Cisco Nexus 7000 シリーズ NX-OS CLI 管理ベスト プラクティス ガイド

Cisco Nexus 7000 Series NX-OS CLI Management Best Practices Guide

2011 年 2 月

Text Part Number: OL-24154-01-J

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコシステムズ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。
あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

Cisco Nexus 7000 シリーズ NX-OS CLI 管理ベスト プラクティス ガイド

CONTENTS

はじめに

ここでは、『*Cisco Nexus 7000 シリーズ NX-OS CLI 管理ベスト プラクティス ガイド*』の対象読者、構成、および表記法について説明します。また、関連マニュアルの入手方法についても説明します。

この章で説明する内容は、次のとおりです。

対象読者

このマニュアルは、Cisco NX-OS デバイスの設定および維持に携わる、十分な経験を持つネットワーク管理者を対象としています。

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	説明
第 1 章 「概要」	このマニュアルの目的を説明します。
第 2 章 「初期設定」	Cisco Nexus 7000 シリーズ スイッチの電源を初めて入れたときに通常設定する Cisco NX-OS のベスト プラクティスについて説明します。
第 3 章 「管理ネットワークへの接続とセキュア アクセス」	Cisco Nexus 7000 シリーズ スイッチを管理ネットワークに接続し、CLI へのアクセスをセキュリティで保護するときの Cisco NX-OS 推奨ベスト プラクティスについて説明します。
第 4 章 「CPU の保護」	Denial of Service（DoS; サービス拒絶）攻撃から CPU を保護するための推奨ベスト プラクティスについて説明します。

章	説明
第 5 章 「統合侵入検知セキュリティ」	Cisco NX-OS ソフトウェアで有効になっている 2 種類の侵入検知システム パケット チェックについて説明します。
第 6 章 「Cisco NX-OS ソフトウェアのアップグレードまたはダウングレード」	Cisco NX-OS システム ソフトウェアをアップグレードまたはダウングレードするときの Cisco NX-OS ベスト プラクティスについて説明します。
第 7 章 「EPLD ソフトウェアのアップグレードまたはダウングレード」	Electronic Programmable Logic Device（EPLD）をアップグレードまたはダウングレードするときの推奨手順について説明します。
第 8 章 「機能の有効化と無効化」	ソフトウェア機能を有効および無効にする処理について説明します。
第 9 章 「IP 管理」	IP 管理プロトコルを設定するときの Cisco NX-OS 推奨ベスト プラクティスについて説明します。
第 10 章 「使いやすくするための管理ツール」	デバイスを管理するための Cisco NX-OS の推奨機能について説明します。
第 11 章 「ハードウェアの診断の確認とロギング」	ハードウェアの障害を管理およびトラブルシューティングするときの Cisco NX-OS の推奨機能と手順について説明します。
第 12 章 「ハードウェア リソース使用率の管理」	CPU、メモリ、I/O モジュール TCAM テーブルの各使用率など、ハードウェア リソースを管理するときの Cisco NX-OS の推奨手順について説明します。
第 13 章 「Cisco TAC に送信するデータの収集」	TAC ケースに添付する必要があるトラブルシューティング情報を収集するときの推奨手順について説明します。

表記法

コマンドの説明では、次の表記法を使用しています。

表記法	説明
太字	コマンド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。
{ }	波カッコの中の要素は、必須です。
[ ]	角カッコの中の要素は、省略可能です。
[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。
string	引用符を付けない一組の文字。string 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 string とみなされます。

出力例では、次の表記法を使用しています。

screen フォント	スイッチ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。
< >	パスワードのように出力されない文字は、山カッコ（<>）で囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

このマニュアルでは、次の表記法を使用しています。

（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。

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。

関連資料

Cisco NX-OS には、次の資料が含まれます。

リリース ノート

『Cisco Nexus 7000 Series NX-OS Release Notes, Release 4.1』

NX-OS コンフィギュレーション ガイド

『*Cisco Nexus 7000 Series NX-OS Getting Started with Virtual Device Contexts, Release 4.1*』

『*Cisco Nexus 7000 Series OTV Quick Start Guide*』

『*Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide, Release 4.1*』

『*Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 4.1*』

『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide, Release 4.1*』

『*Cisco Nexus 7000 Series NX-OS Quality of Service Configuration Guide, Release 4.1*』

『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 4.1*』

『*Cisco Nexus 7000 Series NX-OS Multicast Routing Configuration Guide, Release 4.1*』

『*Cisco Nexus 7000 Series NX-OS MPLS Configuration Guide, Release 5.x*』

『*Cisco Nexus 7000 Series NX-OS Security Configuration Guide, Release 4.1*』
『*Cisco Nexus 7000 Series NX-OS OTV Configuration Guide*』
『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.1*』
『*Cisco Nexus 7000 Series NX-OS FabricPath Configuration Guide*』
『*Cisco Nexus 7000 Series NX-OS Software Upgrade and Downgrade Guide, Release 4.1*』
『*Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 4.1*』
『*Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide, Release 4.1*』
『*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 4.1*』
『*Cisco NX-OS FCoE Configuration Guide*』
『*Configuring the Cisco Nexus 2000 Series Fabric Extender*』
『*Cisco Nexus 7000 Series NX-OS XML Management Interface User Guide, Release 4.1*』
『*Cisco MDS 9000 Family and Nexus 7000 Series NX-OS System Messages Reference, Release 4.1*』
『*Cisco Nexus 7000 Series NX-OS MIB Quick Reference*』

