Simply Better Connections

ATEN Altusen™

SN3001/SN3001P/
SN3002/SN3002P

RS-232C セキュアデバイス

ユーザーマニュアル

EMCに関する情報

連邦通信委員会(FEDERAL COMMUNICATIONS COMMISSION INTERFERENCE STATEMENT)

本製品は、FCC(連邦通信委員会)規則のPart15に準拠したデジタル装置Class Aの制限事項を満たして設計され、検査されています。この制限事項は、商業目的の使用において、有害な障害が発生しないよう、基準に沿った保護を提供するためのものです。この操作マニュアルに従わずに使用した場合、本製品から発生するラジオ周波数により、他の通信機器に影響を与える可能性があります。また、本製品を一般住宅地域で使用した場合、有害な電波障害を引き起こす可能性もあります。その際には、ユーザーご自身の負担で、その障害を取り除いてください。
本製品は、FCC(米国連邦通信委員会)規則のPart15に準拠しています。動作は次の2つの条件を前提としています。(1)このデバイスが有害な干渉を引き起こさないこと、(2)このデバイスが予想外の動作を引き起こす可能性のある干渉も含め、すべての干渉を受け入れなければならないこと。

FCCによる注意事項

本コンプライアンスに対する責任者による明確な承認を得ていない変更または改良を行った場合は、ユーザーの本装置を操作する権利を無効とします。

警告

この装置を居住地域で使用すると、電波干渉を引き起こす可能性があります。

KCCステートメント:

유선 제품용 / A 급 기기 (업무용 방송 통신 기기)
이 기기는 업무용 (A 급) 전자파적합기기로서 판매자 또는 사용자는 이 점을 주의하시기 바라며 , 가정 외의 지역에서 사용하는 것을 목적으로 합니다 .

カナダ産業省による宣言

本Class Aデジタル装置はカナダのICES-003に準拠しています。

CAN ICES-003 (A) / NMB-003 (A)

RoHS

本製品は『電気・電子機器に含まれる特定有害物質の使用制限に関する欧州議会及び理事会指令』、通称RoHS指令に準拠しております。

本マニュアルについて

このマニュアルは、セキュアデバイスサーバーを最大限に活用できるようにするために提供されています。このマニュアルでは、製品の取り付け・セットアップ方法、操作方法のすべてを提供します。

このユーザーマニュアルの対象となるセキュアデバイスサーバーには、次のモデルがあります:

モデル	製品名
SN3001	1ポートRS-232Cセキュアデバイスサーバー
SN3001P	PoE搭載1ポートRS-232Cセキュアデバイスサーバー
SN3002	2ポートRS-232Cセキュアデバイスサーバー
SN3002P	PoE搭載2ポートRS-232Cセキュアデバイスサーバー

マニュアルは下記のとおりに構成されています。

第1章「はじめに」では、セキュアデバイスサーバーについて説明します。特長、機能概要および製品各部名称について説明します。

第2章「ハードウェアのセットアップ」では、セキュアデバイスサーバーを設定するための手順を順を追って説明します。

第3章「ネットワークの設定とログイン」では、Webブラウザーからセキュアデバイスサーバーにログインする方法について説明します。

第4章「Webコンソール」では、セキュアデバイスサーバーの動作環境を設定するために使用する管理手順について説明します。

第5章「ユーザー管理」では、ログインアカウントおよびRADIUSなどのサポートされているサードパーティー認証サービスについて詳しく説明します。

第6章「ポート操作モード」では、セキュアデバイスサーバーの操作モードを紹介し、それぞれの目的について説明します。

第7章「ポートアクセス」では、セキュアデバイスサーバーのCOMポートにアクセスし、SNビューワーを起動する方法について説明します。

第8章「リモートターミナル操作」では、Telnet、SSH、PuTTYなどのリモートターミナルセッションを介してセキュアデバイスサーバーにアクセスする方法について説明します。

第9章「仮想シリアルポートマネージャー」では、仮想COMポートドライバーをインストールし、仮想COMポートを設定および管理する方法を示します。

第10章「シリアルネットワークデバイスマネージャー」では、シリアルネットワークデバイス管理ユーティリティーを使用して、作業上のシリアルポートを簡単に管理するためのデバイスグループを作成およびメンテナンスする方法と、ブラウザーベースの管理ユーティリティーの代わりにAPを使用する方法について説明します。

付録:マニュアルの最後に技術情報とトラブルシューティング情報が記載されています。

マニュアル表記について

このマニュアルでは、次の規則を使用します。

Monospaced	入力するキーを示します。
□	押すべきキーを示します。例えば、[Enter]はEnterキーを押すことを意味します。キーにコードを付ける必要がある場合は、キーの間にプラス記号が付いた同じ括弧内に[Ctrl+Alt]と一緒に表示されます。
1.	番号が付けられている場合は、番号に従って操作を行ってください。
♦	◆印は情報を示しますが、作業の手順を意味するものではありません。
>	次に表示されるオプション(メニューやダイアログボックスなど)を選択することを示します。矢印は操作の手順を示します。例えばStart > Runはスタートメニューを開き、Runを選択することを意味します。
	重要な情報を示しています。

同梱品

SN3001/SN3002

標準のSN3001/SN3002パッケージは以下から構成されています:

- セキュアデバイスサーバー（SN3001/SN3002）×1
- 電源アダプター×1
- ターミナルブロック×1
- フットパッド(4個入)×1
- DINレールマウントキット×1
- クイックスタートガイド*×1

SN3001P/SN3002P

標準SN3001P/SN3002Pパッケージは以下から構成されています:

- PoE搭載セキュアデバイスサーバー(SN3001P/SN3002P)×1
- ターミナルブロック×1
- フットパッド(4個入)
- DINレールマウントキット×1
- クイックスタートガイド*×1

上記のアイテムが揃っているか、ご確認ください。万が一、欠品または破損品があった場合は、販売店にご連絡ください。

このマニュアルをよく読んで、取り付けおよび操作手順を慎重に行い、セキュアデバイスサーバー、またはこの製品のシステムで使用するその他のデバイスに損傷を与えないようにしてください。

＊このマニュアルの公開後に、セキュアデバイスサーバーに機能が追加されている場合があります。最新版のユーザーマニュアルは、弊社のホームページからダウンロードできます。

ユーザーの皆様へ

このマニュアルに記載されているすべての情報、ドキュメント、および仕様は、製造元から事前に通知されることなく変更される場合があります。製造業者は、本契約の内容に関して、明示的または黙示的に表明または保証を行わず、特定の目的のための商業性または適合性に関するいかなる保証も特に放棄します。本マニュアルに記載されている製造者のソフトウェアがそのまま販売またはライセンスされている場合、プログラムが購入後に欠陥があることが判明した場合、購入者(製造者、販売代理店またはそのディーラーではなく)は、必要なすべてのサービス、修理およびソフトウェアの欠陥に起因する付随的または派生的損害の全費用を負担するものとします。

このシステムの製造業者は、この装置に対する許可されていない変更によって引き起こされる無線および/またはTV干渉の責任を負いません。このような干渉を取り除くことは、ユーザの責任です。

製造業者は、動作前に正しい電圧設定が選択されていない場合には、このシステムの動作において被るいかなる損害に対しても責任を負いません。使用前に電圧設定が正しいことを確認してください。

目次

第1章
はじめに

概要

セキュアデバイスサーバーは、RS-232Cシリアルデバイス用にセキュリティー保護されたIPベースのLAN接続を提供し、幅広い操作モードをサポートします。これにより、日常的なRS-232Cシリアルデバイス(PLC、メーター、センサー)をネットワークに接続し、ネットワークを介してどこからでもアクセスおよび管理できるようになります。

セキュアリアルCOM、セキュアTCPクライアント/サーバー、セキュアシリアルトンネル、セキュアコンソール管理などの広範なセキュリティー機能を搭載したセキュアデバイスサーバーは、幅広いセキュリティークリティカルなアプリケーションでRS-232Cシリアルデバイスを管理するための理想的なソリューションです。

既存のシリアル通信ソフトウェアと完全に互換性があるため、セキュアデバイスサーバーは、ソフトウェア開発への以前の投資を確実に保護します。COMまたはTTYポートで動作するように設計されたソフトウェアは、セキュアデバイスサーバーのリアルCOMまたはTTYドライバー使用して、TCP/IPネットワーク経由で接続されたシリアルデバイスにアクセスできます。この機能は、PCハードウェアで発生するポート番号と距離制限の障壁を突破することもできます。

SSLおよびSSHプロトコルに対応し、データ伝送を暗号化することで、セキュアデバイスサーバーは、プライベートネットワークとパブリックネットワークの両方でセキュアなデータ伝送を保証します。

セキュアデバイスサーバーのセットアップはスピーディーかつ簡単に行うことができます。必要となる作業は、適切なポートにケーブルを接続するだけです。また、ブラウザーベースのGUI、Telnet/SSHコンソールセッション、Windowsソフトウェアユーティリティーも提供しており、設定や操作を迅速かつ円滑に行うことができます。

SN3001P/SN3002PはPoE機能を備えており、IEE802.3afに準拠しているため、追加の電源を必要とせずに、PoEスイッチ/アダプターでイーサネットケーブルを通して給電することができます。

いずれにせよ、その高度な機能と作業の容易さにより、セキュアデバイスサーバーは、お客様のシリアルデバイスを遠隔で管理するのに、利便性と信頼性に最も優れており、費用対効果の高い方法です。

特長

シリアル→イーサネット接続

- イーサネットを介したセキュアなシリアルデータ伝送用のRS-232Cシリアルポート(1または2ポート)
- セキュア操作モード - セキュアリアルCOM、セキュアTCPサーバー/クライアント、セキュアシリアルトンネル、コンソール管理(SSH)、およびコンソール管理ダイレクト(SSH)
- 標準操作モード - リアルCOM、TCPサーバー/クライアント、シリアルトンネル、UDP、コンソール管理(Telnet)、およびコンソール管理ダイレクト(Telnet)
- Windows、Linux、およびUNIX用のリアルCOM、リアルTTY、および固定TTYドライバー
- Javaビューワー(SSH/Telnet)またはPuTTYなどのサードパーティークライアントを介した便利なコンソール管理アクセス
- Javaビューワーによる簡易コンソールポートアクセスおよびSun Solari対応(breakfree)
- 複数のユーザーが同一ポートに同時ログイン可能 - 各ポートにつき最大16ユーザーが接続可能

ハードウェア

- フェイルセーフ電源用の冗長電源入力(電源ジャックおよびターミナルブロック)
- IEEE802.3af準拠PoE電源装置(SN3001P/SN3002Pのみ)
- シリアル、イーサネット、および電源のサージ保護
- 壁およびDINレールへの取り付け(オプションキットVE-RMK1Uが必要)、デスクトップ取り付けが利用可能
- 対応ボーレート - 110、134、150、300、600、1200、1800、2400、4800, 7200、9600、19200、38400、57600、115200、230.4k、460.8k、921.6k bps

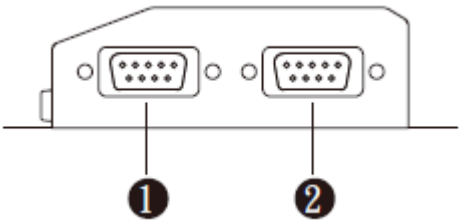
セキュリティー

- TLS1.2データ暗号化とRSA2048ビット証明書によるブラウザーからのセキュアなログインをサポート
- ユーザーに対してポートのアクセスおよび操作の権限を設定可能
- ローカルやリモートからの認証とログインに対応
- サードパーティー認証(RADIUSなど)
- セキュリティー保護のためのIPアドレスフィルター

システム管理

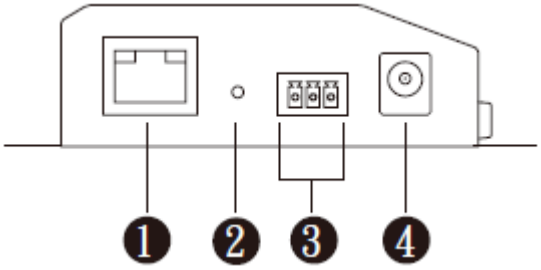
- 直感的なGUIを使ったブラウザーアクセス
- 高速設定のためのWebベースのクイックセットアップウィザード
- メニュー形式のインターフェースによるTelnet/SSH経由でのターミナルベースアクセス
- 接続されたシリアルデバイス(ターミナルブロックを含む)のオンライン/オフライン検出により、デバイスがオフライン(電源障害など)のときに、デバイス状態監視のためにイベント通知を自動的に送信
- システムイベントログは内部メモリーまたはSyslogサーバーに保存
- ポートログは内部メモリーまたはSyslogサーバーに保存
- SNMPエージェント(v1/v2c)
- イベント通知 – SMTPメールとSNMPトラップ(v1/v2c)による通知をサポート
- システム設定のバックアップ/リストアおよびファームウェアのアップグレード可能
- 64 Kbyteポートバッファーによってネットワークがダウンした際のデータ損失を防止
- NTPでタイムサーバーと同期
- 多言語WebベースGUI

SN3001/SN3001P/SN3002/SN3002P フロントパネル



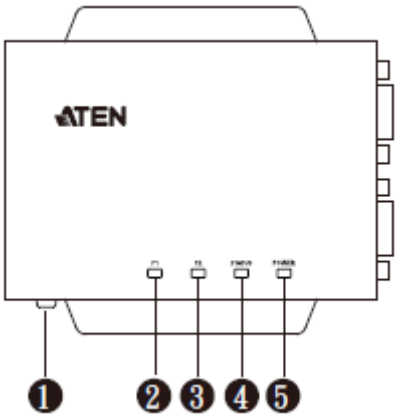
番号	名称	説明
1	RS-232Cシリアルポート1	RS-232Cシリアルデバイスに接続します。
2	RS-232Cシリアルポート2	2台目のRS-232Cシリアルデバイスに接続します。 (SN3002/SN3002Pのみ)

SN3001/SN3001P/SN3002/SN3002P リアパネル



番号	名称	説明
1	LANポート	セキュアデバイスサーバーをネットワークに接続します。 SN3001P/SN3002P(PoE802.3af準拠)の場合、PoEスイッチで同時に電源を供給することができます。
2	リセットボタン	ボタンを押して3秒未満で指を離すと、システムの再起動が実行されます。 3秒以上長押しすると、設定(ユーザーアカウント設定、権限を除く)が購入時の状態に戻ります。
3	電源ターミナル	DC電源リードと付属のターミナルブロックを介して、セキュアデバイスサーバーを電源に接続します。
4	電源ジャック	電源アダプターを使用してセキュアデバイスサーバーを電源に接続します。

SN3001/SN3001P/SN3002/SN3002P　トップパネル



番号	名称	説明
1	グランドターミナル	接地線を使用して、適切な接地された物体に接続し、ユニットを接地します。
2	シリアルポート1 LED	ユニットのRS-232Cシリアルポート1経由でデータを送受信している場合は、緑色またはオレンジ色に点灯します。
3	シリアルポート2 LED	ユニットのRS-232Cシリアルポート2(SN3002/SN3002Pのみ)経由でデータを送受信している場合は、緑色またはオレンジ色に点灯します。
4	ステータスLED	通常動作または起動時はそれぞれ黄色/緑色に点灯または点滅し、エラー(ハードウェア障害、DHCP異常など)が発生すると赤色に点灯します。
5	電源LED	セキュアデバイスサーバーの電源が投入され、準備が完了すると緑色に点灯します。

第2章
ハードウェアのセットアップ

セットアップの前に

1. 機器の設置に際し重要な情報をp.73に記載しています。作業の前に、必ず目を通してください。
2. 接続するすべての機器の電源がOFFになっていることを確認してください。

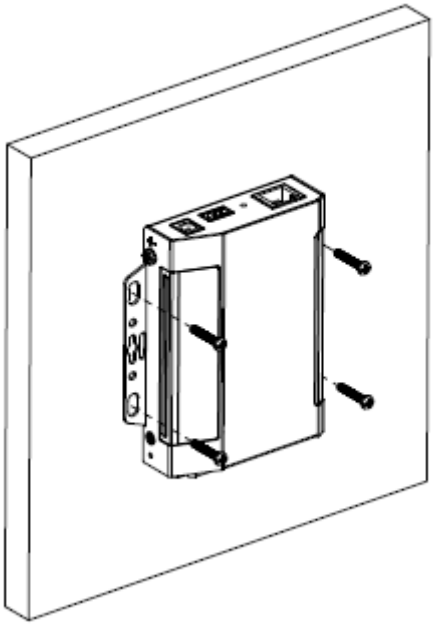
配置オプション

柔軟性と利便性が得られるよう、セキュアデバイスサーバーは、壁またはDINレールに取り付けることができます。説明は次のとおりです。

壁への取り付け

セキュアデバイスサーバーを壁に取り付けるには、次の手順に従って作業を行ってください:

製品本体は、(ご自身で用意された)4本のネジを使用して、下図に示すように、サイドのネジ穴を介して壁に取り付けることができます。

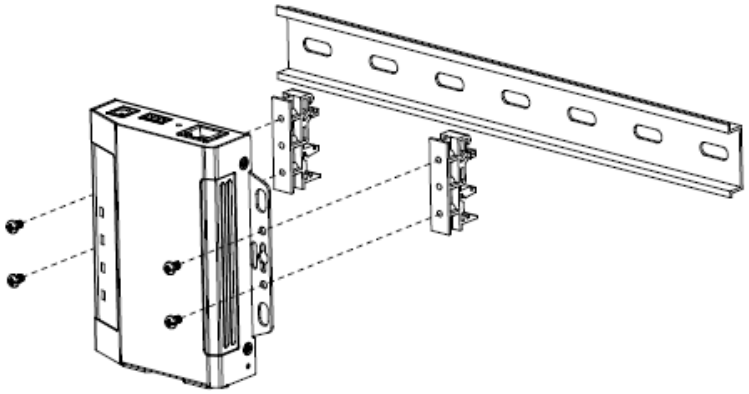


DINレールによるマウント

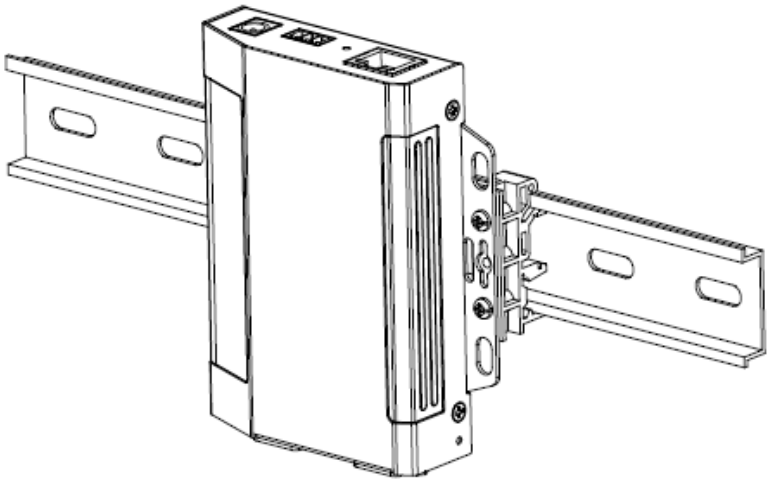
付属のDINレールマウントキットを使用してセキュアデバイスサーバーをDINレールに取り付けるには、次の手順に従って作業を行ってください:

平行DINレールによるマウント

1. DINレールと平行に取り付ける場合は、付属のネジ(4個)を使ってDINレール取付金具(2個)を中央のネジ穴に取り付けてください。

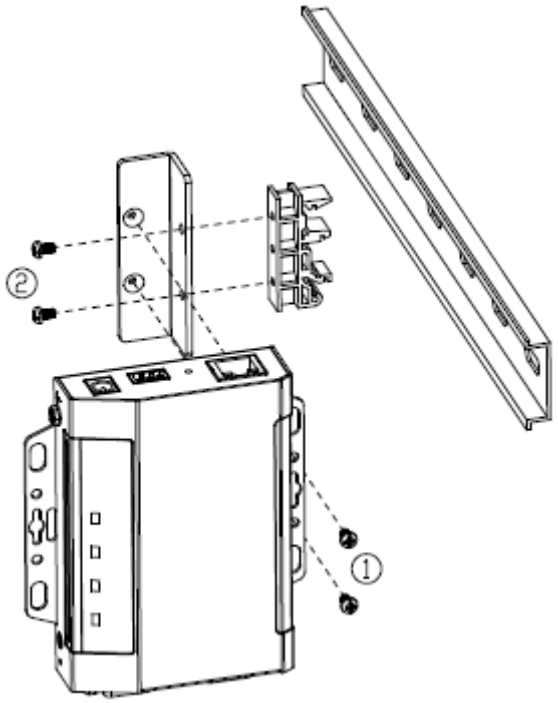


2. ユニットをDINレールに掛けてください。

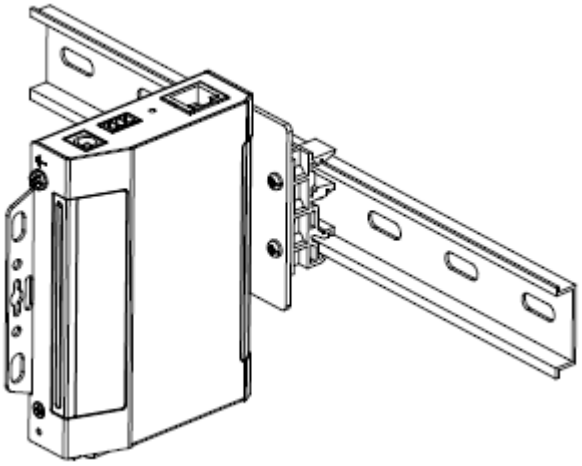


垂直DINレールによるマウント

1. マウント用ブラケット(L字形)を、グランドターミナルとは反対側の中央のネジ穴にM3×6ネジ(2本)を通して本体に取り付けてください。
2. 付属の4本のネジのうち2本を使用して、DINレールマウント用ブラケットをL字型マウント用ブラケットの側面に取り付けてください。



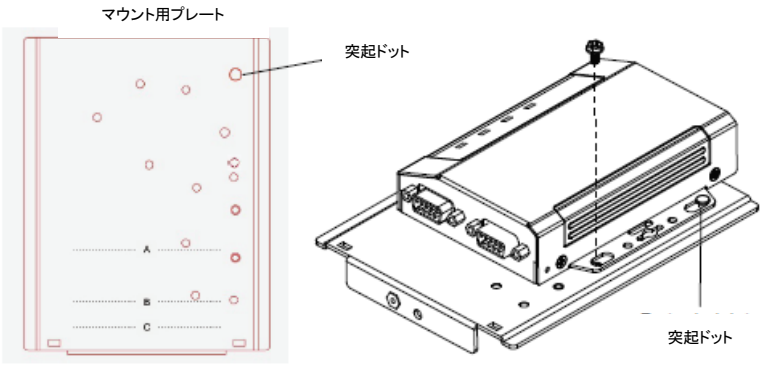
3. ユニットをDINレールに掛けてください。



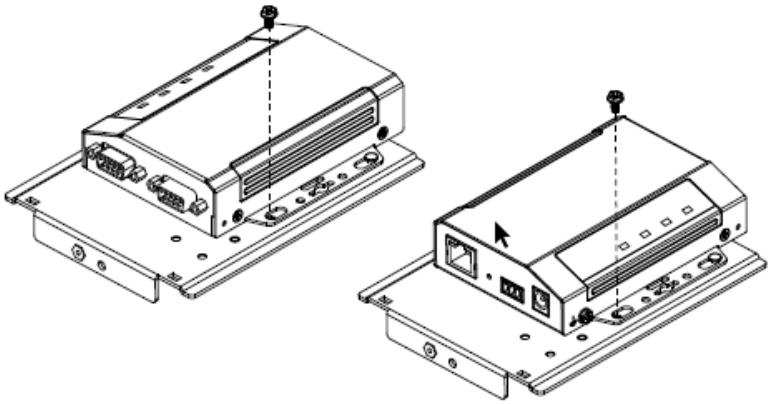
ラックへのマウント

セキュアデバイスサーバーをラックにマウントするには、別売のラックマウントキット(VE-RMK1U)が必要です。手順は次のとおりです:

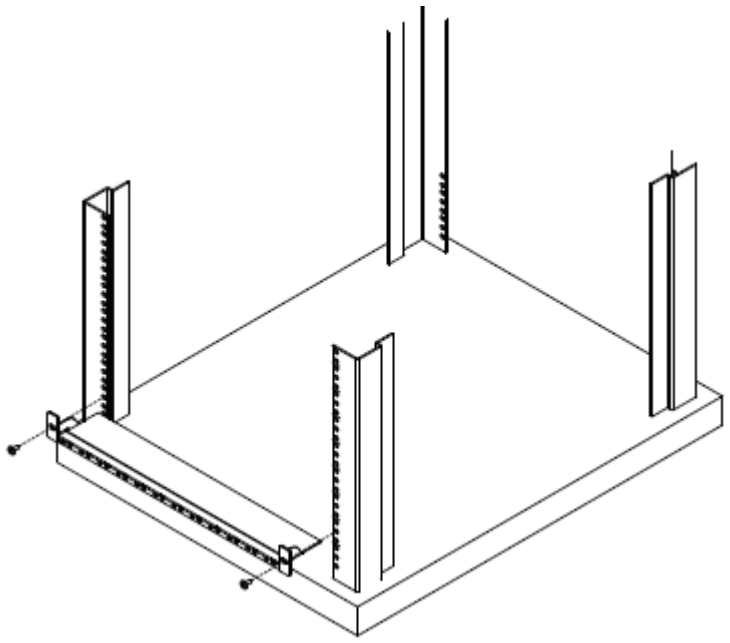
1. 下図に示すように、ラックイヤーの1つを、プレートの突起ドットにラッチで留めながら、デバイスをマウント用プレートに配置してください。



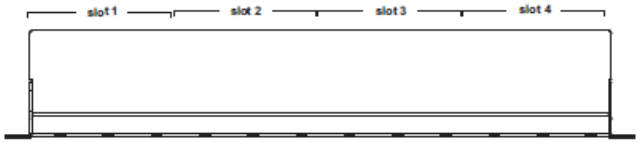
2. 付属の六角ネジを使用してデバイスを取り付け、プレートに固定してください。セキュアデバイスサーバーを固定する際に、シリアルポートは内側と外側のどちらに向けても構いません。



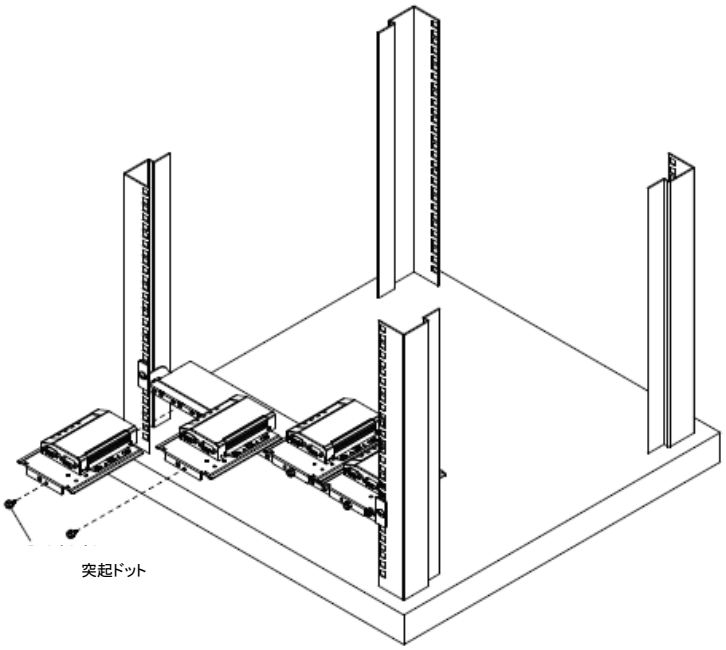
3. 下図に示すように、VE-RMK1Uフレームの穴とラックの穴の位置を合わせ、（ご自身で用意された）2本のネジでフレームをラックに固定してください。



4. デバイスとマウント用プレートの部品をVE-RMK1Uのフレームのスロットの1つに合わせたら、付属のプラスチックネジでマウント用プレートをフレームに固定してください。



VE-RMK1U F　フレーム

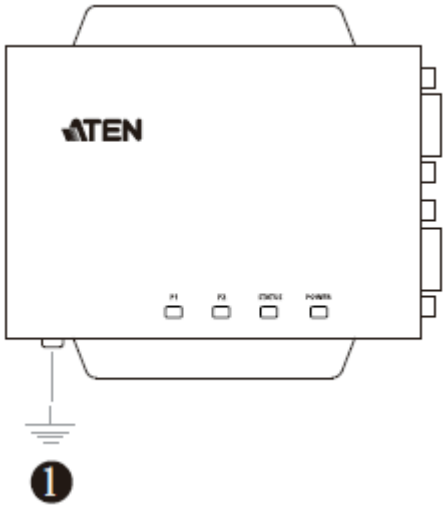


注意:	**VE-RMK1Uのフレームには、最大4台のセキュアデバイスサーバーを取り付けることができます。**

セットアップ

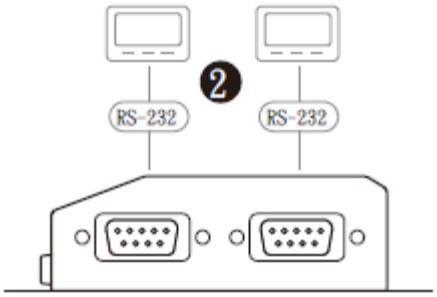
セキュアデバイスサーバーを取り付けるには、次ページの図を参照しながら、以下の手順に従って作業を行ってください(図内の番号はセットアップ手順に対応)。

1. 接地線を使用して、グランドターミナルの一方の端ともう一方の端を適切な接地された物体に接続し、ユニットをアースしてください。



注意:	**この手順は省略しないでください。適切な接地を行うことで電圧変化や静電気による機器の破損防止に一定の効果があります。**

2. ユニットのRS-232Cシリアルポートに、1台または最大2台のシリアルデバイスを接続してください。



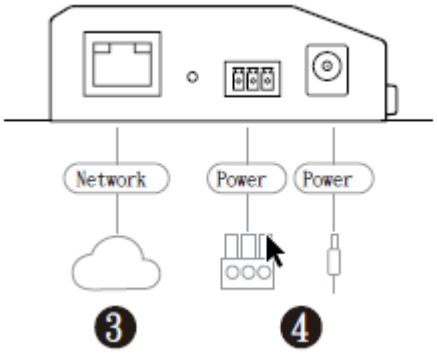
3. ユニットのLANポートとネットワークをCat5e/6ケーブルで接続してください。なお、SN3001P/SN3002P(PoE802.3af準拠)の場合、ユーザーはPoEスイッチを通してユニットに電源を同時に供給できるため、手順4を省略することができます。

4. 冗長電源を行う場合は、次のいずれかまたは両方を実行することで、ユニットを電源に接続してONにしてください:

   - 付属の電源アダプター(SN3001P/SN3002Pには付属していません)をAC電源に接続し、そのケーブルを本体の電源ジャックに差し込んでください。

注意:	**電源アダプターの温度許容差は0～40℃です。環境温度が40～60℃の場合、電源ターミナルを介してのみデバイスに電源を供給することができます。**

   - 付属のターミナルブロックで、DC+線と−線(DC9～48V)をユニットの電源ターミナルに接続してください。



5. 電源投入後、セキュアデバイスサーバーの準備ができるまで約50秒間待機すると、ステータスLEDが緑色に点灯します。

注意:	**複数の電源装置が接続されている場合、他の電源装置が中断されても追加の電源接続は動作を維持します。例えば、製品本体の電源ジャックと電源ターミナルの両方を介してデバイスを電源に接続している場合、電源ターミナルまたは電源ジャックの電源どちらかが故障したとき、片方から給電して動作を維持します。**

シリアルポートのピンアサイン

セキュアデバイスサーバーのRS-232Cシリアルポートのピンアサインを以下に示します:

ピン	設定
	RS-232C
1	DCD
2	RxD
3	TxD
4	DTR
5	GND
6	DSR
7	RTS
8	CTS

第3章
ネットワークの設定とログイン

IPアドレスの設定

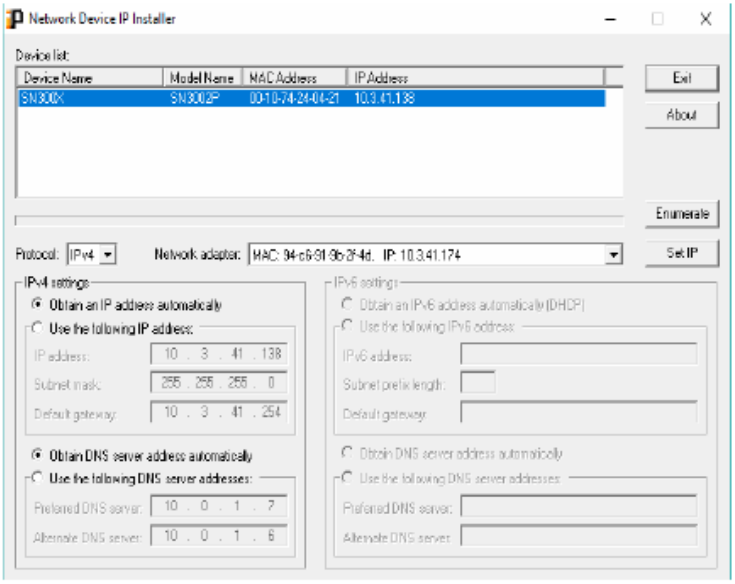
開始する前に、使用するPCがセキュアデバイスサーバーと同じLAN内にあることを確認してください。

セキュアデバイスサーバーのIPアドレスの設定には、Windows PCのIPインストーラーユーティリティーを使用する方法と、PCのみを使用する方法(非DHCPネットワークにのみ適用)の2つの方法があります:

IPインストーラーユーティリティー

Windows PCを使用すると、**IPインストーラーユーティリティー**を使用して、DHCPまたは非DHCPネットワークでセキュアデバイスサーバーのIPアドレスを検索したり、IPアドレスを割り当てたりすることができます。

1. 製品のWebページから「サポート情報」>「マニュアル/ファームウェア」からファイル「**IP Installer.zip**」をダウンロードしてください。
2. ファイルを展開し、「IPInstaller.exe」を実行してください。次のようなダイアログボックスが表示されます。



3. デバイスリストでセキュアデバイスサーバーを選択してください。

注意:	**1. リストが空の場合、またはデバイスが表示されない場合は、正しいネットワークアダプターが選択されていることを再度ご確認の上、「列挙」をクリックしてデバイスリストを更新してください。**

	2. リストに複数のデバイスがある場合は、MACアドレスを使用してデバイスを区別してください。セキュアデバイスサーバーのMACアドレスは、製品本体の底面にあります。

4. セキュアデバイスサーバーのIPアドレスを確認するか、IPアドレスを設定するには、それぞれ「**IPアドレスを自動的に取得する**」または「**次のIPアドレスを使用する**」を選択してください。
   - IPアドレスを設定するには、ネットワーク環境に応じて必要なIPアドレス、サブネットマスク、ゲートウェイ情報を入力してください。
5. 「**IPを設定**」ボタンをクリックしてください。セキュアデバイスサーバーのIPアドレスがデバイスリストに表示されます。
6. 「**終了**」をクリックしてプログラムを閉じてください。

IPインストーラーなし(非DHCPのみ)

Windows以外のシステムの非DHCPネットワークの環境において、ユーザーは以下の手順に従って、デフォルトの192.168.0.60とは異なる静的IPアドレスをセキュアデバイスサーバーに割り当てることができます。

1. PCのIPアドレスを192.168.0.XXXに設定してください。XXXには、10以外の任意の数字を指定できます。
2. デバイスのデフォルトIPアドレス(192.168.0.60)を、ブラウザーのアドレスバーに入力してください。
3. 有効なユーザーネームとパスワードでログインしてください(p.16参照)。
4. セキュアデバイスサーバーのWebインターフェースで、ネットワーク環境に応じて固定IPアドレスを割り当ててください。
5. 設定を保存し、ログアウトしてください。ログアウトしたら、PCのIPアドレスを元の値にリセットしてください。

ログイン

Webブラウザーからセキュアデバイスサーバーにアクセスするには、次の手順を実行してください:

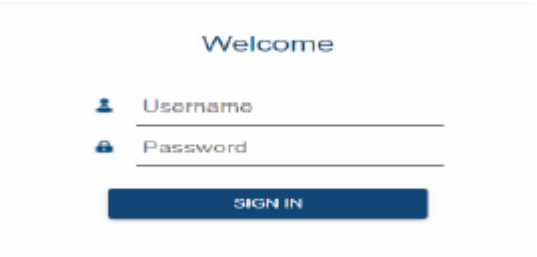
1. ブラウザーを開き、ブラウザーのアドレスバーでアクセスするセキュアデバイスサーバーのIPアドレスを指定してください。

