RouteMagic

RouteMagic Controller

MP200 / MP1200

RMC Version 2.1.1

リリースノート

- 2002/08 -

ROUTREK NETWORKS

RMC-04-005　08/2002

はじめに

本書の目的

本書は、RouteMagic Controller(以下 RMC と記述)上で稼動するソフトウェア・バージョン 2.1.1 に関して、バージョン 2.0.2 との機能的な相違点、および RMC 設置・運用上の留意事項などを中心に記述しています。RouteMagic 製品の仕様ならびに操作方法全般に関しては、「RouteMagic Controller 取扱説明書 Version 2.1」および「RouteMagic Controller クイックリファレンス Version 2.1」をご参照ください。

本リリースの動作環境

RMC ソフトウェア Version2.1 は、RMC MP1200 および MP200（Model 2）ハードウェア上で動作します。RMC Model 1 には未対応ですのでご注意ください。
RMS を利用する場合は、RMS（RouteMagic Server）Ver.sion 2.1 以上の環境が必要となります。

本書の対象読者

本書は、次の方を対象に記述されています。

- RMC のコマンドおよび操作性に関して理解されている方
- ネットワーク環境の設定に関して基礎的な知識のある方

関連ドキュメント

RMC には、本書の他に、次のドキュメントが用意されています。

- Routemagic Controller（RMC-MP1200 / RMC-MP200） 取扱説明書 Version 2.1
  RMC の設置と初期設定の方法を中心に記述しています。RMC の仕様とお取扱いに関してもこちらをご覧ください。
- Routemagic Controller クイックリファレンス Version 2.1
  RMC が提供するコマンドの機能を簡単に記述したハンドブックです。
- RMC 一括セットアップガイド
  多数の RMC を設置される場合の、一括セットアップ／バージョンアップに関して記述しています。
- RMC 活用ガイド
  RMC に Cisco 社のルータ／スイッチ以外の装置を接続して監視対象とする場合の設定や注意事項を記述しています。
- Routemagic Controller コマンドリファレンス Version 2.1
  RMC が提供するコマンドの機能詳細を記述しています。

目次

1. ソフトウェア Version2.1 の変更点

RMC ソフトウェア Version2.1 では、従来の Version2.0.2 からマルチポート対応を始めとした大幅な機能強化が行われています。

RMC-MP1200 には、RMC Version2.1 ソフトウェアが搭載されていますが、旧ソフトウェアで稼動中の RMC-MP200(Model2)を Version2.1 にアップグレードされる場合は、弊社ホームページより、必要なソフトウェアとマニュアルをダウンロードしてご使用ください。現在稼動している RMC のソフトウェアバージョンは、*show version* コマンドにより確認できます。

➡「3. Version 2.1.1 へのアップグレード」参照

1.1 RMC-MP1200（マルチポート版 RMC）対応の機能

RMC ソフトウェア Version2.1 は、従来の RMC Model2（RMC-MP200）に加えて RMC-MP1200 に対応しています。RMC-MP1200 は、監視対象装置接続用として 12 個のシリアルポートを装備したマルチポート対応機種です。

Version2.1 は、RMC-MP1200 対応として以下のような機能性を提供します。これらの機能は、RMC-MP1200 ハードウェアを前提としたものですので、MP200 ではサポートされません。

各種ポートの追加

RMC-MP1200 に装備される各種ポートに対応し、以下の機能追加が行われています。

1. マルチポート対応（COM1~COM12）

RMC-MP1200 は、監視対象装置接続用のシリアルポートを 12 ポート装備しています。
各シリアルポートは COM1~COM12 として定義され、従来の COM1 ポートと同様に利用できます。

2. シリアルコンソール専用ポート（COM A）

シリアルコンソール専用ポート（COMA）を提供します。
RMC-MP1200 はシリアルコンソール専用ポートを装備するため、Version2.1 では従来の COM2 ポートに代わり、COMA ポートがシリアルコンソール接続専用ポートとして定義されます。

3. モデム専用ポート（COMB）

モデム接続専用ポートを提供します。
RMC-MP1200 はモデム接続専用ポートを装備するため、Version2.1 では従来の COM2 ポートに代わり COMB ポートがモデム接続専用ポートとして定義されます。

4. メンテナンス用イーサネットポート対応（ETH1）

メンテナンス用イーサネットポートを提供します。
RMC-MP1200 は、2 個の 100BaseTx イーサネットポートを装備しています。Version2.1 では、新たに ETH1 ポートがメンテナンス用イーサネットポートとして定義されます。メール送信などのイーサネットポートを使用した通常の通信は、従来通り ETH0 ポートを使用して行われます。

ETH1 はメンテナンス用ポートのため、以下の機能的制約があります。

- DHCP による IP アドレスの設定はできません
- デフォルトゲートウェイの指定はできません
- LAN 内の同一セグメントに対してのみ通信可能です

LCD 操作パネルの機能

RMC-MP1200 には、前面パネルに LCD 表示装置（20 文字×2 段）と操作ボタンが装備されています。バージョン 2.1 のソフトウェアでは、この操作パネルを利用して次のような機能を提供します。

LCD 操作パネルの利用に関する詳細は、「RMC-MP1200 取扱説明書」を参照してください。

1. 通常モードでの表示機能

通常の動作状態では、LCD にはイーサネットポート（ETH0）の IP アドレスが表示されます。ボタン操作により ETH1 ポートのアドレス表示も可能です。また、RMC が PPP 接続を行った場合には、PPP ポートの IP アドレスが表示されます。

