

SENA
プロ デバイスサーバー
Hello Device Pro Series
(PS 110/410/810)
ユーザーガイド

Version 1.1_JP
2007-12-20



**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. 03-5795-2895 Fax. 03-5795-2896

InterSolution Marketing Inc.,
EXOS Ebisu Bldg. 5F,
Ebisu 1-24-14, Shibuya, Tokyo Japan 150-0013
Tel. +81 3 5795 2895 Fax. +81 3 5795 2896

コピーライト

プロ シリーズデバイスサーバー 日本語ユーザーガイドは、Sena Technologies 社の英文マニュアルを基に、株式会社インターソリューションマーケティングにより再構成されたものです。製品名、会社名は、各社の商標あるいは登録商標です。本ユーザーガイドを無断でコピー、転載、記載する行為を堅くお断りします。

商標

HelloDevice Pro 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、取扱いを謝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。

煙がでたり臭い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)
- ・直射日光があたる場所(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。

目次

1. はじめに	7
1.1. 概要.....	7
1.2. 同梱品チェックリスト.....	8
1.3. 製品スペック一覧表.....	9
1.4. 用語.....	10
2. 使用準備	12
2.1. パネル・レイアウト.....	12
2.1.1. PS110 パネル・レイアウト.....	12
2.1.2. PS410/810 パネル・レイアウト.....	13
2.2. ハードウェアを接続する.....	14
2.2.1. ネットワークにつなぐ.....	14
2.2.2. シリアル機器につなぐ.....	15
2.2.3. 電源につなぐ.....	16
2.2.4. システムコンソールへのアクセス.....	17
2.2.5. システムコンソールを使用する.....	17
2.2.6. リモート・コンソールを使用する.....	20
2.3. ウェブブラウザ管理インターフェースにアクセスする.....	21
3. ネットワーク設定	23
3.1. IP 設定.....	23
3.1.1. Static(静的)IP アドレスを使用する.....	23
3.1.2. DHCP を使用する.....	24
3.2. SNMP 設定.....	25
3.2.1. MIB-II システムオブジェクト設定.....	26
3.2.2. アクセスコントロール設定.....	27
3.2.3. トラップレシーバー設定.....	27
3.2.4. SNMP を使用したマネージメント.....	27
3.3. 動的 DNS 設定.....	28
3.4. SMTP 設定.....	29
3.5. IP フィルタリング.....	30
3.6. SYSLOG サーバー設定.....	33
3.7.1. 概要.....	34
3.7.2. Locating Server の設定.....	34
3.7.3. Locating Server 通信プロトコル.....	34
3.8. NFS サーバー設定.....	35

3.9. TCP サービス設定	36
4. シリアルポート設定	37
4.1. 概要	37
4.2.1. Port Enable/Disable	39
4.2.2. Port Title	40
4.2.3. Host Mode Configuration	40
4.2.4. Remote Host Configuration (リモートホスト設定)	50
4.2.6. シリアルポートパラメータ	56
4.2.7. モデムの設定 (Modem configuration)	60
4.2.8. Port Logging (ポートロギング)	61
4.2.9. Port イベントの操作設定	62
4.2.10. Copy port Configuration (ポート設定をコピーする)	65
5. システム管理 (System Administration)	65
5.1. System Status (システムステータス)	66
5.2. System Logging (システムロギング)	66
5.3. Change Password (パスワードの変更)	67
5.4. Device Name Configuration (デバイス名設定)	67
5.5. 日付および時刻の設定	68
5.6. ファクトリ・リセット	69
5.7. コンフィギュレーション管理	69
5.8. ファームウェア・アップグレード	70
5.9. ユーザー管理	73
6. システム統計 (System Statistics)	75
6.1. ネットワークインターフェース統計 (Network Interface Statistics)	75
6.2. シリアルポート統計 (Serial Ports Statistics)	75
6.3. IP 統計	76
6.4. ICMP 統計	78
6.5. TCP 統計	81
6.6. UDP 統計	83
7. CLI ガイド	84
7.1. はじめに	84
7.2. Flash 区画	84
7.3. サポートしている Linux ユーティリティ	84
7.3.1. Shell & shell utilities:	84
7.3.2. File and disk utils:	84
7.3.3. System utilities:	84

7.3.4. Network utilities:.....	84
7.4. CLI にアクセスする.....	85
付録1. 接続.....	86
A 1.1. Ethernet ピン配置.....	86
A 1.2. コンソールおよびシリアルポートピン配置.....	86
A 1.3. Ethernet 配線ダイアグラム.....	87
A 1.4. シリアル配線ダイアグラム.....	88
A.1.4.1. RS232 シリアル配線ダイアグラム.....	88
A.1.4.2. RS422/485 シリアル配線ダイアグラム.....	89
付録2. PS デバイスサーバー設定ファイル.....	91
A 2.1. Port1.conf.....	91
A 2.2. filter.conf.....	91
A 2.3. snmp.conf.....	91
付録3. ウェルノウンポート番号.....	92
付録4. BIOS メニュープログラム.....	93
A 4.1. 概要.....	93
A 4.2. メインメニュー.....	93
A 4.3. RTC 設定メニュー.....	93
A 4.4. ハードウェアテストメニュー.....	94
A 4.5. ファームウェア・アップグレード メニュー.....	97
付録5. Serial/IP ソフトウェアで PS デバイスサーバーを使用する.....	99
A 5.1. PS デバイスサーバーと Serial/IP オプションの比較対象表.....	99
A 5.2. 接続例: Telnet および SSL v3 暗号化.....	99

1. はじめに

1.1. 概要

これは SENA テクノロジー社製プロ デバイスサーバーシリーズ PS110/410/810 のユーザーガイドです。

プロ デバイスサーバーシリーズは、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。 DHCP, 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を使用してシリアルデバイスを管理します。

プロ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になります。

プロシリーズは telnet SSH, シリアルコンソール、またはWEBのような様々な方法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が可能になります。

また、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することが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を使用して可能です。

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用に、プロシリーズはデータ暗号化用の SSLv3 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プロシリーズシリアルデバイスに不本意なデータが混入するのを防ぎます。

プロシリーズデバイスサーバーが活躍する主な分野:

- ・ FA
- ・ 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
- ・ メディカルシステム

プロシリーズは RS-232/422/485 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

- ・ PS110/410/810 本体
- ・ 外付け 110V(230V)電源アダプタ
- ・ シリアルケーブルキット
- ・ クイックスタートガイド
- ・ CD-ROM
- ・ 日本語ユーザーガイド

1.3. 製品スペック一覧表

	PS1108	PS410	PS810
シリアルインターフェース	1ポート	4ポート	8ポート
	シリアルスピード 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 RS232 RX, Tx, RTS, CTS, DTR, DSR, DCD, GND RS422 RX+, RX-, Tx+, TX- RS485 Data+, Data-		
	モデム制御: DTR, DSR, DCD		
ネットワークインターフェース	10/100 Base-Tx Ethernet		
	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 v2 -SSLv3 -DNS, Dynamic DNS, HTTP, HTTPS, NFS -SMTP, with/without Authentication, pop-before SMTP -DHCP client, NTP, SNMP v1&v2		
セキュリティ	ユーザーID & パスワード		
	HTTPS		
	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		
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 フラッシュメモリおよび Telnet または Web 経由		
LED 表示	Power Ready (PS810 専用) 10/100 Base Link 10/100 Base Act (PS410/PS810 専用) Serial Rx/Tx (各ポート)		
環境	動作時気温: 0°Cから 50°C 保存時気温: -20°Cから 66°C 湿度: 90% (結露無きこと)		
電源	9~30VDC 0.35A@ 9VDC	9~30VDC 0.4A@ 9VDC	100~240VDC 0.24A
寸法 LxWxH(mm)	114x82x26(mm)	119x227x27(mm)	119x437x44(mm)
重量 (Kg)	0.300	0.750	1.56
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。これらの用語はインターネットワーキングと関係があり、プロ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。プロシリーズの 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

この章ではプロ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する、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する、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。

この箇所を網羅するには以下の物をご用意ください。

- PS 用電源ケーブル(付属品) 1 本
- DB9 メス DB9 メスクロス シリアルデータケーブル(付属品) 1 本
- Ethernet ケーブル(付属品) 1 本
- 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. PS110 パネル・レイアウト

PS110には4つのLED表示があります。上部左側にあるランプは、システム電源オン・オフ状態を表示します。下部左側にあるランプは 10/100Base Ethernet のリンク状態を表示します。右側の 2 つのランプはシリアルポートの送受信状態を表示します。

筐体の底部にはファクトリリセットボタンがあり、押すことによって PS を工場出荷時の値(初期設定値)にリセットすることができます。

Ethernet 差し込み口の横には DIP スイッチがあり、そこでシリアルポートの通信タイプを選択することができます(シリアルポートの通信タイプに関する詳細は 4.2.6.および付録Aを参照してください)。

シリアルポートの横についている Data/Console スイッチで、シリアルポートをコンソール/データモードの変換を行います(2.2.5.からシリアルコンソールアクセス方法に関する詳細情報を参照してください)。

LED ランプ		機能
Status	Power	電源が供給されると、赤色に点灯
	Ethernet Ready	Ethernet ネットワークに接続すると緑色に点灯
Serial Port	Rx	PS110 のシリアルポートを通して入ってくるデータストリームがあるたびに点滅
	Tx	PS110 のシリアルポートを通り送信されるデータストリームがあるたびに点滅

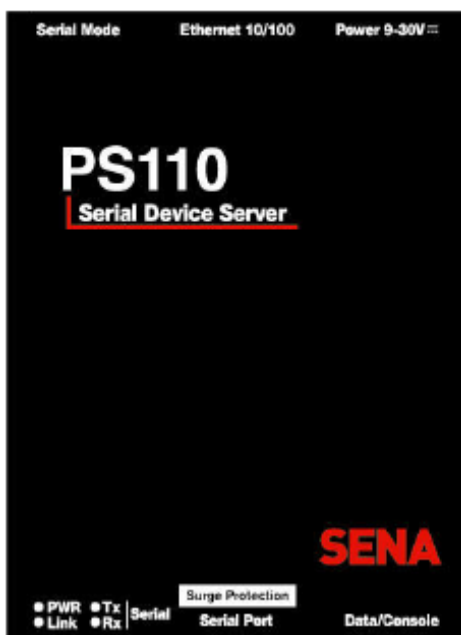


図 2-1 PS110 パネル・レイアウト

2.1.2. PS410/810 パネル・レイアウト

以下の図表に示されているように、PS410/480 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 2 つのランプは Power および Ready です。次のランプは Ethernet および Act です。次のランプはシリアルポートの送受信です。表 2-2 にはそれぞれの LED 表示ランプの意味をリストしています。

表 2-2 PS410/810 の LED 表示の意味

LED ランプ		機能
Status	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できているときに点灯します (PS810 のみ)
Ethernet	Link	Ethernet ネットワーク上に接続された場合に点灯
	Act	Ethernet ポートを通してパケットデータが送受信される場合に点滅
Serial Port	Rx	PS デバイスサーバーのシリアルポートを通して入ってくるデータストリームがあるたびに点滅
	Tx	PS デバイスサーバーのシリアルポートを通り送信されるデータストリームがあるたびに点滅

シリアルコンソールポートの近くにはファクトリリセットボタンがあり、工場出荷時 (初期設定時) の状態にリセットすることができます。

PS410 には 4 つの DIP スイッチがあり、シリアルポートの通信タイプを設定します (4.2.6. および付録 A で詳細情報を参照してください)。

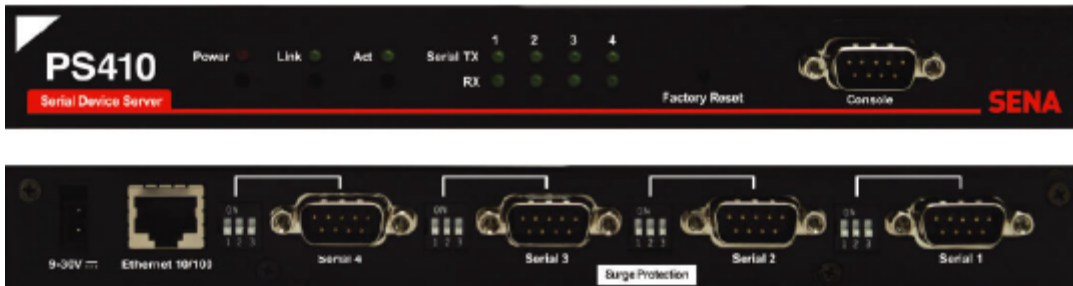


図 2-2 PS410 のパネル・レイアウト



図 2-3 PS810 のパネル・レイアウト

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どのようにプロシリーズ デバイスサーバーをお使いの機器への接続方法を説明します。

- PS デバイスサーバーを Ethernet ハブまたはスイッチにつなぐ
- シリアルデバイスにつなぐ
- PS デバイスサーバーに電源を供給する

2.2.1. ネットワークにつなぐ

Ethernet ケーブルを PS デバイスサーバーの Ethernet ポートにつなぎます。Ethernet のもう片端はネットワークポートにつなぎます。ケーブルが正常につながれているならば、PS デバイスサーバーは Ethernet ネットワークに接続されます。Link ランプは緑色に点灯し、Act ランプは、Ethernet パケットの送受信のたびに点滅します。

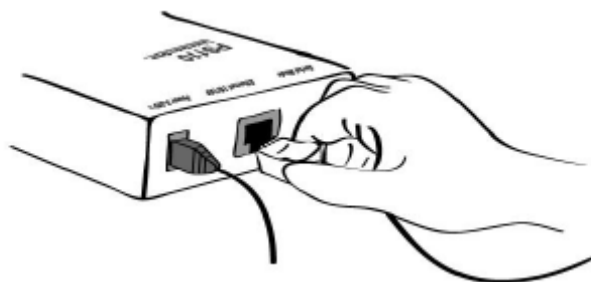


図 2-4 PS110 にネットワークケーブルをつなぐ

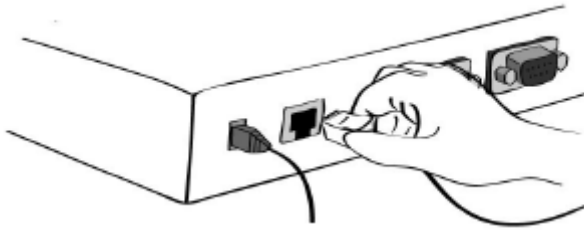


図 2-5 PS410 にネットワークケーブルをつなぐ

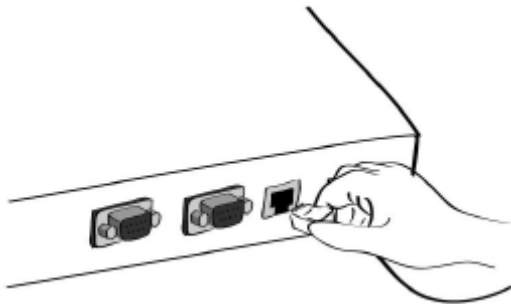


図 2-4 PS810 にネットワークケーブルをつなぐ

2.2.2. シリアル機器につなぐ

コンソールケーブルを PS デバイスサーバーのシリアルポートにつなぎます。シリアルデバイス側のコンソールポートにつなぐには、どのような形状をしているのかをまず確認する必要があります。詳細情報は、「付録 1 接続」を参照してください。

注記： シリアルコンソールによる PS110 の初期設定作業は必須です。最初に、シリアルケーブルをコンフィギュレーションに用いるコンピュータにつないでください。それから Data/Console スイッチを Console 側にしてください。またシリアルモードの DIP スイッチを RS-232 モードにします。PS110 のコンフィギュレーション方法はセクション 2.2.5.にて説明されます。

