NEC Express5800シリーズ
インテリジェントスイッチ

5

スイッチの管理と詳細設定

本装置の運用中の管理に関する説明とより詳細な機能の説明とそのセットアップのための手順について説明します。

NTP（→128ページ）

NTP（Network Time Protocol: RFC1305）機能について説明します。

受信レート制限（→130ページ）

受信レート制限機能について説明します。

QoS機能（→131ページ）

QoS（Quality of Service）について説明します。

Webインタフェースを使った設定（→137ページ）

Webインタフェースを使った設定について説明します。

冗長構成での運用（N8406-005A）（→155ページ）

2つの本装置を利用して耐障害性を考慮した冗長構成の構築について簡単に説明します。

この章での図解説明では、N8406-005Aを使用しています。N8406-006Aをお持ちの場合は、N8406-005Aの図をN8406-006Aに読み替えてください。

システム情報の管理

本装置のシステム情報は、本装置と同じネットワーク上にある管理PCにインストールされたESMPRO/ServerManagerの統合ビューアから監視および確認することができます。
本装置とESMPRO/ServerManager との通信にはSNMPを使用します。通信のためにSNMPエージェントの設定をする必要があります（75ページ参照）。

ファイルの管理

ファイルの管理方法について説明します。

ソフトウェアファイルのインストール

ソフトウェアリリースファイルは、次に示すファイルから構成されています（出荷時にインストール済みです）。

/osloader.	ブートローダーファイル OSをロードする機能を持っています。
/os/△△-A.B.C-r.mai	メインソフトウェアイメージファイル
△△-A.B.C-r.des	ソフトウェア構成定義ファイル FTPサーバ、TFTPサーバからメインソフトウェアイメージファイルをコピーするときに、FTPサーバ、TFTPサーバ上にメインソフトウェアイメージファイルと共に配置します。リリースソフトウェアファイルの正常性をチェックするのに使用されます。このファイルはNVRAM上には必要ありません。

△△: N8406-005Aの場合“sl”・N8406-006Aの場合は“ml”、
A (0-99): ソフトウェアメジャーリリースバージョン
B (0-9): ソフトウェアマイナーリリースバージョン
C (00-99): ソフトウェアパッチリリースバージョン
r: リリースファイルを示すコード

アップデートインストール

アップデートインストールの方法とその他操作手順を示します。

アップデートインストール手順

1. 本装置と通信が可能な位置にTFTPサーバもしくはFTPサーバを用意して、△△-A.B.C-r.maiおよび、△△-A.B.C-r.desを配置する。
2. <FTPサーバにあるファイルからソフトウェアのアップデートを行う場合>

   グローバルモードでupgrade software ftp-serverコマンドを使用する。

   FTPサーバ上のソフトウェアをダウンロードして、既存のソフトウェアと入れ替えます。その後、ファイルの展開とチェックを自動的に行い、装置のリブート後、新しいソフトウェアで起動します。

```
(Conf-global)# upgrade software ftp-server 192.168.1.20
△△-A.B.C-r.des username nec password nec
```

<TFTPサーバにあるファイルからソフトウェアのアップデートを行う場合>

グローバルモードでupgrade software tftp-serverコマンドを使用する。

TFTPサーバ上のソフトウェアをダウンロードして、既存のソフトウェアと入れ替えます。その後、ファイルの展開とチェックを自動的に行い、装置のリブート後、新しいソフトウェアで起動します。

```
(Conf-global)# upgrade software tftp-server
192.168.1.20 △△-A.B.C-r.des
```

3. ソフトウェアアップグレードコマンドを入力後、装置再起動オプションを設定する場合には、upgrade software restartコマンドを使用する。

   装置再起動オプションにはimmediate（即時再起動）、none（再起動しない）、time <DATE>（再起動の時間を指定）の3種類があります。このコマンドを入力しない場合には、自動的に再起動が行われます。

```
(Conf-global)# upgrade software restart none
```

ソフトウェアアップグレードの停止

ソフトウェアアップグレードプロセスを停止する場合には、no upgrade softwareコマンドを使用してください。upgrade softwareコマンドの実行後にのみ入力可能です。

```
(Conf-global)# no upgrade software
```

前ソフトウェアファイルへの復帰

以前使用していたバージョンのソフトウェアに戻す場合には、restore softwareコマンドを使用してください。

```
(Conf-global)# restore software
```

ソフトウェアアップグレードの確認

show upgrade software-statusコマンドでソフトウェア更新プロセスの状態を確認することができます。

```
(Conf-global)# show upgrade software-status
```

show versionコマンドは、装置各種バージョン情報を表示します。ソフトウェアバージョン、使用しているファイル名も表示されます

```
(Conf-global)# show version
```

起動に使用するソフトウェアを手動で指定する

本装置では、使用するソフトウェアのファイル名をコンパクトフラッシュカード以外の不揮発性メモリNVRAMに保存しています。NVRAMには、通常使用するソフトウェアファイル名を記録してあるアクティブ面と、ソフトウェアアップグレード中に異常が発生した場合に自動的に以前のソフトウェアから起動する機能に使用されるスタンバイ面の2面があります。
ソフトウェアアップグレードを「アップデートインストール」の手順に沿って行った後に、装置が正常に連続3回起動しなかった場合には、以前使用されていたソフトウェアを使用して起動を試みます。NVRAM中に起動ファイル名の情報がない場合、または存在しないファイル名が記述されているような場合は、コンパクトフラッシュカード上に存在する予め決められた拡張子を持つファイルが使用されます。
通常は、上記のソフトウェアファイル名は、自動的に設定されますが、本装置では、NVRAMのアクティブ面を書き換えるCLIコマンドを提供しています。NVRAMのアクティブ面を書き換える場合にはboot entryコマンドを使用してください。
本コマンドは、起動に使用するソフトウェアを強制的に指定するためのものであるため、正常に動作をしている場合は使用しないでください。

```
(Conf-global)# boot entry △△-A.B.C-r.mai
```

正常に立ち上がらない場合の処置

コンパクトフラッシュカードの故障やその他、装置の故障によってソフトウェアを正しくインストールできなかったり、装置を正しく立ち上げることができなくなったりした場合は、無理な操作をせずに、お買い求めの販売店または保守サービス会社に保守を依頼してください。

本装置では、お客様によるコンパクトフラッシュカードの交換やその他の部品の交換は認められていません。お客様ご自身での部品交換が起因となった故障、および誤作動などは保証できません。部品の交換はお買い求めの販売店または保守サービス会社に依頼してください。

工場出荷設定への戻し方（スーパーリセット）

本装置をコンソールからのコマンドの投入で工場出荷状態に戻す方法について説明します。以下の手順により、工場出荷値に戻すことができます。

1. show file list configurationコマンドでコンフィグレーションファイルを確認する。

```
(Exec)#show file list configuration
```

2. 実行モードで、clear startup-configurationコマンドによりコンパクトフラッシュカード上のコンフィグレーションファイルを削除する。

   現在のコンフィグレーションファイルをセーブする場合には、後述の「コンフィグレーションファイルの管理」を参照してください。

```
(Exec)#clear startup-configuration
```

3. show file list configurationコマンドでコンフィグレーションファイルが削除されていることを確認する。
4. グローバルコンフィグレーションモードで、SSHホスト鍵およびSSHクライアント公開鍵、HTTPサーバ証明書ファイルを削除する。
5. 実行モードでreloadコマンドを実行する。

   装置が再起動され、工場出荷状態で立ち上がります。

```
(Exec)#reload
```

コンフィグレーションファイルの管理

本装置のコンパクトフラッシュ内にはソフトウェアファイルおよびコンフィグレーションファイルが存在します。ここではコンフィグレーションファイルの管理方法について説明します。

コンフィグレーションファイルの保存

save configurationコマンドによって、現在動作中のコンフィグレーション（running-configuration）をシステム立ち上げ時のコンフィグレーション（startup-configuration）としてコンパクトフラッシュに保存することができます。

```
(Conf-global)# save configuration
```

コンフィグレーションの初期化

clear startup-configurationコマンドによって、フラッシュメモリ内のコンフィグレーションファイルを削除します。動作中のコンフィグレーションも初期化する場合には、reloadコマンドでシステムを再立ち上げをしてください。

```
(Exec)#clear startup-configuration
(Exec)#reload
```

FTPサーバ・TFTPサーバへの保存と読み出し

copyコマンドによって、動作中のコンフィグレーション、またはシステム立ち上げ時のコンフィグレーションをFTPサーバ、TFTPサーバに対して保存・読み出しすることが可能です。

動作中のコンフィグレーションファイルをFTPサーバ、TFTPサーバへコピーするときはcopy running-configurationコマンドを使用してください。

```
(Conf-global)#copy running-configuration ftp-server
192.168.0.1 usser-a password-a filename run20030701.cfg
```

システム立ち上げ時のコンフィグレーションファイルをFTPサーバ、TFTPサーバへコピーするときはcopy startup-configurationコマンドを使用してください。

```
(Conf-global)#copy startup-configuration ftp-server
192.168.0.1 usser-a password-a filename sup20030701.cfg
```

FTPサーバ、TFTPサーバからコンフィグレーションファイルをコンパクトフラッシュ上にコピーするときはcopy configurationコマンドを使用してください。

```
(Conf-global)#copy configuration-file ftp-server
192.168.0.1 f20030701.cfg usser-a password-a flash
```

ポート

本装置のネットワーク通信ポートについて説明します。

ポート種別

本装置では以下のポートを実装します。

- マネージメントポート: 10Base-T/100Base-TX（1ポート）
- CPUポート: N8406-005Aの場合10Base-T/100Base-TX/1000Base-T（6ポート）
  N8406-006Aの場合1000Base-X（20ポート）
- ユーザーポート: 10Base-T/100Base-TX/1000Base-T（3ポート）

ギガビットポート

ギガビットポート（ユーザーポートならびに、N8406-005AのCPUポート）は、以下のいずれかを設定することができます。

- 10Mbps/half
- 10Mbps/full
- 100Mbps/half
- 100Mbps/full
- 1000Mbps/full
- auto(接続する相手装置がAuto-Negotiation機能をサポートしている場合には、duplexの自動認識を行います。)
- 1000Mbps/halfの設定は行えません。工場出荷時は、autoに設定されています。

- マネージメントポートは常にautoで、設定を変更することはできません。
- Auto-Negotiation機能を用いる場合は、ギガビットポートを「auto」に設定します。これによって、接続する相手装置との間で最適なduplex(half duplexまたはfull duplex)を自動で決定します。接続先が「auto」に設定されていない場合は、ギガビットポートを接続先の通信速度/モード(speed/duplex)に合わせて設定する必要があります。
- N8406-006AのCPUポートは、常に1000Mbps/fullとなり、設定を変更することは、できません。

ポートの設定

ポートの設定を変更する場合は、グローバルモードで変更するポートを指定してポートコンフィグレーションモードへ移行し、speedコマンド、duplexコマンドを使用してポートの速度と通信モードを設定します。スピードは、10Mbps・100Mbps・1000Mbpsのいずれかに設定できます。通信モードの設定は、Auto、Full、Halfのいずれかを設定します。デフォルトはAutoに設定されています。

[ポート速度と通信モードの設定]

LAN1を100Mbpsの全二重に設定

```
(Conf-global)#port lan1
(Conf-pt-lan1)#duplex full
(Conf-pt-lan1)#speed 100
```

重要

ギガビットポートと接続先のポートが同じ通信速度(speed)でも通信モード(duplex)が異なる場合、通信性能が低下しますので、ポートの設定には十分注意してください。

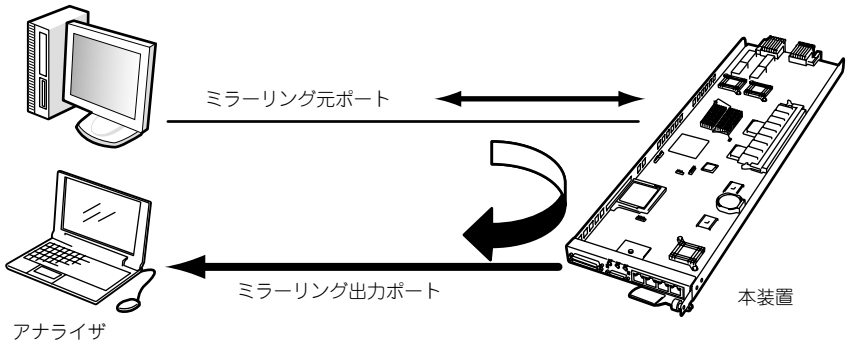
ポートミラーリング

「ポートミラーリング」は、指定したミラーリング元ポート（被観測ポート）で受信、あるいは送信するパケットを全て別に指定したミラーリング出力ポート（観測ポート）にコピーして送信する機能です。
ミラーリング出力ポートにトラフィックアナライザを接続し、ミラーリング元ポートのトラフィックを解析することができます。
本装置のすべてのネットワークポートをミラーリング元ポートとして選択でき、いずれかのLANポートをミラーリング出力ポートとして選択できます。

- 装置に対して1つのミラーリング出力ポートを設定可能
- 装置に対して複数同時にミラーリング元ポートを設定可能
- 以下のミラーリングルールが設定可能
  - ー　ポート入力
  - ー　ポート出力
  - ー　ポート入出力

重要

ミラーリング出力ポートに対する、ミラーリング元ポートの帯域にご注意ください。帯域使用率の高い複数のポートをミラーリング元ポートに設定した場合、ミラーリングされたフレームは輻輳し、廃棄される可能性があります。



ポートミラーリング

ポートミラーリングは、ミラーリング出力ポートとミラーリングルールの両方を登録することにより開始されます。

ミラーリング出力ポートの登録

ミラーリング出力ポートの登録を行うときには、グローバルモードで登録するポートを指定してポートコンフィグレーションモードへ移行し、mirror outputコマンドを使用して登録します。デフォルトVLAN以外に属しているポートをミラーリング出力ポートに指定することはできません。ミラーリング出力ポートとして登録されたポートは、どのVLANにも属さず、ミラーリングされたパケットの送信だけが行われます。no mirror outputコマンドによりミラーリング出力ポートを削除し、ポートをデフォルトVLANに戻します。

```
(Conf-global)#port lan1
(Conf-pt-lan1)#mirror output
(Conf-pt-lan1)#exit
```

ミラーリングルールの登録

ミラーリングルールの登録を行うときには、グローバルモードでミラーリング元となるポートを指定してポートコンフィグレーションモードへ移行し、mirror ruleコマンドを使用してミラーリングルールと出力先ポートを指定します。ミラーリングのルールには、Ingress(受信パケットのみ)、Egress(送信パケットのみ)、Both(送受信パケット)の3種類があります。no mirror ruleコマンドによりミラーリングルールを削除します。

```
(Conf-global)#port lan2
(Conf-pt-lan2)#mirror rule egress
(Conf-pt-lan2)#exit
```

ミラーリングの表示

登録されているミラーリングを表示する場合は、show mirrorコマンドを使用してください。

```
(Conf-global)# show mirror
```

SNMPエージェント

SNMPは、ネットワーク機器間で管理情報の通信をするためのプロトコルです。ネットワーク管理者はSNMPを使用して、ネットワーク稼動状況等を監視したり、ネットワークで発生した問題を特定および解決したりできます。

SNMPエージェントの有効化

SNMPエージェントを有効にする場合は、グローバルコンフィグレーションモードでsnmp-agent enableコマンドを使用してください。工場出荷時の状態では、有効に設定されています。

```
(Conf-global)# snmp-agent enable
```

SNMPエージェントの無効化

SNMPエージェントを無効にする場合は、no snmp-agent enableコマンドを使用してください。

```
(Conf-global)# no snmp-agent enable
```

SNMPエージェントのコミュニティ名、IPアドレスの登録

SNMPマネージャがアクセスするためのコミュニティ名、アクセスを許可するSNMPマネージャを指定する場合は、snmp-agent ip communityコマンドを使用してください。コミュニティ名はSNMPにおけるパスワードに相当します。ネットワーク管理者と検討し、SNMPマネージャと設定を合わせるようにします。
アクセスタイプrwを指定した場合、SNMPマネージャから本装置にSNMPを使用して、設定も表示もできます。roを指定した場合、SNMPマネージャは、本装置に対して現在の状態の表示しかできません。
以下ではコミュニティ名を「necmente」、SNMPマネージャのとIPアドレスを「10.1.1.1」に設定しています。

```
(Conf-global)# snmp-agent ip community necmente access-type
rw access-host 10.1.1.1
```

SNMPエージェントのコミュニティ名、IPアドレスの削除

SNMPマネージャがアクセスするためのコミュニティ名、アクセスを許可するSNMPマネージャを削除する場合は、no snmp-agent ip communityコマンドを使用してください。

```
(Conf-global)# no snmp-agent ip community necmente access-
host 10.1.1.1
```

SNMPトラップ送信先の登録

本装置のSNMPエージェントが送信するSNMP TRAPメッセージの送信先IPv4アドレスを指定するときはsnmp-agent trap destinationコマンドを使用してください。

```
(Conf-global)# snmp-agent trap destination 192.168.0.254
necmente
```

SNMPトラップ送信先の削除

本装置のSNMPエージェントが送信するSNMP TRAPメッセージの送信先IPv4 アドレスを削除するときは、no snmp-agent trap destinationコマンドを使用してください。

```
(Conf-global)# no snmp-agent trap destination 192.168.0.254
```

VLAN

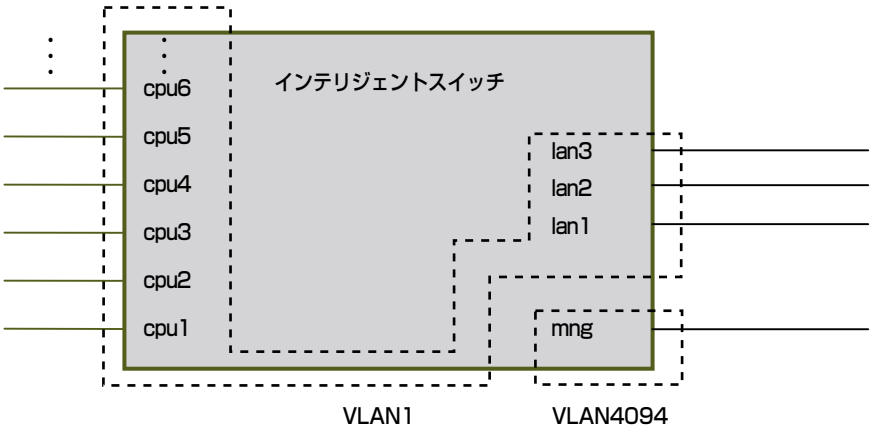
VLANは、装置内の物理ポートをグループ化して分割することで、仮想的な複数のLAN環境を作成することができます。
1つのVLANがブロードキャストドメインに対応しており、ブロードキャストフレームは同じVLANの物理ポートのみに送信されるため、装置内のトラフィック抑制が図られます。また、VLANはルータのインタフェースであり、VLAN間の通信を行う場合はルータ経由での通信が必要となるため、セキュリティの向上が図られます。

特　長

本装置の特長は以下のとおりです。

- 最大128個（使用可能VID: 1～4094）のVLANをサポートします。
- ポートベースVLANをサポートします。
- タグベースVLAN(IEEE802.1Q)をサポートします。
- 本装置の独自機能としてマネージメントVLANをサポートします。

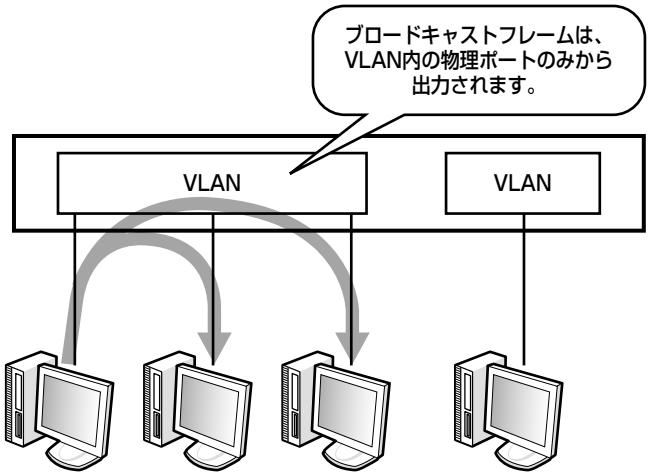
初期設定時ではmngポートを除く全ての物理ポートが、Default VLANと呼ばれるVID1のVLANに所属しています。mngポートは、VID4094のVLANに所属しています。



工場出荷時のVLANの状態

重要

**ネットワークおよびサーバの運用管理を円滑に行うために、管理系のVLANとユーザデータ系のVLANは分離することを推奨します。
同じVLANに対してマネジメントポートとユーザーポートを登録しての、STPおよびリンクアグリゲーション構成をとることはできません。**



