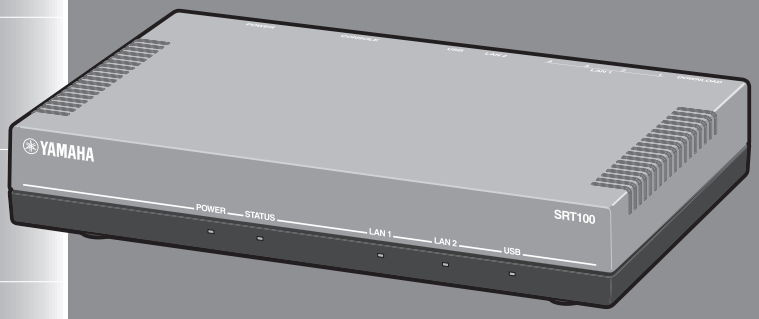
YAMAHA

SRT100

ファイアウォールルーター



コマンド設定運用説明書

ヤマハSRT100をお買い上げいただきありがとうございます。
お使いになる前に本書をよくお読みになり、正しく設置や設定を行ってください。
本書中の警告や注意を必ず守り、正しく安全にお使いください。
本書はなくさないように、大切に保管してください。

安全上のご注意

本製品を安全にお使いいただくために

以下の点を必ず守ってお使いください。

安全のための注意事項を守る

詳しくは、8〜9ページをご覧ください。

故障したら使用を中止する。

お買い上げの販売店またはヤマハのお問い合わせ窓口(46ページ)にご連絡ください。

マークの意味

本書および本製品では、本製品を安全にお使いいただくため、守っていただきたい事項に次のマークを表示していますので、必ずお読みください。また、本書はお使いになる方がなくさないように大切に保管してください。

⚠警告

人体に危険を及ぼしたり、装置に大きな損害を与える可能性があることを示しています。必ず守ってください。

⚠注意

機能停止を招いたり、各種データを消してしまう可能性があることを示しています。十分注意してください。

目次

SRT100でできること

本製品は、中・小規模の企業ネットワークに適した、ファイアウォールルーターです。各種ブロードバンド回線用モデムと本製品をLANケーブルで接続して、FTTHやADSL、CATVなどのブロードバンド回線経由でインターネットなどに接続できます。IPsecに対応しているため、ブロードバンド回線を利用したVPN（仮想プライベートネットワーク）を構築する場合でも、より安全にデータをやり取りできます。

サポートするプロトコル

本製品はIPパケットおよびIPv6パケットの経路制御（ルーティング）をサポートしています。経路制御とは、パケット内部に記録されたIPアドレスやIPv6プレフィックスといったネットワークアドレスに基づいて、パケットの適切な経路を決定・配送することです。

- 経路制御には、本体への設定に基づく静的な経路制御と、ルーター同士が動的に行う動的経路制御があります。
- 動的経路制御ではIPパケットに対してRIP、RIP2、OSPF、BGPプロトコル、IPv6パケットに対してはRIPngプロトコルプロトコルをサポートします。
- 経路制御において、パケットを暗号化することもできます。暗号化プロトコルとしてはIPsecをサポートします。

パケットのフィルタリング機能

主にセキュリティの観点から特定のパケットを遮断する目的で、パケットのフィルタリングを実行できます。

- **入力遮断フィルター**：受信したパケットに対して、IPアドレスやプロトコル、ポート番号を基準に通過・破棄を判別します。
- **ポリシーフィルター**：Stateful Inspection方式による、コネクションを単位とするアクセス制御を実現します。ポリシーは最大4階層まで階層的に並べて定義できるので、「上位階層で大まかなルールを決めてから、次第に詳細化する」といった設定も実現できます。

この他にも、不正なデータを遮断するLANセキュリティ機能として、以下のような機能を利用できます。詳しくは、「コマンドリファレンス」をご覧ください。

- **Winnyフィルタ機能**：ファイル共有ソフトウェア「Winny」が利用するパケットを検出すると共に、該当パケットを破棄し、通信を遮断します。
- **DHCP端末認証機能**：あらかじめ使用を許可した端末（登録済端末）と、許可していない端末（未登録端末）とをネットワーク上で区別します。許可の有無によって、それぞれの端末がアクセス可能なネットワークを制御できます。
- **Dynamic Class Control機能**：帯域を圧迫している特定パソコンの使用帯域を、制限・遮断できます。

Webブラウザ上の設定画面による設定運用管理機能

本製品では、Webブラウザ上の設定画面で、視覚的に優れた設置運用および管理を行うことができます。ただしこの方法では、本製品本体へのアクセス制限に使用するユーザ名やパスワード、本製品の設定内容がネットワーク上で盗聴される危険性がありますのでご注意ください。盗聴の危険性のないネットワークを経由してWebブラウザ上で設定画面を利用する場合の操作については、「取扱説明書」をご覧ください。

その他のルーター機能

- SNMP（Simple Network Management Protocol）に対応しています。RFC1157（SNMP）およびRFC1213（MIB-II）準拠の機能を搭載しています。
- VRRP（Virtual Router Redundancy Protocol）に対応しています。他のVRRP対応ルーターと併設することで、機器を冗長構成にすることができます。
- QoS連携機能（帯域検出機能と負荷通知機能）に対応しています。
- タグVLAN（IEEE802.1Q）に対応しています。
- NATトラバーサルに対応しています。

詳しくは、「コマンドリファレンス」をご覧ください。

ヤマハルーターホームページのご案内

ヤマハルーターホームページで、ヤマハルーターを使った高度な活用例や詳しい解説がご覧いただけます。

http://NetVolante.jp/

http://www.rtpro.yamaha.co.jp/

はじめにお読みください

本製品に実装されているヤマハポリシーフィルタリングモジュールRev.1.02 (2)は、ISO15408認証を取得しております。ヤマハポリシーフィルタリングモジュールのリビジョン番号は、show environmentコマンドの実行後に出力される文字列で確認できます。

出力例
YAMAHA Policy Filtering module Rev.1.02 (2)

この文書では、ヤマハポリシーフィルタリングモジュールのセキュアな設置運用方法の手順を示します。

ヤマハポリシーフィルタリングモジュールについて

ヤマハポリシーフィルタリングモジュールに含まれる機能は、以下の通りです。

- ユーザー識別認証機能(25ページ)
  一般ユーザーと管理ユーザーの2段階に分かれたアクセス管理や、ユーザー登録に関連する機能です。ユーザー毎に設定手段や管理ユーザーへの移行許可、多重接続の許可などを設定できます。
- ポリシーフィルタリング機能(29ページ)
  Stateful Inspection方式による、コネクションを単位とするアクセス制御を実現します。ポリシーは最大4階層まで階層的に並べて定義できます。
- 上記機能に関連する関わるロギング機能(34ページ)
  ログイン・ログアウトの実行や、ポリシーフィルターで処理したパケットの内容、設定内容の変更などを記録として保存できます。

これらの機能で使用するコマンドを以下に示します。

コマンド名	実行権限
syslog execute command	管理ユーザー
syslog notice	管理ユーザー
syslog info	管理ユーザー
security class	管理ユーザー
show environment	管理ユーザー / 一般ユーザー
administrator	一般ユーザー
login password	管理ユーザー
administrator password	管理ユーザー
login user	管理ユーザー
user attribute	管理ユーザー
show status user	管理ユーザー / 一般ユーザー
quit	管理ユーザー / 一般ユーザー
exit	管理ユーザー / 一般ユーザー
ip policy service	管理ユーザー

コマンド名	実行権限
ipv6 policy service	管理ユーザー
ip policy interface group	管理ユーザー
ipv6 policy interface group	管理ユーザー
ip policy address group	管理ユーザー
ipv6 policy address group	管理ユーザー
ip policy service group	管理ユーザー
ipv6 policy service group	管理ユーザー
ip policy filter	管理ユーザー
ipv6 policy filter	管理ユーザー
ip policy filter set	管理ユーザー
ipv6 policy filter set	管理ユーザー
ip policy filter set enable	管理ユーザー
ipv6 policy filter set enable	管理ユーザー
ip policy filter timer	管理ユーザー
show status ip policy filter	管理ユーザー /一般ユーザー
show status ipv6 policy filter	管理ユーザー /一般ユーザー
show status ip policy service	管理ユーザー /一般ユーザー
show status ipv6 policy service	管理ユーザー /一般ユーザー
clear ip policy filter	管理ユーザー
clear ipv6 policy filter	管理ユーザー
show config	管理ユーザー /一般ユーザー
less config	管理ユーザー /一般ユーザー
save	管理ユーザー
cold start	管理ユーザー

- 各コマンドについて詳しくは、コマンドリファレンスをご覧ください。
- コマンドに入力エラーがあった場合やコマンドの実行が失敗した場合は、結果が画面に表示されます。表示内容に従って対応してください。

一般的に、セキュリティを高めるための設置運用方法は、管理性に影響を与えることがあります。本製品の設置される環境やそのセキュリティーポリシーに従って、適切な設置運用手順をご選択ください。