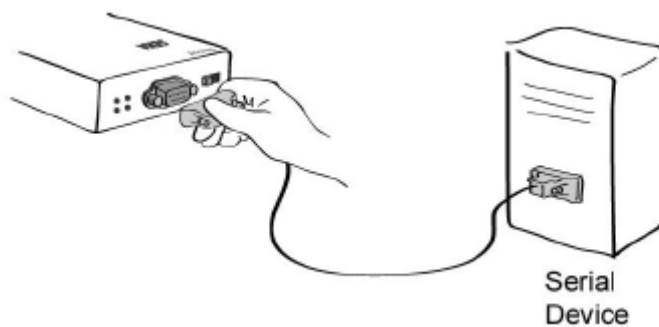


図 2-7 PS110 に機器をつなぐ

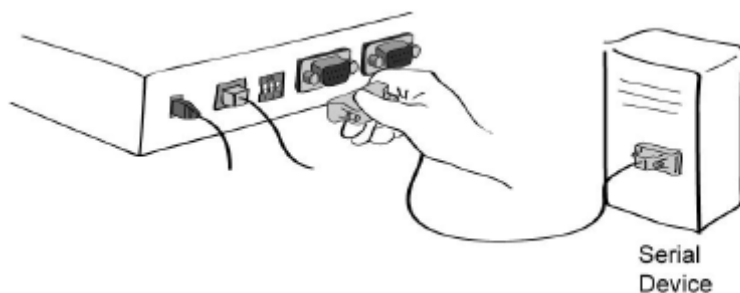


図 2-8 PS410 に機器をつなぐ

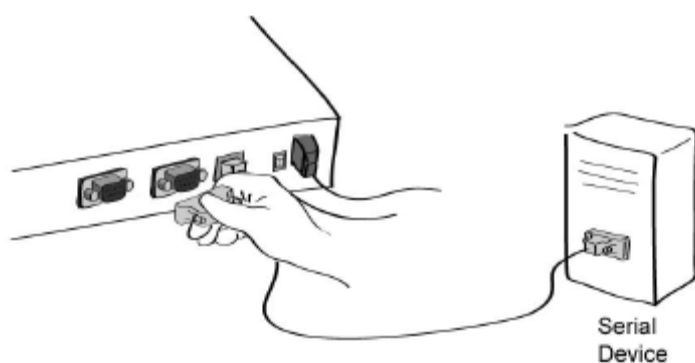


図 2-9 PS810 に機器をつなぐ

2.2.3. 電源につなぐ

PS デバイスサーバーに電源ケーブルをつなぎます。電源が正常に供給されれば、電源 LED ランプは赤色に点灯します。

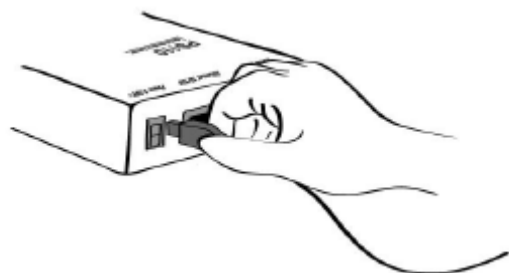


図 2-10 PS110 に電源ケーブルをつなぐ

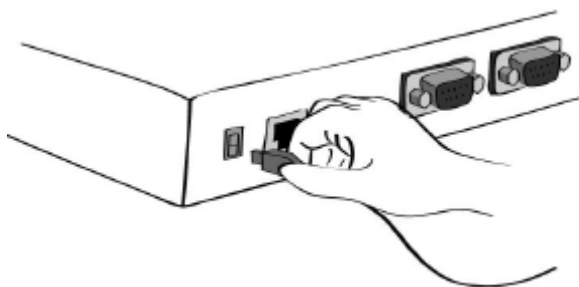


図 2-11 PS410 に電源ケーブルをつなぐ

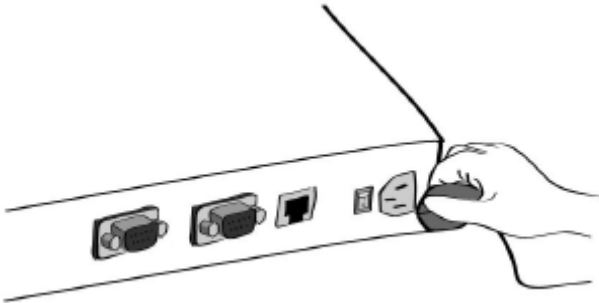


図 2-12 PS810 に電源ケーブルをつなぐ

2.2.4. システムコンソールへのアクセス

PS 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サイトか、もしくはリモートサイトかで変わってきます。または、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シリアルケーブルを用いて直接 PS デバイスサーバーに接続することができます。

- ・ 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 PS デバイスサーバーに Telnet(port23), SSH(Port22)を利用したメニュー表示型インターフェースを使用可能です。

注記: PS デバイスサーバーは SSH v2 のみをサポートしています。ですから SSH v2 をサポートしている SSH を使用する必要があります。

- ・ Web:

PS デバイスサーバー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で可能です。

上記の設定方法は、PS デバイスサーバー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) コンソールケーブルの一方を PS デバイスサーバーにつなぎます。(PS110 の場合は、Data/Console スイッチを Console 側にし、シリアルモードの DIP スイッチを RS-232 モードにします。DIP スイッチの設定方法に関しては付録 1 で詳細が記されます)。

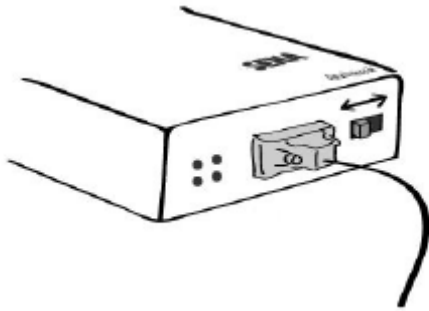


図 2-13 PS110 にシステムコンソールケーブルをつなぐ

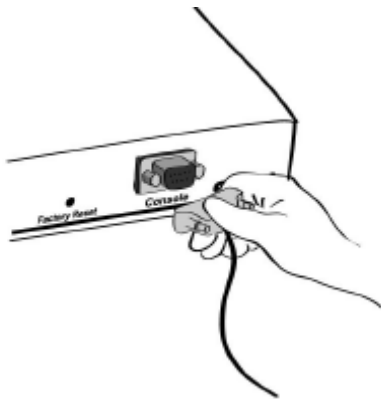


図 2-13 PS410 にシステムコンソールケーブルをつなぐ

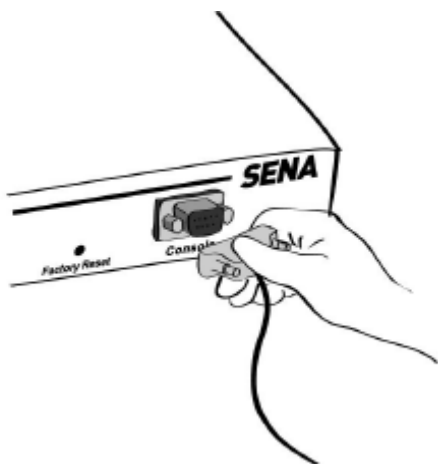


図 2-13 PS110 にシステムコンソールケーブルをつなぐ

- 2) もう片方のシリアルケーブルの端をコンフィギュレーション用のコンピュータにつなぎます。
- 3) ターミナルソフトを起動します (Hyper Terminal 等)。ターミナル祖父と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。
- 4) Enter を押します。
- 5) ユーザー名およびパスワードを入力し PS 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 password: root)

```
ProSeries login: root
Password:
#
```

- 6) ログイン後、コマンドライン上に任意な Shell コマンドを使用することができます。
- 7) “editconf”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、#editconf でメニュー画面に行きます。

```
] / [
1. Network configuration
2. Serial port configuration
3. System administration

COMMAND (Display HELP : help)>save
COMMAND (Display HELP : help)>apply
COMMAND (Display HELP : help)>help
] HELP [
[Enter]      refresh
[ESC]       cancel or go to upper
/           go to root
..          go to upper
clear      clear screen
pwd        display path to current menu
save       save current configuration
apply      apply current configuration
help       display this
exit       exit

COMMAND (Display HELP : help)>[Enter]

] / [
1. Network configuration
2. Serial port configuration
3. System administration

COMMAND (Display HELP : help)>
```

- 8) 図 2-16 が表示されます。

```
# editconf

] / [
1. Network configuration
2. Serial port configuration
3. System administration

COMMAND (Display HELP : help)>save
COMMAND (Display HELP : help)>apply
COMMAND (Display HELP : help)>help
] HELP [
[Enter]      refresh
[ESC]       cancel or go to upper
/           go to root
..          go to upper
clear      clear screen
```

```

pwd          display path to current menu
save        save current configuration
apply      apply current configuration
help       display this
exit       exit

COMMAND (Display HELP : help)> [Enter]

] / [
1. Network configuration
2. Serial port configuration
3. System administration

COMMAND (Display HELP : help)>

```

図 2-16 メインメニュー画面

メインメニュー画面から、メニュー番号を選択し Enter をおすことにより、設定用のメニューアイテムを選択することが可能です。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 PS デバイスサーバーの不揮発性メモリスペースに保管されませんが、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 PS デバイスサーバーにアクセスする前に、IP アドレスを事前に知っておく必要があります（詳細は 3 章 ネットワーク設定を参照）。PS デバイスサーバーのデフォルト 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 PS デバイスサーバーと同一かどうかを確認します。もし必要であれば、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。

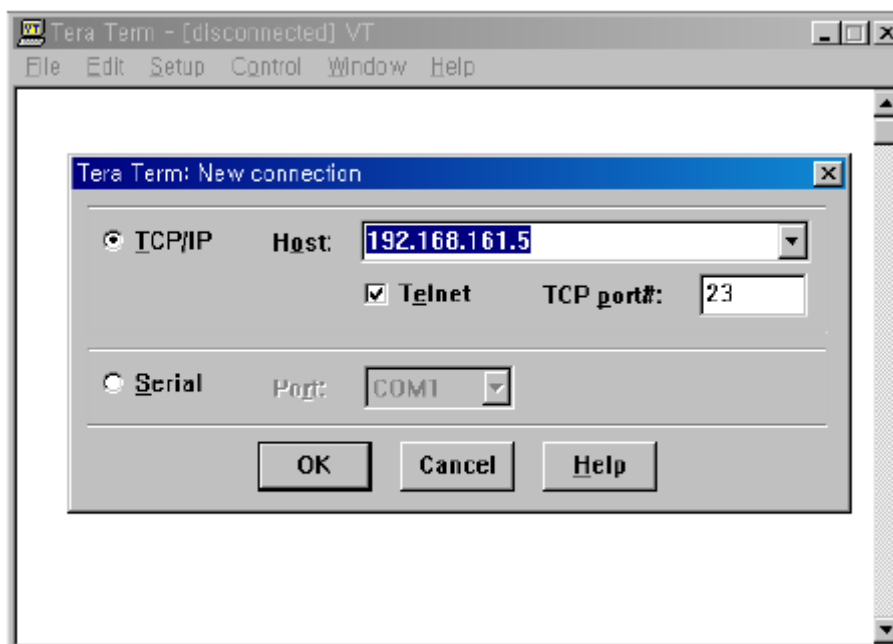


図 2-17 Telnet プログラム設定例 (Tera Term Pro)

- 2) PS デバイスサーバーにログインします。ユーザー名およびパスワードを入力してください。(root)
- 3) ユーザー名およびパスワードを入力後、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する

PS デバイスサーバーは HTTP および HTTPS プロトコルをサポートしています。PS デバイスサーバーには独自の WEB 管理ユーティリティもあります。PS デバイスサーバー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 PS デバイスサーバーの 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 Password: root) です。

注記:PS デバイスサーバーウェブ管理ページにアクセスする前に、PS デバイスサーバーの 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。

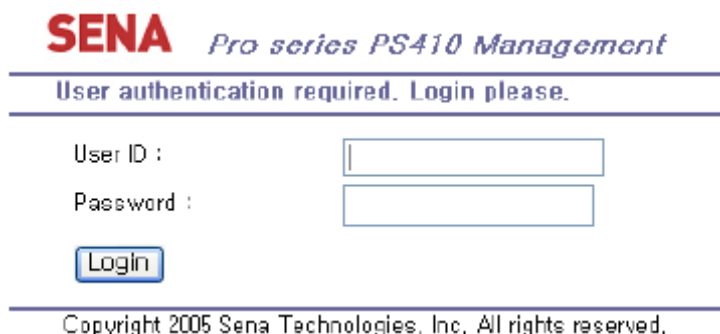


図 2-18 PS デバイスサーバーウェブ管理インターフェースのログイン画面

次の図 2-19 は PS デバイスサーバーのウェブ管理インターフェースの設定用ページです。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、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。もし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。

SENA

Network configuration

- IP configuration
- SNMP configuration
- Dynamic DNS configuration
- SMTP configuration
- IP filtering configuration
- SYSDLOG configuration
- Locating server configuration
- NFS configuration
- TCP configuration

Serial port configuration

- Configuration

System administration

- System status
- System logging
- Device name
- Date and time
- Change password
- User administration
- Factory reset
- Firmware upgrade

System statistics

- Network interfaces
- Serial ports
- IP
- ICMP
- TCP
- UDP

Apply Changes
Logout
Reboot

Pro series PS410 Management

System status : /system/sysstatus

System information

Device name :	ProSeries
Serial No. :	PS410-20050524J0J
F/W Rev. :	v1.1.0rc317
Current time :	03/02/2000 05:12:04
System logging :	Enable
Send system log by email :	Disable

IP information

IP mode :	Static
IP address :	192.168.4.41
Subnetmask :	255.255.0.0
Gateway :	192.168.1.1
Receive/Transmit errors :	0/268
Primary DNS :	168.126.63.1
Secondary DNS :	168.126.63.2

Copyright 2005 Sena Technologies, Inc. All rights reserved.

図 2-19 PS デバイスサーバーウェブ管理画面

3. ネットワーク設定

3.1 IP 設定

PS シリーズはユーザーのネットワーク環境内で操作するには IP アドレスが必要です。もし IP アドレスがないのであれば、システム管理者に問い合わせ IP アドレスを入手してください。PS デバイスサーバーは、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。

PS 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

PS デバイスサーバーは、最初の時点で STATIC モードに設定されています。固定 IP アドレスは 192.168.161.5 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)

IP configuration : /network/ip/

IP mode	<input type="text" value="static IP"/>
IP address	<input type="text" value="192.168.222.9"/>
Subnet mask	<input type="text" value="255.255.0.0"/>
Default gateway	<input type="text" value="192.168.1.1"/>
Primary DNS	<input type="text" value="168.126.63.1"/>
Secondary DNS (optional)	<input type="text" value="168.126.63.2"/>

Copyright 2005 Sena Technologies, Inc. All rights reserved.

図 3-1 IP 設定

3.1.1. Static(静的)IP アドレスを使用する

Static IP アドレスを使用する際、手動で PS の IP アドレスに関連する全ての設定パラメータを指定する必要があります。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: PS 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固有であり、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 によって割り当てられることはありません。この形態を使用している IP アドレスはプライベート・アドレスとみなされます。PS モデルは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。PS 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、PS 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、他のネットワークにとって門(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。PS 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の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。PS 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に必要な IP 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、配布する能力が

あり、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 アドレスを配布します。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ときに、「リース」のようなコンセプトで行いません。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。

注記: DHCP モードの時は、DNS サーバーを含む PS 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。

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 クライアントがブート時毎に異なる IP アドレスを受け取ることとなります。IP アドレスはユーザーが常に最新の PS モデルの IP アドレスを知ることができるように DHCP サーバー側に保管されます。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 PS サーバーの底面に貼られているラベルステッカーに書かれている MAC アドレスが必要です。

3.2. SNMP 設定

PS 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せん。NMS または SNMP ブラウザのようなネットワーク管理者は PS 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、MIP-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 レシーバー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。

SNMP configuration : /network/snmp/

SNMP enable/disable: Enable ▾

sysContact: administrator

sysName: ProSeries

sysLocation: my location

sysService: 7

PowerOnTrapEnable: Disable ▾

AuthTrapEnable: Disable ▾

LoginTrapEnable: Disable ▾

Configure the access control settings

No.	IP address	Community	Permission
1	0.0.0.0	public	Read Only ▾
2	0.0.0.0	public	Read Only ▾
3	0.0.0.0	public	Read Only ▾
4	0.0.0.0	public	Read Only ▾

Configure the trap receiver settings

No.	IP address	Community	Version
1	0.0.0.0	public	v1 ▾
2	0.0.0.0	public	v1 ▾
3	0.0.0.0	public	v1 ▾
4	0.0.0.0	public	v1 ▾

Save Save & Apply Cancel

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 PS モデルの SNMP エージェントによって使用された認証失敗トラップを設定します。各機能の簡単な説明を以下に挙げます。

- sysContact: PS 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、PS モデルはアプリケーション (7) サービスレベルです。
- EnablePoweronTraps: 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。

- EnableAuthenTrap: SNMP エージェントプロセスが認証失敗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。
- EnableLoginTrap: SNMP 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 PS 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 PS 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 PS 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 PS の SNMP エージェントからの重要なイベント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

PS 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 PS デバイスサーバーは 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 PS デバイスサーバーの SNMP エージェントの MIB-II を持つ SNMP ブラウザです。

