SENA

# スーパーターミナルサーバー
# (STS800/1600)
# ユーザーガイド

Version 1.0.0._JP
2008-03-06

InterSolution Marketing キーワードは「つ・な・ぐ」—シリアル・インターネットワーキング—
http://www.intersolutionmarketing.com/

株式会社インターソリューションマーケティング
〒150-0013
東京都渋谷区恵比寿 1-24-14 EXOS恵比寿ビル 5F
Tel. 03-5795-2685 Fax. 03-5795-2686

InterSolution Marketing Inc.,
EXOS Ebisu Bldg. 5F,
Ebisu 1-24-14, Shibuya, Tokyo Japan 150-0013
Tel.+81 3 5795 2685 Fax.+81 3 5795 2688

## コピーライト



## 商標

SecureTerminal Server STS Series™は、Sena Technologies,Inc の商標です。
Windows®は、Microsoft Corporation の登録商標です。
Ethernet®は、XEROX Corporation の登録商標です。

# ■■■ 安全にお使いいただくために ■■■

・本機を正しく使用するために、必ずお読みください。
・この記載内容を守って製品をご使用ください。
パソコンや接続される機器の故障／トラブルや、いかなるデータの消失・破損または、取扱いを誤ったために生じた本製品の故障／トラブルは、弊社の保証対象にはなりません。

● **表記の意味**

**警告表示の意味**

**警告** 人が死亡または重傷を負う可能性が想定される内容を示しています。

**注意** 人が傷害を負う可能性が想定される内容、および、物的損害の発生が想定される内容を示します。

**傷害や事故の発生を防止するための禁止事項**

**一般禁止** その行為を禁止します。

**接触禁止** 特定場所に触れることで傷害を負う可能性を示します。

**水ぬれ禁止** 水がかかる場所での使用、水に濡らすなどして使用すると漏電、感電、発火の可能性を示します。

**火気禁止** 外部の火気によって製品が発火する可能性を示します。

**分解禁止** 分解することにより製品が発火する可能性を示します。

**傷害や事故の発生を防止するための指示事項**

使用者に対して指示に基づく行為を強制するものです。

電源コードのプラグを抜くように指示するものです。

● **警告事項**

**電源ケーブルを傷つけたり、加工、加熱、修復したりしないでください。火災がおきたり感電するおそれがあります。**

**本製品の内部に次のような異物を入れないでください。**
金属物、水などの液体、燃えやすい物質、薬品等回路がショートして火災の原因になります。

本製品は RS-232 スタンダード製品に準拠しています。RS-232 非スタンダード製品を使用した結果機器が故障した場合、責任は負いかねます。

**本製品を改造・分解しないでください。**
感電、発煙、発火の原因になります。

**ボタンに過剰な圧力をかけないでください。**
ボタンに過剰な圧力をかけたり、必要以上に押し続けると、故障の原因になります。

**AC100V(50/60Hz)以外のコンセントには、絶対にプラグを差し込まないでください。**
異なる電圧で使用すると、感電、発煙、火災の原因になります。

**電源ケーブル(または AC アダプター)は必ず本製品付属のものをお使いください。また、製品添付の電源コード(または AC アダプター)を他の機器には使用しないでください。**
本製品付属以外の電源ケーブル、AC アダプターをご使用になると、感電、発煙・発火のおそれがあります。

**本製品を落としたり、強い衝撃を与えたりした場合には、すぐに AC アダプターを抜いてください。**
そのまま使用し続けると、ショートして火災になったり感電したりするおそれがあります。

**煙がでたり異臭がしたり音がしたら、AC コンセントからプラグを抜いてください。**
そのまま使用し続けると、ショートして火災になったり感電したりするおそれがあります。

**本製品を、風呂場など、水分や湿気の多い場所では使用しないでください。**
感電、火災の原因になるおそれがあります。

**周辺機器は、マニュアルの記載されている手順に従って正しく取り付けてください。**
正しく取り付けられていないと、発煙、発火の原因になります。

**電源製品のケーブル、コネクター類、付属品など小さなお子様の手が届かない ように機器を設置してください。**
けがをするおそれがあります。

● **注意事項**

**電源ケーブルが AC コンセントに接続されているときには、濡れた手で本製品に触らないでください。**
感電するおそれがあります。

**静電気による破損を防ぐため、本製品に触れる前に身近な金属(ドアのノブやアルミサッシなど)に手を触れて、身体の静電気を取り除くようにしてください。**
身体の静電気が本製品を破損するおそれがあります。

**次の場所には放置しないでください。**
感電、火災の原因になり、製品に悪い影響を及ぼすかもしれません。

- 強い磁界が発生するところ(故障の原因)
- 静電気が発生するところ(故障の原因)
- 振動が発生するところ(故障、破損の原因)
- 平らでないところ(落下などでけがの原因)
- 直射日光があたるところ(故障や変形の原因)
  火気周辺、熱気がこもるところ(故障や変形の原因)
- 漏電の危険のあるところ(故障や感電の原因)
- 漏水の危険のあるところ(故障や感電の原因)

**本製品を破棄するときには、各地方自治体の条例に従ってください。**
内容については、各地方自治体にお問い合わせください。

# 1. はじめに

## 1.1. 概要

これは SENA テクノロジー社製 セキュア・ターミナルサーバー（デバイスサーバー）、STS シリーズのユーザーガイドです。

STS シリーズは、既存のシリアルデバイスを、標準 Ethernet ネットワークによって管理可能にしたデバイスサーバーです。TCP/IP, UDP のようなオープンネットワーク・プロトコルでお使いのシリアルデバイスに究極のフレキシビリティを与えます。PPPoE(PPP-over-Ethernet)接続機能により、RS232 シリアルデバイスは DSL ブロードバンドネットワーク上で管理できるようになりました。DHCP, PPPoE, Dynamic DNS,のような高速ブロードバンドネットワーク接続プロトコルで、DSL やケーブルモデム接続により、シリアルデバイスの管理を効率化します。

STS シリーズの組み込み式 Dynamic DNS プロトコルは独自のドメイン名でシリアルデバイスにアクセス可能です。

STS シリーズは telnet SSH, シリアルコンソール、またはWEBでシステムステータス表示、ファームウェア・アップグレード、リモートリセット、およびシステムログ表示のような様々な動作を表示します。

また、パスワード保護による Telnet またはシリアルコンソールポートで、ステータス監視、リモートリセット、エラーログ監視、およびファームウェア・アップグレードの全機能をコンフィギュレーションおよび管理します。

セキュアデータ通信が必要なクリティカルアプリケーションのために、STS シリーズはデータ暗号化の SSLv2, SSLv3, および TLSv1をサポートしています。

さらに、IP アドレスフィルタリング機能は STS ターミナルサーバーに不本意なデータが混入するのを防ぎます。

*STS シリーズターミナルサーバーが活躍する主な分野:*

- FA機器
- ネットワーク管理
- リテール・POS
- リモート測量
- リモートディスプレイ表示
- ビル管理
- セキュリティ・アクセス制御システム
- データ取得アプリケーション
- 医療システム

STS シリーズは RS-232 シリアルデバイスの制御、監視、解析、およびデータ収集をリモート操作するのに理想的なソリューションです。

## 1.2. 同梱品チェックリスト

- STS ターミナルサーバー本体
- 外付け 110V(230V)電源アダプタ
- CAT5 ケーブル
- シリアルケーブルキット（設定用シリアルケーブル、変換アダプター）
- クイックスタートガイド
- CD-ROM （Serial/IP Com Port Redirector, STS マネージャソフト、およびマニュアル（英文））
- 日本語ユーザーガイド （弊社ウェブサイトからダウンロード）

## 1.3. 製品スペック一覧表

| | STS800 | STS1600 |
|---|---|---|
| シリアルインターフェース | 8 ポート | 16 ポート |
| | 通信速度 75bps～230Kbps | |
| | フロー制御： ハードウェア RTS/CTS, ソフトウェア Xon/Xoff | |
| | RJ45 コネクタ | |
| | シグナル<br>RS232 RX, Tx, RTS, CTS, DTR, DSR, DCD, GND | |
| | モデム制御： DTR, DSR, および RTS/CTS | |
| ネットワークインターフェース | 10/100 Base-Tx Ethernet<br>RJ-45 Ethernet コネクタ | |
| | 静的/動的 IP アドレスをサポート | |
| プロトコル | -ARP, IP/ICMP, TCP, UDP, Telnet, SSH v1&v2<br>-SSLv2&v3, TLSv1<br>-DNS, Dynamic DNS, HTTP, HTTSTS,<br>-SMTP, with/without Authentication, pop-before SMTP<br>-DHCP client, NTSTSNMP v1&v2 | |
| PCMCIA | 下記のうち一つ：<br>ATA flash memoru card<br>802.11b 無線 LAN カード<br>10/100 Base-TX LAN カード<br>モデムカード | |
| セキュリティ | ユーザーID ＆パスワード | |
| | HTTSTS | |
| | セキュア端末インターフェース SSH | |
| | データ暗号化： SSLv3 | |
| | IP アドレスフィルタリング | |
| | SCP | |
| モデム・エミュレーション | AT コマンドのフルサポート | |
| 管理 | Web, Telnet, SSH, シリアルコンソールポート Hello Device Manager | |
| | サポート O/S: Windows 98,/ME/NT/2000/XP | |
| | システムログ エラーログの自動 e-mail 送信 | |
| | システム解析 全機能状態の表示 | |
| | ファームウェア フラッシュメモリに保存、Telnet または Web 経由でアップグレード | |
| LED 表示 | Power<br>Ready<br>10/100 Base Link, Act<br>Serial in Use/Rx/Tx(各ポート);<br>PC Card | |
| 環境 | 動作時気温： 0℃から 50℃<br>保存時気温： -40℃から 66℃ | |
| 電源 | 5VDC<br>1.5A@ 5VDC | 110～240VAC |
| 寸法 LxWxH(mm) | 245x153x30(mm) | 432x193x44.5(mm) |
| 重量(Kg) | 1.5 | 2.8 |
| 認証 | FCC(A) CE(A) MIC | |
| 保証 | 1 年間 | |

## 1.4. 用語

このセクションではこのマニュアル内で頻繁に用いられる用語の定義を載せます。これらの用語はネットワーク技術に関するものであり、STS シリーズとの関係において定義されます。

・ **MAC アドレス**

ローカルエリアネットワーク、または他のネットワークで、MAC(Media Access Control)アドレスはコンピュータのユニークなハードウェア番号です。(Ethernet LAN では、Ethernet アドレスと同一です)。固有の 12 桁番号で、6 桁の OUI(Organization Unique Identifier)番号(会社の持つ固有識別番号)および 6 桁のハードウェア識別番号から構成されています。STS シリーズの MAC アドレスは次のような構成です: 00-01-95-xx-xx-xx。 MACアドレスは梱包箱の裏側に記載されています。

・ **ホスト**

ネットワークに接続されているユーザーPC のことです。

Internet Protocol 仕様によると、「ホスト」とは、「インターネット上の他のコンピュータと相互にアクセス可能なコンピュータのこと」と定義されます。ホストは特定の「ローカル」または「ホスト番号」を持ち、独自の IP アドレスを構成します。

・ **セッション**

2 台のホスト間で行われる通信の単位のことです。大抵、片方のホスト側がもう片方の指定したホストへ接続を要求し、相手が許可すると、お互いにデータをやりとりし始めます。接続が確立された時点でセッションは始まり、接続が切断すると、セッションも終了します。

**・クライアント/サーバー**

クライアント/サーバーは 2 つのコンピュータの仕事の違いを表し、クライアント側がサービスを要求し、サーバー側がそのサービスを提供します。

サーバーは一つまたは複数の他のコンピュータが要求するサービスをそのとおりに果たすコンピュータプログラムです。一例として、Web ブラウザは、さまざまな要求を世界中のWEBサーバーに送信し、そしてその結果を受け取ることにより、情報を得ることができます。この場合ブラウザがクライアントの役割を果たし、要求された HTML ファイルを受け取り、または返信することができます。要求を処理し、HTML ファイルを送る作業を行うコンピュータがサーバーです。

## 頭字語一覧

| | |
|---|---|
| ISP | Internet Service Provider インターネットサービスプロバイダ |
| PC | Personal Computer パソコン |
| NIC | Network Interface Card ネットワークインターフェースカード |
| MAC | Media Access Control メディア・アクセスコントロール |
| LAN | Local Area Network ローカルエリアネットワーク |
| UTP | Unshielded Twisted Pair 対より線(シールドなし) |
| ADSL | Asymmetric Digital Subscriber Line |
| ARP | Address Resolution Protocol |
| IP | Internet Protocol インターネット・プロトコル |
| ICMP | Internet Control Message Protocol インターネット制御通知プロトコル |
| UDP | User Datagram Protocol ユーザデータグラム・プロトコル |
| TCP | Transmission Control Protocol 伝送制御プロトコル |
| DHCP | Dynamic Host Configuration Protocol |
| SMTP | Simple Mail Transfer Protocol 簡易メール送信プロトコル |
| FTP | File Transfer Protocol ファイル転送プロトコル |
| PPP | Point-To-Point Protocol ポイント トゥ ポイント プロトコル |
| PPPoE | Point-To-Point Protocol over Ethernet |
| HTTP | Hyper Text Transfer Protocol ハイパーテキスト転送プロトコル |
| DNS | Domain Name Service ネームサーバー |
| DDNS | Dynamic Domain Name Service 動的ドメイン名サービス |
| SNMP | Simple Network Management Protocol ネットワーク機器管理プロトコル |
| RADIUS | Remote Access for Dial-In User Service ダイヤルインユーザーサービスの遠隔認証 |
| SSH | Secure Shell セキュアシェル |
| NTP | Network Time Protocol ネットワークタイムプロトコル |
| UART | Universal Asynchronous Receiver/Transmitter |
| BPS | Bits per second (baud rate) ボーレート |
| DCE | Data Communications Equipment |
| DTE | Data Terminal Equipment データ端末装置 |
| CTS | Clear to Send 受信準備完了 |
| DSR | Data Set Ready データセットレディ |
| DTR | Data Terminal Ready データ端末レディ |
| RTS | Request To Send 送信要求 |
| DCD | Data Carrier Detect データキャリア検出 |

# 2. 使用準備

この章では STS シリーズの使用準備および初期設定の方法を説明します。

**-2.1 パネル・レイアウト**では製品各部の説明および LED 表示の説明を行います。

**-2.2 ハードウェア機器を接続**、では電源、ネットワークケーブル、およびその他の機器の接続方法を説明します。

**-2.3 Web ブラウザ管理インターフェースにアクセス**、ではシリアルコンソールを使用してのコンソールポートへのアクセス方法およびリモート(遠隔)からの Telnet および Web メニューでのアクセス方法を説明します。

使用準備に際し、下記の物をご用意ください。

STS 用電源ケーブル(付属品) 1 本
シリアルデータケーブルおよび Ethernet ケーブル(付属品) 1 本
変換アダプター(付属品)
PC (NIC もしくは RS232 シリアルポートを有する) 1 台

## 2.1 パネル・レイアウト

### 2.1.1. STS400/800 パネル・レイアウト

STS400/800 には 3 つのグループの LED 表示があります。左側の最初の 3 つのランプは Power, Ready,PC card Interface を表示、次のランプは Ethernet 100Mbps, Link, および、Actを表示します。そしてその次のランプは各ポートの In Use, Receive および Transmit を表示します。

表 2-1 は各 LED ランプの説明です。後部パネルには RJ45 コネクタのシリアルポート、Ethernet ポート、STS400/800 コンソールポート、および電源ソケットがあります。

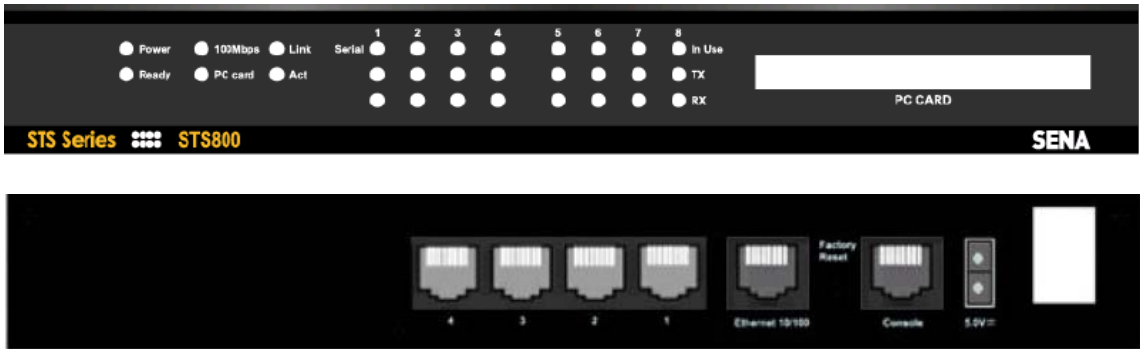


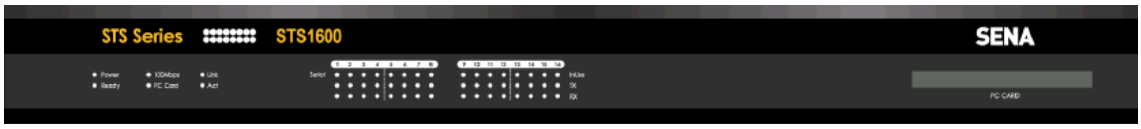

図 2-1 STS800 のパネルレイアウト

*表 2-1 STS シリーズの LED 表示一覧表*

| *LED ランプ* | | *機能* |
|---|---|---|
| *System* | *Power* | *電源が供給されると、赤色に点灯* |
| | *Ready* | *システムが起動準備完了時に点灯* |
| | *PC card* | *PCMCIA デバイスが起動時に点灯* |
| *Ethernet* | *100Mbps* | *100BASE-TX 接続が検知されると点灯* |
| | *LINK* | *イーサネット・ネットワークに接続時に点灯* |
| | *Act* | *STS シリーズのイーサネットポートを通して何らかのアクティビティがある時に点灯* |
| *Serial Port* | *InUse* | *シリアルポート使用時に点灯* |
| | Rx/Tx | STS シリーズのシリアルポートを通して何らかのアクティビティがある時に点灯 |
| | | |

### 2.1.2. STS1600 パネル・レイアウト

以下の図表に示されているように、STS1600 には 3 つのグループ（System, Ethernet, Serial Ports）の LED ランプがあり、現行ステータスを表示します。左側についている 3 つのランプは Power、Ready、および PCMCIA インターフェースの状態を表示します。その隣の3つのランプは Ethernet100Mbps, Link および Act です。次のランプは InUse、シリアルポートの送受信を表します。表 2-2 は LED 表示の一覧です。




## 2.2. ハードウェアを接続する

このセクションでは初期設定において STS シリーズ　デバイスサーバーをお使いの機器へ接続する方法を説明します。

-STS シリーズを電源につなぐ

-STS シリーズをイーサネットハブにつなぐ

-デバイスにつなぐ

### 2.2.1. 電源につなぐ

電源ケーブルを STS シリーズにつなぎます。電源が正常に供給されれば、[Power]ランプが緑色に点灯します。

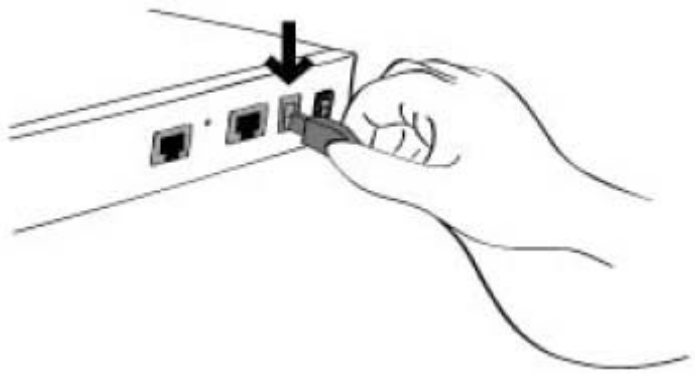


図 2-3 電源ケーブルを STS400/800 につなぐ

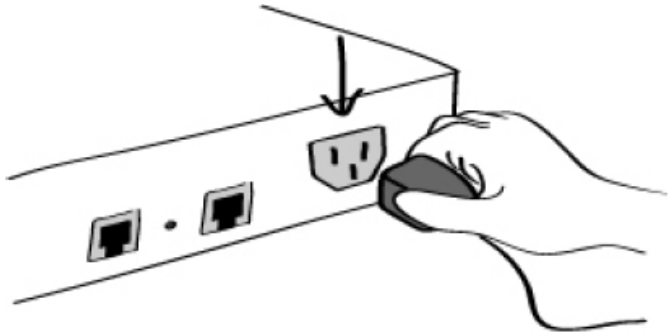


図 2-4 電源ケーブルを STS1600 につなぐ

### 2.2.2. ネットワークにつなぐ

イーサネットケーブルを STS シリーズのイーサネットポートにさしこみ、ケーブルのもう片端はネットワークポートにつなぎます。ケーブルが正しくつないであれば、STS シリーズはイーサネットネットワークに接続されます。これは以下の動作により確認できます。

[Link]ランプが緑色に点灯します。

[Act]ランプがイーサネットパケットの送受信を検知すると、点滅します。

[100Mbps]ランプは 100Base-Tx ネットワークに接続されると、緑色に点灯します。

[100Mbps]ランプは 10Base-T ネットワークに接続されても、点灯しません。

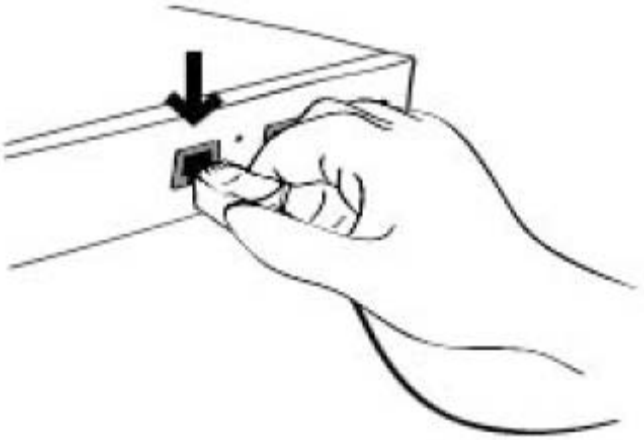


図 2-5 ネットワークケーブルを STS シリーズに接続する

### 2.2.3. 機器につなぐ

コンソールケーブルを STS シリーズのシリアルポートにつなぎます。デバイスのコンソールポートにつなぐには、デバイスのコンソールポートタイプを考慮する必要があります。STS シリーズケーブルキットパッケージには、各種変換アダプタが準備されています。

詳細は「付録 1. 接続」を参照してください。

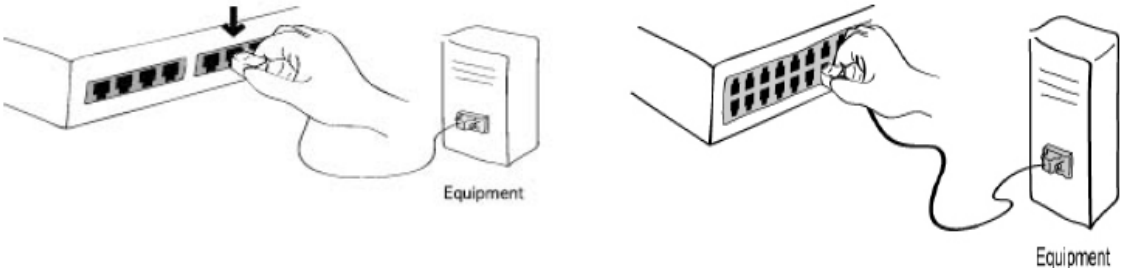



図 2-6 デバイスを STS400/800(左側)・STS1600(右側)につなぐ

### 2.2.4. システムコンソールへのアクセス

STS デバイスサーバーへのアクセス方法はいくつかあります。これらの方法はユーザーがローカル側、もしくはリモート側にいるかで変わってきます。また、メニュー表示型インターフェース、グラフィックインターフェース、または CLI(コマンドラインインターフェース)を選択することができます。

- **システムコンソール**:
  ローカルユーザーはコンソール・イーサネットケーブルと、機器に対応する変換アダプタを用いて直接 STS シリーズのコンソールポートに接続します。
- **リモート・コンソール**:

リモートのユーザーは、Telnet または SSH クライアントを使用して STS シリーズに Telnet(port23), を利用したメニュー表示型インターフェースを使用します。

- **Web:**
  STS シリーズをリモートからウェブブラウザを使用して設定する場合は、Internet Explorer または Netscape Navigator などの一般的に使用されているウェブブラウザから可能です。

上記の設定を行うには、STS シリーズシステムによるユーザー認証が必要です。

### 2.2.5. システムコンソールを使用する

1) コンソール・イーサネットケーブルの一方を STS シリーズのコンソールポートにつなぎます。

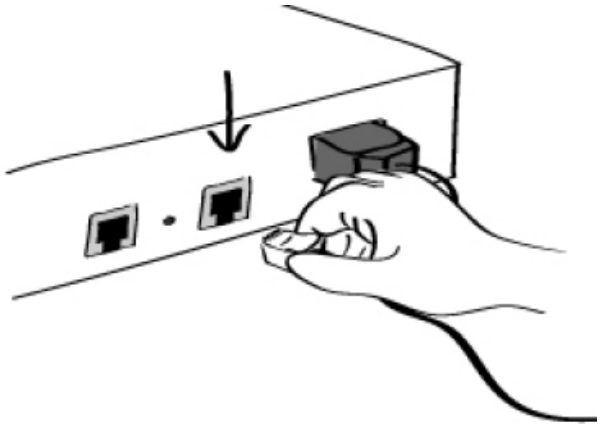


**図 2-7 STS シリーズににシステムコンソールケーブルをつなぐ**

2) 片方のシリアルケーブルの端を RJ-45-DB9 メス変換アダプターを使って設定用のコンピュータにつなぎます。
3) ケーブルのもう片方をユーザーのコンピュータのシリアルポートにつなぎます。
4) ターミナルソフトを起動します（Hyper Terminal 等）。ターミナルソフトのシリアル設定パラメータを次のように設定してください。
   - ■ 9600 Baud rate
   - ■ Data ビット 8
   - ■ Parity なし（None）
   - ■ Stop bits 1
   - ■ No flow control
5) Enter を押します。
6) ユーザー名およびパスワードを入力し STS デバイスサーバーにログインします。工場出荷時の値（Login: root/admin password: root/admin）

```
192.168.161.5 login: root
Password:****
root@192.168.161.5:~#
```

7） 認証後、CLI を使って、設定を行います。CLI に関する詳細は第 8 章、CLI ガイドを参照してください。

8） “ss.edit”コマンドでテキストメニューインターフェースに入ることができ、メニュー画面に行きます。図 2-8 が表示されます。

```
root@192.168.161.5:~#ss.edit

--------------------------------------------------------------------------------
 Welcome to STS-800 configuration page
 Current time: 08/22/2003 21:52:36     F/W REV.: v1.0.1
 Serial No.: STS800438349-42944        MAC address: 00-01-95-04-19-5a
 IP mode: DHCP                         IP address: 192.168.14.7
--------------------------------------------------------------------------------
 Select menu:
  1. Network configuration
  2. Serial port configuration
  3. PC Card configuration
  4. System administration
  5. Save changes
  6. Exit without saving
  7. Exit and apply changes
  8. Exit and reboot
  <Enter> Refresh
 ----->
```

**図 2-8 メインメニュー画面（STS800）**

メインメニュー画面から、メニュー番号を選択し Enter をクリックして、設定用のメニューアイテムを選択します。サブメニュー画面では、オンラインコメントによる必要なパラメータの設定を行なうことができます。全てのパラメータは STS シリーズの不揮発性メモリスペースに保管されますが、設定はメニューで Save コマンドを入力しないかぎり保管されません。

全ての変更はメニュー画面で、“Apply”コマンドを入力した時点で有効になります。

### 2.2.6. リモート・コンソールを使用する

リモート・コンソールで STS デバイスサーバーにアクセスする前に、IP アドレスを事前に確認してください。（詳細は 3 章 ネットワーク設定を参照）。STS シリーズのデフォルト IP アドレスは、192.168.161.5 です。

リモートホストアクセスオプションにてリモートコンソールアクセス機能を OFF にすることができます（3.5 IP フィルタリングを参照してください）

次にリモート・コンソール機能の設定について説明します。

1） Telnet プログラムまたは Telnet 機能を持つプログラムを起動します（Tera-Term Pro または HyperTerminal など）。IP アドレスおよびポート番号が STS シリーズと同一かどうかを確認します。

状況に応じ、ポート 23 を指定します。

コマンドライン上に以下のコマンドを入力します。

Telnet 192.168.161.5

または以下のパラメータにより Telnet プログラムを起動します。

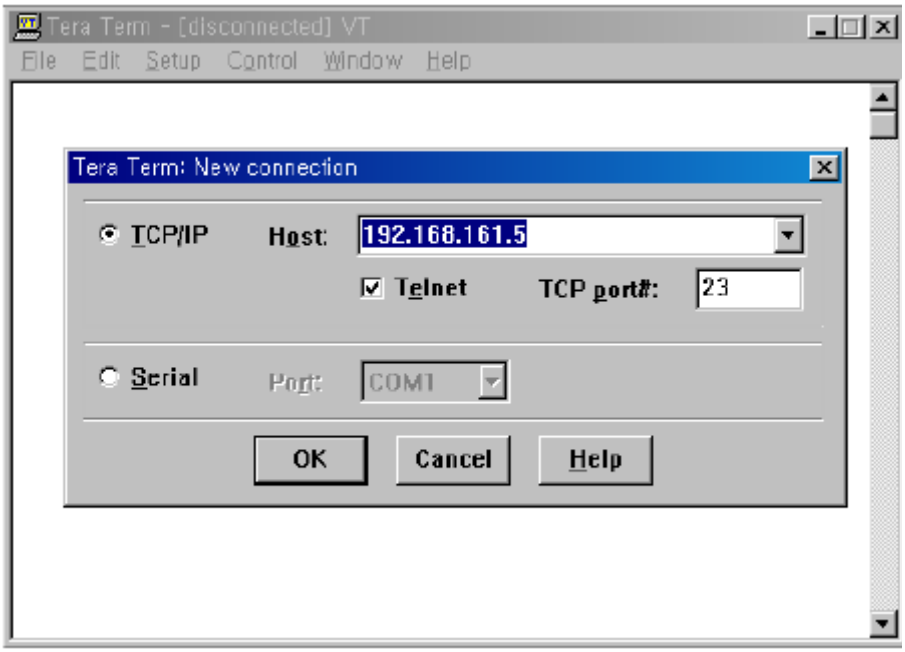



**図 2-9 Telnet プログラム設定例(Tera Term Pro)**

2) STS シリーズにログインします。ユーザー名およびパスワードを入力してください。(root)システム管理者の場合は(admin).

3) ユーザー名およびパスサードを入力後認証が行われ、CLI のコマンドラインプロンプトが表示されます。

## 2.3. ウェブブラウザ管理インターフェースにアクセス

STS シリーズは HTTP および HTTPS プロトコルをサポートしています。STS シリーズには独自の WEB 管理ユーティリティもあります。STS シリーズのウェブ管理ユーティリティにアクセスするには、ウェブブラウザの URL フィールドに STS シリーズの IP アドレスまたはホスト名を入力します。すると、ログイン画面が表示されます。このときに認証が行なわれ、ログイン名およびパスワードを正しく入力してください。工場出荷時(ファクトリ・デフォルト)の ID およびパスワードは(Login: root/admin Password: root/admin)です。

**注記:STS シリーズウェブ管理ページにアクセスする前に、STS シリーズの IP アドレスおよびサブネットマスク設定を確認してください。**

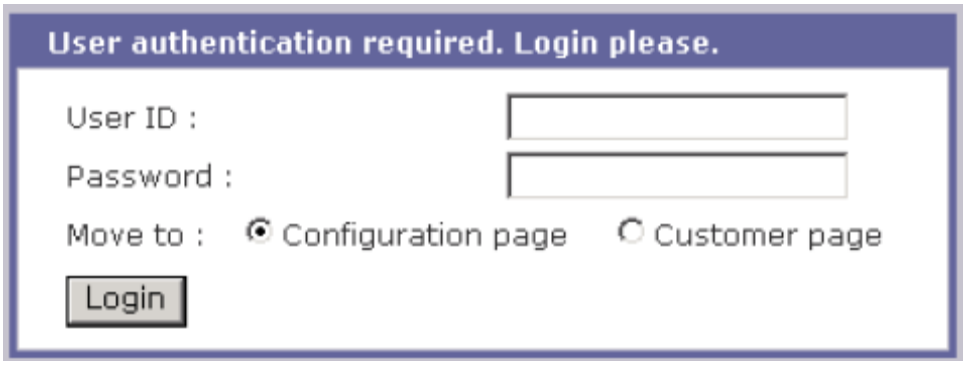



**図 2-10 STS シリーズウェブ管理インターフェースのログイン画面**

次の図 2-10 は STS シリーズのウェブ管理インターフェースの設定用ページです。ログイン後、認証後に最初に表示するページを選択します。Configuration のページを選択すると、図 2－11 にあるような STS シリーズのウェブマネージメント画面が表示されます。もし Customer ページを選択すると、STS シリーズのデフォルトカスタマーサービスページか、またはユーザー任意のページが表示されるようになります。ウェブのカスタマイズについては、「*9.ユーザーカスタマイズガイド*」を参照してください。

図 2-11 は、STS シリーズウェブ管理インターフェースの初期設定です。左側にメニューバーがあります。メニューバーには最優先の設定項目があります。メニューバー内のグループを選択すると、ツリー構造が表示され、それぞれのグループ内のさらに詳細な設定項目を選択可能になります。全てのページには[Save to flash]、[Save&Apply]または[Cancel]を選択可能です。設定パラメータ値を変更した後、[Save]をクリックすることにより、変更点が保存されます。それらの変更を有効にするには、ApplyChanges ボタンをクリックします。このオプションはメニューバーの一番下に位置しています。Apply changes ボタンをクリックして初めて変更した項目が有効になります。新規に設定した項目を保存したくない場合は、Cancel ボタンをクリックします。全ての変更点は失われ、以前に設定した項目が復帰します。しかし、すでに Save した項目はそのまま保存されます。

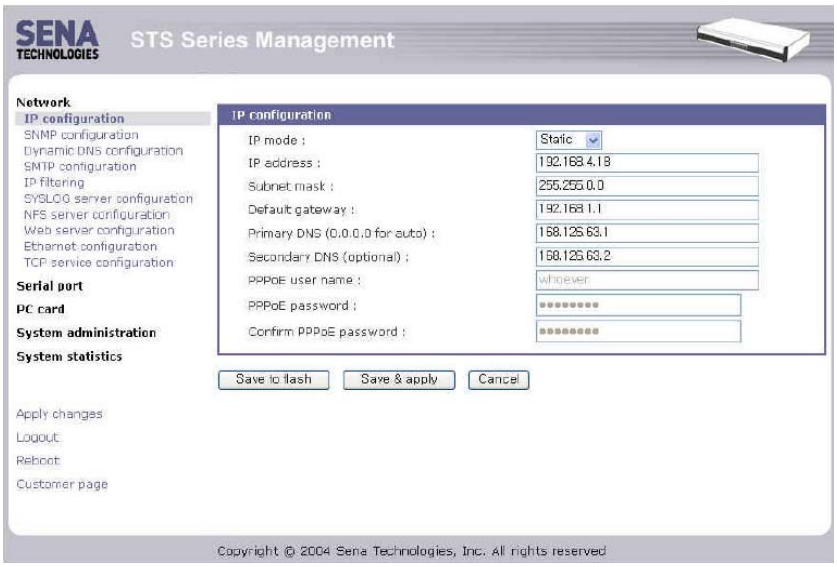



**図 2-11 STS シリーズウェブ管理画面**

# 3. ネットワーク設定

## 3.1 IP 設定

STS シリーズはユーザーのネットワーク環境内で操作するための IP アドレスが必要なので、システム管理者から IP アドレスを入手してください。STS シリーズは、ユーザーネットワークにつなげるために独自の IP アドレスを必要とします。

STS シリーズの IP アドレスを設定するには、3 種類のインターネット・プロトコルから選択することができます。

- Static（静的）IP
- DHCP
- PPPoE

STS シリーズの初期値は STATIC モードに設定されています。デフォルトの IP アドレスは 192.168.16.5 です。表 3-1 には 3 種類全ての IP 設定が表示されています。図 3-1 には実際のウェブ GUI でユーザーの IP 設定の変更する図がのせられています。

表 3-1 IP 設定パラメータ

| | |
|---|---|
| **Static IP** | IP address |
| | Subnet mask |
| | Default gateway |
| | Primary DNS/ Secondary DNS |
| **DHCP** | Primary DNS/ Secondary DNS (Optional) |
| **PPPoE** | PPPoE Username |
| | PPPoE Password |
| | Primary DNS/ Secondary DNS (Optional) |

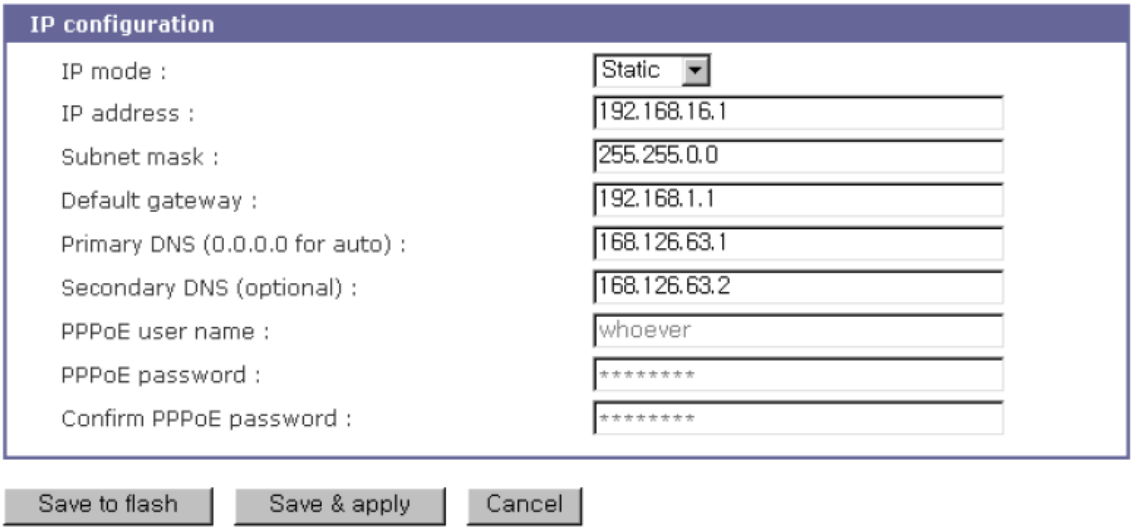



図 3-1 IP 設定

### 3.1.1. Static(静的)IP アドレスを使用する

Static IP アドレスを選択すると、ユーザーが手動で STS の IP アドレスに関連する全てのパラメータを設定します。それには IP アドレス、ネットワーク・サブネットマスク、ゲートウェイ・コンピュータおよびドメインネームサーバーなどが含まれます。このセクションではそれらの詳細を解説します。

