

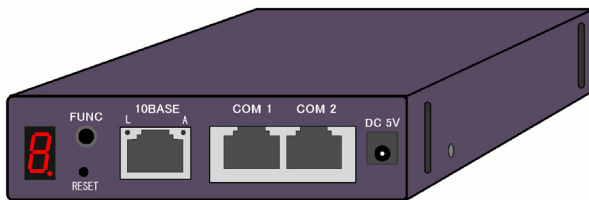
RouteMagic

RouteMagic Controller

RMC-MP200

取扱説明書

RMC Version 2.1



この取扱説明書をよくお読みになり正しくご利用ください

ROUTREK
NETWORKS

はじめに

このたびは RouteMagic Controller (以下 RMC)をお買い上げいただき、まことにありがとうございます。本書は、お客様に RMC を安全で正しくお使いいただくためのものです。当製品をお使いになる前に、必ずお読みになり取り扱い方や注意事項を充分ご理解いただいた上でご使用ください。

ご使用にあたって

- (1) 本書の内容の一部または全部を無断で転載することは固くお断りします。
- (2) 本書の内容については、改良のため予告なしに変更することがあります。
- (3) 本書に記載された使用方法を守らずに起きた故障・事故については保証できませんので、本書を良くお読みの上、かならず保管してください。
- (4) 正常にご使用になり不良が発生した場合は、保障期間内に限り修理または無償交換をさせていただきますが、他の設備・機器への損傷は保証いたしかねます。
- (5) 当製品、および当製品に搭載される、弊社が著作権を持つソフトウェアに対して、無断でコピー、逆アセンブル、逆コンパイル、リバースエンジニアリング等を行うことは固くお断りします。
- (6) 当製品を海外に持ち出す場合、輸出貿易管理令及び外国為替令に基づくパラメータシート（製品が戦略物資に該当するか否かを判定する該非判定書）を要求されることがあります。パラメータシートを必要とされる場合は、弊社宛ご連絡ください。

安全にお使いいただくために

本機器は精密機器です。ご使用にあたっては、次の事項をよく読んで正しくお使いください。



警告

本機器は一般オフィスの OA 機器として設計されています。人命に直接関わる医療機器のような極めて高い信頼性ないし安全性が必要とされる機器には接続しないで下さい。誤って本機を使用した結果、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。

万一、本機から異常な臭いがしたり、過熱や発煙があるとき、および内部に水分や薬品類が入ったときは、直ちに電源コードをコンセントから抜いてください。そのまま使用すると火災や感電の恐れがあります。本機器を取り外して、お買い上げの販売店、もしくは弊社までご相談ください。

本機器を開けて内部の部品に触れたり、改造を行ったりしないでください。感電・故障・火災の原因となります。この場合の故障は、保障期間であっても保証できなくなりますので、ご注意ください。

本機器の電源ケーブルを傷つける・引っ張る・無理に折り曲げるなどを行わないでください。感電・故障・火災の原因となります。

本機器は日本国内用 AC100V(50/60Hz)の電源専用です。他の電源で使用しないでください。感電・故障・火災の原因となります。



注意

本機器を使用される場所の温度・湿度の環境は、本説明書の機器仕様一覧に記載されている定格範囲内でご使用ください。定格外の環境で使用された場合は、火災、故障の原因となります。

本機器を極端に温度差が大きい場所や結露が発生しやすい場所で使用しないでください。感電・火災・故障・動作不良の原因となります。結露が発生した場合は、電源コードを抜き、十分乾燥させてからご使用ください。火災・故障の原因となります。

本機器は屋内で使用されることを前提に設計されています。ほこり、ちり、雨の多いところで使用しないでください。感電・故障・火災・破損の原因となります。

本機器の内部やコネクタに金属類・ほこり・燃えやすいものなどの異物が入らないようご注意ください。感電・火災・故障の原因となります。

本機器を長期間無人で使用される場合は、定期的に保守・点検を行ってください。火災・故障・動作不良の危険があります。

目次

パッケージ内容の確認	1
製品各部の名称	1
RMC の設置	2
■監視対象装置とネットワークへの接続	2
■シリアル端末／モデムとの接続	4
RMC の起動	6
■電源の投入	6
■LED 表示の確認	6
RMC の初期設定	8
■ログインの方法	8
■IP アドレスの設定（DHCP サーバが用意されていない場合）	10
■パスワードの設定	11
■ユーザ名の追加とホスト名の変更	12
■日付と時刻の設定	12
■COM1／COM2 ポートの設定	13
ローカルコンソール／モデム接続の機能と設定	15
■ローカルコンソールとしての利用	15
■モデム接続時の機能と設定	16
■PPP 接続のテスト	19
電子メールサービスの設定	20
■電子メールサービスの設定とサービスの開始	20
■電子メールの送信テスト	22
■電子メールの受信テスト	22
RMC の機能とフィルタ・スクリプト	23
■フィルタとスクリプトの機能	23
■装置種別の定義	24
■フィルタの設定	25
■デフォルトフィルタの利用（重要度別のメール送信）	26
■フィルタの設定確認テスト	27
■スクリプトの設定	28
■RMC の生存確認（キープアライブ）情報の送信	29
■監視対象装置の生存確認	30
■監視対象装置およびネットワーク関連情報の自動送信	31
■RMC 機能の利用と設定コマンド	32

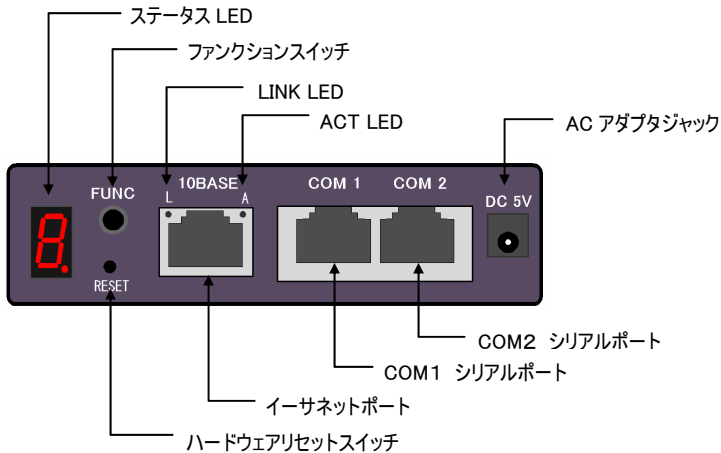
SNMP エージェントの機能と設定	34
■SNMP エージェント機能の設定	34
■SNMP Trap の設定	34
RMS (RouteMagic Server) に対する設定	35
■メールポート (ml0) と COM1/2 の設定	35
■メールの暗号化と認証に関する設定	36
■フィルタの設定	37
■RMS 用 SSH パスワードの設定	37
■RMS への RMC の登録	37
監視対象装置の操作	38
設定の表示と保存	39
ファンクションスイッチの機能	40
ハードウェアリセットと電源のオフ	41
製品に対するお問い合わせ	42
製品仕様	43
■本体仕様	43
■COM/COM2 ポート仕様	43
■付属ケーブル/コネクタ仕様	43
商標とライセンス	45

パッケージ内容の確認

お買い求め頂いた RouteMagic Controller（以下 RMC）には、以下のものが梱包されています。ご使用になる前に、すべてそろっていることを確認してください。

- RouteMagic Controller (RMC)本体 1台
- AC アダプタ 1個
- RJ-45-ROLLED シリアルケーブル（2m） 1本
- RJ-45-DB9 ソケット変換コネクタ 1個
- RJ-45-DB9 プラグ変換コネクタ 1個
- 取扱説明書（本書） 1冊（保証書）
- クイックリファレンス 1冊

製品各部の名称



ステータス LED	RMC の動作状態を表示します。
ファンクションスイッチ	RMC のシャットダウン／リブート、および各種状態の表示／設定機能を提供します。
LINK LED	10BASE-T のリンクが確立すると点灯します。
ACT LED	10BASE-T のデータ送受信時に点滅します。
ハードウェアリセットスイッチ	RMC をリブート（再起動）します。シャットダウンは実行されません。

RMC の設置

■ 監視対象装置とネットワークへの接続

まず、RouteMagic Controller（以下 RMC と記述）を監視対象装置（監視対象とするネットワーク機器）と LAN に接続します。

- ① 監視対象装置のコンソールポートと COM1 / COM2（シリアルポート）を接続
- ② イーサネットポートを LAN に接続
- ③ AC アダプタジャックに付属の AC アダプタを接続（電源ケーブルの脱着防止、参照）

必要なケーブル

- LAN のタイプに合わせたイーサネットケーブル 1 本
- シリアルケーブル 監視対象装置接続用

監視対象装置との接続には、各装置に付属のシリアルケーブルをご使用ください。

（注）モデム／シリアル端末接続用として利用されない場合は、RMC に添付されたシリアルケーブルの利用が可能です。付属のケーブル、および変換コネクタの仕様については、巻末の製品仕様の項をご参照ください。

監視対象装置要件

- RS-232C/D をコンソールポートとして持つこと。
- コンソールポートは ダム端末（ascii 文字出力）として機能すること。
- エラーメッセージ、その他ログをコンソールポートに出力すること。