2. メニューモードでの操作機能

IP アドレス表示の状態から、ボタン操作により以下のような操作が可能です。

メニュー表示	機能
0：RMC soft version	RMC に搭載されているソフトウェアのバージョン、および現在の時刻を表示
1：COM port status	COMA／B、COM1~COM12（シリアルポート）のステータスを表示
2：ETH port status	ETH0／1（イーサネットポート）のステータスを表示
3：Set ETH IP addr	ETH0／1（イーサネットポート）に IP アドレスを設定
4：Set ETH speed	ETH0／1（イーサネットポート）の通信速度と通信方式（10／100Mbps、全二重／半二重）を選択
5：Set LCD light	LCD バックライトの ON／OFF を指定
6：Write config	RMC 設定情報の保存を実行
7：Restart／Halt RMC	再起動（Restart）／シャットダウン（Halt）を実行
8：Erase config	RMC の設定を初期化（工場出荷状態に戻す）

VGA モニタ、キーボードの接続

RMC-MP1200 は、モニタ／キーボード接続用の専用ポートに VGA モニタと PS/2 キーボードを接続してローカルコンソールとして使用することができます。

モニタ／キーボードを使用してログインする場合は、最初にキーボードの種類を尋ねられます。英語キーボードの場合は "1" を、日本語キーボードの場合は "2" を入力してください。

1.2 RMC-MP200（Model2）におけるマルチポート対応

従来の RMC Model2 において、COM1,COM2 双方のポートに監視対象装置を接続することが可能となりました。Version2.1 を使用した場合、COM2 には、監視対象装置／シリアル端末／モデムのいずれかを接続して利用することができます。COM1 は、従来通り、監視対象装置接続専用ポートです。
COM2 に監視対象装置を接続される場合は、COM1 と同様に、監視対象装置の仕様に合わせて COM2 ポートの設定を行ってください。

1.3 Version2.1 新規追加コマンド

フィルタ／スクリプト定義の機能強化

フィルタとスクリプトが従来のメールポート毎／COM ポート毎にカスタマイズする方式から、装置の種類を任意に定義し、装置種別ごとにカスタマイズする方式に変更されました。これにより、監視対象装置の種類に依存したメッセージのフィルタリングや動作仕様定義など、カスタマイズの自由度が大幅に向上します。フィルタ、スクリプトの記述形式も機能強化のため、変更されています。詳しくは、「RMC Version2.1 取扱説明書」および「RMC 活用ガイド」をご参照ください。
なお、従来の形式のフィルタ／スクリプトおよびその関連コマンドは、Version 2.1 でもご使用いただけます。

装置の接続仕様定義に関して、新規に追加されたコマンドは以下の通りです。

- **set [no] user-target-type {target_type}**
  監視対象装置の種別（"target_type"）を新規にユーザ定義します。
  (例: set user-target-type linux)

  ユーザ定義した装置種別は、set target-type の引数として使用可能になります。
  (例: set port com1; set target-type linux ：com1 に接続する装置に linux を指定)

- **set [no] target-filter {target_type} {tflN}**
  指定した装置種別専用のメッセージフィルタ(tfl0～tfl7)を設定します。
  フィルタは awk プログラム形式で記述します。

  フィルタの適用は、従来の hook コマンドではなく set spy コマンドを使用します。
  従来のフィルタ指定コマンドである hook では、メールポートごとに適用するフィルタを指定しましたが、Version2.1 では COM ポートごとに適用するフィルタと出力先のメールポートを設定する方式になります。
  (例:set spy com1 tfl0 ml0 ：com1 からの入力を tfl0 フィルタで処理し、
  メールポート ml0 から送信)

- **filter-test {target_type} {tflN}**
  設定したフィルタのテストを実行します。

- **show target-filter {target_type} [tflN]**
  指定した装置種別に対応するフィルタを表示します。
  フィルタ名を指定しない場合は、その装置種別に関する全てのフィルタを表示します。

- **set [no] target-script**
  {target_type}{command|login|network-info|target-check}
  指定した装置種別の、装置操作用スクリプトを設定します。
  スクリプトの文法は、Ver2.0 のものとは異なっています。
  入力に応じた分岐や条件判断など、より高度な処理が可能になりました。

- **script-test {comN} {command|login|network-info|target-check}**
  設定したスクリプトのテストを実行します。

- **show target-script**
  {target_type} [command|login|network-info|target-check]
  指定した装置種別用のスクリプトを表示します。スクリプト名を指定しない場合は、その装置種別に関する全てのスクリプトを表示します。

- **set [no] target-login-name {login_name}**
  監視対象装置にログインする際のユーザ名を設定します。

SNMP エージェント機能の搭載

Version2.1 では、新たに SNMP エージェント機能が搭載されました。この機能の利用により、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。

- **set snmp-community {community}**
  SNMP コミュニティ名を指定し、SNMP エージェントを起動します。
  RMC では標準 MIB のみサポートしています。

- **set snmp-trap {host_address} {community}**
  SNMP TRAP 先のホスト名もしくは IP アドレスを設定します。
  TRAP は"coldStart Trap", "warmStart Trap"の 2 種類です。

その他の新規追加コマンド

＜タイムゾーンの指定＞

- **set timezone {zonename}**
  RMC が使用する時刻のタイムゾーンを指定します。
  引数なしで実行すると設定可能なタイムゾーンの一覧を表示します。
  現在サポートしているタイムゾーンは、「クイックリファレンス」を参照してください。

＜文字コードの指定＞

- **set lang {en-ascii|ja-euc|ja-sjis}**
  RMC メッセージなどの文字コードを指定します。デフォルトは en-ascii (英語)です。

