Catalyst 6500 シリーズ スイッチ / Cisco 7600 シリーズ ルータ 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

Release 3.6(1)
March 2007

Text Part Number: OL-12753-01-J

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

FCC クラス A 準拠装置に関する記述：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 A デジタル装置の制限に準拠していることが確認済みです。これらの制限は、商業環境で装置を使用したときに、干渉を防止する適切な保護を規定しています。この装置は、無線周波エネルギーを生成、使用、または放射する可能性があり、この装置のマニュアルに記載された指示に従って設置および使用しなかった場合、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。住宅地でこの装置を使用すると、干渉を引き起こす可能性があります。その場合には、ユーザ側の負担で干渉防止措置を講じる必要があります。

FCC クラス B 準拠装置に関する記述：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準拠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 要件に準拠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。

装置の電源を切ることによって、この装置が干渉の原因であるかどうかを判断できます。干渉がなくなれば、シスコシステムズの装置またはその周辺機器が干渉の原因になっていると考えられます。装置がラジオまたはテレビ受信に干渉する場合には、次の方法で干渉が起きないようにしてください。

・干渉がなくなるまで、テレビまたはラジオのアンテナの向きを変えます。

・テレビまたはラジオの左右どちらかの側に装置を移動させます。

・テレビまたはラジオから離れたところに装置を移動させます。

・テレビまたはラジオとは別の回路にあるコンセントに装置を接続します（装置とテレビまたはラジオがそれぞれ別個のブレーカーまたはヒューズで制御されるようにします）。

米国シスコシステムズ社では、この製品の変更または改造を認めていません。変更または改造した場合には、FCC 認定が無効になり、さらに製品を操作する権限を失うことになります。

シスコシステムズが採用している TCP ヘッダー圧縮機能は、UNIX オペレーティング システムの UCB（University of California, Berkeley）パブリック ドメイン バージョンの一部として、UCB が開発したプログラムを最適化したものです。All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコシステムズおよびこれら各社は、商品性や特定の目的への準拠性、権利を侵害しないことに関する、または取り扱い、使用、または取引によって発生する、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコシステムズおよびその代理店は、このマニュアルの使用またはこのマニュアルを使用できないことによって起こる制約、利益の損失、データの損傷など間接的で偶発的に起こる特殊な損害のあらゆる可能性がシスコシステムズまたは代理店に知らされていても、それらに対する責任を一切負いかねます。

Catalyst 6500 シリーズ スイッチ/Cisco 7600 シリーズ ルータ 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

CONTENTS

はじめに

製品番号：

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

このマニュアルでは、Catalyst 6500 シリーズ スイッチ、Catalyst 6000 シリーズ スイッチ、または Network Analysis Module（NAM; ネットワーク解析モジュール）ソフトウェア リリース 3.6(1) を実行する Cisco 7600 シリーズ ルータ NAM のインストレーション手順と、お使いの NAM がサポートするオペレーティング システム（Cisco IOS または Catalyst オペレーティング システム）の CLI（コマンドライン インターフェイス）を使用して NAM を設定する手順について説明します。

NAM Traffic Analyzer アプリケーションを使用して NAM を設定することもできます。使用方法は、Traffic Analyzer のオンライン ヘルプとユーザ ガイドに記載されています。

ソフトウェア設定についての詳細は、「関連資料」（p.x）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については、「安全性に関する概要」（p.x）と、Catalyst 6500 シリーズ スイッチ、Catalyst 6000 シリーズ スイッチ、または Cisco 7600 シリーズ ルータの『*Regulatory Compliance and Safety Information*』を参照してください。

（注） NAM ソフトウェア リリース 3.3 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。ライセンスおよびサードパーティ製ソフトウェア使用上の注意事項については、『*Copyright Notices for the Network Analysis Module*』Release 3.3 を参照してください。

対象読者

このマニュアルに記載された装置の設置、交換、またはサービスは、訓練を受けた認定サービス技術者（IEC 60950 および AS/NZS3260 で定義）だけが行ってください。

マニュアルの構成

このマニュアルの構成は次のとおりです。

章	タイトル	説明
第 1 章	概要	Catalyst 6500 シリーズ スイッチ、Catalyst 6000 シリーズ スイッチ、または Cisco 7600 シリーズ ルータ NAM の概要を説明します。
第 2 章	NAM の要件	NAM のハードウェアおよびソフトウェア要件を説明します。
第 3 章	NAM の設定	NAM のコンフィギュレーション手順を説明します。
第 4 章	NAM の管理	各スイッチ オペレーティング システムの CLI を使った NAM の管理手順を説明します。
第 5 章	NAM のトラブルシューティング	NAM のトラブルシューティング方法について説明します。

表記法

このマニュアルでは、次の表記法を使用しています。

表記	説明
太字	コマンド、コマンド オプションおよびキーワードは**太字**で示しています。
イタリック体	ユーザが値を指定する引数は、*イタリック体*で示しています。
[ ]	角カッコの中の要素は、省略可能です。
{ x | y | z }	必ずどれか 1 つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x | y | z]	どれか 1 つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
ストリング	引用符を付けない一組の文字。ストリングの前後には引用符を使用しません。引用符を使用すると、その引用符も含めてストリングとみなされます。
`screen` フォント	システムが表示する端末セッションおよび情報は、`screen` フォントで示しています。
太字の **`screen`** フォント	ユーザが入力しなければならない情報は、**太字**の **`screen`** フォントで示しています。
イタリック体 の *`screen`* フォント	ユーザが値を指定する引数は、*イタリック体* の *`screen`* フォントで示しています。
^	^ 記号は、Ctrl キーを表します。たとえば、画面に表示される ^D というキーの組み合わせは、Ctrl キーを押しながら D キーを押すことを意味します。
< >	パスワードのように出力されない文字は、かぎカッコ（< >）で囲んで示しています。

（注）は、次のように表しています。

（注） 「*注釈*」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

ヒントは、次のように表しています。

ヒント 「*問題解決に役立つ情報*」です。ヒントには、トラブルシューティングや操作方法ではなく、ワンポイントアドバイスと同様に知っておくと役立つ情報が記述される場合もあります。

注意は、次のように表しています。

注意 「*要注意*」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

安全性に関する概要

誤って行うと危険が生じる可能性のある操作については、安全上の警告が記載されています。各警告文に、警告を表す記号が記されています。

警告 **安全上の重要事項**

「*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。

これらの注意事項を保存しておいてください。

関連資料

- FCC クラスとの適合性の詳細については、『*Catalyst 6500 Series Switch Regulatory Compliance and Safety Information*』を参照してください。
- WS-SVC-NAM-1 および WS-SVC-NAM-2 の詳細については、次のマニュアルを参照してください。
  - 『*Catalyst 6500 Series Switch Network Analysis Module Documentation*』
  - 『*Release Notes for Catalyst 6500 Series Switch and Cisco 7600 Series Router Network Analysis Module Software*』Release 3.3
  - 『*Quick Start Guide for the Catalyst 6500 Series and Cisco 7600 Series Network Analysis Module*』
  - 『*Catalyst 6500 Series Switch and Cisco 7600 series Router Network Analysis Module Command Reference*』
  - 『*User Guide for the Network Analysis Module Traffic Analyzer*』Release 3.3
- NAM Traffic Analyzer アプリケーションの詳細については、オンライン ヘルプおよび『*User Guide for the Network Analysis Module NAM Traffic Analyzer*』Release 3.3（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）を設定する方法の詳細については、『*Configuring the Catalyst 6000 Network Analysis Module with nGenius Real-Time Monitor*』を参照してください。
- Catalyst 6500 シリーズ スイッチおよび CLI コマンドの詳細については、次のマニュアルを参照してください。
  - 『*Release Notes for Catalyst 6500 Series Switch Software*』Release 8.x
  - 『*Catalyst 6500 Series Switch Software Configuration Guide*』
  - 『*Catalyst 6500 Series Switch Command Reference*』
- ハードウェアの詳細な設定方法およびメンテナンス方法については、『*Catalyst 6500 Series Switch Module Installation Guide*』を参照してください。

マニュアルの入手方法

シスコ製品のマニュアルおよびその他の資料は、Cisco.com で入手できます。また、テクニカル サポートおよびその他のテクニカル リソースは、さまざまな方法で入手できます。ここでは、シスコ製品に関する技術情報を入手する方法について説明します。

Cisco.com

シスコの最新のマニュアルは、次の URL からアクセスしてください。

http://www.cisco.com/techsupport

シスコの 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

http://www.cisco.com/jp

シスコの Web サイトの各国語版へは、次の URL からアクセスしてください。

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

Product Documentation DVD

Product Documentation DVD は、ポータブル メディアに収容された、技術的な製品マニュアルの総合的なライブラリです。DVD を使用すると、シスコシステムズのハードウェア製品およびソフトウェア製品の様々なバージョンのインストレーション、コンフィギュレーション、コマンドガイドにアクセスできます。DVD を使用することで、インターネットに接続しなくてもシスコの Web サイトと同じ HTML 形式のマニュアルを参照できます。製品によっては、マニュアルの PDF バージョンも用意されています。

Product Documentation DVD は単独または購読契約で入手できます。Cisco.com（Cisco Direct Customers）に登録されている場合、Cisco Marketplace から Product Documentation DVD（Customer Order Number DOC-DOCDVD= または DOC-DOCDVD=SUB）を発注できます。Cisco Marketplace の URL は次のとおりです。

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

マニュアルの発注方法

Cisco.com に登録されている場合、次の URL にある Cisco Marketplace の Product Documentation Store でシスコ製品のマニュアルを発注できます。

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

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。

シスコ製品のセキュリティ

シスコでは、無償の Security Vulnerability Policy ポータルを次の URL で提供しています。

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

このサイトでは、以下のタスクを実行するための情報を入手できます。

- シスコ製品における脆弱性を報告する。
- シスコ製品のセキュリティ問題に対する支援を受ける。
- シスコからのセキュリティ情報を入手するために登録を行う。

シスコ製品に関するセキュリティ勧告、注意のリスト、および対応については、以下の URL で確認できます。

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

セキュリティ勧告、セキュリティ上の注意事項、およびセキュリティ応答の更新をリアルタイムで確認するには、Product Security Incident Response Team Really Simple Syndication（PSIRT RSS）フィードに登録します。PSIRT RSS フィードの加入に関する詳細については、次の URL にアクセスしてください。

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

シスコ製品のセキュリティ問題の報告

シスコでは、安全な製品を提供することを目指しています。製品のリリース前に社内でテストを実施し、すべての脆弱性を迅速に修正するように努めております。お客様がシスコ製品の脆弱性を発見したと思われる場合は、次の PSIRT にご連絡ください。

- 緊急度の高い問題 — security-alert@cisco.com

  緊急度の高い問題とは、システムが攻撃を受けている状態、または急を要する深刻なセキュリティの脆弱性を報告する必要がある状態を指します。それ以外の状態はすべて、緊急度の低い問題とみなされます。
- 緊急度の低い問題 — psirt@cisco.com

緊急度の高い問題の場合、次の電話番号で PSIRT に問い合わせることができます。

- 1 877 228-7302
- 1 408 525-6532

ヒント お客様が第三者に知られたくない情報をシスコに送信する場合、Pretty Good Privacy（PGP）または PGP と互換性のある製品（GnuPG など）を使用して情報を暗号化することを推奨します。PSIRT は、PGP バージョン 2.*x* ～ 9.*x* で暗号化された情報を取り扱うことができます。

無効な暗号鍵または失効した暗号鍵は使用しないでください。PSIRT への連絡時には、次の URL にある Security Vulnerability Policy ページの Contact Summary セクションにリンクされている有効な公開鍵を使用してください。

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

このページのリンクに、現在使用されている PGP 鍵の ID があります。

PGP を所有または使用していない場合は、機密情報を送信する前に、上記の E メール アドレスまたは電話番号で PSIRT に連絡し、他のデータ暗号化方法についてご確認ください。

テクニカル サポート

Cisco Technical Support では、評価の高い 24 時間体制のテクニカル サポートを提供しています。Cisco.com の Cisco Technical Support & Documentation Web サイトでは、広範囲にわたるオンラインでのサポート リソースを提供しています。さらに、シスコシステムズとサービス契約を結んでいる場合は、Technical Assistance Center（TAC）のエンジニアによる電話サポートも提供されます。シスコシステムズとサービス契約を結んでいない場合は、リセラーにお問い合わせください。