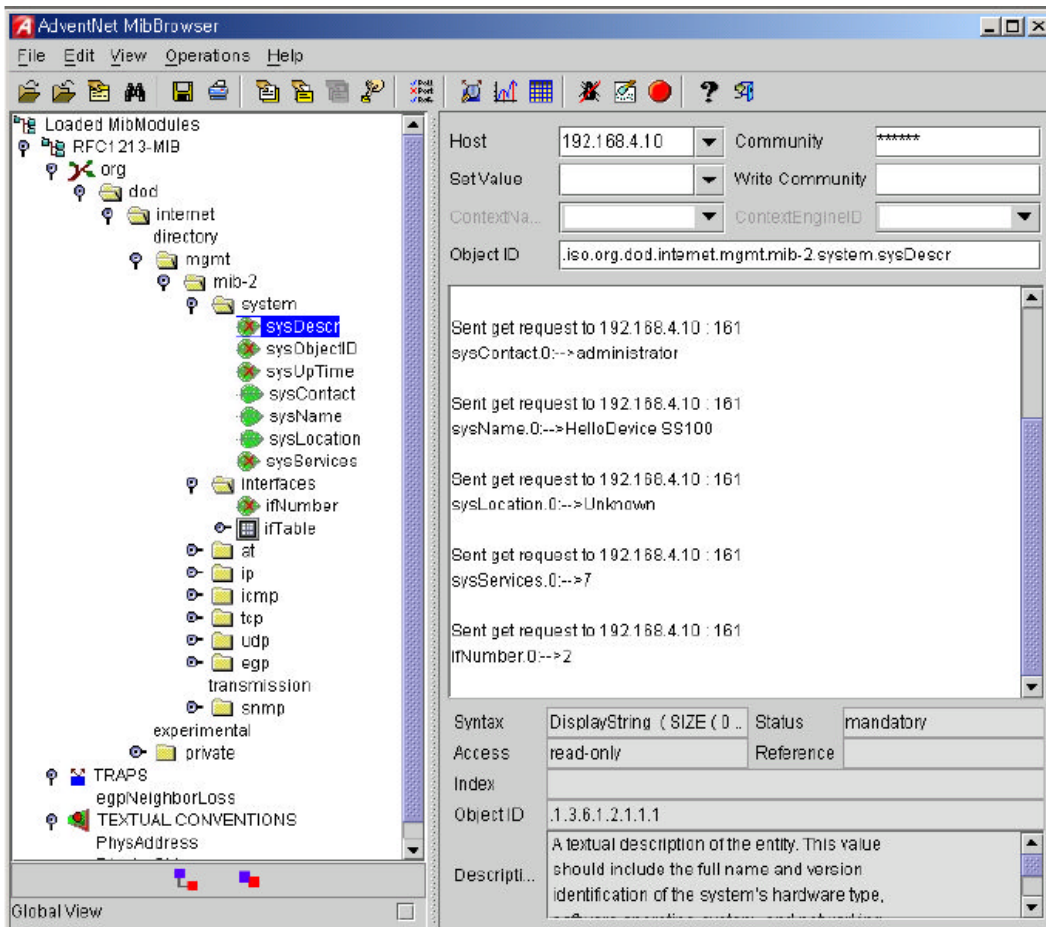


図 3-3 SNMP ブラウザを使用している PS の SNMP エージェントで MIB-II OIDs をブラウズ

3.3 動的 DNS 設定

PS デバイスサーバーで DSL ラインに接続する、もしくは DHCP 設定を行なおうとすると、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 PS デバイスサーバーにアクセス可能になります。

デフォルト値では、PS デバイスサーバーは 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 PS デバイスサーバー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。

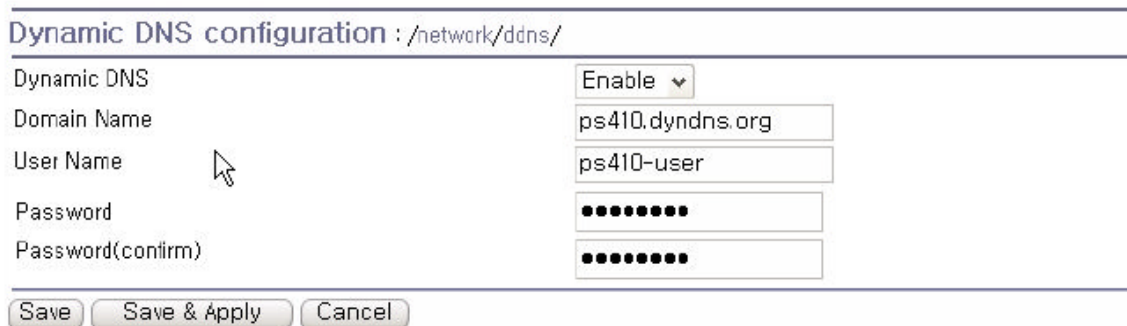


図 3-4 動的 DNS 設定画面

3.4. SMTP 設定

PS 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。PS 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 サーバーの IP アドレス
- SMTP ユーザー名
- SMTP ユーザーパスワード
- 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。

SMTP configuration : /network/smtp/

SMTP	Enable ▾
SMTP server	smtp.yourcompany.com
Mode	SMTP with authentication ▾
Account Name	admin
Password	●●●●
Password(confirm)	●●●●
E-Mail	PS410@yourcompany.c

Save Save & Apply Cancel

Copyright 2005 Sena Technologies, Inc. All rights reserved.

図 3-5 SMTP 設定画面

SMTP configuration : /network/smtp/

SMTP	Enable ▾
SMTP server	smtp.yourcompany.com
Mode	SMTP with authentication ▾
Account Name	POP before SMTP SMTP without authentication SMTP with authentication
Password	
Password(confirm)	●●●●
E-Mail	PS410@yourcompany.c

Save Save & Apply Cancel

Copyright 2005 Sena Technologies, Inc. All rights reserved.

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

PS デバイスサーバーは、フィルタリング方式を用いて IP アドレスを使用するの無許可アクセスから守ります。パラメータ設定を変更することにより次の動作を設定することができます。

- Any host cannot access a specific service of the Pro Series
(指定した PS デバイスサーバーにはどのホストもアクセスできない)。
- Only one host of a specific IP address can access a specific service of the Pro Series

(指定した PS デバイスサーバーには特定の 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 PS デバイスサーバーにアクセス可)
- Any host can access a specific service of the Pro Series
(全てのホストはどの PS デバイスサーバーにもアクセス可)

IP フィルタリング機能は Telnet コンソール、SSH コンソール、NFS、ウェブサーバー、または各ポートからのアクセスを制御し、ON または OFF にできます。このフィルタリング機能のデフォルト値は、"All services and ports are accessible from any host"(全てのホストはどの PS デバイスサーバーにもアクセス可)です。

IP フィルタリング設定のそれぞれのパラメータの意味は以下に挙げます。

- Interface (インターフェース)

IP フィルタリングのルールを PS デバイスサーバーの着信パケットに適用します。このパラメータは変更されません。eth0(Read-Only)

- Option and IP address/mask

ネットワーク上のホストの特定の範囲を説明するための入力フィールドです。1 つのまたは複数のホストが PS デバイスサーバーへのアクセスを許可することができます。ユーザーは IP アドレスまたはアクセスのサブネットを入力する必要があります。リモートホストは PS デバイスサーバーにアクセスするためには、指定したサブネットの範囲にとどまっている必要があります。指定したホストに PS デバイスサーバーへのアクセス許可を与えるには、その指定したホストの IP アドレスを入力し、Normal Option で 255.255.255.255 のサブネットを割り当てます。全てのホストからのアクセスを許可する場合は、IP アドレスおよびサブネットに 0.0.0.0 を割り当てます。

表 3-2 を参照してください。

- Service

IP フィルタリングルールに適用されるサービスです。Telnet, SSH, NFS, HTTP, HTTPS または each serial port を選択してください。

- Chain rule

ホストが Accept, Drop, Reject のどれかで PS デバイスサーバーにアクセスするかどうかを決める基本ルールです。

IP filtering configuration : /network/filter/

IP filtering policy

Policy Reject ▼

IP filtering list

No.	Interface	Option	IP address/mask	Service	Chain rule
Nothing					
NEW	eth0 ▼	Normal ▼	<input type="text"/>	NFS ▼	DROP ▼ ADD

Service

NFS	Drop all ▼
Telnet console	Accept all ▼
SSH console	Drop all ▼
HTTP	Accept all ▼
HTTPS	Accept all ▼
Port 1	Accept all ▼
Port 2	Accept all ▼
Port 3	Accept all ▼
Port 4	Accept all ▼

Save Save & Apply Cancel

図 3-7 IP フィルタリング設定画面

PS デバイスサーバーには Policy オプションがあります。この Policy は IP フィルタリングリスト上にないパケットが入ってきた時に、どのように処理するかを決めます。例えば、まだ IP フィルタリングリストが作成されておらず、全てのサービスが”Accept All”になっている場合、PS デバイスサーバーの Policy が DROP または REJECT に設定されると、全てのパケットに応答しなくなります。

IP filtering policy

Policy Accept ▼

図 3-8 IP Filtering Policy

全てのホストからの特定のサービスまたはシリアルポートをブロックするもっと簡単な設定方法もあります。Service オプションで全てのサービスに Drop all,または Reject all を選択すると、ネットワークからの全てのアクセスをブロックします。

Service

NFS	Drop all ▼
Telnet console	Accept all ▼
SSH console	Drop all ▼
HTTP	Accept all ▼
HTTPS	Accept all ▼
Port 1	Accept all ▼
Port 2	Accept all ▼
Port 3	Accept all ▼
Port 4	Accept all ▼

図 3-9 各サービスおよびシリアルポートのための IP フィルタリング設定画面

表 3-2 オプションおよび IP アドレス/マスクの組み合わせの一覧表

許可可能なホスト	入力フォーマット	オプション
	IP アドレス/マスク	
全てのホスト	0.0.0.0/0.0.0.0	Normal
192.168.1.120 以外のホスト	192.168.1.120/255.255.255.255	Normal
192.168.1.1～ 192.168.1.254	192.168.1.120/255.255.255.255	Invert
192.168.0.1～ 192.168.255.254	192.168.1.0/255.255.255.0	Normal
192.168.1.1～ 192.168.1.126	192.168.0.0/255.255.0.0	Normal
192.168.1.129～ 192.168.1.254	192.168.1.128/255.255.255.128	Normal
なし	0.0.0.0/0.0.0.0	Invert

3.6. SYSLOG サーバー設定

PS デバイスサーバーシリーズは、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 3-10 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。

SYSLOG configuration : /network/syslog/

SYSLOG server service

SYSLOG server IP address

SYSLOG facility

Copyright 2005 Sena Technologies, Inc. All rights reserved.

図 3-10 SYSLOG サーバー設定

PS デバイスサーバー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ウォールの設定を変更してください。

PS デバイスサーバーは 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 PS デバイスサーバー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する詳細は 4.2.8. ポートロギングおよび 5.2. システムロギングを参照してください。

3.7. Locating Server

3.7.1. 概要

PS デバイスサーバーをサーバー(TCP または UDP)として機能させたいのであれば、クライアント側のホストは PS デバイスサーバーの IP アドレスを知る必要があります。しかし DHCP のような任意に PS デバイスサーバーに IP アドレスを割り当てるような環境下では、常に現行の IP アドレス情報を知るための手段が必要となります。この問題を解決するために、PS デバイスサーバーは、Locating Server と呼ばれる場所に、毎回 IP アドレスが新しく割り当てるたびにその情報を送信するように設定することができます。locating Server として特定のホストを操作するか、クライアントホストを Locating Serer として同時に操作することが可能です。

Locating Server を実装するための特別のライブラリまたはツールキットは現在ありません。

詳細情報に関しては弊社技術サポートまでご連絡ください。(info@intersolutionmarketing.com)

3.7.2. Locating Server の設定

Locating Server 画面を図 3-11 に表わします。Locating Server IP アドレス、Locating Server UDP ポート番号、および接続時間間隔と Locatin Server 機能の ON・OFF を選択および入力する必要があります。デフォルト値は OFF です。

Locating server configuration : /network/locserver/	
Locating server service	Enable <input type="button" value="v"/>
Locating server IP address	<input type="text" value="192.168.0.8"/>
Port	<input type="text" value="9000"/>
Locating server Interval (second)	<input type="text" value="30"/>
<input type="button" value="Save"/> <input type="button" value="Save & Apply"/> <input type="button" value="Cancel"/>	

図 3-11 Locating Server 設定画面

3.7.3. Locating Server 通信プロトコル

PS デバイスサーバーが IP アドレス情報を Locating Server に送信するときのフォーマットを以下の表に記載します。

Description	Magic Cookie	Data(0)	Data(1)	...	Data(n)
Bytes	4	Variable	Variable		Variable
Value	F1-AA-AA-BC				

Data(n) format

Description	Data ID	Length	Data
Bytes	1	1	Variable
Value	1~6	Variable	Variable

Data ID

ID	Description	Length
1	Device name	var
2	Model name	var
3	Serial number	var
4	MAC address	6
5	IP address	4
6	Local ports*	1 or 4 or 8

注記:

ローカルポート: 各2バイトデータは対応するシリアルポートの現行ローカルポート設定を表わしています。PS110のローカルポートのデータ長は2バイトであり、PS410およびPS810のデータ長はそれぞれ8バイトおよび16バイトです。設定した各シリアルポートのローカルTCP(UDP)ポート番号は順番に振る必要があります。例えばTCP/UDPポート番号が7000番台ならば最初が7001になります。シリアルポートがOFFになると、そのローカルポートのローカルポート番号は0とみなされます。

PS110の例:

ポート番号が7001(1B59h)の場合、ローカルポートデータは1Bh, 59h

そのポートがOFFの場合、00h, 00h

PS410の例:

Port1=7001(1B59h), Port2=7010(1B62h), Port3=Disable, Port4=7004(1B5Ch)

ローカルポートデータ=1Bh,59h, 1Bh,62h, 00h, 00h, 1Bh,5Ch

3.8. NFS サーバー設定

PS デバイスサーバーは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。

NFS configuration : /network/nfs/

NFS server service	Enable ▾
NFS server IP address	192.168.1.1
Mounting path on NFS server	/
NFS Timeout (sec, 5-3600)	5
NFS mount retrying interval (sec, 5-3600)	5

Save Save & Apply Cancel

Copyright 2010 Sana Technologies, Inc. All rights reserved.

図 3-12 NFS サーバー設定画面

PS デバイスサーバーのログデータを 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 4.2.8 ポートロギング、および 5.2.システムロギングを参照してください。

3.9. 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、PS デバイスサーバーには TCP Keep Alive 機能があります。PS デバイスサーバー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。

PS デバイスサーバーの 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 PS デバイスサーバー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。

TCP configuration : /network/tcp/

TCP keepalive time	<input type="text" value="15"/>
TCP keepalive probes	<input type="text" value="3"/>
TCP keepalive intervals	<input type="text" value="5"/>

Copyright 2005 Sena Technologies, Inc. All rights reserved.

