RouteMagic

RouteMagic Controller

RMC Version 2.0.2

リリースノート

- 2002/05 -

ROUTREK NETWORKS

RMC-04-004　05/2002

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 2.0.2 に関して、バージョン 2.0.0 およびバージョン 1.1 との機能的な相違点、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ましては、「RouteMagic Controller 取扱説明書 Version 2.0」および「RouteMagic Controller クイックリファレンス Version 2.0」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 Version2.0.2 は、RMC 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。
また、RMS を利用する場合は、**RMS**（RouteMagic Server）**Ver.sion 2.0 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 取扱説明書 Version 2.0
  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 2.0
  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 一般機器接続ガイド
  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 2.0
  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Version2.0の変更点

RMC ソフトウェア Version2.0 では、以下のように従来の Version1.1 から大幅な機能強化が行われています。現在稼動している RMC のソフトウェアバージョンを確認する場合は、*show version* コマンドを実行して下さい。

1.1 一般機器(Cisco 製品以外の装置)の対応強化

スクリプトをユーザ定義することで、Cisco 製品以外の装置を接続した場合でも生存確認やネットワーク情報の収集などが行えるようになりました。

関連コマンド:set target-type, set script, script-test

1.2 メール関連の機能強化

1. メッセージのフィルタリング機能を強化

1 つのメールポートに対して複数のフィルタを AND 条件や NOT 条件で設定することが可能になりました。
関連コマンド: hook

2. セットアップ情報、キープアライブメールを任意のメールポートに送信可能

新設された仮想ポート"rmc"を spy することで、上記メールを任意のメールポートに送信可能になりました。なお、デフォルトでは従来通りメールポート 0 に送信されます。
コマンド例: set spy rmc ml1

3. ネットワーク情報、生存確認、操作ログメールを任意のメールポートに送信可能

仮想ポート"target1"を spy することで、監視対象装置に関する上記メールを任意のメールポートに送信可能になりました。なお、デフォルトでは従来通りメールポート 0 に送信されます。
コマンド例: set spy target1 ml1

4. メール 1 通ごとのメッセージ最大行数の指定が可能

関連コマンド: set max-nmr-of-lines

5. RMC が受信したメールの表示が可能

最後に受信したメールを表示します。RMS から受信したメールの確認や、エラーメールの内容確認に使用します。
関連コマンド: show mail

6. POP3 クライアント機能を搭載

指定した POP サーバから定期的にメールを取得することが可能です。外部ネットワークに設置した RMS(RouteMagic Server)から直接メールを受け取れない環境でも、RMC の運用が可能になります。
関連コマンド: set pop-username, set pop-interval, set pop-before-smtp

1.3 セキュリティ関連の強化

1. OpenSSH3.0 を採用

SSH1, SSH2 プロトコルの両方に対応しました。また、公開鍵認証方式にも対応しました。
関連コマンド : set ssh-protocol , set ssh-authentication, set ssh-public-key, show ssh-public-key

2. アクセス制限機能の強化

従来の telnet のアクセス制限機能に加えて、ssh, smtp(メール), tftp のアクセス制限が可能になりました。関連コマンド: set access-list, show access-list

3. RMS とのメール送受信に、独自の暗号化方式をサポート

従来の PGP による暗号化と認証に加えて、独自の暗号化方式(RES: Routrek Encryption Scheme)をサポートします。公開鍵等の設定が不要なため、設定の手間をかけずに RMS との通信を暗号化できます。
関連コマンド: set mail-encryption res

4. ログイン／特権パスワードの強化

パスワードに指定可能な文字列を、最大 8 文字から 127 文字に強化しました。
関連コマンド: set password, set enable-password

5. 設定の一覧表示の際、パスワード文字列を暗号化して表示

ログイン・特権パスワードだけでなく、監視対象装置や PPP アカウントなどすべてのパスワードを暗号化表示します。
関連コマンド: show running-config, show configuration, show port

