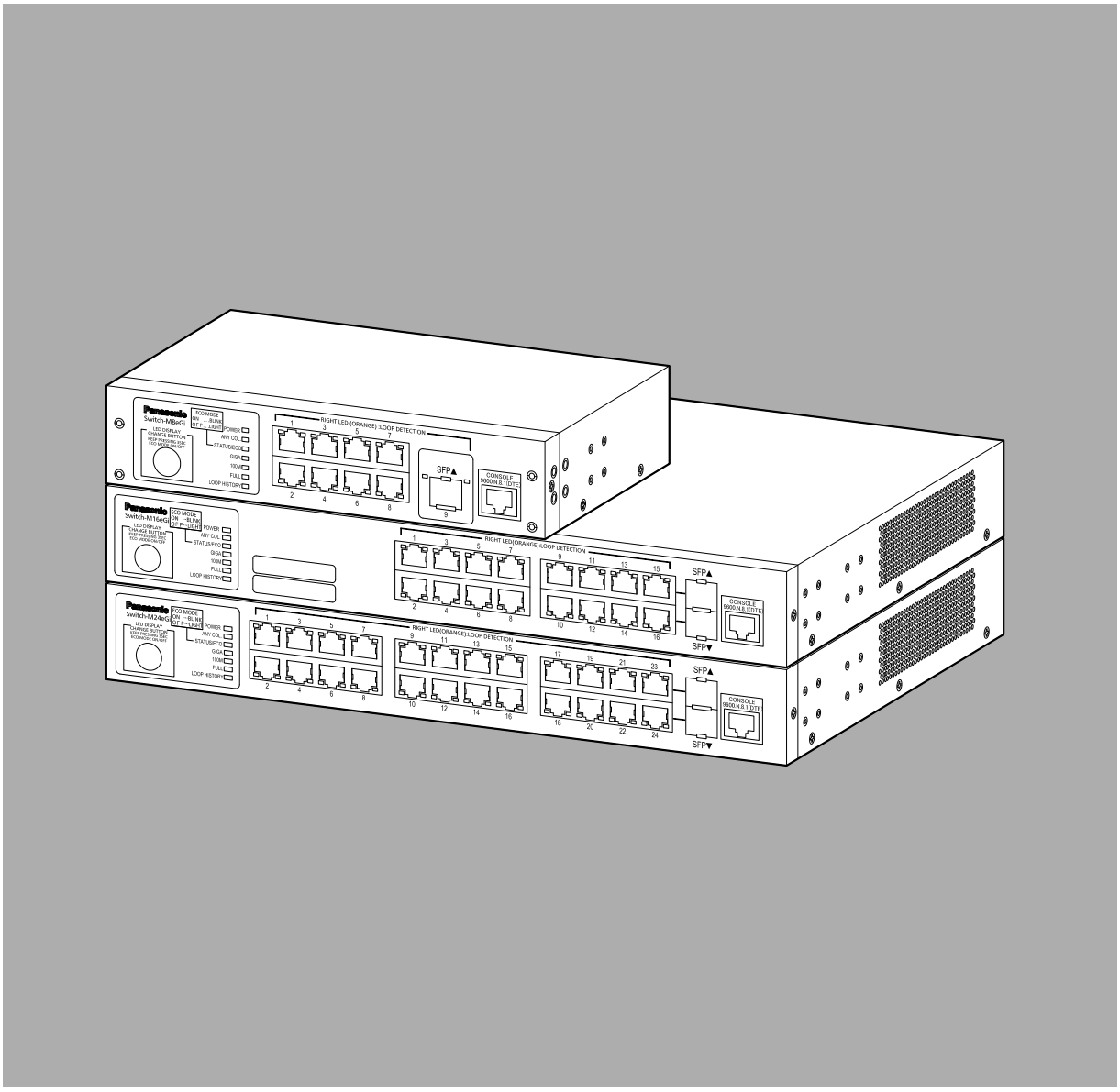
Panasonic®

レイヤ２スイッチングハブ

取扱説明書
WEB 編

品番 PN28080i/PN28160i
PN28240i



本取扱説明書は、以下の機種を対象としています。

品名	品番	ファームウェアバージョン
Switch-M8eGi	PN28080i	3.0.0.02 以上
Switch-M16eGi	PN28160i	3.0.0.02 以上
Switch-M24eGi	PN28240i	3.0.0.02 以上

目次

1. はじめに 6
2. Web ブラウザベースの管理 7
2.1. システム要件 7
2.2. WEB 管理機能へのアクセス 8
2.3. 基本情報の表示 11
3. スイッチの設定 13
3.1. 基本機能設定 13
3.1.1.管理情報設定 13
3.1.2.IP アドレス設定 14
3.1.3.SNMP 送信設定 16
3.1.4.SNMP ユーザ設定 17
3.1.5.SNMP ビュー設定 18
3.1.6.SNMP グループ設定 19
3.1.7.SNMP トラップ設定 20
3.1.8.トラップ送出設定 21
3.1.9.基本ポート設定 23
3.1.10.拡張ポート設定 25
3.1.11.ポート省電力設定 26
3.1.12.アクセス条件設定 28
3.1.13.Syslog 送信設定 30
3.1.14.RADIUS の設定 31
3.1.15.Telnet アクセス制限設定 32
3.1.16.ユーザ名／パスワード設定 33
3.1.17. MAC アドレス学習モード 34
3.1.18.FDB 手動登録 35
3.1.19.FDB テーブル 36
3.1.20.時刻設定 37
3.1.21.ARP エントリ手動登録 38
3.1.22.ARP テーブル 39
3.1.23.NDP テーブル 40
3.2. 拡張機能設定 41
3.2.1.VLAN 情報／修正 41
3.2.1.a. VLAN 修正 43
3.2.2.VLAN 作成 44
3.2.3.VLAN ポート設定 45
3.2.4.トラフィッククラス設定 46
3.2.5.帯域幅制御設定 47
3.2.6.リンクアグリゲーション設定 48
3.2.6.a. リンクアグリゲーション修正 49
3.2.7.ストームコントロール設定 50
3.2.8.認証状態テーブル 51

3.2.9.認証ログ 53
3.2.10.グローバル認証設定 55
3.2.11.ローカルユーザデータベース設定 56
3.2.12.ローカル MAC データベース設定 57
3.2.13.FDB からの MAC アドレスインポート 58
3.2.14.IEEE802.1X 認証設定 59
3.2.15.IEEE802.1X ポートベース認証設定 61
3.2.16.IEEE802.1X MAC 認証設定 63
3.2.17.IEEE802.1X MAC ベース認証サプリカントリスト 65
3.2.18.強制認証 MAC アドレス設定 67
3.2.19.IEEE802.1X 統計情報 68
3.2.20.EAP-Request 送信設定 71
3.2.21.未認証 MAC アドレス表示 72
3.2.22.MAC 認証設定 73
3.2.23.WEB 認証設定 75
3.2.24.WEB ページ表示設定 77
3.2.25.一時利用 DHCP サーバ設定 78
3.2.26.ダイナミック VLAN 設定 79
3.2.27.ポートモニタリングの設定 80
3.2.28.Classifier 設定 81
3.2.29.インプロファイルアクション設定 (In-Profile Action Config) 83
3.2.30.アウトプロファイルアクション設定 84
3.2.31.ポートリスト設定 85
3.2.32.ポリシー設定 86
3.2.33.ループ検知・遮断設定 87
3.2.34.ループヒストリー情報 89
3.2.35.PPS 設定 90
3.2.36.PPS 通知設定 92
3.2.37.PPS ポート設定 93
3.2.38.PPS ネイバー設定 94
3.2.39.PPS コネクション設定 96
3.2.40.ポートグルーピング設定 97
3.2.41.SFP モジュール状態確認（DDM）設定 99
3.2.42.マルチキャストグループの設定 101
3.3. システム管理ツール 102
3.3.1.ファームウェア更新 102
3.3.2.再起動 104
3.3.3.設定情報保存 106
3.3.4.統計情報の表示 (Statistics) 107
3.3.5.システムログ 110
3.3.6.設定ファイル転送 112
3.3.7.Ping の実行 114
3.3.8.例外処理の設定 116
3.3.9.Watchdog Timer 設定 117

付録 A.仕様 118
付録 B.IP アドレス簡単設定機能について 119

1.　はじめに

このたびは Switch-M8eGi/Switch-M16eGi/Switch-M24eGi（以下、この装置といいます）をご購入いただきありがとうございます。このマニュアルでは、この装置の WEB 管理機能を使用するのに必要な情報を説明します。

2. Web ブラウザベースの管理

Web ブラウザベースの管理機能（以下、WEB 管理機能）を使用すると、Microsoft Edge などの Web ブラウザを使用した管理作業（設定や監視など）が簡単になります。
Web ブラウザのユーザインターフェースを使用して、この装置をネットワーク上で設定および監視できます。また、装置の状態を表示できるため、この装置が離れた場所にある場合でも、すぐそばにあるように管理できます。

2.1. システム要件

WEB 管理機能を使用する前に、ネットワーク設定を行う必要があります。

1. システム IP アドレスの設定
   コンソールを使用して、この装置の IP アドレスを設定します。
   [Basic Switch Configuration...] > [System IP Configuration] > [Set IP Address] の順に選択して、IP アドレスを設定します。次に、[Set Subnet Mask] を選択してサブネットマスクを設定します。必要に応じて、[Set Default Gateway] を選択してデフォルトゲートウェイアドレスを設定します。
2. WEB 管理機能の有効化
   この装置の WEB 管理機能を有効にします。
   メインメニューから、[Basic Switch Configuration...] > [System Security Configuration] > [Web Server Status] の順に選択すると、コマンドプロンプトが「Enable or Disable web server(E/D)」に変わります。ここで「e」を入力すると、WEB 管理機能が有効になります。工場出荷時は「 Disable 」に設定されています。

WEB 管理機能の使用には WEB ブラウザ Microsoft Edge に搭載されている Internet Explorer モードの使用を推奨しています。また、ネットワークもしくはこの装置に直接接続されている必要があります。

ご注意： プロキシを使用すると、アクティブなウィンドウが正しく表示されない場合があります。プロキシを使用せずに直接アクセスすることをお勧めします。

2.2.　WEB 管理機能へのアクセス

WEB 管理機能を使用するには、この装置の IP アドレスまたは IPv6 アドレスを Web ブラウザのアドレスバーに入力し、Enter キーを押します。すると、**図 2-1** のようなログイン画面が表示されます。ユーザ名とパスワードを入力します。
工場出荷時のユーザ名とパスワードは、ともに「manager」です。

図 2-1 ログイン画面

ご注意：　ログイン画面が表示されない場合は、以下の点を確認してください。

(1) この装置の IP アドレス、サブネットマスク、デフォルトゲートウェイが正しく設定されていますか。
(2) この装置の IP アドレスが Web ブラウザに入力されていますか。
(3) WEB 管理機能が有効になっていますか。
(4) アクセスする端末のIPアドレスとこの装置のネットワークアドレスが一致していますか。

認証が正しく行われた場合は、図 2-2 のような表示言語選択画面が表示されます。

メニューへ表示させる言語の種類を選択して「OK」を押してください。

図 2-2 表示言語選択画面

言語の選択を行うことで、図 2-3 のようなメイン画面が表示されます。

図 2-3 メイン画面

メイン画面の左側に、利用可能な項目の一覧が表示されます。

(1) 基本情報
この装置の基本情報が一覧で表示されます。

(2) 基本機能設定
IP アドレスやポート設定などの基本機能を設定します。

(3) 拡張機能設定
VLAN、QoS などの拡張機能を設定します。

(4) システム管理ツール
この管理ツールを使用して、ファームウェアの更新およびシステムログの閲覧を行います。

運用管理を実施する場合は、まず「基本機能設定」を行い、その後で他の詳細設定を行うようお勧めします。

2.3.　基本情報の表示

[基本情報] を選択すると、図 2-4 のような画面が表示されます。この画面には、この装置の基本情報が一覧で表示されます。

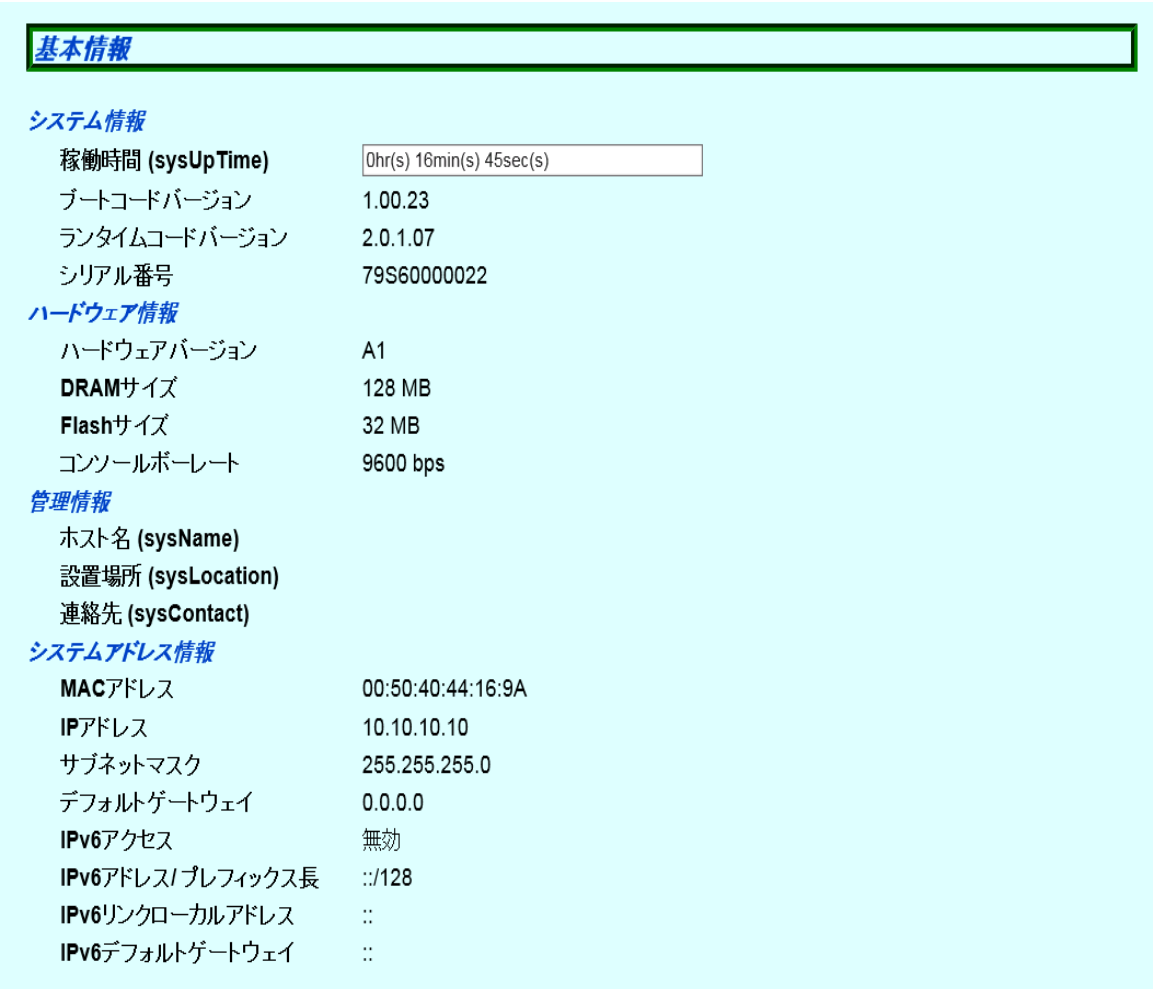


図 2-4 基本情報

画面の説明

システム情報	この装置の稼働時間、ファームウェアバージョンが表示されます。	
	稼働時間	この装置が起動してからの通算の時間が表示されます。
	ブートコードバージョン	この装置のファームウェアのバージョンが表示されます。 * ファームウェアの更新（3.3.1 項で説明）は、ランタイムコードのみが対象です。
	ランタイムコードバージョン	
ハードウェア情報	ハードウェアの情報が表示されます。	
	ハードウェアバージョン	ハードウェアのバージョンが表示されます。
	DRAM サイズ	実装されている DRAM の容量が表示されます。
	Flash サイズ	実装されている Flash メモリの容量が表示されます。
	コンソールボーレート	コンソールのボーレートが表示されます。
管理情報	3.1.1 項の「管理情報設定」の説明に従って、ここに表示される項目を設定します。	
	ホスト名	設定したこの装置の名前が表示されます。工場出荷時には何も設定されていません。設定については、3.1.1 項を参照してください。
	設置場所	設定したこの装置の設置場所が表示されます。工場出荷時には何も設定されていません。設定については、3.1.1項を参照してください。
	連絡先	連絡先が表示されます。工場出荷時には何も設定されていません。設定については、3.1.1 項を参照してください。
システムアドレス情報	3.1.2 項の「IP アドレス設定」の説明に従って、ここに表示される項目を設定します。	
	MAC アドレス	この装置の MAC アドレスが表示されます。この値は個々の装置ごとに固有であるため、変更することはできません。
	IP アドレス	この装置に設定されている IP アドレスが表示されます。工場出荷時には何も設定されていませんので、「0.0.0.0」と表示されます。設定については、3.1.2 項を参照してください。
	サブネットマスク	この装置に設定されているサブネットマスクが表示されます。工場出荷時には何も設定されていませんので、「0.0.0.0」と表示されます。設定については、3.1.2 項を参照してください。
	デフォルトゲートウェイ	デフォルトゲートウェイとなるルータの IP アドレスが表示されます。工場出荷時には何も設定されていませんので、「0.0.0.0」と表示されます。設定については、3.1.2 項を参照してください。
	IPv6 アクセス	IPv6 アドレスの有効・無効が表示されます。
	IPv6 アドレス／プレフィックス長	本装置に設定されているIPv6アドレスとプレフィックス長を表示します。工場出荷時には何も設定されていないため「::/128」と表示されます。設定については 3.1.2 項を参照してください。
	IPv6 リンクローカルアドレス	本装置に設定されている IPv6 リンクローカルアドレスを表示します。工場出荷時には何も設定されていないため「::」と表示されます。設定については 3.1.2 項を参照してください。
	IPv6 デフォルトゲートウェイ	デフォルトゲートウェイとなるルータの IPv6 アドレスを表示します。工場出荷時には何も設定されていないため「::」と表示されます。設定については 3.1.2 項を参照してください。

3.　スイッチの設定

設定が完了したら、3.3.3 項に従って設定情報を保存する必要があります。設定情報を保存しない限り、再起動後にこれまでの設定が反映されません。

3.1.　基本機能設定

3.1.1.　管理情報設定

[基本機能設定] から [管理情報設定] を選択すると、図 3-1 のような画面が表示されます。この画面は、この装置の情報を表示する場合に選択します。この画面では、機器名称などの管理情報を設定します。

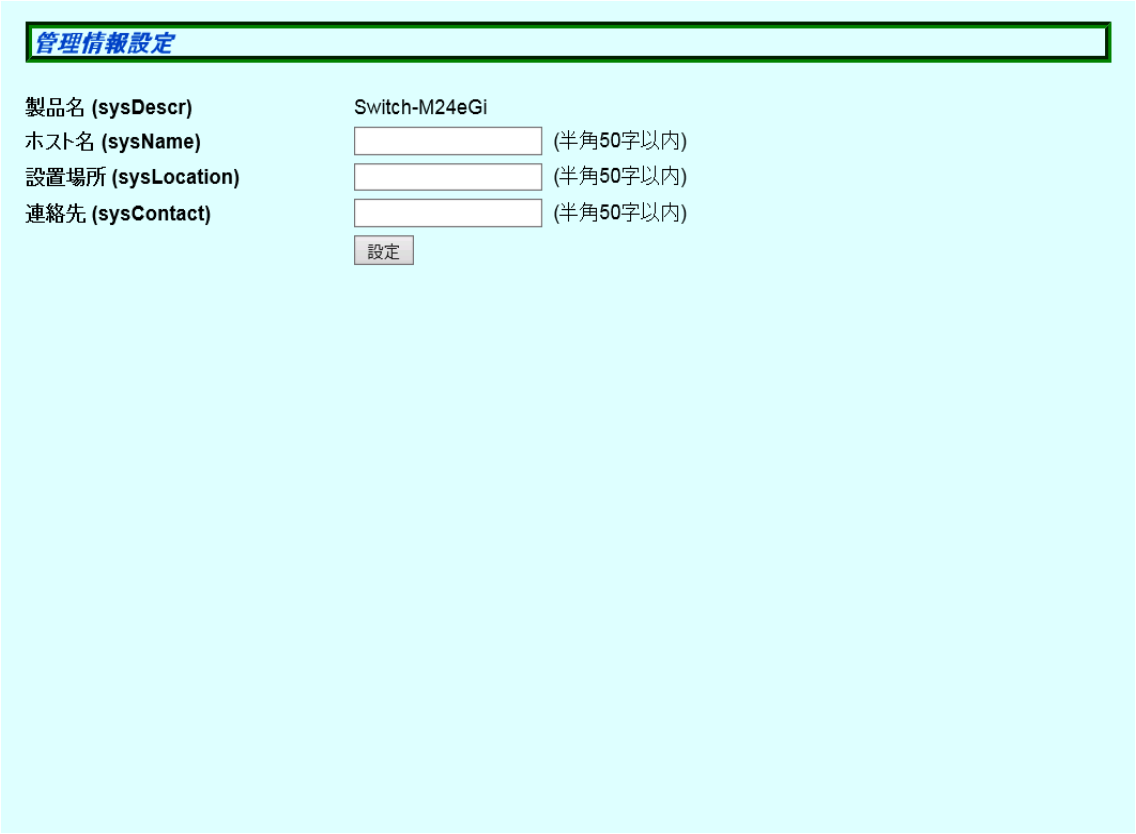


図 3-1 管理情報設定

画面の説明

製品名	システムの説明です。変更できません。
ホスト名	システム名が表示されます。工場出荷時には何も設定されていません。
設置場所	設置場所が表示されます。工場出荷時には何も設定されていません。
連絡先	連絡先が表示されます。工場出荷時には何も設定されていません。

3.1.2.　IP アドレス設定

[基本機能設定] から [IP アドレス設定] を選択すると、図 3-2 のような画面が表示されます。この画面では、この装置の IP アドレスを設定します。

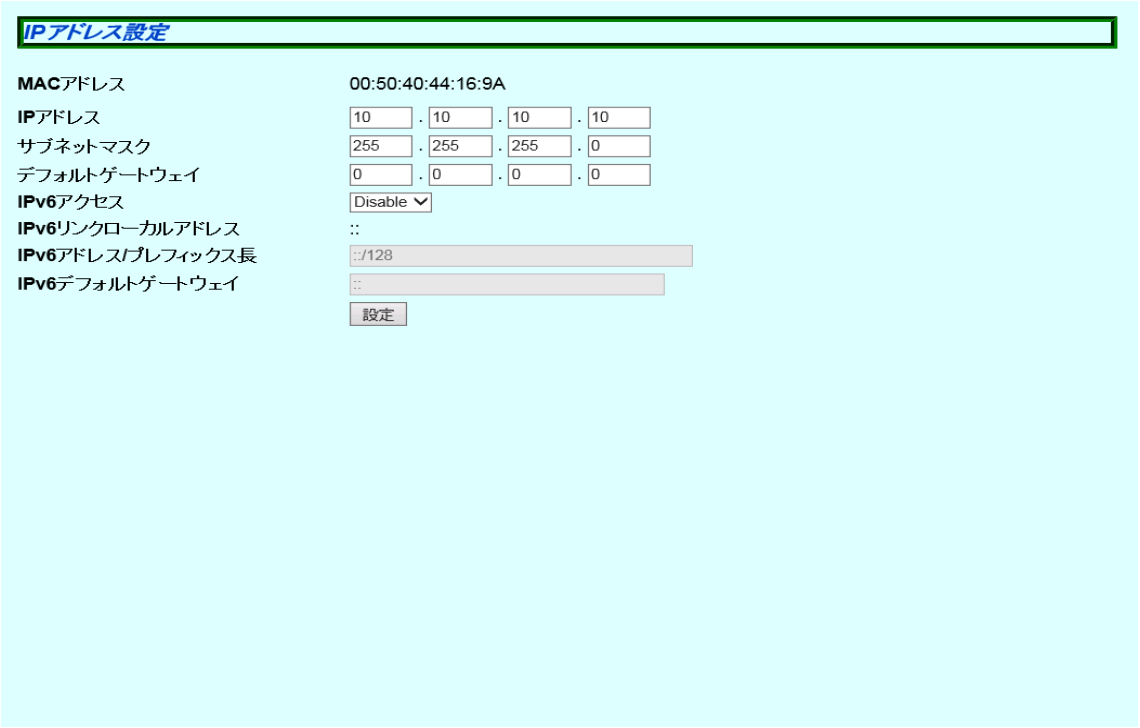


図 3-2 IP アドレス設定

画面の説明

MAC アドレス	この装置の MAC アドレスが表示されます。 この項目は個々の装置ごとに固有であるため、変更することはできません。	
IP アドレス	現在設定されている IP アドレスが表示されます。 工場出荷時には何も設定されていませんので、「0.0.0.0」と表示されます。	
サブネットマスク	現在設定されているサブネットマスクが表示されます。 工場出荷時には何も設定されていませんので、「0.0.0.0」と表示されます。	
デフォルトゲートウェイ	現在設定されているデフォルトゲートウェイとなるルータの IP アドレスが表示されます。 工場出荷時には何も設定されていませんので、「0.0.0.0」と表示されます。	
IPv6 アクセス	IPv6 でのアクセスの有効・無効が表示されます。	
	Enable	IPv6 アクセスを有効にします。
	Disable	IPv6 アクセスを無効にします。（工場出荷時設定）
IPv6 リンクローカルアドレス	現在設定されている IPv6 リンクローカルアドレスを表示します。工場出荷時は設定されていないため「::」と表示されます。	
IPv6 アドレス／プレフィックス長	現在設定されている IPv6 アドレスとプレフィックス長を表示します。工場出荷時は設定されていないため「::/128」と表示されます。	
IPv6 デフォルトゲートウェイ	現在設定されているデフォルトゲートウェイとなるルータの IPv6 アドレスを表示します。工場出荷時は設定されていないため「::」と表示されます。	

ご注意： この項目を設定しなければ SNMP 管理機能と Telnet、SSH によるリモート接続は使用できません。必ず設定してください。どのように設定すればよいか分からない場合は、ネットワーク管理者にご相談ください。IP アドレスはネットワーク上の他の装置のものと重複してはいけません。また、この項目にはこの装置を利用するサブネット上の他の装置と同様のサブネットマスクとデフォルトゲートウェイを設定してください。

3.1.3. SNMP 送信設定

[基本機能設定] から [SNMP 設定]、[SNMP 送信設定] の順に選択すると、図 3-3 のような画面が表示されます。この画面では、SNMP マネージャの設定を行います。

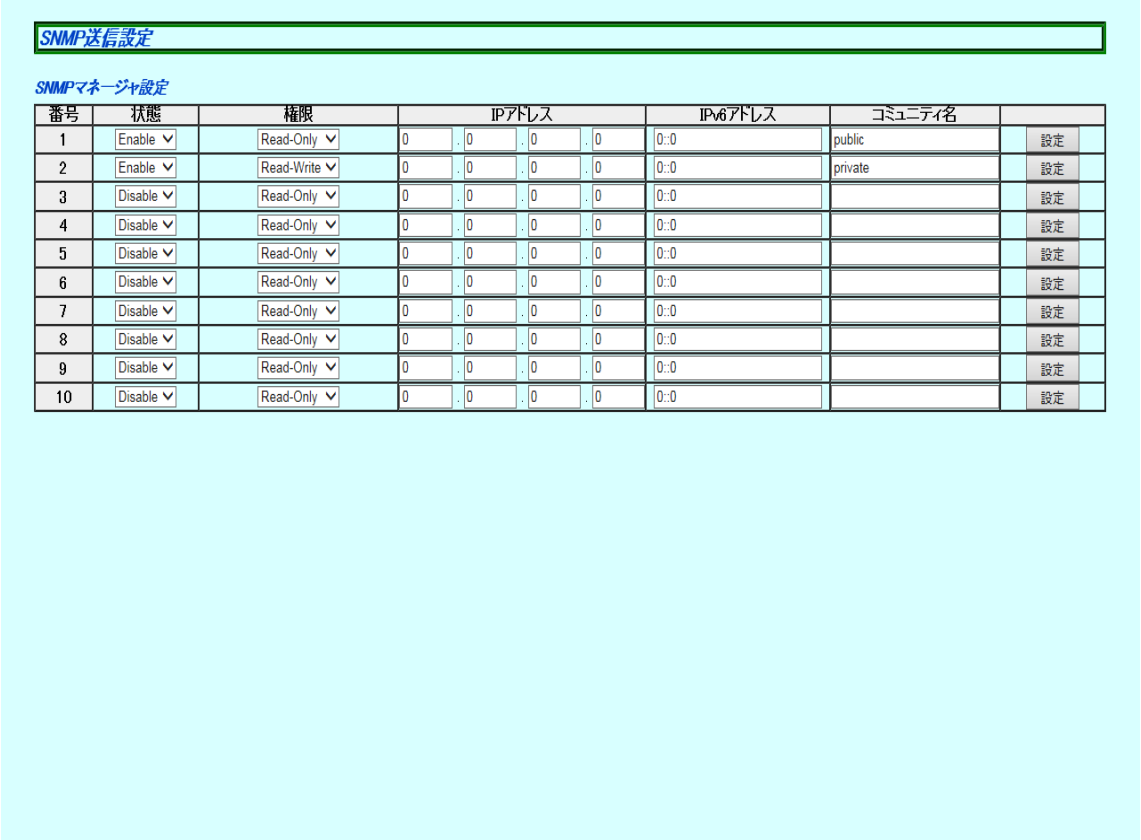


図 3-3 SNMP 送信設定

画面の説明

番号	SNMP マネージャリストのエントリ番号です。	
状態	SNMP マネージャの状態が表示されます。	
	Enable	SNMP マネージャが有効であることを表します。
	Disable	SNMP マネージャは無効であることを表します。
権限	SNMP マネージャのアクセス権限が表示されます。	
	Read-Write	読み書きともに可能です。
	Read-Only	読み取りのみ可能です。
IP アドレス	SNMP マネージャの IP アドレスです。	
IPv6 アドレス	SNMP マネージャの IPv6 アドレスです。	
コミュニティ名	SNMP アクセスに使用するコミュニティ名です。	

3.1.4.　SNMP ユーザ設定

[基本機能設定] から [SNMP 設定]、[SNMP ユーザ設定] の順に選択すると、**図 3-4** のような画面が表示されます。この画面では、SNMP マネージャの設定を行います。

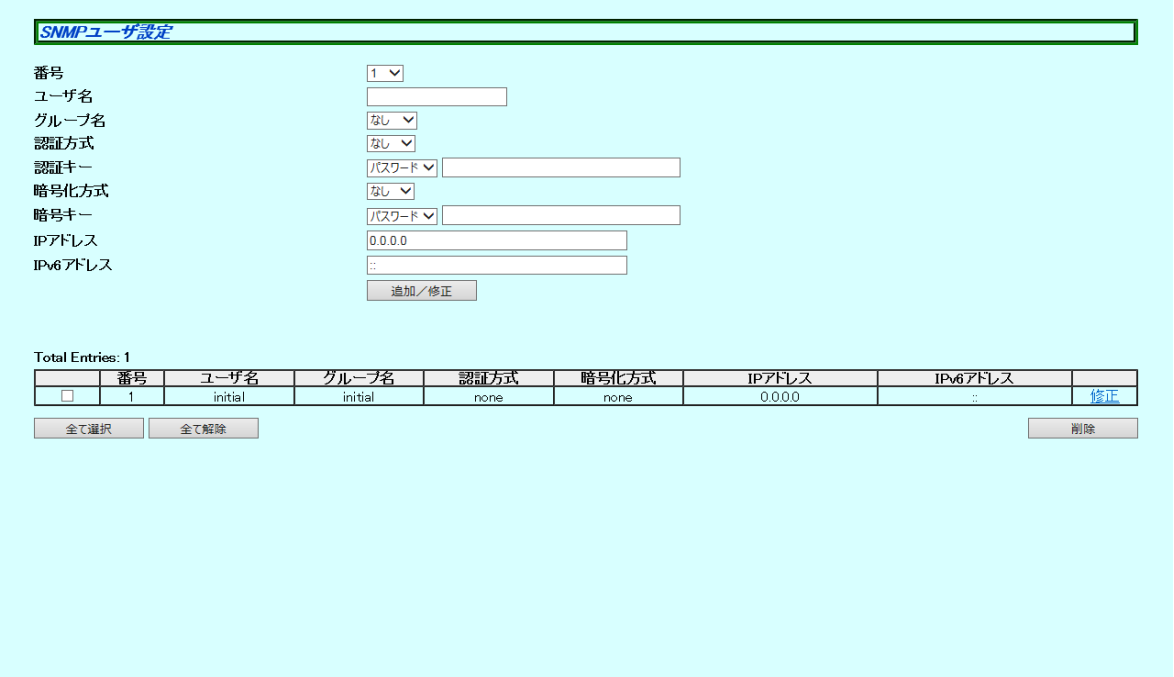


図 3-4 SNMP ユーザ設定

画面の説明

Total Entry	作成されている SNMP のユーザの数 (index の数) を表示します。
番号	SNMP のユーザのエントリ番号です。
ユーザ名	SNMP のユーザ名を表示します。
グループ名	SNMP のグループ名を表示します。
認証方式	認証方式を表示します。認証方式は、(なし),MD5,SHA が使用されます。
認証キー	認証キーを設定します。Password,Key を指定してパスワード , キーを入力します。
暗号化方式	暗号化方式を表示します。暗号化方式は、(なし),DES が使用されます。
暗号キー	暗号キーを設定します。Password,Key を指定してパスワード , キーを入力します。
IPv4 アドレス	SNMP アクセスが可能な IPv4 アドレスを表示します。
IPv6 アドレス	SNMP アクセスが可能な IPv6 アドレスを表示します。

3.1.5.　SNMP ビュー設定

[基本機能設定] から [SNMP 設定]、[SNMP ビュー設定] の順に選択すると、**図 3-5** のような画面が表示されます。この画面では、SNMP マネージャの設定を行います。

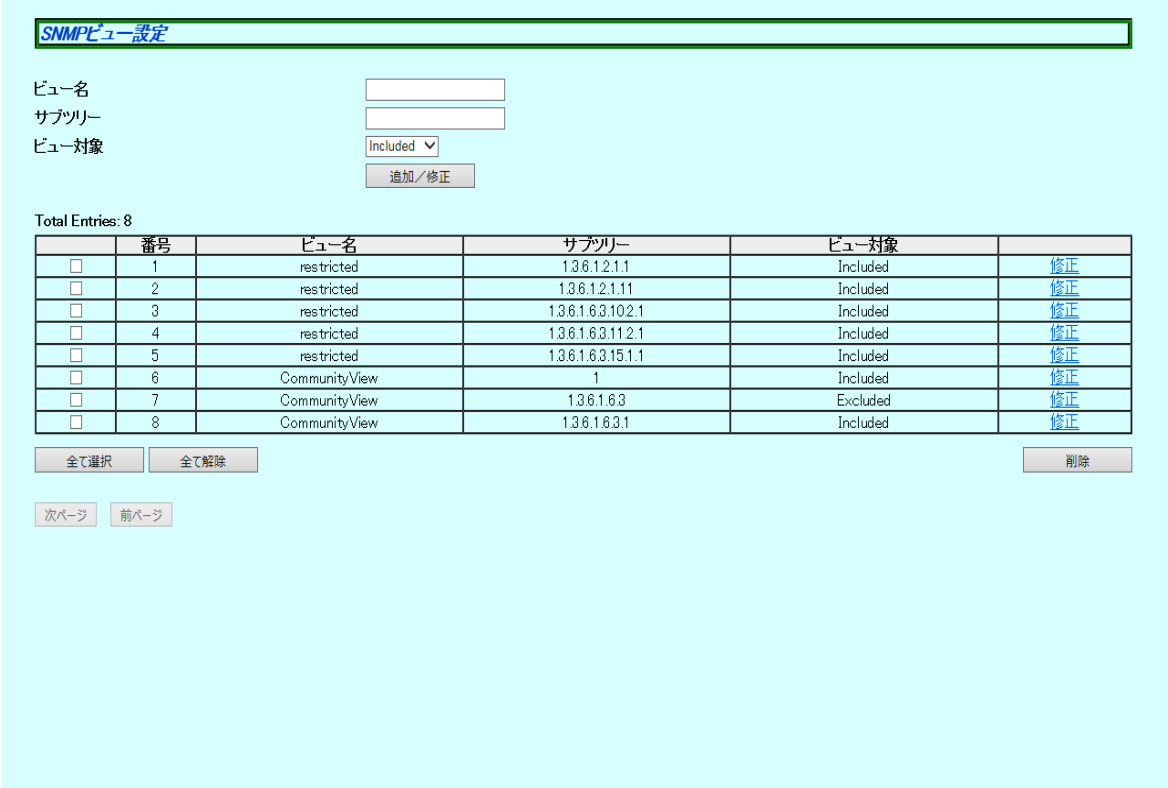


図 3-5 SNMP ビュー設定

画面の説明

Total Entries	作成されている SNMP ビューのエントリ数を表示します。
番号	SNMP ビューのエントリ番号です。
ビュー名	SNMP ビューの名称を表示します。
サブツリー	SNMP ビューのサブツリーを表示します。
ビュー対象	SNMP ビューのタイプを表示します。タイプは、包含 , 除外が使用されます。

3.1.6.　SNMP グループ設定

[基本機能設定] から [SNMP 設定]、[SNMP グループ設定] の順に選択すると、**図 3-6** のような画面が表示されます。この画面では、SNMP マネージャの設定を行います。

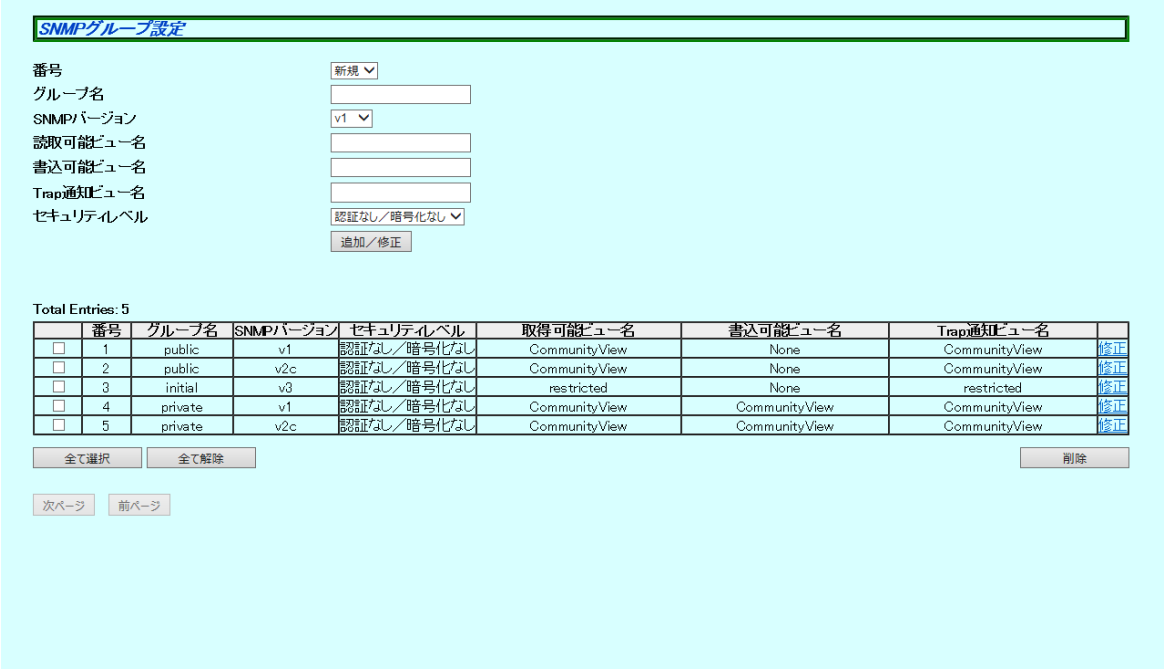


図 3-6 SNMP グループ設定

画面の説明

Total Entry	作成されている SNMP グループのエントリ数を表示します。
番号	SNMP グループのエントリ番号です。
グループ名	SNMP グループの名称を表示します。
SNMP バージョン	SNMP グループのバージョンを表示します。バージョンは、v1,v2c,v3 が使用されます。
取得可能ビュー名	読み込むビューの名称を表示します。
書込可能ビュー名	書き込むビューの名称を表示します。
Trap 通知ビュー名	通知するビューの名称を表示します。
セキュリティレベル	SNMP グループのセキュリティレベルを表示します。セキュリティレベルは、認証なし／暗号化なし , 認証あり／暗号化なし , 認証あり／暗号化ありが使用されます。