- ポートベースVLAN

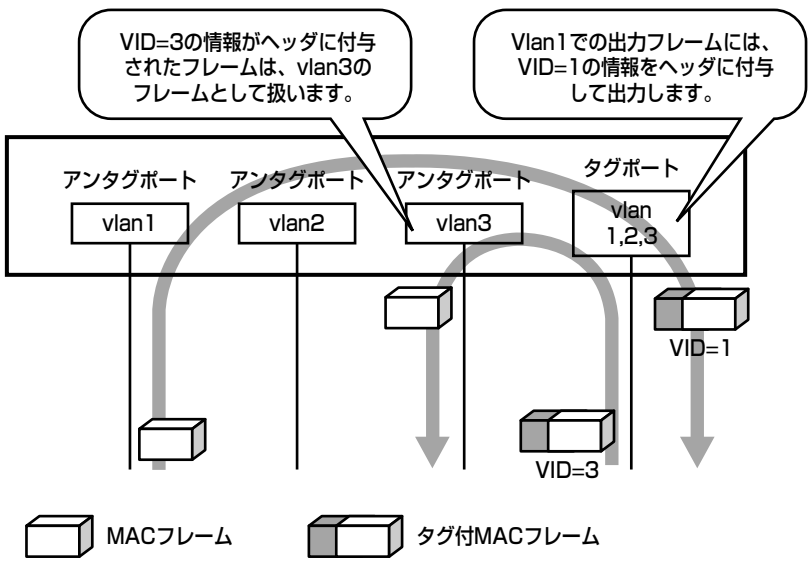
  ポートベースVLANは、1本の物理ポートを1つのVLANで使用します。物理ポートから入力したフレームは、割り当てられたVLANのフレームとして扱われます。

  ポートベースVLANで使用する物理ポートをアンタグポートと呼びます。

- タグベースVLAN

  タグベースVLANは、フレームヘッダ内にVID情報を組み込んだタグと呼ばれる4オクテットの情報を付加することで、1本の物理ポートを複数のVLANで使用します。物理ポートから入力したフレームは、フレームヘッダ内のVID情報により、どのVLANのフレームか判断します。

  タグベースVLANで使用する物理ポートをタグポートと呼びます。



VLANの設定

VLAN名とVLANを構成する物理ネットワークポートを設定する必要があります。装置内部ではVLAN名を数値に置き換えて管理するため、管理番号（VID値）を合わせて設定することになります。これによりVLAN名にVID値が対応することになります。

重要

VID値はネットワーク内部でユニークになるように1以上4094以下の範囲で任意に決めてください。

VLANの登録

vlanコマンドを使用して新規に登録するVID値とVLAN名を対応付けを行います。VLANの登録はグローバルコンフィグレーションモードで行います。

```
(Conf-global)# vlan 3 VLAN0003
```

VLANの表示

登録されているVLANを表示する場合は、show vlanコマンドを使用してください。表示コマンド（一部の表示コマンドを除く）はどこのCLIモードでも使用可能です。

```
(Conf-global)# show vlan
```

VLANの削除

グローバルコンフィグレーションモードでno vlanコマンドを使用して登録されているVLANの削除を行います。

ヒント

VID=1およびVID=4094のVLANは削除できません。

```
(Conf-global)# no vlan 3
```

ポートベースVLANのポートの設定

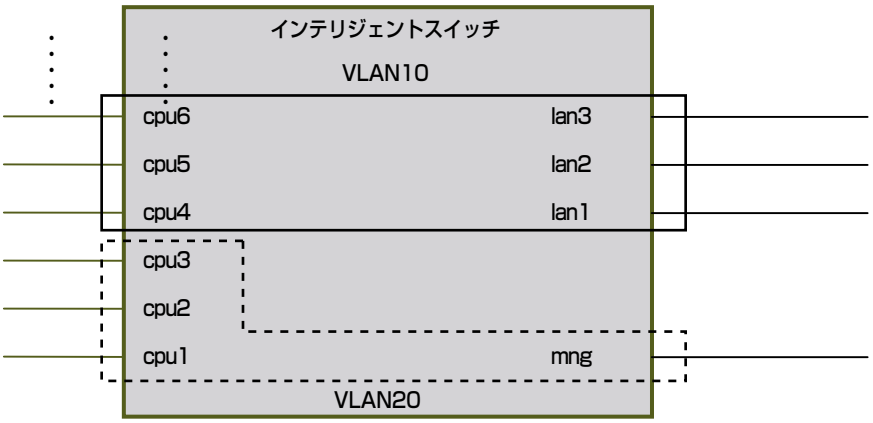
ポートベースVLANを構成する物理イーサネットポートの登録を行います。工場出荷時の状態ではすべてのポート状態はアンタグポートに設定され、VID=1（デフォルトVLAN）がポートのメンバーに設定されています。

ポートベースVLANのポートの登録

ポートのメンバーとなるVLANの変更を行うときには、グローバルモードで変更するポートを指定してポートコンフィグレーションモードへ移行し、memberコマンドを使用してメンバーとなるVLANを設定します。

```
(Conf-global)#port lan1
(Conf-pt-lan1)# member vlan 3
(Conf-pt-lan1)#
```

本装置のポートを2つのポートベースVLANに分けた場合の構成例を示します。



VLANの構成例

ポートベースVLAN10の登録

```
(Conf-global)#vlan 10 VLAN0010
(Conf-global)# port lan1
(Conf-pt-lan1)# member vlan 10
(Conf-pt-lan1)# exit
(Conf-global)#port lan2
(Conf-pt-lan2)# member vlan 10
(Conf-pt-lan2)# exit
(Conf-global)# port lan3
(Conf-pt-lan3)# member vlan 10
(Conf-pt-lan3)# exit
(Conf-global)# port cpu4
(Conf-pt-cpu4)# member vlan 10
(Conf-pt-cpu4)# exit
(Conf-global)# port cpu5
(Conf-pt-cpu5)# member vlan 10
(Conf-pt-cpu5)# exit
(Conf-global)# port cpu6
(Conf-pt-cpu6)# member vlan 10
(Conf-pt-cpu6)# exit
```

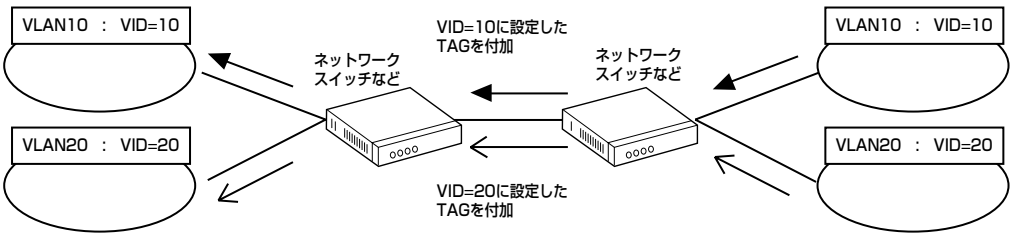
ポートベースVLAN20の登録

```
(Conf-global)#vlan 20 VLAN0020
(Conf-global)# port mng
(Conf-pt-mng)# member vlan 20
(Conf-pt-mng)# exit
(Conf-global)# port cpu1
(Conf-pt-cpu1)# member vlan 20
(Conf-pt-cpu1)# exit
(Conf-global)# port cpu2
(Conf-pt-cpu2)# member vlan 20
(Conf-pt-cpu2)# exit
(Conf-global)# port cpu3
(Conf-pt-cpu3)# member vlan 20
(Conf-pt-cpu3)# exit
```

タグポートの設定

フレームヘッダにVLAN-TAGを付加することで、そのフレームに対応するVLANを識別することができます。そのため、同一リンク上で複数のVLANのフレーム転送ができます。たとえばポートベースVLANを使用した場合には、同じVLANを持つ2つの装置を接続するにはVLAN数分の回線が必要となりますが、VLAN-TAG付きフレームを用いることで1回線で複数のVLANのフレームを送信することが可能になるため、使用ポートを削減することができます。

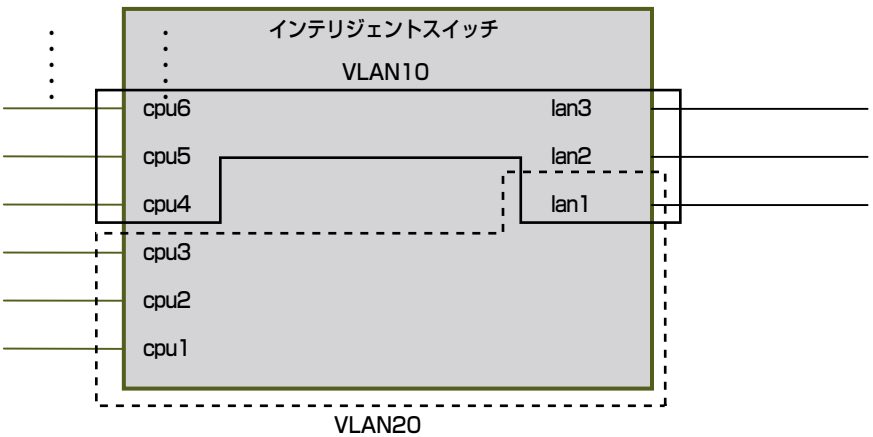
同一リンク上の同一VLANセグメントではTAG付き/TAGなしのどちらか一方のフレームしか送受信できません。すなわち、ポートにTAGなしとして設定されたVLANでTAG付きフレームを受信した場合、そのフレームは廃棄されます。また、ポートにTAG付きとして設定されたVLANでTAGなしフレームを受信した場合、そのフレームは廃棄されます。
VLAN-TAG付きフレームによるVLAN識別を行う場合には、各装置において、VLANに対応するTAG ID（VID）を同じ値に設定する必要があります。



TAGを使用したVLAN構成例

タグポート、メンバー VLANの登録

ポートをタグポートに設定する場合は、変更するポートを指定してポートコンフィグレーションモードへ移行し、encapsulationコマンドを使用してください。



タグポートを含むVLANの構成例（lan1:タグポート）

ポートベースVLAN10の登録

```
(Conf-global)# vlan 10 VLAN0010
(Conf-global)# port lan2
(Conf-pt-lan2)# member vlan 10
(Conf-pt-lan2)# exit
(Conf-global)# port lan3
(Conf-pt-lan3)# member vlan 10
(Conf-pt-lan3)# exit
(Conf-global)# port cpu4
(Conf-pt-cpu4)# member vlan 10
(Conf-pt-cpu4)# exit
(Conf-global)# port cpu5
(Conf-pt-cpu5)# member vlan 10
(Conf-pt-cpu5)# exit
(Conf-global)# port cpu6
(Conf-pt-cpu6)# member vlan 10
(Conf-pt-cpu6)# exit
```

ポートベースVLAN20の登録

```
(Conf-global)# vlan 20 VLAN0020
(Conf-global)# port cpu1
(Conf-pt-cpu1)# member vlan 20
(Conf-pt-cpu1)# exit
(Conf-global)# port cpu2
(Conf-pt-cpu2)# member vlan 20
(Conf-pt-cpu2)# exit
(Conf-global)# port cpu3
(Conf-pt-cpu3)# member vlan 20
(Conf-pt-cpu3)# exit
```

タグポートの登録

```
(Conf-global)# port lan1
(Conf-pt-lan1)# encapsulation dot1q
(Conf-pt-lan1)# member vlan 10,20
(Conf-pt-lan1)# exit
```

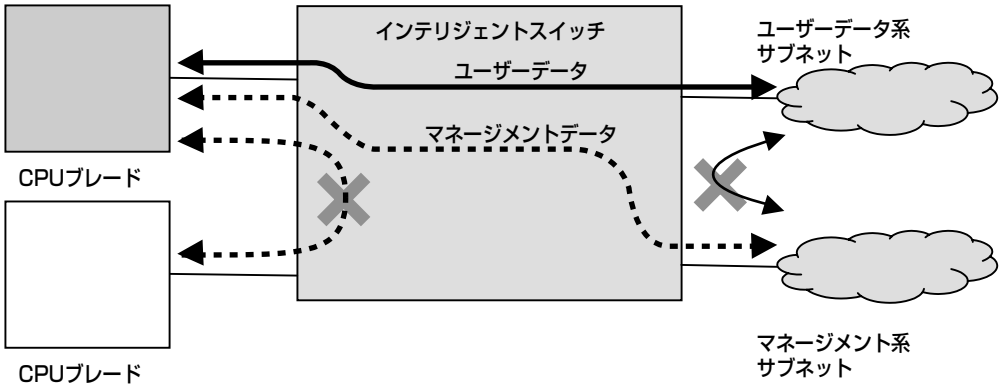
タグポートの削除

タグポートをアンタグポートに変更する場合には、no encapsulationコマンドを使用してください。

```
(Conf-global)# port lan1
(Conf-pt-lan1)# no encapsulation
(Conf-pt-lan1)# exit
```

マネージメントVLAN

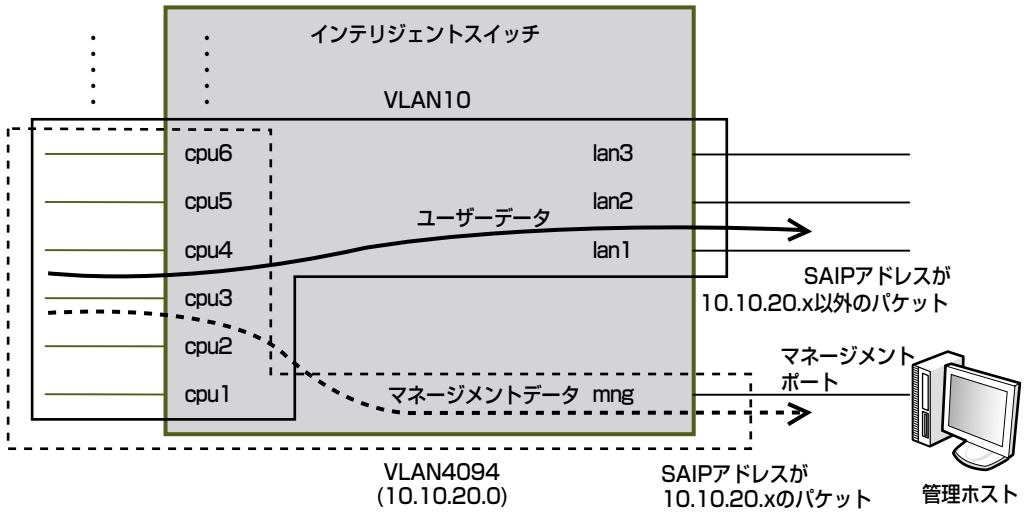
マネージメントVLANは、CPUブレードにVLANタグを設定することなく、ユーザーデータ系ネットワークとマネージメント系ネットワークを分離する機能です。
マネージメントVLANは、複数のCPUと1つのマネージメントポートから構成されます。ユーザーポートはマネージメントVLANに加入することはできません。
マネージメントポートの先には管理ホストが接続され、各CPUブレードと管理ホスト間の通信を保証します。マネージメントVLANサブネットにおいては、CPUブレード間は通信できません。本装置はCPUブレードから送信されるパケットの送信元IPアドレスを確認し、マネージメントVLANサブネットと一致するパケットをマネージメントポートに転送することで本機能を実現しています。



CPUブレードのインタフェースに
ユーザーデータ系サブネットと
マネージメント系サブネットに
それぞれ対応したIPアドレスを
設定することで両サブネットとの
通信が可能になります

マネージメントメントVLANの通信

CPUポートはアンタグポートに設定されている場合でも、マネージメントVLANが登録されている場合には、1つのポートベースVLANとマネージメントVLANを同時にメンバーとすることができます。マネージメントVLAN有効時の本装置内のポートの実装例を下図に示します。



マネージメントVLANの構成例

上図の構成例のコンフィグレーションを以下に示します。

ポートベースVLAN10の登録

```
(Conf-global)# vlan 10 VLAN0010
(Conf-global)# port lan1
(Conf-pt-lan1)# member vlan 10
(Conf-pt-lan1)# exit
(Conf-global)# port lan2
(Conf-pt-lan2)# member vlan 10
(Conf-pt-lan2)# exit
(Conf-global)# port lan3
(Conf-pt-lan3)# member vlan 10
(Conf-pt-lan3)# exit
(Conf-global)# port cpu1
(Conf-pt-cpu1)# member vlan 10
(Conf-pt-cpu1)# exit
(Conf-global)# port cpu2
(Conf-pt-cpu2)# member vlan 10
(Conf-pt-cpu2)# exit
(Conf-global)# port cpu3
(Conf-pt-cpu3)# member vlan 10
(Conf-pt-cpu3)# exit
(Conf-global)# port cpu4
(Conf-pt-cpu4)# member vlan 10
(Conf-pt-cpu4)# exit
(Conf-global)# port cpu5
(Conf-pt-cpu5)# member vlan 10
(Conf-pt-cpu5)# exit
(Conf-global)# port cpu6
(Conf-pt-cpu6)# member vlan 10
(Conf-pt-cpu6)# exit
```

マネージメントVLAN4094の登録

```
(Conf-global)# vlan 4094 Mng-VLAN4094
(Conf-global)# interface vlan4094
(Conf-if-vlan4094)# management subnet 10.10.20.0/24
(Conf-if-vlan4094)# exit
(Conf-global)# port cpu1
(Conf-pt-cpu1)# member vlan 4094
(Conf-pt-cpu1)# exit
(Conf-global)# port cpu2
(Conf-pt-cpu2)# member vlan 4094
(Conf-pt-cpu2)# exit
(Conf-global)# port cpu3
(Conf-pt-cpu3)# member vlan 4094
(Conf-pt-cpu3)# exit
(Conf-global)# port cpu4
(Conf-pt-cpu4)# member vlan 4094
(Conf-pt-cpu4)# exit
(Conf-global)# port cpu5
(Conf-pt-cpu5)# member vlan 4094
(Conf-pt-cpu5)# exit
(Conf-global)# port cpu6
(Conf-pt-cpu6)# member vlan 4094
(Conf-pt-cpu6)# exit
```

ブリッジ機能

ブリッジは、どの物理ポート上にどのノードが存在しているのかを、VLANごとにMACアドレステーブルで管理しています。
物理ポートからMACフレームの入力があった時、MACフレームのヘッダ情報にある送信元MACアドレスを読み取り、そのMACアドレスを持つノードと入力のあった物理ポートとを関連付けし、MACアドレステーブルに登録します（学習）。
転送すべきフレームの送信先MACアドレスが、MACアドレステーブルに存在していなければVLAN内の全物理ポートからフレームを出力（フラッディング）し、存在していれば関連付けされた物理ポートのみからフレームを出力します。ただし、転送する物理ポートが入力した物理ポートと同じであれば、そのフレームは転送する必要がないため廃棄されます。
MACアドレステーブルに登録された情報は、そのMACアドレスを持つノードからのフレーム送信がないまま一定時間を過ぎると、その情報は消去されます（エージング）。

MACアドレステーブルの設定

アドレス学習機能によってMACアドレスを学習するのではなく、あらかじめMACアドレスと物理イーサネットポートおよび仮想イーサネットポートなどの対応を設定しておくことができます。この場合、該当MACアドレスはエージアウトによる削除対象とはなりません。この設定によってMACアドレステーブルにエントリが生成されます。宛先不明によるフラッドパケットを削減したい場合や、端末と物理イーサネットポートを固定的に接続するような場合に設定します。

MACアドレステーブルの表示

設定されているMACアドレステーブルを表示する場合は、show mac addressコマンドを使用してください。

```
(Conf-global)# show mac address
```

MACアドレステーブルへのエントリの追加

MACアドレステーブルにエントリを追加する場合は、グローバルモードで設定するVLANを指定してインタフェースコンフィグレーションモードへ移行し、mac addressコマンドを使用してください。

```
(Conf-global)# interface vlan10
(Conf-if-vlan10)# mac address 00:00:4c:00:00:01 lan1
```

MACアドレステーブルからのエントリの削除

MACアドレステーブルからエントリを削除する場合は、インタフェースコンフィグレーションモードでno mac addressコマンドを使用してください。

```
(Conf-global)# interface vlan10
(Conf-if-vlan10)# no mac address 00:00:4c:00:00:01
```

エージングタイムの設定

この装置はMACアドレス学習機能により作成されたMACアドレステーブルに基づいて、イーサネットパケットをスイッチングすることができます。MACアドレステーブルはMACアドレスと物理イーサネットポートおよび仮想イーサネットポート等を結びつけるためのテーブルです。この学習したMACアドレスを使用するイーサネットパケットが一定時間内に送受信されない場合、該当MACアドレスはMACアドレステーブルから削除されます。この機能をエージングといい、この時間をエージングタイムといいます。この装置は、工場出荷時にエージングタイムを300秒に設定してあります。

エージングタイムの変更

設定されているエージングタイムを変更する場合は、グローバルコンフィグレーションモードでmac aging-timerコマンドを使用してください。

```
(Conf-global)# mac aging-timer 600
```

