SN0108CO/SN0116CO/SN0132CO/ SN0148CO/SN9108CO/SN9116CO/ SN0108COD/SN0116COD/ SN0132COD/SN0148COD



本ドキュメントについて

本書は ATEN ジャパン株式会社において、SN0108CO/SN0116CO/SN0132CO/SN0148CO/SN9108CO/SN9116CO/SN0108COD/SN0116COD/SN0132COD/SN0148COD 取り扱いの便宜を図るため、英語版ユーザーマニュアルをローカライズしたドキュメントです。

製品情報、仕様はソフトウェア・ハードウェアを含め、予告無く改変されることがあり、本日本語版ユーザーマニュアルの内容は、必ずしも最新の内容でない場合があります。また製品の不要輻射仕様、各種安全規格、含有物質についての表示も便宜的に翻訳して記載していますが、本書はその内容について保証するものではありません。

製品をお使いになるときは、英語版ユーザーマニュアルにも目を通し、その取扱方法に従い、正しく運用を行ってください。詳細な製品仕様については英語版ユーザーマニュアルの他、製品をお買い上げになった販売店または弊社テクニカルサポート窓口までお問い合わせください。

ATEN ジャパン株式会社

技術部

TEL: 03-5615-5811

MAIL:support@atenjapan.jp

ユーザーの皆様へ

本マニュアルに記載された全ての情報、ドキュメンテーション、および製品仕様は、製造元である ATEN International により、予告無く改変されることがあります。製造元 ATEN International は、製品および本ドキュメントに関して、品質・機能・商品性および特定の目的に対する適合性について、法定上の、明示的または黙示的であるかを問わず、いかなる保証もいたしません。

弊社製品は一般的なコンピューターのメインフレームおよびインターフェースの操作・運用・管理を目的として設計・製造されております。高度な動作信頼性と安全性が求められる用途、例えば軍事使用、大規模輸送システムや交通インフラの制御、原子力発電所、セキュリティシステム、放送システム、医療システム等における可用性への要求を必ずしも満たすものではございません。

キーボード、マウス、モニター、コンピューター等、弊社製品に接続されるクライアントデバイスは、それぞれベンダーの独自技術によって開発・製造されております。そのため、これらの異なるデバイスを接続した結果、予期できない機器同士の相性問題が発生する可能性があります。また、機器の併用により、それぞれオリジナルで持つ機能を全て発揮できない可能性があります。異なる環境・異なる機器の組み合わせにより、機能面での使用制限が必要になる可能性があります。

本製品および付属のソフトウェア、ドキュメントの使用によって発生した装置の破損・データの損失等の損害に関して、直接的・間接的・特殊な事例・付帯的または必然的であるかを問わず、弊社の損害賠償責任は本製品の代金相当額を超えないものとします。

製品をお使いになる際には、製品仕様に沿った適切な環境、特に電源仕様についてはご注意のうえ、正しくお使いください。

ATEN ジャパン製品保証規定

弊社の規定する標準製品保証は、定められた期間内に発生した製品の不具合に対して、すべてを無条件で保証するものではありません。製品保証を受けるためには、この『製品保証規定』およびユーザーマニュアルをお読みになり、記載された使用法および使用上の各種注意をお守りください。

また製品保証期間内であっても、次に挙げる例に該当する場合は製品保証の適用外となり、有 償による修理対応といたしますのでご留意ください。

- ◆使用上の誤りによるもの
- ◆ 製品ご購入後の輸送中に発生した事故等によるもの
- ◆ ユーザーの手による修理または故意の改造が加えられたもの
- ◆ 購入日の証明ができず、製品に貼付されている銘板のシリアルナンバーも確認できないもの
- ◆ 車両、船舶、鉄道、航空機などに搭載されたもの
- ◆ 火災、地震、水害、落雷、その他天変地異、公害、戦争、テロリズム等の予期しない災害によって故障、破損したもの
- ◆ 日本国外で使用されたもの
- ◆ 日本国外で購入されたもの

【製品保証手順】

弊社の製品保証規定に従いユーザーが保証を申請する場合は、大変お手数ですが、以下の手順に従って弊社宛に連絡を行ってください。

(1)不具合の確認

製品に不具合の疑いが発見された場合は、購入した販売店または弊社サポート窓口に連絡の上、製品の状態を確認してください。この際、不具合の確認のため動作検証のご協力をお願いすることがあります。

(2)本規定に基づく製品保証のご依頼

(1)に従い確認した結果、製品に不具合が認められた場合は、本規定に基づき製品保証対応を 行います。製品保証対応のご依頼をされる場合は、RMA申請フォームの必要項目にご記入の上、 『お客様の製品購入日が証明できる書類』を用意して、購入した販売店までご連絡ください。販売 店が不明な場合は、弊社までお問い合わせください。

(3)製品の発送

不具合製品の発送は宅配便などの送付状の控えが残る方法で送付してください。

【製品保証期間】

製品保証期間は通常製品/液晶ディスプレイ搭載製品で異なります。詳細は下記をご覧ください。

①通常製品	製品納品日~30日	初期不良、新品交換※1
	31 日~3 年間	無償修理
	3年以上	有償修理※2
②型番 CL からはじまる LCD 搭載製品のみ	製品納品日~30日	初期不良、新品交換※1
	31 日~2 年間	無償修理
	3年目以降	有償修理※2

※1…製品購入日から30日以内に確認された不具合は初期不良とし、新品交換を行います。初期 不良の場合の送料は往復弊社にて負担いたします。

※2…有償修理の金額は別途製品を購入された販売店までお問い合わせください。

※ケーブル類、その他レールキット等のアクセサリ類は初期不良の際の新品交換のみ、承ります。

※EOL (生産終了)が確定した製品については、初期不良であっても無償修理対応とさせていただきます。また EOL 製品の修理に関して、上記無償修理期間中であっても、部材調達の都合等により修理不可になる可能性がございます。そのような場合には、機能同等品による良品交換のご対応となる可能性がございます。また、EOL 製品の型番や、修理可否、後継機種については、随時情報更新を行っておりますので、弊社 Web ページにて最新情報をご確認ください。

※製品保証期間の延長や故障時の代替品などの保証オプションについては、弊社 Web ページを ご確認ください。

【補足】

- ・本規定は ATEN 製品に限り適用します。
- ケーブル類は初期不良対応に準じます。
- ・初期不良による新品交換の場合は、ATEN より発送した代替品の到着後、5 営業日以内に不具合品を弊社宛に返却してください。返却の予定期日が守られない場合は弊社から督促を行いますが、それにも係わらず不具合品が返却されない場合は、代替機相当代金を販売代理店経由でご請求いたします。
- ・ラベルの汚損や剥がれなどにより製品のシリアルナンバーが確認できない場合は、すべて有償修理とさせていただきます。

【免責事項】

- 1. 弊社製品は映像関連システムやコンピューターのメインフレームおよびインターフェースの操作・運用・管理を目的として設計・製造されております。しかし、使用環境等によってはその機能が制限されることがあります。弊社では、ご購入前に弊社製品をお試しいただける「評価機貸出サービス」を、無償でご提供しております。評価機貸出サービスに関するお問い合わせは、弊社代理店または弊社 Web サイト(https://www.aten.com/jp/ja/)内の「お問い合わせ」フォームをご利用ください。
- 2. キーボード、マウス、モニター、コンピューター等、弊社製品に接続されるクライアントデバイスは、それぞれベンダーの独自技術によって開発・製造されております。そのため、これらの異なるデバイスを接続した結果、予期できない機器同士の相性問題が発生する可能性があります。また、機器の併用により、それぞれオリジナルで持つ機能を全て発揮できない可能性があります。異なる環境・異なる機器の組み合わせにより、機能面での使用制限が必要になる可能性があります。
- 3. 他社製品のKVMスイッチ、キーボード・マウスコンバーター、キーボード・マウスエミュレーター、 KVM エクステンダー等との組み合わせはサポート対象外となりますが、お客様で自己検証の上で あれば、使用を制限するものではありません。
- 4. 製品に対しての保証は、日本国内で使用されている場合のみ対象とさせて頂きます。
- 5. 製品やサービスについてご不明な点がある場合は、弊社技術部門までお問い合わせください。

製品についてのお問い合わせ

製品の仕様や使い方についてのお問い合わせは、下記窓口または製品をお買い上げになった販売店までご連絡ください。

購入前のお問い合わせ	ATEN ジャパン株式会社 営業部
	TEL:03-5615-5810
	MAIL:sales@atenjapan.jp
購入後のお問い合わせ ATEN ジャパン株式会社 技術部	
	TEL:03-5615-5811
	MAIL :support@atenjapan.jp

目次

ユーザーの皆様へ	i
ATEN ジャパン製品保証規定	ji
製品についてのお問い合わせ	v
EMC に関する情報	7
RoHS	8
バッテリーの安全に関する注意事項	8
安全にお使い頂くために	9
全般	9
DC 電源	11
ラックマウント	12
同梱品	
SN0108CO/SN0116CO	13
SN0108COD/SN0116COD	13
SN0132CO/SN0148CO	13
SN0132COD/SN0148COD	14
SN9108CO/SN9116CO	14
本マニュアルについて	
概要	15
マニュアル表記について	
用語	18
第1章 はじめに	
概要	
特長	21
システムのアクセス性と可用性	21
シリアルコンソール管理	21
セキュリティ	22
システム管理	22
シリアルデバイス管理	23
言語	23
システム要件	24
DTE/DCE 自動検出	25
ブラウザー	25

製品各部名称	26
SN0108CO/SN0108COD フロントパネル	26
SN0116CO/SN0116COD フロントパネル	26
SN0132CO/SN0132COD フロントパネル	28
SN0148CO/SN0148COD フロントパネル	28
SN9108CO フロントパネル	30
SN9116CO フロントパネル	30
SN0108CO リアパネル	32
SN0116CO リアパネル	32
SN0108COD リアパネル(DC 電源)	33
SN0116COD リアパネル(DC 電源)	33
SN0132CO リアパネル	34
SN0148CO リアパネル	34
SN0132COD リアパネル(DC 電源)	35
SN0148COD リアパネル(DC 電源)	35
SN9108CO リアパネル	36
SN9116CO リアパネル	36
第2章 ハードウェアセットアップ	37
セットアップの前に	37
卓上設置およびラックへの取付	37
卓上設置	37
ラックへのマウント	39
シリアルコンソールサーバーのセットアップ	43
SN0108CO/SN0116CO/SN0132CO/SN0148CO のセットアップ	43
SN9108CO/SN9116CO のセットアップ	46
第3章 スーパーアドミニストレーターによる 設定	48
概要	48
初回セットアップ	48
ローカルログイン	48
リモートログイン	52
セットアップ	55
ネットワーク設定	55
スーパーアドミニストレーターのログイン情報の変更	56
第4章 ユーザーインターフェース	57
概要	57
アクセス	57

ローカルコンソールの操作	58
リモート操作	59
Web ブラウザーからのログイン	59
Web ブラウザーのメイン画面	60
画面各部名称	60
タブメニュー	62
SN ビューワー	64
コントロールパネルの機能	65
データのインポート	66
エンコード	67
メッセージボード	67
マクロ	68
ターミナル設定	69
ターミナルアプリケーション	71
第5章 ポート操作モード	72
概要	72
操作モード	73
コンソール管理	73
リアル COM ポート	73
TCP サーバー/TCP クライアント(シリアルトンネル)	74
UDP モード	75
バーチャルモデム	75
コンソール管理ダイレクト	75
無効	76
第 6 章 ポートアクセス	77
概要	77
サイドバー	78
サイドバーのツリービュー	78
フィルター	79
接続	80
Telnet/SSH	82
ポート属性	83
お気に入り	84
履歴	84
ユーザー設定	86
ヤッドノコン	88

アクセス	90
プロパティ	92
ポートバッファー	95
操作モード	96
第7章 ユーザー管理	106
概要	106
ユーザー	107
ユーザーの作成	107
ユーザーアカウントの編集	111
ユーザーアカウントの削除	112
グループ	113
グループの作成	113
グループの編集	115
グループの削除	115
ユーザーとグループ	116
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	116
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	117
グループメニューを使ってユーザーをグループに登録する場合	118
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	119
デバイスの割り当て	120
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	120
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	122
第8章 デバイス管理	123
デバイス	123
全般	123
マウントされたデバイス	125
ポートログの Syslog 設定	127
ポートネームの自動検出	127
ネットワーク	128
IP インストーラー	128
サービスポート	129
ネットワーク設定	129
ANMS	133
イベントの宛先	
認証と権限設定	137
CC 管理の設定	141

OOBC	142
コンソールポートの設定	143
セキュリティ	148
ログイン失敗	148
セキュリティレベル	149
動作モード	149
IP/MAC フィルター	150
アカウントポリシー	152
関連付け	154
日付/時刻	155
現在のシステム時刻	155
新しいシステム時刻	156
タイムゾーン	156
第9章 ログ	157
概要	157
システムログ	157
フィルター	158
ログ通知設定	161
第 10 章 メンテナンス	162
概要	162
バックアップ/リストア	162
バックアップ	163
リストア	
ファームウェアアップグレード	164
証明書	166
付録	
製品仕様	171
SN0108CO/SN0108COD	171
SN0116CO/SN0116COD	173
SN0132CO/SN0132COD	
SN0148CO/SN0148COD	177
SN9108CO/SN9116CO	179
IP アドレスの設定	181
ローカルコンソール	181
IP インストーラー	181
ブラウザー	183

IPv6	184
リンクローカルアドレス	
ステートレス自動設定	
バーチャルモデム詳細	
AT コマンドセットのサポート	
ポートの転送	190
距離とボーレートの関係	190
ログイン情報の消去	191
ピンアサイン	192
DB-9/DB-25 インターフェース	193

EMC に関する情報

FCC(連邦通信委員会)電波干渉声明

本製品は、FCC(米国連邦通信委員会)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為のものです。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、すべての干渉を受け入れなければならないこと。

FCC による注意: 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。

注意:本製品をご家庭で使用した場合、電波干渉を引き起こす可能性があります。

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および理事会指令』、通称 RoHS 指令に準拠しております。



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。

安全にお使い頂くために

全般

- ◆ 本製品は、屋内での使用に限ります。
- ◆ 製品に同梱されるドキュメントは全てお読みください。またドキュメント類は全て保存してください。また、弊社 Web サイトに掲載のオンラインユーザーマニュアルもご確認ください。
- ◆ 製品に関する注意・説明に従って取り扱ってください。
- ◆ 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。
- ◆ 製品が水に濡れるおそれのあるような場所で使用しないでください。
- ◆ 製品は熱源の近く、またはその熱源の上などで使用しないでください。
- ◆ 製品のケースには必要に応じて通気口が設けられています。通気口のある製品は、安定した 運用を行うため、また製品の過熱を防ぐために、開口部を塞いだり覆ったりしないでください。
- ◆ 製品をベッドやソファ、ラグなどの柔らかいものの上に置かないでください。 開口部が塞がれ、 適切な通気が確保できずに製品が過熱するおそれがあります。
- ◆ 製品にいかなる液体もかからないようにしてください。
- ◆ 電源プラグを電源コンセントから抜く場合は、乾いた雑巾でプラグ周りのホコリを掃除してください。液体やスプレー式のクリーナーは使用しないでください。
- ◆ 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、電源の上限を把握しておき、これを超えないように注意してください。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どうか、また、すでに危険な条件がそろっていないかどう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、購入された販売店もしくは電気事業者にお問い合わせください。
- ◆ お使いの装置への損傷を避けるためにも、すべ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。使用される国/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こと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。これらのケーブル類の上には 何も置かないようにしてください。
- ◆ 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行ってください。
 - ♪ パワーサプライを取り外す前に電源ケーブルを抜いてください。
 - ▶ お使いのシステムが複数のパワーサプライをお使いである場合、パワーサプライからすべての電源ケーブルを抜いてお使いのシステムから切り離してください。
- ◆ 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。
- ◆ 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見られる。(修理が必要です)
 - ▶ 製品マニュアルに従って操作しているにもかかわらず、正常に動作しない。
- ◆ 修理が必要となる故障が発生するおそれがありますので、製品マニュアルに従って操作してく ださい。

DC 電源

- ◆ デバイスが、ショート、過電流、およびアース(接地)障害に対して保護されるかは、建物設備の 保護装置に依存しています。建物設備の保護装置がシステムを保護するために適切に評価され、国および地域の規則に準拠していることを確認してください。
- ◆ 建物の設備に組み込む場合、DC 電源ユニットは緊急時にすぐアクセスでき、取り外せるようになっているか確認してください。
- ◆ 本製品には保護接地端子が別に設けられています。これを、常に接地されている状態にして おいてください。
- ◆ DC 電源回路には、UL、AWM VW-1 Style 1015、最小 16AWG、最小 105℃、最小 300V で認定されている DC 電源ケーブルを選択してください。
- ◆ **注意:**この装置は、DC 供給回路の接地導線を、装置の接地導線に接続できるように設計されています。この接続を行う場合は、以下の条件をすべて満たしている必要があります。
 - ▶ 本装置は、直流電源アース極導線、または直流電源アース極導線が接続されている接地 用バーやバスからのボンディングジャンパーに直接接続するものとします。
 - ▶ 本製品は、同じ直流電源から、例えば1つのキャビネット内で複数の機器と同時に給電されている場合、必ず同じアースに接続してください。別系統の直流のアースに繋がないでください。
 - ▶ DC電源は、当製品の近くに設置する必要があります。
 - ➤ 装置の電源入切は、直流電源と接地極導線の接続点との間の接地回路導線内で行わないでください。
- ◆ **警告:**このユニットは、アクセスが制限されている場所に設置することが想定されています。アクセス制限エリア(サーバールーム、データセンターなど)とは、専用の工具、鍵、またはその他のセキュリティ手段を使用して、保守担当者のみがアクセスできる場所であり、その場所を担当する権限に管理されています。

ラックマウント

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

同梱品

シリアルコンソールサーバーの製品パッケージには下記のアイテムが同梱されています。

SN0108CO/SN0116CO

- ◆ SN0108CO/SN0116CO 8/16 ポート シリアルコンソールサーバー(デュアル電源/LAN 対応モデル) ×1
- ◆ ラップトップ USB コンソールケーブル ×1
- ◆ 電源ケーブル×2(AC 電源モデル)
- ◆ マウントキット ×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
- ◆ フットパッドセット(4pcs) ×1
- ◆ クイックスタートガイド* ×1

SN0108COD/SN0116COD

- ◆ SN0108COD/SN0116COD 8/16 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、DC 電源モデル) ×1
- ◆ ラップトップ USB コンソールケーブル ×1
- ◆ マウントキット ×1
- ◆ フットパッドセット(4pcs) ×1
- ◆ クイックスタートガイド* ×1

SN0132CO/SN0148CO

- ◆ SN0132CO/SN0148CO 32/48 ポート シリアルコンソールサーバー(デュアル電源/LAN 対応モデル) ×1
- ◆ ラップトップ USB コンソールケーブル ×1
- ◆ 電源ケーブル×2(AC 電源モデル)
- ◆ マウントキット ×1
- ◆ フットパッドセット(4pcs) ×1
- ◆ クイックスタートガイド* ×1

SN0132COD/SN0148COD

- ◆ SN0132COD/SN0148COD 32/48 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、DC 電源モデル) ×1
- ◆ ラップトップ USB コンソールケーブル ×1
- ◆ マウントキット ×1
- ◆ フットパッドセット(4pcs) ×1
- ◆ クイックスタートガイド* ×1

SN9108CO/SN9116CO

- ◆ SN9108CO/SN9116CO 9/16 ポート シリアルコンソールサーバー(シングル電源/LAN 対応モデル)×1
- ◆ 電源ケーブル×1
- ◆ マウントキット ×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
- ◆ フットパッドセット(4pcs) ×1
- ◆ クイックスタートガイド* ×1

上記のアイテムがそろっているかご確認ください。万が一、欠品または破損品があった場合は お買い上げになった販売店までご連絡ください。

本ユーザーマニュアルをよくお読みいただき、正しい使用法により、本製品および接続する機器を安全にお使いください。

* 本マニュアルの公開後に、製品仕様が追加される場合があります。最新版は弊社 Web サイトにアクセスしてご確認ください。

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システムを最大限に活用するために 提供されています。このドキュメントには、取り付け・セットアップ方法、操作方法のすべてが書か れています。マニュアルは下記のとおりに構成されています。

概要

- **第1章 はじめに**:シリアルコンソールサーバーについて紹介します。特長、機能概要および製品各部名称について説明します。
- **第2章 ハードウェアのセットアップ**:インストールのセットアップ手順と、基本的な操作手順について説明します。
- **第3章 スーパーアドミニストレーターによる設定**:スーパーアドミニストレーターがシリアルコン ソールサーバーに対して行う、ネットワークの設定やデフォルトアカウント(ユーザーネームおよびパスワード)の変更方法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 のレイアウトや構成要素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 ポート操作モード:ポートの操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となるアプリ ケーションで使用されるリアル 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の概要と、この画面で提供されるポートと電源アウト レット操作に関するオプション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やアドミニストレーターが、ユーザーやグループを追加・変更・削除したり、これらのユーザーやグループに対して属性を割り当てたりす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その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されています。
- 付録 製品の仕様および関連する技術情報や操作方法について説明します。

マニュアル表記について

入力するキーを示します。例えば[Enter]はエンターキーを押します。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、作業の手順を意味するものではありません。
- 矢印は操作の手順を示します。例えばStart → Run はスタートメニューを開

 ・ Run を選択することを意味します。



重要な情報を示しています。

※本マニュアルに記載されている商品名・会社名等は、各社の商標ならびに登録商標です。

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され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」と表現されることもあれば、「リモート」と表現されることもあります。

- ◆ 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されたコンピューターのことを指します。
 - 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 されているデバイスのことを指します。

◆ 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 -「*離れた*」場所にあるシリアルコンソールサーバーに接続されたデバイスを、自身のコンピューターから操作している人を「ローカルクライアントユーザー」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場合は、基本的には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なされます。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って行う操作について説明する場合は、ユーザー側の観点に立って説明します。この場合、製品およびその配下にあるサーバーがリモート側と見なされます。

