RouteMagic

RouteMagic Server 2.2

ユーザーズ・ガイド

ーオペレータ編ー

ROUTREK NETWORKS

RMS-02-004　01/2003

はじめに

RouteMagic Server をお買い上げ頂き、ありがとうございます。
RouteMagic Server は、ネットワークの監視と問題解決の作業を支援するソフトウェアです。
本書が、RouteMagic Server を有効にご活用いただくための手助けとなれば幸いです。

本書の目的

本書は、次の目的で記述されています。

- RMC と RMS で構成されるシステムの基本機能をご理解いただくこと
- 主要な監視業務を行う手順と操作方法をご理解いただくこと

本書の対象読者

本書は、RMS をご利用になる方のうち、次の方を対象に記述されています。

- RMS を利用して、RMC に接続された監視対象装置とネットワークの監視およびメンテナンスに従事される方（オペレータ）

また、次の知識をお持ちであることを前提として記述されています。

- Windows を始めとする各種 OS の基本操作ができる
- ブラウザや携帯端末、携帯電話などを使用してインターネットにアクセスできる
- ネットワークの基本的な知識がある

関連ドキュメント

RMS 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 Server　ユーザーズ・ガイド　－管理者編－**
  RMS システム、及び RMS を利用するネットワーク管理システムの運用に責任を持つ方を対象として、RMS を利用する際に必要な初期設定と管理作業を記述しています。

- **RouteMagic Server　インストール・ガイド**
  Linux に関する基礎知識をお持ちの方を対象として、Linux サーバ上への RMS のインストールと初期設定作業に関して記述しています。旧バージョンの RMS からの移行に関しても本ドキュメントをご参照下さい。

- **RouteMagic Server　プラグイン・ユーザーズガイド**
  RMS プラグインの機能とインストール作業について記述しています。

- **RouteMagic Server　リリースノート**
  最新リリースにおいて追加／変更された機能および利用上の注意事項などを記述しています。

- **RouteMagic Server　メンテナンス・ガイド**
  RMS システムを導入されたユーザに必要な日常のメンテナンス作業を記述しています。

ご利用の前に

RouteMagic Server は、RMC から電子メールで送信されてくるデータを元に、監視対象装置の監視と管理を実行します。RMS は、RMC に接続して情報収集可能なすべての装置を監視対象とすることができますが、RMS 対応製品以外の装置を接続される場合は、各装置の仕様に合わせて RMS にあらかじめ組み込まれた機能をご利用いただくことはできません。

ここでは、RouteMagic Server をご利用になる前に、対応製品とその他の一般機器を接続される場合の留意点を示します。

RouteMagic Server の対応製品

RouteMagic Server は、Cisco 社製品　Y2K Compliance IOS 11.0 - 12.2、および Swich Software 2.1 - 6.3　搭載の製品に対応しています。これらの装置は、RMS 上で「ルータ」、「スイッチ」、「IOS スイッチ」として管理され、RMS のすべての機能が利用できます。
また、RMS 2.2 で新たに追加されたプラグインをインストールした場合は、プラグインの対応装置を RMS 対応製品として管理することができます。プラグイン利用時に提供される機能と操作に関しては、各装置の「プラグイン・ユーザーズガイド」をご参照ください。

上記以外の装置は、RMS では「一般機器」として管理されます。「一般機器」を監視対象装置として接続される場合は、次項の「一般機器」接続時の留意点 をお読みください。

「一般機器」使用時の留意点

「一般機器」を監視対象として RMS をご利用になる場合は、次の様な機能上の制約がありますのでご留意ください。

機能	留意点
解説メッセージ	「一般機器」から出力されるコンソールメッセージについて、RMS 上に事前に登録された解説メッセージはありません。 「ユーザ定義の解説データ」（オーナ管理者による登録、もしくはオペレータによるインシデントの対処履歴）機能をご利用いただくことは可能です。
インシデント発生条件、メール配信条件	メッセージの重要度に従ったインシデントの発生／配信条件の設定は、サポートされません。 インシデント発生条件の設定に関しては、「オーナ管理者編」をご覧ください。
ユーザ定義必須機能	「一般機器」の場合には、以下の機能に対するデフォルト設定の機能が用意されていません。「一般機器」を監視対象としてこれらの機能を利用する場合は、各装置を正しく動作させる為の動作シーケンスを RMC および RMS 上に定義して頂く必要があります。 ・監視対象装置、及びネットワーク情報の自動収集 ・定石コマンドの発行 ・監視対象装置の生存確認 ・インシデント発生時に実行するコマンド

機能	留意点
ヘルスチェック (装置／ルーティング設定情報の変更確認機能)	「一般機器」ではご利用になれません。
トポロジーマップの表示機能	「一般機器」の場合、各装置の IP アドレスを手動設定する必要があります。

本書の前提

本書は、RMS が Linux の稼動するサーバ上に既にインストールされており、各種システム要件に合わせた設定がなされていることを前提として記述されています。

RMS で管理される RMC の設定、および監視対象装置やネットワークとの接続に関しては、RMC の「取扱説明書」、「クイックリファレンス」を参照してください。

なお、本書はブラウザとして、Internet Explorer 5.0 を使用することを前提として記述されています。

目次

共通編

操作編

付録

共通編

――「障害監視」から「問題解決支援ソリューション」へ。

このコンセプトの元に開発された RouteMagic Server（以降、RMS と呼ぶ）は、RouteMagic Controller（以後 RMC と呼ぶ）によって監視対象装置のコンソールポートから収集された情報を使用して、ネットワークの監視と問題解決の作業を支援するソフトウェアです。

本編では、RMS がどのようなシステムで、どのような機能が提供されるかを紹介します。

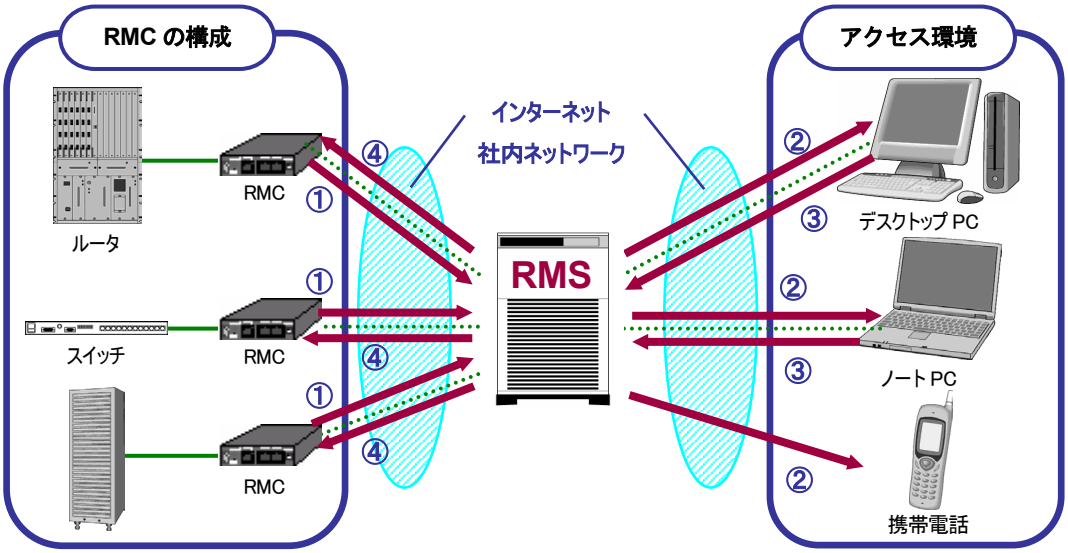
1. RouteMagic Server とは

はじめに、RMS のシステム構成と RMS を使ってどのようなことができるのかを紹介します。

1.1 RMS のシステム構成

RouteMagic は「問題解決支援」機能を提供する RMS と、ルータやスイッチ等のネットワーク機器（本書では「監視対象装置」と呼ばれます）のコンソールポートに接続して、機器情報の収集と遠隔操作機能を提供する RMC で構成されます。
RMS はネットワーク経由で RMC から情報を収集します。RMS の利用者は、インターネットや社内ネットワークを介して、Web インタフェースを利用して RMS にアクセスします。

RMC と RMS を利用するシステムの構成は、下図のようになります。各機器は矢印の方向に向かって、情報の受け渡しを行います。



① RMC からの情報収集と一元管理

RMC はネットワーク機器を常時監視し、機器から出力されるメッセージを取得します。このメッセージは、フィルタリングされ、必要なメッセージのみが接続先の RMS に送信されます。
RMS は、各 RMC から送信されてくるこれらの情報を、ログとして一元管理します。

② RMS から監視・メンテナンス担当者への情報

RMC から送信されてくる情報によって、ネットワーク上に問題が発生したことが検出された場合、RMS は監視・メンテナンス担当者に対して、電子メールでこの情報を通知します。
RMS へはインターネットを通じて接続できるため、担当者はどこにいてもこの通知を受け取り、WEB ブラウザを利用して RMS にアクセスし、トラブルに迅速に対処することができます。

③ 監視・メンテナンス担当者から RMS への情報

RMS の設定情報や定石コマンドの発行等、監視対象装置や RMC に対する操作要求を RMS へ送信します。

④ RMS から RMC・監視対象装置への情報

RMS から RMC・監視対象装置に対して、各装置の操作や情報収集を行うためのコマンドなどが送信されます。この情報は、③で監視・メンテナンス担当者から送信されてきた要求に基づく場合と、あらかじめ設定された定期的なコマンド発行要求による場合があります。

1.2 RMS の機能

これまで熟練技術者がこなしてきたネットワーク障害対応を、知識・経験の浅い技術者が代行して解決を図るにはどうすれば良いか。
技術者の作業効率を向上させ、より早く復旧する術はないのか。

――― その回答を結実させたものが RouteMagic Solution です。

ネットワークに発生した問題の解決には、第一に故障個所の速やかな特定と復旧が急務です。しかし、長期的なネットワークの安定運用には、根本的な原因の究明と解決を欠かすことはできません。RMS は、故障個所を迅速に発見して復旧への最短フローを提供するとともに、障害に対する詳細情報を確実にロギングすることによって、復旧を急ぐあまり疎かになりがちな根本的原因の究明と解決へのアプローチを支援します。RMS の主な機能は、以下のとおりです。

■ アカウント管理

RMS は、RMS を導入する組織と RMS システムの利用者ごとにアカウントを管理します。（RMS の管理する組織と利用者の種別 ➡「2. RouteMagic Server の導入イメージ」参照。）
このアカウント管理機能によって、管理組織単位の情報の機密性を保障するとともに、情報を必要とする各担当者への通知を行います。

■ 障害発生の通知

監視対象に何らかの問題が発生すると、RMC は暗号化された電子メールで障害発生を RMS に通知します。RMS はこのメールを即時に解析し、設定された条件に基づいて「インシデント」（問題）として登録すると同時に、通知の必要な管理者グループに「どこで（障害発生個所）」、「何が（障害状況）」発生したかの情報を電子メールで「同報送信」します。
この障害通知メールは、外出先でも携帯電話メールでも受け取りが可能なため、この時点で関係者全員が一斉にトラブルの発生とその内容を把握できます。

■ ネットワークトポロジーのグラフィカル表示

RMS では、監視対象とするネットワーク上の各装置とその動作状態をグラフィカルに表示します。（➡「操作編　3.2 トポロジーマップ」参照。）
障害を報告した監視対象装置は赤でブリンク表示されるため、メールにより障害の通知を受けた管理者やオペレータは一目でトラブルの状況を把握することができます。

■ 問題のトラッキング

RMS は、監視対象とする装置から出力されたコンソールメッセージや、装置が正常に応答しないといった情報を RMC から受信すると、これを「インシデント」と呼ばれる単位で管理し、解決までの履歴をトラッキングします。「インシデント」は、設定された条件に基づいて RMS が自動的に生成しますが、任意に分割・結合することが可能です。
オペレータは、必要に応じてインシデントの状態を変更したり、対処の履歴を記録することによって、管理グループ内でのトラブルに関する情報共有を円滑化し、作業効率を向上させることができます。また、問題の解決方法に関する履歴を残すことにより、同様の問題が再度発生した場合に、この情報を活用することも可能です。

■ 復旧作業の支援

RMS は、コンソールメッセージに対するガイダンスや過去の対応履歴情報の提供などにより、トラブルの正確な把握を支援します。また、インシデント発生時の自動的なコマンド発行や、ボタン操作でオペレータが簡単にコマンドを発行できる「定石コマンド」の機能などによって、障害を報告した装置の詳細情報を入手し、対応策の検討に役立てることができます。装置の交換が必要な場合、あるいは装置の設定を変更以前の状態に戻したい場合には、RMS が保存している監視対象装置の設定情報を利用していただけます。
RMC を経由すれば、SSH（Secure Shell）を使用したセキュアなリモートログイン機能によって機器の遠隔操作を行っていただくことも可能です。

■ 原因の究明と解決

RMS には、コンソールメッセージのみでなく、オペレータが監視対象装置に対して行った操作の記録や、各装置の設定情報などもロギングすることができます。したがって、暫定的な障害の復旧作業を完了した後でも、各種のログ情報を利用して根本的な原因の究明と解決を最小限の作業で迅速に行うことが可能です。

■ 日常業務の支援

RMS は、監視対象装置から定期的にルーティング情報を含む装置の設定情報を収集し、これを管理しています。こうした設定情報や各種のロギングデータは、トラブルの原因究明に利用するのみでなく、RMS からダウンロードして障害報告書や定期レポートの作成に役立てていただくことができます。

■ セキュリティ対応

RMC と RMS の間では、各装置の設定情報を始めとした機密性の高い情報がやり取りされます。このため、RMC－RMS 間の通信には、PGP や SSH による認証とメール電文の暗号化機能を提供しています。したがって、インターネットのようなオープンなネットワークを経由した情報転送も可能です。

2. RouteMagic Server の導入イメージ

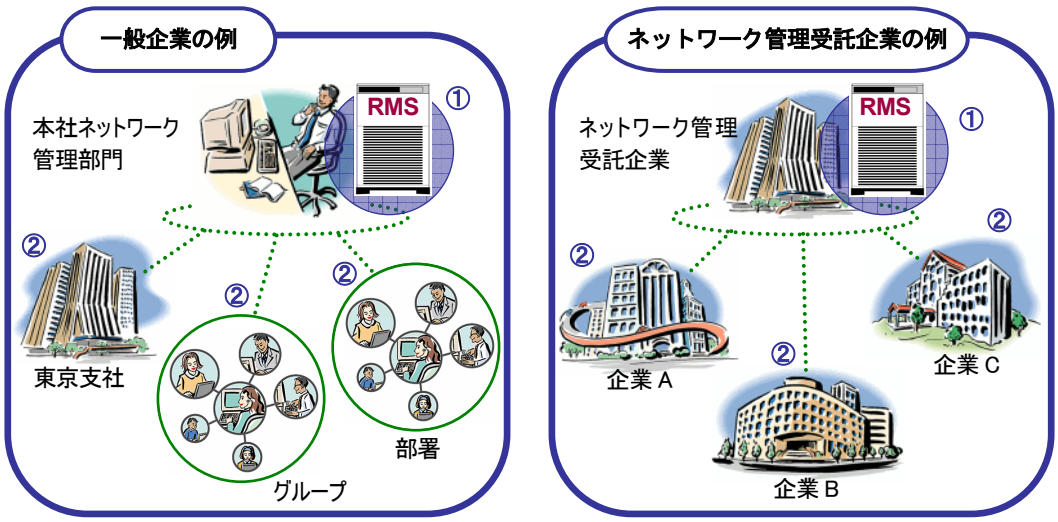
RMS は、自社内のネットワークを管理する企業のネットワーク管理部門や、ネットワークの管理サービスを提供する管理受託企業の管理センターで利用して頂けるようにデザインされています。以下に、RMS を導入したシステムの構成とその利用形態を簡単に紹介します。

2.1 RMS の設置と管理する組織の単位

RMS は、以下のネットワークを管理できます。

- **企業内の複数のネットワーク**
- **ネットワーク管理受託企業などで、複数の顧客企業に対して設置した、顧客企業ごとのネットワーク**

いずれの利用形態の場合も、ネットワーク管理を実施する部門が RMS の設置と管理に責任を持ち、各ユーザ部門、あるいはユーザ企業のネットワークをオーナと呼ばれる単位で監視・管理します。



① RMS の設置単位

一般の企業内の組織を管理する場合、当該企業のネットワーク管理部門に設置します。
ネットワーク管理受託企業で複数の顧客企業のネットワークを管理する場合、ネットワーク管理受託企業に設置します。

② RMS の組織単位

企業内に複数存在する組織のネットワークや、ネットワーク管理受託企業などが管理する複数の顧客企業のネットワークを、RMS では「オーナ」と呼びます。このオーナ単位で管理を行います。

具体的には、RMC を導入した 1 つの企業や組織がオーナとなります。
例えば、RMS が一般企業に導入されている場合は、企業内部の部署やグループ単位で 1 つのオーナになります。（例：東京支社）
また、RMS がネットワーク管理受託企業に設置されている場合は、当該企業が管理を受託している各顧客企業が、それぞれ 1 つのオーナになります。（例：企業 A、企業 B）

なお、RMS では複数のオーナを管理しますが、各オーナ間でのセキュリティは確保されています。

2.2 RMS の利用者区分

RMS では、それぞれの役割に従って、RMS の利用者を「RMS 管理者」「オーナ管理者」「オペレータ」の 3 種類に区分してアカウントを管理します。
ここでは、各利用者について説明します。

利用者の区分

■ RMS 管理者

1 つの RMS システム全体の設置・運用を管理する責任者です。
「オーナ管理者」が「オーナ」のネットワークを管理できるよう手配します。
1 つの RMS に対して 1 人の RMS 管理者を割り当てます。

➡「RouteMagic Server　ユーザーズ･ガイド　ー管理者編ー」参照

■ オーナ管理者

「オーナ」のネットワーク全体の管理と運用に責任者を持つ代表者です。
「オペレータ」が「オーナ」内のネットワークを監視できるよう手配します。
1 つのオーナに対して 1 人のオーナ管理者を割り当てます。

➡「RouteMagic Server　ユーザーズ･ガイド　ー管理者編ー」参照

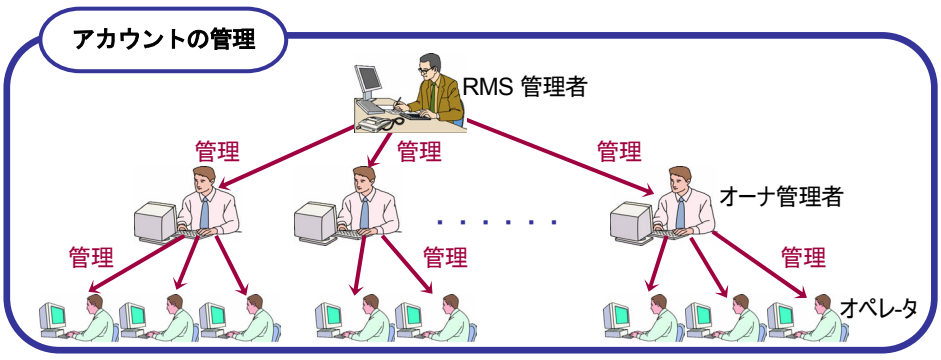
■ オペレータ

実際に、RMC の接続されている監視対象装置とネットワークを監視・メンテナンスし、問題解決作業に携わる担当者です。

➡「操作編」参照

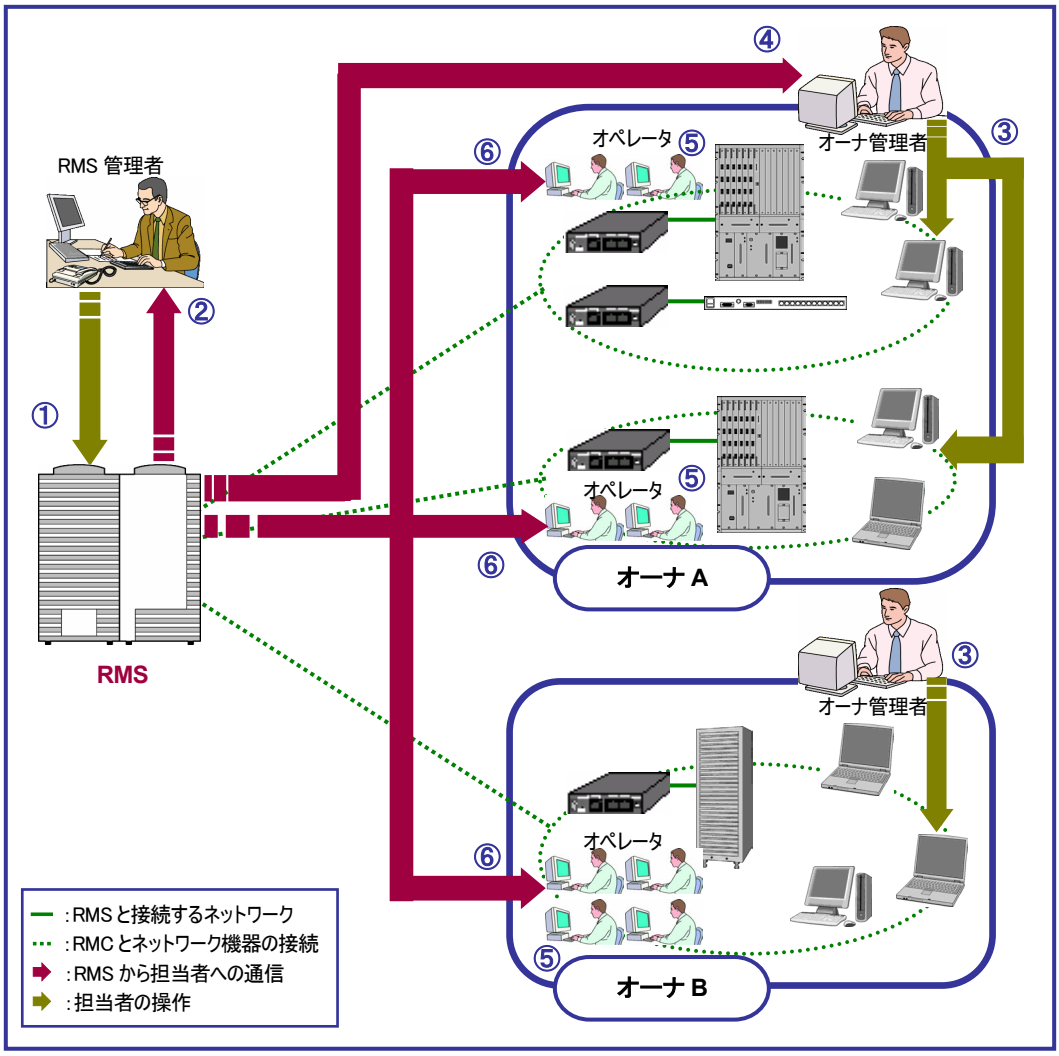
利用者の関係

RMS 管理者は、オーナのアカウントを管理し、オーナ管理者はオペレータのアカウントを管理します。



また、各管理者は、自分が管理するアカウントの機能を利用できます。
すなわち、RMS 管理者は RMS システムの全機能を、オーナ管理者はオーナ管理者とオペレータ用の機能を利用できます。

