Catalyst 6500 シリーズ Network Analysis Module インストレーション コンフィギュレーション ノート

WS-SVC-NAM-1
WS-SVC-NAM-2

このマニュアルでは、Catalyst 6500 シリーズ Network Analysis Module（NAM; ネットワーク解析モジュール）のインストレーション手順と、Catalyst CLI（コマンドライン インターフェイス）、NAM Traffic Analyzer アプリケーション、またはその両方を使用して NAM を設定する手順について説明します。スイッチのソフトウェア設定についての詳細は、「関連資料」（p.85）を参照してください。

このマニュアルでは、WS-X6380-NAM については説明しません。WS-X6380-NAM については、『*Catalyst 6000 Family Network Analysis Module Installation and Configuration Note*』ソフトウェア リリース 2.1 を参照してください。

（注） このマニュアルに記載されている警告の各国語版は、「安全性に関する概要」（p.8）および Catalyst 6500 シリーズ スイッチの『*Regulatory Compliance and Safety Information*』を参照してください。

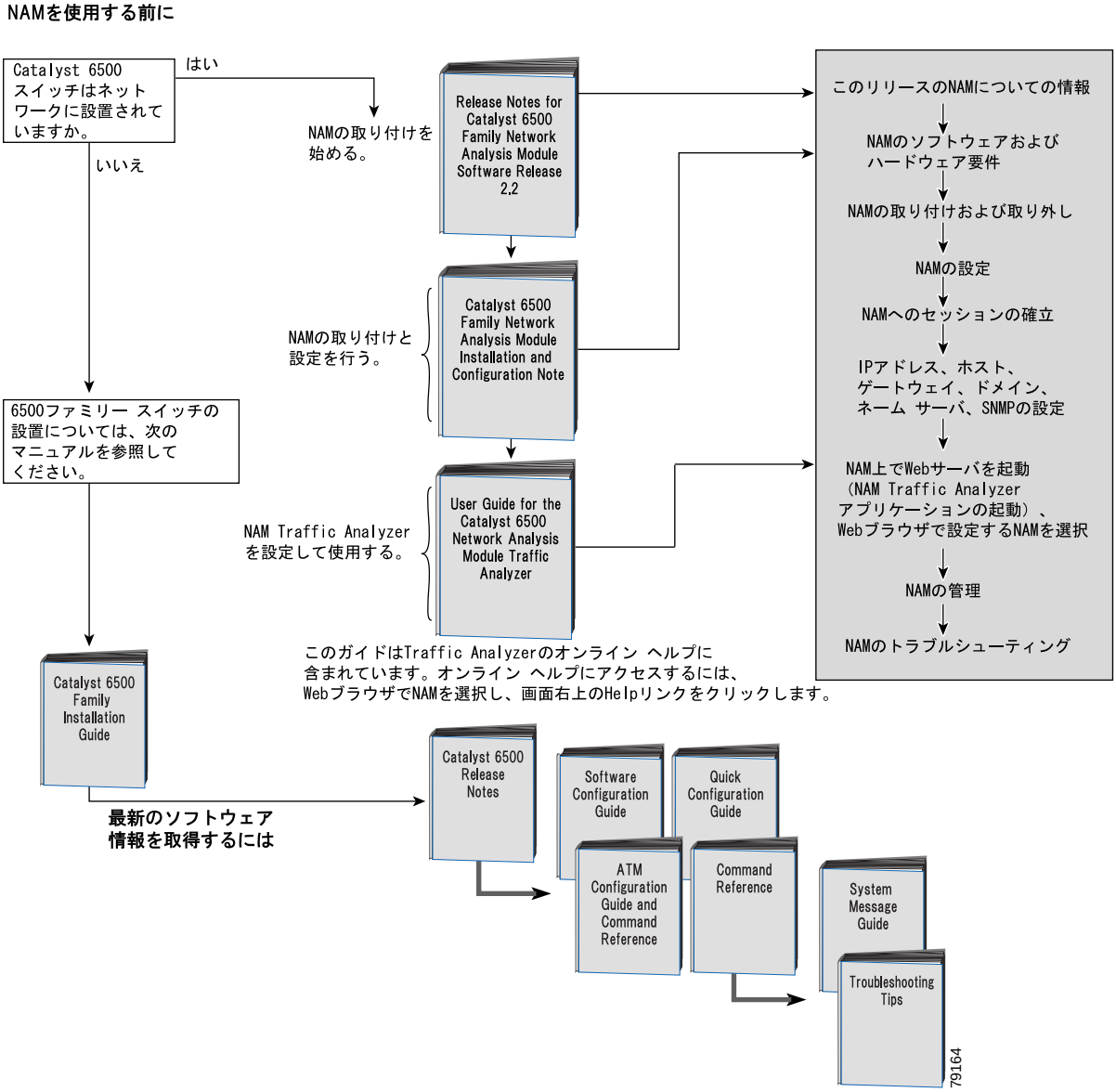
（注） Network Analysis Module ソフトウェア リリース 2.2(1a) には、ライセンス許諾されたサードパーティ製ソフトウェアが含まれています。ライセンスに関する注意事項およびこのようなサードパーティ製ソフトウェアの使用に関する注意事項は、『*Release Notes for Catalyst 6500 Family Network Analysis Module*』ソフトウェア リリース 2.2(1a) に記載されています。

目次

このマニュアルで説明する内容は、次のとおりです。

はじめに

NAM の使用を開始する前に、以下のロードマップを参照してください。



概要

ここでは、Catalyst 6500 シリーズおよび Catalyst 6000 ファミリーの NAM の機能および管理方法について説明します。内容は次のとおりです。

NAM の機能

NAM は、Remote Monitoring（RMON）、スイッチド ネットワーク用の RMON 拡張機能（SMON）、およびその他の Management Information Base（MIB; 管理情報ベース）を使用して、Catalyst 6500 シリーズおよび Catalyst 6000 ファミリー スイッチのネットワーク トラフィックのモニタと解析を行います。NAM がサポートする RMON グループは、次のとおりです。

- RFC 1757 で定義されている RMON グループ
- RFC 2021 で定義されている RMON2 グループ

NAM には、個々のイーサネット VLAN をモニタする機能もあります。この機能によって Catalyst 6500 シリーズおよび Catalyst 6000 ファミリーのスーパバイザ エンジンが提供する基本的な RMON サポートが拡張されます。

他の IETF 準拠 RMON アプリケーションを使用することにより、リンク、ホスト、プロトコル、および応答時間に関する統計情報にアクセスできます。これらの情報は、キャパシティ プランニング、部門別アカウンティング、およびリアルタイムでのアプリケーション プロトコルのモニタリングに役立ちます。さらに、フィルタおよびキャプチャ バッファを使用してネットワークのトラブルシューティングを行うこともできます。

NAM は、次のソースの一方または両方を使用してイーサネット VLAN トラフィックを解析できます。

- イーサネット、ファスト イーサネット、ギガビット イーサネット、トランク ポート、または Fast EtherChannel SPAN/RSPAN 送信元ポート。

  SPAN および RSPAN の詳細は、『*Catalyst 6000 Family Software Configuration Guide*』の「Configuring SPAN and RSPAN」を参照してください。
- Netflow Data Export（NDE; Netflow データ エクスポート）。

  NDE についての詳細は、『*Catalyst 6000 Family Software Configuration Guide*』を参照してください。

NAM の管理

NAM を管理および制御するには、NAM に組み込まれた Web ベースの NAM Traffic Analyzer アプリケーション（NAM から Web ブラウザを起動）、または CiscoWorks2000 にバンドルされているような SNMP（簡易ネットワーク管理プロトコル）管理アプリケーションのいずれか一方または両方を使用します。

NAM Traffic Analyzer アプリケーションを使用すると、Web ブラウザを通じて NAM のデータ / 音声トラフィック管理機能およびモニタ機能にアクセスできます。NAM Traffic Analyzer アプリケーションを使用するには、最初に CLI を使用して NAM の基本設定を行う必要があります。その後は、1 つのコマンドで NAM Traffic Analyzer アプリケーションを起動できるようになります。

NAM Traffic Analyzer を使用して、次の作業を行うことができます。

- SPAN リソースの設定
- 収集の設定
- 統計情報のモニタ
- パケットのキャプチャおよびデコード
- アラームの設定および表示

セキュリティを強化するには、NAM Traffic Analyzer アプリケーションを使用して、NAM がリモート TACACS+ サーバを使用するように設定します。TACACS+ サーバを使用して Web ベース ユーザの認証および許可を行うことができます。また、NAM 上のローカル データベースを使用してセキュリティを確保することもできます。

Cisco NetScout nGenius Real-Time Monitor（RTM）などの SNMP 管理アプリケーションを使用して、NAM を管理することもできます。RTM の詳しい使用方法については、CiscoWorks2000 のマニュアルまたは以下の URL を参照してください。

http://www.Cisco.com/univercd/cc/td/doc/product/lan/cat6000/fam_mod/rel2_1_2/ol_2428.htm

RMON および SNMP エージェント サポートを使用するには、CLI を使用して NAM を設定します。

すでにスイッチ上で NAM を設定し稼働させていて、NAM の使用手順を熟知している場合は、**ip http server enable** CLI コマンドを入力してブラウザで NAM Traffic Analyzer を起動し、NAM Traffic Analyzer アプリケーションの使用を開始できます。

NAM Traffic Analyzer アプリケーションの詳しい使用方法については、『*User Guide for the Catalyst 6500 Network Analysis Module Traffic Analyzer*』を参照してください。

NAM の新機能

ソフトウェア リリース 2.2 を使用する NAM-1 および NAM-2 プラットフォームの新機能は以下のとおりです。

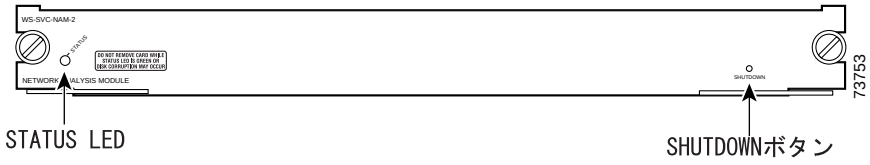
- 新しい高性能な NAM-1 および NAM-2 ハードウェア プラットフォームがサポートされます。新しいプラットフォームにはバスベース アーキテクチャへのインターフェイスと Catalyst 6500 シリーズ スイッチのクロスバーベース アーキテクチャへのインターフェイスが装備されています。
- 最大 100 の未知のプロトコルの自動検出が可能です。これにより、帯域幅を消費しているアプリケーションを識別できます。
- 特定のアプリケーションが稼働しているホストを識別することによりトラフィック　ソースを隔離できます。
- DiffServ Code Point（DSCP）によるホストとアプリケーションの相関機能によって、Quality of Service（QoS; サービス品質）違反の識別機能が向上しています。
- NAM Traffic Analyzer アプリケーションの GUI が強化されています。たとえば、**Setup->SPAN Sources** メニューが変更されています。
- メンテナンス イメージがコンパクト フラッシュに保存されており、アプリケーション イメージがハードディスクに保存されているので、ハードディスクをフォーマットして再度取り付けることができます。
- Secure Shell（SSH）のサポートにより、CLIの使用によるNAMへのセキュア アクセスが可能です。
- CLI 自動入力によって使いやすさが向上しています。
- 別途ライセンスを取得しなくても、NAM を通じて Mini-RMON を使用できます。

（注） WS-X6380-NAM ハードウェア プラットフォームは NAM ソフトウェア リリース 2.2 をサポートしていません。

前面パネル

NAM の前面パネル（図 1）には、STATUS LED と SHUTDOWN ボタンが 1 つずつあります。

図 1　Network Analysis Module



STATUS LED

STATUS LED は、NAM の動作状態を表します（表 1 を参照）。

表 1　STATUS LED の説明

色	説明
グリーン	すべての診断テストにパスしました — NAM は動作可能です。
レッド	個別ポート テスト以外の診断テストに失敗しました。
オレンジ	次の 3 つの条件のいずれかを表します。 • NAM は起動およびセルフテスト診断シーケンスの実行中です。 • NAM はディセーブルです。 • NAM はシャットダウン ステートです。
消灯	NAM の電源がオフです。

SHUTDOWN ボタン

注意 NAM が完全にシャットダウンし、STATUS LED がオレンジになるまで、スイッチから NAM を取り外さないでください。完全にシャットダウンしないうちにスイッチから NAM を取り外すと、NAM が故障する場合があります。

NAMハードディスクの損傷を防ぐには､NAMを正しくシャットダウンした後にシャーシからNAMを取り外すか、または電源を切断する必要があります。このシャットダウン手順は通常、スーパバイザ エンジン CLI プロンプトまたは NAM CLI プロンプトでコマンドを入力して開始します。

NAM がこれらのコマンドに正常に応答しない場合は、前面パネルの SHUTDOWN ボタンを使用してシャットダウン手順を始める必要があります。小さくて先の尖ったもの（例えば、クリップなど）を使用して、このボタンを押します。

シャットダウン手順の完了には、数分かかることがあります。NAM がシャットダウンすると、STATUS LED が消灯します。

仕様

表 2 に、NAM の仕様を示します。

表 2　WS-SVC-NAM-1 および WS-SVC-NAM-2 の仕様

仕様	説明
寸法（高さ × 幅 × 奥行）	1.2×14.4×16 インチ（3.0×35.6×40.6 cm）
重量	最小：3 ポンド（1.36 kg） 最大：5 ポンド（2.27 kg）
環境条件	
動作時の温度	32 ～ 104°F（0 ～ 40°C）
非動作時の温度	–40 ～ 158°F（–40 ～ 70°C）
湿度	10 ～ 90%（結露しないこと）
湿度 — 周囲（結露しないこと）非動作時および保管時	5 ～ 95%
高度	海抜 10,000 フィート（3,050 m）以下

安全性に関する概要

誤って行うと危害が生じる可能性がある操作については、安全上の警告が記載されています。

その他の安全上の注意事項については、「関連資料」（p.85）に記載されている資料を参照してください。

警告

「危険」の意味です。人身事故を予防するための注意事項が記述されています。機器の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止対策に留意してください。

警告

この装置の設置、交換、または保守は、訓練を受けた相応の資格のある人が行ってください。

ソフトウェアの要件

表 3 に、Catalyst OS および Cisco IOS ソフトウェアでサポートされる NAM ソフトウェア バージョンを示します。

表 3　NAM ソフトウェアの互換性

アプリケーション イメージ	メンテナンス イメージ	Catalyst OS ソフトウェア	Cisco IOS ソフトウェア	サポート対象のブラウザ
2.2(1a)	1.1(1)m	7.3(1) 以上のリリース（Supervisor Engine 1A または 2 を使用）	12.1(13)E 以上のリリース（MSFC2 搭載の Supervisor Engine 2 を使用）	Netscape 4.7（Windows 2000 および Solaris を使用） Internet Explorer 5.0 以上（Windows 2000 を使用）

ハードウェアの要件

表 4 に、Catalyst OS および Cisco IOS ソフトウェアでサポートされる NAM ハードウェア バージョンを示します。

表 4　NAM ソフトウェアの互換性

Catalyst OS ソフトウェア	Cisco IOS ソフトウェア
Supervisor Engine 1A または 2	MSFC2 搭載の Supervisor Engine 2

必要な工具

（注） NAM を取り付ける前に、Catalyst 6500 シリーズおよび Catalyst6000 ファミリー スイッチのシャーシを設置し、少なくとも 1 台はスーパバイザ エンジンを搭載しておく必要があります。スイッチシャーシの設置については、『*Catalyst 6000 Family Installation Guide*』を参照してください。

Catalyst 6500 シリーズおよび Catalyst 6000 ファミリー スイッチに NAM を取り付けるには、次の工具が必要です。

- マイナス ドライバ
- プラス ドライバ
- 静電気防止用リスト ストラップまたはその他のアース デバイス
- 静電気防止用マットまたは静電気防止用フォーム

NAM を扱う場合は、必ずリスト ストラップまたはその他のアース デバイスを着用し、ESD（静電気放電）を防止してください。

NAM の取り付けおよび取り外し

警告　次の手順を実行する際には、静電気防止用リスト ストラップを着用して、カードに ESD 破壊が発生しないようにしてください。手や金属製の工具などで直接バックプレーンに触れないでください。感電する可能性があります。

Catalyst 6500 シリーズおよび Catalyst 6000 ファミリー スイッチは、いずれもホットスワップ対応なので、システムの電源を切らずに、モジュールの取り付け、取り外し、交換、または配置変更を行うことができます。スイッチから NAM を取り外す場合の詳細については、「モジュールの取り外し」（p.11）を参照してください。

注意　NAM を取り外す際には、その前に NAM をシャットダウンしてください。

システムは、モジュールの搭載または取り外しを検出すると、診断およびディスカバリ ルーチンを自動的に実行し、モジュールの有無を認識して、システム動作を再開します。

NAM を取り付けて使用するために必要な作業は、次のとおりです。

- スイッチに NAM を取り付けて、基本的なインストレーションを行います。
- スイッチ CLI で、NAM CLI へのセッションを確立し、基本的なコンフィギュレーションを行います。
- NAM にデータ ソースを送信します（Netflow データ、Switched Port Analyzer[SPAN; スイッチド ポート アナライザ] ポート、VLAN、または EtherChannel）。
- モニタの対象とする収集タイプを設定します（ネットワークの要件に応じて、RMON、音声、アプリケーション応答時間など）。
- アラームを設定します。
- モニタされた統計情報およびアラームを表示し、パケット キャプチャ機能またはデコード機能を使用します。

ここでは、Catalyst 6000 ファミリー スイッチに NAM を取り付けて動作を確認する手順について説明します。具体的な内容は、次のとおりです。

スロットの割り当て

Catalyst 6006 および 6506 スイッチ シャーシは 6 スロット、Catalyst 6009 および 6509 スイッチ シャーシは 9 スロット、Catalyst 6513 スイッチ シャーシは 13 スロットです。このモジュールは、Catalyst 6500 シリーズおよび Catalyst 6000 ファミリーのシャーシ内のどのスロットにも搭載できます。

（注）　Catalyst 6509-NEB スイッチは、スロットが縦に並んでおり、右から順に 1 ～ 9 の番号が付けられています。コンポーネント側を右に向けて、モジュールを搭載します。

- スロット 1 は、スーパバイザ エンジン用です。
- スロット 2 には、スロット 1 のスーパバイザ エンジンが故障した場合に備えて、冗長スーパバイザ エンジンを追加できます。
- 冗長スーパバイザ エンジンが不要の場合は、6 スロット シャーシではスロット 2 ～ 6（9 スロット シャーシではスロット 2 ～ 9、13 スロット シャーシではスロット 2 ～ 13）に、NAM などのスイッチング モジュールを搭載できます。
- 空のスロットには、スイッチ シャーシ全体のエアフローが一定になるように、スイッチング モジュール用フィラー プレート（ブランクのスイッチング モジュール フレーム）を取り付けてください。

モジュールの取り外し

ここでは、既存のモジュールをシャーシ スロットから取り外す手順を説明します。

警告　次の手順を実行する際には、静電気防止用リスト ストラップを着用して、カードに ESD 破壊が発生しないようにしてください。手や金属製の工具などで直接バックプレーンに触れないでください。感電する可能性があります。

警告　システムの設置、操作、またはメンテナンスを行う前に、『*Site Preparation and Safety Guide*』を参照してください。このマニュアルには、システムを扱う前に理解しておく必要がある安全に関する重要な情報が記載されています。

警告　接続されていない光ファイバ ケーブルやコネクタからは目に見えないレーザー光が放射されている可能性があります。レーザー光を凝視したり、光機器を直視したりしないでください。

スーパバイザ エンジンまたはモジュールをシャーシから取り外す手順は、次のとおりです。

ステップ 1　スーパバイザ エンジンまたはモジュールに接続されているネットワーク インターフェイス ケーブルを外します。

（注）　NAM にはインターフェイス ケーブル用のコネクタはありません。

ステップ 2　シャーシに搭載されているすべてのモジュールの非脱落型ネジが締められていることを確認します。

この確認が必要なのは、モジュールが取り外された空きスロットのスペースが狭くならないようにするためです。

（注）　非脱落型ネジが緩んでいると、搭載されているモジュールの EMI（電磁波干渉）ガスケットによって、モジュールが空スロットの方に押され、空スロットのスペースが狭くなり、モジュールの再取り付けが難しくなります。

ステップ 3 スーパバイザ エンジンまたはモジュールの 2 つの非脱落型ネジを緩めます。

ステップ 4 シャーシ スロットの形状（水平型または垂直型）に応じて、次のいずれかの手順を行います。

水平型スロット

a. 左右のイジェクト レバーに親指をかけて同時に外側に開き、バックプレーン コネクタからモジュールを外します。

b. モジュールの前面の端を持ち、モジュールをスロットから少し引き出します。もう片方の手をモジュールの下に添えて、モジュールの重さを支えます。モジュールの回路には触れないように注意してください。

垂直型スロット

a. モジュールの上下のイジェクト レバーに親指をかけて同時に外側に開き、バックプレーン コネクタからモジュールを外します。

b. モジュールの端を持ち、モジュールをスロットからまっすぐ引き出します。モジュールの回路には触れないように注意してください。

ステップ 5 静電気防止用マットまたはフォームの上に、取り外したモジュールを置くか、すぐに別のスロットに取り付けます。

ステップ 6 スロットを空のままにしておく場合は、シャーシに埃が入らないように、また、シャーシ全体の空気の流れを適切に保つために、モジュール用フィラー プレートを取り付けます。

警告 ブランクの前面プレート（フィラー パネル）には、3 つの重要な役割があります。シャーシ内部の危険な電圧や電流に触れるのを防ぐこと、他の機器に悪影響を与える EMI を外に出さないようにすること、そしてシャーシ全体に冷気を行き渡らせることです。カードと前面プレートがすべて取り付けられるまで、システムを稼働させないでください。

モジュールの取り付け

ここでは、Catalyst 6500 シリーズおよび Catalyst 6000 ファミリー スイッチにモジュールを取り付ける手順を説明します。

注意 ESD 破壊を防ぐため、モジュールは必ずフレームの縁を持つようにしてください。

警告 次の手順を実行する際には、静電気防止用リスト ストラップを着用して、カードに ESD 破壊が発生しないようにしてください。手や金属製の工具などで直接バックプレーンに触れないでください。感電する可能性があります。

警告 接続されていない光ファイバ ケーブルやコネクタからは目に見えないレーザー光が放射される可能性があります。レーザー光を凝視したり、光機器を直視したりしないでください。

警告　システムの設置、操作、またはメンテナンスを行う前に、『*Site Preparation and Safety Guide*』を参照してください。このマニュアルには、システムを扱う前に理解しておく必要のある安全に関する重要な情報が記載されています。

スーパバイザ エンジンまたはモジュールをシャーシに取り付ける手順は、次のとおりです。

ステップ 1　スーパバイザ エンジンまたはモジュールを搭載するスロットを決めます。

ステップ 2　スーパバイザ　エンジンまたはモジュールのポートにインターフェイス装置を接続できるだけの隙間があるかどうか確認します。モジュールはなるべく、フィルタ プレートだけが取り付けられている空スロットの間のスロットに取り付けてください。

ステップ 3　シャーシに搭載されているすべてのモジュールの非脱落型ネジが締められていることを確認します。

この確認が必要なのは、非脱落ネジによってすべてのモジュールの EMI ガスケットがしっかり圧迫されていないと、新しいモジュールや交換用のモジュールを取り付ける空スロットのスペースが狭くなるためです。