第1章 はじめに

概要

SN01xxCO シリーズと SN91xxCO シリーズは、Cisco ピンアウトと自動検知 DTE/DCE 機能に対応した製品です。さらに、IT インフラの設置に要する時間を節約できるよう、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(および他の互換性のあるデバイス)にダイレクト接続できるのが特長です。また、SN01xxCO および SN91xxCO の各モデルは、接続されているシリアルデバイス(ターミナルブロックを含む)をオンライン検出することができます。接続され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が送信されます。

デュアル LAN とデュアル電源に対応した 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。SN01xxCO シリーズは、より柔軟にシステムが構築できるよう、デュアル DC(下記注意書きを参照)オプションも提供しています。

注意: お客様のご要望により、DC 電源モデル(SN0108COD/SN0116COD/SN0132COD/SN0148COD)も、ご利用いただけます。

このシリアルコンソールサーバーは、8/16/32/48 ポートでモデル展開しており、直接 Telnet/SSH クライアントおよび Java ビューアーを介して、サーバーおよびネットワークデバイスへの帯域内および帯域外(OOB)リモートシリアルコンソールアクセスを提供します。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され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。本番ネットワークでアクセスが困難な場合でも、管理者はコンソールサーバーを介してアクセスできます。このシリーズの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直接コンソール接続、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 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)を介したハイブリッドネットワーク接続といった、帯域外アクセス方式を提供します。

TLS 1.2 データ暗号化、RSA 2048 ビット証明書、ユーザーに対するポートアクセスと制御の権限付与設定、ローカル/リモート/サードパーティー認証と許可、IP/MAC アドレスフィルター、

FIPS 140-2 認証暗号化のような、各種セキュリティテクノロジーを使用して実装された SN01xxCO および SN91xxCO シリアルコンソールサーバーは、管理者が容易かつ高レベルにアクセスするためのセキュリティを保証します。例えば、8/16/32/48 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。データ暗号化によって情報と操作が常に保護されている状態が確保できます。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軽減に役立ちます。上記の例ではセキュリティ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。

SN01xxCO、SN91xxCOシリーズは、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や制御が行えるよう、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されます。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することができます。さらに、SN01xxCOシリーズは、ATENのPDU(下記注意書きを参照)リモート電源管理システムと連携して動作します。どちらも、ATENのCC2000 ソフトウェアを使用して、シリアルデバイスへのアクセスの集約と電源管理の統合が実現できます。

注意: PONポートはPGシリーズ(日本国内では取り扱っておりません。)のPDU用に予約されています。

SN01xxCO および SN91xxCO シリーズは、シリアルデバイスのリモート管理を容易かつ安全に行うことで、ITの生産性の最大化、スケーラビリティーの向上、セットアップや運用にまつわるコストの削減に役立ちます。シリアルコンソールサーバーは、管理者が事実上どこからでもデータセンターを管理できるようにすることで、時間と費用を節約します。つまり、移動コストと MTTR (Mean Time to Repair)コストを最小限に抑え、データセンターのサービスの可用性を最大限に高めます。

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へはセキュアなインバンドおよびアウトオブバンドネットワークアクセスを 使用
- ◆ 直感的な GUI を使ったブラウザアクセス
- ◆ ターミナルベースアクセス メニュー形式の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 PC カードの接続に便利な 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使用して、ノートパソコンを追加ローカルコンソールとして使用可能*
- ◆ 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*
- ◆ デュアル電源*

注意: SN01xxCOシリーズでのみ利用可能です。

シリアルコンソール管理

- ◆ 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
- ◆ 接続されたシリアルデバイス(ターミナルブロックを含む)のオンライン/オフライン状態を検出 デバイス状態監視でデバイスのオフライン状態(例:電源エラー)が検出されるとイベント通知を自動的に送信
- ◆ 応答確認 接続されたシリアルデバイスにおけるシステムの状態を確認し、確認エラー (例:システムクラッシュ)があった場合は通知を送信
- ◆ ポートネームの自動検出 接続されたネットワークスイッチのポートネームを自動的に取得し表示できるため、デバイスの識別や設定が簡単
- ◆ 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クライアント(例:PuTTY)から選択可能
- ◆ 簡単ポートアクセス ActiveX または Java シリアルビューワーから選択可能
- ◆ わかりやすいビューワー機能 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 あらかじめ定義され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されると、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することが可能
- ◆ 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
- ◆ ATEN 製電源管理デバイス*と併用して、ポートや電源アウトレットの関連付けが可能 (SN01xxCOのみ)

注意: PONポートはPGシリーズ(日本国内では取り扱っておりません。)のPDU用に予約されています。

セキュリティ

- ◆ 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-bit 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保護を強化
- ◆ 高度なセキュリティ FIPS140-2 認定の OpenSSL 暗号モジュールを組み込み、FIPS 140-2 Level 1 セキュリティ標準に準拠(証明書番号 #1747、#2398、#2473)
- ◆ セキュリティレベルの設定 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

- ◆ Web 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 (* サポートされるファイルシステム…FAT8、FAT16、FAT32)

- ◆ SNMP エージェント対応
- ◆ イベント通知 SNMP メール、SNMP Trap、SMS(モバイルサービス追加が必要)経由での通知に対応*
- ◆ 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
- ◆ ソフトウェア CC2000 と併用することで、データセンターの統合管理を実現
- ◆ ソフトウェア CCVSR と併用することで、ユーザーセッションの録画が可能

注意: SN01xxCOシリーズでのみ利用可能です。

シリアルデバイス管理

- ◆ 各種シリアル操作モード 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、バーチャルモデムに対応
- ◆ 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*
- ◆ 対応ボーレート 300、600、1200、1800、2400、4800、9600、19200、28800、38400、57600、115200、230400 bps

注意: 固定 TTY ドライバーは次に対応しています。

- 1) OpenServer (Sco Unix)
- 2) UnixWare 7, SVR 5
- 3) UnixWare 2.1, SVR 4.2
- 4) QNX 4.25, QNX 6
- 5) FreeBSD
- 6) Solaris 10
- 7) AIX 5.x
- 8) HP-UX 11i

言語

◆ 多言語対応 Web ベース GUI - 日本語、英語、韓国語、ドイツ語、ロシア語、中国語(簡体字/ 繁体字)

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)
- ◆ コンソール管理の操作モードを使用する場合は、Telnet/SSH クライアント、PuTTY などのサードパーティーのクライアント、または Web ブラウザーをインストールしておく必要があります。
- ◆ ブラウザベースの Windows クライアントを使用する場合は、Active X、コンソール操作モード用 の SN ビューワー、DirectX 8 が動作環境に必要です。また、これらのインストール後の環境に 2MB 以上の空きメモリーがあることをご確認ください。
- ◆ コンソール管理の操作モード用に、ブラウザベースの Java アプレットビューワーや SN ビューワーを使用する場合は、Java Runtime Environment (JRE) 8 以降のバージョンをインストールしてください。また、これらのインストール後の環境に 2MB 以上の空きメモリーがあることをご確認ください。Java は次の Web サイトより無償でダウンロードすることができます。https://java.com
- ◆ 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)の環境では、管理者権限を持つユーザーだけ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することができます。一般ユーザーは、マッピングされたリアル COM ポートを操作することしかできません。
- ◆ 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: UnixWare 7 SVR 5、Unix Ware 2.1 SVR 4.2、QNX 4.25、QNX 6、FreeBSD、Solaris 10、AIX 5.x、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出力については、p.192 の「ピンアサイン」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.193 の「DB-9/DB-25 インターフェース」 を参照してください。

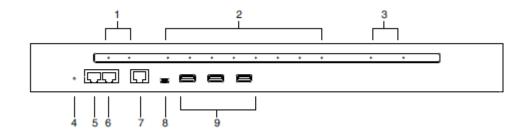
<u>ブラウザー</u>

本製品へのログインに対応したブラウザーは下表のとおりです。

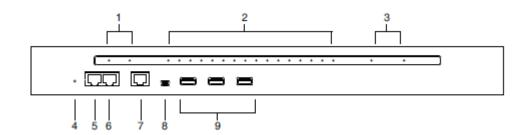
ブラウザー	バージョン
Internet Explorer	11 以降
Chrome	70 以降
Firefox	63 以降
Safari	12 以降

製品各部名称

SN0108CO/SN0108COD フロントパネル



SN0116CO/SN0116COD フロントパネル

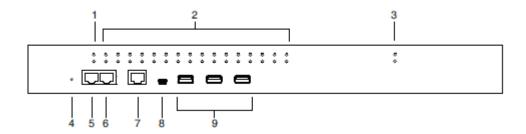


No.	名称	説明
1	電源 LED	電源が投入され、操作できる状態になると点灯します。
2	ポート LED	◆ グリーンに点滅:アクティブ - データが転送中であることを表して
		います。
3	LAN LED	プライマリーおよびセカンダリーの 10/100/1000Mbps LAN LED です。
		◆ レッド:10Mbps
		◆ レッド+グリーン(オレンジ):100Mbps
		◆ グリーン: 1000Mbps
		◆ 点滅中は、シリアルコンソールサーバーが LAN 経由でアクセスさ
		れていることを表します。

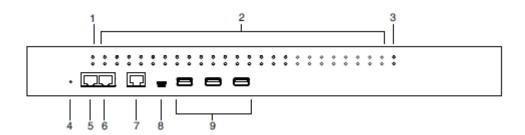
(表は次のページに続きます)

No.	名称	説明
4	リセットスイッチ	注意:このスイッチはくぼんでいるので、ペーパークリップの端やボー
		ルペンなどの小さなもので押し込む必要があります。
		◆ 製品の動作中に、このボタンを押して離すと、システムリセットを実
		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、設定内容
		をリセットし、工場出荷時のデフォルト設定に戻します。
		注意: この操作を行っても、ユーザーアカウントの情報は消去され
		ません。ユーザーアカウント情報の消去については、p.191「ログイ
		ン情報の消去」を参照してください。
		◆ このボタンを押したまま製品本体の電源を ON にすると、これまで
		にアップグレードされたファームウェアの内容を破棄して、工場出
		荷時におけるファームウェアバージョンに戻します。この操作によ
		って、ファームウェアアップグレードの失敗から回復して、アップグ
		レードを再度行うことができます。
		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。
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.43「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
		l' _o
7	ローカル	この RJ-45 ポートは、ローカル側からの管理、およびコンピューターへ
	コンソールポート	のシリアルターミナル接続を介したアクセスのために使用します。
8	ラップトップ USB	こちらの 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
	コンソールポート	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、自動的に端末エミュレーターが起動し、
		SN のテキストメニューが表示されます。
9	USB ポート	これらの3つのType-AメスUSBポートは、USBストレージデバイス(ペ
		ンドライブ/ハードドライブ)、USB ハブ、USB SIM カードリーダーなどの
		USB デバイスを接続するために使用できます。

SN0132CO/SN0132COD フロントパネル



SN0148CO/SN0148COD フロントパネル

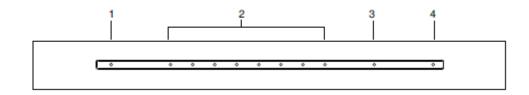


No.	名称	説明
1	電源 LED	製品本体に電源が入り、操作できる状態の時に点灯します。
2	ポートLED	ポート LED は、各 LED に対応するシリアルポートのステータス情報を
		提供します。
		◆ グリーンに点灯:オンライン状態 - ポートに接続されたシリアル機
		器に電源が入っており、準備ができていることを表しています。
		◆ グリーンに点滅:アクティブ - データがポートを介して転送中であ
		ることを表しています。
3	LAN LED	プライマリーおよびセカンダリーの 10/100/1000Mbps LAN LED です。
		◆ レッド:10Mbps
		◆ レッド+グリーン(オレンジ):100Mbps
		◆ グリーン: 1000Mbps
		◆ 点滅中は、シリアルコンソールサーバーが LAN 経由でアクセスさ
		れていることを表します。

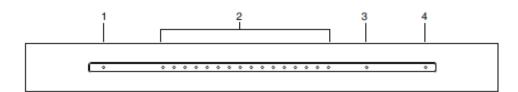
(表は次のページに続きます)

No.	名称	説明
4	リセットスイッチ	注意:このスイッチはくぼんでいるので、ペーパークリップの端やボー
		ルペンなどの小さなもので押し込む必要があります。
		◆ 製品の動作中に、このボタンを押して離すと、システムリセットを実
		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、設定内容
		をリセットし、工場出荷時のデフォルト設定に戻します。
		注意:この操作を行っても、ユーザーアカウントの情報は消去され
		ません。ユーザーアカウント情報の消去については、p.191「ログイ
		ン情報の消去」を参照してください。
		◆ このボタンを押したまま製品本体の電源を ON にすると、これまで
		にアップグレードされたファームウェアの内容を破棄して、工場出
		荷時におけるファームウェアバージョンに戻します。この操作によ
		って、ファームウェアアップグレードの失敗から回復して、アップグ
		レードを再度行うことができます。
		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。
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。詳細については、p.43「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	この RJ-45 ポートは、ローカル側からの管理、およびコンピューターへ
	ルポート	のシリアルターミナル接続を介したアクセスのために使用します。
8	ラップトップ USB	こちらの 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
	コンソールポート	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、自動的に端末エミュレーターが起動し、
		SN のテキストメニューが表示されます。
9	USB ポート	これらの 3 つの Type-A メス USB ポートは、USB ストレージデバイス(ペ
		ンドライブ/ハードドライブ)、USB ハブ、USB SIM カードリーダーなどの
		USB デバイスを接続するために使用できます。

SN9108CO フロントパネル



SN9116CO フロントパネル

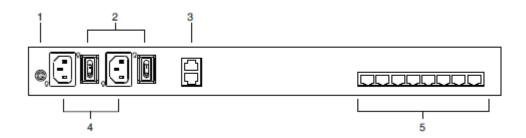


No.	名称	説明
1	電源 LED	電源が投入され、操作できる状態になると点灯します。
2	ポート LED	ポート LED は、各 LED に対応するシリアルポートのステータス情報を
		提供します。
		◆ グリーンに点灯:オンライン状態 -ポートに接続されたシリアル機
		器に電源が入っており、準備ができていることを表しています。
		◆ グリーンに点滅:アクティブ - データがポートを介して転送中であ
		ることを表しています。
3	LAN LED	プライマリーおよびセカンダリーの 10/100/1000Mbps LAN LED です。
		◆ レッド:10Mbps
		◆ レッド+グリーン(オレンジ):100Mbps
		◆ グリーン: 1000Mbps
		◆ 点滅中は、シリアルコンソールサーバーが LAN 経由でアクセスさ
		れていることを表します。

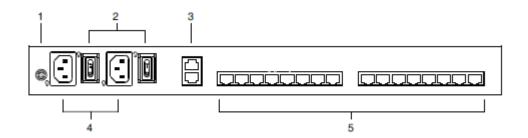
(表は次のページに続きます)

No.	名称	説明
4	リセットスイッチ	注意:このスイッチはくぼんでいるので、ペーパークリップの端やボー
		ルペンなどの小さなもので押し込む必要があります。
		◆ 製品の動作中に、このボタンを押して離すと、システムリセットを実
		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、設定内容
		をリセットし、工場出荷時のデフォルト設定に戻します。
		注意: この操作を行っても、ユーザーアカウントの情報は消去され
		ません。ユーザーアカウントの情報を消去する方法に関する詳細
		は、p.191「ログイン情報の消去」を参照してください。
		◆ このボタンを押したまま製品本体の電源を ON にすると、これまで
		にアップグレードされたファームウェアの内容を破棄して、工場出
		荷時におけるファームウェアバージョンに戻します。この操作によ
		って、ファームウェアアップグレードの失敗から回復して、アップグ
		レードを再度行うことができます。
		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。

SN0108CO リアパネル

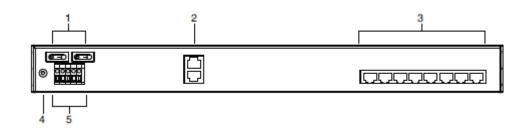


SN0116CO リアパネル

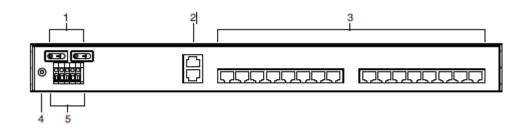


No.	名称	説明
1	グランドターミナル	製品本体を接地するための接地線をここに取り付けます。
2	電源スイッチ	製品本体に電源を入れたり切ったりするための標準的なロッカースイ
		ッチです。
3	LAN ポート	製品本体をプライマリーネットワークおよびバックアップネットワークイ
		ンターフェース(10/100/1000Mbps)に接続するケーブルを接続しま
		す。
4	電源ソケット	電源ケーブルを接続します。
5	シリアルポート	シリアル機器またはRJ-45→シリアルアダプターに接続するCat 5eケ
		ーブルを接続します。

SN0108COD リアパネル(DC 電源)

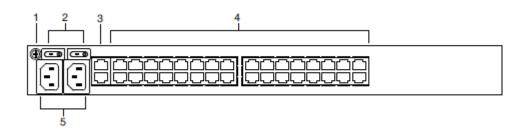


SN0116COD リアパネル(DC 電源)

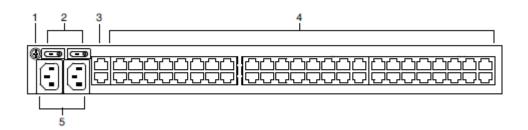


No.	名称	説明
1	電源スイッチ	製品本体に電源を入れたり切ったりするための標準的なロッカー
		スイッチです。
2	LAN ポート	製品本体をプライマリーネットワークおよびバックアップネットワー
		クインターフェース(10/100/1000Mbps)に接続するケーブルを接
		続します。
3	シリアルポート	シリアル機器または RJ-45→シリアルアダプターに接続する Cat
		5e ケーブルを接続します。
4	グランドターミナル	製品本体を接地するための接地線をここに取り付けます。
5	DCターミナルブロック	電源からのリードを、この DC ターミナルブロックに接続します。

SN0132CO リアパネル

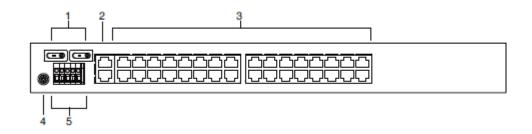


<u>SN0148CO リアパネル</u>

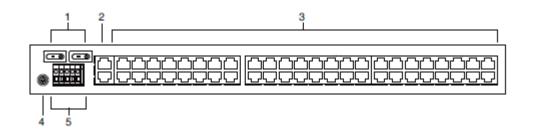


No.	名称	説明
1	グランドターミナル	製品本体を接地するための接地線をここに取り付けます。
2	電源スイッチ	製品本体に電源を入れたり切ったりするための標準的なロッカースイ
		ッチです。
3	LAN ポート	製品本体をプライマリーネットワークおよびバックアップネットワークイ
		ンターフェース(10/100/1000Mbps)に接続するケーブルを接続しま
		す。
4	シリアルポート	シリアル機器またはRJ-45→シリアルアダプターに接続するCat 5eケ
		ーブルを接続します。
5	電源ソケット	電源ケーブルを接続します。

SN0132COD リアパネル(DC 電源)

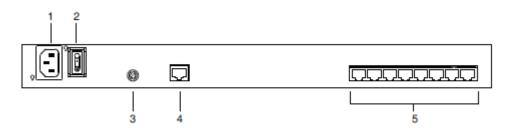


SN0148COD リアパネル(DC 電源)

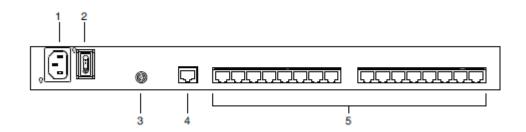


No.	名称	説明
1	電源スイッチ	製品本体に電源を入れたり切ったりするための標準的なロッカ
		ースイッチです。
2	LAN ポート	製品本体をプライマリーネットワークおよびバックアップネットワ
		ークインターフェース(10/100/1000Mbps)に接続するケーブル
		を接続します。
3	シリアルポート	シリアル機器または RJ-45→シリアルアダプターに接続する Cat
		5e ケーブルを接続します。
4	グランドターミナル	製品本体を接地するための接地線をここに取り付けます。
5	DC ターミナルブロック	電源からのリードを、この DC ターミナルブロックに接続します。

<u>SN9108CO リアパネル</u>



<u>SN9116CO リアパネル</u>



No.	名称	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ここに取り付けます。
4	LAN ポート	製品本体をネットワークインターフェース(10/100/1000Mbps)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



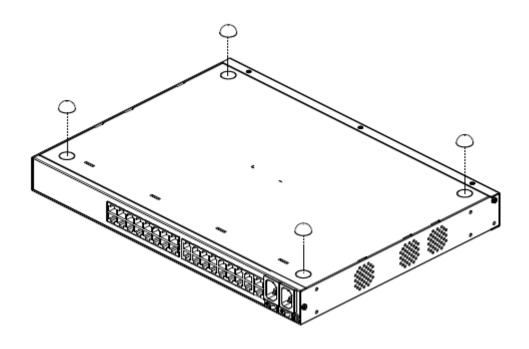
- 1. 機器の設置に際し重要な情報を p.9 に記載しています。作業の前に、必ず 目を通してください。
- 2. 今から接続するデバイスすべての電源がオフになっていることを確認してください。また、デバイスからは電源ケーブルも抜いておいてください。

卓上設置およびラックへの取付

シリアルコンソールサーバーは、卓上に設置することも、ラックに取り付けることもできます。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うる安定した水平な場所であれば、どんな場所にでも設置することができます。製品本体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。

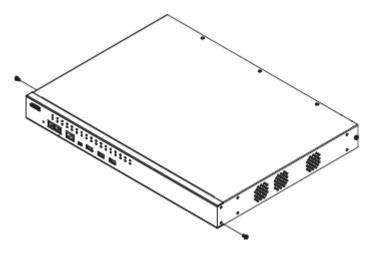
ラックへのマウント

シリアルコンソールサーバーは、19 インチ(1U)ラックに取り付けることができます。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ることができます。