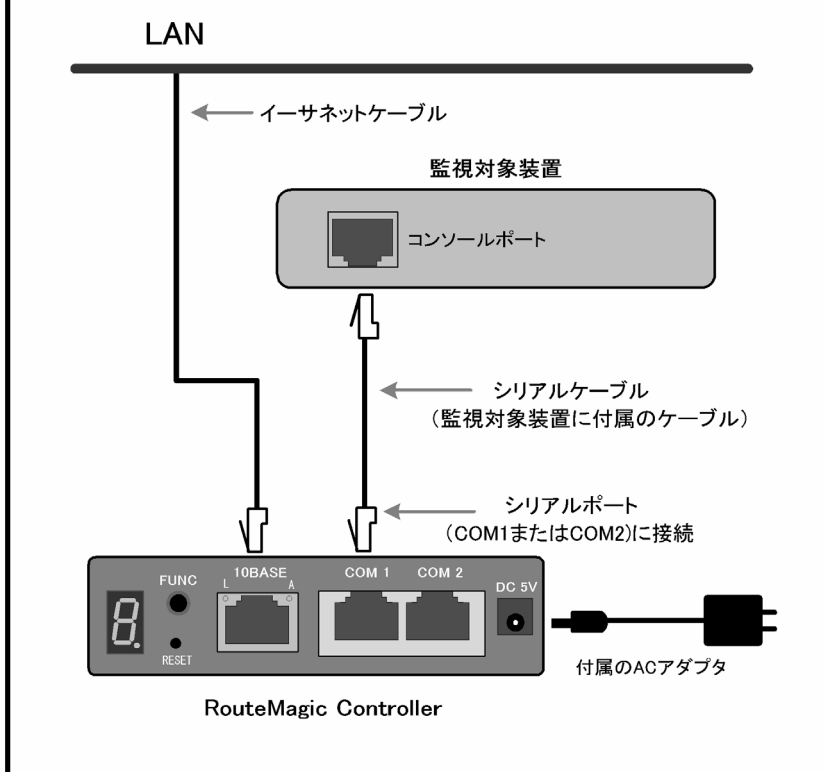
RMC 接続ネットワーク要件

- TCP/IP ネットワーク（IP バージョン 4）であること。
- インターネット上ホストへ SMTP を用いた IP reachable であること。

RMC 接続ネットワーク推奨事項

- 正しく設定された DNS サーバへ IP reachable であること。
- メール送受信先の MTA(Mail Transfer Agent)とダイレクトに通信可能であること(リレーホストや POP でのメール受信を使用しないこと)。
- DHCP または RARP サーバが用意されていること。
- NTP サーバが用意されていること
- TFTP サーバが用意されていること(設定の保存、アップグレード用)
- Internet 経由で RMC と RMS を接続する場合は、RMC-RMS 間通信における認証／暗号化の機能を利用すること。

RMCを監視対象装置のコンソールポートとイーサネットに接続

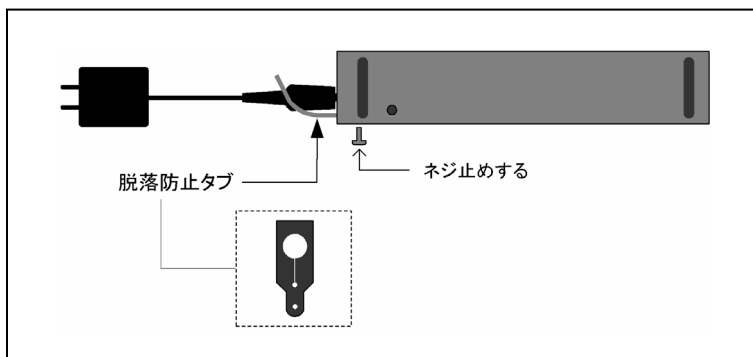


シリアルケーブルの接続は、必ず RMC および接続する機器の電源を切って行ってください。

電源ケーブルの脱落防止

ACアダプタの抜けを防止するため、RMCには脱落防止タブが添付されています。予め期せぬ電源断を防止したい場合は、以下の手順でタブを取り付けてください。

- ① ACアダプタのプラグ部分にタブを通す。
- ② ACアダプタをアダプタジャックに接続する。
- ③ 添付のネジでタブをRMC本体に止め付ける。



■ シリアル端末／モデムとの接続

COM2ポートにシリアル端末あるいはモデムを接続すると、イーサネットポートに接続されたネットワークに障害が発生した場合も、COM2ポートを経由したRMCへのアクセス、あるいはメールの送信が可能になります。(シリアル端末／モデム接続時の機能と設定を参照して下さい。)

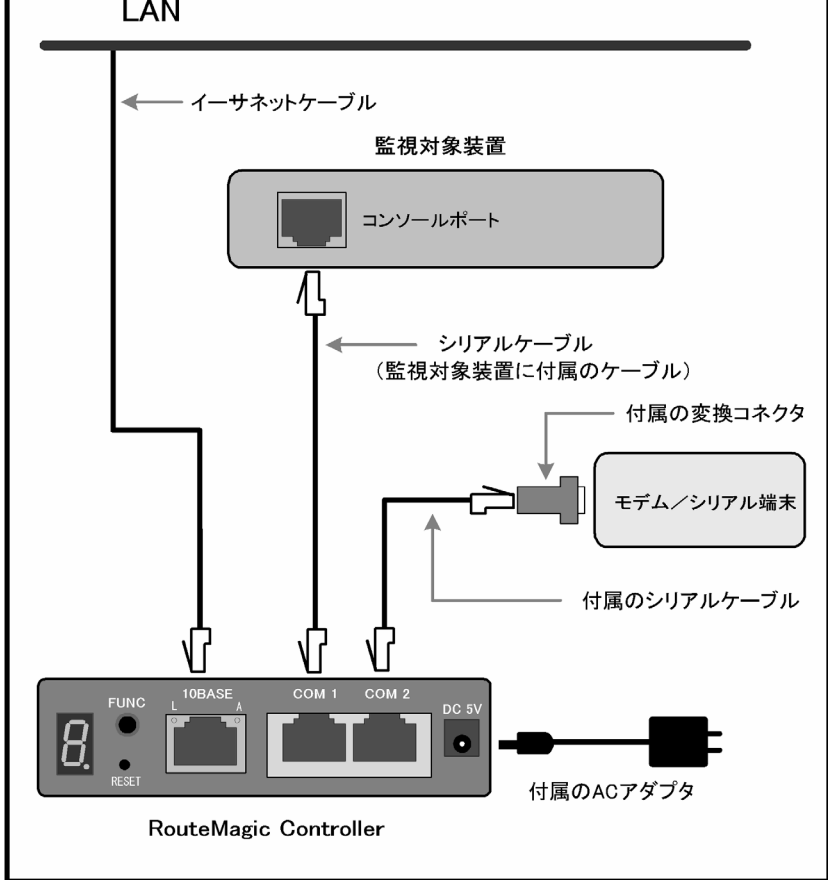
必要なケーブルおよびコネクタ

- 付属のシリアルケーブル 1本
- 付属の変換コネクタ 1個 (RJ45-DB9変換コネクタ)

モデムを接続される場合はプラグ変換コネクタ(オス形状)、シリアル端末(PC)を接続される場合はソケット変換コネクタ(メス形状)をご使用ください。

(注) RMCはDTE動作です。シリアル端末／モデムのコネクタ形状によって、市販の変換コネクタが必要になる場合があります。付属のケーブルおよび変換コネクタの仕様については、巻末の製品仕様をご参照ください。

COM2ポートにシリアル端末またはモデムを接続



シリアルケーブルの接続は、必ず RMC および接続する機器の電源を切ってください。

RMC の起動

■ 電源の投入

監視対象装置との接続が完了したら、AC アダプタの電源プラグを電源コンセントに差し込んでください。RMCには電源スイッチはありません。



RMC の電源を入れて電気的な異常が生じた場合は、速やかに AC アダプタを電源コンセントから外してください。

■ LED 表示の確認

電源投入後、RMC は IP アドレスの取得動作に入ります。この間、LINK LED と ACT LED、ステータス LED は次のように変化します。

ステータス LED 表示
全点灯
内部動作ステータス表示
RMC ソフトウェアバージョン表示
回転表示
IP アドレス表示

IP アドレスの表示 :

IP アドレスが取得された場合、ステータス LED には IP アドレスが表示されます。
(次ページの図参照)

IP アドレス未設定時 :

IP アドレスが取得できなかった場合、ステータス LED には **— no IP AddrESS —** が表示されます。IP アドレスの自動設定機能(「ファンクションスイッチの機能」参照)を実行するか、COM2 ポートに接続したシリアル端末からログインして、IP アドレスの設定を行ってください。

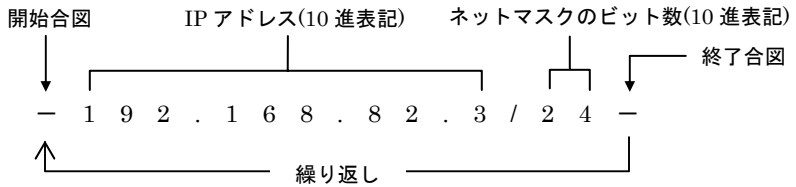
(注 1) ステータス LED が回転表示の間は、電源を落とさないで下さい。

(注 2) 電源投入後、3 分近く経過してもステータス LED が IP アドレス表示もしくは **— no IP AddrESS —** 表示にならない場合は、一旦 AC アダプタを電源コンセントから抜き、再度電源を投入してください。

IP アドレス表示

取得された IP アドレスは下図のように、IP アドレス、“/”、ネットマスクのビット数の順で 1 文字ずつステータス LED に表示されます。各文字は 1 秒間ずつ表示され、終了文字 “-” 表示後、再び先頭からの表示が繰り返されます。

例えば “192.168.82.3 / 255.255.255.0 ” は次のように表示されます。



RMC の初期設定

RMC の起動が完了したら、RMC にログインして RMC 自身と監視対象装置に接続されるシリアルポートの設定を行ってください。

■ ログインの方法

ログインには LAN 上のホストからネットワークを介して行う方法と、COM2 に接続したシリアル端末から行う方法があります。

LAN 上のホストからネットワークを介してログインする場合

RMC 起動時に IP アドレスが設定された場合には、ステータス LED に表示されている IP アドレスに ssh (または telnet) で接続してください。

IP アドレスが設定されていない場合、IP アドレス自動設定機能(「ファンクションスイッチの機能」を参照)を実行することで、一時的に IP アドレスを設定することが可能です。また、RMC にシリアル端末が接続されている場合は、下記のローカル端末からのログインによる初期設定も可能です。

COM2 に接続したシリアル端末からログインする場合

IP アドレスが設定されなかった場合は、まず、COM2 ポートに接続されたシリアル端末からログインしてください。この時、シリアル端末の端末パラメータを予め下記の COM2 ポートのデフォルト値に合わせて設定しておく必要があります。