**注記:STS は毎回起動時にこれら全ての情報を取得します。**

- **IP アドレス**

静的 IP アドレスは「静的」または永久の ID 番号となります。この番号は「ネットワーク上の場所を知らせるアドレス」として割り当てられます。コンピュータはこれらの IP アドレスでネットワーク上において、お互いを識別し、コミュニケーションをとります。それゆえに、IP アドレスはそれぞれユニークであり、かつネットワーク環境のみに限定された IP アドレスです。
注記:192.168.1.x は ISP(インターネットサービスプロバイダー)によって割り当てられるものではなく、プライベート・アドレスとみなされます。インターネットのような公衆ネットワークにアクセスする必要がある場合には、公衆 IP アドレスを割り当てます。

- **サブネットマスク**

サブネットは 1 つの場所、ビルやローカルネットワーク(LAN)のようなネットワークホストを代表します。STS モデルはサブネットマスク設定で全てのパケットの源を調べます。 もしパケットによって指定された TCP/IP ホストがサブネットマスクによって定義された同じ場所(同じローカルネットワークセグメント)にある場合、STS モデルは直接接続を確立します。もしパケットによって指定した TCP/IP ホストがローカルネットワークセグメントに属していないと識別されるなら、接続はデフォルトのゲートウェイを通して確立されます。

- **デフォルトゲートウェイ**

ゲートウェイは、他のネットワークへの入場門(ポータル)として動作するネットワークポイントです。このポイントは大抵コンピュータまたはネットワーク内のトラフィックを制御するコンピュータ、またはローカル ISP です。STS モデルはデフォルトゲートウェイコンピュータの IP アドレスを使い、ローカルネットワーク環境外のコンピュータと通信します。

- **プライマリ・セカンダリ DNS**

DNS(Domain Name System)サーバーは要求されたウェブサイトアドレスに対して正しい IP アドレスに変換し、指定します。ドメイン名とはウェブアドレス(例 www.intersolutionmarketing.com)のことであり、覚えやすいものです。DNS サーバーはそのようなテキストで書かれたドメイン名を数字の IP アドレスに変換し、TCP/IP 接続を可能にします。
DNS サーバーの IP アドレスは与えられたドメイン名でホストサイトにアクセスを可能にします。STS モデ

ルはプライマリおよびセカンダリ DNS サーバーのアドレスを設定する機能があります。(セカンダリ DNS サーバーはプライマリ DNS サーバーが使用不可のときに使用します。

### 3.1.2. DHCP を使用する

DHCP とはネットワーク管理者が組織のネットワークで IP アドレスを自動的に割り当てる管理を行なうプロトコルのことです。DHCP はネットワーク管理者が一箇所から IP アドレスを監視、割り当て、またコンピュータが異なるネットワーク環境に接続されると、自動的に新しい IP アドレスを割り当てます。Static IP モードの時は、IP アドレスは手動で各コンピュータの分を入力する必要があります。コンピュータが新しいネットワーク環境に移動したら、その都度 IP アドレスを割り当てる必要があります。DHCP は IP アドレスが割り当てるとともに、全てのパラメータ、IP アドレス、サブネットマスク、ゲートウェイ、および DNS サーバーが自動的に設定されます。DHCP は IP アドレスをコンピュータに割り当てる時に、「リース(限定期間の貸し出し)」のようなコンセプトで行ないます。そのコンピュータに割り当てられた IP アドレスは一定期間しか有効ではありません。IP アドレスを割り当てるために必要な全てのパラメータは自動的に DHCP サーバー側で設定され、それぞれの DHCP クライアントコンピュータは IP アドレスがブートアップ時に割り当てられる時にこの情報をうけとります。

コンピュータがリセットされる度、STS シリーズはネットワークに DHCP 要求をブロードキャストします。DHCP サーバーは返信を生成し、IP アドレス、サブネットマスク、ゲートウェイアドレス、DNS サーバー、また有効期限の情報を送信します。STS シリーズはそれらの情報を内部メモリに保存します。有効期限が切れると、STS シリーズは DHCP サーバーに更新要求を送信します。DHCP サーバーが更新を許可すると、STS シリーズはそのままその IP アドレスを使用することができます。DHCP サーバーが更新を拒否すると、STS シリーズは DHCP サーバーに新規 IP アドレスを要求します。

**注記:DHCP モードの時は、DNS サーバーを含む STS モデルの全てのネットワーク関連パラメータは自動的に設定されます。DNS サーバーが自動的に設定されない場合は、ユーザーはプライマリおよびセカンダリ DNS IP アドレスを手動で設定する必要があります。DNS アドレスの自動設定を強制的に行うには、プライマリおよびセカンダリ IP アドレスの値を 0.0.0.0 にします。**

DHCP サーバーはネットワーク管理者によって管理されている IP アドレスプールの中から動的に IP アドレスを割り当てます。これは DHCP クライアントが毎ブート時に、異なる IP アドレスを受け取るようになります。IP アドレスはユーザーが常に最新の STS の IP アドレスを知ることができるように DHCP サーバー側に保管してください。DHCP ネットワーク内の IP アドレスを保存するには、管理者が STS サーバーの底面に貼られているラベルステッカー記入されている MAC アドレスが必要です。

### 3.1.3 PPPoE を使用する

PPPoE は、イーサネット LAN(ローカルエリアネットワーク)上の複数のユーザーがモデムを通してリモートサイトに接続するためのものです。PPPoE を使用すると、複数のユーザーが ADSL、ケーブルモデム、または無線接続でインターネットを共有することができます。

PPPoE モードを使用するために、PPPoE のアカウントおよび ADSL モデム等の必要環境を事前に整える必要があります。STS シリーズは PPPoE プロトコルに対応しているので、PPPoE アカウント用のユーザー名およびパスワードを設定してください。

STS シリーズはブートアップ時に PPPoE サーバーへの接続を行います。接続時に STS シリーズは IP アドレス、ゲートウェイ、サブネットマスクおよび DNS サーバー情報を受け取ります。接続が確立すると、STS シリーズはその接続を維持します。接続が切断されると、STS シリーズは新規の接続を要求し、再接続を行います。

**注記： PPPoE モードの時は、DNS サーバーを含むすべてのネットワーク関係のパラメータが自動的に設定されます。DNS サーバーが自動的に設定されない場合は、ユーザーはプライマリおよびセカンダリ DNS IP アドレスを手動で設定する必要があります。DNS アドレスの自動設定を強制的に行うには、プライマリおよびセカンダリ IP アドレスの値を 0.0.0.0 にします。**

## 3.2. SNMP 設定

STS モデルには SNMP v1 および v2 プロトコルをサポートしている SNMP エージェントプロトコルがあります。NMS または SNMP ブラウザのようなネットワーク管理者は STS モデルと情報を交換可能で、必要な機能にアクセスすることもできます。

SNMP プロトコルは GET, SET, GET-Next,および TRAPs を含んでいます。これらの機能で管理者は重要なイベント（TRAPs）を通知されるようになり、さらなる情報を入手したり（GET）、デバイスの状態を変更したりすること（SET）が可能です。SNMPv2 は情報テーブルを入手したり、セキュリティ機能のための GET-Bulk 機能を追加したりします。

SNMP 設定パネルで、MIB-II システムオブジェクト、アクセスコントロール設定、および TRAP 受信設定を行なうことができます。このメニューで設定したマネージャは情報交換および動作制御に使われます。

図 3-2 はウェブインターフェース経由の SNMP 設定画面です。

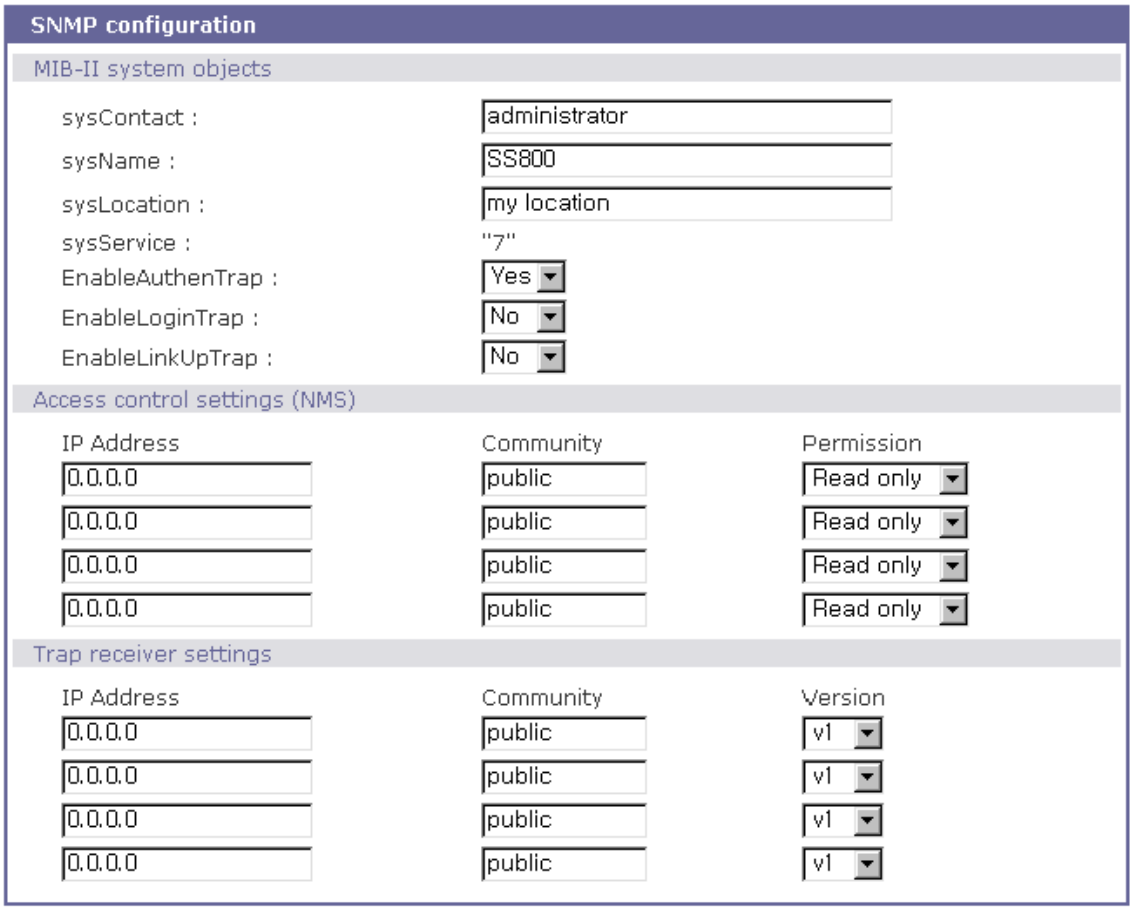



**図 3-2 SNMP 設定**

### 3.2.1. MIB-II システムオブジェクト設定

MIB-II システムオブジェクト設定はシステムコンタクト、名称、および STS モデルの SNMP エージェントによって使用された認証エラートラップを設定します。これらの設定は MIB-II sysName, sysContact, sysLocation, sysService および enableAuthenTrap に使用する値になります。
各機能の簡単な説明を以下に挙げます。

- **sysContact:** STS モデル用のコンタクト情報の ID、およびどのように連絡を取ることができるかの説明。
- **sysName:** システムを見分けるために使用される名前。規則により、これはノードのドメイン名として十分資格があります。
- **sysLocation:** システムの物理的な位置情報(Room 384, Operation Lab, etc.)
- **sysService**(読み取り専用): 連続する値、カンマによって区切られており、システムが提供するサービスの設定を表示します。初期値では、STS モデルはアプリケーション(7)サービスレベルです。
- **EnablePoweronTraSTS:** SNMP エージェントプロセスが Power-on トラップを生成するの

を許可されているかどうかを表示します。

- **EnableAuthenTraSTSNMP:** エージェントプロセスが認証エラートラップを生成することが許可されているかどうかを表示します。このトラップはとても強力で、他のどのようなトラップよりも優先されるため、他のトラップが OFF になることもあります。
- **EnableLoginTraSTSNMP:** エージェントプロセスがコンソール、telnet,およびWebアクセス用にシステムログイントラップを許可しているかどうかを表示します。

MIB を追加、または変更したい場合は,弊社技術サポートまでお問い合わせください。

info@intersolutionmarketing.com

MIB および SNMP に関する詳細情報は、RFC の 1066, 1067, 1098, 1317, 1318, 1213 を参照してください。

### 3.2.2. アクセスコントロール設定

アクセスコントロールとは、マネージャが STS の SNMP エージェントへの「アクセシビリティ」と定義することができます。このメニューで設定したマネージャのみが STS の SNMP エージェントへアクセスし、情報を交換したり、動作の制御を行なうことができます。もし特定の IP アドレスが指定されていなければ、(全ての初期 IP アドレスは 0.0.0.0.です)全てのホストからのマネージャは STS の SNMP エージェントにアクセス可能です。

### 3.2.3. トラップレシーバー設定

トラップレシーバーは STS の SNMP エージェントからの重要なイベント(TRAP)を通知するマネージャです。

### 3.2.4. SNMP を使用したマネージメント

STS モデルは NMS(Network Management System)または SNMP ブラウザを使用して SNMP プロトコルを通して管理可能です。NMS または SNMP ブラウザを使用する前に、ユーザーはアクセスコントロールを正しく設定することにより STS シリーズは NMS または SNMP ブラウザを実行するホストアクセスを許可することになります。

図 3-3 では典型的な STS シリーズの SNMP エージェントの MIB-II を持つ SNMP ブラウザです。

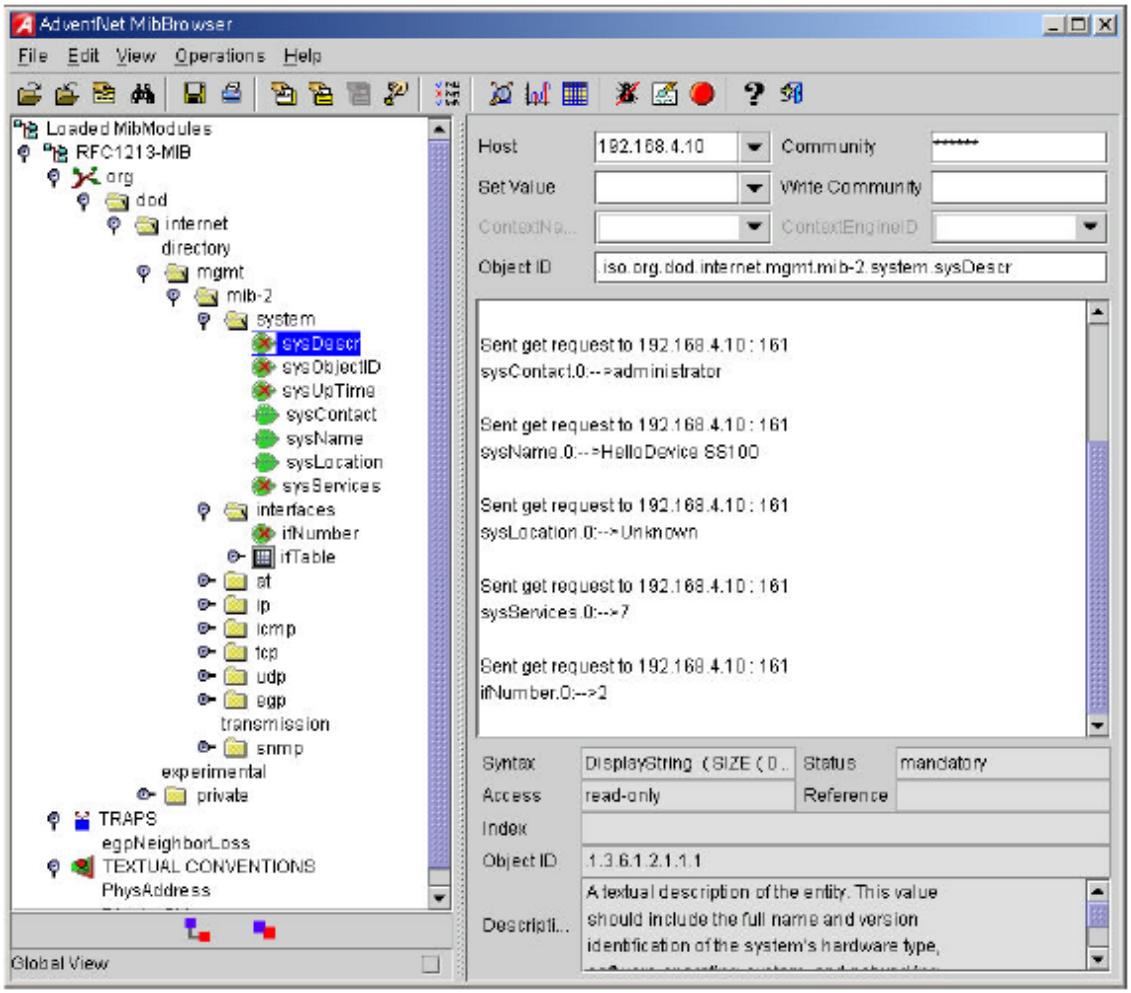



**図 3-3 SNMP ブラウザで STS の SNMP エージェントのMIB-II OIDs をブラウズ**

## 3.3 動的 DNS 設定

STS シリーズで DSL ラインに接続する、もしくは DHCP 設定を行なう時、ネットワークに再接続する度に IP アドレスが変わることがあります。そのためそれぞれの新しい IP アドレスに関連した全てのコンタクトを通知するのは、非常に難しいといえます。加えて管理者がリモート・コンソール以外のアクセス手段がない場合、現在の IP アドレスが何であるか、または変更されたのかどうかもわかりません。

動的 DNS サービスは上記の問題に取り組むために多くの ISP で扱われています。動的 DNS サービスを使うことによって、IP アドレス変更があったとしてもユーザーは動的 DNS サーバーに登録したホスト名で STS シリーズにアクセス可能になります。

デフォルト値では、STS シリーズは Dynamic DNS Network Services, LLC(www.dyndns.org)によって提供されている動的 DNS サービスをサポートしています。他の DNS サービスのサポートに関しては、弊社サポートまでご連絡ください。(info@intersolutionmarketing.com)

Dynamic DNS Services 社により提供された動的 DNS サービスを使うには、ネットワーク情報センター(NIC http://members.dyndns.org)にてメンバー登録を行なう必要があります。それから Dynamic DNS

Network Service 社のメンバーとしてログインして新規の動的 DNS ホストリンクを追加することができます。

Dynamic DNS Configuration メニューで動的 DNS サービスの設定を ON にした後、登録済みのドメイン名、ユーザー名、およびパスワードを入力します。設定変更を有効（Apply）した後、ドメイン名のみで STS シリーズにアクセスすることができます。

図 3-4 では動的 DNS 設定のウェブ画面を表示しています。

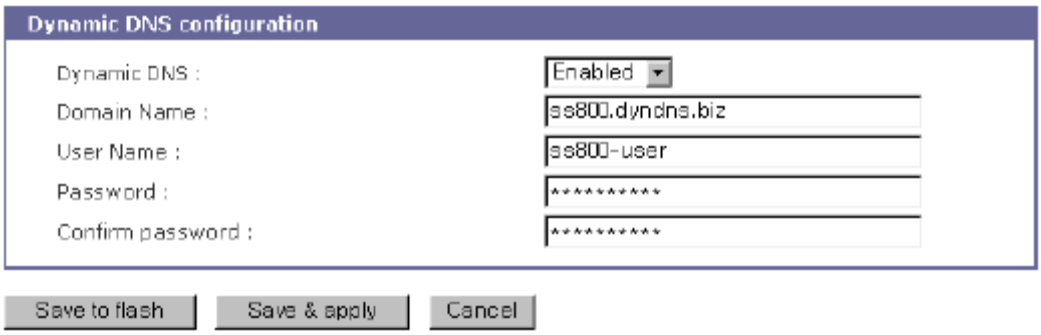



**図 3-4 動的 DNS 設定画面**

## 3.4. SMTP 設定

STS モデルはシステムログメッセージがある一定の値に達すると、またはシリアルポートデータによる特定の問題に対するアラート（警告）メッセージを e-mail にて送ることができます。SMTP サーバーがこれらの自動的に生成された e-mail を送信するように設定する必要があります。STS モデルは、3 種類の SMTP サーバータイプをサポートしています。

- SMTP without authentication （認証なしの SMTP）
- SMTP with authentication （認証が必要な SMTP）
- POP-Before-SMTP

これらの例は図 3-6 にあります。各 SMTP 設定には次のようなパラメータが含まれます。

- SMTP Server Address (SMTP サーバーの IP アドレス)
- SMTP user name (SMTP ユーザー名)
- SMTP user password (SMTP ユーザーパスワード)
- Device mail address (デバイスメールアドレス)

デバイスメールアドレスは全てのログおよびアラーム配信 email 用の送り主の email アドレスを指定します。SMTP サーバーは有効性を確認するために頻繁に e-mail アドレスの送り主のホストドメイン名のみを確認します。結果としてデバイス用に設定した email アドレスは登録したホスト名で任意のユーザー名を使用することができます。

SMTP ユーザー名および SMTP ユーザーパスワードは SMTP with authentication または POP-before-SMTP モードが選択されたときに必要となります。

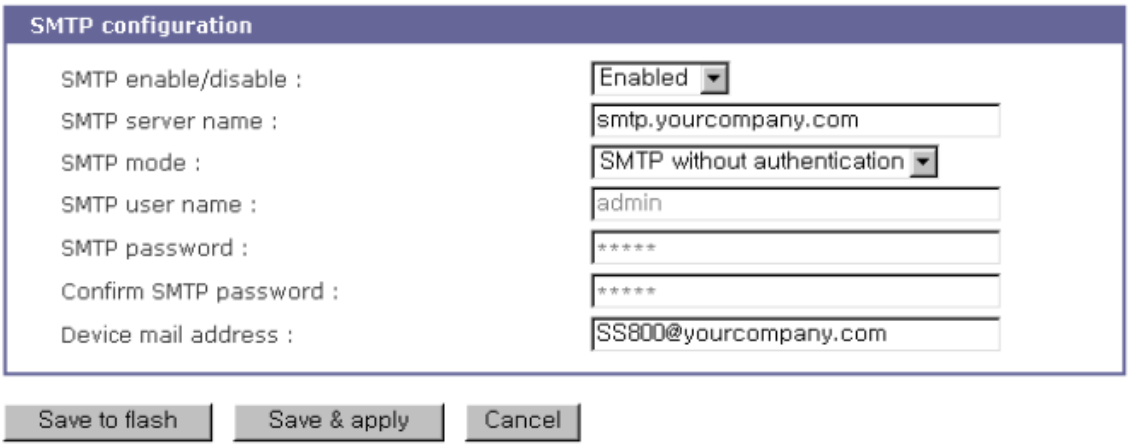



**図 3-5 SMTP 設定画面**

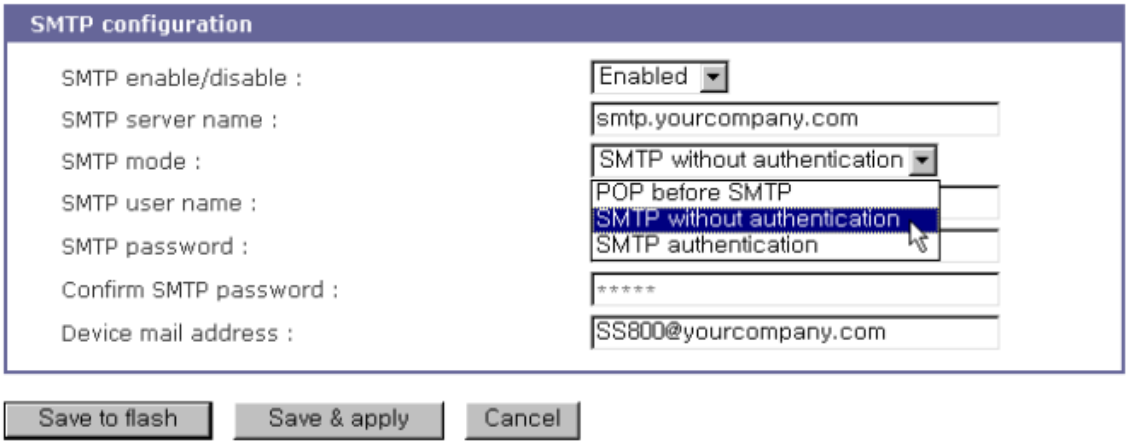



**図 3-6 SMTP 設定の SMTP モード選択画面**

## 3.5. IP フィルタリング

STS シリーズは、フィルタリング方式を用いて IP アドレスを使用しての許可されていないアクセスから保護します。パラメータ設定を変更することにより次の動作を設定します。

- Only one host of a specific IP address can access a specific service of the Pro Series
  （指定した STS シリーズには特定の IP アドレスを持つ 1 つのホスト以外アクセス不可）
- Hosts on a specific subnet can access a specific service of the Pro Series
  （指定したサブネットのホストは指定した STS シリーズにアクセス可）
- Any host can access a specific service of the Pro Series
  （全てのホストはどの STS シリーズにもアクセス可）

IP フィルタリング機能は Telnet コンソール、SSH コンソール、ウェブサーバーからのアクセスを制御

(enabled/disabled)します。このフィルタリング機能のデフォルト値は、"enabled"です。
STS デバイスサーバーの設定する権限のあるホストを割り当てます。そのためにアクセス用の IP アドレスおよびサブネットを入力します。リモートホストにいるユーザーは設定をするためにアクセスするには、指定されたサブネット範囲内にいる必要があります。
一つのホストのみに STS シリーズの設定アクセス権を持たせる場合、特定のホストの IP アドレスを入力し、サブネットには 255.255.255.255 を入力してください。
STS シリーズの設定を誰でもできるように設定する場合、IP アドレスおよびサブネットの値に 0.0.0.0 を割り当てます。
表 3-2 を参照してください。

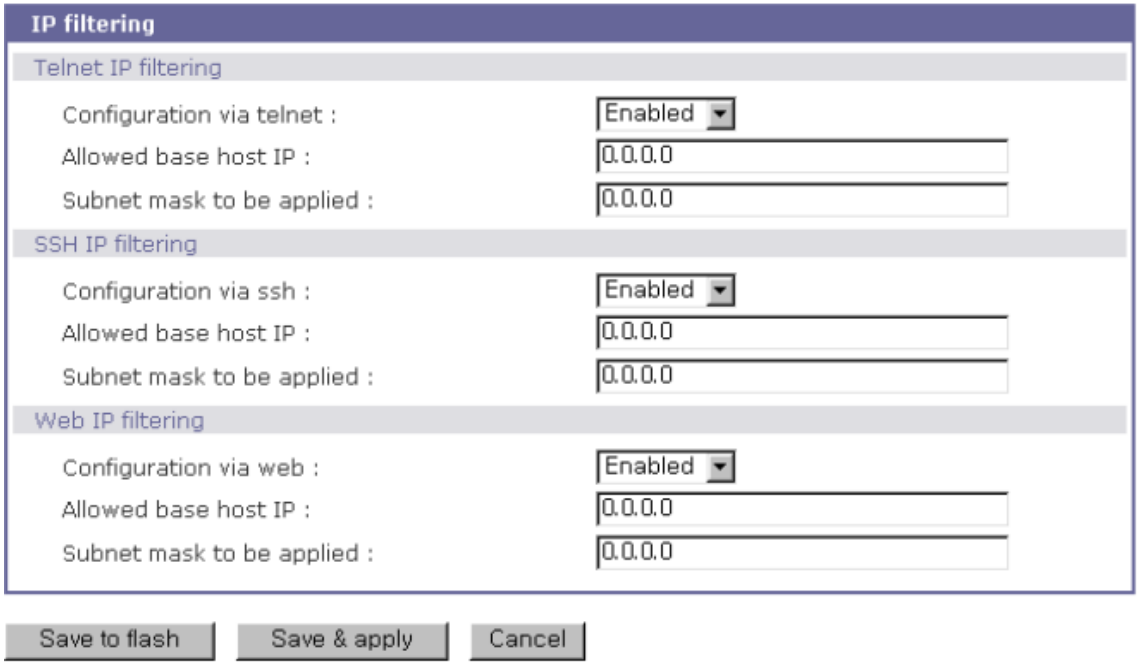



**図 3-7 IP フィルタリング設定画面**

**表 3-2 許可するリモートホストの入力例**

| Allowable Hosts | Input format | |
|---|---|---|
| | Base Host IP address | Subnet mask |
| Any host | 0.0.0.0 | 0.0.0.0 |
| 192.168.1.120 | 192.168.1.120 | 255.255.255.255 |
| 192.168.1.1 ~ 192.168.1.254 | 192.168.1.0 | 255.255.255.0 |
| 192.168.0.1 ~ 192.168.255.254 | 192.168.0.0 | 255.255.0.0 |
| 192.168.1.1 ~ 192.168.1.126 | 192.168.1.0 | 255.255.255.128 |
| 192.168.1.129 ~ 192.168.1.254 | 192.168.1.128 | 255.255.255.128 |

Web アクセスにも IP フィルタリング機能を使用します。この機能は Enabled または Disabled にします。ファクトリデフォルト値は“Enabled”です。Enabled のときは、ユーザーは設定用に STS シリーズにアクセス可能なウェブホストを指定することが可能です。

## 3.6. SYSLOG サーバー設定

STS シリーズは、SYSLOG サービスという、リモートメッセージ・ロギングサービスをサポートしています。この SYSLOG でシステムおよびポートデータのロギングを行ないます。リモート SYSLOG サービスを行なうには、SYSLOG サーバーの IP アドレスおよび使用する施設を指定する必要があります。図 3-8 は、ウェブインターフェース上にある SYSLOG サーバー設定画面です。

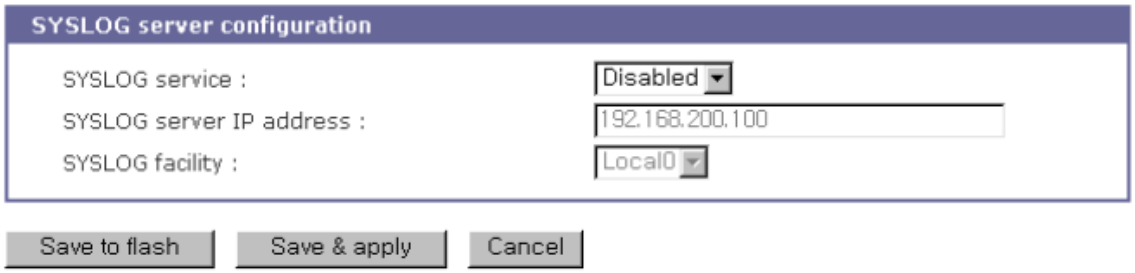



**図 3-10 SYSLOG サーバー設定**

STS シリーズからのログメッセージを受信するには、SYSLOG サーバーは”remote reception allowed”、に設定します。ファイアーウォールが設定してある場合、UDP パケットが行き来できるようにファイアーウォールの設定を変更してください。

STS シリーズは loca10 から loca17 まで SYSLOG 機能をサポートしています。これらの機能を用いて SYSLOG サーバーとは別に STS シリーズ内にメッセージを保存可能です。

SYSLOG サーバーを ON にして、SYSLOG サーバーが正しく設定されていれば、システムログまたはポートデータログの保存先、を指定できます。ポートデータログ、およびシステムログの保存先に関しての詳細は 4.2.11. ポートロギングおよび 6.2. システムロギングを参照してください。

## 3.7. NFS サーバー設定

STS シリーズは NFS（Network File System）サービスをサポートしており、システムおよびポートデータロギング機能を持っています。NFS サーバーの IP アドレスを指定する必要があり、NFS サーバーにパスを設定する必要があります。 図 3-12 はウェブ設定インターフェースにある NFS サーバー設定画面です。

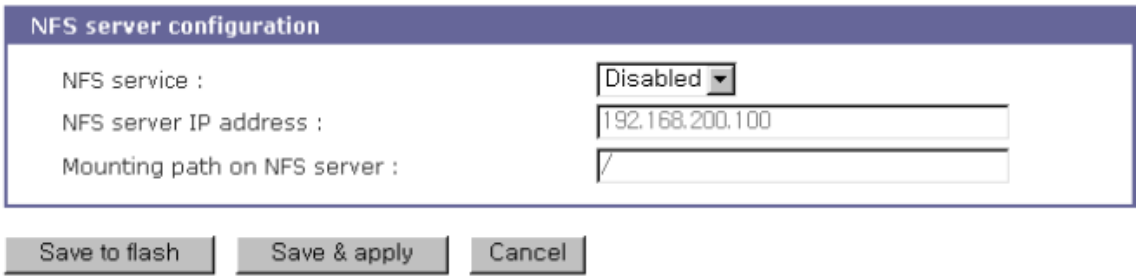



**図 3-9 NFS サーバー設定画面**

STS シリーズのログデータを NFS サーバーに保存するには、NFS サーバーは”read and write allowed”に設定する必要があります。ファイアーウォールが設定されている場合は、NFS サーバーとの間でパケットのやり取りができるように設定してください。

NFS サービスが ON になっており、正しく設定されている場合は、ユーザーはシステムログまたはデータログ用に保存場所を指定します。この場合もファイアーウォールを UDP パケットが通り抜けることができるように設定をしてください。

詳細情報に関しては 4.2.11 ポートロギング、および 6.2.システムロギングを参照してください。

## 3.8. Ethernet 設定

STS シリーズには様々な Ethernet モードがあります。

-Auto negotiation

-100 BaseT Half Duplex

-100 BaseT Full Duplex

-10 BaseT Half Duplex

-10 BaseT Full Duplex

Ethernet モードの変更後、リブートを行ってください。ファクトリデフォルト値は Auto Negotiation モードになっています。ほとんどの環境において Auto Negotiation モードは最適に動作するので推奨します。Ethernet モード設定が正しくないと、STS シリーズはネットワーク上で動作しません。

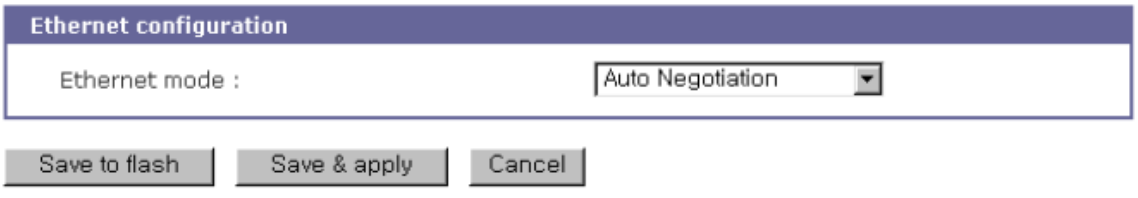



**図 3-10 Ethernet モード設定画面**

## 3.9. Web Server 設定

Web サーバーは同時に HTTP および HTTPS サービスをサポートしています。ユーザーはそれぞれ Enable または Disable と選択することが可能です。図 3-11 は WebServer 設定ページです。

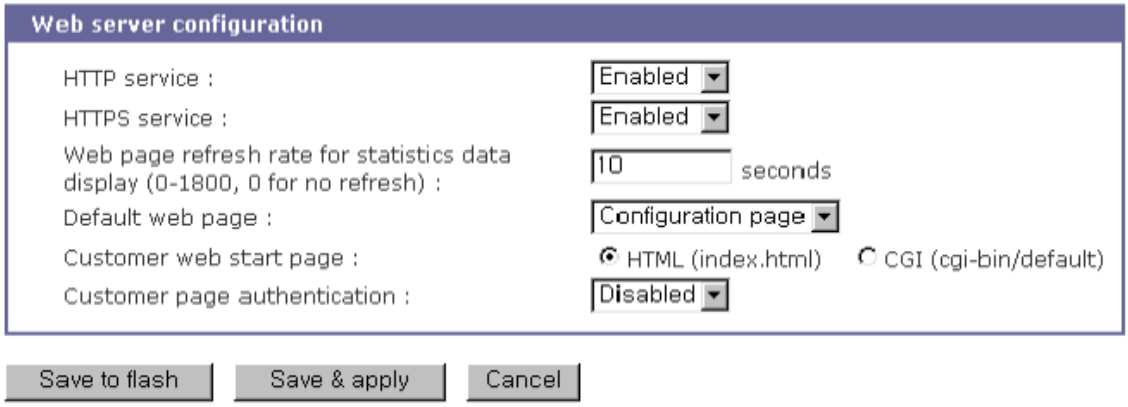



**図 3-11 Web Server 設定ページ**

"Web page refresh rate"はこのページ内で設定することができます。その設定は、ネットワークインターフェース、シリアルポート、IP,ICMP,TCP および UDP のようなシステム解析ページのみ有効です。Web インターフェースの他のページは自動的に更新されません。システム解析に関する詳細な情報は *7 章、「システム解析」*を参照してください。

この設定メニューページで、Web ユーザーインターフェースにログインした時のスタートページを選択することができます。ファクトリデフォルトのスタートページは、Configuration ページですが、これを Customer ページに変更可能です。スタートページを Customer ページにすると、/usr2 ディレクトリにある HTML(index.html)または CGI(default)の一つを Customer ウェブのスタートページとして設定します。お使いになる環境の必要に応じてこのページをカスタマイズします。ユーザーID またはパスワードなしでアクセス可能に設定するには、customer page authentication（カスタマーページ認証）機能を disable(オフ)にしてください。ウェブページのカスタマイズ機能に関しては、*9.3「ユーザー定義のウェブページ」*を参照してください。

## 3.10. TCP サービス設定

2 つのホスト同士間で TCP セッションが確立された場合、その接続は対応する TCP ポートのロックアップを避けるために、どちらかのホストで閉じられる必要があります。このようなロックアップを避けるために、STS シリーズには TCP Keep Alive 機能があります。 STS シリーズは定期的にネットワークを通してパケットをやりとりし、ネットワークが存在するかどうかを確認します。リモートホストからの応答がない場合は自動的にその TCP セッションは閉じられます。

STS シリーズの TCP Keep-alive 機能を使用するには、次の 3 種類の方法があります。

- **TCP keep-alive time:**

  これは STS シリーズが最後に受け取ったパケットの時間および最後に送信したデータの時間を記録します。これらの keep-alive メッセージはリモートホストに送られ、そのセッションがまだ開いていることを確認します。デフォルトは 15sec に設定されています。

- **TCP keep-alive probes:**
  これは、接続が切断されるまでに何回 keep-alive 検査メッセージがリモートホストに送られるのかを表わします。 3 と入力すると、3 回送られた後に切断されます。デフォルト値は 3 です。
- **TCP keep-alive intervals:**
  これは keep-alive パッケージが送信される時間間隔です。デフォルト値は 5 秒です。