3.1.7.　SNMP トラップ設定

[基本機能設定] から [SNMP 設定]、[SNMP トラップ設定] の順に選択すると、図 3-7 のような画面が表示されます。この画面では、SNMP トラップの設定を行います。

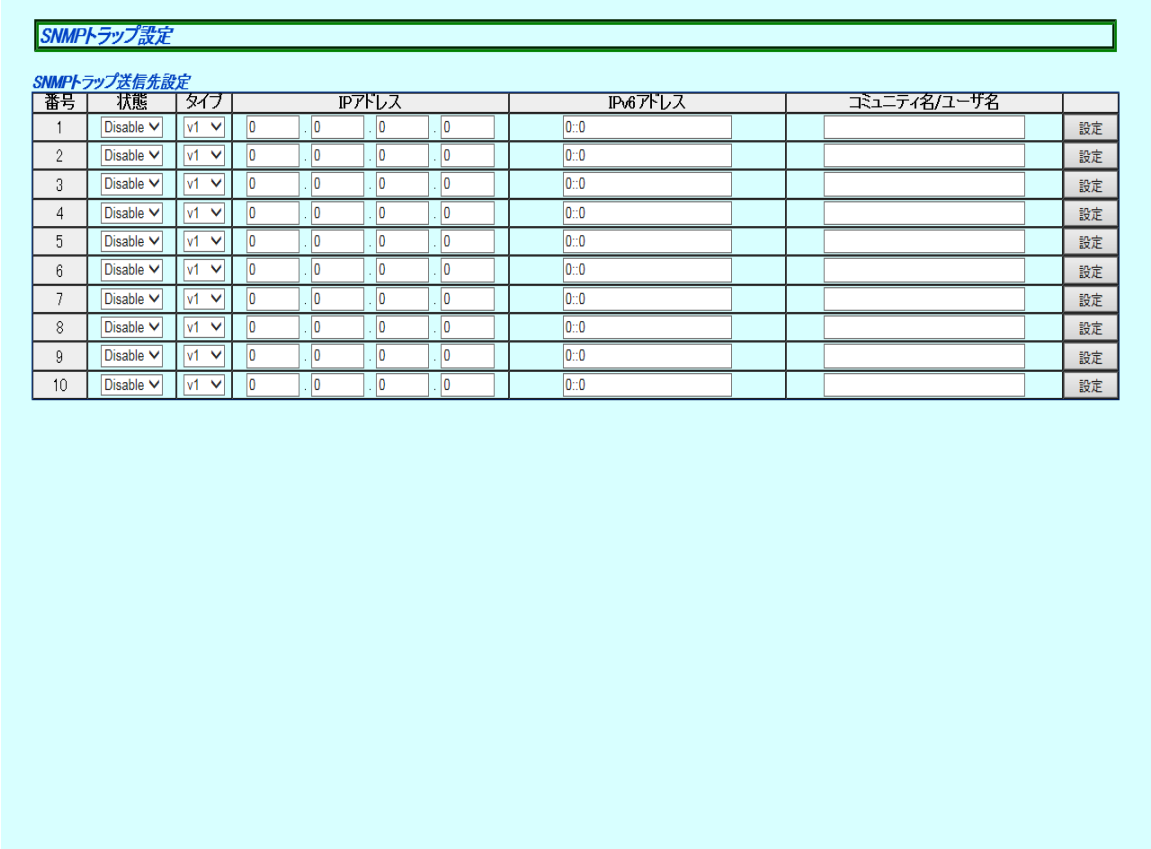


図 3-7 SNMP トラップ設定

画面の説明

番号	トラップ送信先のエントリ番号です。	
状態	トラップを送信するかどうかが表示されます	
	Enable	トラップを送信します。
	Disable	トラップを送信しません。（工場出荷時設定）
権限	トラップの種類が表示されます。	
	v1	SNMP v1 のトラップを送信します。（工場出荷時設定）
	v2c	SNMP v2c のトラップを送信します。
	v3	SNMP v3 のトラップを送信します。
IP アドレス	トラップ送信先の IP アドレスです。	
IPv6 アドレス	トラップ送信先の IPv6 アドレスです。	
コミュニティ名	トラップ送信に使用するコミュニティ名です。	

3.1.8. トラップ送出設定

[基本機能設定] から [SNMP 設定]、[トラップ送出設定] の順に選択すると、図 3-8 のような画面が表示されます。この画面では、トラップ送出の操作を設定します。

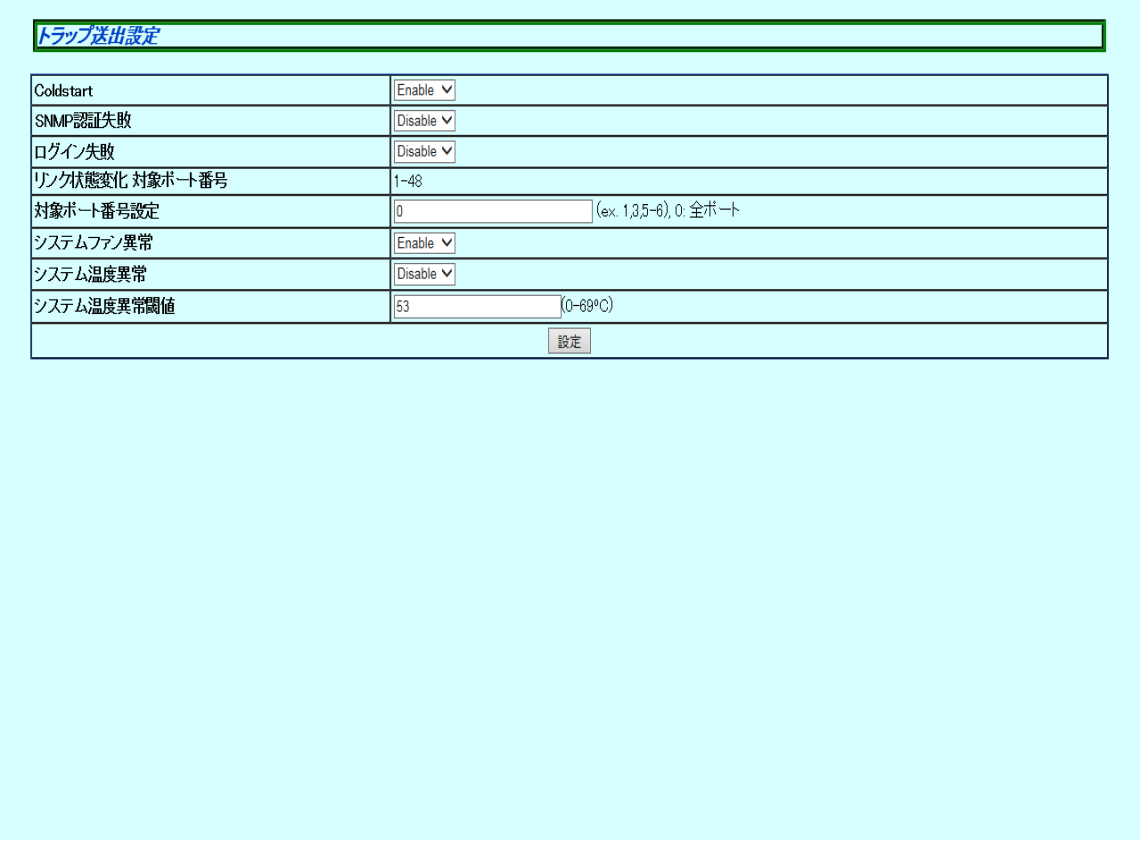


図 3-8 トラップ送出設定

画面の説明

Coldstart	機器起動時のトラップ送出の有効・無効の設定を表示します。	
	Enabled	トラップ送出を有効にします。
	Disabled	トラップ送出を無効にします。(工場出荷時設定)
SNMP Authentication Failure	SNMP 認証失敗時のトラップ送出の有効・無効の設定を表示します。	
	Enabled	トラップ送出を有効にします。
	Disabled	トラップ送出を無効にします。(工場出荷時設定)
Login Failure	ログイン失敗時のトラップ送出の有効・無効の設定を表示します。	
	Enabled	トラップ送出を有効にします。
	Disabled	トラップ送出を無効にします。(工場出荷時設定)
リンク状態変化	リンク状態変更時のトラップ送出の対象ポートを表示・設定します。	
	対象ポート番号	設定済の対象ポートが表示されます。
	対象ポート番号設定	トラップ送出の対象ポートを設定します。
システム温度異常	システム温度異常時のトラップ送出の有効・無効の設定が表示されます。	
	Enable	トラップ送出を有効にします。
	Disable	トラップ送出を無効にします。（工場出荷時設定）
システム温度異常閾値	トラップ送出される温度の閾値設定が表示されます。	
システムファン異常	システムファン異常時のトラップ送出の有効・無効の設定が表示されます。	
	Enable	トラップ送出を有効にします。（工場出荷時設定）
	Disable	トラップ送出を無効にします。

3.1.9.　基本ポート設定

[基本機能設定] から [ポート設定]、[基本ポート設定] の順に選択すると、図 3-9 のような画面が表示されます。この画面では、各ポートの状態表示設定、モードなどの設定を行います。

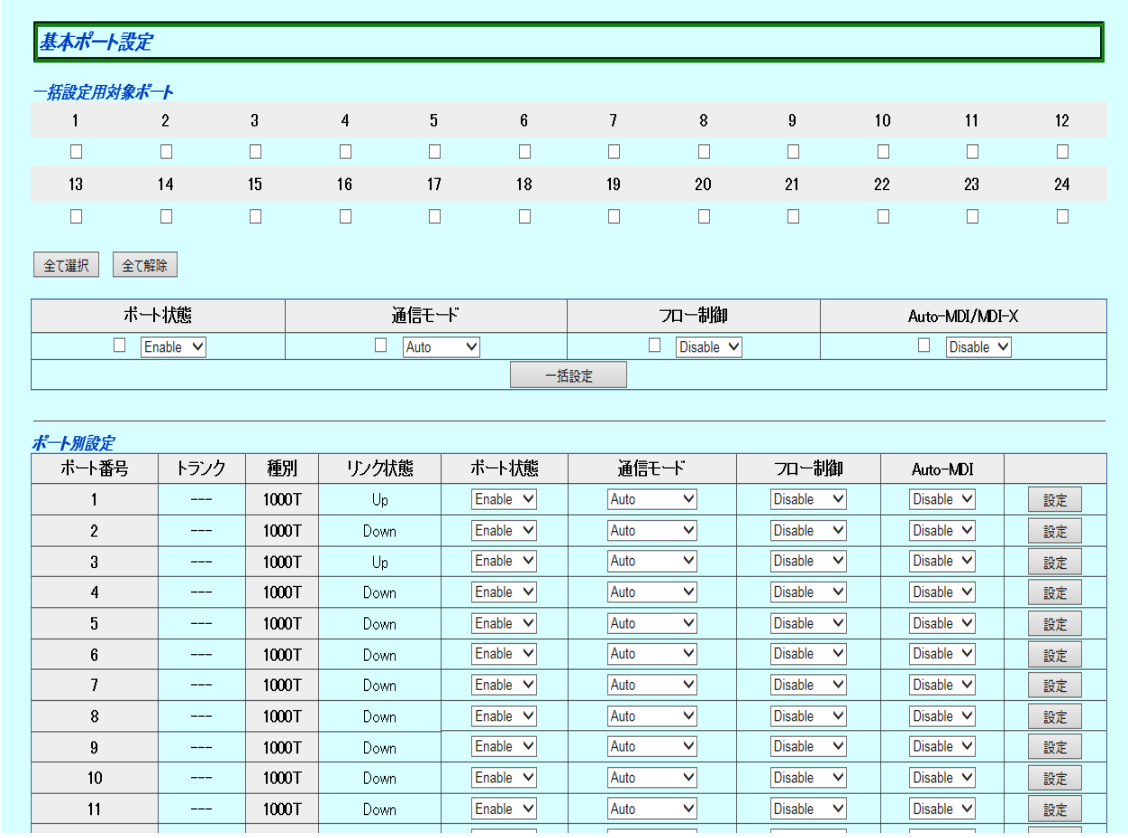


図 3-9 基本ポート設定

画面の説明

一括設定用 対象ポート	複数のポートに対して一括設定を行う際の対象ポートを選択します。 [全て選択] ボタンをクリックすると、全ポートが選択されます。 [全て解除] ボタンをクリックすると、全ポートが選択解除されます。 一括設定用項目を選択・変更後、[一括設定] ボタンをクリックすると、選択中のポートに対して 同一の設定が反映されます。	
ポート番号	ポート番号が表示されます。	
トランク	トランキングの設定状態がグループ番号で表示されます。	
種別	ポートの種類が表示されます。	
	1000T	1000BASE-T を表します。
	1000X	SFP ポートを表します。
リンク状態	現在のリンクの状態が表示されます。	
	Up	リンクが正常に確立した状態を表します。
	Down	リンクが確立していない状態を表します。
ポート状態	現在のポートの状態が表示されます。工場出荷時は全て「 Enable 」に設定されています。	
	Enable	ポートが使用可能です。
	Disable	ポートが使用不可です。
通信モード	通信速度、全 / 半二重の設定状態が表示されます。 工場出荷時は全て「Auto」に設定されています。	
	Auto	オートネゴシエーションモード
	100M/Full	100Mbps 全二重
	100M/Half	100Mbps 半二重
	10M/Full	10Mbps 全二重
	10M/Half	10Mbps 半二重
フロー制御	フローコントロールの設定状態が表示されます。 工場出荷時は全て「 Disable 」に設定されています。	
	Enable	フローコントロール機能が有効であることを表します。
	Disable	フローコントロール機能が無効であることを表します。
Auto-MDI	Auto MDI/MDI-X 機能の設定状態が表示されます。工場出荷時はダウンリンクポートは「 Disable 」、アップリンクツイストペアポートは「Enable」に設定されています。	
	Enable	Auto MDI/MDI-X 機能が有効であることを表します。
	Disable	Auto MDI/MDI-X 機能が無効であることを表します。

3.1.10. 拡張ポート設定

[基本機能設定] から [ポート設定]、[拡張ポート設定] の順に選択すると、図 3-10 のような画面が表示されます。この画面では、各ポートの状態表示設定、モードなどの設定を行います。

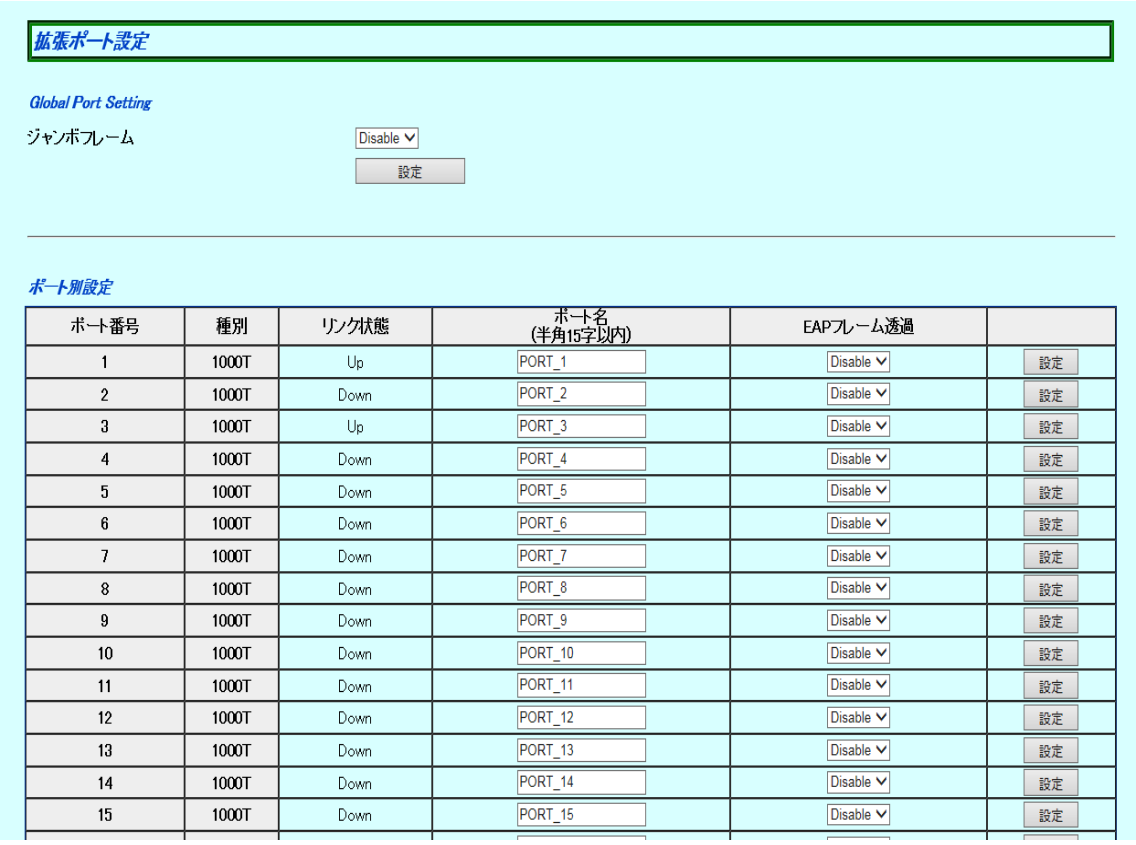


図 3-10 拡張ポート設定

画面の説明

ジャンボフレーム	ジャンボフレームの設定状態が表示されます。	
	Enable	ジャンボフレームが有効であることを表します。
	Disable	ジャンボフレームが無効であることを表します。 (工場出荷時設定)
ポート番号	ポート番号が表示されます。	
種別	ポートの種類が表示されます。	
	1000T	1000BASE-T を表します。
	1000X	SFP 拡張ポートを表します。
リンク状態	現在のリンクの状態が表示されます。	
	Up	リンクが正常に確立した状態を表します。
	Down	リンクが確立していない状態を表します。
ポート名	ポートの名称が表示されます。	
EAP フレーム透過	EAP フレーム透過機能の設定状態が表示されます。全てのポートが工場出荷時は「 Disable 」に設定されています。この項目を「Enable」にすると、IEEE802.1X 認証で使用する EAP フレームが透過されます。この項目を「Disable」に設定すると、EAP フレームが破棄されます。	
	Enable	EAP フレーム透過機能が有効であることを表します。
	Disable	EAP フレーム透過機能が無効であることを表します。

3.1.11. ポート省電力設定

[基本機能設定] から [ポート設定]、[ポート省電力設定] の順に選択すると、図 3-11 のような画面が表示されます。この画面では、ポートの省電力設定を行います。

図 3-11 ポート省電力設定

画面の説明

一括設定用 対象ポート	複数のポートに対して一括設定を行う際の対象ポートを選択します。 [全て選択] ボタンをクリックすると、全ポートが選択されます。 [全て解除] ボタンをクリックすると、全ポートが選択解除されます。 一括設定用項目を選択・変更後、[一括設定] ボタンをクリックすると、選択中のポートに対して同一の設定が反映されます。	
ポート番号	ポート番号が表示されます。	
種別	ポートの種類が表示されます。	
	1000T	1000BASE-T を表します。
	1000X	SFP 拡張ポートを表します。
リンク状態	現在のリンクの状態が表示されます。	
	Up	リンクが正常に確立した状態を表します。
	Down	リンクが確立していない状態を表します。
省電力モード	省電力モードの設定が表示されます。工場出荷時は全て「Half」に設定されています。	
	Full	MNO シリーズ省電力モードの状態が有効 (Full) であることを表します。
	Half	MNO シリーズ省電力モードの状態が有効 (Half) であることを表します。
	Disable	MNO シリーズ省電力モードの状態が無効であることを表します。

省電力型イーサネット (EEE)	EEE(Energy Efficient Ethernet) の状態が表示されます。 工場出荷時は全て「 Disabled 」に設定されています。	
	Enabled	EEE の状態が有効であることを表します。
	Disabled	EEE の状態が無効であることを表します。

3.1.12. アクセス条件設定

[基本機能設定] から [アクセス条件設定]、[アクセス条件設定] の順に選択すると、図 3-12 のような画面が表示されます。この画面では、設定・管理時にこの装置にアクセスする際の諸設定を行います。

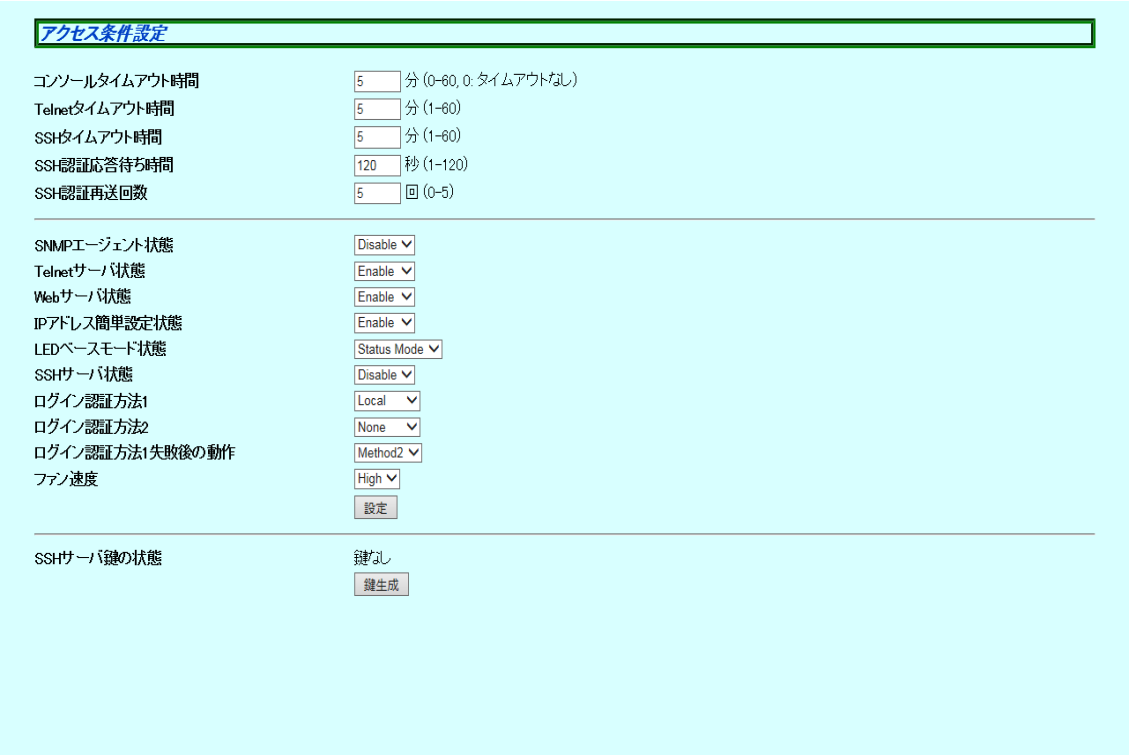


図 3-12 アクセス条件設定

画面の説明

コンソールタイムアウト時間	コンソールで接続しているときに、何も入力がなかった場合のセッションが切れるまでの時間が分単位で表示されます。工場出荷時は 5 分に設定されています。	
Telnetタイムアウト時間	Telnet でリモート接続しているときに、何も入力がなかった場合のセッションが切れるまでの時間が分単位で表示されます。工場出荷時は 5 分に設定されています。	
SSH タイムアウト時間	SSH でリモート接続しているときに、何も入力がなかった場合のセッションが切れるまでの時間が秒単位で表示されます。工場出荷時は 5 分に設定されています。	
SSH 認証応答待ち時間	SSH 認証に対する応答の待ち時間が表示されます。 工場出荷時は 120 秒に設定されています。	
SSH 認証再送回数	SSH 認証の再送回数が表示されます。 工場出荷時は 5 回に設定されています。	
SNMPエージェント状態	SNMP でのアクセスを可能にするかどうかが表示されます。工場出荷時は「Disabled」に設定されています。	
	Enable	アクセス可
	Disable	アクセス不可
Telnet サーバ状態	Telnet でのアクセスを可能にするかどうかが表示されます。工場出荷時は「Enable」に設定されています。	
	Enable	アクセス可
	Disable	アクセス不可

Web サーバ状態	Web でのアクセスを可能にするかどうかが表示されます。工場出荷時は「Disable」に設定されています。	
	Enable	アクセス可
	Disable	アクセス不可
IP アドレス簡単設定状態	IP アドレス設定ソフトウェアでのアクセスを可能にするかどうかが表示されます。工場出荷時は「Enable」に設定されています。※ 注意事項などにつきましては、付録 B をご確認ください。	
	Enable	アクセス可
	Disable	アクセス不可
LED ベースモード状態	現在の LED ベースモードが表示されます。 工場出荷時は「Status Mode」に設定されています。	
	Status Mode	ステータスモードで動作中であることを表します。
	Eco Mode	ECO モードで動作中であることを表します。
SSH サーバ状態	SSH でのアクセスを可能にするかどうかが表示されます。工場出荷時は「Disable」に設定されています。	
	Enable	アクセス可
	Disable	アクセス不可
ログイン認証方法 1/2	ログインする際に使用するユーザ名、パスワードの確認方法が表示されます。 工場出荷時は 1 が「Local」、2 が「None」に設定されています。	
	Local	この装置に設定したユーザ名、パスワードでログインします。
	RADIUS	RADIUS サーバによる認証を利用してログインします。
	None	ログイン認証方法 2 を使用しません。
Method 1 Fail Action	ログイン認証方式 1 で認証が拒否された場合の動作を表示します。 工場出荷時は「 Method 2 」に設定されています。	
	Method 2	ログイン認証方式 1 で認証が拒否された場合に、続けてログイン認証方式 2 の認証処理を実行します。
	Stop	ログイン認証方式 1 で認証が拒否された場合に、認証処理を停止します。ログイン認証方式 1 が RADIUS、かつ全ての RADIUS サーバからの応答がなかった場合に限り、ログイン認証方式 2 の認証処理を実行します。
SSH サーバ鍵の状態	SSH サーバ鍵の状態が表示されます。 [鍵生成] ボタンをクリックすると、SSH サーバ鍵が生成されます。	
	鍵あり	サーバ鍵は存在します。
	鍵なし	サーバ鍵は存在しません。

3.1.13. Syslog 送信設定

[基本機能設定] から [アクセス条件設定]、[Syslog 送信設定] の順に選択すると、**図 3-13** のような画面が表示されます。この画面では、システムログの送信先とする Syslog サーバの設定を行います。

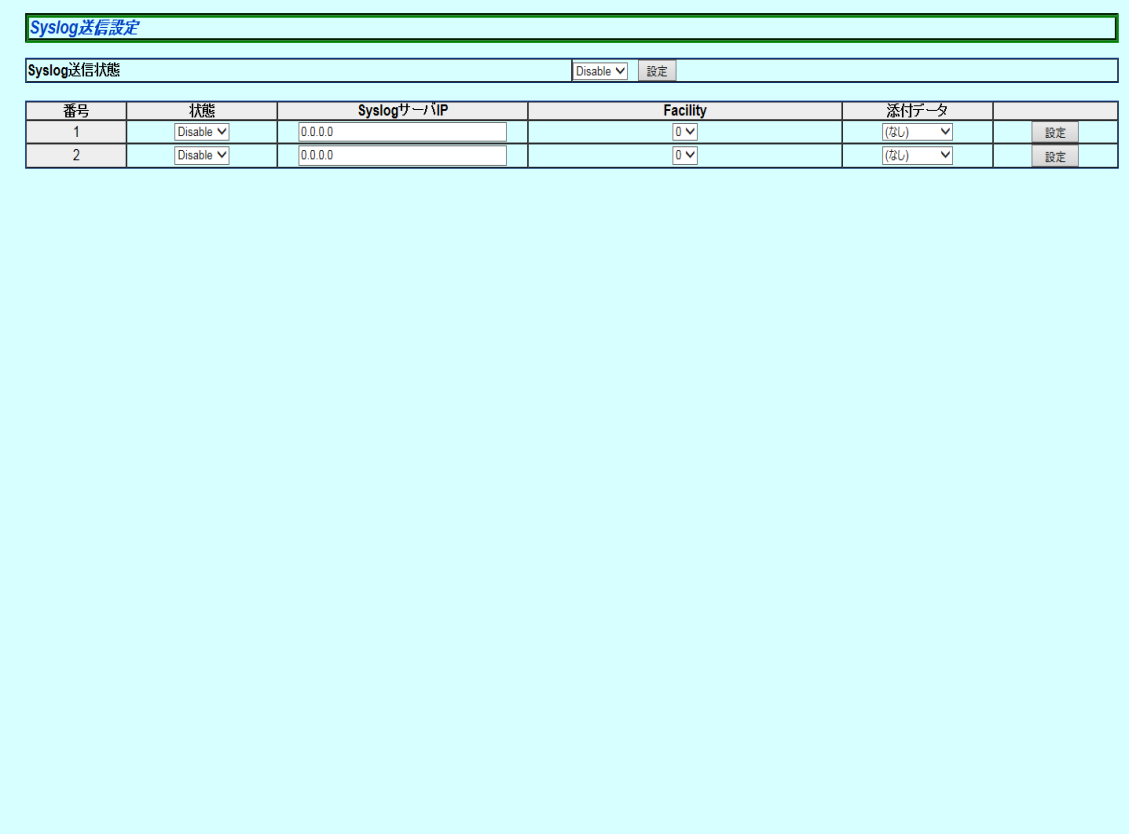


図 3-13 Syslog 送信設定

画面の説明

Syslog 送信状態	Syslog サーバへシステムログを送信するかどうかが表示されます。 工場出荷時は「 Disable 」に設定されています。	
	Enable	Syslog サーバへシステムログを送信します。
	Disable	Syslog サーバへシステムログを送信しません。
番号	Syslog 送信設定のエントリ番号です。	
状態	各エントリの状態が表示されます。 工場出荷時は「 Disable 」に設定されています。	
	Enable	対象エントリの設定が有効です。
	Disable	対象エントリの設定が無効です。
Syslog サーバ IP	Syslog サーバの IP アドレスが表示されます。	
Facility	Facility の値が表示されます。	
添付データ	追加する情報が表示されます。	
	SysName	送信するシステムログにこの装置の SysName を追加します。
	IP アドレス	送信するシステムログにこの装置の IP Address を追加します。

3.1.14. RADIUS の設定

[基本機能設定] から [アクセス条件設定]、[RADIUS 設定] の順に選択すると、**図 3-14** のような画面が表示されます。この画面では、IEEE802.1X 認証で使用する RADIUS サーバの設定を行います。

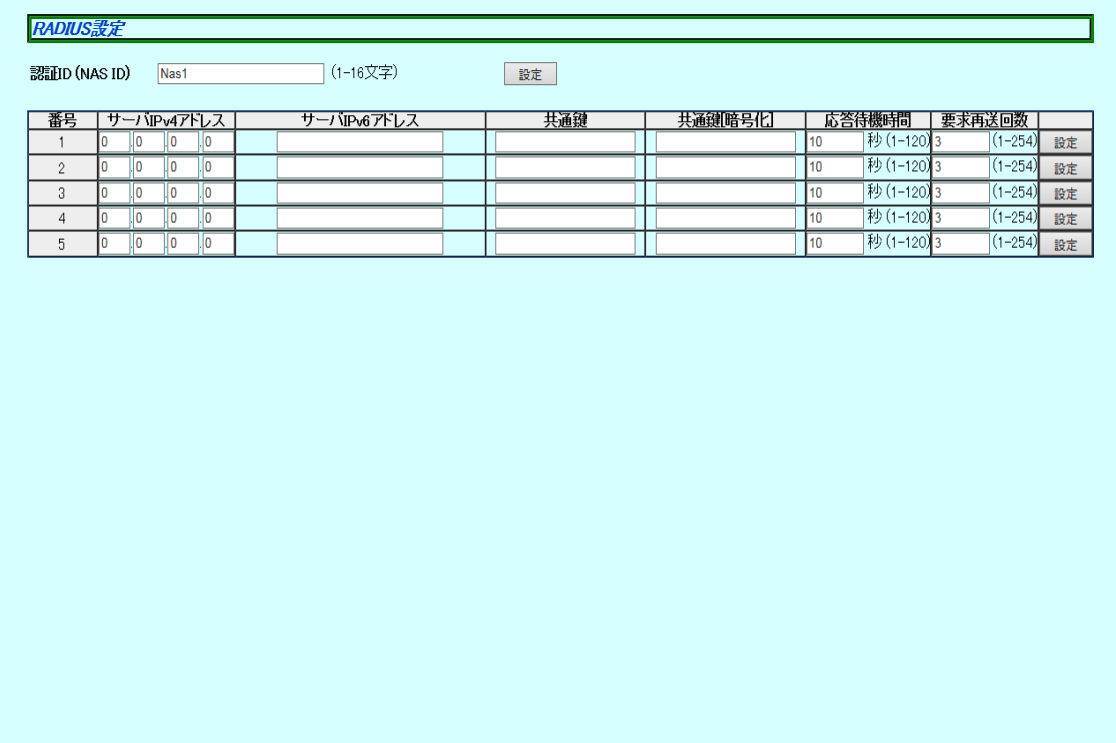


図 3-14 RADIUS の設定

画面の説明

認証 ID (NAS ID)	認証 ID（NAS Identifier）が表示されます。
番号	RADIUS 設定のエントリ番号です。
サーバ IP アドレス	RADIUS サーバの IP アドレスが表示されます。工場出荷時には何も設定されていませんので、「0.0.0.0」と表示されます。
サーバ IPv6 アドレス	RADIUS サーバの IPv6 アドレスが表示されます。工場出荷時には何も設定されていませんので、「::」と表示されます。
共通鍵	認証の際に用いる共通鍵 (Shared Secret) が表示されます。サーバとクライアントには同じ鍵を設定する必要があります。通常システム管理者が設定します。工場出荷時は設定されていません。暗号化されている場合は [encrypted] と表示されます。
応答待機時間	RADIUS サーバへの認証要求に対する最大待機時間が表示されます。工場出荷時は 10 秒に設定されています。
要求再送回数	RADIUS サーバへの認証要求が再送される回数が表示されます。工場出荷時は 3 回に設定されています。

3.1.15. Telnet アクセス制限設定

[基本機能設定] から [アクセス条件設定]、[Telnet アクセス制限設定] の順に選択すると、**図 3-15** のような画面が表示されます。この画面では、Telnet 経由でこの装置へアクセスする機器の制限設定を行います。

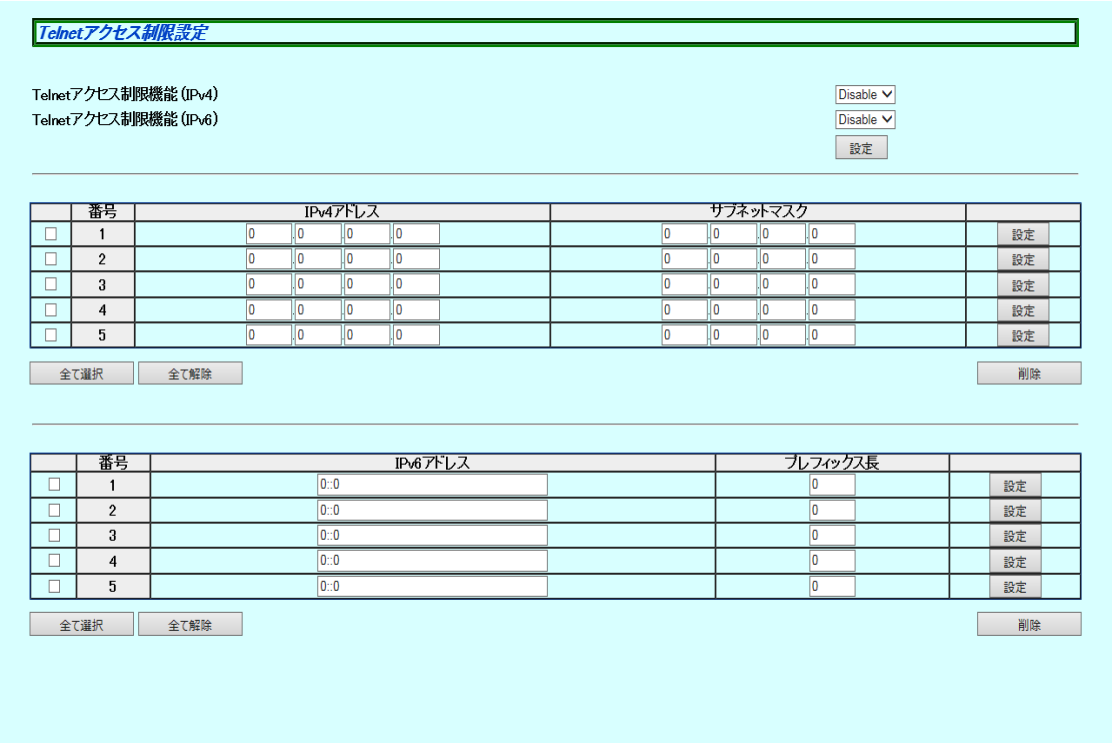


図 3-15 Telnet アクセス制限設定

画面の説明

Telnet アクセス制限機能 (IPv4)	IPv4 Telnet アクセス制限の設定が表示されます。 工場出荷時は「 Disable 」に設定されています。	
	Enable	Telnet アクセス制限を有効にします。
	Disable	Telnet アクセス制限を無効にします。
Telnet アクセス制限機能 (IPv6)	IPv6 Telnet アクセス制限の設定が表示されます。 工場出荷時は「 Disable 」に設定されています。	
	Enable	Telnet アクセス制限を有効にします。
	Disable	Telnet アクセス制限を無効にします。
番号	Telnet アクセス制限設定のエントリ番号です。	
IPv4 アドレス / サブネットマスク	追加するアクセス可能な IPv4 ネットワークの情報が表示されます。 工場出荷時に何も設定されていません。全ての IPv4 アドレスおよびサブネットマスクに「0」が表示されます。	
IPv6 アドレス / プレフィックス長	追加するアクセス可能な IPv6 ネットワークの情報が表示されます。 工場出荷時に何も設定されていません。全ての IPv6 アドレスおよびプレフィックス長に「::」が表示されます。	

3.1.16. ユーザ名／パスワード設定

[基本機能設定] から [アクセス条件設定]、[ユーザ名／パスワード設定] の順に選択すると、**図 3-16** のような画面が表示されます。この画面では、ユーザ名／パスワードの設定を行います。

