Simply Better Connections

SN1100CO / SN1100COD / SN0100CO / SN0100COD / SN9100CO シリーズ

シリアルコンソールサーバー ユーザーマニュアル

本書 日本語マニュアルについて

この日本語マニュアルはATEN International Co., Ltdが作成している英語版ユーザーマニュアルを、日本国内のお客様が製品をご使用になる上での便宜を図るため、ATENジャパン株式会社にて機械翻訳ベースで作成したドキュメントです。用語・表現などは公開前に人為的な修正を加えておりますが、若干の表記ゆれなどが残っている可能性がございますので、ご理解願います。また、グローバル共通のマニュアルを翻訳したドキュメントであるため、日本国内でのお取り扱いがない機種が含まれている場合がありますことを、ご了承ください。

製品の取扱説明書としての整合性は英語版ユーザーマニュアルに準ずるものですが、万が一内容に不備・誤りなどがございましたら、誠にお手数ですが、ATENジャパン株式会社までお問い合わせくださいますよう、お願い申し上げます。

適合性に関する宣言

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を含め、全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。

E3914

カナダ産業省による宣言

Class Aの本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)

VCCIに関する宣言

SN0132CO、SN9108CO、およびSN9116CO はVCCI に準拠しています。

この装置は、クラスA機器です。この装置を住宅環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI－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。

ユーザー情報

ユーザーの皆様へ

このマニュアルに記載されている全ての情報、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。このマニュアルに記載されている製造元のソフトウェアは、そのまま販売またはライセンスを受けています。購入後にプログラムに欠陥が判明した場合、購入者(メーカー、代理店、または販売店は除く)が、必要な全てのサービス、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す無線やTVへの干渉には責任を負いません。このような干渉を取り除くことは、ユーザーの責任です。

動作前に正しい電圧設定が選択されていない場合、製造業者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か確認してください。

バッテリーの安全に関する注意事項

- 不適切なタイプのバッテリーに交換された場合、爆発する危険性があります。使用済みのバッテリーは、関連する指示に従って処分してください。

同梱品

全てのアイテムが正常に動作するか確認してください。問題が発生した場合は、販売店にお問い合わせください。

SN1116CO/SN1132CO/SN1148CO

- SN1116CO/SN1132CO/SN1148CO シリアルコンソールサーバー×1
- ラップトップUSBコンソール(LUC)ケーブル×1
- 電源ケーブル×2
- フットパッド(4pcs)×1
- ラックマウントキット×1
- クイックスタートガイド×1

SN1116COD/SN1132COD/SN1148COD

- SN1116COD/SN1132COD/SN1148COD シリアルコンソールサーバー×1
- ラップトップUSBコンソール(LUC)ケーブル×1
- フットパッド(4pcs)×1
- ラックマウントキット×1
- クイックスタートガイド×1

SN0108CO/SN0116CO

- SN0108CO/SN0116CO シリアルコンソールサーバー×1
- 電源ケーブル抜け防止ホルダー「Lok-U-Plug」×2
- 電源ケーブル抜け防止ホルダー取付工具×1
- ラップトップUSBコンソール(LUC)ケーブル×1
- 電源ケーブル×2
- マウントキット×1

- フットパッド(4pcs)×1
- クイックスタートガイド×1

SN0108COD/SN0116COD

- SN0108COD/SN0116COD シリアルコンソールサーバー×1
- ラップトップUSBコンソール(LUC)ケーブル×1
- マウントキット×1
- フットパッド(4pcs)×1
- クイックスタートガイド×1

SN0132CO/SN0148CO

- SN0132CO/SN0148CO シリアルコンソールサーバー×1
- ラップトップUSBコンソール(LUC)ケーブル×1
- 電源ケーブル×2
- マウントキット×1
- フットパッド(4pcs)×1
- クイックスタートガイド×1

SN0132COD/SN0148COD

- SN0132COD/SN0148COD シリアルコンソールサーバー×1
- ラップトップUSBコンソール(LUC)ケーブル×1
- マウントキット×1
- フットパッド(4pcs)×1
- クイックスタートガイド×1

SN9108CO/SN9116CO

- SN9108CO/SN9116CO シリアルコンソールサーバー×1
- 電源ケーブル抜け防止ホルダー「Lok-U-Plug」×1
- 電源ケーブル抜け防止ホルダー取付工具×1
- 電源ケーブル×1
- マウントキット×1
- フットパッド(4pcs)×1
- クイックスタートガイド×1

目次

本マニュアルについて

このユーザーマニュアルは、シリアルコンソールサーバーを最大限に活用するために作成しています。このマニュアルでは、製品の取り付け・セットアップ方法、操作方法に関する情報を提供します。

このユーザーマニュアルの対象となるシリアルコンソールサーバーの型番は次の通りです。

型番	製品名
SN1116CO/ SN1116COD	16ポート シリアルコンソールサーバー（デュアル電源 / SFP対応）（AC / DC電源モデル）
SN1132CO/ SN1132COD	32ポート シリアルコンソールサーバー（デュアル電源 / SFP対応）（AC / DC電源モデル）
SN1148CO/ SN1148COD	48ポート シリアルコンソールサーバー（デュアル電源 / SFP対応）（AC / DC電源モデル）
SN0108CO / SN0108COD	8ポート シリアルコンソールサーバー（デュアル電源 / LAN対応）（AC / DC電源モデル）
SN0116CO / SN0116COD	16ポート シリアルコンソールサーバー（デュアル電源 / LAN対応）（AC / DC電源モデル）
SN0132CO / SN0132COD	32ポート シリアルコンソールサーバー（デュアル電源 / LAN対応）（AC / DC電源モデル）
SN0148CO / SN0148COD	48ポート シリアルコンソールサーバー（デュアル電源 / LAN対応）（AC / DC電源モデル）
SN9108CO	8ポート シリアルコンソールサーバー（AC電源モデル）
SN9116CO	16ポート シリアルコンソールサーバー（AC電源モデル）

マニュアルは下記の通りに構成しています。

概要

第1章 はじめに：シリアルコンソールサーバーの目的・機能・メリットについて説明します。フロントパネルとリアパネルにおける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：シリアルコンソールサーバーのセットアップ手順を説明します。

第3章 スーパーアドミニストレーターのセットアップ：スーパーアドミニストレーターがシリアルコンソールサーバーのネットワーク環境を設定し、デフォルトのユーザーネ

ームとパスワードを変更するために使用する手順について説明します。

第4章 ユーザーインターフェース:シリアルコンソールサーバーのユーザーインターフェースのレイアウトと各部名称、およびシリアルコンソールへのログイン方法について説明します。また、ローカルコンソール、インターネットブラウザーやWindowsアプリケーション(AP)プログラムを使った、シリアルコンソールサーバーへのログイン方法についても説明します。

第5章 ポート動作モード:ポートの動作モードについて説明します。このモードには、デバイス制御用のコンソール管理モードやコンソール管理ダイレクトモード、および、シリアルからのイーサネット接続やCOMポート、その他TCP/UDPソケット機能が必要なアプリケーションで使用するリアルCOMポート、バーチャルモデム、TCPサーバー、TCPクライアント、UDPモードが含まれます。

第6章 ポートアクセス:ポートアクセス画面と、ポートおよび電源アウトレット管理に関するオプションの設定方法について説明します。

第7章 ユーザー管理:スーパーアドミニストレーターとアドミニストレーターが、ユーザーとグループを作成・変更・削除する方法と、属性を割り当てる方法について説明します。

第8章 デバイス管理:スーパーアドミニストレーターがシリアルコンソールサーバーを設定したり操作したりする方法について説明します。

第9章 ログ:ログサーバーのインストールおよび設定方法について説明します。

第10章 メンテナンス:シリアルコンソールサーバーとファームウェアのバックアップ、リストア、アップグレードの各方法について説明します。また、プライベート証明書に関する情報も記載しています。

付録:技術情報とトラブルシューティング情報が記載しています。

注意:

- ◆ 本書をよくお読みになった上で設置・操作の手順に従い、本機や接続機器の破損を防止してください。
- ◆ ATENでは新規仕様を反映させたファームウェアや関連ドキュメントを定期的にウェブサイトに公開しています。シリアルコンソールサーバーの最新マニュアルについては、以下のウェブサイトを参照してください。

  http://www.aten.com/global/en/

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。

[ ]	入力するキーを示します。例えば[Enter]はEnterキーを押します。複数のキーを同時に押す場合は、[Ctrl] + [Alt]のように表記してあります。
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、作業手順ではありません。
>	次に表示するオプション(メニューやダイアログボックスなど)の選択を示します。矢印は操作の手順を示します。例えば、「スタート」 > 「実行」は「スタート」メニューを開き、「実行」の選択を意味します。
⚠	重要な情報を示しています。

用語

本マニュアルでは、ユーザー、およびシリアルコンソールサーバーに接続したデバイスに関して「ローカル」と「リモート」という用語を使って表現しています。ユーザーおよびサーバーは、状況に応じて「ローカル」と表現すれば、「リモート」とも表現します。

- ◆ シリアルコンソールサーバー側から見た場合
  - リモートユーザー – 「シリアルコンソールサーバーから離れた」場所からネットワーク経由で製品にログインしているユーザーを、「リモート」ユーザーと呼びます。
  - ローカルコンソール – 製品に物理的に直接接続したコンピューターを指します。
  - サーバー、シリアルデバイス、またはポートデバイス – ケーブルを介して製品に接続しているデバイスを指します。
- ◆ ユーザー側から見た場合
  - ローカルクライアントユーザー – シリアルコンソールサーバーに接続したデバイスで操作を実行するコンピューターの前に座っている場合、ユーザーをローカルユーザーと呼びます。

本マニュアルでは、システム構成全体について説明をする時は説明がない限りシリアルコンソールサーバー側の観点に立って説明します。この場合、ユーザーがリ

モート側と見ます。また、ユーザーがネットワーク経由でブラウザー、ビューワー、またアプリケーションを使う操作について説明する時は、ユーザー側の観点に立って説明します。この場合、製品および配下にあるサーバーがリモート側と見ます。

第1章
はじめに

概要

ATEN SN1100COシリーズ(SN1116CO/SN1132CO/SN1148CO)、SN0100COシリーズ(SN0108CO/SN0116CO/SN0132CO/SN0148CO)、SN9100COシリーズ(SN9108CO/SN9116CO) シリアルコンソールサーバーは、IT およびネットワーク管理者に、データセンターまたは遠隔地にあるシリアルデバイス(RS-232およびUSBコンソールを使用したコンソール操作を可能にするネットワークスイッチなど) へのセキュアな帯域外アクセスが可能です。SN11xxCOモデルのデュアル電源/SFP、SN01xxCOモデルのデュアル電源/LAN、およびSN91xxCOモデルのシングル電源/LANは、全て最先端のテクノロジーを統合しており、セットアップの利便性、シリアルデバイスへのセキュアなアクセス、容易な管理、およびデータセンターの包括的な制御ができます。

シリアルコンソールサーバーは全シリーズでCiscoのピン配列と自動感知DTE/DCE機能を備えており、ロールオーバーケーブルなしでCiscoネットワークスイッチ(およびその他の互換デバイス)に直接接続できるため、ITインフラストラクチャーの導入時間を短縮できます。さらに、デバイスの状態を監視するために、接続したシリアルデバイス(ターミナルブロックを含む)のオンライン検出をサポートします。接続したデバイスがオフラインになると、管理者に警告を通知するメールを送信します。デュアルLANとデュアル電源(AC)に対応したSN11xxCO/SN01xxCOは、冗長電源とフェイルオーバー、またはデュアルIPアドレスでのアクセスをサポートするため、シリアルデバイスに対して24時間365日のアクセス可用性を確保します。SN11xxCO/SN01xxCOは、各モデルでDC電源オプションも用意しており、より柔軟な実装が可能です※。

SN11xxCOシリーズは、センサーポートを通じた環境モニタリングをサポートしており、異常を検出するために24時間監視を続けます。リレーポートを介したキャビネットのロックを使用して、ドアアクセスを監査および制御し、セキュリティー対策を強化します。シリアルコンソールサーバーは、全モデルともATEN CC2000ソフトウェアを通じて利用できるため、シリアルデバイスへのアクセスと電源管理の統合が可能です。

8/16/32/48ポートのモデルをラインナップしている SN11xxCO/SN01xxCOシリアルコンソールサーバーは、サーバーおよびネットワークデバイスに対して、Telnet/SSHクライアント、Javaビューア、およびWebClient経由によるインバンドおよびアウトオブ

バンド（OOB）リモート シリアルコンソールとUSBコンソールアクセスの両方で利用できます。OOB管理機能を使うと、IT管理者は、メイン/本番ネットワークから分離した管理ネットワークを使用して、サーバールーム内のネットワークデバイス(ルーター、スイッチ、UPSなど)を管理できます。

運用ネットワークでアクセスに問題が発生した場合でも、管理者はコンソールサーバー経由でアクセスできます。シリアルコンソールサーバーは、ローカルコンピューターからのダイレクトコンソール接続、ノートパソコンからのUSBコンソール接続、モデム経由のPSTN接続、デュアルSFPまたはデュアルLANポート(1つは本番ネットワークに、もう1つは管理ネットワークにそれぞれ接続)を経由したハイブリッドネットワーク接続などアウトオブバンドのアクセス方法があります。

TLS 1.2データ暗号化、RSA 2048ビット証明書、ポートアクセスと制御のための設定可能なユーザー権限、ローカル/リモート/サードパーティー認証と権限設定、IP/MACアドレスフィルター、FIPS 140-2認定暗号など各種セキュリティー技術を実装したSN11xxCO/SN01xxCO/SN91xxCO シリアルコンソールサーバーは、管理者が高レベルのアクセスを簡単に実現できるセキュリティーを保証します。例えば、8/16/32/48カ所のシリアルポートに対して、個別にアクセス権限を適用できます。情報と制御が常時保護されるよう、データ暗号化が利用できます。システムイベントのログとアラートは、問題の迅速な解決とリスクの低減に役立ちます。上記の例ではセキュリティーが保護されていると同時に、パスワード認証が統合されているため、管理が簡素化されます。

シリアルコンソールサーバーは、産業用制御、データ取得、環境監視、リモート設備運用、設備管理などを制御する、要求の厳しいアプリケーションに対してアクセス・制御ができるよう、シリアルデバイスをイーサネット・ネットワークに接続するために使用します。管理者は、コンソール管理、コンソール管理ダイレクト、リアルCOMポート、TCPサーバー/クライアント、UDPサーバー/クライアント、およびバーチャルモデムを含む複数の動作モードを利用できます。SN11xxCO、SN01xxCO、およびSN91xxCOシリーズの包括的な機能により、ITの生産性を最大限に高め、拡張性を向上させ、シリアルデバイスの簡単で安全なリモート管理により、設置コストと運用コストを削減できます。シリアルコンソールサーバーは、管理者がデータセンターを事実上どこからでも管理できるようにし、時間と費用を節約します。移動コストとMTTR（平均修復時間）コストを最小限に抑え、データセンターサービスの可用性を最大限に高めます。

注意：

1. 互換性のあるモデル: Cisco Catalyst 2960-C シリーズ。

2. DC電源モデルには、SN1116COD、SN1132COD、SN1148COD、SN108COD、SN116COD、SN0132COD、SN0148CODがあります。各モデルは、お客様のご要望に応じてご利用いただけます。

特長

システムのアクセス性と可用性

- シリアルコンソールとUSBコンソールに対してセキュアなインバンドおよびアウトオブバンド・アクセスを実現※1
- 直感的なGUIを使ったブラウザーアクセス
- ターミナルベースのアクセス – メニュー形式の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)を使用
- モデムダイヤルイン/ダイヤルバック/ダイヤルアウト対応
- USBストレージデバイスやUSBコンソール※1、ATEN US232B※2の接続に便利なUSBポートをフロントパネルに搭載
- ラップトップUSBコンソールポートを介してノートパソコンを追加し、ローカルコンソールとして使用可能※2
- デュアルイーサネットポート – フェイルオーバーやデュアルIPアドレスのアクセスが可能※2
- デュアル電源※2

シリアルコンソール管理

- 環境監視用※3のセンサーポート搭載
- リレーポートはキャビネットのドアアクセス制御に対応
- DTE/DCE自動認識機能 – ロールオーバーケーブルがなくてもCiscoネットワークスイッチ(および、その他の互換デバイス)にダイレクト接続ができるため、ITインフラの配置がより便利に
- 接続し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/オフライン状態を検出 – デバイス状態監視でデバイスのオフライン状態を検出するとイベント通知を自動的に送信

- レスポンスチェック機能 – 接続されているシリアルデバイスのシステム状態をチェックし、チェックが失敗した場合(システムクラッシュなど)に通知を送信
- シンプルで利便性の高いデバイスアクセス – Telnet/SSHクライアントおよびサードパーティー製クライアント(例:PuTTY)から選択可能
- 簡単ポートアクセス – ActiveX、Javaシリアルビューア、WebClientから選択可能
- わかりやすいビューア機能 – コピー/ペースト、ログ、データのインポート、マクロ、ブロードキャスト機能、メッセージボード
- Sun Solaris対応 – Sun″break/–safe″
- アラート文字列 – あらかじめ定義した文字列が含まれているメッセージがシリアルデバイスから送信すると、シリアルコンソールサーバーからSNMP Trapアラートまたはメールでユーザーへと通知
- コマンドフィルター – アドミニストレーターはユーザーが実行できないコマンドを設定可能
- 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
- 同時アクセスに対する操作モード – 排他・占有・共有

セキュリティー

- ブラウザーからのセキュアログイン – TLS 1.2データ暗号化およびRSA 2048ビット証明書に対応
- 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対応 – RADIUS、TACACS+、LDAP/AD、Kerberos
- IPやMACアドレスを使ったフィルタリング機能でセキュリティー保護を強化
- 高度なセキュリティー – FIPS140-2認定のOpenSSL暗号モジュールを組み込み、FIPS 140-2 Level 1セキュリティー標準に準拠(証明書番号 #1747、#2398、#2473)
- セキュリティーレベルの設定 – 高・中高・中・カスタムから選択し、ネットワークアクセス制御を強化

システム管理

- ウェブブラウザー、Telnet/SSHクライアントおよびローカルコンソールを使用したシステム設定が可能
- システムログおよびイベントログ対応
- イベント通知先 – イベントログはログサーバー、SyslogサーバーおよびUSBドライブに保存※2
- SNMPエージェント v1/v2/v3 対応
- イベント通知 – SMTPメールとSNMPトラップ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が可能
- マルチブラウザー対応 – Internet Explorer、Chrome、Firefoxに対応
- NTPでタイムサーバーと同期
- IPv4/IPv6対応
- LLDP対応※4
- CLI(コマンドライン・インターフェース)対応
- ソフトウェアCC2000と併用し、データセンターの統合管理を実現
- ソフトウェアCCVSRと併用し、ユーザーセッションの録画が可能

シリアルデバイス管理

- 各種シリアル動作モードをサポート – コンソール管理、コンソール管理ダイレクト、リアルCOMポート、TCPサーバー/クライアント、UDPサーバー/クライアント、バーチャルモデム
- リアルCOMドライバー – Windows 2000以降およびWindows Server 2003/2008対応
- リアルTTYドライバー – Linux対応
- 固定TTYドライバー – UNIX対応※5
- 対応ボーレート – 300、600、1200、1800、2400、4800、9600、19200、28800、38400、57600、115200、230400 bps

言語

- 多言語対応のウェブGUI – 日本語、英語、ドイツ語、韓国語、ロシア語、中国語

（簡体字/繁体字）

注意：

1. 互換性のあるモデル：Cisco Catalyst 2960-C シリーズ。
2. SN1100CO/SN1100COD/SN0100CO/SN0100CODシリーズのみ。
3. ATEN製センサーをお使いください。
4. 詳細については、p.43「LLDP」を参照してください。
5. 固定TTYドライバーは次に対応しています。
   - OpenServer(Sco Unix)
   - UnixWare 7、SVR 5
   - UnixWare 2.1、SVR 4.2
   - QNX 4.25、QNX 6
   - FreeBSD
   - Solaris 10
   - AIX 5.x
   - HP-UX 11i

システム要件

- シリアルコンソールサーバーに接続する機器は、次のシリアルプロトコルに対応している必要があります。
  - RS-232(プロトコルまたはターミナル操作)
- コンソール管理の動作モードを使用する場合は、Telnet/SSHクライアント、PuTTYなどサードパーティーのクライアント、またはウェブブラウザーをインストールしておく必要があります。
- ブラウザーベースのWinClient(過去互換機能)を使用する場合は、Active X、コンソール操作モード用のSNビューア、DirectX 8が動作環境に必要です。また、インストール後の環境に2MB以上の空きメモリーがあるかをご確認ください。
- コンソール管理の動作モード用に、ブラウザーベースのJavaビューアやSNビューアを使用する場合は、Java Runtime Environment(JRE) 8 update202をインストールしてください。また、インストール後の環境に2MB以上の空きメモリーがあるかをご確認ください。Javaは、次のウェブサイトから無料でダウンロードできます。

  https://www.oracle.com/java/technologies/javase/javase8-archive-downloads.html
- コンソール管理の動作モードでブラウザーベースのWebClientを使用する場合は、HTML5以降をサポートしているモダンブラウザをご利用ください。
- バーチャルCOMポートドライバー(リアルCOMポート)はWindows 2000以降の環境が必要です。
- Vista (32 ビット版)では、管理者のみがバーチャルポート管理ユーティリティーをインストールできます。一般ユーザーは、マッピングしたリアルCOMポートのみを操作できます。
- 現在のLinuxのTTYドライバーは、2.2、2.4、2.6(最大2.6.39)、および3.1(最大3.1.5-23)のカーネルに対応しています。
- UNIX用の固定TTYドライバーは以下に対応しています：Unix、OpenServer、Unix Ware 7、SVR 5、Unix Ware 2.1、SVR 4.2、QNX 4.25、QNX 6、FreeBSD、Solaris 10、AIX 5.x、およびHP-UX 11i
- ログサーバーを使用する場合は、Microsoft Jet OLEDB 4.0以降のドライバーをイン

ストールしてください。

DTE/DCE自動検出

RJ-45コンソールポートに接続する場合

- Ciscoのピン配列と自動検出DTE/DCE機能を使用すると、シリアルコンソールサーバーはストレートCat5eケーブルでCiscoスイッチ(およびその他の互換性のあるデバイス)に接続できます。
- シリアルポートのピン配列については、p.188「ピン配列」を参照してください。

DB-9またはDB-25デバイスのインターフェースに接続する場合

- シリアルコンソールサーバーは、Ciscoコンソールケーブルを使用してコンピューターのCOMポート(DB-9)に接続できます。
- DB-9またはDB-25アダプターを作成する場合は、p.189「DB-9/DB-25インターフェース」を参照してください。

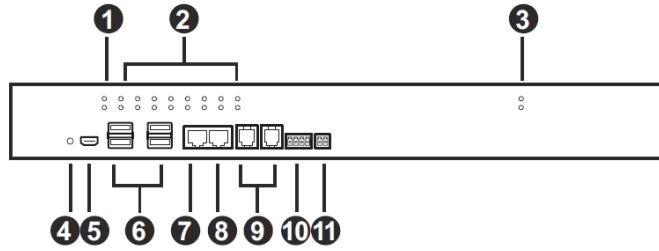
ブラウザー

本製品へのログインに対応したブラウザーは下表の通りです。

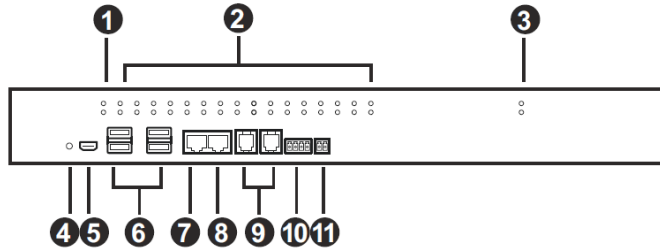
ブラウザー	バージョン
Chrome	70以降
Firefox	63以降
Safari	12以降
Edge (Chromiumベース)	118以降

製品各部名称

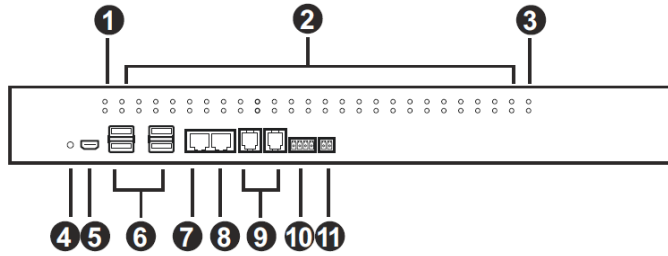
SN1116CO/SN1116COD フロントパネル



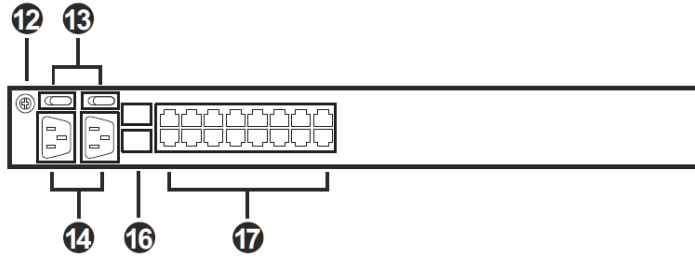
SN1132CO/SN1132COD フロントパネル



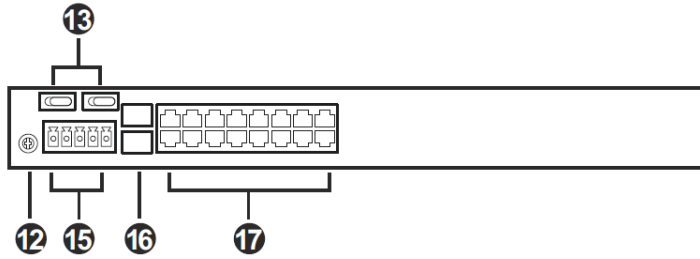
SN1148CO/SN1148COD フロントパネル



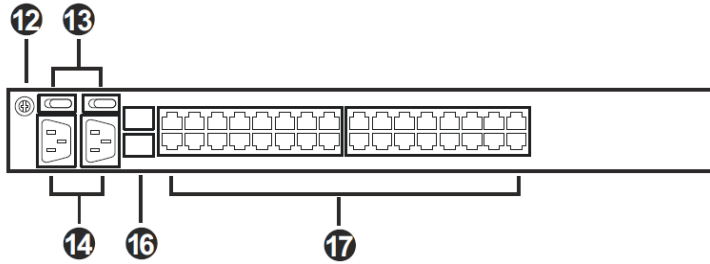
SN1116CO リアパネル



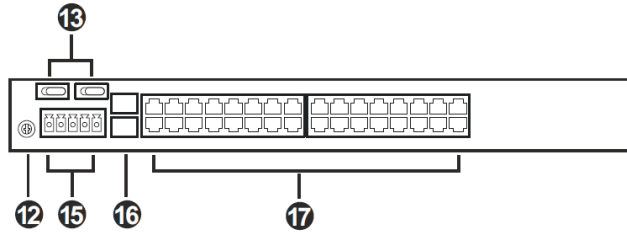
SN1116COD リアパネル (DC電源)



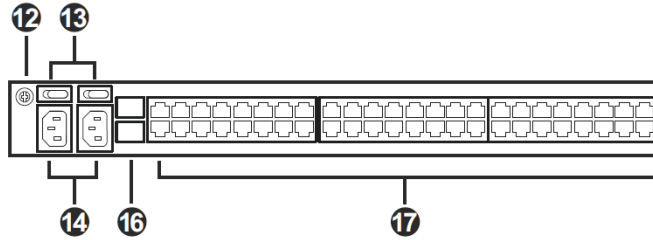
SN1132CO リアパネル



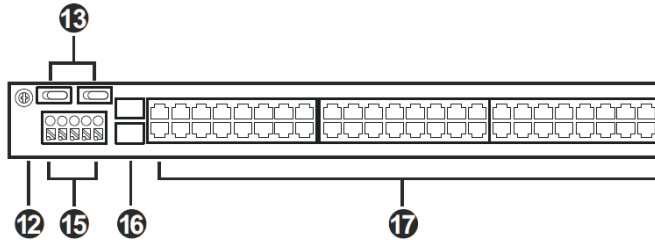
SN1132COD リアパネル (DC電源)



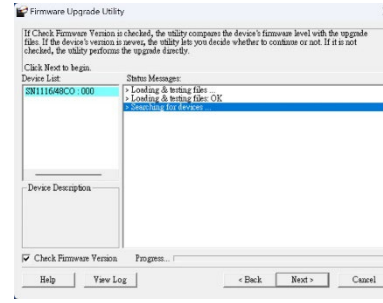
SN1148CO リアパネル



SN1148COD リアパネル (DC電源)

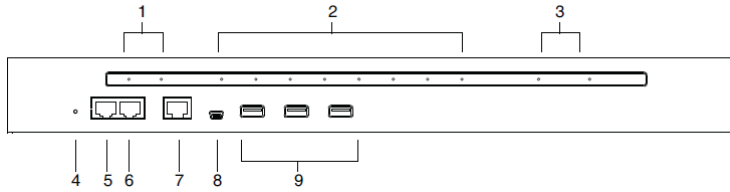


番号	項目	説明
1	電源LED	電源が投入され、操作できる状態になると点灯します。
2	シリアルポートLED	ポートLED は、対応するシリアルポートに関するステータス情報を確認できます。 ◆ グリーンに点灯：オンライン – ポートに接続したシリアルデバイスの電源がオンで、準備ができている状態です。 ◆ グリーンに点滅：アクティブ – ポートを介してデータ伝送している状態です。

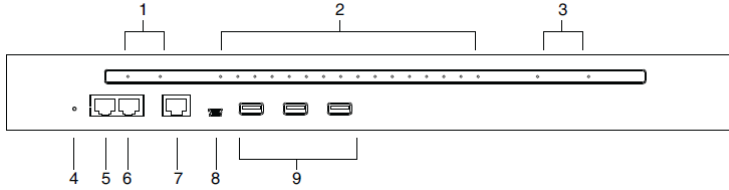
番号	項目	説明
3	LAN LED	プライマリーおよびセカンダリー10/100/1000 Mbps LAN LEDです。 ◆ レッド：10 Mbps ◆ レッド + グリーン（オレンジ）：100 Mbps ◆ グリーン：1000 Mbps ◆ 点滅している場合、シリアルコンソールサーバーがLAN経由でアクセスしている状態を示します。
4	リセットスイッチ	◆ 製品の動作中に、このボタンを押して離すと、ソフトウェアリセット(再起動)を実行します。 ◆ 製品の動作中に、このボタンを3秒以上長押しすると、一部除き設定内容を消去し、工場出荷設定に戻します。 **注意：**この操作をしても、ユーザーアカウントの情報は消去しません。ユーザーアカウント情報の消去については、p.187「ログイン情報の消去」を参照してください。 ◆ ボタンを押したまま製品本体の電源をオンにすると、リカバリーモードとして起動します。ファームウェアアップグレードの失敗した時にこのモード再度書き込み、復旧を試みます。 **注意：**このオプションはファームウェアアップグレードに失敗し、製品本体が操作できなくなった場合にのみ、実行してください。 ◆ リセットボタンが機能せず、フロントパネルにある全てのLED が点滅していれば、シリアルコンソールサーバーがリカバリーモード状態です。ATEN の公式ウェブサイトから「.exe」という拡張子が付いたファームウェアアップグレードパッケージをダウンロードし、ダウンロードしたパッケージを実行して、画面の指示に従います。 

番号	項目	説明
5	ラップトップUSB コンソールポート	このMini USBポートは、コンピューターやノートパソコンを接続してローカル側からアクセスしたり操作したりする際に使用します。パソコンやノートパソコンに接続すると、ターミナルエミュレーターアプリが起動し、SNの操作ができます。
6	USB Type-Aポート	4つのUSB Type-A メス ポートは、USBストレージデバイス(USBメモリ/ハードディスクドライブ)、USBハブ、USBまたはシリアルコンソール経由のCiscoネットワークスイッチなどUSBデバイスの接続に使用できます。シリアルコンソール経由でCiscoネットワークスイッチを接続する場合は、オプション品のUC232Bを推奨します。
7	PONポート	予約済み。
8	RJ-45 ポート (ローカルコンソール)	このRJ-45ポートは、リモートPCのターミナルからSNへのアクセスする時に使用します。このインターフェイスはLANではなくシリアル接続です。Ciscoコンソールケーブルの使用を推奨します。
9	RJ-11ポート (センサー1 /センサー2)	RJ-11ポートは、温度・湿度・空気圧センサーの接続に使用できます。RJ-11互換のセンサーは、ATEN製のオプション品EA1140、EA1240、EA1340 です。 対応センサーは別売りです。製品情報については、ATEN販売店にお問い合わせください。
10	4ピン ターミナルブロック (センサー3)	この4ピン ターミナルブロックは、ドアや水漏れセンサーの接続に使用できます。4ピン ターミナルブロック対応センサーは、EA1440、EA1441、EA1442、EA1540です。対応センサーは別売りです。製品情報については、ATEN販売店にお問い合わせください。
11	2ピン ターミナルブロック (リレー)	この2ピン ターミナルブロックは、ドアアクセス制御の接続に使用できます。
12	グランドターミナル	製品本体を接地するための接地線を取り付けます。
13	電源ソケット	電源ケーブルを接続します。
14	電源スイッチ	製品本体の主電源を入切するためのロッカースイッチです。
15	5ピンターミナルブロック (DC電源)	直流電源からの線を、このDCターミナルブロックに接続します。 **注意：** SN1116COD/SN1132COD/SN1148COD でのみ使用できます。
16	SFP ポート (LAN 1 / LAN 2)	ユニットをネットワークインターフェース(10/100/1000 Mbps) に接続するファイバーケーブルまたは変換モジュールを使用してCat 5eケーブルを接続します。オプション品は、2A-136Gおよび2A-137G SFPモジュールまたは2A-143G 銅モジュールです。製品情報については、ATEN販売店にお問い合わせください。
17	RJ-45 ポート(シリアル)	シリアル機器またはRJ-45→シリアルアダプターに接続するCat 5eケーブルを接続します。

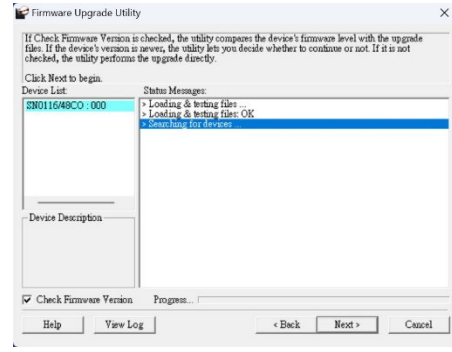
SN0108CO/SN0108COD フロントパネル



SN0116CO/SN0116COD フロントパネル



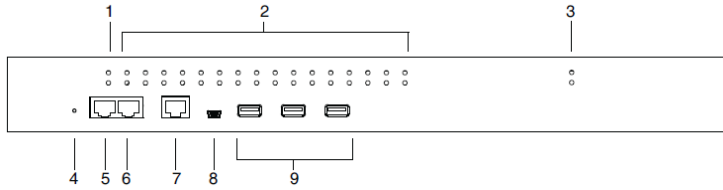
番号	項目	説明
1	電源LED	電源が投入され、操作できる状態になると点灯します。
2	ポートLED	ポートLED は、対応するシリアルポートに関するステータス情報を確認できます。 ◆ グリーンに点滅：アクティブ – ポートを介してデータ伝送している状態です。
3	LAN LED	プライマリーおよびセカンダリー10/100/1000 Mbps LAN LEDです。 ◆ レッド：10 Mbps ◆ レッド + グリーン（オレンジ）：100 Mbps ◆ グリーン：1000 Mbps ◆ 点滅中は、シリアルコンソールサーバーがLAN経由でアクセスしている状態です。

番号	項目	説明
4	リセットボタン	◆ 製品の動作中に、このボタンを押して離すと、ソフトウェアリセット(再起動)を実行します。 ◆ 製品の動作中に、このボタンを3秒以上長押しすると、一部除き設定内容を消去し、工場出荷設定に戻します。 **注意:**この操作をしても、ユーザーアカウントの情報は消去しません。ユーザーアカウント情報の消去については、p.187「ログイン情報の消去」を参照してください。 ◆ ボタンを押したまま製品本体の電源をオンにすると、リカバリーモードとして起動します。ファームウェアアップグレードの失敗した時にこのモード再度書き込み直し、復旧を試みます。 **注意:**このオプションはファームウェアアップグレードに失敗し、製品本体が操作できなくなった場合に実行してください。 ◆ リセットボタンが機能せず、フロントパネルにある全てのLED が点滅していれば、シリアルコンソールサーバーがリカバリーモード状態です。ATEN の公式ウェブサイトから「.exe」という拡張子が付いたファームウェアアップグレードパッケージをダウンロードし、ダウンロードしたパッケージを実行して、画面の指示に従います。 
5	PONポート	予約済み。
6	モデムポート	製品本体がネットワーク経由で利用できない場合に、ダイヤルイン接続するためのポートです。セットアップの詳細については、p.33「シリアルコンソールサーバーのセットアップ」における手順6を参照してください。
7	ローカルコンソールポート	このRJ-45ポートは、リモートPCのターミナルからSNへのアクセスする時に使用します。このインターフェイスはLANではなくシリアル接続です。Ciscoコンソールケーブルの使用を推奨します。

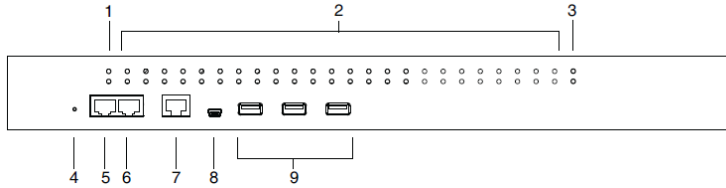
番号	項目	説明

8	ラップトップUSB コンソール（LUC）ポート	このMini USBポートは、コンピューターやノートパソコンを接続して ローカル側からアクセスしたり操作したりする際に使用します。パソ コンやノートパソコンに接続すると、ターミナルエミュレーターアプリ が起動し、SNの操作ができます。
9	USBポート	3つのUSB Type-A メス ポートは、USBストレージデバイス(ペンドライ ブ/ハードディスクドライブ)、USBハブ、USBまたはシリアルコンソール 経由のCiscoネットワークスイッチなどUSBデバイスの接続に使用でき ます。シリアルコンソール経由でCiscoネットワークスイッチを接続する 場合は、オプション品のUC232Bを推奨します。

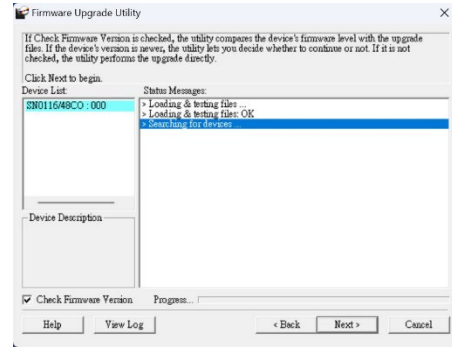
SN0132CO/SN0132COD フロントパネル



SN0148CO/SN0148COD フロントパネル

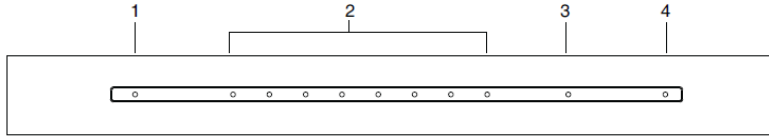


番号	項目	説明
1	電源LED	電源が投入され、操作できる状態になると点灯します。
2	ポートLED	ポートLED は、対応するシリアルポートに関するステータス情報を確認できます。 ◆ グリーンに点灯：オンライン – ポートに接続したシリアルデバイスの電源がオンで、準備ができている状態です。 ◆ グリーンに点滅：アクティブ – ポートを介してデータ伝送している状態です。
3	LAN LED	プライマリーおよびセカンダリー10/100/1000 Mbps LAN LEDです。 ◆ レッド：10 Mbps ◆ レッド + グリーン（オレンジ）：100 Mbps ◆ グリーン：1000 Mbps ◆ 点滅中は、シリアルコンソールサーバーがLAN経由でアクセスしている状態です。

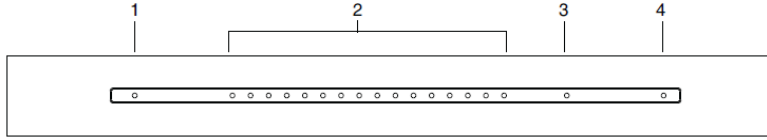
番号	項目	説明
4	リセットボタン	◆ 製品の動作中に、このボタンを押して離すと、ソフトウェアリセット(再起動)を実行します。 ◆ 製品の動作中に、このボタンを3秒以上長押しすると、一部除き設定内容を消去し、工場出荷設定に戻します。 **注意:**この操作をしても、ユーザーアカウントの情報は消去しません。ユーザーアカウント情報の消去については、p.187「ログイン情報の消去」を参照してください。 ◆ ボタンを押したまま製品本体の電源をオンにすると、リカバリーモードとして起動します。ファームウェアアップグレードの失敗した時にこのモード再度書き込み直すし、復旧を試みます。 **注意:**このオプションはファームウェアアップグレードに失敗し、製品本体が操作できなくなった場合に、実行してください。 ◆ リセットボタンが機能せず、フロントパネルにある全てのLED が点滅してれば、シリアルコンソールサーバーがリカバリーモード状態です。ATEN の公式ウェブサイトから「.exe」という拡張子が付いたファームウェアアップグレードパッケージをダウンロードし、ダウンロードしたパッケージを実行して、画面の指示に従います。 
5	PONポート	予約済み。
6	モデムポート	製品本体がネットワーク経由で利用できない場合に、ダイヤルイン接続するためのポートです。セットアップの詳細については、p.33「シリアルコンソールサーバーのセットアップ」における手順6を参照してください。
7	ローカルコンソールポート	このRJ-45ポートは、リモートPCのターミナルからSNへのアクセスする時に使用します。このインターフェイスはLANではなくシリアル接続です。Ciscoコンソールケーブルの使用を推奨します。