パラメータ	デフォルト値
データ転送速度	9600 bps
キャラクタビット長	8 bits
パリティチェック	無し
ストップビット長	1 bit
フロー制御方式	none

ユーザ名とパスワード

いずれの場合も、ログインプロンプトもしくはログイン画面に対して下記のユーザ名とデフォルト・パスワードを入力して RMC にログインします。

ユーザ名	rmc
パスワード	無し

ログインが完了すると下記のプロンプト “ユーザ名@ホスト名>” が表示され、コマンドを受け付けられる状態になります。

```
rmc@myrmc>
```

以後のパラメータ設定は、“特権モード” に移行して行います。RMC の設定や状態を変更するコマンドは、すべて特権モードでのみ実行できます。ログイン直後、RMC は通常モードになっています。enable コマンドを実行して特権モードに移行してから設定操作を行ってください。

特権モードへの移行にはパスワードが必要ですが、工場出荷状態ではパスワードは設定されていません。

- (注 1) 設定された内容はメモリ内に記憶されます。設定した情報をリブート後も有効にするためには write memory コマンドを実行し、メモリ内の設定情報を設定ファイルに書き込んでください。
- (注 2) 各コマンドの機能および設定情報のデフォルト値に関しては、クイックリファレンスをご参照ください。

■ IP アドレスの設定 (DHCP サーバが用意されていない場合)

RMC は DHCP サーバから IP アドレスを自動的に取得しますが、IP アドレスが取得されなかった場合や任意のアドレスに設定変更したい場合は、set address コマンドによって IP アドレスの設定を行ってください。

設定すべき情報は、IP アドレス、ネットマスク、デフォルトゲートウェイ、ブロードキャストアドレス、およびネームサーバ (DNS) です。(デフォルトゲートウェイの設定は省略可能)

以下に、ETH0 イーサネットポートにアドレスを設定する例を示します。

```
rmc@myrmc > enable          ← 特権モードへの移行要求
password:                   ← 特権モード・パスワード入力
[rmc@myrmc]# set port eth0   ← カレントポートを eth0 に指定
[rmc@myrmc(eth0)]# set name-servers xx.xx.xx.xx yy.yy.yy.yy
                               ←ネームサーバ(DNS)の設定
[rmc@myrmc(eth0)]# set broadcast-address xx.xx.xx.xx
                               ←ブロードキャストアドレスの設定
[rmc@myrmc(eth0)]# set address xx.xx.xx.xx yy.yy.yy.yy zz.zz.zz.zz
                               ← IP アドレス、ネットマスク、
                               デフォルトゲートウェイの設定
[rmc@myrmc(eth0)]# show port eth0 ← ポート eth0 の設定を確認
[rmc@myrmc(eth0)]# write memory ← 設定情報を設定ファイルに保存
[rmc@myrmc(eth0)]# disable   ← 通常モードに戻る
rmc@myrmc > quit            ← ログアウトする
```

(注1) リブート後も設定したアドレスを有効にするためには write memory により設定情報を設定ファイルに保存する必要があります。以後の設定も同様です。

(注2) ネットワーク経由でログインして上記の操作を行う場合、set address コマンド実行時点でいったん接続が切れてしまいます。

設定した IP アドレスに ssh (または telnet) で接続して再度ログインし、以降のコマンドを実行してください。リブートの必要はありません。

■ パスワードの設定

RMC にログインして設定などの操作をするためには、ログイン、特権モードのそれぞれにパスワードが必要です。なお、ログインパスワードはユーザごとに設定されますが、特権モードパスワードは全ユーザに共通となります。

(注) 工場出荷時にはパスワードが設定されていません。必ず、次の操作を行って任意のパスワードを設定してください。

RMC ログインパスワード

RMC にログインするためのパスワードです。パスワードの設定／変更はユーザごとに `set password` コマンドによって行います。

```
rmc@myrmc > enable          ← 特権モードへの移行要求
password:                   ← 特権モード・パスワード入力
[rmc@myrmc]# set password   ← パスワード設定コマンド実行
Enter new password:         ← 新しいログインパスワード入力
Re-enter new password:      ← 同一パスワードの再入力
Password changed
[rmc@myrmc]# disable        ← 通常モードに戻る
rmc@myrmc >
```

特権モードパスワード

特権モードで RMC を利用するための全ユーザ共通のパスワードです。パスワードの設定／変更は `set enable-password` コマンドによって行います。特権モードに対するパスワードの設定を行う場合は、旧パスワードの入力が必要とされます。

```
rmc@myrmc > enable          ← 特権モードへの移行要求
password:                   ← 特権モードパスワード入力
[rmc@myrmc]# set enable-password ← 特権パスワード設定コマンド発行
current password:           ← 現在の特権モードパスワード入力
new password:               ← 新しい特権モードパスワード入力
retype new password:        ← 同一パスワードの再入力
password changed
[rmc@myrmc]# disable        ← 通常モードに戻る
rmc@myrmc >
```


■ ユーザ名の追加とホスト名の変更

工場出荷時には、ユーザ名=rmc、ホスト名=myrmc がデフォルト値として設定されています。ユーザ名は set user-name コマンドで追加することができます。また、ホスト名は set hostname コマンドで変更できます。

以下に、ユーザ名"operator"(パスワードは"xxxxx")を追加し、ホスト名を"rmc1"に変更する場合の例を示します。

```
rmc@myrmc > enable
password:
[rmc@myrmc]# set user-name operator xxxxx ← ユーザ"operator"を追加
[rmc@myrmc]# set hostname rmc1          ← ホスト名を"rmc1"に設定
[rmc@rmc1]# show user-names             ← 登録ユーザー名を確認
[rmc@rmc1]# disable
rmc@rmc1 >
```

■ 日付と時刻の設定

RMC は NTP サーバを利用してシステムクロックを自動的に設定することができます。NTP サーバが利用できない場合は、以下の手順でシステムクロックの設定を行ってください。

システムクロックの確認

RMC にログインし、show date コマンドを実行して、システムクロックの値を確認します。

```
rmc@myrmc > show date
Tue Jan 01 14:15:25 JST 2002      ← 現在のシステムクロックを表示
rmc@myrmc >
```

日時が正しく表示されなかった場合は、set ntp-server コマンドによる NTP サーバの設定もしくは set date コマンドにより、日付と時刻およびタイムゾーン (JST 以外の場合) の設定を行う必要があります。

タイムゾーンの設定

日本標準時 (JST) 以外の地域で RMC を利用される場合は、set timezone コマンドによ

リタイムゾーンの設定を行ってください。

タイムゾーンは `set timezone` コマンドの引数として指定します。設定可能な引数は、以下のとおりです。

CST6CDT	(米国中部標準時)	PST8PDT	(米国太平洋標準時)
EST5EDT	(米国東部標準時)	UCT	(Universal Coordinated Time)
JST	(日本標準時)	GMT	(グリニッジ標準時)
KST	(韓国標準時)	GMT±N	
MST7MDT	(米国山地標準時)		

```
rmc@myrmc > enable
password:
[rmc@myrmc]# set timezone PST8PDT          ← タイムゾーンを設定
Thu Jul  4 22:18:37 PDT 2002              ← 設定後の時刻を表示
[rmc@myrmc]# disable
rmc@myrmc >
```

NTP サーバの設定

NTP サーバが利用可能な場合は、利用すべき NTP サーバ名を指定します。

```
rmc@myrmc > enable
password:
[rmc@myrmc]# set ntp-server ntp.xxx.co.jp  ← NTP サーバ名を設定
[rmc@myrmc]# disable
rmc@myrmc >
```

日付と時刻の設定

NTP サーバが利用できない場合は、日付と時刻の設定を行ってください。以下に 2002 年 4 月 1 日午前 10 時 30 分を設定する場合の例を示します。

```
rmc@myrmc > enable
password:
[rmc@myrmc]# set date 040110302002       ← 日付と時刻の設定
[rmc@myrmc]# disable
rmc@myrmc >
```

■ COM1/COM2 ポートの設定

RMC に対する設定が完了したら、監視対象装置のコンソールポートに接続される

COM1 ポートのパラメータを設定してください。COM2 ポートにも監視対象装置を接続する場合は、COM2 ポートにも同様の設定を行う必要があります。

COM1/COM2 ポートのデフォルト設定は、以下の通りです。接続した監視対象装置のシリアルコンソールポートの設定が以下の値と異なっている場合は、必要なコマンドを実行して COM ポートの設定を変更してください。

パラメータ	デフォルト値
データ転送速度	9600 bps
キャラクタビット長	8 bits
パリティチェック	無し
ストップビット長	1 bit
フロー制御方式	none

(注) シリアル端末、モデムを接続していた COM2 ポートに監視対象装置を接続する場合は、必ず、set no exec または set no modem コマンドを実行して端末/モデムの接続状態を解除してください。

以下にデフォルト値を例にとり、COM1 ポートのパラメータを設定する方法を示します。設定可能な値は、クイックリファレンスを参照してください。

```
rmc@myrmc > enable
password:
[rmc@myrmc]# set port com1           ← カレントポートを COM1 に指定
[rmc@myrmc(com1)]# set speed 9600    ← 通信速度の設定
[rmc@myrmc(com1)]# set csize 8       ← 1文字のビット数の設定
[rmc@myrmc(com1)]# set parity none   ← パリティの設定
[rmc@myrmc(com1)]# set stopbits 1    ← ストップビット長の設定
[rmc@myrmc(com1)]# set flowcontrol none ← フロー制御方式の設定
[rmc@myrmc(com1)]# show port com1    ← COM1 の設定を確認
[rmc@myrmc(com1)]# disable
rmc@myrmc >
```

ローカルコンソール／モデム接続の機能と設定

RMC の COM2 ポートは、シリアル端末もしくはモデムの接続により、ローカルコンソールとしての機能やネットワーク経由の通信に問題が発生した場合のアクセス手段を提供することができます。