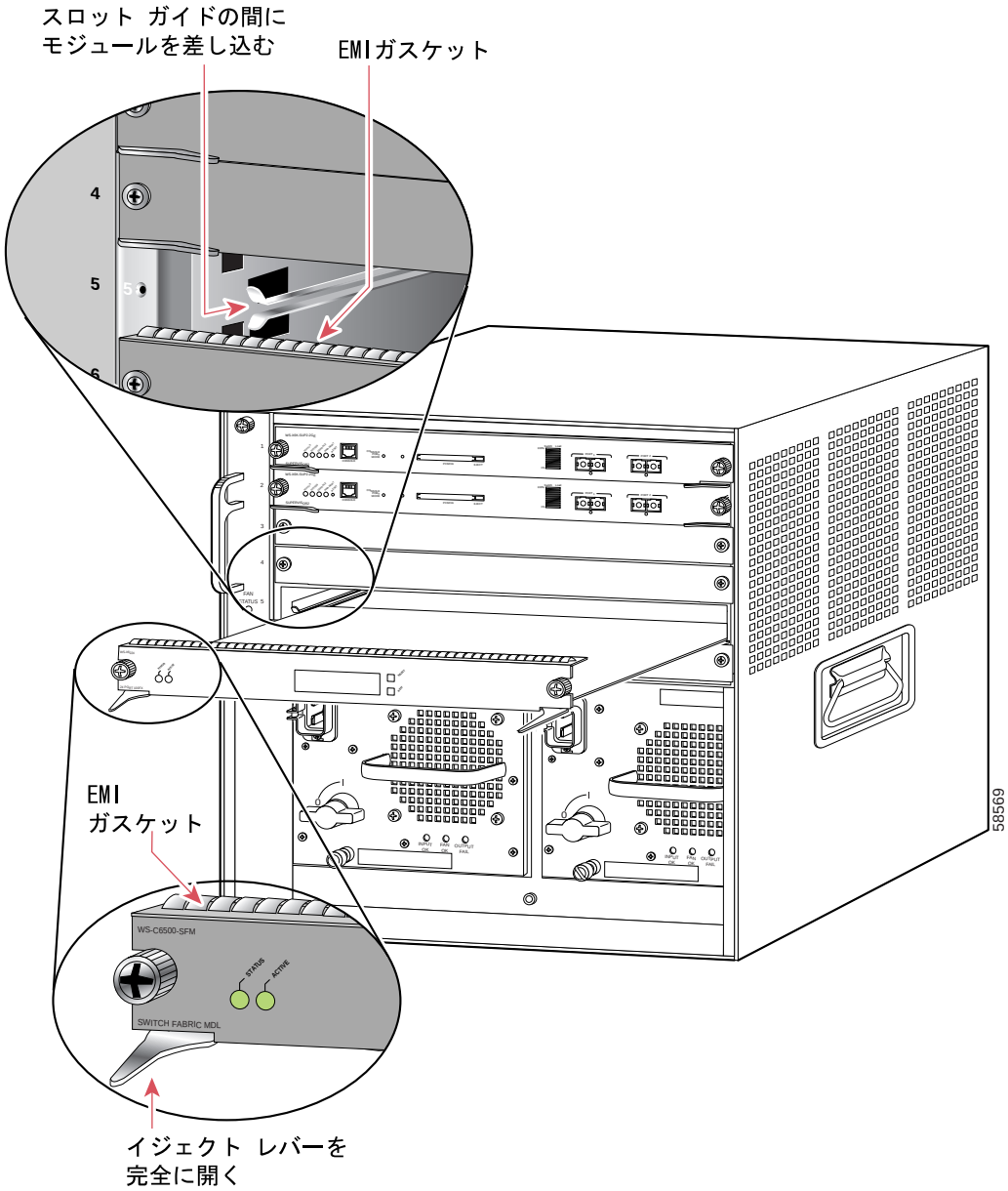
（注）　非脱落型ネジが緩んでいると、搭載されているモジュールの EMI ガスケットによって隣接するモジュールが空スロットの方に押され、空スロットのスペースが狭くなり、モジュールの再取り付けが難しくなります。

ステップ 4　モジュール フィラー プレートから 2 つのなべネジを取り外し、フィラー プレートを外します。

モジュールを取り外す場合は、「モジュールの取り外し」（p.11）を参照してください。

ステップ 5　新しいモジュールまたは交換用のモジュールの両側のイジェクト レバーを完全に開きます（図 2 を参照）。

図 2　　水平型スロット シャーシへのモジュールの取り付け



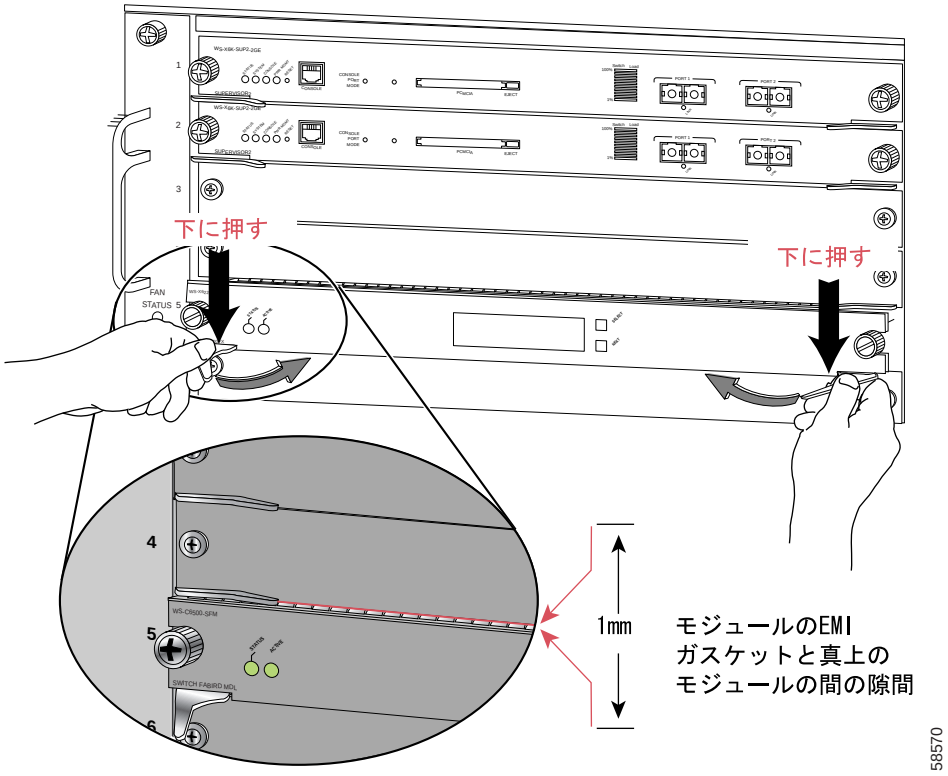
ステップ 6　シャーシ スロットの形状（水平型または垂直型）に応じて、次のいずれかの手順を行います。

水平型スロット

a. スーパバイザ エンジンまたはモジュールをスロットの位置に合わせます（図 2 を参照）。モジュールのフレームの両側面をスロットの両側にあるスロット ガイドに合わせてください。

b. スーパバイザ エンジンまたはモジュールを慎重にスロットに差し込み、モジュール上端の EMI ガスケットが真上に搭載されているモジュールに触れたら、両側のイジェクト レバーをモジュールの前面プレートに対して約 45 度の角度になるまで内側に倒します（図 3 を参照）。

図 3　　水平型スロット シャーシの EMI ガスケットの調整

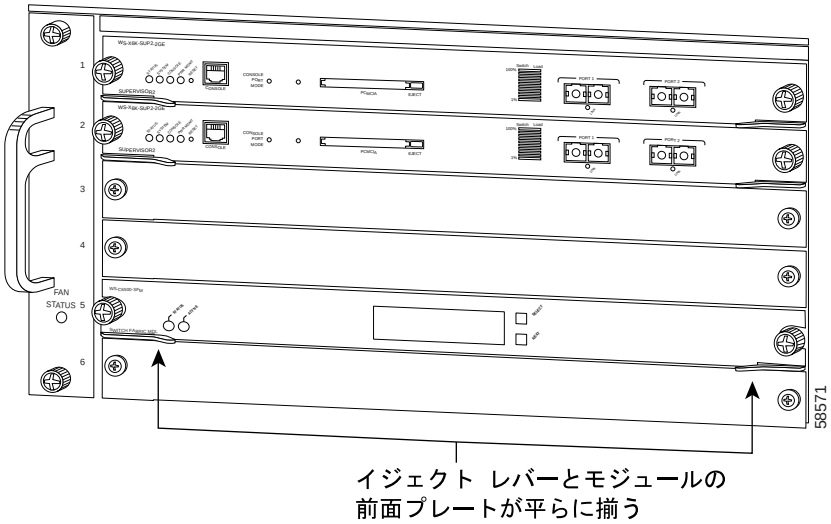


c. 両手の親指と人差し指で 2 つのイジェクト レバーを押し下げて、モジュールの EMI ガスケットと真上のモジュールの間にわずかな隙間（0.040 インチ [1 mm]）をつくります（図 3 を参照）。

注意　レバーを押し下げる力が強すぎると、レバーが曲がったり壊れたりすることがあるので注意してください。

d. 左右のイジェクト レバーを押し下げたまま、同時に内側に閉じます。これによって、スーパバイザ エンジンまたはモジュールがバックプレーン コネクタに完全に装着されます。イジェクト レバーを完全に閉じると、モジュールの前面プレートとイジェクト レバーが平らに揃います（図 4 を参照）。

図 4　　水平型スロット シャーシのイジェクト レバーの閉じ方



（注）　バックプレーンのコネクタにモジュールが完全に装着されていないと、エラー メッセージが表示されることがあります。

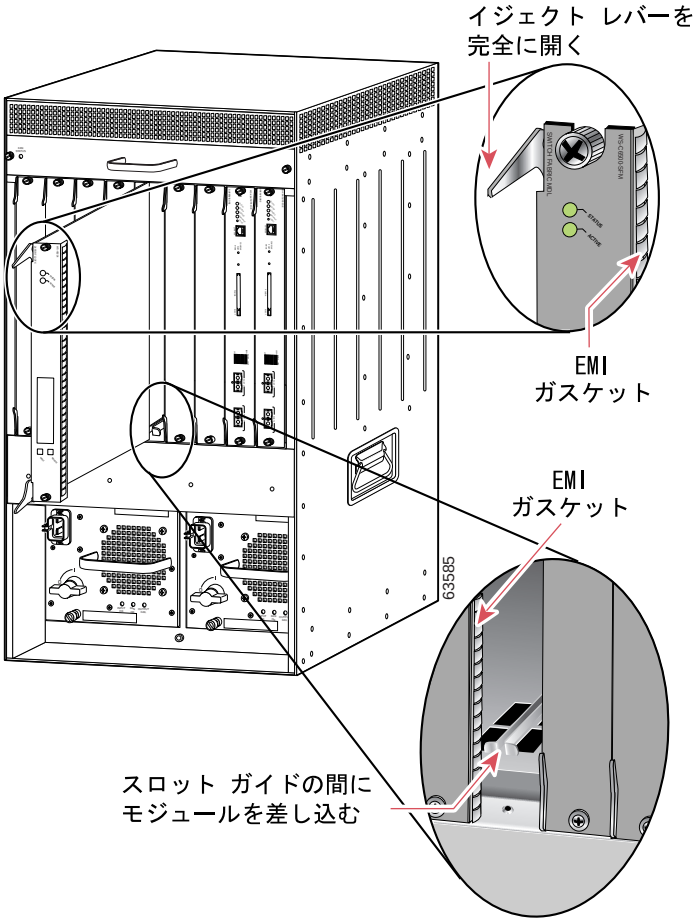
e. スーパバイザ エンジンまたはモジュールの 2 つの非脱落型ネジを締めます。

（注）　非脱落型ネジを締める前に、イジェクト レバーが完全に閉じていることを確認してください。

垂直型スロット

a. スーパバイザ エンジンまたはスイッチング モジュールをスロットの位置に合わせます。（図 5 を参照）。スイッチング モジュールのフレームの両側面をスロットの上下のスロット ガイドに合わせてください。

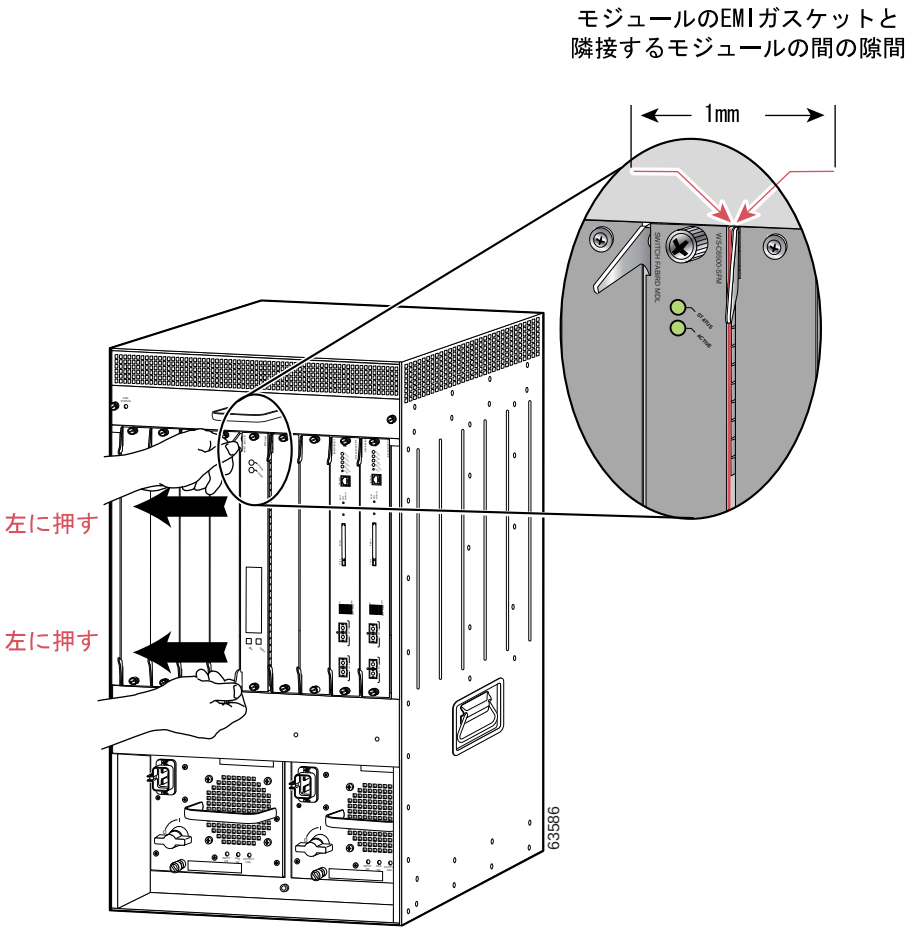
図 5　　垂直型スロット シャーシへのモジュールの取り付け



b. スーパバイザ エンジンまたはモジュールを慎重にスロットに差し込み、モジュール右端の EMI ガスケットが隣接するモジュールに触れたら、両側のイジェクト レバーをモジュールの前面プレートに対して約 45 度の角度になるまで内側に倒します（図 6 を参照）。

c. 両手の親指と人差し指で 2 つのイジェクト レバーを持ち、左の方向に少し押して、モジュールの EMI ガスケットと隣接するモジュールの間にわずかな隙間（約 0.040 インチ [1 mm]）をつくります。（図 6 を参照）。

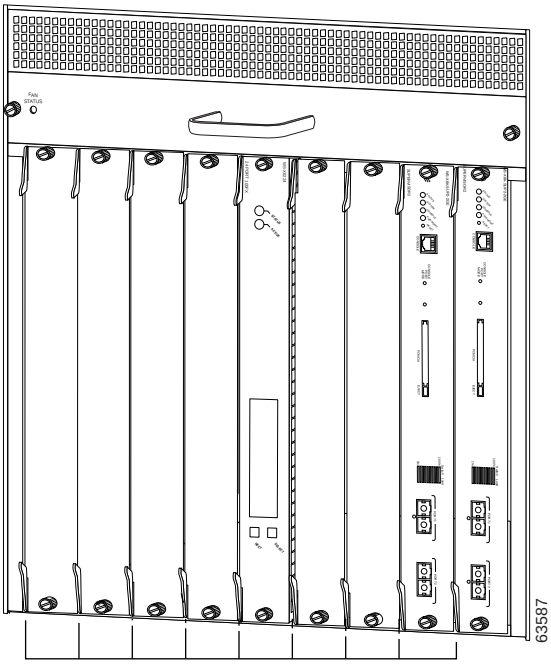
図 6　　垂直型スロット シャーシの EMI ガスケットの調整



注意　イジェクト レバーに力をかけすぎないように注意してください。曲がったり壊れたりするおそれがあります。

d. イジェクト レバーを押しながら、同時に内側に閉じます。これによって、スーパバイザ エンジンまたはモジュールがバックプレーン コネクタに完全に装着されます。イジェクト レバーを完全に閉じると、モジュールの前面プレートとイジェクト レバーが平らに揃います（図 7 を参照）。

図 7　　垂直型スロット シャーシのイジェクト レバーの閉じ方



e. モジュールの 2 つの非脱落型ネジを締めます。

（注）　非脱落型ネジを締める前に、イジェクト レバーが完全に閉じていることを確認してください。

インストレーションの確認

ここでは、NAM のインストレーションを確認する手順について説明します。

Cisco IOS ソフトウェア

システムが新しいモジュールを認識し、モジュールがオンライン状態になっていることを確認するには、**show module** [*mod-num* | **all**] コマンドを入力します。

show module コマンドの出力例を示します。

```
Router#  show module
Mod Slot Ports Module-Type                Model                Sub Status
--- ---- ----- ------------------------- ------------------- --- --------
1   1    2     1000BaseX Supervisor      WS-X6K-S2U-MSFC2    yes ok
15  1    1     Multilayer Switch Feature WS-F6K-MSFC2        no  ok
2   2    3     Network Analysis Module   WS-SVC-NAM-1        no  ok
Router#
```

NAM の初回の起動時には、自動的にメモリ テストの一部が実行されます。完全なメモリ テストを実行する場合は、**hw-module module** *module_number* **reset** *device:partition* **mem-test-full** コマンドを入力します。このコマンドは、Cisco IOS ソフトウェア専用のコマンドなので、Catalyst OS ソフトウェアには使用できません。

メモリのサイズによって異なりますが、完全なメモリ テストは部分的なメモリ テストよりも完了時間がかかります。表 5 に、完全なメモリ テストを行った場合のおおよその起動時間を示します。

表 5　　モジュールの起動時間

モジュール	起動時間
WS-SVC-NAM-1	3 分間
WS-SVC-NAM-2	6 分間

Cisco IOS システムでは、**hw-module module** *module_number* **mem-test-full** コマンドを使用することもできます。モジュール 5 の完全なメモリ テストを実行するには、次のように入力します。

```
Router(config)#  hw-module module 5 mem-test-full
```

Catalyst OS ソフトウェア

スイッチが新しい NAM を認識し、NAM がオンライン状態になっていることを確認するには、**show module** コマンドまたは **show port** [*mod/port*] コマンドを入力します。

show module コマンドの出力例を示します。

```
Console> (enable) show module
Mod Slot Ports Module-Type                Model                Sub Status
--- ---- ----- ------------------------- ------------------- --- --------
1   1    2     1000BaseX Supervisor      WS-X6K-SUP1A-2GE    yes ok
15  1    1     Multilayer Switch Feature WS-F6K-MSFC         no  ok
3   3    2     Network Analysis Module   WS-SVC-NAM-1        no  ok
5   5    48    10/100BaseTX Ethernet     WS-X6248-RJ-45      no  ok
.
.
.
Console> (enable)
```

NAM の初回の起動時には、自動的にメモリ テストの一部が実行されます。Catalyst OS ソフトウェアで完全なメモリ テストを実行する場合は、**set boot device** *bootseq mod#* **mem-test-full** コマンドを入力します。このコマンドは、Catalyst OS ソフトウェア専用のコマンドなので、Cisco IOS ソフトウェアには使用できません。部分的なメモリ テストの実行例を示します。

```
Console (enable) set boot device cf:1 4 mem-test-full
Device BOOT variable = cf:1
Memory-test set to FULL
Warning:Device list is not verified but still set in the boot string.

Console> (enable) show boot device 4
Device BOOT variable = cf:1
Memory-test set to FULL
```

NAM をリセットすると、完全なメモリ テストが実行されます。完全なメモリ テストは部分的なメモリ テストよりも完了に時間がかかります。メモリ テストの所要時間は、表 5 を参照してください。

部分的なメモリ テストをリセットする例を示します。

```
Console> (enable) set boot device cf:1 4
Device BOOT variable = cf:1
Memory-test set to PARTIAL
Warning:Device list is not verified but still set in the boot string.
Console> (enable)
Console> (enable) show boot device 4
Device BOOT variable = cf:1
Memory-test set to PARTIAL
```

NAM の設定

スイッチ上の NAM の設定手順は、Cisco IOS ソフトウェアと Catalyst OS ソフトウェアのいずれを使用しているかによって異なります。ただし、両方のスイッチ オペレーティング システムに共通する手順もいくつかあります。

以下の各項では、CLI を使用して NAM を設定する手順について、スイッチ オペレーティング システム別に説明します。

- Cisco IOS ソフトウェア（p.22）
- Catalyst OS ソフトウェア（p.30）

ソフトウェア別の NAM 属性の設定が完了すると、以下の項に従って、両方のソフトウェアに共通した属性を設定できます。

- オペレーティング システムに依存しない設定（p.37）

Cisco IOS ソフトウェア

ここでは、Cisco IOS を使用して、Catalyst 6500 シリーズおよび Catalyst 6000 ファミリー スイッチから NAM を設定する手順を説明します。

- 初期設定（p.22）
- VLAN の設定（p.26）
- トラフィック ソースとして NDE を使用する場合（p.26）
- トラフィック ソースとして SPAN を使用する場合（p.28）

初期設定

ネットワーク解析に NAM を使用するには、事前に NAM の root アカウントにログインし、次の設定を行う必要があります。

- IP アドレス
- サブネット マスク
- IP ブロードキャスト アドレス
- IP ホスト名
- デフォルト ゲートウェイ
- ドメイン名
- 該当する場合は、DNS ネーム サーバ
- 外部の SNMP マネージャを使用して NAM と通信する場合は、次の設定を行います。
  - SNMP MIB 変数
  - SNMP エージェントのアクセス制御
  - NAM 上のシステム グループ設定

ip http server enable コマンドを使用して、Web サーバを起動します。

NAM に上記のパラメータを設定する手順は、次のとおりです。

ステップ 1 次のコマンドを入力して、NAM が搭載されていて電源が入っていることを確認します。

```
Router#  show module mod
```

ステップ 2 次のコマンドを入力して、NAM とのコンソール セッションを確立します。

```
Router#  session slot module_number processor 1
```

ステップ 3 ログイン プロンプトに **root** と入力し、root アカウントにログインします。

ステップ 4 パスワード プロンプトに、root パスワードとして **root** と入力します。

（注） 出荷時のデフォルト パスワードを変更していない場合は、警告メッセージが表示されます。デフォルトのパスワードを変更する場合は、「NAM CLI パスワードの変更」（p.56）を参照してください。

ステップ 5 次のコマンドを入力して、IP アドレスとサブネット マスクを設定します。

```
root@localhost# ip address ip-address subnet-mask
```

ステップ 6 次のコマンドを入力して、IP ブロードキャスト アドレスを設定します。

```
root@localhost# ip broadcast broadcast-address
```

ステップ 7 次のコマンドを入力して、IP ホスト名を設定します。IP ホスト名は、CLI プロンプト、**show** コマンド、およびログ メッセージで使用されます。

```
root@localhost# ip host [host-name]
```

ステップ 8 次のコマンドを入力して、デフォルト ゲートウェイを設定します。

```
root@localhost# ip gateway default-gateway
```