＜表示のページング処理（More 対応）＞

- **set [no] terminal [line [column]]**
  ページング処理における端末の表示行数と桁数を指定します。主にシリアル経由のログインの場合に使用します。
  (イーサネット経由のログインの場合、端末サイズは自動設定されます)

＜ログイン時のバナー表示設定＞

- **set [no] banner {text}**

  設定された文字列は、ログイン時に表示されます。
  また、RMC-MP1200 の LCD 表示にも反映されます。

＜COM ポートのコメント設定＞

- **set [no] description {text}**

  設定された文字列は、show port comN 実行時にコメントとして表示されます。
  また、RMC-MP1200 の LCD でのシリアルステータス表示にも反映されます。

＜connect の強制解除＞

- **disconnect {comN}**

  指定されたポートの connect 状態を強制的に解除します。

＜POP メールの取得＞

- **mail-pop**

  POP メール取得の手動実行を行います。

＜ポート指定の解除＞

- **end、set no port**

  カレントポート指定(set port 状態)を解除します。CTRL-Z でも同様の動作になります。

1.4 コマンド仕様の変更

- **exit、quit**

  コマンド実行時は、常にログアウトするようにしました。
  特権モードから通常モードに戻るには、disable コマンドを使用してください。

- **set target-type {target_type} [arg1] [arg2] [arg3] [arg4]**

  従来の"cisco", "custom"に加えて、set user-target-type で定義した装置種別の指定が可能になりました。機種毎のフィルタ、スクリプトに渡す引数の設定も可能です。

- **set spy: set spy {comN} [tflN] {comN|mlN|terminal}**

  １）接続先ポートとして terminal の記述が可能になりました。
  set spy comN terminal で、シリアルポートからの入力をログイン端末に表示することが出来ます。
  ２）接続の指定と同時に、装置種別毎に定義されたフィルタ指定が可能になりました。
  set com1 tfl0 ml0 を実行すると、com1 の入力をフィルタ tfl0 で処理し、結果を ml0 からメール送信します。装置固有のフィルタ定義に関しては、set target-filter コマンドを参照してください。

- **show port**

  １）show port comN で監視対象装置の生存確認ステータスを、ポートが使用中の場合はそのユーザ/プロセスを表示するようになりました。
  ２）show port mlN で、メールポートから発信されたメールの総数、および設定されたメールアドレスに対する PGP 公開鍵の有無を表示するようになりました。

- **show version/show memory**

  一時記憶領域(Storage)の総容量および空き容量が表示されるようになりました。

- **connect**

  ポートが使用中の場合は、使用ユーザ/プロセスを表示するようにしました。

- **show log rmc**

  ログ情報が強化され、以下の動作がログに記録されるようになりました。
  ・ネットワーク情報取得
  ・監視対象装置の生存確認ステータス取得
  ・RMS からの定石コマンドメールの実行

- **set [no] filter-list**

  set no filter-list により、指定されたフィルタの削除が可能になりました。

- **set [no] broadcast-address**

  set no broadcast-address により、ブロードキャストアドレスをデフォルト設定に戻すことが可能になりました。詳細は「クイックリファレンス」をご参照ください。

- **mail-test**

  引数として、"setupinfo"オプションが追加されました。
  このオプションを付加した場合、テストメールの代わりに"Setup information"メールが送信されます。

1.5 その他の仕様変更

1. ファンクションスイッチの機能 （RMC-MP200 のみ）

   ファンクション「０」番の機能に、時刻表示が追加されました。
   バージョンの表示の後に "月/日/年 時 分" を表示します。

2. ログ格納サイズの変更

   show log comN で表示されるシリアルログの格納サイズが、100KB から 200KB に拡張されました。

3. PPP 接続時の動作変更

   PPP 接続でメールを送信する場合、10 分間接続した後は一旦回線を切断し、5 分間の着信待ち時間を設けるようにしました。

4. 自動セットアップ／アップグレードサーバ用設定ファイル名の変更

従来	MP200(Model-2)	MP1200
rmc-v2.rc	mp200-v2.rc	mp1200-v2.rc
rmc-v2.cfg	mp200-v2.cfg	mp1200-v2.cfg

1.6 標準設定の変更

RMC のデフォルト設定（工場出荷時の設定状態）が以下のように変更されます。

1. spy 設定の追加

   従来のデフォルト設定に、spy target2 ml0 が追加されました。

   ```
   spy target1 ml0
   spy target2 ml0      ← 追加
   spy rmc ml0
   ```

2. hook 設定の削除

   メールポート０(ml0) に対して設定されていた hook の指定が削除されました。

   Version 2.0 までのデフォルト設定： **hook fl0**

   Version 2.1 のデフォルト設定： **hook no**

   ※フィルタ設定に関しては、「フィルタ,スクリプトの仕様変更」を参照してください。

3. set exec（シリアルコンソール接続）時のフロー制御

   デフォルトの設定が "software" から "none" 固定に変更されました。

   Version 2.0 までのデフォルト設定： **set flowcontrol software**

   Version 2.1 のデフォルト設定： **set flowcontrol none**

1.7　フィルタ、スクリプトの仕様変更

フィルタ機能の変更

従来はメールポート毎にフィルタを設定する形式でしたが、Verson2.1 では、装置の種類別にフィルタを用意し、spy コマンドによって COM ポート毎に使用フィルタを指定する形式に変更されています。
従来の hook コマンド、および set filter-list コマンドも互換性維持のために残されています。