2.3 RMS の導入イメージ



① RMS 管理者は RMS 全体の設定を行います。

② RMS の設定に関わる通知は、インターネット・社内ネットワークを通して、RMS 管理者にメールで通知されます。

③ オーナ管理者はオーナ内のネットワークを管理するための設定を行います。

④ オーナの設定に関わる通知は、インターネット・社内ネットワークを介してオーナ管理者にメールで通知されます。

⑤ オペレータは自分に割り当てられたネットワークの監視対象装置を監視します。

⑥ エラーの発生や管理情報等、監視対象装置に関わる通知は、インターネット・社内ネットワークを通して、オペレータにメールで通知されます。

操作編

本編では、オペレータの行う操作について説明します。

1. オペレータの役割と作業

1.1 オペレータの役割

オペレータの主要な役割は、自分の担当する監視対象装置に発生した問題に対処し、復旧と解決の作業を行うことです。オペレータは、RMS にアクセスして問題解決にあたると同時に、その対応履歴をコメントとして記録します。履歴情報は、同様な問題が発生した場合の対応を円滑化する貴重な資料ですので、RMS が自動的収集することのできない作業の記録を正確に残すこともオペレータの重要な仕事です。

■ ネットワークと監視対象装置の状況確認

RMS は、監視対象装置に問題が発生すると、配信スケジュールに基づいて各オペレータにメールで通知します。担当する装置の障害通知メールを受け取った場合、オペレータは RMS にログインしてメール通知内の「インシデント番号」によってインシデント概要を参照し、障害に関するより詳細な状況と過去の対応履歴を確認することができます。
インシデントの発生要因は監視対象装置から出力されたコンソールメッセージですが、どのようなレベル、またはタイプのメッセージをインシデントとして処理するかの設定は、オーナ管理者の権限で設定します。

■ 問題の対処と復旧作業

RMS では、「インシデント」単位で解決すべき問題のトラッキングを行います。オペレータは、RMS が提供する解説メッセージや、各種のロギング情報、「定石コマンド」（簡易操作によるコマンド発行機能）などを利用してインシデントの解決に当たります。対応作業の状況に応じて、インシデントの状態変更や履歴情報としてのコメント入力を行ってください。

■ 原因の究明と解決

復旧作業が急務である場合、暫定的な復旧作業を完了した後に、RMS に蓄積された各種のログ情報を利用して根本原因の究明と解決を計ることができます。装置のハードウェア交換が必要となった場合でも、設定情報のダウンロード機能を利用して円滑に復旧作業を行うことができます。

■ 対処の記録と報告

インシデントが解決した時点で、当該インシデントのクローズ、すなわち、状態を「解決済み」として解決策などの情報をコメントとして記録する作業を行います。障害報告書や定期レポートの作成には、RMS のロギングデータをダウンロードして利用することも可能です。

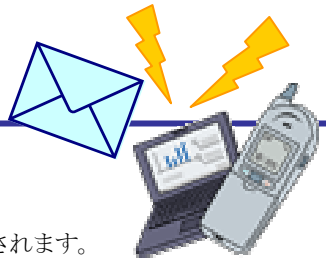
■ 監視対象装置の管理

定期メンテナンスや保守点検の為の停電など、監視対象装置の停止が予定されている場合は、RMS による監視を一時的に停止して不必要なインシデントの発生を防止できます。また、各装置の設定情報管理には、「ヘルスチェック」あるいは「レポート」の機能が利用できます。

1.2 オペレータの作業

ここでは、障害対応時に一般的に実行されるオペレータの作業に基づいて、RMS が提供する主要な機能を紹介します。

メールを受信する

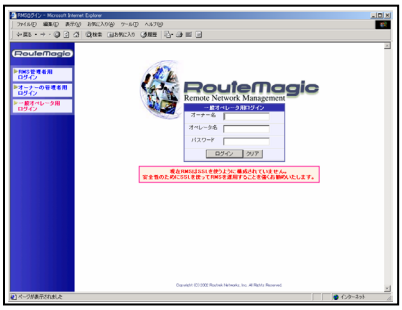


RMS から問題の発生を知らせるメールが届きます。

メール通知の条件は、「配信スケジュール」によって指定されます。

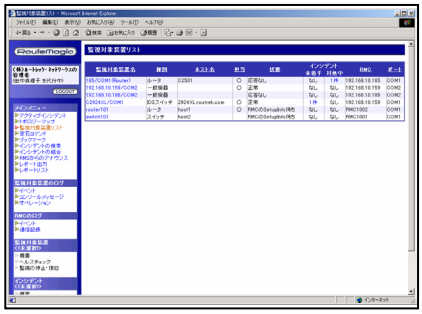
詳しくは➡「－オーナ管理者編－　6. 配信スケジュールの作成」

ログインする



Web ブラウザを使用して RMS にアクセスし、**オーナ名**と**オペレータ名**、**パスワード**を入力して、ログインします。

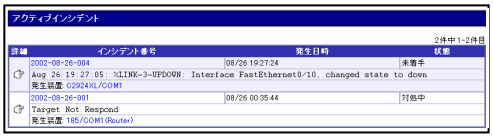
ネットワークの状態を確認する



ログインすると、「監視対象装置リスト」が表示されます。
この画面では監視対象装置が一覧表示され、各装置の現在の状態とインシデントの発生・対処状況が確認できます。

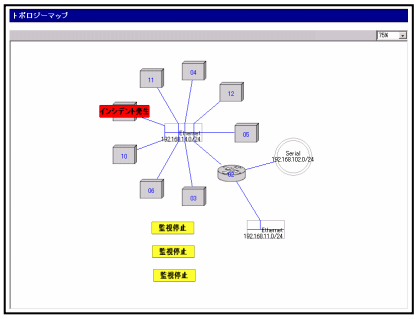
詳しくは➡「3.3 監視対象装置リスト」

対応の必要なインシデントを確認する場合は、
メインメニュー の アクティブインシデント をクリックします。ログインしたオペレータが担当する装置の未解決インシデントが一覧表示されます。

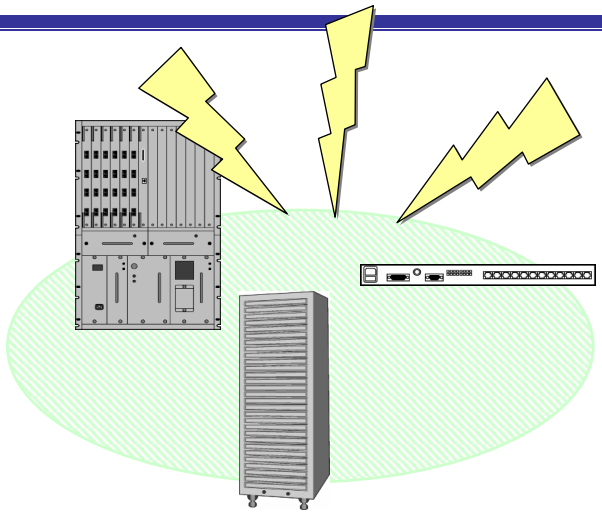


詳しくは➡「3.1 アクティブインシデント」

ネットワーク全体の状態を把握するには、メインメニュー の トポロジーマップ をクリックします。
装置のトポロジーを示すマップ上に、各装置の現在の動作状態が表示されます。



詳しくは➡「3.2 トポロジーマップ」



対処すべきトラブルの発生が確認されたら、
次のような機能を利用して原因の究明と
問題の解決にあたります。

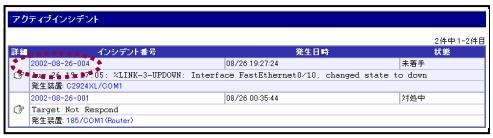
インシデントに対処する

トラブルの迅速な解決に向けて、RMS では障害に関する情報の収集や対処作業を支援するための各種の機能を提供します。

- **インシデント概要の参照**
- **装置情報の収集：**
  インシデント発生時のコマンド発行、設定情報の確認、装置へのコマンド発行
- **ログの参照**
- **インシデントの操作**

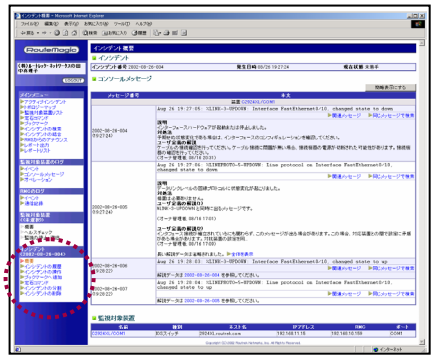
インシデント概要の参照

「インシデント概要」は、装置にどのような問題が発生したかを把握するためのメニューです。



「アクティブインシデント」のリストから、メールで通知された“インシデント番号”をクリックします。

「インシデント概要」が表示され、インシデント メニューのメニュー項目がアクティブになります。



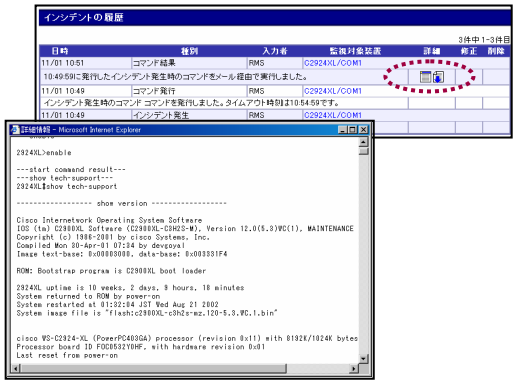
「インシデント概要」では、次のような情報を提供します。

- 装置から出力されたコンソールメッセージ
- メッセージの説明と推奨される対処法
- メッセージに対してユーザが定義した対処履歴や解説情報。

詳しくは➡「6.1 インシデント概要」

発生したインシデントと障害を起こした装置に関するより詳細な情報を収集するには、次のような機能を利用します。

インシデント発生時のコマンド発行



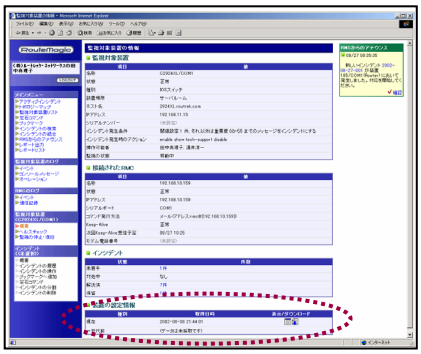
インシデントが発生すると、RMS は自動的にコマンドを発行して装置からの情報を収集します。

コマンドの実行結果は、 インシデント メニューの **インシデントの履歴** で表示またはダウンロードして確認します。

詳しくは➡「6.2 インシデントの履歴」

設定情報の確認

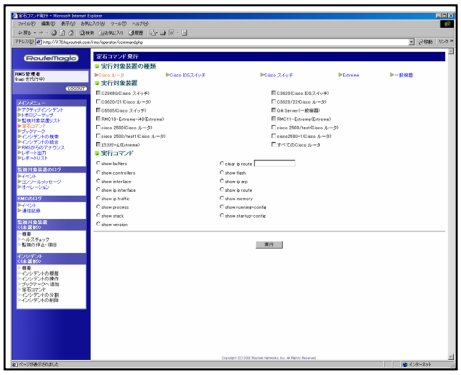
「インシデント概要」の 監視対象装置 **欄に表示された**装置名をクリックすると、「監視対象装置の情報」が表示されます。



装置の設定情報 欄の表示／ダウンロード アイコンをクリックすると、現在、あるいは一世代前の設定情報を表示、またはダウンロードすることができます。

詳しくは➡「5.1 監視対象装置の情報」

装置へのコマンド発行



装置状態の確認などで頻繁に使用されるコマンドは、ボタン操作で簡単に発行することができます。

メインメニュー または インシデント メニューの **定石コマンド** をクリックします。

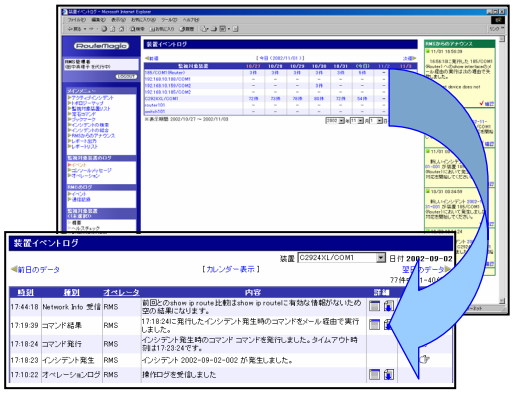
コマンドを発行する“装置の種類”、“装置名”、“コマンド名”を選択することにより、指定された装置にコマンドが発行されます。

コマンドの実行結果は、「装置イベントログ」に保存されます。

詳しくは➡「6.5 定石コマンドの発行」

各種ログの参照

RMS には、コンソールメッセージのみでなく、装置自身や装置に対して実行された操作に関する詳細なログ情報が蓄積されています。

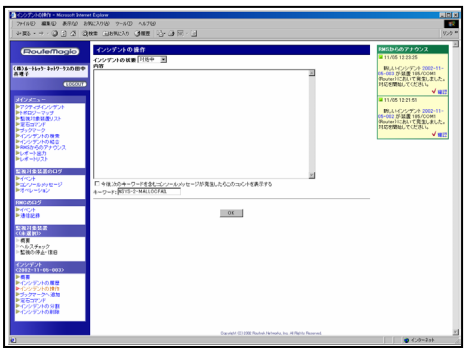


装置関連のログは 監視対象装置のログ メニューでログの種類と参照日付を選択することによって、参照します。

詳しくは➡「4. ログの参照」

インシデントの操作

インシデントの対処の過程では、随時、インシデント状態変更や対処履歴の記録を行うことができます。以後のトラブル対応を、より迅速に行うために有効に利用してください。



インシデント メニューの インシデントの操作 をクリックします。
コメントを入力します。

キーワードの設定により、入力したコメントを、今後同様のインシデントが発生した場合に自動表示させることも可能です。

詳しくは➡「6.3 インシデントの操作」

メニュー項目と機能概要

以下にオペレータに提供されるメニューと各メニューの機能概要を紹介します。各メニューの利用に関する詳細は、参照先ページをご覧下さい。

■ メインメニュー

日常の監視・管理業務で使用される主要な機能は、メインメニューで提供されます。

メニュー項目	説明	参照先
アクティブインシデント	対処の完了していないインシデントが一覧表示されます。このリストには、ログインしたオペレータの担当する装置に関連したインシデントのみが表示されます。	3.1 アクティブインシデント
トポロジーマップ	RMS の管理対象となっている装置のトポロジー情報と各装置の状態がグラフィカルに表示されます。ネットワーク全体の状態の確認に利用します。	3.2 トポロジーマップ
監視対象装置リスト	ログイン直後に表示されるメニュー画面です。RMS で管理されているすべての監視対象装置の状態とインシデントの対応状況が一覧表示されます。	3.3 監視対象装置リスト
定石コマンド	予め登録されたコマンドをボタン操作で発行します。RMS 対応製品では、デフォルトのコマンドが用意されていますが、任意に追加登録可能です。	3.4 定石コマンドの発行
ブックマーク	ブックマークの付いたインシデントを一覧表示します。頻繁に参照するインシデントにブックマークを付けておくと、このメニューから簡単に「インシデント概要」が表示できます。	3.5 ブックマーク
インシデントの検索	条件を指定して、条件にマッチするインシデントを検索します。検索条件としては、“インシデント番号”、“キーワード”、“監視対象装置名”、“インシデントの状態”、“発生日付／期間”が指定できます。	3.6 インシデントの検索
インシデントの結合	複数のインシデントを 1 個のインシデントに結合します。インシデントは、設定に基づいて RMS が自動的に生成しますが、必要に応じて結合または分割して管理することができます。	3.7 インシデントの結合
RMS からのアナウンス	オペレータの対処が必要な事象が発生すると、RMS はアナウンスを表示して作業を促します。このメニューでは、これまでに発生したすべてのアナウンスを一覧表示することができます。	3.8 RMS からのアナウンス
レポート出力	各種のログを、レポート情報として CSV または XML 形式のファイルに出力します。	3.9 レポートの出力とダウンロード 付録 3. レポート出力ファイル仕様
レポートリスト	出力されたレポートファイルをダウンロードします。	

■ 監視対象装置のログ

装置から出力されたコンソールメッセージをはじめとして、監視対象装置に関する情報として蓄積されたログを参照するためのメニューです。

メニュー項目	説明	参照先
イベント	インシデントの発生とそれに伴うコマンドの発行、装置からの定期的情報収集の結果など、装置の動作状態の確認に必要な情報がロギングされています。	4.1 参照するログの指定 4.2 装置イベントログ
コンソールメッセージ	装置から発生したコンソールメッセージがロギングされます。 インシデント発生や、メール通知の対象にならないメッセージもすべてこのログに記録されます。	4.1 参照するログの指定 4.3 コンソールメッセージログ
オペレーション	RMC を経由して実行した装置に対する操作が記録されます。過去に実行した操作の確認や、問題解決後のレポート作成などに利用します。	4.1 参照するログの指定 4.4 オペレーションログ

■ RMC のログ

RMC の動作に関連するログの参照に使用します。主に、RMC / RMS のメンテナンスや RMC－RMS 間の通信状態の確認に利用されるメニューです。

メニュー項目	説明	参照先
イベント	RMC の動作状態や、RMC－RMS 間の通信において発生した事象のログが記録されます。RMC の状態や装置の登録情報を参照する場合に利用します。	4.1 参照するログの指定 4.5 RMC イベントログ
通信記録	RMC－RMS 間で送受信されたすべての通信が記録されます。主に RMS のサポート目的で利用されます。	4.1 参照するログの指定 4.6 通信記録

■ 監視対象装置

監視対象装置ごとの詳細情報の確認や装置のメンテナンスの際に使用されるメニューです。このメニューは、操作対象とする装置が指定された時点でアクティブになります。

メニュー項目	説明	参照先
概要	監視対象装置の状態と設定情報、接続されている RMC に関する情報が表示されます。	5.1 監視対象装置の情報
ヘルスチェック	装置の設定情報とルーティングテーブルに関する変更履歴が参照できます。	5.2 ヘルスチェック
監視の停止・復旧	定期メンテナンスなど、装置の停止が予め予定されている場合に、監視の停止と復旧予定を設定します。	5.3 監視の停止と復旧

■ インシデント

インシデントに関連する操作の実行に利用するメニューです。このメニューを利用して実行したインシデントや装置に対する操作は、インシデント履歴にロギングされます。
このメニューは、操作対象とするインシデントが指定された時点でアクティブになります。

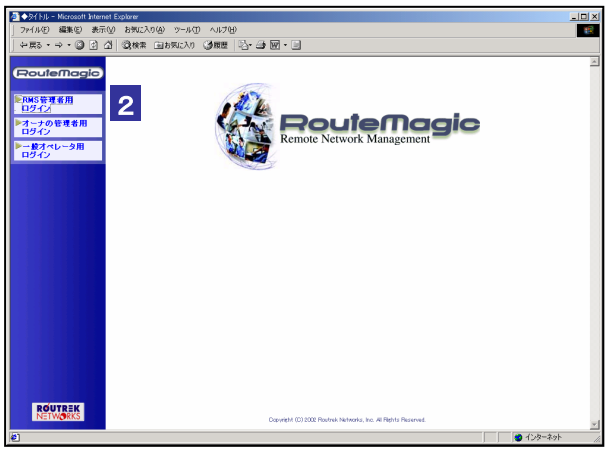
メニュー項目	説明	参照先
概要	インシデントに含まれるメッセージとその説明、過去の対処履歴から得られた情報など、発生した問題に関する概要が把握できます。	6.1 インシデント概要
インシデントの履歴	RMS が自動的に実行した動作も含め、インシデントの発生から解決までに行われた操作の履歴が参照できます。	6.2 インシデントの履歴
インシデントの操作	インシデントの状態変更やコメント入力により、インシデントに関する対処履歴を記録するためのメニューです。	6.3 インシデントの操作
ブックマークへ追加	頻繁に参照するインシデントにブックマークを付加して、簡単にアクセスできるようにします。	6.4 ブックマークへ追加
定石コマンド	インシデントが発生した監視対象装置に対して、予め登録されたコマンドをボタン操作で発行します。RMS 対応製品では、デフォルトのコマンドが用意されていますが、任意に追加登録可能です。	6.5 定石コマンドの発行
インシデントの分割	複数のコンソールメッセージで構成されたインシデントを任意の単位に分割します。	6.6 インシデントの分割
インシデントの削除	対処の必要がないと判断されたインシデントを削除します。	6.7 インシデントの削除

2. 基本操作

2.1 RMS へのログイン

RMS にログインするには、まず RMS システムの初期設定者（インストールと初期設定の担当者）から通知された URL（例：http://(RMS サーバ名)/rms/ ）を使用して RMS に接続します。

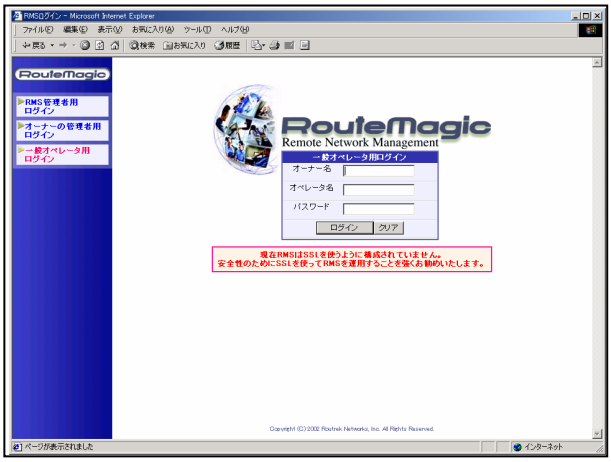
1 ブラウザを起動して、RMS に接続すると下記のイニシャル画面が表示されます。



RMS は、Internet Explorer 5.0 以上、Netscape 6.0 以上の Web ブラウザに対応しています。

1 台の PC 上で、複数のアカウントによる同時ログインは行わないで下さい。

2 一般オペレータ用ログイン をクリックして、オペレータ用ログイン画面を表示します。

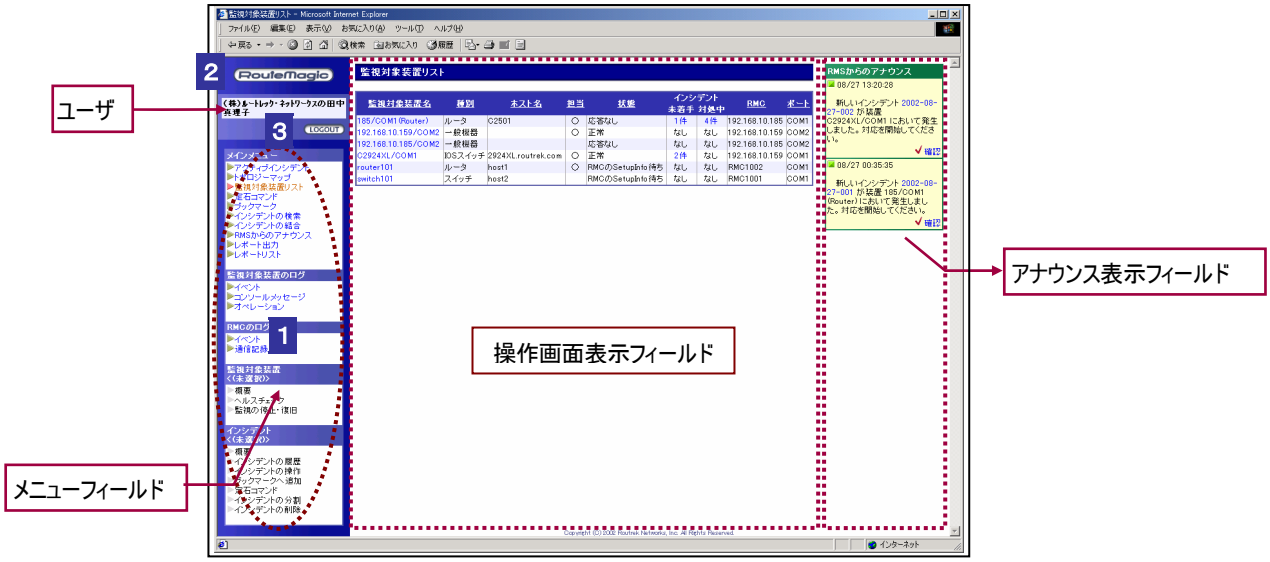


3 オーナ名、オペレータのアカウント名およびパスワードを入力し、 ログイン をクリックします。

オペレータのメインメニューと「監視対象装置リスト」が表示されます。
オペレータアカウント情報は、オーナ管理者が管理します。アカウントの設定が行われていない場合は、オーナ管理者にアカウント登録を依頼してください。