■ ローカルコンソールとしての利用

COM2 ポートにシリアル端末を接続した場合、この端末は RMC のローカルコンソールとして機能します。

COM2 ポートの設定

工場出荷時、RMC の COM2 ポートはローカルコンソール接続の状態となっており、端末パラメータは下記のように設定されています。

モデム、もしくは監視対象装置の接続されていた COM2 を再度ローカルコンソール接続の状態に戻す場合には、`set exec` コマンドを実行します。この場合も、データ転送速度を除く端末パラメータは以下の値に再設定されます。

パラメータ	デフォルト値
データ転送速度	9600 bps
キャラクタビット長	8 bits
パリティチェック	無し
ストップビット長	1 bit
フロー制御方式	none

端末パラメータは、データ転送速度のみが任意に設定可能です。データ転送速度の設定は、`set speed` コマンドを実行して行います。

```
myrmc@myrmc > enable
password:
myrmc@myrmc[# set port com2           ← カレントポートを COM2 に指定
myrmc@myrmc(com2)[# set speed 38400   ← 通信速度を 38400bps に設定
myrmc@myrmc(com2)[# show port com2    ← COM2 の設定を確認
myrmc@myrmc(com2)[# disable
myrmc@myrmc >
```

■ モデム接続時の機能と設定

COM2 ポートにモデムを接続した場合、このポートはネットワークに異常が発生してイーサネットポートからのメール送信ができなくなった時のアクセス手段として使用されます。COM2 ポートにモデム接続の設定がなされていると、イーサネットポートからのメール送信ができなかった場合、RMC は自動的に PPP 接続を実行してモデム経由でメールを送信します。また、無手順接続や PPP 接続で遠隔地から RMC にログインして機器操作を行うことも可能になります。

COM2 ポートの設定

モデム接続機能を利用される場合は、COM 2 ポートに対する端末パラメータの設定、および set modem コマンドの実行が必要です。set modem コマンドは、モデムの種類を指定すると同時に、COM 2 にモデムが接続されていることを RMC に通知します。

(注) RMC で使用可能なモデム名、動作確認済みのモデム等の詳細情報に関しては、「RMC リリースノート」でご案内しています。

COM 2 ポートのデフォルト設定は以下の値となっており、データ転送速度のみが任意に設定可能です。

パラメータ	デフォルト値
データ転送速度	38400 bps
キャラクタビット長	8 bits
パリティチェック	無し
ストップビット長	1 bit
フロー制御方式	hardware

通信速度を 115200bps に変更した後、モデム接続の通知を行う場合の例を以下に示します。

```
rmc@myrmc > enable
password:
[rmc@myrmc]# set port com2           ← カレントポートを COM2 に指定
[rmc@myrmc(com2)]# set speed 115200 ← 通信速度を 115200bps に設定
[rmc@myrmc(com2)]# set modem generic ← モデム名指定とモデム接続の通知
[rmc@myrmc(com2)]# show port comb   ← COM2 の設定を確認
[rmc@myrmc(com2)]# disable
rmc@myrmc >
```

PPP 接続の設定

COM 2 ポートに対する設定を行った後、RMC が PPP 接続するアクセスポイントの指定を行います。設定に必要な情報は、ユーザ名、パスワード、およびアクセスポイントの電話番号です。以下に、ユーザ名：rmcuser、パスワード：routrek、電話番号：111-222-3456 として設定する場合の例を示します。

```
rmc@myrmc > enable
password:
[rmc@myrmc]# set port com2           ← カレントポートを COM2 に指定
[rmc@myrmc(com2)]# set ppp-username rmcuser routrek 1112223456
                                           ← PPP 接続情報を設定
[rmc@myrmc(com2)]# show port com2      ← PPP の設定内容を表示
[rmc@myrmc(com2)]# disable
rmc@myrmc >
```

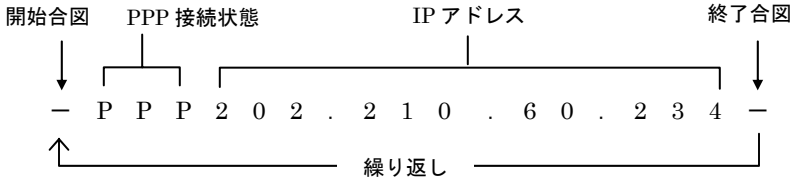
RMC に対して PPP 接続を行う(RMC 側を PPP サーバにする)場合には、PPP 接続時の RMC の PPP アドレスと、接続先の PPP アドレスを指定する必要があります。以下に、RMC の PPP アドレス:192.168.0.1、接続先の PPP アドレス:192.168.0.2 として設定する場合の例を示します。

```
rmc@myrmc> enable
password:
[rmc@myrmc]# set port com2           ← カレントポートを COM2 に指定
[rmc@myrmc(com2)]# set ppp-server 192.168.0.1 192.168.0.2
                                           ← PPP 接続情報を設定
[rmc@myrmc(com2)]# disable
rmc@myrmc>
```

(注) RMC に対して PPP 接続を行う場合、PPP 接続の際の ID・パスワードは、RMC のログインユーザー名・パスワードを指定してください。

PPP 接続時のステータス LED 表示

PPP 接続時は、ステータス LED に PPP ポートの IP アドレスが表示されます。



(注) 上記の表示は、RMC が PPP 接続を行った場合に表示されます。RMC に対して PPP 接続が行われた場合は LED の表示に変更はありません。

ローカルコンソール接続に戻したい場合

set modem が実行されると、RMC は COM2 にモデムが接続されていると認識するため、ローカルコンソールとしての接続ができなくなります。ローカルコンソールとして使用する場合は、ネットワーク経由で RMC にログインし、set exec コマンドを実行してください。

```
rmc@myrmc > enable
password :
[rmc@myrmc]# set port com2      ← カレントポートを COM2 に指定
[rmc@myrmc(com2)]# set exec      ← ローカルコンソール接続の指定
[rmc@myrmc(com2)]# disable
rmc@mvrmc >
```

(注) COM2 ポート経由でリモートサイトからログインして set exec コマンドを実行した場合、コマンド実行直後に RMC との接続は切断されます。

■ PPP 接続のテスト

PPP 接続の設定を確認するため、手動で PPP 接続を開始することができます。
以下に PPP 接続を開始し、traceroute コマンドで経路設定の確認と PPP 関連ログの表示後、PPP 接続を終了する場合の例を示します。

```
rmc@myrmc > enable
password:
[rmc@myrmc]# ppp-on                               ← PPP 接続の開始
[rmc@myrmc]# traceroute www.routrek.co.jp ← 経路設定の確認
[rmc@myrmc]# show port com2                       ← PPP 接続ステータスを表示
[rmc@myrmc]# show log ppp 20                     ← PPP 関連のログを 20 行表示
[rmc@myrmc]# ppp-off                              ← PPP 接続の終了
[rmc@myrmc]# disable
rmc@myrmc >
```

(注) 2 分間通信が無い場合、PPP 接続は自動的に終了します。

電子メールサービスの設定

監視対象装置から出力されたコンソールメッセージを電子メールで送信するには、メールポートの設定を行います。メールポートは0 (ml0) から7 (ml7) まで用意されており、それぞれに宛先やフィルタ規則を設定して、必要に応じた送信先や送信内容を指定することができます。

(注1) メールポート0 (ml0) は、RMS (RouteMagic Server) との通信用にリザーブされています。RMS をご使用の場合、ユーザの任意な利用はできませんのでご注意ください。

(注2) 電子メールサービスは、デフォルトでは停止されています。set mail-service コマンドを実行することで、電子メールサービスが有効になります。

■ 電子メールサービスの設定とサービスの開始

メールポートは、指定のポートから入力されたメッセージを一定の行数または文字数(メールポートバッファ長)ごとに電子メール(メールサブジェクト: "Target message") で指定の宛先に送信します。また、一定時間内に所定の文字数が受信されなかった場合は、それまでに受信した文字列を1つのメールメッセージとして送信します。バッファ長およびタイマ値のデフォルト設定は下記の通りです。

パラメータ	デフォルト値
メールポートのバッファ長	64000 文字、10000 行
送信タイマ値	10 秒

(注1) メールポートのバッファ長の設定を極端に小さくすると、多量のメールが送信される恐れがありますのでご注意ください。

(注2) RMS をご使用の場合、メールポート0 (ml0) のバッファ長はデフォルトの設定でご利用ください。

以下にメールポート1 (ml1) の入力先として COM1 ポート (com1) を、メールの宛先として someone@routrek.co.jp を指定し、1 メールメッセージの最大文字数、最大行数と送信タイマ値を各々20000文字、300行、60秒に設定する場合の例を示します。

```

rnc@myrnc > enable
password:
[rnc@myrnc]# set port ml1                ← カレントメールポートを指定
[rnc@myrnc(ml1)]# set mailto someone@ routrek.co.jp
                                           ← メールアドレスを設定
[rnc@myrnc(ml1)]# set errors-to mail-admin@routrek.co.jp
                                           ← エラーメールの宛先を設定
[rnc@myrnc(ml1)]# set max-nmr-of-chars 20000 ← メールの最大文字数を設定
[rnc@myrnc(ml1)]# set max-nmr-of-lines 300 ← メールの最大行数を設定
[rnc@myrnc(ml1)]# set inactivity-timer 60 ← 送信タイマ値を設定
[rnc@myrnc(ml1)]# show port com1         ← メールポート 1 の設定を確認
[rnc@myrnc(ml1)]# set spy com1 ml1      ← COM1 をメールポート 1 に接続
[rnc@myrnc(ml1)]# show spy              ← 接続設定の確認
[rnc@myrnc(ml1)]# set mail-service      ← メールサービスの開始
[rnc@myrnc(ml1)]# disable
rnc@myrnc >

```

送信先・入力先が複数の場合

1 つの COM ポートに対して複数の送信先を指定する場合は、複数のメールポートを使用して各々にメールアドレスを設定し、COM ポートと接続します。メールメッセージの最大文字数と送信タイマ値もメールポートごとに設定可能です。同様に、COM1、COM2 両ポートの情報を 1 つのメールポートに送信する場合は、各 COM ポートをメールポート ml N に接続してください。

