。

  RV，QI，QRI の値を次に示します。

  ・他装置が代表クエリアで MLDv2 で運用している場合

  RV，QI=受信した Query メッセージから取得

  QRI=10 秒

  ・本装置が代表クエリアで MLDv2 で運用している場合，または MLDv1 で運用している場合

  RV=2

  QI=125 秒

  QRI=10 秒

29.4.2　IPv6 マルチキャストパケットのレイヤ 2 中継

IPv6 マルチキャストパケットの受信 VLAN 内のレイヤ 2 中継は IPv4 マルチキャストパケット同様に MAC アドレスベースで処理します。MLD snooping の結果によるレイヤ 2 中継は，同一 MAC アドレスにマッピングされる IPv6 マルチキャストアドレスの MLD Report（加入要求）メッセージを受信したポートすべてに中継します。

29.4.3　マルチキャストルータとの接続

(1)　マルチキャストルータポートの設定

マルチキャストパケットは受信者だけでなく隣接するマルチキャストルータにも中継する必要があります。そのため，本装置とマルチキャストルータを接続して MLD snooping を使用する場合，マルチキャストパケットをマルチキャストルータに中継するために，マルチキャストルータと接続するポート（以降，マルチキャストルータポートとします）をコンフィグレーションで設定します。

(2)　MLD メッセージの中継

MLD はマルチキャストルータと受信者間で送受信するプロトコルであるため，MLD メッセージはマルチキャストルータおよび受信者が受け取ります。本装置は MLD メッセージを次の表に示すように中継します。

表 29-7　MLDv1 メッセージごとの動作

MLDv1 メッセージの種類	VLAN 内転送ポート	備考
Multicast Listener Query	全ポートへ中継します。	
Multicast Listener Report	マルチキャストルータポートにだけ中継します。	
Multicast Listener Done	ほかのポートにまだグループメンバーが存在する場合はどのポートにも中継しません。 ほかのポートにグループメンバーが存在しない場合はマルチキャストルータポートに中継します。	※

注※

自装置にクエリアを設定し，他装置が代表クエリアの場合の中継動作です。自装置が代表クエリアの場合は，MLDv1 Done メッセージは中継しません。クエリアを設定していない場合は，常にマルチキャストルータポートに中継します。ただし，MLDv1/MLDv2 Report（加入要求）メッセージを受信していないポートで MLDv1 Done メッセージを受信した場合，クエリアの設定にかかわらず MLDv1 Done メッセージは中継しません。

表 29-8　MLDv2 メッセージごとの動作

MLDv2 メッセージの種類		VLAN 内転送ポート	備考
Version2 Multicast Listener Query		全ポートへ中継します。	
Version2 Multicast Listener Report	加入要求の Report	マルチキャストルータポートにだけ中継します。	
	離脱要求の Report	ほかのポートにまだグループメンバーが存在する場合はどのポートにも中継しません。ほかのポートにグループメンバーが存在しない場合はマルチキャストルータポートに中継します。	※

注※

自装置にクエリアを設定し，他装置が代表クエリアの場合の中継動作です。自装置が代表クエリアの場合は，MLDv2 Report（離脱要求）メッセージは中継しません。クエリアを設定していない場合は，常にマルチキャストルータポートに中継します。ただし，MLDv1/MLDv2 Report（加入要求）メッセージを受信していないポートで離脱要求の MLDv2 Report メッセージを受信した場合，クエリアの設定にかかわらず MLDv2 Report（離脱要求）メッセージは中継しません。

29.4.4　MLD クエリア機能

MLD クエリア機能とは，VLAN 内にマルチキャストルータが存在せず，マルチキャストパケットの送信ホストと受信ホストだけが存在する環境で，本装置が MLD Query メッセージを代理で受信ホストに対して送信する機能です。マルチキャストルータは定期的に MLD Query メッセージを送信し，ホストからの応答を受け取ることでグループメンバーの存在有無を確認します。マルチキャストルータが存在しない場合，受信ホストからの応答がなくなるためにグループメンバーを監視することができなくなります。この機能によって，VLAN 内にマルチキャストルータが存在しない場合でも，MLD snooping 機能を使用可能とします。本装置では Query メッセージを 125 秒間隔で送信します。

注

MLDv1 で運用する場合，該当する VLAN では Query Interval を 125 秒で統一してください。

MLD クエリア機能を利用するためには，MLD snooping 機能を利用する VLAN に MLD Query メッセージの送信元 IP アドレスを設定する必要があります。

MLD クエリア機能で使用する IP アドレスの設定方法には，次に示す二つがあります。

- IPv6 インタフェースとして IP アドレスを設定
- コンフィグレーションコマンド ipv6 mld snooping querier で，MLD Query メッセージの送信元 IP アドレスを直接設定

両方を設定した場合は，IPv6 インタフェースとして設定した IP アドレスを優先します。

VLAN 内に MLD Query メッセージを送信する装置が存在する場合，MLD Query メッセージの送信元 IP アドレスの小さい方が代表クエリアとなって MLD Query メッセージを送信します。VLAN 内のほかの装置が代表クエリアの場合，本装置は MLD クエリア機能による MLD Query メッセージの送信を停止します。

代表クエリアが障害などで停止すると新たに代表クエリアを選定します。VLAN 内の他装置が障害などで本装置が代表クエリアに決定すると MLD Query メッセージの送信を開始します。本装置では代表クエリアの監視時間は，Other Querier Present Interval に従います。

注

Other Querier Present Interval は，Robustness Variable（RV）×Query Interval（QI）＋ Query Response Interval（QRI）/2 で算出します。

RV，QI，QRI の値を次に示します。

・他装置が代表クエリアで MLDv2 で運用している場合

RV，QI=受信した Query メッセージから取得

QRI=10 秒

・本装置が代表クエリアで MLDv2 で運用している場合，または MLDv1 で運用している場合

RV=2

QI=125 秒

QRI=10 秒

本装置で送信する MLD Query のバージョンは，MLDv1 をデフォルト値としています。装置起動以降，MLD Query のバージョンは，代表クエリアの MLD バージョンに従います。

29.5　IGMP snooping/MLD snooping 使用時の注意事項

(1)　他機能との共存

「22.3　レイヤ 2 スイッチ機能と他機能の共存について」を参照してください。

(2)　制御パケットのフラッディング

IGMP snooping/MLD snooping が抑止対象とするマルチキャストトラフィックはデータトラフィックであり，ルーティングプロトコルなどの制御パケットは VLAN 内の全ルータや全ホストが受信できるように VLAN 内に flooding する必要があります。そのため，本装置では，次の表に示すアドレス範囲に含まれる宛先 IP アドレスを持つパケットは，VLAN 内の全ポートに中継します。次の表に示すアドレス範囲外の宛先 IP アドレスを持つパケットは，IGMP snooping/MLD snooping の学習結果に従って中継します。

表 29-9　制御パケットのフラッディング

プロトコル	アドレス範囲
IGMP snooping	224.0.0.0/24
MLD snooping	ff02::/16

ただし，制御パケットのマルチキャスト MAC アドレスと重複するマルチキャストグループアドレスは使用できません。上の表に示したアドレス範囲以外のアドレスで，使用できないマルチキャストグループアドレスを次の表に示します。

表 29-10　IGMP snooping で使用できないマルチキャストグループアドレス

プロトコル	マルチキャストグループアドレス
IGMP snooping	224.128.0.0/24
	225.0.0.0/24
	225.128.0.0/24
	226.0.0.0/24
	226.128.0.0/24
	227.0.0.0/24
	227.128.0.0/24
	228.0.0.0/24
	228.128.0.0/24
	229.0.0.0/24
	229.128.0.0/24
	230.0.0.0/24
	230.128.0.0/24
	231.0.0.0/24

プロトコル	マルチキャストグループアドレス
	231.128.0.0/24
	232.0.0.0/24
	232.128.0.0/24
	233.0.0.0/24
	233.128.0.0/24
	234.0.0.0/24
	234.128.0.0/24
	235.0.0.0/24
	235.128.0.0/24
	236.0.0.0/24
	236.128.0.0/24
	237.0.0.0/24
	237.128.0.0/24
	238.0.0.0/24
	238.128.0.0/24
	239.0.0.0/24
	239.128.0.0/24

上の表に示したアドレスをマルチキャストグループアドレスに使用した場合，該当マルチキャストグループアドレス宛てのマルチキャストデータは，VLAN 内の全ポートに中継します。

トランクポートを設定している場合は，Untagged 制御パケットを受信しないように注意してください。構成上，トランクポートで Untagged 制御パケットを扱う場合は，ネイティブ VLAN を設定してください。

(3)　マルチキャストルータポートの設定

(a)　冗長構成時

スパニングツリーによって冗長構成を採り，スパニングツリーによってトポロジー変更でルータとの接続が変わる可能性がある場合は，ルータと接続する可能性のある全ポートに対してマルチキャストルータポートの設定をしておく必要があります。

(b)　レイヤ 2 スイッチ間の接続時

複数のレイヤ 2 スイッチだけで構成される VLAN で，マルチキャストトラフィックの送信ホストを収容するレイヤ 2 スイッチと接続するポートをマルチキャストルータポートに設定しておく必要があります。

冗長構成を採る場合は，送信ホストを収容するレイヤ 2 スイッチと接続する可能性のある全ポートに対してマルチキャストルータポートの設定をしておく必要があります。

(4) マルチキャストルータポートの自動学習

(a) IGMP 監視

ネットワーク上に IGMP に対応した複数のマルチキャストルータが存在する場合，通常はその中の 1 台だけが代表クエリアに選出されるため，代表クエリアを接続しているポートだけをマルチキャストルータポートに自動設定します。本装置が代表クエリアの場合も，ほかのマルチキャストルータは検知しないため，マルチキャストルータポートの自動設定はしません。

(5) IGMP バージョン 3 ホストとの接続

本装置に IGMPv3 ホストを接続する場合，次の対応が必要です。

- IGMPv3 ルータを接続して該当するルータが代表クエリアになるように IP アドレスを設定してください。

また，IGMPv3 ホストからの IGMPv3 メッセージがフラグメント化されない構成で運用してください。

(6) MLD バージョン 2 ホストとの接続

本装置に MLDv2 ホストを接続する場合，次の対応が必要です。

- MLDv2 ルータを接続して該当するルータが代表クエリアになるように IP アドレスを設定してください。

また，MLDv2 ホストからの MLDv2 メッセージがフラグメント化されない構成で運用してください。

(7) 運用コマンド実行によるエントリの再学習

IGMP/MLD snooping の運用コマンドのほかに，下記のコマンドを実行した場合，それまでに学習したエントリをクリアし，再学習を行います。運用コマンド実行後は，一時的にマルチキャスト通信が中断します。

- copy コマンドで running-config に上書きした場合
- restart vlan コマンド

(8) IGMP 即時離脱機能

IGMP 即時離脱機能を使用した場合，IGMPv2 Leave および IGMPv3 Report（離脱要求）メッセージを受信すると，該当ポートへのマルチキャスト通信をすぐに停止します。このため，本機能を使用する場合は，接続ポートに各マルチキャストグループの受信者の端末を 1 台だけ設置することを推奨します。

接続ポートに同一マルチキャストグループの受信者の端末を複数台設置した場合は，一時的にほかの受信者へのマルチキャスト通信が停止します。この場合，受信者からの IGMP Report（加入要求）メッセージを再度受信することで，マルチキャスト通信は再開します。

(9) IGMP Query メッセージの送信間隔

IGMPv2 で運用している場合，他装置を含む該当 VLAN 内では，IGMP Query メッセージの送信間隔を同じ値に設定してください。

30 IGMP snooping/MLD snooping の設定と運用

IGMP snooping/MLD snooping はレイヤ 2 で VLAN 内のマルチキャストトラフィックを制御する機能です。この章では，IGMP snooping/MLD snooping の設定と運用方法について説明します。

30.1　IGMP snooping のコマンドガイド

30.1.1　コマンド一覧

IGMP snooping のコンフィグレーションコマンド一覧を次の表に示します。

表 30-1　コンフィグレーションコマンド一覧

コマンド名	説明
ip igmp snooping (global)	no ip igmp snooping で，本装置の IGMP snooping 機能を抑止します。
ip igmp snooping (VLAN インタフェース)	指定したインタフェースの IGMP snooping 機能を設定します。
ip igmp snooping fast-leave	IGMP 即時離脱機能を設定します。
ip igmp snooping mrouter discovery	マルチキャストルータポート自動学習を有効にします。
ip igmp snooping mrouter discovery extension	マルチキャストルータポート自動学習で検知した IGMP マルチキャストルータ情報の保持時間の加算値を設定します。
ip igmp snooping mrouter interface	IGMP マルチキャストルータポートを設定します。
ip igmp snooping mrouter logging	no ip igmp snooping mrouter logging で，マルチキャストルータ自動学習に関する運用メッセージの出力を抑止します。
ip igmp snooping querier	IGMP クエリア機能を設定します。
ip igmp snooping query-interval	定期的に送信する IGMP General Query メッセージの送信間隔を設定します。

IGMP snooping の運用コマンド一覧を次の表に示します。

表 30-2　運用コマンド一覧

コマンド名	説明
show igmp-snooping	IGMP snooping 情報を表示します。
clear igmp-snooping	IGMP snooping 情報をクリアします。
show igmp-snooping mrouter	マルチキャストルータポート自動学習で検知したマルチキャストルータ情報を表示します。
clear igmp-snooping mrouter	マルチキャストルータポート自動学習で検知したマルチキャストルータ情報をクリアします。
show igmp-snooping mrouter statistics	マルチキャストルータポート自動学習に関する統計情報を表示します。
clear igmp-snooping mrouter statistics	マルチキャストルータポート自動学習に関する統計情報をクリアします。
restart snooping	IGMP snooping/MLD snooping プログラムを再起動します。
dump protocols snooping	イベントトレース情報および制御テーブル情報のファイルを出力します。

30.1.2　IGMP snooping の設定

[設定のポイント]

IGMP snooping を動作させるには，使用する VLAN の VLAN インタフェースコンフィグレーションモードで，次の設定を行います。

VLAN2 に IGMP snooping 機能を有効にする場合を示します。

[コマンドによる設定]

1.**(config)# interface vlan 2**

(config-if)# ip igmp snooping

VLAN2 の VLAN インタフェースコンフィグレーションモードに移行して, IGMP snooping 機能を有効にします。

30.1.3　IGMP クエリア機能の設定

[設定のポイント]

IGMP snooping を設定した VLAN 内にマルチキャストルータが存在しない場合, IGMP クエリア機能を動作させる必要があります。該当 VLAN の VLAN インタフェースコンフィグレーションモードで次の設定を行います。例として，VLAN2 に IGMP クエリア機能を有効にする場合を示します。

[コマンドによる設定]

1.**(config)# interface vlan 2**

(config-if)# ip igmp snooping querier

VLAN2 の VLAN インタフェースコンフィグレーションモードに移行して，IGMP クエリア機能を有効にします。

[注意事項]

本設定は該当インタフェースに IPv4 アドレスの設定がないと有効になりません。

30.1.4　マルチキャストルータポートの設定

(1)　スタティック設定

[設定のポイント]

IGMP snooping を設定した VLAN 内にマルチキャストルータを接続している場合，該当 VLAN の VLAN インタフェースコンフィグレーションモードで，次の設定を行います。例として，VLAN2 のポート 1/0/1 のギガビット・イーサネットインタフェースにマルチキャストルータを接続している場合を示します。

[コマンドによる設定]

1.**(config)# interface vlan 2**

(config-if)# ip igmp snooping mrouter interface gigabitethernet 1/0/1

VLAN2 の VLAN インタフェースコンフィグレーションモードに移行して，マルチキャストルータポートに 1/0/1 を指定します。

(2) マルチキャストルータポート自動学習の有効化

[設定のポイント]