Cisco Technical Support & Documentation Web サイト

Cisco Technical Support & Documentation Web サイトでは、オンラインで資料やツールを利用して、トラブルシューティングやシスコ製品およびテクノロジーに関する技術上の問題の解決に役立てることができます。Cisco Technical Support & Documentation Web サイトは 24 時間ご利用いただけます。次の URL にアクセスしてください。

http://www.cisco.com/techsupport

Cisco Technical Support & Documentation Web サイト上のツールにアクセスする際は、いずれも Cisco.com のログイン ID および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 で登録手続きを行ってください。

http://tools.cisco.com/RPF/register/register.do

（注） テクニカル サポートにお問い合わせいただく前に、Cisco Product Identification（CPI）ツールを使用して、製品のシリアル番号をご確認ください。CPI ツールへは、Documentation & Tools の下にある **Tools & Resources** リンクをクリックして、Cisco Technical Support & Documentation Web サイトからアクセスできます。Alphabetical Index ドロップダウン リストから **Cisco Product Identification Tool** を選択するか、Alerts & RMAs の下にある **Cisco Product Identification Tool** リンクをクリックしてください。CPI ツールは、製品 ID またはモデル名、ツリー表示、または特定の製品に対する **show** コマンド出力のコピー & ペーストによる 3 つの検索オプションを提供します。検索結果には、シリアル番号のラベルの場所がハイライトされた製品の説明図が表示されます。テクニカル サポートにお問い合わせいただく前に、製品のシリアル番号のラベルを確認し、メモなどに控えておいてください。

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/

Service Request ツールの使用

オンラインの TAC Service Request ツールを使えば、S3 および S4 の問題について最も迅速にテクニカル サポートを受けられます（ネットワークの障害が軽微である場合、あるいは製品情報が必要な場合）。状況をご説明いただくと、TAC Service Request ツールが推奨される解決方法を提供します。これらの推奨リソースを使用しても問題が解決しない場合は、TAC の技術者が対応します。TAC Service Request ツールは次の URL からアクセスできます。

http://www.cisco.com/techsupport/servicerequest

問題が S1 または S2 であるか、インターネットにアクセスできない場合は、電話で TAC にご連絡ください（運用中のネットワークがダウンした場合、あるいは重大な障害が発生した場合）。S1 および S2 の問題には TAC の技術者がただちに対応し、業務を円滑に運営できるよう支援します。

電話でテクニカル サポートを受ける際は、次の番号のいずれかをご使用ください。

アジア太平洋：+61 2 8446 7411（オーストラリア：1 800 805 227）
EMEA：+32 2 704 55 55
米国：1 800 553-2447

TAC の連絡先一覧については、次の URL にアクセスしてください。

http://www.cisco.com/techsupport/contacts

問題の重大度の定義

すべての問題を標準形式で報告するために、問題の重大度を定義しました。

重大度 1（S1）— ネットワークがダウンし、業務に致命的な損害が発生する場合。24 時間体制であらゆる手段を使用して問題の解決にあたります。

重大度 2（S2）— ネットワークのパフォーマンスが著しく低下、またはシスコ製品のパフォーマンス低下により業務に重大な影響がある場合。通常の業務時間内にフルタイムで問題の解決にあたります。

重大度 3（S3）— ネットワークのパフォーマンスが低下しているが、ほとんどの業務運用が機能している場合。通常の業務時間内にサービスの復旧を行います。

重大度 4（S4）— 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で、業務への影響がほとんどまたはまったくない場合。

その他の資料および情報の入手方法

シスコの製品、テクノロジー、およびネットワーク ソリューションに関する情報について、さまざまな資料をオンラインおよび印刷物で入手できます。

- 『*Cisco Product Quick Reference Guide*』は、チャネル パートナーを通じて販売されている多くのシスコ製品について、製品概要、主要機能、サンプル製品番号、および簡潔な技術仕様が記載された、便利でコンパクトな参照ツールです。。年 2 回更新され、最新のシスコ製品に関する情報も記載されています。『*Cisco Product Quick Reference Guide*』の発注方法および詳細については、次の URL からアクセスしてください。

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

- Cisco Marketplace では、さまざまなシスコの書籍、参考資料、マニュアル、およびロゴ入り商品を提供しています。Cisco Marketplace には、次の URL からアクセスしてください。

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

- Cisco Press では、ネットワーク、トレーニング、認定関連の出版物を幅広く発行しています。初心者から上級者まで、さまざまな読者向けの出版物があります。Cisco Press の最新の出版情報などについては、次の URL からアクセスしてください。

  http://www.ciscopress.com

- 『*Packet*』は、シスコシステムズが発行するテクニカル ユーザ向けの季刊誌で、インターネットやネットワークへの投資を最大限に活用するのに役立ちます。『*Packet*』には、ネットワーク分野の最新動向、テクノロジーの進展、およびシスコの製品やソリューションに関する記事をはじめ、ネットワークの配置やトラブルシューティングのヒント、設定例、お客様の事例研究、認定やトレーニングに関する情報、および多数の詳細なオンライン リソースへのリンクが盛り込まれています。『*Packet*』には、次の URL からアクセスしてください。

  http://www.cisco.com/packet

- 『*iQ Magazine*』は、シスコのテクノロジーを使って収益の増加、ビジネス効率の向上、およびサービスの拡大を図る方法について学ぶことを目的とした、シスコシステムズが発行する成長企業向けの季刊誌です。この季刊誌は、実際の事例研究や事業戦略を用いて、これら企業が直面するさまざまな課題や、問題解決の糸口となるテクノロジーを明確化し、テクノロジーの投資に関して読者が正しい決断を行う手助けをします。『*iQ Magazine*』には、次の URL からアクセスしてください。

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

  または次の URL でデジタル版をご覧いただけます。

  http://ciscoiq.texterity.com/ciscoiq/sample/

- 『*Internet Protocol Journal*』は、インターネットおよびイントラネットの設計、開発、運用を担当するエンジニア向けに、シスコシステムズが発行する季刊誌です。『*Internet Protocol Journal*』には、次の URL からアクセスしてください。

  http://www.cisco.com/ipj

- シスコシステムズが提供するネットワーク製品およびカスタマー サポート サービスについては、次の URL にアクセスしてください。

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection は、ネットワークの専門家がネットワーク製品やネットワーク技術に関する質問、提案、情報をシスコの専門家および他のネットワーク専門家と共有するためのインタラクティブな Web サイトです。ディスカッションに参加するには、次の URL にアクセスしてください。

  http://www.cisco.com/discuss/networking

- シスコシステムズは最高水準のネットワーク関連のトレーニングを実施しています。トレーニングの最新情報については、次の URL からアクセスしてください。

  http://www.cisco.com/en/US/learning/index.html

CHAPTER 1

概要

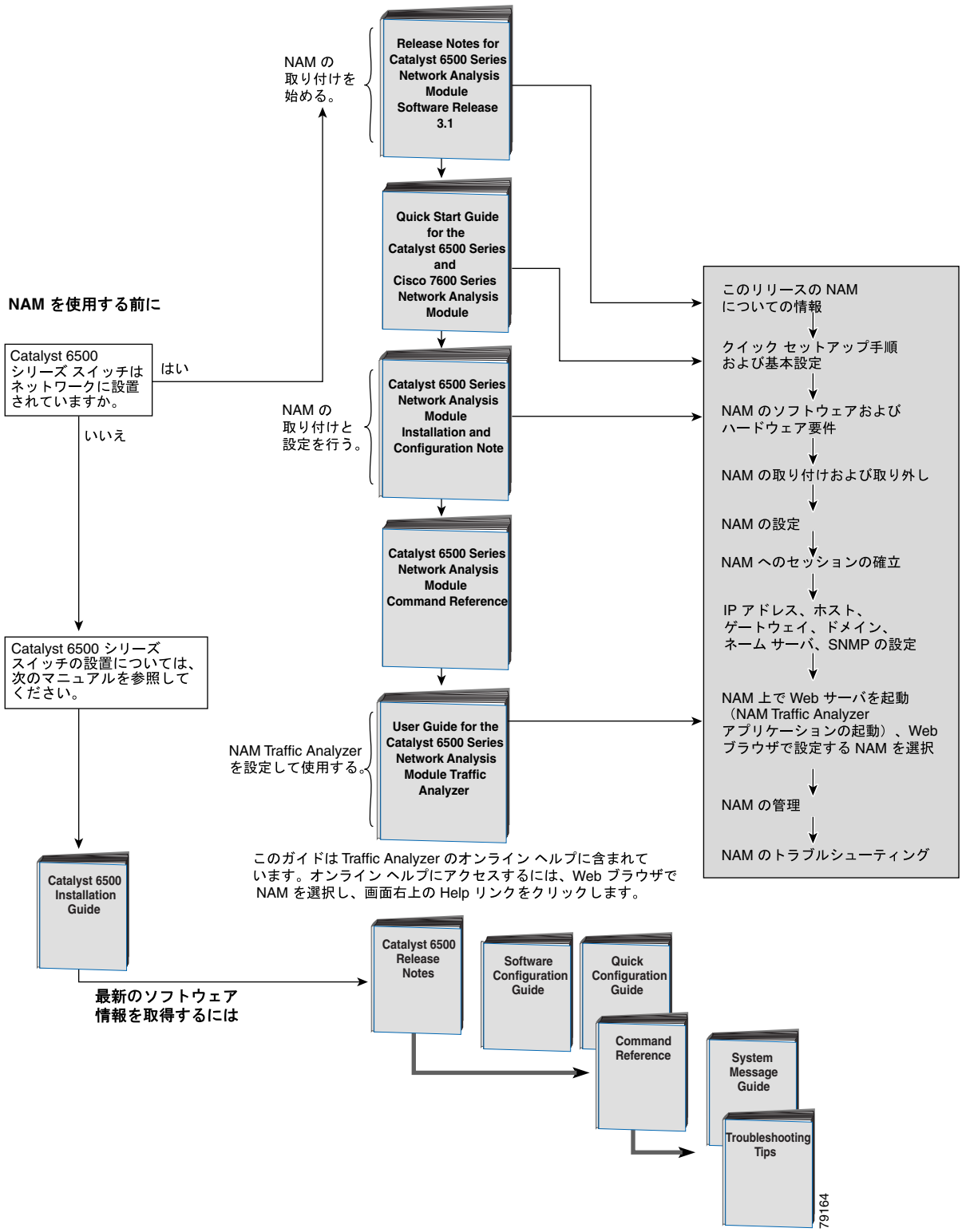
ここでは、Catalyst 6500 シリーズ スイッチ、Catalyst 6000 シリーズ スイッチ、または Cisco 7600 シリーズ ルータ Network Analysis Module（NAM; ネットワーク解析モジュール）の機能および管理方法について説明します。

(注) このインストレーション コンフィギュレーション ノートは、Catalyst オペレーティング システムと Cisco IOS ソフトウェアのユーザにも適用されます。各オペレーティング システムに関する手順については、それぞれのオペレーティングシステムのセクションで個別に明記します。

具体的な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。



NAM の機能

ここでは、Catalyst 6500 シリーズ スイッチ、Catalyst 6000 シリーズ スイッチ、または Cisco 7600 シリーズ ルータ NAM の機能を説明します。具体的な内容は次のとおりです。

- NAM における SPAN の使用方法（p.1-4）
- NAM における VACL の使用方法（p.1-5）
- NAM における NDE の使用方法（p.1-6）

NAM は、Remote Monitoring（RMON; リモート モニタリング）、スイッチド ネットワーク用の RMON 拡張機能（SMON）、および MIB（Management Information Base; 管理情報ベース）を使用してネットワーク トラフィックのモニタと解析を行います。詳細については、「サポート対象の MIB オブジェクト」（p.5-17）を参照してください。

NAM はリモート デバイスの NetFlow をモニタ、解析および表示し、次の RMON グループをサポートします。

- RFC 2819 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
- RFC 3287 で定義されている DSMON グループ
- RFC 3273 で定義されている高キャパシティ RMON グループ（メディア独立型グループをのぞく）
- RFC 2613 で定義されている SMON グループ
- Application Response Time MIB で定義されているすべてのグループ
- NetFlow バージョン 9 のレコード。NetFlow リスニング モードのデータ ソースは NetFlow バージョン 9 を使って表示されます。

NAM には、個々のイーサネット VLAN（仮想 LAN）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 スーパーバイザ 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 Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）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 は次のソースからのイーサネット VLAN トラフィックを解析できます。

- イーサネット、ファースト 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 Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）または RSPAN 送信元ポート。

  SPAN および RSPAN の詳細は、『*Catalyst 6500 Series Switch 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 の詳細は、『*Catalyst 6500 Series Switch Software Configuration Guide*』を参照してください。

表 1-1 に、NAM モニタリングに使用されるトラフィック ソースを示します。

表 1-1　NAM モニタの対象となるトラフィック ソース

トラフィック ソース	LAN		WAN	
	ポート	VLAN	ポート	VLAN
VACL キャプチャ	あり	あり	あり	不可
NDE（ローカル）	あり	あり	あり	あり
NDE（リモート）	あり	あり	あり	あり
SPAN	あり	あり	なし	なし
ERSPAN	あり	あり	なし	なし

NAM における SPAN の使用方法

SPAN セッションでは、パラメータを設定して監視対象のネットワーク トラフィックを指定し、宛先ポートを送信元ポートのセットに関連付けます。スイッチド ネットワークには複数の SPAN セッションを設定できます。

WS-SVC-NAM-1 プラットフォームには SPAN セッションの宛先ポートが 1 つあります。WS-SVC-NAM-2 プラットフォームには SPAN および VACL セッションの宛先ポートが 2 つある可能性があります。NAM への複数 SPAN セッションがサポートされていますが、ポートの宛先は別々にする必要があります。SPAN の GUI（グラフィカル ユーザ インターフェイス）で使用するデフォルトの NAM 宛先ポート名は DATA PORT 1 および DATA PORT 2 です。CLI（コマンドライン インターフェイス）の SPAN ポート名を表 1-2 に示します。

