



スマートスイッチ

BS-GS2108

BS-GS2116

BS-GS2108P

BS-GS2116P

BS-GS2124

BS-GS2124P

BS-GS2124P/HP

BS-GS2148

**ユーザーズマニュアル**

***<https://www.buffalo.jp/>***

# 目次

<b>第 1 章 導入設定 .....</b>	<b>6</b>
本書について .....	6
動作環境 .....	6
ビジネススイッチ設定ツールのインストール .....	6
本製品のIPアドレスを設定する .....	7
設定画面を表示する .....	10
日付・時刻を設定する .....	13
ユーザー名・パスワードを設定する .....	15
MACアドレスの学習方式について .....	16
 <b>第 2 章 本製品の設定画面 .....</b>	 <b>17</b>
システム .....	17
システム情報設定 .....	18
VLAN .....	19
VLAN設定 .....	19
VLANポート設定 .....	24
ルーティング .....	25
レイヤー設定 .....	25
静的ルーティング .....	26
SNMP .....	27
SNMPコミュニティテーブル .....	27
SNMPホストテーブル .....	28
SNMPトラップ .....	29
SNMPv3ユーザー .....	31

LLDP .....	32
設定 .....	32
LLDPポート .....	33
LLDP-MEDポート .....	34
隣接機器情報 .....	35
MACアドレス .....	36
MACアドレス学習方式 .....	36
静的MACフィルター .....	37
動的MACフィルター .....	38
MACアドレス変換 .....	39
静的MACアドレス .....	39
MACアドレスエイジング .....	40
ポート設定 .....	41
ステータス .....	41
速度/モード設定 .....	42
システムセキュリティ .....	43
アカウント管理 .....	43
アクセス管理 .....	43
証明書 .....	44
日付と時刻 .....	46
PoE (PoE対応製品のみ) .....	47
PoEステータス .....	47
PoEガードバンド .....	48
PoEプロファイル設定 .....	49
PoEスケジューラー .....	51
QoS .....	52
QoS設定 .....	52
QoSマッピング .....	53
VoIP優先制御 .....	55

IPv4/MACポリシー .....	55
IPv6ポリシー設定.....	58
ポート設定.....	60
IPv4/MAC優先度設定 .....	60
IPv6優先度設定 .....	61
ステータス.....	61
セキュリティ .....	62
DOS攻撃防止 .....	62
DHCPスヌーピング .....	63
DHCPテーブル.....	64
認証 .....	65
ステータス.....	65
RADIUS.....	66
ポート認証.....	68
ポートトランク .....	70
トラフィック制御.....	71
ミラーリング .....	72
STP .....	72
設定 .....	72
ステータス.....	75
ポート .....	77
IGMP.....	78
ステータス.....	78
設定 .....	79
IGMPクエリア .....	80
静的ルーターポート .....	80
MLD.....	81
ステータス.....	81

設定 .....	81
MLDクエリア .....	82
静的ルーターポート .....	83
ACL .....	83
ACLウィザード .....	83
MAC ACLグループ設定 .....	84
IPv4 ACLグループ設定 .....	87
IPv6 ACLグループ設定 .....	90
ポート設定.....	92
IPv4/MAC ACL優先度設定.....	93
IPv6 ACL優先度設定.....	93
ステータス.....	94
ループ防止機能 .....	95
DHCPリレー .....	97
キキNavi .....	98
ファームウェア更新 .....	99
デュアルイメージ.....	100
設定保存/復元 .....	101
再起動.....	101
初期化.....	102
ARPテーブル.....	103
ポート順 .....	103
IPアドレス順 .....	103
MACアドレステーブル .....	104
ポート順 .....	104
MACアドレス順 .....	104
統計情報 .....	105

ログ .....	107
Syslog設定 .....	108
ネットワーク診断 .....	109
ケーブル診断 .....	110
I'm here .....	111
<b>第3章 困ったときは .....</b>	<b>112</b>
ランプが点灯しない、異常点灯・点滅している .....	112
設定画面が表示できない .....	113
パスワードを忘れた .....	113
<b>付録 .....</b>	<b>114</b>
仕様 .....	114
端子仕様 .....	114
FAN搭載製品 .....	115
初期設定一覧 .....	116
エラー番号一覧 .....	123
ループによるネットワークダウンを防止する .....	123
本書について .....	124
免責事項 .....	124
使用ソフトウェアについて .....	125
商標・登録商標 .....	125

# 第1章 導入設定

---

## 本書について

---

本書では、BS-GS2108Pの画面を例に説明しています。

---

## 動作環境

---

本製品の動作環境は次のとおりです。

### 本製品の対応機器・動作確認済みブラウザ・対応OS

#### 対応機器: 本製品との接続

1000BASE-T/100BASE-TX/10BASE-T対応機器(パソコン、Mac、NAS、スイッチなど)

#### 動作確認済みブラウザ: 本製品の設定変更

下記当社ホームページから確認いただけます。

BS-GS2108: <https://www.buffalo.jp/product/detail/taiou/bs-gs2108.html>

BS-GS2116: <https://www.buffalo.jp/product/detail/taiou/bs-gs2116.html>

BS-GS2108P: <https://www.buffalo.jp/product/detail/taiou/bs-gs2108p.html>

BS-GS2116P: <https://www.buffalo.jp/product/detail/taiou/bs-gs2116p.html>

BS-GS2124: <https://www.buffalo.jp/product/detail/taiou/bs-gs2124.html>

BS-GS2124P: <https://www.buffalo.jp/product/detail/taiou/bs-gs2124p.html>

BS-GS2124P/HP: [https://www.buffalo.jp/product/detail/taiou/bs-gs2124p\\_hp.html](https://www.buffalo.jp/product/detail/taiou/bs-gs2124p_hp.html)

BS-GS2148: <https://www.buffalo.jp/product/detail/taiou/bs-gs2148.html>

#### 対応OS: ビジネススイッチ設定ツール(当社ホームページよりダウンロード)

下記「ビジネススイッチ設定ツールのインストール」で案内している当社ホームページから確認いただけます。

---

## ビジネススイッチ設定ツールのインストール


---

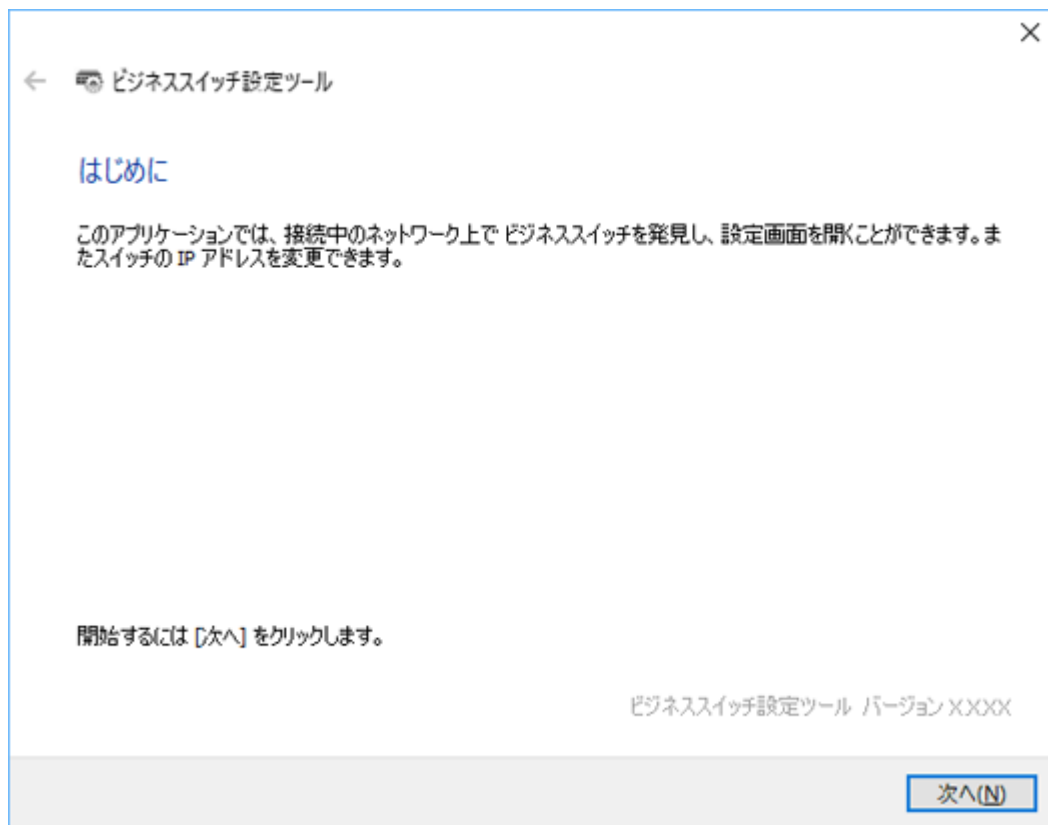
ビジネススイッチ設定ツールは、ビジネススイッチの設定画面を表示するためのソフトウェアです。

本製品を設定する前に、当社ホームページ(<https://www.86886.jp/bsset/>)より「ビジネススイッチ設定ツール」をダウンロードし、インストールしてください(Windowsのみ対応)。

## 本製品のIPアドレスを設定する

本製品の設定画面を表示するために、本製品のIPアドレスが設定用の管理者パソコンと同じセグメントになるように設定します。

- 1 LANケーブル(別売)で、本製品と管理者パソコンおよび既存のネットワーク環境(社内ネットワーク)を接続します。ケーブルを接続したポートのLINK/ACTランプが点灯することを確認してください。
- 2 デスクトップの「ビジネススイッチ設定ツール」()をダブルクリックします。
- 3 [次へ]をクリックして、スイッチの検索を開始します。





**4** 本製品を選択して、[次へ]をクリックします。

← ビジネススイッチ設定ツール

### スイッチの選択

操作したいスイッチを選択してください。リストにない場合は、[再検索]をクリックしてください。

スイッチ名	製品名	Ver.	MAC アドレス	IP アドレス
BSX0000000000X	BS-X000000X	Ver.X.X.X	XX:XX:XX:XX:XX:XX	192.168.1.254

[スイッチが見つからない場合](#) 再検索(R)

選択したら [次へ] をクリックします。

次へ(N) キャンセル

**5** [このスイッチのIPアドレスを設定する]をクリックします。

← ビジネススイッチ設定ツール

### 操作の選択

次のスイッチが選択されました。おこないたい操作を選択してください。

スイッチ名	製品名	Ver.	MAC アドレス	IP アドレス
BSX0000000000X	BS-X000000X	Ver.X.X.X	XX:XX:XX:XX:XX:XX	192.168.1.254

設定画面を開く(W)  
(通常はこちら)

このスイッチの IP アドレスを設定する(I)  
(上級者・管理者向け)

- 6** 管理者パソコンのIPアドレスと同じセグメントになるように本製品のIPアドレスを設定し、[次へ]をクリックします。

← ビジネススイッチ設定ツール

### スイッチの IP アドレス設定

スイッチの新しい IP アドレスを入力してください。

☐ DHCP サーバーから IP アドレスを自動的に取得する(かんたん)(Q)

☒ 次の IP アドレスを使う(上級者・管理者向け)(S)

IP アドレス(I)  [設定方法](#)

サブネット マスク(U)

※ 参考情報 - このパソコンの IP アドレス:  
192.168.11.101 / 255.255.255.0 : イーサネット (Intel(R) 82579V Gigabit Network Conn

[次へ] をクリックすると、設定内容がスイッチに反映されます。

次へ(N)

- 7** パスワードの入力画面が表示されたら、本製品に設定されている管理パスワード(出荷時設定では「password」)を入力して、[次へ]をクリックします。

← ビジネススイッチ設定ツール

### 設定中

このスイッチには、管理パスワードが設定されています。

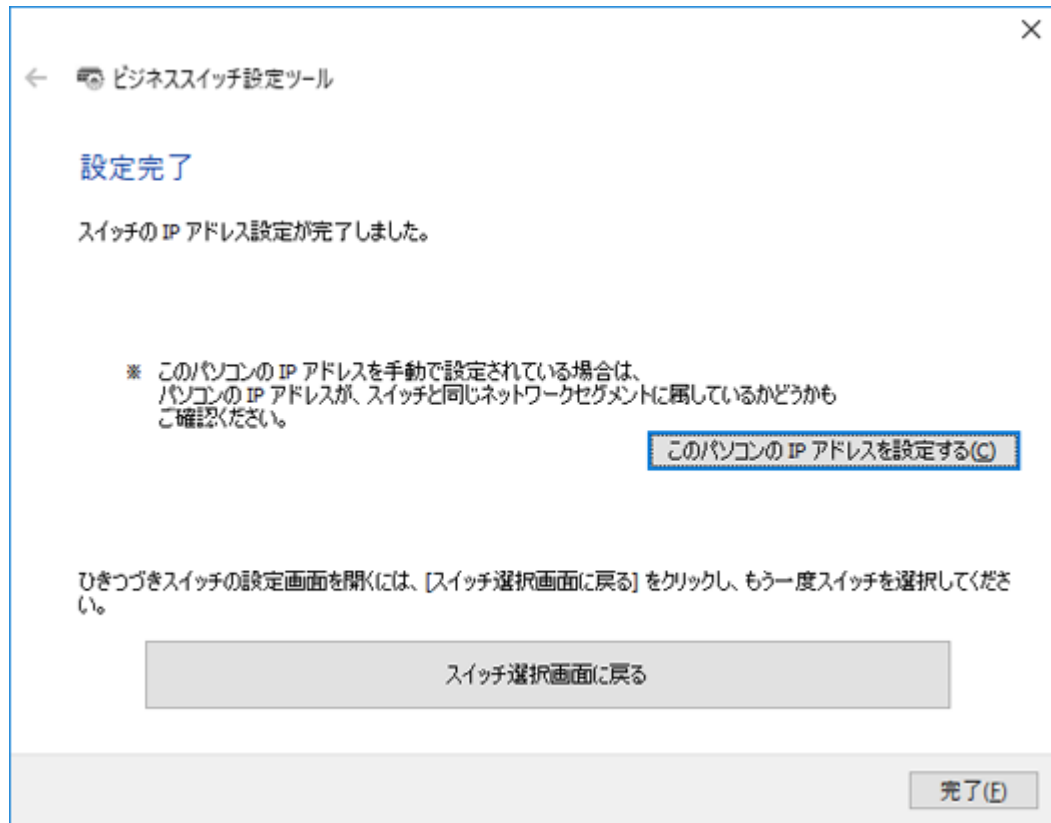
スイッチの管理パスワードを入力してください。

管理パスワード(P)  ☒ 入力文字列を表示(V)

出荷時の設定は、「password」または 無し(空欄) です。

次へ(N)

## 8 [完了]をクリックします。

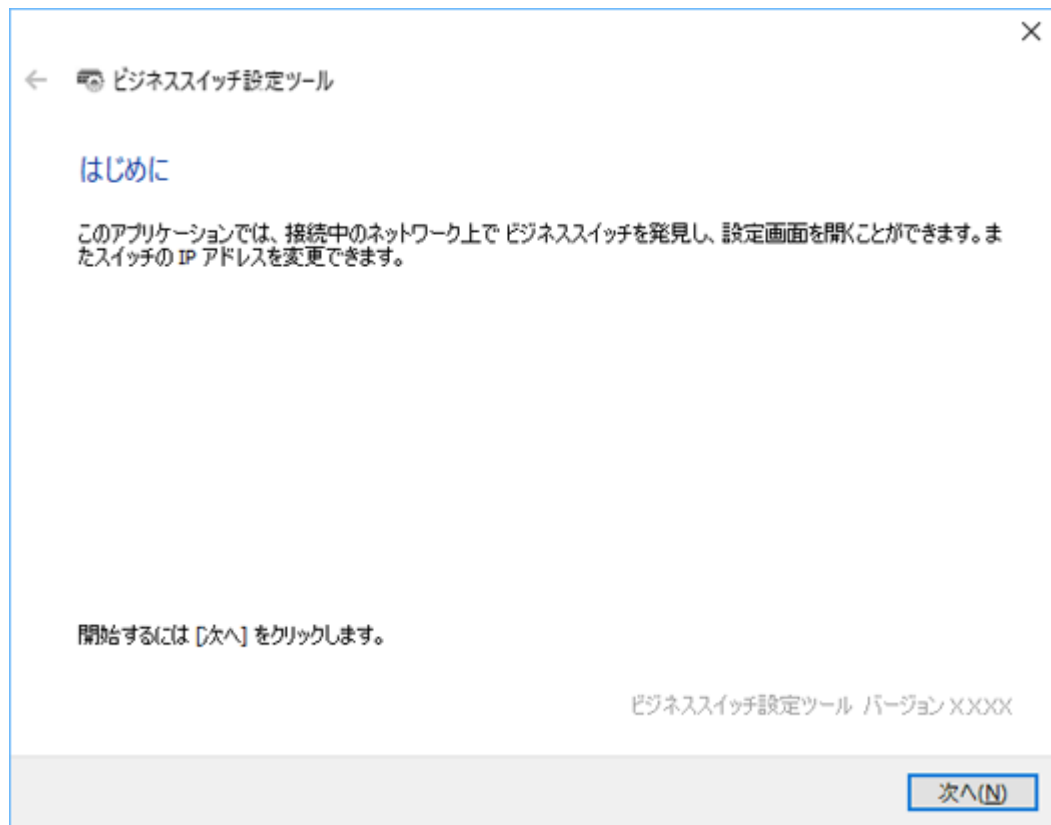


以上で設定は完了です。

## 設定画面を表示する

本製品を設定するために、設定画面を表示します。

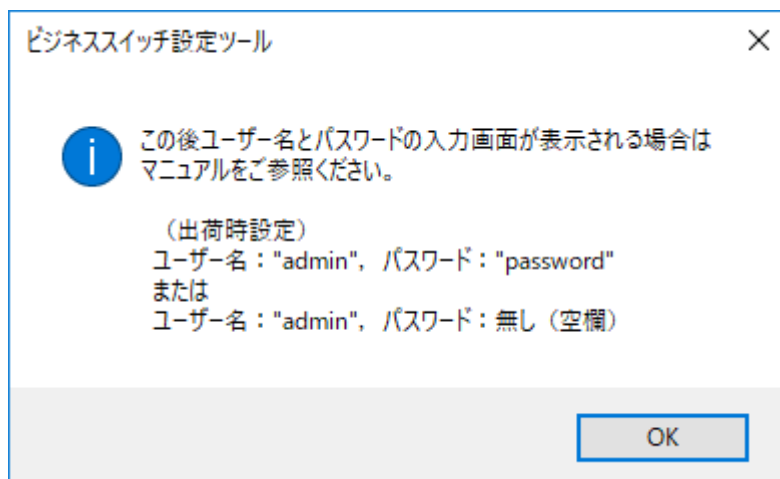
- 1 デスクトップの「ビジネススイッチ設定ツール」() をダブルクリックします。

**2** [次へ]をクリックして、スイッチの検索を開始します。**3** 本製品を選択して、[次へ]をクリックします。

#### 4 [設定画面を開く]をクリックします。



#### 5 [OK]をクリックします。ブラウザーが起動し、ログイン画面が表示されます。



#### 6 ユーザー名に「admin」(小文字)、パスワードに「password」(小文字)を入力して、[ログイン]をクリックします。

ユーザー名	admin
パスワード	●●●●●●●●
ログイン	

**メモ:** 設定画面のウィンドウが開くと、ビジネススイッチ設定ツールのウィンドウに「スイッチの設定画面を開きました」と表示されます。ビジネススイッチ設定ツールのウィンドウの[完了]をクリックしてください。ビジネススイッチ設定ツールが閉じます。

**7** 設定画面が表示されます。

The screenshot shows the Buffalo web management interface. On the left is a sidebar menu with 'システム' (System) selected, containing sub-items: '基本設定' (Basic Settings), '詳細設定' (Advanced Settings), and '管理' (Management). The main area is titled 'システム' (System) and contains a table of system settings.

システム設定	
製品名	BUFFALO BS-GS2108P
スイッチ名	BSXXXXXXXXXX
設置場所	Not defined
管理者	Not defined
稼働時間	0 日、0 時間、5 分、39 秒
OID	XXXXXXXXXXXX
シリアルナンバー	XXXXXXXXXXXX
MACアドレス	XX:XX:XX:XX:XX:XX
IPv4アドレス設定	
IPv4アドレス取得方法	固定IPアドレス
IPv4アドレス設定	192.168.1.254
サブネットマスク	255.255.255.0
デフォルトゲートウェイ	0.0.0.0
IPv6アドレス	

At the bottom left, it says 'BS-GS2108P Version'. At the bottom right, it says 'Copyright © 2022 Buffalo Inc.'.