IGMP snooping を設定した VLAN でマルチキャストルータポート自動学習機能を使用する場合，該当 VLAN の VLAN インタフェースコンフィグレーションモードで，次の設定を行います。例として，IGMP 監視と PIM 監視を同時に行う場合を示します。

[コマンドによる設定]

1. **(config)# interface vlan 2**
   (config-if)# ip igmp snooping mrouter discovery igmp
   VLAN2 の VLAN インタフェースコンフィグレーションモードに移行して，マルチキャストルータポート自動学習を有効にし，監視対象に IGMP を指定します。
2. **(config-if)# ip igmp snooping mrouter discovery pim**
   マルチキャストルータポート自動学習を有効にし，監視対象に PIM を指定します。

[注意事項]

マルチキャストルータポートの設定方式を変更するとき，マルチキャスト中継が停止するおそれがあります。そのため，設定方式は，「(3) スタティック設定から自動学習への変更」「(4) 自動学習からスタティック設定への変更」に示す手順で変更してください。

(3) スタティック設定から自動学習への変更

[設定のポイント]

スタティック設定から自動学習に変更する場合は，次に示す順序で実行してください。

1. 自動学習を有効化
2. 該当ネットワークの IGMP Query インターバル経過後に，自動学習の結果を確認
3. スタティック設定を削除

例として，VLAN2 で，スタティック設定から自動学習（IGMP 監視）に変更する場合を示します。

[コマンドによる設定]

1. **(config)# interface vlan 2**
   (config-if)# ip igmp snooping mrouter discovery igmp
   VLAN2 の VLAN インタフェースコンフィグレーションモードに移行して，マルチキャストルータポート自動学習（IGMP 監視）を有効にします。
2. **(config-if)# save**
   (config-if)# top
   (config)# exit
   # show igmp-snooping mrouter

```
Total entry: 1
VLAN ID: 2
  Port        IP address         Type    Expire
  1/0/1       192.168.11.100     IGMP    04:08

#
```

コンフィグレーションモードから装置管理者モードに移行します。

VLAN2 の IGMP Query インターバル経過後，運用コマンド show igmp-snooping mrouter を実行して，マルチキャストルータポートが自動設定されていることを確認します。

3.**# configure**

(config)# interface vlan 2

(config-if)# no ip igmp snooping mrouter interface gigabitethernet 1/0/1

装置管理者モードからコンフィグレーションモードに移行します。

VLAN2 の VLAN インタフェースコンフィグレーションモードに移行して，VLAN2 のスタティック設定を削除します。

(4)　自動学習からスタティック設定への変更

[設定のポイント]

自動学習からスタティック設定に変更する場合は，次に示す順序で実行してください。

1. スタティック設定を実施
2. 自動学習を無効化

例として，VLAN2 で，自動学習（IGMP 監視）からスタティック設定に変更する場合を示します。

[コマンドによる設定]

1.**(config)# interface vlan 2**

(config-if)# ip igmp snooping mrouter interface gigabitethernet 1/0/1

VLAN2 の VLAN インタフェースコンフィグレーションモードに移行して，マルチキャストルータポートに 1/0/1 をスタティック設定します。

2.**(config-if)# no ip igmp snooping mrouter discovery igmp**

VLAN2 の自動学習（IGMP 監視）を無効にします。

30.2　MLD snooping のコマンドガイド

30.2.1　コマンド一覧

MLD snooping のコンフィグレーションコマンド一覧を次の表に示します。

表 30-3　コンフィグレーションコマンド一覧

コマンド名	説明
ipv6 mld snooping (global)	no ipv6 mld snooping で，本装置の MLD snooping 機能を抑止します。
ipv6 mld snooping (VLAN インタフェース)	指定したインタフェースの MLD snooping 機能を設定します。
ipv6 mld snooping mrouter interface	MLD マルチキャストルータポートを設定します。
ipv6 mld snooping querier	MLD クエリア機能を設定します。

MLD snooping の運用コマンド一覧を次の表に示します。

表 30-4　運用コマンド一覧

コマンド名	説明
show mld-snooping	MLD snooping 情報を表示します。
clear mld-snooping	MLD snooping 情報をクリアします。
restart snooping	IGMP snooping/MLD snooping プログラムを再起動します。
dump protocols snooping	イベントトレース情報および制御テーブル情報のファイルを出力します。

30.2.2　MLD snooping の設定

[設定のポイント]

MLD snooping を動作させるには，使用する VLAN の VLAN インタフェースのインタフェースコンフィグレーションモードで，次の設定を行います。例として，VLAN2 に MLD snooping 機能を有効にする場合を示します。

[コマンドによる設定]

1. **(config)# interface vlan 2**
   (config-if)# ipv6 mld snooping
   VLAN2 の VLAN インタフェースコンフィグレーションモードに移行して，MLD snooping 機能を有効にします。

30.2.3　MLD クエリア機能の設定

[設定のポイント]

MLD snooping を設定した VLAN 内にマルチキャストルータが存在しない場合，MLD クエリア機能を動作させる必要があります。該当 VLAN の VLAN インタフェースコンフィグレーションモードで，

次の設定を行います。例として，VLAN2 に MLD クエリア機能で使用する IPv6 アドレス（fe80::100）を設定する場合を示します。

[コマンドによる設定]

1. (config)# interface vlan 2
   (config-if)# ipv6 mld snooping querier fe80::100
   VLAN2 の VLAN インタフェースコンフィグレーションモードに移行して，MLD クエリア機能を有効にします。

[注意事項]

本設定は該当インタフェースに IPv6 アドレスの設定がないと有効になりません。

30.2.4　マルチキャストルータポートの設定

[設定のポイント]

MLD snooping を設定した VLAN 内にマルチキャストルータを接続している場合，該当 VLAN の VLAN インタフェースコンフィグレーションモードで，次の設定を行います。例として，VLAN2 のポート 1/0/1 のギガビット・イーサネットインタフェースにマルチキャストルータを接続している場合を示します。

[コマンドによる設定]

1. (config)# interface vlan 2
   (config-if)# ipv6 mld snooping mrouter interface gigabitethernet 1/0/1
   VLAN2 の VLAN インタフェースコンフィグレーションモードに移行して，マルチキャストルータポートに 1/0/1 を指定します。

31 IPv4 通信

この章では，IPv4 のアドレッシングおよび通信機能について説明します。

31.1　解説

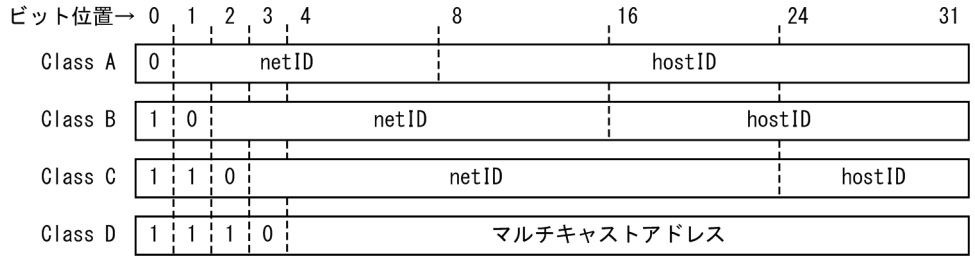
31.1.1　アドレッシング

本装置で使用する IP アドレスのアドレッシングについて概要を示します。

(1)　IP アドレス

本装置は IP アドレスの Class A，B，C，D をサポートします。IP アドレスフォーマットを次の図に示します。

図 31-1　IP アドレスフォーマット



なお，ネットワークブロードキャストアドレスおよびサブネットワークブロードキャストアドレスは，host ID が 2 進数ですべて 1 またはすべて 0 の 2 種類をサポートしており，その選択はインタフェース単位にコンフィグレーションで指定できます。インタフェースについては「(3)　IP アドレス付与単位」を参照してください。

本装置に付与する IP アドレスとして次に示す IP アドレスを使用できます。

- net ID
  net ID は次の範囲の値を使用できます。
  - Class A：1.x.x.x～126.x.x.x
  - Class B：128.1.x.x～191.254.x.x
  - Class C：192.0.1.x～223.255.254.x　(x=host ID)
- host ID
  host ID は次の範囲の値を使用できます。
  - Class A：y.0.0.1～y.255.255.254
  - Class B：y.y.0.1～y.y.255.254
  - Class C：y.y.y.1～y.y.y.254　(y=net ID)

(2)　サブネットマスク

「図 31-1　IP アドレスフォーマット」に示す Class A，B，C の net ID，host ID の境界位置に関係なく，サブネットマスクを使用して任意の境界位置に net ID と host ID の境界位置を指定できます。

サブネットマスクはインタフェースごとにコンフィグレーションで左詰め（2 進数表現で上位の桁から'1'が連続）で指定します。

例えば，サブネットマスクに 255.255.192.0 は設定できますが，255.255.96.0 は設定できません。

(3)　IP アドレス付与単位

本装置では VLAN またはループバックインタフェースに対して IP アドレスを設定します。一つの VLAN に複数の IP アドレスを設定するマルチホーム接続も可能です。ネットワークへの接続形態は，ブロードキャスト型です。

31.1.2　インターネットプロトコル(IP)

(1)　IP パケットフォーマット

本装置が送信する IP パケットのフォーマットおよび設定値は RFC791 に従います。

(2)　IP パケットヘッダ有効性チェック

IP パケット受信時に IP パケットのヘッダの有効性チェックを行います。IP パケットヘッダのチェック内容を次の表に示します。

表 31–1　IP パケットヘッダのチェック内容

IP パケットヘッダ フィールド	チェック内容	チェック異常時 パケット廃棄	パケット廃棄時 ICMP 送信
バージョン	バージョン＝４であること	○	×
ヘッダレングス	ヘッダレングス≧5 であること	○	×
TOS	チェックしない	－	－
トータルレングス	トータルレングス≧4×ヘッダレングスであること	○	×
パケット識別子	チェックしない	－	－
フラグ	チェックしない	－	－
フラグメントオフセット	チェックしない	－	－
TTL	自装置宛に受信したパケットの TTL：チェックしない	－	－
	フォワーディングするパケットの TTL：TTL-1 ＞ 0 であること	○	○※
プロトコル	チェックしない	－	－
ヘッダチェックサム	ヘッダチェックサムが正しいこと	○	×
送信元アドレス	チェックしない	－	－
宛先アドレス	次の条件をすべて満たすこと 1. クラス A，クラス B，クラス C，クラス D 2. ネットワーク番号が 127(内部ループバックアドレス)でないこと 3. ネットワーク番号が 0 でないこと(ただし，0.0.0.0 を除く)	○	×

(凡例)　○：行う　×：行わない　－：該当しない

注※　ICMP Time Exceeded メッセージを送信します。

(3)　IP オプションサポート仕様

本装置がサポートする IP オプションを次の表に示します。

表 31-2　IP オプションサポート仕様

IP オプション	IP パケットの分類	
	本装置が送信するパケット	本装置が受信するパケット
End of Option List	○	−
No Operation	○	−
Loose Source Routing	○	○
Time stamp	×	○
Record Route	○	○
Strict Source Routing	×	○

（凡例）　○：サポートする　×：サポートしない　−：オプション処理なし

31.1.3　ICMP

(1)　ICMP メッセージフォーマット

本装置が送信する ICMP メッセージのフォーマットおよび設定値は RFC792, RFC950, および RFC1122 に従います。

(2)　ICMP メッセージサポート仕様

ICMP メッセージのサポート仕様を次の表に示します。

表 31-3　ICMP メッセージサポート仕様(値は 10 進)

ICMP メッセージ				サポート
タイプ(種別)		コード(詳細種別)		
−	値	−	値	
Echo Reply	0	−	0	○
Destination Unreachable	3	Net Unreachable	0	×
		Host Unreachable	1	×
		Protocol Unreachable	2	○
		Port Unreachable	3	○
		Fragmentation Needed and DF Set	4	×
		Source Route Failed	5	×
		Destination Network Unknown	6	×

ICMP メッセージ				サポート
タイプ(種別)		コード(詳細種別)		
−	値	−	値	
		Destination Host Unknown	7	×
		Network Unreachable for Type of Service	11	×
		Host Unreachable for Type of Service	12	×
		Communication Administratively Prohibited	13	×
		Host Precedence Violation	14	×
		Precedence Cutoff in Effect	15	×
Source Quench	4	−	0	×
Redirect	5	Redirect Datagrams for the Network	0	×
		Redirect Datagrams for the Host	1	○
		Redirect Datagrams for the Type of Service and Network	2	×
		Redirect Datagrams for the Type of Service and Host	3	×
Alternate Host Address	6	Alternate Address for Host	0	×
Time Exceeded	11	Time to Live Exceeded in Transit	0	×
		Fragment Reassembly Time Exceeded	1	○
Parameter Problem	12	Pointer Indicates the Error	0	○
		Missing a Required	1	×
		Bad Length	2	×
Echo Request	8	−	0	○
Timestamp Request	13	−	0	×
Timestamp Reply	14	−	0	○※
Information Request	15	−	0	×
Information Reply	16	−	0	×
Address Mask Request	17	−	0	×
Address Mask Reply	18	−	0	○※
Router Advertisement Message	9	Normal Router Advertisement	0	×
Router Solicitation Message	10	−	−	×

(凡例)　○：サポートする　×：サポートしない　−：該当しない

注※　Request メッセージを受信した場合は，Reply メッセージを返します。

31.1.4　ARP

(1)　ARP パケットフォーマット

本装置が送信する ARP パケットのフォーマット，および設定値は RFC826 に従います。

(2)　ARP パケット有効性チェック

本装置は，受信した ARP パケットの有効性をチェックします。ARP パケットのチェック内容を次の表に示します。

表 31-4　ARP パケットのチェック内容

ARP パケットフィールド	チェック内容	チェック異常時パケット廃棄
ハードウェアタイプ	ハードウェアタイプ= 1（Ethernet）	○
プロトコルタイプ	プロトコル= 0800H（IP）であること 1000H（Trailer packet）であること※	○
ハードウェアアドレス長	6 であること	○
プロトコルアドレス長	4 であること	○
オペレーションコード	オペレーションコード= 1（REQUEST），1 以外は 2（REPLY）として扱う	－
送信元ハードウェアアドレス	以下の値ではないこと • 自装置ハードウェアアドレスと同じ	○
送信元プロトコルアドレス	以下のどちらかであること • ユニキャストアドレス • 0.0.0.0	○
宛先ハードウェアアドレス	チェックしない	－
宛先プロトコルアドレス	以下の値ではないこと • 0.0.0.0	○

（凡例）　○：廃棄する　－：該当しない

注※

Trailer packet の自発送信はしませんが，要求があった場合は応答を返して学習します。

(3)　ARP 受信時の動作

本装置は受信した ARP パケットに基づいて，新規 ARP エントリを学習したり，学習済み ARP エントリを更新したりします。また，必要に応じて ARP パケットを応答します。ARP 受信時の動作を次の表に示します。

表 31-5　ARP 受信時の動作

ARP 種別	宛先プロトコルアドレス	送信元プロトコルアドレス	ARP 応答	新規 ARP 学習	ARP 更新
ARP Request	自装置のアドレス	0.0.0.0 自装置のアドレス	○	−	−
		その他	○	○	○
	その他	自装置のアドレス	○	−	−
		その他	−	−	−
ARP Reply	自装置のアドレス	自装置のアドレス	−	−	−
		その他	−	○	○
	その他	自装置のアドレス	−	−	−
		その他	−	−	○※

（凡例）　○：動作する　−：動作しない

注※　ARP Reply がブロードキャストまたはマルチキャストの場合

(4)　エージングタイマ

ARP 情報のエージング時間はインタフェースごとに分単位で指定できます。指定値は最小 1 分で最大 24 時間です。また，デフォルト値は 4 時間です。

(5)　ARP 情報の設定

ARP プロトコルを持たない製品を接続するために，MAC アドレスと IP アドレスの対応（ARP 情報）をコンフィグレーションコマンド arp で設定できます。