ステップ 9 次のコマンドを入力して、NAM のドメイン名を設定します。

```
root@localhost# ip domain domain-name
```

ステップ 10 次のコマンドを入力して、1 つまたは複数の IP アドレスを DNS ネーム サーバとして設定します。

```
root@localhost# ip nameserver ip-address [name-server1] [name-server2]
```

（注） **ip nameserver** コマンドでは、ネーム サーバのアドレスを 3 つまで設定できます（2 つは任意設定）。

ステップ 11 次のコマンドを入力して、NAM の設定を確認します。

```
root@localhost# show ip
```

ステップ 12 次のコマンドを入力して、SNMP sysLocation MIB 変数を設定します。

```
root@localhost# snmp location location-string
```

（注） ステップ 13 およびステップ 14 で設定する MIB 変数は、有効な DisplayString テキストでなければなりません。長さは 64 文字までです。

ステップ 13 次のコマンドを入力して、SNMP sysContact MIB 変数を設定します。

```
root@localhost# snmp contact contact-string
```

ステップ 14 次のコマンドを入力して、SNMP sysName MIB 変数を設定します。

```
root@localhost# snmp name name-string
```

（注） SNMP ロケーション、SNMP コンタクト、または SNMP 名を削除する場合は、パラメータを指定せずに該当するコマンドを入力します。

ステップ 15 次のコマンドを入力して、SNMP エージェントのコミュニティ ストリング パラメータ パスワードを読み書きアクセス権に設定します。

```
root@localhost# snmp community community-string rw
```

ステップ 16 次のコマンドを入力して、SNMP エージェントのコミュニティ ストリング パラメータ パスワードを読み取り専用アクセス権に設定します。

```
root@localhost# snmp community community-string ro
```

（注） SNMP コミュニティ ストリングを消去する場合は、**snmp delete community** *community-string* コマンドを使用します。

ステップ 17 次のコマンドを入力して、SNMP のアクセス制御および設定値を確認します。

```
root@localhost# show snmp
```

この設定が完了すると、IETF に準拠した任意の RMON アプリケーションで NAM を使用できるようになります。

（注） Real Time Monitor（RTM）を使用する場合は、NAM に入力したものとまったく同じコミュニティ ストリングを RTM に入力する必要があります。

NAM の設定例を示します。

```
Router#  session slot 8 processor 1
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.81 ... Open

Cisco Network Analysis Module (WS-SVC-NAM-1)

login: root
Password:

Network Analysis Module (WS-SVC-NAM-1) Console, 2.1(1)
Copyright (C) 1999, 2000, 2001 Cisco Systems, Inc.

WARNING! Default password has not been changed!

root@localhost# ip address 172.18.52.29 255.255.255.224
root@localhost# ip broadcast 172.18.52.31
root@localhost# ip host nam1
root@localhost# ip gateway 172.69.2.132
root@localhost# ip domain cisco.com
root@localhost# ip nameserver 171.62.2.132
root@localhost# show ip
IP address:        172.20.98.182
Subnet mask:       255.255.255.192
IP Broadcast:      172.20.255.255
DNS Name:          namlab-kom6.cisco.com
Default Gateway:   172.20.98.129
Nameserver(s):     171.69.2.133
HTTP server:       Enabled
HTTP secure server:Disabled
HTTP port:         80
HTTP secure port:  443
TACACS+ configured:No
Telnet:            Enabled
SSH:               Disabled
root@localhost#
root@localhost# snmp location "Cisco Lab, Building X, Floor 1"

root@localhost# snmp contact "Jane Doe, Cisco Systems, (408) 111-1111"
root@localhost# snmp name "6k-NAM - Slot 2"
root@localhost# snmp community public ro
root@localhost# snmp community private rw

root@localhost# show snmp

SNMP Agent:   nam1.cisco.com   172.18.52.29

SNMPv1:  Enabled
SNMPv2C: Enabled
SNMPv3:  Disabled

community public  read
community private write

sysDescr         "Catalyst 6500 Network Management Module (WS-SVC-NAM-1)"
sysObjectID      enterprises.9.5.1.3.1.1.2.914
sysContact       "Jane Doe, Cisco Systems, (408) 111-1111"
sysName          "6k-NAM - Slot 2"
sysLocation      "Cisco Lab, Building X, Floor 1"
root@localhost#
```

VLAN の設定

NAM 管理ポートの VLAN を設定するには、**analysis module** *mod_num* **management-port access-vlan** *vlan_id* コマンドを使用する必要があります。

トラフィック ソースとして NDE を使用する場合

NAM のトラフィック ソースとして NDE を使用する場合は、NetFlow モニタ オプションをイネーブルにして、NAM が NDE ストリームを受信できるようにします。統計情報は、予約された ifIndex.3000 で提供されます。

NDE は、外部データ コレクタが収集したトラフィック統計情報を解析に使用できるようにします。NDE を使用すると、レイヤ 3 スイッチングおよびルーティングが行われたすべての IP ユニキャスト トラフィックをモニタできます。Catalyst 6500 シリーズおよび Catalyst 6000 ファミリー スイッチでは、PFC と MSFC の両方に、フロー ベースのトラフィック統計情報をキャプチャする NetFlow キャッシュがあります。PFC 上のキャッシュはレイヤ 3 スイッチング フローに関する統計情報をキャプチャし、MSFC上のキャッシュはルーティング フローに関する統計情報をキャプチャします。

（注） NDE の詳しい設定手順については、スイッチ ソフトウェア コンフィギュレーション ガイドを参照してください。

Cisco IOS ソフトウェアで NDE を設定する手順は、次のとおりです。

ステップ 1 次のコマンドを入力して、NDE の現在の設定を確認します。

```
Router#  show running-config | include mls
mls rp nde-address 172.18.27.229
mls rp ip route-map
mls rp ip
no mls ip multicast aggregate
no mls ip multicast non-rpf cef
mls aging fast
mls flow ip full
mls flow ipx destination-source
mls nde flow include protocol tcp
mls nde sender
mls qos statistics-export interval 300
mls qos statistics-export delimiter |

Router# show running-config | include flow
ip flow-cache feature-accelerate
mls flow ip full
mls flow ipx destination-source
mls nde flow include protocol tcp
 ip route-cache flow
 ip route-cache flow
 ip route-cache flow
ip flow-export source Vlan2
ip flow-export destination 172.18.27.229 3000
ip flow-aggregation cache as
```

ステップ 2 次のコマンドを入力して、設定されている NDE エクスポートを確認します。

```
Router# show mls nde
 Netflow Data Export enabled
 Exporting flows to 172.18.27.229 (3000)
 Exporting flows from 172.18.27.221 (57675)
 Version:7
 Include Filter is:
   protocol:TCP
 Exclude Filter not configured
 Total Netflow Data Export Packets are:
    0 packets, 0 no packets, 0 records
 Total Netflow Data Export Send Errors:
        IPWRITE_NO_FIB = 0
        IPWRITE_ADJ_FAILED = 0
        IPWRITE_PROCESS = 0
        IPWRITE_ENQUEUE_FAILED = 0
        IPWRITE_IPC_FAILED = 0
        IPWRITE_MTU_FAILED = 0
        IPWRITE_ENCAPFIX_FAILED = 0

Router# show ip flow export
Flow export is enabled
  Exporting flows to 172.18.27.229 (3000)
  Exporting using source interface Vlan2
  Version 1 flow records
  0 flows exported in 0 udp datagrams
  0 flows failed due to lack of export packet
  0 export packets were sent up to process level
  0 export packets were dropped due to no fib
  0 export packets were dropped due to adjacency issues
  0 export packets were dropped due to fragmentation failures
  0 export packets were dropped due to encapsulation fixup failures
  0 export packets were dropped enqueuing for the RP
  0 export packets were dropped due to IPC rate limiting
```

ステップ 3 次の手順で、NDE を設定します。

```
Router(config)# mls nde sender
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)# mls rp nde-address 172.18.27.229

Router(config)# mls flow ip full

Router(config)# mls nde flow include protocol tcp

Router(config)# ip flow-export destination 172.18.27.229 3000
```

（注） UDP ポート番号は、3000 に設定する必要があります。

```
Router(config)# ip flow-export source vlan 2

Router(config)# ip flow-aggregation cache as

Router(config-flow-cache)#enable

Router(config)# interface GigabitEthernet8/6
Router(config)# interface vlan 22
Router(config-if)# ip address 1.2.3.4 255.255.255.0

Router(config-if)# ip route-cache flow
```

NAM モジュールを NDE コレクタとして設定する場合、(NAM モジュールとのセッションによって設定した）NAM の IP アドレスを使用する必要があります。

ステップ 4 次のコマンドを入力して、NDE 関連の情報を NAM と同期化します。

```
Router# hw-module module 5 sync nde-info
```

このコマンドを入力すると、モジュールをリセットするように指示するプロンプトが表示される場合があります。NDE の設定および NAM の設定（NAM 管理ポートの VLAN、VLAN インターフェイスの IP アドレスなど、設定情報の入力）が完了したら、必ずこのコマンドを使用してください。

（注） NAM を NDE コレクタとして使用しない場合、このステップは不要です。このステップは、バージョン 1.2(xx) の NAM だけに該当します（NAM バージョン 1.1(xx) はサポートされていません)。

トラフィック ソースとして SPAN を使用する場合

CLI でも NAM Traffic Analyzer アプリケーションでも、SPAN をトラフィック ソースとして設定できます。

NAM は、イーサネット、ファスト イーサネット、ギガビット イーサネット、トランク ポート、または Fast EtherChannel SPAN 送信元ポートからのイーサネット トラフィックを解析できます。また、イーサネット VLAN を SPAN 送信元に指定することもできます。

SPAN についての詳細は、次の Web サイトにある『*Catalyst 6000 Family IOS Software Configuration Guide*』を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/index.htm

NAM モジュール上のポートを SPAN 送信元ポートとして使用することはできません。

NAM 上で SPAN をイネーブルにするには、次のいずれかの作業を行います。

コマンド	目的
Router (config)# **monitor session** {*session_number*} **{source {interface type** *slot/port*} | **{vlan** *vlan_ID*}} [, | - | **rx** | **tx** | **both**]	モニタ セッションの送信元インターフェイスおよび VLAN を設定します。
Router (config)# **monitor session** {*session_number*} **{destination analysis module** *NAM module number* **data-port** *port*}	NAM のポート 1 を SPAN 宛先ポートとしてイネーブルにします。
Router (config)# **no monitor session** *session_number*	モニタ セッションをディセーブルにします。

コマンド	目的
Router (config)# **monitor session** *{session_number}* **{filter** *{vlan_ID}* [, | -]}	SPAN セッションをフィルタリングして、特定の VLAN だけがスイッチ ポート トランクから見えるようにします。
Router # **show monitor session** *{session_number}*	現在のモニタ セッションを表示します。

NAM 上で SPAN をイネーブルにする例を示します。

```
Router#  show monitor
Session 1
---------
Source Ports:
    RX Only:       None
    TX Only:       None
    Both:          None
Source VLANs:
    RX Only:       None
    TX Only:       None
    Both:          None
Destination Ports:None
Filter VLANs:      None

Session 2
---------
Source Ports:
    RX Only:       None
    TX Only:       None
    Both:          None
Source VLANs:
    RX Only:       None
    TX Only:       None
    Both:          None
Destination Ports:None
Filter VLANs:      None

Router#  conf t
Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)# monitor session 1 source vlan 1 both
```

（注） スイッチの CLI を使用し、NAM-1 へのトラフィック送信元として SPAN を設定する場合、NAM-1 の SPAN 宛先ポートはデータ ポート 1 です。NAM-2 の SPAN 宛先ポート（SPAN ポート 1）もデータ ポート 1 です。宛先データ ポート 2 はこのリリースの NAM では使用できません（スイッチおよびハードウェア サポートは利用可能です）。

```
Router#
00:21:10:%SYS-5-CONFIG_I:Configured from console by console
Router# conf t
Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)#  monitor session 1 destination analysis-module 8 data-port 1
Router#  show monitor
Session 1
---------
 Type        :Local Session
Source Ports:
    RX Only:       None
    TX Only:       None
    Both:          None
Source VLANs:
    RX Only:       None
    TX Only:       None
    Both:          1
Source RSPAN VLAN:None
Destination Ports:analysis-module 8 data-port 1

Filter VLANs:      None
Dest RSPAN VLAN:   None

Session 2
---------
 Type        :Local Session
Source Ports:
    RX Only:       None
    TX Only:       None
    Both:          None
Source VLANs:
    RX Only:       None
    TX Only:       None
    Both:         None
Source RSPAN VLAN:None
Destination Ports:None
Filter VLANs:      None
Dest RSPAN VLAN:   None
```

Catalyst OS ソフトウェア

ここでは、CLI を使用して NAM を設定する手順について説明します。

- 初期設定（p.30）
- VLAN の設定（p.34）
- トラフィック ソースとして NDE を使用する場合（p.34）
- トラフィック ソースとして SPAN を使用する場合（p.35）
- SNMP エージェントの設定（p.35）

初期設定

ネットワーク解析のために NAM を使用するには、事前に NAM の root アカウントにログインし、次の設定を行う必要があります。

- IP アドレス
- サブネット マスク
- IP ブロードキャスト アドレス
- IP ホスト名
- デフォルト ゲートウェイ
- ドメイン名

- 該当する場合は、DNS ネーム サーバ
- 外部の SNMP マネージャを使用して NAM と通信する場合は、次の設定を行います。
  - SNMP MIB 変数
  - SNMP エージェントのアクセス制御
  - NAM 上のシステム グループ設定

ip http server enable コマンドを使用して、Web サーバを起動します。

NAM に上記のパラメータを設定するには、イネーブル モードで次の手順を行います。

ステップ 1 次のコマンドを入力して、NAM が搭載され電源が入っていることを確認します。

```
Console> show module mod
```

ステップ 2 次のコマンドを入力して、NAM アプリケーション イメージを起動します。

```
Console> (enable) reset module no
```

ステップ 3 次のコマンドを入力して、NAM とのコンソール セッションを確立します。

```
Console> (enable) session mod
```

ステップ 4 パスワード プロンプトに、root パスワードとして **root** と入力します。

（注） 出荷時のデフォルト パスワードを変更していない場合は、警告メッセージが表示されます。デフォルトのパスワードを変更する方法については、「NAM CLI パスワードの変更」（p.56）を参照してください。

ステップ 5 次のコマンドを入力して、IP アドレスとサブネット マスクを設定します。

```
root@localhost# ip address ip-address subnet-mask
```

ステップ 6 次のコマンドを入力して、IP ブロードキャスト アドレスを設定します。

```
root@localhost# ip broadcast broadcast-address
```

ステップ 7 次のコマンドを入力して、IP ホスト名を設定します。IP ホスト名は、CLI プロンプト、**show** コマンド、およびログ メッセージで使用されます。

```
root@localhost# ip host name
```

ステップ 8 次のコマンドを入力して、デフォルト ゲートウェイを設定します。

```
root@localhost# ip gateway default-gateway
```

ステップ 9 次のコマンドを入力して、NAM のドメイン名を設定します。

```
root@localhost# ip domain domain-name
```

ステップ 10 次のコマンドを入力して、1 つまたは複数の IP アドレスを DNS ネーム サーバとして設定します。

```
root@localhost# ip nameserver ip-address [ip-address]
```

ステップ 11 次のコマンドを入力して、NAM の設定を確認します。

```
root@localhost# show ip
```

ステップ 12 次のコマンドを入力して、SNMP sysLocation MIB 変数を設定します。

```
root@localhost# snmp location location-string
```

（注） ステップ 13 およびステップ 14 で設定する MIB 変数は、有効な DisplayString テキストでなければなりません。長さは 64 文字までです。

ステップ 13 次のコマンドを入力して、SNMP sysContact MIB 変数を設定します。

```
root@localhost# snmp contact contact-string
```

ステップ 14 次のコマンドを入力して、SNMP sysName MIB 変数を設定します。

```
root@localhost# snmp name name-string
```

（注） SNMP ロケーション、SNMP コンタクト、または SNMP 名を削除する場合は、パラメータを指定せずに該当するコマンドを入力します。

ステップ 15 次のコマンドを入力して、SNMP エージェントのコミュニティ ストリング パラメータ パスワードを読み書きアクセス権に設定します。

```
root@localhost# snmp community community-string rw
```

ステップ 16 次のコマンドを入力して、SNMP エージェントのコミュニティ ストリング パラメータ パスワードを読み取り専用アクセス権に設定します。

```
oot@localhost# snmp community community-string rw
```

（注） SNMP コミュニティ ストリングを消去する場合は、**snmp delete community** *community-string* コマンドを使用します。

ステップ 17 次のコマンドを入力して、SNMP のアクセス制御および設定値を確認します。

```
root@localhost# show snmp
```

この設定が完了すると、IETF に準拠した任意の RMON アプリケーションで NAM を使用できるようになります。

NAM の設定例を示します。

```
Console> (enable) session 2
Trying NAM-2...
Connected to NAM-2.
Escape character is '^]'.

Network Analysis Module (WS-SVC-NAM-1)

login: root
Password:

Network Analysis Module (WS-SVC-NAM-1) Console, 2.2(0.1)
Copyright (c) 1999-2002 by Cisco Systems, Inc.

WARNING! Default password has not been changed!

root@localhost# ip address 172.18.52.29 255.255.255.224
root@localhost# ip broadcast 172.18.52.31
root@localhost# ip host nam1
root@localhost# ip gateway 172.69.2.132
root@localhost# ip domain Cisco.com
root@localhost# ip nameserver 171.62.2.132
root@localhost# show ip
IP address:        172.20.98.182
Subnet mask:       255.255.255.192
IP Broadcast:      172.20.255.255
DNS Name:          namlab-kom6.cisco.com
Default Gateway:   172.20.98.129
Nameserver(s):     171.69.2.133
HTTP server:       Enabled
HTTP secure server:Disabled
HTTP port:         80
HTTP secure port:  443
TACACS+ configured:No
Telnet:            Enabled
SSH:               Disabled
root@localhost#
root@localhost# snmp location "Cisco Lab, Building X, Floor 1"

root@localhost# snmp contact "Jane Doe, Cisco Systems, (408) 111-1111"
root@localhost# snmp name "6k-NAM - Slot 2"
root@localhost# snmp community public ro
root@localhost# snmp community private rw

root@localhost# show snmp

SNMP Agent:   nam1.Cisco.com   172.18.52.29

SNMPv1:  Enabled
SNMPv2C: Enabled
SNMPv3:  Disabled

community public read
community private write

sysDescr         "Catalyst 6500 Network Management Module (WS-SVC-NAM-1)"
sysObjectID      enterprises.9.5.1.3.1.1.2.914
sysContact       "Jane Doe, Cisco Systems, (408) 111-1111"
sysName          "6k-NAM - Slot 2"
sysLocation      "Cisco Lab, Building X, Floor 1"
root@localhost#
```

VLAN の設定

NAM 管理ポートとして VLAN を設定する必要はありません。このポートはスーパバイザ エンジン上のインターフェイス sc0 に割り当てられた VLAN に自動的に同期化されるからです。

（注） **set vlan** *mod/port* コマンドで NAM 管理ポートに VLAN を設定することはできません。

トラフィック ソースとして NDE を使用する場合

NAM のトラフィック ソースとして NDE を使用する場合は、NetFlow モニタ オプションをイネーブルにして、NAM が NDE ストリームを受信できるようにする必要があります。統計情報は、予約された ifIndex.3000 で提供されます。

（注） NetFlow 機能を使用するには、Multilayer Switch Feature Card（MSFC; マルチレイヤ スイッチ フィーチャ カード）の設定が必要です。NDE の設定手順については、『*Catalyst 6000 Family Software Configuration Guide*』を参照してください。

次の手順で、NetFlow モニタ オプションをイネーブルにします。

	作業	コマンド
ステップ 1	NetFlow モニタ オプションをイネーブルにします。	**set snmp extendedrmon netflow** [**enable** | **disable**] *mod*
ステップ 2	NetFlow モニタ オプションがイネーブルに設定されたことを確認します。	**show snmp**
ステップ 3	フローをフルに設定します。	**set mls flow full**
ステップ 4	NDE をイネーブルにします。	**set mls nde enable**

NetFlow モニタ オプションをイネーブルにし、イネーブルに設定されたことを確認する例を示します。

```
Console> (enable) set snmp extendedrmon netflow enable 2
Snmp extended RMON netflow enabled
Console> (enable) show snmp
RMON: Enabled
Extended RMON Netflow Enabled : Module 2
Traps Enabled:
None
Port Traps Enabled: None

Community-Access     Community-String
----------------     --------------------
read-only            public
read-write           private
read-write-all       secret

Trap-Rec-Address                            Trap-Rec-Community
----------------------------------------    --------------------
<テキスト出力は省略>
```

（注） NAM が搭載されている場合、『*Catalyst 6000 Family Software Configuration Guide*』に記述されているように、**set mls nde** *collector_ip* [*udp_port_number*] コマンドで外部データ コレクタを指定する必要はありません。ホストおよびポートが設定されていないというメッセージは無視してください。

トラフィック ソースとして SPAN を使用する場合

SPAN をトラフィック ソースとして設定する場合、スイッチの CLI と NAM Traffic Analyzer アプリケーションのどちらでも使用できますが、NAM Traffic Analyzer の使用を推奨します。

RSPAN トラフィックは、NAM の SPAN 送信元として使用できます。SPAN 送信元が RSPAN に使用されているのと同じ VLAN ID に設定されていることを確認してください。SPAN 宛先は、*nam_module*/*port* に設定する必要があります。

（注） スイッチの CLI を使用し、NAM-1 へのトラフィック送信元として SPAN を設定する場合、宛先ポートは 3 に設定してください。NAM-2 へのトラフィック送信元として SPAN を設定する場合は、SPAN ポートを宛先ポート 7 に設定してください。宛先ポート 8 はこのリリースの NAM では使用できません（スイッチおよびハードウェア サポートは利用可能です）。

（注） NAM ポートを SPAN 送信元ポートとして使用することはできません。

NAM は、イーサネット、ファスト イーサネット、ギガビット イーサネット、トランク ポート、または Fast EtherChannel SPAN 送信元ポートからのイーサネット トラフィックを解析できます。また、イーサネット VLAN を SPAN 送信元に指定することもできます。

SPAN および RSPAN の詳しい設定手順については、スイッチ ソフトウェア コンフィギュレーション ガイドを参照してください。

NAM を SPAN 宛先ポートとして設定するには、イネーブル モードで次の作業を行います。

作業	コマンド
NAMをSPAN宛先ポートとして設定します。	**set span** {*src_mod*/*src_ports* | *src_vlans* | **sc0**} {*dest_mod* | *dest_port*} [**rx** | **tx** | **both**] [**inpkts** {**enable** | **disable**}] [**learning** {**enable** | **disable**}] [**multicast** {**enable** | **disable**}] [**filter** *vlans*...][**create**]

スロット 5 に搭載されている NAM-2 に SPAN VLAN 1 を設定する場合は、次のように入力します。

```
Console> (enable) set span 1 5/7
```

SNMP エージェントの設定

（注） NAM Traffic Analyzer アプリケーションを使用する場合、ここで説明する手順は省略可能です。

SNMP エージェントの設定は、CLI または NAM Traffic Analyzer アプリケーションを使用して行うことができます。外部の SNMP ソースまたは Web サーバを使用して SNMP のサポート用またはハイブリッド モードで NAM を使用するには、事前に NAM の root アカウントにログインして、次の設定を行う必要があります。

- SNMP MIB 変数
- SNMP エージェントのアクセス制御
- NAM 上のシステム グループ設定

NAM に上記のパラメータを設定する手順は、次のとおりです。

ステップ 1 次のコマンドを入力して、SNMP sysLocation MIB 変数を設定します。

```
root@localhost# snmp location location-string
```

