

ELECOM

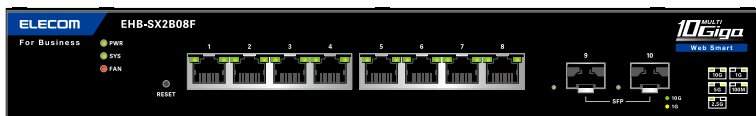
User's Manual

ユーザーズマニュアル

第2版 2025/10/28

レイヤー2 10Gマルチギガ対応 Webスマートスイッチ

EHB-SX2B08F



対象ファームウェア：Ver.1.0.0以降

レイヤー2 2.5Gマルチギガ対応 Webスマートスイッチ

EHB-SQ2B08



対象ファームウェア：Ver.1.0.0以降

この度は、エレコムのギガビットスイッチングハブをお買い上げいただき誠にありがとうございます。
このマニュアルには本製品を使用するにあたっての詳細な設定方法が説明されています。
また、お客様が本製品を安全に扱っていただくための注意事項が記載されています。詳細な設定を行う場合は、必ずこのマニュアルをお読みになってください。

- 本製品の基本的な導入手順については、付属の「クイックセットアップガイド」などをお読みください。

導入編	8
用語	9
このマニュアルで使われている用語	9
このマニュアルで使われている記号	9
このマニュアルをお読みになる前に	10
「クイックセットアップガイド」の主な内容	10
設定リファレンス編	11
管理画面(設定画面)を表示する	18
各メニューについて	19
ダッシュボード	19
モニター	19
システム	20
ポート	22
設定の保存と再起動	31
ダッシュボード	32
モニター	34
ARPテーブル	34
IPアドレステーブル	35
MACアドレステーブル	36
ポートステータス	38
ポートステータス	38
DDMI	41
ポート使用率	43
システム情報	44
システムログ	45
システム	46
一般設定	46
インターフェース設定	48

IP アドレス設定	50
IP アドレスステータス	50
IP アドレス設定	51
【IPv6】ステータス	53
【IPv6】グローバル設定	56
【IPv6】インターフェース設定	57
【IPv6】アドレス設定	59
IPv6 リンクローカルアドレス設定	59
IPv6 グローバルアドレス設定	61
【IPv6】DHCPv6 クライアント設定	63
ユーザーアカウント	65
Administrator	65
ユーザーアカウント編集	66
SNMP	67
SNMP	67
SNMP ユーザー	69
SNMP トラップグループ	72
SNMP トラップポート	73
スイッチ設定	74
Syslog 設定	75
【アドミリンク】基本設定	77
【アドミリンク】詳細設定	78
ポート	80
Green Ethernet	80
リンクアグリゲーション	82
リンクアグリゲーションステータス	82
リンクアグリゲーション設定	84
リンクアグリゲーション制御プロトコル	86
LLDP	88
LLDP ローカルステータス	88
LLDP リモートステータス	91

LLDP 設定	96
Basic TLV Setting	98
Org-specific TLV Setting	99
ポート設定	100
スイッチング	103
ループ防止	103
ミラーリング	104
【マルチキャスト】IPv4 マルチキャスト	105
IPv4 マルチキャストステータス	105
IGMP snooping	106
IGMP snooping VLAN	109
【マルチキャスト】IPv6 マルチキャスト	111
IPv6 マルチキャストステータス	111
MLD snooping プロキシ	112
VLAN	113
ポートロール設定	116
【マルチキャスト】静的マルチキャスト転送	118
【Qos】Diffserv	120
Diffserv	120
DSCP 設定	121
【Qos】キューイング方式	122
【Qos】キュー優先度	124
【Qos】帯域幅制御	125
【スパンニングツリー】ステータス	126
【スパンニングツリー】設定	132
【スパンニングツリー】RSTP	134
【スパンニングツリー】MSTP	137
MSTP	137
MSTP ポート設定	140
静的MACフィルタリング	141
静的MAC転送	143

【VLAN】VLANステータス	145
【VLAN】VLAN設定	147
静的VLAN	147
VLANポート設定	149
【VLAN】Voice VLAN設定	151
VLANアイソレーション	153
VLANマッピング	155
VLANマッピング	155
VLANマッピング設定	156
ネットワーク	158
【ARP設定】ARPラーニング	158
【ARP設定】静的ARP	159
セキュリティ	161
【AAA】RADIUSサーバー設定	161
【AAA】AAA設定	163
【ACL】Classifier	165
Classifierステータス	165
Classifier設定	166
Classifierグローバル設定	170
【ACL】Policy Rule	171
アンチARPスキャン	175
ステータス	175
ホストステータス	176
設定	177
信頼ホスト	178
BPDUガード	180
ステータス	180
設定	181
ストームコントロール	182
Dos攻撃防止	183
Errdisable	185

【IPv4ソースガード】IPv4ソースガード	186
IP ソースガード	186
静的バインディング	187
【IPv4ソースガード】DHCP snooping	190
ステータス	190
設定	193
ポート設定	195
VLAN 設定	196
VLAN ポート設定	197
【IPv4ソースガード】DHCP Option82 プロファイル	199
【IPv4ソースガード】ARP インспекション	201
ステータス	201
VLANステータス	202
ログステータス	203
設定	204
ポート設定	206
VLAN 設定	207
【IPv6ソースガード】IPv6 静的バインディング	208
IPv6 送信元バインディング状態	208
IPv6 静的バインディング	210
【IPv6ソースガード】IPv6 ソースガード	212
ポリシー	212
ポート設定	214
【IPv6ソースガード】IPv6 snooping	215
ポリシー設定	215
VLAN 設定	217
【IPv6ソースガード】DHCPv6 信頼設定	219
ポート認証	221
ポートセキュリティ	223
管理	225
【設定】設定の復元	225
TFTP で更新する場合	225

HTTPで更新する場合	226
【設定】設定のバックアップ	227
TFTPでバックアップする場合	227
HTTPでバックアップする場合	228
【設定】実行設定の消去	230
【設定】設定の保存	231
診断	232
ファームウェア更新	235
新しいファームウェアをアップロードする	236
再起動	238

付録編	239
------------	------------

安全上のご注意	240
使用上のご注意	243
このマニュアルについて	244
製品の保証について	245
製品の保証とサービス	245
サポートサービスについて	246

導入編


用語	9
このマニュアルで使われている用語	9
このマニュアルで使われている記号	9
このマニュアルをお読みになる前に	10
「クイックセットアップガイド」の主な内容	10

このマニュアルで使われている用語

このマニュアルでは、一部の表記を除いて以下の用語を使用しています。

用語	意味
本製品	本マニュアルの表紙に記載された製品を称して「本製品」と表記しています。

このマニュアルで使われている記号

記号	意味
重要	作業上および操作上で特に注意していただきたいことを説明しています。この注意事項を守らないと、故障の原因になることがあります。注意してください。
	説明の補足事項や知っておくと便利なことを説明しています。

このマニュアルをお読みになる前に

本製品には、印刷物で「クイックセットアップガイド」が付属しています。
クイックセットアップガイドには、以下の内容が記載されています。

該当する内容がありましたら、そちらをお読みください。

※ マニュアルの改訂により、内容の一部が変更される場合があります。

「クイックセットアップガイド」の主な内容

- 主な工場出荷時の設定値
- 外観図・各部の名称とはたらき
- 設置について
- セットアップ手順

MEMO

印刷物のマニュアルが見当たらない場合には

エレコム・ホームページより、最新のPDF版をダウンロードすることができます。
各製品ページの「マニュアル」ボタンからご確認ください。

● EHB-SX2B08F

<https://www.elecom.co.jp/r/s729>

● EHB-SQ2B08

<https://www.elecom.co.jp/r/n730>

設定リファレンス編

管理画面 (設定画面) を表示する	18
各メニューについて	19
スイッチング	23
ネットワーク	25
セキュリティ	25
管理	29
設定の保存と再起動	31
ダッシュボード	32
ポートステータス	32
システム構成	32
CPU使用率	33
メモリ使用量	33
温度	33
モニター	34
ARP テーブル	34
IP アドレステーブル	35
MAC アドレステーブル	36
ポートステータス	38
ポート詳細画面	39
DDMI 詳細画面	42
システム情報	44
システム情報	44
メモリ使用率	44
システムログ	45
システム	46
一般設定	46

インターフェース設定	48
インターフェース追加／編集	49
IPアドレス設定	50
DNSサーバー	50
IPインターフェース	50
IPアドレス設定	51
IPインターフェース	52
【IPv6】ステータス	53
DNSサーバー	53
IPv6テーブル	53
IPv6 インターフェース詳細	54
【IPv6】グローバル設定	56
【IPv6】インターフェース設定	57
インターフェース編集画面	58
【IPv6】アドレス設定	59
IPv6 リンクローカルアドレスの編集	60
IPv6 DNSサーバー	61
IPv6 グローバルアドレス設定	61
IPv6 グローバルアドレスの追加／編集	62
【IPv6】DHCPv6 クライアント設定	63
DHCPv6 クライアント編集画面	64
ユーザーアカウント	65
SNMP	67
一般設定	67
トラップの宛先	68
SNMP ユーザーの追加／編集	70
スイッチ設定	74

Syslog 設定	75
Syslog 設定	75
Syslog サーバー設定	76
Syslog サーバーの追加／編集	76
【アドミリンク】基本設定	77
【アドミリンク】詳細設定	78
ポート	80
Green Ethernet	80
表	80
リンクアグリゲーション	82
LLDP	88
Basic TLV	88
LLDP Port Information	89
LLDP Local Port Status Detail 画面	89
LLDP リモートポートステータス詳細画面	92
ポート設定	100
スイッチング	103
ループ防止	103
ミラーリング	104
【マルチキャスト】IPv4 マルチキャスト	105
IGMP snooping VLAN	109
VLAN	110
IGMP snooping VLAN の追加／編集	110
【マルチキャスト】IPv6 マルチキャスト	111
MLD snooping プロキシ VLAN の追加／編集	114
【マルチキャスト】静的マルチキャスト転送	118

静的マルチキャストMACアドレスルールの追加／編集	119
【Qos】Diffserv	120
【Qos】キューイング方式	122
【Qos】キュー優先度	124
【Qos】帯域幅制御	125
【スパニングツリー】ステータス	126
RSTP 設定時	126
RSTP 設定時	128
【スパニングツリー】設定	132
スパニングツリーモード	132
【スパニングツリー】RSTP	134
【スパニングツリー】MSTP	137
ブリッジ	137
インスタンス	138
マルチプルスパニングツリーの追加／編集	139
静的MACフィルタリング	141
静的MACフィルタリングの追加／編集	142
静的MAC転送	143
静的MAC転送ルールの追加／編集	144
【VLAN】VLANステータス	145
VLAN 詳細画面	146
【VLAN】VLAN 設定	147
静的VLANの追加／編集	148
【VLAN】Voice VLAN 設定	151
Voice VLAN グローバル設定	151
Voice VLAN OUI 設定	152
Voice VLANの追加／編集	152

VLANアイソレーション	153
VLANアイソレーションルールの追加／編集	154
VLANマッピング	155
VLAN マッピングの追加／編集	157
ネットワーク	158
【ARP 設定】ARP ラーニング	158
【ARP 設定】静的 ARP	159
静的 ARP の追加／編集	160
セキュリティ	161
【AAA】RADIUS サーバー設定	161
認証サーバー	161
アカウントिंगサーバー	162
属性	162
【AAA】AAA 設定	163
サーバーキー暗号化	163
認証	163
権限付与	164
アカウントング	164
【ACL】Classifier	165
Classifier の追加／編集	167
【ACL】Policy Rule	171
ポリシールールの追加／編集	172
アンチ ARP スキャン	175
フィルタリングされたホストをクリア	176
フィルタリングされたホスト	176
信頼ホストの追加／編集	179

BPDUGuard	180
ストームコントロール	182
Dos 攻撃防止	183
Errdisable	185
【IPv4 ソースガード】IPv4 ソースガード	186
ARP フリーズ	187
静的バインディング	188
IPv4 ソースガード静的バインディングの追加／編集	189
【IPv4 ソースガード】DHCP snooping	190
データベースステータス	190
データベース詳細	191
DHCP snooping 設定	193
データベース	193
DHCP snooping VLAN ポートの追加／編集	198
【IPv4 ソースガード】DHCP Option82 プロファイル	199
DHCP Option82 プロファイルの追加／編集	200
【IPv4 ソースガード】ARP インスペクション	201
ARP インスペクション設定	205
フィルタエージングタイム	205
ログプロファイル	205
【IPv6 ソースガード】IPv6 静的バインディング	208
IPv6 静的バインディングの追加／編集	211
【IPv6 ソースガード】IPv6 ソースガード	212
IPv6 ソースガードポリシーの追加／編集	213
【IPv6 ソースガード】IPv6 snooping	215
IPv6 snooping ポリシーの追加／編集	216
IPv6 snooping VLAN の追加／編集	218

【IPv6 ソースガード】DHCPv6 信頼設定	219
Trust setting	219
ポート設定	219
ポート認証	221
ポートセキュリティ	223
MAC フリーズ	223
ポートセキュリティ	223
管理	225
【設定】設定の復元	225
【設定】設定のバックアップ	227
【設定】実行設定の消去	230
【設定】設定の保存	231
診断	232
Ping テスト	232
Trace Route テスト	233
ケーブル診断	233
ファームウェア更新	235
ファームウェア更新	235
起動ファームウェア	235
「更新方法」に「TFTP」を選択した場合	236
「更新方法」に「HTTP」を選択した場合	237
再起動	238

管理画面(設定画面)を表示する

本製品の各種設定をするために、Web ブラウザーから利用できる設定画面があります。各ボタンの詳しい内容や設定方法については、該当ページをお読みください。

1 本製品の設定に使用するパソコンのネットワークを設定します。

IPアドレス: 192.168.3.xxx

xxxは、2～254までの任意の数字にします。

2 本製品に接続しているパソコンのWebブラウザを開き、以下のWebページを表示します。

認証画面が表示された場合は、ユーザー名とパスワードに「admin」を入力し、「ログイン」をクリックします。

<http://192.168.3.1/>



管理画面が表示されます。



●ご利用のWebブラウザー（Google Chromeなど）のバージョンによっては「保護されていない」などの警告が表示される場合がありますが、セキュリティ上問題ありません。そのまま操作を続けてください。

重要

設定を変更した場合は、必ず各ページの「適用」をクリックして設定を保存してください。

「適用」をクリックせずに他の画面に移動すると、設定が変更されません。
また、各種設定を終了する前に必ず設定画面右上の「保存」をクリックして、
設定を保存してください。

各メニューについて

ダッシュボード

本製品のハードウェア情報やIPアドレスなどのシステム情報が表示されます。

→ [32 ページ](#)

モニター

メニュー項目	内容
ARP テーブル	アドレス解決プロトコル (ARP) の設定をします。 → 34 ページ
IP アドレステーブル	本製品のポート間でパケットがどのように転送またはフィルタリングされるかが表示されます。 → 35 ページ
MAC アドレステーブル	本製品のポート間でフレームがどのように転送またはフィルタリングされるか設定します。 → 36 ページ
ポートステータス	<ul style="list-style-type: none">●ポートステータス 個々のポートの統計情報が表示されます。 → 38 ページ●DDMI DDMI (Digital Diagnostics Monitoring Interface) 機能の設定をします。 → 41 ページ●ポート使用率 ポートで実際に送信または受信されたフレームのリンク速度に対するパーセンテージが表示されます。 → 43 ページ
システム情報	システム情報とハードウェアステータスが表示されます。 → 44 ページ
システムログ	システムログが表示されます。 → 45 ページ

システム

メニュー項目	内容
一般設定	システム名や時刻などの一般的な設定をおこないます。 → 46 ページ
インターフェース設定	IPv6 の VLAN インタフェース設定をします。 → 48 ページ
IP アドレス設定	<p>● IP アドレスステータス IP インタフェースおよび DNS サーバ設定が表示されます。 → 50 ページ</p> <p>● IP アドレス設定 IP アドレスの設定をします。 → 51 ページ</p>
IPv6	
ステータス	IPv6 テーブルと DNS サーバー情報が表示されます。 → 53 ページ
グローバル設定	グローバル IPv6 を 設定します。 → 56 ページ
インターフェース設定	IPv6 インタフェースの設定をします。 → 57 ページ
アドレス設定	<p>● IPv6 リンクローカルアドレス設定 IPv6 のリンクローカルアドレスの設定をします。 → 59 ページ</p> <p>● IPv6 グローバルアドレス設定 IPv6 のグローバルアドレスの設定をします。 → 61 ページ</p>
DHCPv6 クライアント設定	本製品が DHCPv6 クライアントとして動作する際の DHCP 設定をします。 → 63 ページ
ユーザーアカウント	管理者のパスワードを変更したり、ユーザーを編集／追加します。 → 65 ページ

メニュー項目	内容
SNMP	<p>● SNMP SNMP の設定をします。 → 67 ページ</p> <p>● SNMP ユーザー SNMP ユーザーを編集／追加します。 → 69 ページ</p> <p>● SNMP トラップグループ 各 SNMP マネージャに送信する SNMP トラップのタイプを指定します。 → 72 ページ</p> <p>● SNMP トラップポート ポートで受信したトラップを SNMP マネージャに送信するかどうかを設定します。 → 73 ページ</p>
スイッチ設定	<p>スイッチに関する設定をします。 → 74 ページ</p>
Syslog 設定	<p>Syslog サーバーに関する設定をします。 → 75 ページ</p>
アドミリンク	
基本設定	<p>アドミリンクの基本設定をします。 → 77 ページ</p>
詳細設定	<p>アドミリンクの詳細設定をします。 → 78 ページ</p>

ポート

メニュー項目	内容
Green Ethernet	省電力設定をします。 → 80 ページ
リンクアグリゲーション	<p>●リンクアグリゲーションステータス トランクグループに設定したポートや、トランクグループ内の 1 つの論理リンクとして現在データを送信しているポートなどが表示されます。 → 82 ページ</p> <p>●リンクアグリゲーション設定 スタティックリンクアグリゲーションの設定をします。 → 84 ページ</p> <p>●リンクアグリゲーション制御プロトコル リンクアグリゲーション制御プロトコル (LACP) の設定をします。 → 86 ページ</p>
LLDP	<p>● LLDP ローカルステータス LLDP ステータスの状態が表示されます。 → 88 ページ</p> <p>● LLDP リモートステータス 隣接するスイッチングハブとの LLDP 接続ごとに LLDP ステータスの状態が表示されます。 → 91 ページ</p> <p>● LLDP 設定 グローバル LLDP の設定をします。 → 96 ページ</p> <p>● Basic TLV Setting TLV の基本設定をします。 → 98 ページ</p> <p>● Org-specific TLV Setting 組織固有の TLV 設定をします。 → 99 ページ</p>
ポート設定	ポートの設定をします。 → 100 ページ

■ スイッチング

メニュー項目	内容
ループ防止	ポートごとにループ防止機能の設定をします。 → 103 ページ
ミラーリング	ポートミラーリング機能の設定をします。 → 104 ページ
マルチキャスト	
IPv4 マルチキャスト	<ul style="list-style-type: none"> ● IPv4 マルチキャスト ステータス IPv4 マルチキャストグループ情報が表示されます。 → 105 ページ ● IGMP snooping IGMP snooping の設定をします。 → 106 ページ ● IGMP snooping VLAN VLAN で IGMP snooping を実行します。 → 109 ページ
IPv6 マルチキャスト	<ul style="list-style-type: none"> ● IPv6 マルチキャスト ステータス IPv6 マルチキャストグループ情報が表示されます。 → 111 ページ ● MLD snooping プロキシ MLD snooping プロキシの設定をします。 → 112 ページ ● VLAN MLD snooping プロキシ VLAN の設定をします。 → 113 ページ ● ポートロール設定 ポートの MLD snooping プロキシの設定をします。 → 116 ページ
静的マルチキャスト転送	マルチキャストストリームを受信するポートの静的マルチキャスト MAC アドレスを表示および設定します。 → 118 ページ

QoS	
Diffserv	<p>● Diffserv マーキングルールまたは IEEE802.1p プライオリティマッピングを適用します。 → 120 ページ</p> <p>● DSCP 設定 DiffServ to IEEE 802.1p マッピングテーブルに従って、本製品が受信 DSCP 値に基づいてすべてのトラフィックを優先順位付けできるように、DSCP to IEEE 802.1p マッピングを設定できます。 → 121 ページ</p>
キューイング方式	キューの優先度の設定をします。 → 122 ページ
キュー優先度	優先度レベルから物理キューへのマッピングの設定をします。 → 124 ページ
帯域幅制御	最大帯域幅の設定をします。 → 125 ページ
スパニングツリー	
ステータス	RSTP または MSTP の STP ステータスが表示されます。 → 126 ページ
設定	スパニングツリーモードの設定をします。 → 132 ページ
RSTP	RSTP (ラピッドスパニングツリープロトコル) の設定をします。 → 134 ページ
MSTP	<p>● MSTP MSTP (マルチプルラピッドスパニングツリープロトコル) の設定をします。 → 137 ページ</p> <p>● MSTP ポート設定 MSTP ポートの設定をします。 → 140 ページ</p>
静的 MAC フィルタリング	静的 MAC アドレスフィルタの設定をします。 → 141 ページ
静的 MAC 転送	静的な MAC アドレス転送ルールを設定をします。 → 143 ページ
VLAN	
VLAN ステータス	静的 VLAN グループを表示および検索します。 → 145 ページ

VLAN 設定	<p>●静的 VLAN 静的 VLAN の設定をします。 → 147 ページ</p> <p>●VLAN ポート設定 ポートの静的 VLAN (IEEE 802.1Q) 設定をします。 → 149 ページ</p>
Voice VLAN 設定	<p>Voice VLAN の設定をします。 → 151 ページ</p>
VLAN アイソレーション	<p>VLAN 内のポート間で通信を行わないように設定します。 → 153 ページ</p>
VLAN マッピング	<p>● VLAN マッピング VLAN マッピングの有効／無効の設定をします。 → 155 ページ</p> <p>● VLAN マッピング設定 VLAN マッピングルールを表示および設定します。 → 156 ページ</p>

■ ネットワーク

メニュー項目	内容
ARP 設定	<p>● ARP ラーニング 各ポートの ARP 学習モードを設定します。 → 158 ページ</p> <p>●静的 ARP エージアウトしない静的 ARP エントリを表示および構成します。 → 159 ページ</p>

■ セキュリティ

メニュー項目	内容
AAA	
RADIUS サーバー設定	<p>RADIUS サーバーの設定をします。 → 161 ページ</p>
AAA 設定	<p>認証、権限、アカウントिंगの設定をします。 → 163 ページ</p>

ACL	
Classifier	<p>● Classifier ステータス 作成済みの Classifier の状態を確認します。 → 165 ページ</p> <p>● Classifier 設定 Classifier の設定をします。 → 166 ページ</p> <p>● Classifier グローバル設定 Classifier のグローバル設定をします。 → 170 ページ</p>
アンチ ARP スキャン	<p>● ステータス どのポートが信頼され、トラフィックを転送しているか、または無効になっているかを確認します。 → 175 ページ</p> <p>● ホストステータス ブロックされたホストを表示し、特定のポートに接続されているホストのブロックを解除します。 → 176 ページ</p> <p>● 設定 アンチ Arp スキャンを有効にしたり、ポートとホストのしきい値を設定し、信頼または信頼しないポートを設定します。 → 177 ページ</p> <p>● 信頼ホスト IP アドレスとサブネットマスクで識別される信頼できるホストを作成または削除します。 → 178 ページ</p>
BPDU ガード	<p>● ステータス BPDU ガードが有効になっているかどうか、およびポートのステータスが表示されます。 → 180 ページ</p> <p>● 設定 BPDU ガード機能の有効／無効を設定します。 → 181 ページ</p>
ストームコントロール	<p>ポートで 1 秒間に受信するブロードキャスト、マルチキャストおよび DLF (Destination LookupFailure) パケット数を制限します。 → 182 ページ</p>
Dos 攻撃防止	<p>Dos 攻撃防止の設定をします。 → 183 ページ</p>
Errdisable	<p>エラー復旧の設定をします。 → 185 ページ</p>

IPv4 ソースガード	
IP ソースガード	<p>● IP ソースガード DHCP snooping と ARP インспекションの現在のバインディングが表示されます。 → 186 ページ</p> <p>● 静的バインディング DHCP snooping と ARP インспекションの静的バインディングを管理します。 → 187 ページ</p>
DHCP snooping	<p>● ステータス DHCP snooping データベースに関するさまざまな統計情報が表示されます。 → 190 ページ</p> <p>● 設定 DHCP snooping を有効化し、デフォルトの DHCP サーバがある VLAN を指定し、DHCP snooping データベースの設定をします。 → 193 ページ</p> <p>● ポート設定 ポートを DHCP snooping の信頼済みポートにするか、非信頼ポートにするかを指定します。 → 195 ページ</p> <p>● VLAN 設定 各 VLAN で DHCP snooping を有効にし、本製品が各 VLAN の DHCP サーバに中継する DHCP 要求に DHCP リレーエージェントオプション 82 情報を追加するかどうかを指定します。 → 196 ページ</p> <p>● VLAN ポート設定 特定のポートに異なる DHCP オプション 82 プロファイルを適用します。 → 197 ページ</p>
DHCP Option82 プロファイル	→ 199 ページ

ARP インспекション	<p>●ステータス 不正な ARP パケットを識別したために作成された MAC アドレスフィルタの現在のリストが表示されます。 → 201 ページ</p> <p>●VLAN ステータス 各 VLAN の ARP パケットに関するさまざまな統計情報が表示されます。 → 202 ページ</p> <p>●ログステータス ARP パケットによって生成され、まだ syslog サーバーに送信されていないログメッセージが表示されます。 → 203 ページ</p> <p>●設定 ARP インспекション機能の有効／無効を設定します。 また、廃棄した ARP パケットの記録を保存する期間や ARP 検査ログのグローバル設定を行うことができます。 → 204 ページ</p> <p>●ポート設定 ポートを ARP インспекションの信頼されたポートにするか、信頼されていないポートにするかを指定します。 また、各信頼対象外ポートで本製品が ARP パケットを受信する最大レート指定できます。 → 206 ページ</p> <p>●VLAN 設定 各 VLAN で ARP 検査を有効にし、各 VLAN からの ARP パケット受信時にログメッセージを生成するタイミングを指定します。 → 206 ページ</p>
IPv6 ソースガード	
IPv6 静的バインディング	<p>● IPv6 送信元バインディング状態 現在の IPv6 動的バインディングと静的バインディングを確認し、IPv6 アドレスや IPv6 プレフィックスに基づいて動的バインディングを削除します。 → 208 ページ</p> <p>● IPv6 静的バインディング IPv6 ソースガードバインディングテーブルエントリを表示または構成し、IPv6 静的バインディングを管理します。 → 210 ページ</p>

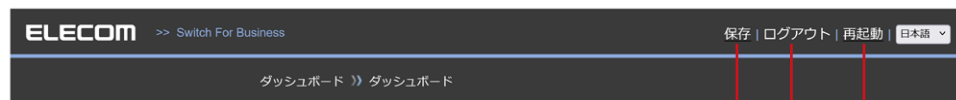
IPv6 ソースガード	<p>●ポリシー</p> <p>IPv6 ソースガードにバインディングテーブルに保存されている有効な IPv6 アドレスや IPv6 プレフィックスを転送させ、すべてのリンクローカルアドレスからのデータトラフィックを許可またはブロックします。</p> <p>→ 212 ページ</p> <p>●ポート設定</p> <p>設定した IPv6 ソースガード ポリシーを指定したポートに適用します。</p> <p>→ 214 ページ</p>
IPv6 snooping	<p>●ポリシー設定</p> <p>DHCPv6 snooping を有効に設定します。</p> <p>→ 215 ページ</p> <p>●VLAN 設定</p> <p>特定の VLAN インタフェースで DHCPv6 snooping ポリシーを有効にします。</p> <p>→ 217 ページ</p>
DHCPv6 信頼設定	<p>DHCPv6 snooping で信頼するポートを指定します。</p> <p>→ 219 ページ</p>
ポート認証	<p>ポートごとに 802.1X 認証 (RADIUS 連携) の動作の設定をします。</p> <p>→ 221 ページ</p>
ポートセキュリティ	<p>ポートセキュリティの設定をします。</p> <p>→ 223 ページ</p>

■ 管理

メニュー項目	内容
設定	
設定の復元	<p>本製品の設定をバックアップしたファイルから復元します。</p> <p>→ 225 ページ</p>
設定のバックアップ	<p>本製品の設定をファイルにバックアップします。</p> <p>→ 227 ページ</p>
実行設定の消去	<p>実行設定 (ユーザ名、パスワード、システムログ、メモリログ、ボーレート、SSH サービス) を削除します。</p> <p>→ 230 ページ</p>
設定の保存	<p>現在の設定内容を本製品に保存します。</p> <p>→ 231 ページ</p>
診断	<p>IP アドレスの ping、tracerout、ポートテストの実行をします。</p> <p>→ 232 ページ</p>

ファームウェア更新	本製品のファームウェアを更新します。 → 235 ページ
再起動	本製品を再起動します。 → 238 ページ

設定の保存と再起動



保存

設定を変更した場合、「保存」ボタンを押して設定を保存します。

ログアウト

管理画面からログアウトします。

再起動

本製品を再起動します。設定を変更した場合は「保存」ボタンを押してから再起動してください。

重要

設定を変更した場合は、必ず各ページの「適用」をクリックして設定を保存してください。

「適用」をクリックせずに他の画面に移動すると、設定が変更されません。

また、各種設定を終了する前に必ず設定画面右上の「保存」をクリックして、設定を保存してください。

「保存」をクリックせずに本製品を再起動すると、設定した内容が最後に「保存」したときの状態に戻ります。

ダッシュボード

本製品のハードウェア情報や IP アドレスなどのシステム情報が表示されます。



■ ポートステータス

LANポートの使用状況が表示されます。使用中のポートは緑で点灯します。ポートをクリックすると、ポートのステータスパネルが開き、ポートの有効／無効の切り替えや、PoEポートのパワーサイクルなどの基本情報が表示されます。

■ システム構成

項目	内容
システム名	本製品に設定されている名称が表示されます。
システムロケーション	本製品に設定されている場所の名称が表示されます。
ブートバージョン	本製品に搭載されているブートモジュールのバージョン番号が表示されます。
ファームウェアバージョン	本製品のファームウェアのバージョンが表示されます。
システム時間	現在の日付と時刻が表示されます。 フォーマットは mm/dd/yyyy hh:mm:ss です。
システム稼働時間	本製品の最終再起動または電源投入からの稼働時間が表示されます。
シリアル番号	本製品のシリアル番号が表示されます。 シリアル番号はデバイスの追跡と制御に使用されます。
ハードウェアバージョン	本製品のハードウェアバージョンが表示されます。
システム MAC アドレス	本製品の MAC アドレスが表示されます。

項目	内容
システム IP アドレス	本製品の IP アドレスが表示されます。
アドミリンク登録状態	アドミリンクの登録状態が表示されます。

■ CPU 使用率

現在の CPU 使用率が表示されます。

■ メモリ使用量

現在のメモリ使用量が表示されます。

■ 温度

本製品の温度レベルが表示されます。

本製品には温度センサがあり、温度が閾値以上に上昇した場合に検知してお知らせします。

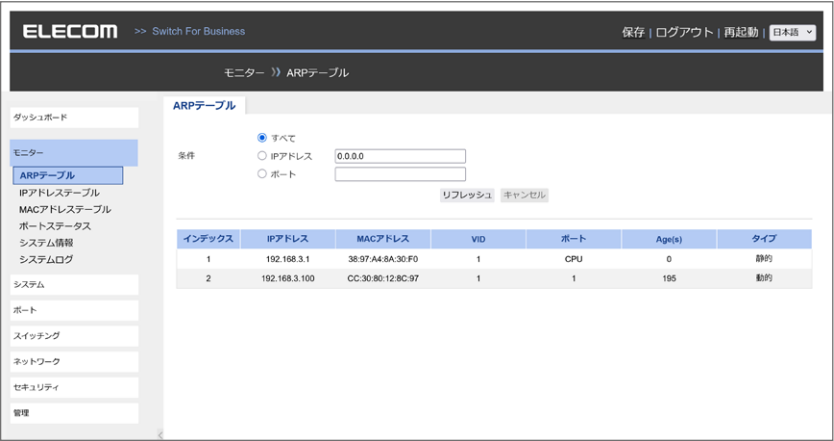
ARP テーブル

IP アドレスとMAC アドレスのマッピングが表示されます。

MEMO

アドレス解決プロトコル（ARP）とは、IP アドレスを、LAN 上の物理的な MAC アドレスにマッピングするためのプロトコルです。

ARP テーブルは、各 MAC アドレスと対応する IP アドレスの関連付けを維持します。



項目	内容
条件	条件を指定して「リフレッシュ」をクリックすると、指定した条件のARP エントリを削除します。
	<div><div>すべて</div><div>すべてのエントリを削除します。</div></div>
	<div><div>IP アドレス</div><div>指定した IP アドレスのエントリを削除します。</div></div>
	<div><div>ポート</div><div>指定したポートのエントリを削除します。 複数のポートを（スペースなし）カンマ（,）またはハイフン（-）で区切って範囲を入力できます。 たとえば、ポート「3、4、5」を指定するときは「3-5」と入力します。 ポート「3、5、7」を指定するときは、「3,5,7」と入力します。</div></div>

IPアドレステーブル

本製品のポート間でパケットがどのように転送またはフィルタリングされるかが表示されます。本製品のポートに転送されるパケットをデバイス（VLANグループに属する場合もあります）が送信すると、デバイスのIPアドレスが本製品のIPアドレステーブル画面に表示されます。また、この画面にはIPアドレスが動的か静的かも表示されます。

The screenshot shows the ELECOM web management interface. At the top, there is a header with the ELECOM logo, a link to 'Switch For Business', and user options: '保存' (Save), 'ログアウト' (Logout), '再起動' (Restart), and a language dropdown set to '日本語'. Below the header, the breadcrumb 'モニター > IPアドレステーブル' is visible. On the left is a sidebar menu with options: 'ダッシュボード', 'モニター' (selected), 'ARPテーブル', 'IPアドレステーブル' (highlighted), 'MACアドレステーブル', 'ポートステータス', 'システム情報', 'システムログ', 'システム', 'ポート', 'スイッチング', 'ネットワーク', 'セキュリティ', and '管理'. The main content area is titled 'IPアドレステーブル' and contains a table with the following data:

インデックス	IPアドレス	VID	ポート	タイプ
1	192.168.3.1	1	CPU	静的
2	192.168.3.100	1	1	動的

MACアドレステーブル

本製品のポート間でフレームがどのように転送またはフィルタリングされるかが表示されます。どのデバイスのMACアドレスがどのポートに転送され、どのVLANグループに属しているか、MACアドレスが動的か静的かが表示されます。

特定のMACアドレスを検索するには、MACテーブル画面を使用します。

また、この画面を使用して、MACテーブルから静的MAC転送テーブル、またはMACフィルタリングテーブルに動的MACアドレスを直接追加することもできます。

インデックス	MACアドレス	VID	ポート	タイプ
1	38:97:A4:8A:30:F9	1	CPU	静的
2	CC:30:80:12:9C:97	1	1	動的

項目	内容	
条件	条件を指定して「検索」をクリックすると、指定した条件に一致する MAC アドレスのみが表示されます。	
	すべて	すべてのエントリが表示されます。
	静的	手動で設定された MAC アドレスのみが表示されます。
	MAC アドレス	指定した MAC アドレスのみが表示されます。
	VID	指定した VLAN に属する MAC アドレスのみが表示されます。
	ポート	指定したポートに転送される MAC アドレスのみが表示されます。
	トランク	トランクグループの ID を入力すると、トランクグループ内のポートから学習されたすべての MAC アドレスが表示されます。
ソート	指定した順番で表示を並び替えます。	

項目	内容	
転送タイプ	Dynamic to MAC forwarding	選択して「適用」をクリックすると、サマリーテーブルの動的に学習された MAC アドレスエントリがすべて静的エントリに変更されます。
	Dynamic to MAC filtering	選択して「適用」をクリックすると、サマリーテーブルにあるすべての動的に学習された MAC アドレスエントリが MAC フィルタリングエントリに変更されます。

ポートステータス

ポートステータス

本製品のポートステータスが表示されます。

ELECOM >> Switch For Business 保存 ログアウト 再起動 日本語										
モニター >> ポートステータス										
ポートステータス DDM ポート使用率										
ポート	ポート名	リンク	状態	LACP	送信パケット数	受信パケット数	エラー	Tx kB/s	Rx kB/s	稼働時間
1		10G-F	転送	無効	2061	1422	0	0.205	0.751	0:09:56
2		DOWN	停止	無効	0	0	0	0.0	0.0	0:00:00
3		DOWN	停止	無効	0	0	0	0.0	0.0	0:00:00
4		DOWN	停止	無効	0	0	0	0.0	0.0	0:00:00
5		DOWN	停止	無効	0	0	0	0.0	0.0	0:00:00
6		DOWN	停止	無効	0	0	0	0.0	0.0	0:00:00
7		DOWN	停止	無効	0	0	0	0.0	0.0	0:00:00
8		DOWN	停止	無効	0	0	0	0.0	0.0	0:00:00
9		DOWN	停止	無効	0	0	0	0.0	0.0	0:00:00
10		DOWN	停止	無効	0	0	0	0.0	0.0	0:00:00

項目	内容
ポート	ポート番号をクリックすると、ポート詳細画面が表示されます。(→ 39 ページ)
ポート名	このポートに割り当てられた名称が表示されます。
リンク	速度が表示されます。 10Mbps は 10M、100Mbps は 100M、1Gbps は 1G、2.5Gbps は 2.5G、5Gbps は 5G、10Gbps は 10G と表示されます。 また、全二重は「F」、半二重は「H」と表示されます。 ポートがどのデバイスにも接続されていない場合は、「Down」と表示されます。 ※ 10Gbps/5Gbps は、EHB-SX シリーズのみ対応。
状態	STP(Spanning Tree Protocol)が有効な場合、ポートの STP 状態が表示されます。 STP が無効の場合、リンクがアップしていれば「転送」と表示され、そうでなければ「停止」と表示されます。 LACP(Link Aggregation Control Protocol)と STP がブロッキング状態の場合は、「ブロッキング」と表示されます。
LACP	LACP (リンクアグリゲーションコントロールプロトコル) がポートで有効になっているかどうかが表示されます。
送信パケット数	このポートの送信パケット数が表示されます。
受信パケット数	このポートの受信パケット数が表示されます。
エラー	このポートの受信エラー数が表示されます。
Tx kB/s	このポートで送信された 1 秒あたりのキロバイト数が表示されます。

項目	内容
Rx kB/s	このポートで受信された毎秒のキロバイト数が表示されます。
稼働時間	ポートが稼働している合計時間（時、分、秒）が表示されます。

■ ポート詳細画面

各ポートのステータスと詳細なパフォーマンスデータが表示されます。

ポートステータス > ポート詳細

ポート情報		TX Packet	
ポート番号	1	Unicast	6006
ポート名		Multicast	426
リンク	1G/F	Broadcast	615
状態	FORWARDING	Pause	0
LACP	無効	RX Packet	
送信/ケット数	7047	Unicast	3808
受信/ケット数	3979	Multicast	145
エラー	0	Broadcast	26
送信 kB/s	0.654	Pause	0
送信使用率 %	0.0	TX Collision	
受信 kB/s	1.659	Single	0
受信使用率 %	0.0	Multiple	0
稼働時間	2:40:11	Excessive	0
		Late	0
		Error Packet	
		RX CRC	0
		Length	0
		Runt	0

Distribution	
64	4059
65 - 127	275
128 - 255	290
256 - 511	1597
512 - 1023	465
1024 - 1518	4340
Giant	0

項目	内容	
ポート情報	ポートの詳細情報が表示されます。	
Distribution	受信したパケット（不良パケットを含む）の数が表示されます。	
	64	長さが 64 オクテットのパケット数
	65-127	長さが 65 ～ 127 オクテットのパケット数
	128-255	長さが 128 ～ 255 オクテットのパケット数
	256-511	長さが 256 ～ 511 オクテットのパケット数
	512-1023	長さが 512 ～ 1023 オクテットのパケット数
	1024-1518	長さが 1024 ～ 1518 オクテットのパケット数
	Giant	1519 から最大フレームサイズまでのパケット数

項目	内容	
TX Packet	Unicast	良好なユニキャストパケットの送信数が表示されます。
	Multicast	良好なマルチキャストパケットの送信数が表示されます。
	Broadcast	良好なブロードキャストパケットの送信数が表示されます。
	Pause	送信された 802.3x ポーズパケット数が表示されます。
RX Packet	Unicast	良好なユニキャストパケットの受信数が表示されます。
	Multicast	良好なマルチキャストパケットの受信数が表示されます。
	Broadcast	良好なブロードキャストパケットの受信数が表示されます。
	Pause	受信された 802.3x ポーズパケット数が表示されます。
Tx Collision	Single	1 つの衝突によって送信が阻害された、正常に送信されたパケットの数が表示されます。
	Multiple	複数の衝突によって送信が阻害された、正常に送信されたパケットの数が表示されます。
	Excessive	再送上限に達して送信失敗したパケットの数が表示されます。
	Late	フレーム先頭 512 bit を超えてから検出された衝突の回数が表示されます。
Error Packet	RX CRC	CRC (Cyclic Redundant Check) エラーで受信したパケット数が表示されます。
	Length	範囲外の長さで受信したパケット数が表示されます。
	Runt	CRC エラーを含む、短すぎる (64 オクテットより短い) パケットを受信した数が表示されます。

DDMI

本製品のSFPトランシーバの DDMI ステータスが表示されます。

MEMO

DDMI (Digital Diagnostics Monitoring Interface)機能をサポートする光SFPトランシーバーでは、トランシーバーのパラメーターを監視して、コンポーネントの監視、障害切り分け、障害予測タスクを実行できます。これにより、予防的なネットワーク・メンテナンスが可能になり、サービスの継続性が確保されます。

ポート	Vendor	Part Number	シリアル番号	リビジョン	Date Code	Transceiver	アクション
32	Elecom	EHB-EX-SFPGLX	51L49720042		2015-01-09	1000BASE-LX	Reset

項目	内容
ポート	SFP トランシーバーを使用しているポート番号が表示されます。 ポート番号をクリックすると、DDMI 詳細画面 (42 ページ) が表示されます。
Vender	光トランシーバーのベンダー名が表示されます。
Part Number	光トランシーバーの部品番号が表示されます。
シリアル番号	光トランシーバーのシリアル番号が表示されます。
リビジョン	光トランシーバーのリビジョン番号が表示されます。
Date Code	光トランシーバーが製造された日付が表示されます。
Transceiver	SFP スロットに取り付けられているトランシーバーのタイプが表示されます。

項目	内容
アクション	<p>SFP ポートで接続エラー（受信はできるがデータを送信できない場合など）が発生した場合は、「Reset」をクリックします。</p> <p>これにより、エラー状態にあるファイバー SFP トランシーバを抜き差しすることなく再起動できます。</p> <p>SFP ポート再起動後、「モニター」→「ポートステータス」→「ポートステータス」で SFP ポートの状態を確認してください。</p> <p>また、本製品のポート LED を確認し、接続が回復したかどうかを確認することもできます。</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>注意 光トランシーバが SFP ポートに正しく挿入されていることを確認してください。</p> </div>

■ DDMI 詳細画面

SFP (Small Form Factor Pluggable) トランシーバー情報と SFP ポートの動作パラメータがリアルタイムで表示されます。

パラメータには、送受信電力やモジュール温度などが含まれます。

現在のトランシーバーのステータスを表示するには、DDMI 画面のポート列のインデックスをクリックします。

The screenshot shows the ELECOM web interface for monitoring port status. The main content area is titled 'Port Status' and 'DDMI Port Utilization'. It displays 'Transceiver Information' and 'DDMI Information'.