Version 2.0 のフィルタ設定：

```
set filter-list flN
set port mlN
hook flN
```

Version 2.1 のフィルタ設定：

```
set user-target-type my_target_type        ←装置種別をユーザ定義
set target-filter my_target_type tflN      ←定義した装置種別に対応するフィルタを設定
set port comN
set target-type my_target_type             ←COM ポートに対して装置種別を指定
set spy comN tflN mlN                      ←COM ポートに接続されるメールポートとフィルタ
                                             を指定
```

スクリプト機能の変更

従来 COM ポート毎に用意されていたスクリプトは、フィルタと同様に装置種別ごとに用意する形式に変更されています。

なお、従来の方式によるスクリプト設定も引き続き利用可能です。

Version 2.0 のスクリプト設定：

```
set port comN
set target-type custom
set script network-info
```

Version 2.1 のスクリプト設定：

```
set user-target-type my_target_type          ←ユーザ定義の装置種別を定義
set target-script my_target_name network-info ←装置種別に対応する network-info
                                               スクリプトを設定
set port comN
set target-type my_target_type               ←COM ポートに対して装置種別を指定
```

1.8 Version 2.1 における制限事項

RMC Version 2.1 では、以下のような機能的制限事項がありますのでご注意ください。

RMC-MP1200/200 共通

- set target-type custom されているポートに対して、script-test コマンドを実行した場合、その実行結果は show log comN には記録されません。また、set spy が設定されていても、spy の対象にはなりません。
- 一般モードで特権モード専用コマンドを実行した場合、V2.0 以前は"can't execute on normal mode."と表示されていましたが、V2.1 からは"command not found."と表示されます。

RMC-MP200

- set exec（COM2 をローカルコンソールとして設定）、または set modem（COM2 をモデム接続に設定）が行われている間は、当該ポートに対する spy の設定は無効になります。
  set no exec / modem を実行し、ローカルコンソール／モデム接続の状態を解除してください。

RMC-MP1200

- VGA コンソール（DISPLAY ポートに接続）からログインした場合は、常に英語表示となります。
- ETH1 ポートはメンテナンス用ポートとなるため、以下の機能制限があります。
  - 同一セグメント上のノードとの通信のみが可能です。
  - set dhcp により、DHCP サーバからアドレスを取得することはできません。
  - set address において、デフォルトゲートウェイを指定することはできません。
- IP アドレスの自動設定機能はサポートされていません。

1.9　既知の問題点への対応

旧バージョンにおいて発生した以下の問題は、Version 2.1 で対応されています。

- 一般機器に対するユーザ定義スクリプトの結果が、show log com1 で表示されない。
- set ntp-server に有効でないサーバを設定している場合、起動に数分間余計にかかる。
- show log mail で、POP メール取得関連のログが表示されない。
- set mail-origin の設定を変更しても、"Target Message"メールに即時に反映されず、再起動や spy の再設定が必要とされる。
- set pop-before-smtp を引数なしで実行した場合、設定が有効にならない。
- POP メール取得でエラーが起きた場合、show log mail にログが記録されない。
- RMC の時刻が PGP 公開鍵作成時刻以前の値に設定されていた場合、PGP メールが送受信共にエラーになってしまう。

2. ソフトウェア Version2.1.1 の変更点

RMC ソフトウェア Version2.1.1 では、Version2.1.0 に対して以下の変更が行われています。

RMC-MP1200 には、RMC Version2.1 ソフトウェアが搭載されていますが、旧ソフトウェアで稼動中の RMC-MP200(Model2)を Version2.1 にアップグレードされる場合は、弊社ホームページより、必要なソフトウェアとマニュアルをダウンロードしてご使用ください。現在稼動している RMC のソフトウェアバージョンは、*show version* コマンドにより確認できます。

➡「3. Version 2.1.1 へのアップグレード」参照

2.1 不具合の修正

RMC V2.1 で対応されている問題点は、以下の通りです。

1. **SNMP エージェントの sysObjectID の内容を弊社独自の値に修正**

   MP200: enterprises.14360.1.200

   MP1200: enterprises.14360.1.1200

2. **起動直後の Cisco ルータの生存確認に失敗する**
3. **copy コマンドで、ユーザ定義の command スクリプトの内容が保存されない**
4. **copy コマンドでの running-config 設定時に、Setup information メールが送信されない場合がある**
5. **MP1200 で、RARP による eth1 のアドレス取得が正常に実行されない場合がある**

3. Version 2.1.1 へのアップグレード

RMC ソフトウェア Version2.1.1 は、RMC-MP1200 および MP200（Model 2）ハードウェア上で稼動します。Version2.1 では、Version1.1 に比べて大幅な機能性の改善などが行われています。旧リリースのソフトウェアを搭載した RMC Model2 をご利用の場合は、最新ソフトウェア Version2.1.1 へのアップグレードをお勧めします。

アップグレード作業を行うために、次の 2 種類の環境が用意されています。

なお、下記の Version2.1.1 アップグレード用ソフトウェアは、RMC に搭載されているソフトウェアが Version2.0.2 またはそれ以降であることを前提としています。それ以前のバージョンのソフトウェアをご利用の場合は、まず、Version2.0.2 へのアップグレードを行った後、Version2.1.1 へのアップグレードを行ってください。

Windows 版　アップグレード

- Window 端末に必要なソフトウェアをダウンロードし、この端末から telnet 接続を利用してアップグレードを実行します。
- アップグレード作業には､RMC と同じネットワークに接続された Windows マシン が必要です。

tftp 版　アップグレード

- ダウンロードしたアップデートファイルを tftp サーバに格納し､RMC 側から upgrade tftp コマンドを実行することにより、アップグレードを実行します。
- RMC から接続可能な tftp サーバを準備する必要があります。Windows の場合でも、フリーソフトの tftp サーバを利用することが出来ます。