(6)　ARP 情報の参照

運用端末から show ip arp コマンドで ARP 情報が参照できます。ARP 情報から該当インタフェースの IP アドレスと MAC アドレスの対応がわかります。

(7)　Gratuitous ARP

本装置の VLAN インタフェースに設定された IP アドレスを Target Protocol Address フィールドにセットし，Gratuitous ARP を送信します。

Gratuitous ARP は，IPv4 アドレスの設定されている VLAN インタフェースがアップする契機，およびアップしている VLAN インタフェースに新たに IPv4 アドレスを設定した契機で送信します。

31.1.5　経路設定

本装置に直接接続されていないサブネットと通信するために，宛先ネットワークとネクストホップを指定して，スタティック経路を設定できます。ネクストホップには，本装置に直接接続されているサブネット内の宛先を指定してください。

31.1.6　IPv4 使用時の注意事項

(1)　本装置の IPv4 アドレスと重複するアドレスが存在する場合について

本装置と重複した IPv4 アドレスを持つ端末からのパケットを受信しても，運用メッセージなどは出力しません。同一の IPv4 アドレスを持つ端末がある場合，本装置と正常に通信できないおそれがあるため，IPv4 アドレスを見直してください。

31.2　コマンドガイド

31.2.1　コマンド一覧

IPv4 通信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 31-6　コンフィグレーションコマンド一覧

コマンド名	説明
arp	スタティック ARP テーブルを作成します。
arp max-send-count	ARP 要求パケットの最大送信回数を指定します。
arp send-interval	ARP 要求パケットの送信リトライ間隔を指定します。
arp timeout	ARP キャッシュテーブルエージング時間を指定します。
ip address	インタフェースの IPv4 アドレスを指定します。
ip mtu	インタフェースでの送信 IP MTU 長を指定します。
ip route	IPv4 のスタティック経路を設定します。
interface loopback※	ループバックインタフェース階層に移動します。
ip address (loopback)※	ループバックインタフェースの IPv4 アドレスを指定します。

注※

「コンフィグレーションコマンドレファレンス」「24　ループバックインタフェース」を参照してください。

IPv4 通信の運用コマンド一覧を次の表に示します。

表 31-7　運用コマンド一覧

コマンド名	説明
show ip-dual interface	IPv4 および IPv6 インタフェースの状態を表示します。
show ip interface	IPv4 インタフェースの状態を表示します。
show ip arp	ARP エントリ情報を表示します。
clear arp-cache	ダイナミック ARP 情報を削除します。
show netstat (netstat)	ネットワークのステータスを表示します。
ping	エコーテストを行います。
traceroute	経由ルートを表示します。
show ip route	IPv4 のルーティングテーブルを表示します。
show tcpdump	本装置に対して送受信されるパケットをモニタします。

31.2.2 インタフェースの設定

[設定のポイント]

VLAN に IPv4 アドレスを設定します。IPv4 アドレスを設定するには，インタフェースコンフィグレーションモードに移行する必要があります。

[コマンドによる設定]

1. **(config)# interface vlan 100**
   VLAN ID 100 の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)# ip address 192.168.1.1 255.255.255.0**
   VLAN ID 100 に IPv4 アドレス 192.168.1.1，サブネットマスク 255.255.255.0 を設定します。

31.2.3 マルチホームの設定

[設定のポイント]

VLAN に複数の IPv4 アドレスを設定します。二つ以降の IPv4 アドレスには secondary パラメータを指定する必要があります。

[コマンドによる設定]

1. **(config)# interface vlan 100**
   VLAN ID 100 の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)# ip address 192.168.1.1 255.255.255.0**
   VLAN ID 100 にプライマリ IPv4 アドレス 192.168.1.1，サブネットマスク 255.255.255.0 を設定します。
3. **(config-if)# ip address 10.1.1.1 255.255.255.0 secondary**
   VLAN ID 100 にセカンダリ IPv4 アドレス 10.1.1.1，サブネットマスク 255.255.255.0 を設定します。

31.2.4 ループバックインタフェースの設定

[設定のポイント]

装置を識別するための IPv4 アドレスを設定します。設定できるアドレスは一つだけです。

[コマンドによる設定]

1. **(config)# interface loopback 0**
   ループバックインタフェースの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)# ip address 192.168.1.1**
   ループバックインタフェースに IP アドレス 192.168.1.1 を設定します。

31.2.5 スタティック ARP の設定

[設定のポイント]

本装置にスタティック ARP を設定します。
インタフェースを指定する必要があります。

[コマンドによる設定]

1. **(config)# arp 192.168.0.1 interface vlan 100 0012.e240.0a00**
   VLAN ID 100 にネクストホップ IPv4 アドレス 192.168.0.1，接続先 MAC アドレス 0012.e240.0a00 でスタティック ARP を設定します。

31.2.6　デフォルト経路の設定

[設定のポイント]

デフォルト経路を設定します。

デフォルト経路の設定には ip route コマンドを使用します。宛先アドレスに 0.0.0.0，サブネットマスクに 0.0.0.0 を指定することによって，デフォルト経路が設定されます。

[コマンドによる設定]

1. **(config)# ip route 0.0.0.0 0.0.0.0 10.1.1.50**
   デフォルト経路のネクストホップとして，隣接装置の IP アドレスである 10.1.1.50 を指定します。

31.2.7　スタティック経路の設定

[設定のポイント]

スタティック経路を設定します。

[コマンドによる設定]

1. **(config)# ip route 192.168.1.0 255.255.255.0 10.1.1.100**
   スタティック経路 192.168.1.0/24 のネクストホップとして，隣接装置のアドレスである 10.1.1.100 を指定します。

32 IPv6 通信

この章では IPv6 通信機能について説明します。

32.1　解説

IPv6 は IPv4 と比較して次のような特長があります。

- **アドレス構造を拡張している**
  アドレス長が 32 ビットから 128 ビットに拡張されています。そのため，ノードへ割り当てができるアドレス数がほぼ無限となり，IPv4 で問題となっていたアドレス枯渇問題が解消されます。また，アドレス構造階層のレベル数が増加したため，新しいアドレスを定義できるようになります。
- **ヘッダ形式を単純化している**
  IPv4 と比較してヘッダフィールドが簡略化され，プロトコル処理のオーバーヘッドが減少しています。
- **拡張ヘッダとオプションヘッダを強化している**
  転送効率の向上，オプションの長さ制限の緩和，また，オプション拡張が容易です。
- **フローラベルを設定できる**
  特定のトラフィックフローを識別するためのラベル付けができます。

本装置で使用する IPv6 ネットワークのアドレッシングについて概要を示します。

32.1.1　IPv6 アドレス

(1)　アドレス表記方法

IPv6 のアドレスは 128 ビット長です。実際に表記するときの方法を次に示します。

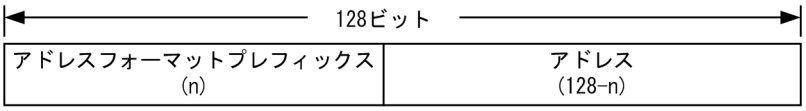
- 16 進数で 16 ビットごとにコロン":"で区切った形式で表記します。
  (例)　3ffe:0501:0811:ff02:0000:08ff:fe8b:3090
- 16 進数の先頭にくる"0"は省略できます。
  (例)　3ffe:501:811:ff02:0:8ff:fe8b:3090
- 連続する"0"は二つのコロン"::"に置換できます。ただし，"::"に置換できるのは一つのアドレス表記に 1 か所までと定義されています。
  (例)　次に示す IPv6 アドレスのときの置換方法
  fe80:0000:0000:0000:0000:0000:0000:3090　→　fe80::3090
  (例)　2 か所以上の"::"は禁止
  fe80:0000:0000:0000:0000:0000:0000:3090　→　fe80::0::3090
- 次に示す形式でアドレスとプレフィックス長を指定できます。
  - IPv6 アドレス／プレフィックス長
  - IPv6 アドレス prefixlen プレフィックス長

  プレフィックス長はアドレス左端から何ビットまでがプレフィックスかを 10 進数で指定します。

(2)　アドレスフォーマットプレフィックス

128 ビット長の IPv6 アドレスが複数のサブフィールドに分割されています。先頭ビットは IPv6 アドレスのタイプを識別する役割があり，アドレスフォーマットプレフィックスと呼ばれます。アドレスフォーマットプレフィックスを次の図に示します。

図 32–1　アドレスフォーマットプレフィックス



（　）内の数字はビット数を示す。

また，アドレスフォーマットプレフィックスの種類を次の表に示します。

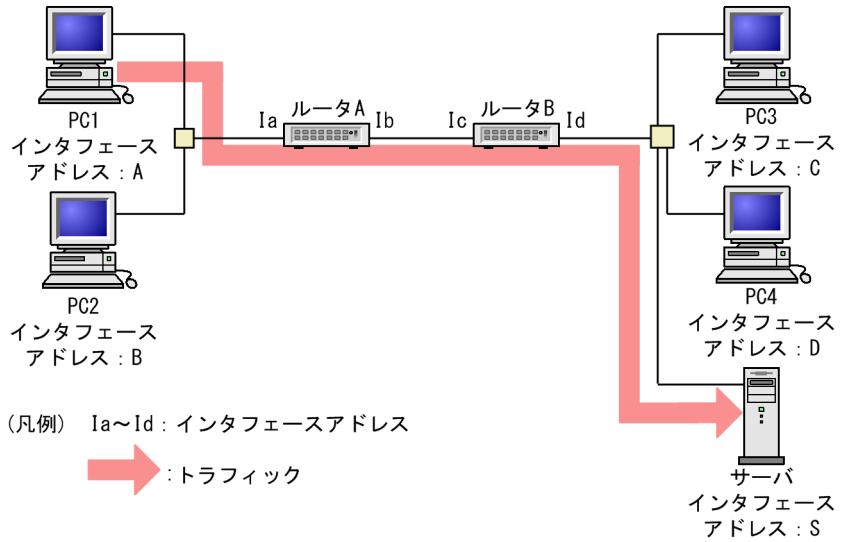
表 32–1　アドレスフォーマットプレフィックスの種類

プレフィックス(2 進数)	割り当て
0000 0000	未割り当て
0000 0001	未割り当て
0000 001	未割り当て
0000 010	未割り当て
0000 011	未割り当て
0000 1	未割り当て
0001	未割り当て
001	集約可能グローバルユニキャストアドレス
010	未割り当て
011	未割り当て
100	未割り当て
101	未割り当て
110	未割り当て
1110	未割り当て
1111 0	未割り当て
1111 10	未割り当て
1111 110	ユニークローカルユニキャストアドレス
1111 1110 0	未割り当て
1111 1110 10	リンクローカルユニキャストアドレス
1111 1110 11	未割り当て
1111 1111	マルチキャストアドレス

(3)　ユニキャストアドレス

単一のインタフェースを示すアドレスです。終点アドレスがユニキャストアドレスのパケットは，そのアドレスが示すインタフェースに配送されます。ユニキャストアドレス通信を次の図に示します。

図 32-2　ユニキャストアドレス通信

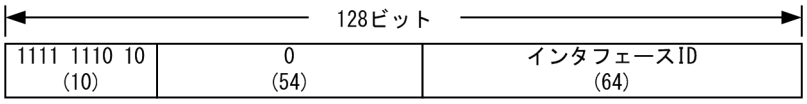


(a)　リンクローカルアドレス

アドレスプレフィックスの上位 64 ビットが fe80::で，64 ビットのインタフェース ID 部を含むアドレスを**IPv6 リンクローカルアドレス**と呼びます。IPv6 リンクローカルアドレスは同一リンク内だけで有効なアドレスで，自動アドレス設定，近隣探索，またはルータが存在しないときに使用されます。パケットの始点または終点アドレスが IPv6 リンクローカルアドレスの場合，本装置はパケットをほかのリンクに転送することはありません。

本装置で IPv6 を使用するインタフェースには IPv6 リンクローカルアドレスが必ず一つ設定されます。二つ以上は設定できません。IPv6 リンクローカルアドレスを次の図に示します。

図 32-3　IPv6 リンクローカルアドレス

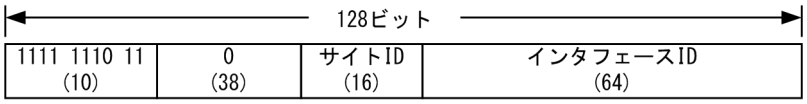


（　）内の数字はビット数を示す。

(b)　サイトローカルアドレス

アドレスプレフィックスの上位 10 ビットが 1111 1110 11 で，64 ビットのインタフェース ID 部を含むアドレスを**IPv6 サイトローカルアドレス**と呼びます。本装置は IPv6 サイトローカルアドレスを「(c)　グローバルアドレス」の IPv6 グローバルアドレスとして扱います。そのため，IPv6 サイトローカルアドレスをインタフェースに設定した場合は，IPv6 サイトローカルアドレス情報がサイト外に出ないようにルーティングやフィルタリングを設定してください。IPv6 サイトローカルアドレスを次の図に示します。なお，サイトローカルアドレスは RFC3879 で廃止されました。

図 32-4　IPv6 サイトローカルアドレス

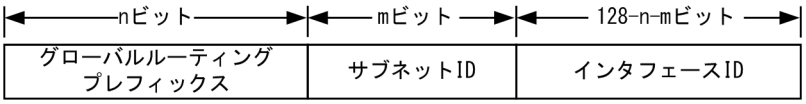


（　）内の数字はビット数を示す。

(c)　グローバルアドレス

アドレスプレフィックスの上位 3 ビットが 001 で始まるアドレスを **IPv6 グローバルアドレス**と呼びます。IPv6 グローバルアドレスは世界で一意なアドレスで，インターネットを介した通信を行う場合に使用されます。パケットの始点アドレスが IPv6 グローバルアドレスの場合，経路情報に従ってパケットが転送されます。IPv6 グローバルアドレスを次の図に示します。

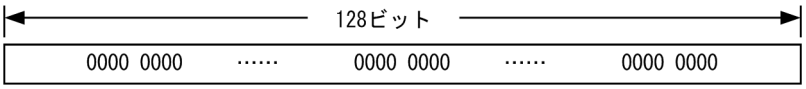
図 32–5　IPv6 グローバルアドレス



(d)　未指定アドレス

すべてのビットが 0 のアドレス 0:0:0:0:0:0:0:0(0::0，または::)は，**未指定アドレス**と定義されています。未指定アドレスはインタフェースにアドレスが存在しないことを表しています。これは，アドレスの割り当てを受けていないノードの接続開始時などに使用されます。未指定アドレスをノードに対して意図的に割り当てることはできません。未指定アドレスを次の図に示します。

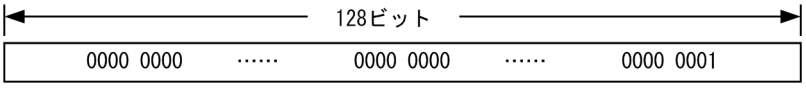
図 32–6　未指定アドレス



(e)　ループバックアドレス

アドレス 0:0:0:0:0:0:0:1(0::1，または::1)は，**ループバックアドレス**と定義されています。ループバックアドレスは自ノード宛て通信を行うときにパケットの宛先アドレスとして使用されます。ループバックアドレスをインタフェースに対して割り当てることはできません。また，終点アドレスがループバックアドレスの IPv6 パケットは，そのノード外に送信することや，ルータによって転送することは禁止されています。ループバックアドレスを次の図に示します。