1.4 遠隔操作性の向上

1. PPP サーバ機能を用意

RMC に対して PPP 接続が可能になり、モデム経由でのメール受信(SMTP 接続)も行うことができます。
関連コマンド: set ppp-server

2. RMS からの SSH 経由コマンド発行に対応

RMS が RMC に対してコマンドを発行する場合、従来のメールに加えて SSH 経由のコマンド発行が可能になりました。RMS と RMC が IP reachable な環境にある場合、コマンド発行のレスポンスをより向上させることができます。
関連コマンド: set user-password

1.5 管理・保守性の向上

1. セットアップサーバを使用した一括初期設定・アップグレードに対応

セットアップサーバ側に RMC の初期設定やアップグレードファイルを用意し、RMC にログインすることなく自動初期設定・アップグレードが可能です。詳細は別途資料をご参照ください。

2. IP アドレスの自動設定機能

ファンクションスイッチ(機能番号 4)で、IP アドレスの自動設定を行えます。DHCP サーバがない環境での初期設定の際にも、イーサネットからのログインが可能になりました。

3. RARP(Reverse ARP)での IP アドレス取得に対応

DHCP サーバが無い環境でも、RARP サーバを用意すれば各 RMC の IP アドレスを集中管理できます。

4. TFTP 経由での設定の保存と復帰に対応

設定のバックアップが容易になりました。また、端末にほぼすべての設定内容をテキスト形式で一括表示することも可能になりました。
関連コマンド: copy

5. TFTP 経由での RMC ソフトウェアアップグレードに対応

関連コマンド: upgrade tftp

6. Version2.0 へのアップグレード時に、以前のバージョンの設定を引き継ぎ

アップグレード後、再設定の必要がありません。

1.6 RMC シェルの強化

1. マルチユーザ・マルチアカウント対応

複数ユーザの同時ログインが可能です。また、新規ログインアカウントの登録も可能になりました。

2. カーソルキー対応

カーソルの移動や、コマンドヒストリの表示などをカーソルキーで操作できます。

1.7 操作性の改善

1. ファンクションスイッチの操作性改善と機能強化

スイッチを押した回数で実行したい機能を選択し、その後長押しすることで実行されます。また、以下の機能が追加されました:

機能番号 0: RMC ソフトウェアバージョンを LED に表示
機能番号 1,2: シリアルの信号線ステータスに加え、通信速度を表示
機能番号 4: IP アドレスを自動設定
機能番号 A: 設定の保存後に再起動

1.8 その他コマンド仕様の変更

1. 一部コマンドが、シリアルポートローカルなコマンドに変更

以下のコマンドは、シリアルポートローカルなコマンドになりました。実行の際にはあらかじめ set port <シリアルポート名>を行う必要があります。

set network-info, set target-check, set connect-log, set target-login-password, set target-enable-password

2. show log

引数に com1, com2 が指定可能になりました。従来の show log target コマンドは、show log com1 相当の動作になります。

3. set speed

引数に 57600, 115200bps の指定が可能になりました。

4. set target-check

監視対象装置の生存確認を行う間隔を、分単位で指定できるようになりました。デフォルトは 15 分、また設定可能な最短時間は 5 分です。

5. set ppp-username

空白のユーザ名、パスワードを指定できるようになりました。空白を指定する場合は引数に" (シングルクオート 2 つ)を指定してください。

6. set user-name

従来はログインユーザ名の変更でしたが、マルチアカウント対応に伴い、ユーザ名の追加・削除を行うコマンドになりました。

7. show port

引数に複数のポートを指定することができます(例: show port com1 com2)。

8. show public-key

PGP 公開鍵の内容を表示するコマンド show public-key が追加されました。

9. show ssh-hostkey

RMC の ssh ホストキーを表示するコマンド show ssh-hostkey が追加されました。

10. set prompt

この設定は、ログイン端末ごとに別々の設定内容を持ちます。また、ログイン直後は常にオン(コマンド実行の確認プロンプトを表示)になります。

2. ソフトウェア Version2.0.2 の変更点

RMC ソフトウェア Version2.0.2 では、Version2.0.0 に対して以下の変更が行われています。

2.1 セキュリティアップグレード

1. OpenSSH のセキュリティホール修正

詳細は以下の URL をご参照ください。
Pine Internet Security Advisory PINE-CERT-20020301: OpenSSH
http://www.pine.nl/advisories/pine-cert-20020301.html