デフォルト値では、5 秒間隔で Keep-alive パケットを 3 回送信し、15 秒後に切断されます。

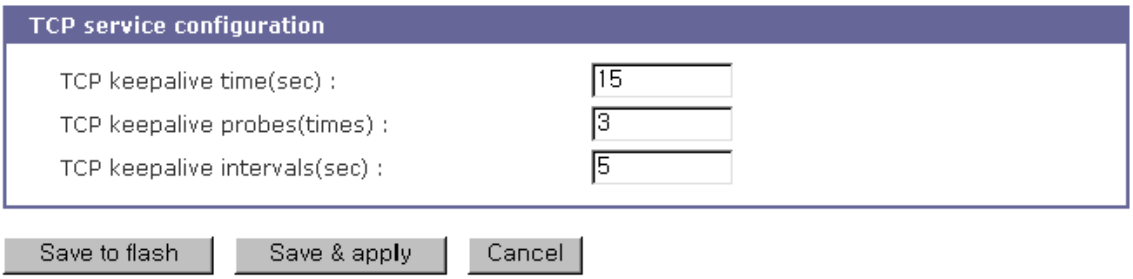



**図 3-12 TCP keep-alive 設定画面**

# 4. シリアルポート設定

## 4.1. 概要

シリアルポート設定機能により、各ポートのホストモード、シリアル通信パラメータ、暗号化、ポートロギングパラメータおよび他の関連したパラメータ設定を行ないます。シリアルポートのホストモードは以下のように設定可能です。

- **TCP:**
  STS シリーズは TCP サーバーおよびクライアントサーバーとして機能します。接続が確立されていない場合、登録済みの全てのリモートホストからの接続を受け入れ、シリアルデバイスからのデータがない場合リモートホストへ接続します。
  STS シリーズは仮想のリモートホストに接続しているかのように機能します。
- **UDP:**
  UDP モード操作はほとんど TCP と同じですが、違いはプロトコルが UDP であるということです。
- **Modem emulation:**
  シリアルデバイスがモデム AT コマンドをサポートする時、または AT コマンドを使用してセッションを操作する状況の時にこのモードを選択します。TCP セッションのみサポートしています。
- **Vertual COM:**
  この機能は将来に追加予定です。

コンソールサーバーモードのポートロギング機能でシリアルポートからのデータは、MEMORY、SYSLOG サーバー、NFS サーバーのストレージ、または PC カードスロットに挿入した ATA/IDE フィックスディスクカードに転送されます。各シリアルポートにキーワードを入力しておくことにより、email または SNMP トラップ通知の送信設定をすることにより、つないでいるシリアルデバイスを監視することができます。 MEMORY を使用すると、電源を OFF にしてもデータを保存することができます。NFS サーバーまたは ATA/IDE フィックスディスクカードでシリアルポートログデータを保存してください。
シリアルポート設定は各ポートごと、、または全ポート同時に設定可能です。表 4-1 はシリアルポート設定に関連したパラメータの一覧です。

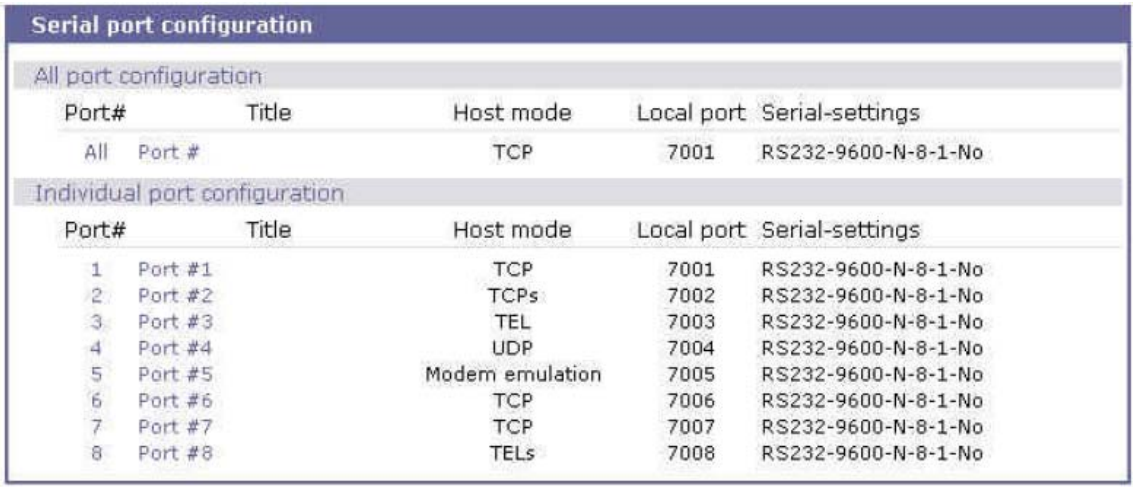
表 4-1 シリアルポート設定パラメーター覧

| | | | |
|---|---|---|---|
| 全シリアルポート設定<br>または<br><br>個別シリアルポート設定<br>#1～#8(1/4) | Port Enable/Disable(ポート ON/OFF) | | |
| | Port title(ポートタイトル) | | |
| | Apply all port settings(すべてのポート設定を適用する) | | |
| | ホストモード | TCP | TCP リスニングポート |
| | | | ユーザー認証 |
| | | | telnet プロトコル |
| | | | 最大接続数 |
| | | | 巡回接続 |
| | | | 非アクティブタイムアウト(0=無制限) |
| | | | |
| | | | |
| | | UDP | UDP リスニングポート |
| | | | 最大接続数 |
| | | | 非アクティブタイムアウト(0=無制限) |
| | | | unlisted 許可 |
| | | | unlisted 送信 |
| | | | |
| | | Modem Emulation | |
| | リモートホスト | リモートホストの追加・編集 | |
| | | プライマリ・ホスト IP アドレス | |
| | | プライマリ・ホストポート | |
| | | セカンダリ・ホスト IP アドレス | |
| | | セカンダリ・ホストポート | |
| | | リモートホストの削除 | |
| | Port IP フィルタリング | 許可されているホスト IP | |
| | | サブネットマスク | |
| | 暗号化 | 暗号化メソッド： なし/SSLv2/SSLv3/SSLv3 rollback to v2/TLSv1/3DES/RC4 | |
| | | Cipher suite selection | |
| | | クライアント認証(Server Mode only) | |
| | | Certificate chain depth(証明書チェーン)認証 | |
| | | Certificate CN(通常名)チェック | |
| | フィルターアプリケーション | フィルターアプリケーションパス | |
| | | フィルターアプリケーション引数 | |
| | シリアルポートパラメータ | ボーレート | |
| | | データビット | |
| | | パリティ | |
| | | ストップビット | |
| | | フロー制御 | |
| | | インターキャラクタ・タイムアウト | |
| | | DTR の振る舞い | |
| | | DSR の振る舞い | |
| | モデム | モデムの ON/OFF | |
| | | モデムの初期ストリング | |
| | | DCD の振る舞い | |
| | ポートロギング<br>Port logging | モデム接続の自動リリース | |
| | | ポートロギングの ON/OFF | |
| | | ポートログの保存場所 | |
| | | ポートログのバッファーサイズ | |
| | | ポートログの表示 | |
| | ポートイベント操作<br>Port event handling | ポートイベント操作の ON/OFF | |
| | | 通知間隔 | |
| | Email 通知<br>Email notification | Email 通知の ON/OFF | |
| | | Email の件名 | |
| | | Email の宛先アドレス | |
| | SNMP 通知<br>SNMP notification | SMMP 通知の ON/OFF | |
| | | SNMP トラップのタイトル | |
| | | SNMP trap 受信者の IP アドレス | |
| | | SNMPtrap コミュニティ | |
| | | SNMPtrap バージョン | |
| | キーワードの追加・編集<br>Keyword string | | |

| | |
|---|---|
| | Email notification<br>SNMP notification<br>Port command |
| | キーワードの削除 |

図 4-1 はウェブベースのシリアルポート設定画面です。シリアルポート設定メイン画面はポート情報を載せています。このサマリーページにはどのホストモードか、ローカルポート番号か、およびシリアルポートパラメータが現在設定されているかがわかります。

対応するシリアルポート番号(Port#)またはタイトル(Title)をクリックして、ポートパラメータを設定します。



Serial port configuration

All port configuration

| Port# | Title | Host mode | Local port | Serial-settings |
|---|---|---|---|---|
| All | Port # | TCP | 7001 | RS232-9600-N-8-1-No |

Individual port configuration

| Port# | Title | Host mode | Local port | Serial-settings |
|---|---|---|---|---|
| 1 | Port #1 | TCP | 7001 | RS232-9600-N-8-1-No |
| 2 | Port #2 | TCPs | 7002 | RS232-9600-N-8-1-No |
| 3 | Port #3 | TEL | 7003 | RS232-9600-N-8-1-No |
| 4 | Port #4 | UDP | 7004 | RS232-9600-N-8-1-No |
| 5 | Port #5 | Modem emulation | 7005 | RS232-9600-N-8-1-No |
| 6 | Port #6 | TCP | 7006 | RS232-9600-N-8-1-No |
| 7 | Port #7 | TCP | 7007 | RS232-9600-N-8-1-No |
| 8 | Port #8 | TELs | 7008 | RS232-9600-N-8-1-No |

**図 4-1 シリアルポート設定メイン画面**

## 4.2. シリアルポート設定

STS シリーズの各ポート設定は１２のカテゴリに分けられます。

1. Port enable/disable
2. Port title
3. Apply all port settings
4. Host mode
5. Remote host: ホストモードが、TCP・UDP モードのみ有効
6. Port IP filtering: ホストモードが、TCP/UDP モードのみ有効
7. Cryptography: ホストモードが TCP および Modem Emulation モードのみ有効
8. Filter application
9. Serial port Parameters
10. Modem configuration
11. Port logging
12. Port event handling

それぞれのポート設定画面の右上にあるリストボックスの[---Move to---]を使用することにより、別のスクリーンに簡単に移行できます。

### 4.2.1. Port Enable/Disable

各シリアルポートは Enable(オン)または Disable(オフ)にできます。シリアルポートが Disable の時は、そのシリアルポートにアクセスできません。図 4-2 は Serialport enable/disable 画面です。

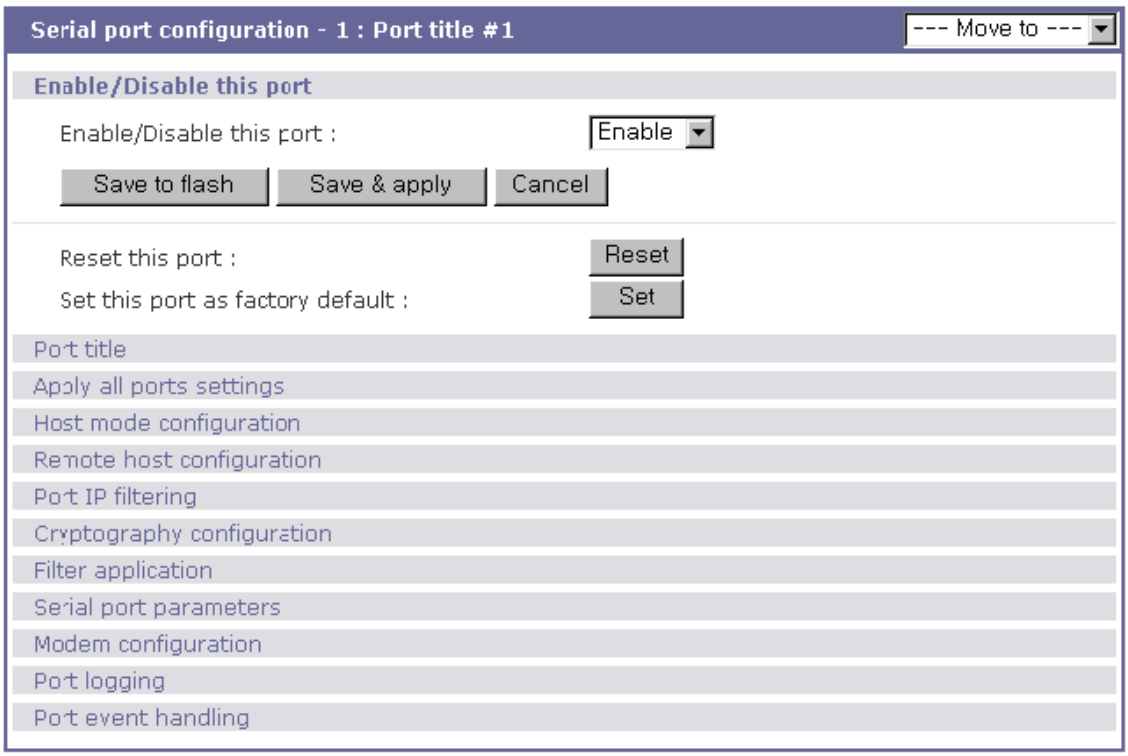



**図 4-2 Serial port enable/disable 画面**

Reset ボタンをクリックすると、フリーズしたシリアルポートをリセットすることができます。 Set ボタンをクリックすると、ポートをファクトリデフォルト値に戻します。

### 4.2.2. Port Title

それぞれのポートに、つないでいるデバイスに関する情報を入力することができます。
デバイスタイプ、製造元、または位置情報などです。

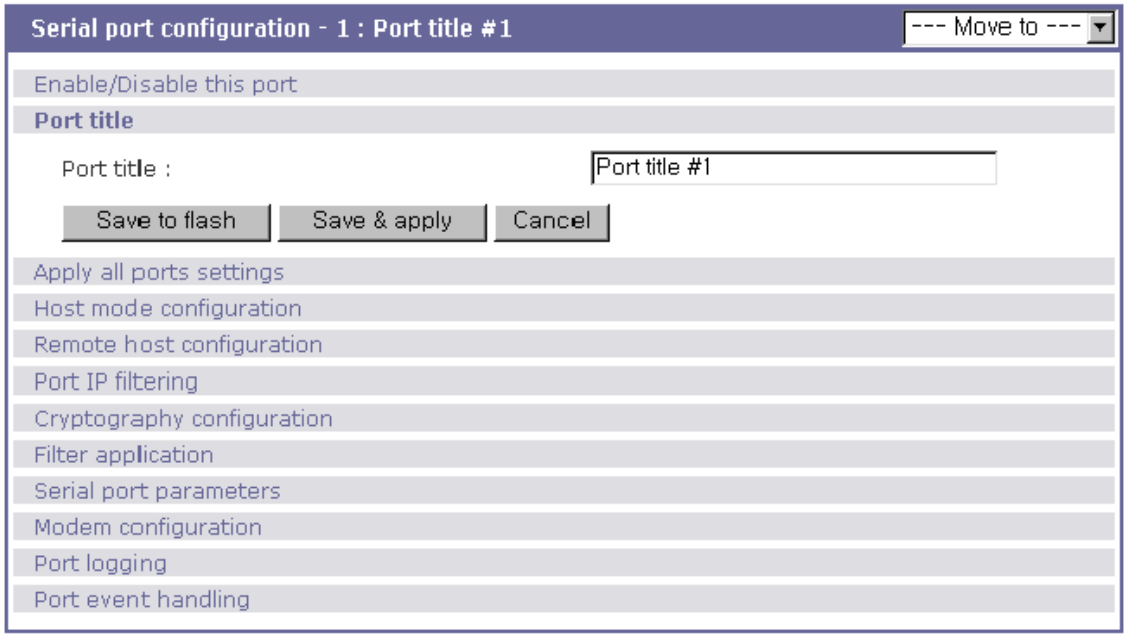



図 4-3 ポートタイトル設定

### 4.2.3. Apply All Port Settings (この変更を全ポートに適用する)

同時に全ポートの設定を誤って変更してしまうミスを避けるために、STS シリーズは、この機能(Apply All Port Settings)を各ポートに enable/disable 選択できるようにしています。 Disable になっているポートは、Apply all port setting が実行されたとしても、その変更は適用されません。図 4-4 を参照してください。

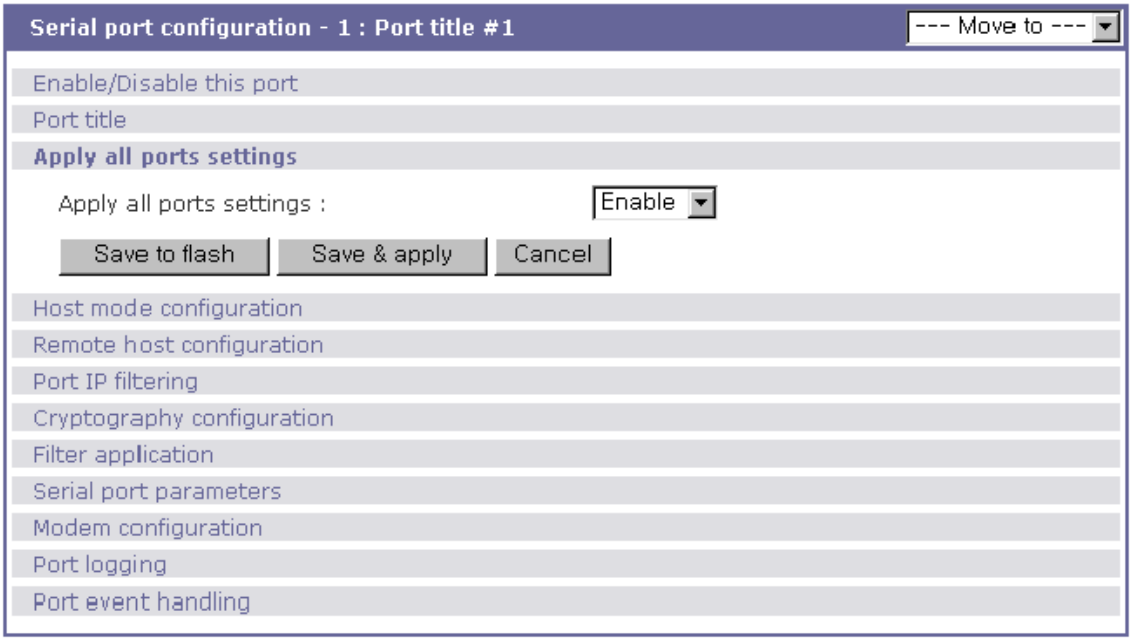



図 4-4 Apply all port setting 設定画面

### 4.2.4. Host Mode Configuration

STS シリーズ操作モードは"host mode"と呼ばれています。それらは TCP mode, UDP mode, Modem emulation mode があります。

**TCP モード**

STS シリーズは TCP サーバーおよびクライアントの役割を果たします。このモードはほとんど全てのアプリケーションにおいて有効です。もし TCP ポートに接続が確立されていなければ、TCP ポートは全ての登録されているリモートホストからの接続要求を許可し、それぞれ対応しているシリアルポートにデータを転送します。シリアルポートからのデータは事前登録してあるリモートホストに接続し、データをリダイレクトします。

**UDP モード**

UDP モードは TCP モードと同じように機能しますが、違いは、UDP プロトコルを使用するということです。

**Modem emulation モード**

シリアルデバイスが AT コマンドをサポートしている場合、このモードを選択します。TCP セッションのみサポートしています。

図 4-4 はホストモード設定のメイン画面を表示しています。

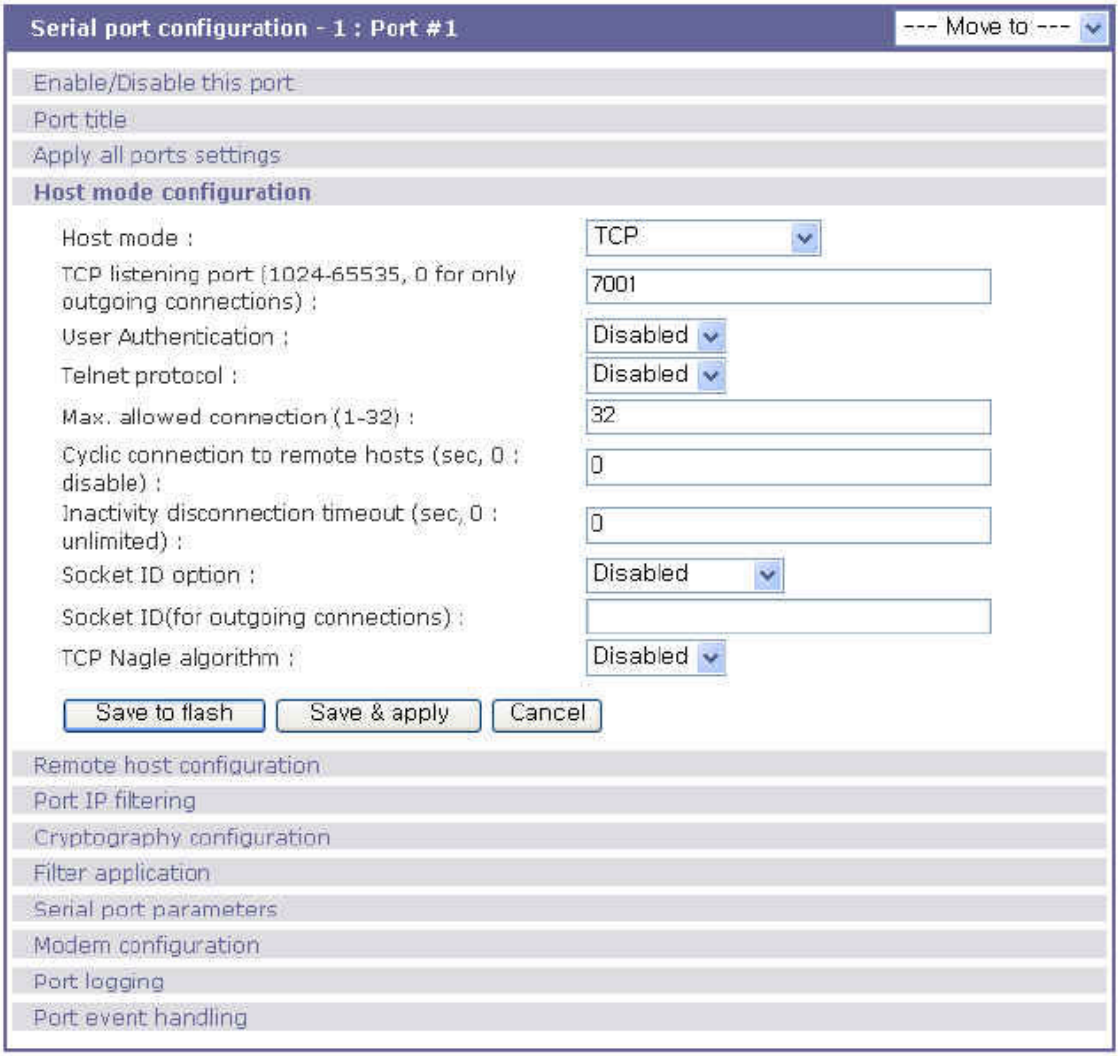



**図 4-5 ホストモード設定画面(TCP モード)**

#### 4.2.4.1. TCP mode

TCP mode のしくみを簡単に理解するには、State Transition Diagram(状態変移図) を利用します。以下にいくつかの TCP 状態の説明を記述します。

**[Listen]**

「登録済みのリモートホストからの接続要求を待機」します。TCP モードに設定した際のデフォルト値です。

**[Closed]**

無接続状態です。リモートホストとSTSシリーズ間の通信が終了すると、リモートホストまたはSTSシリーズ側から通信切断要求をだし、[Closed]に変わります。それから、[Listen]モードへ自動的に変

わります。

[Sync-Received]

リモートホストの一つが接続要求を発信すると、[Listen]状態から[Sybnc-Received]状態へと変わります。STS シリーズが接続を許可すると、[Sync-Received]から[established]に変わります。

[Sync-sent]

STS シリーズ側からリモートホストへ接続要求を出すとき、[Closed]状態は[Sync-Sent]状態へ変わります。この状態はリモートホストが接続を許可するまで続きます。

[Established]

オープン接続を表します。リモートホストまたは STS シリーズ側が接続を許可すると、接続が開き、[Established]状態に変わります。

[Data]

[Established]状態のとき、ホストからのデータはもう一方側に転送されます。TCP セッションの操作について簡単に理解するため、データ転送が行われた状態を[Data]状態と呼びます。実際は RFC793 規定においてデータ転送状態も[Established]に含まれます。

STS シリーズは、状況に応じて TCP サーバーとしてまたはクライアントとして動作します。TCP モードはほとんどのアプリケーションにおいて一般的なものです。データをシリアルポートからまたは TCP ポートからおくります。デフォルトの TCP 状態は[Listen]です。

**1） 典型的な状態変移パターン**

[Listen] → [Sync-Received] → [Established] → [Data] → [Closed] → [Listen]

[Listen] → [Sync-Sent] → [Established] → [Data] → [Closed] → [Listen]

初期状態は[Listen]です。シリアルポートからデータがくるとき、ホストへ TCP クライアントとして接続し、それから TCP ポートを通してデータを送信します。リモートホストからの接続要求が来る場合、TCP サーバーとして接続を許可し、それからシリアルポートを通してデータを送信します。STS シリーズは常に指定したリモートホストに接続されています。

**2） 操作**

**シリアルデータ転送**

シリアルデバイスが STS シリーズのシリアルポートを通してデータを送信するときは、そのデータはまず STS シリーズのシリアルポートバッファー内に蓄積されます。バッファが一杯または文字タイムアウトに到達する場合は、STS シリーズは登録してあるリモートホストに接続します。TCP セッ

ションがまだ確立されていない時は、STS リモートホストと接続が確立されたら、シリアルポートバッファー内のデータはホストへ転送されます。そうでなければ、バッファ内のデータは消去されます。

**セッションの切断**

接続中のセッションはリモートホストが切断要求を送信、または一定期間にシリアルポートからのデータ転送がない場合に切断されます。シリアルポートバッファー内のすべてのデータは切断時に消去されます。

**リモートホストからの接続要求**

TCP 接続要求は TCP クライアントモードのときは拒否されます。

3) **パラメータ**

**TCP リスニングポート**

リモートホストが TCP セッションに接続し、データを送受信可能な TCP 番号のことです。TCP リスニングポート以外のポートへの接続は拒否されます。STS シリーズも 1024 から 65535 番までのポート番号を制限しており、0 only と設定すると、発信接続が制限されます(TCP サーバーモード)。

**User authentication(ユーザー認証)機能**

ユーザー認証がオンになっているとき、ユーザーID とパスワードを入力してからポートにアクセス可能になります。 詳細情報に関しては、(*5.9.ユーザー認証機能*)を参照してください。

**Telnet Protocol(telnet プロトコル)**

TCP モードでは、STS シリーズは Telnet Com Port Control Option(RFC2217 準拠)をサポートしているので、Telnet クライアントプログラムを使用してボーレート、データビット、またはフロー制御オプションなどのシリアルパラメータを制御することができます(詳細は *4.2.6. シリアルポートパラメータ*を参照してください)。通常このオプションは RFC2217 準拠 COM ポートリダイレクターを使用するので、STS シリーズは現在使用しているシリアルポートアプリケーションプログラムを使って各種シリアルパラメータを制御可能です。STS シリーズに同梱されているシリアル IP ソフトウェアはその役割を果たすために機能します。詳細情報は *付録 5、STS シリーズとシリアル IP* を参照してください。

**Max. allowed connection(最大接続数)**

STS シリーズは最大 32 台のホストからの接続を受け入れることができます。もしすでにリモートホストリスト設定によってリモートホストからの接続がある場合は、最大接続数は少なくなります(すでに接続されているホストがあるため)。詳細情報に関しては *4.2.5. リモートホスト設定*を参照してください。

**Cyclic Connection**

Cyclic Connection 機能がオンのときは、STS シリーズは、シリアルポートに一定時間の着信シリアルデータが届かない場合、一定サイクル間隔でユーザーが事前に指定したリモートホストに接続試行を繰り返します。リモートホストからシリアルデバイスへおくらなければいけないデータがある場合、接続が確立後、STS サーバーのシリアルポート経由でシリアルデバイスに転送されます。そのうち、ユーザーはリモートホストに接続されるときはいつでもシリアルコマンドを送信するようになるので、シリアルデバイスを監視することができるようになります。このオプションは定期的にデバイス情報を収集する必要がある時に有効です。シリアルデバイスがデータを送らないような時にも有効です。図 4-6 は TCP モードの状態変移ダイアグラムです。

**Socket ID**

複数の STS デバイスが、同じリモートホストに接続する場合、それぞれのデバイスを認識することが必要です。Socket ID はそのような場合において各デバイスの ID を作成するためのものです。STS シリーズはデータを送信する前のストリングに Socket ID を添付します。指定したストリングで Socket ID
を定義することができます。 TCP モードでは指定した Socket ID ストリングは TCP 接続が確立された時点で一度送信されます。

**TCP Nagle algorithm**

モデム TCP インプリメントには Nagle Altorithm として知られる機能があります。これは小容量のパケットを大量に送信することを防止します。これはインターネットに超過量のパケット送信を防止するようになります。しかし、システムによってはそのような Nagle Algorithm が障害を引き起こす場合もあります。状況に応じて TCP Nagle algorithm 機能を ON・OFF にしてください。

**Inactivity Timeout**

Inactivity Timeout 機能がオンのときは、ここで事前に設定した時間内にデータの送受信がない場合に、リモートホストおよび STS シリーズ間の接続が自動的に切断されます。

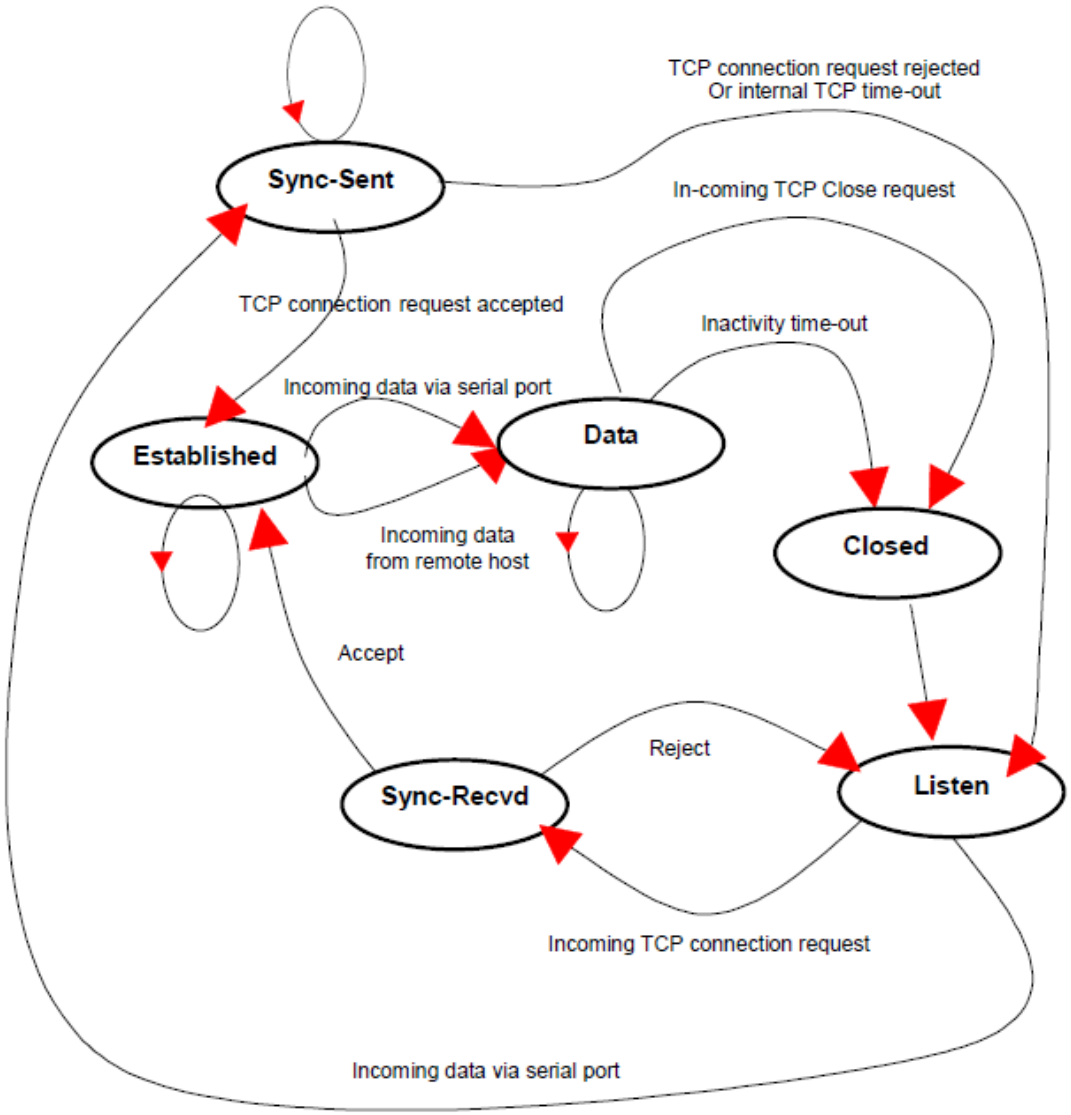



**図 4-6 TCP モードの状態変移ダイアグラム**

#### 4.2.4.2. UDP mode

UDP mode 操作は UDP プロトコルを使用した TCPmode に似ています。STS シリーズは事前に設定したリモートホストのみと通信できます。UDP はコネクションレスプロトコルであるため、Cyclic connection 設定は必要ありません。

**1) 操作方法**

リモートホストが UDP データグラムを STS シリーズの UDP ローカルポートの一つに送信すると、STS シリーズは最初にリモートホスト設定で設定したホストのひとつかどうかをチェックします。

Remote host configuration で設定したホストのひとつであれば、STS シリーズはシリアルポートからデータを転送します。そうでなければ、着信した UDP ダイアグラムを破棄します。しかし、remote host configuration の設定画面で"Accept UDP datagram from unlisted remote host"のパラメータを Yes に設定すると、すべての UDP ダイアグラムを受け入れ、シリアルポートからデータを転送するようになります。リモートポートが開いていない場合は、STS シリーズはデータを転送しません。

**2) パラメータ**

**UDP receiving port (UDP 受信ポート)**

TCP リスニングポートと同様に動作します。詳細は *4.2.4.1.TCPmode パラメータ*を参照してください。

**Max. allowed connection (最大接続可能数)**

TCP 通信とコンセプトは同じです。*4.2.4.1.TCP モードパラメータ*を参照してください。

**Accept UDP datagram from unlisted remote host (リストにないリモートホストからの UDP データグラムを許可する)**

この機能を NO にすると、STS シリーズは remote host configuration で設定したリモートホストからの UDP データグラムのみを受け入れます。YES にすると、STS シリーズは Remote host configuration で設定していてもいなくてもすべての UDP データグラムを受け入れます。

**Send to recent unlisted remote host (最後のリストにないリモートホストに送信)**

Send unlisted 機能が Yes になっているなら、STS シリーズは最後に接続したリモートホストにデータを送信します。Recent unlisted remote host とは STS のシリアルポートからアクセスしたが、remote host configuration にて設定していないリモートホストのことです。STS シリーズは inactivity timeout の間最後に通信を行ったリストにないリモートホストを保存します。

**Inactivity timeout (無活動タイムアウト)**

UDPmode では、inactivity timeout は最後に通信を行ったリストにないリモートホストを保存するために使用します。Inactivity timeout の時間内でリストにないリモートホストと STS 間でのデータのやりとりがない場合、STS シリーズは、そのリストにないリモートホストへデータを送らなくなります。

注記: もしユーザーが UDP モードの inactivity timeout を 0 に設定するなら、STS シリーズは最大接続可能数を超過するとリモートホストからまたはリモートホストへの新しい接続を行いません。

**Socket ID**

多くの STS シリーズが一つのリモートホストへ接続するとき、デバイス一つ一つを識別する必要があります。そのような場合、各デバイスの識別をおこなうための Socket ID が必要になります。

STS シリーズはデータを送信する前のストリングに Socket ID を添付します。指定したストリングで Socket ID を定義することができます。UDP モードでは Socket ID ストリングはすべてのパケットの頭に

添付され送信されます。

#### 4.2.4.3. Modem emulation mode モデムエミュレーション・モード

**1） 操作**

Modem emulation mode では、シリアルデバイスのポートにモデムがついているかのように動作します。モデムがするように AT モデムコマンドを受け入れ、応答します。またモデム信号を正しく処理します。次のような状況では Modem Emulation Mode はとても便利です。

**使用しているシリアルデバイスにすでにモデムが付いている場合**

電話回線接続用にモデムがシリアルデバイスについている場合、STS シリーズのイーサネット接続に交換することができます。IP アドレス（ドメイン名）およびポート番号だけで電話番号を ATA/ATDT コマンドのパラメータとして使用しなくても大丈夫です。

**複数のリモートホストへシリアルデータを送信する場合**

シリアルデバイスがデータを複数のホストへ送信する必要がある場合に Modem Emulation mode は必要です。たとえば、シリアルデータからの最初のデータは最初のデータ収集サーバーへ送られ、2 番目のデータは 2 番目のデータ収集サーバーへ、ということになります。ユーザーデバイスは、デバイスが ATD(T)XXX コマンドを送るたびに IP アドレスおよびポート番号を変更しなければいけません。

STS シリーズの Modem Emulation mode を使用することにより、簡単にシリアルデバイスを Ethernet ネットワークに接続することが容易になり、電話線モデムを使用するよりずっと安価です。表 4-2 は、STS シリーズによってサポートされている AT コマンド一覧表です。図 4-7 には、ATDA コマンドが Ethernet ネットワークにつなぐために使用された場合のシリアルポートコマンドのフロー図です。

