AX8600R 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. 12.8 対応 Rev.2

AX86R-S001-A0

■ 対象製品

このマニュアルは AX8600R を対象に記載しています。

■ 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，富士ゼロックス株式会社の登録商標です。
IPX は，Novell,Inc.の商標です。
Python(R)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。
イーサネットは，富士ゼロックス株式会社の登録商標です。
そのほかの記載の会社名，製品名は，それぞれの会社の商標もしくは登録商標です。

■ マニュアルはよく読み，保管してください。

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

■ ご注意

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

■ 発行

２０２０年　３月 （第１１版） ＡＸ８６Ｒ－Ｓ００１－Ａ０

■ 著作権

All Rights Reserved, Copyright(C), 2012, 2020, ALAXALA Networks, Corp.

変更内容

【Ver. 12.8 対応 Rev.2 版】

表　変更内容

章・節・項・タイトル	追加・変更内容
3.1.2　最大搭載数	•「(2) NIF 最大搭載数」の NLCG-1Q の搭載数を変更しました。
3.1.3　PRU と NIF の搭載	• NLCG-1Q の搭載条件を変更しました。
3.2　収容条件	•「3.2.12　マルチキャストルーティング」の「(2) PIM-SM 関連の収容条件」の記述を変更しました。
18.3.12　SFP+/SFP 共用ポートの設定	• NLXG-6RS および NLXGA-12RS についての記述を追加しました。

なお，単なる誤字・脱字などはお断りなく訂正しました。

【Ver. 12.8 対応 Rev.1 版】

表　変更内容

項目	追加・変更内容
ハードウェア	• NLCG-1Q の記述を追加しました。
最大搭載数	• NLCG-1Q の記述を追加しました。
PRU と NIF の搭載	• NLCG-1Q の記述を追加しました。
収容条件	•「マルチキャストルーティング」に NLCG-1Q の記述を追加しました。
ポートの種類とサポート機能	•「(1) ポートの種類」を追加しました。
100GBASE-R	• 100GBASE-SR4 の記述を追加しました。
SFP+/SFP 共用ポートの設定	• 本項を追加しました。

【Ver. 12.8 対応版】

表　変更内容

項目	追加・変更内容
収容条件	•「リモートアクセス」を追加しました。
SSH(SecureShell)	• 本章を追加しました。

【Ver. 12.7 対応 Rev.1 版】

表　変更内容

項目	追加・変更内容
ハードウェア	• NL1GA-12S の記述を追加しました。
最大搭載数	• NL1GA-12S の記述を追加しました。
PRU と NIF の搭載	• NL1GA-12S の記述を追加しました。
収容条件	•「フィルタ・QoS」にシェーパユーザ個別設定時の収容条件を追加しました。また，シェーパユーザ決定でのシェーパユーザ数に NL1GA-12S の記述を追加しました。 •「トラッキング機能」を追加しました。

項目	追加・変更内容
	• 「IP インタフェースと IP パケット中継」の「(9) VRRP」に，トラッキング連携でのトラック適用数の収容条件を追加しました。 • 「マルチキャストルーティング」に NL1GA-12S の記述を追加しました。
概要	• NL1GA-12S の記述を追加しました。

【Ver. 12.7 対応版】

表　変更内容

項目	追加・変更内容
ハードウェア	• NLXGA-12RS および NLXLG-4Q 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-SHPS および OP-SHPE の記述を追加しました。
最大収容ポート数	• NIF のサポートに伴って，記述を変更しました。
最大搭載数	• NLXGA-12RS および NLXLG-4Q の記述を追加しました。
PRU と NIF の搭載	• PRU と NIF の組み合わせによる NIF の搭載条件の記述を追加しました。
収容条件	• 「テーブルエントリ数」にカスタマイズ配分の記述を追加しました。 • 「経路配分パターン」にカスタマイズ配分の記述を追加しました。 • 「レイヤ 2 スイッチング」の「(3) VLAN」で，VLAN ポート数を変更しました。 • 「レイヤ 2 スイッチング」の「(5) Ring Protocol」で，装置当たりの Ring Protocol の収容条件を変更しました。 • 「フィルタ・QoS」に「(4) 階層化シェーパ」を追加しました。 • 「マルチキャストルーティング」に NLXGA-12RS および NLXLG-4Q の記述を追加しました。 • 「マルチキャストルーティング」の「(3) IGMP/MLD 関連の収容条件」で，IGMP PIM-SSM 連携機能の収容条件を変更しました。
装置のリソース設定	• カスタマイズ配分の記述を追加しました。
PE-NIF の設定	• 本項を追加しました。
PE サービスの確認	• 本項を追加しました。
オプションライセンスのコンフィグレーション	• 本節を追加しました。
オプションライセンスのオペレーション	• 本節を追加しました。
概要	• 40GBASE-R の記述を追加しました。
40GBASE-R	• 本項を追加しました。
イーサネットインタフェースの設定	• 40GBASE-R の記述を追加しました。

【Ver. 12.6 対応 Rev.1 版】

表　変更内容

項目	追加・変更内容
収容条件	• 「テーブルエントリ数」にポリシーベースミラーリングの記述を追加しました。 • 「フィルタ・QoS」に「(2) アクセスリストロギング」を追加しました。 • 「ネットワークの管理」に「(1) ポリシーベースミラーリング」を追加しました。
RADIUS/TACACS+/ローカルを使用したコマンド承認	• 常に実行できるコマンドから disable を削除しました。 • 常に実行できるコマンドに top および end を追加しました。 • コマンド承認で制限できるコマンドにコンフィグレーションコマンドを追加しました。

【Ver. 12.6 対応版】

表　変更内容

項目	追加・変更内容
ハードウェア	• PRU-2A の記述を追加しました。
収容条件	• 「テーブルエントリ数」に PRU-2A の記述を追加しました。 • 「リンクアグリゲーション」にロードバランスグループごとのポート振り分け使用時の収容条件を追加しました。 • 「IP インタフェースと IP パケット中継」のループバックインタフェース関連の値を変更しました。 • 「マルチキャストルーティング」の「(3) IGMP/MLD 関連の収容条件」で，IPv4 マルチキャストの IGMP/MLD PIM-SSM 連携機能の設定数（送信元アドレスとグループアドレスのペア数）を変更しました。また，マルチキャストチャネル参加制限機能についての記述を追加しました。
内蔵フラッシュメモリの未使用容量監視	• 本項を追加しました。
ソフトウェア障害検出時の動作	• 本項を追加しました。
VLAN Tag	• 「(3) TPID」を追加しました。
VLAN Tag の TPID 値の設定	• 「(2) ポート単位の TPID 値の設定」を追加しました。
フレーム送信時のポート振り分け	• 「(3) ロードバランスグループごとのポート振り分け」を追加しました。
振り分け方法の設定	• 「(3) ロードバランスグループごとのポート振り分け」を追加しました。

【Ver. 12.4 対応 Rev.1 版】

表　変更内容

項目	追加・変更内容
収容条件	• 「レイヤ 2 スイッチング」に IGMP/MLD snooping の記述を追加しました。 • 「ユニキャストルーティング」で経路フィルタ ip prefix-list および ipv6 prefix-list のコンフィグレーションの最大設定数を変更しました。 • 「マルチキャストルーティング」で，マルチキャスト送信者の数の最大数を変更しました。また，IGMP および MLD でのグループアドレス当たりの送信元アドレス数の最大数を変更しました。

項目	追加・変更内容
高機能スクリプトの仕様	• イベント起動スクリプトの記述を追加しました。
スクリプトの起動	• イベント起動スクリプトの記述を追加しました。
スクリプト起動契機の取得	• 本項を追加しました。
VLAN インタフェースの MAC アドレス	• 本項を追加しました。

【Ver. 12.4 対応版】

表　変更内容

項目	追加・変更内容
装置構成	• AX8608R の記述を追加しました。
搭載条件	• AX8608R の記述を追加しました。
収容条件	• 「テーブルエントリ数」にハードウェアプロファイル router-1s および配分パターン ipv4-ipv6-uni の記述を追加しました。 • 「経路配分パターン」にハードウェアプロファイル router-1s および配分パターン ipv4-ipv6-uni の記述を追加しました。 • 「リンクアグリゲーション」に AX8608R の記述を追加しました。 • 「レイヤ 2 スイッチング」を追加しました。 • 「フィルタ・QoS」にハードウェアプロファイル router-1s の記述を追加しました。 • 「L2 ループ検知」を追加しました。 • 「IP インタフェースと IP パケット中継」に VLAN インタフェースの記述を追加しました。 • 「BFD」を追加しました。
ハードウェアプロファイルの設定	• 本項を追加しました。
BCU 初期導入ソフトウェアからのアップデートの解説	• 本節を追加しました。
BCU 初期導入ソフトウェアからのアップデートのオペレーション	• 本節を追加しました。
オプションライセンスの解説	• 本節を追加しました。
リンクトラップの送信制御	• VLAN インタフェースのサポートに伴って記述を変更しました。
高機能スクリプト	• 本章を追加しました。
VLAN Tag	• VLAN の記述を追加しました。
本装置の MAC アドレス	• VLAN インタフェース，スパニングツリー，および Ring Protocol の記述を追加しました。
IP インタフェース	• VLAN インタフェースのサポートに伴って記述を変更しました。

【Ver. 12.2 対応版】

表　変更内容

項目	追加・変更内容
収容条件	• 「テーブルエントリ数」の「(4) ハードウェアプロファイルと配分パターンの関係」のフロー系テーブルエントリ数を変更しました。

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 AX8600R のソフトウェア Ver. 12.8 の機能について記載しています。ソフトウェア機能のうち，オプションライセンスで提供する機能については次のマークで示します。

【OP-SHPS】

オプションライセンス OP-SHPS についての記述です。

【OP-SHPE】

オプションライセンス OP-SHPE についての記述です。

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。

●装置の開梱から，初期導入時の基本的な設定を知りたい

クイックスタートガイド (AX86R-Q001)

●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 (AX86R-H001)

●ソフトウェアの機能，コンフィグレーションの設定，運用コマンドを知りたい

▽まず，ガイドで使用する機能や収容条件についてご確認ください。

- **収容条件**
- **ログインなどの基本操作**
- **イーサネット**

コンフィグレーションガイド Vol.1 (AX86R-S001)

- **フィルタ，QoS**
- **ネットワークの管理**

コンフィグレーションガイド Vol.2 (AX86R-S002)

- **IPパケット中継**
- **ユニキャストルーティング**
- **マルチキャストルーティング**

コンフィグレーションガイド Vol.3 (AX86R-S003)

▽必要に応じて，レファレンスをご確認ください。

・コマンドの入力シンタックス，パラメータ詳細について

コンフィグレーション コマンドレファレンス Vol.1 (AX86R-S004)

コンフィグレーション コマンドレファレンス Vol.2 (AX86R-S005)

コンフィグレーション コマンドレファレンス Vol.3 (AX86R-S006)

運用コマンドレファレンス Vol.1 (AX86R-S007)

運用コマンドレファレンス Vol.2 (AX86R-S008)

運用コマンドレファレンス Vol.3 (AX86R-S009)

・システムメッセージとログについて

メッセージ・ログレファレンス (AX86R-S010)

・MIBについて

MIBレファレンス (AX86R-S011)

●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 (AX86R-T001)

■ このマニュアルでの表記

AC	Alternating Current
ACK	ACKnowledge
ARP	Address Resolution Protocol
AS	Autonomous System
AUX	Auxiliary
AXRP	Autonomous eXtensible Ring Protocol
BCU	Basic Control Unit
BEQ	Best Effort Queueing
BFD	Bidirectional Forwarding Detection
BGP	Border Gateway Protocol
BGP4	Border Gateway Protocol - version 4
BGP4+	Multiprotocol Extensions for Border Gateway Protocol - version 4
bit/s	bits per second　*bpsと表記する場合もあります。
BOOTP	Bootstrap Protocol
BPDU	Bridge Protocol Data Unit
C-Tag	Customer Tag

CA	Certificate Authority
CC	Continuity Check
CCM	Continuity Check Message
CFM	Connectivity Fault Management
CFP	C Form-factor Pluggable
CIDR	Classless Inter-Domain Routing
CLI	Command Line Interface
CoS	Class of Service
CRC	Cyclic Redundancy Check
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
DA	Destination Address
DC	Direct Current
DCE	Data Circuit terminating Equipment
DHCP	Dynamic Host Configuration Protocol
DHCPv6	Dynamic Host Configuration Protocol for IPv6
DNS	Domain Name System
DNSSL	Domain Name System Search List
DR	Designated Router
DSA	Digital Signature Algorithm
DSAP	Destination Service Access Point
DSCP	Differentiated Services Code Point
DTE	Data Terminal Equipment
E-mail	Electronic mail
EAP	Extensible Authentication Protocol
EAPOL	EAP Over LAN
EFM	Ethernet in the First Mile
ETH-AIS	Ethernet Alarm Indicator Signal
ETH-LCK	Ethernet Locked Signal
FAN	Fan Unit
FCS	Frame Check Sequence
FE	Forwarding Engine
HDC	Hardware Dependent Code
HMAC	Keyed-Hashing for Message Authentication
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
ICMPv6	Internet Control Message Protocol version 6
ID	Identifier
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
IPX	Internetwork Packet Exchange
ISO	International Organization for Standardization
ISP	Internet Service Provider
L2LD	Layer 2 Loop Detection
LAN	Local Area Network
LCD	Liquid Crystal Display
LED	Light Emitting Diode
LLC	Logical Link Control
LLDP	Link Layer Discovery Protocol
LLPQ	Low Latency Priority Queueing
LLQ	Low Latency Queueing
LLRLQ	Low Latency Rate Limited Queueing
LSA	Link State Advertisement
MA	Maintenance Association
MAC	Media Access Control
MC	Memory Card
MD5	Message Digest 5
MDI	Medium Dependent Interface
MDI-X	Medium Dependent Interface crossover
MEG	Maintenance Entity Group
MEP	Maintenance association End Point/Maintenance entity group End Point
MIB	Management Information Base
MIP	Maintenance domain Intermediate Point
MLD	Multicast Listener Discovery
MP	Maintenance Point
MRU	Maximum Receive Unit
MSTP	Multiple Spanning Tree Protocol
MTU	Maximum Transfer Unit
NAK	Not AcKnowledge
NAS	Network Access Server
NBMA	Non-Broadcast Multiple-Access

NDP	Neighbor Discovery Protocol
NIF	Network Interface
NSAP	Network Service Access Point
NSR	NonStop Routing
NSSA	Not So Stubby Area
NTP	Network Time Protocol
OAM	Operations,Administration,and Maintenance
OSPF	Open Shortest Path First
OUI	Organizationally Unique Identifier
PA	Protocol Accelerator
packet/s	packets per second　　*ppsと表記する場合もあります。
PAD	PADding
PC	Personal Computer
PDU	Protocol Data Unit
PE-ME	Programmable Engine Micro Engine
PE-NIF	Programmable Engine Network Interface
PGP	Pretty Good Privacy
PID	Protocol IDentifier
PIM	Protocol Independent Multicast
PIM-SM	Protocol Independent Multicast-Sparse Mode
PIM-SSM	Protocol Independent Multicast-Source Specific Multicast
PQ	Priority Queueing
PRU	Packet Routing Unit
PS	Power Supply
PSINPUT	Power Supply Input
PSU	Packet Switching Unit
QoS	Quality of Service
QSFP+	Quad Small Form factor Pluggable Plus
QSFP28	28Gbps Quad Small Form factor Pluggable
RA	Router Advertisement
RADIUS	Remote Authentication Dial In User Service
RDI	Remote Defect Indication
RDNSS	Recursive Domain Name System Server
RFC	Request For Comments
RGQ	Rate Guaranteed Queueing
RIP	Routing Information Protocol
RIPng	Routing Information Protocol next generation
RMON	Remote Network Monitoring MIB
RPF	Reverse Path Forwarding
RQ	ReQuest
RR	Round Robin
RSA	Rivest, Shamir, Adleman
S-Tag	Service Tag
SA	Source Address
SD	Secure Digital
SFD	Start Frame Delimiter
SFP	Small Form-factor Pluggable
SFP+	enhanced Small Form-factor Pluggable
SFU	Switch Fabric Unit
SHA1	Secure Hash Algorithm 1
SMTP	Simple Mail Transfer Protocol
SNAP	Sub-Network Access Protocol
SNMP	Simple Network Management Protocol
SNPA	Subnetwork Point of Attachment
SNTP	Simple Network Time Protocol
SOP	System Operational Panel
SPF	Shortest Path First
SSAP	Source Service Access Point
SSH	Secure Shell
SSW	Sub-crossbar SWitch
STP	Spanning Tree Protocol
TA	Terminal Adapter
TACACS+	Terminal Access Controller Access Control System Plus
TCP/IP	Transmission Control Protocol/Internet Protocol
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
URL	Uniform Resource Locator
uRPF	unicast Reverse Path Forwarding
VLAN	Virtual LAN
VPN	Virtual Private Network

VRF	Virtual Routing and Forwarding/Virtual Routing and Forwarding Instance
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network
WFQ	Weighted Fair Queueing
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 本装置の概要 2

1.2 本装置の特長 3

2 装置構成 7

2.1 本装置のモデル 8

2.1.1 装置の外観 8

2.2 装置の構成要素 12

2.2.1 ハードウェア 12

2.2.2 ソフトウェア 15

3 収容条件 17

3.1 搭載条件 18

3.1.1 最大収容ポート数 18

3.1.2 最大搭載数 18

3.1.3 PRU と NIF の搭載 19

3.2 収容条件 21

3.2.1 テーブルエントリ数 21

3.2.2 経路配分パターン 25

3.2.3 リモートアクセス 27

3.2.4 リンクアグリゲーション 27

3.2.5 レイヤ 2 スイッチング 28

3.2.6 フィルタ・QoS 31

3.2.7 L2 ループ検知 36

3.2.8 トラッキング機能 36

3.2.9 ネットワークの管理 37

3.2.10 IP インタフェースと IP パケット中継 39

3.2.11 ユニキャストルーティング 45

3.2.12 マルチキャストルーティング 50

3.2.13 BFD 55

第 2 編　運用管理

4 装置起動とログイン 57

4.1 運用端末による管理 58

4.1.1 運用端末の接続形態 58

4.1.2 運用端末 59

4.1.3 運用管理機能の概要 61

4.2 装置起動 62

4.2.1 起動から停止までの概略 62

4.2.2 装置の起動 62

4.2.3 装置の停止 63

4.3 ログイン・ログアウト 64

5 コマンド操作 65

5.1 コマンド入力モード 66

5.1.1 運用コマンド一覧 66

5.1.2 コマンド入力モード 66

5.2 CLI での操作 68

5.2.1 補完機能 68

5.2.2 ヘルプ機能 68

5.2.3 入力エラーメッセージ 68

5.2.4 コマンド短縮実行 69

5.2.5 ヒストリ機能 70

5.2.6 パイプ機能 71

5.2.7 リダイレクト 71

5.2.8 ページング 72

5.2.9 CLI 設定のカスタマイズ 72

5.3 CLI の注意事項 73

5.3.1 ログイン後に運用端末がダウンした場合 73

5.3.2 CLI の特殊キー操作時にログアウトした場合 73

5.3.3 待機系のファイルにアクセスする場合 73

6 コンフィグレーション 75

6.1 コンフィグレーションの概要 76

6.1.1 起動時のコンフィグレーション 76

6.1.2 運用中のコンフィグレーション 77

6.1.3 ランニングコンフィグレーションの編集の流れ 77

6.1.4 コンフィグレーション入力時のモード遷移 79

6.1.5 初期導入時のコンフィグレーションについて 80

6.1.6 コンフィグレーション・運用コマンド一覧 80
6.2 コンフィグレーションの編集方法 83
6.2.1 コンフィグレーションの編集開始 83
6.2.2 コンフィグレーションの表示・確認 83
6.2.3 コンフィグレーションのコミットモードの設定 85
6.2.4 コンフィグレーションの追加・変更・削除 86
6.2.5 ランニングコンフィグレーションへの反映 87
6.2.6 コンフィグレーションのファイルへの保存 88
6.2.7 コンフィグレーションのファイルからの反映 90
6.2.8 コンフィグレーションの編集終了 91
6.2.9 コンフィグレーションの編集時の注意事項 92
6.3 テンプレートの操作 93
6.3.1 テンプレートの概要 93
6.3.2 テンプレートの作成 94
6.3.3 テンプレートの編集 96
6.3.4 テンプレートの反映 98
6.3.5 テンプレートパラメータの使用方法 99
6.3.6 特記事項 102
6.4 コンフィグレーションの操作 104
6.4.1 コンフィグレーションのバックアップ 104
6.4.2 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 104
6.4.3 ftp コマンドを使用したファイル転送 105
6.4.4 MC を使用したファイル転送 106

7 リモート運用端末から本装置へのログイン 109
7.1 解説 110
7.1.1 マネージメントポート接続 110
7.1.2 通信用ポート接続 110
7.1.3 ダイアルアップ IP 接続 110
7.2 コンフィグレーション 114
7.2.1 コンフィグレーションコマンド一覧 114
7.2.2 マネージメントポートの設定 115
7.2.3 本装置への IP アドレスの設定 116
7.2.4 telnet によるログインを許可する 116
7.2.5 ftp によるログインを許可する 117
7.2.6 VRF での telnet によるログインを許可する 117
7.2.7 VRF での ftp によるログインを許可する 118
7.3 オペレーション 119
7.3.1 運用コマンド一覧 119
7.3.2 リモート運用端末と本装置との通信の確認 120

8 ログインセキュリティと RADIUS/TACACS+ 121
8.1 ログインセキュリティの設定 122
8.1.1 コンフィグレーション・運用コマンド一覧 122
8.1.2 ログイン制御の概要 123
8.1.3 ログインユーザの作成および削除 123
8.1.4 ログインユーザのパスワードの設定および変更 124
8.1.5 装置管理者モード変更のパスワードの設定および変更 125
8.1.6 リモート運用端末からのログインの許可 126
8.1.7 同時にログインできるユーザ数の設定 126
8.1.8 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 127
8.1.9 ログインバナーの設定 127
8.1.10 VRF でのリモート運用端末からのログインの許可 129
8.1.11 VRF での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 129
8.2 RADIUS/TACACS+の解説 132
8.2.1 RADIUS/TACACS+の概要 132
8.2.2 RADIUS/TACACS+の適用機能および範囲 133
8.2.3 RADIUS/TACACS+を使用した認証 139
8.2.4 RADIUS/TACACS+/ローカルを使用したコマンド承認 142
8.2.5 RADIUS/TACACS+を使用したアカウンティング 150
8.2.6 RADIUS/TACACS+との接続 153
8.3 RADIUS/TACACS+のコンフィグレーション 155
8.3.1 コンフィグレーションコマンド一覧 155
8.3.2 RADIUS サーバによる認証の設定 156
8.3.3 TACACS+サーバによる認証の設定 157
8.3.4 RADIUS/TACACS+/ローカルによるコマンド承認の設定 158
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 159
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 160
8.4 RADIUS/TACACS+のオペレーション 161
8.4.1 運用コマンド一覧 161
8.4.2 コマンド承認の確認 161
9 SSH(SecureShell) 163
9.1 解説 164
9.1.1 概要 164
9.1.2 SSH の基本機能 165
9.1.3 サポート機能 166
9.1.4 SSH の接続構成 168
9.1.5 SSHv1 による接続からログインまでの流れ 169
9.1.6 SSHv2 による接続からログインまでの流れ 171

9.1.7 暗号化技術 173
9.1.8 メッセージ認証コード 176
9.1.9 ログインメッセージ表示 176
9.1.10 SSH 使用時の注意事項 177
9.2 コンフィグレーション 178
9.2.1 コンフィグレーションコマンド一覧 178
9.2.2 SSH サーバの基本設定（ローカルパスワード設定） 178
9.2.3 SSHv2 サーバで公開鍵認証をする設定 179
9.2.4 SSHv1 サーバで公開鍵認証をする設定 181
9.2.5 SSH サーバの暗号アルゴリズム関連の設定変更 182
9.2.6 RADIUS 認証と連携した SSH サーバの設定 182
9.2.7 SSHv2 サーバ機能だけを使用してセキュリティを高める 183
9.2.8 VRF での SSH によるログインを許可する 184
9.3 オペレーション 185
9.3.1 運用コマンド一覧 185
9.3.2 SSH クライアントから SSH サーバへのログイン 185
9.3.3 SSH クライアントから本装置で運用コマンドの実行 186
9.3.4 SSH クライアントから SSH サーバへのファイル転送 186
9.3.5 SSH サーバのホスト公開鍵の確認 188
9.3.6 SSH サーバのホスト鍵ペアの変更 188

10 時刻の設定と NTP/SNTP 191
10.1 解説 192
10.1.1 概要 192
10.1.2 時刻の設定と NTP/SNTP に関する注意事項 192
10.2 時刻の設定 193
10.2.1 コンフィグレーションコマンド・運用コマンド一覧 193
10.2.2 システムクロックの設定 193
10.2.3 サマータイムの設定 193
10.3 NTP のコンフィグレーション 196
10.3.1 コンフィグレーションコマンド一覧 196
10.3.2 NTP によるタイムサーバと時刻同期の設定 196
10.3.3 NTP サーバとの時刻同期の設定 197
10.3.4 NTP 認証の設定 197
10.3.5 VRF での NTP による時刻同期の設定 198
10.4 SNTP のコンフィグレーション 199
10.4.1 コンフィグレーションコマンド一覧 199
10.4.2 SNTP によるタイムサーバと時刻同期の設定 199
10.4.3 SNTP 認証の設定 200
10.4.4 VRF での SNTP による時刻同期の設定 200

10.5 オペレーション 201
10.5.1 運用コマンド一覧 201
10.5.2 時刻および NTP/SNTP の状態の確認 201

11 ホスト名と DNS 203
11.1 解説 204
11.1.1 概要 204
11.1.2 ホスト名と DNS に関する注意事項 204
11.2 コンフィグレーション 205
11.2.1 コンフィグレーションコマンド一覧 205
11.2.2 ホスト名の設定 205
11.2.3 DNS の設定 205

12 装置の管理 207
12.1 システム操作パネル 208
12.1.1 スタートアップメッセージ 208
12.1.2 メニュー構造 210
12.1.3 ポート情報の表示 211
12.1.4 CPU 使用率の表示 212
12.1.5 メモリ使用率の表示 213
12.1.6 バージョンの表示 214
12.1.7 温度情報の表示 218
12.1.8 ボードの交換 219
12.1.9 装置の停止 222
12.1.10 障害の表示 222
12.1.11 システム操作パネルの注意事項 224
12.2 装置のリソース設定 225
12.2.1 コンフィグレーション・運用コマンド一覧 225
12.2.2 ハードウェアプロファイルの設定 225
12.2.3 経路系テーブル固定配分の設定 226
12.2.4 フロー系テーブル固定配分の設定 226
12.2.5 経路系テーブルカスタマイズ配分の設定手順 226
12.2.6 カスタマイズ配分の生成 227
12.2.7 カスタマイズ配分の調整 229
12.2.8 カスタマイズ配分のコンフィグレーション設定 231
12.2.9 カスタマイズ配分の確認 232
12.2.10 カスタマイズ配分使用時の注意事項 233
12.3 装置の確認 234
12.3.1 コンフィグレーション・運用コマンド一覧 234
12.3.2 ソフトウェアバージョンの確認 235

12.3.3 装置の状態確認 236
12.3.4 内蔵フラッシュメモリの確認 239
12.3.5 MC の確認 240
12.3.6 温度監視 240
12.3.7 ファンユニットの監視 242
12.3.8 内蔵フラッシュメモリの未使用容量監視 243
12.4 SFU/PRU/NIF の管理 244
12.4.1 コンフィグレーション・運用コマンド一覧 244
12.4.2 ボードの disable 設定 245
12.4.3 PRU の起動優先度の設定 245
12.4.4 SFU の状態確認 245
12.4.5 PRU の状態確認 246
12.4.6 NIF の状態確認 246
12.4.7 NIF 交換時のコンフィグレーション 246
12.4.8 PE-NIF の設定 248
12.4.9 PE サービスの確認 248
12.5 運用情報のバックアップ・リストア 249
12.5.1 運用コマンド一覧 249
12.5.2 BCU 二重化時の手順 249
12.5.3 BCU 一重化時の手順 250
12.6 障害時の復旧 251
12.6.1 障害の種別と復旧内容 251
12.6.2 ソフトウェア障害検出時の動作 252
12.6.3 コンフィグレーション・運用コマンド一覧 253
12.6.4 系切替条件の設定 253

13 ソフトウェアの管理 255
13.1 ソフトウェアアップデートの解説 256
13.1.1 概要 256
13.1.2 ソフトウェアアップデートの対象 256
13.1.3 更新・反映の契機 256
13.1.4 無停止ソフトウェアアップデート 257
13.1.5 ソフトウェアアップデートに関する注意事項 258
13.2 ソフトウェアアップデートのオペレーション 260
13.2.1 運用コマンド一覧 260
13.2.2 アップデートファイルの準備 260
13.2.3 アップデートコマンドの実行 260
13.2.4 SFU・PRU・NIF のアップデート 261
13.2.5 アップデート後の確認 262
13.2.6 アップデート操作時の注意事項 262

13.3 BCU 初期導入ソフトウェアからのアップデートの解説 263
13.3.1 概要 263
13.3.2 BCU 初期導入ソフトウェアからのアップデートの対象 263
13.3.3 BCU 初期導入ソフトウェアからのアップデートの手順 264
13.3.4 BCU 初期導入ソフトウェアからのアップデートに関する注意事項 264
13.4 BCU 初期導入ソフトウェアからのアップデートのオペレーション 265
13.4.1 運用コマンド一覧 265
13.4.2 アップデートファイルの準備 265
13.4.3 アップデートコマンドの実行 265
13.4.4 アップデート後の確認 267
13.5 オプションライセンスの解説 268
13.5.1 概要 268
13.5.2 オプションライセンスを含むコンフィグレーションの操作 268
13.5.3 装置交換時のオプションライセンス再設定 269
13.5.4 オプションライセンスに関する注意事項 269
13.6 オプションライセンスのコンフィグレーション 270
13.6.1 コンフィグレーションコマンド一覧 270
13.6.2 オプションライセンスの設定 270
13.6.3 オプションライセンスの削除 270
13.7 オプションライセンスのオペレーション 272
13.7.1 運用コマンド一覧 272
13.7.2 オプションライセンスの確認 272

14 装置の冗長化 273
14.1 BCU 二重化の解説 274
14.1.1 概要 274
14.1.2 動作 274
14.1.3 ユーザの設定情報および利用情報の同期 275
14.1.4 系切替 275
14.1.5 BCU 二重化構成使用時の注意事項 278
14.2 BCU 二重化のオペレーション 280
14.2.1 運用コマンド一覧 280
14.2.2 待機系 BCU の状態確認 280
14.2.3 BCU の再起動 280
14.2.4 BCU の交換 280
14.2.5 ユーザの設定情報および利用情報の同期の実施 281
14.2.6 系切替の実施 281
14.3 SFU 冗長化の解説 282
14.3.1 冗長化時の装置構成 282
14.3.2 冗長構成の運用方法 282

14.3.3 障害発生時の SFU 動作 282
14.4 SFU 冗長化のオペレーション 284
14.4.1 運用コマンド一覧 284
14.4.2 SFU の状態確認 284
14.5 電源機構（PS）冗長化の解説 285
14.5.1 概要 285
14.5.2 電源ユニット冗長 285
14.5.3 給電系統冗長 285
14.5.4 供給電力の管理 286
14.6 電源機構（PS）冗長化のコンフィグレーション 289
14.6.1 コンフィグレーションコマンド一覧 289
14.6.2 電源ユニット冗長の設定 289
14.6.3 給電系統冗長の設定 289
14.7 電源機構（PS）冗長化のオペレーション 290
14.7.1 運用コマンド一覧 290
14.7.2 PS の状態確認 290
14.7.3 供給電力の確認 291

15 システムメッセージの出力とログの管理 293
15.1 解説 294
15.1.1 メッセージの出力 294
15.1.2 ログの保存 294
15.2 コンフィグレーション 295
15.2.1 コンフィグレーションコマンド一覧 295
15.2.2 運用ログの最小保存件数の設定 295
15.2.3 syslog 出力の設定 296
15.2.4 E-mail 出力の設定 296
15.2.5 メッセージの出力制御 296
15.3 オペレーション 299
15.3.1 運用コマンド一覧 299
15.3.2 ログの参照と削除 299

16 SNMP 301
16.1 解説 302
16.1.1 SNMP 概説 302
16.1.2 MIB 概説 305
16.1.3 SNMPv1，SNMPv2C オペレーション 307
16.1.4 SNMPv3 オペレーション 312
16.1.5 トラップ 316

16.1.6 インフォーム 317
16.1.7 SNMP で使用する IP アドレス 318
16.1.8 RMON MIB 319
16.1.9 SNMP マネージャとの接続時の注意事項 322
16.2 コンフィグレーション 324
16.2.1 コンフィグレーションコマンド一覧 324
16.2.2 SNMPv1，SNMPv2C による MIB アクセス許可の設定 324
16.2.3 SNMPv3 による MIB アクセス許可の設定 325
16.2.4 SNMPv1，SNMPv2C によるトラップ送信の設定 325
16.2.5 SNMPv3 によるトラップ送信の設定 326
16.2.6 SNMPv2C によるインフォーム送信の設定 326
16.2.7 リンクトラップの送信制御 327
16.2.8 RMON イーサネットヒストリグループの制御情報の設定 328
16.2.9 RMON による特定 MIB 値の閾値チェック 328
16.2.10 SNMPv1，SNMPv2C による VRF からの MIB アクセス許可の設定 329
16.2.11 SNMPv3 による VRF からの MIB アクセス許可の設定 329
16.2.12 SNMPv1，SNMPv2C による VRF へのトラップ送信の設定 330
16.2.13 SNMPv3 による VRF へのトラップ送信の設定 330
16.2.14 SNMPv2C による VRF へのインフォーム送信の設定 331
16.3 オペレーション 332
16.3.1 運用コマンド一覧 332
16.3.2 SNMP マネージャとの通信の確認 332

17 高機能スクリプト 335
17.1 解説 336
17.1.1 概要 336
17.1.2 高機能スクリプトの適用例 338
17.1.3 高機能スクリプトの仕様 339
17.1.4 スクリプト使用時の注意事項 340
17.2 スクリプトの作成と実行 342
17.2.1 コンフィグレーション・運用コマンド一覧 342
17.2.2 スクリプトの実行の流れ 343
17.2.3 スクリプトファイルの作成 343
17.2.4 スクリプトファイルの正常性確認 344
17.2.5 スクリプトファイルのインストール 345
17.2.6 スクリプトの起動 346
17.3 本装置の Python サポート内容 349
17.3.1 標準 Python との差分および制限 349
17.3.2 標準ライブラリ 349
17.4 Python 拡張ライブラリの使用方法 352

17.4.1 指定コマンド実行の設定 352
17.4.2 システムメッセージ出力の設定 356
17.4.3 イベント監視機能の設定 357
17.4.4 スクリプト起動契機の取得 360

第 3 編 ネットワークインタフェース

18 イーサネット 363
18.1 接続インタフェースの解説 364
18.1.1 ポートの種類とサポート機能 364
18.1.2 10BASE-T/100BASE-TX/1000BASE-T 366
18.1.3 1000BASE-X 369
18.1.4 10GBASE-R 371
18.1.5 40GBASE-R 371
18.1.6 100GBASE-R 372
18.2 イーサネット共通の解説 373
18.2.1 フローコントロール 373
18.2.2 フレームフォーマット 375
18.2.3 VLAN Tag 378
18.2.4 ジャンボフレーム 380
18.3 コンフィグレーション 381
18.3.1 コンフィグレーションコマンド一覧 381
18.3.2 イーサネットインタフェースの設定 381
18.3.3 複数インタフェースの一括設定 382
18.3.4 速度と全二重/半二重の設定 383
18.3.5 自動 MDI/MDIX 機能の設定 384
18.3.6 フローコントロールの設定 385
18.3.7 VLAN Tag の TPID 値の設定 385
18.3.8 ジャンボフレームの設定 385
18.3.9 リンクダウン検出タイマの設定 386
18.3.10 リンクアップ検出タイマの設定 387
18.3.11 フレーム送受信エラー通知の設定 387
18.3.12 SFP+/SFP 共用ポートの設定 388
18.4 オペレーション 390
18.4.1 運用コマンド一覧 390
18.4.2 イーサネットの動作状態の確認 390

19 リンクアグリゲーション 391
19.1 リンクアグリゲーション基本機能の解説 392
19.1.1 概要 392
19.1.2 リンクアグリゲーションの構成 392
19.1.3 サポート仕様 393
19.1.4 チャネルグループの MAC アドレス 394
19.1.5 フレーム送信時のポート振り分け 394
19.1.6 リンクアグリゲーション使用時の注意事項 396
19.2 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 397
19.2.1 コンフィグレーションコマンド一覧 397
19.2.2 ポートチャネルインタフェースの設定 397
19.2.3 スタティックリンクアグリゲーションの設定 398
19.2.4 LACP リンクアグリゲーションの設定 398
19.2.5 振り分け方法の設定 399
19.2.6 チャネルグループの削除 401
19.2.7 チャネルグループをスイッチポートで使用する場合のポイント 401
19.3 リンクアグリゲーション拡張機能の解説 404
19.3.1 スタンバイリンク機能 404
19.3.2 離脱ポート数制限機能 405
19.3.3 異速度混在モード 406
19.3.4 切り戻し抑止機能 406
19.4 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 409
19.4.1 コンフィグレーションコマンド一覧 409
19.4.2 スタンバイリンク機能の設定 409
19.4.3 離脱ポート数制限機能の設定 410
19.4.4 異速度混在モードの設定 410
19.4.5 切り戻し抑止機能の設定 410
19.5 リンクアグリゲーションのオペレーション 412
19.5.1 運用コマンド一覧 412
19.5.2 リンクアグリゲーションの状態の確認 412
20 IP インタフェースとサブインタフェース 415
20.1 解説 416
20.1.1 概要 416
20.1.2 サブインタフェース 416
20.1.3 ネットワーク構成例 417
20.1.4 IP インタフェース動作仕様 418
20.2 コンフィグレーション 423
20.2.1 コンフィグレーションコマンド一覧 423

20.2.2 IP インタフェースの設定 424
20.2.3 IP インタフェースの削除 425
20.2.4 VLAN インタフェースの MAC アドレス 427
20.2.5 サブインタフェースのシャットダウン 428
20.3 オペレーション 429
20.3.1 運用コマンド一覧 429
20.3.2 IP インタフェースの状態および統計情報の確認 429

付録 431
付録 A 準拠規格 432
付録 A.1 TELNET/FTP 432
付録 A.2 RADIUS/TACACS+ 432
付録 A.3 SSH 432
付録 A.4 NTP 433
付録 A.5 SNTP 433
付録 A.6 DNS 433
付録 A.7 SYSLOG 433
付録 A.8 SNMP 433
付録 A.9 イーサネット 436
付録 A.10 リンクアグリゲーション 436
付録 B 謝辞(Acknowledgments) 437

索引 441

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　本装置の概要

NGN（Next Generation Network）を始めとする通信キャリアの商用ネットワークは，IP 電話，インターネット接続，企業の業務通信，携帯通信など，社会活動に欠かせない通信サービスを提供する社会インフラとしてますます重要な位置を占めてきています。特に，近年は一部の通信サービスのトラフィック量増大が顕著で，ネットワークはより大容量化／高速化されていく傾向にあります。

また，こうしたネットワークに流れる通信データには，企業の利益を左右するミッションクリティカルな重要データや個人視聴のストリーミング動画など，社会的優先度の異なる多種多様なものが混在しています。そのため，情報漏えいや不正アクセスに対するセキュリティの確保，ネットワークの処理能力を超えないようにする適切なトラフィック制御など，高次元のネットワーク管理制御性が求められています。

本装置は，ミッションクリティカルな IT インフラ実現に不可欠な信頼性・可用性・拡張性の高い通信ネットワーク基盤を柔軟に構築するルータ製品です。

製品コンセプト

本装置は，弊社が目指す「ギャランティード・ネットワーク」を実現するために開発してきたキャリアグレード技術を継承しつつ，通信キャリアネットワークに必要とされる大容量／高速性と高密度収容能力を備えた製品です。

本装置は次の機能を実現します。

- 100 ギガビットイーサネットやリンクアグリゲーションを用意し，トラフィック増大に対して余裕を持ったネットワークを実現
- 大規模ネットワークで使用される OSPF，BGP4 などのルーティングプロトコルや，先進の IPv6，マルチキャストなどを装備し，多様で柔軟なネットワークを実現
- ハードウェアの装置内冗長やさまざまなネットワーク冗長機能をサポートし，高信頼・高可用なネットワークを実現
- 装置のシステム容量をスケーラブルに増量できる分散エンジン方式を採用，また，分散エンジンに最大 4 種のネットワークインタフェースカードを搭載できるマイクロラインカード構造によって無駄のない増設を実現
- 通信キャリアネットワークで扱われるさまざまなトラフィック（企業の業務データ，IP 電話データ，テレビ会議，ストリーミング動画など）を，その優先度に応じて QoS 技術などで保護するギャランティ型ネットワークを実現
- 高機能フィルタリングなどのセキュリティ機能で，安全なネットワークを実現

1.2　本装置の特長

(1)　高性能アーキテクチャ

●100 ギガビットイーサネット対応

- 100 ギガビットイーサネットをノンブロッキング中継

●大容量化に適したスイッチファブリック方式，分散エンジン方式を採用

(2)　コンパクト・高効率収容

●前面吸気・背面排気のエアフロー

- コンパクトな筐体に前面吸気・背面排気のエアフロー方式を採用
- 局舎／サーバルームのスペース効率や冷却効率の向上に貢献

●低速回線と高速回線を効率収容

- 既存設備で使用されている 1 ギガビットイーサネットと，今後の増設や大容量化のための 10 ギガビットイーサネットなど，異なるインタフェースを効率良く混載して収容できるマイクロラインカード構造を採用
- 1/4 スロットサイズのネットワークインタフェースカード単位で増設できるため，混載による無駄が少なく，段階的な容量増設の際にも設備投資効率を改善

(3)　ミッションクリティカル対応のネットワークを実現する高信頼性

●高い装置品質

- 厳選した部品と厳しい設計・検査基準による装置の高い信頼性
- 通信キャリア／ISP で実績あるソフトウェアを継承した安定したルーティング処理

●FT アーキテクチャによる単体装置としての高信頼化

- 装置内の電源，CPU 部，パケットフォワーディング部を冗長化することによって，フォールト・トレラント・ネットワーク（FTN：Fault Tolerant Network）を構築

●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 準拠），ホットスタンバイ（VRRP），スタティックポーリング※など
- BFD による高速な障害検知
- ロードバランス

  OSPF イコールコストマルチパスなどによる IP レベルの均等トラフィック分散
- リングプロトコル

  多様なリングネットワーク構成に対応した Autonomous Extensible Ring Protocol を実装

注※

指定経路上の可達性をポーリングによって確認し，動的にスタティックルーティングと連動して経路を切り替えるための監視機能

●ソフトウェアの高負荷防止機構を実装

- ソフトウェアで処理するパケットに対するレートリミット，優先制御によって，DoS 攻撃などからソフトウェアを保護し，ルーティング処理などで安定した動作を実現

(4)　ハードウェアによる強力な QoS で通信品質を保証

●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

- IP-QoS（Diff-Serv，帯域制御，優先制御，廃棄制御など）

(5)　実績あるルーティング機能とレイヤ 2 中継機能をサポート

●安定した高機能ルーティング

- 実績あるルーティングソフトウェアを継承
- 豊富な L2/L3 制御プロトコルによって，多様で柔軟な信頼性の高いネットワークを実現可能
  （スタティック，RIP，RIPng，OSPF，OSPFv3，BGP4，BGP4+，PIM-SM/PIM-SSM，IGMP，MLD，VRF 対応，STP，RING など）

●スケーラブルなルーティング機能

- IPv4/IPv6 デュアルスタックでフルルートに対応
- 大規模 L2/L3 ネットワークに対応した高速な経路制御処理
- VRF などによる多数のルーティングセッションにも対応可能

●レイヤ 2 中継機能

- ポート VLAN，タグ VLAN 機能を実装
- 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

(6)　強固なセキュリティ機能

●高性能できめ細かなパケットフィルタリングが可能

- ハードウェアによる高性能なフィルタリング処理
- フィルタリング条件に L2/L3/L4 ヘッダの指定が可能

●uRPF をサポート

- ルーティングテーブルを利用して不正な送信元を検出，廃棄する uRPF をサポート

●装置ユーザのアカウント制御

- RADIUS/TACACS+による装置へのログインパスワード認証
- ユーザごとに実行できるコマンドを制限可能

(7)　優れたネットワーク管理，保守・運用

●IPv4/IPv6 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

●ポートミラーリングによって，トラフィックの監視，解析が可能（受信側および送信側ポートの両方で可能）

●sFlow や sFlow-MIB によるトラフィック特性の分析が可能

●オンライン保守

ボード・電源・ファンの増設および交換をコマンドレスで実施可能。また，無停止ソフトウェアアップデートに対応。

●SD 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。

●全イーサネットポート，コンソールポート，メモリカードスロットを前面に配置

●システム操作パネル採用

コンソール端末を使用しないで各種情報を表示し，動作指示が可能。

●イーサネット網の保守管理機能の CFM（Connectivity Fault Management），LLDP（Link Layer Discovery Protocol）をサポート

●高度なコンフィグレーション管理

- テンプレート機能，マージ機能，ロールバック機能，手動コミットモードなどの充実したコンフィグレーション管理機能をサポート

●運用管理を効率化／省力化する運用支援スクリプト機能

- 装置にスクリプト言語の実行環境を搭載することで，装置オペレーションのカスタマイズや自動化が可能

(8) 省電力対応

●アーキテクチャ設計，部品選択の段階で低消費電力を志向

- 導入後の TCO（Total Cost of Ownership）の削減に寄与

●消費電力情報の可視化

- 消費電力を運用コマンドで表示

2 装置構成

この章では，本装置の外観や構成要素などについて説明します。

2.1　本装置のモデル

AX8600R シリーズには，次に示すモデルがあります。

- AX8608R
- AX8616R
- AX8632R

AX8600R シリーズは，基本制御機構（BCU），スイッチファブリック機構（SFU），パケットルーティング機構（PRU），ネットワークインタフェース機構（NIF），電源機構（PS），電源入力機構（PSINPUT），筐体，ファンユニット（FAN）などから構成されています。

AX8608R は BCU，PS を冗長化し，PRU を 2 スロット，NIF を 8 スロット収容可能なモデルです。
AX8608R では，SFU を使用しません。

AX8616R は BCU，SFU，PS を冗長化し，PRU を 4 スロット，NIF を 16 スロット収容可能なモデルです。

AX8632R は BCU，SFU，PS を冗長化し，PRU を 8 スロット，NIF を 32 スロット収容可能なモデルです。

AX8608R は，電源を ON にしたまま BCU，PRU，NIF，PS，FAN を交換できます。さらに，BCU，PS は冗長化すると，通信無停止で交換できます。

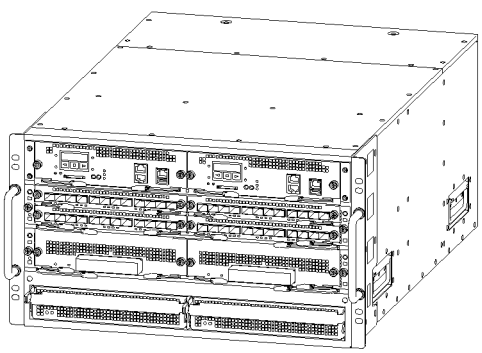
AX8616R および AX8632R は，電源を ON にしたまま BCU，SFU，PRU，NIF，PS，FAN を交換できます。さらに，BCU，SFU，PS は冗長化すると，通信無停止で交換できます。

2.1.1　装置の外観

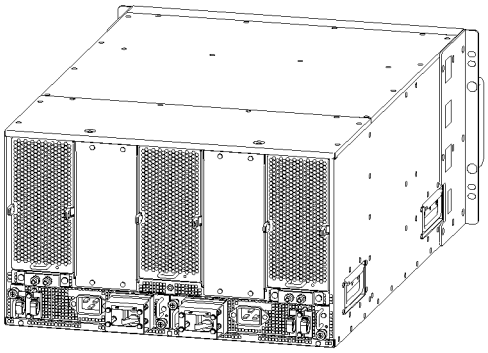
各モデルの装置外観図を次に示します。

(1)　AX8608R

図 2-1　AX8608R モデル



正面



背面

・搭載位置

BCU1	BCU2
NIF1	NIF2
NIF3	NIF4
NIF5	NIF6
NIF7	NIF8
PS1	PS2

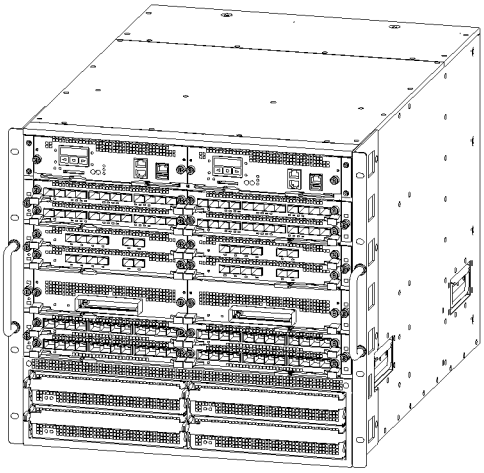
正面

FAN3		FAN2		FAN1
PSINPUT2			PSINPUT1	

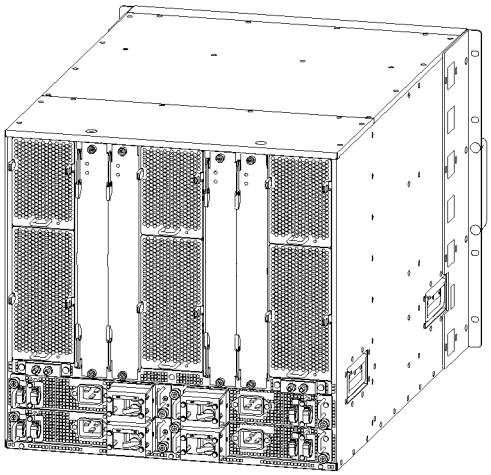
背面

(2)　AX8616R

図 2-2　AX8616R モデル



正面

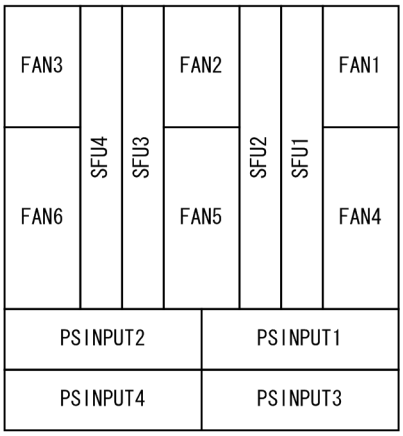


背面

・搭載位置

BCU1	BCU2
NIF1	NIF2
NIF3	NIF4
NIF5	NIF6
NIF7	NIF8
NIF9	NIF10
NIF11	NIF12
NIF13	NIF14
NIF15	NIF16
PS1	PS2
PS3	PS4

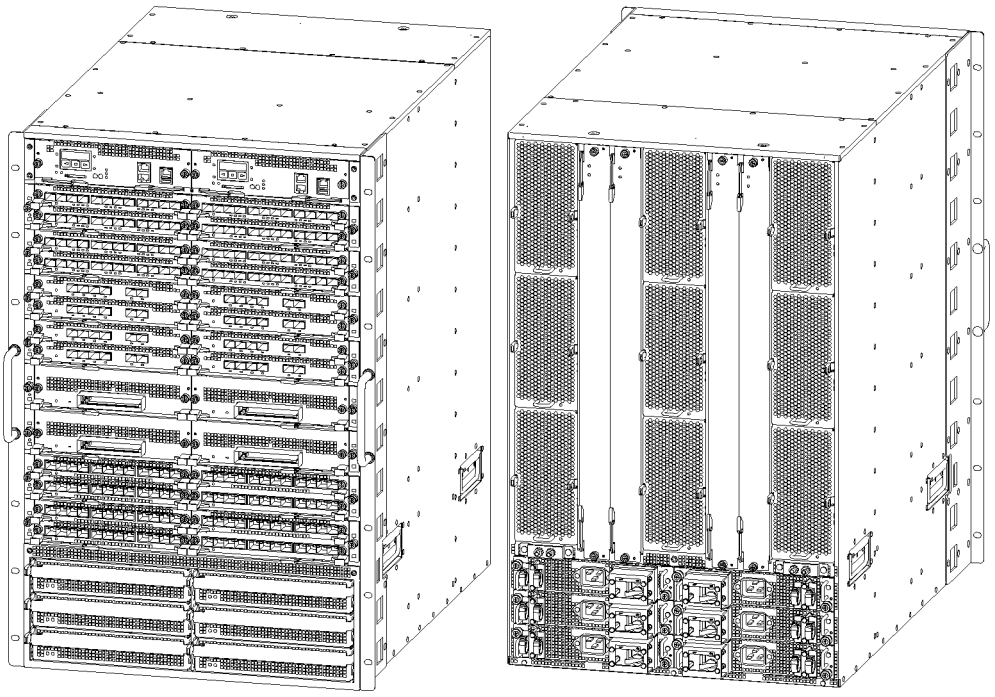
正面



背面

(3)　AX8632R

図 2-3　AX8632R モデル



正面　　背面

・搭載位置

BCU1	BCU2
NIF1	NIF2
NIF3	NIF4
NIF5	NIF6
NIF7	NIF8
NIF9	NIF10
NIF11	NIF12
NIF13	NIF14
NIF15	NIF16
NIF17	NIF18
NIF19	NIF20
NIF21	NIF22
NIF23	NIF24
NIF25	NIF26
NIF27	NIF28
NIF29	NIF30
NIF31	NIF32
PS1	PS2
PS3	PS4
PS5	PS6

正面

<table>
<tr><td>FAN3</td><td rowspan="4">SFU4</td><td rowspan="4">SFU3</td><td>FAN2</td><td rowspan="4">SFU2</td><td rowspan="4">SFU1</td><td>FAN1</td></tr>
<tr><td>FAN6</td><td>FAN5</td><td>FAN4</td></tr>
<tr><td>FAN9</td><td>FAN8</td><td>FAN7</td></tr>
<tr><td colspan="4">PSINPUT2</td><td colspan="3">PSINPUT1</td></tr>
<tr><td colspan="4">PSINPUT4</td><td colspan="3">PSINPUT3</td></tr>
<tr><td colspan="4">PSINPUT6</td><td colspan="3">PSINPUT5</td></tr>
</table>

背面

2.2　装置の構成要素

2.2.1　ハードウェア

本装置は，PS，PSINPUT，FAN，BCU，SFU（AX8608R では不要），PRU および NIF で構成されています。ハードウェアの構成を次に示します。

図 2-4　AX8608R のハードウェアの構成

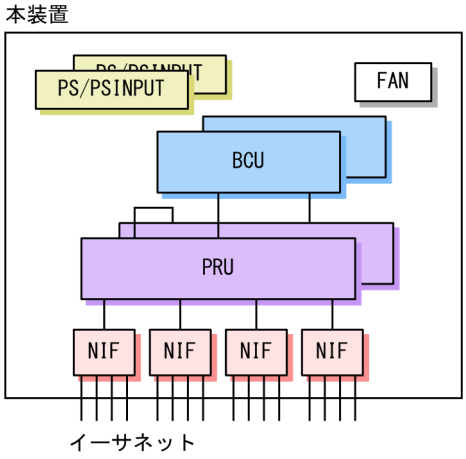
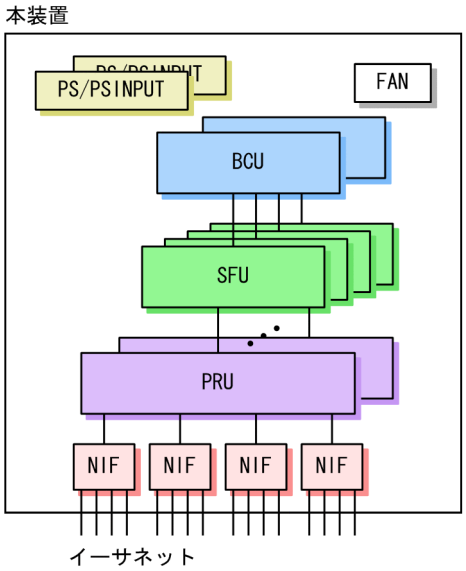


図 2-5　AX8616R および AX8632R のハードウェアの構成



(1)　PS（電源機構）と PSINPUT（電源入力機構）

PS と PSINPUT 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。PS は電源部，PSINPUT は電源入力部です。それぞれ AC 電源と DC 電源があります。

表 2-1　PS 機器一覧

略称	概略仕様
PS-A21	AC 電源 AC100V/200V 系
PS-D21	DC 電源 DC-48V 系

表 2-2　PSINPUT 機器一覧

略称	概略仕様
PSIN-A21	AC 電源入力部 AC100V/200V 系 PSINPUT1，3，5 用
PSIN-A22	AC 電源入力部 AC100V/200V 系 PSINPUT2，4，6 用
PSIN-D21	DC 電源入力部 DC-48V 系 PSINPUT1，3，5 用
PSIN-D22	DC 電源入力部 DC-48V 系 PSINPUT2，4，6 用

(2)　FAN

FAN は装置内部を冷却するファンユニットです。

表 2-3　ファンユニット一覧

略称	概略仕様
FAN-21	AX8616R 用ファンユニット
FAN-22	AX8608R／AX8616R／AX8632R 用ファンユニット

(3)　BCU（基本制御機構）

BCU は装置の共通部分で，装置全体の管理やルーティングプロトコルなどの処理をします。

表 2-4　BCU 機器一覧

略称	概略仕様
BCU-1R	基本制御部 メモリ 16GB

(4)　SFU（スイッチファブリック機構）

SFU は PRU と PRU の間で，高速でパケットを送受信します。なお，AX8608R は，2 枚の PRU を直結して PRU 間でパケットを送受信する構造のため，SFU は搭載不要です。

表 2-5　SFU 機器一覧

略称	概略仕様
SFU-M1	AX8616R 用スイッチファブリック部
SFU-L1	AX8632R 用スイッチファブリック部

(5)　PRU（パケットルーティング機構）

PRU は，ハードウェアによるルーティング，フィルタリング，QoS 制御などで，高速な IP フォワーディングと QoS を実現します。また，PRU の種別によって実装される FE（フォワーディングエンジン）の数が異なります。

表 2-6　PRU 機器一覧

略称	FE 数	概略仕様
PRU-1A	1	パケットルーティングプロセッサ 1A
PRU-2A	2	パケットルーティングプロセッサ 2A

(6)　NIF（ネットワークインタフェース機構）

NIF は各種メディア対応のインタフェース制御部で，複数の種類があり，物理レイヤを処理します。

表 2-7　NIF 機器一覧

略称	概略仕様	サイズ
NL1G-12T	10/100/1000Mbit/s イーサネット 12 回線	シングルハーフ
NL1G-12S	1Gbit/s イーサネット 12 回線　SFP	シングルハーフ
NL1GA-12S	1Gbit/s イーサネット 12 回線　SFP (PE-NIF)	シングルハーフ
NLXG-6RS	1/10Gbit/s イーサネット 6 回線　SFP/SFP+※1	シングルハーフ
NLXGA-12RS	1/10Gbit/s イーサネット 12 回線　SFP/SFP+※2 (PE-NIF)	シングルハーフ
NLXLG-4Q	40Gbit/s イーサネット 4 回線　QSFP+	シングルハーフ
NLCG-1Q	100Gbit/s イーサネット 1 回線　QSFP28	シングルハーフ
NMCG-1C	100Gbit/s イーサネット 1 回線　CFP	シングルフル

注※1

同一の NIF に SFP と SFP+の両方を収容する場合，ポート 1～4 を同一の回線速度，ポート 5，6 を同一の回線速度にして使用してください。

注※2

同一の NIF に SFP と SFP+の両方を収容する場合，SFP はポート 12 から降順で連続するポート番号，SFP+はポート 1 から昇順で連続するポート番号で使用してください。

2.2.2　ソフトウェア

本装置のソフトウェアは基本ソフトとオプションライセンスから構成されています。本装置のソフトウェアを次の表に示します。

表 2-8　ソフトウェア一覧（基本ソフト）

略称	機能概要
OS-RE	イーサネット，レイヤ 2 スイッチング，IPv4/IPv6 パケット中継，ユニキャストルーティング，マルチキャストルーティング，フィルタ，QoS，ネットワーク管理機能，運用管理機能，ほか （暗号機能を含む）

表 2-9　ソフトウェア一覧（オプションライセンス）

略称	機能概要
OP-SHPS	階層化シェーパ標準 • 標準収容数で階層化シェーパを使用できます。 • 1 ライセンスで，1 枚の NIF で階層化シェーパを使用できます。
OP-SHPE	階層化シェーパ拡張 • オプションライセンス OP-SHPS 設定時の収容数を拡張できます。 • 1 ライセンスで，1 枚の NIF の収容数を拡張できます。

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　搭載条件

3.1.1　最大収容ポート数

各モデルの最大収容可能ポート数を次の表に示します。

表 3-1　最大収容可能ポート数

モデル名	イーサネット				
	100GBASE-R	40GBASE-R	10GBASE-R	1000BASE-X	10/100/1000BASE-T
AX8608R	4	32	96	96	96
AX8616R	8	64	192	192	192
AX8632R	16	128	384	384	384

3.1.2　最大搭載数

(1)　機器搭載数

各モデルへのオプション機器を含めた最大機器搭載数を次の表に示します。

表 3-2　最大機器搭載数

機器	AX8608R	AX8616R	AX8632R
BCU	2	2	2
SFU	−	4	4
PRU	2	4	8
NIF（シングルフル）※	4	8	16
NIF（シングルハーフ）※	8	16	32
FAN	3	6	9
PS/PSINPUT（AC 電源）	2	4	6
PS/PSINPUT（DC 電源）	2	4	6
MC（SD タイプ）	1／BCU	1／BCU	1／BCU

（凡例）−：該当なし

注※

単一種別の NIF を搭載した場合の最大搭載数です。

(2)　NIF 最大搭載数

NIF 種別によって最大搭載数が異なります。NIF 種別ごとの装置当たりの最大搭載数を次に示します。なお，ここで示す値は単一種別の NIF を搭載した場合の最大搭載数です。

表 3-3　NIF 種別ごとの装置当たりの最大搭載数

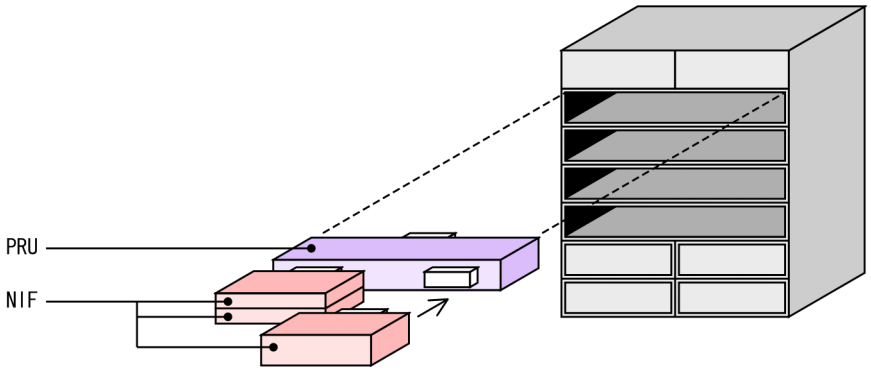
NIF 種別	サイズ	AX8608R	AX8616R	AX8632R
NL1G-12T	シングルハーフ	8	16	32
NL1G-12S	シングルハーフ	8	16	32
NL1GA-12S	シングルハーフ	8	16	32
NLXG-6RS	シングルハーフ	8	16	32
NLXGA-12RS	シングルハーフ	8	16	32
NLXLG-4Q	シングルハーフ	8	16	32
NLCG-1Q	シングルハーフ	8	16	32
NMCG-1C	シングルフル	4	8	16

3.1.3　PRU と NIF の搭載

PRU に NIF を搭載するためのスロットがあり，1 枚の PRU にシングルハーフサイズ NIF を最大 4 枚，シングルフルサイズ NIF を最大 2 枚搭載できます。また，1 枚の PRU にシングルフルサイズ NIF とシングルハーフサイズ NIF を混載できます。

PRU と NIF の搭載イメージを次の図に示します。

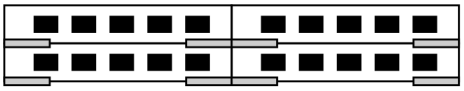
図 3-1　PRU と NIF の搭載イメージ



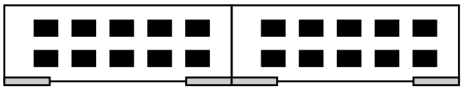
NIF の搭載構成を次の図に示します。

図 3–2　NIF の搭載構成

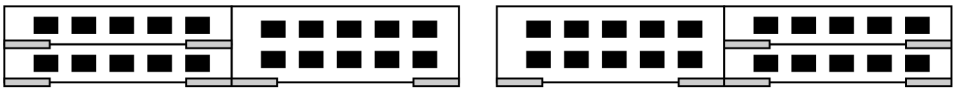
(a) シングルハーフサイズNIFを4枚搭載



(b) シングルフルサイズNIFを2枚搭載



(c) シングルハーフサイズNIFとシングルフルサイズNIFを混載



なお，PRU と NIF の組み合わせによっては NIF の搭載条件があります。搭載条件の有無を次の表に示します。

表 3–4　PRU と NIF の組み合わせによる NIF の搭載条件の有無

NIF 種別	PRU 種別	
	PRU-1A	PRU-2A
NL1G-12T	○	○
NL1G-12S	○	○
NL1GA-12S	△※	○
NLXG-6RS	○	○
NLXGA-12RS	△※	○
NLXLG-4Q	△※	○
NLCG-1Q	△※	○
NMCG-1C	○	○

(凡例)　○：条件なし　△：条件あり

注※

下段の NIF スロットだけに搭載できます。該当する NIF を搭載した場合，その上段の NIF スロットには NIF を搭載できません。また，上段の NIF スロットに NIF を搭載した場合，下段の NIF スロットには該当する NIF を搭載できません。

条件に違反すると，NIF を起動できません。

3.2　収容条件

3.2.1　テーブルエントリ数

(1)　概要

本項で使用するテーブルエントリ数とは，経路数やフィルタ・QoS フローのエントリ数を意味します。

本装置では，ネットワーク構成に合わせて適切なテーブルエントリ数の配分パターンを選べます。さらに，一部のテーブルエントリを拡張が必要なテーブルエントリへ配分するなどのカスタマイズができます。配分パターンはコンフィグレーションコマンドによって変更できます。

エントリの配分パターンは経路系，フロー系をそれぞれ用意しています。経路系テーブルエントリおよびフロー系テーブルエントリの内容を次の表に示します。

表 3-5　経路系テーブルエントリおよびフロー系テーブルエントリの内容

項目	内容
経路系テーブルエントリ	IPv4 ユニキャスト経路 IPv4 マルチキャスト経路 IPv6 ユニキャスト経路 IPv6 マルチキャスト経路 MAC アドレステーブル ARP NDP
フロー系テーブルエントリ	フィルタエントリ QoS フローエントリ

(2)　ハードウェアプロファイル

本装置では，各種テーブルエントリをどのように使用して装置を運用するかをハードウェアプロファイルで指定します。使用するハードウェアプロファイルはコンフィグレーションコマンドで設定します。ハードウェアプロファイルの種類と，対応する BCU および PRU を次の表に示します。

表 3-6　ハードウェアプロファイルの種類

ハードウェアプロファイル	対応 BCU	対応 PRU
router-1	BCU-1R	PRU-1A PRU-2A
router-1s	BCU-1R	PRU-1A PRU-2A

(3)　配分パターン

配分パターンを次に示します。

表 3-7　経路系テーブルエントリの配分パターン

パターン名	意味
default※	全エントリ混在
ipv4-uni	IPv4 ユニキャスト優先（IPv4 ユニキャスト主体，マルチキャストおよび IPv6 なし）
ipv6-uni	IPv6 ユニキャスト優先（IPv6 ユニキャスト主体，マルチキャストなし）
ipv4-ipv6-uni	IPv4 ユニキャストおよび IPv6 ユニキャスト優先（マルチキャストなし）
custom	経路系テーブルエントリのカスタマイズ

注※　デフォルトのパターン

表 3-8　フロー系テーブルエントリの配分パターン

パターン名称	意味
default※	フィルタ，QoS 均等
filter	フィルタ重視
filter-only	フィルタ専用
qos	QoS フロー重視
qos-only	QoS フロー専用
mirror	ポリシーベースミラーリング使用

注※　デフォルトのパターン

(4)　ハードウェアプロファイルと配分パターンの関係

ハードウェアプロファイルごとの経路系テーブルエントリ数とフロー系テーブルエントリ数を次に示します。VRF 機能使用時の最大エントリ数は，全 VRF のエントリ数の合計です。

ここの表で記載している IPv4 ユニキャスト経路数には，次の情報が含まれます。

- RIP，OSPF，BGP4，スタティックを合わせたアクティブ経路
- 他 VRF（グローバルネットワークを含む）からインポートされた，アクティブ状態のエクストラネット経路
- インタフェースに設定した IPv4 アドレス数×2：直結経路のホスト経路，サブネット経路
- ARP エントリ数
- ループバックインタフェースを使用する場合は，ループバックインタフェースごとに 1 経路が加算されます。
- RIP バージョン 2 を使用する場合は 1 経路が加算されます。
  VRF で RIP バージョン 2 を使用する場合は，VRF ごとに 1 経路が加算されます。
- OSPF を使用する場合は 2 経路が加算されます。
  VRF で OSPF を使用する場合は，VRF ごとに 2 経路が加算されます。
- VRRP でアクセプトモードを設定して，マスタ状態になっている場合は 1 経路が加算されます。
- ここに示した以外に 4 経路を装置固定情報として使用します。
  VRF を使用する場合は，VRF ごとに 1 経路を装置固定情報として使用します。

ここの表で記載している IPv6 ユニキャスト経路数には，次の情報が含まれます。

- RIPng，OSPFv3，BGP4+，スタティックを合わせたアクティブ経路
- 他 VRF（グローバルネットワークを含む）からインポートされた，アクティブ状態のエクストラネット経路
- インタフェースに設定した IPv6 アドレス数×2 ＋ IPv6 リンクローカルアドレス数：直結経路のホスト経路（グローバルおよびリンクローカル），サブネット経路（グローバル）
- NDP エントリ数
- ループバックインタフェースを使用する場合は，ループバックインタフェースごとに 1 経路が加算されます。
- VRRP でアクセプトモードを設定して，マスタ状態になっている場合は 1 経路が加算されます。
- ここに示した以外に 1 経路を装置固定情報として使用します。
  VRF を使用する場合は，VRF ごとに 1 経路を装置固定情報として使用します。

(a)　router-1

ハードウェアプロファイル router-1 の経路系テーブルエントリ数を次の表に示します。

表 3-9　router-1 の経路系テーブルエントリ数（1/2）

パターン名	IPv4 ユニキャスト経路	IPv4 マルチキャスト経路	IPv6 ユニキャスト経路	IPv6 マルチキャスト経路
default	1015808	8000	425984	8000
ipv4-uni	1998848	0	0	0
ipv6-uni	32768	0	983040	0
ipv4-ipv6-uni	884736	0	557056	0
custom	32768～1998848	0 または 8000	0～983040	0 または 8000

表 3-10　router-1 の経路系テーブルエントリ数（2/2）

パターン名	MAC アドレステーブル	ARP	NDP	ARP と NDP の合計
default	0	120000	120000	240000
ipv4-uni	0	120000	0	120000
ipv6-uni	0	32000	120000	120000
ipv4-ipv6-uni	0	120000	120000	120000
custom	0	32000～120000	0～120000	32000～240000

ハードウェアプロファイル router-1 のフロー系テーブルエントリ数を次の表に示します。フロー検出モードについては，「コンフィグレーションガイド Vol.2　9.1.3 フロー検出モード」または「コンフィグレーションガイド Vol.2　12.1.3 フロー検出モード」を参照してください。

表 3-11　router-1 のフロー系テーブルエントリ数（PRU 当たり）

フロー検出モード	パターン名	フィルタ	QoS フロー	ポリシーベースミラーリング	受信側ポリサー	送信側ポリサー
エントリ数重視モード	default	64000	64000	−	64000	64000
	filter	96000	32000	−		
	filter-only	128000	−	−		
	qos	32000	96000	−		
	qos-only	−	128000	−		
	mirror	64000	60000	4000		
検出条件数重視モード	default	32000	32000	−		
	filter	48000	16000	−		
	filter-only	64000	−	−		
	qos	16000	48000	−		
	qos-only	−	64000	−		
	mirror	32000	30000	2000		

（凡例）−：該当なし

(b)　router-1s

ハードウェアプロファイル router-1s の経路系テーブルエントリ数を次の表に示します。

表 3-12　router-1s の経路系テーブルエントリ数（1/2）

パターン名	IPv4 ユニキャスト経路	IPv4 マルチキャスト経路	IPv6 ユニキャスト経路	IPv6 マルチキャスト経路
default	1015808	8000	163840	8000
custom	32768～1998848	0 または 8000	0～983040	0 または 8000

表 3-13　router-1s の経路系テーブルエントリ数（2/2）

パターン名	MAC アドレステーブル	ARP	NDP	ARP と NDP の合計
default	245760	120000	120000	240000
custom	16384～524288	32000～120000	0～120000	32000～240000

ハードウェアプロファイル router-1s のフロー系テーブルエントリ数を次の表に示します。フロー検出モードについては,「コンフィグレーションガイド Vol.2　9.1.3 フロー検出モード」または「コンフィグレーションガイド Vol.2　12.1.3 フロー検出モード」を参照してください。

表 3–14　router-1s のフロー系テーブルエントリ数（PRU 当たり）

フロー検出モード	パターン名	フィルタ	QoS フロー	ポリシーベースミラーリング	受信側ポリサー	送信側ポリサー
エントリ数重視モード	default	64000	64000	−	64000	64000
	filter	96000	32000	−		
	filter-only	128000	−	−		
	qos	32000	96000	−		
	qos-only	−	128000	−		
	mirror	64000	60000	4000		
検出条件数重視モード	default	32000	32000	−		
	filter	48000	16000	−		
	filter-only	64000	−	−		
	qos	16000	48000	−		
	qos-only	−	64000	−		
	mirror	32000	30000	2000		

（凡例）−：該当なし

3.2.2　経路配分パターン

ハードウェアプロファイルごとの経路配分パターンに応じた収容条件を次に示します。

(1)　ハードウェアプロファイル router-1 の経路配分パターン

表 3–15　router-1 の経路配分パターン（1/2）

経路配分パターン	最大MACアドレス数	IPv4 ユニキャスト					IPv4 マルチキャスト		IPv4 インタフェース数
		最大経路エントリ数		プロトコル別最大経路エントリ数			PIM-SM/PIM-SSM		
		アクティブ／非アクティブの合計	アクティブ	RIP +OSPF	BGP	スタティック	(S,G)マルチキャスト経路情報最大数	最大インタフェース数	
default	0	4063232	1015808	100000	4063232	262144	8000	4095	16380
ipv4-uni	0	7995392	1998848	100000	7995392	262144	−	−	16380
ipv6-uni	0	131072	32768	30000	131072	32768	−	−	16380
ipv4-ipv6-uni	0	3538944	884736	100000	3538944	262144	−	−	16380
custom	0	7995392	1998848	100000	7995392	262144	8000	4095	16380

表 3-16　router-1 の経路配分パターン（2/2）

経路配分パターン	IPv6 ユニキャスト					IPv6 マルチキャスト		IPv6 インタフェース数
	最大経路エントリ数		プロトコル別最大経路エントリ数			PIM-SM/PIM-SSM		
	アクティブ／非アクティブの合計	アクティブ	RIPng +OSPFv3	BGP4+	スタティック	(S,G)マルチキャスト経路情報最大数	最大インタフェース数	
default	1703936	425984	100000	1703936	262144	8000	4095	16380
ipv4-uni	－	－	－	－	－	－	－	16380
ipv6-uni	3932160	983040	100000	3932160	262144	－	－	16380
ipv4-ipv6-uni	2228224	557056	100000	2228224	262144	－	－	16380
custom	3932160	983040	100000	3932160	262144	8000	4095	16380

（凡例）－：該当なし

(2)　ハードウェアプロファイル router-1s の経路配分パターン

表 3-17　router-1s の経路配分パターン（1/2）

経路配分パターン	最大 MAC アドレス数	IPv4 ユニキャスト					IPv4 マルチキャスト		IPv4 インタフェース数
		最大経路エントリ数		プロトコル別最大経路エントリ数			PIM-SM/PIM-SSM		
		アクティブ／非アクティブの合計	アクティブ	RIP +OSPF	BGP	スタティック	(S,G)マルチキャスト経路情報最大数	最大インタフェース数	
default	245760	4063232	1015808	100000	4063232	262144	8000	4095	16380
custom	524288	7995392	1998848	100000	7995392	262144	8000	4095	16380

表 3-18　router-1s の経路配分パターン（2/2）

経路配分パターン	IPv6 ユニキャスト					IPv6 マルチキャスト		IPv6 インタフェース数
	最大経路エントリ数		プロトコル別最大経路エントリ数			PIM-SM/PIM-SSM		
	アクティブ／非アクティブの合計	アクティブ	RIPng +OSPFv3	BGP4+	スタティック	(S,G)マルチキャスト経路情報最大数	最大インタフェース数	
default	655360	163840	100000	655360	163840	8000	4095	16380
custom	3932160	983040	100000	3932160	262144	8000	4095	16380

3.2.3　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 3-19　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	100 ユーザ／装置
登録できるユーザ公開鍵数	10 個／ユーザ

登録できるユーザ公開鍵の種類を次の表に示します。

表 3-20　登録できるユーザ公開鍵の種類

SSH プロトコル	公開鍵アルゴリズム※1	ビット数※2	公開鍵の種類
SSHv1	RSA	512～2560	SSHv1 形式
SSHv2	RSA（ssh-rsa）	512～5120	SECSH 形式※3
			OpenSSH 形式
	DSA（ssh-dss）	1024	SECSH 形式※3
			OpenSSH 形式

注※1
公開鍵アルゴリズムは RFC4253 に準拠します。

注※2
鍵にコメントが含まれない場合のビット数です（コメントと鍵の部分を合わせて 900 文字までの鍵が登録できます）。

注※3
SECSH 形式は draft-ietf-secsh-publickeyfile-03 に準拠します。

3.2.4　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 3-21　リンクアグリゲーションの収容条件

モデル	装置当たりの最大チャネルグループ数	チャネルグループ当たりの最大ポート数
AX8608R	96	16

モデル	装置当たりの最大チャネルグループ数	チャネルグループ当たりの最大ポート数
AX8616R	192	16
AX8632R	384	16

ロードバランスグループごとのポート振り分け使用時の収容条件を次の表に示します。

表 3-22　リンクアグリゲーションの収容条件（ロードバランスグループごとのポート振り分け使用時）

モデル	装置当たりの最大チャネルグループ数	チャネルグループ当たりの最大ポート数	ロードバランスグループ数
AX8608R	96	4	512
AX8616R	192	4	512
AX8632R	384	4	512

3.2.5　レイヤ 2 スイッチング

(1)　MAC アドレステーブル

レイヤ 2 スイッチ機能では，複数の機能で MAC アドレステーブルを使用します。例えば，MAC アドレス学習機能では，接続された端末の 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。MAC アドレステーブルの最大エントリ数については，「3.2.1　テーブルエントリ数」を参照してください。

MAC アドレステーブルを使用する機能と，その機能による MAC アドレステーブルの使用量を次の表に示します。

表 3-23　MAC アドレステーブルを使用する機能

機能名	使用量
MAC アドレス学習機能 ARP/NDP 学習機能	学習したアドレスごとに 1 エントリ※
IGMP/MLD snooping	• IGMP snooping を有効にした VLAN ごとに 3 エントリ • MLD snooping を有効にした VLAN ごとに 4 エントリ • 学習した MAC アドレスごとに 1 エントリ

注※

MAC アドレスと，対応する ARP または NDP を学習した場合は，合わせて 1 エントリとなります。

MAC アドレステーブルのエントリ数が最大エントリ数に達すると新たなエントリを登録できなくなるため，収容条件内で運用してください。なお，運用中は運用コマンド show pru resouces で MAC アドレステーブルの使用状況を確認できます。

(2)　MAC アドレス学習

MAC アドレス学習数の収容条件は，「3.2.1　テーブルエントリ数」で示した MAC アドレステーブルの最大エントリ数となります。

(3)　VLAN

コンフィグレーションで設定できる VLAN 数および Tag 変換情報エントリ数を次の表に示します。

表 3-24　VLAN の収容条件

項目	収容条件
VLAN 数（装置当たり）	4095
VLAN 数（ポート当たり）	4095
VLAN ポート数※1	200000
Tag 変換情報エントリ数（装置当たり）※2	65536

注※1

VLAN ポート数が収容条件を超えた場合，システムメッセージを出力します。収容条件を超えて設定した VLAN ポートは使用できません。

ポートチャネルインタフェースに設定する場合，チャネルグループ一つを VLAN ポート数一つとして計算します。

また，IP インタフェースとして使用するサブインタフェースの数，およびサブインタフェースが設定されていないイーサネットインタフェースとポートチャネルインタフェースの数も VLAN ポート数として計算します。

注※2

Tag 変換情報エントリをポートチャネルインタフェースに設定する場合, Tag 変換情報エントリ数は該当するチャネルグループのポート数で計算します。

(4)　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，次のポートは，VLAN ポート数に含めません。

- 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
- シャットダウン状態の VLAN の VLAN ポート
- VLAN トンネリングを設定しているポート

表 3-25　PVST+の収容条件

項目	収容条件
対象 VLAN 数	250
VLAN ポート数	1000

表 3-26　シングルスパニングツリーの収容条件

項目		収容条件
対象 VLAN 数		4095
VLAN ポート数	シングルスパニングツリーだけ使用時	10000
	PVST+併用時※	5000

注※

PVST+併用時，PVST+の VLAN ポート数とシングルスパニングツリーの VLAN ポート数との合計が最大値となります。

表 3-27　マルチプルスパニングツリーの収容条件

項目	収容条件
MST インスタンス数	16
MST インスタンスごとの対象 VLAN 数※	200
VLAN ポート数	10000

注※

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 4095 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。

(5)　Ring Protocol

Ring Protocol の収容条件を次の表に示します。

表 3-28　Ring Protocol の収容条件

項目	リング当たり	装置当たり
リング数	－	192
VLAN マッピング数	－	384
VLAN グループ数	2	384
VLAN グループの VLAN 数	4094※1	4094※1
リングポート数※2	2	384

（凡例）－：該当なし

注※1

制御 VLAN 用に VLAN を一つ消費するため，VLAN グループに使用できる VLAN 最大数は 4094 となります。

注※2

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。

(6)　IGMP/MLD snooping

IGMP snooping の収容条件を次の表に示します。IGMP snooping で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。登録できるマルチキャスト MAC アドレス数を次の表に示します。

表 3-29　IGMP snooping の収容条件

マルチキャストとの併用※1	最大数		
	設定 VLAN 数※2	登録エントリ数	マルチキャスト受信者数
併用する	256	4000	256/VLAN 32768/装置

マルチキャストとの併用※1	最大数		
	設定 VLAN 数※2	登録エントリ数	マルチキャスト受信者数
併用しない	256	8000	256/VLAN 32768/装置

注※1

IPv4 マルチキャストまたは IPv6 マルチキャストとの併用になります。

注※2

IGMP snooping が動作するポート数（IGMP snooping を設定している VLAN に収容されるポートの総和）は装置全体で最大 4096 です。例えば，それぞれ 10 ポート収容している 128 個の VLAN で IGMP snooping を動作させる場合，IGMP snooping 動作ポート数は 1280 となります。

MLD snooping の収容条件を次の表に示します。MLD snooping で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。登録できるマルチキャスト MAC アドレス数を次の表に示します。

表 3-30　MLD snooping の収容条件

マルチキャストとの併用※1	最大数		
	設定 VLAN 数※2	登録エントリ数	マルチキャスト受信者数
併用する	256	4000	256/VLAN 32768/装置
併用しない	256	8000	256/VLAN 32768/装置

注※1

IPv4 マルチキャストまたは IPv6 マルチキャストとの併用になります。

注※2

MLD snooping が動作するポート数（MLD snooping を設定している VLAN に収容されるポートの総和）は装置全体で最大 4096 です。例えば，それぞれ 10 ポート収容している 128 個の VLAN で MLD snooping を動作させる場合，MLD snooping 動作ポート数は 1280 となります。

3.2.6　フィルタ・QoS

(1)　フィルタ・QoS フロー

フィルタおよび QoS フローの収容条件を示します。ここでのエントリ数とは，コンフィグレーション（access-list，qos-flow-list）で設定したリストを装置内部で使用する形式（エントリ）に変換したあとの数です。