Transceiver Information

Port No	10
Connector Type	SFP
Vendor	ELECOM
Part Number	E108-LX-SFPGLX
Serial Number	S1L49720042
Revision	2015.01.09
Opt. Code	
Transceiver	1000BASE-LX

DDMI Information

Type	Current	High Alarm Threshold	High Warn Threshold	Low Warn Threshold	Low Alarm Threshold
Temperature(C)	-	-	-	-	-
Voltage(V)	-	-	-	-	-
TX Bias(mA)	-	-	-	-	-
TX Power(dBm)	-	-	-	-	-
RX Power(dBm)	-	-	-	-	-

ポート使用率

ポートで実際に送信または受信されたフレームのリンク速度に対するパーセンテージが表示されます。

ELECOM

>> Switch For Business

保存 | ログアウト | 再起動

日本語

モニター >> ポートステータス

ダッシュボード

モニター

ARPテーブル

IPアドレステーブル

MACアドレステーブル

ポートステータス

システム情報

システムログ

システム

ポート

スイッチング

ポートステータス

DDMI

ポート使用率

ポート	リンク	送信 kB/s	送信使用率 %	受信 kB/s	受信使用率 %
1	1G/F	28.294	0.0	1.149	0.0
2	DOWN	0.0	0.0	0.0	0.0
3	DOWN	0.0	0.0	0.0	0.0
4	DOWN	0.0	0.0	0.0	0.0
5	DOWN	0.0	0.0	0.0	0.0
6	DOWN	0.0	0.0	0.0	0.0
7	DOWN	0.0	0.0	0.0	0.0
8	DOWN	0.0	0.0	0.0	0.0
9	DOWN	0.0	0.0	0.0	0.0
10	DOWN	0.0	0.0	0.0	0.0

項目	内容
ポート	SFP ポートを識別します。
リンク	速度 (10Mbps は 10M、100Mbps は 100M、1Gbps は 1G、2.5Gbps は 2.5G、5Gbps は 5G、10Gbps は 10G) とデュプレックス (全二重は F、半二重は H) です。ポートがどのデバイスにも接続されていない場合は、「DOWN」と表示されます。 ※ 10Gbps/5Gbps は、EHB-SX シリーズのみ対応。
送信 KB/s	このポートで送信されるデータの伝送速度 (キロバイト/秒) が表示されます。
送信使用率 %	このポートで実際に送信されたフレームの Link 速度に対する割合が表示されます。
受信 KB/s	このポートで受信したデータの伝送速度 (キロバイト/秒) が表示されます。
受信使用率 %	このポートで実際に受信したフレームのリンク速度に対する割合が表示されます。

システム情報

本製品の一般的なシステム情報とハードウェアステータスが表示されます。

The screenshot shows the ELECOM system information page. The left sidebar contains navigation links: ダッシュボード, モニター (selected), ARPテーブル, IPアドレステーブル, MACアドレステーブル, ポートステータス, システム情報 (selected), システムログ, システム, ポート, スイッチング, ネットワーク. The main content area is titled 'システム情報' and displays the following information:

- システム名: E1B-SX2B08F
- 型番: E1B-SX2B08F
- ファームウェアバージョン: 1.0.0
- MACアドレス: 38:97:A4:8A:30:F0
- CPU使用率 (%): 2.98

Below this, there is a 'メモリ使用率 (%)' table:

名前	合計 (byte)	使用済み (byte)	使用率 (%)
一般	83207424	3728976	4

■ システム情報

項目	内容
システム名	本製品を識別するための記述名が表示されます。
型番	本製品の製品モデルが表示されます。ファームウェアのアップグレードを検索する際や、Web サイトでその他のサポート情報を検索する際に使用します。
ファームウェアバージョン	本製品の現在のファームウェアのバージョン番号が表示されます。
MAC アドレス	本製品の MAC アドレスが表示されます。
CPU 使用率 (%)	現在の CPU 使用率が表示されます。

■ メモリ使用率

使用可能なDRAMメモリの量と使用中のメモリが表示されます。
また、現在のメモリ使用率も表示されます。

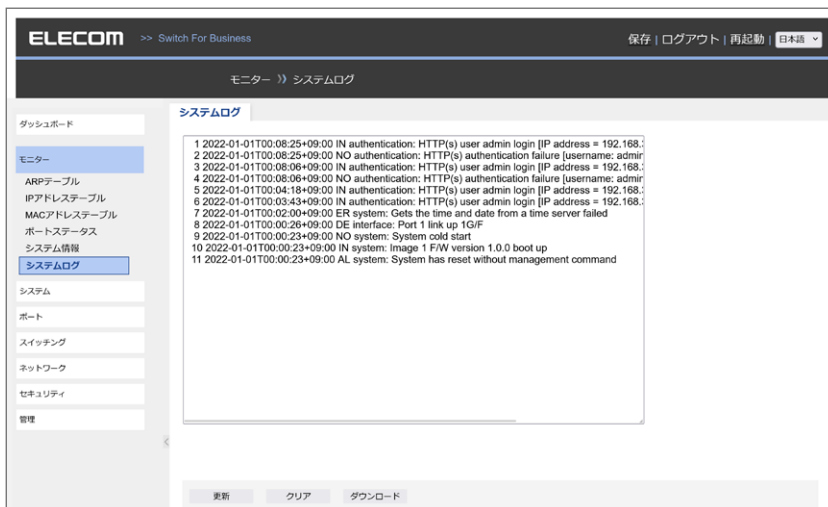
項目	内容
名前	メモリプールの名前が表示されます。
合計 (byte)	メモリプールの合計バイト数が表示されます。
使用済み (byte)	このメモリプールで使用されているバイト数が表示されます。
使用率 (%)	このメモリプールで使用されているメモリの割合 (%) が表示されます。

システムログ

ログメッセージが記録された時間とログメッセージが生成された理由が表示されます。
ログメッセージはテキストデータとして保存することができます。

注意

ログがログ・メッセージの最大数に達すると、新しいログ・メッセージが既存のログ・メッセージを自動的に上書きし、既存のログ・メッセージのうちもっとも古いものから順に上書きされます。



項目	内容
更新	表示内容を最新のものに更新します。
クリア	ログ全体をクリアします。
ダウンロード	ログをテキストデータとしてパソコンに保存します。

一般設定

システム名や時刻などの一般的な設定をおこないます。

ELECOM
>> Switch For Business

保存 | ログアウト | 再起動 | 日本語

システム >> 一般設定

ダッシュボード
モニター
システム
一般設定
インターフェース設定
IPアドレス設定
IPv6
ユーザーアカウント
SNMP
スイッチ設定
Syslog設定
アドミリンク
ポート
スイッチング
ネットワーク
セキュリティ
管理

一般設定

システム名
EHB-SX2B08F
ロケーション
default
担当者名

時刻同期フォーマット
NTP(RFC-1305)
タイムサーバー1
0.pool.ntp.org
タイムサーバー2
1.pool.ntp.org
タイムサーバー3
time.google.com
時刻同期間隔
1440 分
現在時刻
01 : 30 : 41 UTC+09:00
新しい時刻 (hh:mm:ss)
01 : 30 : 41
日付
2022 - 01 - 01
新しい日付 (yyyy-mm-dd)
2022 - 01 - 01
タイムゾーン
UTC+09:00
サマータイム
OFF
開始日
第1 日曜日 1月 0:00
終了日
第1 日曜日 1月 0:00

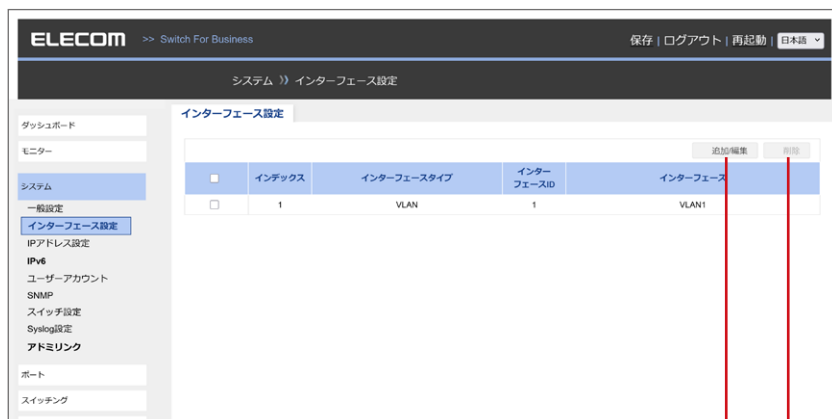
適用 キャンセル

項目	内容
システム名	本製品に設定する名前を入力します。 (最大 64 文字まで。? (クエスチョンマーク) (パイプ) ' (クォーテーション) " (ダブルクォーテーション) , (コンマ) は使用不可)
ロケーション	本製品の設置場所を入力します。 (最大 128 文字まで。? (クエスチョンマーク) (パイプ) ' (クォーテーション) " (ダブルクォーテーション) は使用不可。初期値: default)
担当者	本製品の担当者名を入力してください。スペースは使用可能です。 (最大 32 文字まで。? (クエスチョンマーク) (パイプ) ' (クォーテーション) " (ダブルクォーテーション) , (コンマ) は使用不可)

項目	内容	
時刻同期フォーマット	タイムサーバが使用するタイムサービスプロトコルを選択します。 (初期値：NTP(RFC-1305))	
	Daytime(RFC-867)	タイムゾーン調整なしで日、月、年、時刻を表示します。 このフォーマットを使用する場合は、地理的なタイムゾーン内で Daytime タイムサーバを使用することを推奨します。
	Time(RFC-868)	1970/1/1 の 0:0:0 からの合計秒数を 4 バイトの整数で表示します。
	NTP(RFC-1305)	Time(RFC-868) に似ています。
タイムサーバ 1	タイムサーバの IPv4/IPv6 アドレスまたはドメイン名を入力します。 本製品は 3 つのタイムサーバを、1、2、3 の順番でそれぞれ約 60 秒間検索します。	
タイムサーバ 2		
タイムサーバ 3		
時刻同期間隔	タイムサーバの同期間隔を分単位で入力します。 本製品は同期間隔ごとにタイムサーバを確認します。 (初期値：1440 分)	
現在時刻	この画面を開いた（または画面を更新した）時刻が表示されます。	
新しい時刻 (hh:mm:ss)	新しい時刻を時、分、秒の形式で入力し、「適用」をクリックすると、新しい時刻が「現在時刻」に設定されます。	
日付	この画面を開いた日付が表示されます。	
新しい日付 (yyyy-mm-dd)	新しい時刻を年、月、日の形式で入力し、「適用」をクリックすると、新しい日時日付が設定されます。	
タイムゾーン	タイムゾーンを選択します。 (初期値：UTC+9（日本）)	
サマータイム	サマータイムの有効／無効を切り替えます。 (初期値：無効)	
開始日	サマータイムを有効にした場合の開始日を設定します。	
終了日	サマータイムを有効にした場合の終了日を設定します。	

インターフェース設定

IPv6 の VLAN インタフェースを設定します。



インターフェースを追加したり、選択した
インターフェースを編集します。

→ [49ページ](#)

選択したインターフェースを削除します。

項目	内容
インデックス	エントリのインデックス番号が表示されます。
インターフェースタイプ	インターフェースのタイプが表示されます。
インターフェース ID	インターフェースの識別番号が表示されます。
インターフェース	自動的に生成するインタフェースの記述名が表示されます。 インタフェース種別と ID 番号を組み合わせた名前です。

■ インターフェース追加／編集

インターフェースタイプ

VLAN ▾

インターフェースID

適用

クリア

キャンセル

項目	内容
インターフェースタイプ	設定する IPv6 インタフェースのタイプを選択します。 本製品は IPv6 の VLAN インタフェースタイプをサポートしています。
インターフェース ID	インタフェースに固有の識別番号（1 ～ 4094）を指定します。 IPv6 を正しく機能させるためには、同じ ID 番号のスタティック VLAN を設定する必要があります。 → 「スイッチング」 — 「VLAN 設定」 — 「静的 VLAN」 (217 ページ)
適用	変更内容を本製品のランタイムメモリに保存します。 本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。
クリア	フィールドが工場出荷時のデフォルトにクリアされます。

IP アドレス設定

IP アドレスステータス

本製品の現在のIP インタフェースおよびDNS サーバを設定します。

■ DNS サーバー

項目	内容
DNS サーバー	DNS サーバーの IP アドレスが表示されます。
ソース	DNS サーバーのアドレスが手動で設定されたもの（静的）か、DHCPv4 を使って自動的に取得されたものかが表示されます。

■ IP インターフェース

項目	内容
インデックス	インターフェースのインデックス番号が表示されます。 クリックすると、インターフェースの詳細が表示されます。
IP アドレス	IP ドメイン内の本製品の IP アドレスが表示されます。
サブネットマスク	IP ドメイン内の本製品のサブネットマスクが表示されます。
VID	IP ドメイン内の本製品の VLAN 識別番号が表示されます。

項目	内容	
タイプ	この IP アドレスが DHCP サーバから動的に割り当てられているか (DHCP)、手で割り当てられているか (静的) が表示されます。	
アクション	更新	動的 IP アドレスを更新します。
	リリース	動的 IP アドレスを解放します。

IP アドレス設定

デフォルトゲートウェイ、DNS サーバーの設定や IP ドメインの追加／編集をします。

The screenshot displays the ELECOM web management interface. The top navigation bar includes the ELECOM logo and a language dropdown set to '日本語'. The main header indicates the current path is 'システム >> IPアドレス設定'. On the left, a sidebar menu lists various system settings, with 'IPアドレス設定' currently selected. The main content area is divided into three sections: 'IPアドレスステータス', 'IPアドレス設定', and 'IPインターフェース'. The 'IPアドレス設定' section contains input fields for the default gateway (0.0.0.0), DNS server 1, and DNS server 2, along with '適用' (Apply) and 'キャンセル' (Cancel) buttons. The 'IPインターフェース' section features a table with columns for index, IP address, subnet mask, VLAN ID, and type. Two interfaces are listed: the first is the default gateway (0.0.0.0) configured as DHCP, and the second is a static interface (192.168.3.1) configured as '静的' (Static).

■ IPアドレス設定

項目	内容
デフォルトゲートウェイ	デフォルトの送信ゲートウェイの IP アドレスを、192.168.1.254 のようにドット付き 10 進表記で入力します。
DNS サーバー 1	IP アドレスの代わりにドメイン名を使用できるように、ドメインネームサーバーの IPv4 アドレスを入力します。
DNS サーバー 2	
適用	変更内容を本製品のランタイムメモリに保存します。 本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。

■ IPインターフェース

項目	内容
インデックス	インターフェースのインデックス番号が表示されます。 クリックすると、インターフェースの詳細が表示されます。
IP アドレス	IP ドメイン内の本製品の IP アドレスが表示されます。
IP サブネットマスク	IP ドメイン内の本製品のサブネットマスクが表示されます。
VID	IP ドメイン内の本製品の VLAN 識別番号が表示されます。
タイプ	IP アドレスステータスのタイプです。「静的」または「DHCP」と表示されます。

[IPv6] ステータス

IPv6 テーブルとDNS サーバー情報が表示されます。

The screenshot shows the ELECOM web interface for IPv6 status. The left sidebar contains navigation links like 'ダッシュボード', 'モニター', 'システム', '一般設定', 'インターフェース設定', 'IPアドレス設定', 'IPv6', 'ステータス', 'グローバル設定', 'インターフェース設定', 'アドレス設定', 'DHCPv6クライアント設定', 'ユーザーアカウント', 'SNMP', 'スイッチ設定', 'Syslog設定', and 'アドミリンク'. The main content area is titled 'IPv6ステータス' and contains two tables. The 'DNSサーバー' table has two columns: 'DNSサーバー' and 'ソース'. The 'IPv6テーブル' table has three columns: 'インデックス', 'インターフェース', and '有効'. The 'IPv6テーブル' table shows one entry with index '1', interface 'VLAN1', and status 'ON'.

■ DNS サーバー

項目	内容
DNS サーバー	DNS サーバーの IP アドレスが表示されます。
ソース	DNS サーバーのアドレスが手動で設定されたもの（静的）か、DHCPv6 を使って自動的に取得されたものかが表示されます。

■ IPv6 テーブル

項目	内容
インデックス	インターフェースのインデックス番号が表示されます。 クリックすると、インターフェースの詳細が表示されます。
インターフェース	作成した IPv6 インターフェースの名称が表示されます。
有効	IPv6 インターフェースの有効／無効が表示されます。

■ IPv6 インターフェース詳細

ELECOM
>> Switch For Business
保存 | ログアウト | 再起動 | 日本語

システム >> IPv6 >> ステータス

ダッシュボード
モニター
システム
一般設定
インターフェース設定
IPアドレス設定
IPv6
ステータス
グローバル設定
インターフェース設定
アドレス設定
DHCPv6クライアント設定
ユーザーアカウント
SNMP
スイッチ設定
Syslog設定
アドミリンク

IPv6ステータス
IPv6ステータス > IPv6-インターフェース詳細
インターフェース: VLAN1

静的IPv6有効	ON	DHCPv6クライアント有効	ON
MTUサイズ	1500	識別子関連付け	
ICMPv6レート制限/パケットサイズ	100	IAタイプ	IA-NA
ICMPv6レート制限エラー間隔	1000	IAID	11
ND DAD有効	ON	T1	0
DAD試行回数	1	T2	0
NS間隔 (ミリ秒)	1000	状態	
ND到達可能時間 (ミリ秒)	30000	SID	
リンクローカルアドレス	fe80::3a67:a4f:fe8a:3005/64 [preferred]	アドレス	
グローバルユニキャストアドレス		優先生存期間	0
参加グループアドレス	RO2::2 RO2::1 RO2::1 間隔:3000	有効生存期間	0
		DNS	
		ドメインリスト	

項目	内容
静的 IPv6 有効	IPv6 インターフェースの有効／無効が表示されます。
MTU サイズ	IPv6 パケットの最大伝送単位 (MTU) サイズが表示されます。
ICMPv6 レート制限 パケットサイズ	与えられた時間間隔で送信を許可される ICMPv6 エラーメッセージの最大数が表示されます。 パケットが一杯になると、それ以降のエラーメッセージは抑制されます。
ICMPv6 レート制限 エラー間隔	パケットサイズまでの ICMPv6 エラーメッセージを送信できる時間 (ミリ秒) です。 0 は制限なしを意味します。
ND DAD 有効	Neighbor Discovery (ND) Duplicate Address Detection (DAD) の有効／無効が表示されます。
DAD 試行回数	本製品がこのインタフェースに対して連続して送信するネイバー勧誘の回数が表示されます。
NS 間隔 (ミリ秒)	このインタフェースに対してネイバー勧誘を再送する時間間隔 (ミリ秒) が表示されます。
ND 到達可能時間 (ミリ秒)	このインタフェースに対してネイバーが到達可能とみなされる時間 (ミリ秒単位) が表示されます。
リンクローカルアド レス	本製品のリンクローカル IP アドレスとインタフェースが生成したプレフィックスが表示されます。また、その IP アドレスが有効なアドレスであり、送信者アドレスまたは受信者アドレスとして使用できることを意味する「preferred」かどうかも表示されます。

項目	内容																		
参加グループアドレス	本製品のインタフェースが参加しているグループの IPv6 マルチキャストアドレスが表示されます。																		
DHCPv6 クライアント有効	本製品が DHCPv6 クライアントとして動作し、DHCPv6 サーバから IPv6 アドレスを取得するかどうかが表示されます。																		
識別子関連付け	<table border="1"> <tr> <td>IA タイプ</td><td>IA 内のアドレスのタイプが表示されます。 各 IA は 1 つのタイプのアドレスを保持します。 「IA_NA」は非一時的アドレスの ID アソシエーションを意味し、「IA_TA」は一時的アドレスの ID アソシエーションを意味します。</td></tr> <tr> <td>IAID</td><td>各 IA は、一意の IAID と関連する IP 情報から構成されます。</td></tr> <tr> <td>T1</td><td>DHCPv6 の T1 タイマーです。T1 の後、本製品は DHCPv6 サーバに Renew メッセージを送信します。 IA_NA オプションには T1 と T2 のフィールドが含まれていますが、IA_TA オプションには含まれていません。 DHCPv6 サーバは T1 と T2 を用いて、クライアントが IA_NA に含まれるアドレスのライフタイムが切れる前にサーバとコンタクトしてライフタイムを延長する時間を制御します。</td></tr> <tr> <td>T2</td><td>DHCPv6 の T2 タイマーです。T2 に達してもサーバからの応答がない場合、本製品は利用可能なサーバに Rebind メッセージを送信します。</td></tr> <tr> <td>状態</td><td>TA の状態が表示されます。 Active：本製品が DHCPv6 サーバからアドレスを取得し、TA が生成されます。 Renew：TA のアドレス有効期間が終了し、本製品が Renew メッセージを送信したときに表示されます。 Rebind：元の DHCPv6 サーバからの応答がなく、別の DHCPv6 サーバに Rebind メッセージを送出します。</td></tr> <tr> <td>SID</td><td>DHCPv6 サーバ固有の ID が表示されます。</td></tr> <tr> <td>アドレス</td><td>DHCPv6 サーバが割り当てる本製品のグローバルアドレスが表示されます。</td></tr> <tr> <td>優先生存期間</td><td>グローバルアドレスが優先され続ける時間 (秒) が表示されます。</td></tr> <tr> <td>有効生存期間</td><td>グローバルアドレスが有効である時間 (秒) が表示されます。</td></tr> </table>	IA タイプ	IA 内のアドレスのタイプが表示されます。 各 IA は 1 つのタイプのアドレスを保持します。 「IA_NA」は非一時的アドレスの ID アソシエーションを意味し、「IA_TA」は一時的アドレスの ID アソシエーションを意味します。	IAID	各 IA は、一意の IAID と関連する IP 情報から構成されます。	T1	DHCPv6 の T1 タイマーです。T1 の後、本製品は DHCPv6 サーバに Renew メッセージを送信します。 IA_NA オプションには T1 と T2 のフィールドが含まれていますが、IA_TA オプションには含まれていません。 DHCPv6 サーバは T1 と T2 を用いて、クライアントが IA_NA に含まれるアドレスのライフタイムが切れる前にサーバとコンタクトしてライフタイムを延長する時間を制御します。	T2	DHCPv6 の T2 タイマーです。T2 に達してもサーバからの応答がない場合、本製品は利用可能なサーバに Rebind メッセージを送信します。	状態	TA の状態が表示されます。 Active：本製品が DHCPv6 サーバからアドレスを取得し、TA が生成されます。 Renew：TA のアドレス有効期間が終了し、本製品が Renew メッセージを送信したときに表示されます。 Rebind：元の DHCPv6 サーバからの応答がなく、別の DHCPv6 サーバに Rebind メッセージを送出します。	SID	DHCPv6 サーバ固有の ID が表示されます。	アドレス	DHCPv6 サーバが割り当てる本製品のグローバルアドレスが表示されます。	優先生存期間	グローバルアドレスが優先され続ける時間 (秒) が表示されます。	有効生存期間	グローバルアドレスが有効である時間 (秒) が表示されます。
IA タイプ	IA 内のアドレスのタイプが表示されます。 各 IA は 1 つのタイプのアドレスを保持します。 「IA_NA」は非一時的アドレスの ID アソシエーションを意味し、「IA_TA」は一時的アドレスの ID アソシエーションを意味します。																		
IAID	各 IA は、一意の IAID と関連する IP 情報から構成されます。																		
T1	DHCPv6 の T1 タイマーです。T1 の後、本製品は DHCPv6 サーバに Renew メッセージを送信します。 IA_NA オプションには T1 と T2 のフィールドが含まれていますが、IA_TA オプションには含まれていません。 DHCPv6 サーバは T1 と T2 を用いて、クライアントが IA_NA に含まれるアドレスのライフタイムが切れる前にサーバとコンタクトしてライフタイムを延長する時間を制御します。																		
T2	DHCPv6 の T2 タイマーです。T2 に達してもサーバからの応答がない場合、本製品は利用可能なサーバに Rebind メッセージを送信します。																		
状態	TA の状態が表示されます。 Active：本製品が DHCPv6 サーバからアドレスを取得し、TA が生成されます。 Renew：TA のアドレス有効期間が終了し、本製品が Renew メッセージを送信したときに表示されます。 Rebind：元の DHCPv6 サーバからの応答がなく、別の DHCPv6 サーバに Rebind メッセージを送出します。																		
SID	DHCPv6 サーバ固有の ID が表示されます。																		
アドレス	DHCPv6 サーバが割り当てる本製品のグローバルアドレスが表示されます。																		
優先生存期間	グローバルアドレスが優先され続ける時間 (秒) が表示されます。																		
有効生存期間	グローバルアドレスが有効である時間 (秒) が表示されます。																		
DNS	DHCPv6 サーバによって割り当てられた DNS サーバアドレスが表示されます。																		
ドメインリスト	本製品が DNS サーバにドメイン名の解決を問い合わせる際のアドレスレコードが表示されます。																		
DHCPv6 クライアントの再起動	「再起動」をクリックすると、DHCPv6 サーバに新しい DHCP 要求が送信され、このインタフェースの IPv6 アドレスと DNS 情報が更新されます。																		

[IPv6] グローバル設定

グローバル IPv6 設定を構成します。

項目	内容
IPv6 ホップ制限	ルーター広告の最大ホップ数（1 ～ 255）を指定します。 これは IPv6 パケットが IPv6 ルーターに破棄されるまでに送信を許可される最大ホップ数で、IPv4 の TTL フィールドに似ています。
ICMPv6 レート制限 パケットサイズ	一定時間内に送信できる ICMPv6 エラーメッセージの最大数（1 ～ 200）を指定します。 パケットが一杯になると、それ以降のエラーメッセージは抑制されます。
ICMPv6 レート制限 エラー間隔	パケットサイズまでの ICMPv6 エラーメッセージを送信できる時間（0 ～ 2147483647 ミリ秒）を指定します。0 は制限なしを意味します。
適用	変更内容を本製品のランタイムメモリに保存します。 本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。

【IPv6】インターフェース設定

作成したIPv6 インタフェースの表示および設定します

The screenshot shows the ELECOM web interface for IPv6 settings. The breadcrumb trail is 'システム >> IPv6 >> インターフェース設定'. The left sidebar has a menu with 'システム' selected, and sub-items like '一般設定', 'インターフェース設定', 'IPv6', 'ステータス', 'グローバル設定', 'アドレス設定', 'DHCPv6クライアント設定', 'ユーザーアカウント', and 'SNMP'. The main content area is titled 'IPv6 インターフェース設定' and contains a table with columns: 'インデックス', 'インターフェース', and '有効'. The table has one row with index 1, interface VLAN1, and status ON. An '編集' (Edit) button is in the top right corner of the table.

インデックス	インターフェース	有効
1	VLAN1	ON

選択したインターフェースを編集します。

→ [58ページ](#)

項目	内容
インデックス	インターフェースのインデックス番号が表示されます。
インターフェース	作成した IPv6 インターフェースの名前が表示されます。
有効	IPv6 インターフェースが有効かどうかが表示されます。

■ インターフェース編集画面

インターフェース

VLAN1 ▾

有効

ON ☒

適用

クリア

キャンセル

項目	内容
インターフェース	設定する IPv6 インタフェースを選択します。
有効	インターフェイスの有効／無効を切り替えます。
適用	変更内容を本製品のランタイムメモリに保存します。 本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。

【IPv6】アドレス設定

IPv6 リンクローカルアドレス設定

IPv6 のリンクローカルアドレスを設定します。

選択したリンクローカルアドレス
を編集します。

→ [60 ページ](#)

項目	内容
インデックス	インターフェースのインデックス番号が表示されます。
インターフェース	作成した IPv6 インターフェースの名前が表示されます。
IPv6 リンクローカルアドレス	インターフェイスの静的 IPv6 リンクローカルアドレスが表示されます。
IPv6 ゲートウェイ	インターフェースのデフォルトゲートウェイ IPv6 アドレスが表示されます。

■ IPv6 リンクローカルアドレスの編集

インターフェース	VLAN1 ▼
リンクローカルアドレス	<input type="text"/>
デフォルトゲートウェイ	<input type="text"/>
<div>適用 クリア キャンセル</div>	

項目	内容
インターフェースタイプ	設定する IPv6 インタフェースのタイプを選択します。
リンクローカルアドレス	インターフェースの静的 IPv6 リンクローカルアドレスを手動で設定します。
デフォルトゲートウェイ	インターフェースのデフォルトゲートウェイ IPv6 アドレスを設定します。インターフェイスがフレームの宛先のルーティング情報を見つけれない場合、デフォルトゲートウェイにパケットを転送します。
適用	変更内容を本製品のランタイムメモリに保存します。 本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。
クリア	フィールドが工場出荷時のデフォルトにクリアされます。

IPv6 グローバルアドレス設定

IPv6 のグローバルアドレスを設定します。

IPv6 グローバルアドレスを追加したり、選択した IPv6 グローバルアドレスを編集します。

→ [62 ページ](#)

選択した IPv6 グローバルアドレスを削除します。

■ IPv6 DNS サーバー

項目	内容
DNS サーバー 1	IP アドレスの代わりにドメイン名を使用できるように、ドメインネームサーバーの IPv6 アドレスを入力します。
DNS サーバー 2	
適用	変更内容を本製品のランタイムメモリに保存します。 本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。

■ IPv6 グローバルアドレス設定

項目	内容
インデックス	インターフェースのインデックス番号が表示されます。
インターフェース	作成した IPv6 インターフェースの名前が表示されます。
IPv6 グローバルアドレス/プレフィックス長	インターフェイスの IPv6 グローバルアドレスとプレフィックス長が表示されます。
EUI-64	グローバルアドレスのインタフェース ID が EUI-64 形式で生成されているかどうかが表示されます。

■ IPv6 グローバルアドレスの追加／編集

インターフェース	VLAN1 ▾	
IPv6 グローバルアドレス	<input type="text"/>	<input type="checkbox"/> EUI-64
プレフィックス長	<input type="text"/>	
<div>適用 クリア キャンセル</div>		

項目	内容
インターフェース	設定する IPv6 インタフェースを選択します。
IPv6 グローバルアドレス	インターフェースの静的 IPv6 グローバルアドレスを手動で設定します。
プレフィックス長	ネットワークアドレスを構成するアドレスの最上位ビット数（左から）を指定する IPv6 プレフィックス長を指定します。
EUI-64	EUI-64 形式を使用してインターフェイス ID を自動生成するときはチェックを入れます。
適用	変更内容を本製品のランタイムメモリに保存します。 本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。
クリア	フィールドが工場出荷時のデフォルトにクリアされます。

[IPv6] DHCPv6 クライアント設定

本製品が DHCPv6 クライアントとして動作する際の DHCP 設定をします。

選択した DHCPv6 クライアントを編集します。

→ [64 ページ](#)

項目	内容
インデックス	インターフェースのインデックス番号が表示されます。
インターフェース	作成した IPv6 インターフェースの名前が表示されます。
IA-NA	DHCPv6 サーバから一時的でない IP アドレスを取得しているときは「ON」と表示されます。
Rapid-Commit	Rapid Commit オプションの ON / OFF が表示されます。
DNS	DHCPv6 サーバから DNS サーバ IPv6 アドレスを取得するかどうかが表示されます。
ドメインリスト	DHCP サーバからドメイン名のリストを取得するかどうかが表示されます。
情報更新期間（最小値）	DHCPv6 サーバとその他の設定情報を再度交換する時間間隔（秒）が表示されます。

■ DHCPv6 クライアント編集画面

インターフェース	VLAN1 ▾
IAタイプ	<input checked="" type="checkbox"/> IA-NA <input type="checkbox"/> Rapid-Commit
オプション	<input type="checkbox"/> DNS <input type="checkbox"/> ドメインリスト
情報更新期間(最小値)	86400 秒
<input type="button" value="適用"/> <input type="button" value="クリア"/> <input type="button" value="キャンセル"/>	

項目	内容	
インターフェース	設定する IPv6 インタフェースを選択します。	
IA タイプ	IA-NA	選択すると、本製品はこのインタフェースに対して DHCPv6 サーバから一時的でない IP アドレスを取得します。
	Rapid-Commit	選択すると、DHCPv6 Solicit メッセージに Rapid Commit オプションを付けて送信し、DHCPv6 サーバから 2 メッセージの高速交換で情報を取得できます。本製品は Rapid Commit オプションを含まない Reply メッセージを破棄します。DHCPv6 サーバも Rapid Commit オプションをサポートしている必要があります。
オプション	DNS	選択すると、DNS サーバから IPv6 アドレスを取得します。
	ドメインリスト	選択すると、DHCP サーバからドメイン名のリストを取得します。
情報更新期間（最小値）	DHCPv6 サーバと他のコンフィグレーション情報を再度交換する時間間隔（600 ～ 4294967295 秒）を指定します。（初期値：86400 秒）	
適用	変更内容を本製品のランタイムメモリに保存します。 本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。	

ユーザーアカウント

管理者のパスワードを変更したり、ユーザーを編集／追加します。

ELECOM >> Switch For Business

保存 | ログアウト | 再起動 | 日本語 ▾

システム >> ユーザーアカウント

ダッシュボード
モニター
システム
一般設定
インターフェース設定
IPアドレス設定
IPv6
ユーザーアカウント
SNMP
スイッチ設定
Syslog設定
アドミリンク
ポート
スイッチング
ネットワーク
セキュリティ
管理

ユーザーアカウント

Administrator

古いパスワード

新しいパスワード

新しいパスワード(確認用)

パスワードを変更する際は、必ず新しいパスワードを記録してください。パスワードを忘れると、システムにログインできなくなります。

ユーザーアカウント編集

ログイン	ユーザー名	パスワード	新しいパスワード(確認用)	権限レベル
1				
2				
3				
4				
5				
6				
7				
8				

Administrator

管理者のパスワードを設定します。

項目	内容
古いパスワード	現在のパスワードを入力します。 デフォルトの管理者パスワードは装置ラベルに記載されています。
新しいパスワード	新しいパスワードを入力します。
新しいパスワード (確認用)	(8 文字以上 32 文字以内。? (クエスチョンマーク) と “ (ダブルクォーテーション) を除く半角英数記号のみ)

ユーザーアカウント編集

ユーザーアカウントを作成・編集します。

これらのユーザーは、読み取り専用アクセス権を持つことができます。

項目	内容
ログイン	ユーザーアカウントのインデックス番号です。
ユーザー名	ユーザー名を設定します。 (最大 32 文字まで。? (クエスチョンマーク) (パイプ) " (ダブルクォーテーション) , (コンマ) は使用不可)
パスワード	パスワードを入力します。
新しいパスワード (確認用)	(8 文字以上 32 文字以内。? (クエスチョンマーク) (パイプ) ' (クォーテーション) " (ダブルクォーテーション) (スペース) , (コンマ) : (コロン) は使用不可)
権限レベル	このユーザーの特権レベル以下のいずれかから設定入力します。
	0 基本的なシステム情報を表示します。
	3 構成またはステータスを表示します。
	13 ログインアカウント、SNMP ユーザーアカウント、認証方法シーケンスおよび認証設定、複数ログイン、管理者および有効パスワード、構成情報表示を除く機能を構成します。
	14 ログインアカウント、SNMP ユーザーアカウント、認証方法シーケンスおよび認証設定、複数ログイン、管理者および有効パスワードの設定、および構成情報の表示を行います。

SNMP

SNMP

SNMP の設定をします。

ELECOM >> Switch For Business

保存 | ログアウト | 再起動 | 日本語

システム >> SNMP

ダッシュボード

モニター

システム

一般設定

インターフェース設定

IPアドレス設定

IPv6

ユーザーアカウント

SNMP

スイッチ設定

Syslog設定

アドミニク

ポート

スウィッチング

ネットワーク

セキュリティ

管理

SNMP

SNMPユーザー

SNMPトラップグループ

SNMPトラップポート

一般設定

トラップの宛先

有効 ☐ ON ☒ OFF

SNMPバージョン

v2c

コミュニティ取得

public

コミュニティ設定

public

トラップコミュニティ

public

インデックス

SNMPバージョン

IPアドレス

ポート

ユーザー名

1	<div>v2c</div>	<div>0.0.0.0</div>	<div>162</div>	
2	<div>v2c</div>	<div>0.0.0.0</div>	<div>162</div>	
3	<div>v2c</div>	<div>0.0.0.0</div>	<div>162</div>	
4	<div>v2c</div>	<div>0.0.0.0</div>	<div>162</div>	

適用 キャンセル

■ 一般設定

項目	内容
有効	SNMP 機能の有効／無効を切り替えます。
SNMP バージョン	<p>SNMP バージョンを選択します。</p> <p>本製品の SNMP バージョンは SNMP マネージャのバージョンと一致している必要があります。</p> <p>SNMP バージョン 2c(v2c)、SNMP バージョン 2c(v2c)、SNMP バージョン 3(v3)、またはその両方 (v3v2c) を選択してください。</p> <p>SNMP バージョン 2c は、SNMP バージョン 1 と下位互換性があります。</p>
コミュニティ取得	<p>管理ステーションからの Get- および GetNext- 要求を受信する際のパスワードを入力します。</p> <p>コミュニティ取得文字列は、SNMP バージョン 2c 以下を使用する SNMP マネージャのみが使用します。</p>

項目	内容
コミュニティ設定	管理ステーションから Set- リクエストを受信する際のパスワードを入力します。 コミュニティ設定文字列は、SNMP バージョン 2c 以下を使用する SNMP マネージャーによってのみ使用されます。
トラップコミュニティ	SNMP マネージャへの各トラップと共に送信されるパスワードを入力します。 トラップコミュニティ文字列は、SNMP バージョン 2c 以下を使用する SNMP マネージャーによってのみ使用されます。

■ トラップの宛先

項目	内容
インデックス	トラップ送信先のインデックス番号が表示されます。
SNMP バージョン	SNMP トラップメッセージのバージョンを指定します。
IP アドレス	SNMP トラップを送信する最大 4 つのマネージャの IP アドレスを入力します。
ポート	マネージャが SNMP トラップをリッスンするポート番号を入力します。
ユーザー名	SNMP v3 トラップと共に SNMP マネージャに送信するユーザ名を入力します。 このユーザ名は、既存の SNMP ユーザーと一致している必要があります。 → 「SNMP ユーザー」 (69 ページ)

SNMP ユーザー

SNMP v3を使用するマネージャとの認証用にSNMP ユーザを作成し、SNMPグループに関連付けます。



選択したSNMP ユーザーを編集したり、SNMP ユーザーを追加します。

→ [70ページ](#)

選択したSNMP ユーザーを削除します。

項目	内容
インデックス	ログインアカウントを識別する読み取り専用の番号が表示されます。
ユーザー名	ログインアカウントのユーザ名が表示されます。
セキュリティレベル	このユーザとの SNMP 通信に認証または暗号化を使用するかどうかが表示されます。
認証	このユーザとの SNMP 通信に使用する認証アルゴリズムが表示されます。
暗号化	このユーザーとの SNMP 通信に使用する暗号化方法が表示されます。
グループ	このユーザーが属する SNMP グループが表示されます。

■ SNMP ユーザーの追加／編集

ユーザー名	<input type="text"/>		
セキュリティレベル	認証なし ▾		
認証	MD5 ▾	パスワード	<input type="text"/>
暗号化	DES ▾	パスワード	<input type="text"/>
グループ	管理者 ▾		
<input type="button" value="適用"/> <input type="button" value="クリア"/> <input type="button" value="キャンセル"/>			

項目	内容						
ユーザー名	ログインアカウントのユーザ名を入力します。 (最大半角 32 文字まで。? (クエスチョンマーク) (パイプ) ' (フォーテーション) " (ダブルフォーテーション) (スペース) は使用不可)						
セキュリティレベル	<p>SNMP 通信に認証または暗号化を実装するかどうかを選択します。 SNMP ユーザーのセキュリティレベルは、本製品のセキュリティレベル以上に設定する必要があります。</p> <table> <tr> <td>認証なし</td><td>SNMP マネージャに送信するパスワード文字列としてユーザー名を使用します。これは、SNMP v2c の Get、Set、Trap Community に相当します。最も低いセキュリティレベルとなります。</td></tr> <tr> <td>認証あり</td><td>SNMP メッセージに認証アルゴリズムを実装します。</td></tr> <tr> <td>プライベート</td><td>認証と暗号化を使用します。最も高いセキュリティレベルです。</td></tr> </table>	認証なし	SNMP マネージャに送信するパスワード文字列としてユーザー名を使用します。これは、SNMP v2c の Get、Set、Trap Community に相当します。最も低いセキュリティレベルとなります。	認証あり	SNMP メッセージに認証アルゴリズムを実装します。	プライベート	認証と暗号化を使用します。最も高いセキュリティレベルです。
認証なし	SNMP マネージャに送信するパスワード文字列としてユーザー名を使用します。これは、SNMP v2c の Get、Set、Trap Community に相当します。最も低いセキュリティレベルとなります。						
認証あり	SNMP メッセージに認証アルゴリズムを実装します。						
プライベート	認証と暗号化を使用します。最も高いセキュリティレベルです。						
認証	認証アルゴリズムを選択します。SHA 認証は一般的に MD5 認証よりも強力ですが、認証速度が遅くなります。						
暗号化	<p>SNMP 通信の暗号化方法を指定します。</p> <table> <tr> <td>DES</td><td>広く使用されているデータ暗号化方式です。 各 64 ビットのデータブロックに 56 ビットのキーを適用します。</td></tr> <tr> <td>AES</td><td>秘密鍵を使用するデータ暗号化方式です。 128 ビットのデータブロックに 128 ビットの鍵を適用します。</td></tr> </table>	DES	広く使用されているデータ暗号化方式です。 各 64 ビットのデータブロックに 56 ビットのキーを適用します。	AES	秘密鍵を使用するデータ暗号化方式です。 128 ビットのデータブロックに 128 ビットの鍵を適用します。		
DES	広く使用されているデータ暗号化方式です。 各 64 ビットのデータブロックに 56 ビットのキーを適用します。						
AES	秘密鍵を使用するデータ暗号化方式です。 128 ビットのデータブロックに 128 ビットの鍵を適用します。						
パスワード	SNMP ユーザー認証用のパスワードを入力します。 (最大 32 文字まで。? (クエスチョンマーク) (パイプ) ' (フォーテーション) " (ダブルフォーテーション) , (コンマ) (スペース) は使用不可)						

項目	内容	
グループ	ユーザーが属するグループを指定します。	
	管理者	管理者アカウントの管理を含め、あらゆる種類のシステム構成を実行できます。
	読み書き可能	読み書きできる権限を持ち、ユーザアカウントとAAA コンフィグレーションを除く本製品の MIB を作成および編集できます。
	読み取り専用	読み取り権限のみを持ち、本製品から情報を収集できます。
適用	変更内容を本製品のランタイムメモリに保存します。 本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。	

SNMPトラップグループ

各SNMP マネージャに送信するSNMPトラップのタイプを指定します。

項目	内容
トラップ宛先 IP アドレス	設定したトラップ宛先 IP アドレスのいずれかを選択します。 最初に、トラップ宛先 IP アドレスを構成する必要があります。 → 「SNMP」 (67 ページ)
オプション	本製品が SNMP ステーションに送信する個々の SNMP トラップを選択します。 トラップはカテゴリ別にグループ化されています。 カテゴリを選択すると、そのカテゴリのすべてのトラップが自動的に選択されます。 SNMP ステーションに送信したくないトラップは、個別にチェックボックスを外してください。 カテゴリのチェックボックスを外すと、そのカテゴリのトラップのチェックボックスがすべて自動的にクリアされます。
適用	変更内容を本製品のランタイムメモリに保存します。 本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。

SNMPトラップポート

ポートで受信したトラップをSNMPマネージャに送信するかどうかを設定します。

ポート	有効
*	<input type="checkbox"/>
1	<input checked="" type="checkbox"/>
2	<input checked="" type="checkbox"/>
3	<input checked="" type="checkbox"/>
4	<input checked="" type="checkbox"/>
5	<input checked="" type="checkbox"/>
6	<input checked="" type="checkbox"/>
7	<input checked="" type="checkbox"/>
8	<input checked="" type="checkbox"/>
9	<input checked="" type="checkbox"/>
10	<input checked="" type="checkbox"/>

項目	内容
オプション	ここで設定したいトラップタイプを選択します。
ポート	ポート番号が表示されます。 「*」の行を変更すると、すべてのポートに変更が適用されます。
有効	チェックを入れると、そのポートで受信した関連トラップをSNMPマネージャに送信します。
適用	変更内容を本製品のランタイムメモリに保存します。 本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。