NX-OS コマンド リファレンス

『*Cisco Nexus 7000 Series NX-OS Command Reference Master Index, Release 4.1*』
『*Cisco Nexus 7000 Series NX-OS Fundamentals Command Reference, Release 4.1*』
『*Cisco Nexus 7000 Series NX-OS Interfaces Command Reference, Release 4.1*』
『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, Release 4.1*』
『*Cisco Nexus 7000 Series NX-OS Quality of Service Command Reference, Release 4.1*』
『*Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference, Release 4.1*』
『*Cisco Nexus 7000 Series NX-OS Multicast Routing Command Reference, Release 4.1*』
『*Cisco Nexus 7000 Series NX-OS MPLS Command Reference*』
『*Cisco Nexus 7000 Series NX-OS Security Command Reference, Release 4.1*』
『*Cisco Nexus 7000 Series NX-OS OTV Command Reference*』
『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Command Reference, Release 4.1*』
『*Cisco Nexus 7000 Series NX-OS FabricPath Command Reference*』
『*Cisco Nexus 7000 Series NX-OS System Management Command Reference, Release 4.1*』
『*Cisco NX-OS FCoE Command Reference*』

その他のソフトウェアのマニュアル

『*Cisco Nexus 7000 Series NX-OS Troubleshooting Guide, Release 4.x*』

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。

CHAPTER 1

概要

このマニュアルには、Cisco NX-OS Command-Line Interface（CLI; コマンドライン インターフェイス）を使用して Cisco Nexus 7000 シリーズ スイッチを管理するときの推奨ベスト プラクティスのクイック リファレンスが用意されています。また、実稼動ネットワークに展開されている最も一般的なプロトコルと機能に関する設定のベスト プラクティスと手順上の推奨事項についても説明します。このマニュアルは、cisco.com で参照できる Cisco Nexus 7000 シリーズ スイッチの製品マニュアルを補足することを目的としています。このため、その製品マニュアルの代わりとしてこのマニュアルを使用しないようにしてください。

このマニュアルは、プロトコルと機能が相互に関連しているときに系統立てて明確に理解できるように機能別の章に分かれています。推奨ベスト プラクティスは、同時に、または特定の順序で実装する必要がないことを理解することが重要です。ネットワーク環境によっては、適合しない推奨ベスト プラクティスもあります。

CHAPTER 2

初期設定

この章では、Cisco Nexus 7000 シリーズ スイッチの電源を初めて入れ、ユーザが、アクティブなスーパーバイザ モジュールの RS-232 コンソール ポートに接続したときに通常設定する Cisco NX-OS のベスト プラクティスについて説明します。

この章で説明する内容は、次のとおりです。

セットアップ ユーティリティ（初回セットアップ）

導入：Cisco NX-OS Release 4.0(1)

セットアップ ユーティリティは、Cisco Nexus 7000 シャーシの電源を初めて入れたとき、または **write erase** コマンドを実行して設定を消去し、シャーシをリロードした場合に自動的に実行されます（セットアップ ユーティリティは、**setup** Exec コマンドを使用して手動でいつでも実行できます）。セットアップ ユーティリティは、いくつかの初期設定パラメータを提供して管理者を補助することを目的に用意されています。ただし、必須ではなく、管理者の判断によって使用しないことを選択できます。次の表に、セットアップ ユーティリティを使用して設定できるパラメータを示します。セットアップ ユーティリティを使用しない場合は、「デフォルト値」列の値は自動的に設定されます。初期起動パラメータは、必須です。

表 2-1　　必須の初期起動パラメータ

初期起動パラメータ（必須）	デフォルト値
Enforce Secure Password Standard	yes
Admin Password	デフォルトなし

表 2-2　任意の起動ユーティリティ

起動ユーティリティ（任意）	デフォルト値
Create another login account	no
Configure read-only SNMP community string	no
Configure read-write SNMP community string	no
Enter switch name	デフォルトなし
Enable License Grace Period	no
Out-of-band (mgmt0) management configuration	yes
Mgmt0 IPV4 address	デフォルトなし
Mgmt0 IPv4 netmask	デフォルトなし
Configure the default gateway	yes
IPv4 address of the default gateway	デフォルトなし
Configure advanced IP options	no
Enable Telnet service	no
Enable SSH service	yes
Type of SSH Key (dsa/rsa)	RSA
Number of RSA Key bits	1024
Configure the NTP server	no
Configure the Default Interface Layer (L3/L2)	L3
Configure the default switchport interface state (shut/no shut)	shutdown
Configure best practices CoPP profile (strict/moderate/lenient/none)	strict
Configure CMP processor on current sup (Slot 5)	yes
CMP IPv4 address	デフォルトなし
IPv4 address of the default gateway	デフォルトなし
Configure CMP processor on current sup (Slot 6)	yes
CMP IPv4 address	デフォルトなし
IPv4 address of the default gateway	デフォルトなし

グローバル コンフィギュレーション パラメータ

この項では、一般的なシステム管理に関するグローバル パラメータを設定するときの Cisco NX-OS 推奨ベスト プラクティスについて説明します。

ターミナル CLI アクセス（SSHv2）

導入：Cisco NX-OS Release 4.0(1)

Cisco NX-OS ソフトウェアは、リモート ターミナルからの CLI アクセスに対して SSHv2 と Telnet をサポートしています。SSHv2 はデフォルトで有効になっており、暗号化によってセキュリティが強化されるので使用することを推奨します。ISSHv2 が無効になっている場合、**feature ssh** コマンドで有効にできます（SSHv2 が有効な場合、**feature ssh** コマンドは running-configuration に表示されません）。SSHv2 はデフォルトで 1024 ビットの RSA キーを使用します。**ssh key** コマンドを使用して、新しいまたはより強固な RSA/DSA キーを作成できます。キーがすでに設定されている場合、**force** オプションを使用して既存のキーを上書きできます。

```
n7000(config)# feature ssh
n7000(config)# ssh key rsa 2048
```