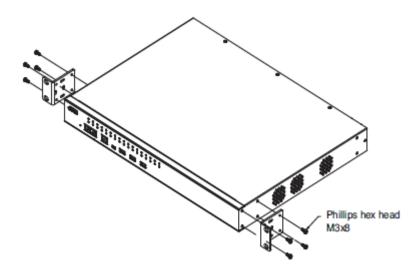
ラックのフロント側への取付

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を行ってください。

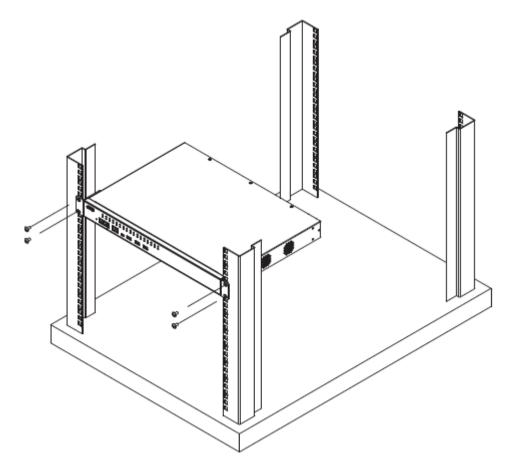
1. 製品本体のフロント側にある左右両方のネジ(合計2個)を外してください。



2. ラックマウントキットに同梱された 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。
- 4. 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。

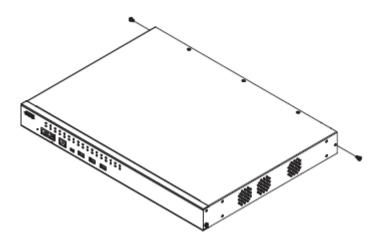


注意: ラックマウントキットにはネジとケージナットは同梱されていません。ネジとケージナット が必要な場合は、ラックの販売店までお問い合わせください。

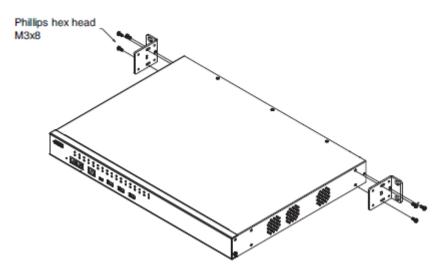
ラックのリア側への取付

製品本体をラックのリア側に取り付ける場合は、下記の手順にしたがって作業を行ってください。

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。

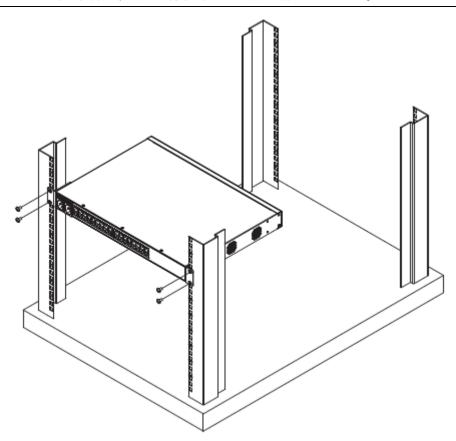


2. ラックマウントキットに同梱された M3 プラスネジ 8mm を使用して、製品本体で左右両方のリア 側にラックマウントブラケットをネジ止めしてください。



- 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。ネジとケージナット が必要な場合は、ラックの販売店までお問い合わせください。



シリアルコンソールサーバーのセットアップ

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.45 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。作業手順は下記のとおりです。

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(本体の背面に位置) 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。適切な接地をすることで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: ピンアサインに関する詳細は p.193「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 のピン定義がシリアルコンソールサーバーと一致していることを確認してください。

次は、互換性のあるネットワークスイッチの一例です: Juniper、HPE、Dell、Huawei、H3C、EdgeCore、TRENDnet、Fortinet、ATEN ES0152

- 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インストールする場合は、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。

ポートを接続できます。

- 6. (オプション) 電源管理を行う場合は、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行う場合は、Cisco 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ローカルコンソールサーバーと、コンソー ルターミナル(またはコンピューター)の DB-9 ポートを接続してください。 DB-9 コネクターのないコンソール端末またはコンピューターでは、UC232B 付きの Cat 5e ケ ーブルを使用して、ローカルコンソールポートとコンソール端末(またはコンピューター)の USB

注意: UC232B USB→RJ-45(RS-232)コンソールアダプターは別売りです。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。

- 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され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)シリアルコンソールサーバーで USB デバイス(USB ストレージデバイスなど)を使用している場合は、これらの3つのUSB Type-A メス ポートに接続してください。

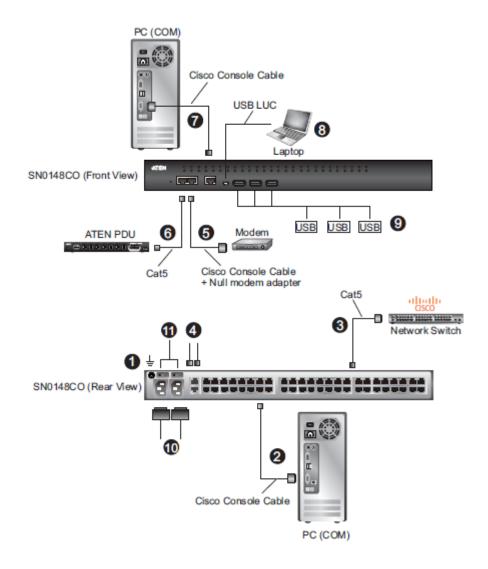
注意: USB ストレージデバイスでサポートされるファイルシステムは、FAT8、FAT16、FAT32です。

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 ON にしてください。

SN0108CO/SN0116CO/SN0132CO/SN0148CO 接続図



注意: 上図はシリアルコンソールサーバーSN0148CO を例にとったものです。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.26「製品各部名称」を参照してください。

SN9108CO/SN9116CO のセットアップ

お使いの SN9108CO/SN9116CO をセットアップする際には、p.47 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。作業手順は下記のとおりです。

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(本体の背面に位置) 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。適切な接地をすることで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 RI-45 ポートを接続してください。

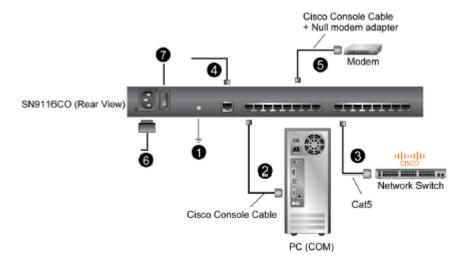
注意: ピンアサインに関する詳細は p.193「DB-9/DB-25 インターフェース」を参照してください。

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 のピン定義がシリアルコンソールサーバーと一致していることを確認してください。

- 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、製品背面にある 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インストールする場合は、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. 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 ON にしてください。

SN9108CO/SN9116CO 接続図



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。

初回セットアップ

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行う必要があります。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。この初回セットアップは、ローカルコンソール(ローカル VT コンソール、またはターミナルアプリケーションソフトウェアが動作しているローカルコンピューター)か、SN ビューワーUSB アプリケーションが動作しているラップトップ USB コンソール(LUC)を使うと、簡単に行えます(後者は SN0108CO / SN0116CO/SN0132CO/SN0148COのみ対応)。また、ユニットのIPアドレスを使用して、Web GUI 経由でリモートからセットアップすることもできます。

注意: ネットワークを設定するリモートアクセスの方法については、p.181「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

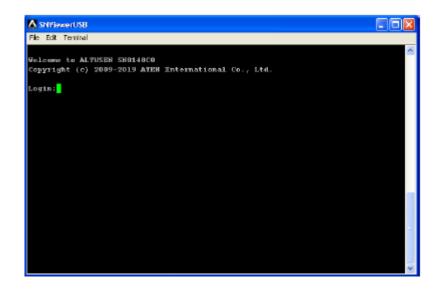
製品本体には、シリアルコンソールサーバーに直接接続されたコンピューターまたはノートパソコン(SN0108CO/SN0116CO/SN0132CO/SN0148CO のみ対応)からローカルログインすることができます(p.43「シリアルコンソールサーバーのセットアップ」参照)。ローカルログインには、SN ビューワーUSB とハイパーターミナルといった2種類の方法があります。

ローカルログインのメインメニューはテキストベースで提供されています。これは、本マニュアル全

体で説明しているブラウザベースの設定や管理機能と同等です。本章で説明する設定のサブメニューを操作する際には、必要に応じて Web ブラウザー版の詳細説明を参照してください(p.54「ブラウザーによるログイン」参照)。

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

ラップトップ USB コンソール (LUC) 接続 (SN0108CO/SN0116CO/SN0132CO/SN0148CO のみ対応) が確立されると、下図のような SN ビューワーUSB アプリケーションが表示されますので、このプロンプトからログインしてください。



初回ログインの際には、デフォルト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

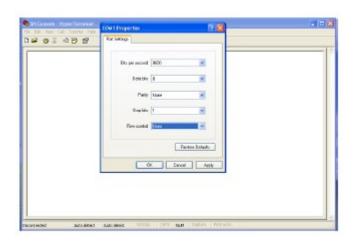
ログインすると、システムからパスワードの変更を促されますので、デフォルトとは異なるパスワード を設定してください。

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。

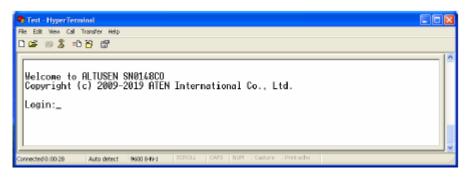
(※Windows7 以降は、市販の Telnet クライアントソフトをご利用ください。)

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行ってください。



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

2. 設定が正しく行われると、下図のようなログインプロンプトが表示されます。



初回ログインの際には、デフォルト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

ログインすると、システムからパスワードの変更を促されますので、デフォルトとは異なるパスワード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 ビューワーUSB でログインすると、テキストベースのメニューが表示されます。



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提供されています。これは、本マニュアル全体で説明しているブラウザベースの設定や管理機能と同等です。本章で説明する設定のサブメニューを操作する際には、必要に応じてWebブラウザー版の詳細説明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 Web ブラウザーを 使ってリモートログインすることができます。

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提供されています。これは、本マニュアル全体で説明しているブラウザベースの GUI や管理機能と同等です。本章で説明する設定のサブメニューを操作する際には、必要に応じて Web ブラウザー版の詳細説明を参照してください(p.54「ブラウザーによるログイン」参照)。

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。そうすると、下図のようなログインプロンプトが表示されます。



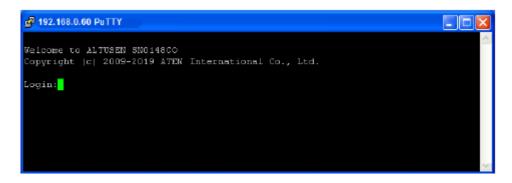
初回ログインの際には、デフォルトアドミニストレーターのアカウントを使用してください。 ユーザーネーム:administrator

パスワード:password

ログインすると、システムからパスワードの変更を促されますので、デフォルトとは異なるパスワード 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。そうすると、下図のようなログインプロンプトが表示されます。



初回ログインの際には、デフォルト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

ログインすると、システムからパスワードの変更を促されますので、デフォルトとは異なるパスワード を設定してください。

ブラウザーによるログイン

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することができます。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行ってください。

- 1. Web 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. 「セキュリティの警告」ダイアログボックスが表示されますが、この証明書は信頼できるものです 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、ログイン画面が表示されます。



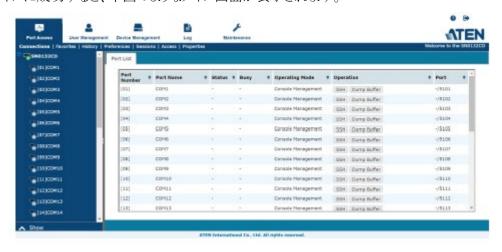
3. 初回ログインの際には、デフォルトアドミニストレーターのアカウントを使用してください。

ユーザーネーム:administrator

パスワード:password

ログインすると、システムからパスワードの変更を促されますので、デフォルトとは異なるパスワード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が表示されます。

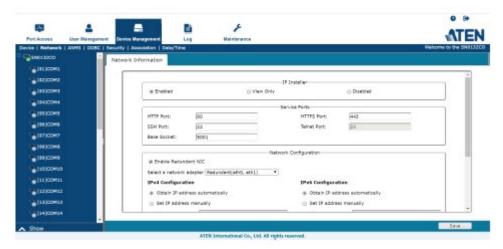


セットアップ

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行ってください。

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

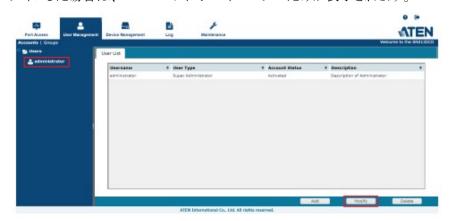


3. p.128「ネットワーク」に記載された情報に従って、各項目に値を入力してください。

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行ってください。

1. 画面上部にある「User Management」(ユーザー管理)タブをクリックしてください。
「User Management」(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提供するリストが表示されます。
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されます。



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) 「Modify」(変更)をクリックしてください。

そうすると、「User Information」(ユーザー情報)画面が表示されます。



- 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ことを確認するために、「Confirm Password」(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)「Save」(保存)をクリックしてください。
- 6. 正常に変更されたこと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されます。ページの外観は、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は、ターミナルアプリケーションソフトウェア (Microsoft のハイパーターミナルなど)や SN ビューワーUSB アプリケーションが動作しているローカルコンソール (ローカル側に接続されたコンピューターまたはノートパソコン) からでも操作できます。また、Telnet (SSH)、PuTTY、または Web ブラウザーを使ってリモートコンピューターからアクセスすることもできます (詳細については p.48「初回セットアップ」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されると、認証ルーティーンから、「Invarid Username or Password」(無効なユーザーネームまたはパスワード)や「Login Failed」(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が表示された場合は、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、再ログインすることができなくなります。詳細については、p.148「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がセットアップされていると(SN0108CO/SN0116CO/SN0132CO/SN0148CO のみ、p.43 参照)、ハイパーターミナルまたは SN ビューワーUSB のアプリケーションを使ってログインすることができます(詳細については p.48「ローカルログイン」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が表示されます。

```
SNØ148CO Main Menu

1. Preferences
2. User Management
3. Port Settings
4. Port Access
5. Device Management
6. Sessions
Q. Logout
Select one:
```

メインメニューはテキストベースで提供されています。これは、本マニュアル全体で説明している ブラウザベースの GUI や管理機能と同等です。本章で説明する設定のサブメニューを操作する際 には、必要に応じて Web ブラウザー版の詳細説明を参照してください。

注意:

- 1. ブラウザー版と同様に、これらのサブメニューの大半へのアクセスは、ユーザーの 操作権限によって制限されています。操作権限がないサブメニューにアクセスして も無効です。
- 2. 一部のサブメニューには終了メニューがありません。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すことができます。
- 4. このメニューは、Windows Telnet クライアントや PuTTY などのリモートターミナルセッションからもアクセスすることができます。

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、Webブラウザー、またはTelnetやPuTTYなどのテキストベースのターミナルアプリケーションを使ってリモートアクセスすることができます。詳細については、後続のセクションで説明します。

Web 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することができます。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行ってください。

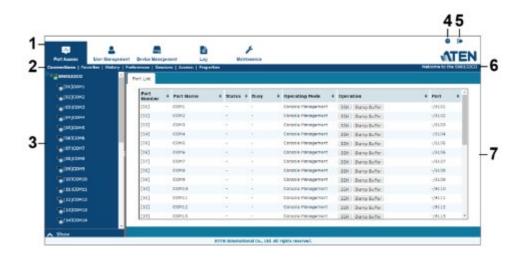
- 1. ブラウザーを起動し、アクセス対象となるシリアルコンソールサーバーの IP アドレス(詳細は p.54「ブラウザーによるログイン」を参照)をブラウザーの URL バーに入力してください。
- 2. 「セキュリティの警告」ダイアログボックスが表示されますが、この証明書は信頼できるものですので、受け入れてください。2 番目の証明書が表示された場合も、同様に受け入れてください。または「このサイトの閲覧を続行する(推奨されません)」をクリックすると、ログイン画面が表示されます。



3. ユーザーネームとパスワード(p.54「ブラウザーによるログイン」参照)を入力して、「**Login**」(ログイン)をクリックして、Web ブラウザーのメイン画面を開いてください。メイン画面については次のページで説明します。

Web 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 Web ブラウザーから操作できるようになっております。後続のセクションでは、Web 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.59 参照)、「Port Access」(ポートアクセス)タブが選択された状態で Web ブラウザーのメイン画面が表示されます。



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、表示されているすべ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

Web 画面における各部名称と説明は、下表のとおりです。

No.	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操作の主なカテゴリがメ
		ニュー別にタブ表示されます。タブバーに表示される項目は、ユーザ
		ーアカウントが作成された際に選択された権限オプションによって決ま
		ります。
2	メニューバー	メニューバーには、タブバーで選択された操作に関連するサブカテゴ
		リーが表示されます。この部分に表示される項目はユーザーアカウント
		が作成された際に選択された許可オプションユーザータイプやユーザ
		ーに与えられた権限によって決まります。

(表は次のページに続きます)

No.	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
		されます。サイドバーのノードをクリックすると、その詳細画面が表示さ
		れます。
		サイドバーの下にある「Filter」(フィルター)ボタンを使うと、ツリーに表
		示されるポートの範囲を変更することができます。
4	About	シリアルコンソールサーバーに現在インストールされているファームウ
	(バージョン情報)	ェアのバージョンに関する詳細が表示されます。
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	ウェルカム	この機能が有効になっている場合(p.87 参照)、ウェルカムメッセージ
	メッセージ	がこの部分に表示されます。
7	詳細表示パネル	メインの作業領域です。ここには、選択され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

ページ上部のタブバーに表示され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、ユーザーに付与された操作権限によって決定します。本章における後続のセクションでは、Web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とおりです。

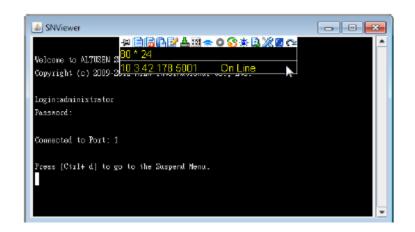
アイコン	機能
	Port Access (ポートアクセス): シリアルコンソールサーバーに接続されているデ
Port Access	バイスへのアクセス・操作を行います。このメニューはすべてのユーザーがアクセ
Pull Nobbas	ス可能です。本メニューの詳細については、p.77 を参照してください。
	User Management (アカウント): ユーザーやグループの作成・管理を行います。
	また、デバイスをユーザーやグループに割り当てることもできます。なお、これ
	は、スーパーアドミニストレーターと、ユーザー管理権限のあるアドミニストレータ
User Management	ーやユーザーのみアクセス可能なメニューです。こ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されません。 本メニューの詳細についてはp.106を
	参照してください。
	Device Management (設定): 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・管理を行います。なお、これはスーパーアドミニストレ
-	ーター、およびデバイス管理権限のあるアドミニストレーターやユーザーのみが
Device Management	アクセス可能なメニューです。これ以外のユーザーがログインした場合、このアイ
	コンは表示されません。本メニューの詳細については、p.123 を参照してくださ
	い。
E	Log (ログ): ログファイルの内容を表示します。 本メニューの詳細については、
Log	p.157 を参照してください。
	Maintenance (ファームウェア): 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
ع	ポートを行います。なお、これはスーパーアドミニストレーター(およびメンテナン
Maintenance	ス権限のあるアドミニストレーターとユーザー)がアクセス可能なメニューです。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されません。本メニュ
	ーの詳細については、p.162 を参照してください。

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とおりです。

アイコン	機能
Ð	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が表示されます。
	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ビューワー

SN ビューワーは、Web 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。SN ビューワーは「Port Access」(ポートアクセス)タブの「Connections」(接続)メニューからアクセスし、そこでシリアル機器に対して「Telnet」または「SSH」ボタンをクリックします(詳細はp.82「Telnet/SSH」を参照)。SN ビューワーを起動すると、マウスカーソルを動かしたときに表示されるコントロールパネルのツールバーが利用できます。これを使うと、セッションの設定を行うことができます。



SN ビューワーのコントロールパネル

SN ビューワーのコントロールパネルは、通常時は画面上部中央に隠れていますが、マウスカーソルをその場所に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 行から構成されています。



- ◆ デフォルトでは、上側のテキスト行にはウィンドウサイズの幅と高さが表示されます。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、その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、その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が自動的にポップアップ表示されます。
- ◆ 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されます。

コントロールパネルの機能

コントロールパネルの各機能は、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
	これはトグルボタンです。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
Jim	ます。言い換えれば、SN ビューワーの画面の上部に常に表示するということで
-	す。もう一度クリックすると、マウスカーソルと画面上部中央に移動させたときにの
	み表示させるという自動非表示モードで表示します。
	画面上で選択されたテキストをコピーします。
	画面上に表示されたすべてのテキストをコピーします。
	コピーされ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 ビューワーに送られたテキスト形式のログファイルを開始します。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.70「ターミナル設定」の「その他 - ログファイル」を参照)。
4	インポートするデータファイルを閲覧します(p.66「データのインポート」参照)。
0101	画面のエンコーディング方法を変更します(p.67「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、一つのポー
	トに対して行った変更を、すべてのブロードキャストポートに対して同様に適用す
	ることができます。ブロードキャスト機能を使用する前に、「Broadcast Timeout」
	(ブロードキャストタイムアウト)と「Broadcast Ports」(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.86「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
	V _o
0	ブレークコマンドを送信します。

(表は次のページに続きます)

アイコン	機能
8	ターミナルをリセットし、デフォルトの設定に戻します。
•	メッセージボード(p.67 参照)を起動します。
	ウィンドウを開いて、カスタムのテキストマクロ一覧を作成します(p.68「マクロ」参照)。
×	フォント、色、その他 SN ビューワーの設定を変更します(p.69「ターミナル設定」 参照)。
5	SN ビューワーのウィンドウ幅の調整を行います。
[™]	ビューワーを終了します。



<u> 基</u> データのインポート

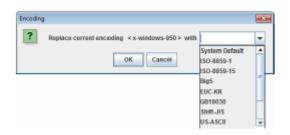
「Data Import」 (データのインポート) アイコンをクリックすると、下図のようにインポートする データを選択できる標準的なブラウザメニューが表示されます。



エンコード

이이

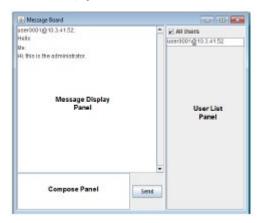
使用するエンコードの種類を選択することができます。下図のように、ドロップダウンメニューからエンコードの種類を選択して、「OK」をクリックしてください。