## 表 4-2 STS シリーズでサポートされている AT コマンド一覧

| コマンド | 内部操作 | レスポンス [9] (Verbose Code) |
|---|---|---|
| +++ | コマンド入力モードに戻る | なし |
| ATD(T)<br>[リモート IP またはドメイン名] :[リモートポート]<br>[CR][LF]<br>Or<br>ATD(T)<br>[remote IP] [remote port] [CR] [LF] | TCP モードを TCP クライアントモードに設定する。<br>e.g. atdt192.168.1.9:1002<br>e.g. atdt19216800100910002<br>IP アドレス 192.168.1.9 port1002 に接続<br>（ポート番号は 1-65534 まで許可）<br>e.g. atdtss.sena.com:1002<br>ss.sena.com,port 1002 のドメインアドレスに接続 | 成功すると、<br>CONNECT[CR][LF]<br>接続エラーの場合、<br>NO<br>CARRIER[CR][LF]<br>他のエラーは、<br>ERROR [CR][LF] |
| AT or ATZ [CR] [LF] | TCP ソケットおよびシリアルポートを初期化 | 成功すると、<br>OK[CR][LF]<br><br>失敗すると、<br>ERROR[CR][LF] |
| ATA/ [CR] [LF] | 最後のコマンドをリピート | |
| ATA<br>[ローカルポート番号] [CR] [LF] | TCP モードを TCP サーバーモードに設定。TCP 状態を“Listen”にする。<br>コマンドパラメータ、ローカルポート番号が指定されていない場合は、TCP セッションパラメータ、ローカルポートが使用される | |
| ATEn [CR] [LF] | E、E0:Echo をオフ<br>E1： Echo をオン | |
| ATOn [CR] [LF] | O,O0: データモードにする | |
| ATQn [CR] [LF] | Q、Q0: レスポンスディスプレイをオン<br>Q1: レスポンスディスプレイをオフ | |
| ATVn [CR] [LF] | V,V0：レスポンス＝<numeric code>[CR][LF]<br>V1(デフォルト):レスポンス=<冗長 verbose code> [CR][LF] | |
| AT&Dn [CR] [LF] | D,D0: DTR(PC)シグナルを無視<br>D2（デフォルト）:TCP セッションを切断 | |
| AT&Fn [CR] [LF] | F,F0,F1: デフォルトのモデム設定に戻す | |
| AT&Kn [CR] [LF] | K,K0:フロー制御オフ<br>K3: RTS/CTS フロー制御<br>K4:Xon/Xoff | |
| AT&Sn [CR] [LF] | S,S0: DSR(PC)はつねにオン<br>S1: DSR(PC)は TCP 接続を表示 | |
| ATHn [CR] [LF] | H,H0: 現行の TCP 接続を切断、すべてのデータは消去<br>H1: 現行の TCP 接続を維持 | OK[CR][LF] |
| ATIn [CR] [LF] | I,I0:“Sena Technologies, Inc.”を表示<br>I3: モデル番号を表示<br>他: “OK”を表示 | <= |
| AT\Tn [CR] [LF] | インアクティビティ（無活動）タイマーを n 分間セットする<br>\T,\T0; インアクティビティタイマーをオフ | OK[CR][LF] |
| AT&Bn, ATCn, ATLn, ATMn, ATNn, ATP, ATT, ATYn, AT%Cn, AT%En, AT&Bn, AT&Gn, AT&In, AT&Qn, AT&V, ATMn, AT\An, AT\Bn, AT\Nn, AT\Xn | なし | OK[CR][LF] |
| ATS?, ATSn=x, AT&Cn, AT&Wn, AT&Zn=x | なし | ERROR[CR][LF] |
| ATFn[CR][LF] | なし | N=1 のとき、<br>OK[CR][LF]<br>それ以外は<br>ERROR[CR][LF] |
| ATWn | なし | N=0 のとき、<br>OK[CR][LF]<br>それ以外は<br>ERROR[CR][LF] |

表 4-3　AT コマンドレスポンスコード

| 冗長コード | 数字コード | 説明 |
|---|---|---|
| OK | 0 | コマンドを実行 |
| CONNECT | 1 | モデムが回線に接続 |
| RING | 2 | リングシグナル検知 |
| NO CARRIER | 3 | モデムがキャリアシグナル消失 |
| ERROR | 4 | 無効なコマンド |

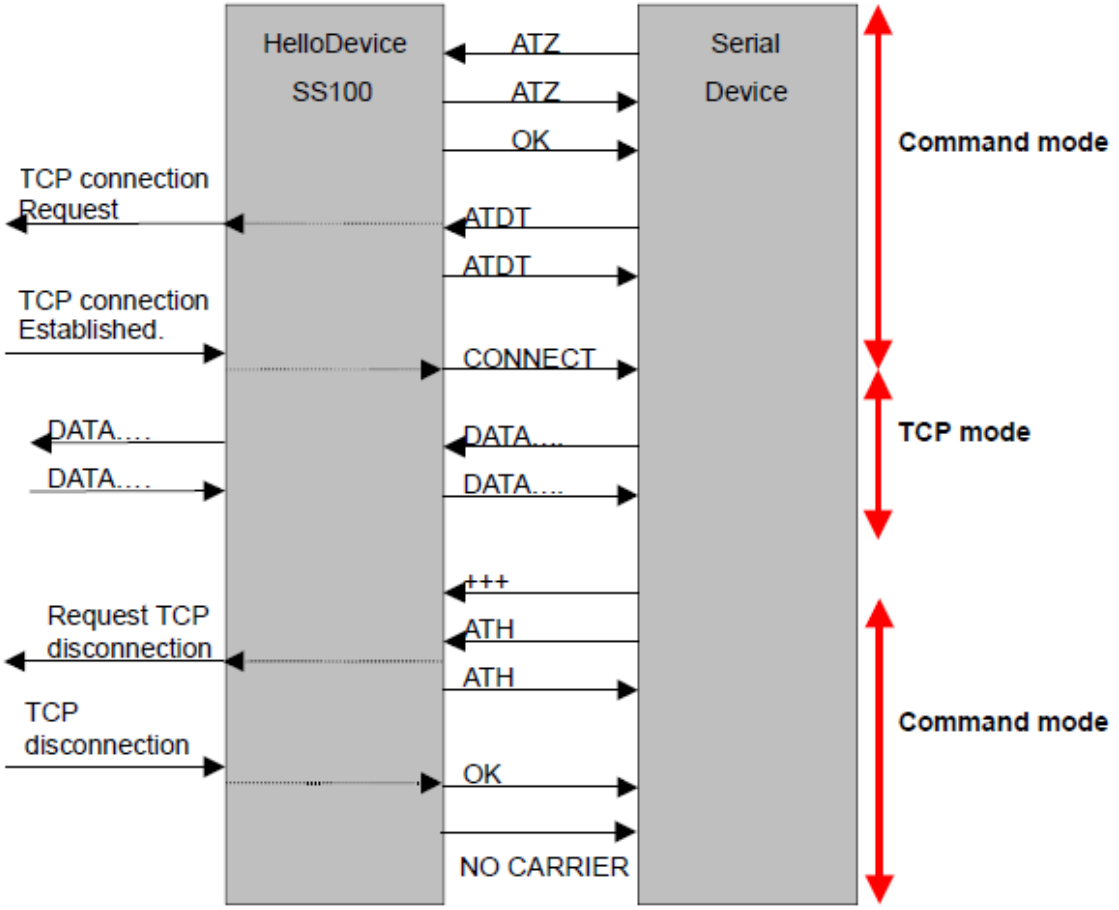



図 4-7modem emulation mode での典型的なコマンド・データの流れ

### 4.2.5. Remote Host Configuration（リモートホスト設定）

Remote Host Configuration は STS シリーズのシリアルポートからデータ送信がある時に STS シリーズのシリアルポートからのデータを受信するホストの一覧のことです。

TCP モードでは、ユーザーはセカンダリ・リモートホスト（バックアップ・ホスト）を設定し STS シリーズがプライマリ・リモートホスト（メイン・ホスト）に接続に失敗するときに接続します。プライマリ・ホストとの接続が成功すれば、セカンダリ・リモートホストへはデータを送信せず、プライマリ・ホストとの接続に失敗

すると、再びセカンダリ・リモートホストに接続します。プライマリ・リモートホストの最大接続数 16 台です。

UDP モードでは、1 台のプライマリ・リモートホストしか接続できませんでした。なぜなら、そのリモートホストとの接続状態をチェックすることができないので、セカンダリ・リモートホストを持つ必要がないからです。図 4-8 にはウェブインターフェースのリモートホスト設定画面です（TCP モード）。

ここで任意のドメイン名を設定することも可能です。

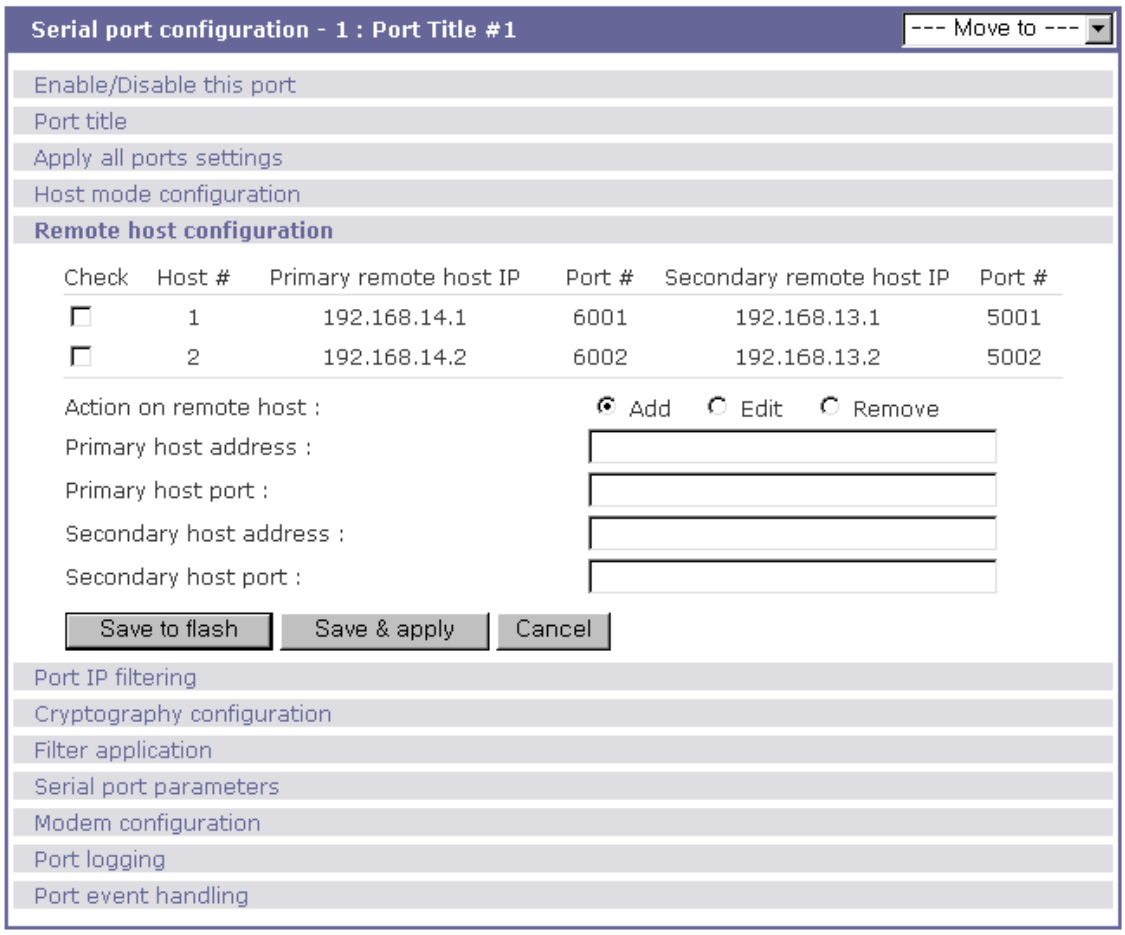



**図 4-8 リモートホスト設定画面**

### 4.2.6. Port IP filtering configuration （IP フィルタリング設定）

STS シリーズのシリアルポートにアクセスを許可しているリモートホストは IP アドレスフィルタリングルール設定で指定することができます。IP アドレスまたはネットワークアドレスおよびそのサブネットマスクを入力することにより、STS シリーズのシリアルポートにアクセス可能になります。3.5. IP filtering の章を参照してください。

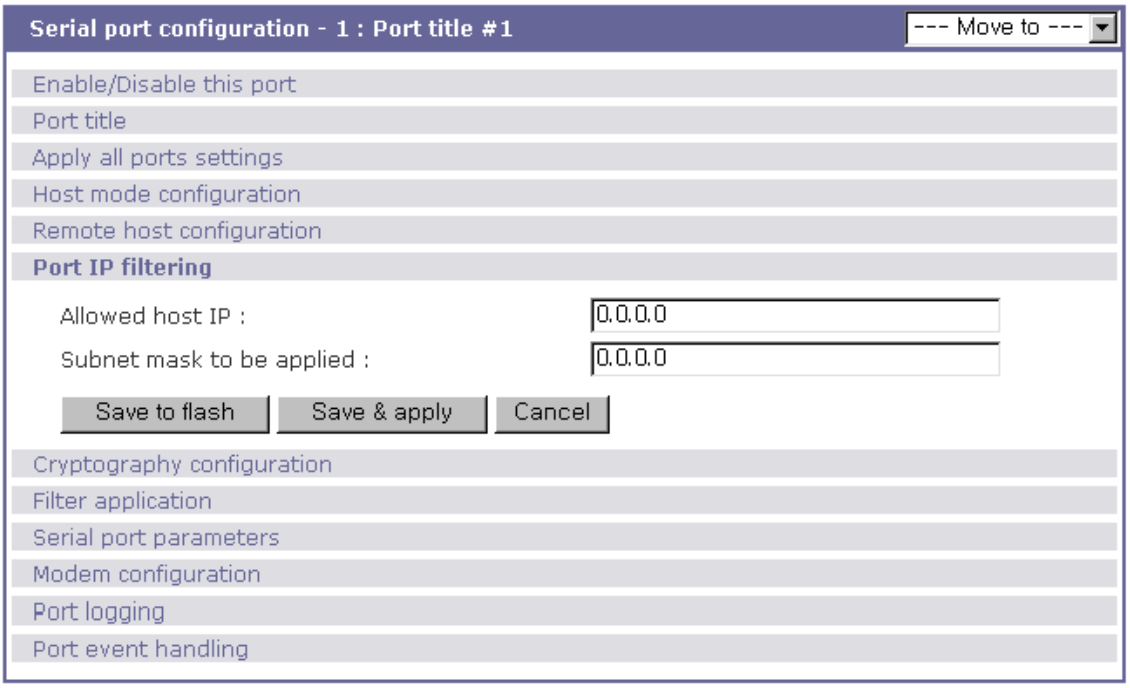



**図 4-9　Port IP filtering 設定**

### 4.2.7. Cryptography configuration （暗号化の設定）

暗号化セッションは modem emulation mode を含む TCP モードのみサポートしています。

#### 4.2.7.1. SSL（Secure Sockets Layers）暗号化設定

SSL を設定することにより、STS シリーズは他のデバイスと暗号化セッション中に SSLv3暗号化メソッドを使用して通信を行います。SSL は Netscape がクライアントとサーバー間の通信を行うために開発されました。 SSL は転送プロトコルの一番上に位置しており、HTTP のようなアプリケーションプロトコルで動作します。SSL はセキュア、高速で、他の Web プロトコルと相性が良いです。SSL はネットワーク間で通信を行うアプリケーションのためのデータセキュリティです。SSL はアプリケーションプロトコルと TCP/IP 間にあるレイヤーのトランスポートレイヤー・セキュリティプロトコルです。

SSL セッションを始めるにはサーバーとクライアント間で SSL ハンドシェークと呼ばれるメッセージの交換が必要になります。SSL プロトコルは公開鍵と対称鍵の暗号化の組み合わせを使用します。対象鍵の暗号化は公開鍵の暗号化よりもより高速ですが、公開鍵の暗号化のほうが認証技術において優れています。ハンドシェークはサーバーが公開鍵技術を使用するクライアントを認証させ、それからクライアントとサーバーが対称鍵を発行し、高速の暗号化、非暗号化、また改ざん検知などに使用します。次にハンドシェークの手続きの詳細を説明します。

1. クライアントはサーバーにクライアントの SSL バージョン番号、暗号設定、ランダム生成デー

タ、およびクライアントが SSL でサーバー側と通信するために必要なその他の情報を送信します。

2. サーバーはクライアント側にサーバーの SSL バージョン番号、暗号設定、ランダム生成データ、およびサーバーが SSL でクライアントと通信するために必要なその他の情報を送信します。サーバーはサーバー用の証明書を送信し、クライアントがクライアント認証のためにサーバーリソースを要求する場合にクライアント証明書を要求します。
3. クライアントはサーバーによって送信された情報の一部を使用してサーバーを認証します。サーバーが認証されない時は、その問題が警告され、暗号化および認証接続は確立されなかったということが通知されます。サーバー認証が成功すると、次のステップに進みます。
4. ハンドシェークによって生成されたすべてのデータを使用して、クライアントはプリマスター・シークレットを生成し、サーバーの公開鍵で暗号化し、それからその暗号化したプリマスター・シークレットをサーバーに送信します。これで共有のマスター・シークレットが作成されました。
5. サーバー側がクライアント認証（ハンドシェークのオプション機能）を要求していれば、クライアントはこのハンドシェーク特有で、サーバー、クライアント両方が知っているデータの一部に署名します。この場合クライアントは署名済みのデータおよびクライアント独自の認証を暗号化したプリマスター・シークレットと共にサーバーに送信します。
6. サーバーがクライアントの認証をリクエストしているなら、サーバーはクライアントの認証を試行します。クライアントが認証されなければ、そのセッションは終了します。もしクライアントの認証が成功すれば、サーバーは秘密（プライベート）鍵でプリマスター・シークレットの暗号解除をおこない、それからマスター・シークレットを生成します。
7. クライアントとサーバーの両方ともマスター・シークレットを使用してセッション鍵を生成します。そのカギは SSL/TLS セッションの間情報交換するための暗号化、暗号解除に使用され、データの保全性、つまり SSL 接続の間に情報が改ざんされていないかをチェックします。
8. クライアントはクライアントからのメッセージはセッション鍵によって暗号化されるということをサーバーに伝えます。それから暗号化されたメッセージを送信し、クライアント側のハンドシェーキングが終了したと伝えます。
9. サーバー側はクライアントに、サーバー側からのメッセージはセッション鍵によって暗号化されるということを伝えます。そしてサーバー側のハンドシェーキングが終了したと伝えます。
10. SSL ハンドシェークは完了し、SSL セッションが開始します。クライアントおよびサーバーはセッション鍵を使用して双方が送信するデータを暗号化、暗号解除し、またデータの保全性も確認します。

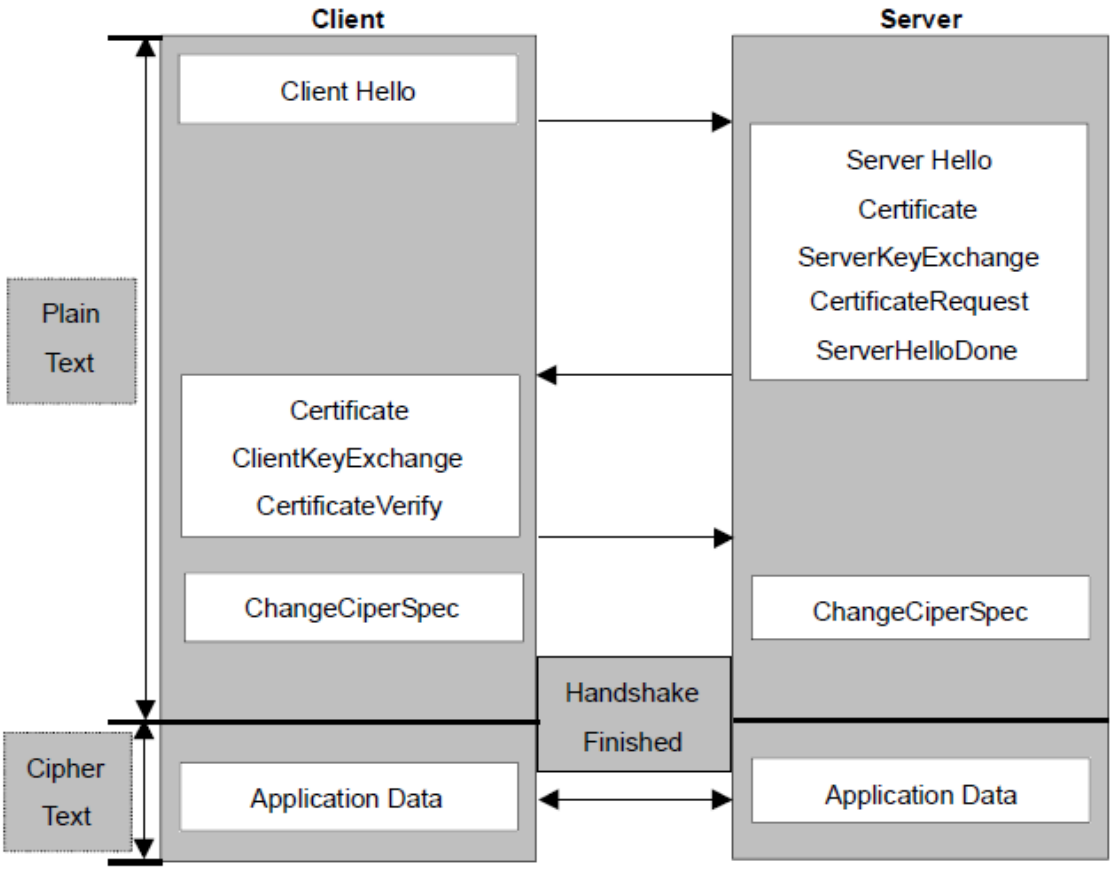



**図 4-10 代表的な SSL ハンドシェークの流れ図**

STS シリーズは TCP モードの状態により、SSL サーバーとして、また SSL クライアントとして動作します。SSL での TCP 接続がリモートホストから最初に開始した場合、STS シリーズは SSL ハンドシェークプロセス中 SSL サーバーとして動作します。それとは対照的に、SSL での TCP 接続が STS シリーズ側のシリアルポートから開始した場合は、SSL ハンドシェークプロセス中は SSL クライアントとして動作します。

SSL/TLS 暗号化メソッドを使用するときは、以下のパラメータを設定してください。

- **Enable/Disable cipher suites(暗号スイートのオン・オフ)**

暗号スイートとは通信の整合性を保護するための鍵暗号(非対称)アルゴリズム、対称暗号アルゴリズム、および Secure Hash Algorithm からなる SSL 暗号化方式のことです。鍵暗号アルゴリズムはサーバーの認証するのに使用し安全に暗号鍵情報を交換します。対象暗号アルゴリズムは SSL/TLS 接続で送信されたバルクデータを暗号化するのに使用します。Hash アルゴリズムは送信中にデータが改変されることを防ぎます。対象および非対称アルゴリズムの鍵の長さを指定する必要があります。

クライアントが SSL/TLS 接続をサーバーに行うと、使用可能な暗号スイートの一覧を送信します。サーバーはその一覧とそのサーバーがサポートしているスイートを比較し、クライアントがサポート

している第一の暗号スイートを選択します
暗号スイートを使うか否かは、使用環境およびセキュリティ条件によります。RSAベースの暗号スイートが最も広く使われています。
STSシリーズは様々な暗号スイートをサポートしており、状況に応じて各暗号のON／OFF を選択可能です。

- **Verify client(server mode 専用)**
  Verify Client オプションを“Yes”に設定すると、STSサーバーはSSLハンドシェーキングプロセス中にクライアント証明書をリクエストします。逆に“No”に設定すると、STSサーバーはSSLハンドシェーキングプロセス中にクライアント証明書をリクエストしません。
- **Verify certificate chain depth**
  Certificate chain(証明書チェーン)とは、証明書のシーケンスのことであり、各証明書は後続の証明書によってサイン済みです。Certificate chain の目的は、ピアの証明書から認証済みのCA証明書へのチェーンを確立するためのものです。CAは証明書に署名をすることにより、ピアの証明書を認証します。CAが信頼のおけるものであれば、ピアの証明書も信頼のおけるものとなります。STSサーバーの場合、証明書チェーンの depth（数）を設定することにより、証明書チェーン内を無限に探し続けることを回避します。

- **Check the certificate CN**
  このオプションをYesにすると、STSサーバーはホスト名が証明書内の一般名CN（Common Name）と適合するかどうかを確認します。適合しなければ、STSサーバーはリモートホストに接続要求を切断します。逆にこのオプションをNoにすると、STSサーバーは証明書内のCNとホスト名が適合するかどうかを検査しません。
  STSサーバーはSSL／TLSクライアントとして動作するとき以外一般名CNを検査することはありません。

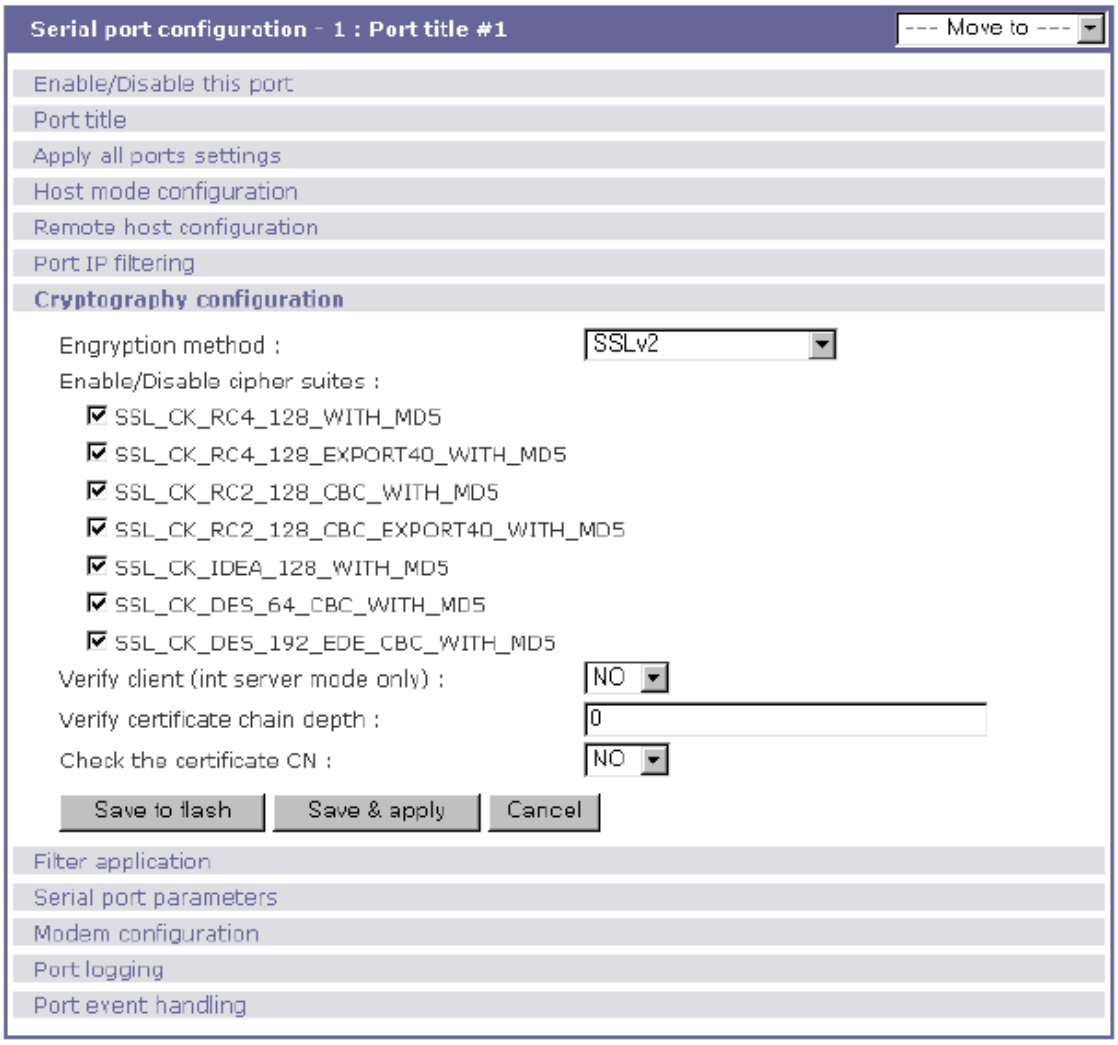



**図 4-11 暗号化設定画面**

#### 4.2.7.2. 3DES 暗号化

3DES に設定すると、STSサーバーは他のサーバー(STSデバイスサーバーまたはPSデバイスサーバー等)と 3DES(168bits)暗号化セッションで通信を行います。

図 4.-12 は各フィールドの意味がある 3DES パケットのフォーマットを表しています。


**図 4-12 3DES パケットの記録フォーマット**

- **Length(長さ)**

  Lengthは 8 ビットの数字です。LengthとはデータおよびPaddingの長さのことです。3DES は 64-bit ブロック暗号アルゴリズムであり、長さは 8 の倍数です。

- **Padding**

  Padding とは標準ブロック暗号化のことです。Pad 値は padding(1-8)の合計 pad bytes です。

STSサーバーの 3DES アルゴリズムでは、鍵および初期ベクター（暗号化されたデータパケットを生成するために使用）はキーブロックから派生します。キーブロックはユーザーが設定したキーストリングを使用することにより生成できます。 図 4-13 はキーの派生するプロセスを表しています。

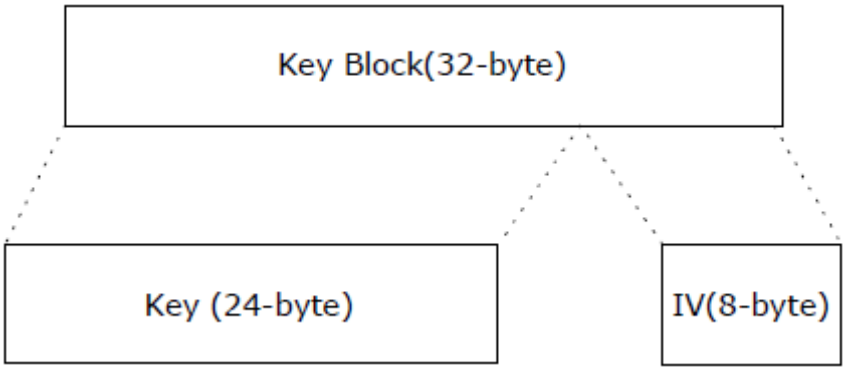



**図 4-13 キーの派生プロセス**

キーブロックは次のように定義されます:

Key_Block = MD5(KEY_STRING) + MD5(MD5(KEY_STRING)+KEY_STRING)
= (16 bytes) + (16 bytes)
Key = first 24bytes of Key Block
IV(Initial Vector) = last 8 bytes of Key block

#### 4.2.7.3. RC4 暗号化メソッド

RC4 暗号化モードでは、STS シリーズはキーストリングを使用してすべての TCP ストリームを暗号化、または暗号解除します。STS シリーズは同じキーストリングの RC4 暗号化モードをサポートする他のデバイスまたは STS シリーズと通信することができます。ヘッダも padding もないため、3DES よりも処理が高速です。

### 4.2.8. フィルターアプリケーション

STSデバイスサーバーはリモートホストとシリアルポートにつないであるシリアルデバイス間の raw データの操作をサポートしています。その操作をフィルターアプリケーションと呼びます。独自のフィルターアプリケーションプログラムをお持ちであれば、STSデバイスサーバーにアップロードし、Filter configuration メニュー画面から設定を行うことができます。フィルターアプリケーションに関する詳細情報は *9.4 「ユーザー独自のコードを作成し起動」*を参照してください。

**注記: ファイルのアップロードはコンソールメニューからのみサポートされています。詳細情報は 6.10 を参照してください。**

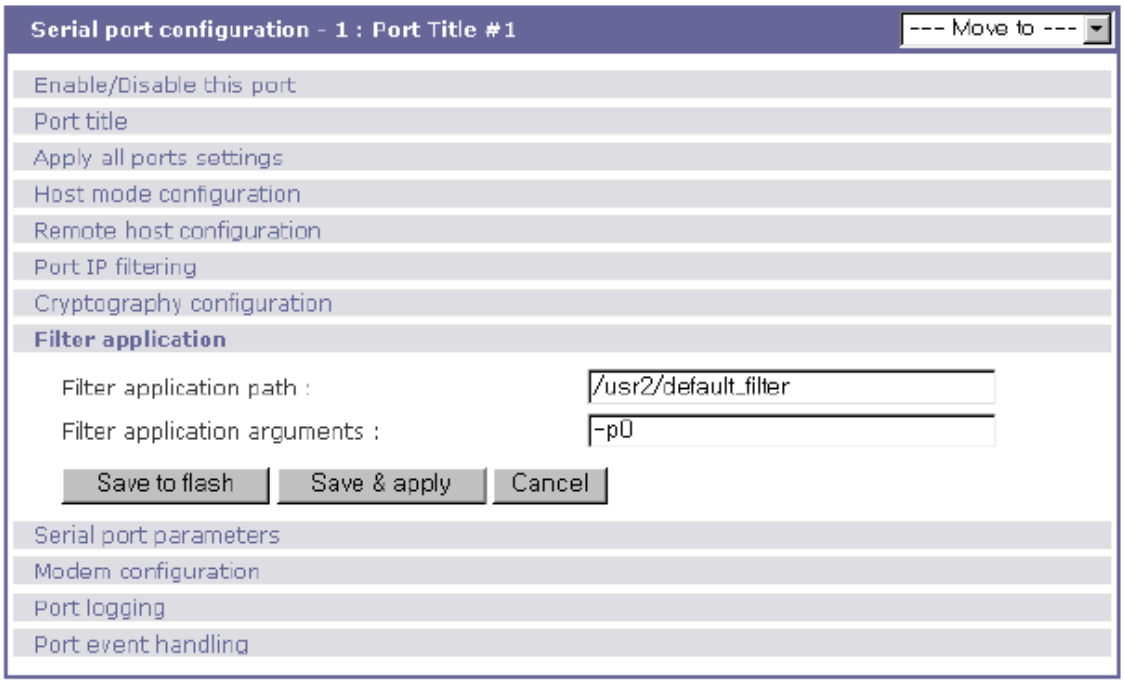



**図 4-14 フィルターアプリケーション画面**

### 4.2.9. シリアルポートパラメータ

シリアルデバイスを STS シリーズのシリアルポートに接続する際、STS シリーズのシリアルポートのパラメータとシリアルデバイス側のパラメータが一致していなければなりません。一致させるパラメータ値は、UART タイプ、ボーレート、データビット、パリティ、ストップビット、フロー制御、DTR/DSR、およびインターキャラクタ・タイムアウトです。

- **Baud rate**

  STS シリーズの変更可能なボーレートは以下です:

  75, 150, 200, 300, 600, 1200, 2400, 4800, 9600, 14400, 19200, 38400, 57600, 115200, 230400 です。

  工場出荷時のデフォルト値は 9600 です。

- **Data bits**

  7 または 8 ビットが選択可能です。

  工場出荷時のデフォルト値は 8 ビットです。

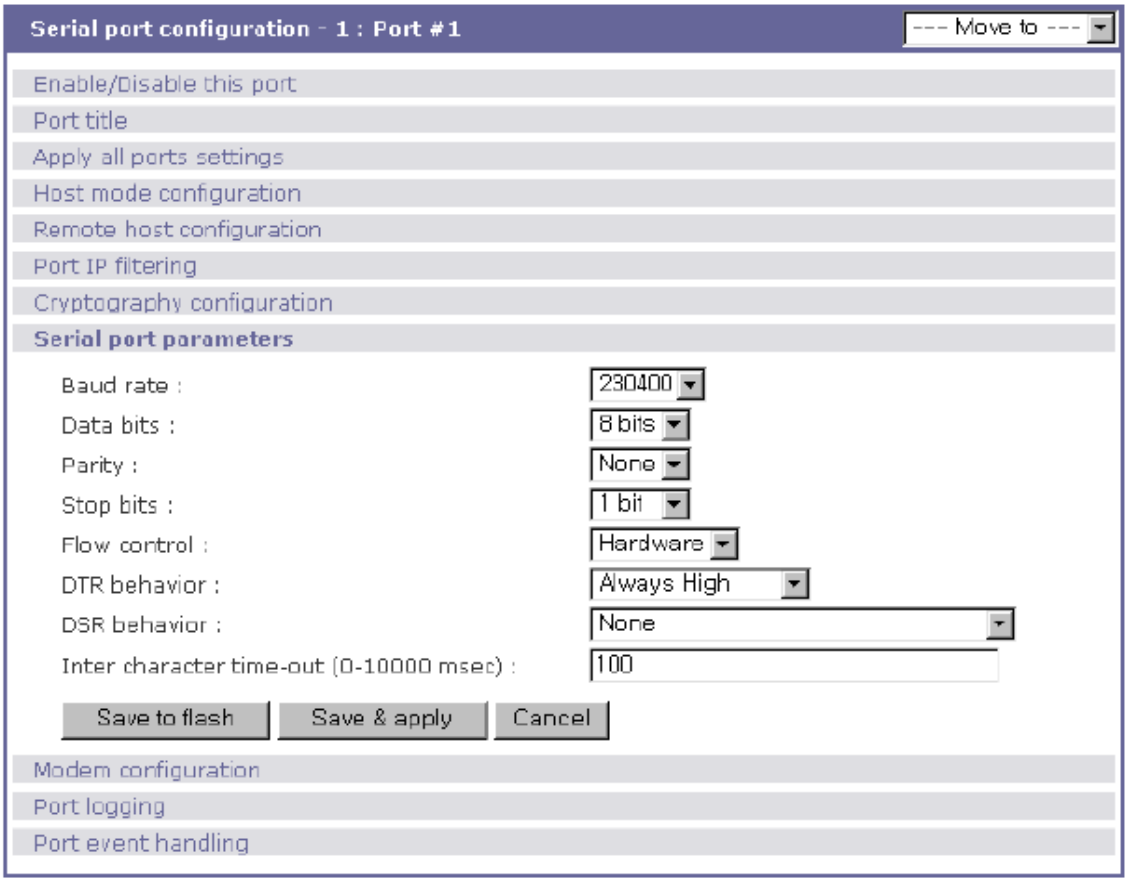



図 4-15 UART 設定

- **Parity**

  この値は、無し(none)、偶数(even)、奇数(odd)に設定することができます。

  工場出荷時のデフォルト値は無し(none)です。

- **Stop bits**

  ストップビットは 1 または 2 に設定可能です。

  工場出荷時のデフォルト値は 1 ビットです。

- **Flow Control （フロー制御）**

  フロー制御のファクトリデフォルト値は無し(None)です。ソフトウェアフロー制御(XON/XOFF)およびハードウェアフロー制御(RTS/CTS)の両方をサポートしています。ソフトウェアフロー制御の場合、特別な文字(0x11/0x13)を接続している 2 つの機器に送ります。ハードウェアフロー制御の場合は 2 つの機器間にシグナルを行き来させてデータ通信を制御します。

- **DTR/DSR behavior**

  DTR/DSRピンは、シリアルポートシグナルでモデムシグナル制御をエミュレート、またはTCP接続状態を制御します。DTR は書き込み専用出力シグナルであり、DSR は読み専用入力シグナルです。

  DTRオプションは3種類のうち1つを選択します。Always high(常にオン), always low(常にオフ), high when TCP/UDP is opened(TCP/UDP接続が確立すると、常時オン)、のうち一つです。

  DSR 入力の動作は 2 種類の中から1つを選択します。 None(無し)または allow TCP/UDP connection only by high(DSRがオンのときだけTCP/UDP接続を許可)です。