シリアルケーブル経由またはSSH経由でのコマンド設定を利用してください

ポリシーフィルター機能を含めて、本製品ではWebブラウザを用いた設定画面で視覚的に優れた設置運用および管理を行うことができます。ただし、本製品の設置運用において、Webブラウザを用いた設定画面による方法では、本製品本体へのアクセス制限に使用するユーザ名、パスワードおよび本製品の設定内容がネットワーク上で盗聴される危険性があります。この危険性を回避してセキュアな設置運用を行うためには、本ドキュメントの手順を参照してシリアルケーブル経由またはSSH経由でのコマンド設定を利用してください。盗聴の危険性のないネットワーク経由でWebブラウザを用いた設定画面を利用する場合の操作については、「取扱説明書」をご覧ください。

⚠警告

本製品を安全にお使いいただくために、下記のご注意をよくお読みになり、必ず守ってお使いください。

- 本製品は一般オフィス向けの製品であり、人の生命や高額財産などを扱うような高度な信頼性を要求される分野に適応するようには設計されていません。
  本製品を誤って使用した結果発生したあらゆる損失について、当社では一切その責任を負いかねますので、あらかじめご了承ください。
- 本製品から発煙や異臭がするとき、内部に水分や薬品類が入ったとき、および電源コードが発熱しているときは、直ちに電源コードをコンセントから抜いてください。そのまま使用を続けると、火災や感電のおそれがあります。
- 濡れた手で電源コードを触らないでください。感電や故障のおそれがあります。
- 電源コードを傷付けたり、無理に曲げたり、引っ張ったりしないでください。火災や感電、故障、ショート、断線の原因となります。
- 本製品の電源部は日本国内用AC100V（50/60Hz）の電源専用です。他の電源で使用すると、火災や感電、故障の原因となります。
- 安全のため、電源コードは容易に外すことのできるコンセントに接続してください。家具の後ろなど手の届かない場所にあるコンセントには接続しないでください。
- 本製品をご使用にならないときは、電源コードを必ずコンセントから外してください。
- 本製品を落下させたり、強い衝撃を与えたりしないでください。内部の部品が破損し、感電や火災、故障の原因となります。
- 本製品を分解したり、改造したりしないでください。火災や感電、故障の原因となります。
- 本製品の通風口を塞いだ状態で使用しないでください。火災や感電、故障の原因となります。
- 電源を入れたままケーブル類を接続しないでください。感電や故障、本製品および接続機器の破損の恐れがあります。
- LAN1/LAN2ポートなどの通信ポートには、本来接続される信号と異なる信号ケーブルを接続しないでください。火災や故障の原因となります。
- 本製品のポートに指や異物を入れないでください。感電や故障、ショートの原因となります。
- 本製品を他の機器と重ねて置かないでください。熱がこもり、火災や故障の原因となることがあります。
- 近くに雷が発生したときは、電源コードやケーブル類を取り外し、使用をお控えください。落雷によって火災や故障の原因となることがあります。

⚠注意

本製品を安全にお使いいただくために、下記のご注意をよくお読みになり、必ず守ってお使いください。

- 直射日光や暖房器等の風が当たる場所、温度や湿度が高い場所には、置かないでください。故障や動作不良の原因となります。
- 極端に低温の場所や温度差が大きい場所、結露が発生しやすい場所で使用しないでください。故障や動作不良の原因となります。結露が発生した場合は、電源コードをコンセントから抜き、乾燥させ、充分に室温に慣らしてから使用してください。
- ほこりが多い場所や油煙が飛ぶ場所、腐蝕性ガスがかかる場所、磁界が強い場所に置かないでください。故障や動作不良の原因となります。
- 同一電源ライン上にノイズを発生する機器を接続しないようにしてください。故障や動作不良の原因になります。
- アースコードは必ず接続してください。感電防止やノイズ防止の効果があります。アース接続は必ず、電源コードをコンセントにつなぐ前に行ってください。また、アース接続をはずす場合は、必ず電源コードをコンセントから取りはずしてから行ってください。
- 本製品を修理や移動等の理由により輸送する場合には、必ず本製品の設定を保存してください。
- 本製品に触れる際には、人体や衣服から静電気を除去する等、静電気対策を十分に行ってください。静電気によって故障する恐れがあります。

使用上のご注意

- 本製品の使用方法や設定を誤って使用した結果発生したあらゆる損失について、当社では一切その責任を負いかねますので、あらかじめご了承ください。
- 本製品のご使用にあたり、周囲の環境によっては電話、ラジオ、テレビなどに雑音が入る場合があります。この場合は本製品の設置場所、向きを変えてみてください。
- 本製品を譲渡する際は、マニュアル類も同時に譲渡してください。
- 本製品を廃棄する場合には不燃物ゴミとして廃棄してください。または、お住まいの自治体の指示に従ってください。本製品はコイン型リチウム電池を内蔵しています。
- 本製品のUSBポートは、すべてのUSBメモリの動作を保証するものではありません。
- USBメモリの内部データは定期的にバックアップすることをお勧めします。本製品のご利用にあたりデータが消失、破損したことによる被害については、弊社はいかなる責任も負いかねますので、あらかじめご了承ください。

重要なお知らせ

セキュリティ対策と本製品のファイアウォール機能について

インターネットを利用すると、ホームページで世界中の情報を集めたり、電子メールでメッセージを交換したりすることができ、とても便利です。その一方で、お使いのパソコンが世界中から不正アクセスを受ける危険にさらされることになります。
特にインターネットに常時接続したり、サーバーを公開したりする場合には、不正アクセスの危険性を理解して、セキュリティ対策を行う必要があります。本製品はそのためのファイアウォール機能を装備していますが、不正アクセスの手段や抜け道(セキュリティホール)は、日夜新たに発見されており、それを防ぐ完璧な手段はありません。**インターネット接続には、常に危険がともなうことをご理解いただくとともに、常に新しい情報を入手し、自己責任でセキュリティ対策を行うことを強くおすすめいたします。**

プロバイダ契約について

本製品をルーターとしてお使いになる前(または新たにプロバイダ契約を行う前)に、必ずルーター経由による複数パソコンの同時接続が、プロバイダによって禁止されていないかどうかご確認ください。**プロバイダによっては、禁止もしくは別の契約が必要な場合があります。契約に違反して本製品を使用すると、予想外の料金を請求される場合があります。**
禁止されている場合は、プロバイダと別途必要な契約を行うか、同時接続を禁止していない他のプロバイダと契約してください。

電波障害自主規制について

この装置は、情報処理装置等電波障害自主規制協議会(VCCI)の基準に基づくクラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

高調波について

JIS C 61000-3-2適合品
JIS C 61000-3-2適合品とは、日本工業規格「電磁両立性−第3-2部：限度値−高調波電流発生限度値(1相当たりの入力電流が20A以下の機器)」に基づき、商用電力系統の高調波環境目標レベルに適合して設計・製造した製品です。

輸出について

本製品は「外国為替および外国貿易法」で定められた規制対象貨物(および技術)に該当するため、輸出または国外への持ち出しには、同法および関連法令の定めるところに従い、日本国政府の許可を得る必要があります。

本書の表記について

略称について

本書ではそれぞれの製品について、以下のように略称で記載しています。

- YAMAHA SRT100：本製品
- Microsoft® Windows®：Windows
- Microsoft® Windows® XP：Windows XP
- Microsoft® Windows Vista™：Windows Vista
- 10BASE-T（100BASE-TX）ケーブル：LANケーブル

設定例について

本書に記載されているIPアドレスやドメイン名、URLなどの設定例は、説明のためのものです。実際に設定するときは、必ずプロバイダから指定されたものをお使いください。

詳細な技術情報について

本製品を使いこなすためには、インターネットやネットワークに関する詳しい知識が必要となる場合があります。付属のマニュアルではこれらの情報について解説しておりませんので、詳しくは市販の解説書などを参考にしてください。

商標について

- イーサネットは富士ゼロックス社の登録商標です。
- Microsoft 、Windowsは米国Microsoft社の米国およびその他の国における登録商標です。
- Adobe 、Acrobatは米国Adobe Systems社の登録商標です。

ヤマハルーター製品のお客様サポートについて（サポート規定）

ヤマハ株式会社はルーター製品を快適に、またその性能・機能を最大限に活かしたご利用が可能となりますように以下の内容・条件にてサポートをご提供いたします。

1. サポート方法

①FAQ、技術情報、設定例、ソリューション例等のWeb掲載
②電話でのご質問への回答
③お問い合わせフォームからのご質問への回答
④カタログ送付
⑤代理店・販売店からの回答
　ご質問内容によっては代理店・販売店へご質問内容を案内し、代理店・販売店よりご回答させていただく場合がありますので予めご了承のほどお願い致します。

2. サポート項目

①製品仕様について
②お客様のご利用環境に適した弊社製品の選定について
③簡易なネットワーク構成での利用方法について
④お客様作成のconfigの確認、およびlogの解析
⑤製品の修理について
⑥代理店または販売店のご紹介

3.免責事項・注意事項

①回答内容につきましては正確性を欠くことのないように万全の配慮をもって行いますが、回答内容の保証、および回答結果に起因して生じるあらゆる事項について弊社は一切の責任を負うことはできません。
また、サポートの結果又は製品をご利用頂いたことによって生じたデータの消失や動作不良等によって発生した経済的損失、その対応のために費やされた時間的・経済的損失、直接的か間接的かを問わず逸失利益等を含む損失およびそれらに付随的な損失等のあらゆる損失について弊社は一切の責任を負うことはできません。
尚、これらの責任に関しては弊社が事前にその可能性を知らされていた場合でも同様です。但し、契約および法律でその履行義務を定めた内容は、その定めるところを遵守するものと致します。