以下に、COM1 の情報をメールポート 1 および 2 に送信する場合の例を示します。

```

[rnc@myrnc]# set port ml1                ← カレントポートを ml1 に指定
[rnc@myrnc(ml1)]# set mailto someone@ routrek.co.jp
                                           ← メールアドレスを設定
[rnc@myrnc(ml1)]# set errors-to mail-admin@routrek.co.jp
                                           ← エラーメールの宛先を設定
[rnc@myrnc(ml1)]# set port ml2          ← カレントポートを ml2 に変更
[rnc@myrnc(ml2)]# set mailto foo@ routrek.co.jp ← メールアドレスを設定
[rnc@myrnc(ml2)]# set errors-to mail-admin@routrek.co.jp
                                           ← エラーメールの宛先を設定
[rnc@myrnc(ml2)]# show port ml1 ml2    ← メールポート 1,2 の設定を確認
[rnc@myrnc(ml2)]# set spy com1 ml1     ← COM1 をメールポート 1 に接続
[rnc@myrnc(ml2)]# set spy com1 ml2     ← COM1 をメールポート 2 に接続
[rnc@myrnc(ml2)]# show spy             ← 接続設定を確認
[rnc@myrnc(ml2)]# set mail-service     ← メールサービスの開始

```

■ 電子メールの送信テスト

メールの宛先の設定が正しく行なわれたかどうかを実際にテストメールを送信して確認することができます。以下にメールポート ml1 にテストメールを送信する例を示します。

```
rmc@myrmc > enable
password:
[rmc@myrmc]# mail-test ml1          ← メールポート ml1 にテストメールを送信
[rmc@myrmc]# show log mail 20      ← メール送信ログを 20 行表示
[rmc@myrmc]# disable
rmc@myrmc >
```

メールポート ml1 に指定された宛先には、以下の内容のメールが送信されます。

```
From: rmc@[RMC の IP アドレス]
Subject : ml1(0001) : RMC message
This is a test mal from RMC port ml1.
```

テストメールが届かない場合、show running-config コマンドで RMC の設定を確認するとともに、show log mail, show log rmc コマンドでメール送受信ログやシステムログの内容を調べてください。

また、設定にエラーがある場合、RMC にエラーメールが返信されている場合があります。RMC が受信したメールの内容は、show mail コマンドの実行により確認できます。

(注1) mail-test コマンドは、メールサービスが停止されている場合でも有効です。

(注2) PPP 接続によるメール送信テストを行う場合は、ppp-on コマンドを実行してからテストメールを送信して下さい。

■ 電子メールの受信テスト

RMS(RouteMagic Server)から RMC に送信されたメールが正しく受信できたかどうかは、show mail コマンドを実行して確認することができます。このコマンドは、RMC が最後に受け取ったメールを表示します。

RMC の機能とフィルタ・スクリプト

RMC は、基本となるメール発信機能に加えて、監視対象装置から必要なメッセージのみを抽出する機能や装置からの自動的情報取得の機能を提供します。これらの機能は、フィルタとスクリプトを利用して実装され、監視対象装置の種別ごとに動作を定義することができます。

監視対象装置が Cisco 社製品（ルータ、スイッチ、IOS スイッチ）の場合、デフォルトの設定値が事前に定義されているため、各機能を利用する際にフィルタやスクリプトを定義する必要はありません。それ以外の機種を監視対象とされる場合は、あらかじめ装置の動作仕様に従って、「装置の種別」、「フィルタ」および「スクリプト」を定義してください。

旧リリースをご利用の方へ

RMC V2.1 のフィルタ (tf10-tf17) とスクリプトは、装置種別 (target_type) ごとに設定する形式に変更されています。従来の形式のフィルタ (f10-f17) およびスクリプトもご利用になれますが、設定の詳細に関しては、RMC V2.0 のマニュアルをご参照ください。

■ フィルタとスクリプトの機能

装置種別の定義

フィルタとスクリプトは、「装置種別」ごとに設定します。Cisco 社製品に対しては、デフォルトの装置種別 (target-type) "cisco" があらかじめ設定されていますが、新たな装置種別を定義して、装置の使用に合わせたフィルタ・スクリプトを設定することも可能です。

装置種別の定義は、set user-target-type コマンドによって行います。種別を定義した後、利用する機能に応じて必要なフィルタとスクリプトの設定を行ってください。

フィルタの機能

初期設定状態では、メールポートは指定された COM ポートからのすべての入力を指定のアドレスに電子メールで転送します。フィルタを利用することにより、特定の文字列（キーワード）を含むメッセージのみを指定アドレスに送信することができます。

フィルタは、監視対象装置の種別ごとに 0 (tf10) から 7 (tf17) までが定義できます。装置種別 "cisco" のフィルタ 0 から 3 (tf10-tf13) には、Cisco 社ルータ、スイッチを監視対象装置とする場合のデフォルト値が設定されています。

ユーザ定義のフィルタを設定する場合は、set target-filter コマンドを実行し、UNIX の awk プログラム形式で記述することによって行います。

スクリプトの機能

スクリプトの利用により、RMC から監視対象装置のコンソールポートを介してコマンドの発行等を実行し、自動的に装置からの情報収集を行うことが可能になります。スクリプトには以下の種類があり、装置に固有の動作仕様を定義することができます。

フィルタと同様に、Cisco 製品に対しては各スクリプトに対するデフォルト値があらかじめ設定されています。Cisco 製品以外の装置を監視対象としてこれらの機能を利用される場合は、各装置の仕様と必要な情報に応じてスクリプトを定義してください。

スクリプトの種類	RMC の提供する機能
network-info	監視対象装置とネットワーク関連情報の自動送信
target-check	監視対象装置の生存確認
command	RMS から監視対象装置へのコマンド発行要求メールの処理
login	装置へのログイン時に必要な動作の設定 (他のスクリプト実行時に利用される)

(注) 上記スクリプトの実行結果として監視対象装置から入力された情報は、comN ポートおよび target N ポートに出力されます。

■ 装置種別の定義

新たに、"cisco"以外の装置種別をユーザ定義する場合は、set target-script コマンドを実行して設定します。装置種別の名称は任意に設定し、この装置種別に対応したフィルタやスクリプトを利用する際に指定します。

```
rmc@myrmc > enable
password:
[rmc@myrmc]# set user-target-type mytarget
← ユーザ定義の装置種別"mytarget"を設定
[rmc@myrmc(com1)]# disable
rmc@myrmc >
```

■ フィルタの設定

監視対象装置からの出力情報を制御するためのフィルタは、装置の種別ごとに 0 (tfl0) から 7 (tfl7) までが定義可能です。各装置のコンソールポートから出力されるメッセージの形式にしたがって設定を行ってください。Cisco 社のルータ・スイッチを監視対象とする場合は、後述のデフォルトフィルタを利用することができます。

フィルタの設定は、set target-filter コマンドを実行し、UNIX の awk プログラム形式で記述することによって行います。監視対象装置 (COM ポート) に対して使用されるフィルタとメールポートの関連は、set spy コマンドによって設定します。

フィルタの設定例

フィルタ記述	機能
/link down/	"link down" という文字列を含む行を送信
\$0 !~ /link up/	"link up" という文字列を含まない行を送信
/[A-Za-z]+[0-3]/	アルファベットで構成される単語に続いて 0 から 3 の 1 桁の数字を含む行を送信
/error/ /warning/	"error" または "warnig" 文字列を含む行を送信
/Error/ { if (\$0 !~ /password/){ print } }	"Error" の文字列を含み、かつ "password" を含まない行を送信

以下に、COM1 に接続された装置の種別を "cisco" としてフィルタ tfl4 を定義し、メールポート 1(ml1) に設定された送付先への送信時に利用する場合の設定例を示します。

```
rmc@myrmc > enable
password:
[rmc@myrmc]# set target-filter cisco tfl4 ← cisco 用フィルタとして tfl4 を定義
[rmc@myrmc]# set port com1 ← カレントポートを com1 に指定
[rmc@myrmc(com1)]# set target-type cisco ← com1 ポートの装置種別を cisco に設定
[rmc@myrmc(com1)]# set port ml1 ← カレントポートを ml1 に指定
[rmc@myrmc(ml1)]# set mailto foo@ routrek.co.jp ← ml1 のメールアドレスを設定
[rmc@myrmc(ml1)]# set spy com1 tfl4 ml1 ← com1 に接続されるメールポートとフィルタを指定
[rmc@myrmc(ml1)]# set mail-service ← メールサービスの開始
[rmc@myrmc(ml1)]# disable
rmc@myrmc >
```

■ デフォルトフィルタの利用（重要度別のメール送信）

監視対象装置が Cisco 社ルータ、スイッチの場合、RMC が提供するデフォルトフィルタを利用することができます。デフォルトフィルタは、装置種別 (target-type) "cisco" のフィルタ 0 から 3 (tfl0-tfl3) を使用して提供されます。

デフォルトフィルタは、監視対象装置からエラーメッセージを抽出し、重要度（エラーメッセージ内の Severity Levels）により分類する機能を提供します。この利用により、重要度レベルに応じたメール送付先の指定が可能になります。

各デフォルトフィルタと対応する Severity Levels は次の通りです。

デフォルトフィルタ	エラーメッセージ内の Severity Levels	
tfl0 (重要度: 全て)	0-7 All	全てのエラーメッセージを通知
tfl1 (重要度: High 0-2)	0-emergency	システム使用不可状態の通知
	1-alert	直ちに対処が必要
	2-critical	重大な問題の発生を通知
tfl2 (重要度: Middle 3-5)	3-error	エラー状態通知
	4-warning	警告状態通知
	5-notification	正常だが重要な状態通知
tfl3 (重要度: Low 6-7)	6-informational	情報通知メッセージ
	7-debugging	デバ깅時のみ発生

(注) フィルタ 0 には Cisco 社製品を接続して RMS を利用する場合の規定値が設定されています。RMS を利用する場合は、デフォルト値のままご使用ください。