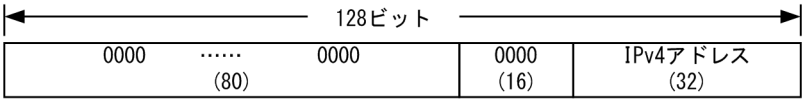
図 32–7　ループバックアドレス



(f)　IPv4 互換アドレス

IPv4 互換 IPv6 アドレスは，二つの IPv6 ノードが IPv4 で経路制御されたネットワークで通信するためのアドレスです。下位 32 ビットに IPv4 アドレスを含む特殊なユニキャストアドレスで，IPv4 ネットワークに接続している機器同士が通信を行う場合に使用します。プレフィックスは 96 ビット長ですべて 0 です。IPv4 互換アドレスを次の図に示します。なお，IPv4 互換アドレスは RFC4291 で廃止されました。

図 32–8　IPv4 互換アドレス

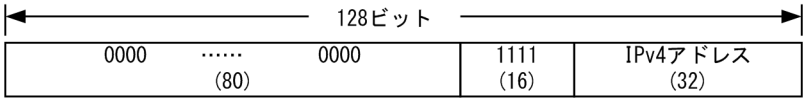


（　）内の数字はビット数を示す。

(g) IPv4 射影アドレス

IPv4 射影 IPv6 アドレスは，IPv6 をサポートしていない IPv4 専用ノードで使用されます。IPv4 しかサポートしないホストと IPv6 ホストが通信する場合に IPv6 ホストは IPv4 射影 IPv4 アドレスを使用します。プレフィックスは 96 ビット長で上位 80 ビットの 0 に続き 16 ビットの 1 が設定されます。IPv4 射影アドレスを次の図に示します。

図 32–9 IPv4 射影アドレス

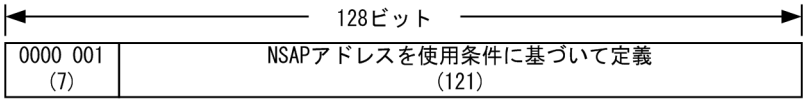


（ ）内の数字はビット数を示す。

(h) NSAP 互換アドレス

IPv6 で NSAP アドレスを変換して使用するためのアドレス形式です。NSAP をサポートするアドレスフォーマットプレフィックスとして上位 7 ビットに 0000 001 が定義されています。NSAP 互換アドレスを次の図に示します。なお，NSAP 互換アドレスは RFC4048 で廃止されました。

図 32–10 NSAP 互換アドレス

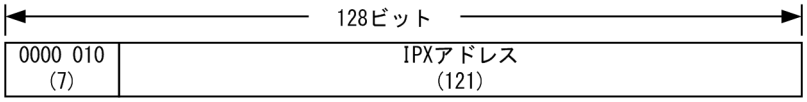


（ ）内の数字はビット数を示す。

(i) IPX 互換アドレス

IPv6 で IPX アドレスを変換して使用するためのアドレス形式です。IPX をサポートするアドレスフォーマットプレフィックスとして上位 7 ビットに 0000 010 が定義されています。IPX 互換アドレスを次の図に示します。なお，IPX 互換アドレスは RFC3513 で廃止されました。

図 32–11 IPX 互換アドレス

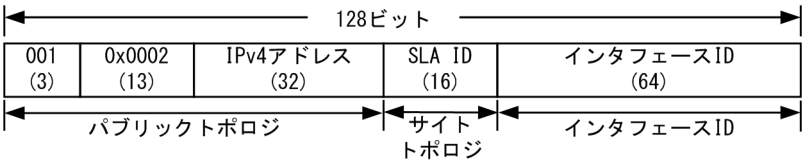


（ ）内の数字はビット数を示す。

(j) 6to4 アドレス

6to4 トンネルで使用するアドレス形式です。プレフィックスとして 2002::/16 が割り当てられていて，17 ビット目から 48 ビット目にトンネルを使用するサイトの IPv4 アドレスを設定します。6to4 アドレスを次の図に示します。

図 32–12　6to4 アドレス



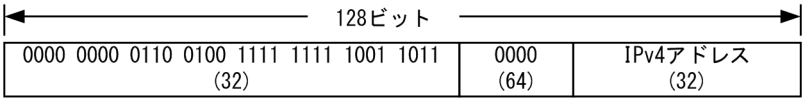
（　）内の数字はビット数を示す。

(k)　IPv4 埋め込み IPv6 アドレス

IPv4 アドレスと IPv6 アドレスの変換に使用されるアドレス形式です。プレフィックスとしてウェルノウン・プレフィックスを使用する形式と，任意のプレフィックスを使用する形式があります。本装置では通常のグローバルアドレスとして扱います。

ウェルノウン・プレフィックス（64:ff9b::/96）を使用する形式では，下位 32 ビットに IPv4 アドレスが格納されます。ウェルノウン・プレフィックスを使用した IPv4 埋め込み IPv6 アドレスを次の図に示します。

図 32–13　IPv4 埋め込み IPv6 アドレス（ウェルノウン・プレフィックスを使用）

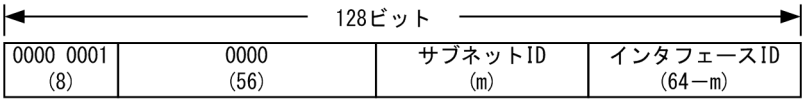


（　）内の数字はビット数を示す。

(l)　廃棄プレフィックスアドレス

特定の送信元または宛先アドレスのパケットを廃棄するために使用されるアドレス形式です。プレフィックスとして 100::/64 が割り当てられています。本装置では通常のグローバルアドレスとして扱います。廃棄プレフィックスアドレスを次の図に示します。

図 32–14　廃棄プレフィックスアドレス

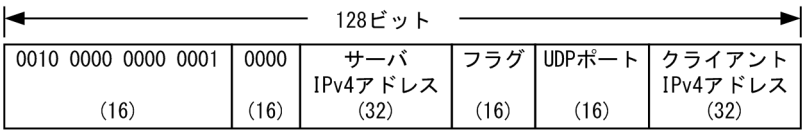


（　）内の数字はビット数を示す。

(m)　Teredo IPv6 アドレス

UDP による IPv6 トンネリングを実現する Teredo で使用されるアドレス形式です。プレフィックスとして 2001::/32 が割り当てられています。本装置では通常のグローバルアドレスとして扱います。Teredo IPv6 アドレスを次の図に示します。

図 32–15　Teredo IPv6 アドレス

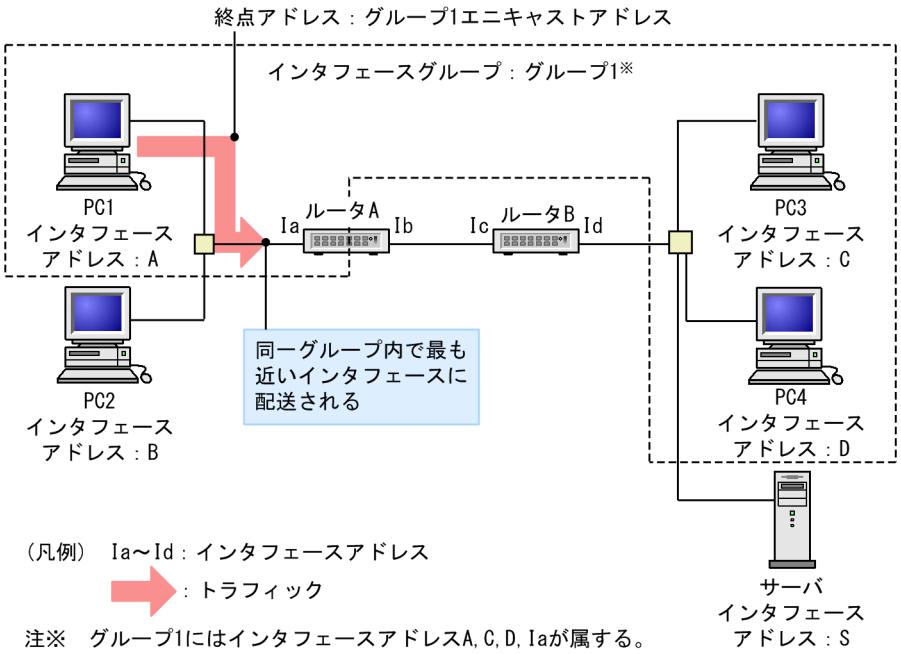


（　）内の数字はビット数を示す。

(4)　エニキャストアドレス

インタフェースの集合を示すアドレスです。終点アドレスがエニキャストアドレスのパケットは，インタフェース集合のうち，経路制御プロトコルによって測定された距離の最も近いインタフェースに配送されます。なお，本装置ではエニキャストアドレスは未サポートです。エニキャストアドレス通信を次の図に示します。

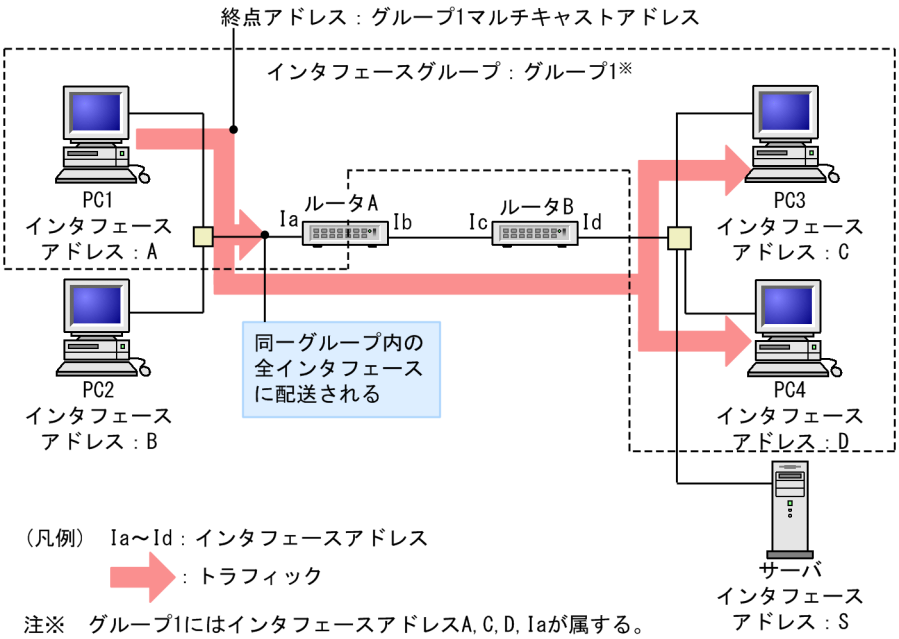
図 32-16　エニキャストアドレス通信



(5)　マルチキャストアドレス

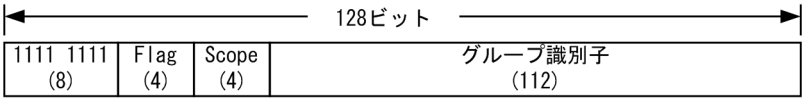
インタフェースの集合を示すアドレスです。終点アドレスがマルチキャストアドレスのパケットは，そのアドレスが示すインタフェース集合のすべてのインタフェースに配送されます。マルチキャストアドレス通信を次の図に示します。

図 32-17　マルチキャストアドレス通信



アドレスフォーマットプレフィックスの上位 8 ビットが ff であるアドレスが定義されています。ノードは複数のマルチキャストグループに属することができます。マルチキャストアドレスは，パケットの始点アドレスとして使用することはできません。マルチキャストアドレスには，アドレスフォーマットプレフィックスに続いて，フラグフィールド(4 ビット)，スコープフィールド(4 ビット)およびグループ識別子フィールド(112 ビット)が含まれます。IPv6 マルチキャストアドレスを次の図に示します。

図 32-18　IPv6 マルチキャストアドレス



（　）内の数字はビット数を示す。

フラグフィールドの 4 ビットは 1 ビットずつフラグとして定義されています。4 ビット目は T(transient)フラグビットと定義されており，次の値になります。

1. T フラグビットが 0：IANA によって永続的に割り当てられた既知のマルチキャストアドレス
2. T フラグビットが 1：一時的に使用される(非永続的な)マルチキャストアドレス

スコープフィールドは 4 ビットのフラグでマルチキャストグループのスコープを限定するために使用します。マルチキャストアドレスのスコープフィールド値を次の表に示します。

表 32-2　マルチキャストアドレスのスコープフィールド値

値	スコープの範囲
0	予約
1	ノードローカルスコープ
2	リンクローカルスコープ
3	未割り当て

値	スコープの範囲
4	アドミンローカルスコープ
5	サイトローカルスコープ
6	未割り当て
7	未割り当て
8	組織ローカルスコープ
9	未割り当て
A	未割り当て
B	未割り当て
C	未割り当て
D	未割り当て
E	グローバルスコープ
F	予約

(a) 予約マルチキャストアドレス

次に示すマルチキャストアドレスはあらかじめ予約されており，どのマルチキャストグループにも割り当てることができません。

1. ff00:0:0:0:0:0:0:0
2. ff01:0:0:0:0:0:0:0
3. ff02:0:0:0:0:0:0:0
4. ff03:0:0:0:0:0:0:0
5. ff04:0:0:0:0:0:0:0
6. ff05:0:0:0:0:0:0:0
7. ff06:0:0:0:0:0:0:0
8. ff07:0:0:0:0:0:0:0
9. ff08:0:0:0:0:0:0:0
10. ff09:0:0:0:0:0:0:0
11. ff0a:0:0:0:0:0:0:0
12. ff0b:0:0:0:0:0:0:0
13. ff0c:0:0:0:0:0:0:0
14. ff0d:0:0:0:0:0:0:0
15. ff0e:0:0:0:0:0:0:0
16. ff0f:0:0:0:0:0:0:0

(b)　全ノードアドレス

全ノードアドレスは，指定されたスコープ内すべての IPv6 ノードの集合体を示すアドレスです。このアドレスを終点アドレスに持つパケットは指定スコープ内すべてのノードで受信されます。全ノードアドレスの種類を次に示します。

1. ff01:0:0:0:0:0:0:1 ノードローカル・全ノードアドレス
2. ff02:0:0:0:0:0:0:1 リンクローカル・全ノードアドレス

(c)　全ルータアドレス

全ルータアドレスは，指定されたスコープ内すべての IPv6 ルータの集合体を示すアドレスです。このアドレスを終点アドレスに持つパケットは指定スコープ内すべてのルータで受信されます。全ルータアドレスの種類を次に示します。

1. ff01:0:0:0:0:0:0:2 ノードローカル・全ルータアドレス
2. ff02:0:0:0:0:0:0:2 リンクローカル・全ルータアドレス
3. ff05:0:0:0:0:0:0:2 サイトローカル・全ルータアドレス

(d)　要請ノードアドレス

要請ノードアドレスは，ノードのユニキャストアドレスとエニキャストアドレスから変換され，要請ノードのアドレス(ユニキャスト，またはエニキャスト)の下位 24 ビットを 104 ビットのプレフィックス ff02:0:0:0:0:1:ff00::/104 に加えたものです。要請ノードアドレスの範囲を次に示します。

ff02:0:0:0:0:1:ff00:0000　～　ff02:0:0:0:0:1:ffff:ffff

集約プロバイダごとに上位プレフィックスが異なるなどの理由で上位の数ビットだけが異なる IPv6 アドレスが生成された場合，これらのアドレスは同じ要請ノードアドレスとなります。これによってノードが加入しなくてはならないマルチキャストアドレスの数を少なくできます。

32.1.2　本装置で使用する IPv6 アドレスの扱い

(1)　設定できるアドレス

本装置のインタフェースに付与する IPv6 アドレスとして次のアドレスを使用できます。

1. グローバルユニキャストアドレス
2. リンクローカルユニキャストアドレス

また，次に示す IPv6 アドレスは設定できますが，グローバルユニキャストアドレスと同等として扱われます。

1. サイトローカルユニキャストアドレス
2. エニキャストアドレス
3. アドレスフォーマットプレフィックスが未割り当てのユニキャストアドレス
4. NSAP 互換アドレス
5. IPX 互換アドレス