（注） ステップ 2 およびステップ 3 で設定する MIB 変数は、有効な DisplayString テキストでなければなりません。長さは 64 文字までです。

ステップ 2 次のコマンドを入力して、SNMP sysContact MIB 変数を設定します。

```
root@localhost# snmp contact contact-string
```

ステップ 3 次のコマンドを入力して、SNMP sysName MIB 変数を設定します。

```
root@localhost# snmp name name-string
```

（注） SNMP ロケーション、SNMP コンタクト、または SNMP 名を削除する場合は、パラメータを指定せずに該当するコマンドを入力します。

ステップ 4 次のコマンドを入力して、SNMP エージェントのコミュニティ ストリング パラメータ パスワードを読み書きアクセスに設定します。

```
root@localhost# snmp community community-string rw
```

ステップ 5 次のコマンドを入力して、SNMP エージェントのコミュニティ ストリング パラメータ パスワードを読み取り専用アクセスに設定します。

```
root@localhost# snmp community community-string ro
```

（注） SNMP コミュニティ ストリングを消去する場合は、**snmp delete community** *community-string* コマンドを使用します。

ステップ 6 次のコマンドを入力して、SNMP のアクセス制御および設定値を確認します。

```
root@localhost# show snmp
```

この設定が完了すると、NetScout nGenius Real-Time Monitor または IETF に準拠した任意の RMON アプリケーションで NAM を使用できるようになります。

NAM の設定例を示します。

```
Console> (enable) session 2
Trying NAM-2...
Connected to NAM-2.
Escape character is '^]'.

Network Analysis Module (WS-SVC-NAM-1)

login: root
Password:

Network Analysis Module (WS-SVC-NAM-1) Console, 2.2(0.1)
Copyright (c) 1999-2002 by Cisco Systems, Inc.

WARNING! Default password has not been changed!

root@localhost# ip address 172.18.52.29 255.255.255.224
root@localhost# ip broadcast 172.18.52.31
root@localhost# ip host nam1
root@localhost# ip gateway 172.69.2.132
root@localhost# ip domain Cisco.com
root@localhost# ip nameserver 171.62.2.132
root@localhost# show ip
IP address:         172.18.52.29
Subnet mask:        255.255.255.224
IP Broadcast:       172.18.52.31
DNS Name:           nam1.Cisco.com
Default Gateway:    172.18.52.1
Nameserver(s):      172.16.2.132
root@localhost#
root@localhost# snmp location "Cisco Lab, Building X, Floor 1"

root@localhost# snmp contact "Jane Doe, Cisco Systems, (408) 111-1111"
root@localhost# snmp name "6k-NAM - Slot 2"
root@localhost# snmp community public ro
root@localhost# snmp community private rw

root@localhost# show snmp

SNMP Agent:   nam1.Cisco.com   172.18.52.29

SNMPv1:  Enabled
SNMPv2C: Enabled
SNMPv3:  Disabled

community public read
community private write

sysDescr         "Catalyst 6500 Network Management Module (WS-SVC-NAM-1)"
sysObjectID      1.3.6.1.4.1.9.5.1.3.1.1.2.223
sysContact       "Jane Doe, Cisco Systems, (408) 111-1111"
sysName          "6k-NAM - Slot 2"
sysLocation      "Cisco Lab, Building X, Floor 1"
```

オペレーティング システムに依存しない設定

ここでは、スイッチのオペレーティング システムに依存しない NAM の設定について説明します。

RMON 自動収集の設定

複数のデータ ソースに対する RMON 収集を、SNMP を通じて管理ステーションで明示的に設定できます。SNMP を通じて明示的に設定された収集は、autostart で指定した収集よりも優先されます。したがって、両方とも設定されている場合、NAM の初期化時には各データ ソースに対して明示的に設定された収集だけが開始されます。

autostart コマンドを使用すると、NAM が初期化されるときに、使用可能なすべてのデータ ソース（すべての既知の VLAN を含む）に対して、いくつかの収集が自動的に設定されます。

（注） 各データ ソースに対して多くの収集が起動されるとパフォーマンスが低下する可能性があるので、autostart を使用するのではなく、必要な収集を明示的に設定することを推奨します。

（注） **autostart** コマンドを入力した場合、コマンドを有効にするには、NAM を再起動する必要があります。

次の収集タイプを自動的に開始できます。

- addressMap — RMON2-MIB（RFC 2021）の addressMapTable

  NMS が addressMapMaxDesiredEntries スカラーを設定しない場合、NAM は値 –1（無制限）を使用します。
- art — draft-warth-rmon2-artmib-01.txt の artControlTable
- etherStat — RMON-MIB（RFC 1757）の etherStatsTable
- prioStats — SMON-MIB（RFC 2613）の smonPrioStatsControlTable
- vlanStats — SMON-MIB（RFC 2613）の smonVlanStatsControlTable

たとえば、**autostart etherstats enable** コマンドを入力して NAM を再起動すると、各データ ソース（インターフェイスまたは VLAN）に（RMON-1 の）etherStatsEntry が設定されます。etherStatsOwner フィールドは *monitor* という値に設定されます。

自動開始プロセスが実行されるのは、管理ステーションによって SNMP 経由で明示的に作成された収集をすべて設定して NAM の NVRAM に保存した後からです。SNMP を通じてすでに自動開始タイプの収集が設定されているデータ ソースに対しては、自動開始タイプの収集は設定されません。

自動開始プロセスの収集をイネーブルにする手順は、次のとおりです。

- NAM の root アカウントに次のコマンドを入力して、etherStat 収集タイプをイネーブルにします。

  ```
  root@localhost# autostart etherstat enable
  ```
- NAM の root アカウントに次のコマンドを入力して、addressMap 収集タイプをイネーブルにします。

  ```
  root@localhost# autostart addressmap enable
  ```
- NAM の root アカウントに次のコマンドを入力して、prioStats 収集タイプをイネーブルにします。

  ```
  root@localhost# autostart priostats enable
  ```
- NAM の root アカウントに次のコマンドを入力して、vlanStats 収集タイプをイネーブルにします。

  ```
  root@localhost# autostart vlanstats enable
  ```
- NAM の root アカウントに次のコマンドを入力して、vlanStats 収集タイプをディセーブルにします。

  ```
  root@localhost# autostart vlanstats disable
  ```

1 つまたは複数の収集タイプをイネーブルまたはディセーブルにした後で、その設定を有効にするには、NAM を再起動する必要があります。

HTTP サーバまたは HTTP セキュア サーバの設定

Web ブラウザ（HTTP または HTTPS）を使用して NAM にアクセスするには、事前に NAM CLI から NAM Traffic Analyzer アプリケーションをイネーブルにする必要があります。HTTP の場合、**ip http server enable** コマンドを使用します。HTTPS の場合、**ip http secure server enable** コマンドを使用します。任意で、HTTP（または HTTPS）サーバがデフォルトとは異なる TCP ポート上で稼働するように設定することもできます。

（注） HTTP サーバまたは HTTP セキュア サーバのどちらでも使用できますが、両方を使用することはできません。

（注） デフォルトでは、**ip http secure** コマンドはすべてディセーブルに設定されています。これらのコマンドをイネーブルにするには、http://www.cisco.com から NAM strong crypto パッチをダウンロードしてインストールする必要があります。

HTTP サーバの設定

NAM に HTTP サーバのパラメータを設定する手順は、次のとおりです。

ステップ 1 （任意）次のコマンドを入力して、HTTP ポートを設定します。

```
root@localhost# ip http port 8080
The HTTP server is enabled now. You must restart the
server to change HTTP port. Continue [y/n]? y
```

ポート番号は、1 ～ 65535 の範囲です。

（注） Web ユーザは CLI ユーザとは異なります。

ステップ 2 次のコマンドを入力して、HTTP サーバをイネーブルにします。

```
root@localhost# ip http server enable
Enabling HTTP server...
No web users configured!
Please enter a web administrator username [admin]:admin
New password:
Confirm password
User admin added.
Successfully enabled HTTP server.
```

Strong Crypto パッチのインストール

デフォルトでは、**ip http secure** コマンドはすべてディセーブルに設定されています。strong crypto パッチをインストールして、HTTP セキュア サーバをイネーブルにする必要があります。Telnet の代わりに SSH を使用する場合は、strong crypto パッチもインストールする必要があります。

strong crypto パッチをインストールする手順は、次のとおりです。

ステップ 1 次のコマンドを入力して、http://www.cisco.com からパッチをダウンロードします。

```
root@localhost# patch ftp-url
```

ftp-url は、strong crypto パッチの FTP ロケーションおよび名前です。

パッチをインストールする例を示します。

```
Console># patch ftp://host/pub/patch_rpms/c6nam-2.2-strong-cryptoK9-patch-1.0-bin

Proceeding with installation. Please do not interrupt.
If installation is interrupted, please try again.

Downloading c6nam-2.2-strong-cryptoK9-patch-1-0.bin Please wait...
ftp://host/pub/patch_rpms/c6nam-2.2-strong-cryptoK9-patch-1-0 (1
K)
-                         [#########################]       1K | 1071.96K/s
2022 bytes transferred in 0.00 sec (1006.91k/sec)

Verifying c6nam-2.2-strong-cryptoK9-patch-1-0. Please wait...
Patch c6nam-2.2-strong-cryptoK9-patch-1-0 verified.

Applying /usr/local/nam/patch/workdir/c6nam-2.2-strong-cryptoK9-patch-1-0. Pleas
e wait...
############################################ [100%]
############################################ [100%]

Patch applied successfully.
```

ステップ 2 （任意）次のコマンドを入力して、HTTPS サーバを設定します。

```
root@localhost# ip http secure port 8080
The HTTP server is enabled now. You must restart the
server to change HTTP port. Continue [y/n]? y
```

ポート番号は、1 ～ 65535 の範囲です。

（注） Web ユーザは CLI ユーザとは異なります。

ステップ 3 次のコマンドを入力して、HTTPS サーバをイネーブルにします。

```
root@localhost# ip http secure server enable
Enabling HTTP server...
No web users configured!
Please enter a web administrator username [admin]:admin
New password:
Confirm password
User admin added.
Successfully enabled HTTP server.
```

証明書の生成

証明書は、セキュア サーバ接続の正当性を確認する目的で使用します。自己署名の証明書を生成することや認証権限者から証明書を取得してインストールすることができます。

自己署名の証明書を生成するには、次のコマンドを入力します。

```
Console> (enable)# ip http secure generate self-signed-certificate

A certificate-signing request already exists. Generating a
new self signed certificate will invalidate the existing
signing request and any certificates already generated from
the existing request.  Enter y to reuse the existing
certificate-signing request or n to generate a new one.
Reuse existing certificate-signing request?[y/n] y

The HTTP server is enabled now. You must restart
to generate the certificate. Continue [y/n]? y
-----BEGIN CERTIFICATE-----
MIIDAzCCAmygAwIBAgIBADANBgkqhkiG9w0BAQQFADBlMQswCQYDVQQGEwJBVTET
MBEGA1UECBMKU29tZS1TdGF0ZTEhMB8GA1UEChMYSW50ZXJuZXQgV2lkZ2l0cyBQ
dHkgTHRkMR4wHAYDVQQDExVuYW1sYWItcGlrMy5jaXNjby5jb20wHhcNMDExMDMw
MTAxMDI4WhcNMDIxMDMwMTAxMDI4WjBlMQswCQYDVQQGEwJBVTETMBEGA1UECBMK
U29tZS1TdGF0ZTEhMB8GA1UEChMYSW50ZXJuZXQgV2lkZ2l0cyBQdHkgTHRkMR4w
HAYDVQQDExVuYW1sYWItcGlrMy5jaXNjby5jb20wgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBANsO1T5ayA6pvkJad413V+N/ibvND0XRyXfFycTQRzeA8F4A+etV
s0Iq0muFfiL9mDr/es9TkyfIM+T2F6+NE13DxJ53ZBbh7ndb6WOnzeHLKh9EDfSI
cy2s775lCPCjfLcMsWQLWSU7XUbi/ExDpb9e2wQQgi6QBED/YRkr73KNAgMBAAGj
gcIwgb8wHQYDVR0OBBYEFIHsyecd8AW4cvt7voCFeZMarXIqMIGPBgNVHSMEgYcw
gYSAFIHsyecd8AW4cvt7voCFeZMarXIqoWmkZzBlMQswCQYDVQQGEwJBVTETMBEG
A1UECBMKU29tZS1TdGF0ZTEhMB8GA1UEChMYSW50ZXJuZXQgV2lkZ2l0cyBQdHkg
THRkMR4wHAYDVQQDExVuYW1sYWItcGlrMy5jaXNjby5jb22CAQAwDAYDVR0TBAUw
AwEB/zANBgkqhkiG9w0BAQQFAAOBgQACDyWhULAUeSIXyt9tuUrdPfF97hrpFkKy
nj1yEU4piuc9qQtxG9yCGsofAm+CiGFg6P4qJZtBF47mq81qF+48JTYwi68CGCye
suZgw0iCPQVv4KDirHBKFc0Vr/2SMrXcJImczoV2WGcxWxsVaXwpkBKF8pcMFFYd
iOULMcvFxg==
-----END CERTIFICATE-----
Disabling HTTP server...
Successfully disabled HTTP server.
Enabling HTTP server...
Successfully enabled HTTP server.
```

認証権限者から証明書を取得するには、まず証明書署名要求を生成し、その要求を認証権限者に手動で提出する必要があります。認証権限者から証明書を取得してから、その証明書をインストールします。

証明書のインストール

認証権限者から取得した証明書をインストールする手順は、次のとおりです。

ステップ 1 次のコマンドを入力して、証明書署名要求を生成します。

```
root@localhost# ip http secure generate certificate-request
A certificate-signing request already exists. Generating a
new one will invalidate the existing one and any certificates
already generated from the existing request. Do you still
want to generate a new one? [y/n] y
5244 semi-random bytes loaded
Generating RSA private key, 1024 bit long modulus
.....................................++++++
.++++++
e is 65537 (0x10001)
Using configuration from /usr/local/nam/defaults/openssl.cnf
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:IN
State or Province Name (full name) [Some-State]:Tamil Nadu
Locality Name (eg, city) []:Chennai
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Cisco Systems
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) [hostname.Cisco.com]:
Email Address []:xxx@Cisco.com
-----BEGIN CERTIFICATE REQUEST-----
MIIBzzCCATgCAQAwgY4xCzAJBgNVBAYTAklOMRMwEQYDVQQIEwpUYW1pbCBOYWR1
MRAwDgYDVQQHEwdDaGVubmFpMRYwFAYDVQQKEw1DaXNjbyBTeXN0ZW1zMR4wHAYD
VQQDExVuYW1sYWItcGlrMy5jaXNjby5jb20xIDAeBgkqhkiG9w0BCQEWEXNla2Fy
YmNAY2lzY28uY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC8+SR503gS
ygkf6pnHuh0LelNf6LqJjzwFfjqjS8vpkFq/QVbwqTNDIggUfbvRAIRWEKVWhpRf
rr+II2o/Xzb0RLpV2J2p3HGgoRrKC3nArIFFiSqXniEU+g2mPqsFNcOyxHNXIxEj
iBQf80DxbmvWFOpunmOQ/pGuEysNfU/46wIDAQABoAAwDQYJKoZIhvcNAQEEBQAD
gYEAVAX89pCAcRDOqPgaBEMQCmWD+wqZPnALovr7C81OLBYTgLLqdwPqoSjSYosE
w/pFnIxWN1sJ7MC8+hjnJJLjoCwbyrEyvoiAvzpsGsnAZgWUVaUpR7jlNbf8x2A1
hAOH9KchS0TpSNy13OyhuAkv0pUcM2AJqB/93u4YvuHfNOA=
-----END CERTIFICATE REQUEST-----
```

ステップ 2 次のコマンドを入力して、認証権限者から取得した証明書をインストールします。

```
root@localhost# ip http secure install certificate
The HTTP server is enabled now. You must restart the
server to install certificate. Continue [y/n]? y

Cut and paste the certificate you received from
Certificate Authority. Enter a period (.), then
press enter to indicate the end of the certificate.
-----BEGIN CERTIFICATE-----
MIIDAzCCAmygAwIBAgIBADANBgkqhkiG9w0BAQQFADBlMQswCQYDVQQGEwJBVTET
MBEGA1UECBMKU29tZS1TdGF0ZTEhMB8GA1UEChMYSW50ZXJuZXQgV2lkZ2l0cyBQ
dHkgTHRkMR4wHAYDVQQDExVuYW1sYWItcGlrMy5jaXNjby5jb20wHhcNMDExMDMw
MTAxMDI4WhcNMDIxMDMwMTAxMDI4WjBlMQswCQYDVQQGEwJBVTETMBEGA1UECBMK
U29tZS1TdGF0ZTEhMB8GA1UEChMYSW50ZXJuZXQgV2lkZ2l0cyBQdHkgTHRkMR4w
HAYDVQQDExVuYW1sYWItcGlrMy5jaXNjby5jb20wgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBANsO1T5ayA6pvkJad413V+N/ibvND0XRyXfFycTQRzeA8F4A+etV
s0Iq0muFfiL9mDr/es9TkyfIM+T2F6+NE13DxJ53ZBbh7ndb6WOnzeHLKh9EDfSI
cy2s775lCPCjfLcMsWQLWSU7XUbi/ExDpb9e2wQQgi6QBED/YRkr73KNAgMBAAGj
gcIwgb8wHQYDVR0OBBYEFIHsyecd8AW4cvt7voCFeZMarXIqMIGPBgNVHSMEgYcw
gYSAFIHsyecd8AW4cvt7voCFeZMarXIqoWmkZzBlMQswCQYDVQQGEwJBVTETMBEG
A1UECBMKU29tZS1TdGF0ZTEhMB8GA1UEChMYSW50ZXJuZXQgV2lkZ2l0cyBQdHkg
THRkMR4wHAYDVQQDExVuYW1sYWItcGlrMy5jaXNjby5jb22CAQAwDAYDVR0TBAUw
AwEB/zANBgkqhkiG9w0BAQQFAAOBgQACDyWhULAUeSIXyt9tuUrdPfF97hrpFkKy
nj1yEU4piuc9qQtxG9yCGsofAm+CiGFg6P4qJZtBF47mq81qF+48JTYwi68CGCye
suZgw0iCPQVv4KDirHBKFc0Vr/2SMrXcJImczoV2WGcxWxsVaXwpkBKF8pcMFFYd
iOULMcvFxg==
-----END CERTIFICATE-----
.
Disabling HTTP server...
Successfully disabled HTTP server.
Enabling HTTP server...
Successfully enabled HTTP server.
```

TACACS+ サーバの使用

TACACS+ は、リモート アクセス認証および関連サービスを提供するシスコシステムズの認証プロトコルです。TACACS+ を使用する場合、ユーザ パスワードは個々のルータではなくセントラルデータベースで管理されます。

ユーザが NAM Traffic Analyzer にログインすると、TACACS+ はそのユーザの名前とパスワードが有効かどうかを確認し、ユーザに割り当てられたアクセス権限を判別します。

NAM で TACACS+ を使用するには、事前に NAM と TACACS+ サーバの両方を設定する必要があります。

NAM に TACACS+ を設定する手順は、次のとおりです。

ステップ 1 NAM Traffic Analyzer アプリケーションを起動します。

ステップ 2 **Admin** タブをクリックします。

ステップ 3 **Users** を選択します。

ステップ 4 **TACACS+** を選択します。

ステップ 5 Enable TACACS+ Administration and Authentication ボックスをクリックします。

ステップ 6 オンライン ヘルプの説明に従ってください。

NAM の管理

スイッチ上の NAM の管理手順は、Cisco IOS ソフトウェアと Catalyst OS ソフトウェアのいずれを使用しているかによって異なります。ただし、両方のスイッチ オペレーティング システムに共通する手順もいくつかあります。

以下の各項では、CLI を使用して NAM を管理する手順について、スイッチ オペレーティング システム別に説明します。

- Cisco IOS ソフトウェア（p.44）
- Catalyst OS ソフトウェア（p.54）

ソフトウェア別の NAM 属性の管理が完了した後、以下の項に従って、両方のソフトウェアに共通した属性を設定できます。

- オペレーティング システムに依存しない NAM 管理（p.63）

ここでは、NAM の管理手順を説明します。

Cisco IOS ソフトウェア

ここでは、Cisco IOS を使用して NAM 上で実行できる各種の管理作業について説明します。

- NAM へのログイン（p.44）
- NAM CLI パスワードの変更（p.46）
- NAM のリセット（p.47）
- NAM ソフトウェアのアップグレード（p.47）
- mini-RMON の設定（p.53）

NAM へのログイン

NAM には、アクセス権の異なる 2 種類のユーザ レベルがあります。

- guest — 読み取り専用アクセス
  デフォルトのパスワードは [guest] です。
- root — すべての読み書きアクセス
  デフォルトのパスワードは [root] です。

（注） root アカウントには # プロンプト、guest アカウントには > プロンプトが使用されます。メンテナンス イメージ用のデフォルトの root パスワードと guest パスワードは **cisco** です。

表 6 に、NAM のユーザ レベルとパスワードを示します。

表 6　NAM のユーザとパスワード

アプリケーション イメージ（ハード ディスクに保存されている）		メンテナンス イメージ（コンパクト フラッシュに保存されている）	
ユーザ	パスワード	ユーザ	パスワード
root	root	root	cisco
guest	guest	guest	cisco

（注） NAM メンテナンス イメージの guest アカウントには、すべての読み取り書き込み権限が与えられます。

アプリケーション イメージとメンテナンス イメージのいずれかを起動して IP 情報を設定すると、その情報は両方のイメージの間で同期化されます。ただし、パスワードを変更した場合、その情報はイメージ間で同期化されず、未変更のイメージには変更は反映されません。

リモート Telnet セッションを可能にするには、**exsession on** コマンドを使用します。SSH を使用して NAM にログインすることもできます。この機能を使用するには、crypto パッチをインストールする必要があります。NAM 上で SSH をイネーブルにするには、**exsession on ssh** コマンドを使用します。

NAM にログインする手順は、次のとおりです。

ステップ 1 Telnet 接続またはコンソール ポート接続を使用して、Catalyst 6000 ファミリー スイッチにログインします。

ステップ 2 CLI プロンプトで、次のように **session slot** *slot_number* **processor 1** コマンドを使用して、NAM とのコンソール セッションを確立します。

```
Router# session slot 8 processor 1
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.81 ... Open

Cisco Network Analysis Module (WS-SVC-NAM-1)
```

ステップ 3 NAM ログイン プロンプトに、**root** と入力して root ユーザとしてログインするか、または **guest** と入力して guest ユーザとしてログインします。

```
login: root
```

ステップ 4 パスワード プロンプトに、アカウントに対応するパスワードを入力します。root アカウントのデフォルトのパスワードは [root] であり、guest アカウントのデフォルトのパスワードは [guest] です。

```
Password:
```

正常にログインできると、次のようにコマンドライン プロンプトが表示されます。

```
Network Analysis Module (WS-SVC-NAM-1) Console, 2.1(1)
Copyright (c) 1999, 2000, 2001 by cisco Systems, Inc.

WARNING! Default password has not been changed!

root@localhost#
```

NAM CLI パスワードの変更

出荷時に設定されたデフォルトのパスワードを変更していない場合は、NAM へのログイン時に警告メッセージが表示されます。

ローカル データベース上の Web アプリケーションを使用できます。管理者が不明の場合は、CLI から **rmwebusers** コマンドを使用して、Web ユーザ データベースからローカル Web ユーザを削除できます。

