産業用マネージド イーサネット スイッチ

ソフトウェア ユーザー マニュアル

ファームウェア バージョン 5.2

改定版 2.1

www.redlion.net

製品情報 8
本マニュアルで扱う製品 8
ファームウェアのダウンロード 9
ソフトウェア ユーザー マニュアルのダウンロード 9
第 1 章 設定 インターフェイスへのアクセス 10
1.1 ウェブ ユーザー インターフェイスのクイック スタート ガイド 10
1.2 USB ドライバのインストール 12
1.3 USB COM ポートの表示 13
1.4 ターミナル ユーザー インターフェイスのクイック スタート ガイド 14
1.5 Microsoft ハイパー ターミナルの使用 15
第 2 章 初期設定とコンフィギュレーション 17
2.1 概要 17
2.2 はじめに 17
2.3 管理用インターフェイスへのアクセス 18
2.3.1 グラフィカル (ウェブ) インターフェイスの使用 18
2.4 ネットワーク アクセスのためのスイッチのコンフィギュレーション 18
2.5 イーサネット ポートのコンフィギュレーション 19
第 3 章 構成管理とファームウェアの更新 22
3.1 ファームウェアのインストール 22
3.1.1 ローカル システムからのインストール 22
3.1.2 リモート サーバからのインストール 22
3.2 ファームウェアの管理 23
3.3 高度な操作 24
3.3.1 ファイルの保存と復元 24
3.4 コンフィギュレーション マネージメント 25
3.5 工場出荷時設定 25
3.6 スイッチのリセット 26
3.7 ウェブ インターフェイスを使用したファームウェアの更新 26
3.8 TFTP サーバを使用したファームウェアの更新 27
3.9 スイッチ ユーティリティを使用したファームウェアの更新 27
第 4 章 スイッチの現在状況の監視 29
4.1 システム情報 29
4.2 ポート ステータス 30
4.3 電源および OK ステータス 30

4.4 ネットワーク統計 31
4.5 リアルタイム リング ステータス 32
4.6 コンフィギュレーション サマリー 33
4.7 モデム ステータス 34
4.8 MAC アドレス テーブル 35
4.9 アラーム (OK) 出力 36
4.9.1 両方の電源入力がオンのとき 36
4.9.2 リング障害 36
4.9.3 ポートがリンクしたとき 36
4.10 Modbus 監視 37
4.10.1 Enabled (有効化) 37
4.10.2 Station Number (ステーション番号) 37
4.10.3 Transport Layers (トランスポート層) 37
4.10.4 TCP Timeout (TCP タイムアウト) 37
4.10.5 TCP Connection Limit (TCP 接続上限) 38
4.10.6 Port (ポート) 38
4.10.7 Register Mapping (レジスタ マッピング) 38
第 5 章 ネットワーク管理 (SNMP および RMON) 41
5.1 SNMP、MIB および RMON グループ 41
5.2 SNMP セキュリティ 41
5.3 SNMP 通知 42
5.4 トラップ マネージャ 43
5.5 ネットワーク統計 43
5.5.1 イーサライク統計 43
5.5.2 RMON 統計 46
5.6 ポート ミラーリング 47
5.7 アラーム (OK) 出力 47
第 6 章 冗長プロトコル 49
6.1 RSTP とは? 49
6.2 リカバリタイム、ホップおよび収束時間 51
6.3 Spanning Tree Settings (スパニング ツリー設定) 52
6.3.1 Redundancy Protocol (冗長プロトコル)(デフォルト = Rapid Spanning Tree Protocol (ラピッド スパニング ツリー プロトコル)) . . 52
6.3.2 Bridge Priority (ブリッジ優先度)(0 ～ 61440、デフォルト =32768 53
6.3.3 Maximum Age (最大エージタイム)(6 ～ 40、デフォルト = 20) 53
6.3.4 Hello Time (ハロー間隔)(1 ～ 10、デフォルト = 2) 54
6.3.5 Forward Delay (転送遅延タイム)(4 ～ 30、デフォルト = 15) 54
6.3.6 Transmission Limit (伝送限界)(1 ～ 10、デフォルト = 6) 54
6.3.7 Region Name (リージョン名)(MSTP) 54
6.3.8 Configuration Revision (コンフィギュレーション リビジョン)(MSTP、0 ～ 65535) 54
6.3.9 Max Hops (最大ホップ数)(MSTP、6 ～ 40、デフォルト = 20) 54
6.3.10 MST インスタンス 55
6.4 スパニング ツリー ポート設定 55

6.4.1 Exclude (除外)(デフォルト = 含む) 56
6.4.2 Port Priority (ポート優先度)(0 ～240、デフォルト = 128) 56
6.4.3 Path Cost (パス コスト)(1 ～200,000,000) 56
6.4.4 Type (タイプ)(デフォルト = Auto (自動)) 56
6.4.5 Port-to-Port MAC (ポートツーポート MAC) (デフォルト = Auto (自動)) 57
6.5 冗長ステータス 57
6.6 STP アルゴリズムのポート状態 58
6.7 RSTP アルゴリズムのポート状態 59
6.8 RSTP 例 59
6.8.1 例 1: 冗長リング内の最大ホップ数とスイッチ 59
6.8.2 例 2: パス コストを使用した一次およびバックアップ接続の確立 60
6.8.3 例 3: マネージドスイッチが 1 つだけのリング トポロジー (まねをしないこと !) 61
6.9 リアルタイム リング設定 63
6.10 リング セットアップ 63
第 7 章 優先度付きキュー (QoS、CoS、ToS/DS) 65
7.1 トラフィック優先度 65
7.2 スケジューリング 66
7.3 QoS / CoS 設定 66
7.4 802.1p タグ設定 67
7.5 メッセージ レート制限 68
7.5.1 自動 68
7.5.2 入力帯域制限 69
7.5.3 出力帯域制限 70
7.6 QoS 例 71
7.6.1 QoS による重要なメッセージの確実なリアルタイム送信 71
7.6.2 仮想シナリオ 71
7.7 トラフィック優先度のスイッチのコンフィギュレーション 72
7.8 結果 73
第 8 章 マルチキャスト フィルタリング (IGMP) 74
8.1 IGMP について 74
8.2 マルチキャスト フィルタリング コンフィギュレーション 75
8.3 IGMP スイッチ設定 75
8.4 IGMP ポート設定 76
8.5 IGMP ステータス 77
8.6 IGMP ポート ステータス 77
8.7 IGMP グループ ステータス 78
8.8 IGMP 例 78
8.8.1 IGMP を有効化する利点 78
第 9 章 仮想ローカル エリア ネットワーク (VLAN) 80
9.1 VLAN 概論 80
9.2 VLAN 設定 81

9.2.1 VLAN のオペレーション モードの選択 . . . 81
9.2.2 コアタイプ . . . 81
9.2.3 ラーニング . . . 81
9.2.4 VLAN の追加、編集または削除 . . . 81
9.3 VLAN ポート設定 . . . 83
9.4 RSTP つき VLAN . . . 84
第 10 章 モデム アクセス設定 (-5MS-MDM のみ) . . . 86
10.1 リモート アクセス概論 . . . 86
10.1.1 ダイヤル イン . . . 86
10.1.2 ダイヤル アウト . . . 87
10.1.3 サイト ツー サイト . . . 87
10.2 モデム設定 . . . 88
10.3 PPP モード . . . 89
10.4 PPP クライアント設定 . . . 89
10.5 PPP サーバ設定 . . . 90
10.6 サーバおよびクライアント モードのための IP アドレス コンフィギュレーション . . . 90
10.7 リモート ユーザー . . . 91
10.8 ルーティング . . . 92
10.9 ダイヤル イン シナリオ コンフィギュレーション . . . 93
10.9.1 サーバとしての 5MS-MDM コンフィギュレーション . . . 93
10.9.2 クライアントとしての Microsoft Windows PC コンフィギュレーション . . . 95
10.10 ダイヤル アウト シナリオ コンフィギュレーション . . . 97
10.10.1 PPP クライアントとしての 5MS-MDM コンフィギュレーション . . . 97
10.10.2 PPP サーバとしての Microsoft Windows PC コンフィギュレーション . . . 99
10.11 サイトツーサイト シナリオ コンフィギュレーション . . . 102
10.12 ダイヤル アウト メッセージング概論 . . . 103
10.12.1 ダイヤル アウト メッセージング設定 . . . 103
10.12.2 イーサネット モデムの ASCII メッセージ送信 . . . 105
10.12.3 ハイパー ターミナル コンフィギュレーション . . . 106
10.12.4 イーサネット モデムの発動 . . . 106
第 11 章 その他の特別機能 . . . 108
11.1 ネットワーク タイム プロトコル . . . 108
11.2 ポートごとの IP の設定 . . . 109
11.3 DHCP サーバ . . . 110
第 12 章 セキュリティ設定 . . . 111
12.1 セキュリティ概要 . . . 111
12.2 リモート アクセス セキュリティ . . . 112
12.3 ポート セキュリティ . . . 114
12.4 ポート セキュリティ MAC エントリ . . . 115
12.5 IPSEC 設定 . . . 115
12.5.1 セキュリティ ポリシー データベース . . . 116

12.5.2 セキュリティ アソシエーション データベース 116
12.6 IKE ポリシー設定 117
12.6.1 IKE フェーズ 1 ポリシー 117
12.6.2 IKE フェーズ 2 ポリシー 118
12.6.3 IKE フェーズ 2 アルゴリズム 118
12.7 IKE 事前共有鍵および証明書 119
12.7.1 IKE 事前共有鍵 119
12.7.2 IKE 証明書 119
12.8 IPSEC のための CLI コマンド 121
12.8.1 SPD/SAD コマンド 121
12.8.2 IKE コマンド 122
第 13 章 コマンドライン インターフェイスの使用 125
13.1 コマンドライン インターフェイス (CLI) 概論 125
13.1.1 CLI にアクセス 126
13.2 CLI コマンド 126
13.2.1 グローバル コマンド 126
13.2.2 アクセス コンフィギュレーション 127
13.2.3 アラーム コンフィギュレーション 127
13.2.4 modbus コンフィギュレーション 128
13.2.5 info コンフィギュレーション 128
13.2.6 ネットワーク コンフィギュレーション 129
13.2.7 ポート セキュリティ コンフィギュレーション 129
13.2.8 ポート コンフィギュレーション 130
13.2.9 リング コンフィギュレーション 131
13.2.10 rstp コンフィギュレーション 131
13.2.11 qos コンフィギュレーション 132
13.2.12 vlan コンフィギュレーション 133
13.2.13 igmp コンフィギュレーション 134
13.2.14 chkpt コンフィギュレーション 135
13.2.15 ファームウェア コンフィギュレーション 135
13.2.16 tftp コンフィギュレーション 135
13.2.17 tz コンフィギュレーション 136
13.2.18 msti コンフィギュレーション 136
13.2.19 一般的コンフィギュレーション 136

付録 A ライセンスとポリシー 140
付録 B 規定に関する声明 143

付録 C デフォルト ソフトウェア コンフィギュレーション設定 145
C.1 デフォルト設定について 145
C.1.1 管理ポート 145
C.1.2 ポート 1 ～ 9 (以上) のためのポート コンフィギュレーション 145
C.1.3 ポート ミラーリング 146
C.1.4 RSTP/STP コンフィギュレーション 146
C.1.5 RSTP/STP ポート コンフィギュレーション 146

C.1.6 SNMP 通知 146
C.1.7 IGMP 設定 146
C.1.8 トラップ マネージャ 147
C.1.9 優先度付きキュー 147
C.1.10 SNMP システム情報 147
C.1.11 リモート アクセス セキュリティ 147
C.1.12 IEEE タギング 148
C.1.13 VLAN モード 148
C.1.14 VLAN ポート設定 148
C.1.15 モデム設定 148
C.1.16 PPP 設定 149
C.1.17 リモート ユーザー 149
C.1.18 ルーティング 149
C.1.19 ダイヤル アウト メッセージング 149

付録 D SNMP サポート 151
付録 E コンセプトと定義 153
付録 F AT コマンド サマリー (-MDM モデルのみ 157
F.1 AT コマンド 157
F.2 S レジスタ 158

付録 G サービス情報 160
付録 H ライセンス契約 162
H.1 PCRE ライブラリ 162
H.2 libpcap ソフトウェア 163
H.3 lighttpd ソフトウェア 164
H.4 spawn-fcgi ソフトウェア 164
H.5 ipsec-tools ソフトウェア 165
H.6 net-snmp ソフトウェア 166
H.7 Fast CGI ライブラリ 171
H.8 ウォッチドッグ ソフトウェア 171
H.9 GPLv2 (一般公衆利用許諾書バージョン 2) 172
H.10 クロスブラウザ /x-tools ライブラリ 177
H.11 OpenSSL ライセンス 189
H.12 Open SSH ライセンス 191
H.13 PPP ライセンス 192
H.14 Shadow ライセンス 197
H.15 Sudo ライセンス 199

製品情報

本マニュアルで扱う製品

本マニュアルは、以下の製品のファームウェア バージョン 5.0 が対象です。

- SLX-5MS-# スリムライン マネージド イーサネット スイッチ、10/100 x 5 ポート
- SLX-5MS-MDM-# マネージド イーサネット スイッチ、10/100 x 5 ポート、および内蔵モデム
- SLX-8MS-# スリムライン マネージド イーサネット スイッチ、10/100 x 8 ポート
- SLX-8MG スリムライン マネージド イーサネット スイッチ、10/100/1000 x 8 ポート
- SLX-10MG マネージド イーサネット スイッチ、10/100 x7 ポート、およびギガビット x3 ポート
- SLX-16MS マネージド イーサネット スイッチ、10/100 x16 ポート
- SLX-18MG マネージド イーサネット スイッチ、10/100 x16 ポート、およびギガビット x2 ポート
- EK26 ラックマウント ギガビット マネージド イーサネット スイッチ、26 ポート
- EF26 ラックマウント マネージド イーサネット スイッチ、10/100 x26 ポート
- EK32 ラックマウント ギガビット マネージド イーサネット スイッチ、32 ポート
- EF32 ラックマウント マネージド イーサネット スイッチ、10/100 x32 ポート
- ET-5MS-OEM -# - 5 ポート OEM マネージド スイッチ
- ET-8MS-OEM -# - 8 ポート PC104 OEM マネージド スイッチ
- ET-8MG-OEM – 8 ポート ギガビット PC104 OEM マネージド スイッチ

ファームウェアのダウンロード

最新のファームウェアは、次のウェブサイトからダウンロードできます。

http://www.redlion.net

ファームウェアのリリース履歴は、次のウェブサイトで参照できます。

http://www.redlion.net

ソフトウェア ユーザー マニュアルのダウンロード

このユーザー マニュアルの最新版はこちらで入手できます。

http://www.redlion.net

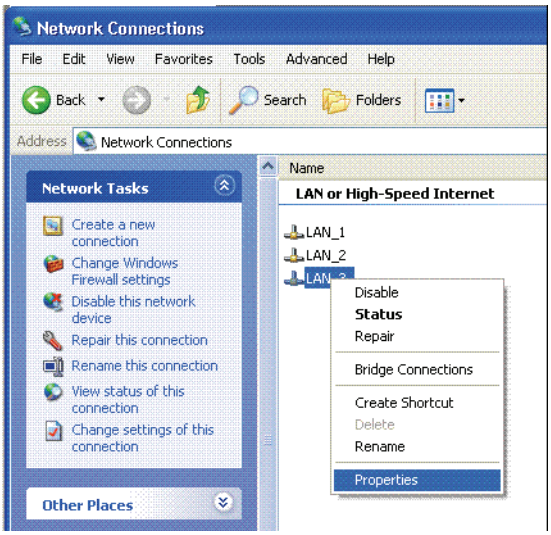
第 1 章 設定 インターフェイスへのアクセス

1.1 ウェブ ユーザー インターフェイスのクイック スタート ガイド

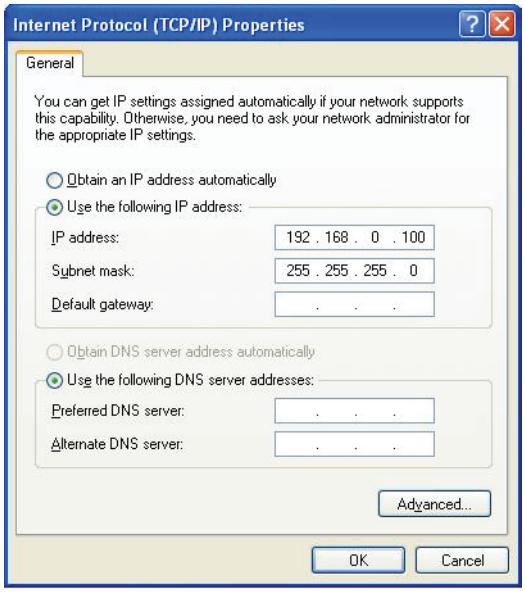
本ガイドを使って、イーサネット経由でスイッチの設定を素早くおこなえます。
注 : 初めてスイッチにアクセスする際に推奨する方法です。

1. スイッチのデフォルトの IP アドレスおよびサブネット マスクは、「192.168.0.1」と「255.255.255.0」です。このため、お使いのパソコンを互換性のある IP アドレス (例：192.168.0.100) に一時的に設定する必要があります。
   以下の手順に従ってください。

   1. お使いのパソコンをローカル エリア ネットワークから切り離します。
   2. パソコンの [コントロール パネル] を開きます。
   3. [ネットワーク接続] を開きます。



   4. お使いの LAN の [プロパティ] ウィンドウを開きます。
   5. [インターネット プロトコル (TCP/IP)] の [プロパティ] を開きます。
   6. 次の IP アドレスを使う] を選び、「192.168.0.100」を [IP アドレス] の欄に入力し、「255.255.255.0」を [サブネット マスク] の欄に入力します。

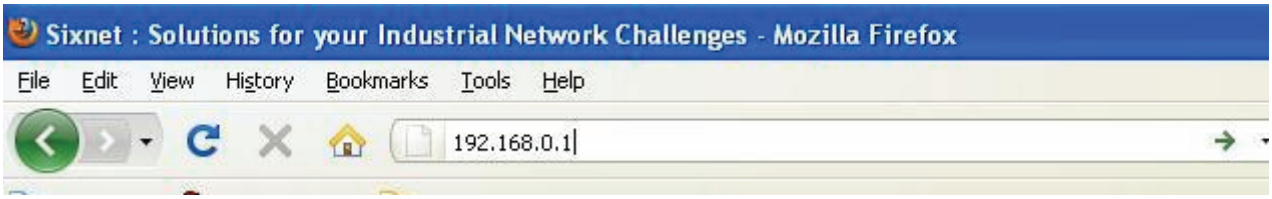


7. [OK] をクリックし、変更を適用します。必要に応じ、パソコンを再起動してください。

2. イーサネット パッチ ケーブルで、お使いのパソコンとスイッチのいずれかの RJ45 イーサネット ポートを繋ぎます。

3. スイッチにアクセスするには、Internet Explorer や Mozilla Firefox などのウェブ ブラウザを使用します。

4. スイッチのデフォルトの IP アドレス「192.168.0.1」をウェブ ブラウザのアドレス バーに入力し、キーボードの [Enter] キーを押します。



5. ログイン名とパスワードの入力を要求するログイン ウィンドウが表示されます。ユーザー名に「**admin**」、パスワードに「**admin**」を入力します。

6. ソフトウェア使用許諾契約を読み、[I accept the License]（使用許諾契約書に同意します）ボタンをクリックします。

7. コンフィギュレーション画面左側に表示されるツリーを使って進めてください。

8. **[Quick Setup]（クイック セットアップ）**をクリックして **[System Settings]（システム設定）**メニューを表示します。IP アドレス (DHCP または静的)、サブネット マスク、冗長プロトコル、システム名、連絡先、および位置情報を設定するために、このメニューを使用します。次の画像を参照してください。

9. スイッチが属するネットワークに対応する希望の IP アドレスとサブネットを設定するか、DHCP を有効にします。[Commit] (実行) をクリックして、新しい設定を有効にします。

10. お使いのパソコンを通常のネットワーク設定 (IP とサブネット) に戻し、LAN に再接続します。

11. スイッチを LAN または属するネットワークに接続し、スイッチにアクセスするために割り当てた IP アドレスを使います。DHCP を [enabled](有効) にしている場合は、LAN 管理者に連絡して、割り当てられた IP アドレスを決定する必要があります。

12. スイッチにアクセスできるようになったら、以下のことがおこなえます。

    a. デフォルトの管理者パスワードは、[Remote Access Security](リモート アクセス セキュリティ) メニューから変更できます。

    b. スイッチの各ポートはデフォルトと自動選択のセットになっており、コンフィギュレーション不要で素早く始められるようになっています。ポートの有効化 / 無効化、速度選択、双方向通信、またはフロー制御によりポート設定をカスタマイズするには、[Port Configuration](ポート コンフィギュレーション) メニューからアクセスします。

    c. ラピッド スパニング ツリー プロトコル (RSTP) は、スイッチのデフォルトでは無効です。RSTP 設定は、[Redundancy Settings](冗長設定) 画面から変更できます。

    d. スイッチの稼働状況を [Monitoring](監視) メニューからアクセスして確認してください。

    e. モデムと PPP 設定は [Remote Access Settings](リモート アクセス設定) メニューで確認できます。

    注：スイッチは、当初はシリアル ポートも使用するように設定されています。しかし、イーサネット方式では上記の方法が推奨されています。シリアル ポート方式の使用については、付録 J を参照してください。

1.2 USB ドライバのインストール

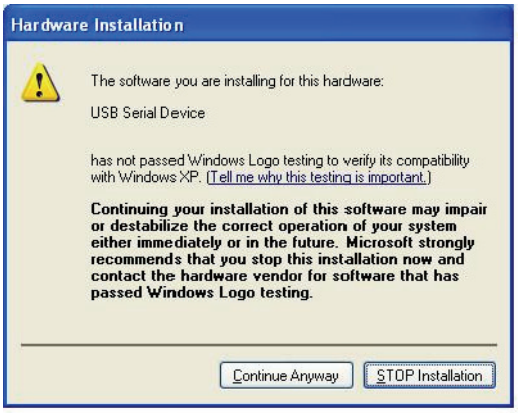
Red Lion のマネージド スイッチは、端末アクセス用に USB ポートと RS232 ポートの両方を備えています。
USB ポートを利用するには、www.redlion.net またはお手持ちの Red Lion CD を参照して、USB ドライバをインストールしてください。

インストールの終了後、USB 経由でスイッチに接続します。[New Hardware Wizard](新しいハードウェアの検出ウィザード) が表示されます。

[No, not this time](いいえ、今回は接続しません) を選択し、[Next](次へ) をクリックします。

次の画面で、[Install the software automatically](ソフトウェアを自動的にインストールする) を選択し、[Next] をクリックします。

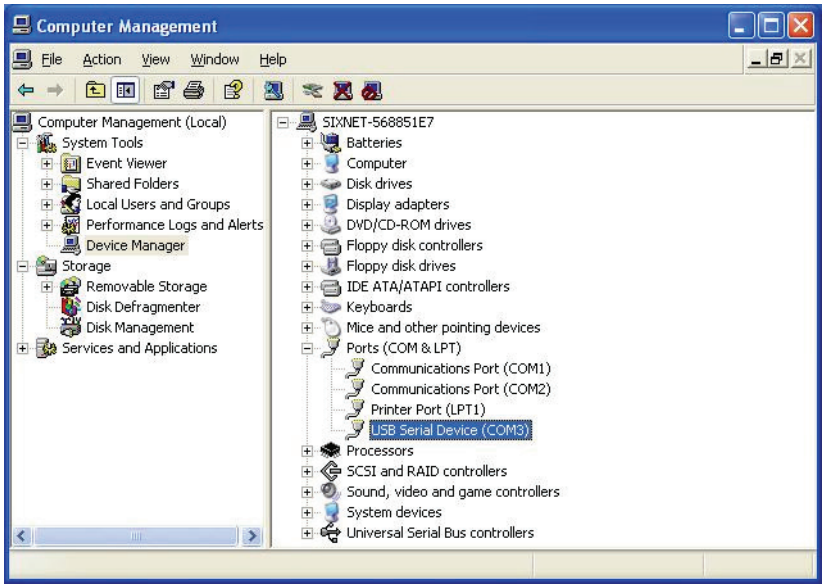
コンピューターがドライバを発見すると、未署名のドライバをインストールするか確認する警告が出ます。
[Continue Anyway](続行) を選択し、[finish](終了) をクリックしてインストールを終了します。



注 : USB ドライバのインストールは、Windows XP にのみ対応しています。Windows Vista をお使いの場合は、Red Lion までお問い合わせください。

1.3 USB COM ポートの表示

USB デバイスが割り当てられた COM ポートを参照するには、Windows デバイス マネージャを開きます。
ポートの (COM & LPT) セクションを開き、[USB Serial Device](USB シリアル デバイス) と表示されているポートを見つけます。



名前の後の COM 番号は、ターミナル インターフェイスを使用してスイッチにアクセスするために使われます。
USB および RS232 ポートは、同時に接続することができません。スイッチとの通信に使用を希望するケーブル タイプのみを取り付けてください。

1.4 ターミナル ユーザー インターフェイスのクイック スタート ガイド

ウェブ インターフェイスの代わりに、このガイドを使って RS232 ポートまたは USB ポート経由で素早くスイッチの設定ができます。

注 : このインターフェイスは、上級ユーザー向けです。本マニュアルの冒頭で説明しているウェブ インターフェイスの使用を推奨します。

1. お使いのパソコンのシリアル ポート (通常は DB9 メス コネクタ) を、スイッチのシリアル ポート (RJ45 メス コネクタ) に接続するか、USB ポートのあるスイッチなら、お使いのパソコンの USB ポートから、USB ケーブルをスイッチの USB ポートに接続します。この接続方法の詳細は、ハードウェア ユーザー マニュアルを参照してください。必要ならば、スイッチの供給元に連絡をし、配線済みインターフェイス ケーブルまたは USB ケーブルを購入してください。

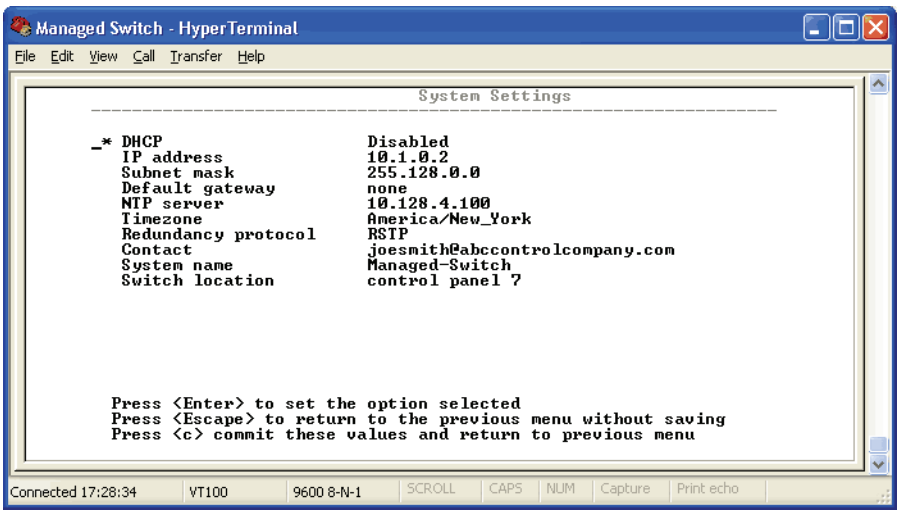
2. 9600、8N1、およびフロー制御の無効などのターミナル プログラム (ハイパー ターミナルなど) の設定をします。詳細は後述の章を参照してください。

3. ログイン名に「admin」、パスワードに「admin」を入力します。

4. お使いのターミナル プログラムがサポートしている適切なターミナル エミュレーションを選択します。

5. キャラクター ユーザー インターフェイスのナビゲーションは、矢印キーでオプションをハイライトし、[Enter] キーが選択、[Esc] キーで前のメニューに戻ります。[c] を押すと、変更をコミットします。[x] を押すと、メイン メニューからログアウトします。

6. [Quick Setup](クイックセット アップ) を選択して [System Settings](システム設定) メニューを表示します。このメニューは、IP アドレス (DHCP または静的)、サブネット マスク、冗長プロトコル、システム名、連絡先、そして位置情報を設定するために使用します。



7. スイッチが属するネットワークに対応する希望の IP アドレスとサブネットを入力するか、DHCP を有効にします。[c] をクリックして、新しい設定を有効にします。

8. これで、ウェブ インターフェイスを経由してスイッチにアクセスできます。または、このテキスト インターフェイスを使ってコンフィギュレーションの変更を続けることもできます。

9. テキスト インターフェイスを使って、次のようなことができます。

    1. デフォルトの管理者パスワードは、[Remote Access Security](リモート アクセス セキュリティ) メニューから変更できます。

    2. スイッチの各ポートはデフォルトと自動選択のセットになっており、コンフィギュレーション不要で素早く始められるようになっています。ポートの有効化 / 無効化、速度選択、双方向通信、またはフロー制御でポート設定をカスタマイズするには、[Port Configuration](ポート コンフィギュレーション) メニューからアクセスします。

    3. ラピッド スパニング ツリー プロトコル (RSTP) は、スイッチのデフォルトでは無効です。RSTP 設定は、[Redundancy Settings](冗長設定) 画面で変更できます。

    4. スイッチの稼働状況を [Monitoring](監視) メニューからアクセスして確認してください。

    5. モデムと PPP 設定は [Remote Access Settings](リモート アクセス設定) メニューで確認できます。

1.5 Microsoft ハイパー ターミナルの使用

Microsoft Windows ハイパー ターミナルをスイッチと共に使用するための設定は、以下の通りです。

1. [ファイル] メニューから [新規接続] を選択し、新規接続を作成します。

2. [接続詳細] ダイアログで、「Managed Switch」などの名前を接続につけ、[OK] をクリックします。

3. [接続先] ダイアログで、適切な COM ポートを選択します。

4. [COM プロパティ] ダイアログで、次の設定を選択します。

Microsoft ハイパー ターミナルの使用

- 毎秒 9600 ビット (Bps または Baud)
- 8 データ ビット、パリティなし、1 ストップ ビット
- フロー制御なし

5. [OK] をクリックします。
6. [ファイル] メニューから [プロパティ] を選択し、[接続プロパティ] を開きます。
7. [設定] をクリックし、設定タブを表示します。
8. エミュレーション リストから [VT100] を選択します。
9. [ターミナル セットアップ] をクリックします。
10. [ターミナル設定] で、[カーソル キーパッド モード] にチェック マークを入れて、[OK] をクリックします。
11. [OK] をクリックして、[接続プロパティ] ダイアログを閉じます。

ターミナル画面が表示されると、スイッチがログイン名の入力を促します。ログイン プロンプトを表示するために、[Enter] を数回押す必要がある場合があります。デフォルトのログイン名およびパスワードは、両方「admin」です。ログインとパスワードの入力が促されたら、[4] を押して [VT100] を選択し、[Enter] を押します。これで、メイン管理メニューが表示され、マネージド スイッチはフル コンフィギュレーションの準備が整いました。

第 2 章 初期設定とコンフィギュレーション

2.1 概要

産業用マネージド イーサネット スイッチは構成変更が可能なデバイスで、イーサネット ネットワーク上のイーサネット デバイスとの相互接続を容易にします。これには、コンピューター、オペレーター インターフェイス、I/O、コントローラー、RTU、PLC、その他スイッチ、ハブ、または標準 IEEE 802.3 プロトコル対応のあらゆるデバイスが含まれます。このスイッチには、イーサネット スイッチのストア アンド フォワード機能に加え、SNMP、RSTP、およびポート ミラーリングといった高度な管理機能がついています。本マニュアルでは、この使いやすいスイッチの様々な管理パラメータの設定方法を詳しく説明します。

2.2 はじめに

スイッチのすべての利用可能な機能とリソースを充分に活用するには、お使いのネットワーク用に設定する必要があります。

このスイッチは、ラピッド スパニング ツリー プロトコル (RSTP) とシンプル ネットワーク管理プロトコル (SNMP) を実装しており、スイッチが提供するサービスのほとんどを供給します。ラピッド スパニング ツリー プロトコルは、マネージド スイッチがお互いに交信することを許可し、各ネットワーク ノードのペア間にアクティブなルートが 1 つだけ確実に存在するようにし、障害時には次の利用可能な冗長ルートへの自動的な切替えを確実に行います。RSTP がどのように機能するかについては、「スパニング ツリー」の項で簡単に説明します。

スイッチは、管理情報を交換するために、ネットワーク上の他の SNMP 対応デバイスと通信することができます。このネットワークの統計取得情報は、スイッチの管理情報ベース (MIB) に保存されます。MIB は、いくつかの異なる情報ストレージ グループに分かれています。本マニュアルの「管理および SNMP 情報」の項で、このグループについて詳しく説明します。

スイッチはインターネット グループ管理プロトコル (IGMP) を実装しており、お使いのネットワークのマルチキャスト トラフィックのフローを最適化します。

VLAN 機能を備えたネットワークを柔軟に統合するために、スイッチはポート ベースとタグ ベースの両方の仮想 LAN に対応し、VLAN 機能を持たないデバイスを支援します。

補足の技術文書は、本マニュアルの付録に記載されています。付録には、重要な用語や定義、管理者メニュー マップ、RSTP ネットワーク トポロジーの例、およびスイッチから抽出した工場出荷時情報が収録されています。

2.3　管理用インターフェイスへのアクセス

スイッチには複数の管理者インターフェイスがあります。

1. スイッチ内蔵のウェブ サーバからアクセス可能なグラフィカル ウェブ インターフェイス。http とセキュア SSL サーバ証明書付き https の両方に対応しています。(注 : スイッチを管理する際に推奨する方法です。)

2. RS232/USB ポート経由、またはテルネットもしくはセキュア シェル (SSH) を利用したネットワーク経由のターミナル インターフェイス。

3. SNMP インターフェイスは、多くの設定の読み書きに使用できます。

4. CLI (コマンド ライン インターフェイス) は、ほとんどの設定の読み書きに使用できます。詳細は、別紙『CLI ユーザー マニュアル』を参照してください。

初期設定はイーサネット接続 (推奨) またはシリアル ポートを利用しておこないます。「第 1 章クイック スタート ガイド」を参照してください。

注 : このインターフェイスは、上級ユーザー向けです。本マニュアルの冒頭で説明しているウェブ インターフェイスの使用を推奨します。

2.3.1　グラフィカル (ウェブ) インターフェイスの使用

グラフィカル インターフェイスは、スイッチのウェブ サーバ経由で提供され、Opera、Mozilla、または Internet Explorer などのウェブ ブラウザからアクセスできます。

注 : グラフィカル インターフェイスを正しく使用するには、お使いのブラウザが JavaScript に対応し、有効でなければなりません。

ウェブ サーバにアクセスするために HTTP および HTTPS(セキュア HTTP) が対応しています。デフォルトでは、プロトコルは両方とも有効です。一方、もしくは両方を無効にすると、スイッチはセキュアになります。(この章の「リモート アクセス セキュリティ」の項目を参照してください。)

グラフィカル インターフェイスにアクセスするには、「HTTP://192.168.0.1」のような URL をお使いのブラウザのアドレスバーに入力してください。 セキュアな http を使うには、「http」を「https」に変更し、工場出荷時設定から変更している場合は、「192.168.0.1」をお客様のスイッチの IP アドレスに変更します。

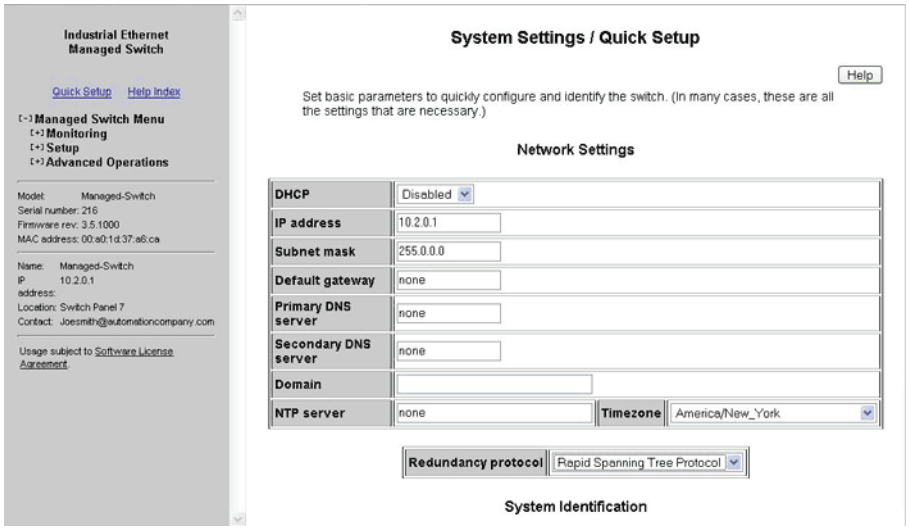
スイッチのウェブ サーバは、署名入りセキュリティ証明書を使用します。https 経由でサーバにアクセスする際には、証明書が不明な機関によって署名されたものであるという、警告ダイアログが表示されることがあります。これは想定内のことであり、今後このメッセージを避けるには、お使いのパソコンに証明書をインストールしてください。

注 : 本マニュアルでは、ウェブ ユーザー インターフェイスを詳しく説明し、図で示しています。ターミナル インターフェイスは特に図で示していませんが、基本的には同じです。

2.4　ネットワーク アクセスのためのスイッチのコンフィギュレーション

ネットワーク経由でスイッチの管理と監視をするには、IP アドレスやサブネット マスクを含む基本的なネットワーク設定をする必要があります。初めてスイッチにアクセスする方法については、「第 1 章クイック スタート ガイド」を参照してください。

ネットワーク アクセスのためにスイッチを設定するには、**[Main Menu](メインメニュー)** から **[Quick Setup] (クイック セットアップ)** を選択し、**[System Settings](システム設定)** メニューへ移動します。 このメニューでの設定は、スイッチ全般のネットワーク構成を制御します。



- **DHCP Enabled/Disabled (有効 / 無効):** スイッチは、ダイナミック ホスト コンフィギュレーション プロトコル (DHCP) を使って、自動的に IP アドレスをサーバから取得できます。ネットワーク管理者が空いている IP アドレスを探す必要が無いので、初期設定がスピードアップします。

- **IP Address (IP アドレス) と Subnet Mask (サブネット マスク) の構成 :** スイッチの IP アドレスをユーザーが定義するアドレスに変更し、またカスタマイズしたサブネット マスクでサブネットを分離できます。

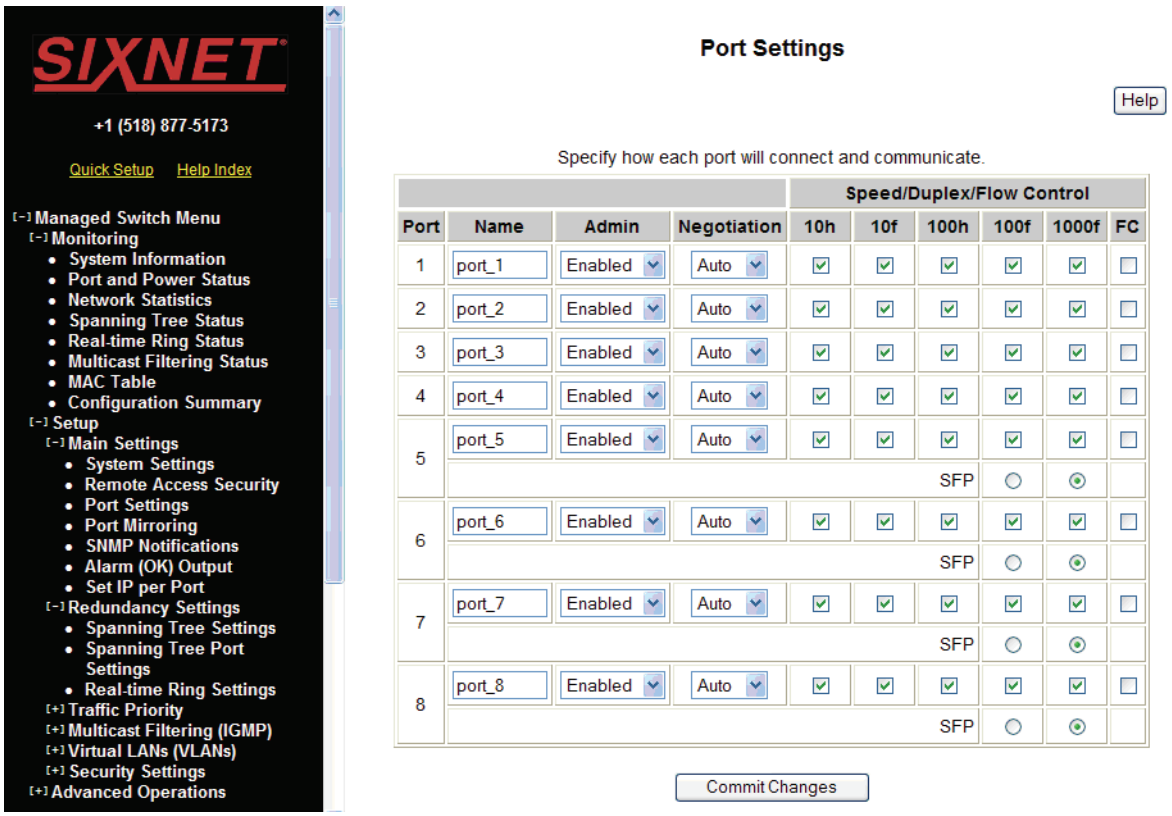
注 : 上級ユーザーは追加セキュリティとして、IP アドレスを「0.0.0.0」に設定して、IP アドレスの使用を無効にすることができます。ただし、IP アドレスが必要な機能 (例 : ウェブ インターフェイスなど) は、使うことができなくなります。

- **Default Gateway (デフォルト ゲートウェイ) 選択 :** ゲートウェイ アドレスは、2 つの異なるネットワークをつなげるルーターのアドレスを選択します。これは IP アドレス、または「domainname.org」などの完全修飾ドメイン名 (FQDN) です。

- **NTP Server (NTP サーバ):** スタートアップ時の現在時刻をスイッチが検索するための NTP (ネットワーク タイム プロトコル) サーバの IP アドレス、またはドメイン名。ドメイン名の使用には、最低 1 つのドメイン名サーバを設定する必要があります。詳細は 108 ページの第 11 章「その他の特別機能」を参照してください。

2.5 イーサネット ポートのコンフィギュレーション

スイッチはデフォルトのポート設定で届くので、コンフィギュレーション不要でイーサネット ポートに接続できます。ポート名、ネゴシエーション設定、またはフロー制御設定の変更が必要な場合は、**[Port Configuration menu](ポート コンフィギュレーション メニュー)** で変更できます。このメニューにアクセスするには、**[Main menu](メインメニュー)** から **[Setup](セットアップ)** を選択し、さらに **[Main Settings](メイン設定)** を選択します。



- **Port Name (ポート名):** マネージド スイッチの各ポートは、カスタム名で区別します。ここで、各ポートの名前を指定してください。

- **Admin (管理):** ポートはマネージド スイッチ内で、enabled (有効) か disabled (無効) にできます。無効のポートは、事実上存在しないことになります。(スイッチ稼働時やスパニング ツリー アルゴリズムから見えません) ポートの有効、無効は個別に選択します。

- **Negotiation (ネゴシエーション):** マネージド スイッチ内のすべてのカッパー ポートとギガビット ファイバ ポートは、最速の帯域を選択するなどのオート ネゴシエーションが可能です。オート ネゴシエーションを有効にするか、固定設定を選択してください。100Mbps のファイバ ポートは、固定速度のみです。

- **Speed (速度)/Duplex (双方向通信)/Flow Control (フロー制御):** マネージド スイッチは、3 つのローカル エリア ネットワーク イーサネット規格に対応します。最初の規格 10BASE-T は、ネットワーク インターフェイス間のツイスト ペア イーサネット ケーブルによって 10 Mbps で動作します。2 つめのローカル エリア ネットワーク規格は 100BASE-T で、同じツイスト ペア イーサネット ケーブルによって 100 Mbps で動作します。最後は 100BASE-F で、光ファイバを使ってファスト イーサネット (100 Mbps) を可能にします。

  次のオプションが利用できます。

  - 10h–10 Mbps、半二重
  - 10f –10 Mbps、全二重
  - 100h–100 Mbps、半二重
  - 100f –100 Mbps、全二重
  - 1000f–1000 Mbps、全二重

マネージド スイッチでギガビット コンビネーション ポートを持つ場合は、チェック ボックス付きの標準的な行と「SFP」と書かれたラジオ ボタン付き行の 2 行があるポートがあります。SFP 設定は、SFP が差し込まれた場合、トランシーバが稼働する速度を個別に設定します。SFP がない場合は、スイッチは固定イーサネット ポートおよびそれに対応する設定を使用します。

注：ギガビット コンビネーション ポートの SFP で 100F が選択されていると、対応する固定イーサネット ジャックは、1000F に変更を戻さないかぎり無効になります。

フロー制御も有効または無効にでき、有効の時は「FC」に表示されます。フロー制御を使用する機器は、受信機器がエラーなしでデータをすべて受信できるようにします。送信機器が受信機器よりも速い速度で送信する場合は、受信機器のバッファはいずれはフルになります。バッファがフルの場合は、それ以上は情報を受け取れないので、フロー制御シグナルが送信機器に送られ、一時的に受信データの流れを停止します。

第 3 章 構成管理とファームウェアの更新

3.1 ファームウェアのインストール

Install Firmware (ファームウェアのインストール) のページで、アクティブでないファームウェアを新しいバージョンに交換できます。

3.1.1 ローカル システムからのインストール

ファームウェアは、ローカル システムからスイッチに直接アップロードできます。[Browse](参照) ボタンを使って「.fwb」ファームウェア ファイルを検索します。ファイルの MD5 チェックサムが利用できる場合は、**[MD5 Checksum (Optional)](オプション)** フィールドに入力します。チェックサムの提供により、ファームウェアに損傷がなく完全な形で確実にスイッチに送ることができます。MD5 チェックサムは必須ではありません。**[Install from file] (ファイルからインストール)** ボタンをクリックすると、ファームウェアのインストール手順が始まります。

3.1.2 リモート サーバからのインストール

「.fwb」ファームウェア ファイルを提供するリモート機器から、スイッチでファームウェアを取得することも可能です。サーバは TFTP、HTTP、HTTPS、FTP または FTPS 経由でファイルを提供しなければなりません。

[Server Address](サーバ アドレス) フィールドにサーバのアドレスを入力します。[**System Settings] (システム設定)** のページで DNS サーバが設定されている場合、IP アドレスまたはドメイン名です。リテラル IPv6 アドレスは角括弧で囲まれていなければなりません。

たとえば、次のアドレスを使うには

fdda:2301::2

下のように入力します。

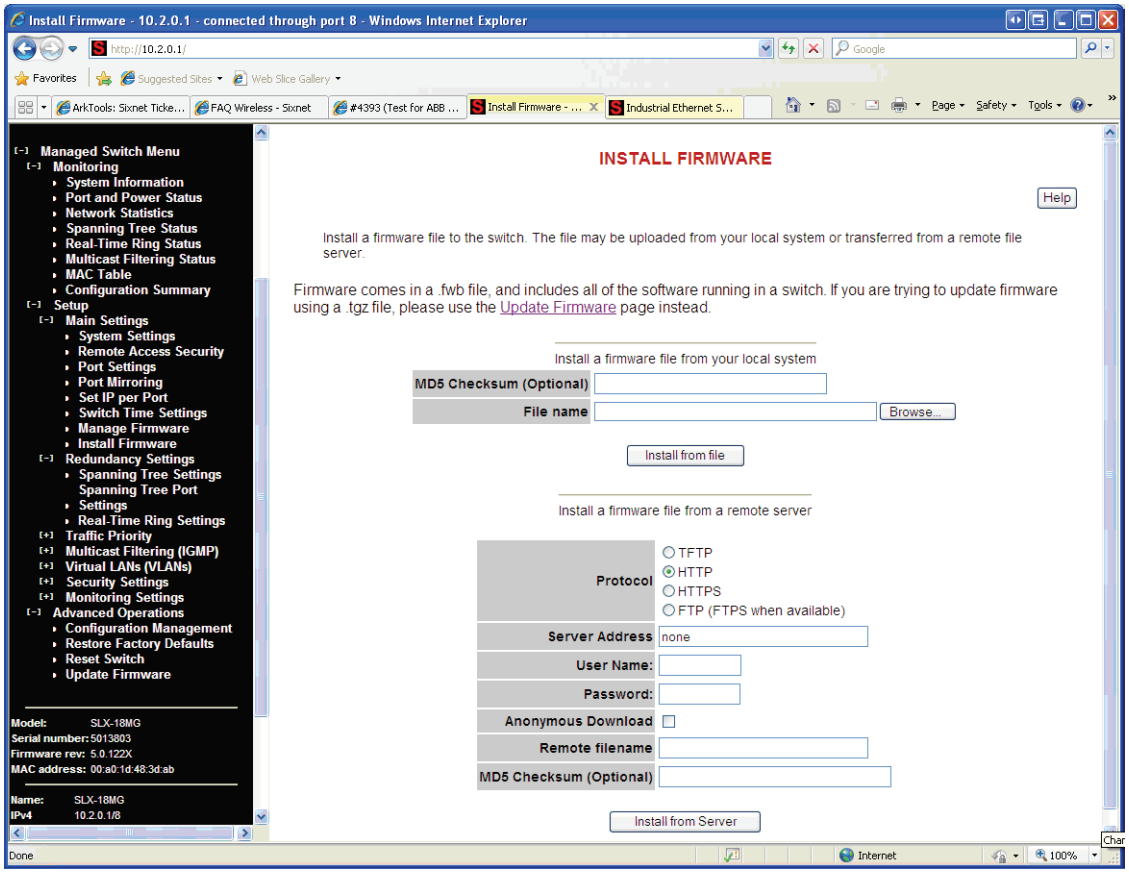
[fdda:2301::2]

サーバがファイルを検索するためにユーザー名とパスワードを必要とする場合は (TFTP では利用できません)、**[User Name](ユーザー名)** と **[Password](パスワード) フィールド**にそれぞれ認証情報を入力します。サーバがこの種類の認証を必要とせず、誰でもファイルがダウンロードできる場合は、**[Anonymous Download](匿名ダウンロード)** のボックスにチェックを入れてください。

[Remote filename](リモート ファイル名) フィールドに、サーバ上のファイルへのフルパスを入力します。

ファイルに MD5 チェックサムが利用できる場合は、[MD5 Checksum (Optional)](オプション) フィールドに入力します。チェックサムの提供により、ファイルに損傷がなく完全な形で確実にスイッチに送ることができます。MD5 チェックサムは必須ではありません。

[Update from Server](サーバから更新) ボタンをクリックすると、ファームウェアのインストール手順が始まります。



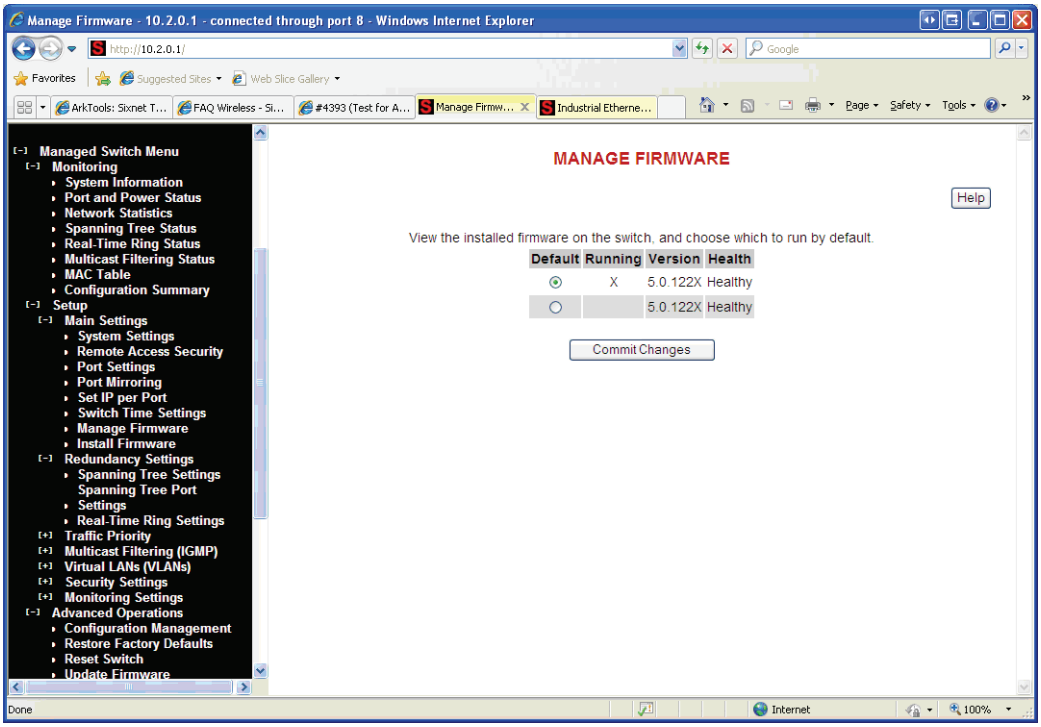
3.2 ファームウェアの管理

[Manage Firmware](ファームウェアの管理) のページでは、スイッチの 2 つのファームウェア イメージのそれぞれの現在のステータスが表示され、次にスイッチがリセットされたときに実行するファームウェアを変更することができます。

- **Default (デフォルト)**– スイッチがリセットされたときに実行される現在のデフォルトのファームウェア イメージを表示。次にリセットされたときは、違うファームウェアを実行するように変更することができます。
- **Running (実行中)**– 現在実行中のファームウェア イメージを表示。最近、スイッチが起動に失敗していると、現在のデフォルトのファームウェア イメージとは異なる可能性があります。
- **Version (バージョン)**– インストール済みファームウェアのそれぞれのファームウェア バージョン番号を表示。バージョンが確定できない場合は、「Unknown」(不明) と報告されます。
- **Health (健全性)**– 各ファームウェア イメージの健全性を表示。健全性は次のうちのいずれか 1 つ。

- **Healthy (正常)**– ファームウェアが実行中か、実行するのに十分良い状態であることが期待されます。
- **Broken (障害)**– ファームウェアが起動できない状態にあります。デフォルトの欄は、このイメージを起動用に選択することはできません。
- **Unknown (不明)**– ファームウェアは起動可能だが、スイッチは確実ではありません。スイッチがデフォルト ファームウェア以外を実行中に発生します。デフォルト ファームウェアが何らかの理由で破損するか、スイッチの起動の最中に電源を失うと発生します。

現在実行中のファームウェアがデフォルトでない場合、かつデフォルトを意識的に保存することなくスイッチがリセットされると、現在のファームウェアが再び実行されます。デフォルトとして印がつけられたファームウェアを起動するには、何も変更せずにこのページの内容をコミットし、スイッチをリセットします。



3.3 高度な操作

[Advanced Operations](高度な操作) メニューを使用して、コンフィギュレーションの保存および復元、工場出荷時設定の再読み込み、スイッチのリセット、ファームウェアの更新、ならびにリモートアクセスのセットアップを行います。

注 : ウェブ インターフェイスは、お使いのブラウザを実行中のシステムからの直接転送に対応します。または、ファイル転送に TFTP（トリビアル ファイル転送プロトコル）を使用することができます。

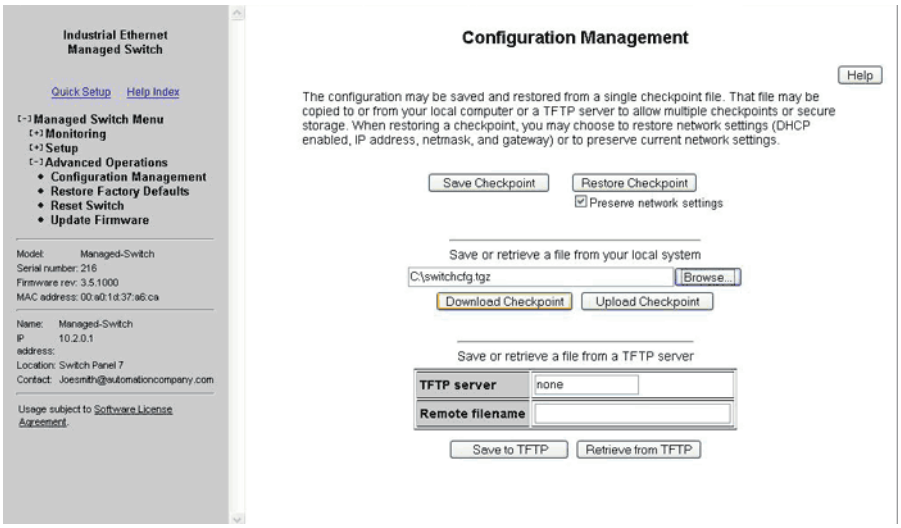
[Advanced Operations] メニューにアクセスするには、[Main menu](メイン メニュー) のオプションを選択します。

3.3.1 ファイルの保存と復元

[Configuration Management](コンフィギュレーション管理) および [Update Firmware](ファームウェアの更新) の機能により、お使いのローカル システムから直接ファイルの保存および復元をするために参照できます。これはもっとも簡単な推奨方法です。または、TFTP (トリビアル ファイル転送プロトコル) サーバを使って、コンフィギュレーションとファームウェア ファイルの保存を集約化することもできます。Windows や Linux 向けの無料 TFTP サーバが、ウェブ上で入手できます。これらは通常、インストールやセットアップが簡単です。

3.4 コンフィギュレーション マネージメント

スイッチのコンフィギュレーションの「checkpoint」(チェックポイント) された (バックアップ) バージョンは、スイッチのローカル ファイルに保存されます。お使いのローカル システム (ウェブ インターフェイスのみ) またはネットワーク上どこかの TFTP サーバであれば無制限にバックアップ保存ができます。



- **Save Checkpoint (チェックポイントの保存):** チェックポイント コンフィギュレーションをスイッチに保存します。変更により望ましくないコンフィギュレーションになってしまった場合、現在の状態に復元するために後で使用することができます。

- **Restore Checkpoint (チェックポイントの復元):** 保存されているチェックポイントの設定に戻します。ネットワーク設定については現在の設定を維持するかチェックポイント ファイルの設定を使用するかをオプションで選ぶことができます。

注 : 現在の管理者用パスワードは、復元後も引き続き有効です。SNMP パスワードは、チェックポイントの値に戻ります。

- **TFTP Configuration (TFTP コンフィギュレーション):** コンフィギュレーション チェックポイントが保存され得る TFTP(トリビアル ファイル転送プロトコル) サーバ名または IP アドレスを指定します。

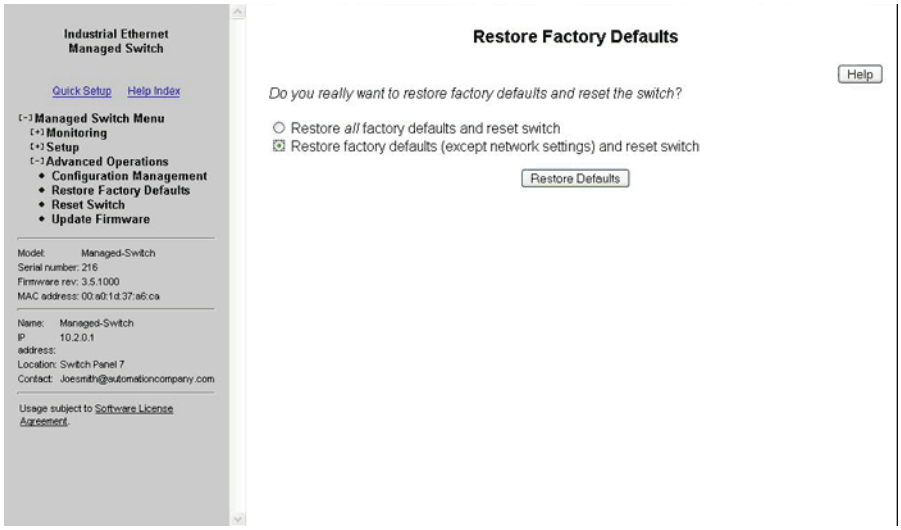
- **Save to TFTP (TFTP に保存):** 現在のコンフィギュレーション チェックポイント ファイルを、指定済み TFTP サーバに保存します。サーバ上での復元ファイル名を指定してください。

- **Retrieve from TFTP (TFTP から検索):** 以前に保存したコンフィギュレーション チェックポイント ファイルを、指定済み TFTP サーバから引出します。引出し後更に、コンフィギュレーションをアクティブな状態に回復する必要があります。

注 : ウェブ インターフェイスでも、お使いのローカル システムから直接ファイルをダウンロード (保存) およびアップロード (復元) できます。TFTP サーバは必要ありません。

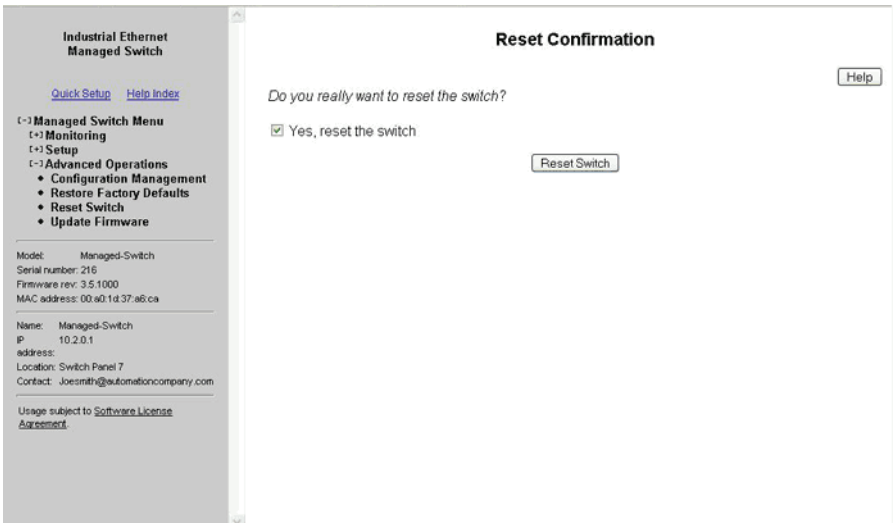
3.5 工場出荷時設定

このオプションでスイッチを工場出荷時設定に戻します。スイッチは初期設定を有効にするため、自動的に再起動 (リセット) します。



3.6　スイッチのリセット

この機能により、スイッチが「ソフト」に再起動します (ソフトウェア リセット)。ソフトウェア リセットは 30 秒以上かかることがあり、また、スイッチのどの機能が有効になっているかによってかかる時間が違います。



3.7　ウェブ インターフェイスを使用したファームウェアの更新

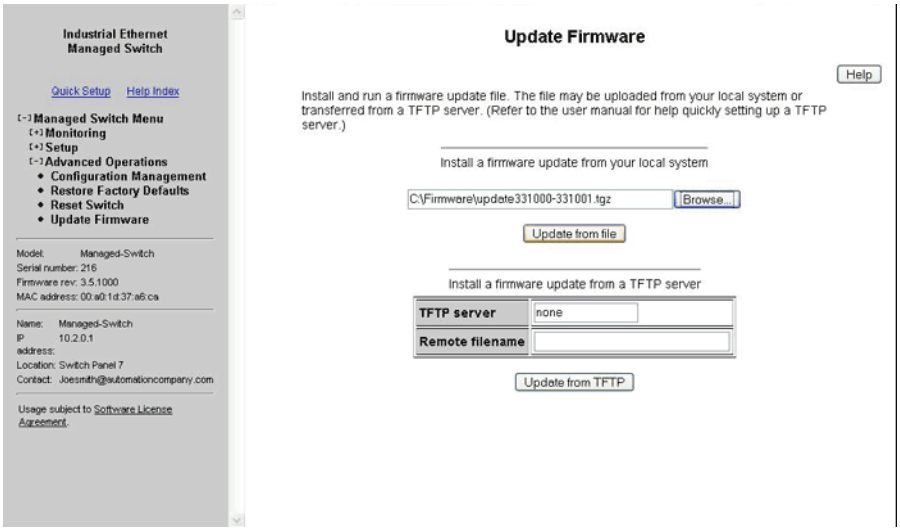
ファームウェアの更新は、機能追加および問題解決のために定期的に公開されます。もっとも簡単で推奨されているファームウェアの更新方法は、ウェブ インターフェイス経由です。ウェブ インターフェイスにより、お使いのローカル コンピューターまたはお使いのローカル ネットワーク上のコンピューターからファームウェアの更新パッケージを参照し、選択することができます。そして、[Update from File](ファイルから更新) ボタンをクリックするだけで、最新のファームウェア ファイルを読み込んでインストールできます。

このファームウェアの更新方法では、ユーザーの設定をすべて維持します。しかし、バックアップとして「チェックポイント」コンフィギュレーションの保存を推奨します。

3.8 TFTP サーバを使用したファームウェアの更新

ファームウェア更新のもう 1 つの方法は、ネットワークのどこかの TFTP サーバ経由でおこなうものです。リモート TFTP サーバの IP アドレスおよび更新するファイル名を指定するだけです。新しいファームウェア ファイルのインストール後、必要に応じてスイッチが自動的に再起動します。再起動後、「Internal Server Error」(内部サーバー エラー) のメッセージが表示されることがあります。この場合、単にブラウザの [最新の情報に更新] ボタンを押して、スイッチとの通信を回復させて下さい。

このファームウェアの更新方法では、ユーザーの設定をすべて維持します。しかし、バックアップとして「チェックポイント」コンフィギュレーションの保存を推奨します。



3.9 スイッチ ユーティリティを使用したファームウェアの更新

ウェブまたは CLI インターフェイスでスイッチにアクセスできない場合は、スイッチ ユーティリティを使用して装置を回復し、再読み込みすることができます。この操作はすべてのコンフィギュレーション設定を消去し、工場出荷時設定にします。

ファームウェアの読み込みは、ユーティリティを使って次の手順でおこないます。

1. スイッチ ユーティリティ プログラムをダウンロードし、インストールします。Java Runtime がスイッチ ユーティリティの実行に必要です。Java Runtime は、インストール手順の過程で読み込まれます。スイッチ ユーティリティは、www.sixnet.com からダウンロード可能です。

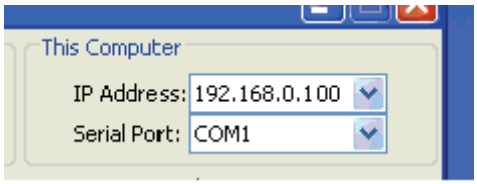
2. 最新のファームウェア バンドルを www.redlion.net からダウンロードし、お使いのパソコンの希望する場所に保存します。

3. スイッチ ユーティリティをデスクトップのショートカットから実行します。

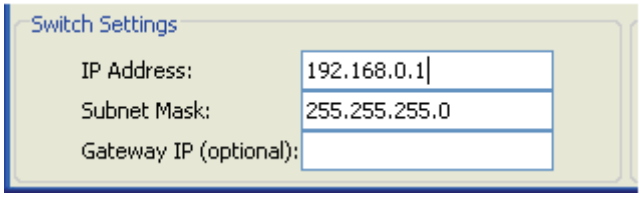
注 : スイッチ ユーティリティを開始する前に、TFTP サービスが実行中でないことと、その他のプログラムがシリアルポートを使用していないことを必ず確認してください。