スイッチ設定

VLAN (Virtual Local Area Network) のタイプ、スイッチングプロトコルの有効化、MAC 学習エージング時間の設定などをします。

項目	内容
VLAN タイプ	VLAN タイプを選択します。
ブリッジプロトコル 透過	「ON」にすると、ブリッジング制御プロトコル（STP など）を処理できるようにします。 「ポート」－「ポート設定」(100 ページ)でBPDU 制御を設定する必要があります。
MAC アドレス学習 エージングタイム	動的に学習された MAC アドレスがエージアウトするまでの時間（MAC アドレステーブルに残る時間）を設定します。 (設定範囲：10 秒～ 1000000 秒) (初期値：300 秒)
ARP エージング タイム	動的に学習された ARP エントリがエージアウトするまでの時間（ARP テーブルに残る時間）を設定します。 (設定範囲：60 秒～ 1000000 秒) (初期値：300 秒) ここでの設定は、[適用]をクリックした後に ARP テーブルに新しく追加される ARP エントリに適用されます。
適用	変更内容を本製品のランタイムメモリに保存します。 本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。

Syslog 設定

Syslog の設定をします。

Syslog サーバーを追加したり、選択した Syslog サーバーを編集します。

→ [76 ページ](#)

選択した Syslog サーバーを削除します。

■ Syslog 設定

項目	内容
有効	Syslog 設定の有効／無効を切り替えます。
カテゴリ	生成できるログのカテゴリ名が表示されます。
有効	Syslog を生成するカテゴリにチェックを入れます。
ファシリティ	ログ機能を使用すると、Syslog サーバーのさまざまなファイルにログを送信できます。詳細については、Syslog プログラムのドキュメントを参照してください。
適用	変更内容を本製品のランタイムメモリに保存します。 本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。

■ Syslog サーバー設定

項目	内容
インデックス	Syslog サーバーエントリーのインデックス番号が表示されます。
有効	Syslog 設定の有効／無効が表示されます。
IP アドレス	Syslog サーバーの IP アドレスが表示されます。
UDP ポート	Syslog サーバーのポートが表示されます。
ログレベル	ログの重大度レベルが表示されます。

■ Syslog サーバーの追加／編集

有効

☐ OFF

サーバーアドレス

UDPポート

514

ログレベル

レベル 0 ▾

適用

クリア

キャンセル

項目	内容
有効	この syslog サーバーにログを送信する設定にするときは「ON」にします。「OFF」にすると、エントリーのみ作成し、ログは送信しません。
サーバーアドレス	Syslog サーバーの IPv4 または IPv6 アドレスを入力します。
UDP ポート	Syslog のサーバーポートを設定します。 (初期値：514)
ログレベル	この syslog サーバーに送信するログの重大度レベルを選択します。数字が小さいほど、ログの重要度が高くなります。 (初期値：レベル 0)
適用	変更内容を本製品のランタイムメモリに保存します。 本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。
クリア	フィールドが工場出荷時のデフォルトにクリアされます。

【アドミリンク】基本設定

アドミリンク機能の基本設定をします。

MEMO

アドミリンク機能を利用する場合、本体の日時設定にNTPサーバーを使用してください。
(→ [46ページ](#))

項目	内容				
アドミリンク 基本設定	<table border="1"> <tr> <td>アドミリンク機能</td><td>アドミリンク機能の「有効」または「無効」を設定します。 (初期値：無効)</td></tr> <tr> <td>登録状態</td><td>アドミリンクサービスへの製品登録状態が表示されます。</td></tr> </table>	アドミリンク機能	アドミリンク機能の「有効」または「無効」を設定します。 (初期値：無効)	登録状態	アドミリンクサービスへの製品登録状態が表示されます。
アドミリンク機能	アドミリンク機能の「有効」または「無効」を設定します。 (初期値：無効)				
登録状態	アドミリンクサービスへの製品登録状態が表示されます。				
デバイス登録 コードの発行	<p>ボタンをクリックするとデバイス登録コードが発行されます。 表示されたデバイス登録コードをコピーして、アドミリンクサーバーのデバイスグループに登録を行います。 (デバイスの登録方法はアドミリンク ユーザーズマニュアルを参照してください)</p>				

※ アドミリンクの詳細やユーザーズマニュアルについては下記URLからご確認いただけます。

<https://www.elecom.co.jp/r/s349>

【アドミリンク】詳細設定

アドミリンク機能の詳細設定をします。

ELECOM
>> Switch For Business
保存 | ログアウト | 再起動 | 日本語

システム
アドミリンク
詳細設定

ダッシュボード
モニター
システム
一般設定
インターフェース設定
IPアドレス設定
IPv6
ユーザーアカウント
SNMP
スイッチ設定
Syslog設定
アドミリンク
基本設定
詳細設定
ポート
スイッチング
ネットワーク
セキュリティ
管理

アドミリンク詳細設定

詳細設定

アドミリンク接続用プロキシ設定

プロキシサーバー

○ 使用する

● 使用しない

アドレス

ポート

ユーザー名

パスワード

遠隔操作許可

設定ファイルアップロード許可

ログファイルアップロード許可

接続クライアントファイルアップロード許可

接続クライアントファイル自動アップロード間隔

○ 有効

● 無効

○ 有効

● 無効

○ 有効

● 無効

○ 有効

● 無効

0分

適用

項目	内容
アドミリンク接続用 プロキシ設定	プロキシサーバー アドミリンクサービスへの接続にプロキシサーバーを使用するか設定します。 プロキシ経由でアドミリンクサービスへ接続する必要がある場合、「使用する」を選択してください。 (初期値：使用しない)
	アドレス プロキシサーバーのアドレスを入力します。
	ポート プロキシサーバーのポート番号を入力します。
	ユーザー名 必要の場合、ユーザー名を入力します。 (最大 64 文字まで。記号は使用不可)
	パスワード 必要の場合、パスワードを入力します。 (最大 64 文字まで。記号は使用不可)

78

項目	内容	
遠隔操作設定	遠隔操作許可	アドミリンクサーバーから遠隔操作を許可するか設定します。(初期値：無効)
	設定ファイルアップロード許可	設定ファイルのアップロードを許可するか設定します。(初期値：無効)
	ログファイルアップロード許可	ログファイルのアップロードを許可するか設定します。(初期値：無効)
	接続クライアントファイルアップロード許可	持続クライアントファイルのアップロードを許可するか設定します。(初期値：無効)
	接続クライアントファイル自動アップロード間隔	接続クライアントファイルを自動的にアップロードする間隔を設定します。 (設定範囲：1 時間 / 3 時間 / 6 時間 / なし) (初期値：6 時間)

Green Ethernet

消費電力削減の設定をします。

ELECOM >> Switch For Business

保存 | ログアウト | 再起動 | 日本語

ポート >> Green Ethernet

ダッシュボード

モニター

システム

ポート

Green Ethernet

リンクアグリゲーション

LLDP

ポート設定

スイッチング

ネットワーク

セキュリティ

管理

Green Ethernet

IEEE802.3az ☐

Auto Power Down ☐

ショートリーチ ☐

ポート	IEEE802.3az	Auto Power Down	ショートリーチ
*	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1	<input 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"/>
9	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

適用

キャンセル

項目	内容
IEEE802.3az	EEE(Energy Efficient Ethernet)の有効／無効を切り替えます。 (初期値：OFF)
Auto Power Down	「ON」にすると、リンクがダウンしているときにポートの物理層機能のほとんどすべての機能をオフにするため、ポートはリンクパートナーからのリンクアップパルスをチェックするためだけに電力を使用します。 リンクアップパルスが検出されると、ポートはオートパワーダウンから復帰し、通常通り動作します。 (初期値：OFF)
ショートリーチ	「ON」にすると、ポートに接続されたケーブルの長さに応じて各ポートの送信電力を調整することで電力を節約します。 (初期値：OFF)

■ 表

項目	内容
ポート	ポート番号が表示されます。 「*」の行を変更すると、すべてのポートに変更が適用されます。

項目	内容
IEEE802.3az	チェックを入れると、そのポートに対して省電力機能が有効になります。
Auto Power Down	
ショートリーチ	
適用	変更内容を本製品のランタイムメモリに保存します。 本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。

リンクアグリゲーション

リンクアグリゲーションステータス

トランクグループに設定したポートや、トランクグループ内の 1 つの論理リンクとして現在データを送信しているポートなどが表示されます。

ELECOM

>> Switch For Business

保存 | ログアウト | 再起動 | 日本語

ポート >> リンクアグリゲーション

ダッシュボード
モニター
システム
ポート
Green Ethernet
リンクアグリゲーション
LLDP
ポート設定
スイッチング

リンクアグリゲーションステータス

リンクアグリゲーション設定

リンクアグリゲーション制御プロトコル

グループID	有効ポート	同期ポート	Aggregator ID	Criteria	ステータス
T1	-	-	-	src-dst-mac	-
T2	-	-	-	src-dst-mac	-
T3	-	-	-	src-dst-mac	-
T4	-	-	-	src-dst-mac	-
T5	-	-	-	src-dst-mac	-
T6	-	-	-	src-dst-mac	-
T7	-	-	-	src-dst-mac	-
T8	-	-	-	src-dst-mac	-

項目	内容
グループ ID	複数のポートを含む 1 つの論理リンクを識別するためのグループ ID です。
有効ポート	リンクアグリゲーション設定画面でトランクグループに設定したポートです。 ポート番号は、このトランクグループが有効化されており、このグループに属するポートが存在する場合のみ表示されます。
同期ポート	このトランクグループ内で現在 1 つの論理リンクとしてデータを伝送しているポートです。
Aggregator ID	リンクアグリゲータ ID は、システム優先度、MAC アドレス、キー、ポート優先度、ポート番号から構成されます。 この ID は、このトランクグループに属するポートがあり、このグループに対して LACP も有効になっている場合にのみ表示されます。

項目	内容	
Criteria	このトランクグループで使用する発信トラフィック分配アルゴリズムが表示されます。同じソースおよび / または同じ宛先からのパケットは、トランク内の同じリンクで送信されます。	
	src-mac	パケットの送信元 MAC アドレスに基づいてトラフィックを分配します。
	dst-mac	パケットの宛先 MAC アドレスに基づいてトラフィックを分配します。
	src-dst-mac	パケットの送信元 MAC アドレスと宛先 MAC アドレスの組み合わせに基づいてトラフィックを分配します。
	src-ip	パケットの送信元 IP アドレスに基づいてトラフィックを分配します。
	dst-ip	パケットの宛先 IP アドレスに基づいてトラフィックを分配します。
	src-dst-ip	送信元 IP アドレスと宛先 IP アドレスの組み合わせに基づいてトラフィックを分配します。
ステータス	ポートがどのようにトランクグループに追加されたかが表示されます。	
	Static	ポートがトランクグループのスタティックメンバーとして設定されている場合に表示されます。
	LACP	ポートが LACP 経由でトランクグループに参加するように設定されている場合に表示されます。

リンクアグリゲーション設定

スタティックリンクアグリゲーションを設定します。

ELECOM
>> Switch For Business
保存 | ログアウト | 再起動 | 日本語

ポート >> リンクアグリゲーション

ダッシュボード
モニター
システム
ポート
Green Ethernet
リンクアグリゲーション
LLDP
ポート設定
スイッチング
ネットワーク
セキュリティ
管理

リンクアグリゲーションステータス
リンクアグリゲーション設定
リンクアグリゲーション制御プロトコル

グループID	有効	Criteria
T1	<input type="checkbox"/>	src-dst-mac
T2	<input type="checkbox"/>	src-dst-mac
T3	<input type="checkbox"/>	src-dst-mac
T4	<input type="checkbox"/>	src-dst-mac
T5	<input type="checkbox"/>	src-dst-mac
T6	<input type="checkbox"/>	src-dst-mac
T7	<input type="checkbox"/>	src-dst-mac
T8	<input type="checkbox"/>	src-dst-mac

ポート	グループ
1	なし
2	なし
3	なし
4	なし
5	なし
6	なし
7	なし
8	なし
9	なし
10	なし

適用
キャンセル

項目	内容
グループ ID	リンクアグリゲーショングループ(複数のポートを含む 1 つの論理リンク)を識別します。
有効	チェックすると、トランググループを有効にします。

項目	内容												
Criteria	発信トラフィック分配タイプを選択します。 同じ送信元および / または同じ宛先からのパケットは、トランク内の同じリンクを介して送信されます。デフォルトでは、本製品は src-dst-mac ディストリビューションタイプを使用します。 本製品がルータの背後にある場合、パケットの宛先または送信元 MAC アドレスは変更されます。この場合、ポートランキングが正常に動作するように、IP アドレスに基づいてトラフィックを分配するように設定してください。												
	<table><tr><td>src-mac</td><td>パケットの送信元 MAC アドレスに基づいてトラフィックを分配します。</td></tr><tr><td>dst-mac</td><td>宛先 MAC アドレスに基づいてトラフィックを分配します。</td></tr><tr><td>src-dst-mac</td><td>パケットの送信元 MAC アドレスと宛先 MAC アドレスの組み合わせに基づいてトラフィックを分配します。</td></tr><tr><td>src-ip</td><td>パケットの送信元 IP アドレスに基づいてトラフィックを分配します。</td></tr><tr><td>dst-ip</td><td>パケットの宛先 IP アドレスに基づいてトラフィックを分配します。</td></tr><tr><td>src-dst-ip</td><td>パケットの送信元 IP アドレスと宛先 IP アドレスの組み合わせに基づいてトラフィックを分配します。</td></tr></table>	src-mac	パケットの送信元 MAC アドレスに基づいてトラフィックを分配します。	dst-mac	宛先 MAC アドレスに基づいてトラフィックを分配します。	src-dst-mac	パケットの送信元 MAC アドレスと宛先 MAC アドレスの組み合わせに基づいてトラフィックを分配します。	src-ip	パケットの送信元 IP アドレスに基づいてトラフィックを分配します。	dst-ip	パケットの宛先 IP アドレスに基づいてトラフィックを分配します。	src-dst-ip	パケットの送信元 IP アドレスと宛先 IP アドレスの組み合わせに基づいてトラフィックを分配します。
	src-mac	パケットの送信元 MAC アドレスに基づいてトラフィックを分配します。											
	dst-mac	宛先 MAC アドレスに基づいてトラフィックを分配します。											
	src-dst-mac	パケットの送信元 MAC アドレスと宛先 MAC アドレスの組み合わせに基づいてトラフィックを分配します。											
	src-ip	パケットの送信元 IP アドレスに基づいてトラフィックを分配します。											
	dst-ip	パケットの宛先 IP アドレスに基づいてトラフィックを分配します。											
src-dst-ip	パケットの送信元 IP アドレスと宛先 IP アドレスの組み合わせに基づいてトラフィックを分配します。												
ポート	ポート番号が表示されます。												
グループ	ポートが属するトランクグループを選択します。												
	<div><div>注意</div><div>本製品でポートセキュリティ機能を有効にし、ポートに対してポートセキュリティ設定を行った場合、そのポートをアクティブなトランクグループに含めることはできません。</div></div>												
適用	変更内容を本製品のランタイムメモリに保存します。 本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。												

リンクアグリゲーション制御プロトコル

Link Aggregation Control Protocol (LACP)を有効にします。

重要

ダイナミックリンクアグリゲーションを有効するときのみ、この画面で設定してください。

ELECOM >> Switch For Business 保存 | ログアウト | 再起動 | 日本語

ポート >> リンクアグリゲーション

リンクアグリゲーションステータス リンクアグリゲーション設定 **リンクアグリゲーション制御プロトコル**

有効 ☒ ON

システム優先度

グループID	LACP Active
T1	<input type="checkbox"/>
T2	<input type="checkbox"/>
T3	<input type="checkbox"/>
T4	<input type="checkbox"/>
T5	<input type="checkbox"/>
T6	<input type="checkbox"/>
T7	<input type="checkbox"/>
T8	<input type="checkbox"/>

ポート	LACP タイムアウト
*	30 ↓
1	30 ↓
2	30 ↓
3	30 ↓
4	30 ↓
5	30 ↓
6	30 ↓
7	30 ↓
8	30 ↓
9	30 ↓
10	30 ↓

適用 キャンセル

項目	内容
有効	リンクアグリゲーション制御プロトコル（LACP）の有効／無効を切り替えます。
システム優先度	<p>LACP（Link Aggregation Control Protocol）を使用するアクティブポートの優先度を設定する番号を入力します。</p> <p>数値が小さいほど優先度が高くなります。</p> <p>LACPのシステムプライオリティは1～65,535の数値です。</p> <p>システム・プライオリティが最も低いスイッチ（システム・プライオリティが同じ場合はポート番号も最も低い）がLACP「サーバ」になります。LACP「サーバ」はLACP設定の動作を制御します。</p> <p>（初期値：65535）</p>

項目	内容
グループ ID	リンクアグリゲーショングループの ID が表示されます。
LACP Active	トランクの LACP を有効にする場合に選択します。
ポート	ポート番号が表示されます。 「*」の行を変更すると、すべてのポートに変更が適用されます。
LACP タイムアウト	トランクグループ内の相手ポートがまだアップしているかどうかを確認するために、個々のポートが LACP パケットを交換する間の時間間隔を設定します。 3 回試みても応答がない場合、ポートは「ダウン」とみなされ、トランクから削除されます。 ビジー状態のトランクリンクには短いタイムアウト（1 秒）を設定し、無効になったポートができるだけ早くトランクグループから削除されるようにします。 (初期設定：30 秒) (設定範囲：1 ～ 30 秒)

LLDP

LLDP ローカルステータス

LLDP ステータスの概要が表示されます。

ELECOM >> Switch For Business

保存 | ログアウト | 再起動 | 日本語

ポート >> LLDP

LLDP ローカルステータス
LLDP リモートステータス
LLDP 設定
Basic TLV Setting
Org-specific TLV Setting

ダッシュボード
モニター
システム
ポート
Green Ethernet
リンクアグリゲーション
LLDP
ポート設定
スイッチング
ネットワーク
セキュリティ
管理

Basic TLV

Chassis ID TLV
Chassis ID Subtype
Chassis ID

MACアドレス
38:97:A4:8A:30:F0

System Name TLV
System Name

EHB-SX2B08F

System Description TLV
System Description

1.0.0

System Capabilities TLV
System Capabilities Supported
System Capabilities Enabled

ブリッジ
ブリッジ

管理アドレス TLV
管理アドレス サブタイプ
インターフェース番号 サブタイプ
インターフェース番号
Object Identifier

IPv4 / all-802
unknown
0
0

LLDP Port Information

ローカルポート	ポートID サブタイプ	ポートID	ポート説明
1	ローカル割り当て	1	
2	ローカル割り当て	2	
3	ローカル割り当て	3	
4	ローカル割り当て	4	
5	ローカル割り当て	5	
6	ローカル割り当て	6	
7	ローカル割り当て	7	
8	ローカル割り当て	8	
9	ローカル割り当て	9	
10	ローカル割り当て	10	

■ Basic TLV

項目	内容
Chassis ID TLV	ローカルスイッチのシャーシ ID です。 シャーシ ID は、シャーシ ID サブタイプによって識別されます。
	Chassis ID Subtype 本製品のシャーシを識別する方法が表示されます。
	Chassis ID ローカルスイッチのシャーシ ID が表示されます。
System Capabilities TLV	サポートされているシステム機能と有効になっているシステム機能が表示されます。
System Name TLV	本製品のホスト名が表示されます。
System Description TLV	本製品のファームウェアバージョンが表示されます。

項目	内容
管理アドレス TLV	ローカル LLDP エージェントに関連するアドレスを識別します。 この TLV には、この管理アドレスに関連するシステムインタフェース番号とオブジェクト識別子 (OID) も含まれます。

■ LLDP Port Information

項目	内容
ローカルポート	リモート機器から LLDPDU を受信する本製品のポート番号です。 ポート番号をクリックすると、LLDP Local Port Status Detail 画面が表示されます。(89 ページ)
ポート ID サブタイプ	ポート ID フィールドの識別方法が表示されます。
ポート ID	この LLDPDU が送信されたポートの識別子を含む英数字の文字列が表示されます。
ポート説明	本製品がこのポートからアドバタイズするポートの説明を示します。

■ LLDP Local Port Status Detail 画面

The screenshot shows the ELECOM web interface for LLDP Local Port Status Details. The breadcrumb trail is: ポート > LLDP > LLDP ローカルステータス > LLDP Local Port Status Details. The page is for Local Port 1. The Basic TLV section shows Port ID TLV with Port ID Subtype as 'Local Port' and Port ID as '1', and Port Description TLV with description 'Port Description'. The 802.1 TLV section shows Port VLAN ID TLV with Port VLAN ID as '1'. The 802.3 TLV section shows MAC PHY Configuration & Status TLV with fields like AN Supported, AN Enabled, AN Advertised Capability, and Oper MAU Type, and Link Aggregation TLV with fields like Aggregation Capability, Aggregation Status, and Aggregated Port ID. The Max Frame Size TLV shows a Max Frame Size of 1518.

項目	内容
ローカルポート	本製品のポート番号が表示されます。

● Basic TLV

項目	内容
ポート ID TLV	LLDP フレームを送信した特定のポートを識別します。
Port Description TLV	ローカルポートの説明が表示されます。
Port VLAN ID TLV	IEEE 802.1 Port VLAN ID TLV によって送信される VLAN ID が表示されます。

● 802.1 TLV

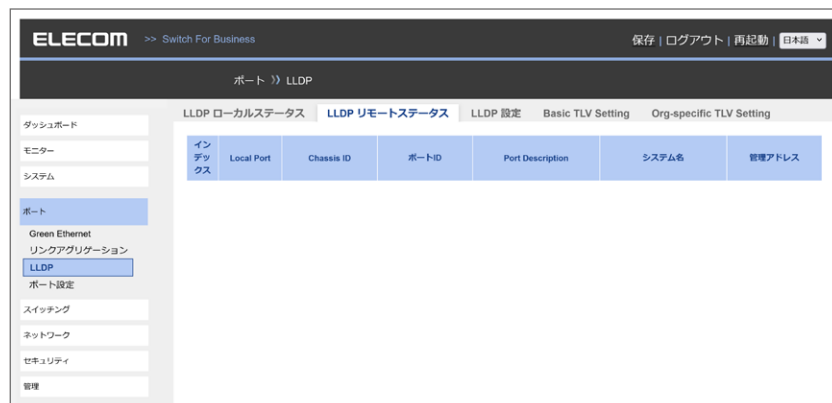
項目	内容
Port VLAN ID TLV	IEEE 802.1 Port VLAN ID TLV によって送信される VLAN ID が表示されます。

● 802.3 TLV

項目	内容	
MAC PHY Configuration & Status TLV	送信側 802.3 ノードのビットレートとデュプレックス能力をアダプタイズします。また、送信ノードの現在のデュプレックスとビットレートをアダプタイズします。最後に、これらの設定がリンク開始時のオートネゴシエーションの結果であるか、手動オーバーライドの結果であるかをアダプタイズします。	
	AN Supported	ポートがオートネゴシエーションをサポートしているかどうかが表示されます。
	AN Enabled	ポートの現在のオートネゴシエーションステータスが表示されます。
	AN Advertised Capability	ポートの自動ネゴシエーション能力が表示されます。
	Oper MAU Type	ポートの現在の MAU (Medium Attachment Unit) タイプが表示されます。
リンクアグリゲーション TLV	リンクアグリゲーション可能かどうか、リンクが現在アグリゲーション中かどうか、アグリゲーション中の場合はアグリゲーションのポート識別が表示されます。	
	Aggregation Capability	ポートの現在のアグリゲーション能力が表示されます。
	Aggregation Status	ポートの現在のアグリゲーションステータスが表示されます。
	Aggregated Port ID	現在のポートのアグリゲーション ID が表示されます。
Max Frame Size TLV	サポートされる最大フレームサイズがオクテット単位で表示されます。	

LLDPリモートステータス

隣接するスイッチングハブとのLLDP 接続ごとにLLDP ステータスの状態が表示されます。



項目	内容
インデックス	本製品に接続されているリモート機器の台数を示しています。 インデックス番号をクリックすると、「LLDP リモートポートステータス詳細」画面が表示されます。(92 ページ)
Local Port	リモート機器から LLDPDU を受信した本製品のポート番号です。
Chassis ID	送信元の LLDP エージェントに関連付けられたリモート機器のシャーシ ID が表示されます。 シャーシ ID は、リモート デバイスの MAC アドレスなど、シャーシ ID サブタイプによって識別されます。
ポート ID	この LLDPDU が送信されたポートの固有識別子を含む英数字の文字列です。 ポート ID はポート ID サブタイプによって識別されます。
Port Description	この LLDPDU が送信されたポートの説明が表示されます。
システム名	リモートデバイスのシステム名が表示されます。
管理アドレス	リモートデバイスの管理アドレスが表示されます。 IP アドレスのハイパーリンクはクリックすることができます。

■ LLDPリモートポートステータス詳細画面

リモート機器のLLDPステータスの詳細が表示されます。

ELECOM

>> Switch For Business

保存 | ログアウト | 再起動 | 目次

ポート >> LLDP

LLDP ローカルステータスLLDP リモートステータスLLDP 設定Basic TLV SettingOrg-specific TLV Setting

LLDP リモートステータス > LLDP Remote Port Status Details

ローカルポート: 1

Basic TLV

Chassis ID TLV	ポート ID TLV
Chassis ID SubtypeMACアドレス	ポート ID サブタイプMACアドレス
Chassis IDCC:30 80 32 C5 CF	ポート IDCC:30 80 32 C5 CF
Time To Live TLV	Port Description TLV
Time To Live3601	Port Description
システム名 TLV	System Description TLV
システム名	System Description
	System Capabilities TLV
	System Capabilities Supported
	System Capabilities Enabled

802.1 TLV

Port VLAN ID TLV	VLAN ID TLV
Port VLAN ID	VLAN ID
	VLAN ID
Protocol Identity TLV	Port-Protocol VLAN ID TLV
Protocol ID	Port-Protocol VLAN ID
	Port-Protocol VLAN ID Supported
	Port-Protocol VLAN ID Enabled

802.3 TLV

MAC PHY Configuration & Status TLV	Max Frame Size TLV
AN SupportedYes	Max Frame Size
AN EnabledYes	
AN Advertised Capability1000baseTFD	Link Aggregation TLV
Oper MAU type0	Aggregation Capability
	Aggregation Status
	Aggregated Port ID

Power Via MDI TLV

Port Class	
MDI Supported	
MDI Enabled	
Pair Controllable	
PSE Power Pairs	
Power Class	

MED TLV

Capabilities TLV	Device Type TLV
Network PolicyNo	Device TypeEndpoint Class I
LocationNo	
Extend Power via MDI PSENo	Location Identification TLV
Extend Power via MDI PDNo	Coordinate base LCI
Inventory ManagementNo	Cable LCI
	ELIN
Extended Power via MDI TLV	Network Policy TLV
Power Type	Voice
Power Source	Voice-Signaling
Power Priority	Guest-Voice
Power Value	Guest-Voice-Signaling
	Softphone-Voice
	Video-Conferencing
	Streaming-Video
	Video-Signaling

Inventory TLV

Hardware Revision	
Software Revision	
Firmware Revision	
Model Name	
Manufacturer	
Serial Number	
Asset ID	

項目	内容
ローカルポート	リモート機器が接続されている本装置のポート番号が表示されます。

● Basic TLV

項目	内容
Chassis ID TLV	Chassis ID Subtype リモートデバイスのシャーシを識別する方法が表示されます。
	Chassis ID リモートデバイスのシャーシ ID が表示されます。 シャーシ ID は、シャーシ ID サブタイプによって識別されます
ポート ID TLV	ポート ID サブタイプ リモートデバイスのポートの識別方法が表示されます。
	ポート ID リモートデバイスのポート ID が表示されます。 ポート ID はポート ID サブタイプによって識別されます。
Time To Live TLV	LLDP フレームの TTL 倍率が表示されます。 近隣機器の機器情報は、対応する TTL が満了するとエージングされ、破棄されます。TTL 値は、TTL 倍率に LLDP フレームの送信間隔を乗じた値です。
Port Description TLV	リモートポートの説明が表示されます。
システム名 TLV	リモートデバイスのシステム名が表示されます。
System Description TLV	リモートデバイスのシステム説明が表示されます。
System Capabilities TLV	リモートデバイスでシステム機能が有効でサポートされているかどうかが表示されます。

● 802.1 TLV

項目	内容	
MAC PHY Configuration & Status TVL	MAC/PHY Configuration/Status TLV は、送信 802.3 ノードのビットレートとデュプレックス能力をアドバタイズします。 また、送信ノードの現在のデュプレックスとビットレートをアドバタイズします。 最後に、これらの設定がリンク開始時のオートネゴシエーションの結果であるか手動によるオーバーライドの結果であるかをアドバタイズします。	
	AN Supported	ポートがオートネゴシエーションをサポートしているかどうかが表示されます。
	AN Enabled	ポートの現在のオートネゴシエーションステータスが表示されます。
	AN Advertised Capability	ポートのオートネゴシエーション機能が表示されます。
	Oper MAU Type	ポートの現在の MAU (Medium Attachment Unit) タイプが表示されます。
Max Frame Size TLV	サポートされる最大フレームサイズ（オクテット単位）が表示されます。	
Link Aggregation TLV	リンクアグリゲーション TLV は、リンクがアグリゲーション可能かどうか、リンクが現在アグリゲーション中かどうか、アグリゲーション中の場合はアグリゲーションのポート識別が表示されます。	
	Aggregation Capability	ポートの現在のアグリゲーション能力が表示されます。
	Aggregation Status	ポートの現在のアグリゲーションステータスが表示されます。
	Aggregation Port ID	現在のポートのアグリゲーション ID が表示されます。
Power Via MDI TLV	ネットワーク管理がリモートデバイス上の送信ポートの MDI 電源サポート機能をアドバタイズし、発見することを可能にします。	

● MED TLV

LLDP Media Endpoint Discovery (MED) は、LLDP の拡張機能で、メディアエンドポイントデバイスをサポートするための追加機能を提供します。MED は、ネットワークポリシーのアドバタイズとディスカバリ、ロケーション データベースを作成するためのデバイスのロケーションディスカバリ、トラブルシューティングのための情報を提供します。

項目	内容
Capabilities TLV	リモートポートがサポートする MED 機能が表示されます。
Device Type TLV	LLDP-MED デバイスクラスが表示されます。

項目	内容	
Location Identification TLV	発呼側の位置情報が表示されます。	
	Coordinate-base LCI	位置構成情報（LCI）の緯度と経度の座標が表示されます。
	Civic LCI	IETF Geopriv Civic Address ベースの位置構成情報が表示されます。
	ELIN	緊急ロケーション識別子番号が表示されます。
Extended Power via MDI TLV	IP 電話やスイッチなどのネットワーク接続デバイスなどのメディア・エンドポイントによって、詳細な電力情報がアダプタイズされることを可能にします。	
	Power Type	現在一次電源で動作しているか、バックアップ電源で動作しているか（バックアップ電源は、エンドポイントデバイスに省電力モードに移行すべきことを示す場合がある）が表示されます。
	Power Source	エンドポイントが現在、外部電源で動作しているかどうかが表示されます。
	Power Priority	エンドポイント・デバイスの電力優先度が表示されます。（ネットワーク接続デバイスは、電力不足時にどのデバイスがサービスを維持するかを優先するために使用場合があります）
	Power Value	現在の構成における電力要件（ワット単位）が表示されます。
Network Policy TLV	指定されたアプリケーションのネットワークポリシーが表示されます。	
Inventory TLV	IP 電話の大半は SNMP などの管理プロトコルをサポートしていないため、LLDP-MED インベントリ TLV を使用してインベントリ情報を本装置などのネットワーク接続機器に提供します。 インベントリ TLV には、以下の情報が含まれます。 <ul style="list-style-type: none">・ハードウェアのリビジョン・ソフトウェアのリビジョン・ファームウェアのリビジョン・モデル名・製造元・シリアル番号・アセット ID	

LLDP 設定

本製品のグローバル LLDP 設定をします。

ELECOM >> Switch For Business 保存 | ログアウト | 再起動 | 日本語

ポート >> LLDP

LLDP ローカルステータス LLDP リモートステータス **LLDP 設定** Basic TLV Setting Org-specific TLV Setting

ダッシュボード
モニター
システム
ポート
Green Ethernet
リンクアグリゲーション
LLDP
ポート設定
スイッチング
ネットワーク
セキュリティ
管理

有効 ☒
送信間隔 30 秒
送信ホールド 4 回
送信遅延 2 秒
再初期化遅延 2 秒

適用 キャンセル

ポート	Admin Status	通知
*	送受信	<input type="checkbox"/>
1	送受信	<input type="checkbox"/>
2	送受信	<input type="checkbox"/>
3	送受信	<input type="checkbox"/>
4	送受信	<input type="checkbox"/>
5	送受信	<input type="checkbox"/>
6	送受信	<input type="checkbox"/>
7	送受信	<input type="checkbox"/>
8	送受信	<input type="checkbox"/>
9	送受信	<input type="checkbox"/>
10	送受信	<input type="checkbox"/>

適用 キャンセル

項目	内容
有効	LLDP 設定の有効／無効を切り替えます。(初期値：ON)
送信間隔	LLDP パケットを送信するまでに待機する秒数を設定します。(初期値：30 秒)
送信ホールド	LLDP フレームの TTL 倍率を設定します。 近隣機器の機器情報は、対応する TTL が満了するとエージングアウトして破棄されます。TTL 値は、TTL 倍率に LLDP パケットの送信間隔を乗じた値です。 (初期値：4 回)
送信遅延	MIB の値やステータスが変化した場合に、LLDPDU を連続して送信するまでの遅延時間（秒）を設定します。(初期値：2 秒)
再初期化遅延	ポートで LLDP が初期化されるまでの待機秒数を設定します。(初期値：2 秒)
適用	変更内容を本製品のランタイムメモリに保存します。 本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。
ポート	ポート番号が表示されます。 [*] の行を変更すると、すべてのポートに変更が適用されます。

項目	内容	
Admin Status	このポートで LLDP の送受信を許可するかどうかを選択します。	
	Disable	許可しない
	Tx-Only	送信のみ
	Rx-Only	受信のみ
	Tx-Rx	送信と受信
通知	このポートで LLDP 通知を有効にするかどうかを選択します。	
適用	変更内容を本製品のランタイムメモリに保存します。 本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。	

Basic TLV Setting

基本TLVの設定をします。

ポート	管理アドレス	Port Description	System Capabilities	System Description	システム名
*	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
10	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

項目	内容
ポート	ポート番号が表示されます。 「*」の行を変更すると、すべてのポートに変更が適用されます。
管理アドレス	ポートの管理アドレス TLV の送信を有効にするか無効にするか設定します。
Port Description	ポートの説明 TLV の送信を有効にするか無効にするか設定します。
System Capabilities	ポートの System CapabilitiesTLV の送信を有効にするか無効にするか設定します。
System Description	ポートのシステム説明 TLV の送信を有効にするか無効にするか設定します。
システム名	ポート上のシステム名 TLV の送信を有効にするか無効にするか設定します。
適用	変更内容を本製品のランタイムメモリに保存します。 本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。

Org-specific TLV Setting

組織固有の TLV 設定を構成します。

項目	内容						
ポート	ポート番号が表示されます。 「*」の行を変更すると、すべてのポートに変更が適用されます。						
802.1 TLV	<table border="1"> <tr> <td>Port VLAN ID</td><td>ポート上の IEEE 802.1 Port VLAN ID TLV の送信を有効にするか無効にするか設定します。 この欄のチェックボックスはすべてデフォルトで有効になっています。</td></tr> </table>	Port VLAN ID	ポート上の IEEE 802.1 Port VLAN ID TLV の送信を有効にするか無効にするか設定します。 この欄のチェックボックスはすべてデフォルトで有効になっています。				
Port VLAN ID	ポート上の IEEE 802.1 Port VLAN ID TLV の送信を有効にするか無効にするか設定します。 この欄のチェックボックスはすべてデフォルトで有効になっています。						
802.3 TLV	<table border="1"> <tr> <td>リンクアグリゲーション</td><td>ポート上の IEEE 802.3 Link Aggregation TLV の送信を有効にするか無効にするか設定します。</td></tr> <tr> <td>MAC/PHY</td><td>ポート上の IEEE 802.3 MAC/PHY Configuration/Status TLV の送信を有効にするか無効にするか設定します。 この欄のチェックボックスはすべてデフォルトで有効になっています。</td></tr> <tr> <td>Max Frame Size</td><td>ポート上の IEEE 802.3 Max Frame Size TLV の送信を有効にするか無効にするか設定します。</td></tr> </table>	リンクアグリゲーション	ポート上の IEEE 802.3 Link Aggregation TLV の送信を有効にするか無効にするか設定します。	MAC/PHY	ポート上の IEEE 802.3 MAC/PHY Configuration/Status TLV の送信を有効にするか無効にするか設定します。 この欄のチェックボックスはすべてデフォルトで有効になっています。	Max Frame Size	ポート上の IEEE 802.3 Max Frame Size TLV の送信を有効にするか無効にするか設定します。
リンクアグリゲーション	ポート上の IEEE 802.3 Link Aggregation TLV の送信を有効にするか無効にするか設定します。						
MAC/PHY	ポート上の IEEE 802.3 MAC/PHY Configuration/Status TLV の送信を有効にするか無効にするか設定します。 この欄のチェックボックスはすべてデフォルトで有効になっています。						
Max Frame Size	ポート上の IEEE 802.3 Max Frame Size TLV の送信を有効にするか無効にするか設定します。						
適用	変更内容を本製品のランタイムメモリに保存します。 本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。						

ポート設定

スイッチのポート設定を構成します。

ELECOM >> Switch For Business

保存 | ログアウト | 再起動 | 日本語

ポート >> ポート設定

ダッシュボード

モニター

システム

ポート

Green Ethernet

リンクアグリゲーション

LLDP

ポート設定

スイッチング

ネットワーク

セキュリティ

管理

ポート設定

ポート	有効	名前	速度/流媒体方式	フローコントロール	802.1pプライオリティ	BPDU制御	メディアタイプ
*	<input type="checkbox"/>		自動	無効	0	ピア	SFP
1	<input checked="" type="checkbox"/>		自動	無効	0	ピア	-
2	<input checked="" type="checkbox"/>		自動	無効	0	ピア	-
3	<input checked="" type="checkbox"/>		自動	無効	0	ピア	-
4	<input checked="" type="checkbox"/>		自動	無効	0	ピア	-
5	<input checked="" type="checkbox"/>		自動	無効	0	ピア	-
6	<input checked="" type="checkbox"/>		自動	無効	0	ピア	-
7	<input checked="" type="checkbox"/>		自動	無効	0	ピア	-
8	<input checked="" type="checkbox"/>		自動	無効	0	ピア	-
9	<input checked="" type="checkbox"/>		自動	無効	0	ピア	SFP
10	<input checked="" type="checkbox"/>		自動	無効	0	ピア	SFP

適用 キャンセル

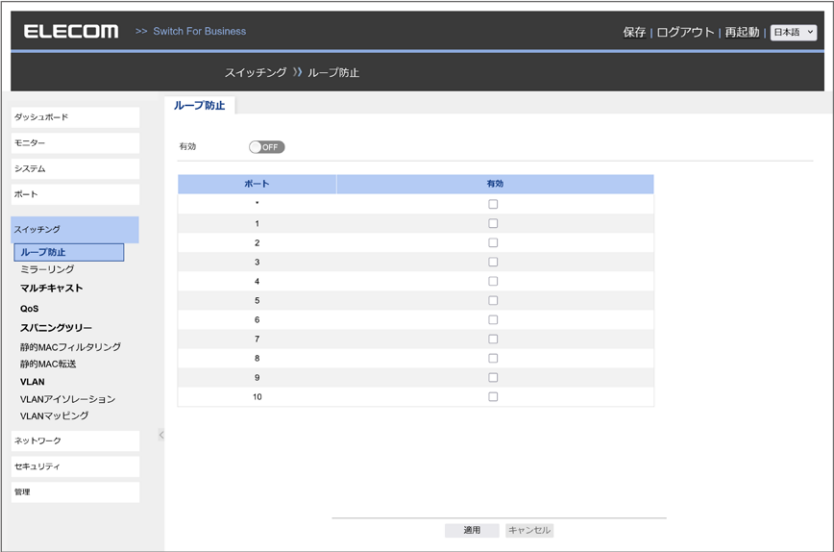
項目	内容
ポート	ポート番号が表示されます。 「*」の行を変更すると、すべてのポートに変更が適用されます。
有効	ポートの有効／無効を切り替えます。すべてのポートの工場出荷時のデフォルトは有効です。データ転送を行うには、ポートを有効にする必要があります。
名前	このポートを識別する説明的な名前を入力します。 (最大 128 文字まで。? (クエスチョンマーク) (パイプ) ' (クォーテーション) " (ダブルクォーテーション) は使用不可) スペースの制限により、設定画面ではポート名が切り捨てられることがあります。

項目	内容								
速度／通信方式	<p>このポートのイーサネット接続の速度とデュプレックスモードを以下から選択します。</p> <p>(自動、自動 -1G、自動 -100M、100M / 全二重、1G / 全二重、2.5G / 全二重、5G / 全二重、10G / 全二重 (ギガビット接続のみ)) (初期値：自動)</p> <p>「自動 -1G」または「自動」を選択すると、1つのポートがピアポートと自動的にネゴシエーションし、両端がサポートする接続速度とデュプレックスモードを取得します。</p> <p>※ 10Gbps/5Gbps は、EHB-SX シリーズのみ対応。</p> <p>オートネゴシエーションがオンの場合</p> <p>本製品のポートは相手ポートと自動的にネゴシエーションを行い、接続速度とデュプレックスモードを決定します。相手ポートがオートネゴシエーションをサポートしていないか、この機能をオフにしている場合、本製品はケーブルの信号を検出して半二重モードを使用して接続速度を決定します。</p> <p>オートネゴシエーションがオフの場合</p> <p>ポートは接続時にあらかじめ設定された速度とデュプレックスモードを使用するため、接続するには相手ポートの設定が同じであることを確認する必要があります。</p>								
フローコントロール	<p>フロー制御の方法を選択します。(初期値：無効)</p> <p>ポートにトラフィックが集中すると、ポートの帯域幅が低下し、バッファメモリがオーバーフローしてパケットの破棄やフレームロスが発生します。</p> <p>フロー制御は、受信ポートの帯域幅に合わせて信号の送信を調整するために使用されます。</p> <p>本製品は、全二重モードでは IEEE 802.3x フロー制御を使用し、半二重モードでは背圧フロー制御を使用します。</p> <p>IEEE 802.3x フロー制御は、全二重モードで使用され、送信ポートに一時停止信号を送信し、受信ポートのメモリバッファがいっぱいになると、一時的に信号の送信を停止させます。</p> <p>バックプレッシャーフロー制御は、通常、半二重モードで使用され、送信ポートに「衝突」信号を送信し (パケット衝突の状態を模倣)、送信ポートに信号の送信を一時的に停止させ、後で再送信させます。</p> <table border="1"> <tr> <td>無効</td><td>フロー制御しません。</td></tr> <tr> <td>送受信</td><td>本製品のポートから接続機器にポーズ信号が送信され、接続機器から本製品にポーズ信号が送信されます。本製品はポーズ信号を受信すると、信号の送信を一時的に停止します。</td></tr> <tr> <td>送信</td><td>本製品のポートから接続機器へポーズ信号が送信されます。</td></tr> <tr> <td>受信</td><td>接続機器から本製品にポーズ信号が送信されます。本製品は一時的に信号の送信を停止します。</td></tr> </table>	無効	フロー制御しません。	送受信	本製品のポートから接続機器にポーズ信号が送信され、接続機器から本製品にポーズ信号が送信されます。本製品はポーズ信号を受信すると、信号の送信を一時的に停止します。	送信	本製品のポートから接続機器へポーズ信号が送信されます。	受信	接続機器から本製品にポーズ信号が送信されます。本製品は一時的に信号の送信を停止します。
無効	フロー制御しません。								
送受信	本製品のポートから接続機器にポーズ信号が送信され、接続機器から本製品にポーズ信号が送信されます。本製品はポーズ信号を受信すると、信号の送信を一時的に停止します。								
送信	本製品のポートから接続機器へポーズ信号が送信されます。								
受信	接続機器から本製品にポーズ信号が送信されます。本製品は一時的に信号の送信を停止します。								
802.1p プライオリティ	<p>このプライオリティ値は、(802.1p) タグのない受信フレームに追加されます。</p>								