番号	項目	説明
8	ラップトップ USBコンソール（LUC）ポート	このMini USBポートは、コンピューターやノートパソコンを接続してローカル側からアクセスしたり操作したりする際に使用します。パソコンやノートパソコンに接続すると、ターミナルエミュレーターアプリが起動し、SNの操作ができます。
9	USBポート	3つのUSB Type-A メス ポートは、USBストレージデバイス(ペンドライブ/ハードディスクドライブ)、USBハブ、USBまたはシリアルコンソール経由のCiscoネットワークスイッチなどUSBデバイスの接続に使用できます。シリアルコンソール経由でCiscoネットワークスイッチを接続する場合は、オプション品のUC232Bを推奨します。

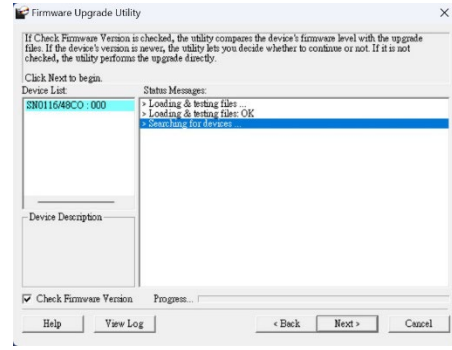
SN9108CO フロントパネル



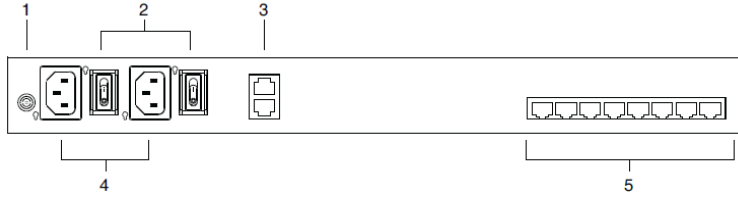
SN9116CO フロントパネル



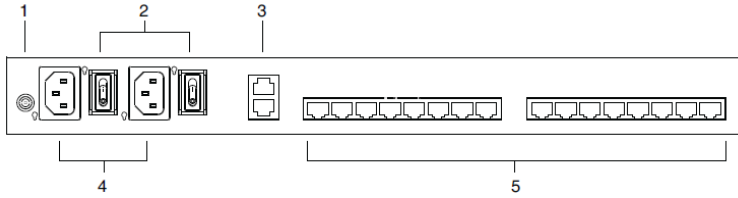
番号	項目	説明
1	電源LED	電源が投入され、操作できる状態になると点灯します。
2	ポートLED	ポートLED は、対応するシリアルポートに関するステータス情報を確認できます。 ◆ グリーンに点灯：オンライン – ポートに接続したシリアルデバイスの電源がオンで、準備ができている状態です。 ◆ グリーンに点滅：アクティブ – ポートを介してデータ伝送している状態です。
3	LAN LED	プライマリーおよびセカンダリー10/100/1000 Mbps LAN LEDです。 ◆ レッド：10 Mbps ◆ レッド + グリーン（オレンジ）：100 Mbps ◆ グリーン：1000 Mbps ◆ 点滅中は、シリアルコンソールサーバーがLAN経由でアクセスしている状態です。

番号	項目	説明
4	リセットボタン	◆ 製品の動作中に、このボタンを押して離すと、ソフトウェアリセット(再起動)を実行します。 ◆ 製品の動作中に、このボタンを3秒以上長押しすると、一部除き設定内容を消去し、工場出荷設定に戻します。 **注意:**この操作をしても、ユーザーアカウントの情報は消去しません。ユーザーアカウント情報の消去については、p.187「ログイン情報の消去」を参照してください。 ◆ ボタンを押したまま製品本体の電源をオンにすると、リカバリーモードとして起動します。ファームウェアアップグレードの失敗した時にこのモード再度書き込み直し、復旧を試みます。 **注意:**このオプションはファームウェアアップグレードに失敗し、製品本体が操作できなくなった場合にのみ、実行してください。 ◆ リセットボタンが機能せず、フロントパネルにある全てのLED が点滅していれば、シリアルコンソールサーバーがリカバリーモード状態です。ATEN の公式ウェブサイトから「.exe」という拡張子が付いたファームウェアアップグレードパッケージをダウンロードし、ダウンロードしたパッケージを実行して、画面の指示に従います。 

SN0108CO リアパネル

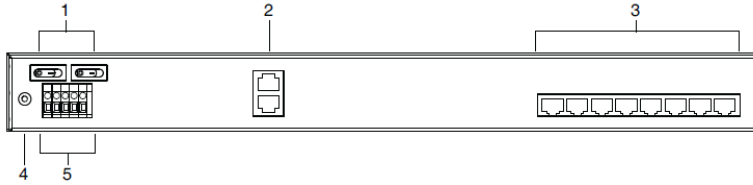


SN0116CO リアパネル

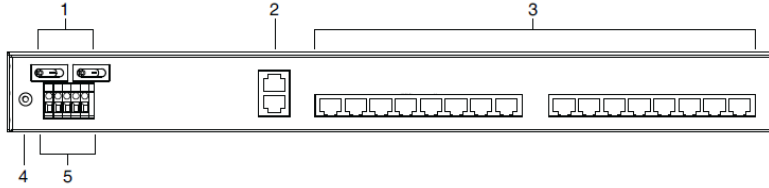


番号	項目	説明
1	グランドターミナル	製品本体を接地するための接地線を取り付けます。
2	電源スイッチ	製品本体に電源を入れたり切ったりするための標準的なロッカースイッチです。
3	LANポート	ユニットをプライマリーやバックアップのネットワークインターフェース（10/100/1000 Mbps）につなぐケーブルを接続します。
4	電源ソケット	電源ケーブルを接続します。
5	シリアルポート	シリアル機器またはRJ-45→シリアルアダプターに接続するCat 5eケーブルを接続します。

SN0108COD リアパネル(DC電源)

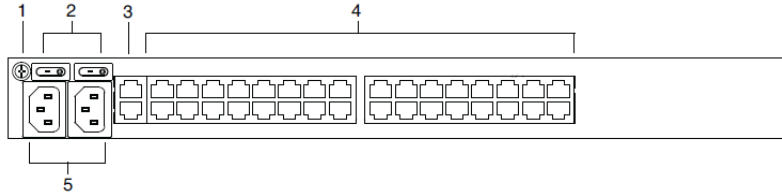


SN0116COD リアパネル(DC電源)

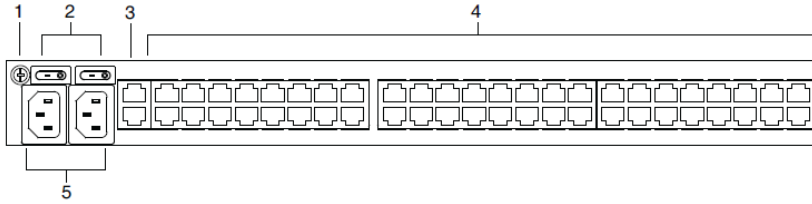


番号	項目	説明
1	電源スイッチ	製品本体に電源を入れたり切ったりするための標準的なロッカースイッチです。 **注意**:電源を入れなおす場合は、電源スイッチをオフにした後、2秒以上経過してから、オンにするようにしてください。
2	LANポート	ユニットをプライマリーやバックアップのネットワークインターフェース(10/100/1000 Mbps)につなぐケーブルを接続します。
3	シリアルポート	シリアル機器またはRJ-45→シリアルアダプターに接続するCat 5eケーブルを接続します。
4	グランドターミナル	製品本体を接地するための接地線を取り付けます。
5	DCターミナルブロック	電源からのリードを、このDCターミナルブロックに接続します。

SN0132CO リアパネル

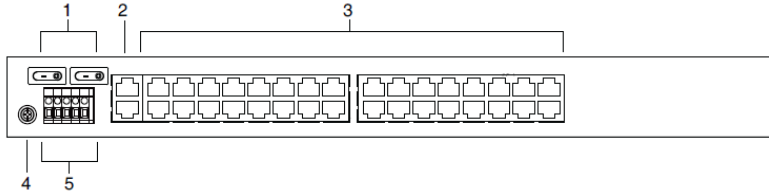


SN0148CO リアパネル

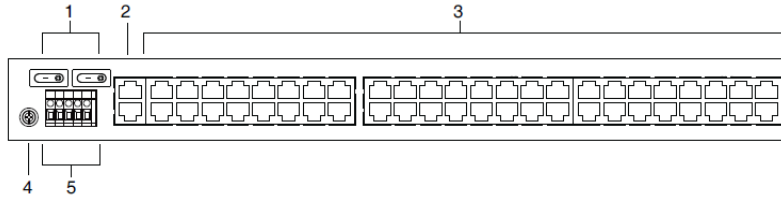


番号	項目	説明
1	グランドターミナル	製品本体を接地するための接地線を取り付けます。
2	電源スイッチ	製品本体に電源を入れたり切ったりするための標準的なロッカースイッチです。
3	LANポート	ユニットをプライマリーやバックアップのネットワークインターフェース（10/100/1000 Mbps）につなぐケーブルを接続します。
4	シリアルポート	シリアル機器またはRJ-45→シリアルアダプターに接続するCat 5eケーブルを接続します。
5	電源ソケット	電源ケーブルを接続します。

SN0132COD リアパネル(DC電源)

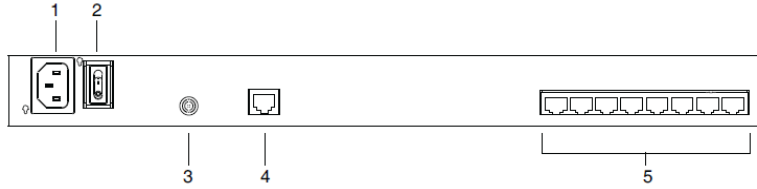


SN0148COD リアパネル(DC電源)

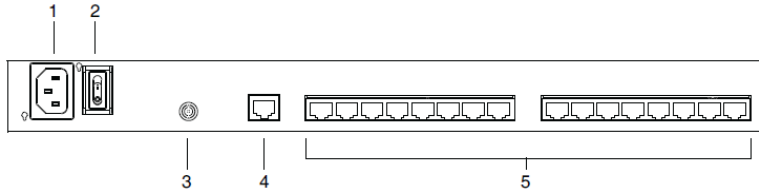


番号	項目	説明
1	電源スイッチ	製品本体に電源を入れたり切ったりするための標準的なロッカースイッチです。 **注意**:電源を入れなおす場合は、電源スイッチをオフにした後、2秒以上経過してから、オンにするようにしてください。
2	LANポート	ユニットをプライマリーやバックアップのネットワークインターフェース(10/100/1000 Mbps)につなぐケーブルを接続します。
3	シリアルポート	シリアル機器またはRJ-45→シリアルアダプターに接続するCat 5eケーブルを接続します。
4	グランドターミナル	製品本体を接地するための接地線を取り付けます。
5	DCターミナルブロック	電源からのリードを、このDCターミナルブロックに接続します。

SN9108CO リアパネル



SN9116CO リアパネル



番号	項目	説明
1	電源ソケット	電源ケーブルを接続します。
2	電源スイッチ	製品本体に電源を入れたり切ったりするための標準的なロッカースイッチです。
3	グランドターミナル	製品本体を接地するための接地線を取り付けます。
4	LANポート	ユニットをネットワークインターフェース(10/100/1000 Mbps)に接続するケーブルを接続します。
5	シリアルポート	シリアル機器またはRJ-45→シリアルアダプターに接続するCat 5eケーブルを接続します。

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

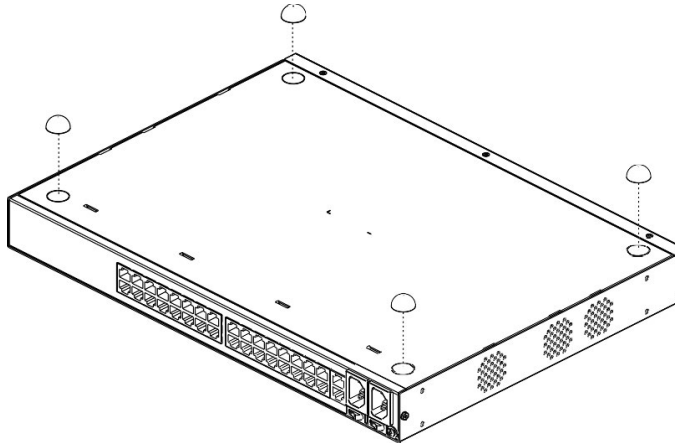
1. 機器の設置に際し重要な情報をp.162に記載しています。作業の前に、必ず目を通してください。
2. 今から接続するデバイス全ての電源がオフか確認してください。また、デバイスからは電源ケーブルも抜いておいてください。

卓上設置とラックへの取り付け

シリアルコンソールサーバーは、卓上に設置したり、ラックに取り付けできます。以下のセクションでは、各方法の手順について説明します。

卓上設置

シリアルコンソールサーバーは、製品本体および接続ケーブルの総重量に耐える安定した水平な場所へ設置できます。製品本体を単体で設置する、または、複数のユニットを重ね置きするには、製品同梱のゴム製フットパッドの裏面の剥離紙をはがしてから、次のページにある図のように本体底面の四隅に貼り付けてください。



注意:

適切な通気を確保するために製品の両側に少なくとも5cm程度、ケーブル取り回しのスペースを確保するために製品リア側に少なくとも13cm程度の余裕を設けて設置してください。

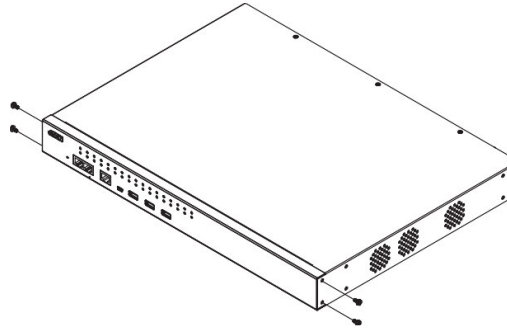
ラックへのマウント

シリアルコンソールサーバーは、19インチサイズのラックに1Uサイズで取り付けられます。マウント用ブラケットは、用途に応じてラックのフロント側、リア側のどちらにも取り付けられます。

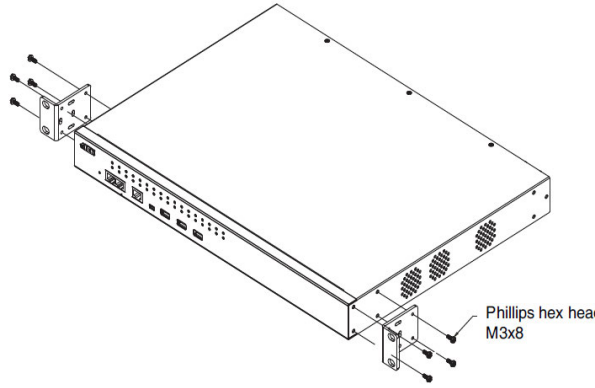
ラックのフロント側への取り付け

製品本体をラックのフロント側に取り付ける場合は、下記の手順に従って作業してください。

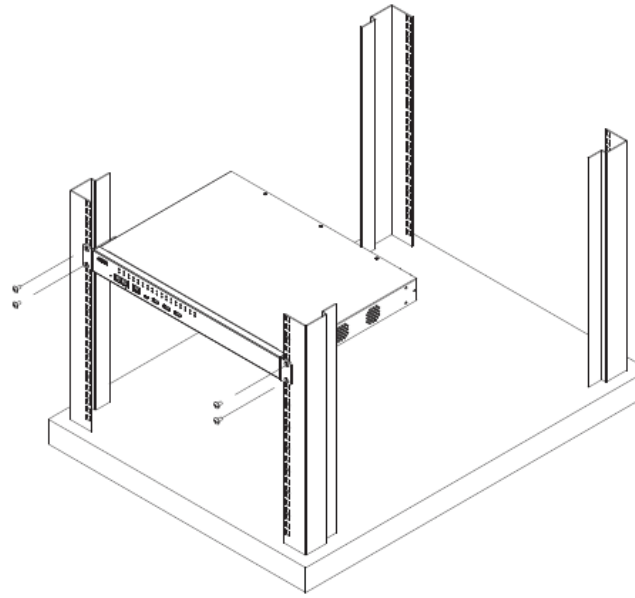
1. 製品本体のフロント側にある左右両方のネジ(合計4個)を外してください。



2. ラックマウントキットに同梱M3プラスネジ8mmを使用して、製品本体で左右両方のフロント側にラックマウントブラケットをネジ止めしてください。



3. 製品本体をラックのフロント側に固定し、ラックのネジ穴とマウント用ブラケットの穴を合わせてください。穴合わせをしたら、マウント用ブラケットをラックのフロント側にネジ止めしてください。



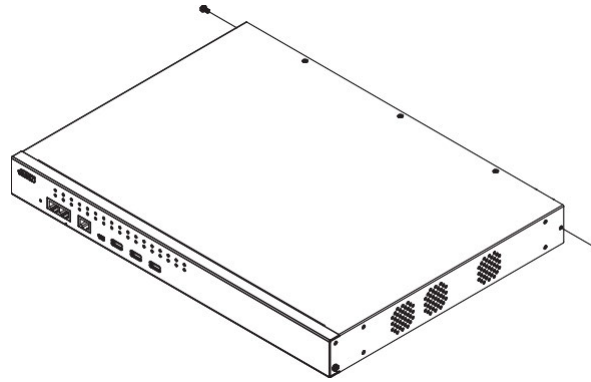
注意：

ラックマウントキットにはネジとケージナットは同梱されていません。

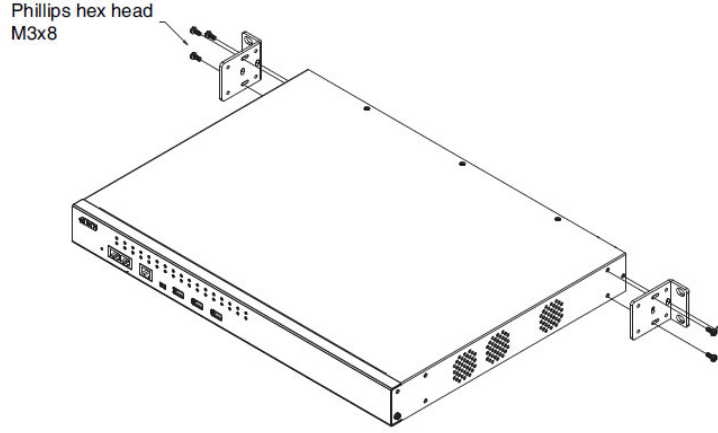
ラックのリア側への取り付け

製品本体をラックのリア側に取り付ける場合は、下記の手順に従って作業してください。

1. 製品本体のリア側近くにある左右両方のネジ各1個(合計2個)を外してください。



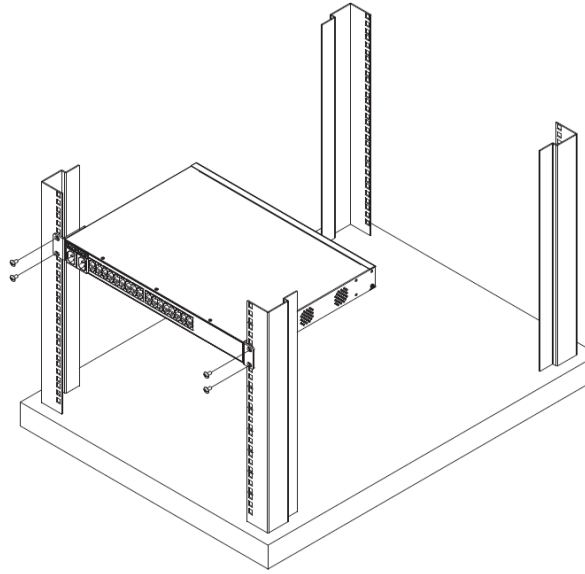
2. ラックマウントキットに同梱M3プラスネジ8mmを使用して、製品本体で左右両方のリア側にラックマウントブラケットをネジ止めしてください。



3. 製品本体をラックのリア側に固定し、ラックのネジ穴とマウント用ブラケットの

穴を合わせてください。

4. マウント用ブラケットをラックのリア側にネジ止めしてください。



注意：

ラックマウントキットにはネジとケージナットは同梱されていません。

シリアルコンソールサーバーのセットアップ

SN1116CO/SN1132CO/SN1148COのセットアップ

SN1116CO/SN1132CO/SN1148COをセットアップするには、p.36の接続図を参照してください。図内における番号は、作業手順の番号に対応しています。作業手順は下記の通りです。

1. 接地線の片方の端をグランドターミナルに、もう片方の端を適切な接地物に接続して、製品本体をアース接続してください。

注意:

この手順は省略しないでください。適切な接地は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. 次のいずれかの方法を使用して、サーバー/シリアルデバイスやネットワークスイッチを接続します。

   ◆ DB-9コネクターを備えたサーバーまたはシリアルデバイスでは、シリアルポートとユニットのリアパネルの使用可能なRJ-45ポートの間に、RJ-45→DB-9(メス)アダプターを備えたCiscoコンソールケーブルまたはCat 5eケーブルを接続します。

   注意:

   ピン配列に関する詳細はp.189「DB-9/DB-25 インターフェース」を参照してください。

   ◆ Ciscoネットワークスイッチ(またはコンソールポートのピン配列に互換性のある任意のネットワークスイッチ)とユニットのリアパネルにある使用可能なRJ-45ポートをTIA/EIA準拠ストレート配線のCat 5eケーブルで接続します。

   注意:

   互換性のあるネットワークスイッチの場合は、対象となるデバイスのRJ-45ポートのピン定義がユニットと一致しているか確認してください。

   互換性のあるネットワークスイッチの例:Juniper、HPE、Dell、Huawei、H3C、EdgeCore、TRENDnet、Fortinet、ATEN ES0152/ES0154。

   ---

3. 遠隔制御をする場合は、ユニットのリアパネルのLAN 1 およびLAN 2 SFP ポートの両方を、別売オプション品のSFP モジュールまたはCat 5eケーブルでネットワークスイッチに接続します。製品情報については、ATEN販売店にお問い合わせください。

4. コンソールターミナル接続を使用するには、次のいずれかを実行します。

   ◆ Ciscoコンソールケーブルを使用して、本体フロントパネルのローカルコンソールポートとコンソールターミナルまたはコンピューターのDB-9コネクターを接続します。

   ◆ DB-9コネクターのないコンソールターミナルまたはコンピューターでは、UC232BのCat 5eケーブルを使用して、コンソールターミナルまたはコンピューターのローカルコンソールとUSBポートを接続します。

   注意:

   USB→RJ-45 (RS-232) コンソールアダプターUC232Bは別売りです。製品情報については、ATEN販売店にお問い合わせください。

5. (オプション)ノートパソコンを使用してユニットをローカルで制御するには、付属のラップトップUSBコンソールケーブルを使って、フロントパネルのユニットのラップトップUSBコンソールポートにノートパソコンを接続します。

6. (オプション) 最大4台のUSB周辺機器をフロントパネルのユニットのUSB Type-Aポートに接続します。

   ◆ USBフラッシュメモリー対応

   注意:

   USBストレージデバイスでサポートするファイルシステムは、FAT8、FAT16、およびFAT32 です。

   ◆ USBコンソールポート経由のネットワークスイッチ。

   ◆ USB→RJ-45 (RS-232) コンソールアダプターUC232Bを使用したシリアルコンソールポート経由のネットワークスイッチ。

   注意:

   別のネットワークスイッチを接続する場合は、リアパネルのシリアルコンソールポートまたはフロントパネルのUSBコンソールポートを使用して、

次のいずれかの方法を使用してください。

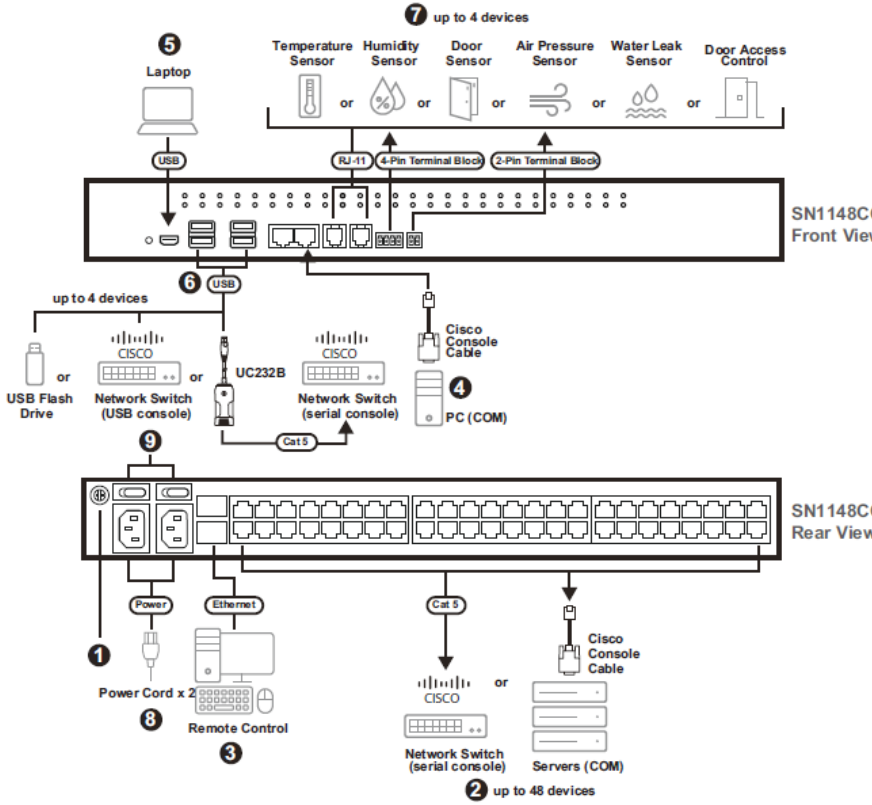
7. (オプション) データ読み取りにセンサーを使用するには、最大4つのセンサーをユニットのRJ-11ポート(センサー1 とセンサー2)、4 ピン ターミナルブロック(センサー3)、および2ピン ターミナルブロック(リレー) に接続します。
   - ◆ RJ-11互換のセンサー:EA1140、EA1240、EA1340
   - ◆ 4ピン ターミナルブロック対応センサー: EA1440、EA1441、EA1442、EA1540

   注意:

   各センサーは別売りです。製品情報については、ATENの販売店にお問い合わせください。

   - ◆ ドアアクセス制御を使用するには、ドアアクセス制御デバイスをユニットの2ピン ターミナルブロック(リレー)に接続します。
8. AC電源モデル(SN1116CO/SN1132CO/SN1148CO)の場合:付属のAC電源コードを本体の電源ソケットに接続します。DC電源モデル(SN1116COD/SN1132COD/SN1148COD)の場合:DC電源を本体のDCターミナルブロックに接続します。
9. 本体の電源スイッチをオンにします。

接続図（SN1116CO/SN1132CO/SN1148CO）



注意：

セットアップを説明するための例として、SN1148CO シリアルコンソールサーバーを使用します。他のシリアルコンソールサーバーの場合と同様、セットアップ方法は、シリアルポートの数が少なくても同じです。

SN0108CO/SN0116CO/SN0132CO/SN0148COのセットアップ

お使いのSN0108CO/SN0116CO/SN0132CO/SN0148COをセットアップする際には、p.39の接続図を参考にしてください。図内における番号は、作業手順の番号に対応しています。作業手順は下記の通りです。

1. 接地線の一方の端をシリアルコンソールサーバーのグランドターミナル（本体のリア側に位置）に接続し、もう一方の端を適切な接地物に接続して、ユニットを接地してください。

注意：

この手順は省略しないでください。適切な接地は電圧変化や静電気による機器の誤動作防止や破損防止に一定の効果があります。

---

2. DB-9ピンコネクターを有したサーバーまたはシリアル機器のそれぞれに対し、CiscoコンソールケーブルまたはRJ-45→DB-9 メス シリアルアダプターを使って、シリアル機器のシリアルポートとシリアルコンソールサーバーのリアパネルにあるRJ-45ポートを接続してください。

注意：

ピン配列に関する詳細はp.189「DB-9/DB-25 インターフェース」を参照してください。

---

3. Ciscoネットワークスイッチ(または互換性のあるネットワークスイッチ)と、シリアルコンソールサーバーのリアパネルにある使用可能なRJ-45ポートの間にCat 5eケーブルを接続してください。

注意：

互換性のあるネットワークスイッチの場合は、対象となるデバイスのRJ-45ポートのピン配列がシリアルコンソールサーバーと一致しているか確認してください。

互換性のあるネットワークスイッチの例：Juniper、HPE、Dell、Huawei、H3C、EdgeCore、TRENDnet、Fortinet、ATEN ES0152/ES0154。

---

4. シリアルコンソールサーバーをネットワークに接続するには、ユニットのリアパネルにあるプライマリーLANポートとバックアップLANポートの両方を、Cat 5eケーブルでネットワークに接続してください。

5. (オプション)アウトオブバンド操作用にシリアルモデムをセットアップする場合は、Ciscoコンソールケーブルをヌルモデムアダプターに接続してください。DB-9コネクターをモデムに接続し、RJ-45コネクターをシリアルコンソールサーバーのフロントパネルのモデムポートに接続してください。

6. (オプション)電源管理をする場合は、ATEN PDUとシリアルコンソールサーバーのフロントパネルにあるPONポートを、Cat 5eケーブルで接続してください。

7. (オプション) コンソールターミナル接続を使用する場合は、Ciscoコンソールケーブルを使用して、フロントパネルのシリアルコンソールサーバーのローカルコンソールポートとコンソールターミナル(またはコンピューター)のDB-9コネクターを接続します。

   DB-9コネクターのないコンソールターミナルまたはコンピューターでは、UC232BのCat 5eケーブルを使用して、コンソールターミナル(またはコンピューター)のUSBポートを接続できます。

注意:

USB→RJ-45 (RS-232) コンソールアダプターUC232Bは別売りです。製品情報については、ATENの販売店にお問い合わせください。

---

8. (オプション)ラップトップUSBコンソールを使用してシリアルコンソールサーバーをローカルで操作する場合は、製品パッケージに同梱しているラップトップUSBコンソールケーブルを使用して、シリアルコンソールサーバーのフロントパネルにあるLUCポートにノートパソコンを接続してください。

9. (オプション) フロントパネルのユニットのUSB Type-AポートにUSB周辺機器(最大3台)を接続します。

   ◆ USBフラッシュメモリー対応

注意:

USBストレージデバイスでサポートするファイルシステムは、FAT8、FAT16、およびFAT32 です。

◆ USBコンソールポート経由のネットワークスイッチ。

◆ USB→RJ-45 (RS-232) コンソールアダプターUC232Bを使用したシリアルコンソールポート経由のネットワークスイッチ。

注意:

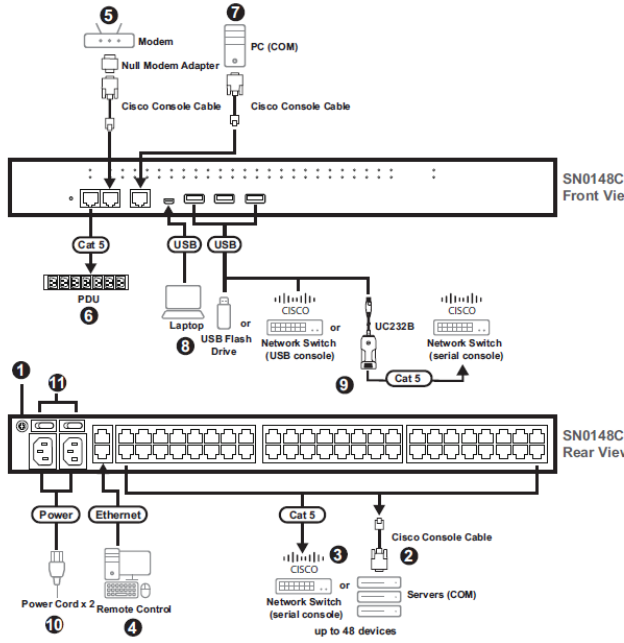
別のネットワークスイッチを接続する場合は、リアパネルのシリアルコンソールポートまたはフロントパネルのUSBコンソールポートを使用して、次のいずれかの方法を使用してください。

---

10. AC電源モデルの場合:製品パッケージに付属のAC電源コードを使用して、SN0108CO/SN0116CO/SN0132CO/SN0148COの電源ソケットをAC電源に接続してください。
    DC電源モデルの場合:DC電源をSN0108COD/SN0116COD/SN0132COD/SN0148CODのDCターミナルブロックに接続してください。

11. 電源スイッチをオンにしてください。

接続図(SN0108CO/SN0116CO/SN0132CO/SN0148CO)



注意:

上図はシリアルコンソールサーバーSN0148COを例にとっています。SN0108CO/SN0116CO/SN0132COにも同様にポートやスイッチがありますが、この図とはレイアウトが若干異なります。詳細については、p.9「製品各部名称」を参照してください。

SN9108CO/SN9116COのセットアップ

SN9108CO/SN9116COをセットアップするには、p.41の接続図を参照してください。図内における番号は、作業手順の番号に対応しています。作業手順は下記の通りです。

1. 接地線の一方の端をシリアルコンソールサーバーのグランドターミナル(本体のリア側に位置)に接続し、もう一方の端を適切な接地物に接続して、ユニットを接地してください。

注意:

この手順は省略しないでください。適切な接地は電圧変化や静電気による機器の誤動作防止や破損防止に一定の効果があります。

2. DB-9ピンコネクターを有したサーバーまたはシリアル機器のそれぞれに対し、CiscoコンソールケーブルまたはRJ-45→DB-9 メス シリアルアダプターを使って、シリアル機器のシリアルポートとシリアルコンソールサーバーのリアパネルにあるRJ-45ポートを接続してください。

注意:

ピン配列に関する詳細はp.189「DB-9/DB-25 インターフェース」を参照してください。

3. Ciscoネットワークスイッチ(または互換性のあるネットワークスイッチ)と、シリアルコンソールサーバーのリアパネルにある使用可能なRJ-45ポートの間にCat 5eケーブルを接続してください。

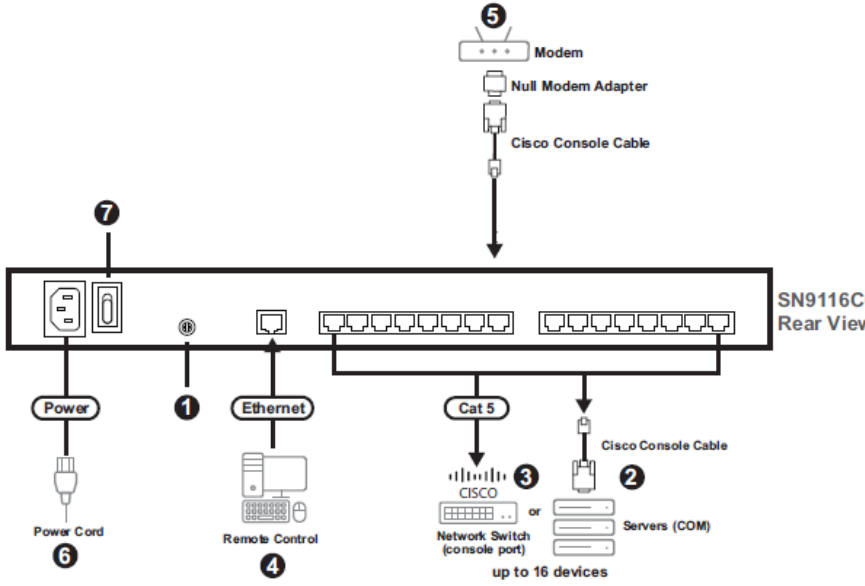
注意:

互換性のあるネットワークスイッチの場合は、対象となるデバイスのRJ-45ポートのピン配列がシリアルコンソールサーバーと一致しているか確認して

ください。

4. シリアルコンソールサーバーをネットワークに接続するケーブルを、製品リアパネルにあるLANポートに接続してください。
5. (オプション)アウトオブバンド操作用にシリアルモデムをセットアップする場合は、Ciscoコンソールケーブルをヌルモデムアダプターに接続してください。DB-9コネクターをモデムに接続し、RJ-45コネクターをシリアルコンソールサーバーのフロントパネルにある使用可能なRJ-45ポートに接続してください。
6. AC電源モデルの場合:SN9108CO/SN9116COの電源ソケットをAC電源に接続するには、製品パッケージに付属のAC電源コードを使用してください。
7. 電源スイッチをオンにしてください。

接続図(SN9108CO/SN9116CO)

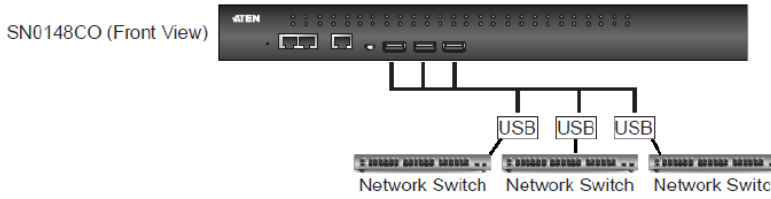


USBコンソールからUSBケーブル経由でネットワークスイッチをセットアップするには

オプションで、最大3台(SN0100CO/SN0100CODシリーズ) / 4台(SN1100CO/SN1100CODシリーズ) のネットワークスイッチをシリアルコンソールサーバーのUSBポートに接続できます。

注意:

- サポートする最新のネットワークスイッチについては、製品ページを参照してください。
- 別のネットワークスイッチを接続するときは、必ず次のいずれかの方法を使用してください。
  - リアパネルのシリアルコンソールポートを使用します。
  - フロントパネルのUSBポート(UC232B経由)を使用します。UC232BでUSBポートを使用する場合、コンソール管理とコンソール管理ダイレクトの各モードのみがサポートします。

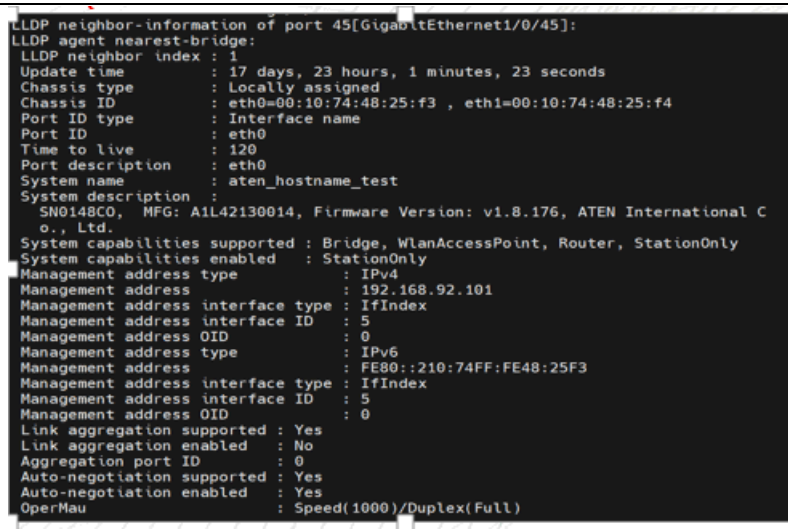


LLDP

シリアルコンソールサーバーがネットワークスイッチに接続している場合、LLDP関連コマンドを使用して、ネットワークスイッチコンソールからシリアルコンソールサーバー上の情報を取得できます。以下に例を示します。

注意:

LLDP関連コマンドの実行方法の詳細については、ネットワークスイッチのユーザーマニュアルまたはユーザーガイドを参照してください。



第3章
スーパーアドミニストレーターによる設定

概要

本章では、スーパーアドミニストレーターが初めてシリアルコンソールサーバーをセットアップする際に必要となる管理手順について説明します。

初期設定

シリアルコンソールサーバーのケーブル接続が終わったら、スーパーアドミニストレーターは製品本体の操作ができるように設定をする必要があります。この設定には、ネットワークパラメーターの設定やデフォルトのスーパーアドミニストレーターのログインの変更といった操作が含まれます。初期設定に最も便利な方法は、ローカルコンソール(ローカルVTコンソールまたはMicrosoft HyperTerminalなどターミナルアプリケーションソフトウェアを実行しているローカルコンピューター)、またはSNビューアUSBアプリケーションを実行しているラップトップUSBコンソール(LUC)(SN1100CO/SN1100COD/SN0100CO/SN0100CODシリーズのみ) からです。また、ユニットのIPアドレスを使用して、ウェブGUI経由でリモートからのセットアップもできます。

注意:

ネットワークのリモート設定方法については、p.179「IPアドレスの設定」を参照してください。

ローカルログイン

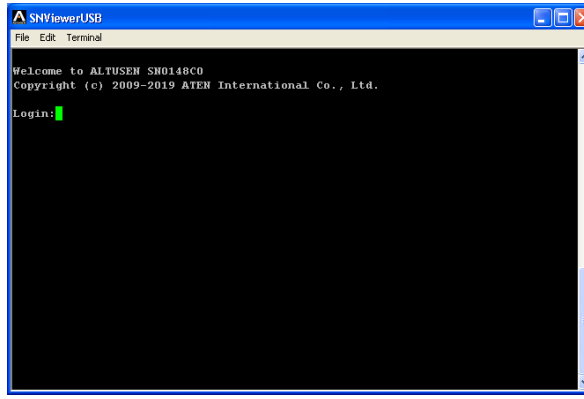
シリアルコンソールサーバーに直接接続したコンピューターまたはノートパソコン(SN1100CO/SN1100COD/SN0100CO/SN0100CODシリーズのみ)からローカルでログインできます(p.33「シリアルコンソールサーバーのセットアップ」を参照)。ローカルログインには、SNビューアUSBとハイパーターミナルといった2種類の方法がありま

す。

ローカルログインのメインメニューは、このマニュアル全体で説明しているブラウザーベースの設定および制御機能をベースにしたテキストです。設定と制御のフル機能を使用したい場合は、ブラウザーベースのウェブGUIの使用を推奨します。詳細はウェブブラウザー版の情報を参照してください（p.50参照）。テキストサブメニューを使用して作業し、この章で説明する設定方法を紹介しています。