(2) 設定できないアドレス

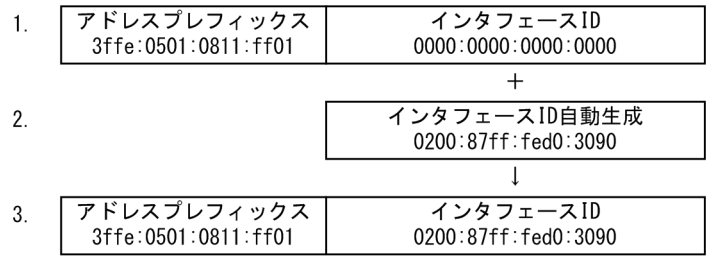
次に示す形式の IPv6 アドレスはインタフェースに付与することはできません。

1. マルチキャストアドレス
2. 未定義アドレス
3. ループバックアドレス
4. IPv4 互換アドレス
5. IPv4 射影アドレス
6. 上位 10 ビットが 1111 1110 10 で始まり，11 ビットから 64 ビットまでがすべて 0 ではないアドレス
7. 上位 10 ビットが 1111 1111 10 で始まり，以降のビットがすべて 0 のアドレス
8. プレフィックス長が 64 以外のときに，インタフェース ID 部がすべて 0 となるアドレス

(3) インタフェース ID 省略時のアドレス自動生成

本装置では，インタフェースへの IPv6 アドレス設定時に，インタフェース ID を省略したプレフィックス形式を指定できます。プレフィックス形式指定の場合，プレフィックス長が 64，または省略した形式で指定すると，インタフェース ID を装置側で MAC アドレスから自動生成できます。アドレス自動生成例を次の図に示します。

図 32-19 アドレス自動生成例



1. アドレスプレフィックス形式を指定する。(例 3ffe:0501:0811:ff01::)
2. インタフェースIDをメディア種別によって自動生成する。(例 0200:87ff:fed0:3090)
3. 生成されたインタフェースIDと指定されたアドレスプレフィックスを合成してアドレスとする。

また，インタフェースにリンクローカルアドレス以外の IPv6 アドレスが指定されたときに該当するインタフェースにリンクローカルアドレスが存在しなかった場合は，自動的にリンクローカルユニキャストアドレスを生成し設定します。さらに，インタフェースに対してリンクローカルユニキャストアドレスだけを自動生成で設定することもできます。

(4) プレフィックス長で設定できる条件

本装置では，インタフェース ID の指定がない場合は自動生成を行います。インタフェース ID の長さは 64 ビット固定となっているため，プレフィックス長で 64 または省略以外の指定が行われた場合は，インタフェース ID を自動生成しないで，入力されたプレフィックスをアドレスとして判断します。そのため下位 64 ビットがすべて 0 になるようなアドレス指定は設定できません。プレフィックス長で設定できる条件を次の表に示します。

表 32-3　プレフィックス長で設定できる条件

アドレス指定形式	設定許可	説明
3ffe:501::/1～3ffe:501::/31	○	プレフィックス長の指定がプレフィックスより短いため，インタフェース ID 部がすべて 0 にはならないので設定できます。
3ffe:501::/32～3ffe:501::/63	×	プレフィックス長の指定がプレフィックスより長いため，インタフェース ID 部がすべて 0 になるので設定できません。
3ffe:501::/64 or 3ffe:501::	○	プレフィックス長が 64 または未指定でインタフェース ID 部が省略されている場合はインタフェース ID を装置で自動生成するため設定できます。

(凡例)　○：設定できる　×：設定できない

(5)　ステートレスアドレス自動設定機能

IPv6 リンクローカルアドレスを装置内で自動生成する機能，およびホストが IPv6 アドレスを自動生成する場合に必要な情報をルータから通知する機能です。本装置では IPv6 ステートレスアドレス自動設定(RFC4862 準拠)をサポートしています。

(6)　IPv6 アドレス付与単位

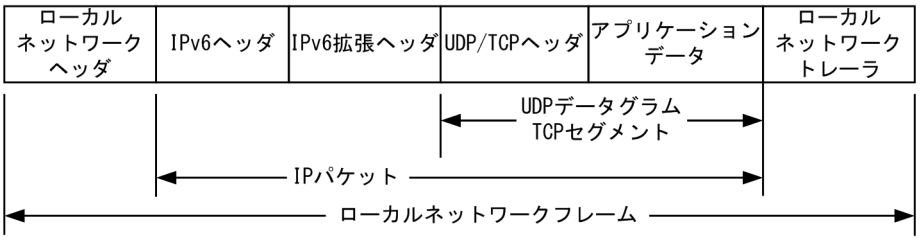
本装置では VLAN に対して IPv6 アドレスを設定します。IPv6 では一つのインタフェースに複数の IPv6 アドレスを設定することができ，IPv6 アドレスを設定した VLAN には自動的に IPv6 リンクローカルアドレスが付与されます。ただし，リンクローカルアドレスをコンフィグレーションで設定した場合を除きます。

32.1.3　インターネットプロトコル　バージョン 6 (IPv6)

(1)　IPv6 パケットフォーマット

本装置が送信する IPv6 パケットのフォーマットおよび設定値は RFC8200 に従います。IPv6 パケットフォーマットを次の図に示します。

図 32-20　IPv6 パケットフォーマット



(2)　IPv6 パケットヘッダ有効性チェック

IPv6 では 40 オクテット長のヘッダに，8 個のフィールドと 2 個のアドレスが含まれます。IPv6 ヘッダ形式を次の図に示します。

図 32-21　IPv6 ヘッダ形式

・バージョン(4ビット)　IPバージョンを示す領域
・トラフィッククラス(8ビット)　クラス，優先度の特定および識別
・フローラベル(20ビット)　パケットの属するフローの番号
・ペイロード長(16ビット)　オクテット単位で示したペイロード長
・次ヘッダ(8ビット)　IPv6ヘッダ直後に続くヘッダの種別
・ホップリミット(8ビット)　中継限界数
・始点アドレス(128ビット)　パケットの送信元アドレス
・終点アドレス(128ビット)　パケットの宛先アドレス

IPv6 パケット受信時に IPv6 パケットヘッダの有効性チェックを行います。IPv6 パケットヘッダのチェック内容を次の表に示します。

表 32-4　IPv6 パケットヘッダのチェック内容

IPv6 パケット ヘッダフィールド	チェック内容	チェック異常時 パケット処理	パケット廃棄時 ICMPv6 送信
バージョン	バージョン＝6 であること	廃棄する	送出しない
トラフィッククラス	チェックしない	－	－
フローラベル	チェックしない	－	－
ペイロード長	パケット長と比較する パケット長<ペイロード長	廃棄する	送出しない
	パケット長と比較する パケット長≧ペイロード長	パケットの後部をペイロード長で削除する	送出しない
次ヘッダ	チェックしない	－	－
ホップリミット	自装置宛てアドレスの受信パケットのホップリミットチェックしない	－	－
送信元アドレス	次の条件を満たすこと 1. リンクローカルアドレスでないこと 2. マルチキャストアドレスでないこと	廃棄する	送出しない
宛先アドレス	次の条件を満たすこと 1. ループバックアドレスでないこと	廃棄する	送出しない

IPv6 パケット ヘッダフィールド	チェック内容	チェック異常時 パケット処理	パケット廃棄時 ICMPv6 送信
	2. インタフェース ID 部が 0 でないこと(ただし，未定義アドレスを除く)		

(凡例)　－：該当しない

(3)　IPv6 拡張ヘッダサポート仕様

本装置がサポートする IPv6 拡張ヘッダの項目を次の表に示します。

表 32-5　IPv6 拡張ヘッダの項目

IPv6 拡張ヘッダ	IPv6 パケットの分類	
	本装置が発局となるパケット	本装置が着局となるパケット※
Hop-by-Hop Options Header	○	○
Routing Header	○	○
Fragment Header	○	○
Authentication Header	×	×
Encapsulating Security Payload Header	×	×
Destination Options Header	○	○

(凡例)　○：サポートする　×：サポートしない　－：ヘッダ処理なし

注※

本装置が着信するパケットが次の条件に該当する場合，パケットは廃棄されます。

・拡張ヘッダが 9 個以上設定されたパケット

・一つの拡張ヘッダ内に 9 個以上のオプションが設定されたパケット

32.1.4　ICMPv6

本装置が送信する ICMPv6 メッセージのフォーマットおよび設定値は RFC4443 に従います。ICMPv6 メッセージのサポート仕様を次の表に示します。

表 32-6　ICMPv6 メッセージサポート仕様

ICMPv6 メッセージ				サポート
タイプ(種別)	値 (10 進)	コード(詳細種別)	値 (10 進)	
Destination Unreachable	1	no route to destination	0	○
		communication with destination administratively prohibited	1	－
		beyond scope of source address	2	－
		address unreachable	3	－

ICMPv6 メッセージ				サポート
タイプ(種別)	値 (10 進)	コード(詳細種別)	値 (10 進)	
		port unreachable	4	○
Packet Too Big	2	−	0	−
Time Exceeded	3	hop limit exceeded in transit	0	−
		fragment reassembly time exceeded	1	−
Parameter Problem	4	erroneous header field encountered	0	○
		unrecognized Next Header type encountered	1	○
		unrecognized IPv6 option encountered	2	○
Echo Request	128	−	0	○
Echo Reply	129	−	0	○
Multicast Listener Query	130	−	0	○
Multicast Listener Report	131	−	0	○
Multicast Listener Done	132	−	0	○
Router Solicitation	133	−	0	○
Router Advertisement	134	−	0	○
Neighbor Solicitation	135	−	0	○
Neighbor Advertisement	136	−	0	○
Redirect	137	−	0	−
ICMP Node Information Response	140	A successful reply. The Reply Data field may or may not be empty	0	−

(凡例)　○：サポートする　−：該当しない

32.1.5　NDP

本装置が送信する NDP フレームのフォーマット，および設定値は RFC4861 に従います。

(1)　NDP エントリの削除条件

次の条件のどれかを満たす場合，該当する NDP エントリを削除します。ただし，コンフィグレーションで設定されたスタティック NDP エントリは削除しません。

- NDP エントリに対応する IPv6 アドレスとの通信が停止した後，10 分が経過した場合
- ステータス状態が stale の NDP エントリに対応する IPv6 アドレスへ通信が再開されたときに到達性がなかった場合
- インタフェース状態が Down となった場合の該当するインタフェースに存在する全 NDP エントリ

(2)　スタティック NDP 情報の設定

NDP プロトコルを持たない製品を接続するために，イーサネットの MAC アドレスと IPv6 アドレスの対応(スタティック NDP 情報)をコンフィグレーションコマンド ipv6 neighbor で設定できます。

(3)　NDP 情報の参照

運用端末から show ipv6 neighbors コマンドで NDP 情報が参照できます。NDP 情報から該当するインタフェースの IPv6 アドレスと MAC アドレスの対応がわかります。

32.1.6　RA

RA（Router Advertisement）は，ルータが端末群に IPv6 アドレス生成に必要な情報やデフォルト経路を配布する機能です。

ルータはアドレスのプレフィックス部だけを一定間隔で配布し，受信した各端末は，端末固有のインタフェース ID 部と RA のプレフィックス情報からアドレスを生成します。こうした特徴によって，RA はサーバレスで端末数に依存しない簡便な Plug & Play を実現します。

本装置では，コンフィグレーションコマンド ipv6 nd accept-ra 設定時，RA 受信による IPv6 アドレスの自動生成が可能です。ルータからプレフィックス部を受信し，装置 MAC アドレスをインタフェース ID として付加した IPv6 グローバルアドレスを自動生成し，受信したインタフェースに設定します。同時に RA 送信元アドレス（=RA を送信したルータのインタフェースリンクローカルアドレス）をデフォルトゲートウェイとして設定します。このデフォルトゲートウェイは，コンフィグレーションコマンド ipv6 route によるデフォルトゲートウェイの設定よりも優先して使用します。

RA で受信した情報が収容条件を超えた場合は，先に受信した情報を優先します。

32.1.7　IPv6 使用時の注意事項

(1)　IPv6 を設定したインタフェースの MTU 長の変更

IPv6 の最小パケット長は 1280 バイト以上と規定されています(RFC8200)。そのため，MTU 長を 1280 バイト未満に設定すると，IPv6 通信ができません。IPv6 通信を行うインタフェースの MTU 長は 1280 バイト以上で使用してください。

(2)　IPv6 アドレス重複

IPv6 には RFC4862 で規定されている DAD (Duplicate Address Detection) 機能があります。DAD でアドレスが重複した場合，その IPv6 アドレスでは通信できません。show ipv6 interface コマンドまたは show ip-dual interface コマンドで表示される IPv6 アドレスの横に duplicated と表示された場合，その IPv6 アドレスは他装置と重複していますので，次のように対応してください。

- 他装置の IPv6 アドレスが誤っている場合

  他装置の IPv6 アドレスを修正後，本装置の IPv6 アドレスをいったん削除して再度設定するか，VLAN インタフェースを一度ダウンさせてからアップさせてください。
- 本装置の IPv6 アドレスが誤っている場合

  コンフィグレーションで本装置の重複している IPv6 アドレスを削除して，正しい IPv6 アドレスを設定してください。
- 自動生成された IPv6 アドレスが重複する場合

VLAN インタフェースでループ構成が発生しているか，本装置の IPv6 アドレスになりすましている端末があります。要因を取り除いてから, いったん no ipv6 enable コマンドを実行後, 再度 ipv6 enable コマンドを実行してください。

(3) スタティック NDP についての注意事項

本装置のインタフェースに設定された IPv6 アドレスと重複するスタティック NDP を設定すると，通信ができなくなるなど，装置の挙動が不安定になります。このため，本装置では，コンフィグレーション入力時にインタフェースの IPv6 アドレスとスタティック NDP の重複チェックを実行しますが，次に示す IPv6 アドレスについては重複チェックが行われません。

- リンクローカルアドレス（自動生成および手動設定）
- インタフェース ID 省略時に自動生成されるグローバルアドレス

したがって，インタフェースに設定されたこれらの IPv6 アドレスと同じスタティック NDP を設定しないようにしてください。誤って設定した場合は，該当スタティック NDP を削除して，該当インタフェースの VLAN をリスタートしてください。

32.2　コマンドガイド

32.2.1　コマンド一覧

IPv6 通信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 32-7　コンフィグレーションコマンド一覧

コマンド名	説明
ipv6 address	IPv6 アドレスを設定します。
ipv6 enable	インタフェースの IPv6 機能を有効にします。このコマンドによって，リンクローカルアドレスが自動生成されます。
ipv6 icmp error-interval	ICMPv6 エラーの送信間隔を指定します。
ipv6 nd accept-ra	ルータ広告メッセージを受信し，ステートレスアドレス自動生成を実行します。
ipv6 neighbor	スタティック NDP テーブルを作成します。
ipv6 route	IPv6 スタティック経路を生成します。
interface loopback※	ループバックインタフェース階層に移動します。
ipv6 address（loopback）※	ループバックインタフェースの IPv6 アドレスを指定します。

注※
「コンフィグレーションコマンドレファレンス」「24　ループバックインタフェース」を参照してください。

IPv6 通信の運用コマンド一覧を次の表に示します。

表 32-8　運用コマンド一覧

コマンド名	説明
show ip-dual interface	IPv4 および IPv6 インタフェースの状態を表示します。
show ipv6 interface	IPv6 インタフェースの状態を表示します。
show ipv6 neighbors	NDP 情報を表示します。
clear ipv6 neighbors	ダイナミック NDP 情報をクリアします。
show netstat (netstat)	ネットワークのステータスを表示します。
ping ipv6	ICMP6 エコーテストを行います。
traceroute ipv6	IPv6 経由ルートを表示します。
show ipv6 route	IPv6 のルーティングテーブルを表示します。
show ipv6 router-advertisement	ルータ広告メッセージ受信によるアドレスおよびデフォルト経路情報を表示します。
show tcpdump	本装置に対して送受信されるパケットをモニタします。