注意: 文字化けが発生した場合は、別のエンコードを試してみてください。例えば、ポートネームを日本語や韓国語、あるいは中国語(簡体字/繁体字)を使って設定していた場合は、エンコードをUTF-8にし、等幅フォントを使ってみてください。

<u>メッセージボード</u>

・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。このため、この問題の回避策として、メッセージボード機能を提供しています。これによって、ログインユーザーは相互にコミュニケーションを取ることができます。



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がこのパネルに表示されます。

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。「Send」(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されます。

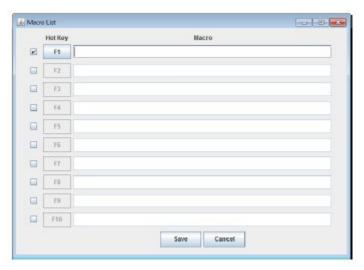
ユーザーリストパネル

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。

- ◆ 「All Users」(すべてのユーザー)にチェックを入れると、メッセージをすべ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、ユーザーの名前が選択された状態で再び全員宛にメッセージを送信したい場合は、「All Users」(すべてのユーザー)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 ビューワー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することができます。「Macro」(マクロ)アイコンをクリックすると、下図のような画面が表示されます。



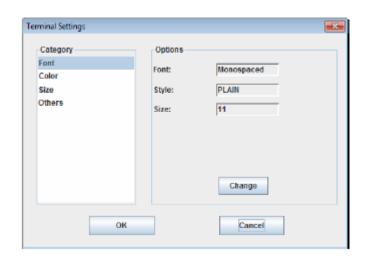
チェックボックスにチェックを入れて、テキストマクロに入力し、「Save」(保存)をクリックしてください。 作成したカスタムテキストマクロを動作させるには、このマクロに関連するファンクションキー(F1~ F12)を使ってください。

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することができます。接続やログインの方法については、p.52「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提供されています。これは、本マニュアル 全体で説明しているブラウザベースの設定や管理機能と同等です。サブメニューを操作する際に は、必要に応じて Web ブラウザー版の詳細説明を参照してください。

ターミナル設定

「Terminal Settings」(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	説明
Font	SN ビューワーのフォント設定を行う場合は「Change」(変更)をクリックしてくださ
(フォント)	い。フォントの種類やサイズ、またスタイルを変更することができます。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することができます。
Color	「Option」(オプション)を選択し、「Change」(変更)をクリックして色の設定を調整
(色)	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。
	色の詳細設定を行う場合は、「HSL」、「Swatches」(見本)、「HSV」の各タブを使
	用してください。
	タブの下には「Preview」(プレビュー) セクションがあります。ここでは、選択した色
	がどのように見えるのかを確認することができます。
	変更内容を保存する場合は「OK」をクリックしてください。変更内容を破棄して終
	了する場合は「Cancel」(キャンセル)をクリックしてください。また、デフォルトの色
	設定に戻す場合は「Reset」(リセット)をクリックしてください。
Size	表示される情報の量は、ウィンドウのサイズによって決まります。「Category」(カテ
(サイズ)	ゴリ) > 「Size」(サイズ)に進み、「Column」(列)と「Row」(行)の各欄の値を変更
	することで、SNビューワーのウィンドウサイズを調整してください。

(表は次のページに続きます)

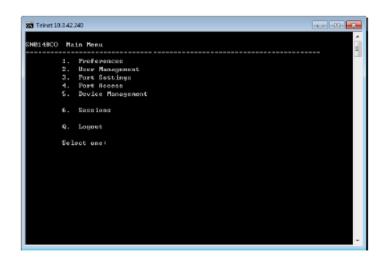
カテゴリ	説明
Others	このセクションは、次の設定を行う際に使用してください。
(その他)	◆ 「Implicit CR in every LF」(改行コードに CR+LF を使用する):このボックス
	にチェックを入れると、[Enter]キーが使用された際に CR(キャリッジリター
	ン)を付加します。このため、カーソルは左端の行頭に移動します。[Enter]
	キーを押した後でテキストが左側の余白で1行にならない場合は、この機能
	を使ってください。
	◆ 「Backspace」(バックスペース)は「Delete」(デリート)キーです。
	◆ 「Local echo」(ローカルエコー):エコーとは、シリアル機器から入力された文
	字列の応答のことです。
	➤ Auto(自動):入力された文字列がエコーされますが、画面には表示さ
	れません。
	➤ Force On(強制 ON):入力された文字列がエコーされ、入力されると画
	面にも表示されます。このモードでは、パスワードも画面に表示されま
	<u>す。</u>
	➤ Force Off(強制 OFF):文字列はシリアル機器からエコーされません。
	◆ Buffer Size (バッファーサイズ):ログファイルの最大容量です。
	◆ Log File(ログファイル):ログファイルは、接続されたシリアル機器から SN ビ
	ューワーに送られるテキストベースのログを生成します。ログは事前にノート
	や Microsoft Word などの外部エディターを使ってテキストファイルとして作
	成して開いておく必要があります。そのあと、SN ビューワーのコントロールパ
	ネルからログ機能を ON にする必要があります(p.65「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

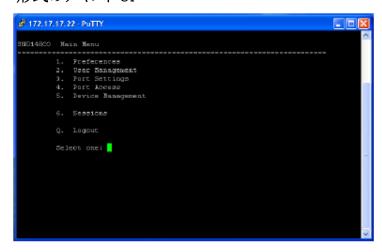
シリアルコンソールサーバーには、Telnet や PuTTY のようなテキストベースのターミナルアプリケーションを使ってリモートログインすることができます。接続やログインに関する詳細は、p.52「リモートログイン」を参照してください。

Telnet や PuTTY のメインメニューはテキストベースで提供されています。これは、本マニュアル全体で説明しているブラウザベースの設定や管理機能と同等です。サブメニューを操作する際には、必要に応じて Web ブラウザー版の詳細説明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が表示されます。

Telnet メニュー形式のテキスト UI



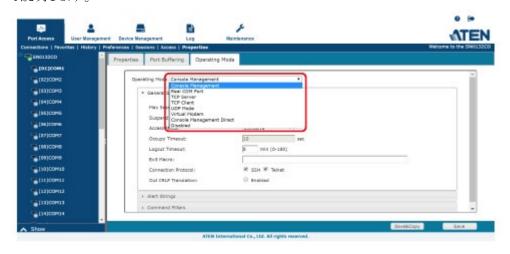
PuTTY メニュー形式のテキスト UI



第5章 ポート操作モード

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。この操作モードには、デバイス制御用の「Console Management」(コンソール管理) モードや「Console Management Direct」(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となるアプリケーションで使用される「Real COM Port」(リアル COM ポート)、「Virtual Modem」(バーチャルモデム)、「TCP Server」(TCP サーバー)、「TCP Client」(TCP クライアント)、「UDP Mode」(UDPモード)が含まれます。各操作モードによって実行される機能については、後続のセクションで説明します。



「Operation Mode」(操作モード)は、上図にあるように、「Port Access」(ポートアクセス)タブの「Properties」(プロパティ)メニューにある、「Operation Mode」(操作モード)の画面から選択することができます。本章で説明する「Port Operation Modes」(ポート操作モード)は、この画面から設定を行うことができます。すべての設定に関する詳細は、p.96「操作モード」を参照してください。

操作モード

各操作モードの設定に関する詳細は、p.96「操作モード」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、最も一般的に使われる動作モードです。ユーザーはこのモードを使うことで、シリアルコンソールサーバーに対して Telnet または SSH セッションを確立し、シリアル機器を管理することができます。このモードでは、ユーザーは Web ブラウザーで動作する SN ビュワーアプリケーションを使って Telnet または SSH 経由でログインすることができます。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 ビューワーUSB アプリケーションをそれぞれ使用して、ログインすることができます。

コンソール管理の設定に関する詳細は、p.96を参照してください。

注意: 「Network」(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ことを確認してください。シリアルコンソールサーバーでデフォルト設定されているポート番号は 5001 です(p.128「ネットワーク」、p.129「ベースソケット」参照)。

リアル COM ポート

このモードは、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されたバーチャル 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されると、そのポートに接続された機器は、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 ポートに直接接続された機器のように表示されます。

このモードは、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のデバイス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に同梱されたソフトウェア CD には、Windows 用のリアル COM ドライバー、および Linux 用の TTY ドライバーが収録されています。

リアル COM ポートの設定に関する詳細は、p.100 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を提供します。

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のリクエストを行います。

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されます。この操作モードは、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。これによって、複数のコンピューターがシリアル機器と同時に通信することが可能になります。

TCP サーバーの設定に関する詳細は、p.101 を参照してください。

注意: 「Network」(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ことを確認してください。シリアルコンソールサーバーでデフォルト設定されているポート番号は 5301 です(p.128「ネットワーク」、p.129「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、この操作モードは、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.102 を参照してください。

UDP モード

UDP (User Datagram Protocol)モードは、TCPよりも、より早く、そして、より効率的に通信を行います。UDP モードでは、コネクションレスな双方向通信を行います。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を行うことができます。

TCP が行う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された低速の TCP よりもリアルタイムアプリケーション(メッセージ表示など)に適しています。

UDP モードの設定に関する詳細は、p.103 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。これによって、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されたソフトウェアは、TCP/IP イーサネット接続でシリアル操作を実行することが可能になります。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。

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.186 に記載されています。

バーチャルモデムの設定に関する詳細は、p.103を参照してください。

注意: この操作モードは、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され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 セッションを確立することができます。このため、接続を確立するに あたり、Web 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 を使って PC から直接シリアルデバイスにログイン することができます。

コンソール管理ダイレクトの設定に関する詳細は、p.104を参照してください。

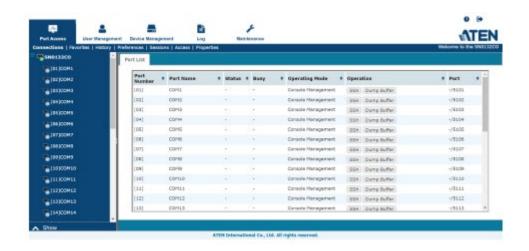
<u>無効</u>

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無効になります。

第6章 ポートアクセス

概要

Web 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、「Port Access」(ポートアクセス) タブの「Connections」(接続)メニューが選択された状態で、メイン画面が表示されます。

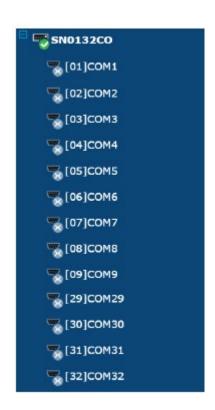


「Connections」(接続)画面は、複数の主要なエリアから構成されています。ユーザーがアクセス権限を持っている機器やポート、および、アウトレットはすべて、画面の左側にあるサイドバーに一覧表示されます。

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が表示される画面が開きます。

サイドバー

製品本体に接続されているシリアルコンソールサーバー、ポート機器や PDU 機器、また、これらのポートやアウトレットはすべて、画面左側にあるサイドバーにツリー形式で一覧表示されます。



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表示できます。
- ◆ 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状態であることを表します。

■ [02]COM2

◆ ポートがグリーンで、チェックマークが入っている場合、ユーザーによってアクセスされていることを表します。



◆ ポート/アウトレットや子機は、親機の下に入れ子にすることができます。機器の前についている「+」を押すとツリーが展開するので、入れ子になったアイテムを表示することができます。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/アウトレットが非表示になります。

フィルター

画面左下に「Show」(表示)という部分があります。これは、サイドバーに表示され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。「Show」(表示)をクリックすると、パネルの下部が下の図のように変わります。

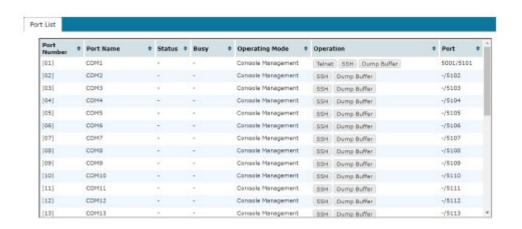


各項目の詳細は下表のとおりです。

項目	説明	
Search	検索したい文字列を入力して「Search」(検索)ボタンをクリックすると、	
(検索)	ポートネームがその文字列に一致するポートだけがツリーに表示され	
	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すること	
	ができます。以下、検索例です。	
	1. 「Web*」という文字列を入力して検索した場合、「Web Server 1」と	
	いう機器と、「Web Server 2」という機器がリストに表示されます。	
	2. 「 W*1 or M*2 」という文字列を入力して検索した場合、「Web	
	Server 1」という機器と、「Mail Server 2」という機器がリストに表示	
	されます。	

接続

「Connections」(接続)画面のメインパネルには、「Port List」(ポート一覧)が表示されます。ここからシリアル機器を選択し、接続ポートを介して接続することができます。



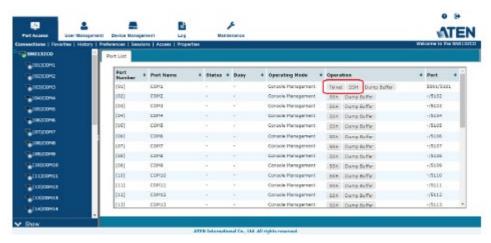
項目	説明
Port Number	機器が接続しているシリアルコンソールサーバー背面の物理ポートを表し
(ポート番号)	ます。
Port Name	ポートネームが表示されます。このポートネームは、「Port Access」(ポート
(ポートネーム)	アクセス)タブの「Properties」 (プロパティ)メニューで変更することができま
	す(詳細はp.92 参照)。
Status	ポートに接続されている機器の状態(ON または OFF)を表します。ポート
(状態)	に機器が接続されていない場合は、「-」が表示されます。
Busy	ポートがユーザーによってシリアルコンソールサーバー経由でアクセスさ
(ビジー)	れていると、この欄に「Busy」(ビジー)と表示されます。
Operation Mode	ポートにアクセスするために設定されている 操作モード が一覧表示されま
(操作モード)	す。最も一般的な設定は、「Console Management」(コンソール管理)で
	す。これは、「Port Access」(ポートアクセス)タブの「Properties」(プロパテ
	ィ)メニューにある「Operation Mode」 (操作モード)タブで設定することがで
	きます(詳細は p.96「操作モード」参照)。
	注意:コンソール管理は、コンソールサーバーに接続されているシリアル
	機器にアクセスして操作する方法です。

(表は次のページに続きます)

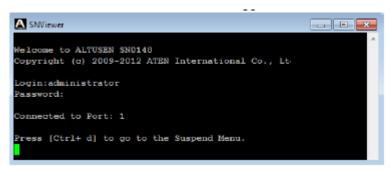
項目	説明
Operation	コンソール管理のアクセス方法を一覧表示します。
(操作)	Telnet および SSH:ポートデバイスを管理する方法です。いずれもクリック
	すると、SN ビューワーのアプリケーションが起動し、そのシリアル機器を管
	理することができます(下記の「Telnet/SSH」参照)。
	Dump Buffer(ダンプバッファー):この機器で発生したアクティビティーの
	バッファーログをダンプして確認することができます。ログを保存する場合
	は、クリックしてください(詳細は p.94「保存とコピー」を参照)。
Port	シリアル機器へのアクセス用に設定された Telnet とSSH の各ポート番号が
(ポート)	表示されます(詳細は p.129「サービスポート」参照)。

Telnet/SSH

シリアルサーバーに接続されたシリアル機器にアクセスするには、「Port Access」(ポートアクセス) 画面の「Connections」(接続)メニューで、そのポートの行に表示されている「Telnet」または「SSH」 のボタンをクリックしてください。



シリアルコンソールサーバーは SN ビューワーを開いて、シリアル機器とのセッションを開始します。 このとき、下図のような画面が表示されます。



シリアル機器へのログインや管理操作は、SNビューワーから行うことができます。SNビューワーの詳しい使用方法については、p.64「SNビューワー」を参照してください。

ポート属性

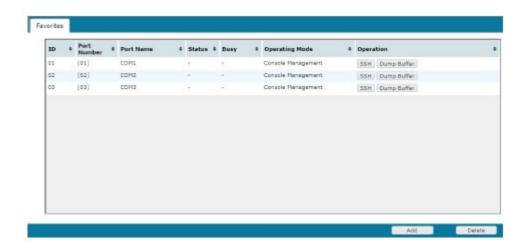
「Port Access」(ポートアクセス)タブの「Connections」(接続)メニューにあるサイドバーで機器をクリックすると、機器や電源管理デバイスのリブートオプションに関する詳細情報を提供する「Port Attributes」(ポート属性)画面が表示されます。



ここでは、画面の下側にある「Telnet」、「SSH」、「Dump Buffer」(ダンプバッファー)の各ボタンを使うことができます。

お気に入り

「Favorite」(お気に入り)タブは、頻繁にアクセスする接続をすべ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、「Add to Favorite」(お気に入りに追加)を選択するか、ポートを選択して「Add」(追加)をクリックしてください。「Favorite」(お気に入り)タブで利用できるレイアウトや機能は、「Port List」(ポートリスト)タブにあるものと全く同じです(詳細は p.80「接続」を参照)。



履歴

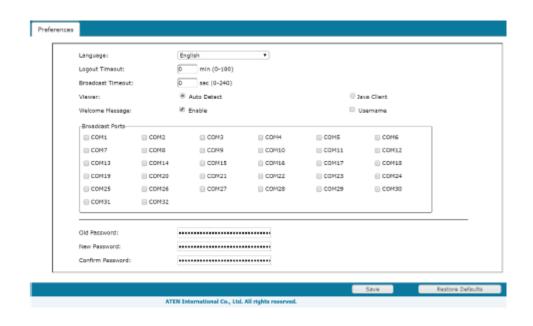
「History」(履歴)タブでは、ポートがアクセスされた記録を提供します。直近で使用されたポートには、ここから簡単にアクセスすることができます。メインパネルに表示されたポートには、「Telnet」または「SSH」の各ボタンを使ってアクセスします。



- ◆ 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が表示されますので、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「Delete」(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、その項目順に表示を変更します。

ユーザー設定

「Preferences」(ユーザー設定)画面では、ユーザー自身の個別の作業環境を設定することができます。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が個別に保存され、ログインダイアログボックスに入力されたユーザーネームに従って作業環境の設定を行います。



各項目の詳細は下表のとおりです。

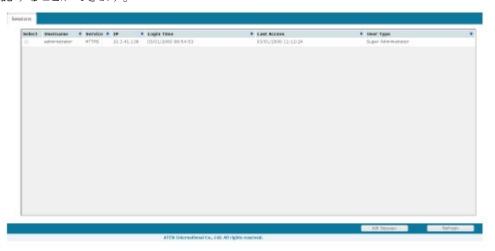
項目	説明
Language	Web GUI で使用する言語を選択してください。
(言語)	
Logout Timeout	ユーザーからの入力がないまま、この機能で設定された時間が経
(ログアウトタイムアウト)	過すると、ユーザーは自動的にログアウトさせられます。一旦ログ
	アウトすると、シリアルコンソールサーバーに再びアクセスするの
	に、またログインが必要になります。

(表は次のページに続きます)

項目	説明
Broadcast Timeout	ユーザーからの入力がないまま、この機能で設定された時間が経
(ブロードキャスト	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
タイムアウト)	の値を入力してください。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「Broadcast
	Port」(ブロードキャストポート)の欄を参照してください。
Viewer	シリアル機器へのアクセスに使用するビューワーを次から選択す
(ビューワー)	ることができます。
	◆ Auto Detect(自動検出):使用しているWebブラウザーに基
	づいて適切なビューワーを選択します。Windows Internet
	Explorer をお使いの場合は Win クライアントが、その他の
	Web ブラウザ (例:Firefox)をお使いの場合は Java クライアン
	トが、それぞれ選択されます。
	◆ Java Client (Java クライアント):使用ブラウザーの種類にかか
	わらず、Java ベースのビューワーを起動します。
Welcome Message	サブメニューバーのウェルカムメッセージやユーザーネームの表
(ウェルカムメッセージ)	示/非表示を選択することができます。 デフォルトでは無効に設定
	されています。
Broadcast Ports	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
(ブロードキャストポート)	定します。ブロードキャストポートを選択すると、あるポートに対す
	して行った変更を、他のブロードキャストポートすべてに対して適
	用することができます。
	注意:ブロードキャスト機能を動作させるには、SN ビューワーを使
	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 ON にしておく必要があります(p.65「コントロ
	ールパネルの機能」を参照)。
Save	「Save」(保存)をクリックすると、ユーザー設定メニューで行った変
(保存)	更内容を確定します。
Changing a Password	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
(パスワード変更)	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、「Change Password」(パスワードの変更)を
	クリックしてください。

セッション

「Sessions」(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や、これらのユーザーのセッション情報を確認することができます。



注意:

- 1. 一般ユーザーはこのメニューを利用することはできません。
- 2. 一般ユーザーのセッション情報を確認することができるのは、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、その項目順に表示を変更します。

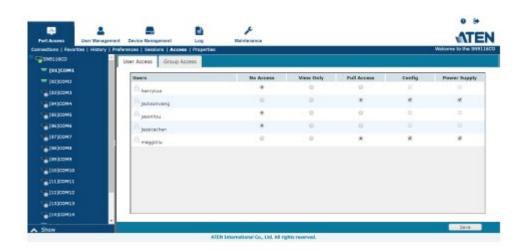
各項目の詳細は下表のとおりです。

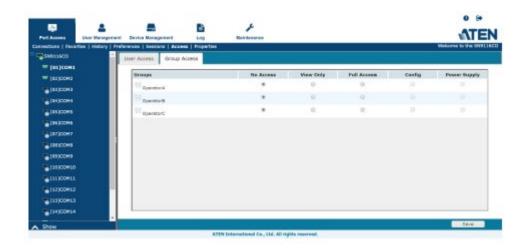
項目	説明
Username	ログイン中のユーザーを表します。
(ユーザーネーム)	
Service	ログインに使用されているセッションの種類(HTTP、HTTPS)を表示します。
(サービス)	
IP	ログインユーザーの IP アドレスを表します。
Login Time	ユーザーがログインした日時を表します。
(ログイン時刻)	
Last Access	ユーザーが前回システムにアクセスした日時を表します。
(前回のアクセス)	
User Type	ログインユーザーの種類を表します。ユーザーの種類は、SA(スーパーアド
(ユーザータイプ)	ミニストレーター)、Administrator(アドミニストレーター)、Normal User(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させることもできます。 対象となるユーザーを「Select」(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 「Kill Session」(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