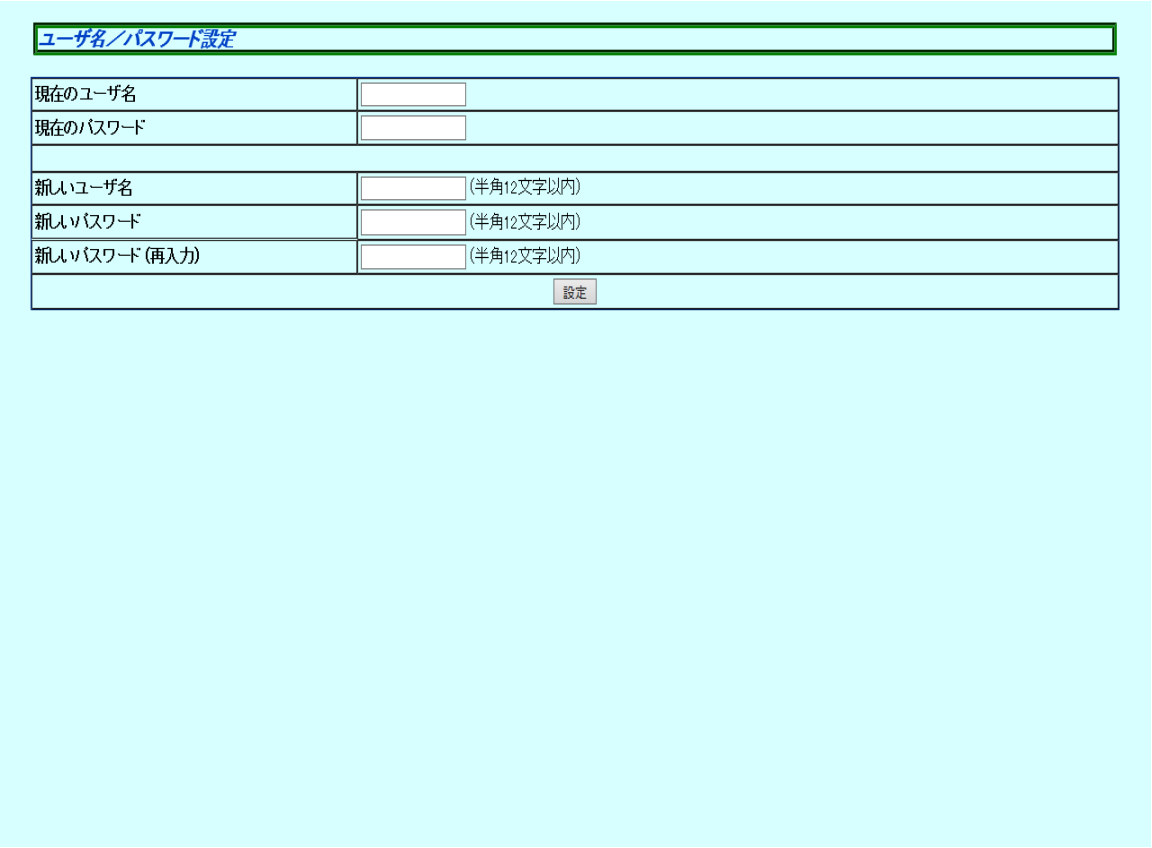


図 3-16 ユーザ名／パスワード設定

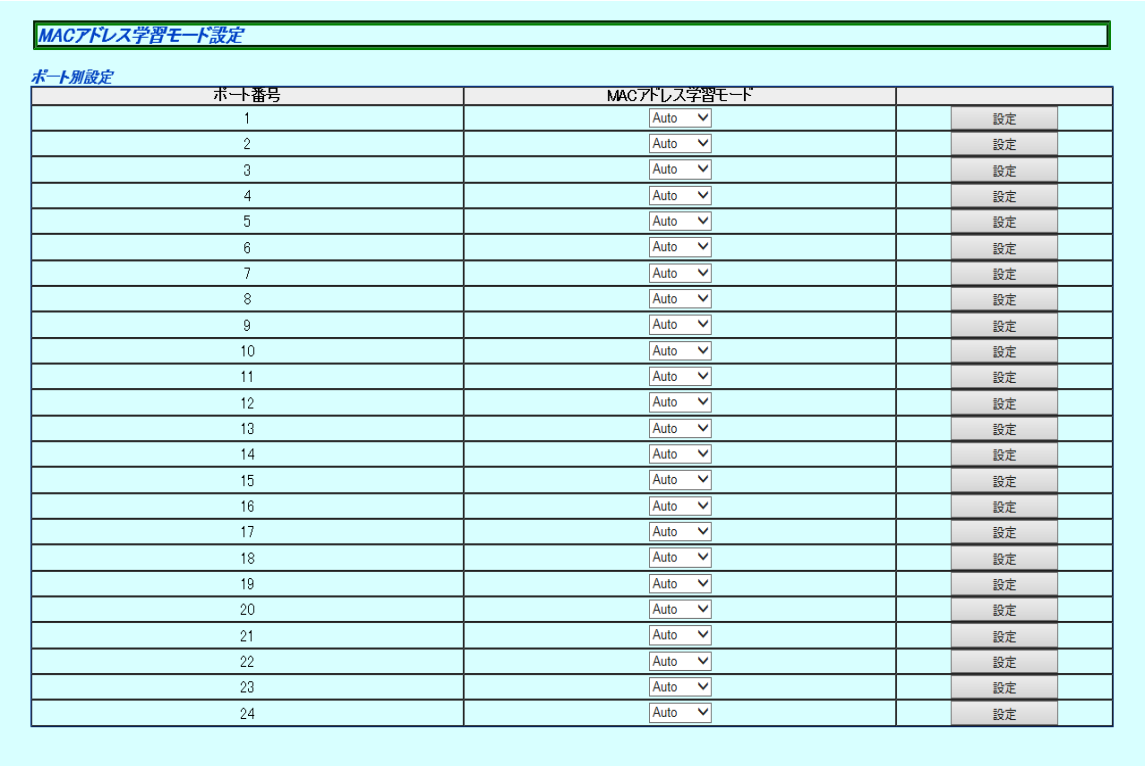
画面の説明

現在のユーザ名	現在のユーザ名を入力します。 この設定を使用して、この装置にログインします。 工場出荷時は「 manager 」に設定されています。
現在のパスワード	現在のパスワードを入力します。 この設定を使用して、この装置にログインします。 工場出荷時は「 manager 」に設定されています。
新しいユーザ名	新しいユーザ名を入力します。
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 (再入力)	パスワードの誤入力を防ぐため、もう一度パスワードを入力します。

ご注意： ユーザ名とパスワードは忘れないでください。
この設定は、コンソール、SSH、Telnet、Webにログインするときに必要になります。

3.1.17. MAC アドレス学習モード

[基本機能設定] から [FDB]、[MAC アドレス学習モード設定] の順に選択すると、**図 3-17** のような画面が表示されます。この画面では、ポート毎の MAC アドレス学習モードの設定を行います。



MACアドレス学習モード設定

ポート別設定

ポート番号	MACアドレス学習モード	
1	Auto	設定
2	Auto	設定
3	Auto	設定
4	Auto	設定
5	Auto	設定
6	Auto	設定
7	Auto	設定
8	Auto	設定
9	Auto	設定
10	Auto	設定
11	Auto	設定
12	Auto	設定
13	Auto	設定
14	Auto	設定
15	Auto	設定
16	Auto	設定
17	Auto	設定
18	Auto	設定
19	Auto	設定
20	Auto	設定
21	Auto	設定
22	Auto	設定
23	Auto	設定
24	Auto	設定

図 3-17 Telnet アクセス制限設定

画面の説明

ポート番号	ポート番号が表示されます。	
MAC アドレス学習モード	ポートの MAC アドレス学習モード状態が表示されます。 工場出荷時は「Auto」に設定されています。	
	Auto	MAC アドレスが自動学習されパケット転送が行われます。
	Disable	MAC アドレスの自動学習が無効であり、静的に MAC アドレスを登録しなければパケット転送が行われません。

ご注意： IEEE802.1X ポートベース認証を使用する場合、MAC アドレスを自動学習させない (Disable) 設定との同時使用はできません。

3.1.18. FDB 手動登録

[基本機能設定] から [FDB]、[FDB 手動設定] の順に選択すると、図 3-18 のような画面が表示されます。この画面では、MAC アドレスを FDB テーブルに手動登録できます。

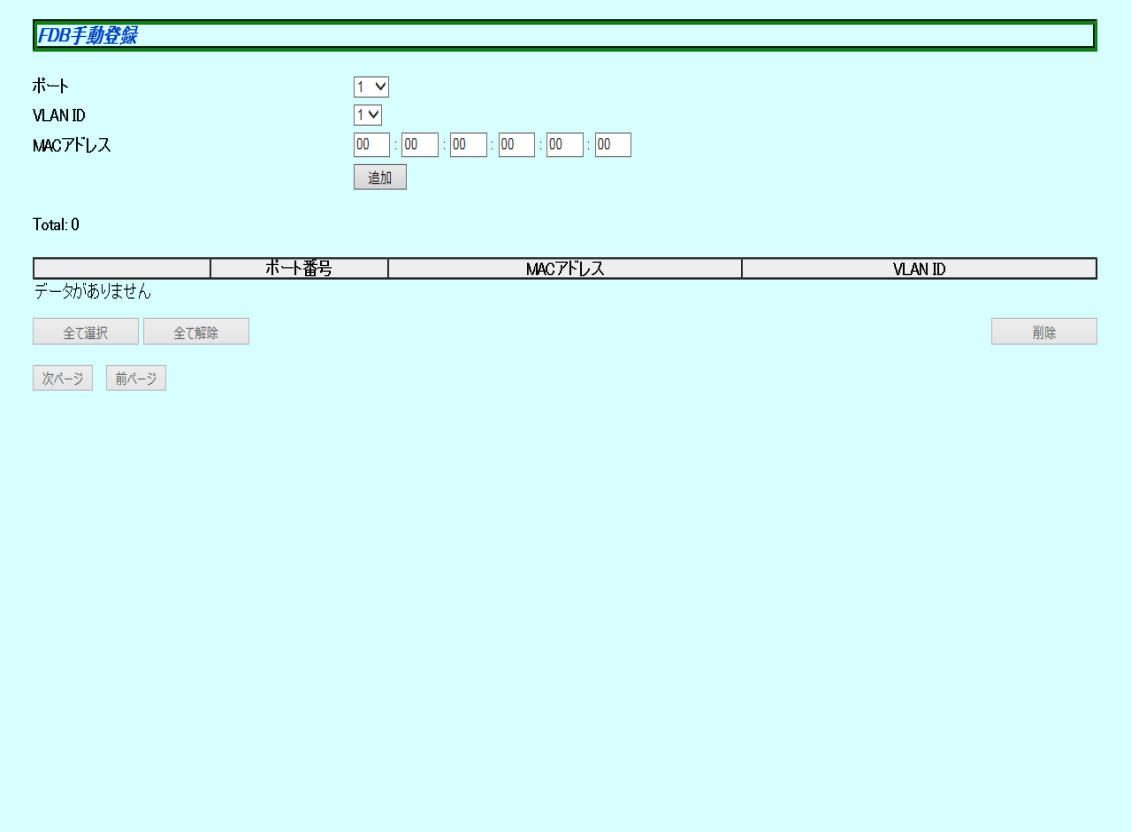


図 3-18 FDB 手動設定

画面の説明

< 追加 >	[追加]ボタンをクリックすると、以下の項目で設定した内容がFDBテーブルへ登録されます。	
	ポート	MAC アドレスの追加先ポートを選択します。
	VLAN ID	追加する MAC アドレスの VLAN ID を選択します。
	MAC アドレス	追加する MAC アドレスを入力します。
< 削除 >	手動登録済 FDB エントリの一覧が表示されます。 [次ページ] ボタンおよび [前ページ] ボタンをクリックすると、表示範囲が切り替わります。 削除対象エントリを選択し、[削除] ボタンをクリックすると、FDB テーブルから削除されます。 [全て選択] ボタンをクリックすると、全エントリが選択されます。 [全て解除] ボタンをクリックすると、全エントリが選択解除されます。	

3.1.19. FDB テーブル

[基本機能設定] から [FDB]、[FDB テーブル] の順に選択すると、図 3-19 のような画面が表示されます。この画面には、FDBテーブルに登録されているMACアドレスが表示されます。

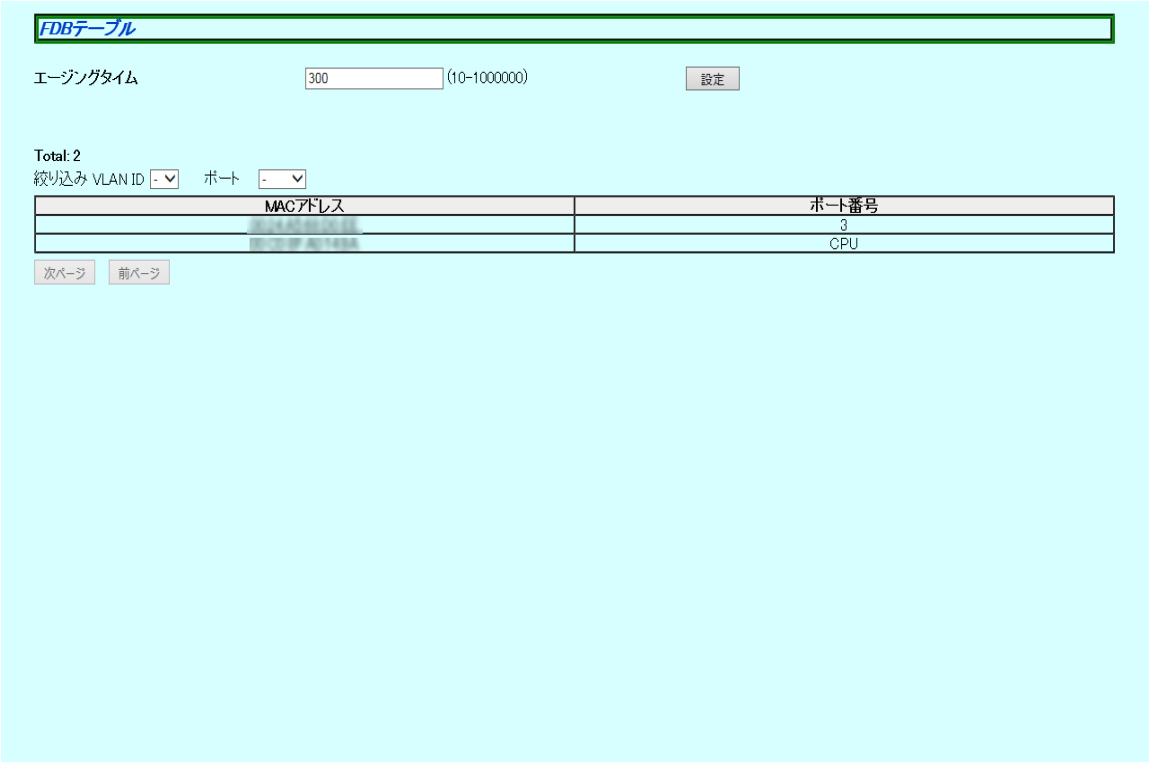


図 3-19 FDB テーブル（ポート別）

画面の説明

エージング タイム	自動学習した FDB エントリを保存する時間が表示されます。 最後にパケットを受信してからの時間となります。 工場出荷時は 300 秒（5 分）に設定されています。
絞り込み VLAN ID	VLAN ID を指定して、表示対象を絞り込みます。
絞り込み ポート	ポート番号を指定して、表示対象を絞り込みます。
MAC アドレス	FDB テーブル内の MAC アドレスが表示されます。
ポート番号	MAC アドレスの属しているポートが表示されます。
次ページ	一覧の表示範囲が切り替わります。
前ページ	

3.1.20. 時刻設定

[基本機能設定] から [時刻設定] を選択すると、**図 3-20** のような画面が表示されます。この画面では、時刻の設定、および SNTP による時刻同期の設定を行います。

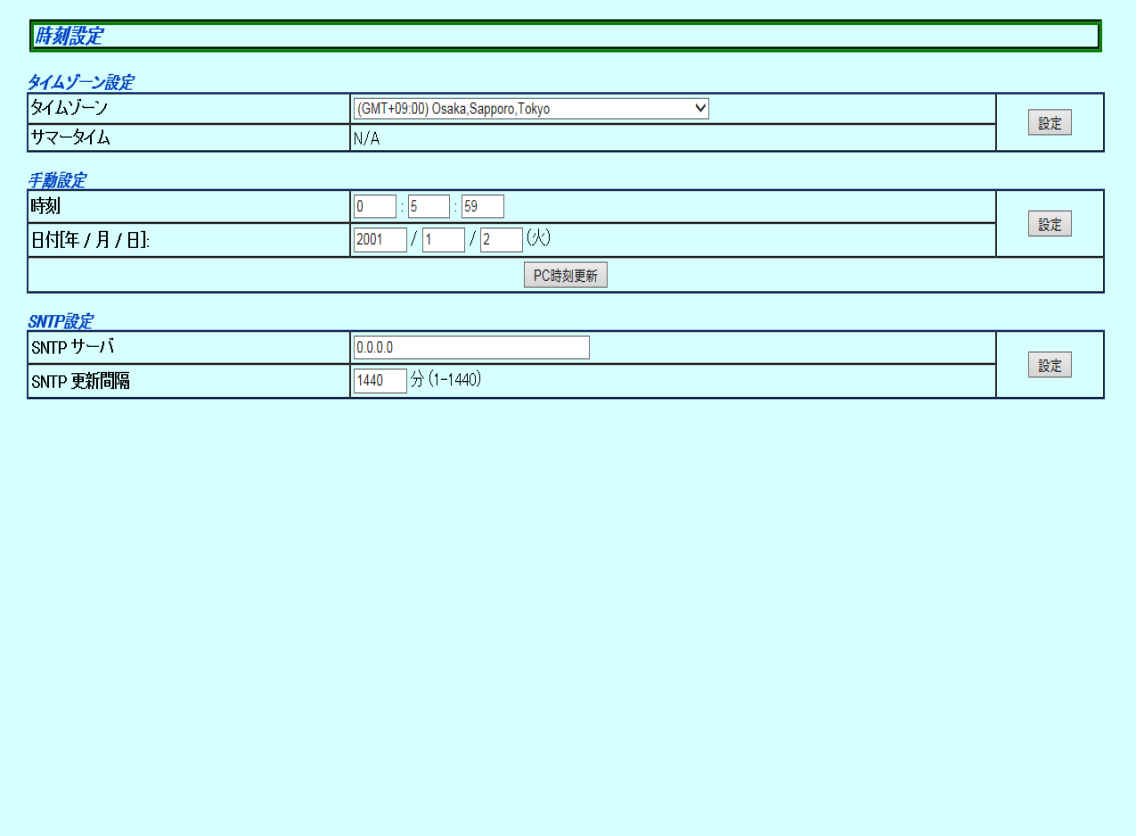


図 3-20 この装置の時刻設定

画面の説明

タイムゾーン	タイムゾーンが表示されます。
サマータイム	Daylight Saving(夏時間) の適用状況が表示されます。 夏時間が適用されないタイムゾーンに設定されている場合、「N/A」と表示され、夏時間を適用することができません。 通常、国内で使用する場合の設定は不要です。
SNTP サーバ	時刻同期を行う SNTP サーバの IP アドレスまたは IPv6 アドレスが表示されます。
SNTP 更新間隔	SNTP サーバとの時刻同期間隔が表示されます。

ご注意： SNTP サーバがファイアウォールの外部にある場合、ネットワーク管理者の設定によっては SNTP サーバと接続できない場合があります。詳しくはネットワーク管理者にお問い合わせください。
また、時刻同期機能を無効にしたい場合は、SNTP Server IP を「0.0.0.0」または「::」に設定してください。

3.1.21. ARP エントリ手動登録

[基本機能設定] から [ARP テーブル]、[ARP エントリ手動登録] の順に選択すると、**図 3-21** のような画面が表示されます。この画面では、IP アドレスと MAC アドレスの関連付けを ARP テーブルに手動登録できます。

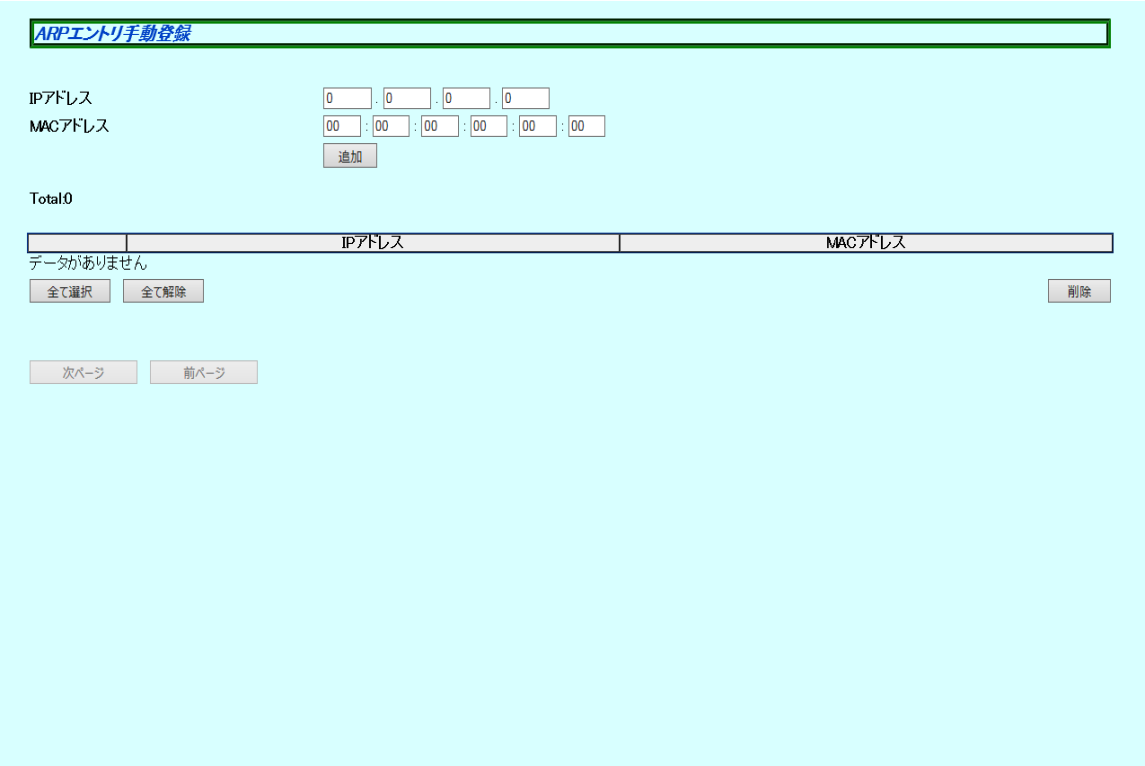


図 3-21 ARP エントリ手動登録

画面の説明

< 追加 >	[追加] ボタンをクリックすると、以下の項目で設定した内容が ARP テーブルへ登録されます。	
	IP アドレス	追加する IP アドレスを入力します。
	MAC アドレス	追加する MAC アドレスを入力します。
< 削除 >	手動登録済 ARP エントリの一覧が表示されます。 [次ページ] ボタンおよび [前ページ] ボタンをクリックすると、表示範囲が切り替わります。 削除対象エントリを選択し、[削除] ボタンをクリックすると、ARP テーブルから削除されます。 [全て選択] ボタンをクリックすると、全エントリが選択されます。 [全て解除] ボタンをクリックすると、全エントリが選択解除されます。	

3.1.22. ARP テーブル

[基本機能設定] から [ARP テーブル]、[ARP テーブル] の順に選択すると、図 3-22 のような画面が表示されます。この画面には、ARP テーブルが表示されます。

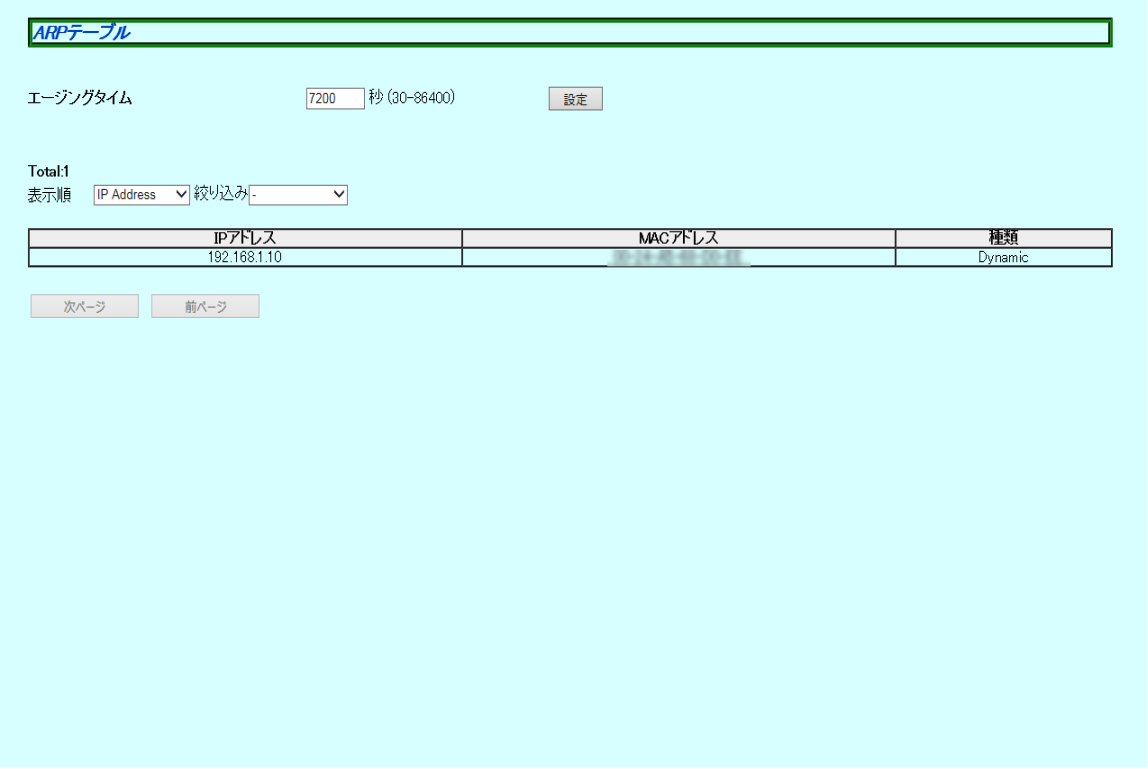


図 3-22 ARP テーブル

画面の説明

エージングタイム	自動学習した ARP エントリが保存されている時間が表示されます。最後にパケットを受信してからの時間となります。工場出荷時は 7200 秒（2 時間）に設定されています。	
表示順	指定した順番で一覧表示を並べ替えます。	
	IP Address	IP アドレスで一覧表示を並べ替えます。
	MAC Address	MAC アドレスで一覧表示を並べ替えます。
	種類	種類で一覧表示を並べ替えます。
IP アドレス	ARP テーブル上にある IP アドレスが表示されます。	
MAC アドレス	ARP テーブル上にある MAC アドレスが表示されます。	
種類	登録された ARP エントリの種類が表示されます。	
	Static	手動登録したことを表します。
	Dynamic	自動学習したことを表します。
次ページ	一覧の表示範囲が切り替わります。	
前ページ		

3.1.23. NDP テーブル

[基本機能設定] から [NDP テーブル] の順に選択すると、図 3-23 のような画面が表示されます。この画面では、NDP テーブルの参照、及び設定を行います。

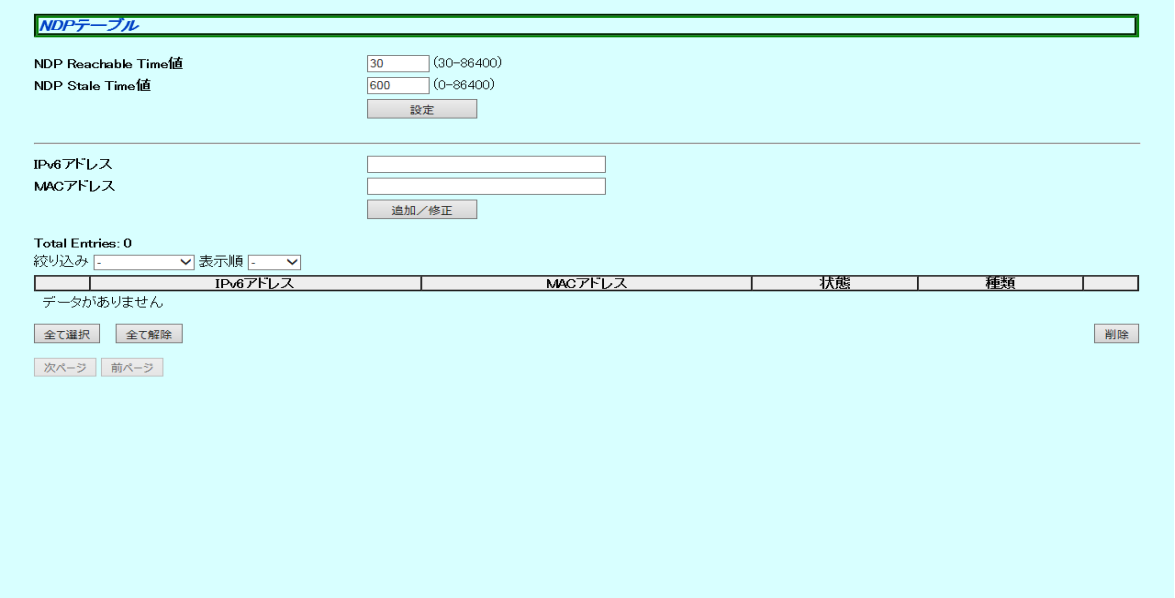


図 3-23 NDP テーブル

画面の説明

NDP Reachable Time 値	Reachable time のタイムアウト値を表示します。	
NDP Stale Time 値	Stale time のタイムアウト値を表示します。	
Total Entry	作成されている NDP テーブルのエントリ数を表示します。	
IPv6 アドレス	NDP テーブル上にある IPv6 アドレスを表示します。	
MAC アドレス	NDP テーブル上にある MAC アドレスを表示します。	
状態	近隣キャッシュの状態を表示します。	
種類	NDP テーブル上にある Type を表示します。	
	Static	手動設定したことを表します。
	Dynamic	自動学習したことを表します。

3.2.　拡張機能設定

3.2.1.　VLAN 情報／修正

[拡張機能設定] から [VLAN 設定]、[VLAN 情報／修正] の順に選択すると、図 3-24 のような画面が表示されます。この画面では、VLAN に関する設定を行います。

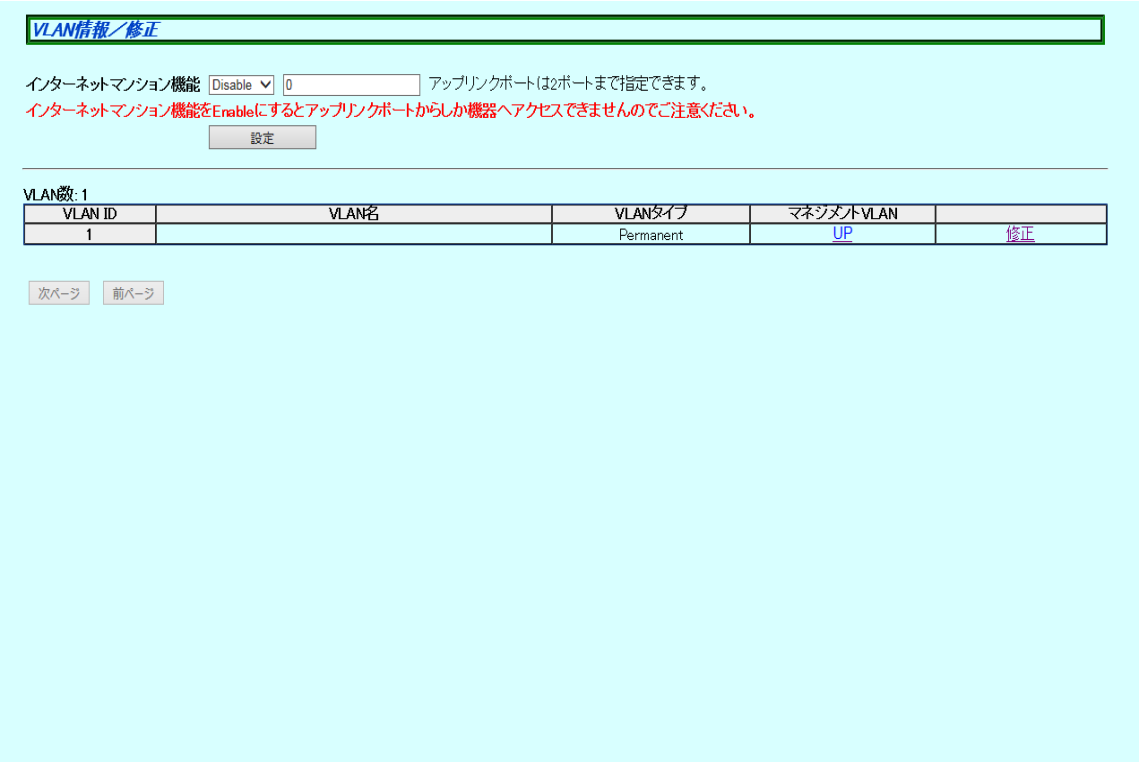


図 3-24 VLAN 情報／修正

画面の説明

インターネットマンション機能	インターネットマンション機能の設定が表示されます。	
	Enable	指定されたポートをアップリンクとして動作していることを表します。
	Disable	無効であることを表します。
VLAN 数	この装置の現在の VLAN 数が表示されます。 各エントリの [削除] ボタンをクリックすると、該当の VLAN 設定が削除されます。	
VLAN ID	VLAN の VLAN ID が表示されます。	
VLAN 名	VLAN 名が表示されます。	
VLAN タイプ	VLAN の種類が表示されます。	
	Permanent	初期設定の VLAN です。 この VLAN は削除できません。
	Static	新たに設定された VLAN です。
マネジメント VLAN	VLAN がマネジメント VLAN かどうかが表示されます。	
	UP	この VLAN がマネジメント VLAN（CPU と通信できる VLAN）であることを表します。
	DOWN	この VLAN がマネジメント VLAN ではないことを表します。
次ページ	一覧の表示範囲が切り替わります。	
前ページ		

3.2.1.a.　VLAN 修正

[VLAN 情報／修正] 画面で [修正] を選択すると、図 3-25 のような画面が表示されます。この画面では、VLAN 設定情報の修正を行います。

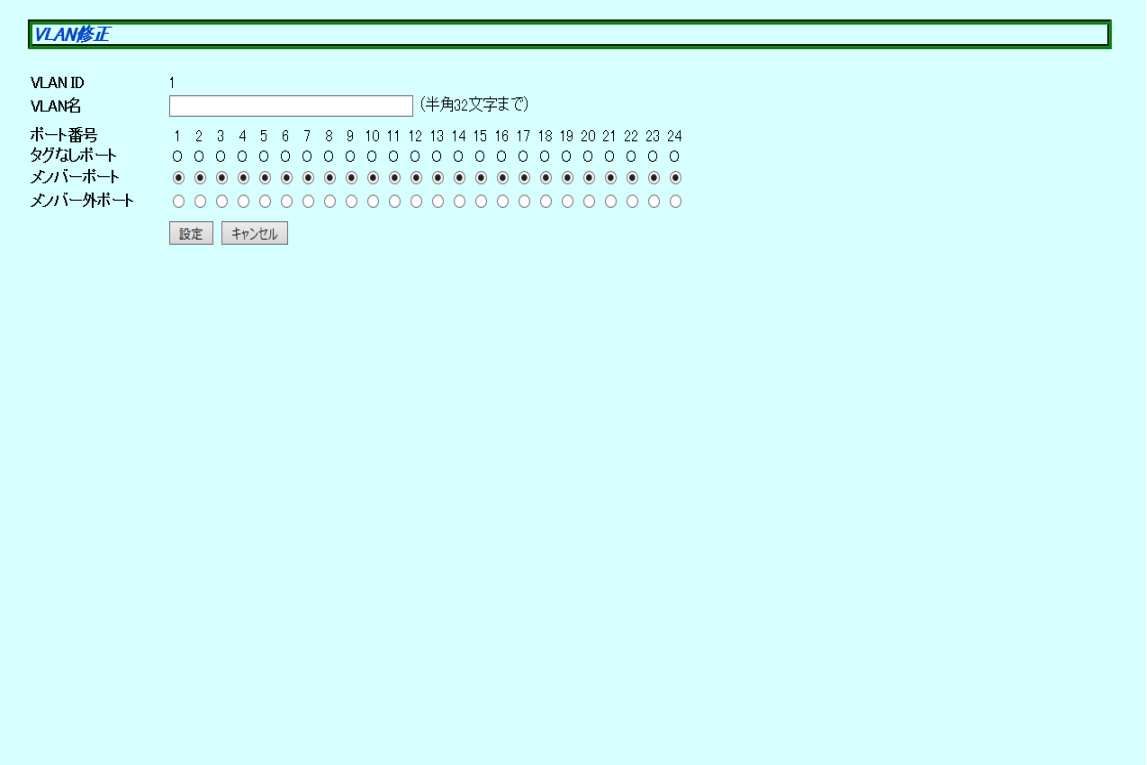


図 3-25 VLAN 修正

画面の説明

VLAN ID	VLAN ID が表示されます。
VLAN 名	VLAN 名が表示されます。
タグなしポート	該当ポートから送信されるフレームにタグを使用しないことを表します。
メンバーポート メンバー外ポート	各ポートを該当 VLAN に割り当てるかどうかを選択します。 [キャンセル] ボタンをクリックすると、現在の割り当て状態に戻ります。

3.2.2.　VLAN 作成

[拡張機能設定] から [VLAN 設定]、[VLAN 作成] の順に選択すると、図 3-26 のような画面が表示されます。この画面では、VLAN の新規作成を行います。

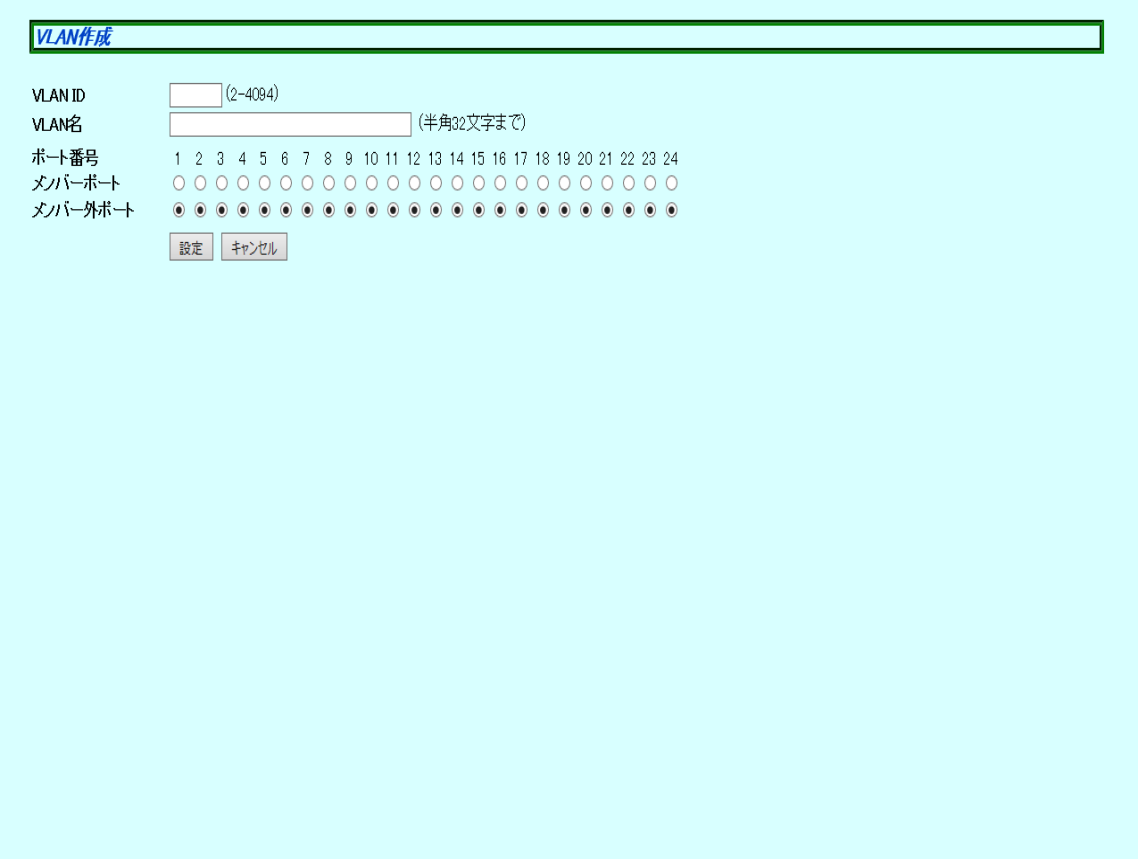


図 3-26 VLAN 作成

画面の説明

VLAN ID	VLAN ID を設定します。
VLAN 名	VLAN 名を設定します。
メンバーポート メンバー外ポート	各ポートを該当 VLAN に割り当てるかどうかを選択します。 [キャンセル] ボタンをクリックすると、現在の割り当て状態に戻ります。

3.2.3.　VLAN ポート設定

[拡張機能設定] から [VLAN 設定]、[VLAN ポート設定] の順に選択すると、図 3-27 のような画面が表示されます。この画面では、指定の VLAN ポートの設定を行います。