項目	内容	
BPDU 制御	このポートで受信した BPDU (Bridge Protocol Data Units) の処理方法を設定します。(初期値：ピア) 設定の前に「システム」－「スイッチ設定」(74 ページ) で「ブリッジプロトコル透過」を「有効」に設定する必要があります。	
	ピア	このポートで受信したすべての BPDU を処理します。
	トンネル	このポートで受信した BPDU を転送します。
	破棄	このポートで受信した BPDU を廃棄します。
	ネットワーク	VLAN タグのない BPDU を処理し、タグ付き BPDU を転送します。
メディアタイプ	10 ギガビット・インタフェースに接続する SFP+ モジュールのメディア・タイプ (SFP+ または DAC10G) を選択します。(初期値：SFP)	
適用	変更内容を本製品のランタイムメモリに保存します。 本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。	

ループ防止

ポートごとにループ防止機能の設定をします。



項目	内容
有効	「ON」にすると、本製品でループ防止が有効になります。 本製品は、ループ防止機能によりポートをシャットダウンした場合、syslog、内部ログメッセージ、SNMPトラップを生成します。
ポート	ポート番号が表示されます。 「*」の行を変更すると、すべてのポートに変更が適用されます。
有効	このポートのループ防止機能を有効にする場合にチェックを入れます。 本製品は、本ポートからプロンプトパケットを送信し、接続先の本製品がループ状態にあるかどうかを確認します。本ポートが接続されている本製品がループ状態の場合、本製品は本ポートをシャットダウンします。
適用	変更内容を本製品のランタイムメモリに保存します。 本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。

ミラーリング

ポートミラーリング機能の設定をします。

ポートミラーリングを使用すると、トラフィックフローをモニターポート（トラフィックをコピーしたポート）にコピーして、干渉を受けずにモニターポートからのトラフィックを調べることができます。

ELECOM >> Switch For Business

保存 | ログアウト | 再起動 | 日本語

スイッチング >> ミラーリング

ダッシュボード

モニター

システム

ポート

スイッチング

ループ防止

ミラーリング

マルチキャスト

QoS

スパンニングツリー

静的MACフィルタリング

静的MAC転送

VLAN

VLANアイソレーション

VLANマッピング

ネットワーク

セキュリティ

管理

ミラーリング

有効 ☐ OFF

モニターポート

ポート	ミラー有効	データ方向
*	<input type="checkbox"/>	入力ポート
1	<input type="checkbox"/>	入力ポート
2	<input type="checkbox"/>	入力ポート
3	<input type="checkbox"/>	入力ポート
4	<input type="checkbox"/>	入力ポート
5	<input type="checkbox"/>	入力ポート
6	<input type="checkbox"/>	入力ポート
7	<input type="checkbox"/>	入力ポート
8	<input type="checkbox"/>	入力ポート
9	<input type="checkbox"/>	入力ポート
10	<input type="checkbox"/>	入力ポート

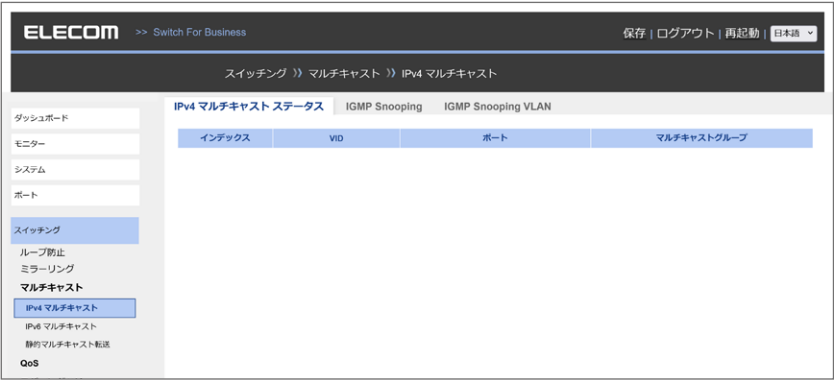
適用 キャンセル

項目	内容
有効	「ON」にすると、本製品でポートミラーリングが有効になります。
モニターポート	<p>モニタポートのポート番号を入力します。</p> <p>モニタポートは、元のポートのトラフィックフローを妨げることなく、トラフィックをより詳細に調べるために、トラフィックをコピーするポートです。</p>
ポート	<p>ポート番号が表示されます。</p> <p>「*」の行を変更すると、すべてのポートに変更が適用されます。</p>
ミラー有効	チェックすると、ポートのトラフィックをミラーリングします。
データ方向	<p>ミラーリングするトラフィックの方向を選択します。</p> <p>(入力ポート／出力ポート／入出力ポート) (初期値：入力ポート)</p>
適用	<p>変更内容を本製品のランタイムメモリに保存します。</p> <p>本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。</p>

【マルチキャスト】IPv4 マルチキャスト

IPv4 マルチキャストステータス

IPv6 マルチキャストグループ情報が表示されます。



項目	内容
インデックス	エントリーのインデックス番号が表示されます。
VID	マルチキャスト VLAN ID が表示されます。
ポート	マルチキャストグループに属するポート番号が表示されます。
マルチキャストグループ	IP マルチキャストグループアドレスが表示されます。

IGMP snooping

グループマルチキャストトラフィックをそのグループのメンバーであるポートにのみ転送します。

ELECOM >> Switch For Business

保存 | ログアウト | 再起動 | 日本語

スイッチング >> マルチキャスト >> IPv4 マルチキャスト

IPv4 マルチキャストステータスIGMP SnoopingIGMP Snooping VLAN

ダッシュボード
モニター
システム
ポート
スイッチング
ループ防止
ミラーリング
マルチキャスト
IPv4 マルチキャスト
IPv6 マルチキャスト
静的マルチキャスト転送
QoS
スパンニングツリー
静的MACフィルタリング
静的MAC転送
VLAN
VLANアイソレーション
VLANマッピング
ネットワーク
セキュリティ
管理

有効
クエリア
Report Proxy
Host Timeout
802.1pプライオリティ
不明なマルチキャストフレーム
予約済 マルチキャストグループ

ON

☐

☒

260

秒

変更なし

フラッディング

フラッディング

☐ 破壊

☐ 破壊

ポート	Normal Leave	Fast Leave	IGMP クエリアモード
*	<input checked="" type="radio"/>	<input type="radio"/>	Auto
1	<input checked="" type="radio"/>	<input type="radio"/>	Auto
2	<input checked="" type="radio"/>	<input type="radio"/>	Auto
3	<input checked="" type="radio"/>	<input type="radio"/>	Auto
4	<input checked="" type="radio"/>	<input type="radio"/>	Auto
5	<input checked="" type="radio"/>	<input type="radio"/>	Auto
6	<input checked="" type="radio"/>	<input type="radio"/>	Auto
7	<input checked="" type="radio"/>	<input type="radio"/>	Auto
8	<input checked="" type="radio"/>	<input type="radio"/>	Auto
9	<input checked="" type="radio"/>	<input type="radio"/>	Auto
10	<input checked="" type="radio"/>	<input type="radio"/>	Auto

適用

キャンセル

項目	内容
有効	「ON」にすると、本製品で IGMP snooping が有効になります。(初期値：OFF)
クエリア	マルチキャストホストが接続されているVLANに対して IGMP General Queryメッセージを送信する場合に選択します。(初期値：無効)

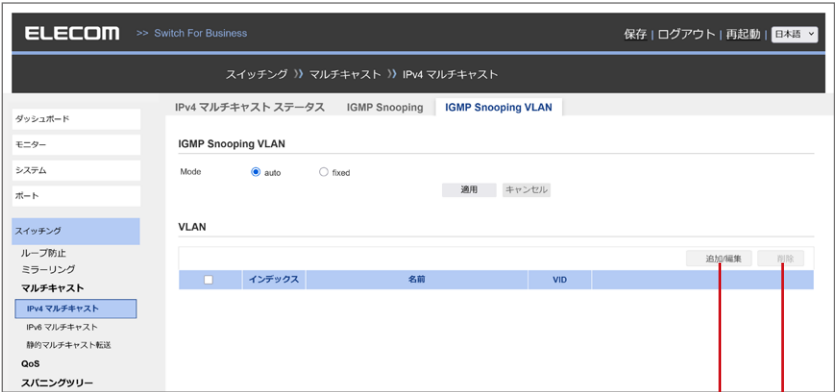
106

項目	内容				
Report Proxy	<p>本製品を IGMP レポートプロキシおよびリーブプロキシとして動作させる場合に選択します。選択すると、接続されているマルチキャストルータにグループの変更を報告します。(初期値:有効)</p> <p>本製品はマルチキャストルータまたはスイッチとマルチキャストホスト間の IGMP パケットをチェックしてマルチキャストグループメンバーシップを知るだけでなく、IGMP v1/v2 レポートの送信元 MAC アドレスを自身の MAC アドレスに置き換えてからマルチキャストルータまたはスイッチに転送します。</p> <p>本製品は、同じマルチキャストグループへの参加を要求する複数の IGMP v1/v2 ジョインレポートを受信した場合、自分の MAC アドレスを持つ新しいジョインレポートだけを送信します。これにより、マルチキャストルータまたはスイッチに渡されるマルチキャスト参加レポートの数を減らすことができます。</p> <p>本製品は、マルチキャストグループの最後のホストからリーブメッセージを受信したときだけ、マルチキャストルータまたはスイッチに MAC アドレス付きのリーブメッセージを送信します。</p>				
Host Timeout	<p>本製品がポートから報告メッセージを受信しない場合に、IGMP グループメンバーシップエントリを削除するまでの時間 (1 ~ 16711450) を秒単位で指定します。(初期値: 260 秒)</p>				
802.1p プライオリティ	<p>本製品が送信する IGMP コントロールパケットの優先度を変更する優先度レベル (0 ~ 7) を選択します。</p> <p>それ以外の場合は、「変更なし」を選択してプライオリティを変更しません。(初期値: 変更なし)</p>				
不明なマルチキャストフレーム	<p>本製品が不明なマルチキャストフレームを受信したときの動作を設定します。(初期値:フラッディング)</p> <table border="1"> <tr> <td>フラッディング</td><td>すべてのポートにフレームを送信します。</td></tr> <tr> <td>破棄</td><td>フレームを廃棄します。</td></tr> </table>	フラッディング	すべてのポートにフレームを送信します。	破棄	フレームを廃棄します。
フラッディング	すべてのポートにフレームを送信します。				
破棄	フレームを廃棄します。				
予約済マルチキャストグループ	<p>本製品が予約マルチキャストアドレスを持つフレームを受信したときの動作を指定します。(初期値:フラッディング)</p> <table border="1"> <tr> <td>フラッディング</td><td>すべてのポートにフレームを送信します。</td></tr> <tr> <td>破棄</td><td>フレームを廃棄します。</td></tr> </table>	フラッディング	すべてのポートにフレームを送信します。	破棄	フレームを廃棄します。
フラッディング	すべてのポートにフレームを送信します。				
破棄	フレームを廃棄します。				
ポート	<p>ポート番号が表示されます。</p> <p>「*」の行を変更すると、すべてのポートに変更が適用されます。</p>				

項目	内容	
Normal Leave	<p>本製品がこのタイムアウトを使用してポートのフォワーディングテーブルを更新する場合に選択します。(初期値：無効)</p> <p>Normal Leave モードでは、本製品があるポートでホストから IGMP leave メッセージを受信した場合、マルチキャストルータが IGMP Group-Specific Query (GSQ) メッセージを送信してから IGMP レポートを待ち、ポートに接続されている他のホストが特定のマルチキャストグループに残るかどうかを判断します。</p> <p>このポートでホストから IGMP leave メッセージを受信した場合、本製品が IGMP snooping のメンバシップエントリを削除するまでに IGMP レポートを何秒待つかを定義します。</p>	
Fast Leave	<p>本製品がこのタイムアウトを使用してポートのフォワーディングテーブルを更新するときに選択します。(初期値：有効)</p> <p>Fast Leave モードでは、ポート上のホストから IGMP リーブメッセージを受信した直後に、本製品は IGMP Group-Specific Query (GSQ) メッセージを送信し、ポートに接続されている他のホストが特定のマルチキャストグループに留まるべきかどうかを判断します。これにより、離脱処理を高速化することができます。</p>	
IGMP クエリアモード	<p>本製品は IGMP クエリポートを IGMP マルチキャストルータ（またはサーバ）に接続されているものとして扱います。</p> <p>本製品は IGMP join または leave パケットを IGMP クエリポートに転送します。</p>	
	Auto (初期値)	ポートが IGMP クエリパケットを受信した場合、IGMP クエリポートとして使用します。
	Fixed	本製品がポートを常に IGMP クエリポートとして使用します。ポートに IGMP マルチキャストサーバを接続する場合に選択します。
	Edge	ポートを IGMP クエリポートとして使用しないようにするときに選択します。本製品はこのポートに IGMP ルータを接続した記録を残しません。また、IGMP の参加パケットおよび離脱パケットをこのポートに転送しません。

IGMP snooping VLAN

VLANでIGMP snoopingを実行します。



IGMP snooping VLANを追加したり、選択したIGMP snooping VLANを編集します。

→ [110ページ](#)

選択したIGMP snooping VLANを削除します。

■ IGMP snooping VLAN

項目	内容				
Mode	本製品は最大 16 個の VLAN（MVR 画面で設定した最大 5 個の VLAN を含む）を学習できます。 例えば、MVR 画面でマルチキャスト VLAN を 1 つ設定した場合、本画面で指定できる VLAN は 15 個までです。 本製品はこの 16 個の VLAN に属さない IGMP 制御メッセージをドロップします。 設定の前に「スイッチング」－「マルチキャスト」－「IPv4 マルチキャスト」－「IGMP snooping」 (106 ページ) で「IGMP snooping」を「有効」に設定する必要があります。				
	<table><tr><td>auto (初期値)</td><td>本製品が任意の VLAN のマルチキャストグループメンバーシップ情報を自動的に学習します。</td></tr><tr><td>fixed</td><td>以下で指定した VLAN のマルチキャストグループメンバーシップ情報のみを学習します。</td></tr></table>	auto (初期値)	本製品が任意の VLAN のマルチキャストグループメンバーシップ情報を自動的に学習します。	fixed	以下で指定した VLAN のマルチキャストグループメンバーシップ情報のみを学習します。
	auto (初期値)	本製品が任意の VLAN のマルチキャストグループメンバーシップ情報を自動的に学習します。			
fixed	以下で指定した VLAN のマルチキャストグループメンバーシップ情報のみを学習します。				
適用	変更内容を本製品のランタイムメモリに保存します。 本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。				

■ VLAN

項目	内容
インデックス	テーブル内の IGMP snooping VLAN エントリの番号が表示されます。
名前	この VLAN グループの説明的な名前が表示されます。
VID	VLAN グループの ID 番号です。

■ IGMP snooping VLAN の追加／編集

名前

VID

適用

クリア

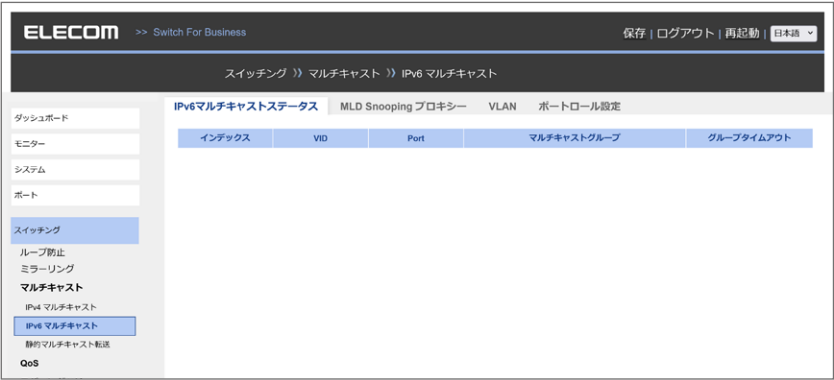
キャンセル

項目	内容
名前	識別のために VLAN の説明的な名前を入力します。 (最大 32 文字まで。? (クエスチョンマーク) (パイプ) ' (クォーテーション) " (ダブルクォーテーション) , (コンマ) は使用不可)
VID	スタティック VLAN の ID を入力します。有効範囲は 1 ～ 4094 です。
適用	変更内容を本製品のランタイムメモリに保存します。 本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。
クリア	フィールドが工場出荷時のデフォルトにクリアされます。

【マルチキャスト】IPv6 マルチキャスト

IPv6 マルチキャストステータス

IPv6 マルチキャストグループ情報が表示されます。



項目	内容
インデックス	エントリーのインデックス番号が表示されます。
VID	マルチキャスト VLAN ID が表示されます。
Port	マルチキャストグループに属するポート番号が表示されます。
マルチキャストグループ	IP マルチキャストグループアドレスが表示されます。
グループタイムアウト	ポートからレポートメッセージを受信しない場合に、本製品が MLD グループメンバーシップエントリを削除するまでの経過時間（秒）が表示されます。

MLD snooping プロキシ

MLD snooping-proxy を設定します。



項目	内容
有効	MLD snooping-proxy の有効／無効を切り替えます。(初期値：無効)
802.1p 優先	MLD メッセージの優先度 (0-7) を選択します。(初期値：0)
適用	変更内容を本製品のランタイムメモリに保存します。 本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。

VLAN

MLD snooping プロキシ VLAN を設定します。



MLD snooping プロキシ VLANを追加したり、選択した
MLD snooping プロキシ VLANを編集します。

→ [114ページ](#)

選択したMLD snooping プロキシ VLANを削除します。

項目	内容
インデックス	MLD snooping プロキシ VLAN エントリのインデックス番号が表示されます。
VID	VLAN グループの ID 番号が表示されます。

■ MLD snooping プロキシ VLAN の追加／編集

VID	<input type="text"/>
アップストリーム	
クエリ間隔	<input type="text" value="125000"/> ミリ秒
最大応答遅延	<input type="text" value="10000"/> ミリ秒
Robustness Variable	<input type="text" value="2"/>
最終メンバークエリ間隔	<input type="text" value="1000"/> ミリ秒
ダウンストリーム	
クエリ間隔	<input type="text" value="125000"/> ミリ秒
最大応答遅延	<input type="text" value="10000"/> ミリ秒
<input type="button" value="適用"/> <input type="button" value="クリア"/> <input type="button" value="キャンセル"/>	

項目	内容				
VID	VLAN の ID 番号を入力します。				
アップストリーム	<p>この値は、接続されているマルチキャストルータで設定されている値とまったく同じにする必要があります。</p> <p>この値は、MLD snooping のメンバシップエントリ（アップストリームポートでのみ学習）がフォワーディングテーブルに残る時間を計算するために使用されます。</p> <table> <tr> <td>クエリ間隔</td><td> アップストリームポートに接続されているルーターから送信される一般的なクエリメッセージ間の時間（ミリ秒）を入力します。 （初期値：12500 ミリ秒） MLD Report メッセージを受信すると、本製品はエントリのタイムアウト時間を $T = (QI \times RV) + MRD^*$ に設定します。 </td></tr> <tr> <td>最大応答遅延</td><td> アップストリームポートに接続されているルーターが、MLD 一般クエリメッセージに対する応答を待機する時間（ミリ秒）を入力します。（初期値：10000 ミリ秒） MLD Report メッセージを受信した場合、本製品エントリのタイムアウト時間を $T = (QI \times RV) + MRD^*$ に設定します。 MLD Done メッセージを受信すると、本製品はエントリの有効期間を Last Member Query Interval と Robustness Variable の積に設定します。 </td></tr> </table> <p>※ T = Timeout、QI = Query Interval、RV = Robustness Variable、MRD = Maximum Response Delay</p>	クエリ間隔	アップストリームポートに接続されているルーターから送信される一般的なクエリメッセージ間の時間（ミリ秒）を入力します。 （初期値：12500 ミリ秒） MLD Report メッセージを受信すると、本製品はエントリのタイムアウト時間を $T = (QI \times RV) + MRD^*$ に設定します。	最大応答遅延	アップストリームポートに接続されているルーターが、MLD 一般クエリメッセージに対する応答を待機する時間（ミリ秒）を入力します。（初期値：10000 ミリ秒） MLD Report メッセージを受信した場合、本製品エントリのタイムアウト時間を $T = (QI \times RV) + MRD^*$ に設定します。 MLD Done メッセージを受信すると、本製品はエントリの有効期間を Last Member Query Interval と Robustness Variable の積に設定します。
クエリ間隔	アップストリームポートに接続されているルーターから送信される一般的なクエリメッセージ間の時間（ミリ秒）を入力します。 （初期値：12500 ミリ秒） MLD Report メッセージを受信すると、本製品はエントリのタイムアウト時間を $T = (QI \times RV) + MRD^*$ に設定します。				
最大応答遅延	アップストリームポートに接続されているルーターが、MLD 一般クエリメッセージに対する応答を待機する時間（ミリ秒）を入力します。（初期値：10000 ミリ秒） MLD Report メッセージを受信した場合、本製品エントリのタイムアウト時間を $T = (QI \times RV) + MRD^*$ に設定します。 MLD Done メッセージを受信すると、本製品はエントリの有効期間を Last Member Query Interval と Robustness Variable の積に設定します。				

項目	内容	
アップストリーム	Robustness Variable	クエリ回数を入力します。(初期値: 2) アップストリームポートに接続されたルータから送信されたクエリに対して、設定したクエリ数以上の応答がない場合に、マルチキャストアドレスエントリ (snooping によってアップストリームポートだけで学習したもの) をフォワーディングテーブルから削除します。
	最終メンバークエリ間隔	MLD Done メッセージを受信したときにアップストリームポートが送信する MLD グループ固有クエリー間の時間 (ミリ秒) を入力します。(初期値: 1000) MLD Done メッセージを受信すると、本製品はエントリの有効期間を Last Member Query Interval と Robustness Variable の積に設定します。
ダウンストリーム	クエリ間隔	ダウンストリームポートから送信される一般クエリメッセージ間の時間 (ミリ秒) を入力します。(初期値: 125000)
	最大応答遅延	本製品がダウンストリームポートから送信された一般クエリメッセージに対する応答を待機する最大時間 (ミリ秒) を入力します。(初期値: 10000)
適用	変更内容を本製品のランタイムメモリに保存します。 本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。	
クリア	フィールドが工場出荷時のデフォルトにクリアされます。	

ポートロール設定

ポートのMLD snooping-proxy 設定をします。

ELECOM
>> Switch For Business

保存 | ログアウト | 再起動 | 日本語

スイッチング
マルチキャスト
IPv6 マルチキャスト

IPv6 マルチキャストステータス
MLD Snooping プロキシ
VLAN
ポートロール設定

ダッシュボード
モニター
システム
ポート

スイッチング
ループ防止
ミラーリング
マルチキャスト
IPv4 マルチキャスト
IPv6 マルチキャスト
QoS
スパンニングツリー
静的MACフィルタリング
静的MAC転送
VLAN
VLANアイソレーション
VLANマッピング
ネットワーク
セキュリティ
管理

MLD Snooping プロキシ
ポートロール設定

MLD Snooping プロキシ-VLAN ID

ポート	ポートロール	Leave Mode	Leave Timeout	Fast Leave Timeout
*	なし	即時		
1	なし	即時	4300	200
2	なし	即時	4300	200
3	なし	即時	4300	200
4	なし	即時	4300	200
5	なし	即時	4300	200
6	なし	即時	4300	200
7	なし	即時	4300	200
8	なし	即時	4300	200
9	なし	即時	4300	200
10	なし	即時	4300	200

適用
キャンセル

項目	内容
MLD snooping プロキシ VLAN ID	ポートの MLD snooping-proxy 設定を行う VLAN ID を選択します。
ポート	ポート番号が表示されます。 「*」の行を変更すると、すべてのポートに変更が適用されます。
ポートロール	<p>ポートの役割を選択します。</p> <p>(なし/アップストリーム/ダウンストリーム) (初期値: なし)</p> <p>本製品のポートは、MLD のダウンストリームポートにもアップストリームポートにもなります。ダウンストリームポートは、MLD ホストに接続し、マルチキャストルータとして動作し、MLD クエリを送信し、MLD ホストの Report および Done メッセージをリッスンします。</p> <p>アップストリームポートは、マルチキャストルータに接続し、マルチキャストルータからクエリを受信するときに Report メッセージまたは Done メッセージを送信するホストとして動作します。</p> <p>その他、ポートがマルチキャストグループに参加していない、またはこの VLAN に所属していない場合は「なし」を選択します。</p>

項目	内容
Leave Mode	<p>この VLAN で指定したダウンストリームポートのリーブモードを選択します。</p> <p>本ポートでホストから MLD leave メッセージを受信した場合、MLD snooping のメンバシップエントリ（ダウンストリームポートで学習）を即座に削除するか（即時）、leave timeout 前に MLD report を待つか（通常）、leave timeout を早くするか（高速）を指定します。 (初期値：即時)</p>
Leave Timeout	<p>ダウンストリームポートのフォワーディングテーブルの更新に使用する MLD snooping normal leave timeout(ミリ秒)を入力します。(初期値: 4000 ミリ秒)</p> <p>これは、ホストから MLD Done メッセージを受信した場合、本製品が（ダウンストリームポートで学習した）MLD snooping のメンバシップエントリを削除するまでの MLD レポート待ち時間を何秒にするかを定義します。</p>
Fast Leave Timeout	<p>指定したダウンストリームポートの Fast Leave Timeout（ミリ秒）を入力します。(初期値：200 ミリ秒)</p> <p>これは、ホストからこのポートで MLD Done メッセージを受信した場合、（ダウンストリームポートで学習した）MLDsnooping メンバシップエントリを削除する前に、本製品が MLD レポートを待機する秒数を定義します。</p>
適用	<p>変更内容を本製品のランタイムメモリに保存します。</p> <p>本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。</p>

【マルチキャスト】静的マルチキャスト転送

マルチキャストストリームを受信するポートの静的マルチキャストMACアドレスを表示したり、設定します。



静的マルチキャストMACアドレスルールを追加したり、選択した静的マルチキャストMACアドレスルールを編集します。

→ [119ページ](#)

選択した静的マルチキャストMACアドレスルールを削除します。

項目	内容
インデックス	静的マルチキャスト MAC アドレスルールのインデックス番号が表示されます。
有効	静的マルチキャスト MAC アドレス転送ルールが有効になっているかが表示されます。 ルールは一時的に無効化することができます。
名前	静的マルチキャスト MAC アドレス転送ルールの識別のための記述名が表示されます。
MAC アドレス	マルチキャストグループを識別するマルチキャスト MAC アドレスが表示されます。
VID	指定したマルチキャスト MAC アドレスを含むフレームを転送する VLAN グループの ID 番号が表示されます。
ポート	指定されたマルチキャスト MAC アドレスを含むフレームを転送する特定 VLAN グループ内のポートが表示されます。

■ 静的マルチキャストMACアドレスルールの追加／編集

有効	<input type="radio"/> OFF
名前	<input type="text"/>
MACアドレス	<input type="text"/>
VID	<input type="text"/>
ポート	<input type="text"/>
<input type="button" value="適用"/> <input type="button" value="クリア"/> <input type="button" value="キャンセル"/>	

項目	内容
有効	このルールの有効／無効を切り替えます。 無効にすると、ルールを削除せずに一時的に非アクティブにすることができます。
名前	この静的マルチキャストMAC アドレス転送ルールの名前を入力します。 (最大 32 文字まで。? (クエスチョンマーク) (パイプ) ' (クォーテーション) " (ダブルクォーテーション) , (コンマ) は使用不可)
MAC アドレス	マルチキャストグループを識別するマルチキャストMAC アドレスを入力します。 マルチキャストMAC アドレスの最初のオクテットペアの最後のバイナリビットは、1 でなければなりません。 例えば、最初のオクテットペア 00000001 は 16 進数で 01 なので、01:00:5e:00:00:0A と 01:00:5e:00:00:27 が有効なマルチキャストMAC アドレスです。
VID	宛先のマルチキャストMAC アドレスが一致するフレームをVLAN グループ内のポートに転送できます。 ここにVLAN グループを識別するIDを入力します。特定のVLANを指定しない場合は、「1」を入力してください。
ポート	上記のエントリと一致した宛先マルチキャストMAC アドレスのフレームを転送するポートを入力します。 複数のポートをカンマ (,) またはハイフン (-) で区切って入力できます。 たとえば、ポート 3、4、5 には「3-5」と入力します。ポート 3、5、7 には「3,5,7」と入力します。
適用	変更内容を本製品のランタイムメモリに保存します。 本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。
クリア	フィールドが工場出荷時のデフォルトにクリアされます。

【Qos】Diffserv

Diffserv

マーキングルールまたはIEEE 802.1p プライオリティマッピングを適用します。

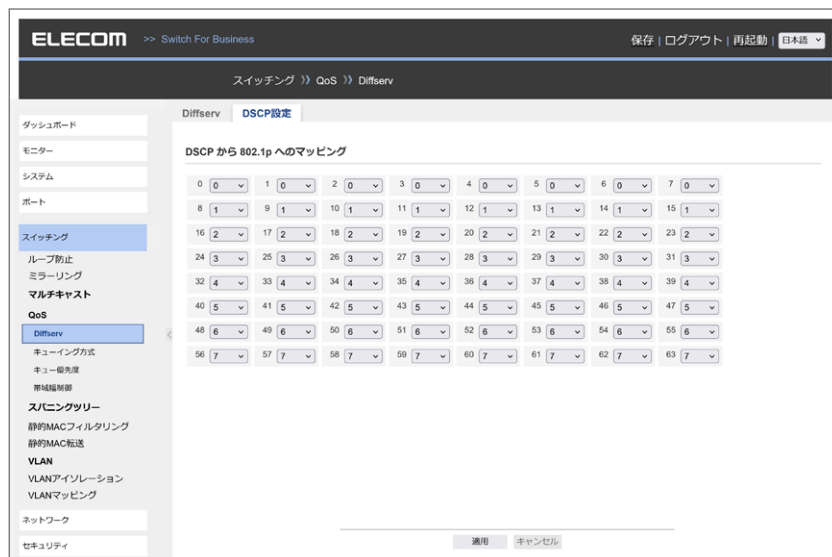
The screenshot shows the ELECOM web interface for configuring Diffserv. The breadcrumb trail is 'スイッチング >> QoS >> Diffserv'. The left sidebar has 'スイッチング' selected. The main area shows the 'Diffserv' configuration page with a 'DSCP設定' sub-tab. A toggle switch for '有効' is currently 'OFF'. Below this is a table with two columns: 'ポート' (Port) and '有効' (Enabled). The table lists ports 1 through 10, all of which are currently disabled. At the bottom of the table are buttons for '適用' (Apply) and 'キャンセル' (Cancel).

ポート	有効
*	<input type="checkbox"/>
1	<input type="checkbox"/>
2	<input type="checkbox"/>
3	<input type="checkbox"/>
4	<input type="checkbox"/>
5	<input type="checkbox"/>
6	<input type="checkbox"/>
7	<input type="checkbox"/>
8	<input type="checkbox"/>
9	<input type="checkbox"/>
10	<input type="checkbox"/>

項目	内容
有効	Diffserv 機能の有効／無効を切り替えます。
ポート	ポート番号が表示されます。 「*」の行を変更すると、すべてのポートに変更が適用されます。
有効	各ポートにおける Diffserv 機能の有効／無効を設定します。
適用	変更内容を本製品のランタイムメモリに保存します。 本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。

DSCP 設定

本製品が受信した IP パケットの DSCP 値を、VLAN タグの優先度（IEEE 802.1p/PCP）にマッピングします。



Diffserv **DSCP 設定**

DSCP から 802.1p へのマッピング

0	1	2	3	4	5	6	7
8	9	10	11	12	13	14	15
16	17	18	19	20	21	22	23
24	25	26	27	28	29	30	31
32	33	34	35	36	37	38	39
40	41	42	43	44	45	46	47
48	49	50	51	52	53	54	55
56	57	58	59	60	61	62	63

適用 キャンセル

項目	内容
0 ～ 63	DSCP 分類識別番号です。 プルダウンメニューから、IEEE 802.1p のプライオリティレベル（0 ～ 7）を割り当てます。
適用	変更内容を本製品のランタイムメモリに保存します。 本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。

【QoS】キューイング方式

キューに優先度を設定します。

ELECOM
>> Switch For Business

保存 | ログアウト | 再起動 | 日本語

スイッチング >> QoS >> キューイング方式

ダッシュボード

モニター

システム

ポート

スイッチング

ループ防止

ミラーリング

マルチキャスト

QoS

Diffserv

キューイング方式

キュー優先度

帯域幅制御

スパンニングツリー

静的MACフィルタリング

静的MAC転送

VLAN

VLANアイソレーション

VLANマッピング

ネットワーク

セキュリティ

キューイング方式

ポート	方式	ウェイト								Hybrid-SPQ Lowest-Queue
		Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	
*	SPQ									なし
1	SPQ	1	2	3	4	5	6	7	8	なし
2	SPQ	1	2	3	4	5	6	7	8	なし
3	SPQ	1	2	3	4	5	6	7	8	なし
4	SPQ	1	2	3	4	5	6	7	8	なし
5	SPQ	1	2	3	4	5	6	7	8	なし
6	SPQ	1	2	3	4	5	6	7	8	なし
7	SPQ	1	2	3	4	5	6	7	8	なし
8	SPQ	1	2	3	4	5	6	7	8	なし
9	SPQ	1	2	3	4	5	6	7	8	なし
10	SPQ	1	2	3	4	5	6	7	8	なし

適用 キャンセル

項目	内容						
ポート	ポート番号が表示されます。						
方式	<p>キューの方式を選択します。(初期値：SPQ)</p> <table> <tr> <td>SPQ</td><td>優先度のみに基づいてキューをサービスします。 最も優先度の高いキューが空になると、次に優先度の高いキューのトラフィックが開始されます。Q7 が最も優先度が高く、Q0 が最も低くなります。</td></tr> <tr> <td>WFQ</td><td>各キューの帯域幅部分(「ウェイト」に設定された数値)に基づいて、各キューの最低帯域幅を保証するために使用されます。 より大きな重みを持つキューは、より小さな重みを持つキューよりも多くの帯域幅を保証されます。</td></tr> <tr> <td>WRR</td><td>キューの重み(「ウェイト」に設定された数値)に基づいて、キューをローテーションでサービスします。より大きな重みを持つキューは、より小さな重みを持つキューよりも多くのサービスを得ます。</td></tr> </table>	SPQ	優先度のみに基づいてキューをサービスします。 最も優先度の高いキューが空になると、次に優先度の高いキューのトラフィックが開始されます。Q7 が最も優先度が高く、Q0 が最も低くなります。	WFQ	各キューの帯域幅部分(「ウェイト」に設定された数値)に基づいて、各キューの最低帯域幅を保証するために使用されます。 より大きな重みを持つキューは、より小さな重みを持つキューよりも多くの帯域幅を保証されます。	WRR	キューの重み(「ウェイト」に設定された数値)に基づいて、キューをローテーションでサービスします。より大きな重みを持つキューは、より小さな重みを持つキューよりも多くのサービスを得ます。
SPQ	優先度のみに基づいてキューをサービスします。 最も優先度の高いキューが空になると、次に優先度の高いキューのトラフィックが開始されます。Q7 が最も優先度が高く、Q0 が最も低くなります。						
WFQ	各キューの帯域幅部分(「ウェイト」に設定された数値)に基づいて、各キューの最低帯域幅を保証するために使用されます。 より大きな重みを持つキューは、より小さな重みを持つキューよりも多くの帯域幅を保証されます。						
WRR	キューの重み(「ウェイト」に設定された数値)に基づいて、キューをローテーションでサービスします。より大きな重みを持つキューは、より小さな重みを持つキューよりも多くのサービスを得ます。						
ウェイト	WFQ または WRR を選択した場合、キューウェイトをここに入力します。 帯域幅は、それぞれの重みに従って、異なるトラフィックキューに分割されます。						

122

項目	内容
Hybrid-SPQ Lowest-Queue	<p>この設定は、「方式」に「WFQ」または「WRR」を選択した場合のみ適用されます。キュー（Q0 ～ Q7）を選択し、ギガビットポートの指定キュー以降のキューに SPQ を使用します。</p> <p>例えば、Q5 を選択した場合、Q5, Q6, Q7 のトラフィックに対して SPQ を使用します。</p> <p>ギガビットポートに常に WFQ または WRR を使用する場合は、「なし」を選択します。</p>

[QoS]キュー優先度

優先度レベルから物理キューへのマッピングを設定します

ELECOM
>> Switch For Business

保存 | ログアウト | 再起動 | 日本語

スイッチング
ループ防止
ミラーリング
マルチキャスト
QoS
Differv
キューイング方式
キュー優先度
帯域幅制御
スパンニングツリー
静的MACフィルタリング
静的MAC転送
VLAN
VLANアイソレーション
VLANマッピング
ネットワーク
セキュリティ

スイッチング
>> QoS
>> キュー優先度

キュー優先度

キュー優先度 割り当て

優先度7
6
5
4
3
2
1
0

7
6
5
4
3
2
1
0

適用
キャンセル

項目	内容
優先度 7	通常、ルーター設定メッセージなどのネットワーク制御トラフィックに使用されます。
優先度 6	通常、ジッター（遅延の変動）に特に敏感な音声トラフィックに使用されます。
優先度 5	通常、高い帯域幅を消費し、ジッターの影響を受けやすいビデオに使用されます。
優先度 4	通常、SNA (Systems Network Architecture) トランザクションなど、負荷が制御され、遅延に敏感なトラフィックに使用されます。
優先度 3	通常、「エクセレント・エフォート」またはベスト・エフォートよりも優れたトラフィックに使用され、多少の遅延を許容できる重要なビジネス・トラフィックが含まれます。
優先度 2	「予備の帯域幅」用です。
優先度 1	通常、バルク転送のようなクリティカルでない「バックグラウンド」トラフィックに使用されます。
優先度 0	通常、ベストエフォート・トラフィックに使用されます。

124

【QoS】帯域幅制御

最大帯域幅を設定します。

ELECOM
>> Switch For Business
保存 | ログアウト | 再起動 | 日本語

スイッチング >> QoS >> 帯域幅制御

ダッシュボード
モニター
システム
ポート
スイッチング
ループ防止
ミラーリング
マルチキャスト
QoS
DiffServ
キューイング方式
キュー優先度
帯域幅制御
スパンニングツリー
静的MACフィルタリング
静的MAC転送
VLAN
VLANアイソレーション
VLANマッピング
ネットワーク
セキュリティ

帯域幅制御

有効
☐

ポート	有効	入力レート	有効	出力レート
*	<input type="checkbox"/>	<input type="text"/> kbps	<input type="checkbox"/>	<input type="text"/> kbps
1	<input type="checkbox"/>	<input type="text" value="64"/> kbps	<input type="checkbox"/>	<input type="text" value="64"/> kbps
2	<input type="checkbox"/>	<input type="text" value="64"/> kbps	<input type="checkbox"/>	<input type="text" value="64"/> kbps
3	<input type="checkbox"/>	<input type="text" value="64"/> kbps	<input type="checkbox"/>	<input type="text" value="64"/> kbps
4	<input type="checkbox"/>	<input type="text" value="64"/> kbps	<input type="checkbox"/>	<input type="text" value="64"/> kbps
5	<input type="checkbox"/>	<input type="text" value="64"/> kbps	<input type="checkbox"/>	<input type="text" value="64"/> kbps
6	<input type="checkbox"/>	<input type="text" value="64"/> kbps	<input type="checkbox"/>	<input type="text" value="64"/> kbps
7	<input type="checkbox"/>	<input type="text" value="64"/> kbps	<input type="checkbox"/>	<input type="text" value="64"/> kbps
8	<input type="checkbox"/>	<input type="text" value="64"/> kbps	<input type="checkbox"/>	<input type="text" value="64"/> kbps
9	<input type="checkbox"/>	<input type="text" value="64"/> kbps	<input type="checkbox"/>	<input type="text" value="64"/> kbps
10	<input type="checkbox"/>	<input type="text" value="64"/> kbps	<input type="checkbox"/>	<input type="text" value="64"/> kbps

適用
キャンセル

項目	内容
有効	帯域幅制御機能の有効／無効を設定します。(初期設定：無効)
ポート	ポート番号が表示されます。 「*」の行を変更すると、すべてのポートに変更が適用されます。
有効	入力レート制限を有効にする場合は、チェックを入れます。
入力レート	ポートの受信トラフィックフローに許容される最大帯域幅をキロビット / 秒 (kbps) で指定します。(初期設定：64kbps) 入力レート帯域幅制御は、レイヤー 2 トラフィックにのみ適用されます。
有効	出力レート制限を有効にする場合は、チェックを入れます。
出力レート	ポートの送信トラフィックフローに許可される最大帯域幅をキロビット / 秒 (kbps) で指定します。(初期設定：64kbps)
適用	変更内容を本製品のランタイムメモリに保存します。 本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。

【スパンニングツリー】ステータス

本製品で設定できる異なるSTPモード（RSTPまたはMSTP）のSTPステータスが表示されます。

この画面は、STPモードの設定によって異なります。

■ RSTP設定時

ELECOM
Switch For Business
保存 | ログアウト | 再起動 | 日本語

スイッチング
スパンニングツリー
ステータス

ダッシュボード
モニター
システム
ポート
スイッチング
ループ防止
ミラーリング
マルチキャスト
QoS
スパンニングツリー
ステータス
設定
RSTP
MSTP
静的MACフィルタリング
静的MAC転送
VLAN
VLANアイソレーション

スパンニングツリーステータス

RSTP

ルートブリッジ		自ブリッジ
ブリッジID	0000-000000000000	0000-000000000000
ハロータイム (秒)	0	0
最大経過時間 (秒)	0	0
転送遅延 (秒)	0	0
ブリッジコスト	0	
ポートID	0x0000	
トポロジー変更カウント	0	
前回変更からの経過時間	0:00:00	

ポート	ポート状態	ポートロール	指定ブリッジID	指定ポートID	指定コスト	ルートガード状態
-----	-------	--------	----------	---------	-------	----------

項目	内容
ブリッジ ID	ブリッジ・プライオリティと MAC アドレスからなる、このブリッジに固有の識別子が表示されます。 この ID は、本製品がルートスイッチの場合、ルートブリッジと自ブリッジで同じになります。
ハロータイム (秒)	ルートスイッチがコンフィグレーションメッセージを送信する時間間隔（秒）が表示されます。 ルートブリッジは、ハロータイム、最大経過時間、転送遅延を決定します。
最大経過時間 (秒)	本製品がコンフィグレーションメッセージを受信せずに再コンフィグレーションを試行できる最大時間（秒）が表示されます。
転送遅延 (秒)	ルートスイッチが状態を変更するまでの時間（秒）が表示されます。
ブリッジコスト	本製品のルートポートからルートスイッチまでのパスコストが表示されます。
ポート ID	本製品がスパンニングツリーのルートと通信するためのポートの優先度と番号が表示されます。