「Access」(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したりするのに用いられる画面です。このメニューは、ユーザー管理の権限があるユーザーにのみ表示されますので、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することができます。グループやユーザーの設定方法については、p.106「ユーザー管理」を参照してください。



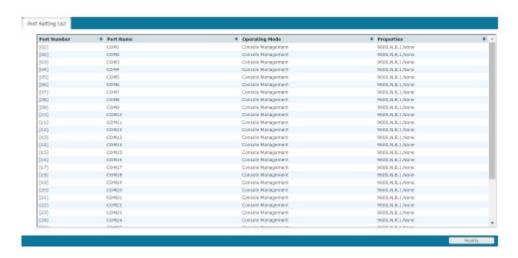


「User Access」(ユーザーアクセス)や「Group Access」(グループアクセス)のメニューで、ラジオボタンを使ってアクセス権限を設定してください。画面の表における各列の説明は、下表のとおりです。

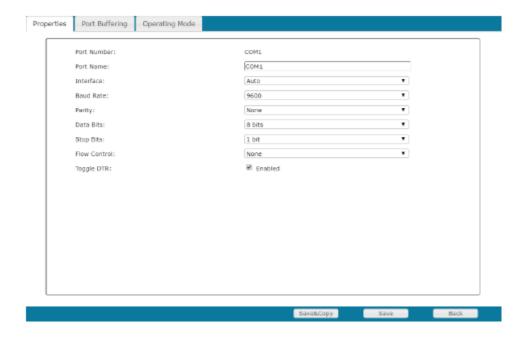
User Access	ミルマルコンハール	・ ・サーバーで作成された各ユーザー(スーパーアドミニス
00011100000	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	
(ユーザーアクセス)		が一覧表示されて、サイドバーに並んでいる各機器に対
	するアクセスや設定	定権限を定義することができます。サイドバーから機器を
	選択し、各ユーザ	ーに対してアクセスや設定権限を定義してください。
Group Access	シリアルコンソール	サーバー上に作成された各グループが一覧表示され
(グループアクセス)	て、サイドバーに並	並んでいる各機器に対するアクセスや設定権限を定義
	することができます	こ。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。
Access Rights	「Access」(アクセス)列では、アクセス権限を設定します。各項目が表す意	
(アクセス権限)	味は下記のとおり	です。
	Full Access	ユーザーは、デバイスの表示や、デバイスに対する操
	(フルアクセス)	作の実行ができます。
	View Only	ユーザーは、デバイスを表示することはできますが、
	(参照のみ)	デバイスに対して操作を実行することはできません。
	No Access	デバイスは、メイン画面のユーザーリストに表示されま
	(アクセス不可)	せん。
Config	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
(設定)	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が与え	
	られていることを表	しています。また、印が付いていない場合は、ユーザー
	に操作権限がない	ことを表しています。
Power Supply	この列では、シリアルコンソールサーバーに接続された電源管理デバイス	
(電源)	のポートで、設定や電源操作を行える権限があるかどうかを設定します。	
	チェックに印(🗸)	がついていると、ユーザーに操作権限が与えられている
	ことを表しています	⁻ 。また、印が付いていない場合は、ユーザーに操作権
	限がないことを表し	しています。

プロパティ

「Properties」(プロパティ)メニューをクリックすると、「Port Setting List」(ポート設定一覧)画面が表示されます。



ポートが「Port Setting List」(ポート設定一覧) やサイドバーからダブルクリックされると、下図のような「Properties」(プロパティ) 画面が表示されます。

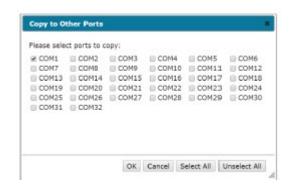


このパネルでは、選択されたポートに対して下表の項目を設定することができます。

設定	意味
Port 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
(ポートID)	ます。この欄は、現在設定しているポートを表しています。
Port Name	この欄にある文字列を編集して、ポートに名前を設定することができます。
(ポートネーム)	
Interface	「Auto」(自動)(デフォルト)、DTE、またはDCEのいずれかを選択します。
(インターフェース)	
Baud Rate	ポートのデータ転送速度を設定します。選択できる値は 300~230400 で
(ボーレート)	す(設定可能な値一覧は実際の画面にあるドロップダウンリストを参照)。
	この設定は、接続機器のボーレートの設定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。
Data Bits	データ1文字を転送するのに使用されるビット数を設定します。設定できる
(データビット)	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)に設定されています。
Parity	このパリティビットは、転送データの整合性をチェックします。設定できる値
(パリティ)	は、「None」(無)、「Odd」(奇数)、「Even」(偶数)です。この設定は、接続
	機器のパリティの設定に合わせてください。デフォルトでは「None」(無)
	(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。
Stop Bits	文字が転送されたことを表すビットです。この設定は、接続機器のストップ
(ストップビット)	ビットの設定に合わせてください。設定できる値は、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)に設定されてい
	ます。
Flow Control	これにより、データフローの制御方法を選択することができます。選択でき
(フローコントロール)	る値は「None」(無)、「Hardware (RTS/CTS)」(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「None」(無)に設定されています。
Toggle DTR	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
(DTR 切替)	ることができます。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

「Properties」(プロパティ)画面の右下にある「Save」(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、「Save & Copy」(保存とコピー)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することができます。



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

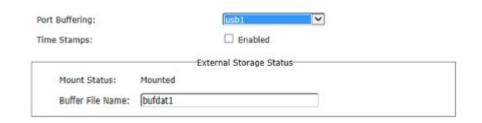
ポートバッファー機能は、ポートがアクセスされた時に発生したアクティビティーのログを作成します。ログはシリアルコンソールサーバー内のメモリーやUSBドライブに保存することができます。シリアルコンソールサーバー内部のメモリーは容量に限りがあるのに対し、USBドライブの場合は、より多くの容量を確保することができます。

注意: USB ドライブは SN01xxCO シリーズでのみ、ご利用いただけます。

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、「Memory」(メモリー)、「NFS」、「Syslog Server」(Syslog サーバー)のいずれかを選択するか、あるいはマウントされた USBドライブを選択してください。「Disable」(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、「Enable」(有効)のチェックボックスを使ってください。



マウントされた USB ドライブを選択した場合は、追加情報が表示されます。



「Buffer File Name」(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することができます。Syslog サーバー、NFS、およびマウントされた USBドライブの詳細については、p.123「デバイス」を参照してください。

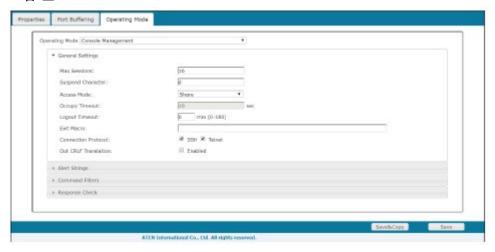
操作モード

「Operating Mode」(操作モード)の画面では、各ポートに対してアクセスや管理方法の設定を行うことができます。この項目によって、各シリアル機器に対して操作モードを使って、どのようにアクセスするかを定義します。各操作モードの設定に関する詳細は、p.73「操作モード」を参照してください。

Operating Mode (操作モード) - 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。最も一般的な設定は、「Console Management」(コンソール管理)です。これは、「Port Access」 (ポートアクセス)タブの「Connections」(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提供されている別のポート操作モードに関する詳細は、p.72「ポート操作モード」をご参照してください。

コンソール管理



◆ General Settings(基本設定)

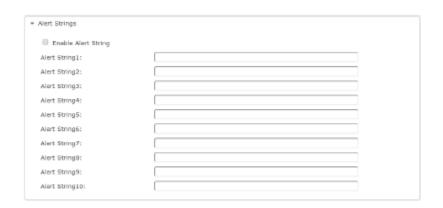
設定	意味
Max Sessions	ここでは、最大同時セッション数を設定します。
(最大セッション数)	
Suspend Character	サスペンド文字は、Telnet セッションでサスペンドメニューを起動
(サスペンド文字)	する際に用いられます。有効な文字は、H、I、J、Mを除くA~Zで
	す。

(表は次のページに続きます)

設定	意味
Access Mode	次のように、複数ユーザーでログインした場合のポートのアクセス
(アクセスモード)	方法について定義します。
	Exclusive(排他):ポートに最初に切り替えたユーザーは、そのポートに対して排他的にアクセスすることができます。他のユーザーはこのポートを参照することができません。また、このモードに設定されている場合、タイムアウト機能は適用されません。 Occupy(占有):ポートに最初に切り替えたユーザーは、そのポートに対してアクセスすることができますが、他のユーザーもそのポートを参照することができます。ポートを操作しているユーザーからの入力がないまま、「Occupy Timeout」(占有タイムアウト)の項目で設定され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。 Share(共有):複数のユーザーで同時にポートを共有して操作することができます。ユーザーからの入力はキューに格納され、古いものから順に実行されます。
Occupy Timeout	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
(占有タイムアウト)	で設定された時間が経過すると、ポートが開放され、別のユーザ
I T'	一が使用できるようになります。
Logout Timeout	ユーザーログインが必要とされないアプリケーションをお使いの
(ログアウト	場合、タイマーはユーザー操作によって設定されるため、
タイムアウト)	「Occupy Timeout」(占有タイムアウト)の設定が機能しないことが
	あります。この場合には、この「Logout Timeout」(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、設定した時間中にユーザギャン組み、ユーザー・パロ野やにコーザマネトを
	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
	せられます。ログアウト後に製品にアクセスするには、再ログイン
D :: 16	が必要です。
Exit Macro	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
(終了マクロ)	マクロをこの項目で設定することができます。
Connection Protocol	SSHやTelnetの接続プロトコルを有効/無効にするには、チェック
(接続プロトコル)	ボックスを使用します。
CRLF Translation	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
(CRLF 変換)	するかどうかを選択することができます。

◆ Alert Strings(警告文字列)

ポートの「Alert Strings」(警告文字列)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されている機器で発生した問題を通知する手段を提供しています。

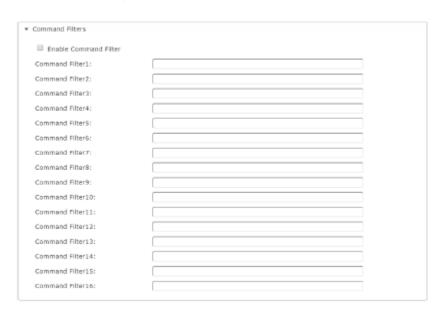


再起動が必要な重大なエラーやSNMPトラップのイベントが発生するなど、機器に何か問題が起こったときに、シリアルポートからシリアルコンソールサーバーの COM ポートにデバッグメッセージを送信することができます。

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、ここで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種類設定することが可能です。

この画面で設定を行うと、特定の警告が発生した際に通知が行われます。

◆ Command Filters (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することができます。

◆ Response Check(応答確認)



この項目を有効にすると、デバイスが正常に応答しているかをチェックすることで、システムが通常通り機能しているかどうかを確認することができます。

注意: この機能は、「Console Management」(コンソール管理) および「Console Management Direct」(コンソール管理ダイレクト) の各モードでのみサポートされます。

デバイスが応答しない場合は、「Response check failed」(応答確認エラー)の通知が送られます(この通知が有効になっている場合)。

Probe string(調査文字列): 応答確認のためにシステムから送信される文字列です。 デフォルトでは、¥x0D に設定されています(¥x0D は[Enter]を、¥x1B は[Esc]を、それぞれ表しています)。

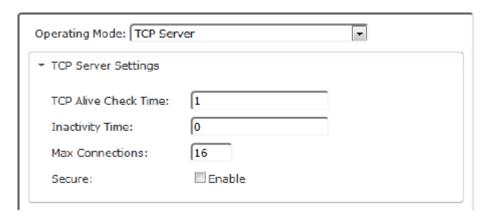
▶ Query frequency(クエリーの頻度):応答確認を送信する頻度です。デフォルトでは 30 (秒)に設定されています。値は 10~9999 の範囲で入力してください。

リアル COM ポート



「Enable」(有効)にチェックを入れると、このセッションで通信されるすべてのデータが暗号化されます。

TCP サーバー



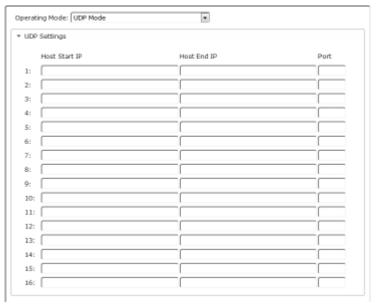
設定	意味
TCP Alive Check	この項目では、シリアルコンソールサーバーがホストコンピュータ
Time	ーに対して生存確認の判断のために TCP ソケット接続をチェック
(TCP 生存確認時間)	する頻度を設定します。この項目には、ホストコンピューターに対
	して TCP 接続をチェックするまでシリアルコンソールサーバーに
	待機させる時間(分)を入力してください。
Inactivity Time	この項目では、接続が中断されるまでにシリアルコンソールサー
(非アクティブ時間)	バーとホストコンピューターの間でデータ通信が行われない場合
	に、待機しなければならない時間を定義します。ここには、その時
	間(分)を入力してください。
Max Connections	ここには、許可される同時接続の最大数を入力してください。シリ
(最大接続数)	アルコンソールサーバーは最大 16 の同時接続を確立することが
	できます。
Secure	「Enable」(有効)にチェックを入れると、このセッションで通信され
(セキュア)	るすべてのデータが暗号化されます。

TCP クライアント



設定	意味
Secure	「Enable」(有効)にチェックを入れると、このセッションで通信さ
(セキュア)	れるすべてのデータが暗号化されます。
Destination Host/Port	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
(送信先ホスト/ポート)	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台のコンピューターに対してデー
	タを一斉送信することができます。

UDP モード



設定	意味	
Host Start IP/Host End	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。	
IP and Port	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	
(ホスト開始 IP/	番号を入力してください。	
ホスト終了 IP とポート)		

バーチャルモデム



「Enable」(有効)にチェックを入れると、このセッションで通信されるすべ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



◆ General Settings(基本設定)

設定	意味	
Max Sessions	最大同時セッション数を設定します。	
(最大セッション数)		
Suspend Character	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	
(サスペンド文字)	する際に用いられます。有効な文字は、H、I、J、M を除くA~Z で	
	す。	
Access Mode	次のように、複数ユーザーでログインした場合のポートのアクセス	
(アクセスモード)	方法について定義します。	
	Exclusive(排他):ポートに最初に切り替えたユーザーは、そのポ	
	ートに対して排他的にアクセスすることができます。他のユーザー	
	はこのポートを参照することができません。また、このモードに設定	
	されている場合、タイムアウト機能は適用されません。	
	Occupy(占有):ポートに最初に切り替えたユーザーは、そのポー	
	トに対してアクセスすることができますが、他のユーザーもそのポ	
	ートを参照することができます。ポートを操作しているユーザーか	
	らの入力がないまま、「Occupy Timeout」(占有タイムアウト)の項	
	目で設定され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。	

(表は次のページに続きます)

項目	説明	
Access Mode	Share(共有):複数のユーザーで同時にポートを共有して操作す	
(アクセスモード)	ることができます。ユーザーからの入力はキューに格納され、古	
- 続き	いものから順に実行されます。	
Occupy Timeout	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	
(占有タイムアウト)	で設定された時間が経過すると、ポートが開放され、別のユーザ	
	一が使用できるようになります。	
Logout Timeout	ユーザーログインが必要とされないアプリケーションをお使いの	
(ログアウト	場合、タイマーはユーザー操作によって設定されるため、	
タイムアウト)	「Occupy Timeout」(占有タイムアウト)の設定が機能しないことが	
	あります。この場合には、この「Logout Timeout」(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	
	せられます。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。	
Exit Macro	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	
(終了マクロ)	マクロをこの項目で設定することができます。	
Connection Protocol	SSHやTelnetの接続プロトコルを有効/無効にするには、チェック	
(接続プロトコル)	ボックスを使用します。	
CRLF Translation	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	
(CRLF 変換)	するかどうかを選択することができます。	

「Alert String」(警告文字列) および「Command Filter」(コマンドフィルター) に関する詳細は、p.98 を、「Response Check」 (応答確認) に関する詳細は p.99 をそれぞれ参照してください。

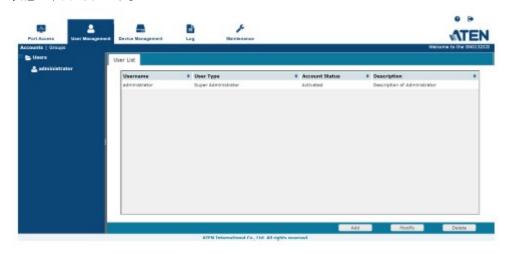
◆ Disabled(無効)

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

「User Management」(ユーザー管理)タブを選択すると、「Accounts」(アカウント)メニューが選択された状態で表示されます。



この画面は、左側のサイドバーと右側の大きなメインパネルといった2つの主な作業領域から構成されています。

- ◆ 画面左側のパネルにはユーザーとグループが表示されます。右側の大きなパネルには、ユーザーやグループのより詳しい情報が提供されます。
 - ▶ 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が別々に表示されます。選択されたメニューアイテムに応じて、ユーザーまたはグループがサイドバーに一覧表示されます。
- ◆ ブラウザーGUI では、メインパネルにある表の列名をクリックすると、情報の表示順を変更する ことができます。
- ◆ 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されます。

ユーザー

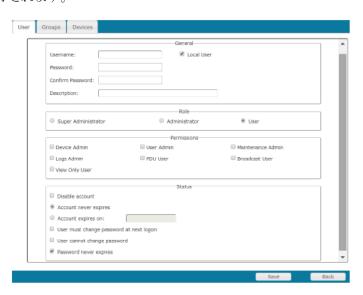
シリアルコンソールサーバーでは、以下の3種類のユーザータイプを提供しています。

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/デバイスへのアクセスおよび管理、ユーザー/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/デバイスへのアクセスおよび管理、ユーザ
	ー/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/デバイスへのアクセス、権限のあるポート/
	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が与えられている場合
	は、他のユーザーの管理を行うことができます。

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「Users」(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「Add」(追加)ボタンをクリックしてください。下図のような「User」(ユーザー)タブが表示されます。



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とおりです。

項目	説明		
Username	アカウントポリシーの設定に応じて、1~16 文字で設定してください。		
(ユーザーネーム)	(p.152 参照)		
Password	アカウントポリシーの設定に応じて、0~16 文字で設定してください。		
(パスワード)	(p.152 参照)		
Confirm Password	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。ここ		
(パスワード確認)	にはパスワードの欄に入力された文字列と同じものを入力してください。		
Description	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。		
(記述)			
Role	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		
(ロール)	の中から選択することができます。システム上作成可能なユーザー数の		
	範囲内であれば、各カテゴリとも作成するアカウントの数に上限はありま		
	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られているため、変更することはできません。		
	◆ 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すべての権限がデフォルトで与えられていますが、権限のチェックボックスにチェックを入れたり、ここからチェックを外したりすることで権限の設定を変更することができます。		
	◆ 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が デフォルトで与えられていますが、権限のチェックボックスにチェック を入れたり、ここからチェックを外したりすることで権限の設定を変更 することができます。		

(表は次のページに続きます)

項目	説明		
Permissions	◆ 「Device Admin」(デバイス管理)の項目にチェックを入れると、コンソ		
(許可)	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		
	可能になります(p.123 参照)。		
	◆ 「User Admin」(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・削除が可能になります。		
	◆ 「Maintenance」(メンテナンス)の項目にチェックを入れると、		
	「Maintenance」(メンテナンス)タブで提供されている操作がすべて		
	利用可能になります(p.162 参照)。		
	◆ 「Log Admin」(ログ管理)の項目にチェックを入れると、システムログ		
	へのアクセスが可能になります(p.157 参照)。		
	◆ 「PDU User」(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になります。		
	◆ 「Broadcast User」(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になります。		
	◆ 「View Only」(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。		

(表は次のページに続きます)

項目	説明			
Status	ユーザーアカウントとデバイスへのアクセスを管理することができます。詳			
(ステータス)	細は以下のとおりです。			
	◆ 「Disable Account」(アカウントを無効にする)の項目にチェックを入			
	れると、そのユーザーアカウントの使用を停止することができます。こ			
	の機能ではユーザーは実際には物理的に削除されませんので、後			
	に必要となった場合でも簡単に設定を戻すことができます。			
	◆ アカウントに有効期限を設けたくない場合は「Account never			
	expires」(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「Account expires			
	on」(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、「User must change password at next logon」(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。この項目を使うことで、初回ログインでは管理者によって発行さ			
	れ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することができます。			
	◆ 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、「User cannot change password」(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することが可能です。			
	パスワードに有効期限を設けない場合は、「Password never			
	expires」(パスワードを無期限にする)の項目を選択してくださ			
	い。これによって、ユーザーはパスワードの有効期限の制限を			
	受けることがありません。			
	▶ パスワードに有効期限を設ける場合は、「Password expires			
	after」(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。ここで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、メインパネルの「Groups」(グループ)タブで新しいユーザーをグループに登録することもできます(p.116 参照)。「Devices」(「デバイス」タブではユーザーにポートアクセス権限を割り当てることができます(p.120 参照)。

注意: グループの設定はここで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たりすることもできます。

- 5. 各項目への入力が終わったら「Save」(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」と表示されます。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「Users」(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が表示されます。
 - ◆ サイドバーのユーザーリストは展開したり閉じたりすることができます。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「+」マークが表示されます。「+」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をそれぞれ表します。
 - ◆ 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された説明、アカウントの状態(有効/無効)が表示されます。

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「User」(ユーザー)リストから、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. 「Modify」(変更)をクリックしてください。
- 3. メイン画面の「User」(ユーザー)タブで内容を変更したら、「Save」(保存)ボタンをクリックして その内容を反映させてください。

注意: 「User」(ユーザー)タブに関する詳細は p.107 に、「Groups」(グループ)タブに 関する詳細は p.116 に、「Devices」(デバイス)タブに関する詳細は p.120 にそれぞれ記載されています。

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、削除対象となるユーザーの名前を選択してください。
- 2. 「Delete」(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。