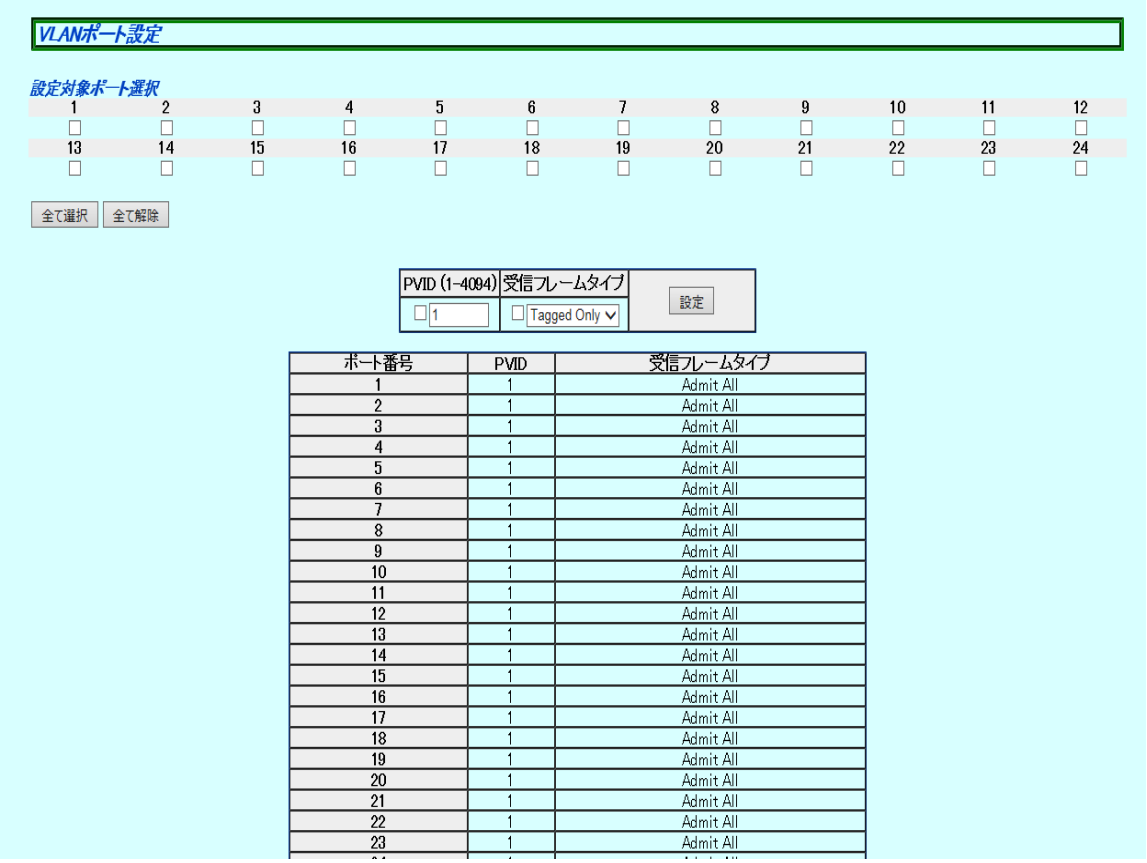


図 3-27 VLAN ポート設定

画面の説明

一括設定用 対象ポート	複数のポートに対して一括設定を行う際の対象ポートを選択します。 [全て選択] ボタンをクリックすると、全ポートが選択されます。 [全て解除] ボタンをクリックすると、全ポートが選択解除されます。 一括設定用項目を選択・変更後、[一括設定] ボタンをクリックすると、選択中のポートに対して同一の設定が反映されます。	
ポート番号	ポート番号が表示されます。	
PVID	ポートの現在の PVID（ポート VLAN ID）が表示されます。PVID はタグなしのフレームを受信した場合にどの VLAN ID に送信するかを表します。工場出荷時は 1 に設定されています。タグ付きのフレームを受信した場合、この値に関係なく、タグを参照して宛先ポートが特定されます。	
受信フレーム タイプ	受信フレームのタイプが表示されます。工場出荷時は全て「Admit All」に設定されています。	
	Admit All	全てのフレームが受信されます。
	Tagged Only	タグ付きのフレームのみが受信されます。

3.2.4. トラフィッククラス設定

[拡張機能設定] から [QoS 設定]、[トラフィッククラス設定] の順に選択すると、**図 3-28** のような画面が表示されます。この画面では、QoS およびトラフィッククラスの設定を行います。

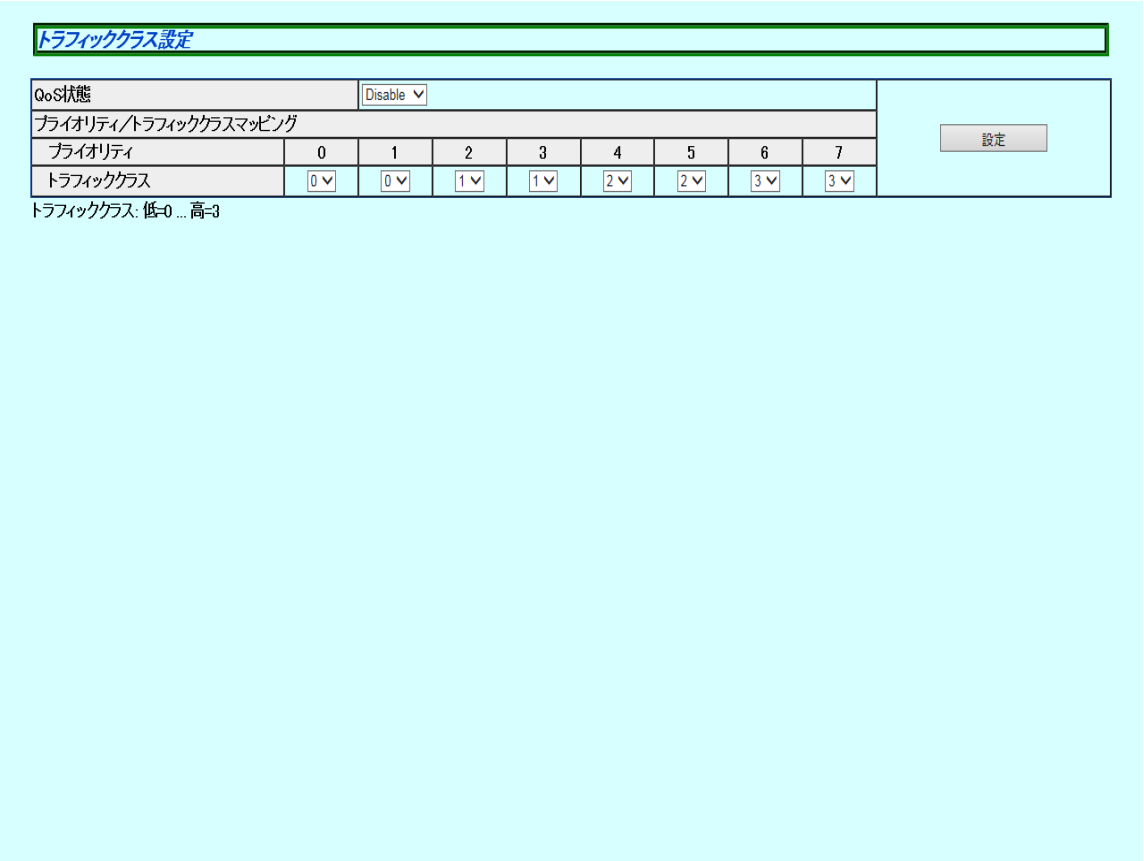


図 3-28 QoS 設定

画面の説明

QoS 状態	IEEE802.1p を使った QoS 機能の設定状態が表示されます。 工場出荷時は「 Disable 」に設定されています。	
	Enable	QoS が有効です。
	Disable	QoS が無効です。
プライオリティ	VLAN タグ内の Priority 値が表示されます。	
トラフィッククラス	フレーム転送の優先度が表示されます。	

3.2.5.　帯域幅制御設定

[拡張機能設定] から [QoS 設定]、[帯域幅制御設定] の順に選択すると、図 3-29 のような画面が表示されます。この画面では、帯域幅制御の設定を行います。

図 3-29 帯域幅制御設定

画面の説明

一括設定用 対象ポート	複数のポートに対して一括設定を行う際の対象ポートを選択します。 [全て選択] ボタンをクリックすると、全ポートが選択されます。 [全て解除] ボタンをクリックすると、全ポートが選択解除されます。 一括設定用項目を選択・変更後、[一括設定] ボタンをクリックすると、選択中のポートに対して同一の設定が反映されます。	
ポート番号	ポート番号が表示されます。	
帯域幅	帯域幅が表示されます。工場出荷時は 1000 に設定されています。(単位は Mbps)	
状態	帯域幅の制御設定の有効・無効が表示されます。	
	Enable	帯域幅の制御設定は有効です。
	Disable	帯域幅の制御設定は無効です。

3.2.6.　リンクアグリゲーション設定

[拡張機能設定] から [リンクアグリゲーション設定] を選択すると、**図 3-30** のような画面が表示されます。この画面では、リンクアグリゲーションのグループ設定を行います。

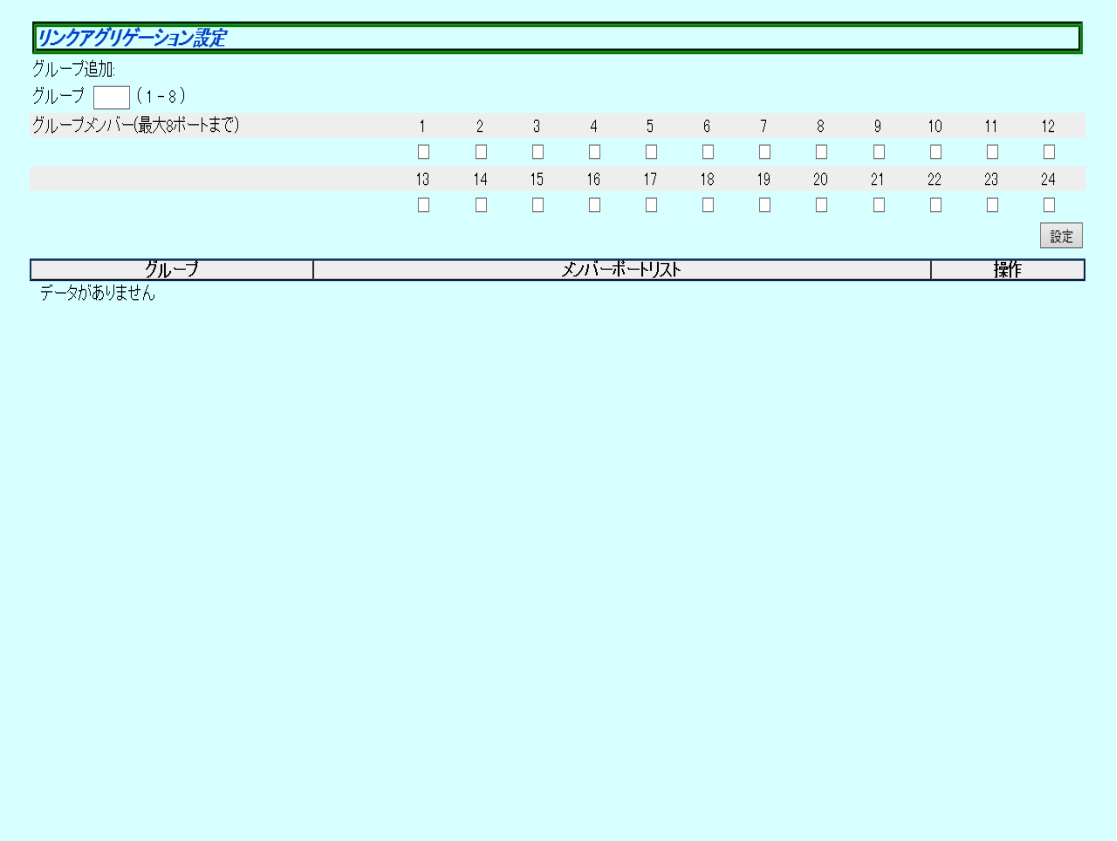


図 3-30 リンクアグリゲーション設定

画面の説明

グループメンバー	リンクアグリゲーションのグループメンバーとなるポートを選択します。
メンバーポートリスト	リンクアグリゲーションのグループに含まれるポートが表示されます。

3.2.6.a.　リンクアグリゲーション修正

[拡張機能設定] から [リンクアグリゲーション設定] を選択し、任意のグループの [修正] ボタンをクリックすると、図 3-31 のような画面が表示されます。この画面では登録済グループの修正を行います。

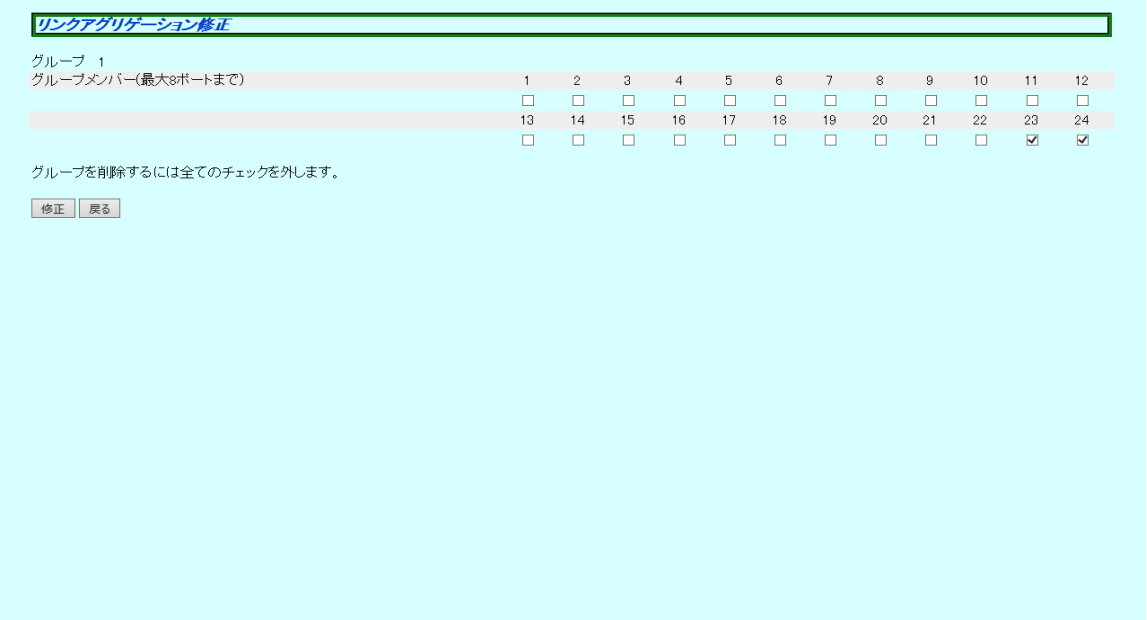


図 3-31 リンクアグリゲーション修正

画面の説明

グループメンバー	リンクアグリゲーションのグループメンバーとなるポートを選択します。

3.2.7.　ストームコントロール設定

[拡張機能設定] から [ストームコントロール設定] を選択すると、図 3-32 のような画面が表示されます。この画面では、ストームコントロールの設定を行います。

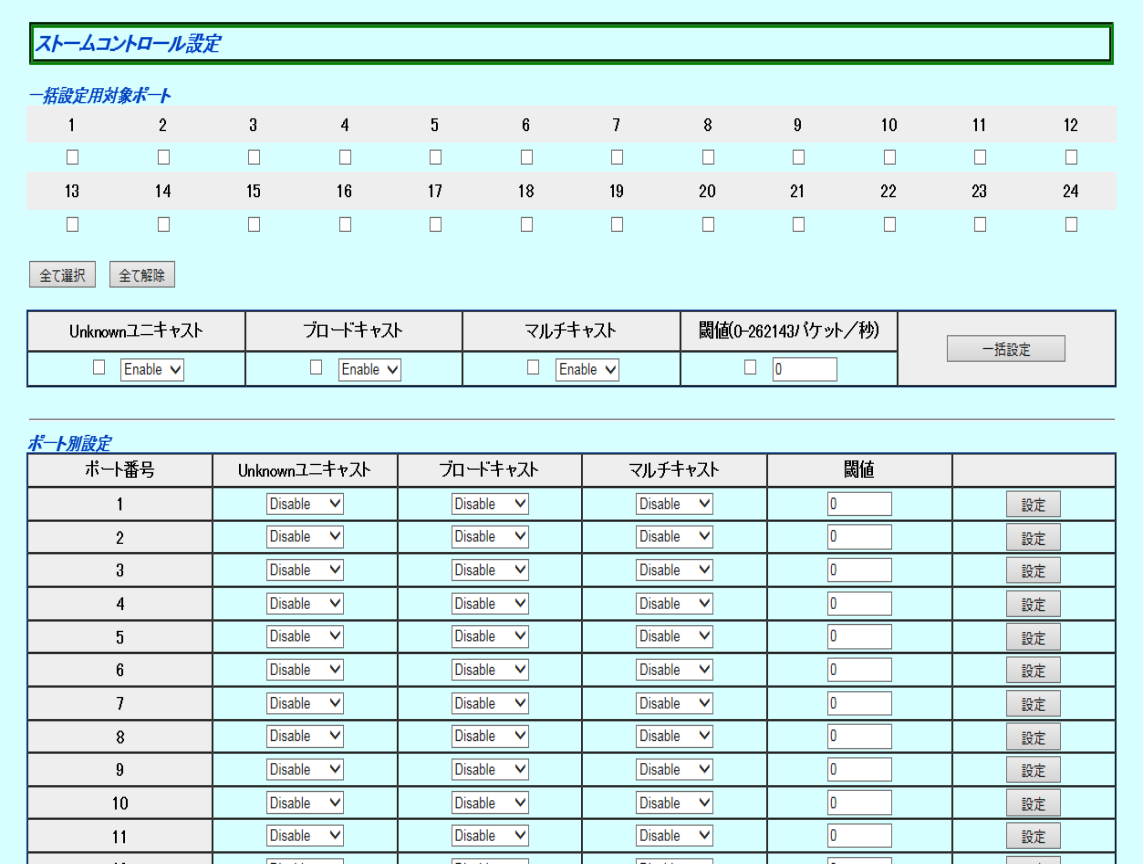


図 3-32 ストームコントロール設定

画面の説明

一括設定用 対象ポート	複数のポートに対して一括設定を行う際の対象ポートを選択します。 [全て選択] ボタンをクリックすると、全ポートが選択されます。 [全て解除] ボタンをクリックすると、全ポートが選択解除されます。 一括設定用項目を選択・変更後、[一括設定] ボタンをクリックすると、選択中のポートに対して同一の設定が反映されます。	
ポート番号	ポート番号が表示されます。	
Unknown ユニキャスト	Unknown ユニキャストのストームコントロールを有効・無効にします。	
	Enable	Unknown ユニキャストのストームコントロールが有効です。
	Disable	Unknown ユニキャストのストームコントロールが無効です。 (工場出荷時設定)
ブロードキャスト	ブロードキャストのストームコントロールを有効・無効にします。	
	Enable	Broadcast のストームコントロールが有効です。
	Disable	Broadcast のストームコントロールが無効です。 (工場出荷時設定)
マルチキャスト	マルチキャストのストームコントロールを有効・無効にします。	
	Enable	Multicast のストームコントロールが有効です。
	Disable	Multicast のストームコントロールが無効です。 (工場出荷時設定)
閾値	パケット数の閾値が表示されます。	

3.2.8. 認証状態テーブル

[認証設定] から [認証状態テーブル] を選択すると、図 3-33 のような画面が表示されます。この画面では、802.1X 認証、MAC 認証および WEB 認証の認証状態を一元管理できる認証状態テーブルの参照を行えます。

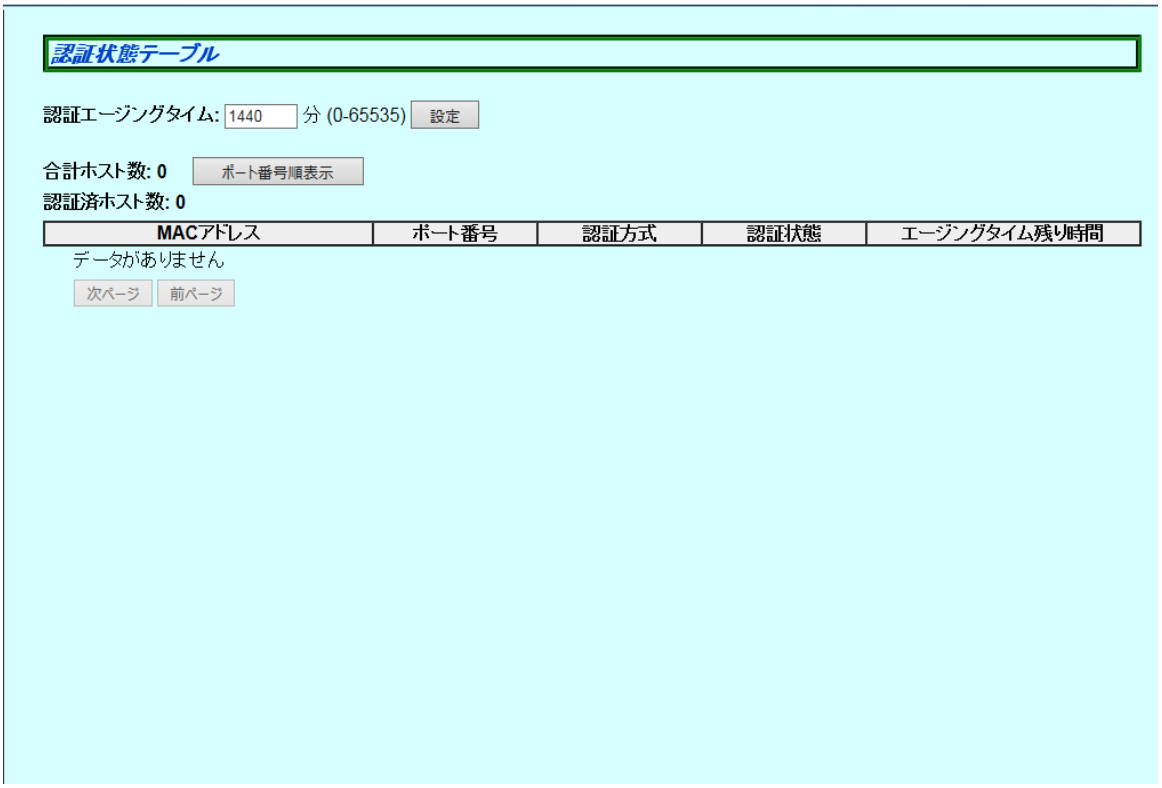


図 3-33 認証状態テーブル

画面の説明

認証エージング タイム	認証エージングタイムを分単位で表示します。（工場出荷時設定：1440）	
合計ホスト数	認証状態テーブルに登録された合計ホスト数を表示します。最大保持数は 384 です。	
認証済ホスト数	認証済みホスト数を表示します。	
MAC アドレス	認証対象となる端末の MAC アドレスを表示します。	
ポート番号	端末が接続されているポート番号を表示します。	
認証方式	認証方式を表示します。 認証状態が Authorized の場合は認証成功時の認証方式を、Unauthorized の場合は待受中の認証方式を表示します。	
	1X/MAC/WEB	802.1X 認証、MAC 認証または WEB 認証を表します。
	1X/MAC	802.1X 認証または MAC 認証を表します。
	1X/WEB	802.1X 認証または WEB 認証を表します。
	MAC/WEB	MAC 認証または WEB 認証を表します。
	802.1X	802.1X 認証を表します。
	MAC	MAC 認証を表します。
	WEB	WEB 認証を表します。
認証状態	認証状態を表示します。	
	Authorized	認証状態であることを表します。
	Unauthorized	未認証であることを表します。 この状態での通信はゲスト VLAN 内に限定されます。
エージングタイム 残り時間	再認証までの残り時間 (分) を表示します。 残り時間が 0 になった場合は認証状態が Unauthorized となり、再度認証処理が実行されます。	

3.2.9. 認証ログ

[認証設定] から [認証ログ] を選択すると、図 3-34 のような画面が表示されます。この画面では、802.1X 認証、MAC 認証および WEB 認証の認証結果のログの参照を行えます。
認証ログの最大保持可能数は 512 個です。

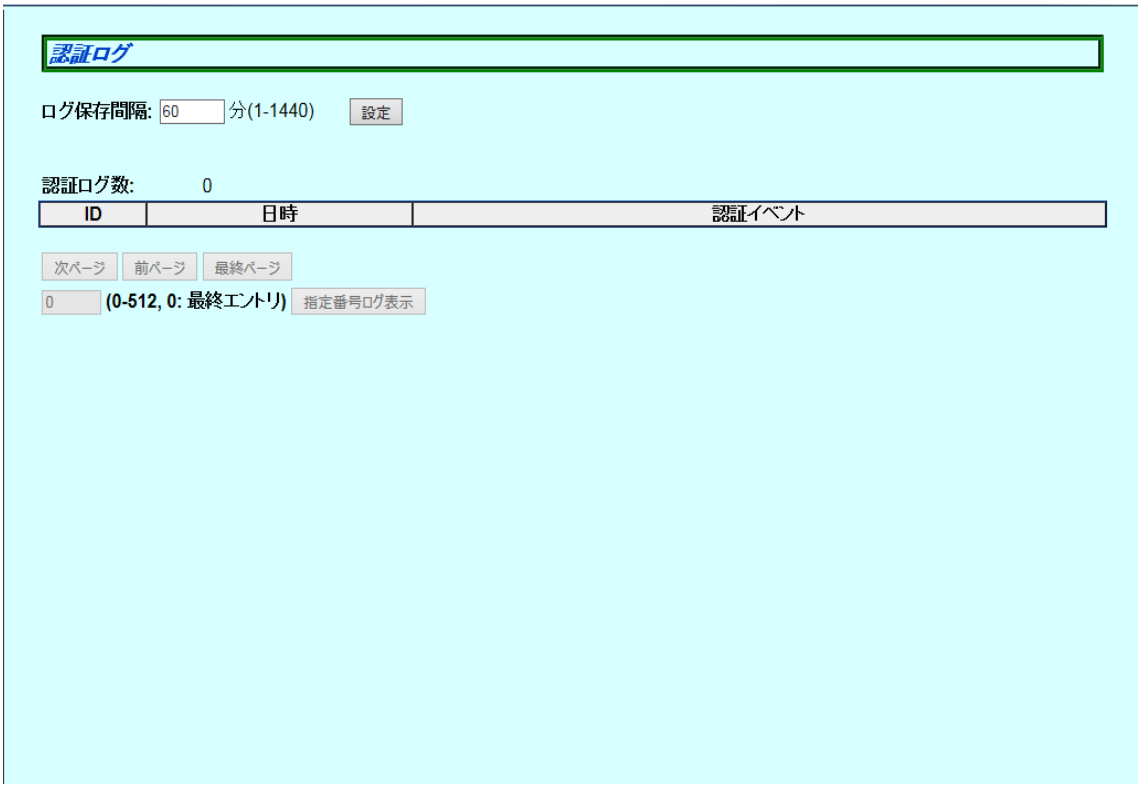


図 3-34 認証ログ

画面の説明

ログ保存間隔	発生した認証ログを実際に本体へ書き込むまでの待機時間を分単位で表示します。 書き込みが行われていない時に再起動や電源 OFF が発生した場合は、それまでの認証ログは消去されます。（工場出荷時設定：60）
認証ログ数	認証状態テーブルに記録された認証イベント数を表示します。 最大保持数は 512 個です。
ID	認証ログの ID を降順で表示します。
日付	認証イベントが発生した日時を表示します。
認証イベント	認証イベントを表示します。
指定番号ログ表示	指定した ID に移動します。0 を入力すると最終エントリを表示します。

認証イベントの内容は以下のとおりです。

認証イベント	Severity	概要
[MAC](RADIUS)Authorized XX:XX:XX:XX:XX:XX on Port xx to VLAN xxxx	info	特定ポートに接続された端末が、RADIUS またはローカルデータベースを用いたMAC認証に成功し特定の VLAN に割り振られた、または失敗したことを表します。
[MAC](Local)Authorized XX:XX:XX:XX:XX:XX on Port xx to VLAN xxxx	info	
[MAC](RADIUS)Rejected XX:XX:XX:XX:XX:XX on Port xx	notice	
[MAC](Local)Rejected XX:XX:XX:XX:XX:XX on Port xx	notice	
[WEB](RADIUS)Authorized user xxxxxxxxxxxxxxxx (XX:XX:XX:XX:XX:XX) on Port xx to VLAN xxxx	info	特定ポートに接続された端末が、RADIUS またはローカルデータベースを用いた WEB 認証に成功し特定の VLAN に割り振られた、または失敗したことを表します。
[WEB](Local)Authorized user xxxxxxxxxxxxxxxx (XX:XX:XX:XX:XX:XX) on Port xx to VLAN xxxx	info	
[WEB](RADIUS)Rejected user xxxxxxxxxxxxxxxx (XX:XX:XX:XX:XX:XX) on Port xx	notice	
[WEB](Local)Rejected user xxxxxxxxxxxxxxxx (XX:XX:XX:XX:XX:XX) on Port xx	notice	
[802.1X](RADIUS)Authorized user xxxxxxxxxxxxxxxx (XX:XX:XX:XX:XX:XX) on Port xx to VLAN xxxx	info	特定ポートに接続された端末が、RADIUS またはローカルデータベースを用いた IEEE802.1X 認証に成功し特定の VLAN に割り振られた、または失敗したことを表します。
[802.1X](RADIUS)Rejected user xxxxxxxxxxxxxxxx (XX:XX:XX:XX:XX:XX) on Port xx	notice	
[802.1X](Local)Authorized user xxxxxxxxxxxxxxxx (XX:XX:XX:XX:XX:XX) on Port xx to VLAN xxxx	info	
[802.1X](Local)Rejected user xxxxxxxxxxxxxxxx (XX:XX:XX:XX:XX:XX) on Port xx	notice	
[MAC]Rejected XX:XX:XX:XX:XX:XX on Port xx (auth table was full)	notice	認証状態テーブルに登録されたホスト数が上限に達しているため、新たな端末の認証が拒否されたことを表します。
[WEB]Rejected XX:XX:XX:XX:XX:XX on Port xx (auth table was full)	notice	
[802.1X]Rejected XX:XX:XX:XX:XX:XX on Port xx (auth table was full)	notice	

3.2.10. グローバル認証設定

[認証設定] から [グローバル認証設定] を選択すると、図 3-35 のような画面が表示されます。この画面では、802.1X 認証、MAC 認証および WEB 認証のグローバル設定および各認証を行う対象ポートの指定を行えます。

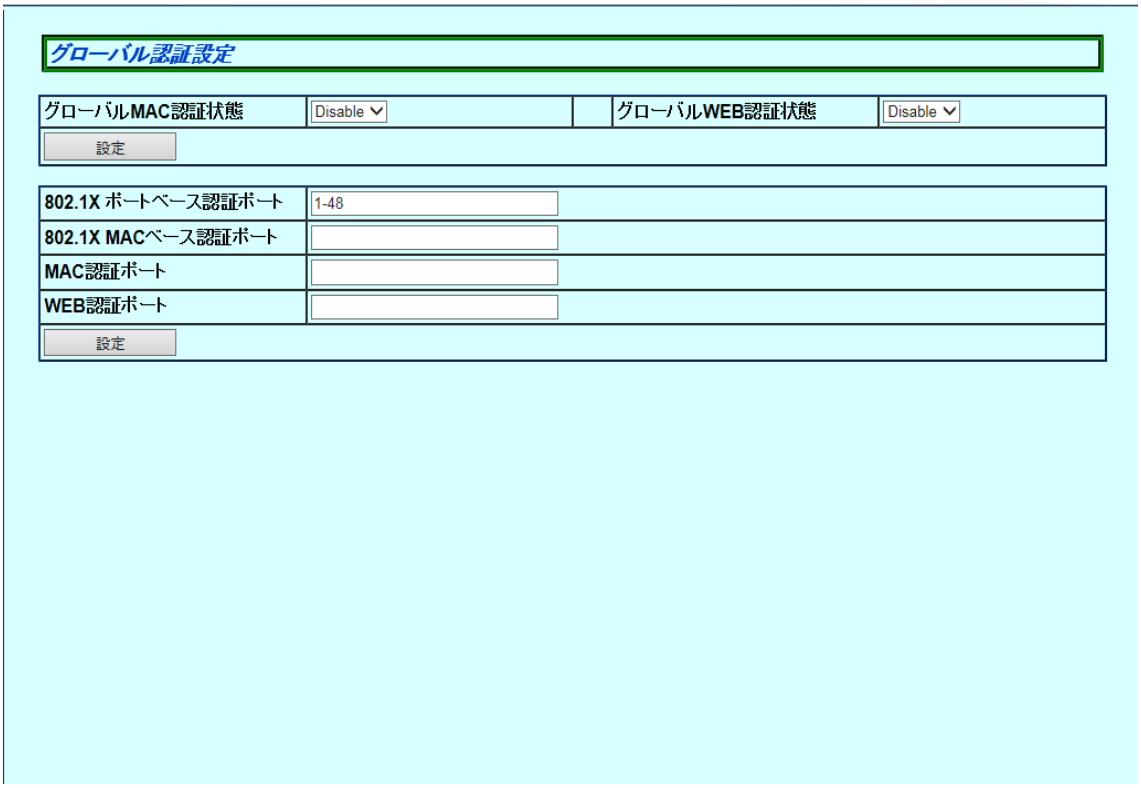


図 3-35 グローバル認証設定

画面の説明

グローバル MAC 認証状態	機器全体の MAC 認証動作状態を表示します。	
	Enable	MAC 認証が有効であることを表します。
	Disable	MAC 認証が無効であることを表します。(工場出荷時設定)
グローバル WEB 認証状態	機器全体の WEB 認証動作状態を表示します。	
	Enable	WEB 認証が有効であることを表します。
	Disable	WEB 認証が無効であることを表します。(工場出荷時設定)
802.1X ポートベース 認証ポート	IEEE802.1X ポートベース認証が有効なポートを表示します。	
802.1X MAC ベース 認証ポート	IEEE802.1X MAC ベース認証が有効なポートを表示します。	
MAC 認証ポート	MAC 認証が有効なポートを表示します。	
WEB 認証ポート	WEB 認証が有効なポートを表示します。	

3.2.11. ローカルユーザデータベース設定

[認証設定] から [ローカルユーザデータベース設定] を選択すると、**図 3-36** のような画面が表示されます。この画面では、IEEE802.1X および WEB 認証で使用するユーザアカウント設定を行えます。

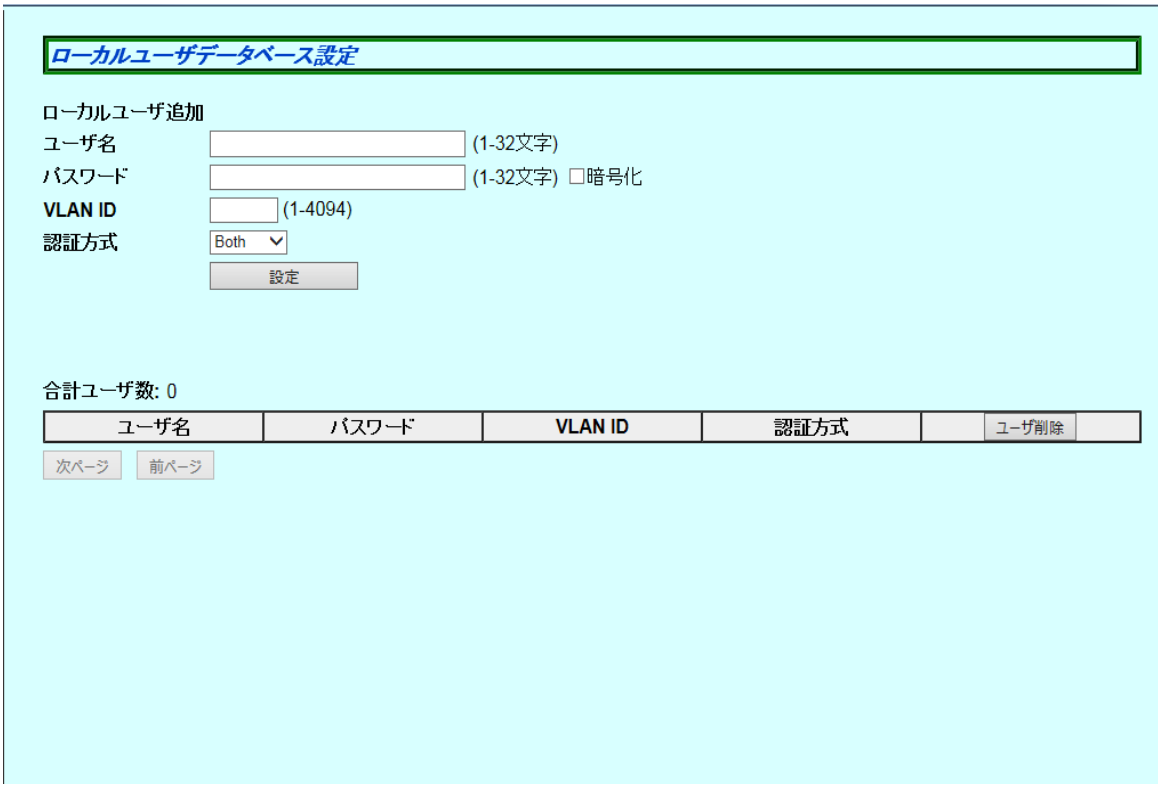


図 3-36 ローカルユーザデータベース設定

画面の説明

ユーザ名	ユーザ名を表示します。	
パスワード	ユーザのパスワードを表示します。 暗号化されている場合は *encrypted* と表示されます。	
暗号化	チェックを入れるとパスワードを暗号化して保存します。 チェックがない場合は、平文で保存します。	
VLAN ID	認証後に割り当てる VLAN ID を表示します。	
認証方式	アカウントを使用する認証方式を表示します	
	Both	802.1X および WEB 認証で使用することを表します。
	WEB	WEB 認証でのみ使用することを表します。
	802.1X	802.1X でのみ使用することを表します。

3.2.12. ローカル MAC データベース設定

[認証設定] から [ローカル MAC データベース設定] を選択すると、図 3-37 のような画面が表示されます。この画面では、MAC 認証で使用するユーザアカウント設定を行えます。

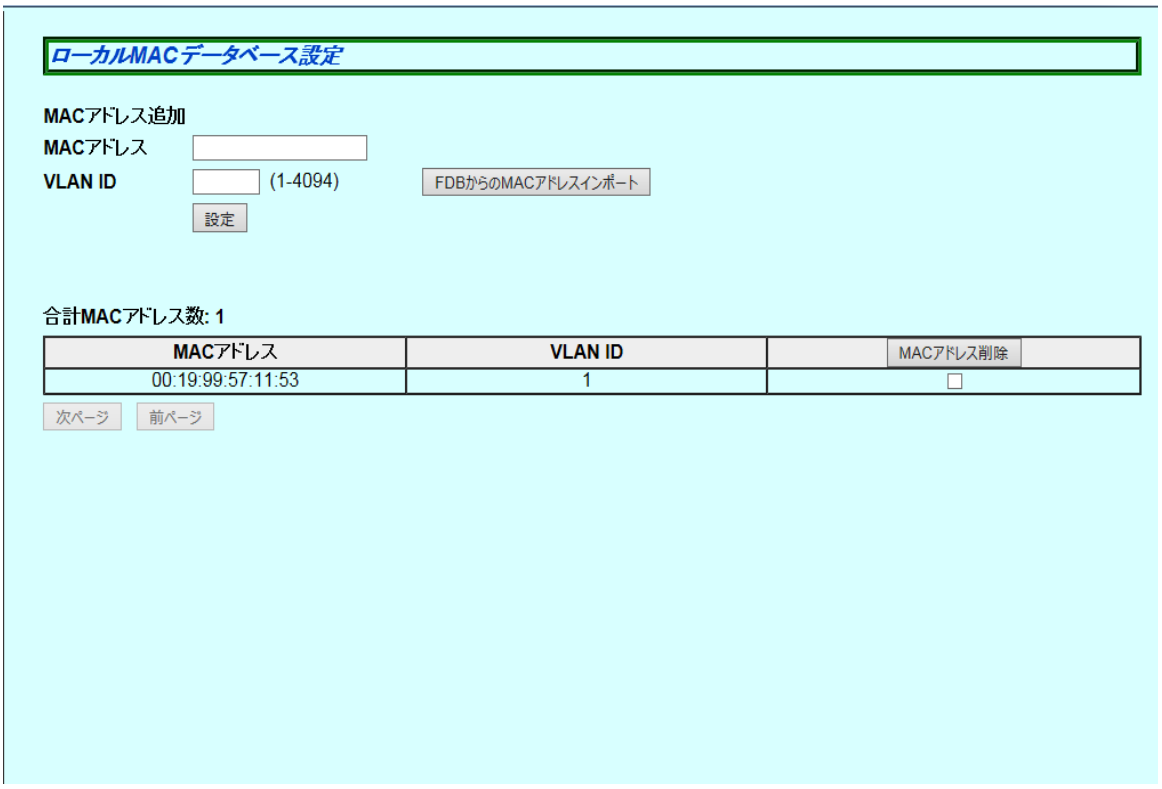


図 3-37 ローカル MAC データベース設定

画面の説明

MAC アドレス	認証を許可する MAC アドレスを表示します。
VLAN ID	認証後に割り当てる VLAN ID を表示します。
MAC アドレス削除	選択された MAC アドレスを削除します。
FDB からの MAC アドレスインポート	FDB テーブルから一括で MAC アドレスをインポートする画面へ移動します。 詳細は次項を参照してください。