4. スイッチ ユーティリティから 5.0 ファームウェア バンドルの保存場所を参照して、選択します。

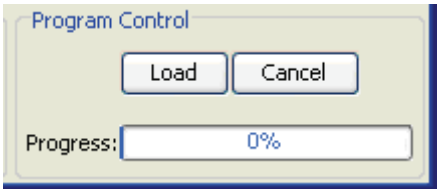
5. スイッチと通信するために使用するネットワーク アダプタ (IP アドレス)、およびシリアルポートを選択します。



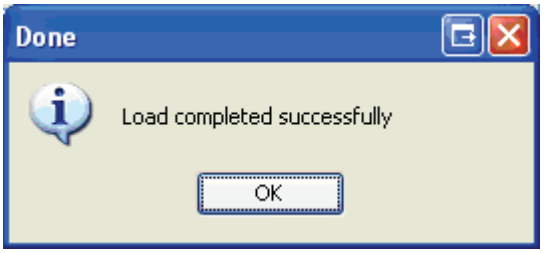
6. 新しいファームウェアが読み込まれた後、スイッチに割り当てを希望する IP アドレスを入力します。スイッチの IP アドレスは、ファームウェアの読み込み元のネットワーク アダプタと互換性のあるサブネット上に存在しなければなりません。



7. **[Load](読み込み)** ボタンをクリックして、ファームウェアの読み込みを開始します。



指示が出たら、スイッチの電源を切ってすぐに入れ直してください。ファームウェアを読み込むと、進行メーターは 100% に上昇し、読み込みが成功したことをメッセージで確認できます。

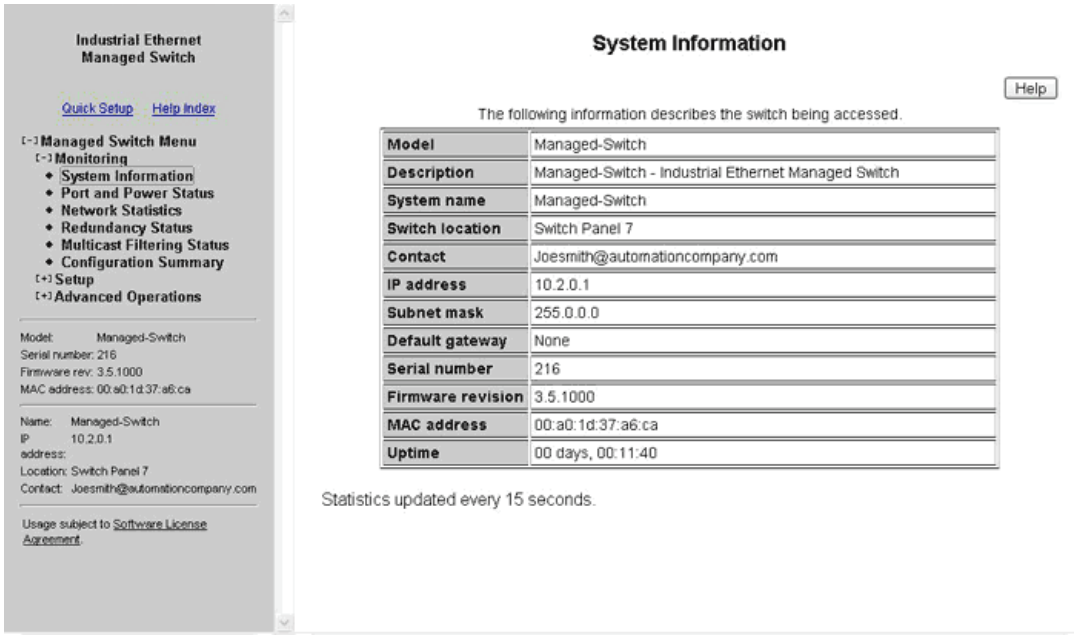


これで、ユーティリティで指定した IP アドレスで、スイッチは完全にアクセスが可能になりました。

第 4 章 スイッチの現在状況の監視

4.1 システム情報

System Information(システム情報) のページでは、スイッチの識別情報や現在のネットワーク設定が表示されます。



- **Model (モデル)** はスイッチの型番
- **Description (詳細)** は SNMP 経由で「SYSTEM.SYSDESCR.0」として利用可能。これは、スイッチの基本的な説明です。
- **System Name (システム名):** スイッチのホスト名。文字、数字、およびハイフンだけで構成されます。これは、SNMP 経由で「SYSTEM.SYSNAME.0」で読み書き可能です。
- **Switch Location (スイッチ ロケーション):** スイッチの物理的な位置。(キャビネット、クローゼット、棚など。置き場所) これは、SNMP 経由で「SYSTEM.SYSLOCATION.0」で読み書き可能です。

- **Contact (連絡先):** 通常このパラメータには、連絡先の名前と E- メールアドレスが含まれています。これは、SNMP 経由で「SYSTEM.SYSCONTACT.0」で読み書き可能です。

- **IP Address (IP アドレス):** スイッチの IP アドレス。

- **Subnet Mask (サブネット マスク):** スイッチのサブネット マスク。「RFC1213-MIB::IPADENTNETMASK.<IPADDRESS>」として SNMP 経由で読めます。<IPADDRESS> はスイッチの IP アドレスです。(例 :10.2.0.1)

- **Gateway (ゲートウェイ):** スイッチに設定されたゲートウェイ IP。「RFC1213-MIB::IPROUTENEXTHOP」として SNMP 経由で読めます。

- **Serial Number (シリアル ナンバー)** は、工場でスイッチに割り当てられた個別のシリアル ナンバーです。この番号はユーザー インターフェイスに設定することはできません。

- **Firmware Revision (ファームウェア リビジョン)** は、スイッチの現在のファームウェアのバージョンです。

- **MAC Address (MAC アドレス):** スイッチのメディア アクセス制御番号です。(設定変更不可)

- **System Up Time (システム アップタイム)** は、「SYSTEM.SYSUPTIME.0」として SNMP 経由で取得できます。これは最後にスイッチの電源が入ってからの通算時間です。

4.2 ポート ステータス

Port Status (ポート ステータス) のページでは、各ポートの現在のステータスが表示されます。5 秒ごとに表示は更新されます。

各ポートの以下の情報が表示されます。

- **Port (ポート):** ポートの数。これはスイッチのラベルに対応します。

- **Name (名前):** ユーザー設定のポート名。

- **Admin (管理):** ポートが設定されている状態（有効または無効）。

- **Link (リンク):** ポートのイーサネット リンクの現在のステータス。接続リンクの状態が良好であれば、[Up] と表示されます。ポートが無効、未接続、または接続障害の場合は、リンク ステータスは、[Down] と表示されます。

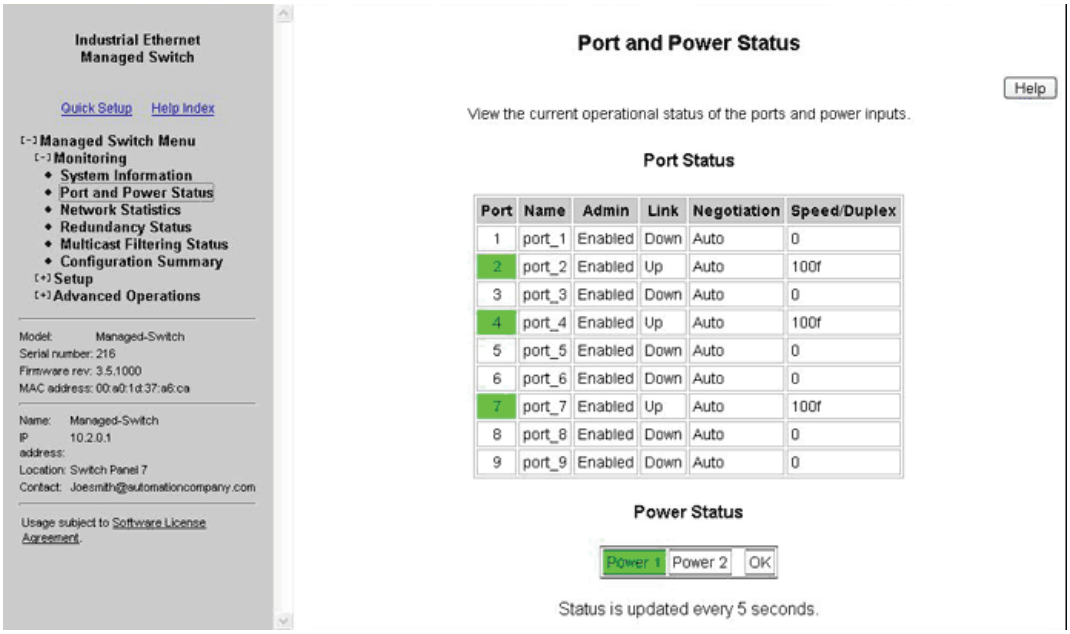
- **Negotiation (ネゴシエーション):** オート ネゴシエーションが有効 (自動) か、無効 (固定) かを表示します。

- **Speed (速度)/Duplex (双方向通信):** 接続速度 (10、100 または 1000 Mbps) と双方向通信のステータス (h = 半二重、f = 全二重) を表示します。

4.3 電源および OK ステータス

ポートステータス表の下側に、スイッチの P1 と P2、OK ステータス LED を模倣した表示があります。P1 が強調されている時は、1 つ目の入力ターミナルの電源が検出されています。P2 が強調されている時は、2 つ目の入力ターミナルの電源が検出されています。

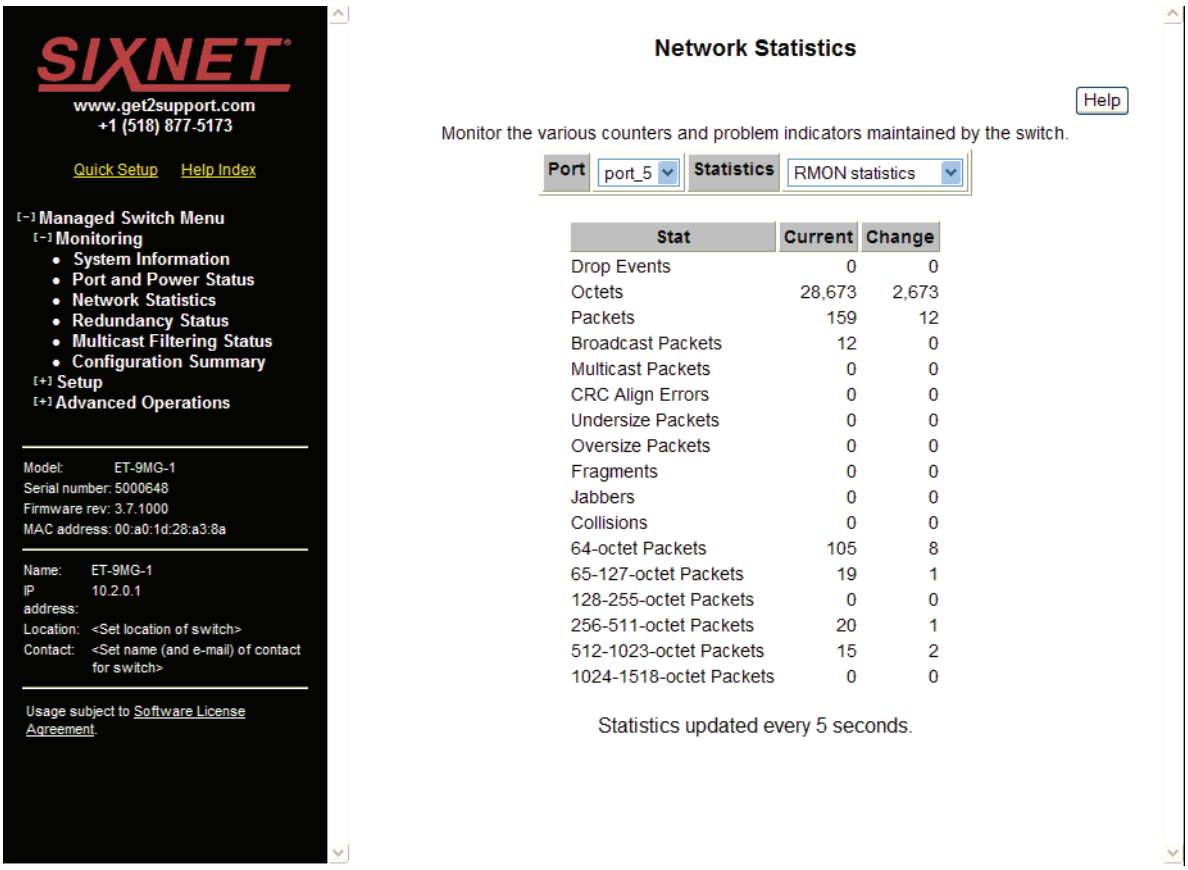
OK (SL-5MS-MDM では [To PLC]) が強調されるのは、1 つ目と 2 つ目の入力ターミナルの電源を検出し、スイッチソフトウェアが実行中の時です。OK 出力も、リングの障害や指定ポートのリンク喪失に対する警報として設定が可能です。



Port	Name	Admin	Link	Negotiation	Speed/Duplex
1	port_1	Enabled	Down	Auto	0
2	port_2	Enabled	Up	Auto	100f
3	port_3	Enabled	Down	Auto	0
4	port_4	Enabled	Up	Auto	100f
5	port_5	Enabled	Down	Auto	0
6	port_6	Enabled	Down	Auto	0
7	port_7	Enabled	Up	Auto	100f
8	port_8	Enabled	Down	Auto	0
9	port_9	Enabled	Down	Auto	0

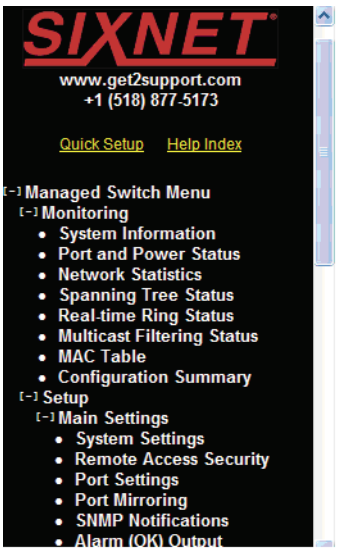
4.4 ネットワーク統計

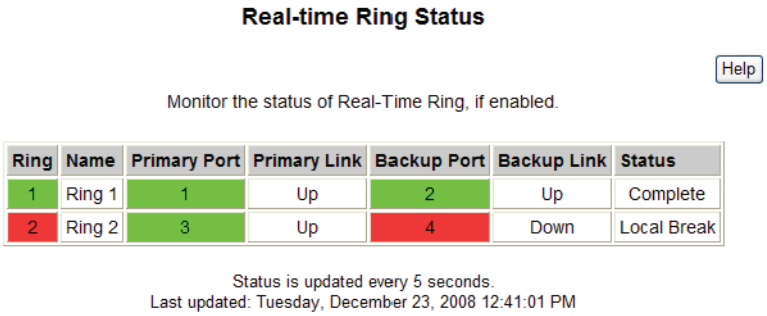
Network Statistics (ネットワーク統計) では、選択したポートのネットワーク統計を表示します。RMON か Ether-like statistics (イーサライク統計) を選択してください。表示は 5 秒ごとに更新され、前回のリフレッシュ後の差分は change (差分) の行に表示されます。



4.5 リアルタイム リング ステータス

Real-Time Ring Status (リアル タイム リング ステータス) ページで、リアル タイム リング全体の状態とともに、プライマリおよびバックアップ ポートの状態を含むスイッチに設定したリングの状態が表示されます。

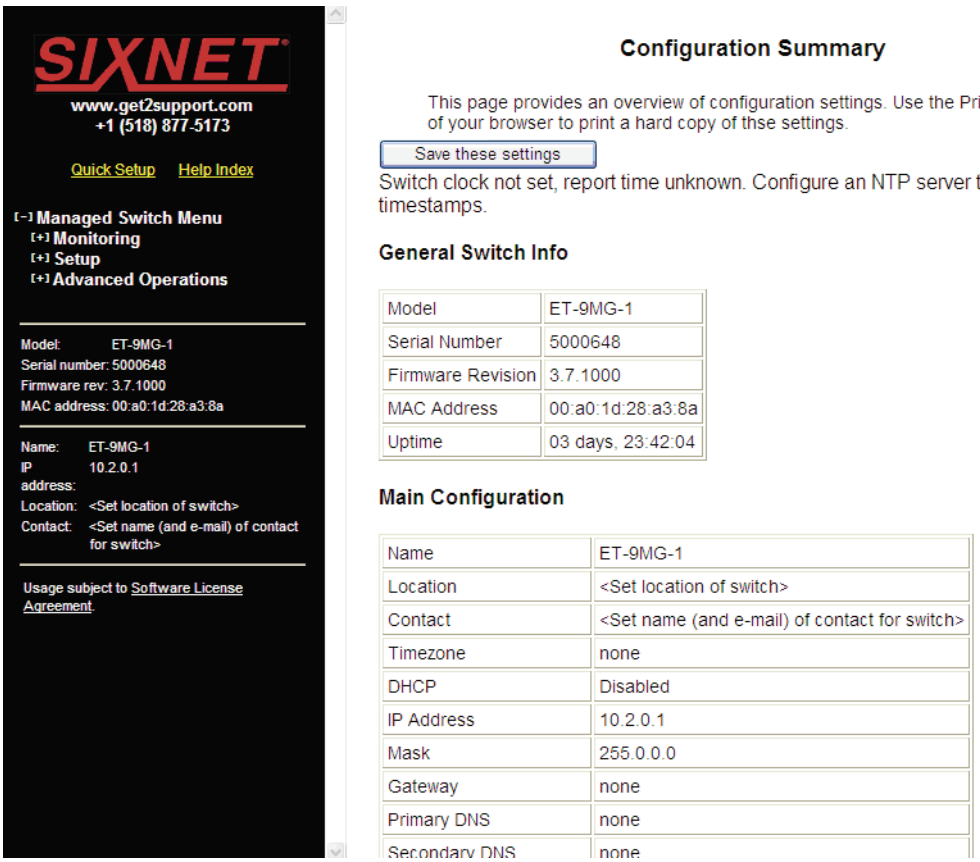




4.6 コンフィギュレーション サマリー

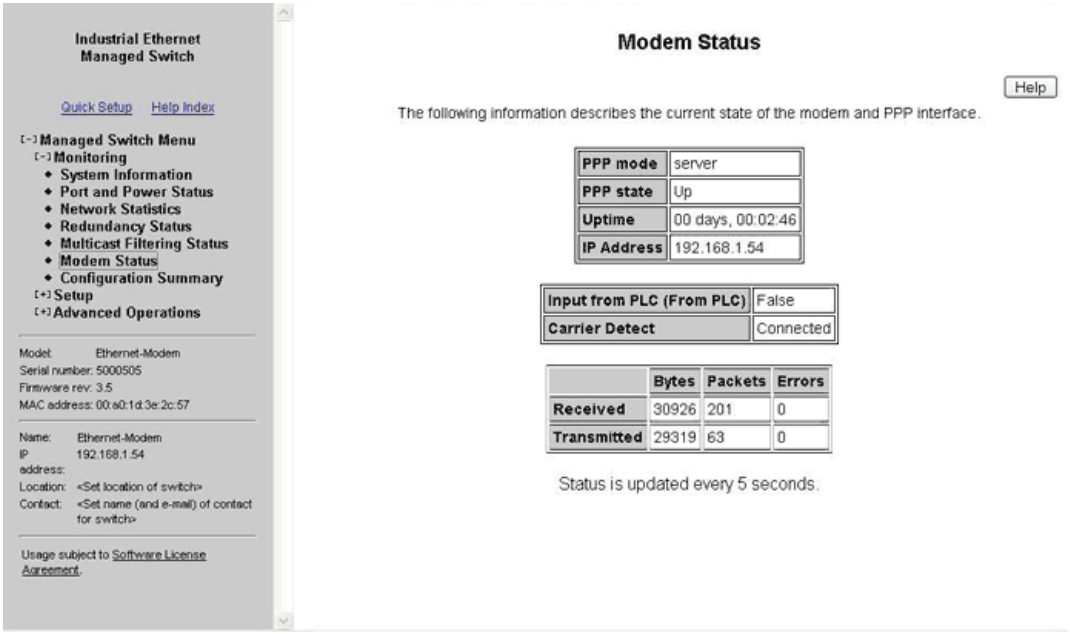
Configuration Summary (コンフィギュレーション サマリー) ページでは、スイッチのコンフィギュレーション設定の概要全体が表示されます。サマリーは、印刷しやすい書式になっています。NTP サーバが設定される場合、レポートは時刻も報告します。これらの設定をコンフィギュレーション ファイルに保存するには、[Save these settings](これらの設定を保存) ボタンをクリックし、[Configuration Management](コンフィギュレーション管理) 画面へ移動して行います。

注 : このページは設定表示のみです。設定を変更するには、それぞれのコンフィギュレーション画面を閲覧してください。



4.7 モデム ステータス

Modem Status (モデム ステータス) のページでは、PPP 接続の状態と統計が、接続したモデムの状態と一緒に表示されます。表示は 5 秒ごとに更新されます。



PPP mode (PPP モード): 5MS-MDM がクライアントまたはサーバ モードかどうかを示します。

PPP state (PPP ステータス): PPP 接続の現在の状態。Up (確立) または Down (確立していない)

Uptime (アップタイム): PPP 接続の継続時間。PPP 接続がない場合は空白になります。

IP Address (IP アドレス): PPP 接続に使用されている IP アドレス

Subnet mask (サブネット マスク): PPP 接続に使用されているサブネット マスク

Received (受信済み): PPP 接続経由で届いたバイト数、パケット数、エラー数。

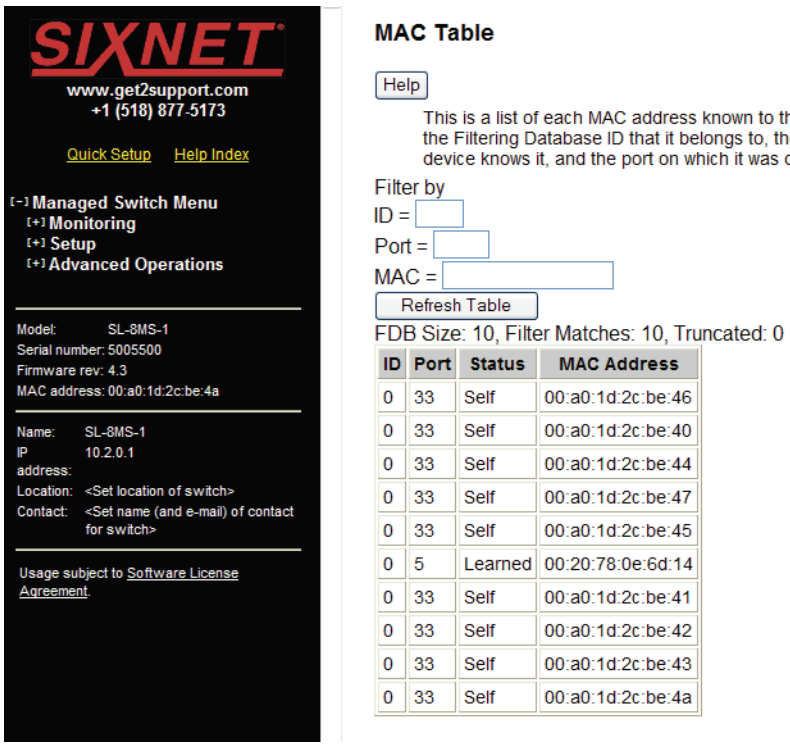
Transmitted (送信済み): PPP 接続経由で送信したバイト数、パケット数、エラー数。

Input From PLC (From PLC)(PLC から入力): SLX-5MS-MDM の「From PLC」入力状態。「TRUE」は PLC 入力 (From PLC) で電圧が検出されたときに表示されます。「FALSE」は電圧が検出されないときに表示されます。

Carrier Detect (CD)(キャリア検出): モデム接続状態を Connected (接続)、または Disconnected (未接続) で表示します。

4.8 MAC アドレス テーブル

MAC address table (MAC アドレス テーブル) のページでは、スイッチの現在の MAC アドレス テーブルが表示されます。このデータは、フィルター データベース ID(FID)、ディスカバリのポート、もしくは MAC アドレスの全体または一部に依ってフィルターをかけることができます。Port 33 または 65 は内部 CPU ポートで、モデルによって異なるので注意してください。



4.9 アラーム (OK) 出力

この設定はアラーム出力を引き起こすイベントを制御します。OK ディスクリート出力は通常の状態のときはオンになり、アラーム条件事象が発生した時はオフになります。

4.9.1 両方の電源入力がオンのとき

両方の電源入力がオフの場合、アラーム条件が発動します。

4.9.2 リング障害

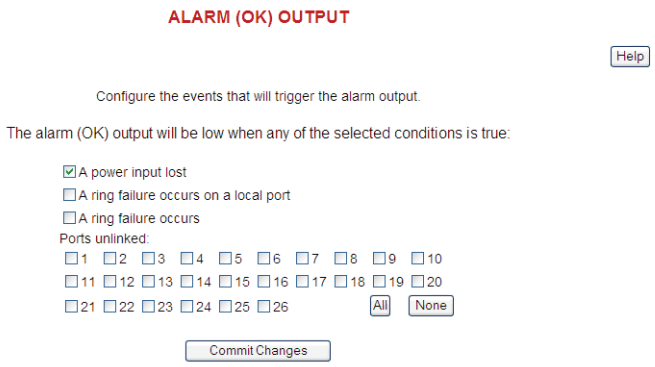
アラーム条件は、リング障害が起こると発動します。

ローカル ポートのリング障害は、リング内隣接スイッチの 1 つがダウンすると発生します。一般的なリング障害オプションは、リング内のどのスイッチがダウンしても起動します。

一般的なリング障害オプションは、ローカル リング ポート障害も検出されていることを意味します。

4.9.3 ポートがリンクしたとき

選択したいずれのポートもリンクしていないときはいつでも、アラーム条件が発動します。



4.10 Modbus 監視

この設定は、スイッチが Modbus リクエストに反応するかどうか、およびどのように反応するかを制御するものです。Modbus レジスタは、各イーサネットポートのリンク ステータス、電源および OK ステータス、ならびに各設定済みのリアルタイム リングのステータスを監視することが可能です。

4.10.1 Enabled (有効化)

選択すると、スイッチは Modbus リクエストに応対します。

4.10.2 Station Number (ステーション番号)

Modbus ステーション番号としてスイッチが応対する番号。

4.10.3 Transport Layers (トランスポート層)

選択されたトランスポート層経由のときだけ、スイッチは Modbus リクエストに応対します。

4.10.4 TCP Timeout (TCP タイムアウト)

これ以上空き接続がないときに新規 TCP 接続を受けた場合 (「**TCP 接続上限**」を参照のこと)、何をすべきかを決定します。

0 もっとも古いアクティブな接続が、新規接続のために終了します。

>0 もっとも古いアクティブな接続が、新規接続のために終了しますが、もっとも古いアクティブな接続が最低指定秒数の間、活動的でなかった場合だけです。

None 新規接続は受けた後、直ちに破棄します。

4.10.5 TCP Connection Limit (TCP 接続上限)

Modbus サーバが維持するアクティブな TCP 接続の最大数。この上限を超えると、新規接続をどのように扱うかの判断に TCP タイムアウトの値が使用されます。

4.10.6 Port (ポート)

新規接続またはリクエストを受け付けるための TCP/UDP ポート番号。

4.10.7 Register Mapping (レジスタ マッピング)

スイッチ状態をポーリングする可能性のある Modbus レジスタ (すべてディスクリート入力)

ポート 1 ～ 16 のリンク ステータス

10001	ポート 1 のリンク ステータス (1 = リンクあり、0 = リンクなし)
10002	ポート 2 のリンク ステータス
...10016	ポートのリンク ステータス (レジスタ - 10000)

リング 1 ～ 4 のリアルタイム リング ステータス

10017	リング 1: リングは完成 (1 = 完成、0 = 故障)
10018	リング 1: 最初のポートをデータが通過中 (1 = アクティブ、0 = ブロック)
10019	リング 1: 2 つ目のポートをデータが通過中 (1 = アクティブ、0 = ブロック)
10020	リング 2: リングは完成
10021	リング 2: 最初のポートをデータが通過中
10022	リング 2: 2 つ目のポートをデータが通過中
10023	リング 3: リングは完成
10024	リング 3: 最初のポートをデータが通過中
10025	リング 3: 2 つ目のポートをデータが通過中
10026	リング 4: リングは完成
10027	リング 4: 最初のポートをデータが通過中
10028	リング 4: 2 つ目のポートをデータが通過中

スイッチ ステータス

10030	OK 出力 (1 = オン / アラームなし、0 = オフ / アラーム)
10031	1 つ目の電源入力がアクティブ (1 = P1 オン、0 = P1 オフ)
10032	2 つ目の電源入力がアクティブ (1 = P2 オン、0 = P2 オフ)

ポート 1 ～ 99 の拡張リンク ステータス

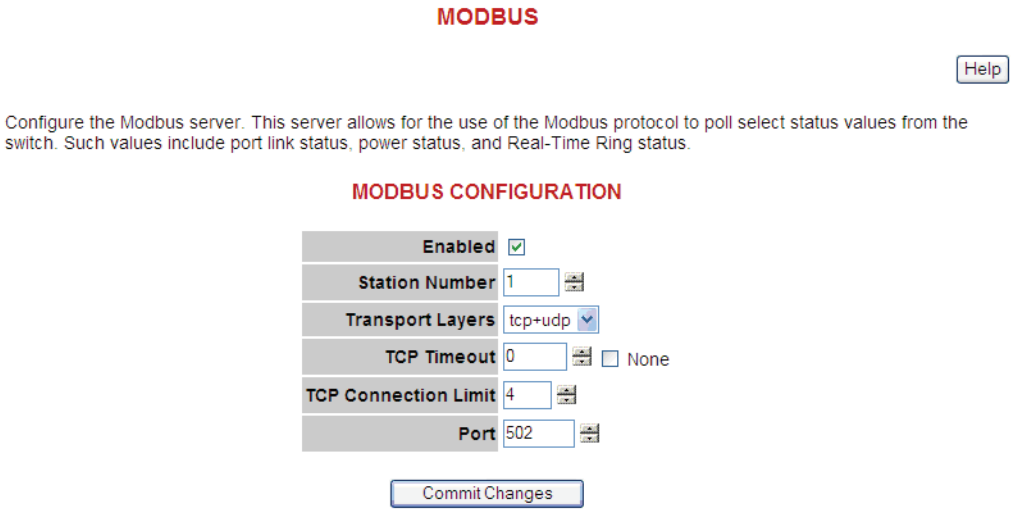
10101	ポート 1 のリンク ステータス (1 = リンクあり、0 = リンクなし)
10102	ポート 2 のリンク ステータス
...10199	ポートのリンク ステータス (レジスタ - 10100)

リング 1 ～ 25 の拡張リング ステータス

10200	リング 1: リングは完成 (1 = 完成、0 = 故障)
10201	リング 1: 最初のポートをデータが通過中 (1 = アクティブ、0 = ブロック)
10202	リング 1: 2 つ目のポートをデータが通過中 (1 = アクティブ、0 = ブロック)
10203	リング 1: 予約済み (常に 0)
...10299	リング X ステータス (X = ?(レジスタ - 10200) ÷ 4? + 1)
	10200 + (X - 1) × 4 + 0 リング X: リングは完成
	10200 + (X - 1) × 4 + 1 リング X: 最初のポートをデータが通過中
	10200 + (X - 1) × 4 + 2 リング X: 2 つ目のポートをデータが通過中
	10200 + (X - 1) × 4 + 3 リング X: 予約済み (常に 0)

拡張スイッチ ステータス

10300	OK 出力 (1 = オン / アラームなし、0 = オフ / アラーム)
10301	1 つ目の電源入力がアクティブ (1 = P1 オン、0 = P1 オフ)
10302	2 つ目の電源入力がアクティブ (1 = P2 オン、0 = P2 オフ)


MODBUS
Help
Configure the Modbus server. This server allows for the use of the Modbus protocol to poll select status values from the switch. Such values include port link status, power status, and Real-Time Ring status.
MODBUS CONFIGURATION
Enabled
Station Number 1
Transport Layers tcp+udp
TCP Timeout 0 None
TCP Connection Limit 4
Port 502
Commit Changes

第 5 章 ネットワーク管理 (SNMP および RMON)

5.1 SNMP、MIB および RMON グループ

SNMP (簡易ネットワーク管理プロトコル) および RMON (リモート監視) は、お客様のネットワークの監視および管理手段です。各 SNMP デバイスは、デバイスのオペレーションおよびコンフィギュレーションの情報を含む管理情報ベース (MIB) を維持します。

注 : 本製品は、Net-SNMP (www.net-snmp.org より入手可能) を使用します。この件に関する著作権およびライセンスについては、こちらを参照してください。
http://www.net-snmp.org/COPYING.txt

MIB には、snmpwalk や snmpget (http://www.net-snmp.org から利用可能なオープン ソース Net-SNMP パッケージの一部) などのシンプルなコマンドライン型式のツールから、さまざまな業者の市販のネットワーク管理製品までのいろいろな SNMP ツールでアクセスできます。MIB の重要な情報は、スイッチの端末やウェブ インターフェイス経由からでも入手できます。

MIB は、関連するオブジェクトのグループに分かれています。オブジェクトは、scalar (スカラー)(一つの値のみ持つ) または、tabular (表形式)(ポート番号ごとなどの経時的に変化する値のリストを持つ) です。

対応する MIB および RMON グループのリストは、「付録 D SNMP サポート」の 151 ページを参照してください。

5.2 SNMP セキュリティ

SNMP では、MIB に安全にアクセスするためにいくつかオプションがあります。SNMPv1 および SNMPv2 は、弱い認証しか提供していません。SNMPv3 は暗号化を利用して、より強いプライバシーおよび認証を追加しています。すべてのバージョンにおいて、読み取り専用または読み書きユーザーを設定できます。

SNMPv1 および SNMPv2 は平文 (非暗号化) で送信される「コミュニティ ストリング」でユーザーを認証し、パスワードは必要ありません。いくつかのセキュリティ対策は、長くて不明瞭なコミュニティ ストリングを設定することで可能です。

SNMPv3 には、3 つのセキュリティと暗号化レベルがあります。

- **None (なし)** – MIB の値の読み書きに、パスワードは必要ありません。

- **Authentication (認証)** – ユーザー資格情報を暗号化するためにパスワードが必要なので、セキュリティ情報は平文で送信されません。暗号化には変形 MD5 が使用されます。

- **Privacy (プライバシー)** – ユーザー資格情報を暗号化するためにパスワードが必要です。2 つめのパスワードは、DES 暗号化を使用した SNMP リクエスト詳細の暗号化に使用されます。

SNMPv3 アクセスは、マネージド スイッチは認証を要求し、プライバシーを維持します。1 つのパスワードだけが設定可能で、認証とプライバシーの両方に使用されます。

以下の Net-SNMP ツールの snmpget 使用例で、マネージド スイッチにアクセスする際の認証およびプライバシーの使用について説明します。

SNMPv2 アクセスが有効な場合、パスワードなしの次のようなコマンドで値を読むことができます。

```
snmpget -v 2c -c public 10.2.0.1 system.sysDescr.0
```

SNMPv3 アクセスが有効な場合、次のようなコマンドで値を読むことができます (すべて 1 行に入力)。

```
snmpget -v 3 -u public -l authNopriv -a MD5
-A publicpwd 10.2.0.1 system.sysDescr.0
```

最後に、SNMPv3 アクセスが有効な場合、認証されたプライベート リクエストは、次のようなコマンドでおこなえます。

```
snmpget -v 3 -u public -l authpriv -a MD5 -A publicpwd
-x DES -X publicpwd 10.2.0.1 system.sysDescr.0
```

スイッチは、SNMPv1、v2、および v3 に対応します。SNMPv1 および v2 アクセスは、セキュリティーの観点から本質的に同じであり、同時に有効と無効にします。SNMPv3 セキュリティは、個別に制御することができます。SNMPv1/v2 アクセスを完全に無効にすることで、スイッチへの非認証アクセスを防止しながら SNMPv3 経由のパスワード認証アクセスを維持することができます。

5.3 SNMP 通知

[SNMP Notifications Menu](SNMP 通知メニュー) を使って有効にし、スイッチの状態が変化したとき、トラップを送信する様にできます。このメニューにアクセスするには、[Main Menu](メイン メニュー) から [Setup](セットアップ) を選択し、さらに [Main Settings] (メイン設定) を選択します。

- **Authentication (認証)** – 無効な資格情報 (認識できないコミュニティ ストリングなど) が SNMP エージェントに提示されたとき、トラップを送信することができます。この設定を有効にすると、認証トラップが生成されます。

- **Topology change (トポロジー変更)** – スパニング ツリーのトポロジーが変わったときに、トラップを送信することができます。この設定を有効にすると、トポロジー変更トラップが生成されます。

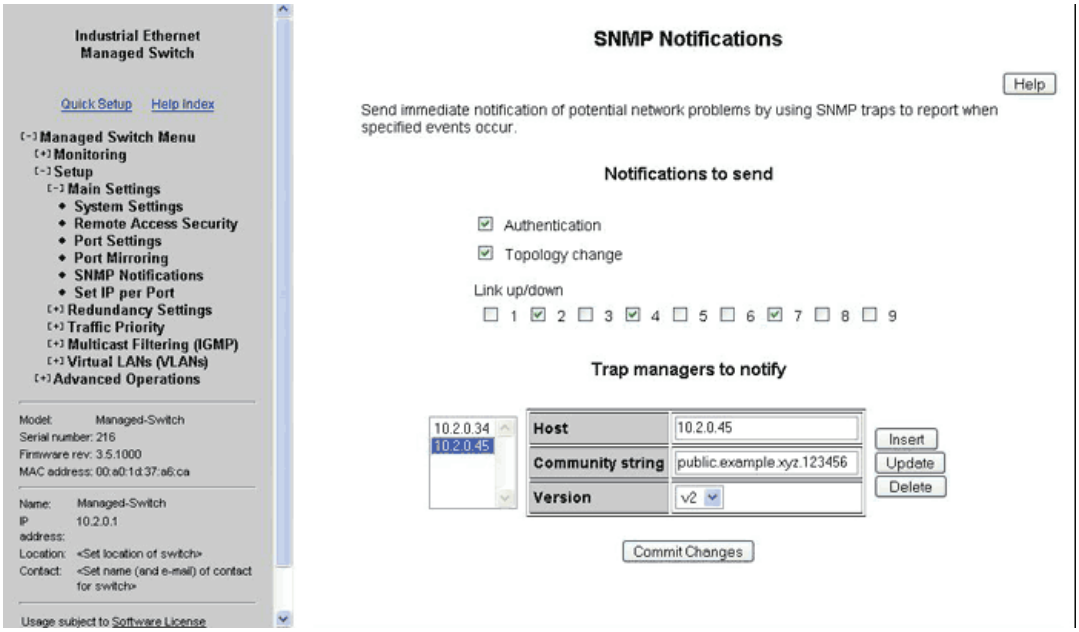
- **Link 1 up/down (リンク 1 アップ / ダウン)-Link 18 up/down (リンク 18 アップ / ダウン)** – リンクがアップまたはダウンしたとき、トラップを送信することができます。(同じ状態が各ポートの LED に反映されています) これらの設定を有効にすると、リンクアップ / ダウントラップが生成されます。

5.4 トラップ マネージャ

[Trap Managers Menu](トラップ マネージャ メニュー) を使って、どこにトラップを送信するかを指定します。[Trap Managers Menu] にアクセスするには、[Main Menu](メインメニュー) から [Setup](セットアップ) を選択し、さらに [Main Settings](メイン設定) を選択します。最大 5 個のトラップ マネージャが設定できます。それぞれ以下の値が指定できます。

- **Host (ホスト)** – トラップ マネージャが配置されているホストの IP アドレスです。
- **Community String (コミュニティ ストリング)**– ホスト上のトラップ マネージャにコンタクトを取るとき、コミュニティス トリングを使います。
- **Version (バージョン)** – 送信する SNMP トラップのバージョン。

注 : 無効にできないシステム トラップが 2 つあり、設定されたトラップ マネージャのいずれかに送信されます。coldStart (コールド スタート) トラップは SNMP エージェントが起動すると、いつでも送信されます。(通常これはスイッチがリセットされたときだけです。) NotifyRestart (通知リスタート) トラップは、SNMP エージェントのコンフィギュレーション変更や再読み込みをすると、いつでも送信されます。たとえば、コンフィギュレーション メニューで、SNMP 設定を含む変更をコミットしたときなどに起こります。

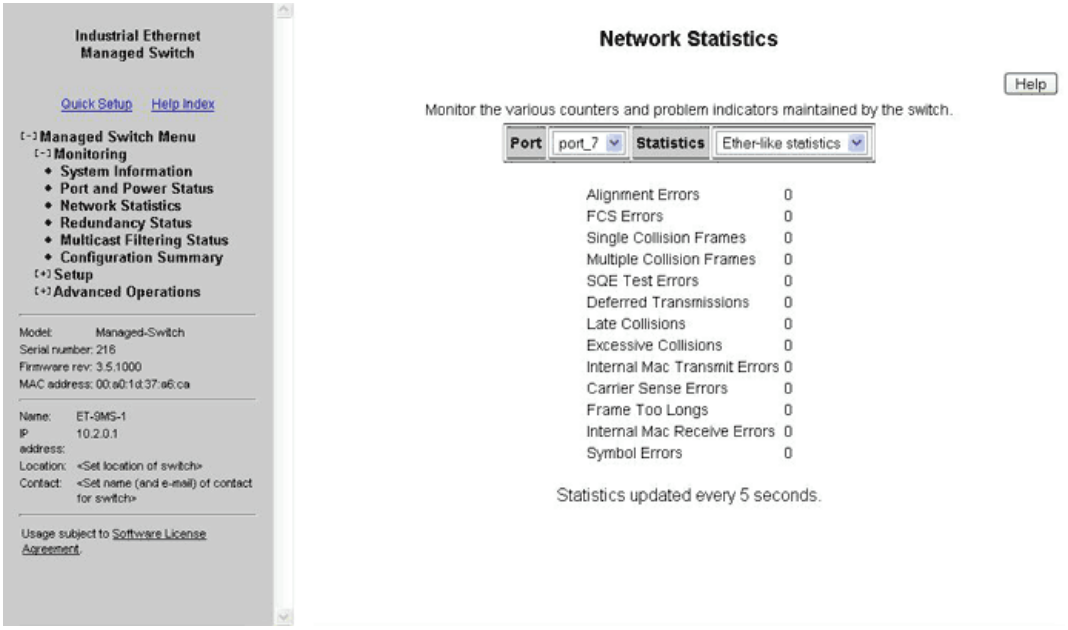


5.5 ネットワーク統計

ネットワーク統計ページは SNMP と RMON のパフォーマンス データの一部を表示します。[RMON statistics](リモート監視統計) または [Ether-like statistics](イーサライク統計) を選択し、希望するポート番号を選択します。5 秒ごとに表示は更新されます。

5.5.1 イーサライク統計

[Ether-like statistics] を選択すると、選択したポートについて、お使いのネットワークがどのように機能しているかを判断するのに使用される、さまざまなイーサネット統計が表示されます。この統計は、Dot3 MIB (RFC 2665) から得ています。



次の統計が提示されます。

- **Alignment Errors (アラインメント エラー)** – イーサネット インターフェイスが、予測した長さでない (受信パケットの CRC が無効 を含む) ために受信パケットと同期できないときに起こります。

  原因 : 干渉と減衰が原因で発生している可能性があります。誤配線、誤った NIC、または干渉、回線ノイズの可能性を確認してください。

- **FCS Errors (FCS エラー)** – このエラーは、パケットに不良フレーム チェック シーケンスが存在するために起こります。

- **Single Collision Frames (シングル コリジョン フレーム)** – イーサネット デバイスがフレームを送信しようとしたとき、ネットワーク上に最低もう 1 つ同時に送信しようとしているデバイスが存在することを発見したときに起こります。(コリジョン検出) コリジョンが検出されると、ランダムな長さの時間待った後に、ネットワーク機器は、ネットワーク媒体に再度アクセスする準備をします。イーサネット ネットワークではコリジョンはよくあることで、コリジョン検出によって、イーサネット ネットワーク上の機器が機能することができます。イーサネット機器が同じフレームを再送信しようとして成功することを、シングル コリジョンといいます。

- **Multiple Collision Frames (マルチプル コリジョン フレーム)** – マルチプル コリジョンは、イーサネット機器がネットワーク媒体を通じてフレームを送信しようとして、コリジョンを検出したときに起こります。イーサネット機器は、ネットワークを通じて同じフレームを再送信しようとしますが、また別のコリジョンに遭遇します。最初の送信を試みた後、特定のフレームが失敗するたびにエラー カウントが増えます。

- **SQE Test Errors (SQE テスト エラー)** – ネットワーク機器は、コリジョン検出回路が正常に動作しているかどうかを知るために信号品質エラー伝送を確認します。何らかの理由でネットワーク機器が SQE 伝送を検出しない場合にも、SQE テスト エラー カウンターは増えます。

- **Deferred Transmissions (送信遅延)** – 機器がネットワークにアクセスを試みたとき、ネットワーク上で他の機器がすでに送信中であるとき (コリジョンではなく、キャリア信号が検出されることによる)、送信は遅延されます。

- **Late Collisions (レイト コリジョン)**– フレーム送信を開始すると、イーサネット機器はネットワーク媒体上でコリジョンを検出しない場合、送信できると認識します。何らかの理由で、イーサネット デバイスが送信をして一定時間後、フレーム送信の最中にコリジョンを検出して送信するには完全にはクリアではなかったことに気づきます。

これをレイト コリジョンと呼びます。10BASE-T ネットワークでは、フレーム送信が始まって 51.2 マイクロ秒後にコリジョンが検出される（フレームを送信している機器によって）と、レイト コリジョンとみなされます。100BASE-T ネットワークでは、フレーム送信が始まって 5.12 マイクロ秒後にコリジョンが検出される（フレームを送信している機器によって）と、レイトコリジョンとみなされます。

原因 : レイト コリジョンは多くの場合、不適切な設定、ネットワーク機器間の規格順守上の問題、誤配線、そしてネットワーク インターフェイス カード不良などのネットワーク上の問題から発生します。

- **Excessive Collisions (過度のコリジョン)** – イーサネット機器がフレームの送信を試みてコリジョンを検出すると、同じフレームを毎回ランダムな時間待った後で再送信しようとします。イーサネット機器が特定のフレームの送信を 16 回失敗すると、イーサネット機器は送信を諦め、そのフレームは送信されません。

- **Internal MAC Transmit Errors (内部 MAC 送信エラー)** – 内部の MAC 副層での送信エラーのため、フレームの送信が正しくおこなわれないとき。

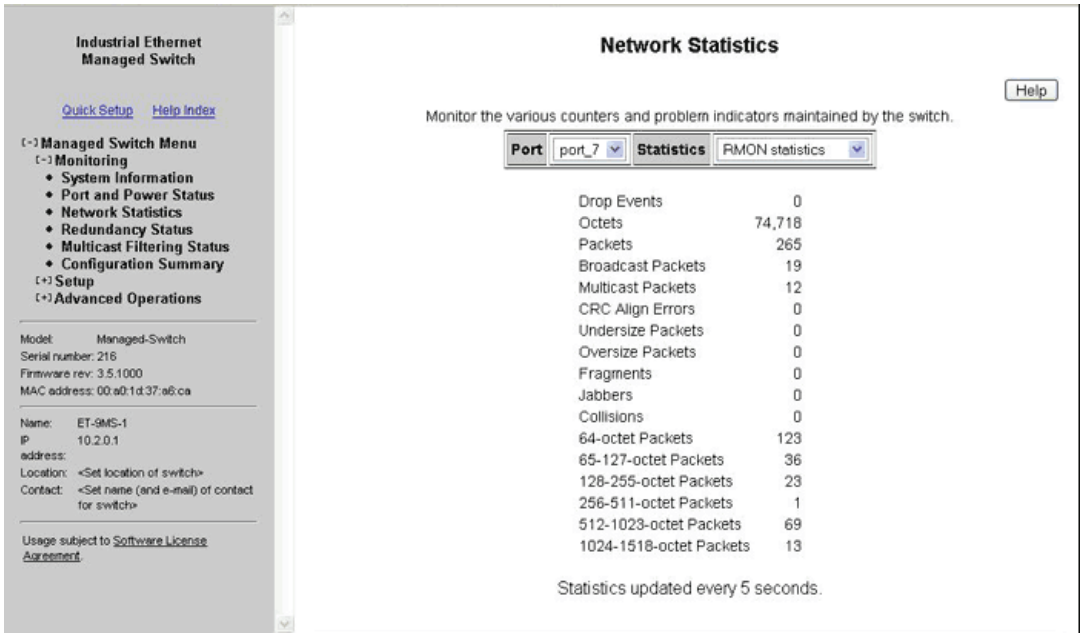
- **Carrier Sense Errors (キャリア センス エラー)** – フレーム送信時に、イーサネット機器が搬送波検知条件を失ったとき。エラーは、送信の試みごとに最高 1 回増えます。(1 回の送信の試みで、何回も搬送波検知条件が変動した場合でも)

- **Frame Too Longs (長すぎるフレーム)** – 最大フレーム サイズを超えるフレームがある毎に。

- **Internal MAC Receive Errors (内部 MAC 受信エラー)** – 内部の MAC 副層での受信エラーのため、フレームの受信が正しくおこなわれないとき。

- **Symbol Errors (シンボル エラー)** – システムが、受信したシンボルを正しくデコードできなかったときに発生します。[RMON Statistics](RMON 統計) を選択すると、選択したポートに関してネットワークがどのように機能しているかを判断するために使用される、リモート監視統計が表示されます。この統計は、RMON MIB (RFC 1757) から得ています。

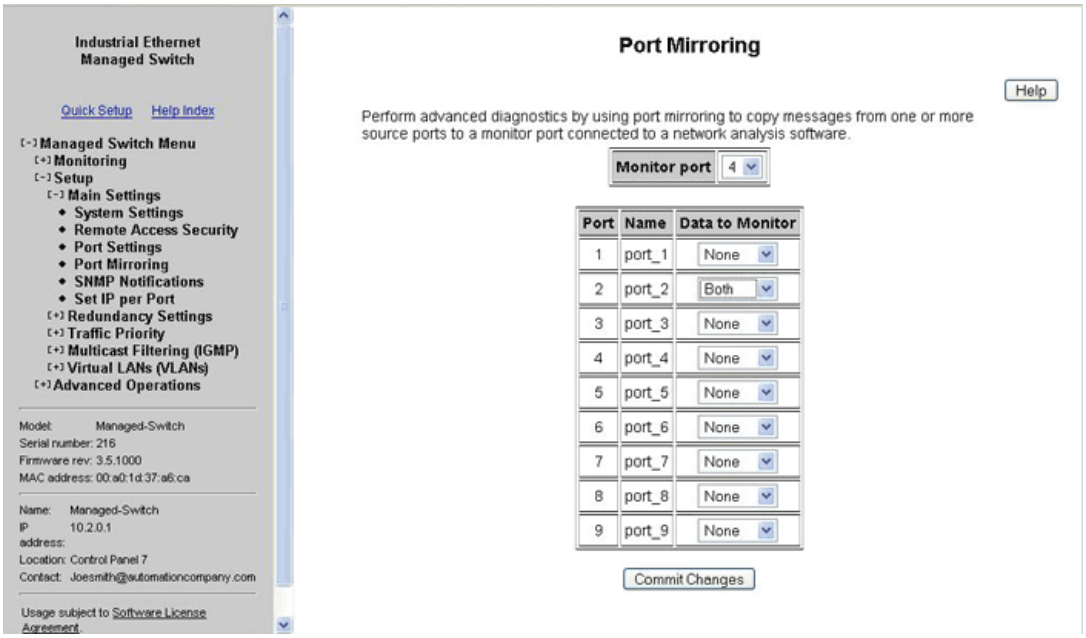
5.5.2 RMON 統計



- **Drop Events (ドロップ イベント)**: スイッチ資源不足のために、ドロップされたパケット。
- **Octets (オクテット)**: 受信したデータ オクテット数。
- **Packets (パケット)**: 受信したパケット数。
- **Broadcast Packets (ブロード キャスト パケット)**: 受信したブロード キャスト パケット数。
- **Multicast Packets (マルチ キャスト パケット)**: 受信したマルチ キャスト パケット数。
- **CRC Align Errors (CRC アラインメント エラー)**: 無効 CRC パケット受信数。
- **Undersize Packets (アンダー サイズ パケット)**: 有効 CRC で 64 バイト未満のパケット受信数。
- **Oversize Packets (オーバー サイズ パケット)**: 有効 CRC で 1536 バイト超のパケット受信数。
- **Fragments (フラグメント)**: 64 バイト未満のパケット受信数。
- **Jabbers (ジャバー)**: 無効 CRC で 1536 バイト超のパケット受信数。
- **Collisions (コリジョン)**: 検出されたコリジョン数。
- **64- octet Packets (64 オクテット パケット)**: 64 バイト サイズのパケット受信数。
- **65-127-octet Packets (65 ～ 127 オクテット パケット)**: 65 から 127 バイトのパケット受信数。
- **128-255-octet Packets (128 ～ 255 オクテット パケット)**: 128 から 255 バイトのパケット受信数。
- **256-511-octet Packets (256 ～ 511 オクテット パケット)**: 256 から 511 バイトのパケット受信数。
- **512-1023-octet Packets (512 ～ 1023 オクテット パケット)**: 512 から 1023 バイトのパケット受信数。
- **1024-1518-octet Packets (1024 ～ 1518 オクテット パケット)**: 1024 から 1518 バイトのパケット受信数。

5.6 ポート ミラーリング

ミラーリング オプションは、1 つ以上のソース ポートから送受信されるトラフィックを監視対象またはターゲット ポートに複製することで診断を実行するのに最適です。[Port Mirroring](ポート ミラーリング) メニューにアクセスするには、[Main Menu](メインメニュー) から [Setup](セットアップ) を選択し、さらに [Main Settings](メイン設定) を選択します。



ポート ミラーリング機能が有効のとき、ミラーされる (監視される) ソース ポートと、トラフィックを監視するための「シンク」ポートを選びます。各ソース ポートごとに、送信されたメッセージ ([Egress] を選択)、受信したメッセージ ([Ingress] を選択)、または送受信されたメッセージ ([Both] を選択) のどれを監視するか選びます。

上のサンプル画像では、port 4 は port 2 からのメッセージを監視しています。

5.7 アラーム (OK) 出力

OK 出力は、アラーム出力を設定することにより、様々な条件のレポートを設定できます。このディスクリート出力は通常の条件のときはハイに、アラームが起動するとローになります。OK 出力を常にオンにしておく場合には、単にすべてのアラーム オプションを無効にします。

- **Power Input Lost (電源入力の喪失):** 冗長電源入力付きのスイッチでは、電源が入力の 1 つに供給されていないと、アラーム条件が起動します。デフォルトで有効なのは、このアラームだけです。

- **Ring Failure (リング障害):** リング障害が起こると、アラーム条件が起動します。

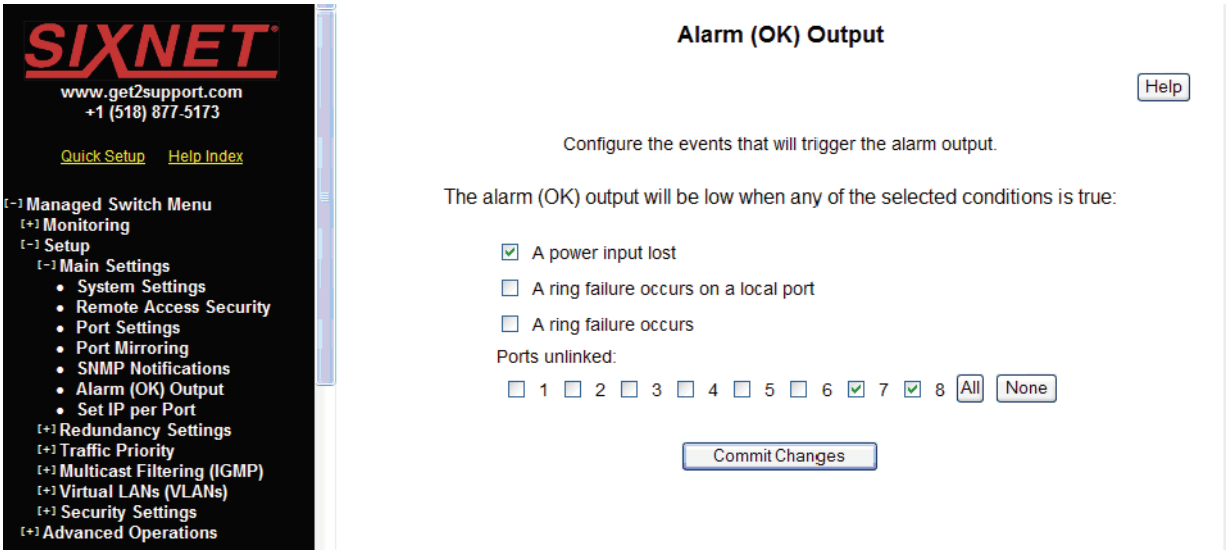
  ローカル ポートのリング障害は、リング内隣接スイッチの 1 つがダウンすると発生します。一般的なリング障害オプションは、リング内のどのスイッチがダウンしても起動します。

  一般的なリング障害オプションは、ローカル リング ポート障害も検出されていることを意味します。

- **No Carrier Detected (キャリア未検出)(-MDM モデルのみ):** 電話回線でキャリア信号が未検出のとき、アラーム条件が起動します。(例 : モデムがキャリア検出に成功すると OK 出力はハイ)

アラーム (OK) 出力

- Ports Unlinked (リンクしていないポート): アラームは 1 つ以上のポートに対して設定することができるため、選択されたポートのうちの 1 つでもリンクしていないと、OK 出力はローになります。



第 6 章 冗長プロトコル

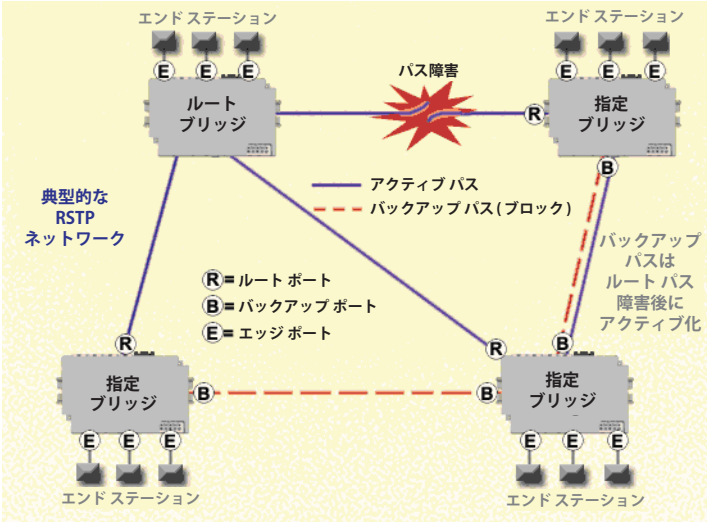
6.1 RSTP とは？

ラピッド スパニング ツリー プロトコル (RSTP) により、イーサネット ネットワークに冗長な接続を付加することができます。もし、ネットワーク上の 2 地点間の 1 つの経路が障害を起こしても、もう一つの経路をメッセージの伝達に使用することができます。もしリンクの 1 つ、またはスイッチが障害を起こしても、他のリンクまたはスイッチが使用者が気付くことなく引継ぎ、不要なダウンタイムを防ぎます。ではさまざまなループ構成でネットワーク上の各スイッチ同士を物理的につなげて、各スイッチへ、またはスイッチから最低 2 つの経路が常に出ているようにするのはどうでしょうか。一見良い考えですが、それではブロード キャストループを生成し、ネットワークがとても早くダウンするでしょう。

アンマネージド　イーサネット　ネットワークでは、ネットワーク上のいかなる 2 つのポート間で経路は 1 つだけ存在できます。1 つのスイッチから他のスイッチへ複数の経路が存在する場合は、ネットワークで送信されたブロードキャスト メッセージは（場合によっては、他のメッセージも）、2 つめの経路から戻ってきてループを完成させるまで転送され続けます。スイッチはすべてのブロードキャストを転送し、転信したメッセージの記録を残さないため、戻ってきたメッセージはループの周りを何度も何度も送信されます。ループの周りを高速で永遠に循環するシングルメッセージは明らかに良くないため、ループは認められません。

1 つの経路だけに限定することで生じる制約は簡単に理解することができます。1 つだけの経路が、ケーブル破損やスイッチの 1 つで起こる電源障害など、なんらかの理由で障害を起こすと、他に経路が無いためネットワーク トラフィックは不通になります。ループを作らないで、代わりの経路を追加しなければなりません。そのため、ループ防止プロトコルであるラピッド スパニング ツリー プロトコルを使い、スイッチ同士が通信して、ループを発見、防止できるようにします。

この図では、ルート ポートが直接ルート ブリッジに接続していて、ポート コストをもっとも低くしています (1 ホップのみ)。他のブリッジ (スイッチ) を通らなくてはいけないパスはポート コストが高く (2 ホップ)、バックアップ ポートに指定されています。直接エンド ステーションに接続されているポートは、エッジ ポートとして割り当てられていて、RSTP はこれらを考慮して通信時間を無駄にしない様にします。



ラピッド スパニング ツリー プロトコルは、ネットワーク経路を有効または無効にしてループを作らず、可能ならば代替経路も用意するという、インテリジェント スイッチ（ブリッジとも呼ぶ）向けに標準化された手法です。なぜラピッド スパニング ツリー プロトコルと呼ばれるのでしょうか？

- 「**Rapid**」**(ラピッド)** ―以前のスパニング ツリー プロトコル (STP) と呼ばれるバージョンよりも高速であるため。(完全に互換性あり)
- 「**Spanning**」**(スパニング)** ―ネットワークのすべてのステーションとスイッチをスパン (接続) するため。
- 「**Tree**」**(ツリー)** ―分技によって、2 地点間に 1 つの接続のみを提供するため。

スパニング ツリー ネットワークでは、LAN にループが存在しないようにするため、1 つのブリッジだけ (マネージド スイッチ) が、2 つの隣接 LAN セグメント間でのパケット転送に責任を持ちます。1 つのブリッジだけに任せるために、ネットワーク上の他のすべてのブリッジはお互いに協力し合って論理スパニング ツリーを構築し、パケットがブリッジからブリッジへ届くような経路を定義します。

論理スパニング ツリーでは 1 つのブリッジだけが、ルートの役割を担います。他のすべてのブリッジは、ルートへの 1 つだけのアクティブ経路を持つ必要があります。ルート ブリッジの役割は、ツリーに接続されたすべてのブリッジに、トポロジー変更やツリー再構築中であることの通知をすることです (ネットワークのどこかの通信リンク障害のため)。ルート ブリッジは、設定されたブリッジの優先順位と MAC アドレスによって決定されます。

デフォルトでは、最小の MAC アドレスを持つブリッジに、ルートの役割が割り当てられます。しかし、ブリッジの優先順位設定を変更することにより、特定のブリッジをルートブリッジにさせることができます。(他のブリッジより小さい番号の方が優先順位が高い)

ネットワーク上の各ブリッジ (マネージド スイッチ) 間のすべての通信経路には、関連コストがあります。この「path cost」(パス コスト) は、速度が遅いとデータを転送するのに時間が余計にかかるので、各セグメントの速度によって決定されます。パス コストは、特定ネットワークの使用を促進したり抑制したりする様に設定できます。例えば、本当に必要なとき以外は特定のデータ課金される高速リンクを使用したくない一方、他のパスは無料といった場合です。

ルート パス コストは、ネットワーク上のルート ブリッジから特定のポートまでのすべてのネットワーク パスの累積コストです。スパニング ツリー ネットワークは常に、ポートとルート ブリッジ間で利用可能な一番低いコスト パスを使用します。利用可能なネットワーク接続が変更になると、必要に応じて再構築を行います。

この章の RSTP トピック例は、一次接続およびバックアップ接続の確立にどのようにパス コストが利用できるかの例として参照してください。

スパニング ツリー ネットワークのスタートアップ中は、すべてのブリッジ (マネージド スイッチ) は、ルートになることを主張するコンフィギュレーション メッセージ (BPDU) を送信します。スイッチが BPDU を受信し、それが自分が送信しているものよりも「優れている」場合は、ただちにルートになるための主張を中止し、代わりに「優れている」ルート情報を送信します。稼働しているネットワーク セグメントが実際にすべてのスイッチに接続していると仮定して、一定時間後には、自分のルート情報を送信しているスイッチは 1 つだけになり、このブリッジがルートになります。他のすべてのスイッチは、ルート ブリッジのハロー間隔か、ポートの 1 つでルートブリッジの BPDU を受信したときに、ルート ブリッジ情報を送信します。

どのスイッチがルート (「もっとも優れている」ルート情報を持つ) なのかを決定するただ 1 つの要因は、ブリッジの優先度と、優先度が同じ場合そのスイッチ MAC アドレスです。スイッチが、ルートからメッセージを得るための経路を 1 つ以上持つ場合は、コンフィギュレーション メッセージの他の情報でどのパスが一番良いか決定します。

ルート ブリッジが決定したら、他のすべてのスイッチは、ルート ブリッジ情報およびルートへの経路についての情報を見ることができます。1 つ以上のポートが、ルートへの経路を提供する場合は、非ルートスイッチはどのポートを使うのか決めなければなりません。すべてのポートを確認して、ルートへの一番良い経路を示すメッセージを受信しているポートを選びます。

各ブリッジで選ばれたポートは、ルート ポートと呼ばれます。ルートと通信するための一番良い経路を提供しています。一番良い経路はまず、ルートにとって一番低い総合パス コストによって決まります。(ルート パス コスト) 各ポートには、ポートでメッセージを受信するためのコスト (通常、速度が基準) を割り当てられます。与えられた経路のためのルート パス コストは、経路の個別ポート コストの合計です。一番低いパス コストは、ルートへの最短で最速の経路を意味します。同じコストを持つ複数の経路がある場合、各ポートに設定されたポート優先度と優先度が同じ場合ポート番号が一番良い経路を選択します。

6.2 リカバリタイム、ホップおよび収束時間

リンク喪失不具合における典型的な RSTP リカバリタイム (バックアップ ポートにメッセージを転送し始める時間) は、「hop」(ホップ) につき <50 ミリ秒です (ファームウェア バージョン 3.1 以降)。ホップは、2 つのスイッチ間のリンクで定義されます。エンド ステーションへのリンクは、ホップとはみなされません。

Max Age (最大エージタイム) 設定は、RSTP メッセージがどれくらいネットワーク内を巡回するかを制御します。Max Age の最大値は 40 のため、RSTP ネットワーク ホップ直径の最大値も 40 です。