(a)　フィルタ・QoS フローエントリ数

ハードウェアプロファイルごとのフィルタおよび QoS フローの最大エントリ数を次に示します。

表 3-31　router-1 でのフィルタ・QoS フローエントリ数

モデル	フィルタの最大エントリ数		QoS フローの最大エントリ数	
	PRU 当たり	装置当たり	PRU 当たり	装置当たり
AX8608R	128000	256000	128000	256000
AX8616R	128000	512000	128000	512000
AX8632R	128000	1024000	128000	1024000

表 3-32　router-1s でのフィルタ・QoS フローエントリ数

モデル	フィルタの最大エントリ数		QoS フローの最大エントリ数	
	PRU 当たり	装置当たり	PRU 当たり	装置当たり
AX8608R	128000	256000	128000	256000
AX8616R	128000	512000	128000	512000
AX8632R	128000	1024000	128000	1024000

(b)　フロー検出条件による使用エントリ数

フロー制御はコンフィグレーションで設定しますが，リストに設定するフロー検出条件パラメータによって使用するエントリ数が異なります。複数エントリを使用するフロー検出条件のパラメータを次の表に示します。

表 3-33　複数エントリを使用するフロー検出条件

複数エントリを使用する フロー検出条件のパラメータ	使用エントリ数算出例
宛先 IPv4 アドレス，送信元 IPv4 アドレス，宛先 IPv6 アドレスを範囲指定	指定された IP アドレスがいくつのサブネットに区切られるかによってエントリ数が決定。 例えば，宛先 IPv4 アドレスに 192.168.0.1-192.168.0.4 と指定した場合，次の三つのサブネットに区切られるため，3 エントリとなります。 • 192.168.0.1/32 • 192.168.0.2/31 • 192.168.0.4/32
宛先ポート番号を範囲指定，送信元ポート番号を範囲指定	指定された値が最大 16 ビットのマスクで区切ったときにいくつに分けられるかによってエントリ数が決定。 例えば，宛先ポート番号に 135-140 と指定した場合，次の三つの領域に区切られるため，3 エントリとなります。 • 135/16：0000 0000 1000 0111（2 進表記） • 136/14：0000 0000 1000 10xx（2 進表記） • 140/16：0000 0000 1000 1100（2 進表記）
TCP セッション維持（ack フラグが ON，または rst フラグが ON のパケット検出）	2 エントリ使用します。

複数エントリを使用する フロー検出条件のパラメータ	使用エントリ数算出例
IP レングスの上限値または下限値を指定	指定された IP レングスが最大 16 ビットのマスクで区切ったときにいくつに分けられるかによってエントリ数が決定。 例えば，上限値を 10 と指定した場合，0-10 の範囲で次の三つの領域に区切られるため，3 エントリとなります。 • 0-7/13：0000 0000 0000 0xxx（2 進表記） • 8-9/15：0000 0000 0000 100x（2 進表記） • 10/16：0000 0000 0000 1010（2 進表記）

1 リストに上記のフロー検出条件を複数指定した場合，おのおののフロー検出条件で使用するエントリ数を掛け合わせた値が，1 リストで使用するエントリ数となります。

1 リストに上記のフロー検出条件を一つ指定した場合は，指定したフロー検出条件で使用するエントリ数が 1 リストで使用するエントリ数となります。

二つ以上指定した場合は，おのおののフロー検出条件で使用するエントリ数を掛け合わせた値が，1 リストで使用するエントリ数となります。

上記のフロー検出条件を指定していない場合は，1 リストで使用するエントリ数は 1 エントリとなります。

(2)　アクセスリストロギング

アクセスリストロギングの収容条件を次の表に示します。

表 3-34　アクセスリストロギングの収容条件

項目	収容条件
アクセスリストロギングを動作に指定できるフィルタのエントリ数	「(1)　フィルタ・QoS フロー　(a)　フィルタ・QoS フローエントリ数」に従う
最大アクセスリストログ統計情報数	10000

(3)　ポリサー

ポリサーの収容条件を示します。

(a)　ポリサーのエントリ数

ポリサーエントリを指定した QoS フローをインタフェースに適用すると，ポリサーのエントリを消費します。ハードウェアプロファイルごとのポリサーの最大エントリ数を次に示します。

表 3-35　router-1 でのポリサーの最大エントリ数

モデル	受信側の最大エントリ数		送信側の最大エントリ数	
	PRU 当たり	装置当たり	PRU 当たり	装置当たり
AX8608R	64000	128000	64000	128000
AX8616R	64000	256000	64000	256000
AX8632R	64000	512000	64000	512000

表 3-36　router-1s でのポリサーの最大エントリ数

モデル	受信側の最大エントリ数		送信側の最大エントリ数	
	PRU 当たり	装置当たり	PRU 当たり	装置当たり
AX8608R	64000	128000	64000	128000
AX8616R	64000	256000	64000	256000
AX8632R	64000	512000	64000	512000

(b)　帯域監視機能による使用エントリ数

ポリサーエントリに指定した帯域監視機能の内容によって，1 ポリサーエントリで使用するエントリ数が異なります。1 ポリサーエントリで使用するポリサーのエントリ数を次の表に示します。

表 3-37　1 ポリサーエントリで使用するポリサーのエントリ数

1 ポリサーエントリに指定した帯域監視機能	使用エントリ数
最大帯域監視だけ	1
最低帯域監視だけ	1
最大帯域監視と最低帯域監視の両方	2

(4)　階層化シェーパ【OP-SHPS】

階層化シェーパの収容条件を示します。

(a)　階層化シェーパを設定できる NIF 数

階層化シェーパを設定できる NIF 数を次の表に示します。

表 3-38　階層化シェーパを設定できる NIF 数

項目	最大数
階層化シェーパ標準モードを設定できる NIF 数	オプションライセンス OP-SHPS の設定数／装置
階層化シェーパ拡張モードを設定できる NIF 数【OP-SHPE】	オプションライセンス OP-SHPE の設定数／装置

(b)　シェーパユーザ個別設定時の装置当たりのシェーパユーザ数

階層化シェーパユーザを，シェーパユーザワンタッチ設定機能を使用しないで個別に設定する場合の収容条件を示します。

シェーパユーザ個別設定で使用する各設定要素の収容条件を次の表に示します。

表 3-39　シェーパユーザ個別設定で使用する各設定要素の収容条件

項目	最大数
帯域制御プロファイルを作成できる数	120／装置
シェーパユーザリストを作成できる数	64／装置

項目	最大数
シェーパユーザリストに設定できるシェーパユーザ数	3058／シェーパユーザリスト※1
シェーパユーザリストを適用できるイーサネットインタフェース数※2	制限なし ただし，階層化シェーパを設定した NIF およびポートであること
イーサネットインタフェースに適用できるシェーパユーザリスト数※2	1／イーサネットインタフェース

注※1　LLRLQ ユーザおよびデフォルトユーザを含みます。
注※2　適用できるインタフェースはイーサネットインタフェースだけです。

装置当たりのシェーパユーザ最大数は，ハードウェアプロファイルで決定します。装置当たりのシェーパユーザ数とは，イーサネットインタフェースに適用されているすべてのシェーパユーザリストに設定したシェーパユーザ数の総和です。例えば，シェーパユーザを三つ設定したシェーパユーザリストを五つのイーサネットインタフェースに適用した場合，シェーパユーザ数は 15 となります。なお，シェーパユーザワンタッチ設定機能で生成したシェーパユーザは対象としません。

表 3-40　装置当たりのシェーパユーザ数

ハードウェアプロファイル	シェーパユーザ最大数
router-1 router-1s	256000／装置※

注※　LLRLQ ユーザおよびデフォルトユーザを含みます。

(c)　ポート当たりのシェーパユーザ数

ポート当たりのシェーパユーザ数は，階層化シェーパで使用するモードによって異なります。使用するモードとシェーパユーザ数の対応を次の表に示します。なお，シェーパユーザワンタッチ設定機能では，シェーパユーザをすべて自動で生成します。

表 3-41　使用するモードとシェーパユーザ数の対応

NIF 略称	ユーザキュー数	シェーパユーザ数	
		標準モード	拡張モード【OP-SHPE】
NL1GA-12S NLXGA-12RS	8	128／ポート※	382／ポート※
	4	256／ポート※	3056／ポート※

注※　LLRLQ ユーザおよびデフォルトユーザを含みません。

(d)　シェーパユーザ決定でのシェーパユーザ数

シェーパユーザ決定を使用して，フローを自動で振り分ける場合の振り分け先シェーパユーザ数は，次に示す条件の組み合わせで決定します。なお，QoS フローによる決定は VLAN ID マッピングと同じになります。

- 階層化シェーパのユーザキュー数
- 拡張モードの使用有無
- シェーパユーザ決定での振り分け方法

これらの組み合わせによる，シェーパユーザ決定でのシェーパユーザ数を次の表に示します。

表 3-42　シェーパユーザ決定でのシェーパユーザ数

NIF 略称	ユーザキュー数	標準モード		拡張モード【OP-SHPE】	
		ランダム振り分け	VLAN ID マッピング／QoS フロー	ランダム振り分け	VLAN ID マッピング／QoS フロー
NL1GA-12S NLXGA-12RS	8	128／ポート※		256／ポート※	382／ポート※
	4	256／ポート※		2048／ポート※	3056／ポート※

注※　LLRLQ ユーザおよびデフォルトユーザを含みません。

3.2.7　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およびネットワーク全体で動作できる装置台数を次の表に示します。

表 3-43　L2 ループ検知の収容条件

項目		収容条件
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，Ring Protocol のどちらかを使用している場合	90pps（推奨値）※2
	スパニングツリー，Ring Protocol のどちらも使用していない場合	600pps（最大値）※3
ネットワーク全体で動作できる装置数		64 台

- 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の送信レート（pps）＝ L2 ループ検知フレーム送信対象の VLAN ポート数÷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 600pps 以内で変動します。

注※2
スパニングツリー，Ring Protocol のどちらかを使用している場合は，90pps 以下に設定してください。90pps より大きい場合，スパニングツリー，Ring Protocol の正常動作を保証できません。

注※3
600pps 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 600pps 以下に設定してください。

3.2.8　トラッキング機能

トラッキング機能に関する収容条件を次の表に示します。

表 3-44　トラッキング機能に関する収容条件

項目	収容条件
トラック名の設定数※	4096

注※　静的監視と動的監視で設定したトラック名の合計です。

静的監視に関する収容条件を次の表に示します。

表 3-45　静的監視に関する収容条件

項目	収容条件
ポーリング監視のトラック数	4096
インタフェース監視のトラック数	4096
リスト監視のトラック数	4096
全リスト監視トラックの延べ参照トラック数	32768
一つのリスト監視トラックの参照トラック数	16

3.2.9　ネットワークの管理

(1)　ポリシーベースミラーリング

ポリシーベースミラーリングの収容条件を次の表に示します。なお，フロー検出モードによって，使用できるエントリ数の最大値が異なります。詳細は，「3.2.1　テーブルエントリ数　(4)　ハードウェアプロファイルと配分パターンの関係」を参照してください。また，複数エントリを使用するアクセスリストのエントリ算出方法については，「3.2.6　フィルタ・QoS　(1)　フィルタ・QoS フロー　(b)　フロー検出条件による使用エントリ数」を参照してください。

表 3-46　送信先インタフェースリストを動作に指定したアクセスリストのエントリ数

モデル	ポリシーベースミラーリングの最大エントリ数	
	PRU 当たり	装置当たり
AX8608R	4000	8000
AX8616R	4000	16000
AX8632R	4000	32000

ポリシーベースミラーリングで使用する送信先インタフェースリストの収容条件を次の表に示します。

表 3-47　ポリシーベースミラーリングの送信先インタフェースリストのエントリ数

項目	エントリ数
ポリシーベースミラーリングの送信先インタフェースリスト数	16※
1 ポリシーベースミラーリングの送信先インタフェースリスト当たりの最大インタフェース数	7

注※

複数のアクセスリストで同一のポリシーベースミラーリングの送信先インタフェースリストを指定できます。その場合，使用するポリシーベースミラーリングの送信先インタフェースリスト数は 1 リストと計算します。

(2)　CFM

CFM を使用できるハードウェアプロファイルを次の表に示します。

表 3-48　CFM のサポート状況

ハードウェアプロファイル	サポート
router-1	○
router-1s	×

（凡例）　○：サポート　×：未サポート

CFM のドメイン，MA，MEP，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 3-49　ドメイン・MA・MEP・CFM ポート総数・リモート MEP 総数の収容条件

モデル	ドメイン数	MA 数	MEP 数	CFM ポート総数 ※1※2	リモート MEP 総数 ※2※3
AX8600R シリーズ共通	8／装置	16380／装置	16380／装置	16380／装置	49152／装置

注※1

CFM ポート総数とは，CFM のフレームを送信するインタフェースの総数です。CFM ポート総数は運用コマンド show cfm summary で確認できます。

また，MEP を設定していない MA も CFM ポート総数に含みます。

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 3-50　CCM 送信間隔による収容条件

モデル	CCM 送信間隔の最小値	CFM ポート総数	リモート MEP 総数
AX8600R シリーズ共通	1 分以上	16380	49152
	10 秒	4096	12288
	1 秒	1024	1024

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。

MEP を設定できる物理ポートおよびチャネルグループの収容条件を次の表に示します。

表 3-51　MEP を設定できる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 を設定できる物理ポートおよびチャネルグループの総数※
AX8600R シリーズ共通	全ポート

注※

MEP 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。

CFM のデータベースの収容条件を次の表に示します。ここで示す値は，IEEE802.1ag と ITU-T Y.1731 を合計した数です。

表 3-52　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	Linktrace データベースエントリ数※
AX8600R シリーズ共通	49152	2048

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 8 ルート分を保持します（2048÷256 装置＝ 8 ルート）。

3.2.10　IP インタフェースと IP パケット中継

(1)　IP インタフェース数

IPv4 アドレスおよび IPv6 アドレスを設定したインタフェースを IP インタフェースと呼びます。本装置では，次のインタフェースに IP アドレスを設定できます。

- イーサネットインタフェース
- イーサネットサブインタフェース
- ポートチャネルインタフェース
- ポートチャネルサブインタフェース
- VLAN インタフェース
- マネージメントポート
- シリアル接続ポート（AUX）
- ループバックインタフェース

本装置で使用できる最大 IP インタフェース数を次の表に示します。なお，IPv4 アドレスと IPv6 アドレスを同一のインタフェースで使用することも，個別に使用することもできます。

表 3-53　最大 IP インタフェース数

IP インタフェース種別	IP インタフェース数
イーサネットインタフェース	16380※1
イーサネットサブインタフェース	
ポートチャネルインタフェース	
ポートチャネルサブインタフェース	
VLAN インタフェース	
マネージメントポート	1
シリアル接続ポート（AUX）※2	1
ループバックインタフェース※3	1537

注※1

イーサネットインタフェース，イーサネットサブインタフェース，ポートチャネルインタフェース，ポートチャネルサブインタフェース，および VLAN インタフェースの合計数です。ただし，イーサネットサブインタフェース，ポー

トチャネルインタフェース，ポートチャネルサブインタフェース，および VLAN インタフェースの合計数は 16000 となります。

注※2

IPv4 アドレスだけを使用できます。

注※3

グローバルネットワークおよび VRF ごとに一つ使用できます。それ以外に，グローバルネットワークおよび任意の VRF に 512 個使用できます。

(2)　マルチホームの最大サブネット数

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 アドレスを設定できます。

(a)　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。ここで示す値は，コンフィグレーションで一つのインタフェースに設定できるアドレス数です。

表 3-54　マルチホームの最大サブネット数（IPv4 の場合）

IP インタフェース種別	マルチホームのサブネット数
イーサネットインタフェース	256
イーサネットサブインタフェース	256
ポートチャネルインタフェース	256
ポートチャネルサブインタフェース	256
VLAN インタフェース	256
マネージメントポート	1
シリアル接続ポート（AUX）	1
ループバックインタフェース	1

(b)　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。ここで示す値は，コンフィグレーションで一つのインタフェースに設定できるアドレス数です。

表 3-55　マルチホームの最大サブネット数（IPv6 の場合）

IP インタフェース種別	マルチホームのサブネット数
イーサネットインタフェース	7
イーサネットサブインタフェース	7
ポートチャネルインタフェース	7
ポートチャネルサブインタフェース	7
VLAN インタフェース	7
マネージメントポート	7

IP インタフェース種別	マルチホームのサブネット数
ループバックインタフェース	1

(3)　IP アドレス最大設定数

(a)　IPv4 アドレス

コンフィグレーションで装置に設定できる IPv4 アドレスの最大数を次の表に示します。

表 3-56　コンフィグレーションで装置に設定できる IPv4 アドレスの最大数

IP インタフェース種別	IPv4 アドレス数
イーサネットインタフェース	16672※
イーサネットサブインタフェース	
ポートチャネルインタフェース	
ポートチャネルサブインタフェース	
VLAN インタフェース	
マネージメントポート	1
シリアル接続ポート（AUX）	1
ループバックインタフェース	1537

注※

イーサネットインタフェース，イーサネットサブインタフェース，ポートチャネルインタフェース，ポートチャネルサブインタフェース，および VLAN インタフェースの合計数です。ただし，イーサネットサブインタフェース，ポートチャネルインタフェース，ポートチャネルサブインタフェース，および VLAN インタフェースの合計数は 16000 となります。

(b)　IPv6 アドレス

コンフィグレーションで装置に設定できる IPv6 アドレスの最大数を次の表に示します。なお，ここで示す値にはコンフィグレーションで設定した IPv6 リンクローカルアドレスの数も含みます。

表 3-57　コンフィグレーションで装置に設定できる IPv6 アドレスの最大数

IP インタフェース種別	IPv6 アドレス数
イーサネットインタフェース	16672※
イーサネットサブインタフェース	
ポートチャネルインタフェース	
ポートチャネルサブインタフェース	
VLAN インタフェース	
マネージメントポート	7
ループバックインタフェース	1537

注※

イーサネットインタフェース，イーサネットサブインタフェース，ポートチャネルインタフェース，ポートチャネルサブインタフェース，および VLAN インタフェースの合計数です。ただし，イーサネットサブインタフェース，ポートチャネルインタフェース，ポートチャネルサブインタフェース，および VLAN インタフェースの合計数は 16000 となります。

一つのインタフェースには必ず一つの IPv6 リンクローカルアドレスが設定されます。コンフィグレーションでインタフェースに IPv6 グローバルアドレスを設定した場合，インタフェースには自動で IPv6 リンクローカルアドレスが設定されます。また，ループバックインタフェースにはリンクローカルアドレスのほかに，VRF ごとに自動でアドレス「::1/128」が一つ設定されます。そのため，実際に装置に設定される IPv6 アドレスの最大数は次の表に示す値となります。

表 3-58　装置に設定される IPv6 アドレスの最大数

IP インタフェース種別	コンフィグレーションで設定する IPv6 アドレス数	自動で設定される IPv6 アドレス数	合計数
イーサネットインタフェース	16672※	16380※	33052※
イーサネットサブインタフェース			
ポートチャネルインタフェース			
ポートチャネルサブインタフェース			
VLAN インタフェース			
マネージメントポート	7	1	8
ループバックインタフェース	1537	2562	4099

注※

イーサネットインタフェース，イーサネットサブインタフェース，ポートチャネルインタフェース，ポートチャネルサブインタフェース，および VLAN インタフェースの合計数です。

(4)　最大相手装置数

本装置が接続する，通信できる最大相手装置数を示します。

(a)　ARP エントリ数

IPv4 の場合，ARP によって，送信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。最大相手装置数は ARP エントリ数によって決まります。ARP エントリは，コンフィグレーションコマンドを使用することで，スタティックにエントリ登録できます。コンフィグレーションで設定できるスタティック ARP エントリの最大数を次の表に示します。

表 3-59　スタティック ARP の収容条件

項目	収容条件
スタティック ARP エントリ数	65535

本装置でサポートする ARP エントリの最大数については，「3.2.1　テーブルエントリ数」を参照してください。なお，ARP エントリの最大数は，スタティック ARP のエントリ数を含みます。

(b)　NDP エントリ数

IPv6 の場合，NDP でのアドレス解決によって，送信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。最大相手装置数は NDP エントリ数によって決まります。NDP エントリは，コンフィグレーションコマンドを使用することで，スタティックにエントリ登録できます。コンフィグレーションで設定できるスタティック NDP エントリの最大数を次の表に示します。

表 3-60　スタティック NDP の収容条件

項目	収容条件
スタティック NDP エントリ数	65535

本装置でサポートする NDP エントリの最大数については，「3.2.1　テーブルエントリ数」を参照してください。なお，NDP エントリの最大数は，スタティック NDP のエントリ数を含みます。

(c)　RA の最大インタフェース数

RA ではルータから通知される IPv6 アドレス情報を基に端末でアドレスを生成します。本装置の最大インタフェース数および最大プレフィックス数を次の表に示します。

表 3-61　RA の収容条件

項目		収容条件
最大インタフェース数		16380
最大プレフィックス数	インタフェース当たり	7
	装置当たり	32760

(5)　VRF

設定できる VRF 数を次の表に示します。VRF 数にグローバルネットワークは含みません。

表 3-62　VRF の収容条件

項目	収容条件
VRF 数	1024

(6)　ポリシーベースルーティング

ポリシーベースルーティングの収容条件を次の表に示します。

表 3-63　装置当たりのポリシーベースルーティングのエントリ数

項目	エントリ数
ポリシーベースルーティングを指定したアクセスリストのエントリ数	「3.2.6　フィルタ・QoS　(1)　フィルタ・QoS フロー　(a)　フィルタ・QoS フローエントリ数」に示す，ハードウェアプロファイルごとの「フィルタの最大エントリ数」に含む※1
IPv4 ポリシーベースルーティングリスト数	4096※2
IPv6 ポリシーベースルーティングリスト数	4096※2

項目	エントリ数
1 ポリシーベースルーティングリスト当たりの最大ネクストホップ数	8

注※1

エントリ数の算出方法は，「3.2.6　フィルタ・QoS」を参照してください。

注※2

複数のアクセスリストで同一のポリシーベースルーティングリストを指定できます。その場合，使用するポリシーベースルーティングリスト数は 1 リストと計算します。

(7)　DHCP/BOOTP リレーエージェント

DHCP/BOOTP リレーエージェントの収容条件を次の表に示します。

表 3-64　DHCP/BOOTP リレーエージェントの収容条件

項目	収容条件
クライアント接続インタフェース数	16379
クライアント数	65516
アドレス割り当て数	65516
サーバ数	4096
サーバ数（グローバルネットワーク当たり）	16
サーバ数（VRF 当たり）	16
サーバ数（インタフェース当たり）	16

(8)　DHCPv6 リレーエージェント

DHCPv6 リレーエージェントの収容条件を次の表に示します。

表 3-65　DHCPv6 リレーエージェントの収容条件

項目	収容条件
クライアント接続インタフェース数	16379
クライアント数	131032
アドレス割り当て数（IA_NA，IA_TA，IA_PD の合計）	131032
サーバ数	4096
サーバ数（グローバルネットワーク当たり）	4096
サーバ数（インタフェース当たり）	16
スタティック経路自動生成数	131032

(9)　VRRP

VRRP の収容条件を次の表に示します。

表 3-66　VRRP の収容条件

項目		収容条件
仮想ルータ最大数※	インタフェース当たり	255
	装置当たり	255
トラッキング連携でのトラック適用数	仮想ルータ当たり	16
	装置当たり	255

注※　IPv4/IPv6 の仮想ルータの合計数です。

表 3-67　VRRP の収容条件（グループ切替機能使用時）

項目		収容条件
仮想ルータ最大数※	インタフェース当たり	255
	装置当たり	16380
トラッキング連携でのトラック適用数	仮想ルータ当たり	16
	装置当たり	255
最大グループ数		255
1 グループ当たりの最大フォロー仮想ルータ数		16379

注※　IPv4/IPv6 の仮想ルータの合計数は 255 までです。ただし，グループ切替機能を利用し，フォロー仮想ルータを作成することで，最大 16380 の仮想ルータが動作できます。

3.2.11　ユニキャストルーティング

(1)　最大隣接ルータ数

最大隣接ルータ数の定義を次の表に示します。

表 3-68　最大隣接ルータ数の定義

ルーティングプロトコル別	最大隣接ルータ数の定義
スタティックルーティング	ネクストホップアドレスの数
RIP，RIPng	本装置の RIP または RIPng が動作するネットワーク上の RIP または RIPng ルータ数
OSPF，OSPFv3	本装置が OSPF または OSPFv3 指定ルータ（DR，BDR）になるネットワークの場合，そのネットワーク上のそのほかすべての OSPF または OSPFv3 ルータ数。本装置が OSPF または OSPFv3 指定ルータにならないネットワークの場合，そのネットワーク上の指定ルータ（DR，BDR）数。
BGP4，BGP4+	BGP4 または BGP4+ピア数

最大隣接ルータ数を次の表に示します。

表 3-69　最大隣接ルータ数

ルーティングプロトコル	最大隣接ルータ数
スタティックルーティング（IPv4，IPv6 の合計）	32760※
RIP	200
RIPng	200
OSPF	250
OSPFv3	125
BGP4	500
BGP4+	500
RIP，RIPng，OSPF，OSPFv3，BGP4，BGP4+の合計	512

注※　動的監視機能を使用する隣接ルータは，ポーリング間隔によって数が制限されます。詳細を次の表に示します。

表 3-70　スタティックの動的監視機能を使用できる最大隣接ルータ数

ポーリング周期	動的監視機能を使用できる最大隣接ルータ数
1 秒	240
5 秒	1200

(2)　経路エントリ数と最大隣接ルータ数の関係

最大経路エントリ数と最大隣接ルータ数の関係を次の表に示します。

表 3-71　経路エントリ数と最大隣接ルータ数の関係

ルーティングプロトコル	経路エントリ数※1	最大隣接ルータ数※2
RIP	2000	100
	10000	20
RIPng	2000	100
	10000	20
OSPF※3※4	1000	250
	5000	50
	10000	25
	100000	3
OSPFv3※3※5	1000	125
	5000	25
	10000	12
	100000	3

ルーティングプロトコル	経路エントリ数※1	最大隣接ルータ数※2
BGP4	※6	500
BGP4+	※6	500

注※1

経路エントリ数は代替経路を含みます。

注※2

各ルーティングプロトコル（RIP，RIPng，OSPF，OSPFv3，BGP4，BGP4+）を併用して使用する場合の最大隣接ルータ数は，それぞれ 1/n（n：使用ルーティングプロトコル数）です。例えば，BGP4，BGP4+を使用しないで，OSPF（1000 経路）と OSPFv3（1000 経路）を併用して使用する場合の最大隣接ルータ数は 1/2 となり，OSPF では 125，OSPFv3 では 62 となります。

注※3

OSPF/OSPFv3 の最大経路エントリ数は LSA 数を意味します。

注※4

VRF で OSPF を使用している場合，装置全体の最大隣接ルータ数は 250 ですが，各 VRF で保持している LSA 数×各 VRF の隣接ルータ数の総計が 25 万を超えないようにしてください。

注※5

VRF で OSPFv3 を使用している場合，装置全体の最大隣接ルータ数は 125 ですが，各 VRF で保持している LSA 数×各 VRF の隣接ルータ数の総計が 12 万 5 千を超えないようにしてください。

注※6

「3.2.2　経路配分パターン」を参照してください。

(3)　本装置で設定できるコンフィグレーションの最大数

ルーティングプロトコルについて，設定できるコンフィグレーションの最大数を次の表に示します。

なお，この表で示す値はコンフィグレーションで設定できる最大数です。運用する際は本章にある収容条件をすべて満たすようにしてください。

表 3-72　コンフィグレーションの最大設定数

分類	コンフィグレーション コマンド	最大数の定義	最大 設定数
IPv4 集約経路	ip summary-address	設定行数	1024
IPv6 集約経路	ipv6 summary-address	設定行数	1024
IPv4 スタティック	ip route	設定行数	262144
IPv6 スタティック	ipv6 route	設定行数	262144
RIP	network	設定行数	256
	ip rip authentication key	設定行数	512
OSPF	area range	設定行数	1024
	area virtual-link	authentication-key，message-digest-key パラメータを設定した行数の総計	512
	ip ospf authentication-key	各設定行数の総計	512

分類	コンフィグレーション コマンド	最大数の定義	最大 設定数
	ip ospf message-digest-key		
	network	設定行数	512
	router ospf	設定行数	256
OSPFv3	area range	設定行数	1024
	ipv6 router ospf	設定行数	128
BGP4	network	設定行数	1024
BGP4+	network	設定行数	1024
経路フィルタ	distribute-list in（RIP） distribute-list out（RIP） redistribute（RIP）	各設定行数の総計	2048
	distribute-list in（OSPF） distribute-list out（OSPF） redistribute（OSPF）	各設定行数の総計	2048
	distribute-list in（BGP4） distribute-list out（BGP4） redistribute（BGP4）	各設定行数の総計	2048
	distribute-list in（RIPng） distribute-list out（RIPng） redistribute（RIPng）	各設定行数の総計	2048
	distribute-list in（OSPFv3） distribute-list out（OSPFv3） redistribute（OSPFv3）	各設定行数の総計	1024
	distribute-list in（BGP4+） distribute-list out（BGP4+） redistribute（BGP4+）	各設定行数の総計	2048
	ip as-path access-list	設定<id>の種類数	1024
		設定行数	4096
	ip community-list	設定<id>の種類数	512
		standard 指定の設定行数	1024
		expanded 指定の設定行数	1024
	ip prefix-list	設定<id>の種類数	2048
		設定行数	80000
	ipv6 prefix-list	設定<id>の種類数	2048
		設定行数	80000

分類	コンフィグレーション コマンド	最大数の定義	最大 設定数
	neighbor in（BGP4） neighbor out（BGP4）	<ipv4 address>の設定行数の総計	1024
		<peer group>の設定行数の総計	1024
	neighbor in（BGP4+） neighbor out（BGP4+）	<ipv6 address>の設定行数の総計	1024
		<peer group>の設定行数の総計	1024
	route-map	設定<id>の種類数	1024
		設定<id>と<seq>の組み合わせ種類数	4096
	match as-path	各設定行で指定したパラメータの総計	4096
	match community	各設定行で指定したパラメータの総計	4096
	match interface	各設定行で指定したパラメータの総計	2048
	match ip address match ipv6 address	各設定行で指定したパラメータの総計	4096
	match ip route-source match ipv6 route-source	各設定行で指定したパラメータの総計	2048
	match origin	設定行数	2048
	match protocol	各設定行で指定したパラメータの総計	4096
	match route-type	設定行数	2048
	match tag	各設定行で指定したパラメータの総計	2048
	match vrf	各設定行で指定したパラメータの総計	4096
	set as-path prepend count set distance set local-preference set metric set metric-type set origin set tag	どれか一つが設定された route-map の，<id>と<seq>の組み合わせ種類数	4096
	set community	各設定行で指定したパラメータの総計	2048
	set community-delete	各設定行で指定したパラメータの総計	2048

3.2.12　マルチキャストルーティング

IPv4 マルチキャストおよび IPv6 マルチキャストの収容条件を次に示します。複数の VRF で IPv4 マルチキャストまたは IPv6 マルチキャストを使用する場合，グローバルネットワークとすべての VRF の合計を本収容条件内に収めてください。

(1)　マルチキャストの収容条件

IPv4 マルチキャストおよび IPv6 マルチキャストの収容条件を次の表に示します。

表 3-73　マルチキャストの収容条件

項目	最大数	
	IPv4 マルチキャスト	IPv6 マルチキャスト
PIM-SM および PIM-SSM マルチキャストインタフェース数	512／装置※1	512／装置
IGMP および MLD 動作インタフェース数	4095／装置※1	4095／装置
マルチキャスト送信者の数	PIM-SM 使用時 256／グループ PIM-SSM 使用時 512／グループ※2 4000／装置	PIM-SM 使用時 256／グループ PIM-SSM 使用時 512／グループ※2 4000／装置
すべてのマルチキャスト中継エントリの下流インタフェースの合計※3	router-1 560000／装置 router-1s 280000／装置	
PIM-SM または PIM-SSM のマルチキャスト経路情報数（(S,G)マルチキャスト経路情報および(*,G)マルチキャスト経路情報の合計） • S：送信元アドレス • G：グループアドレス	router-1 8000／装置※4 router-1s 8000／装置※4	router-1 8000／装置 router-1s 8000／装置
PIM-SM または PIM-SSM のマルチキャスト中継エントリ数※5 (マルチキャスト中継エントリおよびネガティブキャッシュエントリの合計)	router-1 8000／装置 router-1s 8000／装置	router-1 8000／装置 router-1s 8000／装置
IGMP および MLD のマルチキャストグループ参加数※6※7	256／インタフェース 32768／装置	256／インタフェース 32768／装置
IGMP および MLD でのグループアドレス当たりの送信元アドレス数	PIM-SM 使用時 256／グループ PIM-SSM 使用時 512／グループ※2	PIM-SM 使用時 256／グループ PIM-SSM 使用時 512／グループ※2

注※1

PIM Join/Prune メッセージの送信間隔によって，インタフェース数が変わります。「表 3-74　PIM Join/Prune メッセージの送信間隔に対する IPv4 マルチキャストインタフェース数」に示す範囲内で使用してください。

注※2

PIM-SSM だけを使用している場合の収容条件です。PIM-SM および PIM-SSM を併用している場合は，256／グループになります。

注※3

すべてのマルチキャスト中継エントリの下流インタフェースの合計は，IPv4 マルチキャストと IPv6 マルチキャストの合計です。

注※4

PIM Join/Prune メッセージの送信間隔によって，マルチキャスト経路情報数が変わります。「表 3-75　PIM Join/Prune メッセージの送信間隔に対する IPv4 マルチキャスト経路情報数」に示す範囲内で使用してください。

注※5

マルチキャスト中継エントリとは，「3.2.1　テーブルエントリ数」に示す IPv4 マルチキャスト経路および IPv6 マルチキャスト経路を指します。

注※6

マルチキャストグループ参加数は，IGMP Report メッセージおよび MLD Report メッセージの最大受信数を示します。

注※7

装置当たりのマルチキャストグループ参加数とは，すべてのインタフェースで参加しているマルチキャストグループ数の合計です。

表 3-74　PIM Join/Prune メッセージの送信間隔に対する IPv4 マルチキャストインタフェース数

PIM Join/Prune メッセージの送信間隔※	IPv4 マルチキャストインタフェース数
30 秒以上	4095／装置
20～29 秒	2047／装置
19 秒以下	255／装置

注※

各インタフェースに設定している PIM Join/Prune メッセージの送信間隔のうち，最小の値が対象となります。

表 3-75　PIM Join/Prune メッセージの送信間隔に対する IPv4 マルチキャスト経路情報数

PIM Join/Prune メッセージの送信間隔※	IPv4 マルチキャスト経路情報数
10 秒以上	8000／装置
4～9 秒	4000／装置
3 秒以下	1500／装置

注※

各インタフェースに設定している PIM Join/Prune メッセージの送信間隔のうち，最小の値が対象となります。

(2)　PIM-SM 関連の収容条件

本装置で使用する PIM-SM 関連の収容条件を次の表に示します。

表 3-76　PIM-SM 関連の収容条件

項目	最大数	
	IPv4 マルチキャスト	IPv6 マルチキャスト
隣接ルータ数	256／インタフェース	256／インタフェース

項目	最大数	
	IPv4 マルチキャスト	IPv6 マルチキャスト
	512／装置	512／装置
ランデブーポイント候補数	2／グループアドレス	2／グループアドレス
1 装置当たりランデブーポイントで設定できるグループアドレス数※	128／ネットワーク（VPN） 512／装置	128／ネットワーク（VPN） 512／装置
1 ネットワーク（VPN）当たりランデブーポイントに設定できるグループアドレス数	1024／ネットワーク（VPN） 1024／装置	128／ネットワーク（VPN） 512／装置
1 ネットワーク（VPN）当たりのランデブーポイント候補数	1024／ネットワーク（VPN） 1024／装置	128／ネットワーク（VPN） 512／装置
ブートストラップルータ候補数	512／装置	512／装置
静的ランデブーポイントルータアドレス数	16／ネットワーク（VPN） 512／装置	16／ネットワーク（VPN） 512／装置
マルチキャストサーバ仮想接続機能の設定数	－	128／インタフェース 256／装置

（凡例）－：該当なし

注※

グループアドレスを指定しないでランデブーポイントを設定した場合，デフォルトのグループアドレス（IPv4 では 224.0.0.0/4，IPv6 では ff00::/8）が設定されます。なお，グローバルネットワークおよび VRF でランデブーポイントを設定する場合，デフォルトのグループアドレスも 1 グループアドレスとして使用します。

(3)　IGMP/MLD 関連の収容条件

本装置で使用する IGMP および MLD 関連の収容条件を次の表に示します。

表 3-77　IGMP/MLD 関連の収容条件

項目	最大数	
	IPv4 マルチキャスト	IPv6 マルチキャスト
静的グループ参加数※1	256／インタフェース 4000／装置	256／インタフェース 4000／装置
IGMP/MLD PIM-SSM 連携機能の設定数（送信元アドレスとグループアドレスのペア数）※2	2048／装置※3	1024／装置※4
IGMPv3 および MLDv2 で 1Report メッセージ当たり処理できる Record 情報	32Record／メッセージ 32 ソース／Record	32Record／メッセージ 32 ソース／Record
IGMPv3 および MLDv2 で 1Report メッセージ当たり処理できるソース数※5	256 ソース／メッセージ	256 ソース／メッセージ
インタフェースに設定するマルチキャストチャネルリスト数※6	－	8／インタフェース
マルチキャストチャネルリストに設定するアクセスリスト数※7	－	2048／装置

項目	最大数	
	IPv4 マルチキャスト	IPv6 マルチキャスト
マルチキャストチャネルリストに設定するマルチキャストチャネル数	－	32／マルチキャストチャネルリスト
帯域容量を設定したマルチキャストチャネルリスト数	－	2048／装置
帯域容量を設定したマルチキャストチャネル数	－	2048／装置
マルチキャストチャネル受信者数※8	－	65536／装置 400／インタフェース

（凡例）－：該当なし

注※1

静的グループ参加数とは，各マルチキャストインタフェースで静的参加するマルチキャストグループの合計です。複数のインタフェースで同一マルチキャストグループに静的参加した場合，静的グループ参加数は一つではなく，静的参加したインタフェースの数になります。

注※2

マルチキャストで使用するインタフェース数によって，設定できる数が変わります。「表 3–78　使用インタフェース数に対する IGMP/MLD PIM-SSM 連携機能の設定数」に示す範囲内で使用してください。

注※3

マルチキャストグループ参加数によって，1 グループアドレスに連携できる送信元アドレス数が変わります。「表 3–79　IGMP PIM-SSM 連携機能で 1 グループアドレスに連携できる送信元アドレス数」に示す範囲内で使用してください。なお，IGMP PIM-SSM 連携機能は，マルチキャストグループ参加数に関係なく収容条件の最大数まで設定できます。

注※4

マルチキャストグループ参加数によって，設定できる数が変わります。「表 3–80　マルチキャストグループ参加数に対する MLD PIM-SSM 連携機能の設定数」に示す範囲内で使用してください。

注※5

一つの IGMPv3 Report メッセージまたは MLDv2 Report メッセージの各 Record に格納されるソース数の合計です。ソース情報のない Record も 1 ソースとして数えます。

なお，IGMP/MLD PIM-SSM 連携機能を設定している場合は，その設定によって生成されるソース数も本収容条件の対象となります。

注※6

マルチキャストチャネルフィルタ機能，マルチキャストチャネル数制限機能，および帯域管理機能それぞれでの最大設定数です。

注※7

マルチキャストチャネルフィルタ機能，マルチキャストチャネル数制限機能，および帯域管理機能で使用する，マルチキャストチャネルリストに設定するアクセスリストの数です。マルチキャストチャネルフィルタ機能，マルチキャストチャネル数制限機能，および帯域管理機能で一つのアクセスリストを使用する場合，1 として数えます。

注※8

ホストトラッキング機能使用時のマルチキャストチャネルの総受信者数です。

表 3–78　使用インタフェース数に対する IGMP/MLD PIM-SSM 連携機能の設定数

使用インタフェース数	IGMP/MLD PIM-SSM 連携機能設定数
256	1024 以上
512	512

使用インタフェース数	IGMP/MLD PIM-SSM 連携機能設定数
1024	256
4095	64

表 3-79　IGMP PIM-SSM 連携機能で 1 グループアドレスに連携できる送信元アドレス数

マルチキャストグループ参加数※	1 グループアドレスに連携できる送信元アドレス数
128	512
256	256
512	128
1024	64
2048	32
4096	16
8192	8

注※

動的グループ参加数および静的グループ参加数の合計です。IGMP PIM-SSM 連携機能の対象ではないマルチキャストグループ参加も含みます。異なるインタフェースで同一のグループアドレスに参加している場合，マルチキャストグループ参加数は一つではなく，参加しているインタフェースの数になります。

表 3-80　マルチキャストグループ参加数に対する MLD PIM-SSM 連携機能の設定数

マルチキャストグループ参加数※	MLD PIM-SSM 連携機能設定数
64	1024
128	512
256	256
512	128
1024	64
2048	32
4096	16
8192	8

注※

動的グループ参加数および静的グループ参加数の合計です。MLD PIM-SSM 連携機能の対象ではないマルチキャストグループ参加も含みます。異なるインタフェースで同一のグループアドレスに参加している場合，マルチキャストグループ参加数は一つではなく，参加しているインタフェースの数になります。

(4)　VRF 関連の収容条件

VRF でマルチキャストルーティング機能を使用する場合の収容条件を次の表に示します。

表 3-81　VRF 関連の収容条件

項目	最大数	
	IPv4 マルチキャスト	IPv6 マルチキャスト
マルチキャストを設定できる VRF 数	512／装置	512／装置
マルチキャストエクストラネットのマルチキャストフィルタ数※	1024／装置	1024／装置
マルチキャストエクストラネットで使用する route-map 数	512／装置	512／装置

注※

すべての route-map で指定したアクセスリスト内のグループアドレスの合計です。

(5)　マルチキャストパケットの送信者に関する注意

マルチキャストパケットの送信者の中には，マルチキャストパケットをバーストトラフィックとして送信する特性を持つものがあります。この特性を持つ送信者から受信したマルチキャストパケットを，マルチキャスト配信する場合には注意が必要です。

マルチキャスト受信者の回線を収容するネットワークインタフェース機構（NIF）の種類によって，マルチキャストが動作できるインタフェース数が異なります。マルチキャスト送信できるインタフェース数を次の表に示します。なお，IPv4 マルチキャストと IPv6 マルチキャストを同時に使用する場合は，合計のインタフェース数となります。

表 3-82　マルチキャスト送信できるインタフェース数

NIF 略称	マルチキャスト送信できるインタフェース数（推奨値※）
NL1G-12T	ポート当たり 64 インタフェース
NL1G-12S	ポート当たり 64 インタフェース
NL1GA-12S	NIF 当たり 512 インタフェース
NLXG-6RS	ポート当たり 64 インタフェース
NLXGA-12RS	NIF 当たり 512 インタフェース
NLXLG-4Q	ポート当たり 128 インタフェース
NLCG-1Q	ポート当たり 512 インタフェース
NMCG-1C	ポート当たり 1024 インタフェース

注※

推奨値は，送信者がマルチキャストパケットを 8 バーストで送信する特性（8 パケット分のマルチキャストパケットをいったん蓄積したあとに，ネットワークに対して連続で送信する特性）を持っていることを想定しています。バースト数が大きくなるとマルチキャストパケットを一部廃棄することがあるので，マルチキャストを設定するインタフェース数を少なくする必要があります。

3.2.13　BFD

BFD の収容条件を次の表に示します。なお，BFD を設定するトラックの収容条件については，「3.2.8　トラッキング機能」を参照してください。

表 3-83　BFD の収容条件

項目	収容条件
BFD セッション数※	10000

注※

使用できるセッション数は，BFD と連携する機能およびプロトコルの収容条件の総計です。

BFD セッション数と BFD パケットの最小送受信間隔に関する収容条件を次の表に示します。装置に設定される BFD セッション数に合わせて，各 BFD セッションの最小送受信間隔が下限値を下回らないように設計してください。

表 3-84　最小送受信間隔の収容条件

BFD セッション数	最小送受信間隔の下限値（単位：ms）
1～1000	10
1001～5000	50
5001～10000	100

4 装置起動とログイン

この章では，装置を運用するために必要な運用端末と運用管理の概要，装置の起動と停止，およびログインとログアウトについて説明します。

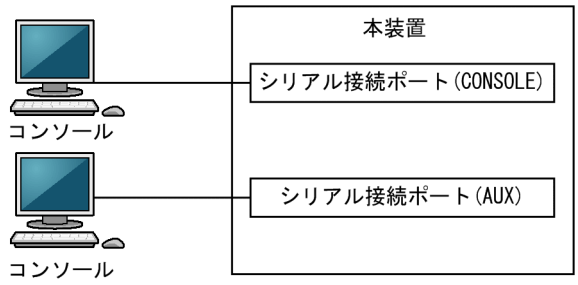
4.1　運用端末による管理

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，本装置のシリアル接続ポート（AUX）に接続することもできます。コンソールの接続形態を次の図に示します。

図 4-1　コンソールの接続形態

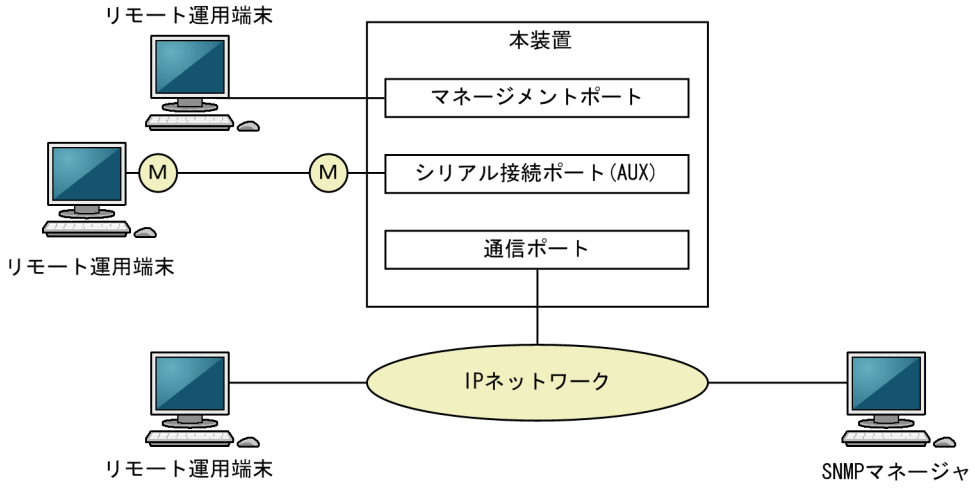


リモート運用端末は，次に示す三つの接続形態がとれます。

- マネージメントポート接続する形態
- 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
- シリアル接続ポート（AUX）にダイアルアップ IP 接続する形態

リモート運用端末の接続形態を次の図に示します。

図 4-2　リモート運用端末の接続形態



（凡例）(M)：モデム

(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介してログインできるので，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)　シリアル接続ポート（AUX）

シリアル接続ポート（AUX）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介してログインできるので，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。なお，シリアル接続ポート（AUX）から接続した場合，Rom，Boot 状態は表示されません。

(3)　マネージメントポート

マネージメントポートを介して，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。このポートを介して 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)　通信用ポート

マネージメントポートと同様の運用ができます。

(5)　シリアル接続ポート（AUX）にダイアルアップ IP 接続

リモート運用端末をマネージメントポート接続した場合と同様の運用ができます。本装置やモデムの設定については，「7.1.3　ダイアルアップ IP 接続」を参照してください。

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：9600bit/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
- フロー制御：なし

シリアル接続ポート（CONSOLE）接続の場合に，通信速度を 9600bit/s 以外（1200／2400／4800／19200bit/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。

なお，シリアル接続ポート（AUX）接続の場合は，通信速度は 9600bit/s 固定です。

図 4-3　コンソール接続時の通信速度の設定例

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

! 注意事項

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るので注意してください。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 9600bit/s 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。

! 注意事項

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。
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。

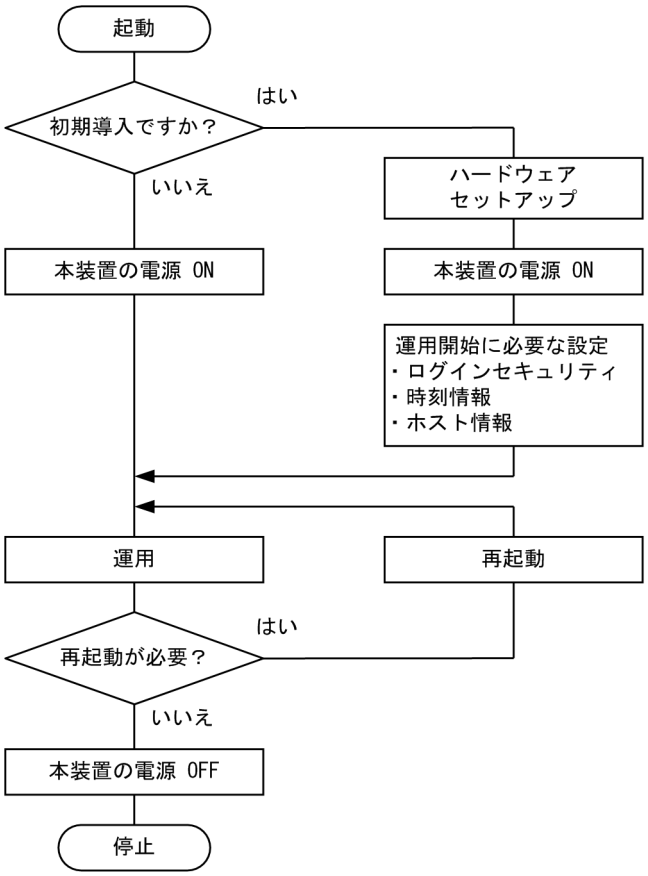
4.2　装置起動

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 4-4　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。	本体の電源スイッチを ON にします。
リセットによる再起動	障害発生などによって本装置をリセットしたい場合に行います。 再起動に掛かる時間はボードごとに異なります。	本体のリセットスイッチを押します。

起動の種類	内容	操作方法
コマンドによる再起動	障害発生などによって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。
デフォルトリスタート	パスワードを忘れてログインできない場合や，コマンド承認の設定ミスなどでコンソールからコマンドが実行できなくなった場合に行います。 デフォルトリスタート中はパスワードによるログイン認証，装置管理者モードへの変更（enable コマンド）時の認証，RADIUS/TACACS+認証，およびコマンド承認を行いません。また，コンフィグレーションにユーザアカウント"operator"の設定がなくても，ユーザ"operator"でログインできます。※セキュリティレベルが低下するため，デフォルトリスタートによる起動を行う場合は十分に注意してください。 なお，コンフィグレーションはデフォルトリスタートによって変更されません。 デフォルトリスタート中に設定したパスワードは，装置再起動後に有効になります。 デフォルトリスタートを実行する場合は，システム操作パネルから装置を停止したあとで実行してください。システム操作パネルから装置を停止する方法は，「12.1.9　装置の停止」を参照してください。 なお，BCU を二重化構成で運用している場合は，両系の BCU に対してデフォルトリスタートを実行してください。実行するときは，運用系，待機系の順で実施してください。	本体のリセットスイッチを５秒以上押します。

注※

コンフィグレーションにユーザアカウント"operator"の設定がない状態でユーザ"operator"を使用してログインする場合，次に示す共通のユーザ情報でログイン処理をします。

・ユーザ名：remote_user

・ホームディレクトリ：/usr/home/share

本装置を起動，再起動したときに STATUS ランプが赤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，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。

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，パスワードなしでログインできます。

図 4-5　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。ただし，デフォルトリスタートによる起動の場合は，コマンドプロンプト表示の前に次のワーニングメッセージを表示します。

```
*****************************************************************************
* WARNING!                                                                  *
* A default restart was performed on the device.                            *
* The security level of the device has been lowered.                        *
*****************************************************************************
```

(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 4-6　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　運用コマンド一覧

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て，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 Vol.1　10. 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を変更したり，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て，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 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できます）	>
装置管理者モード		#
コンフィグレーションモード	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。

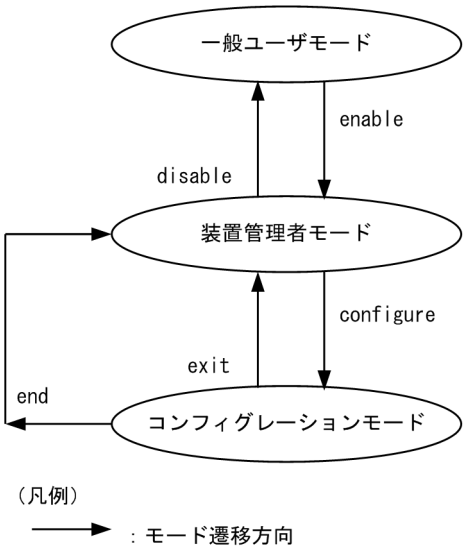
＜例＞

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. コンフィグレーションを編集して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，およびスタートアップコンフィグレーションを変更して編集中のコンフィグレーションと差分が発生した場合，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］キーを入力すると，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
```

また，［Tab］キーを入力すると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。補完機能を使用したパラメータやファイル名の表示例を次の図に示します。

図 5-4　補完機能を使用したパラメータやファイル名の表示例

```
(config)# interface [Tab]
async                 loopback              port-channel
gigabitethernet       mgmt                  range
hundredgigabitethernet  null                tengigabitethernet
(config)# interface
```

5.2.2　ヘルプ機能

コマンドライン上で「?」を入力すると，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 5-5　「?」入力時の表示例

```
> show port ?
  <port list>  <nif no.>/<port no.> ex."1/2", "2/1-5", "3/1,4/1", "*/*"
  statistics   Display the statistics information list of ports
  transceiver  Display the transceiver information list of ports
  <cr>
> show port
```

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］キーを入力したあと「?」を入力してください。

5.2.3　入力エラーメッセージ

コンフィグレーションコマンドまたは運用コマンドを不正に入力した場合，エラー位置を「^」で指摘して，次行にエラーメッセージを表示します。［Tab］キー入力時と「?」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入力してください。入力エラーメッセージの表示例を次に示します。

図 5-6　範囲外の数値を入力した場合の表示例

```
> show nif 33
show nif 33
         ^

% The value at the ^ marker is outside the valid range.
>
```

図 5-7　パラメータが不足している場合の表示例

```
> show ip
show ip
     ^
% The command at the ^ marker is invalid.
>
```

入力エラーメッセージ一覧を次の表に示します。

表 5-3　入力エラーメッセージ一覧

メッセージ	説明
% '<word>' is invalid in this location.	不正な文字'<word>'が入力されています。 <word>：不正な文字
% The combination with the already-entered parameter at the ^ marker is invalid.	「^」の個所で入力済みのパラメータが入力されています。
% The command at the ^ marker is invalid.	「^」の個所でコマンドを実行するのに必要なパラメータが不足しています。
% The command is too long.	一度に入力できる文字数を超えています。
% The command or parameter at the ^ marker is invalid.	「^」の個所で不正なコマンドまたはパラメータが入力されています。
% The format at the ^ marker is invalid.	「^」の個所で入力形式が不正なパラメータが入力されています。
% The IP address format at the ^ marker is invalid.	「^」の個所で不正な IPv4 アドレスまたは IPv6 アドレスが入力されています。
% The name at the ^ marker is invalid.	「^」の個所で不正な名称が入力されています。
% The parameter at the ^ marker is too long.	「^」の個所で桁数の制限以上のパラメータが入力されています。
% The value at the ^ marker is invalid.	「^」の個所で不正な数値が入力されています。
% The value at the ^ marker is outside the valid range.	「^」の個所で範囲外の数値が入力されています。

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て，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特定できる場合，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 5-8　短縮入力のコマンド実行例（show netstat interface の短縮入力）

```
> sh nets in [Enter]
Date 20XX/07/19 12:00:00 UTC
Name       Mtu   Network     Address        Ipkts Ierrs    Opkts Oerrs Colls
Eth1/2     1500  192.168/24  192.168.0.60    3896     2     2602     0     0
>
```

なお，短縮実行できるコンフィグレーションコマンドはコンフィグレーションのモードによって異なります。

コンフィグレーションコマンド show

　コンフィグレーションの各モードで短縮実行できます。

コンフィグレーションコマンド commit，end，quit，exit，rollback，save，status，top

グローバルコンフィグレーションモード，または template コマンド実行後に移行するサブモード（第二階層）でだけ短縮実行できます。ほかのモードで短縮実行すると入力エラーになります。

コンフィグレーションコマンド end-template

template コマンド実行後に移行するサブモード（第二階層）でだけ短縮実行できます。ほかのモードで短縮実行すると入力エラーになります。

コンフィグレーションコマンド delete，insert，replace

template コマンド実行後に移行するサブモード（第二階層）以降のモードで短縮実行できます。ほかのモードで短縮実行すると入力エラーになります。

上記以外の各モードのコンフィグレーションコマンド

各モードで一意に特定できたコマンドを短縮実行できます。

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 5-9 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 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 packets received, 0.0% packet loss
round-trip min/avg/max = 1.329/1.329/1.329 ms
>                                                           <-2
> ping 192.168.0.1 numeric count 1                          <-3
PING 192.168.0.1 (192.168.0.1): 56 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 packets received, 0.0% packet loss
round-trip min/avg/max = 1.225/1.225/1.225 ms
>                                                           <-4
> ping 192.168.0.2 numeric count 1                          <-5
PING 192.168.0.2 (192.168.0.2): 56 data bytes

--- 192.168.0.2 PING Statistics ---
1 packets transmitted, 0 packets received, 100.0% packet loss
>
```

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へ変換したあとで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 5-4　ヒストリのコマンド文字列変換で使用できる文字一覧

指定	説明
!!	直前に実行したコマンドへ変換して実行します。
!n	ヒストリ番号 n※のコマンドへ変換して実行します。
!-n	n 回前のコマンドへ変換して実行します。
!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。
^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。
- 装置を再起動すると，ヒストリ機能のコマンド履歴は消去されます。

5.2.6　パイプ機能

パイプ機能を利用すると，コマンドの実行結果を別のコマンドに引き継げます。実行結果を引き継ぐコマンドに grep コマンドを使うと，コマンドの実行結果をよりわかりやすくできます。「図 5-10　show sessions コマンド実行結果」に show sessions コマンドの実行結果を，「図 5-11　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 5-10　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 aux      -----  1   Jan  6 14:16 (ppp0:200.10.10.1)
operator ttyp0    -----  2   Jan  6 14:16 (192.168.3.7)
operator ttyp1    admin  3   Jan  6 14:16 (192.168.3.7)
```

図 5-11　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 ttyp1    admin  3   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と，コマンドの実行結果をファイルに出力できます。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 5-12　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

ページングが有効な場合，コマンドの実行によって出力される結果が一画面にすべて表示しきれないときに，ユーザのキー入力を契機として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しません。なお，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 でページング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。カスタマイズできる CLI 機能と CLI 環境情報を次の表に示します。

表 5-5　カスタマイズできる 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，入力できる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 で設定できます。または，次に示す運用コマンドで一時的に該当セッションでの動作を変更できます。

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

コンフィグレーションコマンドで設定した場合，一度ログアウトして再度ログインすると設定値が有効となります。運用コマンドで一時的に動作を変更した場合は，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。

5.3　CLI の注意事項

5.3.1　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。

5.3.2　CLI の特殊キー操作時にログアウトした場合

［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。

5.3.3　待機系のファイルにアクセスする場合

/standby ディレクトリ配下のファイルにアクセスする場合は，次の点に注意してください。

- 補完機能は使用できません。
- 運用コマンド cd で，/standby 配下のディレクトリに移動しないでください。
- 運用系のファイルにアクセスする場合に比べて，アクセスに時間が掛かります。

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の概要

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。

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て，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。

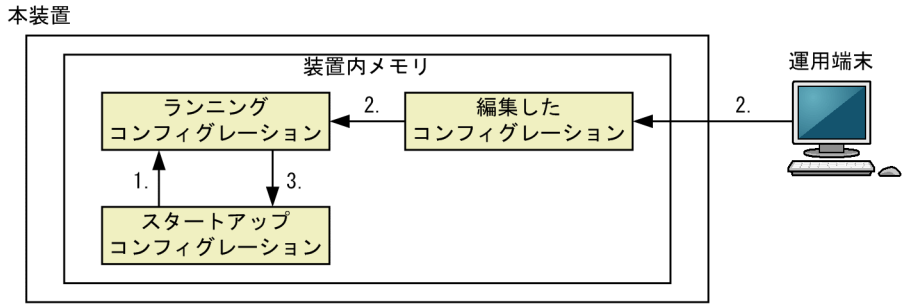
なお，スタートアップコンフィグレーションは，直接編集できません。コンフィグレーションを編集したあとに save コマンドまたは commit コマンドを使用することで，スタートアップコンフィグレーションが更新されます。

本装置では，編集した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に反映する方法が 2 とおりあり，コミットモードの設定によって選択できます。モードごとの反映方法を次に示します。

(1)　逐次コミットモード

編集した内容をすぐにランニングコンフィグレーションに反映します。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（逐次コミットモード）



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て，ランニングコンフィグレーションとしてロードされます。

   ランニングコンフィグレーションの内容で運用を開始します。

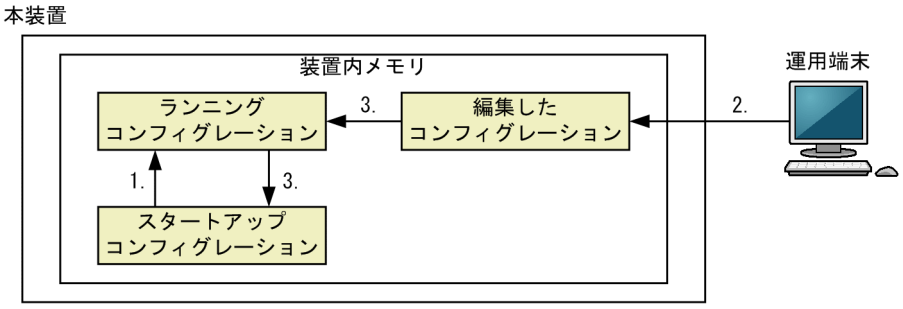
2. コンフィグレーションを編集します。編集内容は，すぐにランニングコンフィグレーションに反映されます。

3. save コマンドを実行すると，変更されたランニングコンフィグレーションがスタートアップコンフィグレーションに保存されます。

(2)　手動コミットモード

編集した内容をすぐにランニングコンフィグレーションに反映しません。commit コマンドを実行すると，編集した内容を一括でランニングコンフィグレーションに反映して，スタートアップコンフィグレーションに保存します。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 6-2　起動時および運用中のコンフィグレーションの概要（手動コミットモード）



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て，ランニングコンフィグレーションとしてロードされます。

   ランニングコンフィグレーションの内容で運用を開始します。

2. コンフィグレーションを編集します。編集内容は，すぐにランニングコンフィグレーションに反映されません。

3. commit コマンドを実行すると，編集したコンフィグレーションがランニングコンフィグレーションに反映されて，スタートアップコンフィグレーションに保存されます。

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，コミットモードが逐次コミットモードの場合，編集した内容をすぐにランニングコンフィグレーションに反映します。save コマンドを実行すると，編集したコンフィグレーションを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します。手動コミットモードの場合，編集した内容をすぐにランニングコンフィグレーションに反映しません。commit コマンドを実行することで，編集した内容を一括でランニングコンフィグレーションに反映して，スタートアップコンフィグレーションに保存します。

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。

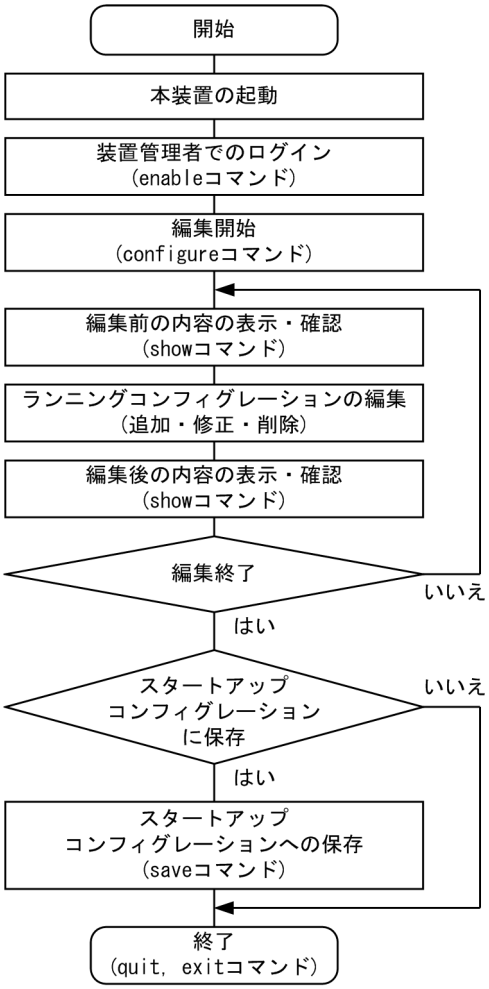
6.1.3　ランニングコンフィグレーションの編集の流れ

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はコンソールから編集する必要があります。

(1)　逐次コミットモードでの流れ

逐次コミットモードでの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。なお，configure コマンドでの編集開始後に，status コマンドでコミットモードが逐次コミットモードであることを確認してください。

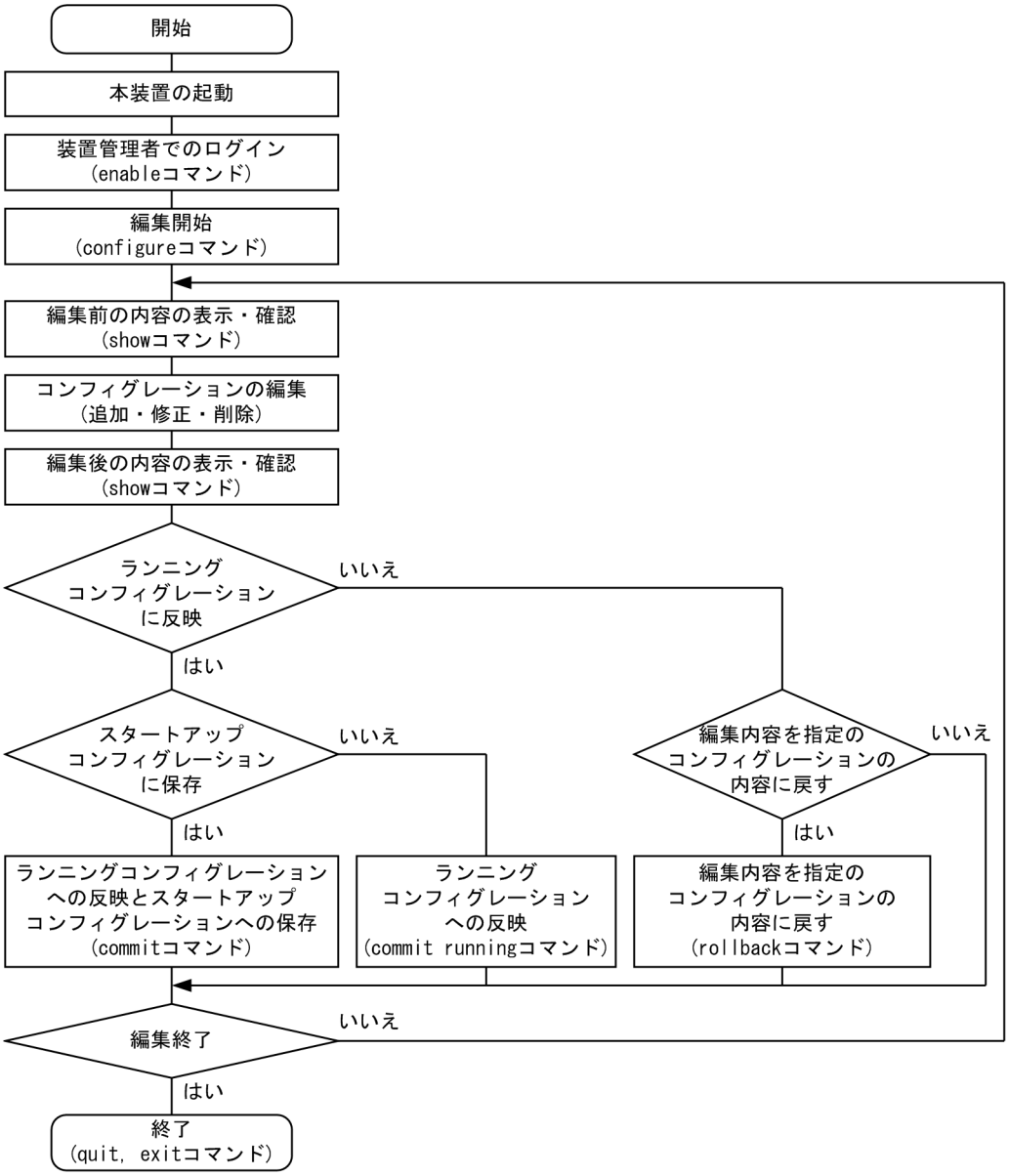
図 6-3　ランニングコンフィグレーションの編集の流れ（逐次コミットモード）



(2)　手動コミットモードでの流れ

手動コミットモードでの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。なお，configure コマンドでの編集開始後に，status コマンドでコミットモードが手動コミットモードであることを確認してください。

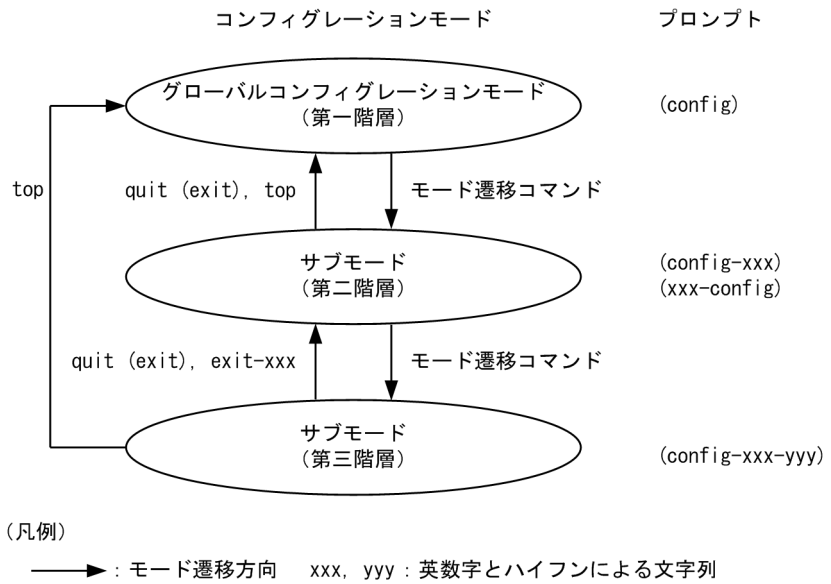
図 6-4　ランニングコンフィグレーションの編集の流れ（手動コミットモード）



6.1.4　コンフィグレーション入力時のモード遷移

コンフィグレーションは,実行できるコンフィグレーションモードで編集します。サブモード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サブ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入力時のモード遷移の概要を次の図に示します。

図 6-5　コンフィグレーション入力時のモード遷移の概要



6.1.5　初期導入時のコンフィグレーションについて

本装置は初期導入時に次のコンフィグレーションを自動生成します。

- 物理インタフェース

  装置に搭載されている NIF に合わせて，NIF の搭載位置，種別を基に各物理インタフェースのコンフィグレーションを生成します。物理インタフェースは，デフォルトでシャットダウン状態となります。
- デフォルトアカウント

  初期導入時に操作できるユーザとして，デフォルトアカウントのコンフィグレーションを生成します。
- ハードウェアプロファイル

  装置に搭載されている BCU または PRU に合わせて，ハードウェアプロファイルのコンフィグレーションを生成します。
- フィルタ・QoS のフロー検出モード

  装置に搭載されている BCU または PRU に合わせて，フィルタ・QoS のフロー検出モードのコンフィグレーションを生成します。
- テーブルエントリの配分パターン

  装置に搭載されている BCU または PRU に合わせて，経路系テーブルエントリとフロー系テーブルエントリの配分パターンのコンフィグレーションを生成します。

6.1.6　コンフィグレーション・運用コマンド一覧

コンフィグレーションの設定，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
apply-template	テンプレートに設定したコンフィグレーションコマンドを編集中のコンフィグレーションに反映します。

コマンド名	説明
commit	編集したコンフィグレーションの内容を，ランニングコンフィグレーションに反映して，スタートアップコンフィグレーションに保存します。
configuration commit-mode	コンフィグレーションのコミットモードを設定します。
delete	テンプレートに設定したコンフィグレーションコマンドを削除します。
end	コンフィグレーションモードを終了して装置管理者モードに戻ります。
end-template	template モードを終了してグローバルコンフィグレーションモードに戻ります。
insert	テンプレートの任意の位置にコンフィグレーションコマンドを挿入します。本コマンド実行後，insert モードに移行します。
load	指定したコンフィグレーションファイルを編集中のコンフィグレーションに反映します。指定したファイルの内容によって設定，変更，および削除ができます。
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モードを終了して装置管理者モードに戻ります。
replace	テンプレートに設定したコンフィグレーションコマンドを上書きします。本コマンド実行後，replace モードに移行します。
rollback	編集中のコンフィグレーションの内容を，指定のコンフィグレーションの内容に戻します。
save	編集したコンフィグレーションの内容を，をスタートアップコンフィグレーションファイルまたはバックアップコンフィグレーションファイルに保存します。
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。
template	コンフィグレーションコマンドのテンプレートを作成します。
top	サブモードからグローバルコンフィグレーションモードに戻ります。

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	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。
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。

コマンド名	説明
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。
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。

6.2　コンフィグレーションの編集方法

6.2.1　コンフィグレーションの編集開始

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，コンフィグレーションが編集できるようになります。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 6-6　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. コンフィグレーションの編集を開始します。

6.2.2　コンフィグレーションの表示・確認

(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 および show startup-config を使用すると，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 6-7　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 XXXXXX-XX
!
hostname "OFFICE01"
!
interface gigabitethernet 1/1
  shutdown
!
interface gigabitethernet 1/2
  shutdown
!
OFFICE01#
```

1. ランニングコンフィグレーションを表示します。

(2)　編集中の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と，編集中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の表示例を「図 6-8　編集中のコンフィグレーションの内容をすべて表示」～「図 6-11　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 6-8　編集中の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 XXXXXX-XX
!
hostname "OFFICE01"
!
interface gigabitethernet 1/1
  shutdown
!
interface gigabitethernet 1/2
  shutdown
```

```
!
OFFICE01(config)#
```

1.パラメータを指定しない場合は，編集中のコンフィグレーションの内容をすべて表示します。

図 6-9 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 1/1
  shutdown
!
interface gigabitethernet 1/2
  shutdown
!
OFFICE01(config)#
```

1.編集中の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 6-10 指定のインタフェース情報を表示

```
OFFICE01(config)# show interface gigabitethernet 1/1       <-1
interface gigabitethernet 1/1
  shutdown
!
OFFICE01(config)#
```

1.編集中のコンフィグレーションのうち，ギガビットイーサネットのインタフェース 1/1 を表示します。

図 6-11 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 1/1
OFFICE01(config-if)# show                               <-1
interface gigabitethernet 1/1
  shutdown
!
OFFICE01(config-if)#
```

1.編集中のコンフィグレーションのうち，ギガビットイーサネットのインタフェース 1/1 を表示します。

(3) 編集中の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との差分の確認

コミットモードが手動コミットモードの場合，コンフィグレーションを編集すると，ランニングコンフィグレーションとの間に差分が発生します。編集中の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との差分の確認例を次の図に示します。

図 6-12 編集中の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との差分の確認例

```
OFFICE01(config)# show > edit-config              <-1
OFFICE01(config)# quit
The changes to the configuration have not been saved.
Do you want to exit configure mode without saving the changes? (y/n): y
OFFICE01# show running-config > running-config    <-2
OFFICE01# diff running-config edit-config         <-3
1c1
< #Last modified by operator at Fri Nov 16 12:00:00 20XX UTC with version XX.XX
---
> #Last modified by operator at Fri Nov 16 12:00:01 20XX UTC with version XX.XX
8a9
>   speed 1000
```

1.編集中のコンフィグレーションの内容をすべてファイルに出力します。

2.ランニングコンフィグレーションの内容をすべてファイルに出力します。

3.編集中の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との差分を出力します。ランニングコンフィグレーションからの変更内容を確認できます。

6.2.3　コンフィグレーションのコミットモードの設定

(1)　コミットモードの確認

コンフィグレーションを編集する前に，コンフィグレーションのコミットモードを確認します。コミットモードの確認例を次の図に示します。

図 6-13　コミットモードの確認例

```
# configure
(config)# status                                    <-1
File name          : running-config
Commit mode        : Auto commit                    <-2
Last modified time : Thu Oct 11 12:00:00 20XX UTC by operator (not modified)
Buffer             : Total     XXXXXXXXXX Bytes
                     Available XXXXXXXXXX Bytes (XXXX%)
                     Fragments XX Bytes (XXXX%)
Login user         : USER  operator  LOGIN  Fri Oct 12 12:00:00 20XX UTC edit
(config)#
```

1. コンフィグレーションモードで status コマンドを実行します。
2. 編集中のコンフィグレーションの情報が表示されるので，「Commit mode」の内容を確認します。「Auto commit」と表示される場合，現在のコミットモードは逐次コミットモードです。「Manual commit」と表示される場合，現在のコミットモードは手動コミットモードです。

(2)　コミットモードの設定

コンフィグレーションのコミットモードを設定します。コミットモードを逐次コミットモードから手動コミットモードへ変更する場合の設定例を次の図に示します。

図 6-14　逐次コミットモードから手動コミットモードへの設定例

```
(config)# configuration commit-mode manual             <-1
!(config)#
```

1. 手動コミットモードを設定します。手動コミットモードの設定はすぐにランニングコンフィグレーションに反映されるため，設定した時点で，手動コミットモードに移行します。

コミットモードを手動コミットモードから逐次コミットモードへ変更する場合の設定例を次の図に示します。

図 6-15　手動コミットモードから逐次コミットモードへの設定例

```
(config)# no configuration commit-mode                 <-1
!(config)# commit                                      <-2
A commit of the configuration finished successfully.
(config)#
```

1. 手動コミットモードの設定を削除します。
2. 1.の内容を，commit コマンドでランニングコンフィグレーションに反映して，スタートアップコンフィグレーションに保存します。commit コマンドの実行が完了した時点で，逐次コミットモードに移行します。

6.2.4 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。コンフィグレーションの編集例を次の図に示します。

図 6-16 コンフィグレーションの編集例

```
(config)# interface gigabitethernet 1/1            <-1
(config-if)# description "PORT001"                 <-2
(config-if)# exit
(config)#
(config)# interface gigabitethernet 1/1            <-3
(config-if)# no description                        <-4
(config-if)# exit
(config)#
```

1. ギガビットイーサネットのインタフェース 1/1 にモードを移行します。
2. 補足説明を設定します。
3. ギガビットイーサネットのインタフェース 1/1 にモードを移行します。
4. 補足説明を削除します。

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」を指定して設定して，機能の抑止を解除する場合に「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。機能の抑止および解除の編集例を次の図に示します。

図 6-17 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 192.0.2.1                 <-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 192.0.2.1 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次の図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。なお，入力したコマンドが反映される契機はコンフィグレーションのコミットモードによって異なります。

図 6-18 正常入力時の出力

```
(config)# interface gigabitethernet 1/1
(config-if)# description "PORT001"
(config-if)#
```

エラーがある場合は次の図に示すように，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 6-19　異常入力時のエラーメッセージ出力

```
(config)# interface tengigabitethernet 1/1
(config-if)# description
description
            ^
% The command at the ^ maker is invalid.
(config-if)#
```

6.2.5　ランニングコンフィグレーションへの反映

(1)　逐次コミットモード

コンフィグレーションのコミットモードが逐次コミットモードの場合，コンフィグレーションの編集内容をすぐにランニングコンフィグレーションに反映します。逐次コミットモードでのランニングコンフィグレーションへの反映例を次の図に示します。

図 6-20　ランニングコンフィグレーションへの反映例（逐次コミットモード）

```
(config)# interface gigabitethernet 1/1
(config-if)# description "PORT001"                <-1
!(config-if)# exit
!(config)#
```

1. コンフィグレーションを編集します。コマンドの実行が完了した時点で，ランニングコンフィグレーションに反映します。

(2)　手動コミットモード

コンフィグレーションのコミットモードが手動コミットモードの場合，commit コマンドを実行することで，コンフィグレーションの編集内容を一括でランニングコンフィグレーションに反映して，スタートアップコンフィグレーションに保存します。手動コミットモードでのランニングコンフィグレーションへの反映例を次の図に示します。

図 6-21　ランニングコンフィグレーションへの反映例（手動コミットモード）

```
(config)# interface gigabitethernet 1/1
(config-if)# description "PORT001"                    <-1
!(config-if)# exit
!(config)# commit                                     <-2
A commit of the configuration finished successfully.
(config)#
```

1. コンフィグレーションを編集します。コマンドの実行が完了した時点では，ランニングコンフィグレーションに反映しません。
2. commit コマンドを実行します。編集内容を一括でランニングコンフィグレーションに反映して，スタートアップコンフィグレーションに保存します。

コンフィグレーションを編集したあと，編集内容を破棄して指定したコンフィグレーションの内容に戻す場合は，rollback コマンドを使用します。コンフィグレーションの編集内容を戻す例を次の図に示します。

図 6-22　コンフィグレーションの編集内容を戻す例

```
(config)# interface gigabitethernet 1/1
(config-if)# description "PORT001"                    <-1
!(config-if)# exit
!(config)# rollback running                           <-2
The configuration being edited will be discarded.
Do you want to roll back the configuration? (y/n): y
A rollback of the configuration finished successfully.
(config)#
```

1. コンフィグレーションを編集します。コマンドの実行が完了した時点では，ランニングコンフィグレーションに反映しません。
2. rollback コマンドを実行します。編集中のコンフィグレーションの内容が，指定したコンフィグレーション（この例ではランニングコンフィグレーション）の内容に戻ります。

6.2.6 コンフィグレーションのファイルへの保存

(1) スタートアップコンフィグレーションファイルへの保存

save コマンドまたは commit コマンドを使用すると，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ファイルに保存できます。

逐次コミットモードでのコンフィグレーションの保存例を次の図に示します。

図 6-23 コンフィグレーションの保存例（逐次コミットモード）

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

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編集します。
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。

手動コミットモードでのコンフィグレーションの保存例を次の図に示します。

図 6-24 コンフィグレーションの保存例（手動コミットモード）

```
# configure                  <-1
(config)#
        :
        :                    <-2
        :
!(config)# commit            <-3
A commit of the configuration finished successfully.
(config)#
```

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編集します。
3. commit コマンドを実行します。編集内容を一括でランニングコンフィグレーションに反映して，スタートアップコンフィグレーションに保存します。

(2) グローバルコンフィグレーションモードでのコンフィグレーションファイルへの部分保存

save コマンドで subset パラメータにコマンド名を指定すると，編集中のコンフィグレーションのうち，指定したコマンド名のコンフィグレーションをファイルに保存します。指定したコマンド名のコンフィグレーションをファイルに保存する例を次の図に示します。

図 6-25 指定したコマンド名のコンフィグレーションをファイルに保存する例

```
(config)# show                                                    <-1
    :
    :
    :
```

```
interface gigabitethernet 1/1
  description ”PORT001”
!
interface gigabitethernet 1/2
  description ” PORT002”
!
    :
    :
    :
(config)# save /usr/home/operator/tmp.cnf subset interface gigabitethernet
                                                                    <-2
Do you want to save the configuration in the file /usr/home/operator/tmp.cnf? (y/n): y
(config)# exit
#cat /usr/home/operator/tmp.cnf                                     <-3
interface gigabitethernet 1/1
  description ”PORT001”
!
interface gigabitethernet 1/2
  description ”PORT002”
!
    :
    :
    :
# configure
(config)# save /usr/home/operator/tmp2.cnf subset interface gigabitethernet 1/1
                                                                    <-4
Do you want to save the configuration in the file /usr/home/operator/tmp2.cnf? (y/n): y
(config)# exit
# cat /usr/home/operator/tmp2.cnf                                   <-5
interface gigabitethernet 1/1
  description ”PORT001”
!
#
```

1. 編集中のコンフィグレーションを確認します。
2. 編集中のコンフィグレーションのうち，設定済みのすべてのギガビットイーサネットのインタフェースのコンフィグレーションを/usr/home/operator/tmp.cnf に保存します。
3. 保存したファイルの内容を表示します。
4. 編集中のコンフィグレーションのうち，設定済みのギガビットイーサネットのインタフェース 1/1 のコンフィグレーションを/usr/home/operator/tmp2.cnf に保存します。
5. 保存したファイルの内容を表示します。

(3)　サブモードでのコンフィグレーションファイルへの部分保存

サブモードでファイル名と subset パラメータを指定して save コマンドを実行すると，編集中のコンフィグレーションのうち，該当するモード以下のコンフィグレーションをファイルに保存します。サブモードでの save コマンド実行例を次の図に示します。

図 6-26　サブモードでの save コマンド実行例