②ファームウェアの修正は弊社が修正を必要と認めたものについて生産終了後2年間行います。

③質問受付対応、修理対応は生産終了後5年間行います。

④実ネットワーク環境での動作保証、性能保証は行っておりません。

⑤期日・時間指定のサポート、および海外での使用、日本語以外でのサポートは行っていません。

⑥お問い合わせの回答を行うにあたって、必要な情報のご提供をお願いする場合があります。情報のご提供がない場合は適切なサポートができない場合があります。

⑦再現性がない、および特殊な環境でしか起きない等の事象に関しては、解決のための時間がかかったり適切なサポートが行えない場合があります。

⑧オンサイト保守・定期保守等は代理店にて有償にて行います。詳細な内容は代理店にご確認をお願い致します。

⑨他社サービス、他社製品、および他社製品との相互接続に関してのサポートは弊社Web上に掲載している範囲に限定されます。

⑩やむを得ない事由によりヤマハルーターの返品・交換が生じた場合は、ご購入店経由となります。尚、交換、返品に際しましてはご購入店、ご購入金額を証明する証憑が必要となります。

⑪製品の修理は代理店・販売店経由で受付けさせて頂きます。弊社への直接持ち込みはできません。また、着払いでの修理品受付は致しておりません。発送は弊社指定の通常宅配便(国内発送のみ)にて行わせて頂きます。修理完了予定期間は変更になる場合がありますのでご了承のほどお願い致します。尚、保証期間中の無償修理(無償例外事項)等の詳細規定は保証書に記載しております。

⑫上記サポート規定は予告なく変更されることがあります。

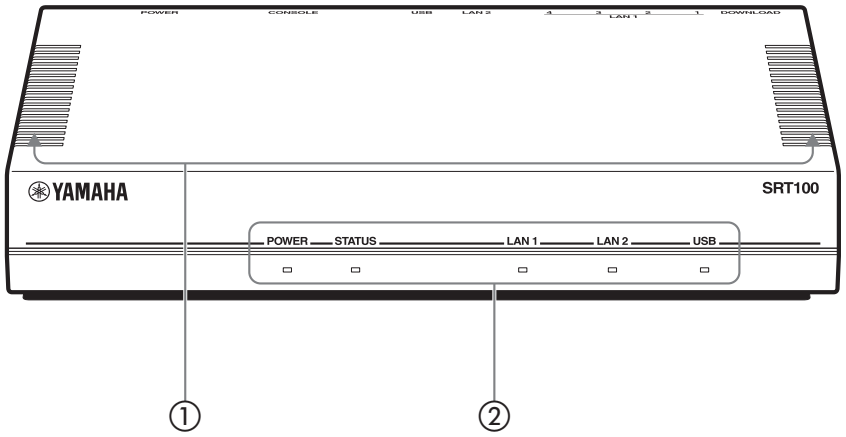
準備および注意事項

本製品の設置前に、以下の準備と注意事項をご確認ください。

- 組織の責任者は、本製品により保護されるべき内部ネットワークリソースを特定して、組織のポリシーを定めてください。
- 組織の責任者は、システム管理者、管理ユーザーとして、セキュリティ意識が高く責任を持って管理ができ、悪意を持った行動をしない者を任命し、それらのセキュリティ意識のレベルを高く維持し続けるよう監督してください。
- 外部ネットワークとの接続は少ないことが望まれます。本製品だけを利用してセキュリティを保つ場合は、内部ネットワークと外部ネットワークとの接続点は一つとして、その境界に本製品を設置してください。
- クロスタイプのシリアルケーブルを用意してください。シリアルケーブルの両端のコネクタは、本製品（D-sub9ピン、オス）とパソコンに適合したタイプを使用してください。
- 本製品のログの出力先とするsyslogサーバーを準備してください。syslogサーバーのディスクは、ログの保存のために十分な容量が必要です。
- 本製品とCONSOLEポートで接続する管理端末およびsyslogサーバー、それらを接続する管理用のネットワークは、システム管理者以外触れられない場所に設置してください。

各部の名称とはたらき

前面



① 通風口

内部の熱を逃がすための穴です。

② ランプ

本製品の動作状態を示します。ランプの点灯状態と本製品の動作の関係については、「前面ランプの点灯状態」(次ページ)をご覧ください。

- **POWER：**本製品の電源の状態を示します。電源が入っているときは点灯します。
- **STATUS：**接続先の機器との通信が不可能な状態になっているかどうかを示します。
- **LAN1：**LAN1ポートの使用状態を示します。接続中は点灯、通信中は点滅します。
- **LAN2：**LAN2ポートの使用状態を示します。接続中は点灯、通信中は点滅します。
- **USB：**USB機器の接続、使用状態を示します。

前面ランプの点灯状態

◉点灯　◌ 点滅　◎消灯

POWERランプ

◉ 電源が入っています。
◎ 電源が切れているか、または停電しています。

STATUSランプ

◉ 通信が不可能な状態になっています。
◎ 通信が不可能な状態になっていません。

LAN1ランプ

◉ LAN1が使用可能な状態です。
◌ LAN1にデータが流れています。
◎ LAN1が使用不可能な状態です。

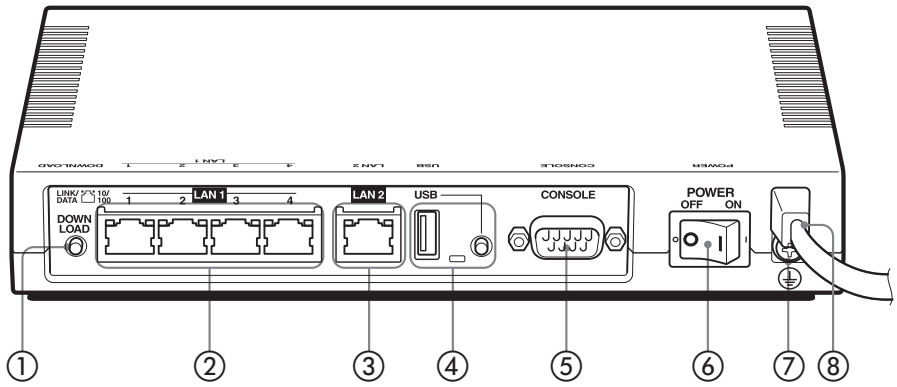
LAN2ランプ

◉ LAN2が使用可能な状態です。
◌ LAN2にデータが流れています。
◎ LAN2が使用不可能な状態です。

USBランプ

◉ USBデバイスがUSBポートに差さっていて、アクセスしていません。
◌ USBデバイスにアクセスしています。
エラー音が鳴る場合は、過電流保護機能によりUSB機能の使用が中断されているか、FOMAリモートセットアップ機能使用時にFOMAを認識できない状態です。
◎ USBデバイスがUSBポートに差し込まれていません。または、ポート に差し込まれているUSBデバイスを取り外すことができる状態です。

背面



① DOWNLOADボタン

DOWNLOADボタンによるリビジョンアップを許可するように設定している場合は、このスイッチを3秒間押し続けるとファームウェアのリビジョンアップを開始します。ボタンの誤操作による意図しないバージョン変更や再起動の危険性がない、セキュアな環境下でこの機能を利用する場合の使用方法については、「取扱説明書」をご覧ください。

② LAN1ポート

パソコンのLANポートまたはHUBのポートとLANケーブルで接続します。
各LAN1ポートの上部には、LINKランプ(左側)とSPEEDランプ(右側)があります。

- **LINKランプ**：リンク状態によって、消灯(リンク喪失)または点灯(リンク確立)、点滅(データ転送中)します。
- **SPEEDランプ**:接続速度によって、消灯(10BASE-T接続)または点灯(100BASE-TX)します。

③ LAN2ポート

ケーブルモデムやADSLモデム、ONUとLANケーブルで接続します。
LAN2ポートの上部には、LINKランプ(左側)とSPEEDランプがあります。動作については、LAN1ポートのランプと同様です。

④ USBポートとボタン

市販のUSBメモリを使用して、設定ファイルのコピーやログの保存、リビジョンアップを実行できます。また、FOMAを接続してリモートアクセスによる設定変更を行うこともできます。
本製品へのアクセスによりこれらの操作を不正に行われる危険性がない、セキュアな環境下でこの機能を利用する場合の使用方法については、「取扱説明書」をご覧ください。