図 3-13 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の設定を行なうことができます。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:**

PS デバイスサーバーは 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。

PS デバイスサーバー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。

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 または NFS サーバーのストレージに転送されます。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します。これは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 を使用することにより、OFF にした際にすべてのデータが消失してしまうことと避けることができます。NFS サーバーでシリアルポートログデータを保存してください。

シリアルポートはひとつずつ、または全て同時に行なうことが可能です。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一覧

全シリアルポート設定 または 個別シリアルポート設定 #1～#8(1/4)	ポート ON/OFF			
	ポートタイトル			
	ホストモード	TCP	ポート番号	
			ユーザー認証	
			telnet サポート	
			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)	
			ソケット ID (発信接続用)	
			TCP Nagle algorithm ON/OFF	
		UDP	ポート番号	
			最大接続数	
			非アクティブタイムアウト(0=無制限)	
			ソケット ID (発信接続用)	
			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		
			ホスト IP アドレス	
			ホストポート	
			ホスト IP アドレスのバックアップ	
			ホストポートのバックアップ	
			リモートホストの削除	
	暗号化	SSLv3		
		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		
		インターキヤラクタ・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			
	モデム接続の自動リリース			
	ポートロギング	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サイズ		
		ポートログの表示		
ポートイベント操作	Email 通知	Email 通知の ON/OFF		
		Email の題		
		宛て先の Email アドレス		
	SNMP 通知	SNMP 通知の ON/OFF		
		SNMP トラップの目標		
		SNMP トラップ受け取り側の IP アドレス		
		SNMP トラップコミュニティ		
		SNMP トラップバージョン		
	イベント・キーワードの追加・編集			
	イベント・キーワード			
	Email 通知			
	SNMP トラップ通知			
ポートコマンド				
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の番号またはタイトルをクリックするとそのポートパラメータを設定することができます。

Serial port configuration : /serial/

No.	Title	Mode	Port#	Serial-Settings
1	Port #1	TCP	7001	RS_485 230400 N 8 1 Hardware
2	Port #2	ME	7002	RS_232 9600 N 8 1 None
3	Port #3	UDP	7003	RS_422 2400 N 8 1 None
4	Port #4	----	-----	- - - - -

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

PS デバイスサーバーの各ポート設定は 8 つのカテゴリに分けられます。

1. Port enable/disable
2. Port title
3. Host mode
4. Cryptography
5. Serial port Parameters
6. Modem configuration
7. Port logging
8. Port event handling

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。

Serial port configuration - 1 : /serial/*1/

Enable/Disable this port ▾

Port title

Host mode configuration

Serial port parameters

Port logging configuration

Port event handling configuration

Copy port configuration

図 4-2 Serial port enable/disable 画面

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もとづいた説明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。

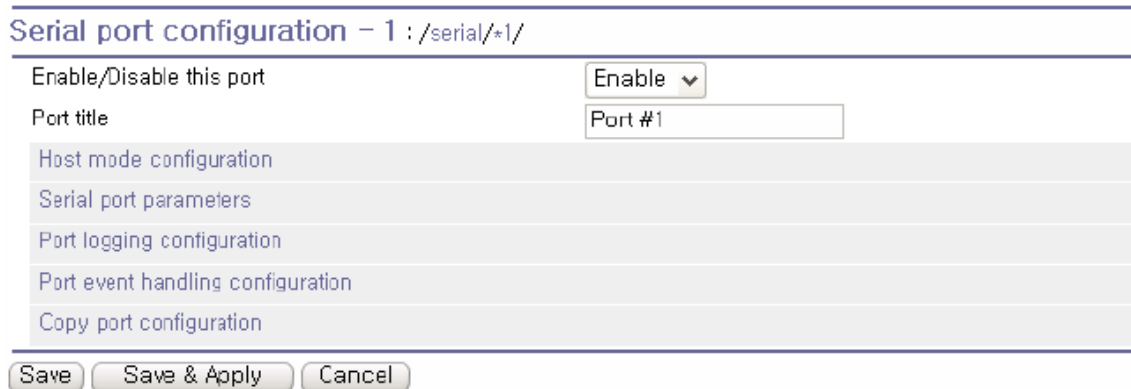


図 4-3 ポートタイトル設定

4.2.3. Host Mode Configuration

PS デバイスサーバー操作モードは”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

PS デバイスサーバーは 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。

Host mode configuration : /serial/*/hostmode/

Enable/Disable this port	Enable <input type="button" value="v"/>
Port title	<input type="text" value="Port #1"/>

Host mode configuration

Host mode	TCP <input type="button" value="v"/>
Port number (1024-65535, 0 for only outgoing connections)	<input type="text" value="7001"/>
User authentication	Disable <input type="button" value="v"/>
Telnet support	Disable <input type="button" value="v"/>
Max. allowed connection (1-8)	<input type="text" value="8"/>
Cyclic connection (sec, 0 : disable)	<input type="text" value="0"/>
Inactivity timeout (sec, 0 : unlimited)	<input type="text" value="100"/>
Socket ID (for outgoing connection)	<input type="text"/>
TCP Nagle algorithm Enable/Disable	Disable <input type="button" value="v"/>

Remote host

Cryptography configuration

Modem configuration

Serial port parameters

Port logging configuration

Port event handling configuration

Copy port configuration

図 4-4 ホストモード設定画面(TCP モード)

4.2.3.1. 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 PS デバイスサーバー間の通信が終了すると、リモートホストまたは PS デバイスサーバー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[Sync-Received]状態へと変わり

まず、PS デバイスサーバーが接続を許可すると、[Sync-Received]から[established]に変わります。

[Sync-sent]

PS デバイスサーバー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PS デバイスサーバー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。

PS デバイスサーバーは、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。PS デバイスサーバー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 PS デバイスサーバー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 PS デバイスサーバーのシリアルポートバッファ内に蓄積されます。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、PS デバイスサーバー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、PS 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。PS デバイスサーバーも 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。詳細情報にかんしては 5.9.ユーザー認証機能をご参照ください。

Telnet Protocol (telnet プロトコル)

TCP モードでは、PS デバイスサーバーは 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、PS デバイスサーバー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。PS デバイスサーバー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、PS デバイスサーバーとシリアル IP を参照してください)。

Max. allowed connection (最大接続数)

PS デバイスサーバーは最大 8 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 4.2.4. 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、PS デバイスサーバーは、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、PS 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できるようになるので、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 4-5 は TCP モードの状態変移ダイアグラムです。

Socket ID

たくさんの PS デバイスが同じリモートホストに接続する場合、デバイスを認識することが大切です。そのような場合に、Socket ID は各デバイスの ID を作成するために用います。PS デバイスサーバー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 Algorithm として知られる機能があります。これは小さな要領の大量のパケットの送信を防ぐようになります。これはインターネットから大量のパケット送信を防ぐようになります。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。TCP Nagle algorithm 機能は ON・OFF にすることができます。

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 PS デバイスサーバー間の接続が自動的に切断されます。

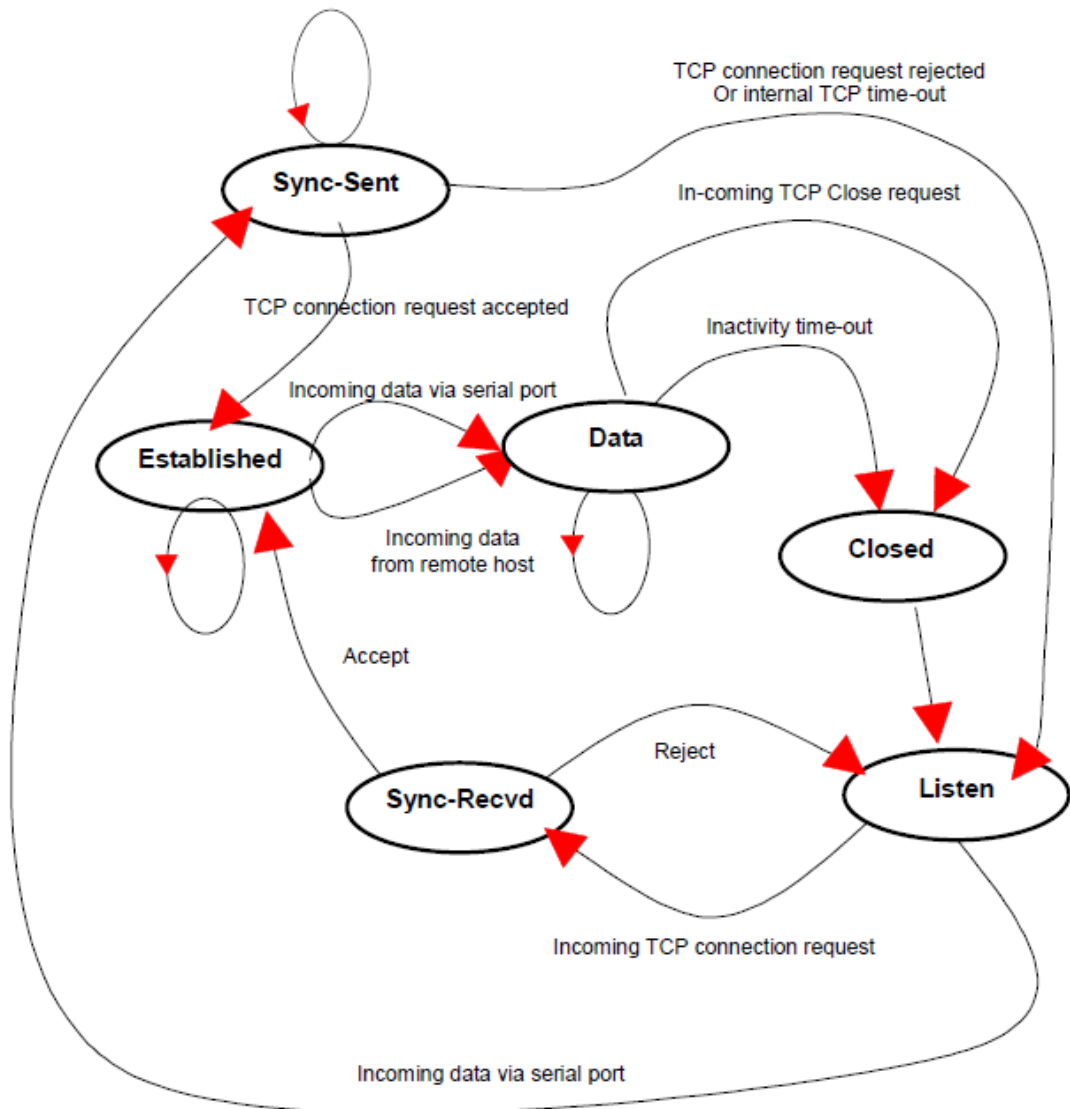


図 4-5 TCP モードの状態変移ダイアグラム

4.2.3.2. 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。PS デバイスサーバーは事前に設定したり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。

Host mode configuration : /serial/+1/hostmode/

Enable/Disable this port	Enable <input type="button" value="v"/>
Port title	Port #1 <input type="text"/>
Host mode configuration	
Host mode	UDP <input type="button" value="v"/>
Port number (1024-65535, 0 for only outgoing connections)	7001 <input type="text"/>
Max, allowed connection (1-8)	8 <input type="text"/>
Inactivity timeout (sec, 10-3600)	100 <input type="text"/>
Socket ID (for outgoing connection)	<input type="text"/>
Accept unlisted	Yes <input type="button" value="v"/>
Send unlisted	Yes <input type="button" value="v"/>
Remote host <input type="text"/>	
Serial port parameters	
Port logging configuration	
Port event handling configuration	
Copy port configuration	

図 4-6 ホストモード設定(UDPmode)

1) 操作方法

リモートホストが UDP データグラムを PS デバイスサーバーの UDP ローカルポートの一つに送信すると、PS デバイスサーバー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、PS デバイスサーバー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、PS デバイスサーバーはデータを転送しません。

2) パラメータ

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 4.2.3.1.の TCPmode パラメータを参照してください。

最大接続可能数

TCP 通信とコンセプトは同じです。4.2.3.1.の 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、PS デバイスサーバーは 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、PS デバイスサーバーは 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、PS デバイスサーバー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 PS 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。PS デバイスサーバーは 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 PS 間でのデータのやりとりがない場合、PS デバイスサーバーは、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、PS デバイスサーバー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 PS デバイスサーバー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。PS デバイスサーバー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。

4.2.3.3. 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、シリアルポートがシリアルデバイスにモデムがついているかのように作業が行われます。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、PS デバイスサーバー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。

PS デバイスサーバーの 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、PS デバイスサーバー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 PS デバイスサーバーでサポートされている AT コマンド一覧

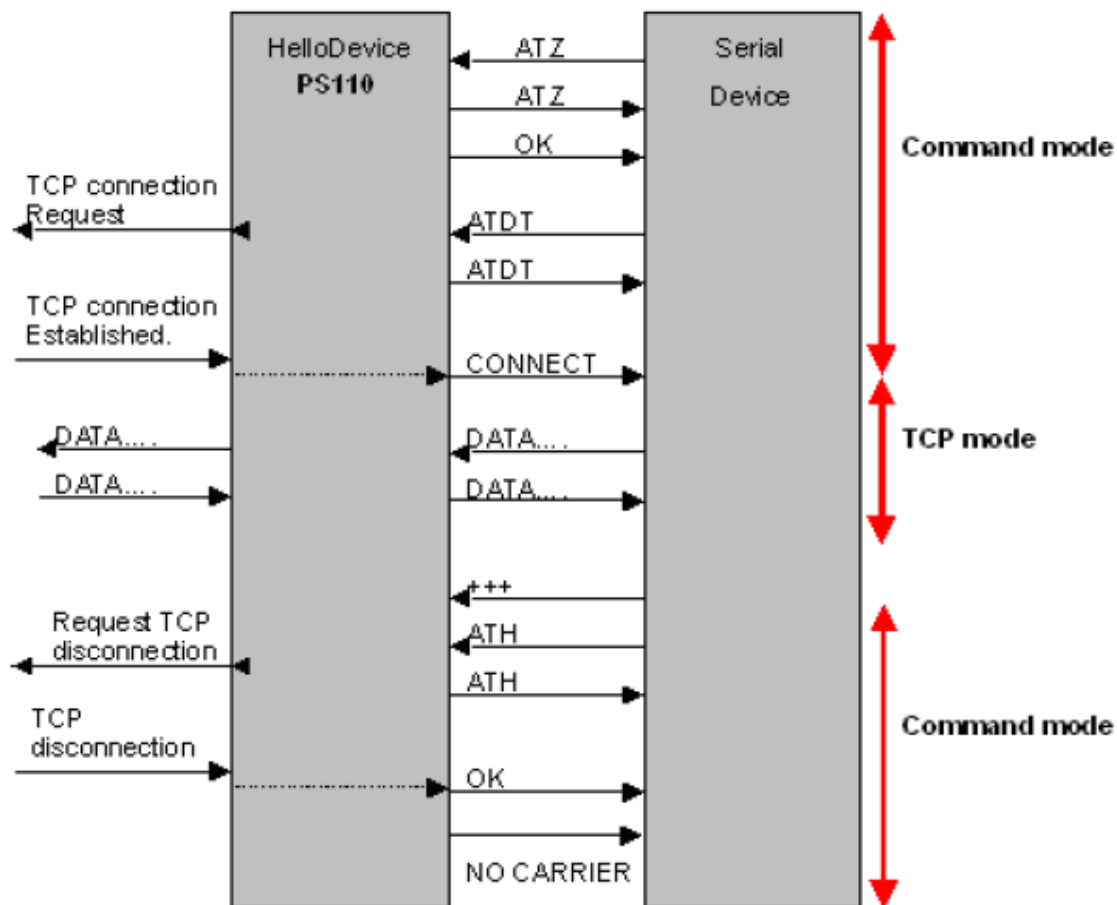


図 4-7 modem emulation mode での典型的なコマンド・データの流れ図

2) パラメータ

Phone number to host address mapping table(ホストアドレスマッピングテーブルへ電話番号)

Modem emulation mode では、指定した電話番号をホストアドレスまたはポートマッピングテーブルに設定することができます。図 4-8 に示されているように電話番号をホストアドレスまたはポートマッピングテーブルに指定すると PS デバイスサーバーは modem emulation mode で 'atdt25737772' コマンドにより 192.168.0.100 のポート 6001 番に接続試行を行います。

CONNECT string in non-verbose mode(ATV0)および CONNECT string in verbose mode (ATV1) (非冗長(non-verbose)モード(ATV0)の CONNECT スtringおよび冗長モード(ATV1)の CONNECT スtring)

Modem emulation mode では、PS デバイスサーバーは表 4-3 のリザルトコードに基づき、AT コマンドで応答します。しかし状況に応じてデバイスはリモートホスト接続のために異なる応答コードが必要になる場合もあります。たとえば、PS デバイスサーバーがリモートホストと接続するとき、“1” (ATV0 コマンドが設定のとき)または CONNECT(ATV1 コマンドが設定のとき)リザルトコードが応答されます。しかし 12(ATV0)または CONNECT9600(ATV1) 応答が必要な場合、図 4-8 にあるように CONNECT スtringsを設定することができます。

Respond to AT&CN, AT&Wn, AT&Zn

以下の 3 種類の AT コマンド

AT&CN, AT&Wn, AT&Zn はユーザーが OK または ERROR の一つを応答として選択可能です。

Command echo delay(ms) (コマンドエコー遅延)

ユーザーによって入力された AT コマンドはこのメニューで指定した遅延でエコーします。これは RS485 モードの modem emulation mode のときに有効です。

Default command echo(デフォルトコマンドエコー)

このメニューにてユーザーが入力した AT コマンドのエコーを On/Off にできます。

Default data mode

Raw TCPmode または Telnet binary mode のどちらかを選択します。Raw TCP は TCP プロトコルではアプリケーションプロトコルのない状態です。Telnet binary mode は TCP プロトコルを Telnet プロトコルで使用する状態です。Telnet binary mode は RFC2217 で定められた Telnet COM port control option をサポートします。RFC2217 と互換性のある COMportRedirector でこのオプションを選択すると、Hyperterminal 等のターミナルソフトウェアを使って PS デバイスサーバーのシリアルポートパラメータを制御することができます。

Host mode configuration : /serial/*1/hostmode/

Enable/Disable this port Enable ▾

Port title Port #1

Host mode configuration

Host mode Modem emulation ▾

Phone number to host address mapping table

CONNECT string in non-verbose mode(ATV0) 1

CONNECT string in verbose mode(ATV1) CONNECT

Respond to AT&Cn with ERROR ▾

Respond to AT&Wn with ERROR ▾

Respond to AT&Zn with ERROR ▾

Command echo delay (ms) 0

Default command echo Enable ▾

Default data mode Raw TCP ▾

Cryptography configuration

Serial port parameters

Port logging configuration

Port event handling configuration

Copy port configuration

Save Save & Apply Cancel

図 4-8 ホストモード設定画面 (Modem emulation mode)