32.2.2 インタフェースの設定

[設定のポイント]

VLAN に IPv6 アドレスを設定します。1 インタフェース当たり七つまでのアドレスが指定できます。ipv6 enable コマンドを設定して，IPv6 機能を有効にする必要があります。ipv6 enable コマンドの設定がない場合，IPv6 設定は無効になります。

[コマンドによる設定]

1. **(config)# interface vlan 100**
   VLAN ID 100 の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)# ipv6 enable**
   VLAN ID 100 に IPv6 アドレス使用可を設定します。
3. **(config-if)# ipv6 address 2001:db8:100::1/64**
   VLAN ID 100 に IPv6 アドレス 2001:db8:100::1，プレフィックス長 64 を設定します。
4. **(config-if)# ipv6 address 2001:db8:200::1/64**
   VLAN ID 100 に IPv6 アドレス 2001:db8:200::1，プレフィックス長 64 を追加します。

32.2.3 リンクローカルアドレスの手動設定

[設定のポイント]

本装置ではコンフィグレーションコマンドの ipv6 enable 実行時に，リンクローカルアドレスを自動生成します。リンクローカルアドレスは，1 インタフェース当たり一つだけ使用でき，手動で設定することもできます。

[コマンドによる設定]

1. **(config)# interface vlan 100**
   VLAN ID 100 の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)# ipv6 enable**
   VLAN ID 100 に IPv6 アドレスの使用可を設定します。このとき，リンクローカルアドレスが自動生成されます。
3. **(config-if)# ipv6 address fe80::1 link-local**
   VLAN ID 100 の自動生成されたリンクローカルアドレスを fe80::1 に変更します。

32.2.4 ループバックインタフェースの設定

[設定のポイント]

装置を識別するための IPv6 アドレスを設定します。インタフェース番号には 0 だけが指定でき，設定できるアドレスは一つだけです。

[コマンドによる設定]

1. **(config)# interface loopback 0**
   ループバックの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)# ipv6 address 2001:db8::1**
   装置に IPv6 アドレス 2001:db8::1 を設定します。

32.2.5　スタティック NDP の設定

[設定のポイント]

本装置にスタティック NDP を設定します。

[コマンドによる設定]

1. **(config)# ipv6 neighbor 2001:db8:100::2 interface vlan 100 0012.e240.0a00**
   VLAN ID 100 にネクストホップ IPv6 アドレス 2001:db8:100::2，接続先 MAC アドレス 0012.e240.0a00 でスタティック NDP を設定します。

32.2.6　RA の設定

[設定のポイント]

本装置で RA 受信時に IPv6 アドレスを自動生成するように設定します。

[コマンドによる設定]

1. **(config)# interface vlan 200**
   VLAN ID 200 の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)# ipv6 nd accept-ra default-gateway**
   VLAN ID 200 で RA 受信によって IPv6 アドレスを自動生成するように設定します。

33 DHCP サーバ機能

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。この章では，DHCP サーバ機能の解説およびコンフィグレーションについて説明します。

33.1　解説

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。この節では，本装置の DHCP サーバ機能の仕様および動作内容を説明します。

33.1.1　サポート仕様

本装置の 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での直結，および DHCP リレーエージェント経由で行います。

表 33-1　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収容
BOOTP サーバ機能	未サポート
ダイナミック DNS 連携	サポート なお，本装置で対応しているのは RFC2136 の DNS UPDATE を使用したダイナミック DNS サーバです。
動的/固定 IP アドレス配布機能	サポート

33.1.2　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 33-2　本装置でクライアントに配布する情報の一覧

情報名	概要
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 アドレスのリストを指定します。リストは優先度の高いものから順に指定します。このリスト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) なお，本オプションをコンフィグレーションで指定しなかった場合，ルータオプションを含めない代わりに，配布する IP アドレスと同じ値をルータオプションに設定してクライアントに返します。
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 アドレスのリストを指定します。リストは優先度の高いものから順に指定します。(Option No：6)

情報名	概要
ホストネームオプション	サーバでクライアントの名前を指定するときに設定します。名前はローカルドメイン名で制限される可能性があります。指定は文字列で行われます。(Option No：12)
ドメイン名オプション	クライアントがドメインネームシステムによってホスト名を変換するときに使用するドメイン名を指定します。(Option No：15)
NetBIOS over TCP/IP ネームサーバオプション	クライアントが参照する NetBIOS ネームサーバ(WINS サーバ)を IP アドレスのリストで指定します。 リストは優先度の高いものから順に指定します。(Option No：44)
NetBIOS over TCP/IP ノードタイプ指定オプション	NetBIOS オーバー TCP/IP クライアントのノードタイプ(NetBIOS 名前解決方法)を設定します。(Option No：46) • コード 1　B ノード(ブロードキャストノード) • コード 2　P ノード(Peer to Peer ノード(WINS を使用)) • コード 4　M ノード(ミックスノード(ブロードキャストで見つからない場合に WINS を使用する)) • コード 8　H ノード(ハイブリッドノード(WINS で見つからない場合に，ブロードキャストを使用する))

33.1.3　ダイナミック DNS 連携

本装置の DHCP サーバは IP アドレス配布と同時にダイナミック DNS サーバに対してエントリレコードを追加する機能（DNS 更新）に対応しています。この機能を使用するには DHCP サーバで対象とするゾーンと要求先 DNS サーバを指定した上で，DNS サーバ側も本装置からのレコード更新を受け付けるように設定する必要があります。

レコード更新の許可には IP アドレスによる許可と HMAC-MD5 の認証キーを使用する方法があります。IP アドレスによる許可は DNS サーバに接続している IP アドレスまたはネットワークからのアクセスを DNS サーバ側で許可するだけですが，認証キーを使用する場合は DNS サーバで指定されたキーと同じキーを DHCP サーバの DNS 認証キー情報に設定する必要があります。

ダイナミック DNS 連携時の注意事項

- 本装置の DHCP サーバでは動的に割り当てる IP アドレスだけ DNS 更新を行います。固定アドレスで配布を行う場合は事前に DNS サーバにレコードを追加してください。
- DNS 更新を行うには IP アドレス配布時に DHCP クライアントが FQDN を DHCP サーバに返す必要があります。必要な情報がない場合，DHCP サーバはそのリースに対する DNS 更新を行いません。具体的な設定については，クライアントに使用する装置の設定方法を参照してください。
- DNS 更新で認証キーを使用する場合，DNS サーバと本装置の時刻情報が一致している必要があります。多くの場合，時刻情報の誤差は UTC 時間で 5 分以下である必要があるため，NTP による時刻情報の同期を行ってください。

33.1.4　IP アドレスの二重配布防止

本装置の DHCP サーバのサービス（DHCP クライアントにアドレスを割り当てた状態）中に本装置が再起動した場合，本装置上にある DHCP アドレスプールはすべて「空き状態」になります。しかし，そのあと本装置が IP アドレスを割り当てる際，事前に割り当てた IP アドレスに対して ICMP エコー要求パケットを送出し，その応答パケットの有無によってすでに使用しているクライアントがいないかを確認し，IP ア

ドレスの二重割り当てを防止します。同時に，以前 IP アドレスを割り当てたクライアントに対しては同じ IP アドレスを割り当てようとするため，クライアントの通信には影響を与えません。

また，ICMP エコー要求パケットの応答が返ってきた（ネットワーク上の端末がすでにその IP アドレスを使っている）場合，show ip dhcp conflict コマンドの実行結果画面に衝突アドレス検出として表示します。

33.1.5　DHCP サーバ機能使用時の注意事項

DHCP サーバ機能使用時の注意事項について説明します。

(1)　マルチホーム接続時の入力インタフェースの IP アドレス

マルチホーム接続では，プライマリ IP アドレスを入力インタフェースの IP アドレスとします。このサブネットに設定している DHCP アドレスプールから IP アドレスを DHCP クライアントに割り当てます。

(2)　リース時間を短くした場合の同時接続数

リース時間を 10 秒とした場合のクライアント最大接続数は 200 以下となるようにしてください。同様に 20 秒とした場合は 400 以下，30 秒の場合は 600 以下となるように同時接続数を調整してください。

33.2　コマンドガイド

33.2.1　コマンド一覧

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 33-3　コンフィグレーションコマンド一覧

コマンド名	説明
client-name	クライアントに配布するホスト名オプションを指定します。ホスト名オプションは，固定 IP アドレス配布でクライアントが使用するホスト名として使われます。
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 アドレスのリストです。
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指定します。ドメインネームサーバオプションは，クライアントで利用可能な DNS サーバの IP アドレスリストです。
domain-name	クライアントに配布するドメインネームオプションを指定します。ドメインネームオプションは，クライアントで配布 IP アドレスに対する名称解決をドメインネームシステムで行う場合に，クライアントが使うべきドメインネームとして使用されます。
hardware-address	クライアント装置に固定の IP アドレスを配布する際に，対象となる装置の MAC アドレスを指定します。本コマンドはホストコマンドとセットで使用します。
host	クライアント装置に固定の IP アドレスを配布する際に，割り当てる IP アドレスを指定します。本コマンドはハードウェアアドレスコマンドとセットで使用します。
ip dhcp dynamic-dns-update	IP アドレス配布時，ダイナミック DNS 連携を有効にするかどうかを設定します。
ip dhcp excluded-address	network コマンドで指定した DHCP アドレスプールのうち，配布対象から除外とする IP アドレスの範囲を指定します。
ip dhcp key	ダイナミック DNS 使用時, DNS サーバとの認証で使用する認証キーを設定します。
ip dhcp pool	DHCP アドレスプール情報を設定します。
ip dhcp zone	ダイナミック DNS 使用時，DNS 更新を行うゾーンの情報を設定します。
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。
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。
netbios-name-server	クライアントに配布する NetBIOS ネームサーバオプションを指定します。NetBIOS ネームサーバオプションは，クライアントで利用可能な NetBIOS ネームサーバ（NBNS//WINS サーバ）の IP アドレスリストです。

コマンド名	説明
netbios-node-type	クライアントに配布する NetBIOS ノードタイプオプションを指定します。NetBIOS ノードタイプオプションは，クライアントが NetBIOS オーバー TCP/IP での名前解決を行う方法を指定します。
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。
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。

DHCP サーバの運用コマンド一覧を次の表に示します。

表 33-4　運用コマンド一覧

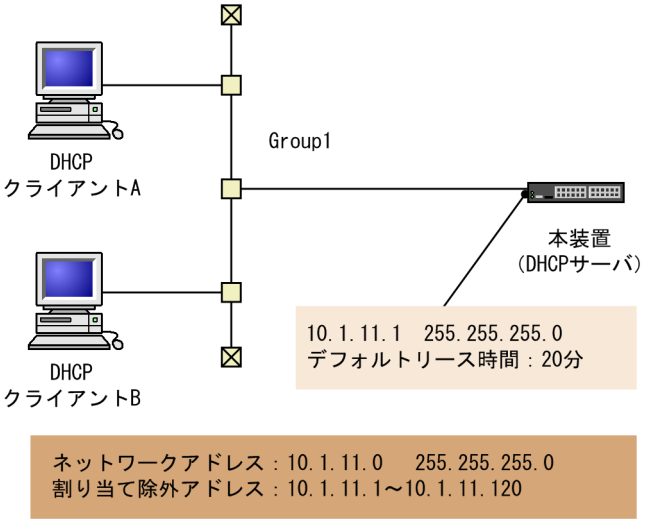
コマンド名	説明
show ip dhcp binding	DHCP サーバ上の結合情報を表示します。
clear ip dhcp binding	DHCP サーバのデータベースから結合情報を削除します。
show ip dhcp import	DHCP サーバのコンフィグレーションで設定されたオプション/パラメータ値を表示します。
show ip dhcp conflict	DHCP サーバによって検出した衝突 IP アドレス情報を表示します。衝突 IP アドレスとは，DHCP サーバの DHCP アドレスプールでは空きとなっていますが，すでにネットワーク上の端末に割り当てられている IP アドレスを指します。衝突 IP アドレスは，DHCP サーバが DHCP クライアントに対して IP アドレスを割り当てる前に ICMP パケット送出の応答有無によって検出します。
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。
restart dhcp	DHCP サーバデーモンプロセスを再起動します。
dump protocols dhcp	DHCP サーバプログラムで採取しているサーバのログおよびパケットの送受信ログをファイルへ出力します。
dhcp server monitor	DHCP サーバで送受信するパケットの送受信ログの採取を開始します。
no dhcp server monitor	DHCP サーバプログラムでのパケットの送受信ログの採取を停止します。

33.2.2　クライアントに IP を配布する設定

［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 33-1　クライアントーサーバ構成（動的 IP アドレス配布時）



[コマンドによる設定]

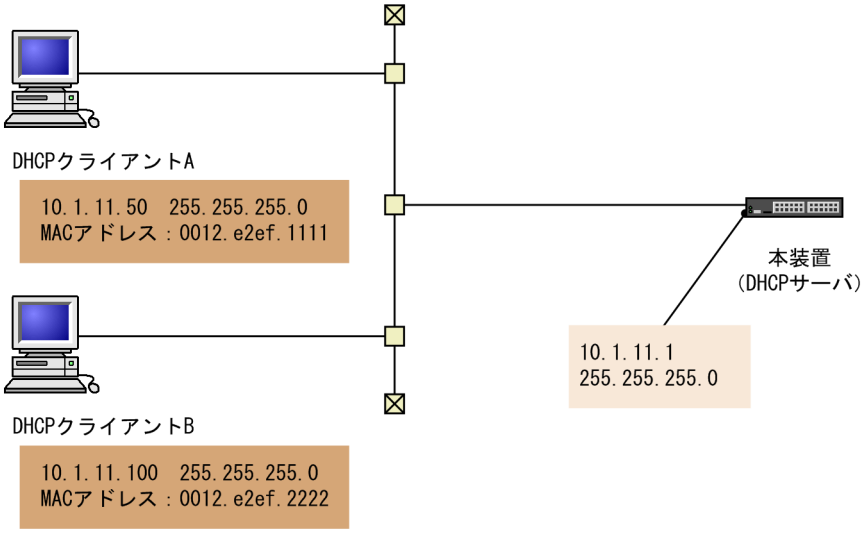
1. **(config)# interface vlan 10**
   (config-if)# ip address 10.1.11.1 255.255.255.0
   (config-if)# exit
   あらかじめ VLAN インタフェースと IP アドレスを設定しておきます。
2. **(config)# service dhcp vlan 10**
   DHCP サーバを有効にする VLAN インタフェース名称を指定します。
3. **(config)# ip dhcp excluded-address 10.1.11.1 10.1.11.120**
   DHCP サーバが DHCP クライアントに割り当てから除外する IP アドレスを設定します。
4. **(config)# ip dhcp pool Group1**
   DHCP アドレスプールを設定します。
   DHCP コンフィグレーションモードへ移行します。
5. **(dhcp-config)# network 10.1.11.0 255.255.255.0**
   DHCP アドレスプールのネットワークアドレスを設定します。
6. **(dhcp-config)# lease 0 0 20**
   DHCP アドレスプールのデフォルトリース時間に 20 分を設定します。
7. **(dhcp-config)# default-router 10.1.11.1**
   サブネット上にあるルータの IP アドレスを設定します。

33.2.3　クライアントに固定 IP を配布する設定

[設定のポイント]