いずれの方法でアップグレードを行っていただく場合も､バージョンアップに必要なソフトウェアは、ホームページから直接ダウンロードできます。バージョンアップに必要な手順等を記述した「RMC アップグレード手順書」もホームページからダウンロード可能ですので、詳細はこちらをご参照ください。

ホームページ：　http://www.routrek.co.jp/support/

※アップグレード作業におけるご注意

- アップグレード時には以前のバージョンの設定が引き継がれますが、アップグレードの前に copy running-config terminal で表示される設定を別途記録しておくことをおすすめします。
- RMC ソフトウェア Version2.1 は、Model1 ハードウェアには対応しておりません。
- RMS(RouteMagic Server)をご利用になる場合、RMS も Version2.1 以上が必要になります。

4. システム動作環境

4.1 シリアル端末／モデムからのログイン

Window 標準添付のハイパーターミナルや、フリーソフトの Tera Term Pro などのターミナルソフトが必要です。また、Local Echo は OFF にしてください。

“Tera Term のホームページ:”
http://hp.vector.co.jp/authors/VA002416/

Unix 系 OS の場合は、tip, minicom などのターミナルソフトをご使用下さい。

4.2 ネットワーク経由でのログイン

SSH1 または SSH2 プロトコル対応の ssh (Secure SHell)、又は telnet でログインします。日本語 EUC に対応している必要があります。また、Local Echo は OFF にしてください。

Windows の場合、Tera Term Pro + SSH Extension が ssh(SSH1 プロトコル)対応しています。また、Windows 標準添付の telnet をご使用の場合、文字コードを日本語 EUC に設定して下さい。

4.3 動作確認済みモデム／ISDN ターミナルアダプタ

RMC での動作を確認したモデムおよび ISDN ターミナルアダプタは以下の通りです。表中の“指定するモデム名”は、***set modem*** コマンド実行時に必要な引数です。

■ アナログモデム

モデム機種名	指定するモデム名
株式会社アイ・オー・データ機器 DFML-560E	指定不要（generic）
アイワ株式会社 PV-BF5606HM	指定不要（generic）
株式会社 メルコ IGM-B56KS	指定不要（generic）

■ ISDN ターミナルアダプタ

モデム機種名	指定するモデム名
日本電気株式会社 Aterm IT42	aterm
日本電気株式会社 Aterm ITX62	aterm

5. メールの設定

5.1 ネットワークの設定

ネットワークに DHCP サーバまたは RARP サーバが存在しない場合、最低限、RMC の IP address、ネットマスク、デフォルト経路の設定が必要です。*set address* コマンドで設定を行って下さい。また、多くの場合ネームサーバ(DNS)の設定も必要です。*set name-servers* コマンドで設定して下さい。
通常、RMC はメール送受信先のメールサーバ(SMTP サーバ)に直接接続を行います。従って、RMC と送受信先の SMTP サーバはお互いに IP reachable である必要があります。
また、リレーホストを使用したメールの送受信にも対応しています。使用するリレーホスト名は *set mail-relayhost* コマンドで設定できます。

5.2 メールアドレスの設定

送信先のメールアドレスはメールポート毎に *set mailto* コマンドで設定します。この際に、*set errors-to* コマンドでエラーメールの送信先も設定しておく事をおすすめします。

5.3 メール送信のテスト

“mail-test メールポート名” を実行すると、メールポートに指定された宛先にテストメールを送信します。コマンドが"ok"で終了し、宛先にメールが届いたら設定は完了です。

6. セキュリティに配慮した運用

セキュリティを重視する場合は、以下のような設定を行ってください。

6.1 ユーザ名、パスワードの設定

RMC のログインパスワードや特権パスワードを適切に設定・管理することが重要です。設定は、*set password, set enable-password* コマンドで行います。

また、RMC にログインする際のユーザ名(初期状態では"rmc")とは別の名前を用意しておくと、不正ログインに対するセキュリティが向上します。変更は、*set username* コマンドで行います。その際、*set user-name2 rmc* * コマンドを実行し、デフォルトで用意されている”rmc”のユーザカウントを無効にしてください。

6.2 ssh(Secure SHell) の使用

ネットワーク経由で RMC にログインする場合、telnet ではなく ssh のご利用をおすすめします。RMC とターミナル間の通信が暗号化されるため、ネットワークの盗聴などに対するセキュリティが向上します。

また、ssh を使用する際は、telnet ログインを無効にしておくことをおすすめします。設定は *set access-list deny telnet 0.0.0.0* で行います。

6.3 アクセス制限の設定

RMC では telnet, ssh, smtp(メール受信), snmp, tftp の各プロトコルについて、特定の相手に限り接続を許可・不許可にすることができます(初期設定ではすべて許可)。

アクセス制限を行う場合、許可するアドレスを *set access-list allow {プロトコル名} {IP アドレス}* コマンドで登録後、それ以外のアドレスからの接続はすべて不許可 (*set access-list allow {プロトコル名} 0.0.0.0)* にすることをおすすめします。例として、192.168.0.* からの ssh ログインだけを許可する場合、以下のコマンドを実行します。

```
set access-list allow ssh 192.168.0.0/24
set access-list deny ssh 0.0.0.0
```

6.4 送信メールの暗号化

RMC には PGP を使用して送信メールの暗号化と、受信メールの認証を行う機能があります。メールを暗号化するには、メールアドレスをキーとした PGP 公開鍵を別途用意し、それを *set public-key コマンドで* RMC に設定する必要があります。
その後、暗号化メールを送信するメールポートに対して *set mail-encryption* を実行すると、送信されるメールが暗号化されます。なお、暗号化の有無はメールポート毎に設定できます。