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

Remote Host Configuration は PS デバイスサーバーのシリアルポートからデータ送信がある時に PS デバイスサーバー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 PS デバイスサーバーがプライマリ・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は 4 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・リモートホストを備える必要がないからです。図 4-9 にはウェブインターフェースによる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。

Remote host : /serial/*1/hostmode/remotehost/

Enable/Disable this port

Port title

Host mode configuration

Host mode

Port number (1024-65535, 0 for only outgoing connections)

User authentication

Telnet support

Max. allowed connection (1-8)

Cyclic connection (sec. 0 : disable)

Inactivity timeout (sec. 0 : unlimited)

Socket ID (for outgoing connection)

TCP Nagle algorithm Enable/Disable

Remote host

No.	Host address	Host port number	Backup host address	Backup port	
1	<input type="text" value="192.168.100.1"/>	<input type="text" value="7001"/>	<input type="text" value="192.168.100.1"/>	<input type="text" value="7002"/>	<input type="button" value="REMOVE"/>
2	<input type="text" value="192.168.100.2"/>	<input type="text" value="7001"/>	<input type="text" value="192.168.100.2"/>	<input type="text" value="7002"/>	<input type="button" value="REMOVE"/>
3	<input type="text" value="remote.domain.com"/>	<input type="text" value="6001"/>	<input type="text" value="remote.domain.com"/>	<input type="text" value="6002"/>	<input type="button" value="REMOVE"/>
NEW	<input type="text" value="192.168.100.3"/>	<input type="text" value="7001"/>	<input type="text" value="192.168.100.3"/>	<input type="text" value="7002"/>	<input type="button" value="ADD"/>

Cryptography configuration

Modem configuration

Serial port parameters

Port logging configuration

Port event handling configuration

Copy port configuration

図 4-9 リモートホスト設定画面

4.2.5. Cryptography configuration (暗号化の設定)

PS デバイスサーバーは modem emulation mode を含む TCP モードのみで暗号化セッションをサポートしています。

Cryptography configuration : /serial/*1/hostmode/ssl/

Enable/Disable this port

Port title

Host mode configuration

Host mode

Port number (1024-65535, 0 for only outgoing connections)

User authentication

Telnet support

Max. allowed connection (1-8)

Cyclic connection (sec, 0 : disable)

Inactivity timeout (sec, 0 : unlimited)

Socket ID (for outgoing connection)

TCP Nagle algorithm Enable/Disable

Remote host

Cryptography configuration

Encryption method

Modem configuration

Serial port parameters

Port logging configuration

Port event handling configuration

Copy port configuration

図 4-10 Cryptography configuration (暗号化設定) 画面

4.2.5.1. SSL (Secure Sockets Layers) 暗号化設定

SSL を設定することにより、PS デバイスサーバー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によって動作します。SSL はセキュアであり、高速で他の Web プロトコルと相性が良いとされています。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 ハンドシェイ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。対称鍵暗号化は公開鍵暗号化よりもより高速ですが、公開鍵暗号化のほうがより認証技術が優れています。ハンドシェイ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。次にハンドシェイ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. ハンドシェイ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(ハンドシェイ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イク特有であり、サーバー、クライアント両方が知っている他の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、データの保水性、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イク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イクが終了したと伝えます。
10. SSL ハンドシェイクは完了し、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、またデータの保水性も確認します。

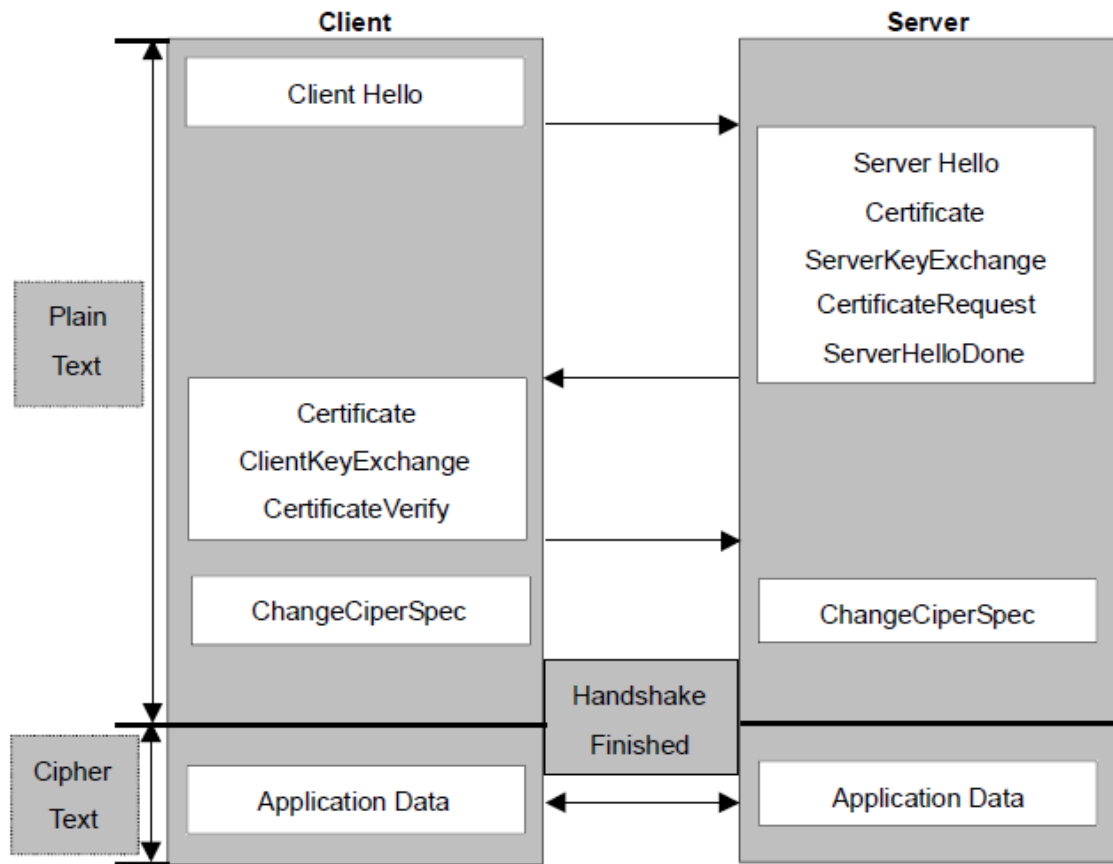


図 4-11 代表的な SSL ハンドシェークの流れ図

PS デバイスサーバーは 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、PS デバイスサーバーは SSL ハンドシェイクプロセス中 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 PS デバイスサーバー側のシリアルポートから開始した場合は、SSL ハンドシェイクプロセス中は SSL クライアントとして動作します。

・ クライアント証明書による認証 (Server mode 専用)

Client Authentication by certificate(クライアント証明書による認証)のオプションを Enable(オン)にすると、PS デバイスサーバーは SSL ハンドシェーキングプロセス中にクライアントの証明書をリクエストします(ステップ2)。それとは対照的に、このオプションを Disable(オフ)にすると、PS デバイスサーバーは SSL ハンドシェーキングプロセス中に証明書をリクエストしません。

4.2.5.1. Upload Certificate (証明書のアップロード)

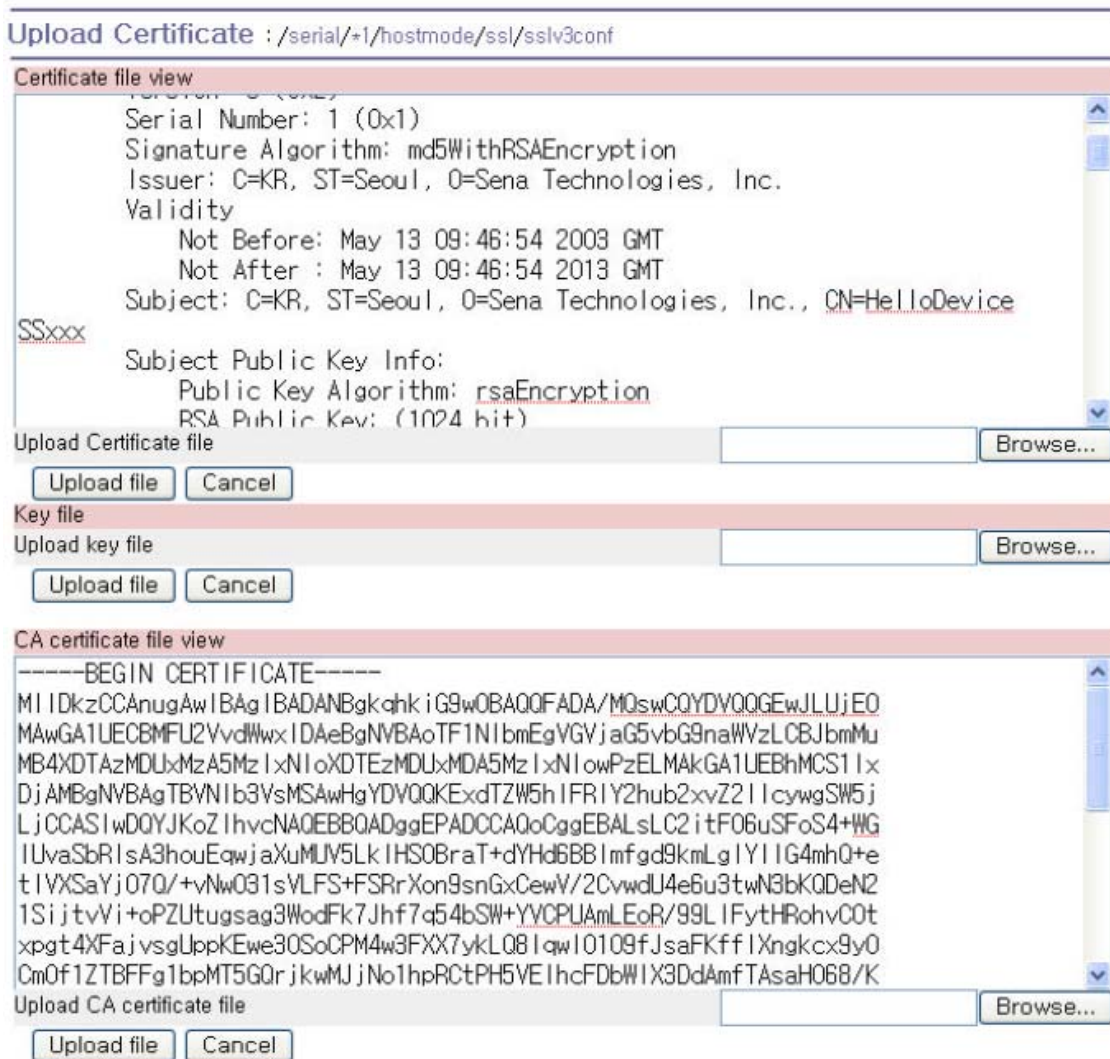


図 4-12 証明書のアップロード画面

ユーザーは証明書、証明書認証、秘密鍵、をアップロードすることができます。それらは PEM フォーマットです。

4.2.5.2. RC4 暗号化メソッド

RC4 暗号化モードでは、PS デバイスサーバー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。PS デバイスサーバー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 PS デバイスサーバーと通信することができます。

SSL/RC4 暗号化メソッドのサンプルアプリケーションプログラムにかんしては、弊社技術サポートにお問い合わせください。(support@intersolutionmarketing.com)

Cryptography configuration : /serial/+1/hostmode/ssl/

Enable/Disable this port ▾

Port title

Host mode configuration

Host mode ▾

Port number (1024-65535, 0 for only outgoing connections)

User authentication ▾

Telnet support ▾

Max. allowed connection (1-8)

Cyclic connection (sec, 0 : disable)

Inactivity timeout (sec, 0 : unlimited)

Socket ID (for outgoing connection)

TCP Nagle algorithm Enable/Disable ▾

Remote host

Cryptography configuration

Encryption method ▾

Key string

Modem configuration

Serial port parameters

Port logging configuration

Port event handling configuration

Copy port configuration

図 4-13 RC4 暗号化設定画面

4.2.6. シリアルポートパラメータ

シリアルデバイスをPS デバイスサーバーのシリアルポートに接続するには、PS デバイスサーバー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。この時に必要となるパラメータ値は、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ー・タイムアウトです。

- **UART type**

最初に、PS サーバーとシリアルデバイスの双方は、シリアル通信タイプにおいて一致している必要があります。RS232, RS422(RS485 全二重), RS485(半二重)モードがあります。PS110/410 の場合には、シリアルポート付近にある DIP スイッチでシリアル通信タイプを選択可能です。シリアル通信タイプを変更するには、図 4-14 にあるように DIP スイッチを移動させることにより変更できます。PS810 に関しては、図 4-17 に示されているようにシリアル通信タイプを設定メニューより変更できます。

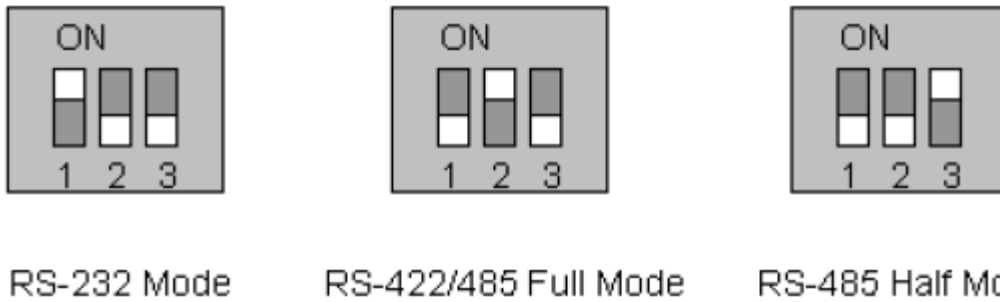


図 4-14 DIP スイッチによるシリアル通信設定の変更(PS110/410 用)

シリアルポートのピン配置および配線ダイアグラムに関する詳細情報は、付録 1 の接続セクションを参照してください。

注記:

1. PS110/410 の DIP スイッチに位置を変更するときには、必ず PS デバイスサーバーの電源を OFF にしてから行ってください。電源を ON にしたまま DIP スイッチを変更すると、故障や不具合の原因となることがあります。(DIP スイッチの位置が間違っている場合、図 4-15 にあるように UI 上の UART タイプが“invalid”と表示されシリアルポートとの通信ができません)。
2. PS810 の場合、設定ソフトウェアを通してのみ UART タイプを変更可能です。PS810 は UART タイプを変更する DIP スイッチがありません。

Serial port configuration : /serial/

No.	Title	Mode	Port#	Serial-Settings
1	Port #1	TCP	7001	RS_485 9600 N 8 1 None
2	Port #2	TCP	7002	RS_485 9600 N 8 1 None
3	Port #3	TCP	7003	RS_232 9600 N 8 1 None
4	Port #4	ME	7004	Invalid 9600 N 8 1 None

図 4-15 Serial port configuration(シリアルポート設定)のメイン画面に表示された invalid(有効でない)UART タイプ設定の場合

• Baud rate

PS デバイスサーバー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。

• 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。

Serial port parameters : /serial/+1/parameter/

Enable/Disable this port

Port title

Host mode configuration

Serial port parameters

UART type

Baudrate

Data bit

Stop bit

Parity bit

Flowcontrol

Inter character time-out (0-10000 msec)

DTR option

DSR behavior

Port logging configuration

Port event handling configuration

Copy port configuration

図 4-16 シリアルパラメータ設定(PS110/410)

Serial port parameters : /serial/+1/parameter/

Enable/Disable this port

Port title

Host mode configuration

Serial port parameters

UART type

Baudrate

Data bit

Stop bit

Parity bit

Flowcontrol

Inter character time-out (0-10000 msec)

DTR option

DSR behavior

Port logging configuration

Port event handling configuration

Copy port configuration

図 4-17 シリアルパラメータ設定画面(PS810)

- **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。

注記: フロー制御は RS232 および RS422 モードのみサポートしています。RS485 モードはフロー制御をサポートしていません。

- **DTR/DSR behavior**

DTR/DSR ピンの目的は、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 接続状態を制御するためにあります。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。

PS デバイスサーバー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、PS デバイスサーバーの TCP/UDP 接続を制御することができます。

注記:

1. 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。
2. DTR/DSR は RS422 および RS485 モードのときは有効ではありません。

- **Inter-Character timeout**

このパラメータは PS デバイスサーバー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、PS デバイスサーバーは内部バッファにデータを蓄積します。PS デバイスサーバー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： $10\text{bit}/1200(\text{bits/s}) * 1000(\text{ms/s}) = 8.3\text{ms}$ 。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。

4.2.7. モデムの設定 (Modem configuration)