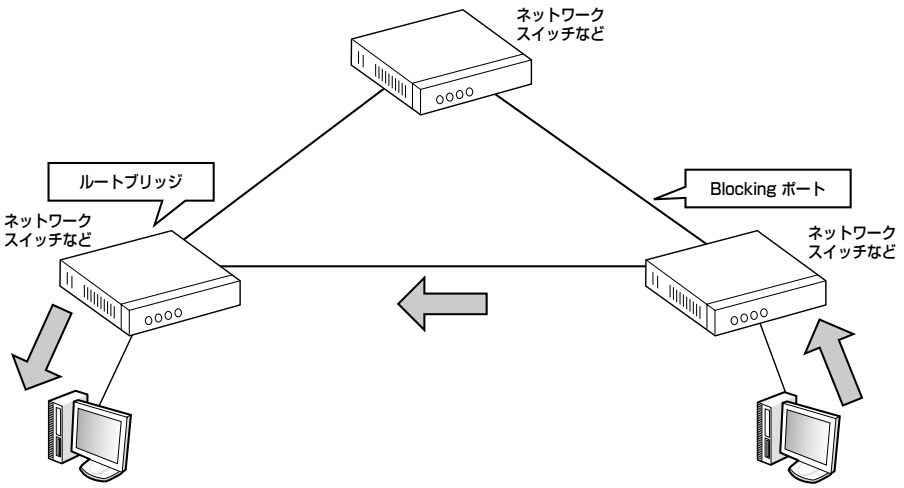
エージングタイムの設定表示

設定されているエージングタイムを表示する場合は、show mac aging-timerコマンドを使用してください。

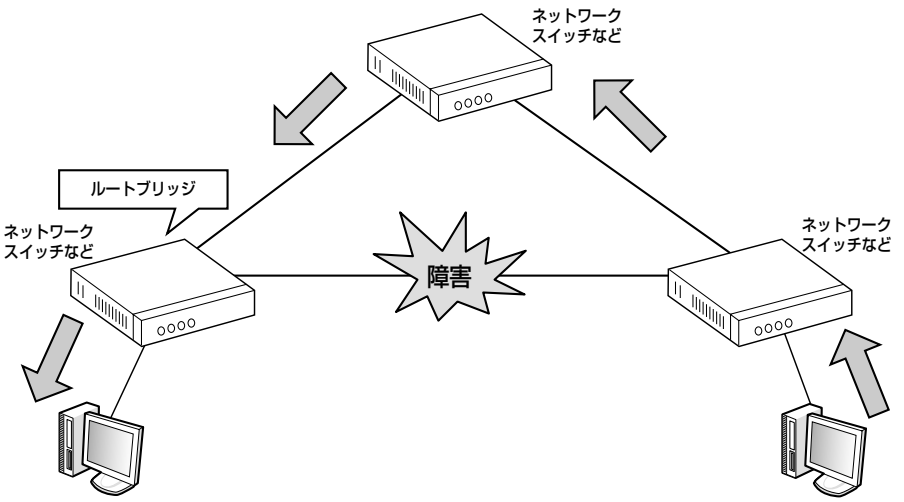
```
(Conf-global)# show mac aging-timer
```

スパニングツリー

スパニングツリーとは、IEEE802.1dで定義されている複数のブリッジを接続して構築されたネットワークにおいて、ループを防止しながら経路の冗長性を実現させるものです。
スパニングツリーを動作させる場合は、スパニングツリーの設定を行ってから、ポートの接続を行うなど、設定手順に十分注意する必要があります。
スパニングツリーは、ネットワークを理論的なツリー構造に構築し、ブリッジ間経路が1経路しか存在しないようループを排除します。ツリー上の経路が障害等で途切れた場合には、それを自動的に検出し、ツリーを再構築します。
本装置は、VLANごとに独立したスパニングツリーを構築することが可能であり、また、VLANごとにツリーを構築するためのスパニングツリーのパラメータを設定・変更することが可能です。複数のVLANに属しているポート(タグポート)においてもスパニングツリーを動作させることができます。



通常のパケット経路



変更時のパケット経路

スパニングツリーのパケット経路変更

Rapidスパニングツリー（IEEE802.1w）は、スパニングツリーと同じように、BPDU（Bridge Protocol Data Unit）を使ってブリッジ間で情報を交換し、LAN 内でデータのループを防止しながら経路の冗長性を実現します。スパニングツリーでは、通信経路の切り替えに数十秒を要しますが、Rapidスパニングツリーでは、ブリッジの装置間でネゴシエーションをとることで、数秒での高速な通信経路の切り替えを行い、通信不通の時間が短く済みます。
本装置では、IEEE802.1dのスパニングツリー、Rapidスパニングツリーの両方による経路冗長が可能です。

スパニングツリーの設定はスパニングツリー機能を行う各VLANに対しての設定とVLANを構成する各ポートに対しての設定が行えます。

スパニングツリーの有効化

スパニングツリーを有効にする場合は、グローバルコンフィグレーションモードでspanning-tree modeコマンドを使用してください。スパニングツリーのモードにはstandard(IEEE802.1d)とrapid（IEEE802.1w）があります。

```
(Conf-global)# spanning-tree mode vlan3 standard
```

スパニングツリーの表示

スパニングツリーの表示を行う場合は、show spanning-treeコマンドを使用してください。

```
(Conf-global)# show spanning-tree vlan3
```

スパニングツリーの無効化

スパニングツリーを無効にする場合は、no spanning-tree modeコマンドを使用してください。

```
(Conf-global)# no spanning-tree mode vlan3
```

スパニングツリーのプライオリティの変更

スパニングツリーのプライオリティを変更する場合は、spanning-tree bridge-priorityコマンドを使用してください。スパニングツリーを行う装置間で最もプライオリティの高い（プライオリティ値が最も小さい）装置がルートブリッジとなります。no spanning-tree bridge-priorityコマンドによりプライオリティをデフォルト値に戻します。

```
(Conf-global)# spanning-tree bridge-priority vlan3 65535
```

スパニングツリーのタイマー値の変更

スパニングツリーのタイマー値を変更にする場合は、spanning-tree timerコマンドを使用してください。スパニングツリーで設定するタイマー値にはMax Age、Hello Time、Forward Delayがあり、以下の関係があります。
2 ×（Forward Delay - 1）≧ Max Age ≧ 2 ×（Hello Time + 1）
Max Ageを40(秒)、Hello Timeを10(秒)、Forward Delayを30(秒)に変更する場合

```
(Conf-global)# spanning-tree timer vlan3 maxage 40 hello 10
forwarddelay 30
```

no spanning-tree timerコマンドによりすべての設定値をデフォルト値に戻します。

スパニングツリーのFast Portの有効化

スパニングツリーのポートをFastPortに設定するとそのポートは、スパニングツリーの影響を受けずに通信を行います。スパニングツリーのポートをFast Portを有効にする場合は、ポートコンフィグレーションモードでspanning-tree fastportコマンドを使用してください。

```
(Conf-global)#port lan1
(Conf-pt-lan1)# spanning-tree fastport
```

ポートがタグポートの場合にはVLANを指定してください。

```
(Conf-global)#port lan1
(Conf-pt-lan1)# spanning-tree fastport vlan3
```

スパニングツリーのFast Portの無効化

スパニングツリーのFast Portを無効にする場合は、ポートコンフィグレーションモードでno spanning-tree fastportコマンドを使用してください。

```
(Conf-global)#port lan1
(Conf-pt-lan1)# no spanning-tree fastport
```

ポートがタグポートの場合にはVLANを指定してください。

```
(Conf-global)#port lan1
(Conf-pt-lan1)# no spanning-tree fastport vlan3
```

スパニングツリーのポートプライオリティの変更

スパニングツリーのポートプライオリティを変更する場合には、ポートコンフィグレーションモードでspanning-tree port-priorityコマンドを使用してください。no spanning-tree port-priorityコマンドによりプライオリティをデフォルト値に戻します。

```
(Conf-global)#port lan1
(Conf-pt-lan1)# spanning-tree port-priority 255
```

ポートがタグポートの場合にはVLANを指定してください。

```
(Conf-global)#port lan1
(Conf-pt-lan1)# spanning-tree port-priority vlan3 255
```

スパニングツリーのパスコストの変更

スパニングツリーのパスコストを変更する場合には、ポートコンフィグレーションモードでspanning-tree port pathcostコマンドを使用してください。no spanning-tree pathcostコマンドによりパスコストをデフォルト値に戻します。パスコストの範囲は、スパニングツリーのモードにより異なります。

standardモードのパスコストの範囲: 1-65535

rapidモードのパスコストの範囲: 1-200000000

```
(Conf-global)#port lan1
(Conf-pt-lan1)# spanning-tree pathcost 1000
```

ポートがタグポートの場合にはVLANを指定してください。

```
(Conf-global)#port lan1
(Conf-pt-lan1)# spanning-tree pathcost vlan3 1000
```

リンクアグリゲーション

本装置ではIEEE802.3adに準拠したリンクアグリゲーションをサポートします。リンクアグリゲーション機能は、複数の物理ポートを収容する仮想的な回線となるLAG(リンクアグリゲーション グループ)を作成することにより、隣接ノードとの通信帯域を広げることができます。また、LAG内のある物理ポートが障害になった場合にも他の物理ポートによる通信が可能ですので、信頼性の向上が図られます。

本装置では、LAGを構成するポートのMACアドレスの1つをLAGのシステムIDとして使用します。LACP（Link Aggregation Control Protocol）を使用している場合に、LAGのシステムIDにMACアドレスが使用されているポートをそのLAGのメンバーリンクから削除すると、隣接装置との間でLACPによるLAGの再構成が行われ、この間LAGがダウン状態になります。
これを避ける方法として、LAGのメンバーリンクを削除する場合には、LAGのシステムIDにMACアドレスが使用されていないポートを削除する、あるいは、あらかじめlag-macコマンドによりスタティックにLAGのシステムIDを登録するなどを行ってください。

LAGのシステムIDはshow lagコマンドのMac Address、ポートのMACアドレスはshow portコマンドのPhysical addressにより確認できます。

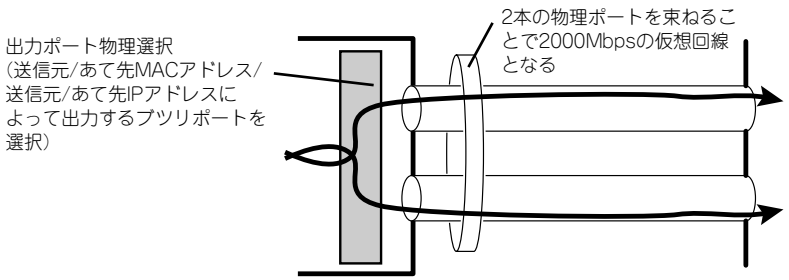
特　長

本装置の特長は以下のとおりです。

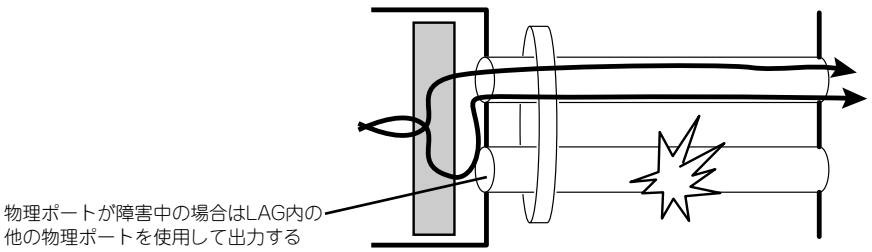
- ポートベースVLANとして使用されている物理ポート（アンタグポート）の他、タグVLANで使用している物理ポート（タグポート）においてもリンクアグリゲーションの設定が可能です。なお、リンクアグリゲーションの設定が可能なポートはLANポートのみです。1つのLAGの最大ポート数は8です。
- 送信元/宛先のMACアドレス/IPアドレスによる送信物理ポートの選択が可能です。
- リンクアグリゲーション の設定に以下の2つの方法があります。
  - IEEE802.3adに準拠したLACPモード
  - 本装置での独自機能として、LACPDU（Link Aggregation Control Protocol）の送受信を行わないStaticモード

重要

- **リンクアグリゲーションに使用しているポートを含むVLANでは、スパニングツリー機能を使用することはできません。**
- **リンクアグリゲーションを動作させる場合は、ループが発生しないようにリンクアグリゲーションの設定を行ってからポートの接続を行う、またはポートのshutdownを行ったうえでリンクアグリゲーションの設定を行うなど、手順に注意する必要があります。**



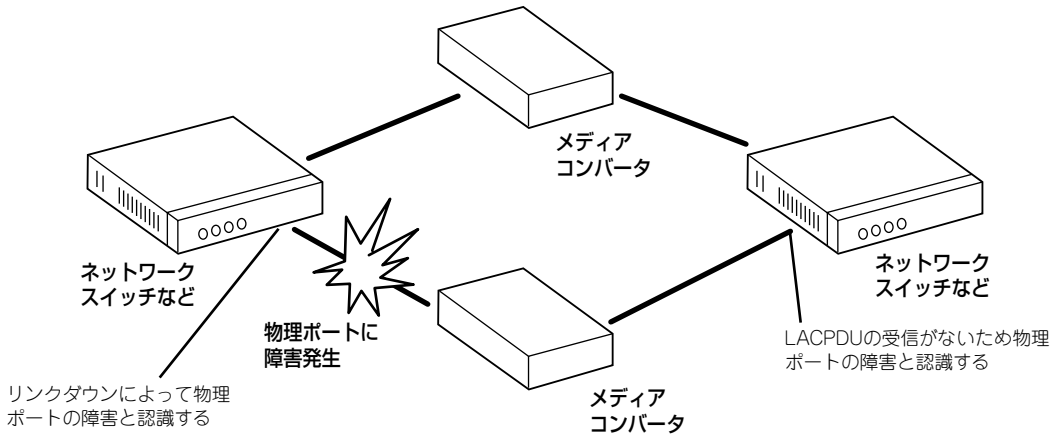
リンクアグリゲーションの動作（正常時）



リンクアグリゲーションの動作（物理ポート障害時）

LAGの動作モード

リンクアグリゲーションを設定し接続されたノード同士では、各物理ポートにおいてLACPDU(Link Aggregation Control Protocol Data Unit)の送受信を行います。一定時間LACPDUの受信がない物理ポートは障害が発生しているものとして扱うことができます。



物理ポート障害の検出

LACPDUにはシステムプライオリティとシステムIDの情報が載っており、接続先装置の識別のために使用されます。システムIDは通常ノードや物理ポートに設定されているMACアドレスになります。
動作モードがactiveであるノードは周期的にLACPDUの送信を行い、動作モードがpassiveであるノードはLACPDUの受信を契機にLACPDUを送信します。動作モードがactiveであるノードとpassiveであるノードが接続されていた場合、両ノードとも設定通りの動作を行いますが、両ノードともに動作モードがactiveであった場合、先にLACPDUを送信したノードがactiveとなり、もう一方のノードはpassiveの動作になります。両ノードともにpassiveモードの場合、LACPDUの送受信がないためリンクアグリゲーションは機能しません。
本装置での独自機能として、LACPDUの送受信を行わないstaticモードが存在します。staticモードでは、LACPDU送受信の処理が行われない分、装置内処理の負担が軽くなるとともに、物理ポート上にLACPDUが流れない分、転送帯域の有効利用が行えます。ただし、物理ポートの障害は、リンクダウンによってのみ検出可能となるので、ノード間を直接接続する必要があります。staticモードを使用する場合は、両ノードともにstaticの設定をする必要があります。

出力物理ポートの選択論理

本装置では、LAG内のどの物理ポートにフレームを出力するかを決定するためのキーとして、送信元MACアドレス、宛先MACアドレス、送信元及び宛先MACアドレス、送信元IPアドレス、宛先IPアドレス、送信元及び宛先IPアドレスの6パターンから選択できます。
出力するフレームから選択されたキーを読み出してハッシュ化し、その結果をLAG内ポートに振り分けることによって出力する物理ポートを決定します。初期設定では、送信元MACアドレスが設定されています。
例えば、サーバなど大量にフレームを送信する端末を受け持つノードでは、初期値である送信元MACアドレスをキーにしたままでは、出力する物理ポートに偏りができてしまうため、宛先MACアドレスを出力物理ポート選択のキーとして選択するなど、ネットワーク環境に応じて変更する必要があります。

リンクアグリゲーションの設定

LAGの登録

lagコマンドを使用して新規に登録するLAGを作成します。LAGの登録はグローバルコンフィグレーションモードで行います。LAGの登録を行うとLAGコンフィグレーションモードに移行します。すでに登録されているLAGの変更を行うときもlagコマンドを使用して変更するLAG IDを指定します。LAG IDの値は、1以上128以下の範囲で任意に決めてください。

LAGの表示

```
(Conf-global)# lag 10
(Conf-lag10)#
```

登録されているLAGを表示する場合は、show lagコマンドを使用してください。

```
(Conf-global)# show lag
```

LAGの削除

グローバルコンフィグレーションモードでno lagコマンドを使用して登録されているLAGの削除を行います。

```
(Conf-global)# no lag 10
```

LAGのポートの登録

LAGを構成する物理イーサネットポートの登録を行います。LAGを構成する物理イーサネットポートのはスピード、Duplex、およびポートが属するVLANのメンバーはすべて同じに設定されている必要があります。
LAGを構成する物理イーサネットポートの登録は、member-linkコマンドを使用してください。

```
(Conf-lag10)# member-link lan1
```

LAGのポートの削除

LAGを構成する物理イーサネットポートを削除するときは、no member-linkコマンドを使用してください。

```
(Conf-lag10)# no member-link lan1
```

LAGの動作モードの変更

LAGの動作モードを変更する場合は、aggregate-typeコマンドを使用してください。モードにはstatic、active、passiveがあり、デフォルト値はstaticです。no aggregate-typeコマンドにより動作モードをデフォルト値に戻します。

```
(Conf-lag10)# aggregate-type active
```

LAGのシステムプライオリティの変更

LAGのシステムプライオリティを変更する場合は、lag-priorityコマンドを使用してください。デフォルト値は32768です。no lag-priorityコマンドによりプライオリティをデフォルト値に戻します。

```
(Conf-lag10)# lag-priority 65535
```

LAGのシステムIDの変更

LAGのシステムID（MACアドレス）を変更する場合は、lag-macコマンドを使用してください。デフォルト値はLAG内物理ポートのうちで一番小さなMACアドレスになります。lag-macコマンドによりシステムIDをデフォルト値に戻します。

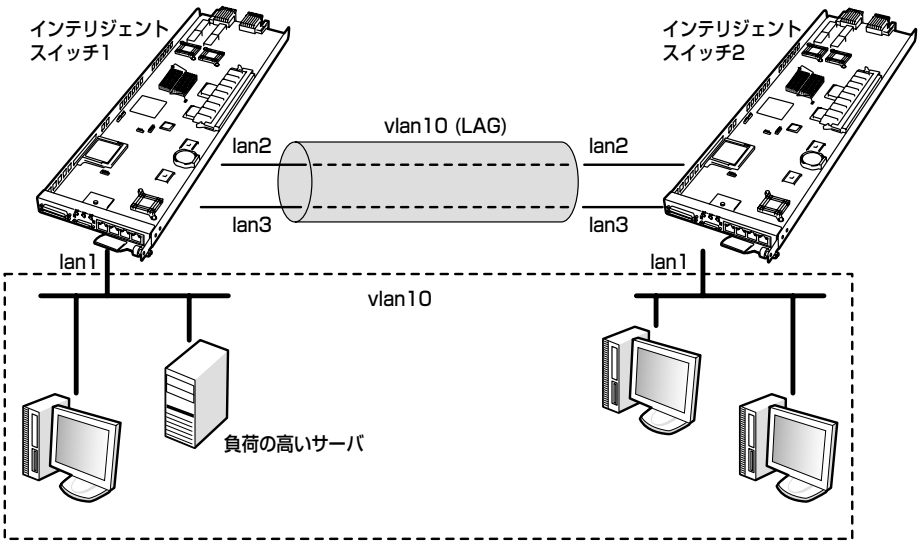
```
(Conf-lag10)# lag-mac 00:00:11:22:33:44
```

出力物理ポートの選択論理の変更

LAG内の出力物理ポートの選択論理を変更する場合は、load-balanceコマンドを使用してください。初期値はsrc-MACです。no load-balance出力物理ポートの選択論理をデフォルト値に戻します。

```
(Conf-lag10)# load-balance src-ip
```

LAGの設定例を示します。
インテリジェントスイッチ1では負荷の高いサーバが存在していますので、LAG内の出力物理ポート選択論理は宛先MACアドレスで行います。



リンクアグリゲーションの構成例

インテリジェントスイッチ1の設定

LAG内物理ポートをAUTOに設定します。
LAGモードをActiveで動作させます。

```
(Conf-global)#vlan 10 vlan10
(Conf-global)#port lan1
(Conf-pt-lan1)#member vlan 10
(Conf-pt-lan1)#exit
(Conf-global)#port lan2
(Conf-pt-lan2)#duplex auto
(Conf-pt-lan2)#member vlan 10
(Conf-pt-lan2)#exit
(Conf-global)#port lan3
(Conf-pt-lan3)#duplex auto
(Conf-pt-lan3)#member vlan 10
(Conf-pt-lan3)#exit
(Conf-global)#lag 10
(Conf-lag10)#member-link lan2
(Conf-lag10)#member-link lan3
(Conf-lag10)#aggregate-type active
(Conf-lag10)#lag-priority 1000
(Conf-lag10)#load-balance dst-mac
(Conf-lag10)#no shutdown
(Conf-lag10)#exit
```