以下に、デフォルトフィルタを利用して、重要度が High のメッセージをメールポート 1 から high@routrtek.co.jp 宛てに送信する場合の例を示します。

```

rmc@myrmc > enable
password:
[rmc@myrmc]# set port com1          ← カレントポートを com1 に指定
[rmc@myrmc(com1)]# set target-type cisco ← com1 ポートの装置種別を cisco に設定
[rmc@myrmc(com1)]# set port ml1      ← カレントポートを ml1 に指定
[rmc@myrmc(ml1)]# set mailto high@ routrek.co.jp ← ml1 のメールアドレスを設定
[rmc@myrmc(ml1)]# set spy com1 tfl1 ml1 ← com1 に接続されるメールポートとフィルタ (tfl1)を指定
[rmc@myrmc(ml1)]# set mail-service   ← メールサービスの開始
[rmc@myrmc(ml1)]# disable
rmc@myrmc >

```

■ フィルタの設定確認テスト

filter-test コマンドを使用することにより、ユーザ定義のフィルタ設定が正しく行なわれたかどうかをあらかじめ確認することができます。以下にフィルタ tfl1 の設定を確認する場合の操作を示します。

```
rmc@myrmc > enable
password:
[rmc@myrmc]# filter-test cisco tfl1          ← フィルタ tfl1 のテストを開始
XXXXXXXXXXXXXXXXXXXXX                       ← テスト文字列(XX...X)入力後
                                              ← Enter キーを押す
>XXXXXXXXXXXXXXXXXXXXX                     ← 入力文字列がフィルタ設定に一致した場合は、
                                              ← 入力文字列が表示される

                                              ← 入力文字列がフィルタ設定に一致しない場合
                                              ← フィルタ後の文字列は表示されない
                                              ← Ctrl-D を押してコマンド終了

[rmc@myrmc]# disable
rmc@myrmc >
```

Cisco 製品用に定義されたフィルタ tfl1（重要度 0 から 2 のメッセージを抽出）を指定した場合の表示は、次のようになります。

- ① **重要度 1**に相当するメッセージをテスト文字列として入力した場合
Feb 9 18:18:22.676: %PIM-1-INVALID_RP_JOIN: ← 入力文字列
>Feb 9 18:18:22.676: %PIM-1-INVALID_RP_JOIN: ← 表示
- ② **重要度 5**に相当するメッセージをテスト文字列として入力した場合
Feb 9 18:18:22.676: %AUTORP-5-MAPPING: ← 入力文字列

上記②では、テスト文字列がフィルタに一致しないため、何も表示されません。

■ スクリプトの設定

RMC を Cisco 社製品(ルータ、スイッチ)以外の装置に接続して、装置からの定期的な情報収集などの機能を利用する場合は、装置種別の定義と利用する機能に応じたスクリプトの設定が必要になります。スクリプトには以下の種類があり、装置種別 "cisco" に対応する各スクリプトについては、デフォルトの設定が行われています。

スクリプトの種類	機能
login	装置へのログインに必要な動作を設定します。このスクリプトは単独では実行されず、他のスクリプトから呼び出して使用されます。
network-info	装置に対してコマンドを発行し、定期的に必要な情報を収集する場合に使用します。このスクリプトは、set net-work-info-time コマンドにより "Network information" メールの定期送信を指定した場合に実行されます。
command	RMS から装置へのコマンド発行要求メールを受信した場合に、実行されます。
target-check	監視対象装置の生存確認に必要な動作を設定します。このスクリプトは、set target-check コマンドにより監視対象装置の定期的な生存確認を指定した場合に実行されます。当スクリプトが未定義の場合、装置の生存確認は装置の RS-232C シグナル状態監視によって行われます。

スクリプト記述は、以下のように、set target-script コマンドを実行して設定します。なお、スクリプト記述の詳細については、「RMC 活用ガイド」をご参照ください。

```
rmc@myrmc > enable
password:
[rmc@myrmc]# set user-target-type mytarget
    ← ユーザ定義の装置種別"mytarget"を設定
[rmc@myrmc(com1)]# set target-script mytarget network-info
    ← mytarget のネットワーク情報収集用スクリプト
    "netork-info" を設定
[rmc@myrmc(com1)]# disable
rmc@myrmc >
```

■ RMC の生存確認（キープアライブ）情報の送信

RMC は、RMC 自身の動作状態を通知するため、設定情報の一部やログインユーザの履歴、動作に関する各種ログを、電子メール（メールサブジェクト: "RMC keep-alive"）で送信する機能を備えています。この機能はデフォルトで有効になっており、電子メールサービスを開始すると送信が開始されます。送信時刻のデフォルト値は、各 RMC に固有の値になっていますが、任意の時刻に設定可能です。

以下に、キープアライブ情報を午前 9 時 0 分と午後 5 時 0 分の 1 日 2 回、メールポート 0 で指定された宛先（別途設定が必要です）に送信する例を示します。

```
rmc@myrmc > enable
password:
[rmc@myrmc]# set keep-alive-time 09,17 0 ← キープアライブ送信時刻の指定
[rmc@myrmc]# set spy rmc ml0             ← キープアライブ送信先メールポートの指定
[rmc@myrmc]# set mail-service           ← メールサービスの開始
[rmc@myrmc]# disable
rmc@myrmc >
```

■ 監視対象装置の生存確認

RMCは監視対象装置の生存確認を定期的に行う機能を提供します。生存確認時に監視対象装置が無応答であった場合、RMCはメールポート0 (ml0)に電子メール(メールサブジェクト: "Target not respond")を送信し異常の発生を通知します。このメールは、RMCが最初に装置の無応答を検知した時点で送信され、応答の復旧が確認された時点でメールポート0に復旧通知(メールサブジェクト: "Target responds")が送信されます。

この機能は、デフォルトでは "OFF" に設定されています。生存確認を行う場合は、`set target-check` コマンドを使用して生存確認機能を "ON" に設定してください。

以下に、COM1ポートに接続された装置の生存確認を実行し、状態確認の結果をメールポート0 (ml0)に送信する場合の例を示します。

```
rmc@myrmc > enable
password:
[rmc@myrmc]# set port com1           ← カレントポートを COM1 に設定
[rmc@myrmc(com1)]# set target-check ← 監視対象装置の生存確認を行う
[rmc@myrmc(com1)]# set spy port ml0 ← 生存確認送信先メールポートを設定
[rmc@myrmc(com1)]# show port com1   ← COM1 の設定を確認
[rmc@myrmc(com1)]# disable
rmc@myrmc >
```

装置の生存確認機能はスクリプトを利用して実行されますが、Cisco社製品(target-type "cisco")を監視対象とする場合は、デフォルトのスクリプトがあらかじめ設定されています。"cisco"以外の種別の装置に対して当機能を利用される場合は、target-checkスクリプトに装置状態を確認するための動作を設定してください。

■ 監視対象装置およびネットワーク関連情報の自動送信

RMC は、監視対象装置から定期的に情報を収集し、電子メール(メールサブジェクト: “Network information”) で送信する機能を備えています。

この機能を有効にするには、情報送信時刻、監視対象装置に対するログインパスワード/特権モードパスワードの設定が必要です。以下に、COM1 ポートに接続された Cisco ルータを監視対象として、ログインパスワードを key1、特権モードパスワードを key2 とし、ネットワーク情報を午前 8 時 0 分と午後 6 時 0 分の 1 日 2 回、メールポート 0 で指定された宛先(別途設定が必要です)に送信する例を示します。

```
rmc@myrmc > enable
password:
[rmc@myrmc]# set port com1          ← カレントポートを COM1 に設定
[rmc@myrmc(com1)]# set target-type cisco      ← 監視対象装置の種類を Cisco に設定
[rmc@myrmc(com1)]# set target-login-password key1      ← ルータのログインパスワードを設定
[rmc@myrmc(com1)]# set target-enable-password key2    ← ルータの特権モードパスワードを設定
[rmc@myrmc(com1)]# set network-info-time 08,18 0      ← ネットワーク情報送信時刻の指定
[rmc@myrmc(com1)]# set spy target1 ml0             ← ネットワーク情報送信先メールポートを設定
[rmc@myrmc(com1)]# show port com1                ← COM1 の設定を確認
[rmc@myrmc(com1)]# set mail-service             ← メールサービスの開始
[rmc@myrmc(com1)]# disable
myrmc >
```

Cisco 社製品 (target-type "cisco") を監視対象とする場合は、装置の設定情報およびネットワーク関連情報の取得機能がデフォルトとして定義されています。Cisco 以外の製品を監視対象として当機能を利用する場合は、network-info スクリプトに、必要な情報を収集するための RMC の動作を設定してください。

■ RMC 機能の利用と設定コマンド

装置の生存確認やネットワーク情報の収集などの付加機能を利用する場合に必要な設定と使用するコマンドは、下記のようになります。各コマンドの機能に関しては、クイックリファレンスを参照してください。

すべての装置種別に共通の設定

設定内容	コマンド
監視対象装置から出力されたメッセージのフィルタおよびメール送信先の設定	<code>set spy comN tflN mlN</code>
RMC 生存確認 (keep-alive) のメール送信先の設定	<code>set spy rmc mlN</code>
監視対象装置の生存確認、ネットワーク情報、操作ログのメール送信先の設定	<code>set spy targetN mlN</code>
監視対象装置のログイン名、パスワードの設定	<code>set target-login-name</code> <code>set target-login-password</code> <code>set target-enable-password</code>
監視対象装置の生存確認の設定	<code>set target-check</code>
ネットワーク情報送信時刻の設定	<code>set network-info-time</code>
監視対象装置の操作ログの記録設定	<code>set connect-log</code>

ユーザ定義の装置種別とフィルタ/スクリプト利用の場合の設定

設定内容	コマンド
装置種別のユーザ定義	<code>set user-target-type</code>
ユーザ定義した装置固有のフィルタの設定	<code>set target-filter</code>
ユーザ定義した装置固有の操作スクリプトの設定	<code>set target-script</code>
COM ポートに対してユーザ定義の装置種別を設定 (各 COM ポートのデフォルト設定は、"cisco")	<code>set target-type</code>