DHCP クライアントごとに IP アドレスを固定で配布するために，クライアントごとに IP アドレスと MAC アドレスを設定します。

図 33-2　クライアントーサーバ構成（固定 IP アドレス配布時）



[コマンドによる設定]

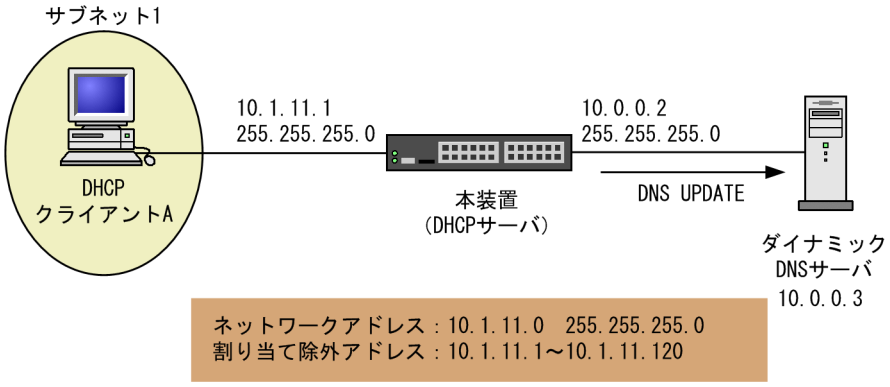
1. **(config)# interface vlan 10**
   (config-if)# ip address 10.1.11.1 255.255.255.0
   (config-if)# exit
   あらかじめ VLAN インタフェースと IP アドレスを設定しておきます。
2. **(config)# service dhcp vlan 10**
   DHCP サーバを有効にする VLAN インタフェース名称を指定します。
3. **(config)# ip dhcp pool Client1**
   DHCP クライアント A の DHCP アドレスプール名称を設定します。
   DHCP コンフィグレーションモードへ移行します。
4. **(dhcp-config)# host 10.1.11.50 255.255.255.0**
   DHCP クライアント A の DHCP アドレスプールに対する固定 IP アドレスを設定します。
5. **(dhcp-config)# hardware-address 0012.e2ef.1111 ethernet**
   DHCP クライアント A の DHCP アドレスプールに対する MAC アドレスを設定します。
6. **(dhcp-config)# default-router 10.1.11.1**
   (dhcp-config)# exit
   サブネット上のルータ IP アドレスを設定します。
7. **(config)# ip dhcp pool Client2**
   (dhcp-config)# host 10.1.11.100 255.255.255.0
   (dhcp-config)# hardware-address 0012.e2ef.2222 ethernet
   (dhcp-config)# default-router 10.1.11.1
   項番 3 から 6 と同様に，DHCP クライアント B にも DHCP アドレスプール名称，固定 IP アドレス，MAC アドレスを設定します。

33.2.4　ダイナミック DNS 連携時の設定

[設定のポイント]

クライアントに対して IP アドレスを配布した際に，クライアントに対応する DNS レコードをダイナミック DNS サーバに通知できるように，ゾーン情報の設定とダイナミック DNS サーバ連携を有効にします。

図 33-3　ダイナミック DNS 連携をする場合の接続構成



[コマンドによる設定]

1. **(config)# interface vlan 10**
   (config-if)# ip address 10.1.11.1 255.255.255.0
   (config-if)# exit
   あらかじめサブネット 1 の VLAN インタフェースと IP アドレスを設定しておきます。
2. **(config)# interface vlan 20**
   (config-if)# ip address 10.0.0.2 255.255.255.0
   (config-if)# exit
   項番 1 と同様に，あらかじめダイナミック DNS サーバの VLAN インタフェースと IP アドレスを設定しておきます。
3. **(config)# service dhcp vlan 10**
   (config)# ip dhcp excluded-address 10.1.11.1 10.1.11.120
   (config)# ip dhcp pool Group1
   (dhcp-config)# network 10.1.11.0 255.255.255.0
   (dhcp-config)# default-router 10.1.11.1
   「33.2.2　クライアントに IP を配布する設定」と同様に IP アドレスを設定します。
4. **(dhcp-config)# domain-name example.net**
   ドメインネームシステムでホスト名称を解決しているときに，クライアントが使うべきドメインネームを設定します。
5. **(dhcp-config)# dns-server 10.0.0.3**
   クライアントが利用可能な DNS サーバの IP アドレスを設定します。
6. **(dhcp-config)# exit**
   DHCP コンフィグレーションモードからグローバルコンフィグレーションモードへ移行します。
7. **(config)# ip dhcp zone example.net. primary 10.0.0.3**

正引きドメイン example.net.に対するゾーン情報を設定し，ダイナミック DNS サーバに 10.0.0.3 を設定します。

8. **(config)# ip dhcp zone 11.1.10.in-addr.arpa. primary 10.0.0.3**

   逆引きドメイン 11.1.10.in-addr.arpa.に対するゾーン情報を設定し，ダイナミック DNS サーバに 10.0.0.3 を設定します。

9. **(config)# ip dhcp dynamic-dns-update**

   ダイナミック DNS 連携を有効にします。

付録

付録 A　準拠規格

付録 A.1　TELNET/FTP

表 A–1　TELNET/FTP の準拠する規格および勧告

規格番号(発行年月)	規格名
RFC854(1983 年 5 月)	TELNET PROTOCOL SPECIFICATION
RFC855(1983 年 5 月)	TELNET OPTION SPECIFICATIONS
RFC959(1985 年 10 月)	FILE TRANSFER PROTOCOL (FTP)

付録 A.2　RADIUS/TACACS+

表 A–2　RADIUS/TACACS+の準拠する規格および勧告

規格番号(発行年月)	規格名
RFC2865(2000 年 6 月)	Remote Authentication Dial In User Service(RADIUS)
RFC2866(2000 年 6 月)	RADIUS Accounting
draft-grant-tacacs-02 (1997 年 1 月)	The TACACS+ Protocol Version 1.78

付録 A.3　SSH

表 A–3　SSH の準拠する規格および勧告

規格番号(発行年月)	規格名
RFC4251(2006 年 1 月)	The Secure Shell (SSH) Protocol Architecture
RFC4252(2006 年 1 月)	The Secure Shell (SSH) Authentication Protocol
RFC4253(2006 年 1 月)	The Secure Shell (SSH) Transport Layer Protocol
RFC4254(2006 年 1 月)	The Secure Shell (SSH) Connection Protocol
RFC4344(2006 年 1 月)	The Secure Shell (SSH) Transport Layer Encryption Modes
RFC4419(2006 年 3 月)	Diffie-Hellman Group Exchange for the Secure Shell (SSH) Transport Layer Protocol
RFC4716(2006 年 11 月)	The Secure Shell (SSH) Public Key File Format
RFC5656(2009 年 12 月)	Elliptic Curve Algorithm Integration in the Secure Shell Transport Layer
RFC6668(2012 年 7 月)	SHA-2 Data Integrity Verification for the Secure Shell (SSH) Transport Layer Protocol
RFC8268(2017 年 12 月)	More Modular Exponentiation (MODP) Diffie-Hellman (DH) Key Exchange (KEX) Groups for Secure Shell (SSH)

規格番号(発行年月)	規格名
draft-ylonen-ssh-protocol-00 (1995 年 11 月)	The SSH (Secure Shell) Remote Login Protocol
draft-ietf-secsh-filexfer-13 (2006 年 7 月)	SSH File Transfer Protocol

付録 A.4　NTP

表 A–4　NTP の準拠する規格および勧告

規格番号(発行年月)	規格名
RFC5905(2010 年 6 月)	Network Time Protocol Version 4: Protocol and Algorithms Specification

付録 A.5　DNS

表 A–5　DNS リゾルバの準拠する規格および勧告

規格番号(発行年月)	規格名
RFC1034(1987 年 3 月)	Domain names - concepts and facilities
RFC1035(1987 年 3 月)	Domain names - implementation and specification

付録 A.6　EEE

表 A–6　EEE の準拠する規格および勧告

規格	規格名
IEEE802.3az (IEEE Std 802.3az-2010)	Media Access Control Parameters, Physical Layers, and Management Parameters for Energy-Efficient Ethernet

付録 A.7　SYSLOG

表 A–7　SYSLOG の準拠する規格および勧告

規格番号(発行年月)	規格名
RFC3164(2001 年 8 月)	The BSD Syslog Protocol
RFC5424(2009 年 3 月)	The Syslog Protocol

付録 A.8　SNMP

表 A–8　SNMP の準拠規格および勧告

規格番号(発行年月)	規格名
RFC1155(1990 年 5 月)	Structure and Identification of Management Information for TCP/IP-based Internets
RFC1157(1990 年 5 月)	A Simple Network Management Protocol (SNMP)
RFC1901(1996 年 1 月)	Introduction to Community-based SNMPv2
RFC1902(1996 年 1 月)	Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC1903(1996 年 1 月)	Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC1904(1996 年 1 月)	Conformance Statements for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC1905(1996 年 1 月)	Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC1906(1996 年 1 月)	Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC1907(1996 年 1 月)	Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC1908(1996 年 1 月)	Coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework
RFC2578(1999 年 4 月)	Structure of Management Information Version 2 (SMIv2)
RFC2579(1999 年 4 月)	Textual Conventions for SMIv2
RFC2580(1999 年 4 月)	Conformance Statements for SMIv2
RFC3410(2002 年 12 月)	Introduction and Applicability Statements for Internet Standard Management Framework
RFC3411(2002 年 12 月)	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
RFC3412(2002 年 12 月)	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
RFC3413(2002 年 12 月)	Simple Network Management Protocol (SNMP) Applications
RFC3414(2002 年 12 月)	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
RFC3415(2002 年 12 月)	View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
RFC3416(2002 年 12 月)	Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)

規格番号(発行年月)	規格名
RFC3417(2002 年 12 月)	Transport Mappings for the Simple Network Management Protocol (SNMP)
RFC3584(2003 年 8 月)	Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework
RFC3826(2004 年 6 月)	The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model
RFC7860(2016 年 4 月)	HMAC-SHA-2 Authentication Protocols in User-Based Security Model (USM) for SNMPv3

表 A-9　MIB の準拠規格および勧告

規格番号(発行年月)	規格名
IEEE8023-LAG-MIB(2000 年 3 月)	Aggregation of Multiple Link Segments
IEEE8021-PAE-MIB(2001 年 6 月)	Port-Based Network Access Control
IEEE8021-CFM-MIB(2007 年 12 月)	Virtual Bridged Local Area Networks Amendment 5: Connectivity Fault Management
LLDP-V2-MIB(2009 年 6 月)	Management Information Base module for LLDP configuration, statistics, local system data and remote systems data components.
RFC1158(1990 年 5 月)	Management Information Base for Network Management of TCP/IP-based internets: MIB-II
RFC1213(1991 年 3 月)	Management Information Base for Network Management of TCP/IP-based internets: MIB-II
RFC1493(1993 年 6 月)	Definitions of Managed Objects for Bridges
RFC1643(1994 年 7 月)	Definitions of Managed Objects for the Ethernet-like Interface Types
RFC1757(1995 年 2 月)	Remote Network Monitoring Management Information Base
RFC2233(1997 年 11 月)	The Interfaces Group MIB using SMIv2
RFC2674(1999 年 8 月)	Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions
RFC2934(2000 年 10 月)	Protocol Independent Multicast MIB for IPv4
RFC3411(2002 年 12 月)	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
RFC3412(2002 年 12 月)	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
RFC3413(2002 年 12 月)	Simple Network Management Protocol (SNMP) Applications
RFC3414(2002 年 12 月)	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)

規格番号(発行年月)	規格名
RFC3415(2002 年 12 月)	View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
RFC3418(2002 年 12 月)	Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)
RFC3621(2003 年 12 月)	Power Ethernet MIB
RFC4022(2005 年 3 月)	Management Information Base for the Transmission Control Protocol (TCP)
RFC4113(2005 年 6 月)	Management Information Base for the User Datagram Protocol (UDP)
RFC4293(2006 年 4 月)	Management Information Base for the Internet Protocol (IP)

付録 A.9　イーサネット

表 A-10　イーサネットインタフェースの準拠規格

種別	規格	名称
10BASE-T, 100BASE-TX, 1000BASE-T, 1000BASE-X, 2.5GBASE-T, 10GBASE-R	IEEE Std 802.3x-1997	IEEE Standards for Local and Metropolitan Area Networks:Specification for 802.3 Full Duplex Operation
	IEEE Std 802.2-1998	IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements - Part 2: Logical Link Control
	IEEE Std 802.3-2018	Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer Specifications
1000BASE-X	IEEE Std 802.3ah-2004	Amendment: Media Access Control Parameters, Physical Layers, and Management Parameters for Subscriber Access Networks
	IEEE Std 802.3z-1998	Media Access Control Parameters, Physical Layers, Repeater and Management Parameters for 1,000 Mb/s Operation, Supplement to Information Technology
2.5GBASE-T	IEEE Std 802.3bz-2016	Media Access Control Parameters, Physical Layers, and Management Parameters for 2.5 Gb/s and 5 Gb/s Operation, Types 2.5GBASE-T and 5GBASE-T
10GBASE-R	IEEE Std 802.3ae-2002	Media Access Control(MAC) Parameters, Physical Layer, and Management Parameters for 10 Gb/s Operation
	IEEE Std 802.3aq-2006	Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications

表 A-11　PoE の準拠規格

規格	名称
IEEE802.3af (IEEE Std 802.3af-2003)	Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications Amendment: Data Terminal Equipment (DTE) Power via Media Dependent Interface (MDI)
IEEE802.3at (IEEE Std 802.3at-2009)	Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications Amendment: Data Terminal Equipment (DTE) Power Via the Media Dependent Interface (MDI) Enhancements
IEEE802.3bt (IEEE Std 802.3bt-2018)	Physical Layer and Management Parameters for Power over Ethernet over 4 pairs

付録 A.10　リンクアグリゲーション

表 A-12　リンクアグリゲーションの準拠規格

規格	名称
IEEE802.1AX (IEEE Std 802.1AX-2008)	Aggregation of Multiple Link Segments

付録 A.11　VLAN

表 A-13　VLAN の準拠規格および勧告

規格	名称
IEEE802.1Q (IEEE Std 802.1Q-2003)	Virtual Bridged Local Area Networks※

注※　GVRP/GMRP はサポートしていません。

付録 A.12　スパニングツリー

表 A-14　スパニングツリーの準拠規格および勧告

規格	名称
IEEE802.1D (ANSI/IEEE Std 802.1D-1998 Edition)	Media Access Control (MAC) Bridges (The Spanning Tree Algorithm and Protocol)
IEEE802.1t (IEEE Std 802.1t-2001)	Media Access Control (MAC) Bridges - Amendment 1
IEEE802.1w (IEEE Std 802.1w-2001)	Media Access Control (MAC) Bridges - Amendment 2: Rapid Reconfiguration
IEEE802.1s (IEEE Std 802.1s-2002)	Virtual Bridged Local Area Networks - Amendment 3: Multiple Spanning Trees

付録 A.13　IGMP snooping/MLD snooping

表 A-15　IGMP snooping/MLD snooping の準拠規格および勧告

規格番号(発行年月)	規格名
RFC4541(2006 年 5 月)	Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches

付録 A.14　IPv4 通信

表 A-16　IPv4 通信の準拠規格および勧告

規格番号(発行年月)	規格名
RFC791(1981 年 9 月)	Internet Protocol
RFC792(1981 年 9 月)	Internet Control Message Protocol
RFC826(1982 年 11 月)	An Ethernet Address Resolution Protocol: Or converting network protocol addresses to 48.bit Ethernet address for transmission on Ethernet hardware
RFC922(1984 年 10 月)	Broadcasting Internet datagrams in the presence of subnets
RFC950(1985 年 8 月)	Internet Standard Subnetting Procedure
RFC1027(1987 年 10 月)	Using ARP to implement transparent subnet gateways
RFC1122(1989 年 10 月)	Requirements for Internet hosts-communication layers
RFC1519(1993 年 9 月)	Classless Inter-Domain Routing (CIDR):an Address Assignment and Aggregation Strategy
RFC1812(1995 年 6 月)	Requirements for IP Version 4 Routers