以上で完了です。

## 日付・時刻を設定する

日付・時刻は以下の手順で設定します。

- 1** 「[設定画面を表示する](#)」(P.10)を参照して、本製品の設定画面にログインします。
- 2** 画面左の「基本設定」－「日付と時刻」をクリックします。

### 3 入力が完了したら、[適用]をクリックします。

自動時刻設定						
SNTP		<input type="checkbox"/> 有効				
手動時刻設定						
時刻設定	YYYY	MM	DD	hh	mm	ss
	2021	/ 01	/ 01	02	: 29	: 00
						<a href="#">パソコンから現在の時刻を取得</a>
SNTPサーバー設定						
サーバーIPアドレス/FQDN		ntp.jst.mfeed.ad.jp				
更新間隔		24 (1~24時間)				
タイムゾーン		(GMT+09:00) Osaka, Sapporo, Tokyo ▼				

**メモ:** SNTPサーバーを変更する場合は、IPアドレスまたはDNS解決可能なホスト名(FQDN)を4~255文字以内で設定してください。FQDNを使用する場合は、[基本設定] - [VLAN] - [VLAN設定]画面でDNSサーバーを設定してください。

以上で設定は完了です。

## ユーザー名・パスワードを設定する

設定画面のユーザー名やパスワードを出荷時設定値の「admin」「password」から任意の値に変更します。  
以下の手順で設定してください。

**1** 「[設定画面を表示する](#)」(P.10)を参照して、本製品の設定画面にログインします。

**2** 画面左の[基本設定]－[システムセキュリティ]－[アカウント管理]をクリックします。

**3** 新しいユーザー名およびパスワード(確認欄も含む)を入力し、[適用]をクリックします。

メモ:

- 管理ユーザー名は1～8文字の半角英数字、ハイフン(-)、アンダースコア(\_)で設定してください。
- 管理パスワードは1～32文字の半角英数字、ハイフン(-)、アンダースコア(\_)で設定してください。

ユーザー名/パスワード	
管理ユーザー名	buffalo
管理パスワード	●●●●●●●●
管理パスワード(確認)	●●●●●●●●

適用

**4** ユーザー名、パスワードに手順3で設定したユーザー名とパスワードを入力して、[ログイン]をクリックします。

ユーザー名 buffalo

パスワード ●●●●●●●●

ログイン

以上で設定は完了です。

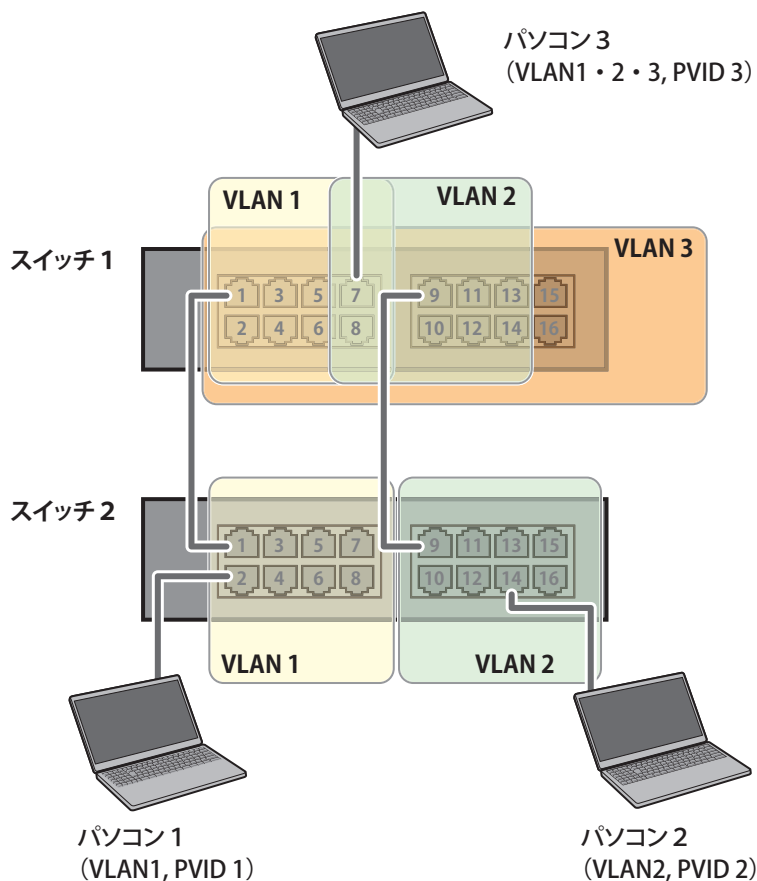


## MACアドレスの学習方式について

本製品のMACアドレス学習方式は、工場出荷時にSVL方式に設定されています。IVL方式に変更する場合は、設定画面の[基本設定]－[MACアドレス]－[MACアドレス学習方式]から、設定を変更してください。

SVL方式は、機器全体で共通のMACアドレステーブルを保持する方式です。IVL方式は、VLANごとにMACアドレステーブルを保持する方式です。それぞれの動作を理解したうえで、本製品のVLANを設定してください。

### SVLとIVLの違い



#### SVLの場合

パソコン1とパソコン3が通信している場合、スイッチ2のポート1にパソコン3が学習されるので、パソコン2とパソコン3が通信できません。

#### IVLの場合

パソコン1とパソコン3が通信している場合でも、パソコン3はVLAN 1とVLAN 2の両方で学習されるため、パソコン2とパソコン3は通信できます。ただし、パソコン3からパソコン1へ送信されるフレームはパソコン2にも届きます。

## 第2章 本製品の設定画面

[「設定画面を表示する」\(P.10\)](#)を参照して、本製品の設定画面にログインします。

### システム

本製品に関する情報を表示します。

#### システム

システム設定	
製品名	BUFFALO BS-GS2108P
スイッチ名	BSXXXXXXXXXX
設置場所	Not defined
管理者	Not defined
稼働時間	0 日、0 時間、5 分、39 秒
OID	XXXXXXXXXXXX
シリアルナンバー	XXXXXXXXXXXX
MACアドレス	XX:XX:XX:XX:XX:XX
IPv4アドレス設定	
IPv4アドレス取得方法	固定IPアドレス
IPv4アドレス設定	192.168.1.254
サブネットマスク	255.255.255.0
デフォルトゲートウェイ	0.0.0.0
IPv6アドレス	
リンクローカルアドレス	::
静的グローバルアドレス	::
静的デフォルトゲートウェイ	::
動的グローバルアドレス	::
動的デフォルトゲートウェイ	::
バージョン	
ファームウェアバージョン	X.X.X.XX/XXX XX 20XX XX:XX:XX
ブートコードバージョン	X.X.X.XX/XXX XX 20XX XX:XX:XX
ハードウェアバージョン	XXXXXXXX

項目	内容
システム設定	本製品の製品名、スイッチ名、シリアルナンバーやMACアドレスなど、本製品のシステムに関する内容を表示します。
IPv4アドレス設定	本製品のIPv4アドレス、サブネットマスク、デフォルトゲートウェイなどの情報を表示します。

項目	内容
IPv6アドレス	本製品のIPv6リンクローカルアドレス、静的・動的グローバルアドレス、デフォルトゲートウェイの情報を表示します。
バージョン	本製品のファームウェア、ブートコード、ハードウェアのバージョンを表示します。

## システム情報設定

本製品のスイッチ名、設置場所、管理者名を設定します。

### 基本設定 > システム情報設定

システム設定		
スイッチ名	BSXXXXXXXXXXXX	(50文字までの半角英数字、「-」、「_」)
設置場所	Not defined	(50文字までの半角英数字、「-」、「_」およびスペース)
管理者	Not defined	(50文字までの半角英数字、「-」、「_」およびスペース)

適用

項目	内容
スイッチ名	本製品に割り当てる名前を入力します(半角英数字、“-”(ハイフン)、“_”(アンダースコア)で50文字まで)。
設置場所	本製品の設置場所を入力します(半角英数字、“-”(ハイフン)、“_”(アンダースコア)、スペースで50文字まで)。
管理者	本製品の管理者名を入力します(半角英数字、“-”(ハイフン)、“_”(アンダースコア)、スペースで50文字まで)。

# VLAN

## VLAN設定

現在のVLANの設定状況およびVLANの新規作成を行います。また、本製品のIPv4/IPv6アドレス、デフォルトゲートウェイ、DNSサーバーなどを設定できます。

基本設定 > VLAN > VLAN設定

### レイヤー2モード時

VLAN設定

VLANモード

☒VLAN設定  
☐インターネットマンション

VLANステータス

	VLAN ID	IPv4アドレス	1	2	3	4	5	6	7	8	VLAN名	管理VLAN
<input type="checkbox"/>	1	192.168.1.254	U	U	U	U	U	U	U	U		Up
	PVID		1	1	1	1	1	1	1	1		
	プロテクトポート		-	-	-	-	-	-	-	-		

T:Static Tagged U:Static Untagged -:Not Member X:有効

編集

削除

VLANの追加/編集

VLAN ID

(2-4094)

VLAN名

管理VLAN

☐

ポート		1	2	3	4	5	6	7	8
Tagged	<div>All</div>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Untagged	<div>All</div>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Not Member	<div>All</div>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>

適用

リセット

キャンセル

項目	内容
VLANモード	通常のVLANモードとインターネットマンションモード(各部屋からルーターへの通信を可能にし、また各部屋間の通信を遮断する機能)のいずれかを選択します。 <b>メモ:</b> VLANとインターネットマンションモードは同時に使用できません。
VLANステータス	現在のVLAN構成およびPVID(Port VLAN ID)を表示します。[編集]をクリックすると、選択したVLANを編集できます。[削除]をクリックすると、選択したVLANを削除できます(ただし、VLAN1は削除できません)。
VLAN ID	VLAN番号を指定します(指定範囲:2~4094)。
VLAN名	VLAN名を指定します(半角英数字、“-”(ハイフン)、“_”(アンダースコア)で17文字まで)。
管理VLAN	管理VLANに設定する場合、チェックします。管理VLANに属する端末からのみ管理インターフェースにアクセスできます。
Tagged	ポートをTagメンバーに割り当てるときに選択します。

項目	内容
Untagged	ポートをUntagメンバーに割り当てるときに選択します。
Not Member	ポートをメンバーに指定しません。
リセット	前回の設定値にします。
Uplink	インターネットマンションモードを選択したときに表示されます。 インターネットに接続するためのルーターを接続するポートです。UplinkポートはすべてのDownlinkポートと通信できます。最低1ポート選択する必要があります。
Downlink	インターネットマンションモードを選択したときに表示されます。 各部屋の端末を接続するポートです。DownlinkポートはUplinkポートと通信できますがDownlinkポート間での通信はできません。

**メモ:** インターネットマンションモードは、Uplinkのみ本製品の設定画面を表示できます。設定用パソコンが接続されているポートをDownlinkポートに設定すると、それ以降は設定画面を表示できなくなります。

以下の項目は、VLAN ID 1を選択して[編集]をクリックしたとき、またはインターネットマンションモードでIPアドレス欄の[編集]をクリックしたときに表示されます。

VLANの追加/編集	
VLAN ID	1 (2-4094)
VLAN名	
管理VLAN	<input checked="" type="checkbox"/>
IPv4アドレス取得方法	
IPv4アドレス取得方法	固定IPアドレス
IPv4アドレス設定	
IPv4アドレス	192.168.1.254
サブネットマスク	255.255.255.0
デフォルトゲートウェイ	0.0.0.0
DNSサーバー	
DNS取得方法	手動設定
プライマリーDNSサーバー	0.0.0.0
セカンダリーDNSサーバー	0.0.0.0
IPv6アドレス設定	
IPv6	<input type="checkbox"/> 有効

**メモ:** 「IPv4アドレス」、「サブネットマスク」、「デフォルトゲートウェイ」、「プライマリーDNSサーバー」、「セカンダリーDNSサーバー」は空欄で設定できません。  
「デフォルトゲートウェイ」、「プライマリーDNSサーバー」、「セカンダリーDNSサーバー」を設定しない場合は「0.0.0.0」(出荷時設定)を入力してください。

項目	内容
IPv4アドレス取得方法	<p>本製品のIPアドレスの設定方法を選択します。</p> <p><b>DHCPサーバーから自動的に取得する</b> DHCPサーバーからIPアドレスを取得します。</p> <p><b>固定IPアドレス</b> 手動でIPアドレスを設定します。</p>

項目	内容
IPv4アドレス	「IPv4アドレス取得方法」で「固定IPアドレス」を選択した場合に使用するIPv4アドレスを入力します。
サブネットマスク	「IPv4アドレス取得方法」で「固定IPアドレス」を選択した場合に使用するサブネットマスクを入力します。
デフォルトゲートウェイ	「IPv4アドレス取得方法」で「固定IPアドレス」を選択した場合に使用するデフォルトゲートウェイを入力します。
DNS取得方法	<p>「IPv4アドレス取得方法」で「DHCPサーバーから自動的に取得する」を選択した場合、DNSサーバーのIPアドレスの取得方法を選択します。</p> <p><b>DHCPサーバーから自動的に取得する</b> DHCPサーバーからIPアドレスを取得します。</p> <p><b>手動設定</b> 手動でIPアドレスを設定します。</p>
プライマリーDNSサーバー	プライマリーDNSサーバーのIPアドレスを入力します。
セカンダリーDNSサーバー	セカンダリーDNSサーバーのIPアドレスを入力します。
IPv6	IPv6を有効にする場合は「有効」にチェックを入れます。
IPv6アドレスの自動取得	IPv6対応ルーターからルーターアドバタイズメントを取得する場合は「有効」にチェックを入れます。
DHCPv6クライアント	DHCPv6クライアントを使用する場合は、「有効」にチェックを入れます。「Rapid Commit」にチェックを入れると、IPv6アドレス取得時にDHCPv6サーバーとの通信を高速化します。DHCPv6サーバーもRapid Commitに対応している必要があります。
リンクローカルアドレス	本製品のリンクローカルアドレスが表示されます。リンクローカルアドレスは、IPv6を有効にすると自動的に生成されます。
静的グローバルアドレス	<p>手動でグローバルアドレスを設定する場合は、グローバルアドレスとプレフィックス長を入力します。プレフィックス長は、1～128の範囲で入力します。</p> <p>「EUI-64」にチェックを入れると、Modified EUI-64(RFC4291)に従って、本製品のMACアドレスを基にIPv6アドレスの下位64bitを自動生成します。</p>
静的デフォルトゲートウェイ	<p>手動でデフォルトゲートウェイを設定する場合は、デフォルトゲートウェイのアドレスを入力します。</p> <p><b>メモ:</b> 静的デフォルトゲートウェイのプレフィックスは、静的グローバルアドレスと同一である必要があります。</p>
動的グローバルアドレス	<p>DHCPv6もしくはルーターアドバタイズメントから取得した動的グローバルアドレスが表示されます。</p> <p>末尾にSF(ステートフル)がついているアドレスはDHCPv6から取得したアドレスです。SL(ステートレス)がついているアドレスはルーターアドバタイズメントから取得したアドレスです。</p>
動的デフォルトゲートウェイ	ルーターアドバタイズメントから取得した動的デフォルトゲートウェイが表示されます。

## レイヤー3モード時

VLAN設定												
VLANモード		<input checked="" type="radio"/> VLAN設定 <input type="radio"/> インターネットマンション										
VLANステータス												
	VLAN ID	IPv4アドレス	1	2	3	4	5	6	7	8	VLAN名	
<input type="checkbox"/>	1	192.168.1.254	U	U	U	U	U	U	U	U		
PVID			1	1	1	1	1	1	1	1		
プロテクトポート			-	-	-	-	-	-	-	-		
T:Static Tagged U:Static Untagged -:Not Member X:有効												
<input type="button" value="編集"/> <input type="button" value="削除"/>												
VLANの追加/編集												
VLAN ID		<input type="text" value=""/> (2-4094)										
VLAN名		<input type="text" value=""/>										
管理VLAN		<input type="checkbox"/>										
IPv4アドレス設定												
IPv4アドレス		<input type="text" value="0.0.0.0"/>										
サブネットマスク		<input type="text" value="0.0.0.0"/>										
ポート		1	2	3	4	5	6	7	8			
Tagged	<input type="button" value="All"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>			
Untagged	<input type="button" value="All"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>			
Not Member	<input type="button" value="All"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>			
<input type="button" value="適用"/> <input type="button" value="リセット"/> <input type="button" value="キャンセル"/>												

項目	内容
VLANモード	レイヤー3モード時は、インターネットマンションモードは使用できません。
VLANステータス	現在のVLAN構成およびPVID (Port VLAN ID)を表示します。[編集]をクリックすると、選択したVLANを編集できます。[削除]をクリックすると、選択したVLANを削除できます(ただし、VLAN1は削除できません)。
VLAN ID	VLAN番号を指定します(指定範囲:2~4094)。
VLAN名	VLAN名を指定します(半角英数字、“-”(ハイフン)、“_”(アンダースコア)で17文字まで)。
管理VLAN	レイヤー3モード時は、IPアドレスを割り当てたVLANはすべて管理VLANとなります。
IPv4アドレス設定	作成するVLANに固定IPアドレスを割り当てる場合は、IPv4アドレスとサブネットマスクを入力します。 <b>メモ:</b> 固定IPv4アドレスを割り当てることができるVLANの数は32個までです。
Tagged	ポートをTagメンバーに割り当てるときに選択します。
Untagged	ポートをUntagメンバーに割り当てるときに選択します。
Not Member	ポートをメンバーに指定しません。
リセット	前回の設定値にします。

以下の項目は、VLAN ID 1を選択して[編集]をクリックしたときに表示されます。

VLANの追加/編集	
VLAN ID	1 (2-4094)
VLAN名	
管理VLAN	<input type="checkbox"/>
IPv4アドレス設定	
IPv4アドレス	192.168.1.254
サブネットマスク	255.255.255.0
DNSサーバー	
DNS取得方法	手動設定 ▼
プライマリDNSサーバー	0.0.0.0
セカンダリDNSサーバー	0.0.0.0
IPv6アドレス設定	
IPv6	<input type="checkbox"/> 有効

項目	内容
DNS取得方法	レイヤー3モード時は、DNSサーバーのIPアドレスの取得方法は「手動設定」(手動でIPアドレスを設定)となります。
プライマリDNSサーバー	プライマリDNSサーバーのIPアドレスを入力します。
セカンダリDNSサーバー	セカンダリDNSサーバーのIPアドレスを入力します。
IPv6	IPv6を有効にする場合は「有効」にチェックを入れます。
IPv6アドレスの自動取得	IPv6対応ルーターからルーターアドバタイズメントを取得する場合は「有効」にチェックを入れます。
DHCPv6クライアント	DHCPv6クライアントを使用する場合は、「有効」にチェックを入れます。「Rapid Commit」にチェックを入れると、IPv6アドレス取得時にDHCPv6サーバーとの通信を高速化します。DHCPv6サーバーもRapid Commitに対応している必要があります。
リンクローカルアドレス	本製品のリンクローカルアドレスが表示されます。リンクローカルアドレスは、IPv6を有効にすると自動的に生成されます。
静的グローバルアドレス	手動でグローバルアドレスを設定する場合は、グローバルアドレスとプレフィックス長を入力します。プレフィックス長は、1～128の範囲で入力します。「EUI-64」にチェックを入れると、Modified EUI-64(RFC4291)に従って、本製品のMACアドレスを基にIPv6アドレスの下位64bitを自動生成します。
静的デフォルトゲートウェイ	手動でデフォルトゲートウェイを設定する場合は、デフォルトゲートウェイのアドレスを入力します。 <b>メモ:</b> 静的デフォルトゲートウェイのプレフィックスは、静的グローバルアドレスと同一である必要があります。
動的グローバルアドレス	DHCPv6もしくはルーターアドバタイズメントから取得した動的グローバルアドレスが表示されます。 末尾にSF(ステートフル)がついているアドレスはDHCPv6から取得したアドレスです。SL(ステートレス)がついているアドレスはルーターアドバタイズメントから取得したアドレスです。
動的デフォルトゲートウェイ	ルーターアドバタイズメントから取得した動的デフォルトゲートウェイが表示されます。



**メモ:** レイヤー3モードでは、IPv4のデフォルトゲートウェイは[ルーティング]－[静的ルーティング]から設定できます。

## VLANポート設定

PVID(ポートVLAN ID)を設定します。

### 基本設定 > VLAN > VLANポート設定

ポート	PVID	受信するフレームの種類	イングレスフィルター	プロテクトポート	
1	<input type="text" value="1"/>	<input type="text" value="すべて"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
2	<input type="text" value="1"/>	<input type="text" value="すべて"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
3	<input type="text" value="1"/>	<input type="text" value="すべて"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
4	<input type="text" value="1"/>	<input type="text" value="すべて"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
5	<input type="text" value="1"/>	<input type="text" value="すべて"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6	<input type="text" value="1"/>	<input type="text" value="すべて"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
7	<input type="text" value="1"/>	<input type="text" value="すべて"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
8	<input type="text" value="1"/>	<input type="text" value="すべて"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

項目	内容
<b>PVID</b>	ポートVLAN IDを指定します。このポートで受信されたUntaggedフレームは、ここで指定した番号のVLANとして認識されます(指定範囲:1～4094)。
<b>受信するフレームの種類</b>	<p><b>すべて</b> Untaggedフレーム、Taggedフレームの両方を受信します。</p> <p><b>Taggedのみ</b> Taggedフレームのみを受信しUntaggedフレームは破棄します。</p>
<b>イングレスフィルター</b>	<p><b>有効</b> 受信フレームのVLAN IDが受信ポートのVLANメンバーでない場合はフレームを破棄します。</p> <p><b>無効</b> すべてのTaggedフレームとUntaggedフレームを受信します。</p>
<b>プロテクトポート</b>	プロテクトポートが有効になっているポート同士は通信ができなくなります。異なるポートに接続した機器との間で通信をさせたくない場合に設定してください。

## ルーティング

### レイヤー設定

本製品の動作モードを設定します。

基本設定 > ルーティング > レイヤー設定

モード設定	
モード	<input type="radio"/> レイヤー3モード <input checked="" type="radio"/> レイヤー2モード

適用

項目	内容
モード	<p>本製品の動作モードを、以下の2つから選択します。</p> <p><b>レイヤー3モード</b> 本製品はレイヤー3スイッチとして動作します。</p> <p><b>レイヤー2モード</b> 本製品はレイヤー2スイッチとして動作します。</p>

**メモ:** モードを切り替えると、静的ルーティングの設定およびVLAN 2以降のVLANが削除されます。

## 静的ルーティング

レイヤー3モード時のみ表示されます。特定のネットワークへアクセスする際に通過するゲートウェイを設定します。

### 基本設定 > ルーティング > 静的ルーティング

静的ルーティング数

現在の静的ルーティング数: 0/32

デフォルトゲートウェイ

IPアドレス

0.0.0.0

適用

静的ルーティング設定

ネットワーク

サブネットマスク

ゲートウェイ

追加

静的ルーティング情報

<input type="checkbox"/>	インデックス	ネットワーク	サブネットマスク	ゲートウェイ	インターフェース	プロトコル
<input type="checkbox"/>	1	192.168.1.0	255.255.255.0	Connected	vlan1	Local

削除

項目	内容
静的ルーティング数	現在設定されている静的ルーティングの数を表示します。
デフォルトゲートウェイ	指定されていないネットワークへアクセスする際に使用するゲートウェイアドレスを入力します。
静的ルーティング設定	<p>以下の項目を入力して、静的ルーティングを設定します。作成できる静的ルートは、32個までです。</p> <p><b>ネットワーク</b> ゲートウェイを設定するネットワークのIPアドレスを入力します。</p> <p><b>サブネットマスク</b> 入力したネットワークアドレスのサブネットマスクを入力します。</p> <p><b>ゲートウェイ</b> 指定したネットワークへアクセスするときに通過するゲートウェイアドレスを入力します。</p>

項目	内容
静的ルーティング情報	設定されている静的ルーティングの情報を表示します。

## SNMP

SNMPを使用するには、別途SNMPモニタリングソフトが必要です。

### SNMPコミュニティテーブル

SNMPコミュニティテーブルを設定します。

基本設定 > SNMP > SNMPコミュニティテーブル

#	コミュニティ名	Get	Set	Trap
1	public	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

適用

項目	内容
コミュニティ名	コミュニティ名を設定します(半角英数字、“-”(ハイフン)、“_”(アンダースコア)で31文字まで)。
Get	コミュニティのメンバーに対して、スイッチのSNMP情報への読み取りアクセスを許可します。
Set	コミュニティのメンバーに対して、スイッチのSNMP情報への書き込みアクセスを許可します。
Trap	コミュニティのメンバーがSNMPトラップを受信できるようにします。

## SNMPホストテーブル

SNMPホストテーブルを設定します。

**メモ:** 登録したホストを削除する場合は、ホスト名とIPアドレスを空欄にして[適用]をクリックしてください。

### 基本設定 > SNMP > SNMPホストテーブル

ホスト認証 ☐ 有効

#	ホスト名	IPアドレス	コミュニティ名
1	<input type="text"/>	<input type="text"/>	public ▼
2	<input type="text"/>	<input type="text"/>	public ▼
3	<input type="text"/>	<input type="text"/>	public ▼
4	<input type="text"/>	<input type="text"/>	public ▼
5	<input type="text"/>	<input type="text"/>	public ▼
6	<input type="text"/>	<input type="text"/>	public ▼
7	<input type="text"/>	<input type="text"/>	public ▼
8	<input type="text"/>	<input type="text"/>	public ▼
9	<input type="text"/>	<input type="text"/>	public ▼
10	<input type="text"/>	<input type="text"/>	public ▼
11	<input type="text"/>	<input type="text"/>	public ▼
12	<input type="text"/>	<input type="text"/>	public ▼
13	<input type="text"/>	<input type="text"/>	public ▼
14	<input type="text"/>	<input type="text"/>	public ▼
15	<input type="text"/>	<input type="text"/>	public ▼
16	<input type="text"/>	<input type="text"/>	public ▼

適用

項目	内容
ホスト認証	SNMPのホスト認証の有効/ 無効を設定します。 有効にすると、指定されたIPアドレスのSNMPマネージャーからのみSNMPのサービスを提供します。読み書き権限はコミュニティによって決定されます。無効にすると、任意のホストからのSNMP要求を受け付けます。読み書き権限はコミュニティによって決定されます。
ホスト名	SNMP要求を許可するホストの名前を設定します。任意の名称を1文字以上入力してください(半角英数字、“-”(ハイフン)、“_”(アンダースコア)で31文字まで)。
IPアドレス	SNMP要求を許可するホストのIPv4/IPv6アドレスを設定します。 <b>メモ:</b> IPv6アドレスのホストと通信する場合は、本製品のIPv6を有効にする必要があります。
コミュニティ名	ホストのコミュニティを選択します。コミュニティはSNMPコミュニティテーブル設定画面で事前に設定しておく必要があります。

## SNMPトラップ

SNMPトラップを設定します。

**メモ:** SNMPトラップを使用する場合は、[基本設定]－[SNMP]－[SNMPホストテーブル]の画面で、トラップを受信するホストをホストテーブルに登録し、コミュニティのトラップ属性を有効にします。一度トラップを有効にしたホストをホストテーブルに登録すると、ホスト認証を無効にしてもトラップを送信します。トラップ送信を中止したい場合は、トラップホストをホストテーブルから削除してください。

### 基本設定 > SNMP > SNMPトラップ

以下の画面に表示される項目は、お使いの製品によって異なります。表示される項目については、後述の表を参照してください。

■ SNMPトラップ (複数選択可)
<input type="checkbox"/> 認証トラップ
<input type="checkbox"/> リンクアップ/ダウン
<input type="checkbox"/> STP
<input type="checkbox"/> ループ検知
<input type="checkbox"/> トランク
<input type="checkbox"/> PoEオーバーロード
<input type="checkbox"/> PoE 給電/非給電