3.2.13. FDB からの MAC アドレスインポート

[認証設定] から [FDB からの MAC アドレスインポート] を選択すると、図 3-38 のような画面が表示されます。この画面では、FDB に学習された MAC アドレスについて、MAC 認証のローカル MAC アドレスとして一括追加ができます。

図 3-38 FDB からの MAC アドレスインポート

画面の説明

絞り込み	VLAN ID およびポート番号にて MAC アドレスの絞り込み表示を行います。
MAC アドレス	認証を許可する MAC アドレスを表示します。
VLAN ID	認証後に割り当てる VLAN ID を表示します。
割当先 VLAN ID	認証成功後に割り当てる VLAN ID を指定します。
インポート	FDB テーブルから一括で MAC アドレスをインポートする画面へ移動します。 詳細は次項を参照してください。

3.2.14. IEEE802.1X 認証設定

[IEEE802.1X 認証設定] から [IEEE802.1X 認証設定] を選択すると、図 3-39 のような画面が表示されます。この画面では、IEEE802.1X グローバル設定およびポートベース認証についての設定を行います。

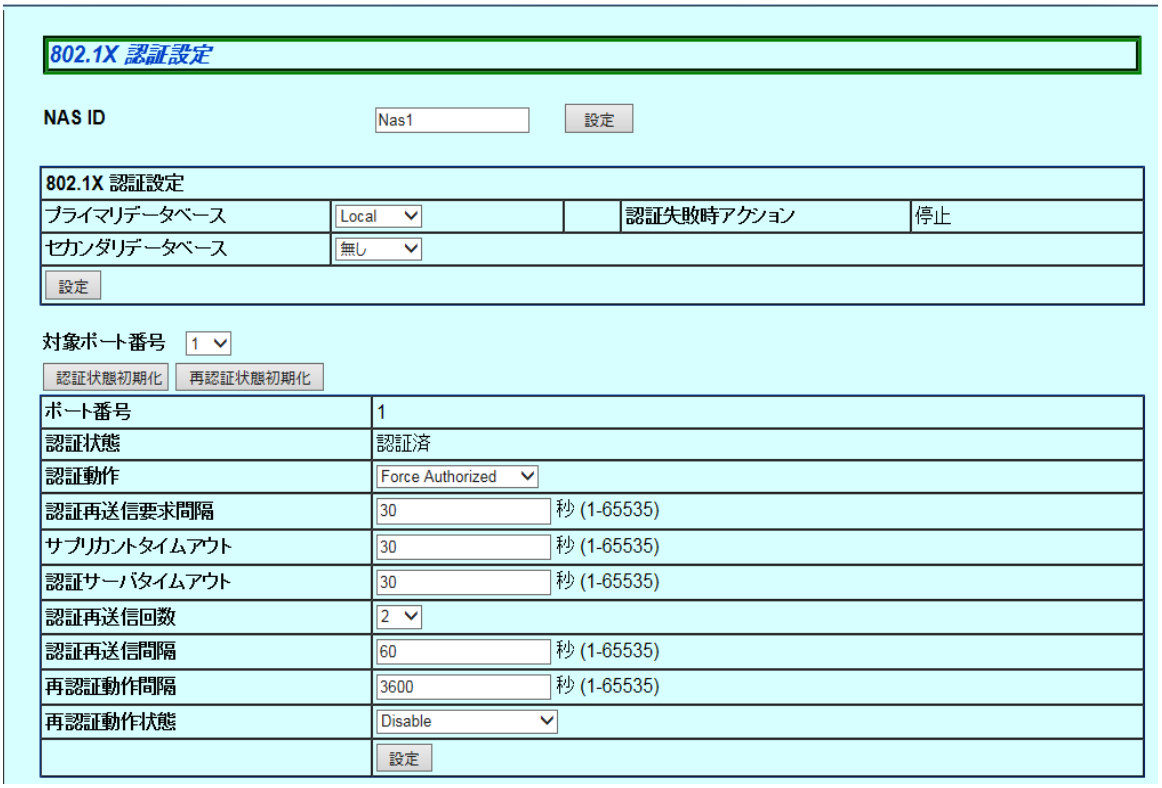


図 3-39 IEEE802.1X 認証設定

画面の説明

NAS ID	NAS ID が表示されます。	
プライマリ データベース	初回の認証問い合わせ先を表示します。	
	RADIUS	RADIUS サーバを使用します。
	Local	ローカルユーザデータベースを使用します。（工場出荷時設定）
セカンダリ データベース	プライマリデータベースでの認証失敗後の認証問い合わせ先を表示します。	
	Local	ローカルユーザデータベースを使用します。
	無し	認証なしで許可することを表します。（工場出荷時設定）
認証失敗時 アクション	プライマリデータベースにおいて認証が失敗した際の動作を表します。	
	停止 (固定)	セカンダリデータベースの認証を実行せず認証処理を停止します。 プライマリデータベースが RADIUS、かつ RADIUS サーバタイムアウトが発生した場合に限り、セカンダリデータベースへ移行します。
対象ポート番号	設定対象のポート番号が表示されます。	
認証状態初期化	認証状態を初期化します。	
再認証状態初期化	再認証の状態を初期化します。	
認証状態	認証の状態が表示されます。この状態は下記の認証動作設定を反映します。	
	未認証	認証が拒否されています。
	認証済	認証が承認されています。

認証動作	認証要求の動作が表示されます。	
	Auto	IEEE802.1X 認証を有効にします。
	Force Unauthorized	全ての通信を遮断します。
	Force Authorized	IEEE802.1X 認証を無効にし、全ての通信を許可します。 （工場出荷時設定）
認証再送信要求間隔	クライアントへ認証再送信を要求する間隔です。 工場出荷時は 30 秒に設定されています。	
クライアントタイムアウト時間	クライアントのタイムアウト時間が表示されます。 工場出荷時は 30 秒に設定されています。	
認証サーバタイムアウト時間	認証サーバのタイムアウト時間が表示されます。 工場出荷時は 30 秒に設定されています。	
認証再送信回数	認証の最大再送信試行回数です。工場出荷時は 2 回に設定されています。	
認証再送信間隔	認証が失敗してから次の認証要求が実行されるまでの時間です。 工場出荷時は 60 秒に設定されています。	
再認証動作間隔	周期的再認証を実行する間隔です。工場出荷時は 3600 秒に設定されています。	
再認証動作状態	周期的再認証の設定が表示されます。	
	Enable (RADIUS timer)	RADIUS サーバが通知した Session-Timeout Attribute を利用して周期的な再認証を実行します。
	Enable (Local timer)	この装置の [再認証動作間隔] の設定値を利用して周期的な再認証を実行します。
	Disable	周期的な再認証が無効です。(工場出荷時設定)

ご注意： IEEE802.1X ポートベース認証を使用する場合、MAC アドレス学習モードを「Disabled」に設定できません。

3.2.15. IEEE802.1X ポートベース認証設定

[IEEE802.1X 認証設定] から [ポートベース認証設定] を選択すると、**図 3-40** のような画面が表示されます。この画面では、IEEE802.1X ポートベース認証についての設定を行います。

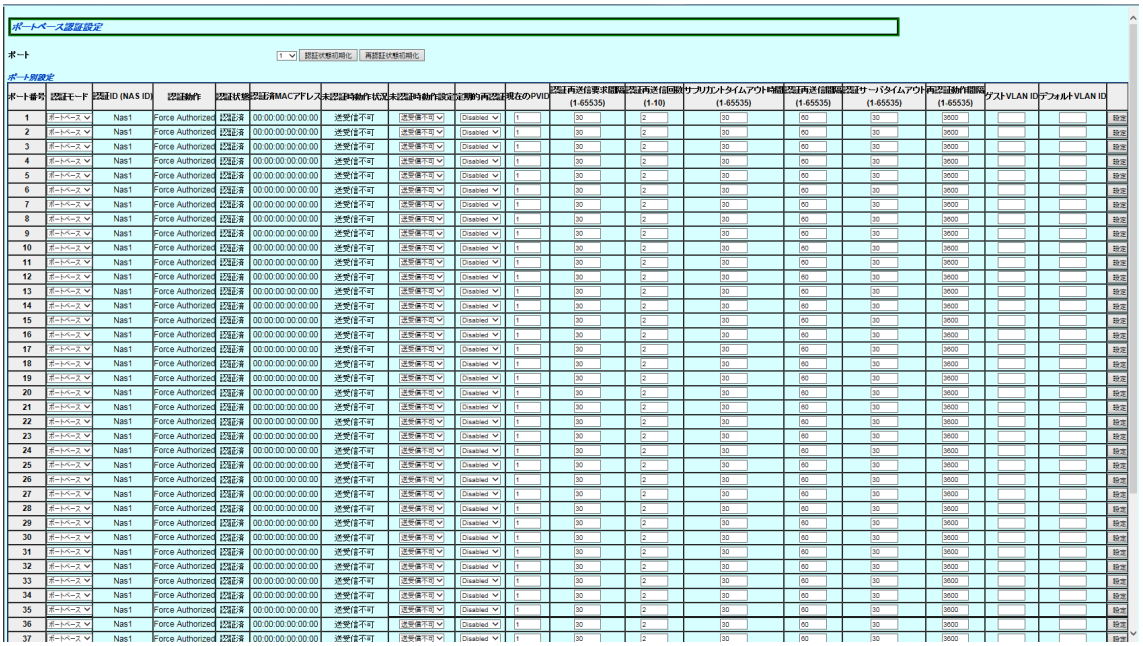


図 3-40 IEEE802.1X ポートベース認証設定

画面の説明

ポート番号	ポート番号を表示します。	
認証モード	認証方式を表示します。	
	ポートベース	IEEE802.1X ポートベース認証を行います。
	MAC ベース	IEEE802.1X MAC ベース認証を行います。
認証 ID	NAS ID を表示します。	
認証動作	認証要求の動作が表示されます。	
	Auto	IEEE802.1X 認証を有効にします。
	Force Unauthorized	全ての通信を遮断します。
	Force Authorized	IEEE802.1X 認証を無効にし、全ての通信を許可します。（工場出荷時設定）
認証状態	認証状態を表示します。	
	未認証	未認証状態を表します。
	認証済	認証済みであることを表します。
認証済 MAC アドレス	IEEE802.1X ポートベース認証の場合に認証済みである MAC アドレスを表示します。	
未認証時動作状況	認証要求時の動作状況が表示されます。	
	送受信不可	認証されていない状態では、対象ポートからのパケット送受信を行いません。
	受信不可	認証されていない状態では、対象ポートからのパケット受信を行いません。

未認証時動作設定	認証要求時の動作設定が表示されます。	
	送受信不可	認証されていない状態では、対象ポートからのパケット送受信を行いません。
	受信不可	認証されていない状態では、対象ポートからのパケット受信を行いません。
定期的再認証	定期的な再認証設定を表示します。	
	Enable	再認証を行います。
	Disable	再認証を行いません。（工場出荷時設定）
現在の PVID	現在の PVID を表示します。	
認証再送信要求間隔	サプリカントへの認証要求の再送信間隔を表示します。（工場出荷時設定：30 秒）	
認証再送信回数	再送信の回数を表示します。（工場出荷時設定：2 回）	
サプリカント タイムアウト時間	サプリカントのタイムアウト時間を表示します。（工場出荷時設定：30 秒）	
認証再送信間隔	認証失敗から再度認証処理が実行されるまでの間隔を表示します。 （工場出荷時設定：30 秒）	
認証サーバ タイムアウト	RADIUS サーバのタイムアウト時間を表示します。（工場出荷時設定：30 秒）	
再認証動作間隔	再認証を実行する間隔を表示します。（工場出荷時設定：3600 秒）	
ゲスト VLAN ID	未認証時に割り当てられる VLAN ID を表示します。	
デフォルト VLAN ID	認証時に RADIUS サーバより Tunnel-Private-Group-ID Attibute による VLAN 情報が通知されない場合に割り当てる VLAN ID を表示します。	

3.2.16. IEEE802.1X MAC 認証設定

[IEEE802.1X 認証設定] から [MAC ベース認証設定] を選択すると、**図 3-41** のような画面が表示されます。この画面では、IEEE802.1X MAC ベース認証についての設定を行います。

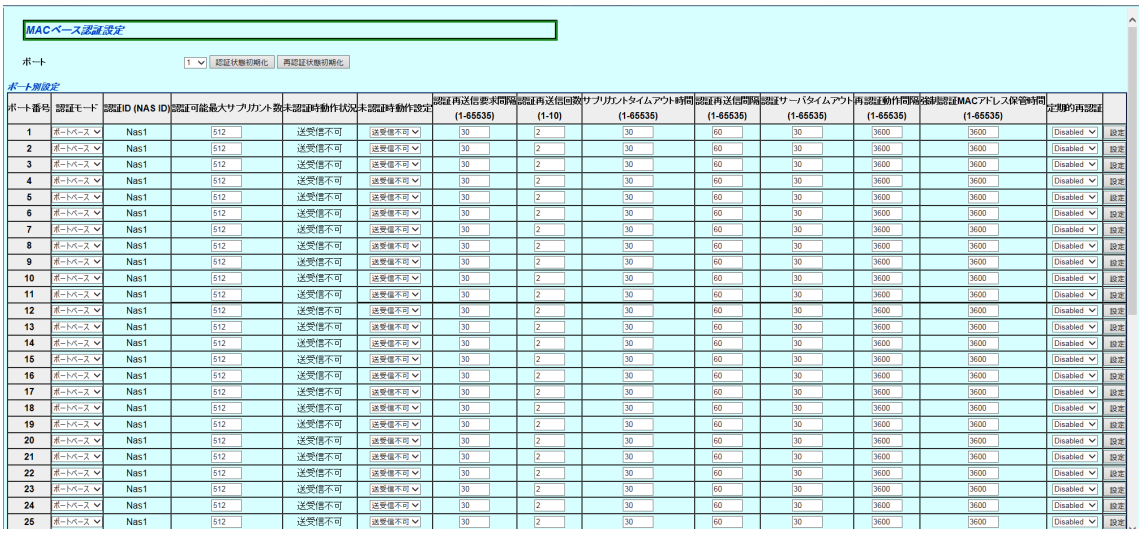


図 3-41 IEEE802.1X MAC ベース認証設定

画面の説明

ポート番号	ポート番号を表示します。	
認証モード	認証方式を表示します。	
	ポートベース	IEEE802.1X ポートベース認証を行います。
	MAC ベース	IEEE802.1X MAC ベース認証を行います。
認証 ID	NAS ID を表示します。	
認証可能 最大サプリカント数	認証を許可する最大サプリカント数を表示します。（工場出荷時設定：512）	
未認証時動作状況	認証要求時の動作状況が表示されます。	
	送受信不可	認証されていない状態では、対象ポートからのパケット送受信を行いません。
	受信不可	認証されていない状態では、対象ポートからのパケット受信を行いません。
未認証時動作設定	認証要求時の動作設定が表示されます。	
	送受信不可	認証されていない状態では、対象ポートからのパケット送受信を行いません。
	受信不可	認証されていない状態では、対象ポートからのパケット受信を行いません。
認証再送信要求間隔	サプリカントへの認証要求の再送信間隔を表示します。（工場出荷時設定：30 秒）	
認証再送信回数	再送信の回数を表示します。（工場出荷時設定：2 回）	
サプリカント タイムアウト時間	サプリカントのタイムアウト時間を表示します。（工場出荷時設定：30 秒）	
認証再送信間隔	認証失敗から再度認証処理が実行されるまでの間隔を表示します。 （工場出荷時設定：30 秒）	
認証サーバ タイムアウト	RADIUS サーバのタイムアウト時間を表示します。（工場出荷時設定：30 秒）	
再認証動作間隔	再認証を実行する間隔を表示します。（工場出荷時設定：3600 秒）	

強制認証 MAC アドレス 保管時間	強制 MAC アドレス認証エントリのエージアウトタイムを表示します。 （工場出荷時設定：3600 秒）	
定期的再認証	定期的な再認証設定を表示します。	
	Enable	再認証を行います。
	Disable	再認証を行いません。（工場出荷時設定）

3.2.17. IEEE802.1X MAC ベース認証サプリカントリスト

[IEEE802.1X 認証設定] から [MAC ベース認証サプリカントリスト] を選択すると、図 3-42 のような画面が表示されます。この画面では、IEEE802.1X MAC ベース認証の対象となるサプリカント一覧を表示します。

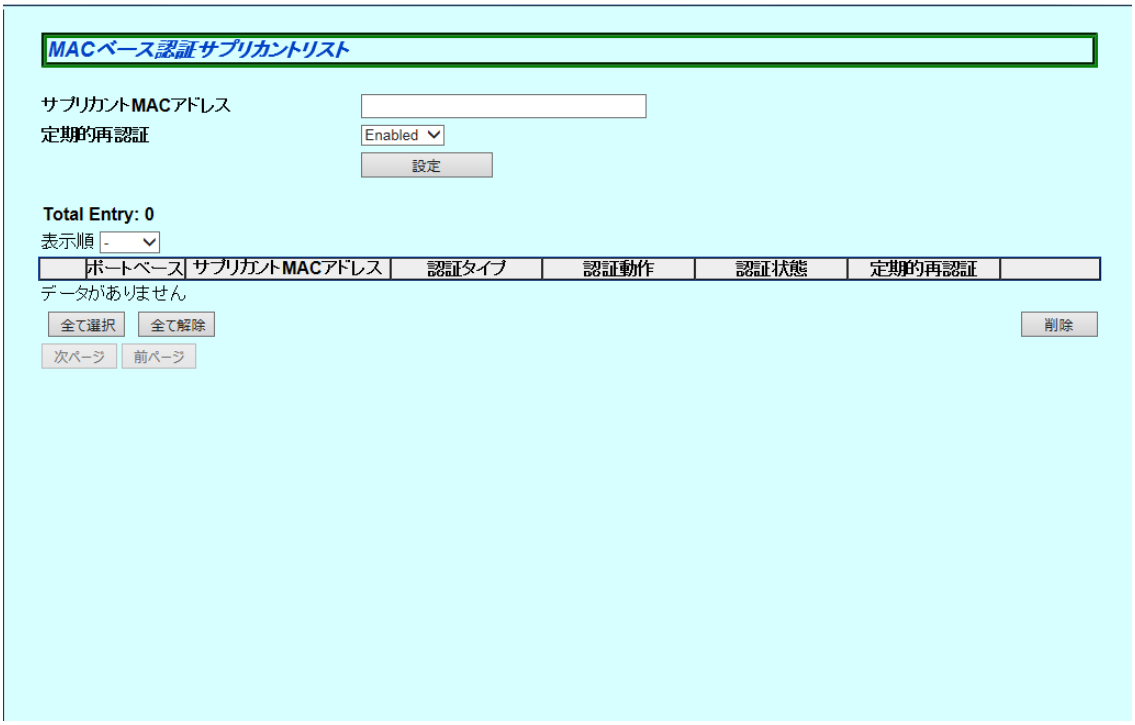


図 3-42 MAC ベース認証サプリカントリスト

画面の説明

サプリカント MAC アドレス	設定対象とする MAC アドレスを入力します。	
定期的再認証	定期的な再認証動作を設定します。	
	Enabled	再認証を行います。
	Disabled	再認証を行いません。（工場出荷時設定）
ポート番号	ポート番号を表示します。	
サプリカント MAC アドレス	認証に成功している端末の MAC アドレスが表示されます。また、強制認証 MAC アドレス設定で登録されている端末が通信している場合、その MAC アドレスが表示されます。	
認証タイプ	認証の種類を表示します。	
	Dynamic	MAC ベース認証にて認証された端末を表します。
	Static	強制認証 MAC アドレス設定で設定された端末を表します。
認証動作	認証動作を表示します。	
	Auto	IEEE802.1X 認証が有効であることを表します。
	Force Authorized	IEEE802.1X 認証が無効ですべての通信を許可していることを表します。（工場出荷時設定）
	Force Unauthorized	すべての通信を遮断していることを表します。
認証状態	認証状態を表示します。	
	未認証	未認証であることを表します。
	認証済	認証済みであることを表します。

定期的再認証	定期的な再認証設定を表示します。	
	Enabled	再認証を行います。
	Disabled	再認証を行いません。（工場出荷時設定）

3.2.18. 強制認証 MAC アドレス設定

[IEEE802.1X 認証設定] から [強制認証 MAC アドレス設定] を選択すると、**図 3-43** のような画面が表示されます。この画面では、IEEE802.1X 認証を行わずに認証を許可 / 不許可する機器の MAC アドレスを設定することができます。

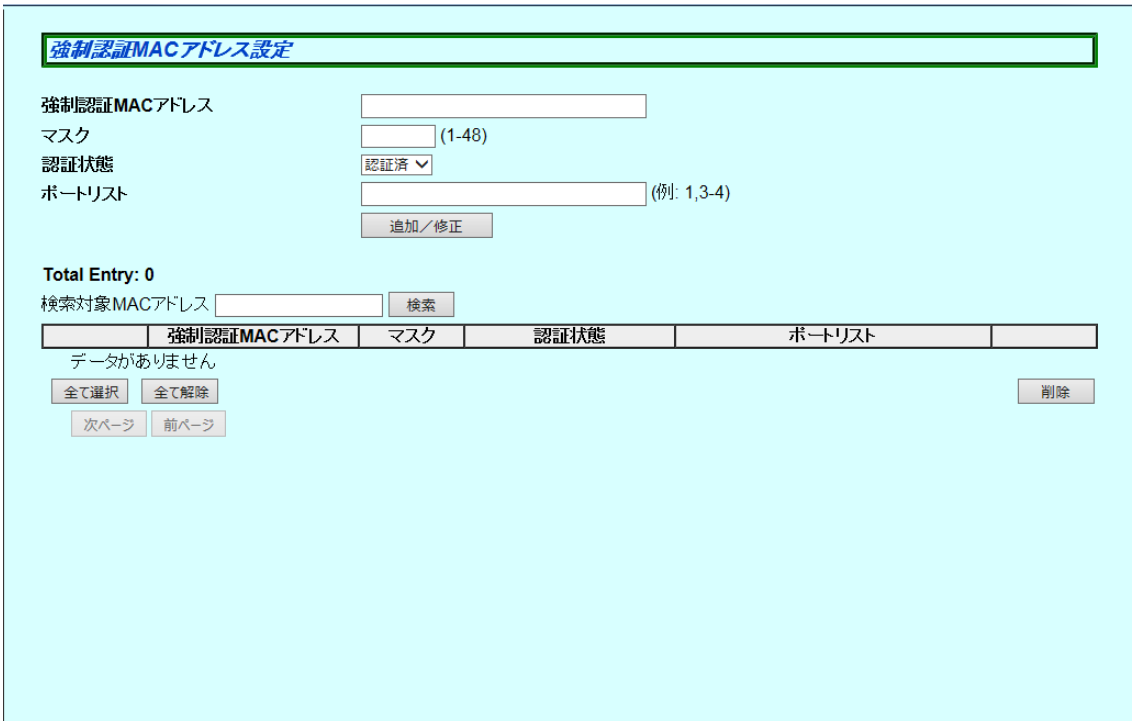


図 3-43 強制認証 MAC アドレス設定

画面の説明

強制認証 MAC アドレス	IEEE802.1X 認証を実行せず静的に認証／拒否を行う端末の MAC アドレスを表示します。	
マスク	対象とする MAC アドレスのマスク長を表示します。	
認証状態	認証状態を表示します。	
	未認証	未認証であることを表します。
	認証済	認証済みであることを表します。
ポートリスト	対象とするポートを表示します。	

3.2.19. IEEE802.1X 統計情報

[IEEE802.1X 認証設定] から [統計情報] を選択すると、図 3-44 のような画面が表示されます。この画面では、IEEE802.1X 認証の統計情報を確認できます。

カウンタ名 / ポート1	合計	秒平均
TxReqId	0	0
TxReq	0	0
TxTotal	0	0
RxStart	0	0
RxLogoff	0	0
RxRespId	0	0
RxResp	0	0
RxInvalid	0	0
RxLenError	0	0
RxTotal	0	0
RxVersion	0	0
LastRxSrcMac	00:00:00:00:00:00	

図 3-44 IEEE802.1X 統計情報

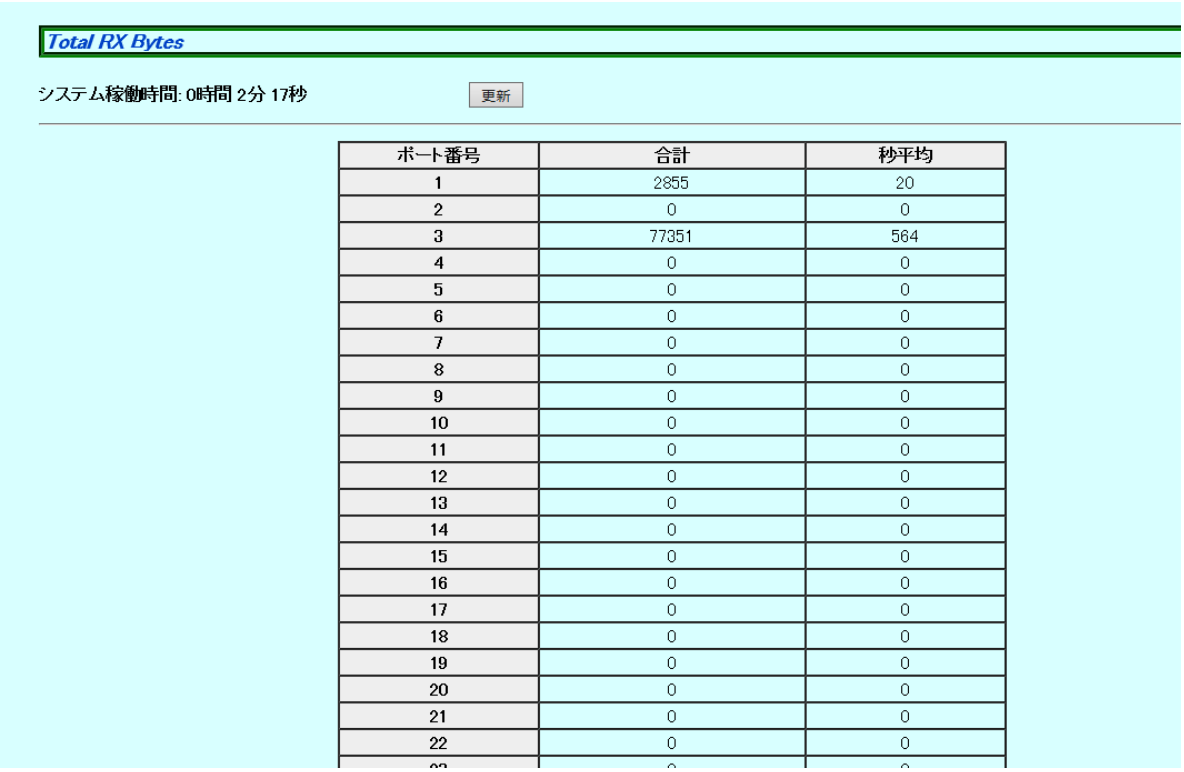
画面の説明

対象ポート番号	表示対象のポート番号を選択します。
カウンタリセット	各カウンタ値のリセットを行い、カウンタがリセットされてからの経過時間が0に戻ります。(起動されてからの経過時間およびカウンタ値はリセットされません)
カウンタリセットから	カウンタがリセットされてからの経過時間およびカウンタ値の表示に切り替わります。
起動時から	起動されてからの経過時間およびカウンタ値の表示に切り替わります。
カウンタ名	カウンタ名が表示されます。
合計	カウンタの値が表示されます。
秒平均	秒あたりのカウンタの平均値が表示されます。

各カウンタの内容は以下のとおりです。

TxReqId	この装置から送信された EAP Request Identity フレームの数が表示されます。
TxReq	この装置から送信された EAP Request フレームの数が表示されます。
TxTotal	この装置から送信された全てのタイプの EAP フレームの総数が表示されます。
RxStart	サプリカントから受信した EAPOL Start フレームの数が表示されます。
RxLogoff	サプリカントから受信した EAPOL Logoff フレームの数が表示されます。
RxRespId	サプリカントから受信した EAP Response Identity フレーム数が表示されます。
RxResp	サプリカントから受信した EAP Response フレーム数が表示されます。
RxInvalid	サプリカントから受信した EAPOL フレームのうち、フレームタイプを認識できないフレームの数が表示されます。
RxLenError	サプリカントから受信した EAPOL フレームのうち、パケット本体の長さを示すフィールドが無効なフレームの数が表示されます。
RxTotal	サプリカントから受信した EAP フレームのうち、有効なフレームの総数が表示されます。
RxVersion	サプリカントから受信した EAP フレームのうち、IEEE802.1X バージョン 1 の形式で受信したフレームの数が表示されます。
LastRxSrcMac	本装置が最後に受信したEAPOLフレームの送信元のMACアドレスが表示されます。

カウンタ名をクリックすると、図 3-45 のような画面が表示されます。この画面には、カウンタの総数および秒あたりの平均数がポート別に表示されます。



Total RX Bytes

システム稼働時間: 0時間 2分 17秒　更新

ポート番号	合計	秒平均
1	2855	20
2	0	0
3	77351	564
4	0	0
5	0	0
6	0	0
7	0	0
8	0	0
9	0	0
10	0	0
11	0	0
12	0	0
13	0	0
14	0	0
15	0	0
16	0	0
17	0	0
18	0	0
19	0	0
20	0	0
21	0	0
22	0	0

図 3-45 ポート別のカウンタ統計情報

画面の説明

システム稼働時間	この装置が起動されてからの経過時間が表示されます。 [更新] ボタンをクリックすると、経過時間およびカウンタ値の表示が更新されます。
ポート番号	ポート番号が表示されます。
合計	カウンタの値が表示されます。
秒平均	秒あたりのカウンタの平均値が表示されます。

3.2.20. EAP-Request 送信設定

[IEEE802.1X 認証設定] から [EAP-Request 送信設定] を選択すると、図 3-46 のような画面が表示されます。この画面では、IEEE802.1X MAC ベース認証時にサプリカントの認証開始のための EAP Request 送信機能についての設定を行います。

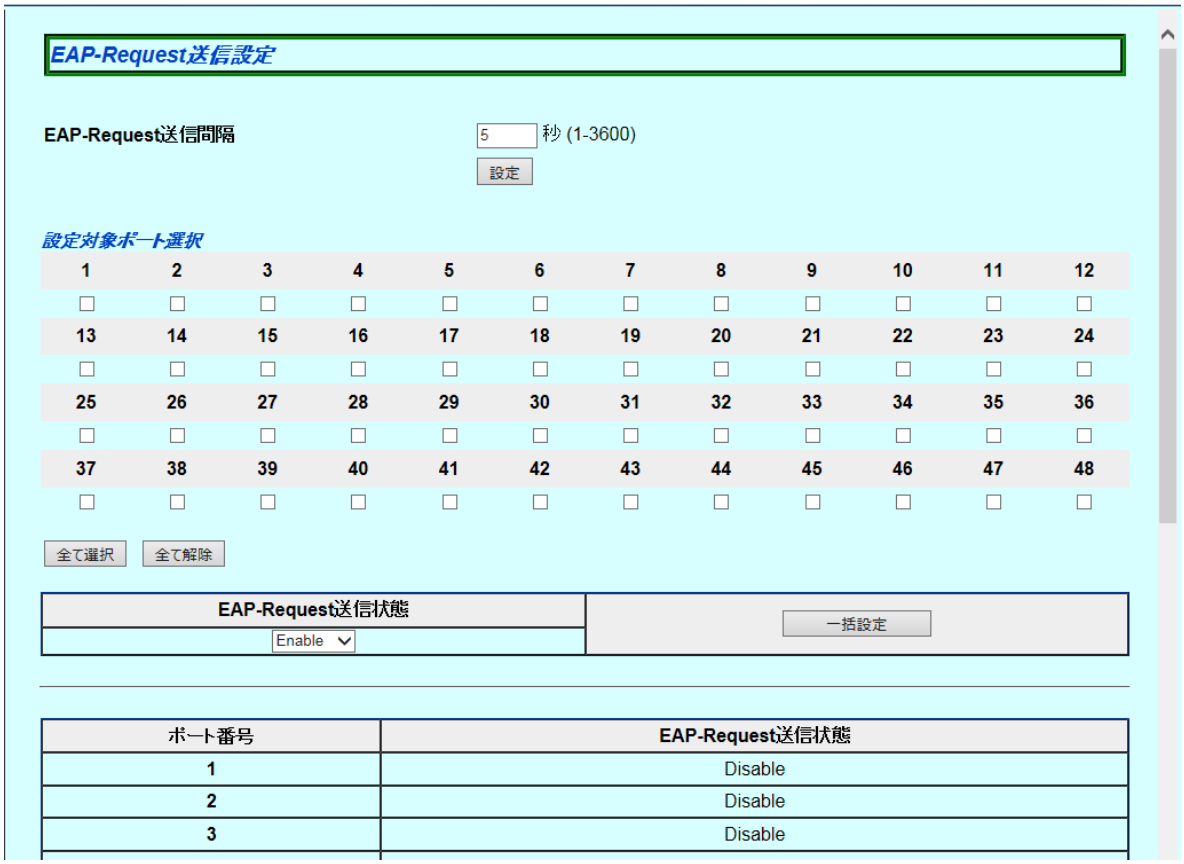


図 3-46 EAP-Request 送信設定

画面の説明

EAP-Request 送信間隔	サプリカントへ EAP Request を送信する間隔を表示します。（工場出荷時設定：5 秒）	
ポート番号	ポート番号を表示します。	
EAP-Request 送信状態	EAP Request の送信状態を表示します。	
	Enable	未認証 MAC アドレステーブルに登録された MAC アドレスに対し、EAP-Request 送信間隔毎に EAP Request を送信します。
	Disable	EAP Request 送信が無効です。（工場出荷時設定）

3.2.21. 未認証 MAC アドレス表示

[IEEE802.1X 認証設定] から [未認証 MAC アドレス表示] を選択すると、図 3-47 のような画面が表示されます。この画面では、EAP Request の送信対象となる未認証 MAC アドレステーブルを表示します。

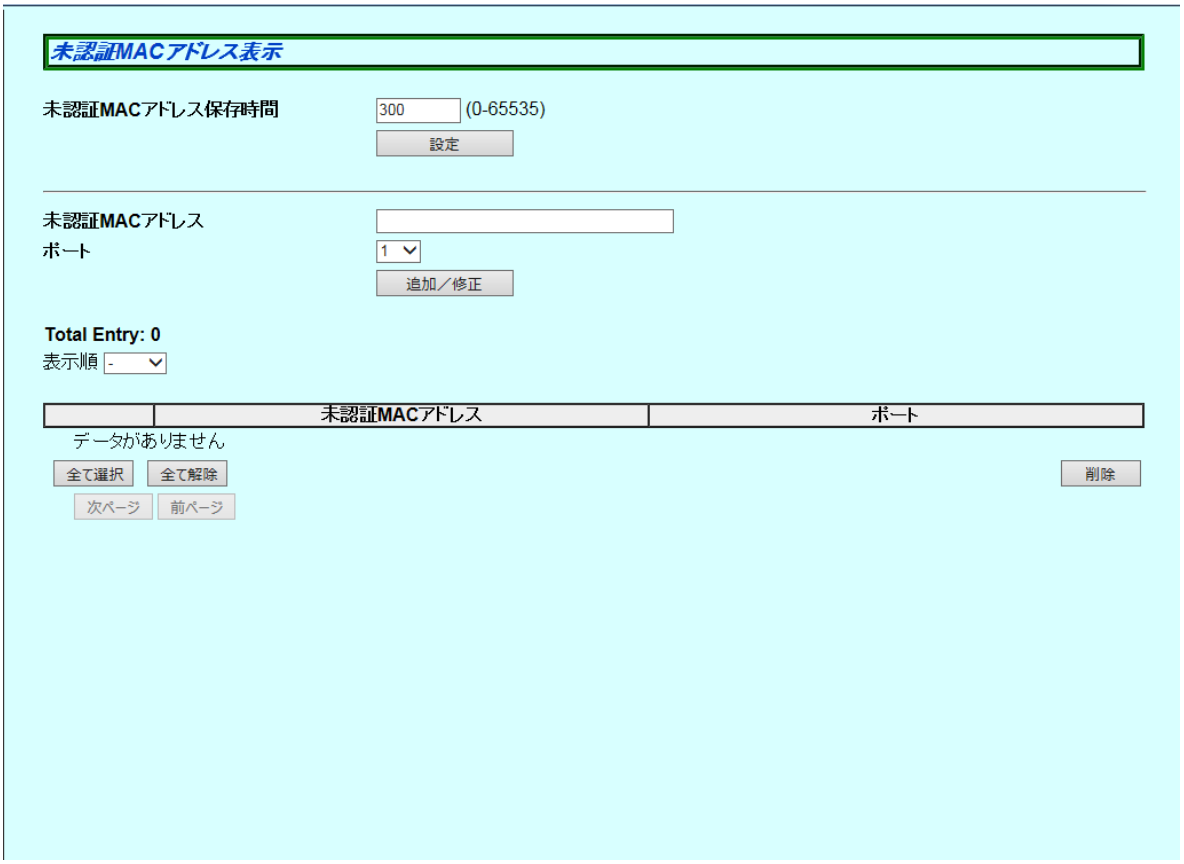


図 3-47 未認証 MAC アドレス表示

画面の説明

未認証 MAC アドレス保存時間	未認証 MAC アドレスが検出されてから保持する （工場出荷時設定：300 秒）
未認証 MAC アドレス	未認証である MAC アドレスを表示します。
ポート	未認証 MAC アドレスが接続されているポート番号を表示します。