```
(config)# interface gigabitethernet 1/1
(config-if)# show                                   <-1
interface gigabitethernet 1/1
  description ”PORT001”
!
(config-if)# save /usr/home/operator/tmp.cnf subset      <-2
Do you want to save the configuration in the file /usr/home/operator/tmp.cnf? (y/n): y
(config)# exit
#cat /usr/home/operator/tmp.cnf                          <-3
interface gigabitethernet 1/1
  description ”PORT001”
!
#
```

1. ギガビットイーサネットのインタフェース 1/1 のコンフィグレーションを確認します。

2. ギガビットイーサネットのインタフェース 1/1 のコンフィグレーションを/usr/home/operator/tmp.cnf に保存します。
3. 保存したファイルの内容を表示します。

6.2.7 コンフィグレーションのファイルからの反映

load コマンドを使用すると，指定したコンフィグレーションファイルの内容を編集中のコンフィグレーションへ反映できます。指定したコンフィグレーションファイルを編集中のコンフィグレーションにマージする例を次に示します。

図 6-27 コンフィグレーションファイルをマージ（追加）する例

```
(config)# show                                    <-1
    :
    :
    :
interface gigabitethernet 1/1
!
    :
    :
    :
(config)# exit
# cat /usr/home/operator/tmp.cnf                  <-2
interface gigabitethernet 1/1
  shutdown
  description "PORT001"
  speed 1000
  no shutdown
!
# configure
(config)# load merge /usr/home/operator/tmp.cnf   <-3
Do you want to apply the specified configuration file to the configuration being edited? (y/n):
 y
!(config)# show                                   <-4
    :
    :
    :
interface gigabitethernet 1/1
  description "PORT001"
  speed 1000
!
!(config)#
```

1. 編集中のコンフィグレーションを確認します。
2. マージするコンフィグレーションファイル/usr/home/operator/tmp.cnf を確認します（コンフィグレーションを追加する指定をします）。
3. /usr/home/operator/tmp.cnf を編集中のコンフィグレーションにマージ（追加）します。
4. マージが完了した編集中のコンフィグレーションを確認します。

図 6-28 コンフィグレーションファイルをマージ（削除）する例

```
# show running-config                             <-1
    :
    :
    :
interface gigabitethernet 1/1
  description "PORT001"
  speed 1000
    :
    :
    :
# cat /usr/home/operator/tmp2.cnf                 <-2
interface gigabitethernet 1/1
  shutdown
  no description
```

```
  no speed
  no shutdown
!
# configure
(config)# load merge /usr/home/operator/tmp2.cnf  <-3
Do you want to apply the specified configuration file to the configuration being edited? (y/n):
 y
!(config)# show                                    <-4
    :
    :
    :
interface gigabitethernet 1/1
!
    :
    :
    :
!(config)#
```

1. 編集中のコンフィグレーションを確認します。
2. マージするコンフィグレーションファイル/usr/home/operator/tmp2.cnf を確認します（コンフィグレーションを削除する指定をします）。
3. /usr/home/operator/tmp2.cnf を編集中のコンフィグレーションにマージ（削除）します。
4. マージが完了した編集中のコンフィグレーションを確認します。

6.2.8　コンフィグレーションの編集終了

(1)　編集内容を保存して編集終了

save コマンドまたは commit コマンドで編集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たあと，グローバルコンフィグレーションモードで quit コマンドまたは exit コマンドを実行します。

逐次コミットモードでのコンフィグレーションの編集終了例を次の図に示します。

図 6-29　コンフィグレーションの編集終了例（逐次コミットモード）

```
!(config)# save
(config)# quit             <-1
```

1. 編集を終了します。

手動コミットモードでのコンフィグレーションの編集終了例を次の図に示します。

図 6-30　コンフィグレーションの編集終了例（手動コミットモード）

```
!(config)# commit
A commit of the configuration finished successfully.
(config)# quit             <-1
```

1. 編集を終了します。

(2)　編集内容を保存しないで編集終了

コンフィグレーションを編集したあと，save コマンドまたは commit コマンドを実行しないで，編集終了の quit コマンドまたは 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モードを終了できません。編集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を次の図に示します。

図 6-31　編集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)# quit
The changes to the configuration have not been saved.
Do you want to exit configure mode without saving the changes? (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編集します。
3. 確認メッセージが表示されます。

6.2.9 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，「The maximum number of entries are already configured. Configuration memory is insufficient. (entry = <エントリ名>)」または「The maximum number of entries are already configured. (failed entry = <エントリ名>)」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＆ペーストをしてください。

(3) 編集中のコンフィグレーションに関する注意事項

手動コミットモードの場合，編集中のコンフィグレーションは，保存しないで編集を終了してもすぐには破棄されないため，終了したときの状態から編集を再開できます。ただし，load merge コマンドでコンフィグレーションにエラーを検出した場合は，編集中のコンフィグレーションは破棄され，次回の編集時はランニングコンフィグレーションの状態から開始となります。

6.3　テンプレートの操作

テンプレートを使用したコンフィグレーションの編集方法について説明します。

6.3.1　テンプレートの概要

(1)　テンプレートの概要

テンプレート機能の特徴は次のとおりです。

- 繰り返し実行する一連のコンフィグレーションコマンドを登録して，テンプレートとして作成できます。作成後もコンフィグレーションコマンドを削除，挿入，および修正して，テンプレートを再編集できます。また，作成したテンプレートを繰り返し装置に反映できます。
- テンプレートに登録するコンフィグレーションコマンドの任意入力のパラメータを，置換できる文字列（以降，テンプレートパラメータと呼びます）として設定できます。テンプレートを装置に反映するときに，テンプレートパラメータを置換する文字列を指定できます。
- テンプレートに登録したコンフィグレーションコマンドは，入力した順で装置に設定できます。例えば，インタフェース情報を変更するときに，一時的にインタフェースを停止して設定を変更したあとインタフェースを再開する，という一連の手順をテンプレート内で再現できます。

テンプレート機能では，まず，コンフィグレーションコマンドを登録したテンプレートを作成します。次に，テンプレートに登録した内容を編集中のコンフィグレーションに反映します。これらの処理は，スクリプトを作成して，それを実行することに似ています。

テンプレートの作成例を次の図に示します。

図 6-32　テンプレートの作成例

```
(config)# template EtherDEF $PORT
(config-TPL)# interface gigabitethernet $PORT
(config-if-TPL)# shutdown
(config-if-TPL)# speed 1000
(config-if-TPL)# no shutdown
(config-if-TPL)# exit
(config-TPL)# show
template EtherDEF $PORT
  interface gigabitethernet $PORT
    shutdown
    speed 1000
    no shutdown
  end-template
!
(config-TPL)# end-template
(config)#
```

ここではテンプレート名を「EtherDEF」としています。template モードで入力したコンフィグレーションコマンドが，テンプレート「EtherDEF」に登録されます。なお，テンプレートを作成した時点では，登録したコンフィグレーションコマンドは編集中のコンフィグレーションに反映されません。テンプレートの内容を編集中のコンフィグレーションに反映するには，apply-template コマンドを使用します。テンプレートの反映例を次の図に示します。

図 6-33　テンプレートの反映例

```
(config)# show interface gigabitethernet 1/1          <-1
interface gigabitethernet 1/1
!
(config)# apply-template EtherDEF 1/1                 <-2
(config)# show interface gigabitethernet 1/1          <-3
interface gigabitethernet 1/1
```

```
  speed 1000
!
(config)#
```

1. ギガビットイーサネットのインタフェース 1/1 のコンフィグレーションを確認します。
2. テンプレート「EtherDEF」をギガビットイーサネットのインタフェース 1/1 に反映します。
3. ギガビットイーサネットのインタフェース 1/1 のコンフィグレーションを確認すると，テンプレート「EtherDEF」の内容が反映されています。

(2)　テンプレートの位置づけ

テンプレートは，コンフィグレーションの一部として位置づけられ，コンフィグレーションの中に設定されます。コンフィグレーションの構造を次の図に示します。

図 6-34　コンフィグレーションの構造

```
(config)# show
    :
    :
    :
template EtherDEF $PORT                    ┐
  interface gigabitethernet $PORT          │
    shutdown                               │
    speed 1000                             │ <-1
    no shutdown                            │
  end-template                             ┘
!
(config)#
```

1. この部分がテンプレートです。

6.3.2　テンプレートの作成

(1)　テンプレートの作成および終了

テンプレートを作成する場合は，グローバルコンフィグレーションモードで template コマンドを使用します。template コマンドを実行するとテンプレートを編集するモード（template モードと呼びます）に移行して，テンプレートにコンフィグレーションコマンドを登録できるようになります。このとき，プロンプトには template モードを示す「-TPL」が付きます。テンプレートの作成例を次の図に示します。

図 6-35　テンプレートの作成例

```
(config)# template EtherDEF $PORT
(config-TPL)# show
template EtherDEF $PORT
  end-template
!
(config-TPL)#
```

テンプレートの編集を終了する場合は，次の表に示すコマンドのどれかを使用します。

表 6-3　テンプレートの編集終了コマンド

コマンド名	説明
end	template モードを終了して，装置管理者モードに移行します。
end-template	template モードを終了して，グローバルコンフィグレーションモードに移行します。
quit (exit)	config-TPL モードの場合，template モードを終了してグローバルコンフィグレーションモードに移行します。config-TPL モード以外の場合，一つ上の階層に移行します。

コマンド名	説明
top	template モードを終了して，グローバルコンフィグレーションモードに移行します。

テンプレートには end-template コマンドが自動で登録されるため，end-template コマンド以外のコマンドで template モードを終了した場合でも，テンプレートには end-template コマンドが登録されます。テンプレートの編集終了例を次の図に示します。

図 6-36　テンプレートの編集終了例

```
(config-TPL)# end-template
(config)#
```

(2)　テンプレートへの登録方法

テンプレートには，コンフィグレーションを設定するコンフィグレーションコマンドとコンフィグレーションを削除するコンフィグレーションコマンドを登録できます。テンプレートへの登録例を次の図に示します。

図 6-37　テンプレートへの登録例

```
(config)# template EtherDEF $PORT
(config-TPL)# interface gigabitethernet $PORT          <-1
(config-if-TPL)# shutdown                              <-1
(config-if-TPL)# speed 1000                            <-1
(config-if-TPL)# no shutdown                           <-2
(config-if-TPL)# exit
(config-TPL)# show
template EtherDEF $PORT
  interface gigabitethernet $PORT
    shutdown
    speed 1000
    no shutdown
  end-template
!
(config-TPL)#
```

1. コンフィグレーションを設定するコンフィグレーションコマンドをテンプレートに登録します。
2. コンフィグレーションを削除するコンフィグレーションコマンドをテンプレートに登録します。

テンプレートには通常のコンフィグレーション編集時と同様のモードがあり，同様にモード遷移します。このとき，すべてのモードでプロンプトに template モードを示す「-TPL」が付きます。テンプレートのモード遷移例を次の図に示します。

図 6-38　テンプレートのモード遷移例

```
(config)# interface gigabitethernet 1/1                <-1
(config-if)#                                           <-1
(config-if)# exit
(config)# template EtherDEF $PORT
(config-TPL)# interface gigabitethernet $PORT          <-2
(config-if-TPL)#                                       <-2
```

1. 通常のコンフィグレーション編集時のモード遷移です。
2. テンプレート編集時のモード遷移です。通常のコンフィグレーション編集時と同様にモード遷移します。プロンプトには template モードを示す「-TPL」が付きます。

template モードでは，コンフィグレーションコマンドは入力した順にテンプレートに登録されます。コマンドの入力順がテンプレートの登録順となる例を次の図に示します。

図 6-39 コマンドの入力順がテンプレートの登録順となる例

```
(config)# template EtherDEF $PORT
(config-TPL)# interface gigabitethernet $PORT          <-1
(config-if-TPL)# shutdown                              <-1
(config-if-TPL)# speed 1000                            <-1
(config-if-TPL)# no shutdown                           <-1
(config-if-TPL)# exit
(config-TPL)# show                                     <-2
template EtherDEF $PORT
  interface gigabitethernet $PORT                      <-3
    shutdown                                           <-3
    speed 1000                                         <-3
    no shutdown                                        <-3
  end-template
!
(config-TPL)#
```

1.テンプレートにコンフィグレーションコマンドを登録します。

2.show コマンドでテンプレートの登録内容を確認します。

3.入力した順にコンフィグレーションコマンドが登録されています。

6.3.3 テンプレートの編集

(1) テンプレートのコマンド再登録（上書き）

テンプレートに登録済みのコマンドとパラメータまで同じコンフィグレーションコマンドを入力した場合，登録済みのコマンドを上書きします。該当するコマンドの既存の登録順が変更になることもありません。

登録済みのコマンドとパラメータの一部が異なるコンフィグレーションコマンドを入力した場合は，別のコマンドとして登録されます。

入力したコマンドがモード遷移するコマンドの場合は，該当するモードに遷移します。また，モード遷移後に入力したコマンドは，そのモード内の最後に新規コマンドとして登録されます。

モードの遷移を伴うコマンドの再登録例を次の図に示します。

図 6-40 コマンドの再登録例

```
(config-TPL)# show
template EtherDEF $PORT
  interface gigabitethernet $PORT
    shutdown
    speed 1000
    no shutdown
  end-template
!
(config-TPL)#
(config-TPL)# interface gigabitethernet $PORT          <-1
(config-if-TPL)# speed auto                            <-2
(config-if-TPL)# exit
(config-TPL)# show
template EtherDEF $PORT
  interface gigabitethernet $PORT
    shutdown
    speed 1000
    no shutdown
    speed auto                                         <-3
  end-template
!
(config-TPL)#
```

1.テンプレートに登録済みのギガビットイーサネットのインタフェース$PORT にモードを遷移します。

2. テンプレートに登録済みのコマンド（speed コマンド）とパラメータが異なるコンフィグレーションコマンドを入力します。
3. ギガビットイーサネットのインタフェース$PORT の最後に，新規コマンドとして登録されます（登録済みの「speed 1000」に上書きされません）。

(2)　テンプレートのコマンド削除

テンプレートに登録済みのコンフィグレーションコマンドを削除する場合は delete コマンドを使用します。delete コマンドの使用例を次の図に示します。

図 6-41　delete コマンドの使用例

```
(config-TPL)# show
template EtherDEF $PORT
  interface gigabitethernet $PORT
    shutdown
    speed 1000
    no shutdown
  end-template
!
(config-TPL)#
(config-TPL)# interface gigabitethernet $PORT          <-1
(config-if-TPL)# delete speed 1000                     <-2
(config-if-TPL)# show
template EtherDEF $PORT
  interface gigabitethernet $PORT                      <-3
    shutdown
    no shutdown
  end-template
!
(config-if-TPL)#
```

1. 削除するコマンドのモードに移行します。
2. delete コマンドを使用して，削除するコマンドを入力します。
3.「speed 1000」が削除されました。

(3)　テンプレートのコマンド挿入

テンプレートの任意の位置にコンフィグレーションコマンドを挿入する場合は insert コマンドを使用します。insert コマンドの使用例を次の図に示します。

図 6-42　insert コマンドの使用例

```
(config-TPL)# show
template EtherDEF $PORT
  interface gigabitethernet $PORT
    shutdown
    no shutdown                                        <-1
  end-template
!
(config-TPL)#
(config-TPL)# interface gigabitethernet $PORT          <-2
(config-if-TPL)# insert speed 1000                     <-3
(config-if-TPL-INS)# no shutdown                       <-4
(config-if-TPL)# show
template EtherDEF $PORT
  interface gigabitethernet $PORT
    shutdown
    speed 1000                                         <-5
    no shutdown
  end-template
!
(config-if-TPL)#
```

1. この位置にコマンドを挿入します。

2. コマンドを挿入するモードに移行します。
3. insert コマンドを使用して，挿入するコマンドを入力します。
4. プロンプトの後ろに「-INS」が付きます。ここで，挿入する位置にある「no shutdown」を入力します。
5. 「no shutdown」の前に「speed 1000」が挿入されました。

(4) テンプレートのコマンド修正

テンプレートに登録済みのコンフィグレーションコマンドやパラメータを修正する場合は replace コマンドを使用します。replace コマンドの使用例を次の図に示します。

図 6-43 replace コマンドの使用例

```
(config-TPL)# show
template EtherDEF $PORT
  interface gigabitethernet $PORT
    shutdown
    speed 1000                                          <-1
    no shutdown
  end-template
!
(config-TPL)#
(config-TPL)# interface gigabitethernet $PORT         <-2
(config-if-TPL)# replace speed auto                   <-3
(config-if-TPL-REP)# speed 1000                       <-4
(config-if-TPL)# show
template EtherDEF $PORT
  interface gigabitethernet $PORT
    shutdown
    speed auto                                          <-5
    no shutdown
  end-template
!
(config-if-TPL)#
```

1. speed コマンドのパラメータを 1000 から auto に変更します。
2. 変更するコマンドのモードに移行します。
3. replace コマンドを使用して，変更後のコマンドを入力します。
4. プロンプトの後ろに「-REP」が付きます。ここで，変更前のコマンドを入力します。
5. パラメータが変更されました。

6.3.4 テンプレートの反映

テンプレートに登録されたコンフィグレーションコマンドを編集中のコンフィグレーションに反映する場合は，グローバルコンフィグレーションモードから apply-template コマンドを実行します。

apply-template コマンドを実行すると，テンプレートに登録されているコンフィグレーションコマンドを最初の行から 1 行ずつ設定したことになります。そのため，設定する順序が決まっているコンフィグレーションは，正しい順序でテンプレートに登録してください。テンプレートから編集中のコンフィグレーションへの反映例を次の図に示します。

図 6-44　テンプレートから編集中のコンフィグレーションへの反映例

```
(config)# show template
template EtherDEF $PORT
  interface gigabitethernet $PORT
    shutdown
    speed 1000
    no shutdown
  end-template
!
(config)# apply-template EtherDEF 1/1
(config)#
```



```
コマンドの実行イメージ
(config)# interface gigabitethernet 1/1
(config-if)# shutdown
(config-if)# speed 1000
(config-if)# no shutdown
(config-if)# exit
(config)#
```

テンプレートの先頭から順に編集中のコンフィグレーションへ反映されるため，この図の「コマンドの実行イメージ」に示す順でコンフィグレーションコマンドを設定したことになります。

6.3.5　テンプレートパラメータの使用方法

(1)　テンプレートパラメータの概要

テンプレートに登録するコンフィグレーションコマンドの任意入力のパラメータを，テンプレートパラメータとしてテンプレートに設定できます。テンプレートパラメータは置換できる文字列です。テンプレートにコンフィグレーションコマンドを登録するときにパラメータの一部をテンプレートパラメータとして設定しておくと，apply-template コマンドでテンプレートを編集中のコンフィグレーションに反映するときに，テンプレートパラメータへ数値や文字列を指定できます。

テンプレートパラメータの書式は，ドル（$）と 31 文字以内の文字列です。例えば，「$PORT」と設定します。

テンプレートパラメータは，コンフィグレーションコマンドの任意入力のパラメータ（<>で囲まれたパラメータ）に対して使用できます。テンプレートで使用するすべてのテンプレートパラメータは，テンプレートの新規作成時に設定してください。また，使用するテンプレートパラメータを変更する場合は，template コマンドの change-parameter パラメータを使用してください。

テンプレートに登録するコンフィグレーションコマンドに使用できるのは，template コマンドで設定したテンプレートパラメータだけです。テンプレート作成時のテンプレートパラメータの使用例を次の図に示します。

図 6-45　テンプレート作成時のテンプレートパラメータの使用例

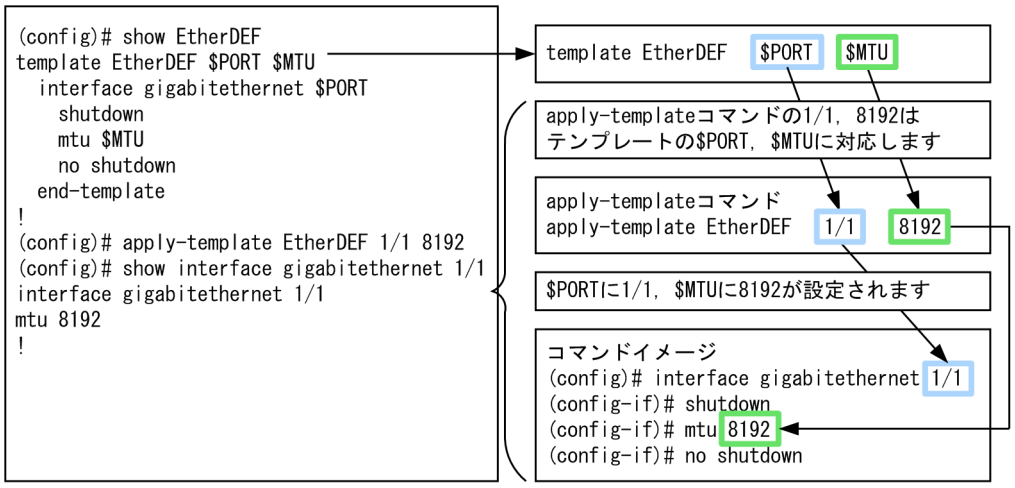
```
(config)# template EtherDEF $PORT $MTU                <-1
(config-TPL)# interface gigabitethernet $PORT         <-2
(config-if-TPL)# shutdown
(config-if-TPL)# mtu $MTU                             <-2
(config-if-TPL)# no shutdown
(config-if-TPL)# exit
(config-TPL)# show
template EtherDEF $PORT $MTU
```

```
  interface gigabitethernet $PORT
    shutdown
    mtu $MTU
    no shutdown
  end-template
!
(config-TPL)#
```

1. テンプレートの新規作成時にテンプレートパラメータを設定します。
2. 1 で設定したテンプレートパラメータを，コマンドのパラメータとして使用できます（1 で設定していないテンプレートパラメータは使用できません）。

テンプレートに設定したテンプレートパラメータには，apply-template コマンド実行時に入力した値が指定されます。テンプレートパラメータの指定例を次の図に示します。

図 6-46　テンプレートパラメータの指定例



この図では，テンプレートで「$PORT」と「$MTU」の順に二つのテンプレートパラメータを使用しています。apply-template コマンド実行時に 1/1，8192 の順で入力すると，「$PORT」に 1/1，「$MTU」に 8192 が指定された状態で編集中のコンフィグレーションへ反映されます。

任意入力のパラメータをテンプレートパラメータとして扱うと，次のことができるようになります。

- 一つのテンプレートを繰り返し使用できます。例えば，インタフェースに設定するテンプレートを作成する場合，「<nif no.>/<port no.>」をテンプレートパラメータとして設定すると，任意のイーサネットインタフェースに適用できるテンプレートになります。
- 設定するテンプレートパラメータの形式を「$<parameter>#<index>」にすると，同じコンフィグレーションコマンドを複数の個所に登録できます。
- 複数指定を設定できないパラメータをテンプレートパラメータにすると，外部のスクリプト機能などを使用してテンプレートパラメータに連続した値（例えば，192.0.2.1，192.0.2.2，…）を指定できるようになります。

(2)　同一コンフィグレーションコマンドの登録

テンプレートに同じコンフィグレーションコマンドを登録する場合は，テンプレートパラメータを「$<parameter>#<index>」の形式で指定します。こうすると同じコマンドでも<index>が異なるため，別のコマンドとして登録できます。なお，apply-template コマンド実行時には「$<parameter>#<index>」の「$<parameter>」部分だけが編集中のコンフィグレーションに反映されます。「$<parameter>#<index>」を使用したテンプレート例を次の図に示します。

図 6-47 「$<parameter>#<index>」を使用したテンプレート例

```
(config)# show template
template LacpSet $PORT $LA_ID
  interface range gigabitethernet $PORT#1              <-1
    shutdown
    channel-group $LA_ID mode active
  lacp system-priority 100
  interface port-channel $LA_ID
    channel-group lacp system-priority 50
  interface range gigabitethernet $PORT#2              <-1
    no shutdown
  end-template
!
(config)#
```

1.「$PORT#1」「$PORT#2」は，apply-template コマンドでコンフィグレーションに反映するときは入力した値が「$PORT」に指定されるため，同じコマンドです。しかし，テンプレート上は表記が異なるため，複数の個所に登録できます。

このテンプレートを使用した編集中のコンフィグレーションへの反映例を次の図に示します。

図 6-48 「$<parameter>#<index>」を使用したテンプレートの反映例

```
(config)# apply-template LacpSet 1/1 10
(config)# show
    :
    :
    :
lacp system-priority 100
!
interface port-channel 10
  channel-group lacp system-priority 50
!
interface gigabitethernet 1/1
  channel-group 10 mode active
!
(config)#
```

この図では，次の順番でコンフィグレーションに反映されます。

1. interface gigabitethernet 1/1
2. shutdown
3. channel-group 10 mode active
4. exit
5. lacp system-priority 100
6. interface port-channel 10
7. channel-group lacp system-priority 50
8. interface gigabitethernet 1/1
9. no shutdown
10. !

(3) テンプレートパラメータの変更

テンプレートで使用できるテンプレートパラメータを追加，変更，および削除する場合，template コマンドの change-parameter パラメータを使用します。change-parameter パラメータを使用すると，template コマンドで設定されたテンプレートパラメータが上書きされます。テンプレートパラメータの変更例を次の図に示します。

図 6-49 テンプレートパラメータの変更例

```
(config)# show EtherDEF
template EtherDEF $PORT
    :
    :
    :
(config)# template EtherDEF change-parameter $PORT $MTU     <-1
(config-TPL)# show
template EtherDEF $PORT $MTU                                <-2
    :
    :
    :
(config-TPL)#
```

1. template コマンドの change-parameter パラメータを使用して，「$PORT $MTU」と変更します。
2. 使用できるテンプレートパラメータに「$MTU」が追加されました。

6.3.6 特記事項

(1) パラメータに複数指定を設定できるコマンド

パラメータに複数指定を設定できるコンフィグレーションコマンドをテンプレートに登録する場合，ユーザが入力したパラメータの内容をそのままテンプレートに登録します。例えば，インタフェースを複数指定してコマンドを入力すると，テンプレートには入力した内容がそのまま登録されます。なお，テンプレートを apply-template コマンドで反映したときに，インタフェースごとに分割されます。インタフェースの複数指定を使用したテンプレート例を次の図に示します。

図 6-50 インタフェースの複数指定を使用したテンプレート例

```
(config)# show template
template EtherDEF
  interface range gigabitethernet 1/1-2                <-1
    shutdown
    speed 1000
    no shutdown
  end-template
!
(config)#
```

1. テンプレートには入力されたコマンドやパラメータがそのまま登録されます。

このテンプレートを使用した編集中のコンフィグレーションへの反映例を次の図に示します。

図 6-51 インタフェースの複数指定を使用したテンプレートの反映例

```
(config)# apply-template EtherDEF                       <-1
(config)# show interface range gigabitethernet 1/1-2
interface gigabitethernet 1/1                           <-2
  speed 1000
!
interface gigabitethernet 1/2                           <-2
  speed 1000
!
```

1. テンプレートを反映します。
2. コンフィグレーションにはインタフェースごとに分割して反映されています。

(2) 特殊なパラメータのテンプレートパラメータ使用方法

特殊なパラメータに対する，template モードでのテンプレートパラメータの設定例および apply-template コマンド実行時のテンプレートパラメータの指定例を次の表に示します。

表 6-4　特殊なパラメータに対するテンプレートパラメータの設定例と指定例

パラメータ	テンプレートパラメータ	
	設定例	指定例
<nif no.>/<port no.>	interface gigabitethernet $PORT	$PORT：1/1
<interface id list>	monitor session 1 source interface add gigabitethernet $PORTS	$PORTS：1/1-2
	monitor session 1 source interface add gigabitethernet $PORTS1, gigabitethernet $PORTS2	$PORTS1：1/1-2 $PORTS2：2/5
インタフェース複数指定	interface range gigabitethernet $PORTS	$PORTS：1/1-2
	interface range gigabitethernet $PORTS1,gigabitethernet $PORTS2	$PORTS1：1/1-2 $PORTS2：2/5
サブインタフェース指定	interface gigabitethernet $PORT.$SUB_INDEX	$PORT：1/1 $SUB_INDEX：1
	interface port-channel $LA_ID.$SUB_INDEX	$LA_ID：1 $SUB_INDEX：1

(3)　特殊なコマンド

設定した内容がエンコードされるコンフィグレーションコマンドをテンプレートに登録した場合, 通常のコンフィグレーションの設定と同様にエンコードした内容がテンプレートに登録されます。banner コマンドのテンプレート登録例を次の図に示します。

図 6-52　banner コマンドのテンプレート登録例

```
(config)# template set_banner
(config-TPL)# banner login plain-text                    <-1
--- Press CTRL+D or only '.' line to end ---
Warning!!! Warning!!! Warning!!!
This is our system. You should not login.
Please close connection.                                 <-2
.
(config-TPL)# show
template set_banner
  banner login encode "V2FybmluZyEhISBXYXJuaW5nISEhIFdhcm5pbmchISEKVGhpcyBpcyBvdXIgc3lzdGVtLiBZ
b3Ugc2hvdWxkIG5vdCBsb2dpbi4KUGxlYXNlIGNsb3NlIGNvbm5lY3Rpb24uCg=="
                                                         <-3
!
(config-TPL)#
```

1. banner コマンドをテンプレートに登録します。
2. ログインメッセージを入力します。
3. テンプレートにはエンコードされた内容が登録されます。

6.4　コンフィグレーションの操作

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。

6.4.1　コンフィグレーションのバックアップ

運用コマンド copy を使用すると，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編集して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ランニングコンフィグレーションおよび編集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に示します。

図 6-53　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@[2001:db8::1]/backup.cnf
Are you sure you want to copy the configuration file to ftp://staff@[2001:db8::1]/backup.cnf? (
y/n): y

Authentication for 2001:db8::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 6-54　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@[2001:db8::1]/backup.cnf
Are you sure you want to copy the configuration file to ftp://staff@[2001:db8::1]/backup.cnf? (
y/n): y

Authentication for 2001:db8::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。

6.4.2　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に反映する場合は，運用コマンド copy を使用します。反映例を次に示します。

図 6-55　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@[2001:db8::1]/backup.cnf startup-config
User account information is set in the configuration file.
The home directory of any deleted users will be deleted.
Are you sure you want to copy the configuration file to startup-config? (y/n): y
```

```
Authentication for 2001:db8::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。

6.4.3　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 6-56　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 192.0.2.1
Connect to 192.0.2.1.
220  FTP server (Version wn-2.4(4) Wed Jan 1 12:00:00 JST 20XX) ready.
Name (192.0.2.1: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
User account information is set in the configuration file.
The home directory of any deleted users will be deleted.
Are you sure you want to copy the configuration file 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コピーします。
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 6-57　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
```

```
Are you sure you want to copy the configuration file to /usr/home/operator/backup.cnf? (y/n): y
# exit
> ftp 192.0.2.1
Connect to 192.0.2.1.
220  FTP server (Version wn-2.4(4) Fri Jan 1 12:00:00 JST 20XX) ready.
Name (192.0.2.1: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. ランニングコンフィグレーションをバックアップコンフィグレーションファイルにコピーします。
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。

6.4.4 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 6-58 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
User account information is set in the configuration file.
The home directory of any deleted users will be deleted.
Are you sure you want to copy the configuration file 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スタートアップコンフィグレーションにコピーします。
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 6-59 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
Are you sure you want to copy the configuration file to /usr/home/operator/backup.cnf? (y/n): y
# exit
```

```
> cp backup.cnf mc-file backup.cnf                    <-2
>
```

1.ランニングコンフィグレーションをバックアップコンフィグレーションファイルにコピーします。

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。

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　マネージメントポート接続

マネージメントポートについて説明します。

(1)　マネージメントポート機能仕様

マネージメントポートはリモート運用端末を接続するためのインタフェースを提供します。マネージメントポートの機能仕様を次の表に示します。

表 7-1　マネージメントポートの機能仕様

機能概要	仕様
インタフェース種別	10BASE-T，100BASE-TX および 1000BASE-T
オートネゴシエーション	サポート
自動 MDI/MDIX 機能	サポート
MAC および LLC 副層制御フレーム	Ethernet V2 形式
対象プロトコル	IPv4/IPv6

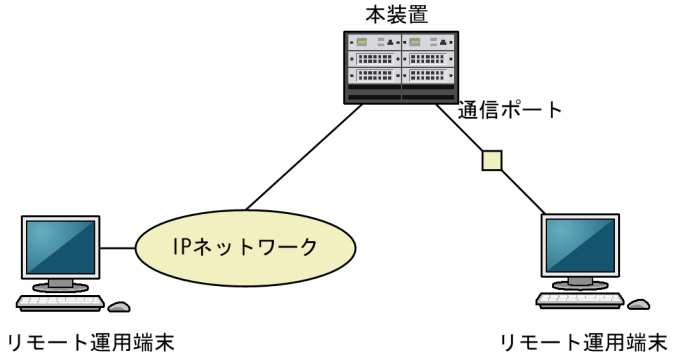
(2)　マネージメントポート使用時の注意事項

マネージメントポートは，リモート運用を主目的としたインタフェースです。マネージメントポートから NIF を経由して通信できますが，お勧めしません。

7.1.2　通信用ポート接続

通信用ポートを経由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 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，IP アドレスなどが設定されていません。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



7.1.3　ダイアルアップ IP 接続

本装置のシリアル接続ポート（AUX）にダイアルアップ IP 接続でリモート運用端末を接続する手順を次に示します。

(1)　本装置の設定

(a)　モデムの準備

あらかじめモデムが自動着信するように設定します。モデムやモデムと AT 互換機を接続するためのストレートケーブルを用意してください。また，本装置ではモデムを設定できないので，PC などに接続して設定してください。

モデムに付属の説明書を参照して，AT コマンドを使用して次の表に示す設定をしてください。拡張 AT コマンドを持つモデムでは，例で示したコマンドと異なるコマンドを使用する場合があります。

表 7-2　モデムの設定

設定項目	設定内容	指定例 (Hayes 互換 AT コマンドの場合)
CD 信号状態	CD 信号は通常オフで，相手モデムのキャリアを受信するとオンにします。	AT&C1
DTR 信号状態	DTR 信号がオンからオフに変わるとモデムを初期化します。	AT&D3
コマンドエコー	入力したコマンドを DTE に出力しません。	ATE0
フロー制御	DTE と DCE 間のフロー制御を設定します。 • RTS/CTS フロー制御有効 • XON/XOFF フロー制御無効	AT&K3
リザルトコード	リザルトコードを DTE に出力しません。	ATQ1
自動着信	自動着信するまでの呼び出し回数を設定します。	ATS0=2
リセット時の設定	モデム内の不揮発性メモリから設定を読み出します。	AT&Y0
設定の保存	設定をモデム内の不揮発性メモリに保存します。	AT&W0

コマンドを DTE に出力しないようにコマンドエコーを設定すると，コマンドを入力しても文字は表示されません。設定が完了したらモデムに設定内容を保存します。設定保存後に設定内容を表示して確認します。

（例）Hayes 互換 AT コマンドでモデムを自動着信に設定する場合

AT&F&C1&D3E0&K3Q1S0=2&W0&Y0&V

シリアル接続（モデム）の場合は，通信ソフトウェアのダイアル機能を使用してダイアルします。ダイアル機能については通信ソフトウェアの説明を参照してください。端末から AT コマンドを使用してダイアル接続できます。ダイアル機能を持たない通信ソフトウェアを使用する場合などは AT コマンドでダイアルしてください。AT コマンドのダイアル方法についてはモデムのマニュアルを参照してください。

（例）Hayes 互換 AT コマンドでダイアルする場合

- 公衆回線を使用してトーンで 123-4567 へダイアルする。
  AT&FE0&S1S0=0S2=255TD123-4567
- 構内交換機を使用してトーンで 123-4567 へダイアルする。
  AT&FX3E0&S1S0=0S2=255TD123-4567
- 構内交換機を使用してトーンで 0 をダイアルして，数秒待ってから 123-4567 へダイアルする。
  AT&FX3E0&S1S0=0S2=255TD0,123-4567

設定したモデムを本装置の AUX ポートに接続します。

(b)　コンフィグレーション設定

本装置で使用する IP アドレスと，リモート運用端末で使用する IP アドレスを設定します。設定するインタフェースは async です。

本装置で使用する IP アドレスが 10.0.0.1，リモート運用端末で使用する IP アドレスが 10.0.0.2 の場合，次の図のようにコマンドを実行します。

図 7-2　async に関するコンフィグレーション設定例

```
(config)# interface async 1
(config-if)# ip address 10.0.0.1 255.255.255.0
(config-if)# peer default ip address 10.0.0.2
```

(2)　リモート運用端末の設定

(a)　モデムの準備

本装置にダイアルアップ IP 接続する運用端末でモデムを使用するための設定方法は，モデムのマニュアルを参照してください。

(b)　接続ソフトの設定

本装置にダイアルアップ IP 接続する運用端末にダイアルアップ IP 接続用のソフトをインストールして，次の表のように設定します。

表 7-3　ダイアルアップ IP 接続設定内容

設定項目	設定内容
サーバの種類	PPP
インターネットプロトコル（TCP/IP）	TCP/IP
IP アドレス	IP アドレスを自動的に取得する
DNS サーバのアドレス	DNS サーバのアドレスを自動的に取得する
認証方式	PAP/パスワードを暗号化しない
電話番号	本装置に接続するモデムで使用する電話番号

(c)　認証に使用するユーザ名とパスワード

ダイアルアップ IP 接続の認証に使用するユーザ名とパスワードは，本装置のログインに使用するユーザ名とパスワードを使用します。なお，パスワードなしのユーザ名で認証を行うと，入力したパスワードは無視されます。

(3)　回線接続とログイン

(a)　回線接続

接続ソフトからダイアルします。

(b)　接続確認

ダイアルアップ IP 接続を行うと IP アドレスが割り当てられます。ping コマンドなどで宛先アドレスへの通信可否を確認できます。

ダイアルアップ IP 接続が正しく行われている場合に本装置上で show sessions コマンドを使用すると，ユーザが aux ポートからログインしているように表示され，運用端末で使用している IP アドレスも表示されます。

図 7-3　show sessions コマンド実行例

```
> show sessions
Date 20XX/01/07 12:00:00 UTC
gilbert console  -----  0   Jan  6 14:16
john    aux      -----  1   Jan  6 14:16 (ppp0:10.0.0.1)     <-1
```

1.「aux」であることを確認します。また，運用端末に割り当てられた IP アドレス（10.0.0.1）が表示されます。

(c)　ログイン

リモート運用端末（リモートログイン）が使用できます。

(4)　回線切断

ダイアルアップ IP 接続は次の要因で切断されます。

- 運用端末からの切断要求
- 他ログインユーザからの killuser コマンドによるユーザ※の強制ログアウト
- 回線障害
- コンフィグレーションコマンド interface async の関連コマンドの変更および削除

注※

ここでは AUX ポートからログインしているユーザを指します。

[注意事項]

ダイアルアップ IP 接続が切断された場合，すぐには再接続できないことがあります。その場合，300 秒程度の間隔を空けてから再接続してください。

7.2　コンフィグレーション

7.2.1　コンフィグレーションコマンド一覧

マネージメントポー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 7-4　コンフィグレーションコマンド一覧

コマンド名	説明
description	補足説明を設定します。
duplex	マネージメントポートの duplex を設定します。
interface mgmt	マネージメントポートのコンフィグレーションを指定します。
shutdown	マネージメントポートをシャットダウン状態にします。
speed	マネージメントポートの回線速度を設定します。
ip address※1	マネージメントポートの IPv4 アドレスを指定します。
ipv6 address※2	マネージメントポートの IPv6 アドレスを指定します。
ipv6 enable※2	マネージメントポートの 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。

注※1

「コンフィグレーションコマンドレファレンス Vol.3　2. IPv4・ARP・ICMP」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 Vol.3　3. IPv6・NDP・ICMPv6」を参照してください。

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 7-5　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。

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

IPv4/IPv6 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，「コンフィグレーションガイド Vol.3　2. IP・ARP・ICMP の設定と運用」または「コンフィグレーションガイド Vol.3　4. IPv6・NDP・ICMPv6 の設定と運用」を参照してください。

7.2.2　マネージメントポートの設定

(1)　マネージメントポートのシャットダウン

[設定のポイント]

マネージメントポー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マネージメントポー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，最初にマネージメントポー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マネージメントポー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 mgmt 0**
   マネージメントポートの設定を指定します。
2. **(config-if)# shutdown**
   マネージメントポートをシャットダウンします。
3. **(config-if)# ＊＊＊＊＊**
   マネージメントポート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**
   マネージメントポートのシャットダウンを解除します。

[関連事項]

運用コマンド inactivate でマネージメントポー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マネージメントポートが active 状態になります。マネージメントポートをシャットダウンした場合は，装置を再起動してもマネージメントポートは disable 状態のままです。マネージメントポートを active 状態にする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。

(2)　IPv4 アドレスの設定

[設定のポイント]

マネージメントポートに IPv4 アドレスを設定します。IPv4 アドレスを設定するには，インタフェースの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 mgmt 0**
   マネージメントポートの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**
   マネージメントポートに 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。

(3)　IPv6 アドレスの設定

[設定のポイント]

マネージメントポートに IPv6 アドレスを設定します。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]

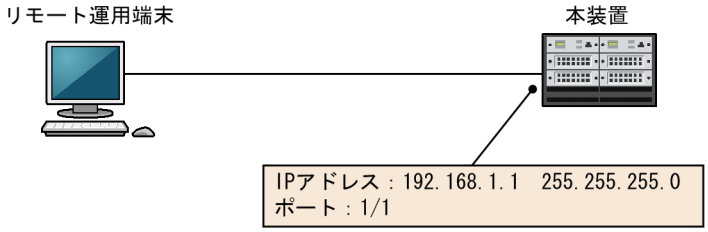
1. **(config)# interface mgmt 0**
   マネージメントポートのコンフィグレーションモードに移行します。
2. **(config-if)# ipv6 enable**
   マネージメントポートに IPv6 アドレス使用可を設定します。
3. **(config-if)# ipv6 address 2001:db8::1/64**
   マネージメントポートに IPv6 アドレス 2001:db8::1，プレフィックス長 64 を設定します。

7.2.3　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 7-4　リモート運用端末との接続例



[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/1**
   ポート 1/1 の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**
   (config-if)# exit
   ポート 1/1 のイーサネットインタフェースに 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。

7.2.4　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には，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。

7.2.5　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には，コンフィグレーションコマンド ftp-server を設定します。なお，本装置に対して同時に ftp プロトコルでリモートアクセスできるユーザ数は最大 16 です。

このコンフィグレーションが設定されていない場合，ftp プロトコルを使用し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。

7.2.6　VRF での telnet によるログインを許可する

(1)　グローバルネットワークを含む全 VRF から telnet によるログインを許可する場合

[設定のポイント]

全 VRF からのアクセスを許可するには，コンフィグレーションコマンド transport input の vrf all パラメータを設定します。この vrf all パラメータが設定されていない場合，グローバルネットワークからのアクセスだけを許可します。

[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。

2. **(config-line)# transport input vrf all telnet**

   (config-line)#

   グローバルネットワークを含む全 VRF で，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。

(2)　指定 VRF から telnet によるログインを許可する場合

[設定のポイント]

指定 VRF からのアクセスを許可するには，コンフィグレーションコマンド transport input の vrf パラメータで VRF ID を設定します。この vrf パラメータが設定されていない場合，グローバルネットワークからのアクセスだけを許可します。

[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。

2. **(config-line)# transport input vrf 2 telnet**

```
(config-line)#
```

VRF 2 で，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。なお，グローバルネットワークは含みません。

7.2.7　VRF での ftp によるログインを許可する

(1)　グローバルネットワークを含む全 VRF から ftp によるログインを許可する場合

[設定のポイント]

全 VRF からのアクセスを許可するには，コンフィグレーションコマンド ftp-server の vrf all パラメータを設定します。この vrf all パラメータが設定されていない場合，グローバルネットワークからのアクセスだけを許可します。

[コマンドによる設定]

1. `(config)# ftp-server vrf all`

   グローバルネットワークを含む全 VRF で，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。

(2)　指定 VRF から ftp によるログインを許可する場合

[設定のポイント]

指定 VRF からのアクセスを許可するには，コンフィグレーションコマンド ftp-server の vrf パラメータで VRF ID を設定します。この vrf パラメータが設定されていない場合，グローバルネットワークからのアクセスだけを許可します。

[コマンドによる設定]

1. `(config)# ftp-server vrf 2`

   VRF 2 で，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。なお，グローバルネットワークは含みません。

7.3　オペレーション

7.3.1　運用コマンド一覧

マネージメントポートで使用する運用コマンド一覧を次の表に示します。

表 7-6　運用コマンド一覧

コマンド名	説明
show ip interface※1	IPv4 インタフェースの状態を表示します。
show ip arp※1	ARP エントリ情報を表示します。
clear arp-cache※1	ダイナミック ARP 情報を削除します。
clear ip duplicate-address※1	Address Conflict Detection によって重複が検出されたアドレスの通信の抑止状態を解除します。
ping※1	IPv4 エコーテストを行います。
show ipv6 interface※2	IPv6 インタフェースの状態を表示します。
show ipv6 neighbors※2	NDP 情報を表示します。
clear ipv6 neighbors※2	ダイナミック NDP 情報をクリアします。
clear ipv6 duplicate-address※2	Duplicate Address Detection によって重複が検出されたアドレスの通信の抑止状態を解除します。
ping ipv6※2	ICMP6 エコーテストを行います。

注※1

「運用コマンドレファレンス Vol.3　2. IPv4・ARP・ICMP」を参照してください。

注※2

「運用コマンドレファレンス Vol.3　3. IPv6・NDP・ICMPv6」を参照してください。

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 7-7　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(SecureShell)」を参照してください。

7.3.2　リモート運用端末と本装置との通信の確認

本装置とリモート運用端末との通信は，運用コマンド ping や ping ipv6 などを使用して確認できます。詳細は，「コンフィグレーションガイド Vol.3　2. IP・ARP・ICMP の設定と運用」または「コンフィグレーションガイド Vol.3　4. IPv6・NDP・ICMPv6 の設定と運用」を参照してください。

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設定

8.1.1　コンフィグレーション・運用コマンド一覧

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）および AUX 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。
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。
enable password	装置管理者モードへの変更（enable コマンド）時に使用するパスワードを設定します。
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。
username	本装置へログインするユーザアカウントを作成して，パスワードを設定します。

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
show users	コンフィグレーションコマンド username で設定したユーザアカウントを表示します。
make hidden-password	コンフィグレーションコマンド username，enable password に設定するハッシュ化パスワード文字列を作成します。
show sessions (who)	本装置にログインしているユーザを表示します。
show whoami (who am i)	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しています。

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，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. VRF で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，ip access-group，ipv6 access-class で制限できます。
7. VRF で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。
8. 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。システム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。
9. 入力したコマンドとその応答メッセージおよびシステム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。
10. 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。
11. 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および削除

コンフィグレーションコマンド username を使用して，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（パスワードを入力）

```
(config)# username newuser password input
New password:********                                  <-1
Retype new password:********                           <-2
(config)#
```

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）。

入力したパスワードは，自動的にハッシュ化されてコンフィグレーションに設定されます。パスワードを入力しないで［Enter］キーを押した場合は，パスワードなしのログインユーザになります。

ログインユーザ作成時に，運用コマンド make hidden-password で作成したハッシュ化パスワードを指定することもできます。ハッシュ化パスワードを指定したログインユーザの作成例を次の図に示します。

図 8-2　ユーザ newstaff を作成（ハッシュ化パスワードを指定）

```
> make hidden-password                                                    <-1
Input password:********                                                   <-2
Retype password:********                                                  <-3

A password was created. Set it in the configuration.
"$6$pRo7aJE ... 3ewCiDAwB1"                                               <-4
> enable
# configure
(config)# username newstaff password hidden "$6$pRo7aJE ... 3ewCiDAwB1"    <-5
(config)#
```

1. 運用コマンド make hidden-password を実行します。
2. 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）。
3. 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）。
4. ハッシュ化パスワード文字列が作成されます。
5. make hidden-password コマンドで作成したハッシュ化パスワード文字列を指定します。

hidden 以降に""を指定した場合は，パスワードなしのログインユーザになります。

なお，作成したログインユーザは運用コマンド show users で確認できます。

使用しなくなったログインユーザはコンフィグレーションから削除してください。ログインユーザの削除例を次の図に示します。

図 8-3　ユーザ newuser を削除

```
(config)# no username newuser
Do you want to delete the user account newuser? (y/n): y        <-1
(config)#
```

1. y を入力すると，指定したログインユーザを削除します。

初期導入時に設定されているログインユーザ「username operator 100 password hidden ""」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で削除することをお勧めします。

ログインユーザを削除するとホームディレクトリも削除されるため，残したいファイルはあらかじめ/usr/home/share へ保存するか，外部にバックアップをしてください。ただし，/usr/home/share 内のファイルはすべてのユーザが読み込みおよび書き込みができるため，ファイルの管理に注意してください。

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。

8.1.4　ログインユーザのパスワードの設定および変更

コンフィグレーションコマンド username を使用して，ログインユーザのパスワードを設定および変更してください。パスワードの設定例を次の図に示します。

図 8-4　ユーザ newuser のパスワード設定および変更（パスワードを入力）

```
(config)# username newuser password input
New password:********                          <-1
Retype new password:********                   <-2
(config)#
```

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）。

入力したパスワードは，自動的にハッシュ化されてコンフィグレーションに設定されます。パスワードを入力しないで［Enter］キーを押した場合は，パスワードなしのログインユーザになります。

パスワードの設定および変更時に，運用コマンド make hidden-password で作成したハッシュ化パスワードを指定することもできます。ハッシュ化パスワードを指定したパスワードの設定例を次の図に示します。

図 8-5　ユーザ newstaff のパスワード設定および変更（ハッシュ化パスワードを指定）

```
> make hidden-password                                                    <-1
Input password:********                                                  <-2
Retype password:********                                                 <-3

A password was created. Set it in the configuration.
"$6$pRo7aJE ... 3ewCiDAwB1"                                              <-4
> enable
# configure
(config)# username newstaff password hidden "$6$pRo7aJE ... 3ewCiDAwB1"  <-5
(config)#
```

1.運用コマンド make hidden-password を実行します。

2.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）。

3.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）。

4.ハッシュ化パスワード文字列が作成されます。

5.make hidden-password コマンドで作成したハッシュ化パスワード文字列を指定します。

hidden 以降に""を指定した場合は，パスワードなしのログインユーザになります。

8.1.5　装置管理者モード変更のパスワードの設定および変更

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ないので認証なしで装置管理者モードに変更します。

しかし，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お勧めできないため，コンフィグレーションコマンド enable password を使用して装置管理者モード変更のパスワードを設定および変更してください。パスワードの設定例を次の図に示します。

図 8-6　装置管理者モード変更のパスワード設定および変更（パスワードを入力）

```
(config)# enable password input
New password:********                          <-1
Retype new password:********                   <-2
(config)#
```

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）。

入力したパスワードは，自動的にハッシュ化されてコンフィグレーションに設定されます。パスワードを入力しないで［Enter］キーを押した場合は，パスワードなしになります。

パスワードの設定および変更時に，運用コマンド make hidden-password で作成したハッシュ化パスワードを指定することもできます。ハッシュ化パスワードを指定したパスワードの設定例を次の図に示します。

図 8-7　装置管理者モード変更のパスワード設定および変更（ハッシュ化パスワードを指定）

```
> make hidden-password                                                    <-1
Input password:********                                                  <-2
```

```
Retype password:********                                          <-3

A password was created. Set it in the configuration.
"$6$pRo7aJE ... 3ewCiDAwB1"                                       <-4
> enable
# configure
(config)# enable password hidden "$6$pRo7aJE ... 3ewCiDAwB1"      <-5
(config)#
```

1. 運用コマンド make hidden-password を実行します。
2. 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）。
3. 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）。
4. ハッシュ化パスワード文字列が作成されます。
5. make hidden-password コマンドで作成したハッシュ化パスワード文字列を指定します。

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。

8.1.6　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 8-8　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 プロトコルを使用し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 プロトコルを使用した本装置へのアクセスはできません。

図 8-9　ftp プロトコルによるアクセス許可の設定例

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

8.1.7　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，この設定に関係なく，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 8-10　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。

8.1.8　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，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。なお，アクセスを許可していない（コンフィグレーションで登録していない）端末からのアクセスがあった場合，すでにログインしているそのほかの端末には，アクセスがあったことを示すシステムメッセージ（メッセージ種別：ACCESS，メッセージ識別子：06000001）が表示されます。アクセスを許可する IP アドレスを変更しても，すでにログインしているユーザのセッションは切れません。

[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:db8:811:ff01::/64 any
   (config-ipv6-nacl)# exit
   ネットワーク(2001:db8:811:ff01::/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:db8:811:ff01::/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。

8.1.9　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 でログインバナーを設定すると，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経由して本装置の 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。

```
##################################################
Only Administrators can connect.
The Administrator's phone number is xxx-xxxx-xxxx.
##################################################
```

[コマンドによる設定]

1. **(config)# banner login plain-text**

   --- Press CTRL+D or only '.' line to end ---

   ##

   Only Administrators can connect.

   The Administrator's phone number is xxx-xxxx-xxxx.

   ##

   .

   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］キー）を入力します。

2. **(config)# show banner**

   banner login encode

   "IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjCk9ubHkgQWRtaW5pc3RyYX
   RvcnMgY2FuIGNvbm5lY3QuClRoZSBBZG1pbmlzdHJhdG9yJ3MgcGhvbmUgbnVtYmVyIGlzIHh4eC14eHh4LXh4eHguC
   iMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIwo="

   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**

   ##

   Only Administrators can connect.

   The Administrator's phone number is xxx-xxxx-xxxx.

   ##

   (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 8-11　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 '^]'.

##################################################
Only Administrators can connect.
The Administrator's phone number is xxx-xxxx-xxxx.
##################################################
login:
```

図 8-12　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-
##################################################
```

```
Only Administrators can connect.
The Administrator's phone number is xxx-xxxx-xxxx.
##################################################
220 10.10.10.10 FTP server ready.
Name (10.10.10.10:staff):
```

8.1.10　VRF での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にログインできるようになります。さらに，コンフィグレーションコマンド transport input の vrf パラメータを設定して，VRF からのアクセスを許可します。この vrf パラメータが設定されていない場合，グローバルネットワークからのアクセスだけを許可します。

グローバルネットワークを含む全 VRF で，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する設定例を次の図に示します。

図 8-13　グローバルネットワークを含む全 VRF で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)# transport input vrf all telnet
(config-line)#
```

指定 VRF で，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する設定例を次の図に示します。なお，グローバルネットワークは含みません。

図 8-14　VRF 2 で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)# transport input vrf 2 telnet
(config-line)#
```

また，リモート運用端末から ftp プロトコルを使用し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。VRF からのアクセスを許可する場合は，vrf パラメータを設定します。この vrf パラメータが設定されていない場合，グローバルネットワークからのアクセスだけを許可します。

グローバルネットワークを含む全 VRF で，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する設定例を次の図に示します。

図 8-15　グローバルネットワークを含む全 VRF でリモート運用端末から ftp プロトコルによるアクセスを許可する設定例

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

指定 VRF で，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する設定例を次の図に示します。なお，グローバルネットワークは含みません。

図 8-16　VRF 2 でリモート運用端末から ftp プロトコルによるアクセスを許可する設定例

```
(config)# ftp-server vrf 2
(config)#
```

8.1.11　VRF での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 アドレスをアクセスリストに設定することで，ログインを制限できます。

アクセスリストは，グローバルネットワークや VRF に対して個別に設定しますが，同一のアクセスリストを，グローバルネットワークを含むすべての VRF に適用する設定もできます。また，これらを組み合わせて設定できますが，複数のアクセスリストを使用する場合は，最後のアクセスリストだけ暗黙の廃棄が適用されます。

なお，アクセス元の VRF に対してアクセスリストがどのように適用される（アクセスリストの適用範囲）かは，アクセス元とアクセスリストの設定個所との関係によって変わります。例として，グローバルネットワーク，VRF 10 および VRF 20 から本装置にアクセスする場合，アクセスリストが設定されている個所によって，どのアクセスリストが適用されるかを次の表に示します（括弧内が，どのアクセスリストが適用されるかを示しています）。

表 8-3　アクセスリストの適用範囲

アクセスリスト設定個所	アクセス元 VRF		
	グローバルネットワーク	VRF 10	VRF 20
• global	(global)	−	−
• global • VRF 10	(global)	(VRF 10)	−
• global • VRF 10 • VRF ALL	(global) ※ 適用後 (VRF ALL)	(VRF 10) ※ 適用後 (VRF ALL)	(VRF ALL)

(凡例)

−：アクセスリストは適用されない。したがって，アクセス制限されない。

global：グローバルネットワーク

VRF 10：VRF 10

VRF ALL：グローバルネットワークを含む全 VRF

注※

個別に設定したアクセスリストは，VRF ALL に設定したアクセスリストよりも優先して適用されます。また，アクセスリストを複数使用しているため，個別に設定したアクセスリストの暗黙の廃棄は無視されます。そのため，個別に設定したアクセスリストに一致しない場合は，VRF ALL に設定したアクセスリストが適用されます。VRF ALL に設定したアクセスリストに一致しない場合は，暗黙の廃棄によって制限されます。

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，アクセスリストを使用します。コンフィグレーションコマンド ip access-list standard，ipv6 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設定していない場合，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。なお，アクセスを許可していない（コンフィグレーションで登録していない）端末からのアクセスがあった場合，すでにログインしているそのほかの端末には，アクセスがあったことを示すシステムメッセージ（メッセージ種別：ACCESS，メッセージ識別子：06000001）が表示されます。

設定例を次に示します。まず，グローバルネットワークを含む全 VRF でのリモート運用端末からのログインを制限します。次に，グローバルネットワークと指定 VRF だけ個別にログインを許可します。これによって，特定のネットワークからだけログインを許可します。

[コマンドによる設定]

1. **(config)# ip access-list standard REMOTE_VRFALL**
   (config-std-nacl)# deny any
   (config-std-nacl)# exit
   グローバルネットワークを含む全 VRF で, ログインを制限するアクセスリスト REMOTE_VRFALL を設定します。
2. **(config)# ip access-list standard REMOTE_GLOBAL**
   (config-std-nacl)# permit 192.168.0.0 0.0.0.255
   (config-std-nacl)# exit
   グローバルネットワークで，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 REMOTE_GLOBAL を設定します。
3. **(config)# ip access-list standard REMOTE_VRF10**
   (config-std-nacl)# permit 10.10.10.0 0.0.0.255
   (config-std-nacl)# exit
   VRF 10 で，ネットワーク（10.10.10.0/24）からだけログインを許可するアクセスリスト REMOTE_VRF10 を設定します。
4. **(config)# line vty 0 2**
   (config-line)# ip access-group REMOTE_VRFALL vrf all in
   (config-line)# ip access-group REMOTE_GLOBAL in
   (config-line)# ip access-group REMOTE_VRF10 vrf 10 in
   (config-line)#
   line モードに遷移し，グローバルネットワークを含む全 VRF にアクセスリスト REMOTE_VRFALL を，グローバルネットワークにアクセスリスト REMOTE_GLOBAL を，VRF10 にアクセスリスト REMOTE_VRF10 を適用します。
   グローバルネットワークでは，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。
   VRF10 では，ネットワーク（10.10.10.0/24）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。
   また，その他の VRF ではログインを制限します。

8.2　RADIUS/TACACS+の解説

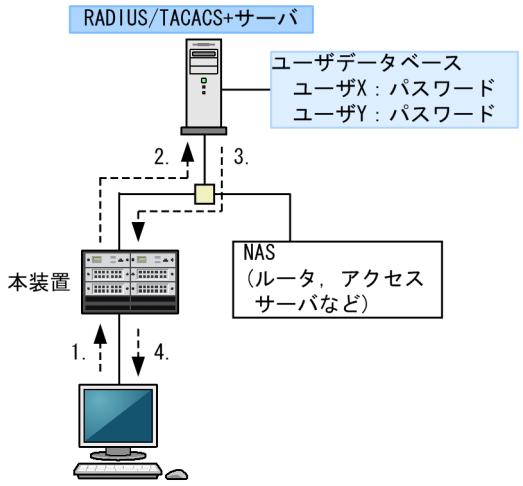
8.2.1　RADIUS/TACACS+の概要

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+認証の流れを次に示します。

図 8-17　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 を実行します。
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します。
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 を認証して，本装置にユーザ X を認証したことを通知します。
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 を許可します。

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+サーバに設定されているコマンドリストに従って，ユーザが実行するコマンドを許可または制限します。

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。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（IPv4/IPv6）
- 本装置への ssh（IPv4/IPv6）
- 本装置への ftp（IPv4/IPv6）
- 本装置への sftp（IPv4/IPv6）
- 本装置への scp（IPv4/IPv6）
- コンソール（RS232C）および AUX 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（IPv4/IPv6）
- 本装置への ssh（IPv4/IPv6）
- コンソール（RS232C）および AUX 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（IPv4/IPv6）によるログイン・ログアウト
- 本装置への ssh（IPv4/IPv6）によるログイン・ログアウト
- 本装置への ftp（IPv4/IPv6）によるログイン・ログアウト
- 本装置への sftp（IPv4/IPv6）によるログイン・ログアウト
- 本装置への scp（IPv4/IPv6）によるログイン・ログアウト
- コンソール（RS232C）および AUX 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）
- システム操作パネルでのコマンド入力（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 8-4　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）

分類	内容
	• 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）
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 8-5　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 8-10　設定するユーザ名属性」に従ってユーザ名を送信します。
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。 • RADIUS サーバへの送信元 IP アドレスが設定されている場合，送信元 IP アドレス • RADIUS サーバへの送信元 IP アドレスが設定されていなくて，ローカルアドレスが設定されている場合，ローカルアドレス • RADIUS サーバへの送信元 IP アドレスおよびローカルアドレスが設定されていない場合，送信インタフェースの IP アドレス
NAS-IPv6-Address	95	Access-Request Accounting-Request	本装置の IPv6 アドレス。 • RADIUS サーバへの送信元 IPv6 アドレスが設定されている場合，送信元 IPv6 アドレス • RADIUS サーバへの送信元 IPv6 アドレスが設定されていなくて，ローカルアドレスが設定されている場合，ローカルアドレス • RADIUS サーバへの送信元 IPv6 アドレスおよびローカルアドレスが設定されていない場合，送信インタフェースの IPv6 アドレス 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。

属性名	属性値	パケットタイプ	内容
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/AUX 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 IPv4/IPv6 アドレス，コンソールは“console”，AUX は“aux”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。
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 8-6　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

分類		内容
		• 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 • 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 8-7　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 8-10　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。

service	属性	説明
		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 8-8　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 8-9　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。

Attribute	Value
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+，ならびにコンフィグレーションコマンド username および enable password 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

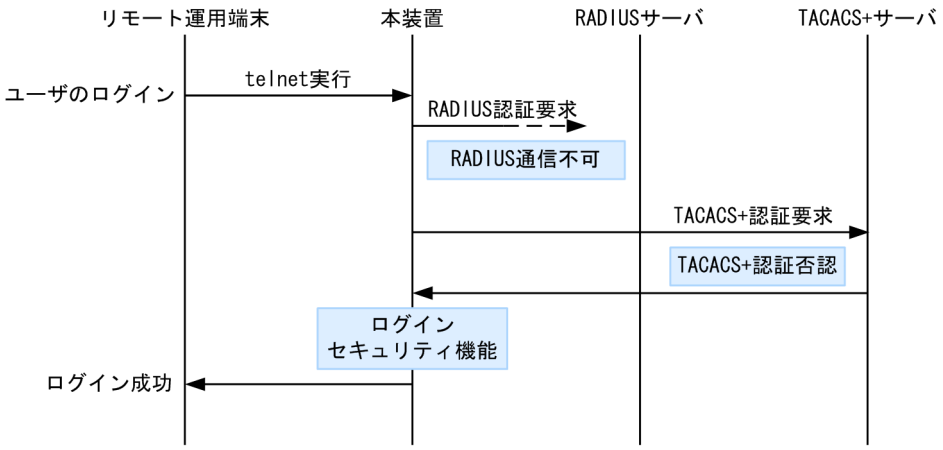
aaa authentication enable end-by-reject

(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 8-18　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

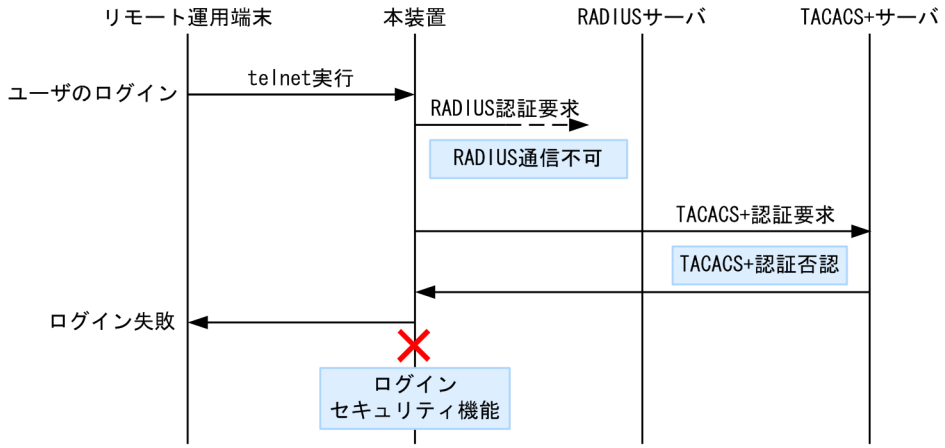
TACACS+サーバでの認証に失敗すると，次に本装置のログインセキュリティ機能での認証を実行します。ここで認証に成功し，ユーザは本装置へのログインに成功します。

(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 8-19　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指定できます。一つのサーバと通信できなくて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，優先順序に従ってアドレスを一つだけ決定して，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，「11.1　解説」を参照してください。

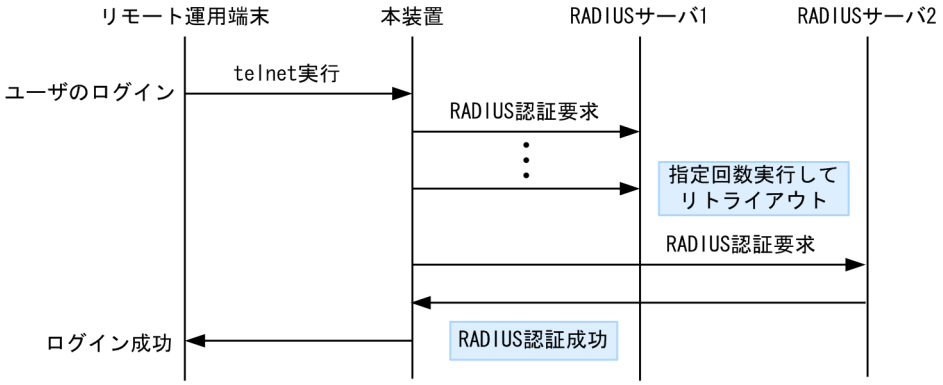
注意

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。

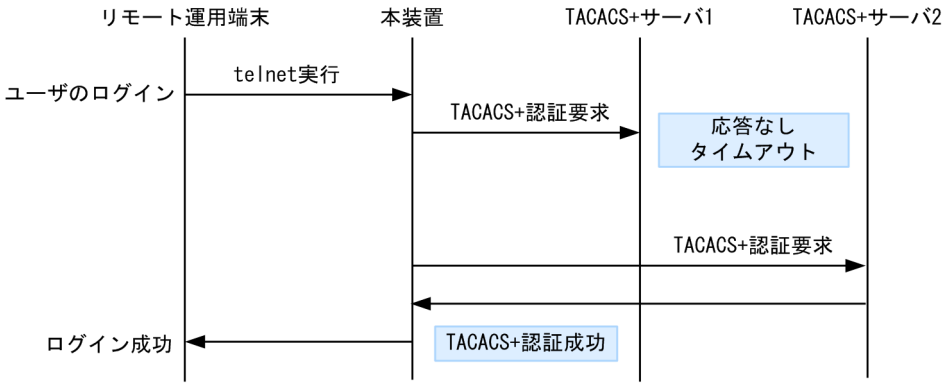
図 8-20　RADIUS サーバ選択のシーケンス



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 に対して本装置から 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 8-21　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 に対して本装置から 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。

- 本装置にコンフィグレーションコマンド username 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。
  - ユーザ名：remote_user
  - ホームディレクトリ：/usr/home/share

本装置に未登録のユーザ名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 8-10　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，使用するサーバによっては，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。

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て，使用できるコマンドの種類を制限できます。これをコマンド承認と呼びます。コマンド承認の制限対象となるコマンドは，コンフィグレーションコマンド，運用コマンド，およびマニュアルに掲載されていないデバッグコマンドです。ただし，一部のコマンドは制限対象になりません。コマンド承認の設定有無に関係なく，常に実行できるコマンドを次の表に示します。

表 8-11　常に実行できるコマンド一覧

分類	コマンド
コンフィグレーションコマンド	top，end※，exit※，quit

分類	コマンド
運用コマンド	logout，exit，quit，set terminal※，show whoami，who am i

注※　その文字列から開始するコマンドも含みます。

ユーザが使用できるコマンドは，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って制御されます。

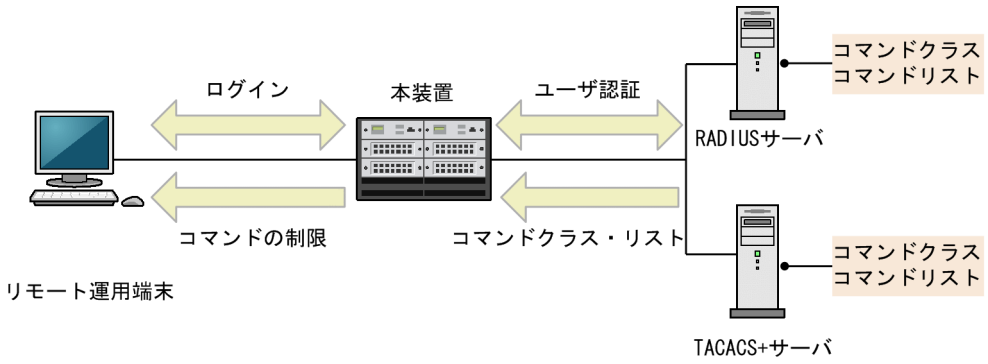
制限したコマンドは，CLI の補完機能で補完候補として表示しません。なお，<vlan id>や<host name>などの，<>で囲まれたパラメータ部分の値や文字列を含んだコマンドを，許可するコマンドリストに指定した場合は，<>部分は補完候補として表示しません。

(1)　コマンド承認の流れ

対象とするユーザのログインに先だって，コマンド承認のための設定をします。RADIUS/TACACS+指定時は，RADIUS/TACACS+のリモート認証サーバにコマンドクラスとコマンドリストを登録します。ローカル指定時は，コマンドクラスとコマンドリストをコンフィグレーションで設定します。

RADIUS サーバおよび TACACS+サーバによるログイン認証とコマンド承認の流れを次の図に示します。

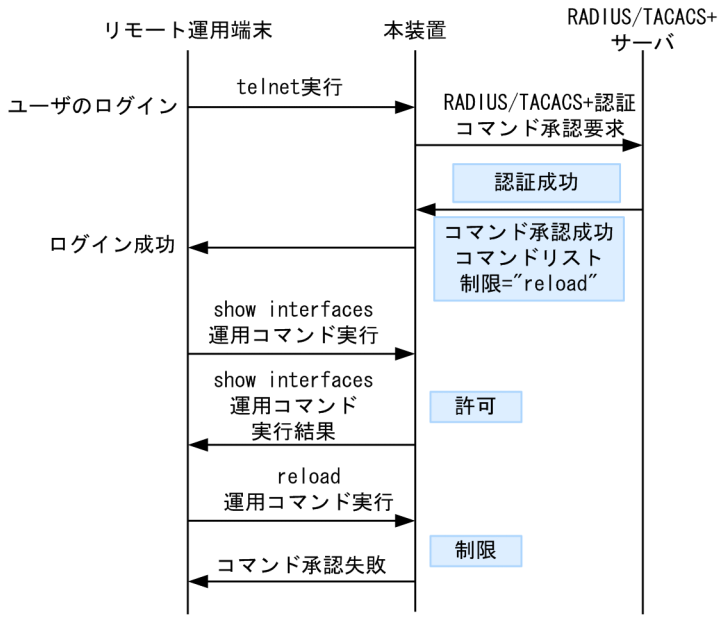
図 8-22　RADIUS/TACACS+サーバによるログイン認証，コマンド承認



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クラスおよび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クラスおよび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クラスおよびコマンドリストに従って，ログイン後のコマンドを許可または制限します。

RADIUS サーバおよび TACACS+サーバによるコマンド承認例を次の図に示します。

図 8-23　RADIUS/TACACS+サーバによるコマンド承認例



この例では，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。

(2)　コマンドクラスの指定

各ユーザに対して，制限または許可するコマンドのポリシーを決定します。本装置では，コマンドクラスを指定することで，一定のポリシーに従ってコマンド群を許可したり制限したりできます。サポートするコマンドクラスとコマンド承認動作を次の表に示します。

表 8-12　コマンドクラスとコマンド承認動作

コマンドクラス	説明	コマンド承認時のコマンドの扱い	
		制限	許可
noenable	コマンド入力モードを装置管理者モードへ変更する運用コマンド enable を制限するコマンドクラスです。一般ユーザモードで入力できる運用コマンドだけを許可します。	• コンフィグレーションコマンド • 運用コマンド enable • 入力モードが装置管理者モードだけの運用コマンド • デバッグコマンド	• 制限以外の運用コマンド
noconfig	コンフィグレーションの変更を制限するコマンドクラスです。	• コンフィグレーションコマンド • 次の文字列から始まる運用コマンド config，copy，erase configuration • デバッグコマンド	• 制限以外の運用コマンド

コマンドクラス	説明	コマンド承認時のコマンドの扱い	
		制限	許可
noauthorization	コマンド承認に関係するコンフィグレーションコマンドを制限するコマンドクラスです。コンフィグレーションの編集と操作に関するコンフィグレーションコマンドおよびコンフィグレーションを操作する運用コマンド（copy，erase configuration）も許可します。	• 次の文字列から始まるコンフィグレーションコマンド aaa，username，radius-server，tacacs-server，parser view • デバッグコマンド	• 制限以外のコンフィグレーションコマンド • 運用コマンド
allcommand	コンフィグレーションコマンドおよび運用コマンドを制限しないコマンドクラスです。	• デバッグコマンド	• コンフィグレーションコマンド • 運用コマンド
root	マニュアルに掲載されていないデバッグコマンド（ps コマンドなど）を含め，すべてのコマンドを制限しないコマンドクラスです。	なし	• コンフィグレーションコマンド • 運用コマンド • デバッグコマンド

(3)　コマンドリストの指定

コマンドクラス以外に，許可するコマンドと制限するコマンドをそれぞれコマンドリストに指定できます。許可コマンドリストおよび制限コマンドリストには，コンフィグレーションコマンドおよび運用コマンドを指定できます。マニュアルに掲載されていないデバッグコマンドは，コマンドリストに指定できません。

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，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，合致するかどうかで判定し（前方一致），コマンドの実行を許可したり制限したりします。

なお，特別な文字列として，all を指定できます。all はコンフィグレーションコマンドおよび運用コマンドのすべてを意味します。

許可コマンドリスト，制限コマンドリスト，およびコマンドクラスの設定有無による動作例を次に示します。

［設定例 1］許可コマンドリストだけを設定した場合

設定された文字列と合致する文字列を含むコマンドだけを許可します。

表 8-13　設定例 1 の内容と指定コマンドの判定結果

設定	指定コマンド	判定
許可コマンドリスト＝"show ip ,ping" 制限コマンドリスト　設定なし	show ip arp	許可
	show ipv6 neighbors	制限
	ping ipv6 ::1	許可

設定	指定コマンド	判定
	reload	制限

許可コマンドリストに"show ip "（ip の後ろに半角スペース）と設定されているため，合致する show ip arp コマンドは許可されますが，合致しない show ipv6 neighbors コマンドは許可されません。

［設定例 2］制限コマンドリストだけを設定した場合

設定された文字列と合致する文字列を含むコマンドだけを制限します。該当しないコマンドは，すべて許可として判定されます。

表 8-14　設定例 2 の内容と指定コマンドの判定結果

設定	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"	show ip arp	許可
	show ipv6 neighbors	許可
	ping ipv6 ::1	許可
	reload	制限

［設定例 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た場合

- 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。
- 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に判定されます。ただし，all 指定は文字数 1 とします。
- 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 8-15　設定例 3 の内容と指定コマンドの判定結果

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 ipv6" 制限コマンドリスト＝"show,ping"	show system	許可
	show ipv6 neighbors	許可
	ping ipv6 ::1	許可
	ping 10.10.10.10	制限
	clear logging	許可

［設定例 4］コマンドクラスとコマンドリストの両方を設定した場合

- root 以外のコマンドクラスを設定した場合は，コマンドクラスごとに規定されたコマンドリストと，設定したコマンドリストを合わせて判定します。コマンドクラスごとに規定されたコマンドリストを次の表に示します。

表 8-16　コマンドクラスごとに規定されたコマンドリスト

コマンドクラス	規定のコマンドリスト
noenable	制限コマンドリスト＝"enable"
noconfig	制限コマンドリスト＝"config,copy,erase configuration"

コマンドクラス	規定のコマンドリスト
noauthorization	制限コマンドリスト＝"aaa,username,radius-server,tacacs-server,parser view"
allcommand	許可コマンドリスト＝"all"

- コマンドクラス root を設定した場合は，コマンドリストの設定は無効になります。

表 8-17　設定例 4 の内容と指定コマンドの判定結果

設定	指定コマンド	判定
コマンドクラス＝"noauthorization" 許可コマンドリスト＝"username user password" 制限コマンドリスト　設定なし	username user password	許可
	username	制限

コマンドクラス noauthorization を設定すると，username から始まるコンフィグレーションコマンドは制限されます。ログインパスワードを変更できるようにしたい場合は，username <user name> password を許可コマンドリストに設定します。

(4)　RADIUS/TACACS+サーバへの登録情報

RADIUS または TACACS+のリモートサーバに，コマンドの制限に対応した属性値を設定します。例として，次の表に示すポリシーでコマンドを制限します。

表 8-18　コマンド制限のポリシー例

ユーザ名	ポリシー例	設定内容
staff	コンフィグレーションコマンドおよび運用コマンドを制限なく使用できる。	コマンドクラス＝"allcommand" 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
guest	制限以外の運用コマンドを使用できる。	コマンドクラス　設定なし 許可コマンドリスト　設定なし 制限コマンドリスト＝"reload,inactivate,enable"
test	指定した運用コマンドだけを使用できる。	コマンドクラス　設定なし 許可コマンドリスト＝"show ip "

(a)　RADIUS サーバへの登録

RADIUS サーバを利用してコマンドを制限する場合は，認証時に次の表に示す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	−	コマンドクラス 次の文字列のどれか一つを指定します。 noenable，noconfig，noauthorization，allcommand，root
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。

属性	ベンダー固有属性	値
		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：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。 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 8-24　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 8-25　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. コマンドクラス allcommand で，デバッグコマンド以外のコマンドを許可します。
2. enable，reload，および inactivate で始まるコマンドを制限します。
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 8-26　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="noenable,allcommand"と記述した場合，noenable だけが有効になります。
- ALAXALA-Deny-Commands, ALAXALA-Allow-Commands のそれぞれで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，次の例のように同一属性を複数エントリに記述し，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 8-27　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,.....”
```

(b)　TACACS +サーバへの登録

TACACS+サーバを使用してコマンドを制限する場合は，TACACS+サーバで承認の設定として次の表に示す属性－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 noenable，noconfig，noauthorization，allcommand，root
	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。 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。 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，次のような設定ファイルイメージになります。

図 8-28　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。
   コマンドクラス allcommand で，デバッグコマンド以外のコマンドを許可します。
2. enable，reload，および inactivate で始まるコマンドを制限します。
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="noenable,allcommand"と記述した場合, noenable だけが有効になります。
- deny-commands，allow-commands のそれぞれで，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。

(5)　コマンド承認の注意事項

- コマンドクラスおよび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。
- RADIUS/TACACS+指定時, サーバ側でコマンドクラスまたはコマンドリストを設定していない場合, ユーザが認証されログインできても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。ローカル指定時，コンフィグレーションコマンドでコマンドクラスまたはコマンドリストを設定していない場合も同様です。これらの場合は，コンソールからログインしてください。
  また，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，デフォルトリスタート後，ログインしてください。
- ローカル指定時，コマンド承認の設定は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。コマンドクラスまたはコマンドリストが設定されていないユーザは，コマンドが制限されて実行できなくなるため，設定に漏れがないように注意してください。

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。

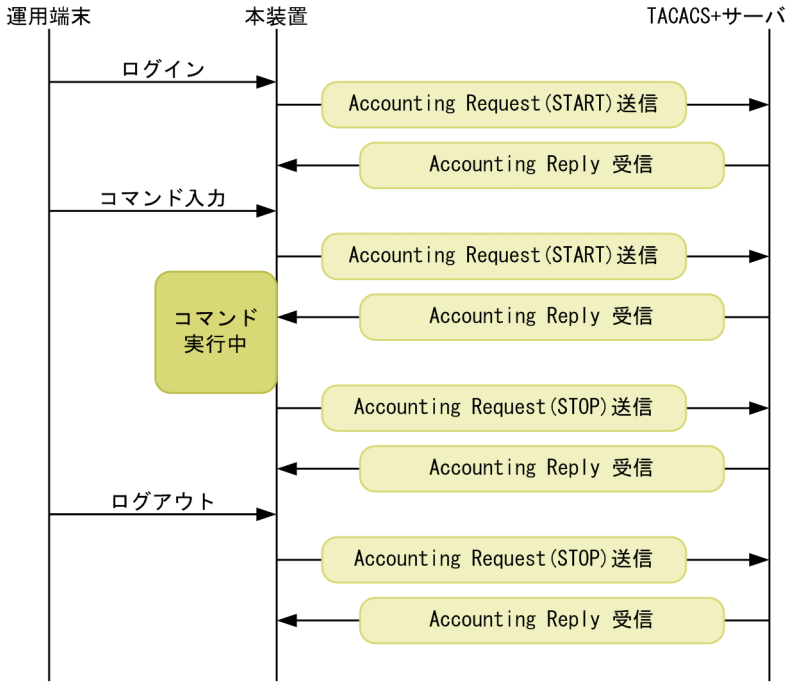
アカウンティングの設定は，ログインとログアウトのイベントを送信するログインアカウンティング指定と，コマンド入力のイベントを送信するコマンドアカウンティング指定があります。コマンドアカウンティングは TACACS+だけでサポートしています。

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。

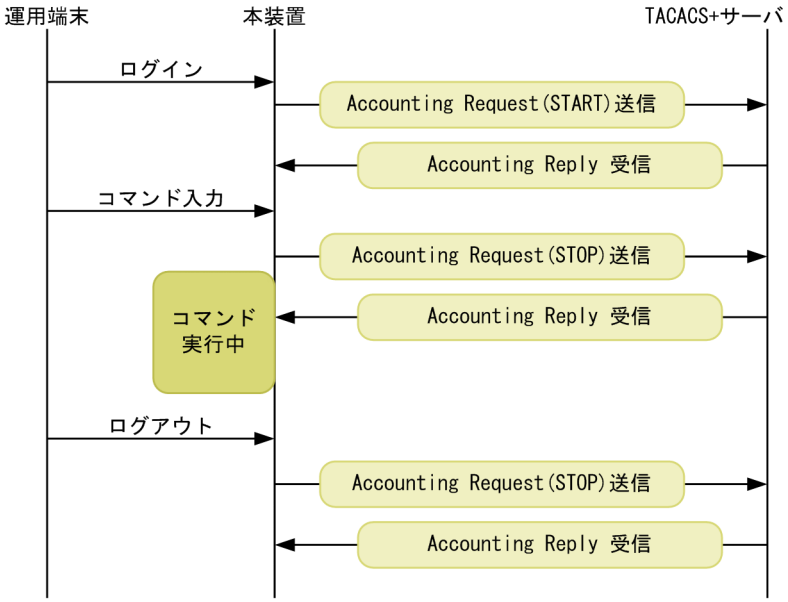
図 8-29　TACACS+アカウンティングのシーケンス（ログイン・コマンドアカウンティングの START-STOP 送信モード時）



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 8-30　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 8-29　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 radius-server host の送信元 IP アドレスが設定されている場合は，そのアドレスを使用します。
- コンフィグレーションコマンド radius-server host の送信元 IP アドレスが設定されていなくて，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使用します。
- コンフィグレーションコマンド radius-server host の送信元 IP アドレス，および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，ローカルアドレスまたはコンフィグレーションコマンド radius-server host の送信元 IP 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，ローカルアドレスまたは radius-server host コマンドの送信元 IP 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，ローカルアドレスまたは radius-server host コマンドの送信元 IP 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 tacacs-server host の送信元 IP アドレスが設定されている場合は，そのアドレスを使用します。
- コンフィグレーションコマンド tacacs-server host の送信元 IP アドレスが設定されていなくて，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使用します。

- コンフィグレーションコマンド tacacs-server host の送信元 IP アドレス，および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。

8.3　RADIUS/TACACS+のコンフィグレーション

8.3.1　コンフィグレーションコマンド一覧

RADIUS/TACACS+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（認証）

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）および AUX 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。
username	本装置へログインするユーザアカウントを作成して，パスワードを設定します。

表 8-24　コンフィグレーションコマンド一覧（コマンド承認）

コマンド名	説明
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）および AUX 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。
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。
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。

表 8-25　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してください。

[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。

(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してください。

[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。

(3)　ローカルコマンド承認の設定例

[設定のポイント]

あらかじめ，ローカル認証を使用する設定をしてください。
コマンドクラスとコマンドリストを同時に設定できますが，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。

[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。

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。

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。

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システムメッセージ（メッセージ種別：ACCESS，メッセージ識別子：27000013）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システムメッセージ（メッセージ種別：ACCESS，

メッセージ識別子：27000013）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実行したときにシステムメッセージ（メッセージ種別：ACCESS，メッセージ識別子：27000013）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。

8.4　RADIUS/TACACS+のオペレーション

8.4.1　運用コマンド一覧

RADIUS/TACACS+に関する運用コマンド一覧を次の表に示します。

表 8-26　運用コマンド一覧

コマンド名	説明
show whoami (who am i)	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。

8.4.2　コマンド承認の確認

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または許可していることを確認してください。

図 8-31　コマンドクラス allcommand を使用した場合の確認例