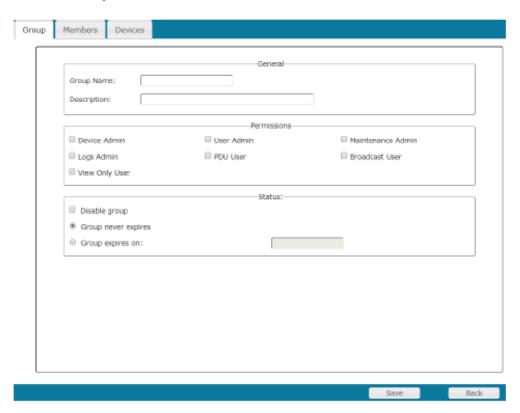
グループ

グループを使用すると、管理者はユーザーやデバイスを簡単かつ効率的に管理することができます。グループ単位で設定を行うことで、デバイスのアクセス権限はグループの全メンバーに適用されますので、管理者は個々のユーザーに対して権限を設定する手間が省けます。複数のグループを定義して、複数のユーザーに特定のデバイスへのアクセスを許可したり、反対に、特定のデバイスへのアクセスを禁止したりすることができます。

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「Groups」(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「Add」(追加)ボタンをクリックしてください。そうすると、グループメニューが開き、「Groups」(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とおりです。

項目	説明	
Group Name	最大 16 文字で設定してください。	
(グループネーム)		
Description	グループに関する付加情報があれば、最大 63 文字でこの欄に入力	
(説明)	してください。	
Permissions	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	
(許可)	スで個別に設定を行ってください。これらの権限は「Users」(ユーザ	
	ー)タブの権限と同じです。詳細は p.109 を参照してください。	

4. この時点で、「Members」(メンバー)タブで新しいユーザーをグループに登録することができます(p.118 参照)。「Devices」(デバイス)タブではグループにポートアクセス権限を割り当てることができます(p.120 参照)。

注意: グループの設定はここで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たりすることもできます。

- 5. 各項目への入力が終わったら「Save」(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」と表示されます。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「**Group**」(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が表示されます。
 - ◆ サイドバーのグループリストは展開したり閉じたりすることができます。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「+」マークが表示されます。「+」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され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の操作を行ってください。この操作を行わないと、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「Group」(グループ)リストから、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. 「Modify」(変更)をクリックしてください。
- 3. メイン画面の「Group」(グループ)タブで内容を変更したら、「Save」(保存)ボタンをクリックして その内容を反映させてください。

注意: 「Group」(グループ)タブに関する詳細は p.113 に、「Members」(メンバー)タブ に関する詳細は p.118 に、「Devices」(デバイス)タブに関する詳細は p.120 に それぞれ記載されています。

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、「Groups」(グループ)アイコンをクリックしてください。
- 2. グループの名前をメインパネルから選択してください。
- 3. 「Delete」(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、「Users」(ユーザー)タブ、「Group」(グループ)タブのどちらからでも操作することができます。

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.107「ユーザーの作成」を参照してください。

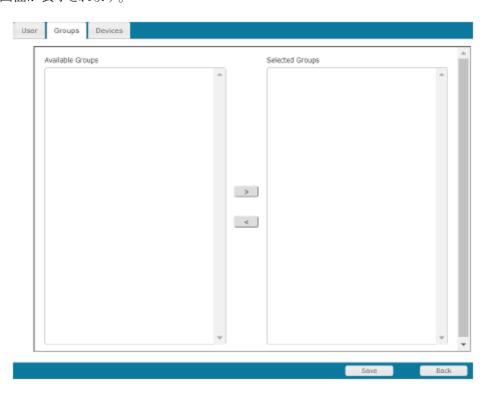
ユーザータブを使ってユーザーをグループに割り当てる場合

「Users」(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「User」(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. 「Modify」(変更)をクリックしてください。
- 3. メインパネルから「Groups」(グループ)タブを選択してください。タブを選択すると、下図のような画面が表示されます。



- 4. 「Available」(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「Selected」(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. グループの選択が完了したら、「Save」(保存)ボタンをクリックしてください。

注意: グループに設定された権限とは別の権限がユーザーに与えられている場合は、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

「User」(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「User」(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. 「Modify」(変更)をクリックしてください。
- 3. メインパネルから「Groups」(グループ)タブを選択してください。タブを選択すると、下図のような画面が表示されます。



- 4. 「Selected」(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。(選択されたグループは「Available」(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. ユーザーの選択が完了したら、「Save」(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登録する場合

「Group」(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、ユーザーの名前を選択してください。

- 2. 「Modify」(変更)をクリックしてください。
- 3. メインパネルから「Members」(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. 「Available」(有効)リストから、手順 1 で選択した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「Selected」(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. メンバーの選択が完了したら、「Save」(保存)ボタンをクリックしてください。

注意: グループに設定された権限とは別の権限がユーザーに与えられている場合は、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

「Group」(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「Group」(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. 「Modify」(変更)をクリックしてください。
- 3. メインパネルから「Member」(メンバー)タブを選択してください。タブを選択すると、下図のような画面が表示されます。



- 4. 「Selected」(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。(選択されたグループは「Available」(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. ユーザーの選択が完了したら、「Save」(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、「Port Access」(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、そのユーザーがアクセスを許可されたポートがすべて、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されたデバイスに対するアクセス 権限は、「User Management」(ユーザー管理)タブの「User」(ユーザー)または「Group」(グループ) リストからポートごとに割り当てられます。

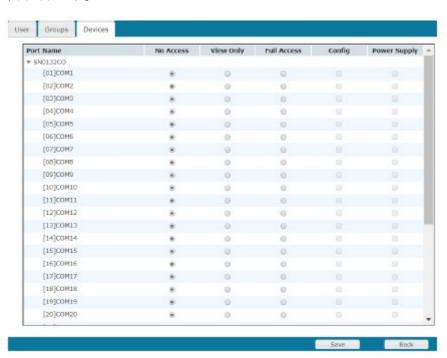
ユーザーメニューを使ってデバイスの操作権限を割り当てる場合

「User」(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. 「Modify」(変更)をクリックしてください。
- 3. メインパネルから「Devices」(デバイス)タブを選択してください。タブを選択すると、下図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行ってください。

「記を参考にしなから、谷小一トの惟政政定を行うしてたさい。				
項目	機能			
Name	現在操作しているユーザーがアクセスできるポートがこの列に表示され			
(名前)	ます。			
Access	デバイスへのアク	ウセス権限を設定します。これらの設定内容を切り替え		
(アクセス)	る場合は、設定を行い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	ンが表す意味は下記のとおりです。		
		ユーザーはリモート画面を参照することができます。		
	Full Access	また、ユーザー自身が使用しているキーボードとモニ		
	(フルアクセス)	ターを使ってリモートサーバーを操作することができ		
		ます。		
	View Only ユーザーはリモート画面を参照することができます			
	(参照のみ) が、操作をすることはできません。			
	No Access このポートへのアクセス権限はなく、ポートはユーザ			
	(アクセス不可) 一のメイン画面にも表示されません。			
Config	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			
(設定)	ユーザーがこの権限を持っていることを表します。また、チェックマーク			
	が入っていない場合は、ユーザーが設定変更の権限を持たないことを			
	表します。			
Power Supply	電源管理デバイスが接続されているポートの電源管理操作に関する権			
(電源)	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			
	限が与えられていることを表しています。また、印が付いていない場合			
	は、ユーザーに持	巣作権限がないことを表しています。		
	注意:この機能に	t 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、「Save」(保存)ボタン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することで複数のポートの属性を同時に定義することができます。選択されたポートで各列をクリックすると、その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

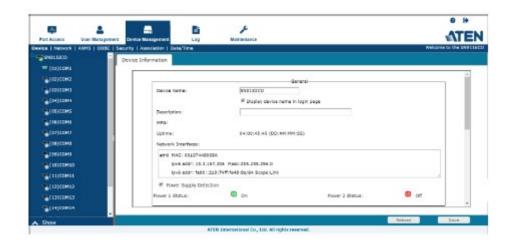
「Group」(グループ)タブを使ってデバイスの操作権限を割り当てる場合は、下記の手順に従って操作してください。

- 1. サイドバーの「Groups」(グループ)リストから、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. 「Modify」(変更)をクリックしてください。
- 3. 表示された「Group」(グループ)メニューから「Devices」(デバイス)タブを選択してください。
- 4. 表示される画面は、「User」(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、グループのすべてのメンバーに適用されることです。p.120「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

「Device Management」(デバイス管理)画面は、サイドバーで選択された最上位のシリアルコンソールサーバーが表示されます。このとき、このシリアルコンソールサーバーの配下にある全ポートは下に表示され、「Device Information」(デバイス情報)画面はメインパネルに表示されます。



全般

「Device Information」(デバイス情報)画面の「General」(全般)セクションでは、シリアルコンソールサーバーの「Device Name」(デバイス名)や「Description」(説明)を設定したり、「Manufacturing (MFG)」(製造)情報を参照したりすることができます。また、「Network Interfaces」(ネットワークインターフェースセクション)では、ネットワーク設定に関する情報を提供します。

ログイン認証情報を入力する部分の下にデバイス名を表示する場合は、「Display decive name in login page」(ログイン画面にデバイス名を表示する)の項目にチェックを入れてください。下図はその例です。



注意: 「MFG 番号」(製造番号)は、ATEN の工場や技術サポートのスタッフが製品を識別する際に使用する内部的なシリアル番号です。この番号が製品保証期間に影響することはありません。お使いの製品に関して購入後のサービスが必要な場合には、製品と型番を識別するために、ATEN の営業または技術サポートのスタッフに、この MFG 番号をお伝えください。

SN0108CO/SN0116CO/SN0132CO/SN0148CO は、冗長電源に対応しています。「Power Supply Detection」(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箇所の電源に関する情報が提供されます。

- ◆ 「Power Supply 1」(電源 1)と「Power Supply 2」(電源 2)のアイコンは、電源に対して電力が供給されていないときはグレーに、また、電源が供給されているときはブルーに、それぞれ表示されます。
- ◆ 「Power Supply Detection」(電源検知)機能が有効になっている(チェックボックスにチェックが 入っている)と、電源が片方にしか供給されなくなった場合に、シリアルコンソールサーバー側 でビープ音が鳴り、問題があることを通知します。デフォルトでは、この機能が有効になってい ます。

ローカルコンソール側で作業をしている場合は、電源供給が片方にしか行われていないことを 確認するメッセージが表示されます。もし、意図的に片方のみの電源で運用しているのであれ ば、このビープ音を止める方法は2つあります。

- 1) チェックボックスからチェックを外すことで電源の警告を無効にすることができます。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を行うことができます。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、システムリセットを行うと、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



「Mounted Devices」(マウントされたデバイス)セクションには、接続された USB および NFS ストレージデバイスに関する情報が表示されます。シリアルコンソールサーバーの前面に USB デバイス が接続されている場合 (SN0108CO/ SN0116CO/SN0132CO/SN0148CO のみ)や、NFS ストレージ のロケーションが設定されている場合 (下記の「NFS」設定を参照)、これらのデバイスは、マウントされたデバイスに関する詳細情報とともに表示されます。

NFS 設定

NFS Settings				
NFS Name	Source	Status	Auto	Operation
nfs1		N/A		Mount
nfs2		N/A		Mount
nfs3		N/A		Mount
nfs4		N/A		Mount

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することができます。「Source」(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、「Mount」(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。「Status」(状態)列には、「N/A」、「Mounted」(マウント済み)、「Unmounted」(マウント解除)のいずれかが表示されます。ストレージデバイスにアクセスできない場合には、「Unmounted」(マウント解除)と表示されます。このように表示された場合は、デバイスがネットワークでアクセス可能かどうか、また、「Source」(ソース)欄に入力した情報が正しいかどうか、それぞれ確認してください。NFSを自動マウントする場合は、「Auto」(自動)にチェックを入れてください。

外付け USB ドライブ

USB Name	Source	Status	Operation
usb1	USB3.0.FLASH DRIVE; Size: 15510536192	Mounted	Unmount
usb2		N/A	Mount
usb3		N/A	Mount

最大3台の外付けUSBドライブをマウントすることができます。ドライブのマウントを行う場合は「Mount」(マウント)を、また、ドライブのマウントを解除する場合は「Unmount」(マウント解除)を、それぞれクリックしてください。「Status」(状態)列には、「N/A」、「Mounted」(マウント済み)、「Unmounted」(マウント解除)のいずれかが表示されます。

なお、USB ストレージデバイスでサポートされるファイルシステムは、FAT8、FAT16、FAT32 です。

ポートログの Syslog 設定

	Syslog Settings for Port Logs		
✓ Enable Syslog			
Server IP/Domain:	10.15.8.12		
Syslog Category:	Local5	•	
Port:	513		
Protocol:	TCP	•	
	☐ Enable secure connection(SSL)		

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することができます。

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

上図に示された各項目に対して、サーバー情報の入力/選択を行ってください。

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**(項目にチェックなし)になっており、サーバーはデフォルトの命名規則に従ってポートネームを表示します(例: COM1、COM2 など)。

この機能が**有効**(項目にチェックあり)になると、サーバーは調査文字列を自動的に送信し、接続されたネットワークスイッチのポートネームを取得して表示します。ポートネームはデバイス情報(メーカーおよびモデル)に従って表示されます。

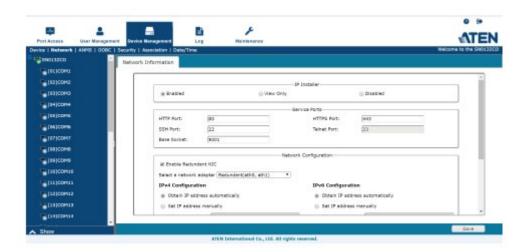
ネットワークスイッチを認識できない場合、サーバーはデフォルトの命名規則に従ってポートネームを表示します。

ネットワークスイッチで最初に検証が必要な場合、サーバーはデフォルトのポートネームをだけを表示します。ただし、認証情報が照合され、スイッチにログインした場合は、シリアルポートへの再接続を試行して、スイッチの情報を表示するためにサーバーがネットワークスイッチを認識できるかどうかを確認することができます。

互換性のあるネットワークスイッチの一例は次のとおりです: Juniper、HPE、Dell、Huawei、H3C、EdgeCore、TRENDnet、Fortinet、ATEN ES0152

ネットワーク

「Network」(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: 「Enable Redundant NIC」(冗長 NIC を有効にする)の項目は、SN0108CO/SN0116CO/SN0132CO/SN0148CO のシリアルコンソールサーバーでのみ、ご利用になれます。

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アドレスを設定することのできる、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、「Enable」(有効)、「View Only」(参照のみ)、「Disabled」(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.128 を参照してください。

注意:

- 1. 「View Only」(参照のみ)を選択した場合、シリアルコンソールサーバーは IP インストーラーのデバイスリストで確認することができますが、この IP インストーラーから IP アドレスを変更することはできません。
- 2. セキュリティを確保するために、IP インストーラーの使用後には、この項目を「View Only」(参照のみ)または「Disabled」(無効)に設定することを強く推奨します。

サービスポート

セキュリティ対策として、システムにファイアーウォールが導入されている場合、管理者はファイアーウォールの設定で許可されたポート番号をシリアルコンソールサーバー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。入力するポート番号が正しくなかったり、入力されていなかったりすると、シリアルコンソールサーバーを検索しても表示されません。各項目の内容は下表のとおりです。

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に設定されています。	
HTTPS	SSL 通信に使用するポート番号です。デフォルトでは443に設定されてい	
	ます。	
SSH Port	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 に設定され	
(SSH ポート)	ています。	
Telnet Port	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に設定され	
(Telnet ポート)	ています。	
Base Socket	TCP 接続をリッスンしたり受信したりするポートです。	
(ベースソケット)		

注意:

- 1. 各サービスポートで有効な値は 1~65535 です。
- 2. これらの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設置されている環境では、ネットワーク管理者とご相談の上、設定してください。

ネットワーク設定

◆ 冗長 NIC*

SN0108CO/SN0116CO/SN0132CO/SN0148CO には、ネットワークインターフェースを 2 ポート搭載しています。「Enable Redundant NIC」(冗長 NIC を有効にする)の項目が有効になっていると(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「eth 0」の IP アドレスを使用します。

この設定を行った場合、セカンドインターフェースは通常、非アクティブな状態になっています。 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. 「Enable Redundant NIC」(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. 「eth 0」がネットワークアダプターリストで選択され、リストボックスは無効になります (「eth 1」の項目は設定できません)。
 - 3. 「eth 0」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 アドレスを設定する ことができます。ユーザーは SN0108CO/SN0116CO/SN0132CO/SN0148CO へのアクセ スの際に両方の IP アドレスを使用することが可能です。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. 「Enable Redundant NIC」(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「eth 0」を選択してください。
 - 3. 「eth 0」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「eth 1」を選択してください。
 - 5. 「eth 1」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: SN0108CO/SN0116CO/SN0132CO/SN0148CO のシリアルコンソールサーバーでのみ利用可能です。SN9108CO/SN9116CO のシリアルコンソールサーバーを設定する場合は、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、IPアドレスを動的に割り当てる(DHCP)か、固定 IPアドレスを割り当てることができます。

◆ 動的 IP アドレスを割り当てる場合は、「Obtain IP address automatically」 (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、「Set IP address manually」(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. 「Obtain IP address automatically」(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された IP アドレス (192.168.0.60/61)に自動的に戻ります。
- 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されていて、なおかつ IP アドレスを確認する必要がある場合は、p.181 の「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、「Obtain DNS Server address automatically」(DNS サーバアドレスの自動取得)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、「Set DNS server address manually」(DNS サーバ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.184「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 アドレスを設定することも、固定 IPv6 アドレスを設定することも可能です。

- ◆ 動的 IP アドレスを割り当てる場合は、「Obtain IP address automatically」 (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、「Set IP address manually」 (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、「Obtain DNS Server address manually」(DNS サーバーアドレスの自動取得)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、「Set DNS server address manually」(DNS サーバ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。

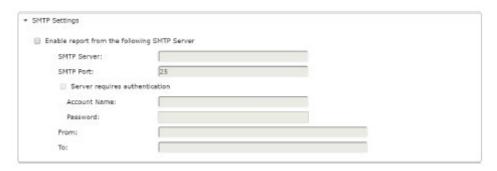
ANMS

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管理に関する設定を行います。このメニューは3つのタブから構成されており、各タブには下図のような関連パネルが表示されます。

イベントの宛先



◆ 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. 「Enable report from the following SMTP server」(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、「Server requires authentication」(サーバー認証が必要)の項目にチェックを入れて、「Account Name」(アカウント名)、「Password」(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. 「From」欄に設定できるメールアドレスは一つだけです。64 バイト以内で設定してください。

- 2. 1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

		▼ Log Server Settings				
Enable report from the following Log	g Server					
MAC Address:						
Service Port: 9	0001					

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、「Enable report from the following Log Server」(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 address」 (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「Service Port」(サービスポート)欄に入力してください。入力可能な値の範囲は 1~65535です。また、デフォルトでは 9001 に設定されています。

注意: このポート番号は、「Program」(プログラム)で指定され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

NMP Settings		
Enable SNMP Agent		
Community for Read:	public	
Enable SNMP Trap		
1. Trap Receiver:		
Receiver Port:	162	
Community:		
2. Trap Receiver:		
Receiver Port:	162	
Community:		
3. Trap Receiver:		
Receiver Port:	162	
Community:		
4. Trap Receiver:		
Receiver Port:	162	
Community:		
Enable SNMP V3		
SNMP V3 Account:		
SNMP V3 Password:		

注意: ♦ SNMP Trap は SNMP v1/v2c に対応しています。

◆ SNMP Agent は SNMP v1/v2c/v3 に対応しています。

SNMP 通知を使用したい場合は、下記の手順に従って設定を行ってください。

- 1. 「Enable SNMP Agent」(SNMP エージェントを有効にする)や「Enable SNMP Trap」(SNMP トラップを有効にする)の項目にチェックを入れ、「Community」(コミュニティー)欄に有効な値を入れてください。
- 2. SNMPトラップの設定を行ってください。SNMPトラップ関連のイベント通知を受けるコンピューターのIPアドレスを「Trap Receiver」(トラップレシーバー)欄に、また、サービスポート番号を「Receiver Port」(レシーバーポート)欄に、それぞれ入力してください。ポート番号の有効な値の範囲は1~65535です。デフォルトのポート番号は162です。

注意: 最大で4つの SNMPトラップレシーバーを定義することができます。ここには、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てください。

3. (SNMPエージェントのみ)SNMP v3を使用する場合は、「Enable SNMP V3」(SNMP V3を有効にする)の項目にチェックを入れてください。

注意: 認証プロトコルのクライアント設定として使用できるのは、SHAと AES-128 暗 号化のみです。

◆ Syslog サーバー

Enable Server IP:	▼ Syslag Server		
	□ Enable		
	Server IP:		
Service Port: 514	Service Port:	514	

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. 「Enable」(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

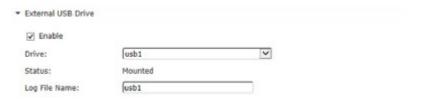


SMS で通知を受け取る場合は、下記の手順に従って設定してください。

- 1. 「Enable」(有効にする)の項目にチェックを入れてください。
- 2. 「Message Center」(メッセージセンター) および「SMS Receiver」(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「Save」(保存)をクリックしてください。

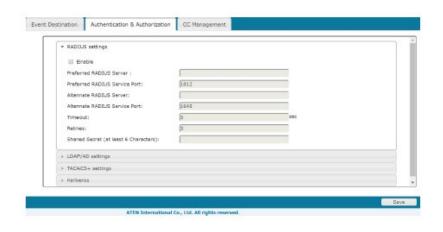
◆ 外付け USB ドライブ



シリアルコンソールサーバーで発生したすべ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. 「Enable」(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



◆ RADIUS 設定

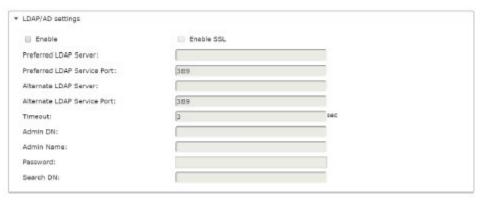
RADIUS サーバー経由でシリアルコンソールサーバーへの認証と権限設定を行う場合は、以下の手順で操作してください。