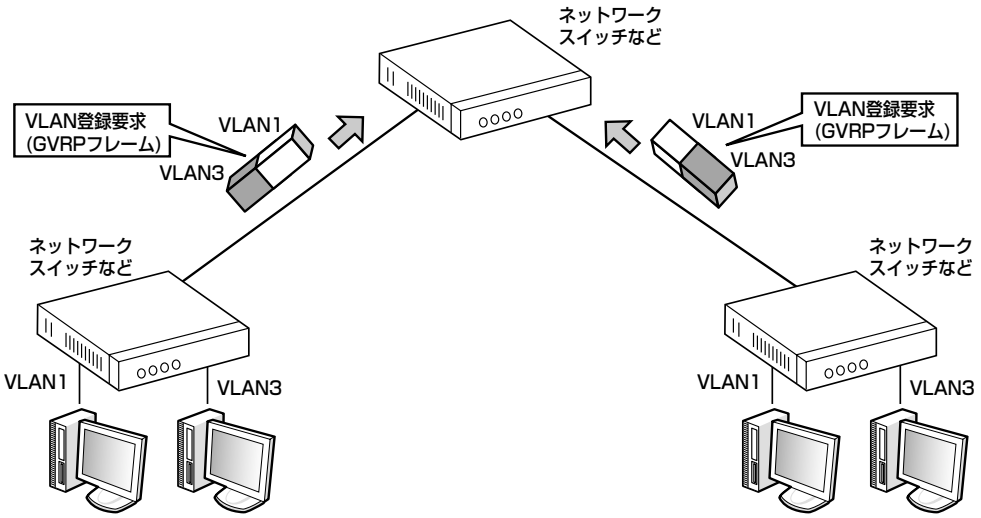
インテリジェントスイッチ2の設定

LAG内物理ポートをAUTOに設定します。
LAGモードをPassiveで動作させます。

```
(Conf-global)#vlan 10 vlan10
(Conf-global)#port lan1
(Conf-pt-lan1)#member vlan 10
(Conf-pt-lan1)#exit
(Conf-global)#port lan2
(Conf-pt-lan2)#duplex auto
(Conf-pt-lan2)#member vlan 10
(Conf-pt-lan2)#exit
(Conf-global)#port lan3
(Conf-pt-lan3)#duplex auto
(Conf-pt-lan3)#member vlan 10
(Conf-pt-lan3)#exit
(Conf-global)#lag 10
(Conf-lag10)#member-link lan2
(Conf-lag10)#member-link lan3
(Conf-lag10)#aggregate-type passive
(Conf-lag10)#load-balance src-mac
(Conf-lag10)#no shutdown
(Conf-lag10)#exit
```

GVRP

GVRP(Garp Vlan Registration Protocol)はGARP(Generic Attribute Registration Protocol)を使用して、自ノードに接続されているVLANのVIDをタグポートで接続されている隣接装置に通知するプロトコルです。これにより、ネットワークの末端に存在する同じVIDを持ったVLANが、あらかじめVLANが固定的に設定されていないノードをまたいでVLANの経路が形成され、相互に通信することが可能になります。タグポートの所属するVLANの設定が不要になるため、ネットワーク設定が簡素化されます。



GVRPによる経路情報の伝達

重要

GVRPによりダイナミックに作成されたVLANのスパニングツリー機能を有効にすることはできません。

装置のグローバルなGVRP機能の有効化

装置のグローバルなGVRP機能を有効にする場合は、グローバルコンフィグレーションモードでgvrp enableコマンドを使用してください。工場出荷時の状態では、GVRP機能は無効になっています。装置のグローバルなGVRP機能を無効にする場合は、no gvrp enableコマンドを使用してください。

```
(Conf-global)# gvrp enable
```

物理ポートのGVRP機能の有効化

GVRPは、タグポートでのみ動作します。物理ポートのGVRP機能を有効にする場合は、ポートコンフィグレーションモードでencapsulation dot1qコマンドにより物理ポートをタグポートに設定した後に gvrp enableコマンドを使用してください。gvrp enableコマンドを入力すると、その物理ポートにmember vlanコマンドにより登録されていたVLANは削除されます。物理ポートのGVRP機能を無効にする場合は、no gvrp enableコマンドを使用してください。

```
(Conf-global)# port lan1
(Conf-pt-lan1)# encapslation dot1q
(Conf-pt-lan1)# gvrp enable
```

GVRP広告の受信動作の設定

隣接ノードからGVRP広告を受信した時の動作を設定する場合は、ポートコンフィグレーションモードでgvrp modeコマンドを使用してください。動作モードにはnormalモード、forbiddenモードの2種類があります。隣接ノードからVLAN情報(VID)の載ったGVRPフレームを受信した（広告があった）場合、normalモードでは該当するVID宛のフレームについての出力を始めます。forbiddenモードではこの情報（広告）を無視します。forbiddenモードは、自ノード配下のVLANを他のノードと共有しない場合に使用します。デフォルトでは、normalモードに設定されています。

```
(Conf-global)# port lan1
(Conf-pt-lan1)# gvrp mode forbidden
```

GVRPによるStatic VLANの広告の設定

装置に登録されたStatic VLANをGVRPの広告の対象にする場合には、グローバルコンフィグレーションモードでgvrp join vlanコマンドを使用してください。装置に登録されたVLANは、デフォルトで広告されます。Static VLANをGVRPの広告の対象にしない場合には、no gvrp join vlanコマンドを使用してください。

```
(Conf-global)#gvrp join vlan 2,5-7
```

GARPタイマの設定

GARPのタイマ値を変更する場合には、グローバルコンフィグレーションモードでgarp timerコマンドを使用してください。タイマにはJoin、Leave、Leaveallの3つがあり、省略されたタイマは、デフォルト値が設定されます。3つのタイマ値は、次の設定ルールがあります。

3 × Join ≦ Leave ＜ Leaveall

Join: 300(msec.)

Leave: 900 (msec.)

Leaveall: 10000 (msec.) に変更する場合

```
(Conf-global)# garp timer join 300 leave 900 leaveall 10000
```

no garp timerコマンドによりすべての設定値をデフォルト値に戻します。

GVRP状態の表示

GVRPの表示を行う場合は、show gvrpコマンドを使用してください。

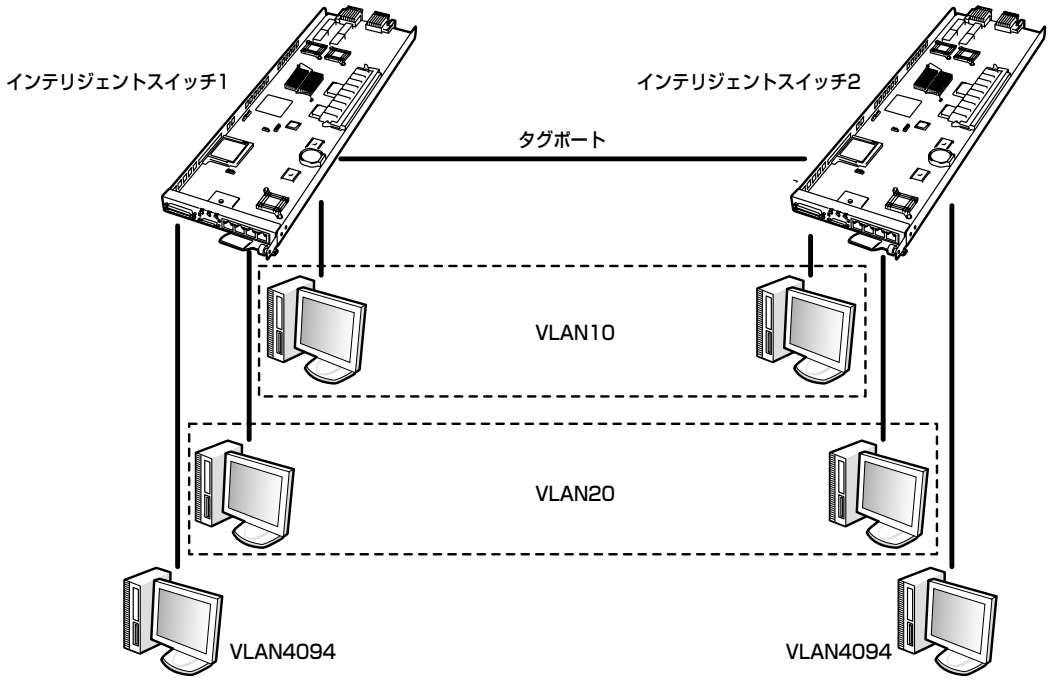
```
(Conf-global)# show gvrp
```

GVRP統計情報の表示

GVRPの統計情報の表示を行う場合は、show gvrp statistics コマンドを使用してください。

```
(Conf-global)# show gvrp statistics lan1
```

GVRPの設定例を示します。
VLAN10とVLAN20をGVRPの広告対象にします。



GVRPの構成例

インテリジェントスイッチ1、インテリジェントスイッチ2の設定

vlan4094をGVRPの広告対象から外します。GVRPをnormalモードで動作させます。

```
(Conf-global)#vlan 10 VLAN10
(Conf-global)#vlan 20 VLAN20
(Conf-global)#vlan 4094 VLAN4094
(Conf-global)#gvrp enable
(Conf-global)#no gvrp join vlan 4094
(Conf-global)#port lan1
(Conf-pt-lan1)#member vlan 10
(Conf-pt-lan1)#port lan2
(Conf-pt-lan2)#member vlan 20
(Conf-pt-lan2)#port mng
(Conf-pt-mng)#member vlan 4094
(Conf-pt-mng)#port lan3
(Conf-pt-lan3)#encapsulation dot1q
(Conf-pt-lan3)#gvrp enable
(Conf-pt-lan3)#gvrp mode normal
```

ルーティング機能

IPデータグラムを目的のホストまで伝送するときに、ネットワーク内で伝送経路を選択することを「ルーティング」と言います。

- スタティックルーティング

  経路情報を運用者があらかじめ装置に設定します。経路変更時は、運用者が装置の設定を変更する必要があります。

本装置でルーティングを行うためには、IPアドレステーブルの設定、IPスタティックルートの設定を行います。

mngポートを含むVLANは、CPUブレードと本装置の監視のためだけに使用してください。mngポートを含むVLANでのL3通信は、ソフト転送により行われますのでCPUに負荷がかかる可能性があります。

IPアドレスの設定

IPアドレステーブルとは、本装置の各仮想インタフェースに割り当てたIPアドレスやサブネットマスクを保持するためのテーブルです。
本装置の内蔵ルータがサポートするインタフェースは仮想インタフェース(VLAN)となりますので、仮想インタフェースに対してIPアドレスやサブネットマスクを割り当てます。これによりIPアドレステーブルに仮想インタフェースとIPアドレスの関連付けを表すエントリが生成されます。

numberedインタフェースの登録

仮想インタフェースにnumberedインタフェースとしてIPアドレスとサブネットマスクを登録します。
numberedインタフェースのエントリを追加する場合は、インタフェースコンフィグレーションモードでip addressコマンドを使用してください。

```
(Conf-global)# interface vlan10
(Conf-if-vlan10)# ip address 192.168.1.254/24
```

numberedインタフェースの表示

設定されているnumberedインタフェースを表示する場合は、show vlanコマンドを使用してください。

```
(Conf-global)# show vlan
```

numberedインタフェースの削除

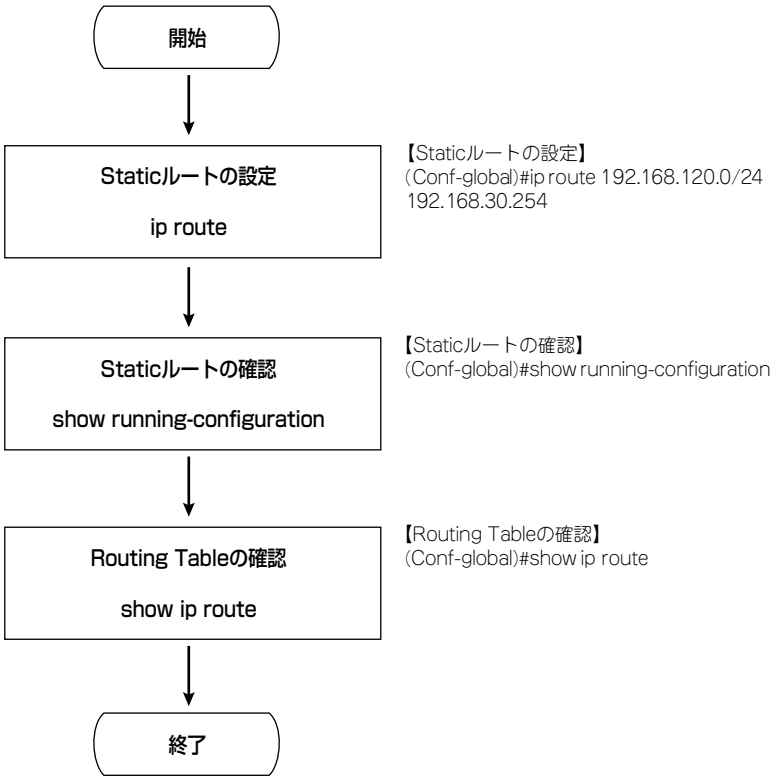
IPアドレステーブルからnumberedインタフェースのエントリを削除する場合は、no ip addressコマンドを使用してください。

```
(Conf-global)# interface vlan10
(Conf-if-vlan10)# no ip address
```

スタティックルートの登録

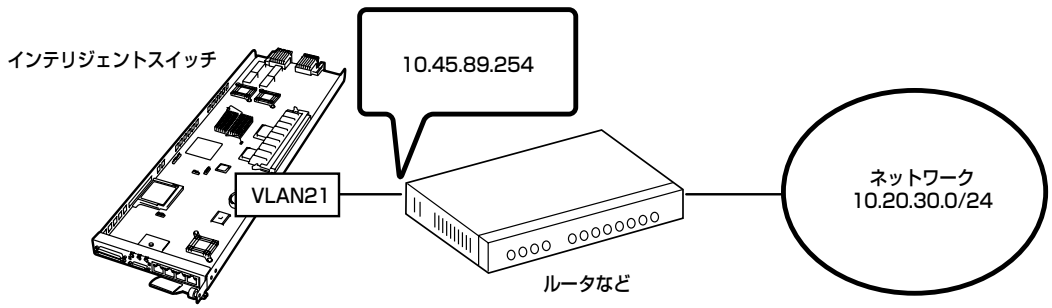
スタティックルーティングは、コマンドにより経路情報をあらかじめ装置へ設定し、ルーティングを行います。本装置では、ip routeコマンドで[対象ネットワークIPアドレス]と［サブネットマスク］に対して、最終到達先向けのインタフェース上の［ネクストホップIPアドレス］を設定することでルーティングテーブルが追加されます。

ルーティング機能を使用するためには、あらかじめ仮想インタフェースを定義し、その仮想インタフェースを内蔵ルータに接続しておく必要があります。スタティックルーティングの設定を行う前にIPアドレステーブルの確認をshow vlanコマンドで行ってください。



スタティックルートの設定

スタティックルートの設定は、宛先ネットワークのアドレスとサブネットマスクにNextHopのアドレスを指定し、設定します。



スタティックルーティングの設定例

```
(Conf-global)# ip route 10.20.30.0/24 10.45.89.254
```

デフォルトルートを登録する場合は、ネットワークアドレス・サブネットマスク共に0.0.0.0/0、もしくは文字列「default」を指定します。

スタティックルートの削除

ルーティングテーブルからスタティックルートエントリを削除する場合は、no ip routeコマンドを使用してください。

```
(Conf-global)# no ip route 10.20.30.0/24
```

スタティックルートの表示

スタティックルートを表示する場合は、show ip routeコマンドを使用してください。

```
(Conf-global)# show ip route
```

IPフィルタ

本装置のパケットフィルタは、装置の入口でパケット単位にフィルタリングを実行します。パケットフィルタを適用することで、本装置で受信するトラフィックに対してパケット単位に廃棄、許可の制御を行うことができます。パケットフィルタを適切に設定し、アクセスを制御することで、ネットワークのセキュリティを向上することができます。
本装置では、以下の組み合わせによるフィルタルールの設定が可能です。

フィルタ条件

- IPアドレス、またはすべてのIPアドレス
- プロトコルタイプ（Telnet/SSH/HTTP/HTTPS）

フィルタ動作

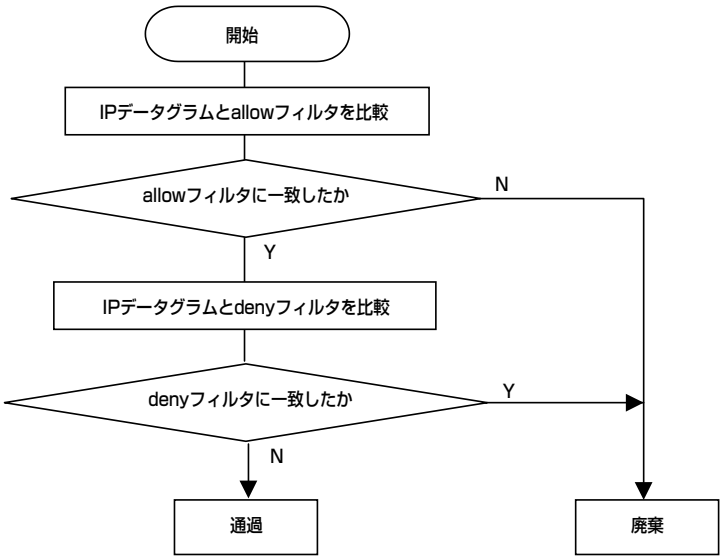
- 許可
- 廃棄

装置で登録できるIPフィルタの最大数は512です。

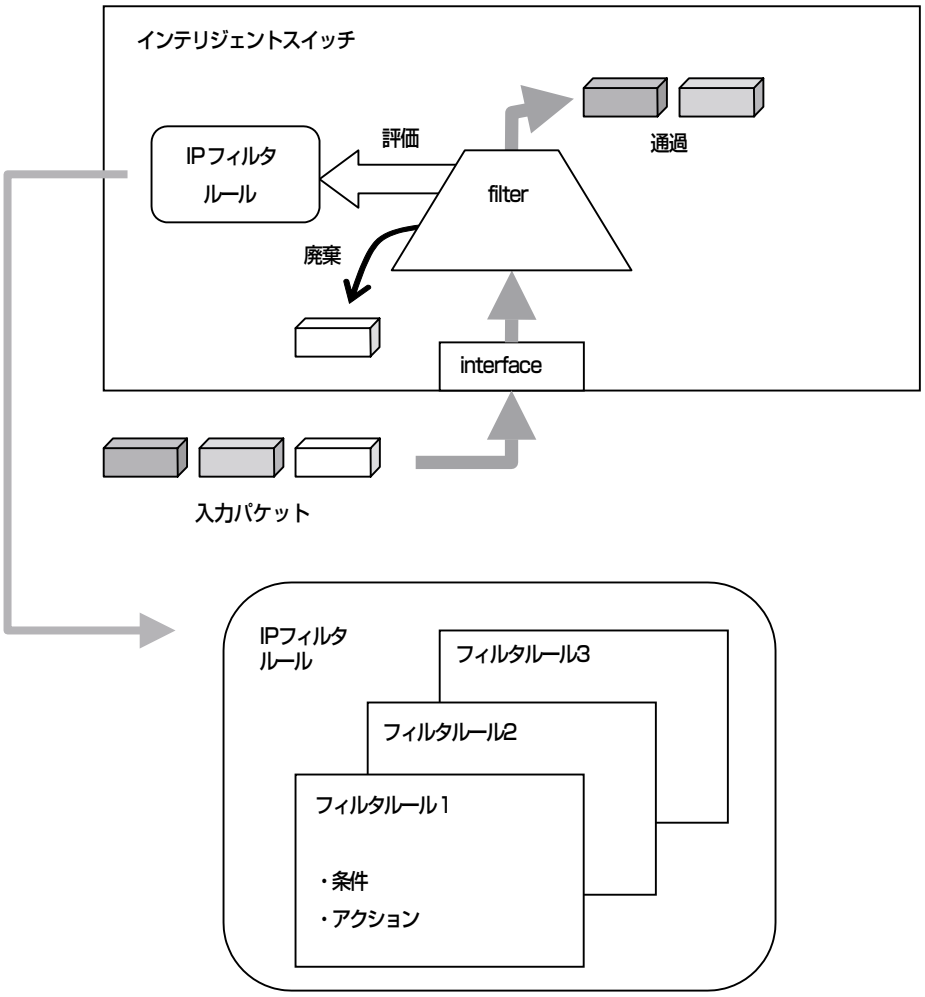
ヒント　工場出荷時の状態では、いずれのプロトコルにおいてもすべてのIPアドレスを許可するようにallow フィルタが設定されています。