3.2.22. MAC 認証設定

[認証設定] から [MAC 認証設定] を選択すると、図 3-48 のような画面が表示されます。この画面では、MAC 認証についての設定を行います。

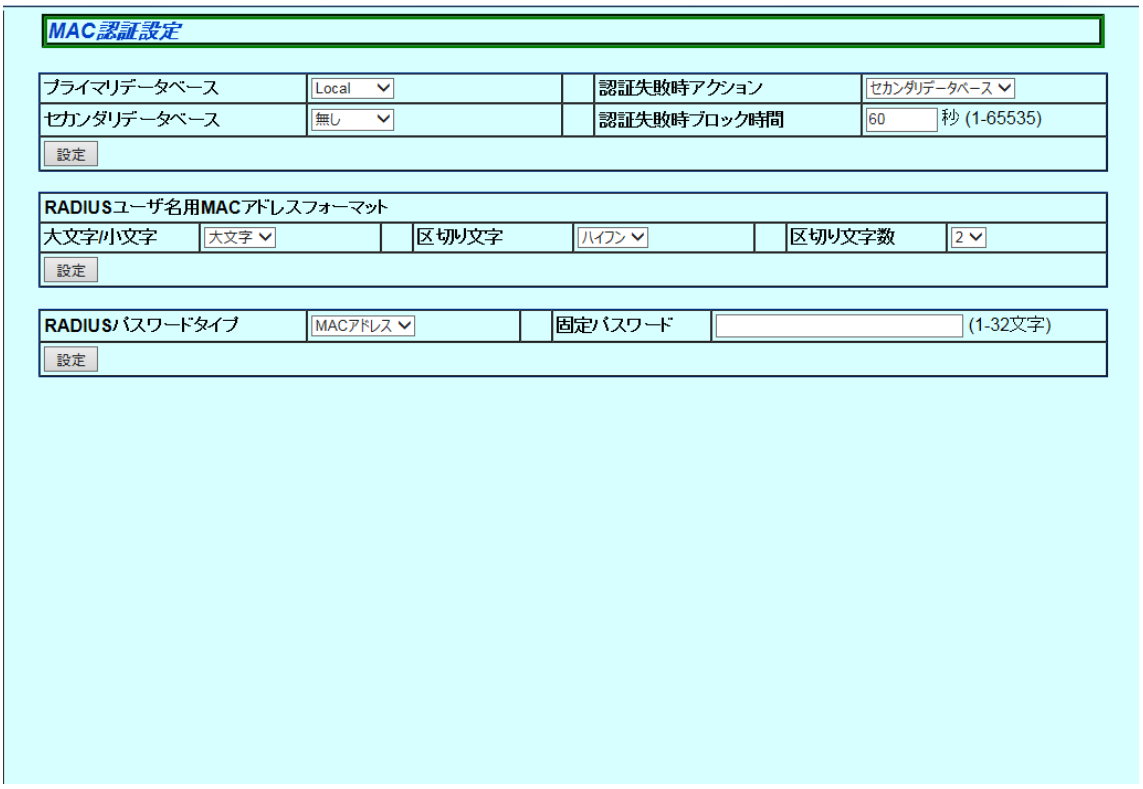


図 3-48 MAC 認証設定

画面の説明

プライマリ データベース	初回の認証問い合わせ先を表示します。	
	RADIUS	RADIUS サーバを使用します。
	Local	ローカルユーザデータベースを使用します。（工場出荷時設定）
セカンダリ データベース	プライマリデータベースでの認証失敗後の認証問い合わせ先を表示します。	
	RADIUS	RADIUS サーバを使用します。
	Local	ローカルユーザデータベースを使用します。
	無し	認証処理なしで許可することを表します。（工場出荷時設定）
認証失敗時 アクション	プライマリデータベースにおいて認証が失敗した際の動作を表します。	
	停止	セカンダリデータベースの認証を実行せず認証処理を停止します。（工場出荷時設定） プライマリデータベースが RADIUS、かつ RADIUS サーバタイムアウトが発生した場合に限り、セカンダリデータベースへ移行します。
	セカンダリ データベース	プライマリデータベースにて認証が失敗した際にセカンダリデータベースでの認証処理を実行します。
認証失敗時 ブロック時間	認証が失敗した際に再試行するまでのブロック時間を表示します。 （工場出荷時設定：60 秒）	
RADIUS ユーザ名用 MAC アドレス フォーマット	MAC 認証において RADIUS サーバを使用する場合に、RADIUS サーバへユーザ名として送信する MAC アドレスの書式を表します。	

大文字 / 小文字	MAC アドレスの大文字 / 小文字を表示します。	
	大文字	大文字で送信することを表します。（工場出荷時設定）
	小文字	小文字で送信することを表します。
区切り文字	MAC アドレスの区切り文字の種類を表示します。	
	ハイフン	ハイフン (-) を使用します。（工場出荷時設定）
	コロン	コロン (:) を使用します。
	ドット	ドット (.) を使用します。
	無し	区切り文字を使用しません。
区切り文字数	MAC アドレスを区切る文字数を表示します。	
	2	2 文字ごとに区切ります。（工場出荷時設定）
	4	4 文字ごとに区切ります。
	6	6 文字ごとに区切ります。
RADIUS パスワードタイプ	MAC 認証において RADIUS サーバを使用する場合に、RADIUS サーバへパスワードとして送信する文字列の書式を表示します。	
	MAC アドレス	MAC アドレスと同一の文字列を使用することを表します。（工場出荷時設定）
	固定	任意の固定文字列を使用することを表します。
固定パスワード	RADIUS サーバへパスワードとして送信する文字列を表示します。 RADIUS パスワードタイプが固定に設定されている場合にのみ使用されます。	

3.2.23. WEB 認証設定

[認証設定] から [WEB 認証設定] を選択すると、図 3-49 のような画面が表示されます。この画面では、WEB 認証についての設定を行います。

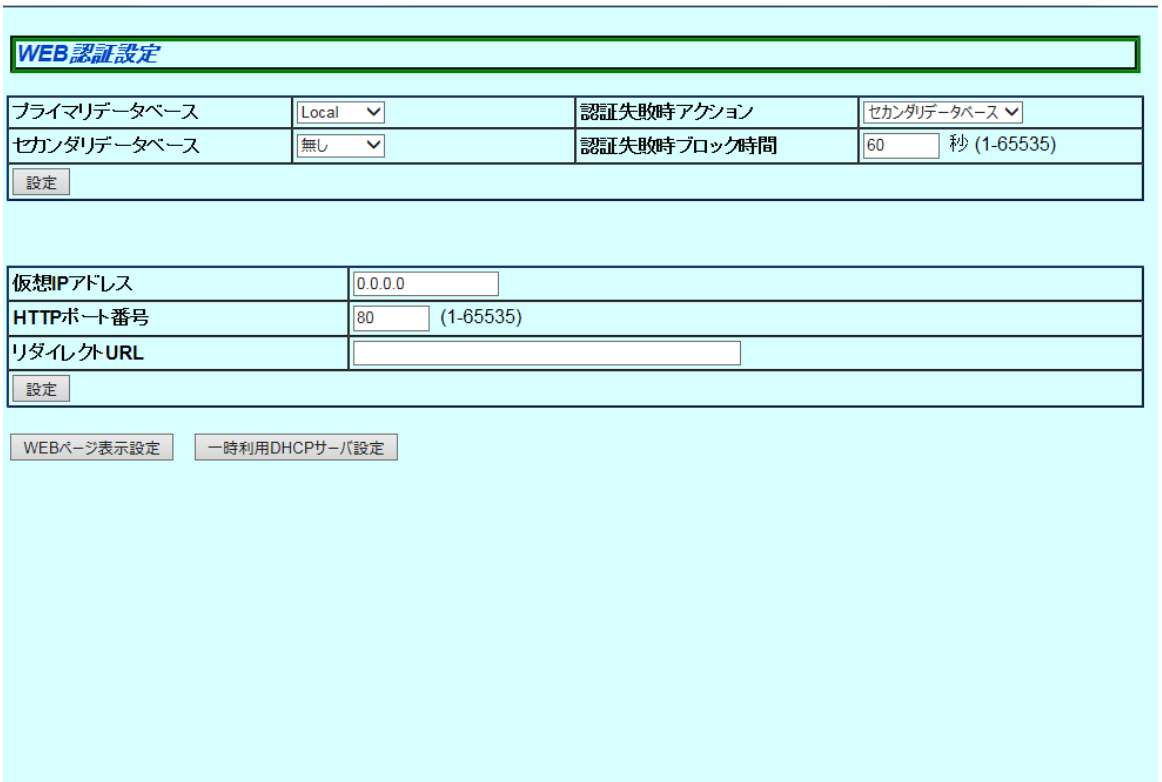


図 3-49 WEB 認証設定

画面の説明

プライマリ データベース	初回の認証問い合わせ先を表示します。	
	RADIUS	RADIUS サーバを使用します。
	Local	ローカルユーザデータベースを使用します。（工場出荷時設定）
セカンダリ データベース	プライマリデータベースでの認証失敗後の認証問い合わせ先を表示します。	
	RADIUS	RADIUS サーバを使用します。
	Local	ローカルユーザデータベースを使用します。
	無し	認証処理なしで許可することを表します。（工場出荷時設定）
認証失敗時 アクション	プライマリデータベースにおいて認証が失敗した際の動作を表します。	
	停止	セカンダリデータベースの認証を実行せず認証処理を停止します。（工場出荷時設定） プライマリデータベースが RADIUS、かつ RADIUS サーバタイムアウトが発生した場合に限り、セカンダリデータベースへ移行します。
	セカンダリ データベース	プライマリデータベースにて認証が失敗した際にセカンダリデータベースでの認証処理を実行します。
認証失敗時 ブロック時間	認証が失敗した際に再試行するまでのブロック時間を表示します。 （工場出荷時設定：60 秒）	
仮想 IP アドレス	WEB 認証ログイン画面で表示される仮想 IP アドレスを表示します。	
HTTP ポート番号	WEB 認証ログイン画面で表示される TCP ポート番号を表示します。 **本設定を変更すると、WEB 設定画面のポート番号も変更されます。** （工場出荷時設定：80）	

リダイレクト URL	WEB 認証成功後にリダイレクト表示させる URL を表示します。

3.2.24. WEB ページ表示設定

[WEB 認証設定] から [WEB ページ表示設定] を選択すると、図 3-50 のような画面が表示されます。この画面では、WEB 認証のログインページに表示する内容のついての設定を行います。

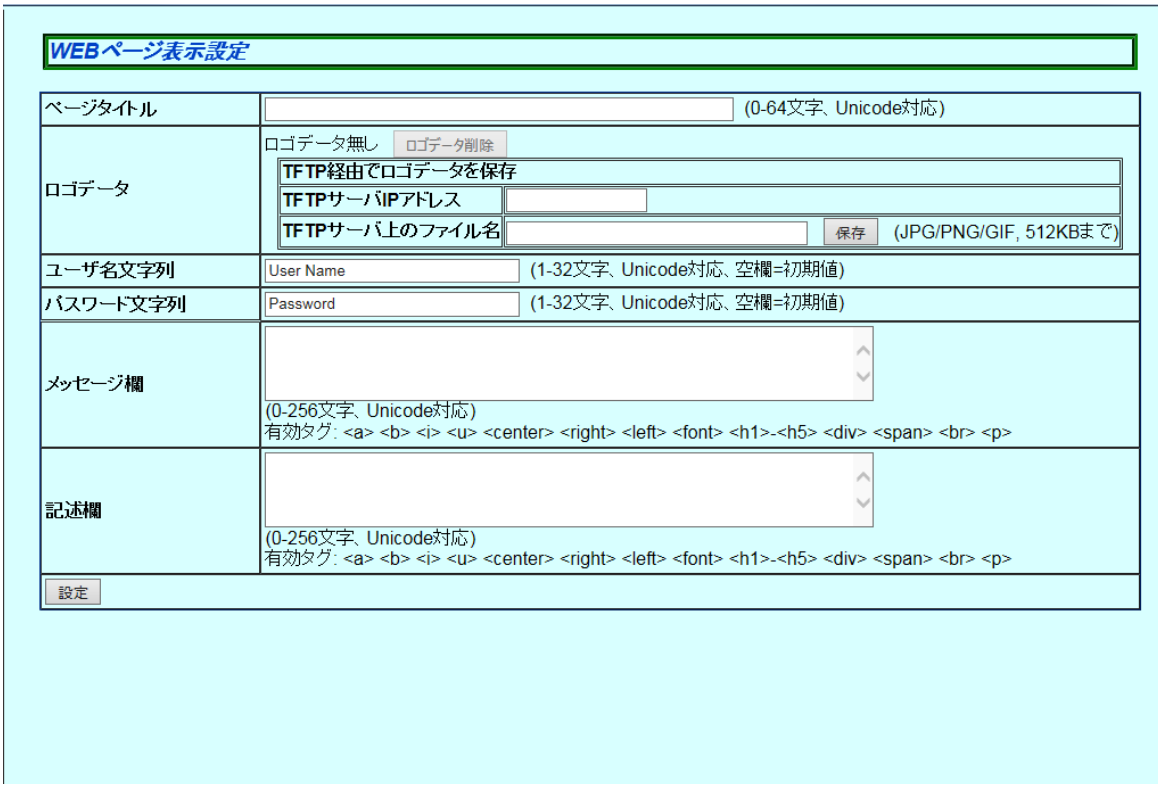


図 3-50 WEB ページ表示設定

画面の説明

ページタイトル	WEB 認証ログインページのタイトル文字列を表示します。 日本語入力が可能です。
ロゴデータ	ロゴデータの有無を表示します。TFTP サーバ経由にて JPG/PNG/GIF 形式の画像データを 512KB まで転送可能です。 ロゴデータが存在する場合は、実際の画像が表示されます。
ユーザ名文字列	ユーザ名入力欄の文字列を表示します。（工場出荷時設定：User Name） 日本語入力が可能です。
パスワード文字列	パスワード入力欄の文字列を表示します。（工場出荷時設定：Password） 日本語入力が可能です。
メッセージ欄	メッセージ欄の表示テキストを表示します。 日本語入力および以下の HTML タグが使用可能です。 <a> <b> <i> <u> <right> <left> <font> <h1> ～ <h5> <p> （他の HTML タグは無効化）
記述欄	記述欄の表示テキストを表示します。 日本語入力および以下の HTML タグが使用可能です。 <a> <b> <i> <u> <right> <left> <font> <h1> ～ <h5> <p> （他の HTML タグは無効化）

3.2.25. 一時利用 DHCP サーバ設定

[WEB 認証設定] から [一時利用 DHCP サーバ設定] を選択すると、図 3-51 のような画面が表示されます。この画面では、WEB 認証ポートかつゲスト VLAN 内の DHCP クライアントが WEB 認証を行う際に必要な IP アドレスを配布するための、一時利用 DHCP サーバの設定を行います。

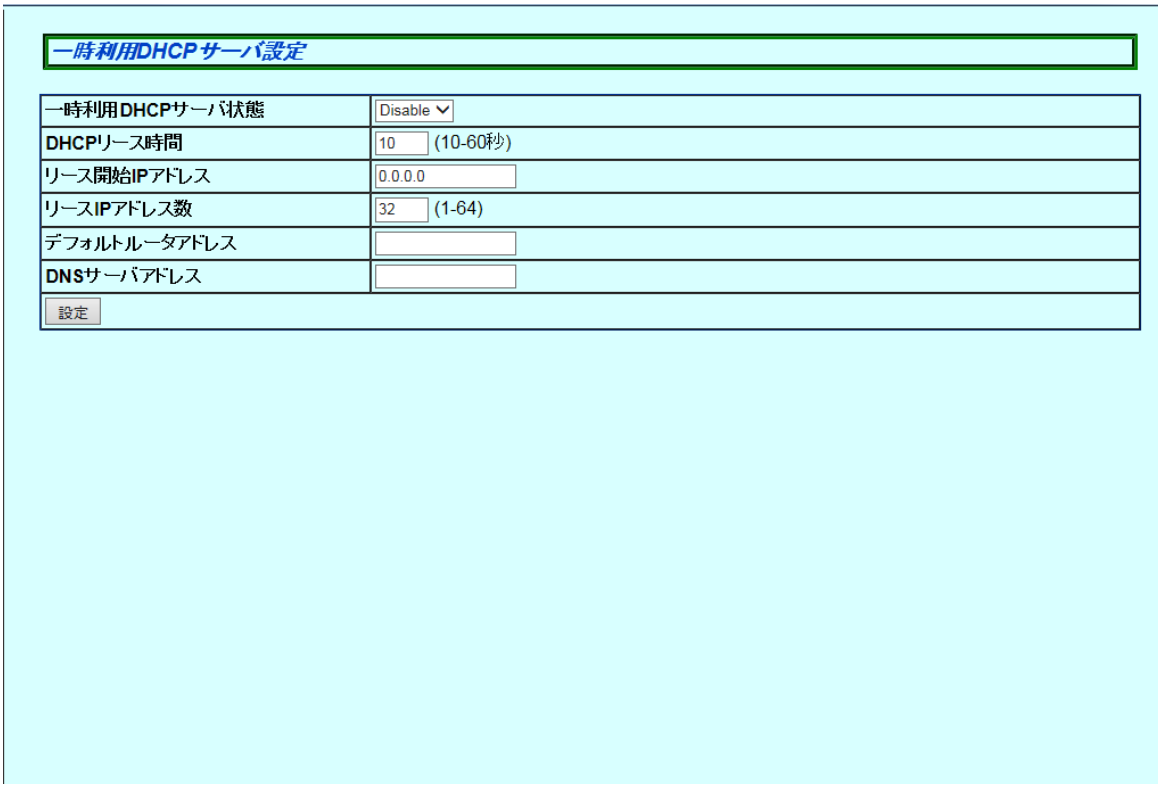


図 3-51 一時利用 DHCP サーバ設定

画面の説明

一時利用 DHCP サーバ状態	一時利用 DHCP サーバの状態を表示します。 ゲスト VLAN かつ WEB 認証が有効なポートに対し、WEB 認証時のアクセスに必要な IP アドレスの払い出しを行います。 本機能を利用するには対象とする WEB 認証ポートに対し、管理 VLAN を有効にしたゲスト VLAN を設定してください。	
	Enable	一時利用 DHCP サーバが有効です。
	Disable	一時利用 DHCP サーバが無効です。（工場出荷時設定）
DHCP リース時間	IP アドレスのリース時間 (秒) を表示します。（工場出荷時設定：30）	
リース開始 IP アドレス	リースする IP アドレスの開始アドレスを表示します。 サブネットマスクは 255.255.255.0 固定です。	
リース IP アドレス数	リースする IP アドレス数を表示します。（工場出荷時設定：32）	
デフォルト ルータアドレス	DHCP で通知するデフォルトルータアドレスの値を表示します。	
DNS サーバアドレス	DHCP で通知する DNS サーバアドレスの値を表示します。	

3.2.26. ダイナミック VLAN 設定

[認証設定] から [ダイナミック VLAN 設定] を選択すると、図 3-52 のような画面が表示されます。この画面では、ダイナミック VLAN の設定を行います。

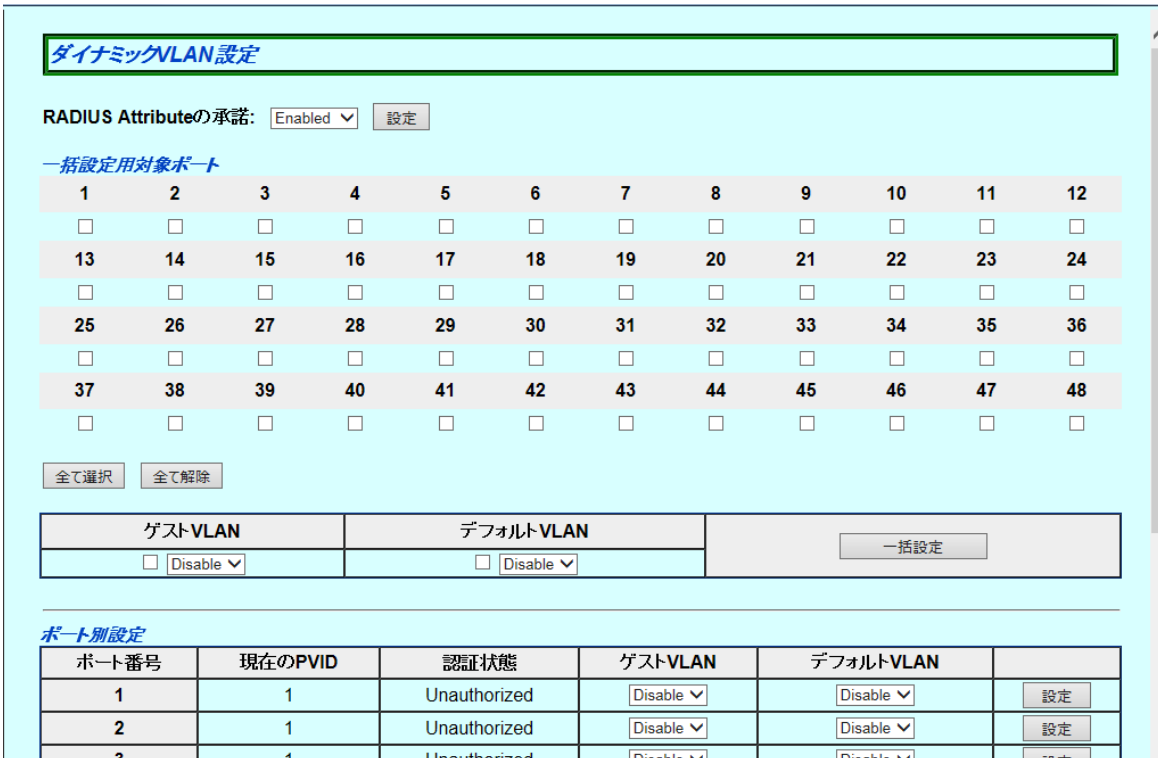


図 3-52 ダイナミック VLAN 設定

画面の説明

RADIUS Attribute の承諾	RADIUS サーバから通知された Attribute の使用可否を表示します。 対象とする Attribute は以下の通りです。 ・Tunnel-Private-Group-ID	
	Enabled	通知された Attribute を使用します。（工場出荷時設定）
	Disabled	この装置の設定を使用します。
ポート番号	ポート番号を表示します。	
現在の PVID	現在の PVID を表示します。	
認証状態	現在のポート認証状態を表示します。	
	Authorized	認証機能が無効、または IEEE802.1X ポートベース認証による認証済ポートを表します。
	Unauthorized	IEEE802.1X MAC ベース認証、MAC 認証、WEB 認証の待受ポートを表します。
ゲスト VLAN	ゲスト VLAN の VLAN ID を表示します。既存の VLAN のみ指定可能です。	
	Disable	ゲスト VLAN が無効です。（工場出荷時設定）
デフォルト VLAN	デフォルト VLAN の VLAN ID を表示します。既存の VLAN のみ指定可能です。 RADIUS Attribute の承諾が Enabled、かつ RADIUS サーバより Tunnel-Private-Group-ID が通知されない場合に割り当てる VLAN を指定します。	
	Disable	デフォルト VLAN が無効です。（工場出荷時設定）

3.2.27. ポートモニタリングの設定

[拡張機能設定] から [ポートモニタリング設定] を選択すると、図 3-53 のような画面が表示されます。この画面では、ポートモニタリングの設定を行うことができます。

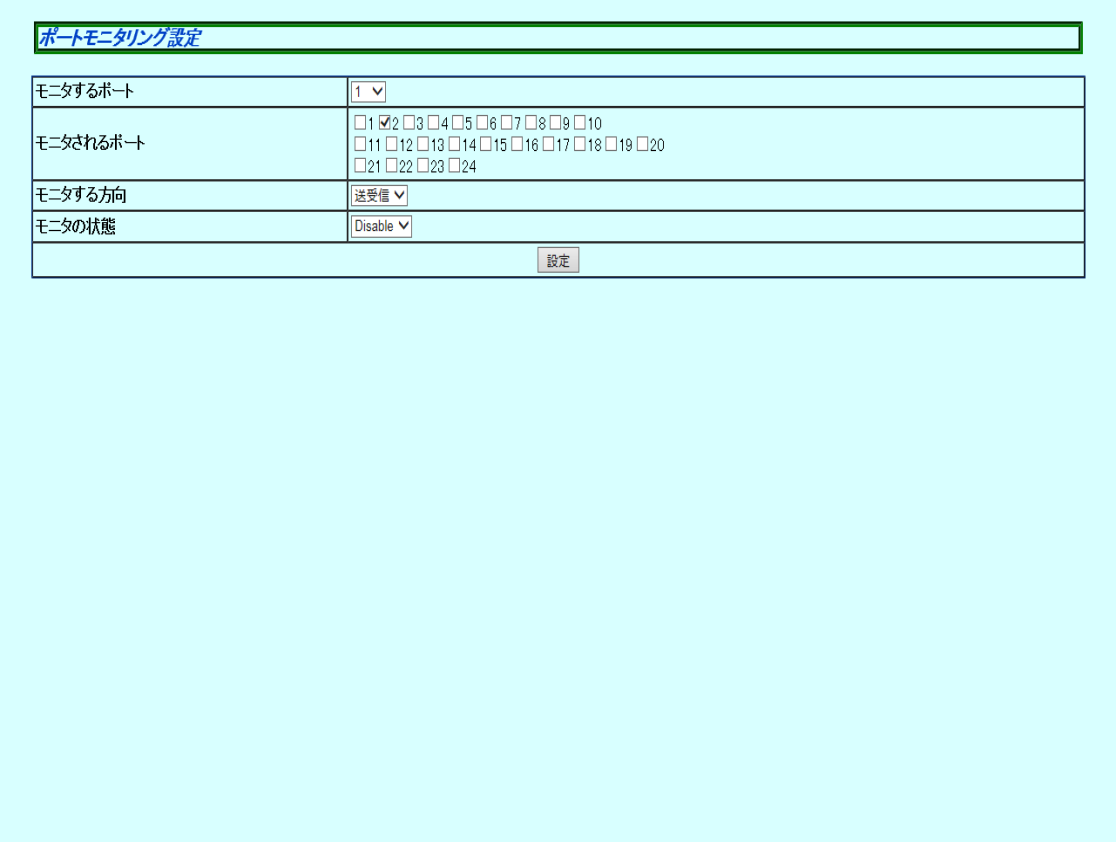


図 3-53 ポートモニタリングの設定

画面の説明

モニタするポート	他のポートからのパケットをモニタ可能なポートのポート番号が表示されます。	
モニタされるポート	モニタされるポートのポート番号が表示されます。	
モニタする方向	モニタされるポートで送受信パケットのどちらがモニタされているのかが表示されます。 工場出荷時は「送受信」に設定されています。	
	送信	送信パケットをモニタします。
	受信	受信パケットをモニタします。
	送受信	送受信パケットをモニタします。
モニタの状態	モニタリングが有効かどうかが表示されます。 工場出荷時は「 Disable 」に設定されています。	
	Enable	パケットをモニタします。
	Disable	パケットをモニタしません。

3.2.28. Classifier 設定

[拡張機能設定] から [アクセスコントロール設定]、[Classifier 設定] の順に選択すると、**図 3-54** のような画面が表示されます。この画面では Classifier の設定を行います。

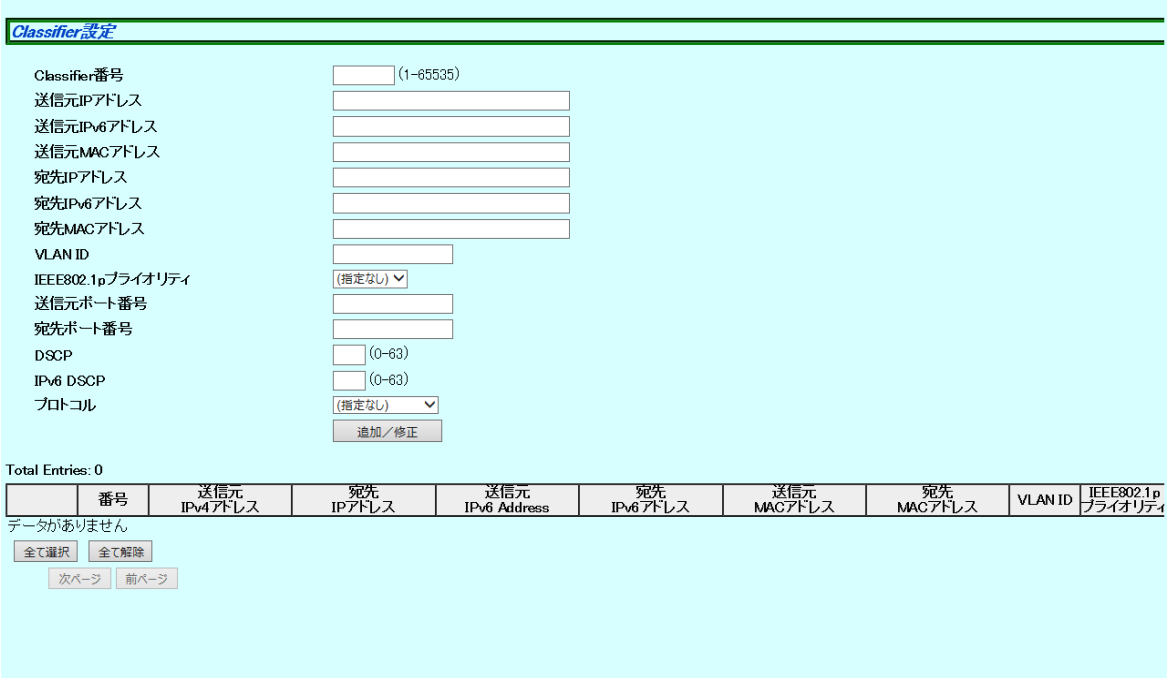


図 3-54 Classifier 設定

画面の説明

Classifier 番号	Classifier の Index 番号を表示します。
Total Entry	作成されている Classifier のエントリ数を表示します。
番号	Classifier の Index 番号を表示します。
送信元 IP アドレス	送信元 IP アドレスを表示します。
宛先 IP アドレス	宛先 IP アドレスを表示します。
送信元IPv6アドレス	送信元 IPv6 アドレスを表示します。
宛先IPv6アドレス	宛先 IPv6 アドレスを表示します。
送信元 MAC アドレス	送信元 MAC アドレスを表示します。
宛先 MAC アドレス	宛先 MAC アドレスを表示します。
VLAN ID	VLAN ID を表示します。
IEEE802.1q プライオリティ	IEEE802.1p のプライオリティを表示します。
送信元ポート番号	TCP/UDP 送信元ポート番号を表示します。
宛先ポート番号	TCP/UDP 宛先ポート番号を表示します。
DSCP	DSCP 値を表示します。
IPv6 DSCP	IPv6 DSCP 値を表示します。
プロトコル	プロトコルの種類を表示します。
TCP SYN フラグ	TCP での SYN フラグのフィルタの有無を表示します。
ICMP タイプ	ICMP のタイプを表示します。

3.2.29. インプロファイルアクション設定 (In-Profile Action Config)

[拡張機能設定] から [アクセスコントロール設定]、[インプロファイルアクション設定] の順に選択すると、図 3-55 のような画面が表示されます。この画面ではインプロファイルの設定を行います。

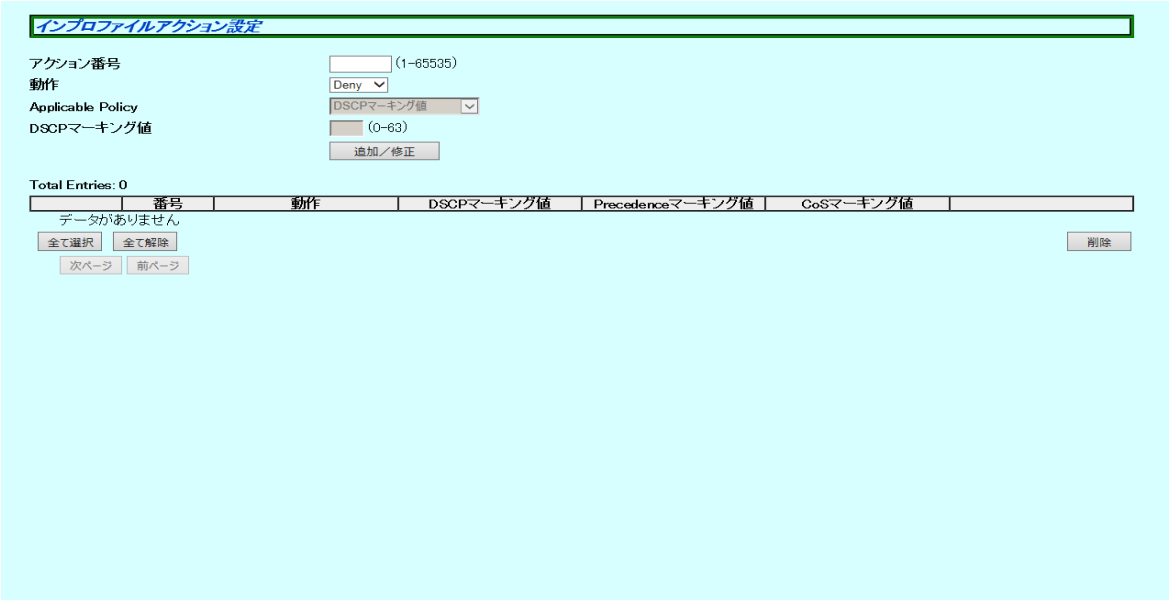


図 3-55 インプロファイルアクション設定

画面の説明

Total Entry	作成されている In-profile の数 (index の数) を表示します。	
アクション番号	In-profile の Index 番号を表示します。	
動作	パケットの拒否 / 許可を表示します。	
	Deny	拒否
	Permit	許可
DSCP マーキング値	DSCP 値をマーキングします。	
Precedence マーキング値	Precedence 値をマーキングします。	
CoS マーキング値	CoS 値をマーキングします。	

3.2.30. アウトプロファイルアクション設定

[拡張機能設定] から [アクセスコントロール設定]、[アウトプロファイルアクション設定] の順に選択すると、**図 3-56** のような画面が表示されます。この画面ではアウトプロファイルの設定を行います。

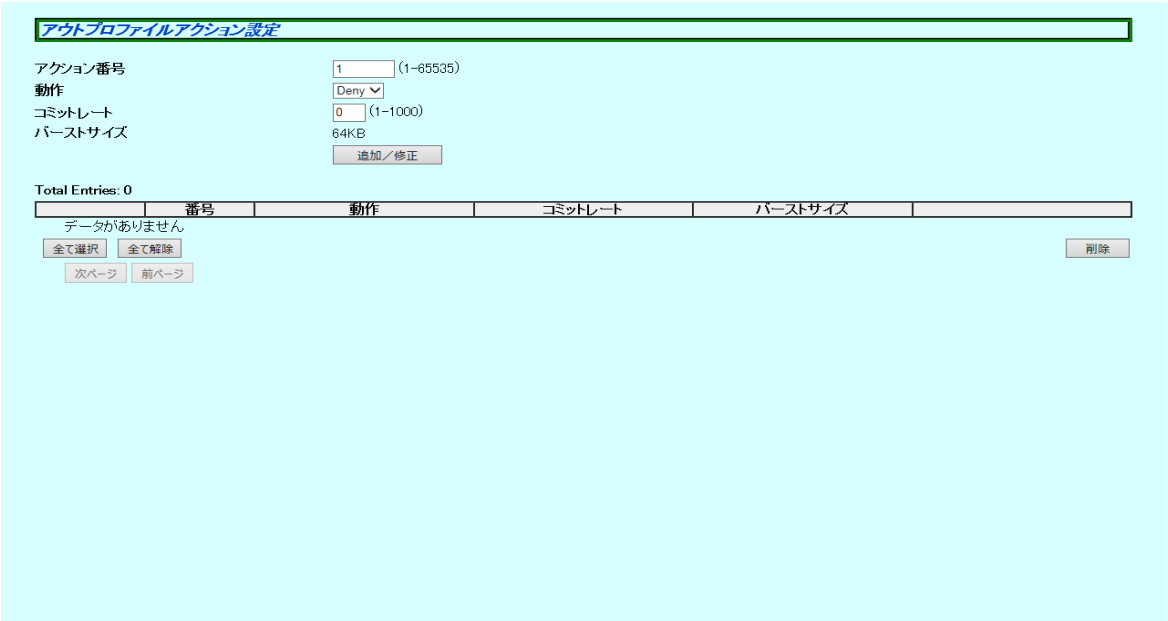


図 3-56 アウトプロファイルアクション設定

画面の説明

Total Entry	作成されている Out-profile の数 (index の数) を表示します。	
アクション番号	Out-profile の Index 番号を表示します。	
動作	パケットの拒否 / 許可を表示します。	
	Deny	拒否
コミットレート	パケットがバッファに入る速度を表示します。	
バーストサイズ	コミットレートを超えて送ることができるトラフィックのバーストサイズを表示します。バーストサイズ 64KB が使用されます。	

3.2.31. ポートリスト設定

[拡張機能設定] から [アクセスコントロール設定]、[ポートリスト設定] の順に選択すると、図 3-57 のような画面が表示されます。この画面ではアクセスコントロールの対象とするポートリストの設定を行います。
アクセスコントロール機能とリンクアグリゲーション機能を併用する場合は、リンクアグリゲーションで作成された論理ポートではなく、実際の物理ポート番号を指定してください。

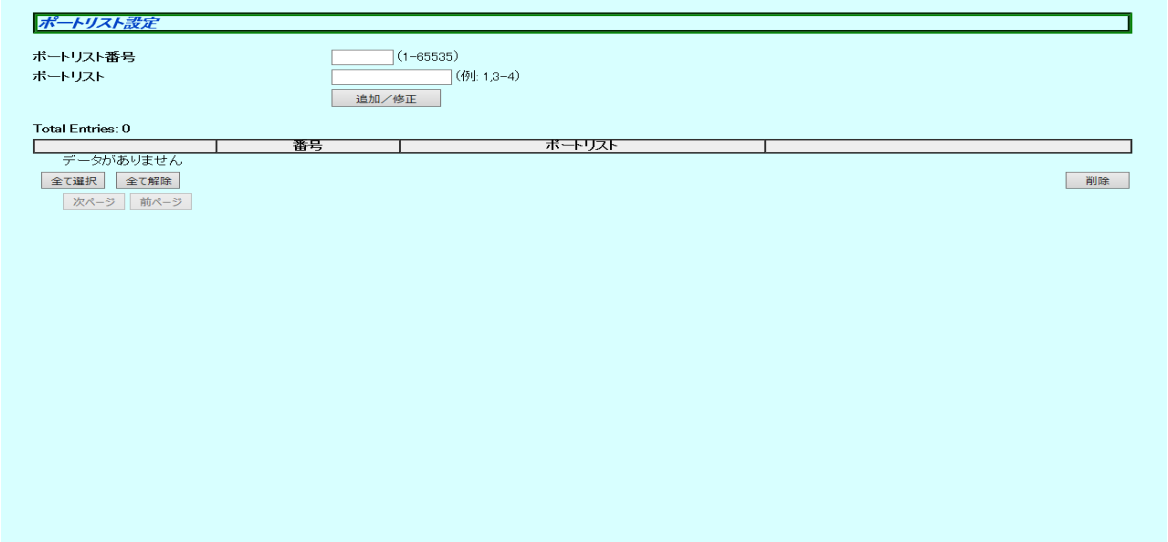


図 3-57 ポートリスト設定

画面の説明

Total Entry	作成されているポートリストの数 (index の数) を表示します。
ポートリスト番号	ポートリストの Index 番号を表示します。
番号	ポートリストの Index 番号を表示します。
ポートリスト	ポートリストに属するポート番号を表示します。

3.2.32. ポリシー設定

[拡張機能設定] から [アクセスコントロール設定]、[ポリシー設定] の順に選択すると、**図 3-58** のような画面が表示されます。この画面では IPv4 のポリシーの設定を行います。

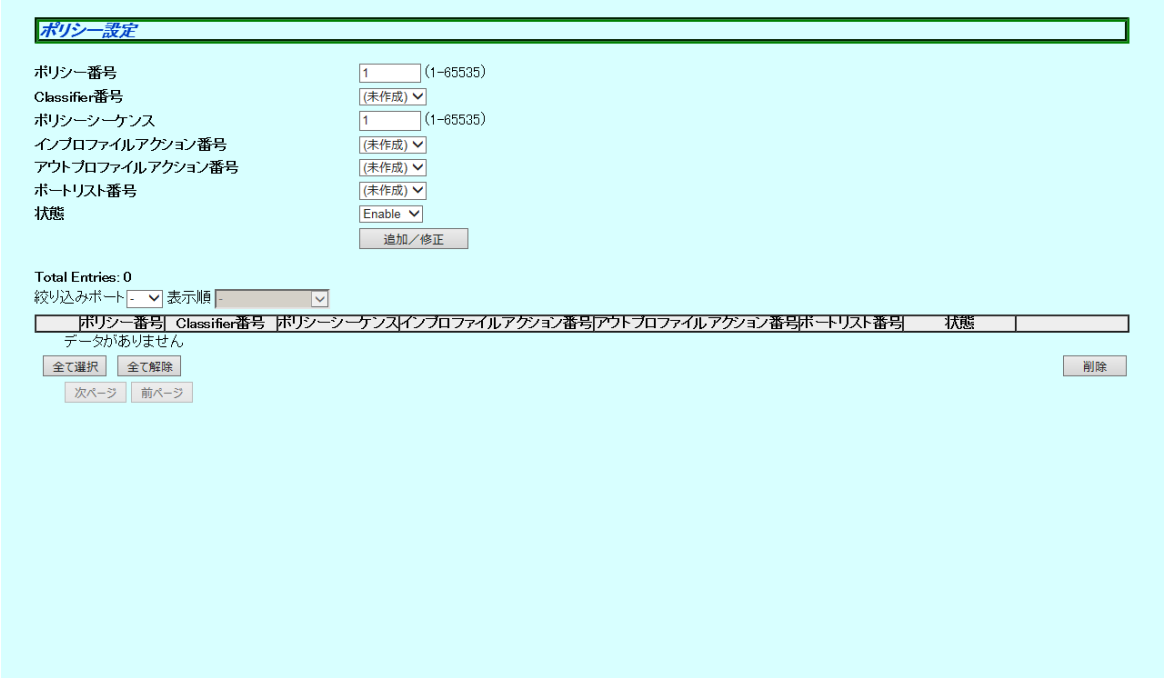


図 3-58 ポリシー設定 (IPv4)