（注）　Cisco NX-OS Release 4.0(1) では、**service ssh** コマンドを使用して SSHv2 を有効にしていました。Cisco NX-OS Release 4.1(2) では、**feature ssh** に変更されました。

ホスト名

導入：Cisco NX-OS Release 4.0(1)

管理者が CLI にアクセスしたときに Cisco Nexus 7000 シリーズ デバイスを識別できるようにわかりやすいホスト名を設定する必要があります。Virtual Device Context（VDC; 仮想デバイス コンテキスト）を設定する場合、VDC ごとに固有のホスト名を設定する必要があります。

```
n7000(config)# hostname N7K-1-Core-L3
```

ブート変数

導入：Cisco NX-OS Release 4.0(1)

ブート変数では、システムがリロードされた後に起動する Cisco NX-OS ソフトウェアのバージョンを指定します。予定外のシャーシのリロードが発生した場合に必要なバージョンの Cisco NX-OS ソフトウェアが確実に起動するように、ブート変数を必ず設定する必要があります。Cisco Nexus 7000 シリーズ スイッチを適切に起動するには、キックスタート イメージとシステム イメージが必要です（イメージのバージョン番号が一致する必要があります）。Cisco NX-OS イメージは bootflash: または slot0: から起動できます（メモリはスーパーバイザ モジュールから取り外すことができないので、bootflash: を使用することを推奨します）。次の例では、Cisco NX-OS Release 5.1(1) のキックスタートおよびシステム ブート変数は、**sup-1** オプションと **sup-2** オプションが指定されていないので、シャーシの両方のスーパーバイザ モジュールに設定されます（デフォルトの動作）。

```
n7000(config)# boot kickstart bootflash:n7000-s1-kickstart.5.1.1.bin
n7000(config)# boot system bootflash:n7000-s1-dk9.5.1.1.bin
```

MOTD ログイン バナー

導入：Cisco NX-OS Release 4.0(1)

Message Of The Day（MOTD）ログイン バナーを使用して、ユーザがデバイスにログインしようとしていることをユーザに通知することを推奨します。このバナーは、ユーザ認証プロセスの前に表示され、権限のないユーザがログインしないようにするための警告として機能します。終了デリミタはバナーの内容に使用できません。次の例では、大文字の Z を使用しています（実稼動デバイスでは、詳細な免責事項を記載する必要があります）。

```
n7000(config)# banner motd Z
Enter TEXT message. End with the character 'Z'.
> Authorized Access Only!
> Z
n7000(config)#
```

パスワードの強度確認

導入：Cisco NX-OS Release 4.1(2)

パスワードの強度確認機能はデフォルトで有効になっているので、認証するためにローカル データベースでユーザを設定するときに安全なパスワードを設定する必要があります。パスワードの強度確認機能は有効のままにしておくことを推奨します。無効にした場合、次のグローバル コンフィギュレーション コマンドを使用して有効にできます。

```
n7000(config)# password strength-check
```

電力バジェット

導入：Cisco NX-OS Release 4.0(1)

電力バジェットは、**show environmental power** コマンドを使用してモニタリングおよび管理できます。Cisco NX-OS Release 5.0(2a) では、Cisco NX-OS Release 5.x ソフトウェアでリリースされたファン トレイとすべての I/O モジュールに関するリアルタイム消費電力が導入されました。設定した電源冗長モードにより、利用可能な電力を割り当てる方法が決まります（電源冗長モードの詳細については、次の項を参照してください）。

```
n7000# show environment power
pow_reserved 4800
Power Supply:
Voltage: 50 Volts
Power                                  Actual        Total
Supply    Model                        Output     Capacity    Status
                                      (Watts )     (Watts )
-------  -------------------  -----------  -----------  --------------
1        N7K-AC-6.0KW               786 W       6000 W     Ok
2        N7K-AC-6.0KW               830 W       6000 W     Ok
3        ------------                 0 W          0 W     Absent

                                       Actual        Power
Module    Model                         Draw    Allocated    Status
                                      (Watts )     (Watts )
-------  -------------------  -----------  -----------  --------------
3        N7K-M108X2-12L             395 W        650 W    Powered-Up
4        N7K-M108X2-12L             382 W        650 W    Powered-Up
5        N7K-SUP1                   N/A          210 W    Powered-Up
6        N7K-SUP1                   N/A          210 W    Powered-Up
```

```
Xb1      N7K-C7010-FAB-1            N/A           60 W    Powered-Up
Xb2      N7K-C7010-FAB-1            N/A           60 W    Powered-Up
Xb3      N7K-C7010-FAB-1            N/A           60 W    Powered-Up
Xb4      N7K-C7010-FAB-1            N/A           60 W    Powered-Up
Xb5      N7K-C7010-FAB-1            N/A           60 W    Powered-Up
fan1     N7K-C7010-FAN-S           116 W         720 W    Powered-Up
fan2     N7K-C7010-FAN-S           116 W         720 W    Powered-Up
fan3     N7K-C7010-FAN-F            11 W         120 W    Powered-Up
fan4     N7K-C7010-FAN-F            11 W         120 W    Powered-Up

N/A - Per module power not available

Power Usage Summary:
--------------------
Power Supply redundancy mode (configured)               Redundant
Power Supply redundancy mode (operational)              Redundant

Total Power Capacity (based on configured mode)              6000 W
Total Power of all Inputs (cumulative)                      12000 W
Total Power Output (actual draw)                             1616 W
```