（注） 新しいパスワードは、6 文字以上の長さにしなければなりません。大文字 / 小文字、数字、および句読点を含めることができます。

（注） NAM メンテナンス イメージの root または guest アカウントのパスワードを忘れた場合、メンテナンス イメージをアップグレードする必要があります。アップグレードすると、パスワードはデフォルトに設定されます。表 6（p.44）または表 8（p.55）を参照してください。

パスワードを変更するには、NAM に root アカウントでログインしているときに、次の作業を行います。

ステップ 1 次のコマンドを入力します。

```
root@localhost# password username
```

（注） NAM リリース 2.2 では、*username* 引数を指定する必要があります。

root パスワードを変更するには、NAM に Telnet で接続し、**password root** コマンドを使用します。

guest パスワードを変更するには、NAM に Telnet で接続し、**password guest** コマンドを使用します。

ステップ 2 新しいパスワードを入力します。

```
Changing password for user root
New UNIX password:
```

ステップ 3 もう一度新しいパスワードを入力します。

```
Retype new UNIX password:
passwd: all authentication tokens updated successfully
```

root アカウントにパスワードを設定する例を示します。

```
root@localhost# password root
Changing password for user root
New UNIX password:
Retype new UNIX password:
passwd: all authentication tokens updated successfully
```

パスワードを忘れた場合は、スイッチの CLI から **clear module password** コマンドを入力すると、root アカウントのパスワードを [root] に、guest アカウントのパスワードを [guest] に戻すことができます。

NAM のリセット

CLI または外部 Telnet セッションから NAM にアクセスできない場合は、**hardware_module module module_number reset** コマンドを入力し、NAM をリセットして再起動します。リセット プロセスには数分かかります。

NAM の初回起動時には、自動的にメモリ テストの一部が実行されます。完全なメモリ テストを実行する場合は、**hw-module module** *module_number* **reset** *device:partition* **mem-test-full** コマンドに **mem-test-full** キーワードを使用します。このコマンドは、Cisco IOS 専用のコマンドなので、Catalyst OS ソフトウェアには使用できません。Catalyst OS ソフトウェアについては、「NAM のリセット」（p.58）を参照してください。

NAM をリセットすると、完全なメモリ テストが実行されます。完全なメモリ テストは部分的なメモリ テストよりも完了に時間がかかります。メモリ テストの所要時間は、表 5 を参照してください。

hw-module module *module_number* **mem-test-full** コマンドでもメモリ テストを実行できます。モジュール 5 の完全なメモリ テストを実行するには、次のように入力します。

```
Router(config)#  hw-module module 5 mem-test-full
```

CLI からこのモジュールをリセットするには、イネーブル モードで次の作業を行います。

作業	コマンド
モジュールをリセットします。	**hw-module module** *mod_num* **reset device:***partition* **mem-test-full** device:*partition* の値は、PC ブート デバイス用のストリングです。たとえば、**hdd:x** はハードディスクを示し、**cf:x** はコンパクト フラッシュを示します。いずれも **x** は各デバイス上のパーティションの番号です。

CLI を使用してスロット 9 に搭載された NAM をリセットする例を示します。

```
Router# hardware_module mod 9 reset cf:1 memtest-full

Proceed with reload of module? [confirm] y
% reset issued for module 9
```

（注） ブート デバイスについては、アプリケーション イメージには hdd:1、メンテナンス イメージには cf:1 を指定できます。

NAM ソフトウェアのアップグレード

アプリケーション ソフトウェアとメンテナンス ソフトウェアの両方をアップグレードできます。アプリケーション ソフトウェアをアップグレードする場合は、「NAM アプリケーション ソフトウェアのアップグレード」（p.60）を参照してください。メンテナンス ソフトウェアをアップグレードする場合は、「NAM メンテナンス ソフトウェアのアップグレード」（p.62）を参照してください。

NAM アプリケーション ソフトウェアのアップグレード

NAM アプリケーション ソフトウェアをアップグレードする手順は、次のとおりです。

ステップ 1 NAM アプリケーション ソフトウェア イメージを、FTP からアクセスできるディレクトリにコピーします。

ステップ 2 コンソール ポートまたは Telnet セッションを使用して、スイッチにログインします。

ステップ 3 NAM がすでにメンテナンス イメージで稼働している場合は、ステップ 4 に進んでください。NAM がメンテナンス イメージで稼働していない場合は、イネーブル モードで次のコマンドを入力します。

```
Router# hardware_module module 9 reset cf:1
Device BOOT variable for reset = cf:1
Warning:Device list is not verified.

Proceed with reload of module? [confirm]
% reset issued for module 9
Router#
00:03:31:%SNMP-5-MODULETRAP:Module 9 [Down] Trap
00:03:31:SP:The PC in slot 9 is shutting down. Please wait ...
00:03:41:%SNMP-5-COLDSTART:SNMP agent on host R1 is undergoing a cold
start
00:03:46:SP:PC shutdown completed for module 9
00:03:46:%C6KPWR-SP-4-DISABLED:power to module in slot 9 set off (admin
request)
00:03:49:SP:Resetting module 9 ...
00:03:49:%C6KPWR-SP-4-ENABLED:power to module in slot 9 set on
00:05:53:%SNMP-5-MODULETRAP:Module 9 [Up] Trap
00:05:53:%DIAG-SP-6-BYPASS:Module 9:Online Diagnostics is Bypassed
00:05:53:%OIR-SP-6-INSCARD:Card inserted in slot 9, interfaces are now
online
Router#
```

ステップ 4 NAM がオンラインに戻ったあと、NAM とのコンソール セッションを確立し、root アカウントにログインします。

```
Router# session slot 9 proc 1
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.91 ... Open

Cisco Network Analysis Module (WS-SVC-NAM-1)

Maintenance Partition

login:root
Password:

Network Analysis Module (WS-SVC-NAM-1) Console, 1.2(1a)m
Copyright (c) 1999, 2000, 2001 by cisco Systems, Inc.
```

ステップ 5 次のコマンドを入力して、NAM アプリケーション ソフトウェアをアップグレードします。

```
root@localhost# upgrade ftp-url
```

ftp-url は、NAM ソフトウェア イメージ ファイルの FTP ロケーションおよび名前です。

（注） FTP サーバが匿名ユーザを受け付けない場合は、*ftp-url* の値に、ftp://user@host/absolute-path/filename の構文を使用してください。入力を要求されたら自分のパスワードを入力します。

ステップ 6 アップグレードの間は、表示されるプロンプトに従ってください。

ステップ 7 アップグレードが完了したら、NAM からログアウトします。

ステップ 8 次のコマンドを入力して、NAM をリセットします。

```
Router# hardware_module mod 9 reset
Device BOOT variable for reset =
Warning:Device list is not verified.

Proceed with reload of module? [confirm]
% reset issued for module 9

Router#
00:26:55:%SNMP-5-MODULETRAP:Module 9 [Down] Trap
00:26:55:SP:The PC in slot 8 is shutting down. Please wait ...
```

ステップ 9 （任意）NAM がオンラインに戻った後、NAM の root アカウントにログインし、次のコマンドを入力して、初期設定を確認します。

```
root@localhost# show ip
root@localhost# show snmp
```

NAM アプリケーション ソフトウェアをアップグレードする例を示します。

```
Router# hardware_module module 9 reset cf:1
Device BOOT variable for reset = cf:1
Warning:Device list is not verified.

Proceed with reload of module? [confirm]
% reset issued for module 9

Router#
00:16:06:%SNMP-5-MODULETRAP:Module 9 [Down] Trap
00:16:06:SP:The PC in slot 9 is shutting down. Please wait ...
00:16:21:SP:PC shutdown completed for module 9
00:16:21:%C6KPWR-SP-4-DISABLED:power to module in slot 9 set off (admin
request)
00:16:24:SP:Resetting module 9 ...
00:16:24:%C6KPWR-SP-4-ENABLED:power to module in slot 9 set on
00:18:21:%SNMP-5-MODULETRAP:Module 9 [Up] Trap
00:18:21:%DIAG-SP-6-BYPASS:Module 9:Online Diagnostics is Bypassed
00:18:21:%OIR-SP-6-INSCARD:Card inserted in slot 9, interfaces are now
online

Router# session slot 9 proc 1
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.91 ... Open

Cisco Network Analysis Module (WS-SVC-NAM-1)

Maintenance image
```

```
login:root
Password:

Maintenance image version:1.1(0.1)

root@localhost.cisco.com# upgrade ftp://namlab-pc1/pub/rmon/c6nam2.2-2-0-8.bin.gz

Downloading the image. This may take several minutes...
ftp://namlab-pc1/pub/rmon/c6nam2.2-2-0-8.bin.gz (59198K)
/tmp/upgrade.gz           [#########################]   59198K |  821.24K/s
60619473 bytes transferred in 72.08 sec (821.23k/sec)

Upgrade file ftp://namlab-pc1/pub/rmon/c6nam2.2-2-0-8.bin.gz is downloaded.
Upgrading will wipe out the contents on the hard disk.
Do you want to proceed installing it [y|N]:y

Proceeding with upgrade. Please do not interrupt.
If the upgrade is interrupted or fails, boot into
Maintenance image again and restart upgrade.

Creating NAM application image file...

Initializing the application image partition...
Applying the image, this may take several minutes...
Performing post install, please wait...
Upgrade complete. You can boot from the Application image.

00:21:50:%NAM-3-NO_RESP:Module 9 is not responding
Upgrade complete. You can boot the new application partition.
root@hostname.cisco.com# exit

[Connection to 127.0.0.91 closed by foreign host]
Router#

Router# hardware_module module 9 reset
Device BOOT variable for reset =
Warning:Device list is not verified.

Proceed with reload of module? [confirm] y
% reset issued for module 9


Router#
00:24:04:%SNMP-5-MODULETRAP:Module 9 [Down] Trap
00:24:04:SP:The PC in slot 9 is shutting down. Please wait ...
00:24:18:SP:PC shutdown completed for module 9
00:24:18:%C6KPWR-SP-4-DISABLED:power to module in slot 9 set off (admin
request)
00:24:21:SP:Resetting module 9 ...
00:24:21:%C6KPWR-SP-4-ENABLED:power to module in slot 9 set on
00:26:19:%SNMP-5-MODULETRAP:Module 9 [Up] Trap
00:26:19:%DIAG-SP-6-BYPASS:Module 9:Online Diagnostics is Bypassed
00:26:19:%OIR-SP-6-INSCARD:Card inserted in slot 9, interfaces are now
online
```

NAM メンテナンス ソフトウェアのアップグレード

NAM メンテナンス ソフトウェアをアップグレードする手順は、次のとおりです。

ステップ 1 NAM メンテナンス ソフトウェア イメージを、FTP からアクセスできるディレクトリにコピーします。

ステップ 2 コンソール ポートまたは Telnet セッションを使用して、スイッチにログインします。

ステップ 3 NAM がすでにアプリケーション イメージで稼働している場合は、ステップ 5 に進んでください。NAM がアプリケーション イメージで稼働していない場合は、イネーブル モードで次のコマンドを入力します。

```
Router# hardware_module module 9 reset hdd:1
Device BOOT variable for reset = hdd:1
Warning:Device list is not verified.

Proceed with reload of module? [confirm]
% reset issued for module 9
Router#
00:31:11:%SNMP-5-MODULETRAP:Module 9 [Down] Trap
00:31:11:SP:The PC in slot 9 is shutting down. Please wait ...
00:31:25:SP:PC shutdown completed for module 9
00:31:25:%C6KPWR-SP-4-DISABLED:power to module in slot 9 set off (admin
request)
00:31:28:SP:Resetting module 9 ...
00:31:28:%C6KPWR-SP-4-ENABLED:power to module in slot 9 set on
00:33:26:%SNMP-5-MODULETRAP:Module 9 [Up] Trap
00:33:26:%DIAG-SP-6-BYPASS:Module 9:Online Diagnostics is Bypassed
00:33:26:%OIR-SP-6-INSCARD:Card inserted in slot 9, interfaces are now
online
```

ステップ 4 NAM がオンラインに戻った後、NAM とのコンソール セッションを確立し、root アカウントにログインします。

ステップ 5 次のコマンドを入力して、NAM メンテナンス ソフトウェアをアップグレードします。

```
root@localhost# upgrade ftp-url
```

ftp-url は、NAM ソフトウェア イメージ ファイルの FTP ロケーションおよび名前です。

（注） FTP サーバが匿名ユーザを受け付けない場合は、*ftp-url* の値に、ftp://user@host/absolute-path/filename の構文を使用してください。入力を要求されたら自分のパスワードを入力します。

ステップ 6 アップグレードの間は、表示されるプロンプトに従ってください。

ステップ 7 アップグレードが完了したら、NAM からログアウトします。

ステップ 8 次のコマンドを入力してメンテナンス イメージを起動し、NAM メンテナンス ソフトウェアをリセットします。

```
Router# hardware_module module 9 reset cf:1
Device BOOT variable for reset = cf:1
Warning:Device list is not verified.

Proceed with reload of module? [confirm]
% reset issued for module 9

Router#
00:16:06:%SNMP-5-MODULETRAP:Module 9 [Down] Trap
00:16:06:SP:The PC in slot 9 is shutting down. Please wait ...
00:16:21:SP:PC shutdown completed for module 9
00:16:21:%C6KPWR-SP-4-DISABLED:power to module in slot 9 set off (admin
request)
00:16:24:SP:Resetting module 9 ...
00:16:24:%C6KPWR-SP-4-ENABLED:power to module in slot 9 set on
00:18:21:%SNMP-5-MODULETRAP:Module 9 [Up] Trap
00:18:21:%DIAG-SP-6-BYPASS:Module 9:Online Diagnostics is Bypassed
00:18:21:%OIR-SP-6-INSCARD:Card inserted in slot 9, interfaces are now
online
Router#
```

ステップ 9 （任意）NAM がオンラインに戻った後、NAM の root アカウントにログインし、次のコマンドを入力して初期設定を確認します。

```
root@localhost# show ip
```

ステップ 10 （任意）次のコマンドを入力して、アプリケーション イメージを再起動します。

```
Router# hardware_module module 9 reset
```

NAM メンテナンス ソフトウェアをアップグレードする例を示します。

```
Router#
Router# hardware_module module 9 reset hdd:1
Device BOOT variable for reset = hdd:1
Warning:Device list is not verified.

Proceed with reload of module? [confirm]
% reset issued for module 9
Router#
00:31:11:%SNMP-5-MODULETRAP:Module 9 [Down] Trap
00:31:11:SP:The PC in slot 9 is shutting down. Please wait ...
00:31:25:SP:PC shutdown completed for module 9
00:31:25:%C6KPWR-SP-4-DISABLED:power to module in slot 9 set off (admin
request)
00:31:28:SP:Resetting module 9 ...
00:31:28:%C6KPWR-SP-4-ENABLED:power to module in slot 9 set on
00:33:26:%SNMP-5-MODULETRAP:Module 9 [Up] Trap
00:33:26:%DIAG-SP-6-BYPASS:Module 9:Online Diagnostics is Bypassed
00:33:26:%OIR-SP-6-INSCARD:Card inserted in slot 9, interfaces are now
online
Router#

Router# session slot 9 proc 1
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.91 ... Open
```

```
Cisco Network Analysis Module (WS-SVC-NAM-2)

login:root
Password:

Cisco Network Analysis Module (WS-SVC-NAM-2) Console, 2.2(0.1)
Copyright (c) 1999-2002 by cisco Systems, Inc.

WARNING! Default password has not been changed!
root@localhost.cisco.com#

root@localhost.cisco.com# upgrade ftp://host/pub/rmon/mp.1-1-0-1.bin.gz

Downloading image...
ftp://host/pub/rmon/mp.1-1-0-1.bin.gz (11065K)
-                        [#########################]   11065K |  837.65K/s
11331153 bytes transferred in 13.21 sec (837.64k/sec)

Uncompressing the image...

Verifying the image...

Applying the Maintenance image.
This may take several minutes...

Upgrade of Maintenance image completed successfully.
root@hostname.cisco.com# exit

Router# hardware_module module 9 reset cf:1
Device BOOT variable for reset = cf:1
Warning:Device list is not verified.

Proceed with reload of module? [confirm]
% reset issued for module 9
Router#
02:27:19:%SNMP-5-MODULETRAP:Module 9 [Down] Trap
02:27:19:SP:The PC in slot 9 is shutting down. Please wait ...
02:27:36:SP:PC shutdown completed for module 9
02:27:36:%C6KPWR-SP-4-DISABLED:power to module in slot 9 set off (admin
request)
02:27:39:SP:Resetting module 9 ...
02:27:39:%C6KPWR-SP-4-ENABLED:power to module in slot 9 set on
02:29:37:%SNMP-5-MODULETRAP:Module 9 [Up] Trap
02:29:37:%DIAG-SP-6-BYPASS:Module 9:Online Diagnostics is Bypassed
02:29:37:%OIR-SP-6-INSCARD:Card inserted in slot 9, interfaces are now
online
Router#
```

mini-RMON の設定

Cisco IOS では、インターフェイスごとに明示的に mini-RMON をイネーブルにする必要があります。各インターフェイスに mini-RMON を設定するには、**rmon collection stats** *collection-control-index* **owner** *owner-string* を入力します。*collection-control-index* および *owner-string* には値を入力する必要があります。

（注） NAM が表示するのは、モニタのオーナー ストリングが設定されている mini-RMON 収集だけです。

ファスト イーサネット モジュール 4 ポート 1 上の mini-RMON にコントロール インデックス 3000 とモニタのオーナー ストリングの使用を設定する場合は、次の例のように入力します。

```
Router#  config term
Router(config)# interface fast4/1
router(config-if)# rmon collection stats 3000 owner monitor
router(config-if)# end
```

Catalyst OS ソフトウェア

ここでは、Catalyst OS ソフトウェアを使用して NAM 上で実行できる各種の管理作業について説明します。

- NAM へのログイン（p.55）
- NAM CLI パスワードの変更（p.56）
- NAM のリセット（p.58）
- NAM ソフトウェアのアップグレード（p.60）
- mini-RMON の設定（p.63）

NAM Traffic Analyzer アプリケーションを使用して NAM を管理できます。Traffic Analyzer についての詳細は、『*User Guide for the Catalyst 6000 Network Analysis Module NAM Traffic Analyzer*』を参照してください。

NAM に関する次の管理作業を行うことができます。

- CLI または NAM Traffic Analyzer アプリケーションを使用して、NAM ユーザの追加と削除およびパスワードの変更を行う。
- スーパーユーザ用パスワードを回復する（ただしパスワードは変更しない）。
- NAM Traffic Analyzer アプリケーションを使用して、ローカルおよびリモート（TACACS+ サーバ）のユーザおよびパスワードを変更する。ユーザおよびパスワードの管理についての詳細は、NAM Traffic Analyzer アプリケーションのオンライン ヘルプ トピック「User and System Administration」を参照してください。

表 7 に、CLI および NAM Traffic Analyzer アプリケーションを使用して実行できるユーザ管理作業について説明します。

表 7　NAM のユーザ管理

ユーザ インターフェイス	ユーザの追加	ユーザの削除	パスワードの設定	パスワードの回復
CLI	不可	Yes **rmwebusers** コマンドを使用して、ローカルデータベースから Web ユーザをすべて削除します。	**password** コマンドを使用します。	不可
Traffic Analyzer	Web サーバの起動時に、CLI を使用して最初のユーザを追加します。その他のユーザは Web GUI を使用してローカルデータベースに追加します。TACACS+ サーバを使用している場合には、TACACS+ サーバ経由で追加します。			

表 7　NAM のユーザ管理（続き）

ユーザ インターフェイス	ユーザの追加	ユーザの削除	パスワードの設定	パスワードの回復
Traffic Analyzer ローカル データベース	可	可	可	NAM 管理者に連絡し、GUIを使用して再設定します。 NAM の CLI から、**rmwebusers** コマンドを使用します。
Traffic Analyzer TACACS+	可	可	可	TACACS+ サーバを使用するか、または **ip http tacacs+ disable** コマンドを使用します。

NAM へのログイン

NAM には権限の異なる 2 つのアクセス レベルがあります。

- Guest — 読み取り専用 CLI アクセス（デフォルトのパスワードは [guest]）
- Root — すべての読み取り書き込みアクセス（デフォルトのパスワードは [cisco]）

（注）　root アカウントには # プロンプト、guest アカウントには > プロンプトが使用されます。メンテナンス イメージ用のデフォルトの root パスワードと guest パスワードは **cisco** です。

表 8 に、NAM のユーザ レベルとパスワードを示します。

表 8　NAM のユーザとパスワード

アプリケーション イメージ（ハード ディスクに保存されている）		メンテナンス イメージ（コンパクト フラッシュに保存されている）	
ユーザ	パスワード	ユーザ	パスワード
root	root	root	cisco
guest	guest	guest	cisco

（注）　NAM メンテナンス イメージの guest アカウントには、すべての読み取り書き込み権限が与えられます。

アプリケーション イメージとメンテナンス イメージのいずれかを起動して IP 情報を設定すると、その情報は両方のイメージ間で同期化されます。ただし、パスワードを変更した場合、その情報はイメージ間で同期化されず、未変更のイメージには変更は反映されません。

NAM にログインする手順は、次のとおりです。

ステップ 1 Telnet 接続またはコンソール ポート接続を使用して、Catalyst 6000 ファミリー スイッチにログインします。

（注） リモート Telnet セッションを確立するには、**exsession on** コマンドを使用します。SSH を使用して NAM にログインすることもできます。この機能を使用するには、crypto パッチをインストールする必要があります。NAM 上で SSH をイネーブルにするには、**exsession on ssh** コマンドを使用します。

ステップ 2 CLI プロンプトに **session** *mod* コマンドを入力し、NAM とのコンソール セッションを確立します。

```
Console> (enable) session 4
Trying NAM-4...
Connected to NAM-4.
Escape character is '^]'.

Cisco Network Analysis Module (WS-SVC-NAM-1)

login:root
Password:
```

ステップ 3 NAM にログインします。ログイン プロンプトに **root** と入力して root ユーザとしてログインするか、または **guest** と入力して guest ユーザとしてログインします。

```
login: root
```

ステップ 4 パスワード プロンプトに、アカウントに対応するパスワードを入力します。root アカウントのデフォルトのパスワードは [root] であり、guest アカウントのデフォルトのパスワードは [guest] です。

```
Password:
```

正常にログインできると、次のようにコマンドライン プロンプトが表示されます。

```
Network Analysis Module (WS-SVC-NAM-1) Console, 2.2(0.1)
Copyright (c) 1999-2002 by Cisco Systems, Inc.
WARNING! Default password has not been changed!

root@localhost#
```

NAM CLI パスワードの変更

次の方法で、パスワードの変更および回復を行うことができます。

- NAM および CLI への Telnet 接続を使用します。

  root パスワードおよび guest パスワードの設定、変更、および回復を行うことができます。

  - パスワードを変更するには、NAM に Telnet で接続し、**password** コマンドを使用します。
  - パスワードを回復するには、スーパバイザ エンジンに Telnet で接続し、**clear module password** *module* コマンドを使用します。
  - パスワードを忘れた場合は、スイッチの CLI から **clear module** *password* コマンドを入力すると、root アカウントのパスワードを [root] に、guest アカウントのパスワードを [guest] に戻すことができます。

- NAM のパスワードを出荷時のデフォルト値に戻すには、イネーブル モードで次のコマンドを入力します。

  ```
  Console> (enable) clear module password module
  ```

- ローカル データベース上で NAM Traffic Analyzer を使用します。

  CLI を使用して、最初の NAM Traffic Analyzer アプリケーション ユーザを作成します。NAM Traffic Analyzer の起動後に、その他のユーザ パスワードの設定と編集を行うことができます。次のようにNAM Traffic AnalyzerまたはTACACS+サーバを使用して、パスワードを変更します。