2.2 基本操作

オペレータとしてログインすると、「監視対象装置リスト」が選択された状態で、オペレータ用画面が表示されます。各メニュー項目の操作については、次章以降を参照してください。



メニューフィールド	オペレータ用の操作メニューが表示される
操作画面表示フィールド	メニューに対応する操作画面が表示される
アナウンス表示フィールド	最新の RMS からのアナウンス（オペレータの作業や確認を促す通知）が最大 5 件まで、表示される ※一部の画面では、アナウンスが存在してもこのフィールドは表示されません。
ユーザ	ログインしたユーザ名（初期設定時に登録したオーナ名とオペレータの名）が表示される

1 作業項目の選択は、メニューフィールドの ▶メニュー項目 のクリックによって行います。

メニューの色表示が ▶ メニュー項目 に変わり、操作画面表示フィールドに、選択したメニューに対応した画面が表示されます。メニュー項目と表示画面については、➡「付録 1 メニューと画面構成」をご覧ください。

2 RouteMagic をクリックすると、ログイン直後の画面（監視対象装置リスト）に戻ります。

「トポロジーマップ」が操作画面フィールドに表示されます。

3 RMS を終了（ログアウト）する場合は、 LOGOUT をクリックします。

> ログインしたまま何も操作せずに一定時間が経過すると、自動的にセッションがクローズされます。操作を継続するには再度ログインしてください。

3. メインメニュー

「メインメニュー」は、特定のインシデントや監視対象装置に依存しない作業に対する操作性を提供します。メインメニューには、次の機能が用意されています。

■ **インシデント対処作業のサポート**

トポロジーマップや対処の完了していないインシデントの一覧表示、過去に発生したインシデントの検索など、トラブルへの対処を円滑に行うための機能を提供します。

■ **監視対象装置の操作**

インシデントへの対処作業とは独立して、監視対象装置の状態や確認や定石コマンドの発行を行うことができます。

■ **日常業務の支援**

各種ログのダウンロード機能により、トラブル対応や日常の監視作業に対する報告業務をサポートします。

利用メニュー

「メインメニュー」では、以下のメニュー項目が選択できます。

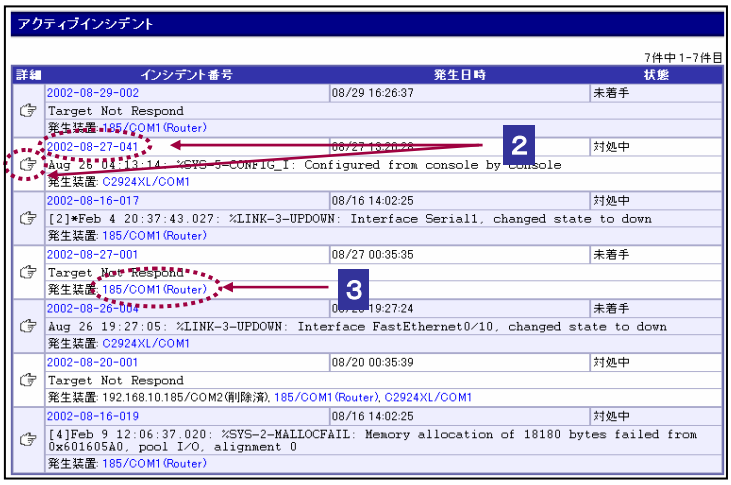
メニュー項目	説明	参照先
アクティブインシデント	未解決のインシデントを一覧表示することによって、対処の必要なインシデントを確認し、操作対象のインシデントを選択する。	3.1
トポロジーマップ	トポロジーマップ上に装置とネットワークの状態を表示する。	3.2
監視対象装置リスト	監視対象装置の一覧表示によって装置の状態を確認し、操作対象とする監視対象装置の選択を行う。	3.3
定石コマンド	監視対象装置に対してコマンドを発行する。	3.4
ブックマーク	インシデントへのブックマークを一覧表示し、編集する。	3.5
インシデントの検索	条件を指定してインシデントを検索する。	3.6
インシデントの結合	複数のインシデントを 1 つに結合する。	3.7
RMS からのアナウンス	RMS からオペレータ宛に通知されたアナウンスを表示する。	3.8
レポート出力	レポート作成用にログデータのファイル出力を要求する。	3.9
レポートリスト	ファイルに出力されたログデータをダウンロードする。	3.9

3.1 アクティブインシデント

アクティブインシデントとは状態が“未着手”または“対処中”のインシデントを指します。この画面には、ログインしたオペレータが担当する装置に発生したインシデントのみが表示されるため、自身で対処しなければならないインシデントを一目で確認できます。

1 メインメニュー ▶アクティブインシデント をクリックします。

未解決のインシデントを示す、「アクティブインシデント」のリストが表示されます。
1インシデントに複数のコンソールメッセージが含まれる場合、この画面では最初に発生したメッセージのみが表示されます。

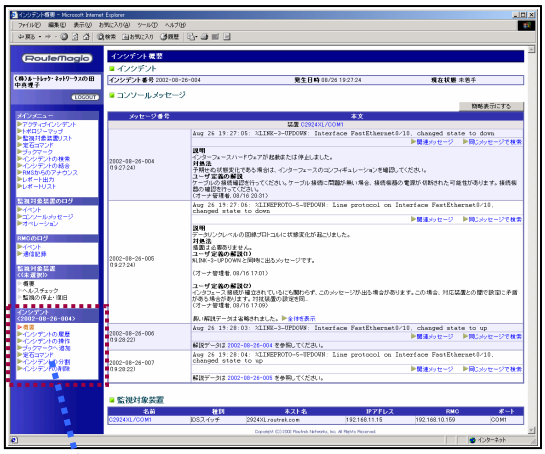


インシデント番号	RMS が自動的に付与するインシデントの識別番号<年/月/日－通し番号※> ※通し番号：同じ日付で 1 つのオーナ内に発生した順に付与される番号
状態	インシデントの状態（オペレータにより設定される） 「未着手」（発生直後）、「対処中」のいずれかが表示される
発生装置	インシデントの発生要因となった装置の名称を表示 ※（削除済）は、当該インシデントは、その監視対象装置からのメッセージを含んでいるが、装置自身は既に削除されていることを示す。 削除済み装置に関する装置情報は表示できない。

監視対象装置の削除を行った場合、削除された装置からのメッセージのみで構成さるインシデントは、状態が“未着手”または“対処中”であってもアクティブインシデントのリストには表示されません。

2 特定のインシデントに関する情報を参照する場合は、インシデントの  あるいは インシデント番号 をクリックします。

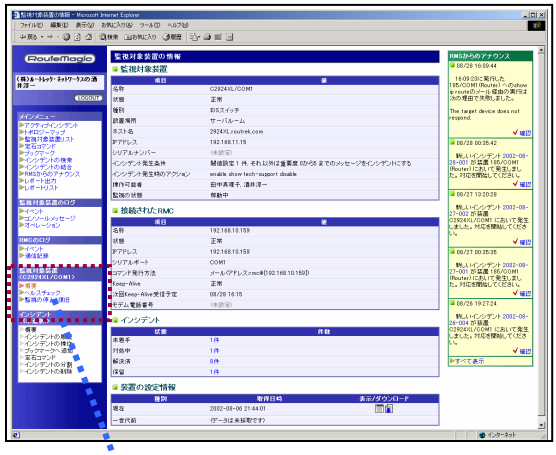
「インシデント概要」が表示され インシデント のメニュー項目がアクティブになります。



➡「6. インシデント」へ

3 **監視対象装置の詳細情報を参照する場合は、対応するインシデントの発生装置に表示された監視対象装置名 をクリックします。**

「監視対象装置の情報」が表示され、監視対象装置 のメニュー項目がアクティブになります。



➡「5. 監視対象装置」へ

監視対象装置の情報に関する詳細は、「5.1 監視対象装置の情報」をご覧ください。

➡ 次の操作

- 選択したインシデントに対処する ➡「6. インシデント」参照
- 選択した監視対象装置に関する操作を行う ➡「5. 監視対象装置」参照

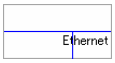
3.2 トポロジーマップ

トポロジーマップは、監視対象装置のシステム構成図を表したものです。監視対象装置に異常が検出されるとトポロジーマップの装置上に異常発生を示す表示が行われ、オペレータにネットワークの状態を解り易く通知します。

トポロジーマップの表示記号

トポロジーマップでは、次の記号を使ってネットワークや監視対象装置を表します。

図	説明
	監視対象装置 ルータ
	監視対象装置 IOS スイッチ、スイッチ
	監視対象装置 一般機器

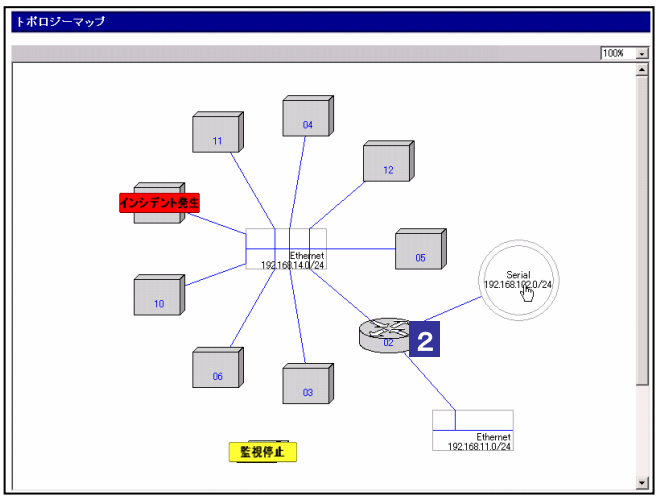
図	説明
	ネットワーク接続（ローカル）
	ネットワーク接続（その他）
	ネットワーク及びが接続している状態

また、装置の異常等を検知した場合、該当する監視対象装置の図に次の表示が点滅します。

応答なし	監視対象装置の生存確認において、装置から応答がない場合に表示される
インシデント発生	監視対象装置に新しいインシデントが発生した場合や未着手のインシデントが存在する場合に表示される
インシデント対処中	監視対象装置に対処中のインシデントが存在する場合に表示される
RMC KA切断	監視対象装置に接続されている RMC 自身、または RMC と RMS 間の通信に異常がある場合に表示される
監視停止	定期点検などにより、装置の監視が一時的に停止されていることを示す

1 メインメニュー ▶トポロジーマップ をクリックします。

監視対象装置の最新の状況が「トポロジーマップ」に表示されます。



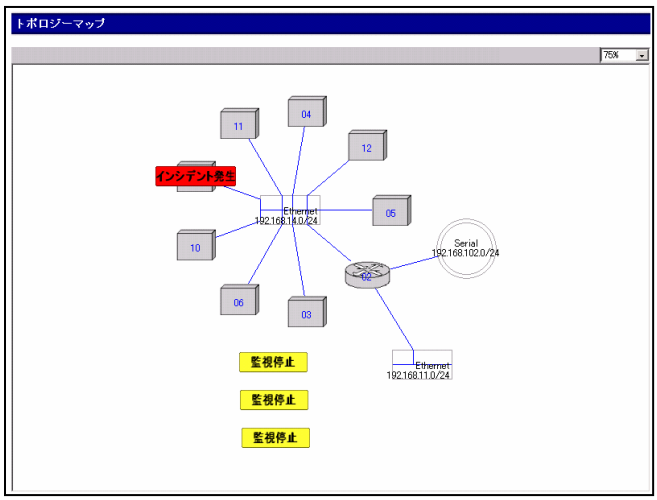
2 監視対象装置名 をダブルクリックすると、当該監視対象装置の情報が参照できます。

「監視対象装置の情報」が表示され、監視対象装置 のメニュー項目がアクティブになります。詳細は、➡「5.1 監視対象装置の情報」参照。

トポロジーマップ表示の編集や、監視対象装置情報の取得による再構築の要求は、オーナ管理者の権限で行います。

3 表示の拡大・縮小を行う場合は、 100% をクリックします。

装置台数が多くマップ全体が画面表示できない場合などに使用します。拡大／縮小は、25%、50%、75%、100%、125%、150%が指定可能です。



➡ 次の操作

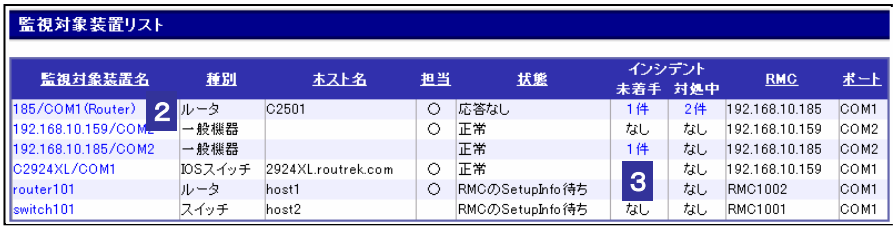
- 発生したインシデントに対処する ➡「6. インシデント」参照
- ログを確認する ➡「4. ログの参照」参照
- 選択した監視対象装置に関する操作を行う ➡「5. 監視対象装置」参照

3.3 監視対象装置リスト

「監視対象装置リスト」は、オペレータがログインした際に、最初に表示される画面です。この画面では、オーナの管理する監視対象装置が一覧表示され、各装置の現在の状態とインシデントの対処状況、接続されている RMC の情報を一目で確認することができます。

1 メインメニュー ▶監視対象装置リスト をクリックします。

監視対象装置リストは装置名順に表示されますが、下線表示のある項目名（例：種別 ）をクリックすると、当該項目をキーとして表示内容をソートすることが可能です。



担当	ログインしたオペレータの担当する装置を ○ で表示
状態	監視対象装置の現在の状態を表示 （”RMC の SetupInfo 待ち”は、当該装置に接続されている RMC からの初期設定メールを受信していないことを示す。この状態では、装置の監視は開始されない。）
インシデント	各装置に対する未解決のインシデント数を表示
RMC	監視対象装置が接続される RMC の名称（デフォルト名は IP アドレス）
ポート	監視対象装置が接続される RMC のポートを表示（COM1~ COM12）

RMS では、監視対象装置ごとに管理担当者の権限が設定されています。インシデントの操作や、定石コマンド発行のような機器に対する操作は、”担当”する監視対象装置に対してのみ実行することができます。担当オペレータの設定は、オーナ管理者の権限で行います。

2 特定の装置の情報を参照する場合は、 監視対象装置名 をクリックします。

「監視対象装置の情報」が表示され、監視対象装置 のメニュー項目がアクティブになります。監視対象装置の情報に関する詳細は、➡「5.1 監視対象装置の情報」をご覧ください。

3 未解決のインシデントがある場合は、インシデント欄に表示された 件数 をクリックします。

選択した”監視対象装置”と”状態”をキーとした検索が実行され、「インシデントの検索」画面の 検索結果に 件数 で表示されていたインシデントが一覧表示されます。

➡ 次の操作……

- 選択した監視対象装置に関する操作を行う ➡「5. 監視対象装置」参照
- 選択したインシデントに対処する ➡「3.6 インシデントの検索」参照
  ➡「6. インシデント」参照

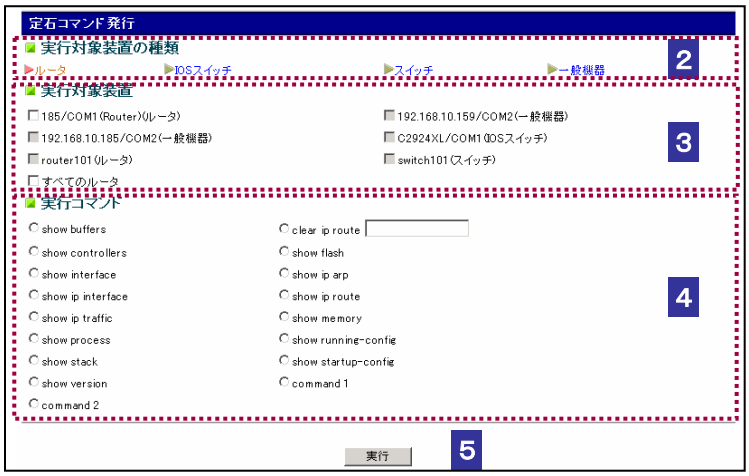
3.4 定石コマンドの発行

RMS では、監視対象装置の監視やメンテナンスにおいて頻繁に使用されるコマンドを「定石コマンド」として登録し、簡単な操作で実行できるようにしています。RMS 対応製品に関しては、一連のコマンドがデフォルトの定石コマンドとして登録されています。その他の製品（一般機器）に対応した定石コマンドの新規登録、あるいは RMS 対応製品への追加コマンドの登録は、オーナ管理者が行います。 ➡「－オーナ管理者編－ 10.2 定石コマンドメニューの登録」参照

ここでは、インシデントに関係なく、監視対象装置に対して定石コマンドを発行する操作について説明します。

1 メインメニュー ▶ 定石コマンド をクリックします。

「定石コマンド発行」が表示されます。



2 実行対象装置の種類 の ▶ 装置の種類 をクリックして、コマンドを発行する監視対象装置の種類を選択します。

実行対象装置には、オーナ内のすべての監視対象装置が表示されます。装置の種類をクリックすると、選択した種類の装置で、操作者が担当オペレータになっている装置のチェックボックスのみが有効になります。

実行コマンド には、選択した種類の装置に対して発行できるコマンドが表示されます。

3 実行対象装置 のチェックボックス（ ☐ ）をクリックして、コマンドを発行する装置を選択します。（複数選択可）

担当オペレータではない装置のチェックボックスを選択することはできません。

4 実行コマンド のラジオボタン（ ○ ）をクリックします。（単一選択）

「clear ip route」、「two parameters」コマンドには、引数が必要です。
デフォルトの値は「*」で、すべてのネットワークインタフェースが対象になります。
特定のネットワークインタフェースに対してのみコマンドを実行する場合は、各コマンドのテキストボックスに適切な引数を入力します。

5 実行 をクリックします。

RMC に対してコマンドの発行要求が送信されます。コマンド発行要求が完了すると、実行ボタンの下に、次のメッセージが表示されます。

コマンドを発行しました。結果が返信されるとイベントログへ記録されます。

コマンドの実行結果は、監視対象装置のイベントログに記録されます。コマンド発行による監視対象装置からの出力、何らかのエラーによりコマンド発行が正常に行われなかった場合のエラー原因などは、すべて装置イベントログに記録されますので、結果を確認してください。

RMS－RMC 間のメール到達性、あるいはネットワーク管理上のポリシーなどにより、”RMS からのコマンド発行を行わない”設定とすることが可能です。この設定を行っている場合、「監視対象装置の情報」 接続された RMC のコマンド発行方法に ”コマンドは発行しない”と表示され、定石コマンドの発行を要求した場合は、装置イベントログにエラーが記録されます。

この指定は、オーナ管理者が RMC ごとに設定する情報ですので、設定内容に関してはオーナ管理者に確認してください。

➡ 関連操作

- 監視対象装置のイベントログを参照する ➡「4.2 装置イベントログ」参照
- インシデントが発生した監視対象装置に対してコマンドを発行する ➡「6.5 定石コマンドの発行」参照

定石コマンドを発行可能な環境

コマンドの発行は、メールまたは SSH を利用して行われるため、RMS から RMC へメールが到達できる環境が必要です。
例えば、ファイアウォールの内側に RMC が、外側に RMS があるような場合は、メールや SSH の要求がこれを通過できるように設定する必要があります。

なお、コマンドの種類によっては、発行後、結果の受信が完了するまでに数秒～数分の時間が掛かる場合があります。 また、あらかじめ鍵がセットアップされている場合に限り、RMC と RMS 間のメール送受信に、PGP を使って署名と暗号化が行われます。これによって、第三者によるコマンドの実行や、結果の盗聴を防止することができます。

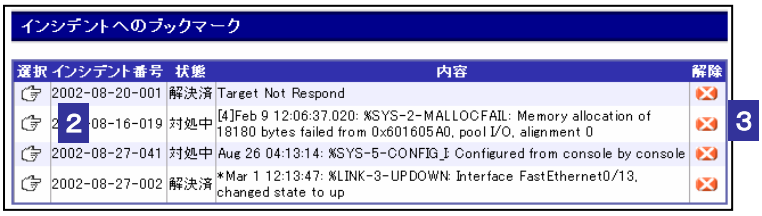
3.5 ブックマーク

「ブックマーク」は、頻繁に参照するインシデントを簡単に表示するための機能です。

ここでは、あらかじめブックマークを付与したインシデントの参照操作について説明します。
ブックマークを付与する操作については、➡「6.4 ブックマークへ追加」をご覧ください。