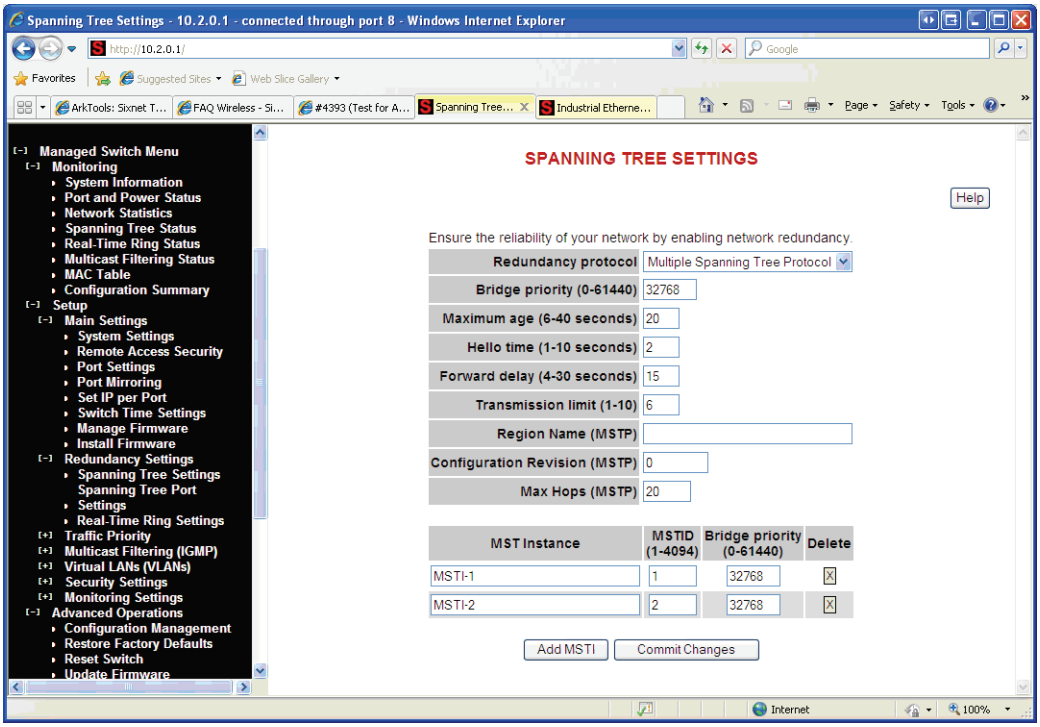
この章の RSTP トピック例では、ホップとリカバリタイムについての詳細が説明されていますので、参照してください。

すべてのスイッチが安定したコンフィギュレーションになり、ネットワーク トラフィックを送信するのにかかる時間は、収束時間と呼ばれます。STP は、収束時間が 1 分以上許されていた時代に開発されましたが、もうそんなことは許されなくなりました。よりよい収束時間への要望の高まりで、ラピッド スパニング ツリー プロトコルが開発され、適切に設定されたネットワークの通常の収束時間は数秒に減少しました。RSTP は、最新のイーサネット リンクは、スイッチ間がポイント ツー ポイント接続であるという事実を利用しています。ポイント ツー ポイント リンクでは、スイッチはリンクがアクティブであるべきか否か素早く決定できます。

6.3 Spanning Tree Settings (スパニング ツリー設定)

スパニング ツリー設定により、冗長プロトコルの選択およびプロトコルに関連するパラメータの設定が可能になります。

スパニング ツリー設定には、[Managed Switch Menu](マネージド スイッチ メニュー) → [Main Settings](メイン設定) → [Setup](セットアップ) → [Redundancy Settings](冗長設定) → [Spanning Tree Settings](スパニング ツリー設定) の順にアクセスしてください。



6.3.1 Redundancy Protocol (冗長プロトコル)(デフォルト = Rapid Spanning Tree Protocol (ラピッド スパニング ツリー プロトコル))

STP (スパニング ツリー プロトコル)、RSTP (ラピッド スパニング ツリー プロトコル) または MSTP (マルチプル スパニング ツリー プロトコル) からプロトコルを選びます。「None」を選択すると、この上級機能を無効にします。STP、RSTP または MSTP を選択することで、自動フェイルオーバーのための冗長ネットワークの配線 (リングなど) が可能になります。RSTP は STP と互換性があるので、多くの場合 RSTP だけを選択できます。STP を選択するのは、このプロトコルだけをスイッチに使用させたいときのみです。STP、RSTP、MSTP は、ネットワーク ステータスをブリッジに報告し続けるために、BPDU (ブリッジ プロトコル データ ユニット) を使用します。

MSTP は RSTP および STP と互換性がありますが、MSTP リージョン内の個別のスパニング ツリー群の VLAN の経路を決める能力があります。スパニング ツリー群を設定するために、STP コンフィギュレーション ページでスパニング ツリー インスタンス群を作成し、VLAN コンフィギュレーション ページでそれらに VLAN を割り当てなければなりません。

MSTP は MSTP リージョン外では RSTP の動作にフォールバックします。リージョンは、リージョン名、コンフィギュレーション リビジョン、そのリージョン内の各スイッチのための VLAN/MSTI 間マッピングの固有の組み合わせで特定されます。これらの値が MSTP を実行中のリンクされたスイッチと一致する場合は、そのスイッチは同じリージョン内にあると認識します。

注意 : VLAN と冗長化 (STP/RSTP/MSTP) が両方とも有効な場合は、物理 LAN に障害がないのに 1 つ以上の VLAN が冗長化アルゴリズムによってブロックされ、この VLAN 経由の通信が不能になる問題が起こることがあります。最良の方法は、常時接続性を保つために、すべてのスイッチ間接続をすべて VLAN メンバーにすることです。

スイッチの冗長ネットワーク接続管理が必要がなければ、[none](なし) を選択します。すべてのポートは、アンマネージド スイッチと同じように、ネットワーク トラフィックを転送します。そうでなければ、通常は RSTP (ラピッド スパニング ツリー プロトコル) を選択してください。STP または RSTP の選択により、スイッチ間の冗長化リンクが許可されるので、プライマリ リンク障害のときでも、リンクがネットワーク接続状態を保ちます。RSTP は、プロトコルの古いバージョンである平易な STP のみ実装しているスイッチと互換性があります。STP が選択されると、オリジナル STP フォーマット メッセージのみが生成されます。 STP を選択することで、ネットワーク パケットの重複や順番の乱れたネットワークパケットを送信される可能性は減りますが、その代わりリコンフィギュレーション タイムがかなり長くなります。

注 : RSTP と VLAN を同時に使用するときは、84 ページの「9.4 VLAN つき RSTP」のネットワーク設定に関する重要情報を参照してください。そうしないと、通信障害が起こる可能性があります。

6.3.2 Bridge Priority (ブリッジ優先度)(0 ～ 61440、デフォルト =32768

ブリッジ優先度は、スパニング ツリーのルート ブリッジを決定するのに使用されます。(MSTP には、CIST ルートの決定にブリッジ優先度が使用されます) 優先度の範囲は 0 から 61440 で (デフォルトは 32768)、4096 の倍数でなければなりません。若い番号は、より好ましい優先度を示します。

デフォルトでは、ブリッジ優先度番号のもっとも若いブリッジがルートに選ばれます。同じ優先度のブリッジが他にもある場合は、優先度番号がもっとも若くて、一番小さい MAC アドレスを持つブリッジが選ばれます。

ルート ブリッジ (スイッチ) の選択方法は、2 種類あります。1 つめは、すべてのブリッジ優先度設定をデフォルト設定の 32768 にしておくことです。すべてのスイッチをデフォルトの優先度に設定しておくと、一番小さい MAC アドレスを持つマネージド スイッチがルートに選ばれます。これは、簡便な、またはトラフィックが平均的に分散しているネットワークに適しています。

2 つめのルート ブリッジの選択方法は、各ブリッジの優先度設定をカスタマイズすることです。ブリッジ優先度設定のカスタマイズにより、ネットワークは、最高のネットワーク パフォーマンスをもたらすルート ブリッジを選ぶことができます。目標は一般的に、ネットワーク トラフィックが可能な限り直接ネットワークを通過することなので、ルートをネットワークの中心にします。ほとんどのメッセージが中央サーバと複数のクライアント間である場合は、おそらく、ルートはサーバのそばのスイッチになるので、メッセージがルートまでの長いパスを通ったり、別の長いパスを通ってサーバへ戻ったりということがありません。

どのスイッチをルートするか決めたら、ネットワークで一番好ましい (もっとも小さい数字) ブリッジ優先度番号を与えます。

6.3.3 Maximum Age (最大エージタイム)(6 ～ 40、デフォルト = 20)

STP の最大エージタイムは、スイッチが他のマネージド スイッチからのコンフィギュレーション メッセージを待つことができる最大の時間 (秒) を示します。時間切れの場合は、スイッチはネットワークのルートにこれ以上接続していないと判断します。スイッチがリンク 喪失を検出できる形でリンクダウンした場合、ネットワークは時間を置かず再構築されます。

RSTP は、スイッチがネットワークのルートにこれ以上接続していないと判断する前に、最大エージタイムの替わりにハロー間隔を 3 回待ちます。しかし、最大エージタイムは、無効だと判断され破棄される前にルートブリッジから伝送するスパニング ツリー情報のホップ数を制限するのに使用されます。さらに、MSTP は、このチェックのために MSTP リージョン外のスイッチへ生じる、またはそこから生じるホップ数をカウントするだけです。次に示す最大ホップ数の値は、MSTP リージョン内のホップ数を制限するのに使用されます。

注 : RSTP/STP ネットワークのすべてのスイッチに同じ最大エージタイムを割り当てます。

最大エージタイムは、下記の制約を満たさなければなりません。

2 x (ハロー間隔 + 1.0 秒) ≤ 最大メッセージエージ ≤ 2 x (転送遅延タイム - 1.0 秒)

6.3.4 Hello Time (ハロー間隔)(1 ～ 10、デフォルト = 2)

コンフィギュレーション メッセージ (BPDU) は、ハロー間隔で設定された期間に基づいて、定期的に他のブリッジに送信されます。ハロー間隔を減らすことで、リカバリタイムが速くなります。また、ハロー間隔を増やすと関連するオーバーヘッドが減少します。

ハロー間隔は、下記の制約を満たさなければなりません。

2 x (ハロー間隔 + 1.0 秒) ≤ 最大メッセージエージ ≤ 2 x (転送遅延タイム - 1.0 秒)

6.3.5 Forward Delay (転送遅延タイム)(4 ～ 30、デフォルト = 15)

転送遅延タイムは、ネットワークのすべてのスイッチで使われる時間 (秒) です。この値はルート ブリッジによって制御され、ネットワーク トポロジーの変化後、ポートがトラフィックを転送し始められるよう、タイムアウト値として使われます。ポートがエッジ ポートとして設定されておらず、RSTP がリンク ステータスを交渉できない場合は、ポートはネットワーク トラフィック転送前に転送遅延タイムの 2 倍の時間待たなければなりません。RSTP (STP ではない) を使用する適切に設定されたネットワークでは、この設定はごくわずかな影響しかありません。STP ネットワークでは、ネットワーク構造が変化するとき (スイッチのオン、オフ、またはリンクが追加されたか壊れている)、設定時間が短すぎると仮ループを許可します。長い設定時間は仮ループを防ぎますが、ネットワーク トラフィックはより長い時間中断されます。

転送遅延タイムのデフォルト値は 15 秒です。この設定を変更する場合、スイッチは次の公式を満たさない限り値を許可しません。

2 x (ハロー間隔 + 1.0 秒) ≤ 最大メッセージエージ ≤ 2 x (転送遅延タイム - 1.0 秒)

6.3.6 Transmission Limit (伝送限界)(1 ～ 10、デフォルト = 6)

伝送限界は 1 秒で送信できる BPDU の最大数を制御します。

伝送限界は、毎秒 1 から 10 メッセージで値を定めることが可能です。(デフォルトは毎秒 6 メッセージ) 伝送限界を増加すると、ネットワークの収束時間を早めることができますが、コンフィギュレーション メッセージが利用可能なネットワーク帯域をより多く使ってしまうという代償を払うことになります。

6.3.7 Region Name (リージョン名)(MSTP)

リージョン名は、コンフィギュレーション リビジョンおよび MSTP リージョンを定義するための VLAN/MSTI 間マッピングと共に使用されます。

6.3.8 Configuration Revision (コンフィギュレーション リビジョン)(MSTP、0 ～ 65535)

コンフィギュレーション リビジョンは、リージョン名および MSTP リージョンを定義するための VLAN/MSTI 間マッピングと共に使用されます。

6.3.9 Max Hops (最大ホップ数)(MSTP、6 ～ 40、デフォルト = 20)

最大ホップ数は、MSTP リージョン内を BPDU が伝搬するスイッチの最大数を決定します。この値は古いデータがリージョン内で延々と循環することを防ぐために使用されます。

6.3.10 MST インスタンス

MSTP には、マルチプル スパニング ツリー インスタンスを設定できます。[Add MSTI](MSTI の追加) をクリックして、インスタンスを追加します。
各 MSTP には、名前、MST ID、およびスパニング ツリー インスタンスでのこのブリッジの優先度設定が可能です。

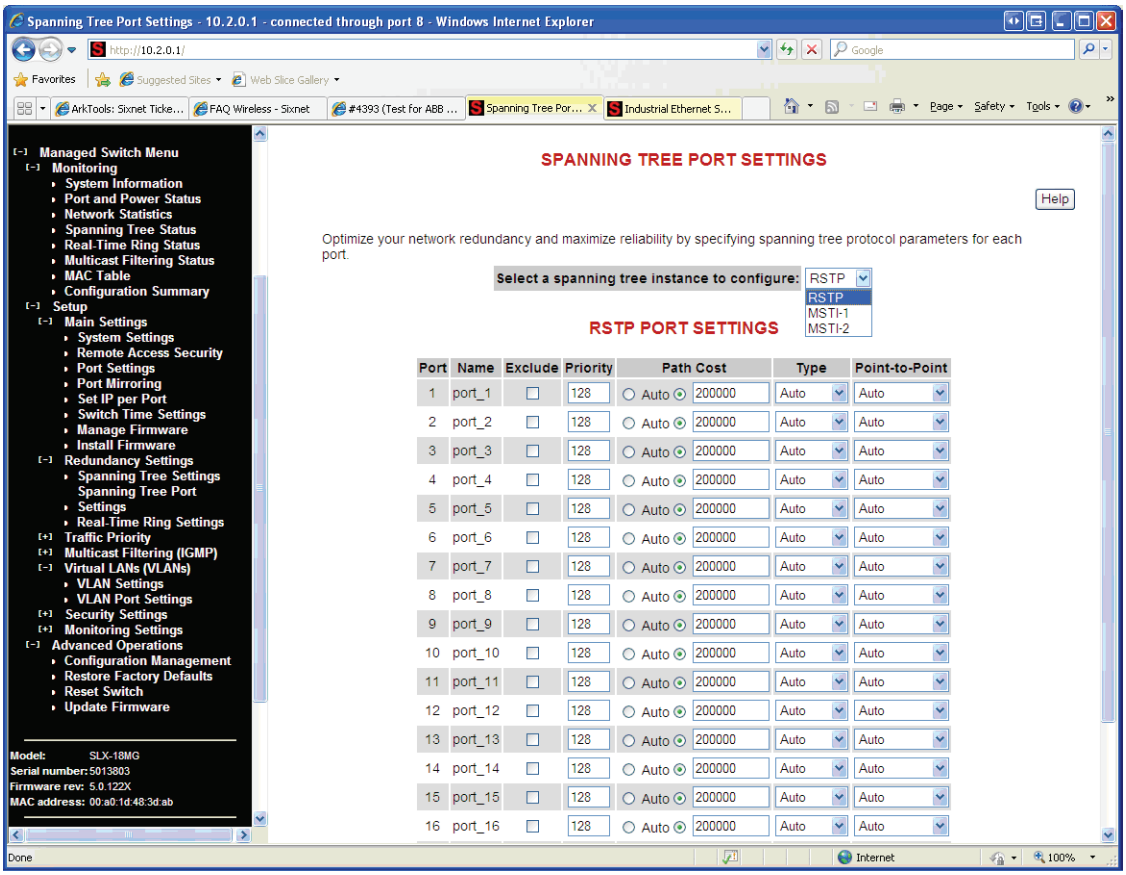
6.4 スパニング ツリー ポート設定

各ポートは STP、RSTP、MSTP スパニング ツリーを整調するための設定ができます。MSTP では各スパニング ツリー インスタンスを個別に調整することが可能です。

MSTP を使用して、CIST (Common Internal Spanning Tree) および MSTP に作成されたスパニング ツリー毎に個別にポート設定ができます。個々の MSTI (マルチプル スパニング ツリー インスタンス) の設定は、同じ MSTP リージョン内のスイッチに接続しているポートにのみ影響します。

デフォルトでは、MSTI は CIST から設定を引き継ぎます。MSTI を個別に設定するためには、ドロップダウンボックスから選択し、インスタンスのための [Customize](カスタマイズ) ボタンをクリックします。スパニング ツリーの値を再び CIST から引き継ぎたいときは、[Inherit](引き継ぎ) をクリックします。

スパニング ツリー ポート設定には、[Menu](メニュー) → [Main Settings](メイン設定) → [Setup](セットアップ) → [Redundancy Settings](冗長設定) → [Spanning Tree Port](スパニング ツリー ポート) の順にアクセスしてください。



次項では、各ポートの設定を説明します。

6.4.1 Exclude (除外)(デフォルト = 含む)

通常、すべてのポートはノーマル ポートまたはエッジ ポートとして、スパニング ツリー ネットワーク トポロジーを決定する場合に含まれています。完全にポートを除外することが可能ですが、その場合、常にネットワーク トラフィックは転送し、決して RSTP または STP のネットワーク メッセージの生成または応答をしません。ポートの除外は高度なオプションなので、本当に必要なとき以外使用しないでください。

このオプションはポートをすべてのスパニング ツリー インスタンスから除外しますが、その他の CIST 設定に表示されます。

6.4.2 Port Priority (ポート優先度)(0 ～ 240、デフォルト = 128)

2 つのポートがループ状に接続されている場合、一番若いポート優先度のポートという原則に基づいて「ルート」となるポートの選択は割り当てられます。ルートブリッジが障害を起こした場合、次に若い優先度のブリッジがルートになります。

このオプションは、各 MSTI のポートごとに設定できます。

スイッチがルート ブリッジへのパスを提供する複数のポートを持ち、それらのルート パス コストが同じ場合は、どのポートを使用するかの選択はポート優先度を基準にします。一番好ましい優先度（一番若い数字）のポートが使用されます。ポート優先度が同じ場合は、スイッチはもっとも小さい番号のポートを使います。ポート優先度は、0 から 240 秒の値を取ることができます。（デフォルトは 128 秒）

6.4.3 Path Cost (パス コスト)(1 ～ 200,000,000)

あらゆるネットワークと同様に、ソース ロケーションからターゲット ロケーションまで行くためにかかる関連コストがあります。RSTP では、ルート パス コストは、ルート ブリッジへの特定の接続で利用可能な帯域に基づき計算されます。ルートへメッセージを送信するコストが一番低いポートが、トラフィックをルートへ送る場合に使用されます。

パス コストは 100Mbps リンクは 200,000、また 10Mbps リンクは 2,000,000 というポート速度に基づく IEEE 標準値が自動的に割り当てられますが、1 から 200,000,000 の範囲で指定することができます。

このオプションは各 MSTI のポートごとに設定できます。

一次接続とバックアップ接続の確立にどのようにパス コストが利用できるかの例として、59 ページの「6.8 RSTP 例」を参照してください。

6.4.4 Type (タイプ)(デフォルト = Auto (自動))

ネットワーク上の他のスイッチに接続するポートは、ループの一部の可能性があります。このようなループが発生しないようにするために、スパニング ツリーが安定するために十分な時間が経過するまで (転送遅延値の 2 倍。デフォルトは 30 秒)、スイッチはポートを転送状態にしません。しかし、ポートがネットワークのエッジで直接単一装置に接続する場合、ほとんどすぐに転送状態にしても問題ありません。ポートタイプは、ポートに接続したのは何かについてのスイッチの推定を制御します。

- Auto: ポートは最初エッジ ポートになると仮定され、それからすぐ転送に移行します。BPDU が受信された場合は自動的にネットワーク ポートになるよう調整し、BPUD が 3 秒間受信されないときはいつでもエッジポートに戻します。

- **Network (ネットワーク):** ポートは転送状態に移行する前に、常に安静期間待機します。
- **Edge (エッジ):** ポートは最初、単一装置に直接接続すると仮定されますが、BPDU を受信すると、ネットワーク ポート変わります。その後、ポートのリンクが再確立するといつでも、常に安静期間待機してから転送に移行します。

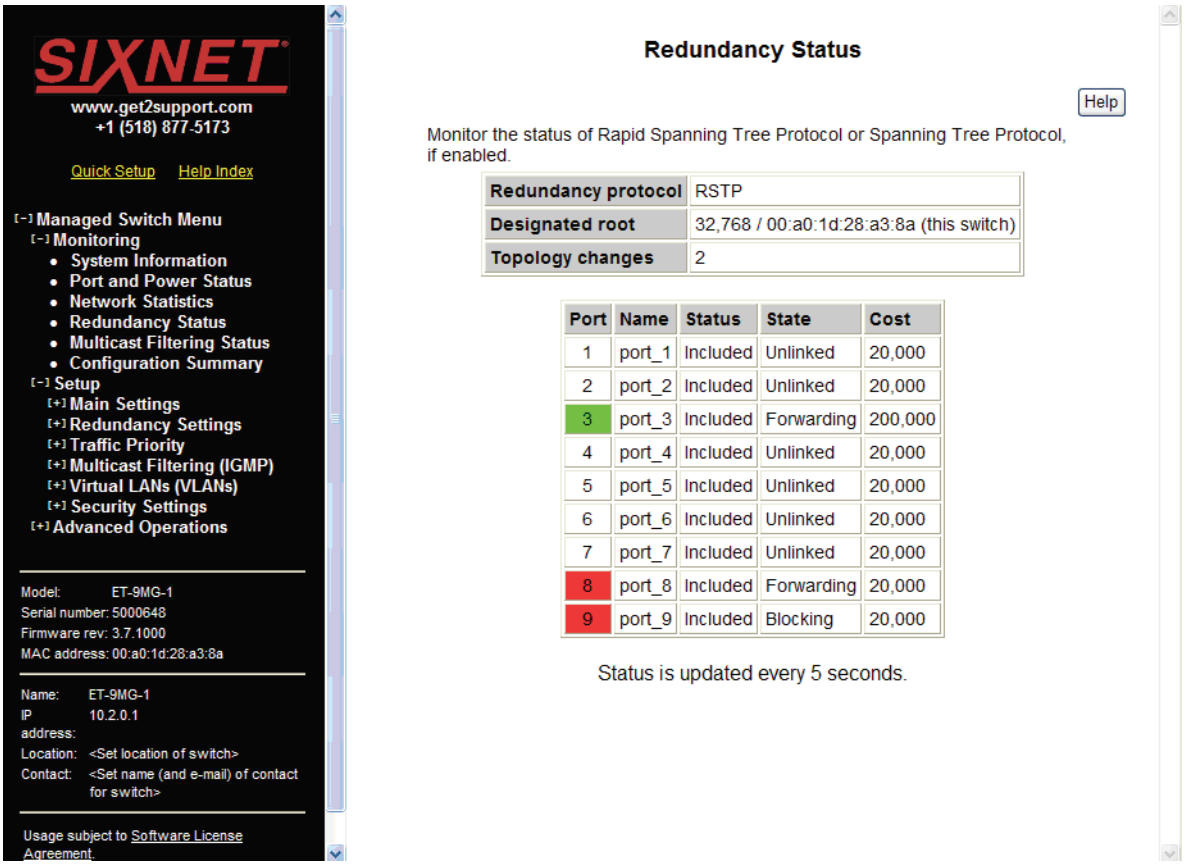
このオプションは各 MSTI のポートごとに設定できます。

6.4.5 Port-to-Port MAC (ポートツーポート MAC) (デフォルト = Auto (自動))

他のネットワーク ポート 1 つだけが接続されているとき、ポートはポイント ツー ポイント ネットワーク セグメントの一部です。RSTP は、ポイント ツー ポイント リンクから他のマネージド スイッチへネットワーク トラフィックを直ちに転送するのが安全かどうか、決定できます。または、ネットワーク トラフィックを転送する前に、ポートは数秒（デフォルトは 30 秒。転送遅延時間の 2 倍）待機しなければなりません。「Auto」に設定されているときは、半二重ポートではなく、全二重リンクがポイント ツー ポイントになると考えられます。この設定は、自動決定が間違っているときは、強制的に「true」または「false」にすることができます。

6.5 冗長ステータス

Redundancy Status (冗長ステータス) ページは、[Main Menu](メイン メニュー) の [Monitoring Menu](監視メニュー) からアクセスします。冗長ステータス ページにはスイッチのスナップ ショットがあり、マネージド ネットワークの機能を提供しています。ページ上部には、使用中のプロトコルが現在のスパニング ツリーのルートの MAC アドレスと共に表示されます。[Topology change](トポロジーの変更) カウンターは、ネットワーク レイアウトの変更数を追跡します。また、スイッチの各ポートの現在の冗長ステータスも表示されます。



- Port (ポート): ポートの数。これはスイッチ ラベルに対応しています。
- Name (名前): ユーザー設定のポート名。
- Status (ステータス): STP プロトコルでのポートの設定状態。(included (含む) または excluded (除外)) 含むポートはマネージド ネットワークの一部となり、他の装置のために他のマネージド スイッチへトラフィックを伝送します。除外ポートは、マネージド ネットワークの一部としては使われません。たとえば、工場の装置のマネージド ネットワークからビジネス ネットワークへの単一アップリンクは、STP の使用から除外されるよう設定されます。
- State (状態) : ポートの STP/RSTP の状態。(下記を参照のこと)
- Cost (コスト): マネージド ネットワークの他の部分へ到達するためのこのポートを使った場合のコスト。
- STP/RSTP Port States (ポート状態): スパニング ツリー プロトコルには、5 つのポート状態があります。ラピッド スパニング ツリー プロトコルは、3 つだけ使用します。表 1-1 および表 1-2 は、ポート状態、アクティブなスパニング ツリー トポロジーへのポート参加、ならびに STP と RSTP それぞれのラーニング MAC アドレスへのポート参加を表しています。イーサネット デバイスに物理的に接続していないすべてのポート、または接続障害のあるポートは、ポート状態部に「unlinked」(リンクされていない) と表示されます。

6.6 STP アルゴリズムのポート状態

- Blocking (ブロッキング)(STP): この状態のポートは、フレーム リレーに参加しません。(受信したフレームを他の場所へ渡す) ポートがこの状態になった場合、アクティブなトポロジーの複数経路によって引き起こされるフレーム重複の可能性を防ぎます。
- Listening (リスニング)(STP): この状態のポートは、フレーム リレーに参加する直前ですが、どのフレーム リレーにも関わっていません (フレームは転送されません)。すぐにフレーム リレーに参加しない理由は、ネットワーク トポロジーが変化するとき、一時的なループが発生しないようにするためです。この状態の間、ブリッジはすべての学習状態のポートを無効にします。ポートが役割を変化させているときに競合状態が発生するのを防ぐためと、転送プロセスがすべてのフレームを破棄し、いかなるフレームも伝送しない様にするためです。一方、アルゴリズムを実行し続けるため、BPDU は引き続き受信と転送ができます。
- Learning (ラーニング)(STP): この状態のポートは、フレーム リレーに参加する直前です。しかし、どのフレーム リレーにも関わっていません。ブリッジ LAN が変化しているアクティブなトポロジーで、一時的なループの発生を防ぐため、フレーム リレーはおこなわれません。さらに、転送プロセスはすべてのフレームを破棄し、いかなるフレームも伝送しない様にします。ラーニングが有効な理由は、フレーム リレー活動の前に情報を収集するためです。集められた情報は、不必要に減らされるフレームの数を減らすため、フィルタリング データベース (MAC テーブル) で使用され保管されます。
- Forwarding (転送)(STP): 転送状態のポートは、現在フレーム リレーに参加しています。BPDU は、アクティブなトポロジーの計算に転送ポートを含めます。受信した BPDU は、スパニング ツリー アルゴリズムによって処理され、ハロー間隔または受信した BPDU 情報に基づいて送信されます。

表 6-1 801.1D STP ポート状態

ポート状態	アクティブなトポロジーへのポート参加	ラーニング MAC アドレスへのポート参加
Disabled (無効)	なし	なし
Blocking (ブロッキング)	なし	なし
Listening (リスニング)	あり	なし
Learning (ラーニング)	あり	あり
Forwarding (転送)	あり	あり

6.7 RSTP アルゴリズムのポート状態

802.1D スパニング ツリー プロトコルの効率を最適化するには、収束時間を速くするために特定の状態が集約されるか除去されます。特に、STP の無効、ブロッキング、およびリスニング状態は、RSTP の破棄状態 1 つへと減っています。

- **Discarding State (破棄状態)(RSTP)**: この状態では、ステーション位置情報はフィルタリング データベース (MAC テーブル) に追加されません。ポートの役割のどのような変更もフィルタリング データベースの情報を不正確にしてしまうためです。

- **Learning State (ラーニング)(RSTP)**: この状態では、ポートの役割は変化していないという仮定のもと、情報はフィルタリング データベースに追加されています。フレーム リレーの前 (転送状態) に収集された情報は、転送状態になったときに送信されるフレームの数を減らします。

- **Forwarding State (転送状態)(RSTP)**: フレームが特定のポートへ、または特定のポートから転送される、それが転送状態です。さらに、転送状態であっても、ラーニング プロセスはステーション情報をフィルタリング データベースに取り入れ続けています。

表 6-2 802.1D RSTP ポート状態

ポート状態	アクティブなトポロジーへのポート参加	ラーニング MAC アドレスへのポート参加
Discarding (破棄)	なし	なし
Learning (ラーニング)	なし	なし
Forwarding (転送)	あり	あり

6.8 RSTP 例

6.8.1 例 1: 冗長リング内の最大ホップ数とスイッチ

最大エージタイム設定は、RSTP メッセージがネットワーク内を巡回する期間を制御します。スイッチがメッセージを受信すると、メッセージ エージと最大エージ タイム (これもメッセージで運ばれる) を比較して、そのエージが最大エージ タイムに到達していれば、メッセージは破棄されます。そうでなければ、メッセージ エージを 1 増やしてからメッセージを転送します。したがって、RSTP ネットワークの最大直径は、最大エージタイムに制御されます。最大エージタイムの最大値は 40 なので、最大 RSTP ネットワーク ホップ 直径も 40 です。

6.8.1.1 ホップ数 vs. リカバリタイム

下の図では、6 つのマネージド スイッチおよび、ステーションの間に 5 つのホップがある典型的な冗長リング ネットワークを示しています。

ネットワーク セグメント障害があるときの全体的なリカバリ タイムは、ホップ数によります。リカバリ タイムは通常、ホップにつき 50 ミリ秒未満です。したがって、下の図の 6 つのマネージド スイッチがついた典型的なリングでは、全体的なリカバリ タイムは、250 ミリ秒未満です。(5 ホップ x <50 ミリ秒)

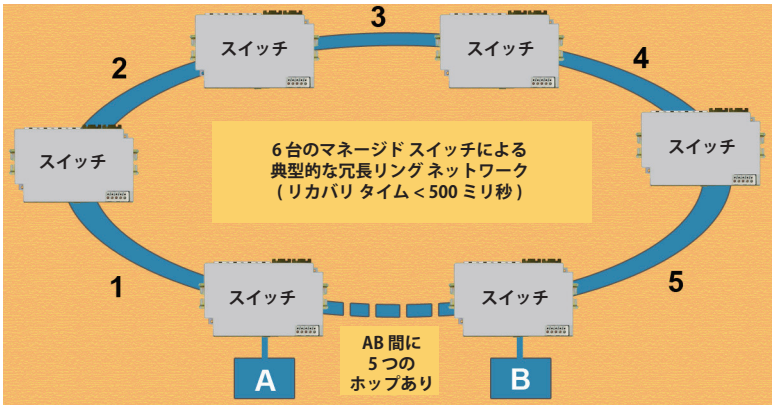
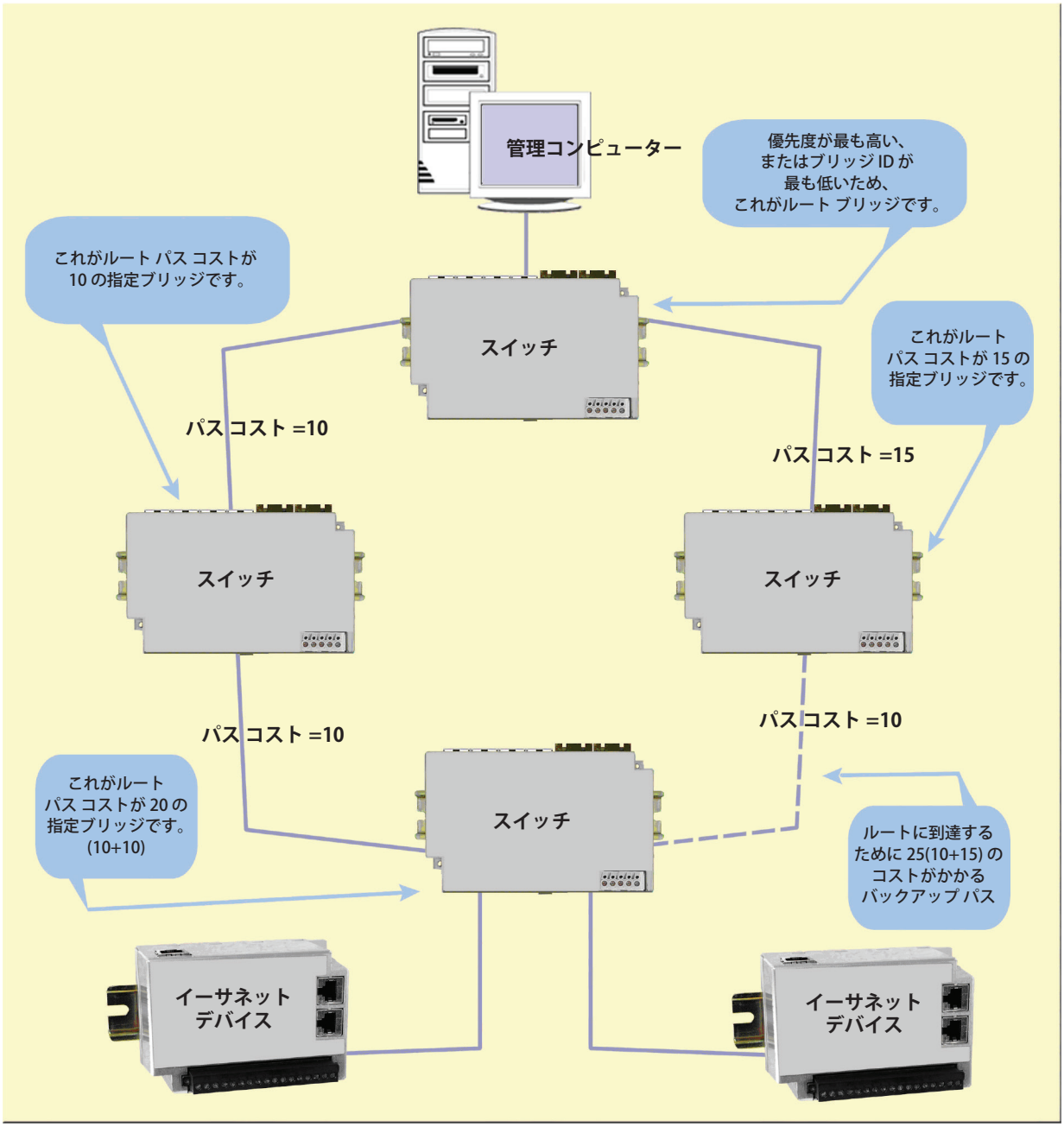


図 6-1 AB 間に 5 つのホップがある典型的な冗長リング

6.8.2 例 2: パス コストを使用した一次およびバックアップ接続の確立

パス コストは、使用に一番良い接続を確立するのに用います。費用が余分に掛かり、遅く、またはあまり望ましくない経路に、より高いコストを割り当てることができます。マネージド スイッチは、パス コストを合計して、ルート スイッチへ戻る一番良い経路を決定します。次の例を参照してください。

注 : ほとんどのネットワークで、パス コストをデフォルト設定にしておくだけで、スイッチは自動的に一番良いパスを決定します。

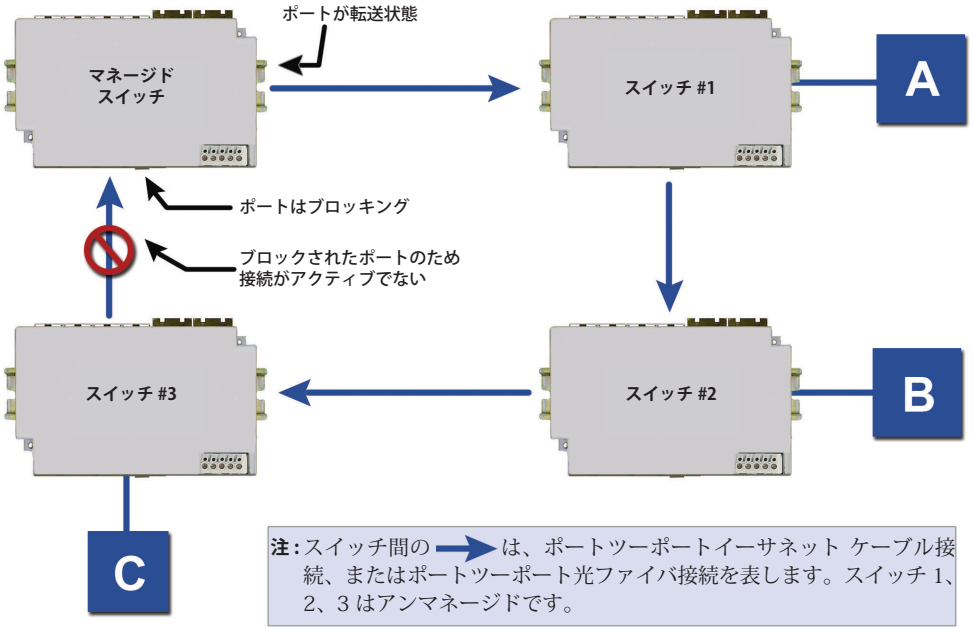


6.8.3 例 3: マネージドスイッチが 1 つだけのリング トポロジー (まねをしないこと！)

お金の節約になるのではないかという理由で、1 台のマネージド スイッチと複数台のアンマネージド スイッチをリング トポロジーに実装することに関して、よく質問があります。一台のマネージド スイッチが各リングの構成員であるときにだけ、トポロジーは正当ですが、推奨しません。下の仮想シナリオでその理由を説明します。

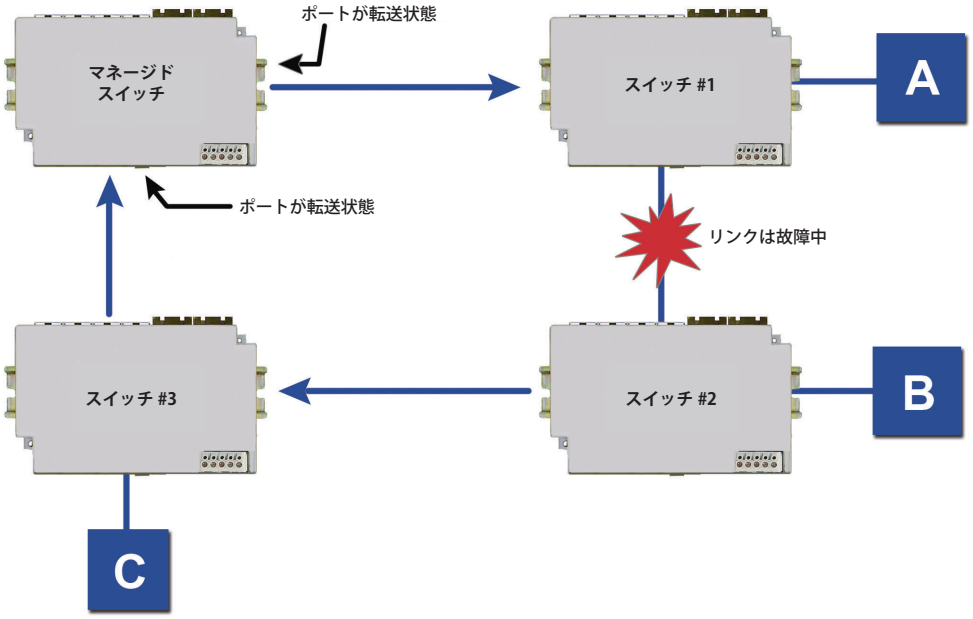
6.8.3.1 仮想シナリオ

インテグレーターが、提案されたネットワークに、シングル イーサネット リング トポロジーの機器の利用を希望しているとします。1 つのマネージド スイッチだけを利用して、ループ上の 3 つ以上のアンマネージド スイッチを接続します。(図 1)



はじめは、ネットワークはすべて順調に動いています。マネージド スイッチが、コンフィギュレーション メッセージを見て、STP パラメータに基づいてループを検出します。転送状態にするポートを 1 つ選び、他方のポートはブロッキング状態にします。ループはなくなり、デバイス A はデバイス B と交信できます。

工場のどこかで、建設車両が間違ってアンマネージド スイッチ #1 とアンマネージド スイッチ #2 の間の接続を切断します。ネットワークのマネージド スイッチは、ブロッキングモードのポートがコンフィギュレーション メッセージを受信していないことと、リスニング、ラーニング、および転送状態へ移行していることに気が付きます。(アンマネージド スイッチに接続しているときは、通常 6 秒くらい) (図 2)



マネージド スイッチの両方のポートが転送モードになり、問題が解決したように見えますが、そうではありません。他の 3 台のスイッチはアンマネージドのため、この 3 台がネットワーク トポロジーが変更されたのを知るインテリジェンスがないのです。装置 A が装置 B と交信しようとしているとき (イーサネット リンクが壊れているので、交信できません)、スイッチ #1 はまだスイッチ #2 に向いています。スイッチ #1 の MAC テーブルが、装置 A および装置 B のエントリをエージアウトするまで待たなければならないので、障害が発見されました。同じことがスイッチ #2 (B が A と交信) およびスイッチ #3 (C が A と交信) と接続している装置にも適用されます。

この「お金の節約」構成の結果、ネットワーク冗長性能が犠牲にされ、スイッチ 1、2、3 の MAC テーブル エントリのエージ アウト時間に委ねるほかありません。アンマネージド イーサネット スイッチのモデルによりますが、MAC テーブルのエントリは通常 5 分以上エージ アウトに掛かります。

これにより、工場に最低 5 分のダウンタイムが発生することになり、工場の運営に関して非常に不利益なコストとなります。スイッチ 1、2、3 をマネージド スイッチに交換することで、ネットワーク収束時間は、1 秒未満まで減らせます。さらなる恩恵は、ネットワークは 1 つの冗長ループだけに限られていないので、ネットワーク上あらゆるポイントで、本当の冗長ネットワーク計画のための接続の「網」を持つことができます。

6.9 リアルタイム リング設定

Real-Time Ring Settings (リアルタイム リング設定) ページへは、[Redundancy Settings](冗長設定) からアクセスでき、対応スイッチに Red Lion のリアルタイム リング プロトコルを設定できます。

リアルタイム リングは、ネットワーク セグメント障害が起きたとき、メッセージ フローに代わりのパスを提供することにより、ネットワーク信頼性を向上させます。リング ポートが通信障害を検出すると、すぐにリングの他のスイッチに通知します。メッセージは、数ミリ秒以内に自動的に代替リング経路に切り替わり伝えられます。

STP (スパニング ツリー プロトコル) は、リング構成に止まらずより柔軟です。しかし、スパニング ツリーのリカバリ タイムは、数百ミリ秒になります。 リアルタイム リング プロトコルは、トポロジの柔軟性を減らす一方で、数十ミリ秒のリカバリ タイムを実現します。

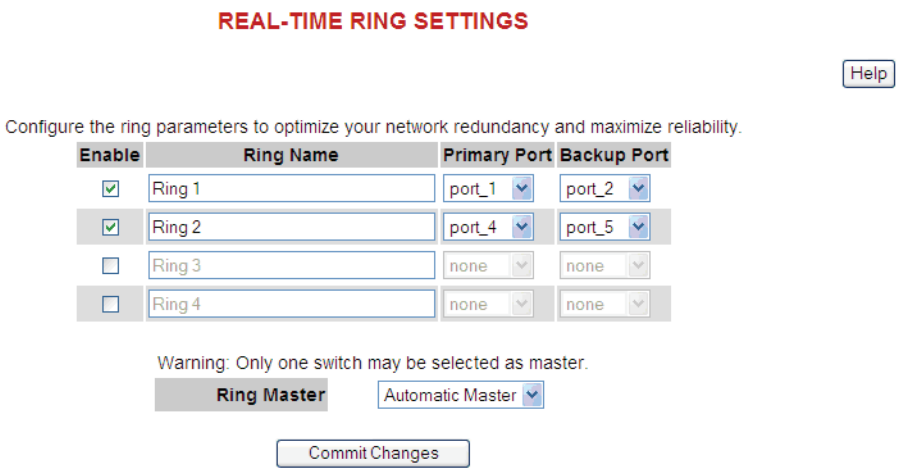
6.10 リング セットアップ

適切な [Enable](有効) チェックボックスを選択し、リングを起動します。スイッチの 2 つのポートごとに、1 つリングを設定できます。

リングが有効のときは、特定のリングとスイッチが接続するために、2 つのポートを使うように選択されていることを確認してください。そのためには、利用可能なポートを [Primary Port](プライマリ ポート) および [Backup Port] (バックアップ ポート) のドロップダウン リストから選択します。各ポートは、1 つのリングだけに割り当てます。

「バックアップ」に定義されたポートは、通常の稼働状況下ではブロックされます。デフォルトでは、リングでもっとも若い MAC アドレス スイッチがマスター スイッチになります。この時リングの通信が、スイッチの 2 つのリング ポートのうちの 1 つによってブロックされることを意味します。リングのマスター スイッチだけが、これを実施できます。[Ring Master](リング マスター) ドロップダウン リストから、希望のスイッチを [This is Master](これがマスター) に選択することで、違うスイッチをマスター スイッチに指定することもできます。リングの他のすべてのスイッチは、デフォルトの [Automatic](自動) 設定にしておきます。

注 : ポートがリング ポートに設定されているときは、そのポートはスイッチへの通信やスイッチ経由の通信に使用できません。マネージド スイッチかリアルタイム リング スイッチのリング ポートにのみ接続することができます。


REAL-TIME RING SETTINGS
Help
Configure the ring parameters to optimize your network redundancy and maximize reliability.
Enable
Ring Name
Primary Port
Backup Port
Ring 1
port_1
port_2
Ring 2
port_4
port_5
Ring 3
none
none
Ring 4
none
none
Warning: Only one switch may be selected as master.
Ring Master
Automatic Master
Commit Changes

第 7 章 優先度付きキュー (QoS、CoS、ToS/DS)

7.1 トラフィック優先度

特別な処理を有効にすることなく、ネットワークはすべてのアプリケーションに「ベスト・エフォート」なサービスを提供します。各スイッチやルーターにおいて、すべてのパケットが平等に扱われるため、特定のアプリケーションに対するクオリティ オブ サービス (QoS) 保証がありません。しかし、特定のアプリケーションでは、適切な稼働を保証するためにネットワークからの決定論的応答が求められます。

工場のボール盤を考えてみても、ローカル ネットワークのどこかでコンピューターで制御されています。ボール盤の掘る深さは重要で、もし掘られた穴が深すぎたら、材料は廃棄しなければなりません。通常状態では、掘削プロセスはスムーズに進みます (コントローラーとコンピューターは、ネットワークを介して効果的に通信しています) が、ネットワーク上の他のユーザーがオンライン データベースから記録にアクセスしようとすると、膨大な量のトラフィックがボール盤とのタイムリーな通信を妨害します。ボール盤とコントローラー間の通信遅延は、ボール盤の削り過ぎを招き、材料は廃棄しなければなりません。このようなことが起こらないようにするために、すべてのボール盤、コントローラー間通信の遅延を避けるため、一定の QoS を提供する必要があります。

信頼性のあるタイムリーなネットワーク通信の実現を助ける、無数の方法があります。マネージドスイッチは、メッセージに優先順位をつける 2 つの一般的な方法、IP ヘッダー及び 802.1p ユーザー優先度に対応しています。

IP ヘッダーはすべてのフレームにあり、優先度フィールドを含んでいます。デフォルトは 0 で、最高 255 まで設定できます。このフィールドは、タイプ オブ サービス (ToS) フィールド、またはディフサーブ (DS または DiffServ) と呼ばれることがあります。

アプリケーションは、0 から 7 で設定可能な優先度フィールドを含んだ IEEE 802.1p タグを追加することができます。各数値は、関連するトラフィック タイプを持っています。たとえば、5 のタグは映像データに指定されています。

スイッチは、アウトバウンド データの高速処理用に、4 つの優先度付きキューを提供します。IP の 256 の優先度および 7 レベルの IEEE 優先度は、高優先度データのスループット最適化の観点から、ポートに反映されます。

7.2 スケジューリング

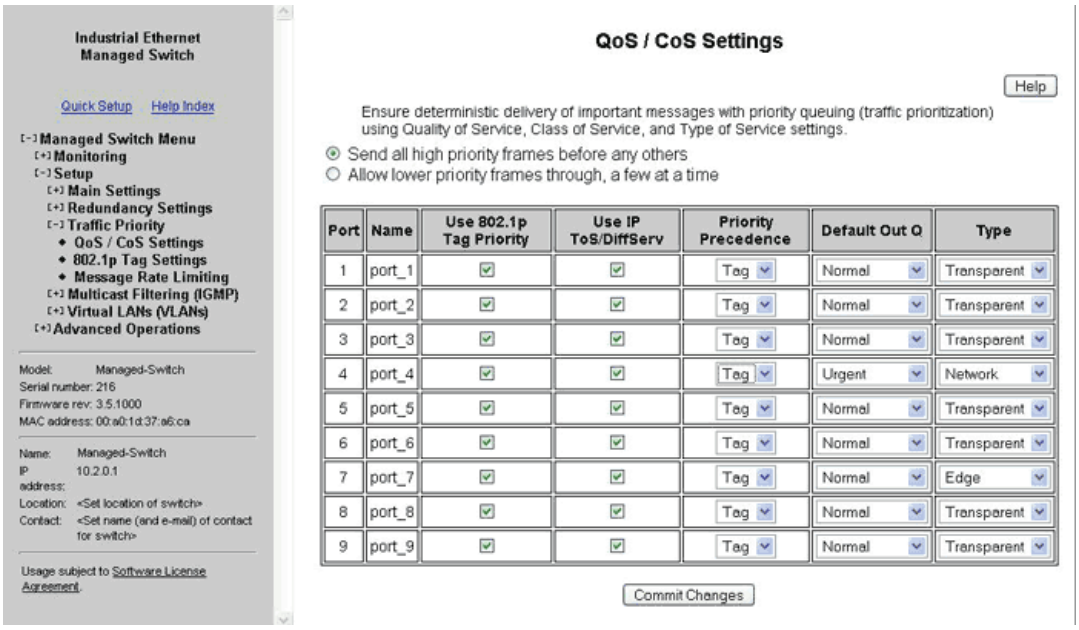
優先度の低いデータの処理方法を選択するとき、スイッチは [strict](厳密) または [fair](均等) スケジューリングを使用できます。この選択は、すべてのポートのすべてのキューに影響します。

Strict スケジューリングでは、もっとも高い優先度付きキューのすべてのデータは、優先度の低いデータの前に送信されます。そして、2 番目に優先度の高いすべてのデータへと続いていきます。こうして優先度の高いデータは、常に可能な限り速く送られるようになります。

Fair スケジューリングでは、ラウンド ロビン アルゴリズムが使用され、重み付けされて、優先度の低いデータよりも優先度の高いデータが多く送信されます。具体的には、スイッチは 8 つのフレームを緊急キューから送信し、4 つを優先キューから、2 つを通常キューから、そして 1 つをバックグラウンド キューから送信し、また緊急キューからの順に戻ります。このようにして、優先度の低いキューも送信機会を得られる様にします。

7.3 QoS / CoS 設定

スイッチの [traffic priority](トラフィック優先度) メニューにアクセスするには、[Main Menu](メイン メニュー) から [Setup](セットアップ) を選択し、さらに [Traffic Priority] を選択します。



各ポートにおいて、以下の設定が可能です。

- **Use 802.1p Tag Priority (802.1p タグ優先度を使用):** この設定は、フレームにタグ付いていたとき、スイッチが IEEE タグを受け入れるかどうかを制御します。有効時、タグ付きデータは、コンフィギュア タグ マッピングに基づいたアウトバウンド優先度付きキューへ送られます (下記を参照のこと)。この設定を無効にすると、すべての受信フレームの IEEE タグを無視します。

- **Use IP ToS/DiffServ (IP ToS/ ディフサーブを使用):** この設定は、スイッチが IP ヘッダーの優先度フィールドを受け入れるかどうかを制御します。有効で IEEE タグによって覆されないとき、データは IPv4 タイプ オブ サービスまたは IPv6 トラフィック クラスに基づいたアウトバウンド優先度付きキューへ送られます。優先度付きキューは、IP 優先度フィールド値を 64 で割ったものです。この設定を無効にすると、IP 優先度フィールドを無視します。

- **Priority Precedence (優先度の優先)**: この設定は、IEEE タグまたは IP ヘッダーが両方とも存在して有効の場合、どちらの優先マークが優先されるかを制御します。Use Tag、または Use IP のどちらかが無効の場合は、何も影響はありません。

- **Default Priority (デフォルト優先度)**: この設定は、判定できないときに、フレームに割り当てるデフォルト優先度を制御します。たとえば、IEEE タグなしのフレームが、Use IP が無効のポートに到着した場合などです。リストからアウトバウンド優先度付きキューを選択します。

- **Port Type (ポートタイプ)**: この設定は、IEEE タグが送出データでどのように扱われるかを制御します。

  - Transparent (トランスペアレント) は、スイッチに入ったとき、フレームに存在していたいずれのタグも維持します。

  - Edge (エッジ) は、すべての送出フレームからタグを除去します。

  - Network (ネットワーク) は、タグが存在しないときにタグを追加します。タグの値は、キューの数の 2 倍です。(キュー 3 は 6、など)

7.4 802.1p タグ設定

8 つの IEEE タグ優先度の値それぞれには、4 つの出力優先度キューの 1 つが割り当てられます。

- Background (バックグラウンド)(0)

- Normal (通常)(1)

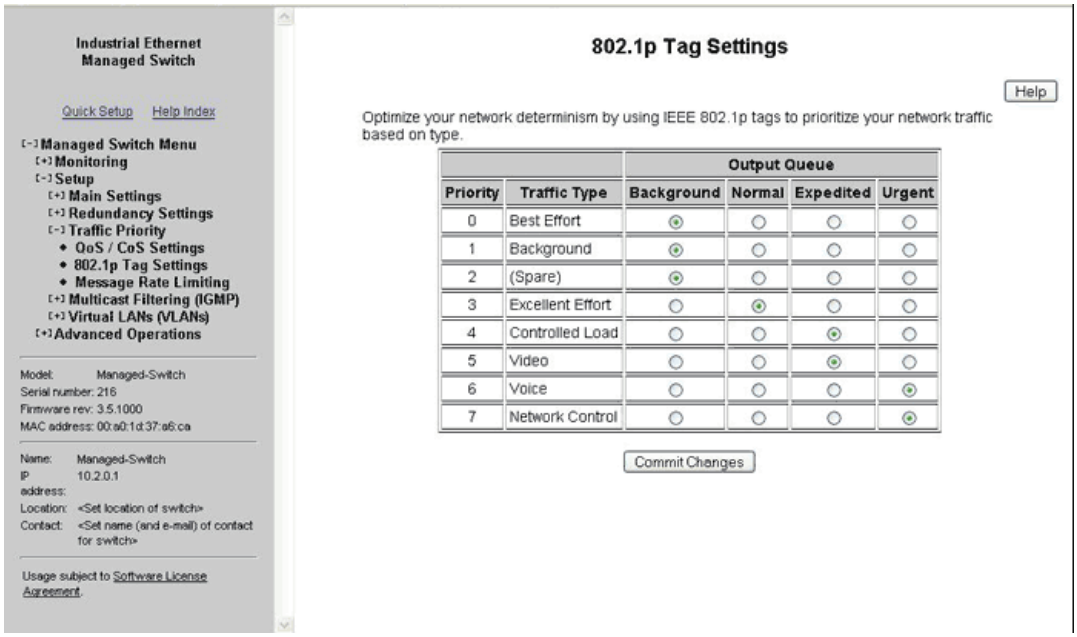
- Expedited (優先)(2)

- Urgent (緊急)(3)

IEEE 802.1p 推奨に従ったデフォルトの割り当ては下の通りです。

表 7-1 デフォルトのタグ割り当て

Priority (優先度)	Traffic Type (トラフィック タイプ)	Queue (キュー)
0	Best Effort (ベスト エフォート)	1
1	Background (バックグラウンド)	0
2	Spare (予備)	0
3	Excellent Effort (エクセレント エフォート)	1
4	Controlled Load (負荷制御型)	2
5	Video (ビデオ)	3
6	Voice (音声)	3
7	Network Control (ネットワーク制御)	3



7.5 メッセージ レート制限

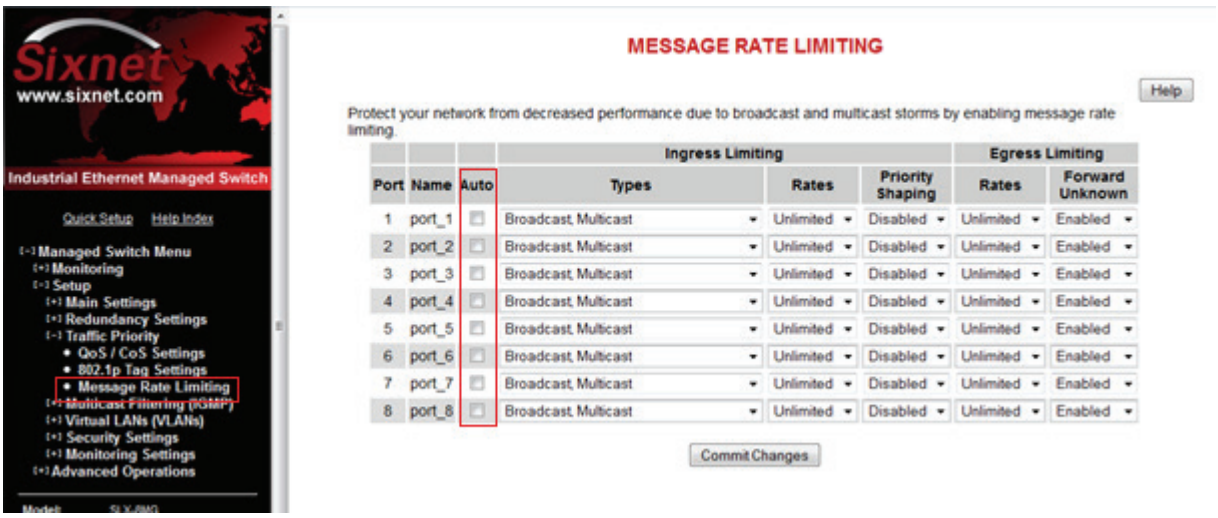
メッセージ レート制限は、お使いのスイッチとネットワークが、大量のブロードキャストおよびマルチ キャストメッセージによって壊滅されることを防ぎます。ポート判定が有効のときは、メッセージ レート制限が、ブロードキャストまたはマルチキャストになることが許可されたトラフィック量を制御します。制限を超えたトラフィックはドロップします。

不適切に設定されたアプリケーションおよび装置、または悪質なユーザーは、ブロードキャスト パケットを送信して、それらがすべてのポートに転送されて、すぐにネットワーク帯域のほとんどを使ってしまい、ネットワークをあふれさせます。マネージド スイッチは、スイッチによって許容されるメッセージレートを制限することで、このような「ブロードキャスト ストーム」から保護する方法を提供しています。

各ポートで、受け入れるブロードキャストおよびマルチキャスト メッセージのレート制限を選択できます。事前に設定した制限を超えたメッセージは破棄されます。

7.5.1 自動

ファームウェア バージョン 5.2 より前は、もっと簡単なレート制限スキームが完装されていました。ポートのこの機能は自動を選択することで有効に成ります。



制限はメッセージのタイプおよび優先度に基づいて行われます。ブロードキャストおよびマルチキャスト メッセージは優先順位付け (例 : ToS より IP など) をしてから、大体次のレートで制限されます。

表 7-2

Priority (優先度)	Limit (制限)
Background (バックグラウンド)	リンク容量の 10%
Normal (通常)	リンク容量の 20%
Expedited (優先)	リンク容量の 40%
Urgent (緊急)	リンク容量の 80%

正確な制限はリンク速度に依存します。

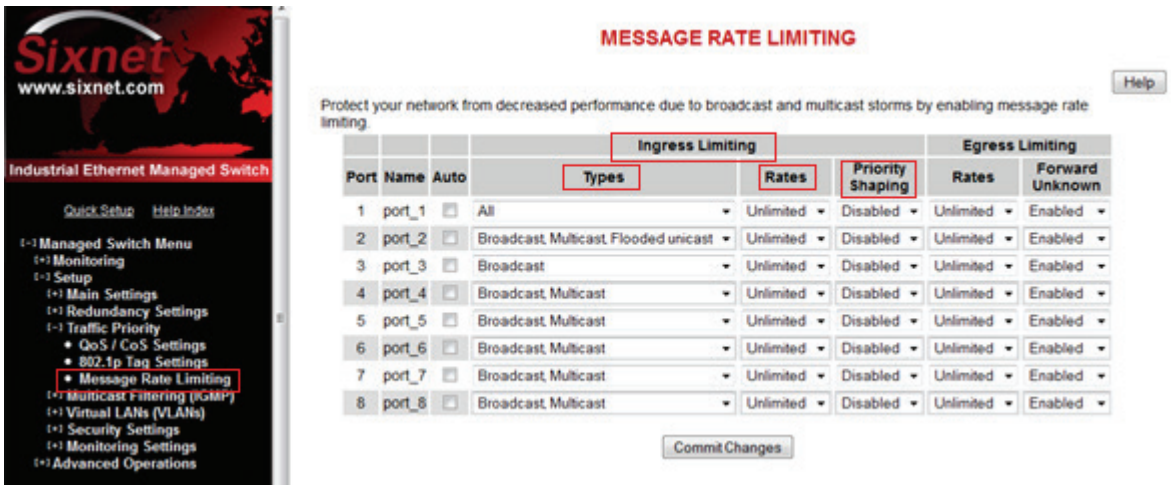
直接 1 台のステーション (ユニキャスト メッセージ) に宛てたメッセージは、メッセージ　レート制限の影響を受けません。

Auto を選択しない場合は、新しくてより柔軟な手法が可能です。詳細は次のとおりです。

7.5.2　入力帯域制限

スイッチに入るトラフィックは、タイプ、帯域、および優先度で制御できます。

メッセージ レート制限



タイプ

入力帯域制限は、異なるタイプのトラフィックに適用できます。

- 全タイプ
- ブロードキャスト、マルチキャストおよびフラッディング ユニキャスト (既知のユニキャスト アドレスが付いたフレームは影響を受けません)
- ブロードキャストおよびマルチキャスト (ユニキャスト アドレスが付いたフレームは影響を受けません)
- ブロードキャスト (マルチキャストまたはユニキャストアドレスが付いたフレームは影響を受けません)

レート

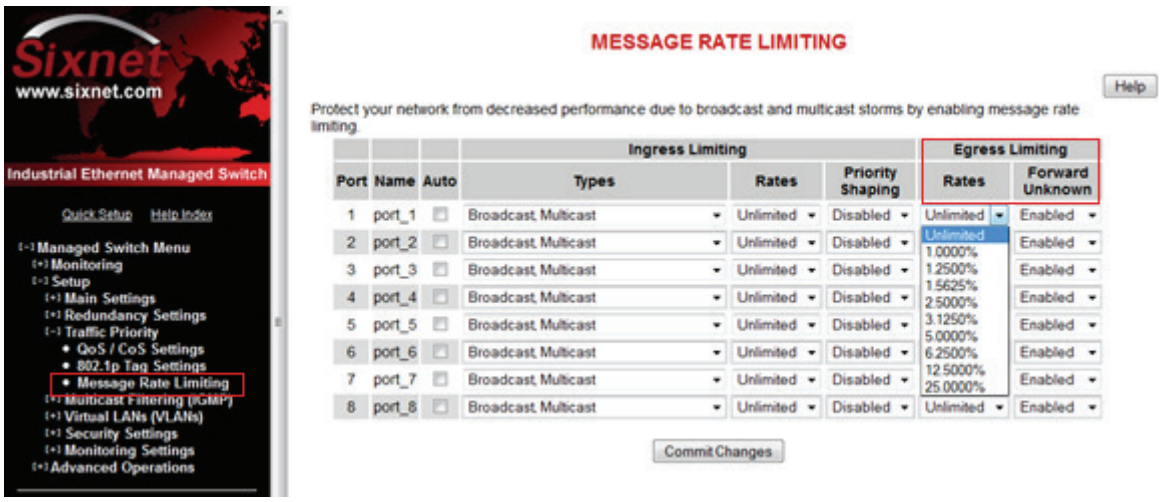
入力トラフィックは段階的に制限されます。ユーザーは、ポートのタイプに対応するパーセンテージ値のリストから選択できます。100Mbps ポートは 5% から 80% の範囲があります。ギガビット (1000 Mbps) ポートは 1% から 25% の範囲です。両方とも基盤となるハードウェアが最大限サポートするレートに基づく増加分があります。

優先シェーピング

設定されたレートはバックグラウンド トラフィックに適用されます。連続する高い優先度値のそれぞれに、同じレート (シェーピングが無効のとき) を使用するか、または二番目に低い制限値の 2 倍 (シェーピングが有効なとき) を使用します。

7.5.3 出力帯域制限

出力トラフィックは段階的に制限されます。ユーザーは、ポートのタイプに対応するパーセンテージ値のリストから選択できます。100 Mbps ポートは 5% から 80% の範囲があります。ギガビット (1000 Mbps) ポートは 1% から 25% の範囲です。両方とも基盤となるハードウェアが最大限サポートするレートに基づく増加分があります。



出力帯域制限はすべてのタイプのトラフィックに適用されます。(ユニキャスト、ブロードキャストおよびマルチキャスト)

7.6 QoS 例

7.6.1 QoS による重要なメッセージの確実なリアルタイム配信

重要なリアルタイム データが、(相対的に言って) 緊急とみなされないデータに干渉されない様にするネットワークの管理方法の詳しい例を、次の通り検証します。

7.6.2 仮想シナリオ

シナリオ : 中央制御システムで制御されている発電所があります。さらに、安全上の観点から、複数のカメラが各機械制御拠点に設置されています。各サイトの機械制御装置とビデオカメラは、イーサネット経由でそれぞれのスイッチと通信します。(明確で分かりやすくするため、ネットワーク上には、ビデオと制御データだけが存在することとします)

問題 : 機械制御装置が、遅延制御データを中央制御システムから受信します。そのため、発電所は本来発電できるはずの最大エネルギーが発電できません。顧客は電圧の低下を経験し、発電所は否定的な詮索をされるでしょう。したがって、カメラによって作成されたビデオ トラフィックがクリティカル データを遅延させないことが、とても重要なのです。