電源冗長モード

導入：Cisco NX-OS Release 4.0(1)

推奨の電源冗長モードは、電源装置の数、入力の数と関連する入力電圧（110 V または 220 V）に応じて Cisco Nexus 7000 シリーズ シャーシごとに異なります。冗長モードによって電力の割り当てが異なるので、管理者は、設置環境に最適なモードを選択できます。デフォルトのモードは **ps-redundant** で、ほとんどの設置環境での推奨モードです。**combined** モードを設定するときには、シャーシに電源の冗長性は提供されないので注意が必要です。

表 2-3　電源冗長モード

冗長モード	説明
combined	このモードでは、シャーシに電源の冗長性が提供されません。すべての入力電力をシャーシに使用できます（他のモードとは異なり、電力はバックアップ用に確保されません）。
insrc-redundant	入力電源（グリッド）の冗長性：使用できる電力は、電源装置を経由する 2 つのグリッドのうち、電力の少ないグリッドに基づいて決まります。その差（50 %）がバックアップ用に確保されます。
ps-redundant	電源装置の冗長性：1 台の電源装置が故障した場合、またはシャーシから取り外された場合に追加の電源装置を提供します。
redundant	入力電源（グリッド）+ 電源装置の冗長性：使用できる電力は、電源装置モードと入力電源電圧に使用できる電力のうち、少ない方です。その差（50 %）がバックアップ用に確保されます。

```
n7000(config)# power redundancy-mode redundant
```

使用していない I/O モジュールとファブリック モジュールの電源を切る

導入：Cisco NX-OS Release 4.0(1)

使用していないすべての I/O（イーサネット）モジュールとファブリック モジュールの電源を切ることを推奨します。また、電源を入れたときに管理者が制御できるように、取り付けられていないすべての I/O モジュールとファブリック モジュールのスロットの電源を切ることを推奨します。この作業では、変更制御ウィンドウの外部で新しく取り付けたモジュールの電源が入らないようにすることで、リスクを軽減します。

```
n7000(config)# poweroff module 1
n7000(config)# poweroff xbar 4

n7000(config)# poweroff module 3
NOTICE: module <3> status is either absent or not powered up (or denied)... Proceeding
anyway
```

Cisco NX-OS のライセンス

この項では、Cisco NX-OS のライセンス モデルとインストール手順について簡単に説明します。必要なすべてのライセンスを必ずインストールして、ライセンスを受けた機能を有効にしたとき、および猶予期間が終了したときに発生する可能性がある不要なネットワークの停止を回避します。

インストール処理

導入：Cisco NX-OS Release 4.0(1)

Cisco NX-OS のライセンス モデルでは、「pay as you grow（成長に合わせた段階的な投資）」方式で機能を有効にできます。Cisco NX-OS ライセンスを購入する際、特定のシャーシにインストールされているシャーシ ホスト ID に基づいてライセンス ファイルを取得します（Cisco NX-OS ソフトウェアは、デフォルトで、基本的なレイヤ 3 機能を備えたレイヤ 2 接続に対応しています）。特定の機能に対するライセンスをお持ちでない場合は、グローバル **license grace-period** コンフィギュレーション コマンドを使用して 120 日間の猶予期間を有効にできます（猶予期間を実稼動ネットワークで使用することは推奨しません）。120 日を過ぎると、ライセンスが必要な機能を有効にしていて、そのライセンスをシャーシにインストールしていない場合、その機能は running-configuration から自動的に削除されます。

各ライセンス タイプに含まれる機能の一覧については、最新の『Cisco Nexus 7000 Series Licensing Configuration Guide』を参照してください。

2 台のスーパーバイザ モジュールをシャーシに取り付けている場合、交換したときに新しいライセンスを再発行し、再インストールする必要があるコンポーネントはシャーシだけです。スーパーバイザ モジュールを含む他のすべてのコンポーネントは、ライセンスを再発行および再インストールしなくても交換できます。スーパーバイザ モジュールを 1 台だけシャーシに取り付けている場合、そのスーパーバイザ モジュールまたはシャーシを交換したときにバックアップ コピーから新しいライセンスを再インストールする必要があります。

ライセンスは、シャーシごとにデフォルトの VDC（1）にインストールします。ライセンスのインストール中に中断は発生しません。

インストール手順の概要：

1. **show license host-id** コマンドを入力して、シャーシ ホスト ID を入手します。この ID を使用して、ライセンスを生成します。
2. Product Authorization Key（PAK; 製品認証キー）を見つけて、cisco.com の Product License Registration Web ページに移動します。
3. 手順に従って、ライセンス ファイルを生成し、ダウンロードします。
4. ライセンス ファイルを Cisco Nexus 7000 シリーズのスーパーバイザ モジュール（つまり、bootflash: または slot0:）に転送します。
5. 次の **install license** Exec コマンドを使用してライセンスをインストールします。

```
n7000# install license bootflash:license_file.lic
Installing license  ..done
```

ライセンス ステータスの確認

導入：Cisco NX-OS Release 4.0(1)

Cisco NX-OS ライセンスのステータスは、次のコマンドを使用して確認できます。

```
n7000# show license usage
Feature                      Ins  Lic   Status Expiry Date Comments
                                Count
--------------------------------------------------------------------------------
SCALABLE_SERVICES_PKG         No    -   Unused             -
TRANSPORT_SERVICES_PKG        No    -   Unused             -
LAN_ADVANCED_SERVICES_PKG     No    -   Unused             -
LAN_ENTERPRISE_SERVICES_PKG   No    -   Unused             -
--------------------------------------------------------------------------------
```