2. zlib(データ圧縮ライブラリ)のセキュリティホール修正

RMC の場合 PGP(GnuPG)および PPP のプログラムが該当しています。詳細は以下の URL をご参照ください。
CERT Advisory CA-2002-07 Double Free Bug in zlib Compression Library
http://www.cert.org/advisories/CA-2002-07.html

2.2 動作仕様の変更

1. 監視対象装置の生存確認を最初に行った時点で、ステータスを必ず送信する

RMC 起動後などで監視対象装置の生存確認を最初に行った際、生存確認成功(サブジェクト:"Target responds")または生存確認失敗(サブジェクト: "Target not respond")のいずれかのステータスをメールで通知するようにしました(従来は、生存確認失敗時のみ通知)。

2.3 不具合の修正

1. フィルタパターンに空行("^$")を指定しても正常にフィルタされない

2. set max-nmr-of-lines で指定した最大行数より 1 行少ないメールが送信される場合がある

3. set public-key で同じ公開鍵を再登録するとエラー扱いになる

エラーとせず、正常終了としました。

4. set pop-interval で引数に 1500 を指定すると引数エラーになる

5. copy terminal running-config を実行しても特権モードパスワードが設定されない

copy running-config terminal で表示された設定内容を、copy terminal running-config で復元する際、set enable-password2 の実行で内部エラーが発生し、特権モードパスワードが設定されていませんでした。

6. 一般機器の生存確認スクリプトが正常に実行されない場合がある

一般機器(Cisco 製品以外の装置)の生存確認スクリプトが設定されており、装置からの応答がない場合、通知メール(サブジェクト:“Target not respond”)が送信されていませんでした。

7. 一部のネットワーク機器との接続において、コンソールポートからの出力を RMC が正常に受信できず、文字の抜けが発生する場合がある

Ver2.0.0 で既知の不具合となっていた項目を修正しました。

8. PGP 暗号化メールが、経路途中のメールサーバでエラーになる場合がある

暗号化メールのヘッダが、一部のメールサーバからエラーとみなされる現象の回避を行いました。

3. V2.0.2 へのアップグレード

RMC ソフトウェア Version2.0.2 は、RMC Model 2 ハードウェア上で稼動します。Version2.0.2 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 Version2.0.2 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なうために、下記の 2 種類の環境が用意されています。

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。

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 show configuration 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 Version2.0.2 は、RMC Model2 ハードウェア専用です。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 Version2.0 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

日本語 EUC に対応した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。
Windows 標準添付のハイパーターミナルは日本語 EUC に対応していません。フリーソフトの Tera Term Pro などのご使用をおすすめします。

“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、最低でも 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、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), 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 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 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. 既知の問題点／制限事項

1. ユーザ定義のスクリプト実行時のシリアルログが show log com1 で表示されない

Cisco 製品以外の監視対象装置を接続し、ユーザ定義のスクリプトを設定してネットワーク情報などを取得する場合、スクリプト実行中のログは *show log com1* での表示対象外になります。

➡ 今後のリリースにて対応を予定

2. モデム経由での POP のメール取得ができない

POP のメール取得は、現在はイーサネット経由のみとなります。

3. POP でのメール取得にエラーがあっても show log mail で表示されるログに記録されない

POP 設定のミスなどで POP でのメール取得にエラーが起きても、show log mail で表示されるログにその旨記録されません。

➡ 今後のリリースにて対応を予定

4. set max-nmr-of-chars の設定通りにコンソールメッセージが分割送信されない。

RMC は、原則として行単位でコンソールメッセージの送信を行います。
したがって、max-nmr-of-chars に 1 行の文字数よりも小さい値を設定した場合、コンソールメッセージは指定した文字数では分割されません。
例）set max-nmr-of-chars 50 と設定していた場合、1 行 100 文字の入力は 50 文字ごとに分割されることなく、100 文字のメールが 1 通送信されます。