ラップトップUSBコンソール(LUC)からのログイン – SNビューアUSB

ラップトップUSBコンソール(LUC) 接続（SN1100CO/SN1100COD/SN0100CO/SN0100CODシリーズのみ）が確立すると、SNビューアUSBアプリケーションを自動的に表示し、下図のような画面でログインパスワードが求められます。



初回ログインの際には、アドミニストレーターのデフォルトのアカウントを使用してください。

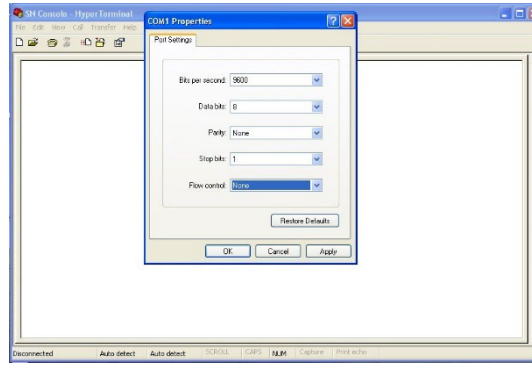
ユーザーネーム：administrator
パスワード：password

ログイン後、システムは強制的にパスワードを変更します。パスワードはデフォルトとは異なる文字列を設定してください。

コンソールからのログイン – ハイパーターミナル

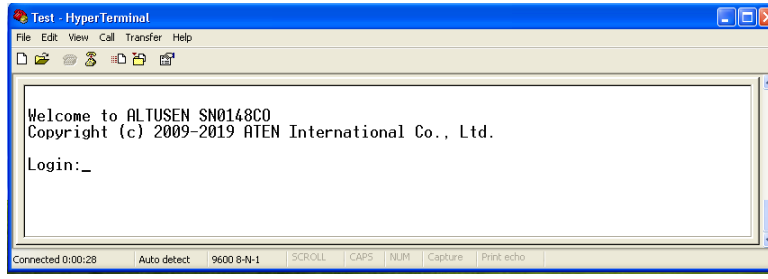
コンピューターとシリアルコンソールサーバーの間で物理的な接続が完了したら、下記の手順でハイパーターミナルのセッションを確立してください。

1. ハイパーターミナルを起動し、COM1ポートのポート設定をしてください。



ボーレート(bps):**9600**、データビット:**8**、パリティー:**なし**、
ストップビット:**1**、フローコントロール:**なし**

2. 設定が正しいと、下図のようなログインプロンプトを表示します。



初回ログインの際には、アドミニストレーターのデフォルトのアカウントを使用してください。

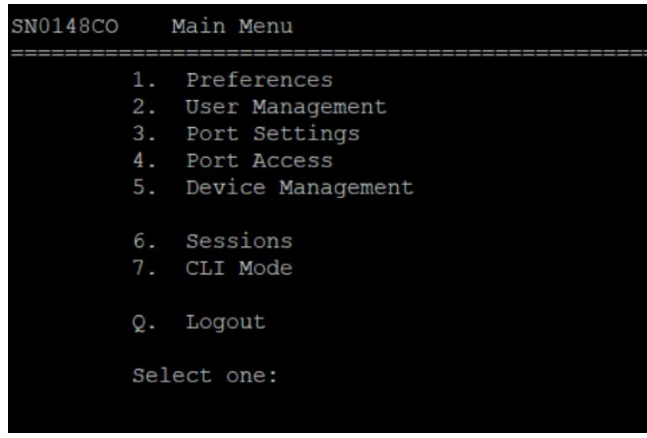
ユーザーネーム:administrator

パスワード:password

ログイン後、システムは強制的にパスワードを変更します。パスワードはデフォルトとは異なる文字列を設定してください。

ローカルコンソールのメインメニュー

ハイパーターミナルまたはSNビューアUSBでログインすると、テキストベースのメニューを表示します。



ローカルログインのメインメニューはテキストベースで利用できます。本マニュアル全体で説明しているブラウザーベースの設定や管理機能と同等です。サブメニューの操作に関しては、ブラウザー版での情報を参照してください。

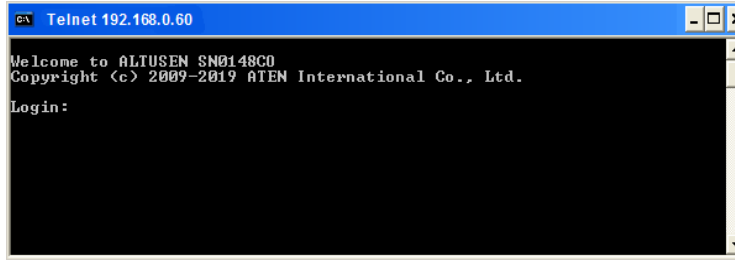
リモートログイン

シリアルコンソールサーバーには、コンピューターから、TelnetやPuTTY、またウェブブラウザーを使ってリモートログインできます。

TelnetやPuTTY用のリモートログインのメインメニューはテキストベースで利用できます。本マニュアル全体で説明しているブラウザーベースのGUIや管理機能と同等です。詳細はウェブブラウザー版の情報を参照してください（p.50参照）。テキストサブメニューを使用して作業し、この章で説明する設定を紹介しています。

Telnetによるログイン

Telnetを起動したら、「open 192.168.0.60」と入力し、**[Enter]**キーを押してください。下図のようなログインプロンプトを表示します。



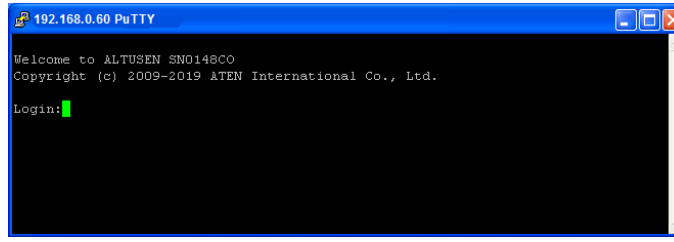
初回ログインの際には、デフォルトのアドミニストレーターのアカウントを使用してください。

ユーザーネーム：administrator
パスワード：password

ログイン後、システムは強制的にパスワードを変更します。パスワードはデフォルトとは異なる文字列を設定してください。

PuTTYによるログイン

PuTTYを起動したら、シリアルコンソールサーバーのデフォルトIPアドレス(192.168.0.60)を入力し、「**Open**」をクリックしてください。下図のようなログインプロンプトを表示します。



初回ログインの際には、アドミニストレーターのデフォルトのアカウントを使用してください。

ユーザーネーム：administrator
パスワード：password

ログイン後、システムは強制的にパスワードを変更します。パスワードはデフォルトとは異なる文字列を設定してください。

ブラウザーからのログイン

シリアルコンソールサーバーがLANに接続すると、各種プラットフォームで動作している対応インターネットブラウザーからアクセスできます。シリアルコンソールサーバーにアクセスするには、下記の手順に従って操作をしてください。

1. ウェブブラウザーを起動し、アドレスバーにシリアルコンソールサーバーのデフォルトIPアドレス(192.168.0.60)を入力したら、**[Enter]**キーを押してください。

2. 「セキュリティーの警告」ダイアログボックスを表示しますが、この証明書は信頼できますので、受け入れてください。

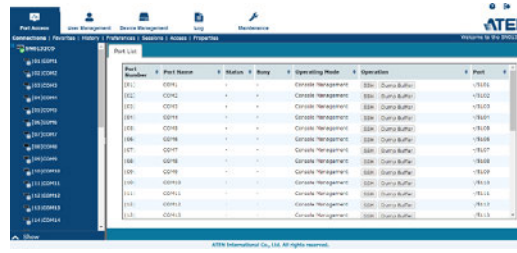
   または「このサイトの閲覧を続行する(推奨されません)」をクリックすると、ログイン画面を表示します。

3. 初回ログインの際には、アドミニストレーターのデフォルトのアカウントを使用してください。

   ユーザーネーム:administrator
   パスワード:password

   ログイン後、システムは強制的にパスワードを変更します。パスワードはデフォルトとは異なる文字列を設定してください。

   ログインに成功すると、下図のようなメイン画面を表示します。



IPインストーラーでログインIPアドレスを検索するには

シリアルコンソールサーバーのデフォルトIPアドレス(192.168.0.60)を使用してログインできない場合は、シリアルコンソールサーバーに別のネットワークデバイス(DHCPまたは固定)から別のIP アドレスが割り当てられている可能性があります。ATEN公式ウェブサイトからIPインストーラーユーティリティーをダウンロードして、新しいIPアドレスを確認できます。

次の手順に従ってIPインストーラーユーティリティーをダウンロードし、ユーティリティーを使用してシリアルコンソールサーバーのIPアドレスを検索します。

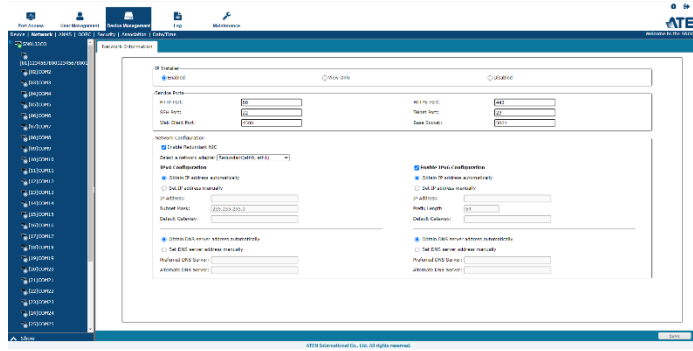
1. 以下のダウンロードリンクに移動します。
   https://www.aten.com/jp/ja/supportcenter/downloads/
2. 「他の製品の資料をダウンロードする」の下の欄にシリアルコンソールサーバーの型番を入力し、「**OK**」を押します。
3. 画面を下にスクロールし、使用可能なシリアルコンソールサーバーをクリックします。
4. 画面を下にスクロールして、「ソフトウェア＆ドライバー」の下にあるIPインストーラーのzipファイルを探して、ダウンロードするファイルをクリックします。
5. ダウンロードしたIPインストーラーを解凍して実行します。ネットワークデバイスのIPインストーラー画面を表示します。
6. 「**一覧表示**」をクリックして、ネットワーク内のATENデバイスを検索します。検出したデバイスをデバイスリストに表示します。
7. 任意のシリアルコンソールサーバーのIPアドレスを使用してログインします。

セットアップ

ネットワーク設定

ネットワークを設定するには、下記の手順に従って操作をしてください。

1. 「**デバイス管理**」タブをクリックしてください。
2. 「**ネットワーク**」タブを選択してください。



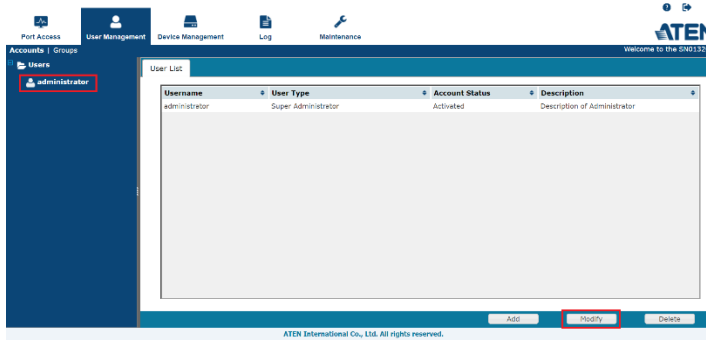
3. p.122「ネットワーク」に記載した情報に従って、各項目に値を入力してください。

スーパーアドミニストレーターのログイン情報の変更

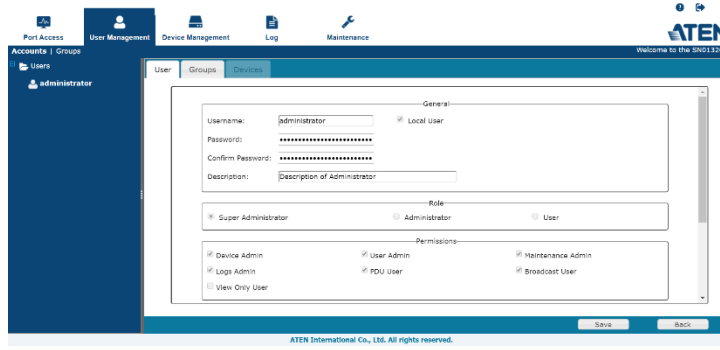
デフォルトのスーパーアドミニストレーターのユーザーネームとパスワードを変更するには、下記の手順に従って操作をしてください。

1. 画面上部にある「**ユーザー管理**」タブをクリックしてください。

   「ユーザー管理」画面は、左側のサイドバーにユーザーとグループのリストが表示され、大きな中央パネルにはユーザーの詳細情報を表示します。初めてログインした場合は、スーパーアドミニストレーターだけが表示します。



2. アカウントを左パネルからクリックするか、中央パネルで選択するかして、(画面下部にある)「**変更**」をクリックしてください。
「ユーザー情報」画面を表示します。



3. ユーザーネームとパスワードを固有のものに変更してください。

4. パスワードが正しいか確認するために、「確認用パスワード」欄にパスワードを再度入力してください。

5. (画面下部にある)「**保存**」をクリックしてください。

6. 正常な変更を知らせるダイアログボックスが表示されたら、「**OK**」をクリックしてください。

第4章
ユーザーインターフェース

概要

ログインに成功すると、シリアルコンソールサーバーのメイン画面が表示します。画面の外観は、ログインの手段によって若干異なります。各インターフェースについては、後続のセクションで説明します。

アクセス

シリアルコンソールサーバーには、ターミナルアプリケーションソフトウェア(Microsoft HyperTerminal など)を実行しているローカルコンソール(ローカルに接続したコンピューターまたはノートパソコン)またはSNビューアUSBアプリケーション、またはTelnet (SSH)、PuTTY、またはウェブベースのブラウザーを使用してリモートコンピューターからアクセスできます(詳細については、p.44「初期設定」を参照)。

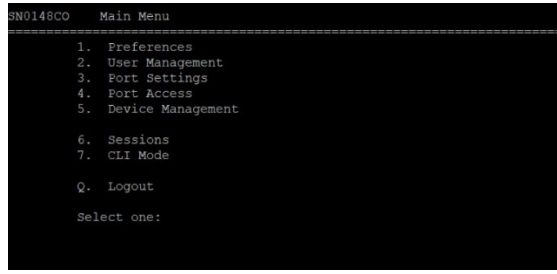
どのような方法でアクセスしても、シリアルコンソールサーバーの認証手順には、正しいユーザーネームとパスワードの入力が必要です。間違ったログイン情報が入力すると、認証ルーティーンから、「無効なユーザーネームまたはパスワード」や「ログイン失敗」のメッセージが返ってきます。この類のメッセージを表示した場合は、正しいユーザーネームとパスワードで再ログインしてください。

注意:

無効なログイン試行が一定の回数を超えると、タイムアウト時間が作動します。この場合、このタイムアウト時間が経過するまで、再ログインができなくなります。詳細については、p.142「ログイン失敗」を参照してください。

ローカルコンソールの操作

ローカルコンソールを接続している場合(SN1100CO/SN1100COD/SN0100CO/SN0100CODシリーズのみ、p.37を参照)、ハイパーターミナルまたはSNビューアUSBアプリケーションを使用してログインできます(詳細については、p.44「ローカルログイン」を参照)。正しいユーザーネームとパスワードを入力し、**[Enter]**キーを押すと、ローカルコンソールのメイン画面を表示します。



メインメニューはテキストベースで利用できます。本マニュアル全体で説明しているブラウザーベースのGUIや管理機能と同等です。設定と制御のフル機能を使用したい場合は、ブラウザーベースのウェブGUIの使用を推奨します。サブメニューの操作に関しては、ブラウザー版の情報を参照してください。

注意:

1. ブラウザー版と同様に、サブメニューの大半へのアクセスは、ユーザーの権限によって制限されます。操作権限がないサブメニューにアクセスしても利用できません。
2. 一部のサブメニューには、「終了」の選択肢がありません。このような場合は、**[Enter]**キーを2回押すと、変更せずに前のメニューに戻ります。
3. セッションが有効である間は、いつでもメインメニューを呼び出せます。
4. このメニューは、Windows Telnetクライアントや PuTTYなどリモートターミナルセッションからもアクセスできます。

セッションを終了したら、メインメニューを呼び出して、**[Q]**キーを押してログアウトしてください。

オフラインになったら、ウィンドウを閉じてください。

リモート操作

リモートコンソールサーバーには、ウェブブラウザー、またはTelnetやPuTTYなどテキストベースのターミナルアプリケーションを使ってリモートアクセスできます。詳細については、後続のセクションで説明します。

ウェブブラウザーからのログイン

シリアルコンソールサーバーには、各種プラットフォームで動作する対応インターネットブラウザーからアクセスできます。シリアルコンソールサーバーにアクセスするには、下記の手順に従って操作してください。

1. ブラウザーを開き、アクセス対象となるシリアルコンソールサーバーのIPアドレスを、ブラウザーのロケーションバーで指定します(詳細はp.50「ブラウザーからのログイン」参照)。

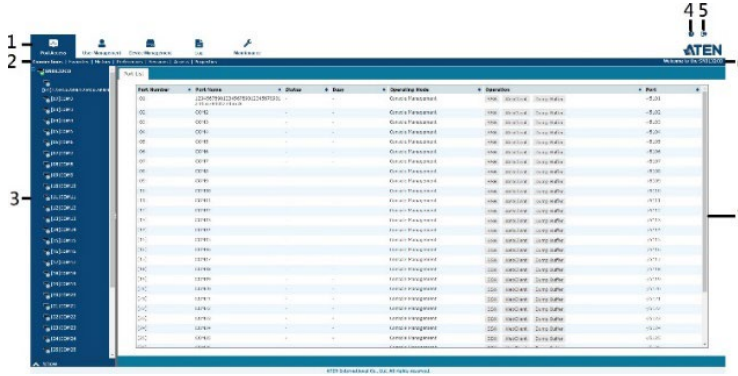
2. セキュリティー警告ダイアログボックスを表示したら、証明書を受け入れます。信頼できるものですので2番目の証明書を表示した場合も、同様に受け入れてください。

   または「このサイトの閲覧を続行する(推奨されません)」をクリックすると、ログイン画面が表示されます。

3. ユーザーネームとパスワードを入力し(p.50参照)、「**ログイン**」をクリックして、次のページで説明するウェブブラウザーのメイン画面を表示します。

ウェブブラウザーのメイン画面

マルチプラットフォームでの操作を保証するために、シリアルコンソールサーバーへのアクセスは、標準的なウェブブラウザーから操作できます。後続のセクションでは、ウェブブラウザー画面における各部分について詳しく説明します。ユーザーがログインし、システムに認証されると(p.56参照)、ウェブブラウザーのメイン画面を表示します。このとき、「ポートアクセス」タブが選択された状態になります。



注意:

説明には、スーパーアドミニストレーター用の画面を使用しております。ユーザーの種類や操作権限によっては、表示している全てのメニューが利用できるとは限りません。

画面各部名称

ウェブ画面における各部名称と説明は、下表の通りです。

番号	項目	説明
1	タブバー	タブバーには、シリアルコンソールサーバーの主な操作カテゴリーを表示します。このタブバーに表示する項目は、ユーザーアカウントを開設した際のユーザーのタイプと割り当てた操作権限によって決まります。
2	メニューバー	メニューバーには、タブバーで選択した操作に関連するサブカテゴリーを表示します。このメニューバーに表示する項目は、ユーザーアカウントを開設した際のユーザーのタイプと割り当てた操作権限によって決まります。

番号	項目	説明
3	サイドバー	操作中のタブやメニューバーに対応したポートリストがこの部分に表示します。サイドバーのノードをクリックすると、詳細画面が表示されます。 サイドバーの下にある「フィルター」ボタンを使うと、ツリーに表示するポートの範囲を変更できます。
4	バージョン情報	シリアルコンソールサーバーに現在インストールしているファームウェアのバージョンに関する詳細を表示します。
5	ログアウト	このボタンをクリックすると、シリアルコンソールサーバーにおける現在のセッションからログアウトします。
6	初期メッセージ	この機能が有効の場合（p.85参照）、ウェルカムメッセージをこの部分に表示します。
7	詳細表示パネル	メインの作業領域です。選択したメニューやサイドバーのノードに応じたメニューが表示されます。

タブメニュー

画面上部のタブメニューに表示するアイコンの数およびタイプは、ユーザータイプ（スーパーアドミニストレーター、アドミニストレーター、ユーザー）や、ユーザーに付与した操作権限によって決定します。後続のセクションでは、ウェブブラウザー画面における各部分について詳しく説明します。各アイコンが表す機能は下表の通りです。

アイコン	機能
	**ポートアクセス**：シリアルコンソールサーバーに接続しているデバイスへのアクセス・操作の項目です。このメニューは全てのユーザーがアクセス可能です。本メニューの詳細についてはp.76を参照してください。
	**ユーザー管理**：ユーザーやグループの作成・管理の項目です。また、デバイスをユーザーやグループに割り当てます。なお、スーパーアドミニストレーターと、ユーザー管理権限のあるアドミニストレーターやユーザーのみアクセス可能です。権限の無いユーザーがログインした場合、このアイコンは表示しません。ユーザー管理については、p.100で説明します。
	**デバイス管理**：シリアルコンソールサーバーの全体的な操作に関するパラメーターの設定・管理タブです。この画面は、スーパーアドミニストレーターのほか、アドミニストレーターおよびデバイス管理の権限を与えたユーザーが利用できます。権限の無いユーザーがログインした場合、このアイコンは表示しません。本メニューの詳細についてはp.116を参照してください。
	**ログ**：ログファイルの内容を表示します。ログ画面については、p.150で説明します。

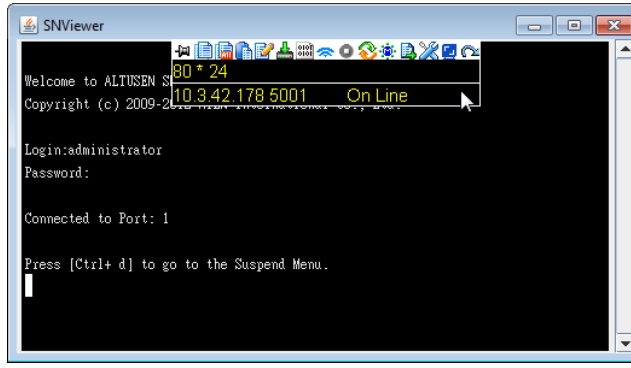
アイコン	機能
Maintenance	**メンテナンス**：製品のファームウェアアップグレード、設定およびアカウント情報のバックアップ・リストア、デフォルト値のリストア、証明書のインポートができます。なお、スーパーアドミニストレーター(およびメンテナンス権限のあるアドミニストレーターとユーザー)がアクセス可能です。それ以外のユーザーがログインした場合、このアイコンは表示しません。メンテナンス画面については、p.155で説明します。

画面右上には、2つの小さなアイコンが表示されます。各アイコンが表す機能は下表の通りです。

アイコン	機能
	このアイコンをクリックすると、シリアルコンソールサーバーのファームウェアバージョンに関する情報を示すパネルを表示します。
	このアイコンをクリックすると、ログアウトし、シリアルコンソールサーバーセッションを終了します。

SNビューア

SNビューアは、ウェブブラウザーからシリアル機器にアクセスする際に使用するメインアプリケーションです。シリアルデバイスの**Telnet** または**SSH** ボタンをクリックすると、SNビューアが起動し、「ポートアクセス」>「接続」画面を表示します（詳細については、p.80「Telnet/SSH/WebClient」を参照）。SNビューアを起動すると、マウスカーソルを動かしたときに表示するコントロールパネルのツールバーが利用できます。コントロールパネルでは、セッションの設定ができます。



SNビューアのコントロールパネル

SNビューアのコントロールパネルは、画面上部中央に隠れていますが、マウスカーソルを移動させると表示されます。このコントロールパネルは上部のメニューアイコン1行と、下部のテキスト2行から構成しています。

◆ デフォルトでは、上側のテキスト行にはウィンドウサイズの幅と高さを表示します。ただし、アイコンバーのアイコンの上にマウスポインターを移動させると、アイコンの機能説明がこの部分に表示されます。また、メッセージボードに他のユーザーからメッセージが書き込まれて、メッセージが未読の場合は、メッセージボードのウィンドウを自動的にポップアップ表示します。

◆ 3段目のテキスト行には、アクセス中の機器のIPアドレスとポート番号が左側に、接続ステータスが右側にそれぞれ表示します。

コントロールパネルの機能

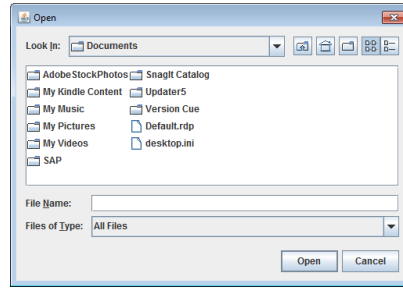
コントロールパネルの各機能は、下表および後続のセクションで説明します。

アイコン	機能
	クリックすると、コントロールパネルを常に前面に表示します。つまり、SNビューア画面の上に常に表示します。もう一度クリックすると、自動非表示モードで表示し、マウスを上に移動したときにのみ表示します。
	画面上で選択したテキストをコピーします。
	画面上に表示した全てのテキストをコピーします。
	コピーしたテキストをペースト(貼り付け)します。
	このアイコンをクリックすると、ログのオン・オフを交互に切り替えます。シリアル機器からSNビューアに送られたテキスト形式のログファイルを開始します。この機能を使うには、最初にテキストベースのログファイルを作成し、インポートしておく必要があります(p.64「ターミナル設定」の「その他 – ログファイル」を参照)。

アイコン	機能
	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)。
	画面のエンコーディング方法を変更します(p.62「エンコード」参照)。
	ブロードキャスト機能を有効にします。ブロードキャスト機能を使うと、1つのポート操作を、全てのブロードキャストポートに対して同様に適用できます。ブロードキャスト機能を使用する前に、「ブロードキャストのタイムアウト」と「ブロードキャストポート」を設定しておいてください(詳細はp.84「ユーザー設定」参照)。 ブロードキャストを機能させるためには、ポートにブロードキャストポートとしてアクセスして、コントロールパネルにあるブロードキャストアイコンをクリックしてください。
	ブレークコマンドを送信します。
	ターミナルをリセットし、デフォルトの設定に戻します。
	クリックすると、メッセージボード(p.62参照)を起動します。
	クリックすると、ウィンドウを開き、カスタムテキストマクロのリストを作成します(p.63「マクロ」参照)。
	フォント、色、その他のSNビューアの設定を変更します(p.64「ターミナル設定」参照)。
	SNビューアのウィンドウ幅を調整します。
	ビューアを終了します。

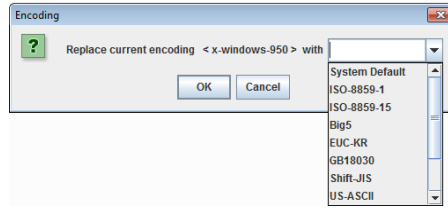
データのインポート

「データのインポート」アイコンをクリックすると、下図のようにインポートするデータを選択できる標準的なブラウザーメニューを表示します。



エンコード

使用するエンコードの種類を選択できます。下図のように、ドロップダウンメニューからエンコードの種類を選択して、「OK」をクリックしてください。

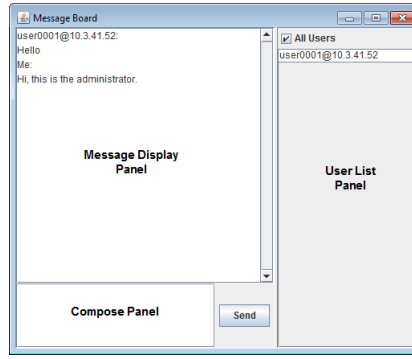


注意:

コードが文字化けした場合は、別のエンコーディングを選択してみてください。例えば、ポート名に韓国語、日本語、繁体字または簡体字中国語の名前を付けた場合は、UTF-8 エンコードを試して、「フォント」に「等幅フォント」を選択します。

メッセージボード

シリアルコンソールサーバーはマルチユーザーによるログインに対応していますが、異なるユーザーによる同時アクセスは、アクセスの競合を招くおそれがあります。この問題を緩和するために、ユーザー同士のコミュニケーションを可能にするメッセージボード機能が利用できます。



メッセージ表示パネル

ユーザーがメッセージボードに送信したメッセージをこのパネルに表示します。

メッセージ編集パネル

メッセージボードに送信したいメッセージをこのパネルで編集してください。「**送信**」ボタンをクリックすると、メッセージがメッセージボードに送信します。

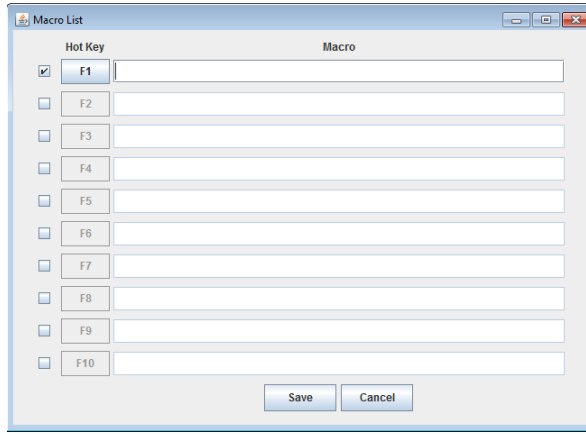
ユーザーリストパネル

現在ログイン中の全ユーザーのユーザーネームとIPアドレスがこのパネルに表示されます。

- 「**全てのユーザー**」にチェックを入れると、メッセージを全てのユーザーに送信します。特定のユーザー宛にメッセージを送信したい場合は、宛先となるユーザーを選択してからメッセージを送信してください。
- 一旦、ユーザーの名前を選択した状態で再び全員宛にメッセージを送信したい場合は、「**全てのユーザー**」を選択してからメッセージを送信してください。

マクロ

この機能を使うと、SNビューアのアプリケーション上で使用するテキストマクロを作成できます。「マクロ」アイコンをクリックすると、以下のような画面が表示されます。



チェックボックスにチェックを入れて、テキストマクロに入力し、「**保存**」をクリックしてください。作成したカスタムテキストマクロを動作させるには、このマクロに関連するファンクションキー(F1～F12)を使ってください。

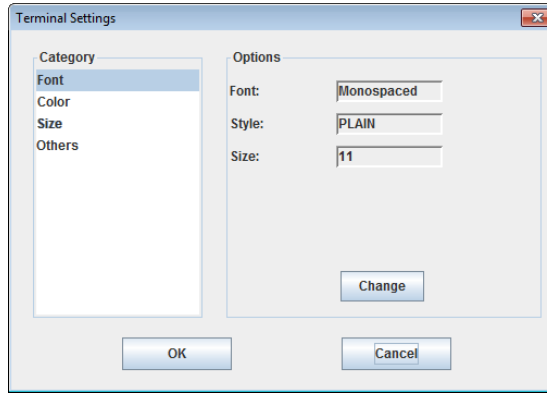
ターミナルアプリケーション

シリアルコンソールサーバーには、TelnetやPuTTYのようなテキストベースのターミナルアプリケーションを使ってリモートログインできます。接続やログインの方法については、p.44「リモートログイン」を参照してください。

TelnetやPuTTYのメインメニューはテキストベースで利用できます。本マニュアル全体で説明しているブラウザーベースの設定や管理機能と同等です。サブメニューの操作に関しては、ブラウザー版の情報を参照してください。ログインすると、次のようなテキストベースのメニューを表示します。

ターミナル設定

「ターミナル設定」画面では、以下に説明するように、ターミナルウィンドウの外観を変更できます。



カテゴリー	説明
フォント	SNビューアのフォント設定を変える場合は「**変更**」をクリックしてください。フォントの種類やサイズ、またスタイルを変更できます。ウィンドウの右側では、設定したフォントのプレビューを確認できます。
色	「**オプション**」を選択してください。オプションには、文字表示色、背景色、カーソルテキストの色、カーソルの色があります。「**変更**」をクリックして色の設定を調整してください。色の詳細設定をする場合は、「HSL」、「見本」、「HSV」の各タブを使用してください。 タブの下には「**プレビュー**」セクションがあります。選択した色がどのように見えるのかを確認できます。 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。

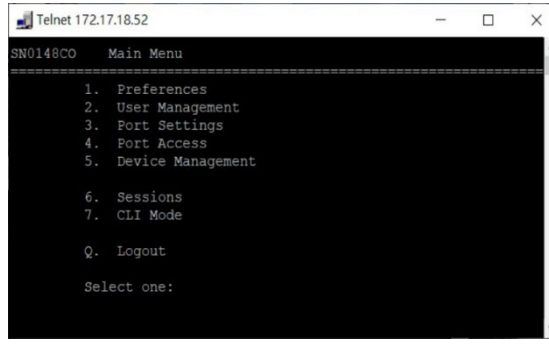
カテゴリー	説明
サイズ	ウィンドウのサイズによって、表示する情報の量が決まる場合があります。SNビューアのウィンドウサイズを設定するには、このカテゴリーに移動して、列サイズと行サイズの各項目を変更します。
その他	このセクションは、次の設定をする際に使用してください。 ◆ 改行コードにCR+LFを使用する：このボックスにチェックを入れると、[Enter]キーを使用した際にCR(キャリッジリターン)を付加します。このため、カーソルは左端の行頭に移動します。[Enter]キーを押した後でテキストが左側の余白で1行にならない場合は、この機能を使ってください。 ◆ Backspaceは[Delete]キーです。 ◆ ローカルエコー：エコーとは、シリアル機器から入力した文字列の応答です。 ➢ **自動**：入力した文字列がエコーしますが、画面には表示されません。 ➢ **強制オン**：入力した文字列がエコーす、入力すると画面にも表示されます。このモードでは、パスワードも画面に表示されます。 ➢ **強制オフ**：文字列はシリアル機器からエコーしません。 ◆ 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、接続したシリアル機器からSNビューア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など外部エディターでテキストファイルとして作成して開いておいてからSNビューアのコントロールパネルからログ機能をオン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)。

ターミナルアプリケーション

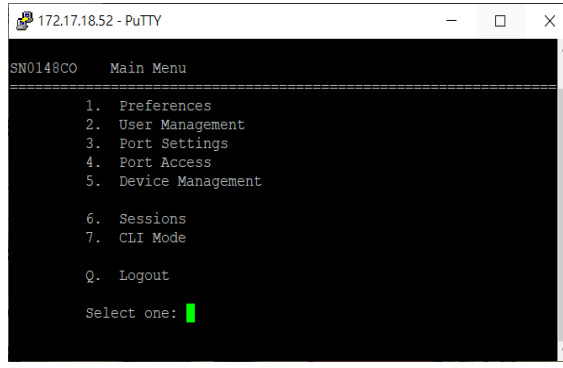
シリアルコンソールサーバーには、TelnetやPuTTYのようなテキストベースのターミナルアプリケーションを使ってリモートログインできます。接続やログインの方法については、p.48「リモートログイン」を参照してください。

TelnetやPuTTYのメインメニューはテキストベースで利用できます。本マニュアル全体で説明しているブラウザーベースの設定や管理機能と同等です。サブメニューの操作に関しては、ブラウザー版の情報を参照してください。ログインすると、次のようなテキストベースのメニューを表示します。

Telnetメニュー形式のテキストUI

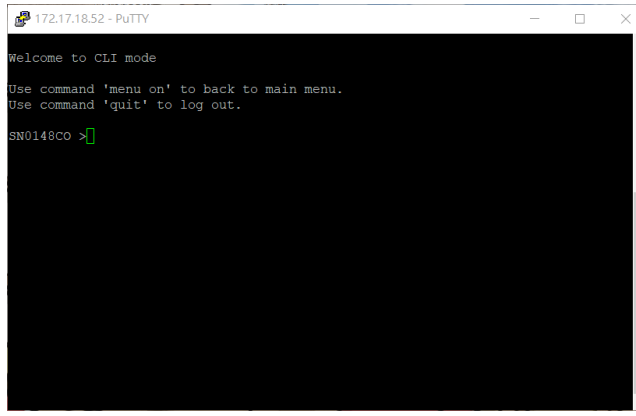


PuTTYメニュー形式のテキストUI



特定のタスクを実行するためにテキスト行を介してコマンドを入力する場合

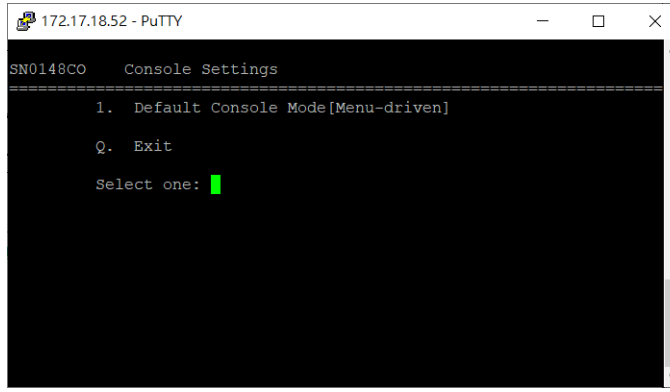
は、項目7の「CLI モード」を選択して、メニュー形式のテキストUI からCLI(コマンドラインインターフェース)に切り替えます。



インターフェースをCLIモードからメニュー駆動モードに切り替えるには、コマンド"menu on"を入力します。

制御および設定のコマンドの詳細については、p.191「CLIコマンド」を参照してください。

テキストベースのメニューまたはCLI モードをデフォルトモードに設定するには、「5 .デバイス管理」>「17.コンソール設定」>「1.デフォルトコンソールモード[メニュー駆動]」に進んでください。



WebClient

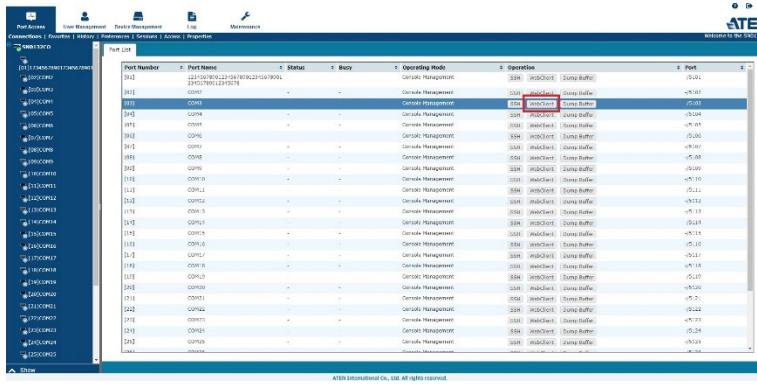
WebClient（マイナーチェンジ版のv3.2.312から搭載機能)にアクセスしてシリアルコンソールサーバーを管理するには、次の手順に従います。

注意：

ポート4500が開いており、アクセス可能であるか確認してください。

---

1. 「ポートアクセス」>「接続」画面に移動したら、ポート一覧から設定するポートを選択し、「操作」メニューの下の「**WebCleint**」をクリックします。



2. ポップアップウィンドウが開き、**[Ctrl] + [d]** を押して、サスペンドメニューに移動します。

```
Connected to Port: 3

Press [Ctrl+ d] to go to the Suspend Menu.
```

3. **ポートID**を入力して**[Enter]**を押すと、別のポートを設定用に選択できます。設定画面に移動するには、**[q] + [Enter]**を押します。

```
SN0132CO    Port Access
================================================================================
 1. 12345678901234567890123456789012345678901234567890123456789012345678
 2. COM2
 3. COM3
 4. COM4
 5. COM5
 6. COM6
 7. COM7
 8. COM8
 9. COM9
10. COM10
11. COM11
12. COM12
13. COM13
14. COM14
15. COM15
16. COM16
17. COM17
18. COM18
19. COM19
20. COM20
21. COM21
22. COM22
23. COM23
24. COM24
25. COM25
26. COM26
27. COM27
28. COM28
29. COM29
30. COM30
31. COM31
32. COM32


 R. Resume [Connect to Port 3]
 B. Send Break    [ to Port 3]
 Q. Exit

 Press [R] to reconnect to the specified port.
 Press [B] to send break to the specified port.
Select one:
```

4. メインメニューを表示します。メインメニューはテキストベースで利用できます。本マニュアル全体で説明しているブラウザーベースのGUIや管理機能と同等です。設定と制御のフル機能を使用したい場合は、ブラウザーベースのウェブGUIの使用を推

奨します。サブメニューの操作に関しては、ブラウザー版の情報を参照してください。

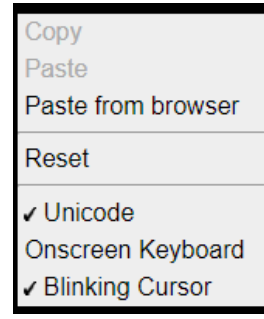
注意:

1. ブラウザー版と同様に、サブメニューの大半へのアクセスは、ユーザーの権限によって制限されます。操作権限がないユーザーはサブメニューにアクセスしても利用できません。
2. セッションが有効である間は、いつでもメインメニューを呼び出せます。

セッションを終了したら、メインメニューを呼び出して、[Q]キーを押してログアウトしてください。オフラインになったら、ウィンドウを閉じてください。

WebClientのその他の機能

WebClient では、マウスを右クリックして他の機能を呼び出せます。

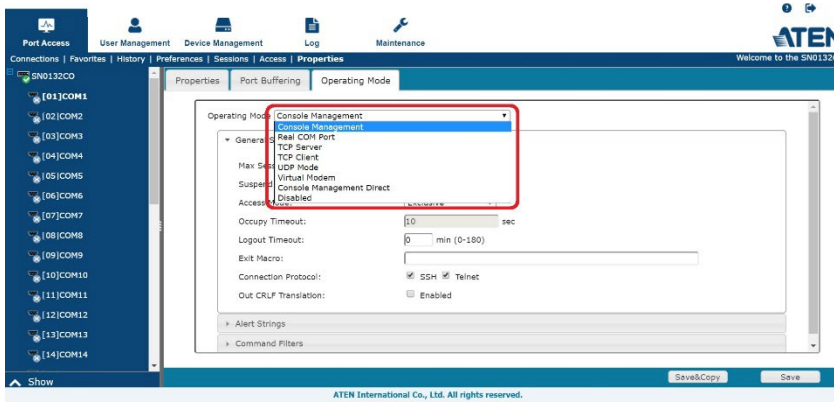


機能	説明
コピー	WebClientで強調表示したテキストをコピーします。
貼り付け	WebClientからコピーしたテキストを貼り付けます。
ブラウザーから貼り付け	コピーしたテキストのうち、WebClientからコピーしていないものを貼り付けます。
リセット	現在のポートをリセットします。
ユニコード	WebClientで文字化けが発生した場合はチェックを入れてください。
オンスクリーンキーボード	チェックを入れた場合は、オンスクリーンキーボードを表示します。
カーソルの点滅	チェックを入れた場合は、カーソルの点滅を有効にします。