PS デバイスサーバー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。PS デバイスサーバーはホストモードが 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、PS デバイスサーバー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 PS デバイスサーバーは 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、PS デバイスサーバー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、PS デバイスサーバーは 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 PS デバイスサーバー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。

Modem configuration : /serial/*1/hostmode/modem/

Enable/Disable this port ▾

Port title

Host mode configuration

Host mode ▾

Port number (1024-65535, 0 for only outgoing connections)

User authentication ▾

Telnet support ▾

Max. allowed connection (1-8)

Cyclic connection (sec, 0 : disable)

Inactivity timeout (sec, 0 : unlimited)

Socket ID (for outgoing connection)

TCP Nagle algorithm Enable/Disable ▾

Remote host

Cryptography configuration

Modem configuration

Enable/Disable modem ▾

Modem init-string

DCD behavior ▾

Automatic release modem connection ▾

Serial port parameters

Port logging configuration

Port event handling configuration

Copy port configuration

図 4-18 Modem Configuration 画面

4.2.8. 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 MEMORY または NES 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 PS デバイスサーバーの内部メモリまたは 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 PS デバイスサーバー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 NFS サーバーに指定します。まず NFS サーバーを設定する必要があります。NFS サーバーの設定方法は 3.8. NFS サーバー設定を参照してください。

- **Port log buffer size(ポートログのバッファサイズ)**

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 10Kbyte です。

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に設定してください。

図 4-19 ポートロギング設定画面

4.2.9. Port イベントの操作設定

PS デバイスサーバーは、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したり、データを監視することが可能になります。PS デバイスサーバーとシリアルデバイス間の接続ステータスおよび PS デバイスサーバーとリモートホスト間の TCP 接続ステータスも同様にモニタ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 PS デバイスサーバー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。PS デバイスサーバー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)**

PS デバイスサーバー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かったり、またはオフであれば、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。

- **Subject 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題名を指定します。

- **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 trap notification (SNMPトラップ通知)**

このパラメータは PS デバイスサーバーの SNMP トラップ通知をオンまたはオフにします。

- **Subject 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 PS デバイスサーバー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's IP address**

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。

Event keywords : /serial/*1/event/port_event_Lkeyword/

Enable/Disable this port ▾

Port title

Host mode configuration

Serial port parameters

Port logging configuration

Port event handling configuration

Enable/Disable port event handling ▾

Enable/Disable E-mail notification ▾

Subject of E-mail

Recipient's E-mail address

Enable/Disable SNMP notification ▾

Subject of SNMP trap

SNMP trap receiver's IP address

SNMP trap community

SNMP trap version ▾

Notification interval

Event keywords

No.	Event keyword	E-mail notification	SNMP trap notification	Port command	
1	<input type="text" value="keyword"/>	<input type="button" value="Disable"/> ▾	<input type="button" value="Disable"/> ▾	<input type="text" value="reaction"/>	<input type="button" value="REMOVE"/>
NEW	<input type="text"/>	<input type="button" value="Disable"/> ▾	<input type="button" value="Disable"/> ▾	<input type="text"/>	<input type="button" value="ADD"/>

Copy port configuration

図 4-20 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。

Event keywords(イベント・キーワード)

イベント・キーワードを割り当てることにより、PS デバイスサーバーはシリアルポートでそのキーワードを検知するとすぐにメール通知を送信したり、SNMPトラップ通知を送信したり、事前に設定したコマンドをシリアルポートに送信します。

- **Event Keyword(イベント・キーワード)**
キーワードとしてどのような単語も設定可能です。
- **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)**
PS デバイスサーバー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。

4.2.10. Copy port Configuration (ポート設定をコピーする)

作成したポート設定を他のポートの設定にコピーすることができます。2 種類の方法があります。“Copy current port configuration to”でポートを指定する方法と、“Copy current port configuration from”で指定するポートです。

注記: Port Title, TCP ポート番号、UDP ポート番号はこの機能でコピーすることはできません。

図 4-21 Copy port configuration 画面

5. システム管理(System Administration)

PS デバイスサーバーは 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 PS デバイスサーバーのネットワーク設定が含まれます。PS デバイスサーバーは、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 PS デバイスサーバーのデバイス名、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。

5.1. System Status (システムステータス)

System status : /system/sysstatus

System information	
Device name :	ProSeries
Serial No. :	PS410-20060624JQJ
F/W Rev. :	v1, 1,0
Current time :	03/02/2005 09:43:27
System logging :	Enable
Send system log by email :	Disable
IP information	
IP mode :	Static
IP address :	192,168,4,41
Subnetmask :	255,255,0,0
Gateway :	192,168,1,1
Receive/Transmit errors :	0/134
Primary DNS :	168,126,63,1
Secondary DNS :	168,126,63,2

図 5-1 System Status 画面

5.2. System Logging (システムロギング)

PS デバイスサーバー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。PS デバイスサーバー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 PS デバイスサーバーの内部メモリ、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、PS デバイスサーバー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のサーバー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。

PS デバイスサーバー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します。この機能をオンにするには、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 5-2 は設定およびシステムログ閲覧画面です。

System logging : /system/log/

Enable/Disable system logging	Enable ▾
System log storage location	RAM disk (10 Kbyte) ▾
Enable/Disable E-mail logging	Enable ▾
Number of E-mail Logs	5
Recipient's E-mail Logs	admin@yourcompany.c

System log view

Save Save & Apply Cancel

Copyright 2005 Sena Technologies, Inc. All rights reserved.

図 5-2 システムログ設定および閲覧画面

5.3. Change Password (パスワードの変更)

PS デバイスサーバー、システム管理ユーザー (root ユーザー) 用のパスワードは、このメニューで変更します。このパスワードでシリアルコンソールへのアクセス、telnet/ssh コンソールへアクセスします。(詳細に関しては 5.9 User Administration を参照してください)。

Change password : /system/changepasswd

User	root
Current Password	<input type="password"/>
New Password	<input type="password"/>
Confirm Password	<input type="password"/>

Change

Figure 5-3 Changing the password

図 5-3 Change Password 画面

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

PS デバイスサーバーは管理することを踏まえ、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。

Device Name : /system/device_name/

Device Name

Copyright 2005 Sena Technologies, Inc. All rights reserved.

図 5-4 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。

5.5. 日付および時刻の設定

PS デバイスサーバーは現在の時刻および日付を表示します。PS410 および PS810 の時間およびカレンダー設定は内部バッテリー電源によりバックアップされます。(PS110 は内部バッテリーを持っておらず、リブート時にすべて日付と時刻はリセットされます。現行の時間を保つために NTP サーバーを使用することを推奨します。) 図 5-5 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。

Date and time : /system/date_time/

Use NTP

Date [mm/dd/yyyy]

Time [hh:mm:ss]

図 5-5 日付および時間設定画面

図 5-6 に示されているように、PS デバイスサーバーは 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 サーバーが 0.0.0.0 に設定されているならば、PS デバイスサーバーはデフォルト NTP サーバーを使用します。この場合、PS デバイスサーバーはネットワークからインターネットにつないでいる必要があります。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。

Date and time : /system/date_time/

Use NTP

NTP server (0.0.0.0 for Auto)

Time offset from UTC (UTC + [x.x]hours)

図 5-6 NTP 設定画面

5.6. ファクトリ・リセット

このメニューでユーザーはいつでもファクトリデフォルト値に戻すことができます。(シリアルコンソールポートの近くにあるボタンを押してもファクトリ値に戻すことが可能です)。



図 5-7 ファクトリ・リセット画面

5.7. コンフィギュレーション管理

現在の設定値を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 5-8 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)

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: Location がファクトリデフォルトの場合、無効になります。

URL: Location が FTP または HTTP の場合、設定ファイルのアドレスを入力してください。

Local Path: 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。

Configuration management : /system/configuration_management

Configuration Export

Encrypt : ▼

File name :

Configuration Import

Location : Local machine FTP or HTTP Factory default

Configuration selection

Select all

Network configuration (include IP configuration)

Serial port configuration

System Configuration

Encrypted :

URL :

Local path :

図 5-8 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. Encrypt オプションを選択
2. File Name を入力
3. 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. Import ボタンをクリック

5.8. 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.intersolutionmarketing.com/downloads.html>

図 5-9 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。
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ポートする



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

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:root

```

2. System logging
3. Device Name : PS110
4. Date and time
5. Change password
6. User Administration
7. Factory reset
8. Firmware upgrade

COMMAND (Display HELP : help)>8

_] Firmware upgrade [
Do you want to upgrade firmware? [yes/no] yes
Transfer firmware by zmodem using your terminal application.
To escape, press Ctrl+X
**B0ff000005b157

```

```

Password:
# editconf

] / [
1. Network configuration
2. Serial port configuration
3. System administration

COMMAND (Display HELP : help)>3

_] System administration [ _____
1. System status

```

図 5-10 Firmware Upgrade コンソール画面

4. オンラインの指示に従ってZmodemプロトコルを使用して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、PS デバイスサーバーはエラーメッセージを表示します。(図 5-12 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。

```

login: root
Password:
# editconf

] / [
1. Network configuration
2. Serial port configuration
3. System administration

COMMAND (Display HELP : help)>3

_] System administration [ _____
1. System status
2. System logging
3. Device Name : PS110
4. Date and time
5. Change password
6. User Administration
7. Factory reset
8. Firmware upgrade

COMMAND (Display HELP : help)>8

_] Firmware upgrade [
Do you want to upgrade firmware? [yes/no] yes
Transfer firmware by zmodem using your terminal application.
To escape, press Ctrl+X
**B0ff000005b157

```

図 5-10 リモートから/シリアルコンソールを使用したファームウェア・アップグレード画面

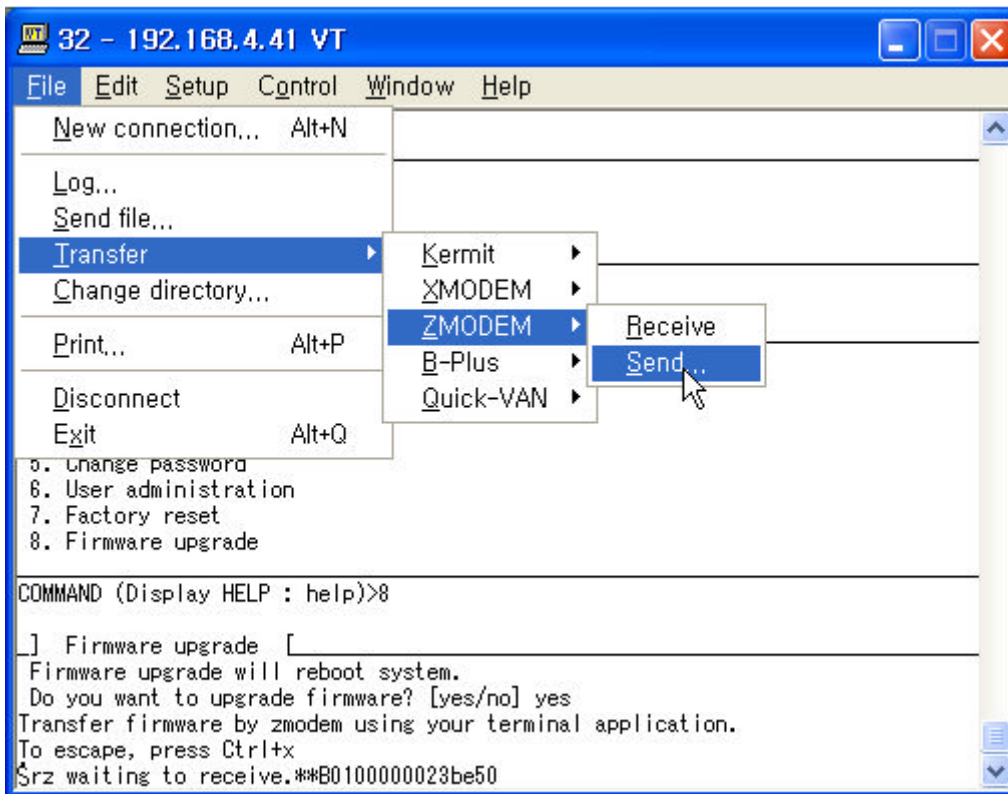


図 5-11 Zmodem(Tera Term Pro)によるバイナリ・ファイルの転送画面

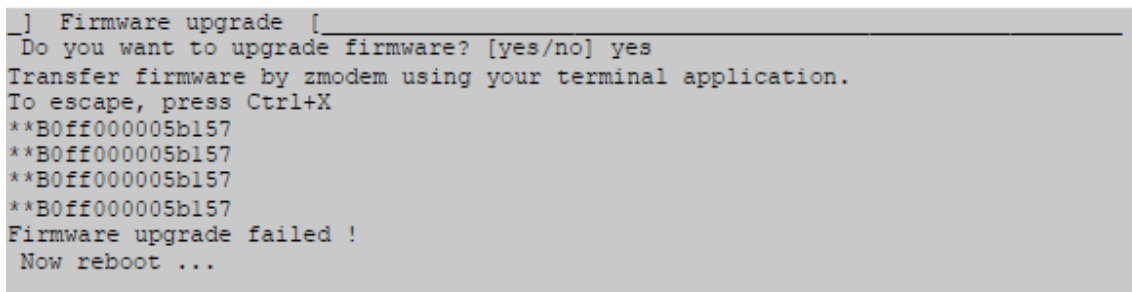


図 5-12 ファームウェア・アップグレード失敗メッセージ時の画面

5.9 ユーザー管理

ユーザーはポート管理(4.2.3.1. TCP mode を参照)をオンにすると、シリアルポートにアクセスするために、各ポートのユーザーID およびパスワードを正しく入力する必要があります。

各シリアルポートのユーザーID およびパスワードはこのメニューから設定可能です。シリアルポートに対して新規ユーザーを追加する場合、それぞれのポートに新規ユーザーのアクセス許可を与えることができます。図 5-13 を参照してください。

User administration : /system/user_auth/

User list

No.	User ID	Port 1	Port 2	Port 3	Port 4	
1	<input type="text" value="user1"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="REMOVE"/>
2	<input type="text" value="user24"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="button" value="REMOVE"/>
3	<input type="text" value="user_all"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="button" value="REMOVE"/>
NEW	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="ADD"/>

図 5-13 Port User Administration(ポートユーザー管理画面)

ポートユーザーのパスワード設定または各ポートユーザーの設定変更は

注記: システムユーザー(root)はこのメニューでポートユーザーとして追加されていない限り、シリアルポートにアクセスすることはできません。

User administration 画面にあるポートユーザー関連の対応する番号をクリックし、それから図 5-14 にあるような Port User settei 画面が表示されます。

User list - 1 : /system/user_auth/user_list/+1/

User ID

Password

Password(confirm)

Port 1

Port 2

Port 3

Port 4

図 5-14 ポートユーザー設定

6. システム統計 (System Statistics)

PS デバイスサーバーの 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、PS 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。

6.1. 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 PS デバイスサーバー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 PS デバイスサーバーの初期(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	0	50386
	Packets	0	583
	Errors	0	0
	Drop	0	0
	FIFO	0	0
	Frame	0	0
	Compressed	0	0
	Multicast	0	0
Transmit	Bytes	0	68026
	Packets	0	102
	Errors	0	2
	Drop	0	0
	FIFO	0	0
	Collisions	0	0
	Carrier	0	1
	Compressed	0	0

図 6-1 ネットワークインターフェース統計画面

6.2. 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)

Serial ports statistics

Port	Baud Rate	Tx	Rx	RTS	CTS	DTR	DSR	CD
1	9600	0	0					
2	9600	0	0					
3	9600	0	0					
4	9600	0	0					

図 6-2 シリアルポート統計画面

6.3. 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のようなデフォルト 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 checksum, 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の欠如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	222
InHdrErrors	0
InAddrErrors	0
ForwDatagrams	0
InUnknownProtos	0
InDiscard	0
InDelivers	213
OutRequests	200
OutDiscards	0
OutNoRoutes	0
ReasmTimeout	0
ReasmReqds	0
ReasmOKs	0
ReasmFails	0
FragOKs	0
FragFails	0
FragCreates	0

図 6-3 IP Statistics(統計)画面

6.4. 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。

NEchoReps,OutEchoReps:

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。

InTimestamps,OutTimestamps:

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。

InAddrMaskReps,OutAddrMaskReps:

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	0
InErrors	0
InDestUnreachs	0
InTimeExcds	0
InParmProbs	0
InSrcQuenchs	0
InRedirects	0
InEchoes	0
InEchoReps	0
InTimestamps	0
InTimestampReps	0
InAddrMasks	0
InAddrMaskReps	0
OutMsgs	0
OutErrors	0
OutDestUnreachs	0
OutTimeExcds	0
OutParmProbs	0
OutSrcQuenchs	0
OutRedirects	0
OutEchoes	0
OutEchoReps	0
OutTimestamps	0
OutTimestampReps	0
OutAddrMasks	0
OutAddrMaskReps	0