ライセンス ファイルのバックアップ

導入：Cisco NX-OS Release 4.0(1)

ライセンス ファイルは、再インストールが必要になる場合に備えて、安全な場所に常に保管する必要があります。特定のシャーシのライセンス ファイルが手元にない場合は、そのライセンスがすでにインストールされている場合はそのシャーシについてバックアップ コピーを作成できます。バックアップ ファイルを作成したら、安全な場所に転送する必要があります。

```
n7000# copy licenses bootflash:license_file.tar
Backing up license done
```

CHAPTER 3

管理ネットワークへの接続とセキュア アクセス

この章では、管理ネットワークへの Cisco Nexus 7000 シリーズ スイッチの接続および CLI へのセキュア アクセスについて、Cisco NX-OS で推奨するベスト プラクティスについて説明します。

この章で説明する内容は、次のとおりです。

アウトオブバンド管理の接続

Nexus 7000 は、通常、異なる接続方式の組み合わせを使用して管理されます。ネットワーク管理者は、CLI にアクセスし、SNMP、Syslog、NTP などの IP 管理プロトコルを使用するシャーシを管理することができます。次の表に、Nexus 7000 シャーシの管理に使用可能な異なる接続方式を示します。アウトオブバンド方式を組み合わせて使用し、実稼動トラフィックから管理トラフィックを分離して、シャーシを管理することを推奨します。このアプローチでは、悪意のあるユーザから発信されたか、不注意によって発生した過剰な購読トラフィックによる、Denial of Service（DoS; サービス拒絶）攻撃を防ぎ、セキュリティが強化されます。

スーパーバイザ モジュール CMP ポートが提供する機能について理解することが重要です。CMP ポートによって、停電時の CLI コンソール アクセスが提供され、SSHv2 または Telnet を使用して IP ネットワークを経由してスーパーバイザ モジュールにアクセスできます。CMP ポートを使用すると、管理者は、コンソールに接続し、コンソールをモニタリングし、スーパーバイザ モジュールまたはシャーシ全体をリロードできます。SNMP または NTP のような IP プロトコルのインバンド管理機能は提供されません。

表 3-1　ポート タイプおよびモジュール タイプの接続オプション

接続オプション	ポート タイプ	モジュールのタイプ
アウトオブバンド（RS-232 シリアル CLI）	コンソール ポート（推奨）	スーパーバイザ
	補助ポート	スーパーバイザ

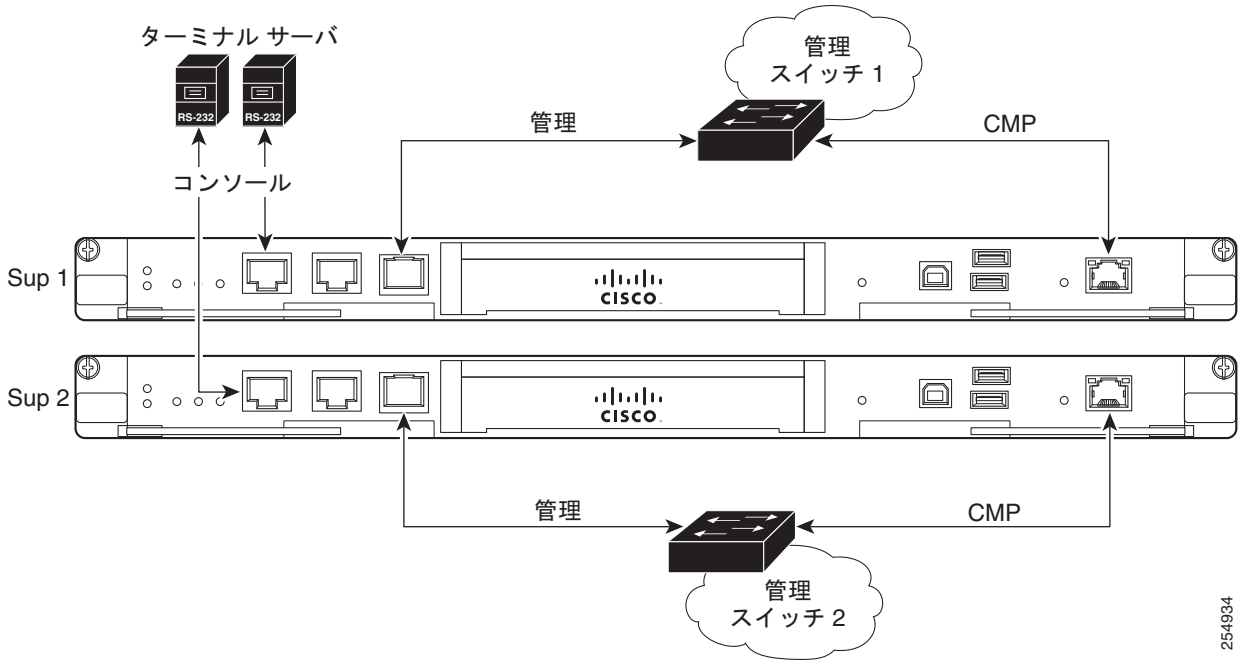
表 3-1　ポート タイプおよびモジュール タイプの接続オプション（続き）

接続オプション	ポート タイプ	モジュールのタイプ
アウトオブバンド（SSH/Telnet CLI）	Connectivity Management Port（CMP）推奨	スーパーバイザ
アウトオブバンド（SSH/Telnet CLI および IP Mgmt）	管理ポート（mgmt0）推奨	スーパーバイザ
インバンド（SSH/Telnet CLI および IP Mgmt）	イーサネット/ループバック/SVI など	I/O モジュール