⑤ CONSOLEポート

コンソールからの設定を行う場合に、パソコンのRS-232C端子(シリアルコネクタ)と接続します。

⑥ POWERスイッチ

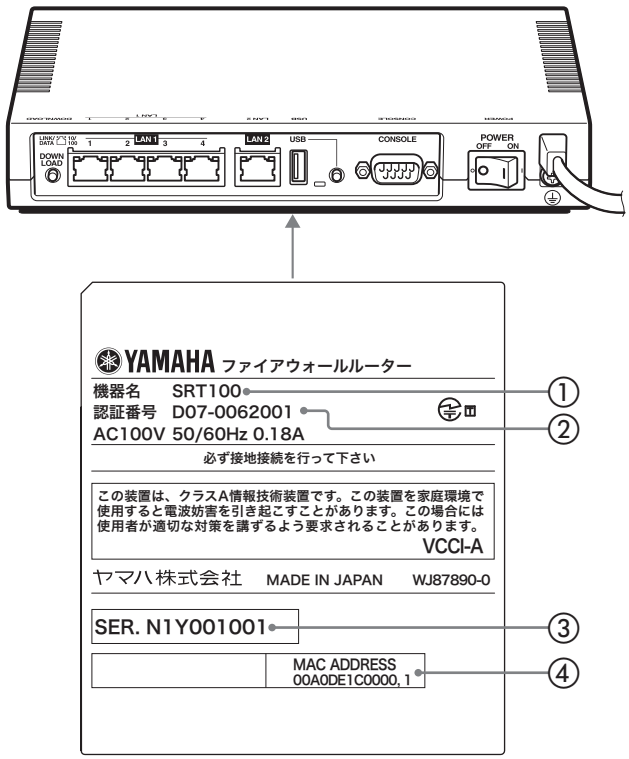
本製品の電源を入／切します。

⑦ アース端子

アースコードを接続します。必ず接続してください。

⑧ 電源コード

底面



① 機器名

本製品の機器名が記載されています。

② 認証番号

本製品の認証番号が記載されています。

③ シリアル番号

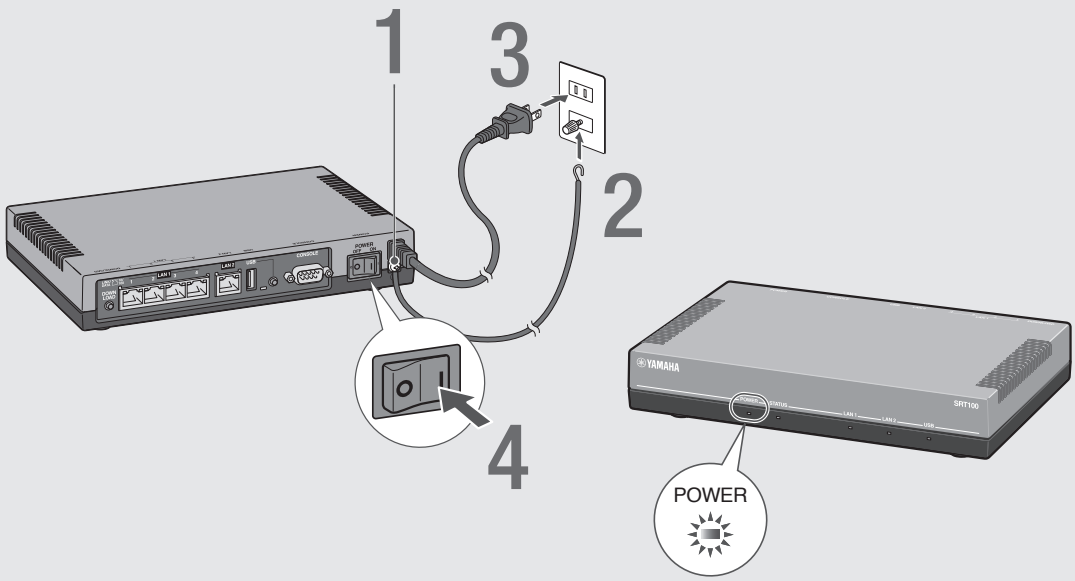
製品を管理／区分するための製造番号です。

④ MACアドレス

LAN1側とLAN2側それぞれに付与されている機器固有のネットワーク識別番号が記載されています。「00A0DE1C0000, 1」という上図の例の場合、LAN1側とLAN2側それぞれのMACアドレスは以下のようになります。

- **LAN1側MACアドレス：**00A0DE1C0000
- **LAN2側MACアドレス：**00A0DE1C0001

ケーブルと電源を接続する



1 アース端子のネジを+ドライバで少しゆるめてから、アースコードをアース端子に接続して固定する。

アースコードは必ず接続してください。感電防止やノイズ防止の効果があります。

2 アースコードをコンセントのアース端子へ接続する。

ご注意

アースコードは必ずコンセントのアース端子に接続してください。ガス管などには、絶対に接続しないでください。

3 本製品の電源コードをコンセントに接続する。

電源コードを取りはずす場合は

先に電源コードを取りはずしてから、アースコードを取りはずしてください。

4 本製品のPOWER（電源）スイッチを「ON」にして、電源を入れる。

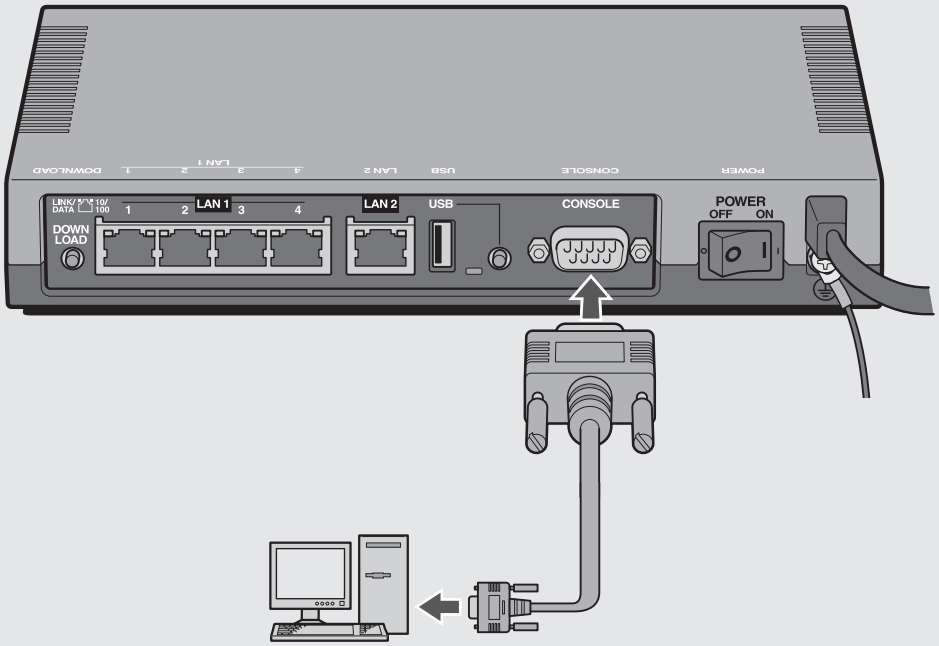
ランプが何回か点滅した後、POWERランプが点灯します。

パソコンをCONSOLEポートに接続する

以下の手順に従って、パソコンをCONSOLEポートに接続します。

1.パソコンを接続する

本製品のCONSOLEポートとパソコンを、クロスタイプのシリアルケーブルで接続します。



ヒント

シリアルケーブルの両端のコネクタは、本製品(D-sub9ピン、オス)とパソコンに適合したタイプをご使用ください。

2.CONSOLEポート番号を確認する

接続に使用するパソコンのシリアルポートが、どのCOMポート番号に割り当てられているのかを確認します。ここでは、Windows XP搭載パソコンから接続する場合を例に説明します。

1 **「スタート」メニューから「マイ コンピュータ」をクリックする。**

2 **「マイ コンピュータ」画面左側の「システムのタスク」欄にある、「システム情報を表示する」をクリックする。**

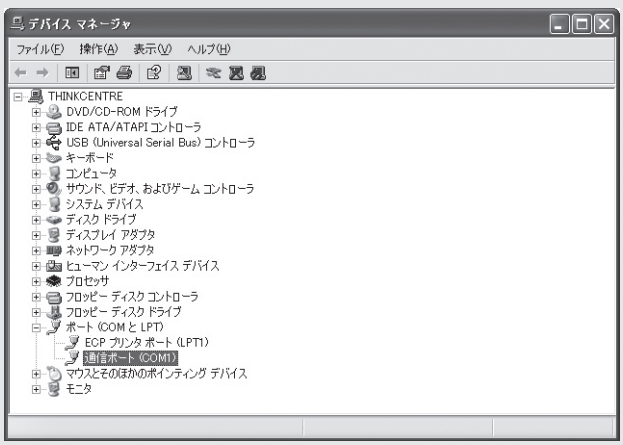
「システムのプロパティ」画面が表示されます。

3 **「ハードウェア」タブをクリックする。**

4 **「デバイス マネージャ」をクリックする。**

「デバイス マネージャ」画面が表示されます。

5 **「ポート（COMとLPT）」を展開して、「通信ポートのポート番号」（COMx）を確認する。**



通常は「COM1」が割り当てられています。

6 **「デバイス マネージャ」画面と「システムのプロパティ」画面を閉じる。**

Windows Vistaの場合は

「デバイス マネージャ」画面を表示するには、「コントロールパネル」画面で「システムとメンテナンス」をクリックしてから、「デバイスマネージャ」をクリックしてください。

3.CONSOLEポートを指定して接続する

CONSOLEポートに接続しているパソコンからターミナルソフトウェアで本製品にログインし、コンソールコマンドを送信して設定します。ここでは、Windows標準の「ハイパーターミナル」を使用する場合を例に説明します。

ご注意

- Windows Vistaには「ハイパーターミナル」などの標準通信ソフトウェアが用意されていません。シリアルポート(RS-232C)経由の通信に対応する、市販のソフトウェアを別途ご用意ください。なお、ボーレートやデータビット、パリティなどRS-232Cの通信設定については、手順4と同様に設定してください。
- コンソールコマンドは、コマンドの動作をよく理解した上でお使いください。Webブラウザ経由で管理者向け設定画面を使用して設定を変更してから、さらにコンソールコマンドで設定を変更すると、意図しない動作につながることがあります。設定後に意図した動作をするかどうか、必ずご確認ください。