第5章
ポート動作モード

概要

シリアルコンソールサーバーのCOMポートは、各種シリアルアプリケーションに対応できるよう、複数のポート動作モードをサポートしています。デバイス制御用のコンソール管理およびコンソール管理ダイレクトモード、シリアル-イーサネット接続用のリアルCOM ポート、バーチャルモデム、TCP サーバー、TCP クライアント、およびUDP モード、および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が含まれます。各動作モードによって実行する機能については、後続のセクションで説明します。



「**動作モード**」は、上図にあるように、「ポートアクセス」タブの「プロパティー」メニューにある、「動作モード」の画面から選択できます。本章で説明する「ポート動作モード」は、この画面から設定できます。全ての設定に関する詳細は、p.92「動作モード」を参照してください。

動作モード

各動作モードの設定に関する詳細は、p.92「動作モード」を参照してください。

コンソール管理

コンソール管理モードは、最も使う動作モードです。ユーザーはこのモードで、シリアルコンソールサーバーに対してリモートからTelnetまたはSSHセッションでアクセスし、シリアル機器への接続を切り替えてアクセスできます。このモードでは、ユーザーはウェブブラウザーで動作するSNビューアのアプリケーションでもTelnetまたはSSH経由でログインできます。また、リモートからはSSHやPuTTY、ダイレクト接続ではハイパーターミナルやSNビューアUSBアプリケーションをそれぞれ使用して、ログインできます。

コンソール管理の設定に関する詳細は、p.92を参照してください。

注意：

「ネットワーク」画面で指定したソケットの設定内容が、機器が実際にリッスンしているポートに対応しているか確認してください。シリアルコンソールサーバーでデフォルト設定のポート番号は5001です（p.122「ネットワーク」およびp.123「ベースソケット」参照）。

リアルCOMポート

リモートユーザーのローカルコンピューターにインストールしたバーチャルCOMドライバーと連動して機能します。シリアルコンソールサーバーのCOMポートがこのモードに設定するとポートに接続した機器は、あたかもリモートユーザーのローカルコンピューター上のCOMポートに直接接続した機器のように表示します。

POSターミナル、バーコードリーダー、シリアルプリンターなどで使うのに便利です。なぜなら、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使用できるからです。

シリアルコンソールサーバー用Windowsシステム用のリアルCOMドライバー、およびLinuxシステム用のTTYドライバーはATEN公式の製品ページからダウンロードします。

リアルCOMポートの設定に関する詳細は、p.95を参照してください。

TCPサーバー/TCPクライアント(シリアルトンネル)

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での通信が利用できます。

TCPサーバー(ローTCP)

TCPサーバー(ローTCP)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シリアルコンソールサーバーとの通信を開始し、シリアルポートに対して接続をリクエストします。

接続が確立すると、ホスト側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、データはホストと機器の間において双方向で通信します。この動作モードは、128ビット/256ビットSSLデータ暗号化通信(TLS v1.0/TLS v1.1/ TLS v1.2)に対応しています。

シリアルコンソールサーバーは、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。複数のコンピューターがシリアル機器と同時に通信可能になります。

TCPサーバーの設定に関する詳細は、p.95を参照してください。

注意:

「ネットワーク」画面で指定したソケットの設定内容が、機器が実際にリッスンしているポートに対応しているか確認してください。シリアルコンソールサーバーでデフォルト設定しているポート番号は5301です。(p.122「ネットワーク」およびp.123「ベースソケット」参照)

TCPクライアント

TCPクライアントモードでは、シリアルデータがシリアルコンソールサーバーのシリアルポートに到達すると、シリアルコンソールサーバーがホストコンピューターと通信を開始し、ホスト側にシリアルデータを送出します。シリアルコンソールサーバーは、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。また、この動作モードは、128ビット/256ビットSSLデータ暗号化通信(TLS v1.0/TLS v1.1/TLS v1.2)に対応しています。

TCPクライアントの設定に関する詳細は、p.96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、より効率的に通信します。UDPモードでは、通信が双方向で行われます。シリアル機器はシリアルコンソールサーバーの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ができます。

TCPのような徹底的な方法ではエラーチェックを行わないため、UDPは、データ精度に最適化した低速の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。

UDPモードの設定に関する詳細は、p.96を参照してください。

バーチャルモデム

バーチャルモデムモードでは、シリアルコンソールサーバーのCOMポートがモデムをエミュレートします。このポートは、リモートサーバーの通信で実在のモデムのような役割を果たします。このモードにてシリアルモデム間のリンクでデータを転送できるように設計したソフトウェアは、TCP/IPイーサネット接続でシリアル操作を実行が可能になります。このモードでは、シリアルコンソールサーバーは通信に適切なポートアドレスを指定して、リモートサーバーのIPにダイヤル接続します。以下は、その例です。

例: atd 10.0.100.101:5000

シリアルコンソールサーバーのバーチャルモデム機能のデータ構造と関連機能の詳細は、p.183に記載しています。

バーチャルモデムの設定に関する詳細は、p.97を参照してください。

注意:

この動作モードは、128ビット/256ビットSSLデータ暗号化通信(TLS v1.0/TLS v1.1/TLS v1.2)に対応しています。

コンソール管理ダイレクト

このモードを使うと、ユーザーはポートに接続しているサーバーやシリアルデバイスに対して、PCから直接TelnetまたはSSHセッションを確立できます。このため、接続を確立するのに、ウェブブラウザー経由でシリアルコンソールサーバーにログインする必要がなくなります。この場合、ユーザーは、Telnet、SSHまたはPuTTYなどシリアルコンソールを使ってPCから直接シリアルデバイスにログインできます。

コンソール管理ダイレクトの設定に関する詳細は、p.98を参照してください。

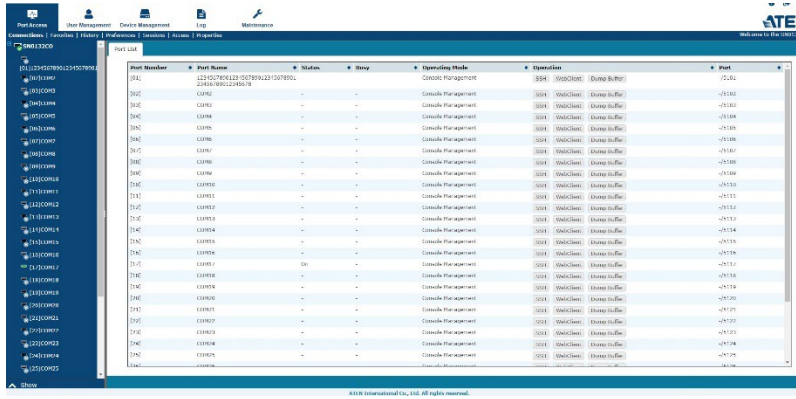
無効

このモードでは、シリアルコンソールサーバーのシリアルポートは動作しません。

第6章
ポートアクセス

概要

ウェブブラウザーからシリアルコンソールサーバーにログインすると、「ポートアクセス」タブの「接続」メニュー選択しているメイン画面を表示します。



「接続」画面は、複数のメインエリアから構成しています。ユーザーがアクセス権限を持っている機器やポート、および、アウトレットは全て、画面の左側にあるサイドバーに一覧表示します。

サイドバーでポートを選択した後、メニューバーの項目をクリックすると、サイドバーで選択したアイテムに関する詳細と設定内容を表示する画面が開きます。

サイドバー

接続している全てのシリアルコンソールサーバー、ポートデバイス、Cisco Catalyst 2960-C シリーズ(サポートしている最新のネットワークスイッチについては製品ページを参照)、USBコンソールポート経由(詳細はファームウェアリリースノートを参照)、およびPDU デバイス(ポートとアウトレットを含む)は、画面左側のサイドバーにツリー構造で表示します。

サイドバーのツリービュー

サイドバーのツリービューには、次のような特長があります。

◆ ユーザーは、自分自身がアクセス権限を持つデバイスとポートのみを参照できます。

◆ ポートがグリーンの場合、シリアルデバイスがオンラインです。

◆ ポートがグリーンで、チェックマークが入っている場合、ユーザーがアクセスしている状態です。

◆ ポートやアウトレットや子機は、親機の下に入れ子にできます。
機器の前についている「+」を押すとツリーが展開し、入れ子になったアイテムを表示できます。反対に、「-」を押すとツリーが折りたたまれて、入れ子になったポートやアウトレットは表示しません。

フィルター

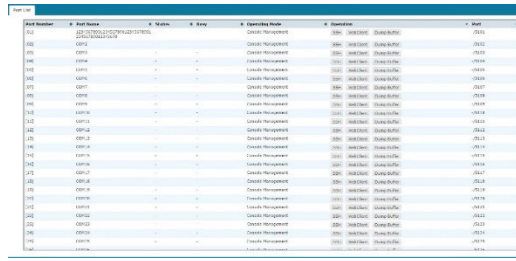
画面左下に「表示」という部分があり、サイドバーに表示するポートの数とタイプを操作できるフィルター機能です。「表示」をクリックすると、パネルの下部が次の図のように変わります。

各項目の詳細は下表の通りです。

選択	説明
検索	検索したい文字列を入力して「検索」ボタンをクリックすると、ポートネームが文字列に一致するポートだけがツリーに表示します。ワイルドカード(1文字の場合は?、複数の文字の場合は*)や、「or」キーワードの使用が可能ですので、複数のポートを表示できます。 次に例を示します。 1. 「**Web***」と入力すると、「Web Server 1」と「Web Server 2」の両方がリストに表示されます。 2. 「**W*1 or M*2**」と入力すると、「Web Server 1」と「Mail Server 2」の両方がリストに表示します。

接続

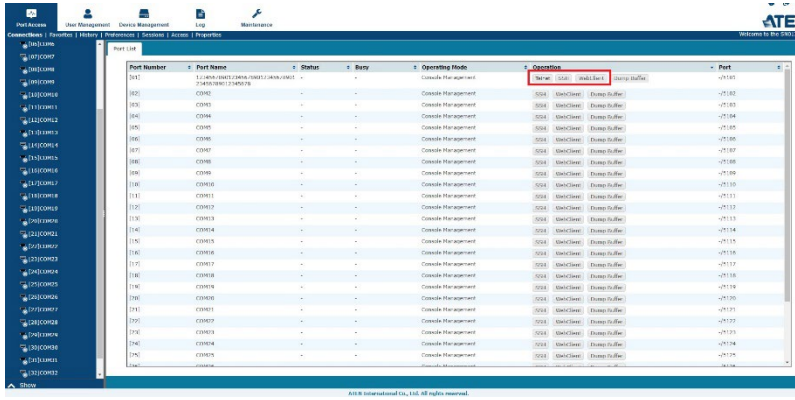
「接続」画面のメインパネルには、「ポート一覧」を表示します。ここからシリアル機器を選択し、この機器に対して接続ポート経由でアクセスできます。



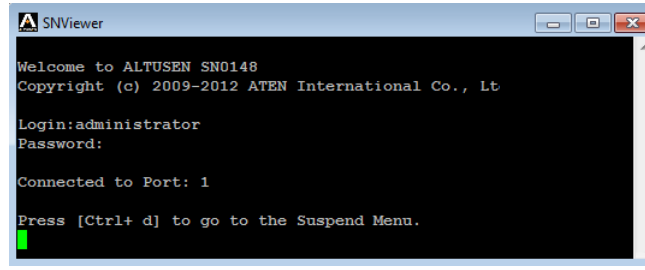
項目	説明
ポート番号	シリアルコンソールサーバーのリアパネルにある各ポートと同じ番号です。
ポートネーム	ポートネームを表示します。このポートネームは、「ポートアクセス」タブの「プロパティー」メニューで変更できます（詳細はp.89参照）。
状態	ポートに接続している機器の状態（**オン**または**オフ**）です。ポートに機器が接続していない場合は、「-」を表示します。
ビジー	ユーザーがシリアルコンソールサーバー経由でアクセスしていると、この欄に「**ビジー**」と表示します。
操作モード	ポートにアクセスするために設定している**動作モード**を一覧表示します。最も汎用性の高い設定は、「コンソール管理」です。「ポートアクセス」タブの「プロパティー」メニューにある「動作モード」タブで設定できます（詳細はp.92「動作モード」参照）。 **注意**：コンソール管理は、コンソールサーバーに接続しているシリアル機器にアクセスして操作する方法です。
操作方法	コンソール管理のアクセス方法を一覧表示します。 **TelnetおよびSSH**：ポートデバイスを管理する方法です。いずれかをクリックすると、SNビューアアプリケーションが開き、シリアルデバイスを管理します（p.80「Telnet/SSH/WebClient」参照）。 **バッファーのダンプ**：この機器で発生したアクティビティーのバッファーログをダンプして確認できます。クリックすると、ログを保存します。（詳細については、p.90「保存とコピー」を参照してください）。
ポート	シリアル機器へのアクセス用に設定したTelnetとSSHの各ポート番号を表示します（詳細はp.123「サービスポート」参照）。

Telnet/SSH/WebClient

シリアルコンソールサーバーに接続しているシリアルデバイスにアクセスするには、ポートの**Telnet**、**SSH**、または**WebClient**（p.68「WebClient」を参照）ボタンを「ポートアクセス」>「接続」画面からクリックします。



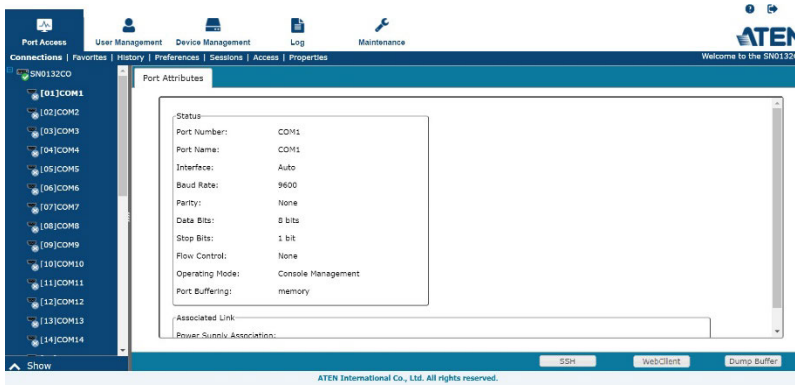
シリアルコンソールサーバーはSNビューアを開いて、シリアル機器とのセッションを開始します。このとき、下図のような画面を表示します。



シリアル機器へのログインや管理操作は、SNビューアからできます。SNビューアの詳しい使用方法については、p.59「SNビューア」を参照してください。

ポート属性

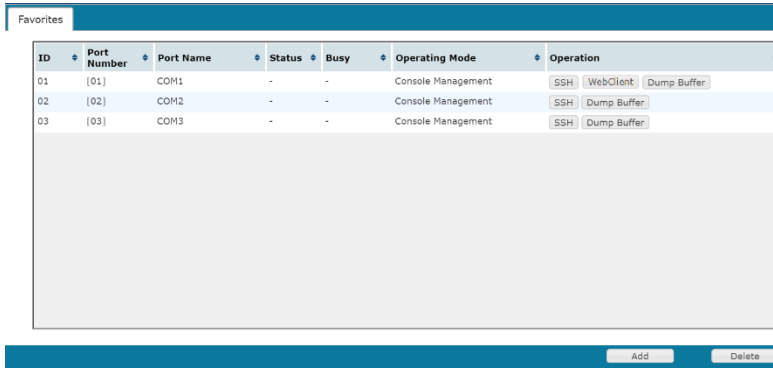
「ポートアクセス」>「接続」画面にあるサイドバーで機器をクリックすると、機器や電源管理デバイスの再起動オプションに関する詳細情報を確認できる「**ポート属性**」画面を表示します。



画面の下側にある「**Telnet**」、「**SSH**」、「**バッファーのダンプ**」の各ボタンを使えます。

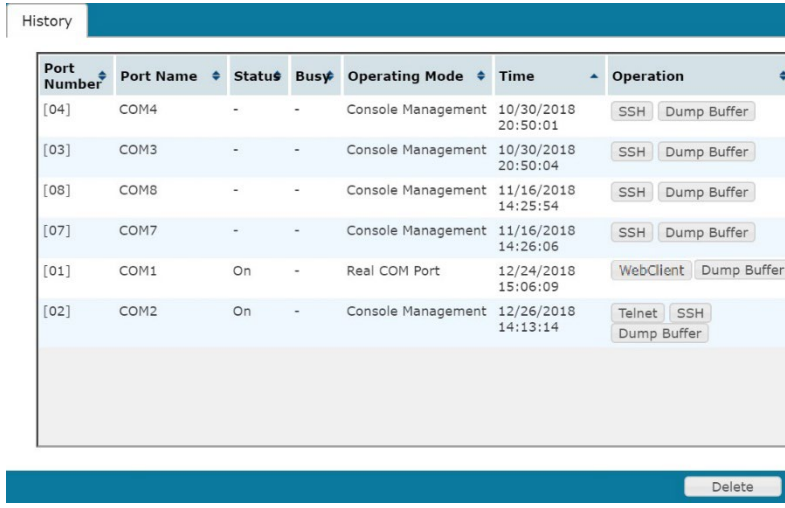
お気に入り

「お気に入り」タブは、頻繁にアクセスする接続を全てひとまとめにして、便利なところに保存しておく機能です。ポートをお気に入りに追加する場合は、サイドバーで対象となるアイテムを右クリックして、「**お気に入りに追加**」を選択するか、ポートを選択して「**追加**」をクリックしてください。「お気に入り」タブで利用できるレイアウトや機能は、「ポートリスト」タブにあるものと全く同じです(詳細はp.79「接続」を参照)。



履歴

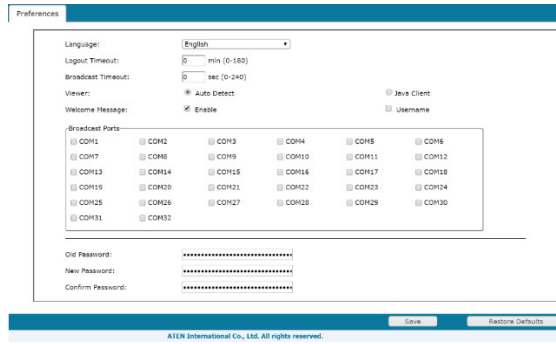
「履歴」タブでは、ポートをアクセスした記録を表示します。直近で使用したポートに簡単にアクセスできます。メインパネルに表示しているポートは、**Telnet**、**SSH**、または**WebClient**ボタンをクリックしてアクセスできます。



- ◆ 一画面を超える数のアイテムがある場合は、右側にスクロールバーを表示しますので、このスクロールバーを使って前のページや後のページにあるアイテムを確認できます。
- ◆ 記録を消去する場合は、画面の右下にある「削除」ボタンをクリックしてください。
- ◆ 一覧の項目をクリックすると、項目順に表示を変更します。

ユーザー設定

「ユーザー設定」画面では、ユーザー別の作業環境を設定できます。シリアルコンソールサーバーには、各ユーザーのプロフィールを個別に保存し、ログインダイアログボックスに入力したユーザーネームに従って作業環境を設定します。



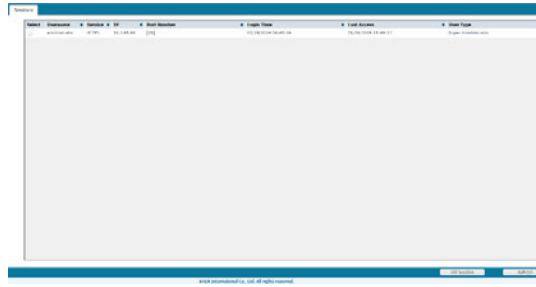
各項目の詳細は下表の通りです。

設定	機能
言語	ウェブGUIで使用する言語を選択してください。
ログアウトタイムアウト	ユーザーからの入力がないまま、この機能で設定した時間が経過すると、ユーザーは自動的にログアウトします。一旦ログアウトすると、シリアルコンソールサーバーに再びアクセスするのに、またログインが必要です。
ブロードキャストタイムアウト	ユーザーからの入力がないまま、この機能で設定した時間を経過すると、ブロードキャスト機能は自動的に終了します。0～240 秒の値を入力します。0(ゼロ)を設定すると、この機能を無効にします。 ブロードキャスト機能に関する詳細は、この表にある「ブロードキャストポート」の欄を参照してください。
ビューア	シリアル機器へのアクセスに使用するビューアを次から選択できます。 ◆ **自動検出**:使用しているウェブブラウザーに基づいて適切なビューアを選択します。Windows Internet Explorerをお使いの場合はWinClientを、その他のウェブブラウザー(例:Firefox)をお使いの場合はJavaClientを選択します。 ◆ **Java Client**:使用ブラウザーの種類にかかわらず、Javaベースのビューアを起動します。

設定	機能
初期メッセージ	サブメニューバーの初期メッセージやユーザーネームの表示・非表示を選択できます。デフォルトでは無効に設定しています。
ブロードキャストポート	ブロードキャストコマンドを受信するポートを、チェックボックスで設定します。ブロードキャストポートを選択すると、あるポートに対して行った操作を、他のブロードキャストポート全てに対して適用できます。 **注意**:ブロードキャスト機能を動作させるには、SNビューアを使ってブロードキャストポートにアクセスし、コントロールパネルで**ブロードキャスト機能**をオンにしておく必要があります(p.60「コントロールパネルの機能」参照)。
保存	「**保存**」をクリックすると、ユーザー設定メニューで変更した内容を確定します。
パスワード変更	◆ ブラウザーGUIでユーザーのパスワードを変更する場合は、旧パスワードと新パスワードをそれぞれ該当欄に入力し、確認用新パスワードの欄には新パスワードを再度入力してください。変更内容を適用する場合は、「**パスワードの変更**」をクリックしてください。

セッション

「セッション」メニューでは、アドミニストレーター、またはユーザー管理権限のあるユーザーが、シリアルコンソールサーバーにログイン中のユーザー情報を確認できます。



注意:

1. 一般ユーザーは「セッション」メニューを利用できません。
2. 一般ユーザーのセッション情報を確認できるのは、ユーザー管理権限のあるユーザーだけです。
3. 一覧の項目をクリックすると、項目順に表示を変更します。

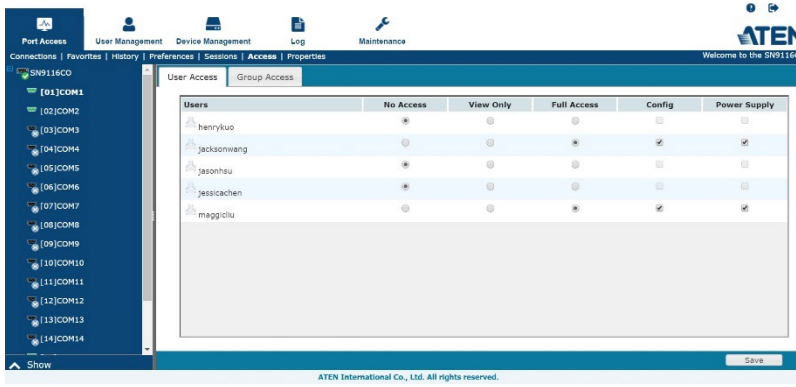
各項目の詳細は下表の通りです。

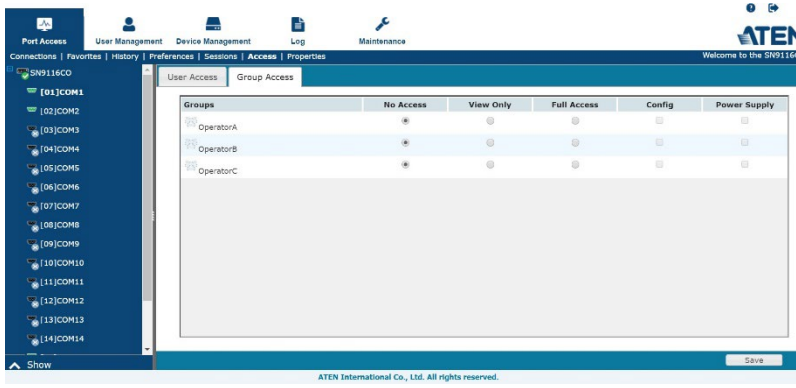
項目	説明
ユーザーネーム	ログイン中のユーザー名を表示します。
サービス	ログインに使用しているセッションの種類(HTTP、HTTPS)を表示します。
IP	ログインユーザーの接続元IPアドレスです。
ログイン時刻	ユーザーがログインした日時です。
前回のアクセス	ユーザーが前回システムにアクセスした日時です。
ユーザータイプ	ログインユーザーの種類です。ユーザーの種類は、「スーパーアドミニストレーター」、「アドミニストレーター」、「一般ユーザー」です。

アドミニストレーターは、この画面で選択したユーザーを強制的にログアウトします。対象となるユーザーを「**選択**」列にあるチェックボックスで選択し、メインパネル下部にある「**セッションの強制終了**」ボタンをクリックしてください。

アクセス

「アクセス」メニューは、アドミニストレーターがユーザーやグループによるアクセスを設定したり、シリアルコンソールサーバーのポートやPDU機器へのアクセス権限を設定する画面です。ユーザー管理権限があるユーザーにのみ表示します。他のユーザーはご利用になれません。アクセス権限はユーザー単位でもグループ単位でも設定できます。グループやユーザーの設定方法については、p.100「ユーザー管理」を参照してください。



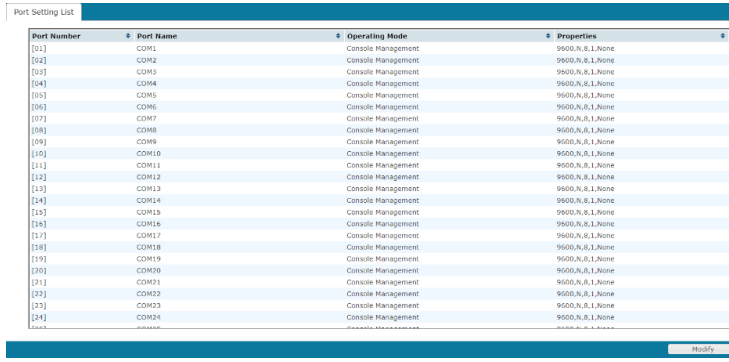


「ユーザーアクセス」や「グループアクセス」のメニューで、ラジオボタンを使ってアクセス権限を設定してください。画面の表における各列の説明は、下表の通りです。

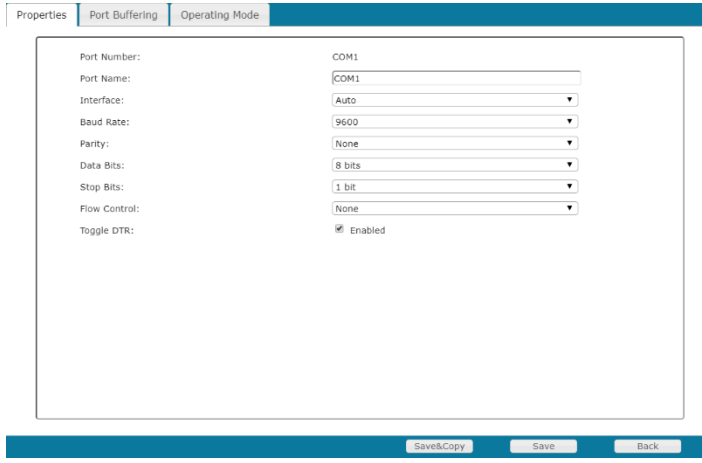
ユーザーアクセス	シリアルコンソールサーバーで作成したユーザー(スーパーアドミニストレーターを除く)が一覧表示して、サイドバーに並んでいる機器に対するアクセスや設定権限を定義できます。サイドバーから機器を選択し、各ユーザーに対してアクセスや設定権限を設定してください。	
グループアクセス	シリアルコンソールサーバー上に作成したグループを一覧表示して、サイドバーに並んでいる機器に対するアクセスや設定権限を定義できます。サイドバーから機器を選択し、各グループに対してアクセスや設定権限を定義してください。	
アクセス権限	「アクセス」列では、アクセス権限を設定します。各項目は下記の通りです。	
	フルアクセス	ユーザーは、デバイスの表示や、デバイスに対する操作の実行ができます。
	参照のみ	ユーザーは、デバイスを表示できますが、デバイスに対して操作を実行できません。
	アクセス不可	デバイスは、メイン画面のユーザーリストに表示しません。
設定	操作権限を設定したり設定を解除したりして、ユーザーのポート設定を変更します。チェックに印(✓)がついていると、ユーザーに操作権限を与えています。また、印が付いていない場合は、ユーザーに操作権限がありません。	
電源	この列では、シリアルコンソールサーバーに接続した電源管理デバイスのポートで、設定や電源操作の権限があるかを設定します。チェックに印(✓)がついていると、ユーザーに操作権限を与えます。また、印が付いていない場合は、ユーザーに操作権限がありません。	

プロパティー

「プロパティー」メニューをクリックすると、「ポート設定一覧」画面を表示します。



ポートが「ポート設定一覧」やサイドバーからダブルクリックすると、下図のような「**プロパティー**」画面を表示します。



このパネルでは、選択したポートに対して下表の項目を設定できます。

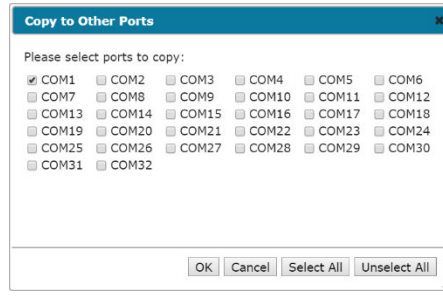
設定	意味
ポートID	シリアルコンソールサーバーの各ポートには、ポートのID番号が付いています。この欄は、現在設定しているポートを表しています。

設定	意味

ポートネーム	「ポートネーム」欄中の文字列を編集して、ポートに名前を設定できます。
インターフェース	「**自動**」(デフォルト)、**DTE**、または**DCE**のいずれかを選択します。
ボーレート	ポートのデータ転送速度を設定します。選択肢は300～230400 です(全オプションを表示するには、リストを展開します)。この設定は、接続機器のボーレートに合わせてください。デフォルトでは9600(大半のシリアル機器のデフォルト設定に同じ)に設定されています。
データビット	データ1文字を転送するのに使用するビット数を設定します。設定できる値は、5、6、7、8です。この設定は、接続機器のデータビットの設定に合わせてください。デフォルトでは8(大半のシリアル機器のデフォルト設定に同じ)です。
パリティー	このパリティービットは、転送データの整合性をチェックします。設定できる値は、「なし」、「奇数」、「偶数」です。この設定は、接続機器のパリティーの設定に合わせてください。デフォルトでは「なし」(大半のシリアル機器のデフォルト設定に同じ)です。
ストップビット	文字が転送されたかを表すビットです。この設定は、接続機器のストップビットの設定に合わせてください。選択肢は1、1.5、2です。デフォルトでは1(大半のシリアル機器のデフォルト設定に同じ)です。
フローコントロール	データフローの制御方法を選択できます。選択できる値は「なし」、「ハードウェア(RTS/CTS)」、「XON/XOFF」です。この設定は、接続機器のフローコントロールの設定に合わせてください。デフォルトでは「なし」に設定されています。
DTR切り替え	このパラメーターを有効にすると、DTR信号を有効または無効に切り替えます。チェックの印(✓)がついていると、この機能を有効にします。

保存とコピー

「プロパティー」画面の右下にある「保存」をクリックすると、選択ポートに対する設定内容を保存します。また、「保存してコピー」をクリックすると、下図のように現在のポートの設定をコピーして、他のポートにも適用できます。



現在の設定内容を適用したいポートを選択し、「**OK**」をクリックしてください。

ポートバッファー

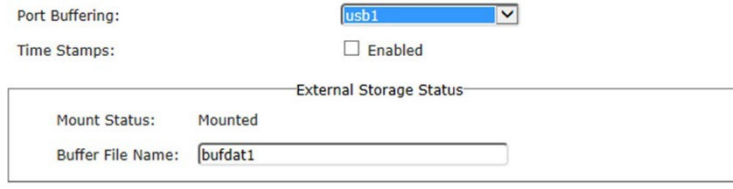
ポートバッファー機能は、ポートへアクセスした時に発生したアクティビティーのログを作成します。ログはシリアルコンソールサーバー内のメモリーやUSBドライブに保存できます。シリアルコンソールサーバー内部のメモリーは容量に限りがあるのに対し、USBドライブの場合は、より多くの容量を確保できます。

注意:

USBドライブは、SN1100CO/SN1100COD/SN0100CO/SN0100CODシリーズのモデルでのみサポートします。

ポートバッファー機能を有効にするには、ドロップダウンメニューから、「メモリー」、「NFS」、「Syslogサーバー」のいずれかを選択するか、あるいはマウントしたUSBドライブを選択してください。「無効」を選択すると、ポートバッファー機能を無効にします。タイムスタンプ機能を有効または無効にするには、「有効」のチェックボックスを使ってください。

マウントしたUSBドライブを選択した場合は、追加情報が表示します。



「バッファーファイル名」の項目では、USBドライブに保存するログのファイル名を変更できます。

Syslogサーバー、NFS、およびマウントしたUSBドライブの詳細については、p.116「デバイス」を参照してください。

動作モード

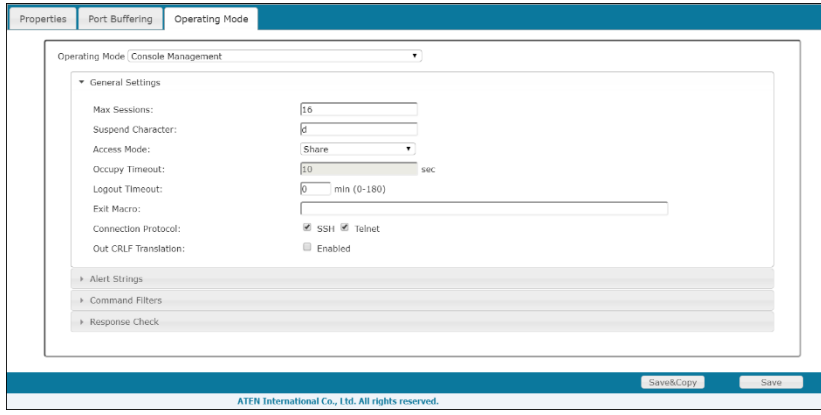
「動作モード」の画面では、各ポートに対してアクセスや管理方法を設定できます。この項目によって、各シリアル機器に対して動作モードを使って、どのようにアクセスするかを定義します。各動作モードの設定に関する詳細は、p.72「動作モード」を参照してください。

動作モード – 管理対象となるポートデバイスにアクセスするモードを設定します。最も汎用的な設定は、「**コンソール管理**」です。「ポートアクセス」タブの「接続」メニューからTelnet/SSHセッションを確立してアクセスする方法です。ドロップダウンメニューからポートの操作モードを選択してください。

注意:

ドロップダウンリストで表示するポート動作モードに関する詳細は、p.71「ポート動作モード」をご参照してください。

コンソール管理



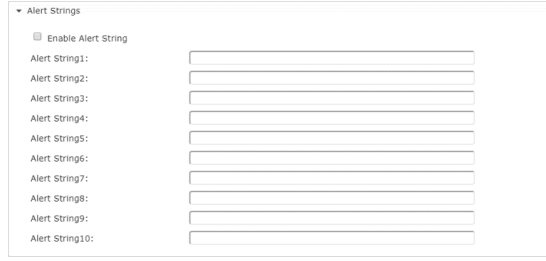
◆ 全般設定

設定	意味
最大セッション数	最大同時セッション数を設定します。
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ます。有効な文字は、H、I、J、Mを除くA～Zです。

設定	意味
アクセスモード	複数ユーザーでログインした場合のポートのアクセス方法について、次のように定義します。 **排他**:ポートに最初に切り替えたユーザーは、ポートに対して排他的にアクセスできます。他ユーザーはこのポートを参照できません。また、このモードに設定している場合、タイムアウト機能を適用しません。 **占有**:ポートに最初に切り替えたユーザーは、ポートに対してアクセスできますが、他のユーザーもポートを参照できます。ポートを操作しているユーザーからの入力がないまま、「占有タイムアウト」の項目で設定した時間が経過すると、次にマウスやキーボードの入力があったユーザーにポートの操作権限が移動します。 **共有**:複数のユーザーで同時にポートを共有して操作できます。ユーザーからの入力はキューに格納し、古いものから順に実行します。
占有タイムアウト	ポートを操作しているユーザーからの入力がないまま、この項目で設定した時間が経過すると、ポートを開放し、別のユーザーが使用できます。
ログアウト タイムアウト	ユーザーログインを必要としないアプリケーションをお使いの場合、タイマーはユーザー操作によって設定するため、「占有タイムアウト」の設定が機能しないケースがあります。この場合には、この「ログアウトタイムアウト」の設定を使用してください。この機能を使用すると、設定した時間内に入力がない場合、ユーザーは自動的にログアウトします。ログアウト後に製品にアクセスするには、再ログインが必要です。
終了マクロ	終了マクロを設定します。シリアル機器を終了する際に実行するマクロをこの項目で設定できます。
接続プロトコル	SSHやTelnetの接続プロトコルを有効または無効にするには、チェックボックスを使用します。
CRLF変換	キャリッジリターン(CR)およびラインフィード(LF)の信号を送信するかを選択できます。

◆ アラート文字列

ポートの「アラート文字列」ダイアログボックスでは、シリアルコンソールサーバーのポートに接続している機器で発生した問題を通知する機能があります。

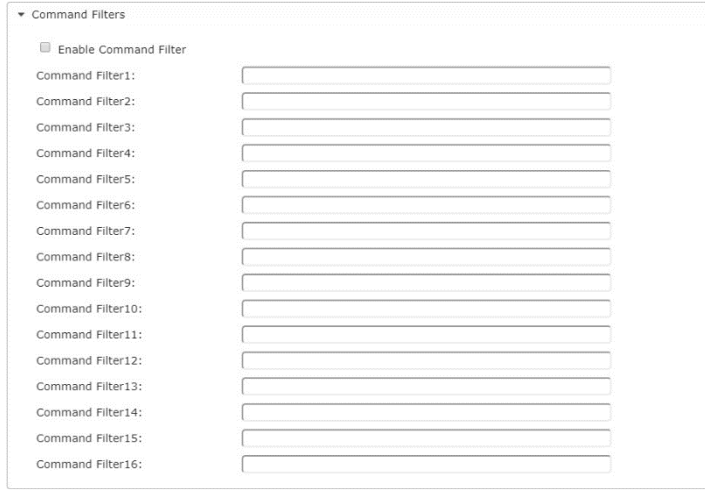


再起動が必要な重大なエラーやSNMPトラップのイベントが発生するなど、機器に何らかの問題が起こったときに、シリアルポートからシリアルコンソールサーバーのCOMポートにデバッグメッセージを送信できます。

シリアルコンソールサーバーがこのようなメッセージを送信すると、指定したユーザーに対して問題の発生を通知するSNMPトラップ警告やEメールを送信します。警告は10種類設定可能です。

この画面で設定すると、特定の警告が発生した際に通知します。

◆ **コマンドフィルター**



この画面では、最大16種類のコマンドフィルターを定義できます。

◆ **レスポンスチェック**

この機能を有効にすると、システムはデバイスが正常に応答しているかをチェックし、システムが正常に機能しているか確認できます。

注意:

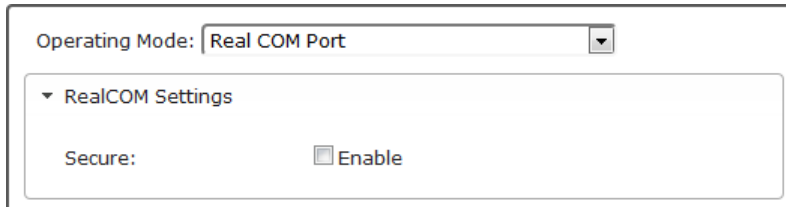
この機能は、コンソール管理およびコンソール管理ダイレクトモードでのみサポートます。

デバイスが応答しない場合、「応答確認失敗」通知(この通知が有効な場合)が送信

します。

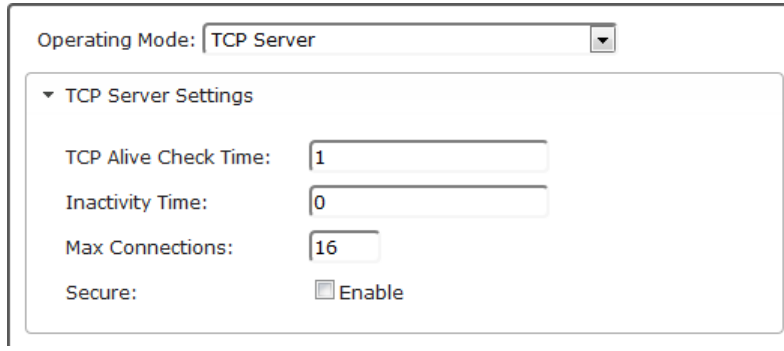
- **プローブ文字列**は、システムがレスポンスチェックのために送信する文字列です。デフォルトは¥x0D です(¥x0D は[Enter]、¥x1B は[ESC] を表します)。
- **クエリーの頻度**は、レスポンスチェックをどれくらいの頻度で送信するかを示します。既定値は30 (秒) で、10～9999 の数値を入力します。