画面の説明

ポリシー優先度	ポリシーの優先度を表示します。優先度は 1,2 の値が使用されます。
Total Entry	作成されているポリシーの数 (index の数) を表示します。
ポリシー番号	ポリシーの Index 番号を表示します。
Classifier 番号	Classifier の Index 番号を表示します。
ポリシーシーケンス	ポリシーの適用順を表すシーケンス番号を表示します。値の小さいポリシーから適用されます。
インプロファイルアクション番号	In-profile の Index 番号を表示します。
アウトプロファイルアクション番号	Out-profile の Index 番号を表示します。
ポートリスト番号	ポートリストの Index 番号を表示します。
状態	ポリシーの適用状態を表示します。

3.2.33. ループ検知・遮断設定

[拡張機能設定] から [ループ検知・遮断設定]、[ループ検知・遮断設定] の順に選択すると、**図 3-59** のような画面が表示されます。この画面では、ループ検知・遮断機能の設定を行います。

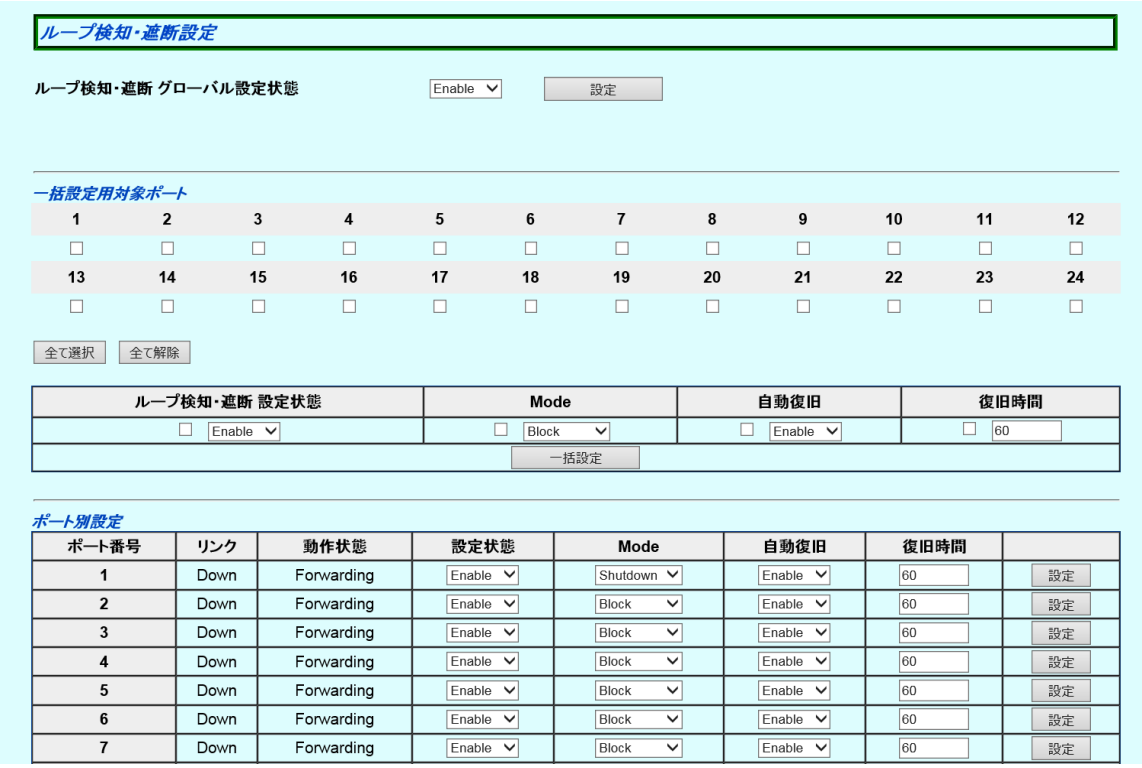


図 3-59 ループ検知・遮断設定

画面の説明

ループ検知・遮断 グローバル設定状態	ループ検知・遮断機能の状態が表示されます。	
	Enable	ループ検知・遮断機能を有効にします。
	Disable	ループ検知・遮断機能を無効にします。
一括設定用 対象ポート	複数のポートに対して一括設定を行う際の対象ポートを選択します。 [全て選択] ボタンをクリックすると、全ポートが選択されます。 [全て解除] ボタンをクリックすると、全ポートが選択解除されます。 一括設定用項目を選択・変更後、[一括設定] ボタンをクリックすると、選択中のポートに対して同一の設定が反映されます。	
ポート番号	ポート番号が表示されます。	
リンク	リンクの状態が表示されます。	
	Up	リンクが正常に確立している状態です。
	Down	リンクが確立されていない状態です。
動作状態	該当ポートにおけるループ検知・遮断機能の動作状態が表示されます。	
	Forwarding	パケットが正常に転送されています。
	Loop Detect	ループが検知され、ポートが遮断されています。
設定状態	該当ポートに対するループ検知・遮断機能の設定状態が表示されます。	
	Enable	ループ検知・遮断機能が有効です。(ダウンリンクポートの工場出荷時設定)
	Disable	ループ検知・遮断機能が無効です。(アップリンクポートの工場出荷時設定)

Mode	該当ポートに対するポートが遮断されたときの動作モードを切り替えます。	
	Block	ループを検知したとき、ポートをブロックします。 (工場出荷時設定)
	Shutdown	ループを検知したとき、ポートをシャットダウンします。
自動復旧	ポートが遮断されたときの自動復旧の有効・無効を切り替えます。	
	Enable	[復旧時間] で設定された時間が経過後にポートの遮断を自動復旧します。 (工場出荷時設定)
	Disable	手動で設定するまでポートの遮断を復旧しません。
復旧時間	ポートが遮断されたときに自動復旧が行われるまでの時間を入力します。 工場出荷時は 60 秒に設定されています。	

3.2.34. ループヒストリー情報

[拡張機能設定] から [ループ検知・遮断設定]、[ループヒストリー情報] の順に選択すると、**図 3-60** のような画面が表示されます。この画面では、ループを検知・遮断した日時およびイベント情報の一覧を表示します。

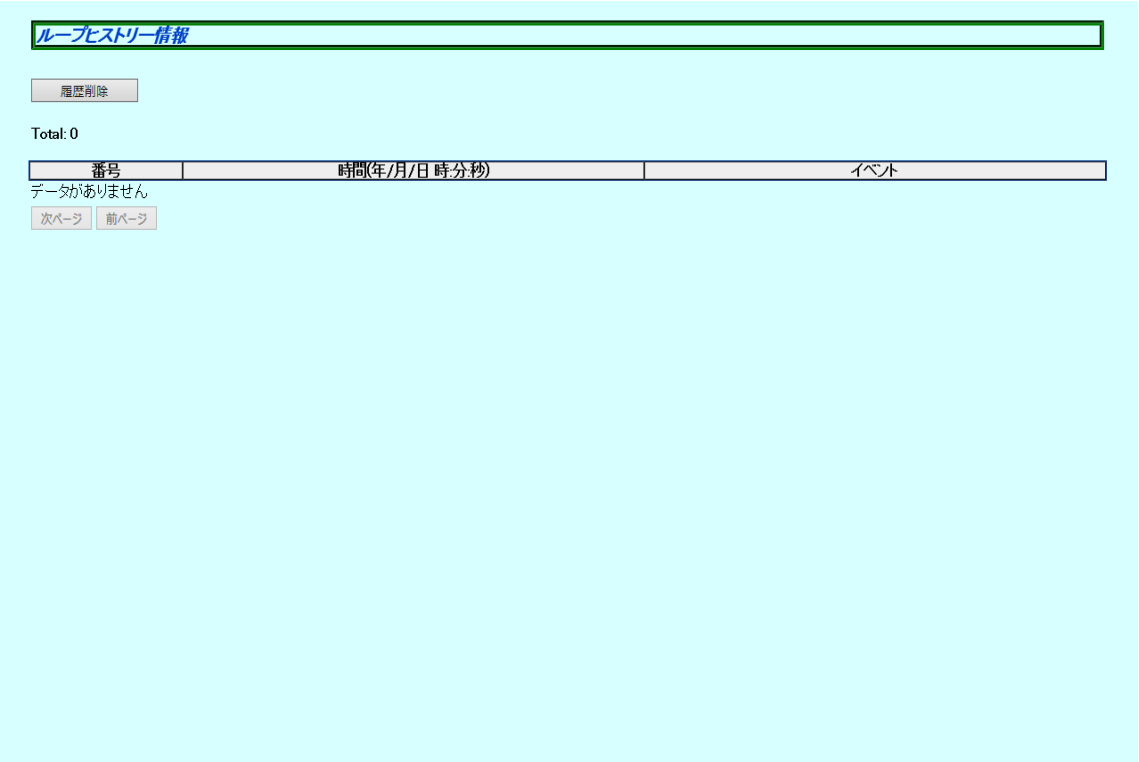


図 3-60 ループヒストリー情報

画面の説明

履歴削除	保存されているループヒストリー情報を削除します。	
番号	ループ検知・遮断のイベント番号が表示されます。	
時刻	ループ検知・遮断イベントの発生した時刻が表示されます。	
イベント	ループ検知・遮断イベントの説明が表示されます。	
	The loop detected on portX.	表示されているポート配下のスイッチでループが発生したことを示します。
	The loop detected between portX and portY.	表示されているポート間でループが発生したことを示します。
	PortX auto recovery.	ループ検知・遮断後に自動復旧が実施されたことを示します。
次ページ	一覧の表示範囲が切り替わります。	
前ページ		

3.2.35. PPS 設定

PPS（Power to Progress SDN）は、ネットワークを構成する複数の装置を一つのソフトウェアで管理し、運用や設定を容易にするための機能です。この機能を用いることで、PPS アプリケーション（別売）から本装置を制御することが可能となります。PPS アプリケーション（別売）から管理できる内容については、PPS アプリケーションの取扱説明書をご参照ください。

[拡張機能設定] から [PPS]、[PPS 設定] の順に選択すると、図 3-61 のような画面が表示されます。この画面では、PPS の状態表示および設定を行います。

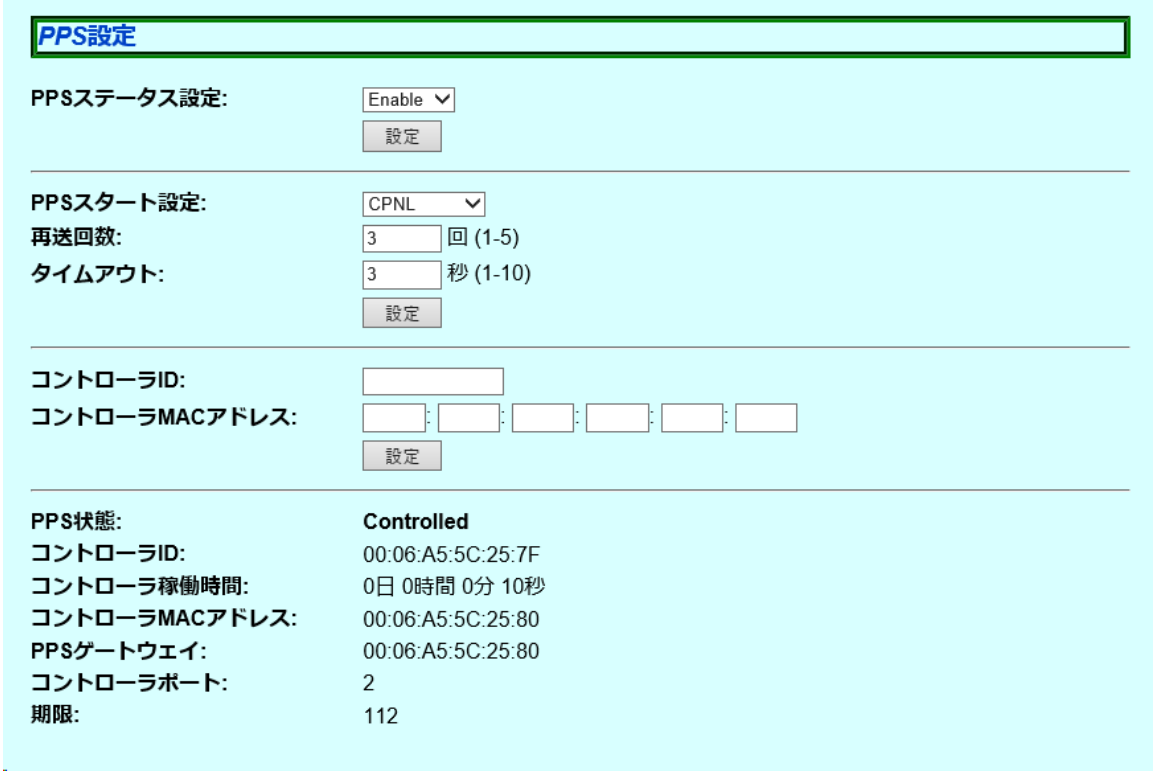


図 3-61 PPS 設定

画面の説明

PPS ステータス設定	PPS の設定状態が表示されます。	
	Enable	PPS が有効です。（工場出荷時設定）
	Disable	PPS が無効です。
	Restart	機器のステータスを Stand Alonen にし、PPSP 機能を再始動します。
PPS スタート状態	PPS の初期動作状態が表示されます。	
	Stand Alone	PPS コントローラに管理されていない状態です。
	CPNL	Controller Port Neightbor Lost 状態になり、コントローラを認識しているが、通信不可な状態になります。 コントローラ ID が存在しない場合は、CPNL を選択しても Stand Alone 状態になります。
再送回数	生存確認を行うパケットの再送回数を設定します。再送回数は 1 ～ 5 回の範囲で指定します。工場出荷時は 3 回に設定されています。	
タイムアウト	生存確認のパケットに対する応答のタイムアウト値を設定します。タイムアウト値は 1 ～ 10 秒の範囲で設定します。工場出荷時は 5 秒に設定されています。	

PPS 状態	現在の PPS の動作状態が表示されます。	
	Stand Alone	PPS コントローラに管理されていない状態です。
	CPNL	Controller Port Neightbor Lost 状態になり、コントローラを認識しているが、通信不可な状態になります。
	Controlled	スイッチングハブがコントローラを認識し、コントローラと通信可能な状態です。
コントローラ ID	PPS コントローラの ID が表示されます。	
コントローラ稼働時間	PPS コントローラの起動からの稼働時間が表示されます。	
コントローラ MAC アドレス	PPS コントローラの MAC アドレスが表示されます。	
PPS ゲートウェイ	PPS ゲートウェイの MAC アドレスが表示されます。	
コントローラポート	PPS コントローラとの通信に利用するポート番号が表示されます。	
期限	コントローラの登録情報が削除されるまでの時間です。工場出荷時は 120 秒に設定されています。	

ご注意： 起動後、Standalone の状態で 1 時間経過すると自動的に PPSP 機能を停止します。
1 時間経過後、PPS コントローラを認識させるには機器の PPSP 機能を再起動、または機器の再起動を行ってください。

ご注意： 本機能を無効にした場合、PPS コントローラから管理できる内容が制限されます。

ご注意： 多拠点の機器（IP セグメントを超えた機器）への設定変更等をする場合は PPSP に対応した当社製レイヤ 3 スイッチングハブにて仮想リンク転送先 IP アドレスの設定が必要です。

3.2.36. PPS 通知設定

[拡張機能設定] から [PPS 設定]、[PPS 通知設定] の順に選択すると、図 3-62 のような画面が表 示されます。この画面では、PPS の通知設定を行います

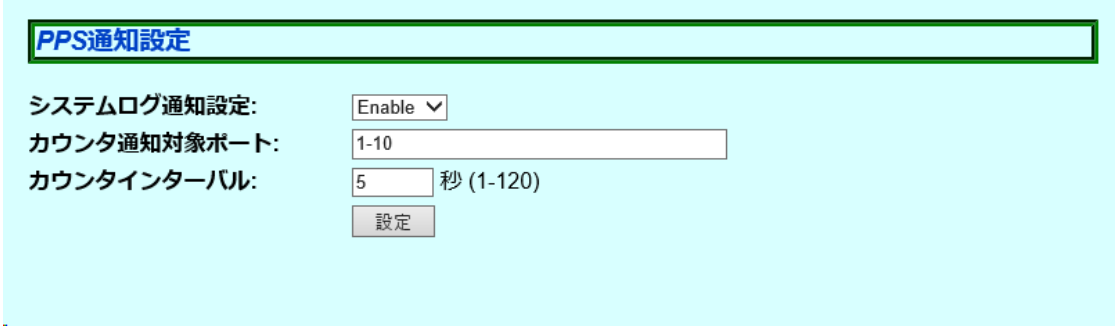


図 3-62 PPS 通知設定

画面の説明

システムログ通知設定	システムログ通知設定の設定状態を設定します。	
	Enable	システムログ通知設定が有効です。
	Disable	システムログ通知設定が無効です。
カウンタログ通知対象ポート	カウンタログ通知対象ポート設定します。	
カウンターインターバル	PPS パケット統計情報通知間隔を設定します。	

3.2.37. PPS ポート設定

[拡張機能設定] から [PPS 設定]、[PPS ポート設定] の順に選択すると、図 4-2-20 のような画面が表 示されます。この画面では、PPS のポート設定を行います

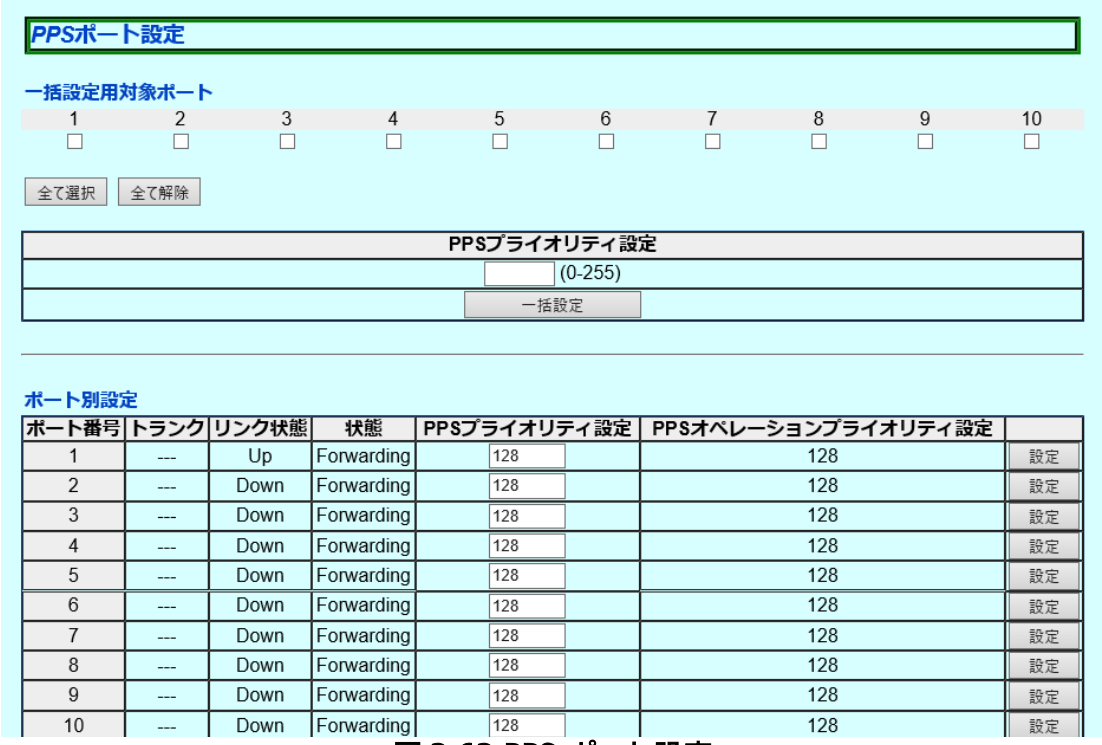


図 3-63 PPS ポート設定

画面の説明

一括設定用対象ポート	一括設定用対象ポートを設定します。チェックボックスにチェックを入れることで一括設定用対象ポートに設定します。	
プライオリティ設定	本スイッチのプライオリティを一括で設定します。	
ポート別設定	ポート番号	スイッチングハブのポート番号が表示されます。
	トランク	トランキングの設定状態をグループ番号で表示します。
	リンク状態	リンク状態を Up/Down で表示します。
	状態	各ポートの通信状態を表示されます。
	PPS プライオリティ設定	各ポートごとに設定された PPS の通信経路の自動判別に用いる優先度が表示されます。設定する優先度を 0 から 255 の範囲で入力してください。値が大きい程、優先度は高くなります。工場出荷時は 128 が設定されています。
	PPS オペレーションプライオリティ設定	各ポートごとに割り当てられた PPS の通信経路の自動判別のための優先度が表示されます。

3.2.38. PPS ネイバー設定

[拡張機能設定] から [PPS 設定]、[PPS ネイバー設定] の順に選択すると、図 3-64 のような画面が表示されます。この画面では、PPS ネイバーテーブルの参照・設定を行います。

図 3-64 PPS ネイバーテーブル

画面の説明

PPS ネイバー エージングタイム	PPS 近接装置のエントリ保有時間を設定します。設定した保有時間を超えて通信のないエントリはテーブルから削除されます。値は 60 ～ 86400 秒の範囲で設定します。工場出荷時は 60 秒に設定されています。	
MAC アドレス	PPS 近接装置 の MAC アドレスが表示されます。	
ポート番号	PPS 近接装置との通信に利用するポート番号が表示されます。	
期限	PPS 近接装置の登録情報が削除されるまでの時間を秒単位で表示します。	
詳細表示	[詳細表示] を選択することで図 3-65 のような PPS 近接装置の詳細情報が表示されます。	
	製品名	PPS 近接装置の製品名が表示されます。
	品番	PPS 近接装置の品番が表示されます。
	シリアル ナンバー	PPS 近接装置のシリアルナンバーが表示されます。PPS 近接装置がシリアルナンバー表示に対応している必要があります。
	MAC アドレス	PPS 近接装置の MAC アドレスが表示されます。
	送信元ポート	PPS 近接装置で通信に使用されているポート番号が表示されます。
	IP アドレス	PPS 近接装置の IP アドレスが表示されます。
	ホスト名	PPS 近接装置のホスト名が表示されます。
削除	削除対象エントリを選択し、[削除] ボタンをクリックすると、PPS ネイバーテーブルから 削除されます。	
次ページ	一覧の表示範囲が次ページに切り替わります。	
前ページ	一覧の表示範囲が前ページに切り替わります。	

PPSネイバーデバイス情報

製品名:	PPS
品番:	PPSController
シリアルナンバー:	Not support
MACアドレス:	00:06:A5:5C:29:09
送信元ポート:	1
IPアドレス:	172.16.222.15
ホスト名:	PPSController

図 3-65 PPS ネイバーデバイス情報

3.2.39. PPS コネクション設定

[拡張機能設定] から [PPS 設定] 、[PPS コネクション設定] の順に選択すると、図 3-66 のような画面が表示されます。この画面では、PPS コネクションテーブルの参照・設定を行います。テーブルに従って対象の機器へパケットを送信します。

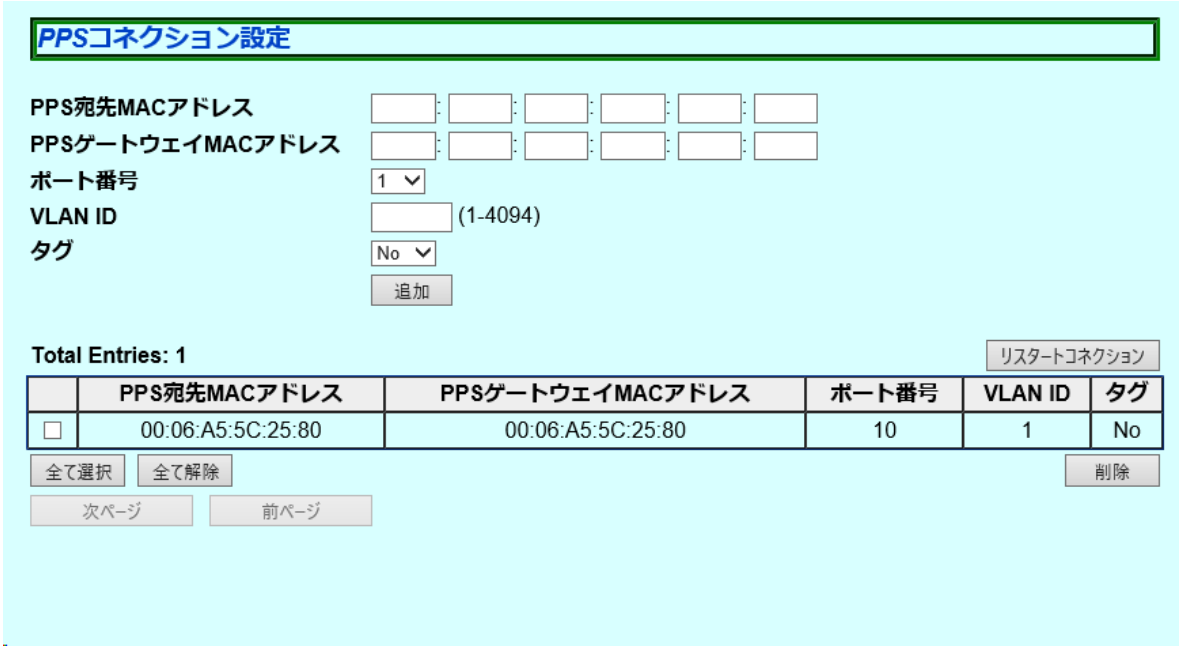


図 3-66 PPS コネクションテーブル

画面の説明

PPS 宛先 MAC アドレス	PPS コネクションテーブルに追加する宛先 MAC アドレスを入力します。
PPS ゲートウェイ MAC アドレス	PPS コネクションテーブルに追加するゲートウェイ MAC アドレスを入力します。
ポート番号	PPS コネクションテーブルに追加する機器のポートを 1 ～ 24 から選択します。
VLAN ID	追加するコネクションの VLAN ID を入力します。
タグ	ゲートウェイに送信するパケットにタグをつける設定をします。Yes か No を選択します。
追加	上記で設定したコネクションを PPS コネクションテーブルに追加します。
リスタート コネクション	PPS コネクションテーブルを再表示します。
削除	削除対象エントリを選択し、[削除] ボタンをクリックすると、PPS コネクションテーブルから 削除されます。
次ページ	一覧の表示範囲が次ページに切り替わります。
前ページ	一覧の表示範囲が前ページに切り替わります。

3.2.40. ポートグルーピング設定

[拡張機能設定] から [ポートグルーピング設定] を選択すると、図 3-68 のような画面が表示されます。この画面ではポートグルーピングの設定を行うことができます。ポートグルーピングを設定すると、ポートグループのメンバーに指定されたポートは、同じグループのメンバーポートとのみ通信が可能となります。各ポートは複数のポートグループに割り当てることが可能です。ポートグルーピングを利用した構成例を図 3-67 に示します。

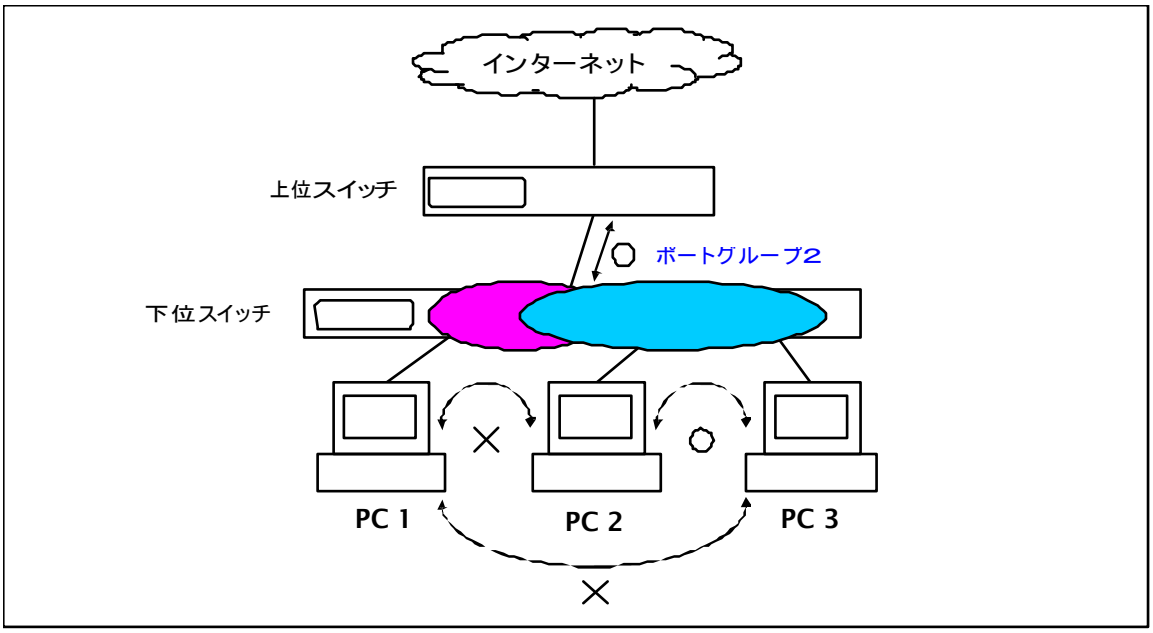


図 3-67 ポートグルーピングを利用した構成例

(PC1— インターネット間、PC2—PC3— インターネット間を通信可能とさせる構成)

ご注意： ループ検知・遮断機能は異なるポートグループ間であってもフレームのループ検知及び遮断を行います。
２つ以上のポートグループに対してリンクアグリゲーションのトランクポートを跨るように設定した場合は、正常にフレームが転送されない場合があります。

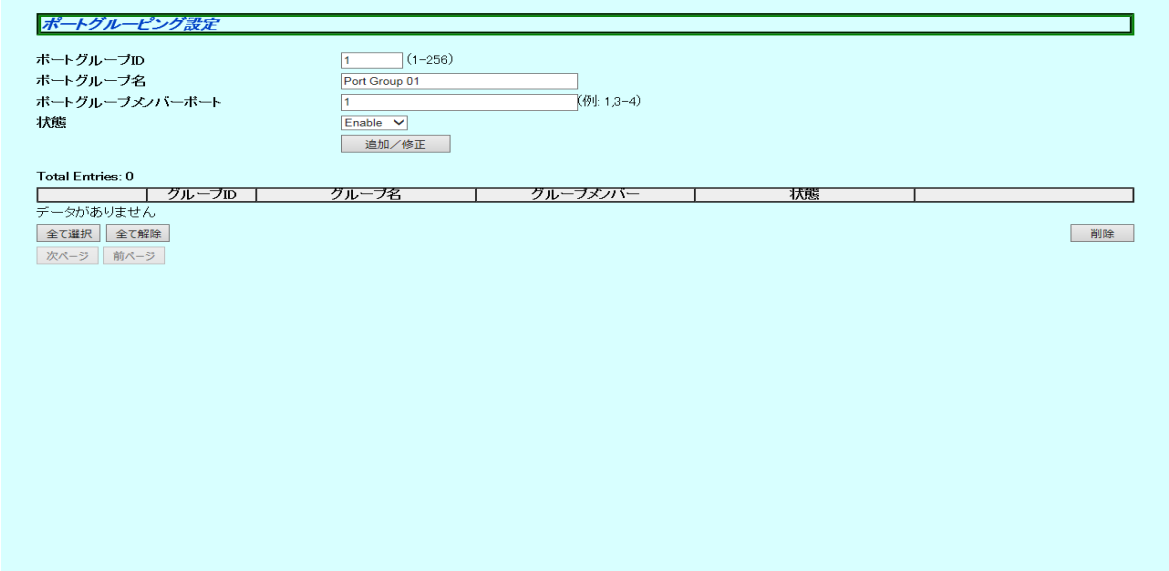


図 3-68 ポートグルーピング設定

画面の説明

ポートグループ ID	ポートグループの ID を表示します。
ポートグループ名	設定されているポートグループの名称を表示します。
ポートグループメンバーポート	ポートグループに所属するメンバーポートを表示します。
Total Entry	作成されているポートグループの数 (index の数) を表示します。
グループ ID	ポートグループの ID を表示します。
グループ名	設定されているポートグループの名称を表示します。
グループメンバー	ポートグループに所属するメンバーポートを表示します。
状態	ポートグループの状態を表示します。

3.2.41. SFP モジュール状態確認（DDM）設定

[拡張機能設定] から [SFP モジュール状態確認 (DDM) 設定] を選択すると、図 3-69 のような画面が表示されます。この画面では、SFP モジュール状態確認（DDM：Digital Diagnostic Monitoring）の設定を行います。

図 3-69 SFP モジュール状態確認（DDM）設定

画面の説明

上下限超過時 Trap 送出	SFP モジュールの状態が設定された閾値を超えた場合に、SNMP トラップを送出するかどうかを設定します。	
	Enable	SNMP トラップを送出します。
	Disable	SNMP トラップを送出しません。
状態確認対象 SFP ポート選択	状態確認を行う SFP ポートを選択します。	
ポート番号	ポート番号が表示されます。	
メーカ名	SFP モジュールのメーカ名が表示されます。	
品番	SFP モジュールの品番が表示されます。	
シリアル番号	SFP モジュールのシリアル番号が表示されます。	
SFP 種別	SFP モジュール種別が表示されます。	
現在の状態	SFP モジュールの現在の状態が表示されます。 [更新] ボタンをクリックすると、最新の状態に更新されます。	
	受信光パワー (dBM)	受信光パワーが表示されます。
	送信光パワー (dBM)	送信光パワーが表示されます。
	温度（℃）	温度が表示されます。
	動作電圧（V）	動作電圧が表示されます。
	動作電圧 (mA)	動作電流が表示されます。

アラーム上限閾値	各状態確認項目に対して、アラームおよび警告が発生する上限・下限閾値を設定します。「999」を設定すると、閾値が自動的に決められます。
警告上限閾値	
アラーム下限閾値	
警告下限閾値	

3.2.42. マルチキャストグループの設定

[拡張機能設定] から [マルチキャストグループ設定]、[マルチキャストグループ設定] の順に選択すると、**図 3-70** のような画面が表示されます。この画面では、マルチキャストグループの設定を行います。

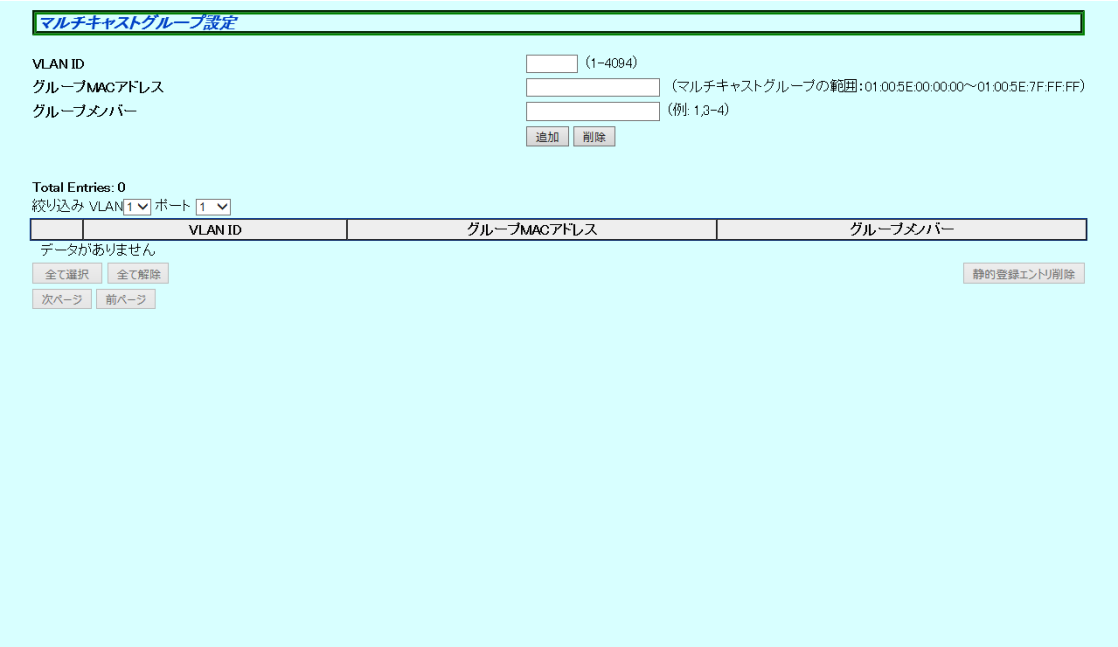


図 3-70 マルチキャストグループの設定

画面の説明

VLAN ID	マルチキャストグループの VLAN ID が表示されます。
グループ MAC アドレス	マルチキャストグループの MAC アドレスが表示されます。
グループメンバー	マルチキャストグループに含まれるポートが表示されます。

3.3.　システム管理ツール

3.3.1.　ファームウェア更新

[システム管理ツール] から [ファームウェア更新] を選択すると、図 3-71 のような画面が表示されます。この画面では、ファームウェアの更新を行います。

図 3-71 ファームウェア更新

画面の説明

現在のファームウェア情報	現在のファームウェアのバージョンが表示されます。
TFTP サーバ IP アドレス	更新するファームウェアの保存されている TFTP サーバの IP アドレスが表示されます。
ファイル名	更新するファームウェアのファイル名が表示されます。

ご注意：ファームウェアの更新前に、3.3.3 項に従って設定情報を保存する必要があります。設定情報を保存しなければ、再起動時にこれまでの設定が削除されます。

[実行] ボタンをクリックすると、図 3-72 のような画面が表示され、ファームウェアデータの転送が開始されます。転送を中断するには [ダウンロード中止] ボタンをクリックします。