また、RMC から送信した暗号化メールを受け取るには、電子メールソフト(MUA)の側も PGP 暗号化メールに対応している必要があります。

7. RMS 関連の設定

RMS(RouteMagic Server)と連携して動作する場合、以下のような機能が強化されています。
なお、本機能を利用するには、RMC と RMS の両方が Version2.0 以上である必要があります。

7.1 RES(独自暗号方式) メールの設定

Version2.0 以降では独自のメール暗号化方式(RES: Routrek Encryption Scheme)をサポートしています。これは RMS と RMC で共通の秘密鍵を自動設定してメールを暗号化する方式で、従来の PGP に比べて以下のようなメリット・デメリットがあります。

メリット:

- 鍵の設定が不要で、セットアップの手間が低減できる。
- 送信メールだけでなく、受信メールも暗号化できる。

デメリット:

- RMS と RMC の間でメールの送受信が可能でないと利用できない。
- PGP に比べ、なりすまし問題(Man in the middle attack)に弱い。

RES 暗号メールを利用する場合、RMC 側で以下の設定を行います(RMS 側の設定は不要です)。
なお、RES 暗号メールは RMS との通信専用となり、メールポート 0(ml0)以外のメールは RES 暗号化できません。

```
―――――
set port ml0
set mail-encryption res
set mail-certification
―――――
```

7.2 RMS からの SSH 経由コマンド発行の設定

RMS から RMC へのコマンド発行は通常メールが使われますが、RMS と RMC がお互いに IP reachable な環境にある場合は、SSH 経由でのコマンド発行も可能です。

SSH 経由でコマンド発行を行う場合、まず RMS 側で「RMC の登録情報－RMS から RMC へのコマンド発行手段」を SSH に設定します。

次に、SSH ログイン用のパスワードを、RMS と RMC の両方に設定する必要があります。RMS と RMC 間のメール送信が RES(独自暗号方式)で行われている場合、パスワードは自動で設定されます。そうでない場合、RMC 側では *set user-password rms* <パスワード> を実行して、ユーザ ID”rms”にパスワードを設定してください。

8. トラブルシューティング／よくあるご質問

1. シリアルポートの接続確認を行ういい方法はありますか

show port comN コマンドの実行、RMC 本体正面のファンクションスイッチ（RMC-MP200）、もしくは LCD 操作パネル（RMC-MP1200）を使用して、COMN ポートの制御信号状態を確認する機能が提供されています(「取扱説明書」"ファンクションスイッチの機能"、または "LCD 操作パネルの使用方法" 参照)。正常に接続されている場合の表示は以下のようになります。

ターミナルや監視対象機器などが正常に接続されている場合

RTS, CTS, DTR, DSR が点灯　(MP200：LED の縦棒が全点灯)

モデムや ISDN ターミナルアダプタが正常に接続されている場合

RTS, CTS, DTR が点灯　(MP200：LED の左側の縦棒と、LED の右側の縦棒下半分が点灯)

表示が上記と異なる場合は、シリアルの電気的な接続に問題があります。ケーブルのクロス／ストレートはあっているかなどを確認してください。

2. COM1 ポートにログイン、またはモデムをつなぐにはどうすればいいでしょう（MP200）

COM1 ポートは、監視対象装置への接続専用になっています。ローカルコンソールやモデム接続用のポートとして使用する事はできません。

3. COM ポートに定期的に ENTER コードが送信されています

監視対象装置の生存確認が ON に設定されている場合、RMC は COM1 に接続された監視対象装置に対して 15 分に 1 回 ENTER コードを送信して生存確認を行います。この機能を OFF にしたい場合は、*set no target-check* コマンドを実行してください。

4. connect コマンドを実行すると「ポートが使用中です」とのエラーが表示されました

他のユーザが connect コマンドを実行しているか、RMC が生存確認やネットワーク情報の取得を実行中の可能性が考えられます。

5. connect コマンドを終了する方法がわかりません

connect コマンドのエスケープ文字(デフォルトでは Ctrl-¥)を入力後、'x'を入力してください。RMC のプロンプトに戻ります。

6. COM ポートに Cisco 製品以外の装置を接続する場合、どういう設定が必要ですか

Cisco 以外の製品を接続した場合、connect コマンドの実行やコンソール出力の spy に関しては、追加の設定なしでもご利用できます。一方、コンソール出力のフィルタ処理や装置の生存確認、ネットワーク情報取得を行いたい場合は、ユーザ定義のフィルタおよびスクリプトを設定する必要があります。

フィルタ、スクリプトの詳細については別途資料をご参照ください。

7. ユーザ定義のスクリプト(ネットワーク情報取得など)がうまく動きません

スクリプトが期待通りの動作を行わない場合、*script-test* コマンドでスクリプトを実行すると、入出力文字や実行ステータスなどのデバッグ情報が表示されます。

8. RMC にログイン後、表示されるメッセージが一部文字化けします

お使いのターミナルソフトの文字コード設定と RMC が表示するメッセージの文字コードが一致しているかを確認して下さい。

RMC が表示するメッセージの文字コードは、set lang コマンドで設定します。

9. コマンドは存在するはずなのに、実行すると "command not found." と表示されます

一部のコマンドは、特権モードに移行してから実行する必要があります。それらのコマンドを一般モードで実行すると、"command not found." が表示されます。特権モードに移行するには、*enable* コマンドを実行して下さい。