目標 : 重要なリアルタイム制御データ転送の最適化、およびネットワークを横断する映像データの影響の最小化または無くすことを同時におこなう。

解決策 : スイッチの設定は、スイッチの優先度キュー設定の調節によって制御データより映像データの優先度を低くする。

7.7　トラフィック優先度のスイッチのコンフィギュレーション

本マニュアルの中で先に述べたとおり、いくつかのアプリケーションは、希望するサービス レベルに達するために、ネットワークの特定のクオリティ オブ サービス (QoS) が必要です。この例では、制御データがタイムリーであることが重要です。スイッチの優先度キュー能力を利用せず、ベストエフォート型ネットワーク モデルを使用します。ネットワークはすべての情報パケットを送信しようと試みますが、特定のアプリケーション データの適時性に関して、いかなる約束や保証をするものではありません。前述の制御とビデオの例を考えても、同時にビデオカメラがデータを送信している場合、制御データに必要なレスポンス タイムを得られるという保証はないのです。

希望する QOS に到達するには、ネットワーク トラフィックの優先順位付けをします。ネットワーク トラフィックの優先順位付けは、たとえ装置 (ビデオカメラと制御システム) が、クオリティ オブ サービス パラメータの選択や構成に対応していなかったとしても、行えます。

スイッチに相互接続するすべてのポートを次のように設定します。

Use 802.1p Tag Priority Checked
Use IP ToS/DiffServ Checked
Default Priority Tag
Output Tag　Add Tag

データの発生場所 (カメラまたは制御システム) では、ビデオカメラ ポートの QoS/CoS 設定は次のように設定します。

Use 802.1p Tag Priority Unchecked
Use IP ToS/DiffServ Unchecked
Default Priority Expedited
Output Tag Remove Tag

また、制御システム ポートは次のように設定します。

Use 802.1p Tag Priority Unchecked
Use IP ToS/DiffServ Unchecked
Default Priority Urgent
Output Tag Remove Tag

このように、スイッチはパケットを適切に処理し、ネットワーク上の他の所で処理が行われるようにタグをつけます。

着信先では、制御システムのポートは次のように設定します。

Use 802.1p Tag Priority Checked
Output Tag Remove Tag

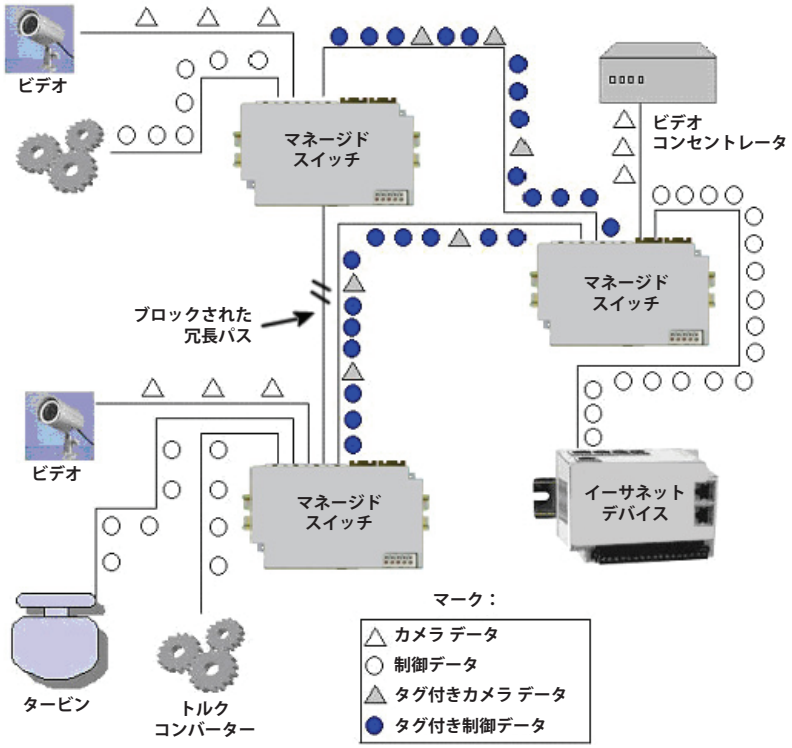
また、ビデオ コンセントレータ ポートは次のように設定します。

Output Tag　　Remove Tag

7.8 結果

結果: 制御データより映像データの方が低い優先度になるように設定するので、結果として制御データには QoS が必要になります。

次の図表には、タービンと複数のトルク コンバーターを制御する IPm があります。さらに、映像データを収集するビデオ コンセントレータもあります。映像データ (三角) が制御データ (丸) よりも低い優先度になるようにスイッチが設定されているので、制御データが映像データよりも頻繁に送信されているのが分かります。明確にするために、図表ではネットワークのタグなしデータを白い三角と白丸で表し、ネットワークのタグつきデータは色付きの三角と丸になっています。これによって制御アプリケーションに必要な QOS を達成しています。



第 8 章 マルチキャスト フィルタリング (IGMP)

8.1 IGMP について

IGMP (インターネット グループ管理プロトコル) は、ネットワークのマルチキャスト トラフィックの転送を最適化するために、ホストとルーターが一緒に作動できるようにします。IGMP がない場合、すべてのマルチキャスト パケットを、ネットワークのすべてのセグメントに転送しなければなりません。IGMP があれば、マルチキャスト トラフィックは、関連ホストが接続されているネットワーク セグメントだけに転送されます。

IGMPv1 は、ホストとルーターがマルチキャスト グループについて通信するための、基本的な構造を提供します。ルーターはクエリ メッセージを送信し、ホストはグループのメンバーシップ レポート メッセージで応答します。

IGMPv2 は、クエリに最大レスポンス タイムを追加し、プロトコルにリーブ メッセージを追加します。IGMPv1 と IGMPv2 は、同じネットワークに存在すべきではありません。また、IGMPv2 ルーターは、IGMPv1 ホストが検出されるセグメントは、IGMPv1 を実行することが期待されています。

IGMP スヌーピング スイッチは、IGMP ルーターの多くの機能を実行します。パッシブ モードでは、マルチキャスト トラフィックを効果的に転送する設定のために、ホストおよびルーターによって送信された IGMP プロトコル メッセージをスイッチが処理します。アクティブ モードでは、スイッチもクエリをネットワークコの収束を促進するために送信します。

ルーターとアクティブ モードの IGMP スヌーピング スイッチは、それぞれに接続されたネットワークの IGMP クエリを定期的に送信します。(クエリ間隔は、たいてい 1 ～ 2 分くらい) グループのメンバーに成ることを希望するホストは、クエリに遭遇したときのタイマーをショートとランダム遅延に設定します。タイマーが切れる前に他のホストからのレポートを見たときは、タイマーをキャンセルし、他のクエリに遭遇するまで次の行動をとりません。もし他のレポートが見られなければ、レポートはタイマーが切れたときに送信されます。ルーターまたはスイッチは、レポートをマルチキャスト転送の設定に使用します。

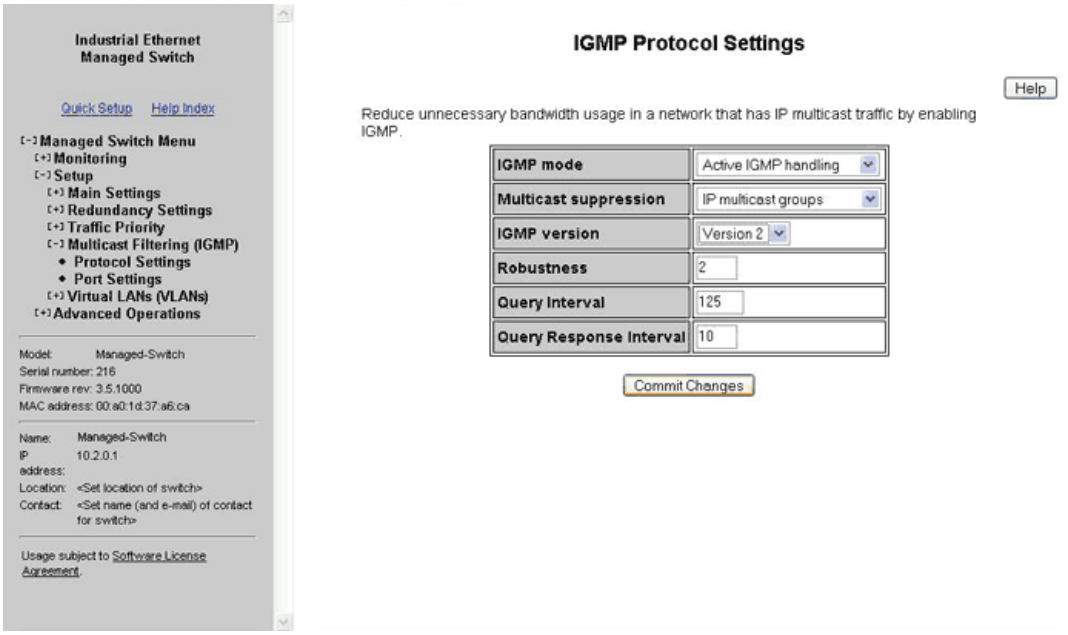
ルーターまたはスイッチは、各グループの各ポートの最新レポートからの経過期間の記録を保管します。グループの期限が切れると、ルーターまたはスイッチは、ポートへのマルチキャストデータの転送を停止します。クエリ間隔は有効期限より短いので、アクティブ グループのデータは、継続して途切れる事なく転送されます。

8.2 マルチキャスト フィルタリング コンフィギュレーション

IGMP は、2 つのメニューから設定できます。

- IGMP Switch Settings (スイッチ設定)
- IGMP Port Settings (ポート設定)

このメニューにアクセスするには、[Main menu](メインメニュー) から [Setup](セットアップ) を選択し、さらに [Multicast Filtering](マルチキャスト フィルタリング) を選択します。



8.3 IGMP スイッチ設定

- **IGMP Mode (IGMP モード):** この設定は、マルチキャスト トラフィックの転送方法を決定するために、どのようにスイッチが IGMP メッセージを処理するかを制御します。
  - IGMP Disabled (IGMP 無効) では、スイッチが IGMP メッセージを無視します。すべてのマルチキャスト トラフィックが、すべてのポートに送信されます。
  - Passive IGMP handling (パッシブ IGMP 処理) では、スイッチは IGMP メッセージを聞き、それに従ってマルチキャスト トラフィックの転送を設定します。
  - Active IGMP handling (アクティブ IGMP 処理) では、スイッチが IGMP ルーターとして機能し、必要なときにクエリを送信し、IGMP メンバーシップ レポートに従って、マルチキャスト トラフィックの転送を設定します。
- **Multicast Suppression (マルチキャスト抑制):** この拡張機能は、どのホストも IGMP で要求していないマルチキャスト パケットを知的に抑制できます。

- None (なし) ― IGMP が有効で、かつ 1 つ以上のクライアントが IGMP レポート リクエストを送信していない限り、マルチキャスト パケットはすべてのポートに送信されます。

- IP multicast groups (IP マルチキャスト グループ) ― IP マルチキャスト グループに対応するマルチキャスト パケット (01:00:5e で始まる MAC アドレスを持つ) は、1 つ以上のクライアントが IGMP レポートメッセージを送信していない限り、抑制されます。他のアドレスを持つマルチキャスト パケットは、すべてのポートに送信されます。

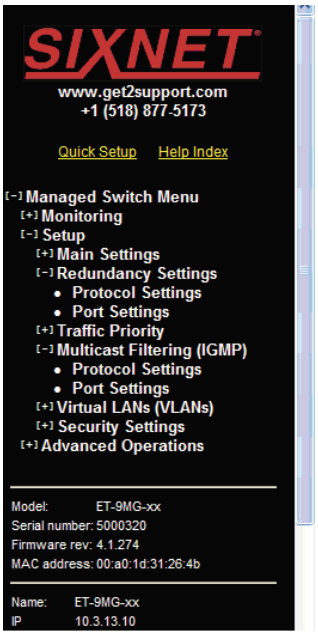
- All unreserved multicast (すべての予約無しマルチキャスト) ― 予約されたマルチキャスト アドレス (01:80:c2:00:00:0x where x is 0..f) を持つマルチキャスト パケットは、すべてのポートに送信されます。他のすべてのマルチキャスト パケットは、1 つ以上のクライアントが IGMP レポート メッセージを送信していない限り、抑制されます。

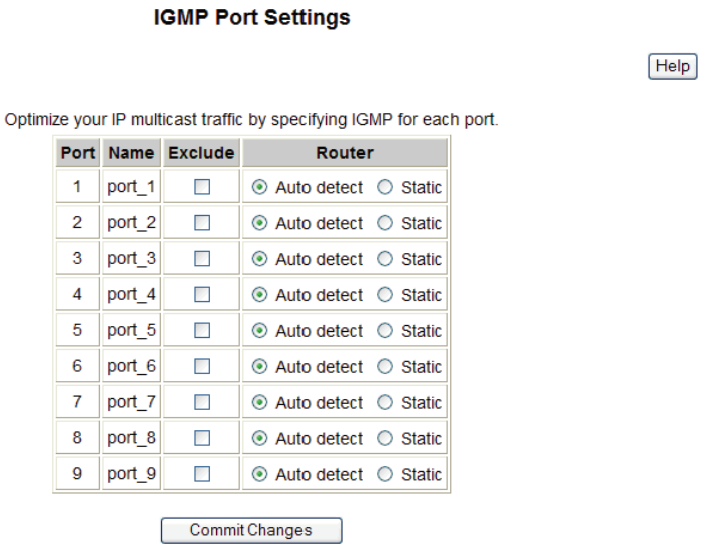
- IGMP Version (IGMP バージョン): この設定は、スイッチが使用する最も高い IGMP バージョンを制御します。ネットワークのすべての IGMP ルーターとスヌーピング スイッチは、同じ IGMP バージョンに設定します。1 または 2 のインストールに適した方を選択してください。

- Robustness (ロバスト性): この設定で、スイッチが IGMP ホストを検出しようとするとき、転送に影響を与える事なく、どれくらいのクエリを失ってもよいか指定します。

- Query Interval (クエリ間隔): この設定は、どれくらいの頻度でスイッチが IGMP クエリを送信するかを指定します。

- Query Response Interval (クエリ応答間隔): この設定は、ホストが IGMP クエリに応答する最大時間を指定します。(IGMPv1 では、これは 10 秒に固定されています)





8.4 IGMP ポート設定

一般的に、スイッチは、IGMP ルーターがどのポートに接続されているのかを、IGMP クエリ メッセージを聞くことにより、動的に学習します。状況によっては、IGMP ルーターへと導くように、静的にポートを設定することが必要です。ルーター タイプで [Static](静的) を選択し、スイッチに IGMP メッセージを特定のポートへ転送するようにさせます。

- **Exclude Port (ポート除外)**: IGMP 処理からポートを除外することができます。除外されたポートで受信した IGMP クエリおよびレポートは無視されるので、除外されたポート経由でつながっている装置は、スイッチでフィルター処理されているマルチキャスト グループに参加できません。IGMP クエリおよびレポートは除外されたポートに転送されず、除外されたポート経由でつながっている IGMP ルーターは、他のポート経由でつながっている装置のメンバーシップを知ることはありません。

- **Static Router (静的ルーター)**: IGMP クエリメッセージを受信しなかったとしても、このポートに IGMP ルーターがつながっていることを、スイッチが想定すべきかどうか指定します。

8.5 IGMP ステータス

IGMP ステータスは、2 つのメニュー経由で監視できます。

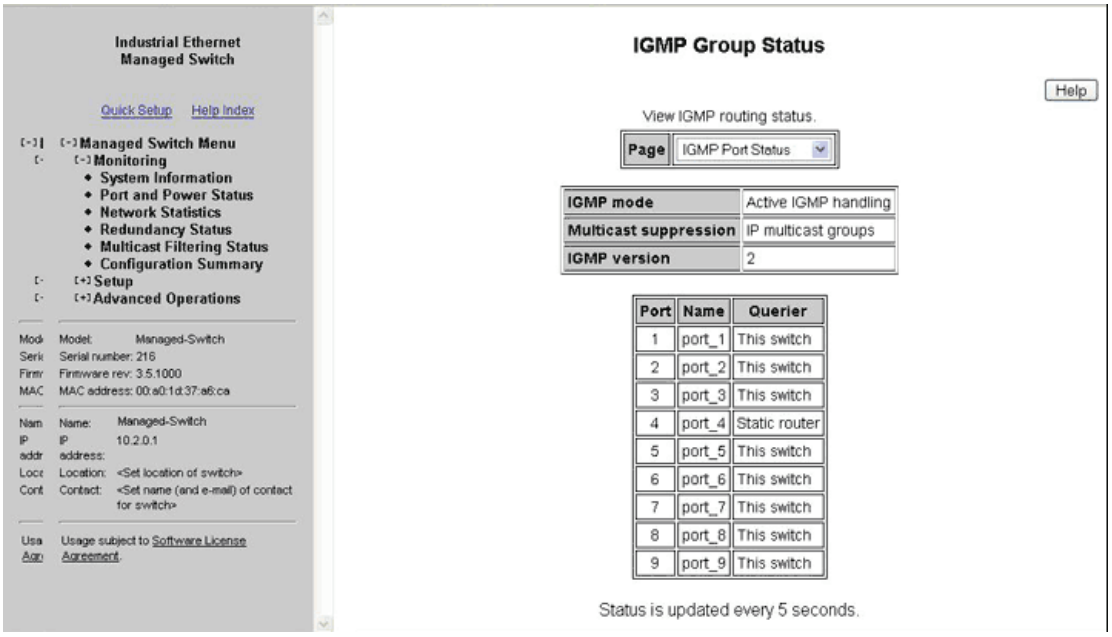
- IGMP Port Status (ポート ステータス)

- IGMP Group Status (グループ ステータス)

これらのメニューにアクセスするには、[Main Menu](メインメニュー) から [Monitoring](監視) を選択します。

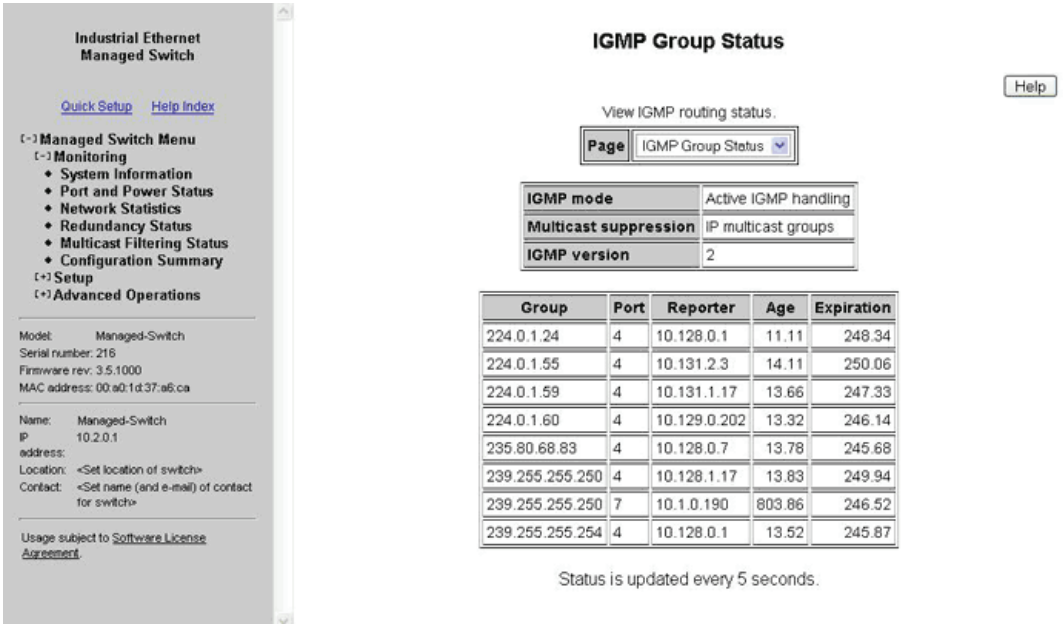
8.6 IGMP ポート ステータス

各ネットワーク セグメントは、アクティブ IGMP クエリ、アクティブ スイッチ、または最も小さい IP アドレス付き IGMP ルーターのうち 1 つだけ持つことができます。この画面では、スイッチの各ポートに付属のネットワーク セグメント上のクエリアの IP アドレスを示します。



8.7 IGMP グループ ステータス

グループ ステータス画面を使って、スイッチによって転送されている IGMP グループを検出します。各グループとポートの組み合わせ毎に、1 行になっています。つまり、グループが 1 つ以上のポートでアクティブな場合は、各ポートは表のなかで別の行を持つことになります。



表示されたデータは、いくつかのフィールドで区分されています。

- **Group (グループ):** 特定のマルチキャスト グループの IP アドレスを表示します。
- **Port (ポート):** 特定のマルチキャスト グループがアクティブなポート番号を表示します。
- **Reporter (リポーター):** このポート上でこのグループのメンバーシップを報告する最新ホストの IP アドレスを表示します。スイッチまたはルーターを特定のマルチキャスト グループの中に持つ目的で、ホストは IGMP レポートをスイッチまたはルーターに送信します。
- **Age (エージ):** このポート上で最後にこのグループが報告されてからの秒数。
- **Expiration (有効期限):** 新しいレポートが受信されない限り、このグループがドロップされるまでの秒数。

8.8 IGMP 例

8.8.1 IGMP を有効化する利点

マルチキャスト データを複数の他のイーサネット装置に送信中のイーサネット装置がある、すでに確立された制御ネットワークを例にとります。マルチキャスト データのソースと、マルチキャスト データに関心のある宛先のイーサネット装置の間で、マルチキャスト パケットはいくつかのスイッチまたはルーターを通過するとします。

この制御ネットワークをもっと効率よくするには、スイッチまたはルーターが IGMP（インターネット グループ管理プロトコル）によるマルチキャスト データ フローの処理方法を理解していなければなりません。

IGMP に対応できないスイッチまたはルーターは、マルチキャスト データをどうしたらよいかわからず、マルチキャス トデータをすべてのポートに転送します。このため、ネットワークの速度が落ちます。

次の図表を参照してください。IGMP サーバがマルチキャスト データのソースで、IGMP ホストが、マルチキャスト データを受信することに関心のある装置です。ネットワーク上の 2 つのスイッチは、1 つは IGMP が有効でもう 1 つは IGMP が無効です。IGMP が有効なスイッチは、マルチキャスト データを関心のあるホスト (イーサネット ステーション 2) にだけ転送しているのが、はっきりと分かります。IGMP が無効のスイッチは、マルチキャスト データをどこに送信したらいいのか分かりません。そのため、ステーション 5 だけが関心のあるホストであるのに、イーサネット ステーション 4 および 6 が不必要なマルチキャスト データを受信します。

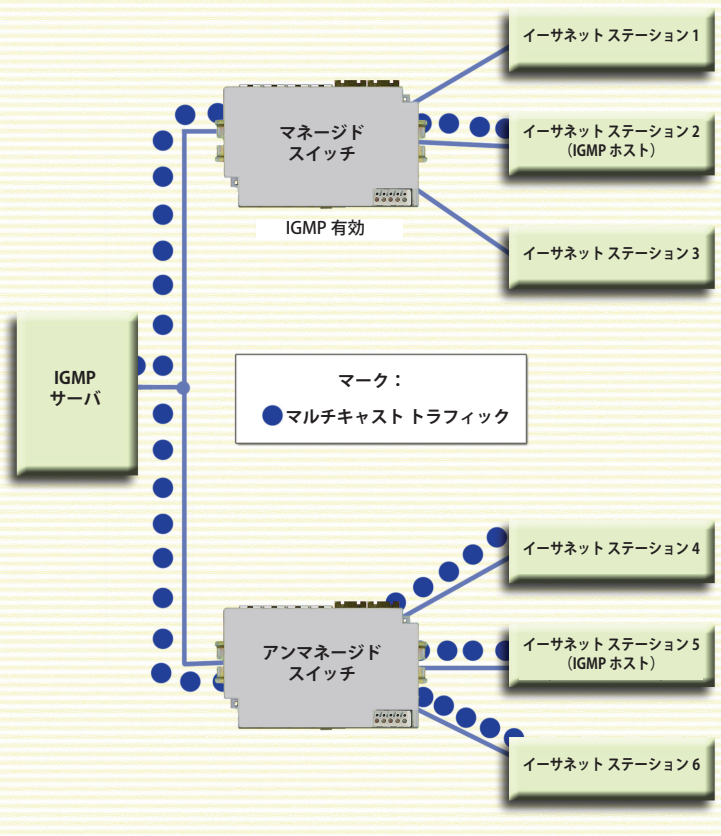


図 8-1 IGMP マルチキャスト フィルタリングの例

第 9 章 仮想ローカル エリア ネットワーク (VLAN)

9.1 VLAN 概論

VLAN は、帯域利用や安全性を促進するために、スイッチを流れるトラフィックを分離します。分離は、ポートのグループのメンバーシップ (ポートベース VLAN) 、または VLAN ID を含む IEEE 802.1Q タグ (タグベース VLAN) に基づいておこなわれます。

ポートベース VLAN は、ポートに入ってくるトラフィックを、そのポートが所属するポートのグループに制限します。たとえば、9 ポートスイッチで、ポート 1、3、5、7、9 がポートベース VLAN に位置する場合、ポート 3 に入ってくるブロードキャスト フレームは、ポート 1、5、7、9 (ポート 3 の VLAN メンバー) に送信され、ポート 2、4、6、8 (メンバーではない) には送信されません。

ポートは、2 つのポートベース VLAN のメンバーであることができますが、このコンフィギュレーションの結果が常に望ましかったり、簡単に予測できたりするものではありません。ポートベース VLAN を初期化するとき、スイッチは、各ポートがデータをメンバーであるすべてのポートベース VLAN のすべてのポートに送信できるよう設定します。たとえば、1 つの VLAN がポート 1 ～ 5 を持ち、他がポート 5 ～ 9 を持つ場合、ポート 1 ～ 4 のトラフィックはポート 1 ～ 5 へ、ポート 6 ～ 9 のトラフィックはポート 5 ～ 9 へ、そしてポート 5 のトラフィックはすべてのポートへ移動します。

タグベース VLAN は、フレームに関連する「タグ」の VLAN ID に基づいてトラフィックを制限します。VLAN タグは、アプリケーションまたは交換機によって、明示的にフレームに配置されるか、暗示的に到着したスイッチ ポートに基づいてフレームに割り当てられます。

VLAN ID は 12 ビットの長さで、利用可能な 4096 の ID を提供しますが、いくつかの値はリザーブされています。

0	タグは VLAN ルーティングに使用されていず、優先度情報を運ぶためだけに使用されていることを示します。(本マニュアル「第 7 章 QoS / CoS トピック」を参照)
1	スイッチ コンフィギュレーションと管理に使用
4095	802.1Q 規格では許可されません

注 : SL-5MS-MDM スイッチでは、PPP ポートは VLAN エッジ ポートです。したがって、すべての VLAN タグが除去されます。

9.2 VLAN 設定

[VLAN Settings Menu](VLAN 設定メニュー) にアクセスするには、[Main Menu](メイン メニュー) から [Setup](セットアップ) を選択し、さらに [Virtual LANs](VLAN) を選択します。このメニューは、VLAN のオペレーション モードの設定、および VLAN 定義の作成、編集、削除に使用されます。

9.2.1 VLAN のオペレーション モードの選択

VLAN モードはいくつかあり、さまざまなレベルの柔軟性と安全性を提供します。VLAN のオペレーション モードを選ぶには、VLAN Mode (モード) と表示されているオプション 1 を選択します。5 つの VLAN モードから 1 つを選択するように指示が出ます。

- **Disabled (無効)**– VLAN 処理はおこなわれません。VLAN ID およびポートベース VLAN は無視されます。
- **Port-Based (ポートベース)**– ポートベース VLAN のみフレーム経路の決定に使われます。VLAN ID は無視されます。
- **Standard (標準)**– ポートベース VLAN は無視されます。すべてのルーティングは、VLAN ID でおこないます。フレームのソースポートは、転送されるフレームの VLAN の一部である必要はありません。
- **Secure (セキュア)**– すべてのルーティングは、VLAN ID でおこないますが、フレームのソースポートがターゲット VLAN のメンバーでない場合は、フレームは落とします。例えば、ID 1024 のタグベース VLAN がポート 1 ～ 5 を含むように設定された場合、VLAN ID 1204 のタグを持つフレームがポート 6 に到着すると、フレームは転送されません。

注意 : VLAN と冗長化 (STP/RSTP/MSTP) が両方とも有効の場合は、物理 LAN は無傷でも 1 つ以上の VLAN が冗長化アルゴリズムにブロックされ、この VLAN 経由の通信が不能になる問題が発生することがあります。最良の方法は、常に接続性を保つために、すべてのスイッチ間接続をすべての VLAN メンバーにすることです。詳細は 84 ページの「9.4 RSTP つき VLAN」を参照してください。

9.2.2 コアタイプ

コア型のポートが送信するダブルタグ ("Q-in-Q") フレームのイーサタイプを指定します。0x のプレフィクスをつけた 16 進数で、値を指定することもできます。

9.2.3 ラーニング

この設定は、異なる VLAN のアドレスがどのようにスイッチによって学習されるかを制御します。

- **Shared (共有)** – すべての VLAN (MSTP が有効の場合、すべての VLAN は同じ MSTI に割り当てられます) が同じ転送データベースを使用。
- **Independent (独立)** – 各タグベース VLAN に使用されている転送データベースは、個別に設定が可能。

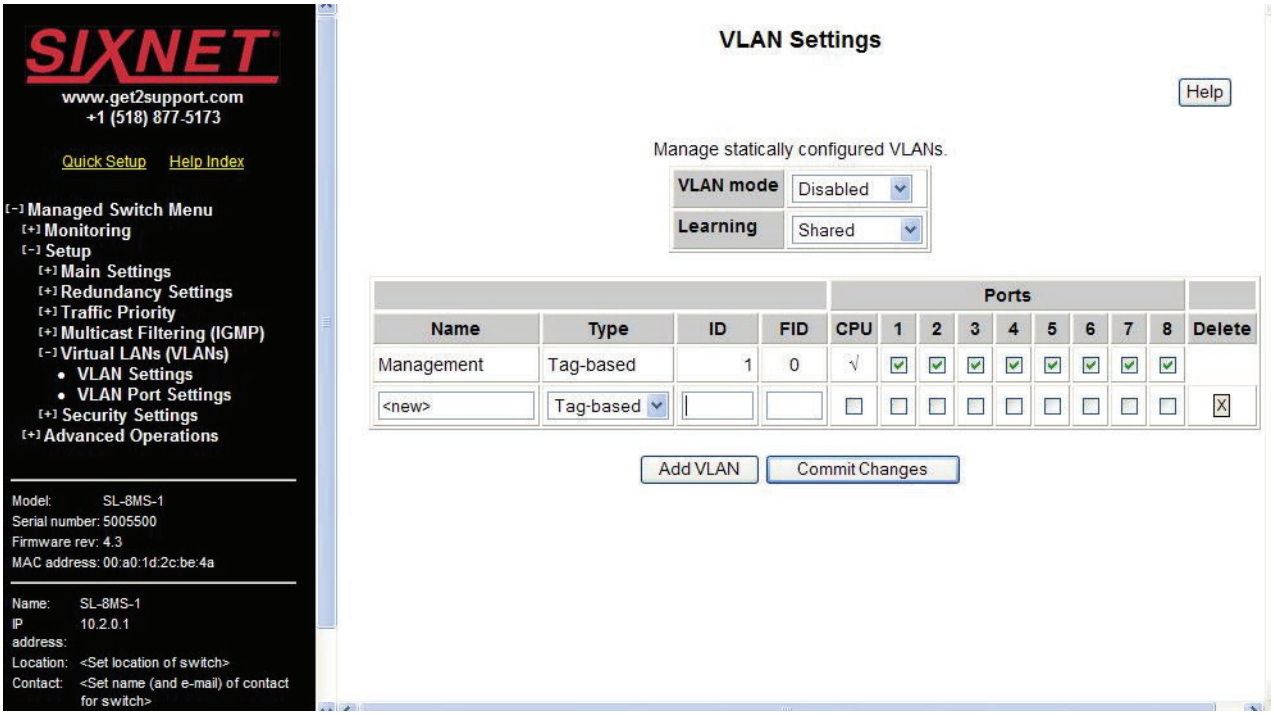
9.2.4 VLAN の追加、編集または削除

スイッチは、最大 63 のコンフィギュラブルな VLAN の処理ができます。このメニューでは、各オプション (option 2 から開始) が最大 8 つの VLAN コンフィギュレーションを処理できます。

例えば、スイッチに 16 の VLAN が定義されているとします。VLAN 設定メニューは、この場合、全部で 3 つの利用可能なオプションを表示します。最初のオプションは、VLAN モード選択用です。(このオプションは、常に存在) 2 つめのオプションは VLAN 1 ～ 8 の編集が可能で、3 つ目のオプションは VLAN 9 ～ 16 の編集が可能です。全部で

VLAN 設定

63 の利用可能な VLAN コンフィギュレーションがあるため、その中から選択できるよう、VLAN 設定メニューは最大 9 つの利用可能なオプションを表示します (新しい VLAN 作成のために、最後のオプションは常に「New」(新規) が最後に付きます)。オプション (2 ～ 9) を選択すると、下記に示されているものと類似したページが表示されます。



<new> と言う言葉が記述子としてあるエントリをリストから選択し、提示された 5 つのオプションから選択します。

- **Name (名前):**「Cell 7」、「Line 4」、「Building 58」といった VLAN のニーモニック名です。これは、表示にのみ使用されます。

- **Type (タイプ):** port-based (ポートベース) か tag-based (タグベース) かといった VLAN のタイプ。

- **ID:** タグベース VLAN のための、タグの中に見つける ID。この ID は、自分のネットワーク上に作成した個別の VLAN を識別するものです。VLAN ID は、2 から 4094 の範囲で指定します。例えば、上のスクリーン ショットでは、Engineering VLAN ID は 56 です。

  注 : 管理 VLAN ID を設定するときは注意してください。設定を行っている装置が VLAN で動作せず、接続したポートが適切な PVID とポートタイプ設定をされていない場合は、管理 VLAN はスイッチをアクセスできないようにしてしまい、再接続のためにはローカル シリアル接続が必要になる事があります。

- **FID:** タグベース VLAN のための独立ラーニングが有効のときに使用する転送データベースです。MSTP を実行中の場合は、同じ MSTP のすべての VLAN は、独立ラーニング モードの同じ転送データベースを使用するように設定しなければなりません。共有されたラーニングは、自動的に各 MSTI に異なる転送データベースを割り当てます。

  このフィルタリング ID は、複数 VLAN のグループ化を許容し MAC アドレス監視ページでの、フィルタリングを容易にします。

3 つの予約された VLAN ID があります。(使用しないでください)

- VLAN ID 0 は、優先度情報だけを運ぶタグを持つフレームの識別に使用されます。
- VLAN ID 1 は通常、スイッチ コンフィギュレーションおよび管理に使用されます。

注 : ギガビット スイッチ モデル (EK/SL-xMG) の管理 VLAN ID は、管理 VLAN ID を 1 から希望の数字に変更設定可能です。

- VLAN ID 4095 は、802.1Q 規格では許可されません。

- **Ports (ポート):** この VLAN に含まれているポートです。

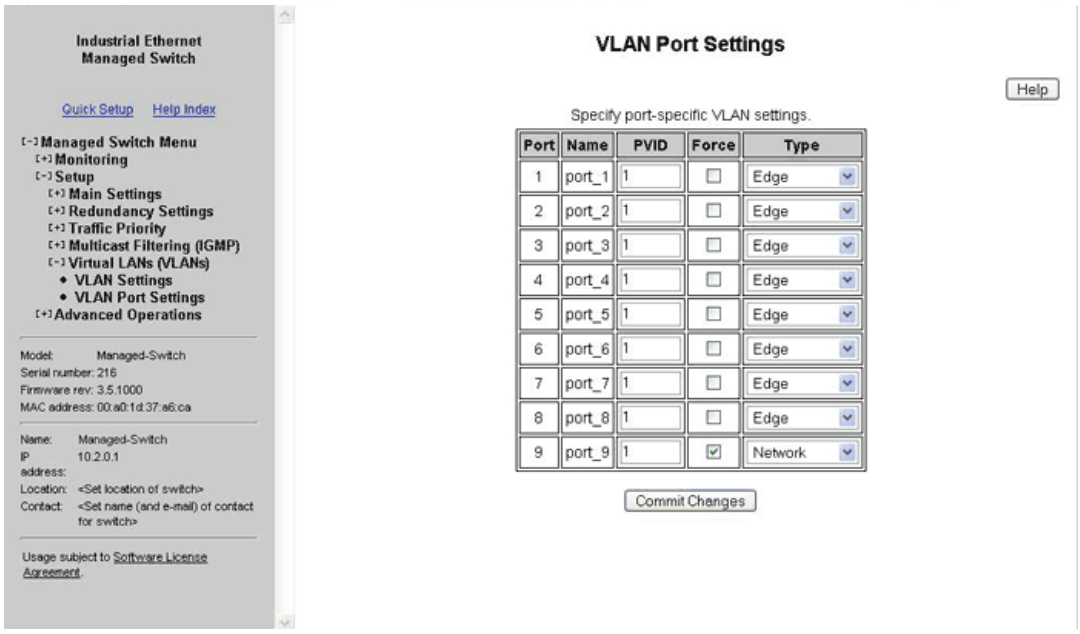
この VLAN に含めるポートを選択するには、含めたいポートの各ボックスに印を入れてください。「CPU」ボックスに印が入っていないと、この VLAN からスイッチに通信することはできませんので注意してください。

注 : タグベース VLAN と連動しているとき、VLAN に含まれるポートは、VLAN タグを処理することができない他のネットワーク装置 (データを適切にルーティングするためのタグを要求する)、もしくはエンド装置につながることがあります。VLAN ポート設定ページを利用して、各ポートに適切なタイプを設定します。

- **Delete (削除):** 変更コミット時に対応 VLAN が削除される様に選択します。これが選択されているときに変更がコミットされると、この VLAN は削除されます。

9.3 VLAN ポート設定

各スイッチ ポートは、ポートを出入りするフレームで、どのように VLAN タグが処理されるかを制御する設定ができます。



- **PVID:** これがポートのデフォルト VLAN ID です。VLAN タグ無しや、優先度のみ VLAN タグ付き (特別な VLAN ID 0 を含むもの) でポートに到着したフレームに適用されます。希望する PVID を設定し、そのポートに到着したタグ無しパケットが、希望する VLAN の他のポートに転送されるようにします。

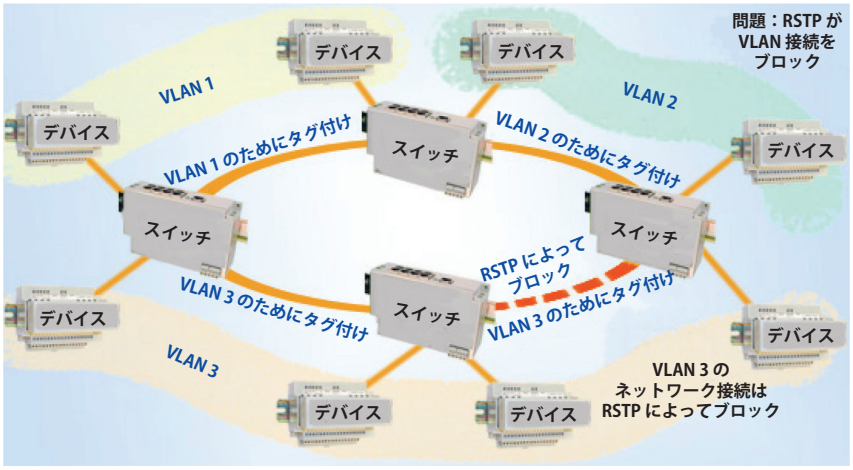
注 : スイッチ管理およびコンフィギュレーションは、PVID が 1 (デフォルト) に設定されている場合にのみポートを通じて可能です。PVID を他の値に設定すると、スイッチはそのポート経由で管理や設定ができなくなります。(スイッチの設定に使っているシステムが、明示的に VLAN 1（すなわち管理 VLAN）にフレームをタグ付けできない限り)

- **Force (強制):** これに印が入っていると、どのような既存タグであろうとも、このポートに到着するすべてのフレームに PVID が強制されます。
- **Type (タイプ):** ポートタイプはこのポートから送信されるフレームで、どのようにタグが処理されるかを、制御します。
  - **Network (ネットワーク):** このポートから送信されるすべてのフレームにタグが付きます。フレームがスイッチに入ったときにタグが提示されない場合、ソース ポートの PVID が使われます。通常ネットワーク ポートは、スイッチの多くのまたはすべてのタグ ベース LAN のメンバーであり、他のスイッチへの VLAN トラフィックの転送に使用され、タグに基づいて他のネットワーク セグメントに配信されます。ネットワーク ポートは、メンバーである VLAN にだけパケットを送信することができます。
  - **Edge (エッジ):** このポートから送信されるフレームにタグは付きません。(この設定は、従来装置につながるポート、または VLAN に対応しないエンド装置のために使用されます)
  - **Transparent (トランスペアレント):** 転送されるフレームは、変更されません。

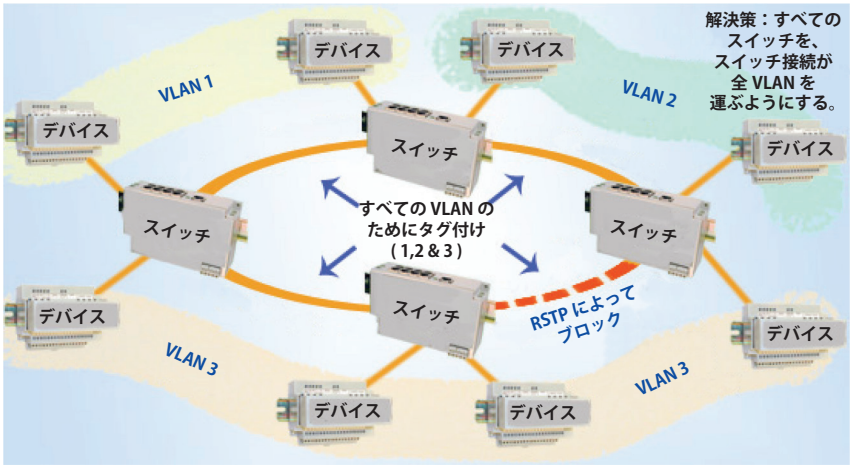
9.4 RSTP つき VLAN

VLAN と冗長化の両方を有効にするときは細心の注意を払わなければなりません。そうしないと、通信障害が発生することがあります。

下の図表は、ラピッド スパニング ツリー プロトコル (RSTP) と VLAN を同時に実行したときの問題を表したものです。IEEE 802.1D ベースの RSTP は、VLAN コンフィギュレーションに気づいていません。したがってこの例では、VLAN 3 ネットワーク ポートの 1 つがブロックされます。(この章の VLAN ポート設定トピックのネットワーク タイプ ポートについてを参照してください) これにより、VLAN 3 はデータをすべてのメンバーに転送できるということができません。



上記の問題に対する解決策は、すべての「ネットワーク」タイプ ポートを、ネットワークの全 VLAN を運ぶように設定することです。言い換えれば、ネットワーク ポートは、スイッチに定義された全 VLAN のメンバーであるべきなのです。次の図表の例を見ると、VLAN 3 はすべてのメンバーに、他のネットワーク ポート接続経由で転送することができます。そして RSTP 接続のブロックの影響を受けていません。


解決策：すべての
スイッチを、
スイッチ接続が
全 VLAN を
運ぶようにする。
VLAN 1
VLAN 2
VLAN 3
VLAN 3
デバイス
デバイス
デバイス
デバイス
デバイス
デバイス
デバイス
スイッチ
スイッチ
スイッチ
スイッチ
すべての VLAN の
ためにタグ付け
(1,2 & 3)
RSTP によって
ブロック

第 10 章 モデム アクセス設定 (-5MS-MDM のみ)

10.1 リモート アクセス概論

ポイント ツー ポイント プロトコル (PPP) は、シリアル接続経由で「IP」パケットを用いて 2 台のコンピューターまたはその他の装置を接続するために使用されます。通常、モデムと電話回線を使用します。PPP は、ピア ツー ピア プロトコルとしてイーサネット ネットワーク接続をシミュレートします。しかし、クライアントとしてリンクを確立するために電話をかけるシステムと、サーバとして電話を受けるシステムを参照するのが便利で慣例です。一般的に、クライアントはアクセスが許可される前に、認証を受けなければなりません。

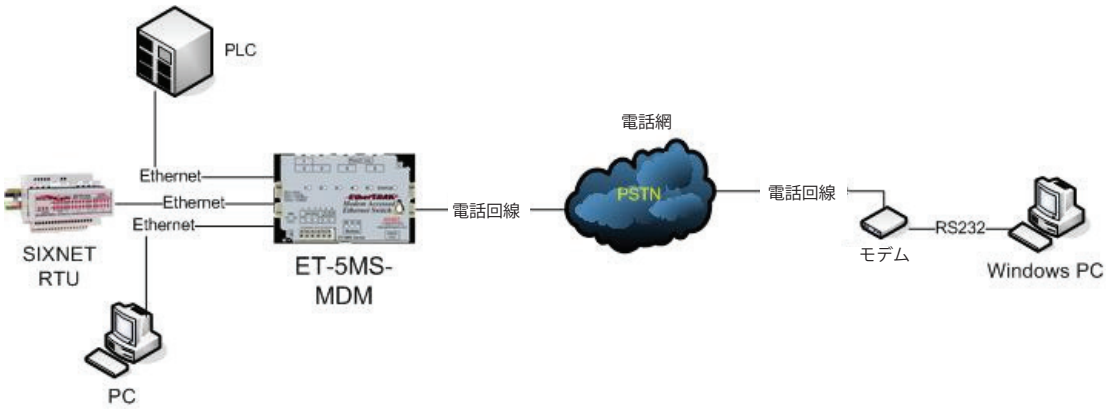
イーサネット ネットワークにリモート アクセスをするには、モデム ダイヤル イン、ダイヤル アウト、およびサイト ツー サイトの 3 つの方法があります。各方法がどのように機能するかの基本的な説明を、この概論で行います。Microsoft Windows PC の設定に関する詳細は、116 ページの「付録 H リモート アクセス チュートリアル (-MDM Models Only)」を参照してください。

10.1.1 ダイヤル イン

ダイヤル インの方法では、Microsoft Windows PC は、PPP 設定ウィンドウでサーバとして設定されているイーサネット モデム (SL-5MS-MDM) にダイヤル インするクライアントの役割を務めます。Microsoft Windows のダイヤル アップ ネットワーキングとリモート アクセス サービス (RAS) を利用して、ユーザーは電話を掛けます。ET/SL-5MS-MDM は、モデム設定のページで設定したベルの回数に応じて電話に応答します。モデムツーモデム接続が確立すると、パソコンは事前に設定済みのユーザー名とパスワードを、クライアント認証のために電話回線を通じてサーバへ送信します。ET/SL-5MS-MDM はその認証を、リモート ユーザー ページで設定されたユーザーのデータベースに基づいて承認、または却下します。接続が無事に交渉されると、ユーザーはスイッチに接続しているイーサネット装置にアクセスできるようになります。次の図は、接続を視覚的に説明しています。

10.1.2 ダイヤル アウト

ダイヤル アウトの方法では、パソコン、Sixnet RTU または他の装置が、パソコン宛てのイーサネット メッセージを生成します。ET/SL-5MS-MDM が PPP 設定ウィンドウでクライアントモードに設定されていると、メッセージを受け取り、イーサネットモデムがダイヤルして Microsoft Windows PC との PPP 接続を確立するまで、メッセージをバッファします。そして、メッセージはパソコンに転送されます。下の図は、接続を視覚的に説明しています。



10.1.3 サイト ツー サイト

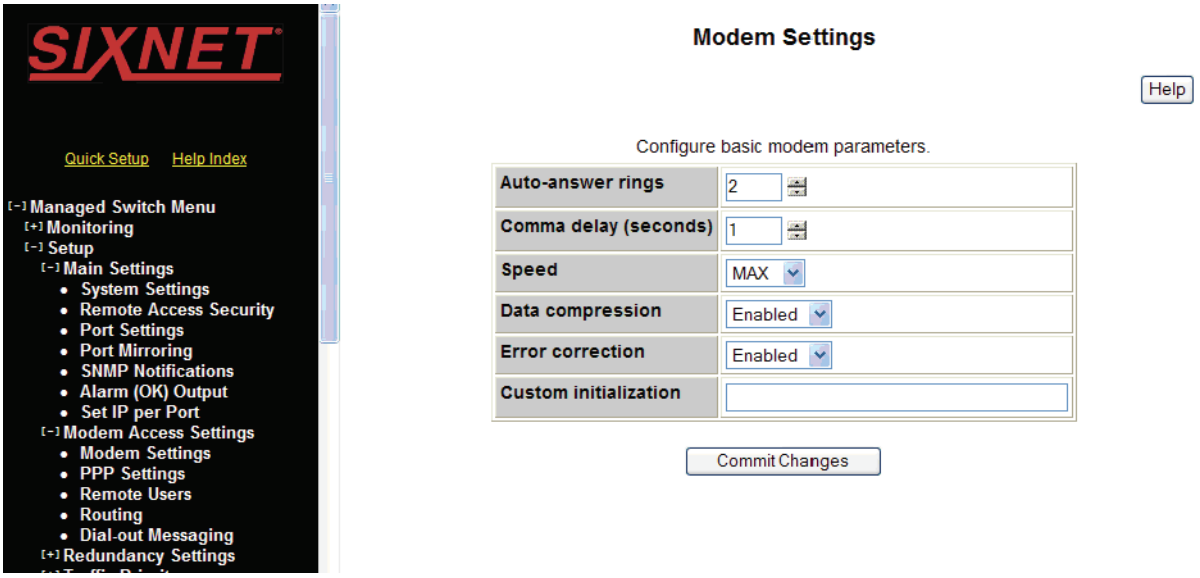
サイト ツー サイトの方法では、PPP 設定ウィンドウでクライアントに設定されている ET/SL-5MS-MDM が、電話をかけて PPP 設定ウィンドウでサーバに設定されている他の SL-5MS-MDM に PPP 接続を 行います。これにより、両方のサイトのシステムがデータを交換できます。下の図は、接続を視覚的に説明しています。

注 : 正しいサブネット マスクと IP アドレスを SL-5MS-MDM およびそれに接続している装置に割り当てることは、ルーティングおよびダイヤリングにとって重要です。詳細は PPP 設定のページを参照してください。

注 : SL-5MS-MDM スイッチでは、PPP ポートは VLAN エッジ ポートです。すべての VLAN タグが削除されます。

10.2 モデム設定

モデムのパラメータをモデム ツー モデム接続ができるように設定します。



- **Auto-answer rings (自動応答):** (0 ～ 255、デフォルト = 2) モデムが電話に応答するまでのベルの回数を指定します。0 は自動応答しません。注 : PPP サーバ モードでは、[Auto-answer rings] は最低 1 で、発信者番号セキュリティは最低 2 です。

- **Comma delay (コンマ遅延) (秒):** (0 ～ 255、デフォルト = 1) 電話番号中のコンマに応じてダイヤリングを遅延させる秒数を指定します。

- **Speed (速度):** (デフォルト = MAX) モデム接続で使用する速度をボーで指定します。MAX とは、発呼および着呼モデムによって交渉された最高速度を使用するということです。

- **Data Compression (データ圧縮):** (デフォルト = Both) データ圧縮が送信データ、受信データ、両方またはどちらでもない、に使用されるかどうかを指定します。データ圧縮はすべての速度で機能するわけではなく、また受信および送信両方のモデムで使用されなければなりません。

  - **None (なし):** リンクのデータ圧縮が無効

  - **Transmit (送信):** 送信データにだけ V.42bis データ圧縮技術を使用

  - **Receive (受信):** 受信データにだけ V.42bis データ圧縮技術を使用

  - **Both (両方):** 双方向に V.42bis データ圧縮を使用

- **Error Correction (エラー訂正):** (デフォルト = Enabled(有効)) エラー訂正の使用を指定します。エラー訂正はすべてのモデム速度で機能するわけでありません。有効に設定されていて、エラー訂正が適切で利用可能な場合に使用されます。

- **Custom initialization (カスタム初期化):** (デフォルト = 空白) このフィールドは、特別な状況下でモデムのパラメータを設定するために使用されるモデムのカスタム初期化文字列を指定します。AT で始める必要があり、最大 48 文字です。AT コマンドの E1 および V1 は、初期化文字列の中で使用しないでください。モデムと適切に通信するためには、スイッチはこの機能を無効にする必要があるからです。

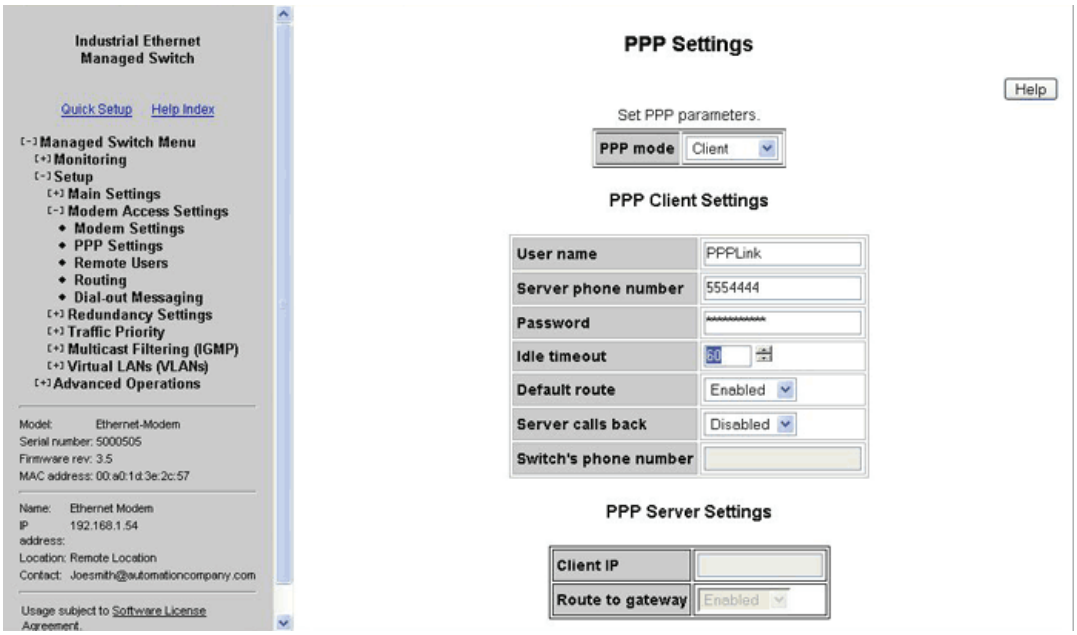
10.3 PPP モード

スイッチが PPP サーバ、PPP クライアント、またはどちらでもないかを指定します。

- **Disabled (無効)**– スイッチは PPP 接続を開始せず、受け入れません。
- **Client (クライアント)**– スイッチはサーバへの PPP 接続を開始します。
- **Server (サーバ)**– スイッチはクライアントからの PPP 接続を受け入れます。

10.4 PPP クライアント設定

他のサブネット宛てのイーサネット メッセージを受け取った時に、PPP サーバへダイヤルするように SL-5MS-MDM を設定します。



- **User name (ユーザー名):** (デフォルト = PPPLink) PPP サーバへ接続するときにこのクライアントのユーザー名を指定します。
- **Server phone number (サーバ電話番号):** PPP サーバの電話番号を指定します。電話回線にアクセスするのに必要であれば、9 のようなプレフィクスを含まなければなりません。また、プレフィクスと電話番号の間にコンマを含めて遅延させることも可能です。
- **Password (パスワード):** (デフォルト = Link2Sixnet) PPP サーバへ接続するときにこのユーザーのパスワードを指定します。

- **Idle timeout (アイドル タイムアウト):** (デフォルト = 60 秒) リンクを自動的に落とす前の、アイドル タイムの秒数を指定します。0 はアイドル時にリンクを落としません。

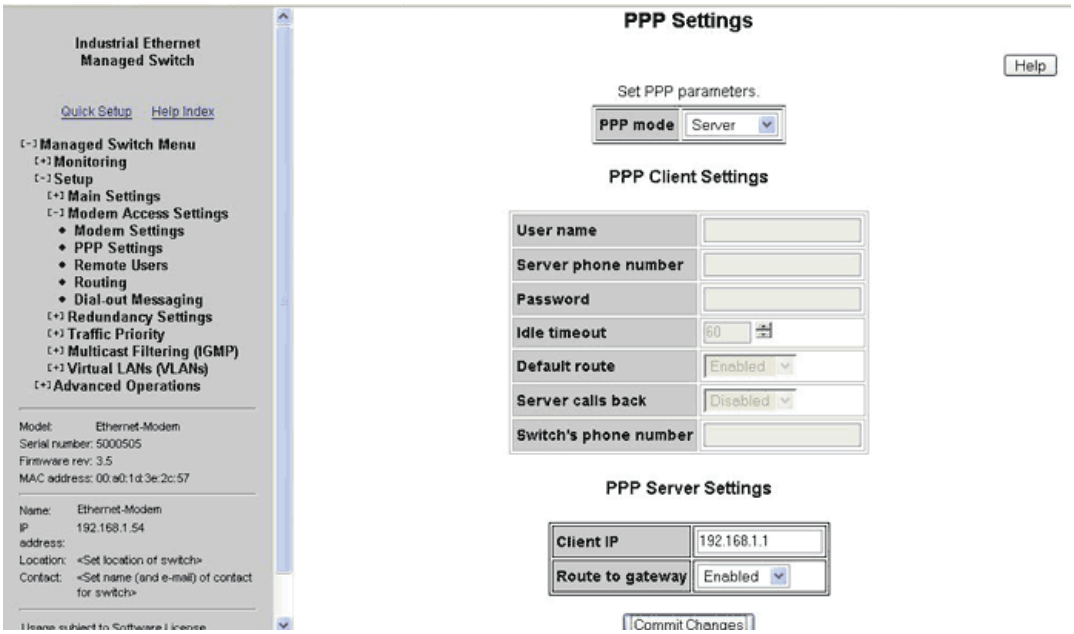
- **Default route (デフォルト ルート):** (デフォルト = Enabled (有効)) PPP サーバに接続されている時、サーバへのリンクをデフォルト ルートとして使用します。

- **Server calls back (サーバ コールバック):** (デフォルト = Disabled (無効)) このスイッチがリンクを開始するときリモートシステム側から接続を切断して、コールバックするかどうかを指定します。

- **Switch's phone number (スイッチの電話番号):** (デフォルト = 空白) サーバがスイッチにコールバックするときに使用する電話番号。サーバがコールバック用に特定の番号を使用するように設定されているときは、空白でいいです。

10.5 PPP サーバ設定

PPP クライアントからのコールに応答し、IP アドレスを与えるように SL-5MS-MDM を設定します。



- **Client IP (クライアント IP):** (デフォルト = 空白) PPP 接続が確立されたとき、PPP クライアントに割り当てられる IP アドレスを入力します。注 : ET/SL- 5MS-MDM のサブネットにフリー IP アドレスを選択することを推奨します。

- **Route to Gateway (ゲートウェイへのルート):** (デフォルト = Disabled(無効)) 有効のとき、ET/SL-5MS-MDM はシステム設定コンフィギュレーション ページで設定されたデフォルトのゲートウェイへ、外部サブネット宛てのすべてのメッセージを送信します。

10.6 サーバおよびクライアント モードのための IP アドレス コンフィギュレーション

正しい IP アドレスを設定することは、メッセージが正しく ET/SL- 5MS-MDM を通るようにするために重要です。スイッチの設定を行うときは、次のことに注意して進めてください。

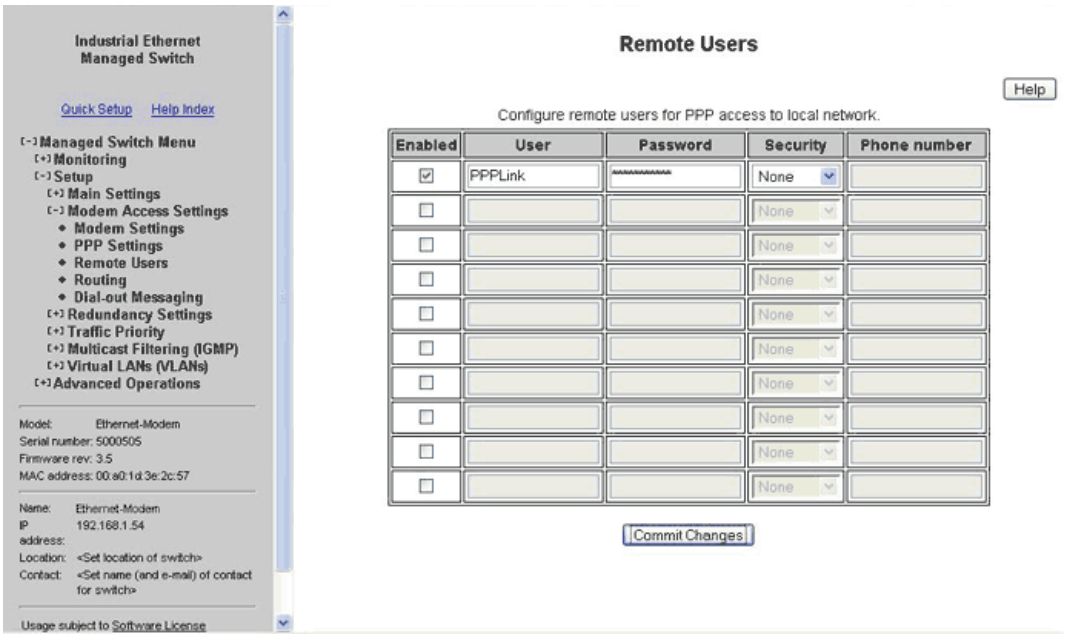
- **Dial-In usage scenario (ダイヤル イン使用シナリオ):** クライアントとしてダイヤルインするパソコンと、サーバとして応答している ET/SL-5MS-MDM は同じサブネット マスク上になければなりません。PPP 設定でクライアント IP を設定するときは、スイッチおよびスイッチに接続するデバイスとして適合性がある (同じサブネット上である) ことを確認します。

- **Dial-Out usage scenario (ダイヤル アウト使用シナリオ):** コールアウトするクライアントとして設定した ET/SL-5MS-MDM は、コールを受けるパソコンとは異なるサブネット上になければなりません。IP アドレスを ET/SL-5MS-MDM および ET/SL-5MS-MDM に接続している装置に割り当てる際は、Windows パソコン リモートアクセスサービス (RAS) で設定された IP アドレスの範囲と適合性がない (同じサブネット上にない) ことを確認します。クライアント ET/SL-5MS-MDM に接続する装置のデフォルト ゲートウェイは、ET/SL-5MS-MDM に割り当てられた IP アドレスを設定しなければなりません。

- **Site-to-Site usage scenario (サイト ツー サイト使用シナリオ):** コールアウトするクライアントとして設定した SL-5MS-MDM は、コールを受ける SL-5MS-MDM とは異なるサブネット上に存在しなければなりません。IP アドレスをクライアント SL-5MS-MDM およびクライアント SL-5MS-MDM に接続している装置に割り当てる際は、サーバ SL-5MS-MDM の IP アドレスと PPP 設定コンフィギュレーションページで設定したクライアント IP が適合性がない (同じサブネット上にない) ことを確認します。クライアント ET/SL-5MS-MDM に接続している装置のデフォルト ゲートウェイは、クライアント SL-5MS-MDM に割り当てられた IP アドレスでなければなりません。サーバ SL-5MS-MDM に接続している装置のデフォルトゲートウェイは、サーバ SL-5MS-MDM に割り当てられた IP アドレスでなければなりません。

10.7 リモート ユーザー

PPP サーバとして設定された SL-5MS-MDM への PPP 接続の確立を承認するユーザーのデータベースを作成します。



- **Enabled (有効):** (デフォルト = Disabled (無効)) ユーザー設定を変更せずにユーザーを有効または無効にします。

- **Disabled (無効)**– このユーザーからのコールを受け付けません。
- **Enabled (有効)**– このユーザーからのコールを受け付けます。

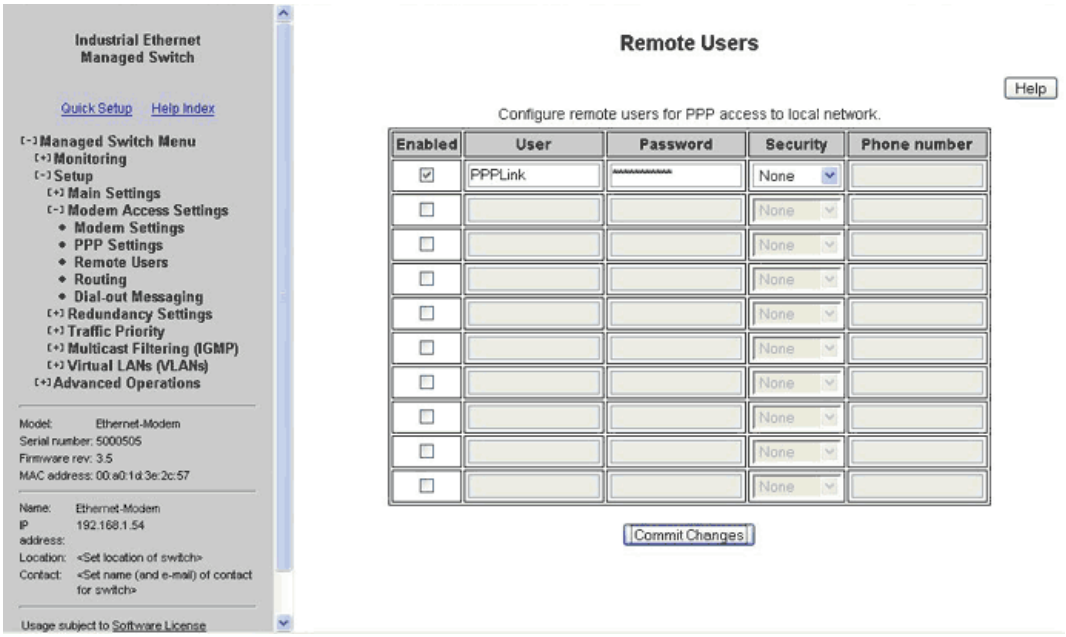
- **User (ユーザー):** ユーザー名を指定します。ユーザー名は最大 16 文字の固有のものでなければなりません。
- **Password(パスワード):** ユーザーのパスワードを指定します。パスワードは大文字と小文字を区別します。アルファベット、数字、記号を含む最大 32 文字です。
- **Phone number (電話番号):** ユーザーの電話番号を指定します。複数のユーザーで同じ電話番号を使用することができます。電話番号は、caller ID (発信者番号) によって提供される番号として用い、照合に利用可能で、最大 32 文字です。

Security (セキュリティ): このユーザーのセキュリティ レベルを選択します。

- **None (なし)**– ユーザーがコールインするとき、接続が維持され、ユーザーはシステムを使用することが可能です。
- **Caller ID** – ユーザーがコールインするとき、発信番号が設定番号と一致する場合、接続が維持されます。