表 1-2　SPAN のポート名

モジュール	Cisco IOS ソフトウェア	Catalyst オペレーティング システム ソフトウェア
NAM-1	data-port 1	*モジュール番号*：3
NAM-2	data-port 1 および data-port 2	*モジュール番号*：7 または *モジュール番号*：8

ポートはそれぞれ独立しています。1 つのポートのトラフィックだけを読み込んでデータポート集合を作成することも、両方のポートからトラフィックを読み込んでデータポート集合を作成することもできます。また、VLAN ベースの集合も作成できます。その場合は、集合を読み込んだ VLAN に対応するポートのパケットを使用します。

SPAN の詳細および SPAN を Catalyst 6000 および 6500 シリーズ スイッチに設定する方法については、次の URL を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sy/swcg/span.htm#1032978

SPAN の詳細および SPAN を Cisco 7600 シリーズ ルータに設定する方法については、次の URL を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/software/122sx/swcg/span.htm

NAM は管理ポートの Encapsulated Remote SPAN（ERSPAN）トラフィックをサポートし、このトラフィックをデータ ソースとして使用します。ERSPAN トラフィックのすべての集合タイプがサポートされます。

ERSPAN は SPAN の拡張版で、Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）パケットにカプセル化されたパケットが ERSPAN の宛先に送信されます。通常、ERSPAN の発信元および宛先は PFC5 以降のリリースの Supervisor Engine 720 です。ERSPAN トラフィックは IP または GRE を使用してルータで送信するパケットをカプセル化し、NAM データ ポートにはカプセル化解除されたトラフィックが送信されます。

NAM における VACL の使用方法

VLAN Access Control List（VACL; VLAN アクセス コントロール リスト）とは、WAN インターフェイスまたは VLAN から NAM のデータ ポートにトラフィックを転送する方法です。VACL には SPAN を使用する方法もあります。VACL は IP および IPX プロトコルのレイヤ 3 アドレスに基づいてアクセスを制御することもできます。サポートされていないプロトコルは、MAC アドレスからアクセスが制御されます。MAC VACL を使って IP または IPX アドレスをアクセス制御することはできません。

VACL には、すべてのブリッジド VLAN パケットまたはルーテッド VLAN パケットをキャプチャするタイプと、すべてのブリッジド VLAN パケットまたはルーテッド VLAN パケットのサブセットを指定してキャプチャするタイプの 2 種類があります。Catalyst オペレーティング システムの VACL を使った場合、VLAN パケットしかキャプチャできません。これは、スイッチ上の VLAN に最初からルーティングまたはブリッジされているためです。

VACL は、VLAN 内でブリッジされているすべてのパケット、VLAN または WAN インターフェイスにルーティングされているすべてのパケット、あるいは VLAN または WAN インターフェイスからルーティングされているすべてのパケットにアクセス制御を提供できます。ただし WAN インターフェイスについてはリリース 12.1(13)E 以降しか対応していません。通常の Cisco IOS 規格や拡張 ACL はルータ インターフェイス専用に設定されており、ルーティングされたパケットにだけ適用されますが、VACL はすべてのパケットに適用でき、任意の VLAN または WAN インターフェイスに適用できます。VACL はハードウェアで処理されます。

VACL は Cisco IOS Access Control List（ACL; アクセス コントロール リスト）を使用します。VACL は、ハードウェアでサポートされない Cisco IOS ACL フィールドを無視します。標準および拡張 Cisco IOS ACL は、パケットを分類するために使用します。分類されたパケットは、アクセス コントロール（セキュリティ）、暗号化、Policy-Based Routing（PBR; ポリシー ベース ルーティング）などの機能の対象になります。標準および拡張 Cisco IOS ACL はルータ インターフェイス専用に設定され、ルーティングされたパケットに適用されます。

VLAN 上に VACL が設定されると、VLAN に届くすべてのパケットは、ルーティングされたものであれブリッジされたものであれ、VACL でチェックします。パケットはスイッチ ポートから VLAN に届く場合と、ルーティング後にルータ ポートから届く場合があります。Cisco IOS ACL とは異なり、VACL には入力や出力の方向が定義されていません。

VACL には、順番の決まった Access Control Entry（ACE; アクセス コントロール エントリ）のリストがあります。ACE にはパケットの内容に対応する多数のフィールドがあります。フィールドには関連付けたビット マスクを含めることができ、どのビットが関連しているかがわかります。ACE にはアクションが関連付けられており、一致した場合にシステムからパケットに対して行う内容が指定されています。アクションは機能に依存しています。Catalyst 6000 シリーズ スイッチ、6500 シリーズ スイッチ、および Cisco 7600 シリーズ ルータのハードウェアは次の 3 種類の ACE をサポートします。IP、IPX、MAC レイヤ トラフィックです。WAN インターフェイスに適用される VACL は IP トラフィックだけをサポートします。

VACL を設定して VLAN に適用した場合、VLAN に届くすべてのパケットを VACL でチェックします。VACL を VLAN に適用し、ACL を VLAN のルーテッド インターフェイスに適用した場合、VLAN に届くパケットはまず VACL でチェックされます。結果が permit であれば、次に入力 ACL でチェックされ、その後ルーテッド インターフェイスで処理されます。このパケットが別の VLAN にルーティングされた場合、まずルーテッド インターフェイスに適用された出力 ACL でチェックされ、結果が permit であれば、宛先 VLAN に設定された VACL が適用されます。VACL がパケット タイプに設定され、そのタイプのパケットと VACL が一致しなければ、デフォルトのアクションは deny です。

VACL を設定する場合は、次のことに注意してください。

- VACL および Context-Based Access Control（CBAC; コンテキストベース アクセス コントロール）を同じインターフェイスに設定することはできません。
- TCP 代行受信とリフレクシブ ACL が同じインターフェイスに設定されている場合、VACL のアクションが優先されます。
- Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）パケットは VACL でチェックされません。

Cisco IOS ソフトウェアで VACL を設定する方法の詳細については『*Network Analysis Module for Catalyst 6500 Series and Cisco 7600 Series Command Reference*』を参照してください。Catalyst オペレーティング システムでセキュリティ ACL を設定する方法の詳細については、『*Catalyst 6500 Series Software Configuration Guide*』および『*Catalyst 6500 Series Command Reference*』を参照してください。

NAM における NDE の使用方法

NDE は、NAM のポート トラフィックが監視できるリモート デバイスです。NAM の NDE データ ソースを使用するには、NAM の UDP ポート 3000 に NDE パケットをエクスポートするようにリモート デバイスを設定します。デバイスはインターフェイスごとに設定する必要があります。Web アプリケーション ユーザ インターフェイスに、NDE デバイスを指定するための画面が追加されています（NDE デバイスは IP アドレスで区別できます）。デフォルトでは、スイッチのローカル スーパーバイザ エンジンは常に NDE デバイスとして使用できます。

IP アドレスとコミュニティ ストリングを指定すると、追加の NDE デバイスが定義できます。コミュニティ ストリングは省略可能です。コミュニティ ストリングは、インターフェイス用に便利なテキスト形式の文字列をリモート デバイスにアップロードして、NetFlow レコードで監視するために使用します。

NAM の NDE データ ソースについては、NAM Traffic Analyzer のオンライン ヘルプで **Contents > Setting Up the Application > Setting Up Data Sources > Understanding NetFlow Interfaces** の順に選択してください。

NAM の管理

NAM を管理するには、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 CiscoWorks 2000 にバンドルされているような Simple Network Management Protocol（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を使用します。

NAM Traffic Analyzer 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 を使用するには、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 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。

- さまざまな統計情報の履歴レポートの設定および表示
- 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 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。Cisco NetScout nGenius RTM は Cisco Works 2000 LAN Management Solution（LMS）のコンポーネントです。RTM の詳しい使用方法については、CiscoWorks のマニュアルまたは次の 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。

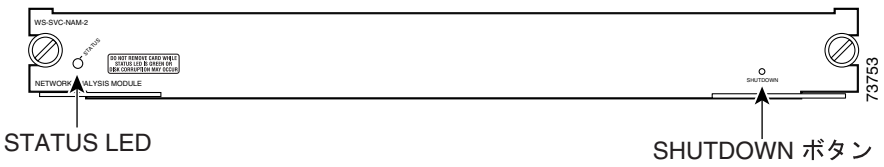
すでにスイッチ上で NAM を設定し稼働させていて、NAM の使用手順を熟知している場合は、**ip http server enable** CLI コマンドを入力してブラウザで NAM Traffic Analyzer を起動し、NAM Traffic Analyzer の使用を開始できます。

NAM Traffic Analyzer の詳しい使用方法については、『*User Guide for the Network Analysis Module Traffic Analyzer*』Release 3.3 を参照してください。

前面パネル

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

図 1-1　Network Analysis Module



STATUS LED

STATUS LED は、NAM の動作状態を表します（表 1-3 を参照）。

表 1-3　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。NAM が完全にシャットダウンする前にスイッチから NAM を取り外すと、ディスクが破損する可能性があります。

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あとにシャーシから 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、スーパーバイザ 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。

（注）　破損したディスクを復旧するには、**--install** オプションを使ってアプリケーション イメージをアップグレードします。「Catalyst オペレーティング システム ソフトウェアを使用した NAM アプリケーション ソフトウェアのアップグレード」（p.19）を参照してください。

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開始します。

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 1-4 に、NAM の仕様を示します。

表 1-4　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）
周囲湿度 （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

CHAPTER 2

NAM の要件

ここでは、Catalyst 6500 シリーズ スイッチ、Catalyst 6000 シリーズ スイッチ、または Cisco 7600 シリーズ ルータ Network Analysis Module（NAM; ネットワーク解析モジュール）をサポートするソフトウェア要件とハードウェア要件について説明します。具体的な内容は次のとおりです。

ソフトウェアの要件

(注) メンテナンス イメージ リリース 2.1(1) 以上のサービス モジュールにはメンテナンス イメージがあります。次の URL を参照してください。
http://www.cisco.com/cgi-bin/tablebuild.pl/cat6000-serv-maint

表 2-1 に、Catalyst オペレーティング システム ソフトウェアおよび Cisco IOS ソフトウェアでサポートされる NAM のソフトウェア リリースを示します。

表 2-1　NAM ソフトウェアの互換性

モジュール	アプリケーション イメージ	メンテナンス イメージ	Catalyst オペレーティング システム 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	Java プラグイン サポート[1]
WS-SVC-NAM-1 WS-SVC-NAM-2	3.6(1)	1.1(1)m 2.1(1)	リリース 7.3(1) 以降（Supervisor Engine 1A または 2 を使用）[2] リリース 8.2(1) 以降（WS-SUP720 を使用）	リリース 12.1(13)E[3] 以降（MSFC2 搭載の Supervisor Engine 2 を使用） リリース 12.1(19)E1 以降（MSFC2 搭載の Supervisor Engine 1A を使用） リリース 12.2(14)SX1（WS-SUP720 を使用）	推奨 — Internet Explorer 6.0 以降（Windows 2000 を使用） Netscape 7.0 または 7.1 以降（Windows 2000 および Solaris を使用） Mozilla 1.7 Firefox 1.5、2.0	1.3.1_03 または 1.4.1_02 1.4.1_02（Windows 2000）および 1.4.0_01（Solaris）
WS-SVC-NAM-1 WS-SVC-NAM-2	3.5(1)	1.1(1)m 2.1(1)	リリース 7.3(1) 以降（Supervisor Engine 1A または 2 を使用）[4] リリース 8.2(1) 以降（WS-SUP720 を使用）	リリース 12.1(13)E[5] 以降（MSFC2 搭載の Supervisor Engine 2 を使用） リリース 12.1(19)E1 以降（MSFC2 搭載の Supervisor Engine 1A を使用） リリース 12.2(14)SX1（WS-SUP720 を使用）	推奨 — Internet Explorer 6.0 以降（Windows 2000 を使用） Netscape 7.0 または 7.1 以降（Windows 2000 および Solaris を使用）	1.3.1_03 または 1.4.1_02 1.4.1_02（Windows 2000）および 1.4.0_01（Solaris）

1. Traffic Analyzer には Java プラグインは不要ですが、Java Virtual Machine（JVM）を使用するときは必要な場合があります。ここに記載されている Java プラグインのバージョンは、JVM のプラグインを必要とするブラウザでテスト済みです。
2. MSFC1 または MSFC2 搭載の Supervisor 1A、または MSFC2 搭載の Supervisor 2 のみ。
3. 12.1(13)E ベースのリリースを使用する場合は、リリース 12.1(13)E11 ～ 12.1(13)E3 の 13E リリースを使用することを推奨します。
4. MSFC1 または MSFC2 搭載の Supervisor 1A、または MSFC2 搭載の Supervisor 2 のみ。
5. 12.1(13)E ベースのリリースを使用する場合は、リリース 12.1(13)E11 ～ 12.1(13)E3 の 13E リリースを使用することを推奨します。