5. Ver1 で set user-name rms と設定していた場合、Ver2 のアップグレード後にユーザ ID”rms”でログインできなくなる

Ver2 では、ユーザ ID”rms”が RMS との通信用に予約されています。

➡ Ver1 からアップグレードする前に、ユーザ ID を別名に変更してください。

6. 一般機器に対して、RMS からの SSH 経由のコマンド実行が正常に行われない

RMS で、「RMS から RMC へのコマンド発行手段」を”SSH”に設定にしている場合、一般機器(Cisco ルータ・スイッチ以外の装置)への定石コマンド実行が正常に行えません。具体的には、RMS の装置イベントログで「監視対象装置からの応答がありません。」と表示されます。

一般機器に対して RMS から定石コマンドを実行する場合、「RMS から RMC へのコマンド発行手段」は”メール” (標準設定)にしてください。

➡ 今後のリリースにて対応を予定

9. 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 com1/com2 コマンドの実行、もしくは RMC 本体正面のファンクションスイッチで、COM1, COM2 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」参照)。正常に接続されている場合の LED 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(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(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

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ご利用できます。一方、生存確認やネットワーク情報取得を行いたい場合はユーザ定義のスクリプトを設定する必要があります。

まず、*set target-type custom* を実行して接続装置の種類を指定します。その後、*set script* コマンドで生存確認・ネットワーク情報取得用スクリプトを定義します。生存確認用スクリプトが未定義の場合でも、シリアルの信号線レベルでの生存確認が行われますが、ネットワーク情報を取得したい場合は、スクリプトを必ず定義する必要があります。

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が、"日本語 EUC"になっているかを確認して下さい。

9. コマンドを実行すると、"can't execute on normal mode."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。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、メールポートに割り付けられているフィルタの設定を確認します。”*show port メールポート名”* 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、”hook フィルタ名"と表示されます。

フィルタが割り付けられている場合、”*show running-config mail”* 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 フィルタ名”* 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

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(取扱説明書の「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、LED に表示された 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

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

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
```

② 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。

③ "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
```

10. マニュアル記載事項の訂正

RMC (RouteMagic Controller) に添付された「取扱説明書 Version 2.0」の記載内容に以下の誤りがございましたので、お詫びして訂正させていただきます。

取扱説明書　31 ページ

- RMS (RouteMagic Server) に対する設定

  カレントポートを COM1 に変更する操作が記述されていませんでした。
  以下のように、監視対象装置のパスワード設定コマンドを実行する前に set port com1 を実行して下さい。

```
rmc@myrmc > enable
password :
[rmc@myrmc]# set port ml0
[rmc@myrmc(ml0)]# set mailto RMS@ routrek.co.jp
[rmc@myrmc(ml0)]# set errors-to RMS_err@routrek.co.jp
[rmc@myrmc(ml0)]# set spy com1 ml0
[rmc@myrmc(ml0)]# set port com1      ← カレントポートの指定を追加
[rmc@myrmc(com1)]# set target-login-password passwd1
[rmc@myrmc(com1)]# set target-enable-password passwd2
[rmc@myrmc(com1)]# set target-check
[rmc@myrmc(com1)]# set network-info-time h m
[rmc@myrmc(com1)]# set connect-log
[rmc@myrmc(com1)]# set spy rmc ml0
[rmc@myrmc(com1)]# set spy target1 ml0
[rmc@myrmc(com1)]# show running-config
[rmc@myrmc(com1)]# set mail-service
```

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。
下記ホームページをご参照ください。

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