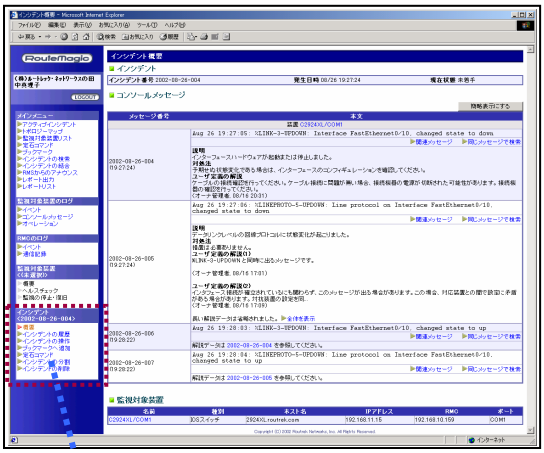
1 メインメニュー ▶ブックマーク をクリックします。

「インシデントへのブックマーク」にブックマークが付与されているインシデントが、一覧表示されます。



2 インシデントに対処、あるいはインシデントを参照する場合は、  をクリックします。

「インシデント概要」が表示され、インシデント のメニュー項目がアクティブになります。



➡「6. インシデント」へ

3 ブックマークを削除する場合は、削除するブックマークの をクリックします。

➡ **次の操作**

- 選択したインシデントに関する操作を行う ➡「6.1 インシデント概要」参照

➡ **関連操作**

- ブックマークを付与する ➡「6.4 ブックマークへ追加」参照

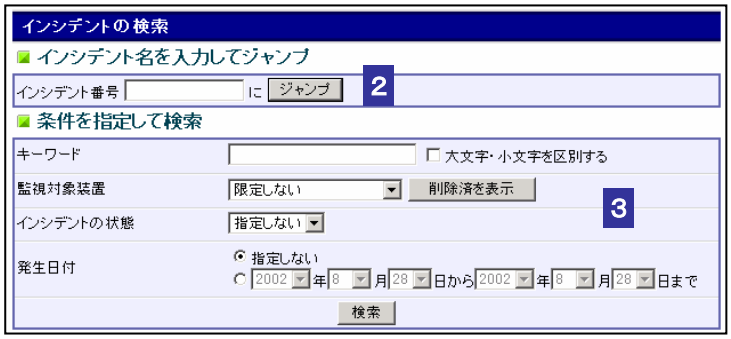
3.6 インシデントの検索

インシデント番号やキーワード等の条件を指定して、目的のインシデントを検索します。

> 監視対象装置を削除した場合、コンソールメッセージなどのログは自動的に削除されますが、関連するインシデントが自動削除されることはありません。

1 メインメニュー ▶インシデントの検索 をクリックします。

「インシデントの検索」が表示されます。



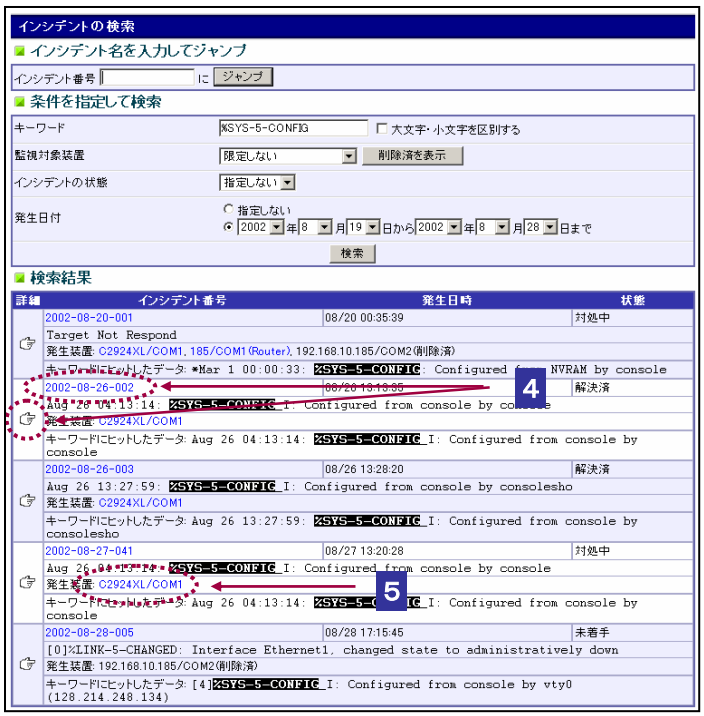
インシデント番号	インシデント番号<年/月/日ー通し番号>を指定して検索する
キーワード	コンソールメッセージに含まれるキーワードで検索する
監視対象装置	特定の監視対象装置に発生したインシデントを検索する 削除済を非表示　削除済みの装置は装置選択メニューに表示しない 削除済を表示　削除された装置も選択選択メニューに表示する（既に削除された装置に関連する履歴情報を検索したい場合に利用します）
インシデントの状態	インシデントの状態（「未着手」「対処中」「解決済」「保留」）を指定して検索する

2 特定のインシデントを検索する場合は、インシデント番号を入力して ジャンプ をクリックします。

指定した番号のインシデントが「インシデント概要」画面に表示され、インシデント のメニュー項目がアクティブになります。 ➡「6.1 インシデント概要」参照

3 条件検索を行う場合は、条件を入力または選択した後、検索 をクリックします。

検索条件に一致するインシデントが、条件設定の下に 検索結果 として一覧表示されます。検索結果の操作は「アクティブインシデント」の操作と同様ですが、インシデント検索の表示結果には、削除済み装置からのメッセージのみで構成されるインシデントも表示されます。 （➡「3.1 アクティブインシデント」参照）



4 参照するインシデントの  あるいは インシデント番号 をクリックします。

「インシデント概要」が表示され インシデント のメニュー項目がアクティブになります。インシデントの対処については、➡「6.1 インシデント概要」参照

5 監視対象装置の詳細情報を参照する場合は、対応するインシデントの発生装置に表示された 監視対象装置名 をクリックします。

「監視対象装置の情報」が表示され、監視対象装置 のメニュー項目がアクティブになります。監視対象装置の情報に関する詳細は、➡「5.1　監視対象装置の情報」参照

既に削除されている装置に関する「監視対象装置の情報」を参照することはできません。

➡ 次の操作

- 選択したインシデントに対処する　➡「6. インシデント」参照
- 選択した監視対象装置に関する操作を行う　➡「5. 監視対象装置」参照

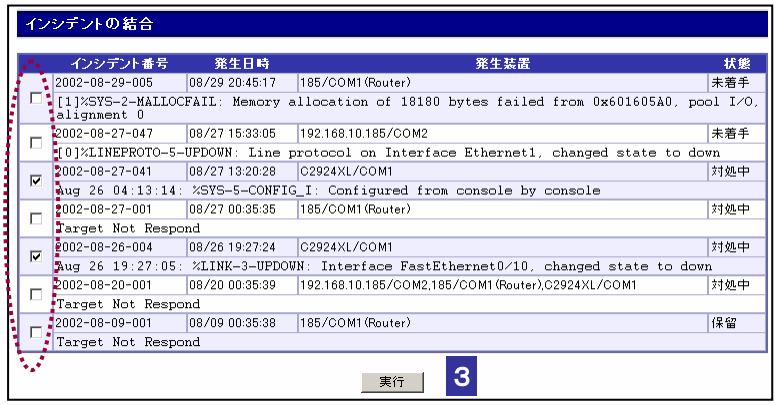
3.7 インシデントの結合

インシデントは、対処作業や管理上の必要性に応じて任意に結合／分割して操作することができます。例えば、一台の監視対象装置で違う時間帯に発生したインシデントを、1 つのインシデントとして扱いたい場合はインシデントの結合操作を行います。

ここでは、複数のインシデントを 1 つに結合する操作について説明します。インシデントの分割については、「6.6 インシデントの分割」を参照してください。

1 メインメニュー ▶インシデントの結合 をクリックします。

「インシデントの結合」に “未着手”、“対処中”、および “保留” 状態のインシデントが「表示されます。状態が “解決済み” のインシデントを結合することはできません。

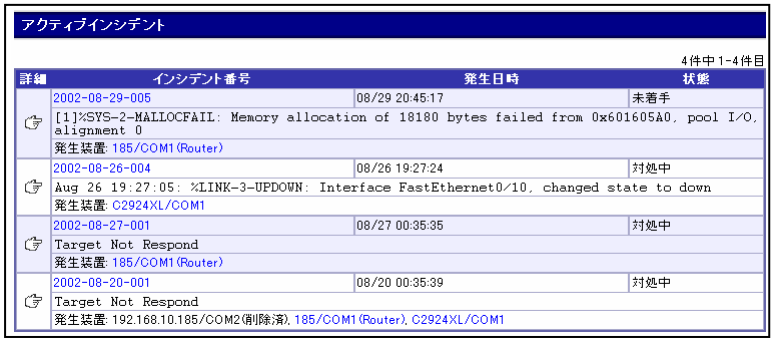


2 結合するインシデントのチェックボックス（ ☐ ）をチェックします。（複数選択可）

1 インシデントに含まれる最大コンソールメッセージ数を超えたインシデントを作成することはできません。デフォルトの最大メッセージ数は 100 ですが、この値はオーナ管理者がオーナごとに設定することができます。

3 OK をクリックします。

選択したインシデントが結合され、「アクティブインシデント」が表示されます。結合後のインシデント番号は、最も若い番号（早く発生したインシデントの番号）になります。



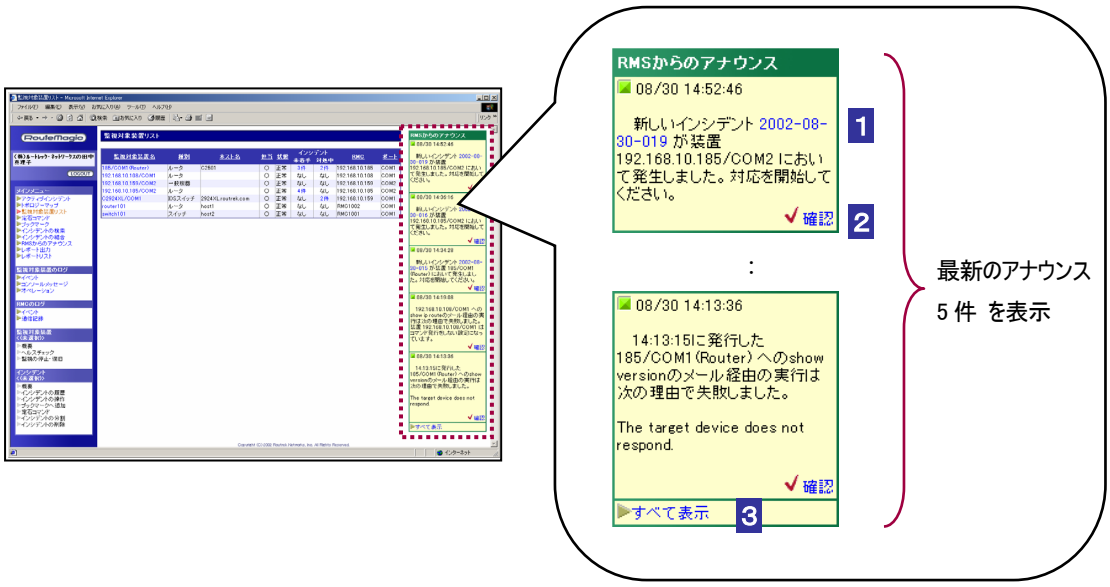
➡ 関連操作

- インシデントを分割する ➡「6.6 インシデントの分割」参照

3.8 RMS からのアナウンス

RMS からのアナウンスは、オペレータの作業や確認を促すメッセージです。インシデントの発生など、オペレータが担当する装置に対応や確認の必要な事象が発生すると、RMS はこれをアナウンスとしてオペレータに通知します。このアナウンスは、一部の画面を除きアナウンス表示画面（画面右側）に未対応の最新アナウンス 5 件が表示される他、対処状況確認のための一覧表示も可能です。

ここでは、アナウンス表示フィールドの操作および RMS からのアナウンスを一括して参照する場合の操作を説明します。



1 アナウンス表示フィールドを確認し、必要な対処を行います。

インシデントの発生など、オペレータの作業を促すアナウンスが表示されている場合、対応作業を行う画面へのリンクが表示されます。（例：インシデント番号）
直ちに対応する場合は、リンクをクリックして必要な作業を行ってください。

2 確認や対応の完了した項目に対しては、✓確認 をクリックします。

メッセージが画面のアナウンス表示フィールドから削除されます。

3 すべてのアナウンスを参照する場合、 メインメニュー の ▶RMS からのアナウンス
またはアナウンス表示フィールドの ▶すべて表示 をクリックします。

「RMS からのアナウンス」にすべてのアナウンスが一覧表示されます。
ここには、✓確認 のクリック操作によってアナウンス表示フィールドから消去されたメッセージも表示されます。

4 特定のアナウンスのみを消去する場合は、**消去** のチェックボックスを使用して消去すべきアナウンスを指定（複数選択可）した後、チェックしたものを消去 をクリックします。

5 アナウンスをすべて消去する場合は、すべて消去 をクリックします。

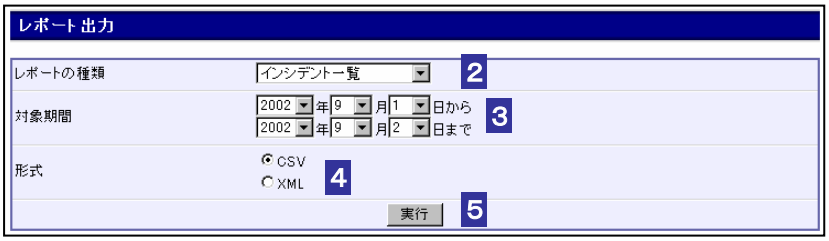
すべてのアナウンス、または指定したアナウンスが削除され、アナウンス表示フィールドのメッセージも消去されます。

3.9 レポートの出力とダウンロード

RMS で管理しているログのデータを、CSV もしくは XML 形式でファイルに保存し、定期レポートの作成データとして利用することができます。レポート情報は、「オーナ」単位で「時系列」（インシデントやイベントの発生順）にファイル出力されます。出力されたファイルは、「レポートリスト」画面で任意のディレクトリにダウンロードして利用してください。出力ファイル形式の詳細に関しては、➡「付録 4.　レポート出力ファイル仕様」を参照してください。

1 メインインメニュー の ▶レポート出力 をクリックします。

「レポート出力」が表示されます。



2 ▼ をクリックして、レポートの種類を選択します。以下の種類のレポートが選択できます。

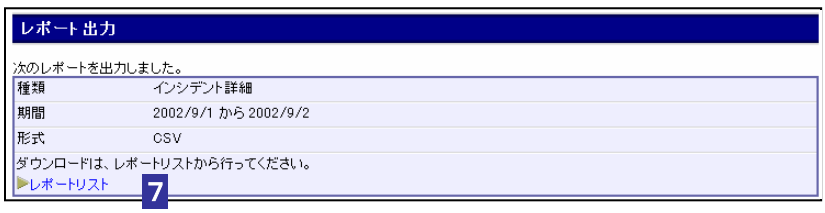
インシデント一覧	インシデントの概要と各インシデントの現在の状態を出力する
インシデント詳細	インシデントの詳細情報（各インシデントに対するコンソールメッセージの内容と対処の履歴）を出力する
設定情報比較	・RMS によって取得された装置の設定情報と、その比較履歴を装置ごとに出力する ・設定情報として、RMC から定期的に送信される Network Information の show running-config（スイッチの場合は write terminal）の実行結果が使用される
コンソールメッセージログ	コンソールメッセージを監視対象装置ごとに出力する
オペレーションログ	RMC 経由で実行された監視対象装置に対する操作ログを、装置ごとに出力する

3 出力するレポートの対象期間を選択します。

4 レポートの出力形式を選択します。（デフォルトは、CSV）

5 実行 をクリックします。

指定された形式のレポートファイルが出力され、下記の画面が表示されます。



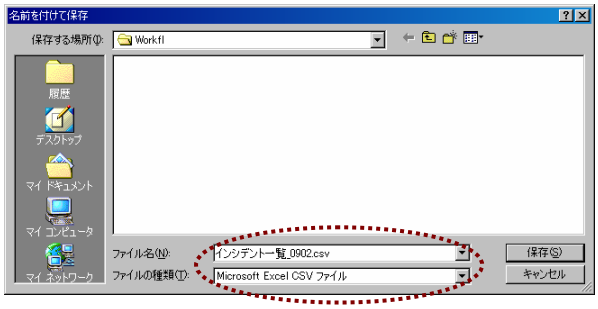
6 複数のレポートを出力する場合は、メインインメニュー の ▶レポート出力 を再度クリックして、2 ～ 5 の操作を繰り返してください。

7 出力されたファイルをダウンロードする場合は、「レポート出力」画面の ▶レポートリスト、または メインインメニュー の ▶レポートリスト をクリックします。

「レポートリスト」に、ダウンロード可能なレポートファイルが表示されます。操作者自身が出力したレポートファイルは、 のクリックにより削除することが可能です。

8 ダウンロードするファイルの をクリックします。

9 ファイルのダウンロード画面において、ファイルの保存場所とファイル名を指定し、保存 をクリックして下さい。



デフォルトのファイル名としては、任意の数字が付与されます。ダウンロードするファイルの内容にしたがってファイル名を指定してください。

選択したレポートファイルが指定のディレクトリにダウンロードされます。

3.10 本製品の破棄について

本製品（CD-ROM などの添付品）を破棄する際には、各自治体の指示に従ってください。

4. ログの参照

ここでは、監視対象装置と RMC に関するログの参照手順と各ログの内容を説明します。

ログの種類と利用メニュー

RMS では、監視対象装置と RMC のログを次のような単位で管理します。

■ 監視対象装置のログ

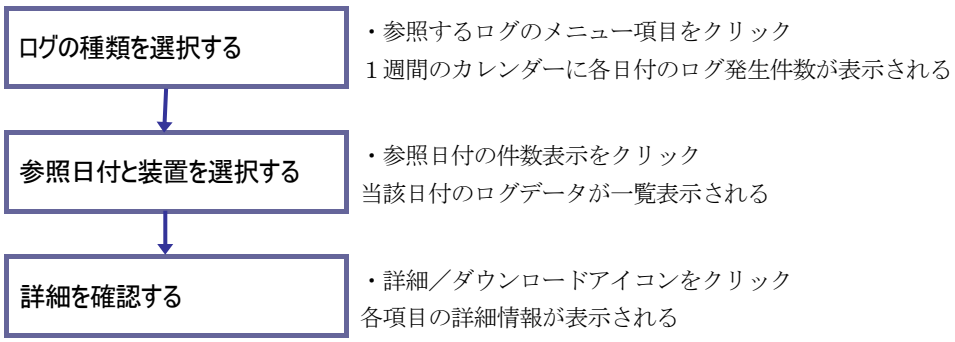
メニュー項目	説明	参照
イベント	・監視対象装置に発生した事象のログ。 ・インシデントの発生や状態の変更、コマンドの発行、コマンド発行結果の受信等が含まれる。	4.2
コンソールメッセージ	監視対象装置のコンソールポートから出力されたコンソールメッセージのログ。	4.3
オペレーション	RMC の connect コマンドを使用して実行した、監視対象装置に対する操作とその結果のログ。	4.4

■ RMC のログ

メニュー項目	説明	参照
イベント	・RMC との通信において発生した事象のログ。 ・RMC-RMS 間の通信の切断／復旧、暗号化機能使用時の鍵交換の記録等が含まれる。	4.5
通信記録	・RMC と RMS 間で送受信されたすべてのメール、および SSH を使用して RMC に発行したコマンドとその結果。 ・主に RMS のサポートを目的として利用する。	4.6

ログの参照手順

ログの参照は、次の手順で行います。ログの種類ごとに操作画面は異なりますが、基本的な操作は共通です。 本章では、参照するログの選択と表示手順 ➡「4.1 参照するログの指定」に続いて、各ログの表示内容と操作を説明します。

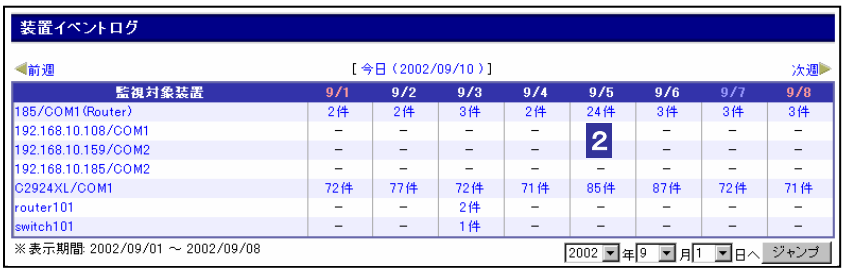


4.1 参照するログの指定

ここでは、監視対象装置のイベントログを例に各ログの参照に共通の操作を説明します。

1 **監視対象装置のログ** メニューの **イベント** をクリックします。（参照するログの種類にしたがって、メニューを選択してください。）

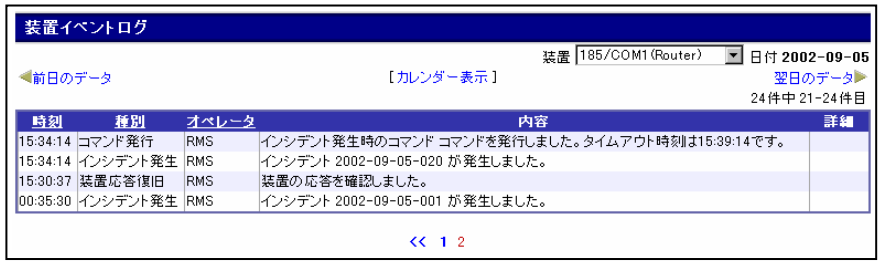
選択したログの表示画面に操作当日を含む 8 日分のカレンダーが表示されます。日付欄には、装置ごとの当日のログ件数が表示されます。



監視対象装置／RMC	監視対象装置、もしくは RMC の名称を表示する
前週	前週 8 日間のログ件数をカレンダー表示する
次週	翌週 8 日間のログ件数をカレンダー表示する
[今日（2002/09/10 ）]	[ ] 内は操作当日の日付。操作日を含むカレンダーを表示する
2002 年 9 月 1 日へ ジャンプ	選択した日付の含まれる週のログ件数をカレンダー表示する

2 ログを参照する装置の日付欄に表示された **件数** をクリックします。

選択したログの内容が一覧表示されます。



前日のデータ	前日のログの内容を一覧表示する
翌日のデータ	翌日のログの内容を一覧表示する
カレンダー表示	カレンダー表示画面に戻る
	ログの詳細を別ウィンドウで表示する
	ログをテキスト形式で保存する
185/COM1(Router)	監視対象装置もしくは RMC を選択し、選択した装置のログを表示する
<< 1 2	データが多量で表示がページ分割された場合に、表示ページを選択する
時刻	下線の付加された項目は、当該項目をキーとした表示順のソートが可能

4.2 装置イベントログ

装置イベントログには監視対象装置に発生した事象が記録されます。ログには、インシデントの発生、それに伴って実行されたコマンドの実行結果、RMC から定期的に受信される装置情報などが含まれます。監視対象装置ごとに動作状況を確認したい場合に参照して下さい。

1 ログを参照する監視対象装置の日付欄に表示された 件数 をクリックすると、当日発生したイベントの概要が表示されます。

時刻	イベントの発生時刻
種別	発生したイベントの種類
オペレータ	・イベント発生の要因となった作業者の名前 ・RMS が実行した動作によるイベントに対しては、"RMS" が表示される
内容	発生したイベントに関する説明
詳細	より詳細な情報がある場合、詳細表示とダウンロード用アイコンが表示される
インシデント	インシデント発生に関連するイベントに対して、リンク用アイコンが表示される
時刻 種別 オペレータ	発生時刻、イベントの種別、オペレータをキーとして表示順序をソートする場合にクリック（表示順のキー指定した項目は、▼ で示される）

2 ログ内容の詳細を確認する場合は、参照するログの をクリックします。

別ウィンドウが開き、「詳細情報」が表示されます。

3 インシデント欄の をクリックすると、関連するインシデントの情報を参照できます。

当該イベントに関連するインシデントの「インシデント概要」が表示されます。

➡「6.1 インシデント概要」参照

4.3 コンソールメッセージログ

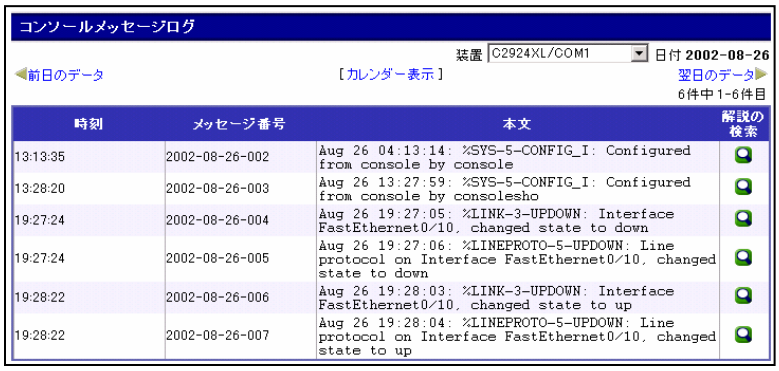
コンソールメッセージログには、インシデント発生やオペレータ通知の対象とならなかったメッセージも含めて、監視対象装置から出力されたすべてのメッセージが記録されます。