ハードウェアの要件

表 2-2 に、Catalyst オペレーティング システム ソフトウェアおよび Cisco IOS ソフトウェアでサポートされる NAM のハードウェア リリースを示します。

表 2-2　NAM ハードウェアの互換性

モジュール	Catalyst オペレーティング システム ソフトウェア	Cisco IOS ソフトウェア	プラットフォーム
WS-SVC-NAM-1 WS-SVC-NAM-2	Supervisor Engine 1A または 2、または WS-SUP720	MSFC2 搭載の Supervisor Engine 1、MSFC2 搭載の Supervisor Engine 2、WS-SUP720、SUP32	Catalyst 6500 シリーズ スイッチ、Cisco 7600 シリーズ ルータ

CHAPTER 3

NAM の設定

ここでは、Catalyst 6500 シリーズ スイッチ、Catalyst 6000 シリーズ スイッチ、または Cisco 7600 シリーズ ルータ Network Analysis Module（NAM; ネットワーク解析モジュール）の設定方法を説明します。具体的な内容は次のとおりです。

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 オペレーティング システム 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。

NAM の初期設定については、『*Quick Start Guide for the Catalyst 6500 Series and Cisco 7600 Series Network Analysis Module*』を参照してください。

NAM を初期設定すると、ネットワーク トラフィック モニタするように VLAN Access Control List（VACL; VLAN アクセス コントロール リスト）、ローカルまたはリモートの NetFlow Data Export（NDE; NetFlow データ エクスポート）、Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）を設定できます。詳細については、「NAM のトラフィックをキャプチャするトラフィック ソースの設定」（p.3-2）を参照してください。

ソフトウェア別の NAM 属性の設定が完了すると、両方のソフトウェアに共通した属性を設定できます。詳細については、「オペレーティング システムに依存しない設定」（p.3-13）を参照してください。

NAM のトラフィックをキャプチャするトラフィック ソースの設定

WS-SVC-NAM-1 プラットフォームには SPAN セッションの宛先ポートが 1 つあります。

WS-SVC-NAM-2 プラットフォームには VACL および SPAN セッションで使用可能な宛先ポートが 2 つあります。デフォルトでは、SPAN の GUI（グラフィカル ユーザ インターフェイス）で使用する宛先ポート名は data-port 1 および data-port 2 です。CLI（コマンドライン インターフェイス）SPAN ポート名は表 1-2 を参照してください。

VACL および SPAN を同じポートに同時に設定することはできません。表 3-1 に、NAM でサポートされる SPAN および VACL ポート設定を示します。

表 3-1　NAM SPAN および VACL ポートの設定

NAM-1	NAM-2
1 つの SPAN セッションのみ	2 つの SPAN セッション
1 つの VACL セッションのみ	1 つの SPAN セッションと 1 つの VACL セッション
	2 つの VACL セッション

SPAN の詳細については、次の URL を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/span.htm

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_8_2/confg_gd/span.htm

VACL の詳細については、次の URL を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/vacl.htm

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_82/confg_gd/acc_list.htm#1053650

NDE の詳細については、次の URL を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/nde.htm#1035105

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_8_2/confg_gd/nde.htm

以下の各セクションでは、VACL、ローカルまたはリモート NDE、SPAN を設定して NAM でネットワーク トラフィックを監視する方法について説明します。

- Cisco IOS ソフトウェア（p.3-2）
- Catalyst オペレーティング システム ソフトウェア（p.3-9）

Cisco IOS ソフトウェア

1 つまたは複数の VLAN から、NAM を監視するトラフィックをキャプチャできます。特定の VLAN だけで監視するには、監視に使用しない VLAN をキャプチャ機能から外します。

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 の詳細については、次の URL で『*Catalyst 6500 Series Switch Cisco 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**]	監視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*	監視セッションをディセーブルにします。
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}*	現在の監視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# configure terminal
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 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 data-port 1 です。NAM-2 の SPAN 宛先ポートは data-port 1 および data-port 2 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
```

トラフィック ソースとして VACL を使用する場合

ここでは、Cisco IOS Release 12.1(13)E1 以降を実行するスイッチに VACL を設定する方法について説明します。Catalyst オペレーティング システム上で LAN VACL を設定する場合、セキュリティ ACL 機能を使用すると同じように設定できます。詳細については、「オペレーティング システムに依存しない設定」（p.3-13）を参照してください。

WAN インターフェイス上での VACL の設定

WAN インターフェイスは SPAN をサポートしません。NAM を使用して WAN インターフェイス上でトラフィックを監視する場合は、スイッチの CLI を使用してスイッチ上に VACL を手動で設定する必要があります。この機能は、WAN インターフェイスの IP トラフィックでのみ有効です。フィルタリング規則を追加して、特定のデータ フローを監視することもできます。

トラフィックを NAM に送信する SPAN セッションがない場合にも VACL が使用できます。この場合は、SPAN の代わりに VACL を設定して VLAN トラフィックを監視します。

次の例では、Cisco IOS Release 12.1(13)E1 以降を実行するスイッチの VACL 設定に必要な手順を示します。Catalyst オペレーティング システムを実行するスイッチに LAN VACL を設定する場合、同じ設定になるように ACL 機能を使用します。

この例では、Asynchronous Transfer Mode（ATM; 非同期転送モード）の WAN インターフェイス上で VACL を設定して NAM に入出トラフィックをどちらも転送する手順を示します。

```
Cat6500# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Cat6509(config)# access-list 100 permit ip any any
Cat6509(config)# vlan access-map wan 100
Cat6509(config-access-map)# match ip address 100
Cat6509(config-access-map)# action forward capture
Cat6509(config-access-map)# exit
Cat6509(config)# vlan filter wan interface ATM6/0/0.1
Cat6509(config)# analysis module 3 data-port 1 capture allowed-vlan 1-4094
Cat6509(config)# analysis module 3 data-port 1 capture
Cat6509(config)# exit
```

出トラフィックのみを監視する場合は、WAN インターフェイス コマンドに関連付けられる VLAN ID が取得できます。次に例を示します。

```
Cat6509# show cwan vlan
Hidden VLAN  swidb->if_number   Interface
-----------------------------------------------
1017          94               ATM6/0/0.1
```

VLAN ID を取得したら、次のように NAM データ ポート キャプチャを設定します。

```
Cat6509(config)# analysis module 3 data-port 1 capture allowed-vlan 1017
```

入トラフィックを監視するには、前回キャプチャ設定した VLAN 1017 を入トラフィックを送信する VLAN ID に置き換えます。たとえば、NAM に次のような設定をすると WAN インターフェイス上の入トラフィックだけが監視できます。

```
Cat6509(config)# analysis module 3 data-port 1 capture allowed-vlan 1
```

LAN VLAN インターフェイス上での VACL 設定

LAN 上で VLAN トラフィックを監視するには、SPAN を使って NAM にトラフィックを転送します。ただし、状況によっては転送されたトラフィックが NAM のモニタリング能力を超えることもあります。このため、あらかじめ LAN トラフィックにフィルタを設定してから NAM に転送することもできます。

次に、LAN VLAN インターフェイスに VACL を設定する例を示します。この例では、VLAN 1 上のサーバ 172.20.122.226 に送信するトラフィックをすべてキャプチャし、スロット 3 に搭載された NAM に転送しています。

```
Cat6500# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Cat6500(config)# access-list 100 permit ip any any
Cat6500(config)# access-list 110 permit ip any host 172.20.122.226
Cat6500(config)# vlan access-map lan 100
Cat6500(config-access-map)# match ip address 110
Cat6500(config-access-map)# action forward capture
Cat6500(config-access-map)# exit
Cat6500(config)# vlan access-map lan 200
Cat6500(config-access-map)# match ip address 100
Cat6500(config-access-map)# action forward
Cat6500(config-access-map)# exit
Cat6500(config)# vlan filter lan vlan-list 1
Cat6500(config)# analysis module 3 data-port 1 capture allowed-vlan 1
Cat6500(config)# analysis module 3 data-port 1 capture
Cat6500(config)# exit
```

トラフィック ソースとして NDE を使用する場合

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 トラフィックを監視できます。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。

NetFlow デバイスに NDE を設定して NDE パケットを NAM にエクスポートする手順は、送信デバイスのプラットフォームやバージョンによって異なります。詳細については、デバイスの NDE 設定ガイドラインを参照してください。

NDE の設定

ローカルおよびリモートの NDE デバイスに Cisco IOS ソフトウェアの NDE を設定する手順は次のとおりです。

ステップ 1　次の手順で、NDE を設定します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface type slot/port
```

ステップ 2　インターフェイスの NetFlow をイネーブルにします。

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

ステップ 3　ルーティングされたフロー キャッシュのエントリを NAM UDP ポート 3000 にエクスポートします。

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

（注） UDP ポート番号は、3000 に設定する必要があります。

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。

次に、基本的な NDE を設定する手順を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface vlan 2
Router(config)# ip route-cache flow
Router(config)# ip flow-export destination 172.20.104.74 3000
Router(config)# exit
```

MLS キャッシュからの NDE の設定

Policy Feature Card（PFC; ポリシー フィーチャ カード）（Multilayer Switching［MLS; マルチレイヤスイッチング］キャッシュ）から NDE を設定する手順は、次のとおりです。

ステップ 1　設定モードを入力します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

ステップ 2　NDE のバージョンを選択します。

```
Router(config)# mls nde sender version version-number
```

（注） NAM は NDE バージョン 1、5、6、7、8 およびバージョン 8 の集計キャッシュをサポートします。NAM で使用できる NDE バージョンについては、スイッチ ソフトウェアがサポートする NDE のバージョンを Cisco IOS のマニュアルで参照してください。

ステップ 3　NDE フロー マスクを選択します。

```
Router(config)# mls flow ip [interface-full | full]
```

（注） full キーワードを使用して、フロー マスクに収集データの詳細が含まれるようにします。

ステップ 4　NetFlow のエクスポートをイネーブルにします。

```
Router(config)# mls nde sender
```

ステップ 5　NetFlow パケットを NAM UDP ポート 3000 にエクスポートします。

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

次に、Multilayer Switch Feature Card（MSFC; マルチレイヤ スイッチ フィーチャ カード）から NDE を設定する方法を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# mls nde sender version 5
Router(config)# mls flow ip full
Router(config)# mls nde sender
Router(config)# ip route-cache flow
Router(config)# ip flow-export destination 172.20.104.74 3000
Router# show ip cache flow
Router# show ip flow export
```

（注）　PFC に NDE を設定する方法の詳細については、次の URL を参照してください。
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/12_1e/swconfig/nde.htm - xtocid14

バージョン 8 集計の NDE の設定

（注）　NAM は NDE 集計をサポートしますが、指定した集計タイプについて受信する内容は集計に限られます。他の内容については受信できません。NDE 設定についての詳細を受け取るには、フル フロー モードを指定します。

NetFlow デバイスが NDE バージョン 8 集計をサポートしている場合、1 つまたは複数のバージョン 8 集計キャッシュからのフローを NAM にエクスポートできます。具体的な手順は次のとおりです。

ステップ 1　NDE バージョン 8 集計を選択します。

```
Router(config)# ip flow-aggregation cache aggregation-type
```

サポートされている集計タイプは次のとおりです。

- 宛先プレフィクス
- 送信元プレフィクス
- プロトコルポート
- プレフィクス

ステップ 2　集計キャッシュをイネーブルにします。

```
Router(config-flow-cache)# enable
```

ステップ 3　集計キャッシュのフロー エントリを NAM UDP ポート 3000 にエクスポートします。

```
Router(config-flow-cache)# export destination NAM-Address 3000
```

ステップ 4　NDE を検証します。

```
Router# show ip cache flow-aggregation aggregation-type
```

次に、NDE バージョン 8 集計の設定方法を示します。

```
Router(config)# ip flow-aggregation cache prefix
Router(config-flow-cache)# enable
Router(config-flow-cache)# export destination 172.20.104.74 3000
Router(config-flow-cache)# exit
Router(config)# show ip cache flow-aggregation prefix
```

Catalyst オペレーティング システム ソフトウェア

1 つまたは複数の VLAN から、NAM を監視するトラフィックをキャプチャできます。特定の VLAN だけで監視するには、監視に使用しない VLAN をキャプチャ機能から外します。

トラフィック ソースとして SPAN を使用する場合

Remote SPAN（RSPAN）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。

SPAN および RSPAN の詳細については、『*Catalyst 6500 Series Switch Software Configuration Guide*』の「Configuring SPAN and RSPAN」を参照してください。

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
```

トラフィック ソースとして LAN VACL を使用する場合

WAN VACL を使用するとインバウンドまたはアウトバウンド VLAN パケットをキャプチャしますが、Catalyst オペレーティング システム VACL は VLAN パケットが最初にスイッチの VLAN にルーティングされたときまたはブリッジされたときに VLAN パケットをキャプチャする場合にだけ使用します。

次に、VACL を作成してスイッチの VLAN 1 から NAM-1 データ ポート 6/3 にブリッジまたはルーティングされるすべての IP パケットをキャプチャする方法を示します。