```
> 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                                                <-1
Wed Jan 7 12:00:10 UTC 20XX
> /bin/date                                                 <-2
The command is not authorized by the RADIUS/TACACS+ server or the configuration.
>
```

1. コマンドが許可されます。
2. コマンドが制限されます。

図 8-32　コマンドリストで運用コマンドを制限した場合の確認例

```
>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                                                <-1
Wed Jan 7 12:00:10 UTC 20XX
> reload                                                    <-2
The command is not authorized by the RADIUS/TACACS+ server or the configuration.
>
```

1. コマンドが許可されます。
2. コマンドが制限されます。

図 8-33　特定のコマンド文字列に合致するコマンドを許可した場合の確認例

```
>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                                                  <-1
> show ipv6 neighbors                                          <-2
The command is not authorized by the RADIUS/TACACS+ server or the configuration.
>
```

1.コマンドが許可されます。

2.コマンドが制限されます。

9 SSH(SecureShell)

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を経由して接続する際に使用する機能です。SSH を使用すると，通信路は暗号化され，厳しい基準で認証できるため，ネットワーク上の悪意のある第三者の盗聴，改ざん，なりすましから通信内容を保護できます。SSH を使用することで，telnet 接続の脅威であった，運用情報の流出，データの改ざん，不正なりすましサーバへの誤接続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（盗聴）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（盗聴）

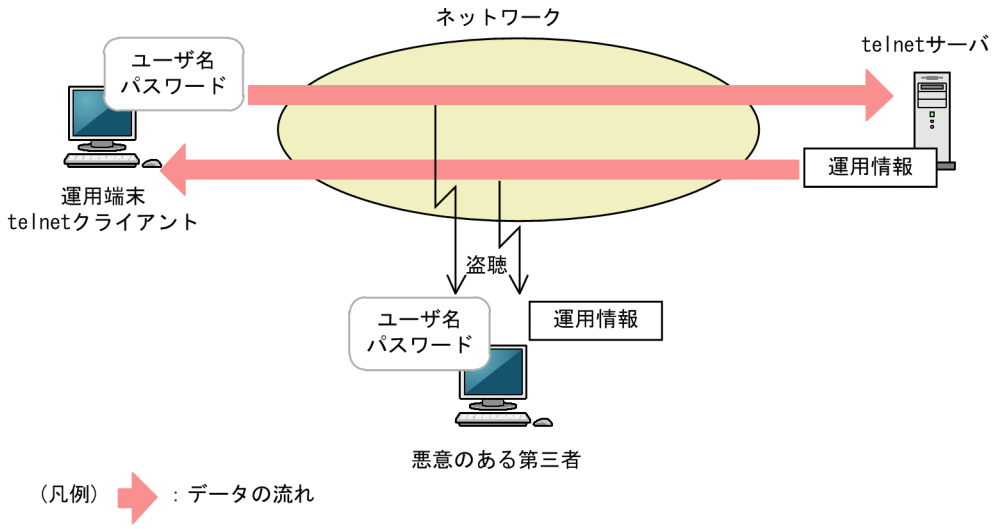
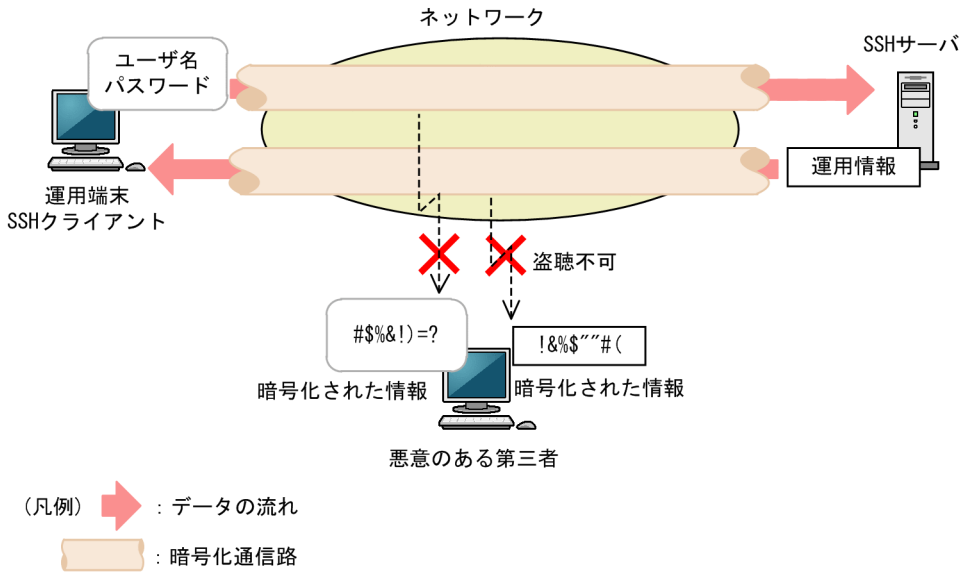


図 9-2　SSH 接続によるセキュアな運用管理



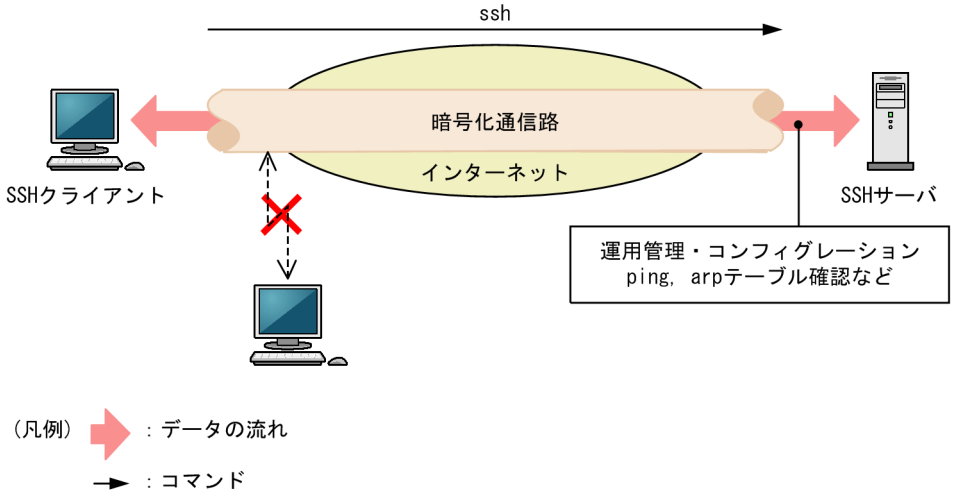
9.1.2　SSH の基本機能

(1)　セキュアリモートログイン

通常，SecureShell（SSH）と呼ばれる機能です。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。さらに，ログインしなくてもサーバのコマンドを実行できます。

本装置で運用する際，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できます。さらに，ログインしないで安全に，ARP テーブルを確認したり，運用コマンド ping による疎通確認テストをしたりできます。セキュアリモートログインについて次の図に示します。

図 9-3　セキュアリモートログイン



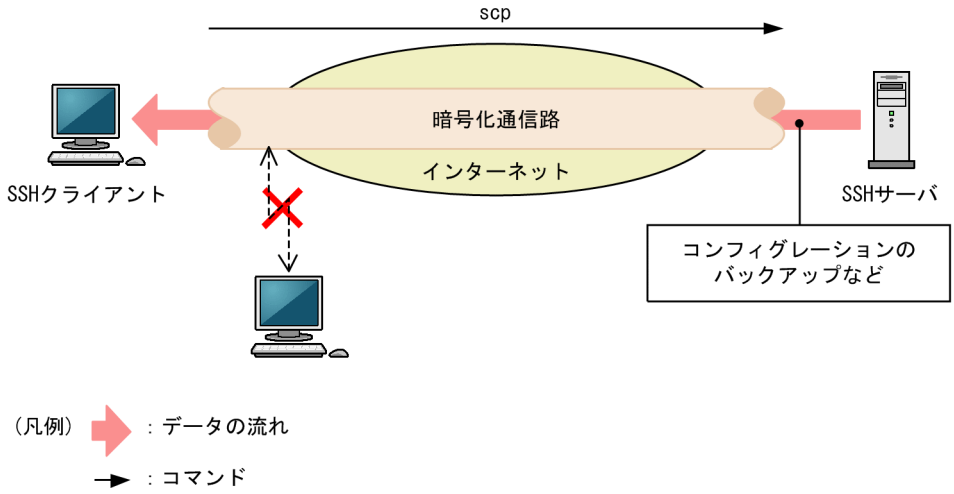
SSH サーバへログインするためのユーザの認証方法には，telnet で使用されていたパスワード認証のほかに，より安全な公開鍵認証を使用できます。公開鍵認証を使用することで，パスワードが漏洩し，他者に利用されることを防ぎます。なお，本装置上で公開鍵認証を使用するには，あらかじめユーザごとにユーザ公開鍵を登録する必要があります。

(2)　セキュアコピー

セキュアコピー（scp）と呼ばれる機能です。セキュアコピーを使用すると，運用端末と SSH サーバ間でファイルを転送できます。また，通信内容を他者に見られたり，改ざんされたりすることがないため，安全な運用管理を実現できます。セキュアコピーは，UNIX のリモートコピーコマンド（rcp）と同様のインタフェースで使用できます。

本装置で運用する際，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。セキュアコピーについて次の図に示します。

図 9-4　セキュアコピー

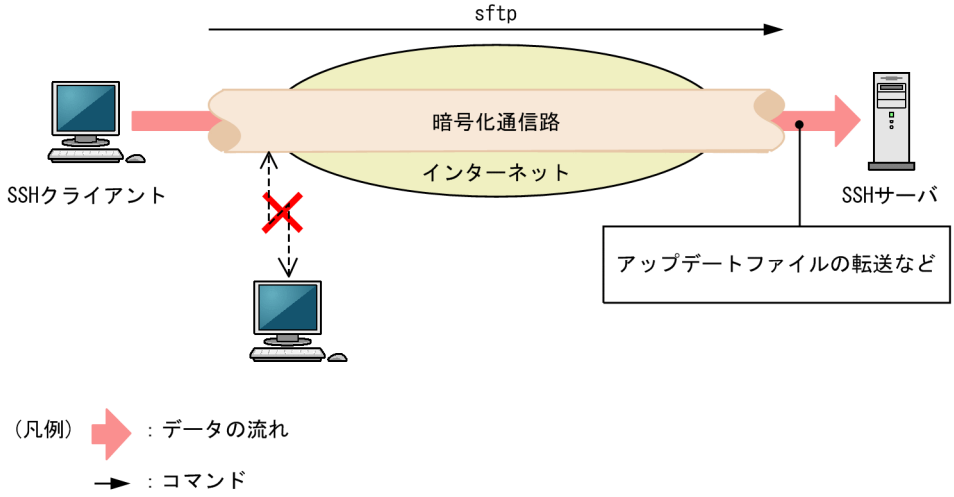


(3)　セキュアファイル転送

セキュア FTP（sftp）と呼ばれる機能です。セキュア FTP を使用すると，運用端末と SSH サーバ間でファイルを転送できます。また，通信内容を他者に見られたり，改ざんされたりすることがないため，安全な運用管理を実現できます。セキュア FTP は，ftp と同様のインタフェースで使用できます。

本装置で運用する際，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。セキュアファイル転送について次の図に示します。

図 9-5　セキュアファイル転送



9.1.3　サポート機能

SSH は，IPv4 および IPv6 による通信を暗号化する各種機能を提供します。SSH には，プロトコルとしてバージョン 1（SSHv1）とバージョン 2（SSHv2）があります。

SSHv2 は鍵の交換に Diffie-Hellman 鍵交換プロトコルを使用し，暗号通信データの完全性を保護するためにメッセージ認証コードを採用しています。そのため，SSHv2 は SSHv1 に比べてセキュリティが向上しています。本装置では，SSHv1 と SSHv2 の SSH サーバおよび SSH クライアントをサポートしています。運用する際は，上記に示すセキュリティ上の理由から，できるだけ SSHv2 を使用してください。

本装置がサポートする SSH 機能一覧を次の表に示します。

表 9-1　SSH 機能サポート一覧

機能名		説明	プロトコルバージョン	本装置
SSH サーバ	セキュアリモートログイン	SSH のリモートログイン（telnet 相当）	SSHv1 SSHv2	○
	セキュアコピー	SSH を使用したファイルコピー（rcp 相当）	SSHv1 SSHv2	○
	セキュアファイル転送	SSH を使用したファイル転送（ftp 相当）	SSHv2	○
SSH クライアント	セキュアリモートログイン	SSH のリモートアクセス（telnet 相当）	SSHv1 SSHv2	○
	セキュアコピー	SSH を使用したファイルコピー（rcp 相当）	SSHv1 SSHv2	○
	セキュアファイル転送	SSH を使用したファイル転送（ftp 相当）	SSHv2	○
認証エージェント		認証エージェント機能	SSHv1 SSHv2	×
ポート転送		ポート転送（TCP トンネリング）	SSHv1 SSHv2	×
X11 プロトコル自動転送		X11 を自動転送する機能	SSHv1 SSHv2	×
データ圧縮		通信のデータを圧縮する機能	SSHv1 SSHv2	×

（凡例）　○：サポート　×：未サポート

本装置でサポートする SSH 詳細機能一覧を次の表に示します。

表 9-2　SSH 詳細機能サポート一覧

詳細機能			プロトコルバージョン	本装置
ユーザ認証方法	公開鍵認証	RSA 公開鍵認証	SSHv1 SSHv2	サーバ：○ クライアント：×
		DSA 公開鍵認証	SSHv2	サーバ：○ クライアント：×
		PGP 鍵を使用した認証	SSHv2	×
		CA 認証を使用した認証	SSHv2	×
	パスワード認証	ローカルパスワード認証	SSHv1 SSHv2	サーバ：○ クライアント：○
		本装置の RADIUS/TACACS+認証と連携したパスワード認証	SSHv1 SSHv2	○

詳細機能		プロトコルバージョン	本装置
	ホストベース/RSARhost 認証	SSHv1 SSHv2	×
	Rhost 認証	SSHv1	×
共通鍵暗号方式	aes128-ctr，aes192-ctr，aes256-ctr，arcfour256，arcfour128，arcfour，aes128-cbc，aes192-cbc，aes256-cbc	SSHv2	○
	3des-cbc，blowfish-cbc	SSHv1 SSHv2	○
	twofish128-cbc	SSHv2	×
	その他	SSHv1 SSHv2	×
メッセージ認証コード方式	hmac-sha1，hmac-sha1-96，hmac-md5，hmac-md5-96	SSHv2	○
	その他	SSHv2	×
ログインメッセージ表示	ログイン前メッセージ表示	SSHv2	○
	ログイン後メッセージ表示	SSHv1 SSHv2	○

（凡例）　○：サポート　×：未サポート

9.1.4　SSH の接続構成

SSH 機能を使用するネットワーク構成例を次に示します。

図 9-6　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

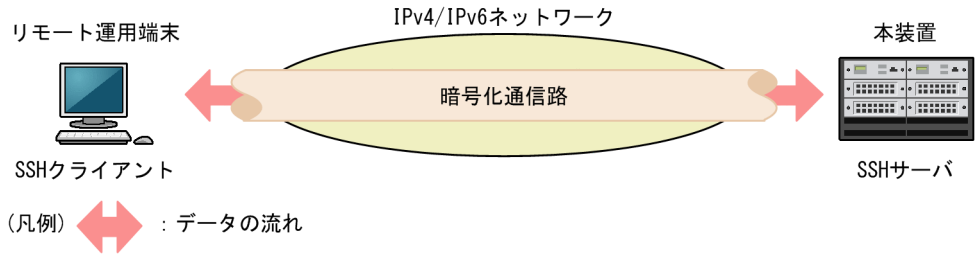


図 9-7　本装置の SSH クライアントからリモートにある SSH サーバへ接続する例

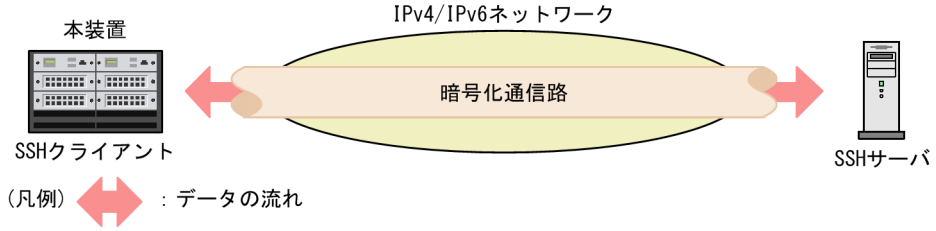
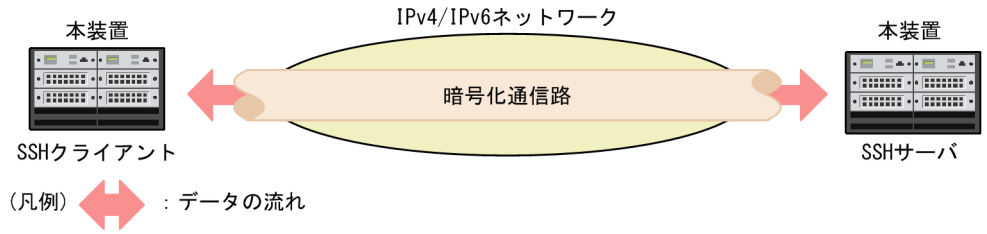


図 9-8　本装置の SSH クライアントからリモートにある別の本装置へ接続する例



9.1.5　SSHv1 による接続からログインまでの流れ

SSHv1 では，SSH クライアントから SSH サーバへ，次に示す手順で接続します。

1. バージョン文字列と各種暗号方式の交換
2. ホスト認証と暗号化通信路の確立
3. ユーザ認証
4. ログイン

以降，SSHv1 による接続の各手順について説明します。

(1)　バージョン文字列と各種暗号方式の交換

接続後，サーバとクライアントの間で SSH バージョン文字列を交換し，SSHv1 で接続するか，SSHv2 で接続するかを決定します。

サーバは，ホスト公開鍵，サーバ公開鍵，および使用できる共通鍵暗号方式のリストをクライアントへ送付します。クライアントでは，そのリストから使用する共通鍵暗号方式を決定します。

(2)　ホスト認証と暗号化通信路の確立

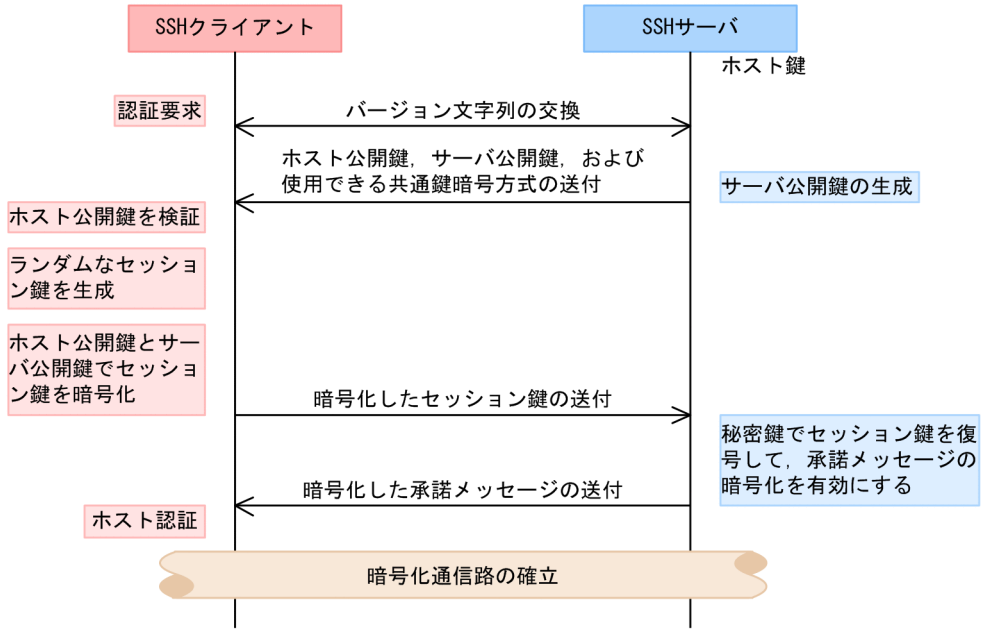
各 SSH サーバは，それぞれ異なるホスト鍵ペア（ホスト公開鍵とホスト秘密鍵）を保持しています。ホスト鍵ペアはインストール時に生成されます。クライアントは，サーバの正当性を確認するために，これらの鍵を使用します。

クライアントでは，サーバから送付されたホスト公開鍵を各ユーザが保持しているホスト公開鍵のデータベースと照合して，ホスト認証をします。その後，暗号化通信路に使用するセッション鍵を生成します。このセッション鍵を，ホスト公開鍵と，同時にサーバから送付されたサーバ公開鍵の両方を使用して暗号化し，サーバに送付します。

サーバでは，送付されたセッション鍵を自身の秘密鍵で復号できると，暗号化した承諾メッセージを送付して，正しいホストであることを証明します。同時に，暗号化通信路が確立されます。

SSHv1 での暗号化通信路の確立までの流れを次の図に示します。

図 9-9　暗号化通信路の確立までの流れ（SSHv1）



(3)　ユーザ認証

ホスト認証後，暗号化通信路が確立されると，公開鍵暗号方式またはローカルパスワードによるユーザ認証をします。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。

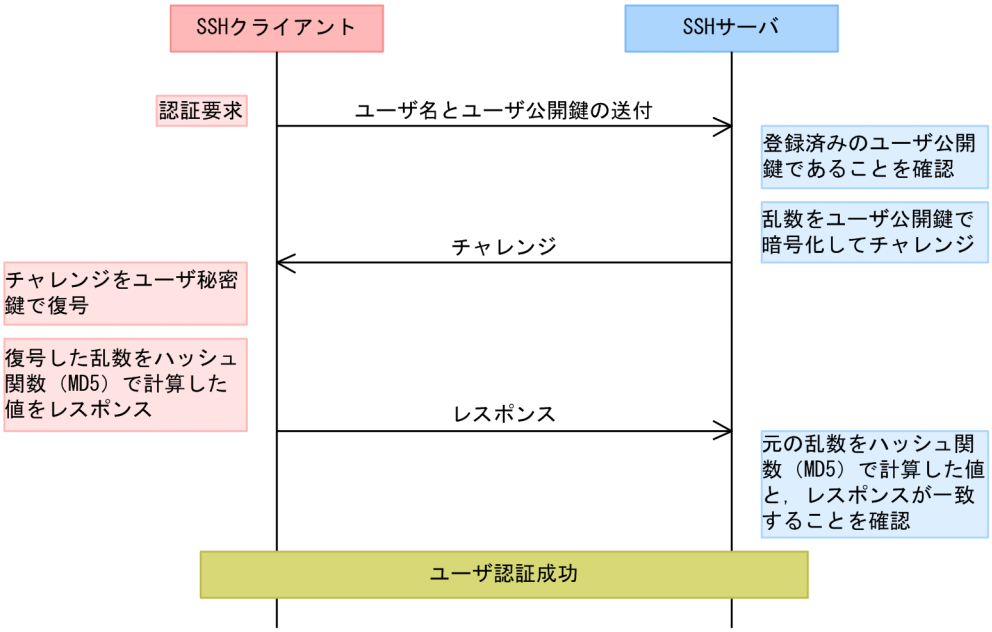
(a)　公開鍵暗号方式によるユーザ認証

サーバでは，あらかじめユーザの公開鍵を登録しておきます。クライアントでは，登録されているユーザ公開鍵に対応した，ユーザが所持している秘密鍵を使用して認証します。

SSHv1 では，「チャレンジ＆レスポンス」という方法を使用します。まず，サーバでは，ユーザから送付されたユーザ公開鍵が登録済みかどうかを確認します。その後，乱数を発生させ，それをユーザ公開鍵で暗号化し，クライアントに送付します（チャレンジ）。クライアントでは，チャレンジを秘密鍵で復号し，元の乱数に戻してから，その乱数をハッシュ関数（MD5）で計算した値をサーバに返送します（レスポンス）。サーバでは，元の乱数をハッシュ関数（MD5）で計算した値と，クライアントから返送された値を照合し，一致すればユーザ認証成功とします。

SSHv1 での公開鍵暗号方式によるユーザ認証の流れを次の図に示します。

図 9-10　公開鍵暗号方式によるユーザ認証の流れ（SSHv1）



(b)　ローカルパスワードによるユーザ認証

telnet と同様に，サーバでローカルに設定されたパスワードを使用してユーザ認証をします。しかし，パスワードは暗号化された通信路を経由するため，第三者には見えません。

(4)　ログイン

ユーザ認証に成功すると，セッションが確立し，ユーザはログインします。ここで，通常はターミナルのセッションが開始されます。クライアントが接続時にコマンドの実行を指定していた場合は，指定したコマンドが実行されます。scp や sftp で接続した場合は，サーバ側で scp や sftp-server コマンドが実行され，ファイルが転送されます。

9.1.6　SSHv2 による接続からログインまでの流れ

SSHv2 では，SSH クライアントから SSH サーバへ，次に示す手順で接続します。

1. バージョン文字列と各種暗号方式の交換
2. ホスト認証と暗号化通信路の確立
3. ユーザ認証
4. ログイン

以降，SSHv2 による接続の各手順について説明します。

(1)　バージョン文字列と各種暗号方式の交換

接続後，サーバとクライアントの間で SSH バージョン文字列を交換し，SSHv1 で接続するか，SSHv2 で接続するかを決定します。

サーバとクライアント間で，使用できる鍵交換方式，希望する公開鍵暗号方式，共通鍵暗号方式，メッセージ認証コード，および圧縮アルゴリズムの各リストを交換します。

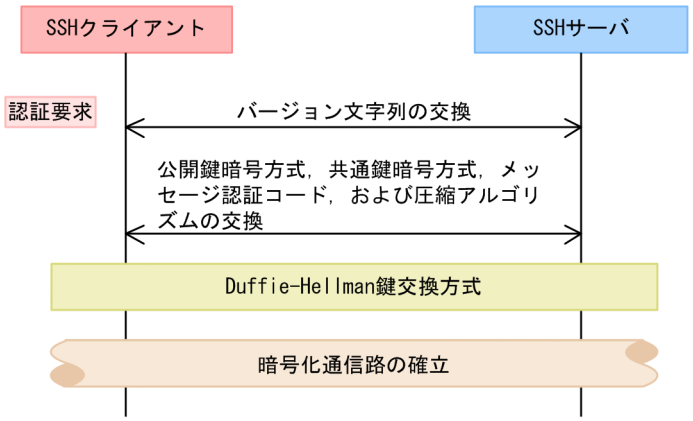
(2)　ホスト認証と暗号化通信路の確立

各 SSH サーバは，それぞれ異なるホスト鍵ペア（ホスト公開鍵とホスト秘密鍵）を保持しています。ホスト鍵ペアはインストール時に生成されます。クライアントは，サーバの正当性を確認するために，これらの鍵を使用します。

サーバおよびクライアントは，交換した共通鍵暗号方式やメッセージ認証コードのリストから，使用するアルゴリズムを決定します。その後，Diffie-Hellman 鍵交換方式で暗号化通信路に使用する共通鍵を交換します。共通鍵の交換中に，サーバのホスト公開鍵を，クライアントで保持しているホスト公開鍵のデータベースと照合して，ホスト認証もします。Diffie-Hellman 鍵交換方式は，交換する鍵を直接送ることなく，両者で鍵を共有できるアルゴリズムです。

SSHv2 での暗号化通信路の確立までの流れを次の図に示します。

図 9-11　暗号化通信路の確立までの流れ（SSHv2）



(3)　ユーザ認証

ホスト認証後，暗号化通信路が確立されると，公開鍵暗号方式またはローカルパスワードによるユーザ認証をします。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。

(a)　公開鍵暗号方式によるユーザ認証

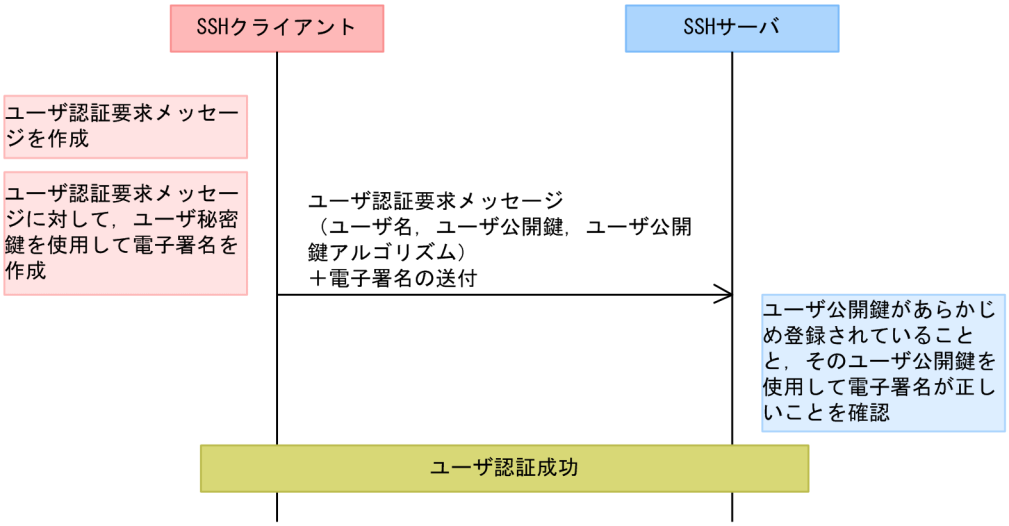
サーバでは，あらかじめユーザの公開鍵を登録しておきます。クライアントでは，登録されているユーザ公開鍵に対応した，ユーザが所持している秘密鍵を使用して認証します。

SSHv2 では，「電子署名」という方法を使用します。まず，クライアントでは，ユーザ名，ユーザの公開鍵，ユーザの公開鍵アルゴリズムを記述した認証要求メッセージを作成します。そして，作成した認証要求メッセージに対して，ユーザの秘密鍵を使用して電子署名を作成します。最後に，サーバに対して，認証要求メッセージに電子署名を付けたものを送付します。

サーバでは，送付された認証要求メッセージから，ユーザ名とユーザ公開鍵を取り出し，登録済みのユーザとユーザの公開鍵であることを確認します。また，登録されているユーザの公開鍵を使用して，送付された電子署名を審査し，正しいユーザの電子署名であることを確認できると，ユーザ認証成功とします。

SSHv2 での公開鍵暗号方式によるユーザ認証の流れを次の図に示します。

図 9-12　公開鍵暗号方式によるユーザ認証の流れ（SSHv2）



(b)　ローカルパスワードによるユーザ認証

telnet と同様に，サーバでローカルに設定されたパスワードを使用してユーザ認証をします。しかし，パスワードは暗号化された通信路を経由するため，第三者には見えません。

(4)　ログイン

ユーザ認証に成功すると，セッションが確立し，ユーザはログインします。ここで，通常はターミナルのセッションが開始されます。クライアントが接続時にコマンドの実行を指定していた場合は，指定したコマンドが実行されます。scp や sftp で接続した場合は，サーバ側で scp や sftp-server コマンドが実行され，ファイルが転送されます。

9.1.7　暗号化技術

SSH プロトコルでは，次に示す二種類の暗号方式（暗号化技術）を使用して，認証および暗号化通信をしています。

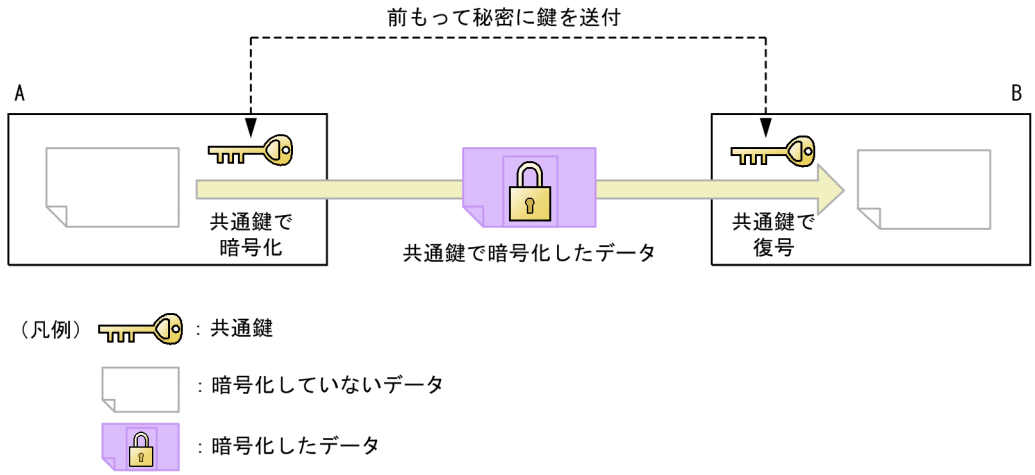
- 共通鍵暗号方式
- 公開鍵暗号方式

それぞれの暗号方式はさまざまなアルゴリズムによって実現されますが，基本的には元のデータに対して，特定のデータである鍵を使用し，特定の処理で暗号化します。また，暗号化されたデータは，ある鍵を使用して，特定の処理で復号します。

(1)　共通鍵暗号方式

A と B で共通の鍵である共通鍵を使用して，暗号化と復号をします。そのため，暗号化通信をする前に，この共通鍵を前もって秘密に送付しておくことが必要です。共通鍵暗号方式での暗号化通信を次の図に示します。

図 9-13　共通鍵暗号方式での暗号化通信



共通鍵暗号方式は，公開鍵暗号方式に比べて，演算の処理量が少ないという利点があります。そのため，SSH プロトコルでは，通信の暗号化にはこの共通鍵暗号方式を採用しています。

本装置では，使用する共通鍵暗号方式の種類を，コンフィグレーションコマンド ip ssh ciphers で設定するか，クライアントコマンドの-c パラメータで指定できます。

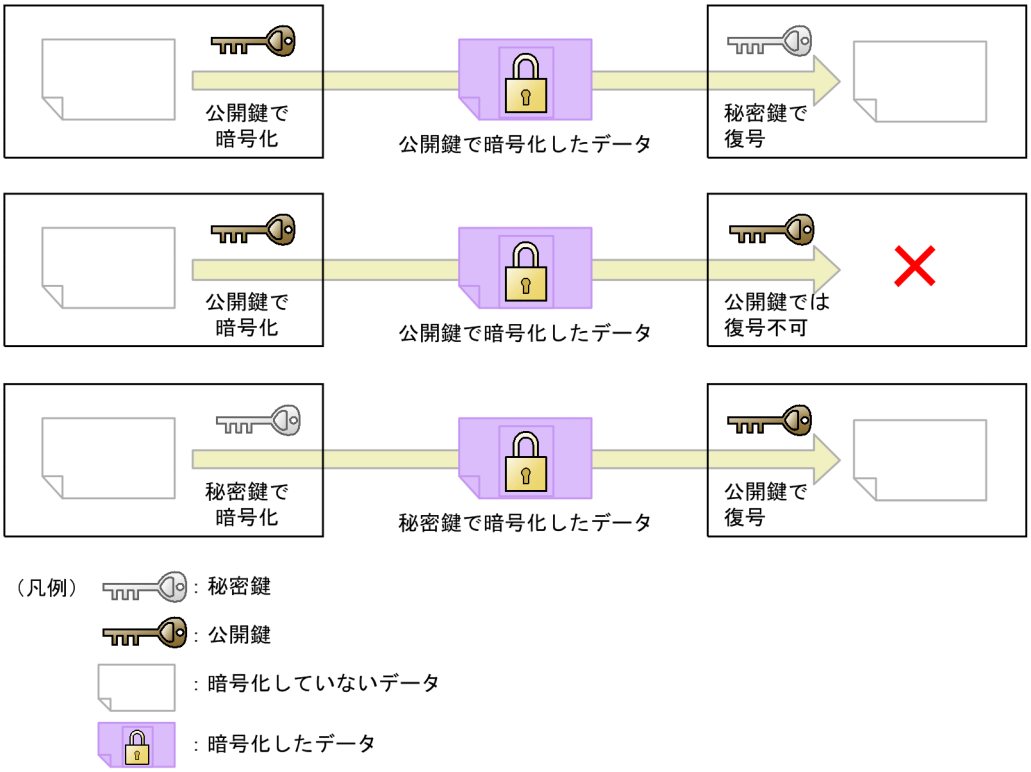
(2)　公開鍵暗号方式

公開鍵暗号方式は，二種類の鍵である公開鍵と秘密鍵を，ペアで使用します。この公開鍵と秘密鍵には次に示す性質があり，公開鍵暗号方式はこれらの性質を利用して暗号化や署名を実現しています。

- 公開鍵で暗号化したデータは，秘密鍵で復号できる
- 公開鍵で暗号化したデータは，公開鍵では復号できない
- 秘密鍵で暗号化したデータは，公開鍵で復号できる
- 公開鍵から秘密鍵を生成できない

公開鍵と秘密鍵の関係を次の図に示します。

図 9-14　公開鍵と秘密鍵の関係

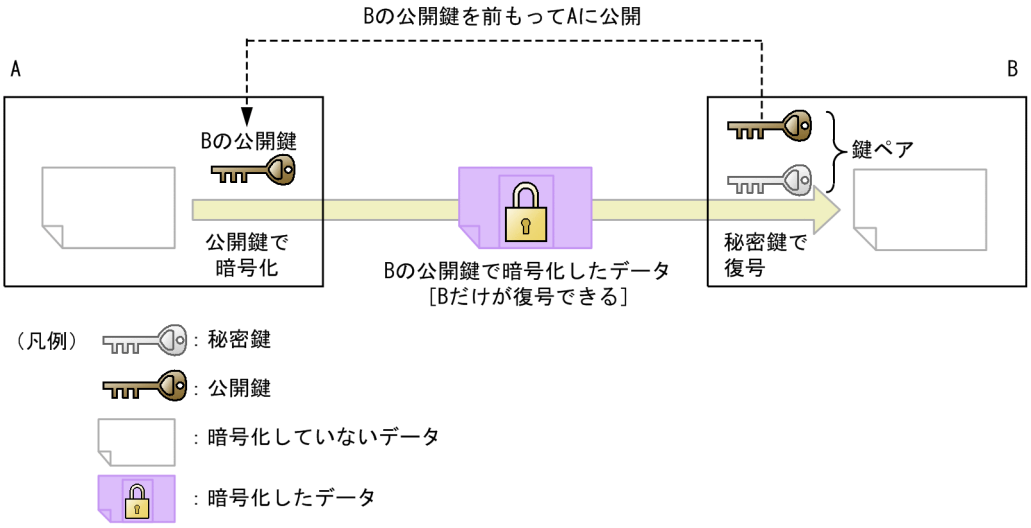


通常，鍵ペアを作成した側は，秘密鍵を任意のパスフレーズで暗号化して非公開で保管し，公開鍵を相手に公開します。相手側は，送信する相手の公開鍵を使用して，データを暗号化し送信します。

また，自身の秘密鍵を使用して暗号化したデータを相手に送付し，相手側が公開鍵で復号できることを確認することが，電子署名による確認です。

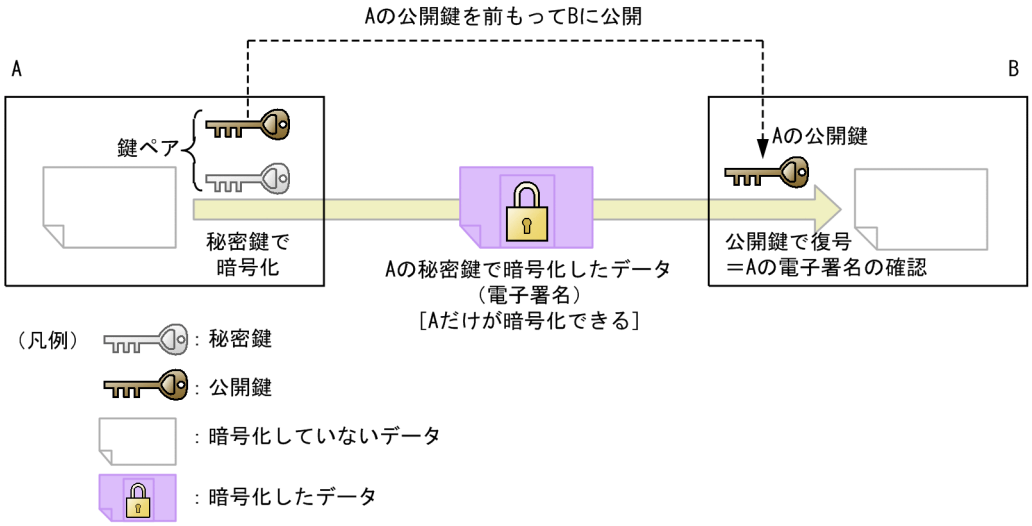
公開鍵暗号方式での暗号化について次の図に示します。この図では，鍵ペアを作成した B が，公開鍵を A に公開しています。A は，公開された B の公開鍵を使用してデータを暗号化して，B へ送付しています。送付されたデータは，B 自身の秘密鍵だけで復号できます。

図 9-15　公開鍵暗号方式での暗号化



公開鍵暗号方式での署名について次の図に示します。この図では，鍵ペアを作成した A が，公開鍵を B に公開しています。A は，自身の秘密鍵で暗号化したデータを B へ送付し，B は A の公開鍵で復号できることを確認することで，A が送付したデータだと確認できます（電子署名）。

図 9-16　公開鍵暗号方式での署名



公開鍵暗号方式は，共通鍵暗号方式に比べて，秘密に鍵を送付する必要がないため便利ですが，演算の処理量が大きいという欠点があります。そのため，SSH プロトコルでは，共通鍵の送付（SSHv1）または交換（SSHv2）と，ホスト認証およびユーザ認証にこの公開鍵暗号方式を採用しています。

本装置では，ユーザ認証の公開鍵認証に使用するユーザ公開鍵を，コンフィグレーションコマンド ip ssh authkey で設定できます。

9.1.8　メッセージ認証コード

SSHv2 では，メッセージ認証コードを使用して，通信内容の改ざんを検出しています。メッセージ認証コードとは，通信内容の改ざんを検出するための固定長のコードです。元の情報から作成した固定長のコードと，通信後のコードを比較します。通信中に元の情報が改ざんされた場合は，異なるコードになります。

本装置では，使用するメッセージ認証コードを，コンフィグレーションコマンド ip ssh macs で設定するか，クライアントコマンドの-m パラメータで指定できます。

9.1.9　ログインメッセージ表示

ログインの前後に，コンフィグレーションコマンド banner の login パラメータまたは motd パラメータで設定されたメッセージを表示します。ssh／sftp／scp の各ログインで，メッセージは共通です。また，login-ftp パラメータおよび motd-ftp パラメータでの設定は使用しません。

ログイン前のメッセージは，ログインプロンプトの前に表示します。SSHv2 だけでサポートします。

ログイン後のメッセージは，ログインしない接続である scp，sftp，または ssh -t でコマンドを実行した場合には表示しません。

9.1.10　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　コンフィグレーション

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　コンフィグレーションコマンド一覧

SSH 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 9-3　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 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※	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制限するために使用します。

注※

「コンフィグレーションコマンドレファレンス Vol.1　2. 運用端末接続」を参照してください。

9.2.2　SSH サーバの基本設定（ローカルパスワード設定）

最も手軽に SSH を使用して暗号化通信をするには，telnet と同じパスワード認証を使用します。この場合でも，telnet とは異なり，ユーザ名やパスワードは暗号化されて送付されるため，外部に漏洩しません。ここでは，ローカルパスワード認証を使用する場合の SSH サーバの設定例を示します。

なお，本装置のクライアントはローカルパスワード認証だけをサポートしているため，本装置間で SSH 接続をする場合は，ローカルパスワード認証を使用する必要があります。

[設定のポイント]

ログイン用のユーザアカウントの作成，および SSH サーバを動作させる設定例を示します。なお，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ません。

[コマンドによる設定]

1. **(config)# username staff password input**
   New password:****
   Retype new password:****
   ユーザ名（staff）とパスワードを設定して，ログイン用のユーザアカウントを作成します。
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，ログインできるユーザ数を 3 に設定します。

9.2.3　SSHv2 サーバで公開鍵認証をする設定

パスワード認証より安全に，SSH を使用して認証するには，公開鍵認証を使用します。公開鍵認証はパスワード認証とは異なり，パスワード自体がネットワーク上を流れません。したがって，たとえ暗号が解読されたとしても，パスワードは外部に漏洩しません。

SSHv2 で登録できる公開鍵の種類と鍵のビット長を次の表に示します。鍵のコメント部分を含めて 900 文字まで入力できます。この表に示すビット長はコメント部分がない場合の値で，コメント部分の文字数によって登録できるビット長は短くなります。

表 9-4　登録できる公開鍵の種類（SSHv2）

公開鍵の種類		登録できるビット長
DSA	SECSH 形式	1024
	OpenSSH 形式	
RSA	SECSH 形式	512～5120
	OpenSSH 形式	

(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 のユーザ公開鍵や OpenSSH 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 version 2**

   SSH サーバでプロトコルバージョン 2 だけ接続を許可します。

2. **(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。

3. **(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。

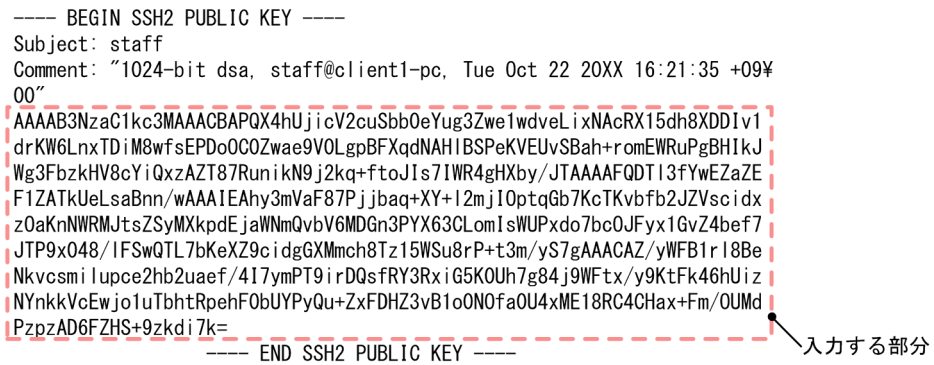
「.ssh」ディレクトリは，本装置の SSH サーバ機能が自動的に生成し，使用します。ユーザがファイルを置いた場合，削除されたり上書きされたりします。

(2) 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 9-17 ユーザ公開鍵（SECSH 形式）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 SECSH 形式の SSHv2 DSA のユーザ公開鍵で説明していますが，SSHv2 RSA 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]

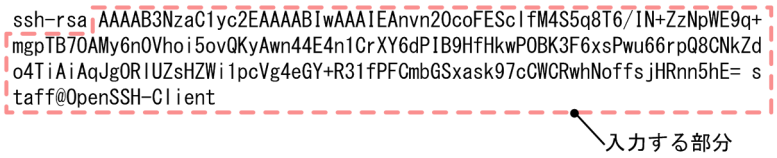
SECSH 形式のユーザ公開鍵には改行コードが含まれているため，すべての改行を取り除いて 1 行の形式にしてください。また，変換後のユーザ公開鍵の部分に空白を含めないでください。空白のあとは，コメントと見なされます。

(3) 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，先頭の「ssh-rsa」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 9-18　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 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-0 "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。

9.2.4　SSHv1 サーバで公開鍵認証をする設定

SSHv1 で登録できる公開鍵の種類と鍵のビット長を次の表に示します。鍵のコメント部分を含めて 900 文字まで入力できます。この表に示すビット長はコメント部分がない場合の値で，コメント部分の文字数によって登録できるビット長は短くなります。

表 9-5　登録できる公開鍵の種類（SSHv1）

公開鍵の種類	登録できるビット長
RSA	512～2560

(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。

[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-v1 load-key-file /usr/home/staff/identity.pub**

   ユーザ（staff）の SSHv1 のユーザ公開鍵を，あらかじめ転送したファイル（/usr/home/staff/identity.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-v1 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。

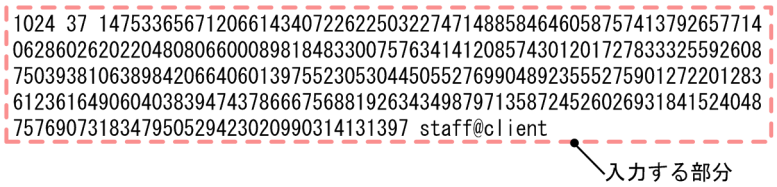
「.ssh」ディレクトリは，本装置の SSH サーバ機能が自動的に生成し，使用します。ユーザがファイルを置いた場合，削除されたり上書きされたりします。

(2)　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作成するユーザ公開鍵の例を次に示します。

図 9-19　作成するユーザ公開鍵（SSHv1 鍵）の例



[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。

9.2.5　SSH サーバの暗号アルゴリズム関連の設定変更

SSH の暗号化通信では，共通鍵暗号とメッセージ認証コードを使用します。本装置の SSH サーバ機能の共通鍵暗号とメッセージ認証コードは，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 ciphers aes128-cbc blowfish**

   SSH サーバの共通鍵暗号アルゴリズムとして，aes128-cbc と blowfish だけを使用する設定をします。

2. **(config)# ip ssh macs hmac-sha1 hmac-md5**

   SSH サーバのメッセージ認証コードアルゴリズムとして，hmac-sha1 と hmac-md5 だけを使用する設定をします。

9.2.6　RADIUS 認証と連携した SSH サーバの設定

SSH を使用して本装置にログインするときのパスワード認証を，RADIUS サーバで管理できます。

[設定のポイント]

RADIUS 認証に使用するサーバを 1 台指定し，RADIUS 認証に失敗した場合には本装置によるローカル認証をするように設定します。また，RADIUS サーバとの接続情報として，タイムアウト時間を 2 秒に設定します。

[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 認証およびローカル認証に設定します。
2. **(config)# radius-server host radius-server1 key "RADIUSKEY"**
   RADIUS 認証に使用するサーバのホスト名と共通鍵を設定します。
3. **(config)# radius-server timeout 2**
   RADIUS サーバからの応答タイムアウト時間を 2 秒に設定します。

9.2.7 SSHv2 サーバ機能だけを使用してセキュリティを高める

本装置は，装置の運用管理のために，telnet および ftp のサーバ機能をサポートしています。これらのサーバ機能は，コンフィグレーションによって使用できる状態になっていることがあります。

ここでは，telnet や ftp のサーバ機能を使用しないで SSH サーバ機能だけを使用して，セキュアな運用管理をする設定をします。

[設定のポイント]

SSH サーバ機能は，telnet や ftp と同等の運用管理機能をサポートしているため，SSH サーバ機能での運用管理に移行して，不要なサーバ機能を停止することをお勧めします。また，SSH サーバ機能はセキュリティの高い SSHv2 だけを使用します。さらに，アクセスリストを適用して，接続できる運用端末を制限します。

[コマンドによる設定]

1. **(config)# ip ssh version 2**
   SSH サーバでプロトコルバージョン 2 だけ接続を許可します。
2. **(config)# ip access-list standard REMOTE**
   (config-std-nacl)# permit 192.168.1.0 0.0.0.255
   (config-std-nacl)# exit
   ネットワーク（192.168.1.0/24）にあるリモート運用端末から本装置へのログインを許可するアクセスリストを作成します。
3. **(config)# ipv6 access-list REMOTE6**
   (config-ipv6-acl)# deny ipv6 any any
   (config-ipv6-acl)# exit
   IPv6 アドレスのリモート運用端末からのログインを拒否するアクセスリストを作成します。
4. **(config)# line vty 0 2**
   (config-line)# transport input ssh
   本装置にログインできるユーザ数を 3 に設定します。また，リモート運用端末から SSH プロトコルによるアクセスだけを許可します。
5. **(config-line)# ip access-group REMOTE in**
   ネットワーク（192.168.1.0/24）にあるリモート運用端末からだけアクセスを許可します。

6. **(config-line)# ipv6 access-class REMOTE6 in**

   IPv6 アドレスのリモート運用端末からのアクセスを拒否します。

9.2.8 VRF での SSH によるログインを許可する

[設定のポイント]

グローバルネットワークを含む全 VRF で，運用端末から本装置への SSH プロトコルによるリモートアクセスを許可する場合の SSH サーバの設定例を示します。

[コマンドによる設定]

1. **(config)# ip access-list standard REMOTE**

   (config-std-nacl)# permit 192.168.1.0 0.0.0.255

   (config-std-nacl)# exit

   ネットワーク（192.168.1.0/24）にあるリモート運用端末から本装置へのログインを許可するアクセスリストを作成します。

2. **(config)# ipv6 access-list REMOTE6**

   (config-ipv6-acl)# deny ipv6 any any

   (config-ipv6-acl)# exit

   IPv6 アドレスのリモート運用端末からのログインを拒否するアクセスリストを作成します。

3. **(config)# line vty 0 2**

   (config-line)# transport input vrf all ssh

   本装置にログインできるユーザ数を 3 に設定します。また，グローバルネットワークを含む全 VRF で，リモート運用端末から SSH プロトコルによるアクセスだけを許可します。

4. **(config-line)# ip access-group REMOTE vrf all in**

   グローバルネットワークを含む全 VRF で，ネットワーク（192.168.1.0/24）にあるリモート運用端末からだけアクセスを許可します。

5. **(config-line)# ipv6 access-class REMOTE6 vrf all in**

   グローバルネットワークを含む全 VRF で，IPv6 アドレスのリモート運用端末からのアクセスを拒否します。

9.3　オペレーション

9.3.1　運用コマンド一覧

SSH の運用コマンド一覧を次に示します。

表 9-6　運用コマンド一覧（SSH クライアント機能）

コマンド名	説明
ssh	SSHv1 および SSHv2 のクライアント機能を提供します。
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。

表 9-7　運用コマンド一覧（SSH サーバ機能）

コマンド名	説明
show ssh hostkey	ホスト公開鍵と Fingerprint を表示します。
set ssh hostkey	ホスト鍵ペアを変更します。
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。

9.3.2　SSH クライアントから SSH サーバへのログイン

ssh コマンドで，SSHv2 および SSHv1 サーバに接続できます。ただし，本装置の SSH クライアント機能はパスワード認証だけをサポートしているため，SSHv2 および SSHv1 サーバ側でパスワード認証を有効にする必要があります。

本装置の SSH クライアントからネットワーク経由で SSHv2 サーバへ接続する例を次の図に示します。

図 9-20　本装置の SSH クライアントから SSHv2 サーバへの接続例

```
> ssh -c aes128-cbc -m hmac-sha1 staff@192.168.1.1                    <-1
The authenticity of host '192.168.1.1 (192.168.1.1)' can't be established.
DSA key fingerprint is 75:c0:fa:9e:ec:4f:1d:98:1f:d5:59:1c:fc:35:07:b2.
Are you sure you want to continue connecting? (y/n): y               <-2
Warning: Permanently added '192.168.1.1' (DSA) to the list of known hosts.
staff@192.168.1.1's password: ******                                 <-3
```

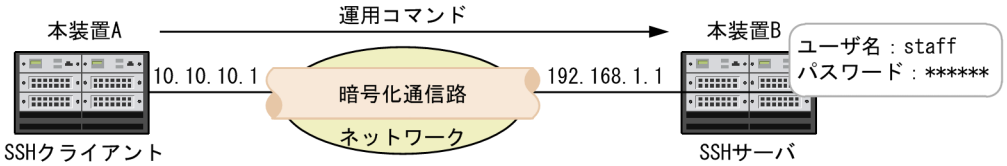
1. SSH サーバ 192.168.1.1 へ，ユーザ staff として接続します。その際，共通鍵暗号方式として aes128 を，メッセージ認証コード方式として hmac-sha1 を使用します。
2. SSHv2 サーバに最初に接続する場合は，クライアントユーザのホスト公開鍵データベースにホスト公開鍵が登録されていないため，登録の確認メッセージが表示されます。Fingerprint（鍵の指紋）を確認し，接続しようとしている SSHv2 サーバの正しいホスト公開鍵であることを確認してください。確認できたら，y と入力することで，データベースに登録し接続を続けます。

   なお，一度ユーザのホスト公開鍵データベースにホスト公開鍵を登録すると，次回の接続時には Fingerprint の確認はありません。
3. staff のパスワードを入力してログインします。

9.3.3　SSH クライアントから本装置で運用コマンドの実行

ssh コマンドで，本装置の SSH クライアントから，ネットワーク上の本装置に対して，ログインしないで運用コマンドを実行できます。本装置 A の SSH クライアントからネットワーク経由で本装置 B の SSH サーバへ SSHv2 で接続してコマンドを実行する構成例を次の図に示します。

図 9-21　SSH クライアントから SSH サーバでコマンドを実行する構成例



本装置 A の SSH クライアントから，本装置 B で運用コマンドを実行する例を次の図に示します。その際，強制的に仮想端末を割り当てるように，クライアント側でパラメータを指定する必要があります。一般的な SSH の実装では，ssh コマンドの-t パラメータを指定します。

図 9-22　本装置 A から本装置 B で運用コマンドを実行する例

```
> ssh -t staff@192.168.1.1 ping 10.10.10.1
staff@192.168.1.1's password: ******
PING 10.10.10.1 (10.10.10.1): 56 data bytes
64 bytes from 10.10.10.1: icmp_seq=0 ttl=255 time=0.108 ms
64 bytes from 10.10.10.1: icmp_seq=1 ttl=255 time=0.113 ms
64 bytes from 10.10.10.1: icmp_seq=2 ttl=255 time=0.116 ms
^C
--- 10.10.10.1 PING statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max = 0.108/0.114/0.118 ms
Connection to 192.168.1.1 closed.
>
```

9.3.4　SSH クライアントから SSH サーバへのファイル転送

(1)　セキュアコピー

scp コマンドで，ファイルを転送できます。ftp とは異なり通信路には SSHv1/SSHv2 を利用しているため，ユーザ名，パスワード，およびファイルは暗号化されて送信され，外部に漏洩したり改ざんされたりしません。

本装置の scp クライアントからネットワーク経由で SSH サーバへ接続し，本装置のコンフィグレーションファイルを転送する例を次に示します。

図 9-23　IPv4 で接続してセキュアコピーで本装置からファイルを転送する例

```
> scp config.txt staff@192.168.1.1:/home/staff/config/                    <-1
staff@192.168.1.1's password: ******                                      <-2
config.txt                                    100% 4062     4.0KB/s   00:00  <-3
>
```

1. SSH サーバ 192.168.1.1 へユーザ staff として接続し，あらかじめホームディレクトリに保存したコンフィグレーションファイル config.txt を，/home/staff/config/配下へ転送します。
2. staff のパスワードを入力します（SSH サーバに 2 回目以降接続するときは，クライアントユーザのホスト公開鍵データベースにホスト公開鍵が登録されているため，ホスト公開鍵の確認メッセージは表示されません）。
3. ファイルが転送されます。

図 9-24 IPv6 で接続してセキュアコピーで本装置からファイルを転送する例

```
> scp config.txt staff@[1111::1]:/home/staff/config/                    <-1
The authenticity of host '1111::1 (1111::1)' can't be established.
DSA key fingerprint is 75:c0:fa:9e:ec:4f:1d:98:1f:d5:59:1c:fc:35:07:b2
Are you sure you want to continue connecting? (y/n): y                 <-2
Warning: Permanently added '1111::1' (DSA) to the list of known hosts.
staff@1111::1's password: ******                                       <-3
config.txt                                    100% 4062     4.0KB/s   00:00  <-4
>
```

1. SSH サーバ 1111::1 へユーザ staff として接続し，あらかじめホームディレクトリに保存したコンフィグレーションファイル config.txt を，/home/staff/config/配下へ転送します。IPv6 アドレスはかぎ括弧[ ]で囲んで入力します。
2. SSHv2 サーバに最初に接続する場合は，クライアントユーザのホスト公開鍵データベースにホスト公開鍵が登録されていないため，登録の確認メッセージが表示されます。Fingerprint（鍵の指紋）を確認し，接続しようとしている SSHv2 サーバの正しいホスト公開鍵であることを確認してください。確認できたら，y と入力することで，データベースに登録し接続を続けます。

   なお，一度ユーザのホスト公開鍵データベースにホスト公開鍵を登録すると，次回の接続時には Fingerprint の確認はありません。
3. staff のパスワードを入力します。
4. ファイルが転送されます。

(2) セキュア FTP

sftp コマンドで ftp と同様のインタフェースでファイルを転送できます。ftp とは異なり通信路には SSHv2 を利用しているため，ユーザ名，パスワード，およびファイルは暗号化されて送信され，外部に漏洩しません。

本装置の sftp クライアントからネットワーク経由で SSH サーバへ接続し，本装置のコンフィグレーションファイルを転送する例を次の図に示します。

図 9-25 セキュア FTP でファイルを転送する例

```
> sftp staff@1111::1                                                   <-1
Connecting to 1111::1...
staff@1111::1's password:******                                        <-2
sftp> cd /home/staff/                                                  <-3
sftp> mkdir config                                                     <-4
sftp> cd config                                                        <-5
sftp> put config.txt                                                   <-6
Uploading config.txt to /home/staff/config/config.txt
config.txt                                    100% 4062     4.0KB/s   00:00
sftp> quit                                                             <-7
>
```

1. sftp コマンドを使用して，SSH サーバ 1111::1 へユーザ staff として接続します。
2. staff のパスワードを入力します（SSH サーバに 2 回目以降接続するときは，クライアントユーザのホスト公開鍵データベースにホスト公開鍵が登録されているため，ホスト公開鍵の確認メッセージは表示されません）。
3. /home/staff へディレクトリを移動します。
4. config ディレクトリを作成します。
5. /home/staff/config へディレクトリを移動します。
6. config.txt をサーバへ転送します。
7. サーバから切断します。

9.3.5 SSH サーバの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 Fingerprint を確認するように警告・承認確認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 Fingerprint（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 Fingerprint が確認できます。

図 9-26　ホスト公開鍵の表示

```
> show ssh hostkey
Date 20XX/01/20 12:00:00 UTC

******* SSHv1 Hostkey *******

1024 35 1091475483 ... 1288400783 1024-bit rsa1 hostkey

Fingerprint for key:
xelic-kovup-vedek-kusom-kumah-fusoz-hokog-kadiv-fydib-kubag-goxux
Fingerprint(HEX) for key:
dc:9b:cb:8b:3e:a0:b1:02:87:f7:06:cd:da:63:52:c2


******* SSHv2 Hostkey *******

ssh-rsa AAAAB3NzaC ... IkiThiGQ== 2048-bit rsa hostkey

Fingerprint for key:
xocig-nulor-sibof-curuk-fuvyh-vehig-hasib-ritev-mihut-zotak-vexex
Fingerprint(HEX) for key:
98:a2:10:90:9c:04:b0:fe:9d:a9:65:25:04:04:e7:98

>
```

本装置の SSH サーバでは, bubblebabble 形式と HEX 形式の Fingerprint をサポートしています。クライアントやサーバの実装によっては，SSHv1 での Fingerprint のサポートはありません。より安全に接続するためにも，SSHv2 で接続することをお勧めします。

9.3.6 SSH サーバのホスト鍵ペアの変更

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。この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，通常では変更する必要はありません。SSH サーバの管理組織の変更など，何かの理由でホスト鍵ペアを変更したい場合に，set ssh hostkey コマンドを実行します。

図 9-27　ホスト鍵ペアの変更

```
> enable
# set ssh hostkey

WARNING!!
Would you wish to change the SSH (v1 and v2) Hostkeys? (y/n): y

*** Changing the SSHv1 Hostkey, Please wait a minute ***
Generating public/private rsa1 key pair.
Your identification has been saved.
Your public key has been saved.
The key fingerprint is:
42:13:3c:08:3f:1e:96:11:3c:be:86:c8:39:f5:48:d9 1024-bit rsa1 hostkey

*** Changing the SSHv2 Hostkey, Please wait a minute ***
Generating public/private rsa key pair.
Your identification has been saved.
```

```
Your public key has been saved.
The key fingerprint is:
98:a2:10:90:9c:04:b0:fe:9d:a9:65:25:04:04:e7:98 2048-bit rsa hostkey

Generation of the SSHv1 and SSHv2 host keys is complete.
#
```

10 時刻の設定と NTP/SNTP

この章では，時刻の設定と NTP/SNTP について説明します。

10.1　解説

10.1.1　概要

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 または SNTP を使用して，ネットワーク上の NTP サーバまたは SNTP サーバと時刻を同期できます。本装置での NTP と SNTP の特徴は次のとおりです。

NTP の特徴

- 複数の NTP サーバを参照して，高い精度で時刻を同期できます。
- 過去の同期情報から時刻の精度を計算して，自動で時刻を補正できます。
- シンメトリック・アクティブ／パッシブモードを構成して，複数の NTP サーバ間で時刻を補正できます。

SNTP の特徴

- IPv6 を使用した時刻の同期をサポートしています。
- NTP のような時刻情報の計算がなく，設計がシンプルです。
- 最大 4096 の SNTP クライアントからの時刻情報の問い合わせに対応できます。

本装置が NTP または SNTP のクライアント機能を使用している場合に，NTP サーバまたは SNTP サーバと同期できます。また，本装置が NTP または SNTP のサーバ機能を使用している場合に，NTP クライアントまたは SNTP クライアントから同期できます。

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。

10.1.2　時刻の設定と NTP/SNTP に関する注意事項

- 時刻が変更された場合，運用コマンド show cpu で表示される CPU 使用率の統計情報は 0 クリアされます。
- サマータイムの設定は過去の時刻をさかのぼって有効となります。
- NTP と SNTP は同時に設定できません。
- NTP モード 6 およびモード 7 のパケットは廃棄します。
- NTP ピアは，同一の接続先 IP アドレスに対して一つだけ接続できます。
- NTP ピアのコンフィグレーションを設定している端末とだけ，ピアで接続します。

10.2　時刻の設定

10.2.1　コンフィグレーションコマンド・運用コマンド一覧

時刻設定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 10-1　コンフィグレーションコマンド一覧

コマンド名	説明
clock summer-time	サマータイムを設定します。
clock timezone	タイムゾーンを設定します。

時刻設定の運用コマンド一覧を次の表に示します。

表 10-2　運用コマンド一覧

コマンド名	説明
set clock	ローカルタイムの日付，時刻を設定，表示します。

10.2.2　システムクロックの設定

タイムゾーンが JST，UTC からのオフセットが+9 の日本時間を設定する例を次に示します。

[設定のポイント]

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 でタイムゾーンを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

   コミットモードが逐次コミットモードの場合は，save コマンドでスタートアップコンフィグレーションに保存します。手動コミットモードの場合は，commit コマンドでランニングコンフィグレーションに反映したあと，スタートアップコンフィグレーションに保存してください。

   そのあと，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 1303221530**

   Fri Mar 22 15:30:00 JST 2013

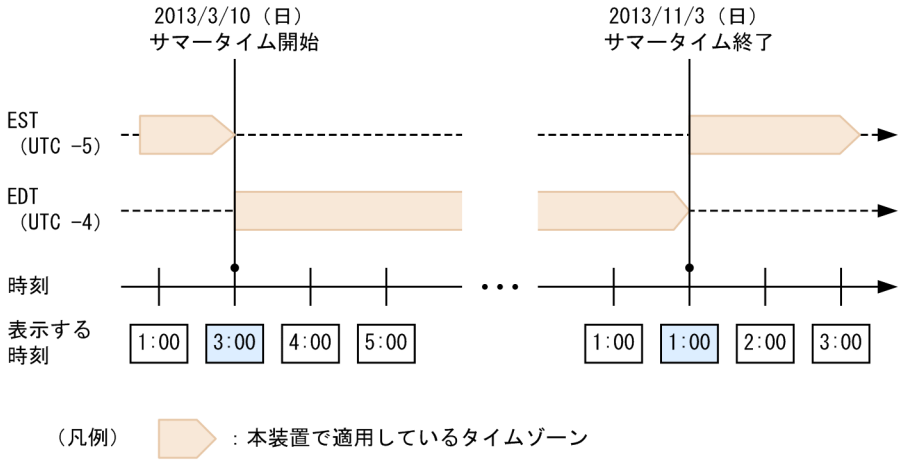
   JST での時間を 2013 年 3 月 22 日 15 時 30 分に設定します。

10.2.3　サマータイムの設定

タイムゾーンとして，標準時だけでなく，サマータイムも設定できます。サマータイムの設定では，サマータイムの適用期間と標準時からの時間差を指定できます。サマータイムへ切り替わる時刻は，コンフィグレーションコマンド clock timezone で指定された標準時を基準とします。

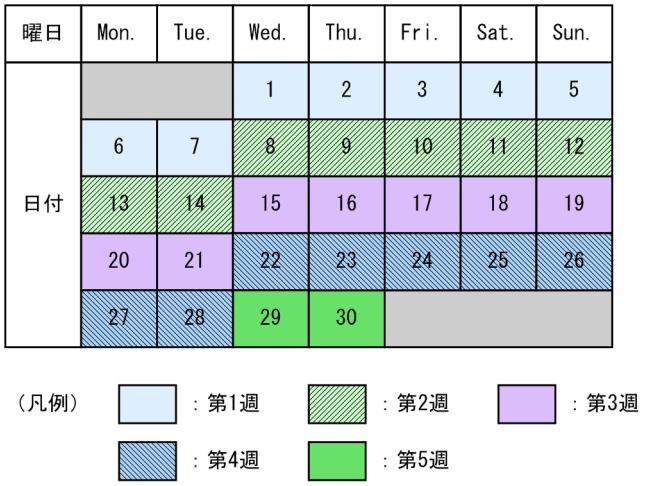
例えば，アメリカ東部標準時（EST）のタイムゾーンにアメリカ東部夏時間（EDT）を適用する場合，アメリカ東部夏時間の適用期間である 3 月第 2 日曜日午前 2 時から 11 月第 1 日曜日午前 2 時までを 1 時間差のサマータイムとして設定します。この場合，アメリカ東部標準時の 3 月第 2 日曜日午前 2 時にサマータイム開始として，時刻を 1 時間進めます。また，アメリカ東部夏時間の 11 月第 1 日曜日午前 2 時にサマータイム終了として，時刻を 1 時間戻します。サマータイムの適用例を次の図に示します。

図 10-1　サマータイムの適用例



なお，サマータイムを設定するとき，適用期間の開始および終了を週で指定します。そのため，実際の適用開始日および終了日は，指定月の最初の曜日によって決定します。例えば，最初の曜日が水曜で 30 日まである場合，週と日付の対応は次のようになります。

図 10-2　週と日付の対応（最初の曜日が水曜の場合）



この例では，第 1 週が 1 日～7 日，第 2 週が 8 日～14 日，第 3 週が 15 日～21 日，第 4 週が 22 日～28 日，第 5 週が 29 日～30 日となります。第 5 週を設定したときにその曜日が第 4 週までしか存在しない場合，第 4 週の指定した曜日でサマータイムが開始または終了します。

[設定のポイント]

サマータイムを設定する場合は，コンフィグレーションコマンド clock summer-time でタイムゾーンからのオフセットを設定する必要があります。

[コマンドによる設定]

1. **(config)# clock timezone EST -5**

   アメリカ東部標準時として，タイムゾーンに EST，UTC からのオフセットを-5 に設定します。

2. **(config)# clock summer-time EDT recurring 3 2 sun 0200 11 1 sun 0200 offset 60**

   アメリカ東部夏時間として，3 月第 2 日曜日午前 2 時から 11 月第 1 日曜日午前 2 時までの期間に EDT を設定します。サマータイム適用期間中は，EST から 60 分時刻を先に進めます。

3. **(config)# save**

   (config)# exit

   コミットモードが逐次コミットモードの場合は，save コマンドでスタートアップコンフィグレーションに保存します。手動コミットモードの場合は，commit コマンドでランニングコンフィグレーションに反映したあと，スタートアップコンフィグレーションに保存してください。

   そのあと，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。

4. **# show clock**

   Fri Mar 22 15:30:00 EDT 2013

   時刻を表示します。2013 年 3 月 22 日はサマータイム適用期間内のため，EST より時刻が 1 時間進みます。また，タイムゾーン名も EDT となります。

10.3　NTP のコンフィグレーション

10.3.1　コンフィグレーションコマンド一覧

NTP 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。

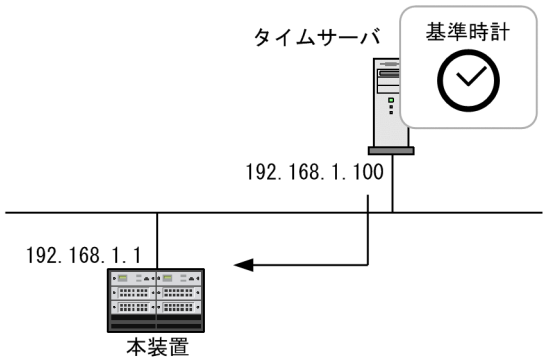
表 10-3　コンフィグレーションコマンド一覧

コマンド名	説明
ntp access-group	アクセスグループを作成して，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 認証機能を有効にします。
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 パケットを送信して，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の設定を指定します。
ntp peer	NTP サーバに，シンメトリック・アクティブ／パッシブモードを構成します。
ntp server	NTP サーバをクライアントモードに設定して，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。

10.3.2　NTP によるタイムサーバと時刻同期の設定

NTP 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）



[設定のポイント]

タイムサーバを複数設定した場合，本装置の同期先には ntp server コマンドで prefer パラメータを指定されたタイムサーバが選択されます。また，prefer パラメータが指定されなかった場合は，タイム

サーバの stratum 値が最も小さいタイムサーバが選択され，すべての stratum 値が同じ場合の同期先は任意となります。

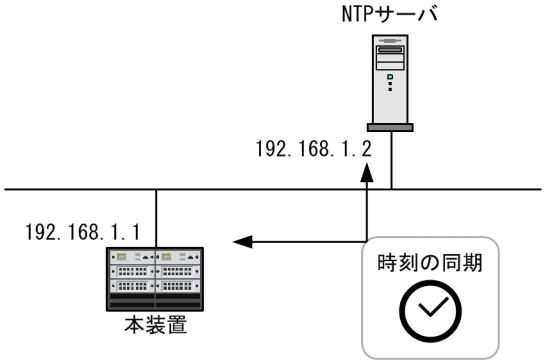
[コマンドによる設定]

1. **(config)# ntp server 192.168.1.100**
   IPv4 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。

10.3.3　NTP サーバとの時刻同期の設定

NTP を使用して，本装置の時刻と 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]

複数の NTP サーバと本装置を同期する場合には，ntp peer コマンドを使用して複数設定する必要があります。

NTP サーバを複数設定した場合，本装置の同期先には ntp peer コマンドで prefer パラメータを指定された NTP サーバが選択されます。また，prefer パラメータが指定されなかった場合は，NTP サーバの stratum 値が最も小さい NTP サーバが選択され，すべての stratum 値が同じ場合の同期先は任意となります。

[コマンドによる設定]

1. **(config)# ntp peer 192.168.1.2**
   IPv4 アドレス 192.168.1.2 の NTP サーバとの間を peer 関係として設定します。

10.3.4　NTP 認証の設定

[設定のポイント]

NTP でほかの装置と時刻を同期する場合に，セキュリティ目的の認証をします。

[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 NtP#001**
   NTP 認証鍵として，鍵番号 1 に「NtP#001」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。

10.3.5　VRF での NTP による時刻同期の設定

NTP を使用して，VRF に存在する NTP サーバや NTP クライアントに対して時刻を同期させる設定をします。

[設定のポイント]

NTP を使用して，本装置の時刻を任意の VRF に存在する NTP サーバに同期させます。また，本装置の時刻が NTP サーバに同期している場合，グローバルネットワークを含む全 VRF に存在する複数の NTP クライアントに本装置の時刻を配布できます。

同期の対象にする NTP サーバと NTP クライアントの VRF が異なる場合，NTP クライアントに対して，本装置の参照先ホストをローカルタイムサーバとして通知します。

[コマンドによる設定]

1. **(config)# ntp server vrf 10 192.168.1.100**

   VRF 10 に存在する IPv4 アドレス 192.168.1.100 の NTP サーバに，本装置の時刻を同期させます。構成はクライアントサーバモードです。

2. **(config)# ntp peer vrf 10 192.168.1.100**

   VRF 10 に存在する IPv4 アドレス 192.168.1.100 の NTP サーバと本装置の時刻を同期させます。構成はシンメトリック・アクティブ／パッシブモードです。

3. **(config)# ntp broadcast client**

   NTP ブロードキャストメッセージで本装置の時刻を同期させます。グローバルネットワークを含む全 VRF 上のサブネットを対象にして，NTP サーバからの NTP ブロードキャストメッセージを受信します。

4. **(config)# interface gigabitethernet 1/3**

   (config-if)# vrf forwarding 20

   (config-if)# ip address 192.168.10.1 255.255.255.0

   (config-if)# ntp broadcast

   VRF が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，VRF 20，IPv4 アドレス 192.168.10.0，サブネットマスク 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。

10.4　SNTP のコンフィグレーション

10.4.1　コンフィグレーションコマンド一覧

SNTP 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。

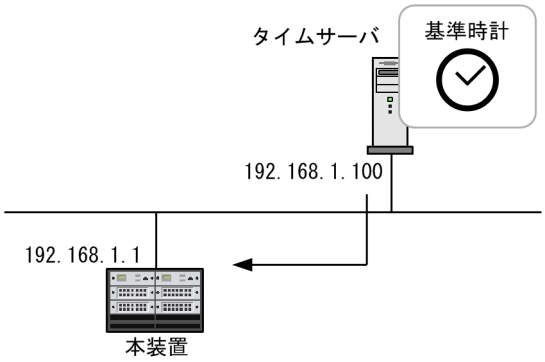
表 10-4　コンフィグレーションコマンド一覧

コマンド名	説明
sntp access-group	アクセスグループを作成して，アドレスフィルタによって SNTP サービスへのアクセスを許可または制限できます。
sntp authenticate	SNTP 認証機能を有効にします。
sntp authentication-key	認証鍵を設定します。
sntp broadcast	インタフェースごとにブロードキャストまたはマルチキャストで SNTP パケットを送信して，ほかの装置が本装置に同期するように設定します。
sntp broadcast client	接続したサブネット上の装置からの SNTP ブロードキャストメッセージまたはマルチキャストメッセージを受け付けるための設定をします。
sntp broadcastdelay	SNTP ブロードキャストサーバまたは SNTP マルチ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。
sntp broadcast send-interval	SNTP クライアントへブロードキャストまたはマルチキャストで時刻情報を配布するための送信間隔を設定します。
sntp client interval	SNTP サーバへ時刻情報を要求する間隔を設定します。
sntp master	ローカルタイムサーバの設定を指定します。
sntp server	SNTP サーバをクライアントモードに設定して，クライアントサーバモードを構成します。
sntp 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。

10.4.2　SNTP によるタイムサーバと時刻同期の設定

SNTP 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 10-5　SNTP 構成図（タイムサーバへの時刻の同期）



[コマンドによる設定]

1. **(config)# sntp server 192.168.1.100**
   IPv4 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。

10.4.3　SNTP 認証の設定

[設定のポイント]

SNTP でほかの装置と時刻を同期する場合に，セキュリティ目的の認証をします。

[コマンドによる設定]

1. **(config)# sntp authenticate**
   SNTP 認証機能を有効にします。
2. **(config)# sntp authentication-key 1 md5 SntP#001**
   SNTP 認証鍵として，鍵番号 1 に「SntP#001」を設定します。
3. **(config)# sntp trusted-key 1**
   SNTP 認証に使用する鍵番号 1 を指定します。

10.4.4　VRF での SNTP による時刻同期の設定

SNTP を使用して，VRF に存在する SNTP サーバや SNTP クライアントに対して時刻を同期させる設定をします。

[設定のポイント]

SNTP を使用して，本装置の時刻を任意の VRF に存在する SNTP サーバに同期させます。また，本装置の時刻が SNTP サーバに同期している場合，グローバルネットワークを含む全 VRF に存在する複数の SNTP クライアントに本装置の時刻を配布できます。

同期の対象にする SNTP サーバと SNTP クライアントの VRF が異なる場合, SNTP クライアントに対して，本装置の参照先ホストをローカルタイムサーバとして通知します。

[コマンドによる設定]

1. **(config)# sntp server vrf 10 192.168.1.100**
   VRF 10 に存在する IPv4 アドレス 192.168.1.100 の SNTP サーバに，本装置の時刻を同期させます。構成はクライアントサーバモードです。
2. **(config)# sntp broadcast client**
   SNTP ブロードキャストメッセージで本装置の時刻を同期させます。グローバルネットワークを含む全 VRF 上のサブネットを対象にして，SNTP サーバからの SNTP ブロードキャストメッセージを受信します。
3. **(config)# interface gigabitethernet 1/4**
   (config-if)# vrf forwarding 20
   (config-if)# ip address 192.168.10.1 255.255.255.0
   (config-if)# sntp broadcast ip
   VRF が指定されたインタフェースに対して SNTP ブロードキャストの設定をします。本装置の時刻が SNTP サーバに同期すると, VRF 20, IPv4 アドレス 192.168.10.0, サブネットマスク 255.255.255.0 のネットワークに SNTP ブロードキャストパケットを送信します。

10.5　オペレーション

10.5.1　運用コマンド一覧

時刻の設定と NTP/SNTP の運用コマンド一覧を次の表に示します。

表 10-5　運用コマンド一覧

コマンド名	説明
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。
set clock sntp	SNTP サーバと手動で時刻を同期します。
show sntp status	接続されている SNTP サーバの動作状態を表示します。
restart sntp	ローカル SNTP サーバを再起動します。

10.5.2　時刻および NTP/SNTP の状態の確認

(1)　時刻の確認

本装置に設定されている時刻情報は，show clock コマンドで確認できます。次の図に例を示します。

図 10-6　時刻の確認

```
> show clock
Wed Mar 22 15:30:00 UTC 20XX
>
```

(2)　NTP の動作状態の確認

NTP を使用して，ネットワーク上の NTP サーバと時刻を同期している場合，show ntp associations コマンドで現在同期している NTP サーバとの動作状態を確認できます。次の図に例を示します。

図 10-7　NTP サーバの動作状態の確認

```
> show ntp associations
Date 20XX/05/01 12:00:00 UTC
  remote         refid      st t when poll reach   delay   offset    disp
==============================================================================
*timesvr    192.168.1.100    3 u    1   64  377     0.89   -2.827    0.27
>
```

(3)　SNTP の動作状態の確認

SNTP を使用して，ネットワーク上の SNTP サーバと時刻を同期している場合，show sntp status コマンドで現在同期している SNTP サーバとの動作状態を確認できます。次の図に例を示します。

図 10-8　SNTP サーバの動作状態の確認

```
> show sntp status
Date 20XX/05/01 12:00:00 UTC
Last SNTP Status
Current server: 192.168.1.100 VRF 30
Status:synchronize
Mode : Unicast, Lapsed time : 14(s), Offset : 1(s)
```