基本動作

IPパケットフィルタは、下図のように入力時に評価されます。パケットを装置で受信したときにフィルタが適用されます。IPフィルタは、複数のフィルタにより構成できます。パケットは、IPフィルタルール内のシーケンス番号の小さいアクセスリストから順に評価されます。各フィルタルールは、一致条件、アクション(許可/廃棄)、から構成され、フィルタルールの一致条件に一致したパケットに対してアクション(許可あるいは廃棄)を行います。同じIPアドレスに対して許可と廃棄の両方が登録されている場合には廃棄のほうが優先されます。



IPフィルタの手順


インテリジェントスイッチ
IPフィルタ
ルール
評価
filter
通過
廃棄
interface
入力パケット
IPフィルタ
ルール
フィルタルール3
フィルタルール2
フィルタルール1
・条件
・アクション

IPフィルタ機能

IPフィルタの設定

IPアドレスを指定したフィルタの登録

IPフィルタの登録は、ip filterコマンドにより行います。フィルタの条件となるIPアドレスとプロトコル種別を設定し、フィルタアクションとしてallow（許可）、deny(廃棄)のいずれかを指定します。no ip filterコマンドにより登録IPフィルタを削除します。

```
(Conf-global)#ip filter 10.1.1.0/24 telnet allow
```

すべてのIPアドレスを対象とするフィルタの登録

すべてのIPアドレスを対象としてIPフィルタの登録を行うときは、IPアドレスの代わりにanyを指定します。

```
(Conf-global)#ip filter any ssh allow
```

IPフィルタの削除

IPフィルタを削除するときは、no ip filterコマンドを使用してください。

```
(Conf-global)#no ip filter 10.1.1.0/24 telnet allow
```

SSHサーバ

SSHサーバ機能は、通常のTelnetに代わり認証機能と通信の暗号化をともなったログイン機能を提供します。この機能を使用する事により、よりセキュアな方法で本装置へのログインを行うことができます。
本装置では次の2通りの認証方法を提供しています。

- パスワード認証
  - usernameコマンドにて指定したパスワードと照合する
  - Radiusクライアント機能によりRADIUSサーバ上に設定されているパスワードと照合する
- 公開鍵認証

  あらかじめクライアントの公開鍵を本装置に登録しておき、クライアントの秘密鍵とのペアで公開鍵認証を行う

本装置のSSHサーバはバージョン1、バージョン2の両方をサポートしています。また、SSHサーバはTCPの22番ポートを使用します。

- 特定のアドレスやネットワークからのアクセスを許可したり禁止したりしたい場合にはIPフィルタ機能を併用してください。IPフィルタ機能については前述の「IPフィルタ」（107ページ）を参照してください。
- 本装置のSSHサーバはOpenSSH（http://www.openssh.com/ja/）をベースに開発されています。

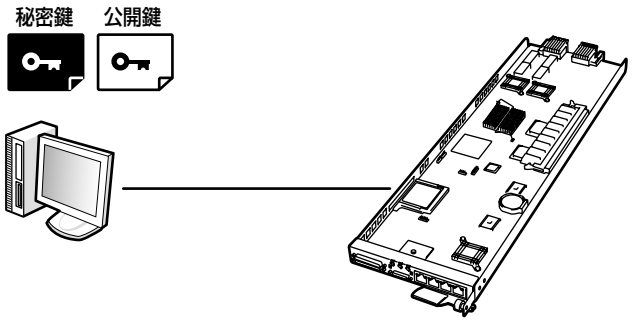
ホスト鍵の取り扱い

SSHサーバが動作するためには本装置上にホスト鍵が必要です。
SSHサーバは初回起動時に自動的にホスト鍵（鍵長は1024ビット）を生成し装置内のコンパクトフラッシュに格納します。通常はこれを変更する必要はありませんが、何らかの理由でホスト鍵を変更したい場合は、削除コマンドによりホスト鍵を削除し、SSHサーバを再起動する必要があります。
また、セキュリティのため秘密鍵は表示したり装置外へ転送したりすることができません。

クライアント公開鍵の取り扱い

本装置では、あらかじめクライアント側の公開鍵を登録しておくことにより公開鍵認証を行うことができます。ただし、公開鍵認証とRadiusクライアント機能を併用する事はできません。公開鍵認証は本装置にあるユーザー、つまり、初期状態で用意されているadmin、またはusernameコマンドにより登録されているユーザーに対してのみ使用できます。
以下にその流れを説明します。

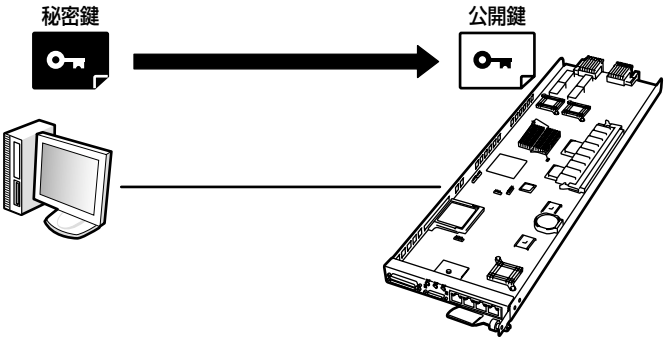
①　PC上でSSH用の公開鍵・秘密鍵を作成



鍵は以下の条件を満たす必要があります。

- SSHバージョン1のRSA認証、およびSSHバージョン2のRSA認証の鍵長は768ビット以上
- SSHバージョン2のDSA認証の鍵長は512ビット以上

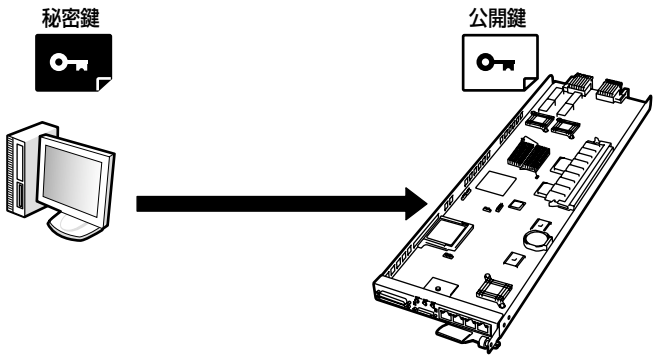
②　FTP/TFTPで公開鍵をPCから本装置上にダウンロード



クライアントの公開鍵は、装置内のコンパクトフラッシュに格納されます。SSHのバージョンおよび使用するユーザー名を指定する必要があります。

本装置上で登録されたユーザーごとに128個（バージョン1、バージョン2それぞれ）までのクライアント公開鍵を格納することができます。

③ SSHセッションの開始



②で指定したユーザー名を使用してSSH経由でログインします。

SSHサーバの設定

SSHサーバの有効化

SSHサーバを起動します。ホスト鍵がコンパクトフラッシュ上にない場合は自動的に作成されます。
最初のホスト鍵は初回起動時に作成されます。
工場出荷時の設定では本機能は有効となっています。

```
(Conf-global)# ssh-server enable
```

SSHサーバの無効化

SSHサーバを停止します。

```
(Conf-global)# no ssh-server enable
```

SSHサーバの設定を表示

SSHサーバが有効となっているかどうか、パスワード認証を許可するかどうかを表示することができます。

```
(Conf-global)# show running-configuration
```

FTPによるクライアント公開鍵のダウンロードおよび登録

クライアント公開鍵をリモートのFTPサーバから取得し、指定されたユーザー名、SSHのプロトコルバージョンに応じて装置に登録します。

```
(Conf-global)# copy ssh-client-cert ftp-server <REMOTE-
HOST> <FILENAME> <USERNAME> <PASSWORD> <username>
<version num>
```

例： IPアドレス1.1.1.1のFTPサーバからファイル名id_rsa.pubをダウンロードし(FTPサーバにログインするためのユーザー名はuser123、パスワードはpass123)、SSHバージョン2用の鍵として本装置上のadminの鍵ファイルにダウンロードしたファイルを追加します。

```
(Conf-global)# copy ssh-client-cert ftp-server 1.1.1.1
id rsa.pub user123 pass123 admin 2
```

TFTPによるクライアント公開鍵のダウンロードおよび登録

クライアント公開鍵をリモートのTFTPサーバから取得し、指定されたユーザー名、SSHのプロトコルバージョンに応じて装置に登録します。

```
(Conf-global)# copy ssh-client-cert tftp-server <REMOTE-
HOST> <FILENAME> <username> <version num>
```

ホスト鍵の表示

本装置上で作製されたホスト鍵のうち公開鍵を表示します。

```
(Exec)# show file content ssh-server-cert
```

秘密鍵を表示することはできません。

ホスト鍵の削除

ホスト鍵を（秘密鍵、公開鍵/バージョン1・2用すべて）削除します。ホスト鍵を再作成するためにはSSHサーバを再起動する必要があります。

```
(Conf-global)# no ssh-server enable
(Conf-global)# remove file ssh-server-cert
(Conf-global)# ssh-server enable
```

クライアント公開鍵の表示

装置に登録されているクライアント公開鍵に行番号をつけて表示します。

```
(Conf-global)# show file content ssh-client-cert <username>
<version num>
```

例： 本装置上のユーザー adminに対して登録されているSSHバージョン1の鍵をすべて表示します。

```
(Conf-global)# show file content ssh-client-cert admin 1
```

クライアント公開鍵の削除

INDEXにはshow file content ssh-client-certコマンドで表示される行番号を指定します。

INDEXを省略するとすべての鍵が削除されます。

```
(Conf-global)# remove file ssh-client-cert <username>
<version num> {<INDEX>}
```

例： 本装置上のユーザー adminに対して登録されているSSHバージョン1の鍵のうち、10行目の鍵を削除します。

```
(Conf-global)# remove file ssh-client-cert admin 1 10
```

パスワード認証の設定

RSA認証のみを使用するためパスワード認証を使用不可にしたい場合、次のコマンドでパスワード認証を禁止することができます。このコマンドはSSHサーバが停止している状態で行う必要があります。

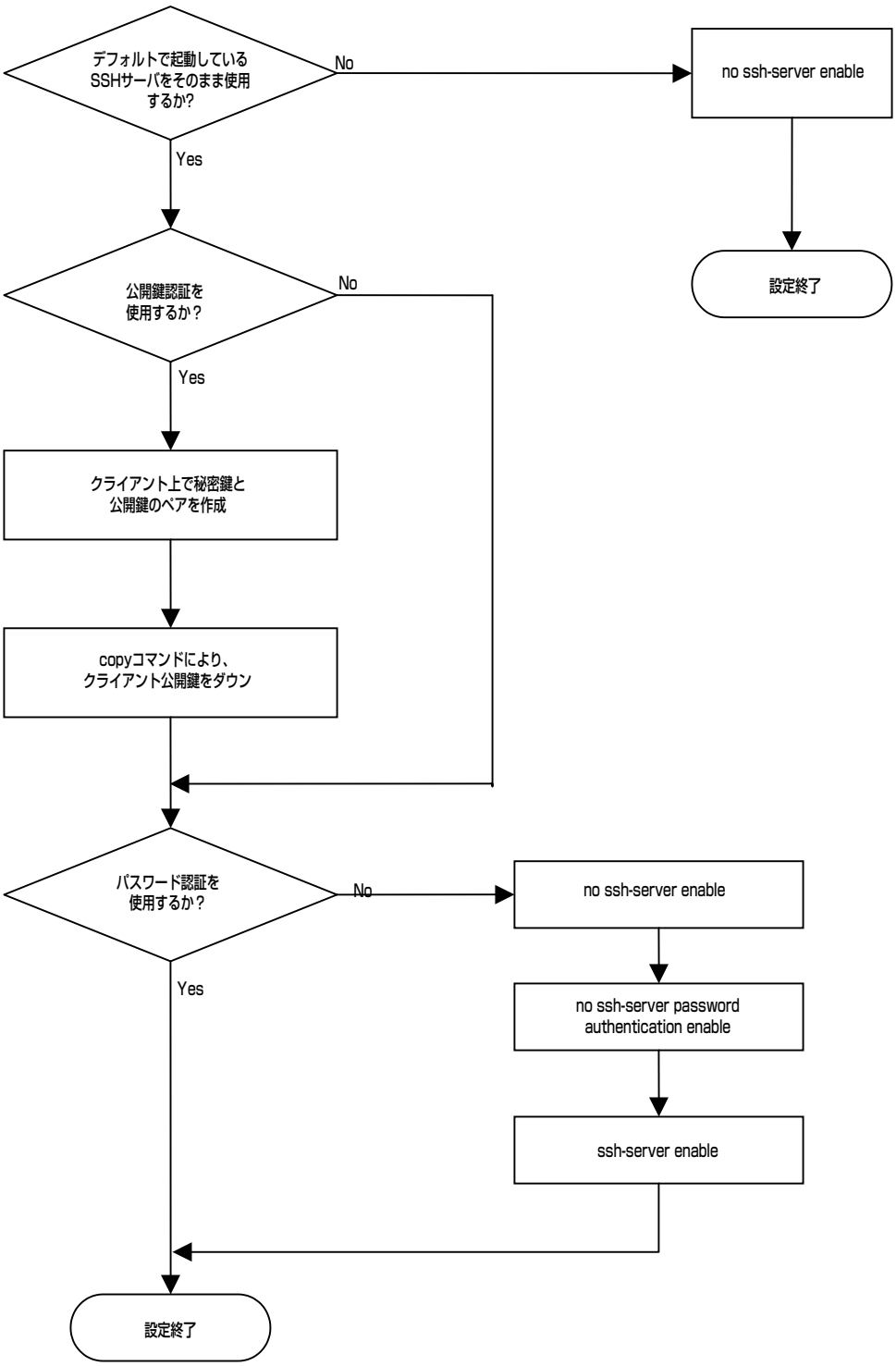
```
(Conf-global)# no ssh-server enable
(Conf-global)# no ssh-server password authentication enable
(Conf-global)# ssh-server enable
```

このコマンドにより使用不可になったパスワード認証を使用可能に戻したい場合は、以下のコマンドを使用してください。このコマンドもSSHサーバが停止している状態で行う必要があります。

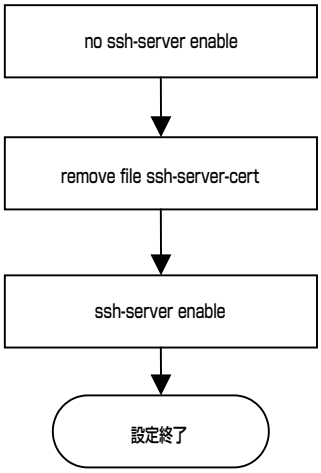
```
(Conf-global)# no ssh-server enable
(Conf-global)# ssh-server password authentication enable
(Conf-global)# ssh-server enable
```

SSHサーバ設定フローチャート

初期設定



ホスト鍵の再作成


no ssh-server enable
remove file ssh-server-cert
ssh-server enable
設定終了

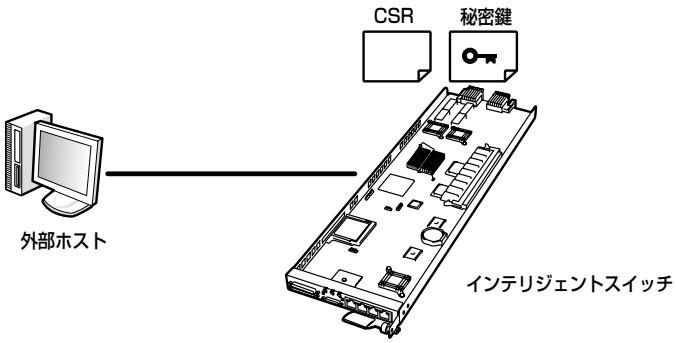
Webサーバ

本装置はWebサーバを搭載しており、本装置の設定の一部をWebブラウザを通して行うことができます。本章ではこのWebサーバ機能の設定方法について説明します。
本装置のWebサーバはHTTPとHTTPSの2つのプロトコルをサポートしています。HTTPSではSSLによりサーバが真正である事を証明し、また通信内容を暗号化して保護します。HTTPはTCPの80番ポートを、HTTPSはTCPの443番ポートをそれぞれ使用します。
特定のアドレスやネットワークからのアクセスを許可したり禁止したりしたい場合にはIPフィルタ機能を併用してください。IPフィルタ機能については前述の「IPフィルタ」を参照してください。

サーバ証明書の取り扱い

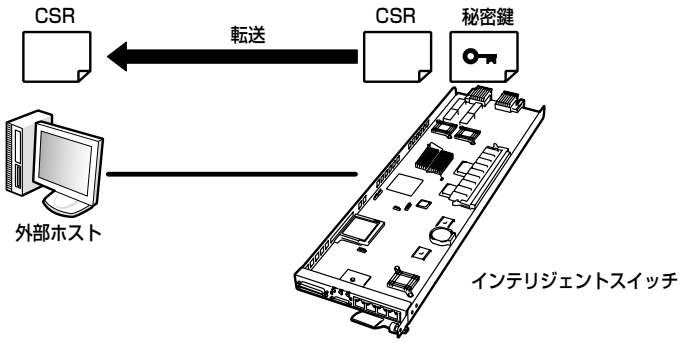
HTTPSを使用する場合、署名済みのサーバ証明書が必要となります。署名済みのサーバ証明書を装置に登録するまでには以下の手順を実行する必要があります。

①　秘密鍵・証明書署名要求の作成



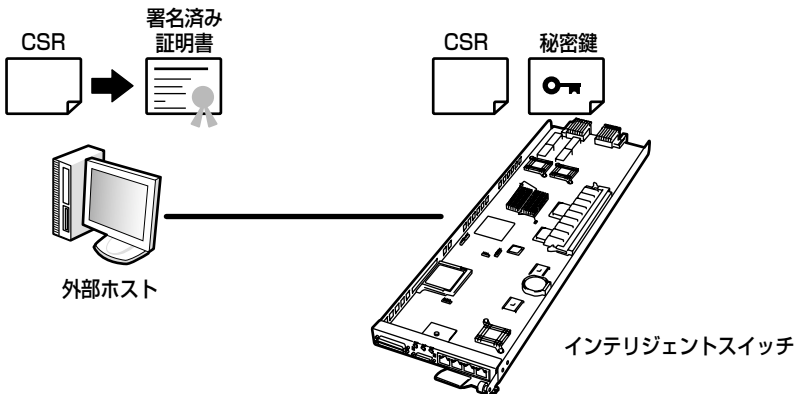
CLIからhttps-server generate-new-certificateコマンドを実行し、秘密鍵および証明書署名要求（CSR・Certificate Signing Request）のペアを本装置上で作成します。作成された秘密鍵および証明書署名要求は本装置内のコンパクトフラッシュ上に格納されます。秘密鍵の鍵長は1024ビット、発行されるCSRはPKCS#10形式となります。

②　証明書署名要求を外部ホストに転送



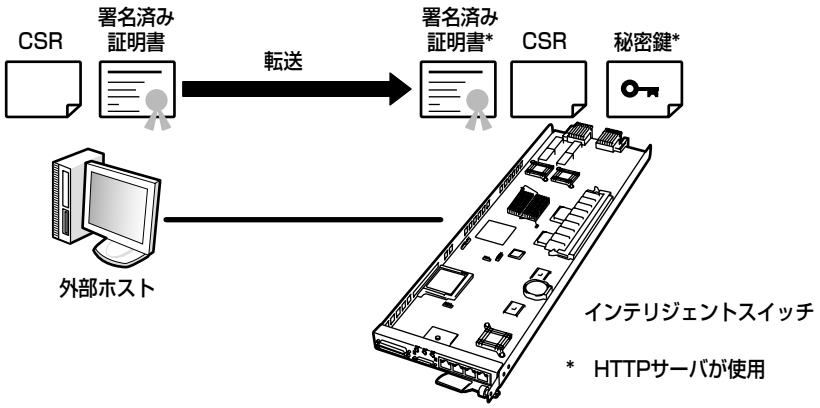
copyコマンドによりCSRを外部ホストに転送します。ここでcopyコマンドを使用せず、telnet/sshで本装置に接続し、showコマンドでCSRの内容を表示してコピー＆ペーストを行ってもかまいません。

③ 外部認証局あるいは独自認証局により署名



署名されたサーバ証明書が作成されます。署名の方法につきましては、外部認証局の場合は認証局に、独自認証局の場合は使用している認証ツールの説明書を確認してください。

④ 署名済み証明書を本装置に転送



外部ホストから署名済みのサーバ証明書を本装置に転送し、コンパクトフラッシュ上に格納します。これにより署名済みのサーバ証明書と秘密鍵のペアが装置上に用意され、HTTPSサーバが起動できる準備が整いました。
本装置は複数の秘密鍵・証明書署名要求・署名済み証明書をコンパクトフラッシュに格納することはできません。同時にコンパクトフラッシュに格納できるのはそれぞれ1種類ずつとなります。