コンソールメッセージログには、RMS が受信したすべてのコンソールメッセージが記録されます。必要なメッセージが受信されない場合は：

① RMC のフィルタ設定を確認してください。

② 監視対象装置が「スイッチ」の場合は、監視対象装置の設定を確認してください。
（スイッチ製品では、ファシリティごとにロギングレベルを設定します。この設定が正しく行われていることを確認してください。）

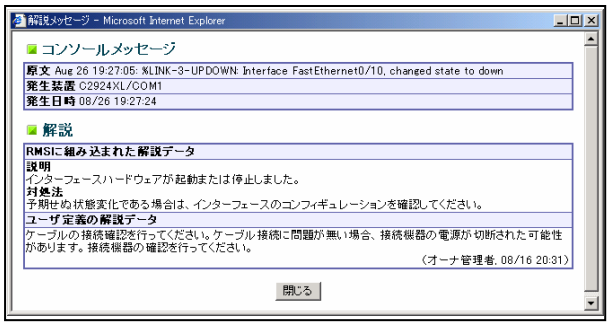
1 ログを参照する監視対象装置の日付欄に表示された 件数 をクリックすると、当日、当該の装置から出力されたコンソールメッセージのリストが表示されます。



時刻	RMC がコンソールメッセージの通知メールを送信した時刻
メッセージ番号	RMS が付与するメッセージ番号　（年 - 月 - 日 - 同一日付内の通番） ※通番は、装置単位ではなく全装置を対象としてメッセージ発生順に付与される。
本文	監視対象装置から出力されたコンソールメッセージ本文 ※装置の無応答が検出された場合、コンソールログ上には "Target Not Respond" が記録されます。
解説の検索	「解説データ」の検索用アイコンが表示される

2 「解説データ」を参照する場合は、 をクリックします。

当該メッセージに対応する「解説データ」（RMS 対応製品のみ表示）および「ユーザ定義の解説データ」（登録されたデータが存在する場合に表示）を検索して内容を表示します。

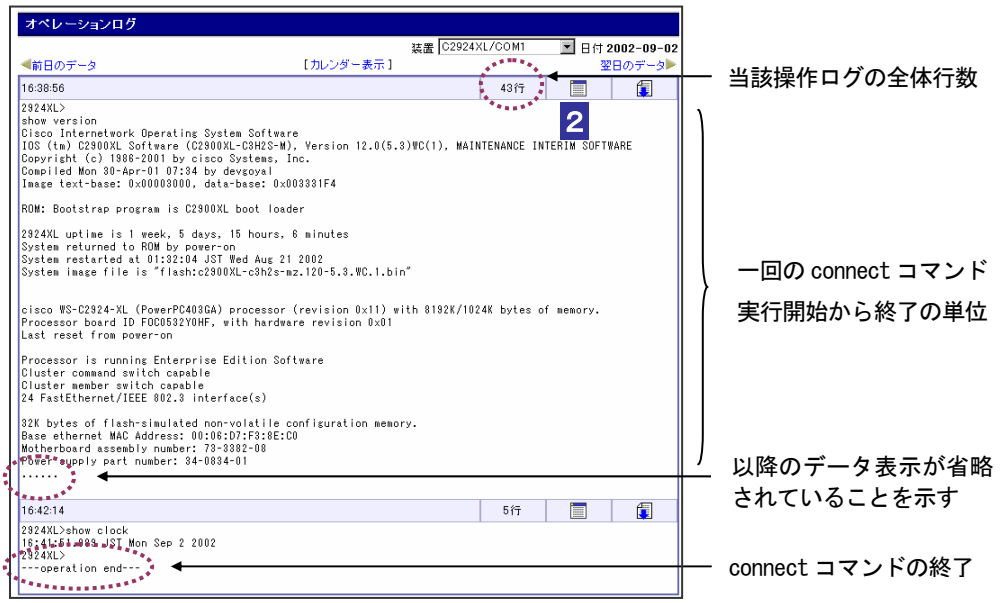


4.4 オペレーションログ

オペレーションログには、RMC を経由して行った監視対象装置に対する操作（RMC の connect コマンドを実行して行った操作）が記録されます。

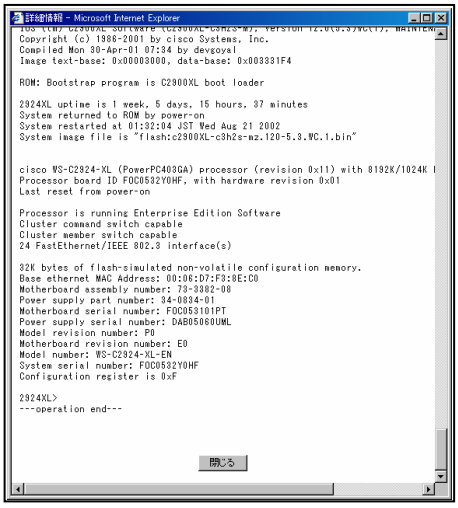
1 ログを参照する監視対象装置の日付欄に表示された 件数 をクリックすると、当日行われた操作のリストが表示されます。

1 回の操作に対するログの全体行数は 1 行目の行数表示で確認できます。(connect の終了は、ログ上では --- operation end --- と記録されます。)
この画面では操作の開始部分から一定行数のみが表示されます。操作内容全体を参照する場合は、 または をクリックして詳細表示もしくはファイルのダウンロードを行ってください。



2 一部のみが表示されている操作ログの全体表示を行う場合は、 をクリックします。

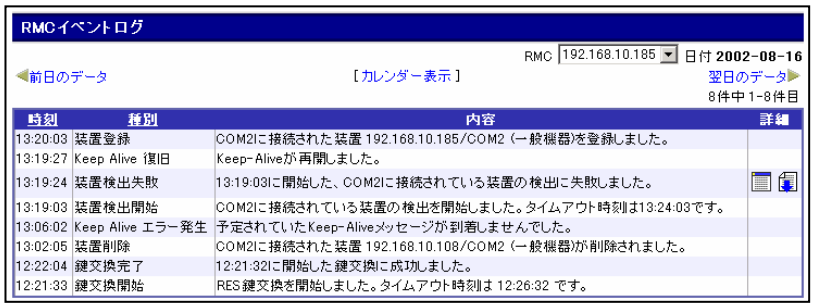
別ウィンドウが開き、「詳細情報」に操作の開始から終了までログが表示されます。



4.5 RMC イベントログ

RMC イベントログには RMC の動作に関連する事象が記録されます。当ログには、RMC からの keep-alive の受信状況、RMC－RMS 間の鍵交換に関する記録などが含まれます。RMC の動作状況や装置の登録に関する記録を確認したい場合に参照して下さい。

1 ログを参照する監視対象装置の日付欄に表示された 件数 をクリックすると、当日発生したイベントの概要が表示されます。

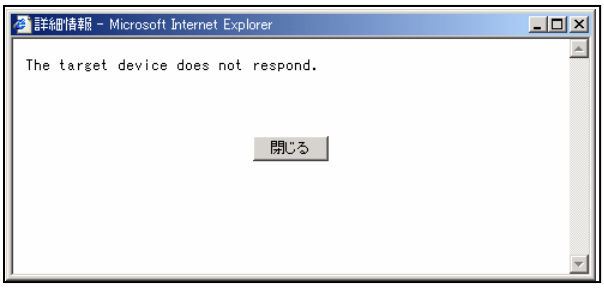


2

時刻	イベントの発生時刻
種別	発生したイベントの種類
内容	発生したイベントに関する説明
詳細	より詳細な情報がある場合、詳細表示とダウンロード用アイコンが表示される
時刻 種別	発生時刻、イベントの種別をキーとして表示順序をソートする場合にクリック （表示順のキー指定した項目は、▼ で示される）

2 ログ内容の詳細を確認する場合、参照するログの  をクリックします。

別ウィンドウが開き、「詳細情報」が表示されます。



4.6 通信記録

通信記録は、RMC と RMS 間で送受信されたすべてのメール、および SSH を使用して RMC に発行したコマンドとその結果を記録したログです。メンテナンス目的で参照するログですので、通常は必要な情報の種類によって、イベントログやコンソールメッセージログを参照します。

1 ログを参照する RMC の日付欄に表示された 件数 をクリックすると、当日 RMC との間で送受信された情報のリストが表示されます。

2

受信時刻	RMC からのメール受信時刻
送信時刻	RMS からのメール送信時刻、または SSH によるコマンド発行時刻
種別	メール受信／メール送信／SSH の種別を示す
Subject	送受信されたメールのサブジェクト、もしくは SSH 実行が記録される
ポート	監視対象装置の接続される RMC ポート
詳細	送受信情報の詳細表示用アイコンが表示される
受信時刻 送信時刻 種類 Subject ポート	各項目をキーとして表示順序をソートする場合にクリック（表示順のキー指定した項目は、▼ で示される）

2 各ログの詳細情報を確認したい場合は、参照するログの  をクリックします。

別ウィンドウが開き、「詳細情報」が表示されます。メールヘッダを表示する場合は、ヘッダも表示 をクリックしてください。

5. 監視対象装置

「監視対象装置」メニューには、次の機能が用意されています。

■ **監視対象装置の操作と情報の参照機能**

監視対象装置の設定情報や最新のインシデント対処状況、装置に接続されている RMC の情報を確認することができます。また、RMS にロギングされている監視設定装置の設定情報を、ダウンロードすることも可能です。

■ **ヘルスチェック機能**

監視対象装置の情報を取得するため、RMC から定期的に（通常は 1 日 1 回）発行されているコマンド（Network Information）の実行結果を元に、装置設定やルーティングテーブルの変化を確認できます。
ヘルスチェックの対象となる監視対象装置は、RMS 対応製品（ルータ、スイッチ、ISO スイッチ）のみです。 ➡「ご利用の前に」参照

■ **監視対象装置の停止・復旧予定機能**

監視対象装置に対する監視を一時的に停止することができます。
定期メンテナンスや保守点検など、監視対象装置の停止があらかじめわかっている場合は、停止と復旧の予定を設定しておくことにより、不要なインシデントの発生を避けて管理作業の混乱を防止できます。

利用メニュー

監視対象装置 メニューは、監視対象装置が選択された場合にアクティブになります。
監視対象装置の選択は、トポロジーマップや装置リスト／インシデントリストから行います。操作の詳細については、下記の節をご覧ください。

- ➡「3.1 アクティブインシデント」
- ➡「3.2 トポロジーマップ」
- ➡「3.3 監視対象装置リスト」
- ➡「6.1 インシデント概要」

「監視対象装置」のメニュー項目では、次の操作を行うことができます。

メニュー項目	説明	参照先
概要	・監視対象装置の設定情報と現在の状態を参照する。 ・監視対象装置の設定情報をダウンロードする。	5.1
ヘルスチェック	・ヘルスチェックの結果を参照する。	5.2
監視の停止・復旧	・監視対象装置の監視を停止する期間を予約する。 ・無期限の指定で停止した監視の再開もこのメニューで行う。	5.3

5.1 監視対象装置の情報

操作対象とする監視対象装置が指定されると、 監視対象装置 メニューに ＜装置名＞ が表示され、メニュー項目がアクティブになります。

監視対象装置 メニューがアクティブな状態で ▶概要 をクリックする、もしくは監視対象装置リストやトポロジーマップなどの画面で 装置名 をクリックすると「監視対象装置の情報」が表示されます。

この画面では、監視対象装置に関する情報と、現在の状況が参照できます。設定情報のダウンロードもこの画面から行ってください。

1 **監視対象装置　メニューがアクティブな状態で　▶概要 をクリックします。**

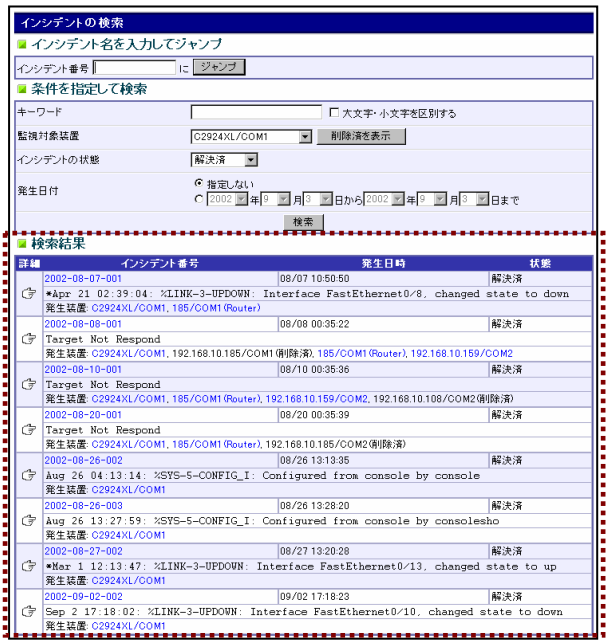
監視対象装置と、この装置に発生したイベントの対応状況、および装置に接続された RMC の情報が表示されます。

項目	説明
監視対象装置	
名称	・監視対象装置のを識別するための装置名称 ・1 オーナ内では、装置ごとにユニークな名称が付与される
状態	監視対象装置の現在の状態
種別	装置の種別（「ルータ」「IOS スイッチ」「スイッチ」「一般機器」） ※プラグインをインストールした場合の装置種別に関しては、「プラグイン・ユーザーズガイド」参照
設置場所	監視対象装置の設置場所（オーナ管理者の設定情報）
ホスト名	監視対象装置のホスト名（オーナ管理者の設定情報）
IP アドレス	監視対象装置の IP アドレス（オーナ管理者の設定情報）
シリアルナンバー	監視対象装置のシリアル番号（オーナ管理者の設定情報）
インシデント発生条件	コンソールメッセージをインシデントとして認識するための条件 （閾値、およびメッセージ内容にしたがった重要度を設定）
インシデント発生時のアクション	インシデント発生時に監視対象装置に対して、自動的に実行される動作 ※RMS 対応製品に関しては、インシデント発生時のデフォルト・アクションが用意される
操作可能者	担当オペレータ（当該装置の操作権限を持つオペレータ）
監視の状態	装置が通常の監視状態（「稼動中」）にあるか、停止予約による監視の停止中（「停止中」）であるかを表示
接続された RMC	
名称	監視対象装置に接続されている RMC の名称
状態	RMC の稼動状態を示す （初期設定メール未受信の場合は、SetupInfo 待ちが表示される）
IP アドレス	RMC の IP アドレス　（RMC を経由した監視対象装置の操作に使用）
シリアルポート	監視対象装置が接続される RMC のポート名（COM1～COM12）
コマンド発行方法	RMC に対するコマンド発行送信の方法（メールまたは SSH）
Keep-Alive	RMC からの Keep-Alive が定時に正常受信されているか否かを示す
次回 Keep-Alive 受信予定	次回の Keep-Alive 受信予定（受信予定時刻を過ぎて一定の時間が経過すると Keep-Alive 切断と見なされる）
モデム電話番号	RMC に接続されるモデムの電話番号 （RMS からの自動発呼機能は未サポート）
インシデント	
未着手	当該装置に関する未着手のインシデント件数が表示される。
対処中	当該装置に関する対処中のインシデント件数が表示される。
解決済	当該装置に関する解決済みのインシデント件数が表示される。
保留	当該装置に関する保留状態のインシデント件数が表示される。
装置の設定情報	
現在	監視対象装置の最新の設定情報
一世代前	一世代前（最新への設定変更前）の設定情報
	設定情報を別ウィンドウで表示する
	設定情報をダウンロードし、テキスト形式で保存する

2 インシデントを参照する場合は、確認する「状態」の 件数 をクリックします。

「インシデントの検索」が表示され、当該の**監視対象装置**と**状態**に対応するインシデントの一覧が **検索結果** に表示されます。

「インシデントの検索」の操作については➡「3.6 インシデントの検索」参照。



3 装置設定情報の参照もしくはダウンロードを行う場合は、表示／ダウンロード欄のアイコンをクリックします。

RMS が保存している、監視対象装置の設定情報（show startup-config または show config 実行結果）をダウンロードすることができます。

	設定情報を別ウィンドウで表示する
	設定情報をダウンロードする

show running-config および write terminal の実行結果、装置設定情報の過去の変更履歴は、ヘルスチェックによって確認してください。 ➡「5.2 ヘルスチェック」参照

5.2 ヘルスチェック

ヘルスチェックでは、監視対象装置の設定情報やルーティングテーブルの変更履歴を確認することができます。ヘルスチェックを実行するために必要なコマンドの発行は、設定にしたがってRMC が自動的に行い、結果を Network information メールで RMS に通知します。

> ヘルスチェックが正常に稼動しない場合は、接続されている RMC の Network Information に関する設定を確認してください。

> ヘルスチェックは、RMS 対応製品でのみ利用できます。

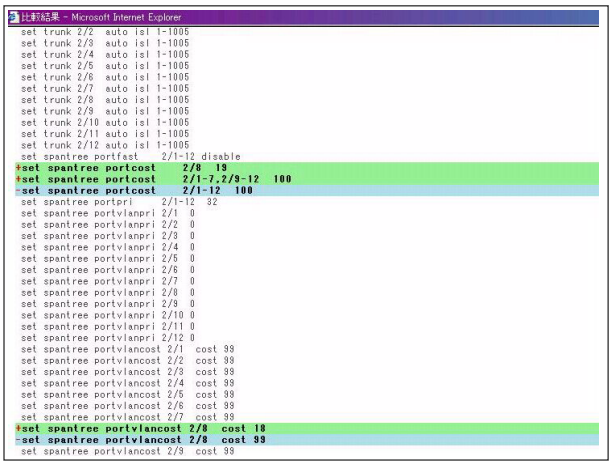
1 監視対象装置 の ヘルスチェック をクリックします。

当該監視対象装置の設定情報に関する変更履歴が表示されます。

2 ヘルスチェックでは、以下のデータ比較が可能です。(監視対象装置の種別により、対応するコマンドには相違があります) ▼ をクリックしてメニューから比較対象を選択して下さい。 OK をクリックすると選択したデータの比較結果が表示されます。

比較対象	内容
show startup-config または show config 実行結果	最新のコマンド実行結果（今回の結果）を前回取得したデータと比較し、差分を表示する
show running-config または write terminal 実行結果	最新のコマンド実行結果（今回の結果）を前回取得したデータと比較し、差分を表示する
show ip route 実行結果	最新のコマンド実行結果（今回の結果）を前回取得したデータと比較し、差分を表示する
show startup-config と show running-config または show config と write terminal の実行結果	双方のコマンドの実行結果を比較し、差分を表示する

3 比較結果に差分がある場合のみ、 が表示されます。このアイコンをクリックすると別ウィンドウが開き、取得データと差分の表示が行われます。



} 差分検出行の表示

＋：旧データに対する追加行

- ：旧データから削除された行

ネットワークの設定や構成を変更した場合

ネットワークの構成やネットワーク機器に対する設定変更に伴って、トラブルの発生するケースが多く見られます。設定が正しく行われていること、および変更情報を保存したことを必ず確認するようにしてください。

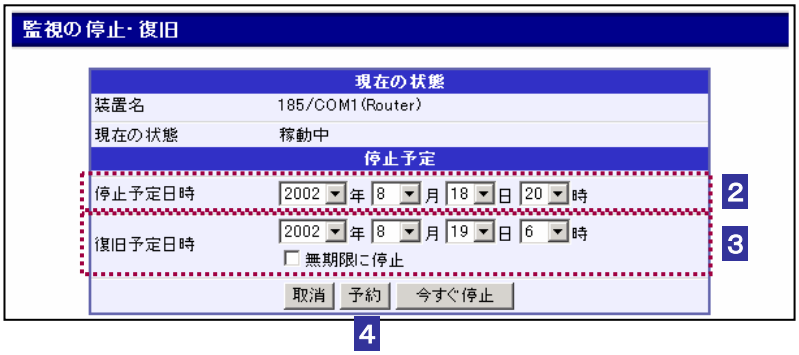
また、特にトラブルが発生していなくても、設定情報に変化があったときには、その理由を把握しておくことが重要です。ヘルスチェック機能を利用して、設定情報に関する変更を定期的に確認し、トラブルの原因究明や、トラブルの防止に役立てて下さい。

5.3 監視の停止と復旧

監視対象装置の監視を停止する期間の設定を行います。これは、装置の定期点検などの際にRMSによる監視を一時的に停止して、不要なインシデントの発生やオペレータへの通知を避けるための機能です。監視対象装置自体の停止（電源断、あるいはシャットダウン操作）を行う機能ではありませんのでご注意ください。

1 監視対象装置 の ▶監視の停止と復旧 をクリックします。

「監視対象装置の監視の停止・復旧」が表示されます。



2 「停止予定日時」を選択します。
直ちに監視を停止する場合は、「今すぐ停止」（ ☐ ）をチェックします。

3 「復旧予定日時」を選択します。
無期限に停止する場合は、「停止は無期限」（ ☐ ）をチェックします。

4 予約 をクリックします。

選択した期間の監視停止予定が設定され、画面に“監視の停止を予約しました。”という確認メッセージが表示されます。

監視の復旧

監視停止中の装置では、「監視の停止・復旧」は下図のように表示されます。復旧予定に「停止は無期限」を選択した場合、あるいは予定よりも早く復旧したい場合は、監視停止中の装置の 今すぐ復旧 をクリックしてください。直ちに装置の監視が再開されます。

6. インシデント

「インシデント」メニューには、次の機能が用意されています。

■ **インシデントに関する情報の参照**

インシデントの発生要因となったコンソールメッセージとそのメッセージに関する解説、過去の対処履歴から得られた情報など、各インシデントの対処に必要な概要情報が参照できます。

■ **インシデント履歴の参照**

RMS が自動実行した操作も含め、インシデントに対する操作とその結果の履歴を参照できます。

■ **インシデントに対する操作**

インシデントに対するコメントの付加や状態の変更など、インシデントに関する操作を行うことができます。インシデントに対するコメントは、対処履歴として登録し、再度、同様なトラブルが発生した場合に活用させる事ができます。
また、インシデントの分割、あるいは削除の機能を利用して、監視作業の状況に即した形でインシデントを管理することができます。

■ **定石コマンドの発行**

インシデントの発生した監視対象装置に対するコマンド発行が、ボタン操作で簡単に行えます。これにより、監視対象装置の状態を詳細に確認することができます。

利用メニュー

インシデント メニューは、操作対象のインシデントが選択された場合にアクティブになります。インシデントの選択は、インシデントリスト上から特定のインシデントを指定することによって行います。操作の詳細については、下記の節をご覧ください。

- ➡「3.1 アクティブインシデント」
- ➡「3.5 ブックマーク」
- ➡「3.6 インシデントの検索」

「インシデント」のメニュー項目では、次の操作を行うことができます。

メニュー項目	説明	参照先
概要	インシデントに関係する情報を参照する。	6.1
インシデントの履歴	インシデントの履歴（発生から現在までの経過）を参照する。	6.2
インシデントの操作	インシデントに対する状態の変更やコメント入力を行う。	6.3
ブックマークへ追加	インシデントをブックマークに追加する。	6.4
定石コマンド	インシデントが発生した監視対象装置にコマンドを発行する。	6.5
インシデントの分割	インシデントを分割する。	6.6
インシデントの削除	インシデントを削除する。	6.7