  Modem emulation モードの場合、リモートホストへの接続は、DSR がオンからオフになる時切断されます。

  STSシリーズに接続されたシリアルデバイスサーバーはDTRシグナルを制御することにより、STSシリーズのTCP/UDP接続を制御することができます。

  **注記: DTR/DSR設定変更はモデムがオンの間は有効ではありません。**

- **Inter-Character timeout**

  このパラメータは STS シリーズがその内部バッファからすべてのシリアルデータを取り出すインターバルを定義します。シリアルポートからの着信データがある場合、STS シリーズは内部バッファにデータを蓄積します。STS シリーズは内部バッファ内が一杯に、または inter character timeout で設定した一定間隔でデータを TCP/IP 経由で送信します。もしこの値が 0 であれば、内部バッファ内にあるデータは間隔をおかずにただちに送信されます。この値の適正値は使用するアプリケーションにより異なりますが、指定した Baud rate より 1 キャラクタ分大きい必要があります。たとえば、1200bps. 8 データビット、1 ストップビット、パリティ無しの場合、送信するビット合計は 10 ビットであるため、1 キャラクタおくるのに要する時間は:10bit/1200(bits/s) *1000(ms/s)=8.3ms. なので、inter-character timeout を 8.3ms より大きくする必要があります。この値は ms の単位で設定します。

### 4.2.10. モデムの設定(Modem configuration)

STS シリーズはシリアルポートへの直接モデム接続をサポートしています。サーバーのシリアルポートにモデムを接続するには、Modem Configuration 画面の Modem-init-string および DCD behavior を設定する必要があります。STSシリーズはホストモードがTCPモードに設定されているときのみモデム接続をサポートします。

- **Enable/Disable modem(モデムをオン・オフ)**

  この部分をオンにすることにより、STSシリーズのシリアルポートに直接モデムを接続することが可能になります。この部分がenableになっていると、このポートはモデム専用として使用されます。

- **Modem init-string**

  このパラメータ設定でモデム初期化ストリングを指定できます。Enable/Disable modem で Enable に設定してシリアルポートをモデムモードに設定すると STS シリーズは DTR ピンがオンになるか、シリアルポート設定関連のパラメータが変更されると、モデム初期化ストリングをシリアルポートに送ります。

- **DCD behavior**

  このパラメータが Allow TCP connection only by HIGH(ON のときだけ TCP 接続を許可)に設定すると、STS シリーズはシリアルポートの DCD が ON のときだけリモートホストからの接続を許可します。この機能はダイヤル・インモデムモードだけでシリアルポートを使用するときに便利です。この場合、モデムからの接続が確立されていない場合、STS シリーズは TCP サイドの接続を許可しません。

- **Automatic release modem connection**

  このパラメータが Enable(オン)の場合、モデム接続は TCP 接続が切断すると同時にモデム接続も終了します。この機能が Disable(オフ)のときは、TCP 接続が終了しても、接続が継続します。しかし、モデムの一方が接続を切断すると、実際の電話回線も切断されるということを明記してください。ですから、すべての TCP 接続が終了するときに STS シリーズのモデム接続が終了するためにあります。

ダイヤルアウト機能を使用する場合、DCD を None に設定してください。なぜならシリアルポートに接続したモデムにアクセスし、ダイヤルアウトコマンドをモデムに最初に送信する必要があるからです。

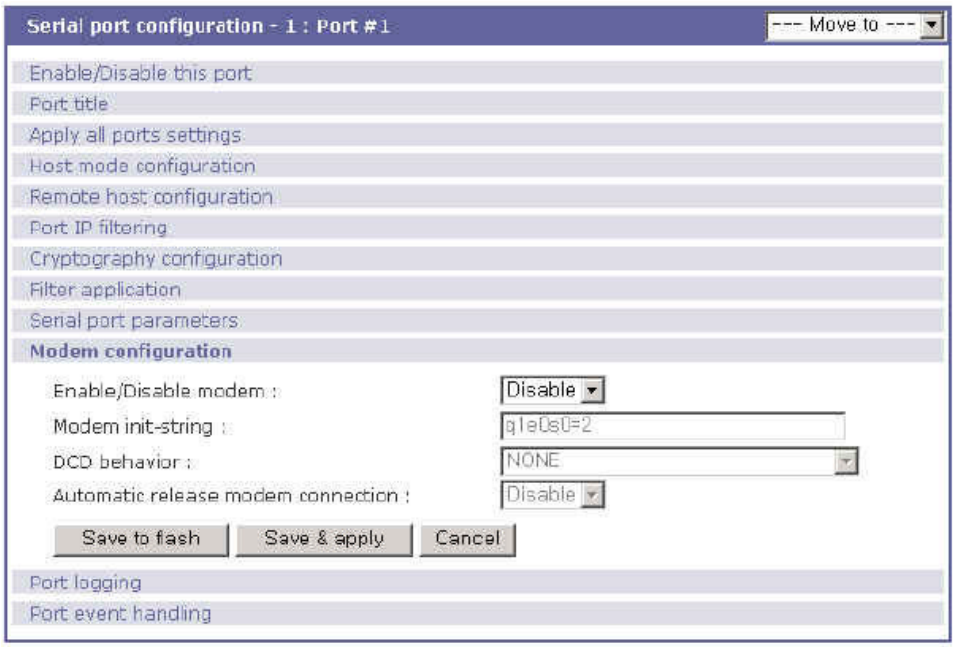



**図 4-16 モデム設定画面**

## 4.2.10. Port Logging(ポートロギング)

ポートロギング機能でシリアルポートから送信されるデータは SYSLOG サーバーまたは NFS サーバーのマウンティングポイントに保存されます。

- **Enable/Disable port logging（ポートロギングをオン・オフ）**
  このパラメータはポートロギング機能を Enabled/Disabled(オン・オフ)にします。
  ファクトリデフォルト値は Disabled（オフ）です。

- **Port log storage location（ポートログの保存場所指定）**
  ポートのログデータは STS シリーズの内部メモリ、ATA/IDE フィックスカード、SYSLOGサーバーまたは NFS サーバーのマウンティングポイントに保存されます。内部メモリがポートログデータを保存するために使用されるならば、ポートログデータは STS シリーズが電源オフになる時点で消去されます。シリアルポートのログデータを保存するには、保存場所をフィックスカード、SYSLOGサーバー、または NFS サーバーに指定します。これらの保存を実行するためには、各種メディアの設定をする必要があります。

- **Port log buffer size(ポートログのバッファーサイズ)**
  このパラメータはログ可能なポートログ数を定義します。内部メモリでログデータを保存する場合、ポートバッファの最大容量は 3200Kbyte です。（各シリアルポートの全ポートバッファーサイズ合計は、3200Kbytes 以下にする必要があります）デフォルト設定値は 4Kbytes です。ATA/IDE ディスクカードを使用するときは、最大容量はカードのスペックによります。NFS サーバーでログデータを保存する場合、最大ポートバッファ数は無制限です。NFS サーバーが正常に動作するよう設定してください。SYSLOG サーバーを使用するときは、ポートログバッファーサイズを設定することはできません。

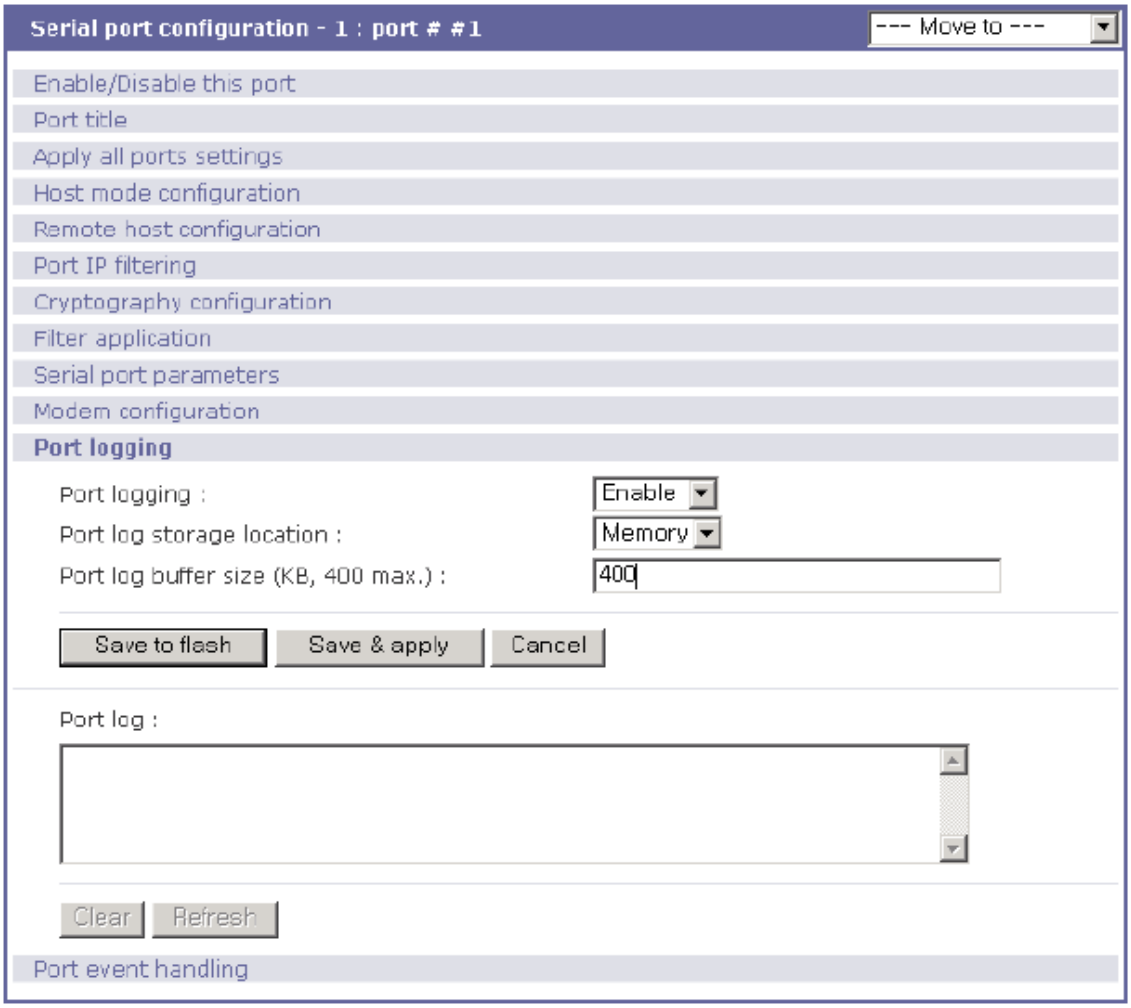



図 4-17 ポートロギング設定画面

### 4.2.11. Port イベント操作の設定

STS シリーズは、Port event handling 設定を行うことにより、シリアルポートにつないであるシリアルポートからのデータを監視またはデータに対してのリアクションを行うことができます。名前の通り、各シリアルポートに e-mail/SNMP 通知や、Port event handling 設定で直接シリアルポートに送信されたコマンドを発動するキーワードを定義します。これはあらかじめ定義したキーワードを検知すると、シリアルポートに直接接続したデバイスを管理または操作、データを監視することが可能になります。STS シリーズとシリアルデバイス間の接続ステータスおよび STS シリーズとリモートホスト間の TCP 接続ステータスも同様に監視および管理することができます。

各リアクションはイベントごとに個々に設定します。リアクションは e-mail 送信、SNMP トラップ送信、コマンド送信、またはすべてのリアクションの組み合わせも可能です。

● **Port event handling(ポートイベントの操作)**

Port event handling 機能をオンにするには、Port event handling を“enable”にしてください。これはグローバル・パラメータですのでこの機能をオフ(disable)にすると STS シリーズはポートイベントにおいてアクションをとりません。

● **Notification interval(通知間隔)**

ポートイベントの操作トラップを回避するために、Notification interval(通知間隔)パラメータがあります。STS シリーズは事前定義したキーワードを検知すると、この通知間隔で e-mail または SNMP トラップを送信します。この数値が小さければ小さいほど、より早い通知を期待できますが、その分多くのシステムリソースを使用します。この値を大きくすることにより、システムリソースを不必要に使用することがなくなります。

**注記: キーワードレスポンスのポートコマンドはこのパラメータにより影響を受けることはありません。ポートコマンドは対応するキーワードが検知されるとすぐに送信されます。**

● **Email notification(メール通知)**

STS シリーズはメール通知機能をオン(Enable)またはオフ(Disable)にすることができます。SMTP サーバー設定で設定された SMTP サーバーを使用します。SMTP サーバーが正しく設定されていない、またはサーバーがオフのときは、このメール機能もオフになります。SMTP サーバー設定の詳細に関しては 3.4. SMTP 設定を参照してください。

● **Title of Email(メールの題名)**

このパラメータは、事前設定されたキーワードが検知された時に送るメールの件名を指定します。

● **Recipient's Email address (メールの宛先)**

このパラメータは、事前設定されたキーワードが検知された時に送るメールの宛先を指定します。

● **SNMP notification (SNMP 通知)**

このパラメータは STS シリーズの SNMP 通知をオンまたはオフにします。

● **Title of SNMP trap(SNMP トラップの題名)**

このパラメータは事前設定されたキーワードが検知された時に STS シリーズによって送信される SNMP トラップの題名を指定します。

● **SNMP trap receiver IP**

このパラメータは事前設定したキーワードが検知された時に、SNMP トラップ通知を受信する

SNMP トラップ受信側の IP アドレスを設定します。

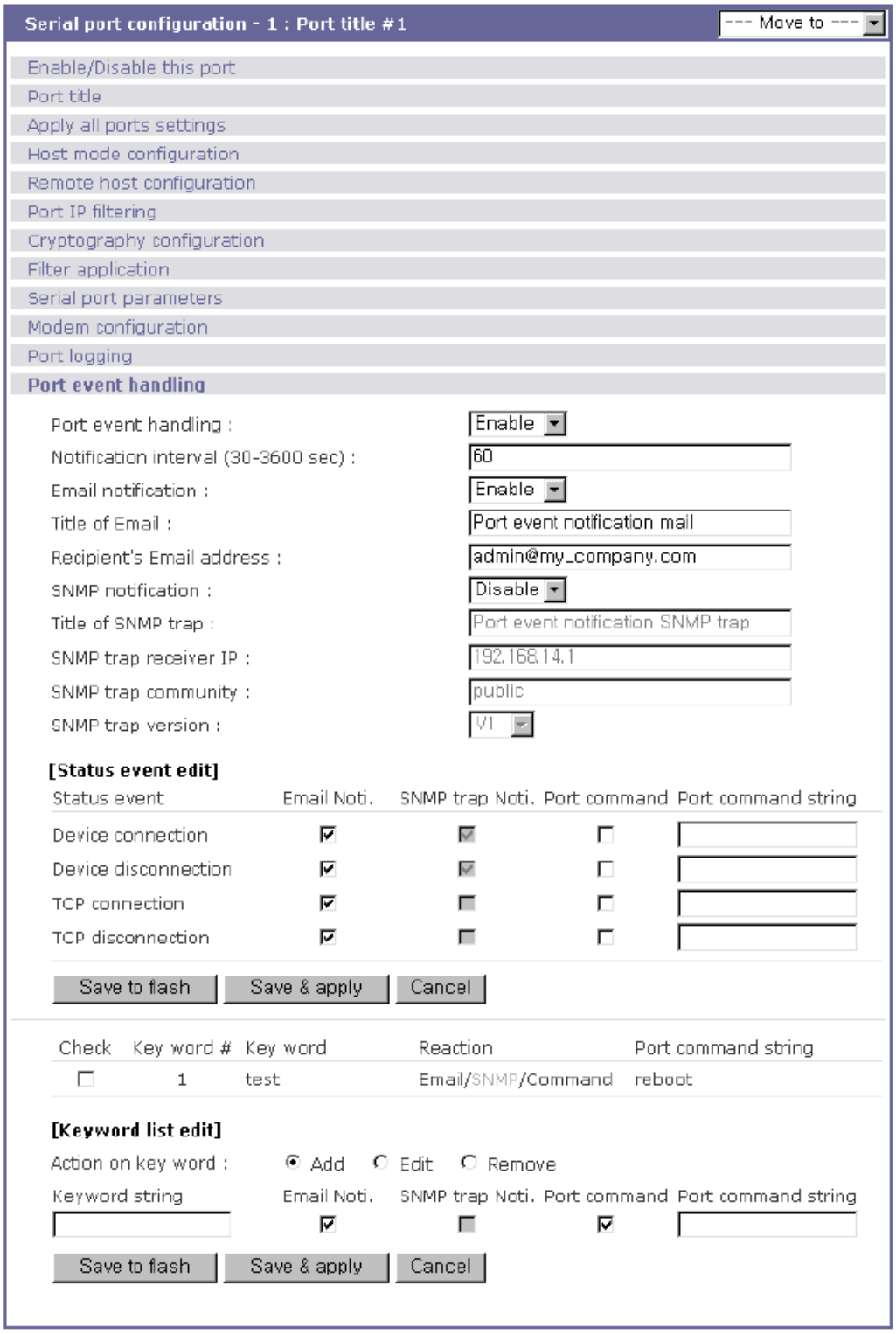



図 4-18 Port event 操作設定画面

● **SNMP trap community**

このパラメータは事前設定したキーワードが検知された時に SNMP トラップメッセージに含まれるコミュニティーを設定します。

- **SNMP trap version**
  このパラメータは事前設定したキーワードが検知された時に送信する SNMP トラップのバージョンを設定します。

**[Status event edit] 状態イベント編集**

- **Device connection/disconnection**
  シリアルデバイス接続・切断イベントにおいて行う動作のボックスにチェックマークを入れてください。
- **TCP connection/disconnection**
  TCP 接続・切断イベントにおいて行う動作のボックスにチェックマークを入れてください。

**[Keyword list edit] キーワードリスト編集**

- **Action on keyword**
  このイベントを選択するには Add, 解除するにはRemoveを選択します。
- **Keyword string**
  ここでキーワードを設定します。
- **Email notification(メール通知)**
  選択したキーワードでメールを通知する/しないを設定します。
- **SNMP trap notification (SNMP トラップ通知)**
  選択したキーワードで SNMP トラップ通知を送信する/しないを設定します。
- **Port Command(ポートコマンド)**
  選択したキーワードでポートコマンドアクションをオン・オフにするかを選択します。
- **Port command string (ポートコマンド・ストリング)**
  STS シリーズは事前に設定したキーワードが検知されるときにシリアルポートにつないであるデバイスに直接の反応をサポートします。このメニューでシリアルポートに送信されるコマンドまたはストリングを指定します。

## 4.3. 全ポート設定

すべてのポートの設定が同様または同じである場合、全ポート設定を同時に行うことが可能です。"all port configuration"機能で変更した内容がすべてのシリアルポートに適用されます。 "apply all port setting"オプションがオフになっているポートには変更は適用されません。

"All port configuration"パラメータには以下の選択肢があります。

1. Port enable/disable ,ポートのオン・オフ

2. Port title ポートのタイトル
3. Host mode ホストモード
4. Remote host configuration リモートホスト設定
5. Port IP filtering ポートIPフィルタリング
6. Cryptography configuration 暗号化設定
7. Filter application フィルターアプリケーション
8. Serial port parameters シリアルポート パラメータ
9. Modem configuration モデム設定
10. Port logging ポートロギング
11. Port event handling ポートイベント操作

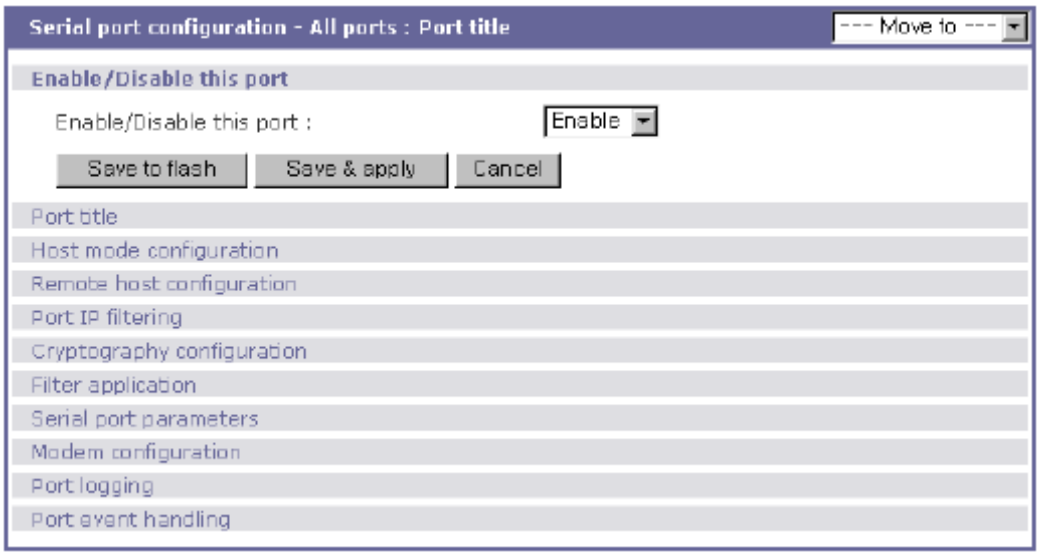



**図 4-19 All port configuration 画面**

- **Port enable/disable**

  このパラメータでポート機能のオン・オフを選択します。

- **Port title**

  このパラメータが特定のストリングに設定されている場合、各シリアルポートのポートタイトルはこのストリングとポート番号との組み合わせで設定されます。たとえば、ポートタイトルが “my server”であり、ポート1を使用している場合 “my server #1”となります。

- **Host mode**

  ホストモードが TCP または UDP モードに設定されている場合、各シリアルポートのリスニングポート番号は次の式によって設定されます。

*（リスニングポート番号＋シリアルポート番号-1）*

各ポートの他パラメータは“all port configuration”により設定した値と同じになります。

- **Remote host configuration, Port IP filtering, Cryptography configuration, Filter application, Serial port parameters, Modem configuration, Port logging, Port event handling**

  “all port configuration”で設定した上記のパラメータはすべてのシリアルポートに同様に適用されます。

# 5. PCカード設定(PC Card Configuration)

STS シリーズには拡張機能用のPCカードスロットが一基あります。4 種類のPCカードをサポートしています。

- Wireless LAN card 無線LANカード
- Modem card モデムカード
- ATA/IDE fixed disk card ATA／IDEフィックスディスクカード

LANまたは無線LANカードで他のネットワーク接続経由でアクセス可能になります。ATA／IDEフィックスディスクカードはユーザーがシステムおよびシリアルポートログデータを保存し、持ち運びが可能になります。

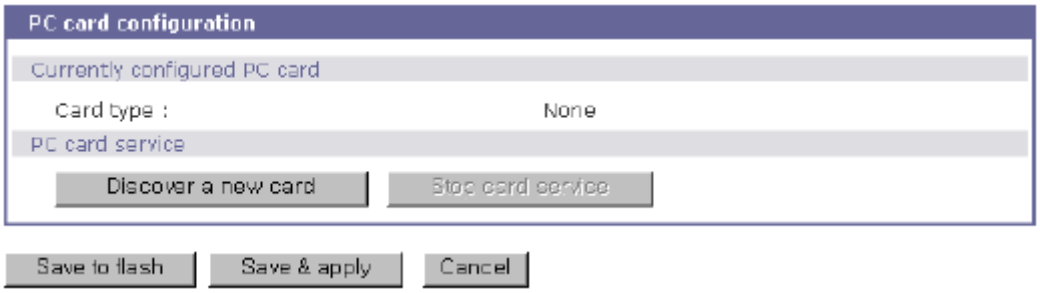



**図 5-1 初期PCカード設定メニュー画面**

PCカードスロットを使用するには、次の手順を完了してください。

Step 1. PCカードをPCカードスロットに挿入します。

Step 2. PCカード設定メニューから Discover a new card を選択します。

Step 3. STSシリーズはプラグ・アンドプレイ機能でカードタイプを検知します。それから設定メニュー画面を表示します。それからカードの操作パラメータが設定可能になります。

Step 4. Save to flash を選択して設定を保存します。

Step 5. [Apply changes]をメニューから選択し、新規の設定を適用します。

STSシリーズがPCカードを認識できない場合、次のエラーメッセージがメニュー画面に表示されます。

**図 5-2 検知エラーメッセージ**

付録B.「STSシリーズがサポートしているPCカード一覧」を参照してください。

PCカードを停止または取り出す場合は、次の手順に従ってください。

Step 1. [(Ban-show the actual button)Stop card service]を選択してください。

Step 2. [Save to flash]を選択し、設定の変更を保存します。

Step 3. [Apply changes]をメニューから選択し、変更を適用します。

Step 4. PCカードスロットからPCカードを取り出します。

**注記: 上記の手順に従わないでPCカードを取り外した場合、障害が生じる場合があります。**

## 5.1. LANカード設定

LAN カードは 2 つのネットワークインターフェースおよび2つのIPアドレスを作成します。各シリアルポートに有効なIPアドレスを割り当てることができます。組み込み式ネットワークインターフェースまたはSTSシリーズのPCカードLANインターフェース環境にとって有効なIPアドレスを使用してください。

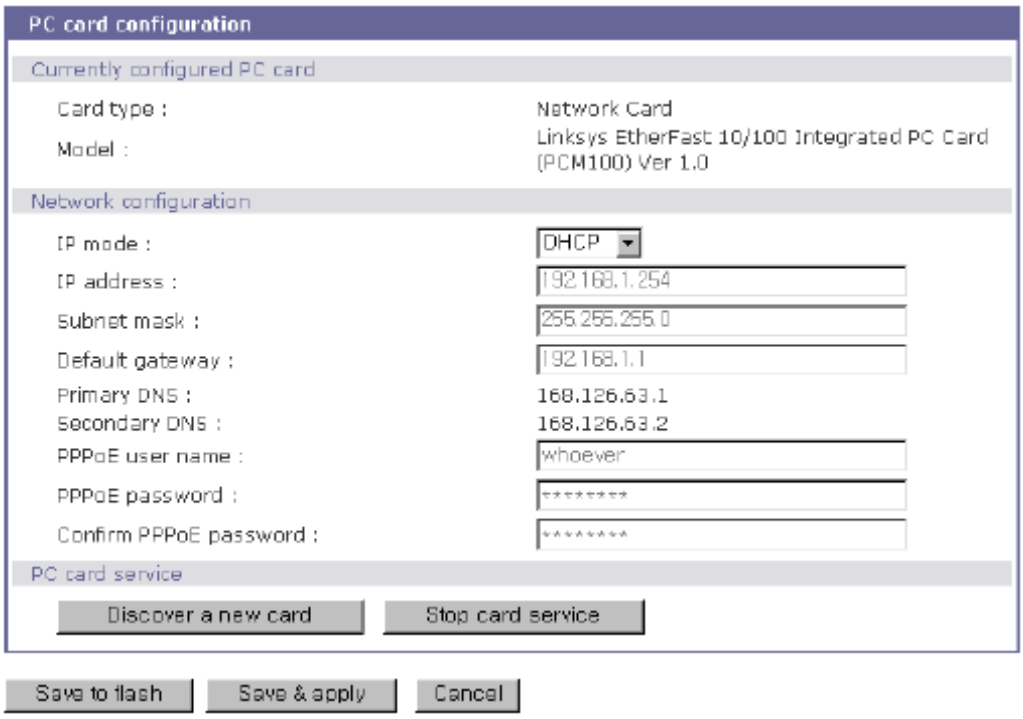



**図 5-3 PC LAN card configuration 画面**

PC LAN カードの設定は手動でカードの種類を選択し、プライマリ・セカンダリDNSサーバーを設定する必要があります。3.1.IP設定に章で詳細な他の設定方法が書かれています。

付録 B.「STSシリーズでサポートしているPCカード一覧」を参照してください。

## 5.2. 無線 LAN カード設定

無線LANカードを使用することにより、2 つのネットワークインターフェース、および 2 つのIPアドレスを持つことになります。各シリアルポートに有効なIPアドレスを割り当ててください。

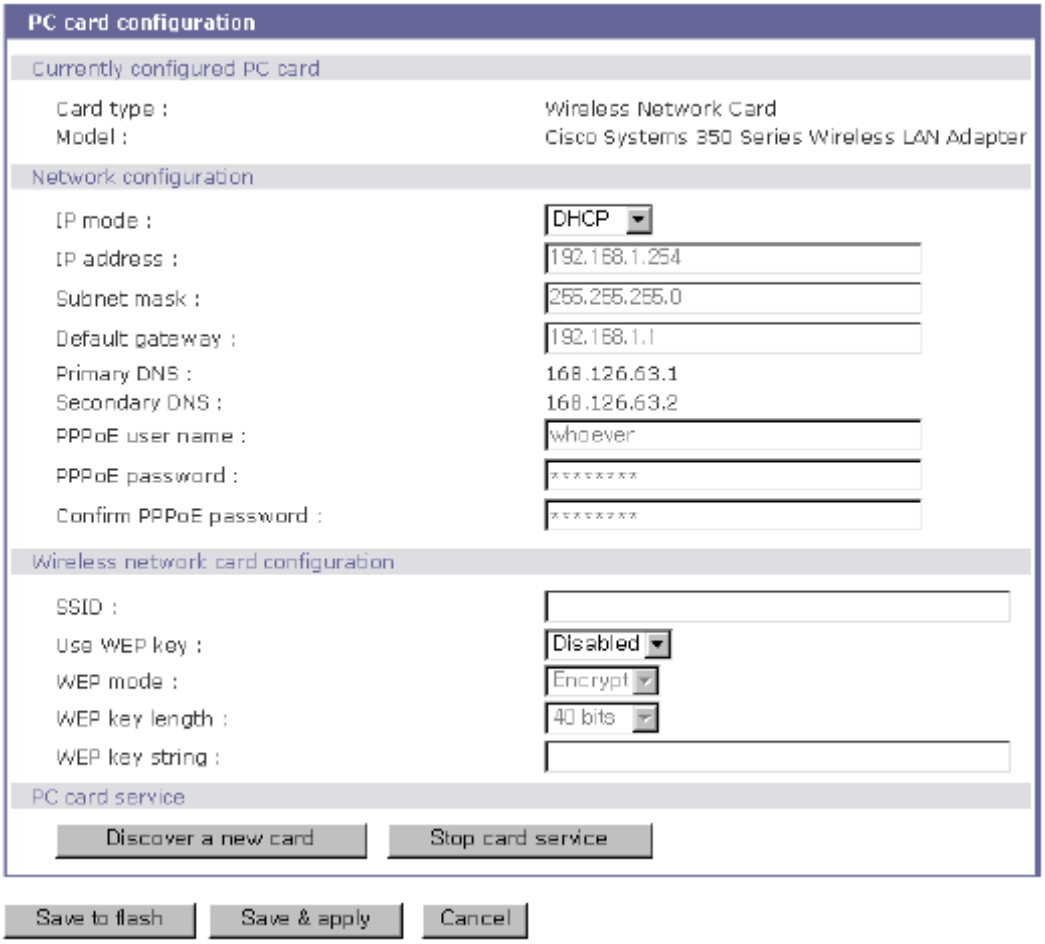



**図 5-4 PC無線LANカード設定画面**

PC 無線 LAN カードの設定は手動でカードの種類を選択し、プライマリ・セカンダリDNSサーバーを設定する必要があります。3.1.IP設定に章で詳細な他の設定方法が書かれています。

付録 B. 「STSシリーズでサポートしているPCカード一覧」を参照してください。

STSシリーズは SSID(Service Set Identifier)および WEP(Wired Equivalent Privacy)キー機能をサポートしています。SSID を設定してアクセスポイントを指定します。また WEP を暗号化または共有化するかの設定を行います。WEPキーの長さは 40 または 128 bits である必要があります。40-bit WEP キーは 5 つの 16 進数コード(コロンなし)を入力します。128-bit キーの場合は 13 の 16 進数(コロンなし)コードを入力します。

例えば、128bits WEP キーオプションを使用するために次のような 13 の 16 進数コードを入力します。

000F25E4C2000F25E4C2000F24

付録 B. 「STSシリーズでサポートしているPCカード一覧」を参照してください。

## 5.3. シリアルモデムカード設定

PCカードスロットをモデムとして使用することにより、外部モデムとシリアルポートを束縛することなくユーザーがオンラインアクセスすることを可能にします。ほとんどの 56Kbps PC シリアルモデムカードはこのPCカードスロットとの互換性があります。付録 B. 「STSシリーズでサポートしているPCカード一覧」を参照してください。

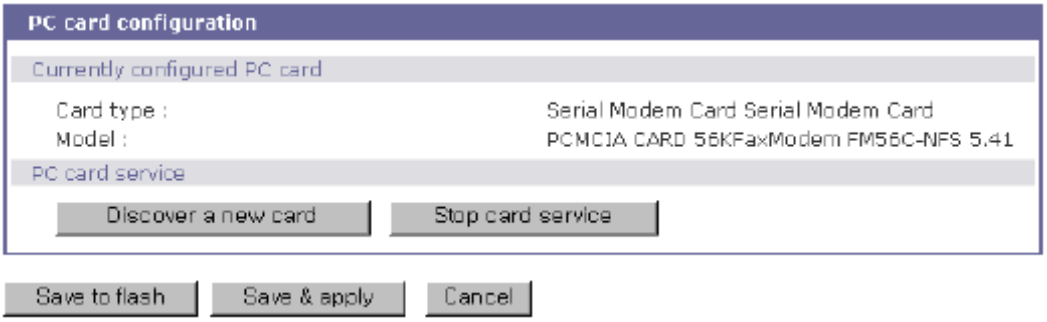



図 5-5 PCシリアルモデムカード設定

## 5.4. ATA/IDE フィックス・ディスクカード設定

システムおよびシリアルポートログを保存するために使用する ATA/IDE フィックスディスクカードのデータサイズをまず設定する必要があります。STS シリーズは自動的に合計保存容量およびディスク容量を認識します。

Delete を選択することにより現行のファイルを削除します。また Format を選択するとカードのフォーマットを行います。STSシリーズはディスクカード用に EXT2 および VFAT ファイルシステムをサポートしています。STSシリーズ設定のエクスポート・インポートすることによりディスクへファイルの設定を保存することができます。

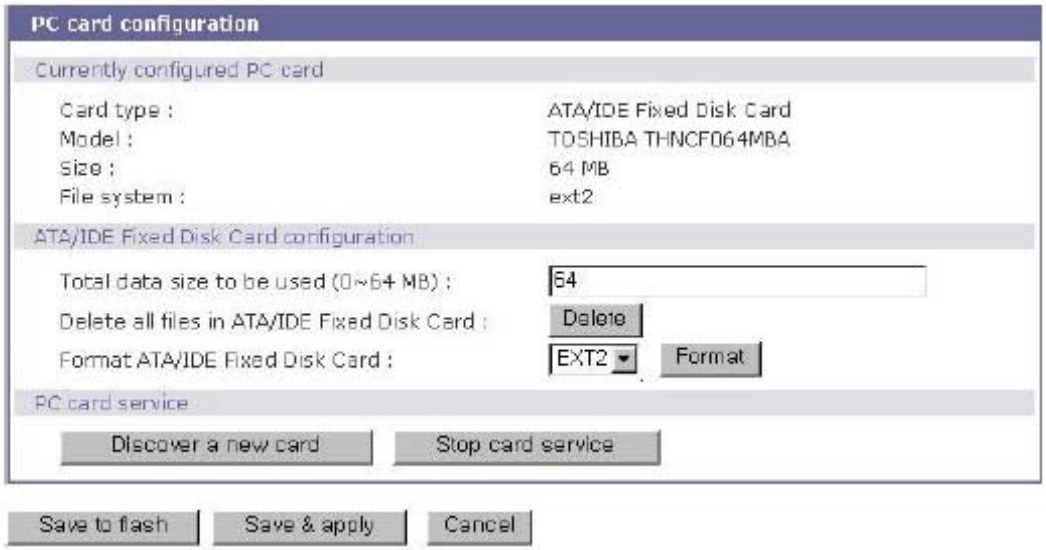



図 5-6 PC ATA/IDE フィックスディスクカード設定

# 6. システム管理(System Administration)

STS シリーズは Status Display Screen 経由でシステムのステータスおよびログデータを表示します。この画面は管理する目的のためにあります。System Status データにはモデル名、シリアル番号、ファームウェア・バージョン、および STS シリーズのネットワーク設定が含まれます。STS シリーズは、System-logging(システムロギング)機能により指定した受信デバイスにログデータを自動的にメールで送信することができます。
この画面で STS シリーズのデバイス名、日時設定、ファクトリデフォルト値へリセット可能です。ウェブインターフェース、リモート・コンソールまたはシリアルコンソールを使用してファームウェアのアップグレードができます。

## 6.1. System Status (システムステータス)

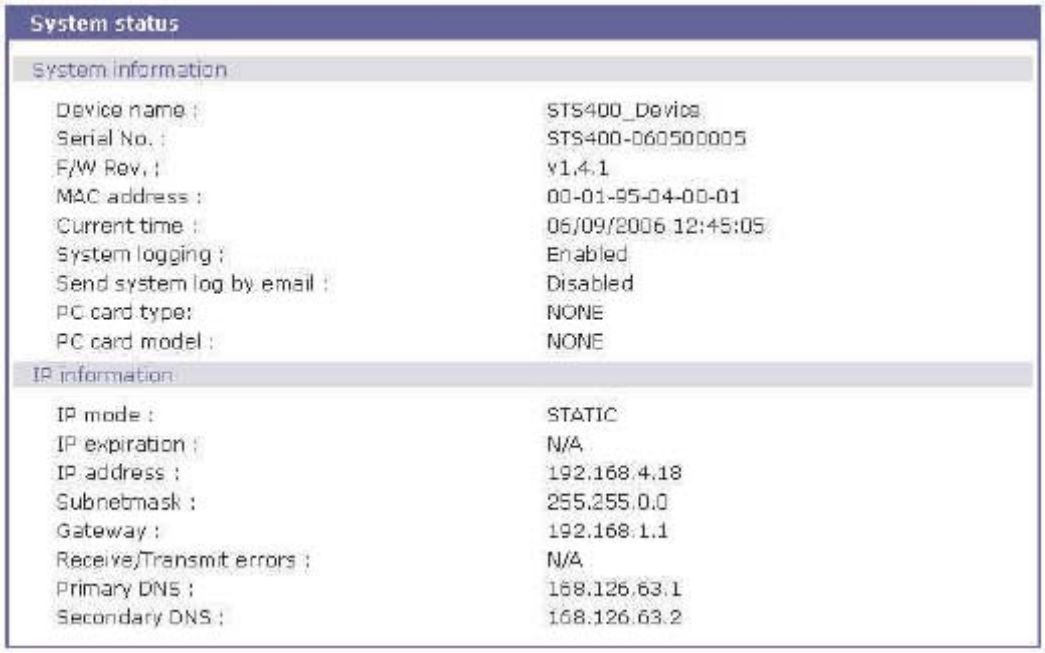



**図 6-1 System Status 画面**

## 6.2. System Logging (システムロギング)

STS シリーズはシステムロギング機能およびシステムログステータス表示を行います。STS シリーズはシステムロギングプロセスのオン/オフ、システムログバッファサイズ、またログ保管場所を設定します。

- **System log storage location(システムログの保存場所)**
  システムログは STS シリーズの内部メモリ、ATA/IDE フィックスディスクカード、NFS サーバーのマ

ウンティングポイント、または SYSLOG サーバーに保存することができます。ログデータの保存場所に内部メモリを使用すると、STS シリーズの電源をオフにする時にデータも消去されます。ログデータを保存するときは、保存先を SYSLOG サーバーもしくは NFS サーバーに設定してください。これには事前にそれらメディアの設定をする必要があります。この設定が正しくなければ、ログは保存されません。