リアルCOMポート



「**有効**」にチェックを入れると、このセッションで通信する全てのデータが暗号化されます。

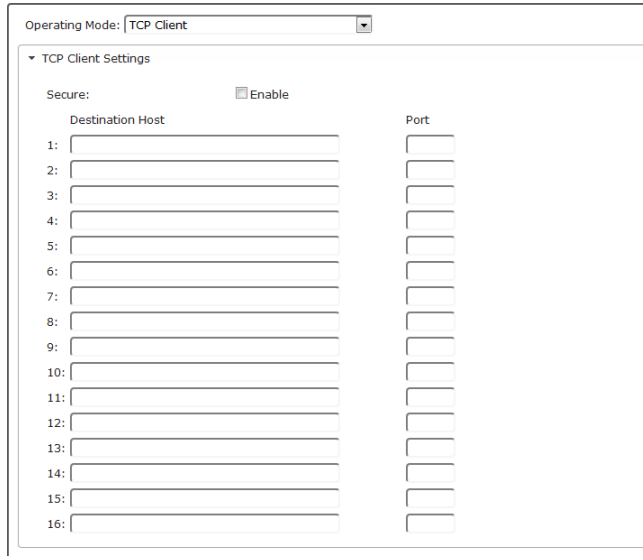
TCPサーバー



設定	意味
TCP生存確認時間	この項目では、シリアルコンソールサーバーがホストコンピューターに対して生存確認を判断するためにTCPソケット接続をチェックする頻度を設定します。この項目には、ホストコンピューターに対してTCP接続をチェックするまでシリアルコンソールサーバーに待機させる時間(分)を入力してください。
非アクティブ時間	この項目では、接続が中断するまでにシリアルコンソールサーバーとホストコンピューターの間でデータ通信が行われない場合に、待機しなければならない時間を定義します。その時間(分)を入力します。

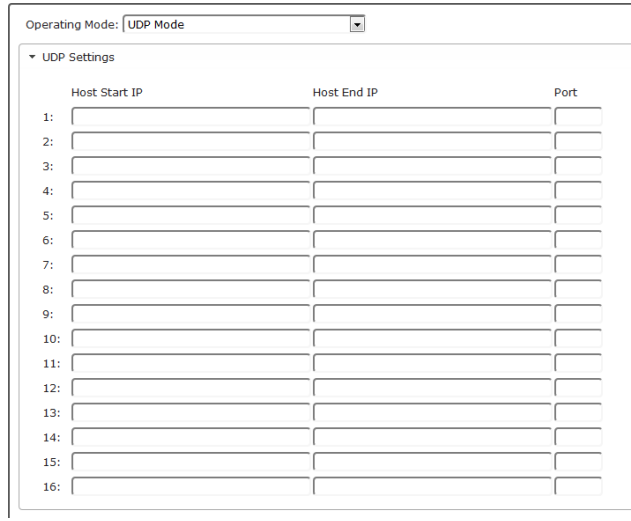
最大接続数	許可する同時接続の最大数を入力します。シリアルコンソールサーバーは、最大16の接続を同時に確立できます。
セキュア	「**有効**」にチェックを入れると、このセッションで通信する全てのデータが暗号化されます。

TCPクライアント



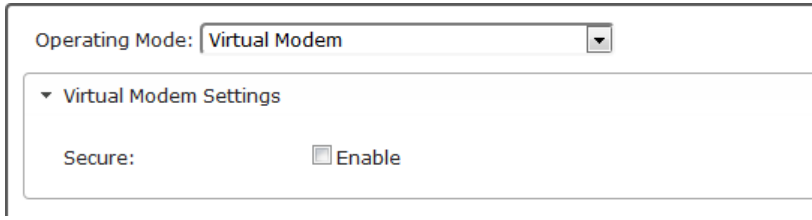
設定	意味
セキュア	「**有効**」にチェックを入れると、このセッションで通信する全てのデータが暗号化されます。
送信先ホスト/ポート	データ転送用のシリアルトンネルを作成するために、シリアルデータを受信するコンピューターの送信先ホスト(IPアドレス)およびTCP/IPサービスポートを入力してください。シリアルコンソールサーバーは、最大16台のホストコンピューターにデータを同時に送信できます。

UDPモード



設定	意味
ホストの開始IP/ホストの終了IPとポート	この項目を使うと、UDPプロトコル経由で接続を確立します。単一のIPアドレス、またはIPアドレスの範囲を指定し、ポート番号を入力してください。

バーチャルモデム



「**有効**」にチェックを入れると、このセッションで通信する全てのデータが暗号化されます。

コンソール管理ダイレクト

◆ 全般設定

設定	意味
最大セッション数	最大同時セッション数を設定します。
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ます。有効な文字は、H、I、J、Mを除くA～Zです。
アクセスモード	複数ユーザーでログインした場合のポートのアクセス方法について、次のように定義します。 **排他**:ポートに最初に切り替えたユーザーは、ポートに対して排他的にアクセスできます。他のユーザーはこのポートを参照できません。また、このモードに設定している場合、タイムアウト機能は適用されません。 **占有**:ポートに最初に切り替えたユーザーは、ポートに対してアクセスできますが、他のユーザーもポートを参照できます。ポートを操作しているユーザーからの入力がないまま、「占有タイムアウト」の項目で設定した時間が経過すると、次にマウスやキーボードの入力があったユーザーにそのポートの操作権限が移動します。 **共有**:複数のユーザーで同時にポートを共有して操作できます。ユーザーからの入力はキューに格納し、古いものから順に実行します。
占有タイムアウト	ポートを操作しているユーザーからの入力がないまま、この項目で設定した時間が経過すると、ポートを開放し、別のユーザーが使用できます。
ログアウト タイムアウト	ユーザーログインが必要としないアプリケーションをお使いの場合、タイマーはユーザー操作によって設定するため、「占有タイムアウト」の設定が機能しないケースがあります。この場合には、この「ログアウトタイムアウト」の設定を使用してください。この機能を使用すると、設定した時間内に入力がない場合、ユーザーは自動的にログアウトされます。ログアウト後に製品にアクセスするには、再ログインが必要です。

設定	意味

終了マクロ	終了マクロを設定します。シリアル機器を終了する際に実行するマクロをこの項目で設定できます。
接続プロトコル	SSHやTelnetの接続プロトコルを有効または無効にするには、チェックボックスを使用します。
CRLF変換	キャリッジリターン(CR)およびラインフィード(LF)の信号を送信するかを選択できます。

アラート文字列、コマンドフィルター、レスポンスチェックについては、p.93を参照してください。

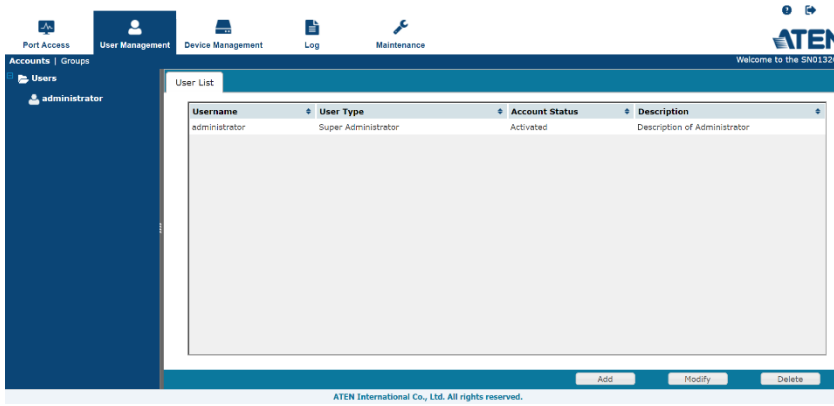
無効

このオプションを選択すると、シリアルコンソールサーバーにおけるシリアルポートの使用を無効にします。

第7章
ユーザー管理

概要

「ユーザー管理」タブを選択すると、アカウント画面を表示します。



画面の左側にはアカウント/グループリストが、右側にはメインパネルが、それぞれ配置されています。

- ユーザーとグループのリストを表示し、メインパネルにはそれぞれの詳細情報が一目でわかります。
  - ブラウザーGUIでは、アカウント(ユーザー)とグループのメニューバーを別々に表示します。選択したメニュー項目に応じて、「ユーザー」または「グループ」のいずれかが一覧表示されます。
- ブラウザーGUI、メインパネルの列見出しをクリックすると、情報の表示順序を変更できます。
- メインパネルの下にあるボタンは、次のセクションに記載されているユーザーやグループの管理に使用します。

ユーザー

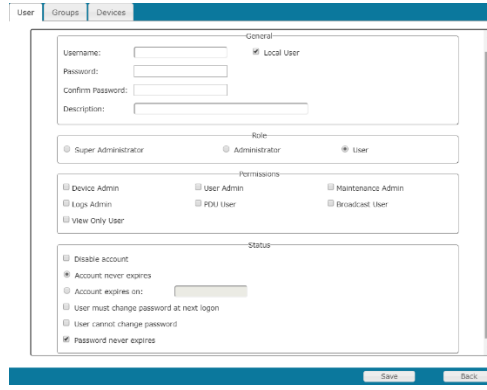
シリアルコンソールサーバー は、表に示す3つのユーザータイプ(最大64ユーザー)をサポートし、64の同時ログインでシステムにアクセスできます。

ユーザータイプ	役割
スーパーアドミニストレーター	ポートやデバイスへのアクセスおよび管理、ユーザーやグループの管理、システム設定全般、個人の作業環境の設定が可能です。
アドミニストレーター	権限のあるポートやデバイスへのアクセスおよび管理、ユーザーやグループの管理、個人の作業環境の設定が可能です。
ユーザー	権限のあるポートやデバイスへのアクセス、権限のあるポートやデバイスへの管理、個人の作業環境の設定が可能です。 **注意**:このタイプのユーザーでも権限を与えている場合は、他のユーザーの管理ができます。

ユーザーの作成

ユーザーを作成する場合は、以下の手順で操作してください。

1. サイドバーから「ユーザー」を選択してください。
2. メインパネル下部にある「**追加**」ボタンをクリックしてください。下図のような「ユーザー」タブを表示します。



3. 必要な項目を入力してください。各項目の詳細は下表の通りです。

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、1～16文字を使用できます。p.146「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、0～16文字を使用できます。p.146「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	パスワードの誤設定を防ぐために、パスワードを再入力してください。2つのエントリーは一致している必要があります。
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。
役割	スーパーアドミニストレーター、アドミニストレーター、ユーザーのカテゴリーの中から選択できます。各カテゴリーで作成できるアカウントの数に制約はありません。 ◆ スーパーアドミニストレーターは、システム全体の設定や保守、ユーザー管理、デバイスやポートの割り当てがそれぞれ可能です。スーパーアドミニストレーターの権限は、システムによって自動的に割り当てているため、変更できません。 ◆ アドミニストレーターには、デバイス管理とユーザー管理以外の全ての権限をデフォルトで与えていますが、権限のチェックボックスにチェックを入れたり、チェックを外すと権限の設定を変更できます。 ◆ ユーザーには、PDUユーザーとブロードキャストユーザーの権限をデフォルトで与えていますが、権限のチェックボックスにチェックを入れたり、チェックを外すと権限の設定を変更できます。
許可	◆ 「デバイス管理」の項目にチェックを入れるとコンソールサーバーの操作全体にかかわるパラメーターの設定や制御が可能です（p.116参照）。 ◆ 「ユーザー管理」の項目にチェックを入れると、ユーザーやグループアカウントの作成・変更・削除が可能です。 ◆ 「メンテナンス」の項目にチェックを入れると、「メンテナンス」タブでの項目が全て利用可能です（p.155参照）。 ◆ 「ログ管理」を有効にすると、ユーザーはシステムログにアクセスできます（p.150「ログ」参照）。 ◆ 「PDUユーザー」の項目にチェックを入れると、電源管理デバイスの設定が可能です。 ◆ 「ブロードキャストユーザー」の項目にチェックを入れると、ブロードキャスト機能の使用が可能です。 ◆ 「参照のみ」の項目にチェックを入れると、ユーザーは製品に接続された機器の画面の参照しかできなくなります。ポートへのアクセスや、キーボードやマウスを使ったポート操作はできません。

項目	説明
状態	ユーザーアカウントとデバイスへのアクセスを管理できます。詳細は以下の通りです。 ◆ 「アカウントを無効にする」の項目にチェックを入れると、ユーザーアカウントを停止できます。この機能ではユーザーは実際には物理的に削除しませんので、後に必要となった場合でも簡単に設定を戻せます。 ◆ アカウントに有効期限を設けたくない場合は「アカウントを無期限にする」の項目にチェックを入れてください。また、アカウントに有効期限を設ける場合は「アカウント失効日」の項目にチェックを入れ、有効期限の日付をテキストボックスに入力してください。 ◆ ユーザーが次回ログインする際にパスワードの変更を要求する場合は、「ユーザーは次回ログイン時にパスワード変更が必要」の項目にチェックを入れてください。この項目で、初回ログインでは管理者によって発行した一時パスワードを使用し、2回目以降はユーザー自身が設定したパスワードを使うという方法で運用できます。 ◆ パスワードを永続的にし、ユーザーに変更されないようにしたい場合は、「ユーザーはパスワード変更不可」の項目にチェックを入れてください。 ◆ セキュリティーのために、アドミニストレーターはユーザーに定期的なパスワードの変更を要求できます。 ➢ パスワードに有効期限を設けない場合は、「パスワードを無期限にする」の項目を選択してください。ユーザーはパスワードの有効期限の制限を受けません。 ➢ パスワードに有効期限を設ける場合は、「パスワード失効まで」の項目を選択し、パスワードの有効日数を入力してください。設定した日数が経過すると、新しいパスワードを設定しなければなりません。

4. この時点で、「グループ」タブを選択して新しいユーザーをグループに割り当てます。「グループ」画面についてはp.106で説明します。また、「デバイス」タブを選択して、ユーザーのポートアクセス権を割り当てます。「デバイス」画面については、p.113を参照してください。

注意:

グループの設定は必須ではありませんので、この手順を省略し、先にユーザーやグループを作成しておいてから、後でユーザーをグループに登録したり、ユーザーに権限を与えます。

5. 各項目への入力が終わったら「**保存**」ボタンをクリックしてください。

6. 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」と表示します。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。

7. メイン画面に戻る場合は、サイドバーの「**ユーザー**」をクリックしてください。サイドバーの一覧とメインパネルに新しいユーザーを表示します。

   ◆ サイドバーのユーザーリストは展開したり閉じたりできます。リストを展開している場合は、「ユーザー」の隣にある「-」をクリックするとツリーが閉じます。また、リストが閉じている場合はアイコンの隣に「+」マークを表示します。「+」をクリックするとリストが展開します。

   ◆ 首に黒い二重のバンドがついているアイコンはスーパーアドミニストレーターを、また、首に赤い一重のバンドがついているアイコンはアドミニストレーターです。

   ◆ 大きいメインパネルにはユーザーの名前、アカウント作成時に設定した説明、アカウントの状態（有効・無効）を表示します。

ユーザーアカウントの編集

ユーザーアカウントを編集する場合は、以下の手順で操作してください。

1. サイドバーの「ユーザー」リストで、ユーザーの名前をクリックしてください。

   または、メインパネルでユーザーの名前を選択してください。

2. 「**変更**」をクリックしてください。

3. メイン画面の「ユーザー」タブで内容を変更したら、「**保存**」ボタンをクリックします。

注意:

「ユーザー」画面についてはp.101で、「グループ」画面についてはp.106で、「デバイス」画面についてはp.113で、それぞれ説明します。

ユーザーアカウントの削除

ユーザーアカウントを削除する場合は、以下の手順で操作してください。

1. メインパネルで、ユーザーの名前を選択してください。
2. 「**削除**」ボタンをクリックしてください。
3. 「**OK**」ボタンをクリックしてください。

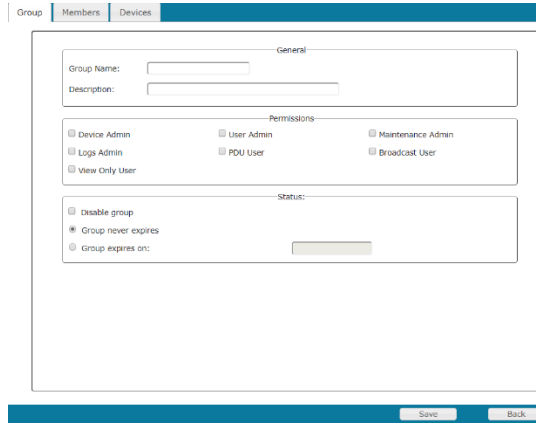
グループ

グループを使用すると、アドミニストレーターはユーザーと関連するデバイスのアクセス権限や設定権限を簡単に管理できます。デバイスのアクセス権がグループに適用すると、グループメンバー全員に同じ権限が適用されます。特定のユーザーに特定のデバイスへのアクセスを許可し、他のユーザーのアクセスを制限するために、最大16個のグループを定義できます。

グループの作成

グループを作成する場合は、以下の手順で操作してください。

1. メニューバーから「グループ」を選択してください。
2. メインパネル下部にある「**追加**」ボタンをクリックしてください。グループメニューが開き、「グループ」タブが選択されます。



3. 必要な項目を入力してください。各項目の詳細は下表の通りです。

項目	説明
グループネーム	最大16文字まで入力できます。
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。最大63文字まで入力できます。
許可	グループに対する操作許可と操作制限は、各操作のチェックボックスで個別に設定してください。各権限は「ユーザー」タブの権限と同じです。詳細はp.113を参照してください。

4. この時点で、「メンバー」タブを選択してユーザーをグループに割り当てます。「メンバー」画面については、p.111で説明します。また、デバイスタブを選択して、グループのポートアクセス権を割り当てます。デバイス画面については、p.113を参照してください。

注意:

グループの設定は必須ではありませんので、この手順を省略し、先にユーザーやグループを作成しておいてから、後でユーザーをグループに登録したり、ユーザーに権限を与えます。

---

5. 各項目への入力が終わったら「**保存**」ボタンをクリックしてください。
6. 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」と表示します。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。
7. メイン画面に戻る場合は、サイドバーの「**グループ**」をクリックしてください。サイドバーの一覧とメインパネルに新しいグループを表示します。
   - ◆ サイドバーのグループリストは展開したり閉じたりできます。リストが展開されている場合は、「ユーザー」の隣にある「-」をクリックするとツリーが閉じます。また、リストが閉じている場合はアイコンの隣に「+」マークが表示します。「+」をクリックするとリストが展開します。
   - ◆ 大きいメインパネルにはグループの名前、グループ作成時に設定した説明が表示されます。

他にも追加するグループがある場合は、上記の操作手順を繰り返してください。

注意:

新しいグループを追加する前に、必ず手順7の通り操作してください。この操作をしないと、作成したばかりのグループが新規に作成しようとしているグループに置き換わってしまいます。

グループの編集

グループを編集する場合は、以下の手順で操作してください。

1. サイドバーの「グループ」リストで、グループの名前をクリックしてください。

   または、メインパネルでグループの名前を選択してください。

2. 「**変更**」をクリックしてください。

3. メイン画面の「グループ」タブで内容を変更したら、「**保存**」ボタンをクリックして内容を反映させます。

注意:

「グループ」画面についてはp.106で、「メンバー」画面についてはp.111で、「デバイス」画面についてはp.113で、それぞれ説明します。

グループの削除

グループを削除する場合は、以下の手順で操作してください。

1. サイドバーで、「グループ」アイコンをクリックしてください。

2. メインパネルで、グループの名前を選択してください。

3. 「**削除**」ボタンをクリックしてください。

4. 「**OK**」ボタンをクリックしてください。

ユーザーとグループ

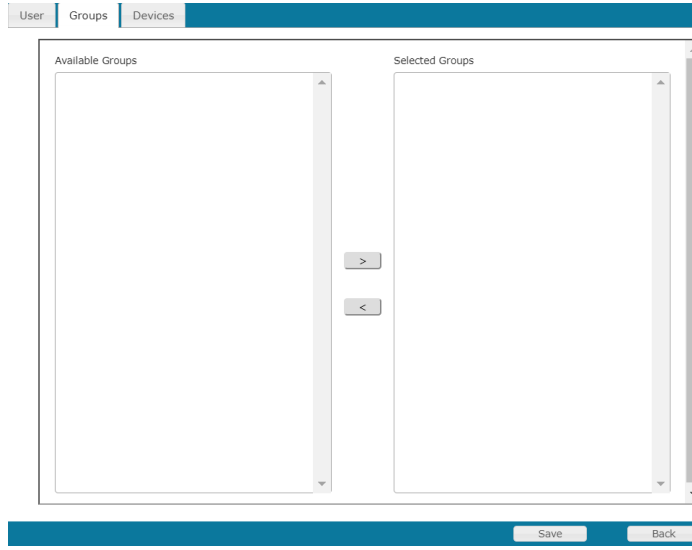
ユーザーやグループの管理は、「ユーザー」タブ、「グループ」タブのどちらからでも操作できます。

注意:
ユーザーをグループに割り当てる前に、必要となるユーザーとグループを事前に作成しておいてください。
詳細については、p.101「ユーザーの作成」を参照してください。

ユーザーメニューを使ってユーザーをグループに割り当てる場合

「ユーザー」タブを使ってユーザーをグループに割り当てる場合は、下記の手順に従って操作してください。

1. サイドバーの「ユーザー」リストで、ユーザーの名前をクリックしてください。
   または、メインパネルでユーザーの名前を選択してください。
2. 「**変更**」をクリックしてください。
3. メインパネルから「グループ」タブを選択してください。以下のような画面を表示します。



4. 「有効」リストから、ユーザーの所属先となるグループを選択してください。
5. **右矢印のボタン**(>>)をクリックして、手順4で選択したグループを「選択」リストに移動させてください。
6. 他にもユーザーの所属グループがある場合は、上記の手順を繰り返してください。
7. 完了したら、「**保存**」ボタンをクリックしてください。

注意:

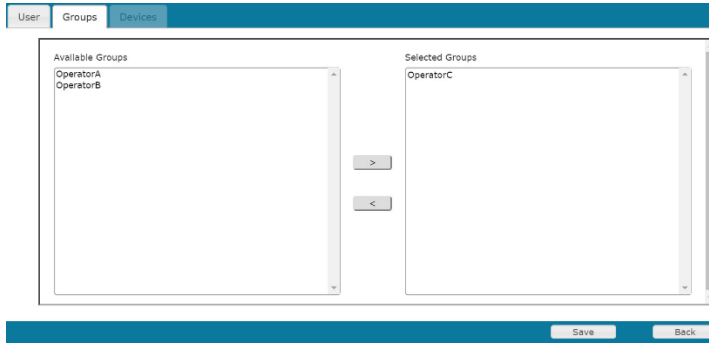
グループに設定した権限とは別の権限をユーザーに与えている場合は、この権限も保持されます。

ユーザーメニューを使ってグループからユーザーを削除する場合

「ユーザー」タブを使ってユーザーをグループから削除する場合は、下記の手順に従って操作してください。

1. サイドバーの「ユーザー」リストで、ユーザーの名前をクリックしてください。

   または、メインパネルでユーザーの名前を選択してください。
2. 「**変更**」をクリックしてください。
3. メインパネルから「グループ」タブを選択してください。以下のような画面が表示されます。



4. 「選択」リストから、ユーザーの登録を解除したいグループを選択してください。
5. **左矢印のボタン**(<<)をクリックして、手順4で選択したグループを削除してください (選択したグループは「有効」リストに戻ります) 。

6. 他にもユーザーの登録を解除したいグループがある場合は、上記の手順を繰り返してください。

7. 完了したら、「**保存**」ボタンをクリックしてください。

グループメニューを使ってユーザーをグループに割り当てる場合

「グループ」タブを使ってユーザーをグループに割り当てる場合は、下記の手順に従って操作してください。

1. サイドバーの「グループ」リストで、グループの名前をクリックしてください。

   または、メインパネルでグループの名前を選択してください。

2. 「**変更**」をクリックしてください。

3. メインパネルから「メンバー」タブを選択してください。以下のような画面が表示されます。

4. 「有効」リストから、グループのメンバーとなるユーザーを選択してください。

5. **右矢印のボタン**(>>)をクリックして、手順4で選択したユーザーを「選択」リストに移動させてください。

6. 他にも追加したいメンバーがいる場合は、上記の手順を繰り返してください。

7. 完了したら、「**保存**」ボタンをクリックしてください。

注意:

グループに設定した権限とは別の権限をユーザーに与えている場合は、この権限も保持されます。

グループメニューを使ってグループからユーザーを削除する場合

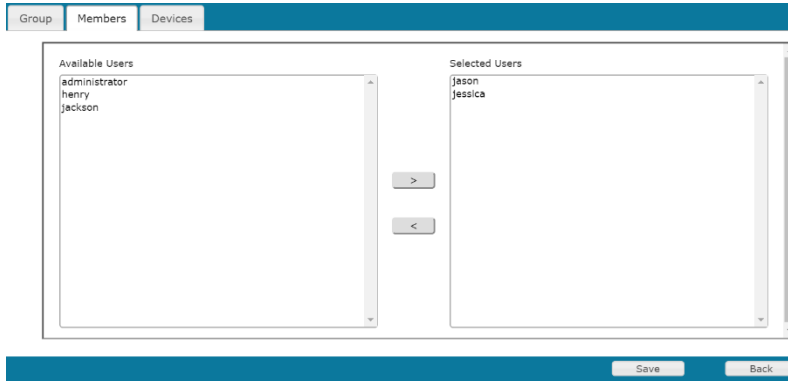
「グループ」タブを使ってユーザーをグループから削除する場合は、以下の手順で操作してください。

1. サイドバーの「グループ」リストで、グループの名前をクリックしてください。

   または、メインパネルでグループの名前を選択してください。

2. 「**変更**」をクリックしてください。

3. メインパネルから「メンバー」タブを選択してください。以下のような画面が表示されます。



4. 「選択」リストから、ユーザーの登録を解除したいグループを選択してください。

5. **左矢印のボタン**(<<)をクリックして、手順4で選択したグループを削除してください（選択したグループは「有効」リストに戻ります）。

6. 他にもグループから除外したいユーザーがいる場合は、上記の手順を繰り返してください。

7. 完了したら、「**保存**」ボタンをクリックしてください。

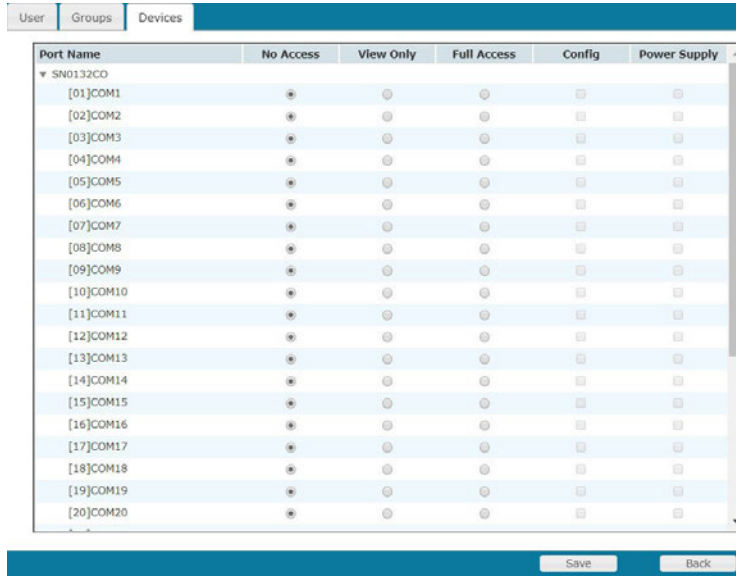
デバイスの割り当て

ユーザーがシリアルコンソールサーバーにログインすると、「ポートアクセス」タブの画面が最初に表示されます。このとき、ユーザーがアクセスを許可したポートが全て、画面左側のサイドバーに一覧表示されます。ポートやポートに接続したデバイスに対するアクセス権限は、「ユーザー管理」タブの「ユーザー」または「グループ」リストからポートごとに割り当てます。

ユーザーメニューを使ってデバイスの操作権限を割り当てる場合

「ユーザー」タブを使ってデバイスの操作権限を割り当てる場合は、以下の手順で操作してください。

1. サイドバーの「ユーザー」リストで、ユーザーの名前をクリックしてください。
   または、メインパネルでユーザーの名前を選択してください。
2. 「**変更**」をクリックしてください。
3. メインパネルから「デバイス」タブを選択してください。以下のような画面が表示されます。



4. 下記を参考にしながら、各ポートの権限設定をしてください。

名前:	現在操作しているユーザーがアクセスできるポートをこの列に表示します。	
アクセス:	デバイスへのアクセス権限を設定します。設定内容を切り替える場合は、設定をしたいポートの行にあるラジオボタンをクリックしてください。各アイコンは下記の通りです。	
	フルアクセス	ユーザーはリモート画面を参照できます。また、ユーザー自身が使用しているキーボードとモニターを使ってリモートサーバーを操作できます。
	参照のみ	ユーザーはリモート画面を参照できますが、操作できません。
	アクセス不可	このポートへのアクセス権限はなく、ポートはユーザーのメイン画面にも表示しません。
	注意: ◆ ローカルユーザー：ローカルユーザーの実際の権限は、アカウントとグループのデバイスタブで設定した結果を結合しています。優先順位は、「フルアクセス」>「参照のみ」>「アクセス不可」です。 ◆ ドメインユーザー：ドメインユーザーの実際の権限は、「ANMS」の「認証と権限設定」タブ（p.131参照）、および「グループ」の「デバイス」タブで設定した内容を結合しています。サードパーティーの認証&権限サーバーとグループリスト（p.106参照）で同じグループ名で作成しているか確認します。優先順位は、「フルアクセス」>「参照のみ」>「アクセス不可」です。 ◆ 「ユーザー」タブの「権限」において「参照のみ」のユーザーを選択している場合、次の優先順位が適用されます。「参照のみのユーザー」>「フルアクセス」>「参照のみ」>「アクセス不可」	
設定:	この列では、ポート設定の変更権限を設定します。チェックマーク（✓）はユーザーがポート設定の変更権限を持ってます。また、チェックマークが入っていない場合、ユーザーは権限を持っていません。	
電源:	管理デバイスを接続するポートの管理操作に関する権限を設定します。チェックに印（✓）がついていると、ユーザーに操作権限を与えています。また、印が付いていない場合は、ユーザーに操作権限がありません。 この機能はPGシリーズのPDUで使用するために予約されています。	

5. 内容を設定したら、「**保存**」をクリックしてください。

6. 確認ダイアログが表示されたら、「**OK**」ボタンをクリックしてください。

注意:

各列の値は、[Shift] キーや[Ctrl]キーを押しながらマウスをクリックして複数のポートの属性を同時に定義できます。選択したポートで各列をクリックすると、列の設定内容を同時に循環しながら切り替えます。

グループメニューを使ってデバイスの操作権限を割り当てる場合

「グループ」タブを使ってデバイスの操作権限を割り当てる場合は、下記の手順に従って操作してください。

1. サイドバーの「グループ」リストで、グループの名前をクリックしてください。

   または、メインパネルでグループの名前を選択してください。

2. 「**変更**」をクリックしてください。

3. 表示した「グループ」メニューから「デバイス」タブを選択してください。

4. 表示する画面は、「ユーザー」メニューからデバイスの操作権限を割り当てる場合と同じです。唯一の違いは、設定が、個々のメンバーではなく、グループの全てのメンバーに適用されます。

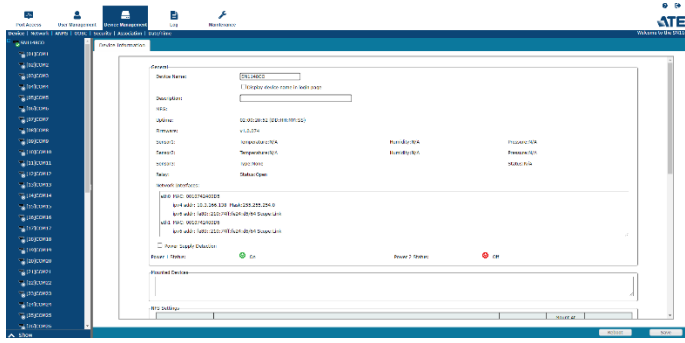
   p.113「ユーザーメニューを使ってデバイスの操作権限を割り当てる場合」の手順に従ってデバイスに操作権限を割り当ててください。

第8章
デバイス管理

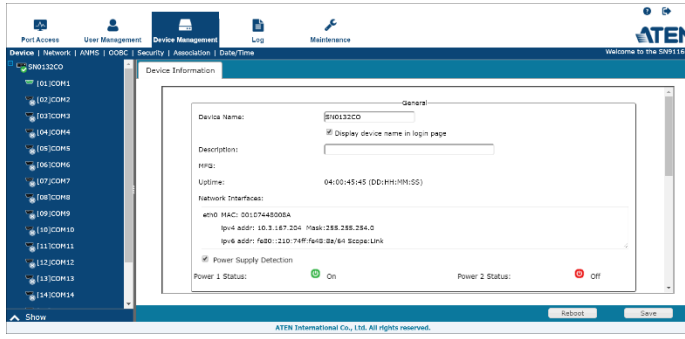
デバイス

「デバイス管理」画面を開くと、サイドバーで最上位のシリアルコンソールサーバーが選択され、全ポートが下に入れ子で表示します。また、デバイス情報画面をメインパネルに表示します。

SN1100CO/SN1100CODシリーズ

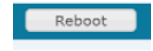


SN0100CO/SN0100COD/SN9100COシリーズ



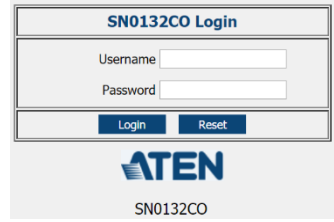
全般

「デバイス情報」画面の「全般」セクションでは、**デバイス名**と**説明**を設定したり、シリアルコンソールサーバーの**製造(MFG)**情報を参照したりできます。また、設定を変更せず再起動するための便利な「**再起動**」ボタンを用意しています。



「ネットワークインターフェース」セクションには、ネットワーク設定に関する詳細情報が表示されます。

ログイン情報を入力するエリアの下にデバイス名を表示させるには、「**ログイン画面でデバイス名を表示する**」の機能をオンにします。次に例を示します。



注意:

「MFG番号 / 製品シリアル番号」(製造番号 / 製品シリアル番号) は、ATENの工場および技術サポートスタッフが製品を識別するために使用する内部シリアル番号です。この番号が製品保証期間への影響はありません。製品にアフターサービスが必要な場合は、製品およびモデル番号を確認するため、MFG番号 / 製品シリアル番号をATENの販売担当者またはテクニカルサポート担当者にお伝えください。MFG 番号には 11桁の数字(xxxxxxxxx)が、製品のシリアル番号には 13桁の数字(xxxx-xxx-xxxx)が付属しています。

SN1100CO/SN1100COD/SN0100CO/SN0100CODシリーズのモデルには2つの電源装置を搭載しています。「電源検知」セクションでは、シリアルコンソールサーバーの2カ所の電源に関する情報が確認できます。

- 「電源1」と「電源2」のアイコンは、電源に対して電力を供給していないときはグレーに、また、電源を供給しているときはブルーに、それぞれ表示します。
- 電源検知機能が有効 (チェックボックスにチェックが入っている)だと、電源が片方にしか供給しなくなった場合に、シリアルコンソールサーバー側でビープ音が鳴

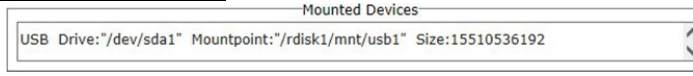
り、問題を通知します。デフォルトでは、この機能が有効です。

ローカルコンソール側で作業をしている場合は、電源が1つしかないとメッセージを表示します。もし、意図的に片方のみの電源で運用していれば、このビープ音を止める方法が2つあります。

1) チェックボックスからチェックを外すと警告を無効にできます。常にこの機能を無効にしたい場合は、この方法で停止してください。

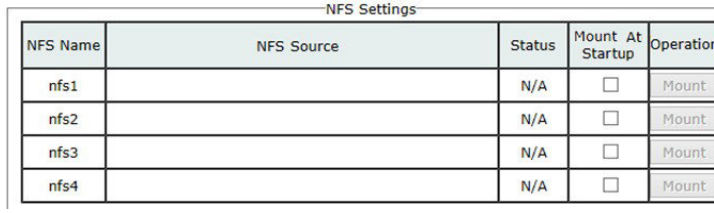
2) ダイアログボックスで確認できます。この警告を一時的に無効にしたい場合は、この方法で停止してください。この方法で停止した場合、システムリセットすると、再びこの警告機能が有効になります。

マウントされたデバイス



「マウントしたデバイス」セクションには、接続したUSBおよびNFSストレージデバイスに関する情報を表示します。USBドライブをシリアルコンソールサーバーのフロントパネルに接続するか(SN1100CO/SN1100COD/SN0100CO/SN0100CODシリーズのみ)、NFSストレージの場所を設定すると(下記の「NFS設定」参照)、マウントされたデバイスの詳細情報とともに表示します。

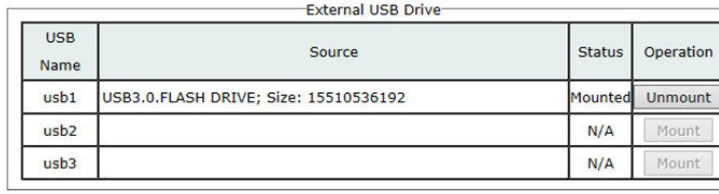
NFS設定



NFS(ネットワークファイルシステム)は、ネットワークを介して別のストレージデバイスをマウントできる機能です。最大4台の機器をマウントできます。「**ソース**」欄に、マウントしたいロケーションのフルパスを含めた形で、ストレージデバイスのネットワークロケーション(IPアドレスまたはネットワーク名)を入力してください。次に、「**マウント**」をクリックしてNFSストレージデバイスをマウントしてください。「**状態**」列には、「N/A」、「マウント済み」、「マウント解除」のいずれかを表示します。ストレージデバイスにアクセスできない場合には、「マウント解除」と表示します。この場

合、デバイスがネットワーク上でアクセス可能であるか確認し、入力したソース情報が正しいか確認します。システムの起動時にNFSストレージデバイスを自動的にマウントするには、「**起動時にマウントする**」をオンにします。

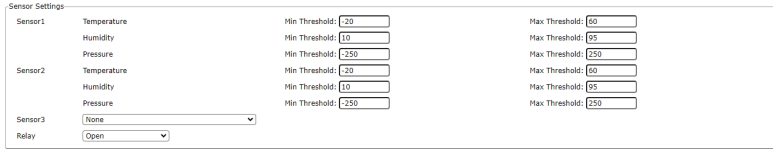
外付けUSBドライブ



最大3台(SN0100CO/SN0100CODシリーズ) / 4台(SN1100CO/SN1100CODシリーズ) の外付けUSB ドライブをマウントできます。ドライブをマウントする場合は「**マウント**」を、また、ドライブのマウントを解除する場合は「**マウント解除**」を、それぞれクリックしてください。「**状態**」列には、「N/A」、「マウント済み」、「マウント解除」のいずれかを表示します。

USB ドライブでサポートするファイルシステムは、FAT8、FAT16、およびFAT32です。

センサー設定(SN1100CO/SN1100CODシリーズのみ)



最大3つのセンサーと、ドアアクセス制御用のリレーをセットアップできます。

- センサー1とセンサー2:温度、湿度、および空気圧センサーの最小しきい値と最大しきい値を調整します。RJ-11互換のセンサーは、EA1140、EA1240、EA1340 です。各センサーは別売りです。製品情報については、ATEN販売店にお問い合わせください。
- センサー3:使用可能なドアセンサーをフォトドアセンサー(EA1440) / 誘導式近接ドアセンサー(EA1441) / リードドアセンサー(EA1442) / 静電容量式漏れセンサー(EA1540) から選択します。各センサーは別売りです。製品情報については、ATENの販売店にお問い合わせください。

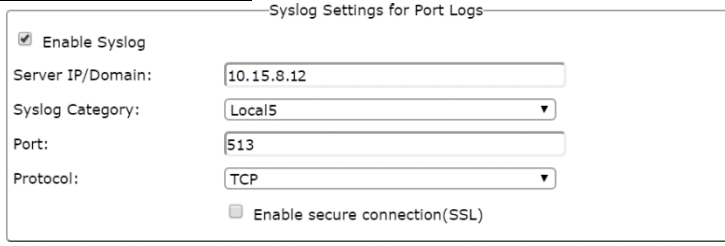
◆ リレー:ドアアクセス制御用のリレーをオープン、クローズ、パルスから調整します。

◆ オープン:電気回路をオープンします。

◆ クローズ:電気回路をクローズします。

◆ パルス:電気回路を3 秒間閉じた後、電気回路をノーマルオープンに変更します。

ポートログのSyslog設定

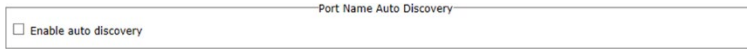


ユーザーに対して、あらかじめ定義されたSyslogサーバーでのログ記録を許可できます。

この機能を有効にするには、「Syslogを有効にする」の項目にチェックを入れてください。この機能が有効だと、ポートバッファー機能で、「Syslogサーバー」のオプションが利用可能になります。

上図に示した各項目に対して、サーバー情報の入力や選択してください。

ポートネームの自動検出



デフォルトでは、この機能は**無効**(オフ)で、サーバーはデフォルトの命名規則(COM1、COM2など)に従ってポート名を表示します。

この機能を**有効**(チェックあり)にすると、サーバーは接続しているネットワークスイッチのポート名を取得して表示するためにプローブ文字列を自動的に送信します。ポートネームは、デバイス情報(ブランドとモデル)に従って表示します。

ネットワークスイッチが認識できない場合、サーバーはデフォルトの命名規則に従ってポート名を表示します。

ネットワークスイッチの初期検証が必要な場合、サーバーにはデフォルト名のみ

が表示します。ただし、確認済み(スイッチにログイン済み)の場合は、シリアルポートを再接続して、スイッチの情報を表示しようとしたときにサーバーがネットワークスイッチを認識できるか確認できます。