10.8 ルーティング

PPP とイーサネット インターフェイスの片方または両方のルーター情報プロトコル (RIP) を有効にします。

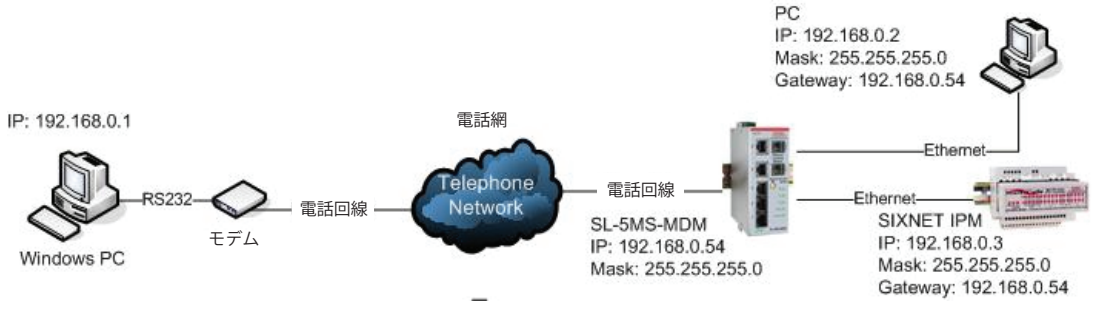


- **RIP mode (モード):** (デフォルト = Disabled) RIP プロトコル使用の有効無効を選択します。このプロトコルは、PPP 接続を通じて 2 つの ET/SL-5MS-MDM 間で、またはイーサネット接続の ET/SL-5MS-MDM と 1 つ以上のルーター間でルーティング テーブル情報を交換するために使用されます。
- **Send (送信):** (デフォルト = version 2) ルーティング テーブル情報を要求するために使用する RIP プロトコルの方式を選択します。

- **Receive (受信):** (デフォルト = version 2) 応答または未承諾メッセージのルーティング テーブル情報を受諾するために使用する RIP プロトコルの方式を選択します。

10.9　ダイヤル イン　シナリオ　コンフィギュレーション

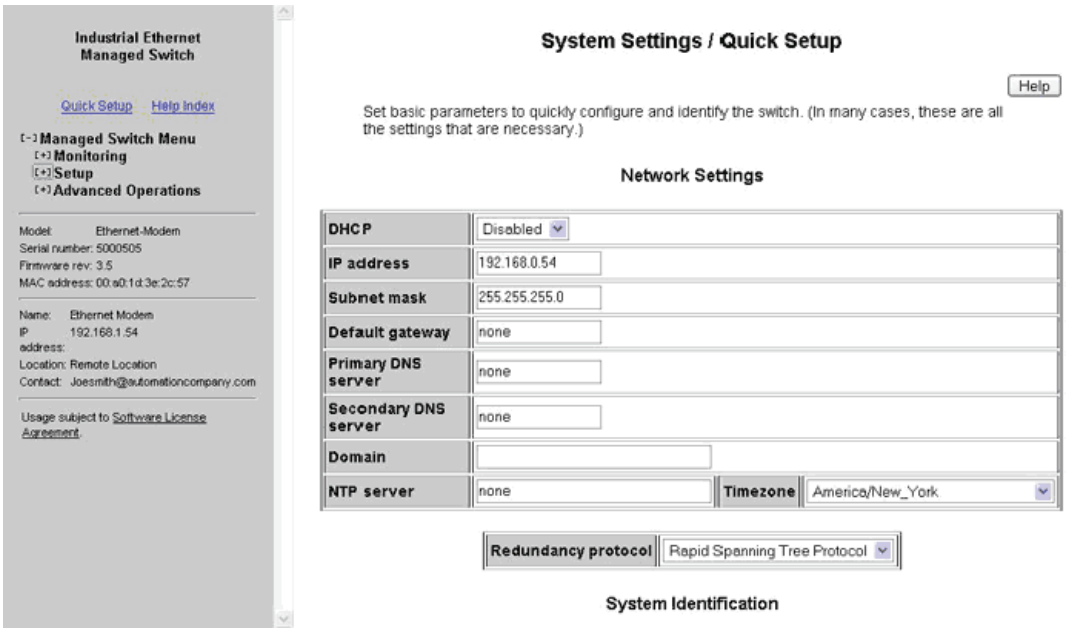
典型的なダイヤル イン　シナリオでは、コールインしているパソコン (クライアント) と、応答している ET/SL-5MS-MDM(サーバ)、ET/SL-5MS-MDM に接続している装置は同じサブネット マスク上になければなりません。接続を試みる前に、すべての装置のすべての IP アドレスが、設定したサブネットに適切なものであることを確認してください。また、5MS-MDM に接続している装置のゲートウェイの設定も必要です。下の例を参照してください。



10.9.1　サーバとしての 5MS-MDM コンフィギュレーション

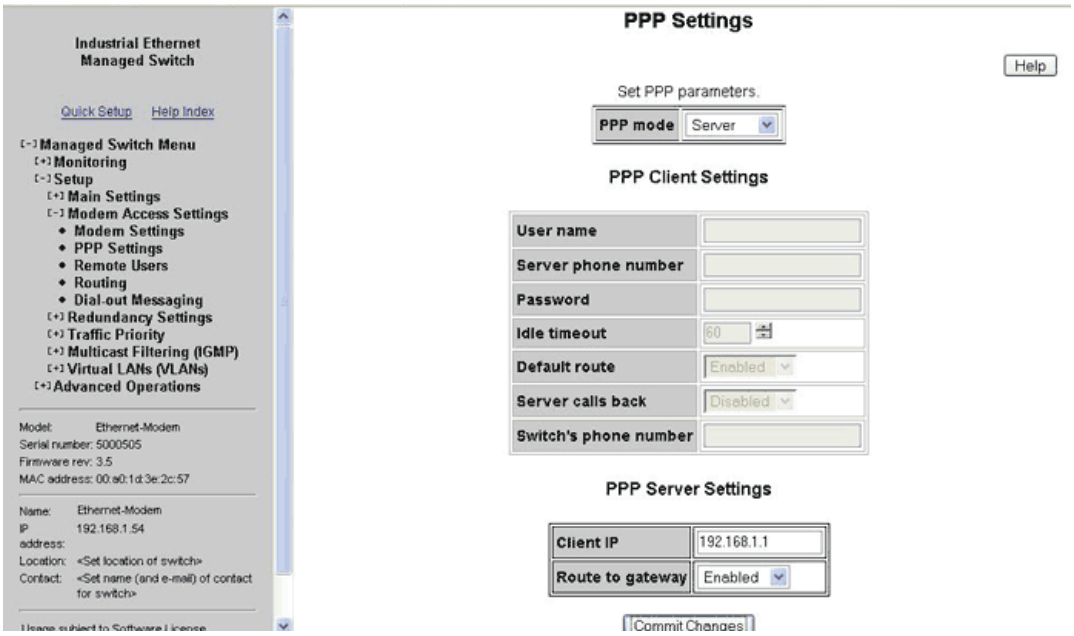
ET/SL-5MS-MDM はサーバとして、ダイヤルインするパソコンに IP アドレスを割り当てる必要があります。ET/SL-5MS-MDM の LAN で使用されていない IP アドレスを定義しなければなりません。そして、リモート ユーザーのリストを追加することにより、リスト上の人物だけがリモート ネットワークに接続できる様になります。次の手順に従ってください。

1. まず、IP アドレスを ET/SL-5MS-MDM に割り当てます。そのために、ET/SL-5MS-MDM のテキスト UI の Quick Setup (クイック セットアップ) ページに移動します。(下のキャプチャー画像を参照してください)

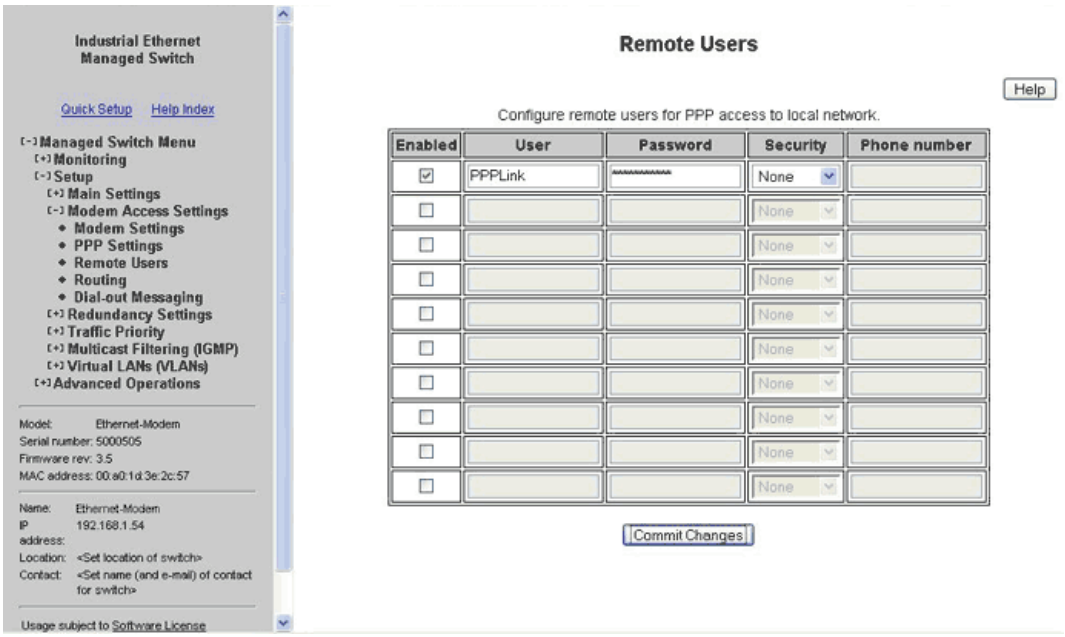


2. 次に [Remote Access Settings](リモート アクセス設定) から [PPP Settings](PPP 設定) にアクセスし、ET/SL-5MS-MDM の PPP モードをサーバに設定します。

3. そして、Windows PC がダイヤル インするときに割り当てる IP アドレスを含め、サーバ設定を設定します。



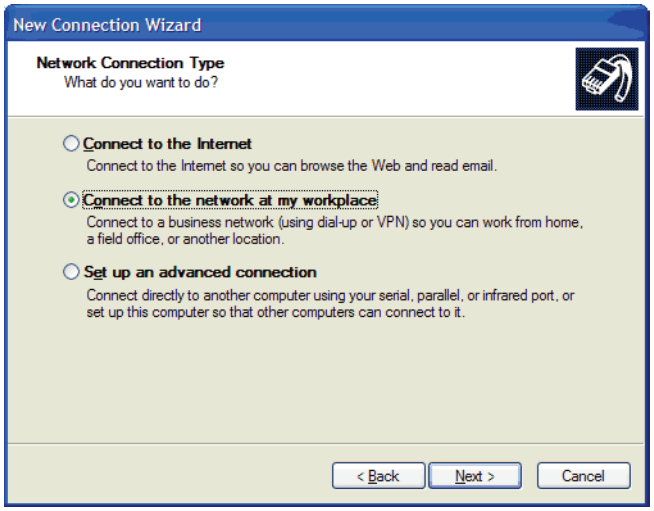
4. 最後に、リモートデバイスにダイヤルインしたりアクセスしたりすることを許可されるリモートユーザーのリストを追加します。この場合、デフォルトのユーザー名は「**PPP Link**」、パスワードは「**Link2 Sixnet**」を使用します。



10.9.2　クライアントとしての Microsoft Windows PC コンフィギュレーション

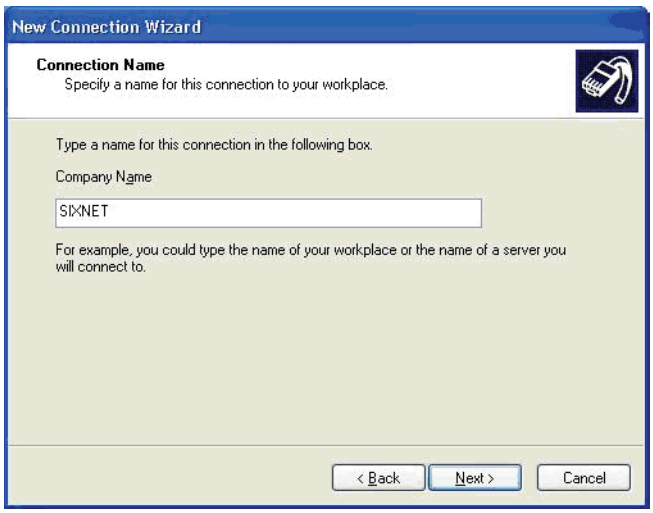
EMicrosoft Windows がダイヤルできるように適切に設定するためには、まず、モデムをインストールする必要があります。モデムの適切なインストール方法の説明は、ユーザー マニュアルのモデムのページを参照してください。それから次の手順に従ってください。

1. Microsoft Windows の [コントロールパネル] で [ネットワーク接続] を選択します。
2. Windows が [ネットワーク接続] ウィンドウを開きます。
3. [ファイル] メニューから [新規接続] を選択すると、新しい接続ウィザードが開きます。
4. [次へ] をクリックします。
5. [職場のネットワークに接続する] を選択し、[次へ] をクリックします。



6. [ダイヤルアップ接続] を選択し、[次へ] をクリックします。

7. この接続に固有の企業名を入力します。この例では、「Sixnet」を使用します。[次へ] をクリックします。



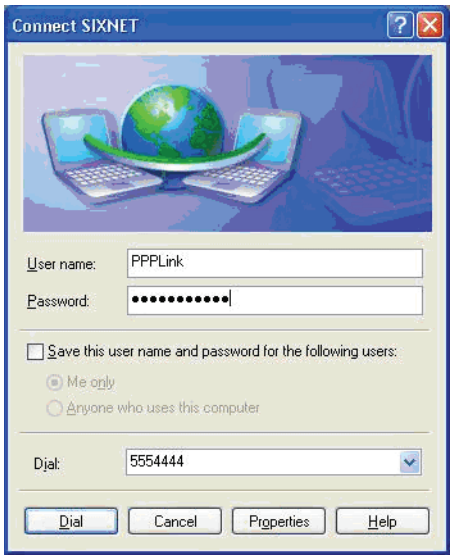
8. ET/SL-5MS-MDM が接続している電話回線の欄に電話番号を入力します (ここでは、電話番号に　5554444 を使用します)。[次へ] をクリックします。

9. この接続で使用するコンピューターの可用性を選択します。[次へ] をクリックします。

10. [終了] をクリックしてウィザードを終了します。接続ウィンドウが開きます。

11. ET/SL-5MS-MDM のリモート ユーザー ページで設定済みのコールするユーザー名とパスワードを入力します。ここでは、デフォルト ユーザー名に「PPPLink」、パスワードに「Link2Sixnet」を使用しています。

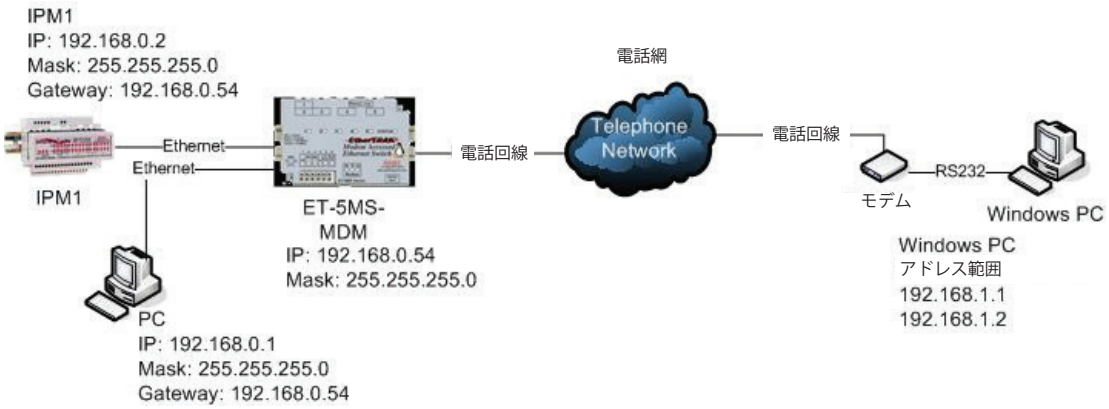
12. [ダイヤル] をクリックしてコールを始めます。



13. 接続が無事に確立されると、作成済みのダイヤルアップ アイコンが接続したことを表示し、ET/SL-5MS-MDM に接続している装置にアクセスできるようになります。

10.10　ダイヤル アウト　シナリオ　コンフィギュレーション

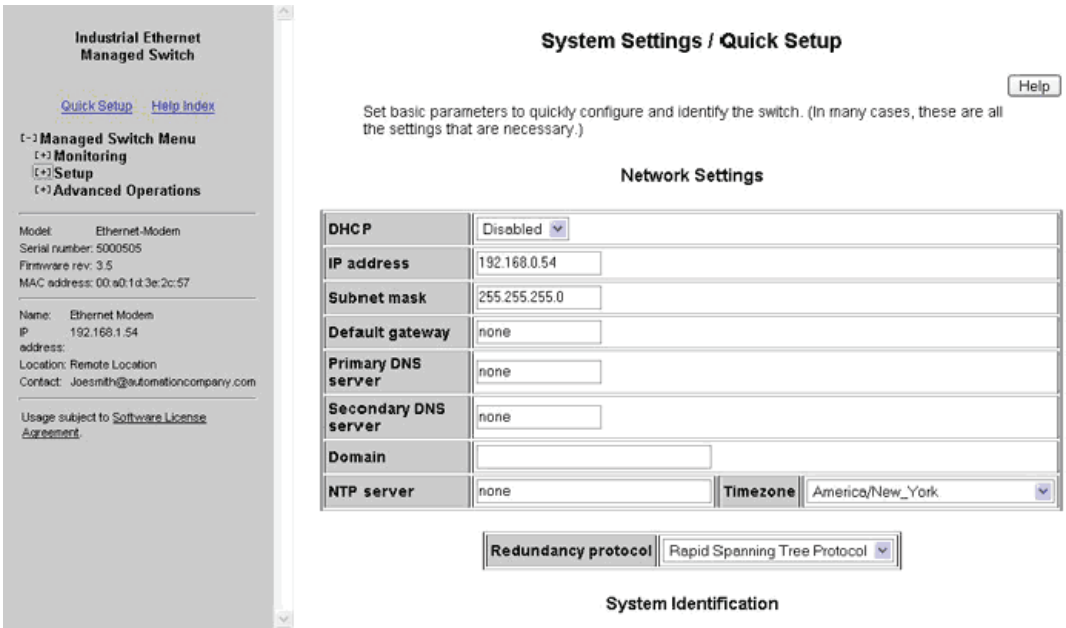
典型的なダイヤル アウト　シナリオでは、コール インしている ET/SL-5MS-MDM (PPP クライアント) と、ET/SL-5MS-MDM に接続されている装置は、応答しているパソコン (PPP サーバ) とは異なるサブネットマスク上に存在しなければなりません。接続を試みる前に、すべてのデバイスのすべての IP アドレスが、設定したサブネットに適切なものであることを確認してください。下の例を参照してください。



10.10.1　PPP クライアントとしての 5MS-MDM コンフィギュレーション

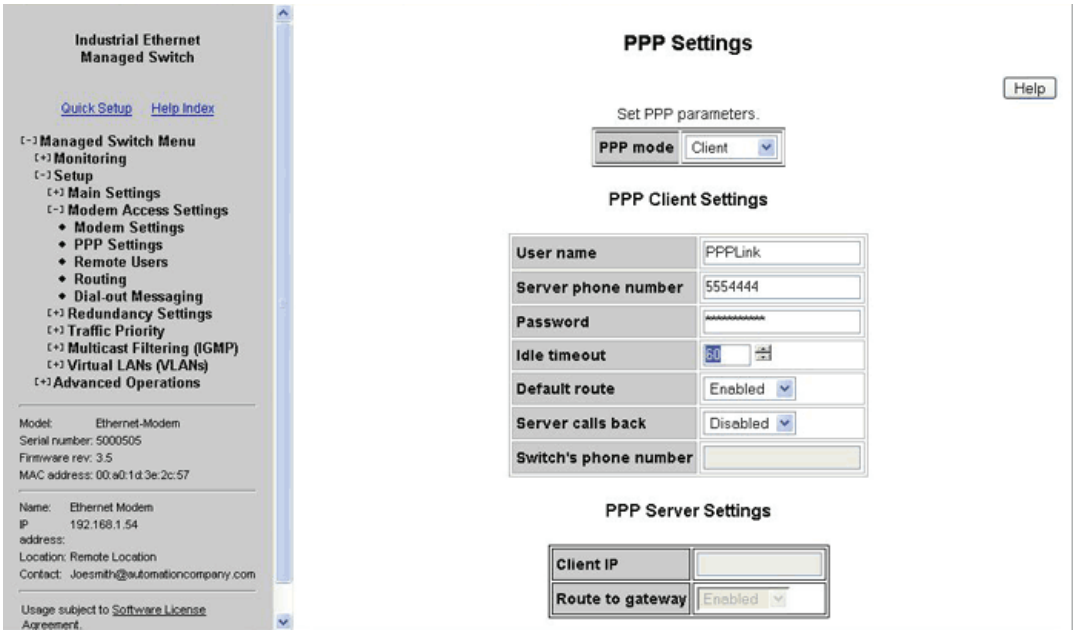
ET/SL-5MS-MDM-1 はクライアントとして、外部ネットワーク宛ての IP アドレスまたは同じ IP アドレス スキームでない IP アドレスを受け取ると、あらかじめ認定された番号にコールします。PPP　接続が確立されると、ET/SL-5MS-MDM-1 は、モデム ポートのサーバとして設定されたパソコンから IP アドレスを取得します。

1. ET/SL-5MS-MDM-1 の設定には、まず、イーサネット モデムのローカル LAN (イーサネット) ポートに接続されている装置に割り当てられた IP アドレスと適合する IP アドレスを割り当てます。そのために、テキスト UI の Quick Setup (クイック セットアップ) ページに行きます。(下のスクリーン ショットを参照してください)

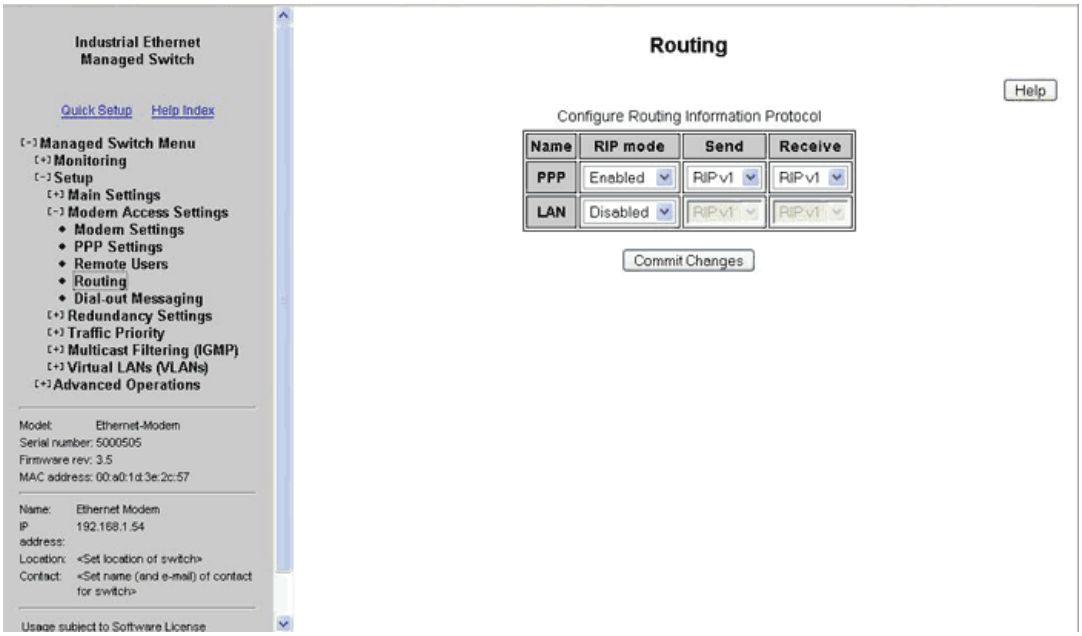


2. 次に、イーサネット モデムをクライアント モードに設定し、ダイヤル アウトすべき事を知って PPP 接続を開始をできるようにします。そのために、[Setup](セットアップ) → [Modem Access Settings](モデム アクセス設定) → [PPP Settings](PPP 設定) の順にアクセスし、[PPP mode](PPP モード) で [Client](クライアント) を選択します。(下のスクリーン ショットを参照してください)

3. そして、クライアントパラメータを選択します。そのために、[Setup] → [Modem Access Settings] → [PPP Settings] → [Client settings](クライアント設定) の順にアクセスします。PPP サーバが承認するように設定したものと同じユーザー名とパスワードを設定します。(デフォルトのユーザー名とパスワードは下記のとおりです) サーバの電話番号は、PPP サーバに接続している電話番号です。デフォルト ルートを有効にし、希望通りのアイドル タイムアウトを設定します。



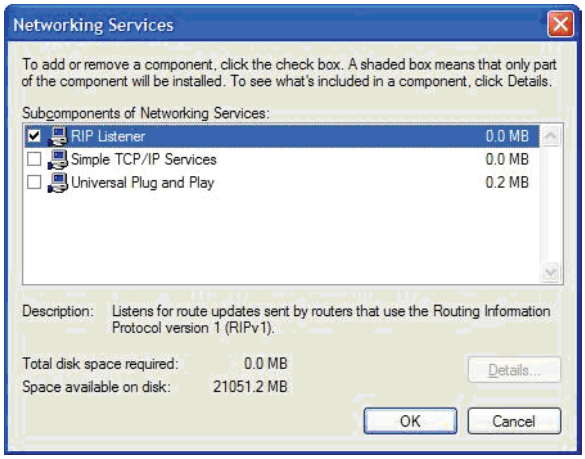
4. 最後に、PPP インターフェイスの RIP (ルーティング情報プロトコル) バージョン 1 を有効にして、パソコンと ET-5MS-MDM がルーティング情報を交換できる様にします。RIP を有効にするには、[Setup] → [Modem Access Settings] → [PPP Settings] → [Routing](ルーティング) の順にアクセスします。PPP インターフェイスの RIP モードを有効に設定し、送受信の両方に RIP v1 を選択します。(次のスクリーン ショットを参照してください)



10.10.2　PPP サーバとしての Microsoft Windows PC コンフィギュレーション

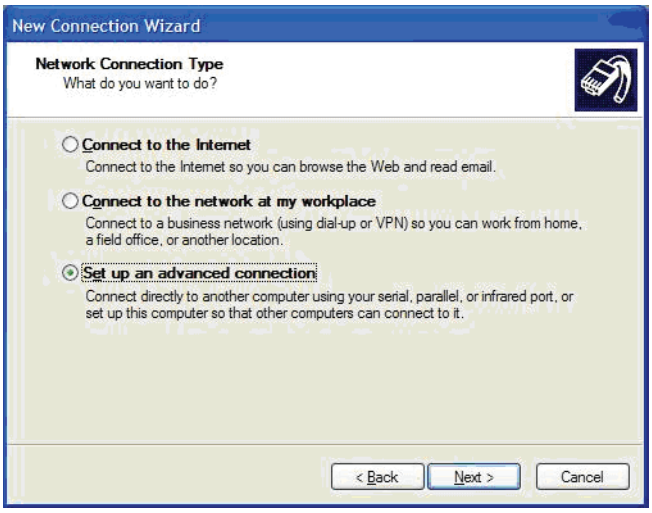
Windows PC をサーバとして適切に設定するためには、すでにモデムがインストール済みである必要があります。モデムの適切なインストール方法の説明は、ユーザー マニュアルのモデムのページを参照してください。それから次の手順に従ってください。PC は着信接続を受け付け、RIP を有効にするように設定しなければなりません。

1. 有効な Windows コンポーネントの 1 つとして RIP リスナーを追加するには、Windows コントロール パネルに移動します。
2. [プログラムの追加と削除] をクリックします。
3. [Windows コンポーネントの追加と削除] をクリックします。
4. [ネットワーク サービス] を反転表示させ、[詳細] をクリックします。
5. RIP リスナーのチェックボックスを確認し、[OK] をクリックします。[次へ] をクリックして終了します。

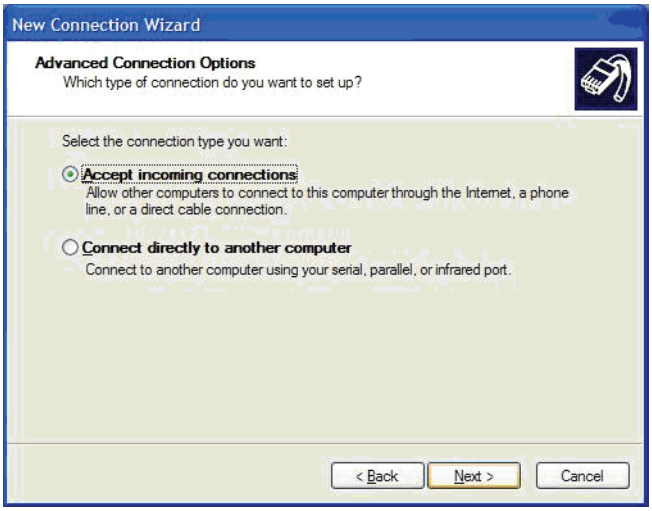


次は、パソコンが PPP 接続へ応答すべき事を知るために、新規着信接続を設定します。着信接続の設定は、次の手順に従ってください。

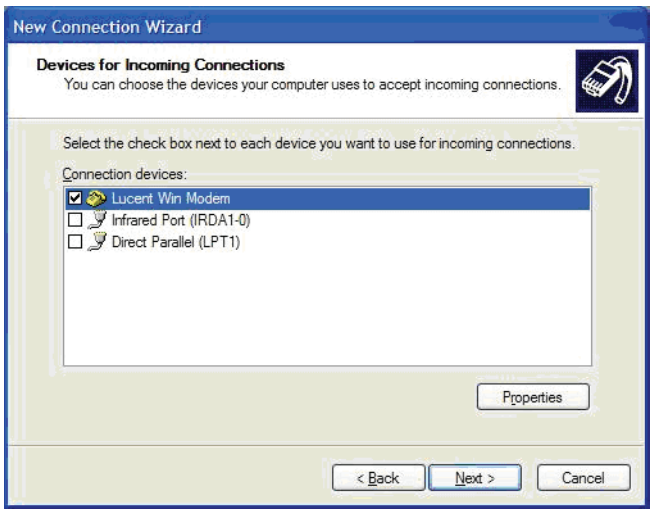
1. Windows の [コントロール パネル] で [ネットワーク接続] をクリックします。
2. [ファイル] メニューから [新規接続] へアクセスし、新規接続を開始します。
3. 新規接続ウィザードが始まったら、[次へ] をクリックします。
4. 詳細接続をセットアップする] を選択します。



5. 次のページで **[着信接続を受け付ける]** を選択します。

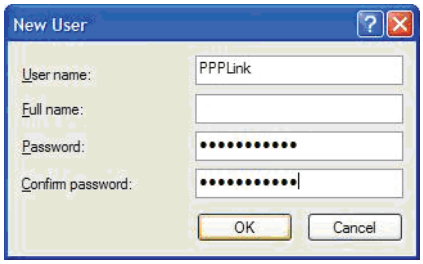


6. コンピューターにインストールしたコールに応答するモデムを選択します。(ここでは、Lucent Win Modem です)

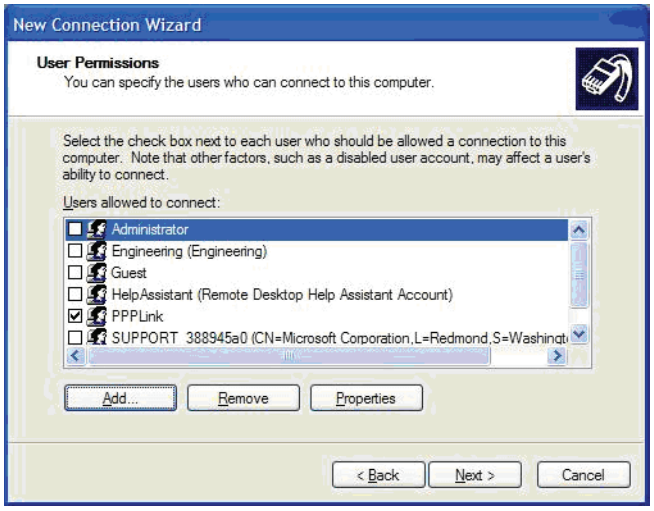


7. 現在のユーザーリストで [追加] をクリックして、新規ユーザーを追加します。

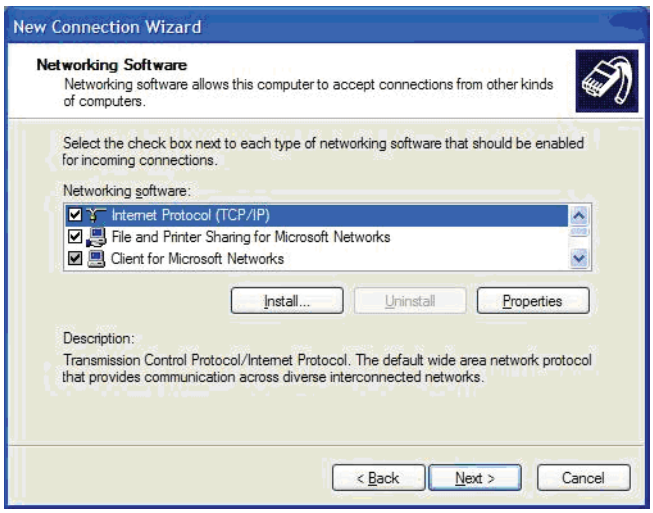
8. 新規ユーザーのユーザー名とパスワードは、ET/SL-5MS-MDM-1 に設定されたユーザー名とパスワードと一致しなければなりません。ここでは、デフォルトの Sixnet ユーザー名「PPPLink」と、パスワード Link2Sixnet」を使用します。



9. 有効な PPP 接続として使用するアクティブなユーザーを選択します。ここでは、新しい PPPLink ユーザーのみが選択されています。

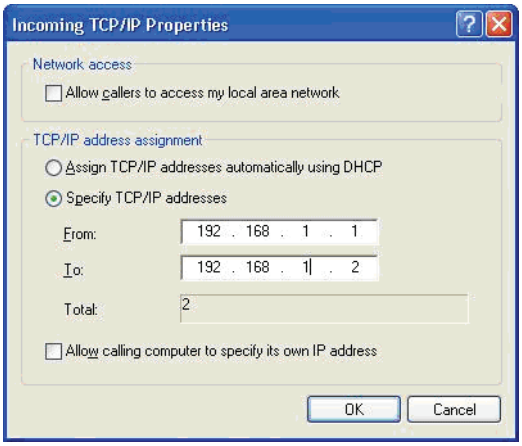


10. [次へ] をクリックします。PPPLink で使用するネットワーク プロトコルを選択します。ここではすべてのプロトコルが選択されていますが、TCP/IP のみ必須です。



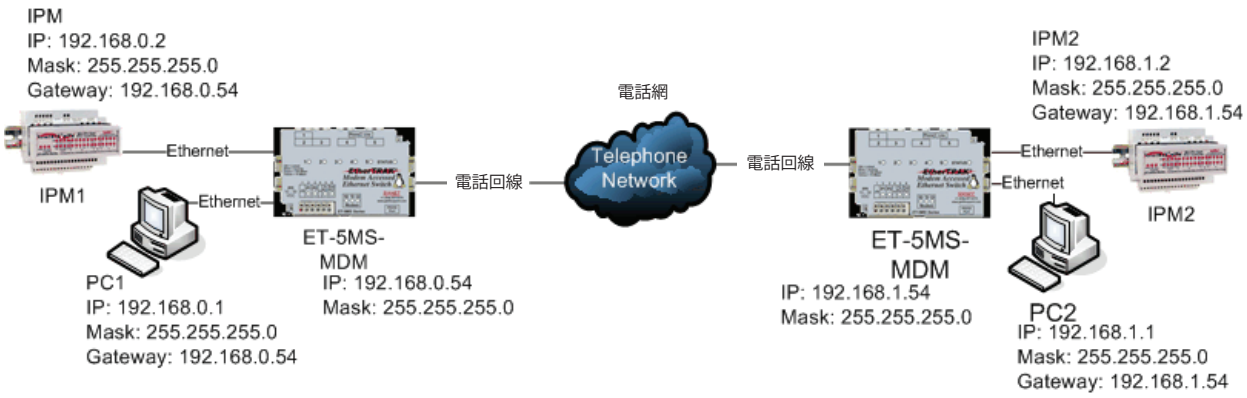
11. TCP/IP を反転表示させ、[プロパティ] をクリックします。

12. お使いのパソコンと ET/SL-5MS-MDM の PPP インターフェイスにアドレスを割り当てるには、[TCP/IP アドレスを指定する] を選択し、[開始アドレス] および [終了アドレス] に、2 つの連続したアドレスを入力します。2 つの連続したアドレスの小さい方がパソコンに割り当てられ、大きい方がイーサネット モデムのモデム ポートに割り当てられます。ここでは、「192.168.1.1」がパソコンに割り当てられ、「192.168.1.2」がイーサネット モデムに割り当てられています。



10.11　サイトツーサイト　シナリオ　コンフィギュレーション

典型的なサイトツーサイト シナリオでは、発呼しているイーサネット モデム (PPP クライアント) と、応答しているイーサネット モデム (PPP サーバ) とは異なるサブネット マスク上になければなりません。接続を試みる前に、すべての装置のすべての IP アドレスが、設定したサブネットに適切なものであることを確認してください。次の例を参照してください。



10.12 ダイヤル アウト メッセージング概論

ダイヤル アウト メッセージングは、PLC または RTU が、10 ～ 30 VDC ディスクリート出力をオンにするだけで、ポケベルまたは SCADA PC にメッセージを送信できることを目的としています。このようにして SCADA PC または技術者に問題が警告され、SL-5MS-MDM にダイヤル イン使用シナリオでコールインし、問題に対処できる様にします。この機能の 2 つの警告方法は、数字とシリアルです。ダイヤル アウト メッセージングがどのように機能するかの基本的な説明を、この概論でおこないます。

- Numeric (数字): SL-5MS-MDM が数字メッセージングに設定されている時に、「From PLC」入力に通電すると、事前に設定した番号がコールされ、小休止後に追加の数字が送信されます。これは手動でポケベルにコールする電話に数字を入力する方法と似ています。数字メッセージが入力できるまで一定の経過時間があります。これにより、接続されている PLC の警報に対処できる現場技術者に警告できます。

- Serial (シリアル): SL-5MS-MDM の「From PLC」入力に通電すると、事前に設定された別のモデムの番号にダイヤルします。モデムツーモデム接続の確立後、SL-5MSMDM は、パソコンが実行中の SCADA ソフトウェアによって受信される様に事前に設定された ASCII メッセージを送信します。オプションで SL-5MS-MDM が確認応答メッセージを探し、確認応答メッセージが見つからない場合はメッセージをリセットします。

10.12.1 ダイヤル アウト メッセージング設定

警報が作動すると数字またはシリアル (ASCII) メッセージを送信するように SL-5MS-MDM を設定します。

- **Digital input action (デジタル入力アクション):** (デフォルト = Disabled (無効)) デジタル入力が通電されたときにとるアクションを指定します。
  - **Disabled** – デジタル入力を無視します。
  - **Enabled (有効)**– ダイヤル アウトしてメッセージを送信します。
- **Primary and Secondary phone number (プライマリおよびセカンダリ電話番号):** (デフォルト = 空白) プライマリおよびセカンダリ電話番号を指定します。値には数字 (0 ～ 9) およびコンマを含むことができます。コンマはダイヤルを遅くします (モデム設定で設定した通り)。たとえば、外部回線につなげるために 9 をダイヤルして、ダイヤル トーンを待たなければならない場合、電話番号は「9,,555-1234」のように設定されます。
- **Number selection (番号選択):** (デフォルト = Alternate(交互)) プライマリおよびセカンダリ電話番号が、ダイヤル アウトにどのように使用されるかを指定します。
  - **Primary** – プライマリ番号のみを使用します。
  - **Alternate** – プライマリとセカンダリ番号を交互に使用します。
  - **Fallback (フォールバック)** – リトライ制限に達するまでプライマリ番号を試みます。制限に達するとセカンダリを試みます。
- **Retry limit (リトライ制限):** (デフォルト = 2) 諦めるまで何回ダイヤルをリトライするかを指定します。0 にセットした場合、モデムは一度ダイヤルをして諦めます。
- **Retry delay (リトライ遅延):** (デフォルト = 2) リダイヤルの試みの間でどれくらい待機するかを指定します。
- **Message type (メッセージ タイプ):** (デフォルト = Numeric(数字)) 接続後、どのようにメッセージを処理するかを指定します。
  - **Serial (シリアル)** – 接続後、モデム経由でメッセージに明記されたテキストを送信します。ユーザーがリモート モデムにダイヤルし、メッセージをタイプする事をシミュレートします。
  - **Numeric** – メッセージの数字をダイヤルし、ダイヤル後に数字事象を送信します。この機能は、ポケベルと携帯電話に数字事象を連絡するためにのみ使用されます。モデムツーモデム接続は確立されません。

注 : プライマリ電話番号だけが数字メッセージに使用されます。

- Message (メッセージ): (デフォルト = 空白) 送信するメッセージ。
- Send message delay (メッセージ送信遅延): (デフォルト = 2) 数字メッセージでは、ダイヤルしてからメッセージ送信までの待機期間を指定します。シリアル メッセージでは、接続してからメッセージの送信までの待機期間を指定します。
- ACK message (ACK メッセージ): (デフォルト = 空白) メッセージ送信後、リモート システムから予想される確認メッセージを指定します。
- Message resend limit (メッセージ再送信制限): (デフォルト = 2) 諦めるまで何回メッセージを送信するかを指定します。0 にセットした場合、モデムは一度メッセージを送信して諦めます。
- Message resend delay (メッセージ再送信遅延): (デフォルト = 2) ACK メッセージを受信しない場合、メッセージを再送信するまでにどれくらい待機するかを指定します。

10.12.2 イーサネット モデムの ASCII メッセージ送信

このセクションでは、イーサネット モデムの「From PLC」入力に通電することにより、どのように ASCII シリアル メッセージがモデムを通じてリモート コンピューターに送信されるかを定義します。このチュートリアルの ASCII メッセージは、ハイパー ターミナル (Windows オペレーティング システムと一緒に配布されるターミナル プログラム) に送信されますが、ASCII メッセージを受け付けるプログラムであればいずれも、イーサネットモデムが送信する警告メッセージ受信に使用することができます。特定のデバイスへのメッセージ送信の詳細は、http://www.redlion.net のテクニカル ノート 648 および 649 に載っています。

すべてのコンフィギュレーションは、[Remote Access Settings](リモート アクセス設定) メニューの [Dial-Out Messaging](ダイヤル アウト メッセージング) コンフィギュレーション ウィンドウでおこなえます。

1. まず、[Dial-input action](ダイヤル入力アクション) を [Enabled](有効) にします。
2. 応答パソコンに取り付けられているモデムの電話番号を、[Primary phone number](プライマリ電話番号) フィールドに入力します。
3. [Message Type](メッセージ タイプ) を [Serial](シリアル) に設定します。
4. 希望するシリアル メッセージを [Message] フィールド入力します。この例では <RemoteLocation> がシステム設定でのスイッチの場所名と一致しているので、接続されたパソコンはどの場所からコールインされているのか決定できます。
5. この例では [Message resend limit] は「2」に設定されています。これは、モデム ツー モデム接続が確立してから、イーサネット モデムがメッセージを送信する回数を示しています。
6. [ACK Message] を「OK」に設定すると、メッセージ送信を止めるようにイーサネットモデムに確認応答メッセージが伝えられます。

10.12.3 ハイパー ターミナル コンフィギュレーション

次の手順に従う前に、お使いのコンピューターにモデムをインストールしておく必要があります。インストールがまだであれば、お使いのパソコン モデムのユーザー マニュアルを参照して、インストールと設定の方法に従ってください。すべてのコンフィギュレーションは、[Remote Access Settings](リモート アクセス設定) メニューの [Dial-Out Messaging](ダイヤル アウト メッセージング) コンフィギュレーション ウィンドウでおこなえます。

1. [コントロール パネル] → [電話とモデム] の順にアクセスし、お使いのモデムを接続するシリアル ポートを決定します。

2. ハイパー ターミナルを開きます。通常は [スタート] → [すべてのプログラム] → [アクセサリ] → [通信] → [ハイパー ターミナル] の順にアクセスしますが、パソコンによっては異なることもあります。接続の名前を入力します。

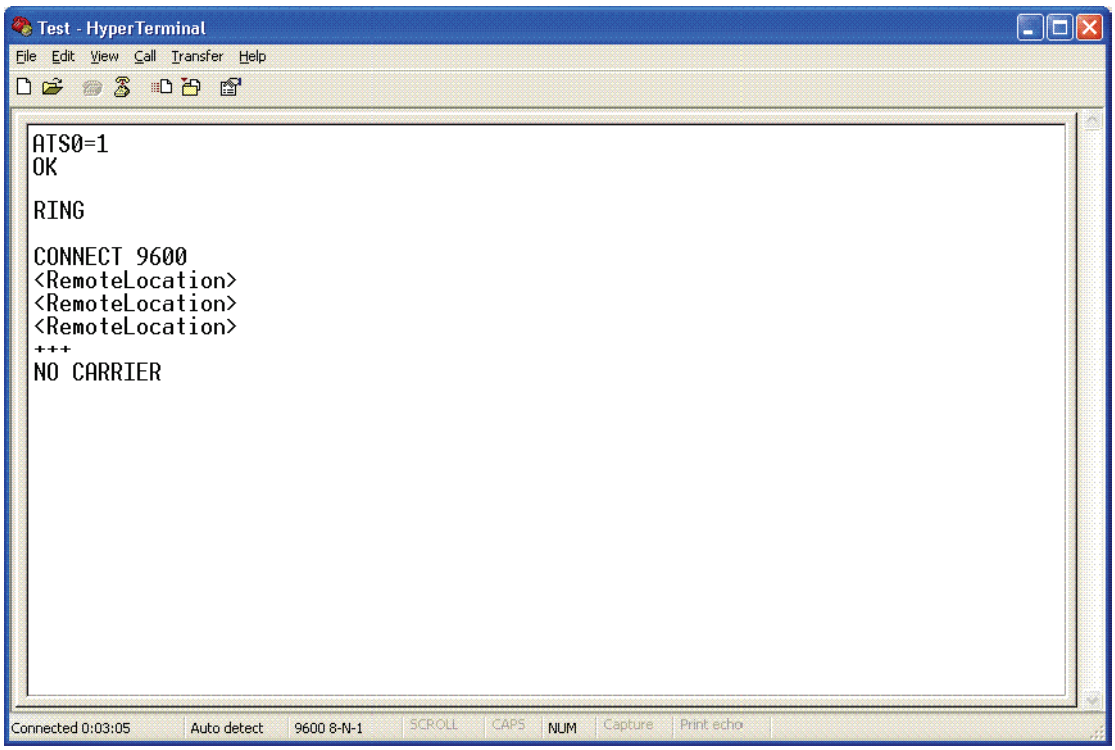
3. [接続方法] で [Direct to Com “X”(Com “X” に直接)] を選択します。“X” はモデムが接続する COM ポート番号です。

4. 希望する [ビット / 秒]、[データ ビット]、[パリティ]、[ストップ ビット]、[フロー制御] を入力します。[OK] をクリックします。

5. 真っ白な画面が表示されます。「ATS0=1<enter>」を入力して、モデムが自動応答にセットされた事を確認します。モデムは「OK」で応答するはずです。(次のスクリーン ショットを参照してください)

10.12.4 イーサネット モデムの発動

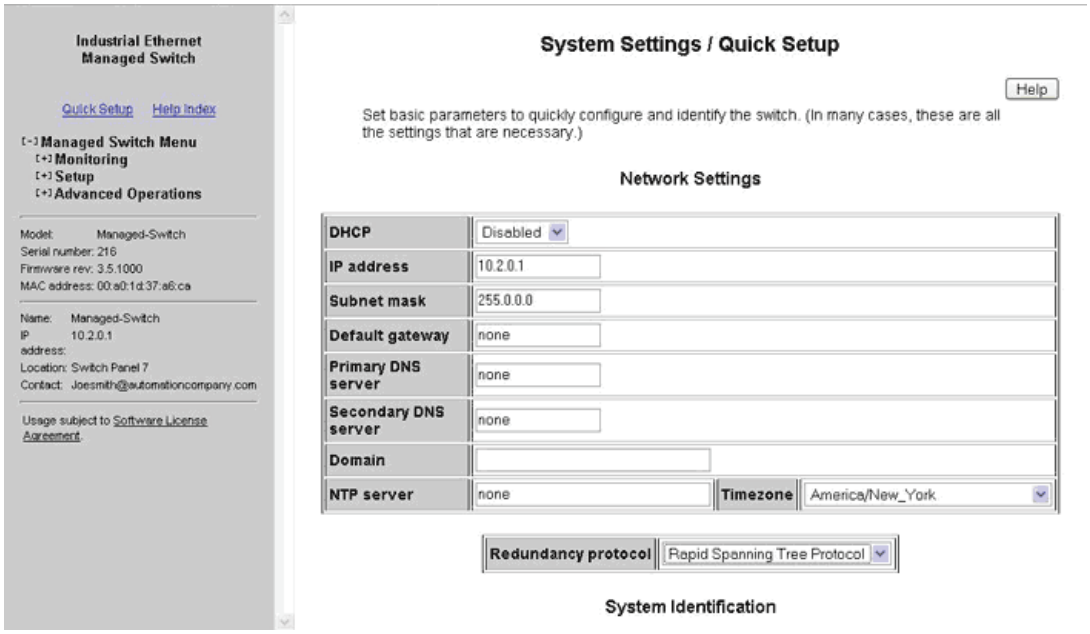
イーサネットモデムを電話回線に接続し、10 ～ 30 VDC を「From PLC」入力に加えてハイパーターミナル スクリーンを見ます。イーサネット モデムからのメッセージが無事にハイパー ターミナルへ送信されると、ウィンドウは次のスクリーン ショットのようになります。


Test - HyperTerminal
File Edit View Call Transfer Help
ATS0=1
OK
RING
CONNECT 9600
<RemoteLocation>
<RemoteLocation>
<RemoteLocation>
+++
NO CARRIER
Connected 0:03:05
Auto detect
9600 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

第 11 章 その他の特別機能

11.1 ネットワーク タイム プロトコル

ネットワークのタイムサーバー用 IP アドレスを設定することができます。起動すると、スイッチは現在時刻を入手するために、ユーザーが指定したサーバーに通信します。そして、タイム スタンプではこの時刻情報を使用します。また、マネージド スイッチが存在するタイム ゾーンも定義が可能です。

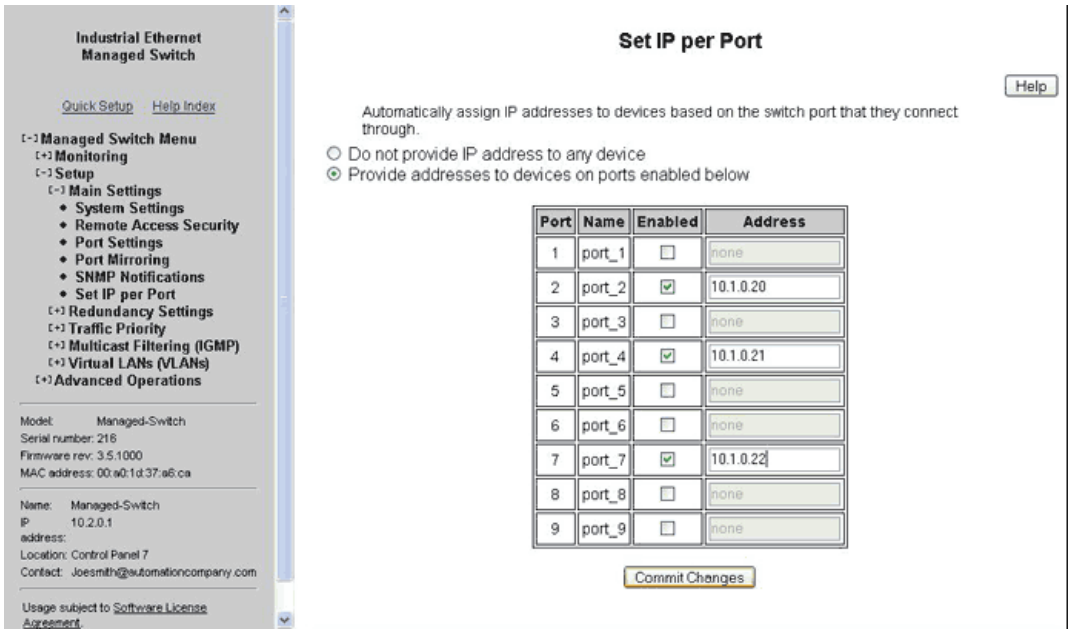


- NTP server (NTP サーバ)(デフォルト = none (なし)): 起動時に、スイッチが現在時刻を手得する NTP サーバの IP アドレス。
- Timezone (タイム ゾーン)(デフォルト = Unset (未設定)): ローカル タイム ゾーン。北アメリカの東海岸時間は「America/New_York」などと表示される。

11.2 ポートごとの IP の設定

スイッチは、各ネットワーク ポートで 1 つのデバイス毎に、IP アドレス 1 つを提供できます。この機能でスイッチ全体をオンオフする事もでき、各ポートを個別に制御することもできます。

スイッチは、統計的に設定された IP アドレスを最初にリクエストした装置に提供することにより、DHCP リクエストに応答します。DHCP のリースに有効期限はありません。

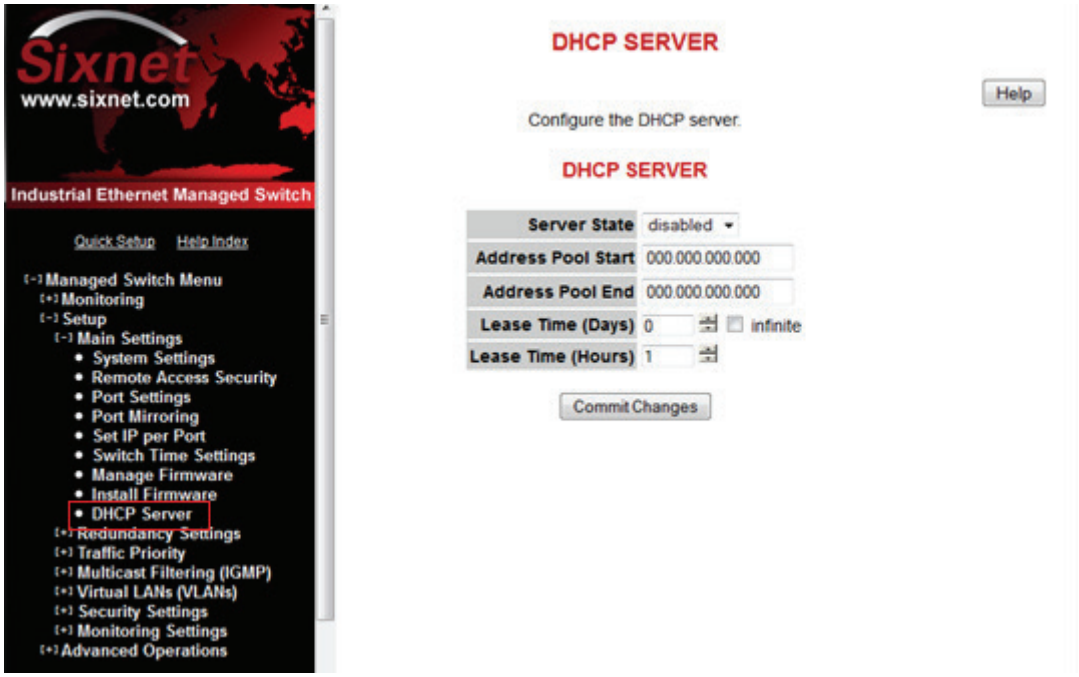


- **Enabled (有効):** このボックスに印が入っているときは、スイッチはポートに来る DHCP リクエストを処理します。
- **Address (アドレス):** このフィールドは、DHCP リクエストに応答するためのアドレスを指定します。

11.3 DHCP サーバ

スイッチは IP アドレスを他の装置に提供することができます。

設定済みプールからランダムに IP アドレスを提供することで、スイッチは DHCP リクエストに応答します。



Server State (サーバ状態)

Disabled (無効) に設定されているときは、DHCP サーバは DHCP リクエストを無視します。Enabled (有効) に設定されているときは、構成済みプールのアドレスでリクエストに応答します。

Address Pool Start (アドレス プール開始)

一番小さい IP アドレスを認定します。

Address Pool End (アドレス プール終了)

一番大きい IP アドレスを認定します。

Lease Time (リース時間)

リース時間は日数または時間で設定できます。リース時間の経過後、装置が新しいアドレスのリクエストをすることが予想されます。Infinite (無限) のチェックボックスに印を入れると、サーバは期限の切れないアドレスをリースします。

第 12 章 セキュリティ設定

12.1 セキュリティ概要

マネージド スイッチには、管理機能への安全なアクセス方法がいくつかあります。以下の方法で、遠隔地から管理（監視および設定）が可能です。

- **Telnet (テルネット)** – これは、ターミナルまたは CLI インターフェイス（コンソール シリアル ポートを通過するのと同じ）にアクセスしますが、イーサネット ネットワーク経由です。このタイプのアクセスは、パスワード保護（認証）のみ提供し、暗号化はしません。

- **SSH** – セキュア シェルは、Telnet のようにイーサネット ネットワーク経由でターミナルまたは CLI インターフェイスにアクセスします。パスワード保護と暗号化の両方を提供します。

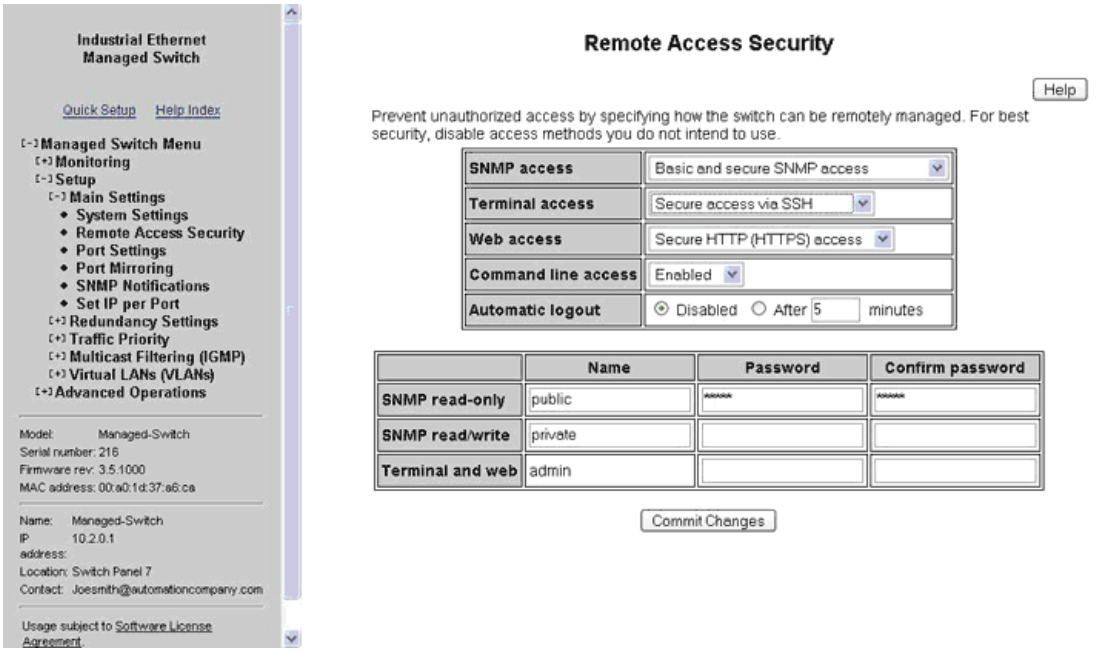
- **SNMP/SNMPv3** – この方法は、SNMP サーバもしくはマスター ユーティリティを使って、管理情報ベース (MIB) にアクセスします。標準 SNMPv1 または SNMPv2 には、パスワード セキュリティがあります。SNMPv3 は暗号化を追加しています。

- **HTTP/HTTPs** – この方法は、ウェブ インターフェイスにアクセスするものです。標準 HTTP には、パスワード セキュリティがあります。さらに安全な HTTPS は、SSL (セキュア ソケット レイヤ) または TLS (トランスポート層セキュリティ) を使った暗号化を追加します。

注 : 最も良いセキュリティの方法は、使用していないアクセス方式をオフにするか、無効にすることです。

12.2 リモート アクセス セキュリティ

この画面では、リモート アクセスのセキュリティ設定ができます。[Remote Access Security](リモート アクセス セキュリティ) にアクセスするには、[Main Menu](メイン メニュー) から [Setup](セット アップ) を選択し、さらに [Main Settings](メイン設定) を選択します。



- SNMP Access (SNMP アクセス): 許可する SNMP アクセスのレベル選択ができます。
  - None (なし) – SNMP アクセスは許可されません。
  - SNMPv2 – コミュニティ ストリングのある SNMPv2 アクセスは、平文を送信し、パスワードは必要ありません。
  - SNMPv3 – 暗号化したパスワードのある SNMPv3 アクセス。
  - Both (両方) – SNMPv2 および v3 アクセスが許可されます。
- Primary and Secondary phone number (プライマリおよびセカンダリ電話番号): (デフォルト = 空白) プライマリおよびセカンダリ電話番号を指定します。値には数字 (0 ～ 9) およびコンマを含むことができます。コンマはダイヤルを遅くします (モデム設定で設定した通り)。たとえば、外部回線につなげるために 9 をダイヤルして、ダイヤル トーンを待たなければならない場合、電話番号は「9,,555-1234」のように設定されます。
- Terminal Access (ターミナル アクセス): ターミナル アクセスのタイプ選択ができます。
  - None – スイッチへのターミナル アクセスは許可されません。
  - Telnet (テルネット) – telnet プロトコル経由のノンセキュア アクセス。このプロトコル経由のリモート アクセスは可能ですが、サーバとクライアント間で交わされるすべての情報は、平文で送信されます。

    安全上の懸念がある場合は、代わりにセキュア シェル プロトコルを使ってください。
  - SSH – 強固な認証ならびに暗号化を採用したセキュアな交信を実装するセキュア シェル プロトコル (SSH) を経由して、セキュアなアクセスが可能です。このプロトコルを使用すると、ログイン情報は決して平文では送信されず、ネットワークからの攻撃の可能性からスイッチは守られます。
  - Both – スイッチにセキュア (SSH)、およびノンセキュア (telnet) ターミナル アクセスを通じてアクセスできます。

スイッチは、これらの SSH 用暗号化アルゴリズムに対応しています。

- 3DES
- Blowfish
- AES
- Arcfour

スイッチの SSH の機能を活用するには、SSH クライアント プログラムを使う必要があります。ホスト (スイッチ) にログオンするために利用可能な SSH クライアント プログラムが複数あります。

以下の 2 つのオープンソース SSH クライアント プログラムは、インターネットで利用可能です。

- プログラム名 : OpenSSH for Windows
  http://sshwindows.sourceforge.net/
- プログラム名 : PuTTY
  http://www.chiark.greenend.org.uk/~sgtatham/putty/

SSH プロトコルは、目的のホストと交信していることをクライアントが確かめるために、何らかの要求をします。ホストは鍵に基づいて「ホスト鍵指紋」を計算し、それを認証のためにクライアントに提供します。最初にクライアントがホスト鍵指紋を見るとき、たいていこのように表示され、質問されます。「The host is offering me these credentials, should I trust it? (ホストが証明書を提供していますが、信用しますか ?)」

同意すると、ホスト鍵指紋は後で再利用するために保管されます。

システムの安全のため、比較に使われるホスト鍵指紋は「帯域外」で送信されなければなりません (ホスト鍵指紋によって安全が確保されるチャンネル以外の方法による)。この例では、ドキュメント経由です。マネージド スイッチの暗号化鍵用 RSA 指紋は、次の通りです

1e:0f:31:39:26:3f:23:8c:ba:7e:e9:d1:56:ff:98:f6

- **Web Access (ウェブ アクセス)**: 許可するウェブ アクセスのレベルを選択します。
  - **None（なし）** – ウェブ アクセスは許可されません。
  - **HTTP** – ベーシック HTTP アクセスが許可されます。
  - **HTTPS** – セキュア HTTP (HTTPS) が必要です。http 経由でスイッチにアクセスを試みると、セキュア プロトコルにリダイレクトされます。
  - **Both (両方)** – ベーシックおよびセキュア HTTP アクセスが許可されます。
- **CLI Access (CLI アクセス)**: 許可するウェブ アクセスのレベル選択をします。
  - **Enabled (有効)** – CLI アクセスが有効
  - **Disabled (無効)** – CLI アクセスが無効
- **Automatic Logout (自動ログアウト)**: 不正アクセスを防ぐため、ターミナル セッションが自動的にログアウトする前の不活発な状態を分数で指定します。デフォルトは 5 分です。
- **SNMP Read-Only Name (SNMP 読み出し専用名)**: このパラメータは、設定の読み出し専用アクセスで SNMP クライアントが使用する SNMPv2 コミュニティ ストリング、および SNMPv3 ユーザー名を設定します。読み出し専用アクセスをセキュアにしたい場合は、自分で選んだ値を入力してください。(デフォルトは「public」)

- **SNMP Read-Only Password (SNMP 読み出し専用パスワード):** このパラメータは、読み出し専用ユーザーによる、セキュア SNMPv3 アクセス用パスワードを設定します。SNMP パスワードは、最低 8 文字の長さでなければなりません。デフォルトの読み出し専用パスワードは、「publicpwd」です。(かっこは含まない)

- **SNMP Read/Write Name (SNMP 読み書き名):** このパラメータは読み書きアクセスで SNMP クライアントが使用する SNMPv2 コミュニティ ストリング、および SNMPv3 ユーザー名を設定します。読み書きアクセスをセキュアにしたい場合は、任意の値を入力してください。(デフォルトは「private」)

- **SNMP Read/Write Password (SNMP　読み書きパスワード):** このパラメータは、読み書きユーザーによる、セキュア SNMPv3 アクセス用パスワードを設定します。SNMP パスワードは、最低 8 文字の長さでなければなりません。デフォルトの読み書きパスワードは、「privatepwd」です。(かっこは含まない)

- **New Admin Password (新規管理者パスワード):** ここで設定されたパスワードは、Telnet およびウェブ アクセスに使用されます。管理者パスワードの変更は、このオプションを選択してください。(デフォルト パスワードは「admin」)