6.1 インシデント概要

操作対象のインシデントが選択されると、 インシデント メニューに <インシデント番号> が表示され、メニュー項目がアクティブになります。

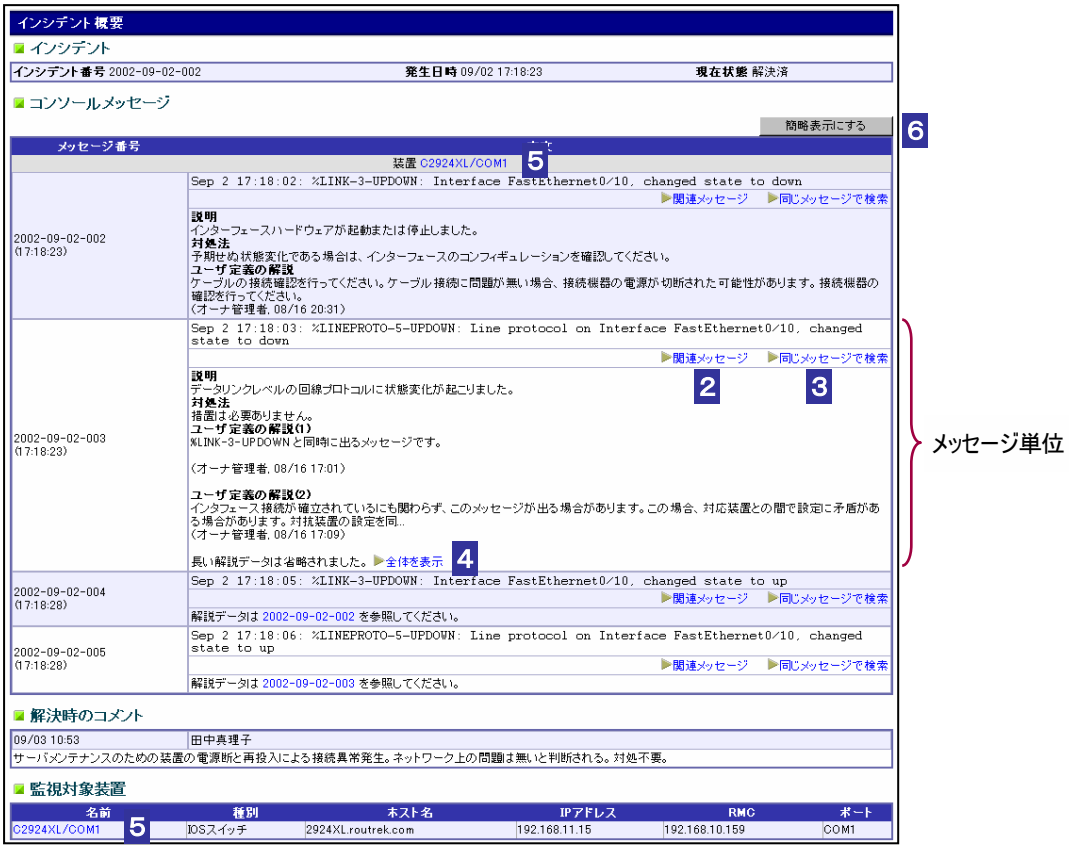
インシデント メニューがアクティブな状態で ▶ 概要 をクリックする、もしくはアクティブインシデントやインシデントの検索結果などの画面で インシデント番号 をクリックすると「インシデント概要」が表示されます。インシデント概要では、発生したインシデントに関する各種の情報を参照し、トラブルの状況確認を行うことができます。

1 インシデント メニューがアクティブな状態で ▶ 概要 をクリックします。

「インシデント概要」には、インシデントの発生要因となったメッセージとそのメッセージに関連する情報が表示されます。

メッセージが連続的に受信された場合は、複数のメッセージが 1 つのインシデントに含まれます。 1 つのインシデントに複数の装置からのメッセージが含まれる場合、メッセージは装置ごとに区分され、発生順に表示されます。この場合、 監視対象装置 には、関連する装置のリストが表示されます。

解決時のコメント には、インシデントの操作においてインシデント状態を“解決済み”とした際に入力されたコメントを表示します。このフィールドは、インシデントの状態が解決済の場合のみ表示されます。



インシデント		インシデントに関する基本情報が表示される
インシデント番号		＜年/月/日－通し番号※＞の形式で表示される ※通し番号：同じ日付で 1 つのオーナ内で発生した順番に振られる
現在状態		・「未着手」「対処中」「解決済」「保留」のいずれかが表示される ・発生直後のインシデントは「未着手」であり、担当者がインシデントの操作を行うことにより状態が変更される
コンソールメッセージ		当該インシデントに含まれるコンソールメッセージが表示されるメッセージは、発生した装置ごとにまとめられ、出力順に表示される
メッセージ番号		年－月－日－通し番号※の形式で表示される ※通し番号：同じ日付で 1 つのオーナ内に発生した順序で付与される （ ）内は、インシデント発生時刻
本文	上段	監視対象装置から出力されたコンソールメッセージ表示される
	中段	関連メッセージ：当該インシデントと関連するコンソールメッセージログの表示 同じメッセージで検索：メッセージ検索画面へのリンク
	下段	・RMS に予め登録されている「解説メッセージ」（“説明”、“対処法”）およびユーザが登録した「ユーザ定義の解説データ」が表示される ・内容が長文で全体表示ができない場合、全文を表示するためのリンク（ 全体を表示 ）が表示される
装置		コンソールメッセージを出力した 監視対象装置名 が表示される 監視対象装置名 をクリックすると、「監視対象装置」へ表示が移動する
解決時のコメント		当該インシデントの状態を解決済とした時に入力されたコメントが表示される。（インシデントの状態が解決済の場合のみ表示）
監視対象装置		インシデントが発生した監視対象装置と、それに接続されている RMC の情報が表示される

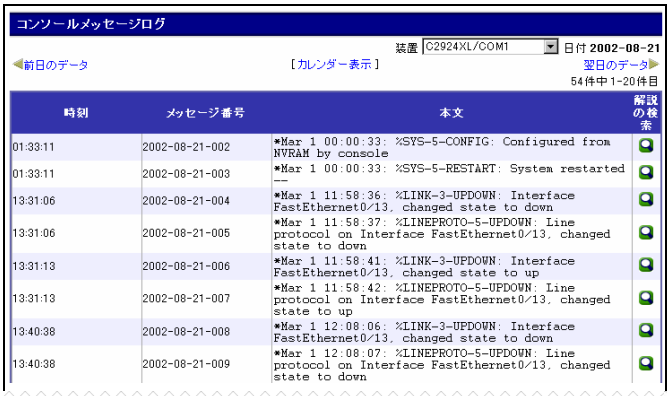
「ユーザ定義の解説データ」の入力と編集に関しては、以下を参照してください。
インシデントの履歴情報（コメント）として、解説データを入力 ➡「6.3 インシデントの操作」
解説データの登録・編集を実行 ➡ オーナ管理者編「10.1 ユーザ定義の解説データ」

インシデント発生の対象となるのは、RMS が受信したコンソールメッセージ中の指定された条件に合致するメッセージのみです。必要なインシデントが発生しない、あるいは必要なメッセージが受信されない場合は：

① RMC のフィルタ設定を確認してください。
② 監視対象装置の「インシデント発生条件」を確認してください。
（設定を変更するには、オーナ管理者の権限が必要です。）
③ 監視対象装置が「スイッチ」の場合は、監視対象装置の設定を確認してください。
（スイッチ製品では、ファシリティごとにロギングレベルの設定が可能です。
ロギングレベルの設定が正しく行われていることを確認してください。）

2 ▶ **関連メッセージ** をクリックすると、当該インシデントに限定せず、同一日にその装置に発生したすべてのコンソールメッセージを参照することができます。

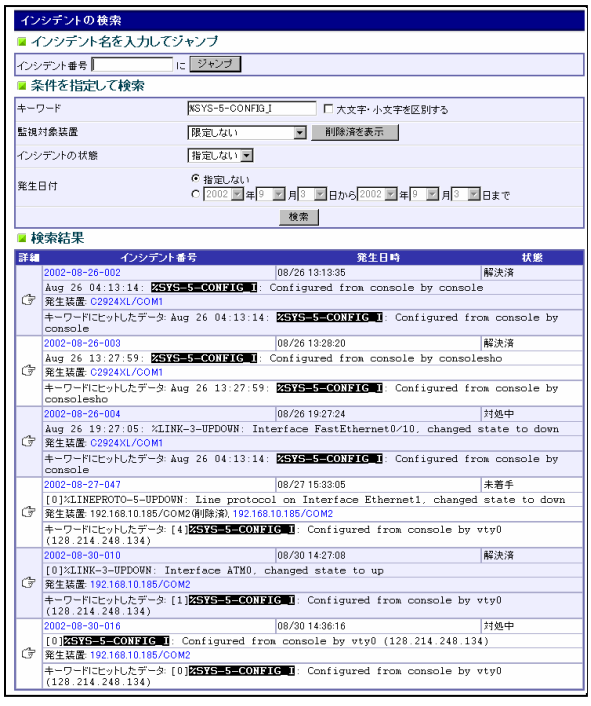
関連メッセージ をクリックしたコンソールメッセージと同一の日付と監視対象装置を選択した状態で、「コンソールメッセージログ」が表示されます。



コンソールメッセージログの参照に関しては、➡「4.3 コンソールメッセージログ」参照。

3 ▶ **同じメッセージで検索** をクリックすると、過去に発生したインシデントから、同一のキーワードを持つコンソールメッセージが含まれたインシデントを検索します。

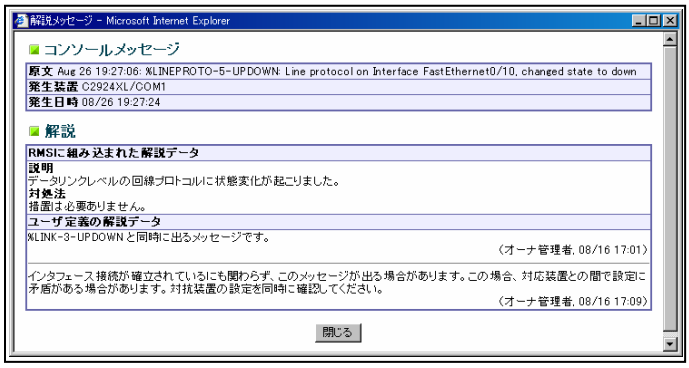
コンソールメッセージに対してキーワードの指定を行った状態で検索が実行され、「インシデントの検索」が表示されます。



インシデント検索の操作に関しては、➡「3.6 インシデントの検索」参照

4 省略表示された解説メッセージの全文を表示する場合は、▶ 全体を表示 をクリックします。

別ウィンドウが開き、「解説メッセージ」に、指定されたコンソールメッセージに対応する解説メッセージとユーザ定義の解説データの全文が表示されます。



5 監視対象装置を参照する場合は、監視対象装置名 をクリックします。

選択された監視対象装置の「監視対象装置の情報」が表示されます。

➡「5.1 監視対象装置の情報」参照

6 簡略表示にする をクリックすると、コンソールメッセージ部の表示形式を簡略化し、メッセージのみを表示することができます。

「解説メッセージ」、「ユーザ定義の解説データ」の表示および、メッセージ検索のためのリンクが省略された表示形式になります。 詳細表示にする をクリックすると、通常の表示形式に戻ります。

監視対象装置の操作

監視対象装置の操作を行う際は、RMC に TELNET もしくは SSH でログインし、**connect** コマンドを発行することによって監視対象装置にログインしてください。監視対象装置に対する操作をオペレーションログとして記録する事ができます。

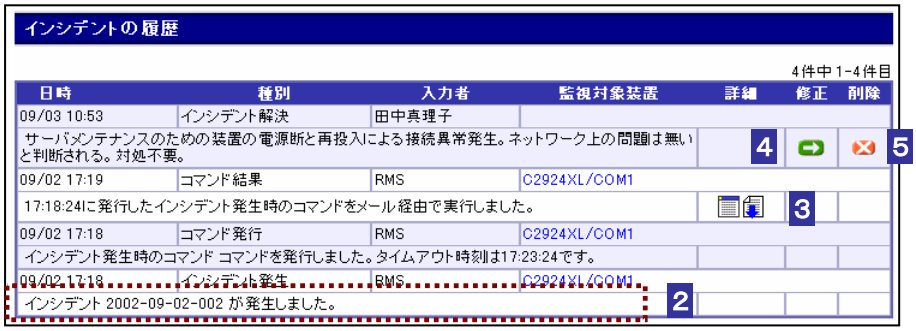
監視対象装置に接続されている RMC の IP アドレスは、操作する監視対象装置の 監視対象装置名 をクリックし、「監視対象装置の情報」を表示して確認します。

6.2 インシデントの履歴

インシデントの履歴では、各インシデントに対する発生時からの対応履歴が参照できます。履歴情報には、インシデントの発生日時、インシデントに対して実行された操作とその操作担当者、インシデントへの対応として監視対象装置に発行されたコマンドとその実行結果などが含まれています。

1 インシデント メニューの インシデントの履歴 をクリックします。

「インシデントの履歴」に、選択したインシデントの履歴情報が表示されます。

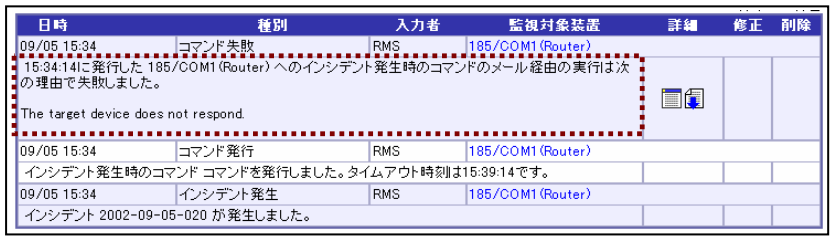


日時	インシデントの発生日時やインシデントに関する操作の発生日時が表示される
種別	インシデントに対してオペレータや RMS が実行した操作、およびイベントの種類が表示される
入力者	オペレータ操作の場合は、当該操作を行った担当者名が表示される RMS が実行した動作については、「RMS」が表示される

2 各イベントに対する対処履歴情報を確認します。

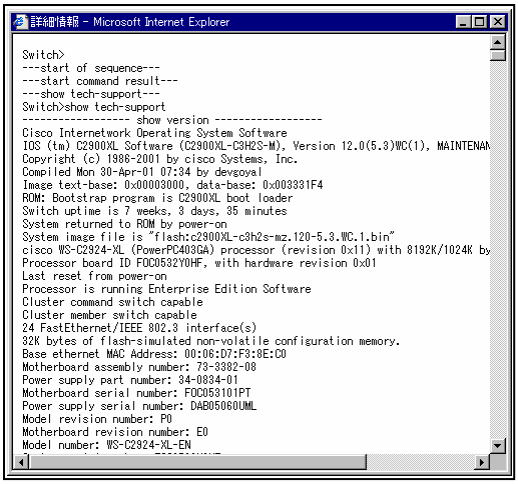
この欄には、オペレータの入力したコメント、RMS が自動的に実行した操作の内容などが表示されます。インシデント発生の場合は、インシデント番号が表示されます。

コマンド発行イベントの場合には、発行要求と実行結果に関する情報が別イベントとして記録されます。コマンド発行が正常に実行されなかった場合は、実行結果イベントには、下図のようにエラー原因に関する情報が表示されます。



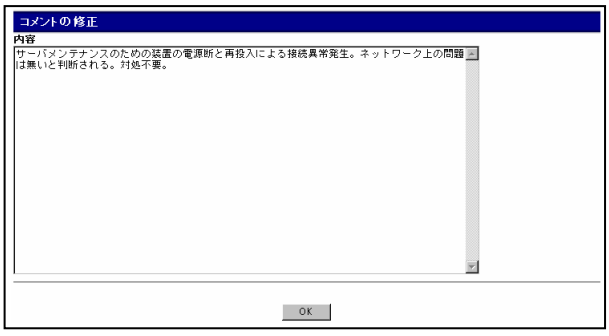
3 コマンド発行結果の確認には、 をクリックします。

別ウィンドウが開き、「詳細情報」に発行されたコマンドとその実行結果（装置からの出力データ）が表示されます。



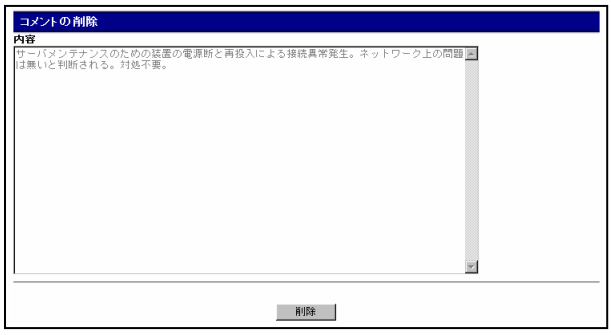
4 オペレータが入力したコメントを修正する場合は、 をクリックします。

「コメントの修正」画面に、現在の内容が表示されます。内容を修正し、 OK をクリックすると、「インシデントの履歴」に修正したコメントが反映されます。



5 履歴を削除する場合は、 をクリックします。

「コメントの削除」に入力されたコメントの内容が表示されます。コメントの内容を確認し、削除する場合は 削除 をクリックします。履歴からコメントが削除され、表示は「インシデントの履歴」に戻ります。



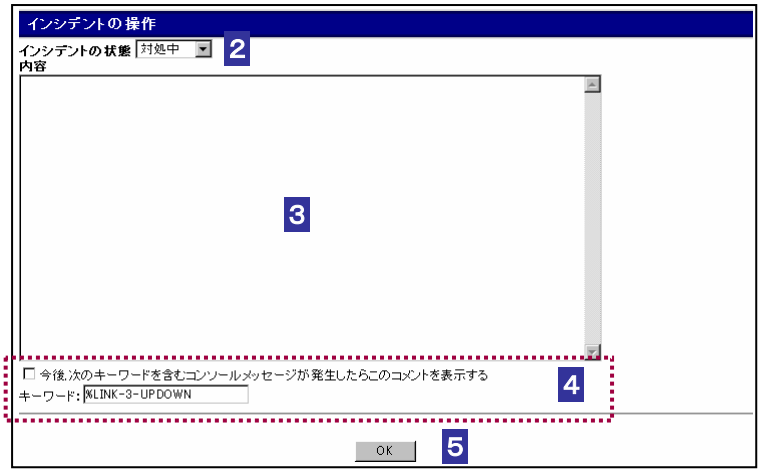
コメントの修正／削除は、入力したオペレータのみが実行できます。他のオペレータが履歴情報を参照した場合には、修正／削除用アイコン（ ）は表示されません。

6.3 インシデントの操作

インシデントの対処状況によって、状態の変更やコメントの入力を行います。
ここで入力したコメントは、インシデントの履歴、あるいはインシデント発生時の解説情報として参照することができます。他の担当者への状況の連絡や、過去の対処履歴情報として利用して下さい。

1 インシデント メニューの ▶インシデントの操作 をクリックします。

「インシデントの操作」が表示され、インシデント状態の変更と履歴情報としてのコメント入力が可能になります。



2 ▼ をクリックして、インシデントの状態を選択します。

インシデントの状態	未着手　：インシデント発生直後の状態 対処中　：インシデントの対処を行っている状態 解決済み：インシデントが解決した状態 保留　　：インシデントへの対処を一時保留している状態 （原因不明のまま暫定的な復旧を行ったような場合に使用する）

3 コメントを入力します。

コメントの入力において http で始まる URL を記述すると、コメント表示時にリンク変換され、指定した URL のページを表示することができます。

4 入力したコメントを過去の対応履歴として利用する場合は、以下の操作を行います。

① 「今後,次のキーワードを・・・・コメントを表示する」（ ☐ ）をチェックします。

② キーワードを指定します。
指定したキーワードを含むコンソールメッセージによってインシデントが発生すると、入力したコメントがインシデント概要の「ユーザ定義の解説」として表示されます。

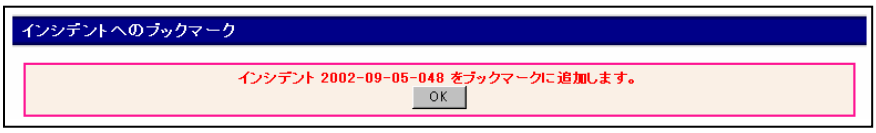
5 OK をクリックします。

6.4 ブックマークへ追加

自分の担当で頻繁にアクセスするインシデントや、解決済みでも参照することの多いインシデントにブックマークを追加することによって、速やかに参照できるようにします。

1 インシデント メニューの ▶ ブックマークへ追加 をクリックします。

「インシデントへのブックマーク」が表示されます。



2 OK をクリックします。

ブックマークが追加され、「インシデント概要」が表示されます。

➡ 関連操作

- ブックマークを確認／削除する ➡「3.5 ブックマーク」参照

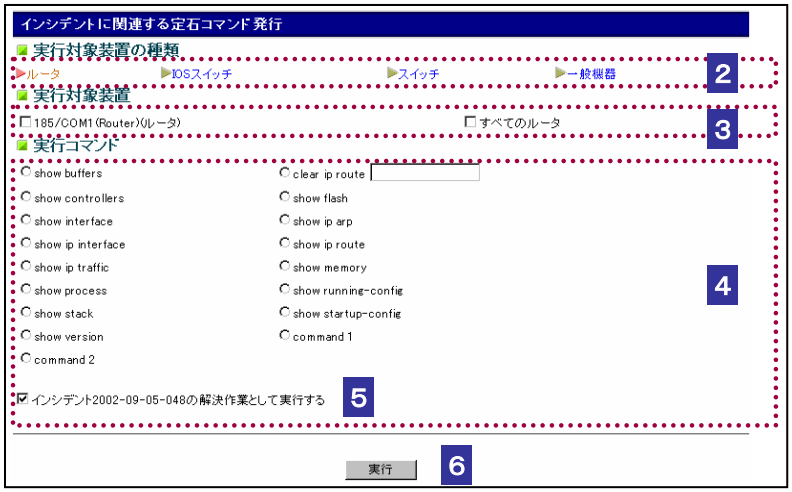
6.5 定石コマンドの発行

RMS では、監視対象装置の監視やメンテナンスにおいて頻繁に使用されるコマンドを「定石コマンド」として登録し、簡単な操作で実行できるようにしています。RMS 対応製品に関しては、一連のコマンドがデフォルトの定石コマンドとして登録されています。その他の製品（一般機器）に対応した定石コマンドの新規登録、あるいは RMS 対応製品への追加コマンドの登録は、オーナ管理者が行います。 ➡「－オーナ管理者編－ 10.2 定石コマンドメニューの登録」参照

ここでは、インシデントが発生した監視対象装置に対して、定石コマンドを発行する操作について説明します。インシデント対応作業としての定石コマンドは、対処中のインシデントに関連する監視対象装置、および当該装置と同一の種類の装置に対してのみ発行できます。

1 インシデント メニューの ▶定石コマンド をクリックします。

「インシデントに関連する定石コマンド発行」が表示されます。



2 実行対象装置の種類 の ▶装置の種類 をクリックして、コマンドを発行する監視対象装置の種類を選択します。

実行対象装置には、対処中のインシデントに関連する監視対象装置が表示されます。装置の種類をクリックすると、選択した種類の装置で、操作者が担当オペレータになっている装置のチェックボックスのみが有効になります。

実行コマンド には、選択した種類の装置に対して発行できるコマンドが表示されます。

3 実行対象装置 のチェックボックス（ ☐ ）をクリックして、コマンドを発行する装置を選択します。（複数選択可）

4 実行コマンド のラジオボタン（ ○ ）をクリックします。（単一選択）

> 「clear ip route」、「two parameters」コマンドには、引数が必要です。
> デフォルトの値は「*」で、すべてのネットワークインタフェースが対象になります。
> 特定のネットワークインタフェースに対してのみコマンドを実行する場合は、各コマンドのテキストボックスに適切な引数を入力します。