本製品で対応しているトラップは以下のとおりです。

- coldStart
- warmStart
- LinkDown(リンクアップ/ダウン)
- LinkUp(リンクアップ/ダウン)
- authenticationFailure(認証トラップ)
- topologyChange(STP)
- LoopDetection(ループ検知)  
プライベートMIB OID 1.3.6.1.4.1.5227.28.1.1.1
- Trunk(トランク)  
プライベートMIB OID 1.3.6.1.4.1.5227.28.1.1.2  
トランクのリンク状態によって以下のように変化します。
  - 1.3.6.1.4.1.5227.28.1.2.1(トランクキー 1-8)
  - 1.3.6.1.4.1.5227.28.1.2.2(リンクアップ:1、リンクダウン:2)
- FanError(FANエラー)([「FAN搭載製品」\(P.115\)](#)のみ)  
プライベートMIB OID 1.3.6.1.4.1.5227.28.1.1.3  
本製品のファンにエラーが発生した場合は以下のとおりになります。  
プライベートMIB OID 1.3.6.1.4.1.5227.28.1.4.1  
<戻り値>
  - 1:FAN1でエラー発生
  - 2:FAN2でエラー発生
  - 3:FAN1とFAN2でエラー発生

• **PoeOverload(PoEオーバーロード)、PoE Power Deliver(PoE給電)(PoE対応製品のみ)**

標準MIB OID 1.3.6.1.2.1.105.1.1.1.6. <ポート番号>

1.3.6.1.2.1.105 PowerEthernetMIB(PoE) / RFC3621

<戻り値>

2:PoE状態が非給電

3:PoE状態が給電

5:本製品の供給電力が以下の最大値を超えている

・BS-GS2108P:90W

・BS-GS2116P、BS-GS2124P:180W

・BS-GS2124P/HP:384W

6:本製品1ポートあたりの供給電力が最大値(30W)を超えている

**メモ:**

- ・「coldStart」「warmStart」以外は有効/無効を切り替えることができます。
- ・プライベートMIBを使用するには、SNMPマネージャーに本製品のプライベートMIB定義ファイルを登録する必要があります。本製品のプライベートMIB定義ファイルは、当社ホームページ([https://www.buffalo.jp/support/download/detail/?dl\\_contents\\_id=60674](https://www.buffalo.jp/support/download/detail/?dl_contents_id=60674))からダウンロードしてください。

項目	内容
<b>SNMPトラップ</b>	以下のすべてのトラップを有効または無効にします。
<b>認証トラップ</b>	有効にすると、コミュニティ名が異なる、許可されていないIPアドレスからSNMPの要求があったときにトラップを送信します。
<b>リンクアップ/ダウン</b>	有効にすると、ポートのリンクアップ/ダウンが検知されたときにトラップを送信します。
<b>STP</b>	有効にすると、STP/RSTP/MSTPのトポロジーチェンジが発生したときにトラップを送信します。
<b>ループ検知</b>	有効にすると、ループ検知したときにトラップを送信します。
<b>トランク</b>	有効にすると、トランクが形成または解除されたときにトラップを送信します。
<b>FANエラー</b> (「 <a href="#">FAN搭載製品</a> 」 ( <a href="#">P.115</a> )のみ)	有効にすると、FANにエラーが発生したときにトラップを送信します。
<b>PoEオーバーロード</b> (PoE対応製品のみ)	有効にすると、PoEオーバーロードが検知されたときにトラップを送信します。
<b>PoE給電/非給電</b> (PoE対応製品のみ)	有効にすると、PoE状態の給電/非給電の変化を検知したときにトラップを送信します。

## SNMPv3ユーザー

SNMPv3で認証するユーザーを設定します。SNMPv3ではコミュニティ名ではなくユーザー名で認証し、認証は暗号化できます。本製品は、以下の認証方式・暗号化方式に対応しています。

認証方式：HMAC-MD5-96/HMAC-SHA-96

暗号化方式：CBC-DES/CFB-AES-128

### 基本設定 > SNMP > SNMPv3ユーザー

エンジンID: XX XX XX XX XX XX XX XX XX XX XX (16進数)

#	ユーザー名	アクセス制限	認証方式	認証キー	暗号化方式	暗号化キー
1	admin	読み込みのみ ▼	なし ▼		なし ▼	
2		読み込みのみ ▼	なし ▼		なし ▼	
3		読み込みのみ ▼	なし ▼		なし ▼	
4		読み込みのみ ▼	なし ▼		なし ▼	
5		読み込みのみ ▼	なし ▼		なし ▼	

適用

項目	内容
エンジンID	SNMPエンジンを識別するための、本製品固有のIDです。このIDは、SNMPv3通信を行ったとき、相手側に通知されます。
ユーザー名	認証するユーザー名を入力します(半角英数字、“-”(ハイフン)、“_”(アンダースコア)で32文字まで)。
アクセス制限	<p>ユーザーのアクセスを制限します。</p> <p><b>読み込みのみ</b> ユーザーによる書き込みを禁止します。</p> <p><b>読み込み/書き込み</b> ユーザーによるアクセスを制限しません。</p>
認証方式	ユーザーを認証する方式を設定します。
認証キー	認証方式に対応するキーを入力します。
暗号化方式	認証を暗号化する方式を設定します。
暗号化キー	暗号化方式に対応するキーを入力します。



# LLDP

## 設定

LLDPを設定します。

基本設定 > LLDP > 設定

LLDPプロパティ		
LLDP送信間隔	<input type="text" value="30"/>	(5-32768 秒)
Hold Multiplier	<input type="text" value="4"/>	(2-10)
Reinitializing Delay	<input type="text" value="2"/>	(1-10 秒)
Transmit Delay	<input type="text" value="2"/>	(1-8192 秒)
<input type="button" value="適用"/>		

LLDP-MEDプロパティ		
Fast Start Duration	<input type="text" value="3"/>	回
<input type="button" value="適用"/>		

項目	内容
LLDP送信間隔	LLDPパケットを送信する間隔を指定します(5～32768秒)。
Hold Multiplier	LLDPパケットを受信した機器が情報を保持する時間(TTL)がLLDP送信間隔の何倍になるかを設定します(2～10)。
Reinitializing Delay	LLDPの送信を無効にしてからもう一度有効になるまでの遅延時間を設定します(1～10秒)。
Transmit Delay	LLDPの設定が変更されてからLLDPパケットが送信されるまでの遅延時間を設定します(1～8192秒)。
Fast Start Duration	LLDP-MED対応機器を検出した直後に、LLDPパケットを送信する回数を指定します(1～10回)。

## LLDPポート

ポートごとにLLDPを設定します。

### 基本設定 > LLDP > LLDPポート

[注意]  
通知を有効にする場合、SNMP Trap設定が必要です。

ポート	ステータス	通知	Port Description TLV	System Name TLV	System Description TLV	System Capabilities TLV	Management Address TLV
1	Tx and Rx ▼	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	Tx and Rx ▼	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	Tx and Rx ▼	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	Tx and Rx ▼	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	Tx and Rx ▼	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6	Tx and Rx ▼	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7	Tx and Rx ▼	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8	Tx and Rx ▼	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

適用

項目	内容
ステータス	<p><b>無効</b> 送信も受信もしません。</p> <p><b>Tx Only</b> 送信のみ行います。</p> <p><b>Rx Only</b> 受信のみ行います。</p> <p><b>Tx and Rx</b> 送受信を行います。</p>
通知	<p>有効にすると、本製品の近隣の機器情報が更新されたときにSNMPトラップをSNMPサーバーに送信します。  <b>メモ:</b> 本機能を使用する際は、SNMPマネージャーとSNMPトラップの設定が必要です。</p>
Port Description TLV	有効にすると、LLDPパケットにポート情報(ポート番号)を含めます。
System Name TLV	<p>有効にすると、LLDPパケットにスイッチ名を含めます。  <b>メモ:</b> スイッチ名は、[基本設定] - [システム情報設定]で設定します。</p>
System Description TLV	有効にすると、LLDPパケットに本製品の製品名を含めます。
System Capabilities TLV	<p>有効にすると、LLDPパケットにSystem Capabilitiesを含めます。  System Capabilitiesは、製品の持つ機能(ブリッジ、ルーター、無線LANなど)を示します。本製品のSystem Capabilitiesはブリッジ、ルーターです。</p>
Management Address TLV	有効にすると、LLDPパケットに本製品のIPアドレスを含めます。

## LLDP-MEDポート

ポートごとにLLDP-MEDを設定します。

### 基本設定 > LLDP > LLDP-MEDポート

[注意]  
LLDP-MEDを使用する場合、LLDPポート設定を有効にする必要があります。

ポート	ステータス	通知	Capabilities TLV	Network Policy TLV	Extend Power TLV	Software Revision TLV
1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

適用

項目	内容
ステータス	有効にすると、LLDP-MEDの送信を行います。 <b>メモ:</b> 本機能を使用するには、「LLDPポート設定」で、ステータスを「Tx Only」か「Tx and Rx」に設定する必要があります。
通知	有効にすると、本製品近隣の機器情報の中でLLDP-MEDの情報が更新されたときに、SNMPトラップをSNMPサーバーに送信します。 <b>メモ:</b> 本機能を使用するには、SNMPマネージャーとSNMPトラップの設定が必要です。
Capabilities TLV	有効にすると、LLDPパケットにCapabilitiesを含めます。 Capabilitiesは、製品が対応しているLLDP-MEDのTLVを示します。本製品が対応している (Capabilities TLVが示す) TLVは、LLDP-MED Capabilities、Network Policy、Extended Power via MDI - PSE、Inventory (Software Revision) です。
Network Policy TLV	有効にすると、LLDPパケットにNetwork Policyを含めます。 VoIP自動優先を有効にしているときにLLDPパケットに含まれます。本製品のアプリケーションタイプはVoiceです。
Extend Power TLV (PoE対応製品のみ)	有効にすると、LLDPパケットにExtend Powerを含めます。 Extended Powerは、PoE機器としての状態を示します。本製品のPower TypeはPSEです。Power Priorityは[PoE] - [PoEプロファイル設定]で設定した優先度を示します。Power valueは給電中の電力を示します。
Software Revision TLV	有効にすると、LLDPパケットに本製品のファームウェアバージョンを含めます。ファームウェアバージョンはInventoryに含まれます。

## 隣接機器情報

本製品に接続されているLLDPに対応した製品の情報を表示します。

### 基本設定 > LLDP > 隣接機器情報

MSAPエントリーナンバー	ローカルポート	Chassis ID Subtype	Chassis ID	Port ID Subtype	Port ID	システム名	
---------------	---------	--------------------	------------	-----------------	---------	-------	--

更新

項目	内容
MSAPエントリーナンバー	検出した機器の通し番号を表示します。
ローカルポート	検出した機器が本製品のどのポートに接続しているかを表示します。
Chassis ID Subtype	検出した機器のChassis IDの種類を表示します。
Chassis ID	検出した機器のChassis IDを表示します。
Port ID Subtype	検出した機器のPort IDの種類を表示します。
Port ID	検出した機器のPort IDを表示します。
システム名	検出した機器のシステム名を表示します。
詳細	<p>クリックすると、隣接機器の詳細情報を表示します。</p> <p><b>メモ:</b> 詳細情報を表示するには、あらかじめ「LLDPポート」、「LLDP-MEDポート」を設定しておく必要があります。</p>

**メモ:** 本機能を使用するには、[基本設定]－[LLDP]－[LLDPポート]でステータスを「Rx Only」または「Tx and Rx」に設定する必要があります。

## MACアドレス

### MACアドレス学習方式

MACアドレス学習方式を設定します。

基本設定 > MACアドレス > MACアドレス学習方式

モード設定	
モード	<input checked="" type="radio"/> SVL
	<input type="radio"/> IVL

適用

項目	内容
モード	MACアドレス学習方式を、以下の2つから選択します。  <b>SVL</b> MACアドレス学習方式はSVL形式として動作します。  <b>IVL</b> MACアドレス学習方式はIVL形式として動作します。

**メモ:**

- MACアドレス学習方式の変更を完了するには、本製品を再起動する必要があります。
- MACアドレス学習方式を変更すると、静的MACフィルターと静的MACアドレスの設定、およびMACアドレステーブルは削除されます。

## 静的MACフィルター

手動で登録したMACアドレスをフィルターする静的MACフィルターを設定します。設定すると、MACアドレスが登録されているポートでは、登録されているMACアドレスをソースMACアドレスに持つフレームのみ通過し、それ以外のフレームは通過できません。フレームのフィルターは、ポートに入ってくるフレームに対して行われます。

### 基本設定 > MACアドレス > 静的MACフィルター

静的MACフィルター
☐ 有効

静的MACフィルター設定
通信を許可するMACアドレスを入力します。

MACアドレス
例: 00:11:22:33:44:55

VLAN ID
 (1-4094)

ポート番号
 1 ▼

適用

静的MACフィルターリスト

<input type="checkbox"/> インデックス	ポート	MACアドレス	VLAN ID
削除			

項目	内容
静的MACフィルター	「有効」にチェックを入れると、静的MACフィルター機能が有効になります。
MACアドレス	フィルターを適用する機器のMACアドレスを入力します(入力例 00:11:22:aa:bb:cc)。 1ポートあたり最大16個まで登録できます。
VLAN ID	MACアドレスの学習方式がIVL方式の場合、静的MACフィルターを適用するVLAN IDを選択します。
ポート番号	静的MACフィルターを適用するポートを選択します。
静的MACフィルターリスト	追加した静的MACアドレスとポート番号を表示します。

**メモ:** マルチキャストMACアドレス、VRRP MACアドレス(00:00:5E:00:01:XX)、ブロードキャストMACアドレスには対応していません。

## 動的MACフィルター

動的MACフィルターを設定します。学習するMACアドレスの上限値をポートごとに設定できます。

### 基本設定 > MACアドレス > 動的MACフィルター

動的MACフィルター <input type="checkbox"/> 有効	
ポート	設定台数
1	<input type="text"/>
2	<input type="text"/>
3	<input type="text"/>
4	<input type="text"/>
5	<input type="text"/>
6	<input type="text"/>
7	<input type="text"/>
8	<input type="text"/>

MACアドレスの学習を許可する台数を入力してください。  
各ポートで1～16384の範囲で設定できますが、製品全体でMACアドレスは16384個までしか学習できません。

項目	内容
動的MACフィルター	「有効」にチェックを入れると、動的MACフィルター機能を有効にします。
設定台数	ポートごとに動的MACアドレスの学習を許可する台数を設定します(1～16384)。

#### メモ:

- 設定台数が空白状態で設定されたポートは、すべてのMACアドレスが許可される設定になります。
- 各ポートで1～16384の範囲で設定できますが、製品全体でMACアドレスは16384個までしか学習できません。16384個を超えた場合、MACアドレスは学習されずに破棄されます。
- 静的MACフィルターと動的MACフィルターが両方とも有効の場合、静的MACフィルターに登録されたMACアドレスは動的MACフィルターの台数にカウントされません。

## MACアドレス変換

学習したMACアドレスを静的MACフィルターリストに追加できます。

基本設定 > MACアドレス > MACアドレス変換

動的MACアドレスを静的MACフィルターリストに追加

ポート番号

1 ▼

追加

☐ インデックス
 ☐ ポート
 ☐ MACアドレス
 ☐ VLAN ID

更新

項目	内容
動的MACアドレスを静的MACフィルターリストに追加	ポート番号を選択すると、そのポートで学習した動的MACアドレスが表示されます。静的MACフィルターリストに追加したいMACアドレスを選択し、[追加]をクリックすると、選択した動的MACアドレスが静的MACフィルターリストに追加されます。

## 静的MACアドレス

MACアドレステーブルに静的にMACアドレスを登録します。そのMACアドレスを持つ機器は、そのポートでのみ通信できます。[管理]－[MACアドレステーブル]から、静的に登録されていることを確認できます。

基本設定 > MACアドレス > 静的MACアドレス

静的MACアドレス設定

MACアドレス

例: 00:11:22:33:44:55

VLAN ID

(1-4094)

ポート番号:

1 ▼

リストに追加

静的MACアドレス

☐ インデックス
 ☐ ポート
 ☐ MACアドレス
 ☐ VLAN ID

削除

項目	内容
MACアドレス	登録するMACアドレスを入力します。製品全体で256個のMACアドレスを登録できます。
VLAN ID	MACアドレスの学習方式がIVL方式の場合、どのVLAN IDに静的MACアドレスを登録するかを指定します。



項目	内容
ポート番号	どのポートに静的MACアドレスを登録するかを指定します。
静的MACアドレス	登録した静的MACアドレスを表示します。

**メモ:**

- マルチキャストMACアドレス、VRRP MACアドレス(00:00:5E:00:01:XX)、ブロードキャストMACアドレスには対応していません。
- 静的MACアドレスに登録した機器は、VLAN内では登録したポート以外では通信できません。

## MACアドレスエージング

MACアドレスエージングタイムを設定します。MACアドレスエージングタイムは、本製品がMACアドレスを最後に参照してから削除されるまでの時間です。

### 基本設定 > MACアドレス > MACアドレスエージング

MACエージングタイム設定

エージングタイム:  (10-1000000 秒)

適用

項目	内容
エージングタイム	本製品がMACアドレスを最後に参照してから削除されるまでの時間を設定します。

## ポート設定

### ステータス

ポートの状態を表示します。

基本設定 > ポート設定 > ステータス

ポート	ポート名	管理	リンク状況	オートネゴシエーション	速度/通信方式	フロー制御	IEEE 802.3az	APD	Jumbo Frame
1	Port 1	On	Up	On	1000Mbps-全二重	Off	Off	On	On
2	Port 2	On	Down	On		Off	Off	On	On
3	Port 3	On	Down	On		Off	Off	On	On
4	Port 4	On	Down	On		Off	Off	On	On
5	Port 5	On	Down	On		Off	Off	On	On
6	Port 6	On	Down	On		Off	Off	On	On
7	Port 7	On	Down	On		Off	Off	On	On
8	Port 8	On	Down	On		Off	Off	On	On

項目	内容
ポート名	ポートの名前を表示します。
管理	ポートの有効(On)または無効(Off)を表示します。
リンク状況	リンクのUpまたはDownを表示します。
オートネゴシエーション	通信のオートネゴシエーションによる自動設定の有効(On)または無効(Off)を表示します。
速度/通信方式	通信速度および通信方式の状態を表示します。
フロー制御	フロー制御の有効(On)または無効(Off)を表示します。
IEEE 802.3az	アイドリングストップ(IEEE802.3az)の有効(On)または無効(Off)を表示します。
APD	APD(Auto Power Down)の有効(On)または無効(Off)を表示します。
Jumbo Frame	Jumboフレームが有効(On)または無効(Off)であることを表示します。 <b>メモ:</b> 本製品が転送できるJumboフレームは12,288バイトまでです。

## 速度/モード設定

ポートの通信速度やフロー制御などを設定します。

### 基本設定 > ポート設定 > 速度/モード設定

ポート	ポート名	管理 ✓	速度/通信方式 ▼	フロー制御 ■	IEEE 802.3az ■	APD ✓	Jumbo Frame ✓	ステータス
1	Port 1	✓	オートネゴシエーション ▼	<input type="checkbox"/>	<input type="checkbox"/>	✓	✓	オートネゴシエーション (1000 Mbps 全二重)
2	Port 2	✓	オートネゴシエーション ▼	<input type="checkbox"/>	<input type="checkbox"/>	✓	✓	-
3	Port 3	✓	オートネゴシエーション ▼	<input type="checkbox"/>	<input type="checkbox"/>	✓	✓	-
4	Port 4	✓	オートネゴシエーション ▼	<input type="checkbox"/>	<input type="checkbox"/>	✓	✓	-
5	Port 5	✓	オートネゴシエーション ▼	<input type="checkbox"/>	<input type="checkbox"/>	✓	✓	-
6	Port 6	✓	オートネゴシエーション ▼	<input type="checkbox"/>	<input type="checkbox"/>	✓	✓	-
7	Port 7	✓	オートネゴシエーション ▼	<input type="checkbox"/>	<input type="checkbox"/>	✓	✓	-
8	Port 8	✓	オートネゴシエーション ▼	<input type="checkbox"/>	<input type="checkbox"/>	✓	✓	-

適用

項目	内容
ポート名	ポートに任意の名前を指定します(“-”(ハイフン)、“_”(アンダースコア)、スペースを含む半角英数字で15文字まで)。
管理	選択したポートの設定を有効(通信可)または無効(通信不可)にします。
速度/通信方式	<p>通信速度、通信方式を「オートネゴシエーション」、「100 Mbps 全二重」、「100 Mbps 半二重」、「10 Mbps 全二重」、「10 Mbps 半二重」から選択します。 16ポート製品のポート17・18は、「オートネゴシエーション」から変更できません。</p> <p><b>オートネゴシエーション</b> 本製品に接続する機器によって、通信速度や通信方式を自動調整します。 通常はこちらに設定してください。</p> <p><b>100 Mbps 全二重、100 Mbps 半二重、10 Mbps 全二重、10 Mbps 半二重</b> 表示の通信速度、通信方式に固定します。</p>
フロー制御	フロー制御を有効または無効にします。
IEEE 802.3az	アイドリングストップ(IEEE802.3az)を有効または無効にします。
APD	APD(Auto Power Down)を有効または無効にします。有効にすると、リンクダウンしているポートの消費電力を抑えることができます。
Jumbo Frame	選択したポートのJumboフレーム設定を有効または無効にします。
ステータス	現在の通信速度および通信方式の状態を表示します。

## システムセキュリティ

### アカウント管理

本製品にログインするためのパスワードを設定します。

基本設定 > システムセキュリティ > アカウント管理

ユーザー名/パスワード	
管理ユーザー名	<input type="text" value="admin"/>
管理パスワード	<input type="password"/>
管理パスワード(確認)	<input type="password"/>
<input type="button" value="適用"/>	

項目	内容
管理ユーザー名	本製品にログインするためのユーザー名です(半角英数字、“-”(ハイフン)、“_”(アンダースコア)で8文字まで)。
管理パスワード	本製品にログインするためのパスワードを入力します。 半角英数字、“-”(ハイフン)、“_”(アンダースコア)で1～32文字まで設定できます。
管理パスワード(確認)	上記に入力したパスワードをもう一度入力します。

### アクセス管理

各種管理インターフェースを設定します。

基本設定 > システムセキュリティ > アクセス管理

サーバー設定	
SNMP	<input type="button" value="有効"/> ▼
HTTPS	<input type="button" value="無効"/> ▼
Webセッション設定	
Webセッションタイムアウト時間	<input type="text" value="5"/> (1-60 分)
Web最大セッション数	<input type="text" value="5"/> (1-64)
HTTPS	
ポート	<input type="text" value="443"/> (1-65535)
HTTPSセッションタイムアウト時間	<input type="text" value="5"/> (1-60 分)
HTTPS最大セッション数	<input type="text" value="2"/> (1-2)

項目	内容
SNMP	SNMP管理インターフェースを有効または無効にします。
HTTPS	HTTPS管理インターフェースを有効または無効にします。 <b>メモ:</b> 本機能を使用するには、[基本設定]－[システムセキュリティ]－[証明書]の画面でSSL証明書をアップロードする必要があります。

項目	内容
<b>Webセッションタイムアウト時間</b>	Web管理インターフェースへHTTPで接続したときのタイムアウト時間を設定します。
<b>Web最大セッション数</b>	Web管理インターフェースへHTTPで接続したときの最大セッション数を設定します。
<b>ポート</b>	HTTPS接続する際のポート番号を指定します。
<b>HTTPSセッションタイムアウト時間</b>	Web管理インターフェースへHTTPSで接続したときのタイムアウト時間を設定します。
<b>HTTPS最大セッション数</b>	Web管理インターフェースへHTTPSで接続したときの最大セッション数を設定します。

## 証明書

証明書のアップロード、ダウンロードを行います。HTTPS通信するための証明書は、お客様ご自身でご用意いただくか、スイッチが自動生成したものをお使いください。

証明書を自動生成するには、「証明書」画面の[削除]をクリックし、証明書を削除した状態で本製品を再起動してください。

対応する証明書タイプは以下のとおりです。

項目	対応方式
証明書形式	X.509
プライベートキー	RSA 2048bitまで(暗号化なしのみ対応)
ハッシュアルゴリズム	SHA1、SHA256、SHA384、SHA512