```
Poll interval: 16
Configured SNTP Status
 SNTP server 2001:db8::1 priority 50
 SNTP server 2001:db5::100 VRF 10 priority 20
*SNTP server 192.168.1.100 VRF 30 priority 10
 SNTP broadcast 192.168.2.255 VRF 20
>
```

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

11.1.1　概要

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 または 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 または 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 または 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 または ipv6 host で設定されているホスト名が優先されます。ip host および ipv6 host を使用して IPv4 と IPv6 で同じホスト名を設定した場合, IPv4 が優先されます。DNS リゾルバ機能で IPv4 と IPv6 が設定されたホスト名を問い合わせた場合，IPv6 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。

11.1.2　ホスト名と DNS に関する注意事項

本装置で DNS サーバの IP アドレスが正しく設定されていない場合，または DNS サーバで逆引き（IP アドレスからホスト名を検索）ができない場合，DNS サーバとの通信や逆引きができないことを検知するまでに時間が掛かります。この場合，本装置に telnet でリモート接続するときにログインプロンプトが表示されるまでの時間が長くなるなど，運用に影響を与えることがあります。

DNS サーバとの接続は，運用コマンド nslookup で確認できます。なお，逆引き機能は，コンフィグレーションコマンド no ip domain reverse-lookup で無効にできます。

11.2　コンフィグレーション

11.2.1　コンフィグレーションコマンド一覧

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:db8:10::100**

   IPv6 アドレス 2001:db8:10::100 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。なお，ネームサーバへは設定した順番で問い合わせます。

[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**
   ネームサーバとして 192.168.0.1 を設定します。ホスト名情報を参照する場合，最初にこのネームサーバへ問い合わせます。
3. **(config)# ip name-server 2001:db8::1**
   ネームサーバとして 2001:db8::1 を設定します。192.168.0.1 のネームサーバへ問い合わせができない場合，このネームサーバへ問い合わせます。
4. **(config)# ip name-server 192.168.0.2**
   ネームサーバとして 192.168.0.2 を設定します。192.168.0.1 および 2001:db8::1 のネームサーバへ問い合わせができない場合，このネームサーバへ問い合わせます。

(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，本装置の管理全般について説明します。

12.1　システム操作パネル

システム操作パネルは BCU に実装されていて，装置情報や動作指示，障害情報を表示できます。

システム操作パネルは，［BACK］キー（ ◀ ），［ENTR］キー（■），［FWRD］キー（ ▶ ）の三つの操作キーと 16 桁×2 行の LCD を持ちます。システム操作パネルは，装置に発生した障害情報を表示する機能のほかに，システム操作パネルのキーを操作して階層構造のメニューをたどることで，装置情報や動作指示，障害情報を表示できます。

システム操作パネルの基本操作は，［BACK］キーおよび［FWRD］キーで項目を選択して，［ENTR］キーで決定します。例えば，ボードの inactivate 処理をしたい場合には，<Main Menu>で「Action」を選択して［ENTR］キーを押して，続いて<ACTION>で「INACT」を選択して［ENTR］キーを押します。

システム操作パネルのキーを操作すると，ディスプレイを点灯します。また，障害情報が表示されるときは自動でディスプレイを点灯します。障害情報が表示されていない場合に 60 秒間キーを操作しないと，ディスプレイを消灯します。

12.1.1　スタートアップメッセージ

(1)　POST メッセージ

本装置は，起動時に BCU で自己診断テスト（ハードウェアの診断）を実施します。このとき，LCD に装置の初期診断の経過を示す POST（Power On Self Test）メッセージを表示します。

図 12-1　POST メッセージの表示例

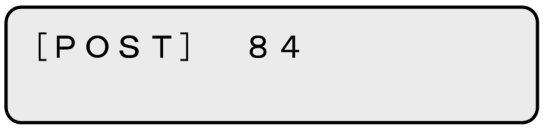


表 12-1　POST メッセージの表示内容

表示位置	表示内容
上段	POST コード
下段	（空行）

(2)　BOOT メッセージ

BCU で自己診断テストが完了すると，装置を起動します。このとき，LCD に装置の起動状態を示すメッセージを表示します。

図 12-2　BOOT メッセージの表示例



表 12-2　BOOT メッセージの表示内容

表示位置	表示内容
上段	BOOT 状態メッセージ
下段	（空行）

(3)　停止メッセージ

起動時の初期診断で異常を検出したり BCU 障害が発生したりした場合，およびユーザがコマンドで BCU を停止した場合，LCD に装置の停止状態を示すメッセージを表示します。

図 12-3　停止メッセージの表示例



表 12-3　停止メッセージの表示内容

表示位置	表示内容
上段	停止状態メッセージ（前半）
下段	停止状態メッセージ（後半） 表示されないこともあります。

(4)　アイドル状態

装置の起動が完了すると，LCD に装置の型名とソフトウェアバージョンを表示します。この状態をアイドル状態といいます。

図 12-4　アイドル状態の表示例

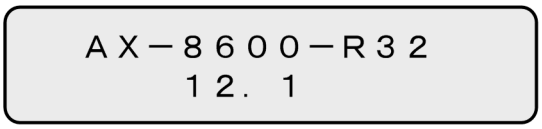


表 12-4　アイドル状態の表示内容

表示位置	表示内容
上段	装置の型名
下段	ソフトウェアバージョン

コンフィグレーションコマンド hostname で識別名称が設定されている場合，装置の型名とソフトウェアバージョンを 5 秒間表示したあと，LCD の下段に装置の識別名称を表示します。

図 12-5　装置の識別名称の表示例



表 12-5　装置の識別名称の表示内容

表示位置	表示内容
上段	（空行）
下段	装置の識別名称 17 文字以上の場合は，左に 1 文字ずつスクロールしながら表示します。最後まで表示すると，先頭から表示を繰り返します。

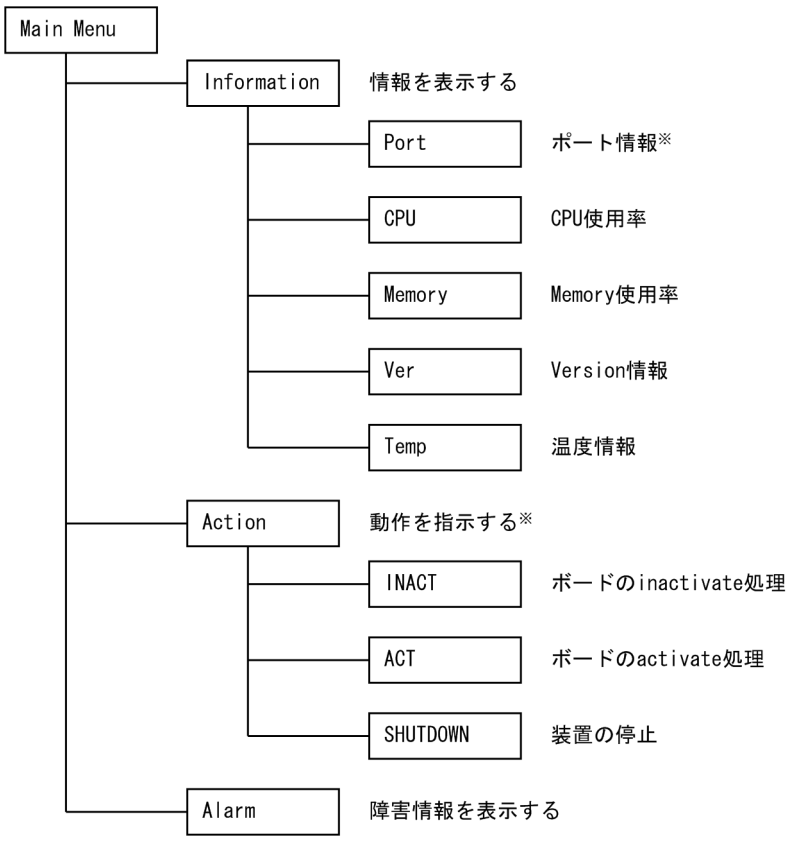
12.1.2　メニュー構造

<Main Menu>以下のメニュー構造を次の図に示します。

上位のメニューに戻るには，［BACK］キーおよび［FWRD］キーで「↑」を選択して［ENTR］キーを押してください。<Main Menu>へ戻るには，［BACK］キーおよび［FWRD］キーで「×」を選択して［ENTR］キーを押してください。また，キーを操作しないで一定時間が経過しても，<Main Menu>へ戻ります。

<Main Menu>を表示してから 30 秒間キーを操作しないと，アイドル状態の表示になります。

図 12-6　メニュー構造



注※　待機系 BCU では操作できません。

なお，待機系 BCU で操作できないメニューを選択した場合，“not supported on standby system”と 3 秒間表示したあと，自動的に<Main Menu>へ戻ります。

図 12-7　待機系 BCU で操作できないメニューを選択した場合の表示



12.1.3　ポート情報の表示

ポートの情報表示では，選択したポート番号のインタフェースの状態を表示します。<INFORMATION>で「Port」を選択して［ENTR］キーを押すと，NIF 番号選択画面を表示します。

Active 状態の NIF がない場合，“No Active NIF”と 3 秒間表示したあと，自動的に<Main Menu>へ戻ります。

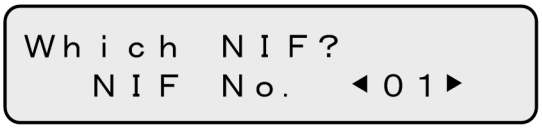
図 12-8　Active 状態の NIF がない場合の表示



(1)　NIF 番号選択

表示するポートの NIF 番号を選択する画面で［FWRD］キーを押すと，選択できる NIF 番号を昇順に表示します。NIF が active 状態でない場合，その NIF 番号の表示はスキップします。[BACK］キーでは［FWRD] キーと逆の順序で NIF 番号を表示します。情報を表示したい NIF 番号を選択して [ENTR] キーで決定すると，ポート情報を表示します。

図 12-9　NIF 番号選択の表示例



(2)　ポート情報表示

ポート情報の表示では，物理インタフェースの状態を表示します。[FWRD］キーを押すと，次のポートの情報を表示します。[BACK] キーでは，逆順となります。Active 状態の NIF が複数ある場合は，[FWRD］キーおよび［BACK］キーで NIF をまたいでポート情報を表示することもできます。

［ENTR］キーを押すと<Main Menu>へ戻ります。また，30 秒間キーを操作しないと自動的に<Main Menu>へ戻ります。

図 12-10　ポート情報の表示例



表 12-6　ポート情報の表示内容

分類	名称	意味
ポート位置	<nif no.>/<port no.>	<nif no.>：NIF 番号 <port no.>：ポート番号
ポート状態	active up	運用中（正常動作中）
	active down	運用中（回線障害発生中）
	initialize	初期化中またはネゴシエーション確立待ち
	fault	障害中
	inactive	次の要因による運用停止状態 • 運用コマンド • ネットワーク監視またはネットワーク管理の機能が動作した 詳細は，運用コマンド show interfaces の表示項目「ポート状態」を参照してください。
	disable	コンフィグレーションコマンドによる運用停止状態
	standby	リンクアグリゲーションのスタンバイリンク機能による運用待機状態
	suspend	次の要因でポートの起動を抑止している状態 • SFU の運用枚数不足 • PRU 初期化中 • NIF が運用系として稼働中以外
	unused	未使用（コンフィグレーション未設定）
	mismatch	搭載されている NIF とコンフィグレーションが不一致
回線速度	回線速度については，運用コマンド show port の表示項目「Speed」を参照してください。	
全二重／半二重	全二重／半二重については，運用コマンド show port の表示項目「Duplex」を参照してください。	

12.1.4　CPU 使用率の表示

BCU-CPU，PA，および PRU-CPU の CPU 使用率を表示します。<INFORMATION>で「CPU」を選択して［ENTR］キーを押すと，CPU の使用率を表示します。

(1)　CPU 種別選択

CPU 使用率の表示中に［FWRD］キーを押すと，CPU 種別を BCU-CPU，PA，PRU-CPU（PRU 番号）の順に表示します。［BACK］キーでは［FWRD］キーと逆の順序で CPU 種別を表示します。

(2)　CPU 使用率

CPU 使用率を 2%刻みの横棒グラフで表示します。表示は 5 秒ごとに最新の状況に更新します。

［ENTR］キーを押すと<Main Menu>へ戻ります。また，1 時間キーを操作しないと自動的に<Main Menu>へ戻ります。

図 12-11　CPU 使用率の表示例

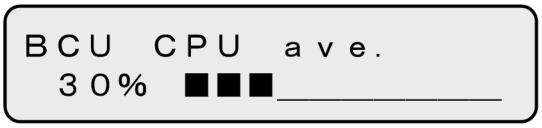


表 12-7　CPU 使用率の表示内容

表示項目	表示内容
BCU CPU ave.	BCU-CPU の CPU 使用率を 1 秒間で集計した平均値（%） 自系の情報を表示します。
PA ave.	PA の CPU 使用率を 1 秒間で集計した平均値（%） 自系の情報を表示します。
PRU<pru no.> CPU ave.	PRU-CPU の CPU 使用率を 1 秒間で集計した平均値（%） <pru no.>：PRU 番号

CPU 使用率の表示時に，PRU の起動が完了していない場合や CPU 使用率の最初の計測がまだ完了していない場合には，下段に「Initialize」を表示します。また，PRU の動作状態が運用中以外の場合には，下段に PRU の動作状態を表示します。

CPU 使用率を取得できなかった場合，数値を表示しません。次回の更新契機で再取得します。

図 12-12　CPU 使用率取得失敗時の表示



12.1.5　メモリ使用率の表示

BCU-CPU，PA，および PRU-CPU のメモリ使用率を表示します。<INFORMATION>で「Memory」を選択して［ENTR］キーを押すと，メモリの使用率を表示します。

(1)　CPU 種別選択

メモリ使用率の表示中に［FWRD］キーを押すと，CPU 種別を BCU-CPU，PA，PRU-CPU（PRU 番号）の順に表示します。［BACK］キーでは［FWRD］キーと逆の順序で CPU 種別を表示します。

(2)　メモリ使用率

メモリ使用率を 2%刻みの横棒グラフで表示します。表示は 5 秒ごとに最新の状況に更新します。BCU-CPU および PRU-CPU のメモリ使用率の表示では，CPU 種別（上段）はスクロールして表示します。

［ENTR］キーを押すと<Main Menu>へ戻ります。また，1 時間キーを操作しないと自動的に<Main Menu>へ戻ります。

図 12-13　メモリ使用率の表示例

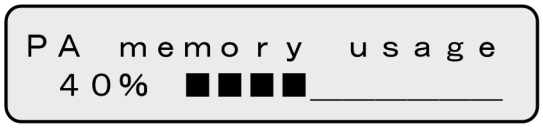


表 12-8　メモリ使用率の表示内容

表示項目	表示内容
BCU memory usage	BCU-CPU の実装メモリの使用率（%） 自系の情報を表示します。
PA memory usage	PA の実装メモリの使用率（%） 自系の情報を表示します。
PRU<pru no.> memory usage	PRU-CPU の実装メモリの使用率（%） <pru no.>：PRU 番号

メモリ使用率の表示時に，PRU の動作状態が運用中以外の場合には，下段に PRU の動作状態を表示します。

12.1.6　バージョンの表示

本装置に組み込まれているソフトウェアと搭載されているボードの情報（型名，シリアル情報，および稼働時間）を表示します。<INFORMATION>で「Ver」を選択して［ENTR］キーを押すと，バージョンを表示します。

(1)　表示対象選択

バージョン表示中に [FWRD] キーを押すと, 次の順で表示対象を表示します。[BACK] キーでは [FWRD] キーと逆の順序で表示対象を表示します。

1. モデル
2. ソフトウェア
3. BCU（BCU 番号）
4. SFU（SFU 番号）
5. PRU（PRU 番号）
6. NIF（NIF 番号）
7. 電源機構（電源機構のスロット番号）
8. ファンユニット（ファンユニットのスロット番号）

待機系 BCU では，4.SFU～8.ファンユニットの表示をスキップします。

(2)　バージョン表示

表示対象を選択すると，最初に型名表示をします。この状態で［ENTR］キーを押すと，表示をシリアル情報表示，稼働時間表示の順に切り替えます。型名，シリアル情報，または稼働時間を表示しているときに［FWRD］キーを押すと，次の表示対象の型名表示に切り替わります。［BACK］キーでは［FWRD］キーと逆の順序で表示します。

稼働時間表示（表示対象がモデルとソフトウェアの場合はシリアル情報表示）のときに［ENTR］キーを押すと，<Main Menu>へ戻ります。また，30 秒間キーを操作しないと自動的に<Main Menu>へ戻ります。

表 12-9　バージョン表示の表示項目一覧

表示対象	型名表示	シリアル情報表示	稼働時間表示
モデル	装置の型名	装置のシリアル情報	－
ソフトウェア	ソフトウェア型名	ソフトウェアバージョン	－
ボード	BCU の型名	BCU のシリアル情報	BCU の稼働時間
	SFU の型名	SFU のシリアル情報	SFU の稼働時間
	PRU の型名	PRU のシリアル情報	PRU の稼働時間
	NIF の型名	NIF のシリアル情報	NIF の稼働時間
電源機構	電源機構の型名	電源機構のシリアル情報	電源機構の稼働時間
ファンユニット	ファンユニットの型名	ファンユニットのシリアル情報	ファンユニットの稼働時間

（凡例）－：該当なし

(a)　型名表示

図 12-14　モデルの表示例

```
ＭＯＤＥＬ
　ＡＸ－８６００－Ｒ３２
```

表 12-10　モデルの表示内容

表示位置	表示内容
上段	「MODEL」固定
下段	装置の型名

図 12-15　ソフトウェア型名の表示例

```
ＯＳ－ＲＥ
　ＡＸ－Ｐ８６００－Ｒ２
```

表 12-11　ソフトウェア型名の表示内容

表示位置	表示内容
上段	ソフトウェア略称
下段	ソフトウェア型名 自系の情報を表示します。

図 12-16　ボード型名の表示例（NIF）

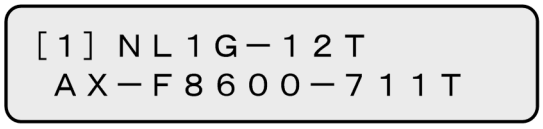


表 12-12　ボード型名の表示内容

表示位置	表示内容
上段	［ボードの搭載スロット番号］＋ボード略称 下段にボードの動作状態が表示されているときは，ボード略称は表示されません。
下段	ボード型名※

注※　ボード/電源機構/ファンユニットの動作状態によって，型名表示で表示する内容が異なります。動作状態ごとの型名表示条件を次の表に示します。

表 12-13　ボード/電源機構/ファンユニットの動作状態ごとの型名表示条件

ボード/電源機構/ファンユニットの動作状態	BCU	SFU	PRU	NIF	電源機構	ファンユニット
active	○	○	○	○	○	○
standby	○	－	－	－	－	－
initialize	○	○	○	○	－	－
disable（ボードが搭載）	－	○	○	○	－	－
disable（ボードが未搭載）	－	×	×	×	－	－
inactive	○	○	○	○	－	－
notconnect	×	×	×	×	×	×
fault	○	○	○	○	○※	○※
power shortage	－	－	○	○	－	－
notsupport	×	×	×	×	×	×
connect	－	－	－	－	×	－
unknown	－	×	×	×	－	－

（凡例）　○：ボード型名を表示　×：ボード/電源機構/ファンユニットの動作状態を表示　－：該当なし

注※　ハードウェア障害のときは，型名および略称が取得できないことがあります。

(b)　シリアル情報表示

図 12-17　ソフトウェアバージョンの表示例

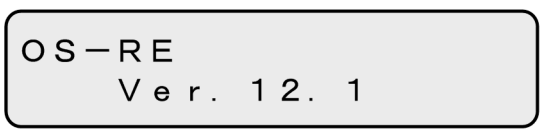


表 12-14　ソフトウェアバージョンの表示内容

表示位置	表示内容
上段	ソフトウェア略称
下段	ソフトウェアバージョン 自系の情報を表示します。

図 12-18　シリアル情報の表示例

```
ＳＩ
＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊
```

表 12-15　シリアル情報の表示内容

表示位置	表示内容
上段	「SI」固定
下段	シリアル情報※ 左に 1 文字ずつスクロールしながら表示します。最後まで表示すると，先頭から表示を繰り返します。

注※　ボード/電源機構/ファンユニットの動作状態によって，シリアル情報表示で表示する内容が異なります。動作状態ごとのシリアル情報表示条件を次の表に示します。

表 12-16　ボード/電源機構/ファンユニットの動作状態ごとのシリアル情報表示条件

ボード/電源機構/ファンユニットの動作状態	BCU	SFU	PRU	NIF	電源機構	ファンユニット
active	○	○	○	○	○	○
standby	○	－	－	－	－	－
initialize	○	○	○	○	－	－
disable（ボードが搭載）	－	○	○	○	－	－
disable（ボードが未搭載）	－	×	×	×	－	－
inactive	○	○	○	○	－	－
notconnect	×	×	×	×	×	×
fault	○	○	○	○	○※	○※
power shortage	－	－	○	○	－	－
notsupport	○	○	○	○	○	○
connect	－	－	－	－	×	－
unknown	－	×	×	×	－	－

（凡例）　○：シリアル情報を表示　×：ボード/電源機構/ファンユニットの動作状態を表示　－：該当なし

注※　ハードウェア障害のときは，シリアル情報が取得できないことがあります。

(c)　稼働時間表示

稼働時間表示では，稼働時間の合計である「Runtime Total」と，入気温度が高温注意状態での稼働時間の合計である「Runtime Caution」を，5 秒ごとに切り替えて表示します。

図 12-19　稼働時間の表示例



表 12-17　稼働時間の表示内容

表示位置	表示内容
上段	「Runtime Total」：稼働時間の累計 「Runtime Caution」：入気温度が高温注意状態での稼働時間の累計
下段	上段が意味する稼働時間（days：日数，hours：時間）※

注※　ボード/電源機構/ファンユニットの動作状態によって，稼働時間表示で表示する内容が異なります。動作状態ごとの稼働時間表示条件を次の表に示します。

表 12-18　ボード/電源機構/ファンユニットの動作状態ごとの稼働時間表示条件

ボード/電源機構/ファンユニットの動作状態	BCU	SFU	PRU	NIF	電源機構	ファンユニット
active	○	○	○	○	○	○
standby	○	−	−	−	−	−
initialize	○	×	×	×	−	−
disable（ボードが搭載）	−	×	×	×	−	−
disable（ボードが未搭載）	−	×	×	×	−	−
inactive	×	×	×	×	−	−
notconnect	×	×	×	×	×	×
fault	×	×	×	×	×	×
power shortage	−	−	×	×	−	−
notsupport	×	×	×	×	×	×
connect	−	−	−	−	×	−
unknown	−	×	×	×	−	−

（凡例）　○：稼働時間を表示　×：ボード/電源機構/ファンユニットの動作状態を表示　−：該当なし

12.1.7　温度情報の表示

BCU の入気温度情報を表示します。<INFORMATION>で「Temp」を選択して［ENTR］キーを押すと，温度情報を表示します。

(1)　温度表示

BCU の入気温度（摂氏）および温度のステータスを表示します。[FWRD] キーおよび [BACK] キーを押しても，表示内容は変わりません。

[ENTR] キーを押すと<Main Menu>へ戻ります。また，30 秒間キーを操作しないと自動的に<Main Menu>へ戻ります。

図 12-20　温度情報の表示例



表 12-19　温度情報の表示内容

表示位置	表示内容
上段	「Temp」固定
下段	温度のステータス※ • Normal：正常 • Caution：高温注意または低温注意 • Critical：高温警告 • Fault：高温停止 自系の情報を表示します。
	BCU 入気温度（摂氏）

注※　温度のステータスについては，「12.3.6　温度監視」を参照してください。

12.1.8　ボードの交換

電源を ON にしたまま，システム操作パネルからボードの交換を指示できます。交換できるボードは，次のとおりです。

- 待機系 BCU
- SFU
- PRU
- NIF

電源を ON にしたまま，各ボードを交換する手順の概略を次に示します。

1. システム操作パネルから「INACT」を選択および実行して，ボードを inactive 状態にする
2. 1.で inactive 状態にしたボードの取り外し
3. 交換用ボードの取り付け
4. システム操作パネルから「ACT」を選択および実行して，ボードを active 状態にする

ボード交換の詳細な手順は，「ハードウェア取扱説明書」を参照してください。

(1)　inactivate/activate 対象ボードの選択

ボードを inactive 状態にする場合

<ACTION>で「INACT」を選択して［ENTR］キーを押すと，inactive 状態にするボードの選択画面を表示します。

ボードを active 状態にする場合

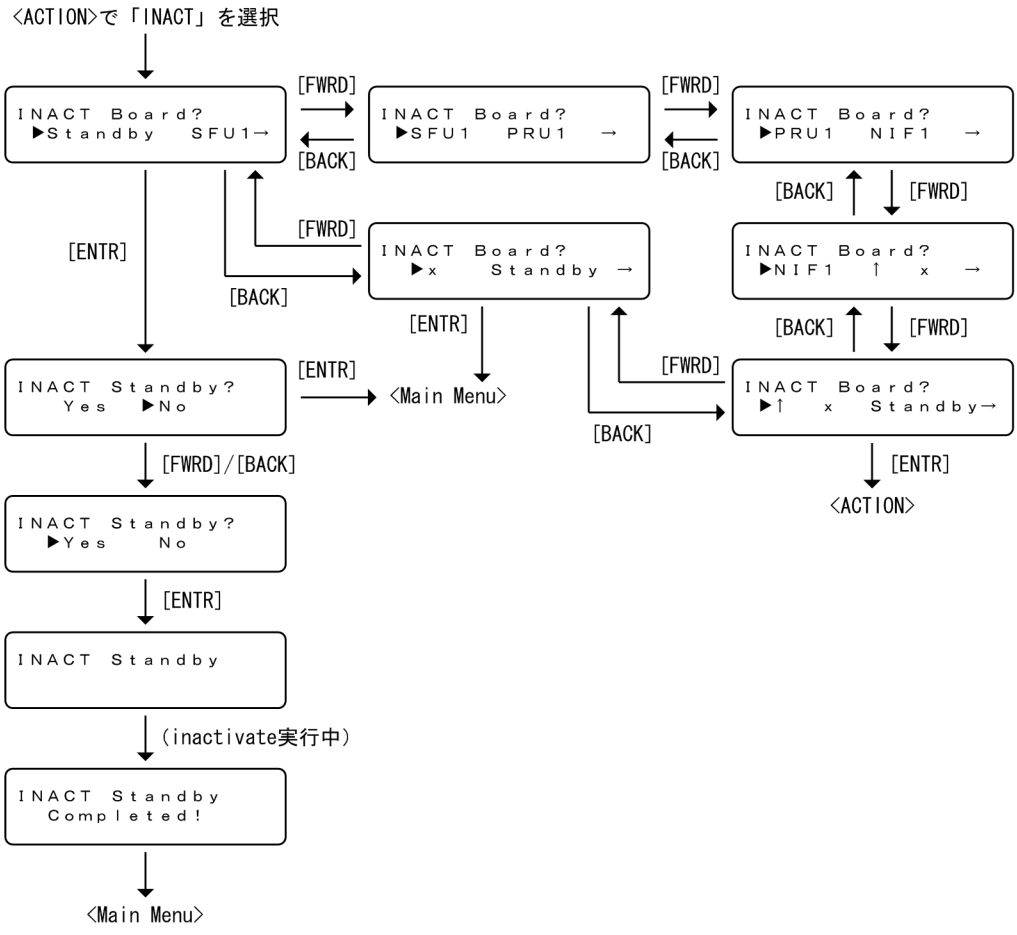
<ACTION>で「ACT」を選択して［ENTR］キーを押すと，active 状態にするボードの選択画面を表示します。

(2)　ほかの情報表示の抑制

ボードの交換の動作を指示している間は，障害情報は表示しません。

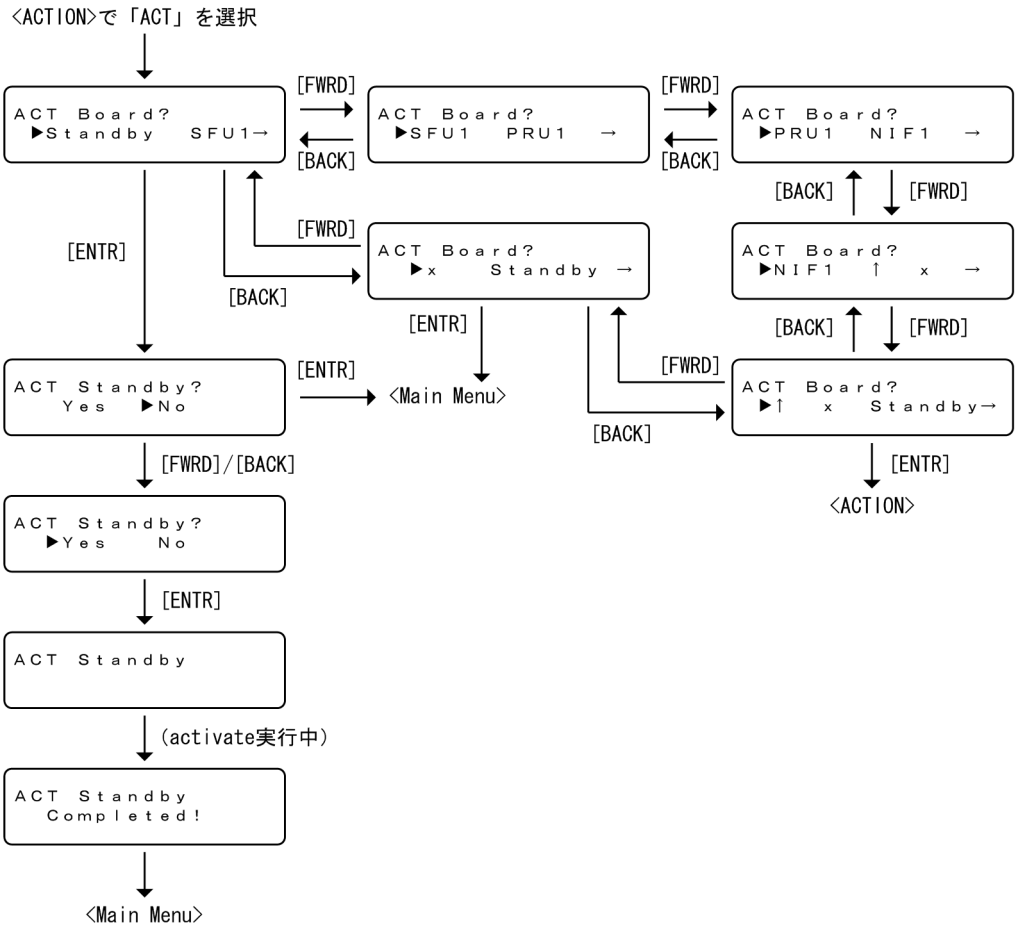
(3)　inactivate の操作

図 12-21　inactivate の操作手順



(4)　activate の操作

図 12-22　activate の操作手順



(5)　inactivate/activate 対象ボードが存在しない場合の表示

<ACTION>で「INACT」を選択したときに inactivate できるボードが存在しない場合，“No Active Board”と 3 秒間表示したあと，自動的に<Main Menu>へ戻ります。

図 12-23　inactivate 対象のボードが存在しない場合の表示



<ACTION>で「ACT」を選択したときに activate できるボードが存在しない場合，“No Inactive Board”と 3 秒間表示したあと，自動的に<Main Menu>へ戻ります。

図 12-24　activate 対象のボードが存在しない場合の表示



12.1.9　装置の停止

システム操作パネルから装置の停止を指示できます。システム操作パネルから装置を停止した場合, 装置を再度起動するには，電源スイッチを一度 OFF にしてから ON にしてください。

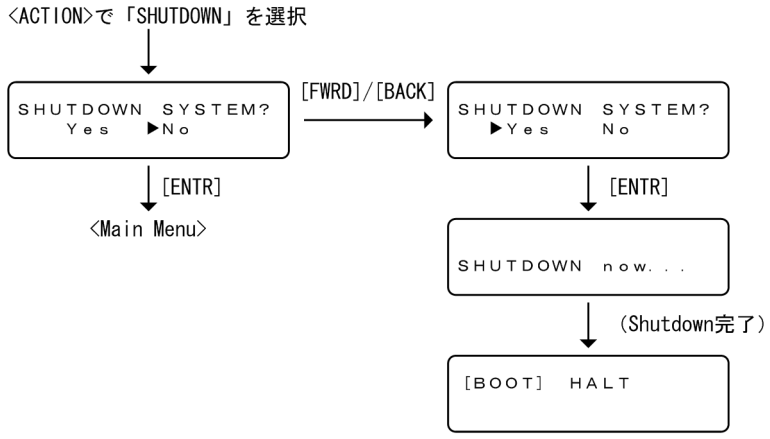
<ACTION>で「SHUTDOWN」を選択して［ENTR］キーを押すと，装置の停止の確認画面を表示します。

(1)　ほかの情報表示の抑制

装置の停止の動作を指示している間は，障害情報は表示しません。

(2)　装置の停止の操作

図 12-25　装置の停止の操作手順



12.1.10　障害の表示

装置内で故障が発生した場合，および装置内で故障が発生中に<Main Menu>から「Alarm」を選択した場合，故障部位または機能の切り分けを行うためにシステム操作パネルに障害を表示します。BCU 上の SYSTEM1 LED が赤点灯している場合は，装置障害が発生していることを示す障害表示をします。また，SYSTEM1 LED が緑点滅している場合は，装置の部分障害が発生していることを示す障害表示をします。

障害表示では，出力されたシステムメッセージのうち，対処が必要な障害（イベントレベルが S1～S4）を表示します。このとき，イベントレベルの数値が小さい障害を優先的に表示します。

障害個所がすべて回復すると，障害表示は自動的に消えて SYSTEM1 LED が緑点灯に戻ります。

(1)　障害表示

障害が発生すると, ディスプレイを点灯してイベントレベルとともにメッセージ種別とメッセージ識別子を表示します。［ENTR］キーを押すと，その障害のメッセージテキストを表示します。再度［ENTR］キーを押すと，<Main Menu>を表示します。メッセージテキストは，画面左側に移動しながら繰り返し表示されます。

図 12-26　障害の表示例（NIF でハードウェア障害を検出した例）



表 12-20　メッセージ識別子の表示内容

表示位置	表示内容
上段	[Sx]：イベントレベル（x：イベントレベルの数値）
	メッセージ種別
下段	メッセージ識別子

表 12-21　メッセージテキストの表示内容

表示位置	表示内容
上段	[Sx]：イベントレベル（x：イベントレベルの数値）
	メッセージ種別の詳細情報
下段	メッセージテキスト 17 文字以上の場合は，左に 1 文字ずつスクロールしながら表示します。最後まで表示すると，先頭から表示を繰り返します。

(2)　障害表示中のメニューの表示

障害表示中，装置情報の表示や動作指示をするために<Main Menu>を表示するには，メッセージ識別子表示の場合は［ENTR］キーを 2 回，メッセージテキスト表示の場合は［ENTR］キーを 1 回押します。

次の場合，メニュー表示から障害表示へ戻ります。

- 動作指示以外の状態で，障害が発生した場合
- <Main Menu>で 10 秒間経った状態で，障害が回復していない場合
- <Main Menu>から「Alarm」が選択された場合

(3)　ほかの情報表示との関係

ほかの情報を表示している場合でも，障害が発生すると障害を優先して表示します。ただし，動作指示をしている場合は，障害が発生しても障害を表示しません。動作指示が終了したあと，障害を表示します。

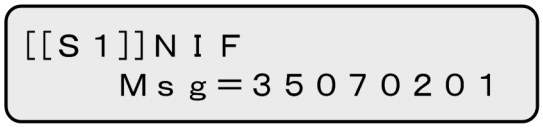
(4)　多重障害時の障害表示

障害が一つだけ発生している場合はイベントレベルを [] で囲んで表示しますが，多重障害が発生している場合は，イベントレベルを［[]］で囲んで表示します。

多重障害時には，［FWRD］キーまたは［BACK］キーを押すごとに，表示モードを維持しながらイベントレベルの数値が小さい順（同一の場合は障害発生順）に切り替えて表示します。例えば，メッセージ識別子を表示している場合はほかのメッセージ識別子を表示して，メッセージテキストを表示している場合はほかのメッセージテキストを表示します。表示中の障害表示が発生している障害の中でイベントレベルの数値

が最も小さい障害（同一の場合は最古の障害）ではない場合は，表示してから 30 秒後にイベントレベルの数値が最も小さい最古の障害表示に戻ります。

図 12-27　多重障害時の障害表示



(5)　障害未発生時の表示

<Main Menu>で「Alarm」を選択したときに障害が発生していない場合，“No Error”と 3 秒間表示したあと，自動的に<Main Menu>へ戻ります。

図 12-28　障害未発生時の表示



12.1.11　システム操作パネルの注意事項

システム操作パネルの操作時に表示内容の取得に失敗した場合，“Error occurred Cannot get data”と 3 秒間表示したあと，自動的に<Main Menu>へ戻ります。このメッセージが表示されたときは，もう一度同じ操作をしてください。

図 12-29　表示内容の取得失敗時の表示



12.2　装置のリソース設定

本装置では，装置の運用を開始する時に，どのハードウェアプロファイルで装置を運用するかを指定します。

経路系テーブルエントリやフロー系テーブルエントリは，使用するハードウェアプロファイルと，それぞれで指定した適用用途ごとの配分パターンによってエントリ数が決定します。これを固定配分と呼びます。

経路系テーブルエントリは，固定配分に加えて，使用するハードウェアプロファイルに応じたリソースの範囲で，適用用途ごとの配分パターンをさらにカスタマイズする方法があります。これをカスタマイズ配分と呼びます。

このように，ハードウェアプロファイルは本装置の基本的な動作条件を設定するものであるため，必ず運用を開始する前に設定してください。

12.2.1　コンフィグレーション・運用コマンド一覧

装置のリソース設定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 12-22　コンフィグレーションコマンド一覧

コマンド名	説明
flow-table allocation	装置のフロー系テーブルエントリ数の配分パターンを設定します。
forwarding-table allocation	装置の経路系テーブルエントリ数の配分パターンを設定します。
hardware profile	ハードウェアプロファイルを設定します。

装置のリソース設定に関する運用コマンド一覧を次の表に示します。

表 12-23　運用コマンド一覧

コマンド名	説明
show system	装置の運用状態および装置のハードウェアプロファイルを表示します。
show pru resources	PRU の運用状態およびリソース使用状況を表示します。

12.2.2　ハードウェアプロファイルの設定

本装置では，各種テーブルエントリをどのように使用して装置を運用するかをハードウェアプロファイルで指定します。

なお，コンフィグレーションの設定内容と稼働状態は，運用コマンド show system で確認できます。

[設定のポイント]

ハードウェアプロファイルの初期状態は router-1 です。設定したハードウェアプロファイルを反映するために，装置を再起動してください。

[コマンドによる設定]

1. **(config)# hardware profile router-1s**

グローバルコンフィグレーションモードで，ハードウェアプロファイルを router-1s に設定します。

12.2.3　経路系テーブル固定配分の設定

[設定のポイント]

経路系テーブルエントリの初期状態は default です。設定した経路系テーブルエントリの配分パターンを反映するために，すべての PRU を再起動してください。

[コマンドによる設定]

1. **(config)# forwarding-table allocation ipv4-uni**

   グローバルコンフィグレーションモードで，経路系テーブルエントリの配分パターンを IPv4 ユニキャスト優先に設定します。

12.2.4　フロー系テーブル固定配分の設定

[設定のポイント]

フロー系テーブルエントリの初期状態は default です。設定したフロー系テーブルエントリの配分パターンを反映するために，すべての PRU を再起動してください。

[コマンドによる設定]

1. **(config)# flow-table allocation filter**

   グローバルコンフィグレーションモードで，フロー系テーブルエントリの配分パターンをフィルタ重視に設定します。

12.2.5　経路系テーブルカスタマイズ配分の設定手順

本装置では，コンフィグレーションで経路系テーブルエントリ内の配分パターンをカスタマイズできます。本装置はカスタマイズ配分パターンを生成，調整，設定，および確認するための支援用高機能スクリプトを提供します。これらのスクリプトは，本装置にプリインストールされています。

支援用高機能スクリプトを使用して，カスタマイズ配分パターンを生成し，生成した配分情報を示すカスタマイズ配分用キー情報をコンフィグレーションに設定します。設定後，すべての PRU を再起動すると，カスタマイズ配分パターンが本装置へ反映されます。

(1)　カスタマイズ配分の設定の流れ

カスタマイズ配分の設定の流れを次に示します。

1. ハードウェアプロファイルの確認

   カスタマイズ配分では，ハードウェアプロファイルによって生成される配分パターンが異なります。カスタマイズ配分を適用するときは，装置に反映するハードウェアプロファイルで以降の手順を実施してください。

2. カスタマイズ配分の生成と調整

   支援用高機能スクリプトを使用して，ハードウェアへの反映可否を確認しつつ，エントリ種別ごとに適用する配分とカスタマイズ配分用キー情報を生成します。また，生成した配分を基に，特定のエントリ種別で配分の増減を調整できます。適用する配分については，スクリプト実行時にハードウェアに適用できる最適な値に補正されます。

   カスタマイズ配分用のスクリプトファイル/scripts/custom_route.pyc は，本装置にプリインストールされています。そのため，運用コマンド install script による装置へのインストールは不要です。なお，ファイルを本装置にインストールした場合，インストールしたファイルを起動します。

3. カスタマイズ配分のコンフィグレーション設定

   支援用高機能スクリプトを使用して，カスタマイズ配分をコンフィグレーションに設定します。コンフィグレーションには，カスタマイズ配分用キー情報だけが設定されます。

4. カスタマイズ配分の確認

   コンフィグレーションに設定されたカスタマイズ配分用キー情報は 32 文字の文字列です。支援用高機能スクリプトを使用してこのキー情報を変換すると，装置に適用されるテーブルエントリ数を確認できます。

5. カスタマイズ配分を運用へ反映

   固定配分の変更時と同様に，設定したカスタマイズ配分を反映するために，すべての PRU を再起動してください。各テーブルエントリ数に関する情報は，運用コマンド show pru resources で確認できます。

(2)　カスタマイズ配分支援用高機能スクリプト

カスタマイズ配分支援用高機能スクリプト一覧を次の表に示します。各スクリプトの入力形式やパラメータについては，「運用コマンドレファレンス Vol.1　21. カスタマイズ配分支援用高機能スクリプト」を参照してください。

表 12-24　カスタマイズ配分支援用高機能スクリプト一覧

高機能スクリプト	説明
python /scripts/custom_route.pyc make	カスタマイズ配分パターンを生成します。
python /scripts/custom_route.pyc remake	カスタマイズ配分パターンを調整します。
python /scripts/custom_route.pyc set	カスタマイズ配分パターンをコンフィグレーションに設定します。
python /scripts/custom_route.pyc show	カスタマイズ配分パターンを表示します。

12.2.6　カスタマイズ配分の生成

カスタマイズ配分の生成用スクリプトを使用して，カスタマイズ配分パターンを生成します。パラメータ不正の場合には usage を表示します。生成時の指定方法は次の 3 とおりです。

(1)　エントリ数指定

スクリプト実行時に，パラメータですべてのエントリ種別のエントリ数を指定して，カスタマイズ配分パターンを生成します。指定したエントリ数に基づいてハードウェアに適用できる最適な値に補正して，配分パターンを生成します。なお，エントリ数の設定範囲については，「3.2.1　テーブルエントリ数」を参照してください。エントリ数指定でのスクリプト実行例を次の図に示します。

図 12-30　カスタマイズ配分の生成（エントリ数指定）

```
# python /scripts/custom_route.pyc make 100 8 50 8 256 16              <-1
 1:AX8600R  2:AX8600S  3:AX8300S
 Specify the model : 1                                                <-2
 1:router-1  2:router-1s
 Specify the hardware profile : 2                                     <-3
    +-------------------------------------------------------------  ┐
    | KEY : 1002ff0004010400011001010000000                        |
    | Hardware profile : router-1s                                 |
    +----------------+--------------------+-------------------------+
    | Entry          | K entries(entries) | Unused K entries(entries)
    +----------------+--------------------+-------------------------+
    | IPv4 unicast   |   128 K ( 131072)  |  +1152 K (+1179648)     |  <-4
```

```
    | IPv4 multicast |     8 K (   8000)  |  +   0 K (+      0)         |
    | IPv6 unicast   |    64 K (  65536)  |  + 576 K (+ 589824)         |
    | IPv6 multicast |     8 K (   8000)  |  +   0 K (+      0)         |
    | MAC address    |   256 K ( 262144)  |  + 256 K (+ 262144)         |
    | ARP and NDP    |    32 K (  32000)  |  + 208 K (+ 208000)         |
    +-------------------------------------------------------------------+
#
```

1.カスタマイズ配分の生成用スクリプト（エントリ数指定）を実行します。

2.装置モデルを選択します。

スクリプト実行時にカスタマイズ配分用キー情報を指定した場合は表示されません。

3.ハードウェアプロファイルを選択します。

スクリプト実行時にカスタマイズ配分用キー情報を指定した場合は表示されません。

4.生成したカスタマイズ配分パターンが表示されます。

ハードウェアのリソースを超過した場合の実行例を次の図に示します。

図 12-31　カスタマイズ配分の生成（エントリ数指定かつリソース超過時）

```
# python /scripts/custom_route.pyc make 1000 8 500 8 256 16             <-1
 1:AX8600R  2:AX8600S  3:AX8300S
 Specify the model : 1
 1:router-1  2:router-1s
 Specify the hardware profile : 2
    +-------------------------------------------------------------------+
    | KEY : (error)
    | Hardware profile : router-1s
    +----------------+--------------------+--------------------------
    | Entry          | K entries(entries) | Unused K entries(entries)
    +----------------+--------------------+--------------------------
    | IPv4 unicast   |  1024 K (1048576)  |      - K (       -)       <-2
    | IPv6 unicast   |   512 K ( 524288)  |      - K (       -)
    | MAC address    |   256 K ( 262144)  |      - K (       -)
    | ARP and NDP    |    32 K (  32000)  |      - K (       -)
    +-------------------------------------------------------------------+
The number of input entries exceeded the capacity.
#
```

1.カスタマイズ配分の生成用スクリプト（エントリ数指定）を実行します。

2.装置全体のハードウェアのリソースを超過した旨のメッセージと入力情報が表示されます。

(2)　固定配分指定

固定配分パターンを基準としたカスタマイズ配分パターンを生成します。生成した固定配分相当のカスタマイズ配分パターンに対して，さらに配分パターンを調整できます。固定配分指定では，パラメータの指定は不要です。固定配分指定でのスクリプト実行例を次の図に示します。

図 12-32　カスタマイズ配分の生成（固定配分指定）

```
# python /scripts/custom_route.pyc make                                 <-1
 1:AX8600R  2:AX8600S  3:AX8300S
 Specify the model : 1                                                 <-2
 1:router-1  2:router-1s
 Specify the hardware profile : 2                                      <-3
 1:default
 Specify the forwarding-table allocation : 1                           <-4
    +-------------------------------------------------------------
    | KEY : 1002ff001f010a00010f050100000000
    | Hardware profile : router-1s
    +----------------+--------------------+--------------------------
    | Entry          | K entries(entries) | Unused K entries(entries)
    +----------------+--------------------+--------------------------
    | IPv4 unicast   |   992 K (1015808)  |  +   0 K (+      0)
```

```
    | IPv4 multicast |     8 K (   8000) |  +   0 K (+      0)
    | IPv6 unicast   |   160 K ( 163840) |  +   0 K (+      0)
    | IPv6 multicast |     8 K (   8000) |  +   0 K (+      0)
    | MAC address    |   240 K ( 245760) |  +   0 K (+      0)
    | ARP and NDP    |   240 K ( 240000) |  +   0 K (+      0)
    +-------------------------------------------------------------
#
```

1. カスタマイズ配分の生成用スクリプト（固定配分指定）を実行します。
2. 装置モデルを選択します。
3. ハードウェアプロファイルを選択します。
4. 経路系テーブルエントリパターンを選択します。
   選択した経路系テーブルエントリパターン相当のカスタマイズ配分パターンが生成されます。

(3)　キー情報指定

スクリプト実行時にカスタマイズ配分用キー情報を指定して，キー情報からカスタマイズ配分パターンを生成します。

カスタマイズ配分を適用後，装置や BCU を再起動したり，系切替をしたりすると，直前のスクリプト実行結果をリセットします。その場合，コンフィグレーションに設定されているカスタマイズ配分用キー情報からカスタマイズ配分パターンを生成すると，そのカスタマイズ配分に対して調整ができます。カスタマイズ配分パターンの表示フォーマットは「図 12-30　カスタマイズ配分の生成（エントリ数指定）」を参照してください。

12.2.7　カスタマイズ配分の調整

カスタマイズ配分の調整用スクリプトを使用して，直前に生成したカスタマイズ配分パターンをエントリ種別単位に調整できます。パラメータ不正の場合には usage を表示します。調整時の指定方法はエントリ種別ごとに次の 3 とおりです。

(1)　エントリ数指定

直前に生成したカスタマイズ配分パターンに対して，エントリ種別とエントリ数を指定して上書きします。カスタマイズ配分パターンを生成したあと，IPv4 ユニキャスト経路数だけを 500K（524288）に変更するスクリプト実行例を次の図に示します。

図 12-33　カスタマイズ配分の調整（エントリ数指定）

```
# python /scripts/custom_route.pyc make 100 8 50 8 256 16
 1:AX8600R  2:AX8600S  3:AX8300S
 Specify the model : 1
 1:router-1  2:router-1s
 Specify the hardware profile : 2
    +-------------------------------------------------------------
    | KEY : 1002ff000401040001100101000000000
    | Hardware profile : router-1s
    +---------------+--------------------+--------------------------
    | Entry         | K entries(entries) | Unused K entries(entries)
    +---------------+--------------------+--------------------------
    | IPv4 unicast  |   128 K ( 131072)  |  +1152 K (+1179648)      ┐
    | IPv4 multicast|     8 K (   8000)  |  +   0 K (+      0)      │
    | IPv6 unicast  |    64 K (  65536)  |  + 576 K (+ 589824)      │ <-1
    | IPv6 multicast|     8 K (   8000)  |  +   0 K (+      0)      │
    | MAC address   |   256 K ( 262144)  |  + 256 K (+ 262144)      │
    | ARP and NDP   |    32 K (  32000)  |  + 208 K (+ 208000)      ┘
    +-------------------------------------------------------------
# python /scripts/custom_route.pyc remake v4uc 500                  <-2
    +-------------------------------------------------------------
    | KEY : 1002ff001001040001100101000000000
    | Hardware profile : router-1s
```

```
    +----------------+--------------------+-------------------------
    | Entry          | K entries(entries) | Unused K entries(entries)
    +----------------+--------------------+-------------------------
    | IPv4 unicast   |   512 K ( 524288)  |  + 768 K (+ 786432)          <-3
    | IPv4 multicast |     8 K (   8000)  |  +   0 K (+      0)        ┐
    | IPv6 unicast   |    64 K (  65536)  |  + 384 K (+ 393216)        |
    | IPv6 multicast |     8 K (   8000)  |  +   0 K (+      0)        | <-4
    | MAC address    |   256 K ( 262144)  |  + 256 K (+ 262144)        |
    | ARP and NDP    |    32 K (  32000)  |  + 208 K (+ 208000)        ┘
    +-------------------------------------------------------------
#
```

1. 直前に生成したカスタマイズ配分パターンです。
2. カスタマイズ配分の調整用スクリプト（エントリ数指定）を実行します。
3. IPv4 ユニキャスト経路の「K entries(entries)」が 512K（524288）に変更されます。
4. IPv4 ユニキャスト経路以外の「K entries(entries)」は直前の生成結果から変更がありません。「Unused K entries(entries)」は，指定したパラメータによって変化します。

(2) 減少調整

直前に生成したカスタマイズ配分パターンに対して，エントリ種別を指定して最小単位でエントリ数を減少させます。減少調整の結果，最小値を下回る場合は変更されません。「(1) エントリ数指定」で調整したあとのカスタマイズ配分パターンから，IPv6 マルチキャスト経路数だけを減少するスクリプト実行例を次の図に示します。

図 12-34 カスタマイズ配分の調整（減少調整）

```
# python /scripts/custom_route.pyc remake -v6mc                        <-1
    +-------------------------------------------------------------
    | KEY : 1002ff0010010400001001010000000
    | Hardware profile : router-1s
    +----------------+--------------------+-------------------------
    | Entry          | K entries(entries) | Unused K entries(entries)
    +----------------+--------------------+-------------------------
    | IPv4 unicast   |   512 K ( 524288)  |  + 800 K (+ 819200)        ┐
    | IPv4 multicast |     8 K (   8000)  |  +   0 K (+      0)        | <-3
    | IPv6 unicast   |    64 K (  65536)  |  + 400 K (+ 409600)        ┘
    | IPv6 multicast |     0 K (      0)  |  +   8 K (+   8000)          <-2
    | MAC address    |   256 K ( 262144)  |  + 256 K (+ 262144)        ┐
    | ARP and NDP    |    32 K (  32000)  |  + 208 K (+ 208000)        ┘ <-3
    +-------------------------------------------------------------
#
```

1. カスタマイズ配分の調整用スクリプト（減少調整）を実行します。
2. IPv6 マルチキャスト経路の「K entries(entries)」が減少します。
3. IPv6 マルチキャスト経路以外の「K entries(entries)」は直前の調整結果から変更がありません。「Unused K entries(entries)」は，指定したパラメータによって変化します。

(3) 増加調整

直前に生成したカスタマイズ配分パターンに対して，エントリ種別を指定して最小単位でエントリ数を増加させます。増加調整の結果，最大値を上回る場合は変更されません。「(2) 減少調整」で調整したあとのカスタマイズ配分パターンから，ARP と NDP の合計だけを増加するスクリプト実行例を次の図に示します。

図 12-35 カスタマイズ配分の調整（増加調整）

```
# python /scripts/custom_route.pyc remake +arp                         <-1
    +-------------------------------------------------------------
    | KEY : 1002ff0010010400001002010000000
    | Hardware profile : router-1s
    +----------------+--------------------+-------------------------
    | Entry          | K entries(entries) | Unused K entries(entries)
```

```
    +---------------+-------------------+-------------------------
    | IPv4 unicast  |   512 K ( 524288) |  + 768 K (+ 786432)      ┐
    | IPv4 multicast|     8 K (   8000) |  +   0 K (+      0)      |
    | IPv6 unicast  |    64 K (  65536) |  + 384 K (+ 393216)      | <-3
    | IPv6 multicast|     0 K (      0) |  +   8 K (+   8000)      |
    | MAC address   |   256 K ( 262144) |  + 256 K (+ 262144)      ┘
    | ARP and NDP   |    96 K (  96000) |  + 144 K (+ 144000)        <-2
    +---------------+-------------------+-------------------------
#
```

1. カスタマイズ配分の調整用スクリプト（増加調整）を実行します。
2. ARP と NDP の合計の「K entries(entries)」が増加します。
3. ARP と NDP の合計以外の「K entries(entries)」は直前の調整結果から変更がありません。「Unused K entries(entries)」は，指定したパラメータによって変化します。

12.2.8　カスタマイズ配分のコンフィグレーション設定

これまでの手順で決定した配分パターンを，コンフィグレーションへ設定します。設定時の指定方法は次の3とおりです。

(1)　エントリ数指定

スクリプト実行時に，パラメータですべてのエントリ種別のエントリ数を指定して，カスタマイズ配分パターンをコンフィグレーションへ設定します。エントリ数指定でのスクリプト実行例を次の図に示します。

図 12-36　カスタマイズ配分のコンフィグレーション設定（エントリ数指定）

```
# python /scripts/custom_route.pyc set 512 8 64 0 256 96                <-1
 1:AX8600R  2:AX8600S  3:AX8300S
 Specify the model : 1                                                  <-2
 1:router-1  2:router-1s
 Specify the hardware profile : 2                                       <-3
    +-----------------------------------------------------------------
    | KEY : 1002ff0010010400001002010000000
    | Hardware profile : router-1s
    +---------------+-------------------+-------------------------
    | Entry         | K entries(entries) | Unused K entries(entries)
    +---------------+-------------------+-------------------------
    | IPv4 unicast  |   512 K ( 524288) |  + 768 K (+ 786432)
    | IPv4 multicast|     8 K (   8000) |  +   0 K (+      0)
    | IPv6 unicast  |    64 K (  65536) |  + 384 K (+ 393216)
    | IPv6 multicast|     0 K (      0) |  +   8 K (+   8000)
    | MAC address   |   256 K ( 262144) |  + 256 K (+ 262144)
    | ARP and NDP   |    96 K (  96000) |  + 144 K (+ 144000)
    +---------------+-------------------+-------------------------
Do you want to apply to the running configuration? (y/n): y             <-4
!#
2016/XX/XX 16:24:39 UTC 1-1(A) S6 CONFIG 3f000001 00 000000000000 A forwarding
 table allocation configuration was changed. Restart all the PRUs.      <-5
!#                                                                      <-6
```

1. カスタマイズ配分のコンフィグレーション設定用スクリプト（エントリ数指定）を実行します。
2. 装置モデルを選択します。これまでの手順で決定した装置モデルを選択してください。

   スクリプト実行時にカスタマイズ配分用キー情報を指定した場合や，パラメータを省略した場合は表示されません。
3. ハードウェアプロファイルを選択します。これまでの手順で決定したハードウェアプロファイルを選択してください。

   スクリプト実行時にカスタマイズ配分用キー情報を指定した場合や，パラメータを省略した場合は表示されません。

4. 表示されたカスタマイズ配分パターンを確認して，コンフィグレーションを変更する場合は「y」を入力します。
5. 正常にカスタマイズ配分のコンフィグレーションが設定された場合にこのシステムメッセージが表示されます。ただし，手動コミットモードの場合は，コンフィグレーションコマンド commit（commit running）を実行した契機で表示されます。
6. このスクリプトでは，コンフィグレーションコマンド save および commit を実行しません。そのため，必要に応じて別途実行してください。

(2)　キー情報指定

スクリプト実行時にカスタマイズ配分用キー情報を指定して，キー情報に基づくカスタマイズ配分パターンをコンフィグレーションへ設定します。カスタマイズ配分パターンの表示フォーマットは「図 12-36　カスタマイズ配分のコンフィグレーション設定（エントリ数指定）」を参照してください。

(3)　生成済みパターン指定

スクリプト実行時にパラメータを指定しないで，直前に生成したカスタマイズ配分パターンをコンフィグレーションへ設定します。カスタマイズ配分パターンの表示フォーマットは「図 12-36　カスタマイズ配分のコンフィグレーション設定（エントリ数指定）」を参照してください。

12.2.9　カスタマイズ配分の確認

カスタマイズ配分の確認用スクリプトを使用して，これまでの手順で生成した配分パターンを確認します。確認時の指定方法は次の 2 とおりです。

(1)　キー情報指定

スクリプト実行時にカスタマイズ配分用キー情報を指定して，キー情報に基づくカスタマイズ配分パターンを表示します。キー情報指定でのスクリプト実行例を次の図に示します。

図 12-37　カスタマイズ配分の確認（キー情報指定）

```
# python /scripts/custom_route.pyc show 1002ff0010010400001002010000000 <-1
    +-------------------------------------------------------------
    | KEY : 1002ff0010010400001002010000000
    | Hardware profile : router-1s                                  <-2
    +----------------+--------------------+--------------------------
    | Entry          | K entries(entries) | Unused K entries(entries)
    +----------------+--------------------+--------------------------
    | IPv4 unicast   |   512 K ( 524288)  |  + 768 K (+ 786432)      ┐
    | IPv4 multicast |     8 K (   8000)  |  +   0 K (+      0)      │
    | IPv6 unicast   |    64 K (  65536)  |  + 384 K (+ 393216)      │ <-2
    | IPv6 multicast |     0 K (      0)  |  +   8 K (+   8000)      │
    | MAC address    |   256 K ( 262144)  |  + 256 K (+ 262144)      │
    | ARP and NDP    |    96 K (  96000)  |  + 144 K (+ 144000)      ┘
    +-------------------------------------------------------------
#
```

1. カスタマイズ配分の確認用スクリプト（キー情報指定）を実行します。
2. 入力したキー情報に対応するハードウェアプロファイルと，PRU へ反映されるカスタマイズ配分パターンが表示されます。

(2)　生成済みパターン指定

スクリプト実行時にパラメータを指定しないで，直前に生成したカスタマイズ配分パターンを表示します。カスタマイズ配分パターンの表示フォーマットは「図 12-37　カスタマイズ配分の確認（キー情報指定）」を参照してください。

12.2.10　カスタマイズ配分使用時の注意事項

- コマンド承認を使用している場合は，コンフィグレーションコマンド aaa authorization commands script で bypass パラメータを指定して，スクリプトによるコマンド実行を許可してください。
- 運用しているハードウェアプロファイルとは異なるハードウェアプロファイルで生成および調整したカスタマイズ配分用キー情報をコンフィグレーションに設定した場合，システムメッセージ（メッセージ種別：CONFIG，メッセージ識別子：3f000015）が表示されます。この状態で PRU を再起動すると，固定配分である配分パターン default が PRU へ反映されます。このシステムメッセージが表示されたときは，再度正しい手順でカスタマイズ配分パターンを生成して，コンフィグレーションへ設定してください。
- カスタマイズ配分支援用高機能スクリプトには，直前に実行した生成用スクリプトおよび調整用スクリプトの結果を元に動作するパラメータがあります。そのため，装置内で複数のユーザが同時にスクリプトを実行するときは，注意が必要です。
- カスタマイズ配分支援用高機能スクリプトには直前に実行したスクリプトの結果を元に動作するパラメータがありますが，装置や BCU を再起動した場合は直前の実行結果をリセットします。そのため，再度カスタマイズ配分を生成する必要があります。

  また，直前の実行結果は BCU ごとに管理しているため，系切替後にスクリプトを実行する場合も同様に，再度カスタマイズ配分を生成してください。

12.3　装置の確認

12.3.1　コンフィグレーション・運用コマンド一覧

装置の確認に関するコンフィグレーションコマンド一覧および運用コマンド一覧を次の表に示します。

表 12-25　コンフィグレーションコマンド一覧（識別名称の設定）

コマンド名	説明
hostname	本装置の識別名称を設定します。

表 12-26　コンフィグレーションコマンド一覧（装置の動作設定）

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 flash-monitor	内蔵フラッシュメモリのユーザ領域の未使用容量を監視して，警告および回復のシステムメッセージを出力します。
system high-temperature-action	BCU の入気温度が動作保証範囲を超えた場合の BCU の動作モードを設定します。
system temperature-warning-level	装置の入気温度が指定温度以上になった場合に，温度を警告するシステムメッセージを出力します。また，装置の入気温度が指定温度以上になったあとで指定温度から 3℃以上下がった場合に，温度の回復を示すシステムメッセージを出力します。
system temperature-warning-level average	装置の平均入気温度が指定温度以上になった場合にシステムメッセージを出力します。

表 12-27　運用コマンド一覧（ソフトウェアバージョンと装置の状態確認）

コマンド名	説明
show version	バージョン情報や搭載されているボードの情報を表示します。
show system	装置の運用状態を表示します。
show environment	装置の環境情報を表示します。
reload	装置を再起動して，そのときにログを採取します。通常動作時は BCU のメモリダンプを採取します。
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。
show power	装置の経過時間および各ボードの消費電力，累計消費電力量を表示します。

表 12-28　運用コマンド一覧（内蔵フラッシュメモリと MC の確認）

コマンド名	説明
show mc※	MC の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。

コマンド名	説明
show flash※	装置内蔵フラッシュメモリの使用状態を表示します。

注※

「運用コマンドレファレンス Vol.1　13. MC と装置内メモリの確認」を参照してください。

表 12-29　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※1	CPU 使用率を表示します。
show processes※1	装置で現在実行中のプロセスの情報を表示します。
show memory※1	装置の物理メモリの実装量，使用量，および空き容量を表示します。
df※1	ディスクの空き領域を表示します。
du※1	ディレクトリ内のファイル容量を表示します。
erase dumpfile※2	ダンプファイル格納ディレクトリ上のダンプファイル，またはコアファイル格納ディレクトリ上のコアファイルを消去します。
show dumpfile※2	ダンプファイル格納ディレクトリ上のダンプファイル，またはコアファイル格納ディレクトリ上のコアファイルの一覧を表示します。

注※1

「運用コマンドレファレンス Vol.1　14. リソース情報」を参照してください。

注※2

「運用コマンドレファレンス Vol.1　15. ダンプ情報」を参照してください。

12.3.2　ソフトウェアバージョンの確認

運用コマンド show version でバージョン情報や搭載されているボードの情報を確認できます。バージョン情報は現在運用しているソフトウェアバージョンを表示しますが，ソフトウェアを入れ替えたあと運用に反映していないときは，()内にインストールバージョンを表示します。次の図に例を示します。

図 12-38　ソフトウェアバージョンの確認

```
> show version software
Date 20XX/04/01 02:54:45 UTC
BCU1: AX-P8600-R2, OS-RE, Ver.12.4.E
      BCU-CPU:           Ver.12.4.E
      BCU-CPU Boot ROM:  Ver.1.1.0
      PA:                Ver.12.4.E
      PA Boot ROM:       Ver.2.1.15
      HDC:               Ver.2.22
      HDC2:              Ver.4.0
BCU2: notconnect
SFU1: HDC:               Ver.2.1
SFU2: notconnect
SFU3: notconnect
SFU4: notconnect
PRU1: PRU-CPU:           Ver.12.4.E
      PRU-CPU Boot ROM:  Ver.2.1.7
      HDC:               Ver.2.38
      HDC2:              Ver.0.9
PRU2: notconnect
PRU3: notconnect
PRU4: notconnect
NIF1: HDC:               Ver.2.0
NIF2: notconnect
```

```
  :
NIF16: notconnect
>
```

12.3.3　装置の状態確認

(1)　運用状態の確認

運用コマンド show system で次の情報を確認できます。

- 装置の情報
- ファン，電源機構，および各ボード（BCU/SFU/PRU/NIF）の情報

次の図に例を示します。

図 12-39　運用状態の確認

```
> show system
Date 20XX/04/01 01:52:01 UTC
System: AX8616R, OS-RE, Ver.12.6, [9896.21]
    Elapsed time: 2 days 04:30
    Name: System
    Contact: Contact
    Location: Location
    Chassis MAC address: 0012.e286.5300
    BCU redundancy status: duplex
    FAN control mode: 1 (normal)
    Temperature warning level: current = 45, average = 45
    High temperature action: stop
    Power redundancy mode: 2 (Power Supply + Input Source)
    Hardware profile
        Configuration: router-1
        Current: router-1
    Failure action (software): unicast switchover
                               multicast switchover
    System MTU: 1518

Hardware information
    FAN1: active
        Elapsed time: 2 days 04:30
        Lamp: STATUS LED = green
    FAN2: active
        Elapsed time: 2 days 04:30
        Lamp: STATUS LED = green
    FAN3: active
        Elapsed time: 2 days 04:30
        Lamp: STATUS LED = green
    FAN4: active
        Elapsed time: 2 days 04:30
        Lamp: STATUS LED = green
    FAN5: active
        Elapsed time: 2 days 04:30
        Lamp: STATUS LED = green
    FAN6: active
        Elapsed time: 2 days 04:30
        Lamp: STATUS LED = green
    PS1: active
        Elapsed time: 2 days 04:30
    PS2: active
        Elapsed time: 2 days 04:30
    PS3: active
        Elapsed time: 2 days 04:30
    PS4: active
        Elapsed time: 2 days 04:30
    BCU1: active
        Elapsed time: 2 days 04:30
        Boot device: primary
        BCU-CPU: active
            Boot: 20XX/03/29 09:10:46 UTC, power on, fatal error restart 0 time
            Board: clock 2.0GHz, memory 16,068,212KB
```

```
        PA: active
            Boot: 20XX/03/29 09:10:46 UTC, power on, fatal error restart 0 time
            Board: clock 1.1GHz, memory 2,097,152KB
        Lamp: STATUS LED = green, ACTIVE LED = green
              SYSTEM1 LED = green, SYSTEM2 LED = light off
        System operation panel: no error
        Management port: active up
            10BASE-T half(auto), 0012.e286.5301
        Temperature: normal (32 degree C)
        Flash: enabled, 6,153,286KB
        MC: notconnect
    BCU2: standby
        Elapsed time: 2 days 04:30
        Boot device: primary
        BCU-CPU: active
            Boot: 20XX/03/29 09:10:53 UTC, power on, fatal error restart 0 time
            Board: clock 2.0GHz, memory 16,068,212KB
        PA: active
            Boot: 20XX/03/29 09:10:53 UTC, power on, fatal error restart 0 time
            Board: clock 1.1GHz, memory 2,097,152KB
        Lamp: STATUS LED = green, ACTIVE LED = green
              SYSTEM1 LED = green, SYSTEM2 LED = light off
        System operation panel: no error
        Management port: unused
            -, -
        Temperature: normal (32 degree C)
        Flash: enabled, 6,153,286KB
        MC: notconnect
    SFU1: active, fatal error restart 0 time
        Elapsed time: 2 days 04:34
        Lamp: STATUS LED = green, ACTIVE LED = green
    SFU2: notconnect
    SFU3: notconnect
    SFU4: notconnect
    PRU1: active, fatal error restart 0 time
        Elapsed time: 2 days 04:30
        Boot: 20XX/03/29 09:20:26 UTC
        Board: clock 0.8GHz, memory 3,760,820KB
        Lamp: STATUS LED = green
        Forwarding database management
            Forwarding-table allocation
                Configuration: default
                Current: default
        Flow database management
            Flow-table allocation
                Configuration: default
                Current: default
            Flow detection mode
                Configuration: quantity-oriented
                Current: quantity-oriented
    PRU2: notconnect
    PRU3: notconnect
    PRU4: notconnect
    NIF1: active, fatal error restart 0 time
        Elapsed time: 2 days 04:34
        Lamp: STATUS LED = green
    NIF2: notconnect
     :
    NIF16: notconnect
>
```

(2) 環境状態の確認

運用コマンド show environment で次の情報を確認できます。

- ファンの情報
- 電源機構の情報
- 電力使用情報
- BCU の入気温度

- 各ボード（BCU/SFU/PRU/NIF）の温度状態
- 各ボード（BCU/SFU/PRU/NIF）の稼働時間情報

次の図に例を示します。

図 12-40 環境状態の確認

```
> show environment
Date 20XX/03/27 06:16:38 UTC

FAN environment
    FAN1: active, Speed = 2600
    FAN2: active, Speed = 2600
    FAN3: fault
    FAN4: active, Speed = 2600
    FAN5: active, Speed = 2600
    FAN6: active, Speed = high
    Mode: 1 (normal)

Power environment
    Input voltage: AC200-240V
    Power redundancy mode: 2 (Power Supply + Input Source)
    Power supply redundancy status
        Power supply: active = 4, required = 1 (Redundant)
        Input source: active = 2(from A) 2(from B), required = 1 (Redundant)
    PS1: active
    PS2: active
    PS3: active
    PS4: active

Power usage
    Total power capacity:                                  10168.00 W
        Input source A:                                     5084.00 W
        Input source B:                                     5084.00 W
    Total power allocated:                                  1477.00 W
    Total power available for additional boards:            8691.00 W
    Power available (Power supply unit redundant case):     6149.00 W
    Power available (Input source redundant case)
        Input source A:                                     3607.00 W
        Input source B:                                     3607.00 W

Inlet temperature
    BCU1: normal (36 degree C)
    BCU2: normal (36 degree C)

Board temperature
    BCU1: normal
    BCU2: normal
    SFU1: normal
    SFU2: notconnect
    SFU3: notconnect
    SFU4: notconnect
    PRU1: normal
    PRU2: notconnect
    PRU3: notconnect
    PRU4: notconnect
    NIF1: normal
    NIF2: notconnect
     :
    NIF16: notconnect

Accumulated running time
                total               caution             critical
    BCU1       2 days 16 hours      1 day   1 hour      0 days   0 hours
    BCU2       2 days 16 hours      1 day   1 hour      0 days   0 hours
    SFU1       2 days 16 hours      1 day   1 hour      0 days   0 hours
    SFU2    notconnect
    SFU3    notconnect
    SFU4    notconnect
    PRU1       2 days 16 hours      1 day   1 hour      0 days   0 hours
    PRU2    notconnect
    PRU3    notconnect
```

```
    PRU4    notconnect
    NIF1       2 days 16 hours      1 day   1 hour       0 days   0 hours
    NIF2    notconnect
     :
    NIF16   notconnect
    PS1        2 days 16 hours      1 day   1 hour       0 days   0 hours
    PS2        2 days 16 hours      1 day   1 hour       0 days   0 hours
    PS3        2 days 16 hours      1 day   1 hour       0 days   0 hours
    PS4        2 days 16 hours      1 day   1 hour       0 days   0 hours
    FAN1       2 days 16 hours      1 day   1 hour       0 days   0 hours
    FAN2       2 days 16 hours      1 day   1 hour       0 days   0 hours
     :
    FAN6       2 days 16 hours      1 day   1 hour       0 days   0 hours
>
```

(3)　温度履歴情報の確認

運用コマンド show environment の temperature-logging パラメータで入気温度履歴情報を最大で 2 年分確認できます。temperature-logging パラメータを指定すると, 6 時間ごとに記録した平均入気温度を表示します。次の図に例を示します。

図 12-41　温度履歴情報の確認

```
> show environment temperature-logging
Date 20XX/04/01 01:44:40 UTC
BCU1
Date         0:00  6:00 12:00 18:00
20XX/04/01   32.9
20XX/03/31   33.0  33.0  33.0  33.0
20XX/03/30   33.0  33.0  33.0  33.0
20XX/03/29      -     -  33.7  33.0

BCU2
Date         0:00  6:00 12:00 18:00
20XX/04/01   32.9
20XX/03/31   33.0  33.0  33.0  33.0
20XX/03/30   33.0  33.0  33.0  33.0
20XX/03/29      -     -  33.7  33.0
>
```

12.3.4　内蔵フラッシュメモリの確認

運用コマンド show flash で内蔵フラッシュメモリの使用状況を確認できます。次の図に例を示します。

図 12-42　内蔵フラッシュメモリの確認

```
> show flash
Date 20XX/04/01 07:09:21 UTC
Warning threshold : 1000MB
Recovery threshold: 1256MB
Flash monitor event level: S6
BCU1 Flash: enabled
    area                used             free            total
    user            185,394KB       2,832,550KB       3,017,944KB
    config            1,682KB       1,601,538KB       1,603,220KB
    dump0             2,816KB         326,416KB         329,232KB
    dump1               998KB       1,064,674KB       1,065,672KB
    log                  11KB         137,207KB         137,218KB
    total           190,901KB       5,962,385KB       6,153,286KB
BCU2 Flash: enabled
    area                used             free            total
    user            185,394KB       2,832,550KB       3,017,944KB
    config            1,682KB       1,601,538KB       1,603,220KB
    dump0             2,816KB         326,416KB         329,232KB
    dump1               998KB       1,064,674KB       1,065,672KB
    log                  11KB         137,207KB         137,218KB
    total           190,901KB       5,962,385KB       6,153,286KB
>
```

12.3.5　MC の確認

運用コマンド show mc で MC の使用状況を確認できます。次の図に例を示します。

図 12–43　MC の確認

```
> show mc
Date 20XX/04/01 07:20:11 UTC
BCU1 MC: enabled
     CID: 00c7000910d06b224743043046534150001
     used:         189,792KB
     free:       3,680,928KB
     total:      3,870,720KB
BCU2 MC: --------
>
```

12.3.6　温度監視

(1)　入気温度の監視

本装置では，運用系および待機系でそれぞれ入気温度を監視します。入気温度が低温や高温になると，システムメッセージを出力したり SNMP 通知を送信したりします。入気温度が高温停止レベルになると，装置を停止します。

なお，入気温度は履歴情報として最大 2 年分参照できます。

(2)　入気温度の監視レベルと動作

入気温度の監視レベルと動作を次の表に示します。

表 12–30　監視レベルと動作

入気温度	監視レベル	運用環境レベル	システムの動作
2℃以下に下降	低温注意	caution	運用を継続します。運用環境レベルが変化した場合にシステムメッセージを出力，および SNMP 通知を送信します。
5℃以上に上昇	低温注意回復	normal	
40℃以下に下降	高温注意回復	normal	
43℃以上に上昇	高温注意	caution	
50℃以下に下降	高温警告回復	caution	
53℃以上に上昇	高温警告	critical	
65℃以上に上昇	高温停止	fault	BCU を停止します。※

注※　コンフィグレーションコマンド system high-temperature-action で，BCU を停止しないように設定できます。

高温停止レベルで BCU を停止する場合の動作を次に示します。

BCU が一重化の場合

システムメッセージを出力，および SNMP 通知を送信して装置を停止します。停止した BCU は自動回復しません。

BCU が二重化で，運用系 BCU（例えば，BCU1）が高温停止レベルとなった場合

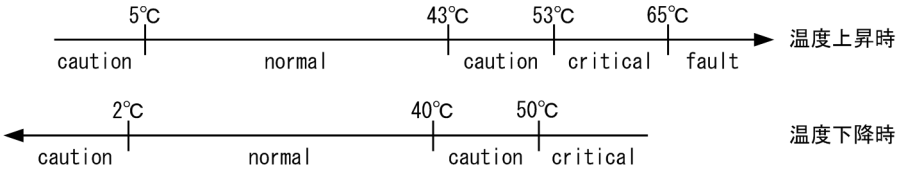
システムメッセージを出力，および SNMP 通知を送信して BCU1 を停止します。系切替をして BCU2 が運用系となり，一重化で運用します。停止した BCU1 は自動回復しません。

BCU が二重化で，待機系 BCU（例えば，BCU2）が高温停止レベルとなった場合

システムメッセージを出力，および SNMP 通知を送信して BCU2 を停止して，一重化で運用します。停止した BCU2 は自動回復しません。

運用環境レベルと温度値について次の図に示します。

図 12-44　運用環境レベルと温度値



(3)　任意の入気温度による警告および回復通知

(a)　入気温度監視

コンフィグレーションコマンド system temperature-warning-level を設定すると，装置の入気温度が指定した温度以上になった場合に温度を警告するシステムメッセージを出力します。また，装置の入気温度が指定した温度以上になったあとで指定した温度から 3℃以上下回った場合，温度の回復を示すシステムメッセージを出力します。ただし，温度を警告するシステムメッセージを出力するのは，温度の回復を示すシステムメッセージを出力したあとです。

(b)　平均入気温度監視

コンフィグレーションコマンド system temperature-warning-level average を設定すると，装置の指定日数当たりの平均入気温度が指定した温度以上になった場合，毎日 12:00 に温度を警告するシステムメッセージを出力します。

(4)　入気温度状態の確認

入気温度の状態は運用コマンド show environment で表示される「Inlet Temperature」の項目で確認できます。また，入気温度に関する履歴情報は，運用コマンド show environment の temperature-logging パラメータで最大 2 年分を確認できます。

(5)　ボードの温度監視

本装置では入気温度の監視とは別に，各ボードの温度を監視します。監視対象のボードは BCU，SFU，PRU，および NIF です。

運用が継続できないほどボードが高温になった場合は，該当するボードを停止します。停止したボードは温度が下がっても自動回復しません。ボードの温度状態の監視レベルと動作を次の表に示します。

表 12-31　監視レベルと動作

監視レベル	運用環境レベル	システムの動作
高温警告回復	normal	該当するボードの運用を継続します。
高温警告検出	critical	
高温停止	fault	システムメッセージを出力，および SNMP 通知を送信して，該当するボードを停止します。

(6)　ボードの温度状態の確認

各ボードの温度状態は運用コマンド show environment で表示される「Board Temperature」の項目で確認できます。

12.3.7　ファンユニットの監視

(1)　ファンユニット状態の監視

ファンユニットの内部には複数の個別ファンがあり，装置は複数のファンユニットを搭載できます。

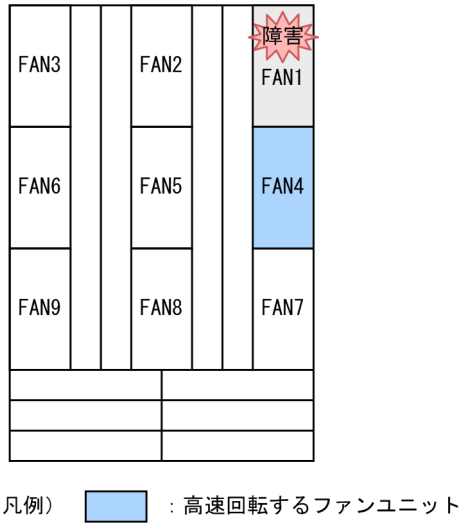
運用中にファンユニットが故障（個別ファンの故障，ファンユニットの障害や抜去など）すると，ファンユニット障害のシステムメッセージを出力および SNMP 通知を送信します。このとき，ファンユニットを高速回転にしたり，ファンユニット回転数の下限を引き上げて一定以上の回転数にしたりして，装置の動作を継続します。装置種別ごとのファンユニット故障時の動作を次の表に示します。

表 12-32　装置種別ごとのファンユニット故障時の動作

装置種別	FAN1 の故障	FAN3 の故障	それ以外の故障
AX8608R	• 回転数下限引き上げ	• 回転数下限引き上げ	• 回転数下限引き上げ
AX8616R	• FAN4 を高速回転 • 回転数下限引き上げ	• FAN6 を高速回転 • 回転数下限引き上げ	• 回転数下限引き上げ
AX8632R	• FAN4 を高速回転 • 回転数下限引き上げ	• FAN6 を高速回転 • 回転数下限引き上げ	• 回転数下限引き上げ

ファンユニット故障時の動作例を次の図に示します。

図 12-45　ファンユニット故障時の動作例（AX8632R で FAN1 のファンユニットが故障した場合）



故障したファンユニットは，装置を運用したまま抜去および交換できます。故障したファンユニットを交換して正常動作すると，ファンユニット障害の回復を示すシステムメッセージを出力および SNMP 通知を送信します。同時に，ファンユニットの高速回転および回転数下限引き上げを解除します。

ファンユニットを高速回転にした場合および高速回転を解除した場合，該当するファンユニットごとにシステムメッセージを出力します。

(2)　ファンユニット状態の確認

各ファンユニットのファン動作状態と回転スピードは，運用コマンド show environment で表示される「Fan environment」の項目で確認できます。

12.3.8　内蔵フラッシュメモリの未使用容量監視

コンフィグレーションコマンド system flash-monitor を設定すると，内蔵フラッシュメモリのユーザ領域の未使用容量を監視して，次の契機でシステムメッセージを出力します。

- 未使用容量がコンフィグレーションで設定した閾値未満になると，任意のイベントレベルの警告のシステムメッセージを出力
- 警告のシステムメッセージの出力後，未使用容量がコンフィグレーションで設定した閾値以上になると，回復のシステムメッセージを出力

本機能によって待機系 BCU で出力したシステムメッセージは，運用系 BCU でも出力します。

12.4　SFU/PRU/NIF の管理

12.4.1　コンフィグレーション・運用コマンド一覧

SFU/PRU/NIF の管理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 12-33　コンフィグレーションコマンド一覧

コマンド名	説明
nif※	pe-service コンフィグレーションで設定した PE サービスを適用する PE-NIF を搭載している NIF 番号を設定します。
pe-service※	PE-NIF に設定する PE サービスの ID と名称を設定します。
power enable※	disable 状態のボードを active 状態にします。また，no power enable を設定するとボードの電力を OFF にします。
service-type※	PE-NIF に適用するサービスタイプを設定します。
system nif board-type※	PE-NIF を搭載する NIF 番号を設定します。
system pru priority※	装置起動時に起動する PRU の優先度を設定します。

注※
「コンフィグレーションコマンドレファレンス Vol.1　11. SFU/PRU/NIF の管理」を参照してください。

SFU/PRU/NIF の管理に関する運用コマンド一覧を次の表に示します。

表 12-34　運用コマンド一覧

コマンド名	説明
show system	SFU および PRU の状態を表示します。
show nif※	NIF の運用状態を表示します。
show pe service※	PE-NIF に設定されている PE サービスの情報を表示します。
clear counters nif※	NIF の統計情報カウンタをクリアします。
activate sfu※	inactive 状態の SFU を active 状態にします。
inactivate sfu※	active 状態の SFU を inactive 状態にします。また，SFU の電力を OFF にします。
reload sfu※	SFU を再起動します。
activate pru※	inactive 状態の PRU を active 状態にします。
inactivate pru※	active 状態の PRU を inactive 状態にします。また，PRU の電力を OFF にします。
reload pru※	PRU を再起動します。
activate nif※	inactive 状態の NIF を active 状態にします。
inactivate nif※	active 状態の NIF を inactive 状態にします。また，NIF の電力を OFF にします。
reload nif※	NIF を再起動します。

注※

「運用コマンドレファレンス Vol.1　12. SFU/PRU/NIF の管理」を参照してください。

12.4.2　ボードの disable 設定

コンフィグレーションコマンド power enable で未使用の SFU，PRU および NIF を disable 状態にします。本設定をしたボードの電力は OFF になります。次に示す例では，SFU を disable 状態にします。

[設定のポイント]

コンフィグレーションコマンドで設定することで，装置の再起動後もこの状態を継続します。

[コマンドによる設定]

1. **(config)# no power enable sfu 1**

   コンフィグレーションモードで，SFU1 を disable 状態にします。

12.4.3　PRU の起動優先度の設定

装置起動時に電力が不足している場合は，一部の PRU だけ起動します。その場合に起動する PRU の優先度を 1～255 の間で設定します。設定した値が小さいほど優先度は高くなります。なお，優先度のデフォルト値は 128 です。

装置起動時には優先度が高い順に PRU を起動します。優先度が同じ場合は，PRU 番号の小さい PRU を優先して起動します。なお，装置起動時に電力が不足していない場合は，本優先度は適用されないで，すべての PRU が起動します。次に示す例では，PRU 番号 1 のボードを高優先，PRU 番号 4 のボードを低優先として設定します。

[設定のポイント]

装置起動時に起動する PRU を明確にするために，各 PRU に異なる優先度を設定してください。

本設定値は装置起動時にだけ適用されます。そのため，初期導入時に設定することをお勧めします。

[コマンドによる設定]

1. **(config)# system pru 1 priority 1**

   (config)# system pru 4 priority 255

   PRU1 の優先度を 1，PRU4 の優先度を 255 に設定します。

12.4.4　SFU の状態確認

運用コマンド show system で SFU の動作状態と更新状態を確認できます。該当する SFU のアップデートを実施している場合，更新状態を表示します。次の図に例を示します。

図 12-46　SFU の状態確認