- **System log buffer size(システムログのバッファーサイズ)**
  このパラメータではシステムログの最大保管量を定義します。内部メモリを使用してデータを保存するときのシステムログの合計サイズは、300 Kbytes を超過してはなりません。
  ATA/IDE フィックスディスクカードでログデータを保存する場合の最大バッファサイズは、カードの容量によります。NFS サーバーの場合、無制限です。NFSサーバーがポートロギングシステムが適正に動作するように事前に設定してください。SYSLOG サーバーは事前に設定をすることはできません。

STS シリーズは未送信のログが事前に設定した値になると、自動的にログデータを送信する機能もあります。この機能をオンにするのであれば、メールを送信するための初期設定が必要になります。これらのパラメータはメール送信を発動するためのパラメータを設定してください。これらのパラメータはメールを送るために必要なログのデータ量、受取人のメール宛先などです。
図 6-2 は設定およびシステムログ閲覧画面です。

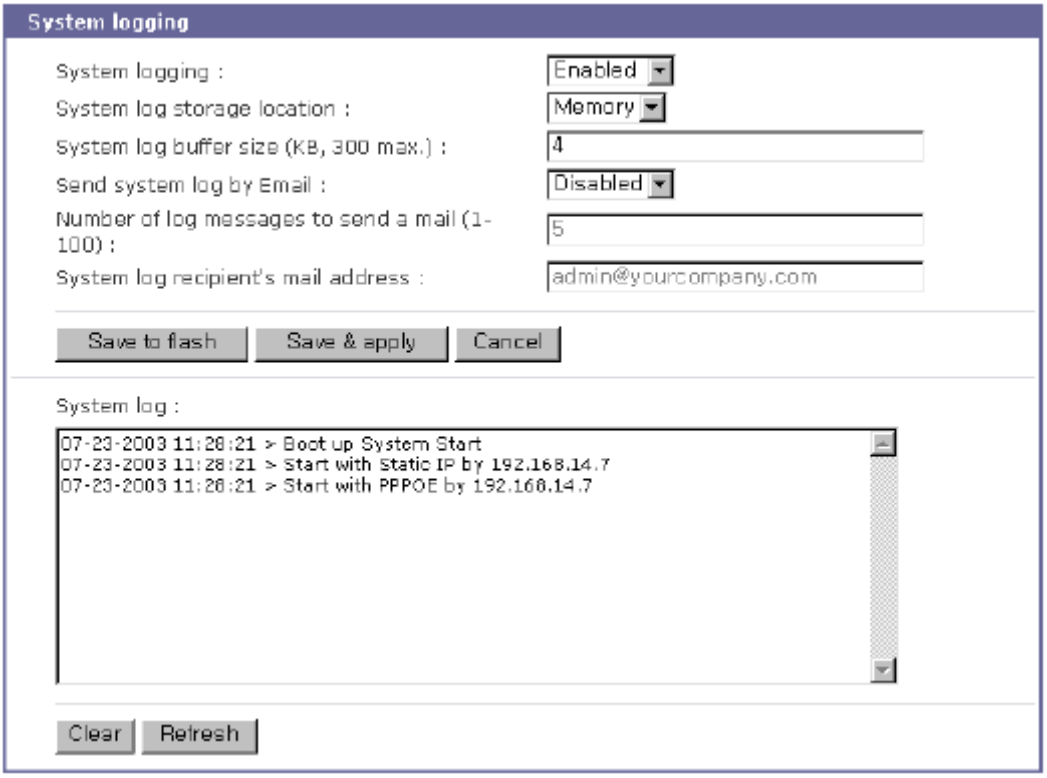



**図 6-2 システムログ設定および閲覧画面**

## 6.4. Users Logged on List (ユーザーログオン・リスト)

STSシリーズのシェルにおける現行および過去のユーザー履歴を閲覧できます。

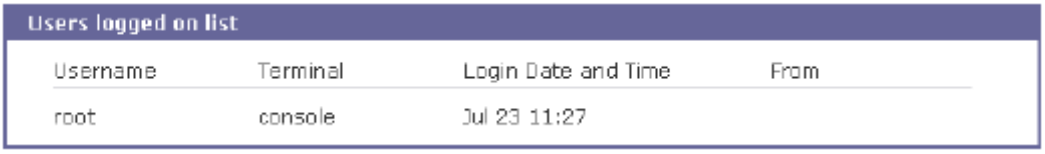



**図 6-3 Users logged on list 画面**

システムにログインしたユーザーの情報は以下です。

ユーザー名

セッションの端末タイプ

接続時間

リモートホストのIPアドレス

**注記: ウェブ経由でアクセスしたユーザーはリスト上に表示されません。接続は常に HTTP/HTTPS プロトコルを使用して行われるとは限りません。**

## 6.4. Change Password (パスワードの変更)

STS シリーズ、システム管理ユーザー用のパスワードは、このメニューで変更します。

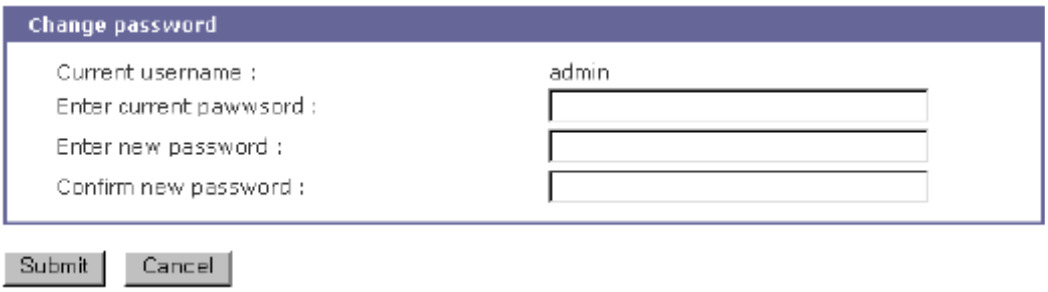



**図 6-4 Change Password 画面**

## 6.5. Device Name Configuration (デバイス名設定)

STS シリーズは管理目的で、固有の名称をもっています。図 5-4 はデバイス名設定画面です。 ユーザーがデバイス名を変更すると、ホスト名も同様に変更されます。


図 6-5 Device name configuration 画面

デバイス名にスペース文字を使用することはできません。デバイス名を空白のままにすると、自動的に IP アドレスがホスト名になります。HelloDeviceManager というデバイスマネージャプログラムにも使用されます。

## 6.6. User Administration （ユーザー管理）

STSシリーズはポートアクセス用のユーザー認証を行います。図 6-6 にあるようにユーザー管理画面でポートアクセスを設定します。ユーザーが追加されると、ユーザーがアクセス許可されるポートが割り当てられます。TCPモードのみこの認証機能を使用することができます。

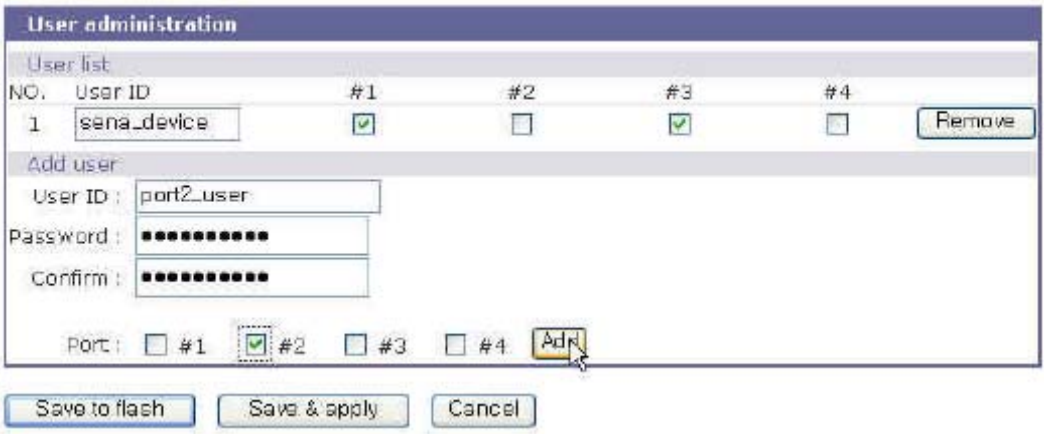



図 6-6 User Administration 画面

## 6.7. 日付および時刻の設定

STS シリーズは現在の時刻および日付を表示します。STS シリーズの時間およびカレンダー設定は内部バッテリ電源によりバックアップされます。 図 6-7 に示されているように、現行時間および日付を変更可能です。

STS シリーズは NTP（Network Time Protocol）サーバーでも時間を設定することができます。NTP 機能がオンのとき、毎リブート時に、NTP サーバーから時間情報を取得し、更新します。NTP サーバーを 0.0.0.0.に設定すると、STS シリーズはデフォルト NTP サーバーを使用します。この場合、STS シリーズはネットワークからインターネットにつないである必要があります。ユーザーの場所に応じて UTC からタイム・オフセットも設定する必要があるかもしれません。

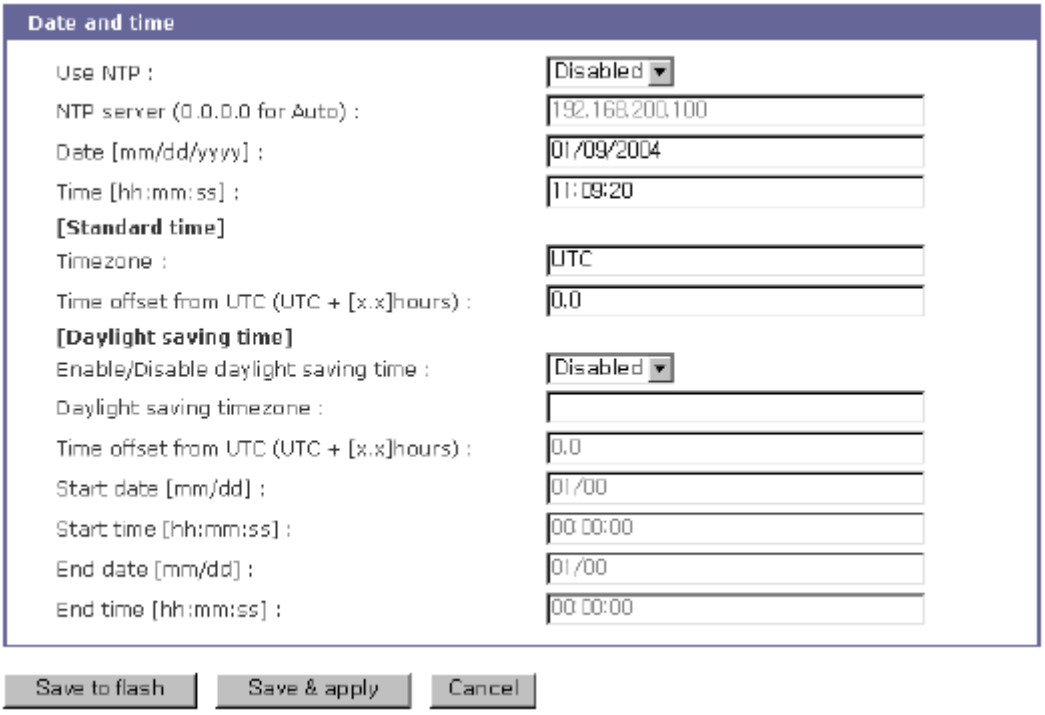



**図 6-7 Date and time configuration 画面**

## 6.8. コンフィギュレーション管理

現在の設定値を CF カード、NFSサーバー、ユーザースペース、またはローカルマシンにあるファイルに送り、それから手に入れた設定を現行の設定にインポートします。

ユーザーは全パラメータをFactory Defaultを選択することにより、ファクトリデフォルト値に戻すことができます。図 6-8 では、設定管理画面です。設定データのインポート/エクスポートを正しく設定するために、以下のパラメータを理解する必要があります。

**Configuration Export(設定値エクスポート)**

**Location:** エクスポート先

**Encrypt: Yes or No**

**File name**

**Configuration import(設定値インポート)**

| | |
|---|---|
| **Location:** | インポートする場所。FactoryDefault を選択すると、設定値が工場出荷時に戻ります。 |
| **Configuration Selection:** | 何の設定値がインポートされたかを識別します。 |
| **Encrypt: Yes or No** | Location がファクトリデフォルトの場合、無効になります。 |
| **File Selection:** | CF カード、NFSサーバーおよびユーザースペースの一つである選択し |

た場所から暗号化オプションのエクスポートしたファイルの一覧を表示します。

**Local :** Location がローカルマシンの場合、ローカルマシンからエクスポートしたファイルを閲覧することができます。

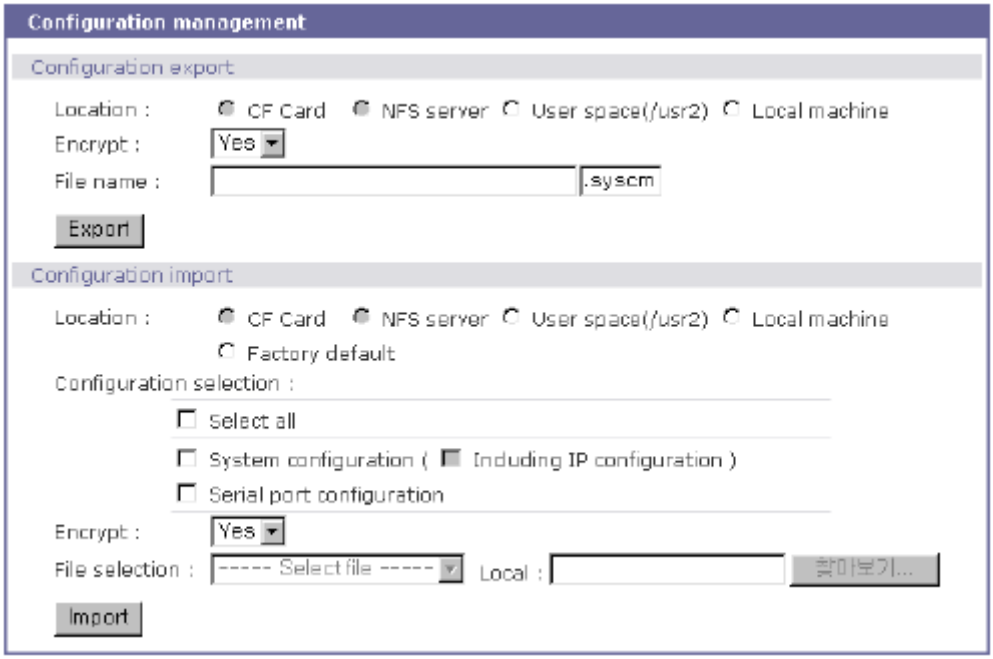



**図 6-8 Configuration management(設定管理)画面**

現行の設定をエクスポートするには、次の作業を行ってください。

1. エクスポート先を選択
2. Encrypt オプションを選択
3. File Name を入力
4. Export ボタンをクリック

エクスポートされた設定をインポートするには、次の作業を行ってください。

1. インポート先の Location を選択
2. インポートする設定を選択 Configuration Selection から
3. 暗号化オプションを選択(オン・オフ)
4. Location がローカルマシンまたは Factory Default でない場合、ファイル選択リストボックス内からインポートするファイルを選択
5. 場所がローカルマシンの場合ブラウズボタンをクリックすることによりインポートするファイルを選択します。
6. Import ボタンをクリック

## 6.9. ファームウェア・アップグレード

ファームウェア・アップグレードはシリアル、リモート・コンソール、またはウェブインターフェースから可能です。最新のアップグレードは弊社サイトから入手可能です。

http://www.intersolultionmarketing.com/downloads.html

図 6-9 にはウェブインターフェース経由のファームウェア・アップグレードを示しています。


**図 5-9 Firmware upgrade ファームウェア・アップグレード画面**

ウェブ経由でのファームウェア・アップグレード方法は以下の手順です。

1. Browse ボタンをクリックし、最新のファームウェア・バイナリを選択する
2. 選択したバージョンをアップロードする
3. アップグレードが完了すると、システムは変更を適用するためにリブートする

リモートまたはシリアルコンソールでファームウェアをアップグレードする場合、TELNET/SSH または Zmodem 転送プロトコルをサポートしたターミナルエミュレーションプログラムを使用します。変更前の設定はファームウェア・アップグレード後に保存されます。

リモート・コンソールからのファームウェアのアップグレード手順

1. 最新のファームウェアを入手
2. TELNET/SSH かシリアルコンソールポートどちらかを使用したターミナルエミュレーションプログラムを接続します。
   （TELNET または SSH を使用することによりファームウェアアップグレードによる所要時間を短縮することができます）。

3. ファームウェアアップグレード画面においてログインを行います。

```
 Login : admin
 Password : *****

------------------------------------------------------------------------------
 Welcome to STS-800 configuration page
 Current time: 07/23/2003 15:04:07    F/W REV.:    v1.0.0
 Serial No.:   STS800438349-42944     MAC address: 00-01-95-04-19-5a
 IP mode:     Static IP            IP address:  192.168.14.7
------------------------------------------------------------------------------
 Select menu:
  1. Network configuration
  2. Serial port configuration
  3. PC Card configuration
  4. System administration
  5. Save changes
  6. Exit without saving
  7. Exit and apply changes
  8. Exit and reboot
  <Enter> Refresh
---> 4
------------------------------------------------------------------------------
 System administration
------------------------------------------------------------------------------
 Select menu:
  1. System status
  2. System logging
  3. Device name: SS800 Device
  4. Date and time
  5. Change password
  6. User file upload
  7. Reload factory default settings
  8. Reload factory default settings except IP settings
  9. Firmware upgrade
  <ESC> Back, <Enter> Refresh
--->9
Do you want to upgrade firmware? (y/n): y
Transfer firmware by zmodem using your terminal application.
To escape, press Ctrl+X
**B0ff000005b157
```

**図 6-10 Firmware Upgrade コンソール画面**

4. オンラインの指示に従って Zmodem プロトコルでファームウェアバイナリファイルを転送します。
5. アップグレードが終了すると、システムは変更を有効化するためにリブートを行います。
6. ファームウェア・アップグレードが失敗すると、STS シリーズはエラーメッセージを表示します。（図 6-12 参照）その場合には現行のファームウェア設定を維持します。

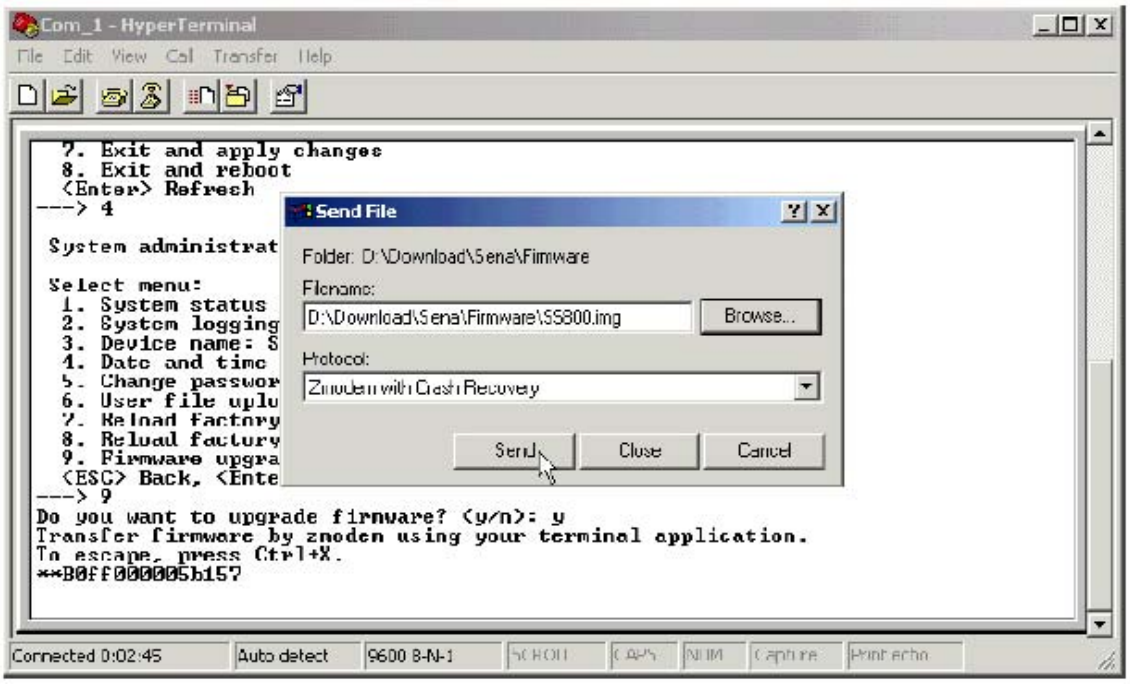



**図 6-11 Zmodem(Tera Term Pro)によるバイナリ・ファイルの転送画面**

```
--->9
Do you want to upgrade firmware? (y/n): y
Transfer firmware by zmodem using your terminal application.
To escape, press Ctrl+X
**B0ff000005b157
**B0ff000005b157
**B0ff000005b157
**B0ff000005b157
Firmware upgrade failed !
 Now reboot ...
```

**図 6-12 ファームウェア・アップグレード失敗メッセージ時の画面**

## 6.10. User File Uploading ファイルのアップロード

ユーザーは独自のファイルをSTSデバイスサーバーにアップロードすることが可能です。このアップロード機能はコンソールメニューのみあります。ファイルアップローディングメニューは、4. System administration → 6. User file upload から入ります。 ユーザーファイルをSTSにアップロードするには、TELNET/SSH またはターミナルソフトプログラム（Zmodem 転送プロトコルサポート）で行います。

次の手順に従ってください。

1. アップロードするファイルを準備する
2. TELNET／SSHまたはシリアルコンソールポートからターミナルエミュレーションプログラムをつなぐ

3. 図 6-13 にあるようにユーザーファイルアップロードメニューから選択する
4. オンラインの指示に従い図 6-11 にあるようにZmodemプロトコルを使用してユーザーファイルを転送する
5. アップロードが完了すると、システムは 6-13 にあるように、メッセージが表示される。

**注記: ユーザーファイルのアップロードはユーザースペースディレクトリ(/usr2)のみ許可されています。STSサーバー内部のファイルシステム情報の詳細は 8.2 フラッシュパーティションセクションを参照してください。**

```
--------------------------------------------------------------------------------
 Welcome to STS-800 configuration page
 Current time: 08/14/2003 11:56:13     F/W REV.    : v1.0.0
 Serial No.  : STS800438349-42944      MAC address: 00-01-95-04-d3-03
 IP mode     : DHCP                    IP address : 192.168.222.206
--------------------------------------------------------------------------------
 Select menu:
  1. Network configuration
  2. Serial port configuration
  3. PC Card configuration
  4. System administration
  5. Save changes
  6. Exit without saving
  7. Exit and apply changes
  8. Exit and reboot
  <Enter> Refresh
---> 4
--------------------------------------------------------------------------------
 System administration
--------------------------------------------------------------------------------
 Select menu:
  1. System status
  2. System logging
  3. Device name: STS800 Device
  4. Date and time
  5. Change password
  6. User file upload
  7. Reload factory default settings
  8. Reload factory default settings except IP settings
  9. Firmware upgrade
  <ESC> Back, <Enter> Refresh
---> 6
 Do you want to upload a file to user space? (y/n): y
 Enter a filename: test.txt
 The file will be saved as /usr2/test.txt.
 Transfer a file by zmodem using your terminal application.
 To escape, press Ctrl+X.
**B01ff000005b157

Uploading a file is completed.
```

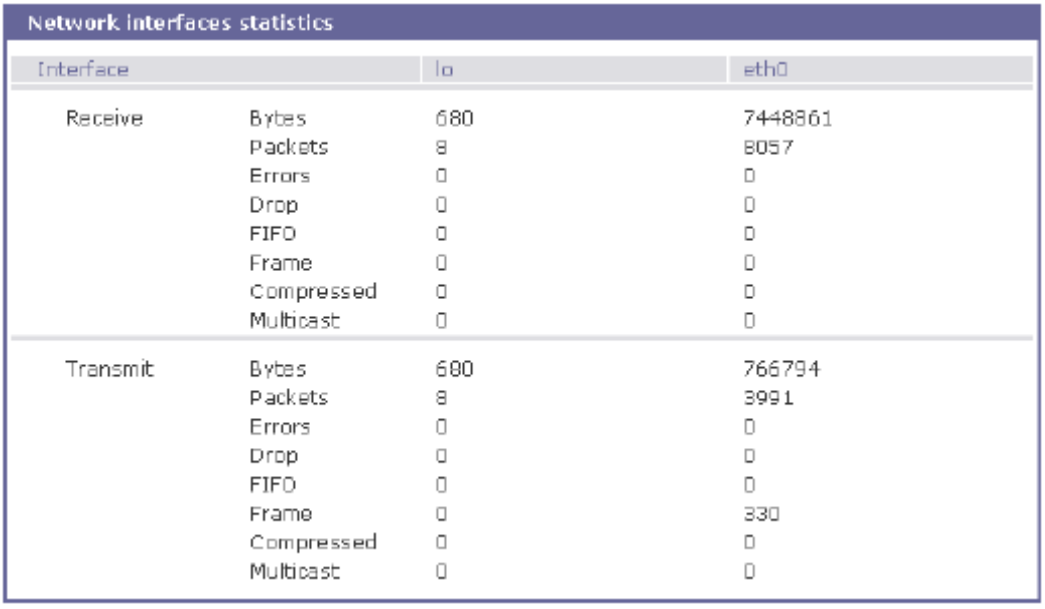
**図 6-13 User file upload menu 画面　アップロード完了のメッセージ**

# 7. システム統計 （System Statistics）

STS シリーズの WEB インターフェースにはシステム統計メニューがあります。これらのメニューで統計データにアクセスし、STS メモリに保管された統計データおよびテーブルにアクセス可能です。
ネットワークインターフェース統計およびシリアルポート統計は統計用のリンクレイヤー、lo, eth およびシリアルポートです。IP, ICMP, TCP, UDP の統計は TCP/IP プロトコルスイートの 4 主要コンポーネントです。

## 7.1. ネットワークインターフェース統計 （Network Interface Statistics）

ネットワークインターフェース統計は STS シリーズにより使用されている基本的なネットワークインターフェース、lo, eth0,を表示します。lo はローカルループバックであり、eth0 は STS シリーズの初期（デフォルト）のネットワークインターフェースです。



Network interfaces statistics

| Interface | | lo | eth0 |
|---|---|---|---|
| Receive | Bytes | 680 | 7448861 |
| | Packets | 8 | 8057 |
| | Errors | 0 | 0 |
| | Drop | 0 | 0 |
| | FIFO | 0 | 0 |
| | Frame | 0 | 0 |
| | Compressed | 0 | 0 |
| | Multicast | 0 | 0 |
| Transmit | Bytes | 680 | 766794 |
| | Packets | 8 | 3991 |
| | Errors | 0 | 0 |
| | Drop | 0 | 0 |
| | FIFO | 0 | 0 |
| | Frame | 0 | 330 |
| | Compressed | 0 | 0 |
| | Multicast | 0 | 0 |

図 7-1 ネットワークインターフェース統計画面

## 7.2. シリアルポート統計 （Serial Ports Statistics）

シリアルポート統計は 32 シリアルポートの使用履歴,通信速度設定、ピンステータスを表示します。
（緑●：ON 白○：OFF）

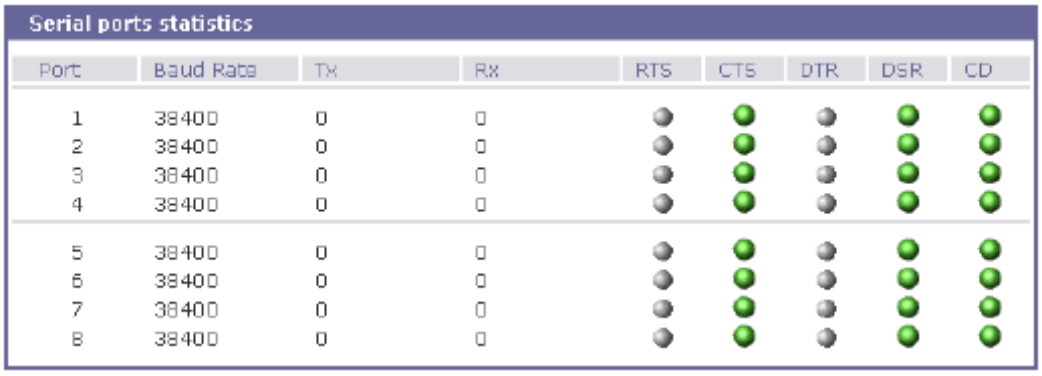



図 7-2 シリアルポート統計画面

## 7.3. IP 統計

IP 統計画面は IP プロトコルを使用しているパケット/接続の統計情報を表示します。各パラメータの定義および説明を以下に記します。

**Forwarding:**

IP forwarding が ON または OFF かを指定します。

**DefaultTTL:**

特定のコンピュータから発生したデータグラム用のデフォルト TTL(time to live)値を設定します。

**InReceives:**

受信したデータグラム数を表示します。

**InHdrErrors:**

ヘッダーエラーがある受信したデータグラムの数を表示します。ヘッダーエラーがある受信したデータグラムは IP ヘッダに bad checksume, バージョン番号の違い、他のフォーマットエラー, TTL 時間の超過、IP オプションのプロセスで発見したエラー、等があります。

**InAddrErrors:**

アドレスエラーがある受信したデータグラム数を表示します。これらのデータグラムは IP ヘッダの宛先フィールドにある IP アドレスがこのエンティティにて受信することができない有効ではないアドレスなので、破棄されます。これには無効なアドレス(例: 0.0.0.0.)およびサポートされていないクラス(例: Class E)が含まれます。

**ForwDatagrams:**

送信されたデータグラムの数を表示します。

**InUnknownProtos:**

受信成功したが、不明なまたはサポートされていないプロトコルゆえに破棄されたローカルアドレスのデータグラムの数を表示します。

**InDiscard:**

バッファースペースの欠如などの理由により、正常なデータグラムであるにも関わらず破棄されたデータグラムの数です。このデータグラムには再アッセンブリーで待機しているデータグラムは含まれません。

**InDelivers:**

受信したデータグラム数です。

**OutRequests:**

送信するために要求した送信データグラム数です。この数には転送されたデータグラムは含まれません。

**OutDiscards:**

破棄された送信したデータグラムの数です。これらは送信するのに何も問題はないが、バッファースペース不足などの理由により削除されたものです。この数字には Datagram Forwarded 内でカウントされた数も含まれる場合があります。

**OutNoRoutes:**

宛先 IP アドレスに送信するための経路が見つからないデータグラムの数です。これらのデータグラムは破棄されます。これは Datagram Forwarded 内でカウントされた数も含まれる場合があります。

**ReasmTimeout:**

すべてのフラグメントダイアグラムが活動可能な時間を表示します。この時間内にすべてのピースが活動しなければ、そのダイアグラムは破棄されます。

**ReasmReqds:**

再アセンブリーされる必要のあるデータグラムの数です。

**ReasmOKs:**

再アセンブリーが成功したデータグラム数です。

**ReasmFails:**

再アセンブリーされなかったデータグラム数です。

**FragOKs:**

フラグメント化に成功したデータグラム数です。

**FragFails:**

フラグメント化が必要だが、IP ヘッダがフラグメント化を許可しないためにフラグメント化ができないデータグラム数です。 たとえば、Don't Fragment フラグが設定されている場合、そのデータグラムはフラグメント化されず、データグラムは破棄されます。

**FragCreates:**

作成されたフラグメント数です。

IP statistics

| | |
|---|---|
| Forwarding | 2 |
| DefaultTTL | 64 |
| InReceives | 8208 |
| InHdrErrors | 0 |
| InAddrErrors | 0 |
| ForwDatagrams | 0 |
| InUnknownProtos | 0 |
| InDiscard | 0 |
| InDelivers | 4892 |
| OutRequests | 4973 |
| OutDiscards | 0 |
| OutNoRoutes | 0 |
| ReasmTimeout | 0 |
| ReasmReqds | 4954 |
| ReasmOKs | 1667 |
| ReasmFails | 0 |
| FragOKs | 21 |
| FragFails | 0 |
| FragCreates | 118 |

**図 7-3 ISTStatistics(統計)画面**

## 7.4. ICMP 統計

ICMP 統計画面は ICMP プロトコルを使用してパケットおよび接続を行う際の統計情報を提供します。各定義および説明は下記をご覧ください。

**InMsgs,OutMsgs:**

受信または送信したメッセージ数です。

**InErrors,OutErrors:**

受信または送信エラーの数です。

**InDestUnreachs,OutDestUnreachs:**

受信または送信時における"Destination-unreachable"メッセージの数です。"Destination-unreachable"メッセージは、送信しようとした宛先にデータグラムが届かなかった場合に、送り主のコンピュータに送信されるメッセージです。

**InTimeExcds,OutTimeExcds:**

受信または送信した TTL(存続時間)超過メッセージを指定します。 TTL 超過メッセージは、TTL 値を超過した数のルーターを通ったゆえにデータグラムが破棄された時に生成されるメッセージです。

**InParmProbs,OutParmProbs:**

受信または送信した Parameter-Problem Message(パラメータ異常メッセージ)の数です。Parameter-problem message はルーターまたはホストがデータグラムの IP ヘッダに異常を検知した時に、送信元のコンピュータに送るメッセージです。

**InSrcQuenchs,OutSrcQuenchs:**

受信または送信した Source quench (発信元)message の数です。Source quench Request (発信元リクエスト)は、パケット送信のレートを減らすリクエストをコンピュータに送信します。

**InRedirects,OutRedirects:**

受信または送信した echoe request(エコーリクエスト)数です。 Echoe Request は受信しているコンピュータが送り主のコンピュータに echo reply(エコー応答)を送るようリクエストします。

**NEchoReSTS,OutEchoReSTS:**

受信または送信した echo reply(エコー応答)の数です。 コンピュータは echoe request に対する返事として echoe reply を送信します。

**InTimestamSTS,OutTimestamSTS:**

受信または送信したタイム・スタンプ・リクエスト数です。 コンピュータは time stamp request に対する返事として time stamp reply を送信します。

**InAddrMasks,OutAddrMasks:**

受信または送信したアドレスマスク・リクエストの数です。コンピュータはアドレスマスク・リクエストを送信することにより、そのローカルサブネットのサブネットマスクのビット数を知ります。

**InAddrMaskReSTS,OutAddrMaskReSTS:**

受信または送信した Address mask response（アドレスマスク・応答）の数です。コンピュータは address mask request の応答メッセージとして address mask response を送信します。

ICMP statistics

| | |
|---|---|
| InMsgs | 4 |
| InErrors | 0 |
| InDestUnreachs | 4 |
| InTimeExcds | 0 |
| InParmProbs | 0 |
| InSrcQuenchs | 0 |
| InRedirects | 0 |
| InEchos | 0 |
| InEchoReps | 0 |
| InTimestamps | 0 |
| InTimestampReps | 0 |
| InAddrMasks | 0 |
| InAddrMaskReps | 0 |
| OutMsgs | 4 |
| OutErrors | 0 |
| OutDestUnreachs | 4 |
| OutTimeExcds | 0 |
| OutParmProbs | 0 |
| OutSrcQuenchs | 0 |
| OutRedirects | 0 |
| OutEchos | 0 |
| OutEchoReps | 0 |
| OutTimestamps | 0 |
| OutTimestampReps | 0 |
| OutAddrMasks | 0 |
| OutAddrMaskReps | 0 |

**図 7-4 ICMSTStatistics 画面**

## 7.5. TCP 統計

TCP 統計画面は TCP プロトコルを使用しているパケットまたは接続についての統計情報を表示します。各パラメータの定義および説明を下記に記します。

**RtoAlgorithm:**

使用中の再送信タイムアウト(RTO)アルゴリズムを指定します。RTO アルゴリズムは次の値です。

| | | | |
|---|---|---|---|
| 0: | CONSTANT | - | 継続タイムアウト |
| 1: | RSRE-MIL | - | STD-1778 AppendixB |
| 2: | VANJ | - | Van Jacobsen's Algorithm |
| 3: | OTHER | - | その他 |

RtoMin:

ミリ秒単位の最少再送信タイムアウト値を指定します。

RtoMax:

ミリ秒単位の最大再送信タイムアウト値を指定します。

MaxConn:

最大接続可能数を指定します。この値を-1 にすると、最大接続可能台数は動的になります。

ActiveOpens:

能動オープンの数です。能動オープンのときはクライアント側がサーバーとの接続を開始します。

Passive opens:

受動オープンの数です。受動オープンのときはサーバー側からの接続リクエストをリスニング(受信待機)します。

AttmptFails:

接続失敗した試行回数です。

EstabResets:

リセットしている確立した接続数です。

CurrEstab:

現在の確立した接続数です。

InSegs:

受信したセグメント数です。

OutSegs:

送信したセグメント数です。この中には再送信した数は含まれません。

RestransSegs:

再送信したセグメント数です。

InErrs:

受信したエラー数です。

OutRsts:

Reset flag set で送信したセグメントの数です。

TCP statistics

| | |
|---|---|
| RtoAlgorithm | 0 |
| RtoMin | 0 |
| RtoMax | 0 |
| MaxConn | 0 |
| ActiveOpens | 0 |
| PassiveOpens | 0 |
| AttemptFails | 0 |
| EstabResets | 0 |
| CurrEstab | 2 |
| InSegs | 1051 |
| OutSegs | 1486 |
| RetransSegs | 0 |
| InErrs | 0 |
| OutRsts | 5 |

**図 7-5 TCP 統計図**

## 7.6. UDP 統計

UDP 統計画面は UDP プロトコルを使用しているパケットまたは接続の統計情報を表示します。各パラメータの定義および詳細説明は下記の通りです。

**InDatagrams:**

受信したデータグラムの数です。

**NoPorts:**

指定したポートが有効でないために破棄された受信データグラムの数です。

**InErrors:**

受信した誤りデータグラムの数です。 Datagrams Received Errors は宛先ポートでのアプリケーション不足以外の理由で届けることのできなかtった受信した UDP データグラム数です。

**OutDatagrams:**

送信したデータグラムの数です。


**図 7-6 UDP 統計図**

# 8. CLI ガイド

## 8.1. はじめに

Root ユーザーはシリアルコンソールまたは TELNET/SSH 経由で STS シリーズの Linux コンソールコマンドライン・インターフェース(CLI)にアクセス可能です。 CLI では、標準の Linux コマンドにて STS シリーズのステータス、設定の編集、設定変更の適用などが可能です。