注意:	**セキュアデバイスサーバーのIPアドレスを決定する様々な方法について、「IPアドレスの設定」(p.15参照)で説明しています。管理者として初めてログインする場合は、こちらを参照してください。**

2. セキュリティー警告が表示された場合は、証明書を受け入れてください。これは信頼できるものです。詳細については、p.42「セキュリティー証明書」を参照

してください。2番目の証明書が表示されたら、それも受け入れてください。

3. 表示されるログイン画面で、ログインするための有効なユーザーネームとパスワードを入力してください。デフォルトのユーザーネームとパスワードは、それぞれadministratorとpasswordです。

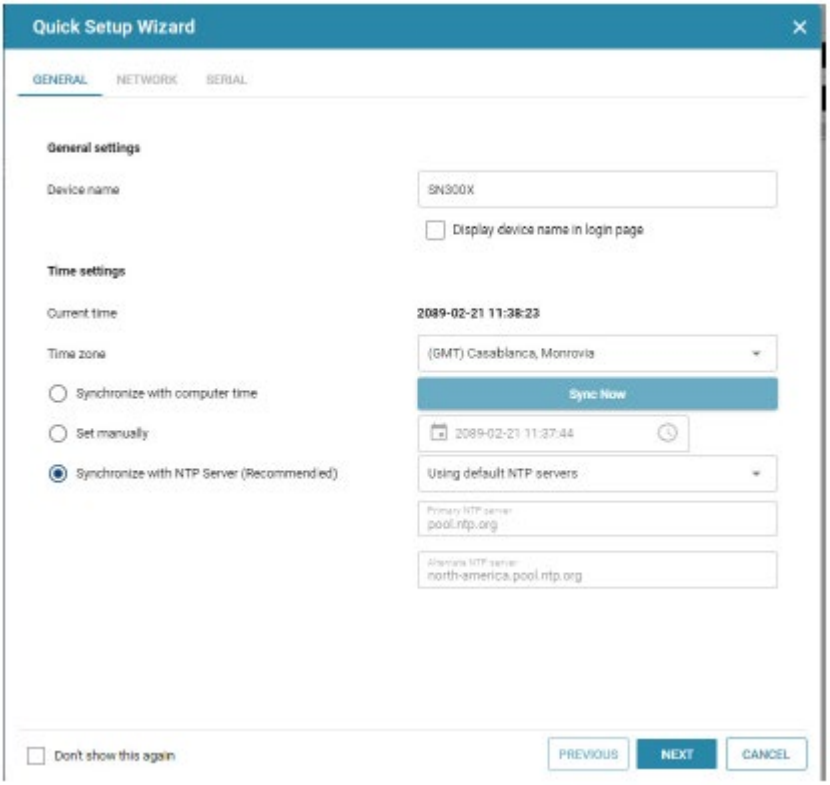


4. ログインに成功すると、セキュアデバイスサーバーのメイン画面が表示されます。初回ログイン時に、ユーザーはセキュアデバイスサーバーのログインパスワードを変更する必要があります。
5. 初回ログイン時に、ユーザーはセキュアデバイスサーバーのログインパスワードを変更する必要があります。
6. ログインすると、クイックセットアップウィザードが表示され、セキュアデバイスサーバーの基本設定を行うことができます。

クイックセットアップウィザード

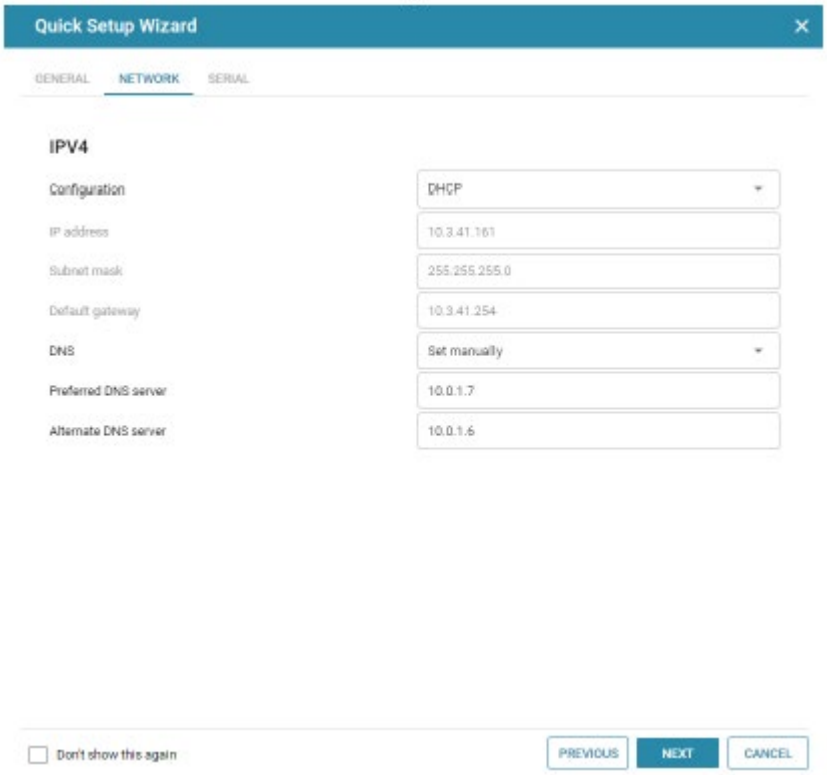
クイックセットアップウィザードは、セキュアデバイスサーバーの基本設定を開始するものです。

全般



項目	説明
デバイス名	セキュアデバイスサーバーの名前を表示します。必要に応じて、デバイス名を変更してください。
現在時刻	デバイスの現在の時刻を表示します。
時刻設定	デバイスの時刻設定を定義します。詳細については、p.34「時刻」を参照してください。

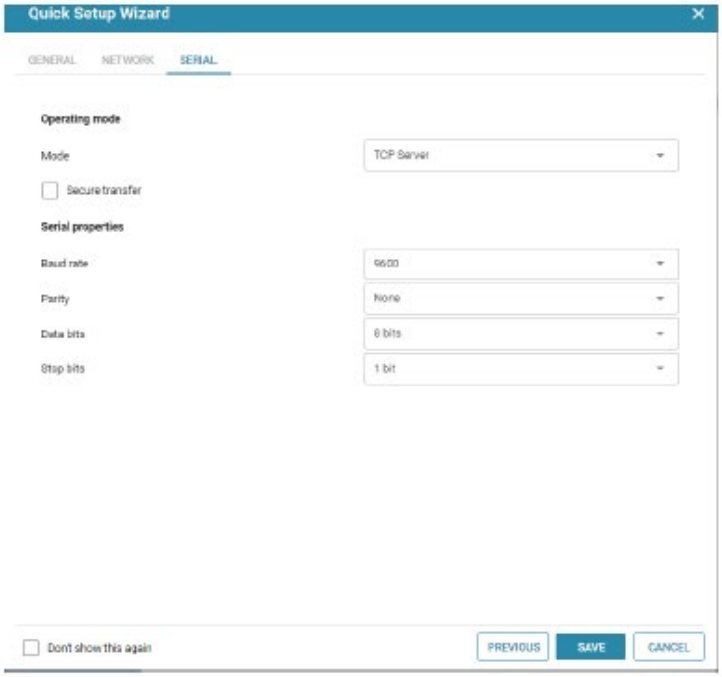
ネットワーク



「ネットワーク」タブでは、セキュアデバイスサーバーのネットワーク設定を定義します。詳細については、p.30「ネットワーク」を参照してください。

シリアル

注意:	「シリアル」タブの設定は、セキュアデバイスサーバーのすべてのシリアルポートに適用されます。



項目	説明
モード	セキュアデバイスサーバーのシリアルポートの操作モードを選択します。「ポート操作モード」を参照してください。
セキュア転送	セキュアなデータ伝送を確認してください。
ボーレート	シリアルポートのデータ転送速度を選択します。
パリティ	送信されたデータの整合性をチェックするために選択します。これは、接続されたシリアルデバイスのパリティ設定と一致させる必要があります。
データビット	1キャラクター分のデータ送信に使用するビット数を選択し、接続されているシリアルデバイスのデータビット設定と一致させます。
ストップビット	キャラクターが送信されたことを示すストップビットを選択し、接続されているシリアルデバイスのストップビットの設定と一致させます。

設定を有効にするには、「**保存**」をクリックしてください。そうすると、セキュアデバイスサーバーにおけるWebコンソールのメイン画面が表示されます。詳細については、「Webコンソール」を参照してください。

第4章
Webコンソール

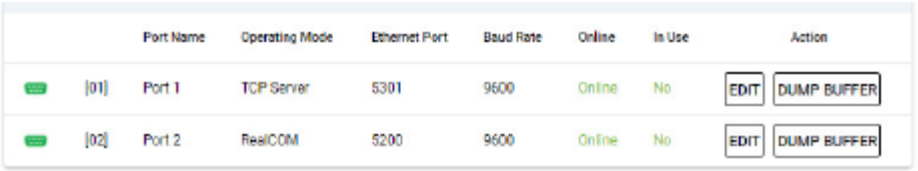
Webインターフェース

セキュアデバイスサーバーのWebインターフェースとそのコンポーネントを以下に示し、説明します:

番号	項目	説明
A	サイドバーメニュー	設定画面の選択インターフェースを提供します。クリックして設定画面を選択するか、サブメニューを展開してください。
B	タスクバー	クイックセットアップウィザード、ユーザー設定(ログアウトを含む)、およびデバイス情報へのアクセスが含まれます。
C	詳細表示パネル	現在選択されている設定画面を表示します。
1	クイックセットアップウィザード	セキュアデバイスサーバーの基本設定を使用します。p.18を参照してください。
2	個人情報	クリックすると、現在ログインしているユーザー、ログイン時間、ユーザー設定オプション、パスワードの変更、ログアウトオプションが表示されます。 インターフェースの言語を変更するには、「環境設定」をクリックしてください。 現在のユーザーアカウントのパスワードを変更するには、「パスワードの変更」をクリックしてください。
3	バージョン情報	クリックすると、デバイスの型番とファームウェアバージョンが表示されます。

シリアルポート

シリアルポート画面には、セキュアデバイスサーバーのシリアルCOMポートの概要(設定や接続されているシリアルデバイスを含む)が表示されます。

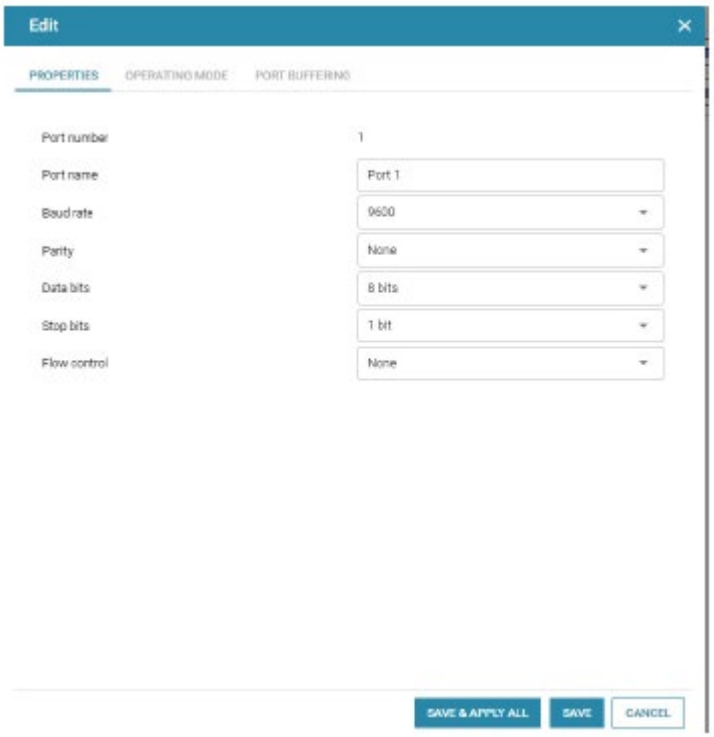


項目	説明
	シリアルポートがオンラインかオフラインかを示します。
ポートネーム	シリアルポートの名前が表示されます。
操作モード	シリアルポートの現在の操作モードを表示します。 25「操作モード」を参照してください。
イーサネットポート	シリアルポートのネットワークポート値を表示します。
ボーレート	シリアルポートのボーレートを表示します。
オンライン	シリアルポートがオンラインかオフラインかを示します。
使用中	シリアルポートにアクティブなデータ送信があるかどうかを示します。
アクション	• 編集:クリックすると、シリアルポートの設定を編集することができます。 • バッファーログ:クリックすると、シリアルポートのポートアクティビティーログがテキストファイルとしてデバイスからダウンロードされます。この機能は、ポートアクティビティーログがデバイスのメモリに保存されている場合にのみ使用できます。p.24「ポートバッファー」を参照してください。 • Telnet/SSH:クリックすると、セキュアデバイスサーバーを設定したり、Telnet/SSHプロトコル経由で接続されたシリアルデバイスにアクセスして操作したりすることができます。この機能は、ポートの操作モードがコンソール管理に設定されている場合にのみ使用できます。「操作モード」(p.25)および「Telnet/SSH」(p.59)を参照してください。 **注意:1箇所のシリアルポートに対する同時接続の最大数は16です。**

シリアルポートの編集

シリアルCOMポートの設定を変更するには、「**編集**」ボタンをクリックしてください。そうすると、「プロパティー」、「操作モード」、「ポートバッファー」の各タブの付いた編集ウィンドウが表示されます。

プロパティー



項目	説明
ポート番号	シリアルポートの番号を表示します。
ポートネーム	シリアルポートの名前を設定します。
ボーレート	シリアルポートのデータ転送速度を選択します。デフォルト= ″9600″
パリティ	選択すると、送信されたデータの整合性をチェックすることができます。これは、接続されているシリアルデバイスのパリティ設定と一致させる必要があります。デフォルト=″None″
データビット	1キャラクター分のデータ送信に使用するビット数を選択し、接続されているシリアルデバイスのデータビット設定と一致させます。デフォルト= ″8″
ストップビット	キャラクターが送信されたことを示すストップビットを選択し、接続されているシリアルデバイスのストップビットの設定と一致させます。デフォルト= ″1″
フローコントロール	データフローの制御方法を選択し、接続されているシリアルデバイスのフローコントロール設定と一致させます。デフォルト=″None″

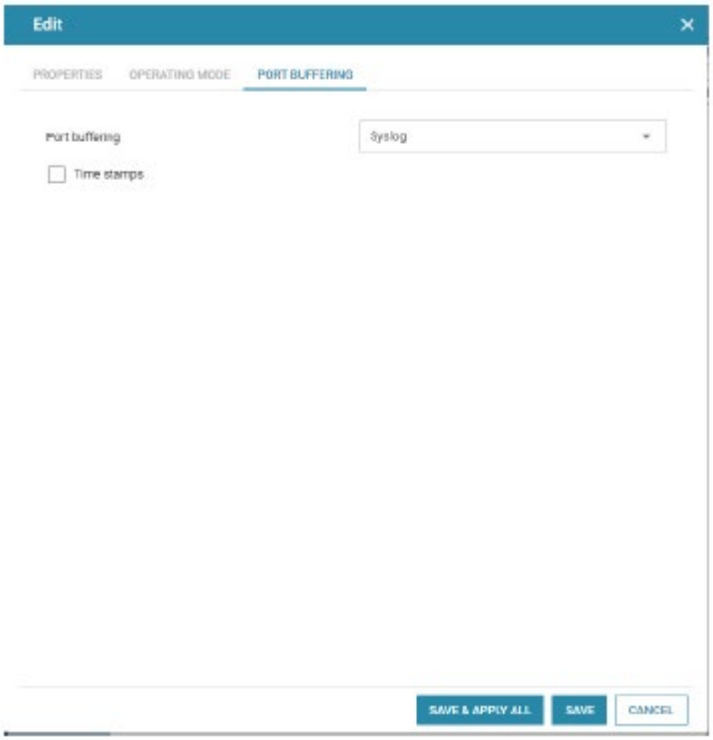
変更を有効にするには、「**保存**」をクリックしてください。

必要に応じて、「**すべて保存して適用**」を選択して、セキュアデバイスサーバーのすべてのシリアルポートに同じ設定を適用してください。

ポートバッファー

ポートバッファー機能は、ポートがアクセスされた時に発生したアクティビティーのログを作成するものです。ログは、セキュアデバイスサーバーの内部メモリー(最大128KB)、またはSyslogサーバーに保存できます。

ポートバッファーを有効にするには、「ポートバッファリング」タブのドロップダウンリストから「**メモリ**」または「**Syslogサーバー**」のいずれかを選択してください。必要に応じて、「タイムスタンプ」の項目にチェックを入れ、作成されたログにタイムスタンプを追加してください。



変更を有効にするには、「**保存**」をクリックしてください。

注意:	**Syslogを選択する前に、Syslogサーバー有効にしてください (p.37「Syslog」参照)。**

必要に応じて「**すべて保存して適用**」をクリックし、セキュアデバイスサーバーのすべてのシリアルポートに対して同じ設定を適用してください。

操作モード

「操作モード」タブでは、セキュアデバイスサーバーのシリアルCOMポートへのアクセス方法を指定します。

注意:	**1箇所のシリアルポートに対する同時接続の最大数は16です。**

各ポートの操作モードの詳細については、第6章「ポート操作モード」を参照してください。

■ リアルCOM

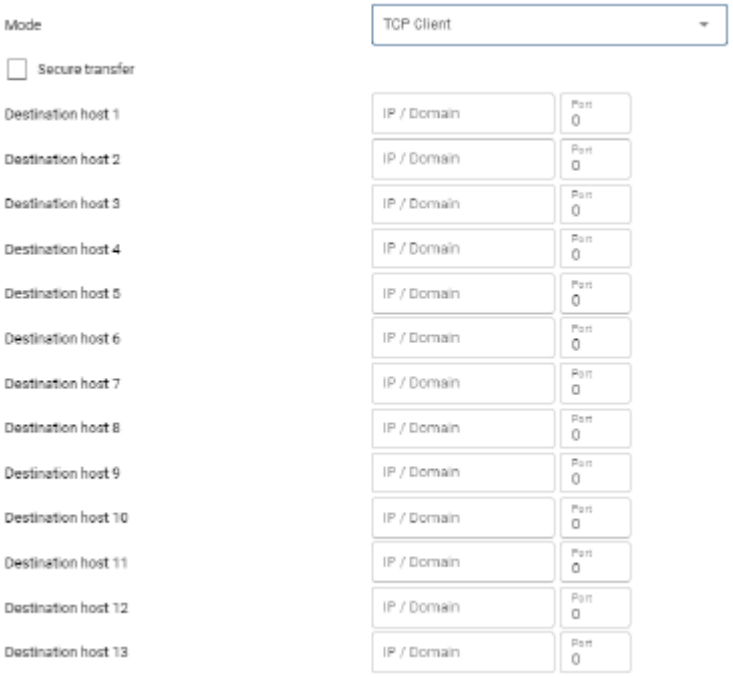
シリアルCOMポート経由でSSLを使用して転送中のすべてのデータを暗号化するには、「**セキュア転送**」にチェックを入れてください。