```
> show system
Date 20XX/12/10 15:11:20 UTC
System: AX8632R, OS-RE, Ver.12.1, [123.1]
              :
              :
    SFU1 : active (restart required), fatal error restart 0 time
        Elapsed time : 2 days 2:30
        Lamp : STATUS LED = green , ACTIVE LED = light off
    SFU2 : notconnect
              :
    SFU4 : active, fatal error restart 0 time
        Elapsed time : 2 days 2:30
```

```
        Lamp : STATUS LED = green , ACTIVE LED = light off
>
```

12.4.5 PRU の状態確認

運用コマンド show system で PRU の動作状態と更新状態を確認できます。該当する PRU のアップデートを実施している場合，更新状態を表示します。次の図に例を示します。

図 12-47 PRU の状態確認

```
> show system
Date 20XX/12/10 15:11:20 UTC
System: AX8632R, OS-RE, Ver.12.1, [123.1]
               :
               :
    PRU1 : active (restart required), fatal error restart 0 time
               :
    PRU2 : notconnect
               :
    PRU8 : active, fatal error restart 0 time
               :
>
```

12.4.6 NIF の状態確認

運用コマンド show nif で NIF の動作状態と更新状態を確認できます。該当する NIF のアップデートを実施している場合，更新状態を表示します。次の図に例を示します。

図 12-48 NIF の状態確認

```
>show nif 1
Date 20XX/04/01 12:00:00 UTC
NIF1: active(restart required)  12-port 10BASE-T/100BASE-TX/1000BASE-T  retry:0
        Average:103Mbps/24Gbps  Peak:150Mbps at 08:10:30
Port1: active up  1000BASE-T full(auto)  0012.e240.0a04
        Bandwidth:1000000kbps  Average out:20Mbps  Average in:10Mbps
        description: test lab area network
Port2: active up  1000BASE-T full(auto)  0012.e240.0a05
        Bandwidth:1000000kbps  Average out:0Mbps  Average in:0Mbps
        description: computer management floor network
Port3: active up  1000BASE-T full(auto)  0012.e240.0a06
        Bandwidth:1000000kbps  Average out:2Mbps  Average in:1Mbps
               :
               :
>
```

12.4.7 NIF 交換時のコンフィグレーション

ポートのコンフィグレーションが存在しない場合，NIF を取り付けると，その NIF に対応するポートのコンフィグレーションが自動で生成されます。しかし，ポートのコンフィグレーションが存在する場合，異なるイーサネット種別（10BASE-T/100BASE-TX/1000BASE-T, 1000BASE-X, 10GBASE-R, 40GBASE-R, 100GBASE-R）を収容する NIF へ交換すると，交換後の NIF に対応するポートのコンフィグレーションが自動で生成されません。その結果，コンフィグレーションと搭載している NIF のイーサネット種別が不一致になるため，該当のポートはリンクアップしません。

交換後の NIF に対応するポートのコンフィグレーションが自動で生成されないときは，交換前のポートのコンフィグレーションを削除してください。交換前のコンフィグレーションを削除したポートは，交換後の NIF に対応するコンフィグレーションが自動で生成されます。

NIF 交換時のポートのコンフィグレーションの自動生成と削除例を次に示します。この例では，NIF を NLXG-6RS から NL1G-12T に交換します。

1. NIF（NLXG-6RS）を取り外します。
2. コンフィグレーションを確認します。

```
(config)# show
interface tengigabitethernet 1/1
!
interface tengigabitethernet 1/2
!
interface tengigabitethernet 1/3
!
interface tengigabitethernet 1/4
!
interface tengigabitethernet 1/5
!
interface tengigabitethernet 1/6
!
```

NIF を取り外しても，対応するポートのコンフィグレーションは削除されません。

3. NIF（NL1G-12T）を取り付けます。
4. コンフィグレーションを確認します。

```
(config)# show
interface tengigabitethernet 1/1
!
                :
                :

!
interface tengigabitethernet 1/6
!
interface gigabitethernet 1/7
!
interface gigabitethernet 1/8
!
interface gigabitethernet 1/9
!
interface gigabitethernet 1/10
!
interface gigabitethernet 1/11
!
interface gigabitethernet 1/12
!
```

ポート 1/1～1/6 は交換前の 10 ギガビットイーサネットインタフェースのコンフィグレーションが存在するため，交換後の NIF に対応するコンフィグレーションが自動で生成されません。

ポート 1/7～1/12 は，交換後の NIF に対応するギガビットイーサネットインタフェースのコンフィグレーションが自動で生成されます。

5. ポート 1/1 のコンフィグレーションを削除します。

```
(config)# no interface tengigabitethernet 1/1
```

6. コンフィグレーションを確認します。

```
(config)# show
interface gigabitethernet 1/1
!
interface tengigabitethernet 1/2
!
                :
                :
!
interface tengigabitethernet 1/6
!
interface gigabitethernet 1/7
!
                :
                :
```

ポート 1/1 は交換前のコンフィグレーションを削除したため，交換後の NIF に対応するコンフィグレーションが自動で生成されます。

12.4.8　PE-NIF の設定

PE-NIF とは，NIF にプログラマブルエンジン（PE）を搭載することで，機能を柔軟に追加できるようにしたものです。

PE-NIF に追加できる機能は，PE-NIF に割り当てるサービスタイプによって決まります。本装置でサポートしているサービスタイプと，サービスタイプごとに使用できる PE-NIF の機能を次の表に示します。

表 12-35　サービスタイプごとに使用できる PE-NIF の機能

サービスタイプ	PE-NIF の機能
generic	階層化シェーパ

PE-NIF にどのサービスタイプを割り当てるかは，PE サービスと呼ばれる識別子で管理します。PE サービスの内容を変更することで，追加した機能を柔軟に，装置内の PE-NIF で提供できるようになります。

[設定のポイント]

PE-NIF を使用する場合，ほかの NIF と同様にコンフィグレーションを設定しなくても active 状態にできますが，PE-NIF のコンフィグレーションを設定してから active 状態にすることを推奨します。なお，動作中の PE-NIF に適用しているコンフィグレーションを削除した場合，PE-NIF が inactive 状態になります。

[コマンドによる設定]

1. **(config)# system nif 1 board-type pe-nif**
   グローバルコンフィグレーションモードで，PE-NIF を搭載する NIF 番号を設定します。
2. **(config)# pe-service 1 pe-1**
   PE サービスを管理するための PE サービス ID と PE サービス名を指定して，PE サービスを設定します。コマンドを実行すると，PE サービスのコンフィグレーションモードに移行します。
3. **(config-pe-service)# nif 1**
   PE サービスを適用する PE-NIF を搭載する NIF 番号を設定します。
4. **(config-pe-service)# service-type generic**
   サービスタイプに generic を設定します。

12.4.9　PE サービスの確認

運用コマンド show pe service で，PE-NIF で動作している PE サービスの情報を確認できます。コマンドの実行結果を次の図に示します。

図 12-49　PE サービスの確認

```
> show pe service
Date 20XX/04/01 12:00:00 UTC
PE service name: srv1
PE service id:   1
NIF no.:         1
Service type:    generic

PE service name: srv2
PE service id:   2
NIF no.:         2, 4-6
Service type:    generic
>
```

12.5　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。

BCU を二重化している場合には，「12.5.2　BCU 二重化時の手順」を実施してください。BCU が一重化の場合に確実かつ簡単に行うためには「12.5.3　BCU 一重化時の手順」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。

12.5.1　運用コマンド一覧

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 12-36　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 MC またはリモートの ftp サーバに保存します。
restore	MC およびリモートの 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。

12.5.2　BCU 二重化時の手順

交換した BCU が待機系で立ち上がっている状態で，次のコマンドによってソフトウェアバージョンおよび設定ファイルを待機系と同期させます。

- update software コマンド
  ソフトウェアバージョンを同期させます。
- synchronize コマンド
  その他の設定ファイルを同期させます。本コマンドで同期する対象にはコンフィグレーションを含みます。

二重化運用時の管理情報の同期処理については，「14.1.3　ユーザの設定情報および利用情報の同期」を参照してください。

なお，BCU 二重化時に運用系および待機系の両系 BCU を同時に交換した場合には，restore コマンドを使用して次の手順で復旧します。

1. restore コマンド実行時に系切替が発生しないよう，inactivate bcu standby コマンドで待機系を inactive 状態にします。
2. 運用系で restore コマンドを実行します。これによって運用系が再起動します。
3. activate bcu standby コマンドで待機系を active 状態にします。
4. update software コマンドおよび synchronize コマンドで運用系と待機系を同期させます。

12.5.3 BCU 一重化時の手順

(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 コマンドを使用し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，MC または外部の FTP サーバに保存します。

次に示す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。

- 装置にインストールされているソフトウェア
- startup-config
- SSH サーバのホスト鍵ペア
- 装置にインストールされている高機能スクリプト

なお，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。

- 運用ログおよび統計ログ
- 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。

12.6　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します。障害の種別に応じて復旧処理を局所化して，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。

12.6.1　障害の種別と復旧内容

障害発生時，障害の内容によって復旧内容が異なります。障害の種別と復旧内容を次の表に示します。

表 12-37　障害の種別と復旧内容

障害の種別	装置の対応	復旧内容	影響範囲
ポートで検出した障害	無限回自動復旧します。	該当するポートを再初期化します。	該当するポートを経由する通信が中断されます。
NIF 障害	3 回まで自動復旧します。※1 自動復旧の回数が 3 回のときに障害が発生すると停止します。ただし，装置起動後 1 時間ごとに自動復旧の回数を初期化します。	該当する NIF を再初期化します。	該当する NIF が収容する全ポートを経由する通信が中断されます。
PRU 障害	3 回まで自動復旧します。※1 自動復旧の回数が 3 回のときに障害が発生すると停止します。ただし，装置起動後 1 時間ごとに自動復旧の回数を初期化します。	該当する PRU を再初期化します。	該当する PRU が収容する全 NIF を経由する通信が中断されます。
SFU 障害	3 回まで自動復旧します。※1 自動復旧の回数が 3 回のときに障害が発生すると停止します。ただし，装置起動後 1 時間ごとに自動復旧の回数を初期化します。	該当する SFU を再初期化します。	SFU を冗長化している場合は通信を維持できます。 該当する SFU 以外に運用系 SFU がない場合，全 NIF を経由する通信が中断されます。
BCU 障害	6 回まで自動復旧します。※1 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，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。	該当する BCU を再初期化します。 6 回目の自動復旧のときは，ランニングコンフィグレーションを初期化して起動します。 BCU を二重化構成にしている場合は系切替による復旧処理をします。	装置内の全ポートを経由する通信が中断されます。 BCU を二重化構成にしている場合は通信を維持できます。
入気温度障害	障害を検出した BCU を停止します。※2	停止した BCU は自動復旧しません。	装置内の全ポートを経由する通信が中断されます。

障害の種別	装置の対応	復旧内容	影響範囲
電源機構障害（PS）	障害を検出した電源機構の給電を停止します。 電源機構が複数搭載されている場合，残りの電源機構からの給電で運用を継続します。	障害を検出した電源機構は自動復旧しません。	電源機構を冗長化している場合，運用を継続します。 電源機構を冗長化していない場合，装置の運用に必要な電力が供給されなくなると正常に運用できません。
ファンユニット障害	FAN1 のファンユニットで障害を検出すると，FAN4 のファンユニットが高速回転します。 FAN3 のファンユニットで障害を検出すると，FAN6 のファンユニットが高速回転します。	障害を検出したファンユニットは自動復旧しません。 障害を検出したファンユニットを交換すると，高速回転を解除します。	通信に影響はありません。ただし，装置内の温度が上昇するおそれがあります。

注※1

障害内容によっては自動復旧しないで，該当するボードを停止します。

注※2

コンフィグレーションコマンド system high-temperature-action で BCU を停止しない設定をしている場合，BCU を停止しません。

12.6.2　ソフトウェア障害検出時の動作

(1)　概要

BCU 上の特定のソフトウェアに障害が発生した場合，そのソフトウェアを再起動するのと同時に BCU を系切替できます。こうすると，BCU を系切替しないで，障害が発生したソフトウェアの再起動だけでサービスを復旧する場合と比べて，サービス停止時間を短縮できることがあります。対象となるソフトウェアは，コンフィグレーションコマンド failure-action software で設定します。

なお，本機能を設定していても，待機系 BCU が搭載されていないなど系切替ができない場合，または本機能による系切替が連続で発生した場合には，システムメッセージを出力して系切替を抑止します。

(2)　ソフトウェア障害検出時の動作に関する注意事項

- コンフィグレーションコマンド failure-action software で unicast パラメータを設定している場合，core-file パラメータを指定して運用コマンド restart unicast を実行すると，BCU の系切替が発生します。
- コンフィグレーションコマンド failure-action software で multicast パラメータを設定している場合，core-file パラメータを指定して運用コマンド restart ipv4-multicast または restart ipv6-multicast を実行すると，BCU の系切替が発生します。
- コンフィグレーションコマンドの実行中，またはコンフィグレーションを操作する運用コマンドの実行中に系切替が発生した場合は，系切替後にコマンドを再実行してください。

  また，コンフィグレーションの編集中に系切替が発生した場合，BCU 間のコンフィグレーションが不一致になることがあります。その場合は出力されたシステムメッセージの対応手順に従って，待機系 BCU を再起動してください。

12.6.3　コンフィグレーション・運用コマンド一覧

ソフトウェア障害検出時の動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 12-38　コンフィグレーションコマンド一覧

コマンド名	説明
failure-action software	ソフトウェア障害が発生したときの動作を指定します。

ソフトウェア障害検出時の動作に関する運用コマンド一覧を次の表に示します。

表 12-39　運用コマンド一覧

コマンド名	説明
show system	ソフトウェア障害が発生したときの動作設定を表示します。

12.6.4　系切替条件の設定

[設定のポイント]

指定した機能に関係するプログラムで障害が発生したときに，BCU を系切替する設定をします。

[コマンドによる設定]

1. **(config)# failure-action software unicast switchover**

   グローバルコンフィグレーションモードで，ユニキャストルーティング機能に関係するソフトウェアで障害が発生したときに，系切替するように設定します。

13 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。

13.1　ソフトウェアアップデートの解説

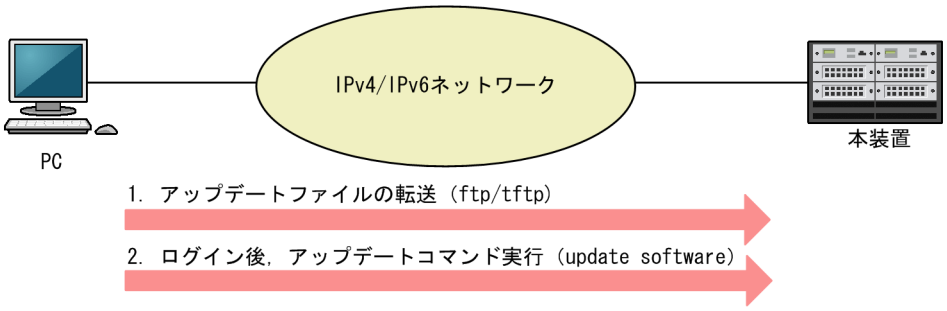
13.1.1　概要

ソフトウェアアップデートとは，ソフトウェアのバージョンを運用中のバージョンとは異なるバージョンに変更することです。装置の各ボードのソフトウェアを更新する処理と，更新したソフトウェアを装置の動作状態に反映する処理から成ります。バージョンアップ，バージョンダウンのどちらもできます。

PC などのリモート運用端末または MC からアップデートファイルを本装置に転送して運用コマンド update software を実行すると，ソフトウェアをアップデートできます。また，ボードの起動時および系切替時には，SFU，PRU，NIF のソフトウェアを自動で運用系 BCU と同じバージョンにアップデートします。アップデート時，コンフィグレーションはそのまま引き継がれます。

運用コマンド update software によるソフトウェアアップデートの概要を次の図に示します。

図 13-1　ソフトウェアアップデートの概要



13.1.2　ソフトウェアアップデートの対象

ソフトウェアアップデートでは，装置の各ボードのソフトウェアおよびハードウェア制御に関するソフトウェア（HDC，PE-ME）を更新します。なお，各ボードにインストール済みのソフトウェアのバージョンとアップデートに使用するソフトウェアのバージョンが同じ場合は，アップデートしません。

ソフトウェアアップデートの対象を次の表に示します。

表 13-1　ソフトウェアアップデートの対象

ボード	アップデート対象
BCU	ソフトウェア，HDC
SFU	HDC
PRU	ソフトウェア，HDC
NIF	HDC，PE-ME（PE-NIF 搭載時だけ）

13.1.3　更新・反映の契機

ソフトウェアは，次に示す二つの契機でアップデートします。

- 運用コマンド update software の実行時
- ボードの起動時

アップデートの契機によって，ソフトウェアの更新および反映のタイミングが異なります。ここでは，各アップデート契機での更新および反映のタイミングについて説明します。

なお, 運用コマンド show version を使用して動作中のバージョンとインストール済みのバージョンを比較すると，ソフトウェアの更新および反映状態を確認できます。

(1)　運用コマンド update software の実行時

BCU 一重化構成の場合

BCU のソフトウェアを更新したあと，装置を自動で再起動して新しいソフトウェアを反映します。同時に，各ボードで新しいソフトウェアを更新および反映します。なお，update software コマンド実行時に自動で再起動させないことも指定できます。

BCU 二重化構成の場合

BCU のソフトウェアを更新したあと，BCU を自動で再起動して新しいソフトウェアを反映します。なお，update software コマンド実行時に自動で再起動させないことも指定できます。

運用系 BCU を対象とした場合，SFU，PRU，および NIF のソフトウェアも更新します。更新したソフトウェアを反映するには，運用コマンド reload で各ボードを再起動してください。

ソフトウェアの反映契機については，「13.2　ソフトウェアアップデートのオペレーション」を参照のこと。

(2)　ボードの起動時

各ボードの起動を契機とした SFU，PRU，または NIF のアップデートでは，自動でソフトウェアを更新および反映します。そのため，起動したボードは運用系 BCU と同じバージョンのソフトウェアで動作します。

13.1.4　無停止ソフトウェアアップデート

無停止ソフトウェアアップデートは, 冗長構成のときに通信を中断しないでソフトウェアをアップデートする機能です。ルーティングテーブルなどを保持し続け, 順に更新することでアップデート作業中の通信を維持します。各ボードでの動作を次に示します。

BCU

二重化構成で系切替をしながらアップデートすることで，通信を維持したままソフトウェアおよび HDC を更新できます。

SFU

冗長構成で順番に SFU を再起動することで，通信を維持したまま HDC を更新できます。

PRU

複数の PRU にわたるリンクアグリゲーションを使用して順番に PRU を再起動することで, 通信を維持したままソフトウェアおよび HDC を更新できます。

NIF

複数の NIF にわたるリンクアグリゲーションを使用して順番に NIF を再起動することで，通信を維持したまま HDC を更新できます。

ソフトウェアのバージョンアップおよびバージョンダウン共に通信無停止でアップデートができます。

無停止ソフトウェアアップデートをするための条件を次の表に示します。

表 13-2　無停止ソフトウェアアップデートの適用条件

項目	適用条件
装置構成	BCU を二重化していること。 SFU を冗長化していること。 複数の PRU にわたるリンクアグリゲーションを使用していること。
	バージョンダウンの場合，アップデート後のソフトウェアバージョンで未サポートのハードウェア（PRU，NIF など）を使用していないこと。
サポート機能	通信無停止の系切替をサポートしている機能を使用していること。 詳細は，「14.1.4　系切替　(1)　通信無停止対応機能一覧」を参照してください。
	バージョンダウンの場合，アップデート後のソフトウェアで未サポートの機能を使用していないこと。
ソフトウェアバージョン	アップデート前，アップデート後どちらも Ver. 12.1 以降であること。
	アップデート前に，運用系 BCU と待機系 BCU が同じバージョンのソフトウェアで動作していること。
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および編集中のコンフィグレーションが，スタートアップコンフィグレーションと一致していること。
	運用系 BCU と待機系 BCU のスタートアップコンフィグレーションが一致していること。

13.1.5　ソフトウェアアップデートに関する注意事項

(1)　電源に関する注意事項

ソフトウェアアップデートの実行中は，電源を OFF にしないでください。

(2)　SFU に関する注意事項

無停止ソフトウェアアップデートをする場合は，SFU が 1 枚停止しても装置が必要とする性能を維持できる数の SFU を搭載することをお勧めします。

SFU の HDC を更新するときは，SFU を順番に再起動する必要があります。このとき，搭載する PRU および NIF の構成と SFU の枚数によって，SFU の再起動中に装置が必要とする性能を下回ることがあるためです。

(3)　コンフィグレーションに関する注意事項

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，ソフトウェアアップデート後にも引き継がれます。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，引き継いだコンフィグレーションの中に，バージョンダウンなどによって未サポートになるコンフィグレーションがあった場合は，該当するコンフィグレーションを削除して運用します。

(4)　ボード交換に関する注意事項

バージョンアップ後のソフトウェアバージョンからサポートするボードを搭載する場合は，サポートするソフトウェアへバージョンアップしたあとで該当するボードを搭載してください。また，バージョンダウン後

のソフトウェアバージョンで未サポートとなるボードがある場合は, 該当するボードを抜去したあとでソフトウェアをバージョンダウンしてください。

13.2　ソフトウェアアップデートのオペレーション

13.2.1　運用コマンド一覧

ソフトウェアの管理に関する運用コマンド一覧を次の表に示します。

表 13-3　運用コマンド一覧

コマンド名	説明
update software	指定したソフトウェアにアップデートします。

13.2.2　アップデートファイルの準備

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 または commit を実行して，コンフィグレーションを保存してください。

   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 BCU 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. アップデートファイル（k.img）がディレクトリ（/usr/var/update）にすでに存在する場合，rm コマンドを実行して該当するファイルを削除してください。

3. show flash コマンドを実行してください。

   BCU1 および BCU2 の内蔵フラッシュメモリのユーザ領域（user）に，次に示す値以上の未使用容量（free）があることを確認します。

   　アップデートファイルのサイズ＋ 10MB

4. 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）に置いてください。

   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。

5. ls -l /usr/var/update コマンドを実行してください。

   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ます。確認が終了したら，「13.2.3　アップデートコマンドの実行」に進んでください。

13.2.3　アップデートコマンドの実行

BCU 一重化構成と BCU 二重化構成で手順が異なります。

(1)　一重化構成でのアップデート

1. cd /usr/var/update コマンドを実行してください。

2. update software k.img active コマンドを実行してください。

   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。

   BCU がアップデート対象の場合

   　ソフトウェアを更新したあと装置が自動で再起動します。再起動したら再度ログインして，「13.2.5　アップデート後の確認」に進んでください。

BCU がアップデート対象ではない場合

SFU，PRU または NIF を手動で再起動する必要があります。「13.2.4　SFU・PRU・NIF のアップデート」に進んでください。

(2)　二重化構成でのアップデート

1. cd /usr/var/update コマンドを実行してください。
2. update software k.img standby コマンドを実行してください。

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。

BCU がアップデート対象の場合

ソフトウェアを更新したあと待機系 BCU が自動で再起動します。再起動したら，手順 3.に進んでください。

BCU がアップデート対象ではない場合

update software k.img active コマンドを実行してください。

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。ソフトウェアを更新したあと，手順 9.に進んでください。

3. show version コマンドを実行してください。

待機系 BCU がアップデート後のソフトウェアで動作していることを確認します。

4. show system コマンドを実行してください。

「Hardware information」欄で，待機系 BCU の動作状態を確認します。

動作状態に「configuration discord」が表示されている場合

update software k.img active コマンドを実行してください。

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。ソフトウェアを更新したあと運用系 BCU が自動で再起動するため，系切替が発生します。系切替したら再度ログインして，手順 9.に進んでください。

動作状態に「configuration discord」が表示されていない場合

手順 5.に進んでください。

5. redundancy force-switchover コマンドを実行してください。

手動で系切替します。系切替したら，新運用系 BCU へ再度ログインしてください。

6. cd /usr/var/update コマンドを実行してください。
7. show system コマンドを実行してください。

「Hardware information」欄で，待機系 BCU の動作状態に「configuration discord」が表示されていないことを確認します。

8. update software k.img standby コマンドを実行してください。

ソフトウェアを更新したあと待機系 BCU が自動で再起動します。

9. show system コマンドを実行してください。

「Hardware information」欄で，待機系 BCU の動作状態が「standby」であることを確認します。確認が終了したら，「13.2.4　SFU・PRU・NIF のアップデート」に進んでください。

13.2.4　SFU・PRU・NIF のアップデート

1. すべての SFU および PRU に対して reload コマンドを実行してください。

すべての SFU，PRU，および NIF を再起動します。このとき，無停止ソフトウェアアップデートの適用条件を満たしていれば，ボードを 1 枚ずつ再起動することで通信を中断しないでソフトウェアを反映できます。再起動したら，「13.2.5　アップデート後の確認」に進んでください。

13.2.5　アップデート後の確認

BCU 一重化構成と BCU 二重化構成で手順が異なります。

(1)　一重化構成での確認

1. show version コマンドを実行してください。
   BCU のバージョンが期待したバージョンと同一であることを確認します。

(2)　二重化構成での確認

BCU 二重化構成では，これまでのアップデート手順によって，運用系 BCU と待機系 BCU が入れ替わっていることがあるため注意してください。

1. show version コマンドを実行してください。
   運用系 BCU のバージョンが期待したバージョンと同一であることを確認します。
2. show system コマンドを実行してください。
   「Hardware information」欄で，待機系 BCU の動作状態に次の表示がないことを確認してください。
   - configuration discord
   - software version discord

13.2.6　アップデート操作時の注意事項

(1)　k.img ファイルの削除時の注意事項

手順で指示があるときにだけ，k.img ファイルを削除してください。それ以外で削除すると，異常終了時にファイルを復旧できなくなります。

(2)　update software コマンド実行時の注意事項

update software 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「Update is undergoing now.」を表示し，異常終了します。

複数のユーザで同時に実行しなくても update software コマンドが異常終了した場合は，このメッセージが表示され，再実行できないことがあります。例えば，通信ソフトの終了による強制ログアウトなどで異常終了したときです。再実行できない場合は，"rm /tmp/ppupdate.exec"コマンドを実行したあと，再度 update software コマンドを実行してください。

13.3　BCU 初期導入ソフトウェアからのアップデートの解説

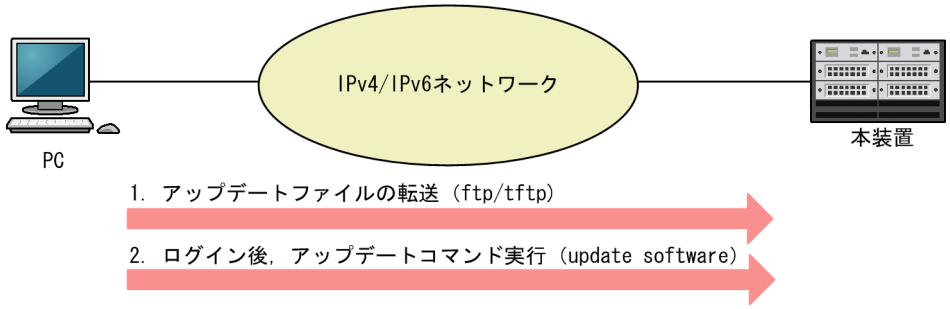
13.3.1　概要

BCU 初期導入ソフトウェアでは，BCU 以外のボードを起動しません。そのため，BCU を使用する前に，運用するバージョンのソフトウェアに更新する必要があります。以降，BCU 初期導入ソフトウェアを運用するソフトウェアに更新することを，BCU 初期導入ソフトウェアからのアップデートといいます。

BCU 初期導入ソフトウェアからのアップデートをするには，PC などのリモート運用端末または MC から運用するソフトウェアのファイルを本装置に転送して，ソフトウェアを更新する運用コマンドを実行します。BCU 初期導入ソフトウェアからのアップデートで使用するソフトウェアは，ソフトウェアアップデートで使用するソフトウェアと同じものです。また，ソフトウェア更新後もコンフィグレーションはそのまま引き継がれます。

BCU 初期導入ソフトウェアからのアップデートの概要を次の図に示します。

図 13-2　BCU 初期導入ソフトウェアからのアップデートの概要



13.3.2　BCU 初期導入ソフトウェアからのアップデートの対象

BCU 初期導入ソフトウェアからのアップデートでは，各ボードのソフトウェアおよびハードウェア制御に関するソフトウェア（HDC，PE-ME）を更新します。

BCU 初期導入ソフトウェアからのアップデートの対象を次の表に示します。

表 13-4　BCU 初期導入ソフトウェアからのアップデートの対象

ボード	アップデート対象
BCU	ソフトウェア，HDC
SFU	HDC
PRU	ソフトウェア，HDC
NIF	HDC，PE-ME（PE-NIF 搭載時だけ）

なお，BCU 初期導入ソフトウェアからのアップデートでは，BCU だけを更新対象としてソフトウェアを更新します。ソフトウェア更新後の装置再起動時に，SFU，PRU，および NIF のソフトウェアを，更新したソフトウェアと同じバージョンのソフトウェアに自動で更新します。

13.3.3　BCU 初期導入ソフトウェアからのアップデートの手順

運用コマンド update software または restore で，ソフトウェアを更新できます。restore コマンドを使用する場合には，あらかじめ運用コマンド backup で，ソフトウェアを含むバックアップを作成しておく必要があります。

BCU 初期導入ソフトウェアからのアップデートは，BCU 一重化構成と BCU 二重化構成で手順が異なります。構成に合った手順で，ソフトウェアを更新してください。

(1)　BCU 一重化構成の場合

BCU 初期導入ソフトウェアからのアップデートでソフトウェアを更新したあと，装置を自動で再起動して新しいソフトウェアを反映します。再起動時に，BCU 以外の各ボードのソフトウェアも自動で更新および反映します。

(2)　BCU 二重化構成の場合

先に待機系 BCU のソフトウェアを更新してから，運用系 BCU のソフトウェアを更新します。その後，装置を再起動して新しいソフトウェアを反映します。再起動時に，BCU 以外の各ボードのソフトウェアも自動で更新および反映します。

13.3.4　BCU 初期導入ソフトウェアからのアップデートに関する注意事項

(1)　電源に関する注意事項

BCU 初期導入ソフトウェアからのアップデートの実行中は，電源を OFF にしないでください。

(2)　BCU 以外の各ボードに関する注意事項

BCU 初期導入ソフトウェアでは，BCU 以外のボードを起動しません。そのため，運用コマンド show system を実行すると，これらのボードに対して notsupport と表示されることがあります。

この状態で，待機系 BCU のソフトウェアを更新して系切替した場合，旧運用系 BCU で notsupport と表示されていたボードは新運用系 BCU でも notsupport のままとなります。その場合は，装置を再起動して各ボードを起動してください。

(3)　コンフィグレーションに関する注意事項

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，ソフトウェア更新後にも引き継がれます。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。

13.4　BCU 初期導入ソフトウェアからのアップデートのオペレーション

ここでは，update software コマンドを使用したオペレーションについて説明します。restore コマンドについては，「12.5　運用情報のバックアップ・リストア」を参照してください。

13.4.1　運用コマンド一覧

BCU 初期導入ソフトウェアからの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 13-5　運用コマンド一覧

コマンド名	説明
update software	指定したソフトウェアを更新します。
restore	MC およびリモートの 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。

13.4.2　アップデートファイルの準備

1. show flash コマンドを実行してください。

   BCU1 および BCU2 の内蔵フラッシュメモリのユーザ領域（user）に，次に示す値以上の未使用容量（free）があることを確認します。

   アップデートファイルのサイズ－「/usr/var/update/k.img」のサイズ＋ 10MB

2. 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）に置いてください。

   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，マネージメントポート経由で接続して，バイナリモードで転送してください。

   なお，FTP を使用するための設定については，「7.2.3　本装置への IP アドレスの設定」および「7.2.5 ftp によるログインを許可する」を参照してください。

3. ls -l /usr/var/update コマンドを実行してください。

   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ます。

4. show system コマンドを実行してください。

   ソフトウェア更新対象の BCU の動作状態が，「active」または「standby」であることを確認します。

   なお，待機系 BCU の動作状態に次の内容が表示されることがありますが，運用系 BCU と待機系 BCU でコンフィグレーションまたはバージョンが異なるために表示されるもので，異常ではありません。

   - configuration discord
   - software version discord

13.4.3　アップデートコマンドの実行

BCU 一重化構成と BCU 二重化構成で手順が異なります。

(1)　一重化構成でのアップデート

1. cd /usr/var/update コマンドを実行してください。
2. enable コマンドを実行してください。

装置管理者モードに移行します。

3. update software k.img active コマンドを実行してください。

更新されるソフトウェアのバージョンと，更新後のソフトウェアのバージョンが表示されて，ソフトウェアを更新します。更新したあと，装置が再起動します。

装置の再起動時に更新後のソフトウェアと各ボードのソフトウェアのバージョンが異なる場合，各ボードのソフトウェアを自動で更新および反映します。その場合には，各ボードが自動で再起動します。

再起動したら再度ログインして，「13.4.4　アップデート後の確認」に進んでください。

(2)　二重化構成でのアップデート

1. cd /usr/var/update コマンドを実行してください。
2. enable コマンドを実行してください。

装置管理者モードに移行します。

3. update software no-reload k.img standby コマンドを実行してください。

待機系 BCU のソフトウェアを更新します。更新されるソフトウェアのバージョンと，更新後のソフトウェアのバージョンが表示されます。

更新したあと，待機系 BCU は自動で再起動しません。コマンドが正常に終了したことを確認して，次に進んでください。

4. show version コマンドを実行してください。

待機系 BCU のソフトウェアが更新されていることを確認します。待機系 BCU のソフトウェア型名の括弧内に表示されているバージョンが，更新後のソフトウェアのバージョンであることを確認してください。

```
# show version
Date 20XX/XX/XX 00:00:00 UTC
                    :
BCUX: AX-F8600-XXX [XXXXXX, XXXXXXXXXXXXXXXXXXXXXX]
      AX-P8600-X0, BOOT-OS-X, Ver.1.1 (Ver.12.4)
                    :
```

5. update software no-reload k.img active コマンドを実行してください。

運用系 BCU のソフトウェアを更新します。更新されるソフトウェアのバージョンと，更新後のソフトウェアのバージョンが表示されます。

更新したあと，運用系 BCU は自動で再起動しません。コマンドが正常に終了したことを確認して，次に進んでください。

6. show version コマンドを実行してください。

運用系 BCU のソフトウェアが更新されていることを確認します。運用系 BCU のソフトウェア型名の括弧内に表示されているバージョンが，更新後のソフトウェアのバージョンであることを確認してください。

```
# show version
Date 20XX/XX/XX 00:00:00 UTC
                    :
BCUX: AX-F8600-XXX [XXXXXX, XXXXXXXXXXXXXXXXXXXXXX]
      AX-P8600-X0, BOOT-OS-X, Ver.1.1 (Ver.12.4)
                    :
```

7. reload no-dump-image コマンドを実行してください。

装置を再起動します。

装置の再起動時に更新後のソフトウェアと各ボードのソフトウェアのバージョンが異なる場合，各ボードのソフトウェアを自動で更新および反映します。その場合には，各ボードが自動で再起動します。

再起動したら再度ログインして，「13.4.4　アップデート後の確認」に進んでください。

13.4.4　アップデート後の確認

BCU 一重化構成と BCU 二重化構成で手順が異なります。

(1)　一重化構成での確認

1. show version コマンドを実行してください。
   BCU のバージョンが期待したバージョンと同一であることを確認します。

(2)　二重化構成での確認

BCU 二重化構成では，これまでのアップデート手順によって，運用系 BCU と待機系 BCU が入れ替わっていることがあるため注意してください。

1. show version コマンドを実行してください。
   運用系 BCU のバージョンが期待したバージョンと同一であることを確認します。
2. show system コマンドを実行してください。
   - 「Hardware information」欄で，待機系 BCU の動作状態に「software version discord」が表示されていないことを確認します。
   - 「Hardware information」欄で，待機系 BCU の動作状態に「configuration discord」が表示されている場合，コンフィグレーションコマンド save を実行してください。

13.5　オプションライセンスの解説

13.5.1　概要

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なライセンスです。付加機能ごとにオプションライセンスを提供します。オプションライセンスが設定されていない場合，付加機能を使用できません。

オプションライセンスは，ライセンスキーを記述した「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」または「ソフトウェア使用条件書」で提供します。なお，オプションライセンスは次のルールに従います。

- 装置に対応したオプションライセンスが必要です。
- 一つのオプションライセンスは，同一装置内でだけ設定できます。
- ある機能のオプションライセンスを設定済みの状態で，異なる機能のオプションライセンスを追加で設定できます。

13.5.2　オプションライセンスを含むコンフィグレーションの操作

オプションライセンスの設定情報は，装置のコンフィグレーションに保存されます。コンフィグレーションの操作ごとのオプションライセンスの扱いは次のとおりです。

(1)　コンフィグレーションのコピー

運用コマンド copy の実行時，コピー元がコンフィグレーションファイルでコピー先がスタートアップコンフィグレーションの場合，コピー元に設定されているオプションライセンスは無視されて，ランニングコンフィグレーションに設定されているオプションライセンスがスタートアップコンフィグレーションに設定されます。コピー元のコンフィグレーションファイルにオプションライセンスを必要とする機能のコンフィグレーションコマンドが設定されている場合は，コンフィグレーションコマンド license を使用して該当するオプションライセンスをランニングコンフィグレーションに設定してから，copy コマンドを実行してください。

(2)　初期導入時のコンフィグレーションに戻す

運用コマンド erase configuration では，指定しないかぎりオプションライセンスを削除しません。license パラメータを指定すると，オプションライセンスを削除します。

(3)　テンプレート

テンプレートには，コンフィグレーションコマンド license を登録できません。

オプションライセンスを必要とする機能のコンフィグレーションコマンドが登録されているテンプレートを反映する場合は，あらかじめ該当するオプションライセンスを設定しておいてください。また，オプションライセンスを必要とする機能のコンフィグレーションコマンドを登録，修正，または削除してテンプレートを編集する場合も，あらかじめ該当するオプションライセンスを設定しておいてください。

(4)　マージ

コンフィグレーションコマンド load の実行時，マージ元のコンフィグレーションファイルに設定されているオプションライセンスは無視されます。マージ元のコンフィグレーションファイルにオプションライセンスを必要とする機能のコンフィグレーションコマンドが設定されている場合は，コンフィグレーションコ

マンド license を使用して該当するオプションライセンスをランニングコンフィグレーションに設定してから，load コマンドを実行してください。

13.5.3　装置交換時のオプションライセンス再設定

装置を交換した場合，オプションライセンスを再設定するには，次に示す操作のうちどれかが必要です。

- コンフィグレーションコマンドによるオプションライセンスの再設定
- あらかじめ作成しておいたバックアップファイルからの運用情報の復旧（一重化構成で BCU を交換した場合）
- コンフィグレーションの同期（二重化構成で BCU を 1 枚だけ交換した場合）
- あらかじめ作成しておいたバックアップファイルからの運用情報の復旧と，コンフィグレーションの同期（二重化構成で BCU を 2 枚交換した場合）

バックアップファイルの作成には運用コマンド backup を使用します。また，復旧には運用コマンド restore を使用します。

なお，ソフトウェアのバージョンアップ時は，オプションライセンスの再設定は不要です。

13.5.4　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が設定されている場合，コマンド入力で，該当する機能のコマンド名を補完します。ただし，オプションライセンスを設定した直後は補完できません。補完できるようにするには，いったん装置からログアウトしたあと，再度ログインしてください。

13.6　オプションライセンスのコンフィグレーション

13.6.1　コンフィグレーションコマンド一覧

オプションライセンス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 13-6　コンフィグレーションコマンド一覧

コマンド名	説明
license	オプションライセンスを設定します。

13.6.2　オプションライセンスの設定

オプションライセンスは，license コマンドでライセンスキーを指定して設定します。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」または「ソフトウェア使用条件書」に記載されているものを使用してください。

オプションライセンスの設定手順を次に示します。

1. 現在のオプションライセンスの設定状況を確認します。

```
> enable
# show license
Date 20XX/06/13 19:30:52 UTC
No optional license information exists.
```

2. オプションライセンスを設定します。

設定するオプションライセンスのライセンスキーを指定してください。ライセンスキーの大文字と小文字は区別しません。また，ハイフン（-）を省略した形式でもライセンスキーを指定できます。

```
# configure
(config)# license 1012-3abc-0014-0000-0123-4567-89ab-cdef
(config)#
```

コマンド実行時にエラーメッセージ「The license key is invalid.」が表示された場合，指定したライセンスキーが正しくありません。正しいライセンスキーを指定して再実行してください。

3. 運用コマンド show license で，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。

```
# show license
Date 20XX/06/13 19:31:50 UTC
    Serial Number        Licensed software
    1012-3abc-0014-0000  OP-SHPS(AX-P8600-XX)
#
```

設定したライセンスキーの先頭 16 桁が表示されます。

13.6.3　オプションライセンスの削除

使用しなくなったオプションライセンスは，コンフィグレーションから削除できます。

オプションライセンスの削除手順を次に示します。

1. 現在のオプションライセンスの設定状況を確認します。

```
> enable
# show license
Date 20XX/06/13 19:40:10 UTC
    Serial Number        Licensed software
    1012-3abc-0014-0000  OP-SHPS(AX-P8600-XX)
```

2. オプションライセンスを削除します。

削除するオプションライセンスのシリアル番号を指定してください。シリアル番号は，運用コマンド show license で表示される 16 桁の英数字です。シリアル番号の大文字と小文字は区別しません。また，ハイフン（-）を省略した形式でもシリアル番号を指定できます。

```
# configure
(config)# no license 1012-3abc-0014-0000
This serial number enables OP-SHPS.
Do you want to delete the license for 1012-3abc-0014-0000? (y/n):
```

コマンド実行時にエラーメッセージ「Deletion is not possible because a function that requires the optional license of the specified serial number is enabled.」が表示された場合，指定したオプションライセンスを必要とする機能が有効なままです。その機能を有効にするコンフィグレーションを削除してから，再実行してください。

3. 削除の確認メッセージに対して，“y”を入力します。

```
Do you want to delete the license for 1012-3abc-0014-0000? (y/n): y
(config)#
```

4. 運用コマンド show license で，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。

```
# show license
Date 20XX/06/13 19:40:48 UTC
No optional license information exists.
#
```

13.7　オプションライセンスのオペレーション

13.7.1　運用コマンド一覧

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 13-7　運用コマンド一覧

コマンド名	説明
show license	装置に設定されたオプションライセンス情報を表示します。

13.7.2　オプションライセンスの確認

show license コマンドで，本装置に設定されているオプションライセンス情報を表示します。シリアル番号とソフトウェア名を確認してください。次の図に例を示します。

図 13-3　オプションライセンスの確認

```
> enable
# show license
Date 20XX/06/13 19:40:10 UTC
    Serial Number        Licensed software
    1012-3abc-0014-0000  OP-SHPS(AX-P8600-XX)
#
```

14 装置の冗長化

この章では，本装置での冗長構成について説明します。

14.1　BCU 二重化の解説

14.1.1　概要

(1)　装置構成

基本制御機構（BCU）を二重化する場合，BCU を 2 枚搭載します。2 枚のボードがそれぞれ運用系 BCU，待機系 BCU として動作します。BCU を二重化することで，障害に対する信頼性を高められます。運用系 BCU に障害が発生した場合は運用系 BCU と待機系 BCU を切り替えて，待機系 BCU が新運用系 BCU となって運用を始めます。

(2)　二重化を構成する条件

BCU を二重化で運用するための条件を次に示します。すべての条件を満たすと，系切替ができます。

- 運用系 BCU が正常に起動している
- 待機系 BCU が正常に起動している
- 両系 BCU のコンフィグレーションが同期できている

どれかの条件を満たせない場合，システムメッセージを出力して警告します。条件を満たすためにはシステムメッセージの記載に従って対応してください。

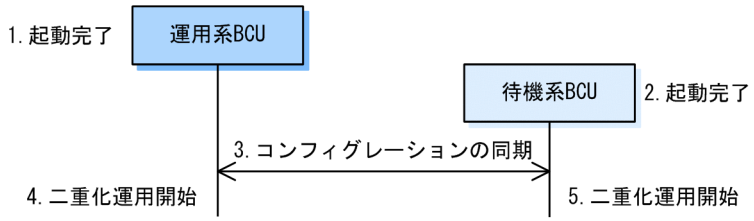
14.1.2　動作

本装置では，BCU の搭載枚数が 1 枚の場合，一重化構成で動作します。

BCU の搭載枚数が 2 枚の場合，一方は待機系 BCU として起動します。その後，二重化を構成するための条件を満たすと，システムメッセージ（メッセージ種別：BCU，メッセージ識別子：01101006）を表示して二重化構成での運用を開始します。

BCU の搭載枚数が 2 枚でも待機系 BCU の起動が完了するまで，一重化構成で動作します。一重化から二重化へ，または二重化から一重化へ構成が変化しても，通信への影響はありません。一重化から二重化で運用開始するまでの流れを次の図に示します。

図 14-1　二重化構成での運用開始時の動作



1. 運用系 BCU だけで一重化運用
2. 待機系 BCU の起動が完了
3. 運用系 BCU と待機系 BCU のコンフィグレーションの同期が完了
4. 運用系 BCU は二重化で運用が開始されたことをシステムメッセージで表示
5. 待機系 BCU は二重化で運用が開始されたことをシステムメッセージで表示

BCU を 2 枚搭載してから装置の電源を入れて起動する場合，BCU1 が運用系として動作して，BCU2 は待機系として運用を開始します。

14.1.3　ユーザの設定情報および利用情報の同期

運用系 BCU と待機系 BCU の間で同期するユーザの設定情報および利用情報を次の表に示します。同期した情報は待機系 BCU の動作にも適用されて，系切替後も矛盾が発生することなく運用できます。

表 14-1　運用中に同期するユーザの設定情報および利用情報

ユーザの設定情報および利用情報	同期する契機	同期状態確認コマンド
ランニングコンフィグレーションおよび編集中のコンフィグレーション	• 二重化運用開始時 • コンフィグレーション変更時	運用コマンド show system
スタートアップコンフィグレーション	• 次のコマンドによるスタートアップコンフィグレーション更新時 ・コンフィグレーションコマンド save ・コンフィグレーションコマンド commit ・運用コマンド copy ・運用コマンド erase configuration • 運用コマンド synchronize 実行時	
ホームディレクトリ下で作成したファイル	• 運用コマンド synchronize 実行時（userfile パラメータ指定時だけ）	運用コマンド synchronize（diff パラメータ指定）
インストールした Python スクリプトファイル	• 運用コマンド install script 実行時 • 運用コマンド uninstall script 実行時 • 運用コマンド synchronize 実行時	

14.1.4　系切替

本装置は BCU を二重化構成で運用している場合，運用コマンド redundancy force-switchover の実行や運用系 BCU の障害などによって運用系 BCU が切り替わります。

コマンドで系切替をすると，コマンドを実行した系は系切替後に待機系 BCU として動作します。系切替の準備ができていない場合などは，コマンドによる系切替が抑止されます。

二重化構成の状態は，「表 14-1　運用中に同期するユーザの設定情報および利用情報」の同期状態確認コマンドで確認できます。起動が完了しない，または系切替の準備ができていない場合は，次の方法で対応してください。

- 運用コマンド show logging を使用して，システムメッセージに従って対応する
- 「トラブルシューティングガイド」に従って対応する

なお，系切替をすると，リモート接続しているユーザはすべてログアウトします。このとき，リモート接続しているユーザが実行中のコマンドは終了するため，切り替え後にログインして再実行してください。

(1)　通信無停止対応機能一覧

通信無停止機能をサポートする機能を次の表に示します。通信無停止機能をサポートしている機能は，系切替時でも各機能が停止しないで動作するため，系切替後も通信を維持できます。運用管理，ネットワーク監視，およびネットワーク管理の機能の一部では，系切替時にプロトコル状態が初期状態に戻っても，通信を

維持できます。通信無停止機能を未サポートの機能は系切替後再学習をするため，ネットワーク情報が再構築されるまでの間通信が中断します。

通信無停止機能の対応状況を次の表に示します。

表 14–2　系切替時の通信無停止機能サポート状況※1

分類	機能	通信無停止可否
運用管理	マネージメントポート	×
	telnet，ssh，ftp	×
	NTP/SNTP	○※2
	RADIUS/TACACS+	×
	SNMP	○
ネットワークインタフェース	全 NIF 共通	○
リンクアグリゲーション	スタティック	○
	LACP	○
	スタンバイリンク　リンクダウンモード	○
	スタンバイリンク　非リンクダウンモード	○
	異速度混在モード	○
	切り戻し抑止	○※3
MAC アドレス学習・VLAN	MAC アドレス学習	○
	ポート VLAN	○
	VLAN トンネリング	○
	Tag 変換	○
	アイソレート VLAN	○
	VLAN debounce	○
スパニングツリー	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	×
Ring Protocol	Ring Protocol	○
IGMP/MLD snooping	IGMP/MLD snooping	○
フィルタ・QoS	フィルタ・QoS	○
	アクセスリストロギング	○
ネットワーク監視機能	L2 ループ検知	×※4
	ストームコントロール	○

分類	機能		通信無停止可否
	トラッキング機能		○
ネットワークの管理	ポートミラーリング		○
	ポリシーベースミラーリング		○
	sFlow 統計（フロー統計）		○
	IEEE802.3ah OAM	UDLD	○※2
		ループ検出	○※2
	CFM		○※2
	LLDP		○※2
IP パケット中継	IPv4，ARP		○
	IPv6，NDP		○
	ポリシーベースルーティング		○※5
	RA		○
	DHCP/BOOTP リレーエージェント		○
	DHCPv6 リレーエージェント		○
	VRRP		×
ユニキャストルーティングプロトコル	スタティックルーティング		○
	RIP，RIP2，RIPng		×
	OSPF，OSPFv3		○※6
	BGP4，BGP4+		○※6
IPv4 マルチキャストルーティングプロトコル	PIM-SM		○※7
	PIM-SSM		○※7
IPv6 マルチキャストルーティングプロトコル	PIM-SM		×
	PIM-SSM		○※7
ネットワーク経路監視機能	BFD		○

（凡例）○：サポート　×：未サポート

注※1

各機能が提供するプロトコルの統計情報は系切替後に新運用系 BCU にてクリアされます。

注※2

各機能が提供するプロトコルの状態は初期状態から開始となります。

注※3

系切替後，再度切り戻し抑止設定時間が経過するまで，切り戻し抑止状態は継続されます。

注※4

系切替前に inactive 状態になったポートは，系切替後自動的に active 状態になりません。

注※5

系切替後のネクストホップの選択抑止中は，系切替前に選択していたネクストホップに中継することで通信を継続します。

注※6

ユニキャストルーティング高可用機能を使用した場合です。

注※7

無停止マルチキャスト中継機能を使用した場合です。ただし，マルチキャストエクストラネットのマルチキャスト中継エントリは対象外です。

(2)　コンフィグレーション不一致時の動作

BCU の増設や交換時など，運用系 BCU と待機系 BCU でコンフィグレーションに差分が発生する場合があります。この状態で系が切り替わると，運用中のハードウェア設定と新運用系 BCU のコンフィグレーションが異なり動作が矛盾するおそれがあります。

このため，本装置では運用系 BCU と待機系 BCU 間のコンフィグレーションで不一致を検出すると，システムメッセージを出力します。また，起動時のコンフィグレーションに差分がある場合も同様に，システムメッセージを出力します。コンフィグレーションの同期によって不一致が解消すると，一致した旨のシステムメッセージを出力します。なお，コンフィグレーションの同期処理中は，一時的にコンフィグレーションの編集が抑止されます。

(3)　Python スクリプトファイル不一致時の動作

BCU の増設や交換時など，運用系 BCU と待機系 BCU でインストールされている Python スクリプトファイルに不一致が発生する場合があります。この状態で系が切り替わると，旧運用系 BCU で起動していた Python スクリプトファイルが新運用系 BCU に存在しない場合，起動できません。

このため，本装置では運用系 BCU と待機系 BCU 間でインストールされている Python スクリプトファイルの不一致を検出すると，システムメッセージを出力します。また，常駐スクリプトおよびイベント起動スクリプトについて，起動試行時にファイルが存在しない場合も，起動不可を示すシステムメッセージを出力します。

「表 14-1　運用中に同期するユーザの設定情報および利用情報」の同期する契機を確認して，Python スクリプトファイルを一致させてください。

14.1.5　BCU 二重化構成使用時の注意事項

(1)　ログインに関する注意事項

運用端末の接続形態によって，次のようにログインできる系が異なります。

- シリアル接続ポート

  運用系 BCU および待機系 BCU のそれぞれにコンソールを接続してログインできます。

- マネージメントポート

  運用系 BCU のマネージメントポートを使用してログインできます。待機系 BCU のマネージメントポートからはログインできません。

- 通信用ポート

  リモート運用端末から通信用ポートを経由してログインする場合は，運用系 BCU にログインします。待機系 BCU にはログインできません。

- シリアル接続ポート（AUX）にダイアルアップ IP 接続

リモート運用端末からダイアルアップ IP 接続してログインする場合は，運用系 BCU および待機系 BCU にログインできます。

(2)　系切替時の注意事項

系切替時，次のどちらかのシステムメッセージが出力されるまでの間，運用コマンドでの表示情報および MIB で取得する情報に系切替後の状態が反映されないことがあります。

- メッセージ種別：BCU，メッセージ識別子：0110100d
- メッセージ種別：BCU，メッセージ識別子：0110100e

14.2　BCU 二重化のオペレーション

14.2.1　運用コマンド一覧

BCU 二重化に関する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
inactivate bcu standby	待機系 BCU を停止します。
activate bcu standby	待機系 BCU を起動します。
redundancy force-switchover	運用系 BCU と待機系 BCU を切り替えます。
synchronize	待機系 BCU のユーザの設定情報および利用情報を，運用系 BCU の内容に同期します。
show system※1	BCU の運用状態を表示します。
reload※1	BCU を再起動します。
show logging※2	運用系 BCU または待機系 BCU の運用ログを表示します。

注※1
「運用コマンドレファレンス Vol.1　11. 装置とソフトウェアの管理」を参照してください。

注※2
「運用コマンドレファレンス Vol.1　17. ログの管理」を参照してください。

14.2.2　待機系 BCU の状態確認

show system コマンドで待機系 BCU の状態を確認できます。また，show logging コマンドの standby パラメータを指定すると，待機系 BCU の運用ログを表示できます。ただし，障害などによって待機系 BCU が起動できない場合は運用ログを表示できません。

14.2.3　BCU の再起動

reload コマンドで standby パラメータを指定すると，待機系 BCU を再起動できます。また，active パラメータを指定すると運用系 BCU を再起動できます。この場合，系切替をして新待機系 BCU となった BCU が再起動します。

すべてのパラメータを省略した場合は，装置が再起動します。

14.2.4　BCU の交換

二重化運用中に待機系 BCU を交換することで，装置の運用を停止しないで BCU を交換できます。交換対象となる待機系 BCU を inactivate bcu standby コマンドで停止してから交換してください。運用系 BCU を交換する場合は，あらかじめ redundancy force-switchover コマンドで系切替をしてから交換してください。交換作業完了後，activate bcu standby コマンドを実行すると待機系 BCU を起動します。

14.2.5　ユーザの設定情報および利用情報の同期の実施

運用中に「表 14-1　運用中に同期するユーザの設定情報および利用情報」で示す情報が両系間で不一致になった場合，同期する契機を確認して情報を一致させてください。

14.2.6　系切替の実施

二重化構成で運用している場合，運用系 BCU から redundancy force-switchover コマンドを実行すると運用系 BCU を切り替えられます。

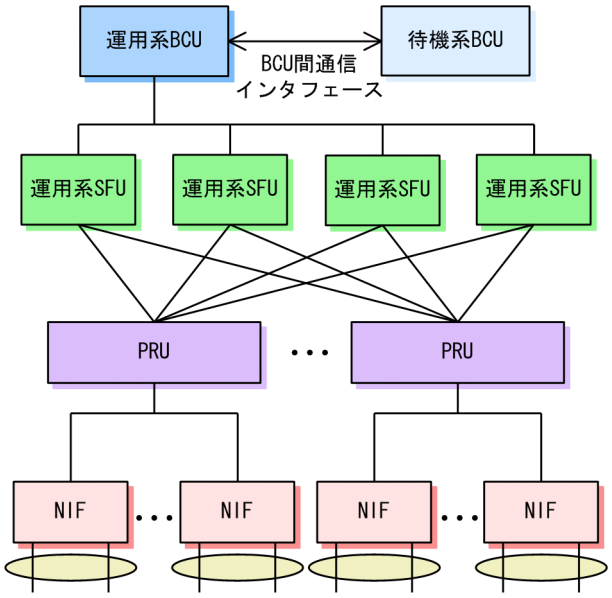
14.3　SFU 冗長化の解説

14.3.1　冗長化時の装置構成

スイッチファブリック機構（SFU）を冗長化する場合，SFU を 2 枚以上搭載します。SFU の冗長化では，すべての SFU が運用系として稼働します。冗長構成時に SFU に障害が発生した場合，運用系として稼働しているほかの SFU を使用して通信を継続します。なお, SFU を 3 枚以上搭載することでパケット転送性能を最大にできます。

BCU-SFU-PRU-NIF 間の冗長構成でのインタフェースを次の図に示します。運用系 SFU はそれぞれ独立したインタフェースで PRU と接続して，パケットを転送します。

図 14–2　BCU-SFU-PRU-NIF 間の冗長構成でのインタフェース



14.3.2　冗長構成の運用方法

すべての SFU が運用系として稼働します。3 枚以上の SFU を運用系にすると, パケット転送性能を最大にします。4 枚の SFU を運用系にした場合，障害発生時にパケット転送性能を維持します。

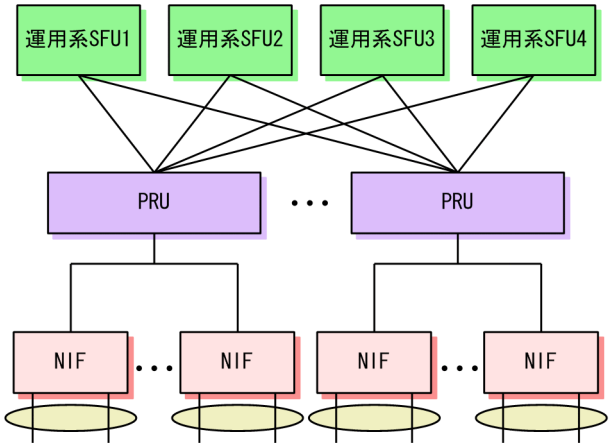
14.3.3　障害発生時の SFU 動作

冗長構成時に SFU に障害が発生した場合，ほかの正常な SFU を使用して通信を継続します。障害発生時の動作例を次に示します。

障害発生前

動作状態が稼働中の SFU が 4 枚で動作しています。障害発生前の動作を次の図に示します。

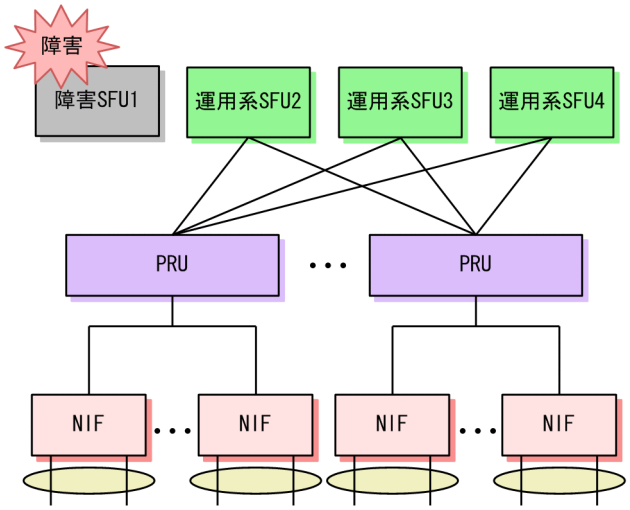
図 14-3　障害発生前の動作



障害発生後

SFU1 に障害が発生した場合，障害が発生していない SFU で動作し続けます。障害発生後の動作を次の図に示します。

図 14-4　障害発生後の動作



14.4　SFU 冗長化のオペレーション

14.4.1　運用コマンド一覧

SFU 冗長化に関する運用コマンド一覧を次の表に示します。

表 14-4　運用コマンド一覧

コマンド名	説明
show system※	SFU の動作状態を表示します。

注※

「運用コマンドレファレンス Vol.1　11. 装置とソフトウェアの管理」を参照してください。

14.4.2　SFU の状態確認

show system コマンドで SFU の動作状態を確認できます。次の図に例を示します。

図 14-5　SFU の動作状態の確認

```
> show system
Date 20XX/12/10 15:11:20 UTC
System: AX8632R, OS-RE, Ver.12.1, [123.1]
               :
               :
    SFU1 : active (restart required), fatal error restart 0 time
        Elapsed time : 2 days 2:30
        Lamp : STATUS LED = green , ACTIVE LED = light off
    SFU2 : notconnect
               :
    SFU4 : active, fatal error restart 0 time
        Elapsed time : 2 days 2:30
        Lamp : STATUS LED = green , ACTIVE LED = light off
               :
>
```

14.5　電源機構（PS）冗長化の解説

14.5.1　概要

本装置は予備の PS を搭載することで，PS を冗長化できます。PS を冗長化すると，一部の PS で障害が発生して電力供給が停止しても，自動的に残りの PS で電力の負荷バランスをとることで電力を安定供給できます。また，障害となった PS は装置を運用したままで交換できます。

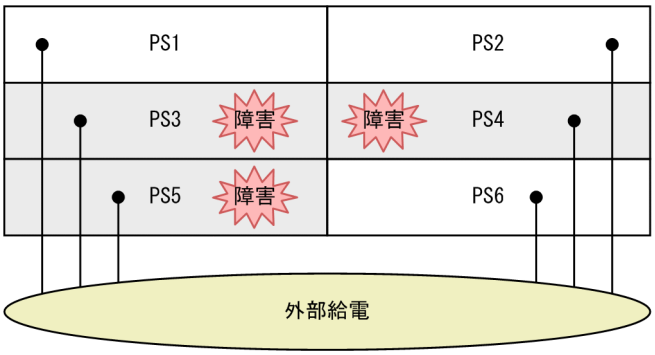
本装置は PS の冗長化方式として，電源ユニット冗長と給電系統冗長をサポートしています。

PS 障害などによって PS が冗長構成でなくなった場合，コンフィグレーションコマンド power redundancy-mode を設定しているとシステムメッセージを出力および SNMP 通知を送信します。冗長構成で運用を継続したい場合は，PS を交換または増設してください。PS の交換，増設，および移設作業については，「ハードウェア取扱説明書」を参照して，注意事項を遵守してください。

14.5.2　電源ユニット冗長

装置の運用に必要な PS の個数に対して，予備の PS を 1 個以上搭載して運用する方式です。一部の PS が故障しても残りの PS で給電を継続します。なお，故障した PS の搭載位置に関係なく，必要な個数以上の PS が動作していれば運用を継続できます。電源ユニット冗長の構成例を次の図に示します。

図 14-6　電源ユニット冗長の構成例



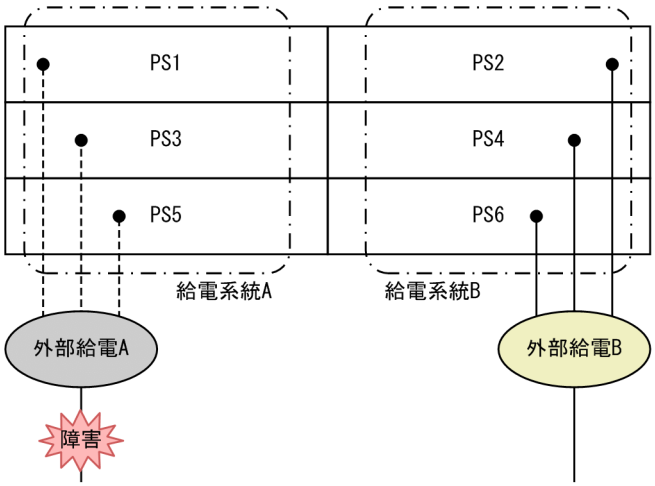
6 個の PS を搭載していて運用に必要な PS が 3 個の場合, 3 個の PS に障害が発生しても運用を継続できます。

PS に障害が発生して PS が冗長構成でなくなったり，障害から回復して冗長構成になったりした場合には，システムメッセージを出力および SNMP 通知を送信します。

14.5.3　給電系統冗長

装置の運用に必要な PS の個数と同数の予備を搭載して，PS を二つのグループに分けて外部給電系統に接続して運用する方式です。電源ユニット冗長と同様に，運用に必要な個数の PS と予備の PS が動作していれば，一部の PS が故障しても残りの PS で給電を継続します。また，一方の外部給電系統からの給電が停止しても, もう一方の外部給電系統から装置への給電を継続します。給電系統冗長の構成例を次の図に示します。

図 14-7　給電系統冗長の構成例



外部給電系統には 2 系統あり，それぞれの系統に接続できる PS は搭載位置が決まっています。給電系統冗長での PS の搭載位置を次の表に示します。

表 14-5　給電系統冗長での PS の搭載位置

モデル	給電系統 A	給電系統 B
AX8608R	PS1	PS2
AX8616R	PS1，PS3	PS2，PS4
AX8632R	PS1，PS3，PS5	PS2，PS4，PS6

PS に障害が発生して PS が冗長構成でなくなったり，障害から回復して冗長構成になったりした場合には，システムメッセージを出力および SNMP 通知を送信します。また，一方の外部給電系統に障害が発生して給電系統が冗長構成でなくなったり，障害から回復して冗長構成になったりした場合にも，システムメッセージを出力および SNMP 通知を送信します。

14.5.4　供給電力の管理

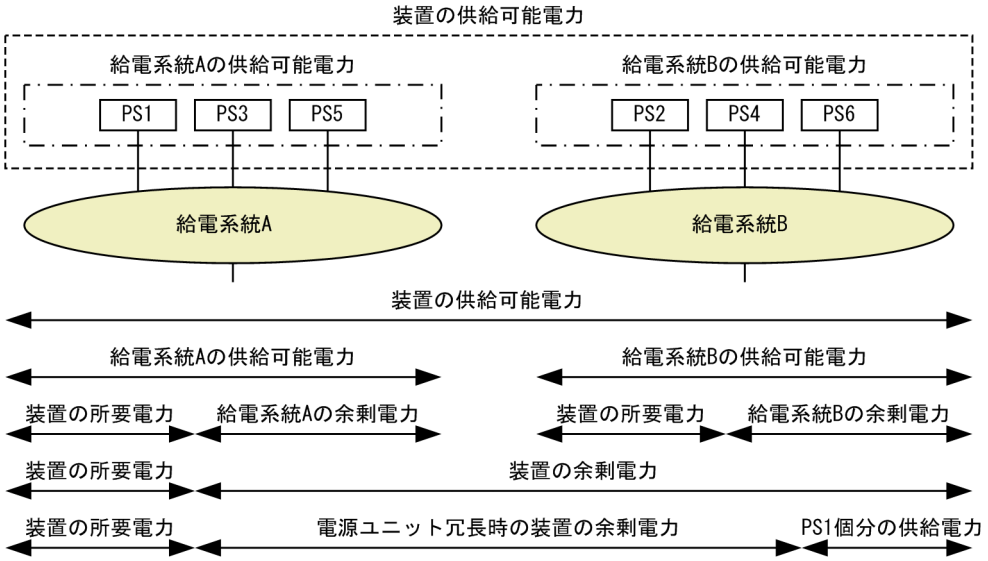
本装置では PS や，PRU および NIF の搭載状態に応じて供給電力を管理します。供給電力の管理に関する用語を次に示します。

表 14-6　供給電力の管理に関する用語

用語	意味
装置の供給可能電力	装置に搭載されて，正常に給電している PS の供給電力の総和。
給電系統 A の供給可能電力	給電系統 A に搭載されて，正常に給電している PS の供給電力の総和。
給電系統 B の供給可能電力	給電系統 B に搭載されて，正常に給電している PS の供給電力の総和。
装置の所要電力	装置の運用に必要な電力。起動していない PRU および NIF の必要電力は含まれません。
装置の余剰電力	電源ユニット冗長および給電系統冗長が不要なときに，本装置で余分に使用できる電力（「装置の供給可能電力」から「装置の所要電力」を除いた電力）。

用語	意味
	マイナスになる場合は，「装置の供給可能電力」が不足しています。
電源ユニット冗長時の装置の余剰電力	電源ユニット冗長を確保した上で，本装置で余分に使用できる電力（「装置の余剰電力」から PS1 個分の供給電力を除いた電力）。 マイナスになる場合は，電源ユニット冗長ができていません。
給電系統 A の余剰電力	給電系統 A で余分に使用できる電力（「給電系統 A の供給可能電力」から「装置の所要電力」を除いた電力）。 マイナスになる場合は，給電系統 A で給電系統冗長ができていません。
給電系統 B の余剰電力	給電系統 B で余分に使用できる電力（「給電系統 B の供給可能電力」から「装置の所要電力」を除いた電力）。 マイナスになる場合は，給電系統 B で給電系統冗長ができていません。

図 14–8　供給電力の管理（PS を 6 個搭載した例）



本装置では次のように動作して供給電力を管理します。

(1)　装置起動時

PRU または NIF を起動させると装置の余剰電力が不足する場合は，システムメッセージを出力および SNMP 通知を送信して PRU または NIF の起動を抑止します。このとき，PRU のスロット単位で抑止します。起動抑止されたボードは電力不足による運用停止状態となります。

(2)　PRU/NIF のボード増設時

PRU または NIF を起動させると装置の余剰電力が不足する場合は，システムメッセージを出力および SNMP 通知を送信して該当するボードの起動を抑止します。起動抑止されたボードは電力不足による運用停止状態となります。

(3)　PS 障害発生時

PS に障害が発生した場合は，PS ごとに PS 障害のシステムメッセージを出力および SNMP 通知を送信します。

PS の障害発生によって装置の余剰電力がマイナスになった場合は，システムメッセージを出力および SNMP 通知を送信して運用を継続します。ただし，PS の数が運用に必要な個数を下回ったときは運用を継続できないおそれがあります。

電源ユニット冗長時の装置の余剰電力がマイナスになって PS 冗長でなくなった場合は，システムメッセージを出力および SNMP 通知を送信します。また，給電系統冗長を構成している状態で，給電系統 A の余剰電力または給電系統 B の余剰電力がマイナスとなって PS 冗長でなくなった場合にも，システムメッセージを出力および SNMP 通知を送信します。

(4) PS 障害回復時

PS が障害から回復した場合は，PS ごとに PS 障害回復のシステムメッセージを出力および SNMP 通知を送信します。

PS の障害回復によって装置の余剰電力が 0 以上になって供給電力不足が解消されても，電力不足による運用停止状態となっている PRU および NIF は自動で起動しません。

電源ユニット冗長時の装置の余剰電力が 0 以上になって PS 冗長になった場合は，システムメッセージを出力および SNMP 通知を送信します。また，給電系統冗長を構成している状態で，給電系統 A の余剰電力または給電系統 B の余剰電力が 0 以上になって PS 冗長になった場合にも，システムメッセージを出力および SNMP 通知を送信します。

14.6　電源機構（PS）冗長化のコンフィグレーション

14.6.1　コンフィグレーションコマンド一覧

電源機構（PS）冗長化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 14-7　コンフィグレーションコマンド一覧

コマンド名	説明
power redundancy-mode	電源冗長の監視モードを設定します。 指定された電源冗長の監視モードに従って，PS が冗長構成になった場合，または冗長構成でなくなった場合にシステムメッセージを表示します。

14.6.2　電源ユニット冗長の設定

電源ユニット冗長の構成で使用する場合，電源ユニットが冗長構成になったときや，冗長構成でなくなったときに，システムメッセージを出力および SNMP 通知を送信できます。

[設定のポイント]

電源ユニット冗長のシステムメッセージを表示させるには，power redundancy-mode コマンドで電源冗長の監視モードとして電源ユニット冗長を指定する必要があります。

[コマンドによる設定]

1. **(config)# power redundancy-mode 1**
   電源冗長の監視モードとして，電源ユニット冗長を設定します。

14.6.3　給電系統冗長の設定

給電系統冗長の構成で使用する場合，本装置は電源ユニット冗長による PS の冗長化の確認に加えて，給電系統の冗長化を確認します。給電系統が冗長構成になった場合や，冗長構成でなくなった場合に，システムメッセージを出力および SNMP 通知を送信できます。

[設定のポイント]

給電系統冗長のシステムメッセージを表示させるには，power redundancy-mode コマンドで電源冗長の監視モードとして給電系統冗長を指定する必要があります。

[コマンドによる設定]

1. **(config)# power redundancy-mode 2**
   電源冗長の監視モードとして，電源ユニット冗長かつ給電系統冗長を設定します。

14.7　電源機構（PS）冗長化のオペレーション

14.7.1　運用コマンド一覧

電源機構（PS）冗長化に関する運用コマンド一覧を次の表に示します。

表 14-8　運用コマンド一覧

コマンド名	説明
show system※	装置の運用状態を表示します。
show environment※	装置の環境情報を表示します。

注※

「運用コマンドレファレンス Vol.1　11. 装置とソフトウェアの管理」を参照してください。

14.7.2　PS の状態確認

show environment コマンドで表示される「Power environment」の項目で，PS 種別，冗長構成，および各 PS の状態を確認できます。

図 14-9　PS の状態確認

```
> show environment
           :
Power environment
    Input voltage: AC200-240V
    Power redundancy mode: 2 (Power Supply + Input Source)
    Power supply redundancy status
        Power supply: active = 4, required = 1 (Redundant)
        Input source: active = 2(from A) 2(from B), required = 1 (Redundant)
    PS1: active
    PS2: active
    PS3: active
    PS4: active
           :
```

確認できる内容を表示項目ごとに説明します。

Power redundancy mode

コンフィグレーションで設定した電源冗長の監視モードが表示されます。

モードが表示されていない場合は，コンフィグレーションが設定されていません。そのため，PS が冗長構成になったときや冗長構成でなくなったときに，システムメッセージを出力したり，SNMP 通知を送信したりしません。

Power supply

装置に給電している PS 数および装置の運用に必要な PS 数を含めた，電源ユニット冗長の状態が表示されます。

装置に給電している PS 数が装置の運用に必要な PS 数以下のときは，電源ユニット冗長になっていません。電源ユニット冗長で運用したい場合は，PS を交換するか，PS を増設してください。

例 1

装置の運用に必要な PS 数が 2，装置に給電している PS 数が 3 の場合（電源ユニット冗長である）

```
Power supply : active = 3                    required = 2 (Redundant)
```

例 2

装置の運用に必要な PS 数が 2，装置に給電している PS 数が 2 の場合（電源ユニット冗長でない）

```
    Power supply : active = 2                    required = 2 (Non-Redundant)
```

Input source

給電系統 A に給電している PS 数，給電系統 B に給電している PS 数，および装置の運用に必要な PS 数を含めた，給電系統冗長の状態が表示されます。

給電系統 A または給電系統 B に給電している PS 数が装置の運用に必要な PS 数未満のときは，給電系統冗長になっていません。給電系統冗長で運用したい場合は，PS を交換するか，PS を増設してください。

例 1

装置を運用するために各給電系統で必要な PS 数が 2，給電系統 A に給電している PS 数が 3，給電系統 B に給電している PS 数が 2 の場合（給電系統冗長である）

```
Input source : active = 3(from A), 2(from B) required = 2 (Redundant)
```

例 2

装置を運用するために各給電系統で必要な PS 数が 2，給電系統 A に給電している PS 数が 3，給電系統 B に給電している PS 数が 1 の場合（給電系統冗長でない）

```
Input source : active = 3(from A), 1(from B) required = 2 (Non-Redundant)
```

PS<ps no.>

各 PS の状態が表示されます。

14.7.3　供給電力の確認

show environment コマンドで表示される「Power usage」の項目で，装置の供給可能電力，所要電力，および余剰電力を確認できます。

図 14-10　電力状況の確認

```
> show environment
          :
Power usage
    Total power capacity:                                  10168.00 W
        Input source A:                                     5084.00 W
        Input source B:                                     5084.00 W
    Total power allocated:                                  1477.00 W
    Total power available for additional boards:            8691.00 W
    Power available (Power supply unit redundant case):     6149.00 W
    Power available (Input source redundant case)
        Input source A:                                     3607.00 W
        Input source B:                                     3607.00 W
            :
```

15 システムメッセージの出力とログの管理

この章では，システムメッセージの出力とログの管理ついて説明します。

15.1　解説

15.1.1　メッセージの出力

本装置では動作情報や障害情報などをシステムメッセージとして通知します。

システムメッセージ，運用コマンド応答メッセージ，およびコンフィグレーションエラーメッセージは運用端末に出力するほか，syslog インタフェースや E-mail 送信機能を使用してネットワーク上の他装置に送信できます。また，システムメッセージは SNMP 通知の機能を使用して，SNMP マネージャに送信できます。これらの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。なお，SNMP 通知によって送信されるシステムメッセージの情報をシステムメッセージトラップと呼びます。

各宛先および運用端末への出力対象は，宛先ごとに適切な条件で指定できます。

syslog 送信では，系切替が発生してから最大 100 件のメッセージを保持します。このとき，送信先の syslog サーバを IP アドレスで指定している場合は指定した syslog サーバに対する通信経路が回復したあと，ホスト名で指定している場合は系切替から 7 分経過したあと，保持したメッセージを送信します。系切替から 7 分経過しても送信先の syslog サーバへの通信経路が回復していないときは，保持したメッセージを廃棄します。

なお，本装置では他装置からの syslog メッセージを受信する機能はサポートしていません。また，本装置で生成した syslog メッセージでは，RFC3164 で定義されている HEADER 部の HOSTNAME 欄は未設定です。

15.1.2　ログの保存

システムメッセージ，運用コマンド応答メッセージ，およびコンフィグレーションエラーメッセージは，運用ログおよび統計ログとして装置内に保存されます。これらの情報で装置の運用状態や障害の発生状況を管理できます。なお，運用ログの保存件数はメッセージ種別ごとに設定できます。運用ログと統計ログの特徴を次に示します。

運用ログ

運用中に発生した事象（イベント）を発生順に記録した情報で，システムメッセージと同様の内容が格納されます。次に示す情報が運用ログとして格納されます。

- 運用コマンドの応答メッセージ
- コンフィグレーションエラーメッセージ
- システムメッセージ

統計ログ

装置内で発生した障害や警告についてのシステムメッセージをメッセージ識別子ごとに分類して，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。

管理者は，運用コマンドでこれらの情報を参照できます。

運用ログと統計ログは，BCU の再起動または停止を契機として，自動的に内蔵フラッシュメモリへ保存されます。しかし，障害による BCU の再起動または停止の場合は，運用ログと統計ログが保存されないことがあります。そのため，syslog メッセージを送信することを推奨します。

15.2　コンフィグレーション

15.2.1　コンフィグレーションコマンド一覧

システムメッセージの出力とログの管理のコンフィグレーションコマンド一覧を次の表に示します。

表 15-1　コンフィグレーションコマンド一覧

コマンド名	説明
logging email	E-mail 送信先の E-mail アドレスを設定します。
logging email-filter	E-mail 送信時の送信条件をメッセージ種別リストおよびイベントレベルで設定します。
logging email-from	E-mail 送信元の E-mail アドレスを設定します。
logging email-interval	E-mail の送信間隔を設定します。
logging email-server	SMTP サーバの情報を設定します。
logging save-count	運用ログの最小保存件数をメッセージ種別ごとに設定します。
logging syslog-facility	syslog 送信データのヘッダ部に付ける facility を設定します。
logging syslog-filter	syslog 送信時の送信条件をメッセージ種別リストおよびイベントレベルで設定します。
logging syslog-host	送信先の syslog サーバを設定します。
logging syslog-severity	syslog 送信データのヘッダ部に付ける severity を設定します。
message-list	メッセージ種別リストを生成します。
message-type	出力条件として制御するメッセージ種別を設定します。
username※1	logging-console パラメータで, システムメッセージの画面出力条件をメッセージ種別リストおよびイベントレベルで設定します。
snmp-server traps※2	system_msg_trap_message_list および system_msg_trap_event_level パラメータで, システムメッセージトラップ送信時の送信条件をメッセージ種別リストおよびイベントレベルで設定します。

注※1

「コンフィグレーションコマンドレファレンス Vol.1　6. ログインセキュリティと RADIUS/TACACS+」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 Vol.1　14. SNMP」を参照してください。

15.2.2　運用ログの最小保存件数の設定

[設定のポイント]

本装置ではメッセージ種別ごとに装置内に保存するログ件数の最小値を設定できます。本設定を使用すると，ログの保存量が保存領域を超えた場合でも設定した数のログを保護できます。なお，ログの保存領域に空きがある場合は，設定値以上のログが保存されます。

[コマンドによる設定]

1. **(config)# logging save-count BCU 3000**
   メッセージ種別 BCU の運用ログを 3000 件保存します。

15.2.3　syslog 出力の設定

[設定のポイント]

syslog 出力機能を使用して，ユーザ入力コマンドおよびメッセージを syslog サーバに送信できます。

[コマンドによる設定]

1. **(config)# logging syslog-host 192.0.2.1**
   送信先の syslog サーバとして IPv4 アドレス 192.0.2.1 を指定します。
2. **(config)# logging syslog-host 2001:db8:1:1::1**
   送信先の syslog サーバとして IPv6 アドレス 2001:db8:1:1::1 を指定します。
3. **(config)# logging syslog-host 192.0.2.1 vrf 2**
   送信先の syslog サーバとして IPv4 アドレス 192.0.2.1，VRF ID 2 を指定します。

15.2.4　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 などに送信できます。

[コマンドによる設定]

1. **(config)# logging email system@example.com**
   送信先の E-mail アドレスとして system@example.com を指定します。
2. **(config)# logging email-server 192.0.2.1**
   E-mail 送信時に使用する SMTP サーバのアドレスとして 192.0.2.1 を指定します。

15.2.5　メッセージの出力制御

本装置では，運用端末のコンソール画面や syslog サーバなど，出力先に応じてメッセージの出力条件を設定できます。

(1)　メッセージ種別リストの作成例

[設定のポイント]

出力対象および出力抑止対象とするメッセージ種別を設定したメッセージ種別リストを作成します。

各出力条件を設定するとき，出力抑止対象を設定したメッセージ種別リストを出力条件として設定すると，指定したメッセージ種別以外が出力対象になります。また，イベントレベルの指定を省略するとイベントレベルの数値が 6 以下のメッセージが，メッセージ種別リストの指定を省略するとすべてのメッセージ種別が出力対象となります。

[コマンドによる設定]

1. **(config)# message-list MSG_LIST**
   メッセージ種別リスト（MSG_LIST）を作成します。

2. **(config-msg-list)# message-type include BCU**
   (config-msg-list)# exit
   メッセージ種別 BCU を出力対象に設定します。
3. **(config)# message-list SAMPLE_LIST**
   メッセージ種別リスト（SAMPLE_LIST）を作成します。
4. **(config-msg-list)# message-type exclude BCU**
   (config-msg-list)# exit
   メッセージ種別 BCU を出力抑止対象に設定します。

(2)　運用端末に出力する条件の設定例

[設定のポイント]

運用端末に出力する条件の設定には，username コマンドの logging-console パラメータを使用します。

[コマンドによる設定]

1. **(config)# username default_user logging-console message-list MSG_LIST event-level 4**
   ログイン中のすべてのユーザの運用端末に出力する条件として，メッセージ種別リスト（MSG_LIST）とイベントレベルの数値 4 以下を設定します。

(3)　syslog サーバに送信する条件の設定例

[設定のポイント]

syslog サーバに送信する条件の設定には，logging syslog-filter コマンドを使用します。

[コマンドによる設定]

1. **(config)# logging syslog-filter message-list MSG_LIST**
   syslog サーバへの送信条件としてメッセージ種別リスト（MSG_LIST）を設定します。

(4)　E-mail サーバに送信する条件の設定例

[設定のポイント]

E-mail サーバに送信する条件の設定には，logging email-filter コマンドを使用します。

[コマンドによる設定]

1. **(config)# logging email-filter event-level 4**
   E-mail サーバへの送信条件としてイベントレベルの数値 4 以下を設定します。

(5)　SNMP サーバに送信する条件の設定例

[設定のポイント]

SNMP サーバに送信する条件の設定には，snmp-server traps コマンドの system_msg_trap_message_list パラメータおよび system_msg_trap_event_level パラメータを使用します。

[コマンドによる設定]

1. **(config)# snmp-server traps system_msg_trap_message_list SAMPLE_LIST system_msg_trap_event_level 4**

   SNMP サーバへの送信条件としてメッセージ種別リスト（SAMPLE_LIST）とイベントレベルの数値４以下を設定します。

15.3　オペレーション

15.3.1　運用コマンド一覧

システムメッセージの出力とログの管理の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
show logging	本装置で収集しているログと収集するログの最小保存件数を表示します。
clear logging	本装置で収集しているログをクリアします。

15.3.2　ログの参照と削除

(1)　ログの参照

show logging コマンドで運用ログおよび統計ログを参照できます。コマンドの実行結果を次の図に示します。

図 15-1　show logging コマンドの実行結果