以下に、監視対象装置の種別とフィルタ・スクリプトを新たにユーザ定義し、これを利用する場合に必要なとなるコマンドの実行シーケンスを示します。

```
rmc@myrmc > enable
password:
----- 以下の設定は、装置種別ごとに必要です -----
set user-target-type mytarget          ← ユーザ定義の装置種別"mytarget"を設定
set target-filter mytarget tf10       ← mytarget の tf10 フィルタを設定
show target-filter mytarget           ← mytarget のフィルタ内容を表示
set target-script mytarget login      ← mytarget の login 用スクリプトを設定
set target-script mytarget command   ← mytarget のコマンド実行用スクリプトを設定
set target-script mytarget network-info ← mytarget のネットワーク情報収集用
                                        スクリプトを設定
set target-script mytarget target-check ← mytarget の生存確認用スクリプトを設定
show target-script mytarget           ← mytarget のスクリプト内容を表示
-----

----- 以下の設定は、監視対象装置（COM ポート）ごとに必要です -----
set port com1
set target-type mytarget              ← 装置の種別を "mytarget" に設定
set target-login-name xxxxx
set target-login-password xxxxx
set target-check
set network-info-tine xxxxx
set connect-log
} 装置ごとの情報と機能の設定

set spy com1 tf10 ml0                ← COM1 のメッセージをフィルタ tf10 で処理し ml0 に送信
set spy target1 ml0                  ← 生存確認・ネットワーク情報の送信先を設定
-----

set mail-service
disable
myrmc>
```

SNMP エージェントの機能と設定

RMC V2.1 では、新たに SNMP エージェント機能が搭載されています。この機能を利用することにより、RMC 自身を SNMP マネージャから監視することが可能になります。

■ SNMP エージェント機能の設定

SNMP エージェント機能を利用する場合は、SNMP エージェントを起動し、コミュニティ名の設定およびネットワークのアクセス許可の設定を行います。

```
rmc@myrmc > enable
password:
[rmc@myrmc]# set snmp-community xxxxxxxx
                                     ← エージェントの起動、コミュニティ名の設定
[rmc@myrmc]# disable
rmc@myrmc >
```

■ SNMP Trap の設定

SNMP Trap 機能により、トラップ情報の送信を行うことも可能です。送信されるトラップ情報は、"coldStart Trap" 及び "warmStart Trap" です。この機能を有効にした場合、RMC のブート時にトラップ情報が指定のホストに送出されます。

この利用する場合は、トラップ送信先の IP アドレスもしくはホスト名、およびコミュニティ名を設定します。

```
rmc@myrmc > enable
password:
[rmc@myrmc]# set snmp-traps xxx.xxx.xxx.xxx yyyyyyy
                                     ← 送信先ホスト名、コミュニティ名の設定
[rmc@myrmc]# write memory
                                     ← 設定情報をファイルに保存
[rmc@myrmc]# disable
rmc@myrmc >
```

(注 1) 'set snmp-traps'で指定されるコミュニティ名は、'set snmp-community'で指定されるコミュニティ名との関連はありません。

(注 2) "coldStart Trap" を発信させる為に、必ず、write memory を実行して設定情報を設定ファイルに保存してください。

RMS (RouteMagic Server) に対する設定

RMS を利用される場合は、RMC-RMS 間の通信と監視対象装置の動作仕様に合わせた設定が必要になります。

■ メールポート (ml0) と COM1/2 の設定

RMC はメールポート 0 (ml0) を使用して RMS と通信を行います。以下に、監視対象装置が Cisco 社製品の場合の設定例を示します。Cisco 製品以外の装置を監視対象として RMS を利用される場合は、「RMC の機能とフィルタ・スクリプト」および「RMC 活用ガイド」の記述を参照して、必要な追加設定を行ってください。

```
rmc@myrmc > enable
password:
[rmc@myrmc]# set port ml0          ← カレントポートを ml0 に指定
[rmc@myrmc(ml0)]# set mailto RMS@ routrek.co.jp
                                     ← RMS のメールアドレスを設定
[rmc@myrmc(ml0)]# set errors-to RMS_err@routrek.co.jp
                                     ← エラーメール送信先の設定
[rmc@myrmc(ml0)]# set spy com1 tf10 ml0 ← COM1 をメールポート 0 に接続
[rmc@myrmc(ml0)]# set port com1     ← カレントポートを com1 に指定
[rmc@myrmc(com1)]# set target-type cisco ← com1 の装置種別を cisco に指定
[rmc@myrmc(com1)]# set target-login-password passwd1
                                     ← 監視対象装置のパスワード設定
[rmc@myrmc(com1)]# set target-enable-password passwd2
                                     ← 監視対象装置の特権モードパスワード設定
[rmc@myrmc(com1)]# set target-check  ← 監視対象装置の生存確認を行う
[rmc@myrmc(com1)]# set network-info-time h m
                                     ← h 時 m 分にネットワーク情報を送信
[rmc@myrmc(com1)]# set connect-log  ← connect 時のログを記録する
[rmc@myrmc(com1)]# set spy target1 ml0
                                     ← 生存確認・ネットワーク情報の送信先を設定
[rmc@myrmc(com1)]# set spy rmc ml0  ← キーブアライブ情報の送信先を設定
[rmc@myrmc(com1)]# show running-config ← RMC の設定を確認
[rmc@myrmc(com1)]# set mail-service ← メールサービスの開始
[rmc@myrmc(ml0)]# disable
```

(注) COM2 ポートにも監視対象装置を接続する場合は、COM ポートに対する設定 (部分) が COM2 に対しても必要になります。

■ メールの暗号化と認証に関する設定

Internet 経由で RMS と通信する場合は、必ずメールの暗号化と認証の設定を行ってください。暗号化については PGP(GnuPG)を使用する方法と、弊社独自の暗号化方式 (RES: Routrek Encryption Scheme) を使用する方法の 2 種類があります。

(注) 工場出荷時は set mail-certification (受信メールの認証) が指定された状態となっています。暗号化と認証が不要な場合は、set no mail-certification を実行して認証指定を解除してください。

<PGP を使用する場合>

PGP を使用する場合、送信メールの暗号化と受信メールの認証が行われます。設定には、RMS のメールアドレスをキーID とした PGP 公開鍵が必要です。PGP 公開鍵は、RMS の管理者により発行されます。

set public-key	← RMS の PGP 公開鍵を設定
show key-list	← 登録された PGP 公開鍵を確認
set port ml0	
set mail-encryption	← 送信メール内容の暗号化を行う
set mail-certification	← RMS からの受信メールに対する認証を行う

<RES(独自暗号化方式)を使用する場合>

RES を使用する場合、送受信メールの両方が暗号化されます。暗号化に必要な鍵は RMS と RMC がお互いにメールを送受信することで自動的に設定されます。

set port ml0	
set mail-encryption res	← RMS に送信するメールを RES 暗号化する
set mail-certification	← RMS から RES 暗号化メールを受信する

(注) 暗号化に RES を使用する場合、RMS と RMC 間で双方向のメール送受信ができる必要があります。

■ フィルタの設定

監視対象装置が Cisco 製品(ルータ、スイッチ)の場合、メールポート 0 (ml0) には、デフォルトフィルタ 0 (tf10)が設定されている必要があります。RMS との通信を開始する以前に下記のコマンドを実行して工場出荷時の状態に戻して下さい。

```
set spy comN tf10 ml0
```

(注) 監視対象装置が Cisco 製品以外の場合は、装置から出力されるメッセージの形式に合わせたフィルタを設定してください。

■ RMS 用 SSH パスワードの設定

RMS から RMC にコマンドを発行する際、通常はメールが利用されますが、RMS から RMC に直接 SSH ログインが可能な環境の場合は、SSH 経由でのコマンド発行が可能です。

RMC と RMS 間のメール送受信に RES (独自暗号化方式) が使用されている場合、SSH ログイン用パスワードは自動で設定されます。そうでない場合は、RMS と RMC の両方に共通の SSH ログイン用パスワードを設定する必要があります。RMC 側の設定は、以下に例を示すように、ユーザ ID "rms" に対して SSH パスワードを設定します。

```
set user-password rms foo ← ユーザ ID "rms" にパスワード "foo" を設定
```

■ RMS への RMC の登録

RMS は、RMC から送信される "Setup information" メールを受信によって RMC を識別し、RMS 上での登録を可能にします。

"Setup information" メールは、RMC の起動時および設定変更時に自動的に送信されますが、以下のコマンド実行により手動送信することも可能です。

```
mail-test setupinfo ml0
```

監視対象装置の操作

COM ポートに接続された監視対象装置を、RMC にログインしている端末から直接操作する場合は、現在の標準入出力と COM n ポートを connect コマンドにより双方向接続します。このコマンド実行後、RMC は監視対象装置のシリアルコンソールとして操作可能です。

- (注) spy コマンドによりメールポートへの入力に COM n が設定されている場合、connect 実行時も COM n からの入力は、指定のメールアドレスに引き続き送信されます。

```
myrmc > enable
password:
[myrmc] # connect com1
```

← 標準入出力を COM1 に接続

監視対象装置との接続の終了は、エスケープキャラクタに続けて x を 1 文字入力することによって行います。エスケープキャラクタのデフォルト設定は Ctrl-¥

(**Ctrl** キーを押しながら ¥ キーを押す) です。

connect された状態では、特定のエスケープコマンド (下記) 以外のキー入力は、そのまま接続された機器に出力されます。

エスケープキャラクタ (Ctrl-¥) の次の入力文字による動作は次の通りです。

x	disconnect (機器との接続を終了し、RMC シェルに戻る)
b	ブレーク信号を出力する
?	エスケープコマンド入力時の動作を表示
Ctrl-¥	エスケープキャラクタ自身を 1 文字出力
その他の文字	入力された文字をそのまま出力

エスケープキャラクタの設定

エスケープキャラクタは、任意のコントロールキャラクタ、**Ctrl** キーを押しながら入力される 1 文字、またはエスケープ、**Esc** キーにより入力される 1 文字に変更可能です。

エスケープキャラクタの変更は set escape-character コマンドによって行い、引数に CTRL-? または CONTROL-? (? は任意の 1 文字) もしくは ESC を指定します。