```
Console> (enable) set security acl ip LANCAPTURE permit ip any any capture
Console> (enable) commit
Console> (enable) set security acl map LANCAPTURE 1
Console> (enable) set security acl capture 6/3
```

次に、VACL を作成して特定の VLAN 1 カンバセーションをキャプチャする方法を示します。

```
Console> (enable) set sec acl ip LANCAPTURE permit ip host 172.20.122.70 host
172.20.122.226 capture
Console> (enable) set security acl ip LANCAPTURE permit ip any any
Console> (enable) commit
Console> (enable) set security acl map LANCAPTURE 1
Console> (enable) set security acl capture 6/3
```

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。ローカル スイッチの統計情報は、NAM の前回のリリースと同様、予約された ifIndex.3000 で提供されます。リモート スイッチは ifIndex.50000 以上を使用します。

(注) NetFlow を使用するには、MSFC の設定が必要です。詳細については、『*Catalyst 6500 Series Switch Software Configuration Guide*』を参照してください。

(注) NetFlow のカスタム データ ソースを作成する CLI コマンドはありません。NetFlow のカスタム データ ソースを作成する場合は、NAM Traffic Analyzer の GUI を使用します。

NDE の設定

次の手順で、Catalyst オペレーティング システムの NetFlow モニタをイネーブルにします。

	作業	コマンド
ステップ 1	NDE のバージョンを選択します。 **（注）** NAM は NDE バージョン 1、5、6、7、8 およびバージョン 8 の集計キャッシュをサポートします。NAM で使用できる NDE バージョンについては、スイッチ ソフトウェアがサポートする NDE のバージョンを Cisco IOS のマニュアルで参照してください。	**set mls nde version** *nde-version-number*
ステップ 2	NDE フロー マスクを full に指定します。 **（注）** NAM は NDE 集計をサポートしますが、指定した集計タイプについて受信する情報はそのときの集計に限られ、他の内容については受信できません。NDE 設定についての詳細を受け取るには、フル フロー モードを指定します。	**set mls flow full**
ステップ 3	NAM に NDE パケットを送信します。	**set snmp extendedrmon netflow** [**enable** | **disable**] ***mod*** **set mls nde** *NAM-address* **3000**
ステップ 4	NDE エクスポートをイネーブルにします。	**set mls nde enable**
ステップ 5	（任意）デバイスが if-index をエクスポートすることを確認します。 **（注）** インターフェイス別の NetFlow データおよび NAM の指示を中止したい場合はこの手順を実行します。	**set mls nde destination-ifindex enable** **set mls nde source-ifindex enable**
ステップ 6	NDE エクスポートを検証します。 ローカル デバイス： リモート デバイス：	 **show snmp and show mls nde** **show mls nde**

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 6500 Series Software Configuration Guide*』で説明されているように、**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。

ブリッジされたフロー統計情報から NDE をエクスポートする

スイッチがブリッジされたフロー統計情報からの NDE のエクスポートをサポートする場合、ブリッジされたフロー統計情報を使って NDE を NAM にエクスポートできます。

次の手順で、ブリッジされたフロー統計情報を NDE にエクスポートします。

	作業	コマンド
ステップ 1	ブリッジされた VLAN 上のフロー統計情報をイネーブルにします。	**set mls bridged-flow-statistics enable** ***vlan-list***
ステップ 2	NDE パケットを NAM の UDP ポート 3000 にエクスポートします。	**set mls nde** ***NAM-address*** **3000**

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。

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。ユーザ名とパスワードは、Web ユーザと CLI ユーザでは区別して管理されています。NAM CLI のユーザ名とパスワードを変更する場合は、「Cisco IOS ソフトウェア」（p.4-1）および「Catalyst オペレーティング システム ソフトウェア」（p.4-13）を参照してください。Web インターフェイスでユーザ名とパスワードを変更する場合は、NAM Traffic Analyzer アプリケーションのオンライン ヘルプと『*User Guide for the Network Analysis Module Traffic Analyzer*』Release 3.3 を参照してください。

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.
```

HTTP セキュア サーバの設定

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　http://www.cisco.com からパッチをダウンロードして、FTP サーバに送信します。

ステップ 2　次のコマンドを入力して、パッチをインストールします。

```
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。

```
root@localhost# patch ftp://host/path/c6nam- 3.3-strong-cryptoK9-patch-1-0.bin

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

Downloading c6nam- 3.3-strong-cryptoK9-patch-1-0.bin. Please wait...
ftp://host/path/c6nam- 3.3-strong-cryptoK9-patch-1-0.bin (1K)
-                         [########################]       1K |  228.92K/s
1891 bytes transferred in 0.01 sec (225.40k/sec)

Verifying c6nam- 3.3-strong-cryptoK9-patch-1-0.bin. Please wait...
Patch c6nam- 3.3-strong-cryptoK9-patch-1-0.bin verified.

Applying /usr/local/nam/patch/workdir/c6nam- 3.3-strong-cryptoK9-patch-1-0.bin.
Please wait...
########################################## [100%]
########################################## [100%]

Patch applied successfully.
```

ステップ 3　（任意）次のコマンドを入力して、HTTPS サーバを設定します。

（注）　デフォルト（443）以外のポートを指定する場合は、*port_number* を追加します。

```
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 4　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局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。

次に、自己署名証明書を生成する方法を示します。

```
root@localhost# ip http secure generate self-signed-certificate

The HTTP secure server is enabled now. You must restart
to generate the certificate. Continue [y/n]? y
5243 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]:US
State or Province Name (full name) [Some-State]:CA
Locality Name (eg, city) []:San Jose
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Cisco Systems, Inc.
Organizational Unit Name (eg, section) []:NAM
Common Name (eg, your name or your server's hostname) [r2d2-186.cisco.com]:
Email Address []:kjchen@cisco.com
Using configuration from /usr/local/nam/defaults/openssl.cnf
-----BEGIN CERTIFICATE-----
MIIDlTCCAv6gAwIBAgIBADANBgkqhkiG9w0BAQQFADCBlDELMAkGA1UEBhMCVVMx
CzAJBgNVBAgTAkNBMREwDwYDVQQHEwhTYW4gSm9zZTEcMBoGA1UEChMTQ2lzY28g
U3lzdGVtcywgSW5jLjEMMAoGA1UECxMDTkFNMRswGQYDVQQDExJyMmQyLTE4Ni5j
aXNjby5jb20xHDAaBgkqhkiG9w0BCQEWDW5hbUBjaXNjby5jb20wHhcNMDQwMjI0
MDAwNDAxWhcNMDUwMjIzMDAwNDAxWjCBlDELMAkGA1UEBhMCVVMxCzAJBgNVBAgT
AkNBMREwDwYDVQQHEwhTYW4gSm9zZTEcMBoGA1UEChMTQ2lzY28gU3lzdGVtcywg
SW5jLjEMMAoGA1UECxMDTkFNMRswGQYDVQQDExJyMmQyLTE4Ni5jaXNjby5jb20x
HDAaBgkqhkiG9w0BCQEWDW5hbUBjaXNjby5jb20wgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBAMDrGqhw2Kt8fimI+b11bk6+z9nTEQago1Qfoo8DehBLZ10eoJ/0
YAWlCqx3fnW3csSmGiHj6aEjJhm0WO5GvJRbzzbxeSPadDv7IdbIhXTLtPklW11g
byhUzvi5R8UFGSmerbbnc7qkTDXQdrQ2vETAfxK4oysq+HF55qVjY2KpAgMBAAGj
gfQwgfEwHQYDVR0OBBYEFEjcj4+vFJmLAo1NjnO9MYE/Hn9eMIHBBgNVHSMEgbkw
gbaAFEjcj4+vFJmLAo1NjnO9MYE/Hn9eoYGapIGXMIGUMQswCQYDVQQGEwJVUzEL
MAkGA1UECBMCQ0ExETAPBgNVBAcTCFNhbiBKb3NlMRwwGgYDVQQKExNDaXNjbyBT
eXN0ZW1zLCBJbmMuMQwwCgYDVQQLEwNOQU0xGzAZBgNVBAMTEnIyZDItMTg2LmNp
c2NvLmNvbTEcMBoGCSqGSIb3DQEJARYNbmFtQGNpc2NvLmNvbYIBADAMBgNVHRME
BTADAQH/MA0GCSqGSIb3DQEBBAUAA4GBAHwBnz9OALHWkyK4qYTTbBno2MFbmI49
gU4IIpFSgWjoqdiXXGJs7c1q0dMPzdmDIG1TjmkLx2HC1+dVuq/2X4RrOFaoog/s
K9GmULi8OtgRkDhXJHT/gDfv+L7gQpQCCpq1TUFMVlzxzAHSsBGnlQ8oTysXScEJ
nSr0tR/OKB0t
-----END CERTIFICATE-----
Disabling HTTP secure server...
Successfully disabled HTTP secure server.
Enabling HTTP secure server...
Successfully enabled HTTP secure server.
root@localhost#
```

認証局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、その要求を認証局に手動で提出する必要があります。認証局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

認証局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、認証局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。

CHAPTER 4

NAM の管理

Catalyst 6500 シリーズ スイッチ、Catalyst 6000 シリーズ スイッチ、Cisco 7600 シリーズ ルータ上の Network Analysis Module（NAM; ネットワーク解析モジュール）を管理する方法は、Cisco IOS ソフトウェアと Catalyst オペレーティング システム ソフトウェアのどちらを使用しているかによって異なります。ただし、両方のオペレーティング システムに共通する手順もいくつかあります。

以下の各セクションでは、CLI（コマンドライン インターフェイス）を使用して NAM を管理する手順について、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.4-1）
- Catalyst オペレーティング システム ソフトウェア（p.4-13）

ソフトウェア別の NAM 属性の設定が完了したら、両方のソフトウェアに共通した属性を設定できます。詳細については、「オペレーティング システムに依存しない NAM 管理」（p.4-23）を参照してください。

Cisco IOS ソフトウェア

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

- Cisco IOS ソフトウェアを使用した NAM へのログイン（p.4-1）
- Cisco IOS ソフトウェアを使用した NAM CLI パスワードの変更（p.4-3）
- Cisco IOS ソフトウェアを使用した NAM のリセット（p.4-4）
- Cisco IOS ソフトウェアを使用した NAM ソフトウェアのアップグレード（p.4-5）
- Cisco IOS ソフトウェアを使用した mini-RMON の設定（p.4-12）

Cisco IOS ソフトウェアを使用した 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 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。WS-SVC-NAM-1 または WS-SVC-NAM-2 の場合、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 4-1 に、NAM のユーザ レベルとパスワードを示します。

表 4-1　NAM のユーザとパスワード

モジュール	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）	
WS-SVC-NAM-1 WS-SVC-NAM-2	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、すべての読み取り権限とすべての書き込み権限が与えられます。

アプリケーション イメージまたはメンテナンス 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。

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（セキュア シェル）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#
```

Cisco IOS ソフトウェアを使用した 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 で **rmwebusers** コマンドを使用すると、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 文字以上にする必要があります。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） WS-SVC-NAM-1 および WS-SVC-NAM-2 モジュールで、NAM メンテナンス イメージ用の 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 4-1 または 表 4-4 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
```

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　この新しいパスワードを再入力します。

```
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 で **clear module pc-module** *module-number* **password** コマンドを入力すると、アプリケーション イメージの 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。

Cisco IOS ソフトウェアを使用した 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、**hw-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** コマンドに **mem-test-full** キーワードを使用します。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 オペレーティング システム ソフトウェアには使用できません

Catalyst オペレーティング システム ソフトウェアについては、「Catalyst オペレーティング システム ソフトウェアを使用した NAM のリセット」（p.4-17）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。

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 boot-device mem-test-full
```

モジュールをリセットして NAM をアプリケーション イメージで起動するには、Cisco IOS CLI プロンプトで **hw-module module** *slot* **reset hdd:1** [**mem-test-full**] コマンドを入力します。

モジュールをリセットして NAM をメンテナンス イメージで起動するには、Cisco IOS CLI プロンプトで **hw-module module** *slot* **reset cf:1** [**mem-test-full**] コマンドを入力します。

次に、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# hw-module mod 9 reset cf:1 memtest-full

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

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。次に、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。

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
```

Cisco IOS ソフトウェアを使用した 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、「Catalyst オペレーティング システム ソフトウェアを使用した NAM アプリケーション ソフトウェアのアップグレード」（p.4-19）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、「Catalyst オペレーティング システム ソフトウェアを使用した NAM メンテナンス ソフトウェアのアップグレード」（p.4-20）を参照してください。

NAM アプリケーション イメージとメンテナンス イメージには互換性がありません。

表 4-2 に、NAM イメージ プレフィクスを示します。

表 4-2　NAM イメージ プレフィクス

モジュール	アプリケーション イメージ	メンテナンス イメージ
WS-SVC-NAM-1	nam-app	c6svc-nam-maint
WS-SVC-NAM-2	nam-app	c6svc-nam-maint

Cisco IOS ソフトウェアを使用した 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、特権モードで次のコマンドを入力します。

```
Router# hw-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。

または

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

（注）　**--install** キーワードはすべての NAM パーティションをクリアして再作成し、工場出荷時のデフォルト設定にします。**--install** キーワードを使用すると、それまでに保存されているレポートやデータがある場合は失われます。