HTTP/HTTPSサーバの設定

HTTPサーバの有効化

HTTPサーバを起動します。工場出荷時には本機能は有効となっています。

```
(Conf-global)# http-server enable
```

HTTPサーバの無効化

HTTPサーバを終了します。

```
(Conf-global)# no http-server enable
```

HTTPSサーバの有効化

HTTPSサーバを起動します。署名済み証明書がない場合はエラーとなり、HTTPSサーバは起動しません。工場出荷時には本機能は無効となっています。

```
(Conf-global)# https-server enable
```

HTTPSサーバの無効化

HTTPSサーバを終了します。

```
(Conf-global)# no https-server enable
```

HTTP/HTTPSサーバの設定の表示

HTTP/HTTPSサーバそれぞれが有効になっているかどうかを表示します。

HTTPサーバはデフォルトで有効になっているため、無効の場合のみ本コマンドの出力に表示されます。一方HTTPSサーバはデフォルトで無効になっているため、有効の場合のみ本コマンドの出力に表示されます。

```
(Conf-global)# show running-configuration
```

秘密鍵・証明書署名要求の作成

本装置内でHTTPSサーバ用の秘密鍵と証明書署名要求が新規に作成され、コンパクトフラッシュ内に格納されます。

```
(Conf-global)# https-server generate-new-cert
```

すでに作成済みの秘密鍵・証明書署名要求・署名済み証明書がコンパクトフラッシュ内にある場合は確認メッセージが表示されます。

```
Warning: Current private key, csr and signed certificate will
be deleted. Proceed? [Y/N]
```

ここで<Y>キーを押して、<Enter>キーを押すと作成済みの秘密鍵・署名済みの証明書・証明書署名要求は削除され、新たな秘密鍵・署名済みの証明書・証明書署名要求が格納されます。

また、Webサーバに関する情報を求められますので、以下の要領で入力します。

例：

```
(Conf-global)# https-server generate-new-certificate
Warning: Current private key, csr and signed certificate
will be deleted. Proceed? [Y/N]
Y[Enter]

Using configuration from /etc/openssl/openssl.cnf
You are about to be asked to enter information that will be
incorporated
into your certificate request.
What you are about to enter is what is called a
Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [JP]: JP ---------------------①
State or Province Name (full name) []: Tokyo -------------②
Locality Name (eg, city) []: Minato-ku --------------------③
Organization Name (eg, company) []: NEC Corporation -------④
Organizational Unit Name (eg, section) []: Sales Unit -----⑤
Common Name (eg, YOUR name) []: www.nec.co.jp -------------⑥
Email Address []:------------------------------------------ ⑦

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []: ----------------------------------⑦
An optional company name []: ------------------------------⑦
```

① 国名（JP）を入力。
② 都道府県名をローマ字で入力。
③ 市町村名をローマ字で入力。
④ 団体名（通常はドメイン名の所有者）を入力。
⑤ 部署名を入力。
⑥ WebサーバのURLを入力。
⑦ 通常は入力不要です（<Enter>キーを押してください）。

必要な入力項目は認証局によって異なる場合があります。

証明書署名要求のFTPによるアップロード

csrファイルをftpにより外部のマシンへアップロードします。外部のマシンではFTPサーバが動作している必要があります。

```
(Conf-global)# copy https-server-cert flash csr ftp-server
<REMOTE-HOST> <USERNAME> <PASSWORD> [filename <FILENAME>]
```

例： コンパクトフラッシュ内のCSRを、FTPを利用してIPアドレス1.1.1.1のFTPサーバに、ユーザー名「user123」、パスワード「pass123」を使用してログインし、FTPサーバ上でのファイル名をcsrとして転送する場合。

```
(Conf-global)# copy https-server-cert flash csr ftp-server
1.1.1.1 user123 pass123 csr
```

証明書署名要求のTFTPによるアップロード

csrファイルをtftpにより外部のマシンへアップロードします。外部のマシンではTFTPサーバが動作している必要があります。使用方法はFTPの場合を参考にしてください。

```
(Conf-global)# copy https-server-cert flash csr tftp-server
<REMOTE-HOST> <FILENAME>
```

署名済み証明書のFTPによるダウンロード

署名済みの証明書をFTPを利用して本装置内にダウンロードします。ダウンロードした証明書はコンパクトフラッシュ内に格納されます。外部のマシンではFTPサーバが動作している必要があります。

```
(Conf-global)# copy https-server-cert ftp-server <REMOTE-
HOST> <USERNAME> <PASSWORD> <FILENAME> flash certificate
```

例： リモートのIPアドレス1.1.1.1のFTPサーバにユーザー名「user123」、パスワード「pass123」を使用してログインし、ファイル名「signed_cert」をFTPによりダウンロードし、署名済み証明書として本装置のコンパクトフラッシュに格納する場合。

```
(Conf-global)# copy https-server-cert ftp-server 1.1.1.1
user123 pass123 signed cert flash certificate
```

署名済み証明書のTFTPによるダウンロード

署名済みの証明書をTFTPを利用して本装置内にダウンロードします。ダウンロードした証明書はコンパクトフラッシュ内に格納されます。外部のマシンではTFTPサーバが動作している必要があります。使用方法はFTPの場合を参考にしてください。

```
(Conf-global)# copy https-server-cert tftp-server <REMOTE-
HOST> <FILENAME> flash certificate
```

秘密鍵・証明書署名要求・署名済み証明書の表示

コンパクトフラッシュに格納されている秘密鍵・証明書署名要求・署名済み証明書の内容を表示します。パラメータを省略した場合は、3種類すべて表示されます。

```
(Exec)# show https-server-cert [{private-
key|csr|certificate}]
```

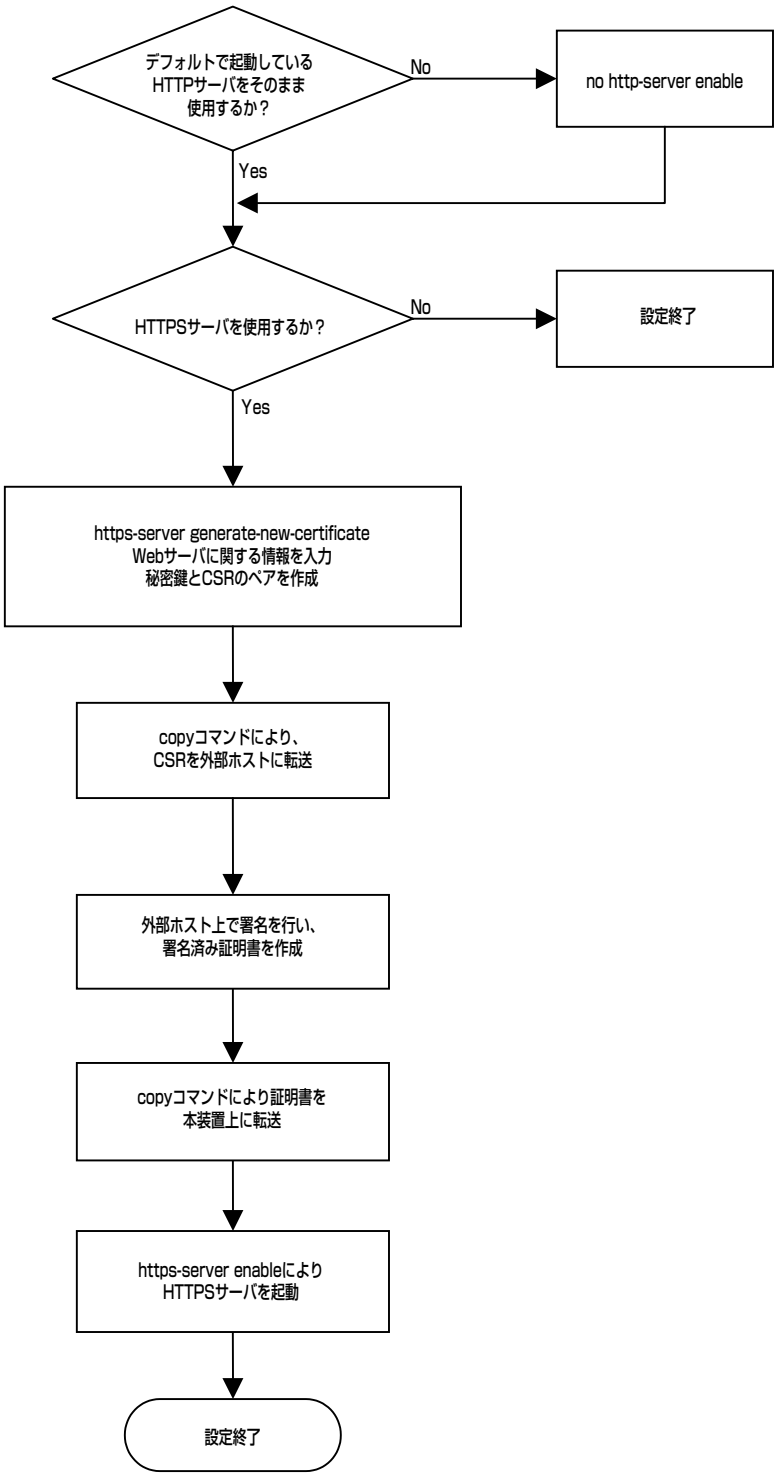
秘密鍵・証明書署名要求・署名済み証明書の削除

コンパクトフラッシュに格納されている秘密鍵・証明書署名要求・署名済み証明書を削除します。

パラメータを省略した場合は、3種類すべて削除されます。

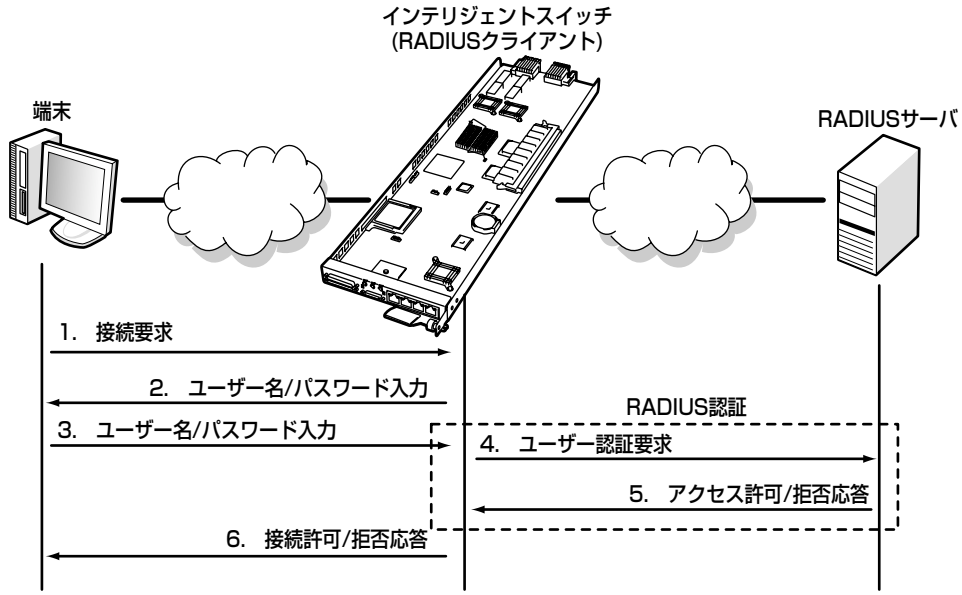
```
(Exec)# remove file https-server-cert [{private-
key|csr|certificate}]
```

Webサーバ設定フローチャート



RADIUSクライアント

RADIUSは、ネットワーク装置のユーザー認証を提供するプロトコルです。構成要素は、ユーザー認証を要求する RADIUSクライアントと、ユーザー認証データベースを持つRADIUSサーバに分類されます。本装置は RADIUSクライアントとして動作し、telnetやコンソール経由で本装置にログインするユーザーの認証を外部のRADIUSサーバに要求する機能を提供します。



RADIUSサーバの登録

RADIUS認証に使用する外部のRADIUSサーバを登録する場合は、グローバルコンフィグレーションモードでradius-serverコマンドを使用してください。第2パラメータはRADIUSサーバに登録してあるパスワードですので、サーバ側と同様の文字列を設定してください。本装置に登録できるRADIUSサーバの最大数は8です。

省略可能なパラメータを省略した場合、認証要求のタイムアウト時間は1秒、リトライ回数は4回、使用UDPポート番号は1812、アクセスを許可したユーザーのユーザー権限はmonitorになります。工場出荷時の状態では、RADIUSサーバは登録されていません。

```
(Conf-global)# radius-server 10.40.20.48 secret
```

登録済みRADIUSサーバの表示

登録したRADIUSサーバを表示する場合は、show radius-serverコマンドを使用してください。

```
(Conf-global)# show radius-server 10.40.20.48
```

登録済みRADIUSサーバの削除

登録したRADIUSサーバを削除する場合は、グローバルコンフィグレーションモードでno radius-serverコマンドを使用してください。

```
(Conf-global)# no radius-server 10.40.20.48
```

装置ログイン時の認証方式および優先度の設定

RADIUS認証を有効にする場合は、グローバルコンフィグレーションモードでaaa authentication login defaultコマンドを使用してください。第1パラメータ、第2パラメータの順に認証を試行します。radius-serverコマンドで複数のRADIUSサーバを登録した場合、その登録順にユーザー認証要求を送信します。RADIUSサーバからアクセス拒否が返ってきた場合、以降の認証は行いません。工場出荷時の状態では、local認証のみが有効に設定されています。なお、RADIUS認証のみを有効とすることはできません。必ずlocal認証を組み合わせて設定してください。

```
(Conf-global)# aaa authentication login default radius
local
```

装置ログイン時の認証方式および優先度の表示

装置ログイン時の認証方式と優先度の情報を表示する場合は、show aaaコマンドを使用してください。

```
(Conf-global)# show aaa
```

RADIUS認証統計情報の表示

RADIUS認証の統計情報を表示する場合は、show radius statisticsコマンドを使用してください。

```
(Conf-global)# show radius statistics 10.40.20.48
```

RADIUS認証統計情報の初期化

RADIUS認証の統計情報を初期化する場合は、clear radius statisticsコマンドを使用してください。

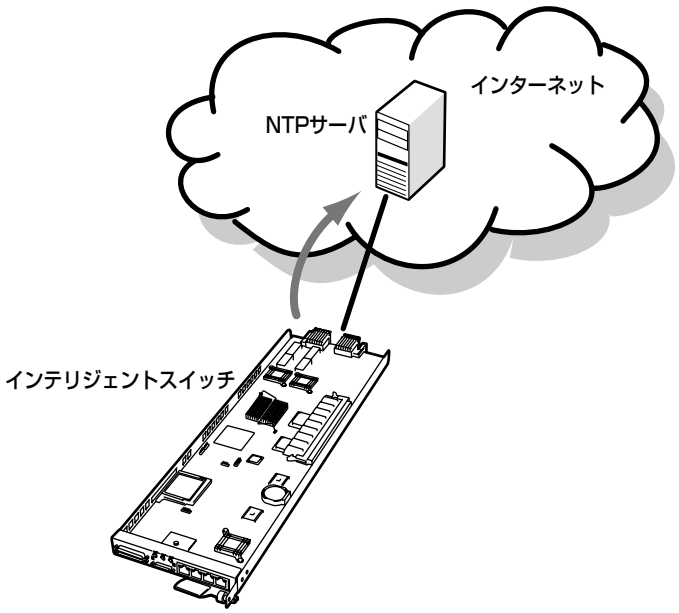
```
(Exec)# clear radius statistics
```

NTP

NTP（Network Time Protocol: RFC1305）機能は、ネットワークに接続された機器間の時刻同期を行うための機能です。NTPは、ネットワークの階層化や、ネットワーク通信の遅延情報等も考慮しているプロトコルのため、非常に高い精度で効率の良い時刻同期が可能です。
本装置は、NTPクライアントとしてのみ動作します。

基本動作

NTPを使ったネットワークでは､基準となる時刻情報を提供するNTPサーバをネットワーク上に複数台用意して､それを基に他のクライアントが時刻を同期させることによって、ネットワーク上の機器が同じ時刻を刻むようにすることができます。
NTPサーバは階層的に構築することができ、最上位のサーバをStratum1のNTPサーバと呼び、これがネットワーク内の機器の基準時刻を提供します。Stratum1のNTPサーバから時刻を取得するNTPサーバをStratum2のNTPサーバと呼びます。このようなNTPサーバの階層を最大15層（Stratum15）まで構築可能です。また、同一階層にNTPサーバを複数台設置することができ、これをPeerと呼びます。
NTPサーバは、他のNTPサーバと通信し時刻同期を行いますが、この際に、その通信時間やばらつき状況を考慮して、時刻精度が低い（応答遅延が大きい等）と判断した場合、時刻同期の頻度を上げるなどして、できるだけ高い精度で時刻が同期できるしくみを持っています。



NTPサーバの設定

NTPサーバの登録を行うときには、グローバルモードでntp serverコマンドを使用して時刻同期を行うNTPサーバを指定します。

```
(Conf-global)# ntp server 10.4.3.223 version 3 key 10
source-interface vlan1 prefer
```

NTPサーバの表示

NTPの状態を表示する場合は、show ntp statusコマンドを使用してください。

```
(Conf-global)# show ntp status
```

システム時刻の表示

システムの時刻を表示する場合は、show clockコマンドを使用してください。

```
(Conf-global)# show clock
```

受信レート制限

受信レート制限機能は、高レートの「ブロードキャスト」・「マルチキャスト」・「あて先不明パケットのフラッディング」を受信ポートで検知しこれを破棄することにより、本装置のCPU負荷およびネットワーク負荷の抑制を行う機能です。本機能は物理ポートごとに、「ブロードキャスト」・「マルチキャスト」・「あて先不明パケットのフラッディング」をそれぞれ異なるレートを設定できます。

受信レート制限の登録

受信レート制限設定を登録する場合は、ポートコンフィグレーションモードでrx-ratelimitコマンドを使用してください。設定を超過するパケットの受信を検知した場合、破棄を行います。単位は[pps]です。工場出荷時の状態では、broadcastとfloodに、それぞれ10000[pps]の受信レート制限が設定してあります。本設定を解除すると、予期せぬ大きなブロードキャスト負荷等で装置の動作が不安定になる場合がありますので、本設定の解除は極力避けてください。

```
(Conf-pt-lan1)# rx-ratelimit broadcast 500 flood 400
```

受信レート制限の表示

登録した受信レート制限設定を表示する場合は、show rx-ratelimitコマンドを使用してください。

```
(Conf-pt-lan1)# show rx-ratelimit
```

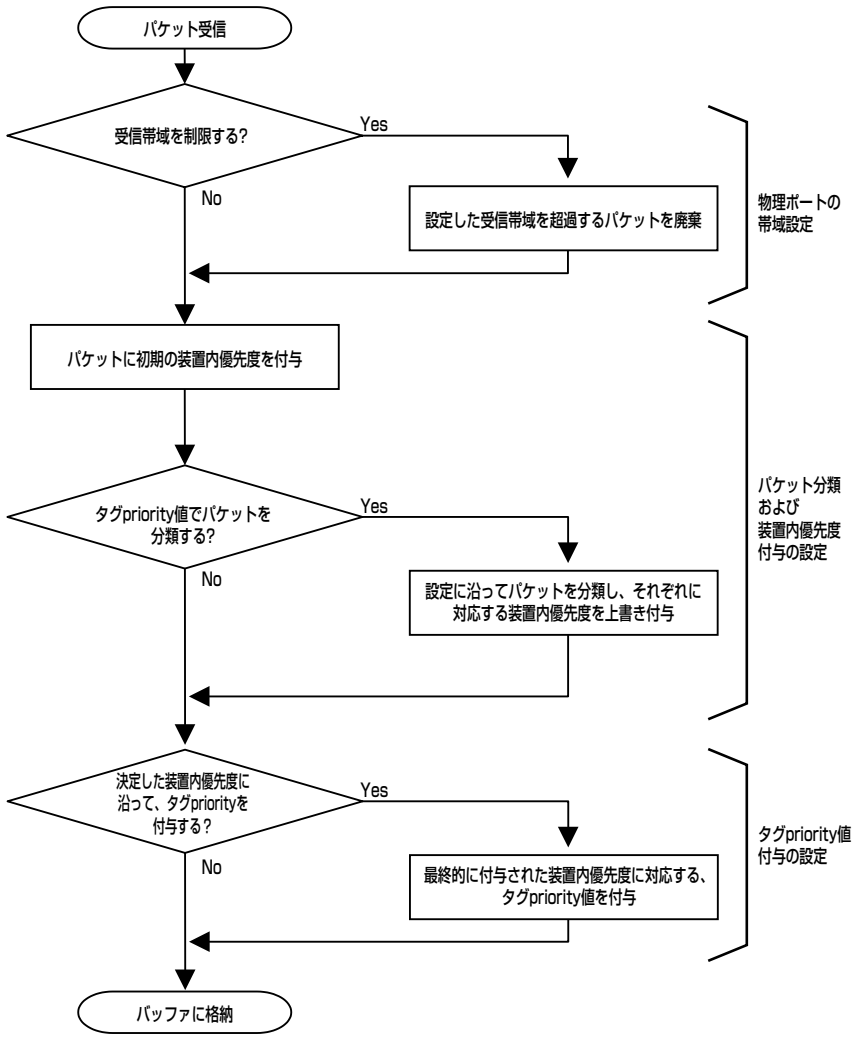
受信レート制限の削除

登録した 受信レート制限を削除する場合は、ポートコンフィグレーションモードでno rx-ratelimitコマンドを使用してください。

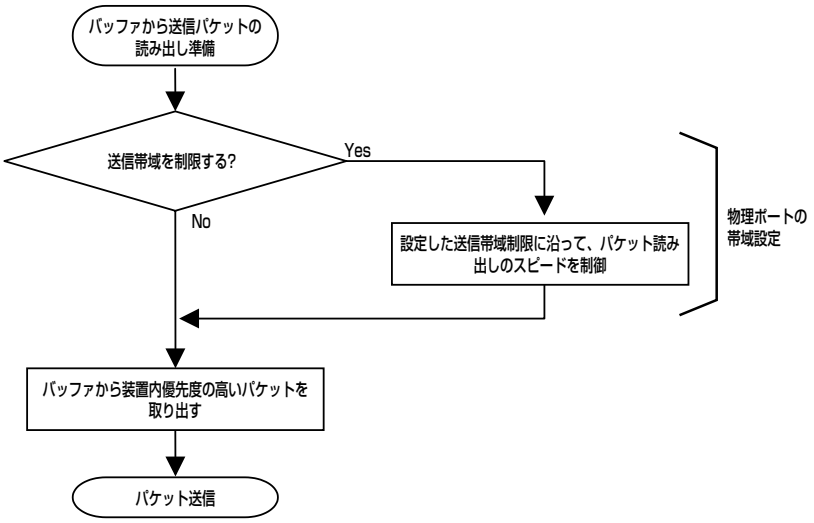
```
(Conf-pt-lan1)# no rx-ratelimit
```

QoS機能

QoSはQuality of Serviceの略語で、回線から受信したパケットを分類することで、回線が輻輳した状態でも重要なパケットを優先的に送信する技術です。本装置では、受信ポート、タグヘッダ内のpriority値を受信パケットの分類に用い、ユーザが指定する装置内優先度を付与します。なお、その装置内優先度に応じてタグヘッダ内のpriority値をパケットに付与することもできます。また、物理回線の受信帯域および送信帯域を設定することもできます。