ヒント

コンソールコマンドの詳細については、「コマンドリファレンス」(付属CD-ROMに収録)をご覧ください。

1 「スタート」メニューから「すべてのプログラム」–「アクセサリ」–「通信」–「ハイパーターミナル」をクリックする。

「接続の設定」画面が表示されます。

2 「名前」欄に接続名を入力する。

接続名は自由に設定してください。

3 「接続方法」で前ページで確認したパソコンのシリアルポート番号を選んでから、「OK」をクリックする。

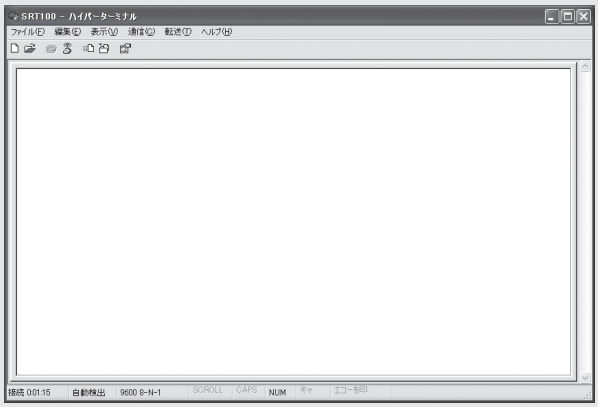
「COMxのプロパティ」画面が表示されます。

4 通信設定を以下の値に変更する。

- ビット/秒：9600
- データビット：8
- パリティ：なし
- ストップビット：1
- フロー制御：Xon/Xoff

5 「OK」をクリックする。

ハイパーターミナルの画面が表示されます。



6 Enterキーを押す。

「Password:」と表示されます。
引き続き、次ページからの説明に従ってコマンドで本製品の初期設定を行います。

初期設定をする

以下の手順に従って、本製品の初期設定を行います。

ヒント

- 各コマンドの書式などについて詳しくは、コマンドリファレンスを参照してください。
- コマンドに入力エラーがあった場合やコマンドの実行が失敗した場合は、結果が画面に表示されます。表示内容に従って対応してください。

1.本製品にログインして、パスワードを登録する

本製品へのアクセス権限は、設定や状態の確認だけを行う一般ユーザーと、設定の変更などを行う管理ユーザーの二段階に分かれています。初期状態では、一般ユーザーでログインしている場合のプロンプトは「>」、管理ユーザーの場合のプロンプトは「#」で表示されます。

本製品にログインして、管理ユーザーへ昇格する

一般ユーザーとして本製品にログインしてから、administratorコマンドで管理ユーザーに昇格します。

```
Password: <一般ユーザーログインパスワードを入力>
> administrator
Password: <管理者パスワードを入力>
#
```

ご注意

入力したパスワードは、画面には表示されません。

ヒント

本製品に初期設定されている一般ユーザーログインパスワードおよび管理者パスワードは、「doremi」です。

管理者パスワードを設定する

不用意にログインされないように、管理者パスワードを設定します。セキュリティ的に強固なパスワードとするために、15文字以上で英字の大文字・小文字、数字を混在させ、記号も使用するようにしてください。また、不揮発性メモリへの保存の際は、パスワードがそのままの形で保存さされないように設定します。

```
# administrator password encrypted
Old_Password:  <旧管理者パスワードを入力>
New_Password:  <新管理者パスワードを入力>
New_Password:  <新管理者パスワードをもう一度入力>
#
```

ご注意

administrator passwordコマンドは、encryptedキーワードを指定して実行してください。encryptedキーワードの指定なしで実行すると、不揮発性メモリにパスワードがそのままの形で保存されるため、設定内容を参照する際にそのままの形で見えることがあります。

2. ユーザーを登録する

必要最小限のユーザーを登録します。

- ユーザーの登録時に、ユーザー毎に管理ユーザーに昇格できるかどうかも設定できます。
- ユーザーのアクセス方法としては、通信パケットを暗号化できるSSHと、本製品への物理的なアクセスが必須となるCONSOLEポート経由だけを許可します。
- 初期設定状態では有効になっている、ユーザー名のないログインを禁止します。

ご注意

- 実行コマンドを出力するよう設定された後(後述するsyslog execute command をonにした後)でlogin userコマンドを実行する場合は、パスワードがログに記録されないようにログインパスワードを省略する入力形式でコマンド設定を行ってください。
- セキュリティ的に強固なパスワードとするために、15文字以上で英字の大文字・小文字、数字を混在させ、記号も使用するようにしてください。
- セキュリティ上、管理ユーザーに昇格できるユーザーは1名だけにしてください。

ユーザー「yamaha」を設定する場合の例

```
# login user yamaha
New_Password: <ログインパスワードを入力>
New_Password: <ログインパスワードをもう一度入力>
#
```

ユーザー「yamaha」の属性を設定する場合の例

```
# user attribute yamaha connection=serial,ssh multi-
    session=off administrator=on
#
```

ユーザー名のないログインを禁止する場合の例

```
# user attribute connection=off
#
```

3. 日付と時刻を設定する

ログで事象の発生時刻を正しく把握するために、本製品の日付と時刻を正しく設定します。必要に応じて定期的にrdateやntpで時刻を設定することもできます(schedule atコマンド、rdateコマンド、ntpdateコマンド)。

2007年5月23日16時30分に設定する場合の例

```
# date 2007/5/23
# time 16:30:00
#
```

4. 本製品へのアクセス方法を制限する

設定の盗聴を防ぐために、本製品へのアクセス方法を限定します。

- 通信パケットを暗号化できるSSHと、直接接続で盗聴の恐れのないCONSOLEポート経由だけを許可するため、セキュリティクラスのレベルを2に設定して、telnet経由やHTTP経由のアクセスを禁止します。
- CONSOLEポート経由での非常用パスワードを使えないように設定します。

```
# security class 2 off off
# telnetd service off
# httpd service off
#
```

5. 使用しないポートを無効化する

意図しないアクセスの可能性を減らすために、使用しないポートを無効にします。

- USBポートおよびダウンロードボタンでの操作を無効にします。
- 必要に応じてLAN1のポートも無効にすることができます(lan shutdownコマンド)。

```
# usbhost use off
# operation http revision-up permit off
#
```

6.syslogサーバーを設置する

意図した動作と異なる動作を本製品が行っている場合に、どのようなパケットを契機としているか、あるいはどのようなパケットがフィルタリングされているか、などを解析したい場合があります。また、本製品が設置される環境のセキュリティポリシーによっては、本製品へのアクセスや設定変更履歴の記録を残す必要があります。このような場合は、本製品のsyslog機能を利用してログを得るように設定します。

- 本製品の内部にもログは格納されますが、ログの量は限られたものとなります。内部に格納されたログを確認したい場合は、show logコマンドを使用します。
- 長時間にわたるログを記録するために、syslogの機能を持ったsyslogホストをsyslogサーバーとして別途用意し、通信ログを送信してsyslogサーバー側にログを記録します。ログの保存に十分なディスク容量を確保したsyslogサーバーを準備し、本製品のLAN1ポートとLANケーブルで接続してください。
- syslogサーバーは、ディスク容量が満杯になる前に管理ユーザーにアラートを出したり、ディスクを自動的にローテーションするなどして、必要なログが消えてしまうことがないように運用します。
- syslogサーバーおよびそれらを接続する管理用のネットワークは、システム管理者以外触れられない場所に設置してください。
- LAN1の各ポートでは、ポート分離機能を利用して特定ポート間の通信を禁止できます。必要に応じて設定してください(lan typeコマンド)。
- セキュリティ機能のログを残すために、noticeタイプおよびinfoタイプのsyslog、実行コマンドを出力するよう設定します。
- 通信量によってはログの量が膨大になることがありますので、必要に応じて設定で出力を切り替えてください。

```
# syslog host <syslogサーバーのIPアドレス>
# syslog facility user
# syslog info on
# syslog notice on
# syslog execute command on
#
```

7.LAN側の設定を変更する

必要に応じて、LAN側の設定を変更します。

- 初期状態で、LAN1には192.168.100.1/24のIPアドレスが設定されています。
- 初期状態で、ネットワークのDHCPサーバーとして動作するように設定されています。

初期設定例

```
# ip lan1 address 192.168.100.1/24
# dhcp service server
# dhcp server rfc2131 compliant except remain-silent
# dhcp scope 1 192.168.100.2-192.168.100.191/24
#
```

8.WAN側の設定を変更する

WAN側にはLAN2インターフェースを使用します。

- 接続形態にあわせて各コマンドを使用してください。
- コマンド設定例については、添付のCD-ROMに収録されている設定例集や、ヤマハホームページ(http://NetVolante.jp)を参照してください。

PPPoE接続の設定例

```
# nat descriptor type 1 masquerade
# pp select 1
pp1# pppoe use lan2
pp1# pp auth accept chap pap
pp1# pp auth myname <接続ID> <接続パスワード>
pp1# ppp ipcp ipaddress on
pp1# ppp ipcp msext on
pp1# ip pp nat descriptor 1
pp1# ppp lcp mru on 1454
pp1# ip pp mtu 1454
pp1# ppp ccp type none
pp1# pp enable 1
pp1# pp select none
# ip route default gateway pp 1
# dns server pp 1
# dns private address spoof on
#
```