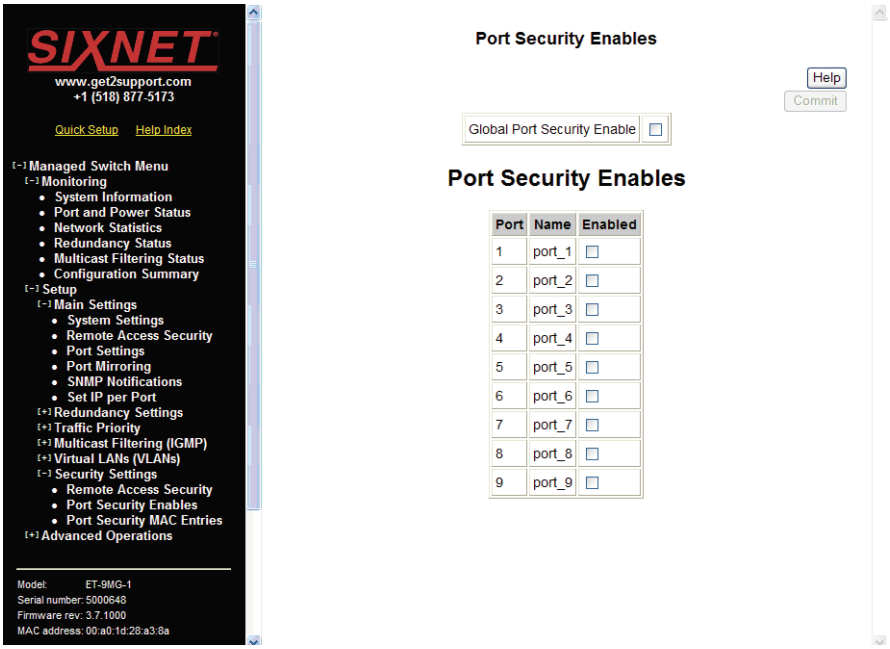
12.3　ポート セキュリティ

追加のセキュリティとして、MAC アドレス レベルで、ポート セキュリティを有効にできます。
この機能は、5MS モデルでは利用できません。

ポート セキュリティを有効にするには、[Global Port Security Enable](グローバル ポート セキュリティ イネーブル) に印を入れます。それから、どの個別ポートが MAC アドレス セキュリティを持つべきか選択します。

目的のポートが有効のときは、[Commit](コミット) ボタンをクリックして変更します。

注 : ポートのポート セキュリティが有効なのに、MAC エントリー テーブルに MAC アドレスがない場合は、そのポートに接続している装置はスイッチと通信できません。すべてのポートのセキュリティを有効にする前に、最低 1 つの MAC アドレスがテーブルに存在するようにしてください。



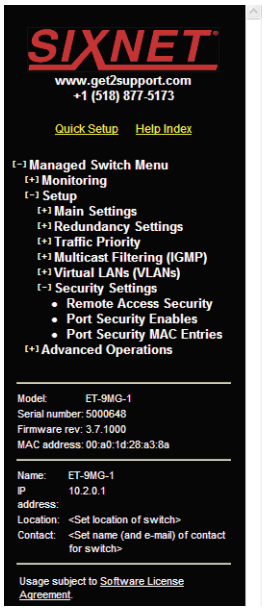
12.4　ポート セキュリティ MAC エントリ

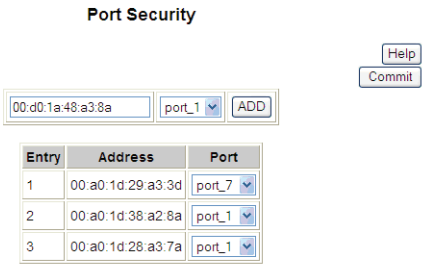
新規の MAC アドレスをポートに追加するには、まずアドレスを入力します。アドレスは、「00:11:22:33:44:55」のフォーマットでなければなりません。次に、アドレスが割り当てられるポートを選択します。そして、[ADD](追加) をクリックします。すると、アドレスとポートの割り当てが表の中に表示されます。しかし、[commit](コミット) ボタンを押すまで、スイッチに適用されません。

既存の MAC アドレスのポート割り当てを変更したり、MAC アドレスを削除したりするには、MAC アドレスの隣にあるポート選択ドロップダウン メニューを使います。これでポートを変更したり、[delete](削除) を選んだりすることができます。[commit] ボタンが押されるまで、変更はスイッチに適用されません。

注 : MAC アドレスがポートに追加されると、その MAC アドレスは割り当てられたポート経由でのみスイッチと通信が可能です。

たとえば MAC 00:a0:1d:38:a2:8a がポート 1 に追加されているが、ポート 2 と接続する場合は、スイッチと通信できません。





12.5　IPSEC 設定

IPsec は、スイッチへ、またはスイッチからの IPv6 トラフィックの認証、暗号化、または圧縮が可能です。このスイッチの IPsec ソフトウェアは、スイッチへ、またはスイッチからの管理トラフィックに影響するのみで、スイッチが IPv6 アドレスで設定されているときにのみ使用できます。

警告 : この画面での不適切な設定は、スイッチのコンフィギュレーション インターフェイスへのネットワーク アクセスをブロックすることがあります。

コンフィギュレーションは 2 つのデータ ベース経由で行われます。SPD は、構成したホストまたはネットワークへの、またはそれらからのトラフィックのために必要な IPsec プロトコルを設定します。SAD は特定のホスト間のトラフィックに SPD によって必要とされるポリシーの実装に必要な、暗号化、圧縮、およびハッシュのためのパラメータを保持してます。

AH IPsec プロトコルは認証に使用されます。暗号文を使用して、受信者と同じハッシュ キーを持つ送信者を検出します。通信には秘匿機能を提供しません。

ESP プロトコルは暗号化に使用されます。暗号化に使用された秘密鍵を持たない者から、通信時のトラフィックの内容を隠すために暗号文を使用します。

IPComp はトラフィックを圧縮するために使用されます。秘匿機能や認証性の保証は提供しません。

12.5.1 セキュリティ ポリシー データベース

このセクションでは、SPD エントリの作成、削除および修正を扱います。

警告 : SPD エントリの設定の際は注意してください。SPD 設定に適切な SAD エントリを設定しない場合は、SPD エントリはスイッチの設定に使っているるホストに影響を及ぼし、スイッチとの通信が不可能になることがあります。

SPD エントリを作成するには、[Add SPD Rule](SPD ルールを追加) をクリックして適切なソース、宛先、方向、およびプロトコル要件を設定します。変更を保存するには、[Commit Changes](変更を適用) をクリックします。

SPD エントリを削除するには、行の最後の [X] をクリックしてから [Commit Changes] をクリックします。

SPD エントリを修正するには、希望通りにパラメータを変更してから [Commit Changes](変更を適用) をクリックします。

注 : SPD エントリは ICMPv6 近隣者発見トラフィックに適用されません。これにより、近隣者発見は IKE と同時に機能し合うようになります。(内部では、近隣通知パケットと近隣要請パケットが IPsec を回避するための高優先度ルールをシステムは追加します)

- **Source (ソース)** – フォームアドレス、address/prefixlen、address/prefixlen [port]、および address [port] 型式のアドレス。ソースホスト、またはこのポリシーが影響を与えるホストを指定します。
- **Destination (宛先)** – ソース フィールドに受け入れられるアドレスで同形式の内の 1 つの形を取る。宛先ホスト、またはこのポリシーが影響を与えるホストを指定します。
- **Direction (方向)** – 方向トラフィックはスイッチを経由で伝わります。スイッチのアドレスがソース フィールドに指定されている場合、方向は [Out] でなければなりません。スイッチのアドレスが宛先フィールドに指定されている場合、方向は [In] でなければなりません。
- **ESP** – 指定したホスト間の通信の暗号化が必要かどうか
- **AH** – 指定したホスト間の通信の認証が必要かどうか
- **IPComp** – 指定したホスト間の通信の圧縮が必要かどうか
- **Delete (削除)** – ボタンをクリックすると、変更が適用されるときに SPD エントリが削除されます。

12.5.2 セキュリティ アソシエーション データベース

このセクションでは、SAD エントリの作成、削除および修正を扱います。

警告 : SAD エントリの設定の際は注意してください。通信している 2 つのホスト間で鍵と SPI 値が同じでなく、セキュリティ ポリシーが暗号化や認証を指定していると、適切な通信ができません。スイッチとの通信が不可能になることがあります。

SAD エントリを作成するには、[Add Security Association](セキュリティ アソシエーションを追加) をクリックして必要に応じたソース、宛先、SPI、モード、暗号、ハッシュ アルゴリズム、および鍵を設定します。変更を保存するには、[Commit Changes](変更を適用) をクリックします。

SAD エントリを削除するには、行の最後の [X] をクリックしてから [Commit Changes] をクリックします。

SAD エントリを修正するには、希望通りにパラメータを変更してから [Commit Changes] をクリックします。

- **Source (ソース)** – フォーム アドレスまたは address [port] のアドレス。セキュリティ アソシエーションのためのソース ホスト (およびオプションのポート) を指定します。

- **Destination (宛先)** – フォーム アドレスまたは address [port] のアドレス。セキュリティ アソシエーションのための宛先ホスト (およびオプションのポート) を指定します。

- **SPI** – このセキュリティ アソシエーションを認識するローカルな固有値。これはローカルに割り当てられ、16 進法または 10 進数形式で指定されます。これは最小 0x100 (10 進数で 256) で、アソシエーションの両端で同じでなければなりません。

- **Mode (モード)** – 使用する IPsec モード。 ESP、AH、ESP と AH、または IPComp。

- **Cipher (暗号)** – ESP モードを選択するときに使用する暗号。

- **Encryption key (暗号鍵)** – ESP が有効のときに使用する鍵。16 進数 (0x で始まる) で指定され、3DES では長さ 24 バイト (48 桁)、または AES では長さ 16、24、または 32 バイト (32、48、または 64 桁) です。

- **Hash (ハッシュ)** – ハッシュ アルゴリズムは、AH モードが選択されるときに使用します。MD5 は推奨しません。

- **Hash key (ハッシュ キー)** – ハッシュ キーは AH が有効のときに使用します。16 進数 (0x で始まる) で指定され、SHA1 では長さ 20 バイト (40 桁)、または SHA256 では長さ 32 バイト (64 桁) です。

- **Delete (削除)** – 削除ボタンをクリックすると、変更が適用されるときにこの SAD エントリは削除されます。

12.6 IKE ポリシー設定

この画面では、IPv6 を通じて IPsec セキュリティ アソシエーションを自動ネゴシエーションするための IKE ポリシーの設定が可能です。

警告 : この画面での不適切な設定は、スイッチのコンフィギュレーション インターフェイスへのネットワーク アクセスをブロックすることがあります。

12.6.1 IKE フェーズ 1 ポリシー

このセクションでは、ISAKMP (IKE フェーズ 1) ポリシーの作成、削除および修正を扱います。フェーズ 1 は相手を安全に認証します。

- **Address (アドレス)** – ポリシーを適用する相手のアドレス。「匿名」のポリシーは、追加のポリシーなしですべての相手に適用します。

- **Exchange Mode (交換モード)** – 好ましい交換モードで、どの提案でも相手に送られます。他の交換モードが指定された場合、受けた提案を受け入れます。アグレッシブ モードでは、送った提案の DH グループは、相手のコンフィギュレーションと完全に一致しなければなりません。

- **Cipher (暗号)** – 暗号は提案の交換を暗号化するときに使用されます。「Cipher」を選択してください。

- **Hash (ハッシュ)** – ハッシュは、提案の交換を認証するときに使用されます。「hash algorithm」を選択してください。

- **DH Group (グループ)** – ディフィー・ヘルマン グループは、べき算に使用されます。より大きなグループはより安全ですが、計算に時間がかかる可能性があるため、タイムアウトのためにネゴシエーションを終了するのが不可能になり、スイッチの管理インターフェイスへの接続が妨げられます。これは、通常接続の双方で同じ値に設定されます。

12.6.2 IKE フェーズ 2 ポリシー

このセクションでは、IKE フェーズ 2 アルゴリズムと共に、フェーズ 1 で認証された相手同士でセキュリティ アソシエーションを確立するために使用されるパラメータの設定を扱います。

使用するポリシーは、ソースまたは宛先セレクタを使用して、セキュリティ ポリシー データベース エントリまたはネゴシエーション発端となった受信 IKE パケットの ID ペイロードから選択します。「匿名」以外の値は正確に一致しなければなりません。

- **Source (ソース)** – 照合するためのソース アドレス。指定したアドレスは、どちらかの値が「匿名」でない限り、相手のフェーズ 2 ポリシーの宛先アドレス フィールドと完全に一致する必要があります。「匿名」値は、他のルールによっては処理されないソースと一致します。

- **Destination (宛先)** – 照合するための宛先アドレス。指定したアドレスは、どちらかの値が「匿名」でない限り、相手のフェーズ 2 ポリシーのソース アドレス フィールドと完全に一致する必要があります。「匿名」値は、他のルールによっては処理されない宛先と一致します。

- **PFS Group (グループ)** – ディフィー・ヘルマンべき算グループは、完全なる前方秘匿性に使用されます。必要でない場合は無効にしますが、それを提示する提案は受け入れます。より大きなグループはネゴシエーションの最中に過剰な処理時間を要することがあり、タイムアウトを引き起こします。

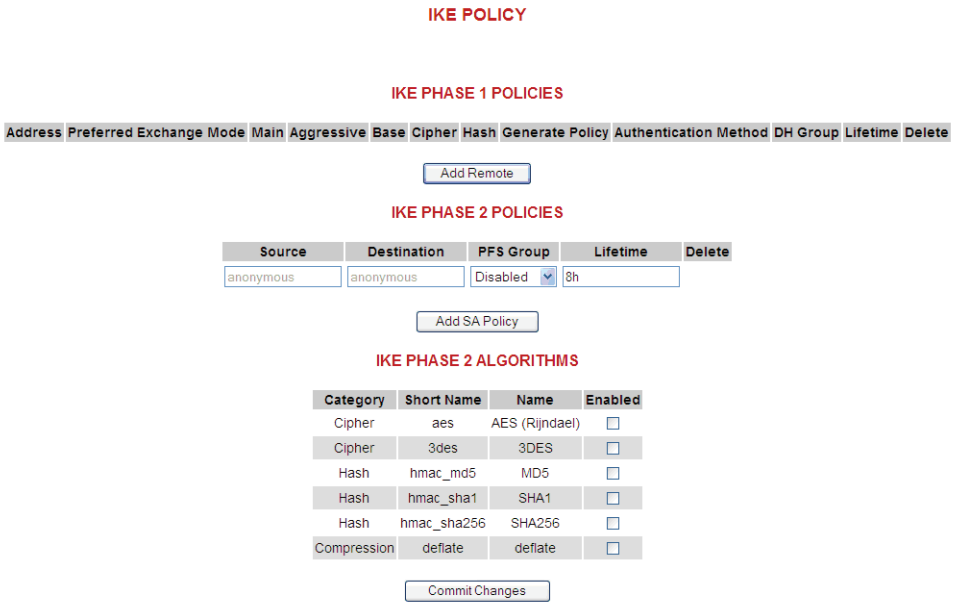
12.6.3 IKE フェーズ 2 アルゴリズム

このセクションでは、フェーズ 2 で使用されるアルゴリズムの設定を扱います。選ばれた正確なアルゴリズムは、ここで指定されたセットと相手のセットの共通部分になります。

各カテゴリー (cipher (暗号)、hash (ハッシュ) および compression(圧縮)) から最低 1 つのアルゴリズムを有効にしなければなりません。スイッチの IPsec ポリシーが必要でなくても、与えられたプロトコルの 1 つが使用されます。

デフォルト値は、ほとんどの実装と互換性があるはずです。

AES (デフォルト = Enabled (有効))	暗号	
3DES (デフォルト = Enabled (有効))	暗号	
SHA1 (デフォルト = Enabled (有効))	ハッシュ	
SHA256 (デフォルト = Enabled (有効))	ハッシュ	
MD5 (デフォルト = Disabled (無効))	ハッシュ	MD5 は安全でないことが知られており、古い実装との互換性のためだけに含めています。
deflate (デフォルト = Enabled (有効))	圧縮	



12.7 IKE 事前共有鍵および証明書

12.7.1 IKE 事前共有鍵

この画面では、IPv6 を通じてスイッチが通信する相手とのネゴシエートに使用する IKE PSKs (事前共有鍵) の設定ができます。

警告 : この画面での不適切な設定は、スイッチのコンフィギュレーション インターフェイスへのネットワーク アクセスをブロックすることがあります。

同じ事前共有鍵を両方のピアに設定しなければなりません。たとえば、事前共有鍵「secret」を持つ fe80::1 と fe80::2 の 2 つのホスト間が通信する場合、fe80::1 は相手 fe80::2 の事前共有鍵として「secret」が設定され、fe80::2 は相手 fe80::1 の事前共有鍵として「secret」が設定されていなければいけません。

- **Peer Identifier (相手識別子)** – この事前共有鍵を使用する相手の識別子。通常、これは相手のアドレスです。
- **Set Key (設定鍵)** – 事前共有鍵に設定する値。空白にすると、現在値が保持されます。
- **Delete (削除)** – これに印を入れて変更が適用されると事前共有鍵が削除されます。

12.7.2 IKE 証明書

この画面では、IPv6 を通じてスイッチが通信するスイッチと IKE 相手の識別に使用するための IKE 証明書の設定ができます。

警告 : この画面での不適切な設定は、スイッチのコンフィギュレーション インターフェイスへのネットワーク アクセスをブロックすることがあります。

NTP などの信頼できるタイム ソースを提供する事を強く推奨します。 IKE はシステム タイムを参照して「not valid before」時間の前や、期限切れの後の有効でない証明書を拒否します。

NTP が使用される場合は、事前共有鍵またはハード ワイヤードのセキュリティ アソシエーションが NTP サーバを伴った IPsec 通信に使用される必要があります。そうしないと、時間の更新に失敗します。

HTTPS 証明書はスイッチのウェブ インターフェイスに使用され、この画面では変更ができません。

12.7.2.1 スイッチ証明書

このセクションでは、スイッチが IKE 経由で自分自身の識別に使用する X.509 証明書の詳細の生成または表示を扱います。

第三者の CA に提供される証明書リクエストも生成されます。CA 署名済み証明書は、ページ下部のフォームを使用してアップロードが可能で、IKE のためにスイッチが使用していた自署証明書を書き替えます。提供された証明書は、スイッチが生成した証明書リクエストから生成されなければなりません。

- **Subject (サブジェクト)** – 証明書の所有者を識別する DN (識別名)
- **Issuer (発行者)** – 証明書の発行者を識別する DN (識別名)
- **Serial (シリアル)** – 証明書のシリアル ナンバー
- **Certificate (証明書)** – 検証のために証明書をダウンロードするためのリンク
- **Request (リクエスト)** – CA によって署名される証明書リクエストをダウンロードするためのリンク
- **Not valid before (以前は無効)** – 証明書が有効であるもっとも早い時間
- **Not valid after (以降は無効)** – 証明書が有効であるもっとも遅い時間
- **Delete (削除)** – 削除をクリックすると証明書と秘密鍵が削除され、新しいものが生成されます。

  この操作は元に戻すことができません。

スイッチに IKE 証明書がないときは、証明書と鍵が生成されます。次のオプションが設定できます。

- **Common Name (コモン ネーム)** – 新しい証明書のサブジェクトとして使用する CN。これによりスイッチを識別します。通常はホスト名または IP アドレスです。スイッチのホスト名がデュフォルト値として設定されます。
- **Bits (ビット)** – 作成する秘密鍵のサイズ。ビット数
- **Expires (有効期限)** – 証明書の有効日数。スイッチの時計に従い、現在の日から開始します。この設定は自署証明書にのみ使用されます。CA には独自の証明書有効期限があります。

12.7.2.2 IKE 証明書

このセクションでは、IKE ネゴシエーションの最中にスイッチによって信頼される証明書の追加、削除、表示を扱います。

- **Subject (サブジェクト)** – 証明書の所有者を識別する DN (識別名)
- **Issuer (発行者)** – 証明書の発行者を識別する DN (識別名)
- **Serial (シリアル)** – 証明書のシリアル ナンバー
- **Not valid before (以前は無効)** – 証明書が有効であるもっとも早い時間

- **Not valid after (以降は無効)** – 証明書が有効であるもっとも遅い時間
- **Delete (削除)** – ボタンをクリックすると、証明書が削除されます。

アップロード フォームを使って証明書をスイッチに追加できます。

- **Certificate Type (証明書タイプ)** – アップロードした証明書をスイッチのアイデンティティとして使用するか (スイッチ証明書)、または IKE 相手とネゴシエートするとき、スイッチが信頼する証明書を追加するか (CA 証明書) です。CA 証明書オプションは、相手からの自署証明書を信頼することに使用されることがあります。

- **Upload (アップロード)** – アップロードする証明書。

12.8 IPSEC のための CLI コマンド

12.8.1 SPD/SAD コマンド

SPD はセキュリティ ポリシー データベースで、さまざまなホストや一連のホストへのトラフィック、それらからのトラフィックで暗号化、認証、またはカプセル化が必要かどうかの設定に使用されます。

SAD はセキュリティ アソシエーション データベースで、特定のホスト間の認証や暗号化に使用される鍵を保持しています。

一般的に、SPD のポリシーはその固有 (ソース、宛先、方向) データベースエントリーによって参照されます。SAD のポリシーは、ローカルホスト上で固有な必要があるインデックスとしての SPI によって参照されます。

1. **ipsec help** 利用可能な他のコマンドを説明します。
2. **ipsec spd list** すべてのセキュリティ ポリシーを表示します。
3. **ipsec spd add <src> <dst> <direction> [esp] [ah] [ipcomp]** 与えられた方向 (インまたはアウト) が、指定のカプセル化使用 (esp、ah または ipcomp) を要求している状況下で、2 つのホストや一連のホスト間にポリシーを追加します。これら 2 つの間にポリシーがすでに存在する場合は、指定のカプセル化は既存ポリシーに追加されます。

4. **ipsec spd remove <src> <dst> <direction>** セキュリティ ポリシーが定められたホスト間に存在する場合は、それを削除します。

5. **ipsec spd remove all** すべてのセキュリティ ポリシーを削除します。

6. **ipsec sad list** 設定されたセキュリティ アソシエーションをリストアップします。(IKE によって動的に追加されたアソシエーションは含みません。)

7. **ipsec sad add <spi> <src> <dst> [<cipher>/<key>] [<hash>/<key>][<compression>]** セキュリティ アソシエーションを与えられたパラメータに追加します。暗号文またはハッシュ アルゴリズムは単独または一緒に指定することができますが、圧縮は単独に指定しなければなりません。

8. **ipsec sad spi <old-spi> <new-spi>** 与えられたポリシーの SPI を変更します。

9. **ipsec sad src <spi> <src>** 新しいソース ホストを指定します。

10. **ipsec sad dst <spi> <dst>** 新しい宛先ホストを指定します。

11. **ipsec sad cipher <spi> <cipher> [<key>]** このアソシエーションで使用される ESP 暗号文と鍵を更新します。(暗号が disabled (無効) にされた場合は、ESP はこのアソシエーションから削除されます。)

12. **ipsec sad hash <spi> <hash> <key>** このアソシエーションで使用される AH ハッシュと鍵を更新します。(disabled (無効) にされた場合は、AH はこのアソシエーションから削除されます。)

13. **ipsec sad ipcomp <spi> <algo>** このアソシエーションで使用された IPComp? アルゴリズムを更新します。現在は、disabled (無効) および deflate (デフレート) のみが選択できます。

14. **ipsec sad remove <spi>** 与えられた SA を削除します。

15. **ipsec sad remove all** すべての設定済みセキュリティ アソシエーションを削除します。

16. **ipsec sad algos** カプセル化と共に (ESP、AH または IPComp?) に適用される利用可能なすべてのアルゴリズム、および許容される鍵の長さをリストアップします。

12.8.2 IKE コマンド

IKE (インターネット鍵交換) は、証明書や事前共有鍵を使って、自動的にセキュリティ アソシエーションをネゴシエートする方法をホストに提供します。2 つのフェーズがあります。各フェーズには、指定のソースおよび宛先ホストに適用できる様々なオプションがあります。または特定のフェーズではデフォルトとしてふるまいます。

フェーズ 1 ポリシーは、リモート 相手識別子によって識別されます。そのように処理されない場合、Racoon (ラクーン) が「匿名」ポリシーに後退します。

フェーズ 2 ポリシーは、ソースおよび宛先相手識別子によって識別されます。ソースまたは宛先が処理されない場合、Racoon がソースまたは宛先が「匿名」に設定されたポリシーの検索をし、最終的には両方とも匿名の場所を検索します。

すべてのフェーズ 2 ポリシーで使用される暗号文とハッシュ アルゴリズムは、全体的に設定使用されます。Racoon がそれらを個別に指定することができるとしても、双方が自動的に対応するアルゴリズムの共通部分を見つけるので、あまり意味はありません。

12.8.2.1 フェーズ 1 コマンド

1. **ike phase1 list** リモート相手のためのすべてのフェーズ 1 のコンフィギュレーションをリストアップします。

2. **ike phase1 add <address|anonymous>** リモート セクションのためのエントリを追加します。

3. ike phase1 preferred_mode <address|anonymous> [<main|aggressive|base>]

4. ike phase1 mode_main <address|anonymous> [<enabled|disabled>]

5. ike phase1 mode_base <address|anonymous> [<enabled|disabled>]

6. ike phase1 mode_aggressive <address|anonymous> [<enabled|disabled>]

7. ike phase1 address <address|anonymous> [<new address|anonymous>] アドレスは固有のものでなければなりません。

8. ike phase1 cipher <address|anonymous> [cipher] 暗号文はフェーズ 1 で Racoon によってサポートされている暗号のいずれも可能です。

9. ike phase1 hash <address|anonymous> [hash] ハッシュはフェーズ 1 で Racoon によってサポートされているハッシュのいずれも可能です。

10. ike phase1 auth_method <address|anonymous> [<pre_shared_key|rsasig>]

11. ike phase1 gen_policy <address|anonymous> [<enabled|disabled>] 既存のポリシーがない場合、Racoon が自動的にリモート用の SPD ポリシーを生成するかを制御します。これは、ローカルでは必要でないが、それを必要とする相手との IKE ネゴシエーションをサポートする場合に使用されます。

12. ike phase1 lifetime <address|anonymous> [new lifetime] ライフタイムは、後に「s」(秒)、「m」(分) または「h」(時間) のオプション単位が付いた番号です。指定しない場合は、ユニットは秒をデフォルト値に設定します。

13. ike phase1 dh_group <address|anonymous> [new DH group] フェーズ 1 のネゴシエーションに使用されるディフィー・ヘルマン グループを制御します。より大きなグループはより安全ですが、膨大な計算負荷が双方にかかります。

12.8.2.2 フェーズ 2 コマンド

1. ike phase2 add <address|anonymous> <address|anonymous> フェーズ 2 ポリシーを追加します。

2. ike phase2 remove <address|anonymous> <address|anonymous> フェーズ 2 ポリシーを削除します。

3. ike phase2 remove all すべてのフェーズ 2 ポリシーを削除します。

4. ike phase2 list すべてのフェーズ 2 ポリシーをリストアップします。

5. ike phase2 src <address|anonymous> <address|anonymous> [new source address] 既存ポリシーのソースアドレスを表示したりまたは新しいソースアドレスを設定します。

6. ike phase2 dest <address|anonymous> <address|anonymous> [new destination address] 宛先アドレスを表示したりまたは新しい宛先アドレス設定します。

7. ike phase2 pfs_group <address|anonymous> <address|anonymous> [new PFS group|disabled] PFS グループを表示または新しい PFS グループを設定するか、PFS の使用を無効にします。このオプションは、ike フェーズ 1 dh_ グループのものと同じで、同じ警告が適用されます。

8. ike phase2 lifetime <address|anonymous> <address|anonymous> [new lifetime] フェーズ 2 でネゴシエートされたセキュリティ アソシエーションのためのライフタイムを設定します。ike フェーズ 1 ライフタイムと同じフォーマットを使用します。

12.8.2.3 アルゴリズム コマンド

1. ike algo list フェーズ 2 アルゴリズムのリストを表示します。
2. ike algo use <algorithm> [enabled|disabled] フェーズ 2 アルゴリズムの使用を有効か無効にします。最低でも暗号文、ハッシュ アルゴリズム、および圧縮アルゴリズムは常に有効でなければなりません。

12.8.2.4 事前共有鍵コマンド

事前共有鍵コマンド

CLI は、ユーザーが設定するまでどんな鍵値なのかわかりません。しかし、既存値は保存時に維持されます。

1. ike psk list 事前共有鍵のリストを表示します。
2. ike psk add <peer> [<key>] 新しい鍵を、可能であれば新しい値と共に追加します。
3. ike psk remove <peer> 与えられた相手から鍵を削除します。
4. ike psk key <peer> [<key>] 与えられた相手の鍵を表示または設定します。

12.8.2.5 証明書管理コマンド

1. ike cert bits [bits] 証明書を生成するときに使用されるビット数を表示または設定します。
2. ike cert days [days] 生成された証明書の有効期限が切れるまでの日数を、表示または設定します。
3. ike cert cn [cn] 証明書を生成するときに使用される共通名を表示または設定します。
4. ike cert generate 上述の 3 つのパラメータを使用して、スイッチが使用するための証明書を生成します。このオペレーションはただちに実行されます。
5. ike cert list すべての相手と CA 証明書を表示します。
6. ike cert mine スイッチの証明書を表示します。
7. ike cert remove <filename|"mine”> 証明書を永久に削除します。このオペレーションはただちに実行されます。
8. ike cert put <filename|"mine"|"request"><url> 証明書 (またはスイッチの証明書または証明書リクエスト) を与えられた URL に保存します。
9. ike cert get <"switch"|"peer"><url> 与えられた URL から証明書 (信頼して相手を認証するために、またはスイッチを識別するために) を復元します。

第 13 章 コマンドライン インターフェイスの使用

13.1 コマンドライン インターフェイス (CLI) 概論

コマンドライン インターフェイス (CLI) は、CLI ベース設定による自動化を目指して構築されています。相互作用は、Telnet、FTP および SMTP などの多くのインターネット プロトコルに使用されているものを手本としています。各コマンドが入力され処理されると、スイッチは数字のステータス コードと人間が解読可能なステータスの説明からなる応答をします。たとえば、RFC 821- Simple Mail Transfer Protocol (簡易メール転送プロトコル) の SMTP プロトコルの仕様 (http://www.faqs.org/rfcs/rfc821.html)、厳密に言うと「Appendix E - Theory of Reply Codes (応答コードの論理)」の詳細を参照して下さい。

コマンドの一般的なフォーマット

```
section parameter [value]
```

ここで、

- **セクション**はパラメータとグループ化するのに使用されます。
- • **パラメータ**はセクション内のパラメータを指定します。たとえば、ネットワーク セクションは DHCP、IP アドレス、サブネット マスクおよびデフォルト ゲートウェイのためのパラメータを保有。
- **値**はパラメータの新しい値です。値が省略される場合、現在値が表示されます。

新しい値は、明示的にコミットされるまで効力が生じませんので気を付けてください。

セクションおよびパラメータ名は、大文字と小文字を区別します。(例:「Network」と「network」は同じではありません)

注 : この章の CLI コマンド セクションのどのコマンドもグローバル コマンドを除いて、所属のセクション名から始めなければなりません。たとえば、スイッチの IP アドレスを変更するにはこのように入力します。

```
network address <newIP>
```

アドレス コマンドはこのマニュアルのネットワーク セクションにあるからです。

13.1.1 CLI にアクセス

CLI インターフェイスにアクセスするには、スイッチへのイーサネットまたはシリアル接続性を確立します。

イーサネットで接続するには、コマンド プロンプト ウィンドウを開き、次のように入力します。

telnet <switchip> (<switchip> の所にはスイッチの IP アドレスが入ります)

スクリーン ショット用プレース ホルダー

ログイン プロンプトでは、ユーザー名には「cli」を、パスワードには「admin」を入力します。スイッチは「Managed switch configuration CLI ready (マネージド スイッチ コンフィギュレーション CLI の準備ができました)」と応答します。

13.2 CLI コマンド

13.2.1 グローバル コマンド

次のグローバル コマンドは、CLI のどこでも利用可能です。

コマンド	効果
commit	値は必要に応じて相互検証を行います。有効の場合、値は適用されます。変更によっては、かなり時間がかかるので注意してください。
defaults	工場出荷時設定に復元します。
quit	CLI を終了します。 適用されていない変更は、通知なしで破棄されます。
reset	スイッチをリセットします。
help	ヘルプ メッセージを印刷します。
Prompt	プロンプトを有効または無効にします。(使用方法 :「prompt enabled」または「prompt disabled」)

工場出荷時設定に復元するとき、ネットワーク設定は「savenw」オプションを追加することで維持が可能です。または

defaults

がすべての値を復元しますが

defaults savenw

は現在の DHCP、IP アドレスなどの設定を除くすべてのデフォルトを復元します。

13.2.2　アクセス コンフィギュレーション

次の管理アクセス設定は CLI 経由で設定できます。

パラメータ	デフォルト	許容値
Snmp	both (両方)	none (なし)、snmpv2、snmpv3、both
terminal	both	none、telnet、ssh、both
web	both	non、http、https、both
cli	1	0、1
uitimeout	0	0 ～ 999
rouser	public (公開)	任意の有効なユーザー名
rwuser	private (非公開)	任意の有効なユーザー名
ropass	none	パスワード、その後は同じパスワードの繰り返し
rwpass	None	パスワード、その後は同じパスワードの繰り返し
adminpass	admin	パスワード、その後は同じパスワードの繰り返し
fwload	serial (シリアル)	「serial」はシリアル ファームウェア ローディング、また「network」はイーサネット限定

13.2.3　アラーム コンフィギュレーション

次の値はアラーム コンフィギュレーションで設定が可能です。

パラメータ	デフォルト	許容値／説明
List	n/a (該当なし)	No value (値なし) すべての現在のアラーム設定を表示。
Powerloss	enabled (有効)	「enabled」、「disabled (無効)」/ 電源入力を失った場合、アラーム出力は低い
ringfailure	disabled	「enabled」、「disabled」/ 電源入力を失った場合、アラーム出力は低い
以下の設定はポート番号が必要です。使用方法は次のとおり alarm <parameter> <port #> [<new value>]		
linkloss	disabled	「enabled」、「disabled」/ 指定のポートでリングがダウンした場合、アラーム出力が始動

13.2.4 modbus コンフィギュレーション

パラメータ	デフォルト	許容値／説明
enabled	0	0 または 1。1 は有効
stanum	1	1 ～ 247。Modbus ステーション番号の取得または設定のために使用
transport	tcp+udp	tcp / udp / tcp+udp。Modbus に許可するトランスポート層を指定
timeout	0	0 ～ 3600 またはなし。タイムは秒
maxcon	4	1 ～ 20。同時接続の最大数を設定
port	502	1 ～ 65535。Modbus ポーリング リクエストを聞くためのポート番号を設定

13.2.5 info コンフィギュレーション

次の値は info コマンドから読むことが可能です。

パラメータ	デフォルト	許容値／説明
fwversion	n/a (該当なし)	現在のファームウェアのバージョンを表示
cfgversion	n/a	コンフィギュレーションのバージョン番号を表示
macaddr	n/a	スイッチの MAC アドレスを表示
link	n/a	「all (すべて)」、ポート番号 / 指定したポート リンク ステータスを表示
support	n/a	役に立つサポート情報を表示 (IP など)
以下の設定は指定のフィルターが必要です info <parameter> <filter type> [<value>]		
mactable	n/a	フィルターは「id」、「port」、「mac」が可能。構文については下記を参照のこと。

info mactable コマンド用フィルター パラメータは次のとおりです。

id={*|#} ID ですべての /1 つの特定のフィルタリング データ ベースを表示

port={*|#[,#[,...]]} すべての /1 つの / 複数の特定のポートを表示

注 : ポート 33 はスイッチ CPU です。

mac={*|xx}:{*|xx}:{*|xx}:{*|xx}:{*|xx}:{*|xx} 与えられたパターンと一致する MAC アドレスのみを表示

13.2.6 ネットワーク コンフィギュレーション

スイッチは DHCP を有効または無効にできます。有効であっても、IP アドレス、サブネット マスク、およびデフォルト ゲートウェイの設定は可能です。値は保存され、DHCP が将来無効に成ったときに使用されます。

次の値はネットワーク コンフィギュレーションで設定可能です。

パラメータ	デフォルト	許容値
dhcp	disabled (無効)	enabled (有効)、disabled
address	192.168.0.1	ドット付き 10 進法の任意の IPv4 アドレス
subnet	255.255.255.0	ドット付き 10 進法の任意の IPv4 アドレス
gateway	none (なし)	ドット付き 10 進法の任意の IPv4 アドレス、またはゲートウェイがないことを示す「none」
Hostname	Model id	任意の有効なインターネット ホスト名。RFC 952 - DoD Internet host table specification (DoD インターネット ホスト テーブル仕様) (http://www.faqs.org/rfcs/rfc952.html) を参照のこと
dns1	none	ドット付き 10 進法の任意の IPv4 アドレス、または「none」
dns2	none	ドット付き 10 進法の任意の IPv4 アドレス、または「none」
domain	“”	有効なインターネット ドメイン
ntp	none	任意の FQDN (dns1 または dns2 が設定されている場合。設定がない場合は、ドット付き 10 進法の任意の IPv4 アドレス)、または ntp サーバがないことを示す「none」

13.2.7 ポート セキュリティ コンフィギュレーション

次の値はポート セキュリティ コンフィギュレーションで設定可能です。

パラメータ	デフォルト	許容値／説明
list	n/a (該当なし)	すべての現在のポート セキュリティ情報をリスト化
enable	n/a	MAC ベース ポート セキュリティを有効化
disable	n/a	MAC ベース ポート セキュリティを無効化
add	n/a	任意の有効な MAC およびポート番号 / 指定したポートの指定した MAC との通信を許可
remove	n/a	任意の有効な MAC / MAC セキュリティ テーブルからアドレスを削除

13.2.8 ポート コンフィギュレーション

次の値はポート コンフィギュレーションで設定可能です。

パラメータ	デフォルト	許容値
list	n/a (該当なし)	値なし。すべてのポート用のすべての設定をリスト化
monitor	1	任意のポート番号
以下の設定にはポート番号が必要です。使用方法は次のとおり。 port <port #> <parameter> [<new value>]		
name	port_# (ポート番号)	文字列
admin	enabled (有効)	enabled、disabled (無効)
negotiation	enabled	enabled (自動ネゴシエーション)、disabled (固定ネゴシエーション)
ratelimit	disabled	enabled、disabled
direction	none (なし)	none、egress (出口)、both (両方)
giveip	disabled	enabled、disabled
ipaddr	none	IP アドレス
sfp	1000	100、1000
Speed	(下記参照)	(下記参照)

オート ネゴシエーションで <speed> は次の場合があります。

10H、10F、100H、100F、1000F または FC

固定ネゴシエーションで <speed> は次の場合があります。

100H または 100F

有効な設定は「enabled」(「disabled」では、自動的に他のスピードに設定されます)

ポート スピード コマンドの構文は次のとおりです。

PORT <PORT #> SPEED …

(negotiation enabled)

speed 10H enabled

speed 10F disabled

. . .

ウェブ 形式でのチェック ボックスのような働きをします。

または、ネゴシエーションが無効の構文は次のとおりです。

speed 10H enabled

speed 100F enabled

. . .

ウェブ形式でのラジオ ボタンのような働きをします。

スピード FC の有効、無効は両方のモードで利用できます。

コンボ ポートでは、SFP スピードは次のように設定することがあります。

port <port#> sfp <speed>

13.2.9 リング コンフィギュレーション

次の値は、リング セクションで設定可能です。

パラメータ	デフォルト	許容値／説明
list	n/a (該当なし)	設定済みリングのリストを表示します。
master	auto (自動)	「auto」、「this」/ どのようにスイッチがリング マスターを決定するかを設定
以下の設定にはリング番号が必要です。使用方法は次のとおり。 ring <parameter> <ring #> [<new value>]		
enable	0	「0」、「1」/ リングが有効かどうかを表示または変更
name	n/a	任意のテキスト値 / 指定したリング名の表示または変更
ports	n/a	(下記参照) / このリングのプライマリおよびバックアップ ポートを表示または変更

指定したリングにプライマリおよびバックアップ ポートを設定するのは、次の構文です。

ring ports <ring#> <primary port #> <secondary port #>

13.2.10 rstp コンフィギュレーション

次の値は RSTP コンフィギュレーションで設定が可能です。

パラメータ	デフォルト	許容値／説明
protocol	rstp	none、stp、rstp または mstp / スパニング ツリー プロトコルを表示または変更
priority	0	0 ～ 61440 の範囲内で 4,096 の倍数 / 優先度を表示または変更

パラメータ	デフォルト	許容値／説明
mma	6	6 ～ 40 の範囲の整数 / 最大メッセージ エージを表示または変更
hellowtime	1	1 ～ 10 の範囲の整数 / ハロー間隔を表示または変更
fwddelay	4	4 ～ 30 の範囲の整数 / 転送遅延を表示または変更
Txlimit	1	1 ～ 10 の範囲の整数 / 伝送限界を表示または変更
Region	n/a (該当なし)	任意の有効なリージョン名
cfgrevision	n/a	任意の有効なリビジョン番号
maxhops	20	6 ～ 40 の任意の番号
以下の設定にはポート番号が必要です。使用方法は次のとおり。 rstp <parameter> <port #>[<new value>]		
exclude	0	「2」、「1」、「0」/ このポートが STP から除外されているかどうかを表示または変更
pprio	0	0 ～ 240 の範囲の整数 / このポートの優先度を表示または変更
pcost	none (なし)	「auto」または 0 ～ 200,000,000 の範囲の整数 / このポートのコストを表示または変更
type	1	「1」、「0」/ このポートのエッジ タイプを表示または変更
ptp	auto (自動)	「ForceTrue」、「ForceFalce」、「Auto」/ このポートのポイント ツー ポイント設定を表示または変更

13.2.11 qos コンフィギュレーション

次の値は QoS コンフィギュレーションで設定が可能です。

パラメータ	デフォルト	許容値／説明
schedule	strict (厳密)	「strict」、「fair (均等)」/ 公平度ルールを表示または変更
下記にはポート番号が必要です。 qos <parameter> <port#> [<new value>]		
usetag	1	「0」、「1」/ タグ優先度が使用されているかどうかを表示または変更
useip	1	「0」、「1」/ IP 優先度が使用されているかどうかを表示または変更
pref	tag (タグ)	「tag」、「ip」/ タグと IP の両方が有効の場合にどちらを使用するかを表示または変更

パラメータ	デフォルト	許容値／説明
priority	1	0 ～ 3 / このポートで受信したパケットに与えるためのデフォルト優先度
type	normal (通常)	「normal」、「add (追加)」、「remove (削除)」、「double (ダブル)」 / このポートへの接続タイプ
下記にはタグ番号が必要です。 qos tag<tag #> [<new value>]		
tag	(タグによる)	0 ～ 3 / 指定したタグの優先度を表示または変更

<new value> が指定されない場合、現在の設定が表示されます。

13.2.12 vlan コンフィギュレーション

次の値は VLAN コンフィギュレーションで設定が可能です。

パラメータ	デフォルト	許容値／説明
vlist	none (なし)	値なし。すべての設定した VLAN をリスト化
plist	none	値なし。各ポート用の VLAN 設定をリスト化
mode	disabled (無効)	「disabled」、「port (ポート)」、「standard (標準)」、「secure (セキュア)」 / VLAN モードを表示または変更
coretype	none	0x のプレフィクスをつけた 16 進数の値 / コア タグ用イーサタイプを表示または設定
mgmtvlan	1	1 ～ 4094 / 管理 VLAN ID を表示または設定
learning	shared (共有)	「shared」、「independent (独立)」 / VLAN 学習モードを変更
mgmtports	all (すべて)	1 ～ 9 / 管理 VLAN ポートを表示または設定
下のコマンドは vlist 中の vlan 番号が必要です。		
name	n/a (該当なし)	33 文字以下のストリング
vtype	n/a	「port」、「tag (タグ)」 / この VLAN のタイプを表示または変更
id	n/a	1 から 4094 の範囲の整数 / この VLAN の ID を表示または変更
ports	n/a	構文 : vlan ports <vlan#> <add/remove> <port#>
下のコマンドにはポート番号が必要です。		
pvid	1	1 から 4094 の有効な範囲の vlist の VLAN 番号
force	0	「0」、「1」

パラメータ	デフォルト	許容値／説明
add	(下記参照)	(下記参照)
remove	(下記参照)	(下記参照)

以下の例で、「port」、「add」、および「remove」コマンドの構文を説明します。

ポート ベース VLAN の追加は次のとおりです。

vlan ports <vlan #> add <port #>

vlan ports <vlan #> remove <port #>

vlan add <name> port <port #> <port #> [...]

タグ ベース VLAN の追加は次のとおりです。

vlan add <name> tag <vlan ID> <port #> <port #> [...]

VLAN の削除は以下の通りです。

vlan remove <vlan # or all>

13.2.13 igmp コンフィギュレーション

下記コマンドは IGMP の設定に使用できます。

パラメータ	デフォルト	許容値／説明
rlist	n/a (該当なし)	値なし / すべてのポート用のルーター設定をリスト化
mode	router (ルーター)	「disabled (無効)」、「snoop (スヌープ)」、「router」/ IGMP モードの表示または変更
msupp	none (なし)	「none」、「ip」、「all (すべて)」/ マルチキャスト抑制方法を表示または変更
version	2	1、2 / IGMP バージョン
robustness	2	1 ～ 99 / IGMP ロバスト性
qinterval	125	60 ～ 125 / IGMP クエリ間隔
qresponse	10	1 ～ 30 / IGMP クエリ応答間隔
下のコマンドはポート番号が必要です。		
router	0	0、1 / IGMP ルーターにつながるポートを識別
exclude	0	0、1 / IGMP リクエストとクエリの処理からポートを除外

13.2.14 chkpt コンフィギュレーション

次の値はチェックポイント コンフィギュレーションで設定が可能です。

パラメータ	デフォルト	許容値／説明
save	n/a (該当なし)	None (なし)/ チェックポイントを保存
restore	n/a	「net」、「nonet」/ net は現在のネットワーク設定を保存。nonet は現在のネットワーク設定を破棄。
ftpsave	n/a	ファイル名
ftprestore	n/a	ファイル名

13.2.15 ファームウェア コンフィギュレーション

パラメータ	デフォルト	許容値／説明
default	n/a (該当なし)	1 または 2。デフォルト ファームウェアを表示または変更
running	n/a	どのファームウェア イメージが実行中かを表示
list	n/a	現在利用可能なファームウェア イメージおよび対応するヘルス ステータスを表示
update	n/a	[showProgress] [md5=<md5>] [url] が続く「showProgress」引数が提供される場合は、印刷の進捗が表示されます。「md5」引数が提供される場合は、受信したファームウェアの MD5 チェックサムが、提供された MD5 チェックサムに対して照合されます。URL は、スイッチが直接アクセスできる有効な HTTP または HTTPS アドレスでなければなりません。
ftpload	n/a	続いて bhe filename は TFTP サーバからアップロードされます。

13.2.16 tftp コンフィギュレーション

次のオプションは TFTP コンフィギュレーションで設定が可能です。

パラメータ	デフォルト	許容値
tftp	“”	有効な完全修飾ドメイン名

13.2.17 tz コンフィギュレーション

次の値はタイムゾーン コンフィギュレーションで設定が可能です。

パラメータ	デフォルト	許容値
list	(下記参照)	(下記参照)
value	none (なし)	リストからのタイムゾーン

注 : すべてのタイムゾーンのリストを表示するには、「tz list [<prefix>]」コマンドを使用し、オプションで <prefix> の文字で始まるタイムゾーンでフィルターをかけます。

13.2.18 msti コンフィギュレーション

パラメータ	デフォルト	許容値
list	n/a (該当なし)	すべての MSTI とその優先度をリスト化
plist	n/a	続く mstid は、指定した MSTI のすべてのポートを、そのコストおよび優先度と共に表示するために使用されます。
add	n/a	name mstid [priority] が続きます。
remove	n/a	任意の有効な MSTI、また all はすべての MSTI を削除
priority	32768	mstid [priority] が続きます。
pprio	varies (変動する)	MSTI ポート優先度ごとに使用される mstid portno [pprio] が続きます。
pcost	varies	MSTI ポート コストごとに使用される mstid portno [pcost] が続きます。
name	n/a	mstid [name] が続きます。
mstid	n/a	mstid [newmstid] が続きます。
inherit	n/a	任意の有効な MSTI。CIST から引き継ぐために使用。

13.2.19 一般的コンフィギュレーション

下のコマンドは一般的なコマンドで、他のサブセクションの一部ではありません。

パラメータ	デフォルト	許容値／説明
location	<set location of switch > (スイッチのロケーションを設定)	任意のテキスト値 / スイッチの位置
contact	<set name (and email) of contact for switch > (スイッチの連絡先の名前 (および E メール) を設定)	任意のテキスト値 / ネットワークまたはサイト管理者の連絡先情報

13.2.19.1 コンフィギュレーション セッション例

次の例では、太字テキストがスイッチによって送信され、通常のテキストがユーザーによって入力されます。スイッチのシリアル ポートに接続すると、ログイン バナーとプロンプトが表示されます。

注 : このソフトウェアへのログインすることにより、本ユーザー マニュアルに記載のソフトウェア ライセンスに従うことにあなたが同意したと認定します。

Switch login: cli

Password: <hidden>

210 Managed switch configuration CLI ready.

network dhcp

212 Current dhcp setting is 'disabled'

network address 192.168.1.1

112 address set to '192.168.1.1'

network hostname switch-1

112 hostname set to 'switch-1'

rstp protocol rstp

113 protocol set to 'rstp'

info link all

219-List of link status

Port#	Name	Link
1	port_1	down
2	port_2	down
3	port_3	100f
4	port_4	down
5	port_5	down
6	port_6	down
7	port_7	down
8	port_8	down

219 List of link status

info fwversion

219 Current fwversion setting is '4.4'

vlan mode standard

117 mode set to 'standard'

vlan mgmtports

217 Current mgmtports setting is 'C 1 2 3 4 5 6 7 8'

Commit

210 Managed switch configuration CLI done.

quit

210 Managed switch configuration CLI done.

quit の後、CLI プログラムが終了し、セッションが終わります。ログイン バナーおよびプロンプトが再び表示されます。

コミット コマンドと CLI の応答の間に最大 1 分の遅延が生じることがありますが、これは正常です。

付録 A ライセンスとポリシー

この付録は、Red Lion 製品のライセンスおよびポリシー情報を提供します。

1. 所有権

本マネージド スイッチ ソフトウェアは、本ソフトウェアのメイン メニューで宣言されている通りライセンサーの所有物であり、米国の著作権法、商標法、および国際条約によって保護されています。本ソフトウェアの所有権がライセンシーに移転することはありません。ライセンシーは、ライセンサーの著作権、商標または所有権通知をソフトウェアや関連する文書から削除したり、目立たなくしたりしてはなりません。ライセンシーは、いかなるソフトウェアの複製物を許可なく作成しないことに同意します。本契約書に明示している場合を除き、ライセンサーは、ライセンサーの特許、著作権、商標または企業秘密に属する情報に基づくいかなる明示または黙示の権利も、ライセンシーに許諾しません。本ソフトウェアは、ファームウェアをライセンサーのハードウェア製品に組み込み一体化させて使用します。このファームウェアは、この許可されたソフトウェアの一部であることに同意します。ライセンサーのハードウェア製品の意匠は、ライセンサーの所有財産であることにも同意します。

2. ライセンス

ライセンスの作成者は、必要な登録を完了し、かつ本契約書の内容および入手した登録のあらゆる制限事項に同意する場合のみ、「ライセンシー」が本ソフトウェアを使用するためのライセンスを許諾します。本ソフトウェアの所有権がライセンシーに移転することはありません。本ライセンスは非独占です。本ライセンスは、ライセンサーとの OEM 契約に基づく場合を除き、譲渡不能です。ライセンシーが本ソフトウェアの複製を許可されるのは、、許諾されたライセンスに従って使用し、これらの複製物がバックアップまたは保管を目的とする場合に限ります。ライセンシーは、無許可で本ソフトウェアまたは供与された登録番号の複製をしないことに同意します。

3. 制限事項

本契約に定める場合を除き、ライセンサーの明示された同意書なしで、ライセンシーは複製、販売、譲渡、貸出、賃借、賃貸、改変、派生物の生成、または製品の改造をすることはできません。ライセンシーは製品のリバース エンジニアリング、逆コンパイル、分解、または使用許諾を受けたソフトウェアからソース コードを抽出するなどの試みをすることはできません。

4. 無保証

ライセンサーは、市販性や特定目的に対する適合性の黙示保証などのソフトウェアに関する保証は一切しません。したがって、そのような性質の保証には一切応じられません。いかなる場合でも、ライセンサーまたはライセンサーの代理人により提示される口頭または書面の情報や助言によって、新たに保証が発生したり、あるいはこの保証の適用範囲が拡大したりすることはありません。

5. 責任制限

過失を含むいかなる場合においても、製品の使用または使用不能の結果による、いかなる付随的、特別な、または結果的に生じる損害に関して、たとえライセンサーがこのような損害の可能性に関する助言を受けていたとしても、ライセンサーに責任はないものとします。ライセンサーは、製品の使用によりライセンシーに生じる可能性のある問題解決のために、相応の努力を払わなければなりません。ライセンサーのライセンシーに対する責任総額は、契約上の一切の破損、損失または訴因、不法行為もしくはその他どのような場合でも、賠償請求の根拠となるライセンシーが払ったソフトウェアまたはハードウェア製品の金額を超えないものとします。

6. 危険性の高い行為

生命へ有害で危険な、またはフェイルセーフなパフォーマンスを必要とする生命に危険性がある環境にあるオンライン制御装置、たとえば原子力施設、航空機航行または航空通信システム、航空管制、直接的な生命維持装置、または兵器システムなどの業務に使用または転売を目的とした製品に取り込むために、ライセンサーが本ライセンス ソフトウェアを耐故障性、設計、製造、対象をしていないことにライセンシーは同意します。ライセンサーは危険性の高い行為に対して、いかなる明示または黙示の適合性の保証には一切応じません。ライセンシーは、本ソフトウェアまたは派生著作物を、危険性の高い行為に使用しないことを明確に示し、保証します。

7. 補償

ライセンシーは、一切の損害賠償、罰金、損失、損害、費用、経費、弁護費用、ライセンシーまたはライセンサー、またはいずれの他方当事者のいずれかに損害を与えるライセンシーによるソフトウェアの使用、販売、または流通に直接または間接的に起因するまたは結果としての訴因または請求のすべてを補償し、ライセンサーに損害、損失を与えないことに同意します。本補償および賠償責任免除特約は、ソフトウェアまたは本ライセンスに関連するすべての問題に適用されます。

8. 知的財産権侵害

ライセンシーは、本契約に基づいてライセンシーがライセンスを許諾されたライセンサーの製品に対して、追加された単一または複数の項目が、第三者の特許権を含むいずれかの知的財産権の侵害または侵害の可能性がある場合は、前記のライセンサーの製品に、任意の単一または複数の項目を追加したり追加されたりしてはいけません。前記の追加された単一または複数の項目は、特定用途向けソフトウェア、コンフィギュレーション ファイル、データまたはドキュメント ファイル、アプリケーション プログラム、ウェブ ページ、GPL (一般公衆利用許諾書) ソフトウェア、第三者のアプリケーション ソフトウェアなどです。

ライセンシーまたはその代理人によって、ライセンサーの製品に追加された特定用途向けソフトウェア、コンフィギュレーション ファイル、データまたはドキュメント ファイル、アプリケーション プログラム、ウェブ ページなどに起因するいずれかの侵害または侵害の可能性に関して、本契約に基づき、ライセンサーはライセンシーに対する責任または義務を提供せず、またそれらがないことにライセンシーは同意します。この責任制限にはすべての GPL (一般公衆利用許諾書)、およびライセンシーへの融通としていずれかの製品に搭載される第三者のアプリケーション ソフトウェアが含まれます。

9. 契約の終了

本契約は、終了するまで有効です。本ライセンスは、ライセンシーが本ライセンスのいかなる条項、または当事者間に存在するいかなる他の契約に従わなかった場合、ライセンサーによる通知なしでただちに終了します。本契約の終了にあたり、ライセンシーは一切のソフトウェアの使用、販売または流通をただちに停止しなければならず、すべての当ソフトウェアの複製物および関係書類を破棄しなければなりません。仲介人を通してライセンス ソフトウェアが購入された場合は、本ソフトウェアのライセンサーは、本取引における第三者の受益者の対象者であり、自らの名義で直接ライセンシーに対し、これを強制する権限があります。

10. 準拠法

本ライセンスは、すべての点においてニューヨーク州の裁判所、管轄区、および州法に準拠するものとします。ライセンシーはソフトウェアまたは素材を、適応される輸出法や規則に違反して輸出することはできません。いかなる理由かで正当な管轄権のある裁判所が、本ライセンスの条項のいずれかまたはその一部が履行不能だと判断した場合、その条項は最大限の範囲で実行されるので、当事者の意図と本許諾契約書のその他の条項は完全に効力が存続します。

Red Lion 保護型技術ポリシー — Red Lion は、長期的に計画された技術および当社独自の保護型技術ポリシーにより、お客様の Red Lion システムへの投資を保護します。当社は、最低 5 年間 (産業用マネージド スイッチについては 20 年) は継続的に Red Lion 規格品の特定の機能をサポートします。各製品の改良および既存のデザインと設定に上位互換性がある新機能を計画します。当社の目標は、新しくリリースされる各ソフトウェアが、お客様の Red Lion システムに新しいパワーを与え、すべての既存の機能、アプリケーション プログラム、データ ファイルを引き続き使えるようにすることです。さらに寛大な 5 年の下取りポリシーにより、お客様の投資を手厚く保護します。新機能の利用や性能の向上のため、規格品の同じ製品のアップグレード版への交換は、5 年間いつでも承ります。配分された下取り価格が、お客様の既存製品に与えられます。Red Lion はお客様の長期的な生産能力を、最新の計画された技術と継続的サポートで保護します。

Red Lion の保証制限 — Red Lion 製品の製造元である Red Lion 社は、ソフトウェアを除く Red Lion が製造した製品に、材料の面でも仕上がりの面でも欠陥がないことを購入者に対し保証いたします。この保証に基づく Red Lion の義務は、Red Lion の選択により、設置日から 5 年以内の欠陥部品の修理または交換に限られます。購入者による製品の返品は、Red Lion から許可を得た後でのみ可能です。購入者は、Red Lion が指定する修理施設あての返品にかかる全送料を前払いしなければなりません。この保証制限は購入者から、または購入者への輸送中に生じる損失または損害、不適切な設置、メンテナンス不良、誤用、不注意、あるいは通常の商業利用や工業利用以外の原因によって生じる損失または損害は保証対象外とします。特に、Red Lion は、市販性または特定の目的への適合性に関する暗黙の保証は一切行っていません。したがって、そのような性質の保証はここに明示的に否認します。Red Lion または Red Lion の代理人により提示される口頭または書面の情報や助言によって、新たに保証が発生したり、あるいはこの保証の適用範囲が拡大したりすることはありません。この保証制限は、口頭であると書面であるとを問わず、また明示であると黙示であるとを問わず、その他すべての保証に代わるものです。Red Lion の責任は、賠償請求の根拠となる個々の機器の価格を上限とします。いかなる場合においても、Red Lion は利益の損失、施設または装置の使用機会の喪失、その他の間接的、偶発的、あるいは結果的な損害に関して、一切責任を負いません。

付録 B 規定に関する声明

設置および危険場所に関する警告 — これらの製品を、正規の安全インターロックの代わりとして使用しないでください。ソフトウェア ベースのデバイス (またはその他のソリッドステート デバイス) は、重要な設備の保守や作業員の安全に対処するよう設計されていません。特に、いずれかの用途でその設備の使用によって直接または結果的に生じる損害について、Red Lion はその使用方法にかかわらず一切の責任を負いません。すべての電源および入出力 (I/O) 配線は、Class I、Division 2 配線方式、および管轄当局の指示に従ってください。

警告 (爆発の危険) 部品の交換により、Class 1、Division 2 (ゾーン 2) に適合しなくなる可能性があります。

警告 (爆発の危険) 危険場所では、装置の交換や配線を行う前に必ず電源を切断してください。

警告 (爆発の危険) 装置の取り外しは、電源を切った状態か、その区域が非危険場所であることが確認された後に行ってください。

米国連邦通信委員会 (FCC) 適合宣言　— 本装置は、FCC 規格第 15 部で定義されているクラス B デジタル装置の規格テストに合格し、準拠していることが証明されています。この基準は、住宅に設置する際、有害な干渉から適切に保護することを目的としたものです。本装置は、高周波エネルギーを生成、使用、および放射することがあり、本書の指示に従って適切に設置および使用しなかった場合には、無線通信にとって有害な干渉が発生することがあります。ただし、特定の設置において干渉が発生しないことは保証されていません。本装置がラジオもしくはテレビの受信に有害な干渉を引き起こしているかどうかは、本装置をオフとオンに切り替えることで確認できます。本装置が有害な干渉を引き起こしている場合は、次のいずれかの方法で干渉を解消することを推奨します。受信アンテナの方向や位置を変える。本装置と受信機の間隔を広げる。本装置を、電気回路の受信機が接続されているものとは異なる差し込み口に接続する。販売元または熟練したラジオ / テレビ技師に相談する。

付録 C デフォルト ソフトウェア コンフィギュレーション設定

C.1 デフォルト設定について

以下の設定は、スイッチを箱から出したときの工場出荷時の初期設定です。このページを参考にして、必要に合わせてスイッチを調整してください。

C.1.1 管理ポート

- DHCP: disabled (無効)
- IP Address (IP アドレス): 192.168.0.1
- Subnet Mask (サブネット マスク): 255.255.255.0
- Default Gateway (デフォルト ゲートウェイ): none (なし)
- NTP: Disabled
- Timezone (タイムゾーン): GMT (グリニッジ標準時間)

C.1.2 ポート 1 ～ 9 (以上) のためのポート コンフィギュレーション

ポート	名称	管理	モード	速度 & 双方向通信	フロー制御
1	Port_1	Enabled (有効)	Auto (自動)	10h 10f 100h 100f	Disabled (無効)
2	Port_2	Enabled	Auto	10h 10f 100h 100f	Disabled
3	Port_3	Enabled	Auto	10h 10f 100h 100f	Disabled
4	Port_4	Enabled	Auto	10h 10f 100h 100f	Disabled
5	Port_5	Enabled	Auto	10h 10f 100h 100f	Disabled
6	Port_6	Enabled	Auto	10h 10f 100h 100f	Disabled
7	Port_7	Enabled	Auto	10h 10f 100h 100f 1000f	Disabled
8	Port_8	Enabled	Auto	10h 10f 100h 100f 1000f	Disabled
9	Port_9	Enabled	Auto	10h 10f 100h 100f 1000f	Disabled

C.1.3 ポート ミラーリング

Mirroring (ミラーリング): Disabled (無効)

C.1.4 RSTP/STP コンフィギュレーション

- edundancy Protocol (冗長プロトコル): RSTP
- Bridge Priority (ブリッジ優先度): 32768
- Max. Age (最大エージタイム): 20
- Hello Time (ハロー間隔): 2
- Forward Delay (転送遅延タイム): 15
- Transmission Limit (伝送限界): 6

C.1.5 RSTP/STP ポート コンフィギュレーション

ポート	名称	R(STP)	優先度	コスト	タイプ	PtpMAC
1	Port_1	Included (あり)	128	200000	Auto (自動)	Auto (自動)
2	Port_2	Included	128	200000	Auto	Auto
3	Port_3	Included	128	200000	Auto	Auto
4	Port_4	Included	128	200000	Auto	Auto
5	Port_5	Included	128	200000	Auto	Auto
6	Port_6	Included	128	200000	Auto	Auto
7	Port_7	Included	128	200000	Auto	Auto
8	Port_8	Included	128	200000	Auto	Auto
9	Port_9	Included	128	200000	Auto	Auto

C.1.6 SNMP 通知

すべてのトラップが無効

C.1.7 IGMP 設定

- IGMP Mode: Active IGMP (アクティブ IGMP)(router mode)(ルーター モード)
- Multicast suppression (マルチキャスト抑制): None (なし)
- IGMP Version (IGMP バージョン): 2

- Robustness (ロバスト性): 2
- Query Interval (クエリ間隔): 125 秒
- Query Response Interval (クエリ応答間隔): 10 秒
- Static Router (静的ルーター): すべてのポートで Disabled (無効)

C.1.8 トラップ マネージャ

トラップ マネージャは設定されていません

C.1.9 優先度付きキュー

- Use 802.1p Tag Priority (802.1p タグ優先度を使用): Enabled (有効)
- Use IP ToS/DiffServ (IP ToS/DiffServ (ディフサーブ) を使用): Enabled
- Priority Precedence (優先度優先): Tag (タグ)
- Default Priority (デフォルト優先度): Normal (通常)
- Type (タイプ): Transparent (透過型)
- QoS Scheduling (スケジューリング): Strict (厳密)

C.1.10 SNMP システム情報

- Contact (連絡先): < スイッチの連絡先名 (および E メール) を設定 >
- System Name (システム名): Managed Switch (マネージド スイッチ)
- Location (ロケーション): < スイッチの位置を設定 >

C.1.11 リモート アクセス セキュリティ

- SNMP Access (SNMP アクセス): SNMPv2 と v3 の両方有効
- Terminal Access (端末アクセス): SSH と telnet の両方有効
- Web Access (ウェブ アクセス): http と https の両方有効
- Inactivity logout (不活動時のログアウト): 5 分
- SNMP Read-only Name (SNMP 読み出し専用名): public
- SNMP Read-only Password (SNMP 読み出し専用パスワード): publicpwd
- SNMP Read/write Name (SNMP 読み書き名): private
- SNMP Read/write Password (SNMP 読み書きパスワード): privatepwd
- Admin Password (管理者パスワード): admin

C.1.12 IEEE タギング

優先度	トラフィック タイプ	キュー
0	Best Effort (ベスト エフォート)	1
1	Background (バックグラウンド)	0
2	Spare (予備)	0
3	Excellent Effort (エクセレント エフォート	1
4	Controlled Load (負荷制御型)	2
5	Video (ビデオ)	2
6	Voice (音声)	3
7	Network control (ネットワーク制御)	3

C.1.13 VLAN モード

Disabled (無効)

C.1.14 VLAN ポート設定

ポート	PVID	Force (強制)	タイプ
1	1	Disabled (無効)	Transparent (透過型)
2	1	Disabled	Transparent
3	1	Disabled	Transparent
4	1	Disabled	Transparent
5	1	Disabled	Transparent
6	1	Disabled	Transparent
7	1	Disabled	Transparent
8	1	Disabled	Transparent
9	1	Disabled	Transparent

C.1.15 モデム設定

- Auto-answer rings (自動応答): 2
- Comma delay (コンマ遅延): 1
- Speed (速度): MAX
- Data Compression (データ圧縮): Both (両方)
- Error Correction (エラー訂正): Enabled (有効)
- Custom initialization (カスタム初期化): 空白
- Digital output meaning (デジタル出力状態): Power OK (電源 OK)

C.1.16 PPP 設定

- PPP Mode (モード): Disabled (無効)
- User name (ユーザー名): PPPLink
- User phone number (ユーザー電話番号): 空白
- Password (パスワード): Link2Sixnet
- Idle Timeout (アイドル タイムアウト): 60 秒
- Default route (デフォルト ルート): Enabled (有効)
- Server calls back (サーバ コールバック): Disabled
- Switch's phone number (スイッチ電話番号): 空白
- Client IP (クライアント IP): 空白
- Route to Gateway (ゲートウェイへのルート): Disabled

C.1.17 リモート ユーザー

すべてのユーザーが無効

C.1.18 ルーティング

- PPP Rip mode: Disabled
- PPP Send (送信): RIP v1
- PPP Receive (受信): RIP v1
- LAN Rip mode: Disabled
- LAN Send: RIP v1
- LAN Receive: RIP v1

C.1.19 ダイヤル アウト メッセージング

Digital input action (デジタル入力アクション): Disabled

Primary phone number (プライマリ電話番号): 空白

Secondary phone number (セカンダリ電話番号): 空白

Number Selection (番号選択): Alternate (交互)