QoS動作概要（受信側）



QoS動作概要（送信側）

QoSの設定

QoSの有効化

QoSを有効化する場合は、ポートコンフィグレーションモードでqos enableコマンドを使用してください。QoSが無効の状態でも、CLIコマンドによるQoSパラメータの設定が可能です。QoSを有効化した際に、すべてのQoSパラメータの設定が反映されます。
工場出荷時の状態では、QoSは無効になっています。

```
(Conf-pt-lan1)# qos enable
```

QoSの無効化

QoSを無効化する場合は、ポートコンフィグレーションモードでno qos enableコマンドを使用してください。QoSを無効にしても、すでに設定済みのQoSパラメータは保持され、再びQoSを有効化したときに設定が復元されます。

```
(Conf-pt-lan1)# no qos enable
```

設定済みQoSパラメータの表示

設定済みQoSパラメータを表示する場合は、show qosコマンドを使用してください。
パラメータを省略すると、すべてのポートにおける設定を表示します。

```
(Conf)# show qos lan1
```

物理ポートの帯域設定

物理ポートの受信帯域設定

物理ポートにおける受信帯域を設定する場合は、ポートコンフィグレーションモードでqos rx-bandwidthコマンドを使用してください。単位は[Mbps]です。
工場出荷時の状態では、設定されていません。

```
(Conf-pt-lan1)# qos rx-bandwidth 300
```

物理ポートの受信帯域設定解除

物理ポートにおける受信帯域設定を解除する場合は、ポートコンフィグレーションモードでno qos rx-bandwidthコマンドを使用してください。

```
(Conf-pt-lan1)# no qos rx-bandwidth
```

物理ポートの送信帯域設定

物理ポートにおける送信帯域を設定する場合は、ポートコンフィグレーションモードでqos tx-bandwidthコマンドを使用してください。単位は[Mbps]です。
工場出荷時の状態では、設定されていません。

```
(Conf-pt-lan1)# qos tx-bandwidth 500
```

物理ポートの送信帯域設定解除

物理ポートにおける送信帯域設定を解除する場合は、ポートコンフィグレーションモードでno qos tx-bandwidthコマンドを使用してください。

```
(Conf-pt-lan1)# no qos tx-bandwidth
```

パケット分類および装置内優先度付与の設定

受信ポートにおける初期の装置内優先度設定

受信ポートにおける入力パケットの初期の装置内優先度を設定する場合は、ポートコンフィグレーションモードでqos default-cosコマンドを使用してください。
工場出荷時の状態では、装置内優先度が0に設定されています。

```
(Conf-pt-lan1)# qos default-cos 3
```

受信ポートにおける初期の装置内優先度設定の初期化

受信ポートにおける入力パケットの初期の装置内優先度設定を初期化する場合は、ポートコンフィグレーションモードでno qos default-cosコマンドを使用してください。

```
(Conf-pt-lan1)# no qos default-cos
```

受信パケットのタグpriority値設定

受信ポートにおける入力パケットの分類方法を設定する場合は、ポートコンフィグレーションモードでqos trustコマンドを使用してください。
工場出荷時の状態では、設定されていません。

```
(Conf-pt-lan1)# qos trust dot1p
```

受信パケットのタグpriority値設定の解除

受信ポートにおける入力パケットの分類設定を解除する場合は、ポートコンフィグレーションモードでno qos trustコマンドを使用してください。

```
(Conf-pt-lan1)# no qos trust
```

受信パケットのタグpriority値→優先度 マッピング設定

入力パケットのタグpriority値と、装置内優先度との対応付けを行う場合は、ポートコンフィグレーションモードでqos trust-mapコマンドを使用してください。尚、実際に有効になるのはqos trustコマンドで選択した分類方法に対応するマッピングパターンです。
工場出荷時の状態では、タグpriority値0～7が、それぞれ装置内優先度の0～7に設定されています。

```
(Conf-pt-lan1)# qos trust-map dot1p 7 5
```

受信パケットのタグpriority値→優先度マッピング設定の初期化

入力パケットのタグpriority値、装置内優先度との対応付けを初期化する場合は、ポートコンフィグレーションモードでno qos trust-mapコマンドを使用してください。

```
(Conf-pt-lan1)# no qos trust-map dot1p
```

タグpriority値付与の設定

受信パケットのタグpriority値付与設定

受信ポートにおいて付与された装置内優先度に応じて、入力パケットのタグpriority値の付与を行う場合は、ポートコンフィグレーションモードでno qos overrideコマンドを使用してください。タグpriority値の付与はタグフレームによる通信に対して実行されます。
工場出荷時の状態では、設定されていません。

```
(Conf-pt-lan1)# qos override dot1p
```

受信パケットのタグpriority値付与設定の解除

受信ポートにおける入力パケットのタグpriority値の付与を解除する場合は、ポートコンフィグレーションモードでqos overrideコマンドを使用してください。

```
(Conf-pt-lan1)#no qos override
```

Webインタフェースを使った設定

ブラウザを使用したWebインタフェースによる設定では以下のことができます。

- 本装置のBMCコンフィグレーション
- 本装置のBMCファームウェア/SDRのアップデート
- CPUブレードの電源制御
- リモートKVM（キーボード・ビデオ・マウス）コンソール機能(MNGポートからのみ)

管理PC側の設定

ここではWebブラウザを使用したWebインタフェース機能を使用する場合にクライアントPC側で考慮しなければならない内容について説明します。

ブラウザの設定

以下の設定を行ってください。

- SSLを有効にしてください。
- Cookieを有効にしてください。
- JavaScriptを有効にしてください。

動作対応ブラウザ

以下のブラウザについて、動作を確認しております。

- Microsoft Internet Explorer 6.0
- Netscape 7.0
- Mozilla 1.6

Java2 Runtime Environment

Java2 Runtime Environment, Standard Edition 1.4.2_04以降が必要です。以下の場所よりダウンロードできます。

http://java.sun.com/j2se/

未インストールでログインページにアクセスすると、右のようなメッセージが表示される場合があります。内容を確認して、実行してください。

ビデオドライバの組み込み（ブレード本体装置のOSがLinuxの場合）

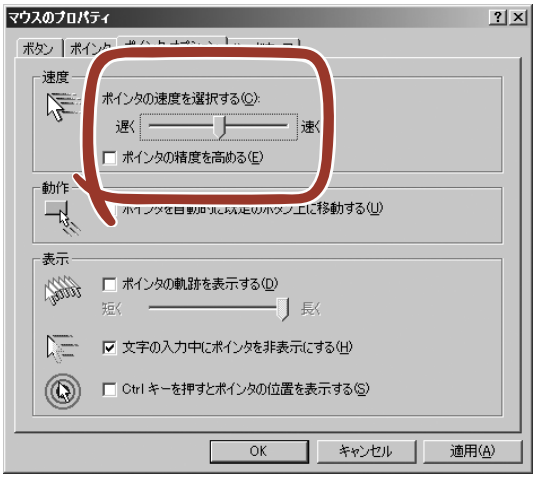
チェック

Linuxの場合、構成により自動でモニタ/Driver/ビデオメモリの設定が反映されない場合がありますので、テキストモードでの運用をお勧めします。

Linuxの対応については、『8番街』：http://nec8.com/の「Linux on Express5800」から最新/詳細情報を入手してください。

マウスのプロパティの変更

本体装置のOSがWindows Server 2003 の場合、下記に示す「マウスのプロパティ」の「ポインタオプション」にあります「速度」の設定で、「ポインタの精度を高める」のチェックボックスを外してください。
また、リモートKVMコンソールにて、マウスカーソルが画面右下まで動かせないときは、ここの「ポインタの速度を選択する」を調節してください。



Webサーバへの接続

Webブラウザからデフォルト設定では以下のURLにアクセスしてください。なお、本装置の取り付けられたスロットでアクセスするURLが異なります。

- N8406-005A/スロット7 または N8406-006A/スロット21

  URL: http://192.168.58.1/index.html

- N8406-005A/スロット8 または N8406-006A/スロット22

  URL: http://192.168.58.2/index.html

192.168.58.1/2はip addressコマンドで変更可能な、マネージメントポートを収容するVLAN4094に対してのIPアドレスです。ip addressコマンドについては 本書の244ページを参照ください。

Webブラウザの以下の項目を有効にしてアクセスしてください。
- Cookie
- JavaScript

ログイン

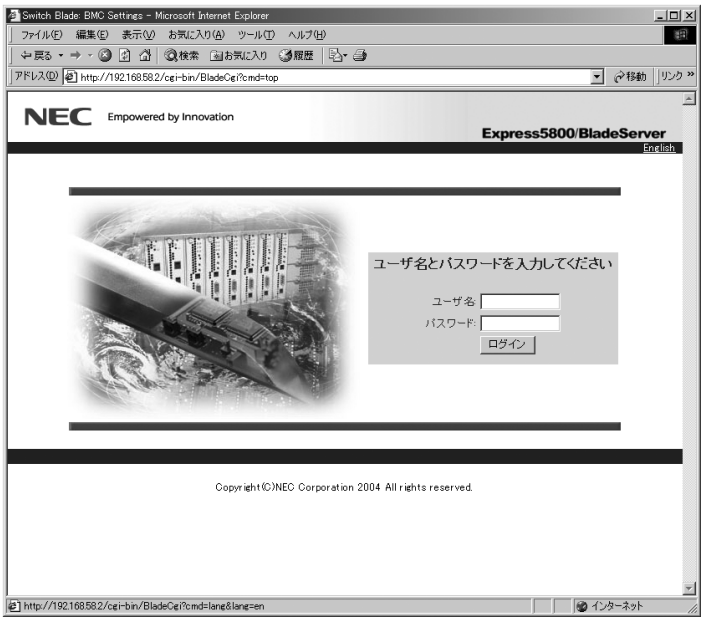
上記のアドレスへアクセスするとログインページが表示されます。
ユーザー名/パスワードを入力し、[ログイン]をクリックしてください。

重要

Webインタフェースによる設定をする前にCLIで接続しているクライアントをすべて切り離してください。

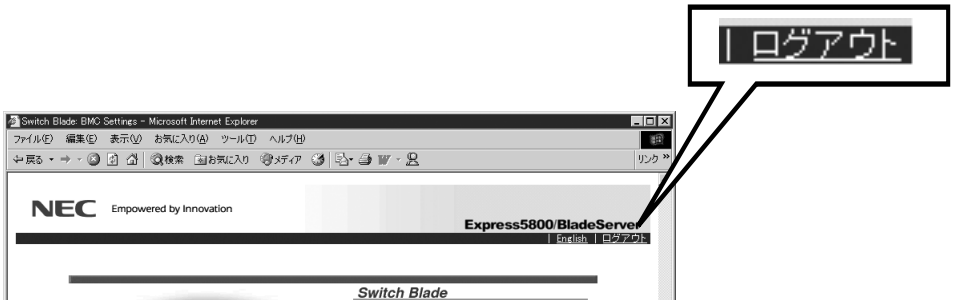
ヒント

- Webインターフェースからログイン可能なユーザーは usernameコマンドのuser-interfaceオプションにより「web」または「all」に設定されたユーザーのみです。各ユーザーの設定はshow running-configurationコマンドで確認できます。
  デフォルトではユーザー「admin」は「all」に設定されています。
- ユーザー名/パスワードに関しては、3章の「ログインとユーザー権限」（40ページ）を参照してください。



ログアウト

右上のリンク[ログアウト]をクリックすることでログアウトできます。
ログアウトすると、ログインページに戻ります。

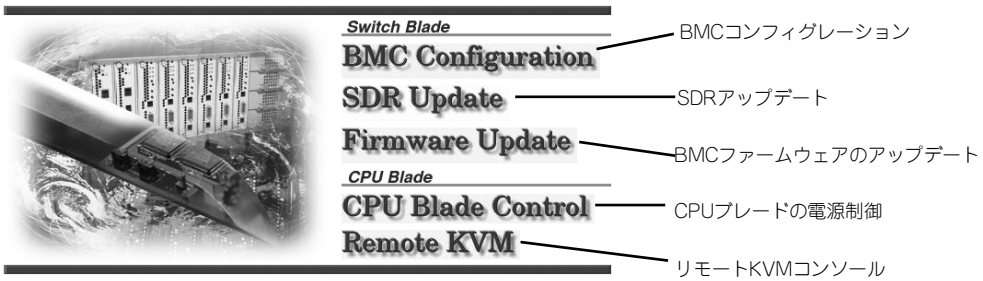


言語切り替え

デフォルトでは英語モードが表示されます。
右上のリンク[Japanese]をクリックすることで、日本語モードに切り替えることが可能です。また、日本語モードから英語モードへ切り替えるには[English]をクリックしてください。

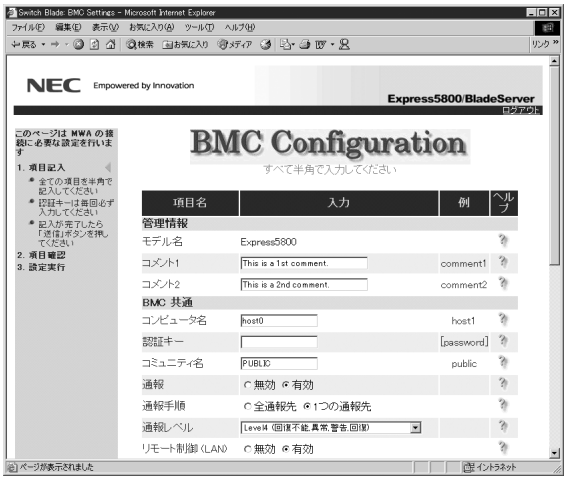
項目の選択

ログインに成功すると、Topページとして以下のメニューが表示されます。
メニューは以下の5種類です。



BMCコンフィグレーション（BMC Configuration）

Topページで[BMC Configuration]をクリックすることで、BMCコンフィグレーションページにジャンプします。
このページでは、本装置とDianaScope^{TM}の接続に必要な設定を行います。またBMCの「リモートKVMコンソール（Remote KVM）」（148ページ）を利用する場合にも設定が必要となります。
ページの左部分に簡単な説明・注意事項が表示されています。参照してください。



Webサーバ機能を使用してBMCコンフィグレーションの設定を行う場合は以下の手順に従います。

1. 項目記入

   このページでは、BMCに設定する値を記入します。

   現在BMCに設定されている値が、各項目のデフォルトとして表示されます。ただし、IPアドレスとサブネットマスクは本装置のマネージメントポートを収容するVLANに設定されている値が表示されます。また、パスワードは空欄となっていますので、必ず入力してください。変更したい部分を書き換えて、[送信]をクリックしてください。

2. 項目確認

このページでは、記入内容の確認を行います。

記入した内容が表示されます。内容に誤りがなければ[登録]をクリックしてください。修正を行いたい場合は、ブラウザの[戻る]で項目記入ページに戻り、記入内容を修正してください。

[登録]をクリックすると、記入した内容をBMCへ登録します。
正常に登録が完了すると、以下のメッセージが表示されます。

[データが正常に登録されました]

BMCコンフィグレーション設定項目

項目		説明	設定例	備考
コメント1		コメントを入力します（リモートからの参照はできなせん）。	空白等	
コメント2		コメントを入力します（リモートからの参照はできなせん）。	空白等	
BMC共通	コンピュータ名	インテリジェントスイッチの名前を設定します。DianaScope上で表示される本装置のサーバ名になります。各サーバで異なる名前をつける必要があります。	Switch1	
	認証キー	本装置上のBMCとDianaScopeでの接続用の認証キー(パスワード)を設定します。	Sw1tch	
	コミュニティ名	本装置が送信するSNMPトラップのコミュニティ名を設定します。	public	
	通報	通報の有効/無効を設定します。 有効: 下記通報手順、通報レベルおよび通報先の有効/無効の設定に従って通報されます。 無効: すべての通報先に対して通報されません。	有効	
	通報手順	全通報先と1つの通報先のどちらかを選択します。 全通報先: 通報設定が有効な全ての通報先へ通報します。 1つの通報先: 1箇所への通報が成功した場合は優先順位の低い通報先へは通報しません。	全通報先	本装置ではLAN経由の通報のみです。モデム、ページャによる通報は未サポートです。
	通報レベル	管理サーバ上で発生したイベントの重要度に応じて通報するか否かを設定します。	Level4	
	リモート制御(LAN)	LAN経由でのリモート管理の有効/無効を設定します。 有効: DianaScopeからのLAN経由での接続を可能にします。 無効: DianaScopeからのLAN経由での接続はできなません。また本装置からのLAN経由通報も送信されません。	有効	DianaScopeを使用する場合は有効に設定してください。
	リダイレクション(LAN)	COMの出力をLANポートにリダイレクトします。	無効	本装置ではこの機能は未サポートです。無効に設定してください。

BMCコンフィグレーション設定項目

項目		説明	設定例	備考
サーバ設定	IPアドレス	本装置のBMCのIPアドレスを設定します。本装置のマネジメントLANとは異なるIPアドレスを設定してください。	192.168.58.101	リモートKVMコンソールを使用する場合は設定が必要です。管理CPUとは異なるアドレスを設定してください。
	サブネットマスク	本装置のBMCのサブネットマスクを設定します。	255.255.255.0	リモートKVMコンソールを使用する場合は設定が必要です。
	デフォルトゲートウェイ	本装置のデフォルトゲートウェイのIPアドレスを設定します。	0.0.0.0	DianaScopeサーバと本装置間でゲートウェイを介さない場合は設定しないでください(0.0.0.0のまま)。
通報設定	通報先/管理PC IPアドレス	通報先の管理PCであるDianaScopeサーバのIPアドレスを設定します。	192.168.58.100	
	通報リトライ(0-7)	通報のリトライ数を設定します。	3	
	通報タイムアウト	通報タイムアウト時間(秒)を設定します。	6	

SDRアップデート（SDR Update）

Topページで[SDR Update]をクリックすることで、SDR（Sensor Data Record）アップデートページにジャンプします。このページでは、本装置のSDRをアップデートするときに使用します。
ページの左部分に簡単な説明・注意事項が表示されていますので、参照してください。

ヒント

SDR情報とは、本体装置上の各種センサについての定義情報です。この情報に従ってBMCは本体装置のセンサ監視を行います。

Webサーバ機能を使用してSDRのアップデートを行う場合は以下の手順に従います。

1. ファイルの選択

   このページでは、アップデートするファイルを選択します。

   現在のSDRレビジョンが表示されます。[参照]をクリックして、SDRアップデートファイルを選択してください。ファイルの選択後、[送信]をクリックしてください。

2. レビジョンの確認

   このページでは、現在のレビジョンと更新後のレビジョンを確認します。

   確認後、[開始]をクリックしてください。アップデートを開始します。再度ファイルを選択し直す場合は、ブラウザの[戻る]でファイル選択ページに戻り、選択し直してください。