9.フィルターを登録する

本製品が設置される環境のセキュリティポリシーに従い、フィルターを登録します。

- ヤマハポリシーフィルタリングモジュールのリビジョン番号は、show environment コマンドで確認できます。

バージョンの表示例

```
# show environment
SRT100 BootROM Ver.1.00
SRT100 Rev.10.00.21 (Thu Jul  5 14:15:39 2007)
YAMAHA Policy Filtering module Rev.1.02(2)
...
```

- フィルターが一つも登録されていない状態では、すべての通信パケットが通過します。
- 許可するパケットだけを通過させるために、ポリシーフィルターを一つ以上登録します。
- 必要に応じて入力遮断フィルターなども登録します。

ポリシーフィルターの設定例

```
# ip policy interface group 101 name=Private local lan1
# ip policy interface group 102 name=Global pp*
# ip policy address group 101 name=Private 192.168.100.0/24
# ip policy address group 102 name=Any *
# ip policy service group 101 name="Open Services"
# ip policy service group 102 name=General dns
# ip policy service group 103 name=Mail pop3 smtp
# ip policy filter 1100 reject-log lan1 * * * *
# ip policy filter 1110 pass-nolog * * * * 102
# ip policy filter 1120 static-pass-nolog * 101 * * *
# ip policy filter 1121 static-pass-log * * 101 * http
# ip policy filter 1140 pass-nolog * pp1 * * *
# ip policy filter 1500 reject-log 102 * * * *
# ip policy filter 1510 reject-log * 101 * * *
# ip policy filter 1511 pass-log * * * * 101
# ip policy filter 1700 pass-nolog local * * * *
# ip policy filter 1710 static-pass-nolog * lan1 * * *
# ip policy filter 2000 reject-log * * * * *
# ip policy filter set 1 1100 [1110 1120 [1121] 1140] 1500 [1510
   [1511]] 1700 [1710] 2000
# ip policy filter set enable 1
#
```

入力遮断フィルターの設定例

```
# ip inbound filter 1001 reject-nolog * * tcp,udp * 135
# ip inbound filter 1002 reject-nolog * * tcp,udp 135 *
# ip inbound filter 1003 reject-nolog * * tcp,udp * netbios_ns-
   netbios_ssn
# ip inbound filter 1004 reject-nolog * * tcp,udp netbios_ns-
   netbios_ssn *
# ip inbound filter 1005 reject-nolog * * tcp,udp * 445
# ip inbound filter 1006 reject-nolog * * tcp,udp 445 *
# ip inbound filter 1007 reject-nolog 192.168.100.0/24 * * * *
# ip inbound filter 1008 pass-nolog * * * * *
# pp select 1
pp1# ip pp inbound filter list 1001 1002 1003 1004 1005 1006
   1007 1008
pp1#
```

10.設定を保存する

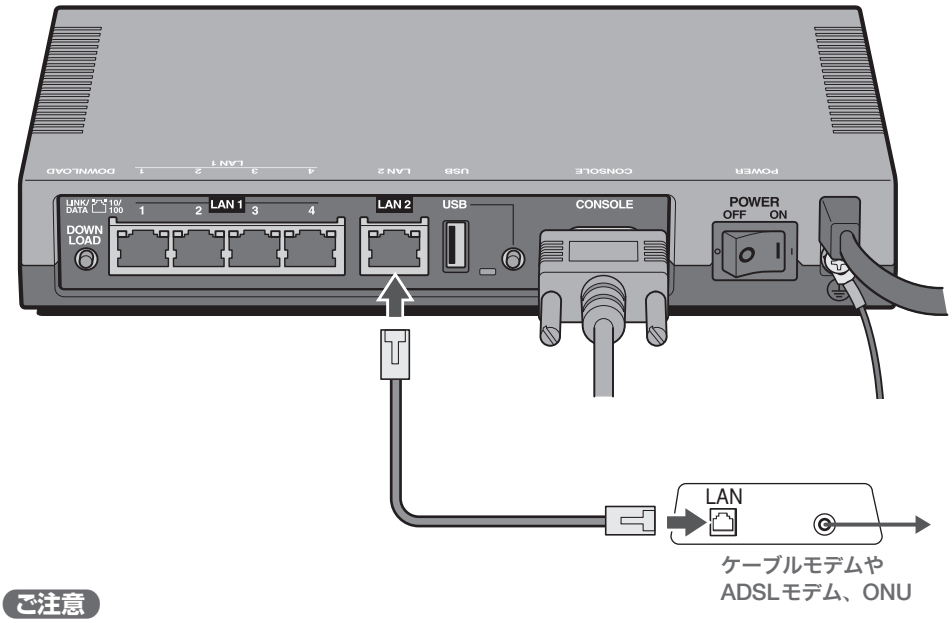
これまでに設定した内容を本製品の内蔵不揮発性メモリに保存します。不揮発性メモリに保存することで、再起動後も同じ設定内容で動作することができます。

```
# save
セーブ中... CONFIG0 終了
#
```

11.WAN側のケーブルを接続する

ケーブルモデムやADSLモデム、ONUのLANポートと本製品のLAN2ポートを、LANケーブルで接続する。

プロバイダの資料やADSLモデム、ONUの取扱説明書もあわせてご覧ください。



ご注意

- セキュリティ的に危険性のあるネットワークに接続する場合は、あらかじめ適切なフィルタリングの設定をしてからケーブルを接続してください。
- ケーブルモデムやADSLモデム、ONUとパソコンを直接接続している環境を本製品との接続に切り替えたり、設置されていたルーターを本製品に置き換えた場合に、アドレスが取得できないなどの原因で正常接続できないことがあります。場合により、環境の変更後に何らかの設定やリセット操作、指定時間(例:20分以上)待つこと、などが必要となる場合があります。詳しくは、それらの取扱説明書の指示に従ってください。

12.接続を確認して、ログアウトする

ケーブルの接続後に、状態表示のコマンドを使用して接続の状態を確認します。

- WAN側への接続が成功しているか(show status ppコマンドやshow status dhcpcコマンド)
- フィルターは機能しているか(show status ip policy filterコマンド)
- 必要なコマンド操作が終了したら、速やかにexitコマンドを使用して管理ユーザーから抜け、さらにもう一度exitコマンドを使用してログアウトしてください。

```
# exit
> exit
```

SSHを使用する

本製品の設定参照および変更を遠隔から行う場合は、SSHを使用します。
ホスト側で使用するSSHクライアントは、MacOS X の「ターミナル」アプリケーションやUNIX 環境では標準的に搭載されていますが、Windows 系OSでは標準では搭載されていません。SSHクライアントが搭載されていない環境では、フリーソフトウェアなどでSSHクライアント機能のあるものを用意してください。使用にあたっての注意事項と、使用するための手順を以下に示します。

使用にあたっての注意事項

本製品のSSHサーバ機能では、以下の機能をサポートしていないことに注意してください。

- SSHプロトコルバージョン1
- パスワード認証以外のユーザ認証(ホストベース認証、公開鍵認証、チャレンジ・レスポンス認証、GSSAPI 認証)
- ポートフォワーディング(X11/TCP 転送)
- Gateway Ports(ポート中継)
- 空パスワードの許可
- scp
- sftp

SSHサーバー機能を有効にする

19～24ページまでの説明に従って本製品への接続およびログインを完了してから、以下の手順でSSHサーバ機能を有効にします。

- SSHサーバー機能を使用するためには、事前に設定したユーザー「yamaha」(25ページ)のように、名前のあるユーザーをlogin userコマンドで登録する必要があります。
- sshd host key generateコマンドを実行してDSAまたはRSAの公開鍵、および秘密鍵のペアを生成します(コマンドの処理には時間がかかる場合があります)。
- sshd serviceコマンドを実行して、SSHサーバー機能を有効にします。
- SSHでアクセスするホストを限定したり(sshd hostコマンド)、ポート番号を変更したり(sshd listenコマンド)することもできます。

```
# sshd host key generate
Generating public/private dsa key pair ...
|*******
Generating public/private rsa key pair ...
|*******
# sshd service on
#
```

鍵が生成されると、SSHクライアントからパスワード認証方式でアクセスできます。

通信状態を確認する

本製品の動作状態や通信状態を確認できます。代表的なコマンドを以下に示します。他にも各種機能にあわせて、様々な状態表示コマンドがあります。詳しくは、コマンドリファレンスをご覧ください。

ヒント

- 本製品への接続およびログインを完了してから、各コマンドを実行してください。
- 各コマンドの書式などについて詳しくは、コマンドリファレンスを参照してください。
- コマンドに入力エラーがあった場合やコマンドの実行が失敗した場合は、結果が画面に表示されます。表示内容に従って対応してください。