付録 A.15　IPv6 通信

表 A-17　IPv6 通信の準拠規格および勧告

規格番号(発行年月)	規格名
RFC2474(1998 年 12 月)	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers
RFC2710(1999 年 10 月)	Multicast Listener Discovery for IPv6
RFC4291(2006 年 2 月)	IP Version 6 Addressing Architecture
RFC4443(2006 年 3 月)	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification
RFC4861(2007 年 9 月)	Neighbor Discovery for IP Version 6 (IPv6)
RFC4862(2007 年 9 月)	IPv6 Stateless Address Autoconfiguration
RFC8200(2017 年 7 月)	Internet Protocol, Version 6 (IPv6) Specification

付録 A.16　DHCP サーバ機能

表 A-18　DHCP サーバ機能の準拠規格

規格番号(発行年月)	規格名
RFC2131(1997 年 3 月)	Dynamic Host Configuration Protocol
RFC2132(1997 年 3 月)	DHCP Options and BOOTP Vendor Extensions
RFC2136 (1997 年 4 月)	Dynamic Updates in the Domain Name System (DNS UPDATE)
RFC3679 (2004 年 1 月)	Unused Dynamic Host Configuration Protocol (DHCP) Option Codes

索引

数字

6to4 アドレス　496

A

absolute 方式〔MIB 監視〕　209
alarm グループ　209
ARP　484
ARP 情報の参照　485
ARP 情報の設定　485
ARP パケットのチェック内容　484
ARP パケットフォーマット　484
ARP パケット有効性チェック　484

C

CLI 環境情報　51
CLI 設定のカスタマイズ　51

D

delta 方式〔MIB 監視〕　209
DHCP snooping〔収容条件〕　31
DHCP サーバ機能　513
DHCP サーバ機能使用時の注意事項　516
DHCP サーバ機能のサポート仕様　514
DHCP サーバの運用コマンド一覧　518
DHCP サーバのコンフィグレーションコマンド一覧　517

E

EEE　184
EEE 機能　184
event グループ　211

G

GetBulkRequest オペレーション　199
GetNextRequest オペレーション　198
GetRequest オペレーション　197
Gratuitous ARP　485

H

history グループ　208

I

ICMP　482
ICMPv6　505
ICMPv6 メッセージサポート仕様　505
ICMP メッセージサポート仕様　482
ICMP メッセージフォーマット　482
IGMP snooping　457
IGMP snooping/MLD snooping 概要　455
IGMP snooping/MLD snooping 使用時の注意事項　468
IGMP snooping/MLD snooping の解説　453
IGMP snooping/MLD snooping の概要　454
IGMP snooping/MLD snooping の設定と運用　471
IGMP snooping および MLD snooping 概要　455
IGMP snooping の運用コマンド一覧　472
IGMP snooping のコンフィグレーションコマンド一覧　472
IGMPv1/IGMPv2 メッセージごとの動作　461
IGMPv3 メッセージごとの動作　461
IGMP クエリア機能〔IGMP snooping〕　462
IGMP 即時離脱機能〔IGMP snooping〕　462
Inform　207
IPv4 埋め込み IPv6 アドレス　497
IPv4 互換アドレス　495
IPv4 射影アドレス　496
IPv4 使用時の注意事項　486
IPv4 通信　479
IPv4 通信の運用コマンド一覧　487
IPv4 通信のコンフィグレーションコマンド一覧　487
IPv4 マルチキャストアドレスと MAC アドレスの対応　457
IPv4 マルチキャストパケットのレイヤ 2 中継〔IGMP snooping〕　458
IPv6 アドレス　492
IPv6 アドレス付与単位　503
IPv6 拡張ヘッダサポート仕様　505
IPv6 拡張ヘッダの項目　505
IPv6 グローバルアドレス　495
IPv6 サイトローカルアドレス　494
IPv6 使用時の注意事項　507
IPv6 通信　491
IPv6 通信の運用コマンド一覧　509
IPv6 通信のコンフィグレーションコマンド一覧　509
IPv6 パケットフォーマット　503
IPv6 パケットヘッダのチェック内容　504

IPv6 パケットヘッダ有効性チェック　503
IPv6 ヘッダ形式　504
IPv6 マルチキャストアドレスと MAC アドレスの対応　464
IPv6 マルチキャストアドレス〔IPv6 パケット中継〕　499
IPv6 マルチキャストパケットのレイヤ 2 中継〔MLD snooping〕　465
IPv6 リンクローカルアドレス　494
IPv6 を設定したインタフェースの MTU 長の変更　507
IPX 互換アドレス　496
IP アドレス　480
IP アドレスによるオペレーション制限　201
IP アドレスの設定〔本装置〕　71
IP アドレスの二重配布防止〔DHCP サーバ機能〕515
IP アドレスフォーマット　480
IP オプションサポート仕様　482
IP パケットフォーマット　481
IP パケットヘッダのチェック内容　481
IP パケットヘッダ有効性チェック　481

L

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コマンド一覧　355
LLC の扱い　264
LPI　184

M

MAC VLAN のコンフィグレーションコマンド一覧　340
MAC アドレス学習　307
MAC アドレス学習の運用コマンド一覧　312
MAC アドレス学習のコンフィグレーションコマンド一覧　312
MAC アドレスの学習〔IGMP snooping〕　457
MAC アドレスの学習〔MLD snooping〕　464
MAC 副層フレームフォーマット　264
MC 運用モード　159
MC 運用モードの運用コマンド一覧　163
MC 運用モードのコンフィグレーションコマンド一覧　163
MDI／MDI-X のピンマッピング　254
MIB オブジェクトの表し方　196
MIB 概説　195
MIB 構造　195
MIB 取得の例　192
MIB を設定できない場合の応答　199
MLD snooping　464
MLD snooping の運用コマンド一覧　476
MLD snooping のコンフィグレーションコマンド一覧　476
MLDv1 メッセージごとの動作　466
MLDv2 メッセージごとの動作　466
MLD クエリア機能〔MLD snooping〕　466

N

NDP　506
NDP エントリの削除条件　506
NDP 情報の参照　507
NSAP 互換アドレス　496

P

PoE　266
PVST+のコンフィグレーションコマンド一覧　378

R

RADIUS　82
RADIUS/TACACS+に関するコンフィグレーションコマンド一覧　107
RADIUS/TACACS+の解説　82
RADIUS/TACACS+の概要　82
RADIUS/TACACS+の適用機能および範囲　82
RADIUS のサポート範囲　83
RA の設定　511
Ring Protocol の運用コマンド一覧　444
Ring Protocol の解説　407
Ring Protocol のコンフィグレーションコマンド一覧　444
Ring Protocol の設定と運用　443
RMON MIB　208

S

SetRequest オペレーション　199
SNMP　191
SNMP/RMON に関する運用コマンド一覧　212
SNMP/RMON に関するコンフィグレーションコマンド一覧　212
SNMPv1，SNMPv2C オペレーション　197
SNMPv3 オペレーション　202
SNMPv3 でのオペレーション制限　205
SNMPv3 による MIB アクセス許可の設定　213
SNMP エージェント　192
SNMP エンジン　193
SNMP エンティティ　193

SNMP オペレーションのエラーステータスコード 202
SNMP 概説 192
SNMP マネージャとの接続時の注意事項 211
SSH(Secure Shell) 113
SSH クライアント機能の運用コマンド一覧 128
SSH サーバ機能の運用コマンド一覧 127
SSH サーバのコンフィグレーションコマンド一覧127
statistics グループ 208

T

TACACS+ 82
Tag 変換のコンフィグレーションコマンド一覧 352
Teredo IPv6 アドレス 497
Trap 206
TYPE／LENGTH フィールドの扱い 264

V

VLAN 315
VLAN debounce 機能のコンフィグレーションコマンド一覧 362
VLAN インタフェースのコンフィグレーションコマンド一覧 345
VLAN 拡張機能 347
VLAN 基本機能のコンフィグレーションコマンド一覧 322
VLAN トンネリングのコンフィグレーションコマンド一覧 350
VLAN の運用コマンド一覧 322
VLAN マッピング 437

あ

アップデートに関する運用コマンド一覧 175
アドレス自動生成例 502
アドレス表記方法 492
アドレスフォーマットプレフィックス 492
アドレスフォーマットプレフィックスの種類 493
アドレッシング 480

い

イーサネット 247
イーサネットの運用コマンド一覧 271
イーサネットのコンフィグレーションコマンド一覧 271
インターネットプロトコル(IP) 481
インターネットプロトコル バージョン 6 (IPv6) 503
インタフェース ID 省略時のアドレス自動生成 502
インタフェースの設定 488
インタフェースの設定〔IPv6〕 510
インデックス 196
インフォーム 207
インフォーム概説 207
インフォームリクエストフォーマット 208

う

運用端末の接続形態 38
運用端末の接続とリモート操作に関する運用コマンド一覧 71
運用端末の接続とリモート操作に関するコンフィグレーションコマンド一覧 71

え

エージングタイマ 485
エニキャストアドレス通信 498
エニキャストアドレス〔IPv6 アドレスの定義〕 498
エラーステータスコード 202

お

オプションライセンス 178
オプションライセンスに関する運用コマンド一覧 179

く

クライアントへの配布情報〔DHCP サーバ機能〕 514
グローバルアドレス 495

こ

高機能スクリプト 219
高機能スクリプトの運用コマンド一覧 226
高機能スクリプトのコンフィグレーションコマンド一覧 226
コマンド操作 45
コマンド入力モードの切り換えおよびユーティリティに関する運用コマンド一覧 46
コミュニティによるオペレーション 201
コミュニティによるオペレーション制限 201
コンソール 39
コンフィグレーション 55
コンフィグレーションの編集および操作に関する運用コマンド一覧 59
コンフィグレーションの編集および操作に関するコンフィグレーションコマンド一覧 59

さ

サイトローカルアドレス 494
サブネットマスク〔IP ネットワーク〕 480

サポート機能〔IGMP snooping/MLD snooping〕 456
サポート仕様〔DHCP サーバ機能〕 514

し

時刻設定および NTP に関する運用コマンド一覧 142
時刻設定および NTP に関するコンフィグレーションコマンド一覧 142
時刻の設定と NTP 135
自動 MDI/MDIX 機能 254
ジャンボフレーム 265
収容条件 15
受信フレームの廃棄条件 265
冗長化構成による高信頼化〔収容条件〕 32
省電力機能 183
省電力機能の運用コマンド一覧 185
省電力機能のコンフィグレーションコマンド一覧 185
シングルスパニングツリーのコンフィグレーションコマンド一覧 384

す

スタティック ARP の設定 488
スタティック NDP 情報の設定 507
スタティック NDP の設定 511
ステートレスアドレス自動設定機能 503
スパニングツリー 363
スパニングツリー共通機能のコンフィグレーションコマンド一覧 403
スパニングツリーの運用コマンド一覧 372
スパニングツリーのコンフィグレーションコマンド一覧 372

せ

接続インタフェース〔1000BASE-X〕 256
接続インタフェース〔10BASE-T／100BASE-TX／1000BASE-T〕 250
接続インタフェース〔10GBASE-R〕 257
接続時の注意事項〔1000BASE-X〕 257
接続時の注意事項〔10BASE-T／100BASE-TX／1000BASE-T〕 256
接続時の注意事項〔10GBASE-R〕 258
接続仕様〔1000BASE-X〕 257
接続仕様〔10BASE-T／100BASE-TX／1000BASE-T〕 250
接続仕様〔10GBASE-R〕 258
設定できないアドレス〔IPv6 アドレス〕 502
設定できるアドレス〔IPv6 アドレス〕 501
ゼロタッチプロビジョニング 165
ゼロタッチプロビジョニングの運用コマンド一覧 169
ゼロタッチプロビジョニングのコンフィグレーションコマンド一覧 169
全ノードアドレス 501
全ルータアドレス 501

そ

装置管理者モード変更のパスワードの設定 78
装置構成 5
装置の管理 151
装置へのログイン 37
装置を管理する上で必要な運用コマンド一覧 152
装置を管理する上で必要なコンフィグレーションコマンド一覧 152
ソフトウェアの管理 171

た

ダイナミック DNS 連携〔DHCP サーバ機能〕 515
ダイレクトアタッチケーブル 249
ダウンシフト機能 255
多重障害監視 VLAN 429
多重障害監視機能 428
多重障害監視フレーム 429

と

同時にログインできるユーザ数の設定 79
トラップ 206
トラップ概説 206
トラップの例 193
トラップフォーマット（SNMPv1） 206
トラップフォーマット（SNMPv2C, SNMPv3） 207

に

認証方式シーケンス（end-by-reject 設定時） 90
認証方式シーケンス（end-by-reject 未設定時） 89

ね

ネットワーク管理 192

は

廃棄プレフィックスアドレス 497
バックアップリング 428
バックアップ・リストアに使用する運用コマンド一覧 154
パッドの扱い 265

ひ

標準 MIB　195

ふ

フィルタ・QoS〔収容条件〕　27
プライベート MIB　195
フレームフォーマット　264
プレフィックス長で設定できる条件　502
フローコントロール　259
プロトコル VLAN のコンフィグレーションコマンド一覧　333

ほ

ポート VLAN のコンフィグレーションコマンド一覧　328
ポート間中継遮断機能のコンフィグレーションコマンド一覧　358
ポートの電力供給 OFF　184
ホスト名と DNS　147
ホスト名・DNS に関するコンフィグレーションコマンド一覧　149
本装置で使用する IPv6 アドレスの扱い　501
本装置の概要　1
本装置のサポート MIB　197

ま

マルチキャストアドレス通信　499
マルチキャストアドレスのスコープフィールド値 499
マルチキャストアドレス〔IPv6 アドレスの定義〕498
マルチキャストグループアドレス　454
マルチキャストルータとの接続〔IGMP snooping〕　459
マルチキャストルータとの接続〔MLD snooping〕465
マルチプルスパニングツリーのコンフィグレーションコマンド一覧　394
マルチホームの設定　488

み

未指定アドレス　495

ゆ

ユーザ認証と暗号化機能　193
ユニキャストアドレス通信　494
ユニキャストアドレス〔IPv6 アドレスの定義〕　493

よ

要請ノードアドレス　501
予約マルチキャストアドレス　500

り

リモート運用端末　40
リモート運用端末からのログインを許可する IP アドレスの設定　79
リモート運用端末から本装置へのログイン　69
リンクアグリゲーション　283
リンクアグリゲーション拡張機能のコンフィグレーションコマンド一覧　295
リンクアグリゲーション基本機能のコンフィグレーションコマンド一覧　287
リンクアグリゲーションの運用コマンド一覧　287
リンクアグリゲーション〔収容条件〕　18
リンクローカルアドレス　494
リンクローカルアドレスの手動設定　510

る

ループバックアドレス　495
ループバックインタフェースの設定　488
ループバックインタフェースの設定〔IPv6〕　510

れ

レイヤ 2 スイッチ概説　297
レイヤ 2 スイッチ〔収容条件〕　19
レイヤ 2 認証〔収容条件〕　29

ろ

ログイン制御の概要　77
ログインセキュリティと RADIUS/TACACS+　75
ログインセキュリティに関する運用コマンド一覧　76
ログインセキュリティに関するコンフィグレーションコマンド一覧　76
ログインユーザの作成と削除　77
ログ出力機能　187
ログ出力機能に関する運用コマンド一覧　189
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　189