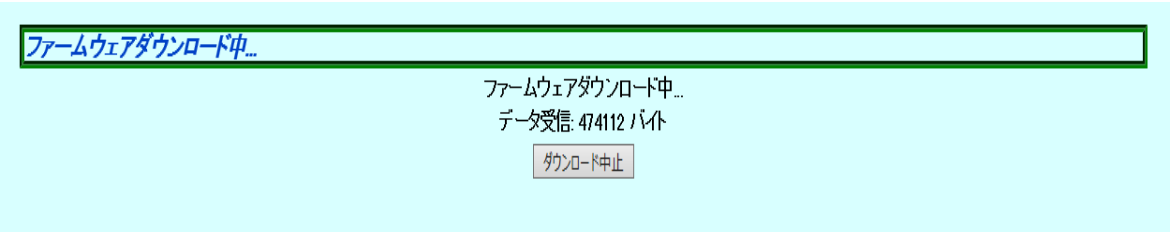


図 3-72 ファームウェアデータ転送中

転送が完了すると、図 3-73 のような画面が表示され、ファームウェアデータの書き換えが行われます。

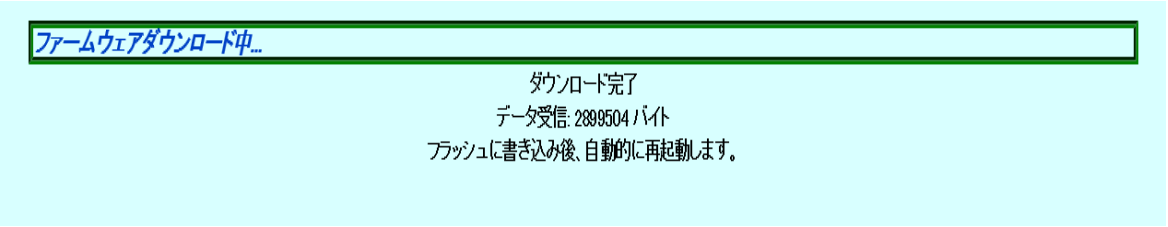


図 3-73 ファームウェアデータ書き換え中

書き換えが完了すると、この装置は自動的に再起動します。

3.3.2.　再起動

[システム管理ツール] から [再起動] を選択すると、図 3-74 のような画面が表示されます。この画面では、この装置の再起動を行うことができます。

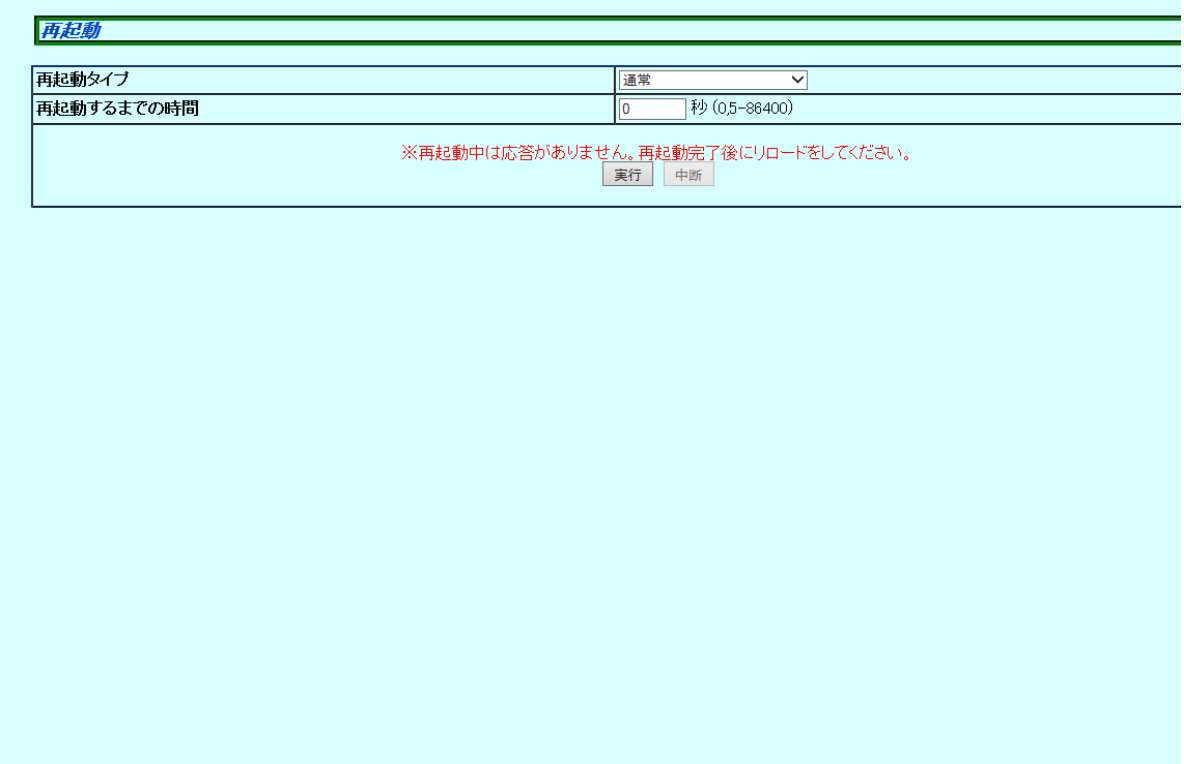


図 3-74 再起動

画面の説明

再起動タイプ	再起動の方法が表示されます。工場出荷時は「通常」に設定されています。	
	通常	通常の再起動が実行されます。
	設定初期化	全ての設定が工場出荷時の状態に戻ります。
	IP アドレス以外の設定初期化	IP アドレスの設定以外が工場出荷時の状態に戻ります。
再起動するまでの時間	再起動の実行から実際に再起動するまでの時間が表示されます。 工場出荷時は 0 秒に設定されています。	

ご注意： 再起動の進行中には、応答はありません。再起動完了後に設定を再読み込みします。

[実行] ボタンをクリックすると、図 3-75 のような画面が表示され、再起動が開始されます。

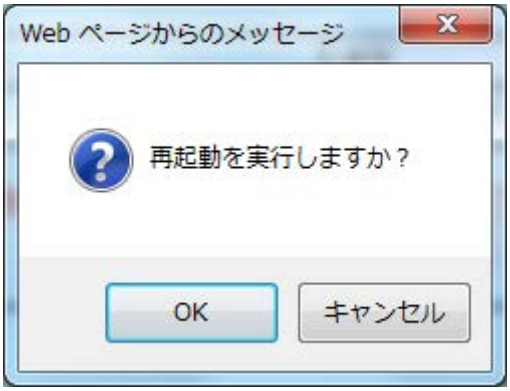


図 3-75 再起動中

再起動が完了すると、[再読み込み] ボタンが有効になりますので、クリックして画面の再読み込みを行ってください。

3.3.3.　設定情報保存

[システム管理ツール] から [設定情報保存] を選択すると、図 3-76 のような画面が表示されます。この画面では、設定情報を保存します。

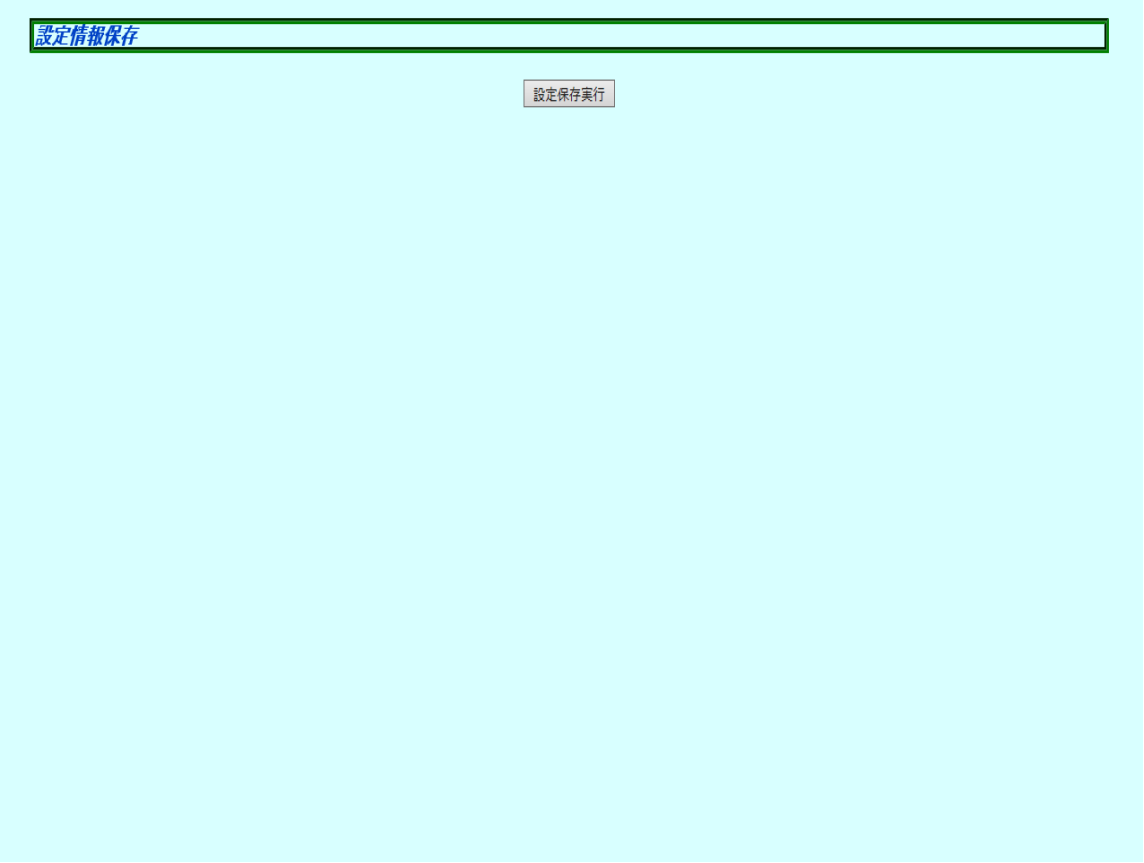


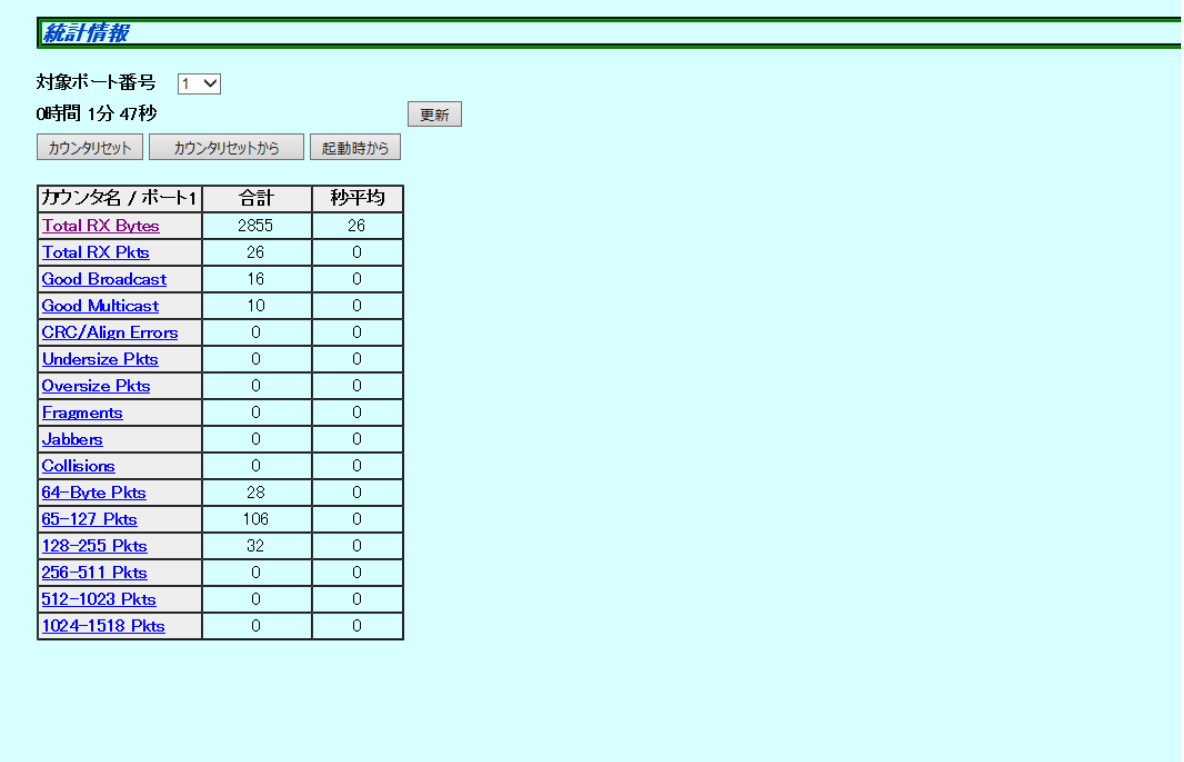
図 3-76 設定情報保存

[設定保存実] をクリックして、この装置の設定を内蔵のメモリに保存します。設定情報を保存しない限り、再起動後にこれまでの設定が反映されません。

保存が完了すると、メッセージ「**設定の保存に成功しました。**」が表示されます。

3.3.4. 統計情報の表示 (Statistics)

[システム管理ツール] から [統計情報] を選択すると、図 3-77 のような画面が表示されます。この画面では、統計情報を確認できます。



カウンタ名 / ポート1	合計	秒平均
Total RX Bytes	2855	26
Total RX Pkts	26	0
Good Broadcast	16	0
Good Multicast	10	0
CRC/Align Errors	0	0
Undersize Pkts	0	0
Oversize Pkts	0	0
Fragments	0	0
Jabbers	0	0
Collisions	0	0
64-Byte Pkts	28	0
65-127 Pkts	106	0
128-255 Pkts	32	0
256-511 Pkts	0	0
512-1023 Pkts	0	0
1024-1518 Pkts	0	0

図 3-77 統計情報

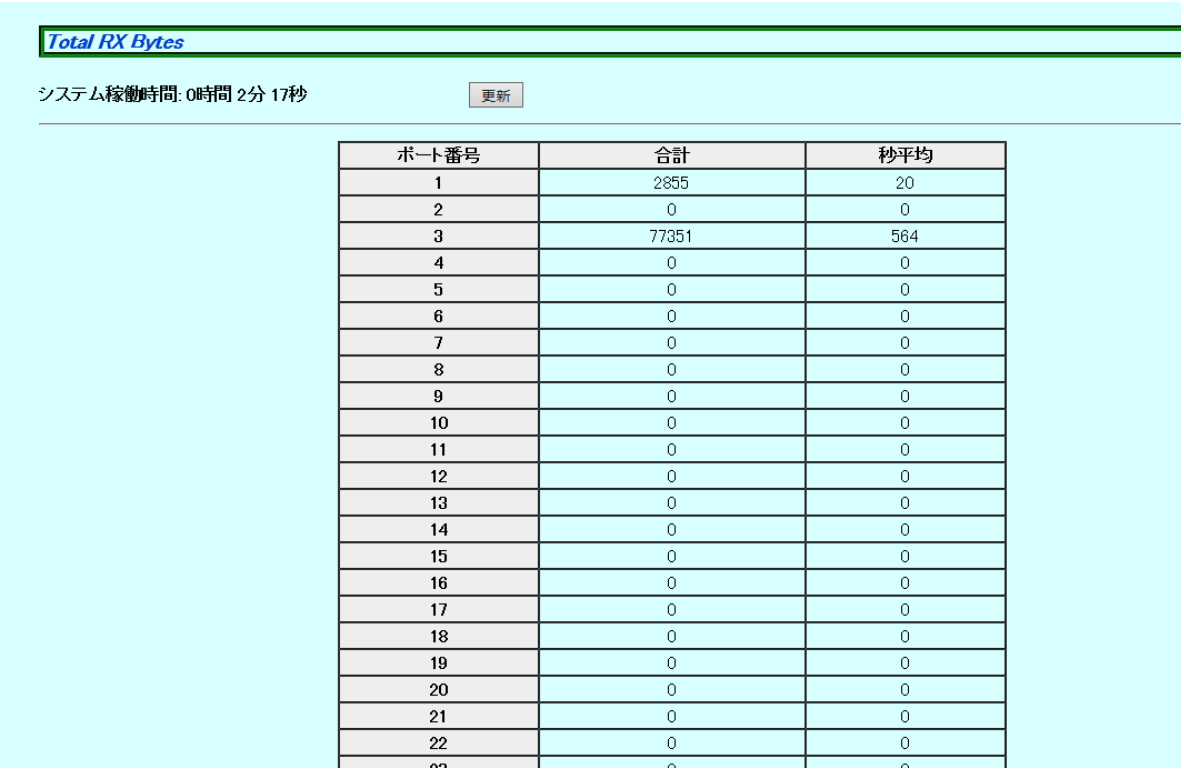
画面の説明

対象ポート番号	表示対象のポート番号を選択します。
経過時間	この装置が起動またはカウンタがリセットされてからの経過時間が表示されます。 [更新] ボタンをクリックすると、経過時間およびカウンタ値の表示が更新されます。
カウンタリセット	各カウンタ値のリセットを行い、カウンタがリセットされてからの経過時間が0に戻ります。 (起動されてからの経過時間およびカウンタ値はリセットされません)
カウンタリセットから	カウンタがリセットされてからの経過時間およびカウンタ値の表示に切り替わります。
起動時から	起動されてからの経過時間およびカウンタ値の表示に切り替わります。
カウンタ名	カウンタ名が表示されます。
合計	カウンタの値が表示されます。
秒平均	秒あたりのカウンタの平均値が表示されます。

カウンタの値を以下に示します。

Total RX Bytes	受信した全てのパケットのバイト数が表示されます。
Total RX Pkts	受信した全てのパケット数が表示されます。
Good Broadcast	受信したブロードキャストパケット数が表示されます。
Good Multicast	受信したマルチキャストパケット数が表示されます。
CRC/Align Errors	エラーパケットで正常なパケット長 (64 ～ 1518 バイト) ではあるが、誤り検出符号（FCS）で誤りが発見されたパケット数が表示されます。そのうちパケットの長さが 1 バイトの整数倍のものは CRC（FCS）エラー、そうでないものはアラインメントエラーです。
Undersize Pkts	エラーパケットで、パケット長が 64 バイトより短いが、その他には異常がないパケット数が表示されます。
Oversize Pkts	< ジャンボフレームが無効な場合 > パケット長が 1518 バイトより長いパケット数が表示されます。 < ジャンボフレームが有効な場合 > パケット長が 9216 バイトより長いパケット数が表示されます。
Fragments	エラーパケットでパケット長が 64 バイトより短く、かつ CRC エラーまたはアラインメントエラーを起こしているパケット数が表示されます。
Jabbers	エラーパケットでパケット長が 1518 バイトより短く、かつ CRC エラーまたはアラインメントエラーを起こしているパケット数が表示されます。
Collisions	パケットの衝突の発生した回数が表示されます。
64-Byte Pkts	パケット長が 64 バイトのパケットの総数が表示されます。
65-127 Pkts	パケット長が 65 ～ 127 バイトのパケットの総数が表示されます。
128-255 Pkts	パケット長が 128 ～ 255 バイトのパケットの総数が表示されます。
256-511 Pkts	パケット長が 256 ～ 511 バイトのパケットの総数が表示されます。
512-1023 Pkts	パケット長が 512 ～ 1023 バイトのパケットの総数が表示されます。
1024-1518 Pkts	パケット長が 1024 ～ 1518 バイトのパケットの総数が表示されます。

カウンタ名をクリックすると、図 3-78 のような画面が表示されます。この画面には、カウンタの総数および秒あたりの平均数がポート別に表示されます。



Total RX Bytes

システム稼働時間: 0時間 2分 17秒　更新

ポート番号	合計	秒平均
1	2855	20
2	0	0
3	77351	564
4	0	0
5	0	0
6	0	0
7	0	0
8	0	0
9	0	0
10	0	0
11	0	0
12	0	0
13	0	0
14	0	0
15	0	0
16	0	0
17	0	0
18	0	0
19	0	0
20	0	0
21	0	0
22	0	0

図 3-78 ポート別のカウンタ統計情報

画面の説明

システム稼働時間	この装置が起動されてからの経過時間が表示されます。 [更新] ボタンをクリックすると、経過時間およびカウンタ値の表示が更新されます。
ポート番号	ポート番号が表示されます。
合計	カウンタの値が表示されます。
秒平均	秒あたりのカウンタの平均値が表示されます。

3.3.5.　システムログ

[システム管理ツール] から [システムログ] を選択すると、図 3-79 のような画面が表示されます。この画面には、この装置で発生したイベントのログが表示されます。イベントを表示すると、この装置で発生した現象を常に把握できるため、ネットワーク管理に役立ちます。

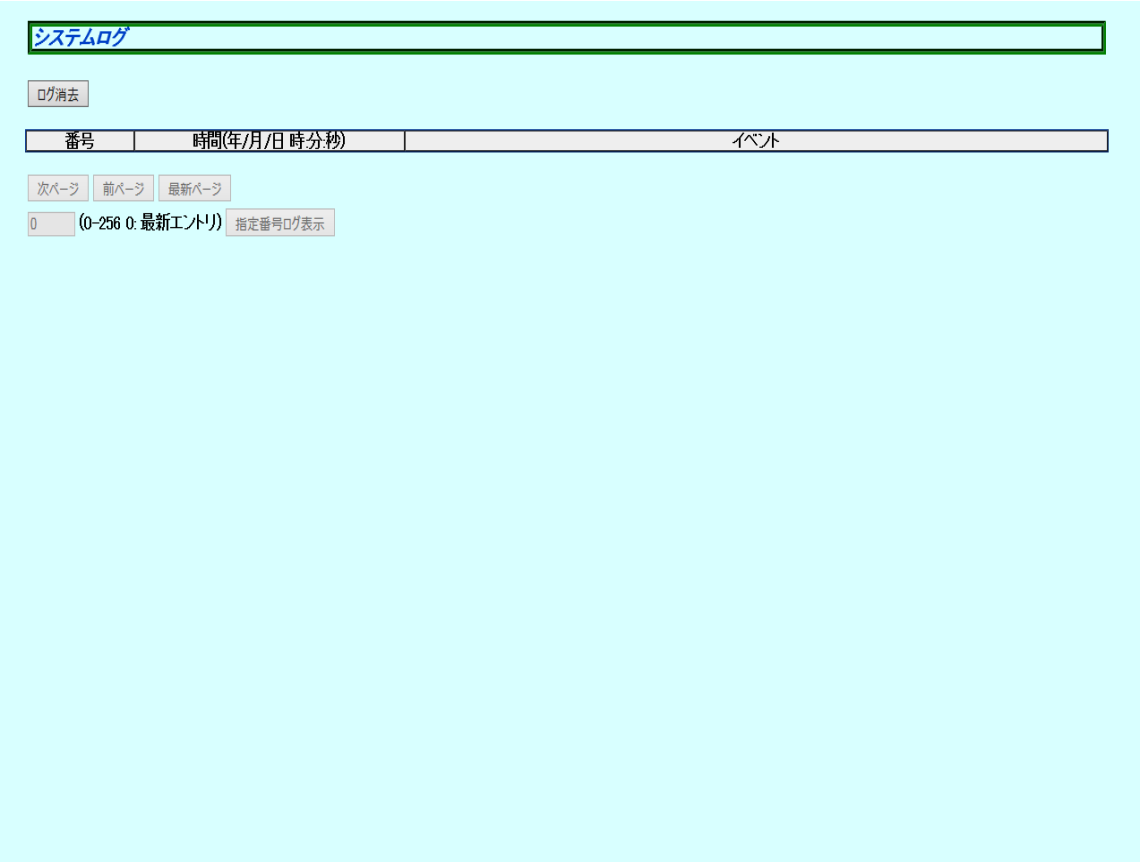


図 3-79 システムログ

この画面に表示されるイベントのいくつかは、SNMP トラップにリンクされています。トラップの発生が設定されている場合はイベントとして表示されます。トラップとの関係は下記をご参照ください。

画面の説明

ログ消去	保存済のシステムログを削除します。	
番号	イベントの番号が表示されます。	
時刻	イベントの発生した時刻が表示されます。 時刻が設定されていない場合は、この装置が起動してからの通算の時間が表示されます。	
イベント	この装置で発生したイベントの内容が表示されます。	
	< 実機確認中 >	< 実機確認中 >
次ページ	一覧の表示範囲が切り替わります。	
前ページ		
最新ページ	最新のイベントを含む範囲で一覧が表示されます。	
指定番号ログ表示	指定番号のイベントを含む範囲で一覧が表示されます。	

ご注意： 最大 256 件のシステムログが保存されます。257 件以上のシステムログが作成された場合は、最も古いシステムログが削除され、新しいログで上書きされます。

3.3.6.　設定ファイル転送

[システム管理ツール] を選択し、[設定ファイル転送] を選択すると、図 3-80 のような画面が表示されます。この画面では、設定ファイルのアップロードおよびダウンロードを行います。

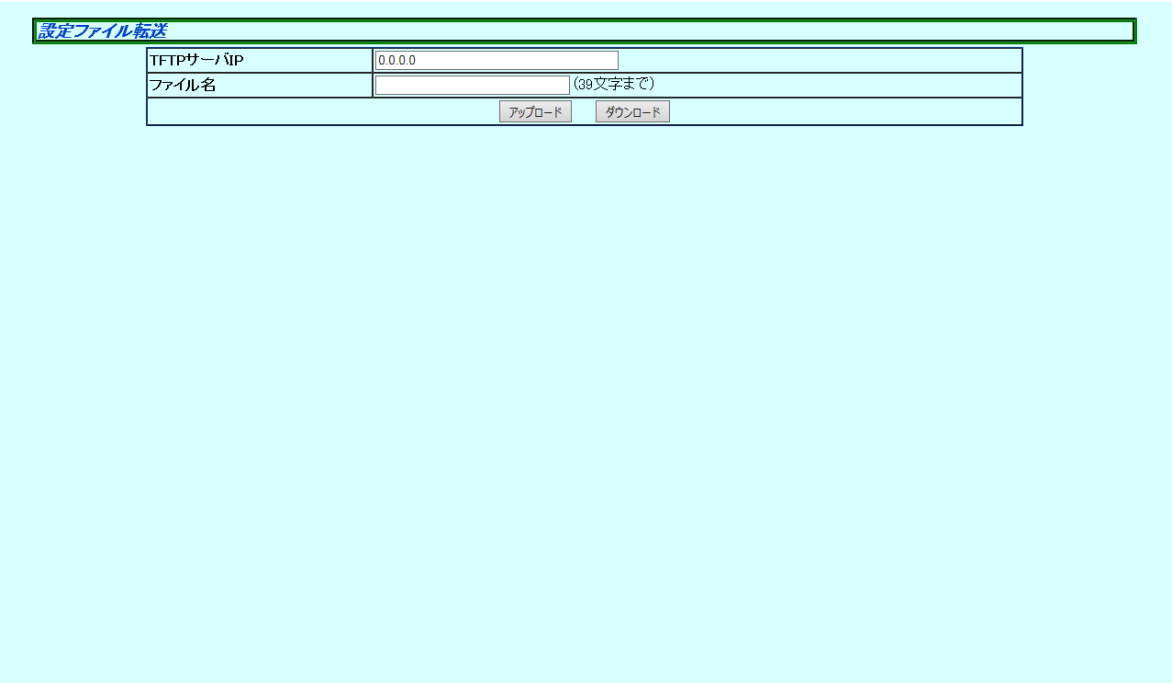


図 3-80 設定ファイル転送

画面の説明

TFTP サーバ IP	設定情報の保存と読み込みを行う TFTP サーバの IP アドレスが表示されます。
ファイル名	設定情報のファイル名が表示されます。

[アップロード] を選択して設定情報を TFTP サーバに保存するか、[ダウンロード] を選択してこの装置に設定情報を読み込みます。

アップロードまたはダウンロードが完了すると、図 3-81 のような画面が表示されますので、実行結果を確認して下さい。
[前のページに戻る] をクリックすると、[設定ファイル転送] 画面に戻ります。

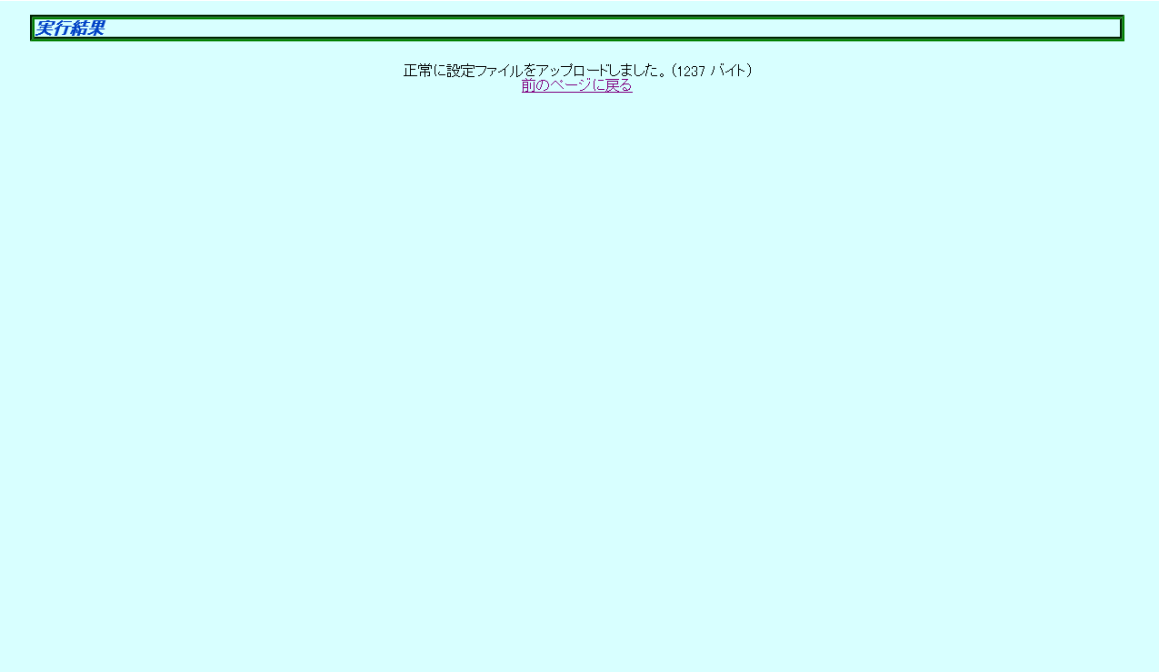


図 3-81 実行結果（アップロード完了後）

3.3.7. Ping の実行

[システム管理ツール] から [Ping 実行] を選択すると、図 3-82 のような画面が表示されます。この画面では、この装置に接続されている他の機器に対して Ping を送信することにより、通信確認を行うことができます。

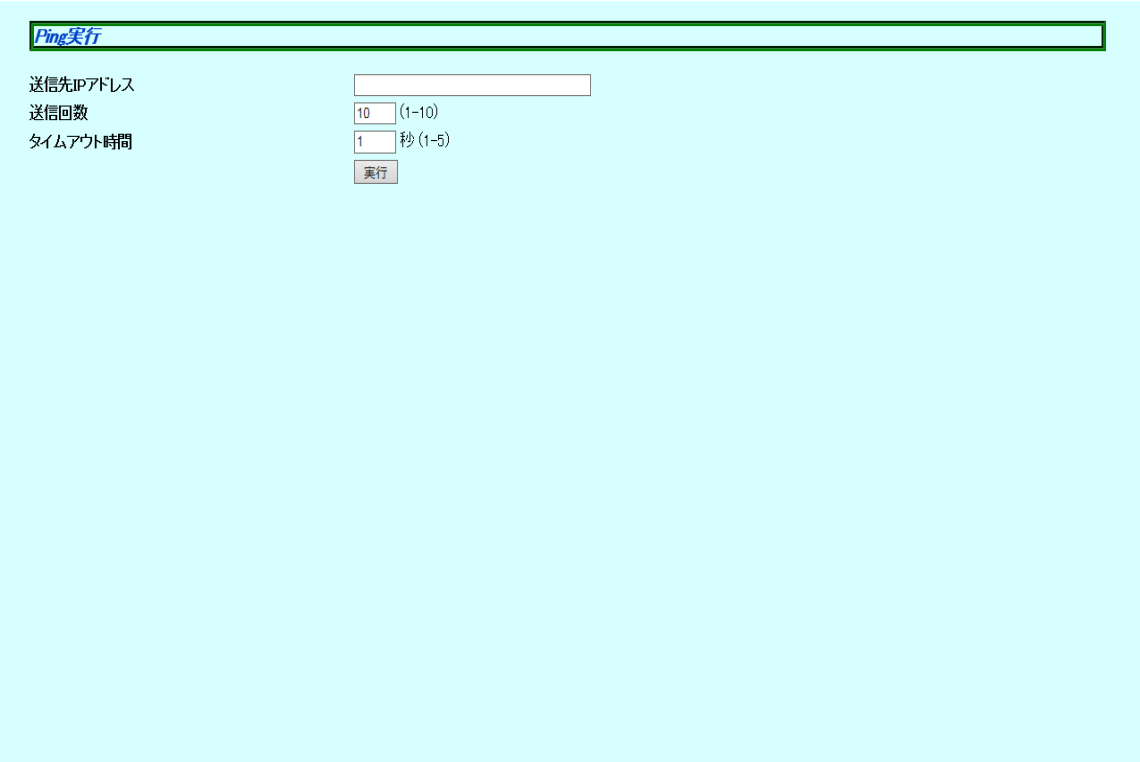


図 3-82 Ping の実行

画面の説明

送信先 IP アドレス	Ping 送信先の IP アドレスまたは IPv6 アドレスが表示されます。
送信回数	Ping の送信回数が表示されます。工場出荷時は 10 回に設定されています。
タイムアウト時間	タイムアウト時間が表示されます。工場出荷時は 3 秒に設定されています。

[実行] ボタンをクリックすると、Ping の送信が開始されます。指定回数の Ping 送信が完了すると、図 3-83 のように実行結果が表示されます。

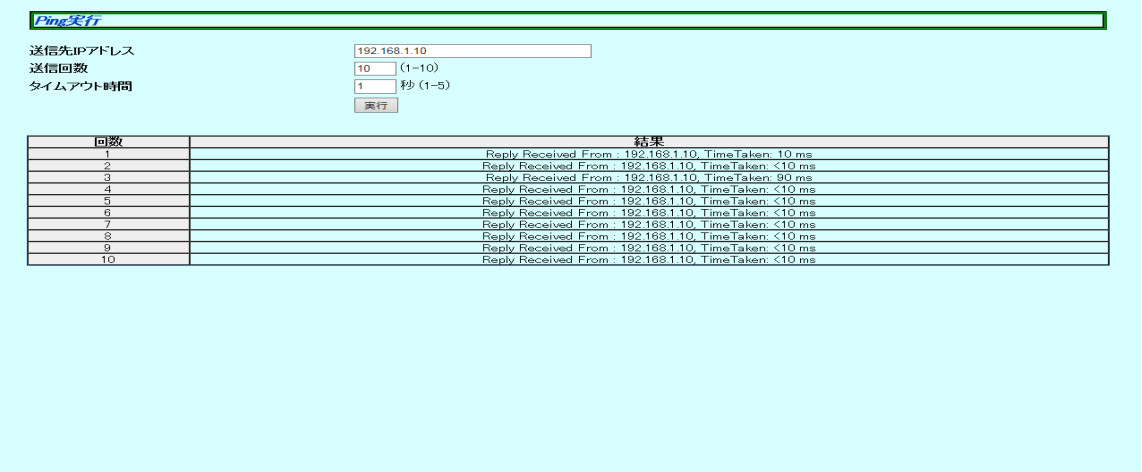


図 3-83 Ping 実行結果

3.3.8.　例外処理の設定

[システム管理ツール] から [例外処理設定] を選択すると、図 3-84 のような画面が表示されます。この画面では、ソフトウェア例外発生時の動作を設定することができます。
例外処理機能を有効にすると、ソフトウェア例外を検出した際、[例外処理方法] で設定した処理を実行します。

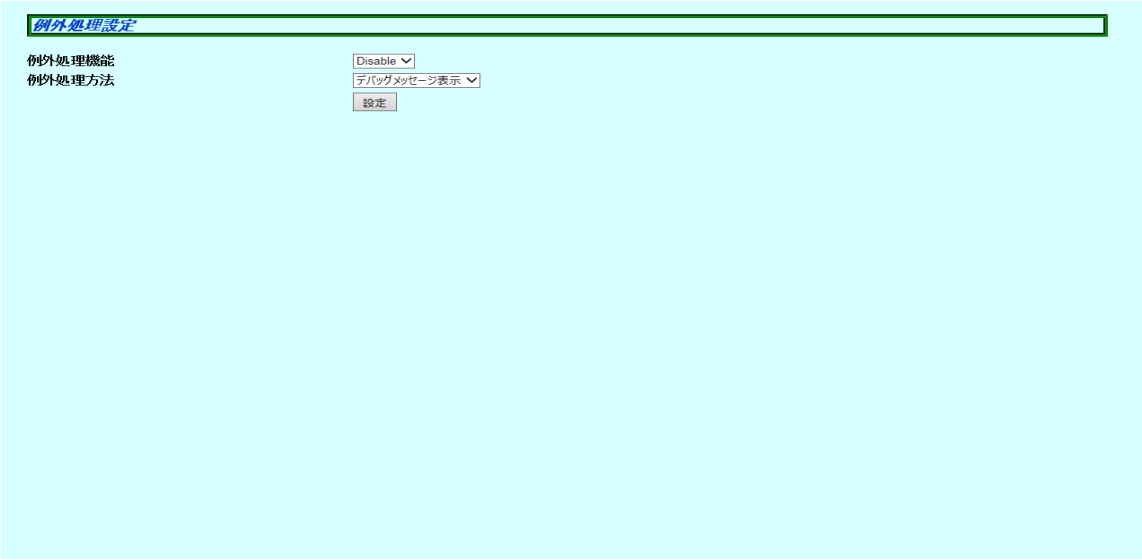


図 3-84 Ping の実行

画面の説明

例外処理機能	例外処理機能の状態が表示されます。	
	Enable	例外処理機能を有効にします。
	Disable	例外処理機能を無効にします。 (工場出荷時設定)
例外処理方法	例外処理の方法が表示されます。	
	デバッグメッセージ表示	例外処理を検出した際、コンソール上にデバッグメッセージを出力します。 (工場出荷時設定)
	再起動	例外処理を検出した際、自動的に再起動を実行します。
	両方	例外処理を検出した際、コンソール上にデバッグメッセージを出力した後、自動的に再起動を実行します。

3.3.9. Watchdog Timer 設定

[システム管理ツール] から [Watchdog Timer 設定] を選択すると、図 3-85 のような画面が表示されます。Watch Dog Timer 機能はシステム上で動作しているソフトウェアが正常に動作していることを定期的に監視する機能です。Watch Dog Timer 機能を有効にすると、ソフトウェアに異常が発生した場合に装置の再起動を行います。

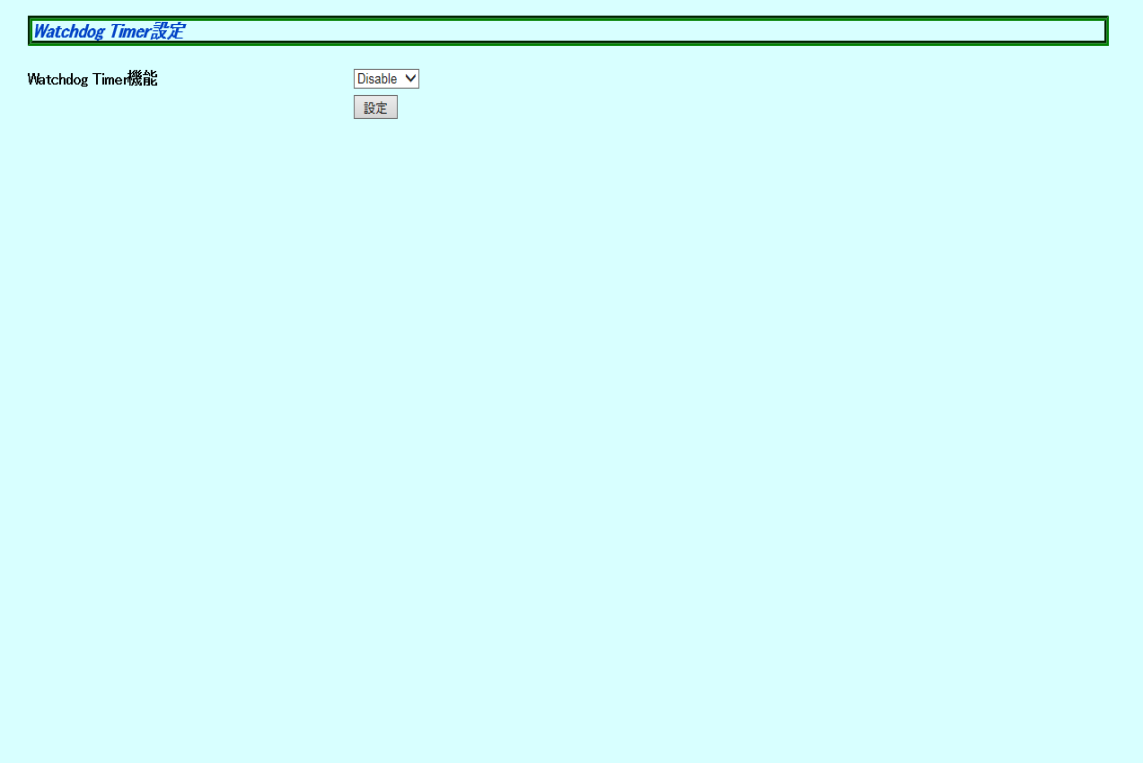


図 3-85 Watchdog Timer 設定

画面の説明

Watchdog Timer 機能	Watchdog Timer 機能の状態が表示されます。	
	Enable	Watchdog Timer 機能を有効にします。
	Disable	Watchdog Timer 機能を無効にします。(工場出荷時設定)

付録 A.仕様

仕様については、この装置の「メニュー編」を参照してください。

付録 B.IP アドレス簡単設定機能について

IP アドレス簡単設定機能を使用する際の注意点について説明します。

【動作確認済ソフトウェア】
『ZEQUO assist Plus』Ver.1.2.7.1

【設定可能項目】
・ IP アドレス、サブネットマスク、デフォルトゲートウェイ

【制限事項】
・ セキュリティ確保のため、電源投入時より 20 分間のみ設定変更が可能です。
ただし、IP アドレス / サブネットマスク / デフォルトゲートウェイ / ユーザ名 / パスワードの設定が工場出荷時状態の場合、時間の制限に関係なく設定が可能です。
※ 制限時間を過ぎても一覧には表示されますので、現在の設定を確認することができます。

© Panasonic Electric Works Networks Co., Ltd. 2018-2024

パナソニックEWネットワークス株式会社

〒105-0021　東京都港区東新橋 2 丁目 12 番 7 号　住友東新橋ビル 2 号館 4 階
TEL 03-6402-5301 / FAX 03-6402-5304
URL: https://panasonic.co.jp/ew/pewnw/

P0318-5094