5 インシデントの対処作業としてコマンドを発行する場合は、「インシデント＜番号＞の解決作業として実行する」(☐)をチェックします。

> この項目をチェックしなかった場合、コマンド発行要求とその結果は「インシデントの履歴」には残りません。装置イベントログへの記録のみとなります。

6 実行 をクリックします。

RMC に対してコマンドの発行要求が送信されます。
コマンド発行要求が完了すると、実行ボタンの下に、次のメッセージが表示されます。

コマンドを発行しました。結果が返信されるとイベントログへ記録されます。

定石コマンドの実行結果は、監視対象装置のイベントログに記録されます。コマンド発行による監視対象装置からの出力、あるいは何らかのエラーによりコマンド発行が正常に行われなかった場合のエラー原因などは、すべて装置イベントログに記録されますので、結果を確認してください。

> RMS－RMC 間のメール到達性、あるいはネットワーク管理上のポリシーなどにより、”RMS からのコマンド発行を行わない”設定とすることが可能です。この設定を行っている場合、「監視対象装置の情報」 接続された RMC のコマンド発行方法に ”コマンドは発行しない”と表示され、定石コマンドの発行を要求した場合は、装置イベントログにエラーが記録されます。
>
> この指定は、オーナ管理者が RMC ごとに設定する情報ですので、設定内容に関してはオーナ管理者に確認してください。

➡ 関連操作

- 監視対象装置のイベントログを参照する ➡「4.2 装置イベントログ」参照
- インシデントとは関係なく監視対象装置に対してコマンドを発行する ➡「3.4 定石コマンドの発行」参照

定石コマンドを発行可能な環境

コマンドの発行は、メールまたは SSH を利用して行われるため、RMS から RMC へメールが到達できる環境が必要です。
例えば、ファイアウォールの内側に RMC が、外側に RMS があるような場合は、メールや SSH の要求がこれを通過できるように設定する必要があります。

なお、コマンドの種類によっては、発行後、結果の受信が完了するまでに数秒～数分の時間が掛かる場合があります。 また、あらかじめ鍵がセットアップされている場合に限り、RMC と RMS 間のメール送受信に、PGP を使って署名と暗号化が行われます。 これによって、第三者によるコマンドの実行や、結果の盗聴を防止することができます。

6.6 インシデントの分割

RMS では、複数のコンソールメッセージが連続的に受信された場合、これを 1 つのインシデントとして管理します。このインシデントを任意のコンソールメッセージ単位に分割し、それぞれを別のインシデントとして扱うことができます。インシデントの分割は、当該インシデントに関係する監視対象装置の担当オペレータのみが実行できます。また、インシデントの状態が解決済みのインシデントを分割する事はできません。

1 インシデント メニューの インシデントの分割 をクリックします。

「インシデントの分割」が表示されます。

2 をクリックして、分割方法を選択します。

チェックした項目としていない項目で全体を 2 分割	チェックしたコンソールメッセージと、チェックしていないコンソールメッセージの 2 つに分割する
チェックした項目それぞれを単独のインシデントに分離する	チェックしたコンソールメッセージを 1 メッセージごとに単独のインシデントとし、チェックしていないコンソールメッセージはまとめて 1 つのインシデントとする

3 選択した分割方法に基づいて、コンソールメッセージをチェックします。

当該インシデントに含まれるコンソールメッセージのすべて、あるいはいずれかの装置に関連するメッセージのすべてを個々に独立したインシデントとする場合は、「チェックした項目それぞれを単独のインシデントに分離する」を選択し、「すべてチェック」「この装置の全メッセージをチェック」（ ）をチェックします。

4 実行 をクリックします。

2 で選択した分割方法でコンソールメッセージが分割され、独立のインシデントとして「アクティブインシデント」に表示されます。

➡ 関連操作

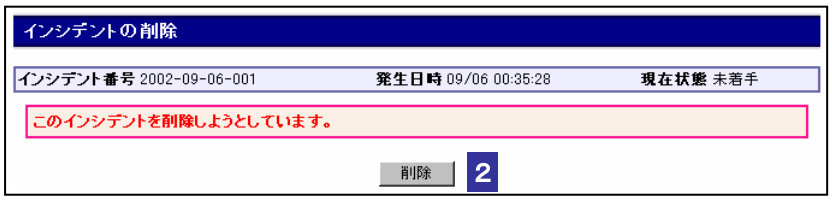
- 分割したインシデントを結合する ➡「3.7 インシデントの結合」参照

6.7 インシデントの削除

対処の必要がないと判断されたインシデントは、削除することができます。
インシデントの削除は、当該インシデントに関係する監視対象装置の担当オペレータのみが実行できる機能です。

1 インシデント メニューの ▶インシデントの削除 をクリックします。

「インシデントの削除」に選択したインシデントの番号、発生日時、現在の状態が表示されます。



2 表示内容を確認し、削除する場合は 削除 をクリックします。

指定したインシデントが削除され、「アクティブインシデント」が表示されます。

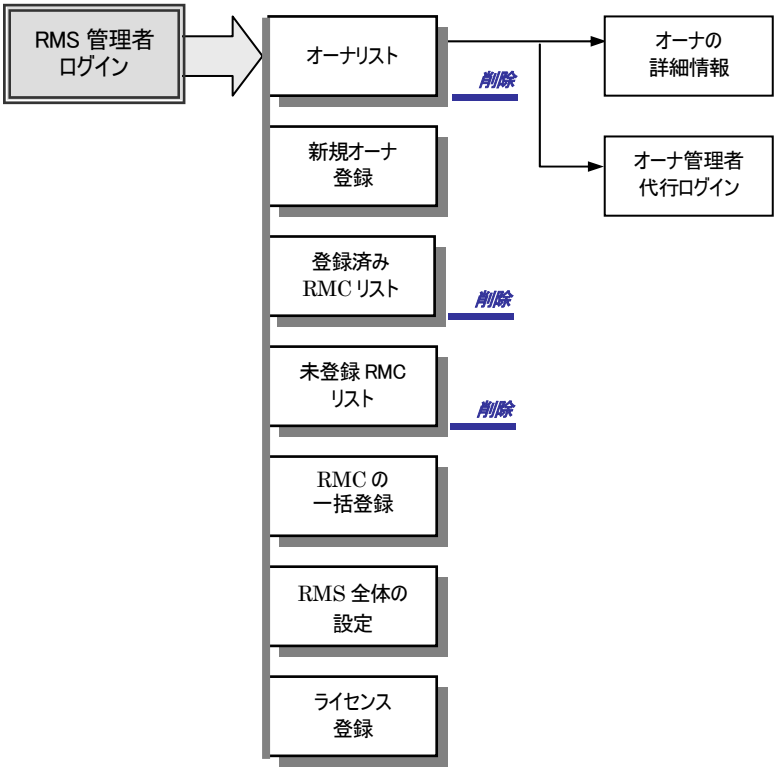
付録

1. メニューと画面構成

RMS 管理者メニュー （RMS 管理者編参照）

メニュー項目	説明	参照先
オーナ管理		
オーナリスト	登録されたオーナを一覧表示する。 ・オーナのアカウントを変更、削除する。	4.2
新規オーナ登録	オーナを新規登録する。	4.1
ＲＭＣ管理		
登録済み RMC リスト	オーナ登録された RMC を一覧表示する。 ・RMC のオーナ登録を抹消する。	5.3
未登録 RMC リスト	未登録の RMC を一覧表示し、オーナ登録する。 ・RMC の登録を抹消する。	5.1 5.4
RMC の一括登録	RMC をオーナに一括登録する。	5.2
ＲＭＳ管理		
RMS 全体の設定	RMS 管理者の登録情報と、RMS の情報を表示する。	2.3
ライセンス登録	RMS のライセンスを登録する。	2.2

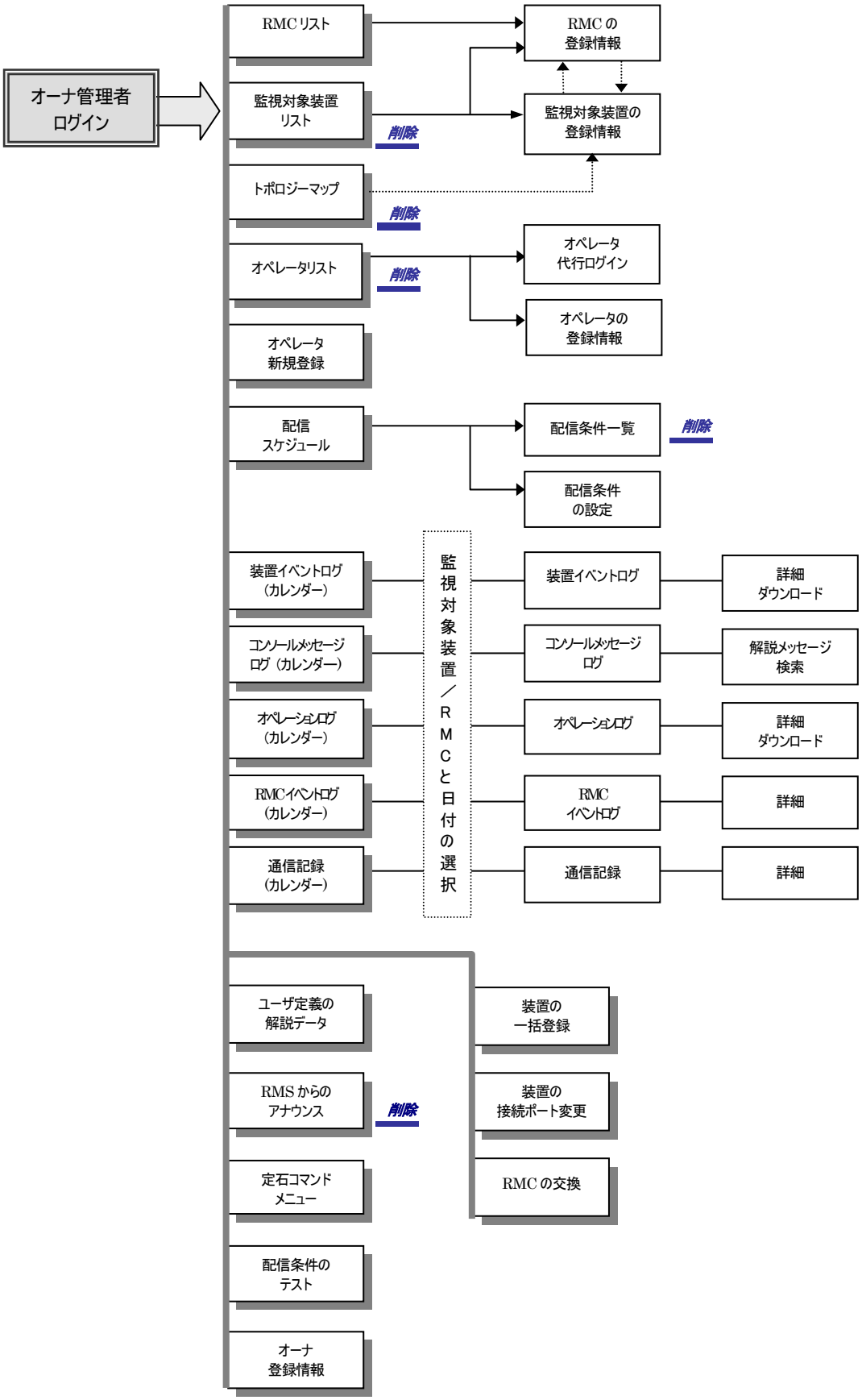
RMS 管理者画面構成


RMS 管理者
ログイン
オーナリスト
削除
オーナの
詳細情報
オーナ管理者
代行ログイン
新規オーナ
登録
登録済み
RMC リスト
削除
未登録 RMC
リスト
削除
RMC の
一括登録
RMS 全体の
設定
ライセンス
登録

オーナ管理者メニュー （オーナ管理者編参照）

	説明	参照先
監視対象装置		
監視対象装置リスト	登録済みの監視対象装置を一覧表示する。 ・監視対象装置の情報を参照／変更・削除する。 監視対象装置ごとに担当オペレータを設定する。	4.5 5.1
RMC リスト	登録済みの RMC を一覧表示する。 ・RMC の設定情報を登録／変更する。 ・監視対象装置を登録する。 RMC を交換する。	4.1 4.2 4.7
トポロジーマップ	トポロジーマップを参照、編集する。	7.2
オペレータ管理		
オペレータリスト	オペレータを一覧表示する。 ・登録済オペレータのアカウント変更、削除する。 オペレータごとに担当する監視対象機器を設定する。	3.2 5.2
オペレータ新規登録	オペレータを新規登録する。	3.1
配信スケジュール	配信スケジュールのカレンダーを表示する。 ・新規配信条件を作成、変更、削除する。 ・既存の設定を利用して配信条件を作成する。	6.2 6.3
監視対象装置のログ		
イベント	監視対象装置に発生した事象のログの参照と詳細確認を行う。	9.2
コンソールメッセージ	監視対象装置から出力されたメッセージのログを参照する。	9.3
オペレーション	RMC を経由して実行した、監視対象装置に対する操作とその結果のログを参照する。	9.4
RMCのログ		
イベント	RMC および RMC と RMS との通信において発生した事象のログを参照する。	9.5
通信記録	RMC－RMS 間で送受信されたすべての通信の記録を参照する。	9.6
ユーティリティ		
装置の一括登録	監視対象装置を一括登録する。	4.4
装置の接続ポート変更	監視対象装置を RMC の別のポートに接続する。	4.6
RMC の交換	RMC を別の RMC と交換する。	4.7
ユーザ定義の解説データ	ユーザ定義の解説データを一覧表示し、編集、削除をする。	10.1
RMS からのアナウンス	RMS からのアナウンスを一覧表示、消去をする。	8.2
定石コマンドメニュー	新規コマンドを登録する。	10.2
配信条件のテスト	設定した配信条件をテストする。	10.3
オーナ登録情報	オーナの登録情報の参照、変更をする。	10.4

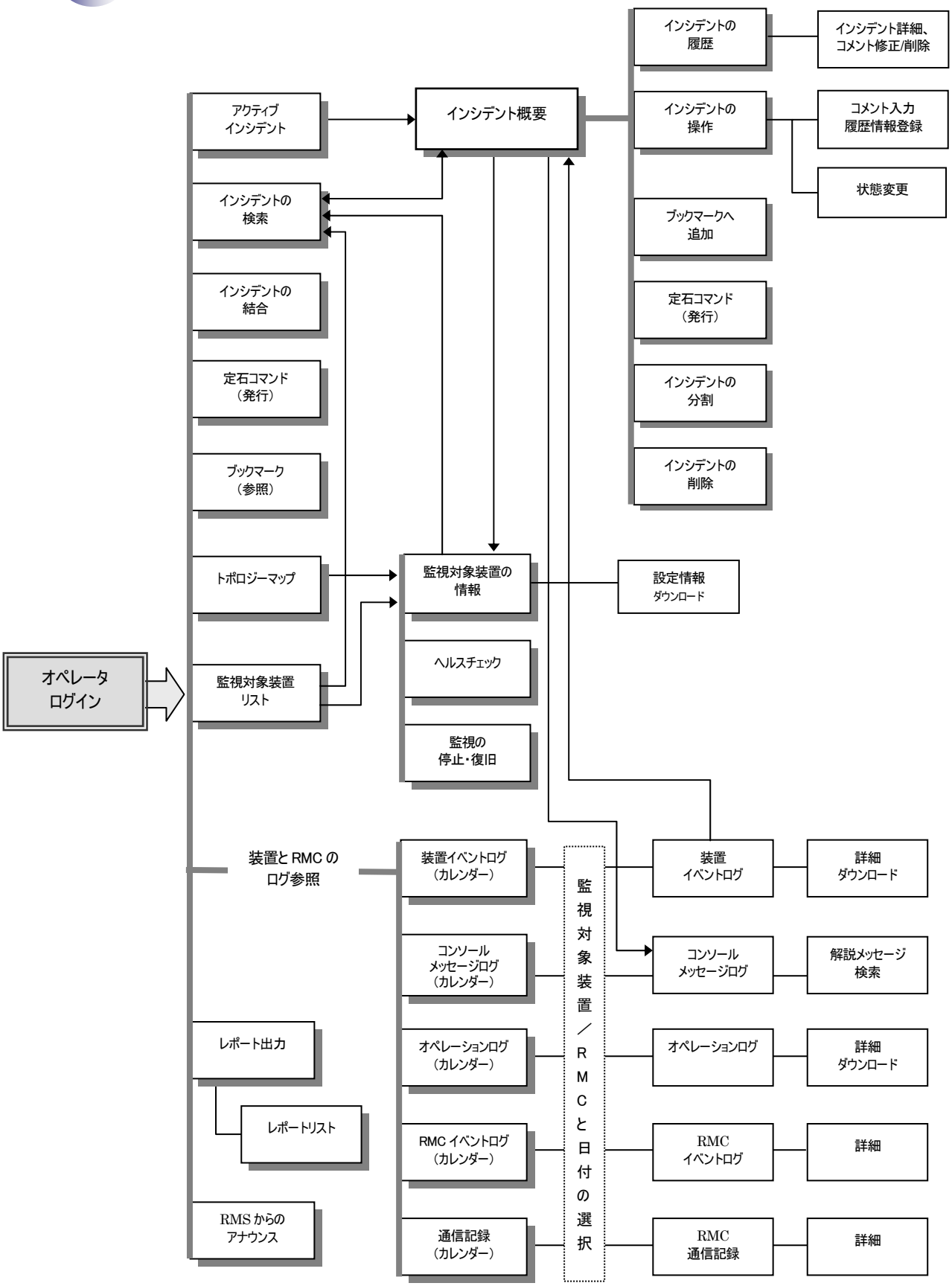
オーナ管理者画面構成


オーナ管理者
ログイン
RMC リスト
監視対象装置
リスト
削除
トポロジーマップ
削除
オペレータリスト
削除
オペレータ
新規登録
配信
スケジュール
RMC の
登録情報
監視対象装置の
登録情報
オペレータ
代行ログイン
オペレータの
登録情報
配信条件一覧
削除
配信条件
の設定
装置イベントログ
（カレンダー）
コンソールメッセージ
ログ（カレンダー）
オペレーションログ
（カレンダー）
RMCイベントログ
（カレンダー）
通信記録
（カレンダー）
監視対象装置／RMCと日付の選択
装置イベントログ
コンソールメッセージ
ログ
オペレーションログ
RMC
イベントログ
通信記録
詳細
ダウンロード
解説メッセージ
検索
詳細
ダウンロード
詳細
詳細
ユーザ定義の
解説データ
RMS からの
アナウンス
削除
定石コマンド
メニュー
配信条件の
テスト
オーナ
登録情報
装置の
一括登録
装置の
接続ポート変更
RMC の交換

オペレータメニュー

メニュー項目	説明	参照先
メインメニュー		
アクティブインシデント	インシデントを一覧表示し、操作対象のインシデントを選択する。	3.1
トポロジーマップ	トポロジーマップを表示し、障害状況を確認する。	3.2
監視対象装置リスト	監視対象装置を一覧表示し、操作対象の監視対象装置を選択する。	3.3
定石コマンド	監視対象装置に対してコマンドを発行する。	3.4
ブックマーク	インシデントへのブックマークを一覧表示し、編集する。	3.5
インシデントの検索	条件を指定してインシデントを検索する。	3.6
インシデントの結合	複数のインシデントを 1 個のインシデントにまとめる。	3.7
RMS からのアナウンス	RMS からオペレータ宛に通知されたアナウンスを表示する。	3.8
レポート出力	ログデータをレポートファイルに出力する。	3.9
レポートリスト	出力されたレポートファイルをダウンロードする。	3.9
監視対象装置のログ		
イベント	監視対象装置に発生した事象のログを参照し、ログの詳細内容を確認する。	4.2
コンソールメッセージ	監視対象装置から出力されたコンソールメッセージのログを参照する。	4.3
オペレーション	RMC を経由して実行した、監視対象装置に対する操作とその結果のログを参照する。	4.4
RMCのログ		
イベント	RMC および RMC と RMS との通信において発生した事象のログを参照する。	4.5
通信記録	RMC－RMS 間で送受信されたすべての通信の記録を参照する。	4.6
監視対象装置		
概要	監視対象装置に関する情報を参照する。	5.1
ヘルスチェック	設定情報の変更履歴を参照する。	5.2
監視の停止・復旧	監視対象装置の監視を停止する期間の予約、および監視再開操作を行う。	5.3
インシデント		
概要	インシデントの概要情報を参照する。	6.1
インシデントの履歴	インシデントの履歴（発生から現在までの経過）を参照する。	6.2
インシデントの操作	インシデントの状態変更やコメントの入力を行う。	6.3
ブックマークへ追加	インシデントをブックマークに追加する。	6.4
定石コマンド	インシデントが発生した監視対象装置にコマンドを発行する。	6.5
インシデントの分割	インシデントを分割する。	6.6
インシデントの削除	インシデントを削除する。	6.7

オペレータ画面構成


オペレータ
ログイン
アクティブ
インシデント
インシデントの
検索
インシデントの
結合
定石コマンド
（発行）
ブックマーク
（参照）
トポロジーマップ
監視対象装置
リスト
インシデント概要
監視対象装置の
情報
ヘルスチェック
監視の
停止・復旧
インシデントの
履歴
インシデントの
操作
ブックマークへ
追加
定石コマンド
（発行）
インシデントの
分割
インシデントの
削除
インシデント詳細、
コメント修正/削除
コメント入力
履歴情報登録
状態変更
設定情報
ダウンロード
装置とRMCの
ログ参照
装置イベントログ
（カレンダー）
コンソール
メッセージログ
（カレンダー）
オペレーションログ
（カレンダー）
RMC イベントログ
（カレンダー）
通信記録
（カレンダー）
監視対象装置／RMCと日付の選択
装置
イベントログ
コンソール
メッセージログ
オペレーションログ
RMC
イベントログ
RMC
通信記録
詳細
ダウンロード
解説メッセージ
検索
詳細
ダウンロード
詳細
詳細
レポート出力
レポートリスト
RMS からの
アナウンス

2. RMS から送信されるメール

RMS からは、インシデントの発生通知のみでなく、RMS が何らかの異常を検知した場合なども管理者やオペレータの作業を促すメールが送信されます。

RMS から送信されるメールには次の種類があります。

メールサブジェクト	内容	通知先
Target Message	監視対象装置からコンソールメッセージが出力され、インシデントが発生したことを通知するメールです。 コンソールメッセージ本文とインシデント番号、メッセージを発生した装置名、障害状況に対する簡単な説明が含まれます。	オペレータ
Keep-Alive Failure	RMS の障害、もしくは RMC－RMS 間のネットワークに何らかの問題が生じたことを通知するメールです。RMC からの Keep-Alive（生存確認）メールが所定の時間内に届かなかった場合に送信されます。 （一時的な輻輳などによるメール到達の遅延の可能性もあります）	オペレータ
Keep-Alive Recovery	Keep-Alive の切断状態が復旧したことを通知します。 切断状態であった RMC からのメールが受信され、正常に動作していることが確認された場合に送信されます。	オペレータ
Target Not Respond	監視対象装置の無応答を通知するメールです。 RMC が実行する監視対象装置の応答確認において、装置の無応答が検知された場合に送信されます。	オペレータ
Target Recovery	無応答だった監視対象装置が復旧したことを通知します。 装置からの応答が確認された場合に送信されます。	オペレータ
Confirmation from RMS	オペレータの新規登録時に、アドレス確認用メールの送付を指定した場合に送信されます。	オペレータ
Topology map construction result	RMS がトポロジーマップの構築を実行した際の実行結果を報告するメールです。	オーナ管理者
Unexpected mail from RMC	RMC から RMS で正常に処理できないメールを受信した場合に送信されるメールです。 RMS の設定に誤りがある可能性がありますので確認してください。	オーナ管理者