互換性のあるネットワークスイッチには、Cisco、Juniper、HPE、Dell、Huawei、H3C、EdgeCore、TRENDnet、Fortinet、ATEN ES0152 などがあります。

ネットワーク

「ネットワーク」画面は、ネットワーク環境を定義する際に使用します。

この画面における各項目については、後続のセクションで説明します。

注意:

「冗長NICを有効にする」オプションは、SN1100CO/SN1100COD/SN0100CO/SN0100CODシリーズのシリアルコンソールサーバーでのみ使用できます。

IPインストーラー

IPインストーラーは、シリアルコンソールサーバーに外部からIPアドレスを設定できる、Windows用ソフトウェアです。

IPインストーラーの用途に応じて、「有効」、「参照のみ」、「無効」のいずれかのラジオボタンをクリックしてください。IPインストーラーの詳細についてはp.179を参照してください。

注意:

1. 「参照のみ」を選択すると、IPインストーラーのデバイス一覧にシリアルコンソールサーバーが表示されますが、IPアドレスを変更できません。
2. セキュリティーを確保するためには、IPインストーラーの使用後には、この項目を「参照のみ」または「無効」へ設定してご利用ください。

サービスポート

セキュリティー対策として、システムにファイアーウォールを導入している場合、アドミニストレーターはファイアーウォールの設定で許可したポート番号を製品本体側でも設定する必要があります。デフォルト以外のポートを使っている場合、ユーザーはログインの際にIPアドレスの一部分としてポート番号を入力しなくてはなりません。無効なポート番号(またはポート番号なし)を指定した場合、シリアルコンソールサーバーが見つかりません。各項目の内容は下表の通りです。

項目	説明
HTTP	ブラウザーからのログインの際に使用するポート番号です。デフォルトでは80です。
HTTPS	SSL通信に使用するポート番号です。デフォルトでは443です。
SSHポート	SSHによるアクセスで使用するポートです。デフォルトでは22です。
Telnetポート	Telnetでのアクセスに使用するポートです。デフォルトでは23です。
ベースソケット	TCP接続をリッスンしたり受信したりするポートです。

注意:

1. 全てのサービスポートの有効なエントリーは1～65535 です。
2. 各ポートはそれぞれ固有のポートを割り当て、項目間で値が重複しないように設定してください。
3. ファイアーウォールがない場合(例えば、イントラネット上)、各数値を何に設定していても影響はありません。
4. インターネットを介してSN1100CO/SN1100COD/SN0100CO/SN0100CODシリーズのデバイスを接続する方法については、p.186「ポート転送」を参照してください。

ネットワーク設定

◆ 冗長NIC*

SN1100CO/SN1100COD/SN0100CO/SN0100CODシリーズのデバイスには、2つのネットワークインターフェースを搭載しています。「冗長NICを有効にする」の項目が有効だと(デフォルト設定)、両方のインターフェースでネットワークアダプター「eth0」のIPアドレスを使用します。

この設定をした場合、セカンドインターフェースは利用時は非アクティブな状態です。ただし、第1インターフェースにネットワーク障害が発生した場合、シリアルコンソールサーバーは自動的に第2インターフェースに切り替わります。

◆ 冗長ネットワーク有効 – 両方のインターフェースに同じIPアドレスを設定します。冗長ネットワークを有効にするには、以下の手順で操作してください。

1. 「冗長NICを有効にする」の項目にチェックを入れてください。
2. このとき、ネットワークアダプターのリストボックスで「eth0」が選択しており、リストボックスが無効です。「eth1」を設定できません。
3. 「eth0」で使用するIPアドレスとDNSサーバーのIPアドレスを設定してください(次のセクションを参照)。

◆ 冗長ネットワーク無効 – 両方のインターフェースに異なるIPアドレスを設定します。

冗長ネットワークを無効にすると、両方のインターフェースに異なるIPアドレスを設定できます。ユーザーはどちらのIPアドレスでもSN1100CO/SN1100COD/SN0100CO/SN0100CODシリーズのコンソールサーバーにログインできます。この方法でシリアルコンソールサーバーをセットアップする場合は、以下の手順で操作してください。

1. 「冗長NICを有効にする」の項目にチェックが入っている場合は、クリックしてチェックを外してください。
2. ネットワークアダプターのリストボックスから「eth0」を選択してください。
3. 「eth0」で使用するIPアドレスとDNSサーバーのIPアドレスを設定してください(次のセクションを参照)。
4. ネットワークアダプターのリストボックスから「eth1」を選択してください。
5. 「eth1」で使用するIPアドレスとDNSサーバーのIPアドレスを設定してください。

注意:

SN1100CO/SN1100COD/SN0100CO/SN0100CODシリーズのデバイスでのみ使用できます。SN9100COシリーズのシリアルコンソールサーバーを設定するには、下記の「IPv4設定」を参照してください。

◆ IPv4設定

◆ IPアドレス:

IPv4はIPアドレスの従来の設定方法です。シリアルコンソールサーバーには、動的IPアドレスか、固定IPアドレスを割り当てます。

◆ 動的IPアドレスを割り当てる場合は、「IPアドレスを自動的に取得する」のラジオボタンを選択してください(デフォルト設定です)。

◆ 固定IPアドレスを設定する場合は、「IPアドレスを手動で設定する」のラジオボタンを選択し、お使いのネットワーク環境で有効なIPアドレスを入力してください。

注意:

1. 「IPアドレスを自動的に取得する」の項目を選択し、DHCPを使って製品のIPアドレスを自動的に取得する場合、製品は起動後にDHCPサーバーからのIPアドレスの割り当てを待機します。1分経過してもIPアドレスが割り当てられない場合は、工場出荷時にデフォルトで設定したIPアドレス (192.168.0.60/61)に戻ります。
2. 製品が、DHCPがアドレスを割り当てるネットワークに接続していて、なおかつIPアドレスを確認する必要がある場合は、p.179「IPアドレスの設定」を参照してください。

◆ DNSサーバー

◆ DNSサーバーのアドレスを自動的に割り当てる場合は、「DNSサーバーのアドレスを自動的に取得する」のラジオボタンを選択してください。

◆ DNSサーバーのアドレスを手動で割り当てる場合は、「DNSサーバーアドレスの手動設定」のラジオボタンを選択し、お使いのネットワークの優先DNSサーバーと代替DNSサーバーのIPアドレスをそれぞれ入力してください。

注意:

代替DNSサーバーのアドレスは任意で設定してください。

◆ IPv6設定

◆ IPアドレス:

IPv6はIPアドレス設定の新しいフォーマット(128ビット)です(詳細についてはp.181「IPv6」参照)。シリアルコンソールサーバーには、DHCPを使用して動的IPv6アドレスの設定または、固定IPv6アドレスの設定も可能です。

◆ 動的IPアドレスを割り当てる場合は、「IPアドレスを自動的に取得する」のラジオボタンを選択してください(デフォルト設定です)。

◆ 固定IPアドレスを設定する場合は、「IPアドレスを手動で設定する」のラジオボタンを選択し、お使いのネットワーク環境で有効なIPアドレスを入力してください。

◆ DNSサーバー

◆ DNSサーバーのアドレスを自動的に割り当てる場合は、「DNSサーバーのアドレスを自動的に取得する」のラジオボタンを選択してください。

◆ DNSサーバーのアドレスを手動で割り当てる場合は、「DNSサーバーアドレスの手動設定」のラジオボタンを選択し、お使いのネットワークの優先DNSサーバーと代替DNSサーバーのIPアドレスをそれぞれ入力してください。

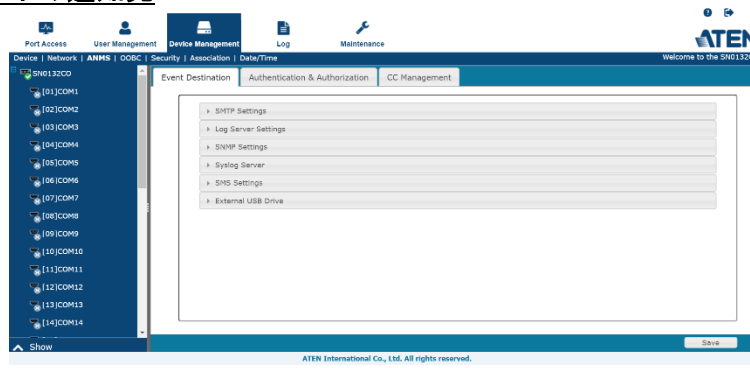
注意:

代替DNSサーバーのアドレスは任意で設定してください。

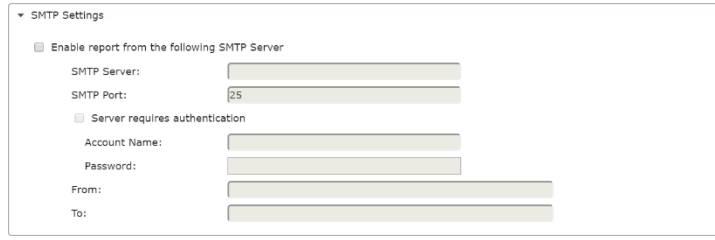
ANMS

ANMS (Advanced Network Management Settings)メニューでは外部システムからのログイン認証および権限を設定します。このメニューは3つのタブから構成しており、各タブには下図のような関連パネルを表示します。

イベントの通知先



◆ SMTP設定



SMTPサーバーからのレポートをユーザーにメール通知する場合は、以下の手順で操作してください。

1. 「以下のSMTPサーバーからの通知を有効にする」の項目にチェックを入れ、お使いのSMTPサーバーのIPv4アドレス、IPv6アドレス、ドメイン名のいずれかを入力してください。
2. SMTPポートを入力してください。
3. サーバーで認証が必要な場合は、「サーバー認証が必要」の項目にチェックを入れて、「アカウント名」、「パスワード」の各欄にお使いの環境に適した値

を設定してください。

4. レポートの差出人となるメールアドレスを「From」欄に入力してください。

注意:

1. 「差出人」フィールドで利用できるメールアドレスは1つだけで、64バイトを超えられません。
2. バイトは半角英数字1文字に相当します。

---

5. レポートの宛先となるメールアドレスを「To」欄に入力してください。

注意:

複数の宛先にレポートを配信する場合は、アドレスをセミコロンで区切ってください。また、宛先のアドレス全体が256バイト以内になるように設定してください。

◆ ログサーバー

ログインや内部ステータスメッセージなど、シリアルコンソールサーバーの内部で発生した重要なイベントは、自動的にログファイルに記録されます。

◆ この機能を有効にするには、「次のログサーバーからのレポートを有効にする」の項目にチェックを入れてください。

◆ ログサーバーが動作しているコンピューターのMACアドレスを「MACアドレス」欄に入力してください。

◆ ログサーバーが動作しているコンピューターがログデータをリッスンしているポートの番号を「サービスポート」欄に入力してください。有効なポート範囲は1～65535です。デフォルトでは9001です。

注意:

このポート番号は、「プログラム」で指定したポートとは別のポートを使用してください。

◆ SNMPサーバー

注意:

- ◆ SNMPトラップはSNMP v1/v2cをサポートします。
- ◆ SNMPエージェントはSNMP v1/v2c/v3をサポートします。

SNMPイベントの通知を受ける場合は、下記の手順に従って設定します。

1. 「SNMPエージェントを有効にする」および/または「SNMPトラップを有効にする」をオンにして、コミュニティーを入力します。
2. 「SNMPトラップ」には、IPアドレス(「**トラップ受信者**」欄に入力)と、SNMPトラップイベントを通知するコンピューターのサービスポート番号(**受信ポート**)欄に入力)を入力します。入力可能な値の範囲は1～65535です。また、デフォルトのポート番号は162です。

注意:

最大4つのSNMPトラップレシーバーを指定できます。SNMPレシーバーとなるコンピューターと同じポート番号を入力するようにします。

3. (SNMP エージェントのみ)SNMPv3 を使用するには、「SNMP V3を有効にする」をオンにして、アカウントとパスワードを入力します。

注意:

認証プロトコルのクライアント設定として、SHA およびAES-128 暗号化のみを使用してください。

◆ Syslogサーバー

シリアルコンソールサーバーの内部で発生した全イベントを記録し、Syslogサーバーに書き込む場合は、下記の手順に従って設定してください。

1. 「有効にする」の項目にチェックを入れてください。
2. SyslogサーバーのIPv4アドレス、IPv6アドレス、ドメイン名のいずれかを入力してください。
3. ポート番号を入力してください。ポート番号の有効な値の範囲は1～65535です。

◆ SMS設定

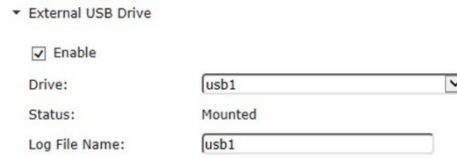
SMSで通知を受け取る場合は、下記の手順に従って設定してください。

1. 「有効にする」の項目にチェックを入れてください。
2. 「メッセージセンター」および「SMSレシーバー」の各欄に電話番号を入力してください。

注意:

入力内容の変更が完了したら、必ず画面右下にある「保存」をクリックしてください。

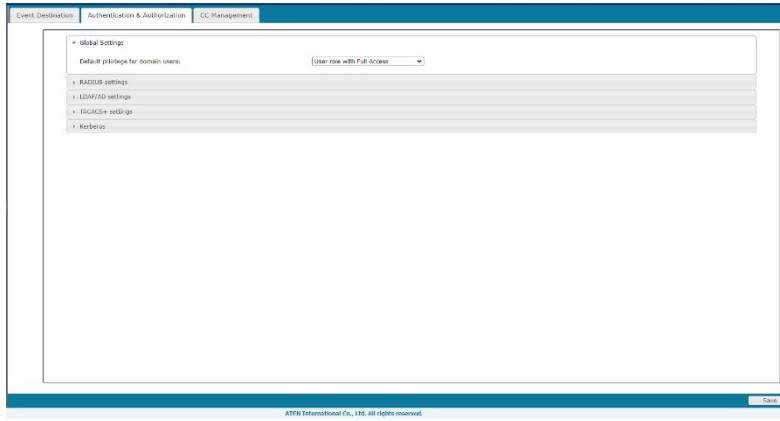
◆ 外付けUSBドライブ



シリアルコンソールサーバーで発生した全てのイベントを記録し、外部USBドライブに書き込むには、下記の手順に従って設定してください。

1. 「有効にする」の項目にチェックを入れてください。
2. イベントを書き込むドライブを選択してください。
3. ログのファイル名を入力してください。

認証と権限設定



◆ グローバル設定

ドメインユーザーの役割とアクセス権限を選択します。

- ◆ アクセス不可のユーザーロール：ドメインユーザーを、アクセス性を持たないユーザーロールに設定し、全てのシリアルポートに対する編集権限を設定します。
- ◆ フルアクセスのユーザーロール（デフォルト）：ドメインユーザーをユーザーの役割に設定し、全てのシリアルポートにアクセス権を設定します。
- ◆ フルアクセスの管理者ロール：ドメインユーザーを、アクセス性を持つ管理者ロールに設定し、全てのシリアルポートに対する編集権限を設定します。

注意：

- ◆ ドメインユーザー：ドメインユーザーの実際の権限は、ドメインユーザーの実際の権限は、「ANMS」の「認証と権限設定」タブ（p.131参照）、および「グループ」の「デバイス」タブで設定した内容を結合しています。サードパーティーの認証&権限サーバーとグループリスト（p.106参照）で同じグループ名が作成しているか確認します。優先順位は、「フルアクセス」

＞「参照のみ」＞「アクセス不可」です。

◆ 「権限」タブで「参照のみ」のユーザーを選択した場合（p.101参照）の優先順位は、次の通りです。「参照のみ」のユーザー ＞「フルアクセス」＞「参照のみ」＞「アクセス不可」。

◆ RADIUS設定

RADIUSサーバー経由でシリアルコンソールサーバーへの認証と権限設定をする場合は、以下の手順で操作してください。

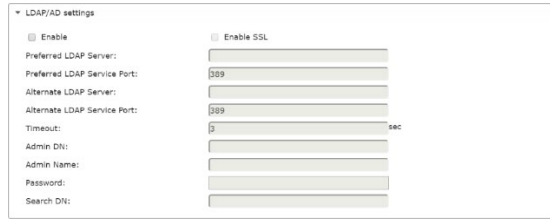
1. 「**有効にする**」の項目にチェックを入れてください。
2. 優先RADIUSサーバーと代替RADIUSサーバーのIPアドレスおよびポート番号をそれぞれ入力してください。IPの各欄は、IPv4アドレス、IPv6アドレス、ドメイン名のいずれかで設定できます。
3. 「タイムアウト」の項目に、シリアルコンソールサーバーがRADIUSサーバーの応答を待機する最大時間(秒)を入力してください。
4. 「再試行」の項目に、RADIUSサーバーを使ったログインの再試行可能回数を設定してください。
5. 「共有シークレット」の項目に、RADIUSサーバーとの認証で使用する共有シークレットの文字列を入力してください。入力には6文字以上が必要です。
6. RADIUSサーバーでは、以下のいずれかの方法でユーザー認証ができます。
   - ◆ ユーザーエントリーを「**su/xxxx**」として設定する。

     「xxxx」の部分は、シリアルコンソールサーバーでアカウントを作成したユーザーネームに置き換えてください。
   - ◆ RADIUSサーバー側とシリアルコンソールサーバー側で同じユーザーネームを使用する。
   - ◆ RADIUSサーバー側とシリアルコンソールサーバー側で同じグループネームを使用する。
   - ◆ RADIUSサーバー側とシリアルコンソールサーバー側で同じユーザーネーム、グループネームを使用する。

いずれの方法においても、ユーザーのアクセス権限は、グループユーザーがシリアルコンソールサーバーで作成した際に割り当てた権限となります（p.101「ユー

ザーの作成」参照）。

◆ LDAP/AD設定



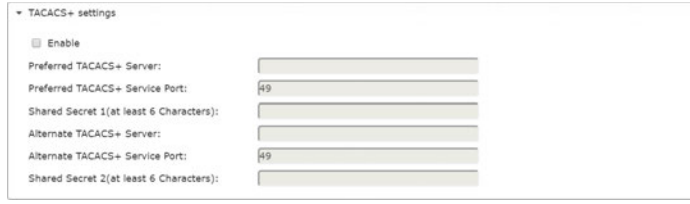
シリアルコンソールサーバーにログインするユーザーの認証および権限設定をLDAP/ADで行う場合は、以下の表を参照してください。

項目	アクション
有効にする	「有効にする」チェックボックスをオンにすると、LDAP を有効にします。また、「SSL を有効にする」をオンにすると、LDAPS認証および承認を有効にします。
LDAP サーバーIP/ LDAPサービスポート	LDAP/LDAPSサーバーのIPアドレスやポート番号を入力してください。 ◆ 「LDAPサーバー」欄は、IPv4アドレス、IPv6アドレス、ドメイン名を使って設定できます。 ◆ LDAPの場合、デフォルトのポート番号は389、LDAPSの場合、デフォルトのポート番号は636です。
代替LDAP サーバーIP/ サービスポート	代替LDAP/LDAPSサーバーのIPアドレスやポート番号を入力してください。 ◆ 「代替LDAPサーバー」欄は、IPv4アドレス、IPv6アドレス、ドメイン名を使って設定できます。 ◆ 代替LDAP サービスポートの場合、デフォルトのポート番号は389です。代替LDAPS サービスポートの場合、デフォルトのポート番号は636 です。
アドミニストレーターDN	この項目はLDAPまたはLDAPSサーバーの管理者にご確認の上、設定してください。以下、設定例です。 ou=kn4132,dc=aten,dc=com
アドミニストレーター名	LDAPアドミニストレーターのユーザーネームを入力してください。
管理者のパスワード	LDAPアドミニストレーターのパスワードを入力してください。
サーチDN	検索ベースの識別名を設定してください。ユーザーネームの検索を開始するDNS名です。
タイムアウト	シリアルコンソールサーバーがLDAP/LDAPSサーバーの応答を待機する時間(秒)を設定してください。

LDAP/ADサーバーでは、下記のいずれかの方法でユーザー認証ができます。

- スキーマなし – シリアルコンソールサーバーで使用するユーザーネームのみがLDAP / LDAPS サーバー上の名前と照合されます。ユーザー権限は、シリアルコンソールサーバー側で定義したものと同じです。
- スキーマなし – AD内のグループのみが照合されます。ユーザー権限は、シリアルコンソールサーバー上で、ユーザーが属しているグループに設定している権限と同じです。
- スキーマなし – ADのユーザーネームとグループが照合されます。ユーザー権限は、ユーザーが属しているグループとユーザーに設定している権限と同じです。

- TACACS+設定

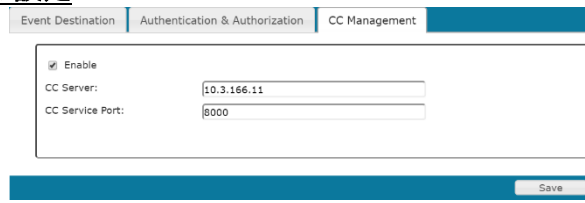


- TACACS+ を**有効**にし、次の情報を入力してください。
  - 優先TACACS+サーバー
  - 優先TACACS+サービスポート
  - 共有シークレット1
  - 代替TACACS+サーバー
  - 代替TACACS+サービスポート
  - 共有シークレット2

- Kerberos

- Kerberosを有効にし、次の情報を入力してください。
  - Kerberosサーバー
  - Kerberosサービスポート
  - Kerberos領域

CC管理の設定



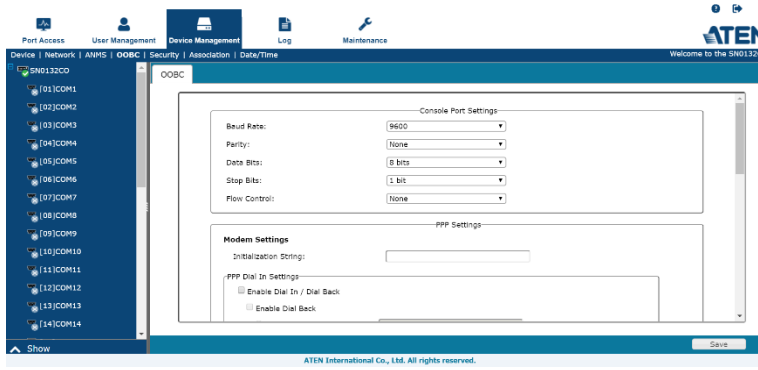
CC(Control Center)サーバー経由でシリアルコンソールサーバーの認証をする場合は、「有効にする」の項目にチェックを入れ、CCサーバーのIPアドレスと通信に使用するポートを、該当する項目に入力してください。「CCサーバーIP」欄は、IPv4アドレス、IPv6アドレス、ドメイン名のいずれかで設定できます。

注意:

この機能が有効だと、シリアルコンソールサーバー上で電源管理デバイスを設定していたとしても、サイドバーには表示しません。というのは、各デバイスがCCサーバーによって管理されているためです。

OOBC

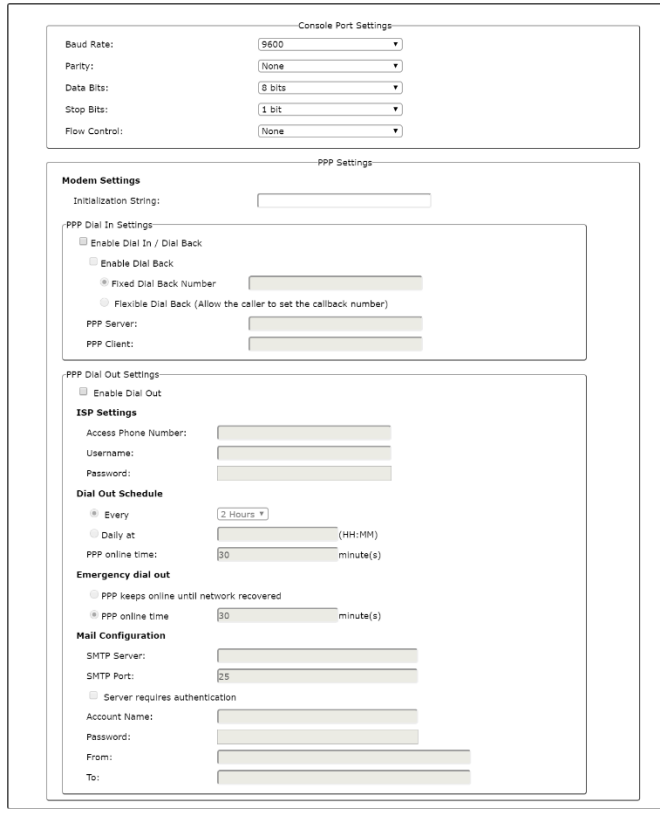
万が一、シリアルコンソールサーバーがTCP/IPネットワーク経由でアクセスできなくなった場合でも、製品本体のモデムポート、またはモデム用に設定したシリアルポート(SN9108CO/SN9116CO)でアクセス可能です。



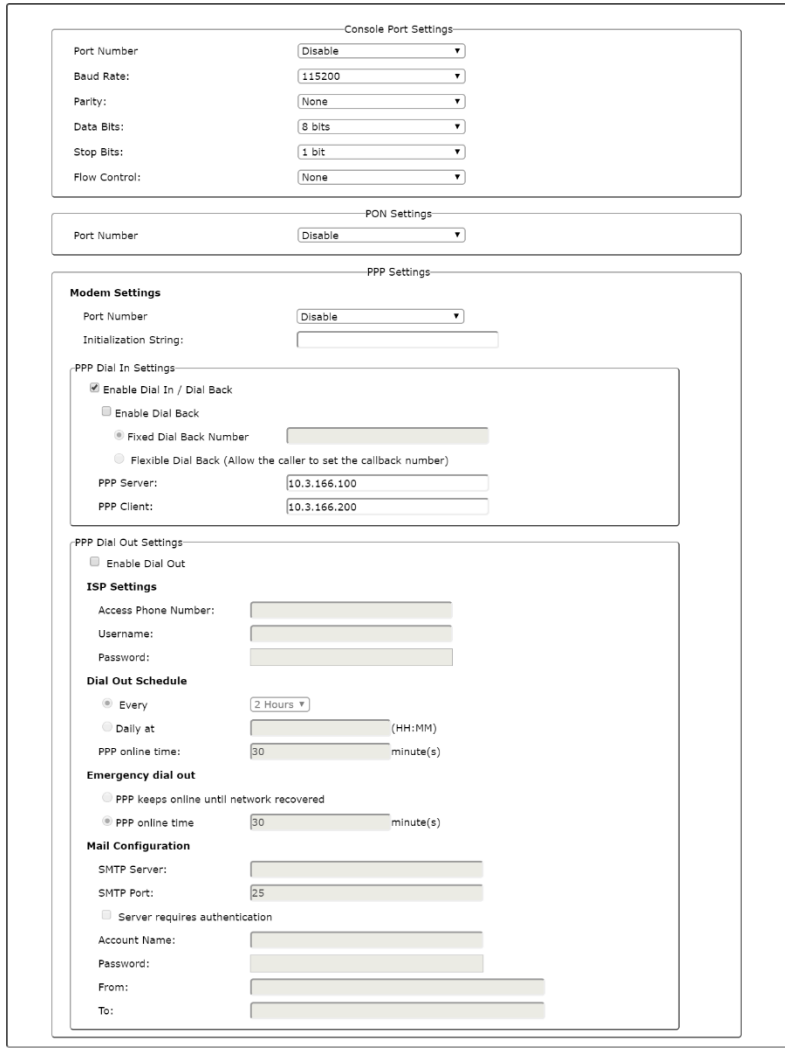
コンソールポートの設定

SN1100CO/SN1100CODシリーズ

SN0100CO/SN0100CODシリーズ



SN9100COシリーズ



SN9100COシリーズのリアパネルで、コンソール、電源管理デバイス(予約済み)、モデムが接続しているポートのポート番号を選択してください。デフォルトでは、SN9100COシリーズのコンソールポートのポート番号は無効です。

ダイヤルバックを有効にする (SN0100CO/SN0100COD/SN9100COシリーズのみ)

「アウトオブバンド・アクセス」を有効にすると、以降のセクションで説明する「ダイヤルバックを有効にする」と「ダイヤルアウトを有効にする」の機能が使えます。新たに追加したセキュリティー機能として、この機能が有効になると、シリアルコンソールサーバーは自身へのダイヤルイン接続を切断し、下表で定義したエントリーの1つにダイヤルバック接続します。

項目	アクション
固定番号へのダイヤルバックを有効にする	「固定番号へのダイヤルバックを有効にする」の項目が有効だと、シリアルコンソールサーバーは着電があった際に、モデム接続を切断し、設定した電話番号のモデムにダイヤルバック接続します。 「電話番号」欄には、シリアルコンソールサーバーにダイヤルバックさせたい番号を入力してください。
フレキシブルダイヤルバックを有効にする	フレキシブルダイヤルバックが有効だと、シリアルコンソールサーバーがダイヤルバックするモデムは固定である必要はありません。この場合、次のように、任意のモデムにダイヤルバックできます。 1. ユーザーが「パスワード」欄に指定する必要があるパスワードを入力します。 2. シリアルコンソールサーバーのモデムに接続する際には、ユーザーは、製品がダイヤルバック接続する先となる電話番号を「ユーザーネーム」欄に、また、パスワードを「パスワード」欄にそれぞれ指定します。

ダイヤルアウトを有効にする (SN0100CO/SN0100COD/SN9100COシリーズのみ)

ダイヤルアウト機能の場合は、インターネットサービスプロバイダーとアカウントを確立し、モデムを使用してISP アカウントにダイヤルアップ接続する必要があります。ダイヤルアウトを有効にする項目の説明を以下の表に示します。

項目	アクション
ISPの設定	ISPへの接続に使用するための電話番号、アカウント名(ユーザーネーム)、およびパスワードを指定します。

項目	アクション
ダイヤルアウト スケジュール	ISP接続でシリアルコンソールサーバーがダイヤルアウトする頻度を設定します。 ◆ 「繰り返し」では、1～4時間ごとに定時で実行するように設定できます。 ◆ 例えば、2時間ごとに設定した場合、シリアルコンソールサーバーは次の00分から2時間おきにダイヤルアウトで接続します。 ◆ 決まったスケジュールでシリアルコンソールサーバーにダイヤルアウト接続しない場合は、リストから「**なし**」を選択してください。 ◆ 「毎日」のラジオボタンを選択すると、指定した時刻に日次でダイヤルアウトにて接続します。時刻の時と分をセミコロンで区切り、「hh:mm」のフォーマットで設定してください。 ◆ 「PPPオンライン時間」欄では、セッションが終了し、モデムとの接続を切断するまでISP接続のオンライン状態を持続する時間を設定します。0を設定すると、常にオンラインになります。
緊急 ダイヤルアウト	シリアルコンソールサーバーがネットワークから切断された、または、ネットワークがダウンした場合、この機能を使うと、ISPのダイヤルアップ接続でシリアルコンソールサーバーをオンラインにできます。 ◆ 「ネットワーク回復までPPPがオンラインを持続する」を選択すると、ネットワークが復旧するかシリアルコンソールサーバーがネットワークに再接続するまでISPへのPPP接続が持続します。 ◆ 「PPPオンライン時間」を選択すると、設定した時間が経過した後にISPへの接続が終了します。0を設定すると、常にオンラインになります。

項目	アクション
メール設定	このセクションでは、発生した問題の電子メール通知について説明します シリアルコンソールサーバーのポートに接続したデバイス(p.127「SMTP設定」を参照)。 **注意:**このメール通知機能は、社内のメールサーバーではなくISPのメールサーバーを使って処理をするため、p.127で説明したSMTP設定での通知機能とは若干異なります。 ◆ 「SMTPサーバーIPアドレス」欄に、お使いのSMTPサーバーのIPv4アドレス、IPv6アドレス、ドメイン名のいずれかを入力してください。 ◆ SMTP サーバーのSMTP ポートを入力します。デフォルトはポート番号とポートネーム(PORT NUMBER+PORT NAME)です。ポート番号がわからない場合は、SMTPサーバー管理者に問い合わせてください。 ◆ サーバーで認証が必要な場合は、「SMTPサーバーで認証が必要」チェックボックスをオンにし、認証アカウント名とパスワードを該当欄に入力します。認証アカウント名とパスワードがわからない場合や、サーバーで認証が必要かわからない場合は、SMTP サーバー管理者に問い合わせてください。 ◆ 「差出人」フィールドに、SMTP サーバーの管理者(または同等の権限があるアドミニストレーター) の電子メールアドレスを入力します。 ◆ 「To」欄に、レポートの宛先となるメールアドレスを入力してください。複数のアドレスに送信する場合は、コンマまたはセミコロンでアドレスを区切ってください。

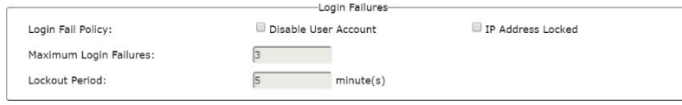
この画面で項目への入力・設定が完了したら、「**保存**」ボタンをクリックしてください。

セキュリティー

「セキュリティー」メニューは、以下のセクションで説明する4つのメインパネルから構成しています。

ログイン失敗

セキュリティーを強化するために、「ログイン失敗」のセクションでは、ユーザーのログインエラーを処理する際に適用するポリシーを設定できます。



設定する場合は、複数あるチェックボックスで該当するものにチェックを入れてください。各項目が表す内容は下表の通りです。

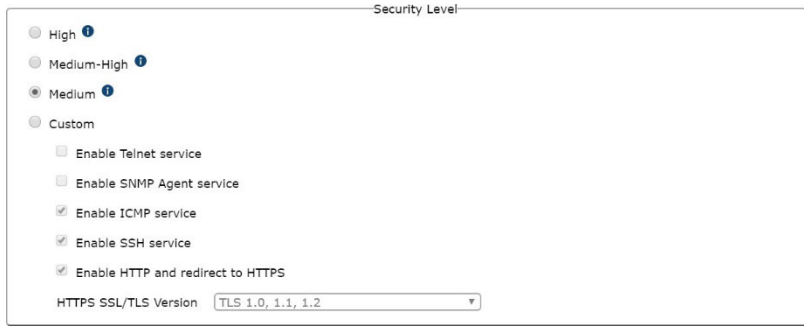
項目	説明
ログイン失敗ポリシー	設定したセキュリティーパラメーターに従って、ユーザーがログインに失敗した場合の処理方法を決定します。ユーザーのログインエラーの回数が上限に達した場合、シリアルコンソールサーバーは次の処理のいずれかができます。 ◆ ユーザーアカウントを無効にする ◆ IPアドレスをロックする このポリシーが有効になる時間については、「ロックアウト期間」の項目で設定します。
最大ログイン試行回数	ログイン失敗ポリシーが有効になるまでにユーザーがログインを再試行できる回数を設定します。
ロックアウト期間	アクセスが再び可能になるまでに、ユーザーアカウントが無効になる時間、またはIPアドレスをロックする時間を設定します。この時間を過ぎると、アクセスは再びアクティブになります。

注意:

ログイン失敗ポリシーが無効の場合、ユーザーは無制限で何度でもログイン試行が可能です。セキュリティー上の理由から、この機能とロックアウトポリシーを有効にすることを推奨します。

セキュリティーレベル

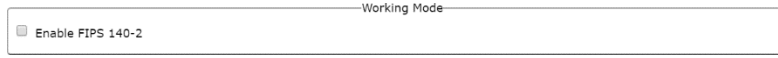
セキュリティーを強化するために、セキュリティー機能を「高」、「中高」、「中」または「カスタム」のラジオボタンで選択してください。



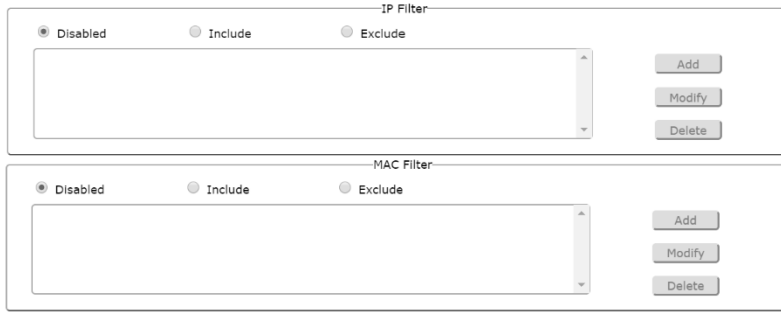
1. 高 – SSHv2、HTTPS(TLS v1.2)を除く、全てのサービスを無効にします。
2. 中高 – SSHv2、HTTPからHTTPSへのリダイレクト、HTTPS(TLS v1.2)、ICMPを有効にします。
3. 中 – SSHv2を有効にし、HTTPSをHTTPS、HTTPS(TSL v1.0、1.1、1.2)、ICMPにリダイレクトします(デフォルト)。
4. カスタム – 次のセキュリティーオプションから適用したい項目にチェックを入れてください。
   - ◆ Telnetサービスを有効にする
   - ◆ SNMPエージェントサービスを有効にする
   - ◆ ICMPサービスを有効にする
   - ◆ SSHサービスを有効にする(デフォルトで選択状態)
   - ◆ HTTP を有効にし、HTTPS にリダイレクトする(デフォルトでオン)
     HTTPS SSL/TLS バージョン:「TLS 1.2」、「TLS 1.0、1.1、1.2」(デフォルト)、「SSL 3.0、TLS 1.0、1.1、1.2」から選択します。

動作モード

セキュリティーを強化するために、このチェックボックスで暗号化モジュールの「FIPS 140-2」のセキュリティー機能を有効にできます。



IP/MACフィルター



◆ IP/MACフィルター

IP/MACフィルター機能は、シリアルコンソールサーバーへの接続を試みるコンピューターのIPアドレス、またはMACアドレス、あるいは両方に基づいて、シリアルコンソールサーバーへのアクセスを制御します。フィルターはIP、MAC各フィルターともそれぞれ最大で100項目作成できます。フィルターを設定すると、IPフィルターは上部のリストボックスに、MACフィルターは下部のリストボックスにそれぞれ表示します。

IPやMACのフィルターの機能を有効にする場合は、次のいずれかのラジオボタンを選択してください。

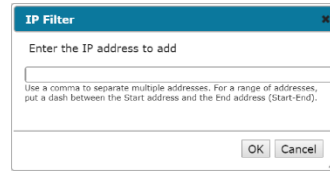
◆ 「**含む**」ラジオボタンを選択している場合は、指定のアドレスもしくは指定範囲内のアドレスからのアクセスを許可します。指定以外のアドレスからのアクセスは全て拒否されます。

◆ 「**除く**」ボタンを選択している場合は、指定のアドレスもしくは指定範囲内のアドレスからのアクセスを拒否します。指定以外のアドレスからのアクセスは全て許可されます。

◆ フィルター項目の追加

IPアドレスのフィルター項目は以下の手順で追加してください。

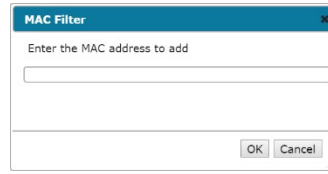
1. 「**追加**」ボタンをクリックしてください。下図のようなダイアログが表示されます。



2. フィルタリングの対象となるIPアドレスを入力してください。
3. IPアドレスを入力したら、「**OK**」ボタンをクリックしてください。
4. 他にもフィルター項目がある場合は、上記手順の操作を繰り返して設定してください。

MACアドレスのフィルター項目は以下の手順で追加してください。

1. 「**追加**」ボタンをクリックしてください。ダイアログボックスが表示されます。



2. ダイアログボックスでMACアドレスを入力したら、「**OK**」ボタンをクリックしてください。
3. フィルタリングする追加のMACアドレスに対して、各手順を繰り返してください。

◆ IPフィルターとMACフィルターの競合

IPフィルターとMACフィルターの間に競合がある場合(つまり、コンピューターのアドレスが一方のフィルターで許可しているものの、もう一方のフィルターでブロックしている場合)、ブロックフィルターを優先します(コンピューターのアクセスをブロックします)。

◆ フィルターの変更

フィルターを変更する場合は、対象となる項目をIPフィルターリスト、またはMACフィルターリストのボックスから選択し、「**変更**」をクリックしてください。フィルター追加時に表示するものと同様のダイアログボックスが表示されますの

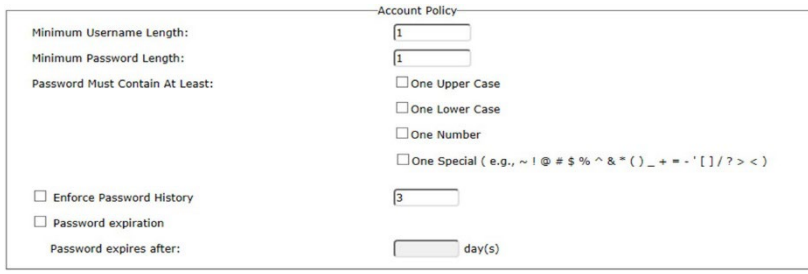
で、古いアドレスを削除して新しいアドレスに変更してください。

◆ フィルターの削除

フィルターを削除する場合は、対象となる項目をIPフィルターリスト、またはMACフィルターリストのボックスから選択し、「**削除**」ボタンをクリックしてください。