2 つのスーパーバイザ モジュールで Nexus 7000 への接続を失う可能性を抑制するには、スーパーバイザ モジュールごとにコンソール ポート、CMP、および管理ポートを接続することを推奨します。

コンソールポートを 2 つの異なるターミナル サーバおよびスーパーバイザ CMP に接続し、mgmt0 ポートを冗長アウトオブバンド イーサネット ネットワークに接続して、可用性およびセキュリティを改善する必要があります。次の図に、冗長スーパーバイザ モジュールでシャーシごとに必要な接続を示します。

図 3-1　冗長スーパーバイザ モジュールでのシャーシごとの接続



（注）　このアウトオブバンド管理の設計では、イーサネット、ループバック、ポート チャネル、SVI などの I/O モジュール ポートに設定されている IP アドレスがある場合、インバンド管理プロトコルを拒否するよう、CoPP ポリシーを変更する必要があります。

（注）　これは単なる基本例です。冗長ネットワーク管理の設計は、このマニュアルに記載の範囲を超える場合があります。

コンソール ポートの設定

ここでは、コンソール ポートで Cisco NX-OS が推奨するベスト プラクティスについて説明します。

Exec-Timeout

導入：Cisco NX-OS Release 4.0(1)

コンソール ポートでは、指定された時間の間アイドル状態の管理者が自動的にログアウトするよう、タイムアウトを設定する必要があります。コンソールの **exec-timeout** は、デフォルトでディセーブルです。ほとんどのセキュリティ ポリシーでは、通常、10 ～ 15 分のタイムアウトが受け付けられます。

```
n7000(config)# line console
n7000(config-console)# exec-timeout 10
```

ポート速度

導入：Cisco NX-OS Release 4.0(1)

コンソール ポートの速度（ボー レート）は、接続されているターミナル サーバでサポートされている最大値まで増やす必要があります。コンソールの速度は、デフォルトで 9,600 bps で、最大で 115,200 bps まで設定できます。最大値によって、コンソール ポートに表示されるデータの速度が大きくなり、ユーザー エクスペリエンスが改善されます。

```
n7000(config)# line console
n7000(config-console)# speed 115200
```

VTY ポートの設定

ここでは、SSHv2 セッションおよび Telnet セッションで使用される VTY（ターミナル）ポートの設定に関する、Cisco NX-OS 推奨のベスト プラクティスについて説明します。

Exec-Timeout

導入：Cisco NX-OS Release 4.0(1)

VTY ポートでは、指定された時間の間アイドル状態のユーザが自動的にログアウトするよう、タイムアウトを設定する必要があります。VTY の **exec-timeout** は、デフォルトでディセーブルです。ほとんどのセキュリティ ポリシーでは、通常、10 ～ 15 分のタイムアウトが受け付けられます。

```
n7000(config)# line vty
n7000(config-line)# exec-timeout 10
```

セッションの制限

導入：Cisco NX-OS Release 4.0(1)

VTY セッションの限度では、SSHv2 セッションの数、Telnet セッションの数、または両方のセッションを同時にアクティブにできる数が決定されます。session-limit では、デフォルトで 32 のアクティブ セッションが認められます。セキュリティを強化するには、5 セッションまたは 10 セッションなどの実用的な制限まで削減する必要があります。

```
n7000(config)# line vty
n7000(config-line)# session-limit 5
```

アクセス リスト

導入：Cisco NX-OS 5.1(1)

セキュリティを強化するには、特定のソースおよび宛先 IP アドレスに対する SSH アクセスおよび Telnet アクセスを制限することによって、アクセス クラスを VTY ポートに適用する必要があります。VTY ポートに設定するアクセス クラスは、インバンドまたはアウトオブバンドの管理手順の使用時に適用できます。access-class はトラフィックの方向ごとに設定されます。**in** はインバンド セッションに適用され、**out** はアウトバンド セッションに適用されます。

統計は、アクセス リスト **statistics per-entry** でイネーブルにすることができます。次に、特定のサブネットから現在の VDC に設定されているすべての IP アドレスへの SSH トラフィックを許可する基本ポリシーの例を示します。すべてのトラフィックは、access-class が VTY ポートに適用され、関連付けられている access-list が設定から削除される場合に、許可されます。

```
n7000(config)# ip access-list vty-acl-in
n7000(config-acl)# permit tcp x.x.x.x/24 any eq 22

n7000(config)# line vty
n7000(config-line)# ip access-class vty-acl-in in
```

スーパーバイザ管理ポートの設定

ここでは、スーパーバイザ モジュール mgmt0 ポートで Cisco NX-OS が推奨するベスト プラクティスについて説明します。

アクセス リスト

導入：Cisco NX-OS Release 4.0(1)

セキュリティを強化するには、Nexus 7000 に設定されている特定の管理プロトコル宛ての特定のソース ホスト/サブネット アドレスへのアクセスを制限することによって、インバンド アクセス リストでスーパーバイザ モジュール mgmt0 ポートを設定する必要があります。access-list エントリは、イネーブルにされている管理ポートによって異なります。ACL コマンド **statistics per-entry** が設定されている場合、access-list 統計は ACL エントリごとに追跡できます。access-list が mgmt0 ポートに適用されるときに、スーパーバイザ モジュール CPU によって access-list の処理が実行されます。

```
n7000(config)# ip access-list mgmt0-access
n7000(config-acl)# statistics per-entry
n7000(config-acl)# permit tcp x.x.x.x/x b.b.b.b/32 eq 22
n7000(config-acl)# permit udp x.x.x.x/x b.b.b.b/32 eq snmp
n7000(config-acl)# permit tcp x.x.x.x/x b.b.b.b/32 eq tacacs
n7000(config-acl)# permit udp x.x.x.x/x b.b.b.b/32 eq ntp

n7000(config)# interface mgmt0
n7000(config-if)# ip access-group mgmt0-access in
n7000(config-if)# ip address b.b.b.b/xx
```