図 6-4 ICMP statistics 画面

6.5. 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。

RetransSegs:

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	1
RtoMin	200
RtoMax	120000
MaxConn	-1
ActiveOpens	0
PassiveOpens	20
AttemptFails	0
EstabResets	3
CumEstab	1
InSegs	194
OutSegs	273
RetransSegs	0
InErrs	0
OutRsts	0

図 6-5 TCP 統計図

6.6. 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つた受信した 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。

UDP statistics :	
InDatagrams	0
NoPorts	0
InErrors	0
OutDatagrams	0

図 6-6 UDP 統計図

7. CLIガイド

7.1. 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 PS デバイスサーバーの 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 PS デバイスサーバーのステータス、設定の編集、設定変更の適用などが可能です。

7.2. Flash セグメント

PS デバイスサーバー内部フラッシュは下記のテーブルにあるようにセグメント化されています。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 PS デバイスサーバー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	Bios	None	128
Mtdblock1	Kernel & ROM file system	/	1024
Mtdblock2	CRAMFS (Read only)	/mtd	2880
Mtdblock3	EXT2 (R/W)	/cnf (normally unmounted)	64
Total			4096

7.3. サポートしている Linux ユーティリティ

7.3.1. Shell & shell utilities:

cat, echo, more, pwd

7.3.2. File and disk utils:

ls, cp, mv, rm, mkdir, rmdir, touch, gunzip, gzip, tar, df, du, vi, e2fsck, mount, umount

7.3.3. System utilities:

date, free, hostname, kill, killall, ps, reboot

7.3.4. Network utilities:

ifconfig, iptable, route, ping

7.4. 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 PS デバイスサーバー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) PS デバイスサーバーに root ログインする

Telnet コンソール:

- 1) telnet Pro_Series_ip_address

SSH コンソール

- 1) ssh -2 Pro_Series_ip_address

注記: PS デバイスサーバーは SSH v2 プロトコルのみをサポートしています。

付録1. 接続

A 1.1. Ethernet ピン配置

PS デバイスサーバーは標準 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。

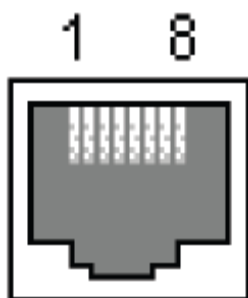
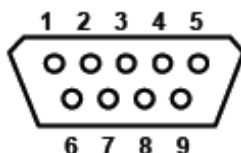


表 A-1 RJ45 コネクタのピン配置

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

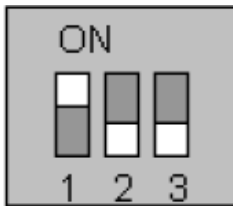
A 1.2. コンソールおよびシリアルポートピン配置

PS デバイスサーバーの 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。

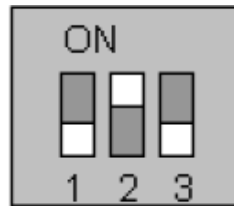


Pin	RS232 (console and serial ports)	RS422 (serial ports only)	RS485 (serial ports only)
1	DCD	Tx+	Tx+
2	Rx	RX+	RX+
3	Tx	RTS+	-
4	DTR	CTS+	-
5	GND	GND	GND
6	DSR	TX-	TX-
7	RTS	RTS-	-
8	CTS	RX-	RX-
9	-	CTS-	-

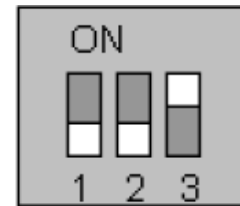
シリアル通信タイプはシリアルポートの近くにある DIP スイッチでも設定可能です (PS110 および PS410 のみ)。シリアル通信タイプを変更するには、下図で示しているように DIP スイッチの位置を変更します。DIP スイッチを変更するときには必ず PS デバイスサーバーの電源はオフにしてください。



RS-232 Mode



RS-422/485 Full Mode



RS-485 Half Mode

A 1.3. Ethernet 配線ダイアグラム

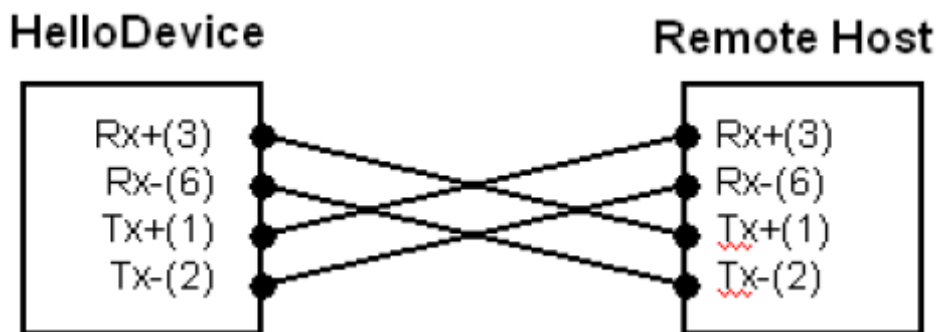


図 A-4 クロス・イーサネットケーブル接続

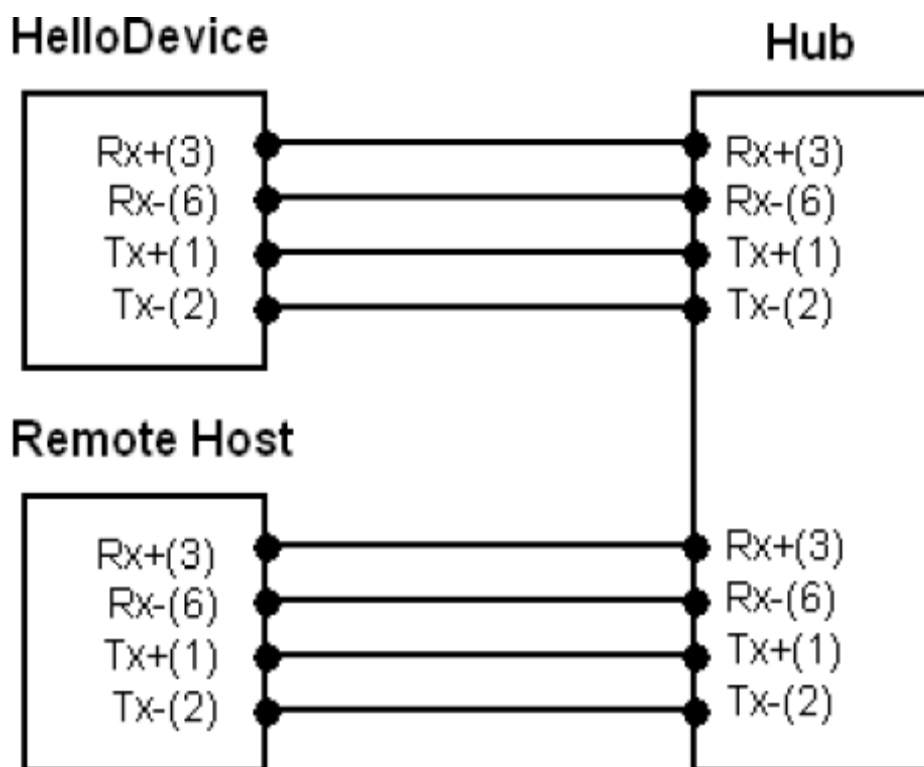
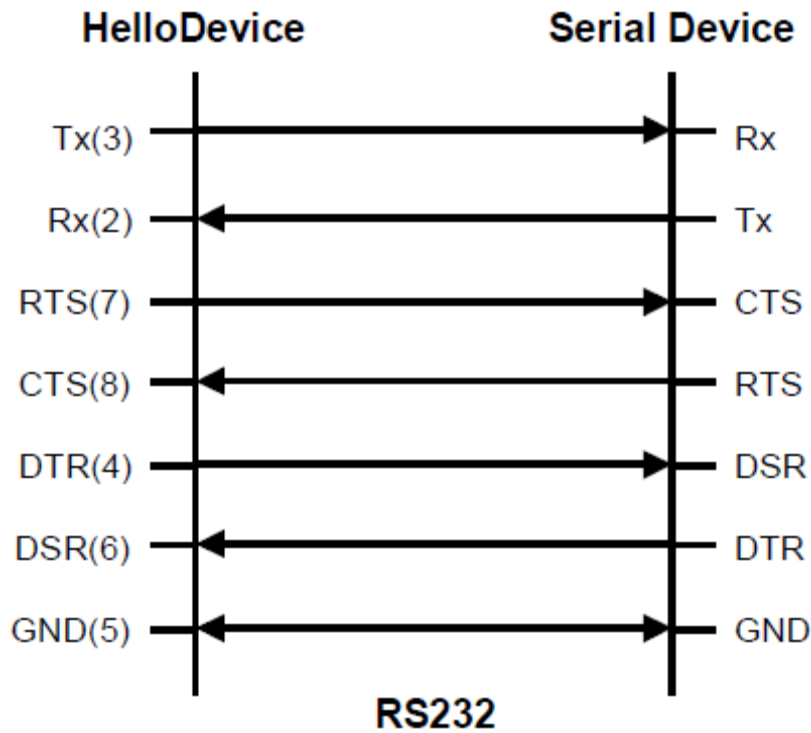


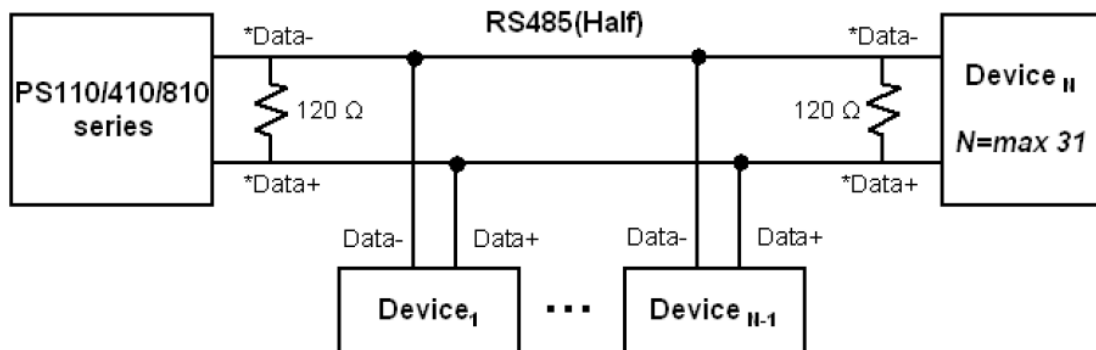
図 A-5 ストレート・イーサネットケーブルでつないだ場合

A 1.4. シリアル配線ダイアグラム

A.1.4.1. RS232 シリアル配線ダイアグラム

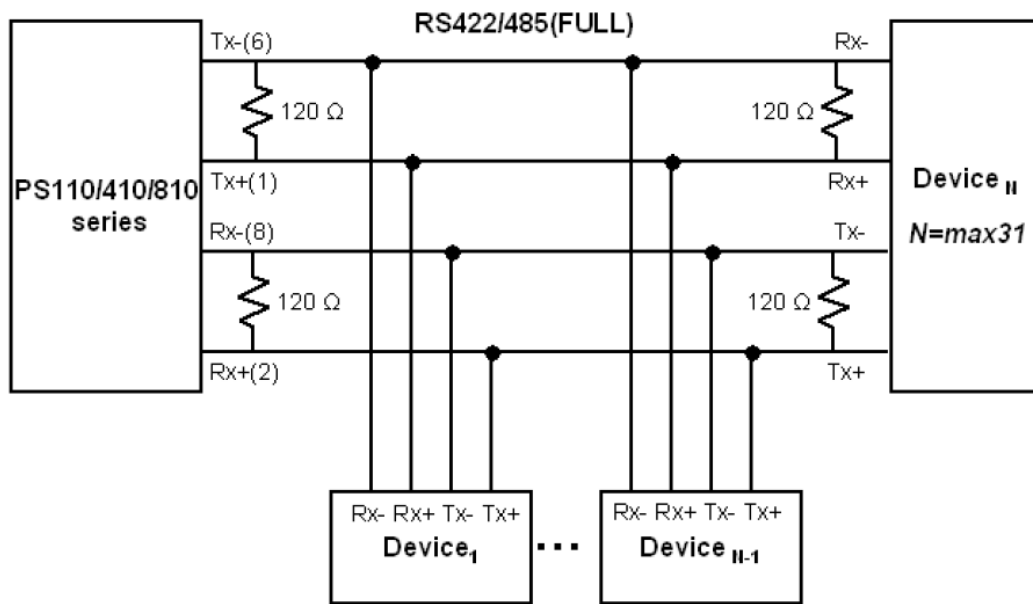


A.1.4.2. RS422/485 シリアル配線ダイアグラム



*Data+ means that coupling of Tx+(1) pin and Rx+(2) pin

*Data- means that coupling of Tx-(6) pin and Rx-(8) pin



* Termination Resistor at Tx side can be omitted if the signal status is good.

付録2. PS デバイスサーバー設定ファイル

A 2.1. Port1.conf

```
/serial/*1/parameter/baudrate=9600
/serial/*1/parameter/databit=0
/serial/*1/parameter/stopbit=0
/serial/*1/parameter/parity=0
/serial/*1/parameter/flowcontrol=0
/serial/*1/parameter/interchar to=0
/serial/*1/parameter/dtr option=0
/serial/*1/parameter/dsr option=0
/serial/*1/modem/modem init string=q1e0s0=2
/serial/*1/modem/modem dcd option=0
/serial/*1/modem/modem auto disconnection enable=0
/serial/*1/modem/modem enable=0
/serial/*1/event/event email enable=0
/serial/*1/event/event snmp enable=0
/serial/*1/event/event notification interval=30
/serial/*1/event/event enable=0
/serial/*1/hostmode/accept unlisted=1
/serial/*1/hostmode/send unlisted=1
/serial/*1/enable=1
/serial/*1/title=Port #1
/serial/*1/hostmode/mode=0
/serial/*1/hostmode/port=7001
/serial/*1/hostmode/userauth=0
/serial/*1/hostmode/telnet=0
/serial/*1/hostmode/max connection=8
/serial/*1/hostmode/cyclic time=0
/serial/*1/hostmode/inactive_time=0
```

A 2.2. filter.conf

```
/network/filter/specification/telnet=1
/network/filter/specification/ssh=1
/network/filter/specification/http=1
/network/filter/specification/https=1
/network/filter/specification/port1=1
/network/filter/specification/port2=1
/network/filter/specification/port3=1
/network/filter/specification/port4=1
```

A 2.3. snmp.conf

```
/network/snmp/syscontact=administrator
/network/snmp/sysname=ProSeries
/network/snmp/syslocation=my location
/network/snmp/syservice=7
/network/snmp/powerontrapenable=0
/network/snmp/authtrapenable=1
/network/snmp/linkuptrapenable=0
/network/snmp/loqintrapenable=0
/network/snmp/nms/*1=0.0.0.0 public 0
/network/snmp/nms/*2=0.0.0.0 public 0
/network/snmp/nms/*3=0.0.0.0 public 0
```

```
/network/snmp/nms/*4=0.0.0.0 public 0
/network/snmp/trap/*1=0.0.0.0 public 0
/network/snmp/trap/*2=0.0.0.0 public 0
/network/snmp/trap/*3=0.0.0.0 public 0
/network/snmp/trap/*4=0.0.0.0 public 0
```

付録3. 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4. BIOS メニュープログラム

A 4.1. 概要

BIOS メニューは災害時回復オプションとして TFTP を使用して PS デバイスサーバーをリカバリーし、システムハードウェアを診断する方法です。PS デバイスサーバー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 BIOS 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。

注記: PS110 は、Data/Console スイッチが Console 側になっている必要があります。

A 4.2. メインメニュー

BIOS 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。

```

-----
BIOS v1.0.0 (c) 1998-2005 Sena Technologies, Inc.
-----

Welcome to Boot Loader Configuration page
-----

Select menu
1. RTC Configuration
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-9 BIOS Menu のメイン画面

A 4.3. RTC 設定メニュー

RTC Configuration メニューを使用して、PS デバイスサーバーのシステムタイムを設定することができます。(PS110 は対応していません)

```

-----
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 BIOS Menu プログラムの RTC 設定画面

A 4.4. 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、PS デバイスサーバーの 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-11 BIOS 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 auto-detect and auto-test *****
[DRAM]
DRAM Test -----[ PASSED]
[FLASH]
FLASH Test -----[ PASSED]
[EEPROM]
EEPROM Test -----[ PASSED]