  - NAM Traffic Analyzer アプリケーションの管理者として、パスワードを再設定できます。
  - 管理者が不明の場合は、CLI から **rmwebusers** コマンドを使用して、Web データベースからローカル Web ユーザ データベースを削除できます。

- TACACS+ サーバのマニュアルに記載されている説明に従ってください。

（注） NAM メンテナンス イメージの root アカウントまたは guest アカウントのパスワードを忘れた場合は、メンテナンス イメージをアップグレードする必要があります。アップグレードすると、パスワードはデフォルトに設定されます。表 6（p.44）または表 8（p.55）を参照してください。

出荷時に設定されたデフォルトのパスワードを変更していない場合は、NAM へのログイン時に警告メッセージが表示されます。

（注） 新しいパスワードは、6 文字以上の長さにしなければなりません。大文字 / 小文字、数字、および句読点を含めることができます。

パスワードを変更するには、NAM に [root] としてログインしているときに、次の作業を行います。

ステップ 1 次のコマンドを入力します。

```
root@localhost# password [username]
```

（注） リリース 2.2 の NAM ソフトウェアでは、*username* 引数を指定する必要があります。

root パスワードを変更するには、NAM に Telnet で接続し、**password root** コマンドを使用します。guest パスワードを変更するには、NAM に Telnet で接続し、**password guest** コマンドを使用します。

ステップ 2 新しいパスワードを入力します。

```
Changing password for user root
New UNIX password:
```

ステップ 3 もう一度新しいパスワードを入力します。

```
Retype new UNIX password:
passwd: all authentication tokens updated successfully
```

root アカウントにパスワードを設定する例を示します。

```
root@localhost# password root
Changing password for user root
New UNIX password:
Retype new UNIX password:
passwd: all authentication tokens updated successfully
```

パスワードを忘れた場合は、CLI から **clear module password** コマンドを入力すると、root アカウントのパスワードを [root] に、guest アカウントのパスワードを [guest] に戻すことができます。

NAM のリセット

CLI または外部 Telnet セッションから NAM にアクセスできない場合は、**reset** *mod_num boot_string* コマンドを入力し、NAM をリセットして再起動します。リセット プロセスには数分かかります。

NAM の初回の起動時には、自動的にメモリ テストの一部が実行されます。完全なメモリ テストを実行する場合は、**set boot device** *bootseq mod#* **mem-test-full** コマンドを入力します。このコマンドは、Catalyst OS ソフトウェア専用のコマンドなので、Cisco IOS ソフトウェアには使用できません。Cisco IOS については、「NAM のリセット」（p.47）を参照してください。

完全なメモリ テストをイネーブルにするには、**set boot device** *bootseq mod#* **mem-test-full** コマンドを入力します。完全なメモリ テストの実行例を示します。

```
Console (enable) set boot device cf:1 4 mem-test-full
Device BOOT variable = cf:1
Memory-test set to FULL
Warning:Device list is not verified but still set in the boot string.

Console> (enable) show boot device 4
Device BOOT variable = cf:1
Memory-test set to FULL
```

NAM をリセットすると、完全なメモリ テストが実行されます。

部分的なメモリ テストをリセットする例を示します。

```
Console> (enable) set boot device cf:1 4
Device BOOT variable = cf:1
Memory-test set to PARTIAL
Warning:Device list is not verified but still set in the boot string.
Console> (enable)
Console> (enable) show boot device 4
Device BOOT variable = cf:1
Memory-test set to PARTIAL
```

CLI を使用して NAM をリセットするには、イネーブル モードで次の作業を行います。

作業	コマンド
NAM をリセットします。	**reset** *mod_num boot_string* *mod_num boot_string* 変数は、PC ブート デバイス用のストリングです。**hdd:x** はハードディスクを示し、**cf:x** はコンパクト フラッシュを示します。いずれも **x** は各デバイス上のパーティションの番号です。

スロット 9 に搭載された NAM をリセットする例を示します。

```
Router#  reset 9 hdd:1

Proceed with reload of module? [confirm] y
% reset issued for module 9
```

（注） ブート デバイスについては、アプリケーション イメージには hdd:1、メンテナンス イメージには cf:1 を指定できます。

```
Router#
00:26:55:%SNMP-5-MODULETRAP:Module 9 [Down] Trap
00:26:55:SP:The PC in slot 8 is shutting down. Please wait ...
```

モジュールをメンテナンス イメージにリセットするには、イネーブル モードから次のコマンドを入力します。

```
Console> (enable) reset <module #> cf:1
```

モジュールを NAM アプリケーション イメージにリセットするには、イネーブル モードから次のコマンドを入力します。

```
Console> (enable) reset <module #>
```

CLI を使用してスロット 4 に搭載された NAM をリセットする例を示します。

```
Console> (enable) reset 4
This command will reset module 4.
Unsaved configuration on module 4 will be lost
Do you want to continue (y/n) [n]? y
ResetPcBlade:start shutdown module 4
SendShutDownMsg - proc_id (1):shut down PC success.
Module 4 shut down in progress, please don't remove module until shutdown comple
ted.
Module 4 is online.
```

完全なメモリ テストをイネーブルにするには、**set boot device** *bootseq mod#***mem-test-full** コマンドを入力します。このオプションは、デフォルトではディセーブルになっています。完全なメモリ テストを実行する例を示します。

```
Console (enable) set boot device cf:1 4 mem-test-full
Device BOOT variable = cf:1
Memory-test set to FULL
Warning:Device list is not verified but still set in the boot string.

Console> (enable) show boot device 4
Device BOOT variable = cf:1
Memory-test set to FULL
```

NAM をリセットすると、完全なメモリ テストが実行されます。完全なメモリ テストは部分的なメモリ テストよりも完了に時間がかかります。メモリ テストの所要時間は、表 5 を参照してください。

部分的なメモリ テストをリセットする例を示します。

```
Console> (enable) set boot device cf:1 4
Device BOOT variable = cf:1
Memory-test set to PARTIAL
Warning:Device list is not verified but still set in the boot string.
Console> (enable)
Console> (enable) show boot device 4
Device BOOT variable = cf:1
Memory-test set to PARTIAL
```

NAM ソフトウェアのアップグレード

アプリケーション ソフトウェアとメンテナンス ソフトウェアの両方をアップグレードできます。アプリケーション ソフトウェアをアップグレードする場合は、「NAM アプリケーション ソフトウェアのアップグレード」（p.60）を参照してください。メンテナンス ソフトウェアをアップグレードする場合は、「NAM メンテナンス ソフトウェアのアップグレード」（p.62）を参照してください。

NAM アプリケーション ソフトウェアのアップグレード

NAM アプリケーション ソフトウェアをアップグレードする手順は、次のとおりです。

ステップ 1 NAM アプリケーション ソフトウェア イメージを、FTP からアクセスできるディレクトリにコピーします。

ステップ 2 コンソール ポートまたは Telnet セッションを使用して、スイッチにログインします。

ステップ 3 NAM がすでにメンテナンス イメージで稼働している場合には、ステップ 4 に進んでください。NAM がメンテナンス イメージで稼働していない場合は、イネーブル モードで次のコマンドを入力します。

```
Console> (enable) reset mod cf:1
```

ステップ 4 NAM がオンラインに戻った後、NAM とのコンソール セッションを確立し、root アカウントにログインします。

ステップ 5 次のコマンドを入力して、NAM アプリケーション ソフトウェアをアップグレードします。

```
root@localhost# upgrade ftp-url
```

ftp-url は、NAM ソフトウェア イメージ ファイルの FTP ロケーションおよび名前です。

（注） FTP サーバが匿名ユーザを受け付けない場合は、*ftp-url* の値に、ftp://user@host/absolute-path/filename の構文を使用してください。入力を要求されたら自分のパスワードを入力します。

ステップ 6 アップグレードの間は、表示されるプロンプトに従ってください。

ステップ 7 アップグレードが完了したら、メンテナンス イメージからログアウトします。

ステップ 8 次のコマンドを入力して、NAM アプリケーション イメージにリセットします。

```
Console> (enable) reset mod
```

ステップ 9 （任意）NAM がオンラインに戻った後に、NAM の root アカウントにログインし、次のコマンドを入力して、初期設定を確認します。

```
root@localhost# show ip
root@localhost# show snmp
```

NAM アプリケーション ソフトウェアをアップグレードする例を示します。

```
Console> (enable) reset 4 cf:1
This command will reset module 4.
Unsaved configuration on module 4 will be lost
Do you want to continue (y/n) [n]? y
ResetPcBlade:start shutdown module 4
2002 May 07 22:21:20 %SYS-5-MOD_RESET:Module 4 reset from Software
Console> (enable) 2002 May 07 22:24:41 %SYS-3-SUP_OSBOOTSTATUS:MP OS Boot Status
:finished booting

Console> (enable) session 4
Trying NAM-4...
Connected to NAM-4.
Escape character is '^]'.

Maintenance image

login:root
Password:

Maintenance image version:1.1(0.1)

root@localhost# upgrade ftp://namlab-pc1/pub/rmon/c6nam2.2-2-0-8.bin.gz
Downloading the image. This may take several minutes...
ftp://namlab-pc1/pub/rmon/c6nam2.2-2-0-8.bin.gz (59198K)
/tmp/upgrade.gz           [#########################]   59198K |  821.24K/s
60619473 bytes transferred in 72.08 sec (821.23k/sec)

Upgrade file ftp://namlab-pc1/pub/rmon/c6nam2.2-2-0-8.bin.gz is downloaded.
Upgrading will wipe out the contents on the hard disk.
Do you want to proceed installing it [y|N]:y

Proceeding with upgrade. Please do not interrupt.
If the upgrade is interrupted or fails, boot into
Maintenance image again and restart upgrade.

Creating NAM application image file...

Initializing the application image partition...
Applying the image, this may take several minutes...
Performing post install, please wait...
Upgrade complete. You can boot from the Application image.

Console> (enable) reset 4
This command will reset module 4.
Unsaved configuration on module 4 will be lost
Do you want to continue (y/n) [n]? y
ResetPcBlade:start shutdown module 4
SendShutDownMsg - proc_id (1):shut down PC success.
Module 4 shut down in progress, please don't remove module until shutdown comple
ted.
Console> (enable) 2002 May 07 23:19:03 %SYS-5-MOD_OK:Module 4 is online
```

NAM メンテナンス ソフトウェアのアップグレード

NAM メンテナンス ソフトウェアをアップグレードする手順は、次のとおりです。

ステップ 1 NAM メンテナンス ソフトウェア イメージを、FTP からアクセスできるディレクトリにコピーします。

ステップ 2 コンソール ポートまたは Telnet セッションを使用して、スイッチにログインします。

ステップ 3 NAM がすでにアプリケーション イメージで稼働している場合は、ステップ 4 に進んでください。NAM がアプリケーション イメージで稼働していない場合は、イネーブル モードで次のコマンドを入力します。

```
Console> (enable) reset mod
```

ステップ 4 NAM がオンラインに戻った後、NAM とのコンソール セッションを確立し、root アカウントにログインします。

ステップ 5 次のコマンドを入力して、NAM メンテナンス ソフトウェアをアップグレードします。

```
root@localhost# upgrade ftp-url
```

ftp-url は、NAM ソフトウェア イメージ ファイルの FTP ロケーションおよび名前です。

（注） FTP サーバが匿名ユーザを受け付けない場合は、*ftp-url* の値に、ftp://user@host/absolute-path/filename の構文を使用してください。入力を要求されたら自分のパスワードを入力します。

ステップ 6 アップグレードの間は、表示されるプロンプトに従ってください。

ステップ 7 アップグレードが完了したら、NAM からログアウトします。

ステップ 8 次のコマンドを入力してメンテナンス イメージを起動し、NAM メンテナンス ソフトウェアをリセットします。

```
Console> (enable) reset mod cf:1
```

ステップ 9 （任意）NAM がオンラインに戻った後に、NAM の root アカウントにログインし、次のコマンドを入力して、初期設定を確認します。

```
root@localhost# show ip
root@localhost# show snmp
```

ステップ 10 （任意）次のコマンドを入力して、アプリケーション イメージを再起動します。

```
Console> (enable) reset mod
```

NAM メンテナンス ソフトウェアをアップグレードする例を示します。

```
Console> (enable) reset 4
This command will reset module 4.
Unsaved configuration on module 4 will be lost
Do you want to continue (y/n) [n]? y
ResetPcBlade:start shutdown module 4
SendShutDownMsg - proc_id (1):shut down PC success.
Module 4 shut down in progress, please don't remove module until shutdown comple
ted.
Console> (enable) 2002 May 07 23:19:03 %SYS-5-MOD_OK:Module 4 is online

Console> (enable) session 4
Trying NAM-4...
Connected to NAM-4.
Escape character is '^]'.

Cisco Network Analysis Module (WS-SVC-NAM-2)

login:root
Password:

Cisco Network Analysis Module (WS-SVC-NAM-2) Console, 2.2(0.1)
Copyright (c) 1999-2002 by cisco Systems, Inc.

WARNING! Default password has not been changed!
root@localhost.cisco.com#
root@localhost.cisco.com# upgrade ftp://host/pub/rmon/mp.1-1-0-1.bin.gz

Downloading image...
ftp://host/pub/rmon/mp.1-1-0-1.bin.gz (11065K)
-                        [#########################]   11065K |  837.65K/s
11331153 bytes transferred in 13.21 sec (837.64k/sec)

Uncompressing the image...

Verifying the image...

Applying the Maintenance image.
This may take several minutes...

Upgrade of Maintenance image completed successfully.
```

mini-RMON の設定

Catalyst OS ソフトウェアでは、スイッチの mini-RMON をイネーブルにできます。

mini-RMON の設定例を示します。

```
Console (enable)# set snmp rmon enable
```

オペレーティング システムに依存しない NAM 管理

ここでは、スイッチ オペレーティング システムに依存しないNAMの管理作業について説明します。

NAM パッチ ソフトウェアの追加

NAM にパッチをインストールするには、次の作業を行います。

ステップ 1 コンソール ポートまたは Telnet セッションを使用して、スイッチにログインします。

ステップ 2 NAM がすでにアプリケーション イメージで稼働している場合は、ステップ 4 に進んでください。NAM がメンテナンス イメージで稼働している場合は、イネーブル モードで次のコマンドを入力します。

Cisco IOS ソフトウェアの場合は、次のコマンドを入力します。

```
Console> (enable) hardware_module module module_number reset
```

Catalyst OS ソフトウェアの場合は、次のコマンドを入力します。

```
Console> (enable) reset mod hdd:1
```

ステップ 3 NAM がオンラインに戻った後に、NAM とのコンソール セッションを確立し、root アカウントにログインします。

ステップ 4 次のコマンドを入力して、NAM ソフトウェアにパッチ ソフトウェアをインストールします。

```
root@localhost# patch ftp-url
```

ftp-url は、NAM パッチ ソフトウェア イメージ ファイルの FTP ロケーションおよび名前です。

（注） FTP サーバが匿名ユーザを受け付けない場合は、*ftp-url* の値に、ftp://user@host/*absolute-path*/*filename* の構文を使用してください。入力を要求されたら自分のパスワードを入力します。

ステップ 5 パッチ アプリケーションの処理中は、表示されるプロンプトに従ってください。

ステップ 6 （任意）NAM がオンラインに戻った後に、NAM の root アカウントにログインし、次のコマンドを入力して初期設定を確認します。

```
root@localhost# show ip
root@localhost# show patches
```

Catalyst OS ソフトウェアで、パッチ ソフトウェアを適用する例を示します。

```
Console> (enable) reset 4
This command will reset module 4.
Unsaved configuration on module 4 will be lost
Do you want to continue (y/n) [n]? y
ResetPcBlade:start shutdown module 4
SendShutDownMsg - proc_id (1):shut down PC success.
Module 4 shut down in progress, please don't remove module until shutdown comple
ted.
Console> (enable) 2002 May 07 23:19:03 %SYS-5-MOD_OK:Module 4 is online

Console> (enable) session 4
Trying NAM-4...
Connected to NAM-4.
Escape character is '^]'.

Cisco Network Analysis Module (WS-SVC-NAM-2)

login:root
Password:
Cisco Network Analysis Module (WS-SVC-NAM-2) Console, 2.2(0.1)
Copyright (c) 1999-2002 by cisco Systems, Inc.

WARNING! Default password has not been changed!
root@localhost.cisco.com#

root@localhost# patch ftp://host/pub/patch_rpms/c6nam-
2.2-strong-cryptoK9-patch-1-0.bin

Proceeding with installation. Please do not interrupt.
If installation is interrupted, please try again.

Downloading c6nam-2.2-strong-cryptoK9-patch-1-0.bin Please wait...
ftp://host/pub/patch_rpms/c6nam-2.2-strong-cryptoK9-patch-1-0 (1
K)
-                         [#########################]       1K | 1071.96K/s
2022 bytes transferred in 0.00 sec (1006.91k/sec)

Verifying c6nam-2.2-strong-cryptoK9-patch-1-0. Please wait...
Patch c6nam-2.2-strong-cryptoK9-patch-1-0 verified.

Applying /usr/local/nam/patch/workdir/c6nam-2.2-strong-cryptoK9-patch-1-0. Pleas
e wait...
############################################ [100%]
############################################ [100%]

Patch applied successfully.
```

その他の NAM ソフトウェア管理コマンド

NAM は、次の管理コマンドをサポートします。

コマンド	説明
clear ip	インターフェイスのネットワーク設定を消去します。
clear log upgrade	アプリケーション イメージのアップグレード ログ ファイルを消去します。このコマンドを使用できるのは、メンテナンス イメージが稼働している場合だけです。メンテナンス イメージの guest アカウントで使用できます。

コマンド	説明
config clear	次のように、NVRAM コンフィギュレーションが消去されて、出荷時のデフォルト状態に戻ります。 • すべての RMON 制御テーブルを削除 • すべての RMON1 および RMON2 フィルタを削除 • RMON コンフィギュレーション ファイルをデフォルトの設定に戻す • プロトコル ディレクトリをデフォルトの設定に戻す IP ホスト コンフィギュレーション データは削除されません。 変更を有効にするには、**config clear** コマンドを入力した後に NAM をリセットする必要があります。 このコマンドを使用できるのは、root アカウントだけです。
coredump ftp://host/*absolute-path*	RMON エージェントのクラッシュ後に、匿名 FTP サーバにコア ファイルを送信します。このコマンドによって、複数のコア ファイルがアップロードされる可能性があります。このコマンドは、/usr/local/nam/bin ディレクトリの下にある [core] 形式のすべてのコア ファイルをアップロードします。TAC に問い合わせる前に、必ずこの情報をファイルにコピーし、保存してください。TAC は、この情報を使用して、NAM を分析し、トラブルシューティングを行います。維持されるコア ダンプ ファイルは 1 つだけです。コア ダンプ ファイルが新しく作成されると、既存のコア ダンプ ファイルが上書きされます。このコマンドを使用できるのは、root アカウント*だけ*です。 （注） FTP サーバが匿名ユーザを受け付けない場合は、**coredump ftp:**//*user:password@host/absolute-path* という構文を使用してください。
disable-guest	メンテナンス イメージから、guest アカウントをディセーブルにします。
enable-guest	メンテナンス イメージから、guest アカウントをイネーブルにします。
exsession [*on* | *off*] [**ssh**]	（注） SSH をイネーブルまたはディセーブルに設定するには、crypto パッチをインストールする必要があります。「Strong Crypto パッチのインストール」（p.39）を参照してください。 NAM がスイッチ外部からの外部 Telnet セッションを受け付けるかどうかを制御します。デフォルトでは off に設定されます。**exsession** コマンドが off に設定されている場合、NAM に Telnet でアクセスできるのは、スイッチ上のスーパバイザ エンジンからだけになります。**exsession** コマンドが on に設定されている場合は、有効なあらゆる IP アドレスからの新しい Telnet 要求が受け入れられます。このコマンドによって、オープンされているセッションが切断されることはありません。このコマンドを使用できるのは、root アカウントだけです。 **exsession on —** Telnet をイネーブルにします。 **exsession on ssh —** SSH をイネーブルにします。 **exsession off —** Telnet をディセーブルにします。 **exsession off ssh —** SSH をディセーブルにします。

コマンド	説明
[*command*] **help**	最上位レベルのコマンドのリスト、または個々のコマンドの補足情報を表示します。 （注） メンテナンス イメージにはこのコマンドはありません。ヘルプ情報を利用するには、代わりに **?** を入力する必要があります。
ip	IP パラメータを設定します。このコマンドは、アプリケーション イメージとメンテナンス イメージで利用できます。メンテナンス イメージでは、guest アカウントで使用できます。
ip address *ip-address netmask*	ネットワーク上のノードの IP アドレスおよびサブネットを指定します。
ip broadcast *broadcast-address*	ネットワーク上のノードの IP ブロードキャスト アドレスを指定します。
ip domain *domain-name*	ドメイン名を指定します。
ip gateway *gateway-address*	デフォルトの IP ゲートウェイを指定します。
ip host *hostname*	IP ホスト名を指定します。
ip hosts add *ip address host_name* [**alias 1**] [**alias 2**]	hosts ファイルにホスト エントリを追加します。
ip hosts add *ftp://user:passwd@host/full-path/filename*	リモート ファイルからのホスト エントリを hosts ファイルに追加します。
ip hosts delete	hosts ファイルからホスト エントリを削除します。
ip hosts delete *ftp://user:passwd@host/full-path/filename*	hosts ファイル内のリモート ファイルからのホスト エントリを削除します。
ip nameserver [*name-server1*] [*name-server2*] [*name-server3*]	ネットワーク名からネットワーク アドレスへの変換に使用する IP ネーム サーバを指定します。
ip nameserver disable	設定されているネーム サーバをディセーブルにします。
logout	メンテナンス イメージのシェルおよびメンテナンス イメージの guest アカウントからログアウトします。
nslookup *hostname* [**server**]	ホストに関する情報をネーム サーバに照会できるようにします。server を指定しない場合、NAM DNS サーバが使用されます。
passwd	現在のユーザのパスワードを設定します。
passwd-guest	メンテナンス イメージから、guest アカウントのパスワードを設定します。
patch *ftp://user:passwd@host/full-path/filename*	指定した場所から、アプリケーション ソフトウェアにパッチを適用します。
ping [**-nv**] [**-c** *count*] [**-i** *wait*] [**-p** *pattern*] [**-s** *packetsize*] **hostname** | **IP address**	ネットワーク上の他のノードに ICMP エコー要求パケットを送信します。引数を指定しないコマンドを使用して ping を設定することもできます。 次のオプションがサポートされています。 **-n** — ネットワーク アドレスを数字で表示します。 **-v** — 冗長な出力を提供します。 **-c** *count* — count 個の ECHO_REQUEST パケットを送信した後、停止します。 **-i** *wait* — パケットを送信するたびに、指定する秒数だけ待機します。 **-p** *pattern* — 最大 16 パッド バイトを使用して、送信するパケットを充填できます。 **-s** *packetsize* — 8 バイトの ICMP ヘッダー データ。