（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# hw-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 ...
```

（注） NAM のパフォーマンスを最適にするには、NAM ソフトウェアをアップグレードしたあとでアプリケーション パーティションを起動し、その後すぐにもう 1 度再起動します。

ステップ 9　（任意）NAM がオンラインに戻ったあと、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
root@localhost# show version
```

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。

```
root@localhost# hw-module module 7 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 7
root@localhost# show mod
Mod Ports Card Type                                Model              Serial No.
--- ----- ---------------------------------------- ------------------ -----------
  2     8  Network Analysis Module                 WS-SVC-NAM-2       SAD060301SS
  3     8  Network Analysis Module                 WS-SVC-NAM-2       SAD060301SR
  5     2  Supervisor Engine 720 (Active)          WS-SUP720-BASE     SAD0813071R
  7     8  Network Analysis Module (MP)            WS-SVC-NAM-2       SAD065002TK
  8     0  2 port adapter Enhanced FlexWAN         WS-X6582-2PA       JAB093000QE
  9    48  48 port 10/100 mb RJ-45 ethernet        WS-X6248-RJ-45     SAD03462861

Mod MAC addresses                       Hw     Fw           Sw           Status
--- ----------------------------------- ------ ------------ ------------ -------
  2  0003.feab.1180 to 0003.feab.1187   3.0    7.2(1)       3.4(1a)      Ok
  3  00e0.b0ff.33f8 to 00e0.b0ff.33ff   0.101  Unknown      Unknown      PwrDown
  5  000d.2910.3f68 to 000d.2910.3f6b   3.1    7.7(1)       12.2(18)SXE2 Ok
  7  0005.9a3b.9d10 to 0005.9a3b.9d17   1.0    7.2(1)       2.1(2)m      Ok
  8  0013.800f.be10 to 0013.800f.be4f   2.0    12.2(18)SXE2 12.2(18)SXE2 Ok
  9  0030.962c.6750 to 0030.962c.677f   1.1    4.2(0.24)VAI 8.5(0.46)ROC Ok
```

```
Mod Sub-Module                  Model              Serial        Hw     Status
--- --------------------------- ------------------ ------------ ------- -------
  5 Policy Feature Card 3       WS-F6K-PFC3A       SAD081302ST   2.2    Ok
  5 MSFC3 Daughterboard         WS-SUP720          SAD081305DT   2.2    Ok

Mod Online Diag Status
--- -------------------
  2 Pass
  3 Unknown
  5 Pass
  7 Pass
  8 Pass
  9 Pass

root@localhost# session slot 7 processor 1
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.71 ... Open

Cisco Maintenance image

login: root
Password:

Maintenance image version: 2.1(2)

root@localhost# upgrade ftp://user@pc1//home/userdir/nam-app.3-5-0-10-Eng.bin.gz
Downloading the image. This may take several minutes...
Password for pc1:
ftp://pc1//home/user/nam-app.3-5-0-10-Eng.bin.gz (74629K)
/tmp/upgrade.gz           [########################]   74629K | 10586.05K/s
76421024 bytes transferred in 7.05 sec (10585.89k/sec)

Upgrade file ftp://pc1//home/user/nam-app.3-5-0-10-Eng.bin.gz is dow
nloaded.
Upgrading will wipe out the contents on the storage media.
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.
This process may take several minutes...

Applying the image, this process may take several minutes...

Performing post install, please wait...
Application image upgrade complete. You can boot the image now.
root@localhost# exit
logout

[Connection to 127.0.0.71 closed by foreign host]
root@localhost# hw-module module 7 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 7
root@localhost#
```

Cisco IOS ソフトウェアを使用した 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# hw-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。

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# hw-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あと、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# hw-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# hw-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,  3.3(0.1)
Copyright (c) 2004 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# hw-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#
```

Cisco IOS ソフトウェアを使用した mini-RMON の設定

Cisco IOS ソフトウェアでは、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。**Setup** タブを使って、NAM Traffic Analyzer アプリケーションで mini-RMON をイネーブルにすることもできます。

(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 オペレーティング システム ソフトウェア

Catalyst オペレーティング システムソフトウェアを使用して、以下の管理作業を NAM で実行できます。

NAM Traffic Analyzer を使用して NAM を管理できます。詳細については、『*User Guide for the Network Analysis Module NAM Traffic Analyzer*』Release 3.3 を参照してください。

NAM について、次の管理作業を行うことができます。

- CLI または NAM Traffic Analyzer 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 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の詳細については、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 4-3 に、CLI および NAM Traffic Analyzer 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 4-3　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	なし	なし	**password** コマンドを使用します。	次の CatOS コマンドを使用して CLI パスワードを NAM デフォルトにリセットします。**clear module password** *slot*
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。また、CLI の **web-user** コマンドを使用して Web ユーザを作成することもできます。	**no web-user** コマンドまたは NAM Traffic Analyzer を使用してユーザを削除します。		
Traffic Analyzer ローカル データベース	あり	あり	あり	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+	あり	あり	あり	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。

Catalyst オペレーティング システム ソフトウェアを使用した 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 4-4 に、NAM のユーザ レベルとパスワードを示します。

表 4-4　NAM 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、すべての読み取り権限とすべての書き込み権限が与えられます。

アプリケーション イメージまたはメンテナンス 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** 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,  3.3(0.1)
Copyright (c) 2004 by Cisco Systems, Inc.
WARNING! Default password has not been changed!

root@localhost#
```

Catalyst オペレーティング システム ソフトウェアを使用した 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、スーパーバイザ 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 のパスワードを工場出荷時のデフォルト設定に戻すには、特権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、パスワードをリセットできます。

— 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 4-1 または 表 4-4 を参照してください。

工場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 文字以上にする必要があります。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　この新しいパスワードを再入力します。

```
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。

Catalyst オペレーティング システム ソフトウェアを使用した 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。

Cisco IOS ソフトウェアについては、「Cisco IOS ソフトウェアを使用した NAM のリセット」（p.4-4）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。次に、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。

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
```

モジュールをリセットして NAM をアプリケーション イメージで起動するには、Catalyst オペレーティング システム CLI プロンプトで **reset** *mod* **hdd:1** コマンドを実行します。

モジュールをリセットして NAM をメンテナンス イメージで起動するには、Catalyst オペレーティング システム CLI プロンプトで **reset** *mod* **cf:1** コマンドを実行します。

次に、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 ...
```

次に、モジュールをイネーブル モードからメンテナンス イメージにリセットする例を示します。

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

次に、モジュールをイネーブル モードから NAM アプリケーション イメージにリセットする例を示します。

```
Console> (enable) reset mod_num
```

次に、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ります。次に、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。

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
```

Catalyst オペレーティング システム ソフトウェアを使用した 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、「Catalyst オペレーティング システム ソフトウェアを使用した NAM アプリケーション ソフトウェアのアップグレード」（p.4-19）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、「Catalyst オペレーティング システム ソフトウェアを使用した NAM メンテナンス ソフトウェアのアップグレード」（p.4-20）を参照してください。

Catalyst オペレーティング システム ソフトウェアを使用した 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、特権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。

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。

または

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

（注）　**--install** キーワードは、すべての NAM パーティションをクリアして再作成し、工場出荷時のデフォルト設定にします。

（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あと、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 3 cf:1
This command will reset module 3.
Unsaved configuration on module 3 will be lost
Do you want to continue (y/n) [n]? y
ResetPcBlade:start shutdown module 3
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

Router-sup2# session 3
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.31 ... Open

Cisco Maintenance image

login: root
Password:

Maintenance image version: 2.1(0.7)

root@localhost# upgrade ftp://pc1/pub/rmon/nam-app.3-3-0-15.bin.gz
Downloading the image. This may take several minutes...
ftp://pc1/pub/rmon/nam-app.3-3-0-15.bin.gz (58699K)
/tmp/upgrade.gz           [########################]   58699K | 6499.18K/ss
60108348 bytes transferred in 9.03 sec (6499.05k/sec)

Upgrade file ftp://pc1/pub/rmon/nam-app.3-3-0-15.bin.gz is downloaded.
Upgrading will wipe out the contents on the storage media.
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.
This process may take several minutes...

Applying the image, this process may take several minutes...

Performing post install, please wait...
Application image upgrade complete. You can boot the image now.
root@localhost#
```

Catalyst オペレーティング システム ソフトウェアを使用した 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、特権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。

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　メンテナンス イメージで起動し、次のように入力して 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あと、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 completed.
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,  3.3(0.1)
Copyright (c) 2004 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.
```

Catalyst オペレーティング システム ソフトウェアを使用した mini-RMON の設定

Catalyst オペレーティング システム ソフトウェアを使用して、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、特権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) hw-module module module_number reset
```

Catalyst オペレーティング システム 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。

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あと、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
```

（注）　HTTP または HTTPS サーバの稼働中に NAM Traffic Analyzer の Web アプリケーションを実行している場合、GUI の **About** をクリックするとインストールされているパッチが表示されます。何も表示されない場合、インストールされているパッチはありません。

Catalyst オペレーティング システム 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 3
This command will reset module 3.
Unsaved configuration on module 3 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 3 shut down in progress, please don't remove module until shutdown completed.
Console> (enable) 2002 May 07 23:19:03 %SYS-5-MOD_OK:Module 3 is online

Router-sup2# session slot 3 processor 1
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.31 ... Open

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

login: root
Password:
Terminal type: vt100

Cisco Network Analysis Module (WS-SVC-NAM-1) Console, 3.3(0.15)
Copyright (c) 1999-2004 by cisco Systems, Inc.

WARNING! Default password has not been changed!
root@localhost# patch
ftp://guest@pc1/home/guest/patch_rpms/nam-app.3-3.cryptoK9.patch.1-0.bin

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

Downloading nam-app.3-3.cryptoK9.patch.1-0.bin. Please wait...
Password for guest@pc1:
ftp://guest@pc1/home/guest/patch_rpms/nam-app.3-3.cryptoK9.patch.1-0.bin (1K)
-                         [#########################]       1K |  114.28K/s
1891 bytes transferred in 0.02 sec (112.09k/sec)

Verifying nam-app.3-3.cryptoK9.patch.1-0.bin. Please wait...
Patch nam-app.3-3.cryptoK9.patch.1-0.bin verified.

Applying /usr/local/nam/patch/workdir/nam-app.3-3.cryptoK9.patch.1-0.bin. Please
wait...
########################################### [100%]
########################################### [100%]
```

その他の NAM ソフトウェア管理コマンド

NAM CLI で使用できる NAM コマンドについては、『*Catalyst 6500 Series and Cisco 7600 Series Network Analysis Module Command Reference*』を参照してください。

CHAPTER 5

NAM のトラブルシューティング

この章では Network Analysis Module（NAM; ネットワーク解析モジュール）のトラブルシューティングについて説明します。具体的な内容は次のとおりです。

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

NetFlow データ エクスポート

ここでは、NetFlow Data Export（NDE; NetFlow データ エクスポート）のトラブルシューティング方法について説明します。

Web アプリケーション

説明　Monitor > Hosts、Monitor > Apps、または Monitor > Conversations ページで、データが 1 回おきまたはそれ以上の間隔でしか自動更新されない。この問題の原因は、NDE ソース デバイスの実行処理にあります。NetFlow キャッシュのエントリは、一定時間非アクティブな状態が続いたり接続の終了が検出された場合、または有効時間が過ぎた場合は無効になります。無効になったフローは出力先にエクスポートされます。エージング タイムが NAM の更新間隔よりも長い場合、NAM の更新間隔内でフローや NetFlow のパケット フローが無効になることはありません。

推奨処置　この問題を解決するには、Setup > Preferences メニューで自動更新間隔を長くするか、NetFlow エントリのエージング タイムを変更します。NDE ソース デバイスのエージング タイムを変更する場合は、まずパフォーマンスに関する NDE の使用上の注意事項を参照してください。

Cisco IOS ソフトウェア

Multilayer Switch Feature Card（MSFC; マルチレイヤ スイッチ フィーチャ カード）やルータに次のコマンドを使用してエージング タイムを指定します。

```
Router(config)# ip flow-cache timeout "active"||"inactive" seconds
Router(config)# mls aging "fast time" | "long" | "normal" seconds
```

Catalyst オペレーティング システム ソフトウェア

Policy Feature Card（PFC; ポリシー フィーチャ カード）で次のコマンドを使用してエージング タイムを指定します。

```
Console(enable) set mls agingtime [long-duration | fast | ip]
```

アクティブな時間が長いフローにエージング タイムを設定するには、**long-duration** キーワードを使用します。

パケットのしきい値を超えないフローにエージング タイムを設定するには、**fast** キーワードを使用します。

IP フローにエージング タイムを設定するには、**ip** キーワードを使用します。

説明　Monitor > Hosts ページおよび Monitor > Conversations ページにアクティブなフロー データが含まれていない。この問題は、アクティブなフローの有効期限が切れていないために生じた可能性があります。またはデバイスに NDE フィルタが設定されているか、フル キャッシュ状態にあるため新しいエントリが追加できない可能性があります。NAM にエクスポートする NetFlow パケットにアクティブなフローがありません。

推奨処置　フィルタの持続エージング タイムが長すぎないか、またはフロー パケットがドロップしていないかを確認します。具体的な方法は次のとおりです。

次のコマンドを使用して持続エージング タイムを確認します。