[ETHERNET]
ETHERNET Test -----[ PASSED]
[UART]
<--Internal Loop Test-->
Port # 1 test in progressing(MODE)-----[ RS232]
                                     (Read/WRIte)-----[ SUCCESS]
Port # 2 test in progressing(MODE)-----[ RS232]
                                     (Read/WRIte)-----[ SUCCESS]
Port # 3 test in progressing(MODE)-----[ RS232]
                                     (Read/WRIte)-----[ SUCCESS]
Port # 4 test in progressing(MODE)-----[ RS232]
                                     (Read/WRIte)-----[ SUCCESS]

<--External Uart Test-->
Port # 1 test in progressing(MODE)-----[ RS232]
                                     (Read/WRIte)-----[ SUCCESS]
                                     (RTS/CTS)-----[ SUCCESS]
                                     (DTR/DSR)-----[ SUCCESS]
Port # 2 test in progressing(MODE)-----[ RS232]
                                     (Read/WRIte)-----[ SUCCESS]
                                     (RTS/CTS)-----[ SUCCESS]
                                     (DTR/DSR)-----[ SUCCESS]
Port # 3 test in progressing(MODE)-----[ RS232]
                                     (Read/WRIte)-----[ SUCCESS]
                                     (RTS/CTS)-----[ SUCCESS]
                                     (DTR/DSR)-----[ SUCCESS]
Port # 4 test in progressing(MODE)-----[ RS232]
                                     (Read/WRIte)-----[ SUCCESS]
                                     (RTS/CTS)-----[ SUCCESS]
                                     (DTR/DSR)-----[ SUCCESS]

***** Hardware auto-detect and auto-test SUMMARY *****
1. DRAM Test -----[ PASSED]
2. FLASH Test -----[ PASSED]
3. EEPROM Test -----[ PASSED]
4. ETHERNET Test -----[ PASSED]
5. UART Test Summary
-----
Port Number |Port Mode | Data Communication Test | RTS/CTS | DTR/DSR |
-----
Port # 1(Internal) | UNKNOWN | FAILED | SKIPPED | SKIPPED |
Port # 1(External) | UNKNOWN | FAILED | FAILED | FAILED |
-----
Port # 2(Internal) | UNKNOWN | FAILED | SKIPPED | SKIPPED |
Port # 2(External) | UNKNOWN | FAILED | FAILED | FAILED |
-----
Port # 3(Internal) | UNKNOWN | FAILED | SKIPPED | SKIPPED |
Port # 3(External) | UNKNOWN | FAILED | FAILED | FAILED |
-----
Port # 4(Internal) | UNKNOWN | FAILED | SKIPPED | SKIPPED |
Port # 4(External) | UNKNOWN | FAILED | FAILED | FAILED |
-----
Hardware test is end. Press any key to return the test menu!!

```

図 A-12 BIOS 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. EEPROM test
5. Ethernet test
6. UART Mode test
<ESC> Back, <ENTER> Refresh
-----> 1

***** Hardware auto-detect and auto-test *****

[DRAM]
DRAM Test ----- [SKIPPED]

[FLASH]
FLASH Test ----- [SKIPPED]
```

図 A-13 ESC キーで特定のテストをスキップしている画面

A 4.5. 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 [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 [ps.img]
5. Start firmware upgrade
<ESC> Back, <ENTER> Refresh
----->
```

図 A-14 BIOS 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 [TFTP]  
2. IP address assigned to Ethernet interface [192.168.6.6]  
3. Server's IP address [192.168.6.1]  
4. Firmware File Name [ps110a.img]  
5. Start firmware upgrade  
<ESC> Back, <ENTER> Refresh  
  
-----> 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  
net trying to load image....  
TFTP Boot image(ps110a.img) loading at 0xb00000.. 3019495 Bytes  
3019495 bytes receive done.  
kernel upgrade start.  
Kernel Block : Write to Flash... done  
kernel upgrade complete.  
Cramfs upgrade start.  
Cramfs Block : Write to Flash... done  
Cramfs upgrade complete.  
Configuration upgrade start.  
Configuration Block : Write to Flash... done  
Configuration upgrade complete.  
  
Firmware upgrde is finished successfully..  
  
-----  
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 [ps.img]  
5. Start firmware upgrde  
<ESC> Back, <ENTER> Refresh  
----->
```

図 A-15 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5. Serial/IP ソフトウェアで PS デバイスサーバーを使用する

A 5.1. PS デバイスサーバーと Serial/IP オプションの比較対象表

Serial Port Configuration of Pro Series			Serial/IP Configuration		
Host mode Configuration		Cryptography Configuration	Credentials	Connection Protocol	Security
Host mode	Telnet Protocol	SSL			
TCP	Disabled	None	No login required	Raw TCP connection	Disable
TCP	Enabled	None	No login required	Telnet	Disable
TCP	Disabled	Enabled	No login required	Raw TCP connection	SSLv3 or TLSv1/SSLv3 only
TCP	Enabled	Enabled	No login required	Telnet	SSLv3 or TLSv1/SSLv3 only

PS デバイスサーバーは SSLv3のみをサポートしています。

A 5.2. 接続例: Telnet および SSL v3 暗号化

Step 1. PS デバイスサーバーのポート#1を次のように設定してください。

Host mode= TCP

Port number=7001

Telnet Protocol = Enabled

Host mode configuration : /serial/*1/hostmode/

Enable/Disable this port	Enable ▼
Port title	Port #1
Host mode configuration	
Host mode	TCP ▼
Port number (1024-65535, 0 for only outgoing connections)	7001
User authentication	Disable ▼
Telnet support	Enable ▼
Max. allowed connection (1-8)	8
Cyclic connection (sec, 0 : disable)	0
Inactivity timeout (sec, 0 : unlimited)	0
Socket ID (for outgoing connection)	
TCP Nagle algorithm Enable/Disable	Disable ▼
Remote host	
Cryptography configuration	
Modem configuration	
Serial port parameters	
Port logging configuration	
Port event handling configuration	
Copy port configuration	

Save Save & Apply Cancel

図 A-16 Host mode configuration

Step 2 次のようにPS デバイスサーバーのシリアルポート#1 の暗号設定を Cryptography Configuration 画面にて行います。

SSL enable = Enable (オン)

Cryptography configuration : /serial/*1/ssl/

Enable/Disable this port	Enable ▼
Port title	Port #1
Host mode configuration	
Cryptography configuration	
SSL enable	Enable ▼
Serial port parameters	
Modem configuration	
Port logging configuration	
Port event handling configuration	

Save Save & Apply Cancel

図 A-17 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 PS デバイスサーバーのシリアルポート#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。

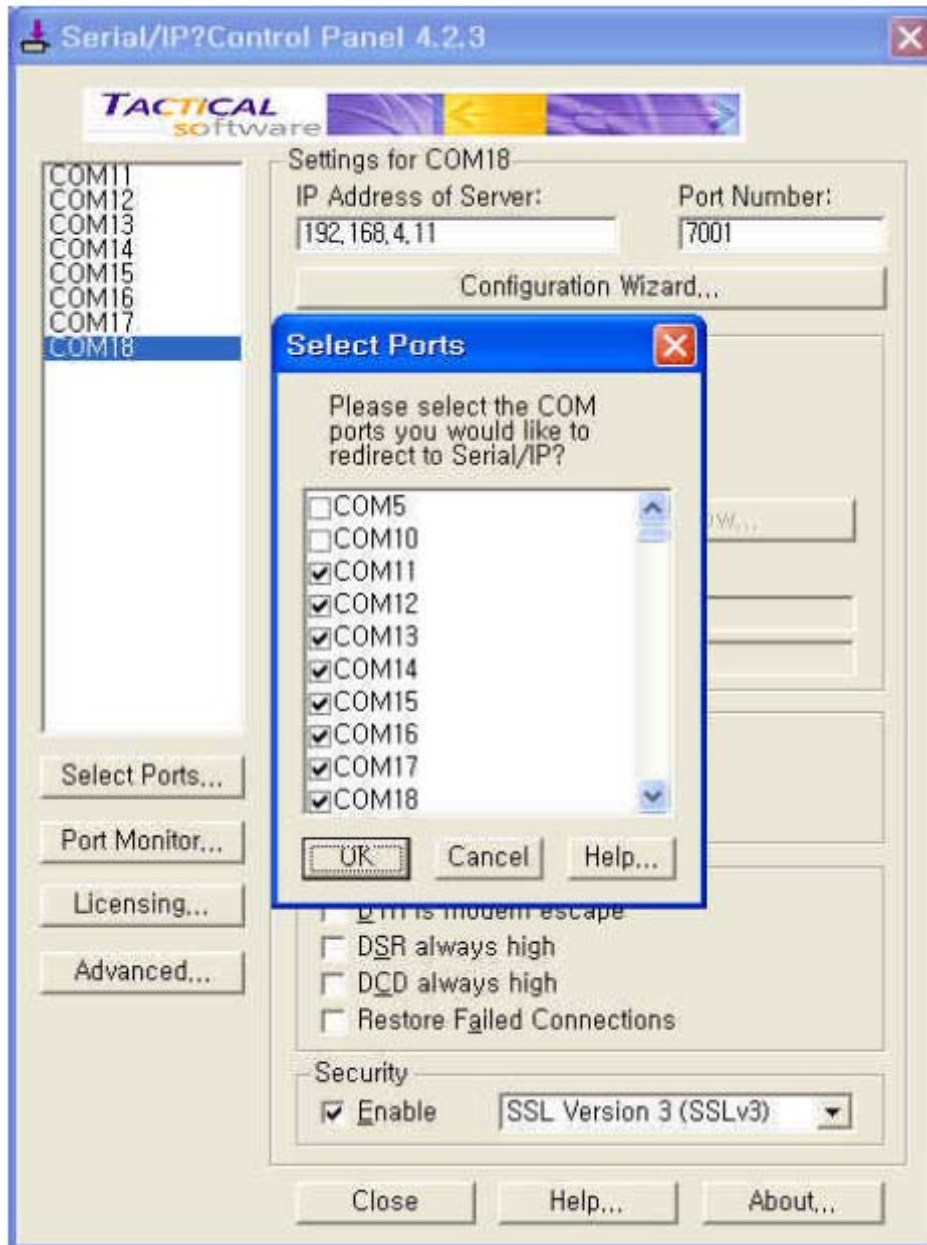


図 A-18 Serial/IP Control Panel にてポートを選択する画面

Step 4 サーバーの IP アドレス(PS デバイスサーバーの 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)

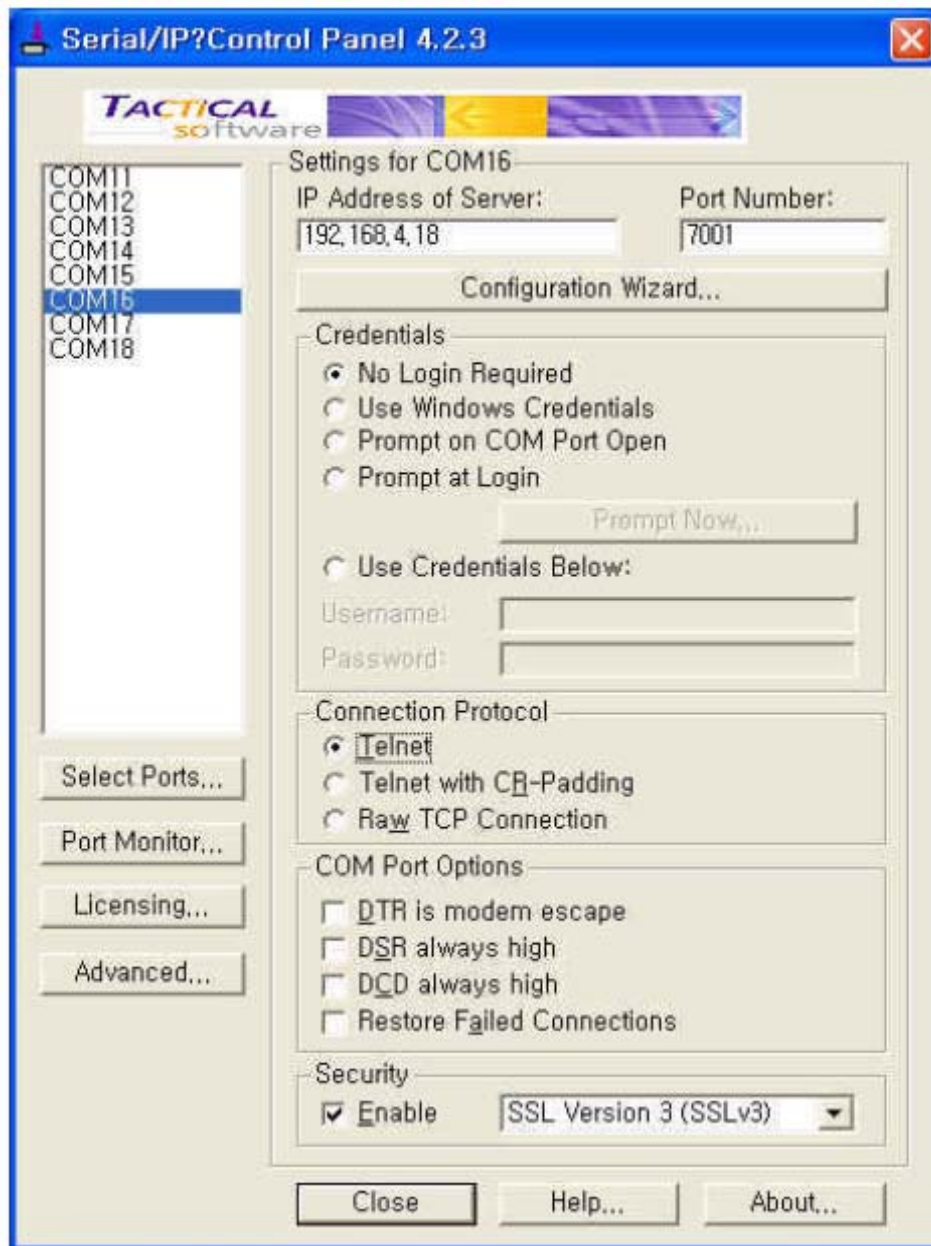


図 A-19 Serial/IP Control Panel のパラメータ設定画面

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 PS デバイスサーバーのシリアルポートを使用することが可能です。



図 A-20 Serial/IP で PS デバイスサーバー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。

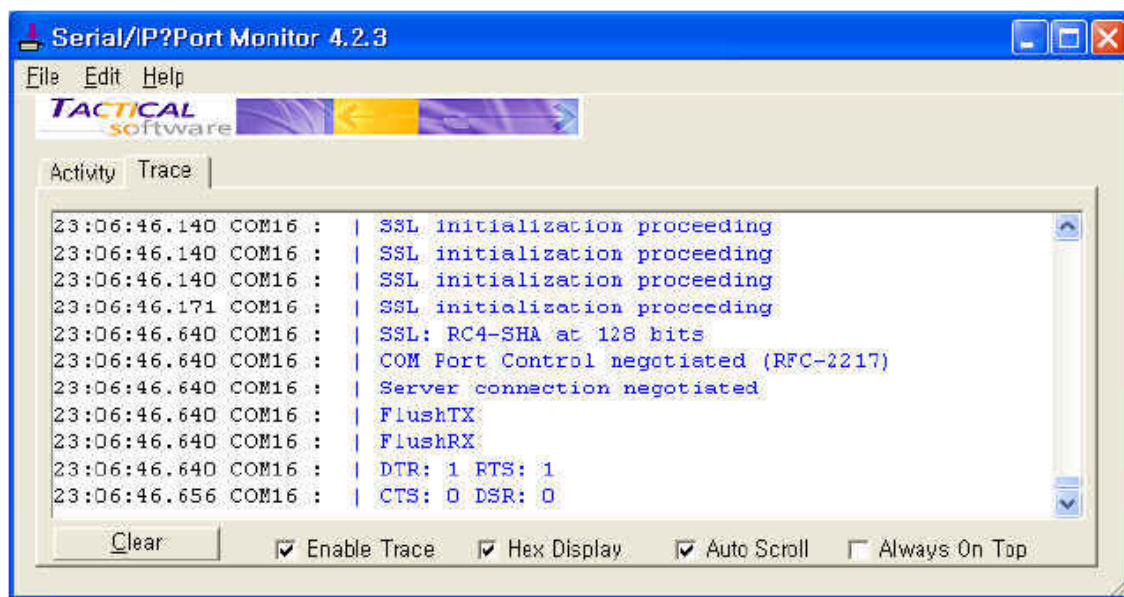


図 A-21 Serial/IP Trace Window

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

©2007 (株)インターソリューションマーケティング viiiixvi

- Pro Series Device Server の開発・製造は SENA Technologies です。
- Serial/IP は Tactical Software LLC の登録商標です。無断で転載はお断りします。
- 製品名、会社名は、各社の商標あるいは登録商標です。
- 無断でコピー、転載、記載を堅くお断りします。