設定例

```
set escape-character CTRL-x    エスケープキャラクタを Ctrl-x に設定
set escape-character ESC      エスケープキャラクタを Escape に設定
```

設定の表示と保存

現在有効な設定の表示

show running-config コマンドで、RMC の現在の設定内容を表示します。
また、show port <ポート名> コマンドで、ポートに関する設定とステータスを表示します。

- (注) 設定を保存せずに RMC を再起動した場合、それまでの設定内容が破棄されますのでご注意ください。設定の保存は、下記の write memory コマンドで行います。

保存されている設定の表示

show configuration コマンドで、RMC に保存されている設定内容を表示します。

現在の設定を保存

write memory コマンドで、現在の設定を保存します。
RMC が再起動された場合には、この保存された設定が利用されます。

保存されている設定の初期化

write erase コマンドで、保存されている設定を初期化し、工場出荷状態に戻すことができます。

設定のバックアップとリストア

copy running-config terminal で、すべての設定を表示します。
copy running-config tftp で、すべての設定を tftp サーバに保存できます。
保存した内容を RMC に再設定する場合は、以下のコマンドを実行します。

- コンソール経由：
write-erase および reload 実行後、copy terminal running-config を実行
- tftp 経由：
copy tftp startup-config を実行し、reload

ファンクションスイッチの機能

製品正面の“FUNC”スイッチを押すと LED に“0.”が表示され、機能番号の選択モードになります。スイッチを押すたびにステータス LED の表示がカウントアップされるので、実行したい機能番号が表示された時点でスイッチを1秒以上長押ししてください。表示が点滅した後に機能が実行されます。

なお、10秒以上スイッチを押さなかった場合は機能選択を中断し、通常のIPアドレス表示状態に戻ります。

ステータス LED に表示される機能番号と RMC の動作は、次の通りです。

表示	RMC 動作
0	LED にソフトウェアバージョン、及び日付と時刻を表示する
1	LED に COM1 ポートの制御信号状態を表示する（下図参照）
2	LED に COM2 ポートの制御信号状態を表示する（下図参照）
3	COM2 ポートの設定をデフォルト値に戻し、ローカルコンソールに設定（ログイン中の全ユーザは強制的にログアウトされる）
4	IP アドレスを自動設定する（注）
5-6	shutdown コマンドを実行（システムを停止）
7-8	reload コマンドを実行（シャットダウン後、システムを再起動）
9	write erase, reload コマンドを実行 （設定値を工場出荷時の値に戻して、再起動）
A	write memory, reload コマンドを実行（設定を保存して、再起動）

（注） 本機能実行の際は、あらかじめ RMC をネットワークに接続してください。



（注） ステータス LED は、信号が“オン”の状態でも点灯します。状態表示は4秒間継続した後、COMポートの通信速度を表示します。

ハードウェアリセットと電源のオフ

RMC は下記の動作中を除き、シャットダウン操作を実行せずにハードウェアリセットもしくは電源オフを行っても問題がないように作られています。電源をオフにする際は念のため shutdown コマンドを実行するようにしてください。

なお、RMC の故障の原因となりますので、下記動作実行中は電源のオフを行わないようご注意ください。

- システムのブート時（ステータス LED が回転表示の間）
- 以下のコマンド実行中
 - write memory** 設定情報の保存用コマンド
 - write erase** 設定情報の削除コマンド
 - copy** 設定情報の保存・復帰用コマンド
 - upgrade** RMC ソフトウェアのアップグレードコマンド
- ファンクションスイッチで 機能番号"9"または"A" の実行時

製品に対するお問い合わせ

製品に関するご質問や障害に関するお問い合わせは、下記の宛先にて電子メールまたは、FAXにてお受け致します。

ルートマジック・サポートセンター

- 電子メール
support@routrek.co.jp
- FAX
044-829-4362

また、弊社ホームページ上でも製品に関する最新情報をご案内しております。最新のマニュアルも下記ホームページよりダウンロード可能ですのでご参照ください。

- ホームページ
<http://www.routrek.co.jp>

製品仕様

■ 本体仕様

インタフェース	シリアルポート EIA-RS232D (RJ-45) × 2
ネットワークポート	IEEE802.3 10BASE-T (RJ-45) × 1
表示機能	ステータス LED (7セグメント), LINK LED, ACT LED
電源	DC 5V (AC アダプタ 定格入力 100V AC ±10% 50/60Hz)
消費電力	DC 5V 1A
使用条件	気温 0~40℃ 湿度 15~85% ただし結露しないこと
EMI	VCCI クラス B
外形寸法 (WxDxH)	85x110x23 (mm)
重量	140g

■ COM1/COM2 ポート仕様



87654321

ピン番号	信号	入出力
1	RTS	OUT
2	DTR	OUT
3	TXD	OUT
4	SG	—
5	SG	—
6	RXD	IN
7	DSR	IN
8	CTS	IN

■ 付属ケーブル／コネクタ仕様

RJ-45 ROLLED シリアルケーブル仕様 (クロス)

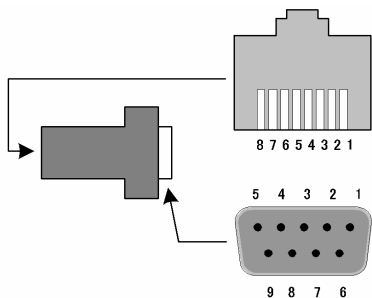


RJ-45 RJ-45

1-----8
 2-----7
 3-----6
 4-----5
 5-----4
 6-----3
 7-----2
 8-----1

RJ-45・DB9 ソケット変換コネクタ仕様（ストレート／シリアル端末接続用）

RJ-45 8 極ジャック ピン配置
（プラグ挿入方向より見る）

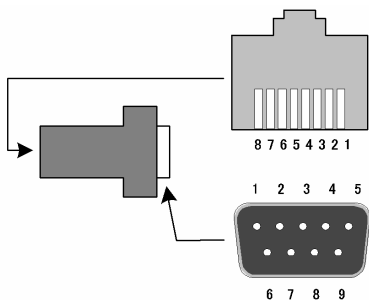


RJ-45 ジャック (メス)	9 極ソケット (メス)	信号
1	7	CTS
2	4	DSR
3	3	RXD
4	5	GND
5	5	GND
6	2	TXD
7	6	DTR
8	8	RTS

D-sub 9 極ソケット ピン配置
（プラグ挿入方向より見る）

DB25・DB9 プラグ変換コネクタ仕様（クロス／モデム接続用）

RJ-45 8 極ジャック ピン配置
（プラグ挿入方向より見る）



RJ-45 ジャック (メス)	9 極プラグ (オス)	信号
1	8	CTS
2	6	DSR
3	2	RXD
4	5	GND
5	5	GND
6	3	TXD
7	4	DTR
8	7	RTS

D-sub 25 極プラグ ピン配置
（ソケット挿入方向より見る）

Open SSL

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)

This product includes cryptographic software written by Eric Young (eyay@cryptsoft.com)."

Postfix mail system

Copyright (c) 1997,1998,1999, International Business Machines Coproration and others.

All Rights Reserved.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

- a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
- b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
- c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

- a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

net-snmp

Copyright 1989, 1991, 1992 by Carnegie Mellon University

Derivative Work - 1996, 1998-2000

Copyright 1996, 1998-2000 The Regents of the University of California

All Rights Reserved

CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF

MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU OR THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM THE LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Copyright (c) 2001-2002, Networks Associates Technology, Inc

All rights reserved.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Portions of this code are copyright (c) 2001-2002, Cambridge Broadband Ltd.

All rights reserved.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

ルートレック・ネットワークスのロゴ、RouteMagic は、株式会社ルートレック・ネットワークスの登録商標です。本書に記載されているハードウェアもしくはソフトウェア製品名等の固有名詞は、各社の商標もしくは登録商標です。

保証規定

1. 保障期間内に、取扱い説明書の注意書きによる正常なご使用状態において万一故障した場合は、無償で修理もしくは交換いたします。
2. 保証期間内でも次のような場合は有償修理となります。
3. 保証書のご提示がないとき。
 - ① 本保証書の所定事項の未記入、字句を書き換えられたもの、および販売店名の表示がないとき。
 - ② 天災・地震・水害・落雷・その他の天災、公害や異常電圧による故障および損傷
 - ③ お買い上げ後の輸送、移動時の落下など、お取扱いが不適当なために生じた故障および損傷。
 - ④ 取扱説明書に記載の使用方法、注意に反するお取扱いによって発生した故障、または損傷
 - ⑤ 改造または、ご使用者の責任に帰すと認められる故障、または損傷
 - ⑥ 接続している他の機器、その他外部的要因に起因して本製品に故障を生じた場合。
4. 修理を依頼される場合は、お買い上げの販売店へ保証書を添えてご持参ください。
5. 本製品が、ご贈答品等で修理を依頼される場合、あるいはご転居後に修理を依頼される場合は、本保証書に記載された販売店にご相談ください。
6. 本書は、日本国内においてのみ有効です。

* この保証書は、本書に明示した期間、条件のもとでの無償修理をお約束するものです。したがって、本書によってお客様の法律上の権利を制限するものではありませんので、保障期間経過後の修理等についてご不明の点は、お買い上げの販売店にお問い合わせください。

製品保証書

本保証書は、お買い上げの日から下記保障期間中に故障が発生した場合、本書裏面記載内容で無料修理もしくは交換を行うことをお約束するのものです。詳細は裏面をご参照下さい。本書は再発行いたしませんので、大切に保管してください。

* 販売店欄に記入の無い場合は無効となりますので、必ず記入の有無をご確認ください。

商品名	RouteMagic Controller
モデル名	RMC-M2-01
製造番号	(製品本体に記載)
ご購入日	年 月 日
保障期間	(お買い上げ日より) 1年間

お客様名			
ご住所	〒		
電話番号		Email	

販売店(店名・住所・電話)

株式会社ルートレック・ネットワークス

ROUTREK
NETWORKS

〒213-0011 神奈川県川崎市高津区久本3-5-7
ニッセイ新溝ノロビル
Tel. 044-829-4361 Fax. 044-829-4362