```
> show logging
Date 20XX/11/07 15:54:12 UTC
System information
    AX8616R, OS-RE, Ver.12.1, BCU1(active)
Logging information
20XX/11/07 15:54:12 UTC 1-1(A) S6 KEY operator(tty00): > show logging
20XX/11/07 15:53:45 UTC 1-1(A) S6 BCU 01101001 00 023902000000 Initialization is complete.
20XX/11/07 15:49:34 UTC 1-1(A) S3 PS 01202020 00 0aec02000000 The power supply is insufficient.
```

show logging コマンドで message-type パラメータや event-level パラメータを指定すると，運用ログをフィルタリングして出力できます。コマンドの実行結果を次に示します。

図 15-2　show logging コマンド（message-type パラメータ指定時）の実行結果

```
> show logging message-type BCU
Date 20XX/11/07 15:54:12 UTC
System information
    AX8616R, OS-RE, Ver.12.1, BCU1(active)
Logging information
20XX/11/07 15:53:45 UTC 1-1(A) S6 BCU 01101001 00 023902000000 Initialization is complete.
```

図 15-3　show logging コマンド（event-level パラメータ指定時）の実行結果

```
> show logging event-level 4
Date 20XX/11/07 15:54:12 UTC
System information
    AX8616R, OS-RE, Ver.12.1, BCU1(active)
Logging information
20XX/11/07 15:49:34 UTC 1-1(A) S3 PS 01202020 00 0aec02000000 The power supply is insufficient.
```

(2)　ログの削除

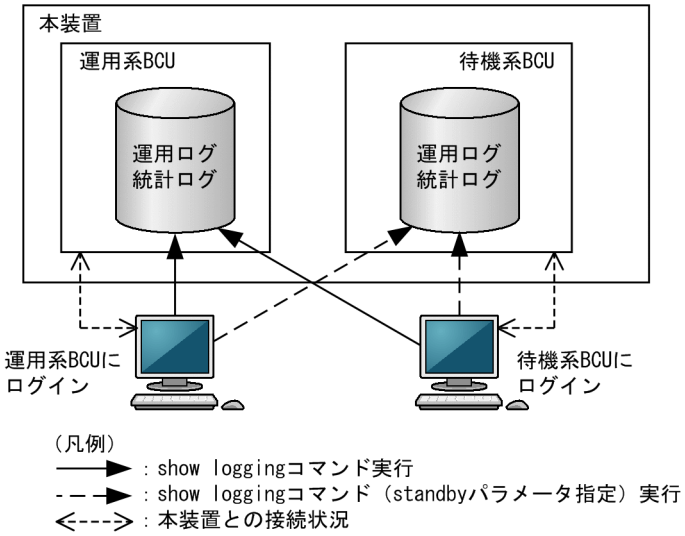
clear logging コマンドで運用ログおよび統計ログを削除できます。

(3)　BCU 二重化時のログの参照と削除

BCU 二重化時にログを参照または削除する場合，standby パラメータの有無によって対象となる系が異なります。

show logging コマンドで standby パラメータを指定した場合の参照対象を次の図に示します。なお，待機系 BCU から運用系 BCU のログは削除できません。

図 15-4　BCU 二重化時のログの参照



(4)　運用ログの保存件数の確認

show logging コマンドで save-count パラメータを指定すると，設定した運用ログの保存件数を確認できます。

16 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。

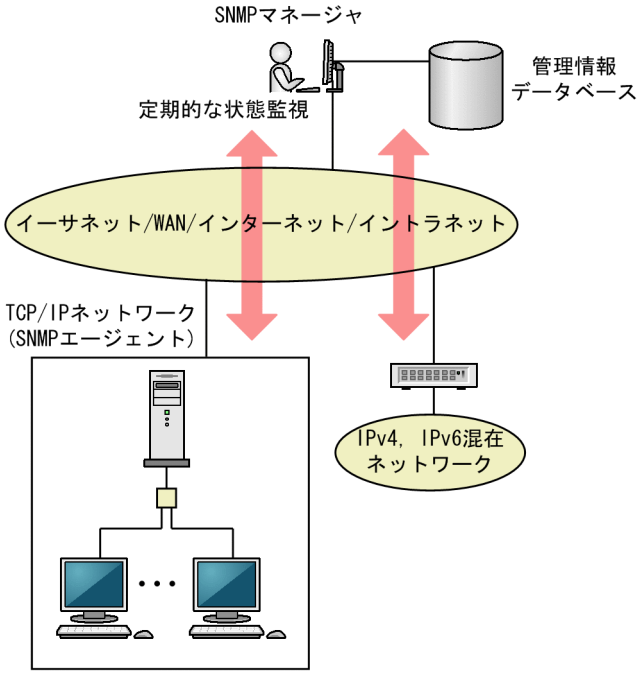
16.1　解説

16.1.1　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。

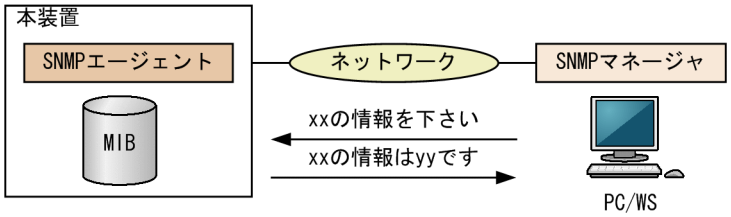
図 16-1　ネットワーク管理の概要



(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 16-2　MIB 取得の例

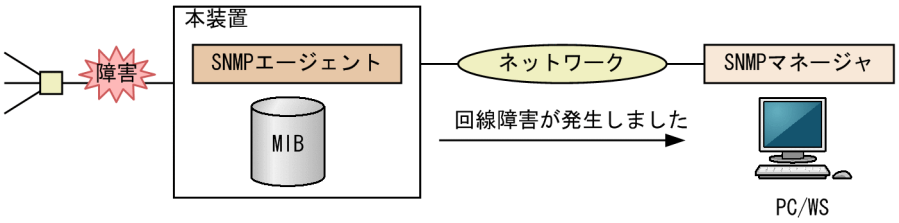


本装置の運用コマンドには MIB 情報を表示するための SNMP コマンドがあります。このコマンドは，自装置およびリモート装置の SNMP エージェントの MIB を表示します。

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。

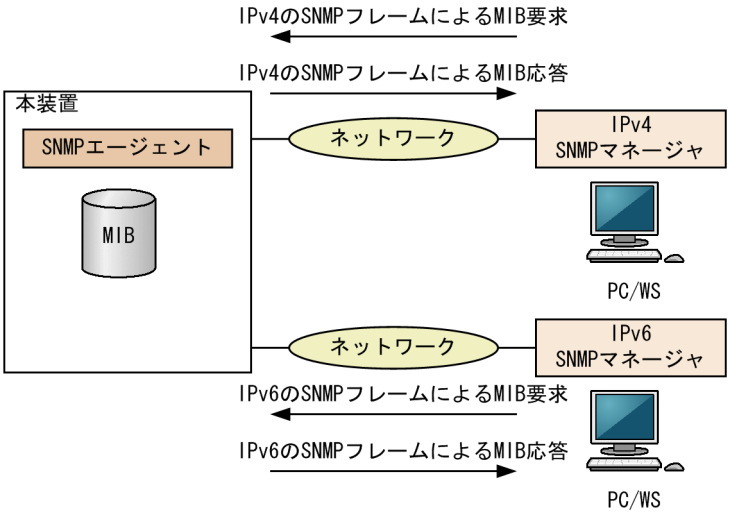
図 16-3　トラップの例



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。

本装置の SNMP プロトコルは IPv6 に対応しています。コンフィグレーションに設定した SNMP マネージャの IP アドレスによって，IPv4 または IPv6 アドレスが設定されている SNMP マネージャからの MIB 要求や，SNMP マネージャへの SNMP 通知を送信できます。IPv4/IPv6 SNMP マネージャからの MIB 要求と応答の例を次の図に示します。

図 16-4　IPv4/IPv6 SNMP マネージャからの MIB 要求と応答の例



(3) SNMPv3

SNMPv3 は SNMPv2C までの全機能に加えて，管理セキュリティ機能が大幅に強化されています。ネットワーク上を流れる SNMP パケットを認証・暗号化することによって，SNMPv2C でのコミュニティ名と SNMP マネージャの IP アドレスの組み合わせによるセキュリティ機能では実現できなかった，盗聴，なりすまし，改ざん，再送などのネットワーク上の危険から SNMP パケットを守ることができます。

(a) SNMP エンティティ

SNMPv3 では，SNMP マネージャおよび SNMP エージェントを「SNMP エンティティ」と総称します。本装置の SNMPv3 は，SNMP エージェントに相当する SNMP エンティティをサポートしています。

(b) SNMP エンジン

SNMP エンジンは認証，および暗号化したメッセージ送受信と管理オブジェクトへのアクセス制御のためのサービスを提供します。SNMP エンティティとは 1 対 1 の関係です。SNMP エンジンは，同一管理ドメイン内でユニークな SNMP エンジン ID によって識別されます。

(c) ユーザ認証とプライバシー機能

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 にはなかったプライバシー機能（暗号化，復号化）も SNMPv3 でサポートされています。ユーザ認証とプライバシー機能は，ユーザ単位に設定できます。

本装置では，ユーザ認証プロトコルとして次の二つプロトコルをサポートしています。

- HMAC-MD5-96（メッセージダイジェストアルゴリズムを使用した認証プロトコル。128 ビットのダイジェストのうち，最初の 96 ビットを使用する。秘密鍵は 16 オクテット）
- HMAC-SHA-96（SHA メッセージダイジェストアルゴリズムを使用した認証プロトコル。160 ビットの SHA ダイジェストのうち，最初の 96 ビットを使用する。秘密鍵は 20 オクテット）

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。

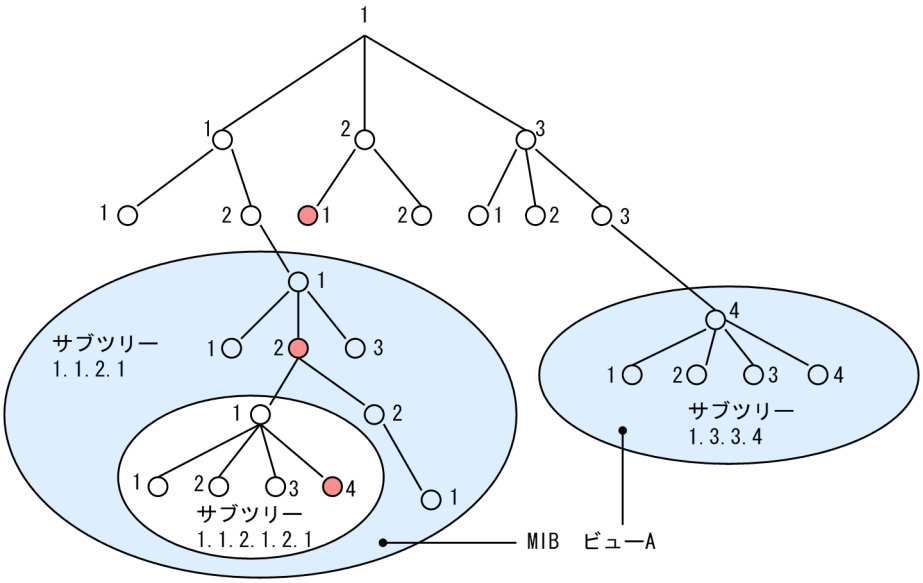
- CBC-DES（Cipher Block Chaining - Data Encryption Standard。共通鍵暗号アルゴリズムである DES（56 ビット鍵）を，CBC モードで強力にした暗号化プロトコル）

(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 16-5　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 16-5 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
```

16.1.2 MIB 概説

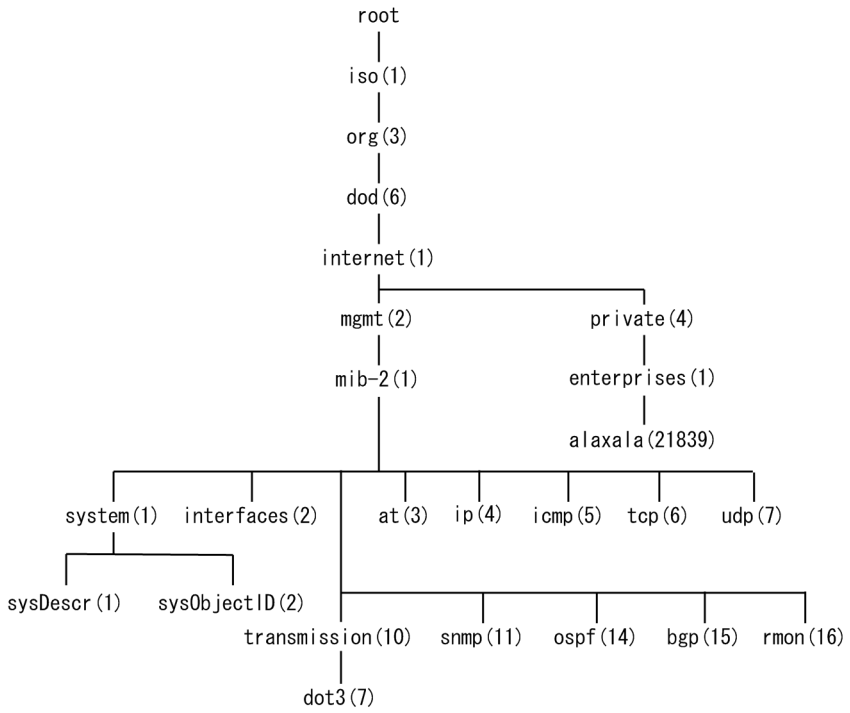
装置が管理し，SNMP マネージャに提供する MIB は，RFC で規定されたものと，装置の開発ベンダーが独自に用意する情報の 2 種類があります。

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 16-6 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 に一つの情報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 の後ろに数字を付けて表し，何番目の情報かなどを示すために使用します。

一つの MIB に一つの情報だけがある場合，MIB のオブジェクト ID に".0"を付けて表します。一つの MIB に複数の情報がある場合，MIB のオブジェクト ID の後ろに数字を付け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 の最後に付けて 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。

16.1.3　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。

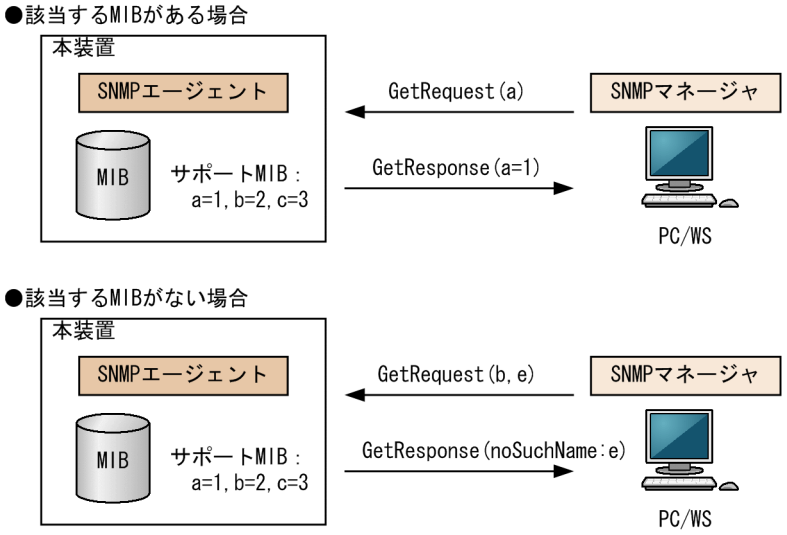
各オペレーションは SNMP マネージャから装置（SNMP エージェント）に対して行われます。各オペレーションについて説明します。

(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。

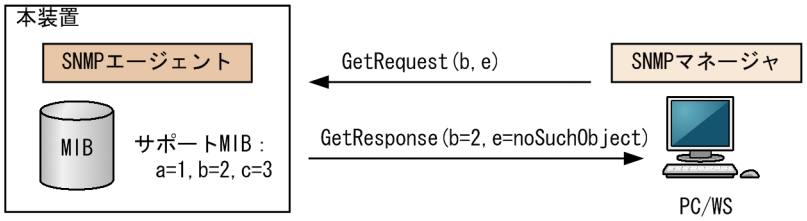
装置が該当する MIB を保持している場合，GetResponse オペレーションで MIB 情報を応答します。該当する MIB を保持していない場合は，GetResponse オペレーションで noSuchName を応答します。
GetRequest オペレーションを次の図に示します。

図 16-7　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 16-8 GetRequest オペレーション（SNMPv2C）

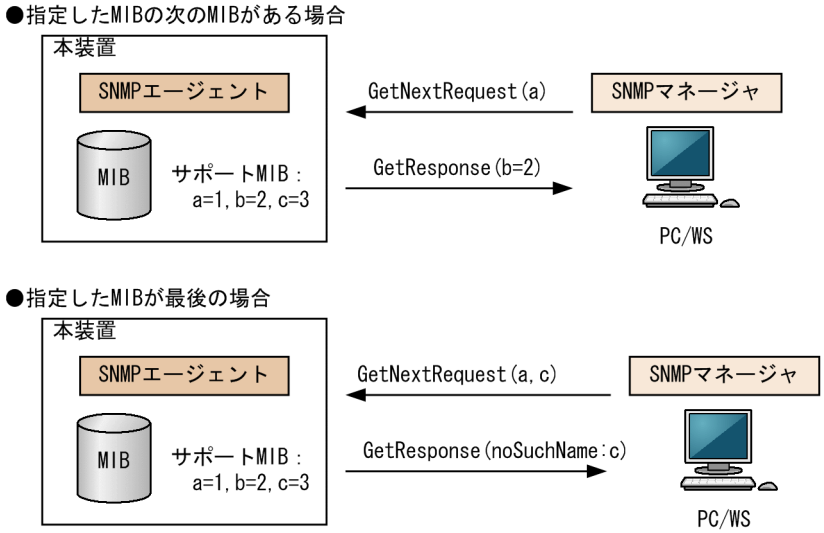


(2) GetNextRequest オペレーション

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。

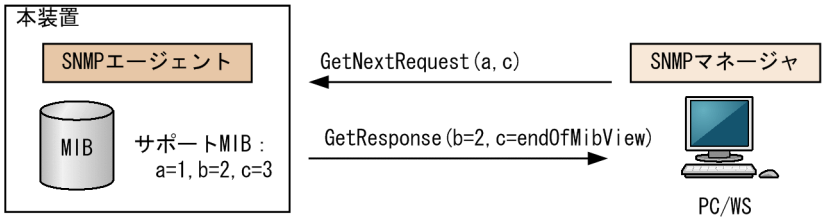
装置が指定した次の MIB を保持している場合は，GetResponse オペレーションで MIB を応答します。指定した MIB が最後の場合は，GetResponse で noSuchName を応答します。GetNextRequest オペレーションを次の図に示します。

図 16-9 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 16-10 GetNextRequest オペレーション（SNMPv2C）

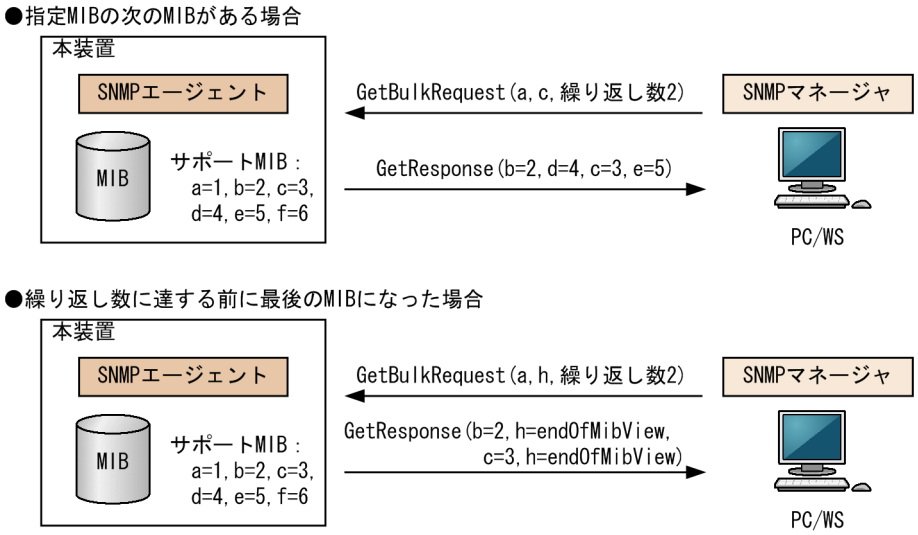


(3) GetBulkRequest オペレーション

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 16-11 GetBulkRequest オペレーション

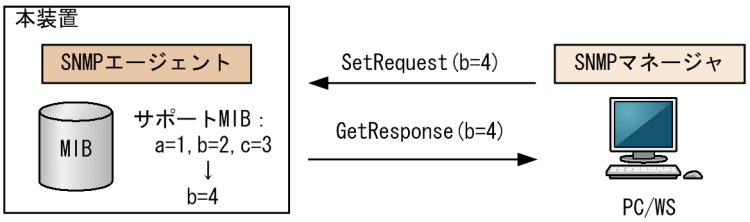


(4) SetRequest オペレーション

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 16-12 SetRequest オペレーション



(a) MIB を設定できない場合の応答

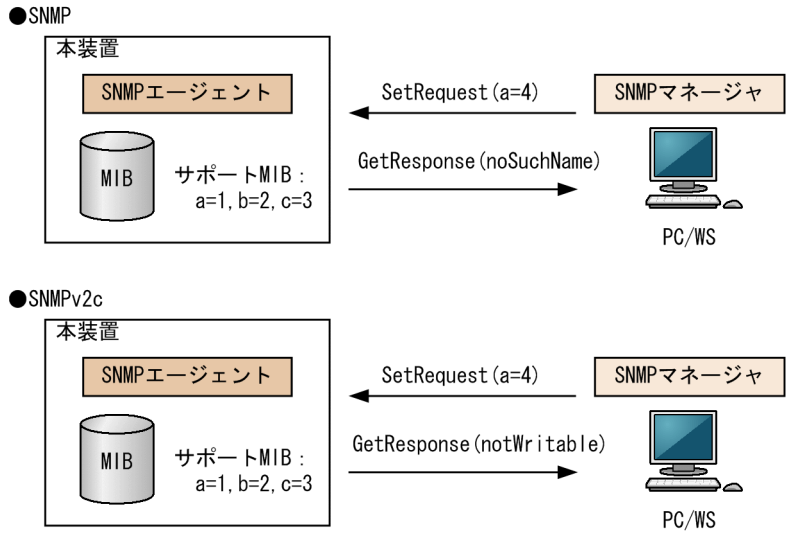
MIB を設定できないケースは，次に示す 3 とおりです。

- 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

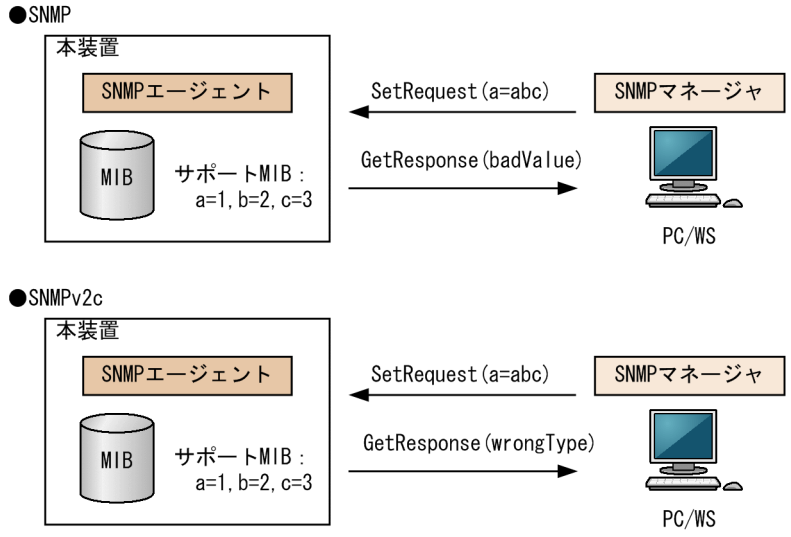
各ケースによって，応答が異なります。MIB が読み出し専用の場合，noSuchName の GetResponse 応答をします。SNMPv2C の場合，MIB が読み出し専用のときは notWritable の GetResponse 応答をします。MIB が読み出し専用の場合の SetRequest オペレーションを次の図に示します。

図 16-13　MIB 変数が読み出し専用の場合の SetRequest オペレーション



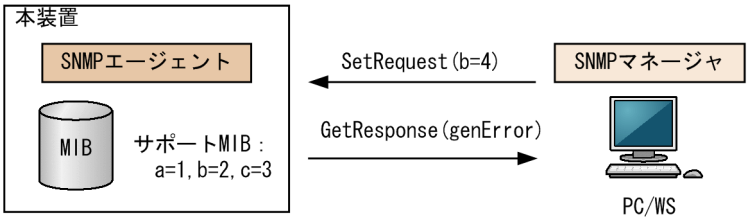
設定値のタイプが正しくない場合，badValue の GetResponse 応答をします。SNMPv2C の場合，設定値のタイプが正しくないときは wrongType の GetResponse 応答をします。設定値のタイプが正しくない場合の SetRequest オペレーションを次の図に示します。

図 16-14　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。

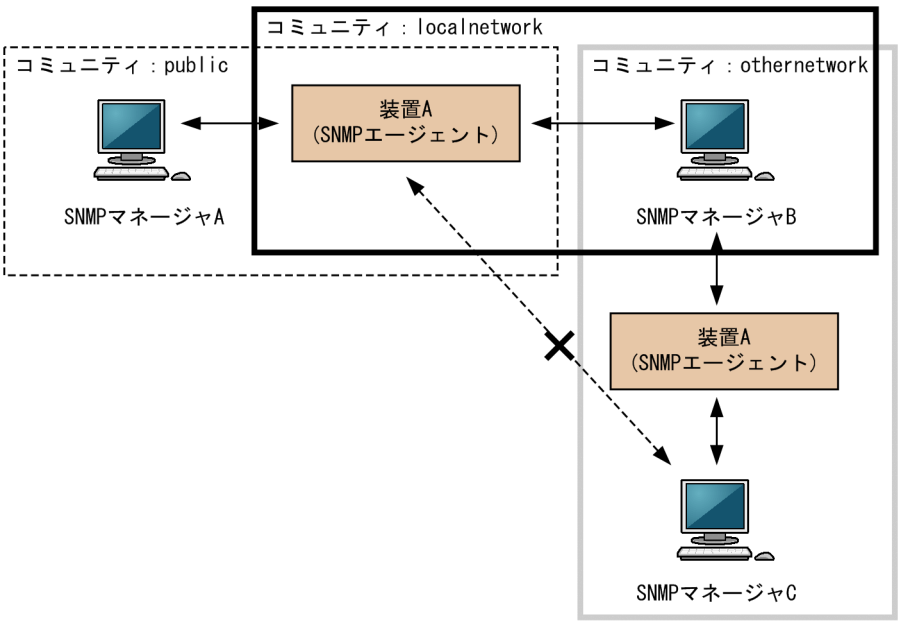
図 16-15　装置の状態によって設定できない場合の SetRequest オペレーション



(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 16-16　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 16-1 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。

16.1.4 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 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。

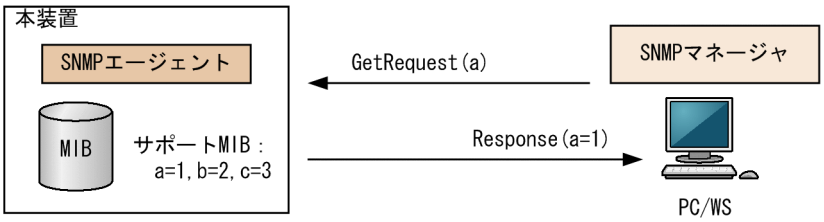
各オペレーションは SNMP マネージャから装置（SNMP エージェント）に対して行われます。各オペレーションについて説明します。

(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 16-17 GetRequest オペレーション

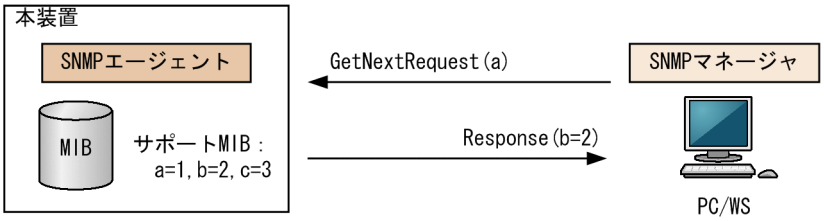


(2) GetNextRequest オペレーション

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 16-18 GetNextRequest オペレーション

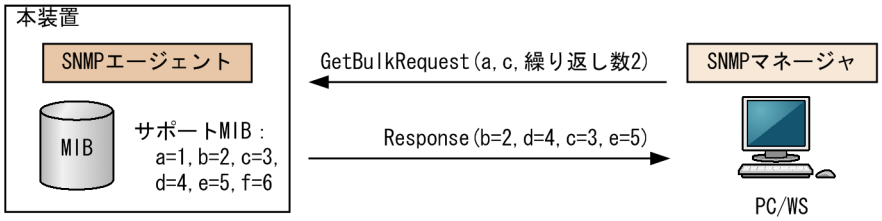


(3) GetBulkRequest オペレーション

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 16-19 GetBulkRequest オペレーション



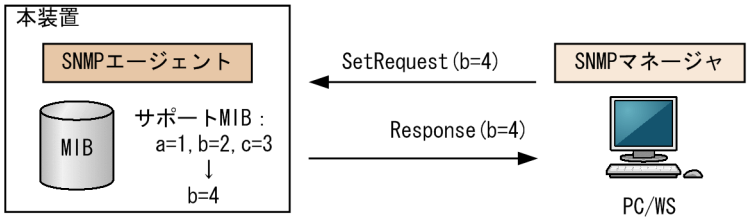
(4) SetRequest オペレーション

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 16-20 SetRequest オペレーション



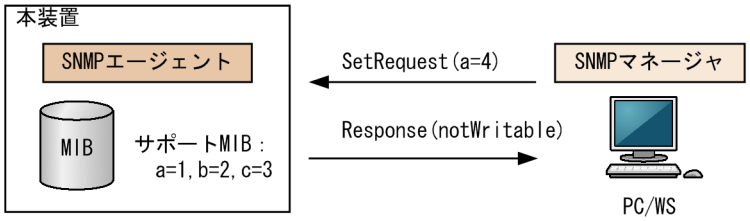
(a) MIB を設定できない場合の応答

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

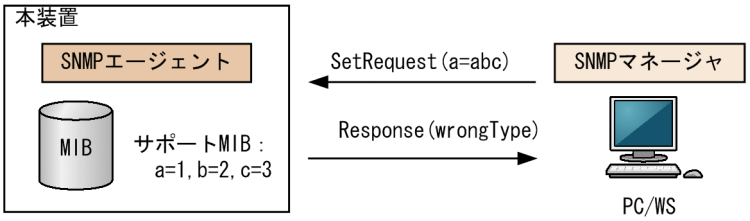
各ケースによって，応答が異なります。MIB が読み出し専用のときは notWritable の Response 応答をします。MIB が読み出し専用の場合の SetRequest オペレーションを次の図に示します。

図 16-21 MIB 変数が読み出し専用の場合の SetRequest オペレーション



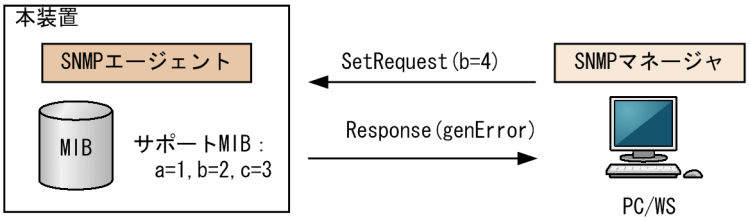
設定値のタイプが正しくないときは wrongType の Response 応答をします。設定値のタイプが正しくない場合の SetRequest オペレーションを次の図に示します。

図 16-22　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 16-23　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 16-2　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。

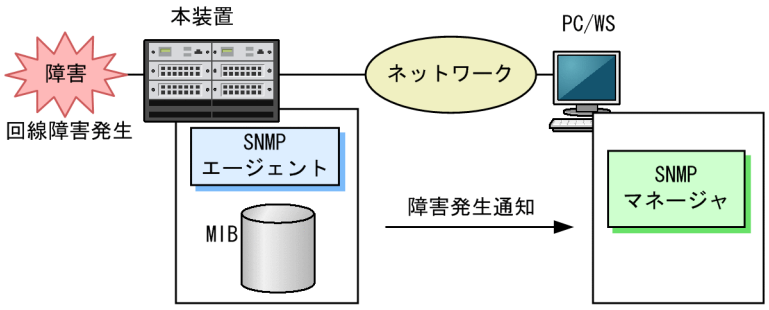
16.1.5　トラップ

(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。

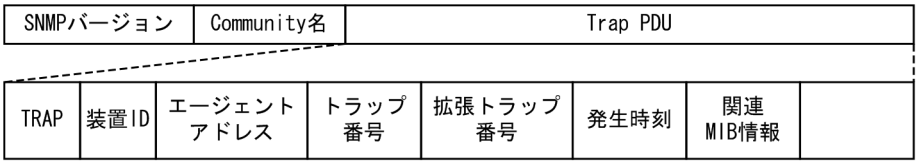
図 16-24　トラップの例



(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）を次に示します。

図 16-25 トラップフォーマット（SNMPv1）

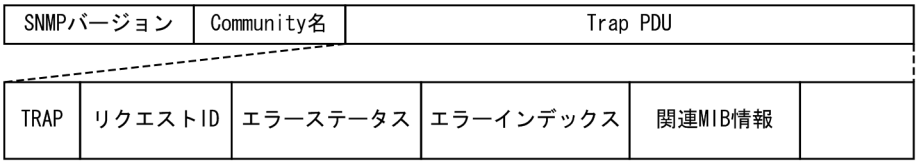


図中の表記	説明
装置 ID	装置の識別 ID（通常 MIB-II の sysObjectID の値が設定される）
エージェントアドレス	トラップが発生した装置の IP アドレス
トラップ番号	トラップの種別を示す識別番号
拡張トラップ番号	トラップ番号の補足をするための番号
発生時刻	トラップが発生した時間（装置が起動してからの経過時間）
関連 MIB 情報	このトラップに関連する MIB 情報

(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）を次に示します。

図 16-26 トラップフォーマット（SNMPv2C，SNMPv3）



図中の表記	説明
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

16.1.6 インフォーム

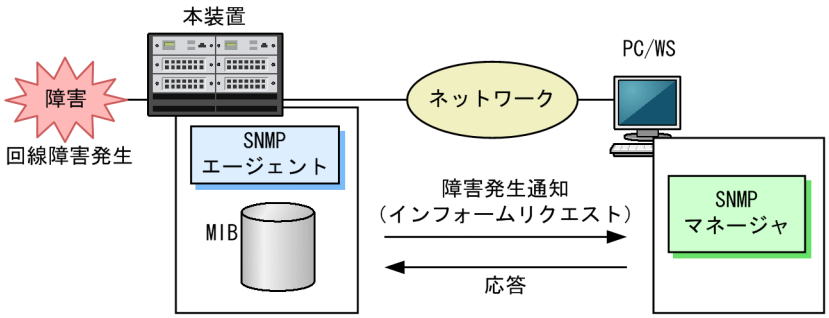
(1) インフォーム概説

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。

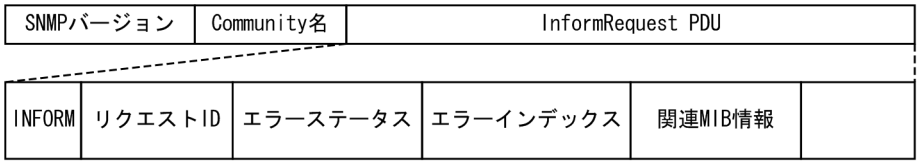
図 16-27　インフォームの例



(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に示します。

図 16-28　インフォームリクエストフォーマット



図中の表記	説明
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

16.1.7　SNMP で使用する IP アドレス

本装置から SNMP パケットを送信するときに IP ヘッダに付ける IP アドレスは，オペレーションによって異なります。SNMP で使用する IP アドレスを次の表に示します。

表 16-3　SNMP で使用する IP アドレス

オペレーション	送信元 IP アドレス	宛先 IP アドレス
• GetResponse • Response	GetResponse および Response の元になるオペレーション（GetRequest,	GetResponse および Response の元になるオペレーション（GetRequest,

オペレーション	送信元 IP アドレス	宛先 IP アドレス
	GetNextRequest，GetBulkRequest，SetRequest）受信時の宛先 IP アドレス	GetNextRequest，GetBulkRequest，SetRequest）受信時の送信元 IP アドレス
• トラップ • インフォーム	次の順で決定します。 1. 送信元インタフェースを設定した場合，設定したループバックインタフェースの IP アドレス 2. ループバックインタフェースに IP アドレスを設定した場合，ループバックインタフェースの IP アドレス ただし，コンフィグレーションコマンド no system-source-address が設定されたループバックインタフェースは対象外とします。 3. 上記以外の場合，送信インタフェースの IP アドレス	宛先 SNMP マネージャの IP アドレス

16.1.8 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 RFC2819 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て，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を設定するための 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掛けることが少なく，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。

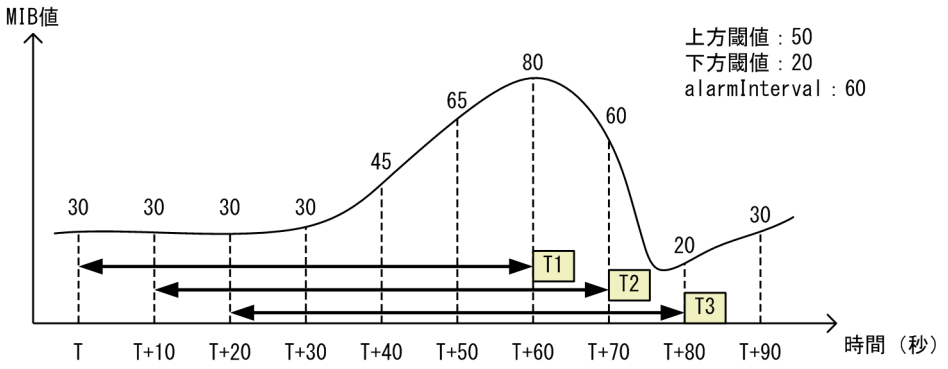
表 16-4　alarmInterval ごとの閾値チェック回数

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 16-29 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

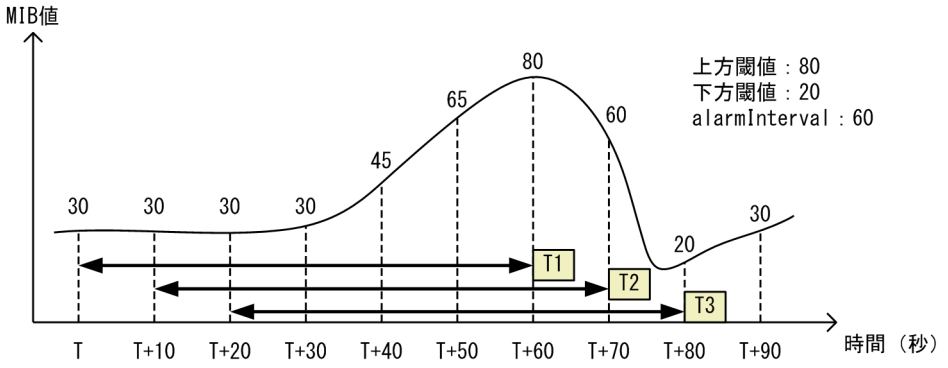
閾値と比較する値が 30（T+70（秒）の MIB 値 60－T+10（秒）の MIB 値 30）のため，閾値検出なし

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 16-30 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おそれがありますので注意してください。

16.1.9 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

(2) SNMP オペレーションメッセージの最大長

SNMP オペレーションのメッセージには最大長があります。各 Request のメッセージが最大長を超えた場合，メッセージは廃棄されます。ただし，GetBulkRequest オペレーションの場合，指定した繰り返し回数個分の MIB 値を取得するか，最大メッセージサイズまで MIB を取得してから，GetResponse または Response を応答します。

SNMP オペレーションのメッセージフォーマット，およびメッセージの最大長を次に示します。

図 16-31 SNMPv1，SNMPv2C オペレーションのメッセージフォーマット

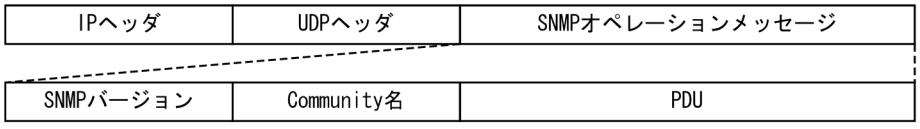


図 16-32　SNMPv3 オペレーションのメッセージフォーマット

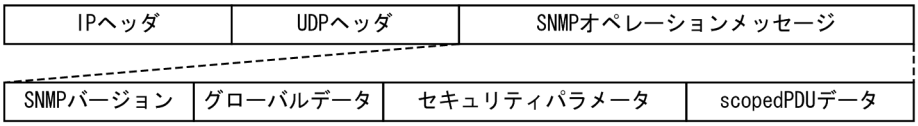


表 16-5　SNMP オペレーションメッセージの最大長（オクテット）

オペレーション		Request の最大長	GetResponse または Response の最大長
• GetRequest • GetNextRequest	• SNMPv1 • SNMPv2C	2048	4096
	• SNMPv3	2048	65507
• GetBulkRequest※	• SNMPv2C • SNMPv3	2048	2048
• SetRequest	• SNMPv1 • SNMPv2C • SNMPv3	2048	2048

注※

指定した MIB や繰り返し回数によって，指定した繰り返し回数個分の MIB を取得できないことがあります。次の MIB を例として，取得最大数の目安を示します。

・ifTable：87

・ifXTable：89

・axIfStatsTable：68

なお，本装置と SNMP マネージャとの間の最小 MTU の値によっては，SNMP オペレーションのメッセージがこの最大長を超えていない場合でも，フラグメント化してファイアウォールやフィルタを通過できないおそれがあります。SNMP オペレーションのメッセージサイズに関係なく，フラグメント化しない程度のパケットサイズにすることを推奨します。

16.2 コンフィグレーション

16.2.1 コンフィグレーションコマンド一覧

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 16-6 コンフィグレーションコマンド一覧

コマンド名	説明
rmon alarm	RMON アラームグループの制御情報を設定します。
rmon collection history	RMON 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 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 RFC3418 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 RFC3418 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	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場合，サブインタフェースまたは VLAN インタフェースがアップまたはダウンした場合の，SNMP 通知（linkDown および linkUp）の送信を制御します。

16.2.2 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設定をします。

[コマンドによる設定]

1. **(config)# ip access-list standard LIST1**
   (config-std-nacl)# 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を設定します。
2. **(config)# snmp-server community "NETWORK" ro LIST1**
   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
- アクセスリスト名：LIST1
- アクセスモード：read only

16.2.3 SNMPv3 による MIB アクセス許可の設定

[設定のポイント]

SNMPv3 で MIB にアクセスするために，アクセスを許可する MIB オブジェクトの集合を MIB ビューとして設定し，ユーザ認証とプライバシー機能の情報を 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
   - 暗号化プロトコル：CBC-DES
   - 暗号化パスワード：XYZ/+6789
3. **(config)# snmp-server group "ADMIN_GROUP" v3 priv read "READ_VIEW" write "WRITE_VIEW"**
   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

16.2.4 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

16.2.5 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 通知の内容を設定します。

[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
   - 暗号化プロトコル：DES
   - 暗号化パスワード：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

16.2.6 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

16.2.7　リンクトラップの送信制御

次の契機で送信する SNMP 通知（linkDown および linkUp）をリンクトラップと呼びます。

- 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
- サブインタフェースがアップまたはダウンしたとき
- VLAN インタフェースがアップまたはダウンしたとき

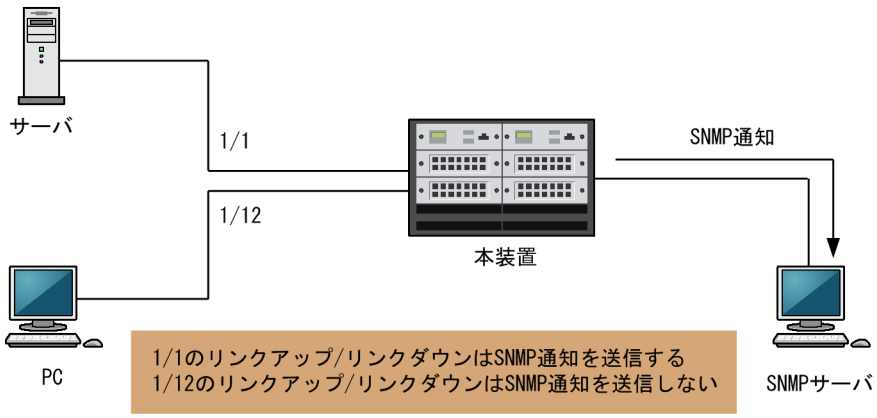
本装置では，コンフィグレーションによって，インタフェースごとにリンクトラップの送信を制御できます。例えば，サーバと接続するイーサネットインタフェースのように重要度の高いインタフェースだけ SNMP 通知を送信して，そのほかのイーサネットインタフェースのリンクトラップの送信を抑止することで，本装置，ネットワーク，および SNMP マネージャの不要な処理を削減できます。

なお，インタフェース種別によって送信のデフォルト動作が異なります。イーサネットインタフェースでは，デフォルト動作として SNMP 通知を送信します。サブインタフェースおよび VLAN インタフェースでは，デフォルト動作として SNMP 通知を送信しません。

[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 16-33　リンクトラップの構成図



ここでは，ポート 1/1 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 1/12 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 1/12**
   (config-if)# no snmp trap link-status
   リンクアップおよびリンクダウン時に SNMP 通知を送信しません。

2. **(config-if)# exit**

16.2.8 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 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 1/5**

   ギガビット・イーサネットインタフェース 1/5 のコンフィグレーションモードに移行します。

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

16.2.9 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 RMON の SNMP 通知を送信するよう SNMP マネージャの設定が必要です。

[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.1" 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.1
   - 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

16.2.10 SNMPv1, SNMPv2C による VRF からの MIB アクセス許可の設定

[設定のポイント]

VRF に存在する SNMP マネージャから本装置の MIB へのアクセスを許可する設定をします。

[コマンドによる設定]

1. **(config)# ip access-list standard LIST2**
   (config-std-nacl)# 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を設定します。
2. **(config)# snmp-server community "NETWORK" ro LIST2 vrf 2**
   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
   - アクセスリスト名：LIST2
   - アクセスモード：read only
   - VRF ID：2

16.2.11 SNMPv3 による VRF からの MIB アクセス許可の設定

[設定のポイント]

SNMPv3 で MIB にアクセスするために，アクセスを許可する MIB オブジェクトの集合を MIB ビューとして設定し，ユーザ認証とプライバシー機能の情報，およびアクセスを許可する VRF ID 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" vrf 2**
   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
- 暗号化プロトコル：CBC-DES
- 暗号化パスワード：XYZ/+6789
- VRF ID：2

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

16.2.12 SNMPv1，SNMPv2C による VRF へのトラップ送信の設定

[設定のポイント]

VRF に存在する SNMP マネージャに対して，トラップを送信する設定をします。

[コマンドによる設定]

1. **(config)# snmp-server host 10.1.1.1 vrf 2 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
   - VRF ID：2

16.2.13 SNMPv3 による VRF への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 通知の内容を設定します。SNMP セキュリティユーザで登録する VRF ID と SNMP マネージャに設定する VRF ID は，同一である必要があります。

[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" vrf 2**
   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
- 暗号化プロトコル：DES
- 暗号化パスワード：XYZ/+6789
- VRF ID：2

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 vrf 2 traps "ADMIN" version 3 priv snmp**
   SNMPv3 によって SNMP マネージャに標準トラップを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
   - VRF ID：2

16.2.14 SNMPv2C による VRF へのインフォーム送信の設定

[設定のポイント]

VRF に存在する SNMP マネージャに対して，インフォームを送信する設定をします。

[コマンドによる設定]

1. **(config)# snmp-server host 10.1.1.1 vrf 2 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
   - VRF ID：2

16.3 オペレーション

16.3.1 運用コマンド一覧

SNMP/RMON に関する運用コマンド一覧を次の表に示します。

表 16-7 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。
snmp walk	指定した MIB ツリーを表示します。
snmp getif	interface グループの MIB 情報を表示します。
snmp getroute	ipRouteTable（IP ルーティングテーブル）を表示します。
snmp getarp	ipNetToMediaTable（IP アドレス変換テーブル）を表示します。
snmp getforward	ipForwardTable（IP フォワーディングテーブル）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。
snmp rgetroute	指定したリモート装置の ipRouteTable（IP ルーティングテーブル）を表示します。
snmp rgetarp	指定したリモート装置の ipNetToMediaTable（IP アドレス変換テーブル）を表示します。

16.3.2 SNMP マネージャとの通信の確認

本装置に SNMP エージェント機能を設定して SNMP プロトコルによるネットワーク管理を行う場合，次のことを確認してください。

- ネットワーク上の SNMP マネージャから本装置に対して MIB を取得できること
- 本装置からネットワーク上の SNMP マネージャへ SNMP 通知が送信されていること，さらに，インフォームの場合は応答を受信できること

show snmp コマンドで SNMP マネージャとの通信状態を確認できます。

図 16-34 show snmp コマンドの実行結果

```
> show snmp
Date 20XX/03/18 13:34:17 UTC
Contact: snmp@example.com
Location: Japan
SNMP packets input  : 149346    (get:186696 set:0)
    Get-request PDUs    : 1992
```

```
    Get-next PDUs       : 147354
    Get-bulk PDUs       : 0
    Set-request PDUs    : 0
    Response PDUs       : 0    (with error 0)
    Error PDUs          : 0
        Bad SNMP version errors: 0
        Unknown community name : 0
        Illegal operation      : 0
        Encoding errors        : 0

SNMP packets output : 149475
    Trap PDUs           : 125
    Inform-request PDUs : 4
    Response PDUs       : 149346    (with error 499)
        No errors              : 148847
        Too big errors         : 0
        No such name errors    : 499
        Bad values errors      : 0
        General errors         : 0
    Timeouts            : 1
    Drops               : 0

[TRAP]
    Host: 192.168.0.65, sent:3
    Host: 192.168.0.210, sent:61

[INFORM]
    Timeout(sec)        : 30
    Retry               : 3
    Pending informs     : 2/25 (current/max)
    Host: 192.168.0.1
        sent    :2          retries:1
        response:0          pending:2          failed:0          dropped:0
    Host: 2001:db8::10
        sent    :1          retries:0
        response:0          pending:1          failed:0          dropped:0
```

SNMP マネージャから MIB が取得できない場合は，「SNMP packets input」の項目で，「Error PDUs」の値が増加していないこと，および PDU を受信できていることを確認してください。「Error PDUs」の値が増加しているときは，コンフィグレーションの内容を確認してください。PDU を受信できていないときは，ネットワークの設定が正しいか，また，SNMP マネージャまでの経路上で障害が発生していないかを確認してください。

SNMP マネージャで SNMP 通知が受信できない場合は，「[TRAP]」と「[INFORM]」の項目で，SNMP マネージャの IP アドレスが「Host」として設定されていることを確認してください。設定されていないときは，コンフィグレーションコマンド snmp-server host を実行して，SNMP マネージャに関する情報を設定してください。

なお，これらの方法で解決できない場合は「トラブルシューティングガイド」を参照してください。また，本装置から取得できる MIB および SNMP 通知については「MIB レファレンス」を参照してください。

17 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。

17.1　解説

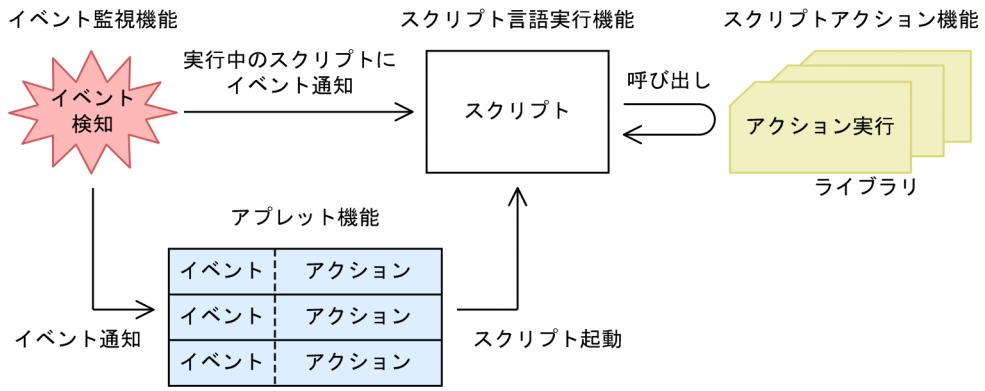
17.1.1　概要

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，システム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，ユーザが作成したシステム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 17-1　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，コマンド実行やシステム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 17-1　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。
システムメッセージ出力	指定した任意の文字列をシステム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 17-2　監視イベントの一覧

監視イベント	説明
システムメッセージ監視	出力されたシステム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。

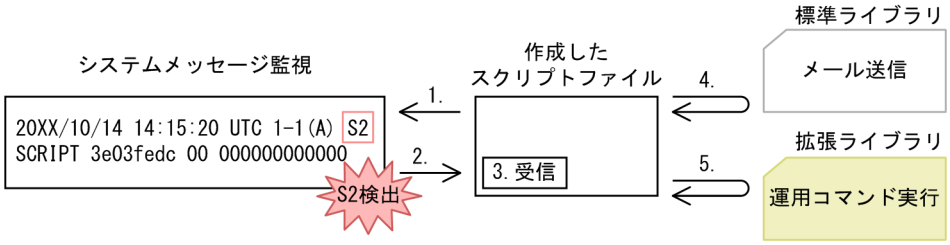
作成したスクリプトをスクリプト言語実行機能で実行すると，スクリプトに記載した各処理が実行されます。このように，高機能スクリプトを使用すると，本装置のコンフィグレーションやオペレーションをプログラミングして実行できるようになります。

17.1.2　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。この図ではシステムメッセージを監視して，レベル S1 または S2 のシステム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 17-2　システム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

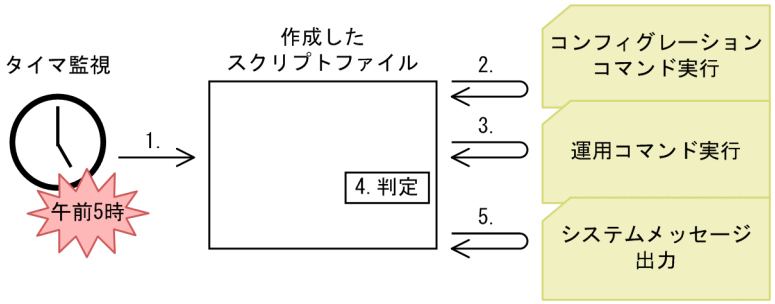


1. システムメッセージ監視イベントを登録して，イベントの発生を待ちます。
2. レベル S1 または S2 のシステムメッセージ出力を検出したら，イベントを通知します。
3. イベントを受信します。
4. イベントを受信したスクリプトは，Python の標準ライブラリを使用してオペレータにメールを送信します。
5. 関連する運用コマンドを実行して，事象発生時の解析情報を収集します。

(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，システムメッセージを出力します。

図 17-3　タイマ監視によるコマンド実行およびシステムメッセージ出力



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システムメッセージを出力して，オペレータへ通知します。

17.1.3　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 17–3　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 17–4　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 17–5　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 17-6　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 17-7　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

(6)　系切替時の動作

系切替時のスクリプトの動作について次の表に示します。

表 17-8　系切替時のスクリプトの動作

スクリプト種別	新運用系	新待機系
コマンドスクリプト	スクリプトは自動で実行されません。	運用系で実行中だったスクリプトは強制終了します。
常駐スクリプト	新しく常駐スクリプトを起動します。	
イベント起動スクリプト	新運用系で新たにイベントを検出すると起動します。	

17.1.4　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 17-9　作業ディレクトリ

ディレクトリ名	容量
/opt/script※	16MB

注※

BCU 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。

17.2　スクリプトの作成と実行

17.2.1　コンフィグレーション・運用コマンド一覧

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 17-10　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システム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 17-11　運用コマンド一覧

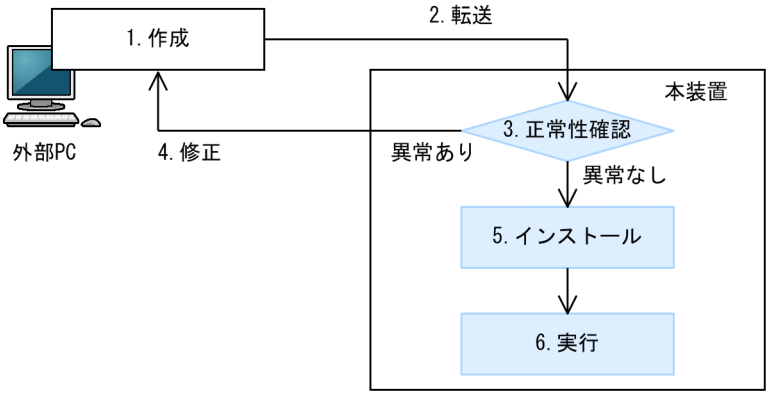
コマンド名	説明
python	Python を実行します。
stop python	起動中のスクリプトを停止します。
pyflakes	スクリプトファイルの文法チェックをします。
install script	作成したスクリプトファイルを本装置にインストールします。
uninstall script	本装置にインストールされているスクリプトファイルを削除します。
show script installed-file	本装置にインストールされているスクリプトファイルの情報を表示します。
show script running-state	スクリプトの起動情報を表示します。
show event 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。

コマンド名	説明
	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。
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。

17.2.2　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 17-4　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。

17.2.3　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。

17.2.4　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 17-12　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 17-5　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 17-6　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 17-7　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。

17.2.5　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 17-13　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 17-8　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。

17.2.6　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 17-9　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 17-10　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 17-11　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 17-12　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。

監視イベントをシステム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 17-13　イベント起動スクリプトの設定例（システムメッセージ監視）

```
# install script sample.py                        <-1
# configure
(config)# event manager applet PORT_UP            <-2
(config-applet)# event sysmsg message-id 25010001 <-3
(config-applet)# action 1 python sample.py        <-4
(config-applet)#
```

```
20XX/02/05 19:00:18 UTC 1-1(A) S6 PORT PORT:1/1 25010001 01 000000000000 The port status is 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 25010001 のシステムメッセージ出力を監視する，システム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 25010001）に該当するシステム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 17-14　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。

17.3　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。

17.3.1　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 17-14　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。

17.3.2　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 17-15　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。

17.4　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 Vol.1　20. Python 拡張ライブラリ」を参照してください。

17.4.1　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 17-16　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 17-15　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 17-16　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 17-17　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 17-18　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 17-19　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 17-20　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 17-17　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，パラメータエラー（illegal name エラー）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）および AUX 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）または AUX 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

17.4.2　システム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，指定した文字列をシステム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 17-18　sysmsg モジュールの関数一覧

関数名	説明
send	システム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

システム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 17-21　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(3, 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. 出力するシステムメッセージを，次のように指定します。
   - イベントレベル S3
   - 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. システム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 の実行結果およびシステムメッセージの出力例を次に示します。

図 17-22　スクリプト（test1.py）実行結果

```
# python test1.py
send success.
#
```

図 17-23　システムメッセージ出力例

```
20XX/10/15 13:25:45 UTC 1-1(A) S3 SCRIPT 3e03fedc 00 ba9876543210 Script Start!!
```

17.4.3　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 17-19　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	監視するシステム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)　システムメッセージをイベントとして監視する例

システム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 17-24　スクリプト記載例 1

```
import sys
import extlib.eventmonitor                                             <-1

try:
```

```
    event_sysmsg=extlib.eventmonitor.regist_sysmsg(event_level=3,
    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。次の条件を満たすシステムメッセージの出力を監視します。

- イベントレベル S3
- 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 17-25　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 17-26　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 17-27　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 17-28　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。

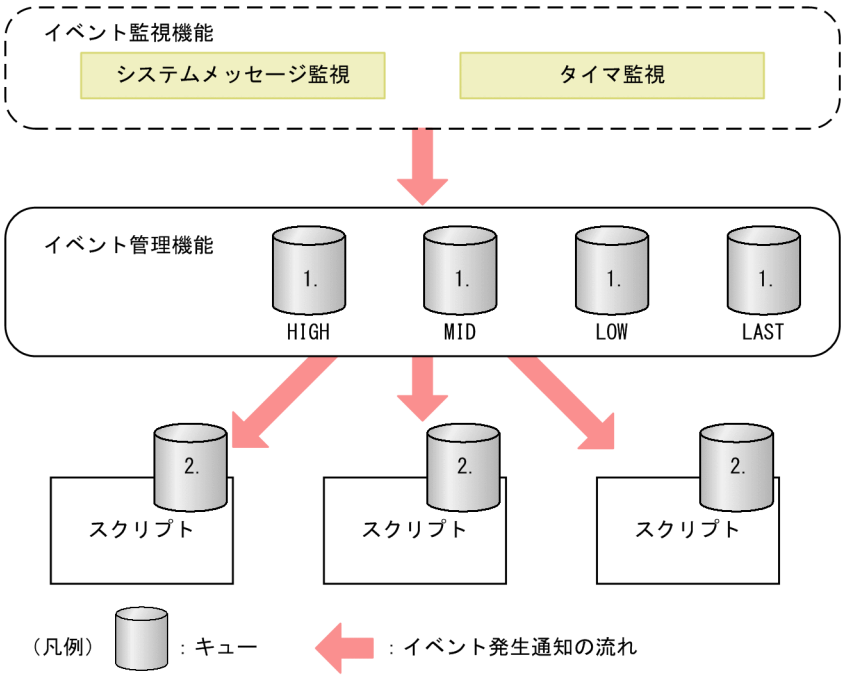
4. イベント受信関数を呼び出します。受信タイムアウトなしのブロッキングモードで受信します。

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 17-29　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。

17.4.4　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 17-30　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
    # システムメッセージイベント

        ## システム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システムメッセージを表示
        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. 起動要因がシステム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システムメッセージの情報を取得します。

18 イーサネット

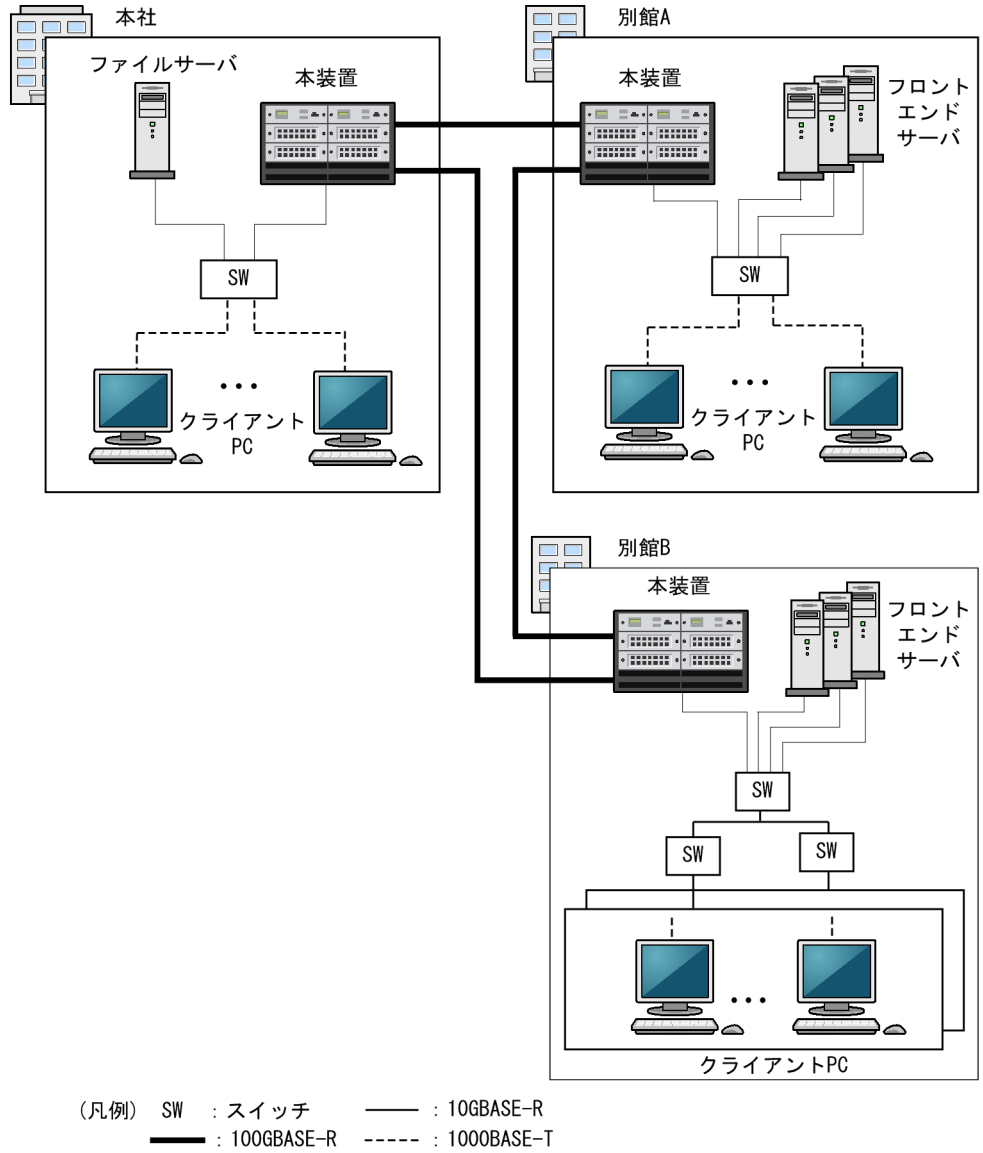
この章では，本装置のイーサネットについて説明します。

18.1　接続インタフェースの解説

18.1.1　ポートの種類とサポート機能

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 100GBASE-R で接続することによって，10BASE-T/100BASE-TX/1000BASE-T，1000BASE-X および 10GBASE-R よりもサーバ間のパフォーマンスが向上します。

図 18-1　イーサネットの構成例



(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 18-1　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
SFP ポート	10BASE-T，100BASE-TX，1000BASE-T，1000BASE-X
SFP+ポート	10GBASE-R
SFP+/SFP 共用ポート	10BASE-T※，100BASE-TX※，1000BASE-T，1000BASE-X，10GBASE-R
QSFP+ポート	40GBASE-R
QSFP28 ポート	100GBASE-R
CFP ポート	100GBASE-R

注※

NLXG-6RS では 10BASE-T/100BASE-TX の接続をサポートしていません。

(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)　SFP ポート

10BASE-T/100BASE-TX/1000BASE-T で接続する場合，10BASE-T/100BASE-TX/1000BASE-T 用の SFP-T をサポートしています。

1000BASE-X で接続する場合，1000BASE-SX，1000BASE-SX2，1000BASE-LX，1000BASE-LH，および 1000BASE-BX の SFP をサポートしています。

(c)　SFP+ポート

10GBASE-SR，10GBASE-LR，10GBASE-ER，および 10GBASE-ZR の SFP+をサポートしています。

(d)　SFP+/SFP 共用ポート

10BASE-T/100BASE-TX/1000BASE-T で接続する場合，10BASE-T/100BASE-TX/1000BASE-T 用の SFP-T を使用します。

1000BASE-X で接続する場合，1000BASE-SX，1000BASE-SX2，1000BASE-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-ZR の SFP+をサポートしています。

(e)　QSFP+ポート

40GBASE-SR4 および 40GBASE-LR4 の QSFP+をサポートしています。

(f)　QSFP28 ポート

100GBASE-SR4 および 100GBASE-LR4 の QSFP28 をサポートしています。

(g)　CFP ポート

100GBASE-LR4 の CFP をサポートしています。

(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 18-2　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※1	• 半二重固定※2 • 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※2	• フローコントロール • 自動 MDI／MDIX 機能
100BASE-TX※1	• 半二重固定※2 • 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※2	• フローコントロール • 自動 MDI／MDIX 機能 • 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	• フローコントロール • 自動 MDI／MDIX 機能 • 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
40GBASE-R	• 全二重固定	• フローコントロール • ジャンボフレーム
100GBASE-R	• 全二重固定	• フローコントロール • ジャンボフレーム

注※1

NLXG-6RS では 10BASE-T/100BASE-TX の接続をサポートしていません。

注※2

次の NIF では半二重をサポートしていないため，半二重では接続できません。

・NL1GA-12S

・NLXGA-12RS

18.1.2　10BASE-T/100BASE-TX/1000BASE-T

10BASE-T／100BASE-TX／1000BASE-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 ではオートネゴシエーション（自動認識機能）と固定接続機能をサポートしています。接続方法と対応するインタフェースについて次の表に示します。

表 18-3　接続方法と対応するインタフェース

接続方法	接続インタフェース
オートネゴシエーション	10BASE-T，100BASE-TX，1000BASE-T（全二重）
固定接続	10BASE-T，100BASE-TX

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
- 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

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，対向装置間でやりとりをして接続動作を決定する機能です。本装置では，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。

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。

1000BASE-T は，全二重のオートネゴシエーションだけの接続となります。

表 18-4　伝送速度および，全二重および半二重モードごとの接続仕様

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
		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	×	×	×	×	×

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	
	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 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	10BASE-T 半二重	×	100BASE-TX 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。半二重および全二重固定時は MDI 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 18–5　MDI／MDI-X のピンマッピング

RJ45 Pin No.	MDI			MDI-X		
	1000BASE-T	100BASE-TX	10BASE-T	1000BASE-T	100BASE-TX	10BASE-T
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
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

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。

注 2

1000BASE-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）

(4)　接続時の注意事項

- 伝送速度，および全二重／半二重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すると，以降の通信が停止することがあります。この場合，該当ポートに対して運用コマンド inactivate および activate 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し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。

18.1.3　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-SX2，1000BASE-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-SX2

マルチモード光ファイバを使用して 2km の伝送距離を実現します（マルチモード，最大 2km）。

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，対向装置間でやりとりをして接続動作を決定する機能です。本装置では，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 18-6 伝送速度および，全二重および半二重モードごとの接続仕様

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	×	×

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
	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。

18.1.4　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-ZR 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-ZR

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 80km）。

(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-ZR は IEEE802.3ae 規格にない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。

18.1.5　40GBASE-R

40GBASE-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

40GBASE-SR4 および 40GBASE-LR4 をサポートしています。回線速度は 40Gbit/s 全二重固定です。

40GBASE-SR4

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。

40GBASE-LR4

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）。

(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。

18.1.6 100GBASE-R

100GBASE-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

100GBASE-SR4 および 100GBASE-LR4 をサポートしています。回線速度は 100Gbit/s で，全二重固定です。

100GBASE-SR4

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 100m※）。

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。

100GBASE-LR4

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）。

(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。

18.2　イーサネット共通の解説

18.2.1　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，ポーズパケットで相手装置にフレームの送信を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を受信すると送信規制をします。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

本装置では受信バッファの使用状況を監視して，相手装置の送信規制をする場合にポーズパケットを送信します。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。

フローコントロールは，コンフィグレーションコマンド flowcontrol で設定します。送信と受信でそれぞれ，次に示すモードから選択できます。

- 有効
- 無効
- ネゴシエーション結果によって動作を決定

なお，本装置と相手装置の設定を送信と受信が一致するように合わせてください。

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 18-7　ポーズパケットの送信設定とフローコントロール動作

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する
off	無効	相手装置が送信規制をしない
desired	Desired	相手装置が送信規制をする

（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 18-8　ポーズパケットの受信設定とフローコントロール動作

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する
off	無効	本装置が送信規制をしない
desired	Desired	本装置が送信規制をする

（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 の場合は，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 18-9　オートネゴシエーション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	する	する
			無効	on	off	しない	しない
			Desired	on	on	する	する
		無効	有効	on	on	しない	する
			無効	on	off	しない	しない
			Desired	on	on	する	する
		Desired	有効	on	on	する	する
			無効	on	off	しない	しない
			Desired	on	on	する	する
off		有効	有効	on	on	する	する
			無効	off	on	する	しない
			Desired	on	on	する	する
		無効	有効	on	on	しない	する
			無効	off	off	しない	しない
			Desired	on	on	する	する
		Desired	有効	on	on	する	する
			無効	off	on	する	しない
			Desired	on	on	する	する
desired	on	有効	有効	on	on	する	する
			無効	off	on	する	しない
			Desired	on	on	する	する
		無効	有効	on	on	しない	する

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	しない	しない
			Desired	on	on	する	する
		Desired	有効	on	on	する	する
			無効	off	on	しない	しない
			Desired	on	on	する	する
	off	有効	有効	off	off	しない	しない
			無効	off	off	しない	しない
			Desired	off	off	しない	しない
		無効	有効	on	off	しない	する
			無効	off	off	しない	しない
			Desired	on	off	しない	する
		Desired	有効	off	off	しない	しない
			無効	off	off	しない	しない
			Desired	off	off	しない	しない
	desired	有効	有効	on	on	する	する
			無効	off	off	しない	しない
			Desired	on	on	する	する
		無効	有効	on	on	しない	する
			無効	off	off	しない	しない
			Desired	on	on	する	する
		Desired	有効	on	on	する	する
			無効	off	off	しない	しない
			Desired	on	on	する	する

(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

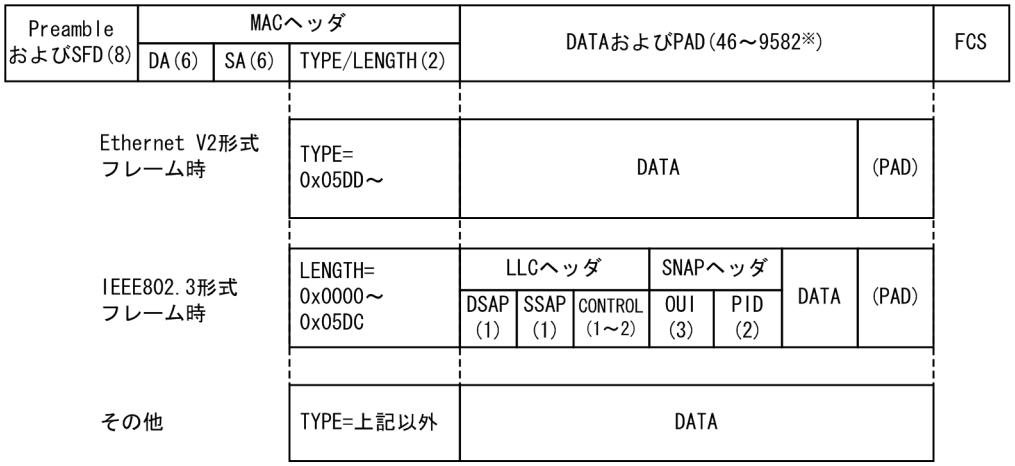
on：ポーズパケットを送信する

off：ポーズパケットを送信しない

18.2.2　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 18-2　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，Ethernet V2 形式フレームだけ 9582 です。IEEE802.3 形式フレームおよびその他の形式のフレームでは 1500 です。

(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 フィールドの意味を次の表に示します。

表 18-10　TYPE／LENGTH フィールドの意味

TYPE／LENGTH 値	フィールドの意味
0x0000～0x05DC	IEEE802.3 CSMA/CD のフレーム長
0x05DD～	Ethernet V2 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 副層フレームフォーマット

IEEE802.2 の LLC タイプ 1 をサポートしています。Ethernet V2 では LLC 副層はありません。

(a)　DSAP

LLC 情報部の宛先のサービスアクセス点を示します。

(b)　SSAP

LLC 情報部を発信した特定のサービスアクセス点を示します。

(c)　CONTROL

情報転送形式，監視形式，および非番号制御形式の三つの形式を示します。

(d)　OUI

SNAP 情報部を発信した組織コードフィールドを示します。

(e)　PID

SNAP 情報部を発信したイーサネットタイプフィールドを示します。

(3)　LLC の扱い

IEEE802.2 の LLC タイプ 1 をサポートしています。また，次に示す条件に合致したフレームだけを中継の対象にします。それ以外のフレームは，廃棄します。

(a)　CONTROL フィールド

CONTROL フィールドの値と送受信サポート内容を次の表に示します。

表 18-11　CONTROL フィールドの値と送受信サポート内容

種別	コード（16 進数）	コマンド	レスポンス	備考
XID	BF または AF	受信サポート	送信サポート	IEEE802.2 の仕様に従って，XID レスポンスを返送します。ただし，XID レスポンスの情報部は 129.1.0（IEEE802.2 の規定による ClassI を示す値）とします。
TEST	F3 または E3	受信サポート	送信サポート	IEEE802.2 の仕様に従って，TEST レスポンスを返送します。

この XID フレームおよび TEST フレームに対するレスポンスについて，次の表に示します。

表 18-12　XID フレームおよび TEST フレームに対するレスポンス

MAC ヘッダの DA	フレーム種別	DSAP	応答
ブロードキャストまたはマルチキャスト	XID および TEST	AA（SNAP） 42（BPDU） 00（null） FF（global）	返す
		上記以外	返さない
個別アドレスで自局アドレス	XID および TEST	AA（SNAP） 42（BPDU）	返す

MAC ヘッダの DA	フレーム種別	DSAP	応答
		00（null） FF（global）	
		上記以外	返さない
個別アドレスで他局アドレス	XID および TEST	すべてのアドレス	返さない

(4)　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。

- フレーム長がオクテットの整数倍ではない
- 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は，受信中に衝突が発生したフレーム

(5)　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。

18.2.3　VLAN Tag

(1)　概要

IEEE802.1Q 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，VLAN ID，および QoS のプライオリティを識別できます。

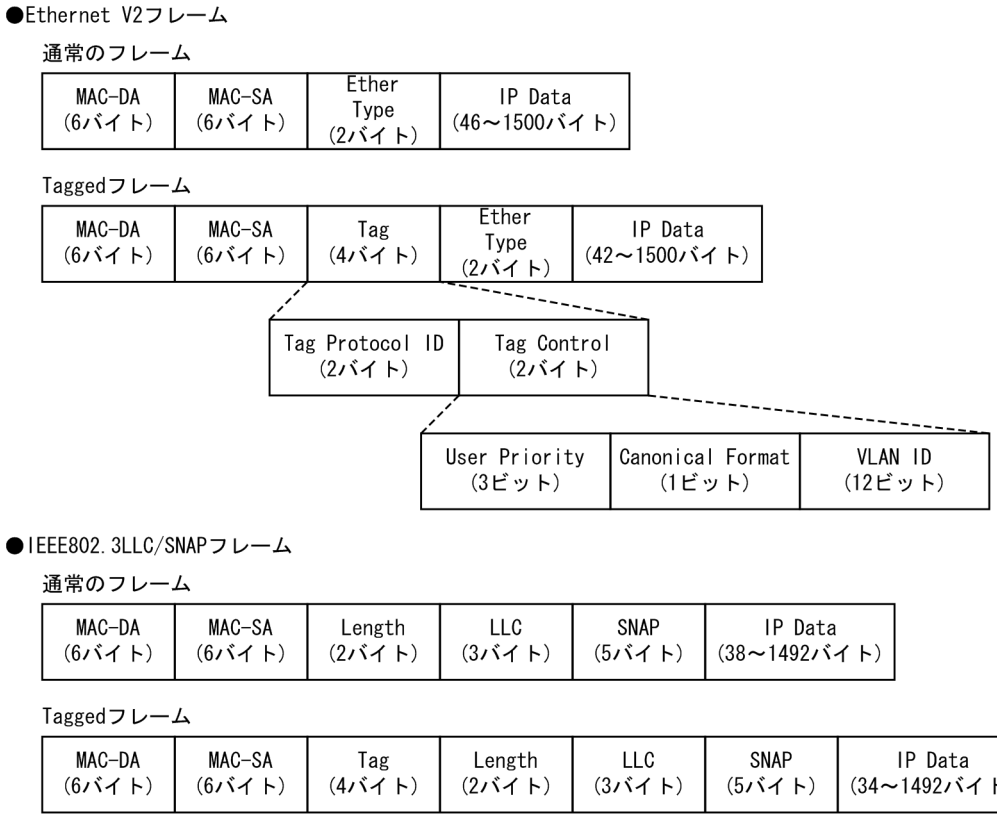
VLAN Tag は，VLAN のトランクポート，およびイーサネットサブインタフェースまたはポートチャネルサブインタフェースに VLAN Tag の VLAN ID を割り当てて，VLAN ID ごとに異なるインタフェースとして使用します。

(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伝えられます。

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には，Ethernet V2 フォーマットと IEEE802.3 フォーマットの 2 種類があります。

図 18-3　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 18-13　VLAN Tag のフィールド

フィールド	説明	本装置での扱い
TPID (Tag Protocol ID)	IEEE802.1Q VLAN Tag が続くことを示す EtherType 値を示します。	装置または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。VLAN ID ＝ 0 を受信した場合は，User Priority を識別します。
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。	IEEE802.1Q で規定の標準（0）かどうかの識別はしません。 • 自発パケットは常に標準（0）です。 • レイヤ 2 中継する Tag の CF ビットを引き継ぎます。
VLAN ID	VLAN ID を示します。	ユーザが使用できる VLAN ID は 1～4095 です。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 は送信しません。

(3)　TPID

VLAN Tag の TPID（Tag Protocol IDentifier）値は，装置のデフォルトでは 0x8100 を使用します。コンフィグレーションコマンド dot1q ethertype で任意の TPID 値を装置に，コンフィグレーションコマンド dot1q-ethertype で任意の TPID 値をポート単位に設定できます。装置およびポート単位の両方を設定した場合は，ポート単位の TPID 値が優先されます。

コンフィグレーションコマンドの設定（装置とポート単位の組み合わせ）と，該当ポートでの受信許容 TPID 値および送信 TPID 値の対応を次の表に示します。

表 18-14　コンフィグレーションコマンドの設定と該当ポートでの TPID 値の対応

コマンドの設定		ポートのフレーム送受信の TPID 値	
装置	ポート単位	受信許容 TPID 値	送信 TPID 値
設定なし	設定なし	0x8100	0x8100
任意の値	設定なし	装置の任意の値，0x8100	装置の任意の値
設定なし	任意の値	ポート単位の任意の値，0x8100	ポート単位の任意の値
任意の値	任意の値	ポート単位の任意の値，0x8100	ポート単位の任意の値

TPID 値はフレーム上で，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。TPID 値には EtherType 値として使用していない値を設定してください。

18.2.4　ジャンボフレーム

ジャンボフレームは，フレームフォーマットの MAC ヘッダから DATA 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。

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。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 18-15　ジャンボフレームサポート機能

項目	フレーム形式		備考
	Ethernet V2	IEEE802.3	
フレーム長（オクテット）	1519～9596	×	MAC ヘッダから DATA の長さ。FCS は含みません。
受信機能	○	×	IEEE802.3 フレームは，LENGTH フィールド値が 0x05DD（1501 オクテット）以上の場合に廃棄します。
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），1000BASE-T（全二重）だけをサポートします。

18.3　コンフィグレーション

18.3.1　コンフィグレーションコマンド一覧

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 18–16　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。
dot1q ethertype	本装置が付ける VLAN Tag の TPID 値を設定します。
dot1q-ethertype	ポートが付ける VLAN Tag の TPID 値を設定します。
duplex	全二重／半二重を設定します。
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 fortygigabitethernet	40GBASE-R のコンフィグレーションを指定します。
interface gigabitethernet	10BASE-T/100BASE-TX/1000BASE-T/1000BASE-X のコンフィグレーションを指定します。
interface hundredgigabitethernet	100GBASE-R のコンフィグレーションを指定します。
interface tengigabitethernet	10GBASE-R 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	イーサネットの最大フレーム長を設定します。
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 mtu	イーサネットの最大フレーム長の装置としての値を設定します。

18.3.2　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。接続インタフェースとモード移行コマンドの対応を次の表に示します。

表 18–17　接続インタフェースとモード移行コマンドの対応

接続インタフェース	モード移行コマンド
10BASE-T，100BASE-TX，1000BASE-T，1000BASE-X	interface gigabitethernet

接続インタフェース	モード移行コマンド
	interface tengigabitethernet※
10GBASE-R	interface tengigabitethernet
40GBASE-R	interface fortygigabitethernet
100GBASE-R	interface hundredgigabitethernet

注※
SFP+/SFP 共用ポートのモード移行コマンドは interface tengigabitethrenet です。

(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 1/10**
   イーサネットインタフェース 1/10 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。使用しないポートはシャットダウンしておいてください。また，この設定によってポートの電力を OFF にします。

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。

18.3.3　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 1/1-4, gigabitethernet 1/7-12, tengigabitethernet 3/1

   ギガビットイーサネットのインタフェース 1/1 から 1/4，1/7 から 1/12，および 10 ギガビットイーサネットのインタフェース 3/1 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。

18.3.4　速度と全二重/半二重の設定

本装置の 10BASE-T/100BASE-TX/1000BASE-T ポートおよび 1000BASE-X ポートは，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場合は，回線速度と全二重／半二重を設定します。