コマンド	説明
reboot	アプリケーション イメージから NAM を再起動します。
rmon artmib {enable | disable}	アプリケーション イメージから RMON artmib をイネーブルまたはディセーブルに設定します。
show	メンテナンス イメージのシステム パラメータおよびメンテナンス イメージの guest アカウントを表示します。
show autostart	統計情報、アドレス マッピング、VLAN、および MIB のレポートをイネーブルにします。
show bios	NAM のシリアル番号を含め、BIOS およびモジュールに関するシステム情報が表示されます。TAC が、これらの情報をトラブルシューティングのために必要とする場合があります。TAC に連絡する前に、この情報をファイルにコピーし、保存してください。このコマンドは、root アカウントと guest アカウントのどちらでも使用できます。
show certificate	セキュア サーバ用にインストールした証明書を表示します。
show certificate-request	セキュア サーバ用の暗号化された証明書要求を表示します。
show cpu	すべての機能を合計して、NAM CPU 上の現在のプロセッサ負荷が表示されます。このコマンドは、root アカウントと guest アカウントのどちらでも使用できます。
show date	NAM が維持している現在の時刻情報が表示されます。このコマンドは、root アカウントと guest アカウントのどちらでも使用できます。
show diaglog	メンテナンス イメージの guest アカウントで診断ログ ファイルを表示します。
show ethif	メンテナンス イメージの guest アカウントでイーサネット インターフェイス情報を表示します。
show hosts	hosts ファイルが表示されます。
show images	NAMアプリケーション イメージにインストールされているイメージをリストします。このコマンドを使用できるのは、メンテナンス イメージの場合だけです。
show ip	現在の IP コンフィギュレーション（HTTP サーバ、セキュア サーバ、ポート、セキュア ポート、および TACACS+ 情報を含む）が表示されます。
show log	アプリケーション イメージのログが表示されます。
show log upgrade	アプリケーション イメージで NAM が稼働している場合は、メンテナンス イメージのアップグレード ログが表示されます。 メンテナンス イメージで NAM が稼働している場合は、アプリケーション イメージのアップグレード ログが表示されます。
show memory	システム メモリの統計情報が表示されます。メモリ サイズは、最も近い MB に収められます。このコマンドは、root アカウントと guest アカウントのどちらでも使用できます。
show options	ART MIB および音声モニタリングの設定ステータスが表示されます。
show patches	インストールされているソフトウェア パッチが表示されます。
show rxcounters	RX データ カウンタが表示されます。
show snmp	SNMP の設定が表示されます。
show tech-support	TAC がトラブルシューティングのために必要とするシステム情報が表示されます。TAC に連絡する前に、この情報をファイルにコピーし、保存してください。このコマンドを使用できるのは、root アカウントだけです。

コマンド	説明
show version	NAM メンテナンス イメージのバージョン、ドータカード情報、NAM アプリケーション イメージのバージョンが表示されます。 • メンテナンス イメージから **show version** コマンドを実行した場合、その出力には、NAM アプリケーション イメージのバージョンは表示されません。 • アプリケーション イメージから **show version** コマンドを実行した場合、その出力には、NAM メンテナンス イメージのバージョンは表示されません。
snmp community *community-string* **{ro | rw}**	SNMP コミュニティ ストリングの値を設定します。
traceroute [**-Inv**] [**-f** *first_ttl*] [**-m** *max_ttl*] [**-p** *port*] [**-s** *src_addr*] [**-t** *tos*] [**-w** *waittime*] **destination host name** | **IP address** [*packetlen*]	次のオプションがサポートされています。 **-I —** UDP データグラムの代わりに ICMP ECHO を使用します。 **-n —** ホップ アドレスを数値で表示します。 **-v —** 冗長な出力を提供します。 **-f** *first_ttl* **—** 最初の発信パケットで使用される初期的な Time-To-Live（TTL）を設定します。 **-m** *max_ttl* **—** 使用する最大の TTL（最大ホップ数）を設定します。 **-p** *port* **—** プローブで使用されるベース UDP ポート番号を設定します。 **-s** *src_addr* **—** 送信元アドレスを、パケット送信に使用するインターフェイスの IP アドレス以外にします。 **-t** *tos* **—** パケットの Type of Service（ToS; サービス タイプ）を指定する値に設定します。 **-w** *waittim* **—** プローブへの応答を待機する時間（秒）を設定します。
upgrade [*ftp-url*] [*device:partition-num*]	NAM がアプリケーション イメージで起動されている場合に、指定のロケーションからメンテナンス イメージをアップグレードします。このコマンドは、メンテナンス イメージの guest アカウントからも使用できます。 NAM がメンテナンス イメージで起動されている場合に、指定のロケーションから NAM アプリケーション イメージをアップグレードします。
upgrade bios	新しい BIOS イメージをインストールします。このコマンドは、メンテナンス イメージの guest アカウントで使用できます。 ⚠ **注意** このコマンドは、適切に使用しないと、NAM が動作不能になることもあります。
voice monitoring	アプリケーション イメージから、音声モニタをイネーブルにします。

NAM は、スーパバイザ エンジン用の CLI コマンドもサポートします。各コマンドの詳細については、『*Catalyst 6000 Family Command Reference*』を参照してください。

Cisco IOS コマンド

NAM は、次の CLI コマンドもサポートします。各コマンドの詳細については、『*Catalyst 6000 Family IOS Command Reference* 』を参照してください。これらのコマンドは、モード別に分類されています。ここでは、NAM との対話式の Cisco IOS コマンドについて説明します。

- EXEC コマンド（p.70）
- コンフィギュレーション コマンド（p.71）

EXEC コマンド

次のコマンドは、いずれも EXEC モードで実行します。

コマンド	説明
analysis module *slot_number* **management-port access-vlan** *vlan_number*	NAM の管理ポートおよびインターフェイスのキャプチャモードの特性を設定します。インターフェイスがキャプチャ モードの場合に許可される VALN を指定します。
analysis module *slot_number* **data-port** *port_number* **capture** [**allowed-vlan** *vlan-list*]	NAM のデータ ポートおよびインターフェイスのキャプチャ モードの特性を設定します。インターフェイスがキャプチャ モードの場合に許可される VALN を指定します。
set boot device *partition_number module_number* [**fast**]	**set boot device** *partition_number module_number* [**fast**] コマンドでブート デバイス パーティションを設定する際に、高速起動をイネーブルにできます。このオプションは、デフォルトではディセーブルになります。このオプションを指定すると、Cisco IOS の [**fast**] コマンド オプションと同様に、BIOS メモリ テストが省略され、NAM の起動が高速になります。
show analysis module *slot_number* **management-port** *state* | *traffic*	管理ポートの設定値が表示されます。
show analysis module *slot_number* **data-port** *port_number state* | *traffic*	データ ポートの設定値が表示されます。
show module	搭載されているモジュール、バージョン、およびステートが表示されます。 （注） このコマンドでは、シグニチャ レベルは表示されません。
reload	スイッチ全体をリロードします。
show running-config	現在実行中のコンフィギュレーションを表示します。
show startup-config	保存されているコンフィギュレーションを表示します。

hardware_module module *module_number* **reset** *word* [**fast**]	モジュールをデフォルトでアプリケーション イメージにリセットします。fast オプションを指定すると、BIOS メモリテストが省略され起動が高速になります。
	（注） このコマンドでブート デバイスを指定しないと、次のような **<empty>** メッセージが表示されます。
	`Router# hardware_module module 3 reset`
	`Device BOOT variable for reset = <empty>`
	`Warning:Device list is not verified.`

hw-module *module slot_number* **reset cf:1**	モジュールをメンテナンス イメージにリセットします。
hw-module *module slot_number* **shutdown**	モジュールをメンテナンス イメージにリセットしてからシャットダウンします。

コマンド	説明
show interfaces Gigabit *slot_number/port_number*	インターフェイスのステータスを表示します。
show interfaces switchport *module slot_number*	インターフェイスに関する現在のスイッチの設定値を表示します。
show interface trunk *module slot_number*	インターフェイスに関する現在のトランクの設定値を表示します。
clock set time date	現在の日時を設定します。
clock update-calendar	カレンダー時刻をクロック時刻に更新します。
clock read-calendar	クロック時刻をカレンダー時刻に更新します。

コンフィギュレーション コマンド

次のコマンドは、いずれもグローバル コンフィギュレーション モードまたはインターフェイス コンフィギュレーション モードで実行します。

- グローバル コンフィギュレーション モード（p.71）
- インターフェイス コンフィギュレーション モード（p.71）

グローバル コンフィギュレーション モード

次のコマンドは、いずれもグローバル コンフィギュレーション モードで実行します。

コマンド	説明
power enable module *slot_number*	NAM の電源がオンになっていない場合、電源をオンにします。
no power enable module *slot_number*	NAM をシャットダウンし、電源をオフにします。
clock timezone *zone offset*	スイッチまたは NAM のタイムゾーンを設定します。
clock summer-time *zone* **recurring**	スイッチがサマータイム設定値を使用するように設定します。
clock calendar valid	起動時に現在のカレンダー時刻をスイッチ時刻として設定します。
interface GigabitEthernet *slot number/port number*	各 NAM ポートの設定を開始します。
monitor session session {source {interface *interface interface-number* | {**vlan** *vlan-id*}} [, | - | **rx**| **tx** | **both**]	SPAN セッションの送信元を設定します。
monitor session {*session_number*} **{destination analysis module** *NAM module number* **data-port** *port*}	SPAN セッションの宛先を設定します。

インターフェイス コンフィギュレーション モード

次のコマンドは、いずれもインターフェイス コンフィギュレーション モードで実行するコンフィギュレーション コマンドです。

コマンド	説明
switchport	インターフェイスをスイッチポートとして設定します。
switchport trunk encapsulation dot1q	カプセル化タイプを dot1q に設定します。
switchport trunk native vlan *vlan*	トランク ポートのネイティブ VLAN を設定します。
switchport trunk allowed vlan *vlans*	トランクの許可 VLAN を設定します。
switchport mode trunk	インターフェイスをトランク ポートとして設定します。
switchport capture	インターフェイスをキャプチャ ポートとして設定します。
switchport access vlan *vlan*	インターフェイスのアクセス VLAN を設定します。
switchport mode access	インターフェイスをアクセス ポートとして設定します。

サポートされないスーパバイザ エンジン CLI コマンド

次の CLI コマンドは、NAM ではサポートされていません。

- **set port broadcast**
- **set port channel**
- **set port cops**
- **set port disable**
- **set port enable**
- **set port flowcontrol**
- **set port gmrp**
- **set port gvrp**
- **set port host**
- **set port inlinepower**
- **set port jumbo**
- **set port membership**
- **set port negotiation**
- **set port protocol**
- **set port qos**
- **set port rsvp**
- **set port security**
- **set port speed**
- **set port trap**
- **set protocolfilter**
- **set rgmp**
- **set rspan**
- **set snmp**
- **set spantree**
- **set trunk**
- **set udld**
- **set vlan**
- **set vtp**

NAM のトラブルシューティング

ここでは、NAM のトラブルシューティング方法について説明します。

（注） NAM Traffic Analyzer アプリケーションのオンライン ヘルプ トピック「Troubleshooting」で、トラブルシューティングに関する詳しいヘルプを参照できます。

現象 スーパバイザCLIから**reset**コマンドを入力すると、常にメンテナンス イメージが起動される。

考えられる原因 スーパバイザのブート デバイスが cf:1 に設定されている場合、**reset** *module* コマンドを入力すると必ずメンテナンス イメージが起動されます。

対処方法 リセット中にブート ストリングを入力することによって、スーパバイザに設定されているブート デバイスを変更します。

- Cisco IOS ソフトウェアで、アプリケーション イメージが起動されるようにするには、hardware_module **mod 9 reset hdd:1** コマンドを使用します。
- Catalyst OS ソフトウェアで、アプリケーション イメージが起動されるようにするには、**reset 9 hdd:1** コマンドを使用します。

現象 NAM にパッチをインストールするとき、[verification failed] メッセージが表示される。

考えられる原因 NAM に設定された時刻と日付が正しくない、パッチがシスコの正式なパッチでない、パッチが旧リリースの NAM 用のパッチである、FTP プロセスでエラーが生じている、指定された FTP イメージがパッチではない（フル アプリケーション イメージ）といった原因が考えられます。

対処方法 シグニチャ検証を利用して、パッチが正式なものであり、現在のリリースに対応していることを確認してください。また、NAM の時刻と日付が正確であり、シスコの正式なパッチだけがインストールされていることを確認してください。

現象 NAM アプリケーション イメージと同じパスワードでメンテナンス イメージにログインできない。

考えられる原因 NAM アプリケーション イメージとメンテナンス イメージでは、root アカウントおよび guest のアカウント用のパスワード データベースが異なります。メンテナンス イメージと NAM アプリケーション イメージの root および guest のデフォルト パスワードはそれぞれ異なります。NAM アプリケーション イメージでパスワードを変更しても、メンテナンス イメージのパスワードは変更されず、またその逆も同様です。

対処方法 メンテナンス イメージのパスワードを使用してください。

現象　メンテナンス イメージのパスワードを忘れてしまったので、回復したい。

考えられる原因　スイッチからメンテナンス イメージのパスワードをリセットすることはできません。メンテナンス イメージをアップグレードすると、メンテナンス イメージの root パスワードと guest パスワードがデフォルトの設定になります。

対処方法　メンテナンス イメージのデフォルト パスワードを使用してください。表 6（p.44）または表 8（p.55）を参照してください。

現象　WS-X6380-NAM に新しい NAM 2.2 イメージをロードしようとすると、次のメッセージが表示される。

```
Incompatible image! Upgrade aborted.
```

考えられる原因　WS-X6380-NAM は、このイメージをサポートしていません。

対処方法　WS-X6380-NAM では、NAM ソフトウェア リリース 2.2 イメージは使用しないでください。WS-X6380-NAM と新しい WS-SVC-NAM-1 および WS-SVC-NAM-2 では、アプリケーションとメンテナンスのファイル イメージ フォーマットが異なります。新しい NAM には共通のフォーマットが使用されており、アップグレード用に同じイメージ ファイル名を使用できます。

現象　Traffic Analyzer **Active SPAN** ウィンドウに SPAN セッションが表示されない。

考えられる原因　Catalyst OS ソフトウェアでは、宛先ポートが含まれているモジュールがスイッチシャーシから取り外されると、SPAN セッションは非アクティブになります。SPAN の設定はスーパバイザ エンジンによって SNMP エージェントから削除されるので、NAM は SPAN セッションで認識されません。

対処方法　モジュールを元どおり取り付けてください。

現象　Cisco IOS ソフトウェアで、部分的に設定された SPAN セッションとして SPAN の create 要求がエラーになる。

考えられる原因　NAM は部分的に設定された SPAN セッションを認識しません。また、送信元タイプまたは宛先ポートに衝突があると、SPAN の create 要求はエラーになる可能性があります。

対処方法　SPAN セッションの送信元または宛先のいずれか一方だけしか定義されていない可能性があるので、送信元と宛先の両方を定義して SPAN セッションを再設定してください。

現象　NAM の初回起動時に完全なメモリ テストを実行したいが、自動的にメモリ テストの一部が実行される。

考えられる原因　デフォルトの設定では、部分的なメモリ テストが実行されます。

対処方法　完全なメモリ テストを実行するには、**hw-module module** *module_number* **reset** *device:partition* **mem-test-full** コマンドを入力します。

（注） 完全なメモリ テストは完了するのに非常に時間がかかります。

このコマンドは、Cisco IOS 専用のコマンドなので、Catalyst OS ソフトウェアには使用できません（「NAM のリセット」[p.47] を参照してください）。

hw-module module *module_number* **mem-test-full** コマンドも使用できます。たとえば、次のように入力します。

```
Router(config)#  hw-module module 5 mem-test-full
```

Catalyst OS ソフトウェアで完全なメモリ テストをイネーブルにするには、**set boot device** *bootseq mod#* **mem-test-full** コマンドを入力します。このオプションは、デフォルトではディセーブルになります。たとえば、次のように入力します。

```
Console (enable) set boot device cf:1 4 mem-test-full
Device BOOT variable = cf:1
Memory-test set to FULL
Warning:Device list is not verified but still set in the boot string.

Console> (enable) show boot device 4
Device BOOT variable = cf:1
Memory-test set to FULL
```

次に、部分的なメモリ テストをリセットする方法を示します。

```
Console> (enable) set boot device cf:1 4
Device BOOT variable = cf:1
Memory-test set to PARTIAL
Warning:Device list is not verified but still set in the boot string.
Console> (enable)
Console> (enable) show boot device 4
Device BOOT variable = cf:1
Memory-test set to PARTIAL
```

現象 **Set up->Switch Parameters** メニュー ウィンドウの **Test** ボタンをクリックすると、スイッチへの SNMP の読み取りと書き込みが両方ともできないことを示すポップアップ ウィンドウが表示される。

考えられる原因 入力されている SNMP 読み取り / 書き込みコミュニティ ストリングがそのスイッチに設定されている SNMP 読み取り / 書き込みコミュニティ ストリングと同じかどうか確認してください。

（注） このパスワードは大文字 / 小文字を区別して入力する必要があります。

対処方法 コミュニティ ストリングが正しいにも関わらずテストがエラーになる場合は、次の手順に従って、スイッチの設定で IP 許可リストがイネーブルになっていることを確認してください。

ステップ 1 イネーブル モードでスイッチにログインします。

ステップ 2 **show IP permit** コマンドを入力します。

IP 許可リストがイネーブルになっている場合は、NAM 内部アドレスが IP 許可リストに追加されていることを確認します。NAM アドレスは、127.0.0.X です。この X は、NAM モジュール番号の 10 倍です。たとえば、NAM がモジュール 4 であれば、アドレスは 127.0.0.40 になります。

NAM の内部 IP アドレスを求めたら、ステップ 3 に進みます。

ステップ 3 **set IP permit NAM-address SNMP** コマンドを入力します。

現象 NAM にパッチをインストールする際に、[verification failed] メッセージが表示される。

考えられる原因 NAM に設定された日付および時刻が正しくないか、またはパッチがシスコの正式なパッチではありません。

対処方法 インストールしようとしているパッチがご使用のNAMバージョンに対応したシスコの正式なパッチであることを確認してください。また、NAM に設定されている日付と時刻が正しいことを確認してください。

現象 Catalyst OS ソフトウェアが稼働しているスイッチで NAM を使用する場合、**ping** コマンドまたは NAM Traffic Analyzer アプリケーションを使用すると、NAM で [unreachable] と表示されることがある。

考えられる原因 NAM の IP アドレスとスイッチ（インターフェイス sc0）の IP アドレスが、同じサブネットに属していません。スイッチの IP アドレスおよび NAM の VLAN 割り当てを変更した場合に、この問題が発生することがあります。NAM は自身の VLAN 割り当てを、スイッチ（インターフェイス sc0）が存在する VLAN と自動的に同期化させます。この場合、NAM の IP アドレスは、NAM に割り当てられた VLAN とは異なるサブネットに存在することになります。したがって、ルータは NAM の IP アドレスを宛先とするパケットを廃棄します。不適切な VLAN 割り当てとサブネット指定によるルート重複のため、ルータにスタティック ルートを追加できません。

対処方法 NAM の IP アドレスとスイッチの IP アドレスが、同じ VLAN 上の同じサブネットに属しているかどうかを確認します。

現象 NAM に接続できない。

考えられる原因 初期設定が正しくないか、未設定です。

対処方法 「NAM の設定」（p.22）の説明に従って、NAM を再設定してください。

現象 NAM Traffic Analyzer アプリケーションに接続できない。

考えられる原因 HTTP サーバの設定が正しくありません。

対処方法 「HTTP サーバまたは HTTP セキュア サーバの設定」（p.39）の説明に従って、HTTP サーバに関する NAM の設定を確認してください。

現象　NAM のアップグレードがエラーになる。

考えられる原因　サーバへの URL またはイメージ名が正しくありません。

対処方法　指定した URL が有効であるかどうかを確認してください。また、その URL で指定したイメージ名がシスコの正式なイメージ名であるかどうかを確認してください。

現象　HTTP サーバをイネーブルにできない。

考えられる原因　Web ユーザがまったく設定されていないか、またはセキュア サーバがすでにイネーブルになっています。

対処方法　「HTTP サーバまたは HTTP セキュア サーバの設定」（p.39）の説明に従って、Web ユーザを設定してください。

現象　設定したにもかかわらず、TACACS+ 認証および許可に失敗する。

考えられる原因　考えられる原因は 3 つあります。TACACS+ サーバ上のログイン設定で名前とパスワードが一致していないか、NAM に設定されている TACACS+ シークレット キーがサーバに設定されているシークレット キーと一致していないか、NAM に設定されている TACACS+ サーバの IP アドレスが正しくないと考えられます。

対処方法　次の手順に従って原因を特定し、適切な措置を行います。

ステップ 1　ローカル ユーザとしてログインします。

ステップ 2　**Admin > Diagnostics > Tech Support** を選択します。

ステップ 3　下へスクロールして、/var/log/messages エリアを表示します。

ステップ 4　ログの最後の方に次のメッセージがないかどうかを調べ、推奨措置を行います。

```
...PAM-tacplus[612]:auth failed:Login incorrect
```

考えられる原因　TACACS+ サーバ上のログイン設定で名前とパスワードが一致していません。

対処方法　TACACS+ サーバにログインし、NAM ユーザの認証および許可を設定します（ログイン設定についての詳細は、TACACS+ のマニュアルを参照してください）。

```
...httpd:tac_authen_pap_read:invalid reply content, incorrect key?
...PAM-tacplus[616]:auth failed:Authentication error, please contact
administrator.
```

考えられる原因　NAM に設定されている TACACS+ シークレット キーが、TACACS+ サーバに設定されているキーと一致していません。

対処方法　**Admin > User > TACACS+** を選択し、正しいシークレット キーを入力します。

```
...httpd:tac_connect:connection to 172.18.122.183 failed:Connection timed out
...httpd:tac_connect:all possible TACACS+ servers failed
...PAM-tacplus[613]:connection failed srv 0:Connection timed out
...PAM-tacplus[613]:no more servers to connect
```

考えられる原因　NAM に設定されている TACACS+ サーバの IP アドレスが正しくありません。

対処方法　**Admin > User > TACACS+**を選択し、正しいTACACS+サーバ アドレスを入力します。

現象　TACACS+ ユーザは正常にログインできるが、NAM Traffic Analyzer アプリケーションにアクセスすると [Not authorized...] というエラー メッセージが表示される。

考えられる原因　必要なアクセス権限が割り当てられていません。

対処方法　TACACS+ サーバにログインし、該当するユーザにアクセス権限を与えます（ログイン設定についての詳細は、TACACS+ のマニュアルを参照してください）。

Web ユーザ名およびパスワードについての注意事項

Web ユーザ名およびパスワードについては、次の点に注意してください。

- CLI のユーザ名（root または guest）とパスワードを使用して NAM Traffic Analyzer アプリケーションにログインすることはできません。これらは別々に管理されているからです。また、NAM Traffic Analyzer アプリケーションのユーザ名とパスワードを使用して NAM CLI にログインすることもできません。

  Web ユーザは、ローカル データベースと TACACS+ のどちらでも作成できます。Web ユーザは、CLI で使用するものと同じユーザ名とパスワードで作成できます。ただし、その場合にもパスワードは両方の場所で変更する必要があります。
- ローカル データベースに加えて TACACS+ を使用することも、ローカル データベースの代わりに TACACS+ を使用することもできます（ローカル データベースが常に最初にチェックされます）。TACACS+ だけを使用するには、次のいずれかの方法でローカル データベース ユーザを削除します。
  - NAM CLIの**rmwebusers**コマンドを使用して、ローカル ユーザだけを削除します。TACACS+ ユーザは TACACS+ サーバで個別に管理されるので削除しません。
  - **Admin** タブで **Users** をクリックし、すべてのローカル データベース ユーザを個別に削除します。

注意　NAM Traffic Analyzer アプリケーションに TACACS+ ユーザとしてログインできることを確認してから、ローカル データベース Web ユーザをすべて削除してください。

- ローカル Web admin ユーザ パスワードを忘れた場合や、アカウント権限を持つ別のユーザがログインしてローカル Web admin ユーザ パスワードを変更した場合は、パスワードを回復できます。

NAM に TACACS+ サーバが設定されていない場合は、次の手順でパスワードを回復します。

ステップ 1 NAM CLI にアクセスします。

ステップ 2 次のコマンドを入力して、Web ユーザをすべて削除します。

```
rmwebusers
WARNING: Doing this will stop the web server and remove
all locally defined web users from web user database.

Are you sure you want to continue (y/n) [n]? y

Disabling HTTP server...
Successfully disabled HTTP server.

All locally defined web users have been
removed from web user database.
root@namlab-kom2.cisco.com#
```