注意:	**リアルCOMの操作モードは、ATENのバーチャルCOMポートユーティリティーと組み合わせて使用する必要があります。p.66「仮想シリアルポートマネジャー」を参照してください。**

■ TCPサーバー

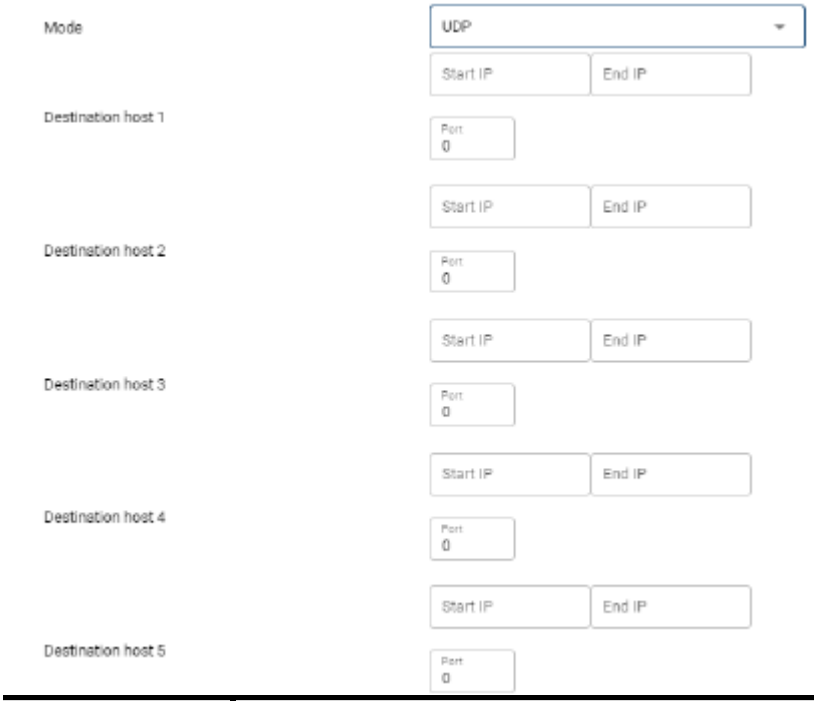
項目	説明
セキュア転送	SSLを使用して、TCPサーバークライアントモードを介してセキュアデバイスサーバーのシリアルCOMポート間で転送されるすべてのデータを暗号化する場合に、チェックを入れてください。

■ TCPクライアント



項目	説明
セキュア転送	SSLを使用して、TCPクライアントサーバーモードを介してセキュアデバイスサーバーのシリアルCOMポート間で転送されるすべてのデータを暗号化する場合に、チェックを入れてください。
送信先ホスト	データ送信先ホストのIPアドレスとサービスポートを入力してください。デバイスは、最大16の送信先ホストに対してデータを同時送信できます。

■ UDP



項目	説明
送信先ホスト	UDPプロトコル経由で宛先ホストに接続するためのIPアドレスの範囲とポート値を入力してください。セキュアデバイスサーバーは、最大16の送信先ホストに対して同時接続できます。

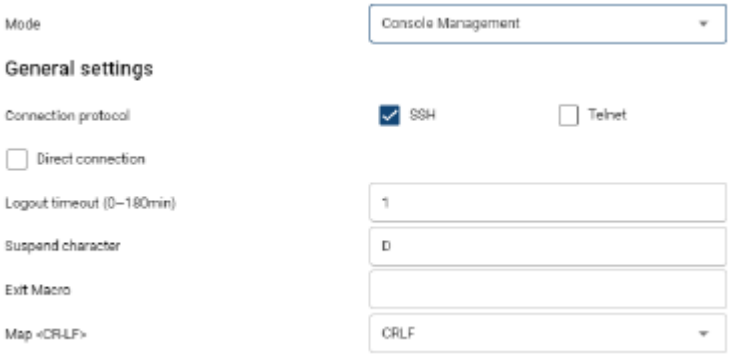
■ シリアルトンネル・サーバー

項目	説明
TCPポート	シリアルトンネル・サーバーとして動作するシリアルポートのTCP/IPポート値を設定します。
セキュア転送	シリアルトンネル・サーバー/クライアントを介して2台のセキュアデバイスサーバー間でシリアルCOMポートを経由で転送されるすべてのデータをSSLで暗号化する場合に、チェックを入れてください。

■ シリアルトンネル・クライアント

項目	説明
宛先	データ送信先のシリアルトンネル・サーバーのIPアドレスとポート値を入力してください。
セキュア転送	SSLを使用して、セキュアトンネル・クライアント/サーバー経由で2つのセキュアデバイスサーバー間でシリアルCOMポート経由で転送されるすべてのデータを暗号化するには、チェックを入れてください。

■ コンソール管理



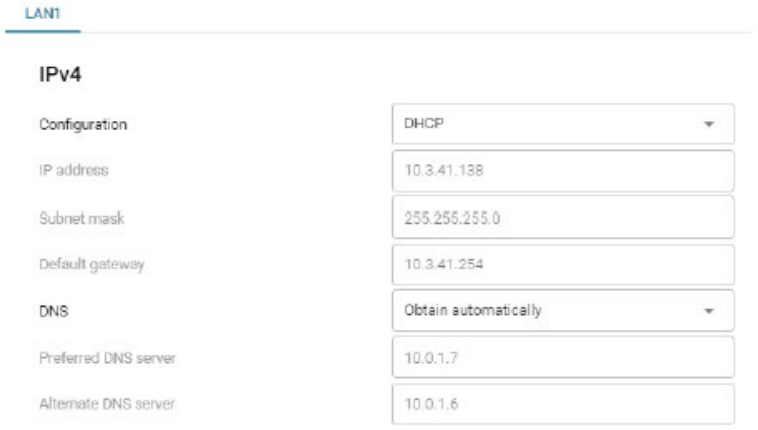
項目	説明
接続プロトコル	SSHおよびTelnet接続プロトコルを有効にする場合はチェックを入れ、無効にするにはチェックを外してください。
ダイレクト接続	コンソール管理ダイレクト操作モードの場合に選択してください。使用可能な各種操作モードの詳細については、第6章「ポート操作モード」を参照してください。
ログアウトタイムアウト(0～180分)	設定された時間、ユーザーによる入力がない場合、自動的にユーザーのアクセスをログアウトします。「0」は、ユーザーが自動的にログアウトされないことを意味します。
サスペンド文字	サスペンド文字は、Telnetセッションでサスペンドメニューを起動する際に用いられます。有効な文字には、H、I、J、Mを除くA～Zが含まれます。
終了マクロ	シリアルデバイス終了時に実行する終了マクロを設定します。
マップ<CR-LF>	キャリッジリターン(CR)および/またはラインフィード(LF)信号を送信する場合に選択してください。

■ 無効

シリアルポートの使用を無効にする場合に選択してください。

ネットワーク

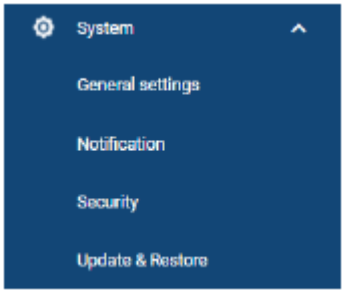
「ネットワーク」画面には、以下の表に記載されているセキュアデバイスサーバーのネットワーク設定が含まれています。



項目	説明
設定	セキュアデバイスサーバーのIPアドレスを設定するための設定タイプを、DHCPまたはスタティックIPから選択してください。
IPアドレス サブネットマスク デフォルトゲートウェイ	スタティックIPの場合は、お使いのネットワーク環境に合わせて、機器のIPアドレス、サブネットマスク、ゲートウェイを設定してください。
DNS	DNSサーバーの取得方法を「自動取得」または「手動設定」から選択します。
優先DNSサーバー 代替DNSサーバー	DNSサーバーを手動で設定するには、デバイスに対する優先DNSサーバーおよび代替DNSサーバーの各アドレスを入力してください。

システム

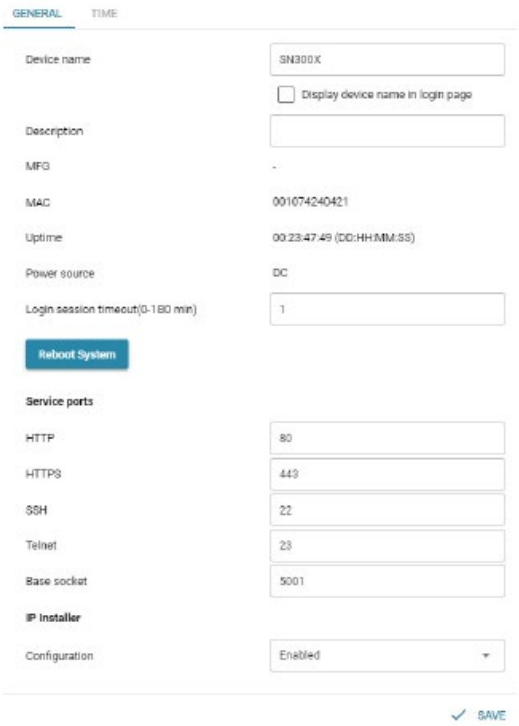
クリックすると、「全般設定」、「通知」、「セキュリティー」、「アップデート＆リストア」を含む、セキュアデバイスサーバーのすべてのシステム関連設定のシステムサブメニューが展開されます。



全般設定

全般設定には、「全般」と「時刻」の2つのタブがあります。

全般



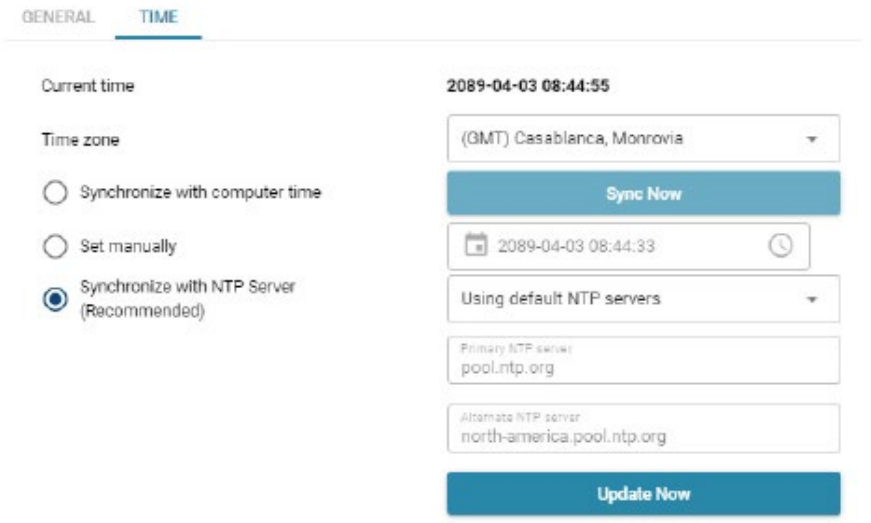
項目	説明
デバイス名	セキュアデバイスサーバーのデバイス名を設定します。
説明	必要に応じて、デバイスの説明を入力します。
MFG	デバイスのMFG(製造番号)を表示します。 **注意:製造番号は、ATENの工場および技術サポートスタッフが必要に応じて製品を識別するために使用する内部シリアル番号です。製品修理や技術的な問い合わせではこの番号ではなく、本体底面のシールに記載されているシリアル番号をご提示ください。**
MAC	セキュアデバイスサーバーのMACアドレスを表示します。
稼働時間	デバイスが稼働している時間が表示されます。
電源	デバイスの現在の電源を表示します。

項目	説明
ログインセッションタイムアウト (0～180分)	設定された時間、セキュアデバイスサーバーのWebインターフェースで実行されたアクションがない場合、ユーザーを自動的にログアウトします。"0" の場合は、ユーザーが自動的にログアウトされないことを意味します。
システムの再起動	セキュアデバイスサーバーを再起動します。
サービスポート	次のサービスポート値を設定します: • HTTP:ブラウザーアクセスに使用されます(デフォルト=80)。 • HTTPS:セキュアなブラウザーアクセスに使用されます(デフォルト=443)。 • SSH:SSHアクセスに使用されます(デフォルト=22)。 • Telnet:Telnetアクセスに使用されます(デフォルト=23)。 • ベースソケット:TCP接続の受信と受け入れに使用されます(デフォルト=5001)。例えば、ベースソケット値が5001の場合、TelnetおよびSSH経由のポート1/2のデバイスのTCPポート値は、それぞれ5001/5002および5101/5102になります。 **注意:** 1. すべてのサービスポートに対する有効なエントリーは1～65535です。 2. サービスポートの設定を変更した場合は、システムの再起動が必要です。
IPインストーラーの設定	これを選択すると、IPインストーラーユーティリティーがセキュアデバイスサーバーのIPアドレスを検出および/または変更できるかどうかを判断します。 • 有効:IPインストーラーは、ユニットのIPアドレスを検出して変更できます。 • 参照のみ:IPインストーラーはユニットのIPアドレスのみを検出できますが、変更することはできません。 • 無効:IPインストーラーはユニットのIPアドレスの検出や変更を行うことができません。

変更を有効にするには、「**保存**」をクリックしてください。

時刻

「時刻」タブには、以下の表で説明するように、セキュアデバイスサーバーの時刻設定が含まれます。



項目	説明
タイムゾーン	次のいずれかを選択して、セキュアデバイスサーバーの時刻を設定してください。 • コンピューター時刻と同期:クライアントPCの時刻と同期します。 • 手動で設定:希望する時刻をデバイスに対して手動で設定します。 • NTPサーバーと同期:NTPサーバーを使用してデバイスの時刻を同期します。 **注意:コンピューターの時刻との同期または手動で設定を使用する場合は、セキュアデバイスサーバーが再起動されるたびに時刻設定を再構成する必要があります。**

通知

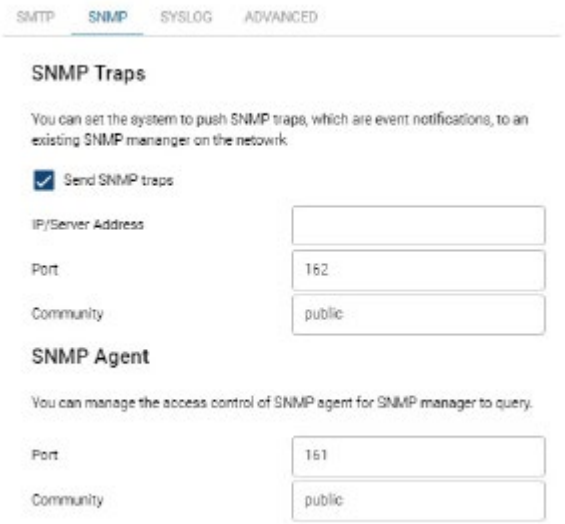
通知画面には、「SMTP」、「SNMP」、「Syslog」、および「詳細」の4つのタブがあります。

SMTP

項目	説明
SMTPサービスを有効にする	「詳細」タブ(p.37参照)で指定されているように、SMTPサービスを有効にし、Eメールでイベント通知を送信するようにするには、この項目にチェックを入れてください。
サーバーアドレス/ポート	SMTPサーバーのアドレスとサービスポートの値を入力してください。
Eメール	送信者のメールアドレスを入力してください。
サーバー認証が必要	SMTPサーバーで認証が必要かどうかを確認し、認証時に有効なユーザーネームとパスワードを入力してください。
宛先	宛先のメールアドレスを入力します。

SNMP

注意:	**SNMPを使用する前に、必ず「システム」>「 セキュリティー」 > 「セキュリティーレベル」でSNMPエージェントサービスを有効にしてください。**



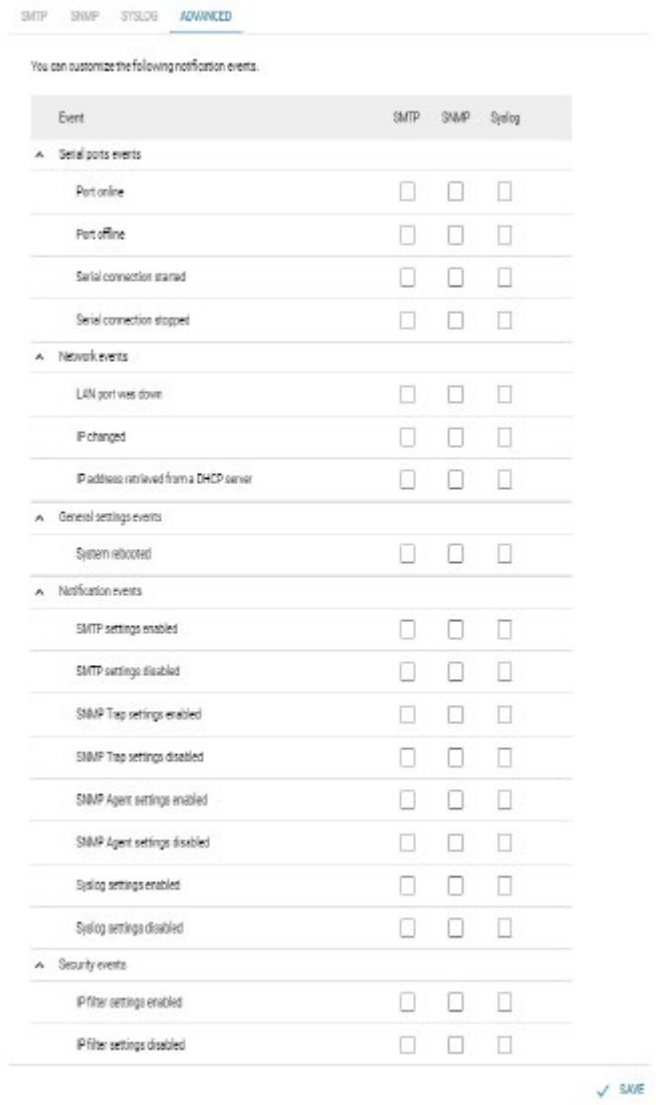
項目	説明
SNMPトラップを送信する	「詳細」タブで指定されているように、SNMPトラップイベント通知を送信するためのSNMPサービスを有効にするには、この項目にチェックを入れてください(p.37参照)。SNMP v1およびv2cがサポートされています。
IP/サーバーアドレス	SNMPトラップイベントを受信するIP/サーバーアドレスを入力してください。
ポート	SNMPトラップイベントを受信するサーバーのサービスポートを入力してください。
コミュニティー	SNMPコミュニティーを入力してください。
SNMPエージェント	SNMPエージェントのサービスポートとコミュニティーを入力してください。