Retry Limit (リトライ制限): 2

Retry delay (リトライ遅延): 120 秒

Message type (メッセージ タイプ): Numeric (数字)

デフォルト設定について

Message (メッセージ): 空白

Send Message delay (メッセージ送信遅延): 2 秒

ACK Message: 空白

Message resend limit (メッセージ再送信制限): 2

Message resend delay (メッセージ再送信遅延): 2 秒

付録 D SNMP サポート

グループ	概要	ロケーションと RFC	サポート
System (システム)	システムとしてのスイッチに関する情報。名称、記述、物理的位置、アップタイム、連絡先、および MIB の他のグループのリスト	1.3.6.1.2.1.1 RFC 1213	この MIB は完全に対応しています
Interfaces (インターフェイス)	インターフェイス層のポートごとの情報	1.3.6.1.2.1.2 RFC 1229	ifTable: 基本インターフェイス情報 ifXTable: 拡張インターフェイス情報 ifStackTable: インターフェイス層 (VLAN 用)
AT	IP アドレスを MAC アドレスにマップするためのアドレス変換情報	1.3.6.1.2.1.3 RFC 1213	この MIB は完全に対応しています
IP	管理対象ノードの IP 層の記録を付けるために使用する情報	1.3.6.1.2.1.4 RFC 2011	この MIB は完全に対応しています
TCP	TCP を使用するアプリケーションエンティティの記録を付けるために使用する情報	1.3.6.1.2.1.6 RFC 2012	この MIB は対応していますが、ホスト指向性 MIB なので、特に役には立たないかもしれません。
UDP	ユーザー データグラム プロトコルを使用するアプリケーション エンティティの記録を付けるために使用する情報	1.3.6.1.2.1.7 RFC 2013	この MIB は対応していますが、ホスト指向性 MIB なので、特に役には立たないかもしれません。

グループ	概要	ロケーションと RFC	サポート
Dot3	「イーサライク」装置のためのパフォーマンス統計	1.3.6.1.2.1.10.7 RFC 2665	この MIB は完全に対応しています
SNMP	SNMP プロトコル エンティティおよび装置が応答する管理トラフィック量の追跡に関する統計情報	1.3.6.1.2.1.11 RFC 1213	この MIB は完全に対応しています
RMON	リモート監視	1.3.6.1.2.1.16 RFC 1757	グループ 1: イーサネット統計 グループ 2: イーサネット履歴 (30 秒間 8 サンプル、および各ポート毎に 30 分間隔)
Dot1dBridge	STP/RSTP MIB	1.3.6.1.2.1.17 RFC 1493	dot1dStpPortTable: スパニング ツリー プロトコル情報 dot1dTpFdbTable: 学習した MAC アドレスとポートとの関連づけ dot1dTpPortTable: RMON と類似のポート情報
Dot1dBase	基本 STP/RSTP 情報	1.3.6.1.2.1.17.1 RFC 1493	この MIB は完全に対応しています
Dot1dStp	スパニング ツリー プロトコル オペレーティング パラメータ	1.3.6.1.2.1.17.2 RFC 1493	この MIB は完全に対応しています
Dot1dTp	透過型ルーティング パラメータおよびパフォーマンス	1.3.6.1.2.1.17.4 RFC 1493	この MIB は完全に対応しています
Dot1qBridge	VLAN MIB	1.3.6.1.2.1.17.7 RFC 2674	この MIB は完全に対応しています
IGMPStdMIB	IGMP MIB	1.3.6.1.2.1.85 RFC 2933	この MIB は、すべての関連事項に完全に対応しています
ETxMS	スイッチ特化データ (プライベート MIB)	1.3.6.1.4.1.20540.2.1	この MIB は完全に対応しています。下記を参照のこと。

- 最新の Sixnet MIB テキスト ファイルは、こちらで参照してください。

  http://www.sixnet.com

付録 E コンセプトと定義

10/100BASE-Tx、100BASE-FX、1000BaseT/F	これはポートのタイプを表します。10BASE-T は 10 Mbps カッパー (RJ45) ポートで、100BASE-TX は 100 Mbps カッパー ポート、100BASE-FX は 100 Mbps 光ファイバ ポートで、1000BaseT/F は 1000 Mbps カッパーまたは光ファイバ ポートです。
Active Communication (アクティブな通信)	防害 (ブロックされた状態のポートなど) のない 2 つのデバイス間の有効な通信です。ルートからいずれのエンド ノードへもアクティブな通信パスが 1 つだけである限り、アクティブ トポロジー内にループは発生しません。
Auto-MDI/MDIX Crossover (自動 MDI/MDIX クロスオーバー)	スイッチの RJ45 (カッパー) ポートは自動的にケーブルの種類 (ストレートまたはクロス) を検出し、それに従って再設定します。
Auto-Polarity (自動極性)	スイッチの RJ45 (カッパー) ポートは、TD と RD のペアの逆極性を知的に修正します。
Auto-Sensing or Auto-Negotiation (自動検知または自動ネゴシエーション)	スイッチの RJ45 (カッパー) ポートは知的に速度 (10BASE-T - 10 Mbps または 100BASE-TX - 100 Mbps) と双方向通信 (半二重または全二重) を検出します。光ファイバ ポートは 100BASE-FX に固定されており、双方向通信が設定可能です。
BPDU	ブリッジ プロトコル データ ユニット。このデータ ユニットは、ネットワーク ステータスをブリッジに通知し続けるために使用されます。
Bridge Priority (ブリッジ優先度)	どのスイッチがルートになるかについての階層レベルの作成を助ける設定
Bridge (ブリッジ)	2 つのネットワーク間の接続または通信の手段に使用される装置。「スイッチ」とも呼ばれます。
CoS	クラス オブ サービスは、トラフィック タイプに基づくネットワーク トラフィックの優先付けをする方法です。(QoS、ToS、トラフィック クラスの項を参照のこと)
Designated Bridge (指定ブリッジ)	各マネージド ブリッジは、接続している LAN (指定ポート経由で) に指定されています。ルート ブリッジは、マネージド ネットワークのすべての LAN に指定されています。
DHCP	ダイナミック ホスト コンフィギュレーション プロトコル。ネットワークで IP アドレスを割り当てるために使用するプロトコルです。ネットワークへアクセスするためにこのプロトコルを使用する装置は、毎回異なる IP アドレスを持つかも知れないという、動的に変化する IP アドレスを取得します。

DNS	ドメイン名サーバ。このサーバはドメイン名を IP アドレスに変換します。
Duplex (双方向通信) (全二重または半二重)	半二重は一度に 1 つの方向にしかメッセージが流れません。全二重は同時に両方向にメッセージが流れます。スイッチの RJ45 ポートは自動的に全二重と半二重の両方のフロー制御に対応 (自動検知) します。光ファイバ ポートは、全二重と半二重のフロー制御をソフトウェアで設定が可能です。
Edge Port (エッジ ポート)	1 つのエンド ステーションにだけリンクしていて、ネットワークにループを作成できないポート。
Forward Delay (転送遅延タイム)	STP で使用する時間で、ポートがネットワーク トラフィックを転送する様に移行することが安全かどうかを決定する前に待機する時間。
Full Duplex (全二重)	1 つのリンクを通して両方向へ同時にデータを送信します。
Gateway IP (ゲートウェイ IP)	2 つのネットワークをつなぐために使用する装置の IP アドレス。
GDA	グループ宛先アドレス。マルチキャスト データのために宛先アドレスとして使用するクラス D の IP アドレス。クラス D の IP アドレスは最上位ビット 1110 を持ち、224.0.0.0 から 239.255.255.255 の範囲です。
Half Duplex (半二重)	いかなる時点でも装置中 1 台だけがデータを送信します。
Hello Timer (ハロー タイマー)	タイマーの値は、STP コンフィギュレーション メッセージがルート ブリッジから送信される間隔を示します。
IEEE 802.3	これがイーサネットの基本規格です。このスイッチはこの基本規格と、802.3u (100BASE-TX)、802.3x (フロー制御付き全二重)、802.1D-2004 (STP、RSTP) などのさまざまな関連する副規格に適合します。
IEEE 802.1Q	このスイッチは、仮想 LAN オペレーション用のこの規格に準拠します。
IGMP	インターネット グループ管理プロトコルは IP マルチキャスト フィルタリングに使用されます。
IP Address (IP アドレス)	IP パケットが行くべき宛先を示すのに使用するアドレス
IPv4	インターネット プロトコル バージョン 4
IPv6	インターネット プロトコル バージョン 6
Latency (遅延)	1 つのポートから他のポートへと、スイッチ内部を通ってメッセージ伝送する時間です。典型的なメッセージの遅延は 5 マイクロ秒 (Mbps) またはそれより速いです。
MAC Address (MAC アドレス)	各イーサネット装置は固有の「MAC」アドレスを、送信する各メッセージに挿入します。付与された MAC アドレスが利用するスイッチのポートは、フレームをそのアドレスから受信すると自動的に学習します。一度アドレスを学習すると、ハブのようにすべてのポートにメッセージをブロードキャストしてしまうのではなく、スイッチはメッセージを適切なポートにだけ送ります。新しいアドレスを学習すると、タイム スタンプもメモリに記録されます。このタイムスタンプは、300 秒間使用していない MAC アドレスをテーブルから削除するエージング機能で使用されます。装置が移動する場合、スイッチの関連ポートも、必要に応じて変更 (移動) されます。最大 2,048 個の MAC アドレスがいつでも保持され、監視されます。

Managed Switch (マネージド スイッチ)	LAN 間でパケットを転送する装置。この装置はスパニング ツリー プロトコルを使用してループ構成を実現する能力もあります。ループ構成は、ネットワーク上の単一ハードウェア障害を防ぐために使用されます。ネットワークに関する管理情報も、MIB にクエリすることでスイッチから取得します。
Multicast (マルチキャスト)	すべてのホストにデータをブロードキャストすることなく複数のホストにメッセージを送信する手段。また関心のあるホストそれぞれにメッセージを個別に送信することなく、関心あるホストが存在するネットワーク セグメントにだけマルチキャスト トラフィックを伝送する必要がある場合、IGMP をマルチキャスト メッセージのルーティングの最適化に使用することがあります。
Max Message Age (最大メッセージ エージ)	再構築が必要になる前に STP アルゴリズムが待機する時間の長さ。
MIB	管理情報ベース。ネットワーク管理システム (マネージド スイッチなど) のある形態によって使用されるオブジェクトのデータベース。SNMP や RMON は MIB から情報を取得するための一般的なツールです。
Mirroring (ミラーリング)	この診断機能により、1 つ以上の元ポートからのメッセージを複数のターゲット (監視) ポートにコピーすることが可能です。そして、ポート分析機または「スニファー」プログラムを使って、スイッチの稼働に影響を与えずにトラフィックを監視することができます。
Notification (通知)	「Trap」の項を参照のこと。
Path Cost (パス コスト)	情報パケットが通過しなければいけない各経路には、関連コストがあります。数字が送信元ポートから宛先ポートへのコストを表示するのに用いられます。特定の送信元および宛先への一連の経路の中で一番小さい数 (もっとも低いコスト) が、選択肢中の最適経路として選ばれます。
PPP	ポイント ツー ポイント プロトコル。低速ネットワーク接続であるかのようにシリアル接続が使用できます。
Point to Point MAC (ポイント ツーポイント MAC)	この指標は、STP アルゴリズムの収束時間の最適化に使用されます。
Port Priority (ポート優先度)	ポートに与えられた数値で、指定ポートになるための階層順位を示します。
QoS	クオリティ オブ サービス。遅延、フレーム損失、ユーザー優先度などのネットワークパラメータの一般的表記述 (CoS と ToS の項も参照のこと)。
RMON (リモート監視)	このネットワーク管理プロトコルにより、ネットワークに関する広範囲にわたる詳細情報を提供している豊富な MIB にアクセスできます。
Root Bridge (ルート ブリッジ)	スパニング ツリー トポロジーを制御するブリッジ。
Root Port (ルート ポート)	このポートはルート ブリッジへの接続 (直接または間接的に) を提供します。
RSTP	ラピッド スパニング ツリー プロトコル。このプロトコルはオリジナルの STP 技術を改良したもので、速い収束時間を提供します。
SNMP	シンプル ネットワーク マネージメント プロトコル。複雑なネットワークの管理に使用されるプロトコル。コンピューターまたは装置がプロトコル データ ユニットを用いて SNMP エージェントのデータを要求します。エージェントは MIB に保管されているデータを返送します (管理情報ベース)。

SNMP Agent (SNMP エージェント)	マネージド スイッチなどの装置の状態を監視するソフトウェアで、状態に関する情報をリクエストに応答する形か、通知の送信によりクライアントに提供します。
Store & Forward (ストア アンド フォワード)	スイッチの標準運転モード
STP	スパニング ツリー プロトコル。このプロトコルは、ブリッジのネットワークでループを防ぐために使用されますが、単一ハードウェア障害の予防手段として冗長接続もできます。
Subnet (サブネット)	サブネットは、IP アドレスの同じ一部分を共有するネットワークの一部分です。セキュリティの観点から、ネットワークはサブネット マスクを使って多くのサブネットに分割することができます。装置のサブネットマスク設定は、サブネット ID を識別するために 2 進数 IP アドレスと組み合わせます。IP ネットワーク上では、同じサブネット ID を持つ装置だけが互いに通信できます。
Telnet	このターミナル エミュレーション プログラムは、Telnet サーバにアクセスするために使用します。Telnet サーバに接続しログインすると、まるでユーザーがサーバのそばにいるかのごとく、コマンドをリモートで実行することができます。
ToS	タイプ オブ サービス。IPv4 ヘッダーのフィールドで、パケット処理の際に要求されるサービスのタイプを指定します。値は 0 から 255 まであります。(CoS と QoS の項も参照のこと)
Traffic Class (トラフィック クラス)	IPv6 ヘッダーのフィールドで、関連するフレームの相対的な優先度を指定します。値は 0 から 255 まであります。
Trap (トラップ)	SNMP エージェントから SNMP トラップ マネージャに送信されるメッセージで、エージェントが監視している装置の状態変化をマネージャに通知します。トラップの例にはコールド スタート (装置の電源を入れる)、認証失敗 (エージェントに接続を試みるときにユーザーが無効の認証情報を提供)、およびリンク アップ リンク ダウン (ポートへの接続が確立または切断) があります。
VLAN	VLAN は、帯域利用またはセキュリティの改善のためスイッチを通るトラフィックを分離します。分離はポートのグループのメンバーシップ (ポートベース VLAN) に基づいて行われるか、VLAN ID を含む IEEE 802.1Q タグ (タグベース VLAN) で行われます。ルーターが介在しない限り、1 つの VLAN 上の装置は他の VLAN 上の装置と交信できません。

付録 F AT コマンド サマリー (-MDM モデルのみ

F.1 AT コマンド

このセクションで定義する AT コマンドは、モデム設定コンフィギュレーション画面でモデムを設定するために入力します。先進アプリケーション向けです。

%C - V.42bis Data Compression (データ圧縮)	n=0 データ圧縮無効 n=1 双方向データ圧縮 n=2 データ圧縮送信のみ n=3 データ圧縮受信のみ
\Nn - Error Control Mode (エラー制御モード)	n=0 通常モード n=2 MNP が必要 n=3 V.42 自動信頼モード * n=4 接続に LAPM が必要 n=5 V.42 または MNP が必要
&Z - Sleep Mode (スリープ モード)	着呼覚醒

F.2 S レジスタ

このセクションで定義する S レジスタは、モデム設定コンフィギュレーション画面でモデムを設定するために入力します。先進アプリケーション向けです。

S0 - Answer on nth Ring
(n 回目の呼出し音で応答):

S0 はモデムを n 回目の呼出し音で自動応答する様に設定します。
S0 を 0 に設定すると自動応答は無効になります。
Range (範囲): 0 ～ 255
Units (単位): Rings (呼出し音)
Default (デフォルト): 0

S1 - Ring Count
(呼出し音回数):

S1 は、検出された呼出し音回数を表示する読み出し専用レジスタです。呼出し音が 8 秒以内に検出されない場合は、S1 はリセットされます。
Range (範囲): 0 ～ 255
Units (単位): Rings (呼出し音)
Default (デフォルト): 0

S6 - Dial Tone Wait Time
(ダイヤル トーン待機時間):

S6 はダイヤルする前にモデムがダイヤル トーンをどの位の時間待機するかを定義します。ダイヤル トーン待機時間は 2 秒 未満に設定できません。
Range (範囲): 0 ～ 255
Units (単位): Seconds (秒)
Default (デフォルト): 2

S7 - Wait for Carrier after Dialing
(ダイヤル後キャリア待機):

S7 は、ダイヤル後にモデムが有効なキャリア信号をどの位の時間待機するかを定義します。
Range (範囲): 0 ～ 255
Units (単位): Seconds (秒)
Default (デフォルト): 80

S8 - Comma Pause Time
(コンマ ポーズ時間):

S8 は、ダイヤル文字中にコンマで生ずるポーズの長さを定義します。ポーズは通常 2 回目のダイヤル トーンを待っているときに使われます。
Range (範囲): 0 ～ 255
Units (単位): Seconds (秒)
Default (デフォルト): 2

S9 - Carrier Detect Response Time
(キャリア検出反応時間):

S9 は有効だと認識されるためにリモート モデムのキャリアが存在しなければならない時間の長さを設定します。
Range (範囲):1 ～ 255
Units (単位): 0.1 Seconds (秒)
Default (デフォルト): 6

S10 - Carrier Off Disconnect Delay (キャリア オフ 切断遅延):

S10 はモデムが接続を切断する前にどのくらいキャリアが失われている必要があるかを選択します。S10 が S9 より小さい、または S10 が 255 に設定されている場合は、モデムはキャリアの喪失で接続を切断しません。

Range (範囲):1 ～ 255
Units (単位): 0.1 Seconds (秒)
Default (デフォルト): 14

S14 - Wait for Dial Tone Delay (ダイヤル トーン 遅延の待機):

S14 は、W ダイヤル修飾子が使われたとき、どのくらいモデムがダイヤルトーンを待つのかを決定します。

Range (範囲): 0 ～ 255
Units (単位): Seconds (秒)
Default (デフォルト): 12

S24 - Sleep Inactivity Timer (スリープ非活動 タイマー):

S24 はモデムがスリープ モードに入る前の非活動時の長さを設定します。0 はスリープ モードを無効にします。

Range (範囲): 0 ～ 255
Units (単位): Seconds (秒)
Default (デフォルト): 0

S30 - Disconnect Inactivity Timer (切断非活動タイマー):

S30 は何のデータも流れていないときに、モデムがどのくらいオンラインを維持するかを設定します。0 はタイマーを無効にします。

Range (範囲): 0 ～ 255
Units (単位): Minutes (分)
Default (デフォルト): 0

S38 - Hang Up Delay Timer (ハング アップ 遅延タイマー):

S38 は、ATH0 コマンドの受信からモデムの接続切断までの間の最大遅延を決定します。

Range (範囲): 0 ～ 255
Units (単位): Seconds (秒)
Default (デフォルト): 20

S50 Minimum Off-Hook Duration (最低オフ フック期間):

S50 はモデムがオフ フックを維持する最低期間を決定します。このタイマーの期限が切れる前に回線を切断しようとしても、モデムに無視されます。

Range (範囲): 0 ～ 255
Units (単位): Seconds (秒)
Default (デフォルト): 3

付録 G サービス情報

Red Lion 製品を問題なくお使いいただけるよう努めておりますが、万が一、アフター サービスが必要な場合は、Red Lion 社の技術サポート 1-877-432-9908 までお電話ください。訓練されたスペシャリストが、すみやかに問題の原因を突き止めるように致します。多くの問題はお電話 1 本で簡単に解決します。当社に返品する必要がある場合は、RMA (障害機器返品確認) 番号をお客様にお伝えします。

Red Lion ではスピーディな対応を保証するため、独自の RMA システムを使用して返品の流れを追跡しています。返品に迅速に対応できるようにするため、梱包の外側に必ずこの RMA 番号を明記してください。

RMA 請求用紙は、電話を受けたアプリケーション エンジニアが記入します。ユニットにシリアル番号が記載されている場合には、詳しい会計情報は必要ありません。シリアル番号が記載されていない場合には、必ずオリジナルの発注番号と購入日をお知らせください。

修理が保証範囲外の場合があるため、修理発注番号もお知らせください。保証の範囲内であれば、修理は無償です。

問題点はできるだけ詳しくお知らせください。お客様からの情報は RMA フォームに記入され、ユニットの到着前に修理担当部署に送られます。こうすることで最善のサービスをできるだけ速やかに提供いたします。通常、修理は 2 日で完了します。問題の解決が困難な場合は、さらに日数を要することがあります。

早い納期をご希望の場合は、当社まで航空便で機器を送ってください。翌日配達で到着した機器に関しましては、優先的にサービスを提供します。午前の中頃 (通常の翌日配達) までに到着したほとんどの修理依頼品は、同日に修理が終了し、すみやかに返送することが可能です。

修理が必要なお客様には、ご不便をおかけして大変申し訳ございません。すみやかに修理サービスを行うよう努めておりますので、ご了承ください。サービス向上につながるご提案などありましたら、お気軽にご連絡ください。お客様のお声に耳を傾け、今後とも、より良いサービスの提供に努めてまいります。

購入情報

必要に応じて参照するため、下の空欄に記入して、このマニュアルをお使いの Red Lion システムとともに保管してください。

発注番号

購入日

購入先

G.1 製品サポート

Sixnet 社製品のサポートは以下で入手できます。

オンライン サポート : http://www.redlion.net　　電話 : 877-432-9908
Fax: (518) 877-8346
最新の製品情報 : http://www.redlion.net　　E メール : support@redlion.net
住所 : Red Lion Controls, 331 Ushers Road, Ballston Lake, NY 12019

付録 H ライセンス契約

下記は、ソフトウェアのライセンス契約およびファームウェアの開発に使用したライブラリのリストです。

この付録に記載のすべてのソフトウェアとライブラリのソースコードを入手するには、Red Lion の support@redlion.net まで E メールでお問い合わせください。

H.1 PCRE ライブラリ

PCRE は、構文と意味が可能な限り Perl 5 言語のものに近い正規表現をサポートする関数のライブラリです。

PCRE のリリース 8 は、下記のとおり「BSD」ライセンスの条件で配布されます。PCRE のドキュメントは「doc」ディレクトリにあり、ソフトウェア本体と同じ条件で配布されます。

基本のライブラリ関数は C 言語で書かれており、フリースタンディングです。また、C++ ラッパー関数のセットも配布に含まれています。

THE BASIC LIBRARY FUNCTIONS (基本のライブラリ関数)

作成者 : Philip Hazel (フィリップ・ヘーゼル)
E メール ローカル パート : ph10
E メール ドメイン : cam.ac.uk

University of Cambridge Computing Service,
Cambridge, England.

THE C++ WRAPPER FUNCTIONS (C++ ラッパ関数)

提供元 : Google Inc.

「BSD」ライセンス

ソースおよびバイナリ形式の再配布および使用は、改変の有無にかかわらず、以下の条件に合うものは許可されています。

- ソースコードの再配布は、前述の著作権表示、本条件一覧および後述の免責事項を残しておかなければなりません。
- バイナリ形式の再配布は、前述の著作権表示、本条件一覧および後述の免責事項を、配布時に提供する文書およびまたはその他の資料内に複製しなければなりません。
- the University of Cambridge の名称または Google Inc. の名称、または貢献者の名前のいずれも、特定の事前の書面による許可なしで、本ソフトウェアから派生した製品の推奨または宣伝に使用することはできません。

本ソフトウェアは、著作権所有者および貢献者によって「現状のまま」提供されており、商品性および特定目的への適合性に関する暗黙の保証などの明示または黙示の保証責任を否認します。著作権所有者または貢献者は、原因のいかんにかかわらず、また責任理論が契約の記述、厳格責任、または不法行為かを問わず (過失その他を含む)、次のような損害の可能性を知らされていたとしても、本ソフトウェアの使用に起因するいかなる直接的、間接的、付随的、特別、懲罰的または派生的損害 (代替商品またはサービスの調達、使用、データまたは利益の損失、あるいは営業中断など) に対して一切責任を負いません。

H.2 libpcap ソフトウェア

ライセンス : BSD

ソースおよびバイナリ形式の再配布および使用は、改変の有無にかかわらず、以下の条件に合うものは許可されています。

1. ソースコードの再配布は、前述の著作権表示、本条件一覧および後述の免責事項を残しておかなければなりません。
2. バイナリ形式の再配布は、前述の著作権表示、本条件一覧および後述の免責事項を配布時に提供する文書およびまたはその他の資料内に複製しなければなりません。
3. 開発者の名前は、特定の事前の書面による許可なしで、本ソフトウェアから派生した製品の推奨または宣伝に使用することはできません。

本ソフトウェアは、「現状のまま」提供されており、商品性および特定目的への適合性に関する暗黙の保証などの明示または黙示の保証はありません。

H.3 lighttpd ソフトウェア

ソースおよびバイナリ形式の再配布および使用は、改変の有無にかかわらず、以下の条件に合うものは許可されています。

- ソースコードの再配布は、前述の著作権表示、本条件一覧および後述の免責事項を残しておかなければなりません。
- バイナリ形式の再配布は、前述の著作権表示、本条件一覧および後述の免責事項を、配布時に提供する文書およびまたはその他の資料内に複製しなければなりません。
- 「増分」の名前または貢献者の名前のいずれも特定の事前の書面による許可なしで、本ソフトウェアから派生した製品の推奨または宣伝に使用することはできません。

本ソフトウェアは、著作権所有者および貢献者によって「現状のまま」提供されており、商品性および特定目的への適合性に関する暗黙の保証などの明示または黙示の保証責任を否認します。著作権所有者または貢献者は、原因のいかんにかかわらず、また責任理論が契約の記述、厳格責任、または不法行為かを問わず (過失その他を含む)、次のような損害の可能性を知らされていたとしても、本ソフトウェアの使用に起因するいかなる直接的、間接的、付随的、特別、懲罰的または派生的損害 (代替商品またはサービスの調達、使用、データまたは利益の損失、あるいは営業中断など) に対して一切責任を負いません。

H.4 spawn-fcgi ソフトウェア

ソースおよびバイナリ形式の再配布および使用は、改変の有無にかかわらず、以下の条件に合うものは許可されています。

- ソースコードの再配布は、前述の著作権表示、本条件一覧および後述の免責事項を残しておかなければなりません。
- バイナリ形式の再配布は、前述の著作権表示、本条件一覧および後述の免責事項を、配布時に提供する文書およびまたはその他の資料内に複製しなければなりません。
- 「増分」の名前または貢献者の名前のいずれも特定の事前の書面による許可なしで、本ソフトウェアから派生した製品の推奨または宣伝に使用することはできません。

本ソフトウェアは、著作権所有者および貢献者によって「現状のまま」提供されており、商品性および特定目的への適合性に関する暗黙の保証などの明示または黙示の保証責任を否認します。著作権所有者または貢献者は、原因のいかんにかかわらず、また責任理論が契約の記述、厳格責任、または不法行為かを問わず (過失その他を含む)、次のような損害の可能性を知らされていたとしても、本ソフトウェアの使用に起因するいかなる直接的、間接的、付随的、特別、懲罰的または派生的損害 (代替商品またはサービスの調達、使用、データまたは利益の損失、あるいは営業中断など) に対して一切責任を負いません。

H.5 ipsec-tools ソフトウェア

これは ipsec ツールのデビアン パッケージ版です。

このパッケージのソースは、こちらのウェブサイトで参照できます。http://ipsec-tools.sourceforge.net/

コードは 1995 年、1996 年、1997 年、1998 年、1999 年に WIDE プロジェクトによって著作権保護されており、BSD ライセンスに基づき許可を受けています。デビアン システムでは、ライセンスのコピーは /usr/share/common-licenses/BSD にあります。

GSSAPI コードは 2000 年に Wasabi Systems, Inc によって著作権保護されており、次のライセンスに基づき許可を受けています。

ソースおよびバイナリ形式の再配布および使用は、改変の有無にかかわらず、以下の条件に合うものは許可されています。

- ソースコードの再配布は、前述の著作権表示、本条件一覧および後述の免責事項を残しておかなければなりません。
- バイナリ形式の再配布は、前述の著作権表示、本条件一覧および後述の免責事項を、配布時に提供する文書およびまたはその他の資料内に複製しなければなりません。
- 本ソフトウェアの機能または使用に言及するすべての宣伝物は、次の承認文を表示しなければなりません。本製品は Zembu Labs, Inc. のために Wasabi Systems が開発したソフトウェアが含まれます。
  http://www.zembu.com/
- Wasabi Systems, Inc の名前を特定の事前の書面による許可なしで、本ソフトウェアから派生した製品の推奨または宣伝に使用することはできません。

本ソフトウェアは、WASABI SYSTEMS, INC. によって「現状のまま」提供されており、商品性および特定目的への適合性に関する暗黙の保証などの明示または黙示の保証責任を否認します。WASABI SYSTEMS, INC. は、原因のいかんにかかわらず、また責任理論が契約の記述、厳格責任、または不法行為かを問わず (過失その他を含む)、次のような損害の可能性を知らされていたとしても、本ソフトウェアの使用に起因するいかなる直接的、間接的、付随的、特別、懲罰的または派生的損害 (代替商品またはサービスの調達、使用、データまたは利益の損失、あるいは営業中断など) に対して一切責任を負いません。

ラクーン ツール perl スクリプトは次のとおりです。

Copyright Matthew Grant, Catalyst IT Ltd 2004

このプログラムはフリー ソフトウェアです。フリー ソフトウェア財団によって公開されており、GNU 一般公衆利用許諾書の条件に基づいて再配布およびまたは改変を行うことができます。1991 年 6 月付バージョン 2。

本プログラムを役立てて欲しいという思いから配布していますが、いかなる保証も、商品性または特定目的への適合性に関する暗黙の保証もありません。詳細は、GNU 一般公衆利用許諾書の条件を参照してください。

デビアン GNU/Linux システムでは、GNU 一般公衆利用許諾書の条件の全文を「/usr/share/common-licenses/GPL」で見ることができます。また、GNU 一般公衆利用許諾書の条件のコピーはこちらで入手可能です。

<URL:http://www.gnu.org/copyleft/gpl.html>

さらに、フリー ソフトウェア財団に、Free Software Foundation, Inc., 51 Franklin St, Fifth Floor, Boston, MA 02110-1301, USA まで書面にて請求も可能です。

H.6 net-snmp ソフトウェア

さまざまな著作権が本パッケージに適用されます。以下にさまざまな別々の部分を記載しました。すべてを読むようにしてください。

---- パート 1: CMU/UCD 著作権表示 : (BSD と類似) -----

Copyright 1989, 1991, 1992 by Carnegie Mellon University
Derivative Work – 1996, 1998-2000
Copyright 1996, 1998-2000 The Regents of the University of California
All Rights Reserved

上記の著作権表示がすべての複製に表示され、その著作権表示と本許可告知が補足文書に表示されており、CMU および The Regents of the University of California の名称が特定の事前の書面による許可なしで、本ソフトウェアから派生した製品の推奨または宣伝に使用しないかぎり、いずれかの理由のために無料で本ソフトウェアおよび文書の使用、複製、改変、および配布することはここに許可されます。

CMU および THE REGENTS OF THE UNIVERSITY OF CALIFORNIA は、本ソフトウェアに関する、商品性および特定目的への適合性に関する暗黙の保証を含むすべての保証責任を否認します。CMU および THE REGENTS OF THE UNIVERSITY OF CALIFORNIA は、本ソフトウェアの使用または性能に関連して起こる契約の行動、過失またはその他の不法行為かどうかにかかわらず、本ソフトウェアの使用に起因するいかなる特別、間接的、または派生的損害あるいは使用、データまたは利益の損失に起因するいかなる損害に対して一切責任を負いません。

---- パート 2: Networks Associates Technology, Inc 著作権表示 (BSD) -----

Copyright (c) 2001-2003,Networks Associates Technology, Inc
All rights reserved.

ソースおよびバイナリ形式の再配布および使用は、改変の有無にかかわらず、以下の条件に合うものは許可されています。

- ソースコードの再配布は、前述の著作権表示、本条件一覧および後述の免責事項を残しておかなければなりません。

- バイナリ形式の再配布は、前述の著作権表示、本条件一覧および後述の免責事項を、配布時に提供する文書およびまたはその他の資料内に複製しなければなりません。

- Networks Associates Technology, Inc の名称、または貢献者の名前のいずれも特定の事前の書面による許可なしで、本ソフトウェアから派生した製品の推奨または宣伝に使用することはできません。

本ソフトウェアは、著作権所有者および貢献者によって「現状のまま」提供されており、商品性および特定目的への適合性に関する暗黙の保証などの明示または黙示の保証責任を否認します。著作権所有者または貢献者は、原因のいかんにかかわらず、また責任理論が契約の記述、厳格責任、または不法行為かを問わず (過失その他を含む)、次のような損害の可能性を知らされていたとしても、本ソフトウェアの使用に起因するいかなる直接的、間接的、付随的、特別、懲罰的または派生的損害 (代替商品またはサービスの調達、使用、データまたは利益の損失、あるいは営業中断など) に対して一切責任を負いません。

---- パート 3: Cambridge Broadband Ltd. 著作権表示 (BSD) -----

Portions of this code are copyright (c) 2001-2003, Cambridge Broadband Ltd.
All rights reserved.

ソースおよびバイナリ形式の再配布および使用は、改変の有無にかかわらず、以下の条件に合うものは許可されています。

- ソースコードの再配布は、前述の著作権表示、本条件一覧および後述の免責事項を残しておかなければなりません。

- バイナリ形式の再配布は、前述の著作権表示、本条件一覧および後述の免責事項を、配布時に提供する文書およびまたはその他の資料内に複製しなければなりません。

- Cambridge Broadband Ltd. の名称を特定の事前の書面による許可なしで、本ソフトウェアから派生した製品の推奨または宣伝に使用することはできません。

本ソフトウェアは、著作権所有者によって「現状のまま」提供されており、商品性および特定目的への適合性に関する暗黙の保証などの明示または黙示の保証責任を否認します。著作権所有者は、原因のいかんにかかわらず、また責任理論が契約の記述、厳格責任、または不法行為かを問わず (過失その他を含む)、次のような損害の可能性を知らされていたとしても、本ソフトウェアの使用に起因するいかなる直接的、間接的、付随的、特別、懲罰的または派生的損害 (代替商品またはサービスの調達、使用、データまたは利益の損失、あるいは営業中断など) に対して一切責任を負いません。

---- パート 4: Sun Microsystems, Inc. 著作権表示 (BSD) -----

Copyright © 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara,
California 95054, U.S.A. All rights reserved.

使用は以下のライセンス規約に従うことになります。

この配布には第三者が開発した資料が含まれることがあります。

Sun、Sun Microsystems、the Sun logo および Solaris は商標、または米国およびその他の国で登録された Sun Microsystems, Inc の登録商標です。

net-snmp ソフトウェア

ソースおよびバイナリ形式の再配布および使用は、改変の有無にかかわらず、以下の条件に合うものは許可されています。

- ソースコードの再配布は、前述の著作権表示、本条件一覧および後述の免責事項を残しておかなければなりません。

- バイナリ形式の再配布は、前述の著作権表示、本条件一覧および後述の免責事項を、配布時に提供する文書およびまたはその他の資料内に複製しなければなりません。

- Sun Microsystems, Inc. の名称または貢献者の名前のいずれも、特定の事前の書面による許可なしで、本ソフトウェアから派生した製品の推奨または宣伝に使用することはできません。

本ソフトウェアは、著作権所有者および貢献者によって「現状のまま」提供されており、商品性および特定目的への適合性に関する暗黙の保証などの明示または黙示の保証責任を否認します。著作権所有者または貢献者は、原因のいかんにかかわらず、また責任理論が契約の記述、厳格責任、または不法行為かを問わず (過失その他を含む)、次のような損害の可能性を知らされていたとしても、本ソフトウェアの使用に起因するいかなる直接的、間接的、付随的、特別、懲罰的または派生的損害 (代替商品またはサービスの調達、使用、データまたは利益の損失、あるいは営業中断など) に対して一切責任を負いません。

---- パート 5: Sparta, Inc 著作権表示 (BSD) -----

Copyright (c) 2003-2009, Sparta, Inc
All rights reserved.

ソースおよびバイナリ形式の再配布および使用は、改変の有無にかかわらず、以下の条件に合うものは許可されています。

- ソースコードの再配布は、前述の著作権表示、本条件一覧および後述の免責事項を残しておかなければなりません。

- バイナリ形式の再配布は、前述の著作権表示、本条件一覧および後述の免責事項を、配布時に提供する文書およびまたはその他の資料内に複製しなければなりません。

- Sparta, Inc の名称または貢献者の名前のいずれも特定の事前の書面による許可なしで、本ソフトウェアから派生した製品の推奨または宣伝に使用することはできません。

本ソフトウェアは、著作権所有者および貢献者によって「現状のまま」提供されており、商品性および特定目的への適合性に関する暗黙の保証などの明示または黙示の保証責任を否認します。著作権所有者または貢献者は、原因のいかんにかかわらず、また責任理論が契約の記述、厳格責任、または不法行為かを問わず (過失その他を含む)、次のような損害の可能性を知らされていたとしても、本ソフトウェアの使用に起因するいかなる直接的、間接的、付随的、特別、懲罰的または派生的損害 (代替商品またはサービスの調達、使用、データまたは利益の損失、あるいは営業中断など) に対して一切責任を負いません。

---- パート 6: Cisco/BUPTNIC 著作権表示 (BSD) -----

Copyright (c) 2004, Cisco, Inc and Information Network
Center of Beijing University of Posts and Telecommunications.
All rights reserved.

ソースおよびバイナリ形式の再配布および使用は、改変の有無にかかわらず、以下の条件に合うものは許可されています。

- ソースコードの再配布は、前述の著作権表示、本条件一覧および後述の免責事項を残しておかなければなりません。
- バイナリ形式の再配布は、前述の著作権表示、本条件一覧および後述の免責事項を、配布時に提供する文書およびまたはその他の資料内に複製しなければなりません。
- Cisco, Inc の名称、Beijing University of Posts and Telecommunications の名称、または貢献者の名前のいずれも、特定の事前の書面による許可なしで、本ソフトウェアから派生した製品の推奨または宣伝に使用することはできません。

本ソフトウェアは、著作権所有者および貢献者によって「現状のまま」提供されており、商品性および特定目的への適合性に関する暗黙の保証などの明示または黙示の保証責任を否認します。著作権所有者または貢献者は、原因のいかんにかかわらず、また責任理論が契約の記述、厳格責任、または不法行為かを問わず (過失その他を含む)、次のような損害の可能性を知らされていたとしても、本ソフトウェアの使用に起因するいかなる直接的、間接的、付随的、特別、懲罰的または派生的損害 (代替商品またはサービスの調達、使用、データまたは利益の損失、あるいは営業中断など) に対して一切責任を負いません。

---- パート 7: Fabasoft R&D Software GmbH & Co KG 著作権表示 (BSD) -----

Copyright (c) Fabasoft R&D Software GmbH & Co KG, 2003
oss@fabasoft.com

開発者 : Bernhard Penz (バーナード・ペンス) bernhard.penz@fabasoft.com

ソースおよびバイナリ形式の再配布および使用は、改変の有無にかかわらず、以下の条件に合うものは許可されています。

- ソースコードの再配布は、前述の著作権表示、本条件一覧および後述の免責事項を残しておかなければなりません。
- バイナリ形式の再配布は、前述の著作権表示、本条件一覧および後述の免責事項を、配布時に提供する文書およびまたはその他の資料内に複製しなければなりません。
- Fabasoft R&D Software GmbH & Co KG の名称、またはその子会社の名称、ブランドまたは製品名は、特定の事前の書面による許可なしで、本ソフトウェアから派生した製品の推奨または宣伝に使用することはできません。

本ソフトウェアは、著作権所有者によって「現状のまま」提供されており、商品性および特定目的への適合性に関する暗黙の保証などの明示または黙示の保証責任を否認します。著作権所有者は、原因のいかんにかかわらず、また責任理論が契約の記述、厳格責任、または不法行為かを問わず (過失その他を含む)、次のような損害の可能性を知らされていたとしても、本ソフトウェアの使用に起因するいかなる直接的、間接的、付随的、特別、懲罰的または派生的損害 (代替商品またはサービスの調達、使用、データまたは利益の損失、あるいは営業中断など) に対して一切責任を負いません。

---- パート 8: Apple Inc. 著作権表示 (BSD) -----

Copyright (c) 2007 Apple Inc. All rights reserved.

ソースおよびバイナリ形式の再配布および使用は、改変の有無にかかわらず、以下の条件に合うものは許可されています。

- ソースコードの再配布は、前述の著作権表示、本条件一覧および後述の免責事項を残しておかなければなりません。
- バイナリ形式の再配布は、前述の著作権表示、本条件一覧および後述の免責事項を、配布時に提供する文書およびまたはその他の資料内に複製しなければなりません。
- Apple Inc. の名称、または貢献者の名前のいずれも、特定の事前の書面による許可なしで、本ソフトウェアから派生した製品の推奨または宣伝に使用することはできません。

本ソフトウェアは、APPLE および貢献者によって「現状のまま」提供されており、商品性および特定目的への適合性に関する暗黙の保証などの明示または黙示の保証責任を否認します。APPLE または貢献者は、原因のいかんにかかわらず、また責任理論が契約の記述、厳格責任、または不法行為かを問わず (過失その他を含む)、次のような損害の可能性を知らされていたとしても、本ソフトウェアの使用に起因するいかなる直接的、間接的、付随的、特別、懲罰的または派生的損害 (代替商品またはサービスの調達、使用、データまたは利益の損失、あるいは営業中断など) に対して一切責任を負いません。

---- パート 9: ScienceLogic, LLC 著作権表示 (BSD) -----

Copyright (c) 2009, ScienceLogic, LLC
All rights reserved.

ソースおよびバイナリ形式の再配布および使用は、改変の有無にかかわらず、以下の条件に合うものは許可されています。

- ソースコードの再配布は、前述の著作権表示、本条件一覧および後述の免責事項を残しておかなければなりません。
- バイナリ形式の再配布は、前述の著作権表示、本条件一覧および後述の免責事項を、配布時に提供する文書およびまたはその他の資料内に複製しなければなりません。
- Science Logic, LLC の名称、または貢献者の名前のいずれも、特定の事前の書面による許可なしで、本ソフトウェアから派生した製品の推奨または宣伝に使用することはできません。

本ソフトウェアは、著作権所有者および貢献者によって「現状のまま」提供されており、商品性および特定目的への適合性に関する暗黙の保証などの明示または黙示の保証責任を否認します。著作権所有者または貢献者は、原因のいかんにかかわらず、また責任理論が契約の記述、厳格責任、または不法行為かを問わず (過失その他を含む)、次のような損害の可能性を知らされていたとしても、本ソフトウェアの使用に起因するいかなる直接的、間接的、付随的、特別、懲罰的または派生的損害 (代替商品またはサービスの調達、使用、データまたは利益の損失、あるいは営業中断など) に対して一切責任を負いません。

H.7 Fast CGI ライブラリ

本 Fast CGI アプリケーション ライブラリのソースおよびオブジェクト コード (以下「本ソフトウェア」とする)、ならびにその文書 (以下「文書」とする) は Open Market, Inc (以下「Open Market」とする) によって著作権保護されています。以下の規定は、個々のファイルで明確に否定されていない限り、本ソフトウェアおよび文書に関連するすべてのファイルに適用されます。

Open Market は、すべての複製物に既存の著作権表示を残し、本表示がいかなる配布物にも一語一句含まれている限り、いかなる目的にでも本ソフトウェアおよび文書の使用、複製、改変、配布およびライセンスを許可します。いずれの正当な使用にも、書面による同意、ライセンスまたは使用料は必要ありません。本ソフトウェアおよび文書の改変は、開発者によって著作権保護されている可能性があり、ここに記載のライセンス規約に従う必要はありません。本ソフトウェアおよび文書の改変に新しいライセンス規約がある場合、新しい規約は、適用される各ファイルの最初のページに明らかに表示されなければなりません。

OPEN MARKET は、本ソフトウェアまたは本文書に関して商品性および特定目的への適合性に関する暗黙の保証などの明示または黙示の保証責任を否認します。OPEN MARKET は、原因のいかんにかかわらず、また責任理論が契約の記述、厳格責任、または不法行為かを問わず (過失その他を含む)、OPEN MARKET が次のような損害の可能性を知らされていたとしても、本ソフトウェアまたは文書に起因するまたは関連するいかなる直接的、特別、または派生的損害あるいはデータまたは利益の損失を含む類似の損害に関して、ユーザーまたはいずれかの第三者に対し一切責任を負いません。本ソフトウェアおよび文書は、「現状のまま」提供されています。OPEN MARKET は、本ソフトウェアまたは文書に起因する契約の記述、不法行為、過失またはその他に責任を負いません。

H.8 ウォッチドッグ ソフトウェア

Copyright (C) 1996-1999 Michael Meskes

ウォッチドッグはフリー ソフトウェアです。フリー ソフトウェア財団によって公開されており、GNU 一般公衆利用許諾書の条件に基づいて再配布およびまたは改変を行うことができます。バージョン 1 または (ユーザーの判断により) それ以降のバージョンです。

ウォッチドッグを役立てて欲しいという思いから配布していますが、いかなる保証も、商品性または特定目的への適合性に関する暗黙の保証もありません。詳細は、GNU 一般公衆利用許諾書の条件を参照してください。

H.9 GPLv2 (一般公衆利用許諾書バージョン 2)

以下のソフトウェアが GPLv2 に基づいて配布されています。

- busybox
- iptables
- quagga and quagga libs
- mgetty
- linux
- dhcpcd

GPLv2 は下記の通りです。

GNU 一般公衆利用許諾書

バージョン 2、1991 年 6 月

はじめに

ソフトウェア向けライセンスの大半は、あなたがそのソフトウェアを共有したり変更したりする自由を奪うように設計されています。対照的に、GNU 一般公衆利用許諾書は、あなたがフリー ソフトウェアを共有したり変更したりする自由を保証すること、ソフトウェアがそのユーザーすべてにとってフリーであることを保証することを目的としています。この一般公衆利用許諾書はフリー ソフトウェア財団のソフトウェアのほとんどに適用されており、また GNU GPL を使用すると決めたフリー ソフトウェア財団以外の作成者による他のプログラムにも適用されています (いくつかのフリー ソフトウェア財団のソフトウェアには、GNU GPL ではなく GNU ライブラリ一般公衆利用許諾書が適用されています)。あなたもまた、ご自分のプログラムに GNU GPL を適用することが可能です。

私たちがフリー ソフトウェアについて語るとき、それは利用の自由について言及しているのであって、価格のことではありません。私たちの一般公衆利用許諾書は、あなたがフリー ソフトウェアの複製物を配布する自由を保証するよう設計されています (希望であればそのサービスに課金することが保証されています)。また、あなたがソース コードを受け取るか、あるいは望めばそれを入手することが可能であるということ、あなたがソフトウェアを変更し、その一部を新たなフリーのプログラムで利用できるということ、そして、以上で述べたようなことが可能だということをあなたが知ることも保証されます。

あなたの権利を守るため、誰かがあなたの有するこれらの権利を否定することや、これらの権利を放棄するよう要求することを禁止するという制限を加える必要があります。あなたがソフトウェアの複製物を配布または改変したりする場合は、この制限によりあなたに特定の責任が発生することになります。

たとえば、あなたがこのようなプログラムの複製物を配布する場合、無償、有償に関わらず、あなたが有する権利を全て受領者に与えなければなりません。また、受領者もソース コードを受け取るか手に入れることができるよう保証しなければなりません。そして、あなたは受領者にこの規約を提示し、受領者が持つ権利を知ることができるようにしなければなりません。

私たちはあなたの権利を二段階の手順で保護します。(1) まずソフトウェアを著作権で保護し、(2) あなたに対して、本ソフトウェアの複製、配布または改変についての法的な許可を与える本許諾書を提示します。

また、各作成者と私たちを保護するため、本フリー ソフトウェアには何の保証も存在しないということを誰もが確実に理解できるようにします。ソフトウェアが他の誰かによって改変され、伝達された場合、その受領者は入手したソフトウェアがオリジナルでは無いこと、他人が引き起こしたいかなる問題もオリジナルの作成者の名声に影響しないということを周知させたいと考えます。

最後に、いずれのフリー プログラムも絶え間なくソフトウェア特許に脅かされています。私たちは、フリー プログラムの再配布者が個々に特許ライセンスを取得し、事実上プログラムをプロプライエタリ的にするという危険を避けたいと考えています。このような事態を予防するために、私たちはいかなる特許も誰もが自由に利用できるようライセンスされるか、まったくライセンスされないかのどちらかでなければならないことを明確にしました。

複製、配布、および改変についての利用条件の詳細は以下の通りです。

GNU 一般公衆利用許諾書

複製、配布、および改変に関する利用条件

0. この利用許諾書は、本一般公衆利用許諾書の条件に基づいて配布することが可能であると定める著作権所有者による表示を含む、いずれかのプログラムまたはその他の著作物に適用します。以下の「プログラム」とは、このようないずれかのプログラムや著作物を指し、また「プログラムを基にした著作物」とはプログラムまたは著作権法の下で派生物と見なされるものを指します。すなわち、プログラムまたはその一部を、逐語的あるいは改変を加えたか、およびまたは他の言語に翻訳された形を含む著作物のことです。(以降は翻訳も「改変」に含めます) 各ライセンシーは「あなた」とします。

複製、配布または改変以外の活動は、本許諾書では取り扱いません。それらはこの本許諾書の対象外です。プログラムを実行する行為に制限はありません。また、そのようなプログラムの出力結果は、その内容がプログラムを基にした著作物を構成する内容の場合のみ本許諾書で取り扱います。(プログラムを実行したことによって作成されたということとは無関係) それが真実かどうかは、プログラムが何をするのかによります。

1. それぞれの本プログラムのソース コードの複製物において適切な著作権表示と保証の否認を目立つよう適切に掲載し、本許諾書およびいかなる保証の不存在に関するすべての表示をそのまま残し、そして本許諾書の複製物を本プログラムのいかなる受領者にも本プログラムと共に配布する限り、あなたは本プログラムのソース コードの逐語的な複製物を、あなたが受け取った通りの形で、いかなる媒体においても複製または配布することができます。

あなたは、物理的に複製物を譲渡するという行為に対して課金することができ、あなたの判断により有償の製品保証を提供することができます。

2. あなたは自分のプログラムの複製物かその一部を改変してプログラムを基にした著作物を形成し、上記第 1 節に定める条件の下でそのような改変や著作物を複製し配布することができますが、以下の条件すべてを満たすことも必要です。

a. あなたがそれらのファイルを変更した事実と変更日時を、改変されたファイルに目立つように表示しなければなりません。

b. 全部または一部に本プログラムまたはその一部を含む著作物、あるいは全部または一部が本プログラムまたはその一部から派生している著作物を配布または公開する場合は、その全体を本許諾書の条件に従い第三者へ利用を無償で許諾しなければなりません。

c. 改変されたプログラムが、通常実行する際に対話的にコマンドを読むようになっている場合、そのプログラムを最も一般的な方法で対話的に実行する際、適切な著作権表示および無保証であること (あるいはあなたが保証を提供するということ)、およびユーザーがプログラムを本許諾書の条件に基づいて配布することができるということ、そして本許諾書の複製物の閲覧方法のユーザーへの説明を含む通知が印刷されるか、あるいは画面に表示されるようにしなければなりません。

以上の必要条件は改変された著作物全体に適用されます。その著作物の認識される部分が本プログラムから派生したものではなく、別の独立した著作物であると合理的に考えられるならば、それらを別の著作物として配布する場合、本許諾書とその条件はこれらの部分に適用されません。しかし、本プログラムを基にした著作物全体の一部として同じ部分を配布するならば、全体としての配布物は、本許諾書が課す条件に従わなければなりません。というのは、本許諾書が他のライセンシーに与える許可はプログラム丸ごと全体に及び、誰が書いたかは関係なく各部分のすべてを保護するからです。

したがって、すべてあなたによって書かれた著作物に対し、権利を主張することやあなたの権利に異議を申し立てることはこの節の意図するところではありません。むしろ、その趣旨は本プログラムを基にした派生物ないし集合著作物の配布を管理する権利を行使するということにあります。

また、本プログラムを基にしていないその他の著作物を本プログラム (または本プログラムを基にした著作物) と一緒に集めただけのものをストレージの 1 ボリュームまたは配布媒体に収めても、その他の著作物まで本許諾書の適用範囲にはなりません。

3. あなたは上記第 1 節および 2 節の条件に従い、本プログラム (または第 2 節における派生物) をオブジェクト コードまたは実行形式で複製および配布することができます。ただし、その場合あなたは以下のうちどれか 1 つを実施しなければなりません。

a. 著作物にプログラムに完全に対応した機械で読み取り可能なソース コードを添付すること。ただし、ソース コードは上記第 1 節および 2 節の条件に従い、ソフトウェアの交換で習慣的に使われる媒体で配布しなければなりません。または、

b. 配布に要する物理的コストを上回らない程度の手数料で、プログラムに完全に対応した機械で読み取り可能なソース コードをいかなる第三者に対しても提供するという、少なくとも 3 年間は有効な書面による申し出を著作物に添付すること。ただし、ソース コードは上記第 1 節および 2 節の条件に従いソフトウェアの交換で習慣的に使われる媒体で配布しなければなりません。または、

c. 対応するソース コード配布の申し出については、あなたが得た情報を著作物に添付すること。(この選択肢は、非営利目的の配布で、あなたが上記小節 b で指定されているような申し出と共にオブジェクト コードあるいは実行形式のプログラムを入手した場合に限り許可されます)

著作物のソース コードとは、それに対して改変を加える上で好ましいとされる著作物の形式を意味します。実行形式の著作物にとっての完全なソース コードとは、それが含むすべてのモジュールのソース コード全部に加え、関連するインターフェイス定義ファイルのいずれかとライブラリのコンパイルやインストールを制御するために使われるスクリプトも加えたものを意味します。しかし特別な例外として、そのコンポーネント自体が実行形式に付随しない限り、配布されるソース コードの中に実行形式が実行されるオペレーティング システムの主要なコンポーネント (コンパイラやカーネルなど) と通常一緒に (ソースまたはバイナリ形式のどちらかで) 配布されるものを含んでいる必要はありません。

実行形式またはオブジェクト コードの配布が、指定された場所からコピーするためのアクセス手段を提供することで成立し、ソース コードも同等のアクセス手段によって同じ場所からコピーできるようになっている場合は、第三者がオブジェクト コードと一緒にソースも強制的にコピーさせられるようになっていなくても、ソース コード配布の条件を満たしているものとします。

4. あなたは、本許諾書において明示された場合を除き、本プログラムを複製や改変、サブライセンス、または配布してはいけません。本プログラムを複製や改変、サブライセンス、または配布する試みはいずれも無効であり、本許諾書に基づいてあなたの権利は自動的に終了することになります。しかし、複製物や権利を本許諾書に従ってあなたから得た当事者に関しては、そのような人々が本許諾書に完全に従っている限り彼らのライセンスは終了しません。

5. あなたは本許諾書に署名していないため、これを受諾する必要はありません。しかし、本許諾書以外に、あなたに対して本プログラムやその派生物を改変または配布する許可を与えるものは存在しません。これらの行為は、あなたが本許諾書を受け入れない限り、法によって禁じられています。従って、本プログラム (あるいは本プログラムを基にした著作物) を改変または配布することにより、あなたは自分がそのような行為を行うために本許諾書を受諾したということ、そして本プログラムとそれに基づく著作物の複製、配布または改変について本許諾書が課す条件をすべて受け入れたということを示したものと見なします。

6. あなたが本プログラム (または本プログラムを基にしたいずれかの著作物) を再配布するたびに、その受領者は元々のライセンサーから、本許諾書の条件の下で本プログラムを複製、配布または改変する許可を自動的に得ます。あなたは、受領者がここで認められた権利を行使することに関してこれ以上他のいかなる制限も課してはいけません。あなたには、第三者が本許諾書に従うことを強制する責任はありません。

7. 特許侵害あるいはその他の理由 (特許関係に限らない) から、裁判所の判決あるいは申し立ての結果としてあなたに (裁判所命令や契約などにより) 本許諾書の条件と矛盾する制約が課された場合でも、あなたが本許諾書の条件を免除されるわけではありません。もし本許諾書の下であなたに課せられた義務と他の関連する義務を同時に満たすような形で配布できないならば、結果としてあなたは本プログラムを配布することは一切できません。たとえば、特許ライセンスが、あなたから直接または間接的を問わず複製物を受け取った人が皆、本プログラムを無償で再配布することを認めていない場合、あなたがその制約と本許諾書を両方とも満たすには本プログラムの配布を完全に中止するしかありません。

この節の一部分が特定の状況の下で無効ないし実施不可能な場合でも、節の残りの部分は適用されるよう意図されており、その他の状況では、節が全体として適用されるよう意図されています。

特許の侵害やその他の所有権の請求をしたり、そのような請求の正当性に異議を唱えたりするよう、あなたを誘導することがこの節の目的ではありません。この節には、公有使用許諾として実現されてきたフリーソフトウェア配布システムの完全性を守る、という目的しかありません。多くの人々が、フリー ソフトウェアの配布システムが整合的に適用されるという信頼の下、このシステムを通じて配布される多様なソフトウェアに寛大な貢献をしてきましたが、どのようなシステムを通じてソフトウェアの配布を希望するかはあくまでも作成者または寄与者次第であり、ライセンシーが選択を押しつけることはできません。

この節は、本許諾書のこの節以外の部分の結果になると考えられるものを徹底的に明らかにすることを目的としています。

8. 本プログラムの配布およびまたは利用が、特定の国において特許または著作権で保護されているインターフェイスのいずれかによって制限されている場合、本プログラムに本許諾書を適用した元の著作権所有者は、それらの国を除外した明確な地理的配布制限を加え、そこで除外されていない国において、またはそれらの国の間でのみ配布が許可されるようにしても構いません。その場合、そのような制限は本許諾書本文で書かれているのと同様に見なされます。

9. フリー ソフトウェア財団は、随時改訂およびまたは新版の一般公衆利用許諾書を公開することができます。そのような新版は既存のバージョンとその精神においては似たものになりますが、新たな問題や懸念に対処するため細部では異なる可能性があります。

それぞれのバージョンには、識別のためのバージョン番号が振られています。本プログラムが適用する本許諾書のバージョン番号を指定し、更に「それ以降のいかなるバージョン (any later version)」にも適用する場合、あなたは次の条件を選択肢として、指定のバージョンか、フリー ソフトウェア財団によって発行された指定のバージョン以降の版のどれか 1 つのどちらかを選ぶことができます。本プログラムが本許諾書のバージョン番号が指定しない場合は、今までにフリー ソフトウェア財団から発行されたバージョンの中から任意で選ぶことが可能です。

10. もしあなたが本プログラムの一部を、本許諾書と異なる配布条件の他のフリー プログラムとの統合を希望する場合は、作成者に許可を求めてください。フリー ソフトウェア財団が著作権で保護するソフトウェアについては、フリー ソフトウェア財団に連絡してください。このような場合のために、特例を設けることもあります。私たちが決定を下すにあたり、私たちのフリー ソフトウェアの派生物すべてがフリーな状態に保たれるということと、一般的にソフトウェアの共有と再利用を促進するという二つの目標を規準に検討します。

無保証

11. 本プログラムは無償で利用が許諾されるので、適用法が認める限りにおいて、本プログラムのための保証は存在しません。書面により言明されている場合を除き、著作権所有者およびまたはその他の当事者は、本プログラムを「現状のまま」提供しており、商品性および特定目的への適合性に関する暗黙の保証などの明示または黙示の一切の保証はありません。本プログラムの質と性能に関するリスクのすべてはあなたに帰属します。本プログラムに欠陥があると判明した場合、必要な保守点検や補修、修正に要する経費はあなたが負います。

12. 適用法によって命じられるか書面での同意がない限り、著作権所有者または上記で許可されている通りに本プログラムを改変およびまたは再配布したその他の当事者は、あなたに対してプログラムの使用または使用不能によって生じた通常、特別、付随的、または派生的損害 (データの損失またはデータの不正確なレンダリング、もしくはあなたまたは第三者が被った損失、もしくは本プログラムが他のソフトウェアと一緒に動作しないという不具合など) に一切責任を負いません。そのような損害が生ずる可能性について、著作権所有者またはその他の当事者が忠告されていたとしても同様です。

条件は以上

あなたの新しいプログラムへの上記条件の適用方法

あなたが新しいプログラムを開発し、公衆によってそれが利用される可能性を最大にしたい場合、そのプログラムを本許諾書の条件に従って、誰でも再配布または変更できるようフリー ソフトウェアにするのが最善です。

そのためには、当該プログラムに以下のような表示を添付してください。その場合、保証が排除されているということを最も効果的に伝えるために、それぞれのソース ファイルの冒頭に表示を添付するのが最も安全です。少なくとも「著作権」の行、および表示全文がある場所へのポインタを各ファイルに含めてください。

> < この 1 行にプログラム名と簡単な説明を記入 >
> Copyright (C) < 西暦年 > < 作成者名 >
>
> このプログラムはフリー ソフトウェアです。フリー ソフトウェア財団によって公開されており、GNU 一般公衆利用許諾書の条件に基づいて再配布およびまたは改変を行うことができます。本許諾書はバージョン 2 または (あなたの判断で) それ以降のバージョンのいずれかです。
>
> 本プログラムを役立てて欲しいという思いから配布していますが、いかなる保証も、商品性または特定目的への適合性に関する暗黙の保証もありません。詳細は、GNU 一般公衆利用許諾書の条件を参照してください。
>
> あなたは、本プログラムと共に GNU 一般公衆利用許諾書の複製を受領しているはずです。そうでない場合は、フリー ソフトウェア財団まで書面にて問い合わせてください。

E メールまたは郵便であなたに連絡する方法についての情報も記載します。

プログラムが対話的な場合、対話モードで起動した際に、次のような短い告知を出力するようにしてください。

> Crossbrowser/x-tools Library Gnomovision version 69, Copyright (C) year name of author Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'. This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

この仮想コマンド「show w」と「show c」は、一般公衆利用許諾書の適切な部分を表示しなければなりません。もちろん、あなたが使うコマンドは「show w」や「show c」以外の呼び名にできるので、マウスのクリックやメニューのアイテムなどあなたのプログラムに合うものにしても構いません。

また、必要ならば (プログラマーとして働いている場合) あなたの雇用主、または学校にそのプログラムに関する「著作権放棄声明 (copyright disclaimer)」に署名してもらうべきです。以下は例ですので、名前を変えてください。

> Yoyodyne, Inc., hereby disclaims all copyright interest in the program `Gnomovision' (which makes passes at compilers) written by James Hacker.
>
> <signature of Ty Coon>, 1 April 1989
> Ty Coon, President of Vice

この一般公衆利用許諾書は、あなたのプログラムをプロプライエタリ プログラムに統合することを認めていません。あなたのプログラムがサブルーチン ライブラリの場合、プロプライエタリ アプリケーションとあなたのライブラリをリンクすることを許可したほうがさらに便利であることがあります。それを希望する場合は、本許諾書の代わりに GNU ライブラリ一般公衆利用許諾書を使用してください。

H.10 クロスブラウザ /x-tools ライブラリ

クロスブラウザ /x-tools ライブラリは、GNU 一般公衆利用許諾書バージョン 3 および GNU 劣等一般公衆利用許諾書バージョン 3 に基づいて配布されます。

許諾書は下記の通りです。

GNU 一般公衆利用許諾書

バージョン 3、2007 年 6 月 29 日

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/> 本使用許諾書の逐語的な複製を複製し、配布することは誰にでも認められていますが、改変は許可されていません。

はじめに

GNU 一般公衆利用許諾書は、ソフトウェアおよびその他の著作物について、フリーかつコピーレフトを主張するライセンスです。

ソフトウェア向けおよびその他の実用的な著作物向けのライセンスの大半は、あなたが著作物を共有したり変更したりする自由を奪うように設計されています。対照的に、GNU 一般公衆利用許諾書は、あなたがプログラムの全てのバージョンを共有したり変更したりする自由を保証すること、ソフトウェアがそのユーザーすべてにとってフリーであり続けることを保証することを目的としています。私たちフリー ソフトウェア財団は、ほとんどの私たちのソフトウェアに GNU 一般公衆利用許諾書を使用しています。他の著作物についても、作成者が同様の方法で著作物を公開するのであれば、GNU 一般公衆利用許諾書を適用することが可能です。あなたもまた、ご自分のプログラムに GNU GPL を適用することが可能です。

私たちがフリー ソフトウェアについて語るとき、それは利用の自由について言及しているのであって、価格のことではありません。私たちの一般公衆利用許諾書は、あなたがフリー ソフトウェアの複製物を配布する自由を保証するよう設計されています (希望であればそのサービスに課金することが保証されています) また、あなたがソース コードを受け取るか、あるいは望めばそれを入手することが可能であるということ、あなたがソフトウェアを変更し、その一部を新たなフリーのプログラムで利用できるということ、そして、以上で述べたようなことが可能だということをあなたが知ることも保証されます。

あなたの権利を守るため、誰かがあなたの有するこれらの権利を否定することや、これらの権利を放棄するよう要求することを防ぐ必要があります。したがって、あなたがソフトウェアの複製物を配布または改変したりする場合は、あなたに責任があります。他者の自由を尊重するという責任です。

たとえば、あなたがこのようなプログラムの複製物を配布する場合、無償、有償に関わらず、あなたが保有する同じ自由を受領者に与えなければなりません。また、受領者もソース コードを受け取るか手に入れることができるよう保証しなければなりません。そして、あなたは受領者にこの規約を提示し、受領者が持つ権利を知ることができるようにしなければなりません。

GNU GPL を使用する開発者はあなたの権利を二段階の手順で保護します。(1) まずソフトウェアに対する著作権を主張し、(2) あなたに対して、本ソフトウェアの複製、配布または改変についての法的な許可を与える本許諾書を提示します。

開発者と作成者を保護するため、GPL は、本フリー ソフトウェアには何の保証も存在しないということを明確にしています。ユーザーと作成者両方の便宜のため、GPL は、改変されたバージョンには改変された旨を表記するよう要求しており、これにより改変されたバージョンの問題が、以前のバージョンの作成者に起因すると誤解されることがないようにしています。

一部の機器では、内蔵されているソフトウェアを改変してインストールまたは実行することがメーカーには可能でも、ユーザーには不可能なように設計されています。これはユーザーがソフトウェアを改変できる自由を守るという GPL の目的と根本的に相容れません。このような悪用の体系的なパターンは個人向け製品の分野で起こりますが、まさにそれを最も容認しがたい分野です。したがって、私たちは GPL の本バージョンで、そうした製品について上記の行為を禁止するようにしました。同種の問題が他の領域にまで相当程度拡大してきた場合は、ユーザーの自由を守る必要があるため、GPL の将来のバージョンにおいてこの規定をそうした領域にも拡張すべく準備を整えています。

最後に、プログラムはどれも絶え間なくソフトウェア特許に脅かされています。国家は、特許が汎用コンピューターにおけるソフトウェアの開発と利用を制限することを認めるべきではありません。しかし、そういったことを認めてしまっている国では特許がフリーなプログラムに適用され、実質的にプログラムがプロプライエタリにされてしまうという特別な脅威を避けたいと思います。こうした事態を防ぐために GPL では、プログラムを非フリーなものにするために特許を用いることはできない、ということを保証しています。