10. RMC からメールが送られてきません

まず「メールの設定」の章を参照し、”*mail-test* メールポート名” を実行してテストメールが送信されるかどうかを確認して下さい。
また、テストメール以外のメールは、メールサービスが ON になっていないと送信されません。*show running-config mail* を実行し”*set mail-service*”の行を確認して下さい。”set no mail-service”と表示される場合は、*set mail-service* を実行して下さい。

11. *mail-test* コマンドは”ok”で終了したのに、メールが届きません

RMC にエラーメールが返送されている場合があります。*show mail* コマンドで受信メールの内容を確認してください。
また、*set errors-to* でエラーメールの送信先を指定していた場合は、そちらにエラーメールが届いている可能性があります。
エラーメールが届いていない場合は、*show log mail* コマンドを実行し、ログの内容を確認して下さい。

12. テストメールは正常に送られてくるが、監視対象装置からのメッセージがメールされません

以下の内容を順番に設定・確認して下さい。

まず、*show running-config* を実行し"set mail-service"の行を確認して下さい。”set no mail-service”と表示される場合は、*set mail-service* を実行し、メールサービスを ON にします。また、*show log com1* コマンドを実行し、監視対象装置からの入力が実際にあるのかどうかの確認も必要です。

次にシリアルポートからの入力が、メールポートに接続されているかどうかを確認して下さい。確認には、*show spy* コマンドを実行します。接続されていない場合は、”*set spy com1 メールポート名*” を実行して、COM1 ポートからの入力をメールポートに接続するように設定します。

次に、フィルタの設定を確認します。”*show spy*” を実行してください。フィルタが割り付けられている場合は、"set spy com1 tfl0 ml0" というように表示されます。

フィルタが割り付けられている場合、”*show target-filter*” を実行して、フィルタの内容を確認してください。また、”*filter-test*” コマンドを実行して、フィルタの動作を実際に確認することができます。

13. RMC が送信したメールが届くのに、数分間の遅れがあります

show log mail で表示されるメール送信記録中の”delay”の値(単位は秒)が数分と大きい場合、メール受信側の MTA(メール送受信プログラム)で DNS の逆引きを行う際に遅延(DNS タイムアウト等)が発生している可能性があります。この場合、メール受信側の MTA もしくは DNS の設定を変更する必要があります。

14. POP3 でのメール受信を、モデム経由で行うにはどうすればいいでしょう

現バージョンでは、POP3 でのメール受信は常にイーサネット経由で行います。モデム経由でのご利用はできません。

15. RMC にログインしていたのに、しばらくすると接続が切断されています

初期設定では、RMC を 3 分間操作しない状態が続くと自動ログアウトします。*set exec-timeout* コマンドで、自動ログアウトするまでの時間を設定できます。

16. RMC にネットワーク経由でログインしようとすると、ログインプロンプトが出るまでに数十秒かかります

RMC でのネームサーバ(DNS)の設定が正しいかどうかを確認してください。ログイン元のホスト名の解決がうまくいっていない可能性が考えられます。

17. DHCP が無い環境で、RMC の初期設定をネットワーク経由で行えますか（MP200）

LED に ”-no IP address-” が表示されている場合、RMC 正面のファンクションスイッチを操作して、IP アドレスを自動的に取得・設定する機能が用意されています(MP200 :「取扱説明書」"ファンクションスイッチの機能" を参照)。

この機能を実行して、表示された IP アドレスに ssh/telnet 接続してください。

18. IP アドレスの自動設定はどのような仕組みで行われますか（MP200）

IP アドレスの自動設定機能が実行された場合、RMC はネットワークに流れる ARP(Address Resolution Protocol)パケットをまず監視します(この間、明示的にネットワーク内で ping などを実行すると、自動設定処理を早く行うことができます)。その後、得られた ARP パケットに含まれる情報を元に、ネットワーク内の使われていない IP アドレスを探索・設定します。なお、一定時間内に ARP パケットが取得できない場合は、192.168.0.x を設定します

19. ネットワーク経由でログイン時に、set address コマンドを実行すると接続が切れてしまい、IP アドレスの設定が行えません

set address で設定したアドレスにログインできない環境の場合、設定を保存するには以下のような方法があります。1) すべての設定を行った後に、*set address* コマンドを実行。接続が切断されるが、ファンクションスイッチの機能番号 A(設定を保存後に再起動)を実行して、設定を保存。2) *copy terminal running-config* コマンドを実行。*set address* を含む設定を記述し、最後に *write memory* コマンドを記入後に CTRL-D を入力。

20. 設定を間違って、ネットワーク／シリアルポートの両方からログインできなくなりました（MP200）

RMC 正面のファンクションスイッチの機能番号 3 で、COM2 ポートをローカルコンソールの設定に戻す機能が提供されています。「取扱説明書」の "ファンクションスイッチの機能" を参照してください。

21. RMC の設定をバックアップする方法はありますか

copy コマンドを利用してください。テキスト形式で設定をバックアップする場合、*copy running-config terminal* または *copy startup-config terminal* を実行し、表示される内容を端末のログ機能を使って保存します。設定を復元する場合は、*copy terminal running-config* を実行し、保存していた設定内容を端末から送信します。
また、tftp サーバにバイナリ形式で設定をバックアップする場合、*copy running-config tftp* または *copy startup-config tftp* を実行してください。設定を復元する場合は、*copy tftp startup-config* を実行します。