126

項目	内容										
トポロジ変更回数	スパニングツリーの再設定回数が表示されます。										
前回変更からの時間	スパニングツリーを最後に再設定してからの時間が表示されます。										
ポート	本製品のポート番号が表示されます。										
ポート状態	<p>STP におけるポートの状態が表示されます。</p> <table border="1"> <tr> <td>DISCARDING</td><td>ポートは受信したフレームの転送や処理、MAC アドレスの学習は行いませんが、BPDU のリッスンを行います。</td></tr> <tr> <td>LEARNING</td><td>ポートは MAC アドレスを学習し、BPDU を処理しますが、まだフレームを転送しません。</td></tr> <tr> <td>FORWARDING</td><td>ポートは正常に動作しています。MAC アドレスを学習し、BPDU を処理し、受信したフレームを転送します。</td></tr> </table>	DISCARDING	ポートは受信したフレームの転送や処理、MAC アドレスの学習は行いませんが、BPDU のリッスンを行います。	LEARNING	ポートは MAC アドレスを学習し、BPDU を処理しますが、まだフレームを転送しません。	FORWARDING	ポートは正常に動作しています。MAC アドレスを学習し、BPDU を処理し、受信したフレームを転送します。				
DISCARDING	ポートは受信したフレームの転送や処理、MAC アドレスの学習は行いませんが、BPDU のリッスンを行います。										
LEARNING	ポートは MAC アドレスを学習し、BPDU を処理しますが、まだフレームを転送しません。										
FORWARDING	ポートは正常に動作しています。MAC アドレスを学習し、BPDU を処理し、受信したフレームを転送します。										
ポートロール	<p>STP におけるポートの役割が表示されます。</p> <table border="1"> <tr> <td>Root</td><td>非ルートブリッジ上のフォワーディングポートで、パスコストが最も低く、非ルートブリッジからルートブリッジへの最良のポートです。ルートブリッジはルートポートを持ちません。</td></tr> <tr> <td>Designated</td><td>接続されている各 LAN セグメントの指定ブリッジの転送ポートです。指定ブリッジは、LAN セグメントに接続されているブリッジの中で、ルートブリッジまでのパスコストが最も低くなります。ルートブリッジ（ルートスイッチ）上のポートはすべて指定ポートです。</td></tr> <tr> <td>Alternate</td><td>ルートブリッジへの最良の代替パスを持つブロックポートです。この経路は、ルート・ポートを使用するのとは異なります。LAN セグメントの指定ポートに障害が発生すると、このポートはフォワーディング状態に移行します。</td></tr> <tr> <td>Backup</td><td>スイッチが同じ LAN セグメントへのリンクを 2 つ持っている場合、指定ポートがすでに接続されている LAN セグメントへのバックアップまたは冗長パスを持つブロックされたポートです。</td></tr> <tr> <td>Disabled</td><td>厳密には STP の一部ではありません。ポートは手動で無効にできます。</td></tr> </table>	Root	非ルートブリッジ上のフォワーディングポートで、パスコストが最も低く、非ルートブリッジからルートブリッジへの最良のポートです。ルートブリッジはルートポートを持ちません。	Designated	接続されている各 LAN セグメントの指定ブリッジの転送ポートです。指定ブリッジは、LAN セグメントに接続されているブリッジの中で、ルートブリッジまでのパスコストが最も低くなります。ルートブリッジ（ルートスイッチ）上のポートはすべて指定ポートです。	Alternate	ルートブリッジへの最良の代替パスを持つブロックポートです。この経路は、ルート・ポートを使用するのとは異なります。LAN セグメントの指定ポートに障害が発生すると、このポートはフォワーディング状態に移行します。	Backup	スイッチが同じ LAN セグメントへのリンクを 2 つ持っている場合、指定ポートがすでに接続されている LAN セグメントへのバックアップまたは冗長パスを持つブロックされたポートです。	Disabled	厳密には STP の一部ではありません。ポートは手動で無効にできます。
Root	非ルートブリッジ上のフォワーディングポートで、パスコストが最も低く、非ルートブリッジからルートブリッジへの最良のポートです。ルートブリッジはルートポートを持ちません。										
Designated	接続されている各 LAN セグメントの指定ブリッジの転送ポートです。指定ブリッジは、LAN セグメントに接続されているブリッジの中で、ルートブリッジまでのパスコストが最も低くなります。ルートブリッジ（ルートスイッチ）上のポートはすべて指定ポートです。										
Alternate	ルートブリッジへの最良の代替パスを持つブロックポートです。この経路は、ルート・ポートを使用するのとは異なります。LAN セグメントの指定ポートに障害が発生すると、このポートはフォワーディング状態に移行します。										
Backup	スイッチが同じ LAN セグメントへのリンクを 2 つ持っている場合、指定ポートがすでに接続されている LAN セグメントへのバックアップまたは冗長パスを持つブロックされたポートです。										
Disabled	厳密には STP の一部ではありません。ポートは手動で無効にできます。										
指定ブリッジ ID	<p>ポートが指定ポートの場合、このポートが属する指定ブリッジの識別子が表示されます。</p> <p>それ以外の場合は、このポートが接続されている LAN セグメントの指定ブリッジの識別子が表示されます。</p>										
指定ポート ID	指定ブリッジが蓄積されたコンフィギュレーションメッセージを送信する（指定ブリッジ上の）ブリッジポートの優先度と番号が表示されます。										

項目	内容				
指定コスト	ポートが指定ポートの場合、ポートが接続されている LAN セグメントまでのパスコストが表示されます。それ以外の場合は、このポートが接続されている LAN セグメントの指定ポートからルートブリッジまでのパスコストが表示されます。				
ルートガード状態	<p>ルートガードが有効になっているポートの状態が表示されます。</p> <table border="1"> <tr> <td>Root-inconsistent</td><td>ポートで上位 BPDU を受信し、ポートをブロックします。</td></tr> <tr> <td>Forwarding</td><td>ブロックを解除し、ポートが再びフレームを転送できるようにします。</td></tr> </table>	Root-inconsistent	ポートで上位 BPDU を受信し、ポートをブロックします。	Forwarding	ブロックを解除し、ポートが再びフレームを転送できるようにします。
Root-inconsistent	ポートで上位 BPDU を受信し、ポートをブロックします。				
Forwarding	ブロックを解除し、ポートが再びフレームを転送できるようにします。				

■ RSTP 設定時

ELECOM >> Switch For Business

保存 | ログアウト | 再起動 | 日本語

スイッチング >> スパンニングツリー >> ステータス

スパンニングツリーステータス

ダッシュボード

モニター

システム

ポート

スイッチング

ループ防止

ミラーリング

マルチキャスト

QoS

スパンニングツリー

ステータス

設定

RSTP

MSTP

静的MACフィルタリング

静的MAC転送

VLAN

VLANアイソレーション

VLANマッピング

ネットワーク

セキュリティ

管理

MSTP

CST

	ルートブリッジ	自ブリッジ
ブリッジID	0000-000000000000	0000-000000000000
ハロータイム (秒)	0	0
最大経路時間 (秒)	0	0
転送遅延 (秒)	0	0
ブリッジコスト	0	0
ポートID	0x0000	0x0000
設定名	3897a46a5000	
リビジョン番号	0	
設定ダイジェスト	0	
トポロジ変更回数	0	
前回変更からの時間	0:00:00	

インスタンス

インスタンス	VLAN
0	1-4094

MSTI 0

	リージョナルルート	自ブリッジ
ブリッジID	0000-000000000000	0000-000000000000
内部コスト	0	0
ポートID	0x0000	0x0000

ポート

ポート状態

ポートロール

指定ブリッジID

指定ポートID

指定コスト

ルートガード状態

● CST

項目	内容
ブリッジ ID	ブリッジ・プライオリティと MAC アドレスからなる、このブリッジに固有の識別子が表示されます。 この ID は、本製品がルートスイッチの場合、ルートブリッジと自ブリッジで同じになります。
ハロータイム (秒)	ルートスイッチがコンフィギュレーションメッセージを送信する時間間隔 (秒) が表示されます。 ルートブリッジは、ハロータイム、最大経過時間、転送遅延を決定します。
最大経過時間 (秒)	本製品がコンフィギュレーションメッセージを受信せずに再コンフィギュレーションを試行できる最大時間 (秒) が表示されます。
転送遅延 (秒)	ルートスイッチが状態を変更するまでの時間 (秒) が表示されます。
ブリッジコスト	本製品のルートポートからルートスイッチまでのパスコストが表示されます。
ポート ID	本製品がスパニングツリーのルートと通信するためのポートの優先度と番号が表示されます。
設定名	この MST リージョンの設定名が表示されます。
リビジョン番号	この MST リージョンのリビジョン番号が表示されます。
設定ダイジェスト	VLAN-MSTI マッピング情報から生成されます。 これは MSTP BPDU に含まれる 16 オクテットの署名です。 また、システムで MSTP がアクティブになったときのダイジェストです。
トポロジ変更回数	スパニングツリーの再設定回数が表示されます。
前回変更からの時間	スパニングツリーを最後に再設定してからの時間が表示されます。

● インスタンス

各スパニングツリーインスタンスにおいて、どの VLAN が動作しているかが表示されます。

項目	内容
インスタンス	MSTI ID が表示されます。
VLAN	どの VLAN が MSTI にマッピングされているかが表示されます。

● MSTI

項目	内容
MSTI	表示する MST インスタンス設定を選択します。
ブリッジ ID	ブリッジプライオリティ+ MAC アドレスで構成されます。このブリッジに固有の識別子です。本製品がルートスイッチの場合、この ID はルートと自ブリッジで同じになります。
内部コスト	MST インスタンスのルートポートからリージョナルルートスイッチまでのパスコストです。

項目	内容
ポート ID	本製品が MST インスタンスのルートと通信する必要がある本製品のポートの優先度と番号です。

●テーブル

項目	内容										
ポート	本製品のポート番号が表示されます。										
ポート状態	<p>STP におけるポートの状態が表示されます。</p> <table border="1"> <tr> <td>DISCARDING</td><td>ポートは受信したフレームの転送や処理、MAC アドレスの学習は行いませんが、BPDU のリスンは行います。</td></tr> <tr> <td>LEARNING</td><td>ポートは MAC アドレスを学習し、BPDU を処理しますが、まだフレームを転送しません。</td></tr> <tr> <td>FORWARDING</td><td>ポートは正常に動作しています。MAC アドレスを学習し、BPDU を処理し、受信したフレームを転送します。</td></tr> </table>	DISCARDING	ポートは受信したフレームの転送や処理、MAC アドレスの学習は行いませんが、BPDU のリスンは行います。	LEARNING	ポートは MAC アドレスを学習し、BPDU を処理しますが、まだフレームを転送しません。	FORWARDING	ポートは正常に動作しています。MAC アドレスを学習し、BPDU を処理し、受信したフレームを転送します。				
DISCARDING	ポートは受信したフレームの転送や処理、MAC アドレスの学習は行いませんが、BPDU のリスンは行います。										
LEARNING	ポートは MAC アドレスを学習し、BPDU を処理しますが、まだフレームを転送しません。										
FORWARDING	ポートは正常に動作しています。MAC アドレスを学習し、BPDU を処理し、受信したフレームを転送します。										
ポートロール	<p>STP におけるポートの役割が表示されます。</p> <table border="1"> <tr> <td>Root</td><td>非ルートブリッジ上のフォワーディングポートで、パスコストが最も低く、非ルートブリッジからルートブリッジへの最良のポートです。ルートブリッジはルートポートを持ちません。</td></tr> <tr> <td>Designated</td><td>接続されている各 LAN セグメントの指定ブリッジの転送ポートです。指定ブリッジは、LAN セグメントに接続されているブリッジの中で、ルートブリッジまでのパスコストが最も低くなります。ルートブリッジ（ルートスイッチ）上のポートはすべて指定ポートです。</td></tr> <tr> <td>Alternate</td><td>ルートブリッジへの最良の代替パスを持つブロックポートです。この経路は、ルート・ポートを使用するのとは異なります。LAN セグメントの指定ポートに障害が発生すると、このポートはフォワーディング状態に移行します。</td></tr> <tr> <td>Backup</td><td>スイッチが同じ LAN セグメントへのリンクを 2 つ持っている場合、指定ポートがすでに接続されている LAN セグメントへのバックアップまたは冗長パスを持つブロックされたポートです。</td></tr> <tr> <td>Disabled</td><td>厳密には STP の一部ではありません。ポートは手動で無効にできます。</td></tr> </table>	Root	非ルートブリッジ上のフォワーディングポートで、パスコストが最も低く、非ルートブリッジからルートブリッジへの最良のポートです。ルートブリッジはルートポートを持ちません。	Designated	接続されている各 LAN セグメントの指定ブリッジの転送ポートです。指定ブリッジは、LAN セグメントに接続されているブリッジの中で、ルートブリッジまでのパスコストが最も低くなります。ルートブリッジ（ルートスイッチ）上のポートはすべて指定ポートです。	Alternate	ルートブリッジへの最良の代替パスを持つブロックポートです。この経路は、ルート・ポートを使用するのとは異なります。LAN セグメントの指定ポートに障害が発生すると、このポートはフォワーディング状態に移行します。	Backup	スイッチが同じ LAN セグメントへのリンクを 2 つ持っている場合、指定ポートがすでに接続されている LAN セグメントへのバックアップまたは冗長パスを持つブロックされたポートです。	Disabled	厳密には STP の一部ではありません。ポートは手動で無効にできます。
Root	非ルートブリッジ上のフォワーディングポートで、パスコストが最も低く、非ルートブリッジからルートブリッジへの最良のポートです。ルートブリッジはルートポートを持ちません。										
Designated	接続されている各 LAN セグメントの指定ブリッジの転送ポートです。指定ブリッジは、LAN セグメントに接続されているブリッジの中で、ルートブリッジまでのパスコストが最も低くなります。ルートブリッジ（ルートスイッチ）上のポートはすべて指定ポートです。										
Alternate	ルートブリッジへの最良の代替パスを持つブロックポートです。この経路は、ルート・ポートを使用するのとは異なります。LAN セグメントの指定ポートに障害が発生すると、このポートはフォワーディング状態に移行します。										
Backup	スイッチが同じ LAN セグメントへのリンクを 2 つ持っている場合、指定ポートがすでに接続されている LAN セグメントへのバックアップまたは冗長パスを持つブロックされたポートです。										
Disabled	厳密には STP の一部ではありません。ポートは手動で無効にできます。										
指定ブリッジ ID	ポートが指定ポートの場合、このポートが属する指定ブリッジの識別子が表示されます。それ以外の場合は、このポートが接続されている LAN セグメントの指定ブリッジの識別子が表示されます。										
指定ポート ID	指定ブリッジが蓄積されたコンフィギュレーションメッセージを送信する（指定ブリッジ上の）ブリッジポートの優先度と番号が表示されます。										

項目	内容	
指定コスト	ポートが指定ポートの場合、ポートが接続されている LAN セグメントまでのパスコストが表示されます。それ以外の場合は、このポートが接続されている LAN セグメントの指定ポートからルートブリッジまでのパスコストが表示されます。	
ルートガード 状態	ルートガードが有効になっているポートの状態が表示されます。	
	Root-inconsistent	ポートで上位 BPDU を受信し、ポートをブロックします。
	Forwarding	ブロックを解除し、ポートが再びフレームを転送できるようにします。

【スパニングツリー】設定

STPモードの設定をします。

ELECOM >> Switch For Business

保存 | ログアウト | 再起動 | 日本語

スイッチング >> スパニングツリー >> 設定

ダッシュボード

モニター

システム

ポート

スイッチング

ループ防止

ミラーリング

マルチキャスト

QoS

スパニングツリー

ステータス

設定

RSTP

MSTP

静的MACフィルタリング

静的MAC転送

VLAN

VLANアイソレーション

VLANマッピング

ネットワーク

セキュリティ

スパニングツリー設定

スパニングツリーモード

☒ ラビッドスパニングツリー (RSTP)

☐ マルチプルスパニングツリー (MSTP)

自動バスクコストモード

☐ Short

☒ Long

☐ ユーザー定義 :

10M 2000000

100M 200000

1G 20000

2.5G 8000

5G 4000

10G 2000

適用

キャンセル

■ スパニングツリーモード

項目	内容
スパニングツリーモード	STP モードを選択します。

項目	内容						
自動パスコストモード	リンク速度に応じて各ポートのパスコストを自動的に設定します。 本製品はパスコストを使用して、スパニングツリーのルートブリッジへの最良のパスを決定します。(初期設定: Long)						
	<table><tr><td>Short</td><td>本製品が定義する 16 ビットのオートパスコスト値を使用する場合に選択します。</td></tr><tr><td>Long</td><td>本製品が定義する 32 ビットのオートパスコスト値を使用する場合に選択します。Long を選択した場合、ネットワーク内のすべてのスイッチも Long パスコスト方式を使用する必要があります。そうしないと、スパニングツリーが正しく収束しない可能性があります。</td></tr><tr><td>ユーザー定義</td><td>手動で設定します。</td></tr></table>	Short	本製品が定義する 16 ビットのオートパスコスト値を使用する場合に選択します。	Long	本製品が定義する 32 ビットのオートパスコスト値を使用する場合に選択します。Long を選択した場合、ネットワーク内のすべてのスイッチも Long パスコスト方式を使用する必要があります。そうしないと、スパニングツリーが正しく収束しない可能性があります。	ユーザー定義	手動で設定します。
	Short	本製品が定義する 16 ビットのオートパスコスト値を使用する場合に選択します。					
	Long	本製品が定義する 32 ビットのオートパスコスト値を使用する場合に選択します。Long を選択した場合、ネットワーク内のすべてのスイッチも Long パスコスト方式を使用する必要があります。そうしないと、スパニングツリーが正しく収束しない可能性があります。					
	ユーザー定義	手動で設定します。					
スパニングツリーネットワークシステム内のすべてのスイッチで、同じオートパスコストモードを使用することを推奨します。 自動パスコスト機能を使用するには、ポートのパスコストを「0」に設定します。 「RSTP」(134 ページ) または「MSTP」(137 ページ) 本製品はポートのパスコストを、選択した自動パスコストモード定義された自動パスコスト値に自動的に設定します。							
適用	変更内容を本製品のランタイムメモリに保存します。 本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。						

【スパニングツリー】RSTP

高速スパニングツリープロトコルの設定をします。

ELECOM >> Switch For Business

保存 | ログアウト | 再起動 | 日本語

スイッチング >> スパニングツリー >> RSTP

ダッシュボード

モニター

システム

ポート

スイッチング

ループ防止

ミラーリング

マルチキャスト

QoS

スパニングツリー

ステータス

設定

RSTP

MSTP

静的MACフィルタリング

静的MAC転送

VLAN

VLANアイソレーション

VLANマッピング

ネットワーク

セキュリティ

RSTP

有効 ☐ ON ☒ OFF

ブリッジ優先度 32768

ハロータイム 2 秒

最大経過時間 20 秒

転送遅延 15 秒

ポート	有効	エッジ	ルートガード	優先度	パスコスト
*	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	128	2
2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	128	2
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	128	2
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	128	2
5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	128	2
6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	128	2
7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	128	2
8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	128	2
9	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	128	2
10	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	128	2

適用 キャンセル

項目	内容
有効	<p>「ON」にすると、本製品で RSTP が有効になります。</p> <p>RSTP を有効にするには、「スイッチング」－「スパニングツリー」－「設定」(132 ページ)の「スパニングツリーモード」で「ラピッドスパニングツリー (RSTP)」を選択している必要があります。</p>
ブリッジ優先度	<p>ブリッジ優先度を選択します。(初期値: 32768)</p> <p>数値が低いほど、このブリッジのプライオリティは高くなります。</p> <p>ブリッジ優先度は、ルート・スイッチ、ルート・ポート、および指定ポートの決定に使用されます。プライオリティが最も高い(数値が最も小さい)スイッチが STP ルートスイッチになります。</p> <p>すべてのスイッチのプライオリティが同じ場合は、MAC アドレスが最小のスイッチがルート・スイッチになります。</p> <p>ブリッジ優先度はルート・ブリッジを決定し、それによってハロータイム、最大経過時間、および転送遅延が決定されます。</p>
ハロータイム	<p>ルートスイッチが BPDU (ブリッジプロトコルデータユニット) コンフィグレーションメッセージを生成するまでの時間間隔 (秒) です。(設定範囲: 1 ~ 10 秒) (初期値: 2 秒)</p>

134

項目	内容
最大経過時間	<p>再コンフィグレーションを試みる前に、スイッチが BPDU を受信せずに待機できる最大時間 (秒) です。すべてのスイッチポート (指定ポートを除く) は、一定間隔で BPDU を受信する必要があります。</p> <p>STP 情報 (最後の BPDU で提供される) をエージングアウトしたポートは、アタッチされた LAN の指定ポートになります。ルートポートの場合は、ネットワークに接続されているスイッチポートの中から新しいルートポートが選択されます。</p> <p>(設定範囲: 6 ~ 40 秒) (初期値: 20 秒)</p>
転送遅延	<p>スイッチが状態を変更するまでの最大時間 (秒) を設定します。 (初期値: 15 秒)</p> <p>各スイッチはフレームの転送を開始する前に、トポロジーの変更に関する情報を受信する必要があります。この遅延が必要です。</p> <p>さらに、各ポートは、ブロッキング状態に戻るような競合情報をリッスンする時間が必要です。そうしないと、一時的なデータループが発生する可能性があります。</p> <p>一般的なルールとして以下となるように設定します。</p> <p>$(\text{転送遅延時間} - 1) \geq \text{最大経過時間} \geq 2 * (\text{ハロータイム} + 1)$</p>
ポート	<p>ポート番号が表示されます。</p> <p>[*] の行を変更すると、すべてのポートに変更が適用されます。</p>
有効	このポートの RSTP を有効にする場合にチェックを入れます。
エッジ	<p>コンピュータに直接接続されているポートをエッジポートとして設定するときにチェックを入れます。</p> <p>エッジポートは、ポートがエッジポートとして設定された直後やリンクステータスが変わったときに、リスニング状態や学習状態を経ることなく、STP ポートの初期状態をブロッキング状態からフォワーディング状態に即座に変更します。また、エッジポートは、ブリッジプロトコルデータユニット (BPDU) を受信するとすぐに非エッジポートになります。</p>
ルートガード	<p>チェックを入れると、ポートに接続されているスイッチがルートブリッジになるのを防ぐために、このポートでルートガードが有効になります。</p> <p>ルートガードを有効にすると、本製品がそのポートで上位 BPDU を受信した場合、ポートはブロックされます。本製品は、ポートに接続されたスイッチが上位 BPDU の送信を停止すると、このポートのトラフィックを再び通過させます。</p>
優先度	<p>各ポートのプライオリティを設定します。</p> <p>プライオリティは、スイッチ内で複数のポートがループを形成している場合に、どのポートを無効にするかを決定します。優先順位の数値が高いポートから順に無効化されます。</p> <p>(設定範囲: 0 ~ 255) (初期値: 128)</p>
パスコスト	<p>パスコストは、そのポートを経由して LAN にフレームを送信する際のコストです。</p> <p>ブリッジの速度に応じてこの値を割り当てることをお勧めします。</p> <p>メディアの速度が遅いほど、コストは高くなります。</p> <p>デフォルトのパスコスト値は、選択したデフォルトのパスコスト方法によって異なります。</p>

項目	内容
適用	<p>変更内容を本製品のランタイムメモリに保存します。</p> <p>本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。</p>

【スパニングツリー】MSTP

MSTP

マルチプルスパニングツリープロトコルの設定をします。

マルチスパニングツリーを追加したり、選択したマルチスパニングツリーを編集します。

→ [139ページ](#)

選択したマルチスパニングツリーを削除します。

■ ブリッジ

項目	内容
有効	「ON」にすると、本製品で MSTP が有効になります。 MSTP を有効にするには、「スイッチング」－「スパニングツリー」－「設定」(132 ページ)の「スパニングツリーモード」で「マルチプルスパニングツリー (MSTP)」を選択している必要があります。
ハロータイム	ルートスイッチが BPDU (ブリッジプロトコルデータユニット) コンフィグレーションメッセージを生成するまでの時間間隔 (秒) です。(設定範囲: 1 ～ 10 秒) (初期値: 2 秒)

項目	内容
最大経過時間	<p>再コンフィグレーションを試みる前に、スイッチが BPDU を受信せずに待機できる最大時間（秒）です。すべてのスイッチポート（指定ポートを除く）は、一定間隔で BPDU を受信する必要があります。</p> <p>STP 情報（最後の BPDU で提供される）をエージングアウトしたポートは、アタッチされた LAN の指定ポートになります。ルートポートの場合は、ネットワークに接続されているスイッチポートの中から新しいルートポートが選択されます。</p> <p>（設定範囲：6 ～ 40 秒）（初期値：20 秒）</p>
転送遅延	<p>スイッチが状態を変更するまでの最大時間（秒）を設定します。（初期値：15 秒）</p> <p>各スイッチはフレームの転送を開始する前に、トポロジの変更に関する情報を受信する必要があるため、この遅延が必要です。</p> <p>さらに、各ポートは、ブロッキング状態に戻るような競合情報をリッスンする時間が必要です。そうしないと、一時的なデュータループが発生する可能性があります。</p> <p>一般的なルールとして以下のように設定します。</p> <p>$(\text{転送遅延時間} - 1) \geq \text{最大経過時間} \geq 2 * (\text{ハロータイム} + 1)$</p>
最大ホップ数	<p>BPDU が破棄され、ポート情報がエージングされるまでの MSTP リージョン内のホップ数（1 ～ 255）を入力します。（初期値：20）</p>
設定名	<p>MST リージョンの説明的な名前（最大 32 文字）を入力します。</p>
リビジョン番号	<p>リージョンのコンフィギュレーションを識別するための番号を入力します。同じリージョンに属するデバイスは、同じリビジョン番号でなければなりません。</p>
適用	<p>変更内容を本製品のランタイムメモリに保存します。</p> <p>本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。</p>

■ インスタンス

項目	内容
インスタンス	<p>MST インスタンスの ID が表示されます。</p>
VLAN	<p>MST インスタンスがマッピングされる VID（または VID 範囲）が表示されます。</p>
有効ポート	<p>MST インスタンスに参加するように構成されたポートが表示されます。</p>

■ マルチプルスパニングツリーの追加／編集

インスタンス

ブリッジ優先度

32768 ▾

VLANリスト

ポート	有効	優先度	パスコスト
*	<input type="checkbox"/>		
1	<input type="checkbox"/>	128	2
2	<input type="checkbox"/>	128	2
3	<input type="checkbox"/>	128	2
4	<input type="checkbox"/>	128	2
5	<input type="checkbox"/>	128	2
6	<input type="checkbox"/>	128	2
7	<input type="checkbox"/>	128	2
8	<input type="checkbox"/>	128	2
9	<input type="checkbox"/>	128	2
10	<input type="checkbox"/>	128	2

適用

クリア

キャンセル

項目	内容
インスタンス	本製品でこの MST インスタンスを識別するために使用する番号を入力します。 (設定範囲: 0 ~ 16)
ブリッジ優先度	特定のスパニングツリーインスタンスに対する本製品の優先度を設定します。 数値が低いほど、本製品がスパニングツリーインスタンス内のルートブリッジとして選択される可能性が高くなります。 (設定範囲: 0 ~ 61440 の間で 4096 刻み。4096 / 8192 / 12288 / 16384 / 20480 / 24576 / 28672 / 32768 / 36864 / 40960 / 45056 / 49152 / 53248 / 57344 / 61440) (初期値: 32768)
VLAN リスト	VLAN ID の範囲を入力します。複数の VLANID 範囲を (スペースなし) カンマ (,) またはハイフン ("-") で区切って指定できます。 例えば、VLAN1,3,5,6,7 の場合は「1,3,5-7」と入力します。
ポート	ポート番号が表示されます。 [*] の行を変更すると、すべてのポートに変更が適用されます。
有効	チェックを入れると、このポートを MST インスタンスに追加します。
優先度	各ポートのプライオリティを設定します。 優先度は、複数のポートが本製品内でループを形成している場合に、どのポートを無効にするかを決定します。優先度の数値が高いポートが最初に無効になります。 (設定範囲: 0 ~ 255) (初期値: 128)
パスコスト	そのポートを経由して LAN にフレームを送信する際のコストです。 ブリッジの速度に応じてこの値を割り当てることをお勧めします。 メディアの速度が遅いほど、コストは高くなります。

MSTP ポート設定

マルチプルスパニングツリープロトコルのポート設定をします。

ポート	エッジ	ルートガード
*	<input type="checkbox"/>	<input type="checkbox"/>
1	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="checkbox"/>	<input type="checkbox"/>
6	<input type="checkbox"/>	<input type="checkbox"/>
7	<input type="checkbox"/>	<input type="checkbox"/>
8	<input type="checkbox"/>	<input type="checkbox"/>
9	<input type="checkbox"/>	<input type="checkbox"/>
10	<input type="checkbox"/>	<input type="checkbox"/>

項目	内容
ポート	ポート番号が表示されます。 「*」の行を変更すると、すべてのポートに変更が適用されます。
エッジ	コンピュータに直接接続されているポートをエッジポートとして設定するときにチェックを入れます。 エッジポートは、ポートがエッジポートとして設定された直後やリンクステータスの変更されたときに、リスニング状態や学習状態を経ることなく、STP ポートの初期状態をブロッキング状態からフォワーディング状態に即座に変更します。また、エッジポートは、ブリッジプロトコルデータユニット (BPDU) を受信するとすぐに非エッジポートになります。
ルートガード	チェックを入れると、ポートに接続されているスイッチがルートブリッジになるのを防ぐために、このポートでルートガードが有効になります。 ルートガードを有効にすると、本製品がそのポートで上位 BPDU を受信した場合、ポートはブロックされます。本製品は、ポートに接続されたスイッチが上位 BPDU の送信を停止すると、このポートのトラフィックを再び通過させます。
適用	変更内容を本製品のランタイムメモリに保存します。本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。

静的MACフィルタリング

MACフィルタリングの設定をします。



静的MACフィルタリングルールを追加したり、選択した
静的MACフィルタリングルールを編集します。

→ [142 ページ](#)

選択した静的MACフィルタリングルールを削除します。

項目	内容
インデックス	静的 MAC フィルタリングルールのインデックス番号が表示されます。
有効	静的 MAC フィルタリングルールが有効かどうかが表示されます。 ルールは一時的に無効化できます。
名前	静的 MAC フィルタリングルールの識別のための名称が表示されます。
MAC アドレス	フィルタリング数 MAC アドレスが表示されます。
VID	VLAN グループの ID 番号が表示されます。
動作	フィルタリング時の動作が表示されます。

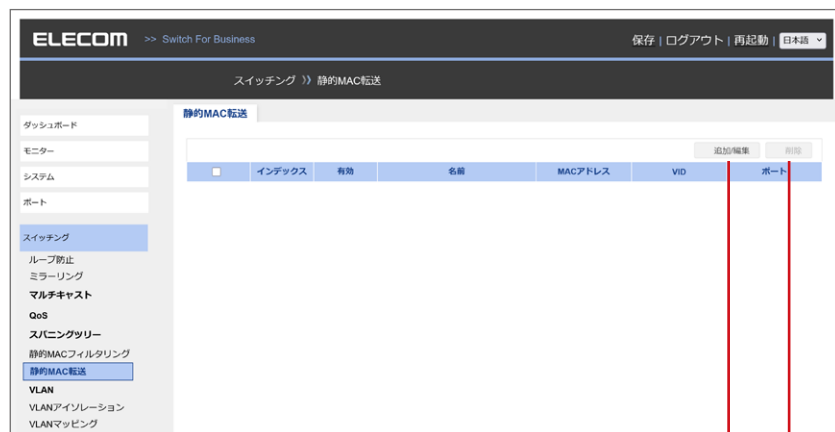
■ 静的MACフィルタリングの追加／編集

有効	<input type="radio"/> OFF
名前	<input type="text"/>
動作	<input type="checkbox"/> 送信元を破棄 <input type="checkbox"/> 宛先を破棄
MAC	<input type="text"/>
VID	<input type="text"/>
<input type="button" value="適用"/> <input type="button" value="クリア"/> <input type="button" value="キャンセル"/>	

項目	内容				
有効	静的 MAC フィルタリングルールの有効／無効を切り替えます。 無効にすると、ルールを削除せずに一時的に非アクティブにすることができます。				
名前	この静的 MAC フィルタリングルールの名前を入力します。 (最大 32 文字まで。? (クエスチョンマーク) (パイプ) ' (クォーテーション) " (ダブルクォーテーション) , (コンマ) は使用不可)				
動作	フィルタリングしたときの動作を選択します。 <table> <tr> <td>送信元を破棄</td><td>受信フレームの送信元 MAC アドレスが設定した MAC アドレスと一致したら、破棄します。</td></tr> <tr> <td>宛先を破棄</td><td>受信フレームの宛先 MAC アドレスが設定した MAC アドレスと一致したら、破棄します。</td></tr> </table>	送信元を破棄	受信フレームの送信元 MAC アドレスが設定した MAC アドレスと一致したら、破棄します。	宛先を破棄	受信フレームの宛先 MAC アドレスが設定した MAC アドレスと一致したら、破棄します。
送信元を破棄	受信フレームの送信元 MAC アドレスが設定した MAC アドレスと一致したら、破棄します。				
宛先を破棄	受信フレームの宛先 MAC アドレスが設定した MAC アドレスと一致したら、破棄します。				
MAC	フィルタリングを実行する MAC アドレスを有効な MAC アドレス形式 (16 進数 6 文字のペア) で入力します。 静的 MAC アドレスはエージアウトしません。				
VID	VLAN 識別番号を入力します。				
適用	変更内容を本製品のランタイムメモリに保存します。 本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。				
クリア	フィールドが工場出荷時のデフォルトにクリアされます。				

静的MAC転送

ポートに静的MACアドレスを割り当てます。



静的MAC転送ルールを追加したり、選択した静的MAC転送ルールを編集します。

→ [144ページ](#)

選択した静的MAC転送ルールを削除します。

項目	内容
インデックス	静的MACアドレスルールのインデックス番号が表示されます。
有効	静的MACアドレス転送ルールがアクティブかどうかが表示されます。ルールは一時的に無効化できます。
名前	静的MACアドレス転送ルールの識別のための記述名が表示されます。
MACアドレス	転送されるMACアドレスと、そのMACアドレスが属するVLAN識別番号が表示されます。
VID	VLANグループのID番号が表示されます。
ポート	MACアドレスが転送されるポートが表示されます。

■ 静的MAC転送ルールの追加／編集

有効

☐ OFF

名前

MACアドレス

VID

ポート

適用

クリア

キャンセル

項目	内容
有効	ルールの有効／無効を切り替えます。 無効にすると、ルールを削除せずに一時的に非アクティブにすることができます。
名前	この静的 MAC アドレス転送ルールの名前を入力します。 (最大 32 文字まで。? (クエスチョンマーク) (パイプ) ' (クォーテーション) " (ダブルクォーテーション) , (コンマ) は使用不可)
MAC アドレス	MAC アドレスを有効な MAC アドレス形式(16 進数 6 文字のペア)で入力します。 静的 MAC アドレスはエージアウトしません。
VID	VLAN 識別番号を入力します。
ポート	MAC アドレスが自動的に転送されるポートを入力します。
適用	変更内容を本製品のランタイムメモリに保存します。 本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。
クリア	フィールドが工場出荷時のデフォルトにクリアされます。

[VLAN]VLANステータス

静的 VLAN グループを表示および検索します。



項目	内容				
VID による VLAN 検索	既存の VLAN ID 番号（個々の VLAN を区切るにはカンマ（,）を、VLAN の範囲を示すにはダッシュ（-）を使用）を入力し、[検索] をクリックすると、下のリストに指定した VLAN だけが表示されます。 例えば、「3,4」または「3-9」などを入力し、[検索] をクリックすると、指定した VLAN だけが下のリストに表示されます。 空欄のまま [検索] をクリックすると、本製品に設定されているすべての VLAN が表示されます。				
VLAN 数	本製品に設定されている VLAN の数が表示されます。				
インデックス	VLAN のインデックス番号です。インデックス番号をクリックすると VLAN の詳細が表示されます。(146 ページ)				
VID	VLAN の識別番号が表示されます。				
名前	VLAN の名称が表示されます。				
タグ付きポート	VLAN に参加しているタグ付きポートが表示されます。				
タグなしポート	VLAN に参加しているタグなしポートが表示されます。				
経過時間	通常 VLAN の登録または静的 VLAN の設定からの経過時間が表示されます。				
状態	この VLAN がどのように本製品に追加されたかが表示されます。 <table><tr><td>Dynamic</td><td>GVRP を使用</td></tr><tr><td>静的</td><td>恒久的なエンドリリーとして追加</td></tr></table>	Dynamic	GVRP を使用	静的	恒久的なエンドリリーとして追加
Dynamic	GVRP を使用				
静的	恒久的なエンドリリーとして追加				

■ VLAN詳細画面

静的 VLAN グループの詳細なポート設定とステータスが表示されます。

ELECOM

>> Switch For Business

保存 | ログアウト | 再起動 | 日本語

スイッチング >> VLAN >> VLAN ステータス

ダッシュボード

モニター

システム

ポート

スイッチング

ループ防止

ミラーリング

マルチキャスト

QoS

スパンニングツリー

静的MACフィルタリング

静的MAC転送

VLAN

VLAN ステータス

VLAN 設定

VLAN ステータス

VLAN ステータス > VLAN ステータス詳細

VID1
経過時間0:57:30
状態静的

ポート番号

U:タグなし T:タグ付き

2	4	6	8	10
1	3	5	7	9
U	U	U	U	U
U	U	U	U	U

項目	内容
ポート番号	VLAN に参加しているポートが表示されます。
	Tタグ付きポート
	Uタグなしポート
	-VLAN に参加していないポート

[VLAN] VLAN 設定

静的 VLAN

静的 VLAN の設定をします。

項目	内容
VLAN 学習方式	VLAN の学習方式を選択します。
適用	変更内容を本製品のランタイムメモリに保存します。 本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。
VID	VLAN グループの ID 番号が表示されます。
有効	VLAN 設定の有効／無効が表示されます。
名前	VLAN グループの名称が表示されます。

■ 静的 VLAN の追加／編集

有効 ☒ 有効 ☐ 無効

名前

VLANグループID

ポート	制御			タグ付き
*	通常 <input checked="" type="radio"/> 通常 <input type="radio"/> Fixed <input type="radio"/> Forbidden			<input checked="" type="checkbox"/> 送信タグ付き
1	<input checked="" type="radio"/> 通常	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> 送信タグ付き
2	<input checked="" type="radio"/> 通常	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> 送信タグ付き
3	<input checked="" type="radio"/> 通常	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> 送信タグ付き
4	<input checked="" type="radio"/> 通常	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> 送信タグ付き
5	<input checked="" type="radio"/> 通常	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> 送信タグ付き
6	<input checked="" type="radio"/> 通常	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> 送信タグ付き
7	<input checked="" type="radio"/> 通常	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> 送信タグ付き
8	<input checked="" type="radio"/> 通常	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> 送信タグ付き
9	<input checked="" type="radio"/> 通常	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> 送信タグ付き
10	<input checked="" type="radio"/> 通常	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> 送信タグ付き

項目	内容						
有効	静的 VLAN の有効／無効を切り替えます。						
名前	VLAN グループの名前を入力します。 (最大 64 文字まで。？ (クエスチョンマーク) (パイプ) ' (クォーテーション) " (ダブルクォーテーション) , (コンマ) は使用不可)						
VLAN グループ ID	この静的 VLAN の ID を入力します。有効範囲は 1 ～ 4094 です。 [Voice VLAN 設定] (151 ページ) で使用した VLAN ID を追加しないでください。						
ポート	ポート番号が表示されます。 [*] の行を変更すると、すべてのポートに変更が適用されます。						
制御	<table><tr><td>通常 (初期値)</td><td>ポートが GVRP を使用してこの VLAN グループに動的に参加する場合に選択します。</td></tr><tr><td>Fixed</td><td>ポートをこの VLAN グループのパーマnentメンバーにする場合に選択します。</td></tr><tr><td>Forbidden</td><td>この VLAN グループへのポートの参加を禁止する場合に選択します。</td></tr></table>	通常 (初期値)	ポートが GVRP を使用してこの VLAN グループに動的に参加する場合に選択します。	Fixed	ポートをこの VLAN グループのパーマnentメンバーにする場合に選択します。	Forbidden	この VLAN グループへのポートの参加を禁止する場合に選択します。
通常 (初期値)	ポートが GVRP を使用してこの VLAN グループに動的に参加する場合に選択します。						
Fixed	ポートをこの VLAN グループのパーマnentメンバーにする場合に選択します。						
Forbidden	この VLAN グループへのポートの参加を禁止する場合に選択します。						
タグ付き	この VLAN グループ ID で送信されるすべての送信フレームにタグを付ける場合は、チェックを入れます。						

VLAN ポート設定

ポートの静的 VLAN (IEEE 802.1Q) 設定をします。

ELECOM
>> Switch For Business

保存 | ログアウト | 再起動 | 日本語

スイッチング >> VLAN >> VLAN 設定

ダッシュボード

モニター

システム

ポート

スイッチング

ループ防止

ミラーリング

マルチキャスト

QoS

スパンニングツリー

静的MACフィルタリング

静的MAC転送

VLAN

VLAN ステータス

VLAN 設定

Voice VLAN設定

VLANアイソレーション

VLANマッピング

静的VLAN

VLANポート設定

ポート	入力フィルタリング	PVID	許可フレームタイプ	VLAN トランキング	分類
*	<input type="checkbox"/>		すべて	<input type="checkbox"/>	<input type="checkbox"/>
1	<input type="checkbox"/>	1	すべて	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	1	すべて	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	1	すべて	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	1	すべて	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="checkbox"/>	1	すべて	<input type="checkbox"/>	<input type="checkbox"/>
6	<input type="checkbox"/>	1	すべて	<input type="checkbox"/>	<input type="checkbox"/>
7	<input type="checkbox"/>	1	すべて	<input type="checkbox"/>	<input type="checkbox"/>
8	<input type="checkbox"/>	1	すべて	<input type="checkbox"/>	<input type="checkbox"/>
9	<input type="checkbox"/>	1	すべて	<input type="checkbox"/>	<input type="checkbox"/>
10	<input type="checkbox"/>	1	すべて	<input type="checkbox"/>	<input type="checkbox"/>

適用 キャンセル

項目	内容
ポート	ポート番号が表示されます。 「*」の行を変更すると、すべてのポートに変更が適用されます。
入力フィルタリング	チェックを入れると、本製品はこのポートがメンバーセットに含まれていない VLAN の受信フレームを破棄します。 チェックボックスをオフにすると、入力フィルタリングは無効になります。
PVID	Port VLAN ID (PVID) は、ポートで受信したタグなしフレームを、タグが定義する VLAN グループに転送するために本製品が付加するタグです。 ポート VLAN ID として 1 ～ 4094 の数値を入力します。
許可フレームタイプ	<div> <div> <div>すべて</div> <div>このポートですべてのタグなしまたはタグ付きフレームを受け入れます。</div> </div> <div> <div>タグ付きのみ</div> <div>このポートではタグ付きフレームのみを受け付けます。</div> </div> <div> <div>タグなしのみ</div> <div>このポートではタグなしフレームのみを受け付けます。 タグ付きフレームはすべて廃棄されます。</div> </div> </div> <p>ポートで許可されるフレームのタイプを指定します。 (すべて／タグ付きのみ／タグなしのみ) (初期値：すべて)</p>
VLAN トランキング	他のスイッチやルータに接続されているポート（エンドユーザに直接接続されているポートは不可）で VLAN トランキングを有効にし、未知の VLAN グループに属するフレームを通過させます。

項目	内容
分離	このポートを CPU 管理ポートおよびアイソレーション機能が有効になっていないポートとのみ通信できるようにします。
適用	変更内容を本製品のランタイムメモリに保存します。 本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。

[VLAN]Voice VLAN 設定

Voice VLANに優先レベルを設定し、OUI（Organizationally Unique Identifiers）から ID を使用して特定のメーカーの IP 電話の MAC アドレスを追加します。

Voice VLANを追加したり、選択した Voice VLAN を編集します。

→ [151 ページ](#)

選択した Voice VLAN を削除します。

■ Voice VLAN グローバル設定

項目	内容
Voice VLAN	Voice VLAN 機能を有効にする場合は、2 番目のラジオボタンを選択し、Voice VLAN に関連付けられた VLAN ID 番号を入力します。 Voice VLAN 機能を有効にしない場合は、「無効」を選択します。
優先度	音声トラフィックの優先度を 0 ～ 7 から選択します。 数値が高いほど、この音声トラフィックの優先度は高くなります。 (初期値：5)
適用	変更内容を本製品のランタイムメモリに保存します。 本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。

■ Voice VLAN OUI設定

項目	内容
インデックス	Voice VLAN のインデックス番号が表示されます。
OUI アドレス	Voice VLAN の OUI アドレスが表示されます。
OUI マスク	Voice VLAN の OUI マスクアドレスが表示されます。
説明	OUI アドレスを持つ音声 VLAN の説明が表示されます。

■ Voice VLANの追加／編集

OUIアドレス	<input type="text"/>
OUIマスク	<input type="text"/>
説明	<input type="text"/>
<input type="button" value="適用"/> <input type="button" value="クリア"/> <input type="button" value="キャンセル"/>	