```
Console(enable) show ip cache flow
```

または

```
Console(enable) show mls netflow aging
```

または

```
Console(enable) show mls
```

持続エージング タイムが長く設定されているアクティブ タイムのアクティブ フローの有効期限が切れておらず、NAM にエクスポートされていません。エージング タイムの値を小さくします。デバイスに関する情報は、NDE の使用上の注意事項を参照してください。

次のコマンドを使用して、フロー パケットがドロップしていないかどうかを確認します。

```
Console(enable) show ip cache flow
```

または

```
Console(enable) show mls netflow aging
```

または

```
Console(enable) show mls
```

フローは期限が切れた時点でキャッシュに入って NAM にエクスポートできる状態でなければドロップする可能性があります。ネットワークがビジー状態にあり NetFlow キャッシュがフルになっていることもあります。問題を解決するには、キャッシュ サイズを大きくするか、NDE フロー マスクまたはバージョン 8 集計キャッシュを使用して NDE エクスポートを調節します。デバイスに関する情報は、NDE の使用上の注意事項を参照してください。

説明　デバイスのデフォルトの NetFlow データ ソースにデータがない。

推奨処置　GUI（グラフィカル ユーザ インターフェイス）で、Setup > Data Sources > NetFlow > Listening Mode ページに移動し、**Start** をクリックします。数回自動更新されるのを待ちます。表にデバイスが表示されていない場合、NAM はデバイスから NetFlow パケットを受信していません。ネットワークに問題があるか、デバイスが正しく設定されていません。

NAM の UDP ポート 3000 に NetFlow パケットを送信するように NetFlow デバイスが設定されているかどうかを確認するには、次のコマンドを使用します。

```
Console> show ip flow export
```

または

```
Console> show mls nde
```

NetFlow エクスポートがイネーブルかどうか表示され、NetFlow パケットがエクスポートされている IP アドレスとポートが表示されます。表示された内容が正しくない場合、『*User Guide for the Network Analysis Module Traffic Analyzer*』Release 3.3 で設定の項目を確認し、正しく設定します。

説明　特定のインターフェイスに設定した NetFlow データ ソースにデータがない。ただし、デバイスのデフォルトの NetFlow データ ソースにはデータがある。

推奨処置　指定したインターフェイスの情報を持つ NetFlow レコードがないために、この問題が発生している可能性があります。NetFlow レコードのインターフェイスを確認するには、次の手順を実行します。

ステップ 1　Setup > Data Sources > NetFlow > Listening Mode 画面に移動します。

ステップ 2　**Start** をクリックし、リスニング プロセスを開始します。

ステップ 3　デバイスの列の NDE パケットが 4 つ以上になるまで待ちます。

ステップ 4　デバイスを選択します。

ステップ 5　**Details** をクリックします。ウィンドウが開き、NAM が NDE パケットで確認するインターフェイスのリストが表示されます。

ステップ 6　NetFlow　デバイスで選択したインターフェイスがリストに含まれていることを確認します。インターフェイスがリストに含まれていない場合、次のコマンドを使用して NetFlow ソース デバイスを設定します。

IP ルーティングされたキャッシュの場合、次のコマンドを使用します。

```
Console(config) interface type slot/port
Console(config-if) ip route cache flow
```

MLS キャッシュの場合、Cisco IOS ソフトウェアの次のコマンドを使用します。

```
Console(config)# mls nde interface
```

MLS キャッシュの場合、Catalyst オペレーティング システム ソフトウェアの次のコマンドを使用します。

```
Console>(enable) set mls nde destination-ifindex enable
```

または

```
Console(enable) set mls nde source-ifindex enable
```

フロー マスクの設定が full、interface-destination-source または interface-full であることを確認します。

表示された内容が正しくない場合、『*User Guide for the Network Analysis Module Traffic Analyzer*』Release 3.3 で設定の項目を確認し、正しく設定します。

説明　Setup > Data Sources > NetFlow > Custom Data Sources 画面で NetFlow データ ソースを作成しても、ドロップダウン ボックスにはローカル デバイスのアドレスしか表示されない。

推奨処置　デバイスは Setup > Data Sources > NetFlow > Devices 画面で作成されます。この画面でデバイスを追加すると、このデバイスのデフォルトの NetFlow データ ソースが Setup > Data Sources > Netflow > Custom Data Sources 画面に表示されます。また、ドロップダウン ボックスのリストにもデバイスのアドレスが表示されます。

説明　NetFlow データ ソースを作成しても、使用できるインターフェイスのリストが表示されない。

コミュニティ ストリングが正しいことを確認するには、次の手順を実行します。

ステップ 1　Setup > Data Sources > NetFlow > Devices メニューに移動します。

ステップ 2　デバイスのラジオ ボタンをクリックし、インターフェイスに関する情報を表示します。

ステップ 3　**Test** をクリックします。

デバイスの状態を表示するポップアップ ウィンドウが開きます。このウィンドウでエラーが表示されると、コミュニティ ストリングが正しくない可能性があります。コミュニティ ストリングを訂正してください。具体的には、デバイスを選択し **Edit** をクリックして、正しいコミュニティ ストリングを指定します。また、リモート デバイスが SNMP（簡易ネットワーク管理プロトコル）接続を受け付けることを確認します。

説明　Monitor > Conversations の順に選択して表示されるページのソース カラムのエントリが、すべて 0.0.0.0 になっている。この問題は、NDE デバイスのフロー マスクが destination に設定されていると発生します。

Cisco IOS ソフトウェア

Cisco IOS ソフトウェアを使用して、フロー マスクを full、interface-destination-source または interface-full に設定する場合は、次のコマンドを入力します。

```
Router(config)# mls flow ip
"full"|"interface-destination-source"|"interface-full"
```

Catalyst オペレーティング システム ソフトウェア

Catalyst オペレーティング システム ソフトウェアを使用して、フロー マスクを full、interface-destination-source または interface-full に設定する場合は、次のコマンドを入力します。

```
Console(enable)# set mls flow "destination-source" | "full"
```

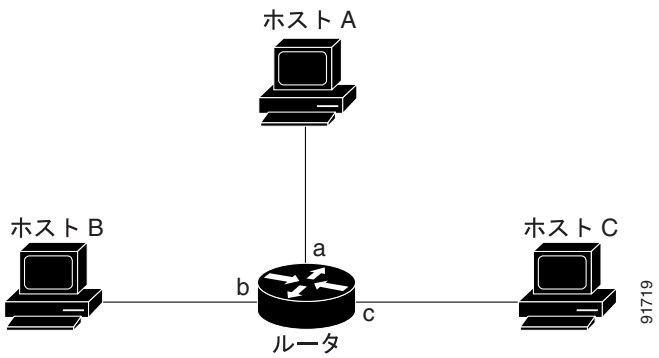
（注）　NAM は、NDE のバージョン 1、5、6、7、8、送信元プレフィクス、宛先プレフィクス、プレフィクス、プロトコルポート集計をサポートします。

NDE フロー レコードのインターフェイス

説明　1 つの NDE パケットに複数の NDE フロー レコードがある。各フロー レコードに、フロー入力 SNMP if-index フィールドとフロー出力 SNMP if-index フィールドがある。Cisco IOS や Catalyst オペレーティング システムのバージョンが NDE 機能をサポートしていない場合や NDE フロー マスクの設定が間違っている場合は、フィールドの情報が利用できない場合もあります。

図 5-1 および図 5-2 に、このような場合のネットワーク構成を示します。また表 5-1 および表 5-2 に、フロー レコードのレポートを示します。

図 5-1　NDE の構成



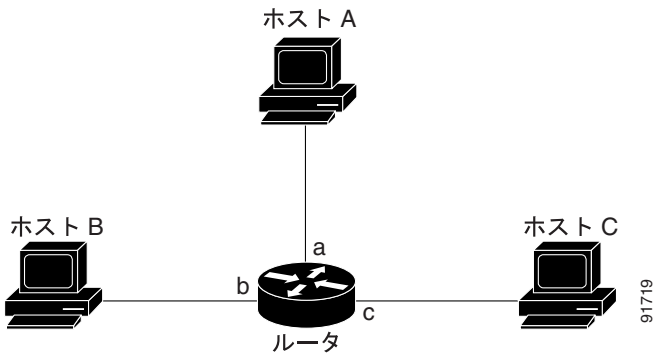
次のような構成になっています。

```
Router# configuration terminal
Router(config)# interface a
Router(config-if)# ip route cache flow
Router(config-if)# exit
Router(config)# ip flow export destination NAM-Address 3000
Router config)# exit
Router#
```

表 5-1　フロー レコードのレポート

入力インターフェイス	出力インターフェイス	フローのレポートの有無
a	b	あり
a	c	あり
b	c	なし
b	a	なし
c	a	なし
c	b	なし

図 5-2　NDE の構成




```
Router# configuration terminal
Router(config)# interface a
Router(config-if)# ip route cache flow
Router(config-if)# exit
Router(config)# interface b
Router(config-if)# ip route cache flow
Router(config-if)# exit
Router(config)# ip flow export destination NAM-Address 3000
Router(config)# exit
Router#
```

表 5-2　フロー レコードのレポート

送信元	宛先	フローのレポートの有無
a	b	あり
a	c	あり
b	c	あり
b	a	あり
c	a	なし
c	b	なし

推奨処置　ほとんどの場合、インターフェイスの NetFlow をオンにすると、スイッチまたはルータに NetFlow キャッシュが発生してフローはインターフェイスの入力方向に向かいます。その結果、フロー レコードの入力 SNMP if-index フィールドのインターフェイスは if-index となり、インターフェイスの NetFlow はオンになります。

インターフェイスの特別な（0）

説明　NDE パケットの NetFlow レコードに、入力 if-index フィールドおよび出力 if-index フィールドのどちらか一方または両方が 0 で始まるものがある。これには、次のような 1 つまたは複数の理由が考えられます。

- フローの終端がデバイスである
- デバイスの設定の問題
- デバイスのプラットフォームで NetFlow 機能がサポートされていない

推奨処置　デバイスで終端するフローを削除し、デバイスの設定をチェックし、デバイスのプラットフォームに非サポートの機能がないことを確認します。

NDE フロー マスクとバージョン 8 集計キャッシュ

ここでは、フローマスクと NDE バージョン 8 の集計フローが NAM のデータ収集画面に与える影響について説明します。具体的な影響の内容を表 5-3 に示します。情報が不足しているため、Monitor > Apps ページには「Others」とだけ表示され、Monitor > Hosts および Monitor > Conversation ページには 0.0.0.0 と表示されることがあります。

表 5-3　データ収集画面への影響

フロー	影響
フローマスクがサポートされている	強く推奨します。フル フローマスクの適用方法については、デバイスでの NDE の使用上の注意事項を参照してください。 **(注)** NAM は NDE 集計をサポートしますが、指定した集計タイプについて受信する情報は集計に限られます。他の内容については受信できません。NDE 設定についての詳細を受け取るには、フル フロー モードを指定します。
宛先専用フローマスク	• Monitor > Apps には「Others」しか表示されません。 • Monitor > Apps の詳細ウィンドウにはデータがありません。 • Monitor > Hosts が 0.0.0.0 となっています。詳細ウィンドウにはデータがありません。 • 一部のホストで Monitor > Conversations が 0.0.0.0 となっています。詳細ウィンドウにはデータがありません。 • 特定のインターフェイスに設定した NetFlow カスタム データ ソースをサポートします。
宛先/送信元フローマスク	• Monitor > Apps には「Others」しか表示されません。 • Monitor > Apps の詳細ウィンドウにはデータがありません。 • Monitor > Hosts にはデータがあります。詳細ウィンドウにはデータがありません。 • Monitor > Conversations にはデータがあります。詳細ウィンドウにはデータがありません。 • 特定のインターフェイスに設定した NetFlow カスタム データ ソースをサポートします。
NDE バージョン 8 プロトコルポート集計	• Monitor > Apps はデータを表示します。 • Monitor > Apps の詳細ウィンドウには 0.0.0.0 だけが表示されます。 • Monitor > Host には 0.0.0.0 だけが表示されます。 • Monitor > Conversation には 0.0.0.0 ～ 0.0.0.0 だけが表示されます。 • 特定のインターフェイスに設定したカスタム NetFlow データ ソースにはデータがありません。 • ToS 0 および DSCP 0 以外の DiffServ がありません。 • Setup > Data Sources > NetFlow Listening Mode 詳細ウィンドウを開いても、インターフェイスの情報が表示されません。
NDE バージョン 8 宛先プレフィクス集計	• Monitor > Apps には「Others」しか表示されません。 • Monitor > Host に表示されるデータはサブネット（0.0.0.0）です。詳細ウィンドウにはデータがありません。 • Monitor > Conversation に表示されるデータは 0.0.0.0 ～サブネット（0.0.0.0 ～ 0.0.0.0）です。詳細ウィンドウにはデータがありません。 • 特定のインターフェイスに設定した NetFlow カスタム データ ソースをサポートします。 • ToS 0 および DSCP 0 以外の DiffServ がありません。

表 5-3　データ収集画面への影響（続き）

フロー	影響
NDE バージョン 8 プレフィクス集計	• Monitor > Apps には「Others」しか表示されません。 • Monitor > Host のデータはサブネット（0.0.0.0）として表示されます。詳細ウィンドウにはデータがありません。 • Monitor > Conversation にはデータ（0.0.0.0 ～ 0.0.0.0）が表示されます。詳細ウィンドウにはデータがありません。 • 特定のインターフェイスに設定した NetFlow カスタム データ ソースをサポートします。 • ToS 0 および DSCP 0 以外の DiffServ がありません。
NDE バージョン 8 送信元プレフィクス集計	• Monitor > Apps には「Others」しか表示されません。 • Monitor > Host に表示されるデータはサブネット（0.0.0.0）です。詳細ウィンドウにはデータがありません。 • Monitor > Conversation にはサブネット～ 0.0.0.0（0.0.0.0 ～ 0.0.0.0）のデータが表示されます。詳細ウィンドウにはデータがありません。 • 特定のインターフェイスに設定した NetFlow カスタム データ ソースをサポートします。 • ToS 0 および DSCP 0 以外の DiffServ がありません。
NDE バージョン 8AS 集計	サポート対象外です。

エラー メッセージ

現象　スーパーバイザ CLI（コマンドライン インターフェイス）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　スーパーバイザ エンジンのブート 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。

推奨処置　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、スーパーバイザ エンジン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、**hw-module mod 9 reset hdd:1** コマンドを使用します。
- Catalyst オペレーティング システム 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（ファイル転送プロトコル）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。

推奨処置　パッチがシスコの正式なパッチであり、正しい NAM リリースのパッチであることを示す署名証明が使用されていることを確認します。たとえば、NAM 2.2 リリースのパッチは NAM 3.3 ソフトウェアが動作している NAM には適用できません。NAM に設定された時刻と日付の設定がスイッチに同期するのか、Network Time Protocol（NTP）に同期するのかを確認します。パッチの URL が正しいことを確認します（ユーザ名を確認）。

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。

（注）　このメッセージは WS-SVC-NAM-1 モジュールおよび WS-SVC-NAM-2 モジュールだけに適用できます。

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。

推奨処置　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。

推奨処置　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 4-1（p.4-2）または表 4-4（p.4-14）を参照してください。

現象　NAM に新しい NAM 3.3 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　指定した NAM ではこのイメージがサポートされていません。NAM 3.3 で使用できるイメージは 2 つで、WS-SVC-NAM-1 および WS-SVC-NAM-2 に 1 つずつです。このエラーは、互換性のないイメージを使用すると発生します。

推奨処置　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　WS-SVC-NAM-1 または WS-SVC-NAM-2 に間違った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。