22. copy startup-config tftp を実行すると、”File not found.”エラーがでます

tftp サーバに設定を保存する際、サーバ側にあらかじめファイルが存在し、かつパブリックに書き込み権限が与えられている必要があります。

23. tftp サーバに保存している設定内容を参照する方法はありますか

copy tftp terminal コマンドを実行してください。tftp サーバに保存されている設定内容を端末に表示します。

24. copy startup-config running-config を実行しても、show configuration と show running-config の内容が同じになりません。

copy コマンドで、コピー先に running-config を指定した場合、コピー元の内容が現在の設定にマージされる形になります。コピー元の設定で現在の設定が置き換えられるわけではないのでご注意ください。

25. ssh で RMC にログインしようとすると、警告が表示されます

ssh で以下のような警告が出る場合があります(Linux 等の Unix 系 ssh の場合)。

```
_____________________________________________________________
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@       WARNING: HOST IDENTIFICATION HAS CHANGED!         @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that the RSA1 host key has just been changed.
The fingerprint for the RSA1 key sent by the remote host is
5e:2d:11:6c:db:63:1d:a1:06:b1:08:eb:b0:70:dc:9f.
Please contact your system administrator.
Add correct host key in /home/xxx/.ssh/known_hosts to get rid of this message.
  :
_____________________________________________________________
```

初期状態の RMC は、ssh の暗号化に使われるホストキーを、起動の度に新規作成します。このため、上記の警告(ホストキーが変更された)が表示される場合があります。これを防ぐには、RMC 上で *write memory* コマンドを実行し、ホストキーを含む設定内容を保存する必要があります。設定保存後は、RMC を再起動した場合にも以前のホストキーが引き続き使用されます。

なお、RMC の起動時などに送信される”Setup information”メール中には、ssh のホストキーおよびそのフィンガープリントの情報が含まれているので、ホストキーが改ざんされていないかどうかをチェックすることもできます。

26. RMC が送信した PGP 暗号化メールを受け取るには、どのような環境が必要ですか

PGP(5.x 以上)または GnuPG などの暗号化ソフトウェアと、暗号化メールに対応した電子メールソフト(MUA)が必要になります。詳細については、以下のホームページが参考になります。

″日本の公式 PGP ホームページ″(IIJ 技術研究所によって運営)
http://pgp.iijlab.net/

″PGP User's Manual for Windows″
http://www.cla-ri.net/pgp/

27. PGP 暗号化メールを使用していますが、RMC と RMS 間のやり取りが正常におこなわれていないようです

PGP の公開鍵をセットアップした後に発生した現象の場合は、公開鍵の設定誤り、もしくは複数の公開鍵が設定されているためのトラブルである可能性があります。この場合、メールは正常に送受信されますが、RMS はメールを正常に処理できません。以下の確認を行ってください。

① show key-list を実行します。

```
[rmc@rmc1(ml0)]# show key-list
--------------------------------
pub   1024D/E031E04B 2002-01-17 rms-system <rms@server.example.com>
      Key fingerprint = 7869 1846 C6CB 5E81 EC81   8D85 3E29 37FF E031 E04B
sub   1024g/C3D077A0 2002-01-17

pub   1024D/543CD2C0 2002-03-08 rms-system <rms@server.example.com>
      Key fingerprint = 5956 B395 BAB2 470A 87D5   F4C9 E7ED 1594 543C D2C0
sub   1024g/ F77CB5E3 2002-03-08

ok
```

上記のように、1 つのメールアドレスに対して複数の公開鍵が設定されてしまっている場合、暗号化機能が正常に動作しません。また、複数個の鍵が設定されていない場合でも、RMS 側の登録情報との一致を確認する必要があります。

② RMS で作成した公開鍵の fingerprint を出力します。RMS 上で、下記のコマンドを実行します。（rms ユーザとして Linux にログインして操作する必要があります。詳細は、RMS Version 2.0 インストール･ガイド「2.8 gnupg の基本設定」をご参照ください。）

```
$ gpg   --fingerprint   rms@server.example.com
```

上記 "rms@server.example.com" は、鍵を作成した時のメールアドレスを指定します。次のような内容が出力されます。

```
gpg: Warning: using insecure memory!
/var/lib/rms/.gnupg/pubring.gpg
pub   1024D/543CD2C0 2002-03-08 rms-system <rms@server.example.com>
      Key fingerprint = 5956 B395 BAB2 470A 87D5   F4C9 E7ED 1594 543C D2C0
sub   1024g/F77CB5E3 2002-03-08
```

③ RMC の "show key-list" と RMS の "gpg" コマンドで出力された Key fingerprint の文字列が一致していることを確認します。不一致があった場合、RMC の公開鍵を正しく再設定する必要があります。

④ "show key-list" の結果、RMS のメールアドレスに対して複数の鍵が設定されていた場合、RMS 側の出力結果と KeyID (上記 　　)の一致する公開鍵を残し、他の設定を削除します。

前記の例の場合、以下のコマンドを実行して KeyID E031E04B の設定を削除してください。

```
set no public-key E031E04B
```

9. マニュアル記載事項の訂正

RMC Version 2.1 マニュアルの記載事項に以下の誤りがありましたので、お詫びして訂正させていただきます。

RMC-MP1200「取扱説明書」

- P50、 ”商標とライセンス”記載条項の追加

  下記のライセンス条項が記載漏れとなっておりました。

net-snmp License

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.

製品に関するお問い合わせ

製品に関する技術的なご質問や、障害に関するお問い合わせは、下記にて電子メールまたはFAXでお受けしております。

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。最新リリースのマニュアルも下記ホームページからダウンロードすることができますのでご参照ください。

ホームページ

http://www.routrek.co.jp/

株式会社ルートレック・ネットワークス
〒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