Syslog

項目	説明
Syslogサービスを有効にする	「詳細」タブで指定されているように、Syslogサーバーイベント通知を送信するためにSyslogサービスを有効にするには、この項目にチェックを入れてください(p.37参照)。
サーバーアドレス/ポート	Syslogサーバーのアドレスとポートの値を入力してください。

詳細設定

「詳細」タブでは、SMTP、SNMP、および/またはSyslogサーバー経由で送信されるイベント通知のタイプを設定します。オプションには、以下に示す例が含まれますが、これらに限定されるわけではありません。



これらのイベントが発生したときにSMTP/SNMP/Syslog通知を送信するには、各イベントタイプの横にあるSMTP/SNMP/Syslogチェックボックスにチェックを入れてください。

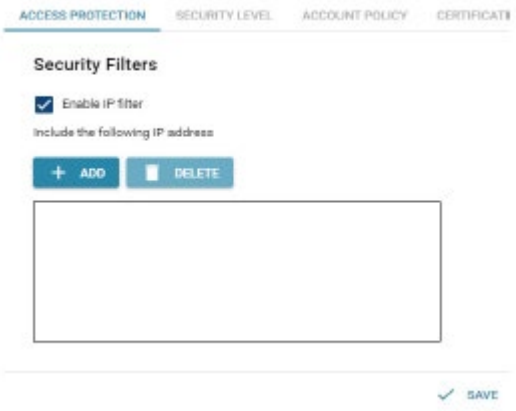
注意:	**指定された通知を送信するには、必要なSMTP/ SNMP/Syslogサービスが適切に設定されていることを確認してください。**

セキュリティー

「セキュリティー」画面には、セキュアデバイスサーバーのセキュリティー設定と証明書情報が含まれ、「アクセス保護」、「セキュリティーレベル」、「アカウントポリシー」、「証明書」の4つのタブに分かれています。

アクセス保護(IPフィルター)

アクセス保護機能は、IPフィルターを設定して、追加されたIPアドレスからのみリモートアクセスを許可し、他のすべてのリモートアクセスを拒否します。



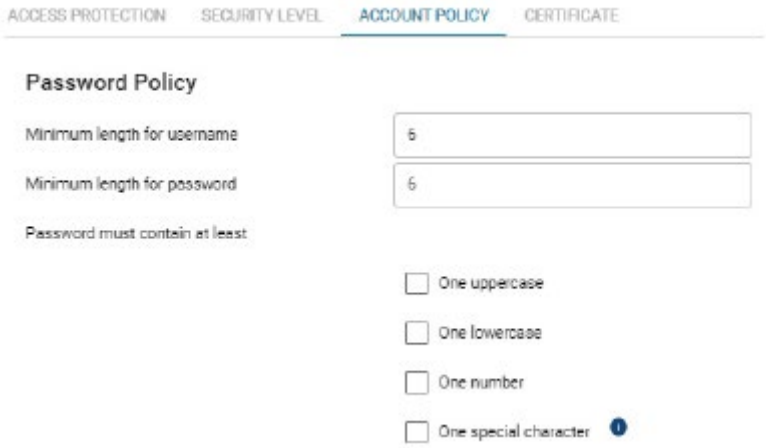
特定のIPアドレスに対してのみ排他アクセスを有効にするには、「**IPフィルターを有効にする**」の項目にチェックを入れて、「**追加**」ボタンを選択し、目的のIPアドレスを追加してください。

変更を有効にするには、「**保存**」をクリックしてください。

セキュリティーレベル

項目	説明
Telnet/SNMPエージェント/ICMP/SSHサービスを有効にする	Telnet/SNMPエージェント/ICMP/SSHサービスを有効にするには、該当する項目にチェックを入れてください。また各種サービスを無効にするには、該当する項目からチェックを外してください。 **注意:SNMPエージェントの設定が変更された場合は、システムの再起動が必要です。**
HTTPを有効にし、HTTPSにリダイレクトする	この項目にチェックを入れると、HTTPが有効になり、すべてのHTTPアクセスがHTTPSに自動的にリダイレクトされ、セキュアなWebブラウザーアクセスが可能になります。 **注意:この設定を変更した場合は、システムの再起動が必要です。**

アカウントポリシー

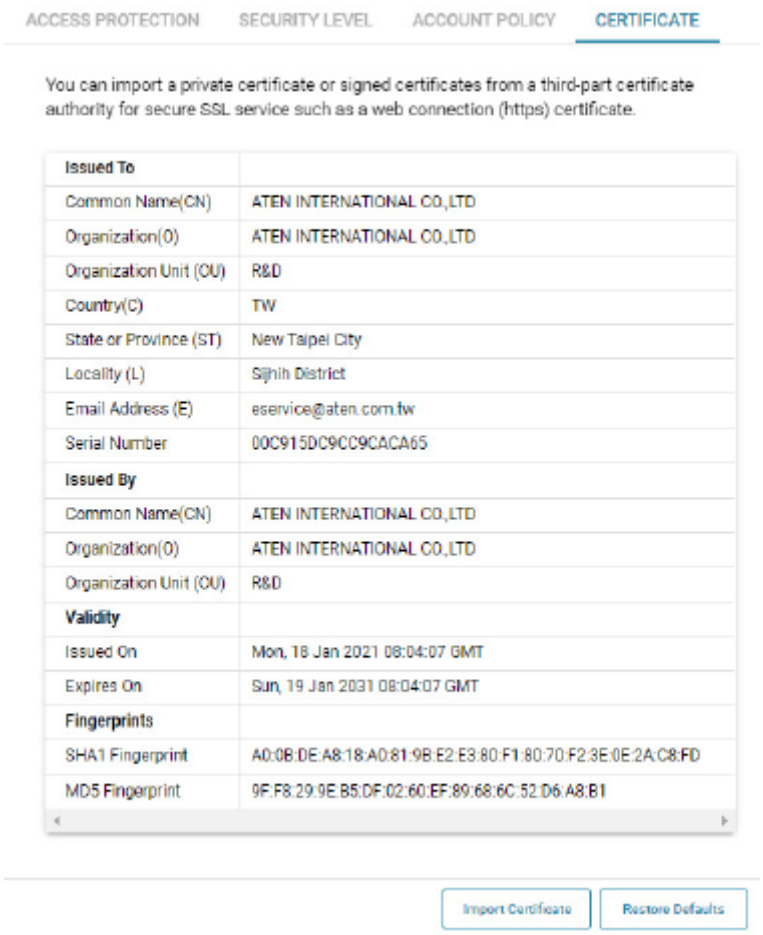


項目	説明
ユーザーネーム/パスワードの最小長	新しく設定されたすべてのログインユーザーネーム/パスワードに必要な最小文字数を設定してください。デフォルト= ″6″
パスワードには以下が必須	新しく設定されたすべてのパスワードに対して、どの文字を少なくとも1つ以上含めるかを設定します。大文字/小文字/数字/特殊文字から必要に応じて、チェックを入れてください。

セキュリティー証明書

「セキュリティー証明書」タブには、使用されているセキュリティー証明書の情報が表示されます。

セキュリティーを強化するために、ユーザーはデフォルトのATEN証明書ではなく、独自のプライベート暗号化キーと署名付き証明書を使用できます。



プライベート証明書を確立するには、2つの方法があります:

- 自己署名済み証明書の作成

  自己署名済み証明書を作成する場合は、「openssl.exe」というフリーツールをインターネットでダウンロードして使うことができます。

- CA署名付きSSLサーバー証明書の取得

  セキュリティーを確保するために、CA(認証局)のWebサイトから取得したサードパーティーのCA署名付きSSL証明書を使用することを推奨します。取得した証明書とそのプライベート暗号化キーは必ずPCに保存してください。

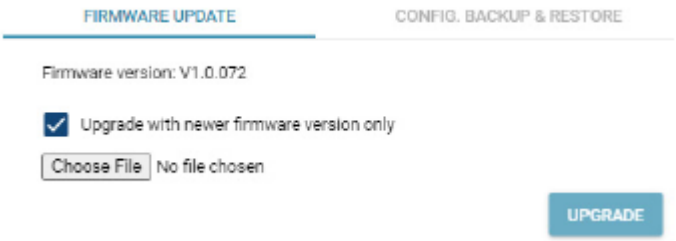
セキュリティーを強化するために、ユーザーはデフォルトのATEN証明書ではなく、独自のプライベート暗号化キーと署名付き証明書を使用できます。

項目	説明
証明書のインポート	PCからプライベートまたはCA署名付きのセキュリティー証明書をインポートします。
デフォルト値のリストア	デフォルトのATEN証明書の使用に戻します。

アップデート＆リストア

「アップデート＆リストア」画面では、セキュアデバイスサーバーのファームウェアのアップグレードや、デバイス設定のバックアップ/リストアを行うことができます。

ファームウェアのアップデート



項目	説明
ファームウェアバージョン	現在のファームウェアバージョンを表示します。
新しいファームウェアバージョンでのみアップグレード	新しいファームウェアバージョンでのファームウェアアップグレードのみを許可するには、この項目にチェックを入れてください。
ファイルの選択	アップグレードに使用するファームウェアファイルを選択してください。
アップグレード	ファームウェアファイルを選択した状態で、デバイスファームウェアをアップグレードします。

バックアップ&リストア

「バックアップ&リストア」画面では、セキュアデバイスサーバーにおける
システム設定のバックアップやリストアを行うことができます。

■ システム設定のバックアップ

セキュアデバイスサーバーのシステム設定をバックアップするには、リストアに使用するパスワードを入力し、「**バックアップ**」をクリックしてください。そうすると、システム設定のバックアップを「System.conf」ファイルとしてPCに保存します。このファイルには、パスワードやユーザー権限などのアカウント関連の設定も含まれます。

■ システム設定のリストア

以前にバックアップしたシステム設定ファイルをリストアするには、そのパスワードを入力し、「ファイルの選択」をクリックしてください。
ファイルを選択してPC上で検索したら、「**リストア**」をクリックしてください。

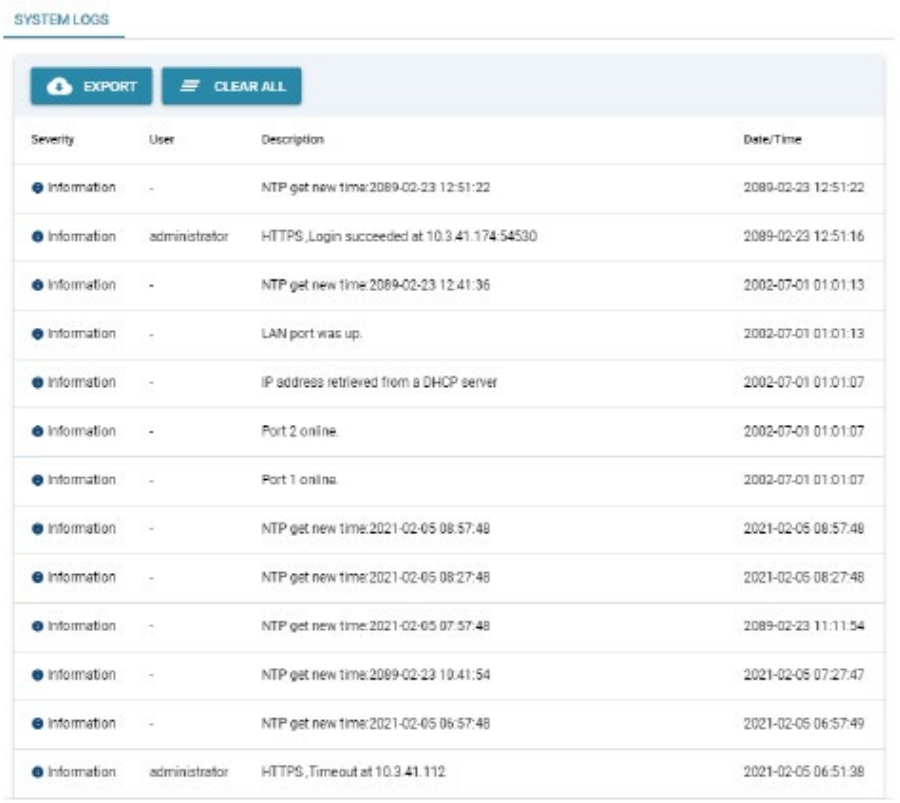
ユーザーアカウント

「ユーザーアカウント」サブメニューは、「ユーザー」画面と「認証サービス」画面から構成されています。ユーザーは、ログインアカウントを追加/編集したり、セキュアデバイスサーバーのユーザーアカウントを管理するためにサードパーティーの認証サービスを利用したりすることができます。

ユーザーアカウントとサードパーティー認証サービスの設定の詳細については、第5章「ユーザー管理」を参照してください。

ログ

「ログ」画面には、セキュアデバイスサーバーにおけるシステムログの情報がすべて一覧表示されます。



項目	説明
エクスポート	ログをPCに「log.txt」ファイルとしてエクスポートし、ダウンロードします。
すべてクリア	すべてのログ情報を消去します。

この画面には、最大2048件のログを保存して表示することができます。

第5章
ユーザー管理

概要

この章では、アドミニストレーターを含むセキュアデバイスサーバーのログインアカウントを追加または編集する方法と、サードパーティーの認証サービスを使用する方法について説明します。

ユーザー

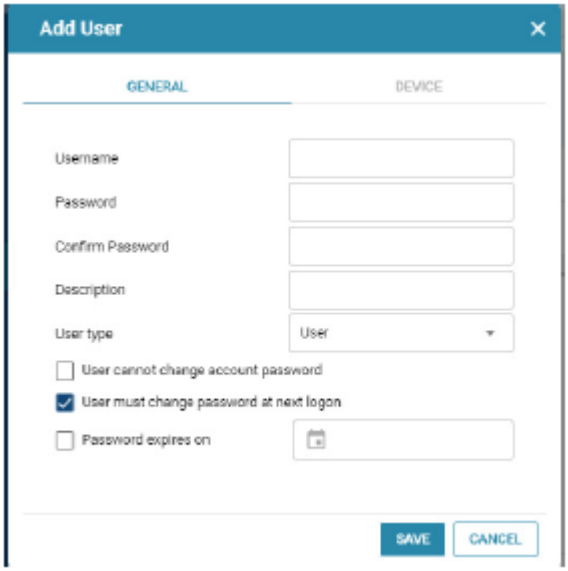
セキュアデバイスサーバーは、次の2種類のユーザーを含む最大16のユーザーアカウントをサポートします:

ユーザータイプ	役割
アドミニストレーター	すべてのシリアルポートへのアクセスと設定、およびその他のログインアカウントの管理が可能です。
ユーザー	アドミニストレーターの許可に従って、許可されたシリアルポートにのみアクセスおよび/または設定が可能ですが、デバイスのシステム設定を行うことはできません。

項目	説明
名前	ユーザーアカウントのユーザーネームを表示します。
タイプ	アカウントの種類(アドミニストレーターまたはユーザー)を表示します。
説明	ユーザーアカウントの説明に使用する追加情報です。
状態	以下を含むユーザーアカウントのステータスを表示します: • 通常:アカウントは通常どおりに機能します。 • パスワード期限付き:アカウントのパスワードには期限が設定されており、定期的に変更する必要があります。

ユーザーの追加

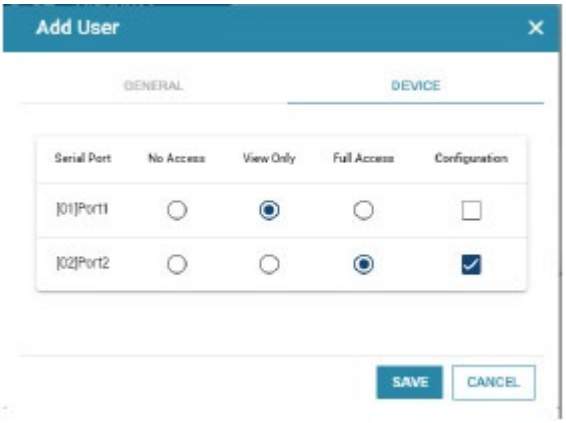
1. セキュアデバイスサーバーのWebインターフェースで、「**ユーザーアカウント**」>「**ユーザー**」>「**ユーザー**」の順にクリックしてください。
2. 「**追加**」ボタンをクリックしてください。そうすると、「ユーザーの追加」ウィンドウの「**全般**」タブが表示されます。次の表の説明に従って、必須項目に値を入力してください。



項目	説明
ユーザーネーム	アカウントポリシーの設定に応じて、1～32文字を使用できます。p.41「アカウントポリシー」を参照してください。
パスワード	アカウントポリシーの設定に応じて、1～16文字を使用できます。p.41「アカウントポリシー」を参照してください。
パスワードの確認	「パスワード」項目に合うように、確認用パスワードを入力してください。
説明	ユーザーに関する付加情報があれば、この欄に入力してください。
ユーザータイプ	フルアクセスと設定の権限が与えられている「アドミニストレーター」を選択するか、設定されているシリアルポートのアクセス権と設定権のみが許可されている「ユーザー」を選択してください。
ユーザーはアカウントパスワードの変更不可	ユーザーによるアカウントのパスワードの変更を制限するには、この項目にチェックを入れてください。
ユーザーは次回ログイン時にパスワード変更が必須	次回ログイン時にユーザーにパスワードの変更を要求する場合にチェックします。