証明書は以下のようにプライベートキーを含める必要があります。

```
-----BEGIN CERTIFICATE-----
...
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
...
-----END RSA PRIVATE KEY-----
```

基本設定 > システムセキュリティ > 証明書

HTTPS証明書のアップロード

証明書ファイル

選択

アップロード

HTTPS証明書のダウンロード

SSL証明書をスイッチからダウンロードします。

ダウンロード

SSL証明書情報	
名称	概要
Buffalo_Self_Generation	CN=BSXXXXXXXXXXXX, O=Buffalo Inc.
削除	

項目	内容
HTTPS証明書のアップロード	HTTPSの証明書をアップロードします。
HTTPS証明書のダウンロード	HTTPSの証明書をダウンロードします。
SSL証明書情報	アップロードした証明書の情報が表示されます。[削除]をクリックすると、アップロードした証明書を削除します。 <b>メモ:</b> 証明書を削除した状態で本製品を再起動すると、スイッチが証明書を自動生成します。

## 日付と時刻

SNTPや手動で時刻を設定します。

### 基本設定 > 日付と時刻

<b>自動時刻設定</b>						
SNTP	<input type="checkbox"/> 有効					
<b>手動時刻設定</b>						
時刻設定	YYYY	MM	DD	hh	mm	ss
	2021	/ 01	/ 01	02	: 29	: 00
<input type="button" value="パソコンから現在の時刻を取得"/>						
<b>SNTPサーバー設定</b>						
サーバーIPアドレス/FQDN	ntp.jst.mfeed.ad.jp					
更新間隔	24 (1~24時間)					
タイムゾーン	(GMT+09:00) Osaka, Sapporo, Tokyo ▼					

項目	内容
SNTP	SNTPサーバーからの時刻取得を有効または無効に設定します。
時刻設定	SNTPが無効の場合に、時刻を設定します。
サーバーIPアドレス/ FQDN	SNTPサーバーのIPアドレスまたはDNS解決可能なホスト名(FQDN)を設定します。FQDNを設定する場合は、[基本設定] - [VLAN] - [VLAN設定]画面でDNSサーバーを設定してください。
更新間隔	SNTPサーバーに時刻を問い合わせる間隔(時間)を指定します。
タイムゾーン	タイムゾーンを設定します。

## PoE(PoE対応製品のみ)

### PoEステータス

PoEの状態を表示します。

基本設定 > PoE > PoEステータス

電力						
最大:		90000 mW				
使用中:		0 mW				
使用可能:		90000 mW				
ポート	PoE	ステータス	クラス	優先度	供給電力 (mW)	電流値 (mA)
1	有効	非給電	0	低	0	0
2	有効	非給電	0	低	0	0
3	有効	非給電	0	低	0	0
4	有効	非給電	0	低	0	0
5	有効	非給電	0	低	0	0
6	有効	非給電	0	低	0	0
7	有効	非給電	0	低	0	0
8	有効	非給電	0	低	0	0

項目	内容
電力	供給可能な最大電力、現在使用中の電力、使用可能な電力を表示します。 <b>※モ:</b> 供給可能な最大電力は以下のとおりです。 BS-GS2108P: 最大90 W(90000 mW) BS-GS2116P: 最大180 W(180000 mW) BS-GS2124P: 最大180 W(180000 mW) BS-GS2124P/HP: 最大384 W(384000 mW)
PoE	PoE機能の有効/無効を表示します。
ステータス	PoEの給電状態を表示します。
クラス	接続された受電機器のクラスを表示します。
優先度	ポートごとの優先度を表示します。
供給電力	ポートごとの供給電力を表示します。
電流値	ポートごとの供給電流を表示します。



## PoEガードバンド

PoEの供給電力が供給能力の上限を超えないように制限します。

基本設定 > PoE > PoEガードバンド

ガードバンド電力設定	
ガードバンド電力	0 ▼ (W)

適用

項目	内容
ガードバンド電力	使用可能な電力が指定の値以下となった場合に、新しくPoEポートに接続したPoE機器に給電しないようにできます。供給能力の上限を超えることによる給電の停止を防止できます。 「0」、「10」、「20」、「30」、「40」から選択します。

## PoEプロフィール設定

PoEをプロフィールごとに設定します。各プロフィールは、「PoEスケジューラー」画面で使用します。

### 基本設定 > PoE > PoEプロフィール設定

Profile1
Profile2
Profile3
Profile4

プロフィール名

Profile1
変更

ポート	PoE ✓	優先度	ハイパワー
1	<input checked="" type="checkbox"/>	低▼	at▼
2	<input checked="" type="checkbox"/>	低▼	at▼
3	<input checked="" type="checkbox"/>	低▼	at▼
4	<input checked="" type="checkbox"/>	低▼	at▼
5	<input checked="" type="checkbox"/>	低▼	at▼
6	<input checked="" type="checkbox"/>	低▼	at▼
7	<input checked="" type="checkbox"/>	低▼	at▼
8	<input checked="" type="checkbox"/>	低▼	at▼

ランプを消灯する
消灯しない▼

[適用]をクリックすると、すべてのプロフィール設定の変更が反映されます。

適用
初期化

プロフィールをコピーする

コピー元: Profile1▼
コピー先: Profile1▼

プロフィールをコピーする

項目	内容
プロフィール名	プロフィール名を変更する場合は、新しいプロフィール名を入力して[変更]をクリックします。
PoE	PoE機能を有効/無効に設定します。
優先度	PoE給電の優先度を設定します。供給電力が最大値を超えた場合、優先度の高いポートを優先して電力を供給します。優先度が同じ場合は、ポート番号の小さいポートが優先されます。
ハイパワー	ハイパワー給電機能を設定します。  <b>無効</b> 802.3af対応機器に15.4Wまで給電できます。  <b>at</b> 802.3at対応機器に30Wまで給電できます。
ランプを消灯する	「消灯する」を選択すると、Powerランプ以外のランプが消灯状態となります。
初期化	[初期化]をクリックすると、選択しているプロフィールを初期化します。
プロフィールをコピーする	コピー元のプロフィールとコピー先のプロフィールを選択して[プロフィールをコピーする]をクリックすると、コピー元プロフィールと同じ設定がコピー先のプロフィールに設定されます。

**メモ:**

- LLDPによる動的な給電をする場合、[基本設定]－[LLDP]－[LLDPポート]の画面で、ステータスを「Tx and Rx」に設定する必要があります。
- 給電許容量を超えた場合、ポート番号の小さいものを優先して給電します。

## PoEスケジューラー

PoEスケジューラーを設定します。PoEスケジューラーは、複数のPoEプロファイル設定を手動、または日時を設定して自動的に切り替える機能です。時刻は15分単位で設定できます。

### 基本設定 > PoE > PoEスケジューラー



項目	内容
スケジューラー機能	<b>無効(手動切替)</b> 手動でプロファイルを切り替えます。
	<b>有効(自動切替)</b> 以下の設定に従って自動でプロファイルを切り替えます。  <b>メモ:</b> スケジューラー機能を有効にするには、SNTPを有効にしておく必要があります。SNTPが有効でもサーバーから時刻の取得ができない場合は、製品の内部時計に従ってスケジュール設定されているプロファイルが適用されます。
プロフィール(手動切替時)	スケジューラー機能無効時に使用するプロファイルを選択します。
スケジュール一覧	現在設定されているスケジュールの一覧が表示されます。[編集]をクリックすると、スケジュールを編集する画面に移動します。
表示	<b>週間スケジュール</b> 曜日ごとのスケジュールが表示されます。
	<b>すべてのスケジュール</b> 日付ごとのスケジュールが表示されます。

項目	内容
スケジュール一覧の[編集]	をクリックしたときに表示される画面
時間外に使用するプロファイル	スケジュールを設定していない時間帯に適用されるプロファイルを選択します。
指定方法	タイムテーブルの指定方法を選択します。
年月日	「指定方法」で「年月日」を選択した場合、タイムテーブルを追加する日付を指定します。
曜日	「指定方法」で「曜日と時刻」を選択した場合、タイムテーブルを追加する曜日を指定します。
期間	「指定方法」で「曜日と時刻」を選択した場合、タイムテーブルを追加する時間を指定します。
プロファイル選択	プロファイルの選択方法を指定します。「指定方法」で「曜日と時刻」を選択した場合は、「別の曜日のプロファイルを使用する」は選択できません。
プロファイル	「プロファイル選択」で「以下のプロファイルを使用する」を選択した場合、プロファイルを選択します。[確認]をクリックすると、各プロファイルのPoE設定状況を確認できます。
曜日	「プロファイル選択」で「別の曜日のプロファイルを使用する」を選択した場合、曜日を選択します。
スケジュール一覧	設定されているスケジュールの一覧が表示されます。

## QoS

### QoS設定

優先度を設定します。

詳細設定 > QoS > QoS設定

設定

QoS機能

☐ 有効

スケジュール方法

WRR ▼

優先度選択

☐ DSCP

☒ CoS

☐ IP Precedence

項目	内容
QoS機能	QoSを有効または無効に設定します。[詳細]をクリックすると、ポートごとにQoSの有効/無効を設定できます。

項目	内容
スケジュール方法	<p>キュースケジューリングのタイプを設定します。</p> <p><b>Strict</b> 絶対優先 (Strict Priority) に基づくキュースケジューリングを行います。キューの優先度の高いものから優先的に送信します。優先度の高いキューにデータが残っている場合は、それより優先度の低いキューからデータを送信できません。</p> <p><b>WRR</b> 重み付きラウンドロビン (Weighted Round Robin) に基づくキュースケジューリングを行います。それぞれのキューに指定されている出力データ数の比率や最大送信データ数に従って送信します。優先度の低いキューでも、ある一定の割合で送信できます。優先度は、0 (最低) ~ 7 (最高) の範囲で指定します。</p> <p><b>メモ:</b> VLAN タグのないパケットは、優先度の最も低いキューに入ります。</p>
優先度選択	DSCP、CoS、IP Precedence のうち使用する優先度パラメーターを選択します。

## QoSマッピング

DSCP、CoS、IP Precedence、ポートベースの各優先度を設定します。

### 詳細設定 > QoS > QoSマッピング

ポート優先度	
ポート	優先度
1	0 最低 ▼
2	0 最低 ▼
3	0 最低 ▼
4	0 最低 ▼
5	0 最低 ▼
6	0 最低 ▼
7	0 最低 ▼
8	0 最低 ▼
CoSマッピング	
CoS値	優先度
0	2 ▼
1	0 最低 ▼
2	1 ▼
3	3 ▼
4	4 ▼
5	5 ▼
6	6 ▼
7	7 最高 ▼

適用

項目	内容
ポート優先度	各ポートに対応する優先度を設定します。
DSCPマッピング	DSCPの0～63に対応する優先度を設定します。
CoSマッピング	CoSの0～7に対応する優先度を設定します。
IP Precedenceマッピング	IP Precedenceの0～7に対応する優先度を設定します。
優先度	優先度を0～7で設定します。

**メモ:** DSCPマッピング、CoSマッピング、IP Precedenceマッピングは、現在有効になっている設定のみ表示されます。

## VoIP優先制御

SIP, H.323, SCCPの優先制御を行います。

詳細設定 > QoS > VoIP優先制御

設定	
VoIP優先制御機能	<input type="checkbox"/> 有効 <a href="#">詳細</a>
CoS	7 ▼

[適用](#)

項目	内容
VoIP優先制御機能	VoIP優先制御機能を有効または無効にします。[詳細]をクリックすると、ポートごとに有効/無効を切り替えることができます。
CoS	SIP, H.323, SCCPのVoIPパケットにのみ適用され、指定したCoS値に書き換えます。QoSが有効になっている場合は、CoSの優先度に従って処理されます。

## IPv4/MACポリシー

DiffServで適用するポリシーを設定します。ここではMACアドレスおよびIPv4アドレスが指定できます。有効にしたポリシーは、スイッチにパケット/フレームが入力されたときに適用されます。

詳細設定 > QoS > DiffServ > IPv4/MACポリシー

ポリシー数	
現在のポリシー数	0/128
現在有効なポリシー数	0/128

ポリシー名	
<input type="checkbox"/>	<input type="text"/>
<a href="#">適用</a>	<a href="#">名前の変更</a> <a href="#">削除</a>

項目	内容
現在のポリシー数	作成したポリシーの数を表示します。
現在有効なポリシー数	作成したポリシーのうち、現在有効なものの数を表示します。
ポリシー名	空欄にポリシー名を入力し[適用]をクリックすると、新しいポリシーが作成されます。[詳細]をクリックすると、ポリシーの内容を詳細に設定できます。作成済みのポリシーにチェックを入れて入力欄に新しいポリシー名を入力し、[名前の変更]をクリックすると、チェックを入れたポリシーが入力した名前に変更されます。



以下の画面は、[詳細]をクリックしたときに表示されます。

IPv4/MACポリシー設定			
ポリシー名	001		
CoS	すべて ▼		
送信先MACアドレス	すべて ▼	アドレス: <input type="text"/>	マスク: <input type="text"/> (例: 00:11:22:33:44:55)
送信元MACアドレス	すべて ▼	アドレス: <input type="text"/>	マスク: <input type="text"/> (例: 00:11:22:33:44:55)
イーサertype	すべて ▼	<input type="text"/> (0600-FFFF Hex)	
VLAN	すべて ▼		
プロトコル	すべて ▼	<input type="text"/> (0-255)	
送信先IPv4アドレス	すべて ▼	アドレス: <input type="text"/>	マスク: <input type="text"/> (例: 0.0.0.0)
送信先ポート	すべて ▼	<input type="text"/> (0-65535)	
送信元IPv4アドレス	すべて ▼	アドレス: <input type="text"/>	マスク: <input type="text"/> (例: 0.0.0.0)
送信元ポート	すべて ▼	<input type="text"/> (0-65535)	
サービスの種類	<input checked="" type="radio"/> すべて <input type="radio"/> IP DSCP <input type="text"/> (0-63) <input type="radio"/> IP Precedence <input type="text"/> (0-7)		
DiffServポリシー			
<input checked="" type="radio"/> 許可 <input type="radio"/> 拒否			
<input type="radio"/> Egressキュー <input type="text"/> 0 最低 ▼			
<input type="radio"/> CoS書き換え <input type="text"/> 0 最低 ▼			
<input type="radio"/> DSCP書き換え <input type="text"/> (0-63)			
<input type="radio"/> IP Precedence書き換え <input type="text"/> (0-7)			
<input type="radio"/> 動作プロファイル			
<input type="button" value="保存"/> <input type="button" value="戻る"/>			

項目	内容
ポリシー名	選択したポリシー名が表示されます。
CoS	フレームのCoS値を条件に追加します。
送信先MACアドレス	フレームの送信先MACアドレスを条件に追加します。アドレスの入力方法については、下記の「アドレスとマスクについて」を参照してください。
送信元MACアドレス	フレームの送信元MACアドレスを条件に追加します。アドレスの入力方法については、下記の「アドレスとマスクについて」を参照してください。
イーサertype	フレームのイーサertypeを条件に追加します。
VLAN	フレームのVLAN IDを条件に追加します。
プロトコル	パケットのプロトコルを条件に追加します。
送信先IPv4アドレス	パケットの送信先IPv4アドレスを条件に追加します。アドレスの入力方法については、下記の「アドレスとマスクについて」を参照してください。
送信先ポート	パケットの送信先ポートを条件に追加します。
送信元IPv4アドレス	パケットの送信元IPv4アドレスを条件に追加します。アドレスの入力方法については、下記の「アドレスとマスクについて」を参照してください。
送信元ポート	パケットの送信元ポートを条件に追加します。
サービスの種類	パケットのサービスの種類を条件に追加します。 IP DSCP、IP Precedenceを選択した場合は、一つの値のみ指定できます。

項目	内容
DiffServポリシー	<p>上記で設定した条件を満たすとき、どのような操作を行うかを設定します。</p> <p><b>許可</b> 該当パケット/フレームの転送を許可します。</p> <p><b>拒否</b> 該当パケット/フレームを破棄します。</p> <p><b>Egressキュー</b> 該当パケット/フレームの処理優先度を変更します。</p> <p><b>CoS書き換え</b> 該当パケット/フレームのCoS値を、指定した値に書き換えます。</p> <p><b>DSCP書き換え</b> 該当パケット/フレームのDSCP値を、指定した値に書き換えます。</p> <p><b>IP Precedence書き換え</b> 該当パケット/フレームのToS Precedence値を、指定した値に書き換えます。</p> <p><b>動作プロファイル</b> 「指定レート」を基準に、該当パケット/フレームの処理方法を決定します。該当パケット/フレームが指定レート以下の場合は「プロファイル適合時」の動作になり、指定レートを超えた場合は「プロファイル不適合時」の動作になります。</p> <ul style="list-style-type: none"> <li>・ <b>指定レート</b> 該当パケット/フレームの処理方法を判別する通信レートを指定します。</li> <li>・ <b>指定バースト</b> 瞬間的に該当パケット/フレームが指定レートを超えた場合にプロファイル適合時の動作を行うバーストサイズを指定します。指定したサイズを超えた場合は、プロファイル不適合時の動作になります。</li> <li>・ <b>プロファイル適合時</b> 該当パケット/フレームが指定レート以下の場合の処理方法を指定します。</li> <li>・ <b>プロファイル不適合時</b> 該当パケット/フレームが指定レートを超えた場合の処理方法を指定します。CoS値の書き換えは指定できません。</li> </ul>

### アドレスとマスクについて

本製品のDiffServは、ワイルドカードマスクを採用しています。

送信先MACアドレス、送信元MACアドレスのマスクの設定は、以下の例を参考に行ってください。

- ・ 00:11:22:ab:cd:00～00:11:22:ab:cd:ffの範囲を指定したい場合  
「アドレス」欄に「00:11:22:ab:cd:00」、「マスク」欄に「00:00:00:00:00:ff」と入力します。
- ・ 00:11:22:ab:cd:efのみを指定したい場合  
「アドレス」欄に「00:11:22:ab:cd:ef」、「マスク」欄に「00:00:00:00:00:00」と入力します。

送信先IPv4アドレス、送信元IPv4アドレスのマスクの設定は、以下の例を参考に行ってください。

- ・ 192.168.1.0～192.168.1.254の範囲を指定したい場合  
「アドレス」欄に「192.168.1.0」、「マスク」欄に「0.0.0.255」と入力します。
- ・ 192.168.1.1のみを指定したい場合  
「アドレス」欄に「192.168.1.1」、「マスク」欄に「0.0.0.0」と入力します。

## IPv6ポリシー設定

DiffServで適用するポリシーを設定します。ここではIPv6アドレスが指定できます。有効にしたポリシーは、スイッチにパケット/フレームが入力されたときに適用されます。

### 詳細設定 > QoS > DiffServ > IPv6ポリシー

The screen shows the summary of IPv6 policy configuration. It includes a section for 'ポリシー数' (Policy Count) with '現在のポリシー数' (Current Policy Count) at 0/64 and '現在有効なポリシー数' (Currently Active Policy Count) at 0/64. Below this is a section for 'ポリシー名' (Policy Name) with a text input field and three buttons: '適用' (Apply), '名前の変更' (Change Name), and '削除' (Delete).

項目	内容
現在のポリシー数	作成したポリシーの数を表示します。
現在有効なポリシー数	作成したポリシーのうち、現在有効なものの数を表示します。
ポリシー名	空欄にポリシー名を入力し[適用]をクリックすると、新しいポリシーが作成されます。[詳細]をクリックすると、ポリシーの内容を詳細に設定できます。作成済みのポリシーにチェックを入れて入力欄に新しいポリシー名を入力し、[名前の変更]をクリックすると、チェックを入れたポリシーが入力した名前に変更されます。

以下の画面は、[詳細]をクリックしたときに表示されます。

The detailed configuration screen for an IPv6 policy. It shows the 'IPv6ポリシー設定' (IPv6 Policy Setting) section with fields for 'ポリシー名' (Policy Name) set to '002', '送信先IPv6アドレス' (Destination IPv6 Address) set to 'すべて' (All), and '送信元IPv6アドレス' (Source IPv6 Address) set to 'すべて' (All). Below this is the 'DiffServポリシー' (DiffServ Policy) section with radio buttons for '許可' (Allow) and '拒否' (Deny), and checkboxes for 'Egressキュー' (Egress Queue), 'CoS書き換え' (CoS Rewrite), 'DSCP書き換え' (DSCP Rewrite), and 'IP Precedence書き換え' (IP Precedence Rewrite), each with a dropdown menu. At the bottom are '保存' (Save) and '戻る' (Back) buttons.

項目	内容
ポリシー名	選択したポリシー名が表示されます。
送信先IPv6アドレス	パケットの送信先IPv6アドレスを条件に追加します。アドレスの入力方法については、下記の「アドレスとマスクについて」を参照してください。
送信元IPv6アドレス	パケットの送信元IPv6アドレスを条件に追加します。アドレスの入力方法については、下記の「アドレスとマスクについて」を参照してください。

項目	内容
DiffServポリシー	<p>上記で設定した条件を満たすとき、どのような操作をするかを設定します。</p> <p><b>許可</b> 該当パケット/フレームの転送を許可します。</p> <p><b>拒否</b> 該当パケット/フレームを破棄します。</p> <p><b>Egressキュー</b> 該当パケット/フレームの処理優先度を変更します。</p> <p><b>CoS書き換え</b> 該当パケット/フレームのCoS値を、指定した値に書き換えます。</p> <p><b>DSCP書き換え</b> 該当パケット/フレームのDSCP値を、指定した値に書き換えます。</p> <p><b>IP Precedence書き換え</b> 該当パケット/フレームのToS Precedence値を、指定した値に書き換えます。</p> <p><b>動作プロファイル</b> 「指定レート」を基準に、該当パケット/フレームの処理方法を決定します。該当パケット/フレームが指定レート以下の場合は「プロファイル適合時」の動作になり、指定レートを超えた場合は「プロファイル不適合時」の動作になります。</p> <ul style="list-style-type: none"> <li>• <b>指定レート</b> 該当パケット/フレームの処理方法を判別する通信レートを指定します。</li> <li>• <b>指定バースト</b> 瞬間的に該当パケット/フレームが指定レートを超えた場合にプロファイル適合時の動作を行うバーストサイズを指定します。指定したサイズを超えた場合は、プロファイル不適合時の動作になります。</li> <li>• <b>プロファイル適合時</b> 該当パケット/フレームが指定レート以下の場合の処理方法を指定します。</li> <li>• <b>プロファイル不適合時</b> 該当パケット/フレームが指定レートを超えた場合の処理方法を指定します。CoS値の書き換えは指定できません。</li> </ul>

### アドレスとマスクについて

本製品のDiffServは、ワイルドカードマスクを採用しています。送信先IPv6アドレス、送信元IPv6アドレスのマスクの設定は、以下の例を参考に行ってください。

- 2001:db8::~2001:db8::ffffの範囲を指定したい場合  
「アドレス」欄に「2001:db8::」、「マスク」欄に「::ffff」と入力します。
- 2001:db8::1のみを指定したい場合  
「アドレス」欄に「2001:db8::1」、「マスク」欄に「::」と入力します。

## ポート設定

DiffServポリシーを適用するポートを設定します。

**メモ:** ACLが有効になっているポートでは、DiffServは使用できません。

詳細設定 > QoS > DiffServ > ポート設定

ポート設定

現在有効なIPv4/MACポリシー数

0/128

現在有効なIPv6ポリシー数

0/64

ポリシー名

▼

ポート

1

2

3

4

5

6

7

8

☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐

適用

項目	内容
現在有効なIPv4/MACポリシー数	IPv4/MACポリシーのうち、現在有効なものの数を表示します。
現在有効なIPv6ポリシー数	IPv6ポリシーのうち、現在有効なものの数を表示します。
ポート設定	ポリシー名を選択し、そのポリシーを適用したいポートにチェックを入れて[適用]をクリックします。
IPv4/MAC(IPv6)ポリシーリスト	選択したポリシーに設定したルールが表示されます。

## IPv4/MAC優先度設定

IPv4アドレスおよびMACアドレスベースのDiffServポリシーの優先度を設定します。

詳細設定 > QoS > DiffServ > IPv4/MAC優先度

IPv4/MACポリシー一覧 (優先度順)