本製品のファームウェアバージョンや動作状況を確認する

```
show environment
```

WAN側への接続状態を確認する

PPPoE接続などの場合

```
show status pp
```

DHCPクライアントとして接続している場合

```
show status dhcpc
```

LANインタフェースの状態を確認する

```
show status lan
```

ポリシーフィルターの状態を確認する

```
show status ip policy filter
```

経路情報テーブルを確認する

```
show ip route
```

ログインしているユーザーを確認する

```
show status user
```

ログを確認する

syslogサーバーに格納されるログを管理することで、本製品へのアクセスや操作、通信パケットの監視などを行うことができます。

ヒント

- 本製品への接続およびログインを完了してから、各コマンドを実行してください。
- 各コマンドの書式などについて詳しくは、コマンドリファレンスを参照してください。
- コマンドに入力エラーがあった場合やコマンドの実行が失敗した場合は、結果が画面に表示されます。表示内容に従って対応してください。

必要な情報をログに残すために、以下のコマンド設定で運用してください

```
syslog execute command on
syslog info on
syslog notice on
```

ヒント

- syslog execute command onは実行に成功したコマンド入力をログに出力し、操作履歴を残すためのものです。
- infoレベルのログは、主にログインログアウトやコマンド実行などの情報です。
- noticeレベルのログは、主にフィルタリングで処理されるパケットに関わる情報のログです。

ご注意

show logコマンドで本製品内部に一時的に格納されているログを確認できますが、本製品内部に格納できるログの量には制限があります。

ログの表示例

表示されるログの例を示します(斜体字部分は、状況により変化することを表します)。

一般ユーザーのログイン(成功時)

2007/03/15 20:23:31: Login succeeded for ***Serial***: *ユーザー名*

一般ユーザーのログイン(失敗時)

2007/03/15 20:27:21: Login failed for ***Serial***

管理ユーザーのログイン(成功時、administratorコマンド)

2007/03/15 20:23:36: 'administrator' succeeded for ***Serial***
user: *ユーザー名*

管理ユーザーのログイン(失敗時、administratorコマンド)

2007/03/15 20:28:00: 'administrator' failed for ***Serial*** user:
ユーザー名

一般ユーザーのログアウト
（exitまたはquitコマンド使用時、あるいはタイマ満了時）

2007/03/15 20:23:44: Logout from ***Serial***: *ユーザー名*

ユーザーの追加

2007/03/15 20:23:31: [MMI] Executed by ***Serial(****ユーザー名****)***: login user ***user***

ロギング機能の無効化

2007/03/15 19:32:34: [MMI] Executed by ***Serial(****ユーザー名****)***:syslog info off

2007/03/15 19:32:36: [MMI] Executed by ***Serial(****ユーザー名****)***:syslog notice off

2007/03/15 19:32:38: [MMI] Executed by ***Serial(****ユーザー名****)***:syslog execute command off

ロギング機能の有効化

2007/03/15 19:32:40: [MMI] Executed by ***Serial(****ユーザー名****)***:syslog execute command on

2007/03/15 19:32:42: [MMI] Executed by ***Serial(****ユーザー名****)***:syslog info on

2007/03/15 19:32:44: [MMI] Executed by ***Serial(****ユーザー名****)***:syslog notice on

ポリシーに合致するコネクションやパケットの発生

2007/03/15 20:23:31: ***Passed/Rejected/Restricted*** at Policy Filter***(****ポリシー番号****)***: *プロトコル パケットの情報*

ポリシーの設定

2007/03/15 20:23:31: [MMI] Executed by ***Serial(****ユーザー名****)***: ip policy filter 1 reject-log lan2 lan1 * * telnet

2007/03/15 20:23:31: [MMI] Executed by ***Serial(****ユーザー名****)***: ip policy filter 2 pass-log lan1 lan2 * * ping

2007/03/15 20:23:31: [MMI] Executed by ***Serial(****ユーザー名****)***: ip policy filter set 1 1 2

2007/03/15 20:23:31: [MMI] Executed by ***Serial(****ユーザー名****)***: ip policy filter set enable 1

ユーザーを管理する

ユーザーの追加や削除、ログイン状態のユーザーを確認できます。

ヒント

- 本製品への接続およびログインを完了してから、各コマンドを実行してください。
- 各コマンドの書式などについて詳しくは、コマンドリファレンスを参照してください。
- コマンドに入力エラーがあった場合やコマンドの実行が失敗した場合は、結果が画面に表示されます。表示内容に従って対応してください。

ユーザーを追加する

「初期設定する」の「2.ユーザーを登録する」(25ページ)をご覧ください。

ユーザーを削除する

login userコマンドとuser attributeコマンドを消去します。

ユーザー「yamaha」を削除する場合の例

```
# no login user yamaha
# no user attribute yamaha
```

ログイン状態のユーザーを確認する

show status userコマンドを使用して、ログイン状態のユーザーを確認できます。

パスワードを変更する

セキュリティ的に強固なパスワードとするために、15文字以上で英字の大文字・小文字、数字を混在させ、記号も使用するようにしてください。

ヒント

- 本製品への接続およびログインを完了してから、各コマンドを実行してください。
- 各コマンドの書式などについて詳しくは、コマンドリファレンスを参照してください。
- コマンドに入力エラーがあった場合やコマンドの実行が失敗した場合は、結果が画面に表示されます。表示内容に従って対応してください。

一般ユーザーパスワードを変更する

ユーザー「yamaha」のパスワードを変更する場合

```
# login user yamaha
Old_Password:<旧パスワードを入力>
New_Password:<新パスワードを入力>
New_Password:<新パスワードをもう一度入力>
```

管理者パスワードを変更する

「初期設定する」の「1.本製品にログインして、パスワードを登録する」(24ページ)をご覧ください。

フィルターの設定を変更する

本製品を設置する環境のセキュリティポリシーを変更した場合や、ログから意図しない通信やフィルターの動作を確認した場合には、フィルターの設定を変更して対処します。

ヒント

- 本製品への接続およびログインを完了してから、各コマンドを実行してください。
- 各コマンドの書式などについて詳しくは、コマンドリファレンスを参照してください。
- コマンドに入力エラーがあった場合やコマンドの実行が失敗した場合は、結果が画面に表示されます。表示内容に従って対応してください。

例1：LAN2からLAN1への一切のアクセスを禁止し、LAN1からLAN2へのHTTPDによるアクセスだけを許可する場合

```
# ip policy filter 1 reject-log * * * * *
# ip policy filter 20 reject-log lan1 local * * *
# ip policy filter 30 reject-log local lan2 * * *
# ip policy filter 40 reject-log lan1 lan2 * * *
# ip policy filter 200 pass-log * * * * udp/53
# ip policy filter 300 pass-log * * * * udp/53
# ip policy filter 400 pass-log * * * * tcp/80
# ip policy filter set 1 1 [20 [200] 30 [300] 40 [400]]
# ip policy filter set enable 1
```

例2：必要な通信パケットが破棄されている場合

例1（前ページ）の設定環境において、本製品へのSSH接続を許可する場合を考えます。
例1の設定ではSSH接続はできずに、SSH接続を試みても接続は失敗します。
この時点でログを確認すると、

```
2007/07/23 18:12:29: Rejected at Policy Filter(20): TCP
   192.168.100.2:1583 > 192.168.100.1:22
```

と表示され、ポリシーフィルター20番の設定によりSSHのパケットが破棄されていることがわかります。従って、以下のようにSSHのパケットを通過させる設定を追加します。

```
# ip policy filter 100 pass-log * * * * tcp/22
# ip policy filter set 1 1 [100 20 [200] 30 [300] 40 [400]]
# ip policy filter set enable 1
```

設定後にSSH接続が正しくできることを確認します。ログを確認すると、追加した100番のフィルターによってSSHのパケットが正しく通過していることがわかります。

```
2007/07/23 18:13:06: Passed at Policy Filter(100): TCP
   192.168.100.2:1584 > 192.168.100.1:22
2007/07/23 18:13:11: Login succeeded for SSH: 192.168.100.2
   yamaha
```

この時点でのポリシーフィルターの設定は、以下のようになります。

```
ip policy filter 1 reject-log * * * * *
ip policy filter 20 reject-log lan1 local * * *
ip policy filter 30 reject-log local lan2 * * *
ip policy filter 40 reject-log lan1 lan2 * * *
ip policy filter 100 pass-log * * * * tcp/22
ip policy filter 200 pass-log * * * * udp/53
ip policy filter 300 pass-log * * * * udp/53
ip policy filter 400 pass-log * * * * tcp/80
ip policy filter set 1 1 [100 20 [200] 30 [300] 40 [400]]
ip policy filter set enable 1
```

例3：不要な通信パケットが通過している場合

例2（前ページ）の設定環境において、LAN1側から本製品へのSSH接続だけを許可したい場合を考えます。例2の設定ではLAN2側からも本製品へSSH接続でき、LAN1とLAN2の間でもSSHのパケットが通過できます。
例えばLAN2側を172.16.0.1/24としてLAN2側のホスト172.16.0.2から本製品にSSHで接続すると、接続は成功します。この時点でログを確認すると、以下のように記録されています。

```
2007/07/23 18:15:48: Passed at Policy Filter(100): TCP
   172.16.0.2:4174 > 172.16.0.1:22
```

ここで本製品へのSSH接続を、LAN1からだけに限定するように設定を変更します。

```
# no ip policy filter 100 pass-log * * * * tcp/22
# ip policy filter 201 pass-log * * * * tcp/22
# ip policy filter set 1 1 [20 [200 201] 30 [300] 40 [400]]
# ip policy filter set enable 1
```