## 8.2. Flash パーティション

STS シリーズ内部フラッシュは下記のテーブルにあるようにパーティション化されています。ユーザーは /var ディレクトリでこのファイルに入ることが可能です。これらのファイルにアクセスするだけでは、リブート後に何らかの影響を及ぼすことはありませんが、saveconf コマンドを使用すると内部フラッシュメモリ内での変更が行われてしまいます。これはリブート後もそれらの変更が残る結果となります。不正な設定の変更は STS シリーズの動作に深刻な誤動作を招く危険性があります。

| Block | Type | Mount point | Size (KB) |
|---|---|---|---|
| Mtdblock0 | Bootloader | None | 128 |
| Mtdblock1 | Kernel | None | 768 |
| Mtdblock2 | CRAMFS (Read only) | / | 6080 |
| Mtdblock3 | Ram disk image (4MB) | /etc, /var, /tmp | 64 |
| Mtdblock4 | EXT2 (R/W) | /cnf (normally unmounted) | 64 |
| Mtdblock5 | JFFS2 (R/W) | /usr2 | 1024 |
| Mtdblock6 | Reserved | None | 64 |
| Total | | | 8192 |

## 8.3. サポートしている Linux ユーティリティ

### 8.3.1. Shell & shell utilities:

Sh, ash, bash, echo, env, false, grep, more, sed, which, pwd

### 8.3.2. File and disk utilities:

ls, cp, mv, rm, mkdir, rmdir, ln, mknod, cmod, touch, sync, gunzip, gzip, zcat, tar, df, du, vi, tail, mkdosfs, mke2fs, e2fsck, fsck, mount, umount, scp

### 8.3.3. System utilities:

date, free, hostname, sleep, sty, uname, reset, insmod, rmmod, lsmod, modprobe, kill, killall, ps, halt, shutdown, poweroff, reboot, telinit, init, useradd, userdel, usermod, whoami, who, passwd, id, su, who

### 8.3.4. Network utilities:

ifconfig, iptables, route, telnet, ftp, ssh, ping

## 8.4. CLI にアクセスする

**シリアルコンソール:**

1） PC シリアルポートと STS シリーズのコンソールポートをつなぐ
2） PC のターミナルソフトウェアを起動する
3） PC シリアルポートを 9600-8-N-1 No flow control に設定する
4） Enter を押す
5） STS シリーズに root ログインする

**Telnet コンソール:**

1） telnet STS Series_ip_address

## 8.5. CLI でSTSシリーズ設定の編集をする

### 8.5.1. ファイル保存/ロードメカニズムの設定

1） ブート時、STSシリーズは /cnf/cnf.tar.gz を/tmp/cnf/*に解凍し、/cnf にアンマウントします。
2） 設定を変更時、STS シリーズは/tmp/cnf 内ファイルを変更します。
3） 設定を保存する時、STSシリーズは/cnf をマウントし、/tmp/cnf/*を/cnf/cnf.tar.gz に圧縮します（Web[Save to flash]または CLI 内の”saveconf”）。

### 8.5.2. CLIで設定変更

CLI でSTSシリーズの設定変更を行うために、メニュー操作のユーティリティ（configmenu）を起動するか、下記の手順のように手動で行います。

1） Vi コマンドで手動いより設定ファイルを編集します。（付録C: STS シリーズ設定ファイルを参照してください。）
2） “saveconf”ユーティリティで設定ファイルを flash 内に保存します。
3） “applyconf”ユーティリティですべての変更を適用します。

```
root@192.168.0.117:~# configmenu

or

root@192.168.0.117:~# cd /tmp/cnf
root@192.168.0.117:/tmp/cnf# vi redirect.cnf
root@192.168.0.117:/tmp/cnf# saveconf
root@192.168.0.117:/tmp/cnf# applyconf
```

## 8.6. ユーザー定義スクリプトを起動する

STSシリーズのブート時、シェルスクリプト、/usr2/rc.user が自動的に呼び出されます。rc.user ファイルを変更し、ユーザー定義のスクリプトまたはバイナリを実行してください。

```
#!/bin/bash
#
# rc.user : Sample script file for running user programs at boot time
#
#PATH=/bin:/usr/bin:/sbin:/usr/sbin
# Add shell command to execute from here

echo 'This is the welcome message defined by users'exit 0
```

## 8.7. ファイル送信

ファイル送信用に ftp クライアントを使用し、データの read/write 用に/usr2 を使用します。

```
root@192.168.0.117:~# cd /usr2
root@192.168.0.117:/usr2# ftp 192.168.2.3
Connected to 192.168.2.3.
220 lxtoo.senalab.co.kr FTP server (Version wu-2.6.1-16) ready.
Name (192.168.2.3:root): sena
331 Password required for sena.
Password:
230 User sena logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> get test.tgz
local: test.tgz remote: test.tgz
200 PORT command successful.
150 Opening BINARY mode data connection for test.tgz (350 bytes).
226 Transfer complete.
350 bytes received in 0.04 secs (9.6 kB/s)
ftp> bye
```

通常の FTP クライアントに加えて、acp クライアントプログラムを使用して暗号化することにより、セキュアにファイルをコピーすることができます。STS シリーズ（192.168.0.120）からお使いのPCにファイルをコピーする場合、PCに次のコマンドを入力してください。

```
[root@localhost work]# scp root@192.168.0.120:/usr2/rc.user /work
The authenticity of host '192.168.0.120 (192.168.0.120)' can't be established.
RSA key fingerprint is c1:70:ab:52:48:ab:e5:dc:47:9c:94:ed:99:6f:94:4f.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.0.120' (RSA) to the list of known hosts.
root@192.168.0.120's password:
rc.user           100% |*****************************|   173      00:00
[root@localhost work]#
```

## 8.8. サンプル例

### 8.8.1. ユニットの Telnet Port をオフにする。

STS シリーズはそれぞれのリモートコンソールポートを個別にオフにする機能を持っていません。（SSH 用の port 22 または Telnet 用の port23）

現在のところ、リモートコンソールをすべてオン/オフにすることしかできません。これはユーザーインターフェースまたはコンソール設定メニューから行います。

ただ一つだけのリモートコンソールをオフにするには、’rc.user’ スクリプトを編集することにより可能となります。どのように行うかは下記の例を参照してください。

例 1. ‘inetd.conf’ を変更する

Step 1　/etc/inetd.conf を変更 （telnet サービスを削除）

Step 2 inetd.conf を/usr2/inetd.conf にコピー

Step 3 usr2/rc.user スクリプトを次の通りに変更

```
#!/bin/bash
#
# rc.user : Sample script file for running user programs at boot time
#

#PATH=/bin:/usr/bin:/sbin:/usr/sbin

# Add shell command to execute from here
# Add shell command to execute from here

cp -a /usr2/inetd.conf /etc/inetd.conf
ps -ef
while killall inetd 2>/dev/null;
do sleep 1;
ps -ef
done
/usr/sbin/inetd
ps -ef

exit 0
```

これでシステムのブートアップ時毎に telnet サービスをオフにすることが可能になりました。

**Iptables ルールを実行**

Step 1 次のように usr2/rc.user スクリプトを変更する。

```
#!/bin/bash
#
# rc.user : Sample script file for running user programs at boot time
#

#!/bin/bash
#
# rc.user : Sample script file for running user programs at boot time
#

#PATH=/bin:/usr/bin:/sbin:/usr/sbin

# Add shell command to execute from here

# if user wants to disable telnet service from all host
iptables -A INPUT -p tcp -s --dport 23 -j DROP

# if user wants to enable telnet service only from specific hosts(192.168.0.0 ~
192.168.0.255)
#iptables -A INPUT -p tcp -s ! 192.168.0.1/255.255.255.0 --dport 23 -j DROP

exit 0
```

これでシステムブート時毎に telnet サービスをオフにすることが可能です。

ＳＴＳシリーズをファクトリデフォルトにリセットすると、/usr2/rc.user スクリプトファイルは

/usr2/rc.user.old#ファイルとリネームされ、デフォルトの rc.user ファイルが復元されます。

### 8.8.2. 定期プログラムの実行

Crontab コマンドで特定のプログラムを定期的に実行することができます。Crontab で定期プログラムを実行するには、次のステップを参照してください。

Step 1 /usr2 ディレクトリに crontab ファイルを作成します。次のサンプル crontab ファイルは、current_date ファイルを/tmp ディレクトリ以下に作成し、内容を 2 分ごとに更新します。

```
SHELL=/bin/bash
# Sample crontab job
# Run every two minutes
* * * * * echo `date` > /tmp/current_date
```

Step 2 次のコマンドで crontab ファイルを登録します。

```
root@SS800_Device:/usr2# crontab samplecrontab_file
```

Step 3 この定期動作ジョブを毎ブート時に行うには、uc.user スクリプトを下記の通りに使用してください。

```
#!/bin/bash
#
# rc.user : Sample script file for running user programs at boot time
#

#PATH=/bin:/usr/bin:/sbin:/usr/sbin

# Add shell command to execute from here
crontab /usr/samplecrontab file

exit 0
```

-e オプション（editor を使用した現行 crontab の変更）をSTSはサポートしていません。Vi editor を使って crontab ファイル内のコンテンツを変更してください。

# 9. ユーザーカスタマイズガイド

## 9.1. はじめに

STS シリーズには様々なカスタマイズ方法があり、ユーザーの使い勝手に合わせた機器にカスタマイズできます。STS シリーズは次のカスタマイズ方法を提供しています。

- 定期プログラムの実行
- ユーザー定義のウェブページ
- ユーザー独自のコードを作成および実行

## 9.2. 定期プログラムの実行

Crontab で特定のプログラムを定期的に実行することができます。Crontabを使った定期作業をオンにするには、次のステップに従ってください。

Step 1. /usr2 ディレクトリに crontab ファイルを作成します。 次の crontab ファイルは、/tmp ディレクトリ以下に current_date ファイルを生成し、2 分ごとに内容の更新を行うサンプル例です。

```
SHELL=/bin/bash
# Sample crontab job
# Run every two minutes
* * * * * echo `date` > /tmp/current_date
```

Step 2. 次のコマンドで crontab を登録します。

```
root@SS800_Device:/usr2# crontab samplecrontab_file
```

Step 3 この定期動作ジョブを毎ブート時に行うには、uc.user スクリプトを次のように使用してください。

```
#!/bin/bash
#
# rc.user : Sample script file for running user programs at boot time
#

#PATH=/bin:/usr/bin:/sbin:/usr/sbin

# Add shell command to execute from here
crontab /usr/samplecrontab file

exit 0
```

–e オプション（editor を使用した現行 crontab の変更）をSTSはサポートしていません。Vi editor を使って crontab ファイル内のコンテンツを変更してください。

## 9.3. ユーザー定義のウェブページ

STS シリーズはユーザー定義のウェブページをサポートしています。Web UI にユーザーログイン後に現れる最初の画面をユーザー定義のものにすることができます。詳細情報に関しては *3.9 Web サーバー設定画面* を参照してください。

デフォルトのウェブページが Customer page に変更されると、毎回ログインごとにそのページが表示されます。内容の変更は index.html またはデフォルトの CGI プログラムに変更を加えます。これらニつのファイルは/usr2 ディレクトリにあります。

Index.html のコンテンツを変更するには、そのまま内容の変更をすることが可能ですが、CGI プログラムの内容を変更するには、オリジナルのソースコードを変更後CGIプログラムのソースコードをコンパイルする必要があります。CGIプログラムのソースコードをコンパイルするには、STS シリーズ用にクロス開発環境 cross development environment またはSDK（Software Development Kit）が必要です。詳細情報に関しては弊社技術サポートまでお問い合わせください（info@intersolutionmarketing.com）。

## 9.4. ユーザー独自のコードを作成および実行

ユーザー独自のアプリケーションコードを作成するにはSTS用のクロス開発環境 Cross development environment またはSDK（Software Development Kit）が必要です。詳細は弊社サポートまでお問い合わせください（info@intersolutionmarketing.com）。

STS シリーズの SDK で、STSシリーズ内のCLIに独自のプログラムを作成することが可能となります。その環境内で、Linux 搭載のPCでプログラミングを行い、CFカードにより、プログラムをSTSに転送します。STSシリーズでこのプログラムを実行するには、ユーザースクリプトファイルまたは crontab プログラムを使用します。シリアルデータの操作を目的としたプログラムであれば、フィルターアプリケーションメニューを使用できます。詳細情報に関しては、*4.2.8 フィルターアプリケーション*を参照してください。

# 付録 1 . 接続

## A 1.1. Ethernet ピン配置

STS シリーズは標準 Ethernet コネクタを使用しています。 AT&T258 に準拠しています。表 A-1 にピン配置およびワイヤ色を記します。

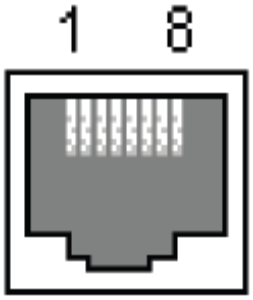



**表 A-1 RJ45 コネクタのピン配置**

| Pin | Description | Color |
|---|---|---|
| 1 | Tx+ | White with orange |
| 2 | Tx- | Orange |
| 3 | Rx+ | White with green |
| 4 | NC | Blue |
| 5 | NC | White with blue |
| 6 | Rx- | Green |
| 7 | NC | White with brown |
| 8 | NC | Brown |

## A 1.2. コンソールおよびシリアルポートピン配置

STS シリーズの DB9 コネクタのピン配置を表 A-2 に記します。各ピンにはシリアル通信方式設定に基づいた機能があります。

| Pin | RS232 (console and serial ports) |
|---|---|
| 1 | CTS |
| 2 | DSR |
| 3 | RxD |
| 4 | GND |
| 5 | DCD |
| 6 | TxD |
| 7 | DTR |
| 8 | RTS |

## A 1.3. Ethernet 配線ダイアグラム

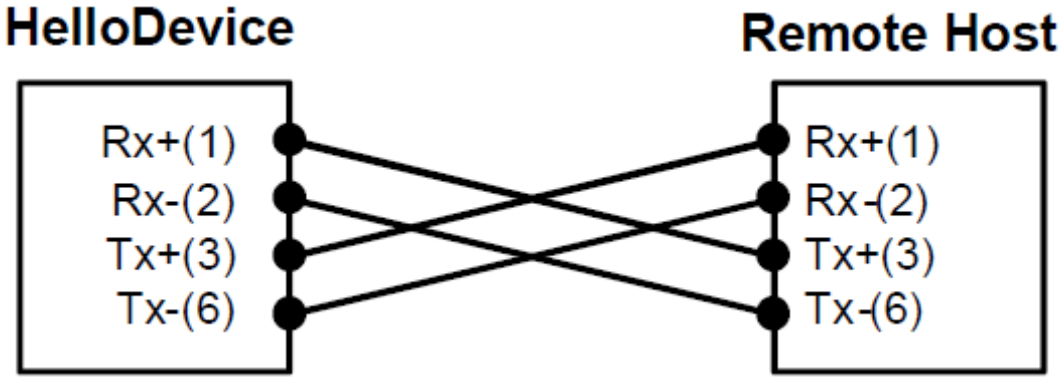



図 A-3 クロス・イーサネットケーブル接続

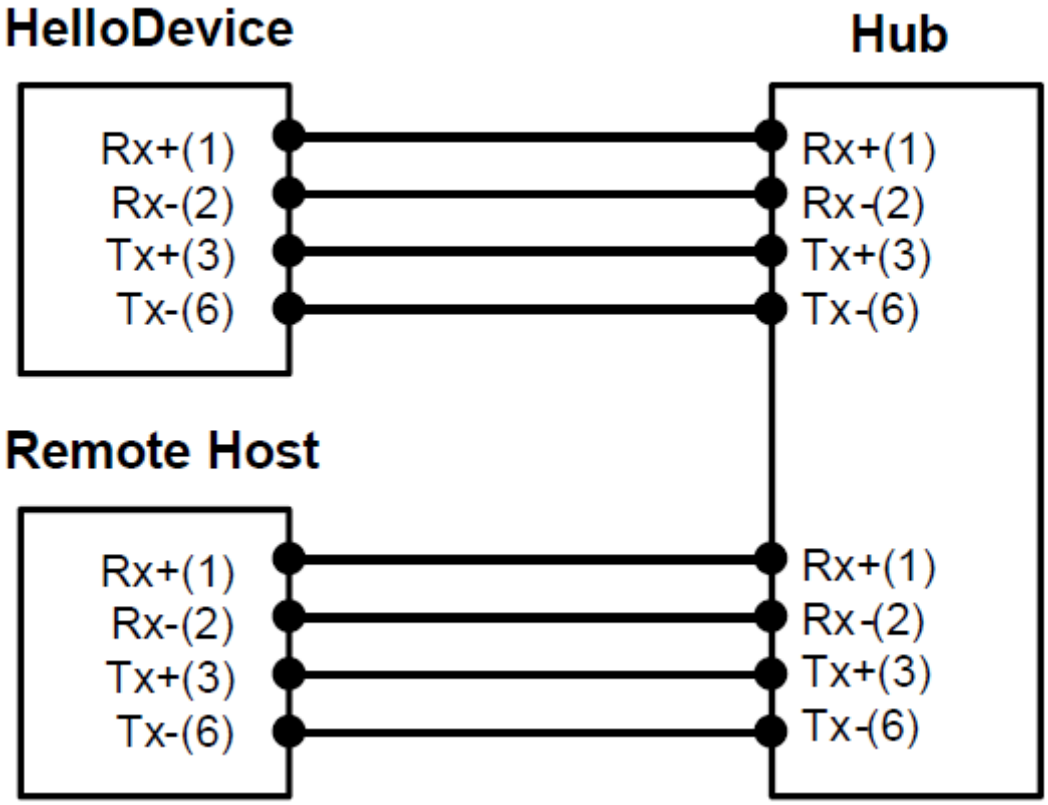



図 A-3 ストレート・イーサネットケーブルでつないだ場合

## A 1.4. RS232 シリアル配線ダイアグラム

## RJ45-DB9 female adapter

*Using RJ45 to DB9(Female)* ***Cross-over*** *Cable*

| Description (RJ45) | Internal Cable Color | RJ45 Pin No. | DB9 Pin No. | Description (DB9) |
|---|---|---|---|---|
| CTS | Blue | 1 | 7 | RTS |
| DSR | Orange | 2 | 4 | DTR |
| RXD | Black | 3 | 3 | TXD |
| GND | Red | 4 | 5 | GND |
| DCD | Green | 5 | 1 | DCD |
| TXD | Yellow | 6 | 2 | RXD |
| DTR | Brown | 7 | 6 | DSR |
| RTS | White | 8 | 8 | CTS |

## RJ45-DB25 female adapter

*Using RJ45 to DB25(Female)* ***Cross-over*** *Cable*

| Description (RJ45) | Internal Cable Color | RJ45 Pin No. | DB25 Pin No. | Description (DB25) |
|---|---|---|---|---|
| CTS | Blue | 1 | 4 | RTS |
| DSR | Orange | 2 | 20 | DTR |
| RXD | Black | 3 | 2 | TXD |
| GND | Red | 4 | 7 | GND |
| DCD | Green | 5 | 8 | DCD |
| TXD | Yellow | 6 | 3 | RXD |
| DTR | Brown | 7 | 6 | DSR |
| RTS | White | 8 | 5 | CTS |

## RJ45-DB25 male adapter

*Using RJ45 to DB25(Male)* ***Cross-over*** *Cable*

| Description (RJ45) | Internal Cable Color | RJ45 Pin No. | DB25 Pin No. | Description (DB25) |
|---|---|---|---|---|
| CTS | Blue | 1 | 4 | RTS |
| DSR | Orange | 2 | 20 | DTR |
| RXD | Black | 3 | 2 | TXD |
| GND | Red | 4 | 7 | GND |
| DCD | Green | 5 | 8 | DCD |
| TXD | Yellow | 6 | 3 | RXD |
| DTR | Brown | 7 | 6 | DSR |
| RTS | White | 8 | 5 | CTS |

## RJ45-DB25 male adapter

*Using RJ45 to DB25(Male)* ***Straight*** *Cable*

| Description (RJ45) | Internal Cable Color | RJ45 Pin No. | DB25 Pin No. | Description (DB25) |
|---|---|---|---|---|
| CTS | Blue | 1 | 5 | CTS |
| DSR | Orange | 2 | 6 | DSR |
| RXD | Black | 3 | 3 | RXD |
| GND | Red | 4 | 7 | GND |
| DCD | Green | 5 | 8 | DCD |
| TXD | Yellow | 6 | 2 | TXD |
| DTR | Brown | 7 | 20 | DTR |
| RTS | White | 8 | 4 | RTS |

# 付録2. STS シリーズによりサポートされているPCカード一覧

## A 2.1. ネットワークカード

| Manufacturer | Model/Name | STS probed Model name | Specification |
|---|---|---|---|
| 3COM | 3CXE589ET-AP | 3Com Megahertz 589E TP/BNC LAN PC Card | 10 Mbps LAN card |
| Linksys | Linksys EtherFast 10/100 Integrated PC Card (PCM100) | Linksys EtherFast 10/100 Integrated PC Card (PCM100) Ver 1.0 | 10/100 Mbps LAN card |
| Corega | FetherII PCC-TXD | corega K.K. corega FEtherII PCC-TXD | 10/100 Mbps LAN card |
| Netgear | 16bit PCMCIA Notebook Adapter FA411 | NETGEAR FA411 Fast Ethernet | 10/100 Mbps LAN card |

## A 2.2. 無線LANネットワークカード

| Manufacturer | Model/Name | STS probed Model name | Specification |
|---|---|---|---|
| Cisco Systems | AIR-PCM340/Aironet 340 | Cisco Systems 340 Series Wireless LAN Adapter | 11 Mbps Wireless LAN Adapter |
| Lucent Technologies | PC24E-H-FC/Orinoco Silver | Lucent Technologies WaveLAN/IEEE Version 01.01 | 11 Mbps Wireless LAN Adapter |
| Lucent Technologies | PC24E-H-FC/Orinoco Gold | Lucent Technologies WaveLAN/IEEE Version 01.01 | 11 Mbps Wireless LAN Adapter |
| Agere Systems (Lucent Technologies) | Orinoco Classic Gold (PC24E-H-FC/Orinoco Gold) | Lucent Technologies WaveLAN/IEEE Version 01.01 | 11 Mbps Wireless LAN Adapter |
| Buffalo | AirStation (WLI-PCM-L11GP) | MELCO WLI-PCM-L11 Version 01.01 | 11 Mbps Wireless LAN Adapter |

## A 2.3. ATA/IDE フィックスディスクカード

| Manufacturer | Model/Name | STS probed Model name | Specification |
|---|---|---|---|
| Advantech | CompactFlash | CF 48M | 48 MB Storage card |
| SanDisk | SDP series | SunDisk SDP 5/3 0.6 | 64 MB Storage card |
| SanDisk | SDP series | SanDisk SDP 5/3 0.6 | 256 MB Storage card |
| Kingston | CompactFlash Storage Card | TOSHIBA THNCF064MAA | 64 MB Storage card |
| Viking | CompactFlash | TOSHIBA THNCF064MBA | 64 MB Storage card |
| | | | |

## A 2.4. シリアルモデムカード

| Manufacturer | Model/Name | STS probed Model name | Specification |
|---|---|---|---|
| Billionton Systems Inc. | FM56C series | PCMCIA CARD 56KFaxModem FM56C-NFS 5.41 | Ambient (Intel) V.90 FAX/MODEM PC Card |
| Viking | PC Card Modem 56K | Viking V.90 K56flex 021 A | MODEM PC Card |
| KINGMAX | KIT PCMCIA 56K Fax/Modem Card | CIRRUS LOGIC 56K MODEM CL-MD56XX 5.41 | V.90 FAX/MODEM PC Card |
| TDK | TDK DH6400 | TDK DH6400 1.0 | 64Kbps |
| NTT DoCoMo | Mobile Card Triplex N | NTT DoCoMo Mobile Card Triplex N | 64Kbps |

# 付録3.　　STS設定ファイル

## A 3.1. System.cnf

```
#
# system.cnf
#
#   system configuration which exist only one place on this file.
#

# kind of IP configuration mode
# 1 - static ip , 2 - dhcp , 3 - pppoe
ipmode = 1

# system ip addres
ipaddr = 192.168.161.5

# system subnet mask
subnet = 255.255.0.0

# system gateway
gateway = 192.168.1.1

# dns configuration
# 'p dns' is a primary dns ip address and 's dns' is a secondary dns ip address
# if you want to set dns authmatically in case of dhcp or pppoe,
# you can set 'bmanual dns' to 0.
p dns = 168.126.63.1
s dns = 168.126.63.2

# pppoe configuration
# 'ppp_usr' is pppoe account name and 'ppp_pwd" is a password for that account
ppp usr = whoever
ppp pwd = pppoepwd

# Email logging configuration
# if you want to send log via E-mail, set 'emaillog' to 1
# 'emaillog num' trigger sending email.
# The number of logs are greater than 'emaillog num", then send it.
emaillog = 0
emaillog num = 5

# SMTP configuration
# 'smtpsvr' is a SMTP server .
# 'sysmailaddr' is a sender address.
# 'recvmailaddr' is a receiver address.
# 'smtp mode' means a SMTP server authentication mode.
#  1 - smtp w/o authentication , 2 - pop before smtp , 3 - smtp w/
authentication
# If 'smtp mode" is 2 or 3, you need SMTP account information.
# 'smtp user' is a SMTP account name and 'smtp pwd" is a password.
bsmtp = 0
smtpsvr = smtp.yourcompany.com
sysmailaddr = SS800@yourcompany.com
recvmailaddr = admin@yourcompany.com
smtp mode = 1
smtp_user = admin
smtp pwd = admin

# 'device name' mean a unit name assigned. A unit name will be a identifier
among PS products.
device_name = SS800 Device

# IP filtering configuration
```

```
# By setting 'btelnet' to 1, you can use remote console.
# Similarly by setting 'bweb' to 1, you can use remote console.
# 0 means that protect any access.
# 'enable ip', 'enable netmask' pair is a source rule specification for remote
console filtering.
# 'enable webip', 'enable webnetmask' pair is for web filtering.
btelnet = 1
bweb = 1
enable ip = 0.0.0.0
enable netmask = 0.0.0.0
enable webip = 0.0.0.0
enable webnetmask = 0.0.0.0

# dynamic DNS(DDNS) configuration
# dynamic dns can be enabled by setting 'bdyndns' to 1. 0 for disable.
# 'dyn dn' is a domain name for your DDNS.
# 'dyn user' is a account name for DDNS and 'dyn pwd" is a password for it.
bdyndns = 0
dyn dn = ss800.dyndns.biz
dyn user = ss800-user
dyn pwd = ss800-pwd

# NTP configuration
# 'ntp enable' set to 1 for using NTP or set to 0.
# 'ntp serverip' is the IP address of NTP server and 'ntp offset' is a your
offset from UTC.
# If you don't know any NTP server IP, then set 'ntp auto conf' to 1.
ntp_enable = 0
ntp auto conf = 1
ntp offset = 0.0
ntp serverip = 192.168.200.100

# Log configuration
# system logging is enabled by 'log enable' to 1.
# 'logbuf size' is a variable for representing log buffer size by KB.
# 'log stoloc' is a location to save log.
#  1 = memory 2 = CF card 3 = NFS 4 = SYSLOGD
# If you choose log location to SYSLOGD, 'logbuf_size' you've set will loose his
role - limiting log file size.
log enable = 1
logbuf size = 4
log stoloc = 1

# syslog configuration
# You can run or kill syslogd by setting 'bsyslog service' to 1 or 0.
# 'syslog ip' is a IP addresss of a remote syslog server.
# 'syslog 2ndip' is a IP address of a secondary syslogd server which will get
the same logs.
# 'syslog_facility' specify what type of program is logging. 0 ~ 7 for LOCAL0 to
LOCAL7
bsyslog service = 0
syslog ip = 192.168.200.100
syslog_facility = 0

# NFS configuration
# You can mount or unmount NFS by setting 'bnfs service'  to 1 or 0.
# 'nfs ip' is a NFS server IP addresss and 'nfs path' is a mount path.
bnfs_service = 0
nfs_ip = 192.168.200.100
nfs path = /

# WEB configuration
# If you want to support HTTP, then set 'bweb_http' to 1. If not, set tot 0.
# 'bweb https' is for HTTPS.
# 'web refresh rate' is for refresh the changing page when you see the system
status page.
bweb_http = 1
```

```
bweb https = 1
web refresh rate = 10

# TCP configuration
# 'keepalive time' is a time before keep alive takes place.
# 'keepalive probes' is the number of allowed keep alive probes.
# 'keepalive intvl' is a time interval between keep alive probes.
keepalive time = 15
keepalive probes = 3
keepalive intvl = 5

# Ethernet configuration
# 'ethernet mode' is a ethernet mode.
# 0 = Auto Negotiation,  1 = 100BaseT Half Duplex, 2 = 100BaseT Full Duplex,
# 3 = 10BaseT Half Duplex, 4 = 10BaseT Full Duplex
ethernet mode = 0

# PCMCIA configuration
# 'pcmcia card type' shows a pcmcia card type.
# 0 for empty , -1 for unsupported card, 1 for CF card, 2 for Network card,
# 3 for Wireless Network card, 4 for Serial Modem card
pcmcia card type = 0

# PCMCIA ipconfiguration
# same with system ip configuration
pcmcia ipmode = 2
pcmcia ip = 192.168.1.254
pcmcia_subnet = 255.255.255.0
pcmcia gateway = 192.168.1.1
pcmcia ppp usr = whoever
pcmcia ppp pwd = pppoepwd
pcmcia bmanual dns = 0

# In case of serial modem card, 'pcmcia modem initstr' means a modem init string.
pcmcia modem initstr = q1e0s0=2

# Wireless network card configuration
# To enable or disable Wired Equivalent Privacy(WEP), set 'pcmcia_wep_enb' to 1
or 0.
# 'pcmcia web mode' is a WEP mdoe. 1 for encrypted, 2 for shared
# 'pcmcia wep length' is a length for WEP. 1 for 40 bits, 2 for 128 bits
# 'pcmcia wep key str' is a key string for WEP.
pcmcia wep enb = 0
pcmcia wep mode = 1
pcmcia wep length = 1

# 'pcmcia cf conf max' is a maximum size to use in case of CF card.
pcmcia_cf_conf_max = 0
```

## A 3.2. Redirect.cnf

```
#
# redirect.cnf
#
#   Port configuration is placed on this file.
#   Basically keys followed by 'port' key are data for those port.
#   Port number is zero base index and the maximum value for port is used as all
port configuration
#   Data followed by all port are default values and will NOT be applied.

# 'port' key notify the port data follow.
# If you want to activate the port, set 'benable' to 1. If not, set to 0.
# If you set 'bmanset' to 1, you don't want to change the port data by changing
```

```
all port configuration.
# If you want to change the port data by changing all port configuration, set to
0.
port = 0
benable = 0
bmanset = 0
port = 1
benable = 0
bmanset = 0
port = 2
benable = 0
bmanset = 0
port = 3
benable = 0
bmanset = 0
port = 4
benable = 0
bmanset = 0
port = 5
benable = 0
bmanset = 0
benable = 0
port = 6
bmanset = 0
benable = 0
port = 7
bmanset = 0
benable = 0

# As refered, maximum port (in case 8 port machine ,8) represents the
# defaults values for all port configuration.
port = 8
benable = 0
bmanset = 0

# Serial parameter configuration
# 'uarttype' is for UART type. But PS only support RS232.
# So set 'uarttype' to 0 and DO NOT CHANGE.
# 'baudrate' is for baudrate. From 1200 to 230400 is available.
# 'stopbits' is for stop bits. 1 for 1 bit, 2 for 2 bits
# 'databits' is for data bits. 7 for 7 bits, 8 for 8 bits.
# 'parity' is for parity. 0 for none, 1 for even , 2 for odd parity.
# 'flowcontrol" is for flow control. 0 for none, 1 for XON/XOFF,
#                                    2 for hardware flow control
# 'dtropt' is for DTR pin option.
#  1 = Always HIGH, 2 = Always LOW, 3 = High when open
# 'dsropt' is for DSR pin option.
#  0 = None, 1 = Allow TCP connection only by HIGH 2 = open/close TCP connection
# 'interchartimeout' is for inter-character timeout. It works ONLY FOR RAWTCP
# mode.
uarttype = 0
baudrate = 9600
stopbits = 1
databits = 8
parity = 0
flowcontrol = 0
dtropt = 0
dsropt = 0
interchartimeout = 100

# Host mode configuration
# 'hostmode' means a host mode.
#  0 = TCP mode, 1 = UDP mode, 2 = Mode emulation
hostmode = 0
# In TCP mode, 'localport' is a listening port.
localport = 0
# 'max connection' is a maximum allowed number of remote host
```

```
# 'snmp trap receiver community' is community of SNMP Trap
# 'snmp trap receiver version' is SNMP trap version
# 0 = v1, 1 = v2c
event enable = 1
notification interval = 0
bmail handle = 1
mail title = jungoj@sena.com
mail address = junq@sss.com
bsnmp handle = 1
snmp title = khfgj
snmp trap receiver ip = 192.168.0.8
snmp trap receiver community = public
snmp trap receiver version = 0

# Event Keyword option
# 'keyword index' is a index of keyword event
# 'keyword str' is a event keyword
# 'snmp enable' is a SNMP notification option for keyword
# 0 = Disable, 1 = Enable
# 'mail enable' is a email notification option for keyword
# 0 = Disable, 1 = Enable
# 'command enable' is a port command option for keyword
# 0 = Disable, 1 = Enable
# 'port command' is a port command string for keyword
keyword index = 0
keyword str = test
snmp enable = 1
mail_enable = 1
command enable = 1
port command = fghfgh

# Port buffering configuration
# Enable of disable port buffering by setting 'pb enable' to 1 or 0.
# 'pb size' is a maximum port buffering size. Maximum value are different by
location.
# 'pb loc' is a location to store port buffer data.
#  1 = memory 2 = CF card 3 = NFS 4 = SYSLOGD
pb_enable = 0
pb size = 4
pb loc = 1
```

```
max connection = 32
# 'remotehost' is a remote host list
#                    (Primary IP address:port Secondary IP address:port)
remotehost = 192.168.0.135:7000 192.168.0.135:7001
# 'cyclictime ' is a cyclic connection time in seconds
cyclictime = 10
# 'inactivitytimeout' is a inactivity timeout in seconds.
inactivitytimeout = 100

# Cryptography Options
# 'encryptionmode' is encryption mode
# 0 = None, 1 = SSLv2, 2 = SSLv3, 3 = SSLV3 rollback v2, 4 = TLSv1
# 'encryptionkey' is encryption key file name
# 'key password' is password for encryption key file
# 'cipher suite' represents a combination of cipher suite.
# 'verify client' is Verify client(server mode only) option
#  0 = No, 1 = Yes
# 'verify chain depth' is a number of chain depth to be searched
# 'verify cn' is Compare the certificate CN and hostname option
#  0 = No, 1 = Yes
encryptionmode = 2
encryptionkey =
key password = testing
cipher suite = 524287
verify client = 1
verify chain depth = 3
verify cn = 1


# In UDP mode,
# 'accept unlisted' is Accept UDP datagram from unlisted remote host option
# 0 = No, 1 = Yes
# 'send to unlisted' Send to recent unlisted remote host option
# 0 = No, 1 = Yes
accept unlisted = 1
send to unlisted = 1

# IP filtering configuration
# 'allow ip', 'allow netmask' pair is a source rule specification for serial
port access filtering.
allow ip = 0.0.0.0
allow netmask = 0.0.0.0

# 'porttitle' is a port title.
porttitle = Port Title

# Mode configuration option
# 'modem_mode' is modem mode option
# 0 =Disable, 1 =Enable
# 'modem initstr' is a modem initialization string
# 'modem dcd option' is modem DCD pin option
# 0 = None, 1 = Allow TCP connection only by HIGH
modem_mode = 0
modem initstr =
modem dcd option = 0

# Event notification configuration
# Enable of disable Event notification by setting 'event_enable' to 1 or 0.
# 'notification_interval' is interval of event notification.
# 'bmail handle' is a Enable/Disable E-mail notification option
# 0 = Disable, 1 = Enable
# 'mail title' is a title of email notification.
# 'mail_address' is a mail recipient's address
# 'bsnmp handle' is a Enable/Disable SNMP notification option
# 0 = Disable, 1 = Enable
# 'snmp title' is a title of SNMP trap notification.
# 'snmp trap receiver ip' is a IP address of SNMP Trap receiver
```

# 付録4.　　ウェルノウン・ポート番号

ポート番号は3つのレンジに分けることができます。ウェルノウン・ポート・登録済みポート、動的/プライベートポートです。ウェルノウン・ポートは0から1023番の間です。登録済みポートは1024から49151番です。動的/プライベート・アドレスには49152から65535番が割り当てられています。
ウェルノウン・ポートはIANAにより割り当てられ、システムプロセス、または特別なユーザーによって実行されるプログラムによって使用されます。表A-3はウェルノウン・ポートの一覧です。
ウェルノウン・ポートの詳細情報は下記URLを参照:
http://www.iana.org/assignments/port-numbers

**表A-3　ウェルノウン・ポート番号**

| Port number | Protocol | TCP/UDP |
|---|---|---|
| 21 | FTP (File Transfer Protocol) | TCP |
| 22 | SSH (Secure Shell) | TCP |
| 23 | Telnet | TCP |
| 25 | SMTP (Simple Mail Transfer Protocol) | TCP |
| 37 | Time | TCP, UDP |
| 39 | RLP (Resource Location Protocol) | UDP |
| 49 | TACACS, TACACS+ | UDP |
| 53 | DNS | UDP |
| 67 | BOOTP server | UDP |
| 68 | BOOTP client | UDP |
| 69 | TFTP | UDP |
| 70 | Gopher | TCP |
| 79 | Finger | TCP |
| 80 | HTTP | TCP |
| 110 | POP3 | TCP |
| 119 | NNTP (Network News Transfer Protocol) | TCP |
| 161/162 | SNMP | UDP |
| 443 | HTTPS | TCP |

# 付録5.　Bootloader menu プログラムガイド

## A 5.1.　概要

Bootloader メニューは災害時回復オプションとして TFTP を使用して STS シリーズをリカバリーし、システムハードウェアを診断する方法です。STS シリーズの電源を立ち上げてから 3 秒以内に ESC キーを押すと、ユーザーは Bootloader メニュープログラムに入ります。このメニュープログラムから、さまざまなシステムパラメータを設定、システムハードウェアをテスト、またファームウェア・アップグレードを実行することが可能です。

## A 5.2.　メインメニュー

Bootloader メニュープログラムに入ったら、次のメインメニューページが表示されます。

```
Bootloader 1.1.0 (May 23 2003 - 22:48:25)

CPU     :  XPC855xxZPnnD4 (50 MHz)
DRAM    :  64 MB
FLASH   :   8 MB
PC CARD  :  No card
EEPROM   :  A Type exist
Ethernet :  AUTO-NEGOTIATION
Autoboot Start:  0
-------------------------------------------------------------------------------
 Welcome to Boot Loader Configuration page
-------------------------------------------------------------------------------
 Select menu
 1. RTC configuration [ Feb 14 2003 - 11:00:26 ]
 2. Hardware test
 3. Firmware upgrade [S/W Version : v1.0.0]
 4. Exit and boot from flash
 5. Exit and reboot
  <ESC> Back, <ENTER> Refresh
 ----->
```