アカウントポリシー

システム管理者はこのセクションでユーザーネームやパスワードの管理ポリシーを設定できます。

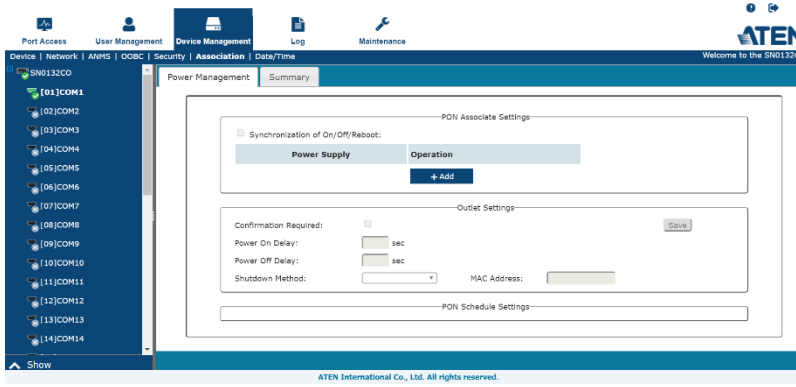


このセクションにおける各項目の内容は下表の通りです。

項目	説明
ユーザーネーム最小文字数	ユーザーネームの設定に最低限入力が必要な文字数を設定します。許容値は1～16 です。デフォルトでは6です。
パスワード最小文字数	パスワードの設定に最低限入力が必要な文字数を設定します。許容値は0～16 です。0を設定した場合は、パスワードの入力が不要です。ユーザーはユーザーネームだけでログインできるようになります。デフォルトでは6です。
パスワードには以下が必須	いずれかをチェックすると、ユーザーはパスワードに少なくとも1つの大文字、1つの小文字、1つの番号、または1つの特殊文字を含める必要があります。 **注意**:このポリシーは既存のユーザーアカウントには適用されません。有効後にユーザーを作成したり、パスワードを変更したりした場合に、このポリシーが適用されます。
パスワード履歴を実行する	この項目では、古いパスワードを再度使用できるようにするまでに、固有のパスワードを設定しなければならない回数(X)を設定できます。Xは、ダイアログボックスに入力した番号に相当します。
パスワード期限	パスワードの有効日数を入力してください。

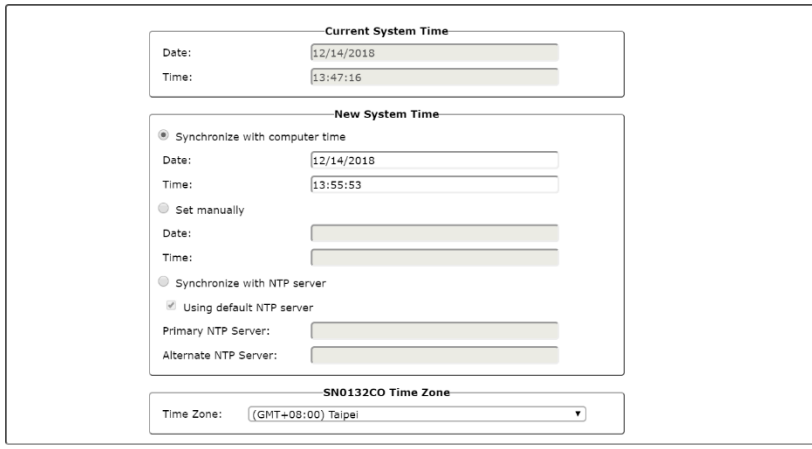
関連付け

「関連付け」メニューは予約済みの機能です。



日付/時刻

「日付/時刻」ダイアログ画面では、シリアルコンソールサーバーの時刻パラメーターを設定します。



パラメーターは下記を参考にしながら設定してください。

現在のシステム時刻

このセクションには、製品本体に現在設定している日時を表示します。日付と時刻の欄は読み取り専用のため、編集できません。

注意:

ブラウザーUI では、システム時刻には、ウェブブラウザーセッションが発生したタイムゾーンからの相対時間を表示します。本装置のタイムゾーンではありません。ウェブブラウザーのセッションの開始場所と製品の設置場所のタイムゾーンが異なる場合、ここで表示する時刻は、製品内部のシステム時刻とは異なります。

新規システム時刻

製品本体の日時設定は、各項目を使って、下記の通りに変更してください。

- ◆ 製品本体の日時を、自分がログインしているコンピューターの日時に合うように変更する場合は、「コンピューターの時刻と同期する」のラジオボタンを

選択してください。

注意:

コンピューターの日時は、この項目の下に表示しています。各項目は情報提供のみを目的としています。

- 日時を手動で変更する場合は、「**手動設定**」のラジオボタンを選択して、日付は「YYYY-MM-DD」の形式で、時刻は「HH:MM:SS」の形式でそれぞれ入力してください。

注意:

日付/時刻の形式は、選択したインターフェース言語によって異なる場合があります。

- 時刻をネットワークタイムサーバーと自動的に同期させる場合は、「**NTPサーバーと同期する**」のラジオボタンを選択してください。
  - お使いのネットワークのデフォルトタイムサーバーを使用したい場合は、「デフォルトNTPサーバーを使用する」の項目にチェックを入れてください。
  - タイムサーバーを指定したい場合は、「デフォルトNTPサーバーを使用する」の項目からチェックを外して、使用するタイムサーバーのIPアドレスを「優先NTPサーバー」の欄に入力してください。代替タイムサーバーも設定する場合は、サーバーのIPアドレスを「代替NTPサーバー」の欄に入力してください。
  - 変更内容を適用する場合は「**保存**」をクリックしてください。

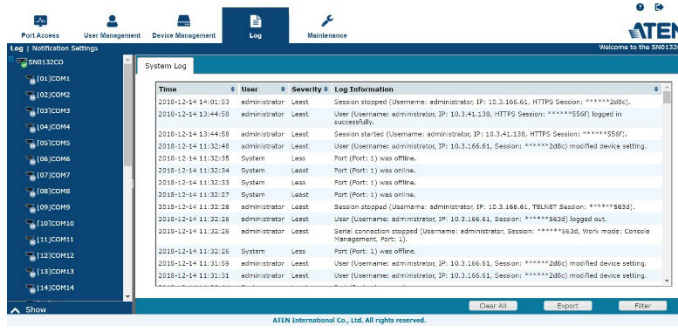
タイムゾーン

- シリアルコンソールサーバーの設置場所のタイムゾーンを設定する場合は、「タイムゾーン」のリストを展開し、場所に最も近い都市を選択してください。
- 変更内容を適用する場合は「**保存**」をクリックしてください。

第9章
ログ

概要

シリアルコンソールサーバーで発生した全イベントは、製品内部でログとして記録します。ログの内容を確認する場合は、「ログ」タブをクリックしてください。デバイスのログ情報を表示します。



システムログ

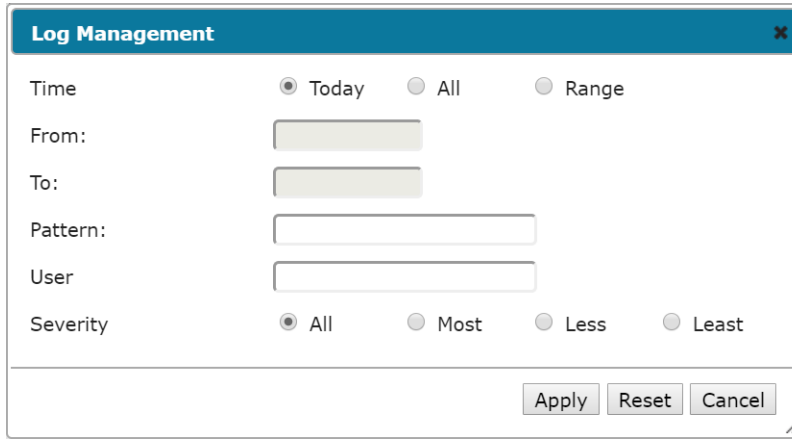
「システムログ」メニューには、シリアルコンソールサーバーの製品内部で発生したイベントや、イベントの時刻、重要度、ユーザーの概要、またログ情報がそれぞれ表示します。列の見出しをクリックすると、項目で表示順を変更します。

システムログのメモリサイズは1MB です。ログの内容に応じて、最小512 件以上のイベントを表示できます。記録したイベントの数が512になると、新しいイベントが発生した際に、一番古いイベントを切り捨てます。画面下部にあるボタンの詳細は下表の通りです。

ボタン	説明
ログのクリア	ログファイルの内容を消去します。
ログのエクスポート	ログの内容をお使いのコンピューター上にファイルとして保存します。
フィルター	日付、特定の文字列等でイベントを検索します(次のセクションに記載)。

フィルター

この機能を使うと、表示するログイベント情報を、発生時間、メッセージに含まれているキーワード、ユーザーネームなどの条件で絞り込めます。この機能を呼び出すと、画面下部に下図のようなメニューが表示されます。



この画面に表示する各項目の内容は下表の通りです。

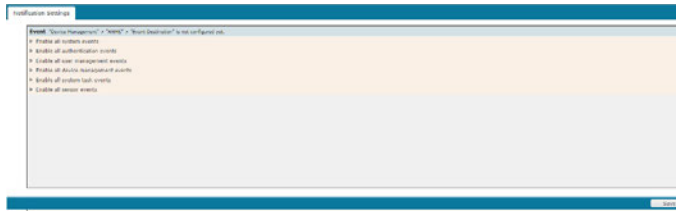
項目	説明
時刻	この機能を使用すると、特定の時間に発生したイベントを次のようにフィルタリングできます。 **本日のみ**:現在の日付で発生したイベントのみ表示します。 **全て**:ログファイル内の全イベントを表示します。 **範囲**:特定の期間に発生したイベントを検索します。「**From**」欄と「**To**」欄をクリックし、表示したカレンダーコントロールから日付を選択してください。
パターン	特定のキーワードを含むイベントを検索します。キーワードはテキストボックスに入力してください。その文字列を含むイベントだけが表示します。ワイルドカード(1文字の場合は?、複数の文字の場合は*)や、「or」キーワードを使えます。例えば、「h*ds」は「hand」と「hoods」を返し、「h?nd」は「hard」と「hand」を返しますが、「hard」は返しません。「h*ds or h*ks」は「hand」と「hook」を返します。
ユーザー	特定のユーザーに関連するイベントを検索します。この条件で検索する場合は、テキストボックスに対象ユーザーのユーザーネームを入力して「**適用**」ボタンをクリックしてください。この文字列を含むユーザーネームに関連したイベントのみが表示します。 **注意**:検索条件に合致するユーザーが存在しない、または入力を誤ると、検索結果の一覧に表示しません。

項目	説明
重要度	イベントの重要度に基づいてイベントを検索します。イベントの重要度が低いイベントは黒で、やや低いイベントは青で、また、最大のイベントは赤色でそれぞれ表示されます。 この条件で検索する場合は、指定したい重要度のレベルのラジオボタンを「全て」、「最大」、「中」、「最小」のいずれかから選択してください。 指定した重要度に一致したイベントのみ表示します。
適用	指定した条件で検索します。
リセット	検索条件をデフォルトの状態に戻します。
キャンセル	変更を適用せずに、ログフィルター機能を終了します。

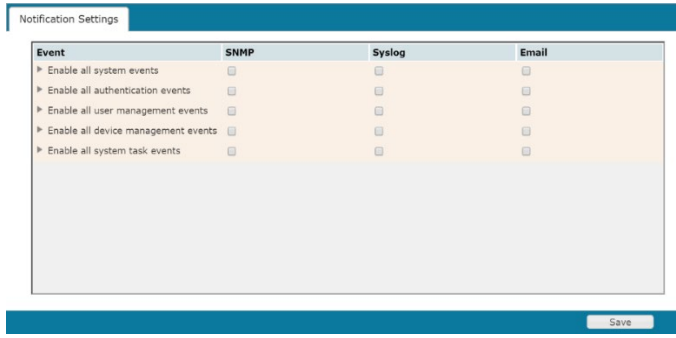
ログ通知設定

「通知設定」メニューでは、通知のトリガーとなるイベントを選択できます。

SN1100CO/SN1100CODシリーズ



SN0100CO/SN0100COD/SN9100COシリーズ

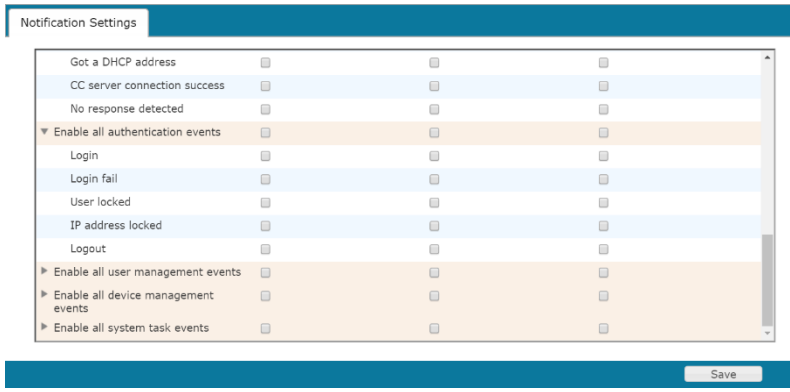


イベント通知は、5つのグループに分かれます。次から選択して有効にできます。

- ◆ 全てのシステムイベント
- ◆ 全ての認証イベント
- ◆ 全てのユーザー管理イベント
- ◆ 全てのデバイス管理イベント
- ◆ 全てのシステムタスクイベント
- ◆ 全てのセンサーイベント(SN1100CO/SN1100CODシリーズのみ)

特定の通知のオン・オフを切り替えるには、▶のアイコンをクリックしてグループを

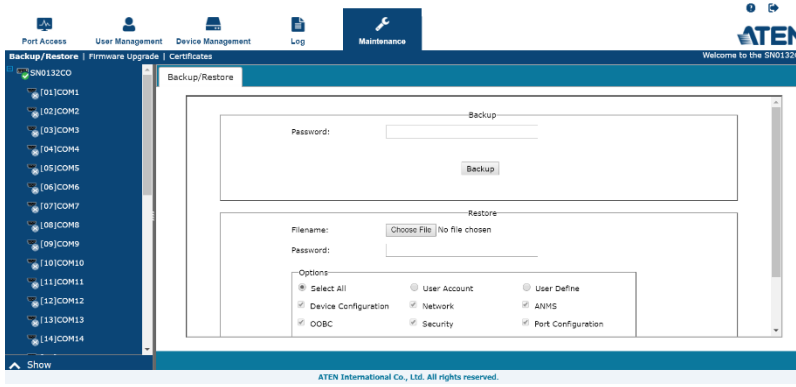
展開し、個々の通知のチェックを操作してオン・オフにしてください。



第10章
メンテナンス

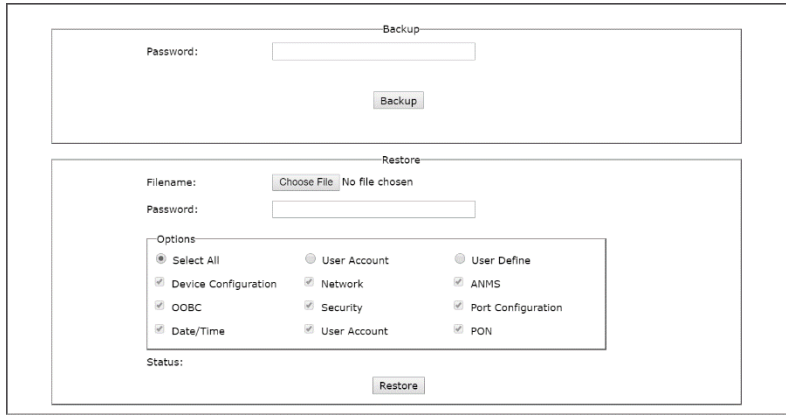
概要

「メンテナンス」タブでは、ファームウェアのアップグレード、設定値やアカウント情報のバックアップ/リストア、デフォルト値のリストアができます。



バックアップ/リストア

「メンテナンス」タブをクリックすると、「バックアップ/リストア」画面が開きます。この画面では、シリアルコンソールサーバーの設定やユーザープロファイル情報のバックアップができます。



バックアップ

デバイスの設定のバックアップを作成する場合は、以下の手順で操作してください。

1. 「パスワード」の項目に、ファイルの復元に必要となるパスワードを入力してください。

注意:

1. パスワードの設定は任意です。パスワードを設定しない場合、ファイルはパスワードなしで復元します。
2. パスワードを設定する場合、リストアの際にこのパスワードが必要になりますので、忘れないように記録しておいてください。

---

2. 「**バックアップ**」ボタンをクリックしてください。
3. ブラウザーからファイルの保存方法を問うダイアログを表示した場合は、「保存」を選択し、お使いのコンピューターのドライブの適当な場所に保存してください。

リストア

バックアップの内容をリストアする場合は、以下の手順で操作してください。

1. 「**参照...**」ボタンをクリックし、バックアップファイルを保存しているフォルダーを選択してください。

注意:

デフォルト設定のファイル名を変更しても、新しい名前でそのままお使いいただけます。元の名前に変更する必要はありません。

---

2. バックアップファイル作成の際にパスワードを設定している場合は、「パスワード」欄に、パスワードと同じ文字列を入力してください。
3. ファイルに保存した内容のうち、リストアしたい項目にチェックを入れてください(複数選択可)。
4. 「**リストア**」ボタンをクリックしてください。

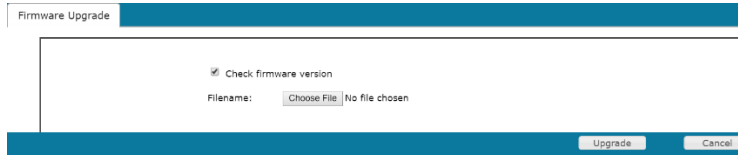
   ファイルがリストアすると、処理に成功したという内容のメッセージを表示します。

ファームウェアアップグレード

ファームウェアをアップグレードするには、下記の手順に従って操作してください。

1. ウェブインターフェースで❓をクリックして、シリアルコンソールサーバーのハードウェアプラットフォーム(AXまたはAXA) を確認します。
   次に例を示します。

2. シリアルコンソールサーバーのハードウェアプラットフォームに基づいてファームウェアファイルをダウンロードします。
3. シリアルコンソールサーバーにログインし、「メンテナンス」タブをクリックして、「ファームウェアアップグレード」の画面を開いてください。

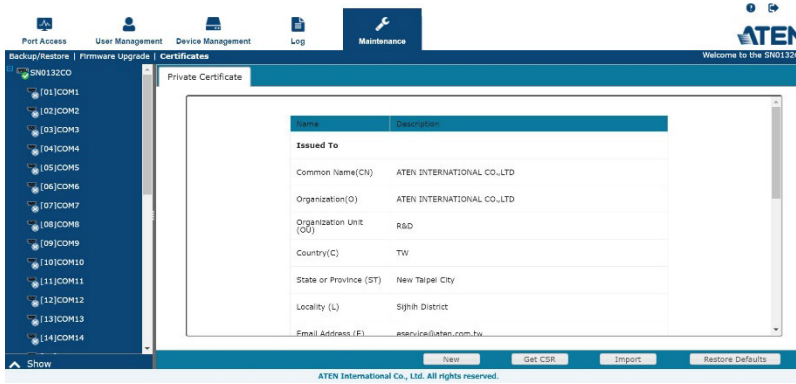


4. 「**参照**」をクリックし、新しいファームウェアファイルがあるディレクトリーに移動して、ファイルを選択します。
5. 「**ファームウェアアップグレード**」ボタンをクリックし、アップグレードを実行してください。
   - ◆ 「ファームウェアバージョンを確認する」の項目にチェックが入っていると、現在使用しているファームウェアとインストールしようとしているファームウェアファイルとの間でバージョンを比較します。2つのバージョンが同じ、もしくは現在使用しているファームウェアのバージョンの方が新しい場合、状況を通知するポップアップメッセージを表示し、アップグレードが中断されます。
   - ◆ 「ファームウェアバージョンを確認する」の項目にチェックが入っていない場合は、バージョンを比較せずファームウェアをアップグレードします。
   - ◆ アップグレードの進行状況は、プログレスバーで確認できます。
   - ◆ アップグレードに成功すると、シリアルコンソールサーバーは再起動します。
6. シリアルコンソールサーバーに再度ログインし、ファームウェアのバージョン情

報が更新されているか確認してください。

証明書

この画面では、プライベート証明書に関する情報を確認できます。



プライベート証明書

SSL接続でログインすると、ユーザーが意図するサイトにログインしようとしているか検証するために署名済み証明書が使われます。デフォルトのATEN証明書を使うのではなく、このセクションで自分のプライベート暗号キーと署名済み証明書を使うように設定し、セキュリティーを強化できます。

- プライベート証明書の作成方法には、自己署名証明書を作成する方法と、サードパーティーの証明局(CA)によって署名された証明書をインポートする方法の2つの方法があります。
- CA署名付きSSLサーバー証明書の取得

  セキュリティーを最大限に高めるために、サードパーティーの認証局(CA)署名付き証明書の使用を推奨します。サードパーティー署名付き証明書を取得するには、p.159「証明書署名要求」を参照してください。
- 自己署名済み証明書の作成

  独自の自己署名証明書を作成する場合は、無料のユーティリティーopenssl.exeをウェブ経由でダウンロードできます。

  プライベートに信頼済SSL/TLS 証明書は、**内部**ネットワーク内のユーザーとデバイスの認証のみに使用してください。詳細については、p.190「自己署名SSL/TLS証明書」を参照してください。

注意:

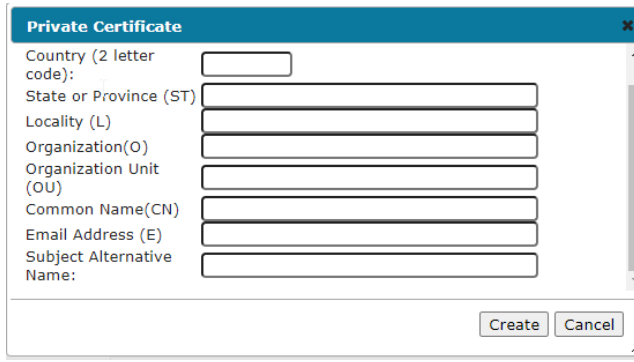
「**デフォルトのリストア**」をクリックすると、デバイスはデフォルトのATEN証明書を使用するようになります。

証明書署名要求

「証明書署名要求(CSR)」セクションでは、CA 署名付きSSLサーバー証明書を自動的に取得してインストールできます。

この操作をする場合は、下記の手順に従ってください。

1. 「**新規**」をクリックしてください。下図のようなダイアログボックスが表示されます。



2. お使いの環境で有効な値を、項目に入力してください。下記に例を示します。

情報	例
国(2文字のコード)	TW
州または都道府県	Taiwan
市区町村	Taipei
組織	Your Company, Ltd.
部署	Tech Department

情報	例
コモンネーム	mycompany.com **注意:** 証明書を有効にしたいサイトのドメイン名を正確に入力してください。サイトのドメイン名がwww.mycompany.comで、mycompany.com のみを指定した場合、証明書は有効になりません。
メールアドレス	administrator@yourcompany.com
サブジェクト別名	DNS: aten.com Email : ian@aten.com.tw URI : http://www.aten.com.tw IP : 10.0.0.1 **注意:** サポートはPEM形式のみです。

3. フォームへの入力(全項目への入力が必須)が完了したら、「**作成**」をクリックしてください。

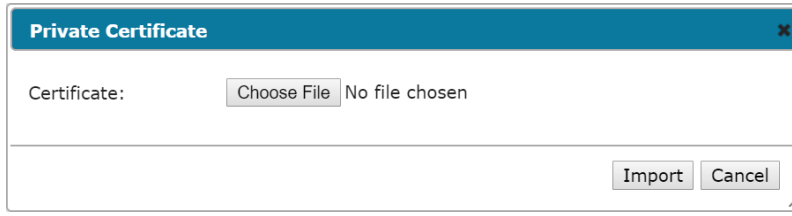
   入力した情報に基づく自己署名証明書がSNデバイスに保存されます。

4. 「**CSRの取得**」をクリックし、証明書ファイル(custom.csr)をコンピューター上の都合の良い場所に保存します。

   これは、署名済みSSL証明書の申請の際にサードパーティーの認証局へ提出が必要となるファイルです。

5. 認証局から証明書が送られて来たら、この証明書をお使いのコンピューターの適当なフォルダーに保存してください。

6. 下のメニューバーにある「**インポート**」をクリックしてください。下図のような「プライベート証明書」のウィンドウをポップアップ表示します。



7. 「**ファイルを選択**」をクリックしてファイルを置いたら、「証明書ファイル名」として選択ください。「**インポート**」をクリックして、ファイルをシリアルコンソールサーバーに保存してください。

注意：

ファイルをアップロードすると、シリアルコンソールサーバーではファイルをチェックし、特定の情報が一致しているかを確認します。もし、一致していれば、このファイルを受け入れます。一致しなければ、このファイルを拒否します。

(例えば、ドメイン名の変更で新しい証明書に置き換えたいなどの理由で)証明書を削除する場合は、「**デフォルトをリストアする**」をクリックしてください。

付録

安全にお使いいただくために

全般

- 本製品は、屋内での使用に限ります。
- 製品の同梱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。
- また、弊社ウェブ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、または熱源となる機器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を設けています。通気口のある製品は、安定した運用をするため、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。
- 電気回路が過負荷状態に陥らないようにしてください。電気機器を回路に接続する前に、電源装置の制限を把握し、超えないようにしてください。回路の電気仕様を常に見直して、危険な条件を生じさせていないかまた、すでに危険な条件がそろっていないかを確認してください。電気回路の過負荷は火災や機器破損の原因となります。
- 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、購入し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、全ての装置を適切に接地するようにしてください。
- 製品付属の電源ケーブルは安全のために3ピンタイプのプラグを使用しています。電源コンセントの形状が異なりプラグを接続できない場合には電気事業者に問い合わせて適切に処置してください。アース極を無理に使用できない状態にしないでください。使用する国/地域の電源形状に従ってください。
- 電源コード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コードを設置してください。
- 電源の延長コードや電源タップを使用する場合は、合計容量とコードまたはタップの仕様が適合しているかを確認してください。電源コンセントにつながれている製品全ての合計アンペア数は15アンペアを超えないようにしてください。
- 突然の供給電力不安定や電力過剰・電力不足からお使いのシステムを守るために、サージサプレッサー、ラインコンディショナー、または無停電電源装置(UPS)をご使用ください。
- 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。ケーブル類の上には何も置かないようにしてください。
- ホットプラグ対応パワーサプライの取り付け、または取り外しする場合は、以下の注意事項に従ってください。
  - 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してください。
  - 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全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。
- 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。
- 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。全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。

◆ 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。

- 電源コードが破損した。
- 装置の上に液体をこぼした。
- 装置が雨や水にぬれた。
- 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ある。(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。

DC電源

- この製品は、短絡、過電流、およびアース（接地）障害に対する保護として、建物設備内の保護装置に依存しています。建物に設置している保護装置がシステムを保護するために適切に定格しており、国および地方自治体の規定に準拠しているかを確認してください。
- 建物の設置配線に、すぐにアクセスできる切断装置が組み込まれているかを確認してください。
- この製品には別個の保護接地端子を設けています。製品使用時は常に接地している状態にしておいてください。
- DC電源回路には、UL、AWM VW-1 Style 1015、最小16AWG、最小105℃、最小300Vで認定DC電源ケーブルを選定してください。
- **注意**:この装置は、DC 電源回路の接地導体を装置の接地導体に接続できるように設計しています。アース接続をする場合は、以下の条件を全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し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、他の場所に接地しないでください。
  - DC電源は、本製品と同じ構内に設置する必要があります。
  - 装置の切り替えや切断は、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しないでください。
- **警告**:この製品は、アクセスが制限されている場所への設置を想定しています。立入制限区域(サーバールーム、データセンターなど)とは、アクセスが、特別なツール、ロックおよびキー、またはその他のセキュリティー手段を使用してサービス担当者のみが訪問でき、その場所を担当する機関によって管理する場所を指します。

ラックへのマウント

- ラックでの作業を始める前に、スタビライザーをラックに固定した床に接し、ラック全体が安定した場所に置かれているか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、結合し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か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。
- デバイスをラックに挿入したら、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。
- ラックにマウントしたデバイスは、電源タップを含め、全て正しく接地しているか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。
- 本製品で定めている保管温度を超えないように、ラックが設置している場所の室温を調節してください。
- ラックに設置し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

SN1116CO/SN1132CO/SN1148CO

機能		SN1116CO	SN1132CO	SN1148CO
シリアル接続		16	32	48
コネクター	シリアル	RJ-45 メス×16	RJ-45 メス×32	RJ-45 メス×48
	LAN	SFPスロット×2		
	電源	IEC60320/C14×2		
	ローカルコンソール	RJ-45 メス×1		
	PON	RJ-45 メス×1(予約済み)		
	ラップトップUSB コンソール(LUC)ポート	Mini USB×1		
	USBポート	USB Type-A メス×4		
	環境センサーポート	RJ-11 メス×2 4ピン ターミナルブロック×1		
	リレー	2ピン ターミナルブロック×1 *ノーマルオープン、絶縁リレー: *接点定格: 最大DC24V, 2A		
スイッチ	リセット	ピンホール型スイッチ×1		
	電源	ロッカースイッチ×2		
LED	シリアルポートの状態	16(Green)	32(Green)	48(Green)
	10 / 100 / 1000 Mbps	2(Red / Orange / Green)		
	電源	2(Blue)		
電源仕様	AC	100～240 VAC、50/60Hz、1.0A		
消費電力		AC110V:9.2W:96BTU AC220V:9.2W:96BTU	AC110V:11.2W:105BTU AC220V:11.3W:105BTU	AC110V:11.8W:108BTU AC220V:12W:109BTU
動作モード		コンソール管理、コンソール管理ダイレクト、リアルCOMポート、 TCPサーバー/クライアント、UDPサーバー/クライアント、バーチャルモデム		
動作環境	動作温度	0～55℃		
	保管温度	-20～60℃		
	湿度	0～80% RH、結露なきこと		
ケース	ケース材料	メタル		
	重量	4.51kg (9.93 ポンド)	4.60kg (10.13 ポンド)	4.67kg (10.29 ポンド)
	サイズ(W×D×H)	43.84×32.84×4.40cm(17.26×12.93×1.73 インチ)		

SN1116COD/SN1132COD/SN1148COD

機能		SN1116COD	SN1132COD	SN1148COD
シリアル接続		16	32	48
コネクター	シリアル	RJ-45 メス×16	RJ-45 メス×32	RJ-45 メス×48
	LAN	SFPスロット×2		
	電源	5ピン ターミナルブロック×1(Green)		
	ローカルコンソール	RJ-45 メス×1		
	PON	RJ-45 メス×1(予約済み)		
	ラップトップUSB コンソール(LUC)ポート	Mini USB×1		
	USBポート	USB Type-A メス×4		
	環境センサーポート	RJ-11 メス×2 4ピン ターミナルブロック×1		
	リレー	2ピン ターミナルブロック×1 *ノーマルオープン、絶縁リレー: *接点定格: 最大DC24V, 2A		
スイッチ	リセット	ピンホール型スイッチ×1		
	電源	ロッカースイッチ×2		
LED	シリアルポートの状態	16(Green)	32(Green)	48(Green)
	10 / 100 / 1000 Mbps	2(Red / Orange / Green)		
	電源	2(Blue)		
電源仕様	AC	100～240 VAC、50/60Hz、1.0A		
消費電力		DC 48V:9.3W	DC 48V:11.3W	DC 48V:12W
動作モード		コンソール管理、コンソール管理ダイレクト、リアルCOMポート、 TCPサーバー/クライアント、UDPサーバー/クライアント、バーチャルモデム		
動作環境	動作温度	0～55℃		
	保管温度	-20～60℃		
	湿度	0～80% RH、結露なきこと		
ケース	ケース材料	メタル		
	重量	4.51kg (9.93 ポンド)	4.60kg (10.13 ポンド)	4.67kg (10.29 ポンド)
	サイズ(W×D×H)	43.84×32.84×4.40cm(17.26×12.93×1.73 インチ)		

SN0108CO/SN0116CO (AXAプラットフォーム)

機能		SN0108CO	SN0116CO
シリアル接続		8	16
コネクター	シリアル	RJ-45 メス×8	RJ-45 メス×16
	LAN	RJ-45×2	
	電源	IEC 60320/C14×2	
	PON	RJ-45 メス×1(予約済み)	
	モデム	RJ-45 メス×1	
	USB	USB Type-A メス×3	
	USBコンソール(LUC)	Mini USB×1	
	ローカルコンソール	RJ-45 メス×1	
スイッチ	リセット	ピンホール型スイッチ×1	
	電源	ロッカースイッチ×2	
LED	シリアルポートの状態	8(Green)	16(Green)
	10 / 100 / 1000 Mbps	2(Red / Orange / Green)	
	電源	2(Blue)	
電源仕様	AC	100-240 V～; 50/60Hz; 1A	
消費電力		AC 110V:5.3W AC 220V:5.2W	AC 110V:5.5W AC 220V:5.5W
動作モード		コンソール管理、コンソール管理ダイレクト、リアルCOMポート、 TCPサーバー/クライアント、UDPサーバー/クライアント、 バーチャルモデム	
動作環境	動作温度	0～40℃	
	保管温度	-20～60℃	
	湿度	0～80% RH、結露なきこと	
ケース	ケース材料	メタル	
	重量	4.35 kg	4.38 kg
	サイズ(W×D×H)	43.72×32.98×4.40cm (19インチ1U)	43.72×32.98×4.40cm (19インチ1U)

SN0108CO/SN0116CO (AXプラットフォーム)

機能		SN0108CO	SN0116CO
シリアル接続		8	16
コネクター	シリアル	RJ-45 メス×8	RJ-45 メス×16
	LAN	RJ-45×2	
	電源	IEC 60320/C14×2	
	PON	RJ-45 メス×1(予約済み)	
	モデム	RJ-45 メス×1	
	USB	USB Type-A メス×3	
	USBコンソール(LUC)	Mini USB×1	
	ローカルコンソール	RJ-45 メス×1	
スイッチ	リセット	ピンホール型スイッチ×1	
	電源	ロッカースイッチ×2	
LED	シリアルポートの状態	8(Green)	16(Green)
	10 / 100 / 1000 Mbps	2(Red / Orange / Green)	
	電源	2(Blue)	
電源仕様	AC	100-240 V～; 50/60Hz; 1A	
消費電力		110V/14.1W 220V/14W	110V/15.4W 220V/14.9W
動作モード		コンソール管理、コンソール管理ダイレクト、リアルCOMポート、 TCPサーバー/クライアント、UDPサーバー/クライアント、バーチャルモデム	
動作環境	動作温度	0～40℃	
	保管温度	-20～60℃	
	湿度	0～80% RH、結露なきこと	
ケース	ケース材料	メタル	
	重量	4.45 kg	4.48 kg
	サイズ(W×D×H)	43.72×32.98×4.40cm (19インチ1U)	43.72×32.98×4.40cm (19インチ1U)

SN0108COD/SN0116COD (AXAプラットフォーム)

機能		SN0108COD	SN0116COD
シリアル接続		8	16
コネクター	シリアル	RJ-45 メス×8	RJ-45 メス×16
	LAN	RJ-45×2	
	電源	5ピン ターミナルブロック×1(Green)	
	PON	RJ-45 メス×1(予約済み)	
	モデム	RJ-45 メス×1	
	USB	USB Type-A メス×3	
	USBコンソール(LUC)	Mini USB×1	
	ローカルコンソール	RJ-45 メス×1	
スイッチ	リセット	ピンホール型スイッチ×1	
	電源	ロッカースイッチ×2	
LED	シリアルポートの状態	8(Green)	16(Green)
	10 / 100 / 1000 Mbps	2(Red / Orange / Green)	
	電源	2(Blue)	
電源仕様	DC	36-48 V DC、5ピン ターミナルブロックで1.6 A	
消費電力		DC 48V:5.3W	DC 48V:5.5W
動作モード		コンソール管理、コンソール管理ダイレクト、リアルCOMポート、TCPサーバー/クライアント、UDPサーバー/クライアント、バーチャルモデム	
動作環境	動作温度	0～40℃	
	保管温度	-20～60℃	
	湿度	0～80% RH、結露なきこと	
ケース	ケース材料	メタル	
	重量	4.55 kg	4.59 kg
	サイズ(W×D×H)	43.72×32.85×4.40 cm	

SN0108COD/SN0116COD (AXプラットフォーム)

機能		SN0108COD	SN0116COD
シリアル接続		8	16
コネクター	シリアル	RJ-45 メス×8	RJ-45 メス×16
	LAN	RJ-45×2	
	電源	5ピン ターミナルブロック×1(Green)	
	PON	RJ-45 メス×1(予約済み)	
	モデム	RJ-45 メス×1	
	USB	USB Type-A メス×3	
	USBコンソール(LUC)	Mini USB×1	
	ローカルコンソール	RJ-45 メス×1	
スイッチ	リセット	ピンホール型スイッチ×1	
	電源	ロッカースイッチ×2	
LED	シリアルポートの状態	8(Green)	16(Green)
	10 / 100 / 1000 Mbps	2(Red / Orange / Green)	
	電源	2(Blue)	
電源仕様	DC	36-48 V DC、5ピン ターミナルブロックで1.6 A	
消費電力		DC 48V:15.79W	DC48V:16.22W
動作モード		コンソール管理、コンソール管理ダイレクト、リアルCOMポート、 TCPサーバー/クライアント、UDPサーバー/クライアント、バーチャルモデム	
動作環境	動作温度	0～40℃	
	保管温度	-20～60℃	
	湿度	0～80% RH、結露なきこと	
ケース	ケース材料	メタル	
	重量	4.46 kg	4.5 kg
	サイズ(W×D×H)	43.72×32.85×4.40 cm	

SN0132CO/SN0148CO (AXAプラットフォーム)

機能		SN0132CO	SN0148CO
シリアル接続		32	48
コネクター	シリアル	RJ-45 メス×32	RJ-45 メス×48
	LAN	RJ-45×2	
	電源	IEC 60320/C14×2	
	PON	RJ-45 メス×1(予約済み)	
	モデム	RJ-45 メス×1	
	USB	USB Type-A メス×3	
	USBコンソール(LUC)	Mini USB×1	
	ローカルコンソール	RJ-45 メス×1	
スイッチ	リセット	ピンホール型スイッチ×1	
	電源	ロッカースイッチ×2	
LED	シリアルポートの状態	32(Green)	48(Green)
	10 / 100 / 1000 Mbps	2(Red / Orange / Green)	
	電源	2(Blue)	
電源仕様	AC	100-240 V～、50/60Hz、1.8A	
消費電力		AC 110V:9.8W AC 220V:9.7W	AC 110V:10.3W AC 220V:10.2W
動作モード		コンソール管理、コンソール管理ダイレクト、リアルCOMポート、 TCPサーバー/クライアント、UDPサーバー/クライアント、バーチャルモデム	
動作環境	動作温度	0～40℃	
	保管温度	-20～60℃	
	湿度	0～80% RH、結露なきこと	
ケース	ケース材料	メタル	
	重量	4.55 kg	4.61 kg
	サイズ(W×D×H)	43.84×32.77×4.40 cm	

SN0132CO/SN0148CO (AXプラットフォーム)

機能		SN0132CO	SN0148CO
シリアル接続		32	48
コネクター	シリアル	RJ-45 メス×32	RJ-45 メス×48
	LAN	RJ-45×2	
	電源	IEC 60320/C14×2	
	PON	RJ-45 メス×1(予約済み)	
	モデム	RJ-45 メス×1	
	USB	USB Type-A メス×3	
	USBコンソール(LUC)	Mini USB×1	
	ローカルコンソール	RJ-45 メス×1	
スイッチ	リセット	ピンホール型スイッチ×1	
	電源	ロッカースイッチ×2	
LED	シリアルポートの状態	32(Green)	48(Green)
	10 / 100 / 1000 Mbps	2(Red / Orange / Green)	
	電源	2(Blue)	
電源仕様	AC	100-240 V~; 50/60Hz; 1.8A	
消費電力		110V/20.2W 220V/21W	110V/25.8W 220V/26.2W
動作モード		コンソール管理、コンソール管理ダイレクト、リアルCOMポート、 TCPサーバー/クライアント、UDPサーバー/クライアント、バーチャルモデム	
動作環境	動作温度	0～40℃	
	保管温度	-20～60℃	
	湿度	0～80% RH、結露なきこと	
ケース	ケース材料	メタル	
	重量	4.84 kg	4.92 kg
	サイズ(W×D×H)	43.84×32.77×4.40 cm	

SN0132COD/SN0148COD (AXAプラットフォーム)

機能		SN0132COD	SN0148COD
シリアル接続		32	48
コネクター	シリアル	RJ-45 メス×32 (Black)	RJ-45 メス×48 (Black)
	LAN	RJ-45×2(Black)	
	電源	5ピン ターミナルブロック×1(Green)	
	PON	RJ-45 メス×1(予約済み)	
	モデム	RJ-45 メス×1	
	USB	USB Type-A メス×3	
	USBコンソール(LUC)	Mini USB×1	
	ローカルコンソール	RJ-45 メス×1	
スイッチ	リセット	ピンホール型スイッチ×1	
	電源	ロッカースイッチ×2	
LED	シリアルポートの状態	32(Green)	48(Green)
	10 / 100 / 1000 Mbps	2(Red / Orange / Green)	
	電源	2(Blue)	
電源仕様	DC	36-48 V DC、5ピン ターミナルブロックで1.6 A	
消費電力		DC 48V:9.8W	DC 48V:10.3W
動作モード		コンソール管理、コンソール管理ダイレクト、リアルCOMポート、 TCPサーバー/クライアント、UDPサーバー/クライアント、バーチャルモデム	
動作環境	動作温度	0～40℃	
	保管温度	-20～60℃	
	湿度	0～80% RH、結露なきこと	
ケース	ケース材料	メタル	
	重量	4.83 kg	4.89 kg
	サイズ(W×D×H)	43.84×32.77×4.40 cm	

SN0132COD/SN0148COD (AXプラットフォーム)