■	ポリシー番号	ステータス	ポリシー名	DiffServタイプ	ポート
---	--------	-------	-------	-------------	-----

ポリシーの移動

移動

☒ 選択したポリシーの一つ上に移動
 ☐ 選択したポリシーの一つ下に移動
  (ポリシー番号)

移動

編集

有効

無効

削除

項目	内容
IPv4/MACポリシー一覧	IPv4アドレスおよびMACアドレスベースのDiffServポリシーを一覧表示します。優先順位の高いグループから順に表示されます。
ポリシーの移動	優先順位を移動したいポリシーを選択し、移動したい位置の一つ上(または下)となるポリシー番号を入力します。「指定したポリシーの一つ上に移動」(または「指定したポリシーの一つ下に移動」)を選択し、[移動]をクリックします。

## IPv6優先度設定

IPv6アドレスベースのDiffServポリシーの優先度を設定します。

詳細設定 > QoS > DiffServ > IPv6優先度

**IPv6ポリシー一覧 (優先度順)**

■	ポリシー番号	ステータス	ポリシー名	DiffServタイプ	ポート
<b>ポリシーの移動</b> 移動 <input checked="" type="radio"/> 選択したポリシーの一つ上に移動 <input type="radio"/> 選択したポリシーの一つ下に移動 <input type="text"/> (ポリシー番号)					

移動 編集 有効 無効 削除

項目	内容
IPv6ポリシー一覧	IPv6アドレスベースのDiffServポリシーを一覧表示します。優先順位の高いグループから順に表示されます。
ポリシーの移動	優先順位を移動したいポリシーを選択し、移動したい位置の一つ上(または下)となるポリシー番号を入力します。「指定したポリシーの一つ上に移動」(または「指定したポリシーの一つ下に移動」)を選択し、[移動]をクリックします。

## ステータス

DiffServの設定状況を表示します。

詳細設定 > QoS > DiffServ > ステータス

**ポリシー一覧 (優先度順)**

ポートフィルター

■	ポリシー番号	ステータス	ポリシー名	DiffServタイプ	ポート		
<b>IPv4/MACポリシー一覧</b>							
■	ポリシー名	ポリシー番号	ポリシー	指定レート	指定バースト	プロファイル適合時	プロファイル不適合時
<b>IPv6ポリシー一覧</b>							
■	ポリシー名	ポリシー番号	ポリシー	指定レート	指定バースト	プロファイル適合時	プロファイル不適合時

項目	内容
ポリシー一覧	DiffServのポリシーを一覧表示します。優先順位の高いグループから順に表示されます。「ポートフィルター」でポートを選択すると、選択したポートに適用しているポリシーだけが表示されます。
IPv4/MACポリシー一覧	IPv4アドレスまたはMACアドレスベースのDiffServポリシーが表示されます。ルールが設定されたポリシーの左端に表示されている[+]ボタンをクリックすると、そのポリシーに設定されているルールが一覧表示されます。優先順位の高いルールから順に表示されます。

項目	内容
IPv6ポリシー一覧	IPv6アドレススペースのDiffServポリシーが表示されます。ルールが設定されたポリシーの左端に表示されている[+]ボタンをクリックすると、そのポリシーに設定されているルールが一覧表示されます。優先順位の高いルールから順に表示されます。

## セキュリティ

### DOS攻撃防止

指定したパケットを破棄します。

詳細設定 > セキュリティ > DOS攻撃防止

☒ すべて選択

☐ Land攻撃

☐ 最小TCPヘッダー

☐ TCP/UDP L4ポート

☐ ICMP

☐ TCPフラグ

適用

項目	内容
Land攻撃	有効にすると、送信元、送信先のIPアドレスが同じパケットを破棄します。
最小TCPヘッダー	TCPヘッダーサイズが20バイトを下回るパケットを破棄します。
TCP/UDP L4ポート	TCP/UDPプロトコルで送信元/送信先ポート番号が同一のパケットを破棄します。 DHCPリレーを使用する場合は、無効に設定してください。
ICMP	ICMP header+Dataが512バイト以上のICMPパケットを破棄します。
TCPフラグ	不正なTCPフラグのパケットを破棄します。



## DHCPスヌーピング

DHCPスヌーピング機能を設定します。DHCPスヌーピングは、不正なDHCPサーバーが接続されたときにIPアドレスが払い出されるのを防ぐ機能です。

### 詳細設定 > セキュリティ > DHCPスヌーピング

設定	
DHCPスヌーピング	<input type="checkbox"/> 有効
DHCPオプション82	<input type="checkbox"/> 有効
レート制限 (pps)	0 レート制限 (pps)
ポート	ステータス
1	Trusted ▼
2	Trusted ▼
3	Trusted ▼
4	Trusted ▼
5	Trusted ▼
6	Trusted ▼
7	Trusted ▼
8	Trusted ▼

適用

項目	内容
<b>DHCPスヌーピング</b>	DHCPスヌーピングを有効または無効にします。
<b>DHCPオプション82</b>	本製品がDHCPクライアントから受け取ったDHCPパケットにオプション82を付加します(RFC3046)。クライアントが本機能を使用してDHCPサーバーからIPアドレスを取得するには、DHCPサーバーがオプション82に対応している必要があります。
<b>レート制限(pps)</b>	本製品が一秒あたりにすべてのポートで受信するDHCPクライアントからのDHCPパケットを、指定した値に制限します。レート制限を超えたDHCPクライアントからのDHCPパケットは破棄されます。
<b>ステータス</b>	<p><b>Trusted</b> ポートをTrustedに指定すると、そのポートに接続したDHCPサーバーはIPアドレスを払い出すことができます。</p> <p><b>Untrusted</b> ポートをUntrustedに指定すると、そのポートに接続したDHCPサーバーからのDHCPパケットは遮断されます。</p>



## DHCPテーブル

本製品を経由してDHCPサーバーからIPv4アドレスを取得したDHCPクライアントを表示します。記録できるクライアントは256台までです。

### 詳細設定 > セキュリティ > DHCPテーブル

**[注意]**

DHCPテーブルを使用する場合は、DHCPスヌーピングを有効にしてください。

MACアドレス

IPv4アドレス

リース期間

VLAN ID

ポート

更新

**メモ:** DHCPテーブルは、DHCPスヌーピングを有効にしたときのみ使用できます。

項目	内容
MACアドレス	DHCPクライアントのMACアドレスを表示します。
IPv4アドレス	DHCPクライアントが取得したIPv4アドレスを表示します。
リース期間	DHCPクライアントが取得したIPv4アドレスの残りのリース期間を表示します。
VLAN ID	DHCPクライアントが接続されているVLANを表示します。
ポート	DHCPクライアントが接続されているポートを表示します。

## 認証

### ステータス

認証サーバーおよびポート認証のステータスを表示します。

詳細設定 > 認証 > ステータス

プライマリー	
認証	有効
IPv4アドレス	1.1.1.1
ポート	1812
セカンダリー	
認証	無効
IPv4アドレス	1.1.1.1
ポート	1812

認証状態			
ポート	認証設定	認証状態	
1	なし	なし	
2	なし	なし	
3	なし	なし	
4	なし	なし	
5	なし	なし	
6	なし	なし	
7	なし	なし	
8	なし	なし	

項目	内容
プライマリー/セカンダリー	認証サーバーの有効/ 無効、認証サーバーのIPアドレス、認証ポート番号を表示します。
認証状態	各ポートの認証ステータスを表示します。 802.1X MACまたはMAC認証の端末ごとの認証状態は、[管理]－[MACアドレステーブル]の「端末の認証状態」で確認できます。

## RADIUS

認証サーバー (RADIUS サーバー) を設定します。

詳細設定 > 認証 > RADIUS

プライマリー認証サーバー	
認証	<input checked="" type="checkbox"/> 有効
認証サーバーIPv4アドレス	<input type="text" value="1.1.1.1"/>
認証サーバーポート	<input type="text" value="1812"/>
共有暗号化キー	<input type="text"/>
セカンダリー認証サーバー	
認証	<input type="checkbox"/> 有効
認証サーバーIPv4アドレス	<input type="text" value="1.1.1.1"/>
認証サーバーポート	<input type="text" value="1812"/>
共有暗号化キー	<input type="text"/>
詳細設定	
リセットタイマー	<input type="text" value="3600"/> 秒
拡張設定	<input type="checkbox"/> Accounting <input type="checkbox"/> Termination-Action <input type="checkbox"/> ダイナミックVLAN

適用

項目	内容
認証	認証サーバーの有効/無効を設定します。
認証サーバーIPアドレス	認証サーバーのIPアドレスを設定します。
認証サーバーポート	認証サーバーのポート番号を設定します(1～65535)。
共有暗号化キー	認証サーバーの共有暗号化キーを、半角英数字、“-”(ハイフン)、“_”(アンダースコア)で最大20文字までで設定します。
リセットタイマー	再認証までの時間(秒)を設定します。 <b>メモ:</b> RADIUSサーバーからSession-timeoutが通知されている場合は、Session-timeoutの値に従い再認証します。

項目	内容
拡張設定	<p><b>Accounting</b> 有効にすると、接続状態をRADIUSサーバーに通知します。</p> <p><b>Termination-Action</b> 有効にすると、サーバーから通知されたTermination-Actionに従って、再認証の可否を決定します。無効にすると、サーバーからTermination-Actionの通知の有無にかかわらず、再認証を行います。MAC認証を使用している場合、本項目の設定および、サーバーからTermination-Actionの通知の有無にかかわらず、再認証を行います。 <b>メモ:</b> 本項目は、認証方式として802.1Xポート及び802.1X MACを使用している場合に有効です。</p> <p><b>ダイナミックVLAN</b> 有効にすると、RADIUSサーバーから受け取った認証情報に基づいて、ポートの所属するVLANを動的に変更できます。あらかじめRADIUSサーバー側でダイナミックVLANを使用するための属性を設定しておく必要があります。詳細は、下記の「ダイナミックVLAN使用時のRADIUSサーバー設定について」を参照してください。</p>

**メモ:**

- 通常は、プライマリー認証サーバーのみを使用してください。バックアップサーバーが存在するときのみ、セカンダリー認証サーバーを使用してください。
- RADIUSサーバーとの通信におけるタイムアウトは5秒、確認回数は3回に固定されています。
- 一度設定された共有暗号化キーを削除するには、本製品の初期化が必要です(共有暗号化キーを変更する場合は初期化は不要です)。

**ダイナミックVLAN使用時のRADIUSサーバー設定について**

ダイナミックVLANを使用するときは、RADIUSサーバーに以下の属性を追加してください。

属性名	属性値
Tunnel-Type	13(VLAN)
Tunnel-Medium-Type	6(IEEE-802)
Tunnel-Private-Group-ID	認証成功時に所属させるVLAN ID

## ポート認証

ポートごとに認証を設定します。別途、認証サーバー(RADIUSサーバー)をご用意ください。

### 詳細設定 > 認証 > ポート認証

[注意] トランクポートに指定されているポートや、MACフィルターが設定されているポートは選択できません。

ポート	1	2	3	4	5	6	7	8
802.1Xポート	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
802.1X MAC	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
MAC認証	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

適用

#### 拡張設定

EAP透過設定 ☐ 認証機能が無効のとき、EAPを透過する

適用

ゲストVLAN ☐ 有効

ポート	VLAN ID	ゲストVLAN移行期限
1	0	60 30-180秒
2	0	60 30-180秒
3	0	60 30-180秒
4	0	60 30-180秒
5	0	60 30-180秒
6	0	60 30-180秒
7	0	60 30-180秒
8	0	60 30-180秒

適用

項目	内容
802.1Xポート	ポートベースで802.1X認証を行います。認証完了した場合、ポートに接続しているすべての機器が通信可能となります。 <b>メモ:</b> トランクポートに指定されているポートや、MACフィルターが設定されているポートは選択できません。
802.1X MAC	MACアドレスベースで802.1X認証を行います。認証完了した機器のみ通信可能となります。1ポートにつき最大12個のMACアドレスを認証できます。 <b>メモ:</b> トランクポートに指定されているポートや、MACフィルターが設定されているポートは選択できません。
MAC認証	MAC認証を有効にします。1ポートにつき最大12個のMACアドレスを認証できます。 <b>メモ:</b> トランクポートに指定されているポートや、MACフィルターが設定されているポートは選択できません。
EAP透過設定	全ポートの認証機能が無効の場合、受信したEAPフレームを透過させる場合に有効にします。

項目	内容
ゲストVLAN	<p>「有効」をクリックすると、ゲストVLAN機能を有効にします。各ポートのゲストVLAN移行期限を入力し、その期限が過ぎても認証できなかったユーザーを割り当てるVLAN IDを入力します。認証に失敗した場合は、ゲストVLAN移行期限に関わらずゲストVLANへ移行します。</p> <p><b>メモ:</b></p> <ul style="list-style-type: none"> <li>• ゲストVLANのVLAN IDを「0」に設定しているポートは、ゲストVLAN機能が無効になります。</li> <li>• 802.1X MAC認証を行う場合、サブリカントからEAPOL-Startを発行して認証を始める必要があります。EAPOL-Startにより認証が始まらない場合、VLAN移行期限を過ぎてもゲストVLANへ移行されません。</li> </ul>

MAC認証を設定したポートでは、IPパケット受信時に送信元のMACアドレスを使用して認証を行います。

ユーザー名:送信元MACアドレス

パスワード:送信元MACアドレス

として、RADIUSサーバーに認証を行います。

例:IPパケットの送信元MACアドレスが00:11:22:33:AA:BBの場合

ユーザー名:00112233aabb

パスワード:00112233aabb

※アルファベットは小文字で入力してください。

上記のユーザー名、パスワードでRADIUS requestがRADIUSサーバーに送信されます。RADIUSサーバー側では、あらかじめユーザー登録する必要があります。

本製品の認証は、以下の暗号化方式に対応しています。

認証	対応暗号化方式	同時設定
802.1X Port	802.1X(EAP-MD5、TLS、PEAP)	×
802.1X MAC	802.1X(EAP-MD5、TLS、PEAP)	○
MAC認証	PAP	○

**メモ:**

- 802.1X MAC認証を行う場合、サブリカントからEAPOL-Startを発行して認証を始める必要があります。
- 802.1X Port認証を行った場合、当該ポートではMACフィルターが使用できなくなります。

## ポートトランク

ポートトランクを設定します。

### 詳細設定 > ポートトランク

トランクグループ										
トランクキー	トランクモード	トランク名	1	2	3	4	5	6	7	8
T: トランクメンバー A: アクティブメンバー -: 非メンバー										
<div>編集</div> <div>削除</div>										
トランク設定										
トランクモード	LACP ▼									
トランクキー			(1 ~ 8)							
トランク名			(15文字までの半角英数字)							
システム優先度	32768		(1 ~ 65535)							
グループ	1	2	3	4	5	6	7	8		
メンバー	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
*トランクグループは8ポート以下で設定してください。										

適用

項目	内容
トランクモード	トランクのモードとトランクメンバーを設定します。
トランクキー	トランクグループを識別するためのキーを設定します。
トランク名	トランクの名称を設定します。
システム優先度	トランクを構築する際、本製品と相手の機器でどちらの設定を使用するかを設定します。システム優先度の数字が小さい方の機器の設定が優先されます。数字が同じ場合、MACアドレスの小さい方の機器の設定が優先されます。
メンバー	トランクメンバーにするポートを設定します。

#### メモ:

- LACPと手動設定は、合計で8グループ、1グループにつき8ポートまで設定できます。
- 同一トランクグループのポートは同じVLANに所属している必要があります。
- LACPでトランクグループを構成する場合、対向のスイッチはLACP Active/Passive設定の両方で構成できます。

## トラフィック制御

各ポートのトラフィックを設定します。各種パケットがここで設定された制限レート(閾値)を超えた場合、超えた分のパケットは破棄されます。

### 詳細設定 > トラフィック制御

[注意]  
入力帯域制限の値が、ループ防止機能の受信レート閾値よりも小さい場合、ループが検知できない場合があります。

ポート	ブロードキャスト	マルチキャスト	DLF	入力帯域制限		出力帯域制限	
1	無制限 ▼	無制限 ▼	無制限 ▼	1000	Mbps	1000	Mbps
2	無制限 ▼	無制限 ▼	無制限 ▼	1000	Mbps	1000	Mbps
3	無制限 ▼	無制限 ▼	無制限 ▼	1000	Mbps	1000	Mbps
4	無制限 ▼	無制限 ▼	無制限 ▼	1000	Mbps	1000	Mbps
5	無制限 ▼	無制限 ▼	無制限 ▼	1000	Mbps	1000	Mbps
6	無制限 ▼	無制限 ▼	無制限 ▼	1000	Mbps	1000	Mbps
7	無制限 ▼	無制限 ▼	無制限 ▼	1000	Mbps	1000	Mbps
8	無制限 ▼	無制限 ▼	無制限 ▼	1000	Mbps	1000	Mbps

適用

項目	内容
ブロードキャスト	ブロードキャストの通過を許可するレートを設定します。
マルチキャスト	マルチキャストの通過を許可するレートを設定します。
DLF	DLF(宛先不明ユニキャスト)の通過を許可するレートを設定します。
入力帯域制限	各ポートのスイッチへの入力に対する通信速度を設定した値に制限します。 <b>メモ:</b> 入力帯域制限の値が、「ループ防止機能」の「受信レート閾値」よりも小さい場合、ループが検知できない場合があります。
出力帯域制限	各ポートのスイッチからの出力に対する通信速度を設定した値に制限します。

**メモ:** ブロードキャストを基準にして制限レートを設定した場合、マルチキャストやDLF(宛先不明ユニキャスト)がパケットの伝播によるトラフィックの違いによって流れなくなることがあります。制限レートには、通常使用するフレーム数を考慮して余裕のある値を設定してください。



## ミラーリング

トラフィックをモニタリング(通信内容をミラー元からミラー先へコピー)するための設定をします。

### 詳細設定 > ミラーリング

ミラーポートグループ	有効	ミラー元ポート								ミラー先ポート
		1	2	3	4	5	6	7	8	
ミラー 1	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1 ▼
ミラー 2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	3 ▼

適用

項目	内容
有効	ミラーリングを有効または無効にします。
ミラー元ポート	トラフィックをモニタされるポートを設定します。
ミラー先ポート	トラフィックをモニタするポートを設定します。

## STP

### 設定

STP(スパンニングツリー機能)を設定します。

設定することで、ループ検出時にポートをブロックし、自動的に経路を切り替え、ループによるネットワークダウンを防止できます。

#### メモ:

- 設定するには、セグメント内のすべての機器がSTPに対応している必要があります。  
対応していない場合、代わりに[詳細設定] - [ループ防止機能]画面からループ防止機能を設定することで、ループによるネットワークダウンを防止できます。  
ただし、ループ防止機能ではループの対策(通信経路の切り替え)は行われませんので、注意してください。
- STPとループ防止機能の違いは、[「ループによるネットワークダウンを防止する」\(P.123\)](#)を参照してください。

### 詳細設定 > STP > 設定

#### STP設定:無効(出荷時設定)

設定	
STP設定	無効 ▼
BPDU転送	<input type="checkbox"/> STPが無効のときは、BPDUフレームを透過させる

適用

項目	内容
STP設定	STPの種類を、「STP」、「RSTP」、「MSTP」から選択し、[適用]をクリックします。 <b>メモ:</b> MSTPは、[詳細設定]－[ループ防止機能]画面でLDFが有効になっている状態では使用できません。
BPDU転送	STPが無効のときにBPDUフレームを透過させる場合は有効にします。

### STP設定:STP

設定		
STP設定	STP ▼	
Hello Time	2	(1-10 秒)
Max Age	20	(6-40 秒)
Forward Delay	15	(4-30 秒)
Bridge Priority	32768	(0-61440)

適用

項目	内容
Hello Time	本製品がルートブリッジになった場合のBPDU送信間隔を設定します。
Max Age	本製品がBPDUを受信しない状態で、再設定を試みるまでに待機する最大の時間(秒)を設定します。
Forward Delay	本製品が各状態を遷移する(Listening～Learning～Forwarding)際に待機する時間(秒)を設定します。
Bridge Priority	ルートブリッジを選択する際の本製品の優先度を設定します。

**メモ:** 設定する値は以下の関係式を満たす必要があります。満たさない場合、適用時にエラーが表示されます。

$$2 \times (\text{Forward Delay} - 1) \geq \text{Max Age}$$

$$\text{Max Age} \geq 2 \times (\text{Hello Time} + 1)$$

### STP設定:RSTP

設定		
STP設定	RSTP ▼	
Hello Time	2	(1-10 秒)
Max Age	20	(6-40 秒)
Forward Delay	15	(4-30 秒)
Bridge Priority	32768	(0-61440)

適用

項目	内容
Hello Time	本製品がルートブリッジになった場合のBPDU送信間隔を設定します。

項目	内容
Max Age	本製品がBPDUを受信しない状態で、再設定を試みるまでに待機する最大の時間(秒)を設定します。
Forward Delay	本製品が各状態を遷移する(Listening～Learning～Forwarding)際に待機する時間(秒)を設定します。
Bridge Priority	ルートブリッジを選択する際の本製品の優先度を設定します。

✕モ: 設定する値は以下の関係式を満たす必要があります。満たさない場合、適用時にエラーが表示されます。

$2 \times (\text{Forward Delay} - 1) \geq \text{Max Age}$

$\text{Max Age} \geq 2 \times (\text{Hello Time} + 1)$

## STP設定:MSTP

CST設定	
STP設定	MSTP ▼
Hello Time	2 (1-10 秒)
Max Age	20 (6-40 秒)
Forward Delay	15 (4-30 秒)
Max Hop Count	20 (6-40)
Bridge Priority	32768 (0-61440)
MSTリージョン設定	
MST Configuration Name	XX-XX-XX-XX-XX-XX
MST Revision Level	0 (0-65535)
Configuration Digest	00000000000000000000000000000000

適用

MSTI設定	
MSTI ID	(1-4094)
VLAN ID	1 すべて <input type="checkbox"/>
Bridge Priority	(0-61440)

追加

MSTPステータス		
MSTI ID	Bridge Priority	VLAN ID

編集 削除

項目	内容
Hello Time	本製品がルートブリッジになった場合のBPDU送信間隔を設定します。

項目	内容
Max Age	本製品がBPDUを受信しない状態で、再設定を試みるまでに待機する最大の時間(秒)を設定します。
Forward Delay	本製品が各状態を遷移する(Listening～Learning～Forwarding)際に待機する時間(秒)を設定します。
Max Hop Count	BPDUの最大ホップ数を指定します。
Bridge Priority	ルートブリッジを選択する際の本製品の優先度を設定します。
MST Configuration Name	MSTリージョン名を設定します。同一リージョンに所属させたい機器には、同じ名前を指定する必要があります。
MST Revision Level	MSTリビジョンを設定します。同一リージョンに所属させたい機器には、同じ値を指定する必要があります。
Configuration Digest	MSTIステータス情報をMD5ダイジェストメッセージで表示します。
MSTI設定	MSTI IDを追加します。MSTI ID、Bridge Priorityを入力し、適用するVLAN IDを選択して[追加]をクリックします。
MSTPステータス	MSTI IDの設定状況を表示します。MSTI IDを選択して[編集]をクリックすると、適用するVLAN IDとBridge Priorityを変更できます。

**メモ:** 設定する値は以下の関係式を満たす必要があります。満たさない場合、適用時にエラーが表示されます。  
 $2 \times (\text{Forward Delay} - 1) \geq \text{Max Age}$   
 $\text{Max Age} \geq 2 \times (\text{Hello Time} + 1)$

## ステータス

ポートごとのSTPの状態を表示します。

### 詳細設定 > STP > ステータス

ステータス					
Root Port	0				
Root Port Path	0				
Hello Time	2				
Max Age	20				
Forward Delay	15				
Root Bridge Priority	0				
Root MACアドレス	XX:XX:XX:XX:XX:XX				
スイッチのMACアドレス	XX:XX:XX:XX:XX:XX				
ポート	優先度	パスコスト	Fastlink	状態	役割
1	128	0	無効	Forwarding	Disabled
2	128	0	無効	Forwarding	Disabled
3	128	0	無効	Forwarding	Disabled
4	128	0	無効	Forwarding	Disabled
5	128	0	無効	Forwarding	Disabled
6	128	0	無効	Forwarding	Disabled
7	128	0	無効	Forwarding	Disabled
8	128	0	無効	Forwarding	Disabled