複製、配布、および改変についての利用条件の詳細は以下の通りです。

条件

0. 定義

「本許諾書」とは、GNU 一般公衆利用許諾書バージョン 3 を指します。

「著作権」とは、半導体マスクのようなその他の著作物に適用される著作権に類似した法も意味します。

「本プログラム」とは、本許諾書に基づき許諾された著作権保護が可能な著作物を意味します。各ライセンシーは「あなた」という。「ライセンシー」および「受領者」は、個人でも組織でも構いません。

著作物を「改変」するとは、正確な複製物を作成すること以外で、著作権の許可を必要とする方法で著作物の全部または一部を複製または適用することを意味します。その結果生まれる著作物は、以前の著作物の「改変バージョン」、または以前の著作物に「基づく」著作物と呼ばれます。

「対象著作物」とは、未改変の本プログラムまたは本プログラムに基づく著作物を意味します。

著作物を「プロパゲート」するとは、許可なく著作物に何かをすることで、適用する著作権法に基づく直接または二次的侵害の責任をあなたに負わせることです。コンピューターによる実行または個人的複製物の改変は除きます。プロパゲートには、複製、配布 (改変の有無を問わず)、公衆が利用できるようにすること、およびいくつかの国においてはその他の行為も含まれます。

著作物を「コンベイ」するとは、他方当事者が複製品を作成または受領することができるようにするあらゆる種類のプロパゲートを意味します。コンピュータ ネットワークを通じたユーザーとの単なる交流、複製品の移動なしの交流はコンベイではありません。

対話的なユーザー インターフェイスが「適切な法的通知」を表示する場合、当該インターフェイスは (1) 適切な著作権表示を表示し、(2) ユーザーに対して、著作物に関して何の保証もないこと (別途保証が提供されている場合は除く)、ライセンシーは本許諾書に基づいて著作物をコンベイできるということ、および本許諾書の複製の参照方法などの便利で顕著な目立つ機能を含みます。当該インターフェイスがメニューのようなユーザー コマンドやオプションの一覧を表示する場合、一覧の明確な項目はこの基準を満たします。

1. ソース コード

「著作物」のソース コードとは、著作物を改変するための著作物の好ましい形を意味します。「オブジェクト コード」とは、著作物のソース形式以外のすべてを意味します。

「標準インターフェイス」とは、認知された標準化団体にとって定義された公式規格のインターフェイス、または特定のプログラミング言語のために指定されたインターフェイスの場合、その言語を使用している開発者たちに広く使われているものを意味します。

実行可能な著作物の「システム ライブラリ」とは、著作物全体以外は何でも含みます。(a) 主要コンポーネントのパッケージの通常形式に含まれるが、主要コンポーネントの一部ではないもの、ならびに (b) 主要コンポーネントと一緒に著作物の利用を可能にすることだけに役立つもの、またはソース コード形式で公衆が利用可能な実装のための標準インターフェイスを実現するものです。本文書内の「主要コンポーネント」とは、実行可能な著作物を実行する (もしあれば) 特定のオペレーティング システムの主要な必須コンポーネント (kernel、window システムなど)、または著作物を作成するために使用されるコンパイラ、または著作物を実行するために使用されるオブジェクト コード インタプリタを意味します。

オブジェクト コード形式の著作物の「対応ソース」とは、オブジェクト コードの生成、インストール、および (実行可能な著作物には) 実行を必要とし、これらのアクティビティを制御するスクリプトを含む著作物を改変するすべてのソース コードを意味します。しかし、これには著作物のシステム ライブラリ、または汎用ツール、またはこれらのアクティビティの遂行を改変しないために使用されるが著作物の一部ではない一般的に利用できるフリー プログラムは含まれません。たとえば、対応ソースには著作物のソース ファイルに関連するインターフェイス定義ファイル、ならびに共有ライブラリのソース コード、および詳細データ通信またはサブプログラムと著作物のその他の部分の間の制御フローによるような、著作物が特に要求するように設計された動的にリンクしたサブプログラムが含まれます。

対応ソースは、ユーザーが対応ソースの他の部分から自動的に再生成するいかなるものも含む必要はありません。

ソース コード形式の著作物の対応ソースは同じ作業です。

2. 基本的な許可

本許諾書に基づいて許諾されたすべての権利は、本プログラムの著作権の条件に許可を与え、前述の条件を満たす限り取消不能です。本許諾書は、未改変のプログラムを実行するためのあなたの無条件の許可を明示的に確認します。実行中の対象著作物の出力は、その出力がそのコンテンツを与えられ、対象著作物を構成する場合、本許諾書で保証されます。本許諾書は、著作権法に規定されている通り、公正な使用のあなたの権利またはその他の同様の権利に同意します。

あなたのライセンスが有効である限り無条件で、譲渡しない対象著作物の作成、実行およびプロパゲートが可能です。あなたのためだけに改変を行うという唯一の目的のため、またはあなたが制御できない著作権のすべての製品を譲渡する本許諾書の条件にあなたが従う限り、実行中のこれら著作物の機能をあなたに提供するため、他者へ対象著作物の譲渡が可能です。したがって、あなたにとって対象著作物の作成または実行は、あなたの指示および制御の下、あなたとの関係以外であなたの著作権に保護されている物質のあらゆる複製物の作製を禁止する条件に基づき、あなたのためだけに行わなければなりません。

その他の状況下での譲渡は、下記の条件に従う限り許可されています。サブライセンスは認められていません。第 10 節がサブライセンスを不必要にします。

3. 迂回防止法からのユーザーの法的権利の保護

いかなる対象著作物も、1996 年 12 月 20 日採択の WIPO 著作権条約第 11 条の定める義務を充足する準拠法、またはその措置の迂回の禁止や制限を定めるそれに類する法における、効果的な技術手段の一部と見なされません。

対象著作物をコンベイするとき、対象著作物に関して本許諾書に基づく権利の行使に影響を与えるこのような迂回に関して、あなたは技術手段の迂回を禁止するいかなる法的権限も放棄します。また、当該著作物のユーザー、あなたまたは第三者の技術手段の迂回を禁止する法的権利に対して強制する手段として、当該著作物の操作または改変を制限する意思を放棄します。

4. 逐語的複製物のコンベイ

それぞれのプログラムのソース コードの複製物に適切な著作権表示を目立つよう適切に掲載し、本許諾書の主張、およびコードに適用される第 7 節に合わせて追加されたいかなる非許容の条件に関するすべての表示をそのまま残し、いかなる保証の不存在に関するすべての表示をそのまま残し、そして本許諾書の複製物をすべての受領者にプログラムと共に配布する限り、あなたはプログラムのソース コードの逐語的な複製物をあなたが受け取った通りの形で、いかなる媒体においてもコンベイすることができます。

あなたはコンベイするそれぞれの複製物を有償にすることも無償にすることもでき、有償のサポートおよび製品保証を提供することもできます。

5. 改変済みソース バージョンのコンベイ

次の条件すべてを満たす限り、第 4 節の条件の下、ソース コード形式で本プログラムに基づく著作物をコンベイすること、または本プログラムから著作物を作り出すための改変が可能です。

a. 当該著作物は、あなたがそれを改変したことを示す目立つ表示、および関連する日付を記載しなければなりません。

b. 当該著作物は、本許諾書および第 7 節に基づき追加されたあらゆる条件に基づいてリリースされていることを示す目立つ表示を記載しなければなりません。この要件は第 4 節の「すべての表示をそのまま残す」要件を修正します。

c. あなたは本許諾書に基づき、複製物を所有する誰に対しても、著作物全体の完全な使用を許可しなければなりません。したがって、どのようにパッケージされていても著作物全体、およびそのすべての部分にいずれかの適用される第 7　節の追加条項とともに、本許諾書が適用されます。本許諾書は、その他の方法での著作物の許諾を認めませんが、あなたが別に受領した場合は、このような許可は無効ではありません。

d. 著作物にインタラクティブ ユーザー インターフェイスがある場合は、それぞれ適切な法定通知を表示しなければなりません。しかし、本プログラムにインタラクティブ インターフェイスがあり、適切な法定通知が表示されない場合は、あなたの著作物は表示する必要はありません。

ストレージのボリューム内またはその上、もしくは配布媒体に、本質的に対象著作物の拡張ではなく、さらに大きなプログラムを形成するために組み合わせているわけでもない、他の分離独立した著作物と対象著作物の編集物は、編集物およびその結果としての著作権が、個々の著作物の許諾範囲を超えて編集物のユーザーのアクセス制限または法的権力に使用されない場合、「集積物」と呼ばれます。集積物に対象著作物を含めても、集積物のその他の部分に本許諾書を適用することはありません。

6. 非ソース形式のコンベイ

本許諾書の条件の次のうちの 1 つに基づいて機械で読み取り可能な対応ソースもコンベイする限り、第 4 節および第 5 節の条件に基づき、オブジェクト コード形式の対象著作物をコンベイすることができます。

a. オブジェクト コードを物理的製品 (物理的分配媒体を含む) に入れ、または組み込み、通例としてソフトウェア交換に使用される耐久性のある物理的媒体に固定した対応ソースと共にコンベイする。

b. オブジェクト コードを物理的製品 (物理的分配媒体を含む) に入れ、または組み込み、あなたが当該の製品モデルに対し、スペア部品または顧客サービスをを提供し続ける限り、少なくとも 3 年間は有効な書面による申し出を添付してコンベイする。オブジェクト コードを所有する誰かのために、(1) このソースのコンベイに要する物理的コストを上回らない程度の手数料で、本許諾書で保証される製品に搭載のすべてのソフトウェアの対応ソースの複製物、またはソフトウェア交換に使用される耐久性のある物理的媒体を供与する、または (2) ネットワーク サーバから対応ソースを複製するためのアクセスを無料で供与します。

c. 対応ソースを提供する書面による申し出の複製物を添付したオブジェクト コードの個別複製物をコンベイします。この選択肢は、適時および非営利目的でのみ許可され、第 6b 節に従ってあなたがこのような申し出を添付したオブジェクト コードを受領した場合に限ります。

d. (無料または有料で) 指定場所からアクセスする申し出、および追加料金なしで同じ場所を通じて同じ方法で対応ソースに同様のアクセスをする申し出により、オブジェクト コードをコンベイします。受領者にオブジェクト コードと共に対応ソースを複製させる必要はありません。オブジェクト コードを複製する場所がネットワーク サーバの場合、あなたが次のオブジェクト コードに、どこで対応ソースを発見するかの明白な支持を出し続ける限り、対応ソースを同様の複製設備をサポートする異なるサーバ上 (あなたまたは第三者によって運営されている) に置くことができます。どのサーバが対応ソースをホストするかに関わらず、あなたはこれらの要件を満たすために必要な限り、それが確実に利用可能であるようにする義務を負います。

e. サブセクション 6d に基づき、無料で著作物のオブジェクト コードと対応ソースが公衆に提供される場所を他のピアに連絡する限り、ピア ツー ピア伝送を使用してオブジェクト コードをコンベイします。

システム ライブラリとして対応ソースから除外されているソース コードを持つオブジェクト コードの分離部分は、オブジェクト コードの著作物のコンベイに含む必要はありません。

「ユーザー製品」は、(1) 通常、個人、家族、または家庭用に使用されるいずれかの有形の個人財産を意味する「消費財」または (2) 住居に取り込むために設計または販売されている物のいずれかです。製品が消費財かどうかを決定するには、疑問のあるケースは補償のためにも解決しておくべきです。特定のユーザーが受領した特定の製品のために、その特定のユーザーのステータス、または特定のユーザーの実際の使用方法、または当該製品の使用を期待するまたは期待されるにかかわらず、「通常の使用」とは典型的または一般的な分類の製品の使用方法です。製品は、当該製品が実質的に商業用、工業用、または非消費財に関わらず、そのような使用が当該製品の使用方法の唯一の重要なモードでない限り消費財です。

ユーザー製品のための「インストール情報」とは、いかなる方法、手順、認証キー、または対応ソースの改変バージョンからユーザー製品の対象著作物の改変バージョンをインストールして実行する必要のあるその他の情報を意味します。その情報は、改変したオブジェクト コードの継続する機能が、改変が行われたためだけに、決して妨害または邪魔をされないことを確実にするために十分でなければなりません。

このセクションに基づいて、オブジェクト コードの著作物をユーザー製品にコンベイする場合、またはユーザー製品と共にコンベイする場合、または特にユーザー製品で使用するためにコンベイする場合、ユーザー製品の所有権および使用権を永久または一定期間受領者に譲渡する取引の一環として行われる場合 (取引がどのように特徴づけられるとしても)、このセクションに基づいてコンベイされた対応ソースは、インストール情報を添付しなければなりません。しかしこの要件は、あなたもしくは第三者のいずれも、ユーザー製品に改変したオブジェクト コードをインストールする能力を持たない場合は適用されません。(たとえば、著作物が ROM にインストールされている場合)

提供するインストール情報の要件には、受領者によって改変またはインストールされた著作物、または改変またはインストールされていたユーザー製品への継続的なサポート サービスの提供、保証または更新は含まれません。改変自体がネットワークの運用に著しく悪影響を与える、またはネットワーク全体の通信ルールおよびプロトコルを無視するときは、ネットワークへのアクセスを拒否することができます。

このセクションに従って対応ソースがコンベイされ、インストール情報が提供されるには、公開文書化され (およびソースコード形式で公衆が実装可能な)、解凍、読み出し、または複製に特別なパスワードやキーを必要としない形式でなければなりません。

7. 追加条項

「追加的許可」とは、1 つ以上の条件から例外を認めて、本許諾書の条項を補足する条項です。追加の許可はプログラム全体に適用可能で、適用法の下でそれが有効な限り、本許諾書に含まれているように扱わなければなりません。追加の許可が本プログラムの一部にのみ適用される場合は、その部分はこれらの許可に基づき別に使用できますが、追加的許可には関係なく、プログラム全体は本許諾書に準拠のままです。

対象著作物の複製物をコンベイするときは、あなたの判断でいかなる追加的許可も、その複製物またはそのいずれかの部分から削除することができます。(あなたが著作物を改変するときに特定の事例において追加的許可を削除できるよう、書かれていることがあります) あなたが適切な著作権の許可を持つまた許諾できる、あなたが対象著作物に追加した部分に追加的許可を定めることができます。

本許諾書の他の条項に関わらず、あなたが対象著作物に追加した部分について、(その材料の著作権所有者に承認されている場合) 本許諾書の条件を次の条項で補足できます。

a. 本許諾書の第 15 節および第 16 節の条件とは異なる保証の放棄または責任の制限。または

b. 追加した部分の特定の合理的な法定通知、または作成者の帰属、もしくは追加部分を含む著作物に表示された適切な法定通知の維持を要求すること。または

c. 追加部分の起源の不当表示の禁止、または追加部分の改変バージョンに適切な方法でオリジナル バージョンと異なることを表示するよう要求すること。または

d. 当該部分のライセンサーまたは作成者の名前を宣伝目的で使用することを制限。または

e. いくつかの商標名、商標またはサービスマークの使用における商標法に基づく権利の許諾の拒否。または

f. 当該部分 (またはその改変バージョン) をコンベイするいずれかの者が受領者に対する契約上の責任を負う場合、ライセンサーおよびその部分の作成者に直接席に課されるいずれかの責任の免責を要求すること。

他のすべての許可されていない追加条項は、セクション 10 の意義の範囲内で「さらなる制限」とみなされます。あなたが受領したとおりの本プログラム、またはそのいずれかの部分が、さらなる制限の条件と共に本許諾書に準拠しているとする表示を含む場合、あなたはその条件を削除できます。さらなる制限を含むライセンス文書が、本許諾書に基づく再ライセンスまたはコンベイを許可する場合、さらなる制限がそのような再ライセンスやコンベイに存続しない限り、あなたはそのライセンス文書の条件に準拠する部分を対象著作物に追加できます。

あなたがこのセクションに従って対象著作物に条件を追加する場合、関連ソース ファイルに、これらのファイルに対して追加条項が適用されるという文、または適用条項がどこで発見できるかを示す告知を表示しなければなりません。

追加条項、許可的であっても非許可的であっても、別の書面による許諾の形式、または例外として言及されることがあります。前述の要件はいずれの方法にも適用されます。

8. 終了

本許諾書に基づいて明示的に提供される場合を除き、対象著作物をプロパゲートまたは改変できません。プロパゲートまたは改変のいずれの試みも無効であり、自動的に本許諾書に基づくあなたの権利は終了します。(第 11 節の第 3 パラグラフに基づいて許諾されたいずれかの特許ライセンスを含む)

しかし、本許諾書に違反するすべてが中止された場合、特定の著作権保有者から供与されたあなたのライセンスは (a) その著作権保有者が、明示的かつ最終的にあなたのライセンスを終了するまで暫定的に回復し、(b) 違反行為中止後、合理的手段により 60 日より前に、その著作権保有者が違反をあなたに通知できない場合、永久的に回復します。

さらに、特定の著作権保有者が、合理的手段により違反をあなたに通知し、その著作権保有者から本許諾書の違反 (いかなる著作物に対する) 通知を受け取ったのが初めてで、その通知を受領した後 30 日より前に違反を解決する場合、特定の著作権保有者から供与されたあなたのライセンスは永久的に回復します。

このセクションに基づくあなたの権利の終了は、複製物や権利を本許諾書に基づいてあなたから受領した当事者のライセンスを終了しません。あなたの権利が終了していて、永久的に回復しない場合、あなたに第 10 節に基づいて同じ部分の新しいライセンスを受け取る資格はありません。

9. 複製物の所有に関する承諾の不要

本プログラムの複製物を受領または実行するために、本許諾書を承認する必要はありません。ピア ツー ピア伝送を使用して複製物を受領する結果としてのみ発生する対象著作物の付随的プロパゲートも、同様に承認を必要としません。しかし本許諾以外の何も、あなたに対象著作物のプロパゲートまたは改変許可を許諾しません。あなたが本許諾書を承認しない場合、これらの行為は著作権を侵害します。したがって、対象著作物の改変またはプロパゲートにより、あなたはあなたが本許諾書を承認することを示したことになります。

10. ダウンストリーム受領者への自動的な許諾

あなたが対象著作物をコンベイするたび、受領者は、オリジナル ライセンサーから自動的に本許諾書に従って著作物を実行、改変、およびプロパゲートするためのライセンスを受領します。あなたに本許諾書を第三者に従うよう強制する責任はありません。

「エンティティの取引」とは、ある組織の事業譲渡、またはそれの実質上すべての資産、または組織の細分化、または組織の合併に関する取引です。対象著作物のプロパゲートがエンティティの取引に起因する場合、当該著作物の複製物を受領したその取引の各当事者は、その前任者が従前のパラグラフに基づいて所有した、または所有し得た当該著作物のどのようなライセンスも受領します。またその前任者が当該著作物の対応ソースを所有している、または合理的な努力によってそれを得られる場合、利害関係のある前任者から当該著作物の対応ソースを所有する権利を引き継ぎます。

本許諾書に基づき、許諾または認められた権利の行使に対し、さらなる制限を課すことはできません。たとえば、ライセンス料、使用料、またはその他の本許諾書に基づいて許諾された権利の行使に対する課金を強制することはできません。また、本プログラムまたはそのいずれかの部分を作成、使用、販売、販売の申し出または輸入することにより、いずれかの特許請求が侵害されていると主張して訴訟 (交差請求および反訴を含む) を先導することはできません。

11. 特許

「貢献者」は、本プログラム、または本プログラムに基づく著作物の本許諾書の下で使用を認める著作権保有者です。このように許諾された当該著作物は、貢献者の「貢献者バージョン」と呼ばれます。

貢献者の「必須特許請求」は、すでに取得済み、または今後取得する見込みで、本許諾書で認められたその貢献者バージョンを作成、使用または販売などのいくつかの方法によって侵害することになる、その貢献者によって所有される、または支配されるすべての特許請求です。しかし、貢献者バージョンのさらなる改変の結果としてのみ侵害される請求は含まれません。この定義の目的は、「支配」に本許諾書の要件と一致する方法での許諾された特許の再ライセンスの権利が含まれます。

各貢献者は貢献者の必須特許請求に基づき、貢献者バージョンのコンテンツの作成、使用、販売、販売の申し出、輸入やその他実行、改変、およびプロパゲートの非独占的、世界的、使用料無料の特許ライセンスを許諾します。

以下の 3 つのパラグラフにおいて、「特許ライセンス」とは、特許を強制しない明示的な契約または約束です。(特許の明示的な実施許諾、または特許侵害訴訟を提起しないことへの合意など) このような特許ライセンスを当事者に「許諾」するということは、その当事者に対して特許を強制しないそのような契約または約束を意味します。

特許ライセンスに依存していること、ならびにその著作物の対応ソースは一般に入手可能であるネットワーク サーバまたはその他の簡単にアクセスできる手段を通じ、誰も複製できず、無料でなく、本許諾書の条項に基づいていないことを承知の上で対象著作物をコンベイする場合は、あなたは (1) 対応ソースをそのように利用可能にする、または (2) この特定の著作物の特許ライセンスの利益を自分から剥奪するように手配する、または (3) 本許諾書の要件に一致する方法で、ダウンストリーム受領者に特許ライセンスが適用されるように手配しなければなりません。「依存していることを承知の上で」とは、特許ライセンスの許諾なくあなたがある国で対象著作物をコンベイする、またはあなたの受領者がある国で対象著作物を使用することは、あなたが有効だと信じる理由を持つ国における 1 つ以上の認識可能な特許を侵害することを実際に知っているということです。

1 回の取引または約束に従ってまたはそれに関連して、あなたが対象著作物をコンベイする、またはコンベイされた対象著作物を入手することによりプロパゲートする場合、著作物を受領する一部の当事者に対し、著作物の特定の複製物の使用、プロパゲート、改変またはコンベイを承認されている特許ライセンスを許諾する場合、あなたが許諾したその特許ライセンスは、自動的に当該対象著作物および、それに基づく著作物のすべての受領者まで拡大されます。

特許ライセンスが「差別的」とは、本許諾書の下で明確に許諾された 1 つ以上の権利が特許ライセンスの対象範囲に含まれない場合、本許諾書の下で明確に許諾された複数の権利の行使が禁止される場合、または本許諾書の下で明確に許諾された複数の権利の不行使を条件とする場合です。ソフトウェア配布事業を営む第三者と、あなたが当該著作物のコンベイの活動範囲に基づいて第三者に対価を支払うこと、およびあなたから対象著作物を受領するいずれかの当事者に第三者が、(a) あなたがコンベイした対象著作物の複製物に関連する (またはその複製物から作成された複製物) または (b) 特許ライセンスが許諾された限り、対象著作物を含む特定の製品または編集物に主に関連する、差別的特許ライセンスを許諾する協定において、あなたが当事者の場合、対象著作物をコンベイできません。2007 年 3 月 28 日より前にあなたが協定を結んだ場合を除きます。

本許諾書のいかなる記述も、いずれの暗示的ライセンスまたは適用される特許法に基づいてあなたが利用できるその他の侵害に対する弁護も除外または制限する、と解釈されてはいけません。

12. 他者の自由の放棄をしない

あなたに本許諾書の条件と矛盾する条件が強制される (裁判所命令、同意などに関わらず) 場合でも、本許諾書の条件からあなたは免除されません。本許諾書に基づくあなたの義務とその他の関連義務を同時に満たすように対象著作物をコンベイできない場合、結果として、あなたは対象著作物を全くコンベイできません。たとえば、あなたがコンベイした本プログラムをさらにコンベイする者に対する使用料を徴収する義務をあなたに課す条項にあなたが同意する場合、それらの条項と本許諾書の両方を満たすことができる唯一の方法は、本プログラムのコンベイを完全にやめることです。

13. GNU Affero　一般公衆利用許諾書との併用

本許諾書の他の条項にかかわらず、あなたはいずれかの対象著作物を、GNU Affero　一般公衆利用許諾書のバージョン　3　の下で許諾された著作物とリンク、または組み合わせて単一の結合著作物とすること、およびその結果としての著作物をコンベイすることができます。本許諾書の条件は、引き続き当該対象著作物のその部分に適用されますが、GNU Affero 一般公衆利用許諾書の第 13 節のネットワーク経由の交流に関する特別要件が、そのような結合著作物に適用されます。

14. 本許諾書の改訂版

フリー ソフトウェア財団は、随時改訂およびまたは新版の GNU 一般公衆利用許諾書を公開することができます。そのような新版は既存のバージョンとその精神においては似たものになりますが、新たな問題や懸念に対処するため細部では異なる可能性があります。

それぞれのバージョンには、識別のためのバージョン番号が振られています。プログラムが適用する GNU 一般公衆利用許諾書の特定のバージョン番号を指定し、「またはそれ以降のいかなるバージョン (or any later version)」にも適用する場合、あなたは次の条件を選択肢として、指定のバージョンか、フリー ソフトウェア財団によって発行された指定のバージョン番号以降の版のどれか 1 つのどちらかを選ぶことができます。プログラムが GNU 一般公衆利用許諾書のバージョン番号が指定しない場合は、今までにフリー ソフトウェア財団から発行されたバージョンの中から任意で選ぶことが可能です。

プロキシがどの将来版の GNU 一般公衆利用許諾書を使用するか決定できると本プログラムが指定する場合は、そのプロキシのバージョン受諾の恒久的な公式声明は、あなたが本プログラムのバージョンを選択することを承認します。

以降の許諾書のバージョンは、あなたに追加または異なる許可を付与する可能性があります。しかし、あなたが以降のバージョンに従うことを選択したことにより、追加の義務がいかなる作成者または著作権保有者に対し課せられることはありません。

15. 保証の否認

適用法が認める限りにおいて、プログラムのための保証は存在しません。書面により言明されている場合を除き、著作権所有者およびまたはその他の当事者は、プログラムを「現状のまま」提供しており、商品性および特定目的への適合性に関する暗黙の保証などの明示または黙示の一切の保証はありません。プログラムの質と性能に関するリスクのすべてはあなたに帰属します。プログラムに欠陥があると判明した場合、必要な保守点検や補修、修正に要する経費はあなたが負います。

16. 責任制限

適用法によって命じられるか書面での同意がない限り、著作権所有者または上記で許可されている通りにプログラムを改変およびまたはコンベイしたその他の当事者は、あなたに対してプログラムの使用または使用不能によって生じた通常、特別、付随的、または派生的損害 (データの損失またはデータの不正確なレンダリング、もしくはあなたまたは第三者が被った損失、もしくはプログラムが他のソフトウェアと一緒に動作しないという不具合など) に一切責任を負いません。そのような損害が生ずる可能性について、著作権所有者またはその他の当事者が忠告されていたとしても同様です。

17. 第 15 節と第 16 節の解釈

上に記載の保証の否認と責任制限に、それらの条件に従ったその地の法的効力が与えられない場合は、上級裁判所が、本プログラムに関連するすべての民事責任の絶対的放棄に最も密接に近づくその地の法律を適用するのは、料金と引き換えの本プログラムの複製物に保証または責任の引き受けが伴わない場合に限ります。

条件は以上

あなたの新しいプログラムへの上記の条件の適用方法

あなたが新しいプログラムを開発した場合、公衆によってそれが利用される可能性を最大にしたいなら、そのプログラムを本許諾書の条件に従って、誰でも再配布または変更できるようフリー ソフトウェアにするのが最善です。

そのためには、プログラムに以下のような表示を添付してください。その場合、保証が排除されているということを最も効果的に言明するために、それぞれのソースファイルの冒頭に表示を添付するのが最も安全です。少なくとも、「著作権」の行、および表示全文がある場所へのポインタを各ファイルに含めてください。

> < この 1 行にプログラム名と簡単な説明を記入 >
> Copyright (C) < 西暦年 > < 作成者名 >
>
> このプログラムはフリー ソフトウェアです。フリー ソフトウェア財団によって公開されており、GNU 一般公衆利用許諾書の条件に基づいて再配布およびまたは改変を行うことができます。本許諾書はバージョン 3 または (あなたの判断で) それ以降のバージョンのいずれかです。
>
> 本プログラムを役立てて欲しいという思いから配布していますが、いかなる保証も、商品性または特定目的への適合性に関する暗黙の保証もありません。詳細は、GNU 一般公衆利用許諾書の条件を参照してください。
>
> あなたは、本プログラムと共に GNU 一般公衆利用許諾書の複製物を受領しているはずです。そうでない場合は、こちらを参照してください。<http://www.gnu.org/licenses/>

E メールまたは郵便であなたに連絡する方法についての情報も記載します。

プログラムがターミナル インタラクションを行う場合、対話モードで起動した際に、次のような短い告知を出力するようにしてください。

> < プログラム > Copyright (C) < 西暦年 > < 作成者名 >
> This program comes with ABSOLUTELY NO WARRANTY; for details type `show w'. This is freesoftware, and you are welcome to redistribute it under certain conditions; type `show c' for details.

この仮想コマンド「show w」と「show c」は、一般公衆利用許諾書の適切な部分を表示しなければなりません。もちろん、あなたのプログラムのコマンドは違うもので構いません。GUI インターフェイスでは「about box」を使用します。

また、必要ならば (プログラマーとして働いている場合) あなたの雇用主、または学校にそのプログラムに関する「著作権放棄声明 (copyright disclaimer)」に署名してもらうべきです。詳細ならびに GNU GPL の適用方法および準拠方法はこちらを参照してください。<http://www.gnu.org/licenses/>

GNU 一般公衆利用許諾書は、あなたのプログラムをプロプライエタリ プログラムに取り入れることを許可していません。あなたのプログラムがサブルーチン ライブラリの場合は、プロプライエタリアプリケーションとライブラリのリンクを許可することが、もっと有益だと考えるかもしれません。もしそれを希望する場合は、本許諾書の代わりに GNU 劣等一般公衆利用許諾書を使用してください。まずは、こちらを読んでください。
<http://www.gnu.org/philosophy/why-notlgpl.html>

GNU 劣等一般公衆利用許諾書

バージョン 3、2007 年 6 月 29 日

GNU 劣等一般公衆利用許諾書の本バージョンは、GNU 一般公衆利用許諾書のバージョン 3 の利用条件を取り入れており、以下に列挙する追加的許可によって補足されます。

0. 追加定義

本許諾書において「本許諾」とは GNU 劣等一般公衆利用許諾書のバージョン 3 を指し、「GNU GPL」とは GNU 一般公衆利用許諾書のバージョン 3 を指します。

「本ライブラリ」とは、下記で定義されているアプリケーションや結合著作物以外の本許諾書に準拠する対象著作物を指します。

「アプリケーション」は、ライブラリに提供されたインターフェイスを使用するが、ライブラリに基づかないいずれかの著作物です。ライブラリに定義されたクラスのサブクラスの定義は、ライブラリに提供されたインターフェイスと使用するモードとみなされます。

「結合著作物」とは、アプリケーションとライブラリを組み合わせまたはリンクして制作した著作物です。結合著作物と一体の特定のライブラリのバージョンは、「リンク バージョン」とも呼ばれます。

結合著作物の「最小限の対応ソース」とは、リンク バージョンではなく、アプリケーションに基づく結合著作物の部分で分離しているとみなされるソース コードの一部を除いた、結合著作物の対応ソースを意味します。

結合著作物の「対応アプリケーション コード」とは、アプリケーションから結合著作物を再作成するために必要なデータや汎用プログラムを含み、結合著作物のシステム　ライブラリは除いた、アプリケーションのためのオブジェクト コードおよびまたはソース コードを意味します。

1. GNU GPL の第 3 節の例外

GNU GPL の第 3 節に束縛されることなく、本許諾書の第 3 節および第 4 節に基づいて対象著作物をコンベイすることができます。

2. 改変バージョンのコンベイ

あなたがライブラリの複製物を改変し、あなたの改変物で、設備が参照する関数またはデータが設備を使用するアプリケーションによって供給される (設備が起動されるとき、引数が通過する以外) 場合、あなたは改変バージョンの複製物をコンベイすることができます。

a. 本許諾書の下、アプリケーションが関数またはデータを供給しない場合に、設備はまだ操作中で、あなたが善意から努力して確実に有意義なままの目的の部分を何としても遂行しようとするとき。または

b. GNU GPL の下、その複製物に適用する本許諾書の追加的許可が何もないとき。

3. ライブラリ ヘッダ ファイルからマテリアルを組み込むオブジェクト コード

アプリケーションのオブジェクト コード形式は、ライブラリの一部であるヘッダ ファイルのマテリアルを組み込むことができます。あなたの選択する条件の下、ただし、その組み込んだマテリアルが数値パラメータ、データ構造レイアウトおよびアクセサ、またはスモール マクロ、インライン関数およびテンプレート (10 以下の桁数) に制限されないならば、そのようなオブジェクト コードをコンベイすることができます。以下の両方を行います。

a. オブジェクト コードの各複製物に、ライブラリが中で使用されていて、ライブラリとその使用が本許諾書で保証されているという目立つ表示を掲載する。

b. オブジェクト コードに GNU GPL と本許諾書の文書の複製物を添付する。

4. 結合著作物

あなたの選択する条件の下、統合すれば、結合著作物に含まれるライブラリの部分の改変、およびこのような改変のデバッグのリバース エンジニアリングを事実上制限しません。また、以下の各項目を行う場合、あなたは結合著作物をコンベイすることができます。

a. 結合著作物の各複製物に、ライブラリが中で使用されていて、ライブラリとその使用が本許諾書で保証されているという目立つ表示を掲載する。

b. 結合著作物に GNU GPL と本許諾書の文書の複製物を添付する。

c. 実行中に、ユーザーを GNU GPL と本許諾書の文書の複製物へと誘導する参照だけでなく、ライブラリ用の著作権表示を含む著作権表示を表示する結合著作物のため。

d. 次のうち 1 つを行う

0) 最小対応ソースを本許諾書の条件の下でコンベイし、ユーザーに最適な形式の対応アプリケーション コードおよび許可する条件の下、改変した結合著作物を作成するために、対応ソースをコンベイするための GNU GPL の第 6 節で指定された方法で、ユーザーはアプリケーションをリンク バージョンの改変バージョンに再結合または再リンクします。

1) ライブラリとリンクするために適切な共有ライブラリ メカニズムを使用します。適切なメカニズムは (a) ユーザーのコンピューター システムに既に存在するライブラリの複製物のランタイムに使用し、(b) リンク バージョンとインターフェイス互換性のあるライブラリの改変バージョンと共に正しく作動します。

e. GNU GPL の第 6 節の下、あなたがインストール情報を提供する必要がある場合に限り、また、そのような情報が、アプリケーションとリンク バージョンの改変バージョンを再結合、または再リンクして作成された結合著作物の改変バージョンをインストール、または実行する必要がある範囲においてのみインストール情報を提供します。(オプション 4d0 を使用する場合は、インストール情報は最小対応ソースおよび対応アプリケーショ ンコードを添付しなければなりません。オプション 4d1 を使用する場合は、対応ソースをコンベイするための GNU GPL の第 6 節で指定された方法でインストール情報を提供しなければなりません)

5. 結合ライブラリ

アプリケーションでなく、本許諾書で保証されておらず、あなたの選択する条件の下、そのような結合ライブラリをコンベイする他のライブラリ設備と単一ライブラリで並んでいる、ライブラリに基づく著作物のライブラリ設備を以下の両方を行う場合、置くことができます。

a. 他のライブラリ設備とは結合しておらず、本許諾書の条件の下コンベイするライブラリに基づく同じ著作物の複製物を結合ライブラリに添付します。

b. 結合ライブラリに、その一部はライブラリに基づいた著作物であるということ、および添付の同じ著作物の非結合形式をどこで発見できるかという目立つ説明表示を掲載する。

6. GNU 劣等一般公衆利用許諾書の改訂版

フリー ソフトウェア財団は、随時改訂およびまたは新版の GNU 劣等一般公衆利用許諾書を公開することがあります。そのような新版は既存のバージョンとその精神においては似たものになりますが、新たな問題や懸念に対処するため細部では異なる可能性があります。

それぞれのバージョンには、識別のためのバージョン番号が振られています。あなたが受領したライブラリが適用する GNU 劣等一般公衆利用許諾書の特定のバージョン番号を指定し、「またはそれ以降のいかなるバージョン (or any later version)」にも適用する場合、あなたは次の条件を選択肢として、その発行バージョンか、フリー ソフトウェア財団によって発行されたバージョン以降の版のどれか 1 つのどちらかを選ぶことができます。本ライブラリが GNU 劣等一般公衆利用許諾書のバージョン番号を指定しない場合は、今までにフリー ソフトウェア財団から発行された GNU 劣等一般公衆利用許諾書のバージョンの中から任意で選ぶことが可能です。

将来版の GNU 劣等一般公衆利用許諾書を適用するかどうか、プロキシが決定できるとあなたが受領したライブラリが指定する場合は、そのプロキシのいずれかのバージョン受諾の公式声明は、あなたがそのバージョンをライブラリに選択するための恒久的な承認です。

H.11 OpenSSL ライセンス

ライセンスの問題

OpenSSL ツールキットはデュアル ライセンス下のままです。たとえば、OpenSSL ライセンスとオリジナルの SSLeay ライセンスの両方の条件が、このツール キットに適用されます。実際のライセンス文は以下を参照してください。実際、両ライセンスは BSD スタイル オープンソース ライセンスです。OpenSSL に関連するライセンスの問題がある場合は、こちらまでお問い合わせください。openssl-core@openssl.org

OpenSSL ライセンス

Copyright (c) 1998-2008 The OpenSSL Project. All rights reserved.

ソースおよびバイナリ形式の再配布および使用は、改変の有無にかかわらず、以下の条件に合うものは許可されています。

- ソースコードの再配布は、前述の著作権表示、本条件一覧および後述の免責事項を残しておかなければなりません。

- バイナリ形式の再配布は、前述の著作権表示、本条件一覧および後述の免責事項を、配布時に提供する文書およびまたはその他の資料内に複製しなければなりません。

- 本ソフトウェアの機能または使用に言及するすべての宣伝物は、次の承認文を表示しなければなりません。“This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)”

- 「OpenSSL Toolkit」および「OpenSSL Project」の名称は、特定の事前の書面による許可なしで、本ソフトウェアから派生した製品の推奨または宣伝に使用することはできません。書面による許可についてのお問い合わせはこちらです。openssl-core@openssl.org

- 本ソフトウェアから派生した製品は「OpenSSL」とは呼ばれないことがあり、OpenSSL Project の事前の書面による許可なしで「OpenSSL」をその製品の名称に使用することはできません。

- いかなる形式の再配布も、次の承認文を表示しなければなりません。“This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”

本ソフトウェアは、OpenSSL PROJECT によって「現状のまま」提供されており、商品性および特定目的への適合性に関する暗黙の保証などの明示または黙示の保証責任を否認します。OpenSSL PROJECT またはその貢献者は、原因のいかんにかかわらず、また責任理論が契約の記述、厳格責任、または不法行為かを問わず (過失その他を含む)、次のような損害の可能性を知らされていたとしても、本ソフトウェアの使用に起因するいかなる直接的、間接的、付随的、特別、懲罰的または派生的損害 (代替商品またはサービスの調達、使用、データまたは利益の損失、あるいは営業中断など) に対して一切責任を負いません。

本製品には、エリック・ヤング氏 (eay@cryptsoft.com) によって作成された暗号ソフトウェアが使用されています。本製品には、ティム・ハドソン氏 (tjh@cryptsoft.com) によって作成されたソフトウェアが使用されています。

オリジナル SSLeay ライセンス

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
All rights reserved.

本パッケージは、エリック・ヤング氏 (eay@cryptsoft.com) によって作成された SSL を実装しています。Netscape の SSL に適合させるためにインプリメンテーションは作成されました。

本ライブラリは、次の条件を順守する限り、商用または非商用の使用においてフリーです。次の条件はこの配布内で見つかるすべてのコードに適用されます。RC4、RSA、lhash、DES などのコードのことで、ただの SSL コードではありません。この配布を含む SSL ドキュメンテーションには、ティム・ハドソン氏が所有者であるものを除き、同じ著作権の条件で保護されています。

著作権はエリック・ヤング氏に帰属し、コードのそのようないかなる著作権表示も排除されません。製品内で本パッケージが使用されている場合、ライブラリが使用されている部分の作成者として、エリック・ヤング氏に帰属します。プログラムの起動時のテキスト メッセージでも、パッケージと共に提供されるドキュメント (オンラインまたは文書) 内のテキスト メッセージの形式でも構いません。

ソースおよびバイナリ形式の再配布および使用は、改変の有無にかかわらず、以下の条件に合うものは許可されています。

- ソースコードの再配布は、前述の著作権表示、本条件一覧および後述の免責事項を残しておかなければなりません。

- バイナリ形式の再配布は、前述の著作権表示、本条件一覧および後述の免責事項を、配布時に提供する文書およびまたはその他の資料内に複製しなければなりません。

- 本ソフトウェアの機能または使用に言及するすべての宣伝物は、次の承認文を表示しなければなりません。

  “This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

  「cryptographic」と言う言葉は、ライブラリからのルーティンに暗号化に関連するものが使用されていない場合、省いても構いません。

- apps ディレクトリから (アプリケーションコード) Windows 特有コードを何か含む場合は、次の承認文を含まなければなりません。“This product includes software written by Tim Hudson (tjh@cryptsoft.com)”

本ソフトウェアは、エリック・ヤングによって「現状のまま」提供されており、商品性および特定目的への適合性に関する暗黙の保証などの明示または黙示の保証責任を否認します。作成者またはその貢献者は、原因のいかんにかかわらず、また責任理論が契約の記述、厳格責任、または不法行為かを問わず (過失その他を含む)、次のような損害の可能性を知らされていたとしても、本ソフトウェアの使用に起因するいかなる直接的、間接的、付随的、特別、懲罰的または派生的損害 (代替商品またはサービスの調達、使用、データまたは利益の損失、あるいは営業中断など) に対して一切責任を負いません。

一般に入手可能なバージョン、または本コードから派生した本ライセンスおよび配布の条件は、変更できません。たとえば、本コードをただ複製して、他の配布ライセンス下に置くことはできません。(GNU 一般公衆利用許諾書を含む)

H.12 Open SSH ライセンス

本ファイルは Open SSH ソフトウェアの一部です。

本ソフトウェアのコンポーネントである本ライセンスは、次のとおりに該当します。まず、すべてのコンポーネントが BSD ライセンス下にあること、またはそれよりもフリーなライセンス下にあることをまとめます。

Open SSH は GPL コードを含みません。

1)

Copyright (c) 1995 Tatu Ylonen <ylo@cs.hut.fi>, Espoo, Finland
All rights reserved

私に関する限りは、本ソフトウェアのために私が作成した本コードは、いかなる目的にもフリーで使用することが可能です。本ソフトウェアのいかなる派生版も、その派生著作物がファイルのプロトコル記述と互換性がない場合は、はっきりとそのことを表示し、「ssh」または「Secure Shell」以外の名前で呼ばれなければなりません。

[Tatu 続く]

しかし、いずれかのライセンスを、第三者が保有するいずれかの特許または著作権に与えることは暗示していません。また、本ソフトウェアには私の直接管理下にない部分が含まれています。私が知る限り、含まれているソース コードはすべて関連するライセンス契約に準拠して使用されていて、いかなる目的のためにも自由に使用することができます。(GNU 許諾がもっとも制約があります) 詳細は次を参照してください。

[しかし、現在のところ、この条件はどれも関連がありません。Tatu 氏が述べたこれらすべての制限された許諾ソフトウェア コンポーネントは、OpenSSH から削除されました。たとえば

- RSA はもう含まれていません。OpenSSL ライブラリで見つかります。
- IDEA はもう含まれていません。その使用は非推奨です。
- DES は現在外付けで、OpenSSL ライブラリにあります。

- GMP はもう使用されていません。その代わりに OpenSSL の BN コードを呼びます。
- Zlib は現在外付けで、ライブラリにあります。
- make-ssh-known-hosts スクリプトはもう含まれていません。
- TSS は削除されました。
- MD5 は現在外付けで、OpenSSL ライブラリにあります。
- RC4 サポートは OpenSSL の ARC4 サポートに代わりました。
- Blowfish は現在外付けで、OpenSSL ライブラリにあります。

[ライセンス続く]

本ソフトウェアで使用されているいずれかの情報および暗号化アルゴリズムは、インターネット上、大手書店、科学図書館および特許庁で全世界的に一般に入手可能であることに気を付けてください。詳細は「http://www.cs.hut.fi/crypto」などで参照できます。

本プログラムの法的地位は、これらすべての許可及び制限のいくつかの組み合わせです。あなた自身の責任の下でのみ使用できます。あなたは、いかなる自身への法的影響に対しても責任を負います。私はこれの所有または使用があなたの国において合法または違法であっても、何ら請求をしません。また、あなたの代わりに責任を負うこともありません。

H.13 PPP ライセンス

BSD-like ライセンスは下のとおりです。そのすべてが pppd のすべての部分に適用されるわけではありません。

Copyright (c) 2003 Paul Mackerras. All rights reserved.

ソースおよびバイナリ形式の再配布および使用は、改変の有無にかかわらず、以下の条件に合うものは許可されています。

- ソースコードの再配布は、前述の著作権表示、本条件一覧および後述の免責事項を残しておかなければなりません。
- 本ソフトウェアの作成者名は、特定の事前の書面による許可なしで、本ソフトウェアから派生した製品の推奨または宣伝に使用することはできません。
- いかなる形式の再配布も、次の承認文を表示しなければなりません。“This product includes software developed by Paul Mackerras <paulus@samba.org>”.

本ソフトウェアの作成者は、本ソフトウェアに関する、商品性および特定目的への適合性に関する暗黙の保証を含むすべての保証責任を否認します。作成者は、本ソフトウェアの使用または性能に関連して起こる契約の行動、過失またはその他の不法行為かどうかにかかわらず、本ソフトウェアの使用に起因するいかなる特別、間接的、または派生的損害あるいは使用、データまたは利益の損失に起因するいかなる損害に対して一切責任を負いません。

Copyright (c) 1995 Pedro Roque Marques. All rights reserved.

ソースおよびバイナリ形式の再配布および使用は、改変の有無にかかわらず、以下の条件に合うものは許可されています。

- ソースコードの再配布は、前述の著作権表示、本条件一覧および後述の免責事項を残しておかなければなりません。バイナリ形式の再配布は、前述の著作権表示、本条件一覧および後述の免責事項を、配布時に提供する文書およびまたはその他の資料内に複製しなければなりません。

- 本ソフトウェアの作成者名は、特定の事前の書面による許可なしで、本ソフトウェアから派生した製品の推奨または宣伝に使用することはできません。

- いかなる形式の再配布も、次の承認文を表示しなければなりません。“This product includes software developed by Pedro Roque Marques <pedro_m@yahoo.com>”

本ソフトウェアの作成者は、本ソフトウェアに関する、商品性および特定目的への適合性に関する暗黙の保証を含むすべての保証責任を否認します。作成者は、本ソフトウェアの使用または性能に関連して起こる契約の行動、過失またはその他の不法行為かどうかにかかわらず、本ソフトウェアの使用に起因するいかなる特別、間接的、または派生的損害あるいは使用、データまたは利益の損失に起因するいかなる損害に対して一切責任を負いません。

Copyright (c) 1995 Eric Rosenquist. All rights reserved.

- ソースコードの再配布は、前述の著作権表示、本条件一覧および後述の免責事項を残しておかなければなりません。

- バイナリ形式の再配布は、前述の著作権表示、本条件一覧および後述の免責事項を、配布時に提供する文書およびまたはその他の資料内に複製しなければなりません。

- 本ソフトウェアの作成者名は、特定の事前の書面による許可なしで、本ソフトウェアから派生した製品の推奨または宣伝に使用することはできません。

本ソフトウェアの作成者は、本ソフトウェアに関する、商品性および特定目的への適合性に関する暗黙の保証を含むすべての保証責任を否認します。作成者は、本ソフトウェアの使用または性能に関連して起こる契約の行動、過失またはその他の不法行為かどうかにかかわらず、本ソフトウェアの使用に起因するいかなる特別、間接的、または派生的損害あるいは使用、データまたは利益の損失に起因するいかなる損害に対して一切責任を負いません。

Copyright (c) 2002 Google, Inc. All rights reserved.

ソースおよびバイナリ形式の再配布および使用は、改変の有無にかかわらず、以下の条件に合うものは許可されています。

- ソースコードの再配布は、前述の著作権表示、本条件一覧および後述の免責事項を残しておかなければなりません。

- バイナリ形式の再配布は、前述の著作権表示、本条件一覧および後述の免責事項を、配布時に提供する文書およびまたはその他の資料内に複製しなければなりません。

- 本ソフトウェアの作成者名は、特定の事前の書面による許可なしで、本ソフトウェアから派生した製品の推奨または宣伝に使用することはできません。

本ソフトウェアの作成者は、本ソフトウェアに関する、商品性および特定目的への適合性に関する暗黙の保証を含むすべての保証責任を否認します。作成者は、本ソフトウェアの使用または性能に関連して起こる契約の行動、過失またはその他の不法行為かどうかにかかわらず、本ソフトウェアの使用に起因するいかなる特別、間接的、または派生的損害あるいは使用、データまたは利益の損失に起因するいかなる損害に対して一切責任を負いません。

Copyright (c) 2001 by Sun Microsystems, Inc. All rights reserved.

全部または部分的なソースおよびバイナリ形式での本ソフトウェアの再分配、改変、翻訳および使用における非独占的権利は、本契約により付与されます。しかし、上記の著作権表示をいかなるソース形式においても複製し、著作権保有者名または作成者名のいずれも、本ソフトウェアから派生した製品の推奨または宣伝に使用しない場合に限ります。

本ソフトウェアは、「現状のまま」提供されており、商品性および特定目的への適合性に関する暗黙の保証などの明示または黙示の保証はありません。

Copyright (c) 1999 Tommi Komulainen. All rights reserved.

ソースおよびバイナリ形式の再配布および使用は、改変の有無にかかわらず、以下の条件に合うものは許可されています。

- バイナリ形式の再配布は、前述の著作権表示、本条件一覧および後述の免責事項を、配布時に提供する文書およびまたはその他の資料内に複製しなければなりません。

- 本ソフトウェアの作成者名は、特定の事前の書面による許可なしで、本ソフトウェアから派生した製品の推奨または宣伝に使用することはできません。

- いかなる形式の再配布も、次の承認文を表示しなければなりません。“This product includes software developed by Tommi Komulainen <Tommi.Komulainen@iki.fi>”

本ソフトウェアの作成者は、本ソフトウェアに関する、商品性および特定目的への適合性に関する暗黙の保証を含むすべての保証責任を否認します。作成者は、本ソフトウェアの使用または性能に関連して起こる契約の行動、過失またはその他の不法行為かどうかにかかわらず、本ソフトウェアの使用に起因するいかなる特別、間接的、または派生的損害あるいは使用、データまたは利益の損失に起因するいかなる損害に対して一切責任を負いません。

Copyright (c) 1984-2000 Carnegie Mellon University. All rights reserved.

ソースおよびバイナリ形式の再配布および使用は、改変の有無にかかわらず、以下の条件に合うものは許可されています。

- ソースコードの再配布は、前述の著作権表示、本条件一覧および後述の免責事項を残しておかなければなりません。
- バイナリ形式の再配布は、前述の著作権表示、本条件一覧および後述の免責事項を、配布時に提供する文書およびまたはその他の資料内に複製しなければなりません。
- 「Carnegie Mellon University」の名称は、特定の事前の書面による許可なしで、本ソフトウェアから派生した製品の推奨または宣伝に使用することはできません。

  Office of Technology Transfer
  Carnegie Mellon University
  5000 Forbes Avenue
  Pittsburgh, PA 15213-3890
  電話 (412) 268-4387、ファックス : (412) 268-7395
  tech-transfer@andrew.cmu.edu

- いかなる形式の再配布も、次の承認文を表示しなければなりません。“This product includes software developed by Computing Services at Carnegie Mellon University (http://www.cmu.edu/computing/).”

CARNEGIE MELLON UNIVERSITY は、本ソフトウェアに関する、商品性および特定目的への適合性に関する暗黙の保証を含むすべての保証責任を否認します。CARNEGIE MELLON UNIVERSITY は、本ソフトウェアの使用または性能に関連して起こる契約の行動、過失またはその他の不法行為かどうかにかかわらず、本ソフトウェアの使用に起因するいかなる特別、間接的、または派生的損害あるいは使用、データまたは利益の損失に起因するいかなる損害に対して一切責任を負いません。

****

Copyright (C) 1990, RSA Data Security, Inc. All rights reserved.

本ソフトウェアまたは本関数に言及または参照するすべてのマテリアルで、「RSA Data Security, Inc. MD5 Message-Digest Algorithm」として確認されている限り、本ソフトウェアの複製および使用のライセンスは許諾されています。

また、派生著作物に言及または参照するすべてのマテリアルで、「derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm」として確認されている限り、そのような派生著作物の作成および使用のライセンスが許諾されています。

RSA Data Security, Inc. は、本ソフトウェアの商品性または特定用途への本ソフトウェアの適合性に関して明言しません。本ソフトウェアは「現状のまま」提供されており、明示または黙示のいかなる保証もありません。

本文書およびまたはソフトウェアのいかなる部分のすべての複製物に、これらの表示が保たれなければなりません。

****

「chat」プログラムはすでに公知となっています。spinlock.c および tdb.c は、GNU LGPL バージョン 2 またはそれ以降のバージョンの下で許諾されています。これらは次のとおりです。

PPP ライセンス

Copyright (C) Anton Blanchard 2001

Copyright (C) Andrew Tridgell 1999-2004

Copyright (C) Paul `Rusty' Russell 2000

Copyright (C) Jeremy Allison 2000-2003

Debian システムでは、GNU 一般公衆利用許諾書の条件の全文を「/usr/share/common-licenses/GPL」で見ることができます。

pppd/plugins/rp-pppoe/* は :

Copyright (C) 2000 by Roaring Penguin Software Inc.

本プログラムは、GNU 一般公衆利用許諾書バージョン 2 または (あなたの判断で) それ以降のいずれかのバージョンの条件に従って配布することができます。

rp-pppoe の作成者は、Marco d'Itri への非公開の E メールで、ライセンスの例外として OpenSSL へのリンクを認めるとはっきりと述べています。

pppd/plugins/winbind.c は、GNU GPL バージョン 2 またはそれ以降のバージョンの下で許諾されており、次のとおりです。

Copyright (C) 2003 Andrew Bartlet <abartlet@samba.org>
Copyright 1999 Paul Mackerras, Alan Curry.
Copyright (C) 2002 Roaring Penguin Software Inc.

pppd/plugins/pppoatm.c は、GNU GPL バージョン 2 またはそれ以降のバージョンの下許諾されており、次のとおりです。

Copyright 2000 Mitchell Blank Jr.

次の著作権表示は「plugins/radius/*」に適用されます。

Copyright (C) 2002 Roaring Penguin Software Inc.

本著作権表示および許可告知がすべての複製物および補足文書に表示されており、Roaring Penguin Software Inc. の名前を、特定の事前の許可および Roaring Penguin Software Inc. の許可を得た複製物および配布であるという補足文書内の表示なしで、本プログラムから派生した製品の推奨または宣伝に使用しないかぎり、いずれかの理由のために無料で本ソフトウェアを使用、複製、改変、および配布することはここに許可されます。

Roaring Penguin Software Inc. は、どのような目的においても本ソフトウェアの適合性に関して明言しません。本ソフトウェアは「現状のまま」提供されており、明示または黙示の保証はありません。

Copyright (C) 1995,1996,1997,1998 Lars Fenneberg <lf@elemental.net>

本著作権表示および許可告知がすべての複製物および補足文書に表示されており、Lars Fenneber の名前を、特定の事前の許可および Lars Fenneberg の許可を得た複製および配布であるという補足文書内の表示なしで、本プログラムから派生した製品の推奨または宣伝に使用しないかぎり、いずれかの理由のために無料で本ソフトウェアを使用、複製、改変、および配布することはここに許可されます。

Lars Fenneberg は、どのような目的においても本ソフトウェアの適合性に関して明言しません。本ソフトウェアは「現状のまま」提供されており、明示または黙示の保証はありません。

Copyright 1992 Livingston Enterprises, Inc.
Livingston Enterprises, Inc. 6920 Koll Center Parkway Pleasanton, CA 94566

本著作権表示および許可告知がすべての複製物および補足文書に表示されており、Livingston Enterprises, Inc. の名前を、特定の事前の許可および Livingston Enterprises, Inc. の許可を得た複製および配布であるという補足文書内の表示なしで、本プログラムから派生した製品の推奨または宣伝に使用しないかぎり、いずれかの理由のために無料で本ソフトウェアを使用、複製、改変、および配布することはここに許可されます。

Livingston Enterprises, Inc. は、どのような目的においても本ソフトウェアの適合性に関して明言しません。本ソフトウェアは「現状のまま」提供されており、明示または黙示の保証はありません。

[C] The Regents of the University of Michigan and Merit Network, Inc. 1992,1993, 1994, 1995
All Rights Reserved

上記著作権表示および本許可告知が、本ソフトウェアの複製物および派生著作物またはその改変版すべてに表示されており、補足文書内に著作権表示および本許可告知および免責告知が表示される限り、いずれかの理由のために無料で本ソフトウェアおよびその文書を使用、複製、改変、および配布することはここに許可されます。

本ソフトウェアは「現状のまま」提供されており、商品性および特定目的への適合性に関する保証などの明示または黙示の一切の保証はありません。THE REGENTS OF THE UNIVERSITY OF MICHIGAN および MERIT NETWORK, INC. は、本ソフトウェア内に含まれる関数がライセンス要件を満たす、もしくはその動作に支障がない、またはエラーフリーであることを保証しません。THE REGENTS OF THE UNIVERSITY OF MICHIGAN および Merit Network, Inc. は、本ソフトウェアの使用に起因する、ライセンシーまたは第三者の請求に関するいかなる特別、間接的、付随的、または派生的損害に対して責任を負いません。

Copyright (C) 1991-2, RSA Data Security, Inc. Created 1991.
All rights reserved.

本ソフトウェアまたは本関数に言及または参照するすべてのマテリアルで、「RSA Data Security, Inc. MD5 Message-Digest Algorithm」として確認されている限り、本ソフトウェアの複製および使用のライセンスは許諾されています。

また、派生著作物に言及または参照するすべてのマテリアルで、「derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm」として確認されている限り、そのような派生著作物の作成および使用のライセンスが許諾されています。

RSA Data Security, Inc. は、本ソフトウェアの商品性または特定用途への本ソフトウェアの適合性に関して明言しません。本ソフトウェアは「現状のまま」提供されており、明示または黙示のいかなる保証もありません。

本文書およびまたはソフトウェアのいかなる部分のすべての複製物に、これらの表示が保たれなければなりません。

radius.c

Copyright (C) 2002 Roaring Penguin Software Inc.

本プラグインは、GNU 一般公衆利用許諾書バージョン 2 または (あなたの判断で) それ以降のいずれかのバージョンの条件に従って配布することができます。

H.14 Shadow ライセンス

本ソフトウェアの一部は、copyright 1988 - 1994, Julianne Frances Haugh.
All rights reserved.

Shadow ライセンス

本ソフトウェアの一部は、copyright 1997 - 2001, Marek Michałkiewicz.
All rights reserved.

本ソフトウェアの一部は、copyright 2001 - 2004, Andrzej Krzysztofowicz
All rights reserved.

本ソフトウェアの一部は、copyright 2000 - 2007, Tomasz Kłoczko.
All rights reserved.

ソースおよびバイナリ形式の再配布および使用は、改変の有無にかかわらず、以下の条件に合うものは許可されています。

- ソースコードの再配布は、前述の著作権表示、本条件一覧および後述の免責事項を残しておかなければなりません。
- バイナリ形式の再配布は、前述の著作権表示、本条件一覧および後述の免責事項を、配布時に提供する文書およびまたはその他の資料内に複製しなければなりません。
- Julianne F. Haugh の名前、または貢献者の名前のいずれも、特定の事前の書面による許可なしで、本ソフトウェアから派生した製品の推奨または宣伝に使用することはできません。

本ソフトウェアは、Julianne F. Haugh および貢献者によって「現状のまま」提供されており、商品性および特定目的への適合性に関する暗黙の保証などの明示または黙示の保証責任を否認します。著作権所有者または貢献者は、原因のいかんにかかわらず、また責任理論が契約の記述、厳格責任、または不法行為かを問わず (過失その他を含む)、次のような損害の可能性を知らされていたとしても、本ソフトウェアの使用に起因するいかなる直接的、間接的、付随的、特別、懲罰的または派生的損害 (代替商品またはサービスの調達、使用、データまたは利益の損失、あるいは営業中断など) に対して一切責任を負いません。

本ソースコードは現在、USENET アーカイブの一部である comp.sources.misc の ftp.uu.net に保管されています。また、本パッケージについて何か質問がある場合は、作成者の Julianne F. Haugh 氏に jockgrrl@ix.netcom.com まで問い合わせることも可能です。

本ソフトウェアは、現状のまま配布されています。作成者は使用によって生じるいかなる結果に対し、一切の責任を負いません。そのユーザーは、本ソフトウェアパッケージの保守に対し、単独で責任を負います。作成者は、改変または改良したものを提供する一切の義務がありません。ユーザーは、情報または機械の資料を不慮の損失から保護するために、あらゆる手段を講じるのが望ましいです。

素晴らしいテストに対する努力を示してくれた Chip Rosenthal 氏、本コードの BSD への移植をしてくれた Steve Simmons 氏、そしてレーザージェット プリンターに時間と熱意を費やして貢献してくれた Bill Kennedy 氏に深く感謝します。また、イニシャル shadow パスワード情報を提供してくれた Dennis L. Mumaugh 氏と、System V Release 4 の変更をしてくれた Tony Walton 氏 (olapw@olgb1.oliv.co.uk) に感謝します。SunOS への移植に尽力してくれたのは、Dr. Michael Newberry (miken@cs.adfa.oz.au) と Micheal J. Miller, Jr. 氏 (mke@kaberd.rain.com) です。AT&T UNIX System V Release 4 への移植に尽力してくれたのは、Andrew Herbert 氏 (andrew@werple.pub.uu.oz.au) です。本ソフトウェアの Linux ポートを引き継いでくれた Marek Michalkiewicz 氏 (marekm@i17linuxb.ists.pwr.wroc.pl) に深く感謝します。

ソースファイル : ogin_access.c、login_desrpc.c、login_krb.c は、次のライセンス下の logdaemon-5.0 パッケージから派生したものです。

****
Copyright 1995 by Wietse Venema. All rights reserved. 個別ファイルは他の著作権によって保護されています。(ファイル自体に記載あり)

本マテリアルは、もともとオランダのアイントホーヘェン工科大学の Wietse Venema 氏によって、1990 年、1991 年、1992 年、1993 年、1994 年および 1995 年に作成され、まとまられたものです。

ソースおよびバイナリ形式の再配布および使用は、改変の有無にかかわらず、以下の条件に合うものは許可されています。

本ソフトウェアは「現状のまま」提供されており、商品性および特定目的への適合性に関する暗黙の保証などの明示または黙示のいかなる保証もありません。

****

いくつかの部分は、実質的に GNU の su の先祖から派生した src/su.c にあります。シェルは偽装ユーザーとグループ ID で実行します。

Copyright (C) 1992-2003 Free Software Foundation, Inc.

このプログラムはフリー ソフトウェアです。フリー ソフトウェア財団によって公開されており、GNU 一般公衆利用許諾書の条件に基づいて再配布およびまたは改変を行うことができます。本許諾書はバージョン 2 または (あなたの判断で) それ以降のバージョンのいずれかです。

本プログラムは役に立ってほしいという思いから配布していますが、いかなる保証も、商品性または特定目的への適合性に関する暗黙の保証もありません。詳細は、GNU 一般公衆利用許諾書の条件を参照してください。

Debian GNU/Linux システムでは、GNU 一般公衆利用許諾書の条件の全文を「/usr/share/common-licenses/GPL」で見ることができます。

H.15 Sudo ライセンス

Sudo は次の ISC-style ライセンス下で配布されています。

Copyright (c) 1994-1996, 1998-2009
Todd C. Miller Todd.Miller@courtesan.com

上記著作権表示および許可告知がすべての複製物に表示される限り、いずれかの理由のために無償または有償で本ソフトウェアを使用、複製、改変、および配布することはここに許可されます。

本ソフトウェアは「現状のまま」提供されており、その作成者は、本ソフトウェアに関する商品性および適合性に関する暗黙の保証を含む一切の保証責任を否認します。作成者は、本ソフトウェアの使用または性能に関連して起こる契約の行動、過失またはその他の不法行為かどうかにかかわらず、本ソフトウェアの使用に起因するいかなる特別、直接的、間接的、または派生的損害あるいは使用、データまたは利益の損失に起因するいかなる損害に対して一切責任を負いません。

契約書番号 F39502-99-1-0512 の下、国防総省国防高等研究事業局および空軍研究所、米空軍資材コマンド、USAF から一部資金提供を受けました。

さらに、fnmatch.c、fnmatch.h、getcwd.c、glob.c, glob.h および snprintf.c は、次のライセンスを持っています。

ソースおよびバイナリ形式の再配布および使用は、改変の有無にかかわらず、以下の条件に合うものは許可されています。

- ソースコードの再配布は、前述の著作権表示、本条件一覧および後述の免責事項を残しておかなければなりません。
- バイナリ形式の再配布は、前述の著作権表示、本条件一覧および後述の免責事項を、配布時に提供する文書およびまたはその他の資料内に複製しなければなりません。
- 大学名、または貢献者の名前のいずれも、特定の事前の書面による許可なしで、本ソフトウェアから派生した製品の推奨または宣伝に使用することはできません。

本ソフトウェアは、THE REGENTS および貢献者によって「現状のまま」提供されており、商品性および特定目的への適合性に関する暗黙の保証などの明示または黙示の保証責任を否認します。著作権所有者または貢献者は、原因のいかんにかかわらず、また責任理論が契約の記述、厳格責任、または不法行為かを問わず (過失その他を含む)、次のような損害の可能性を知らされていたとしても、本ソフトウェアの使用に起因するいかなる直接的、間接的、付随的、特別、懲罰的または派生的損害 (代替商品またはサービスの調達、使用、データまたは利益の損失、あるいは営業中断など) に対して一切責任を負いません。

nonunix.h と vasgroups.c は、次のライセンスを持っています。

ソースおよびバイナリ形式の再配布および使用は、改変の有無にかかわらず、以下の条件に合うものは許可されています。

- ソースコードの再配布は、前述の著作権表示、本条件一覧および後述の免責事項を残しておかなければなりません。
- バイナリ形式の再配布は、前述の著作権表示、本条件一覧および後述の免責事項を、配布時に提供する文書およびまたはその他の資料内に複製しなければなりません。
- Quest Software, Inc. の名前、または貢献者の名前のいずれも、特定の事前の書面による許可なしで、本ソフトウェアから派生した製品の推奨または宣伝に使用することはできません。

本ソフトウェアは、著作権所有者および貢献者によって「現状のまま」提供されており、商品性および特定目的への適合性に関する暗黙の保証などの明示または黙示の保証責任を否認します。著作権所有者または貢献者は、原因のいかんにかかわらず、また責任理論が契約の記述、厳格責任、または不法行為かを問わず (過失その他を含む)、次のような損害の可能性を知らされていたとしても、本ソフトウェアの使用に起因するいかなる直接的、間接的、付随的、特別、懲罰的または派生的損害 (代替商品またはサービスの調達、使用、データまたは利益の損失、あるいは営業中断など) に対して一切責任を負いません。