項目	説明
パスワードの有効期限	ログインアカウントのパスワードの有効期限が切れる日付を指定し、再定義します。 **注意:ユーザーのパスワードの有効期限が切れても、旧パスワードでログインできますが、ログイン時に強制的に変更されます。**

3. タイプが「ユーザー」の場合のみ – 「**デバイス**」タブをクリックし、下の表の説明に従って、各シリアルポートのアクセスおよび/または権限の設定を許可してください。



項目	説明
アクセス不可	シリアルポートへのアクセスを制限する場合に選択してください。
参照のみ	TelnetおよびSSHセッションを制限しながら、シリアルポートへの参照アクセスのみを許可する場合に選択してください。
フルアクセス	シリアルポートへのフルアクセスを許可する場合に選択してください。
設定	シリアルポートの設定が可能である場合に選択してください。 この設定には、プロパティー、操作モード、ポートバッファーの各設定が含まれます。詳細はp.23「シリアルポートの編集」を参照してください。

4. 「**保存**」をクリックして完了してください。
5. 操作に成功すると、メッセージボックスに「オペレーション成功」と表示されます。そうしたら、ダイアログの「**OK**」ボタンをクリックして、操作を終了してください。

ユーザーの編集

ユーザーアカウントを編集するには、そのアカウントを選択して「**編集**」をクリックしてください。

「ユーザーの編集」ウィンドウで、p.48「ユーザーの追加」を参考にしながら変更を行い、「**保存**」をクリックしてください。

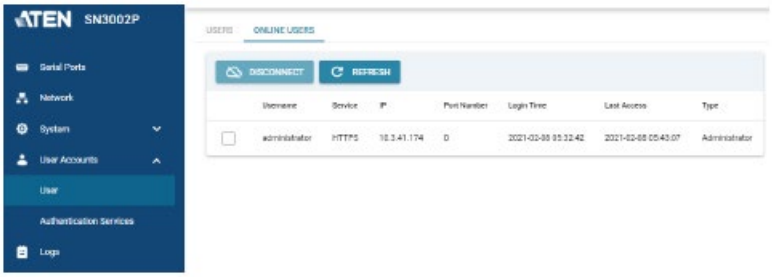
ユーザーの削除

ユーザーアカウントを削除するには、ユーザーアカウントを選択して「**削除**」をクリックしてください。

「削除しますか?」と尋ねられたら、「**OK**」をクリックして確認してください。

オンラインユーザー

「オンラインユーザー」タブには、現在セキュアデバイスサーバーにアクセスしているユーザーアカウントが表示されます。



アドミニストレーターは、現在ログインしている他のユーザーアカウントを選択するかどうかを確認し、「**切断**」を選択して、それらのユーザーのアクセスセッションを終了することができます。

認証サービス

セキュアデバイスサーバーでは、外部のサードパーティー認証サービス、つまりRADIUSを使って、ユーザーアカウントの管理と認証を行うことができます。

注意:	**RADIUSを認証に使用する場合、PAPのみがサポートされます。**

このようなサービスを有効にするには、Webインターフェースで「ユーザーアカウント」>「認証サービス」を選択します。

RADIUS

1. RADIUSによる認証を使用するには、以下の表を参照して、セキュアデバイスサーバーでサービスを有効にしてください。

項目	説明
優先サーバーIP/アドレスとサーバーポート	プライマリー(優先)RADIUSサーバーのIPアドレスとサービスポートを入力してください。
代替サーバーIP/アドレスとサーバーポート	代替RADIUSサーバーのIPアドレスとサービスポートを入力してください。
タイムアウト	セキュアデバイスサーバーがRADIUSサーバーを待機する時間を秒単位で設定してください。
再試行	RADIUSが再試行できる回数を設定してください。
共有シークレット(6文字以上)	セキュアデバイスサーバーとRADIUSサーバー間の認証に使用する文字列を入力します。

2. RADIUSサーバーで、次の表に示す属性情報に従って、それぞれのアクセス権を設定してください。

属性	説明
u	(User)ユーザーには、一部のポートにアクセスして設定する権限があります。この属性は、デバイスにアクセスするすべてのユーザーに対して指定する必要があります。
T	(True)ユーザーには、この属性が指定されたポートにアクセスして設定する権限があります。
F	(False)ユーザーはポートを設定できません。
A	(All)ユーザーには、すべてのポートにアクセスして設定する権限があります。

例:

U,T,1

ユーザーはポート1に対して、アクセス権限と設定権限が与えられています。

注意:	**1. 文字は大文字と小文字を区別しません。つまり、大文字でも小文字でも同じように動作します。また、複数の文字はカンマで区切ってください。** **2. 文字列に無効な文字が含まれていると、ユーザーのセキュアデバイスサーバーに対するアクセスが禁止されます。**

第6章
ポート操作モード

概要

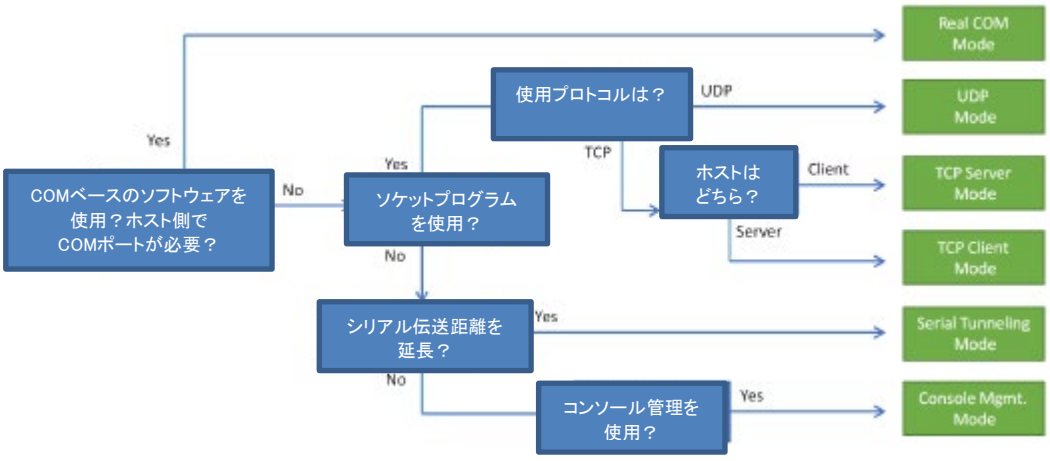
幅広いシリアルアプリケーションに対応できるよう、セキュアデバイスサーバーのCOMポートは複数のポート操作モードをサポートしています。

これらには、シリアルからイーサネットへの接続用のリアルCOM、TCPサーバー&クライアント、UDP、およびシリアルトンネルサーバー&クライアントの各種モード、コンソール管理、およびデバイス制御用のコンソール管理ダイレクトが含まれます。また、COMポート、シリアルトンネル、またはTCP/UDPソケット機能が必要なアプリケーションも含まれます。

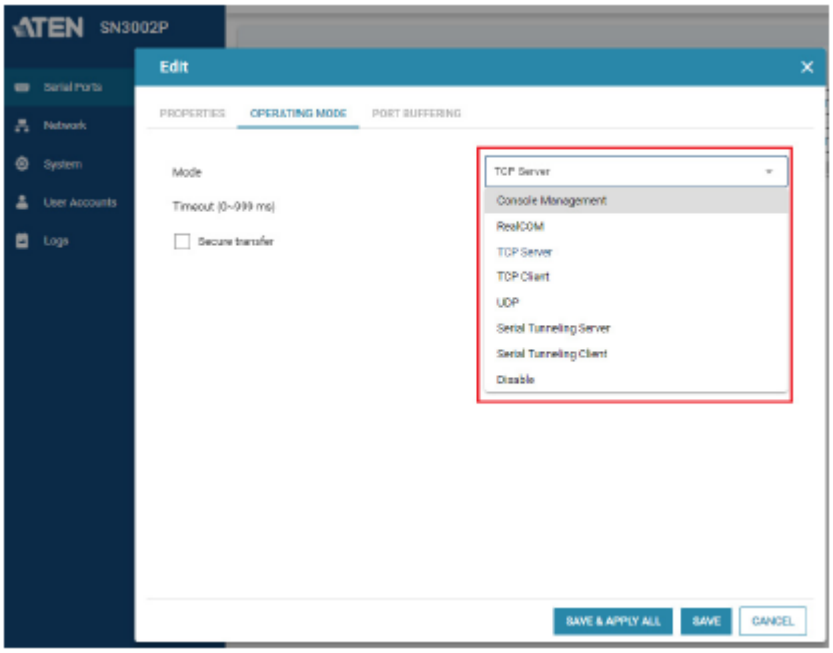
注意:	**1箇所のシリアルポートに対する同時接続の最大数は16です。**

操作モードの選択

以下に、操作モードを選択する際に考慮すべきいくつかの質問を示します。



操作モードは、下に示すように、「シリアルポート」>「編集」>「操作モード」から選択できます。



この画面から、セキュアデバイスサーバーのシリアルポートを、使用可能な各種ポート操作モードに設定することができます。詳細は後続のセクションで説明します。

操作モード

シリアルポートの操作モードを設定するには、p.25「操作モード」を参照してください。

リアルCOM

このモードは、リモートPCにインストールされている仮想COMポートドライバーと一緒に使用されます(第9章「仮想シリアルポートマネージャー」を参照)。セキュアデバイスサーバーのCOMポートがこのモードに設定されている場合、接続されているデバイスは、リモートPCのCOMポートに直接接続されているかのように表示されます。

このモードは、純粋なシリアル通信アプリケーション用に書かれたソフトウェアをユーザーが使用できるため、POS端末、バーコードリーダー、シリアルプリンターなどのデバイスで有用です。.

セキュアデバイスサーバーには、Windowsシステム用のリアルCOMドライバー(バーチャルサーバーポートユーティリティー)とLinuxシステム用のTTYドライバーが付属しています。

TCPサーバー&クライアント

TCP(Transmission Control Protocol)は、ソケットプログラミングを使ってTCPプロトコル上でシリアルデータを通信するのに、信頼性の高いトランスポート層を提供します。

TCPサーバー

TCPサーバーモードでは、データ転送が双方向で行われます。このモードでは、ホストコンピューターが著作権保護機能を持つデバイスとの通信を開始し、シリアルポートに対して接続のリクエストを行います。

接続が確立すると、ホストはシリアル機器から送られたデータを受信します。この時点から、ホストとデバイス間で両方向にデータを送信できます。この操作モードでは、SSLデータ暗号化がサポートされています。

著作権保護機能を持つデバイスは、このモードにおいて最大16台のホストコンピューターからの同時接続に対応しています。これによって、複数のコンピューターがシリアル機器と同時に通信することが可能になります。

注意:	**「全般設定」画面で指定されている「ベースソケット」の項目が、デバイスがリッスンするポートに対応していることを確認してください。セキュアデバイスサーバーでデフォルト設定されているポート番号は5001です(p.32「全般」参照)。**

TCPクライアント

TCPクライアントモードでは、セキュアデバイスサーバーはシリアルポートでシリアルデータを受信した際に、ホストコンピューターとの接続を開始し、ホストへのシリアルデータの送信を開始します。
セキュアデバイスサーバーは最大16台のホストコンピューターに同時にデータを送信できます。また、この操作モードではSSLデータ暗号化をサポートします。

シリアルポートの操作モードの設定については、p.25「操作モード」を参照してください。

シリアルトンネル・サーバー/クライアント

シリアルトンネルでは、イーサネットを介した2つのセキュアデバイスサーバー間のダイレクト接続を確立し、クライアントとサーバーの関係で動作します。
片方のデバイスはシリアルトンネル・クライアントとして指定され、もう片方のデバイスはシリアルトンネル・サーバーとして指定されます。

注意:	**この設定では、どちらのデバイスをクライアントまたはサーバーとして指定しても構いません。**

2台のうち1台のCOMポートはコンピューターのCOMポートに接続し、もう1台のCOMポートはアクセスするシリアルデバイスに接続します。
2台のユニットはIPアドレスとポートアドレスを介して相互に通信し、SSLデータ暗号化をサポートします。
ポートアドレスは、「全般設定」ページの「ベースソケット」の項目によって設定されます。詳細はp.32「全般」を参照してください。

UDPモード

UDP(User Datagram Protocol)モードは、TCPよりも、より早く、そして、より効率的に通信を行います。UDPモードでは、通信は双方向で行われます。シリアル機器はセキュアデバイスサーバーのCOMポートを介して、最大16台のホストコンピューターとデータの送受信を行うことができます。

TCPが実行する完全な方法ではエラーチェックを実行しないため、UDPは、データ精度に最適化された低速のTCPよりもリアルタイムアプリケーション(メッセージ表示など)に適しています。

コンソール管理

コンソール管理では、接続されているシリアルデバイスを管理および制御するために、ユーザーがセキュアデバイスサーバーに対してTelnetおよび/またはSSHセッションを確立することができます。ユーザーは、TelnetまたはSSH経由で、またはTelnet、SSH、またはPuTTY経由でリモートからJava SNビューワー アプリケーションを使用してログインできます。

注意:	**1. 「全般設定」画面で指定されたベースソケットエントリーが、デバイスがリッスンするポートに対応していることを確認してください。5001は、セキュアデバイスサーバーのデフォルト設定です(p.32「全般」参照)。** **2. このモードにおいて、セキュアデバイスサーバーは、Ciscoコンソールケーブル(DB-9→RJ45)を使用してCiscoネットワークスイッチに接続することもできます。**

コンソール管理ダイレクト

コンソール管理モードのダイレクトオプションが有効になっている場合、ユーザーはWebブラウザー経由でログインする必要はなく、PCからセキュアデバイスサーバーに接続されたシリアルデバイスにTelnetまたはSSHセッションを直接確立することができます。ユーザーは、PCから直接Telnet SSHまたはPuTTYを使用して、接続されたシリアルデバイスにログインできます。

シリアルポートの操作モードの設定については、p.25「操作モード」を参照してください。

無効

このモードにおいて、セキュアデバイスサーバーのシリアルポートは無効になります。

シリアルポート操作モードの設定については、p.25「操作モード」を参照してください。

第7章
ポートアクセス

概要

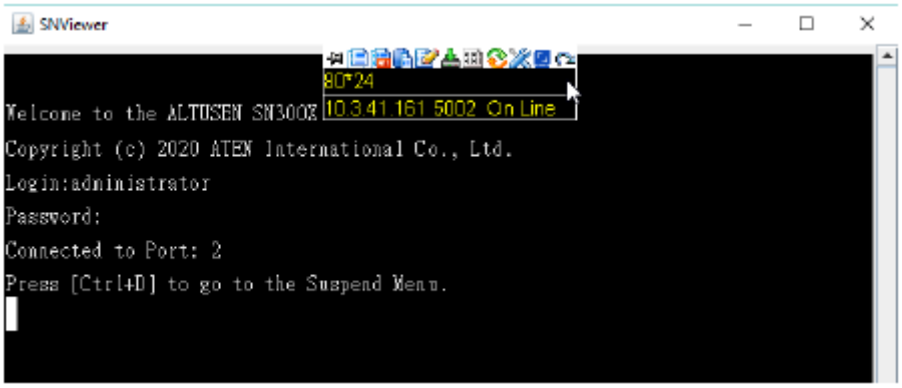
セキュアデバイスサーバーのWebインターフェースにログインすると、シリアルポート画面が表示されます。以下で説明するボタンを使用して、デバイスのシリアルCOMポートにアクセスし、制御を行ってください。

ボタン	機能
EDIT	シリアルポートの設定を編集します。p.23「シリアルポートの編集」を参照してください。
TELNET	SNビューワーを使用してセキュアデバイスサーバーとのTelnetセッションを開き、その設定メニューにアクセスするか、シリアルデバイスをそのCOMポートに接続します。詳細は、p.59「Telnet/SSH」を参照してください。
SSH	SNビューワーを使用してセキュアデバイスサーバーとのSSHセッションを開き、その設定メニューにアクセスするか、シリアルデバイスをCOMポートに接続します。詳細は、p.59「Telnet/SSH」を参照してください。
DUMP BUFFER	シリアルポートのポートアクティビティーログ(最大128KB)をファイル「log.txt」としてダウンロードします。p.24「ポートバッファー」を参照してください。

注意:	**ユーザーが実行を許可されている機能のボタンだけがアクティブになります。**

Telnet/SSH

セキュアデバイスサーバーの設定メニュー、またはTelnetまたはSSH経由でCOMポートに接続されているシリアルデバイスにアクセスするには、「シリアルポート」画面にある「**Telnet**」または「**SSH**」ボタンをクリックしてください。そうすると、Javaアプリケーション（SNビューワー）が起動し、以下に示すようにTelnet SSHセッションが開きます。

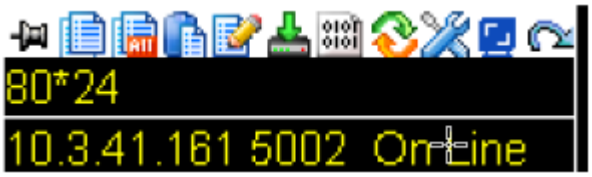


注意：	1. **SNビューワーを実行するには、JRE8がインストールされている必要があります。** 2. **Telnet/SSHボタンを表示するには、セキュアデバイスサーバーのCOMポートをコンソール管理モードに設定する必要があります（p.25「操作モード」を参照）。**

SNビューワー

SNビューワーは、Telnet/SSHプロトコルを介してWeb上のセキュアデバイスサーバーに接続されたシリアルデバイスにアクセスするために使用されるJavaアプリケーションです。

マウスカーソルをSNビューワーの上に移動すると、コントロールパネルが表示されます。コントロールパネルは、アイコン行と2つのテキスト行の3行で構成されています。



- デフォルトでは、上側のテキスト行にはウィンドウの幅と高さが表示されます。コントロールパネルのアイコンの上にマウスカーソルが移動すると、上部のテキスト行の情報が変わり、そのアイコンの機能が示されます。
- 下の行には、アクセスしているデバイスのIPアドレスとポート、および現在の接続ステータスが表示されます。