項目	内容
MSTI/CIST (MSTPのみ)	MSTP選択時は、MSTI IDまたはCISTごとにステータスを表示します。ステータスを表示するMSTI/CISTを選択します。

項目	内容
Root Port	ルートポートを表示します。本製品がルートブリッジの場合、0と表示されます。
Root Port Path	ルートブリッジまでのパスコストを表示します。本製品がルートブリッジの場合、0と表示されます。
Regional Root Port Path (MSTPのみ)	MSTリージョン内のCISTルートブリッジまでのパスコストを表示します。
Hello Time	本製品がルートブリッジになった場合のBPDU送信間隔を表示します。
Max Age	本製品がBPDUを受信しない状態で、再設定を試みるまでに待機する最大の時間(秒)を表示します。
Forward Delay	本製品が各状態を遷移する(Listening～Learning～Forwarding)際に待機する時間(秒)を表示します。
Max Hop Count (MSTPのみ)	BPDUの最大ホップ数を表示します。
Root Bridge Priority (STP/RSTPのみ)	ルートブリッジを選択する際の本製品の優先度を表示します。
Root MACアドレス (STP/RSTPのみ)	ルートブリッジのMACアドレスを表示します。
CIST Root Bridge Priority (MSTPのみ)	CISTルートブリッジのブリッジプライオリティを表示します。
CIST Root MACアドレス (MSTPのみ)	CISTルートブリッジのMACアドレスを表示します。
Regional Root Bridge Priority (MSTPのみ)	MSTリージョン内のルートブリッジのブリッジプライオリティを表示します。
Regional Root MACアドレス (MSTPのみ)	MSTリージョン内のルートブリッジのMACアドレスを表示します。
スイッチのMACアドレス	本製品のMACアドレスを表示します。
優先度	ポートの優先度を表示します。
パスコスト	ポートのパスコストを表示します。
Fastlink	Fastlink機能の有効/無効を表示します。
状態	ポートの状態を表示します。
役割	ポートの役割を表示します。

## ポート

ポートごとにSTPを設定します。MSTPを設定している場合は、MSTI IDまたはCISTごとに設定します。パスコストは、自動設定と手動設定を切り替えることができます。

### 詳細設定 > STP > ポート

パスコスト 自動 ▼

ポート	優先度	パスコスト	Fastlink
1	128	20000	無効 ▼
2	128	20000	無効 ▼
3	128	20000	無効 ▼
4	128	20000	無効 ▼
5	128	20000	無効 ▼
6	128	20000	無効 ▼
7	128	20000	無効 ▼
8	128	20000	無効 ▼

適用

項目	内容
優先度	<p>ポートの優先度を設定します。設定した値が小さいポートが優先されます。設定できる値は、0または16の倍数のみです(0～240)。 ルートブリッジまでの最適なパスを決定する際に用いられます。</p>
パスコスト	<p>「手動」を選択したときのみ、値を編集できます。 ポートのパスコストを設定します。ルートブリッジまでの最適なパスを決定する際に用いられます。通信速度によってコストを調整し、より多く帯域を確保できる経路が選択されるように設定します。 「自動」の場合、パスコストはリンク速度によって、以下のように自動で変化します。</p> <ul style="list-style-type: none"> <li>10Mbps :2000000</li> <li>100Mbps :200000</li> <li>1000Mbps:20000</li> </ul> <p><b>メモ:</b>「自動」の場合のパスコストは、お使いの製品によって異なる場合があります。 例:BS-GS20シリーズ、BS-GS20Pシリーズ、BS-GS20P/HPシリーズ [詳細設定]－[STP]－[設定]の「STP設定」で「STP」選択時</p> <ul style="list-style-type: none"> <li>10Mbps :100</li> <li>100Mbps :19</li> <li>1000Mbps:4</li> </ul>
Fastlink	<p>Fastlinkを有効にすると、ポートが各状態を遷移するのを省略し、すぐにForwardingの状態になります。通常、パソコンを接続するポートは有効にすることをおすすめします。STPを使用するスイッチを接続するポートは、無効にしてお使いください。 <b>メモ:</b> トランク設定時は、Fastlinkは無効になります。</p>

## IGMP

### ステータス

IGMPの状態を表示します。

詳細設定 > IGMP > ステータス

VLAN ID	マルチキャストアドレス	グループメンバー
<input type="button" value="更新"/>		

### ルーターポートステータス

S : 静的 , D : 動的	
VLAN ID	ルーターポート
<input type="button" value="更新"/>	

項目	内容
IGMPステータス	マルチキャストアドレスのテーブルを表示します。
ルーターポートステータス	マルチキャストルーター(サーバー)が接続されているポートを表示します。

## 設定

IGMPスヌーピングを設定します。本製品は、IGMPv1,v2,v3スヌーピングに対応しています。

### 詳細設定 > IGMP > 設定

IGMPスヌーピング設定	
IGMPスヌーピング	<input type="checkbox"/> 有効
未知のマルチキャストをフィルタリングする	<input type="checkbox"/> 有効
ホストタイムアウト	<input type="text" value="260"/> (130-1225 秒)
ルーターポートタイムアウト	<input type="text" value="125"/> (60-600 秒)

適用

項目	内容
IGMPスヌーピング	IGMPスヌーピングを有効または無効にします。 IGMPスヌーピングを有効にすると、マルチキャストグループに参加しているホストが接続されているポート以外に、マルチキャストパケットが送信されることを防げます。 <b>メモ:</b> 224.0.0.1～224.0.0.255(224.0.0.22を除く)はスヌーピングの対象になりません。
未知のマルチキャストをフィルタリングする	224.0.0.1～224.0.0.255以外の、学習していないマルチキャストアドレスのパケットを破棄します。
ホストタイムアウト	マルチキャストを受信するホストのタイムアウト時間(秒)を設定します。
ルーターポートタイムアウト	マルチキャストルーター(サーバー)のタイムアウト時間(秒)を設定します。

**メモ:** IGMPスヌーピングが有効時にマルチキャスト放送などが視聴できず、[詳細設定]－[IGMP]－[ステータス]のルーターポートステータスにマルチキャストルーター(サーバー)を接続したポートが表示されていない場合、[詳細設定]－[IGMP]－[静的ルーターポート]から、マルチキャストルーター(サーバー)を接続したポートを指定してください。



## IGMPクエリア

IGMPクエリアを有効にすると、マルチキャストルーターが存在しない場合でもIGMPスヌーピングを行うことができるようになります。

### 詳細設定 > IGMP > IGMPクエリア

IGMPクエリア設定	
IGMPクエリア	<input type="checkbox"/> 有効
IGMPクエリア送信間隔	60 (1-18000 秒)
送信元IPv4アドレス	0.0.0.0
Max Response Time	10 (1-25 秒)

適用

項目	内容
IGMPクエリア	「有効」にチェックを入れると、IGMPクエリア機能が有効になります。IGMPクエリは、すべてのVLANから送信されます。
IGMPクエリア送信間隔	マルチキャストグループのメンバーの存在を確認するクエリを送信する間隔を設定します。
送信元IPv4アドレス	クエリの送信元IPv4アドレスを入力します。
Max Response Time	クエリを送信してから返答があるまでの最大期間を指定します。この期間内に返答があったメンバーを存在するものとして扱います。

## 静的ルーターポート

VLAN IDごとにマルチキャストルーター(サーバー)を接続するポートを指定します。

### 詳細設定 > IGMP > 静的ルーターポート

ポート設定									
VLAN ID	<input type="text"/> (1-4094)								
ポート	1	2	3	4	5	6	7	8	
すべて	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
リストに追加									
<input type="checkbox"/>	VLAN ID	ルーターポート							
削除									

項目	内容
ポート設定	設定するVLAN IDを入力し、マルチキャストルーター(サーバー)を接続するポートを指定して[リストに追加]をクリックします。

## MLD

### ステータス

MLDの状態を表示します。

詳細設定 > MLD > ステータス

VLAN ID	マルチキャストアドレス	グループメンバー
更新		

### ルーターポートステータス

S : 静的 , D : 動的

VLAN ID	ルーターポート
更新	

項目	内容
MLDステータス	マルチキャストアドレスのテーブルを表示します。
ルーターポートステータス	マルチキャストルーター(サーバー)が接続されているポートを表示します。

### 設定

MLDスヌーピングを設定します。

詳細設定 > MLD > 設定

MLDスヌーピング設定	
MLDスヌーピング	<input type="checkbox"/> 有効
未知のマルチキャストをフィルタリングする	<input type="checkbox"/> 有効
ホストタイムアウト	<input type="text" value="260"/> (130-1225 秒)
ルーターポートタイムアウト	<input type="text" value="125"/> (60-600 秒)

適用

項目	内容
MLDスヌーピング	MLDスヌーピングを有効または無効にします。 MLDスヌーピングを有効にすると、マルチキャストグループに参加しているホストが接続されているポート以外に、マルチキャストパケットが送信されることを防げます。 <b>メモ:</b> FF02::~FF02::FF (FF02::16を除く) および FF0X:: はスヌーピングの対象になりません。
未知のマルチキャストをフィルタリングする	FF02::~FF02::FF および FF0X:: 以外の学習していないマルチキャストアドレスのパケットを破棄します。
ホストタイムアウト	マルチキャストを受信するホストのタイムアウト時間(秒)を設定します。
ルーターポートタイムアウト	マルチキャストルーター(サーバー)のタイムアウト時間(秒)を設定します。

**メモ:** MLDスヌーピングが有効時にマルチキャスト放送などが視聴できず、[詳細設定] - [MLD] - [ステータス] のルーターポートステータスにマルチキャストルーター(サーバー)を接続したポートが表示されていない場合、[詳細設定] - [MLD] - [静的ルーターポート] から、マルチキャストルーター(サーバー)を接続したポートを指定してください。

## MLDクエリア

MLDクエリアを有効にすると、マルチキャストルーターが存在しない場合でもMLDスヌーピングを行うことができますようになります。

### 詳細設定 > MLD > MLDクエリア

MLDクエリア設定	
MLDクエリア	<input type="checkbox"/> 有効
MLDクエリア送信間隔	60 (1-18000 秒)
送信元IPv6アドレス	::
Max Response Time	10 (1-25 秒)

適用

項目	内容
MLDクエリア	「有効」にチェックを入れると、MLDクエリア機能が有効になります。MLDクエリアは、すべてのVLANから送信されます。
MLDクエリア送信間隔	マルチキャストグループのメンバーの存在を確認するクエリを送信する間隔を設定します。
送信元IPv6アドレス	クエリの送信元IPv6アドレスを入力します。
Max Response Time	クエリを送信してから返答があるまでの最大期間を指定します。この期間内に返答があったメンバーを存在するものとして扱います。

## 静的ルーターポート

VLAN IDごとにマルチキャストルーター(サーバー)を接続するポートを指定します。

詳細設定 > MLD > 静的ルーターポート

項目	内容
ポート設定	設定するVLAN IDを入力し、マルチキャストルーター(サーバー)を接続するポートを指定して[リストに追加]をクリックします。

## ACL

### ACLウィザード

ウィザード形式でACLを設定します。画面の指示に従って設定してください。

詳細設定 > ACL > ACLウィザード

次へ

項目	内容
送信元MACアドレス	指定した送信元MACアドレスを許可/拒否するように設定します。
送信先MACアドレス	指定した送信先MACアドレスを許可/拒否するように設定します。
送信元IPv4アドレス	指定した送信元IPv4アドレスを許可/拒否するように設定します。
送信先IPv4アドレス	指定した送信先IPv4アドレスを許可/拒否するように設定します。
送信元IPv6アドレス	指定した送信元IPv6アドレスを許可/拒否するように設定します。
送信先IPv6アドレス	指定した送信先IPv6アドレスを許可/拒否するように設定します。

ACLウィザードを使用したACLの設定例は、本製品の「設定事例集」を参照してください。

## MAC ACLグループ設定

MACアドレスベースのACLを作成します。

### 詳細設定 > ACL > MAC ACLグループ設定

ACL数

現在のACLグループ数 0/126

現在有効なルール数 0/126

ACLグループ名	ルール数
<input type="checkbox"/> <input type="text"/>	

項目	内容
現在のACLグループ数	現在設定しているACLグループの数を表示します。
現在有効なルール数	現在有効になっているルールの数を表示します。
ACLグループ名	<p>空欄にグループ名を入力し[適用]をクリックすると、新しいACLグループが作成されます。[詳細]をクリックすると、ACLグループの内容を詳細に設定できます。</p> <p>作成済みのACLグループにチェックを入れて入力欄に新しいグループ名を入力し、[名前の変更]をクリックすると、チェックを入れたACLグループが入力した名前に変更されます。</p>
ルール数	ACLグループに設定しているルールの数を表示します。

以下の項目は、[詳細]をクリックしたときに表示されます。ルールは、1つのグループに最大10個まで設定できます。

ACLルール一覧（優先度順）											
<input type="checkbox"/>	ルール番号	CoS	送信先MACアドレス	送信先マスク	送信元MACアドレス	送信元マスク	イーサertype	VLAN	許可/拒否	Egressキュー	リダイレクトポート
<input type="checkbox"/>	1	すべて	すべて	すべて	すべて	すべて	すべて	すべて	許可	なし	なし

ルールの移動  
 移動 ☒ 選択したルールの一つ上に移動 ☐ 選択したルールの一つ下に移動  (ルール番号)

---

ACLルール設定	
ACLグループ名	001
CoS	<input type="button" value="すべて"/>
送信先MACアドレス	<input type="button" value="すべて"/> アドレス: <input type="text"/> マスク: <input type="text"/> (例: 00:11:22:33:44:55)
送信元MACアドレス	<input type="button" value="すべて"/> アドレス: <input type="text"/> マスク: <input type="text"/> (例: 00:11:22:33:44:55)
イーサertype	<input type="button" value="すべて"/> (0600-FFFF Hex)
VLAN	<input type="button" value="すべて"/>
ACLの動作	
許可/拒否	<input type="button" value="許可"/>
Egressキュー	<input type="button" value="なし"/>
リダイレクトポート	<input type="button" value="なし"/>
<input type="button" value="保存"/> <input type="button" value="戻る"/>	

項目	内容
ACLルール一覧	選択したACLグループに設定しているルールを一覧表示します。優先順位の高いルールから順に表示されます。
ルールの移動	優先順位を移動したいルールを選択し、そのルールの一つ上(または下)となるルール番号を入力します。「選択したルールの一つ上に移動」(または「選択したルールの一つ下に移動」)を選択し、[移動]をクリックします。
ACLグループ名	選択しているACLグループ名を表示します。
CoS	フレームのCoS値に基づいてフィルターするように設定します。
送信先MACアドレス	フレームの送信先MACアドレスに基づいてフィルターするように設定します。 <b>メモ:</b> マスクの入力は、サブネットマスクではなくワイルドカードマスクで入力します。 アドレスの入力方法については、下記の「アドレスとマスクについて」を参照してください。
送信元MACアドレス	フレームの送信元MACアドレスに基づいてフィルターするように設定します。 <b>メモ:</b> マスクの入力は、サブネットマスクではなくワイルドカードマスクで入力します。 アドレスの入力方法については、下記の「アドレスとマスクについて」を参照してください。
イーサertype	フレームのイーサertypeに基づいてフィルターするように設定します。
VLAN	フレームのVLAN IDに基づいてフィルターするように設定します。

項目	内容
許可/拒否	<p>条件に合致したフレームをほかのポートに転送するかどうかを設定します。  <b>メモ:</b> 許可もしくは拒否ルールを設定した場合、設定したMACアドレス範囲外のパケット/フレームは破棄されます。</p> <p><b>許可</b>            ポートに入ってくるフレームをほかのポート(および本製品との通信)に転送します。</p> <p><b>拒否</b>            ポートに入ってくるフレームを破棄します。</p>
Egressキュー	<p>条件に合致したフレームにスケジューリングを適用し、優先度を設定します。優先度は、0(最低)～7(最高)で設定します。            スケジューリングはStrictまたはWRRによって行われます。StrictかWRRかは、[詳細設定]－[QoS設定]のスケジューリング方法に依存します。QoS機能が無効の場合はWRRとなります。</p>
リダイレクトポート	<p>条件に合致したフレームを指定したポートに転送します。その場合、本来の送信先には送信されません。            許可/拒否が拒否の場合はフレームは破棄され、本来の送信先にも指定したポートにも送信されません。</p>

### アドレスとマスクについて

本製品のACLは、ワイルドカードマスクを採用しています。送信先MACアドレス、送信元MACアドレスのマスクの設定は、以下の例を参考に行ってください。

- 00:11:22:ab:cd:00～00:11:22:ab:cd:ffの範囲を指定したい場合  
 「アドレス」欄に「00:11:22:ab:cd:00」、「マスク」欄に「00:00:00:00:00:ff」と入力します。
- 00:11:22:ab:cd:efのみを指定したい場合  
 「アドレス」欄に「00:11:22:ab:cd:ef」、「マスク」欄に「00:00:00:00:00:00」と入力します。

## IPv4 ACLグループ設定

IPv4アドレスベースのACLを作成します。

### 詳細設定 > ACL > IPv4 ACLグループ設定

ACL数

現在のACLグループ数 0/126

現在有効なルール数 0/126

ACLグループ名	ルール数
<input type="checkbox"/> <input type="text"/>	

項目	内容
現在のACLグループ数	現在設定しているACLグループの数を表示します。
現在有効なルール数	現在有効になっているルールの数を表示します。
ACLグループ名	<p>空欄にグループ名を入力し[適用]をクリックすると、新しいACLグループが作成されます。[詳細]をクリックすると、ACLグループの内容を詳細に設定できます。</p> <p>作成済みのACLグループにチェックを入れて入力欄に新しいグループ名を入力し、[名前の変更]をクリックすると、チェックを入れたACLグループが入力した名前に変更されます。</p>
ルール数	ACLグループに設定しているルールの数を表示します。



以下の項目は、[詳細]をクリックしたときに表示されます。ルールは、1つのグループに最大10個まで設定できます。

ACLルール一覧（優先度順）											
<input type="checkbox"/>	ルール番号	プロトコル	送信先IPv4アドレス	送信先マスク	送信先ポート	送信元IPv4アドレス	送信元マスク	送信元ポート	サービスの種類	許可/拒否	Egressキュー
<input type="checkbox"/>	1	すべて	すべて	すべて	すべて	すべて	すべて	すべて	すべて	許可	すべて

ルールの移動  
 移動 ☒ 選択したルールの一つ上に移動 ☐ 選択したルールの一つ下に移動  (ルール番号)

---

ACLルール設定	
ACLグループ名	001
プロトコル	すべて▼ (0-255)
送信先IPv4アドレス	すべて▼ アドレス: マスク: (例: 0.0.0.0)
送信先ポート	すべて▼ (0-65535)
送信元IPv4アドレス	すべて▼ アドレス: マスク: (例: 0.0.0.0)
送信元ポート	すべて▼ (0-65535)
サービスの種類	<input checked="" type="radio"/> すべて <input type="radio"/> IP DSCP (0-63) <input type="radio"/> IP Precedence (0-7) <input type="radio"/> IP ToS Bits: マスク: (00-FF)
ACLの動作	
許可/拒否	許可▼
Egressキュー	なし▼
<input type="button" value="保存"/> <input type="button" value="戻る"/>	

項目	内容
ACLルール一覧	選択したACLグループに設定しているルールを一覧表示します。優先順位の高いルールから順に表示されます。
ルールの移動	優先順位を移動したいルールを選択し、そのルールの一つ上(または下)となるルール番号を入力します。「選択したルールの一つ上に移動」(または「選択したルールの一つ下に移動」)を選択し、[移動]をクリックします。
ACLグループ名	選択しているACLグループ名を表示します。
プロトコル	パケットのプロトコルに基づいてフィルターするように設定します。
送信先IPv4アドレス	パケットの送信先IPv4アドレスに基づいてフィルターするように設定します。 <b>メモ:</b> マスクの入力は、サブネットマスクではなくワイルドカードマスクで入力します。 アドレスの入力方法については、下記の「アドレスとマスクについて」を参照してください。
送信先ポート	パケットの送信先ポートに基づいてフィルターするように設定します。
送信元IPv4アドレス	パケットの送信元IPv4アドレスに基づいてフィルターするように設定します。 <b>メモ:</b> マスクの入力は、サブネットマスクではなくワイルドカードマスクで入力します。 アドレスの入力方法については、下記の「アドレスとマスクについて」を参照してください。
送信元ポート	パケットの送信元ポートに基づいてフィルターするように設定します。
サービスの種類	パケットのサービスの種類に基づいてフィルターするように設定します。 IP DSCP、IP Precedenceを選択した場合は、一つの値のみ許可/拒否できます。 IP ToSを選択すると、範囲で指定できます。詳細は、下記の「IP ToSマスクについて」を参照してください。

項目	内容
許可/拒否	<p>条件に合致したパケットをほかのポートに転送するかどうかを設定します。</p> <p><b>メモ:</b> 許可もしくは拒否ルールを設定した場合、設定したIPアドレス範囲外のパケット/フレームは破棄されます。ただし、ARP、EAPなどのMACフレームはすべて許可されて転送されます。</p> <p><b>許可</b> ポートに入ってくるパケットをほかのポート(および本製品との通信)に転送します。</p> <p><b>拒否</b> ポートに入ってくるパケットを破棄します。</p>
Egressキュー	<p>条件に合致したフレームにスケジューリングを適用し、優先度を設定します。優先度は、0(最低)～7(最高)で設定します。</p> <p>スケジューリングはStrictまたはWRRによって行われます。StrictかWRRかは、[詳細設定]－[QoS設定]のスケジュール方法に依存します。QoS機能が無効の場合はWRRとなります。</p>

### アドレスとマスクについて

本製品のACLは、ワイルドカードマスクを採用しています。送信先IPアドレス、送信元IPアドレスのマスクの設定は、以下の例を参考に行ってください。

- 一般的なサブネットマスク表記、例として「255.255.255.0」は、ワイルドカードマスクでは反転させて「0.0.0.255」と記載します。
- 192.168.1.0～192.168.1.254の範囲を指定したい場合、本製品のACLでは「アドレス」欄に「192.168.1.0」、「マスク」欄に「0.0.0.255」と入力します。
- 192.168.1.1のみを指定したい場合、本製品のACLでは「アドレス」欄に「192.168.1.1」、「マスク」欄に「0.0.0.0」と入力します。

### IP ToSマスクについて

IP ToSマスクは、ワイルドカードマスクを採用しています。「サービスの種類」に「IP ToS」を選択すると、IP DSCPやIP Precedenceの値を範囲で指定できます。指定する際は、以下の例を参考にしてください。

DSCPの1～7の範囲を指定したい場合は、  
Bits:0 マスク:1C  
と入力します。

## IPv6 ACLグループ設定

IPv6アドレスベースのACLを作成します。

### 詳細設定 > ACL > IPv6 ACLグループ設定

ACL数

現在のACLグループ数 0/64

現在有効なルール数 0/64

ACLグループ名	ルール数
<input type="checkbox"/> <input type="text"/>	

適用

名前の変更

削除

項目	内容
現在のACLグループ数	現在設定しているACLグループの数を表示します。
現在有効なルール数	現在有効になっているルールの数を表示します。
ACLグループ名	空欄にグループ名を入力し[適用]をクリックすると、新しいACLグループが作成されます。[詳細]をクリックすると、ACLグループの内容を詳細に設定できます。 作成済みのACLグループにチェックを入れて入力欄に新しいグループ名を入力し、[名前の変更]をクリックすると、チェックを入れたACLグループが入力した名前に変更されます。
ルール数	ACLグループに設定しているルールの数を表示します。

以下の項目は、[詳細]をクリックしたときに表示されます。ルールは、1つのグループに最大10個まで設定できます。

ACLルール一覧 (優先度順)

ルール番号	送信元IPv6アドレス/マスク	送信元IPv6アドレス/マスク	許可/拒否	Egressキュー
<div>ルールの移動</div> <div> 移動 <input checked="" type="radio"/> 選択したルールの一つ上に移動 <input type="radio"/> 選択したルールの一つ下に移動 <input type="text"/> (ルール番号) </div> <div> 移動 編集 削除 </div>				