項目	内容
OUI アドレス	IP 電話メーカーの OUI MAC アドレスを入力します。 最初の 3 バイトは製造者識別子で、最後の 3 バイトは一意のステーション ID です。
OUI マスク	指定した IP 電話メーカーの OUI（ベンダ識別子）MAC アドレスに対するマスクを入力し、パケットの MAC アドレスのどのビットを一致させるかを決めます。 一致させたいビットには、指定した MAC アドレスの各ビットに「f」を入力します。 任意の値（どの 16 進数でも可）でよいビットには「0」を入力します。 例：MAC アドレスを 00:13:49:00:00:00、マスクを ff:ff:ff:00:00:00 に設定した場合、 MAC アドレスが 00:13:49:12:34:56 のパケットはこの条件に一致します。
適用	変更内容を本製品のランタイムメモリに保存します。 本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。
クリア	フィールドが工場出荷時のデフォルトにクリアされます。

VLANアイソレーション

VLAN内のポート間で通信を行わないように設定します。



VLANアイソレーションルールを追加したり、選択した
VLANアイソレーションルールを編集します。

→ [151ページ](#)

選択したVLANアイソレーションルールを削除します。

項目	内容
インデックス	このルールのインデックス番号が表示されます。
有効	このルールが有効かどうかが表示されます。
名前	このルールの説明的な名前が表示されます。
VLAN ID	このルールが適用される VLAN が表示されます。
混合ポート	同じ VLAN 内のどのポートとも通信できるポートが表示されます。

■ VLANアイソレーションルールの追加／編集

有効

☐ OFF

名前

VLAN ID

混合ポート

適用

クリア

キャンセル

項目	内容
有効	この VLAN アイソレーションルールの有効／無効を切り替えます。
名前	識別のために名称を入力します。 (最大 32 文字まで。?(クエスチョンマーク) (パイプ)'(クォーテーション)"(ダブルクォーテーション)，(コンマ) は使用不可)
VLAN VID	1 ～ 4094 の VLAN ID を入力します。これは、このルールが適用される VLAN です。
混合ポート	この VLAN に属するすべてのポートと通信できるポートを指定します。 1 ～ 10 のポート番号を入力します。 この VLAN に属するポートはここで指定したポートとのみ送受信が可能となります。
適用	変更内容を本製品のランタイムメモリに保存します。 本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。
クリア	フィールドが工場出荷時のデフォルトにクリアされます。

VLAN マッピング

VLAN マッピング

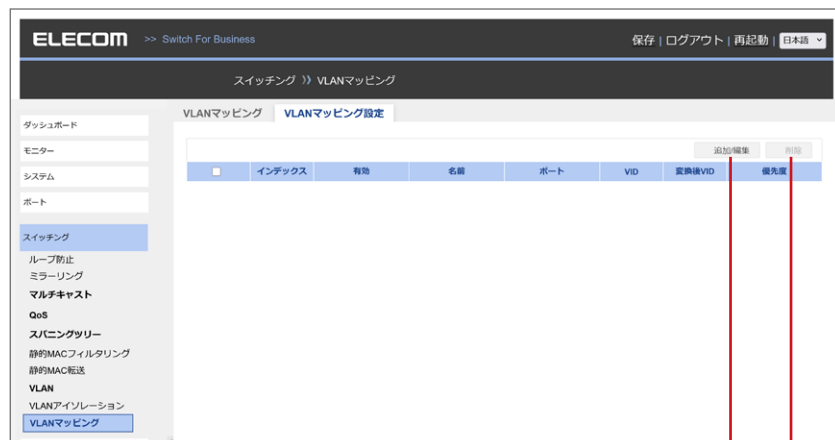
本製品およびポートで VLAN マッピングを有効にします。



項目	内容
有効	「ON」にすると、本製品で VLAN マッピングが有効になります。
ポート	ポート番号が表示されます。 「*」の行を変更すると、すべてのポートに変更が適用されます。
有効	チェックを入れると、このポートの VLAN マッピング機能が有効になります。
適用	変更内容を本製品のランタイムメモリに保存します。 本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。

VLAN マッピング設定

VLAN マッピングルールを表示および設定します。



VLAN マッピングを追加したり、選択した VLAN マッピングを編集します。

→ [157 ページ](#)

選択した VLAN マッピングを削除します。

項目	内容
インデックス	テーブル内の VLAN マッピングエントリ番号が表示されます。
有効	このエントリの有効／無効が表示されます。
名前	このルールの説明的な名前が表示されます。
ポート	このルールが適用されるポート番号が表示されます。
VID	受信パケットのカスタマー VLAN ID が表示されます。
変換後 VID	タグ付きパケットの顧客 VLAN ID に代わる VLAN ID です。
優先度	タグ付きパケットでカスタマーの優先度レベルを置き換える優先度レベルが表示されます。

■ VLAN マッピングの追加／編集

有効	<input type="checkbox"/> OFF
名前	<input type="text"/>
ポート	<input type="text"/>
VID	<input type="text"/>
変換後VID	<input type="text"/>
優先度	<input type="text" value="0"/>
<input type="button" value="適用"/> <input type="button" value="クリア"/> <input type="button" value="キャンセル"/>	

項目	内容
有効	このマッピングルールの有効／無効を切り替えます。
名前	このマッピングルールの名前を入力します。 (最大 32 文字まで。? (クエスチョンマーク) (パイプ) ' (フォーテーション) " (ダブルフォーテーション) , (コンマ) は使用不可)
ポート	このルールに含めるポートを入力します。
VID	1 から 4094 までの VLAN ID を入力します。 これはパケットで運ばれる VLAN タグで、変換後 VID フィールドで指定した VID に変換されます。
変換後 VID	パケットに含まれるカスタマー VID が変換される VLAN ID (1 ～ 4094) を入力します。
適用	変更内容を本製品のランタイムメモリに保存します。 本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。
クリア	フィールドが工場出荷時のデフォルトにクリアされます。

【ARP 設定】ARP ラーニング

各ポートの ARP 学習モードを設定します。



項目	内容	
ポート	ポート番号が表示されます。 「*」の行を変更すると、すべてのポートに変更が適用されます。	
ARP ラーニングモード	本製品がポートで使用する ARP 学習モードを選択します。(初期値：ARP 応答)	
	ARP 応答	本製品が送信した ARP リクエストに対する ARP リプライのみで ARP テーブルを更新します。
	Gratuitous-ARP	ARP リプライまたは無償 ARP リクエストで ARP テーブルを更新します。
	ARP 要求	ARP リプライ、無償 ARP リクエスト、ARP リクエストの両方で ARP テーブルを更新します。

【ARP 設定】静的 ARP

エージアウトしない静的 ARP エントリを表示および構成します。



静的ARPを追加したり、選択した
静的ARPを編集します。

→ [160 ページ](#)

選択した静的ARPを削除します。

項目	内容
インデックス	エントリーのインデックス番号が表示されます。
有効	このエントリーが有効かどうかが表示されます。
名前	このエントリーの説明的な名前が表示されます。
IP アドレス	本製品のポートに接続されているデバイスの IP アドレスが表示されます。
MAC アドレス	IP アドレスに対応するデバイスの MAC アドレスが表示されます。
VID	デバイスが属する VLAN が表示されます。
ポート	デバイスが接続するポートが表示されます。

■ 静的ARPの追加／編集

有効

☐ OFF

名前

IPアドレス

MACアドレス

VID

ポート

適用

クリア

キャンセル

項目	内容
有効	このルールの有効／無効を切り替えます。 無効にすると、ルールを削除せずに一時的に非アクティブにすることができます。
名前	このルールの名前を入力します。 (最大 32 文字まで。? (クエスチョンマーク) (パイプ) ' (クォーテーション) " (ダブルクォーテーション) , (コンマ) は使用不可)
IP アドレス	本製品のポートに接続されている機器の IP アドレスを入力します。
MAC アドレス	上記 IP アドレスに対応する機器の MAC アドレスを入力します。
VID	機器が属する VLAN の ID 番号を入力します。
ポート	接続先のポート番号を入力します。
適用	変更内容を本製品のランタイムメモリに保存します。 本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。
クリア	フィールドが工場出荷時のデフォルトにクリアされます。

[AAA]RADIUSサーバー設定

RADIUS サーバーの設定をします。

ELECOM >> Switch For Business

保存 | ログアウト | 再起動 | 日本語

セキュリティ >> AAA >> RADIUSサーバー設定

ダッシュボード

モニター

システム

ポート

スイッチング

ネットワーク

セキュリティ

AAA

RADIUSサーバー設定

AAA設定

ACL

アンチARPスキャン

BPDUGuard

ストームコントロール

DoS攻撃防止

Errisable

IPv4ソースガード

IPv6ソースガード

ポート認証

ポートセキュリティ

管理

RADIUSサーバー設定

認証サーバー

モードインデックス優先
タイムアウト30秒

用路	インデックス	IPアドレス	UDPポート	共有鍵	暗号化共有鍵
<input type="checkbox"/>	1		1812		
<input type="checkbox"/>	2		1812		

アカウントingサーバー

タイムアウト30秒

用路	インデックス	IPアドレス	UDPポート	共有鍵	暗号化共有鍵
<input type="checkbox"/>	1		1813		
<input type="checkbox"/>	2		1813		

属性

NAS-IPアドレス0.0.0.0

適用 キャンセル

■ 認証サーバー

項目	内容	
モード	インデックス優先 (初期値)	最初に設定された RADIUS サーバーで認証。 最初の RADIUS サーバーが応答しない場合、スイッチは 2 番目の RADIUS サーバーを試みます。
	ラウンドロビン	認証要求を送信する RADIUS サーバ間を交互に切り替えます。
タイムアウト	スイッチが RADIUS サーバからの認証要求応答を待つ時間 (秒) です。 (初期値 : 30 秒) 2 台の RADIUS サーバを使用する場合、タイムアウトは 2 台の RADIUS サーバ間で分割されます。	

項目	内容
削除	既存の RADIUS サーバエントリを本製品から削除する場合にチェックします。 このエントリは「適用」をクリックすると削除されます。
インデックス	RADIUS サーバエントリを表す番号が表示されます。
IP アドレス	RADIUS サーバの IP アドレスを入力します。
UDP ポート	RADIUS サーバの認証用ポートを入力します。(初期値: 1812)
共有鍵	RADIUS サーバとスイッチ間で共有するパスワードを入力します。
暗号化共有鍵	「AAA 設定ページ」(163 ページ) で「サーバーキー暗号化」を有効にした場合に、暗号化された共有シークレットを「*」形式で表示します。 「サーバーキー暗号化」を有効にすると、シークレットは暗号化され続けます。

■ アカウンティングサーバー

項目	内容
タイムアウト	本製品が RADIUS アカウンティングサーバからのアカウンティング要求応答を待つ時間 (単位: 秒) です。(初期値: 30 秒)
削除	既存の RADIUS サーバエントリを本製品から削除する場合にチェックします。 このエントリは「適用」をクリックすると削除されます。
インデックス	RADIUS サーバエントリを表す番号が表示されます。
IP アドレス	RADIUS サーバの IP アドレスを入力します。
UDP ポート	RADIUS サーバの認証用ポートを入力します。(初期値: 1813)
共有鍵	RADIUS サーバとスイッチ間で共有するパスワードを入力します。
暗号化共有鍵	「AAA 設定ページ」(163 ページ) で「サーバーキー暗号化」を有効にした場合に、暗号化された共有シークレットを「*」形式で表示します。 「サーバーキー暗号化」を有効にすると、シークレットは暗号化され続けます。

■ 属性

項目	内容
NAS-IP アドレス	ネットワーク・アクセス・サーバの IP アドレスを入力します。

[AAA] AAA 設定

AAA の設定をします。

ELECOM >> Switch For Business

保存 | ログアウト | 再起動 | 日本語

セキュリティ >> AAA >> AAA設定

ダッシュボード

モニター

システム

ポート

スイッチング

ネットワーク

セキュリティ

AAA

RADIUSサーバー設定

AAA設定

ACL

アンチARPスキャン

BPDUガード

ストームコントロール

DOS攻撃防止

Errdisable

IPv6ソースガード

IPv6ソースガード

ポート認証

ポートセキュリティ

管理

AAA設定

サーバーキー暗号化

有効 ☐

認証

タイプ	方式 1	方式 2
ログイン	ローカル	

権限付与

タイプ	有効	方式
Dot1x	<input type="radio"/>	RADIUS

アカウントिंग

更新間隔 1 分

タイプ	有効	ブロードキャスト	モード	方式
システム	<input type="radio"/>	<input type="checkbox"/>	-	RADIUS
Dot1x	<input type="radio"/>	<input type="checkbox"/>	start-stop	RADIUS

適用 キャンセル

■ サーバーキー暗号化

項目	内容
有効	RADIUS サーバーのサーバー鍵（共有秘密）暗号化を有効／無効にします。

■ 認証

項目	内容
タイプ	管理者アカウントの認証に使用するデータベースを指定します。
方式 1	ローカル「システム」－「ユーザーアカウント」画面で設定した管理者アカウントを確認します。
方式 2	RADIUSRADIUS Server で設定した管理者アカウントを確認します。

■ 権限付与

項目	内容
タイプ	IEEE 802.1x クライアントに、外部サーバーを介して異なる帯域制限または VLAN ID を割り当てることを許可します。
有効	有効を「ON」にすると、802.1X 認証に成功した後に RADIUS が返す属性を本製品に適用します。「OFF」にすると、属性は無視し、認証だけ通してデフォルト設定で接続します。
方式	認証に RADIUS を使用します。

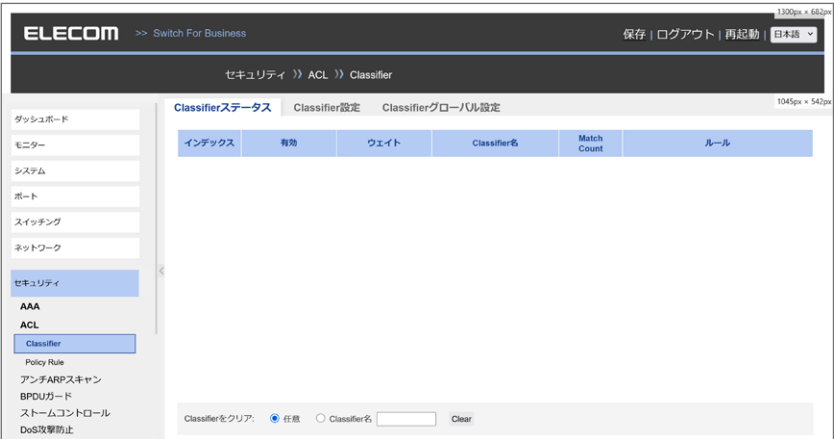
■ アカウンティング

項目	内容				
更新期間	本製品がアカウンティングサーバーにアップデートを送信する時間を設定します。「start-stop」モード選択時のみ有効です。(初期値: 1 分)				
タイプ	<table border="1"> <tr> <td>システム</td><td>次のシステムイベントが発生したときに情報を送信するように本製品を設定します。 システムのブートアップ、システムのシャットダウン、システムアカウンティングが有効、システムアカウンティングが無効。</td></tr> <tr> <td>Dot1x</td><td>IEEE 802.1x クライアントがセッションを開始（本製品経由で認証）したとき、セッションを終了したとき、およびセッションの中間更新が発生したときに情報を送信するように設定します。</td></tr> </table>	システム	次のシステムイベントが発生したときに情報を送信するように本製品を設定します。 システムのブートアップ、システムのシャットダウン、システムアカウンティングが有効、システムアカウンティングが無効。	Dot1x	IEEE 802.1x クライアントがセッションを開始（本製品経由で認証）したとき、セッションを終了したとき、およびセッションの中間更新が発生したときに情報を送信するように設定します。
システム	次のシステムイベントが発生したときに情報を送信するように本製品を設定します。 システムのブートアップ、システムのシャットダウン、システムアカウンティングが有効、システムアカウンティングが無効。				
Dot1x	IEEE 802.1x クライアントがセッションを開始（本製品経由で認証）したとき、セッションを終了したとき、およびセッションの中間更新が発生したときに情報を送信するように設定します。				
有効	指定されたイベントタイプに対してアカウンティングを有効にするか無効にするか設定します。				
ブロードキャスト	チェックを入れると、設定されているすべてのアカウンティングサーバに同時にアカウンティング情報を送信します。				
モード	<p>RADIUS アカウンティングで送信するメッセージ種別のモードを選択します。(Dot1x のみ) (初期値: start-stop)</p> <table border="1"> <tr> <td>start-stop</td><td>以下のタイミングで送信します。 ・ユーザーがセッションを開始したとき ・ユーザーのセッション中（更新期間を過ぎたとき） ・ユーザーがセッションを終了したとき</td></tr> <tr> <td>stop-only</td><td>ユーザーがセッションを終了したときのみを送信します。</td></tr> </table>	start-stop	以下のタイミングで送信します。 ・ユーザーがセッションを開始したとき ・ユーザーのセッション中（更新期間を過ぎたとき） ・ユーザーがセッションを終了したとき	stop-only	ユーザーがセッションを終了したときのみを送信します。
start-stop	以下のタイミングで送信します。 ・ユーザーがセッションを開始したとき ・ユーザーのセッション中（更新期間を過ぎたとき） ・ユーザーがセッションを終了したとき				
stop-only	ユーザーがセッションを終了したときのみを送信します。				
方式	アカウンティングに RADIUS を使用します。(変更不可)				
適用	<p>変更内容を本製品のランタイムメモリに保存します。</p> <p>本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。</p>				

[ACL] Classifier

Classifier ステータス

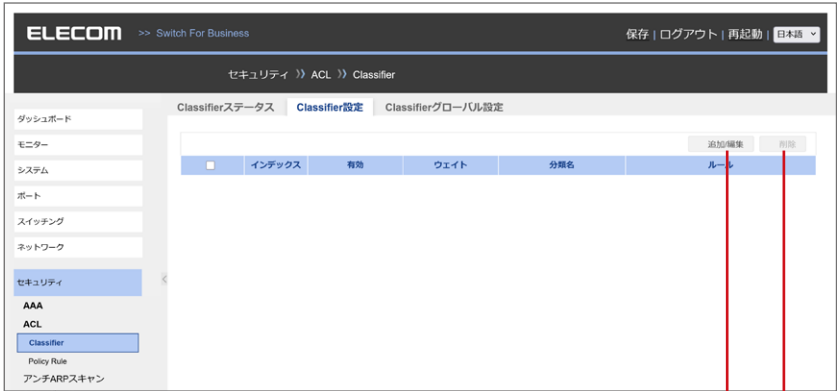
作成済みの Classifier の状態を確認します。



項目	内容				
インデックス	ルールのインデックス番号が表示されます。				
有効	ルールが有効かどうかが表示されます。				
ウェイト	「Classifier グローバル設定」(170 ページ) で、「マッチ順序」が「手動」に設定されている場合に、ルールの優先順位を示します。				
Classifier 名	このルールの識別のための名称が表示されます。				
Match Count	ルールが適用された回数が表示されます。 ルールがカウントを有効にしていない場合、「-」と表示されます。				
ルール	分類ルールの概要が表示されます。				
Classifier をクリア	<table><tr><td>任意</td><td>選択して「Clear」をクリックすると、すべてのルールのマッチカウントをクリアします。</td></tr><tr><td>Classifier 名</td><td>マッチカウントをクリアする Classifier 名を入力し、「Clear」をクリックすると、その Classifier のマッチカウントをクリアします。</td></tr></table>	任意	選択して「Clear」をクリックすると、すべてのルールのマッチカウントをクリアします。	Classifier 名	マッチカウントをクリアする Classifier 名を入力し、「Clear」をクリックすると、その Classifier のマッチカウントをクリアします。
任意	選択して「Clear」をクリックすると、すべてのルールのマッチカウントをクリアします。				
Classifier 名	マッチカウントをクリアする Classifier 名を入力し、「Clear」をクリックすると、その Classifier のマッチカウントをクリアします。				

Classifier 設定

Classifier の設定をします。



Classifier を追加したり、選択した Classifier を編集します。

→ [167 ページ](#)

選択した Classifier を削除します。

項目	内容
インデックス	ルールのインデックス番号が表示されます。
有効	ルールが有効かどうかが表示されます。
ウェイト	一致順序が手動モードの場合のルールの優先度が表示されます。ウェイトが高いほど優先度が高くなります。
分類名	このルールの識別のための名称が表示されます。
ルール	分類ルールの概要が表示されます。

■ Classifier の追加／編集

有効

☒ 有効

分類名

ウェイト

ログ記録

☐

カウント

☐

Time Range

入力ポート

☒ 任意

Port

トランク

☒ 任意

トランク

レイヤー2

☒ 任意

VLAN

優先度

☒ 任意

優先度

EtherType

☒ 任意

その他

(16進)

送信元MACアドレス

☒ 任意

MACマスク

/

宛先MACアドレス

☒ 任意

MACマスク

/

レイヤー3

☒ 任意

IPv4 DSCP

IPv6 DSCP

優先順位

☒ 任意

優先順位

ToS

☒ 任意

ToS

IPプロトコル

☒ 任意

確立のみ

☐

その他

(10進)

IPv6 Next Header

☒ 任意

確立のみ

☐

その他

(10進)

送信元IPアドレスプレフィックス

/

宛先IPアドレスプレフィックス

/

レイヤー4

☒ 任意

送信元ソケット番号

~

宛先ソケット番号

~

適用

クリア

キャンセル

項目	内容
有効	このルールの有効／無効を切り替えます。
分類名	このルールの名前を入力します。 (最大 32 文字まで。？(クエスチョンマーク) (パイプ) ' (クォーテーション) " (ダブルクォーテーション) , (コンマ) は使用不可)
ウェイト	ルールの重みを指定します。(設定範囲: 0 ~ 65535) (初期値: 32767) 「Classifier グローバル設定画面」(170 ページ) の「マッチ順序」で「手動」の場合、ウェイトが高いほど優先度が高くなります。
ログ記録	チェックを入れると、ルール適用時にログメッセージを作成し、特定の時間間隔でマッチしたパケット数を記録します。 「Classifier グローバル設定画面」(170 ページ) でも「ログ記録」を有効にしてください。
カウント	チェックを入れると、ルールの適用回数をカウントします。
Time Range	ルールに適用する設定済みのスケジュール名を選択します。

● 入力ポート

項目	内容
Port	<p>ルールを適用するポート番号を入力します。</p> <p>すべてのポートに「None」を選択できます。</p> <p>複数のポートを（スペースなし）カンマ (,) またはハイフン (-) で区切って入力できます。</p> <p>たとえば、ポート 3、4、5 には「3-5」と入力します。ポート 3、5、7 には「3,5,7」と入力します。</p>
トランク	<p>すべてのトランクグループにルールを適用する場合は「任意」を選択し、複数のトランクにルールを適用する場合はトランクグループ ID を入力します。</p> <p>複数のトランクを入力する場合は、(t) または (T) の後に、トランクグループ ID をスペースなしのカンマ (,) またはハイフン (-) で区切って入力します。</p> <p>例えば、トランク 3、4、5 には「t3-t5」と入力します。トランク 3、5、7 には「T3,T5,T7」と入力してください。</p>

● レイヤー 2

項目	内容
VLAN	<p>任意の VLAN からのトラフィックを分類するときは、「任意」を選択します</p> <p>ポートを指定する場合は、2 番目のラジオボタンを選択し、入力欄にソース VLAN ID を入力します。</p>
優先度	<p>任意の優先度レベルからのトラフィックを分類するときは、「任意」を選択します。</p> <p>優先度を指定するときは、2 番目のラジオボタンを選択し、優先度を選択します。</p>
Ether Type	<p>EtherType からトラフィックを分類するときは、プルダウンメニューから選択します。</p> <p>その他の Ether Type を指定するときは、2 番目のラジオボタンを選択し、16 進法で指定します。</p>
送信元 MAC アドレス	<p>すべての送信 MAC アドレスにルールを適用するときは、「任意」を選択します。</p> <p>範囲を選択するときは、2 番目のラジオボタンを選択し、MAC アドレスとビットマスクを入力します。</p>
宛先 MAC アドレス	<p>すべての宛先 MAC アドレスにルールを適用するときは、「任意」を選択します。</p> <p>範囲を選択するときは、2 番目のラジオボタンを選択し、MAC アドレスとビットマスクを入力します。</p>

● レイヤー 3

項目	内容
IPv4 DSCP	<p>すべての DSCP からトラフィックを分類するには、「任意」を選択します。</p>
IPv6 DSCP	<p>DSCP を指定する場合は、2 番目のラジオボタンを選択し、0 ～ 63 の DSCP (DiffServ Code Point) 番号を指定します。</p>

項目	内容
優先順位	すべての優先順位からトラフィックを分類するには、「任意」を選択します。 優先順位を指定する場合は、2 番目のラジオボタンを選択し、0 ～ 7 の IP 優先順位 (8 ビット ToS フィールドの最初の 3 ビット) 値を指定します。
ToS	すべての ToS からトラフィックを分類するには、「任意」を選択します。 ToS を指定する場合は、2 番目のラジオボタンを選択し、0 ～ 255 の Type of Service (8 ビット ToS フィールドの最後の 5 ビット) 値を指定します。
IP プロトコル	IPv4 プロトコルタイプを選択するか、「その他」を選択してプロトコル番号を 10 進数で入力します。 確立のみ TCP コネクションを確立するために送信されるパケットを選択します。
IPv6 Next Header	IPv6 プロトコルタイプを選択するか、「その他」を選択して IPv6 パケットの 8 ビットのネクストヘッダーを入力します。 IPv6 プロトコル番号の範囲は 1 ～ 255 です。 確立のみ TCP コネクションを確立するために送信されるパケットを選択します。
送信元 IP アドレス / プレフィックス	ドット付き 10 進数表記で送信元 IP アドレスを入力します。
宛先 IP アドレス / プレフィックス	ドット付き 10 進数表記で宛先 IP アドレスを入力します。

● レイヤー 4

項目	内容
送信元ソケット番号	すべての TCP/UDP プロトコルポート番号にルールを適用するには、「任意」を選択します。 送信元ソケット番号を指定する場合は、2 番目のラジオボタンを選択して TCP/UDP プロトコルポート番号を入力します。
宛先ソケット番号	すべての TCP/UDP プロトコルポート番号にルールを適用するには、「任意」を選択します。 宛先ソケット番号を指定する場合は、2 番目のラジオボタンを選択して TCP/UDP プロトコルポート番号を入力します。

項目	内容
適用	変更内容を本製品のランタイムメモリに保存します。 本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。
クリア	フィールドが工場出荷時のデフォルトにクリアされます。

Classifierグローバル設定

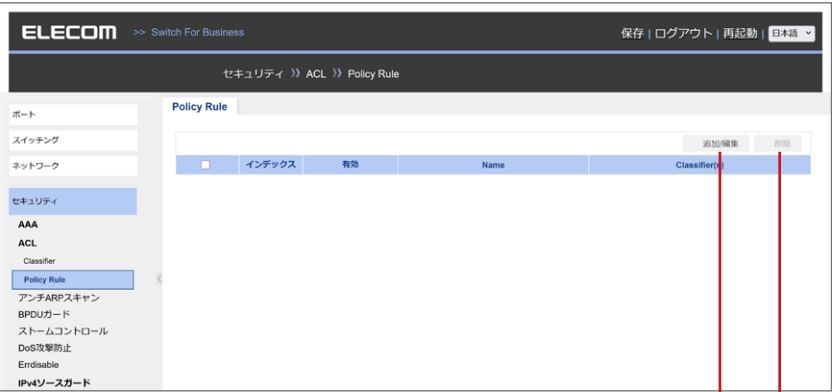
Classifierのグローバル設定をします。



項目	内容				
マッチ順序	<p>ルールに設定された項目のレイヤに従って分類ルールが適用されるようにするには、「自動」を選択します。(初期設定：自動)</p> <p>レイヤ 4 のアイテムの優先度が最も高く、レイヤ 2 のアイテムの優先度が最も低くなります。</p> <p>トラフィックフローは 1 つの分類子にのみ分類できます。トラフィックフローが複数の分類ルールに一致する場合、本製品はマッチ順序に基づいてトラフィックを分類します。</p> <p>「Classifier 設定」(166 ページ) で設定した各ルールの重みに従って分類ルールが適用されるようにするには、「手動」を選択します。</p>				
ログ記録	<table><tr><td>有効</td><td>定義した時間間隔で、パケットがクラシファイアルールに一致した場合に、本製品がログを作成することを許可します。</td></tr><tr><td>間隔</td><td>クラシファイアルールに一致したパケットをカウントする時間 (秒) を設定します。 0 ～ 65535 の整数を入力します。0 に設定すると、ログを記録しません。</td></tr></table>	有効	定義した時間間隔で、パケットがクラシファイアルールに一致した場合に、本製品がログを作成することを許可します。	間隔	クラシファイアルールに一致したパケットをカウントする時間 (秒) を設定します。 0 ～ 65535 の整数を入力します。0 に設定すると、ログを記録しません。
有効	定義した時間間隔で、パケットがクラシファイアルールに一致した場合に、本製品がログを作成することを許可します。				
間隔	クラシファイアルールに一致したパケットをカウントする時間 (秒) を設定します。 0 ～ 65535 の整数を入力します。0 に設定すると、ログを記録しません。				

[ACL] Policy Rule

ACLのポリシールールを設定します。



ポリシールールを追加したり、選択した
ポリシールールを編集します。

→ [172ページ](#)

選択したポリシールールを削除します。

項目	内容
インデックス	このポリシーのインデックス番号が表示されます。
有効	このポリシーが有効かどうかが表示されます。
Name	このポリシーの説明的な名前が表示されます。
Classifier	このポリシーが適用される分類子の名前が表示されます。

■ ポリシールール追加／編集

Source & Destination

有効

OFF

Name

Classifier(s)

General Parameters

VLAN ID

1

出力ポート

1

優先度

0

DSCP

ToS

0

Metering Parameters

帯域幅

0

Kbps

Out of Profile DSCP

アクション

転送

変更なし

パケットを破棄

優先度

変更なし

802.1p優先度を設定

802.1p優先度を内部802.1p優先度で置換

Diffserv

変更なし

ToSフィルートを設定

Diffservコードポイントを設定

Outgoing

パケットをミラーポートに送信

パケットを出力ポートに送信

VLAN IDを変更

Metering

OFF

Out of profileアクション

パケットを破棄

DSCP値を変更

適用

クリア

キャンセル

● Source & Destination

項目	内容
有効	このポリシールールの有効／無効を切り替えます。
Name	識別のために名称を入力します。 (最大 32 文字まで。? (クエスチョンマーク) (パイプ) " (ダブルクォーテーション) , (コンマ) は使用不可)
Classifier(S)	このフィールドには、「Classifier 設定」(166 ページ) で設定したアクティブなクラシファイアが表示されます。 このポリシールールが適用される分類子を選択します。複数のクラシファイアを選択するには、SHIFT キーを押しながら同時に選択します。

● General Parameters

項目	内容
VLAN ID	1 ～ 4094 の VLAN ID を入力します。
出力ポート	送信ポートの番号を入力します。
優先度	優先レベルを選択します。

172

項目	内容
DSCP	DSCP (DiffServ Code Point) 番号を 0 ～ 63 の間で指定します。
ToS	TOS (Type Of Service) の優先度を選択します。

● Metering Parameters

項目	内容
帯域幅	帯域幅をキロビット / 秒 (kbps) で指定します。 (設定範囲: 1 ～ 1000000kbps)
Out of Profile DSCP	アウトオブプロファイルトラフィックの DSCP 番号を置き換える、または変更する場合は、新しい DSCP 番号 (0 ～ 63) を指定します。

● アクション

項目	内容
転送	変更なし パケットを転送します。
	パケットを破棄 パケットを破棄します。
優先度	変更なし 優先度設定を維持します。
	802.1p 優先度を設定 パケットの 802.1p 優先度フィールドを、「優先度」で設定した値で置き換え、パケットを指定されたキューに入れます。
	802.1p 優先度を設定 内部 802.1p 優先度 に置換 802.1p 優先度フィールドを内部の 802.1p 優先度の値に置き換えます。
Diffserv	変更なし パケットの ToS/DSCP フィールドを維持します。
	ToS フィールドを設定 IPv4 の DS フィールド 8 ビット全体を「Tos」設定した値で置き換えます。
	Diffserv コードポイントを設定 DSCP6 ビットだけを、DSCP で設定した値で置き換えます。
Outgoing	パケットをミラーポートに送信 パケットをミラーポートに送信します。
	パケットを出力ポートに送信 パケットをイグレスポートに送信します。
	VLAN ID を変更 パケットの VLAN ID を設定します。

項目	内容	
Metering	トラフィックフローの帯域幅制限を有効にしてから、プロファイル外のパケットに対して実行するアクションを設定します。	
	パケットを破棄	プロファイル外のトラフィックを破棄します。
	DSCP 値を変更	DSCP フィールドをプロファイル外 DSCP フィールドで指定された値で置き換えます。

項目	内容
適用	変更内容を本製品のランタイムメモリに保存します。 本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。
クリア	フィールドが工場出荷時のデフォルトにクリアされます。

アンチ ARP スキャン

ステータス

どのポートが信頼され、トラフィックを転送しているか、または無効になっているかを確認することができます。



項目	内容
アンチ ARP スキャン	本製品でアンチ ARP スキャンが有効か無効かを示します。
ポート	ポート番号が表示されます。
信頼済	ポートが信頼済かどうかを示します。信頼済みのポートでは Anti-ARP スキャンは実行されません。
状態	ポートが正常にトラフィックを転送できる状態 (転送中) か、無効な状態 (Err-Disable) かを示します。

ホストステータス

ブロックされたホストを表示し、特定のポートに接続されているホストのブロックを解除することができます。



■ フィルタリングされたホストをクリア

項目	内容
ポートリスト	ポート番号またはカンマとスペースで区切られた一連のポート番号を入力し、「クリア」をクリックすると、これらのポートに接続されているすべてのホストのブロックを解除します。

■ フィルタリングされたホスト

項目	内容
インデックス	ブロックされている IP アドレス（ホスト）のインデックス番号が表示されます。
ホスト IP	ブロックされたホストの IP アドレスが表示されます。
MAC アドレス	ブロックされたホストの MAC アドレスが表示されます。
VLAN	ブロックされたホストがどの VLAN にあるかを示す VLAN ID が表示されます。
ポート	ブロックされたホストが接続されているポート番号が表示されます。
状態	このホストからの ARP リクエストレートがしきい値を超えている場合、Err-Disable と表示されます。転送中のホストは表示されません。

設定

アンチ ARP スキャン機能の有効化および設定をおこないます。

項目	内容
有効	アンチ ARP スキャン機能の有効／無効を切り替えます。
ポートしきい値	ポートがブロックされるまでに許容される 1 秒あたりの最大パケット数を入力します。 (設定範囲：2 ～ 255) (初期値：100pps) 受信パケット数がしきい値を超えると、ポートは Err-Disable 状態になります。
ホストしきい値	ホストがブロックされる前に許可される ARP 要求パケットの最大数を入力します。 (設定範囲：2 ～ 100) (初期値：10pps) ポートのしきい値は、ホストのしきい値よりも大きく設定する必要があります。 ホストのしきい値は、全ホストに対するグローバル閾値レートです。ホストのレートがしきい値を超えている場合、そのホストは MAC アドレスフィルタを使用してブロックされます。ブロックされたホストは、MAC エージング時間が経過すると自動的に解除されます。
ポート	ポート番号が表示されます。 「*」の行を変更すると、すべてのポートに変更が適用されます。
信頼状態	ポートの「Untrusted」または「Trusted」を選択します。アンチ ARP スキャンは Trusted ホストでは実行されません。
適用	変更内容を本製品のランタイムメモリに保存します。 本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。

信頼ホスト

信頼できるホストを作成または削除します。



信頼ホストを追加したり、選択した信頼ホストを編集します。

→ [179 ページ](#)

選択した信頼ホストを削除します。

項目	内容
インデックス	エントリーのインデックス番号が表示されます。
名前	このエントリーの説明的な名前が表示されます。
ホスト IP	信頼済みホストの IP アドレスが表示されます。
マスク	信頼済みホストのサブネットマスクが表示されます。

■ 信頼ホストの追加／編集

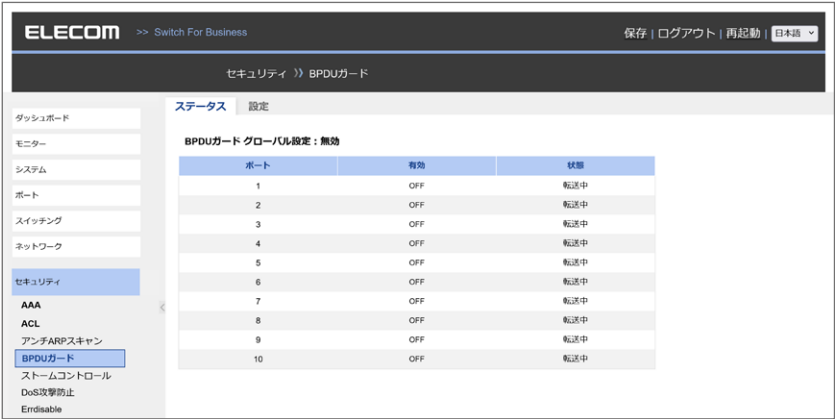
名前	<input type="text"/>
ホストIP	<input type="text"/>
マスク	<input type="text"/>
<div>適用 クリア キャンセル</div>	

項目	内容
名前	この信頼ホストの名前を入力します。 (最大 32 文字まで。? (クエスチョンマーク) (パイプ) ' (フォーテーション) " (ダブルフォーテーション) , (コンマ) は使用不可)
ホスト IP	ホストの IP アドレスを入力します。
マスク	信頼できるホストは、IP アドレスのサブネットで構成されている場合があります。 サブネットマスクを入力して、単一のホストまたはホストのサブネットを作成します。
適用	変更内容を本製品のランタイムメモリに保存します。 本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。
クリア	フィールドが工場出荷時のデフォルトにクリアされます。

BPDUGuard

Status

This product displays whether BPDUGuard is enabled or not, and the status of the port.