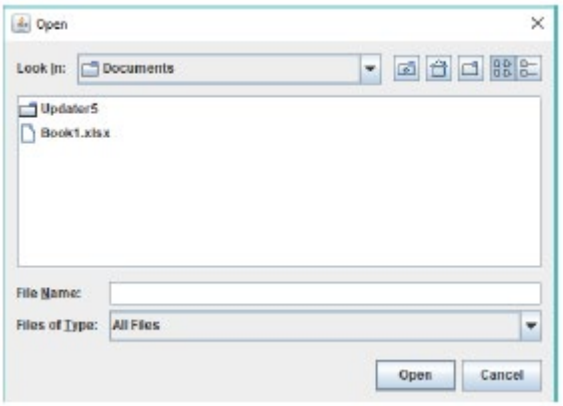
コントロールパネルの機能

コントロールパネルの機能については、以下の表とその後のセクションで説明します。

アイコン	機能
	コントロールパネルのピン止め/ピン止め解除を行います。ピン止めすると、常に上に表示します。また、ピン止めを解除すると自動非表示モードで表示されます。
	選択したテキストを画面にコピーします。
	画面に表示されているすべてのテキストをコピーします。
	コピーした文字を貼り付けます。
	ログオン/ログオフを切り替えます。これは、シリアル機器からSNビューワーに送られたテキスト形式のログファイルを開始します。最初にテキストベースのログファイルを作成してインポートする必要があります(p.46「ログ」参照)。
	インポートするデータファイルを参照します(p.61「データのインポート」参照)。
	ページのエンコーディングを変更します(p.61「エンコード」参照)。
	ターミナルをデフォルト設定にリセットします。
	SNビューワーのフォント、色、その他の表示設定を変更します(p.61「ターミナル設定」を参照)。
	SNビューワーのウィンドウ幅の調整を行います。
	ビューワーを終了します。

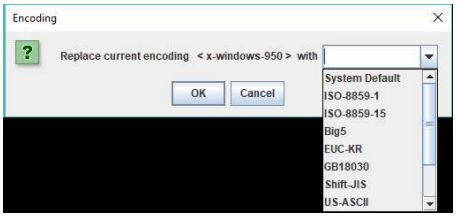
データのインポート

「データのインポート」オプションは、以下に示すように、データファイルをインポートするための標準的なブラウザメニューを開きます。



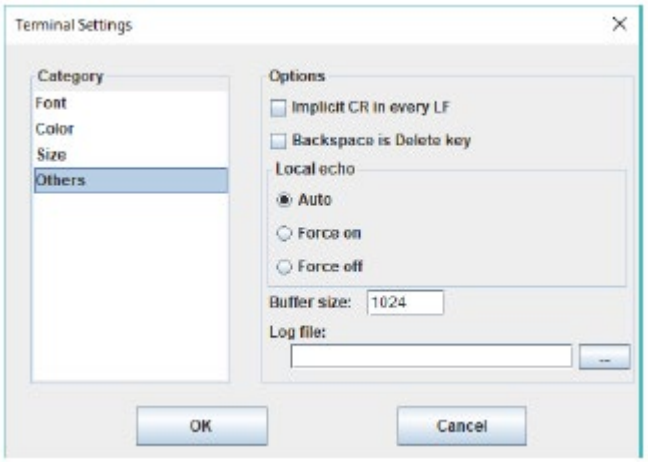
エンコード

「エンコード」オプションは、以下に示すように、使用するエンコーディングのタイプを選択します。



ターミナル設定

「ターミナル設定」オプションを使用すると、ユーザーはターミナルセッションの表示パラメーターと設定を次のように変更できます。



カテゴリー	説明
フォント	フォントの種類、サイズ、スタイルなど、SNビューワーのフォント設定を行います。右側に設定例が表示されます。
色	フォアグラウンド、バックグラウンド、カーソルテキスト、カーソルの色を変更します。色の詳細設定を行う場合は、「HSL」、「見本」、「HSV」の各タブを使用してください。タブの下には、色の変化がどのように見えるかを確認できる「**プレビュー**」があります。 変更を保存するには「**OK**」を、変更を削除して終了するには「**キャンセル**」を、デフォルトの色設定に戻すには「**リセット**」を、それぞれクリックしてください。
サイズ	ウィンドウのサイズによって、表示される情報の量が決まります。列サイズと行サイズを設定して、SNビューワーのウィンドウサイズを変更してください。
その他	このセクションは、次の下記の設定を行う際に使用します。 ◆ すべてのLFで暗黙的CR:このチェックボックスをONにすると、[Enter]キーを使用した場合にキャリッジリターンが追加されるため、カーソルは左マージンに揃えて戻されます。[Enter]キーを押した後でテキストが左側の余白で1行にならない場合は、この機能を使ってください。 ◆ 削除キーには、バックスペースを使用します。 ◆ ローカルエコー:エコーとは、シリアル機器から入力された文字列の応答のことです。 ➢ **自動:**入力された文字列がエコーされますが、画面には表示されません。 ➢ **強制ON:**入力された文字列がエコーされ、入力されると画面にも表示されます。有効にするとパスワードが表示されます。 ➢ **強制OFF:**文字列はシリアル機器からエコーされません。 ◆ バッファーサイズ:ログファイルの最大容量です。 ◆ ログファイル:ログファイルは、接続されたシリアル機器からSNビューワーに送られるテキストベースのログを生成します。ログは事前にノートやMicrosoft Wordなどの外部エディターを使ってテキストファイルとして作成して開いておく必要があります。次に、SNビューワーのコントロールパネルからログオンを有効にする必要があります(p.60「コントロールパネルの機能」参照)。

第8章
リモートターミナル操作

概要

セキュアデバイスサーバーは、以下のセクションで説明するように、Telnet、SSH、またはPuTTYなどのいくつかの方法を介してリモートターミナルセッション経由でアクセスできます。

ターミナルログイン

ユーザーは、Webブラウザーを使用する以外に、Telnet、SSH、PuTTYなどのテキストベースのターミナルアプリケーションを使用してリモートでログインすることもできます。

Telnetによるログイン

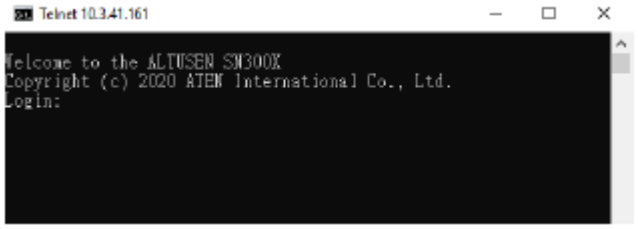
ターミナル(コマンドライン)セッションを開始し、セキュアデバイスサーバーのIPアドレスを次の形式で入力してください:

telnet[IPアドレス]

[Enter]を押してください。

注意:	**デフォルトのTelnetポートは23です。セキュアデバイスサーバーのCOMポートに接続されているデバイスを制御するには、メインメニューを開くのではなく、全般設定のベースソケットエントリーで設定されているポート番号を指定してください(p.32「全般設定」参照)。次に例を示します。** **telnet 192.168.0.60 5001**

そうすると、ログインプロンプトが表示されます:



初回ログインの場合は、デフォルトのユーザーネーム「administraror」とパスワード「password」をそれぞれ入力し、[Enter]キーを押してログインしてください。

SSHログイン(Linux)

ターミナル(コマンドライン)セッションを開始し、セキュアデバイスサーバーのIPアドレスを次の形式で入力してください:

ssh[ユーザーネーム@IPアドレス]

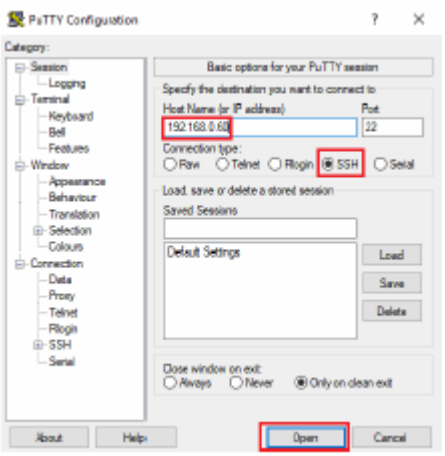
[Enter]を押してから、セキュアデバイスサーバーのパスワードを入力してログインしてください。

注意:	**デフォルトのSSHポートは22です。メインメニューを開くのではなく、セキュアデバイスサーバーのCOMポートに接続されているデバイスを制御するには、「全般設定」(p.32参照)の「ベースソケット」エントリーによって取得されたポート番号を指定してください。** **例は次のとおりです:sshadministrator@192.168.0.60-P5001**

サードパーティーユーティリティー(Windows)

SSHセッションは、Win32およびUnixプラットフォーム用のTelnetおよびSSHの無料実装であるPuTTYなどのサードパーティーユーティリティーを使用して、Windowsでもアクセスできます。PuTTY経由でSSH接続を行うには、次の手順を実行します:

1. 「ホスト名」に、セキュアデバイスサーバーのIPアドレスを入力してください。



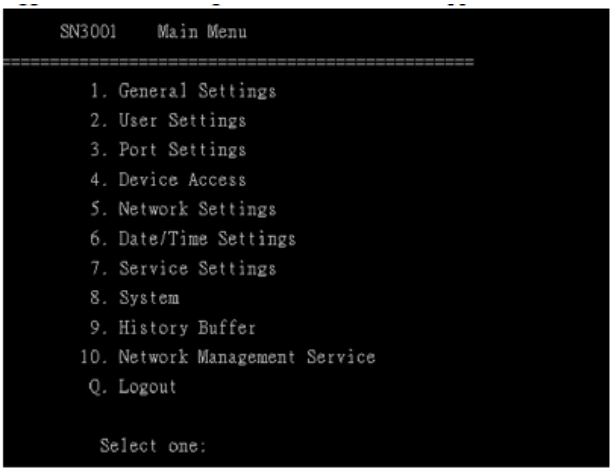
2. プロトコルでSSHを選択したら、「開く」をクリックしてください。

3. 接続が完了したら、セキュアデバイスサーバーにログインするための有効なユーザーネームとパスワードを入力してください。

注意:	**ログインに失敗した場合、SSHプロトコルでは再試行は許可されません。PuTTYを閉じてからやり直す必要があります。**

ターミナルのメインメニュー

ログインすると、次のテキストベースのメインメニューが表示されます。



ターミナルセッションのメインメニューには、先に説明したWebブラウザー版と同様のテキストベースの設定が含まれていますが、ファームウェアのアップグレードや設定のバックアップとリストアを実行できないなど、いくつかの制限があります。

サブメニューの操作方法については、ブラウザー版で提供される情報(p.21「Webコンソール」を参照)を参照してください。

注意:	**ブラウザー版と同様に、これらのサブメニューの大半のアクセスは、アドミニストレーターまたはCOMポートアクセス権限を持つユーザーに制限されます。許可されていないサブメニューを選択しても、何も起こりません。**

セキュアデバイスサーバーに接続されているシリアルデバイスのターミナルにアクセスしたい場合は、「4.デバイスアクセス」からポートを選択するとご利用いただけます。

注意:	**接続されたシリアルデバイスにアクセスするには、シリアルポートの操作モードをコンソール管理に設定する必要があります(p.25「操作モード」参照)。**

ターミナルセッションを閉じるには、メインメニューを呼び出し、[Q]を押してログアウトしてください。次に、ウィンドウを閉じてください。

第9章
仮想シリアルポートマネージャー

概要

セキュアデバイスサーバーには、Windows用の仮想COMポートドライバー、Linux用のリアルTTYドライバー、およびOpenServer、Solaris、FreeBSD、AIX、Mac用の固定TTYドライバーが用意されています。

PCでドライバーを実行すると、セキュアデバイスサーバーのCOMポートに接続されているデバイスが、そのPCのCOMポートに直接接続されているかのように表示されます。

注意:	**シリアルポートの操作モードは、仮想ポートとして設定するために、リアルCOMとして設定する必要があります(p.21「操作モード」参照)。**

データ転送は、PCの仮想COMポートと、セキュアデバイスサーバーのCOMポートに接続されているデバイスとの間において、イーサネット経由で行われます。

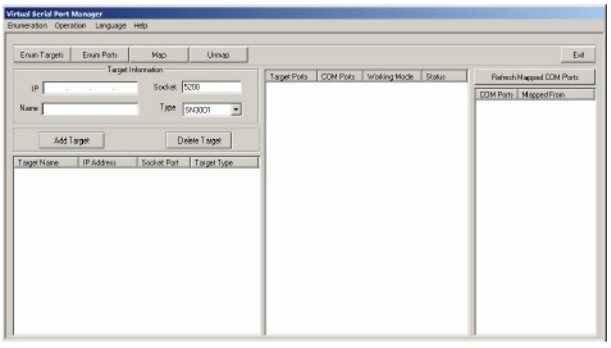
ユーザーは、自分のPCのOSに対応するドライバーを、セキュアデバイスサーバーの製品Webページからダウンロードしてインストールできます。

リアルCOMポート管理 – 仮想シリアルポートマネージャー

仮想シリアルポートマネジャーは、COMポートのマッピングに便利なインターフェースを提供するユーティリティーです。

注意:	**仮想シリアルポートマネジャーは、Windowsおよび、カーネル4.15.0–43および4.2.0–27のLinuxのみをサポートします。Linuxシステムの他のバージョンについては、p.72「リアルCOM ポート管理 – Linuxコマンド」を参照してください。**

仮想シリアルポートマネジャー(「スタート 」>「仮想ポート管理ユーティリティー」>「仮想シリアルポートマネジャー」)を起動してください。次のダイアログボックスが表示されます。



ユーティリティーインターフェース

仮想シリアルポートマネジャーのインターフェースは、次のようにレイアウトされています:

- メニューおよびボタンバーは、デバイスおよびポートの自動列挙と一覧表示を可能にします。
- メニューバーとボタンバーの下には、自動列挙の方法ではターゲットデバイスが表示されない場合に、デバイスを手動で一覧表示するために必要な情報を入力する欄があります。
- 列挙または手動入力によって検出されたすべてのデバイスは、左側のパネルに一覧表示されます。
- 選択したデバイスで見つかったすべてのポートは中央パネルに列挙されます。
- 右側のパネルには、作成された仮想COMポートマッピングが表示されます。

メニューとツールバー

仮想シリアルポートマネジャーメニューとツールバーは、同じ機能で構成されています。ユーザーは、メニュー項目またはボタンをクリックして、下の表に記載されているように、目的の機能を呼び出すことができます。

項目	アクション
ターゲットの列挙	この機能は、LAN内のすべてのSNデバイスを検索し、一覧表示します。 – これらには、セキュアデバイスサーバーとATENシリアルコンソールサーバーが含まれます。結果は「ターゲットリスト」パネルに表示されます(詳細については、p.68「ターゲットリスト」参照)。ターゲットリストに表示されているすべてのデバイスは、削除機能が呼び出された場合に削除されることに注意してください。 削除機能を呼び出す前に、削除しないデバイスをリストから必ず除外してください。
ポートの列挙	この機能は、ターゲットリストで現在選択されているターゲットデバイスにおける既存のポートを一覧表示します。結果は、「ポートリスト」パネルに表示されます。
マッピング	「ポートリスト」パネルからポートを選択した後、この機能を選択すると、デバイスのCOMポートがユーザーのPCの仮想COMポートにマッピングされます。
マッピング解除	「マッピング済みポート」リストからポートを選択した後、この機能を選択すると、PCとデバイスのCOMポート間のマッピングが削除されます。

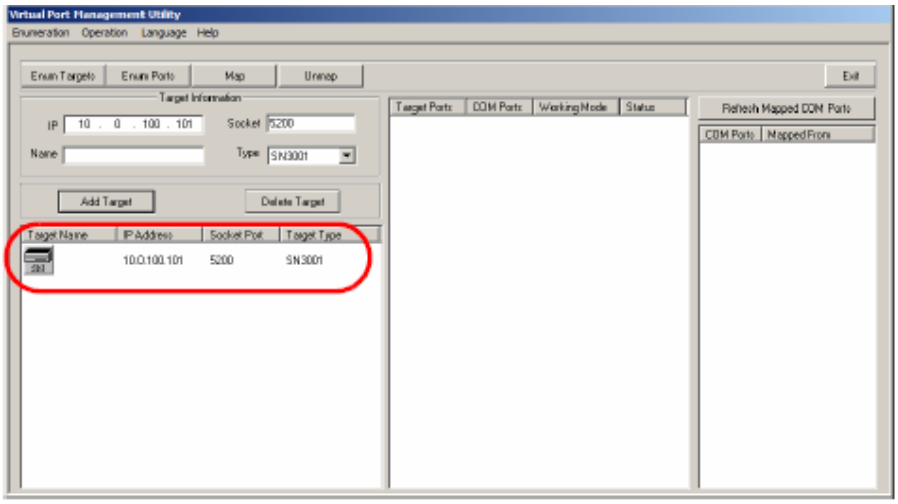
ターゲット情報

「ターゲット情報」項目では、以下で説明するように、オフラインのターゲットデバイスに対してポートを割り当てる(マッピングする)ことができます。

項目	アクション
ターゲットIPアドレス	COMポートをマッピングするターゲットのIPアドレスを入力してください。
ベースソケットポート	ターゲットデバイスのベースソケットポートです。リアルCOMポート操作の場合、デフォルトのベースソケットポートは5200です。
ターゲット名	ターゲットの名前です。ターゲットの実際の名前と異なる場合は、実際の名前に置き換えられます。名前はマッピング/マッピング解除プロセスに関連しないことに注意してください。関連するのは、IPアドレス、ソケットポート、ターゲットタイプのみです。
ターゲットタイプ	マッピングされるターゲットのタイプです。SN3001/SN3002およびATENシリアルコンソールサーバーは、有効なターゲットタイプです。 **注意:SN3001にはSN3001Pが含まれ、SN3002にはSN3002Pが含まれます。**
ターゲットの追加	上記の情報に基づいて、ターゲットリストにエントリーを作成します。
ターゲットの削除	現在選択されているターゲットをターゲットリストから削除します。

ターゲットリスト

左側のパネルには、列挙機能で検出されたデバイスおよび「ターゲット情報」欄で手動追加されたデバイスがすべて表示されます。



注意:	**リスト内の項目をダブルクリックすると、「ポートの列挙」を選択した場合と同じ機能が呼び出され、「ポートリスト」列に選択したターゲットのポートの数と操作モードが表示されます。**