機能		SN0132COD	SN0148COD
シリアル接続		32	48
コネクター	シリアル	RJ-45 メス×32 (Black)	RJ-45 メス×48 (Black)
	LAN	RJ-45×2(Black)	
	電源	5ピン ターミナルブロック×1(Green)	
	PON	RJ-45 メス×1(予約済み)	
	モデム	RJ-45 メス×1	
	USB	USB Type-A メス×3	
	USBコンソール(LUC)	Mini USB×1	
	ローカルコンソール	RJ-45 メス×1	
スイッチ	リセット	ピンホール型スイッチ×1	
	電源	ロッカースイッチ×2	
LED	シリアルポートの状態	32(Green)	48(Green)
	10 / 100 / 1000 Mbps	2(Red / Orange / Green)	
	電源	2(Blue)	
電源仕様	DC	36-48 V DC、5ピン ターミナルブロックで1.6 A	
消費電力		DC 48V:22.1W	DC 48V:27.3W
動作モード		コンソール管理、コンソール管理ダイレクト、リアルCOMポート、 TCPサーバー/クライアント、UDPサーバー/クライアント、バーチャルモデム	
動作環境	動作温度	0～40℃	
	保管温度	-20～60℃	
	湿度	0～80% RH、結露なきこと	
ケース	ケース材料	メタル	
	重量	4.99 kg	5.06 kg
	サイズ(W×D×H)	43.84×32.77×4.40 cm	

SN9108CO/SN9116CO (AXAプラットフォーム)

機能		SN9108CO	SN9116CO
シリアル接続		8	16
コネクター	シリアル	RJ-45 メス×8	RJ-45 メス×16
	LAN	RJ-45×1	
	電源	IEC60320/C14×1	
スイッチ	リセット	ピンホール型スイッチ×1	
	電源	ロッカースイッチ×1	
LED	シリアルポートの状態	8(Green)	16(Green)
	10 / 100 / 1000 Mbps	1(Red / Orange / Green)	
	電源	1(Blue)	
電源仕様	AC	100-240 V～、50/60Hz、1A	
消費電力		AC 110V:9.7W AC 220V:9.6W	AC 110V:10.9W AC 220V:11.6W
動作モード		コンソール管理、コンソール管理ダイレクト、リアルCOMポート、 TCPサーバー/クライアント、UDPサーバー/クライアント、バーチャルモデム	
動作環境	動作温度	0～40℃	
	保管温度	-20～60℃	
	湿度	0～80% RH、結露なきこと	
ケース	ケース材料	メタル	
	重量	3.12 kg	3.16 kg
	サイズ(W×D×H)	43.72×21.76×4.40cm (19インチ1U)	43.72×21.76×4.40cm (19インチ1U)

SN9108CO/SN9116CO (AXプラットフォーム)

機能		SN9108CO	SN9116CO
シリアル接続		8	16
コネクター	シリアル	RJ-45 メス×8	RJ-45 メス×16
	LAN	RJ-45×1	
	電源	IEC60320/C14×1	
スイッチ	リセット	ピンホール型スイッチ×1	
	電源	ロッカースイッチ×1	
LED	シリアルポートの状態	8(Green)	16(Green)
	10 / 100 / 1000 Mbps	1(Red / Orange / Green)	
	電源	1(Blue)	
電源仕様	AC	100-240 V～、50/60Hz、1A	
消費電力		AC 110V:9.7W AC 220V:9.6W	AC 110V:10.9W AC 220V:11.6W
動作モード		コンソール管理、コンソール管理ダイレクト、リアルCOMポート、 TCPサーバー/クライアント、UDPサーバー/クライアント、バーチャルモデム	
動作環境	動作温度	0～40℃	
	保管温度	-20～60℃	
	湿度	0～80% RH、結露なきこと	
ケース	ケース材料	メタル	
	重量	3.12 kg	3.16 kg
	サイズ(W×D×H)	43.72×21.76×4.40cm (19インチ1U)	43.72×21.76×4.40cm (19インチ1U)

IPアドレスの設定

管理者として最初にログインした場合には、他のユーザーがTCP/IPネットワーク経由でログインできるように、シリアルコンソールサーバーに対してIPアドレスを設定する必要があります。設定方法は全部で3種類ありますが、どの方法でも設定に使用するコンピューターはシリアルコンソールサーバーと同一のネットワークセグメントにセットアップしていなければなりません。シリアルコンソールサーバーに接続しログインすると、シリアルコンソールサーバーに固定IPアドレスを設定できます(p.122「ネットワーク」参照)

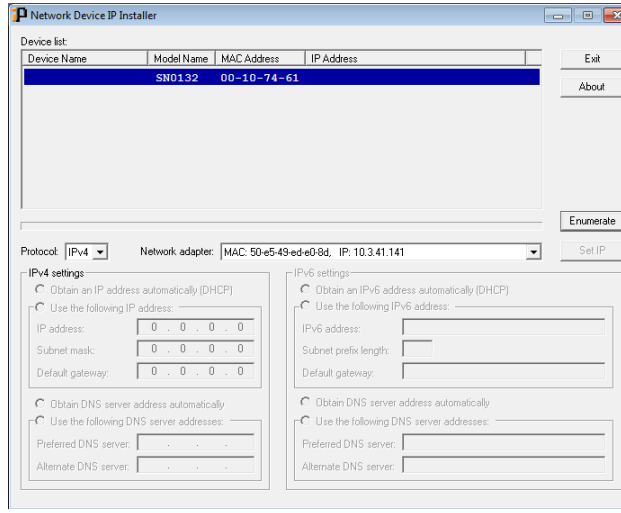
ローカルコンソール

最も簡単なIPアドレスの設定方法はローカルコンソールから設定する方法です。関連する手順の詳細については、p.44「初期設定」を参照してください。

IPインストーラー

Windowsをインストールしたコンピューターをお使いの場合は、IPインストーラーというツールを使用してIPアドレスを設定できます。IPインストーラーは弊社ウェブサイトのダウンロードページからダウンロードできます。ダウンロード画面の「ドライバー＆ソフトウェア」のリストから、お使いのシリアルコンソールサーバーの型番を選択してください。IPインストーラーをお使いのコンピューターにダウンロードしたら、以下の手順に従ってIPアドレスを設定してください。

1. ダウンロードしたファイル「IPInstaller.zip」をお使いのコンピューター上の適当なフォルダーに解凍してください。
2. 手順1でIPインストーラーを解凍したフォルダーに移動し、IPインストーラーの実行ファイル(IPInstaller.exe)を起動してください。
   以下のようなダイアログボックスが表示されます。



3. 「デバイス一覧」からシリアルコンソールサーバーを選択してください。

注意:

1. リストに何も表示されない、また、対象となるユニットが表示しない場合は、「**一覧表示**」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必要なデバイスを選択します。製品のMACアドレスは本体底面に貼っているラベルに記載しています。

---

4. DHCPを使ってIPアドレスを自動的に取得する場合は「IPアドレスを自動取得する」を、固定IPアドレスを設定する場合は「IPアドレスを指定する」をそれぞれ選択してください。後者を選択した場合は、製品をセットアップしているネットワークで有効なIPアドレス、サブネットマスク、ゲートウェイをそれぞれ該当欄に入力してください。

5. 「**IPを設定**」ボタンをクリックしてください。

6. IPアドレスが「デバイス一覧」に表示したら、「**終了**」ボタンをクリックしてください。IPインストーラーについての詳細はp.122を参照してください。

ブラウザー

1. クライアントコンピューターのIPアドレスを「192.168.0.XXX」に設定してください。「XXX」の部分には、1～255の範囲の任意の整数値を使用してください。ただし、60はシリアルコンソールサーバーのデフォルトのIPアドレス(192.168.0.60)に使用していますので、この値以外を使用してください。
2. ウェブブラウザーのアドレスバーに、シリアルコンソールサーバーのデフォルトIPアドレス(192.168.0.60)を指定すると、接続できるようになります。
3. シリアルコンソールサーバーをセットアップしているネットワークで有効な固定IPアドレスを設定してください。
4. ログアウトしたら、手順1で設定を変更したコンピューターのIPアドレスを元の値に戻しておいてください。

IPv6

現在、シリアルコンソールサーバーでは、IPv6の「リンクローカルアドレス」と「ステートレス自動設定」、「ステートフル自動設定(DHCPv6)」の3種類に対応しています。

リンクローカルIPv6アドレス

シリアルコンソールサーバーに電源を入れると、自動的にIPv6のリンクローカルアドレスが設定します(例:fe80::210:74ff:fe61:1ef)。このリンクローカルアドレスの内容を確認する場合は、シリアルコンソールサーバーにIPv4のアドレスでログインし、「デバイス管理」>「デバイス情報」メニューを開いてください。アドレスが「全般」リスト(p.117参照)に表示されます。

IPv6アドレスの内容が確定すると、ブラウザーやWindows、Javaの各クライアントソフトウェアからログインする際にこのアドレスを使えます。

次に例を示します。

ブラウザーからログインする場合には、URLバーにアドレスをこのように入力してください。

http://[fe80:2001:74ff:fe6e:59%5]

また、クライアントソフトウェアからログインする場合には、「サーバー」パネルの「IP」

欄にアドレスを次のように入力します（p.48「リモートログイン」参照）。

fe80: 2001:74ff:fe6e:59%5

注意：

1. Link Local IPv6 Address でログインするには、クライアントコンピューターがシリアルコンソールサーバーと同じローカルネットワークセグメントに存在する必要があります。
2. 「%5」は、クライアントコンピューターで使用する「%interface」です。クライアントコンピューターのIPv6アドレスを確認する場合は、コマンドラインから下記のコマンドを実行してください。ipconfig /all「%」値はIPv6アドレスの最後に現れます。

IPv6ステートレス自動設定

シリアルコンソールサーバーをセットアップしているネットワーク環境で、IPv6ステートレス自動設定機能に対応したデバイス(例：ルーター)を使用している場合、製品はIPv6アドレスを生成するために、このデバイスからプレフィックス情報を取得できます。例えば、「2001::74ff:fe6e:59」です。

先に述べたように、アドレスは「デバイス管理」＞「デバイス情報」メニューの「全般」リスト（p.117参照）に表示されます。

IPv6アドレスの内容が確定すると、ブラウザーやWindows、Javaの各クライアントソフトウェアからログインする際にこのアドレスを使えます。

次に例を示します。

ブラウザーからログインする場合には、URLバーにアドレスをこのように入力してください。

http://[2001:74ff:fe6e:59]

また、クライアントソフトウェアからログインする場合には、「サーバー」パネルの「IP」欄にアドレスを次のように入力します。

2001:74ff:fe6e:59

バーチャルモデムの詳細

シリアルコンソールのバーチャルモデム機能は、ハードウェアモデムをエミュレートして、TCP/IPを使ってイーサネットLANまたはWAN上で高速なシリアルモデム機能を実現できるため、電話回線を使ったモデム通信による通信速度や信頼性の問題を解消できます。

サポートするATコマンド

シリアルコンソールサーバーは、下表に示すように、Hayes標準コマンドセットのサブセット、および拡張したコマンドの一部をサポートします。

コマンド	操作方法	レスポンス
+++	コマンドモードに戻ります。エスケープコードはS2レジスターによって変更できます。	なし
A/	最後に実行したコマンドを再実行します。	成功した場合：OK[CR][LF] 失敗した場合：ERROR[CR][LF]
ATA[CR]	アンサーモードです。バーチャルモデムが提供された待機ポート5301でTCP 接続を待機できるようにします。	成功した場合：OK[CR][LF] 失敗した場合：ERROR[CR][LF]
ATD(T) リモートIP:リモートポート[CR]	TCP接続の確立を試み、特定のリモートホストに接続します。 例：ATDT10.0.0.72:50001 **注意：**ATDコマンドの後ろに**T**や**P**をつけて入力してもエラーにはなりませんが、無視されます。	成功した場合：CONNECT[CR][LF] 接続に失敗した場合： NO CARRIER[CR][CF] その他のエラーが発生した場合： ERROR[CR][LF]
ATE*n*[CR]	*n* は数値文字(0 または1) を表します。 E0：コマンドエコーを無効にします。 E1：echoコマンドを有効にします。	成功した場合：OK[CR][LF] 失敗した場合：ERROR[CR][LF]
ATH[CR]	接続がアクティブである場合に現在のTCP接続を切断します。 **注意：**ATH、ATH0、ATH1 は全て同じく動作します。	成功した場合：OK[CR][LF] 失敗した場合：ERROR[CR][LF]
ATI*n*[CR]	問い合わせコマンドです。(*n* は数値文字を表します。0 または1です。) E0：ATEN International Co.Ltdを表示します。 E1：シリアルコンソールサーバーを表示します。	成功した場合：OK[CR][LF] 失敗した場合：ERROR[CR][LF]
ATO*n*[CR]	オンラインデータモードに戻ります。(*n*の部分には0または1の数字を入力します。) モデムがオンラインコマンドモードの場合、このコマンドによりオンラインデータモードになります。モデムがオフラインコマンドモード(TCP接続が確立されていない)の場合は、ERRORが返ってきます。 O0, O1：アクティブな接続がある場合は、モデムをデータモードに切り替えます。	TCP接続がアクティブである場合： OK[CR][LF] それ以外の場合：ERROR[CR][LF]

コマンド	操作方法	レスポンス
ATQ*n*[CR]	リザルトコード制御コマンドです（*n* の部分には0または1の数字を入力します）。 Q0：DTEへのリザルトコード有効(デフォルト値) Q1：DTEへのリザルトコード無効	成功した場合：OK[CR][LF] 失敗した場合：ERROR[CR][LF]
ATS*n*?[CR]	Sレジスターの値を報告します（*n* の部分にはレジスターの番号を入力します）。	成功した場合：OK[CR][LF] 失敗した場合：ERROR[CR][LF]
ATSn=v[CR]	Sレジスターの値を設定します（*n* の部分にはレジスターの番号を、*v* の部分にはSレジスターの値をそれぞれ入力します）。	成功した場合：OK[CR][LF] 失敗した場合：ERROR[CR][LF]
ATV*n*[CR]	リザルトコードを返す際の形式を設定します（*n* の部分には0または1の数字を入力します）。 V0：レスポンスは<番号形式>[CR][LF] V1：レスポンスは<言葉による説明>[CR][LF]	成功した場合：OK[CR][LF] 失敗した場合：ERROR[CR][LF]
ATZ[CR]	モデムコマンドをリセットします。 アクティブな接続を終了し、Sレジスターおよび汎用オプションのステータスを、保存している値にリセットします。	成功した場合：OK[CR][LF] 失敗した場合：ERROR[CR][LF]
AT&Cn[CR]	DCDオプションです（*n* の部分には0または1の数字を入力します）。 &C0：DCDは常にオンです。 &C1：DCDはTCP接続の状態と一致します。	成功した場合：OK[CR][LF] 失敗した場合：ERROR[CR][LF]
AT&D*n*[CR]	DTRオプションです（*n* の部分には0～3の数字を入力します）。 &D0： DTRはオンであるものと見なし、モデムはDTRラインを無視します。 &D1： DTR OFFは、通信を切断せずモデムをコマンドモードに切り替えます。 &D2： DTR OFFは、モデムをコマンドモードに切り替え、通信を中断し、自動応答機能を無効にします（デフォルト）。 &D3： DTR OFFはモデムを初期化します。	成功した場合：OK[CR][LF] 失敗した場合：ERROR[CR][LF]
AT&F[CR]	工場出荷時の設定に戻します。 Sレジスターおよび汎用オプションのステータスを、デフォルト値にリセットします。	成功した場合：OK[CR][LF] 失敗した場合：ERROR[CR][LF]
AT&W[CR]	設定を保存します。 Sレジスターおよび汎用オプションのステータスを含む現在の設定内容を、メモリーに書き込みます。	成功した場合：OK[CR][LF] 失敗した場合：ERROR[CR][LF]
ATB[CR]	なし	OK[CR][LF]
ATC[CR]	なし	OK[CR][LF]
ATL[CR]	なし	OK[CR][LF]
ATM[CR]	なし	OK[CR][LF]

コマンド	操作方法	レスポンス
ATN[CR]	なし	OK[CR][LF]
ATX[CR]	なし	OK[CR][LF]
ATY[CR]	なし	OK[CR][LF]
ATW[CR]	なし	OK[CR][LF]
その他の ATコマンド	なし	OK[CR][LF]

ポート転送

デバイスをルーターの内側にセットアップしている場合、特定のポート経由で特定のデバイス宛に送信したデータをルーターが転送できるように、ルーター側でポート転送の設定をする必要があります。ポート転送のパラメーターを設定して特定のポートに送信したデータをどのデバイスに転送すればよいのかを、ルーターに判別できます。

例えば、特定のルーターに接続したシリアルコンソールサーバーに「192.168.1.180」というIPアドレスが設定している場合、ルーターの設定プログラムにログインした後、ポート転送(場合によってはバーチャルサーバー)の設定画面にアクセスし、先ほどのIPアドレス「192.168.1.180」および開放したいポート(例えばインターネットアクセスでは9000番を使用)を設定します。

ルーターごとに設定方法は異なりますので、ポート転送の詳細についてはお使いのルーターのユーザーマニュアルを参照してください。

距離とボーレートの関係

シリアルポートは各ボーレートをサポートし、シリアルポート接続の距離を決定します。

以下の表を参照してください。

ボーレート	距離
300	90m
9600 (デフォルト)	30m
115200	3m
230400	1.5m

ログイン情報の消去

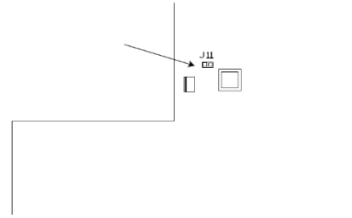
アドミニストレーターがユーザーネームやパスワードを間違えたり、または忘れてしまったりして、アドミニストレーターとしてログインできなくなった場合、下記の作業にてログイン情報を消去できます。

注意:

この作業をすると、全ての設定内容がデフォルト値に戻ります。

ログイン情報を消去する(全ての設定内容をデフォルト値に戻す)場合は、次の手順で作業をしてください。

1. シリアルコンソールサーバー本体の電源を切り、ケースを取り外してください。
2. ジャンパーキャップを使用して、SN0132/SN0148/SN1132/SN1148の場合はメインボードの「**J11/J18**」と書かれた場所(下図参照)を、SN9108/SN9116/SN0108/SN0116/SN1116の場合は「**J17/J18**」と書かれた場所を、それぞれショートさせてください。



3. シリアルコンソールサーバーの電源を入れてください。
4. ビープ音が鳴り始めたら、シリアルコンソールサーバーの電源を切ります。
5. 「**J11/J18**」(SN0132/SN0148/SN1132/SN1148の場合)または「**J17/J18**」(SN9108/SN9116/SN0108/SN0116/SN1116の場合)からジャンパーキャップを外してください。
6. ケースを元に戻し、シリアルコンソールサーバーに電源を入れてください。

   ユニットの電源を入れた後、デフォルトのスーパーアドミニストレーターのユーザーネームとパスワード(p.44「初期設定」を参照)を使用してログインできます。

   この手順を実行した後、初めてログインするときにパスワードの変更を強制します。

ピン配列

シリアルコンソールサーバーには、Ciscoネットワークスイッチやその他の互換性のあるデバイスに直接接続するためのDTE/DCE自動検出機能があります。

各種モードにおけるシリアルポートのピン配列を以下に示します。

DCEモードのピン配列

ピン	定義
1	CTS
2	DSR
3	RxD
4	GND
5	GND
6	TxD
7	DTR
8	RTS

DTEモードのピン配列

ピン	定義
1	RTS
2	DTR
3	TxD
4	GND
5	GND
6	RxD
7	DSR
8	CTS

DB-9/DB-25インターフェース

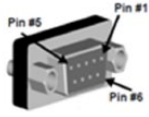
DB-9またはDB-25インターフェースを使用する場合は、以下の表を参照してください。

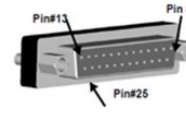
DB-9

RJ-45ピン	信号	DB-9Fピン	信号
1	CTS	7	RTS
2	DSR	4	DTR
5	GND		
3	RxD	3	TxD
4	GND	5	GND
6	TxD	2	RxD
7	DTR	1	GND
		6	DSR
8	RTS	8	CTS

DB-25

RJ-45ピン	信号	DB-25Fピン	信号
1	CTS	4	RTS
2	DSR	20	DTR
5	GND		
3	RxD	2	TxD
4	GND	7	GND
6	TxD	3	RxD
7	DTR	6	GND
		8	DSR
8	RTS	5	CTS





自己署名SSL/TLS証明書

プライベートに信頼されるSSL/TLS 証明書は、**内部**ネットワーク内のユーザーとデバイスの認証のみに使用してください。

1. SNデバイスのウェブブラウザーで、「**メンテナンス**」>「**プライベート証明書**」に移動します。
2. プライベート証明書 ページの下部から「**CSRを取得**」をクリックします。
「custom.csr」というファイルを取得します。

3. 「openssl.exe」を使用して、次のコマンドで「new.cer」ファイルを生成します。
   - openssl req –new –newkey rsa:2048 –days 3653 –nodes –x509 – keyout ca.key –out ca.cer
   - openssl ca –policy policy_anything –config openssl.cnf –cert ca.cer –in *custom.csr –keyfile ca.key –days 360 –out new.cer*
4. 「**インポート**」をクリックして、「new.cer」ファイルをSNデバイスにインポートします。

CLIコマンド

CLIコマンドは、基本設定と制御をするにあたり、TelnetまたはSSHを介してシリアルコンソールサーバーにアクセスする際に、CLIモードで使用します。

システム設定コマンド

set hostname=<host_name>

例:

set hostname=SN9108CO

説明:

「SN9108CO」をシリアルコンソールサーバーのホスト名またはデバイス名として設定します。

read sysinfo

例:

read sysinfo

説明:

システム情報を表示します。

reboot

例:

reboot

説明:

システムを再起動します。

read log

例:

read log

説明:

システムログを表示します。

quit

例:

quit

説明:

システムをログアウトします。

help

例:

help

説明:

「SN9108CO」をシリアルコンソールサーバーのホスト名またはデバイス名として設定します。

menu on

例:

menu on

説明:

メニュー駆動モードに切り替えます。

set logintimeout=<timeout_minutes>

例:

set logintimeout=1

説明:

ログインタイムアウトを1分に設定します。

タイムアウト値<timeout_minutes> を0～180分の範囲で指定します。値が0の場合はタイムアウトしません。

set securitylevel=<1/2/3>

例:

set securitylevel=1

説明:

セキュリティーレベルを1に設定します。

使用可能なセキュリティーレベルは以下のとおりです。

- ◆ 1 = 高
  SSHv2 およびHTTPS(TLS v1.2)以外の全てのサービスを無効にします。
- ◆ 2 = 中-高
  SSHv2を有効にし、HTTPからHTTPS、HTTPS (TLS v1.2)、またはICMPにリダイレクトします。
- ◆ 3 = 中
  SSHv2を有効にし、HTTPからHTTPS、HTTPS (TLS v1.0、1.1、1.2)、SNMPエージェント、またはICMPにリダイレクトします。

ネットワーク設定コマンド

CLIコマンドを使用してネットワーク設定を構成するには、CLIコマンドでネットワークインターフェース名を示すパラメーターを使用して設定を指定できます。

- ◆ **eth0**:LANポート1
- ◆ **eth1**:LANポート2
- ◆ **bond:** eth0とeth1は冗長です

netconfig

例:

netconfig

説明:

IPv4およびIPv6ネットワーク設定とサービスポートを表示します。

netconfig if <eth0/eth1/bond> <v4/v6> ip <IP_address> nm<subnet_mask> gw <gateway_address>

例:

netconfig if eth0 v4 ip 192.168.1.1 nm 255.255.255.0 gw 192.168.1.255

説明:

以下を設定します。

- ◆ LANポート1のIPアドレス:192.168.1.1
- ◆ サブネットマスク:255.255.255.0
- ◆ ゲートウェイアドレス:192.168.1.255

netconfig if <eth0/eth1/bond> <dhcp/dhcpv6>

例:

netconfig if eth0 dhcp

説明:

DHCP経由でLANポート1のIPアドレスを設定します。

netconfig service <http/https/ssh/telnet/base> port <port_number>

例1:

netconfig service http port 8080

説明1:

HTTPのサービスポートを8080に設定します。

例2:

netconfig service base port 10000

説明2:

ベースソケットのサービスポートを10000に設定します。

dnsconfig if <eth0/eth1/bond> <v4/v6> set <pref_DNSaddr> <alter_DNSaddr>

例:

dnsconfig if eth0 v4 set 192.168.0.22 192.168.0.23

説明:

「LANポート1」の優先IPv4 DNSアドレスとして「192.168.0.22」を設定し、代替IPv4 DNSアドレスとして「192.168.0.23」を設定します。

dnsconfig if <eth0/eth1/bond> <dhcp/dhcpv6>

例:

dnsconfig if eth0 dhcp

説明:

DHCP経由でLANポート1のIPv4 DNSアドレスを設定します。

ユーザー管理コマンド

user

例:

user

説明:

ユーザーリストを表示します。

user name <username>

例:

user name gene

説明:

「gene」のユーザー情報を表示します。

group

例:

group

説明:

グループリストを表示します。

group name <groupname/*>

例1:

group name SD1

説明1:

「SD1」のグループ情報を表示します。

例2:

group name *

説明2:

全てのグループの情報を一覧表示します。

session

例:

session

説明:

現在ログインしているユーザーを一覧表示します。

session name <username> delete

例:

セッション名が削除されます

説明:

特定のセッション「willy」を強制終了します。

session index <index_number> delete

例:

session index 1 delete

説明:

特定のセッション(インデックス1)を強制終了します。

user name <user name> pwd <password> group <group name> role <1/2/3> add

例:

user name gene pwd pppWWW group SD1 role 1 add

説明:

ユーザーネームが「gene」、パスワードが「pppWWW」、割り当てたユーザーロールタイプが「role 1」、グループが「SD1」のユーザーアカウントを作成します。

注意:

- 次のパラメーターは、割り当てるユーザーロールのタイプです。
  - role 1:スーパーアドミニストレーター
  - role 2:アドミニストレーター
  - role 3:ユーザー
- 各ロールへの権限は、システムがデフォルトで割り当てる内容に基づいています。

---

user name <username> pwd <password>

例:

user name gene pwd pppWWW

説明:

ユーザーネームが「gene」のアカウントに対して、パスワードを「pppWWW」に設定します。

user name <username> group <group name>

例:

user name gene group SD1

説明:

ユーザーアカウント「gene」をグループ「SD1」に割り当てます。

group name <group name> user <username> remove

例:

group name SD1 user gene remove

説明:

ユーザーアカウント「gene」をグループ「SD1」から削除します。

user name <username> port <port number> priv <0000/0100/0101/0010/0011>

例:

user name gene port 1,2,3,8,9 priv 0010

説明:

ユーザー「gene」に、シリアルポート1、シリアルポート2、シリアルポート3、シリアルポート8、シリアルポート9 に対する「フルアクセス」の権限を割り当てます。

注意:

割り当てる権限レベルは次の通りです。

- **0000**:アクセス不可
- **0100**:参照のみ
- **0101**:参照のみ＋設定
- **0010**:フルアクセス
- **0011**:フルアクセス＋設定

---

group name <group_name> delete

例:

group name SD1 delete

説明:

グループ「SD1」を削除します。

group name <group_name> role <1/2/3> add

例:

group name SD1 role 1 add

説明:

「SD1」という名前のグループを作成し、この新しく作成されたグループに「role 1」のロールタイプを割り当てます。

注意:

- 以下のパラメーターは、割り当てるロールタイプです。
  - **role 1**:スーパーアドミニストレーター
  - **role 2**:アドミニストレーター
  - **role 3**:ユーザー
- 各ロールへの権限は、システムがデフォルトで割り当てる内容に基づいています。

---

group name <group_name> port <port_number> priv <0000/0100/0101/0010/0011>

例:

group name SD1 port 1,2,3,5,8,9 priv 0010

説明:

グループ「SD1」に、シリアルポート1、シリアルポート2、シリアルポート3、シリアルポート8、シリアルポート9 に対して、「フルアクセス」の権限を割り当てます。

注意:

割り当てる権限レベルは次の通りです。

- **0000**:アクセス不可
- **0100**:参照のみ
- **0101**:参照のみ＋設定
- **0010**:フルアクセス
- **0011**:フルアクセス＋設定

---

group name <group_name> delete

例:

group name SD1 delete

説明:

グループ「SD1」を削除します。

シリアルポート設定コマンド

serial

例:

serial

説明:

シリアルポートリストを表示します。

serial port <port_number>

例:

serial port 1

説明:

シリアルポート1のシリアルポートプロパティーを表示します。

serial port <port_number> log

例:

serial port 1 log

説明:

シリアルポート1のポートログを表示します。

注意:

このコマンドは、ポートバッファー機能が有効であるという前提で動作します。詳細については、p.91「ポートバッファー」を参照してください。

---

serial port <port_number> baud <300/600/1200/1800/2400/4800/9600/19200/28800/38400/57600/115200/230400>

例:

serial port 1,4,7,12 baud 9600

説明:

シリアルポート1、シリアルポート4、シリアルポート7、シリアルポート12のボーレートを9600bpsに設定します。

serial port <port_number> mode <00/11/12/13/21/22/23>

例:

serial port 1,3,9 mode 13

説明:

シリアルポート1、シリアルポート3、シリアルポート9の場合は、動作モードを「コンソール管理」に設定し、SSH とTelnet も有効にします。

注意:

コマンドラインで次のパラメーターを使用して、シリアルポートの動作モードを設定します。

- **mode 00**:無効
- **mode 11**:コンソール管理。SSHが有効です。
- **mode 12**:コンソール管理。Telnetが有効です。
- **mode 13**:コンソール管理。SSHとTelnetの両方が有効です。
- **mode 21**:コンソール管理ダイレクト。SSHが有効です。
- **mode 22**:コンソール管理ダイレクト。Telnetが有効です。
- **mode 23**:コンソール管理ダイレクト。SSHとTelnetの両方が有効です。

---

serial port <port_number> access

例:

serial port 1 access

説明:

シリアルポート1にアクセスします。

注意:

SNコンソールに戻るには、[Ctrl]+[d] を押してください。

---

serial port <port_number> name <port_name>

例:

serial port 1 name Cisco

説明:

シリアルポート1のポート名を「Cisco」に設定します。

設定のバックアップ/リストアコマンド

backup pwd <password> path <usb1/usb2/usb3/usb4>

例:

backup pwd pppWWW path usb1

説明:

システム設定をバックアップし、外部USB ドライブ「USB1」に保存します。また、このバックアップファイルをパスワード「pppWWW」で暗号化します。

注意:

この機能はSN1100CO/SN1100COD/SN0100CO/SN0100CODシリーズのみでお使いいただけます。

---

restore pwd <password> path <usb1/usb2/usb3/usb4> filename <file_name>

例:

restore pwd pppWWW path usb1 filename sysconf.dat

説明:

暗号化されたシステム設定ファイル「sysconf.dat」を外部ドライブ「USB1」のルートディレクトリーから復元し、パスワード「pppWWW」で暗号化を解除します。

注意:

この機能はSN1100CO/SN1100COD/SN0100CO/SN0100CODシリーズのみでお使いいただけます。

---

backup pwd <password> path <tftp://host_address/folder>

例:

backup pwd pppWWW path tftp://192.168.0.100/ATEN

説明:

IPが「192.168.0.100」、パスが「/ATEN」のTFTP サイトにシステム設定をバックアップします。また、このバックアップファイルをパスワード「pppWWW」で暗号化します。

restore pwd <password> path <tftp://host_address/ folder> filename <file_name>

例:

restore pwd pppWWW path tftp://192.168.0.100/ATEN filename sysconf.dat

説明:

IPが「192.168.0.100」で、パスが「/ATEN」のTFTP サイトから暗号化されたシステム設定ファイル「sysconf.dat」をリストアし、パスワード「pppWWW」で暗号化を解除します。

backup pwd <password> path <ftp://host_address/folder> ftpuser <username> ftppwd <password>

例:

backup pwd pppWWW path ftp://192.168.0.100/ATEN ftpuser willy ftppwd pppWWW

説明:

システム構成をバックアップし、IP が「192.168.0.100」、パスが「/ATEN」のFTP サイトに保存し、このバックアップファイルをパスワード「pppWWW」で暗号化します。FTPサイトにログインするためのユーザーネームは「willy」で、ログインパスワードは「pppWWW」です。

restore pwd <password> path <ftp://host_address/folder> filename <file_name> ftpuser <username> ftppwd <password>

例:

restore pwd pppWWW path ftp://192.168.0.100/ATEN filename sysconf.dat ftpuser willy ftppwd pppWWW

説明:

IPアドレスが「192.168.0.100」で、パスが「/ATEN」のFTPサイトからシステム設定ファイル「sysconf.dat」をリストアし、パスワード「pppWWW」で暗号化を解除します。FTPサイトにログインするためのユーザーネームは「willy」で、ログインパスワードは「pppWWW」です。

restore pwd <password> path <usb1/usb2/usb3 または tftp://host_address/folder/ または ftp://host_address/folder> filename <file_name> ftpuser <username> ftppwd <password> netconfig if <eth0/eth1/bond> <v4/v6> ip <IP_address> nm <subnet_mask> gw <gateway_address> set hostname=<host_name>

例:

restore pwd pppWWW path ftp://192.168.0.100/ATEN filename sysconf.dat ftpuser willy ftppwd pppWWW netconfig if eth0 v4 ip 192.168.1.1 nm 255.255.255.0 gw 192.168.1.255 set hostname=SN9108CO

説明:

IPアドレスが「192.168.0.100」で、パスが「/ATEN」のFTPサイトからシステム設定ファイル「sysconf.dat」をリストアし、パスワード「pppWWW」で暗号化を解除します。FTPサイトにログインするためのユーザーネームは「willy」で、ログインパスワードは「pppWWW」です。

一方、LANポート1 のIPアドレスは「192.168.1.1」、サブネットマスクは「255.255.255.0」、ゲートウェイアドレスは「192.168.1.255」に設定します。

「SN9108CO」をシリアルコンソールサーバーのホスト名またはデバイス名として設定します。

注意:

パラメーター「ftpuser」と「ftppwd」は、リストア操作を実行するにあたりFTPサイトからバックアップファイルを取得するときに必要です。

ファームウェアアップグレードコマンド

update path <usb1/usb2/usb3> filename <file_name>

例:

update path usb1 filename SN01_SN91xx_V1.7.161.001.fw

説明:

外部ドライブ「USB1」のルートディレクトリーに保存しているアップデートファイル「SN01_SN91xx_V1.7.161.001.fw」でファームウェアをアップデートします。

注意:

この機能は、SN01xxCO/SN01xxCODのみでお使いいただけます。

---

update path <tftp://host_address/folder> filename <file_name>

例:

update path tftp://192.168.0.100/ATEN filename SN01_SN91xx_V1.7.161.001.fw

説明:

IP が「192.168.0.100」、パスが「/ATEN/」のTFTP サイトに保存しているアップデートファイル「SN01_SN91xx_V1.7.161.001.fw」でファームウェアを更新します。

update path <ftp://host_address/folder> filename <file_name> ftpuser <username> ftppwd <password>

例:

update path ftp://192.168.0.100/ATEN filename SN01_SN91xx_V1.7.161.001.fw ftpuser willy ftppwd pppWWW

説明:

IPが「192.168.0.100」、パスが「/ATEN/」、FTPサイトにログインするためのユーザーネームが「willy」、ログインパスワードが「pppWWW」のFTPサイトに保存しているアップデートファイル「SN01_SN91xx_V1.7.161.001.fw」でファームウェアを更新します。

IPフィルターコマンド

ipfilter <include/exclude>

例:

ipfilter include

説明:

インクルードモードでIPフィルター機能を有効にします。

ipfilter off

例:

ipfilter off

説明:

IPフィルター機能を無効にします。

ipfilter

例:

ipfilter

説明:

全てのフィルター条件のリストを表示します。

ipfilter cond <filter_condition> add

例:

ipfilter cond 192.168.0.10 add

説明:

フィルター条件の1つに「192.168.0.10」を追加して、このIPアドレスを含めるか除外します。

注意:

- カンマを使用して、複数のアドレスを区切ります。(例:192.168.1.10, 192.168.1.99)
- IPアドレスの範囲の場合は、開始アドレスと終了アドレスの間にダッシュを入れます。(例:192.168.0.10-192.168.0.100)

---

ipfilter index <index_number> delete

例:

ipfilter index 1 delete

説明:

インデックス1のフィルター条件を削除します。

アカウントポリシーコマンド

acctp

例:

acctp

説明:

アカウントポリシーの設定を表示します。

acctp name <min_length>

例:

acctp name 8

説明:

ユーザーネームの最小長を少なくとも8の値に設定します。パラメーター<min_length>の使用可能な値は1～32です。

acctp pwd <min_length>

例:

acctp pwd 8

説明:

パスワードの最小長を8以上の値に設定します。パラメーター<min_length>の使用可能な値は1～32です。

acctp pwdup <on/off>

例:

acctp pwdup on

説明:

パスワードには少なくとも1 つの大文字を含める必要があります。

acctp pwdlow <on/off>

例:

acctp pwdlow on

説明:

パスワードには少なくとも1つの小文字を含める必要があります。

acctp pwdnum <on/off>

例:

acctp pwdnum on

説明:

パスワードには1つ以上の数字を含める必要があります。

acctp pwdspec <on/off>

例:

acctp pwdspec on

説明:

パスワードには、1つ以上の特殊文字(記号)を含める必要があります。

set systime=<YYYMMDDHHMMSS>

例:

set systime=20221005133400

説明:

システム時刻の日付を「10/05/2022」に、時刻を「13:34:00」に、それぞれ手動設定します(YYYY:年、MM:月、DD:日、HH:時、MM:分、SS:秒)。

set ntp=<pref_NTPaddr> <alter_NTPaddr>

例:

set ntp=192.168.0.31 192.168.0.32

説明:

NTP サーバー「192.168.0.31」を優先 NTPアドレスとして、また、「192.168.0.32」を代替NTPアドレスとして、システム時刻を同期します。

set timezone=<timezone_number>

例:

set timezone=61

説明:

システムのタイムゾーンを「(GMT+09:00)大阪、札幌、東京」に設定します。タイムゾーン番号については、以下のタイムゾーン一覧を参照してください。

タイムゾーン一覧:

1. (GMT-12:00)エニウェトク、クワジェリン
2. (GMT-11:00)ミッドウェイアイランド、サモア
3. (GMT-10:00)ハワイ
4. (GMT-09:00)アラスカ
5. (GMT-08:00)太平洋時刻(米国およびカナダ)、ティフアナ
6. (GMT-07:00)山岳部標準時(米国およびカナダ)
7. (GMT-07:00)アリゾナ
8. (GMT-06:00)中部標準時(米国およびカナダ)
9. (GMT-06:00)メキシコシティ
10. (GMT-06:00)サスカチュワン
11. (GMT-06:00)中央アメリカ
12. (GMT-05:00)東部標準時(米国およびカナダ)
13. (GMT-05:00)インディアナ(東部)
14. (GMT-05:00)ボゴタ、リマ、キト
15. (GMT-04:00)大西洋標準時(カナダ)
16. (GMT-04:00)カラカス、ラパス
17. (GMT-04:00)サンティアゴ
18. (GMT-03:30)ニューファンドランド
19. (GMT-03:00)ブエノスアイレス、ジョージタウン
20. (GMT-03:00)ブラジリア
21. (GMT-03:00)グリーンランド
22. (GMT-02:00)中部大西洋岸
23. (GMT-01:00)アゾレス
24. (GMT-01:00)カーボベルデ諸島

25. (GMT)カサブランカ、モンロビア
26. (GMT)グリニッジ標準時:ダブリン、エディンバラ、リスボン、ロンドン
27. (GMT+01:00)アムステルダム、コペンハーゲン、マドリード、パリ、ビリニュス
28. (GMT+01:00)西中央アフリカ
29. (GMT+01:00)ベオグラード、サラエボ、スコピエ、ソフィア、ザグレブ
30. (GMT+01:00)ブラチスラバ、ブダペスト、ルブリャナ、プラハ、ワルシャワ
31. (GMT+01:00)ブリュッセル、ベルリン、ベルン、ローマ、ストックホルム、ウィーン
32. (GMT+02:00)カイロ
33. (GMT+02:00)ハラレ、プレトリア
34. (GMT+02:00)エルサレム
35. (GMT+02:00)ブカレスト
36. (GMT+02:00)ヘルシンキ、リガ、タリン
37. (GMT+02:00)アテネ、イスタンブール、ミンスク
38. (GMT+03:00)クウェート、リヤド
39. (GMT+03:00)ナイロビ
40. (GMT+03:00)バグダッド
41. (GMT+03:00)モスクワ、サンクトペテルブルク、ヴォルゴグラード
42. (GMT+03:30)テヘラン
43. (GMT+04:00)アブダビ、マスカット
44. (GMT+04:00)バクー、トビリシ、エレバン
45. (GMT+04:30)カブール
46. (GMT+05:00)イスラマバード、カラチ、タシケント
47. (GMT+05:00)エカテリンブルグ
48. (GMT+05:30)カルカッタ、チェンナイ、ムンバイ、ニューデリー
49. (GMT+05:45)カトマンズ
50. (GMT+06:00)アスタナ、ダッカ
51. (GMT+06:00)スリジャヤワルダナプラコッテ
52. (GMT+06:00)アルマトイ、ノボシビルスク
53. (GMT+06:30)ヤンゴン
54. (GMT+07:00)バンコク、ハノイ、ジャカルタ
55. (GMT+07:00)クラスノヤルスク
56. (GMT+08:00)北京、重慶、ホンコン、ウルムチ

57. （GMT+08:00）パース
58. （GMT+08:00）クアラルンプール、シンガポール
59. （GMT+08:00）台北
60. （GMT+08:00）イルクーツク、ウランバートル
61. （GMT+09:00）大阪、札幌、東京
62. （GMT+09:00）ソウル
63. （GMT+09:00）ヤクーツク
64. （GMT+09:30）ダーウィン
65. （GMT+09:30）アデレード
66. （GMT+10:00）キャンベラ、メルボルン、シドニー
67. （GMT+10:00）ブリスベン
68. （GMT+10:00）グアム、ポートモレスビー
69. （GMT+10:00）ホバート
70. （GMT+10:00）ウラジオストク
71. （GMT+11:00）マガダン、ソロモン諸島、ニューカレドニア
72. （GMT+12:00）フィジー、カムチャッカ半島、マーシャル諸島
73. （GMT+12:00）オークランド、ウェリントン
74. （GMT+13:00）ヌクアロファ