項目	内容
BPDUGuard グローバル設定	本製品で BPDUGuard が有効か無効かを示します。
ポート	ポート番号が表示されます。
有効	ポートが BPDUGuard が有効かどうかを示します。
状態	ポートがシャットダウン (Err-disable) か、パケット送信可能 (転送中) かが表示されます。

設定

BPDU 機能の有効化および設定をおこないます。



項目	内容
有効	BPDU 機能の有効／無効を切り替えます。
ポート	ポート番号が表示されます。 「*」の行を変更すると、すべてのポートに変更が適用されます。
有効	チェックを入れると、このポートで BPDU ガード機能が有効になります。 本製品は、ポートで BPDU フレームを受信した場合、このポートをシャットダウンします。
適用	変更内容を本製品のランタイムメモリに保存します。 本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。

ストームコントロール

ポートが 1 秒間に受信するブロードキャストパケット、マルチキャストパケット、宛先検索失敗 (DLF) パケットの数に制限をかけます。

ELECOM >> Switch For Business

保存 | ログアウト | 再起動 | 日本語

セキュリティ >> ストームコントロール

ダッシュボード
モニター
システム
ポート
スイッチング
ネットワーク
セキュリティ
AAA
ACL
アンチARPスキャン
BPDUガード
ストームコントロール
DoS攻撃防止
Errdisable
IPv4ソースガード
IPv6ソースガード
ポート認証
ポートセキュリティ

ストームコントロール

有効 OFF

ポート	ブロードキャスト (パケット/秒)	マルチキャスト (パケット/秒)	DLF (パケット/秒)
*	<input type="checkbox"/> <input type="text"/>	<input type="checkbox"/> <input type="text"/>	<input type="checkbox"/> <input type="text"/>
1	<input type="checkbox"/> <input type="text"/>	<input type="checkbox"/> <input type="text"/>	<input type="checkbox"/> <input type="text"/>
2	<input type="checkbox"/> <input type="text"/>	<input type="checkbox"/> <input type="text"/>	<input type="checkbox"/> <input type="text"/>
3	<input type="checkbox"/> <input type="text"/>	<input type="checkbox"/> <input type="text"/>	<input type="checkbox"/> <input type="text"/>
4	<input type="checkbox"/> <input type="text"/>	<input type="checkbox"/> <input type="text"/>	<input type="checkbox"/> <input type="text"/>
5	<input type="checkbox"/> <input type="text"/>	<input type="checkbox"/> <input type="text"/>	<input type="checkbox"/> <input type="text"/>
6	<input type="checkbox"/> <input type="text"/>	<input type="checkbox"/> <input type="text"/>	<input type="checkbox"/> <input type="text"/>
7	<input type="checkbox"/> <input type="text"/>	<input type="checkbox"/> <input type="text"/>	<input type="checkbox"/> <input type="text"/>
8	<input type="checkbox"/> <input type="text"/>	<input type="checkbox"/> <input type="text"/>	<input type="checkbox"/> <input type="text"/>
9	<input type="checkbox"/> <input type="text"/>	<input type="checkbox"/> <input type="text"/>	<input type="checkbox"/> <input type="text"/>
10	<input type="checkbox"/> <input type="text"/>	<input type="checkbox"/> <input type="text"/>	<input type="checkbox"/> <input type="text"/>

適用 キャンセル

項目	内容
有効	トラフィックストーム制御機能の有効／無効を切り替えます。
ポート	ポート番号が表示されます。 「*」の行を変更すると、すべてのポートに変更が適用されます。
ブロードキャスト (パケット / 秒)	ポートが 1 秒間に受信できるブロードキャスト・パケット数を指定します。 チェックを入れると有効になります。
マルチキャスト (パケット / 秒)	ポートが 1 秒間に受信できるマルチキャストパケット数を指定します。 チェックを入れると有効になります。
DLF (パケット / 秒)	ポートが 1 秒間に受信できる宛先検索失敗 (DLF) パケット数を指定します。 チェックを入れると有効になります。
適用	変更内容を本製品のランタイムメモリに保存します。 本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。

Dos 攻撃防止

Dos 攻撃防止の設定をします。

ELECOM >> Switch For Business

保存 | ログアウト | 再起動 | 日本語

セキュリティ >> DoS攻撃防止

ダッシュボード

モニター

システム

ポート

スイッチング

ネットワーク

セキュリティ

AAA

ACL

アンチARPスキャン

BPDUGuard

ストームコントロール

DoS攻撃防止

ErrDisable

IPv4ソースガード

IPv6ソースガード

ポート認証

ポートセキュリティ

管理

DoS攻撃防止

DoS攻撃防止	有効	パラメータ
*	<input type="checkbox"/>	
DMAC == SMAC	<input type="checkbox"/>	
Ping of Death Attack	<input type="checkbox"/>	
Land Attack	<input type="checkbox"/>	
ICMP Fragment Packets	<input type="checkbox"/>	
UDP Blat Attack	<input type="checkbox"/>	
TCP Blat Attack	<input type="checkbox"/>	
TCP SYN (SPORT < 1024)	<input type="checkbox"/>	
TCP Null Scan Attack	<input type="checkbox"/>	
TCP Xmas Scan Attack	<input type="checkbox"/>	
TCP SYN-FIN Attack	<input type="checkbox"/>	
TCP SYN-RST Attack	<input type="checkbox"/>	
TCP Fragment (Offset == 1)	<input type="checkbox"/>	
TCP Min Header Length	<input type="checkbox"/>	20 バイト (0~31, デフォルト 20)
Smurf Attack	<input type="checkbox"/>	0 ネットマスク長 (0~32, デフォルト0)
IPv6最小フラグメントサイズ	<input type="checkbox"/>	1240 バイト (0~65535, デフォルト1240)
Ping最大パケットサイズ	<input type="checkbox"/> ICMPv4 <input type="checkbox"/> ICMPv6	512 バイト (0~65535, デフォルト512)

適用 キャンセル

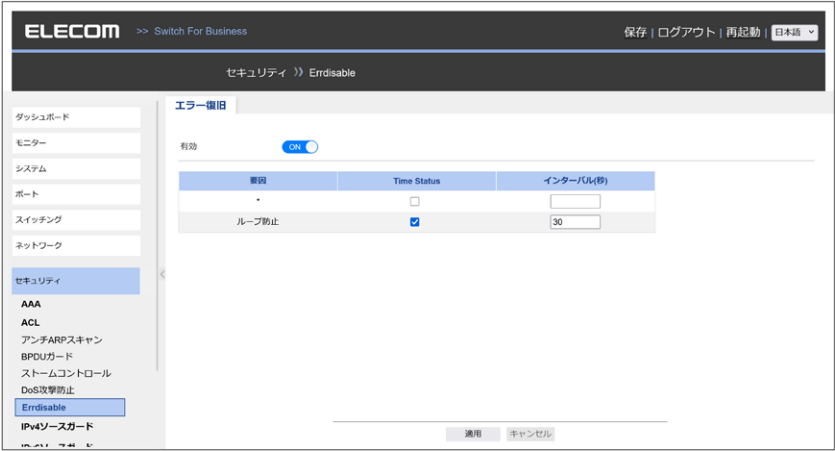
項目	内容
*	すべてのオプションを一括して有効／無効にします。
DMAC == SMAC	宛先 MAC =送信元 MAC というフレームを破棄します。
Ping of Death Attack	再組立てで巨大化する過大 ICMP を拒否します。
Land Attack	送信元 IP =宛先 IP (+同一ポート) の不正 SYN 等を拒否します。
ICMP Fragment Packets	断片化 ICMP を拒否します。
UDP Blat Attack	高レート の UDP 連打を検知して遮断します。
TCP Blat Attack	高レート の TCP 連打を遮断します。
TCP SYN (SPORT < 1024)	送信元ポート <1024 の SYN を不正とみなし拒否します。
TCP Null Scan Attack	フラグ無し (NULL) スキャンのパケットを拒否します。
TCP Xmas Scan Attack	FIN+URG+PSH 等の Xmas ツリースキャンを拒否します。
TCP SYN-FIN Attack	SYN と FIN 同時の不正フラグを拒否します。

183

項目	内容
TCP SYN-RST Attack	SYN と RST 同時の不正フラグを拒否します。
TCP Fragment (Offset == 1)	フラグメントオフセット=1 を拒否します。
TCP Min Header Length	TCP ヘッダの最小長を指定値未満なら拒否します。 (設定範囲: 0 ~ 31) (初期値: 20)
Smurf Attack	ブロードキャスト ICMP (送信元スプーフ) 対策として、ネットマスク長でブロードキャスト範囲を判定します。 (設定範囲: 0 ~ 32) (初期値: 0)
IPv6 最小フラグメントサイズ	IPv6 の極小フラグメントを拒否します。 (設定範囲: 0 ~ 65535) (初期値: 1240)
Ping 最大パケットサイズ	Echo 要求の上限サイズを超えるものを拒否します。 (設定範囲: 0 ~ 65535) (初期値: 512)
適用	変更内容を本製品のランタイムメモリに保存します。 本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。

Errdisable

自動復旧機能の設定をします。



項目	内容
有効	自動復旧機能の有効／無効を切り替えます。
要因	設定するエラーの要因が表示されます。 「*」はすべての要因に対して設定を反映します。
Time Status	チェックを入れると、「インターバル」で設定した時間経過後に、自動的に復旧を試みます。
インターバル (秒)	エラーが出てから再有効化を試すまでの時間を入力します。(初期値：30 秒)
適用	変更内容を本製品のランタイムメモリに保存します。 本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。

[IPv4 ソースガード] IPv4 ソースガード

IP ソースガード

DHCP snoopingとARP インспекションの現在のバインディングを確認します。



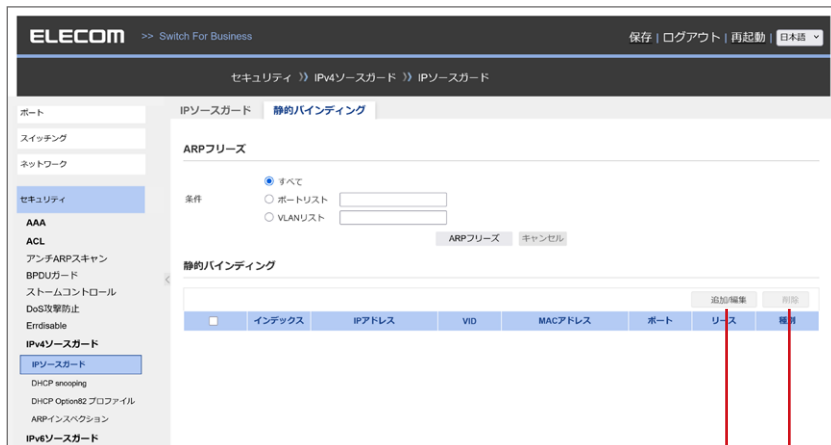
項目	内容				
インデックス	各バインディングの連番が表示されます。				
IP アドレス	バインディングの MAC アドレスに割り当てられた IP アドレスが表示されます。				
VID	バインディングのソース VLAN ID が表示されます。				
MAC アドレス	バインディングのソース MAC アドレスが表示されます。				
ポート	バインディングのポート番号が表示されます。 このフィールドが空白の場合、バインディングはすべてのポートに適用されます。				
リース	バインディングが何日、何時間、何分、何秒間有効かが表示されます。 例えば、2d3h4m5s は、バインディングが 2 日、3 時間、4 分、5 秒間有効であることを意味します。 バインディングが常に有効な場合（静的バインディングなど）は、無限大を示します。				
種別	本製品がバインディングをどのように学習したかが表示されます。 <table><tr><td>static</td><td>管理者が手動で提供した情報から学習されたバインディングです。</td></tr><tr><td>dhcp-snooping</td><td>DHCP パケットをスヌープすることで学習されたバインディングです。</td></tr></table>	static	管理者が手動で提供した情報から学習されたバインディングです。	dhcp-snooping	DHCP パケットをスヌープすることで学習されたバインディングです。
static	管理者が手動で提供した情報から学習されたバインディングです。				
dhcp-snooping	DHCP パケットをスヌープすることで学習されたバインディングです。				

静的バインディング

DHCP snoopingとARP インспекションの静的バインディングを管理します。

MEMO

静的バインディングは、MAC アドレスとVLAN IDによって一意に識別されます。各MAC アドレスとVLAN IDは、1つのスタティックバインディングにのみ設定できます。既存の静的バインディングと同じMAC アドレスとVLAN IDを持つ静的バインディングを作成しようすると、新しい静的バインディングが元の静的バインディングを置き換えます。



静的バインディングを追加したり、選択した静的バインディングを編集します。

→ [189ページ](#)

選択した静的バインディングを削除します。

■ ARP フリーズ

ARP フリーズは、本製品のバインディングテーブルが一杯になるまで、現在のARP エントリ（動的に学習されたARP エントリまたは静的ARP エントリ）から静的バインディングを自動的に作成する機能です。

ARP フリーズ機能を使用する前に、「ネットワーク」－「ARP 設定」－「ARP ラーニング」（[158ページ](#)）画面でARP ラーニングモードを「ARP 要求」に設定する必要があります。

項目	内容	
条件	すべて	これを選択して「ARP フリーズ」をクリックすると、本製品は現在のすべての ARP エントリを静的バインディングテーブルに自動的に追加します。
	ポートリスト	ポート番号をカンマ区切りで入力します。 複数のポートを（スペースなし）カンマ (,) またはハイフン (-) で区切って入力し、範囲を指定できます。例えば、ポート 3、4、5 には「3-5」と入力します。ポート 3、5、7 には「3,5,7」と入力します。 指定したポートで学習した ARP エントリは、「ARP フリーズ」をクリックした後、静的バインディングテーブルに追加されます。
	VLAN リスト	VLAN の ID 番号（カンマ区切り）を入力します。「ARP フリーズ」をクリックすると、指定した VLAN の ARP エントリが静的バインディングテーブルに追加されます。

■ 静的バインディング

項目	内容	
インデックス	各バインディングの連番が表示されます。	
IP アドレス	バインディングの MAC アドレスに割り当てられた IP アドレスが表示されます。	
VID	バインディングのソース VLAN ID が表示されます。	
MAC アドレス	バインディングのソース MAC アドレスが表示されます。	
ポート	バインディングのポート番号が表示されます。 このフィールドが空白の場合、バインディングはすべてのポートに適用されます。	
リース	バインディングが何日、何時間、何分、何秒間有効かが表示されます。 例えば、2d3h4m5s は、バインディングが 2 日、3 時間、4 分、5 秒間有効であることを意味します。 バインディングが常に有効な場合（静的バインディングなど）は、無限大を示します。	
種別	本製品がバインディングをどのように学習したかが表示されます。	
	static	管理者が手動で提供した情報から学習されたバインディングです。

■ IPv4 ソースガード静的バインディングの追加／編集

IPアドレス

VLAN

MACアドレス

☒ 任意

☐

ポート

☒ 任意

☐

適用

クリア

キャンセル

項目	内容
IP アドレス	バインディングの MAC アドレスに割り当てられた IP アドレスを入力します。
VLAN	バインディングのソース VLAN ID を入力します。
MAC アドレス	バインディングのソース MAC アドレスを入力します。 このバインディングがすべての MAC アドレスに適用される場合は、「任意」を選択します。
ポート	バインディングのポートを指定します。 このバインディングにポートが 1 つある場合は、下のラジオボタンを選択し、右側のフィールドにポート番号を入力します。 このバインディングがすべてのポートに適用される場合は、「任意」を選択します。
適用	変更内容を本製品のランタイムメモリに保存します。 本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。
クリア	フィールドが工場出荷時のデフォルトにクリアされます。

[IPv4 ソースガード] DHCP snooping

ステータス

DHCP snooping データベースに関するさまざまな統計情報を確認します。

ELECOM >> Switch For Business

保存 | ログアウト | 再起動 | 日本語

セキュリティ >> IPv4ソースガード >> DHCP snooping

ポート
スイッチング
ネットワーク
セキュリティ
AAA
ACL
アンチARPスキャン
BPDUガード
ストームコントロール
DoS攻撃防止
Ermisable
IPv4ソースガード
IPv4ソースガード
DHCP snooping
DHCP Option82 プロファイル
ARPインスパクション
IPv6ソースガード
ポート認証
ポートセキュリティ
管理

ステータス
設定
ポート設定
VLAN設定
VLANポート設定

DHCP snooping

データベースステータス		データベース詳細	
エージェントURL		最初のアクセス成功	なし
書き込み遅延タイマー	300	最後に無視されたバインディングカウンター	
中止タイマー	300	バインド衝突	0
エージェント実行中	なし	無効なインターフェース	0
遅延タイマーの期限切れ	実行されていません	解析失敗	0
中止タイマーの期限切れ	実行されていません	リース期限切れ	0
最終成功時間	なし	サポートされていない VLAN	0
最終失敗時間	なし	最後に無視された時刻	なし
最終失敗理由	失敗記録なし	無視されたバインディングの合計カウンター	
カウンター		バインド衝突	0
合計試行回数	0	無効なインターフェース	0
起動失敗	0	解析失敗	0
成功した転送	0	リース期限切れ	0
失敗した転送	0	サポートされていない VLAN	0
成功した読み取り	0		
失敗した読み取り	0		
書き込み成功	0		
書き込み失敗	0		

■ データベースステータス

項目	内容
エージェント URL	DHCP snooping データベースの場所が表示されます。
書き込み遅延タイマー	本製品が DHCP snooping データベースの特定の更新を完了してからあきらめるまでの時間（秒）が表示されます。
中止タイマー	現在のバインディングが変更された後、本製品が DHCP snooping データベースの更新を待機する時間（秒）が表示されます。
エージェント実行中	現在の DHCP snooping データベースの更新またはアクセスの状態が表示されます。
遅延タイマーの期限切れ	本製品が現在の更新をあきらめるまでの時間（秒）が表示されます。 現在 DHCP snooping データベースを更新していない場合は「実行されていません」と表示されます。

項目	内容																
中止タイマーの期限切れ	本製品が DHCP snooping データベースを再度更新するタイミング（秒）が表示されます。 前回の更新から現在のバインディングに変更がない場合は、「実行されています」と表示されます。																
最終成功時間	本製品が最後に DHCP snooping データベースの更新に成功した時刻が表示されます。																
最終失敗時間	本製品が最後に DHCP snooping データベースの更新に失敗した時刻が表示されます。																
最終失敗理由	本製品が DHCP snooping データベースの更新に失敗した理由が表示されます。																
カウンター	<table border="1"> <tr> <td>合計試行回数</td><td>本製品が何らかの理由で DHCP snooping データベースへのアクセスを試行した回数が表示されます。</td></tr> <tr> <td>起動失敗</td><td>本製品の起動時または DHCP snooping データベースに新しい URL を設定したときに、DHCP snooping データベースの作成または読み出しに失敗した回数が表示されます。</td></tr> <tr> <td>成功した転送</td><td>本製品が DHCP snooping データベースのバインディングの読み込みまたは更新に成功した回数が表示されます。</td></tr> <tr> <td>失敗した転送</td><td>本製品が DHCP snooping データベースからバインディングを読み出せなかった回数、または DHCP snooping データベース内のバインディングを更新できなかった回数。</td></tr> <tr> <td>成功した読み取り</td><td>本製品が DHCP snooping データベースからバインディングの読み出しに成功した回数が表示されます。</td></tr> <tr> <td>失敗した読み取り</td><td>本製品が DHCP snooping データベースからバインディングを読み取れなかった回数が表示されます。</td></tr> <tr> <td>書き込み成功</td><td>本製品が DHCP snooping データベースのバインディングの更新に成功した回数が表示されます。</td></tr> <tr> <td>書き込み失敗</td><td>本製品が DHCP snooping データベースのバインディングを更新できなかった回数が表示されます。</td></tr> </table>	合計試行回数	本製品が何らかの理由で DHCP snooping データベースへのアクセスを試行した回数が表示されます。	起動失敗	本製品の起動時または DHCP snooping データベースに新しい URL を設定したときに、DHCP snooping データベースの作成または読み出しに失敗した回数が表示されます。	成功した転送	本製品が DHCP snooping データベースのバインディングの読み込みまたは更新に成功した回数が表示されます。	失敗した転送	本製品が DHCP snooping データベースからバインディングを読み出せなかった回数、または DHCP snooping データベース内のバインディングを更新できなかった回数。	成功した読み取り	本製品が DHCP snooping データベースからバインディングの読み出しに成功した回数が表示されます。	失敗した読み取り	本製品が DHCP snooping データベースからバインディングを読み取れなかった回数が表示されます。	書き込み成功	本製品が DHCP snooping データベースのバインディングの更新に成功した回数が表示されます。	書き込み失敗	本製品が DHCP snooping データベースのバインディングを更新できなかった回数が表示されます。
合計試行回数	本製品が何らかの理由で DHCP snooping データベースへのアクセスを試行した回数が表示されます。																
起動失敗	本製品の起動時または DHCP snooping データベースに新しい URL を設定したときに、DHCP snooping データベースの作成または読み出しに失敗した回数が表示されます。																
成功した転送	本製品が DHCP snooping データベースのバインディングの読み込みまたは更新に成功した回数が表示されます。																
失敗した転送	本製品が DHCP snooping データベースからバインディングを読み出せなかった回数、または DHCP snooping データベース内のバインディングを更新できなかった回数。																
成功した読み取り	本製品が DHCP snooping データベースからバインディングの読み出しに成功した回数が表示されます。																
失敗した読み取り	本製品が DHCP snooping データベースからバインディングを読み取れなかった回数が表示されます。																
書き込み成功	本製品が DHCP snooping データベースのバインディングの更新に成功した回数が表示されます。																
書き込み失敗	本製品が DHCP snooping データベースのバインディングを更新できなかった回数が表示されます。																

■ データベース詳細

項目	内容
最初のアクセス成功	本製品が DHCP snooping データベースに初めてアクセスした回数が表示されます。

項目	内容	
最後に無視されたバインディングカウンター	バインド衝突	同じ MAC アドレスおよび VLAN ID のバインディングがすでに存在するため、本製品がバインディングを無視した回数が表示されます。
	無効なインターフェース	ポート番号がトラステッドインタフェースであるか、または存在しないため、本製品が無視したバインディング数が表示されます。
	解析失敗	本製品が DHCP バインディングデータベースのバインディングを理解できなかったために無視したバインディングの数が表示されます。
	リース期限切れ	リース期間がすでに終了しているため、本製品が無視したバインディング数が表示されます。
	サポートされていない VLAN	VLAN ID が存在しないため、本製品が無視したバインディング数が表示されます。
	最後に無視された時刻	本製品が DHCP バインディングデータベースから何らかの理由でバインディングを無視した最後の時間が表示されます。
無視されたバインディングの合計カウンター	バインド衝突	本製品が同じ MAC アドレスおよび VLAN ID のバインディングをすでに持っていたために無視したバインディング数が表示されます。
	無効なインターフェース	ポート番号がトラステッドインタフェースであるか、または存在しないため、本製品が無視したバインディング数が表示されます。
	解析失敗	本製品が DHCP バインディングデータベースのバインディングを理解できなかったために無視したバインディングの数が表示されます。
	リース期限切れ	リース期間がすでに終了しているため、本製品が無視したバインディング数が表示されます。
	サポートされていない VLAN	VLAN ID が存在しないため、本製品が無視したバインディング数が表示されます。

設定

本製品でDHCP snoopingを有効化したり、DHCP snoopingデータベースを設定します

■ DHCP snooping設定

項目	内容
有効	DHCP snooping 機能の有効／無効を切り替えます。 特定の VLAN で DHCP snooping を有効にし、信頼できるポートを指定する必要があります。 DHCP が有効で、信頼できるポートがない場合、DHCP リクエストは成功しません。
DHCP VLAN	特定の VLAN 上の DHCP サーバに DHCP パケットを転送する場合は、VLAN ID を選択します。 「VLAN 設定」(217 ページ) で DHCP snooping を有効にする必要があります。 DHCP パケットを特定の VLAN に転送したくない場合は「無効」を選択します。

■ データベース

項目	内容
エージェント URL	DHCP snooping データベースの場所を以下の形式で入力します。 tftp://{ドメイン名または IP アドレス}/ディレクトリ(該当する場合)/ファイル名; (例) tftp:// 192.168.10.1/database.txt (? (クエスチョンマーク) (パイプ) " (ダブルクォーテーション), (コンマ) は使用不可)

項目	内容
タイムアウト時間	本製品が DHCP snooping データベースの特定の更新を完了させてからあきらめるまでの時間を入力します。 (設定範囲: 10 ~ 65535 秒) (初期値: 300 秒)
書き込み遅延間隔	DHCP snooping データベースの更新後、現在のバインディングが初めて変更された場合に、本製品がデータベースの更新を待機する時間を入力します。 (設定範囲: 10 ~ 65535 秒) (初期値: 300 秒) 次の更新がスケジュールされると、現在のバインディングの追加変更は自動的に次の更新に含まれます。
DHCP snooping URL 更新	DHCP snooping データベースの場所を入力し、本製品に読み込ませたい場合は「更新」をクリックします。 これを使用すると、「エージェント URL」指定したデータベースとは異なる DHCP snooping データベースからダイナミックバインディングをロードできます。 本製品は DHCP snooping データベースから動的バインディングをロードするとき、現在の動的バインディングを最初に破棄しません。 競合がある場合、本製品は動的バインディングを揮発性メモリに保持し、「DHCP snooping」[ステータス] 画面の「バインド衝突」カウンタを更新します。
適用	変更内容を本製品のランタイムメモリに保存します。 本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。

ポート設定

ポートをDHCP snoopingの信頼済みポートにするか、非信頼ポートにするかを指定します。

注意

DHCP snoopingが有効になっていても、信頼できるポートがない場合、DHCP要求はDHCPサーバに届きません

ポート	サーバー信頼状態	レート (pps)
*	Untrusted ▼	<input type="text"/>
1	Untrusted ▼	<input type="text" value="0"/>
2	Untrusted ▼	<input type="text" value="0"/>
3	Untrusted ▼	<input type="text" value="0"/>
4	Untrusted ▼	<input type="text" value="0"/>
5	Untrusted ▼	<input type="text" value="0"/>
6	Untrusted ▼	<input type="text" value="0"/>
7	Untrusted ▼	<input type="text" value="0"/>
8	Untrusted ▼	<input type="text" value="0"/>
9	Untrusted ▼	<input type="text" value="0"/>
10	Untrusted ▼	<input type="text" value="0"/>

項目	内容
ポート	<p>ポート番号が表示されます。</p> <p>「*」の行を変更すると、すべてのポートに変更が適用されます。</p>
サーバー信頼状態	<p>このポートが信頼できるポート (Trusted) か信頼できないポート (Untrusted) かを選択します。</p> <p>Trusted ポートは DHCP サーバまたは他のスイッチに接続されており、本製品は DHCP パケットの到達率が高すぎる場合にのみ、Trusted ポートからの DHCP パケットを破棄します。</p> <p>Untrusted ポートは加入者に接続されており、本製品は以下の場合に Untrusted ポートからの DHCP パケットを廃棄します。</p> <ul style="list-style-type: none"> ● パケットが DHCP サーバパケット（例えば、OFFER、ACK、または NACK）である。 ● パケットの送信元 MAC アドレスと送信元 IP アドレスが現在のバインディングのどれとも一致しない。 ● パケットが RELEASE または DECLINE パケットで、ソース MAC アドレスとソースポートが現在のバインディングのいずれとも一致しない。 ● DHCP パケットの到着レートが高すぎる。

項目	内容
レート (pps)	本製品が各ポートから毎秒受信する DHCP パケットの最大数を指定します。 (設定範囲: 1 ~ 2048) 本製品はそれ以上の DHCP パケットを破棄します。 この制限を無効にするには 0 を入力します。

VLAN 設定

各 VLAN で DHCP snooping を有効にし、本製品が各 VLAN の DHCP サーバに中継する DHCP 要求に DHCP リレーエージェントオプション 82 情報を追加するかどうかを指定します。

項目	内容
VID で VLAN を検索	管理する VLAN ID を入力し、「検索」をクリックすると、指定した範囲の VLAN が下のテーブルに表示されます。 個々の VLAN を区切るにはカンマ (,) を、VLAN の範囲を示すにはハイフン (-) を使用します。(例) 「3,4」「3-9」
VLAN 数	VLAN の検索結果の数が表示されます。
VID	上記で指定した範囲の各 VLAN の VLAN ID です。VLAN を設定した場合、設定はすべての VLAN に適用されます。

項目	内容
有効／無効	VLAN で DHCP snooping を有効にする場合は、「有効」を選択します。 なお、本製品で DHCP snooping を有効にし、Trusted Port を指定する必要があります。 DHCP snooping を有効にしても、Trusted ポートがない場合、本製品はすべての DHCP リクエストをドロップします
DHCP Option32 プロファイル	本製品が指定された VLAN の全ポートに適用する定義済みの DHCP オプション 82 プロファイルを選択します。 本製品は、プロファイルで指定された情報（スロット番号、ポート番号、VLAN ID、システム名など）を DHCP VLAN (指定されている場合) または VLAN にブロードキャストする DHCP リクエストに追加します。 DHCP VLAN は、「セキュリティ」－「IPv4 ソースガード」－「DHCP snooping」－「設定」(193 ページ) 画面で指定します。
適用	変更内容を本製品のランタイムメモリに保存します。 本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。

VLAN ポート設定

特定のポートに異なる DHCP オプション 82 プロファイルを適用します。



DHCP snooping VLAN ポートを追加したり、選択した DHCP snooping VLAN ポートを編集します。

→ [198 ページ](#)

選択した DHCP snooping VLAN ポートを削除します。

項目	内容
インデックス	エントリのインデックス番号が表示されます。
VID	ポートが属する VLAN が表示されます。
ポート	本製品が設定を適用するポートが表示されます。
プロファイル名	本製品がポートに適用する DHCP オプション 82 プロファイルが表示されます。

■ DHCP snooping VLAN ポートの追加／編集

VID

ポート

DHCP Option82 プロファイル

default1 ▼

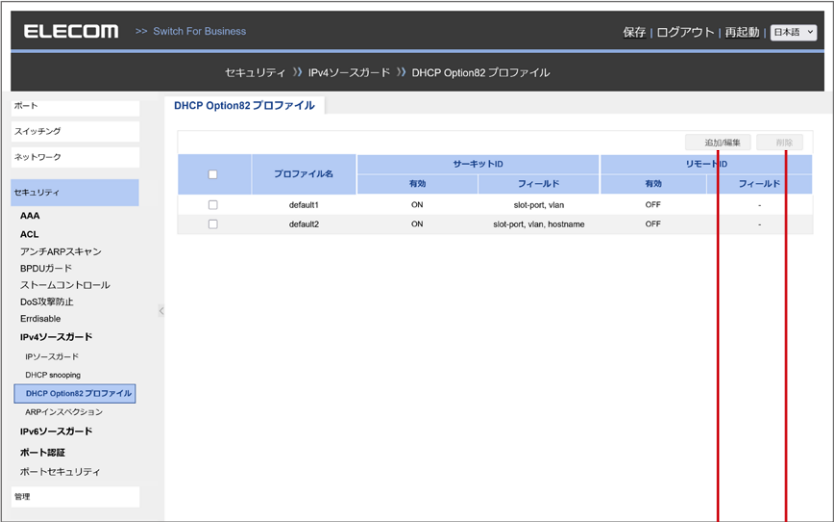
適用

クリア

キャンセル

項目	内容
VID	VLAN の ID 番号を入力します。
ポート	指定した DHCP オプション 82 プロファイルを適用するポートの数を入力します。 複数のポートをカンマ (,) またはハイフン (-) で区切って入力できます。 たとえば、ポート 3、4、5 には「3-5」と入力します。ポート 3、5、7 には「3,5,7」と入力します。
DHCP Option82 プロファイル	この VLAN 内の指定されたポートに本製品が適用する定義済みの DHCP オプション 82 プロファイルを選択します。 本製品は、プロファイルで指定された情報（スロット番号、ポート番号、VLAN ID、システム名など）を DHCP VLAN（指定されている場合）または VLAN にブロードキャストする DHCP リクエストに追加します。 DHCP VLAN は、「セキュリティ」－「IPv4 ソースガード」－「DHCP snooping」－「設定」(193 ページ) 画面で指定します。 注意：ここで選択したプロファイルは、「VLAN 設定」(196 ページ) 画面で選択したプロファイルよりも優先されます。
適用	変更内容を本製品のランタイムメモリに保存します。 本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。
クリア	フィールドが工場出荷時のデフォルトにクリアされます。

[IPv4 ソースガード] DHCP Option82 プロファイル



DHCP Option82 プロファイルを追加したり、選択した DHCP Option82 プロファイルを編集します。

→ [200 ページ](#)

選択した DHCP Option82 プロファイルを削除します。

項目	内容	
プロファイル名	プロファイルの名称が表示されます。	
サーキット ID	スイッチ（リレーエージェント）固有の情報を含む、サーキット ID サブオプションが表示されます。	
	有効	サーキット ID サブオプションがクライアントの DHCP リクエストに追加されているかどうかが表示されます。
	フィールド	サーキット ID サブオプションに含まれる情報が表示されます。
リモート ID	スイッチ（リレーエージェント）を識別する情報を含む、リモート ID サブオプションが表示されます。	
	有効	リモート ID サブオプションがクライアントの DHCP リクエストに追加されているかどうかが表示されます。
	フィールド	リモート ID サブオプションに含まれる情報が表示されます。

■ DHCP Option82 プロファイルの追加／編集

プロファイル名

サーキットID

☐ 有効

☐ slot-port ☐ VLAN ☐ ホスト名

任意文字列

リモートID

☐ 有効

☐ MACアドレス

任意文字列

適用

クリア

キャンセル

項目	内容
プロファイル名	プロファイル名を入力します。 (最大 32 文字まで。? (クエスチョンマーク) (パイプ) ' (クォーテーション) " (ダブルクォーテーション) , (コンマ) は使用不可)
サーキット ID	中継機能を持つスイッチ固有の情報が含まれるように、サーキット ID サブオプションを設定します。
	<div><div>有効</div><div>選択すると、スイッチがサーキット ID サブオプションを、クライアントの DHCP リクエストに追加して DHCP サーバーへ中継します。</div></div>
	<div><div>slot-port</div><div>選択すると、DHCP クライアントが接続されているポート番号をスイッチが追加します。</div></div>
	<div><div>VLAN</div><div>選択すると、そのポートが所属する VLAN の ID をスイッチが追加します。</div></div>
	<div><div>ホスト名</div><div>選択すると、クライアント DHCP リクエストに、「システム」 — 「一般設定」で設定したシステム名が追加されます。</div></div>
	<div><div>任意文字列</div><div>スイッチがクライアント DHCP リクエストに追加する任意の文字列を、入力します。 (最大 64 文字まで。? (クエスチョンマーク) (パイプ) ' (クォーテーション) " (ダブルクォーテーション) , (コンマ) は使用不可)</div></div>
リモート ID	中継機能を持つスイッチを識別できる情報が含まれるように、リモート ID サブオプションを設定します。
適用	変更内容を本製品のランタイムメモリに保存します。 本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。
クリア	フィールドが工場出荷時のデフォルトにクリアされます。

[IPv4 ソースガード] ARP インспекション

ステータス

本製品が不正な ARP パケットを識別したために作成された MAC アドレスフィルタの現在のリストを確認できます。



項目	内容
バインド数	本製品が不正な ARP パケットを識別したために作成された MAC アドレスフィルタの現在の数です。
インデックス	各 MAC アドレスフィルタの連番が表示されます。
MAC アドレス	MAC アドレスフィルタの送信元 MAC アドレスが表示されます。
VID	MAC アドレスフィルタのソース VLAN ID が表示されます。
ポート	廃棄された ARP パケットの送信元ポートが表示されます。
有効期限 (秒)	MAC アドレスフィルタが本製品に残っている時間 (秒) が表示されます。 手動でレコードを削除 (Delete) することもできます。
削除	選択したエントリを削除します。

VLAN ステータス

各 VLAN の ARP パケットに関するさまざまな統計情報を確認できます。



項目	内容
VID で VLAN を検索	VLAN ID を入力し、「検索」をクリックすると、指定した範囲の VLAN が下のテーブルに表示されます。 個々の VLAN を区切るにはカンマ (,) を、VLAN の範囲を示すにはハイフン (-) を使用します。(例) 「3,4」 「3-9」
VLAN 数	VLAN の検索結果の数が表示されます。
VID	上記で指定した範囲の各 VLAN の VLAN ID です。
受信済	本製品が前回再起動してから、VLAN から受信した ARP パケットの総数が表示されます。
リクエスト	本製品が前回再起動してから VLAN から受信した ARP Request パケットの総数が表示されます。
応答	本製品が最後に再起動してから、VLAN から受信した ARP Reply パケットの総数が表示されます。
転送済	本製品が最後に再起動してから、VLAN に対して転送した ARP パケットの総数が表示されます。
ドロップ数	本製品が最後にリスタートしてから、VLAN に対して廃棄した ARP パケットの総数が表示されます。

ログステータス

ARP パケットによって生成され、まだ syslog サーバーに送信されていないログメッセージを確認します。



項目	内容
ログステータステーブルのクリア	「クリア」をクリックすると、ARP パケットによって生成され、まだ syslog サーバーに送信されていないすべてのログメッセージが削除されます。
バインド数	ARP パケットによって生成され、まだ syslog サーバーに送信されていないログメッセージの数が表示されます。 利用できないバッファのために 1 つ以上のログメッセージがドロップされた場合、現在のドロップされたログメッセージの数を持つ overflow というエントリがあります。
インデックス	各ログメッセージの連番が表示されます。
ポート	ARP パケットの送信元ポートが表示されます。
VID	ARP パケットの送信元 VLAN ID が表示されます。
送信元 MAC	ARP パケットの送信元 MAC アドレスが表示されます。
送信元 IP	ARP パケットの送信元 IP アドレスが表示されます。
パケット番号	このログメッセージに統合された ARP パケット数です。 本製品では、ログ連結間隔内の ARP パケットによって生成された同一のログメッセージを 1 つのログメッセージに連結します。この間隔は「設定」(204 ページ)画面で設定できます。

項目	内容	
理由	ログメッセージが生成された理由が表示されます。	
	dhcp deny	同じ MAC アドレスと VLAN ID を持つダイナミックバインディングに違反したため、ARP パケットが破棄されました。
	static deny	同じ MAC アドレスと VLAN ID のスタティックバインディングに違反したため、ARP パケットが破棄されました。
	deny	同じ MAC アドレスと VLAN ID を持つバインディングがなかったため、ARP パケットは破棄されました。
	dhcp permit	動的バインディングに一致したため、ARP パケットが転送されました。
	static permit	静的バインディングに一致したため、ARP パケットが転送されました。
	「設定」(204 ページ) 画面で、ARP パケットの VLAN ID に基づいて、ARP パケットが破棄または転送されたときにログメッセージを生成するように本製品を設定できます。	
時間	ログメッセージが生成された時刻が表示されます。	

設定

ARP インспекションを有効にしたり、本製品が廃棄した ARP パケットの記録を保存する期間や ARP インспекションログのグローバル設定を行うことができます。

ELECOM >> Switch For Business 保存 | ログアウト | 再起動 | 日本語

セキュリティ >> IPv4ソースガード >> ARP-インспекション

ポート ステータス VLANステータス ログステータス **設定** ポート設定 VLAN設定

ARP-インспекション設定

有効 ☒

フィルター-エージングタイム

フィルター-エージングタイム 300 秒

ログプロファイル

ログバッファサイズ 32 エントリー

Syslogレート 5 エントリー

ログ間隔 1 秒

ポート
スイッチング
ネットワーク
セキュリティ
AAA
ACL
アンチARPスキャン
BPDUガード
ストームコントロール
DoS攻撃防止
Errdisable
IPv4ソースガード
IPソースガード
DHCP snooping
DHCP Option82 プロファイル
ARP-インспекション
IPv6ソースガード

■ ARPインスペクション設定

項目	内容
有効	ARP インスペクション機能の有効／無効を切り替えます。

■ フィルターエージングタイム

項目	内容
フィルターエージングタイム	<p>本製品が不正な ARP パケットを識別した後、MAC アドレスフィルタを本製品に残す時間を入力します。(設定範囲: 1 ~ 2147483647 秒) (初期設定: 300 秒)</p> <p>その後、本製品は自動的に MAC アドレスフィルタを削除します。</p> <p>MAC アドレスフィルタを永続させたい場合は 0 を入力してください。</p> <p>この設定は既存の MAC アドレスフィルタには影響しません。</p>

■ ログプロファイル

項目	内容
ログバッファサイズ	<p>ARP パケットによって生成され、まだ syslog サーバーに送信されていないログメッセージの最大数を入力します。</p> <p>(設定範囲: 1 ~ 1024) (初期値: 32)</p> <p>このとき、「Syslog レート」と「ログ時間」で設定する値に対して適切な値にしてください。</p> <p>本製品内のログ件数がこの値を超えると、新たなログの記録を停止し、バッファ不足で破棄されたエントリ数のカウントのみを行います。</p> <p>ログを消去してこのカウンタをリセットするには、「ログステータス」(203 ページ)画面の「ログステータステーブルのクリア」をクリックします。</p>
Syslog レート	<p>本製品が 1 回のバッチで syslog サーバへ送信できる syslog メッセージの最大件数を入力します。(初期設定: 5)</p> <p>バッチの送信頻度は Log Interval で決まるため、この数値はレートとして扱われます。これを利用するには syslog サーバ側の設定が必要です。</p> <p>ARP パケットで生成されたログを syslog サーバへ送らない場合は 0 を入力します。</p> <p>Syslog Rate と Log Interval の関係 (例):</p> <p>1 秒あたり不正 ARP が 4 件、Syslog レート=5、Log 時間=1: スイッチは毎秒 4 件送信。</p> <p>1 秒あたり不正 ARP が 6 件、Syslog レート=5、Log 時間=2: スイッチは 2 秒ごとに 5 件送信。</p>
ログ時間	<p>本製品が syslog サーバに syslog メッセージを一括送信する頻度を入力します。</p> <p>(設定範囲: 1 ~ 86400 秒) (初期設定: 1 秒)</p> <p>syslog メッセージを即時送信する場合は 0 を入力してください。</p> <p>Syslog レートと Log 時間の関係例については、「Syslog レート」を参照してください。</p>

ポート設定

ポートをARP インспекションの信頼されたポートにするか、信頼されていないポートにするかを指定します。また、各信頼対象外ポートで本製品がARP パケットを受信する最大レートを指定できます。

ポート	信頼状態	制限	
		レート(pps)	バースト間隔(秒)
*	Untrusted	<input type="text"/>	<input type="text"/>
1	Untrusted	15	1
2	Untrusted	15	1
3	Untrusted	15	1
4	Untrusted	15	1
5	Untrusted	15	1
6	Untrusted	15	1
7	Untrusted	15	1
8	Untrusted	15	1
9	Untrusted	15	1
10	Untrusted	15	1

項目	内容
ポート	ポート番号が表示されます。 「*」の行を変更すると、すべてのポートに変更が適用されます。
信頼状態	<p>このポートが信頼できるポート (Trusted) か、信頼できないポート (Untrusted) かを選択します。</p> <p>本製品は、信頼できるポートの ARP パケットをいかなる理由でも廃棄しません。信頼できないポートでは、次の場合に ARP パケットを破棄します。</p> <ul style="list-style-type: none"> ● ARP パケット内の送信者情報が、現在のバインディング (IP-MAC-ポート) に一致しない。 ● ARP パケットの到着レートが高すぎる。(Untrusted ポートで許容する最大レートを指定できます)
レート (pps)	<p>本製品が各ポートから ARP パケットを受信する最大レートを指定します。 (設定範囲: 1 ~ 2048pps) (初期設定: 15pps)</p> <p>本製品はそれ以上の ARP パケットを破棄します。 この制限を無効にするには 0 を入力します。</p>
バースト間隔 (秒)	<p>バーストインターバルの長さを入力します。 (設定範囲: 1 ~ 15 秒) (初期設定: 1 秒)</p> <p>バースト間隔は、各ポートの ARP パケットのレートを監視する時間の長さです。 例えば、Rate が 15pps でバースト間隔が 1 秒の場合、本製品は 1 秒間隔で最大 15 個の ARP パケットを受け付けます。 バースト間隔が 5 秒の場合、5 秒間隔で最大 75 個の ARP パケットを受け付けます。</p>

VLAN 設定

各 VLAN で ARP 検査を有効にし、各 VLAN からの ARP パケット受信時にログメッセージを生成するタイミングを指定します。



項目	内容								
VID で VLN を検索	管理する VLAN ID を入力し、「検索」をクリックすると、指定した範囲の VLAN が下のテーブルに表示されます。 個々の VLAN を区切るにはカンマ (,) を、VLAN の範囲を示すにはハイフン (-) を使用します。(例) 「3,4」 「3-9」								
VLAN 数	VLAN の検索結果の数が表示されます。								
VID	上記で指定した範囲の各 VLAN の VLAN ID です。VLAN を設定した場合、設定はすべての VLAN に適用されます。								
有効／無効	VLAN の ARP 検査を有効にするか無効にするかを選択します。								
ログ	VLAN からの ARP パケット受信時に本製品がログメッセージを生成するタイミングを指定します。 <table><tr><td>なし</td><td>VLAN から ARP パケットを受信してもログメッセージを生成しません。</td></tr><tr><td>許可</td><td>VLAN からの ARP パケットを転送したときにログメッセージを生成します。</td></tr><tr><td>拒否</td><td>VLAN からの ARP パケットを破棄したときにログメッセージを生成します。</td></tr><tr><td>すべて</td><td>VLAN から ARP パケットを受信するたびにログメッセージを生成します。</td></tr></table>	なし	VLAN から ARP パケットを受信してもログメッセージを生成しません。	許可	VLAN からの ARP パケットを転送したときにログメッセージを生成します。	拒否	VLAN からの ARP パケットを破棄したときにログメッセージを生成します。	すべて	VLAN から ARP パケットを受信するたびにログメッセージを生成します。
なし	VLAN から ARP パケットを受信してもログメッセージを生成しません。								
許可	VLAN からの ARP パケットを転送したときにログメッセージを生成します。								
拒否	VLAN からの ARP パケットを破棄したときにログメッセージを生成します。								
すべて	VLAN から ARP パケットを受信するたびにログメッセージを生成します。								
適用	変更内容を本製品のランタイムメモリに保存します。 本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。								

[IPv6 ソースガード] IPv6 静的バインディング

IPv6 送信元バインディング状態

現在の IPv6 動的バインディングと静的バインディングを確認し、IPv6 アドレスまたは IPv6 プレフィックスに基づいて動的バインディングを削除します。

MEMO

バインディングは、ネットワーク内で許可されたパケットと許可されていないパケットを区別するために使用されます。本製品は、DHCP パケットをスヌープすること (動的バインディング)、および管理者が手動で提供する情報 (静的バインディング) からバインディングを学習します。

ELECOM >> Switch For Business

保存 | ログアウト | 再起動 | 日本語

セキュリティ >> IPv6 ソースガード >> IPv6 静的バインディング

トップメニュー
モニター
システム
ポート
スイッチング
ネットワーク
セキュリティ
AAA
ACL
アンチARPスキャン
BPDUガード
ストームコントロール
DoS攻撃防止
Errdisable
IPv4 ソースガード
IPv6 ソースガード

IPv6 送信元バインディング状態

IPv6 静的バインディング

動的送信元バインディングのクリア

☒ すべて

☐ IPv6 アドレス

☐ IPv6 プレフィックス

一括消去

キャンセル

インデックス	送信元アドレス	MACアドレス	VLAN	ポート	リース	種別
--------	---------	---------	------	-----	-----	----

項目	内容	
動的送信元 バインディング のクリア	「一括消去」をクリックしたときに、動的な IPv6 ソースバインディングエントリをどのように削除するかを指定します。	
	すべて	IPv6 ソースバインディングテーブルからすべての動的エントリを削除します。
	IPv6 アドレス	指定した IPv6 アドレスでスヌープされた動的エントリを削除します。
	IPv6 プレフィックス	指定したプレフィックスでスヌープされた動的エントリを削除します。
インデックス	各バインディングの連番が表示されます。	

208

項目	内容				
送信元アドレス	バインディングのソース IP アドレスが表示されます。 空白の場合、このフィールドはバインディングではチェックされません。				
MAC アドレス	バインディングのソース MAC アドレスが表示されます。 空白の場合、このフィールドはバインディングでチェックされません。				
VLAN	バインディングのソース VLAN ID です。 空白の場合、このフィールドはバインディングでチェックされません。				
ポート	バインディングのポート番号が表示されます。 このフィールドが空白の場合、バインディングはすべてのポートに適用されます。				
リース	バインディングが何日、何時間、何分、何秒間有効かを示します。 例えば、2d3h4m5s は、バインディングが 2 日、3 時間、4 分、5 秒間有効であることを意味します。 バインディングが常に有効な場合（静的バインディングなど）は、無限大を示します。				
種別	<p>本製品がバインディングをどのように学習したかを示します。</p> <table> <tr> <td>S</td><td>管理者が手動で入力した情報から学習した静的バインディングです。</td></tr> <tr> <td>DH</td><td>DHCP パケットを snooping して学習した DHCP-snooping バインディングです。</td></tr> </table>	S	管理者が手動で入力した情報から学習した静的バインディングです。	DH	DHCP パケットを snooping して学習した DHCP-snooping バインディングです。
S	管理者が手動で入力した情報から学習した静的バインディングです。				
DH	DHCP パケットを snooping して学習した DHCP-snooping バインディングです。				

IPv6 静的バインディング

IPv6 ソースガードバインディングテーブルエントリを表示または構成し、IPv6 静的バインディングを管理します。

MEMO

静的バインディングは、ソース IPv6 アドレス / プレフィックスによって一意に識別されます。各ソース IPv6 アドレス / プレフィックスは、1 つの静的バインディングにのみ存在できます。既存の静的バインディングと同じソース IPv6 アドレス / プレフィックスを持つ静的バインディングを作成しようとすると、新しい静的バインディングが元の静的バインディングを置き換えます。



IPv6 静的バインディングを追加したり、選択した IPv6 静的バインディングを編集します。

→ [211 ページ](#)

選択した IPv6 静的バインディングを削除します。

項目	内容
インデックス	各バインディングの連番が表示されます。
送信元アドレス	バインディングのソース IP アドレスが表示されます。 空白の場合、このフィールドはバインディングではチェックされません。
MAC アドレス	バインディングのソース MAC アドレスが表示されます。 空白の場合、このフィールドはバインディングでチェックされません。
VLAN	バインディングのソース VLAN ID です。 空白の場合、このフィールドはバインディングでチェックされません。