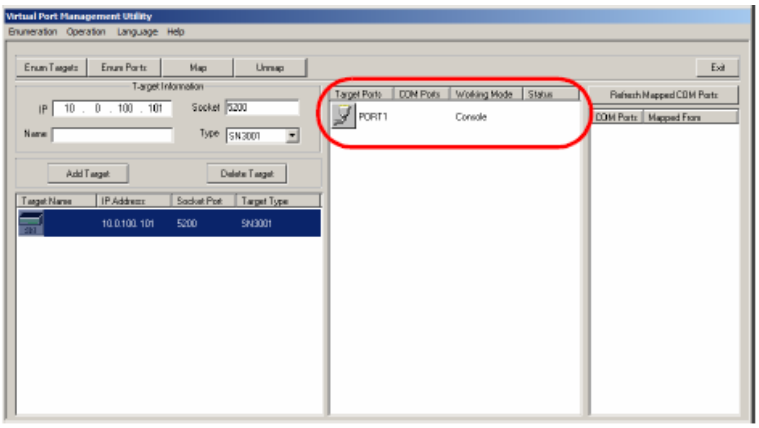
- 列挙処理の結果としてデバイスが自動的に一覧表示された場合、その左側のアイコンが緑色のドットと線で描画されます。これは、ターゲットがオンラインで、マッピングの準備ができていることを示しています。
- デバイスが手動でリストに追加され、オフラインの場合、左側のアイコンは黒い点と線で描画されます。手動で追加された項目をダブ

ルクリックすると、その情報がポートリストに表示されますが、操作モード情報は正確ではなく、すべてのデバイスのポートがリアルCOMモードであると想定する必要があります。ポートモードの詳細については、p.25「操作モード」を参照してください。

- ターゲットがオフラインである場合、またはオンラインではあるもののポートの列挙を要求して2秒以内に応答しない場合、操作モード情報は正確ではなく、すべてのデバイスのポートがリアルCOMモードであると想定する必要があります。ポートモードの詳細については、p.25「操作モード」を参照してください。

ポートリスト

このリストには、選択したターゲットのポート情報が表示されます(一度に選択できるターゲットは1つだけです)。



1. 左側の列にはターゲットのポート番号、2番目の列にはマッピング先のCOMポート(存在する場合)、3番目の列にはその操作モード、右側の列にはそのステータスが表示されます。

注意:	**操作モードは、シリアルポートが設定されている操作モードを示します。詳細はp.25「操作モード」を参照してください。**

2. ポートリストでポートをダブルクリックすると、「ポートのマッピング」ダイアログボックスが表示されます。マッピングの詳細については、p.70「ポートのマッピング」を参照してください。

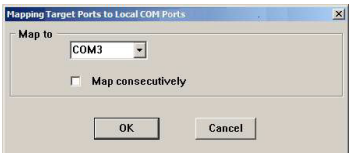
注意:	**「ポートのマッピング」ダイアログボックスは、ツールバーの「マッピング先」、またはメニューの「マッピング先」をクリックして呼び出すこともできます。**

ポートのマッピングとマッピング解除

ポートのマッピング

仮想COMポートをマッピングするには:

1. ポート一覧にある対象項目をダブルクリックすると、「ポートのマッピング」ダイアログボックスが表示されます:

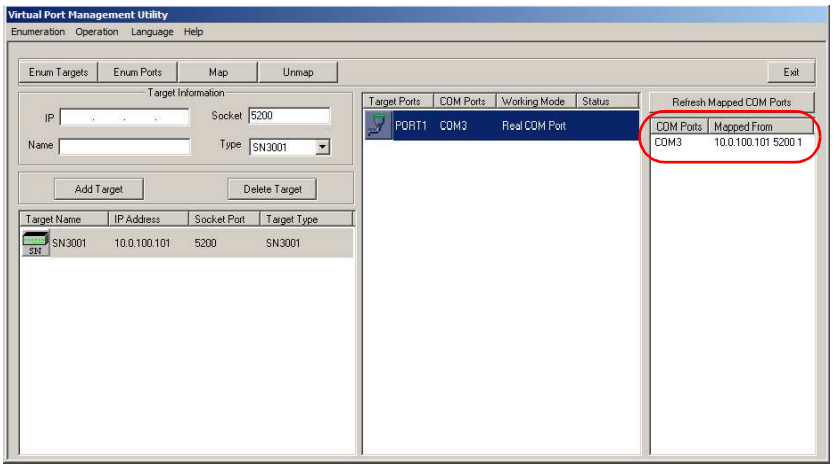


2. ドロップダウンリストから、ターゲットポートをマッピングするCOMポートを選択してください。
3. 「**OK**」ボタンをクリックしてください。

注意:	**警告ダイアログボックスが表示された場合は、無視しても問題ありません。操作を完了するには、「続行する」をクリックしてください。**

マッピングされたCOMポート

仮想ポート管理の右端のパネルには、マッピングされたCOMポートが表示されます。エントリーは、アプリケーションが起動するとすぐに生成され、マッピングされたCOMポート設定が、作業と削除の結果として変更されるたびに更新されます。

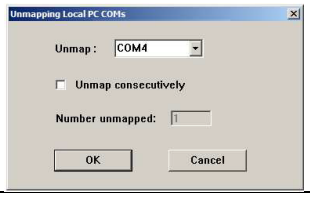


Windowsシステムでは、最大256個のポートをマッピングできます。

ポートのマッピング解除

仮想COMポートのマッピングを解除するには、次の手順を実行します:

1.マッピングされたCOMポート(右端のパネル)を選択して、「ポートのマッピング解除」ダイアログボックスを表示します:



注意:	**ダイアログボックスが表示されない場合は、ボタンバーの「マッピング解除」をクリックするか、メニューから「マッピング解除」を選択してください。**

2.「OK」をクリックして操作を完了してください。

仮想ポートのマッピング/マッピング解除

仮想ポートをマッピングまたはマッピング解除するには、次の手順を実行してください:

1. rootで、/usr/lib/AtenVPortディレクトリーに移動してください。
2. 次のコマンドを発行してください:

   /AtenVPMapping

この処理は、インタラクティブモードまたは高速モードのどちらでも実行できます。インタラクティブモードでは、コマンドラインでパラメーターを指定する必要はありません。ユーザーは、プログラムの実行時に生成された質問に基づいて、マッピング/マッピング解除の選択を行います。

高速モードでは、次の例に示すように、ユーザーはコマンドラインでパラメーターを指定して、マッピング/マッピング解除のオプションを示す必要があります:

1. マッピング(入力はすべて1行に収めてください):

   ./AtenVPMapping map(1) PCポート(0-255) ターゲットIP(a.b.c.d)

   ターゲットポート(1～48) マッピング数(1～48)

2. マッピング解除(入力はすべて1行に収めてください):

   ./AtenVPMapping unmap(0) PCPort(0～255) NumberofUnMapping(1～48)

Linuxシステムでは、最大256個のポートをマッピングできます。

仮想ポートの命名規則

Linux配下のすべてのATEN SN仮想ポートには、接頭辞ttyaが付いています。

マッピングされた仮想ポートは/devディレクトリーにあります。これらはすべて、ttyaというプレフィックスを持ちます。
(ttya000、ttya001など)。範囲はttya000～ttya255です。

付録

安全にお使いいただくために

全般

- 製品に同梱されるドキュメントは全てお読みください。またドキュメント類は全て保存してください。
- 本製品は、屋内での使用に限ります。
- また、弊社Webサイトに掲載のオンラインユーザーマニュアルもご確認ください。
- 落下による事故・製品の破損を防ぐため、設置場所は不安定な面(台車、簡易的なスタンドやテーブル等)を避けるようにしてください。
  装置が落下すると、深刻な損傷が生じます。
- 製品が水に濡れるおそれのあるような場所で使用しないでください。
- 製品は熱源の近く、またはその熱源の上などで使用しないでください。
- 製品のケースには必要に応じて通気口が設けられています。通気口のある製品は、安定した運用を行うため、また製品の過熱を防ぐために、開口部を塞いだり覆ったりしないでください。
- 製品をベッドやソファ、ラグなどの柔らかいものの上に置かないでください。開口部が塞がれ、適切な通気が確保できずに製品が過熱するおそれがあります。
- 製品にいかなる液体もかからないようにしてください。
- 電源プラグを電源コンセントから抜く場合は、乾いた雑巾でプラグ周りのホコリを掃除してください。液体やスプレー式のクリーナーは使用しないでください。お手入れには、湿らせて固く絞った布を使用してください。
- 製品はラベルに記載されたタイプの電源に接続して運用してください。電源タイプについて不明な場合は、購入された販売店もしくは電気事業者にお問い合わせください。
- お使いの装置への損傷を避けるために、すべての装置を適切に接地するようにしてください。
- 電源ケーブルやケーブルの上に物を置かないでください。人が通行するような場所を避けて電源ケーブルを設置してください。
- システムケーブルや電源ケーブルは丁寧に取り扱ってください。これらのケーブル類の上には何も置かないようにしてください。
- 危険な電源ポイントへの接触やショートによって、発火したり感電したりするおそれがありますので、キャビネットの空きスロット等に押し込まないようにしてください。危険な電圧ポイントに触れたり、部品がショートしたり、火災や電気的な衝撃の危険性がある場合があります。
- 装置をご自身で修理せず、ご不明な点がございましたら技術サポートまでご相談くださいすべての保守については、適格な保守担当者に問い合わせてください。

- ホットプラグ対応電源装置に電源を接続または切断する場合は、次のガイドラインに従ってください:
  - 電源ケーブルを接続する前に、パワーサプライのセットアップを行ってください。
  - パワーサプライを取り外す前に電源ケーブルを抜いてください。
  - お使いのシステムが複数のパワーサプライをお使いである場合、パワーサプライからすべての電源ケーブルを抜いてお使いのシステムから切り離してください。
- 下記の現象が発生した場合、コンセントからはずして技術サポートに修理を依頼してください。
  - 電源ケーブルが破損した。
  - 装置の上に液体をこぼした。
  - 装置が雨や水に濡れた。
  - 装置を誤って落下させた、ないしはキャビネットが破損した。
  - 装置の動作に異変が見られる。(修理が必要です)
  - 製品マニュアルに従って操作しているにもかかわらず、正常に動作しない。
- 修理が必要となる故障が発生するおそれがありますので、製品マニュアルに従って操作してください。他のコントロールの不適切な調整は、修理する資格のある技術者による広範な作業を必要とする損傷をもたらす可能性があります。
- ソケットコンセントは装置の近くに設置し、容易にアクセスできるものとします。

DC電源

- デバイスは、ショート、過電流、およびアース(接地)障害に対して保護されるように、建物設備の保護装置に依存しています。建物設備の保護装置がシステムを保護するために適切に評価され、国および地域の規則に準拠していることを確認してください。
- すぐにアクセスできる取り外し可能なデバイスが、建物の設備配線に組み込まれていることを確認してください。
- 本製品には保護接地ターミナルが別に設けられています。これを、常に接地されている状態にしておいてください。
- DC電源回路には、UL、AWMVW-1Style1015、最小16AWG、最小105° C、最小300Vの認証を受けたDC電源ケーブルを選択してください。
- 注意:この装置は、DC供給回路の接地導線を、装置の接地導線に接続できるように設計されています。この接続を行う場合は、以下の条件をすべて満たしている必要があります。⚠
  - 本装置は、直流電源アース極導線、または直流電源アース極導線が接続されている接地用バーやバスからのボンディングジャンパーに直接接続するものとします。
  - 本製品は、同一直流電源回路の接地線と接続し、かつ直流系統の接地点を接続する他の製品と同一直近(隣接する筐体など)に配置するものとします。DCシステムは、どこにも接地しないでください。
  - DC電源は、この装置と同じ構内に設置する必要があります。
  - 装置の切替や切断は、直流電源と接地極導線の接続点との間の接地回路導線内で行わないでください。
- **警告:このユニットは、アクセスが制限されている場所に設置することが想定されています。アクセス制限エリア(サーバールーム、データセンターなど)とは、専用の工具、鍵、またはその他のセキュリティー手段を使用して、保守担当者のみがアクセスできる場所であり、その場所を担当する権限に管理されています。**

ラックへのマウント

- ラックでの作業を始める前に、スタビライザーがラックに固定され床に接していること、また、ラック全体が安定した場所に置かれていることを確認してください。作業する前に、シングルラックにフロントとサイドのスタビライザーを取り付けるか、結合された複数のラックにフロントスタビライザーを取り付けてください。
- ラックには下から上に向かって、一番重いアイテムから順番に取り付けてください。
- デバイスを拡張する前にラックが水平で安定していることを確認してください。
- デバイスレールのリリース用ラッチを押しながらデバイスをスライドさせてラックに出し入れする際にはスライドレールに指を挟まないようにご注意ください。
- デバイスがラックに挿入されたら、慎重にレールをロックする位置までスライドしてください。
- ラックに供給するAC電源の分岐回路が過剰供給にならないようご注意ください。ラック全体の電源負荷は分岐回路の80%を越えないように設定する必要があります。
- ラックにマウントされたデバイスは、電源タップも含め、すべて正しく接地されていることを確認してください。
- ラックへの通気を十分に確保してください。
- 本製品で定められている保管温度を超えないように、ラックが設置されている場所の室温を調節してください。
- ラックに設置されているデバイスが動作している際に、デバイスを踏んだりデバイスによじ登ったりしないでください。

仕様

機能			仕様
コネクター	シリアル		DB-9ピン オス×1(Black) DB-9 オス×1(Black、SN3002/SN3002Pのみ)
	ネットワーク		RJ-45 メス×1(Black)
	電源	PWR1	DCジャック×1(Black)
		PWR2	3極ターミナル×1(Green)
		PWR3	RJ-45PoE、 IEEE802.3af×1(SN3001P/SN3002Pの み)
スイッチ	リセット		ピンホール型スイッチ×1
LED	電源		1(Green)
	状態		(Yellow Green/Red) ×1
	ポート1/ポート2		(Green/Orange)×1 (Green/Orange)×1 (SN3002/SN3002Pのみ)
	10 / /100Mbps		1(Green) 1(Orange)
電源入力	電源ジャック		9V DC
	電源ターミナル		9～48V DC
	PoE		DC 48V (SN3001P/SN3002Pのみ)
消費電力		SN3001	DC9V:0.634W:3BTU DC48V:0.804W:4BTU
		SN3002	DC9V:0.769W:4BTU DC48V:0.939W:4BTU
		SN3001P	DC9V:0.805W:4BTU DC48V:0.975W:5BTU PoE:1.22W:6BTU
		SN3002P	DC9V:0.94W:4BTU DC48V:1.11W:5BTU PoE:1.39W:7BTU

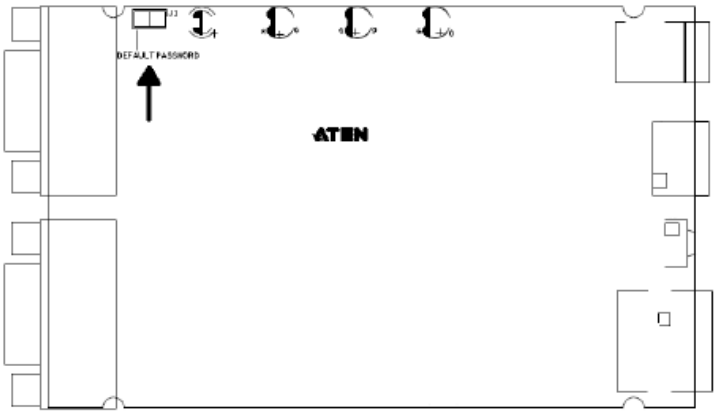
インターフェース	シリアル	標準	RS-232C
		ボーレート	110, 134, 150, 300, 600, 1200, 1800, 2400, 4800, 7200, 9600, 19200, 38400, 57600, 115200, 230400, 460800, 921600
		RS-232C信号	TxD,RxD,RTS,CTS,DTR,DSR,DCD ,GND
		パリティ	なし、偶数、奇数、マーク、スペース
		データビット	5, 6, 7, 8
		ストップビット	1, 1.5, 2
		フロー コントロール	RTSi CTS,DTR/DSR,XON i XOFF,None
	ネットワーク	標準	10i100BaseTX;自動認識
		保護	1.5KVマグネティック・アイソレーション
		プロトコル	ARP,DHCP,DNS,HTTP,HTTPS,ICMP,IP,TCP,UDP,NTP,PPP,RADIUS,Telnet,SNMP,SNMP Trap,SMTP,SSH
規格準拠		EMC	EN55032i35
		EMI	CISPR32,FCC Part15B Class A
		EMS	IEC61000-4-2ESD:Contact:4kV;Air8kV IEC61000-4-3RS:80MHz～1GHz3Vim IEC61000-4-4EFT:Power:1kV;Signal:0.5kV IEC61000-4-5 Surge:Power:2kV(Power Adapter), 1kV(Terminal Block); Signal:1kV IEC61000-4-6CS:150kHz to10MHz3Vim;10 kHz to30MHz:3to1Vim;30kHz to80MHz1Vi m IEC61000-4-8PFMF IEC61000-4-11DIP
		Safety	UL60950-1およびUL62368-1規格準拠
		指令	
環境	動作温度		0～60℃
	保存温度		-40～75℃
	湿度		5～95% RH、結露なきこと
ケース	ケース材料		メタル
	重量	SN3001	0.20 kg
		SN3002	0.21 kg
		SN3001P	0.21 kg
		SN3002P	0.22 kg
	サイズ(W×D×H)		9.80×11.7×2.60cm

ログイン情報の消去

管理者によるログインを(ログイン資格情報の破損や消失などの理由で)実行できない場合、次の手順を実行してログイン情報を消去できます。

注意:	**この手順を実行すると、すべての設定が工場出荷時のデフォルトに戻ります。**

1. セキュアデバイスサーバーの電源を切り、ケース上蓋を横面のネジをドライバーを使って取り外してください。
2. ジャンパーキャップを使って、J1(DEFAULT PASSWORD)とラベルの付いたジャンパーをショートさせてください。



3. セキュアデバイスサーバーの電源を入れてください。
4. ステータスLEDが点滅したら、デバイスの電源をOFFにしてください。
5. J1からジャンパーキャップを取り外してください。
6. ケースを元に戻し、機器に電源を入れてください。
   電源を投入すると、デフォルトの管理者ユーザーネームとパスワードを使用してログインできます。p.16「ログイン」を参照してください。

この手順を実行すると、初回ログイン時にパスワードの変更を求めるプロンプトが表示されます。

トラブルシューティング

操作上の問題は、様々な原因が考えられます。解決するための最初の手順は、すべてのケーブルがしっかりと接続され、ソケットに完全に装着されていることを確認することです。

また、製品のファームウェアをアップデートすると、以前のバージョンがリリースされてから検出され、修正された問題が解決される場合があります。製品で最新のファームウェアバージョンが実行されていない場合は、アップグレードすることを強く推奨します。アップグレードの詳細については、p.43「ファームウェアのアップデート」を参照してください。

更新日:2021-04-21