アクセス リスト ロギング

導入：Cisco NX-OS Release 5.0(2a)

アクセス リストは、**log** キーワードを使用して mgmt0 ポートに設定し、エントリごとに追加データを収集できます。access-list ロギング キャッシュを表示して、記録された access-list エントリから収集されるデータを監査できます。

```
n7000(config)# ip access-list mgmt0-access
n7000(config-acl)# permit tcp x.x.x.x/x b.b.b.b/32 eq 22 log

n7000# show log ip access-list cache
Source IP        Destination IP     S-Port  D-Port    Interface   Protocol          Hits
-------------------------------------------------------------------------------------
x.x.x.x          x.x.x.x             60741   22        mgmt0      (6)TCP            136

Number of cache entries: 1
-------------------------------------------------------------------------------------
```

スーパーバイザ CMP ポートの設定

ここでは、スーパーバイザ モジュール Connectivity Management Port（CMP）の設定に Cisco NX-OS が推奨するベスト プラクティスについて説明します。

アクセス リスト

導入：Cisco NX-OS Release 4.0(1)

セキュリティを強化するには、CMP ポートでイネーブルに設定されている特定の管理プロトコル宛ての特定のソース ホスト/サブネット アドレスへのアクセスを制限することによって、アクセス リストでスーパーバイザ モジュール CMP ポートを設定する必要があります。SSHv2 は、通常、CMP ポートでのみ必要なプロトコルです。**attach cmp** コマンドを使用して、access-list で CMP ポートを設定します。

```
n7000-cmp5(config)# ip access-list cmp-access
n7000-cmp5(config-acl)# permit tcp x.x.x.x 0.0.0.0 range 1024 65535 b.b.b.b 0.0.0.0 range 22 22

n7000-cmp5(config)# interface cmp-mgmt
n7000-cmp5(config-if)# ip address b.b.b.b/xx
n7000-cmp5(config-if)# ip access-group cmp-access in
```

（注）　CMP ポートの access-list の構文は、Cisco NX-OS の access-list の構文と異なります。

CHAPTER 4

CPU の保護

この章では、Denial of Service（DoS; サービス拒絶）攻撃から CPU を保護するための推奨ベスト プラクティスについて説明します。

この章で説明する内容は、次のとおりです。

CoPP ポリシー

ここでは、Control Plane Policing（CoPP）ポリシーの概略について説明します。CoPP ポリシーは、スーパーバイザ モジュール CPU に影響を及ぼすおそれがある Denial of Service（DoS; サービス拒絶）攻撃を防ぐための、重要なセキュリティ機能です。Cisco NX-OS ソフトウェアでは、最も共通の脅威から CPU を守るために開発された「strict」ポリシーが、デフォルトで適用されます。イーサネット ポート、SVI、ポート チャネルなどの I/O ポートに IP アドレスが設定されている場合には、常に、CoPP ポリシーをイネーブルにすることを推奨します。CoPP ポリシーについての詳細な説明および推奨事項は、このマニュアルの範囲外で、このマニュアルには含まれていません。

インバンド管理プロトコルの拒否

導入：Cisco NX-OS Release 4.0(1)

このマニュアルでは、CoPP ポリシーの詳細については説明していませんが、Cisco Nexus 7000 シリーズ スイッチ宛てのインバンド管理トラフィックをドロップするには、CoPP ポリシーを変更することを推奨します。すべての IP 管理トラフィックがアウトオブバンド管理ネットワークを経由する場合、IP 管理トラフィックをインバンドで受信する必要はありません。CoPP ポリシーは、mgmt0 インターフェイスで受信されるトラフィックには適用されません。

推奨手順：

1. SSHv2、SNMP、SCP、TFTP、FTP など、インバンドでドロップする必要があるトラフィックがある、イネーブルになっている管理プロトコルを特定します。
2. 新しいアクセス コントロール リストおよび新しいクラス マップを作成するか、または、既存のアクセス コントロール リストを参照する **class-map type control-plane match-any copp-system-class-management** コマンドで、既存のクラス マップを参照します。
3. 既存の CoPP サービス ポリシー（copp-system-policy）で、新しいクラス マップを挿入するか、または、手順 2 で特定された既存のクラス マップを変更し、次に、ポリシーに準拠するすべてのトラフィックをドロップするよう設定します。

次に、既存の **copp-system-class-management** クラス マップおよび関連付けられている ACL を使用する例を示します。ポリシーに準拠するトラフィックが積極的にドロップされるよう、ポリシー レートが変更されました。

```
n7000(config)# policy-map type control-plane copp-system-policy
n7000(config-pmap)# class copp-system-class-management
n7000(config-pmap-c)# police 1 conform drop
```

（注）　Cisco NX-OS Release 5.1(1) から、デフォルトの **copp-system-class-management** クラス マップには、FTP、NTP、NTP6、RADIUS、SFTP、SNMP、SSH、SSH6、TACACS、Telnet、TFTP、TFTP6、RADIUS、TACACS6、および Telnet6 の各プロトコルが含まれます。

Syslog メッセージのしきい値

導入：Cisco NX-OS Release 5.1(1)