項目	内容
ポート	バインディングのポート番号が表示されます。 このフィールドが空白の場合、バインディングはすべてのポートに適用されます。

■ IPv6 静的バインディングの追加／編集

送信元アドレス	<input checked="" type="radio"/> IPv6アドレス <input type="text"/> <input type="radio"/> IPv6プレフィックス <input type="text"/> / <input type="text"/>
MACアドレス	<input type="radio"/> 任意 <input checked="" type="radio"/> <input type="text"/>
VLAN	<input type="radio"/> 任意 <input checked="" type="radio"/> <input type="text"/>
ポート	<input type="radio"/> 任意 <input checked="" type="radio"/> <input type="text"/>
<input type="button" value="適用"/> <input type="button" value="クリア"/> <input type="button" value="キャンセル"/>	

項目	内容
送信元アドレス	バインディングの IPv6 アドレスまたは IPv6 プレフィックス+プレフィックス長を入力します。
MAC アドレス	バインディングの送信元 MAC アドレス を入力します。 この項目を照合対象にしない場合は「任意」を選択します。
VLAN	バインディングの送信元 VLAN ID を入力します。 この項目を照合対象にしない場合は「任意」を選択します。
ポート	バインディングのポートを指定します。1 ポートのみの場合は最初のラジオボタンを選び、右側の欄にポート番号を入力します。
適用	変更内容を本製品のランタイムメモリに保存します。 本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。
クリア	フィールドが工場出荷時のデフォルトにクリアされます。

※ MAC アドレス／VLAN／ポート の 3 項目すべてを「任意」にすることはできません。
少なくとも 1 項目は指定してください。

[IPv6 ソースガード] IPv6 ソースガード

ポリシー

IPv6 ソースガードにバインディングテーブルに保存されている有効な IPv6 アドレス、または IPv6 プレフィックスを転送させ、すべてのリンクローカルアドレスからのデータトラフィックを許可またはブロックさせます。



IPv6 ソースガードポリシーを追加したり、選択した IPv6 ソースガードポリシーを編集します。

→ [213 ページ](#)

選択した IPv6 ソースガードポリシーを削除します。

項目	内容
インデックス	各ポリシーの連番が表示されます。
名前	この IPv6 ソースガードポリシーの識別のための名称が表示されます。
アドレス検証	この IPv6 ソースガードポリシーの Validate Address ステータスが表示されます。
プレフィックス検証	この IPv6 ソースガードポリシーの Validate Prefix ステータスが表示されます。
リンクローカル	この IPv6 ソースガードポリシーの Link Local トラフィックステータスが表示されます。

■ IPv6 ソースガードポリシーの追加／編集

名前	<input type="text"/>
アドレス検証	<input type="radio"/> OFF
プレフィックス検証	<input type="radio"/> OFF
リンクローカル	<input type="button" value="Deny"/> ▼
<input type="button" value="適用"/> <input type="button" value="クリア"/> <input type="button" value="キャンセル"/>	

項目	内容
名前	この IPv6 ソースガードポリシーの名前を入力します。 (最大 32 文字まで。? (クエスチョンマーク) (パイプ) ' (フォーテーション) " (ダブルフォーテーション) は使用不可)
アドレス検証	「有効」にすると、バインドテーブルに保存されている有効なアドレスを IPv6 ソースガードに転送させます。
プレフィックス検証	「有効」にすると、バインドテーブルに保存されている有効なプレフィックスを IPv6 ソースガードに転送させます。
リンクローカル	すべてのリンクローカルアドレスからのデータトラフィックを許可するには「Permit」を選択します。 許可しない場合は設定を「Deny」のままにします。 リンクローカルアドレスとは、リンクローカルプレフィックス FE80::/10 と修正 EUI-64 形式のインターフェース識別子を用いて、任意のインターフェース上で自動設定される IPv6 ユニキャストアドレスのことです。
適用	変更内容を本製品のランタイムメモリに保存します。 本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。
クリア	フィールドが工場出荷時のデフォルトにクリアされます。

ポート設定

設定したIPv6 ソースガードポリシーを指定したポートに適用します。

ELECOM >> Switch For Business

保存 | ログアウト | 再起動 | 日本語

セキュリティ >> IPv6ソースガード >> IPv6ソースガード

ポート

スイッチング

ネットワーク

セキュリティ

AAA

ACL

アンチARPスキャン

BPDUGuard

ストームコントロール

DoS攻撃防止

Errdisable

IPv6ソースガード

IPv6ソースガード

IPv6静的バインディング

IPv6ソースガード

IPv6 snooping

DHCPv6信頼設定

ポート認証

ポートセキュリティ

管理

ポリシー

ポート設定

ポート	ポリシー名
*	
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	

適用 キャンセル

項目	内容
ポート	ポート番号が表示されます。 「*」の行を変更すると、すべてのポートに変更が適用されます。
ポリシー名	このポートに適用するIPv6 ソースガードポリシーを選択します。
適用	変更内容を本製品のランタイムメモリに保存します。 本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。

[IPv6 ソースガード] IPv6 snooping

ポリシー設定

DHCPv6 snoopingを有効にします。



IPv6 snooping ポリシーを追加したり、選択した IPv6 snooping ポリシーを編集します。

→ [216 ページ](#)

選択した IPv6 snooping ポリシーを削除します。

項目	内容
インデックス	各 IPv6 snooping ポリシーの連番が表示されます。
名前	この IPv6 snooping ポリシーの識別のための名称が表示されます。
プロトコル	DHCPv6 スニффイングパケットから学習したプロトコルが表示されます。
プレフィックス収集	DHCPv6 スニффイングパケットから学習した IPv6 プレフィックスが表示されます。
アドレス数制限	IPv6 snooping ポリシーを使って学習した IPv6 アドレスとプレフィックスの数が表示されます。

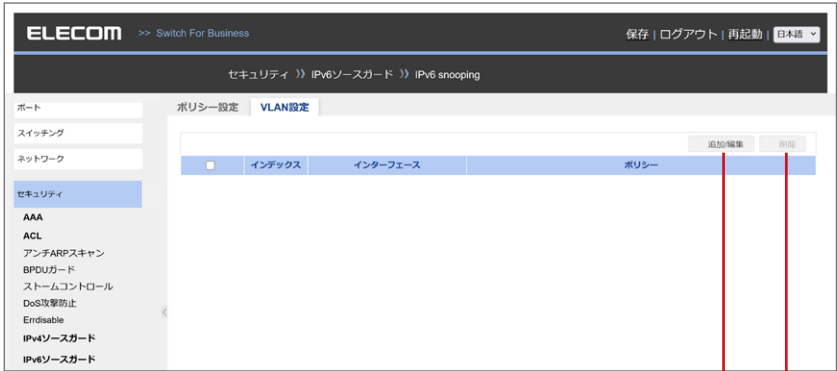
■ IPv6 snooping ポリシーの追加／編集

名前	<input type="text"/>
プロトコル	<input type="checkbox"/> DHCP
プレフィックス収集	<input checked="" type="radio"/> OFF
アドレス数制限	<input type="text"/>
<input type="button" value="適用"/> <input type="button" value="クリア"/> <input type="button" value="キャンセル"/>	

項目	内容
名前	この IPv6 snooping ポリシーの名前を入力します。 (最大 32 文字まで。? (クエスチョンマーク) (パイプ) ' (クォーテーション) " (ダブルクォーテーション) , (コンマ) は使用不可)
プロトコル	DHCPv6 サーバから DHCPv6 クライアントへ送信される DHCPv6 パケットを本製品がスニッフする場合は、「DHCP」を選択します。
プレフィックス収集	「有効」にすると、DHCPv6 をスヌーピングしたパケットから IPv6 のプレフィックスとプレフィックス長を学習します。
アドレス数制限	IPv6 snooping ポリシーで学習される IPv6 アドレスとプレフィックスの上限数を入力します。 設定できる最大値は、IPv6 ソースガードのバインディングテーブルの最大サイズと同じです。
適用	変更内容を本製品のランタイムメモリに保存します。 本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。
クリア	フィールドが工場出荷時のデフォルトにクリアされます。

VLAN 設定

特定の VLAN インタフェースで DHCPv6 snooping ポリシーを有効にします。



IPv6 snooping VLANを追加したり、選択した
IPv6 snooping VLANを編集します。

→ [218ページ](#)

選択したIPv6 snooping VLANを削除します。

項目	内容
インデックス	各バインディングの連番が表示されます。
インターフェース	VLAN インターフェースが表示されます。
ポリシー	DHCPv6 snooping ポリシーが表示されます。

■ IPv6 snooping VLANの追加／編集

インターフェース

VLAN1 ▾

ポリシー

▾

適用

クリア

キャンセル

項目	内容
インターフェース	選択した DHCPv6 snooping ポリシーを適用する VLAN インタフェースを選択します。
ポリシー	この VLAN インタフェースに適用する IPv6 snooping ポリシーを選択します。
適用	変更内容を本製品のランタイムメモリに保存します。 本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。
クリア	フィールドが工場出荷時のデフォルトにクリアされます。

[IPv6 ソースガード] DHCPv6 信頼設定

DHCPv6 snooping で信頼するポートを指定します。

ELECOM >> Switch For Business

保存 | ログアウト | 再起動 | 日本語

セキュリティ >> IPv6ソースガード >> DHCPv6信頼設定

ポート

スイッチング

ネットワーク

セキュリティ

AAA

ACL

アンチARPスキャン

BPDUGuard

ストームコントロール

DoS攻撃防止

Errdisable

IPv4ソースガード

IPv6ソースガード

IPv6静約バインディング

IPv6ソースガード

IPv6 snooping

DHCPv6信頼設定

ポート認証

ポートセキュリティ

管理

DHCPv6信頼設定

Trust Setting

有効 ☐ OFF

ポート設定

ポート	信頼状態
*	Untrusted
1	Untrusted
2	Untrusted
3	Untrusted
4	Untrusted
5	Untrusted
6	Untrusted
7	Untrusted
8	Untrusted
9	Untrusted
10	Untrusted

適用 キャンセル

■ Trust setting

項目	内容
有効	有効にすると、DHCP (IPv6) snooping において各ポートを Trusted (信頼) か Untrusted (非信頼) に指定できます。 これを選択しない場合は IPv6 DHCP Trust は使用されず、すべてのポートが自動的に Trusted として扱われます。

■ ポート設定

項目	内容
ポート	ポート番号が表示されます。 「*」の行を変更すると、すべてのポートに変更が適用されます。

項目	内容
信頼状態	<p>このポートを Trusted（信頼）か Untrusted（非信頼）に指定します。 Trusted ポートは DHCPv6 サーバまたは他のスイッチに接続されます。 Untrusted ポートは加入者（クライアント）に接続され、次の場合、スイッチは Untrusted ポートからの DHCPv6 パケットを破棄します。</p> <ul style="list-style-type: none">● パケットが DHCPv6 サーバ側パケット（例：ADVERTISE、REPLY、RELAY-REPLY）である。● パケット内の 送信元 MAC アドレスおよび 送信元 IP アドレスが、現在のバインディング のいずれとも一致しない。
適用	<p>変更内容を本製品のランタイムメモリに保存します。 本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。</p>

ポート認証

ポートごとに 802.1X 認証 (RADIUS 連携) の動作を設定します。

ELECOM

>> Switch For Business

保存 | ログアウト | 再起動 | 日本語

セキュリティ >> ポート認証 >> 802.1x

アクションバー

モニター

システム

ポート

スイッチング

ネットワーク

セキュリティ

AAA

ACL

アンチARPスキャン

BPDUGuard

ストームコントロール

DoS攻撃防止

ErrDisable

IPv6ソースガード

IPv6ソースガード

ポート認証

802.1x

ポートセキュリティ

管理

802.1x

有効 ☒ OFF

EAPOLフラッド ☒ OFF

ポート	有効	最大リクエスト	再認証	再認証間隔 (秒)	静止間隔 (秒)	送信間隔 (秒)	サブリカントタイムアウト (秒)
*	<input type="checkbox"/>	<input type="text"/>	On	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
1	<input type="checkbox"/>	2	On	3600	60	30	30
2	<input type="checkbox"/>	2	On	3600	60	30	30
3	<input type="checkbox"/>	2	On	3600	60	30	30
4	<input type="checkbox"/>	2	On	3600	60	30	30
5	<input type="checkbox"/>	2	On	3600	60	30	30
6	<input type="checkbox"/>	2	On	3600	60	30	30
7	<input type="checkbox"/>	2	On	3600	60	30	30
8	<input type="checkbox"/>	2	On	3600	60	30	30
9	<input type="checkbox"/>	2	On	3600	60	30	30
10	<input type="checkbox"/>	2	On	3600	60	30	30

適用

キャンセル

項目	内容
有効	「ON」にすると、本製品で 802.1x 認証を許可します。 各ポートに設定する前に、まず本製品で 802.1x 認証を有効にする必要があります。
EAPOL フラッド	「ON」にすると、同じ VLAN 内のすべてのポートに EAPOL パケットをフラッドします。 802.1x 認証が有効になっている場合、EAPOL フラッドは有効になりません。
ポート	ポート番号が表示されます。 「*」の行を変更すると、すべてのポートに変更が適用されます。
有効	チェックを入れると、このポートで 802.1x 認証を許可します。
最大リクエスト	応答がないポートを Guest VLAN に送る前に、クライアントの認証を試行する回数を指定します。(初期値: 2)
再認証	サブスクリババがポートへの接続を維持するために、定期的にユーザ名とパスワードを再入力する必要があるかどうかを指定します。(初期値: On)
再認証期間 (秒)	クライアントがポートへの接続を維持するためにユーザ名とパスワードを再入力するまでに必要な時間の長さを指定します。(初期値: 3600 秒)
静止期間 (秒)	認証交換に失敗した後、ポートが HELD 状態を維持し、接続されたクライアントからの認証要求を拒否する秒数を指定します。(初期値: 60 秒)

項目	内容
送信期間 (秒)	本製品がクライアントに ID 要求を再送するまでのクライアントからの応答待ち秒数を指定します。(初期値: 30 秒)
サブリカント タイムアウト (秒)	チャレンジリクエストに対するクライアントからの応答を待って再リクエストを送信する秒数を指定します。(初期値: 30 秒)
適用	変更内容を本製品のランタイムメモリに保存します。 本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。

ポートセキュリティ

ポートセキュリティを設定します。

The screenshot shows the ELECOM web interface for configuring Port Security. The sidebar on the left contains navigation links: ダッシュボード, モニター, システム, ポート, スイッチング, ネットワーク, セキュリティ, AAA, ACL, アンチARPスキャン, BPDUガード, ストームコントロール, DoS攻撃防止, Errdisable, IPv4ソースガード, IPv6ソースガード, ポート認証, 802.1x, and ポートセキュリティ. The main content area is titled 'ポートセキュリティ' and includes a 'MACフリーズ' section with a text input field and a 'ポートセキュリティ' section with a toggle switch set to 'OFF'. Below the toggle is a table for configuring port security settings.

ポート	有効	アドレス学習	学習可能MACアドレス数
*	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>
1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="0"/>
2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="0"/>
3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="0"/>
4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="0"/>
5	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="0"/>
6	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="0"/>
7	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="0"/>
8	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="0"/>
9	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="0"/>
10	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="0"/>

At the bottom of the table, there are buttons for '適用' (Apply) and 'キャンセル' (Cancel).

■ MACフリーズ

項目	内容
ポートリスト	<p>ポートセキュリティを有効化し、MAC アドレス学習を無効化したいポート番号を（カンマ区切りで）入力します。</p> <p>「MAC フリーズ」をクリックすると、指定したポートでこれまでに学習された MAC アドレスはすべて静的 MAC アドレスに変換され、「スイッチング」―「静的 MAC 転送」（143 ページ）画面に表示されます。</p>

■ ポートセキュリティ

項目	内容
有効	ポートセキュリティ機能の有効／無効を切り替えます。
ポート	<p>ポート番号が表示されます。</p> <p>「*」の行を変更すると、すべてのポートに変更が適用されます。</p>

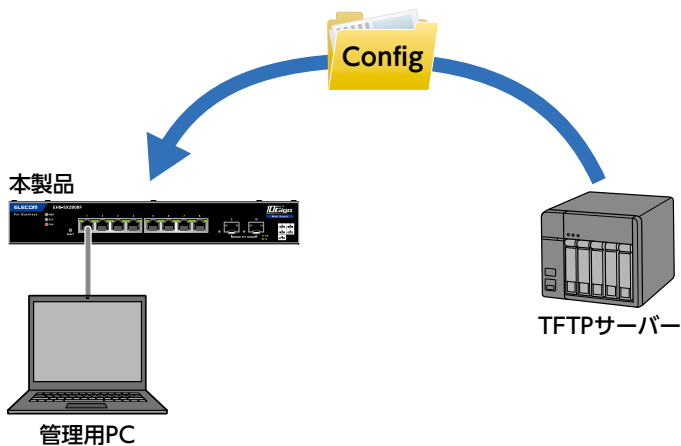
項目	内容
有効	チェックを入れると、このポートでポートセキュリティ機能を有効にします。 本製品は、このポートの MAC アドレス表に登録された MAC アドレスを持つパケットだけを転送します。一致しない MAC アドレスのパケットは破棄されます。 このチェックボックスをクリアすると、ポートセキュリティ機能を無効にし、このポートのすべてのパケットを転送します。
アドレス学習	MAC アドレス学習は、送信ブロードキャストトラフィックを削減します。 ポートで MAC アドレス学習を行うには、ポート自体がアドレス学習を有効にしてアクティブになっている必要があります。
学習可能 MAC アドレス数	ポートで学習できる（動的）MAC アドレス数の上限を設定します。 （設定範囲：0 ～ 16384） 0 にすると、この機能は無効になります。 例：ポート 2 でこの値を「5」にすると、同時にポート 2 を利用できるのは学習済みの 5 個の MAC アドレスを持つ端末だけです。 6 台目は、その 5 個のうちいずれかがエージアウトするまで待機します。 MAC アドレスのエージング時間は「システム」－「スイッチ設定」(74 ページ) 画面で設定できます。
適用	変更内容を本製品のランタイムメモリに保存します。 本製品の電源が切れると、変更内容は失われるため、「適用」をクリックしたら必ず画面上部の「保存」をクリックして、変更内容を不揮発性メモリに保存してください。

【設定】設定の復元

保存した Config ファイルで設定を復元します。

TFTPで更新する場合

TFTP サーバーに保存した Config ファイルをアドレスを指定して復元します。



ELECOM >> Switch For Business

保存 | ログアウト | 再起動 | 日本語

管理 >> 設定 >> 設定の復元

ダッシュボード

モニター

システム

ポート

スイッチング

ネットワーク

セキュリティ

管理

設定

設定の復元

設定のバックアップ

設定の復元

デバイス設定をファイルから復元するには、設定ファイルの場所を参照し「復元」ボタンをクリックしてください。

更新方法 ☒ TFTP ☐ HTTP

サーバーアドレス

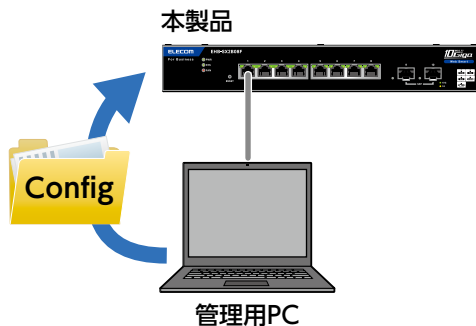
ファイル名

実行

項目	内容
更新方法	TFTP を選択します。
サーバーアドレス	TFTP サーバーのホスト名または IP アドレスを入力します。
ファイル名	復元用ファイルの名称を入力します。
実行	復元を実行します。

HTTPで更新する場合

管理用PCに保存したConfigファイルを指定して設定を復元します。



ELECOM >> Switch For Business 保存 | ログアウト | 再起動 | 日本語

管理 >> 設定 >> 設定の復元

設定の復元

デバイス設定をファイルから復元するには、設定ファイルの場所を参照し「復元」ボタンをクリックしてください。

更新方法 ☐ TFTP ☒ HTTP

ファイルの場所 ファイルが選択されていません。

ダッシュボード
モニター
システム
ポート
スイッチング
ネットワーク
セキュリティ
管理
設定
設定のバックアップ
設定のバックアップ

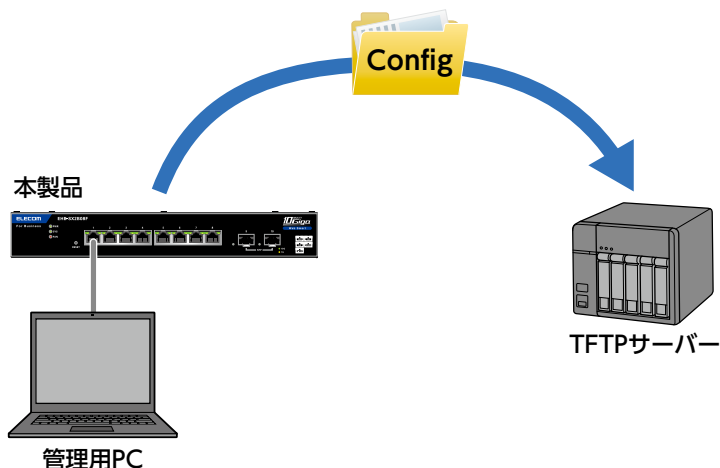
項目	内容
更新方法	HTTP を選択します。
ファイルの場所	「参照」をクリックして、バックアップで保存した復元用の config ファイルを選択します。
実行	復元を実行します。

【設定】設定のバックアップ

設定を Config ファイルにバックアップします。

TFTP でバックアップする場合

指定した TFTP サーバーに Config ファイルを保存します。



ELECOM
>> Switch For Business

保存 | ログアウト | 再起動 | 日本語

管理
>> 設定
>> 設定のバックアップ

ダッシュボード
モニター
システム
ポート
スイッチング
ネットワーク
セキュリティ
管理
設定
設定の復元
設定のバックアップ

設定のバックアップ

現在の設定をお使いの機器にバックアップできます。

更新方法 ☒ TFTP ☐ HTTP

サーバーアドレス

ファイル名

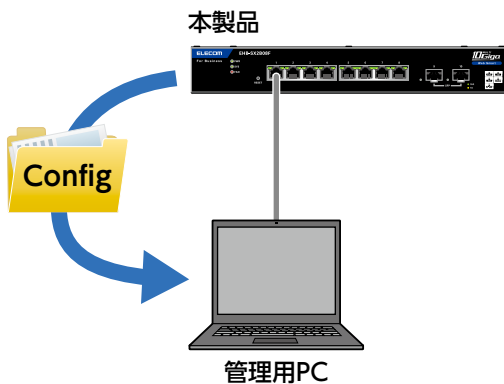
設定

項目	内容
更新方法	TFTP を選択します。
サーバーアドレス	TFTP サーバーのホスト名または IP アドレスを入力します。
ファイル名	復元用ファイルの名称を入力します。

項目	内容	
設定	バックアップする設定を選択します。	
	実行設定	実行中の設定内容をバックアップします。
	設定 1	「設定 1」に保存されている設定内容をバックアップします。
	設定 2	「設定 2」に保存されている設定内容をバックアップします。
実行	バックアップを実行します。	

HTTPでバックアップする場合

管理用PCにConfig ファイルを保存します。



ELECOM
>> Switch For Business

保存 | ログアウト | 再起動 | 日本語

管理 >> 設定 >> 設定のバックアップ

ダッシュボード

モニター

システム

ポート

スウィッチング

ネットワーク

セキュリティ

管理

設定

設定の復元

設定のバックアップ

設定のバックアップ

現在の設定をお使いの機器にバックアップできます。

更新方法

☐ TFTP
☒ HTTP

設定

実行設定

実行

項目	内容
更新方法	HTTP を選択します。

項目	内容	
設定	バックアップする設定を選択します。	
	実行設定	実行中の設定内容をバックアップします。
	設定 1	「設定 1」に保存されている設定内容をバックアップします。
	設定 2	「設定 2」に保存されている設定内容をバックアップします。
実行	バックアップを実行します。	

【設定】実行設定の消去

「実行」をクリックすると、本製品のランニングコンフィグレーションが削除されます。
工場出荷状態にリセットした場合とは異なり、ユーザ名、パスワード、システムログ、メモリログ、ボーレート、SSHサービスは削除されません。



【設定】設定の保存

「設定 1」をクリックすると、現在の設定内容が本製品の「設定 1」に永続的に保存されます。
「設定 2」をクリックすると、現在の設定内容が本製品の「設定 2」に永続的に保存されます。

The screenshot displays the ELECOM management interface. At the top, the header includes the ELECOM logo, a link to 'Switch For Business', and user options: '保存' (Save), 'ログアウト' (Logout), '再起動' (Restart), and a language dropdown set to '日本語'. Below the header, a breadcrumb trail shows '管理' (Management) > '設定' (Settings) > '設定の保存' (Save Settings). The left sidebar contains a menu with categories: 'ダッシュボード' (Dashboard), 'モニター' (Monitor), 'システム' (System), 'ポート' (Port), 'スイッチング' (Switching), 'ネットワーク' (Network), 'セキュリティ' (Security), '管理' (Management), and '設定' (Settings). The '設定' category is expanded, showing sub-items: '設定の権限' (Setting Permissions) and '設定のバックアップ' (Setting Backup). The main content area is titled '設定の保存' and contains a table with two columns: '設定の保存先' (Save Destination) and a timestamp. The table has two rows: '設定1' (Setting 1) with a timestamp of '2022-01-01 08:39:08' and '設定2' (Setting 2) with a timestamp of '--'.

設定の保存先	
設定1	2022-01-01 08:39:08
設定2	--

診断

IP アドレスのping、tracerout、ポートテストを実行します。

■ Pingテスト

項目	内容
IPv4	IPv4 アドレスに ping を送信する場合に選択します。 それ以外の場合は「-」を選択し、本製品の全 VLAN に ping 要求を送信します。
IPv6	IPv6 アドレスに ping を送信する場合に選択します。 また、vlan を選択し、Ping 送信先の VLAN の ID 番号を指定します。 その他、本製品の全 VLAN に ping 要求を送信する場合は「-」を選択します。
IP アドレス / ホスト名	接続をテストするために ping を送信するデバイスの IP アドレスまたはホスト名を入力します。「実行」をクリックすると、本製品が IP アドレスに ping を送信します。
送信元 IP アドレス	接続をテストするために ping を送信するソース IP アドレスを入力します。 「実行」をクリックすると、本製品が IP アドレスに ping を送信します。
回数	連続して送信する ICMP エコー要求 (ping) メッセージ数を入力します。 (初期設定：3)

■ Trace Route テスト

項目	内容
IPv4	IPv4 アドレスを持つデバイスへのルートパケットをトレースする場合は、このオプションを選択します。 トレースルートを実行するデバイスは、ここで指定した VLAN に属している必要があります。
IPv6	IPv6 アドレスのデバイスへのルートパケットをトレースする場合は、このオプションを選択します。
IP アドレス / ホスト名	トレースルートを行いたい機器の IP アドレスまたはホスト名を入力します。 「実行」をクリックすると、本製品にトレースルート機能を実行させます。 これにより、パケットが指定した装置までの経路を決定します。
TTL	ICMP Echo Request パケットの TTL(Time To Live) 値を入力します。 (初期値: 30) これは、パケットが通過できるホップ（ルーター）の最大数を設定するものです。 経路上の各ルーターは TTL 値を 1 つ減らし、パケットを転送します。 TTL 値がゼロになり、宛先が見つからない場合、ルーターはパケットをドロップし、送信者に通知します。
待機時間	本製品が別のトレースルートを実行する前に、プローブに対する応答を何秒待つかを指定します。(初期値: 2 秒)
クエリ	本製品がトレースルート機能を実行する回数を指定します。(初期値: 3)

■ ケーブル診断

項目	内容
ポート	イーサネットポート番号を入力し、「実行」をクリックすると、指定したポートのイーサネット接続の物理的なワイヤペアテストを実行します。ポートを診断すると診断画面 (234 ページ) が表示されます。

● ポート診断結果画面

Port	Channel	Pair status	Cable length (m)	Distance to fault (m)
7	pairA	Ok	0.01	N/A
	pairB	Ok	1.00	N/A
	pairC	Ok	1.00	N/A
	pairD	Ok	1.18	N/A

項目	内容										
Port	本製品の物理イーサネットポートの番号です。										
Channel	ケーブル内のワイヤペアの名称が表示されます。 イーサネットケーブルには通常 4 対のワイヤがあります。10BASE-T または 100BASE-TX ポートでは 2 ペアしか使用およびテストしませんが、1000BASE-T ポートでは 4 ペアすべてが必要です。										
Pair status	<table> <tr> <td>Ok</td><td>ワイヤーペア間の物理的な接続は問題ありません。</td></tr> <tr> <td>Open</td><td>ワイヤーペア間の物理的な接続がありません（オープン回路が検出された）。</td></tr> <tr> <td>Short</td><td>ワイヤペア間の短絡が検出されました。</td></tr> <tr> <td>Unknown</td><td>本製品は、このポートに接続されたケーブルのケーブル診断の実行に失敗しました。</td></tr> <tr> <td>Unsupported</td><td>ポートがファイバーポートであるか、アクティブではありません。</td></tr> </table>	Ok	ワイヤーペア間の物理的な接続は問題ありません。	Open	ワイヤーペア間の物理的な接続がありません（オープン回路が検出された）。	Short	ワイヤペア間の短絡が検出されました。	Unknown	本製品は、このポートに接続されたケーブルのケーブル診断の実行に失敗しました。	Unsupported	ポートがファイバーポートであるか、アクティブではありません。
Ok	ワイヤーペア間の物理的な接続は問題ありません。										
Open	ワイヤーペア間の物理的な接続がありません（オープン回路が検出された）。										
Short	ワイヤペア間の短絡が検出されました。										
Unknown	本製品は、このポートに接続されたケーブルのケーブル診断の実行に失敗しました。										
Unsupported	ポートがファイバーポートであるか、アクティブではありません。										
Cable length(m)	「Pair status」が「Ok」で、本製品のチップセットがこの機能をサポートしている場合、ポートに接続されているイーサネットケーブルの全長が表示されます。 「Pair status」が「Open」または「Short」の場合、「N/A」と表示されます。障害までの距離をチェックしてください。 本製品のチップセットがケーブル長の表示をサポートしていない場合、「Unsupported」と表示されます。										
Distance to fault(m)	ポートからケーブルがオープンまたはショートしている場所までの距離が表示されます。「Pair status」が「Ok」の場合は「N/A」と表示されます。 本製品のチップセットが距離の表示をサポートしていない場合は「Unsupported」と表示されます。										

ファームウェア更新

本製品のファームウェアをアップグレードします。

ELECOM >> Switch For Business 保存 | ログアウト | 再起動 | 日本語

管理 >> ファームウェア更新

ファームウェア更新

ファームウェア名	ファームウェアバージョン
E14B-SX2B08F	現在のファームウェア 1.0.0
	ファームウェア1 1.0.0
	ファームウェア2 0.0.4

起動ファームウェア

現在の起動ファームウェア ファームウェア 1
 起動ファームウェアの設定 ファームウェア 1

適用 キャンセル

ファームウェアの保存先と新しいファームウェアを選択して「適用」を押してください。

ファームウェア 1

更新方法 ☒ TFTP ☐ HTTP

サーバーアドレス

ファイル名

適用

新しいファームウェアをアップロードします。

→ [236ページ](#)

■ ファームウェア更新

項目	内容
ファームウェア名	本製品の名称が表示されます。
ファームウェアバージョン	本製品には、ファームウェア 1 とファームウェア 2 の 2 つのファームウェアがフラッシュに格納されています。 現在本製品で使用しているファームウェアと、ファームウェア 1 とファームウェア 2 のバージョン番号が表示されます。

■ 起動ファームウェア

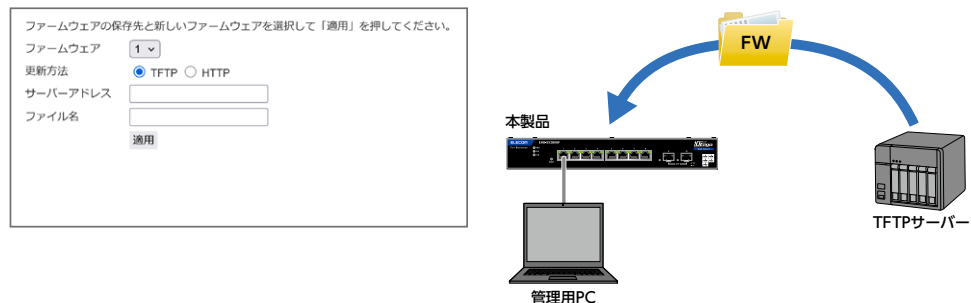
項目	内容
現在の起動ファームウェア	本製品で現在使用中のファームウェア（ファームウェア 1 またはファームウェア 2）が表示されます。
起動ファームウェアの設定	起動に使用するファームウェアを選択します。 「適用」をクリックすると、起動ファームウェアの設定が本製品の揮発性メモリに保存されます。

新しいファームウェアをアップロードする

TFTP 経由か HTTP 経由かを選択します。

■ 「更新方法」 に 「TFTP」 を選択した場合

TFTP サーバーに保存したファームウェアファイルをアドレスを指定してアップデートします。



項目	内容
ファームウェア	新しいファームウェアを、ファームウェア 1、ファームウェア 2 のどちらに適用するか選択します。
更新方法	TFTP を選択します。
サーバーアドレス	TFTP サーバーのホスト名または IP アドレスを入力します。
ファイル名	ファームウェアファイルの名称を入力します。
適用	新しいファームウェアが更新されます。 新しいファームウェアは再起動したあとに適用されます。 再起動は、「再起動」(238 ページ) 画面からおこないます。

■「更新方法」に「HTTP」を選択した場合

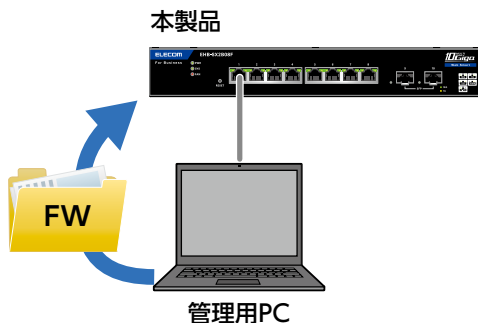
管理用PCに保存したファームウェアファイルを指定してアップデートします。

ファームウェアの保存先と新しいファームウェアを選択して「適用」を押してください。

ファームウェア 1 ▾

更新方法 ☐ TFTP ☒ HTTP

ファイルの場所 ファイルが選択されていません。

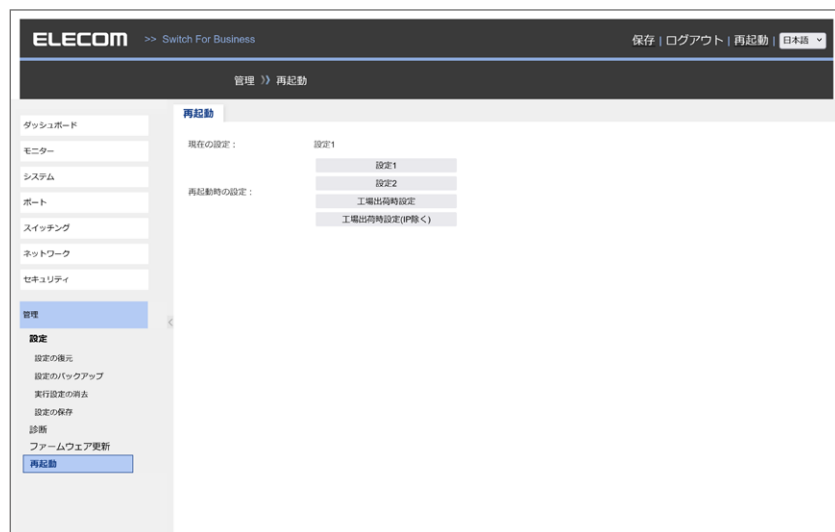


項目	内容
ファームウェア	新しいファームウェアを、ファームウェア 1、ファームウェア 2 のどちらに適用するか選択します。
更新方法	HTTP を選択します。
ファイルの場所	管理用 PC に保存しているファームウェアファイルを指定します。
適用	新しいファームウェアが更新されます。 新しいファームウェアは再起動したあとに適用されます。 再起動は、「再起動」(238 ページ) 画面からおこないます。

再起動

物理的に電源を切ることなく本製品を再起動できます。

- ① 再起動後に適用する設定プロファイルを選択します。
- ② 確認ダイアログボックスが表示されますので、「確認」をクリックします。
本製品が再起動されます（2分程度かかります）。



付録編

安全上のご注意	240
使用上のご注意	243
このマニュアルについて	244
製品の保証について	245
製品の保証とサービス	245
サポートサービスについて	246





安全上のご注意

製品を正しく安全に使用するための重要な注意事項を説明しています。必ずご使用前にこの注意事項を読み、記載事項にしたがって正しくご使用ください。

本製品は、人命にかかわる設備や機器、および高い信頼性や安全性を必要とする設備や機器（医療関係、航空宇宙関係、輸送関係、原子力関係）への組み込みは考慮されていません。これらの機器での使用により、人身事故や財産損害が発生しても、弊社はいかなる責任も負いかねます。

■表示について

この「安全上のご注意」では以下のような表示（マークなど）を使用して、注意事項を説明しています。内容をよく理解してから、本文をお読みください。

	警告	この表示を無視して取り扱いを誤った場合、使用者が死亡または重傷を負う危険性がある項目です。
	注意	この表示を無視して取り扱いを誤った場合、使用者が傷害を負う危険性、もしくは物的損害を負う危険性がある項目です。
		丸に斜線のマークは何かを禁止することを意味します。丸の中には禁止する項目が絵などで表示されている場合があります。
		塗りつぶしの丸のマークは何かの行為を行わなければならないことを意味します。丸の中には行わなければならない行為が絵などで表示されている場合があります。

警告



万一、異常が発生したとき。

本体から異臭や煙が出た時は、ただちに電源を切り、販売店にご相談ください。



異物を入れないでください。

本体内部に金属類を差し込まないでください。また、水などの液体が入らないように注意してください。故障、感電、火災の原因となります。

※ 万一異物が入った場合は、ただちに電源を切り販売店にご相談ください。



落雷の恐れがあるときや雷発生時は、いったん電源を切って使用を中断してください。

感電、火災、故障の原因となります。



水気の多い場所での使用、濡れた手での取り扱いはおやめください。

感電・火災の原因となります。



付属または弊社が指定する仕様・型番のACアダプター、電源ケーブルや信号ケーブル以外を本製品に使わないでください。

仕様が合わないACアダプター・ケーブル等を接続すると、本製品が故障・発煙・発火する恐れがあります。



装置の上に物を置かないでください。

本製品の上に重いものや、水の入った容器類、または虫ピン、クリップなどの小さな金属類を置かないでください。故障や感電、火災の原因になります。



揮発性液体の近くの使用は避けてください。

マニキュア、ペディキュアや除光液などの揮発性液体は、装置の近くで使わないでください。装置の中に入って引火すると火災の原因になります。



同梱の部品は、本製品でのみご使用ください。

製品に同梱されているACアダプター、あるいは電源コードは、他の電子機器では使用しないでください。仕様の違いにより、火災・故障の原因となります。



注意



通風孔はふさがないでください。

過熱による火災、故障の原因となります。



高温・多湿の場所、長時間直射日光の当たる場所での使用・保管は避けてください。

屋外での使用は禁止します。また、周辺の温度変化が激しいと内部結露によって誤動作する場合があります。



本体は精密な電子機器のため、衝撃や振動の加わる場所、または加わりやすい場所での使用／保管は避けてください。

故障や、接触不良による発火や火災の原因となります。



ラジオ・テレビ等の近くで使用しますと、ノイズを与える事があります。また、近くにモーター等の強い磁界を発生する装置がありますとノイズが入り、誤動作する場合があります。必ず離してご使用ください。



電源が入っている状態で本体に長時間（10 秒以上）触れないでください。

低温やけどの原因となるおそれがあります。



地震・振動・落下対策について。

地震などによる振動で装置の落下、移動、転倒あるいは窓からの飛び出しが発生し、重大な事故へと発展するおそれがあります。これを防ぐため、必要に応じて保守会社や専門業者にご相談頂くなど、地震・振動・落下対策を実施してください。

使用上のご注意

- 高温・多湿の場所、長時間直射日光の当たる場所での使用・保管は避けてください。
- 屋外で使用しないでください。
- 周辺の温度変化が激しいと内部結露によって誤動作する場合があります。
- 本体は精密な電子機器のため、衝撃や震動の加わる場所、または加わりやすい場所での使用・保管は避けてください。
- ラジオ・テレビ等の近くで使用すると、ノイズを与えることがあります。また、近くにモーター等の強い磁界を発生する装置があると、ノイズが入り、誤動作する場合があります。必ず離してご使用ください。
- 本製品の仕様および価格は、製品の改良等により予告無しに変更する場合があります。
- 本製品に付随するドライバー、ソフトウェア等を逆アセンブル、逆コンパイルまたはその他リバースエンジニアリングすること、弊社に無断でホームページ、FTPサイトに登録するなどの行為を禁止させていただきます。
- 本製品を使用した結果によるお客様のデータの消失、破損など他への影響につきましては、上記にかかわらず責任は負いかねますのでご了承ください。重要なデータについてはあらかじめバックアップするようにお願いいたします。

このマニュアルについて

- このマニュアルの著作権は、エレコム株式会社が所有しています。
- このマニュアルの内容の一部または全部を無断で複製／転載することを禁止させていただきます。
- このマニュアルの内容に関しては、製品の改良のため予告なしに変更する場合があります。
- このマニュアルの内容に関しては、万全を期しておりますが、万一ご不審な点がございましたら、弊社サポート窓口までご連絡ください。
- 本書に掲載されている商品名／社名などは、一般に商標ならびに登録商標です。

製品の保証について

製品の保証とサービス

本製品には保証とご使用にあたっての注意について記載した文書「安全にお使いいただくために」が付いています。

●保証期間

保証期間はお買い上げの日より3年間です。保証期間を過ぎての修理は有料になります。詳細については製品情報に記載の保証規定をご確認ください。保証期間中のサービスについてのご相談は、お買い上げの販売店にお問い合わせください。

●保証範囲

次のような場合は、弊社は保証の責任を負いかねますのでご注意ください。

- ・ 弊社の責任によらない製品の破損、または改造による故障
- ・ 本製品をお使いになって生じたデータの消失、または破損
- ・ 本製品をお使いになって生じたいかなる結果および、直接的、間接的なシステム、機器およびその他の異常

詳しい保証規定につきましては、「安全にお使いいただくために」に記載の保証規定をご確認ください。

●その他のご質問などに関して

次ページ「サポートサービスについて」をお読みください。

サポートサービスについて

よくあるお問い合わせ、対応情報、マニュアルなどをインターネットでご案内しております。ご利用が可能であれば、まずご確認ください。

詳細は…

サポートポータルサイト「えれさぽ」へ



エレコム法人様サポートセンター

TEL: **0570-070-040**

【受付時間】 9:00 ～ 12:00 / 13:00 ～ 18:00 （月曜日～金曜日）

※ 祝日、夏期、年末年始特定休業日を除く

ネットワークサポートにお電話される前に

お問い合わせの前に以下の内容をご用意ください。

- ・ 弊社製品の型番
 - ・ ご質問内容 (症状、やりたいこと、お困りのこと)
- ※ 可能な限り、電話しながら操作可能な状態でご連絡ください。

日本以外でご購入されたお客様は、購入国の販売店舗へお問い合わせください。

エレコム株式会社は、日本以外の国でのご購入・ご使用による問い合わせ・サポート対応は致しかねます。また、日本語以外の言語でのサポートは致しかねます。商品交換は保証規定に沿って対応致しますが、日本以外からの商品交換は対応致しかねます。

This product is designed for use in Japan only.

A customer who purchases outside Japan should contact the local retailer in the country of purchase for enquiries. In "ELECOM CO., LTD. (Japan)", no customer support is available for enquiries about purchases or usage in/from any countries other than Japan. Also, no foreign language other than Japanese is available. Replacements will be made under stipulation of the Elecom warranty, but are not available from outside of Japan.



レイヤー 2 Webスマートギガスイッチ EHB-SX2B08F
レイヤー 2 10G Webスマートスイッチ EHB-SQ2B08

ユーザーズマニュアル

発行 エレコム株式会社