**図 A-4　Bootloader Menu のメイン画面**

## A 5.3.　RTC 設定メニュー

RTC Configuration メニューを使用して、STS シリーズのシステムタイムを設定することができます。

```
-------------------------------------------------------------------------------
RTC Configuration
-------------------------------------------------------------------------------
 Select Menu
 1. Data(mm/dd/yy) : 05/19/05
 2. Time(hh:mm:ss) : 15:02:28
```

```
 <ESC> Back, <ENTER> Refresh
 ----->1
 Enter Current Data(mm/dd/yy) : 05/20/05
 Press the ENTER key to continue!!
--------------------------------------------------------------------------------
RTC Configuration
--------------------------------------------------------------------------------
 Select Menu
 1. Data(mm/dd/yy) : 05/20/05
 2. Time(hh:mm:ss) : 15:02:41
 <ESC> Back, <ENTER> Refresh
 ----->2
 Enter Current Data(hh:mm:ss) : 15:03:40
 Press the ENTER key to continue!!
--------------------------------------------------------------------------------
RTC Configuration
--------------------------------------------------------------------------------
 Select Menu
 1. Data(mm/dd/yy) : 05/20/05
 2. Time(hh:mm:ss) : 15:03:41
 <ESC> Back, <ENTER> Refresh
 ----->
```

**図 A-10 Bootloader Menu プログラムの RTC 設定画面**

## A 5.4. ハードウェアテストメニュー

Hardware test メニューで、ハードウェアコンポーネントのテストを行えます。3 種類のテストモードがあります。

- One time
- Looping (without External test in Auto test)
- Looping(with External test in Auto test)

One time を選択すると、Auto test(自動テスト)およびコンポーネントテストは一度だけ行われます。このテストでリモートホストへの Ping テストおよび UART テストも一度だけ行われます。

Looping(without External test in Auto test)を選択すると、<ctrl-c>キーを押すまでオートテストは繰り返し実行されます。Ping テストおよび UART テストも繰り返し行われます。

Looping(with External test in Auto test)を選択すると、<ctrl-c>キーを押すまで、Auto テストは繰り返されます。Ping テストおよび UART テストも繰り返し行われます。

**注記: Ethernet および UART にて適正にテストを行うには、STS シリーズの Ethernet ポートに Ethernet ケーブルをつなぎ、すべてのシリアルポートにループバックコネクタを差し込みます。リモートホストの IP アドレスは有効なものである必要があります。デフォルトのサーバーIP アドレスは 192.168.0.128 で、この値は[Firmware upgrade]メニューにて変更可能です。**

```
--------------------------------------------------------------------------------
Hardware Test
--------------------------------------------------------------------------------
Select menu
0. Test Mode - One Time
1. Auto test
2. DRAM test
3. FLASH test
4. EEPROM test
5. Ethernet test
6. UART Mode test
 <ESC> Back, <ENTER> Refresh
-----> 0
--------------------------------------------------------------------------------
Hardware Test
--------------------------------------------------------------------------------
Select menu
0. Test Mode - Looping(Without External test in Auto Test)
1. Auto test
2. DRAM test
3. FLASH test
4. EEPROM test
5. Ethernet test
6. UART Mode test
 <ESC> Back, <ENTER> Refresh
-----> 0
--------------------------------------------------------------------------------
Hardware Test
--------------------------------------------------------------------------------
Select menu
0. Test Mode - Looping(With External test in Auto Test)
1. Auto test
2. DRAM test
3. FLASH test
4. EEPROM test
5. Ethernet test
6. UART Mode test
 <ESC> Back, <ENTER> Refresh
-----> 0
--------------------------------------------------------------------------------
Hardware Test
--------------------------------------------------------------------------------
Select menu
0. Test Mode - One Time
1. Auto test
2. DRAM test
3. FLASH test
4. EEPROM test
5. Ethernet test
6. UART Mode test
 <ESC> Back, <ENTER> Refresh
----->
```

**図 A-6 Bootloader メニュープログラムのハードウェアテストメニュー画面**

[Auto test]を選択すると、すべてのハードウェアコンポーネントのテストは自動的に行われます。

```
--------------------------------------------------------------------------------
 Hardware Test
--------------------------------------------------------------------------------
 Select menu
 0. Test Mode - One time
 1. Auto test
 2. DRAM test
 3. FLASH test
 4. LED test
 5. EEPROM test
 6. UART test
 7. PC card test
 8. Ethernet test
  <ESC> Back, <ENTER> Refresh
 ----->1

******* Hardware auto-detect and auto-test *******
[DRAM]
DRAM Test in progress ----------------------------------------[65536KB]
DRAM Test ----------------------------------------------------[SUCCESS]

[FLASH]
Flash Test Status---------------------------------------------[  100 %]
Flash Test ---------------------------------------------------[SUCCESS]

[FAN]
Fan Status ---------------------------------------------------[7020 RPM]

[LED]
SERIAL READY LED ON/OFF---------------------------------------3 time(s)

[EEPROM]
EEPROM   :  A Type exist
EEPROM Test ---------------------------------------------- [SUCCESS]

[UART]
<--Internal loop test-->
Port # 1 test in progressing(Read/Write)----------[SUCCESS]
Port # 2 test in progressing(Read/Write)----------[SUCCESS]
.
.
.
Port # 7 test in progressing(Read/Write)----------[SUCCESS]
Port # 8 test in progressing(Read/Write)----------[SUCCESS]

<--External loop test-->
Port # 1 test in progressing(Read/Write)----------[SUCCESS]
                      (RTS/CTS)-------------[SUCCESS]
                      (DTR/DSR)-------------[SUCCESS]
Port # 2 test in progressing(Read/Write)----------[SUCCESS]
                      (RTS/CTS)-------------[SUCCESS]
                      (DTR/DSR)-------------[SUCCESS]
.
.
.
Port # 7 test in progressing(Read/Write)----------[SUCCESS]
                      (RTS/CTS)-------------[SUCCESS]
                      (DTR/DSR)-------------[SUCCESS]
Port # 8 test in progressing(Read/Write)----------[SUCCESS]
                      (RTS/CTS)-------------[SUCCESS]
                      (DTR/DSR)-------------[SUCCESS]

[PCMCIA]
```

```
 5V CARD
 5.0V card found: Lucent Technologies WaveLAN/IEEE Version 01.01
          Network Adapter Card

[Ethernet]
Ethernet chip test-------------------------------------------[SUCCESS]
PING 192.168.0.135 from 192.168.161.5 : 64 bytes of ethernet packet.
64 bytes from 192.168.0.135 : seq=0 ttl=255 timestamp=11172879 (ms)
64 bytes from 192.168.0.135 : seq=1 ttl=255 timestamp=11173874 (ms)
64 bytes from 192.168.0.135 : seq=2 ttl=255 timestamp=11174875 (ms)
64 bytes from 192.168.0.135 : seq=3 ttl=255 timestamp=11175876 (ms)

      *******  Hardware auto-detect and auto-test  SUMMARY *******
1. DRAM Test  ------------------------------------------------[SUCCESS]
2. FLASH Test ------------------------------------------------[SUCCESS]
3. FAN Test   ------------------------------------------------[SUCCESS]
4. EEPROM Test-----------------------------------------------[SUCCESS]
5. UART Test Summary
  Port NO |  exist status  |   exist status  | exist status  | exist  status
-------------------------------------------------------------------------------
--
Port 01-04|  YES  SUCCESS  |   YES  SUCCESS  |  YES  SUCCESS  |  YES  SUCCESS
Port 05-08|  YES  SUCCESS  |   YES  SUCCESS  |  YES  SUCCESS  |  YES  SUCCESS

6.PC CARD Test Summary
 5V CARD
 5.0V card found: Lucent Technologies WaveLAN/IEEE Version 01.01
          Network Adapter Card
7. PING Test  ------------------------------------------------[SUCCESS]

PRESS any key to continue!!
```

図 A-7 Bootloader メニュープログラムの Hardware Test 画面

各ハードウェアコンポーネントのテストは,<ESC>キーを押すことでスキップできます。

```
-------------------------------------------------------------------------------
 Hardware Test
-------------------------------------------------------------------------------
 Select menu
 0. Test Mode - One time
 1. Auto test
 2. DRAM test
 3. FLASH test
 4. LED test
 5. EEPROM test
 6. UART test
 7. PC card test
 8. Ethernet test
  <ESC> Back, <ENTER> Refresh
 -----> 1

          *******  Hardware auto-detect and auto-test *******
[DRAM]
DRAM Test in progress ----------------------------------------[  640KB]
DRAM Test ----------------------------------------------------[SKIPPED]

[FLASH]
Flash Test Status---------------------------------------------[    2 %]
FLASH Test ---------------------------------------------------[SKIPPED]
```

図 A-8 ESC キーで特定のテストをスキップしている画面

Looping モードでAutotestを行っている間にエラーが生じた場合、テストは停止され、InUse LEDが点滅してハードウェアテストのエラーを知らせます。この場合、<ctrl-c>キーでメニューページに戻ります。

## A5.5. ファームウェアアップグレード メニュー

Firmware Upgrade メニューでユニットのファームウェアをアップグレードすることが可能です。
ファームウェアのアップグレードを行う前に、Main menu ページから 3 を選択し現在のファームウェア・バージョンを確認してください。リモートからのファームウェアダウンロードには TFTP プロトコルをサポートしています。TFTP サーバーを使用する際には、ユニットの IP アドレスを適正に設定してある必要があります。デフォルトの IP アドレスは 192.168.161.5 です。ファームウェア・アップグレードには、[Firmware File Name] および[Server's IP address]のファイルがサーバーにある必要があります。

```
--------------------------------------------------------------------------------
 Firmware upgrade
--------------------------------------------------------------------------------
 Select menu
 1. Protocol [BOOTP]
 2. IP address assigned to Ethernet interface [192.168.161.5]
 3. Server's IP address [192.168.0.128]
 4. Firmware File Name [sts800.bin]
 5. Start firmware upgrade
  <ESC> Back, <ENTER> Refresh
 -----> 1
 Select protocol ( 1 = BOOTP, 2 = TFTP) : 2


--------------------------------------------------------------------------------
 Firmware upgrade
--------------------------------------------------------------------------------
 Select menu
 1. Protocol [TFTP]
 2. IP address assigned to Ethernet interface [192.168.161.5]
 3. Server's IP address [192.168.0.128]
 4. Firmware File Name [sts800.bin]
 5. Start firmware upgrade
  <ESC> Back, <ENTER> Refresh
 ----->
```

**図 A-9 Bootloader Menu プログラムの Firmware upgrade 画面**

[Start firmware upgrade]を選択すると、画面に確認メッセージが表示されます。Y を入力すると、ファームウェアのアップグレードプロセスが開始されます。これが一度始まると終了するまで一旦停止させることはできません。

```
--------------------------------------------------------------------------------
 Firmware upgrade
--------------------------------------------------------------------------------
```

```
Select menu
 1. Protocol [BOOTP]
 2. IP address assigned to Ethernet interface [192.168.161.5]
 3. Server's IP address [192.168.0.128]
 4. Firmware File Name [sts800.bin]
 5. Start firmware upgrade
 -----> 5
Firmware upgrade cannot be stopped until finished.
And all configuration parameters are restored to default values.
Do you really want to start firmware upgrade(y/n)?y
BOOTP broadcast 1
ARP broadcast 1
TFTP from server 192.168.0.128; our IP address is 192.168.161.5
Filename 'sts800.bin'.
Load address: 0x100000
Loading: ###################################################################
         ###################################################################
         ###################################################################
         ###################################################################
         ###################################################################
         ###################################################################
         ###################################################################
         ###################################################################
         ###################################################################
         ###################################################################
         ###################################################################
         ###################################################################
         ###################################################################
         ###################################################################
         ###################################################################
         ###################################
done
Bytes transferred = 5838194 (591572 hex)

Erase Flash Sectors 9-20 in Bank # 1
BLOCK 1 : Copy to Flash... done
Erase Flash Sectors 21-115 in Bank # 1
BLOCK 2 : Copy to Flash... done
Erase Flash Sectors 116-116 in Bank # 1
BLOCK 3 : Copy to Flash... done
BLOCK 4 : Erase Flash Sectors 117-117 in Bank # 1
Firmware upgrade is finished successfully.


--------------------------------------------------------------------------------
 Firmware upgrade
--------------------------------------------------------------------------------
Select menu
 1. Protocol [BOOTP]
 2. IP address assigned to Ethernet interface [192.168.161.5]
 3. Server's IP address [192.168.0.128]
 4. Firmware File Name [sts800.bin]
 5. Start firmware upgrade
  <ESC> Back, <ENTER> Refresh
 ----->
```

**図 A-10 Firmware アップグレード画面**

ファームウェア・アップグレード作業が終了したら、成功しましたというメッセージがメインメニューに表示されます。

# 付録6. Serial/IP ソフトウェアで STS シリーズを使用する

## A 6.1. STS シリーズと Serial/IP オプションの比較対象表

| Serial Port Configuration of STS Series | | | Serial/IP Configuration | | |
|---|---|---|---|---|---|
| Host mode Configuration | | Cryptography Configuration | Credentials | Connection Protocol | Security |
| Host mode | Telnet Protocol | Encryption Method | | | |
| TCP | Disabled | None | No login required | Raw TCP connection | Disable |
| TCP | Enabled | None | No login required | Telnet | Disable |
| TCP | Disabled | "SSLv2" or "SSLv3 rollback to v2" | No login required | Raw TCP connection | Negotiate SSLv3/TSLv1 |
| TCP | Disabled | "SSLv3" or "SSLv3 rollback to v2" | No login required | Raw TCP connection | SSLv3 |
| TCP | Disabled | "TLSv1" or "SSLv3 rollback to v2" | No login required | Raw TCP connection | TSLv1 |
| TCP | Enabled | "SSLv2" or "SSLv3 rollback to v2" | No login required | Telnet | Negotiate SSLv3/TSLv1 |
| TCP | Enabled | "SSLv3" or "SSLv3 rollback to v2" | No login required | Telnet | SSLv3 |
| TCP | Enabled | "TLSv1" or "SSLv3 rollback to v2" | No login required | Telnet | TSLv1 |

STS シリーズの SSLv3 rollback to v2"は、Serial/IP の"negotiate SSLv3/TSLv1 のことです。
STS シリーズの暗号化方法が"SSLv3"に設定されている場合、クライアント側（Serial/IP）は"Negotiate SSLv3/TSLv1"オプションで STS シリーズに接続できません。

## A 6.2. 接続例： Telnet および SSL v3 暗号化

**Step 1.** STS シリーズのポート#1を次のように設定してください。

Host mode= TCP

Port number=7001

Telnet Protocol = Enabled

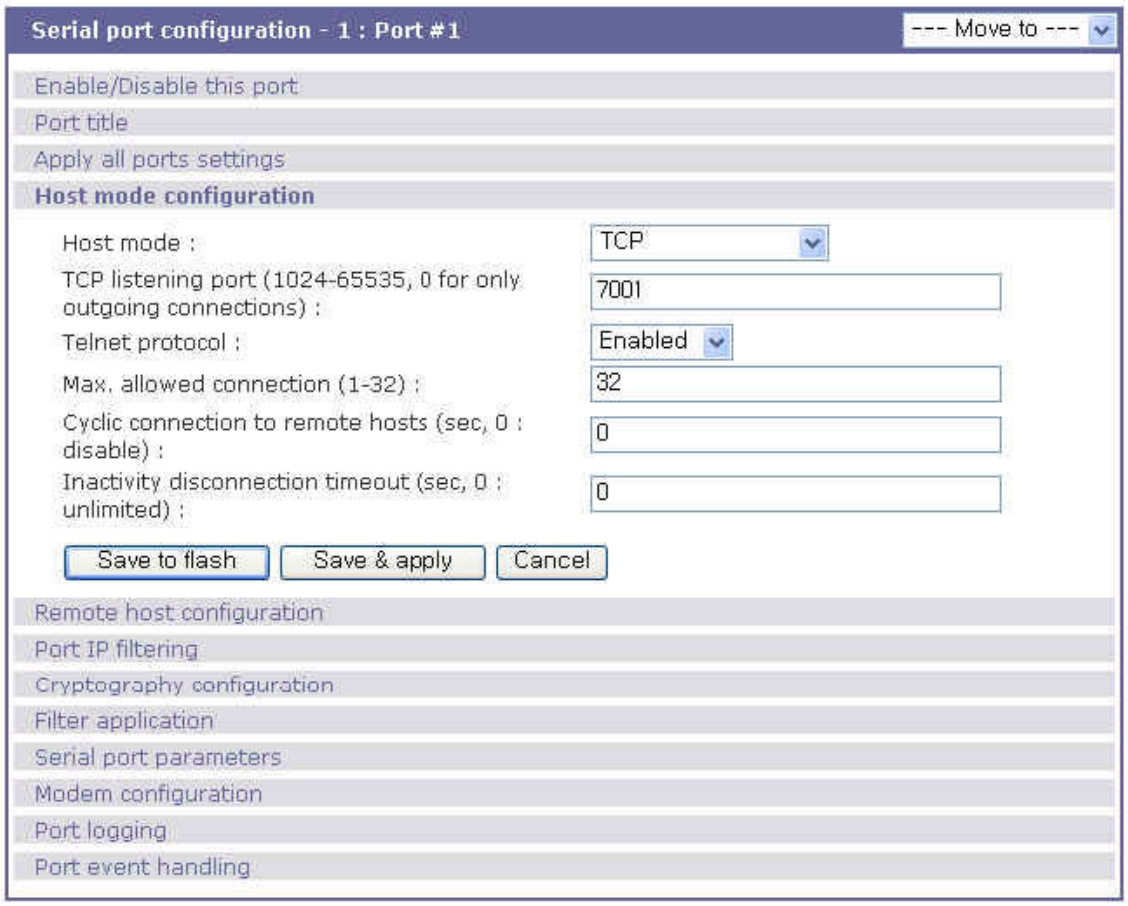



**図 A-11 Host mode configuration**

**Step 2** 次のように STS シリーズのシリアルポート#1 の暗号設定を Cryptography Configuration 画面にて行います。

Encryption method = SSLv3

他のオプションをファクトリデフォルト値にしてください。

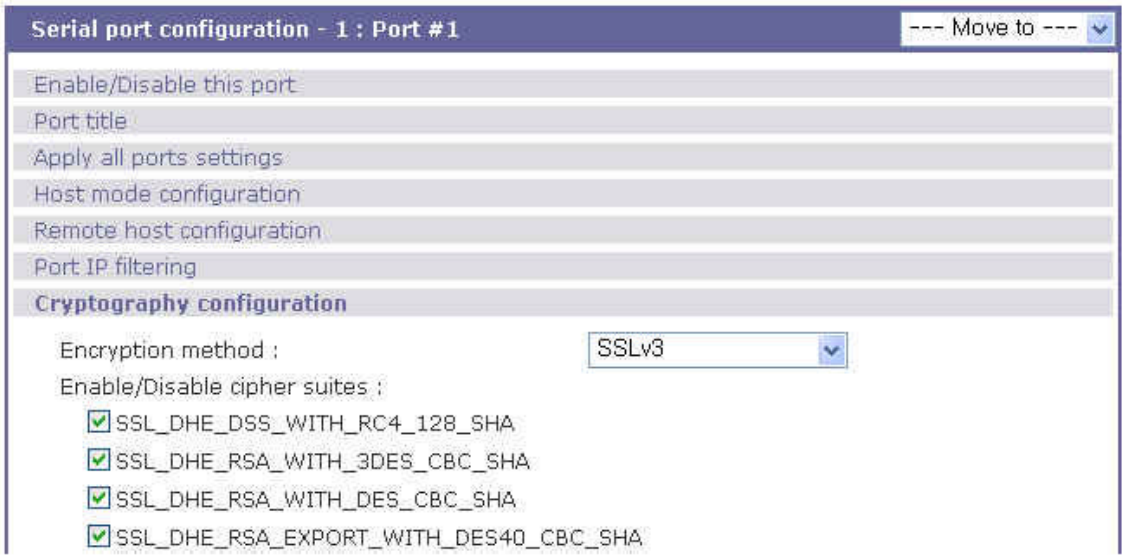



図 A-12 Cryptography Configuration

**Step 3.** Serial/IP Control Panel(シリアル/IP 制御パネル)を開き、"Select Ports"ボタンをクリックして STS シリーズのシリアルポート#1 と通信するために使用する COM ポートにチェックマークを入れます。

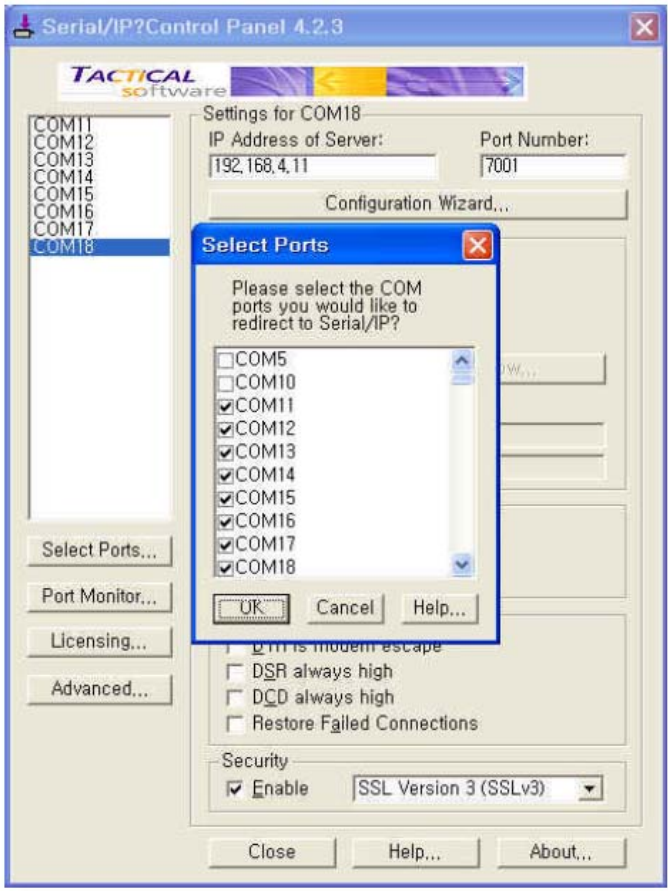



図 A-13 Serial/IP Control Panel にてポートを選択する画面

**Step 4** サーバーの IP アドレス（STS シリーズの IP アドレス）およびポート番号（ポート#1）を入力し、次のパラメータを選択します。

Credentials 証明書=No Login Required （ログインの必要なし）

Connection Protocol(接続プロトコル)=Telnet

Security(セキュリティ)= SSL Version 3 (SSLv3)

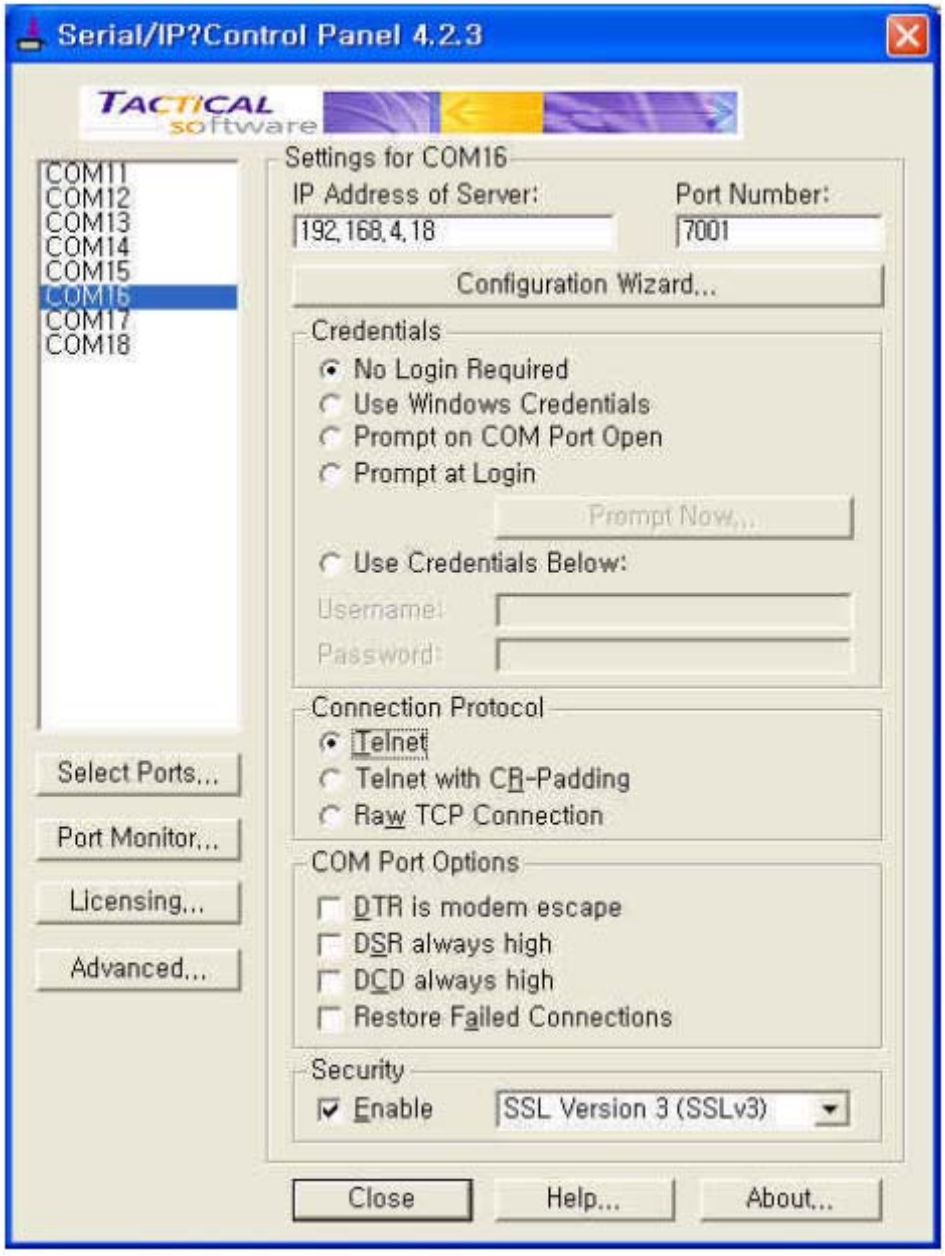



**図 A-19 Serial/IP Control Panel のパラメータ設定画面**

**Step 5.** ターミナルソフトを起動し対応する COM ポートを選択します。 これで、PC 側から STS シリーズのシリアルポートを使用することが可能です。

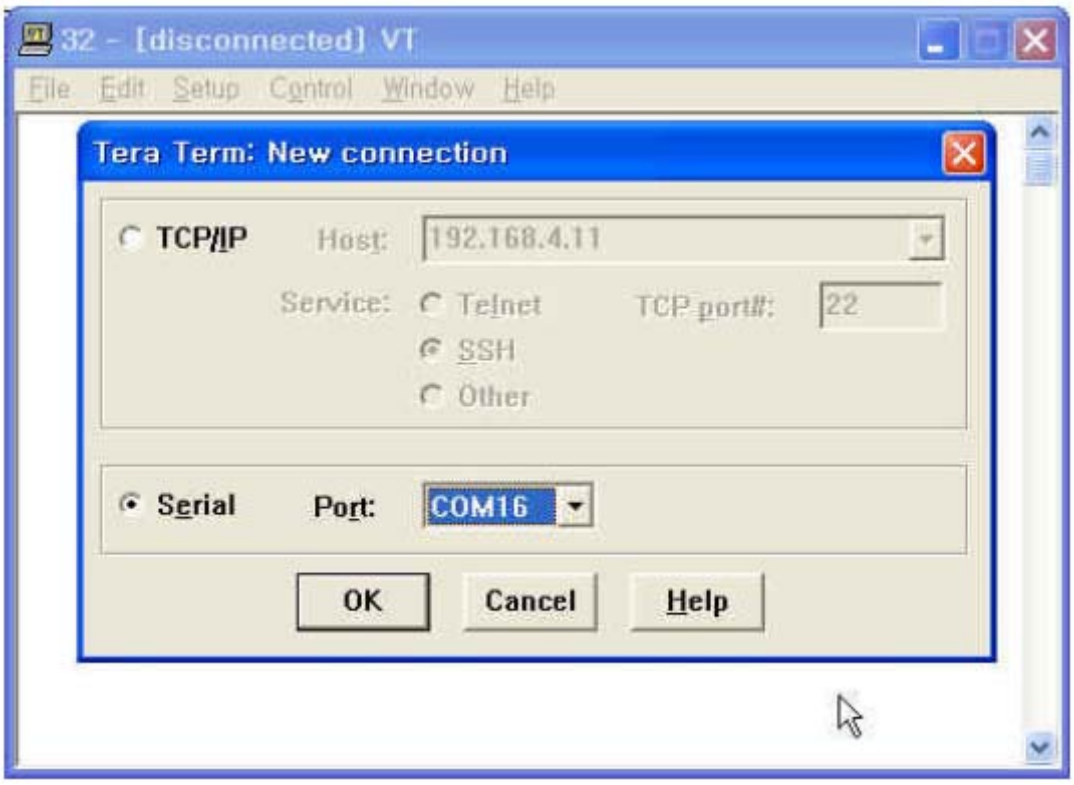



**図 A-15 Serial/IP で STS シリーズのシリアルポートに接続**

**Step 6** Serial/IP Port Monitor を使用して接続状態を監視することができます。

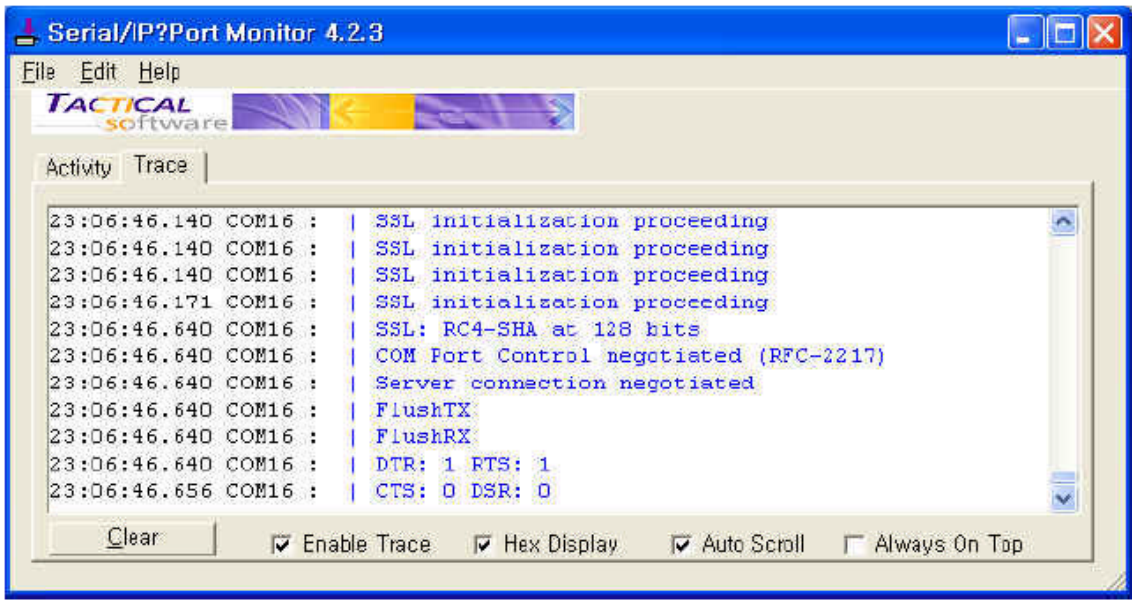



**図 A-16 Serial/IP Trace Window**

# 付録7.　Serial/IP ソフトウェアで STS シリーズを使用する

## A 7.1.　OpenSSL パッケージのインストール

**Step 1.**　最新版の OpenSSL パッケージをダウンロードする

**Step 2.**　OpenSSL パッケージをインストールする

**[Windows ユーザー]**

Windows バイナリファイル用にOpenSSLをダウンロードし、実行する。

( http://www.slproweb.com/products/Win32OpenSSL.html )

**[Linux ユーザー]**

OpenSSLソースコードをダウンロードし、コンパイルする。

```
# cd /work/
# tar -xvzf openssl-0.9.7d.tar.gz
# cd openssl-0.9.7d
# ./config
# make
# make test
# make install
```

## A 7.2.　root CA (self-signed)を作成

Step 1.　Openssl configuration ファイルを編集

デフォルトの configuration ファイルの場所を以下に記します。

[Windows]

C:\Program Files\OpenSSL\bin

[Linux]

/Usr/share/ssl/openssl.cnf

[req_distinguished_name]セクションを次のように変更します。

```
countryName             = Country Name (2 letter code)
countryName default     = KR
countryName min         = 2
countryName max         = 2

stateOrProvinceName     = State or Province Name (full name)
#stateOrProvinceName default    = Some-State

localityName          = Locality Name(eg, city)
localityName default        = Seoul

0.organizationName      = Organization Name (eg, company)
0.organizationName_default  = Sena Technologies Inc.
```

```
# we can do this but it is not needed normally :-)
#1.organizationName     = Second Organization Name (eg, company)
#1.organizationName default = World Wide Web Pty Ltd

organizationalUnitName      = Organizational Unit Name (eg, section)
#organizationalUnitName default =

commonName           = Common Name (eg, your name or your server\'s hostname)
commonName_default      = Sena Technologies
commonName max          = 64

emailAddress         = Email Address
emailAddress_max     = 40
```

[req_attributes]セクションを次のように変更します。

```
challengePassword min =0
challengePassword_max =0
```

**Step 2.** Self-signed Root CA(Certificate Authority)を作成する

**[Windows]**

# cd /work/openssl-0.9.7d/

**[Linux]**

# cd/work/openssl-0.9.7d/

# mkdir CA

# cd CA

# sh /usr/local/ssl/misc/CA.sh –newca

```
CA certificate filename (or enter to create)
   ;(Press Enter to use default value)
Making CA certificate ...
; openssl is called here as follow from CA.sh
; openssl req -new -x509 -keyout ./demoCA/private/./cakey.pem \
;  -out ./demoCA/./cacert.pem -days 365
Using configuration from /usr/local/ssl/lib/ssleay.cnf
Generating a 1024 bit RSA private key
........++++++
.....................++++++
writing new private key to './demoCA/private/./cakey.pem'
Enter PEM pass phrase:   ; CA Password (Enter password and remember this)
Verifying password - Enter PEM pass phrase:  ; CA Password
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----  ; CA's Information
Country Name (2 letter code) [AU]: KR
State or Province Name (full name) [Some-State](Enter)
Locality Name (eg, city) []:Seoul
Organization Name (eg, company) [Internet Widgits Pty Ltd]: Sena Technologies
Organizational Unit Name (eg, section) [](Enter)
Common Name (eg, YOUR name) []:Sena Technologies
Email Address []:(Enter)
#
```

Step 3. CA key ファイル(demoCA/private/cakey.pem)および CA 証明書(demoCA/cacert.pem)が生成されているかどうかを確認する。

# ls demoCA/

```
cacert.pem certs   crl index.txt      newcerts
private    serial
```

# ls demoCA/private

```
cakey.pem
```

## A 7.3. 証明書リクエストを作成

新規証明書を作成するには証明書リクエストを最初に作成する必要があります。

# cd /work/openssl-0.9.7c/CA

次のコマンドを実行してください。

# openssl genrsa -out key.pem 1024

# openssl req -new -key key.pem -out req.pem

(この例はサンプル設定ファイル"openssl.conf.sena"を利用した場合です)

```
Using configuration from /usr/share/ssl/openssl.cnf
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [US]:  (Enter)
State or Province Name (full name) [Minnesota]:  (Enter)
Locality Name (eg, city) [Minneapolis]:  (Enter)
Organization Name (eg, company) [Digi International]:  (Enter)
Organizational Unit Name (eg, section) []:(Enter)
Common Name (eg, your name or your server's hostname) []:Sena VTS
Email Address []:(Enter)

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:(Press Enter - Do not enter any other characters)
An optional company name []:(Press Enter - Do not enter any other characters)
```

## A 7.4. 証明書リクエストに署名する

Step 1. 証明書リクエストに署名する

# cd /work/openssl-0.9.7c/CA

# cp req.pem newreq.pem

# sh /usr/local/ssl/misc/CA.sh -sign

```
Using configuration from /usr/share/ssl/openssl.cnf
Enter PEM pass phrase: CA Password (Enter CA password in step 2-2)
Check that the request matches the signature
Signature ok
The Subjects Distinguished Name is as follows
countryName           :PRINTABLE:'US'
stateOrProvinceName   :PRINTABLE:'Minnesota'
localityName          :PRINTABLE:'Minneapolis'
organizationName      :PRINTABLE:'Digi International'
commonName            :PRINTABLE:'Digi PortServer CM'
Certificate is to be certified until Oct  6 09:39:59 2013 GMT (3653 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1 (0x1)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: C=US, ST=Minnesota, L=Minneapolis, O=Digi International, CN=Digi
International
        Validity
            Not Before: Oct  6 09:39:59 2003 GMT
            Not After : Oct  6 09:39:59 2013 GMT
        Subject: C=US, ST=Minnesota, L=Minneapolis, O=Digi International, CN=Digi
PortServer CM
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
....
-----BEGIN CERTIFICATE-----
....
-----END CERTIFICATE-----
Signed certificate is in newcert.pem
```

Step 2. 署名された証明書が生成されたかどうかを確認する

# ls

```
demoCA       key.pem     newcert.pem      newreq.pem     req.pem
```

## A 7.5. STS 用の証明書を作成

Step 1. Newcert.pem file のヘッダーを削除する。

# cd /work/openssl-0.9.7c/CA

# cp newcert.pem server.pem

# vi server.pem

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1 (0x1)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: C=KR, ST=, L=Seoul, O=Sena Technologies Inc., CN= Sena
```

```
Technologies
       Validity
          Not Before: Oct  6 09:39:59 2003 GMT
          Not After : Oct  6 09:39:59 2013 GMT
       Subject: C=US, ST=Minnesota, L=Minneapolis, O=Digi International, CN=Digi
PortServer CM
       Subject Public Key Info:
          Public Key Algorithm: rsaEncryption
          RSA Public Key: (1024 bit)
....
== Removing above lines ===
-----BEGIN CERTIFICATE-----
....
-----END CERTIFICATE-----
```

**Step 2.** Key.pem ファイルを server.pem へ連結する。

```
# cat key.pem >> server.pem
```

**株式会社インターソリューションマーケティング**
〒150-0013 東京都渋谷区恵比寿 1-24-14 EXOS 恵比寿ビル 5F
Phone: 03-5795-2685 Fax: 03-5795-2686
URL: http://www.intersolutionmarketing.com
Mail: info@intersolutionmarketing.com