設定後にLAN2からのSSH接続ができないこと、LAN1からのSSH接続ができることを確認します。ログを確認すると、LAN2からのSSHのパケットは破棄され、LAN1からのSSHのパケットは正しく通過していることがわかります。

```
2007/07/23 18:20:29: Rejected at Policy Filter(1): TCP
   172.16.0.2:4175 > 172.16.0.1:22
2007/07/23 18:21:41: Passed at Policy Filter(201): TCP
   192.168.100.2:1593 > 192.168.100.1:22
2007/07/23 18:21:45: Login succeeded for SSH: 192.168.100.2
   yamaha
```

この時点でのポリシーフィルターの設定は、以下のようになります。

```
ip policy filter 1 reject-log * * * * *
ip policy filter 20 reject-log lan1 local * * *
ip policy filter 30 reject-log local lan2 * * *
ip policy filter 40 reject-log lan1 lan2 * * *
ip policy filter 200 pass-log * * * * udp/53
ip policy filter 201 pass-log * * * * tcp/22
ip policy filter 300 pass-log * * * * udp/53
ip policy filter 400 pass-log * * * * tcp/80
ip policy filter set 1 1 [20 [200 201] 30 [300] 40 [400]]
ip policy filter set enable 1
```

ファームウェアを バージョンアップする(リビジョンアップ)

ヤマハホームページから入手したファームウェアを本製品にtftpで転送して、リビジョンアップを行います。リビジョンアップしても設定内容は保存されます。

ご注意

- リビジョンアップが終了して、本機が再起動するまでの間は、絶対に本機の電源を切らないでください。不揮発性メモリへの書き込み中に電源を切ると、本機を再度起動することができない状態になります。
- 万一電源を入れ直しても再起動できなくなった場合には、ヤマハルーターお客様ご相談センターまでご連絡ください。

ここでは本製品側の設定を変更してから、LAN上のパソコンからファームウェアを転送する場合の操作について説明します。

ヒント

- TFTPの実行形式はそれぞれのOSに依存します。次のポイントに注意して実行してください。
  - 転送モードはバイナリにします(binaryやbin と表現されます)。
  - 本機側のファイル名はexecで固定されています。送信元のファイル名は、SRT100の場合srt100.binです。
- 本製品への接続およびログインを完了してから、各コマンドを実行してください。
- 各コマンドの書式などについて詳しくは、コマンドリファレンスを参照してください。
- コマンドに入力エラーがあった場合やコマンドの実行が失敗した場合は、結果が画面に表示されます。表示内容に従って対応してください。

1 本製品側の設定を変更する。

TFTPでファームウェアを転送する、ホストのIPアドレスを指定します。また、リビジョンアップ中の不安定な状態を避けるために、PP側の通信を中止します。

ホストのIPアドレスが192.168.112.25の場合の例

```
> administrator
Password:
# save
セーブ中．．．
セーブ終了
# tftp host 192.168.112.25
# pp disable all
#
```

ご注意

- saveコマンドの後で実行されたコマンドは、不揮発性メモリには保存されていません。本製品の再起動後には、それらの設定は有効ではないことにご注意ください。
- 通信中にリビジョンアップすることもできますが、タイミングによっては、その直後動作が不安定になることがあります。そのような場合は、電源を入れ直してください。

2 TFTPでファームウェアを転送するホスト側(Windows XPパソコン)で、「スタート」メニューから「すべてのプログラム」–「アクセサリ」–「コマンド プロンプト」をクリックする。

コマンドプロンプトが起動します。

3 「コマンド プロンプト」画面上で、用意したファームウェアが保存されているディレクトリに移動する。

4 「コマンド プロンプト」画面上でTFTPコマンドを使用して、ファームウェアを本機へ転送する。

本製品のIPアドレスが192.168.100.1の場合の例

```
C:\>tftp -i 192.168.100.1 put srt100.bin exec
```

パソコンから本製品へファイル転送が始まると

本製品のコンソール画面では、経過が順次表示されます。不揮発性メモリへの書き込みが終了すると、本製品は自動的に再起動します。

```
Update exec file receiving... Testing received file... Writing
   to Nonvolatile memory... done
Restarting ...
```

再起動してから約10～20秒後に通信可能な状態になります。

5 本製品のコンソール画面でshow environmentコマンドを実行して、ファームウェアのリビジョンを確認する。

```
# show environment
SRT100 BootROM Ver.1.00
SRT100 Rev.10.00.21 (Thu Jul  5 14:15:39 2007)
YAMAHA Policy Filtering module Rev.1.02(2)
...
```

複数の設定ファイルを利用する

本製品は設定ファイル(config)を最大5つ保持できます。saveコマンドで不揮発性メモリに保存する際にファイル名を指定するだけでなく、コメントを付与したり、起動時の設定ファイルを選択することもできます。

1 本製品のPOWERスイッチをON にする。

POWERランプが点灯します。
本製品のCONSOLEコネクタにシリアル端末が接続されている場合は、本製品のファームウェアのバージョンが表示され、Enterキーの入力待ち状態になります。(10秒間)。

2 「Will start automatically in～ 」のカウントダウンが終わらないうちに、シリアル端末側でEnterキーを押す。

タイムアウトがキャンセルされ、設定ファイル待ち状態になります。

複数の設定ファイルが存在する場合の例

```
SRT100 BootROM Ver.1.00
Copyright (c) 2007 Yamaha Corporation

Press 'Enter' or 'Return' to select a configuration.
Default settings :  config0

No.   Date       Time     Size    Sects   Comment
----- ---------- -------- ------- ------- --------------------
0    2007/05/29 21:34:12     213 130/130 tokyo
1    2007/05/29 21:34:07     219 131/131 test_config
2    2007/05/29 21:34:27     217 129/129 hamamatsu
----- ---------- -------- ------- ------- --------------------
Select the configuration :
```

シリアル端末が接続されていない場合や、接続されていてもキー入力がない場合は

10秒後にデフォルト設定ファイルで自動的に起動します。

- 工場出荷設定では、設定ファイル0で起動します。
- set-default-configコマンドが設定されている場合は、指定されたデフォルト設定ファイルで起動します。
- デフォルト設定ファイルが存在しない場合は、「何も設定されていない」状態で起動します。

3 **0〜4.2のうちで、使用したい設定ファイル名を指定してから Enterキーを押す。**

ファームウェアが起動すると

- ファームウェアのリビジョンなどをシリアル端末に表示して、ルーターとして動作を始めます。
- 本製品の電源を入れ直す場合には、電源を切ってから再度電源を入れるまでの間に、10秒以上の時間をおいてください。

設定を工場出荷時の状態に戻す

本機をまったく別のネットワークで使用するために移動させて使う場合や、問題の設定箇所が特定できないためにすべての設定をやり直したい場合には、本機の設定内容をすべて消去して設定し直した方が時間を節約できることがあります。

ヒント

- 本製品への接続およびログインを完了してから、各コマンドを実行してください。
- 各コマンドの書式などについて詳しくは、コマンドリファレンスを参照してください。
- コマンドに入力エラーがあった場合やコマンドの実行が失敗した場合は、結果が画面に表示されます。表示内容に従って対応してください。

すべての設定を工場出荷時の状態に戻す場合は、cold startコマンドを使用します。
このコマンドを実行すると管理パスワードの入力を要求されます。管理パスワードの照合が確認されると、以下の処理を行った上で自動的に再起動します。

- デフォルト値が存在する設定は、すべてデフォルト値になります。
- フィルターの定義やIPアドレスなどの情報は消去されます。

```
> administrator
Password:
# cold start
Password:
Restarting ...
```

ご注意

cold startコマンドを使用すると、IPアドレスをはじめとする通信のための設定も消去されます。SSHでログインしている場合は、通信が切断されてしまいますのでご注意ください。

cold startコマンドと restartコマンドの違い

cold startコマンドでは不揮発性メモリの内容を工場出荷直後の設定に書き換えてから再起動しますが、restartコマンドでは現在の不揮発性メモリの内容に従って再起動します。

サポート窓口のご案内

お問い合わせの前に

本書をもう一度ご確認ください

本書をよくお読みになり、問題が解決できるかどうかご確認ください。
また、取扱説明書の「困ったときは」もあわせてご覧ください。

ログ情報や設定情報をご確認ください

お客様のルーターの状態を把握するために、弊社の担当者がログ(Syslog)情報や設定(config)情報を確認させていただくことがあります。ログ情報や設定情報を問題の症状とあわせてお知らせいただくことで、問題の解決が早まることがあります。
ログ情報はshow logコマンドあるはsyslogサーバーでのログ、設定情報はshow configコマンドでご確認ください。

お問い合わせ窓口

本製品に関する技術的なご質問やお問い合わせは、下記へご連絡ください。

ヤマハルーターお客様ご相談センター

TEL：053-478-2806
FAX：053-460-3489

ご相談受付時間

9:00~12:00 13:00~17:00
（土・日・祝日、弊社定休日、年末年始は休業とさせて頂きます。）

お問い合わせページ

http://NetVolante.jp/
http://www.rtpro.yamaha.co.jp/

●ヤマハルーターお客様ご相談センター
TEL 053-478-2806
FAX 053-460-3489
ご相談受付時間
9:00～12:00　13:00～17:00
（土・日・祝日、弊社定休日、年末年始は休業とさせて頂きます。）
お問い合わせページ
http://NetVolante.jp/
http://www.rtpro.yamaha.co.jp/

WM77580

（0707第1版）