ステップ 3 次のコマンドを入力して、HTTP（該当する場合は HTTPS）サーバを起動します。

```
ip http server enable
ip http secure server enable
```

ステップ 4 プロンプトで、Web admin ユーザ名およびパスワードを入力します。

新しい admin アカウントを使用してログインし、**Admin** タブ、**Users** の順にクリックして、他の Web アカウントを作成できます。

NAM に TACACS+ サーバが設定されている場合は、次の手順でパスワードを回復します。

ステップ 1 NAM Traffic Analyzer アプリケーションに TACACS+ ユーザとしてログインします。

この手順を行うには、TACACS+ サーバ上でアカウント管理権限を持つユーザでなければなりません。

ステップ 2 ローカル Web admin ユーザのパスワードを変更します。

（注） TACACS+ サーバが設定されている場合、ローカル Web ユーザ アカウントが削除されていても、TACACS+ サーバ上で Web admin ユーザを作成できます。この場合、TACACS+ サーバ上で作成された admin ユーザが NAM Traffic Analyzer アプリケーションにログインし、ローカル Web admin ユーザのパスワードを変更できます。他の admin ユーザを作成する必要はありません。

TACACS+ の設定が NAM サーバと TACACS+ サーバとで食い違っていると考えられる場合、NAM 上の TACACS+ の設定を修正するためのローカル データベース ユーザ アカウントがないと、TACACS+ サーバからこの問題を修正することは不可能です。パスワードを回復する手順は、次のとおりです。

ステップ 1 NAM CLI にアクセスします。

ステップ 2 次のコマンドを入力します。

```
rmwebusers
ip http tacacs+ disable
ip http server enable
```

（HTTPS を使用する場合は **ip http secure server enable**）

ステップ 3 プロンプトが表示されたら、新しいローカル データベース admin ユーザ名およびパスワードを入力します。

ステップ 4 NAM Traffic Analyzer アプリケーションにログインします。

ステップ 5 **Admin** タブをクリックします。

ステップ 6 **Users** をクリックします。

ステップ 7 表示される内容から、**TACACS+** をクリックします。

ステップ 8 正しい情報を入力します。

ステップ 9 **Apply** をクリックします。

アップグレードまたはパッチの適用を行う場合、パスワードの使用についての制約があります。upgrade コマンドおよび patch コマンドの引数としてパスワードを含めないでください。次のコマンド構文を使用してください。

```
patch ftp://user@host/full-patch/filename
```

プロンプトが表示されたら、パスワードを入力します。

サポート対象の MIB オブジェクト

表 9 に、スーパバイザ エンジンおよび NAM がサポートする RMON および RMON2 の MIB オブジェクトを示します。スーパバイザ エンジンには、表 9 のように RMON MIB の一部のオブジェクトが実装されています。スーパバイザ エンジンの RMON の実装は、NAM の実装から完全に独立しており、MIB オブジェクトが共有されることはありません。

スイッチ上の物理インターフェイスから etherStats を収集するには、NAM ではなくスーパバイザ エンジン上に etherStatTable を設定します。etherStats は、複数の物理インターフェイスで同時に正確に収集されます。

特定の VLAN について etherStats を収集するには、NAM 上に etherStatsTable を設定します。データソースには、目的とする VLAN に対応する ifIndex を使用します。

スーパバイザ エンジン上で設定された alarmVariable は、スーパバイザ エンジン上の MIB オブジェクトを参照しなければなりません。NAM 上で設定された alarmVariable は、NAM 上の MIB オブジェクトを参照しなければなりません。

（注） スーパバイザ エンジン上の MIB オブジェクトを参照する NAM に alarmVariable を設定することはできません。また、NAM 上の MIB オブジェクトを参照するスーパバイザ エンジンに alarmVariable を設定することもできません。

表 9　スーパバイザ エンジン モジュールおよび NAM の RMON サポート

モジュール	Object Identifier（OID; オブジェクト識別子）および説明	ソース
スーパバイザ エンジン	...mib-2(1).rmon(16).statistics(1).etherStatsTable(1)...mib-2(1).rmon(16).statistics(1).tokenRingMLStatsTable(2) ...mib-2(1).rmon(16).statistics(1).tokenRingPStatsTable(3)	RFC 1757（RMON-MIB） RFC 1513（TOKEN-RING-RMON MIB） RFC 1513（TOKEN-RING-RMON MIB）
	パケット、オクテット、ブロードキャスト、エラーなどのカウンタ	
スーパバイザ エンジン	...mib-2(1).rmon(16).history(2).historyControlTable(1) ...mib-2(1).rmon(16).history(2).etherHistoryTable(2) ...mib-2(1).rmon(16).history(2).tokenRingMLHistoryTable(3) ...mib-2(1).rmon(16).history(2).tokenRingPHistoryTable(4)	RFC 1757（RMON-MIB） RFC 1757（RMON-MIB） RFC 1513（TOKEN-RING-RMON MIB） RFC 1513（TOKEN-RING-RMON MIB）
	あとで検索できるように、統計グループ カウンタを定期的にサンプリングして保存	
スーパバイザ エンジン	...mib-2(1).rmon(16).alarm(3)	RFC 1757（RMON-MIB）
	ネットワーク管理目的で、重要な RMON 変数に設定できるスレッシュホールド	
ネットワーク解析	...mib-2(1).rmon(16).alarm(3)	RFC 1757（RMON-MIB）
	ネットワーク管理目的で、重要な RMON 変数に設定できるスレッシュホールド	
ネットワーク解析	...mib-2(1).rmon(16).hosts(4)	RFC 1757（RMON-MIB）
	セグメントまたはポート上の各ホスト デバイスに関する統計を維持	
ネットワーク解析	...mib-2(1).rmon(16).hostTopN(5)	RFC 1757（RMON-MIB）
	Hosts グループに関するユーザ定義のサブセット レポート（統計カウンタに基づいてソート）	

表 9　スーパバイザ エンジン モジュールおよび NAM の RMON サポート（続き）

モジュール	Object Identifier（OID; オブジェクト識別子）および説明	ソース
ネットワーク解析	...mib-2(1).rmon(16).statistics(1).etherStatsTable(1)	RFC 1757（RMON-MIB）
ネットワーク解析	...mib-2(1).rmon(16).matrix(6)	RFC 1757（RMON-MIB）
	ネットワーク上のホスト間の対話に関する統計を維持	
ネットワーク解析	...mib-2(1).rmon(16).filter(7)	RFC 1757（RMON-MIB）
	特定のパターンと一致するフレームからパケット ストリームを生成するフィルタ エンジン	
ネットワーク解析	...mib-2(1).rmon(16).capture(8)	RFC 1757（RMON-MIB）
	管理コンソールにアップロードするために Filter グループがキャプチャしたパケット用のバッファを管理	
スーパバイザ エンジン	...mib-2(1).rmon(16).event(9)	RFC 1757（RMON-MIB）
	Alarm グループのスレッシュホールドを超えたときに SNMP トラップを生成してイベントを記録	
ネットワーク解析	...mib-2(1).rmon(16).event(9)	RFC 1757（RMON-MIB）
	Alarm グループのスレッシュホールドを超えたときに SNMP トラップを生成してイベントを記録	
スーパバイザ エンジン	...mib-2(1).rmon(16).tokenRing(10).ringStationControlTable(1) ...mib-2(1).rmon(16).tokenRing(10).ringStationTable(2) ...mib-2(1).rmon(16).tokenRing(10).ringStationOrderTable(3) ...mib-2(1).rmon(16).tokenRing(10).ringStationConfigControlTable(4) ...mib-2(1).rmon(16).tokenRing(10).ringStationConfigTable(5) ...mib-2(1).rmon(16).tokenRing(10).sourceRoutingStatsTable(6)	RFC 1513（TOKEN-RING-RMON MIB） RFC 1513（TOKEN-RING-RMON MIB） RFC 1513（TOKEN-RING-RMON MIB） RFC 1513（TOKEN-RING-RMON MIB） RFC 1513（TOKEN-RING-RMON MIB） RFC 1513（TOKEN-RING-RMON MIB）
	詳細なトークンリング統計情報の集計	
ネットワーク解析	...mib-2(1).rmon(16).protocolDir(11)	RFC 2021（RMON2-MIB）
	NAM がモニタして統計を維持するプロトコルのテーブル	
ネットワーク解析	...mib-2(1).rmon(16).protocolDist(12)	RFC 2021（RMON2-MIB）
	protocolDir(11) の各プロトコルに関する統計情報のテーブル	
ネットワーク解析	...mib-2(1).rmon(16).addressMap(13)	RFC 2021（RMON2-MIB）
	MAC/ ネットワーク レイヤ アドレス バインディングのリスト	
ネットワーク解析	...mib-2(1).rmon(16).nlHost(14)	RFC 2021（RMON2-MIB）
	各ネットワーク レイヤ アドレスに関する統計	
ネットワーク解析	...mib-2(1).rmon(16).nlMatrix(15)	RFC 2021（RMON2-MIB）
	ネットワーク レイヤ アドレスのペアに関するトラフィック統計	
ネットワーク解析	...mib-2(1).rmon(16).alHost(16)	RFC 2021（RMON2-MIB）
	各ネットワーク アドレスに関するアプリケーション レイヤ プロトコル別の統計	
ネットワーク解析	...mib-2(1).rmon(16).alMatrix(17)	RFC 2021（RMON2-MIB）
	ネットワーク レイヤ アドレスのペアに関するアプリケーション レイヤ プロトコル別のトラフィック統計	
ネットワーク解析	...mib-2(1).rmon(16).usrHistory(18)	RFC 2021（RMON2-MIB）
	RMON、RMON2、MIB-I、または MIB-II 統計が含まれるように、RMON1 リンク レイヤ統計を超えてヒストリを拡張	

表 9　スーパバイザ エンジン モジュールおよび NAM の RMON サポート（続き）

モジュール	Object Identifier（OID; オブジェクト識別子）および説明	ソース
スーパバイザ エンジン	...mib-2(1).rmon(16).probeConfig(19)	RFC 2021（RMON2-MIB）
	エージェントの機能および設定を示したリストを表示	
ネットワーク解析	...mib-2(1).rmon(16).switchRMON(22).smonMIBObjects(1). dataSourceCaps(1).dataSourceCapsTable(1)	RFC 2613（SMON-MIB）
	物理エントリおよび VLAN を ifEntry にマッピング	
ネットワーク解析	...mib-2(1).rmon(16).switchRMON(22).smonMIBObjects(1). smonStats(2).smonVlanStatsControlTable(1)	RFC 2613（SMON-MIB）
	VLAN ID 番号別のトラフィック統計	
ネットワーク解析	...mib-2(1).rmon(16).switchRMON(22).smonMIBObjects(1). smonStats(2).smonPrioStatsControlTable(3)	RFC 2613（SMON-MIB）
	802.1p ユーザ プライオリティ値別のトラフィック統計	
ネットワーク解析	...frontier(141).mibdoc2(2).netscout2(1).art(5).artControlTable(2)	draft-warth-rmon2-artmib-01.txt（ART-MIB）
	アプリケーション応答時間の統計	
ネットワーク解析	...mib-2(1).rmon(16).mediaIndependentStats(21)	（HC-RMON-MIB）
	パケット、オクテット、ブロードキャスト、エラーなどのカウンタ	
	rmon.dsmonMib(26).dsmonObjects(1).dsmonAggObjects(1). dsmonMaxAggGroups(1) rmon.dsmonMib(26).dsmonObjects(1).dsmonAggObjects(1). dsmonAggControlLocked(2) rmon.dsmonMib(26).dsmonObjects(1).dsmonAggObjects(1). dsmonAggControlChanges(3) rmon.dsmonMib(26).dsmonObjects(1).dsmonAggObjects(1) .dsmonAggControlLastChangeTime(4) rmon.dsmonMib(26).dsmonObjects(1).dsmonAggObjects(1) dsmonAggControlTable(5) rmon.dsmonMib(26).dsmonObjects(1).dsmonAggObjects(1). dsmonAggProfileTable(6) rmon.dsmonMib(26).dsmonObjects(1).dsmonAggObjects(1). .dsmonAggGroupTable(7)	（DSMON-MIB）
	集計またはプロファイル制御変数およびテーブル	
	rmon.dsmonMib(26).dsmonObjects(1).dsmonStatsObjects(2). dsmonStatsControlTable(1) rmon.dsmonMib(26).dsmonObjects(1).dsmonStatsObjects(2). dsmonStatsTable(2)	（DSMON-MIB）
	データ ソース別の統計収集テーブル	

表 9　スーパバイザ エンジン モジュールおよび NAM の RMON サポート（続き）

モジュール	Object Identifier（OID; オブジェクト識別子）および説明	ソース
	rmon.dsmonMib(26).dsmonObjects(1).dsmonPdistObjects(3). dsmonPdistCtlTable(1) rmon.dsmonMib(26).dsmonObjects(1).dsmonPdistObjects(3). dsmonPdistStatsTable(2) rmon.dsmonMib(26).dsmonObjects(1).dsmonPdistObjects(3). dsmonPdistTopNCtlTable(3) rmon.dsmonMib(26).dsmonObjects(1).dsmonPdistObjects(3). dsmonPdistTopNTable(4)	（DSMON-MIB）
	プロトコル別の統計収集テーブル	
	rmon.dsmonMib(26).dsmonObjects(1).dsmonHostObjects(4). dsmonHostCtlTable(1) rmon.dsmonMib(26).dsmonObjects(1).dsmonHostObjects(4). dsmonHostTable(2) rmon.dsmonMib(26).dsmonObjects(1).dsmonHostObjects(4). dsmonHostTopNCtlTable(3) rmon.dsmonMib(26).dsmonObjects(1).dsmonHostObjects(4). dsmonHostTopNTable(4)	（DSMON-MIB）
	ホスト別の統計収集テーブル	
	rmon.dsmonMib(26).dsmonObjects(1).dsmonCapsObjects(5). dsmonCapabilities(1)	（DSMON-MIB）
	DSMON 機能変数	
	rmon.dsmonMib(26).dsmonObjects(1).dsmonMatrixObjects(6). dsmonMatrixCtlTable(1) rmon.dsmonMib(26).dsmonObjects(1).dsmonMatrixObjects(6). dsmonMatrixSDTable(2) rmon.dsmonMib(26).dsmonObjects(1).dsmonMatrixObjects(6). dsmonMatrixDSTable(3) rmon.dsmonMib(26).dsmonObjects(1).dsmonMatrixObjects(6). dsmonMatrixTopNCtlTable(4) rmon.dsmonMib(26).dsmonObjects(1).dsmonMatrixObjects(6). dsmonMatrixTopNTable(5)	（DSMON-MIB）
	マトリクス統計収集テーブル	

適合規格

適合規格については、『*Catalyst 6000 Family Installation Guide*』の Appendix A「Specifications」および『*Catalyst 6000 Regulatory Compliance and Safety Information*』を参照してください。

FCC クラス B との適合性

この装置はFCC ルール Part 15 に規定された仕様のクラス B デジタル装置の制限に適合しています。

FCC クラス B 適合装置に関する記述 : このマニュアルに記載された装置は、無線周波エネルギーを生成および放射する可能性があります。シスコシステムズの指示する設置手順に従わずに装置を設置した場合、ラジオおよびテレビの受信障害が起こることがあります。この装置はテスト済みであり、FCC ルール Part 15 に規定された仕様のクラス B デジタル装置の制限に適合していることが確認済みです。これらの仕様は、住宅地で使用したときに、このような干渉を防止する適切な保護を規定したものです。ただし、特定の設置条件において干渉が起きないことを保証するものではありません。

シスコシステムズの書面による許可なしに装置を改造すると、装置がクラス A またはクラス B のデジタル装置に対する FCC 要件に適合しなくなることがあります。その場合、装置を使用するユーザの権利が FCC 規制により制限されることがあり、ラジオまたはテレビの通信に対するいかなる干渉もユーザ側の負担で矯正するように求められることがあります。

（注） シスコシステムズの許可なしに装置を改造すると、装置を操作する権限を失うことになります。

FCC クラスとの適合性についての詳細は、『*Catalyst 6000 Family Installation Guide*』および『*Catalyst 6000 Regulatory Compliance and Safety Information*』を参照してください。

関連資料

- FCC クラスとの適合性についての詳細は、『*Catalyst 6000 Regulatory Compliance and Safety Information*』を参照してください。
- NAM についての詳細は、『*Catalyst 6000 Family Network Analysis Module Installation and Configuration Note*』を参照してください。
- NAM Traffic Analyzer アプリケーションについての詳細は、オンライン ヘルプおよび『*User Guide for the Catalyst 6000 Network Analysis Module NAM Traffic Analyzer*』（オンライン ヘルプで PDF 版が提供されています）を参照してください。
- NAM に Real Time Monitor（RTM）を設定する方法についての詳細は、『*Configuring the Catalyst 6000 Network Analysis Module with nGenius Real-Time Monitor*』を参照してください。
- Catalyst 6000 ファミリー スイッチおよびコマンドライン インターフェイス（CLI）コマンドについての詳細は、次のマニュアルを参照してください。
  - 『*Release Notes for Catalyst 6000 Family Software Release 6.x*』
  - 『*Catalyst 6000 Family Software Configuration Guide*』
  - 『*Catalyst 6000 Family Command Reference*』
  - 『*Site Preparation and Safety Guide*』
- ハードウェア構成およびメンテナンス手順についての詳細は、『*Catalyst 6000 Family Module Installation Guide* 』を参照してください。

マニュアルの入手方法

ここでは、シスコ製品のマニュアルを入手する方法について説明します。

WWW

WWW 上の次の URL から、シスコ製品の最新資料を入手することができます。

http://www.cisco.com

http://www.cisco.com/jp

各国語版のマニュアルは、次の URL から入手できます。

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

シスコ製品のマニュアルおよびその他の資料は、製品に付属の Cisco Documentation CD-ROM パッケージでご利用いただけます。Documentation CD-ROM は毎月更新されるので、印刷資料よりも新しい情報が得られます。この CD-ROM パッケージは、単独 または年間契約で入手することができます。

マニュアルの発注方法

シスコ製品のマニュアルは、次の方法でご発注いただけます。

- Cisco.com（Cisco Direct Customers）に登録されている場合、Networking Products MarketPlace からシスコ製品のマニュアルを発注できます。次の URL にアクセスしてください。

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Cisco.com 登録ユーザの場合、Subscription Store からオンラインで Documentation CD-ROM を発注できます。次の URL にアクセスしてください。

  http://www.cisco.com/go/subscription

- Cisco.com に登録されていない場合、製品を購入された代理店へお問い合わせください。

テクニカル サポート

シスコシステムズでは、技術上のあらゆる問題の支援窓口として Cisco.com を運営しています。お客様およびパートナーは、Technical Assistance Center（TAC）Web サイトのオンライン ツールからマニュアル、トラブルシューティングに関するヒント、およびコンフィギュレーション例を入手できます。Cisco.com にご登録済みのお客様は、TAC Web サイトで提供するすべてのテクニカル サポート リソースをご利用いただけます。Cisco.com へのご登録については、製品を購入された代理店へお問い合わせください。

Cisco.com

Cisco.com は、いつでもどこからでも、シスコシステムズの情報、ネットワーキング ソリューション、サービス、プログラム、およびリソースにアクセスできる対話形式のネットワーク サービスです。

Cisco.com は統合インターネット アプリケーションであり、優れた使いやすいツールとして、広範囲の機能やサービスを通してお客様に次のような利点を提供します。

- 業務の円滑化と生産性の向上
- オンライン サポートによる技術上の問題の解決
- ソフトウェア パッケージのダウンロードおよびテスト
- シスコのトレーニング資料および製品の発注
- スキル査定、トレーニング、認定プログラムへのオンライン登録

また、Cisco.com に登録することにより、各ユーザに合った情報やサービスをご利用いただくことができます。Cisco.com には、次の URL からアクセスしてください。

http://www.cisco.com
http://www.cisco.com/jp

TAC

シスコの製品、テクノロジー、またはソリューションについて技術的な支援が必要な場合には、TAC をご利用いただくことができます。TAC では 2 種類のサポートを提供しています。TAC Web サイトと TAC Escalation Center です。

TAC への問い合わせは、問題の緊急性に応じて分類されます。

- プライオリティ レベル 4（P4）— シスコ製品の機能、インストレーション、基本的なコンフィギュレーションについて、情報または支援が必要な場合。
- プライオリティ レベル 3（P3）— ネットワークのパフォーマンスが低下している。ネットワークが十分に機能していないが、ほとんどの業務運用は継続できる場合。
- プライオリティ レベル 2（P2）— ネットワークのパフォーマンスが著しく低下したため業務に重大な影響があるにもかかわらず、対応策が見つからない場合。
- プライオリティ レベル 1（P1）— ネットワークがダウンし、すぐにサービスを回復しなければ業務に致命的な損害が発生するが、対応策が見つからない場合。

問題のプライオリティおよびサービス契約の内容に応じて、適切な TAC サービスを選択してください。

TAC Web サイト

P3 および P4 レベルの問題については、TAC Web サイトを利用して、お客様ご自身で問題を解決し、コストと時間を節約することができます。このサイトでは各種のオンライン ツール、ナレッジベース、およびソフトウェアを、いつでも必要なときに利用できます。TAC Web サイトには、次の URL からアクセスしてください。

http://www.cisco.com/tac

シスコシステムズとサービス契約を結んでいるお客様、パートナー、リセラーは、TAC Web サイトのすべてのテクニカル サポート リソースをご利用いただけます。TAC Web サイト にアクセスするには、Cisco.com のログイン ID とパスワードが必要です。サービス契約が有効で、ログイン ID またはパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

http://www.cisco.com/register/

Cisco.com 登録ユーザは、TAC Web サイトで技術上の問題を解決できなかった場合、TAC Case Open ツールのオンライン サービスを利用することができます。TAC Case Open ツールの URL は次のとおりです。

http://www.cisco.com/tac/caseopen

インターネットでアクセスする場合には、TAC Web サイトで P3 および P4 レベルの情報を参照することをお勧めします。

Japan TAC Web サイト

Japan TAC Web サイトでは、利用頻度の高い TAC Web サイト（http://www.cisco.com/tac）のドキュメントを日本語で提供しています。Japan TAC Web サイトには、次の URL からアクセスしてください。

http://www.cisco.com/jp/go/tac

サポート契約を結んでいない方は、「ゲスト」としてご登録いただくだけで、Japan TAC Web サイトのドキュメントにアクセスできます。

Japan TAC Web サイトにアクセスするには、Cisco.com のログイン ID とパスワードが必要です。ログイン ID とパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

http://www.cisco.com/jp/register/

TAC Escalation Center

TAC Escalation Center では P1 および P2 レベルの問題に対応しています。このレベルに分類されるのは、ネットワークの機能が著しく低下し、業務の運用に重大な影響がある場合です。TAC Escalation Center にお問い合わせいただいた P1 または P2 の問題には、TAC エンジニアが対応します。

TAC フリーダイヤルの国別電話番号は、次の URL を参照してください。

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

ご連絡に先立って、お客様が契約しているシスコ サポート サービスがどのレベルの契約となっているか（たとえば、SMARTnet、SMARTnet Onsite、または Network Supported Accounts [NSA; ネットワーク サポート アカウント] など）、お客様のネットワーク管理部門にご確認ください。また、お客様のサービス契約番号およびご使用の製品のシリアル番号をお手元にご用意ください。

このマニュアルは、「関連資料」に記載されたマニュアルと併せてご利用ください。

お問い合わせは、購入された各代理店へご連絡ください。