3. レポート出力ファイル仕様

ここでは、レポート機能で出力するファイルのフォーマットを示します。
レポート出力の操作については、➡「3.9 レポートの出力とダウンロード」をご覧ください。

全般（全レポート共通）

すべてのレポートに共通するフォーマットを示します。

■ 出力形式

CSV または XML（出力時にユーザが指定）

■ 文字コード

Shift_JIS

■ 1 行目出力内容

レポートの種類、オーナ情報、出力日時
（"レポートの種類","アカウント名","正式名","出力日","出力時刻"）

■ 2 行目以後の出力内容

本文（選択したレポートの種類に依存）

■ 注意事項

・1 フィールド内に改行コードが存在する場合、そのコードが CR+LF であっても LF を出力する。
・データ中にバックスペース・コードが含まれた場合、RMS はこれを自動的に処理し、直前の 1 文字を消去する。
・日付表示形式は、yyyy/mmmm/dd
・時刻表示形式は、HH:mm:ss （24 時間表示）

以降では、「インシデント一覧」、「インシデント詳細」、「設定情報比較」、「コンソールログ」、「オペレーションログ」の順に、出力フォーマットを示します。

インシデント一覧

指定期間内に当該オーナに発生したインシデントと各インシデントの現在の状態を出力する。

■ 出力対象

指定した期間内に当該オーナにおいて発生したインシデントの概要を出力する。

■ 出力順序

インシデント発生順

■ 出力書式

(1 行目)	レポート全体の情報	
	1 列	タイトル (レポートの種類)
	2 列	オーナアカウント名
	3 列	オーナ正式名
	4 列	レポート出力日付
	5 列	レポート出力時刻
(2 行目～最終行)	インシデント情報	
	1 列	ファイル内の通番
	2 列	インシデント番号
	3 列	発生日付
	4 列	発生時刻
	5 列	現在のインシデント状態
	6 列	解決日付 (未解決のインシデントは空欄)
	7 列	解決時刻 (未解決のインシデントは空欄)
	8 列	インシデントの先頭に記録されたコンソールメッセージ

■ 出力例

```
"インシデント一覧","routrek","(株)ルートレック・ネットワークス",2002/09/03,10:30:45
1,"2002-08-30-004",2002/08/30,14:10:24,"解決済",2002/08/31,10:17:36,"%LINK-3-UPDOWN: Interface Ethernet5, changed state to up"
2,"2002-08-30-010",2002/08/30,14:27:08,"解決済",2002/08/31,10:22:51,"%LINK-3-UPDOWN: Interface ATM0, changed state to up"
3,"2002-08-30-015",2002/08/30,14:34:28,"解決済",2002/08/31,10:25:40,"%PIM-1-INVALID_RP_JOIN: Received (*, 224.0.1.24) Join from 157.24.76.2 for invalid RP 193.166.5.252"
4,"2002-08-30-016",2002/08/30,14:36:16,"対処中",,,"%SYS-5-CONFIG_I: Configured from console by vty0 (128.214.248.134)"
5,"2002-08-30-019",2002/08/30,14:52:46,"保留",,,"%SYS-2-MALLOCFAIL: Memory allocation of 18180 bytes failed from 0x601605A0, pool I/O, alignment 0"
6,"2002-09-02-002",2002/09/02,17:18:23,"未着手",,,"Sep  2 17:18:02: %LINK-3-UPDOWN: Interface FastEthernet0/10, changed state to down"
7,"2002-09-03-001",2002/09/03,00:35:36,"解決済",2002/09/03,09:57:57,"Target Not Respond"
8,"2002-09-03-003",2002/09/03,09:55:32,"未着手",,,"[1]%LINK-3-UPDOWN: Interface Serial0, changed state to up"
```

インシデント詳細

指定期間内に当該オーナに発生したインシデントの詳細情報を出力する。

■ 出力対象

指定した期間内に当該オーナに於いて発生したインシデントを対象とし、各インシデントに属するコンソールメッセージ、及び各インシデントの対処作業により発生したイベントの詳細を出力する。

■ 出力順序

インシデント発生順（各インシデント内ではメッセージ、及びイベントの発生順）

■ 出力書式

（1 行目）	**レポート全体の情報**	
	1 列	タイトル（レポートの種類）
	2 列	オーナアカウント名
	3 列	オーナ正式名
	4 列	レポート出力日付
	5 列	レポート出力時刻
（2 行目～最終行）	**インシデント詳細**	
	1 列	インシデント番号
	2 列	インシデント内の通番
	3 列	メッセージ／イベントの発生日付
	4 列	メッセージ／イベントの発生時刻
	5 列	種別（"メッセージ"、もしくはイベントの種別）
	6 列	コンソールメッセージ番号（コンソールメッセージのみ）
	7 列	オペレータ名（イベントのみ、RMS が発行したイベントでは「RMS」）
	8 列	装置名（コンソールメッセージ、及び特定装置に関連するイベントのみ）
	9 列	コンソールメッセージ本文、またはイベントの説明
	10 列	イベント発行時の詳細情報（イベントのみ。コマンド実行結果、コメント入力内容など）

■ 出力例

```
"インシデント詳細","routrek","(株)ルートレック・ネットワークス",2002/09/03,10:54:38
"2002-09-02-002",1,2002/09/02,17:18:23,"メッセージ","2002-09-02-002","C2924XL/COM1","Sep  2
17:18:02: %LINK-3-UPDOWN: Interface FastEthernet0/10, changed state to down","
"2002-09-02-002",2,2002/09/02,17:18:23,"メッセージ","2002-09-02-003","C2924XL/COM1","Sep  2
17:18:03: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/10, changed state to down","
"2002-09-02-002",3,2002/09/02,17:18:28,"メッセージ","2002-09-02-004","C2924XL/COM1","Sep  2
17:18:05: %LINK-3-UPDOWN: Interface FastEthernet0/10, changed state to up","
"2002-09-02-002",4,2002/09/02,17:18:28,"メッセージ","2002-09-02-005","C2924XL/COM1","Sep  2
17:18:06: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/10, changed state to up","
"2002-09-02-002",5,2002/09/02,17:18:23,"インシデント発生","","RMS","C2924XL/COM1","インシデント
2002-09-02-002 が発生しました。","
"2002-09-02-002",6,2002/09/02,17:18:24,"コマンド発行","","RMS","C2924XL/COM1","インシデント発生時のコマ
ンド コマンドを発行しました。タイムアウト時刻は 17:23:24 です。","
"2002-09-02-002",7,2002/09/02,17:19:39,"コマンド結果","","RMS","C2924XL/COM1","17:18:24 に発行したインシ
デント発生時のコマンドをメール経由で実行しました。","
2924XL>
---start of sequence---

---start command result---
---enable---
2924XL>enable

---start command result---
---show tech-support---
2924XL#show tech-support

------------------ show version ------------------

Cisco Internetwork Operating System Software
IOS (tm) C2900XL Software (C2900XL-C3H2S-M), Version 12.0(5.3)WC(1), MAINTENANCE INTERIM SOFTWARE
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Mon 30-Apr-01 07:34 by devgoyal
Image text-base: 0x00003000, data-base: 0x003331F4

ROM: Bootstrap program is C2900XL boot loader
                .
                .
                .
CPU3 buffers, 1524 bytes (total 4, permanent 4):
        2 in free list (0 min, 4 max allowed)
        56941142 hits, 0 misses
CPU4 buffers, 1524 bytes (total 4, permanent 4):
        2 in free list (0 min, 4 max allowed)
        56941141 hits, 0 misses




---start command result---
---disable---
2924XL#disable

---end command result---
"
"2002-09-02-002",8,2002/09/03,10:53:29,"インシデント解決","","田中真理子","接続装置の電源断と再投入によ
る接続異常発生のため、問題なし。対処不要。","
"2002-09-03-001",1,2002/09/03,00:35:36,"メッセージ","2002-09-03-001","185/COM1(Router)","Target Not
Respond","
"2002-09-03-001",2,2002/09/03,00:35:36,"インシデント発生","","RMS","185/COM1(Router)","インシデント
2002-09-03-001 が発生しました。","
"2002-09-03-001",3,2002/09/03,09:57:57,"インシデント解決","","田中真理子","","
"2002-09-03-003",1,2002/09/03,09:55:32,"メッセージ","2002-09-03-003","185/COM1(Router)","%LINK-3-UPD
OWN: Interface Serial0, changed state to up","
                .
                .
                .
```

設定情報比較

監視対象装置の設定情報と前回取得情報との比較履歴を装置ごとに出力する。

■ 出力対象

当該オーナにおいて、指定した期間内に受信した Network Information のログ
（IOS : show running-config、Switch Software : write terminal）

■ 出力順序

装置名順（装置ごとの情報は発生順）

■ 出力書式

（1 行目）	**レポート全体の情報**	
	1 列	タイトル（レポートの種類
	2 列	オーナアカウント名
	3 列	オーナ正式名
	4 列	レポート出力日付
	5 列	レポート出力時刻
（2 行目～最終行）	**設定情報**	
	1 列	ファイル内の通番
	2 列	監視対象装置名
	3 列	Network Information 実行日付
	4 列	Network Information 実行時刻
	5 列	前回の config データ（前回が存在しない場合は空欄）
	6 列	今回の config データ
	7 列	比較結果（0：前回データなし、1：前回と同一、2：差分あり）
	8 列	差分データ（7 列が 2 の場合のみ）

■ 出力例

```
"設定情報比較","Routrek","(株)ルートレック・ネットワークス",2002/02/21,14:11:39
1,"199/IOSswitch/COM1",2002/02/18,00:01:37,"
Building configuration...
                ・
                ・
                ・
4,"199/IOSswitch/COM1",2002/02/18,17:46:39,"
Building configuration...

Current configuration:
!
version 12.0
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Switch
!
no spanning-tree vlan 1
ip subnet-zero
!
interface FastEthernet0/1
!
interface FastEthernet0/2
                ・
                ・
interface FastEthernet0/24
!
interface VLAN1
 ip address 192.168.10.XXX 255.255.255.0
 no ip directed-broadcast
 no ip route-cache
!
no cdp run
!
line con 0
 transport input none
 stopbits 1
line vty 0 4
 password routrek
 login
line vty 5 15
 login
!
end
","Building configuration...

Current configuration:
!
version 12.0
no service pad
service timestamps debug datetime localtime
service timestamps log datetime localtime
no service password-encryption
!
hostname Switch
!
no spanning-tree vlan 1
ip subnet-zero
!
interface FastEthernet0/1
!
interface FastEthernet0/2
                                        (右に続く)
```

```
                ・
                ・
interface FastEthernet0/24
!
interface VLAN1
 ip address 192.168.10.XXX 255.255.255.0
 no ip directed-broadcast
 no ip route-cache
!
no cdp run
!
line con 0
 transport input none
 stopbits 1
line vty 0 4
 password routrek
 login
line vty 5 15
 login
!
end
″,2,″   Building configuration...

  Current configuration:
  !
  version 12.0
  no service pad
+ service timestamps debug datetime localtime
+ service timestamps log datetime localtime
- service timestamps debug uptime
- service timestamps log uptime
  no service password-encryption
  !
  hostname Switch
  !
  no spanning-tree vlan 1
  ip subnet-zero
  !
  interface FastEthernet0/1
  !
  interface FastEthernet0/2
                ・
                ・
  interface FastEthernet0/24
  !
  interface VLAN1
   ip address 192.168.10.XXX 255.255.255.0
   no ip directed-broadcast
   no ip route-cache
  !
  no cdp run
  !
  line con 0
   transport input none
   stopbits 1
  line vty 0 4
   password routrek
   login
  line vty 5 15
   login
  !
  end
″
5,″199/IOSswitch/COM1″,2002/02/18,17:51:31,″Building configuration...
                ・
                ・
```

コンソールメッセージログ

指定期間内に当該オーナの監視対象装置に発生したコンソールメッセージのログを出力する。

■ 出力対象

当該オーナにおいて、指定期間内に記録されたコンソールログ

■ 出力順序

装置名順（装置ごとの情報は発生順）

■ 出力書式

（1 行目）	レポート全体の情報	
	1 列	タイトル（レポートの種類）
	2 列	オーナアカウント名
	3 列	オーナ正式名
	4 列	レポート出力日付
	5 列	レポート出力時刻
（2 行目～最終行）	コンソールメッセージログ	
	1 列	ファイル内の通番
	2 列	監視対象装置名
	3 列	コンソールメッセージ番号
	4 列	コンソールメッセージ発生日
	5 列	コンソールメッセージ発生時刻
	6 列	コンソールメッセージ本文

■ 出力例

```
"コンソールメッセージ","routrek","(株)ルートレック・ネットワークス",2002/09/03,11:38:51
1,"C2924XL/COM1","2002-09-02-002",2002/09/02,17:18:23,"Sep  2 17:18:02: %LINK-3-UPDOWN: Interface
FastEthernet0/10, changed state to down"
2,"C2924XL/COM1","2002-09-02-003",2002/09/02,17:18:23,"Sep  2 17:18:03: %LINEPROTO-5-UPDOWN: Line
protocol on Interface FastEthernet0/10, changed state to down"
3,"C2924XL/COM1","2002-09-02-004",2002/09/02,17:18:28,"Sep  2 17:18:05: %LINK-3-UPDOWN: Interface
FastEthernet0/10, changed state to up"
4,"C2924XL/COM1","2002-09-02-005",2002/09/02,17:18:28,"Sep  2 17:18:06: %LINEPROTO-5-UPDOWN: Line
protocol on Interface FastEthernet0/10, changed state to up"
5,"185/COM1(Router)","2002-09-01-001",2002/09/01,00:35:31,"Target Not Respond"
6,"185/COM1(Router)","2002-09-02-001",2002/09/02,00:35:34,"Target Not Respond"
7,"185/COM1(Router)","2002-09-03-001",2002/09/03,00:35:36,"Target Not Respond"
8,"185/COM1(Router)","2002-09-03-002",2002/09/03,09:55:32,"%LINK-5-CHANGED: Interface Ethernet2,
changed state to administratively down"
9,"185/COM1(Router)","2002-09-03-003",2002/09/03,09:55:32,"%LINK-3-UPDOWN: Interface Serial0, changed
state to up"
                    .
                    .
                    .
```

オペレーションログ

オペレーションログの本文フォーマットを示します。

■ 出力対象

当該オーナにおいて、指定期間内に記録されたオペレーションログ

■ 出力順序

装置名順（装置ごとの情報は発生順）

■ 出力書式

（1 行目）	**レポート全体の情報**	
	1 列	タイトル（レポートの種類）
	2 列	オーナアカウント名
	3 列	オーナ正式名
	4 列	レポート出力日付
	5 列	レポート出力時刻
（2 行目～最終行）	**オペレーションログ**	
	1 列	ファイル内の通番
	2 列	監視対象装置名
	3 列	オペレーション実行日付
	4 列	オペレーション実行時刻
	5 列	オペレーションログ内容

■ 出力例

```
"オペレーションログ","Routrek","(株)ルートレック・ネットワークス",2002/02/21,16:24:15
1,"199/IOSswitch/COM1",2002/02/18,17:39:27,"
Switch>en
Switch#sh runn
Building configuration...

Current configuration:
!
version 12.0
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Switch
!
!
!
no spanning-tree vlan 1
ip subnet-zero
!
!
interface FastEthernet0/1

Switch#conf term
Enter configuration commands, one per line.   End with CNTL/Z.
Switch(config)#ser
Switch(config)#service ti
Switch(config)#service timestamps de
Switch(config)#service timestamps debug d l
Switch(config)#ser
Switch(config)#service ti
Switch(config)#service timestamps l
Switch(config)#service timestamps log d l
Switch(config)#^Z
Switch#
*Apr 28 08:04:41: %SYS-5-CONFIG_I: Configured from console by console
Switch#
Switch#
Switch#
Switch#
Switch#sh runn
Building configuration...

Current configuration:
!
version 12.0
no service pad
service timestamps debug datetime localtime
service timestamps log datetime localtime
no service password-encryption
!
hostname Switch
!
!
!
!
no spanning-tree vlan 1
ip subnet-zero
!
!
interface FastEthernet0/1

Switch#disa
Switch>
---operation end---
"
2,"199/IOSswitch/COM1",2002/02/18,18:07:07,"
Switch>en
Switch#
                .
                .
                .
```

4. 用語集

用　語	説　明
Keep-Alive	RMC が正常に稼動していることを確認する機能。 RMC から RMS に定期的に送信される「Keep-Alive」というサブジェクトのメールが RMS に到着しなかった場合、RMS はこの RMC が正常に動作していないと判断し、「Keep-Alive Failure」というサブジェクトのメールを担当オペレータに送信する。 この状態は、ネットワークの混雑によるメール配送の遅延やネットワーク上の障害などによっても発生する可能性がある。
RMC-ID	RMS が個々の RMC を識別するための値。 この ID には RMC に内蔵されたイーサネットの MAC アドレスが使用される。
RMS からのアナウンス	RMS が生成し、管理者やオペレータに何らかの作業もしくは確認を促すメッセージ。
RMS 管理者	RMS システムの設置と管理／運用に責任を持つ管理者。 RMS 管理者は、RMS を利用するオーナおよびオーナに所属する RMC の登録に責任を持つと同時に、RMS システム全体の管理とメンテナンスを行う。
アカウント名	RMS でオーナやオペレータを一意に識別するために使用する。 アカウント名はログインのたびに入力するため、英数字のみの使用が推奨される。 本名は別途登録でき、そこでは漢字も使用可能。
アクティブ インシデント	オペレータの対処を必要とするインシデント。 状態が「未着手」もしくは「対処中」のインシデントを指す。
イベントログ	特定の監視対象装置、またはそれに接続された RMC で発生したすべての事象に関する時系列的な履歴。
インシデント	監視対象装置から一定のレベル以上の重要度（Severity Levels）を持つコンソールメッセージを受信した場合に発生する。重要度の高いメッセージを連続的に受信した場合、これらは 1 インシデントとして扱われる。 重要度を示すフィールドは 0 から 7 までの値があり、0 が最も重要度の高い問題であることを示す。（一般機器ではこの値は無効であり、全メッセージをインシデントの発生対象とする、もしくはインシデントを発生させないの選択が可能） デフォルトでは 0 から 4 までの重要度を持つメッセージをインシデント発生要因とするが、より重要度の低いメッセージもインシデントとして処理するように設定できる。 重要度はオーナ管理者によって設定され、監視対象装置ごとに設定できる。
オーナ	RMC を使用してネットワークシステムの監視・管理業務を行う 1 つの企業あるいは組織単位。RMS では、複数オーナによる複数ネットワークシステムを同時に管理できる。
オーナ管理者	RMS が管理する企業や組織（オーナ）の代表者であり、1 つの RMS 上で複数のオーナを管理する場合は、各々にオーナ管理者を設定する。 オーナ管理者は、各オーナに属するアカウントの管理に責任を持ち、実際にネットワークの監視・メンテナンスを行うオペレータの登録や各オペレータが担当する RMC との関連付け、ならびに RMS が送信するメールの配信条件などを設定する。
オペレーションログ	RMC 経由で監視対象装置にログインして行った操作と、その結果の履歴。

（次ページに続く）

（前ページから続き）

用　語	説　明
オペレータ	実際にネットワークの監視・メンテナンスを行う担当者。 オペレータは一つのオーナに所属し、そのオーナが所有する RMC と、RMC に接続された監視対象装置を管理する。
解説メッセージ	RMS に予め登録されている、監視対象装置のコンソールメッセージに対する説明と対処法。
監視対象装置	RM C が接続されているネットワーク機器。
監視の停止・復旧	監視対象装置の定期メンテナンスや保守点検のための停電など、あらかじめ、監視対象装置の停止が予定されている場合に、一時的に監視対象から外す機能。 RMS は、停止中の監視対象装置に関するオペレータへのメール通知、および Keep-Alive チェックを停止するが、この間に RMC から受信されたメールは各種のログとして RMS に記録される。
コメント	インシデントに対処する過程で、任意に追加できる対処履歴情報。 RMS が自動的に作成する履歴として残らない対処措置や、将来の問題解決に役立てたい情報をコメントとして記録し、他のオペレータと共有することができる。 コメントは、同様のインシデント発生時に自動表示されるよう指示できる。
コンソールメッセージ	監視対象装置がコンソールポートに出力するメッセージ。
コンソール メッセージログ	監視対象装置のコンソールポートのから出力されたコンソールメッセージの履歴。 RMC で設定されたフィルタを通過したデータのみが記録される。
閾値	インシデント発生条件の指定要素。特定のメッセージが指定された以上の頻度で発生した場合に、これをインシデントとみなす。
定石コマンド	RMS 上で事前定義される監視対象装置に対するコマンド。 定石として定義されたコマンドは、定石コマンドのメニュー選択によりボタン操作で実行可能となる。RMS 対応機種に関しては、RMS がデフォルトの定石コマンドを提供する。
代行ログイン	上位の管理者が下位ユーザの操作を代行するために、ユーザの代わりにログインすること。UNIX の su コマンドと近い意味合いを持つ。 RMS 管理者はオーナ管理者もしくはオペレータとして、オーナ管理者はオペレータとして代行ログインし、管理者もしくはオペレータの作業を代行できる。
担当オペレータ	RMC およびそれに接続された監視対象装置を監視・メンテナンスする責任者。RMC と監視対象装置の操作は、担当オペレータのみが行う。 ただし、非担当オペレータでも、同一オーナ内であれば、担当外の監視対象装置に関するメールの受信、および履歴情報の参照などは可能。
通信記録	RMC－RMS 間で送受信されたすべてのメール、および SSH を使用して RMC に発行したコマンドとその実行結果のログ。（主に、RMS のサポート目的で利用される。）
トポロジーマップ	RMC を経由して監視対象装置から取得された情報に基づいて、RMS が自動生成するネットワークのトポロジー表示機能。
配信スケジュール	RMS からオペレータに対して配信されるメールの送信条件と宛先を設定する機能。オーナ単位で管理される。 メールの宛先は、監視対象装置からのメッセージ内の重要度（一般機器を除く）とキーワード、および時間帯に応じて設定できる。「Keep-Alive Failure」のように RMS が生成するメッセージは、重要度・キーワードの条件設定にかかわりなく、当該スケジュールに指定されたすべての宛先に送付される。

（次ページに続く）

（前ページから続き）

用　語	説　　明
ブックマーク	頻繁にアクセスするインシデントを検索せずに参照できるようにする機能。
プラグイン	特定の監視対象装置に対して、RMS 対応製品としての付加機能を提供する。
ヘルスチェック	監視対象装置の設定情報の変化を確認する機能。 この機能は、RMC が監視対象装置に対して定期的に所定のコマンドを発行し、収集したデータに基づいて実行される。（RMS 対応製品でのみ利用可能。）
レポート	RMS で管理しているログデータを、CSV もしくは XML 形式でファイルに保存し、定期レポートの作成データとして利用する機能。

製品に関するお問い合わせ

製品に関するお問い合わせやテクニカルサポートについては、下記の弊社サポートページをご覧ください。

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

また、製品に関する最新情報やマニュアルも上記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。

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