なお，回線速度と全二重／半二重が正しい組み合わせで設定されていない場合は，オートネゴシエーションで相手装置と接続します。

(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。

[コマンドによる設定]

1. (config)# interface gigabitethernet 1/1
   (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/100BASE-TX/1000BASE-T ポートで，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 1/10
   (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，10BASE-T/100BASE-TX/1000BASE-T ポート使用時に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，10BASE-T/100BASE-TX/1000BASE-T ポートで，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 1/10**

(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。

18.3.5 自動 MDI/MDIX 機能の設定

本装置の 10BASE-T/100BASE-TX/1000BASE-T ポートは，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，自動 MDI／MDIX 機能を無効にすることで，MDI 設定を MDI に固定できます。

[設定のポイント]

MDI 設定を MDI に固定する場合は，固定したいインタフェースで自動 MDI／MDIX 機能を無効にします。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/24**

イーサネットインタフェース 1/24 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 機能を無効にして，MDI 設定を MDI に固定します。

18.3.6　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 gigabitethernet 1/10**
   (config-if)# shutdown
   (config-if)# flowcontrol send on
   (config-if)# flowcontrol receive on
   イーサネットインタフェースをシャットダウンして，相手装置とのポーズパケット送受信を有効にします。
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。

18.3.7　VLAN Tag の TPID 値の設定

(1)　装置の TPID 値の設定

[設定のポイント]

装置の TPID 値を 0x9100 に設定します。全ポートで VLAN Tag を 0x9100 として動作します。

[コマンドによる設定]

1. **(config)# dot1q ethertype 9100**
   グローバルコンフィグレーションモードで装置の TPID 値を 0x9100 に設定します。

(2)　ポート単位の TPID 値の設定

[設定のポイント]

イーサネットインタフェース 1/1 の TPID 値を 0xa100 に設定します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/1**
   イーサネットインタフェース 1/1 のコンフィグレーションモードに移行します。
2. **(config-if)# dot1q-ethertype a100**
   イーサネットインタフェース 1/1 の TPID 値を 0xa100 に設定します。

18.3.8　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最大フレーム長（MAC ヘッダから DATA まで）は規格上 1518 オクテットです。本装置は，ジャンボフレームを使用して最大フレーム長を拡張して，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最大フレーム長を設定します。ポートの最大フレーム長の設定値は，ネットワークおよび相手装置と合わせて決定します。

(1) ポート単位の最大フレーム長の設定

[設定のポイント]

ポート 1/10 のポートの最大フレーム長を 8192 オクテットに設定します。この設定によって，8192 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 1/10**
   (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，ポートの最大フレーム長を 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最大フレーム長を設定していても，10BASE-T または 100BASE-TX 半二重で接続する場合（オートネゴシエーションの結果が 10BASE-T または 100BASE-TX 半二重になった場合も含みます）は，ポートの最大フレーム長は 1518 オクテットになります。

(2) 全ポート共通の最大フレーム長の設定

[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最大フレーム長を 4096 オクテットに設定します。この設定によって，4096 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，ポートの最大フレーム長を 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最大フレーム長を設定していても，10BASE-T または 100BASE-TX 半二重で接続する場合（オートネゴシエーションの結果が 10BASE-T または 100BASE-TX 半二重になった場合も含みます）は，ポートの最大フレーム長は 1518 オクテットになります。

18.3.9 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と，リンクが不安定になることを防げます。

[設定のポイント]

リンクダウン検出時間は，リンクが不安定に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にならない場合は，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 1/10**

イーサネットインタフェース 1/10 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げますが，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。

18.3.10　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と，ネットワーク状態が不安定になることを防げます。

[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に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にならない場合は，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 1/10**

イーサネットインタフェース 1/10 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。

18.3.11　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 パラメータを設定します。

[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 パラメータを設定します。

[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 パラメータを設定します。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

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回数（エラーフレーム数）の閾値を設定する場合の設定例を示します。

[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]

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 回に設定して，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。

18.3.12 SFP+/SFP 共用ポートの設定

SFP+/SFP 共用ポートを SFP で使用するため，1000BASE-X に設定します。コンフィグレーションの設定後に NIF を再起動すると，1000BASE-X で動作できます。

[設定のポイント]

NLXG-6RS で同一の NIF に SFP と SFP+の両方を収容する場合，ポート 1～4 を同一の回線速度，ポート 5，6 を同一の回線速度に設定します。

NLXGA-12RS で同一の NIF に SFP と SFP+の両方を収容する場合, SFP はポート 12 から降順で連続するポート番号，SFP+はポート 1 から昇順で連続するポート番号に設定します。

この例では，NLXG-6RS の SFP+/SFP 共用ポートで，SFP+を使用した 10GBASE-R インタフェースで運用しているポートから，SFP を使用した 1000BASE-X インタフェースのポートへ移行します。

[コマンドによる設定]

1. **(config)# interface range tengigabitethernet 1/1-4**

   (config-if-range)# shutdown

   SFP+/SFP 共用ポートを SFP で使用するため，コンフィグレーションモードに移行して，ポート 1/1 から 1/4 をシャットダウン状態にします。

   その後，SFP+を取り外します。

2. **(config-if-range)# speed auto 1000**

   回線速度を 1000BASE-X の設定にします。この設定によって，SFP+/SFP 共用ポート設定の移行状態を表すシステムメッセージが出力されます。

3. **(config-if-range)# exit**

   (config)# end

   NIF を再起動するために，コンフィグレーションモードから装置管理者モードに戻ります。

4. **# reload nif 1**

   Are you sure you want to restart nif 1? (y/n): y

   装置管理者モードで，SFP+/SFP 共用ポートの設定をした NIF を再起動します。再起動することで，SFP が使用できる 1000BASE-X インタフェースとなります。

   その後，SFP を取り付けます。

5. **(config)# interface range tengigabitethernet 1/1-4**

   (config-if-range)# no shutdown

   コンフィグレーションモードに移行して，ポート 1/1 から 1/4 のシャットダウン状態を解除します。

[注意事項]

SFP+/SFP 共用ポートのポート組み合わせが不完全なコンフィグレーションを設定した状態で, NIF の再起動や NIF の交換をした場合，該当する NIF の全ポートが 10GBASE-R（SFP+）で起動します。

18.4　オペレーション

18.4.1　運用コマンド一覧

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 18-18　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。
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。

18.4.2　イーサネットの動作状態の確認

show port コマンドを実行すると，本装置に搭載している NIF のイーサネットの状態を確認できます。使用するイーサネットの Status の表示が up になっていることを確認します。コマンドの実行結果を次の図に示します。

図 18-4　show port コマンドの実行結果

```
> show port
Date 20XX/04/01 12:00:00 UTC
Port Counts: 12
Port  Status   Speed          Duplex     FCtl FrLen Description
 1/1  up       1000BASE-SX    full(auto) off  1518  server 100
 1/2  up       1000BASE-SX    full       on   1518  server 101
 1/3  dis      1000BASE-SX    full(auto) -    -     server 102
 1/4  inact    1000BASE-SX    full(auto) -    -     -
      :
      :
```

19 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。

19.1　リンクアグリゲーション基本機能の解説

19.1.1　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て，それらを束ねて一つのポートとして扱う機能です。この束ねた一つのポート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。

19.1.2　リンクアグリゲーションの構成

(1)　ポートの追加および削除

チャネルグループを構成するポートは，コンフィグレーションで設定します。コンフィグレーションによるポートの設定を追加，コンフィグレーションによるポートの削除を削除と呼びます。

- 追加（add）：チャネルグループ内にポートを追加します。
- 削除（remove）：チャネルグループ内のポートを削除します。

(2)　ポートの集約および離脱

ポートをチャネルグループとして動作させることを集約，チャネルグループとしての動作からポートを除外することを離脱と呼びます。

- 集約（attach）：チャネルグループ内のポートを通信可能にします。
- 離脱（detach）：チャネルグループ内のポートを通信停止にします。

(3)　チャネルグループの UP および DOWN

チャネルグループ内のポートが一つでも集約されると，チャネルグループは UP となります。UP になるとチャネルグループを使用して通信できます。

チャネルグループ内のポートがすべて離脱すると，チャネルグループは DOWN となります。DOWN になるとチャネルグループを使用した通信が停止します。

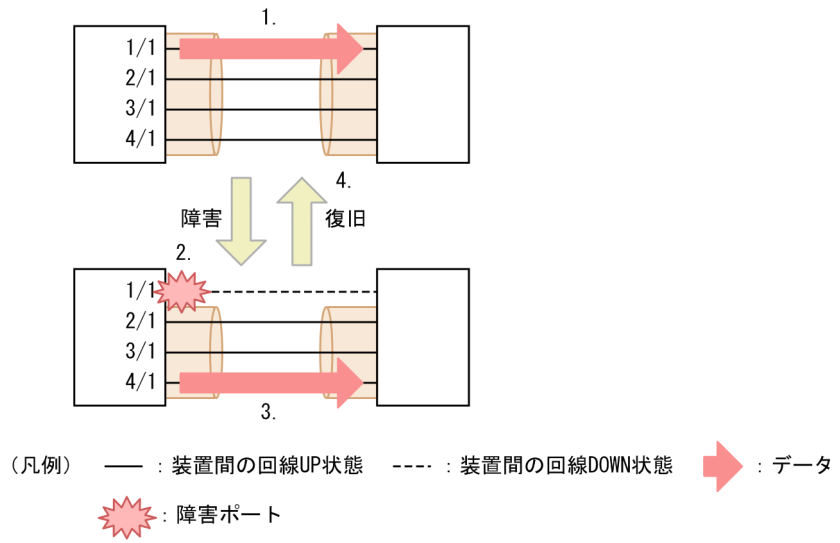
(4)　切り替えおよび切り戻し

フレーム送信ポートは集約しているポートから選択します。フレーム送信ポートが障害などによって変更となる動作を切り替え，障害から復旧してフレーム送信ポートが元のポートに戻る動作を切り戻しと呼びます。

(5)　構成例

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一つが障害となった場合には，チャネルグループから離脱して，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 19-1　リンクアグリゲーションの構成例



1. 4 ポートを集約しています。フレームはポート 1/1 から送信します。
2. ポート 1/1 に障害が発生したため，チャネルグループから離脱します。また，フレーム送信ポートを切り替えます。
3. 離脱したポート 1/1 を除いた 3 ポートを集約しています。フレームはポート 4/1 から送信します。
4. ポート 1/1 が障害から復旧したため，チャネルグループに集約します。また，フレーム送信ポートを切り戻します。

19.1.3　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
  IEEE 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追加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)　リンクアグリゲーションのサポート仕様

リンクアグリゲーションのサポート仕様を次の表に示します。

表 19-1　リンクアグリゲーションのサポート仕様

項目	サポート仕様
リンクアグリゲーションのモード	• LACP • スタティック

項目	サポート仕様
回線速度	• デフォルト時（異速度混在モード未設定） 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。 • 異速度混在モード時 チャネルグループを構成するすべてのポートを同時に集約します。
Duplex モード	• LACP リンクアグリゲーション 全二重で動作しているポートを集約します。 • スタティックリンクアグリゲーション 全二重または半二重で動作しているポートを集約します。チャネルグループ内で Duplex モードの混在を許容します。

19.1.4　チャネルグループの MAC アドレス

本装置は，チャネルグループの MAC アドレスとして，チャネルグループごとにユニークな MAC アドレスを使用します。

LACP リンクアグリゲーションでは，装置 MAC アドレスを装置識別子として使用します。

19.1.5　フレーム送信時のポート振り分け

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て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。ポートの振り分け方法には次に示す 3 種類があり，コンフィグレーションによってチャネルグループごとに指定できます。

- フレーム内情報によるポート振り分け
- VLAN Tag ごとのポート振り分け
- ロードバランスグループごとのポート振り分け

(1)　フレーム内情報によるポート振り分け

フレーム内の情報を基にポートを選択して送信します。レイヤ 2 中継時，IP レイヤ中継時，および自発送信時の参照情報をそれぞれの表に示します。

表 19-2　レイヤ 2 中継時の参照情報

分類	参照情報
IP のフレーム	• 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
その他のフレーム	• 宛先 MAC アドレス • 送信元 MAC アドレス

表 19-3　IP レイヤ中継時の参照情報

分類	参照情報
IP のフレーム	• 宛先 IP アドレス • 送信元 IP アドレス
その他のフレーム	−

（凡例）−：該当しない

表 19-4　自発送信時の参照情報

分類	参照情報
IP のフレーム	• 宛先 IP アドレス • 送信元 IP アドレス
その他のフレーム	• 宛先 MAC アドレス • 送信元 MAC アドレス

(2)　VLAN Tag ごとのポート振り分け

送信するフレームの VLAN Tag ごとにポートを選択して送信します。VLAN Tag ごとのポート振り分け動作を次の表に示します。

表 19-5　VLAN Tag ごとのポート振り分け動作

動作分類	情報元
レイヤ 2 中継	フレームを送信する VLAN Tag ごとに振り分け
IP レイヤ中継	
自発送信	送信する VLAN Tag ごとに振り分け

(3)　ロードバランスグループごとのポート振り分け

(a)　概要

ポートチャネルインタフェースまたはポートチャネルサブインタフェースをロードバランスグループと呼ばれる単位でグループ化して，フレームの送信先をポート単位で振り分けます。フレーム送信ポートとして最初に選択する第 1 優先ポート，次に選択する第 2 優先ポートをコンフィグレーションで指定します。本機能は，VLAN に所属しないポートだけに設定できます。

(b)　振り分け先の決定方法

第 1 優先ポートと第 2 優先ポートの状態（集約または離脱）によって，振り分け先のポートを選択します。第 1 優先ポートおよび第 2 優先ポート以外では，VLAN Tag ごとのポート振り分けに従ってポートを選択します。第 1 優先ポートと第 2 優先ポートの状態による振り分け先一覧を次の表に示します。

表 19-6　第 1 優先ポートと第 2 優先ポートの状態（集約または離脱）による振り分け先一覧

ポートの状態	振り分け先
第 1 優先ポートが集約	第 1 優先ポートを選択

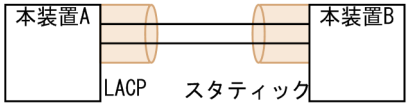
ポートの状態	振り分け先
第 1 優先ポートが離脱 第 2 優先ポートが集約 その他のポートが集約	第 2 優先ポートを選択
第 1 優先ポートが離脱 第 2 優先ポートが離脱 その他のポートが集約	VLAN Tag ごとのポート振り分けに従ってポートを選択

19.1.6　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

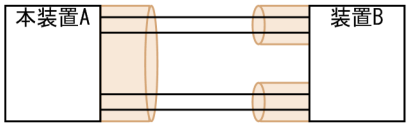
リンクアグリゲーション構成時には，装置間での設定が一致している必要があります。リンクアグリゲーションが不可能な構成例を次に示します。

図 19-2　装置間でモードが異なる構成



この図のように装置間でモードが異なる構成にすると，LACP のネゴシエーションが成立しないで通信断状態になります。

図 19-3　装置間でチャネルグループがポイントーマルチポイントである構成



この図のように装置間でチャネルグループがポイントーマルチポイントである構成にすると，本装置 A から送信したフレームが装置 B を経由して戻るループ構成となるなど，正常に動作しません。

(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はリンクダウン状態で設定して，「(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。

19.2　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

19.2.1　コンフィグレーションコマンド一覧

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 19-7　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 load-balance	フレーム送信時のポート振り分け方法を指定します。
channel-group load-balance-group	ポートチャネルインタフェースまたはポートチャネルサブインタフェースをロードバランスグループに追加します。
channel-group load-balance-group name	ロードバランスグループ名称を指定します。
channel-group load-balance-group priority	ロードバランスグループごとのフレーム送信ポートの優先度を指定します。
channel-group mode	ポートをチャネルグループへ追加します。また，チャネルグループのモードを設定します。
channel-group periodic-timer	対向装置の 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またはポートチャネルサブインタフェースを設定します。
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。

19.2.2　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，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と自動で生成されます。

(1)　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，IP アドレス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，ポートチャネルインタフェース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 1/1-2
(config-if-range)# channel-group 10 mode on
```

```
(config-if-range)# exit
```

ポート 1/1, 1/2 をスタティックモードのチャネルグループ 10 に追加します。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 のコンフィグレーションモードに移行します。

3. `(config-if)# ip address 192.0.2.1 255.255.255.0`

ポートチャネルに IP アドレスを設定します。

(2) ポートチャネルインタフェースの shutdown

[設定のポイント]

ポートチャネルを shutdown に設定すると, チャネルグループに追加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，リンクアップした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 1/1-2
(config-if-range)# channel-group 10 mode on
(config-if-range)# exit
```

ポート 1/1，1/2 をスタティックモードのチャネルグループ 10 に追加します。

2.
```
(config)# interface port-channel 10
(config-if)# shutdown
```

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 1/1，1/2 の通信が停止して，チャネルグループ 10 は停止状態になります。

19.2.3 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，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と動作を開始します。

[コマンドによる設定]

1. `(config)# interface range gigabitethernet 1/1-2`

ポート 1/1，1/2 のコンフィグレーションモードに移行します。

2. `(config-if-range)# channel-group 10 mode on`

ポート 1/1，1/2 を，スタティックモードのチャネルグループ 10 に追加します。

19.2.4 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，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 1/1-2**

   ポート 1/1，1/2 のコンフィグレーションモードに移行します。

2. **(config-if-range)# channel-group 10 mode active**

   ポート 1/1，1/2 を LACP モードのチャネルグループ 10 に追加します。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)　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，リンクダウンを伴わない障害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られます。

[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ため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）にすると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。

19.2.5　振り分け方法の設定

フレーム送信時のポート振り分け方法を設定します。

(1)　フレーム内情報によるポート振り分け

[設定のポイント]

チャネルグループにフレーム内情報によるポート振り分けを設定します。

[コマンドによる設定]

1. **(config)# interface port-channel 10**

   (config-if)# channel-group load-balance frame

   チャネルグループ 10 の振り分け方法を，フレーム内情報によるポート振り分けに設定します。

(2)　VLAN Tag ごとのポート振り分け

[設定のポイント]

チャネルグループに VLAN Tag ごとのポート振り分けを設定します。

[コマンドによる設定]

1. **(config)# interface port-channel 10**

```
(config-if)# channel-group load-balance vlan
```

チャネルグループ 10 の振り分け方法を，VLAN Tag ごとのポート振り分けに設定します。

(3) ロードバランスグループごとのポート振り分け

[設定のポイント]

フレーム送信時の振り分け方法をロードバランスグループごとに設定して，関連のコンフィグレーションを設定するとロードバランスグループごとのポート振り分けができます。

ロードバランスグループ関連のコンフィグレーションに第 1 優先ポートおよび第 2 優先ポートのどちらも指定がない場合，VLAN Tag ごとのポート振り分けで動作します。

[コマンドによる設定]

1.
```
(config)# interface range gigabitethernet 1/1, gigabitethernet 2/1, gigabitethernet 3/1, gigabitethernet 4/1
(config-if-range)# channel-group 10 mode on
(config-if-range)# exit
```

ポート 1/1，2/1，3/1，4/1 をスタティックモードのチャネルグループ 10 に追加します。

2.
```
(config)# interface port-channel 10
(config-if)# channel-group load-balance load-balance-group
(config-if)# exit
```

チャネルグループ 10 の振り分け方法を，ロードバランスグループごとのポート振り分けに設定します。

3.
```
(config)# channel-group load-balance-group name LBG100
```

ロードバランスグループ名称を LBG100 として設定します。

4.
```
(config)# interface port-channel 10.100
(config-subif)# encapsulation dot1q 100
(config-subif)# ip address 192.0.2.100 255.255.255.0
```

ポートチャネルサブインタフェース 10.100 で使用する VLAN Tag 100，IP アドレス 192.0.2.100 を設定します。

5.
```
(config-subif)# channel-group load-balance-group LBG100
(config-subif)# exit
```

ポートチャネルサブインタフェース 10.100 にロードバランスグループ LBG100 を設定します。

6.
```
(config)# interface gigabitethernet 1/1
(config-if)# channel-group load-balance-group LBG100 priority primary
(config-if)# exit
```

チャネルグループ 10 に所属しているポート 1/1 をロードバランスグループ LBG100 の第 1 優先ポートとして設定します。

7.
```
(config)# interface gigabitethernet 2/1
(config-if)# channel-group load-balance-group LBG100 priority secondary
(config-if)# exit
```

チャネルグループ 10 に所属しているポート 2/1 をロードバランスグループ LBG100 の第 2 優先ポートとして設定します。

19.2.6　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。

(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します。

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 の設定は自動で削除されません。チャネルグループ全体の削除については，「(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 1/1**
   (config-if)# shutdown
   ポート 1/1 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**
   チャネルグループからポート 1/1 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追加されていたポートはそれぞれ個別のポートとして動作します。

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，追加していた各ポートから channel-group mode コマンドの設定が自動で削除されます。

[コマンドによる設定]

1. **(config)# interface range gigabitethernet 1/1-2**
   (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追加されているポートをすべて shutdown に設定して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 1/1，1/2 に設定されている channel-group mode コマンドの設定も自動で削除されます。

19.2.7　チャネルグループをスイッチポートで使用する場合のポイント

(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では，チャネルグループ上で動作する機能を設定します。それらの機能は，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でも設定できます。

このような機能を設定するコマンドには，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があります。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がある，ポートチャネルインタフェースの関連コマンドを次の表に示します。

表 19-8　ポートチャネルインタフェースの関連コマンド

機能	関連コマンド
VLAN	switchport access
	switchport isolate
	switchport mode
	switchport trunk
	switchport vlan mapping
	switchport vlan mapping enable
スパニングツリー	spanning-tree bpdufilter
	spanning-tree bpduguard
	spanning-tree cost
	spanning-tree guard
	spanning-tree link-type
	spanning-tree mst cost
	spanning-tree mst port-priority
	spanning-tree port-priority
	spanning-tree portfast
	spanning-tree single cost
	spanning-tree single port-priority
	spanning-tree vlan cost
	spanning-tree vlan port-priority
L2 ループ検知	loop-detection

(2)　チャネルグループ設定時の推奨手順

関連コマンドを設定するときは，ポートチャネルインタフェースを指定して設定してください。

ポートチャネルインタフェースに関連コマンドを設定すると，channel-group mode コマンドが設定されているイーサネットインタフェースにも同じ設定が反映されます。

(3)　関連コマンド設定時の制限事項

- ポートチャネルインタフェースを設定していない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，自動でポートチャネルインタフェースを生成します。このとき，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ると，channel-group mode コマンドを設定できません。

- 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，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に設定されている関連コマンドが一致していないと，channel-group mode コマンドを設定できません。

19.3　リンクアグリゲーション拡張機能の解説

19.3.1　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げます。

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。

(2)　スタンバイリンクの選択方法

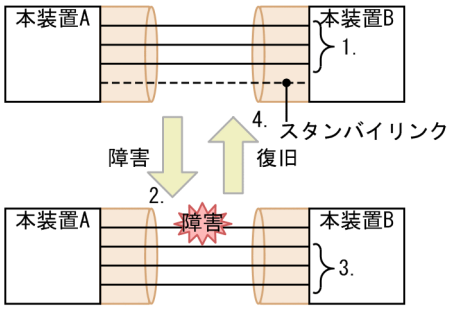
コンフィグレーションでチャネルグループとして運用する最大ポート数を設定します。グループに所属するポートのうち，設定した最大ポート数を超えた分のポートが待機用ポートになります。

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 NIF 番号およびポート番号の順で，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，NIF 番号，ポート番号の順に判断します。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. NIF 番号
   NIF 番号の大きい順に待機用ポートとして選択されます。
3. 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構成例を次の図に示します。この例では，グループに所属するポート数を 4，運用する最大ポート数を 3 としています。

図 19-4　スタンバイリンク機能の構成例



1. 4 ポートのチャネルグループに対して，3 ポートの使用を設定します。
2. リンク障害が発生しました。
3. スタンバイリンクを使用して，帯域減なしでリンクアグリゲーションを運用します。
4. リンク障害が復旧しました。

(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。この機能は本装置だけに設定してください。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，待機用ポートでも障害を監視できます。また，待機用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とも接続できます。

(4)　スタンバイリンクの各モードでのチャネルグループ状態

リンクダウンモードを使用している場合，集約ポートが一つの状態でそのポートで障害が発生すると，待機用ポートに切り替わるときにチャネルグループがいったん DOWN になります。非リンクダウンモードの場合，DOWN にならないで待機用ポートを使用します。

集約ポートが一つの状態とは，次に示すどちらかの状態です。

- 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。
- 異速度混在モードを未設定で，最高速のポートが一つだけ，そのほかのポートが一つ以上ある状態。

19.3.2　離脱ポート数制限機能

(1)　解説

離脱ポート数制限機能とは，離脱ポート数がコンフィグレーションの最大離脱ポート数を超えた場合に，チャネルグループ全体を障害と見なして該当チャネルグループを DOWN にする機能です。

離脱ポート数制限機能は，LACP リンクアグリゲーションだけで使用できます。この機能は，本装置だけに設定することを推奨します。

(2)　離脱ポート数制限機能での LACP システム優先度

離脱ポート数制限機能使用時は，本装置の LACP システム優先度を対向装置より高くすることを推奨します。どちらの装置が高い優先度を持つかは，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 LACP システム ID の MAC アドレスの順で判断されます。すなわち，LACP システム優先度が同じ場合は，LACP システム ID の MAC アドレスで判断します。なお，本装置では LACP システム ID の MAC アドレスに装置 MAC アドレスを使用します。

離脱ポート数制限機能を動作させ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. LACP システム ID の MAC アドレス
   MAC アドレスの小さい装置が優先されます。

19.3.3 異速度混在モード

(1) 解説

異なる速度のポートを一つのチャネルグループで同時に使用するモードです。通常は同じ速度のポートでチャネルグループを構成しますが, 異なる速度のポートで構成することでチャネルグループの構成を容易に変更できます。

なお, フレーム送信時のポート振り分けには回線速度は反映しません。例えば, 異速度混在モードで 1Gbit/s のポートと 10Gbit/s のポートを使用していても，その速度の差はフレーム振り分けには反映しません。通常の運用時は同じ速度のポートで運用することをお勧めします。

(2) チャネルグループの構成変更例

本機能によって，チャネルグループで利用する回線速度を変更（ネットワーク構成の変更）するときに，チャネルグループを DOWN にしないで構成を変更できます。

異速度混在モードを利用したチャネルグループの速度移行について, 手順の具体例を次に示します。この手順で示すコンフィグレーションは，本装置と対向装置それぞれで設定してください。

1. 従来状態で運用（1Gbit/s の 2 ポートとします）
2. 異速度混在モードを設定
3. チャネルグループに 10Gbit/s の 2 ポートを追加
4. 手順 3 で追加した 10Gbit/s の 2 ポートをリンクアップ
5. 従来の 1Gbit/s の 2 ポートにコンフィグレーションコマンド shutdown を設定
6. 従来の 1Gbit/s の 2 ポートをチャネルグループから削除
7. 異速度混在モードを削除
8. 10Gbit/s の 2 ポートに移行完了

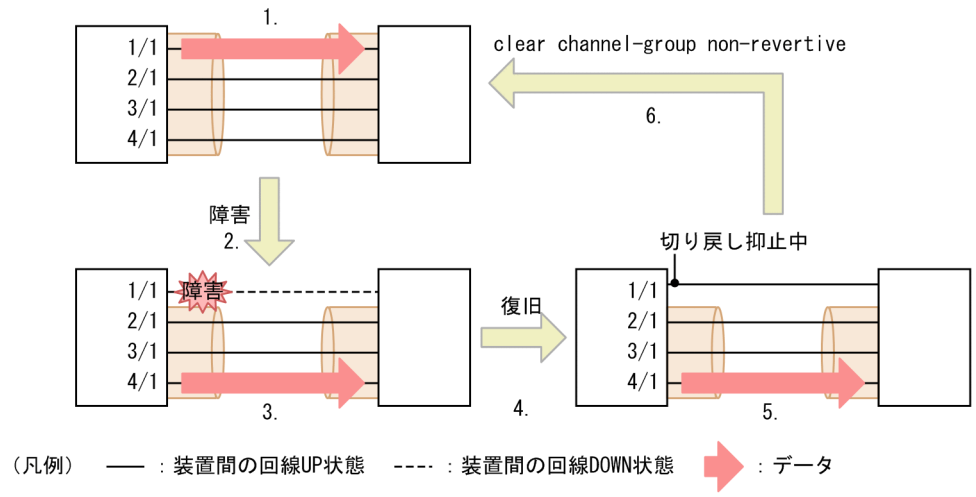
19.3.4 切り戻し抑止機能

(1) 解説

切り戻し抑止機能とは，チャネルグループに集約しているポートが障害などで離脱したあと，障害から復旧した場合に切り戻しを抑止する機能です。

切り戻し抑止中のポートを集約するには，運用コマンド clear channel-group non-revertive を実行します。運用コマンドで切り戻し抑止中のポートを集約するため, 運用に影響が少ないタイミングでオペレータが意図的に切り戻しできます。切り戻し抑止機能の概要を次の図に示します。

図 19-5　切り戻し抑止機能の概要



1. 4 ポートを集約しています。フレームはポート 1/1 から送信します。
2. ポート 1/1 に障害が発生したため，チャネルグループから離脱します。また，フレーム送信ポートを切り替えます。
3. 離脱したポート 1/1 を除いた 3 ポートを集約しています。フレームはポート 4/1 から送信します。
4. ポート 1/1 が障害から復旧します。
5. ポート 1/1 は切り戻し抑止中のポートです。フレームはポート 4/1 から送信します（変更しません）。
6. 運用コマンド clear channel-group non-revertive を実行して，ポート 1/1 をチャネルグループに集約します。また，フレーム送信ポートを切り戻します。

(2)　切り戻し抑止機能の遅延時間

チャネルグループとして追加したポートをすべて集約するため，チャネルグループが DOWN から UP に遷移するときは切り戻し抑止機能が動作しません。チャネルグループが UP になってから切り戻し抑止機能が動作するまでの遅延時間を，コンフィグレーションコマンド non-revertive で設定できます。遅延時間が満了するまでの間，切り戻し抑止機能は無効となります。

遅延時間が満了するまでの間に系切替が発生すると，遅延時間を更新します。スタティックリンクアグリゲーションでは，運用系 BCU で遅延時間が満了している場合でも，待機系 BCU の起動から遅延時間分経過するまでの間に系切替が発生すると，遅延時間を再更新します。そのため，再び遅延時間が満了するまで，切り戻し抑止機能は無効となります。

(3)　切り戻し抑止機能動作時の障害について

集約ポートがなくなったときに切り戻し抑止ポートがある場合，切り戻し抑止ポートを自動で集約します。

(4)　切り戻し抑止機能の設定について

切り戻し抑止機能は，本装置だけに設定してください。また，LACP リンクアグリゲーションで切り戻し抑止機能を使用する場合は，本装置の LACP システム優先度を対向装置より高くすることを推奨します。

(5)　異なる速度のポートで構成するリンクアグリゲーションでの動作

集約しているポートよりも高速な回線を追加する場合，これまで集約していたポートは離脱します。また，追加したポートは切り戻し抑止機能によって集約しません。このため，集約しているポートがなくなって，

チャネルグループが DOWN します。そのあと，「(3)　切り戻し抑止機能動作時の障害について」に従って追加したポートを集約すると，チャネルグループが UP します。

切り戻し抑止機能を優先する場合は，異速度混在モードを使用してください。

(6)　スタンバイリンク機能との併用

スタティックリンクアグリゲーションでスタンバイリンク機能を使用している場合, 切り戻し抑止中のポートに対して運用コマンド clear channel-group non-revertive を実行すると，該当ポートは次のどちらかになります。

- スタンバイポートになる
- チャネルグループに集約される

19.4　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

19.4.1　コンフィグレーションコマンド一覧

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 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
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。離脱ポート数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	離脱ポート数制限機能を設定します。
channel-group multi-speed	異速度混在モードを設定します。
channel-group non-revertive	チャネルグループに切り戻し抑止機能を設定します。
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。離脱ポート数制限機能で集約条件を判定する装置を決定します。

19.4.2　スタンバイリンク機能の設定

[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。

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。

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。

[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 として，非リンクダウンモードを設定します。

5. **(config)# interface gigabitethernet 1/1**
   (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 1/1 を追加して，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。

19.4.3　離脱ポート数制限機能の設定

[設定のポイント]

チャネルグループに離脱ポート数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を指定します。15 を指定した場合は離脱ポート数制限機能を設定しない場合と同じです。

離脱ポート数制限機能は，LACP リンクアグリゲーションだけで使用できます。この機能は本装置だけに設定して，対向装置よりも本装置の LACP システム優先度を高くすることを推奨します。

[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 に離脱ポート数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 として，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見なします。
3. **(config-if)# channel-group lacp system-priority 100**
   チャネルグループ 10 の LACP システム優先度を 100 に設定します。

19.4.4　異速度混在モードの設定

[設定のポイント]

チャネルグループに異速度混在モードを設定します。本機能を設定すると，回線速度は離脱条件ではなくなります。

[コマンドによる設定]

1. **(config)# interface port-channel 10**
   チャネルグループ 10 のコンフィグレーションモードに移行します。
2. **(config-if)# channel-group multi-speed**
   チャネルグループ 10 に異速度混在モードを設定します。

19.4.5　切り戻し抑止機能の設定

[設定のポイント]

チャネルグループに切り戻し抑止機能を設定します。本機能を設定すると，チャネルグループに集約しているポートが障害などで離脱したあと，障害から復旧したときに自動で集約することを抑止します。

[コマンドによる設定]

1.**(config)# interface port-channel 10**

チャネルグループ 10 のコンフィグレーションモードに移行します。

2.**(config-if)# channel-group non-revertive**

チャネルグループ 10 に切り戻し抑止機能を設定します。

19.5　リンクアグリゲーションのオペレーション

19.5.1　運用コマンド一覧

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 19-10　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。
clear channel-group non-revertive	リンクアグリゲーションの切り戻し抑止状態を解除します。
restart lacp	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 lacp	リンクアグリゲーション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。

19.5.2　リンクアグリゲーションの状態の確認

(1)　リンクアグリゲーションの接続状態の確認

リンクアグリゲーションの情報を show channel-group コマンドで表示します。CH Status でチャネルグループの接続状態を確認できます。また，設定が正しいことを各項目で確認してください。

show channel-group コマンドの実行結果を次の図に示します。

図 19-6　show channel-group コマンドの実行結果

```
> show channel-group
Date 20XX/04/01 12:00:00 UTC
ChGr:1      Mode:LACP
  CH Status:Up          Elapsed Time:10:10:39          Bandwidth:3000000kbps
  Multi Speed:Off    Load Balance:frame
  Non Revertive:On
  Max Active Port:16
  Max Detach Port:15
  Description:4 ports aggregated.
  MAC address:0012.e2ac.8301
  Periodic Timer:Short
  Actor information
    System Priority:1        MAC:0012.e212.ff02    KEY:1
  Partner information
    System Priority:10000    MAC:0012.e2f0.69be    KEY:10
  Port(4)         :1/1-4
  Up Port(3)      :1/1-3
  Down Port(1)    :1/4
>
```

(2)　各ポートの運用状態の確認

show channel-group detail コマンドで各ポートの詳細な状態を表示します。ポートの通信状態を Status で確認してください。Status が Down 状態のときは Reason で理由を確認できます。

show channel-group detail コマンドの実行結果を次の図に示します。

図 19-7　show channel-group detail コマンドの実行結果

```
> show channel-group detail
Date 20XX/04/01 12:00:00 UTC
ChGr:1      Mode:LACP
  CH Status:Up          Elapsed Time:10:10:39          Bandwidth:3000000kbps
  Multi Speed:Off    Load Balance:frame
  Non Revertive:On
  Max Active Port:16
  Max Detach Port:15
  Description:4 ports aggregated.
  MAC address:0012.e2ac.8301
  Periodic Timer:Short
  Actor information
    System Priority:1        MAC:0012.e212.ff02    KEY:1
  Partner information
    System Priority:10000    MAC:0012.e2f0.69be    KEY:10
  Port:1/1      Status:Up      Reason:-
                Speed:1G      Duplex:Full    LACP Activity:Active
                Actor Priority:128      Partner Priority:100
  Port:1/2      Status:Up      Reason:-
                Speed:1G      Duplex:Full    LACP Activity:Active
                Actor Priority:128      Partner Priority:100
  Port:1/3      Status:Up      Reason:-
                Speed:1G      Duplex:Full    LACP Activity:Active
                Actor Priority:128      Partner Priority:100
  Port:1/4      Status:Down    Reason:Non Revertive
                Speed:1G      Duplex:Full    LACP Activity:Active
                Actor Priority:128      Partner Priority:100
>
```

(3)　切り戻し抑止状態の確認と解除

切り戻し抑止状態は clear channel-group non-revertive コマンドで解除します。切り戻し抑止状態の確認と解除例を次に示します。

1. show channel-group detail コマンドで，ポート 1/4 が切り戻し抑止状態であることを確認します。

```
> show channel-group detail
                :
                :
  Port:1/4      Status:Down    Reason:Non Revertive
                Speed:1G      Duplex:Full    LACP Activity:Active
                Actor Priority:128      Partner Priority:100
                :
                :
>
```

2. clear channel-group non-revertive コマンドで，ポート 1/4 の切り戻し抑止状態を解除します。

```
> clear channel-group non-revertive port 1/4
Are you sure you want to make the channel-group revertive? (y/n) :y
>
```

3. show channel-group detail コマンドで，ポート 1/4 が集約されていることを確認します。

```
> show channel-group detail
                :
                :
  Port:1/4      Status:Up      Reason:-
                Speed:1G      Duplex:Full    LACP Activity:Active
                Actor Priority:128      Partner Priority:100
                :
                :
>
```

20 IP インタフェースとサブインタフェース

この章では，インタフェースに IP アドレスを設定して通信する方法について説明します。

20.1　解説

20.1.1　概要

IPv4 アドレスまたは IPv6 アドレスを設定したインタフェースを IP インタフェースと呼びます。インタフェースには，IPv4 アドレスもしくは IPv6 アドレスの一方，または両方を設定できます。

IP アドレスを設定できるインタフェースの種類を，次の表に示します。

表 20-1　IP アドレスを設定できるインタフェースの種類

インタフェースの種類	説明
イーサネットインタフェース	イーサネットインタフェースに直接 IP アドレスを設定します。1 ポートを一つのインタフェースとして使用できます。
イーサネットサブインタフェース	イーサネットインタフェースにインデックスを割り当てて，VLAN Tag の VLAN ID を設定します。これによって，VLAN Tag ごとに異なるインタフェースとして使用できます。サブインタフェースに IP アドレスを設定します。
ポートチャネルインタフェース	ポートチャネルインタフェースに直接 IP アドレスを設定します。チャネルグループの 1 グループを一つのインタフェースとして使用できます。
ポートチャネルサブインタフェース	ポートチャネルインタフェースにインデックスを割り当てて，VLAN Tag の VLAN ID を設定します。これによって，VLAN Tag ごとに異なるインタフェースとして使用できます。サブインタフェースに IP アドレスを設定します。
VLAN インタフェース	VLAN インタフェースに直接 IP アドレスを設定します。一つの VLAN ID を一つのインタフェースとして使用できます。
マネージメントポート	リモート運用端末を接続するためのツイストペアケーブル（UTP）を使用したインタフェースです。直接 IP アドレスを設定します。
シリアル接続ポート（AUX）	リモート運用端末を接続するためのシリアル接続ポート（AUX）を使用したインタフェースです。直接 IP アドレスを設定します。
ループバックインタフェース	装置本体を示す特殊なインタフェースです。IP アドレスを設定します。
Null インタフェース	物理回線に依存しないパケット廃棄用の仮想的なインタフェースです。IP アドレスは指定できません。

なお，このマニュアルでは，IP インタフェースを単に，インタフェースと表現することがあります。

20.1.2　サブインタフェース

サブインタフェースは，イーサネットサブインタフェースとポートチャネルサブインタフェースの総称です。サブインタフェースは元となるイーサネットのポート番号またはポートチャネルのチャネルグループ番号に，サブインタフェースインデックス（サブインタフェースを識別するための番号）をピリオド（.）でつないで表します。

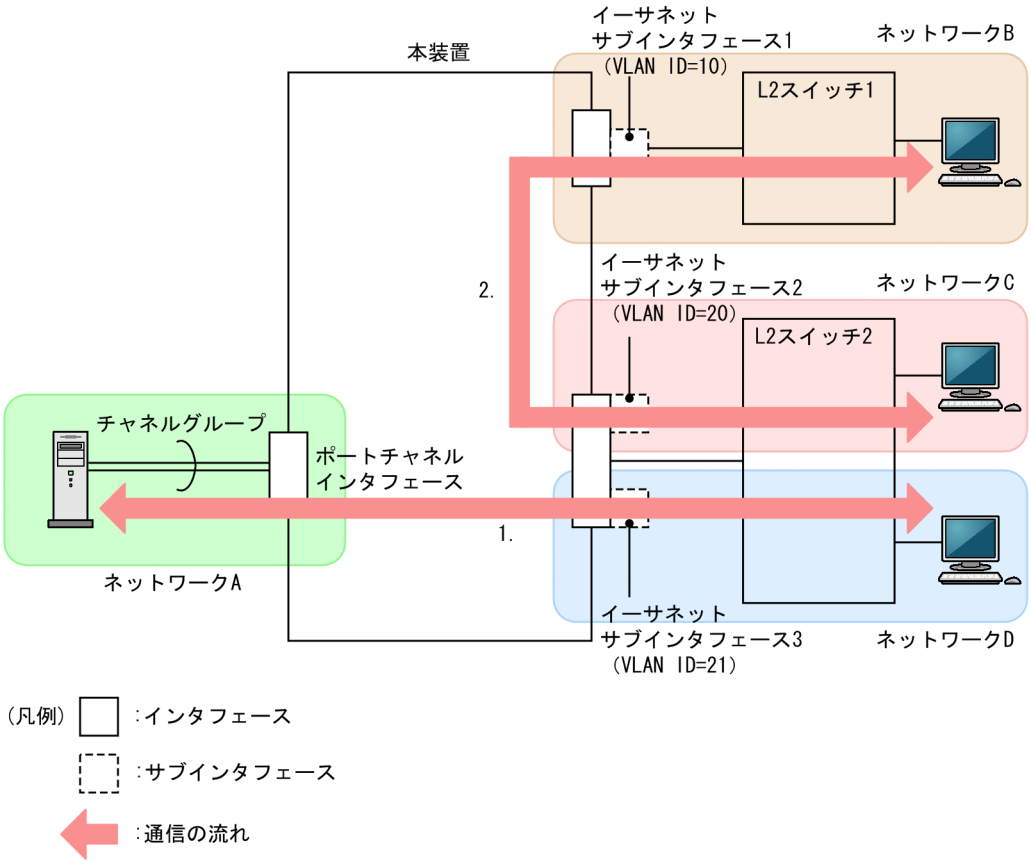
例：1/1.5

サブインタフェースとして，VLAN Tag を使用するインタフェースおよび VLAN Tag を使用しないインタフェースのどちらも設定できます。

20.1.3　ネットワーク構成例

IP インタフェースを使用するネットワーク構成例を次の図に示します。

図 20-1　IP インタフェースを使用するネットワーク構成例



[本装置の設定]

- ネットワーク A のサーバとの接続
  ポートチャネルインタフェースを設定します。
- ネットワーク B の L2 スイッチ 1 との接続
  イーサネットポートに一つのサブインタフェースを設定して，VLAN ID=10 を設定します。
- ネットワーク C およびネットワーク D の L2 スイッチ 2 との接続
  イーサネットポートに二つのサブインタフェースを設定して，それぞれ VLAN ID=20 および 21 を設定します。

上記の各インタフェースに IP アドレスを指定して，それぞれ IP インタフェースに設定します。

[通信内容] 図中の通信の流れの番号に対応

1. ネットワーク A とネットワーク D 間のレイヤ 3 中継（異なるサブネット間中継）
   ネットワーク A のサーバとは，Untagged フレームを送受信します。
   ネットワーク D の L2 スイッチ 2 とは，Tagged フレーム（VLAN ID=21）を送受信します。
2. ネットワーク B とネットワーク C 間のレイヤ 3 中継（異なるサブネット間中継）
   ネットワーク B の L2 スイッチ 1 とは，Tagged フレーム（VLAN ID=10）を送受信します。
   ネットワーク C の L2 スイッチ 2 とは，Tagged フレーム（VLAN ID=20）を送受信します。

20.1.4　IP インタフェース動作仕様

(1)　IP インタフェースのサポート仕様

IP インタフェースでは，インタフェースの種類ごとに，設定できるコンフィグレーションコマンドやコンフィグレーションで適用される値が異なります。コンフィグレーションとインタフェース種別の対応を次の表に示します。

表 20-2　コンフィグレーションとインタフェース種別の対応

コマンド名	インタフェースの種類（設定単位）				説明
	イーサネットインタフェース	ポートチャネルインタフェース	サブインタフェース	VLAN インタフェース	
description	○	○	○	○	各インタフェースに設定できます。
mtu（ポート）	○	－	－	－	ポートの最大フレーム長が，ポートチャネルインタフェース，サブインタフェース，および VLAN インタフェースに適用されます。
ip mtu	○	○	○	○	ip mtu コマンドを設定した場合，ポート単位で設定したポートの最大フレーム長と本コマンドの length パラメータ値を比較して，小さい方の値が該当するインタフェースの IP MTU 長として適用されます。
dot1q-ethertype	○	－	－	－	ポートに設定した TPID 値が，サブインタフェースおよび VLAN インタフェースに適用されます。
shutdown	○	○	○	○	各インタフェースに設定できます。
snmp trap link-status	○	－	○	○	サブインタフェースおよび VLAN インタフェースのデフォルトは，SNMP 通知を送信しません。

（凡例）○：設定できる　－：設定できない

（設定単位）

イーサネットインタフェース：ポート単位

ポートチャネルインタフェース：チャネルグループ単位

サブインタフェース：サブインタフェース単位

VLAN インタフェース：VLAN 単位

(2)　IP インタフェースで使用する MAC アドレス

IP インタフェースで使用する MAC アドレスは，インタフェースの種類によって異なります。IP インタフェースの種類ごとの MAC アドレスを次の表に示します。

表 20-3　IP インタフェースの種類ごとの MAC アドレス

IP インタフェースの種類	使用する MAC アドレス
イーサネットインタフェース	装置 MAC アドレス
イーサネットサブインタフェース	装置 MAC アドレス
ポートチャネルインタフェース	装置 MAC アドレス
ポートチャネルサブインタフェース	装置 MAC アドレス
VLAN インタフェース	装置 MAC アドレスまたは VLAN ごと MAC アドレス
マネージメントポート	マネージメントポートの MAC アドレス
シリアル接続ポート（AUX）	－
ループバックインタフェース	－
Null インタフェース	－

（凡例）－：MAC アドレスを使用しない

装置 MAC アドレスは，装置を識別するために本装置が一つ持っている MAC アドレスです。運用コマンド show system で装置 MAC アドレスを確認できます。

VLAN インタフェースで使用する VLAN ごと MAC アドレスは，コンフィグレーションコマンド vlan-mac-prefix および vlan-mac で設定します。vlan-mac-prefix コマンドでは，生成する MAC アドレスの上位 32bit までのプレフィックスを指定します。さらに，vlan-mac コマンドで，VLAN インタフェースで VLAN ごと MAC アドレスを使用することを設定します。このとき，下位 16bit に VLAN ID ごとの一意の値を使用して MAC アドレスを生成しますが，コンフィグレーションコマンド vlan-mac-suffix vlan-id を設定すると，下位 16bit に VLAN ID の値を使用して MAC アドレスを生成します。

(3)　IP インタフェースで使用する MTU

IP インタフェースでは，次の情報のうち，最小の値がインタフェースの IP MTU 値になります。

- 装置単位で設定する全ポート共通の最大フレーム長－18
- ポート単位で設定するポートの最大フレーム長－18
- インタフェース単位で設定する IP MTU 情報

インタフェースの IP MTU 値決定マトリクスを次の表に示します。

表 20-4　インタフェースの IP MTU 値決定マトリクス

全ポート共通の最大フレーム長	ポートの最大フレーム長	IP MTU 情報	IP MTU 値
設定あり	設定あり	設定あり	次の情報を比較して，小さい方の値 • ポートの最大フレーム長で指定したポート内の最小値－18 • IP MTU 情報の設定値
設定あり	設定なし	設定あり	次の情報を比較して，小さい方の値 • 全ポート共通の最大フレーム長の設定値－18

全ポート共通の最大フレーム長	ポートの最大フレーム長	IP MTU 情報	IP MTU 値
			• IP MTU 情報の設定値
設定あり	設定あり	設定なし	次の情報を比較して，小さい方の値 • ポートの最大フレーム長で指定したポート内の最小値－18 • 9216
設定あり	設定なし	設定なし	次の情報を比較して，小さい方の値 • 全ポート共通の最大フレーム長の設定値－18 • 9216
設定なし	設定あり	設定あり	次の情報を比較して，小さい方の値 • ポートの最大フレーム長で指定したポート内の最小値－18 • IP MTU 情報の設定値
設定なし	設定なし	設定あり	次の情報を比較して，小さい方の値 • IP MTU 情報の設定値 • 1500
設定なし	設定あり	設定なし	次の情報を比較して，小さい方の値 • ポートの最大フレーム長で指定したポート内の最小値－18 • 9216
設定なし	設定なし	設定なし	1500

注 1

回線種別が 10BASE-T（全二重および半二重）または 100BASE-TX（半二重）の場合は，設定内容に関係なく，IP MTU の最大値は 1500 です。

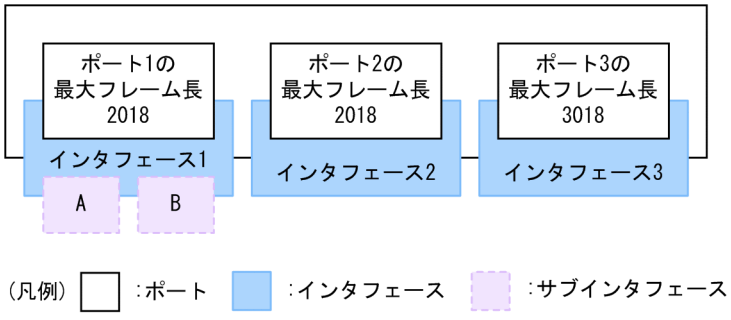
注 2

最大フレーム長は，FCS を除いた Ethernet V2 形式フレームの最大長です。

(a)　インタフェースとポートが 1 対 1 に対応する場合の IP MTU 値

イーサネットインタフェースやイーサネットサブインタフェースに IP アドレスを設定したインタフェースの IP MTU 値は次のように決定します。

図 20-2　インタフェースとポートが 1 対 1 に対応する場合の IP MTU 値の例



● IP MTU 情報を設定しない場合の各インタフェースの IP MTU 値

IP MTU の決定値
　サブインタフェース A：2000
　サブインタフェース B：2000
　インタフェース 2：2000
　インタフェース 3：3000

● IP MTU 情報を設定した場合の各インタフェースの IP MTU 値

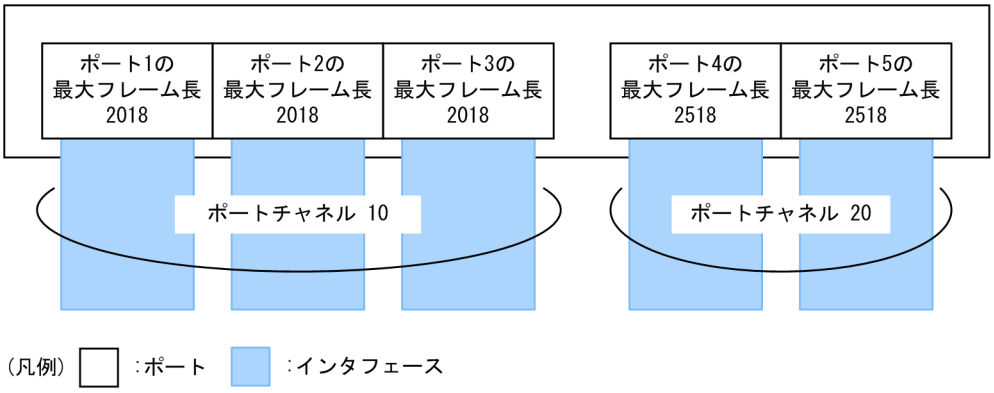
設定する IP MTU 長
　サブインタフェース A：1000
　サブインタフェース B：3000
　インタフェース 2：2500
　インタフェース 3：2500

IP MTU の決定値
　サブインタフェース A：1000
　サブインタフェース B：2000
　インタフェース 2：2000
　インタフェース 3：2500

(b)　インタフェースとポートが 1 対 n に対応する場合の IP MTU 値

ポートチャネルインタフェースや VLAN インタフェースのように，複数のポートが対応するインタフェースの IP MTU 値は次のように決定します。

図 20-3　ポートチャネルインタフェースの IP MTU 値の例



● IP MTU 情報を設定しない場合の各インタフェースの IP MTU 値

IP MTU の決定値
　ポートチャネル 10：2000
　ポートチャネル 20：2500

● IP MTU 情報を設定した場合の各インタフェースの IP MTU 値

設定する IP MTU 長
　ポートチャネル 10：1000

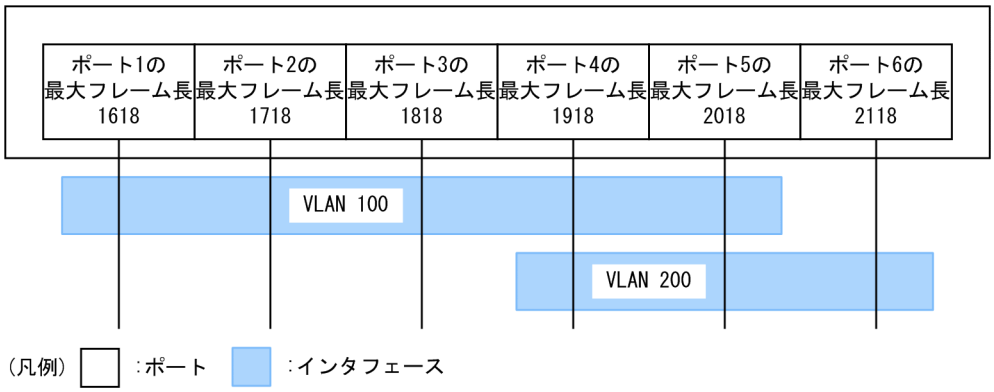
ポートチャネル 20：3000

IP MTU の決定値

ポートチャネル 10：1000

ポートチャネル 20：2500

図 20-4　VLAN インタフェースの IP MTU 値の例



● IP MTU 情報を設定しない場合の各インタフェースの IP MTU 値

IP MTU の決定値

VLAN 100：1600

VLAN 200：1900

20.2　コンフィグレーション

20.2.1　コンフィグレーションコマンド一覧

IP インタフェースとサブ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 20-5　コンフィグレーションコマンド一覧

コマンド名	説明
description	サブインタフェースの補足説明を設定します。
encapsulation dot1q	サブインタフェースに VLAN Tag の VLAN ID を設定します。
shutdown	サブインタフェースをシャットダウンに設定します。
interface fortygigabitethernet※1	40GBASE-R のイーサネットインタフェースまたはイーサネットサブインタフェースを設定します。
interface gigabitethernet※1	10BASE-T/100BASE-TX/1000BASE-T/1000BASE-X のイーサネットインタフェースまたはイーサネットサブインタフェースを設定します。
interface hundredgigabitethernet※1	100GBASE-R のイーサネットインタフェースまたはイーサネットサブインタフェースを設定します。
interface tengigabitethernet※1	10GBASE-R のイーサネットインタフェースまたはイーサネットサブインタフェースを設定します。
interface port-channel※2	ポートチャネルインタフェースまたはポートチャネルサブインタフェースを設定します。
interface vlan※3	VLAN インタフェースを設定します。
vlan-mac※3	VLAN ごと MAC アドレスを使用することを設定します。
vlan-mac-prefix※3	VLAN ごと MAC アドレスのプレフィックスを設定します。
vlan-mac-suffix vlan-id※3	VLAN ごと MAC アドレスのサフィックスを設定します。
ip address※4	インタフェースの IPv4 アドレスを設定します。

注※1
「コンフィグレーションコマンドレファレンス Vol.1　16. イーサネット」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 Vol.1　17. リンクアグリゲーション」を参照してください。

注※3
「コンフィグレーションコマンドレファレンス Vol.2　3. VLAN」を参照してください。

注※4
「コンフィグレーションコマンドレファレンス Vol.3　2. IPv4・ARP・ICMP」を参照してください。

20.2.2　IP インタフェースの設定

(1)　イーサネットインタフェースの設定

[設定のポイント]

イーサネットのコンフィグレーションモードで IP アドレスを設定します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/10**
   イーサネットインタフェース 1/10 のコンフィグレーションモードに移行します。
2. **(config-if)# ip address 192.0.2.1 255.255.255.0**
   イーサネットインタフェース 1/10 に IP アドレスを設定します。

(2)　イーサネットサブインタフェースの設定

[設定のポイント]

イーサネットサブインタフェースのコンフィグレーションモードで VLAN Tag の VLAN ID と IP アドレスを設定します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/10.5**
   イーサネットサブインタフェース 1/10.5 のコンフィグレーションモードに移行します。
2. **(config-subif)# encapsulation dot1q 100**
   イーサネットサブインタフェース 1/10.5 に VLAN Tag の VLAN ID として 100 を設定します。
3. **(config-subif)# ip address 192.0.2.1 255.255.255.0**
   イーサネットサブインタフェース 1/10.5 に IP アドレスを設定します。

(3)　ポートチャネルインタフェースの設定

[設定のポイント]

ポートチャネルのコンフィグレーションモードで IP アドレスを設定します。

[コマンドによる設定]

1. **(config)# interface port-channel 10**
   ポートチャネルインタフェース 10 のコンフィグレーションモードに移行します。
2. **(config-if)# ip address 192.0.2.1 255.255.255.0**
   ポートチャネルインタフェースに IP アドレスを設定します。

(4)　ポートチャネルサブインタフェースの設定

[設定のポイント]

ポートチャネルサブインタフェースのコンフィグレーションモードで VLAN Tag の VLAN ID と IP アドレスを設定します。

[コマンドによる設定]

1. **(config)# interface port-channel 10.110**

ポートチャネルサブインタフェース 10.110 のコンフィグレーションモードに移行します。

2. **(config-subif)# encapsulation dot1q 100**
   ポートチャネルサブインタフェース 10.110 に VLAN Tag の VLAN ID として 100 を設定します。
3. **(config-subif)# ip address 192.0.2.1 255.255.255.0**
   ポートチャネルサブインタフェース 10.110 に IP アドレスを設定します。

(5)　VLAN インタフェースの設定

[設定のポイント]

VLAN インタフェースのコンフィグレーションモードで IP アドレスを設定します。

[コマンドによる設定]

1. **(config)# interface vlan 10**
   VLAN インタフェース 10 のコンフィグレーションモードに移行します。指定した VLAN ID が未設定の VLAN ID の場合，自動でポート 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 IP アドレスを設定します。

20.2.3　IP インタフェースの削除

(1)　イーサネットインタフェースの削除

[設定のポイント]

イーサネットインタフェースから IP アドレスを削除します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/1**
   イーサネットインタフェース 1/1 のコンフィグレーションモードに移行します。
2. **(config-if)# no ip address 192.0.2.1**
   イーサネットインタフェース 1/1 から IP アドレスの設定を削除します。

(2)　イーサネットサブインタフェースの削除

[設定のポイント]

イーサネットサブインタフェースを削除する場合，IP アドレスと VLAN Tag の設定を削除してから，イーサネットサブインタフェースを削除します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/1.5**
   イーサネットサブインタフェース 1/1.5 のコンフィグレーションモードに移行します。
2. **(config-subif)# no ip address 192.0.2.1**
   イーサネットサブインタフェース 1/1.5 から IP アドレスの設定を削除します。
3. **(config-subif)# no encapsulation dot1q**
   (config-subif)# exit

イーサネットサブインタフェース 1/1.5 から VLAN Tag の設定を削除して，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)# no interface gigabitethernet 1/1.5**
   イーサネットサブインタフェース 1/1.5 を削除します。

(3) ポートチャネルインタフェースの削除

[設定のポイント]

ポートチャネルインタフェースから IP アドレスを削除します。

[コマンドによる設定]

1. **(config)# interface port-channel 10**
   ポートチャネルインタフェース 10 のコンフィグレーションモードに移行します。
2. **(config-if)# no ip address 192.0.2.1**
   ポートチャネルインタフェース 10 から IP アドレスの設定を削除します。

(4) ポートチャネルサブインタフェースの削除

[設定のポイント]

ポートチャネルサブインタフェースを削除する場合，IP アドレスと VLAN Tag の設定を削除してから，ポートチャネルサブインタフェースを削除します。

[コマンドによる設定]

1. **(config)# interface port-channel 3.5**
   ポートチャネルサブインタフェース 3.5 のコンフィグレーションモードに移行します。
2. **(config-subif)# no ip address 192.0.2.1**
   ポートチャネルサブインタフェース 3.5 から IP アドレスの設定を削除します。
3. **(config-subif)# no encapsulation dot1q**
   (config-subif)# exit
   ポートチャネルサブインタフェース 3.5 から VLAN Tag の設定を削除して，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)# no interface port-channel 3.5**
   ポートチャネルサブインタフェース 3.5 を削除します。

(5) VLAN インタフェースの削除

[設定のポイント]

VLAN インタフェースを削除する場合，IP アドレスの設定を削除してから，VLAN インタフェースを削除します。

[コマンドによる設定]

1. **(config)# interface vlan 10**
   VLAN インタフェース 10 のコンフィグレーションモードに移行します。
2. **(config-if)# no ip address 192.168.1.1**
   (config-if)# exit
   VLAN 10 から IP アドレスの設定を削除して，グローバルコンフィグレーションモードに戻ります。

3. **(config)# no interface vlan 10**

   VLAN インタフェース 10 を削除します。VLAN インタフェース 10 を削除すると，ポート VLAN 10 も削除されます。

20.2.4　VLAN インタフェースの MAC アドレス

VLAN を IP インタフェースとして使用する場合，VLAN インタフェースごとに MAC アドレスを付けられます。MAC アドレスは vlan-mac-prefix コマンドおよび vlan-mac コマンドで設定します。また，MAC アドレスの下位 16bit に VLAN ID の値を使用する場合は，vlan-mac-suffix vlan-id コマンドを設定します。

MAC アドレスの値は，IPv4 の場合は運用コマンド show ip interface，IPv6 の場合は運用コマンド show ipv6 interface で確認できます。

(1)　VLAN ごと MAC アドレスのプレフィックスの設定

[設定のポイント]

VLAN ごと MAC アドレスは，vlan-mac-prefix コマンドで上位 32bit までのプレフィックスを指定し，かつ VLAN インタフェースごとに vlan-mac コマンドで VLAN ごと MAC アドレスを使用することを設定します。

[コマンドによる設定]

1. **(config)# vlan-mac-prefix 0012.e200.0000 ffff.ffff.0000**

   VLAN ごと MAC アドレスに使用するプレフィックス（上位 32bit）を指定します。マスクは 32bit で指定する場合 ffff.ffff.0000 です。

2. **(config)# interface vlan 10**

   VLAN インタフェース 10 のコンフィグレーションモードに移行します。

3. **(config-if)# vlan-mac**

   VLAN インタフェース 10 で VLAN ごと MAC アドレスを使用することを設定します。

[注意事項]

VLAN ごと MAC アドレスの設定で，VLAN インタフェースの MAC アドレスが変更になります。

MAC アドレスを変更した VLAN の IP インタフェースはいったんダウンし，通信が停止します。その後，IP インタフェースはアップし，通信が再開します。

(2)　VLAN ごと MAC アドレスのサフィックスの設定

[設定のポイント]

生成する VLAN ごと MAC アドレスの下位 16bit に，VLAN ID の値を使用することを設定します。vlan-mac-suffix vlan-id コマンドの設定後，設定を装置に反映させるために，コンフィグレーションを保存してから装置を再起動してください。

本設定は，装置の運用開始時に実施してください。運用開始後に設定する場合は，装置のコンフィグレーションをいったん工場出荷時の初期状態に戻してから設定してください。

[コマンドによる設定]

1. **(config)# vlan-mac-prefix 0012.e200.0000 ffff.ffff.0000**

   VLAN ごと MAC アドレスに使用するプレフィックス（上位 32bit）を指定します。

2. **(config)# vlan-mac-suffix vlan-id**

VLAN ごと MAC アドレスの下位 16bit に VLAN ID の値を使用することを設定します。このコマンドの設定後，コンフィグレーションを保存してから装置を再起動してください。

3. **(config)# interface vlan 10**

   VLAN インタフェース 10 のコンフィグレーションモードに移行します。

4. **(config-if)# vlan-mac**

   VLAN インタフェース 10 で VLAN ごと MAC アドレスを使用することを設定します。

[注意事項]

サフィックスの設定を変更して装置を再起動するとき，コンフィグレーションの設定量に応じて，装置の起動に通常よりも長い時間が掛かることがあります。初期導入時のコンフィグレーションに戻した状態で，サフィックスを設定してください。

20.2.5　サブインタフェースのシャットダウン

[設定のポイント]

サブインタフェースはイーサネットおよびポートチャネルと同じようにシャットダウンに設定できます。サブインタフェース単位で設定します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/10.5**

   イーサネットサブインタフェース 1/10.5 のコンフィグレーションモードに移行します。

2. **(config-subif)# shutdown**

   イーサネットサブインタフェース 1/10.5 をシャットダウンします。

3. **(config-subif)# ＊＊＊＊＊**

   イーサネットサブインタフェース 1/10.5 に対するコンフィグレーションを設定します。

4. **(config-subif)# no shutdown**

   イーサネットサブインタフェース 1/10.5 のシャットダウンを解除します。

[関連事項]

運用コマンド inactivate でサブインタフェース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サブインタフェースが active 状態になります。サブインタフェースをシャットダウンした場合は，装置を再起動してもサブインタフェースは disable 状態のままです。サブインタフェースを active 状態にする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。

20.3　オペレーション

20.3.1　運用コマンド一覧

IP インタフェースとサブインタフェースの運用コマンド一覧を次の表に示します。

表 20-6　運用コマンド一覧

コマンド名	説明
activate	inactive 状態のサブインタフェースを active 状態にします。
inactivate	active 状態のサブインタフェースを inactive 状態にします。
show interfaces summary	サブインタフェースの状態を表示します。
show ip-dual interface※1	IPv4 と IPv6 の IP インタフェースの状態および統計情報を表示します。
show ip interface※1	IPv4 の IP インタフェースの状態および統計情報を表示します。
clear ip interface statistics※1	IPv4 の IP インタフェースの統計情報をクリアします
show ipv6 interface※2	IPv6 の IP インタフェースの状態および統計情報を表示します。
clear ipv6 interface statistics※2	IPv6 の IP インタフェースの統計情報をクリアします。

注※1

「運用コマンドレファレンス Vol.3　2. IPv4・ARP・ICMP」を参照してください。

注※2

「運用コマンドレファレンス Vol.3　3. IPv6・NDP・ICMPv6」を参照してください。

20.3.2　IP インタフェースの状態および統計情報の確認

show ip-dual interface コマンドで IP インタフェースの状態と統計情報を確認できます。イーサネットサブインタフェースを指定した show ip-dual interface コマンドの実行結果を次の図に示します。

図 20-5　show ip-dual interface コマンドの実行結果

```
>show ip-dual interface gigabitethernet 1/2.5 detail
Date 20XX/01/01 12:00:00 UTC
Eth1/2.5    VRF: 10
   Status: UP,MULTICAST,BROADCAST
   mtu: 1500   MAC address: 0012.e286.5300
   IPv4: 192.0.2.1/24 broadcast 192.0.2.255  PRIMARY,SUBNETBROD
   IPv4: 192.0.2.10/24 broadcast 192.0.2.255  VRRP
   IPv6: 2001:db8:100::1/64
   IPv6: fe80::212:e2ff:fe86:5300%Eth1/2.5/64
   IPv4 uRPF: Strict Mode  VRRP: Enable   Multicast Routing: Disable
   IPv6 uRPF: Strict Mode  VRRP: Disable  Multicast Routing: Disable
   Time-since-last-status-change: 30,00:10:00
   Last down at: 20XX/01/01 11:00:00 UTC
   VLAN ID: 100
   Description: subnetwork100
   Detail status: Disable
   [Out octets/packets counter]
      IPv4 Out All octets              :                20000
      IPv6 Out All octets              :                60000
      IPv4 Out All packets             :                  250
      IPv6 Out All packets             :                  750
      IPv4 Out Discards packets        :                  130
      IPv6 Out Discards packets        :                  290
      IPv4 Out Discards(BCU-CPU) packets:                   4
```

```
   IPv6 Out Discards(BCU-CPU) packets:                   6
[In octets/packets counter]
   IPv4 In All octets                :                28000
   IPv6 In All octets                :                36000
   IPv4 In All packets               :                  350
   IPv6 In All packets               :                  450
   IPv4 In Error packets             :                   50
   IPv6 In Error packets             :                   75
   IPv4 In Discards packets          :                   15
   IPv6 In Discards packets          :                   20
   IPv4 In NoRoutes packets          :                   30
   IPv6 In NoRoutes packets          :                   40
   IPv4 In Error(BCU-CPU) packets    :                   25
   IPv6 In Error(BCU-CPU) packets    :                   35
   IPv4 In Discards(BCU-CPU) packets :                    2
   IPv6 In Discards(BCU-CPU) packets :                    3
```

付録

付録 A　準拠規格

付録 A.1　TELNET/FTP

表 A–1　TELNET/FTP の準拠規格および勧告

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+の準拠規格および勧告

規格番号(発行年月)	規格名
RFC2865(2000 年 6 月)	Remote Authentication Dial In User Service(RADIUS)
RFC2866(2000 年 6 月)	RADIUS Accounting
RFC3162(2001 年 8 月)	RADIUS and IPv6
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
draft-ylonen-ssh-protocol-00 (1995 年 11 月)	The SSH (Secure Shell) Remote Login Protocol
draft-ietf-secsh-dh-group-exchange-02 (2002 年 1 月)	Diffie-Hellman Group Exchange for the SSH Transport Layer Protocol
draft-ietf-secsh-publickeyfile-03 (2002 年 10 月)	SSH Public Key File Format

付録 A.4　NTP

表 A–4　NTP の準拠規格および勧告

規格番号(発行年月)	規格名
RFC1305(1992 年 3 月)	Network Time Protocol (Version 3) Specification, Implementation and Analysis

付録 A.5　SNTP

表 A–5　SNTP の準拠規格および勧告

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.6　DNS

表 A–6　DNS リゾルバの準拠規格および勧告

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.7　SYSLOG

表 A–7　SYSLOG の準拠規格および勧告

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)

規格番号(発行年月)	規格名
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)
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

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
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

規格番号(発行年月)	規格名
RFC1215(1991 年 3 月)	A Convention for Defining Traps for use with the SNMP
RFC1354(1992 年 7 月)	IP Forwarding Table MIB
RFC1643(1994 年 7 月)	Definitions of Managed Objects for the Ethernet-like Interface Types
RFC1657(1994 年 7 月)	Definitions of Managed Objects for the Fourth Version of the Border Gateway Protocol (BGP-4) using SMIv2
RFC2452(1998 年 12 月)	IP Version 6 Management Information Base for the Transmission Control Protocol
RFC2454(1998 年 12 月)	IP Version 6 Management Information Base for the User Datagram Protocol
RFC2465(1998 年 12 月)	Management Information Base for IP Version 6: Textual Conventions and General Group
RFC2466(1998 年 12 月)	Management Information Base for IP Version 6: ICMPv6 Group
RFC2787(2000 年 3 月)	Definitions of Managed Objects for the Virtual Router Redundancy Protocol
RFC2819(2000 年 5 月)	Remote Network Monitoring Management Information Base
RFC2863(2000 年 6 月)	The Interfaces Group MIB
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)
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)
RFC3635(2003 年 9 月)	Definitions of Managed Objects for the Ethernet-like Interface Types
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)
RFC4188(2005 年 9 月)	Definitions of Managed Objects for Bridges
RFC4293(2006 年 4 月)	Management Information Base for the Internet Protocol (IP)

規格番号(発行年月)	規格名
RFC4363(2006 年 1 月)	Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering, and Virtual LAN Extensions
RFC4750(2006 年 12 月)	OSPF Version 2 Management Information Base
RFC5132(2007 年 12 月)※	IP Multicast MIB
RFC5643(2009 年 8 月)	Management Information Base for OSPFv3
draft-ietf-vrrp-unified-mib-04 (2005 年 9 月)	Definitions of Managed Objects for the VRRP over IPv4 and IPv6
draft-ietf-bfd-mib-13 (2013 年 6 月)	BFD Management Information Base

注※　この規格は IPv4 関連部だけ準拠しています。

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および勧告

種別	規格	規格名
10BASE-T, 100BASE-TX, 1000BASE-T, 1000BASE-X, 10GBASE-R, 40GBASE-R, 100GBASE-R	IEEE Std 802.3x-1997	Specification for 802.3x Full Duplex Operation
	IEEE Std 802.2, 1998 Edition	IEEE Standard for Information Technology - Telecommunications andInformation Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements - Part 2: Logical Link Control
	IEEE Std 802.3 2008 Edition	Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer Specifications
40GBASE-R, 100GBASE-R	IEEE Std 802.3ba 2010	Media Access Control (MAC) Parameters, Physical Layer, and Management Parameters for 40Gb/s and 100Gb/s Operation
	IEEE Std 802.3bm2015	Physical Layer Specifications and Management Parameters for 40 Gb/s and 100 Gb/s Operation over Fiber Optic Cables

付録 A.10　リンクアグリゲーション

表 A-11　リンクアグリゲーションの準拠規格および勧告

規格	規格名
IEEE802.1AX (IEEE Std 802.1AX-2008)	Aggregation of Multiple Link Segments

付録 B　謝辞(Acknowledgments)

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)

This product includes software developed at the Information Technology Division, US Naval Research Laboratory.

This product includes software developed by Adam Glass and Charles M. Hannum.

This product includes software developed by Adam Glass.

This product includes software developed by Berkeley Software Design, Inc.

This product includes software developed by Brini.

This product includes software developed by Bruce M. Simpson.

This product includes software developed by Charles D. Cranor and Washington University.

This product includes software developed by Charles D. Cranor, Washington University, the University of California, Berkeley and its contributors.

This product includes software developed by Charles M. Hannum.

This product includes software developed by Christopher G. Demetriou for the NetBSD Project.

This product includes software developed by Christopher G. Demetriou.

This product includes software developed by Christos Zoulas.

This product includes software developed by Chuck Silvers.

This product includes software developed by Computing Services at Carnegie Mellon University (http://www.cmu.edu/computing/).

This product includes software developed by Darrin B. Jewell

This product includes software developed by Eduardo Horvath.

This product includes software developed by Emmanuel Dreyfus

This product includes software developed by Frank van der Linden for the NetBSD Project.

This product includes software developed by Gordon W. Ross

This product includes software developed by Gordon W. Ross and Leo Weppelman.

This product includes software developed by Internet Initiative Japan Inc.

This product includes software developed by Jason L. Wright

This product includes software developed by Jason R. Thope for And Communications, http://www.and.com/

This product includes software developed by John Polstra.

This product includes software developed by Jonathan Stone and Jason R. Thorpe for the NetBSD Project.

This product includes software developed by Jonathan Stone for the NetBSD Project.

This product includes software developed by Kenneth Stailey.

This product includes software developed by Leo Weppelman.

This product includes software developed by Manuel Bouyer.

This product includes software developed by Mats O Jansson.

This product includes software developed by Michael Graff.

This product includes software developed by Michael Shalayeff.

This product includes software developed by Niels Provos.

This product includes software developed by Paul Mackerras <paulus@samba.org>.

This product includes software developed by Pedro Roque Marques <pedro_m@yahoo.com>

This product includes software developed by Rolf Grossmann.

This product includes software developed by Ross Harvey for the NetBSD Project.

This product includes software developed by Softweyr LLC, the University of California, Berkeley, and its contributors.

This product includes software developed by Terrence R. Lambert.

This product includes software developed by TooLs GmbH.

This product includes software developed by WIDE Project and its contributors.

This product includes software developed by Winning Strategies, Inc.

This product includes software developed by Yen Yen Lim and North Dakota State University

This product includes software developed by Zembu Labs, Inc.

This product includes software developed by the Alice Group.

This product includes software developed by the Charles D. Cranor, Washington University, University of California, Berkeley and its contributors.

This product includes software developed by the Computer Systems Engineering Group at Lawrence Berkeley Laboratory.

This product includes software developed by the NetBSD Foundation, Inc. and its contributors.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)

This product includes software developed by the SMCC Technology Development Group at Sun Microsystems, Inc.

This product includes software developed by the University of California, Berkeley and its contributors.

This product includes software developed by the University of California, Lawrence Berkeley Laboratories.

This product includes software developed by the University of California, Lawrence Berkeley Laboratory and its contributors.

This product includes software developed by the University of California, Lawrence Berkeley Laboratory.

This product includes software developed for the NetBSD Project by Jason R. Thorpe.

This product includes software developed for the NetBSD Project by Perry E. Metzger.

This product includes software developed for the NetBSD Project by Frank van der Linden

This product includes software developed for the NetBSD Project by John M. Vinopal.

This product includes software developed for the NetBSD Project by Wasabi Systems, Inc.

This product includes software developed for the NetBSD Project. See http://www.NetBSD.org/ for information about NetBSD.

This product includes software written by Tim Hudson (tjh@cryptsoft.com)

索引

A

absolute 方式〔MIB 監視〕　320
alarm グループ　319

B

BCU 初期導入ソフトウェアからのアップデート　263
BCU 初期導入ソフトウェアからのアップデートに関する運用コマンド一覧　265
BCU 二重化に関する運用コマンド一覧　280

C

CLI 環境情報　72
CLI 設定のカスタマイズ　72

D

delta 方式〔MIB 監視〕　320

E

event グループ　322

G

GetBulkRequest オペレーション　309
GetNextRequest オペレーション　308
GetRequest オペレーション　307

H

history グループ　319

I

Inform　317
IPv4/IPv6 SNMP マネージャからの MIB 要求と応答の例　303
IP アドレスによるオペレーション制限　311
IP アドレスの設定〔本装置〕　116
IP インタフェース　415
IP インタフェースとサブインタフェースの運用コマンド一覧　429
IP インタフェースとサブインタフェースのコンフィグレーションコマンド一覧　423

L

LLC 副層フレームフォーマット　376

M

MAC 副層フレームフォーマット　376
MDI／MDI-X のピンマッピング　369
MIB オブジェクトの表し方　306
MIB 概説　305
MIB 構造　305
MIB 取得の例　302
MIB を設定できない場合の応答　309

N

NTP のコンフィグレーションコマンド一覧　196

R

RADIUS　132
RADIUS/TACACS+に関する運用コマンド一覧 161
RADIUS/TACACS+に関するコンフィグレーションコマンド一覧　155
RADIUS/TACACS+の解説　132
RADIUS/TACACS+の概要　132
RADIUS/TACACS+の適用機能および範囲　133
RADIUS のサポート範囲　133
RMON MIB　319

S

SetRequest オペレーション　309
SFU/PRU/NIF の管理　244
SFU/PRU/NIF の管理に関する運用コマンド一覧　244
SFU/PRU/NIF の管理に関するコンフィグレーションコマンド一覧　244
SFU 冗長化に関する運用コマンド一覧　284
SNMP　301
SNMP/RMON に関する運用コマンド一覧　332
SNMP/RMON に関するコンフィグレーションコマンド一覧　324
SNMPv1，SNMPv2C オペレーション　307
SNMPv3 オペレーション　312
SNMPv3 でのオペレーション制限　315
SNMPv3 による MIB アクセス許可の設定　325
SNMP エージェント　302

SNMP エンジン　304
SNMP エンティティ　304
SNMP オペレーションのエラーステータスコード　312
SNMP 概説　302
SNMP で使用する IP アドレス　318
SNMP マネージャとの接続時の注意事項　322
SNTP のコンフィグレーションコマンド一覧　199
SSH(SecureShell)　163
SSH の運用コマンド一覧　185
SSH のコンフィグレーションコマンド一覧　178
statistics グループ　319

T

TACACS+　132
template モード　94
Trap　316
TYPE／LENGTH フィールドの意味　376

い

イーサネット　363
イーサネットの運用コマンド一覧　390
イーサネットのコンフィグレーションコマンド一覧　381
インデックス　306
インフォーム　317
インフォーム概説　317
インフォームリクエストフォーマット　318

う

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　119
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　114
運用ログ　294

え

エラーステータスコード　312

お

オプションライセンスに関する運用コマンド一覧 272
オプションライセンスに関するコンフィグレーションコマンド一覧　270

か

カスタマイズ配分　225

こ

高機能スクリプト　335
高機能スクリプトの運用コマンド一覧　342
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　342
固定配分　225
コマンド操作　65
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　66
コミュニティによるオペレーション　311
コミュニティによるオペレーション制限　311
コンソールの接続形態　58
コンフィグレーション　75
コンフィグレーションの設定，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　80
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　81

さ

サブインタフェース　415

し

時刻設定のコンフィグレーションコマンド一覧　193
時刻の設定と NTP/SNTP　191
時刻の設定と NTP/SNTP の運用コマンド一覧　201
時刻の設定の運用コマンド一覧　193
システム操作パネル　208
システムメッセージの出力とログの管理　293
システムメッセージの出力とログの管理の運用コマンド一覧　299
システムメッセージの出力とログの管理のコンフィグレーションコマンド一覧　295
自動 MDI/MDIX 機能　369
ジャンボフレーム　380
収容条件　17
受信フレームの廃棄条件　378

す

スタートアップメッセージ　208

せ

接続インタフェースごとの接続モードとサポート機能　366
接続インタフェース〔1000BASE-X〕　369
接続インタフェース〔100GBASE-R〕　372
接続インタフェース〔10BASE-T/100BASE-TX/1000BASE-T〕　366

接続インタフェース〔10GBASE-R〕　371
接続インタフェース〔40GBASE-R〕　372
接続時の注意事項〔1000BASE-X〕　371
接続時の注意事項〔100GBASE-R〕　372
接続時の注意事項〔10BASE-T/100BASE-TX/1000BASE-T〕　369
接続時の注意事項〔10GBASE-R〕　371
接続時の注意事項〔40GBASE-R〕　372
接続仕様〔1000BASE-X〕　370
接続仕様〔100GBASE-R〕　372
接続仕様〔10BASE-T/100BASE-TX/1000BASE-T〕　367
接続仕様〔10GBASE-R〕　371
接続仕様〔40GBASE-R〕　372

そ

装置管理者モード変更のパスワードの設定および変更　125
装置起動とログイン　57
装置構成　7
装置の確認に関する運用コマンド一覧　234
装置の確認に関するコンフィグレーションコマンド一覧　234
装置の管理　207
装置の冗長化　273
装置のリソース設定に関する運用コマンド一覧　225
装置のリソース設定に関するコンフィグレーションコマンド一覧　225
ソフトウェア障害検出時の動作に関する運用コマンド一覧　253
ソフトウェア障害検出時の動作に関するコンフィグレーションコマンド一覧　253
ソフトウェアの管理　255
ソフトウェアの管理に関する運用コマンド一覧　260

て

電源機構（PS）冗長化に関する運用コマンド一覧　290
電源機構（PS）冗長化に関するコンフィグレーションコマンド一覧　289
伝送速度および，全二重および半二重モードごとの接続仕様〔1000BASE-X〕　370
伝送速度および，全二重および半二重モードごとの接続仕様〔10BASE-T/100BASE-TX/1000BASE-T〕　367
テンプレート　93
テンプレートパラメータ　93

と

統計ログ　294
同時にログインできるユーザ数の設定　126
トラップ　316
トラップ概説　316
トラップの例　303
トラップフォーマット（SNMPv1）　316
トラップフォーマット（SNMPv2C，SNMPv3）　317

に

認証方式シーケンス（end-by-reject 設定時）　140
認証方式シーケンス（end-by-reject 未設定時）　139

ね

ネットワーク管理　302

は

バックアップ・リストアに使用する運用コマンド一覧　249
パッドの扱い　378

ひ

標準 MIB　305

ふ

プライベート MIB　305
フレームフォーマット　376

ほ

ポーズパケットの受信設定とフローコントロール動作　373
ポーズパケットの送信設定とフローコントロール動作　373
ホスト名と DNS　203
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　205
本装置の概要　1
本装置のサポート MIB　307

ま

マネージメントポートで使用する運用コマンド一覧　119
マネージメントポートのコンフィグレーションコマンド一覧　114

め

メッセージの出力　294

ゆ

ユーザ認証とプライバシー機能　304

り

リモート運用端末　60
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　127
リモート運用端末から本装置へのログイン　109
リモート運用端末と本装置との通信の確認　120
リモート運用端末の接続形態　58
リンクアグリゲーション　391
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　409
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　397
リンクアグリゲーションの運用コマンド一覧　412

ろ

ログイン制御の概要　123
ログインセキュリティと RADIUS/TACACS+　121
ログインセキュリティに関する運用コマンド一覧 122
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　122
ログインユーザの作成および削除　123
ログインユーザのパスワードの設定および変更　124
ログの保存　294