```
ERROR: /tmp/upgrade:No space left on device
```

考えられる原因　指定した NAM ではこのイメージがサポートされていません。NAM 3.3 で使用できるイメージは 2 つで、WS-SVC-NAM-1 および WS-SVC-NAM-2 に 1 つずつです。このエラーは、互換性のないイメージを使用すると発生します。

推奨処置　従来の NAM リリースと新しい WS-SVC-NAM-1 および WS-SVC-NAM-2 では、アプリケーションおよび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 Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）セッションが表示されない。

考えられる原因　Catalyst オペレーティング システム 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 の設定はスーパーバイザ 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。

推奨処置　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。

推奨処置　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 の初回起動時に自動的に完全なメモリ テストを実行したいが、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。

推奨処置　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 ソフトウェア専用のコマンドなので、Catalyst オペレーティング システム ソフトウェアには使用できません（「Catalyst オペレーティング システム ソフトウェアを使用した NAM のリセット」（p.4-17）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。次のように入力します。

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

Catalyst オペレーティング システム 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。次に、完全なメモリ テストをイネーブルにする例を示します。

```
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
```

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定義されている 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。

推奨処置　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 倍に 1 を加えた数字です。たとえば、NAM がモジュール 4 であれば、アドレスは 127.0.0.41 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　Catalyst オペレーティング システム 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（仮想 LAN）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。

推奨処置　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。

推奨処置　「NAM の設定」（p.3-1）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。

推奨処置　「HTTP サーバまたは HTTP セキュア サーバの設定」（p.3-13）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。

推奨処置　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。

推奨処置　「HTTP セキュア サーバの設定」（p.3-14）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+ 秘密鍵がサーバに設定されている秘密鍵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。

推奨処置　問題の原因を特定するには、次の手順を実行します。

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。

推奨処置　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+ 秘密鍵が、TACACS+ サーバに設定されている鍵と一致していません。

推奨処置　**Admin > User > TACACS+** を選択し、正しい秘密鍵を入力します。

```
...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。

推奨処置　**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。

推奨処置　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）。

現象　**configure network** コマンドを使って設定をインポートするとコンフィギュレーション ファイルは正しくダウンロードされるが、インポートは失敗してエラー メッセージが表示される。

考えられる原因　コンフィギュレーション ファイルが正しくありません。

推奨処置　**show log config** コマンドを使うと、どの設定が間違っているかを調べることができます。コンフィギュレーション ファイルを無視するか修正し、**config network** コマンドを再入力します。

現象　NAM-1 または NAM-2 のアプリケーション イメージをメンテナンス イメージにアップグレードしようとすると、次のメッセージが表示されます。

```
Image verification failed.
```

考えられる原因　アップグレードしようとしているイメージは正しいメンテナンス イメージではありません。またはこのリリースとの互換性がありません。

推奨処置　NAM-1 または NAM-2 の正しいメンテナンス イメージを使用する必要があります。WS-X6380-NAM メンテナンス イメージは使用できません。

現象　WS-X6380-NAM アプリケーション イメージをアップグレ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 イメージは NAM-1 または NAM-2 に使用できません。

推奨処置　WS-X6380-NAM の正しいメンテナンス イメージを使用する必要があります。NAM-1 または NAM-2 メンテナンス イメージは使用できません。

現象　WS-X6380-NAM メンテナンス イメージをアップグレードしようとすると、次のメッセージが表示される。

```
restore operation failed.
```

考えられる原因　アップグレード プロセスに問題がありました。

推奨処置　WS-X6380-NAM アプリケーション イメージをロードすれば、この問題は解決できます。

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 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 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。

  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。

```
web-user
user name name
exit
```

ステップ 3　プロンプトに新しいパスワードを入力します。

ステップ 4　**Y** を入力して新しいパスワードを確認します。

NAM TACACS+ の設定が間違っており、Web インターフェイスでローカル データベース ユーザ アカウントを使用してもこの問題が解決できない場合は、CI インターフェイスを使用して TACACS+ の設定を訂正します。

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。

```
ip http tacacs+ enable tacacs+ server
```

ステップ 3　コマンドに続けて TACACS+ 秘密鍵を入力します。

サポート対象の MIB オブジェクト

表 5-4 に、スーパーバイザ エンジンおよび NAM がサポートする Remote Monitoring（RMON）および RMON2 の MIB（管理情報ベース）オブジェクトを示します。スーパーバイザ エンジンには、表 5-4 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。スーパーバイザ 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 ではなくスーパーバイザ 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。

スーパーバイザ エンジン上で設定された alarmVariable は、スーパーバイザ 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）　スーパーバイザ 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ーバイザ エンジンに alarmVariable を設定することもできません。

表 5-4　スーパーバイザ 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 ID）および説明	ソース
スーパーバイザ 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 2819（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	
スーパーバイザ 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 2819（RMON-MIB） RFC 2819（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	

表 5-4　スーパーバイザ 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 ID）および説明	ソース
スーパーバイザ エンジン	...mib-2(1).rmon(16).alarm(3)	RFC 2819（RMON-MIB）
	ネットワーク管理目的で、重要な RMON 変数に設定できるしきい値	
ネットワーク解析	...mib-2(1).rmon(16).alarm(3)	RFC 2819（RMON-MIB）
	ネットワーク管理目的で、重要な RMON 変数に設定できるしきい値	
ネットワーク解析	...mib-2(1).rmon(16).hosts(4)	RFC 2819（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 2819（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）	
ネットワーク解析	...mib-2(1).rmon(16).statistics(1).etherStatsTable(1)	RFC 2819（RMON-MIB）
ネットワーク解析	...mib-2(1).rmon(16).matrix(6)	RFC 2819（RMON-MIB）
	ネットワーク上のホスト間の会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 2819（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 2819（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	
スーパーバイザ エンジン	...mib-2(1).rmon(16).event(9)	RFC 2819（RMON-MIB）
	Alarm グループのしきい値を超えたときに 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 2819（RMON-MIB）
	Alarm グループのしきい値を超えたときに SNMP トラップを生成してイベントを記録	
スーパーバイザ 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	

表 5-4　スーパーバイザ 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 ID）および説明	ソース
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	
スーパーバイザ 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)	RFC 3273（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	

表 5-4　スーパーバイザ 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 ID）および説明	ソース
	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)	RFC 3287（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)	RFC 3287（DSMON-MIB）
	データソース別の統計収集テーブル	
	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)	RFC 3287（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)	RFC 3287（DSMON-MIB）
	ホスト別の統計収集テーブル	
	rmon.dsmonMib(26).dsmonObjects(1).dsmonCapsObjects(5). dsmonCapabilities(1)	RFC 3287（DSMON-MIB）
	DSMON 機能変数	

表 5-4　スーパーバイザ 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 ID）および説明	ソース
	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)	RFC 3287（DSMON-MIB）
	マトリクス統計収集テーブル	

NAM ifTable のローカル インターフェイス

ここでは、新しい NAM-1 および NAM-2 と旧バージョンの WS-X6380-NAM との違いを説明します。NAM には次の 3 つのバージョンがあります。

- WS-X6380-NAM
- WS-SVC-NAM-1
- WS-SVC-NAM-2

WS-X6380-NAM は、スーパーバイザ エンジン CLI および ifTable で 2 つのポートとして認識されます。最初のポートはデータ ポートで、SPAN トラフィックの受信に使用されます。2 つめのポートは管理ポートです。NAM では、この 2 つのポートが ifTable で最初の 2 つのポートとして認識されます。データ ポートは ifIndex.1、管理ポートは ifIndex.2 です。

WS-SVC-NAM-1 は、スーパーバイザ エンジン CLI（Catalyst オペレーティング システムの場合）および ifTable で 3 つのポートとして認識されます。最初のポートは未使用です。2 つめのポートは管理ポートです。3 つめのポートはデータ ポートで、SPAN トラフィックを受信します。スーパーバイザ エンジン CLI（Cisco IOS ソフトウェアの場合）は、ポートを（“analysis module .. .”）に解析します。NAM の ifTable では、管理ポートは最初のポート（ifIndex.1）、データ ポートは 2 つめのポート（ifIndex.2）として認識されます。

WS-SVC-NAM-2 は、スーパーバイザ エンジン CLI（Catalyst オペレーティング システムの場合）および ifTable で 8 つのポートとして認識されます。ポート 1、3、4、5 および 6 は未使用です。ポート 2 は、WS-SVC-NAM-1 と同じく管理ポートです。ポート 7 と 8 はどちらもデータ ポートで、SPAN を受信します。スーパーバイザ エンジン CLI（Cisco IOS ソフトウェアの場合）は、ポートを（“analysis module .. .”）に解析します。NAM の ifTable のインターフェイスは次のとおりです。

- ifIndex.1：管理ポートに指定
- ifIndex.2：両方のデータ ポートからのトラフィックを表す（[All SPAN] ともいう）
- ifIndex.3：最初のデータ ポートからのトラフィックを表す（[data port 1] という）
- ifIndex.4：2 つめのデータ ポートからのトラフィックを表す（[data port 2] という）

（注） WS-SVC-NAM-1 および WS-SVC-NAM-2 のデータ ポートは IEEE 802.1Q トランク ポートです。受信するパケットのヘッダーは 802.1Q で（ネイティブ VLAN ID のポートのパケットを除く）、パケットのオフセット（たとえば IP ヘッダーのフィルタ）に影響します。

表 5-5 に NAM のローカル インターフェイスの宛先を示します。

表 5-5　NAM ローカル インターフェイスの宛先

	WS-X6380-NAM	WS-SVC-NAM-1	WS-SVC-NAM-2
SNMP OID	cisco.5.1. 3. 3.3.2.223	cisco.5.1. 3. 3.3.2.914	cisco.5.1. 3. 3.3.2.291
スーパーバイザ エンジンのポート数	2	3	8
スーパーバイザ エンジンの管理ポート	2	2	2
スーパーバイザ エンジンのデータ ポート	1	3	7、8
NAM の管理ポート	ifIndex.2	ifIndex.1	ifIndex.1
NAM のデータ ポート	ifIndex.1	ifIndex.2	ifIndex.2、ifIndex.3、ifIndex.4

INDEX

し

せ

そ

た

て

と

は

ほ

ま

め

も

ゆ