- 1. 「Enable」(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 で設定することができます。
- 3. 「Timeout」(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. 「Retries」(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. 「Shared Secret」(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を行うことができます。
 - ▶ 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際にユーザーに与えられ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された際に割り当てられた権限になります。(p.107「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	説明		
Enable	LDAP を有効にする場合は「Enable」(有効にする)の項目にチェ		
(有効にする)	ックを入れてください。また、LDAPS による認証と権限設定を有		
	効にする場合は、「Enable SSL」(SSLを有効にする)の項目にチ		
	ェックを入れてください。		
LDAP Server IP and	LDAP/LDAPS サーバーの IP アドレスやポート番号を入力してく		
LDAP Service Port	ださい。		
(LDAP サーバー	◆ 「LDAP Server」(LDAP サーバー)欄は、IPv4 アドレス、IPv6		
IP/LDAP サービスポー	アドレス、ドメイン名を使って設定できます。		
F)	◆ LDAP サーバーのデフォルトポート番号は 389、LDAPS サ		
	ーバーのデフォルトポート番号は 636 です。		

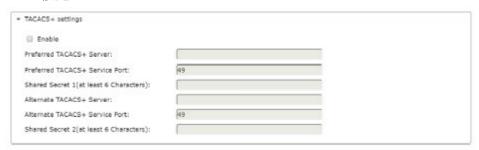
(表は次のページに続きます)

項目	説明
Alternate LDAP	代替 LDAP/LDAPS サーバーの IP アドレスやポート番号を入力
Server IP and LDAP	してください。
Service Port	◆ 「Alternate LDAP Server」(代替 LDAP サーバー)欄は、
(代替 LDAP サーバー	IPv4 アドレス、IPv6 アドレス、ドメイン名を使って設定できま
IP/サービスポート)	す。
	◆ 代替 LDAP サービスポートのデフォルトポート番号は 389、
	代替 LDAPS サービスポートのデフォルトポート番号は 636
	です。
Admin DN	この項目に入力する値は LDAP/LDAPS サーバーの管理者にご
(アドミニストレーターDN)	確認ください。以下、設定例です。
	ou=kn4132,dc=aten,dc=com
Admin Name	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
(アドミニストレーター名)	V ₀
Admin Password	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。
(パスワード)	
Search DN	検索ベースの識別名を設定してください。これはユーザーネー
(サーチ DN)	ムの検索を開始する DNS 名です。
Timeout	シリアルコンソールサーバーが LDAP/LDAPS サーバーの応答
(タイムアウト)	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を行うことができます。

- ◆ スキーマを使用せず、シリアルコンソールサーバーで使用されているユーザーネームだけを、 LDAP/LDAPS サーバー上の名前と照合させる。ユーザー権限は、シリアルコンソールサーバー側で定義されたものと同じ。
- ◆ スキーマを使用せず、Active Directory のグループだけを照合させる。ユーザー権限は、シリアルコンソールサーバー上で、そのユーザーが属しているグループに設定されている権限と同じ。
- ◆ スキーマを使用せず、Active Directory のユーザーネームとグループを照合させる。ユーザー 権限は、そのユーザーが属しているグループとユーザーに設定されている権限と同じ。

◆ TACACS+ 設定



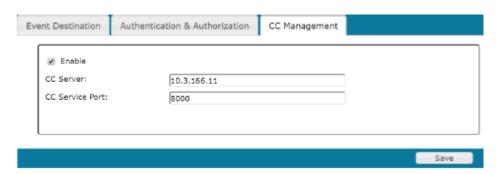
- ➤ TACACS+ を有効にし、次の情報を入力してください。
 - ◆ 優先 TACACS+ サーバー
 - ◆ 優先 TACACS+ サービスポート
 - ◆ 共有シークレット 1
 - ◆ 代替 TACACS+ サーバー
 - ◆ 代替 TACACS+ サービスポート
 - ♦ 共有シークレット 2

♦ 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行う場合は、「Enable」 (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 Server」(CC サーバー)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することができます。

注意: この機能が有効になっていると、シリアルコンソールサーバー上で電源管理デバイス が設定されていたとしても、これらのデバイスはサイドバーには表示されません。という のは、これらのデバイスが 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通常の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されたシリアルポート (SN9108CO/SN9116CO)を使うことでアクセスが可能です。



コンソールポートの設定

SN0108CO/SN0116CO/SN0132CO/SN0148CO

Baud Rate:	9600	ville Port Settings	
Parity:	None	•	
Data Bits:	5 bits	•	
Stop Bits:	1 bit	*	
Flow Control:	None	*	
		PP Settings	
Modern Settings			
Initialization String:			
PPP Dial In Settings			
Enable Dial In / Dial Back			
Enable Dial Back			
® Fixed Dial Back Numi	ber		
Flexible Dial Back (A	Now the caller to set the ca	liback number)	
PPP Server:			
PPP Cilent:			
PPP Dial Out Settings			
Enable Dial Out			
ISP Settings			
Access Phone Number:			
Username:			
Password:			
Dial Out Schedule			
® Every	2 Hours *		
Daily at		(HH:MM)	
PPP online time:	30	minute(s)	
Emergency dial out			
PPP keeps online until r	network recovered		
® PPP online time	30	minute(s)	
Mail Configuration			
SMTP Server:			
SMTP Port:	25		
Server requires author	ntication		
Account Name:			
Password:			
From:			
			1

SN9108CO/SN9116CO

	Console Po	ort Settings			
Port Number	Disable	7			
Baud Rate:	115200	,			
Perity:	None	*			
Deta Bits:	5 bits	¥			
Stop Bits:	1 bit	*			
Flow Control:	None	,			
	DON 5	ettings			
Port Number	Disable	*			
lodem Settings	PPP S	ettings			
Port Number	Dizable	•			
Initialization String:	D. SEDIO		-		
-					
PPP Dial In Settings Enable Dial In / Dial Back					
Enable Dial In / Dial Back					
Fixed Dial Back Numb					
	er low the caller to set the callbac	h			
PPP Server:	10.3.166.100	x number)			
PPP Clant:	10.3.166.200				
PPP Dial Out Settings Enable Dial Out					
ISP Settings					
Access Phone Number:					
Username:					
Password:					
Dial Out Schedule					
® Every	2 Hours *				
		HH:MH)			
Daily at		HH:MPI)			
Daily at PPP online time:		ninute(s)			
PPP online time:	[30 n				
PPP online time: Emergency dial out	SD n				
PPP online time: Emergency dial out PPP keeps online until n	SD n	ninute(s)			
PPP online time: Emergency dial out PPP keeps online until n PPP online time	SD n	ninute(s)			
PPP online time: Emergency dial out PPP keeps online until n PPP online time Mail Configuration	SD n	ninute(s)			
PPP online time: Emergency dial out PPP keeps online until n PPP online time Mail Configuration SMTP Server:	30 n etwork recovered 30 n	ninute(s)			
PPP online time: Emergency dial out PPP keeps online until n PPP online time Mail Configuration SMTP Server: SMTP Ports	30 n etwork recovered 30 n	ninute(s)			
PPP online time: Emergency dial out PPP keeps online until n PPP online time Mail Configuration SMTP Server: SMTP Port: Server requires authern	30 n etwork recovered 30 n	ninute(s)			

SN9108CO/SN9116CO の背面で、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、SN9108CO/SN9116CO のコンソールポートのポート番号が無効になっています。

ダイヤルバックを有効にする

アウトオブバンドアクセスを有効にすると、次のセクションで説明されているように、「Enable Dial Back」(ダイヤルバックを有効にする)や、「Enable Dial Out」(ダイヤルアウトを有効にする)の項目が使用可能になります。新たに追加されたセキュリティ機能として、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、下表で定義されたエントリ

ーの1つにダイヤルバック接続します。

項目	説明
Enable Fixed	「Enable Fixed Number Dial Back」(固定番号へのダイヤルバックを
Number Dial Back	有効にする)の項目が有効になっていると、シリアルコンソールサー
(固定番号へのダイヤルバ	バーは着電があった際に、モデム接続を切断し、ここで設定された
ックを有効にする)	電話番号のモデムにダイヤルバック接続します。「Phone Number」
	(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。
Enable Flexible Dial Back	フレキシブルダイヤルバックが有効になっていると、シリアルコンソ
(フレキシブルダイヤルバッ	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
クを有効にする)	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する
	ことができます。
	1. ユーザーが「Password」(パスワード)欄に指定しなければなら
	ないパスワードを入力してください。
	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
	「Username」(ユーザーネーム)欄に、また、パスワードを
	「Password」 (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

ダイヤルアウト機能を使用する場合は、ISP(インターネットサービスプロバイダー)と契約を結び、 この ISP で発行されたアカウントに対して、モデム経由でダイヤルアップ接続してください。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	説明
ISP Settings	お使いの ISP に接続する際に使用する、電話番号、アカウントネ
(ISPの設定)	ーム(ユーザーネーム)、パスワードをそれぞれ該当欄に入力して
	ください。

(表は次のページに続きます)

項目	説明
Dial Out Schedule	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
(ダイヤルアウト	度を設定します。
スケジュール)	◆ 「Every」(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
	ウト接続を行います。
	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「Never」
	(なし)を選択してください。
	◆ 「Daily」(毎日)のラジオボタンを選択すると、指定された時
	刻に日次でダイヤルアウト接続を行います。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 online time」(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。
Emergency Dial Out	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
(緊急ダイヤルアウト)	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す
	ることができます。
	◆ 「PPP stays online until network recovery」(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 online time」(PPP オンライン時間)を選択すると、ここ
	で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。

(表は次のページに続きます)

	説明
Mail Configuration	このセクションでは、シリアルコンソールサーバーのポートに接続
(メールの設定)	された機器で問題が発生した場合に通知するメールに関連した
	パラメーターを設定することができます(p.133「SMTP 設定」参
	照)。
	TRY.
	 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行うため、p.133 で説明し
	た SMTP 設定での通知機能とは若干異なります。
	◆ 「SMTP Server」(SMTP サーバー) 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 Port」(SMTP ポート)欄に、SMTP サーバーのポート
	を入力してください。 デフォルトは 25 番ポートです。 ポート
	番号がご不明な場合は、お使いの SMTP サーバーの管理
	者の方にご確認ください。
	◆ サーバーで認証が必要とされる場合は、「SMTP server
	requires authentication」(SMTP サーバーは認証が必要)の
	項目にチェックを入れて、認証に適切なアカウント名とパス
	ワードを該当欄に入力してください。認証アカウントやパス
	ワード、また、認証の必要性の有無がご不明な場合は、お
	使いの SMTP サーバーの管理者の方にご確認ください。
	◆ 「From」欄に、SMTP サーバーの責任者またはアドミニストレ
	ーターと同等の権限を持ったユーザーのメールアドレスを
	入力してください。
	◆ 「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、「Save」(保存)ボタンをクリックしてください。

セキュリティ

「Security」(セキュリティ)メニューは、以下のセクションで説明するように、4 つのメインパネルから構成されています。

ログイン失敗

セキュリティを強化するために、このセクションでは、ユーザーのログイン失敗を処理する際に 適用されるポリシーを設定することができます。



これらのポリシーを設定する場合は、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とおりです。

項目	説明
Login Fail Policy	ここで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
(ログイン失敗ポリシー)	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失
	敗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
	理のいずれかを行うことができます。
	◆ Disable User Account (ユーザーアカウントを無効にする)
	◆ IP Address Locked (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、「Lockout Period」(ロック
	アウト期間)の項目で設定します。
Maximum login Failures	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
(最大ログイン試行回数)	行できる回数を設定します。
Lockout Period	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
(ロックアウト期間)	時間、または IP アドレスがロックされ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有効になっていない場合、ユーザーは無制限で何度でもログインを試行することが可能になってしまいます。セキュリティ上の理由から、この機能を有効にし、ロックアウトポリシーを有効にすることを推奨します。

セキュリティレベル

セキュリティを強化するために、「High」(高)、「Medium-high」(中高)、「Medium」(中)または「Custom」(カスタム)のラジオボタンを選択してください。「Custom」(カスタム)を選択した場合は、その下にある項目を必要に応じて有効/無効にしてください。



- 1. High(高) SSHv2、HTTPS(TLS v1.2)を除く、すべてのサービスを無効にします。
- 2. Medium-high(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. Medium(中) SSHv2、HTTP から HTTPS へのリダイレクト、HTTPS(TLS v1.0、1.1、1.2)、SNMP エージェント、ICMP を有効にします。(**デフォルト**)
- 4. Custom(カスタム) 次のセキュリティ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。
 - ◆ Enable Telnet service (Telnet サービスを有効にする)
 - ◆ Enable SNMP Agent service (SNMP エージェントサービスを有効にする)
 - ◆ Enable ICMP service (ICMP サービスを有効にする)
 - ◆ Enable SSH service (SSH サービスを有効にする) (デフォルトで選択状態)
 - ◆ Enable HTTP and redirect to HTTPS(HTTP および HTTPS へのリダイレクトを有効にする)(デフォルトで選択状態)
 - ◆ HTTPS SSL/TLS version(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」の中から選択してください。

動作モード

セキュリティを強化するために、ここにあるチェックボックスを使って、暗号化モジュールの「FIPS 140-2」のセキュリティ機能を有効にすることができます。



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、あるいはその両方に基づいて、シリアルコンソールサーバーへのアクセスを制御するものです。フィルターは IP、MAC 各フィルターともそれぞれ最大で 100 項目作成することができます。フィルターは設定されると、IP フィルターの場合は上部のリストボックスに、MAC フィルターの場合は下部のリストボックスにそれぞれ表示されます。

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。

- ➤ 「Include」(含む)ラジオボタンが選択されている場合は、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。それ以外のアドレスからのアクセスはすべて拒否されます。
- ➤ 「Exclude」(除く)ボタンが選択されている場合は、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。それ以外のアドレスからのアクセスはすべて許可さ 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. 「**Add**」(追加)ボタンをクリックしてください。そうすると、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. 「**Add**」(追加)ボタンをクリックしてください。そうすると、下図のようなダイアログが表示されます。



- 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. 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。

◆ IP フィルターと MAC フィルターの競合

あるコンピューターがIPアドレスによるフィルタリングではアクセスが許可されているにもかかわらず、MACアドレスによるフィルタリングではアクセスが禁止されているといったように、フィルタリングの内容に矛盾がある場合、ブロックのフィルターが優先されるため、そのコンピューターからのアクセスはブロックされます。

◆ フィルターの変更

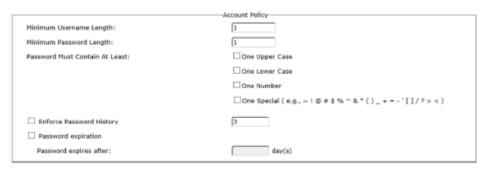
フィルターを変更する場合は、対象となる項目を IP フィルターリスト、または MAC フィルターリストのボックスから選択し、「Modify」(変更)をクリックしてください。この変更ダイアログボックスは、追加時のダイアログボックスに似ています。表示されたら、古いアドレスを削除し、新しいアドレスに置き換えてください。

◆ 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、「Delete」(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することができます。



このセクションにおける各項目の内容は下表のとおりです。

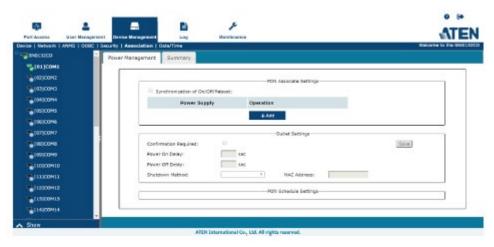
	-
項目	説明
Minimum Username Length	ユーザーネームの設定に最低限入力が必要な文字数を設定
(ユーザー名最小文字数)	します。設定できる値は1~16です。デフォルトでは6に設定さ
	れています。
Minimum Password Length	パスワードの設定に最低限入力が必要な文字数を設定しま
(パスワード最小文字数)	す。 設定できる値は 0~16 です。 0 を設定した場合は、パスワ
	ードの入力が不要です。この場合、ユーザーはユーザーネー
	ムだけでログインできるようになります。デフォルトでは6に設定
	されています。

(表は次のページに続きます)

項目	説明
Password Must Contain At	これらの項目にチェックを入れると、パスワードに含めなければ
Least	ならない文字の条件を追加することができます。
(パスワードには以下が必須	
です)	One Upper Case(大文字 1 文字)
	- 半角英字の大文字を1文字以上入力
	One Lower Case (小文字 1 文字)
	- 半角英字の小文字を1文字以上入力
	One Number
	- 数字1文字 - 半角数字を1文字以上入力
	One Special Character
	- 記号1文字 - 半角記号を1文字以上入力
	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。
Enforce Password History	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
(パスワード履歴を実行する)	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
	設定することができます。X の値をダイアログボックスに入力し
	てください。
Password Expiration	パスワードの有効日数を入力してください。
(パスワード期限)	

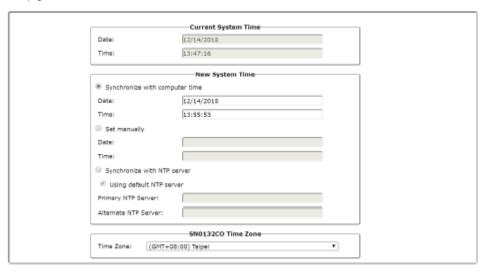
関連付け

「Association」(関連付け)メニューは予約済みの機能です。



日付/時刻

「Date/Time」(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されている日時が表示されます。日付と時刻の欄は読み取り専用のため、編集することができません。

注意: ブラウザーUIでは、システム時刻が、製品本体が設置されている場所のタイムゾーンではなく、Webブラウザーのセッションが開始している場所のタイムゾーンに基づいて表示されます。Web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、ここで表示される時刻は、製品内部のシステム時刻とは異なります。

新しいシステム時刻

製品本体の日時設定は、これらの項目を使って、下記のとお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、「Synchronize with computer time」(コンピューターの時刻と同期)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されています。これらの項目は情報 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、「Set manually」(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、「Synchronize with NTP server」(NTP サーバーと同期)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、「Using default NTP server」(デフォルト NTP サーバーを使用)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、「Using default NTP server」(デフォルトNTP サーバーを使用)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「Primary NTP Server」(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、そのサーバーの IP アドレスを「Alternate NTP Server」(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「Save」(保存)をクリックしてください。

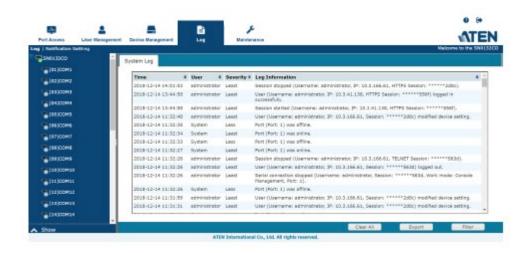
タイムゾーン

- ◆ 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、「Time Zone」(タイムゾーン)のリストを展開し、その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「Save」(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されます。ログの内容を確認する場合は、「Log」(ログ)タブをクリックしてください。タブをクリックすると、デバイスのログ情報が表示されます。



システムログ

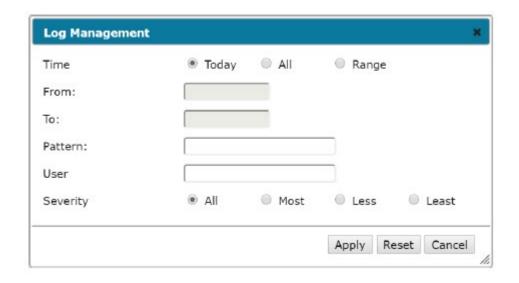
「System Log」(システムログ)メニューには、シリアルコンソールサーバーの製品内部で発生したイベントや、イベントの時刻、重要度、ユーザーの概要、またログ情報がそれぞれ表示されます。列の見出しをクリックすると、その項目で表示順を変更します。

ログファイルは、最大 512 件のイベントを記録します。記録されたイベントの数が 512 件になると、新しいイベントが発生した際に、一番古いイベントが切り捨てられます。画面下部にあるボタンの詳細は下表のとおりです。

ボタン	説明
Clear Log	ログファイルの内容を消去します。
(ログのクリア)	
Export Log	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
(ログのエクスポート)	します。
Filter	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
(フィルター)	に記載)。

フィルター

この機能を使うと、表示され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むことができます。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。



この画面に表示される各項目の内容は下表のとおりです。

項目	説明
Time	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
(時間)	ルタリングできます。
	Today(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。
	All(すべて):ログファイル内の全イベントを表示します。
	Range(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、表示され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。
Pattern	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
(パターン)	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されま
	す。ここでは、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」キーワードを使うことができます。
	例 1:「h*ds」という文字列を指定した場合、「hands」と「hoods」がヒットし
	ます。
	例 2:「h?nd」という文字列を指定した場合、「hand」または「hind」がヒット
	しますが、「hard」はヒットしません。
	例 3: 「h*ds or h*ks」という文字列を指定した場合、「hands」と「hooks」が
	ヒットします。
User	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
(ユーザー)	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「Apply」(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されます。
	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されません。
-	

(表は次のページに続きます)

項目	説明
Severity	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
(重要度)	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「All」(すべて)、「Most」(最大)、「Less」(中)、「Least」(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が表示されます。
Apply	指定された条件で検索を行います。
(適用)	
Reset	検索条件をデフォルトの状態に戻します。
(リセット)	
Cancel	変更を適用せずに、ログフィルター機能を終了します。
(終了)	

ログ通知設定

「Notification Setting」(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することができます。



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することができます。

- ◆ すべてのシステムイベント
- ◆ すべての認証イベント
- ◆ すべてのユーザー管理イベント
- ◆ すべてのデバイス管理イベント
- ◆ すべてのシステムタスクイベント

特定の通知の ON/OFF を切り替えるには、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 ON/OFF にしてください。



第 10 章 メンテナンス

概要

「Maintenance」(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を行うことができます。



バックアップ/リストア

「Maintenance」(メンテナンス)タブをクリックすると、「Backup/Restore」(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を行うことができます。



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. 「Password」(パスワード)の項目に、ファイルのリストア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 ワードなしでリストアされます。
- 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. 「Backup」(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が表示された場合は、「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が保存され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ので、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、「Password」(パスワード) 欄に、そのパスワードと同じ文字列を入力してください。
- 3. ファイルに保存された内容のうち、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. 「Restore」(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されると、処理に成功したという内容のメッセージが表示されます。