ACLルール設定

ACLグループ名

001

送信元IPv6アドレス/マスク

すべて

アドレス:

マスク:

(例: 2001:db8:0:0:1:0:0:1)

送信元IPv6アドレス/マスク

すべて

アドレス:

マスク:

(例: 2001:db8:0:0:1:0:0:1)

ACLの動作

許可/拒否

許可

Egressキュー

なし

保存

戻る

項目	内容
ACLルール一覧	選択したACLグループに設定しているルールを一覧表示します。優先順位の高いルールから順に表示されます。

項目	内容
<b>ルールの移動</b>	優先順位を移動したいルールを選択し、そのルールの一つ上(または下)となるルール番号を入力します。「選択したルールの一つ上に移動」(または「選択したルールの一つ下に移動」)を選択し、[移動]をクリックします。
<b>ACLグループ名</b>	選択しているACLグループ名を表示します。
<b>送信先IPv6アドレス/マスク</b>	パケットの送信先IPv6アドレスに基づいてフィルターするように設定します。アドレスの入力方法については、下記の「アドレスとマスクについて」を参照してください。
<b>送信元IPv6アドレス/マスク</b>	パケットの送信元IPv6アドレスに基づいてフィルターするように設定します。アドレスの入力方法については、下記の「アドレスとマスクについて」を参照してください。
<b>許可/拒否</b>	<p>条件に合致したパケットをほかのポートに転送するかどうかを設定します。</p> <p><b>許可</b> ポートに入ってくるパケットをほかのポート(および本製品との通信)に転送します。許可ルールを設定した場合、許可したIPv6アドレス範囲外のパケット/フレームは破棄されます。ただし、EAPなどのMACフレームはすべて許可されて転送されます。</p> <p><b>拒否</b> ポートに入ってくるパケットを破棄します。</p>
<b>Egressキュー</b>	<p>条件に合致したフレームにスケジューリングを適用し、優先度を設定します。優先度は、0(最低)～7(最高)で設定します。</p> <p>スケジューリングはStrictまたはWRRによって行われます。StrictかWRRかは、[詳細設定]－[QoS設定]のスケジューリング方法に依存します。QoS機能が無効の場合はWRRとなります。</p>

### アドレスとマスクについて

本製品のACLは、ワイルドカードマスクを採用しています。送信先IPv6アドレス、送信元IPv6アドレスのマスクの設定は、以下の例を参考に行ってください。

- 2001:db8::～2001:db8::ffffの範囲を指定したい場合  
「アドレス」欄に「2001:db8::」、「マスク」欄に「::ffff」と入力します。
- 2001:db8::1のみを指定したい場合  
「アドレス」欄に「2001:db8::1」、「マスク」欄に「::」と入力します。

## ポート設定

ACLグループを適用するポートを設定します。

MAC ACL、IPv4 ACL、IPv6 ACLで合わせて126個までACLルールを適用できます。

### 詳細設定 > ACL > ポート設定

ポート設定

有効なIPv4/MAC ACLルール数

0/126

有効なIPv6 ACLルール数

0/64

ACLグループ名

▼

ポート選択

1

2

3

4

5

6

7

8

☐
☐
☐
☐
☐
☐
☐
☐

適用

項目	内容
有効なIPv4/MAC ACL ルール数	現在有効になっているIPv4 ACLおよびMAC ACLルールの数を表示します。
有効なIPv6 ACLルール 数	現在有効になっているIPv6 ACLのルールの数を表示します。
ポート選択	ACLグループ名を選択し、そのグループを適用するポートを選択して[適用]をクリックします。
ルール一覧	選択しているACLグループに設定されているルールが表示されます。

**メモ:** ルールを設定していないグループをポートに設定した場合、すべてのパケット/フレームが許可され、転送されます。ルールを設定しているグループをポートに設定した場合、どのルールにも該当しないパケット/フレームは破棄されます。

## IPv4/MAC ACL優先度設定

IPv4およびMAC ACLグループの優先度を設定します。MAC ACLはIPv4パケット、IPv6パケットの両方に適用されます。IPv4 ACLの送信先/送信元ポートによるフィルターは、IPv6パケットには適用されません。

### 詳細設定 > ACL > IPv4/MAC ACL優先度設定

**IPv4/MAC ACLグループ一覧 (優先度順)**

グループ番号	ステータス	ACLグループ名	ACLタイプ	対象ポート
グループの移動				
移動 <input checked="" type="radio"/> 選択したグループの一つ上に移動 <input type="radio"/> 選択したグループの一つ下に移動 <input type="text"/> (グループ番号)				

項目	内容
IPv4/MAC ACLグループ一覧	ACLグループを一覧表示します。優先順位の高いグループから順に表示されます。
グループの移動	優先順位を移動したいグループを選択し、移動したい位置の一つ上(または下)となるグループ番号を入力します。「選択したグループの一つ上に移動」(または「選択したグループの一つ下に移動」)を選択し、[移動]をクリックします。

## IPv6 ACL優先度設定

IPv6 ACLグループの優先度を設定します。IPv6 ACLは、MAC ACL、IPv4 ACLよりも優先されます。

### 詳細設定 > ACL > IPv6 ACL優先度設定

**IPv6 ACLグループ一覧 (優先度順)**

グループ番号	ステータス	ACLグループ名	ACLタイプ	対象ポート
グループの移動				
移動 <input checked="" type="radio"/> 選択したグループの一つ上に移動 <input type="radio"/> 選択したグループの一つ下に移動 <input type="text"/> (グループ番号)				

項目	内容
IPv6 ACLグループ一覧	ACLグループを一覧表示します。優先順位の高いグループから順に表示されます。
グループの移動	優先順位を移動したいグループを選択し、移動したい位置の一つ上(または下)となるグループ番号を入力します。「選択したグループの一つ上に移動」(または「選択したグループの一つ下に移動」)を選択し、[移動]をクリックします。

## ステータス

ACLの設定状況を表示します。

### 詳細設定 > ACL > ステータス

ACLグループ一覧 (優先度順)				
ポートフィルター		すべて ▼		
グループ番号	ステータス	ACLグループ名	ACLタイプ	対象ポート

#### MAC ACL

MAC ACLルール一覧 (優先度順)		
ACLグループ名	グループ番号	

#### IPv4 ACL

IPv4 ACLルール一覧 (優先度順)		
ACLグループ名	グループ番号	

#### IPv6 ACL

IPv6 ACLルール一覧 (優先度順)		
ACLグループ名	グループ番号	

項目	内容
ACLグループ一覧	ACLグループを一覧表示します。優先順位の高いグループから順に表示されます。「ポートフィルター」でポートを選択すると、選択したポートに適用しているACLグループだけが表示されます。
MAC ACLルール一覧	MAC ACLグループ名が表示されます。ルールが設定されたグループ名の左端に表示されている[+]ボタンをクリックすると、そのグループに設定されているルールが一覧表示されます。優先順位の高いルールから順に表示されます。
IPv4 ACLルール一覧	IPv4 ACLグループ名が表示されます。ルールが設定されたグループ名の左端に表示されている[+]ボタンをクリックすると、そのグループに設定されているルールが一覧表示されます。優先順位の高いルールから順に表示されます。
IPv6 ACLルール一覧	IPv6 ACLグループ名が表示されます。ルールが設定されたグループ名の左端に表示されている[+]ボタンをクリックすると、そのグループに設定されているルールが一覧表示されます。優先順位の高いルールから順に表示されます。

## ループ防止機能

ループ防止機能を設定します。

設定することで、ループ検出時に一時的にポートを無効にし、ループによるネットワークダウンを防止できます。

### メモ:

- ループ防止機能ではループの対策(通信経路の切り替え)は行われませんので、注意してください。  
ループ検出時にポートをブロックし、自動的に経路を切り替えるように設定したい場合は、[詳細設定]－[STP]－[設定]画面でSTP(スパニングツリー機能)を設定してください。
- ループ防止機能とSTPの違いは、[「ループによるネットワークダウンを防止する」\(P.123\)](#)を参照してください。

### 詳細設定 > ループ防止機能

ループ検出時の動作	
動作	<input type="radio"/> 何もしない <input checked="" type="radio"/> ポートを無効にする
無効化継続時間	60 秒
ループ検知方式	
MACスラッシング	<input type="checkbox"/> 有効
LDF	<input type="checkbox"/> 有効 MSTPが有効のときは、LDFを使用できません。
受信レート	<input type="checkbox"/> 有効 各ポートにおいて受信レートが下記の設定値を超えた場合にループと判断します。 受信レート閾値がトラフィック制御の入力帯域制限の値よりも大きい場合、ループが検知できない場合があります。
ポート受信レート閾値	
1	700 Mbps
2	700 Mbps
3	700 Mbps
4	700 Mbps
5	700 Mbps
6	700 Mbps
7	700 Mbps
8	700 Mbps

適用



項目	内容
動作	<p>ループ検出時の動作を設定します。</p> <p><b>メモ:</b> ループ検知方式を有効にしないとループ検出時の動作は実行されません。</p> <p><b>何もしない</b> ループを検出したポートに対して、何も操作を行いません。ただし、DIAGランプとループ検知されたポートのランプが「無効化継続時間」で設定された秒数だけ点滅します。設定した秒数経過後はいったん通常動作に戻りますが、もう一度ループが検知された場合はこの動作を繰り返します。</p> <p><b>ポートを無効にする</b> ループを検出したポートに対して、「無効化継続時間」で設定された秒数だけポートを無効にし、同時にDIAGランプとループ検知されたポートのランプが点滅します。設定した秒数経過後はいったん通常動作に戻りますが、もう一度ループが検知された場合はこの動作を繰り返します。</p>
無効化継続時間	ループ検出時の動作で「ポートを無効にする」を設定した際、ポートを無効にする時間(秒)を設定します。
MACスラッシング	ループ検知機能MACスラッシング方式を有効にします。1秒間に本製品のMACアドレスの学習回数が設定した閾値を超えた場合、ループと判断します。
LDF	<p>ループ検知機能LDF方式を有効にします。LDFパケットを2秒間隔で送信します。送信したLDFパケットを受信した場合、ループと判断します。</p> <p><b>メモ:</b> LDFはMSTPが有効の状態では使用できません。</p>
受信レート	ループ検知機能受信レート方式を有効にします。設定した受信レートを超えた場合、ループと判断します。
受信レート閾値	<p>ループと判断する受信レート閾値(1~1000Mbps)を設定します。</p> <p><b>メモ:</b> 受信レート閾値が、「トラフィック制御」の「入力帯域制限」の値よりも大きい場合、ループが検知できない場合があります。</p>

## DHCPリレー

レイヤー3モード時のみ表示されます。ほかのネットワークのDHCPメッセージを中継するDHCPリレーを設定します。

### 詳細設定 > DHCPリレー

DHCPリレーの有効化

DHCPリレー機能
☐有効

DHCPリレー設定

DHCPリレー

☒VLAN全体で1つのDHCPサーバーを設定する
☐VLANごとにDHCPサーバーを設定する

DHCPサーバー設定

DHCPサーバーIPv4アドレス

適用

項目	内容
DHCPリレー機能	「有効」にチェックを入れると、DHCPリレー機能が有効になります。
DHCPリレー設定	<p>一つのDHCPサーバーをすべてのVLANに適用する場合は「VLAN全体で1つのDHCPサーバーを設定する」を、VLANごとにDHCPサーバーを設定する場合は「VLANごとにDHCPサーバーを設定する」を選択してください。</p> <p>「VLAN全体で1つのDHCPサーバーを設定する」を選択した場合は、DHCPサーバーのIPv4アドレスを入力します。</p> <p>「VLANごとにDHCPサーバーを設定する」を選択した場合は、DHCPリレー機能を有効にするVLANにチェックを入れ、DHCPサーバーのIPv4アドレスを入力します。</p>

## キキNavi

キキNavi(インターネットを経由して遠隔地に設置した機器と管理者をつなぐ、当社のリモート管理サービス)に登録するために設定します。

### メモ:

- キキNaviのサービス概要、利用申請、使いかた、動作環境などについての詳細は、当社ホームページ(<https://www.buffalo.jp/biz/service/detail/kikinavi.html>)を参照してください。
- キキNaviを使用するには、SNTPを「使用する」にしてください。
- キキNavi使用中は、Admin Toolsは使用できません。
- 設定画面にキキNaviが表示されないときは、設定画面を表示させているブラウザを一度終了し、もう一度ブラウザを起動して設定画面を表示させてください。

### 詳細設定 > キキNavi

キキNaviは、インターネット経由で本製品を遠隔管理するサービスです。  
キキNaviを使用するには、SNTPを有効にしてください。  
インターネットへの経路にプロキシサーバーが設置されている場合は、プロキシサーバーを設定してください。そのとき、HTTPS 通信対応のプロキシサーバーを指定してください。

#### キキNavi設定

キキNavi ☒ 使用する

デバイス登録キー

#### SNTP設定

SNTP ☒ 使用する

サーバーIPアドレス/FQDN

ntp.jst.mfeed.ad.jp

更新間隔

24 (1~24時間)

#### プロキシ設定

プロキシ ☐ 使用する

サーバーIPアドレス/FQDN

ポート

ユーザー名

パスワード

適用

#### 登録状態

登録状態 クラウドサービスと通信できません。

更新

項目	内容
キキNavi	キキNaviを使用するかどうかを設定します。 <b>メモ:</b> キキNaviを使用する場合は、本製品がインターネット接続できる状態で設置されている必要があります。
デバイス登録キー	本製品をキキNaviに登録する際に使用するデバイス登録キー(12桁の数字)を入力します。 <b>メモ:</b> デバイス登録キーは、キキNaviの管理画面から発行します。詳細は、当社ホームページ( <a href="https://www.buffalo.jp/biz/service/detail/kikinavi.html">https://www.buffalo.jp/biz/service/detail/kikinavi.html</a> )に掲載の取扱説明書(「キキNaviユーザーマニュアル」)を参照してください。
SNTP	SNTPを使用するかどうかを設定します。 <b>メモ:</b> キキNaviを使用する場合は、SNTPを「使用する」に設定する必要があります。
サーバーIPアドレス/ FQDN	SNTPサーバーのIPアドレスまたはDNS解決可能なホスト名(FQDN)を設定します。FQDNを設定する場合は、[基本設定] - [VLAN] - [VLAN設定]画面でDNSサーバーを設定してください。
更新間隔	SNTPサーバーに時刻を問い合わせる間隔を時間で指定します。 単位は時間で、1～24時間の範囲で指定します。
プロキシ	インターネットへの経路にプロキシサーバーが設置されている場合は、プロキシサーバーを設定してください。 サーバーIPアドレス/FQDN: プロキシサーバーのIPアドレスまたは、ドメイン名・ホスト名を入力します。 ポート: プロキシサーバーで使用するポート番号を入力します。 ユーザー名: プロキシサーバーで設定されているユーザー名を入力します。 パスワード: 上記ユーザー名のパスワードを入力します。
登録状態	登録の状態を表示します。

## ファームウェア更新

ファームウェアファイルを使用して、ファームウェアの更新を行います。  
更新するファームウェアイメージを選択し、[選択]をクリックしてファームウェアイメージを選択して[更新]をクリックします。

### メモ:

- ファームウェア更新中は、本製品の電源をOFFにしたり、ブラウザを閉じたりしないでください。
- ファームウェアの更新を完了するには、本製品を再起動する必要があります。

### 管理 > ファームウェア更新

ファームウェア選択

ファイルイメージ

イメージ1 ▼

選択

更新

項目	内容
ファイルイメージ	更新するファームウェアイメージを選択します。

## デュアルイメージ

本製品はファームウェアを2つまで保持し、起動時にどちらのファームウェアを読み込むかを設定できます。

### 管理 > デュアルイメージ

イメージ名	動作	バージョン	イメージの説明
イメージ1	アクティブ	X.X.X.XX	
イメージ2	なし	X.X.X.XX	

デュアルイメージ設定	
イメージ名	イメージ1 ▼
動作	アクティブ ▼
イメージの説明	<input type="text"/>

適用

項目	内容
イメージ名	動作を変更したいイメージを選択します。
動作	<p>「イメージ名」で選択したファームウェアイメージに対する動作を設定します。</p> <p><b>アクティブ</b> ファームウェアイメージを使用します。 設定した内容は、本製品の再起動後に適用されます。</p> <p><b>なし</b> ファームウェアイメージを使用しません。 設定した内容は、本製品の再起動後に適用されます。</p> <p><b>削除</b> ファームウェアイメージを削除します。 [適用]をクリックすると、即時適用されます。</p>
イメージの説明	<p>選択したイメージに関する備考を入力します(半角英数字で50文字以下)。</p> <p><b>メモ:</b> イメージの説明は、本製品を初期化した場合でも出荷時設定(空欄)には戻りません。</p>

**メモ:** 現在アクティブにしているファームウェアよりも古いバージョンに切り替えると、一部の設定が削除されることがあります。

## 設定保存/復元

本製品の設定情報を保存したり復元したりします。

### 管理 > 設定保存/復元

設定の保存

現在の設定をファイルに保存します。

設定の復元

ファイル    
設定の復元中は、各設定を行うことはできません。

項目	内容
設定の保存	[保存]をクリックすると、現在の設定を保存します。 [詳細設定]－[キキNavi]および、[管理]－[ログ]の内容は保存されません。
設定の復元	[選択]をクリックして設定ファイルを選択し、[復元]をクリックすると設定の復元が開始します。 <b>メモ:</b> 設定の復元を完了するには、本製品を再起動する必要があります。

## 再起動

本製品を再起動します。

### 管理 > 再起動

再起動

システムの再起動

項目	内容
システムの再起動	[実行]をクリックすると、本製品を再起動します。

## 初期化

本製品の設定を工場出荷時の状態に戻します。

### 管理 > 初期化

初期化

IPアドレス以外のすべての設定を出荷時に戻す

出荷時設定に戻す

リセットボタン

有効 ▼

項目	内容
IPアドレス以外のすべての設定を出荷時に戻す	[実行]をクリックすると、IPv4/IPv6アドレスの設定だけを保持し、その他のすべての設定を出荷時に戻します。
出荷時設定に戻す	[実行]をクリックすると、すべての設定を出荷時に戻します。
リセットボタン	本製品本体のリセットボタンの有効/無効を設定します。

#### メモ:

- リセットボタンが「有効」の場合、約3秒間リセットボタンを押し続けると本製品の設定をご購入時の状態に戻すことができます。
- リセットボタンが「無効」で、本製品のユーザー名やパスワードを忘れた場合は、保証の有無に関わらず、有償修理となります。当社修理センターに修理をご依頼ください。

## ARPテーブル

レイヤー3モード時のみ表示されます。

**メモ:** ARPテーブルに保持できる機器の数は512台までです。

### ポート順

本製品に接続している機器のIPアドレスとMACアドレスをポート順に表示します。ポート番号を選択すると、選択したポートに接続されている機器だけを表示します。

管理 > ARPテーブル > ポート順

ホストエントリー数  
現在のホストエントリー数: 1/512

ホストエントリー情報  
ポート番号 すべて

<input type="checkbox"/>	インデックス	IPv4アドレス	MACアドレス	VLAN	ポート	タイプ
<input type="checkbox"/>	1	192.168.1.5	XX:XX:XX:XX:XX:XX	1	1	動的

削除

更新

クリア

### IPアドレス順

本製品に接続している機器のIPアドレスとMACアドレスをIPアドレス順に表示します。

管理 > ARPテーブル > IPアドレス順

ホストエントリー数  
現在のホストエントリー数: 1/512

ホストエントリー情報

<input type="checkbox"/>	インデックス	IPv4アドレス	MACアドレス	VLAN	ポート	タイプ
<input type="checkbox"/>	1	192.168.1.5	XX:XX:XX:XX:XX:XX	1	1	動的

削除

更新

クリア



## MACアドレステーブル

### ポート順

MACアドレステーブルをポート順に表示します。ポート番号を選択すると、選択したポートに接続されているMACアドレスだけを表示します。

管理 > MACアドレステーブル > ポート順

ポート番号 <span>すべて</span> ▼					
インデックス	ポート	VLAN ID	MACアドレス	ステータス	端末の認証状態
1	1	-	XX-XX-XX-XX-XX-XX	動的	未認証
<span>更新</span> <span>クリア</span>					

### MACアドレス順

MACアドレステーブルをMACアドレス順に表示します。

管理 > MACアドレステーブル > MACアドレス順

インデックス	ポート	VLAN ID	MACアドレス	ステータス	端末の認証状態
1	1	-	XX-XX-XX-XX-XX-XX	動的	未認証
<span>更新</span> <span>クリア</span>					

#### メモ:

- 802.1X ポートで認証が成功した場合でも、「端末の認証状態」は「未認証」と表示されます。802.1X ポートの認証状態は、「詳細設定」－「認証」－「ステータス」で確認できます。
- 802.1X MACまたはMAC認証の認証状態は、「端末の認証状態」に「未認証」、「認証済み」、「ゲストVLAN(VID: <VLAN番号>）」、「ダイナミックVLAN(VID: <VLAN番号>）」のいずれかで表示されます。

## 統計情報

本製品の統計情報を表示します。

メモ:

- 各統計情報の上限値は、4,294,967,295です。上限に達すると0に戻ります。
- 本製品を再起動すると、統計情報は0に戻ります。

### 管理 > 統計情報

<input type="checkbox"/>	ポート	ポート名	受信オクテット	受信パケット	送信オクテット	送信パケット	
<input type="checkbox"/>	1	Port 1	3392511	11362	6304619	6514	詳細
<input type="checkbox"/>	2	Port 2	0	0	0	0	詳細
<input type="checkbox"/>	3	Port 3	0	0	0	0	詳細
<input type="checkbox"/>	4	Port 4	0	0	0	0	詳細
<input type="checkbox"/>	5	Port 5	0	0	0	0	詳細
<input type="checkbox"/>	6	Port 6	0	0	0	0	詳細
<input type="checkbox"/>	7	Port 7	0	0	0	0	詳細
<input type="checkbox"/>	8	Port 8	0	0	0	0	詳細

更新 クリア

項目	内容
ポート名	ポートの名称が表示されます。
受信オクテット	受信したデータの総オクテット数が表示されます。
受信パケット	受信したパケットの総数が表示されます。
送信オクテット	送信したデータの総オクテット数が表示されます。
送信パケット	送信したパケットの総数が表示されます。
詳細	クリックすると、詳細情報が表示されます。
ポート統計情報	選択したポートが受信・送信したパケットなどの総数を表示します。
EAP統計情報	EAPパケットの受信・送信したパケットなどの総数を表示します。

以下の項目は、「詳細」をクリックしたときに表示されます。

項目	内容
受信オクテット	受信したデータの総オクテット数が表示されます。
受信ユニキャストパケット	受信したユニキャストパケット数が表示されます。
受信マルチキャストパケット	受信したマルチキャストパケット数が表示されます。
受信ブロードキャストパケット	受信したブロードキャストパケット数が表示されます。
破棄された受信パケット	受信したパケットのうち、ほかのポートに転送されず破棄されたパケットの数が表示されます。
受信エラーパケット	受信したパケットのうち、FCSエラーによって破棄されたパケットの数が表示されます。
送信オクテット	送信したデータの総オクテット数が表示されます。

項目	内容
送信ユニキャストパケット	送信したユニキャストパケット数が表示されます。
送信マルチキャストパケット	送信したマルチキャストパケット数が表示されます。
送信ブロードキャストパケット	送信したブロードキャストパケット数が表示されます。
破棄された送信パケット	送信に失敗したパケット数が表示されます。
Rx合計フレーム	受信したEAPパケット数が表示されます。
Tx合計フレーム	送信したEAPパケット数表示されます。
Rx開始フレーム	受信したEAPOL Startパケット数が表示されます。
Rxログオフフレーム	受信したEAPOL Logoffパケット数が表示されます。
Txリクエスト/IDフレーム	送信したEAPパケットのうち、Code:Request (1) Type:Identity (1)の数が表示されます。
Txリクエストフレーム	送信したEAPパケットのうち、Code:Request (1) Type:Identity (1)以外の数が表示されます。
Rx応答/IDフレーム	受信したEAPパケットのうち、Code:Response (2) Type:Identity (1)の数が表示されます。
Rx応答フレーム	受信したEAPパケットのうち、Code:Response (2) Type:Identity (1)以外の数が表示されます。
Rx無効フレーム	受信したEAPパケットのうち、Typeが不正である数が表示されます。
Rxエラー長フレーム	受信したEAPパケットのうち、パケット長が不正である数が表示されます。
最終フレームバージョン	そのポートで最後に受信したEAPパケットのバージョンが表示されます。
最終フレームソース	そのポートで最後に受信したEAPパケットの送信元MACアドレスが表示されます。

**メモ:**

- ・ 本製品がレイヤー2モードのとき、本製品宛てのパケット(本製品へのpingや設定画面を表示するためのhttp通信など)は「受信ユニキャストパケット」および「破棄された受信パケット」として扱われます。
- ・ 本製品がレイヤー3モードのとき、本製品宛てのパケットは「受信ユニキャストパケット」として扱われます。
- ・ 統計情報でカウントされるパケットは、MACフレームおよびIPv4/IPv6パケットの両方が対象です。

## ログ

本製品のログ情報を表示します。

### メモ:

- 本製品に記録できるログは、合計で512件までです。512件を超えた場合、最も古いものから削除されます。
- 記録されたログは、本製品の電源を切るとすべて削除されます。

### 管理 > ログ

ログ

表示するログ システム ▾

古い << < > >> 新しい 消去

時刻	ログ
2021/01/01 00:00:15	Cold start
2021/01/01 00:00:15	Port 1 link up

項目	内容
表示するログ	表示するログメッセージの種類を選択します。

## Syslog設定

本製品のログ情報をSyslogサーバーに転送するように設定します。

### 管理 > Syslog設定

Syslog設定	
ログ情報転送機能	<input type="checkbox"/> 有効
IPアドレス/FQDN	<input type="text" value="0.0.0.0"/>
ヘッダーに付加する情報	MACアドレスとシステム名 ▼

ログの種類	
設定	通知 + 詳細 ▼
認証	通知 + 詳細 ▼
デバイス	通知 + 詳細 ▼
システム	通知 + 詳細 ▼
キキNavi	通知 + 詳細 ▼

項目	内容
ログ情報転送機能	Syslogサーバーの有効/無効を設定します。
IPアドレス/FQDN	SyslogサーバーのIPアドレスまたは、ドメイン名・ホスト名を入力します。
ヘッダーに付加する情報	転送するデータのヘッダーに付加する情報を選択します。
ログの種類	送信するログの種別を選択します。

## ネットワーク診断

特定のIPアドレスに対して通信テストを行います。

### 管理 > ネットワーク診断

The screenshot shows two test sections. The first section is titled 'Ping' and contains a text input field labeled 'IPアドレス' (IP Address) and a button labeled '適用' (Apply). The second section is titled 'Traceroute' and also contains a text input field labeled 'IPアドレス' (IP Address) and a button labeled '適用' (Apply).