3. 更新実行

   アップデートが完了するまでに1分程度かかる場合がありますが、そのままお待ちください。

重要

アップデート中に本装置の電源をOFFにしないでください。また、アップデート中にブラウザの[戻る]や[再読み込み]などの操作は行わないでください。

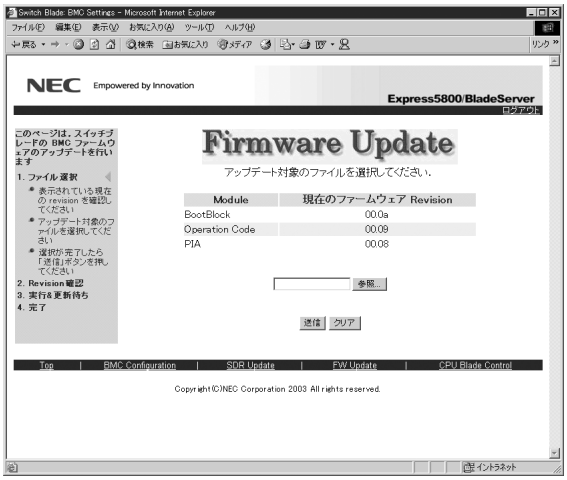
4. 完了

   アップデートが正常に完了すると、更新後のレビジョンと以下のメッセージが表示されます。

   [アップデートが正常に完了しました]

BMCファームウェアのアップデート (Firmware Update)

Topページで[Firmware Update]をクリックすることで、BMCファームウェアのアップデートページにジャンプします。
このページでは、本装置のBMCファームウェアをアップデートするときに使用します。
ページの左部分に簡単な説明・注意事項が表示されています。参照してください。



Webサーバ機能を使用してBMCファームウェアのアップデートを行う場合は以下の手順に従います。

1. ファイルの選択

   このページでは、アップデートするファイルを選択します。

   現在のBMCファームウェアのレビジョンが表示されます。　BMCファームウェア本体は[Operation Code]と呼ばれる部分になります。[参照]をクリックして、BMCファームウェアのアップデートファイルを選択してください。ファイル選択後、[送信]をクリックしてください。

2. レビジョンの確認

   このページでは、現在のレビジョンと更新後のレビジョンを確認します。

   確認後、[開始]をクリックしてください。BMCファームウェアのアップデートを開始します。再度ファイルを選択し直す場合は、ブラウザの[戻る]でファイル選択ページに戻り、選択し直してください。

3. 更新実行

   アップデートが完了するまでに3分程度かかる場合がありますが、そのままお待ちください。

   重要 **アップデート中に本装置の電源をOFFにしないでください。また、アップデート中にブラウザの[戻る]や[再読み込み]などの操作は行わないでください。**

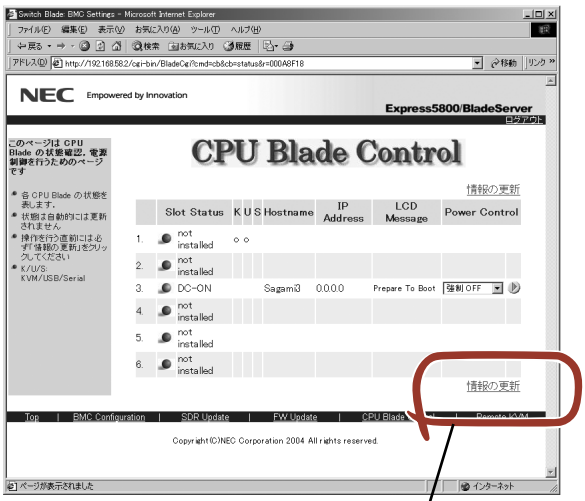
4. 完了

   アップデートが正常に完了すると、更新後のレビジョンと以下のメッセージが表示されます。

   [アップデートが正常に完了しました]

CPUブレード電源制御（CPU Blade Control）

Topページで[CPU Blade Control]をクリックすることで、同じブレード収納ユニットに実装されたCPUブレードの電源制御ページにジャンプします。
このページでは､本装置と同じブレード収納ユニットに実装されたCPUブレードの電源状態の確認と電源制御を行うときに使用します。
ページの左部分に簡単な説明・注意事項が表示されています。参照してください。



- **状態表示**

  以下の情報が表示されます。

  - 各CPUブレードの電源状態（Slot Status）
  - 各CPUブレード上のBMCに設定されているコンピュータ名（Hostname）
  - 各CPUブレード上のBMCに設定されているIPアドレス（IP Address）
  - 各CPUブレード上のBMCが保持する仮想LCDの表示内容（LCD Message）
  - KVM選択スロット(選択は○で表示)（K）
  - USB/MEDIA選択スロット(選択は○で表示)（U）
  - Serial/SIO選択スロット(選択は○で表示)（S）

- **電源制御**

  右端のプルダウンメニューで実行したい動作を選択し、右端の をクリックしてください。

  実行前に[情報の更新]をクリックして、最新情報を読み込んでください。実行に1分程度かかる場合がありますが、そのままお待ちください。

重要　**実行中、ブラウザの[戻る]や[再読み込み]などの操作は行わないでください。**

リモートKVMコンソール（Remote KVM）

CPUブレードのローカルコンソールをマネジメントポートを経由したネットワークを通して管理PCのwebブラウザに転送することができます。
管理PCから本体装置に対して、ビデオ、キーボード、およびマウスを使用して完全にアクセスできるようになります。

チェック

- リモートKVMコンソールは、以下の4種類の解像度をサポートしています。解像度は、これらのいずれかに設定してください。
  サポート外の解像度の場合、リモートKVMコンソールには表示されません。
  - 1024×768・60Hz
  - 800×600・60Hz
  - 640×480・60Hz
  - 720×400・60Hz
- リモートKVMコンソールは、プロキシを経由した接続では利用できません。
  リモートKVMコンソールを使用する場合は、プロキシを使用しない設定でログインしてください。
- リモートKVMコンソールはマネージメントポートを経由したネットワークを通してのみアクセスできます。
- リモートKVMコンソールを起動中はブラウザの「戻る」ボタンや「更新」ボタンを使わないでください。
- リモートKVMコンソールはマスタ側(マスタLEDが点灯)の本装置で使用できます。スレーブ側では使用できません。

ヒント

- KVMとは、キーボード(Keyboard)、ビデオ(Video)、マウス(Mouse)の頭文字をとった略語です。
  リモートKVMコンソールは、従来のシリアルコンソールをリモートで使用するものとは違いグラフィックスをそのままリモートで使用できるものです。
- 画面に表示される色によっては表示上の色が安定せず、ちらついた表示になることがあります。そのような場合はCPUブレード側の表示色を変更すると改善されます。
  Windows等での背景は単色に設定することをお薦めします。

BMCのIPアドレス設定

リモートKVMコンソールを使用するにはBMCのIPアドレスの設定が必要です。「BMCコンフィグレーション（BMC Configuration）」（142ページ）を参照してBMCのIPアドレス設定を行ってください。

リモートKVM機能を使用するにはBMCコンフィグレーション項目のうちIPアドレスとサブネットマスクの設定が必要です。

重要

BMCのIPアドレスは管理CPUのIPアドレスと異なるアドレスを設定する必要があります。

工場出荷時は以下のように設定されています。

管理CPU
　192.168.58.1（N8406-005A: slot7、N8406-006A: slot21）
　192.168.58.2（N8406-005A: slot8、N8406-006A: slot22）

BMC
　192.168.1.1（N8406-005A: slot7、N8406-006A: slot21）
　192.168.1.1（N8406-005A: slot8、N8406-006A: slot22）

リモートKVMコンソールウィンドウの起動

次の手順に従ってリモートKVMコンソールウィンドウを表示します。

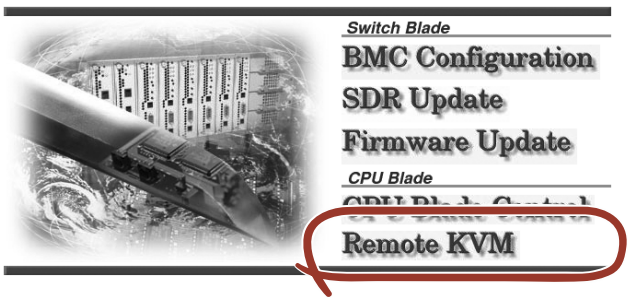
1. **Webサーバに接続する。**

   「Webサーバへの接続」（139ページ）を参照してください。

2. **Webサーバにログインする。**

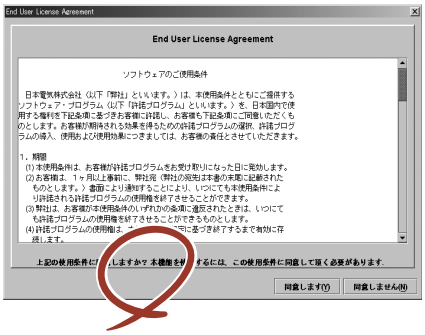
   「ログイン」（140ページ）を参照してください。

3. **Topページから「Remote KVM」をクリックする。**



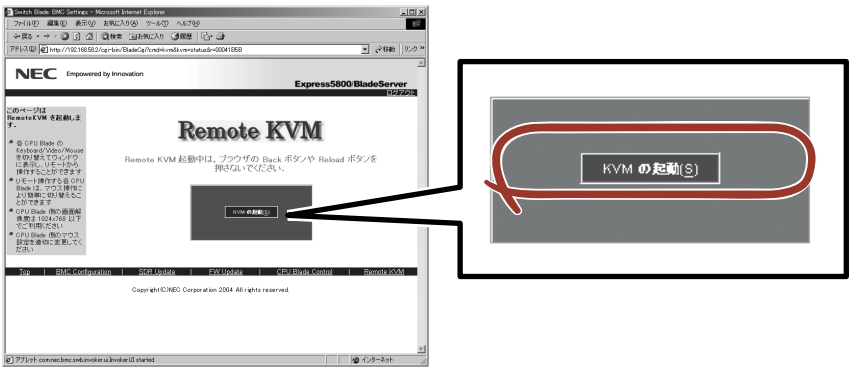
セキュリティ警告のウィンドウが現れます。

4. 「はい」をクリックする。



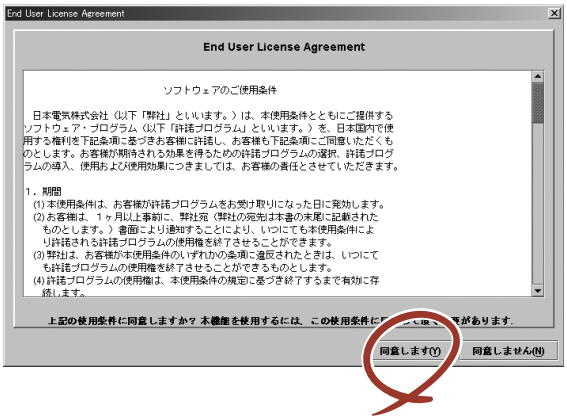
Remote KVMと書かれたページが表示されます。

5. 「KVMの起動」をクリックする。

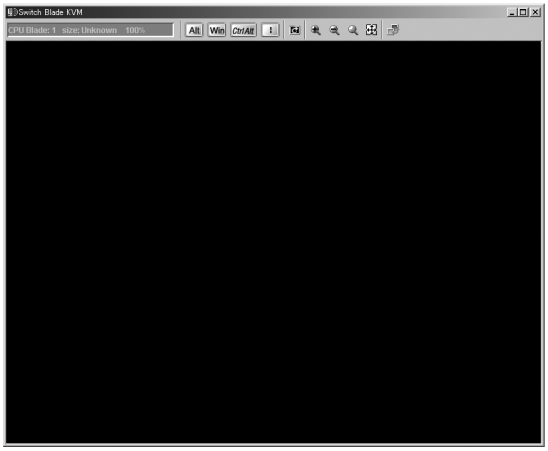


End User License Agreementウィンドウが現れます。

6. 「同意します」をクリックする。



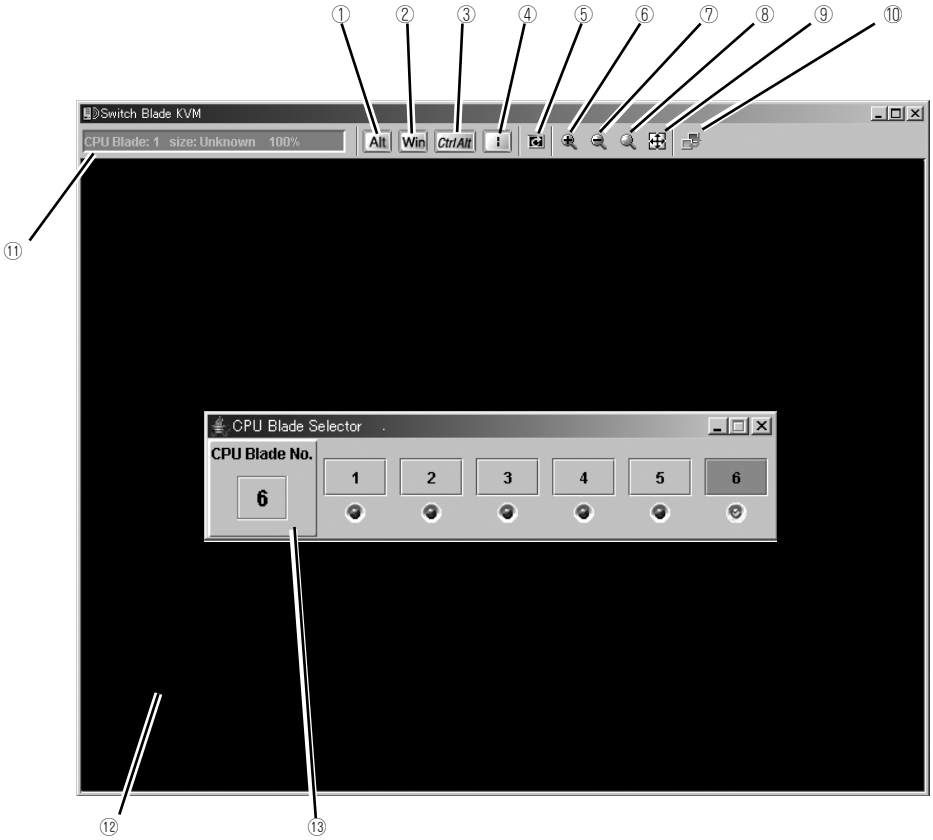
KVMコンソールウィンドウが表示されます。



重要

本体装置のローカルコンソールから、本体装置自身のBMCに対してログインした場合、リモートKVMコンソールは絶対に開かないでください。キーボードやマウスの入力が不可能な状態になってしまいます。

リモートKVMコンソールウィンドウの各部の名称



①・②・③・④ - - - 特殊キーアイコンです。特殊キーを入力するときに使用します。
⑤ - - - - - - - - - - - - 画面リフレッシュアイコンです。画面をリフレッシュするときに使用します。
⑥ - - - - - - - - - - - - 拡大アイコンです。表示を拡大したいときに使用します。
⑦ - - - - - - - - - - - - 縮小アイコンです。表示を縮小したいときに使用します。
⑧ - - - - - - - - - - - - 等倍アイコンです。表示を等倍に戻したいときに使用します。
⑨ - - - - - - - - - - - - ウィンドウリサイズアイコンです。ウィンドウサイズを画面サイズに合わせます。
⑩ - - - - - - - - - - - - CPUブレード切替画面(CPU Blade Selector)の起動アイコンです。⑬のウィンドウが表示されます。
⑪ - - - - - - - - - - - - KVMインジケータです。解像度などの情報が表示されます。
⑫ - - - - - - - - - - - - リモートKVMコンソール画面です。本体装置の画面が表示されます。
⑬ - - - - - - - - - - - - CPUブレードの切替画面（CPU Blade Selector）です。ここでCPUブレードの選択ができます。

特殊キーの入力

特殊キーについては、管理PCのキーボードから入力しても、本体装置には届きません。以下の4種類の特殊キーアイコンをクリックすることで、ホストサーバに対して入力することができます。

Alt（開放状態）、Alt（押下状態）：クリックするたびに変化します。

CtrlAlt（開放状態）、CtrlAlt（押下状態）：クリックするたびに変化します。

例えば、「Ctrl+Alt+Delete」を入力する場合は、[Ctrl+Atl]アイコンをクリックし、キーボードの<Delete>キーを押すと、本体装置へ「Ctrl+Alt+Delete」が送信されます。入力後、[Ctrl+Atl]アイコンを再度クリックして、特殊キー入力を解除してください。

Win（Windowsキーアイコン）

！（“｜”：パイプキーアイコン）

ヒント

- リモートKVMコンソール側でサポートしていない特殊キーは以下のようなキーです。
  - 「半角／全角」、「無変換」、「変換」、「カタカナ」キーなどの日本語入力キー
  - 「Print Screen」キーなど
- リモートKVMコンソール側でAppletのALT、Win、CTRL+ALTのボタンを押した状態にしておくとローカルコンソール側のキーボード入力に対しても本特殊キー入力が反映されます。
- <ALT>キーおよび<CTRL>+<ALT>キーは押し下げてから30秒経つと自動的に解除されます。

画面の拡大・縮小

拡大アイコン[ ]をクリックすると、表示内容が大きくなります。
縮小アイコン[ ]をクリックすると、表示内容が小さくなります。
等倍アイコン[ ]をクリックすると、ホストサーバ上と同じ大きさの表示となります。
ウィンドウリサイズアイコン[ ]をクリックすると、リモートKVMコンソールウィンドウのサイズをリモート画面サイズに合わせます。

画面のリフレッシュ

画面リフレッシュアイコン[ ]をクリックすると、リモートKVMコンソール画面のリフレッシュを行います。画面表示が乱れた場合は、リフレッシュを行ってください。

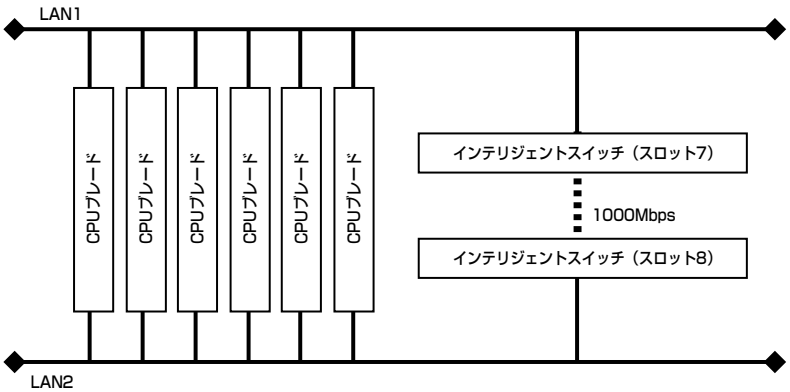
CPUブレードの選択

CPUブレード切替画面(CPU Blade Selector)の起動アイコン[]をクリックするとCPUBlade Selectorウィンドウが表示されます。

リモート画面表示やリモート操作したいCPUブレードの番号ボタンをクリックすると、操作/表示対象のCPUブレードの画面が表示されます。

冗長構成での運用（N8406-005A）

N8406-005A インテリジェントスイッチはスロット7/8間の接続用内部ポート（1000Mbps）を持っています。



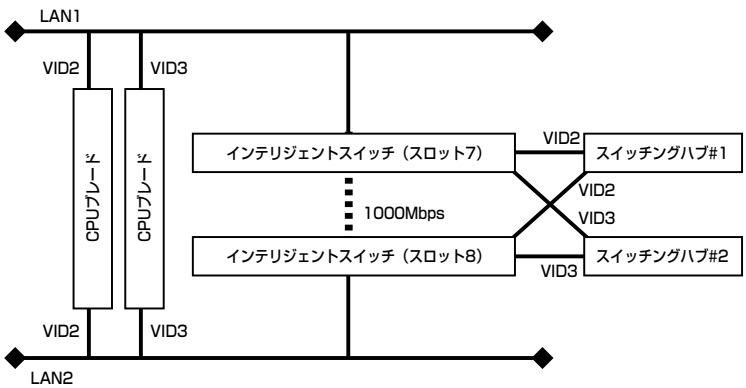
デフォルト状態でこのリンクは無効となっていますが、冗長機能を使用する場合にはredundancy mode enableコマンド（「redundancy mode enable」（180ページ））を両方の装置に投入して、内部ポートを有効化してください。この接続はデフォルトで無効となっていて、ポート間は接続されていません。
接続するためには2台の本装置に対して、redundancy mode enable コマンド（180ページ）でenableを設定してください。

重要

正しく運用するために、2台の本装置のredundancy modeの設定は同じにしてください。

ヒント

- CPUブレードに搭載された2つのネットワークインタフェースでAFT(アダプティブ・フォルト・トレランス)機能をお使いになる場合は、同一サブネットに接続している必要があります。ユーザーポートの先で同一サブネットに接続、または、「redundancy mode enable」（180ページ）によって接続することでも解決できます。
- redundancy mode enableをenableに設定することで、すべてのVLANはこのポートに自動的に加入されます。



外部スイッチを利用した冗長構成ネットワーク構成例
（スパニングツリー設定）

メ　モ