ファームウェアアップグレード

このメニューは、シリアルコンソールサーバーのファームウェアをアップグレードする際に使用します。新しいバージョンのファームウェアが利用可能になると、弊社 Web サイト (https://www.aten.com/jp/ja/)に公開され、ダウンロードできるようになります。このサイトを定期的にご確認いただき、最新のファームウェアにアップグレードしてください。ダウンロードは、1) 製品ページ内の「サポートとダウンロード」メニューからアクセス、または、2) ホームページのトップページの右上に表示される(表示画面のサイズによっては画面左上に三本線のアイコンが表示されるので、それをクリックすると表示される)「サポートとダウンロード」→「ダウンロード」→「他の製品の資料をダウンロードする」に型番を入力して検索する方法で行えます。

ファームウェアをアップグレードするには、下記の作業を行ってください。

- 1. 弊社 Web サイトから本製品の新しいファームウェアファイルをダウンロードし、お使いのコンピューターのハードディスクの適当な場所に保存してください。
- 2. シリアルコンソールサーバーにログインし、「Maintenance」(メンテナンス)タブをクリックして、「Firmware Upgrade」(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。



- 3. 「**参照…**」ボタンをクリックし、手順1で保存したファイルをダイアログから選択してください。
- 4. 「Upgrade Firmware」(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。
 - ◆ 「Check Firmware Version」(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の比較を行います。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が表示され、アップグレードが中断されます。
 - ◆ 「Check Firmware Version」(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、バージョンの比較を行うことなくファームウェアのアップグレードを行います。

- ◆ アップグレードの進行状況は、プログレスバーで確認することができます。
- ◆ 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がリセットされます。
- 5. 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ことを確認してください。

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提供します。



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どうかを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することで、セキュリティを強化することができます。

プライベート証明書の作成方法には、自己署名された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。

◆ 自己署名済み証明書の作成

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

◆ CA 署名済み SSL サーバー証明書の取得

セキュリティを強化するために、サードパーティーの認証局(CA)によって署名された証明書を使うことを推奨します。サードパーティーによって署名された証明書を取得する場合は、認証局の Web サイトにアクセスし、SSL 証明書を申請してください。CA から証明書が送られてきたら、お使いのコンピューターのハードディスクドライブの適当なフォルダーに保存してください。

◆ プライベート証明書のインポート

プライベート証明書をインポートする場合は、下記の手順に従って操作してください。

1. 「Private Certificate」(プライベート証明書)画面の下部にある「Import」(インポート)をクリックしてください。



- 2. 「Certificate Filename」(証明書ファイル名)の右にある「**参照**」ボタンをクリックして、ダイアログからプライベート暗号キーのファイルがあるフォルダーに移動し、このファイルを選択してください。
- 3. 「Import」(インポート)をクリックして操作を完了してください。

注意: 「Restore Default」(デフォルトをリストアする)をクリックすると、シリアルコンソールサーバーはデフォルトの ATEN 証明書を使用するようになります。

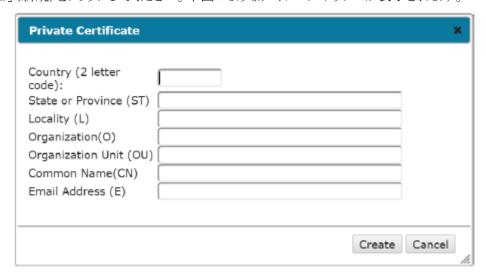
証明書署名要求

証明書署名要求のセクションでは、CA署名済みSSLサーバー証明書の取得とインストールを 自動的に行います。



この操作を行う場合は、下記の手順に従ってください。

1. 「New」(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. 下表の例を参考にしながら、お使いのサイトで有効な値をフォームに入力してください。

情報	例
Country (2 letter code)	TW
(国(2文字のコード))	
State or Province	Taiwan
(州または都道府県)	
Locality	Taipei
(市区町村)	
Organization	Your Company, Ltd.
(組織)	
Organization Unit	Tech Department
(部署)	
Common Name	mycompany.com
(コモンネーム)	注意:ここには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。もし、サイトのドメイン名が
	「 <u>www.mycompany.com</u> 」で、この欄に「mycompany.com」
	とだけしか入力しなかったとしたら、この証明書は有効に
	はなりません。
Email Address	administrator@yourcompany.com
(メールアドレス)	

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、「Create」(作成)をクリックしてください。

先ほど入力した情報に基づいて作成された自己署名済み証明書が、シリアルコンソールサー バーに保存されます。

- 4. 「Get CSR」(CSR を取得する)をクリックし、証明書ファイル(csr.cer)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。
 - 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「Import」(インポート)をクリックしてください。そうすると、下図のような「Private Certificate」(プライベート証明書)のウィンドウがポップアップ表示されます。



7. 「**参照**」をクリックしてファイルを置いて、これを「Certificate Filename」(証明書ファイル名)として選択ください。それから、また「**Import**」(インポート)をクリックして、これ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のチェックを行い、特定の情報が一致しているかどうかを確認します。もし、一致しているのであれば、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、「Restore Defaults」(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

製品仕様

SN0108CO/SN0108COD

機能	SN0108CO/SN0108COD		
接続	8		
コネクター			
シリアル	RJ-45×8		
LAN ポート	RJ-45×2		
電源	【AC 電源モデル : SN0108CO】		
	3 極 AC 電源ソケット×2(IEC60320/C14)		
	【DC 電源モデル : SN0108COD】		
	2ピン ターミナルブロック×2(Green)		
PON	RJ-45×1(PG シリーズ対応予定ポート)		
モデム	RJ-45×1		
ローカルコンソール	RJ-45×1		
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×3		
スイッチ			
電源	ロッカースイッチ×2		
リセット	ピンホール型スイッチ×1		
LED			
シリアル	8 (Green)		
10/100/1000 Mbps	2(Red / Orange / Green)		
電源	2(Blue)		

_____ (表は次のページに続きます)

機能	SN0108CO/SN0108COD
最大電源仕様	【AC 電源モデル : SN0108CO】
	AC 100~240V, 50/60Hz, 1A
	(日本仕様はPSE対応 3P/100V 電源コードを同梱)
	【DC 電源モデル : SN0108COD】
	DC 36~48V、1.6A(5ピン ターミナルブロック)
消費電力	110V / 14.1W
	220V / 14W
操作モード	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°C
保管温度	-20∼60°C
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
サイズ(W×D×H)	437.2×329.8×44 mm
同梱品	ラップトップ USB コンソールケーブル×1
	電源ケーブル×2(AC 電源モデル)
	マウントキット×1
	ケーブル抜け防止ホルダー「Lok-U-Plug」×2
	ケーブル抜け防止ホルダー取付工具×1
	フットパッドセット(4pcs)×1
	クイックスタートガイド×1

SN0116CO/SN0116COD

機能	SN0116CO/SN0116COD
接続	16
コネクター	
シリアル	RJ-45×16
LAN ポート	RJ-45×2
電源	【AC 電源モデル : SN0116CO】
	3 極 AC 電源ソケット×2(IEC60320/C14)
	【DC 電源モデル : SN0116COD】
	2ピン ターミナルブロック×2(Green)
PON	RJ-45×1(PG シリーズ対応予定ポート)
モデム	RJ-45×1
ローカルコンソール	RJ-45×1
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×3
スイッチ	
電源	ロッカースイッチ×2
リセット	ピンホール型スイッチ×1
LED	
シリアル	16 (Green)
10/100/1000 Mbps	2(Red / Orange / Green)
電源	2(Blue)
最大電源仕様	【AC 電源モデル : SN0116CO】
	AC 100~240V, 50/60Hz, 1A
	(日本仕様は PSE 対応 3P/100V 電源コードを同梱)
	【DC 電源モデル : SN0116COD】
	DC 36~48V、1.6A(5ピン ターミナルブロック)
消費電力	110V / 15.4W
	220V / 14.9W

(表は次のページに続きます)

機能	SN0116CO/SN0116COD	
操作モード	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°C	
湿度	0~80% RH、結露なきこと	
ケース		
ケース材料	メタル	
重量	4.48 kg	
サイズ(W×D×H)	437.2(突起物含む)×329.8×44 mm	
同梱品	ラップトップ USB コンソールケーブル×1	
	電源ケーブル×2(AC 電源モデル)	
	マウントキット×1	
	ケーブル抜け防止ホルダー「Lok-U-Plug」×2	
	ケーブル抜け防止ホルダー取付工具×1	
	フットパッドセット(4pcs)×1	
	クイックスタートガイド×1	

SN0132CO/SN0132COD

機能	SN0132CO/SN0132COD
接続	32
コネクター	
シリアル	RJ-45×32
LAN ポート	RJ-45×2
電源	【AC 電源モデル : SN0132CO】
	3 極 AC 電源ソケット×2(IEC60320/C14)
	【DC 電源モデル : SN0132COD】
	2ピン ターミナルブロック×2(Green)
PON	RJ-45×1(PG シリーズ対応予定ポート)
モデム	RJ-45×1
ローカルコンソール	RJ-45×1
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×3
スイッチ	
電源	ロッカースイッチ×2
リセット	ピンホール型スイッチ×1
LED	
シリアル	32 (Green)
10/100/1000 Mbps	2(Red / Orange / Green)
電源	2 (Blue)
最大電源仕様	【AC 電源モデル : SN0132CO】
	AC 100~240V, 50/60Hz, 1A
	(日本仕様はPSE対応 3P/100V 電源コードを同梱)
	【DC 電源モデル : SN0132COD】
	DC 36~48V、1.6A(5ピン ターミナルブロック)
消費電力	110V / 20.2W
	220V / 21W

	SN0132CO/SN0132COD
操作モード	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°C
保管温度	-20∼60°C
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
サイズ(W×D×H)	438.4×327.7×44 mm
同梱品	ラップトップ USB コンソールケーブル×1
	電源ケーブル×2(AC 電源モデル)
	マウントキット×1
	ケーブル抜け防止ホルダー「Lok-U-Plug」×2
	ケーブル抜け防止ホルダー取付工具×1
	フットパッドセット(4pcs)×1
	クイックスタートガイド×1

SN0148CO/SN0148COD

機能	SN0148CO/SN0148COD
接続	48
コネクター	
シリアル	RJ-45×48
LANポート	RJ-45×2
電源	【AC 電源モデル : SN0148CO】
	3 極 AC 電源ソケット×2(IEC60320/C14)
	【DC 電源モデル : SN0148COD】
	2ピン ターミナルブロック×2(Green)
PON	RJ-45×1(PG シリーズ対応予定ポート)
モデム	RJ-45×1
ローカルコンソール	RJ-45×1
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×3
スイッチ	
電源	ロッカースイッチ×2
リセット	ピンホール型スイッチ×1
LED	
シリアル	48 (Green)
10/100/1000 Mbps	2 (Red / Orange / Green)
電源	2 (Blue)
最大電源仕様	【AC 電源モデル : SN0148CO】
	AC 100~240V, 50/60Hz, 1A
	(日本仕様はPSE対応 3P/100V 電源コードを同梱)
	【DC 電源モデル : SN0148COD】
	DC 36~48V、1.6A(5ピン ターミナルブロック)
消費電力	110V / 25.8W
	220V / 26.2W

機能	SN0148CO/SN0148COD
操作モード	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°C
保管温度	-20~60°C
湿度	0~80% RH、結露なきこと
ケース	
ケース材料	メタル
重量	4.92 kg
サイズ(W×D×H)	438.4×327.7×44 mm
同梱品	ラップトップ USB コンソールケーブル×1
	電源ケーブル×2(AC 電源モデル)
	マウントキット×1
	ケーブル抜け防止ホルダー「Lok-U-Plug」×2
	ケーブル抜け防止ホルダー取付工具×1
	フットパッドセット(4pcs)×1
	クイックスタートガイド×1

<u>SN9108CO/SN9116CO</u>

機能	SN9108CO	SN9116CO
接続	8	16
コネクター		
シリアル	RJ-45×8	RJ-45×16
LAN ポート	RJ-45×1	
電源	3極AC電源ソケット×1	3極AC電源ソケット×1
	(IEC60320/C14)	(IEC60320/C14)
スイッチ		
電源	ロッカースイッチ×1	
リセット	ピンホール型スイッチ×1	
LED		
シリアル	8(Green)	16 (Green)
10/100/1000 Mbps	1 (Red / Orange / Green)	
電源	1 (Blue)	
最大電源仕様	AC 100~240V, 50/60Hz, 1A	
	(日本仕様は PSE 対応 3P/100	V 電源コードを同梱)
消費電力	110V / 9.7W	110V / 10.9W
	220V / 9.6W	220V / 11.6W
操作モード	コンソール管理、コンソール管理	タイレクト、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°C	
保管温度	-20∼60°C	
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)	437.2×217.6×44 mm	

機能	SN9108CO	SN9116CO
同梱品	電源ケーブル×1	
	マウントキット×1	
	ケーブル抜け防止ホルダー「Lok-U	$J-Plug J \times 2$
	ケーブル抜け防止ホルダー取付工	
	フットパッドセット(4pcs)×1	
	クイックスタートガイド×1	

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され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 アドレスを設定することができます(p.128「ネットワーク」参照)。

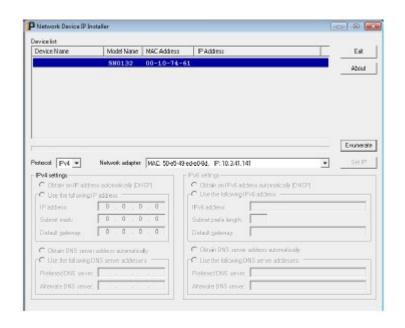
ローカルコンソール

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。設定方法の詳細については p.48 を参照してください。

IP インストーラー

Windows がインストールされ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シリアルコンソールサーバーに IP アドレスを設定することができます。IP インストーラーは弊社 Web サイトのダウンロードページからダウンロードすることができます。ダウンロードページの「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。次のようなダイアログボックスが表示されます。



3. 「Device List」(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:

- 一覧に何も表示されない、また、対象となる製品が表示されない場合は、「Enumerate」(一覧表示)をクリックして、「Device List」(デバイス一覧)を更新してください。
- 2. 一覧に複数のデバイスが表示されている場合は、MAC アドレスを使って目的のデバイスを識別してください。製品の MAC アドレスは本体底面に貼られているラベルに記載されています。
- 4. DHCP を使って IP アドレスを自動的に取得する場合は「Obtain an IP address automatically (DHCP)」 (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「Specify an IP address」 (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、製品がセットアップされ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. 「Set IP」(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「Device List」(デバイス一覧)に表示されたら、「**Exit**」(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.128 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。 「XXXX」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)に使用されていますので、これ 以外の値を使用してください。
- 2. Web 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がセットアップされ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されます(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、「Device Management」(デバイス管理) \rightarrow 「Device Information」(デバイス情報)メニューを開いてください。アドレスが「General」(全般)リスト(p.123 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うことができます。

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(p.52 参照) でアドレスを次のように入力してください。

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

注意:

- 1. IPv6 リンクローカルアドレスを使ってログインする場合には、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一のローカルネットワークセグメントにセットアップされている必要があります。
- 2. 「%5」の部分は、クライアントコンピューターによって使用される「%インターフェース」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。

ステートレス自動設定

シリアルコンソールサーバーがセットアップされ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することができます。例えば、「2001::74ff:fe6e:59」です。

先に述べたように、アドレスは「Device Management」(デバイス管理)→「Device Information」 (デバイス情報)メニューの「General」(全般)リスト(p.123 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うことができます。

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てください。

2001::74ff:fe6e:59

バーチャルモデム詳細

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することで、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することができますので、電話回線を使ったモデム通信に見られた通信速度や信頼性の問題を解消することができます。

AT コマンドセットのサポート

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、および拡張されたコマンドの一部をサポートします。

コマンド	操作	レスポンス
+++	コマンドモードに戻ります。エスケープコー	なし
	ドはS2レジスターによって変更することがで	
	きます。	
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]
	取後に美1]したコマントを円美1]しまり。 	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	成功した場合:OK[CR][LF]
	5301 番のポートで TCP 接続の通信をリッス	失敗した場合:ERROR[CR][LF]
	ンするようにします。	
ATD(T)	TCP 接続の確立を試み、特定のリモートホ	成功した場合:
リモート IP:リ	ストに接続します。	CONNECT[CR][LF]
モートポート		
[CR]	例)ATDT 10.0.0.72:50001	接続に失敗した場合:
		NO CARRIER[CR][LF]
	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、これ	その他のエラーが発生した場合:
	らの文字は無視されます。	ERROR[CR][LF]
ATEn[CR]	nの部分には0または1の数字を入力しま	成功した場合:OK[CR][LF]
	す。	失敗した場合:ERROR[CR][LF]
	E0:エコーバックを無効にする。	
	E1:エコーバックを有効にする。	

コマンド	操作	レスポンス
ATH[CR]	接続がアクティブである場合に現在の TCP	成功した場合:OK[CR][LF]
	接続を切断します。	失敗した場合:ERROR[CR][LF]
	注意:ATH、ATHO、ATH1 はどれも同様に	
	動作します。	
ATIn[CR]	問い合わせコマンドです。(n の部分には 0	成功した場合:OK[CR][LF]
	または1の数字を入力します。)	失敗した場合:ERROR[CR][LF]
	E0:ATEN International Co.Ltd.を表示	
	E1:シリアルコンソールサーバーを表示	
ATOn[CR]	オンラインデータモードに戻ります。(n の部	TCP 接続がアクティブである場
	分には0または1の数字を入力します。)	合:
	モデムがオンラインコマンドモードの場合、	OK[CR][LF]
	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	それ以外の場合:
	ード(TCP 接続が確立されていない)の場	ERROR[CR][LF]
	合は、ERROR が返ってきます。	
	00、01: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てください。	N - 1 N - 1 H - A
ATQ <i>n</i> [CR]	リザルトコード制御コマンドです。(nの部分	成功した場合:OK[CR][LF]
	には0または1の数字を入力します。)	失敗した場合:ERROR[CR][LF]
	Q0:DTE へのリザルトコードを有効にする	
	(デフォルト)	
	Q1:DTE へのリザルトコードを無効にする	
ATSn?[CR]	Sレジスターの値を報告します。(nの部分	成功した場合:OK[CR][LF]
	にはレジスターの番号を入力します。)	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	成功した場合:OK[CR][LF]
	にはレジスターの番号を、vの部分にはSレ	失敗した場合:ERROR[CR][LF]
	ジスターの値をそれぞれ入力します。)	
		(+,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,

コマンド	操作	レスポンス
ATVn[CR]	リザルトコードを返す際の形式を設定しま	成功した場合:OK[CR][LF]
	す。(nの部分には0または1の数字を入力	失敗した場合:ERROR[CR][LF]
	します。)	
	V0: レスポンスは 〈番号形式〉[CR][LF]	
	V1: レスポンスは 〈単語形式〉[CR][LF]	
ATZ[CR]	モデムコマンドをリセットします。	成功した場合:OK[CR][LF]
	アクティブな接続を終了し、Sレジスターお	失敗した場合:ERROR[CR][LF]
	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。	
AT&Cn[CR]	DCD オプションです。(nの部分には0また	成功した場合:OK[CR][LF]
	は1の数字を入力します。)	失敗した場合:ERROR[CR][LF]
	&C0:DCD を常に ON にする	
	&C1:DCD を TCP 接続の状態に合わせる	
AT&D <i>n</i> [CR]	DTR オプションです。(n の部分には 0~3	成功した場合:OK[CR][LF]
	の数字を入力します。) 	失敗した場合:ERROR[CR][LF]
	&D0:DTR は ON であるものと見なされ、モ	
	デムは DTR ラインを無視する	
	&D1:DTR OFF は、通信を切断することなく	
	モデムをコマンドモードに切り替える	
	&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	
	に切り替え、通信を中倒し、日勤心谷機能を無効にする(デフォルト)	
	を無効にする(ケンオルド) &D3:DTR OFF により、モデムを初期化す	
	abs.Dik Off により、モノムを初期にり	
AT&F[CR]	工場出荷時の設定に戻します。	 成功した場合:OK[CR][LF]
	Sレジスターおよび汎用オプションのステー	失敗した場合:ERROR[CR][LF]
	タスを、デフォルト値にリセットします。	· · · · · · · · · · · · · · · · · · ·
-		(

コマンド	操作	レスポンス
AT&W[CR]	設定を保存します。	成功した場合:OK[CR][LF]
	Sレジスターおよび汎用オプションのステー	失敗した場合:ERROR[CR][LF]
	タスを含む現在の設定内容を、メモリーに	
	書き込みます。	
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]
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]

ポートの転送

ルーターの内側にセットアップされているデバイスがある場合、特定のポート経由で特定のデバイス宛に送信され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することによって、特定のポートに送信されたデータをどのデバイスに転送すればよいのかを、ルーターに判別させることができます。

例えば、特定のルーターに接続されたシリアルコンソールサーバーに「192.168.1.180」というIPアドレスが設定されている場合、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。

ルーターの設定方法は、製品ごとに異なりますので、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種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	30m
115200	3m
230400	1.5m

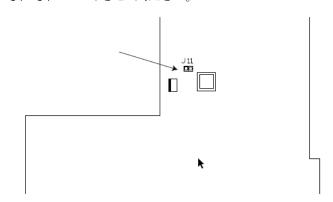
ログイン情報の消去

アドミニストレーターがユーザー名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、下記の作業を行ってログイン情報を消去することができます。

注意: この作業を行うと、すべ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(すべ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 行ってください。

- 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、SN0132CO/SN0148CO の場合はメインボードの「**J11**」と書かれた場所(下図参照)を、SN9108CO/SN9116CO/SN0108CO/SN0116CO の場合は「**J17**」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. 製品本体からビープ音が聞こえ出したら、シリアルコンソールサーバーの電源を切ってください。
- 5. 「**J11**」(SN0132CO/SN0148CO の場合)または「**J17**」(SN9108CO/SN9116CO/SN0108CO/SN0116CO)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。

電源を入れると、デフォルトのユーザー名とパスワード(p.48「初回セットアップ」参照)を使用してログインできます。なお、この手順でログイン情報を消去した後の初回ログイン時には、システムからパスワードの変更を求められます。

ピンアサイン

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アサインを以下に示します。

DCE モードのピンアサイン

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

DTE モードのピンアサイン

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-9F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