項目	内容
Ping	確認するIPv4/IPv6アドレスまたはDNS解決可能なホスト名(FQDN)を入力して[適用]をクリックすると、その宛先に対してPingテストを行います。
Traceroute	確認するIPv4アドレスまたはDNS解決可能なホスト名(FQDN)を入力して[適用]をクリックすると、その宛先に対してTracerouteテストを行います。

**メモ:** DNS解決可能なホスト名(FQDN)を入力する場合は、[基本設定]－[VLAN]－[VLAN設定]画面でDNSサーバーを設定しておく必要があります。

## ケーブル診断

[診断実行]をクリックすると、各ポートに接続されているLANケーブルの異常を確認します。診断を正しく実行するには、あらかじめ本製品と接続先の機器に以下を設定してください。

- ・オートネゴシエーション:有効
- ・IEEE 802.3az(EEE):無効
- ・オートパワーダウン(APD):無効

### 管理 > ケーブル診断

ポート	ケーブルステータス
1	Open
2	Open
3	Open
4	Open
5	Open
6	Open
7	Open
8	Open

診断実行

項目	内容
ケーブルステータス	<p>ケーブルの状態を表示します。</p> <p><b>Open</b> ケーブルが接続されていません。</p> <p><b>OK</b> ケーブルが接続されており、ケーブルに異常はありません。</p> <p><b>ショート</b> ケーブルが短絡している可能性があります。</p> <p><b>不明</b> 診断できません。</p>

## I'm here

スイッチを複数台使用している環境で本製品を見つけるときに使用します。

管理 > I'm here



実行

停止

項目	内容
LED点滅時間	[実行]をクリックすると入力した時間(秒)、POWERランプを除く本製品のすべてのランプが点滅します。 点滅中に[停止]をクリックすると点滅が停止します。



## 第3章 困ったときは

### ランプが点灯しない、異常点灯・点滅している

現象	対処方法
POWERランプが点灯しない	電源ケーブルまたはACアダプターがコンセントに接続されているかを確認してください。
DIAGランプが赤色点滅している	<ul style="list-style-type: none"><li>1秒間隔で点滅している場合、ループを検知しています。各ポートの配線を見直してください。</li><li>高速点滅している場合、ファンのエラーが発生しています(<a href="#">「FAN搭載製品」(P.115)</a>のみ)。一度電源ケーブルを取り外し、挿し直してください。それでも点滅している場合は、当社サポートセンターまでお問い合わせください。</li></ul>
LINK/ACTランプが点灯しない	<ul style="list-style-type: none"><li>LANケーブルが本製品と接続している機器の両方に正しく接続されているか確認してください。</li><li>本製品と接続している機器の両方の電源がオンになっているかを確認してください。</li><li>適切なタイプのLANケーブルを使用しているか、また、LANケーブルの長さが規格を超えていないかを確認してください。</li><li>お使いの機器の通信規格が本製品に対応しているかを確認してください。</li><li>通信方式の設定変更ができる機器をお使いの場合は、お使いの機器と本製品の通信方式をオートネゴシエーション(自動認識)に設定してから接続してください。</li></ul>
PoEランプが緑色点滅している PoEランプが点灯しない (PoE対応製品のみ)	<p>PoE受電機器の電源をOFFにした後や、動作モードを休止やサスペンドにしているときなど、PoE受電機器の消費電流が少なくなったときに、PoEが給電状態(緑色点灯)と非給電状態(消灯)を繰り返す場合があります。</p> <p>これにより、PoEランプが緑色点滅しているように見えたり、消灯しているように見えたりする場合がありますが、故障ではありません。動作モードを休止やサスペンドにしている場合は、設定の変更をお試しください。</p> <p><b>メモ:</b></p> <ul style="list-style-type: none"><li>この場合、[基本設定]－[SNMP]－[SNMPトラップ]で「PoE給電/非給電」のトラップを有効にしていると、PoEランプが消灯していても、PoEの給電/非給電の繰り返しによりトラップが数秒間隔で送信されることがあります。</li><li>この場合、PoEランプが消灯していても、[基本設定]－[PoE]－[PoEステータス]では給電中のステータスで表示されることがあります。</li></ul>
本製品のリセットボタンを押しても設定を初期化できない	<ul style="list-style-type: none"><li>設定画面で本製品のリセットボタンが無効になっていないか確認してください。</li><li>リセットボタンが無効になっている状態で本製品のユーザー名やパスワードを忘れた場合は、有償修理となります。当社修理センターに修理をご依頼ください。</li></ul>

---

## 設定画面が表示できない

---

- 設定画面を表示したい機器が本製品に正しく接続されているかを確認してください。
- 本製品に設定したIPアドレス(出荷時は192.168.1.254)で設定画面にアクセスしてください。
- ユーザー名(出荷時は「admin」)とパスワード(出荷時は「password」)が正しいかを確認してください。  
ユーザー名やパスワードを忘れた場合は、本体前面のリセットボタンを約3秒間押して初期化してください。
- ブラウザーでプロキシ設定がされている場合は、プロキシ設定を解除するか、プロキシの例外設定に本製品のIPアドレスを登録してください。
- 設定画面を表示したい機器を管理アクセス用VLANのメンバーであるLAN端子に接続しているかを確認してください。

---

## パスワードを忘れた

---

- ユーザー名やパスワードを初期設定(ユーザー名「admin」、パスワード「password」)から変更している場合は、リセットボタンを押して初期化してください。
- 設定画面でリセットボタンを無効にする設定をしている場合、ユーザー名やパスワードを初期設定に戻すことができなくなるため有償修理が必要となります。当社修理センターに修理を依頼してください。

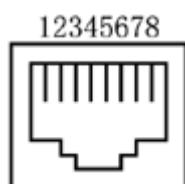
# 付録

## 仕様

ハードウェア仕様については、製品に付属の「取扱説明書」を確認してください。

## 端子仕様

LAN端子/Internet端子仕様  
形状(RJ-45型8極)



100BASE-TX/10BASE-T		
ピン番号	信号名	信号機能
1	RD+/TD+	受信データ(+)/送信データ(+)
2	RD-/TD-	受信データ(-)/送信データ(-)
3	TD+/RD+	送信データ(+)/受信データ(+)
4	(Not Use)	未使用
5	(Not Use)	未使用
6	TD-/RD-	送信データ(-)/受信データ(-)
7	(Not Use)	未使用
8	(Not Use)	未使用
1000BASE-T		
ピン番号	信号名	信号機能
1	BI_DA+/BI_DB+	送受信データA(+)/送受信データB(+)
2	BI_DA-/BI_DB-	送受信データA(-)/送受信データB(-)
3	BI_DB+/BI_DA+	送受信データB(+)/送受信データA(+)
4	BI_DC+/BI_DD+	送受信データC(+)/送受信データD(+)
5	BI_DC-/BI_DD-	送受信データC(-)/送受信データD(-)
6	BI_DB-/BI_DA-	送受信データB(-)/送受信データA(-)
7	BI_DD+/BI_DC+	送受信データD(+)/送受信データC(+)
8	BI_DD-/BI_DC-	送受信データD(-)/送受信データC(-)

✕モ: Auto MDI/MDI-X機能により、送信/受信データを自動的に切り替えます。

PoE仕様(PoE対応製品のみ、Alternative A)

ピン番号	出力
1	Negative Vpse
2	Negative Vpse
3	Positive Vpse
4	-
5	-
6	Positive Vpse
7	-
8	-

## FAN搭載製品

本書に記載の「FAN搭載製品」の型番は以下のとおりです。

- BS-GS2116P
- BS-GS2124P
- BS-GS2124P/HP
- BS-GS2148

## 初期設定一覧

機能		項目	出荷時設定
システム情報設定		スイッチ名	BS + 本製品のMACアドレス
		設置場所	Not defined
		管理者	Not defined
VLAN	VLAN設定	VLANモード	VLAN設定
		VLAN ID	1
		VLAN名	なし
		管理VLAN	有効
		IPv4アドレス取得方法	固定IPアドレス
		IPv4アドレス	192.168.1.254
		サブネットマスク	255.255.255.0
		デフォルトゲートウェイ	0.0.0.0
		DNS取得方法	手動設定
		プライマリーDNSサーバー	0.0.0.0
		セカンダリーDNSサーバー	0.0.0.0
		IPv6	無効
		ポート	すべて「Untagged」
	VLANポート設定	PVID	すべて「1」
		受信するフレームの種類	すべて「すべて」
		イングレスフィルター	すべて有効
		プロテクトポート	すべて無効
ルーティング	レイヤー設定	モード	レイヤー2モード
	静的ルーティング (レイヤー3モード時のみ)	デフォルトゲートウェイ	0.0.0.0

機能		項目	出荷時設定
SNMP	SNMPコミュニティテーブル	コミュニティ名	#1のみ「public」
		Get	#1のみ有効
		Set	無効
		Trap	無効
	SNMPホストテーブル	ホスト認証	無効
	SNMPトラップ	認証トラップ	無効
		リンクアップ/ダウン	無効
		STP	無効
		ループ検知	無効
		トランク	無効
		FANエラー (「 <a href="#">FAN搭載製品</a> 」(P.115)のみ)	無効
		PoEオーバーロード (PoE対応製品のみ)	無効
		PoE給電/非給電 (PoE対応製品のみ)	無効
	SNMPv3ユーザー	ユーザー名	#1のみ「admin」
		アクセス制限	読み込みのみ
		認証方式	なし
		認証キー	なし
		暗号化方式	なし
		暗号化キー	なし

機能		項目	出荷時設定
LLDP	設定	LLDP送信間隔	30秒
		Hold Multiplier	4
		Reinitializing Delay	2秒
		Transmit Delay	2秒
		Fast Start Duration	3回
	LLDPポート	ステータス	すべて「Tx and Rx」
		通知	すべて無効
		Port Description TLV	すべて無効
		System Name TLV	すべて無効
		System Description TLV	すべて無効
		System Capabilities TLV	すべて無効
		Management Address TLV	すべて無効
	LLDP-MEDポート	ステータス	すべて無効
		通知	すべて無効
		Capabilities TLV	すべて無効
		Network Policy TLV	すべて無効
		Extend Power TLV (PoE対応製品のみ)	すべて無効
		Software Revision TLV	すべて無効
MACアドレス	MACアドレス学習方式	モード	SVL
	静的MACフィルター	静的MACフィルター	無効
	動的MACフィルター	動的MACフィルター	無効 設定台数:なし
	MACアドレスエージング	エージングタイム	300秒
ポート設定	速度/モード設定	ポート名	Port 1～(ポート番号の数字が入ります)
		管理	すべて有効
		速度/通信方式	すべて「オートネゴシエーション」
		フロー制御	すべて無効
		IEEE 802.3az	すべて無効
		APD	すべて有効
		Jumbo Frame	すべて有効

機能		項目	出荷時設定
システムセキュリティ	アカウント管理	管理ユーザー名	admin
		管理パスワード	password
	アクセス管理	SNMP	有効
		HTTPS	無効
		Webセッションタイムアウト時間	5分
		Web最大セッション数	5
		ポート	443
		HTTPSセッションタイムアウト時間	5分
		HTTPS最大セッション数	2
		日付と時刻	
時刻設定	2021/01/01 00:00:00		
サーバーIPアドレス/FQDN	ntp.jst.mfeed.ad.jp		
更新間隔	24時間		
タイムゾーン	(GMT+09:00) Osaka, Sapporo, Tokyo		
PoE (PoE対応製品のみ)	PoEガードバンド	ガードバンド電力	0W
	PoEプロファイル設定	プロファイル名	Profile1～4
		PoE	すべて有効
		優先度	すべて「低」
		ハイパワー	すべて「at」
		ランプを消灯する	消灯しない
	PoEスケジューラー	スケジューラー機能	無効(手動切替)
		プロファイル(手動切替時)	Profile1
		表示	週間スケジュール
QoS	QoS設定	QoS機能	無効
		スケジュール方法	WRR
		優先度選択	CoS
	QoSマッピング	ポート優先度	すべて「0」
		CoSマッピング	CoS値0～7の順に、2、0、1、3、4、5、6、7
	VoIP優先制御	VoIP優先制御機能	無効
		CoS	7



機能		項目	出荷時設定
セキュリティ	DOS攻撃防止	Land攻撃	無効
		最小TCPヘッダー	無効
		TCP/UDP L4ポート	無効
		ICMP	無効
		TCPフラグ	無効
	DHCPスヌーピング	DHCPスヌーピング	無効
		DHCPオプション82	無効
		レート制限	なし
		ステータス	すべて「Trusted」
認証	RADIUS	認証	プライマリー認証サーバー:有効 セカンダリー認証サーバー:無効
		認証サーバーIPアドレス	1.1.1.1
		認証サーバーポート	1812
		共有暗号化キー	なし
		リセットタイマー	3600秒
		拡張設定	Accounting:無効 Termination-Action:無効 ダイナミックVLAN:無効
	ポート認証	802.1Xポート	すべて無効
		802.1X MAC	すべて無効
		MAC認証	すべて無効
		EAP透過設定	無効
		ゲストVLAN	無効
		VLAN ID	すべて「0」
		ゲストVLAN移行期限	すべて「60」
ポートトランク	トランクモード		LACP
	トランクキー		なし
	トランク名		なし
	システム優先度		32768
	メンバー		なし
トラフィック制御	ブロードキャスト		すべて無制限
	マルチキャスト		すべて無制限
	DLF		すべて無制限
	入力帯域制限		1000 Mbps
	出力帯域制限		1000 Mbps
ミラーリング	有効		ミラー1:無効 ミラー2:無効
	ミラー元ポート		ミラー1:2 ミラー2:4
	ミラー先ポート		ミラー1:1 ミラー2:3

機能		項目	出荷時設定
STP	設定	STP設定	無効
		Hello Time	2秒
		Max Age	20秒
		Forward Delay	15秒
		Max Hop Count (MSTPのみ)	20
		Bridge Priority	32768
		BPDU転送 (STP無効時のみ)	無効
		MST Configuration Name (MSTPのみ)	本製品のMACアドレスから自動的に生成
		MST Revision Level (MSTPのみ)	0
	ポート	MSTI/CIST (MSTPのみ)	CIST
パスコスト		自動	
優先度		すべて128	
パスコスト		すべて20000	
Fastlink		すべて無効	
IGMP	設定	IGMPスヌーピング	無効
		未知のマルチキャストを フィルタリングする	無効
		ホストタイムアウト	260秒
		ルーターポートタイムアウト	125秒
	IGMPクエリア	IGMPクエリア	無効
		IGMPクエリア送信間隔	60秒
		送信元IPv4アドレス	0.0.0.0
		Max Response Time	10秒
MLD	設定	MLDスヌーピング	無効
		未知のマルチキャストを フィルタリングする	無効
		ホストタイムアウト	260秒
		ルーターポートタイムアウト	125秒
	MLDクエリア	MLDクエリア	無効
		MLDクエリア送信間隔	60秒
		送信元IPv6アドレス	::
		Max Response Time	10秒

機能	項目	出荷時設定
ループ防止機能	動作	ポートを無効にする
	無効化継続時間	60秒
	MACスラッシング	無効
	LDF	無効
	受信レート	無効
	受信レート閾値	700 Mbps
DHCPリレー (レイヤー3モード時のみ)	DHCPリレー機能	無効
	DHCPリレー	VLAN全体で1つのDHCPサーバーを設定する
	DHCPサーバーIPv4アドレス	0.0.0.0
キキNavi	キキNavi	使用しない デバイス登録キー:なし
	SNTP	使用しない サーバーIPアドレス/FQDN: ntp.jst.mfeed.ad.jp 更新間隔:24時間毎
	プロキシ	使用しない サーバーIPアドレス/FQDN、ポート、 ユーザー名、パスワード:なし
初期化	リセットボタン	有効
Syslog設定	ログ情報転送機能	無効
	IPアドレス/FQDN	0.0.0.0
	ヘッダーに付加する情報	MACアドレスとシステム名
	設定	通知 + 詳細
	認証	通知 + 詳細
	デバイス	通知 + 詳細
	システム	通知 + 詳細
	キキNavi	通知 + 詳細
I'm here	LED点滅時間	60秒

## エラー番号一覧

本製品に異常が発生している場合、以下のエラーがキキNaviに表示されます。

**メモ:** エラー番号を表示するにはキキNaviの設定が必要です。

エラー番号	概要	対処
E10 (PoE対応製品のみ)	各ポートに決められているPoEの最大供給電力を超えたポートを検出しました。	本製品から電力供給が可能かどうか、ネットワーク機器の仕様を確認してください。 本製品からの電力供給が不足する場合、PoEからの電力供給をやめて電源ケーブルやACアダプターなどから電力を供給してください。
E11 (PoE対応製品のみ)	PoE全体の最大供給電力を超えました。	本製品の最大供給電力の範囲内におさまるように、電力を供給するネットワーク機器の台数を減らしてください。
E30	ネットワークのループを検出しました。	ループが検知されたポートの配線を見直してください。
E20 (「 <a href="#">FAN搭載製品</a> 」(P.115)のみ)	ファンの動作にエラーを検出しました。	ファンに異物やホコリがないか確認してください。異物やホコリがあったときは、ピンセットやエアダスターなどで除去した後に本製品を再起動してください。除去を行い再起動した後もエラーが発生する場合は、当社サポートセンターまでお問い合わせください。

## ループによるネットワークダウンを防止する

ループによるネットワークダウンを防止する場合、「ループ防止機能」または「STP(スパニングツリー機能)」をご利用いただけます。機能の違いは以下のとおりです。お使いの環境に合わせてご利用ください。

「ループ防止機能」の設定画面についての説明は、[「ループ防止機能」\(P.95\)](#)を参照してください。

「STP(スパニングツリー機能)」の設定画面についての説明は、[「STP」\(P.72\)](#)を参照してください。

	ループ防止機能	STP(スパニングツリー機能)
ループ検出時の動作	ポートを一定時間無効にします。 ※設定した時間が経過後は、無効化したポートを有効にします。	ポートを自動的にブロックし、通信経路を切り替えます。
ループ解消方法	手動 ※ポートが無効になっている間は、一時的に通信できます。 ※ストームコントロールを有効にしている場合を除き、ループが解消されるまで通信できません。	自動 ※経路の切り替え中は、通信が途切れます。
推奨環境	小規模ネットワーク	すでにSTPが設定されている大・中規模ネットワーク、およびループを完全に防止したい環境

---

## 本書について

---

- 本書の著作権は当社に帰属します。本書の一部または全部を当社に無断で転載、複製、改変などを行うことは禁じられております。
- 本書に記載された仕様、デザイン、その他の内容については、改良のため予告なしに変更される場合があります。現に購入された製品とは一部異なることがあります。
- 本書の内容に関しては万全を期して作成していますが、万一ご不審な点や誤り、記載漏れなどがありましたら、お買い求めになった販売店または当社サポートセンターまでご連絡ください。
- 本製品(付属品等を含む)を輸出または提供する場合は、外国為替及び外国貿易法および米国輸出管理関連法規等の規制をご確認の上、必要な手続きをおとりください。
- 本製品の使用に際しては、本書に記載した使用方法に沿ってご使用ください。特に、注意事項として記載された取扱方法に違反する使用はお止めください。

---

## 免責事項

---

- 本製品は、医療機器、原子力設備や機器、航空宇宙機器、輸送設備や機器など人命に関わる設備や機器、及び高度な信頼性を必要とする設備や機器としての使用またはこれらに組み込んだ使用は意図されておりません。これら、設備や機器、制御システムなどに本製品を使用され、本製品の故障により、人身事故、火災事故、社会的な損害などが生じても、当社ではいかなる責任も負いかねます。設備や設計、制御システムなどにおいて、冗長設計、火災延焼対策設計、誤動作防止設計など、安全設計に万全を期されるようご注意願います。
- 本製品は、日本国内での使用を前提に設計・製造されています。日本国外での使用における故障・不具合についての責任は負いかねますので、あらかじめご了承ください。
- 当社は、製品の故障に関して一定の条件下で修理を保証しますが、記憶されたデータが消失・破損した場合には、保証しておりません。本製品がハードディスク等の記憶装置の場合または記憶装置に接続して使用するものである場合は、本書に記載された注意事項を遵守してください。また、必要なデータはバックアップを作成してください。お客様が、本書の注意事項に違反し、またはバックアップの作成を怠ったために、データを消失・破棄に伴う損害が発生した場合であっても、当社はその責任を負いかねますのであらかじめご了承ください。
- 本製品に起因する債務不履行または不法行為に基づく損害賠償責任は、当社に故意または重大な過失があった場合を除き、本製品の購入代金と同額を上限と致します。
- 本製品に契約の不適合があった場合、無償にて当該契約不適合を修補し、または契約不適合のない同一製品または同等品に交換致しますが、当該契約不適合に基づく損害賠償の責に任じません。
- 本書に記載された責任は、日本国内においてのみ有効です。

---

## 使用ソフトウェアについて

---

本製品は、GPL/LGPL の適用ソフトウェアを使用しており、これらのソフトウェアのソースコードの入手、改変、再配布の権利があることをお知らせします。オープンソースとしての性質上著作権による保証はなされておきませんが、本製品については保証書記載の条件により当社による保証がなされています。GPL/LGPL のライセンスについては、当社ホームページをご覧ください。変更済みGPL 対象モジュール、その配布方法については、当社のホームページ(<https://www.buffalo.jp/download/>)をご覧ください。サポートセンターにご連絡ください。配布時発生する費用は、お客様のご負担となります。

---

## 商標・登録商標

---

本書に記載されている他社製品名は、一般に各社の商標または登録商標です。本書では一部を除き、™、®、©などのマークは記載していません。