Syslog メッセージのしきい値は、コントロール プレーンのポリシー マップで、CoPP クラス マップごとに設定できます。CoPP ポリシーがトラフィックをドロップしていることを、適切な人員に通知する方式として、クラス マップの Syslog メッセージのしきい値を設定することを推奨します。次に、クラスが Critical（ルーティング プロトコル）以内のパケットのドロップが記録されるよう、重大度レベル 5 で 39,600 Kb/s にしきい値を設定する例を示します。

```
n7000(config)# policy-map type control-plane copp-system-policy
n7000(config-pmap)# class copp-system-class-critical
n7000(config-pmap-c)# logging drop threshold 39600000 level 5
```

Syslog メッセージの例：

```
n7000# show log logfile

%COPP-5-COPP_DROPS5: CoPP drops exceed threshold in class: copp-system-class-critical,
check show policy-map interface control-plane for more info.
```

CPU レート制限のロギング

導入：Cisco NX-OS Release 5.1(1)

この項は、参考のために記載しており、必要のない場合があります。

スーパーバイザ モジュール CPU へ、または、スーパーバイザ モジュール CPU から、送信されるパケットが、設定された packet per second（pps）のしきい値を超過した場合、グローバルに、および、インターフェイスごとに、レート制限を設定し、システム ログ メッセージを作成できます。レート リミッタを設定し、**input**（受信）オプション、**output**（送信）オプション、または **both**（送受信を同時に設定）オプションを使用して、方向に基づいてトラフィックを測定できます。**both** に設定されるグローバルなデフォルトしきい値は 10,000 pps です。しきい値は、0 ～ 100,000 pps の値に変更できます。この機能は、グローバルに、および、インターフェイスごとに、設定できます。この機能では、パケットはドロップされず、通知ログ メッセージが送信されるだけです。

グローバルに設定：

```
n7000(config)# rate-limit cpu direction both pps 2000 action log
```

インターフェイスごとに設定：

```
n7000(config)# interface ethernet 1/26
```

```
n7000(config-if)# rate-limit cpu direction both pps 2000 action log
```

確認：

グローバルに確認：

```
n7000# show system internal pktmgr internal control sw-rate-limit
inband pps global threshold 2000  outband pps global threshold 2000
```

インターフェイスごとの確認：

```
n7000# show system internal pktmgr interface ethernet 1/26
Ethernet1/26, ordinal: 305
  SUP-traffic statistics: (sent/received)
    Packets: 5412033 / 6677105
    Bytes: 1614312187 / 2003104556
    Instant packet rate: 2872 pps / 2871 pps
    Packet rate limiter (Out/In): 2000 pps / 2000 pps
    Average packet rates(1min/5min/15min/EWMA):
    Packet statistics:
      Tx: Unicast 5365387, Multicast 46640
          Broadcast 6
      Rx: Unicast 6677093, Multicast 0
          Broadcast 12
```

Syslog：

```
n7000# show log logfile

%NETSTACK-5-NOTICE:  netstack [3647]  Ingress PPS (2861) exceeding threshold on i/f
Ethernet1/26
```

CHAPTER 5

統合侵入検知セキュリティ

Cisco NX-OS ソフトウェアは、IPv4 と IPv6 の侵入検知パケット チェックによって特定の条件に一致し、ほとんどの実稼動ネットワークでは通常必要のないパケットをドロップして、ネットワークのセキュリティを強化します。デフォルトでは、ほとんどの Intrusion Detection System（IDS; 侵入検知システム）パケット チェックが有効になっています。このチェックを無効にする明確な理由がない限り、有効にしておく必要があります。

この章で説明する内容は、次のとおりです。

IDS チェックのステータスとカウンタの確認

導入：Cisco NX-OS Release 4.0(1)

show hardware forwarding ip verify コマンドを使用して、IDS パケット チェックのステータスとカウンタを確認する必要があります。「Packets Failed」カウンタでは、パケットが IDS チェックに当てはまったかどうかを確認できます。この出力は、ネットワーク トラフィックを確認するとき、アプリケーションの問題をトラブルシューティングするときに役立ちます。場合によっては、IDS パケット チェックを無効にする必要があります。Cisco NX-OS Release 5.0(3) では、パケットがドロップされたときの Syslog メッセージと Embedded Event Manager（EEM）イベント トリガーのサポートが導入されました。

```
n7000# show hardware forwarding ip verify

IPv4 and v6 IDS Checks          Status     Packets Failed
-----------------------------+---------+------------------
address source broadcast        Enabled    0
address source multicast        Enabled    0
address destination zero        Enabled    0
address identical               Enabled    0
address reserved                Enabled    0
address class-e                 Disabled   --
checksum                        Enabled    0
protocol                        Enabled    0
fragment                        Disabled   --
length minimum                  Enabled    0
length consistent               Enabled    0
length maximum max-frag         Enabled    0
length maximum udp              Disabled   --
length maximum max-tcp          Enabled    0
tcp flags                       Disabled   --
tcp tiny-frag                   Enabled    0
```

```
version                          Enabled    0
------------------------------+---------+------------------
IPv6 IDS Checks                  Status     Packets Failed
------------------------------+---------+------------------
length consistent                Enabled    0
length maximum max-frag          Enabled    0
length maximum udp               Disabled   --
length maximum max-tcp           Enabled    0
```

IDS パケット チェックの無効化と有効化

導入：Cisco NX-OS Release 4.0(1)

この項は、参考のために記載しており、必要のない場合があります。

アプリケーションが適切に機能するように、IDS パケット チェックを無効にする必要がある場合があります。次のグローバル コマンドを使用して、パケット チェックを無効および有効にすることができます。この例では、「length maximum max-tcp」IDS チェックを無効および有効にします。他のパケット チェックも同じ手順で設定できます。

```
n7000(config)# no hardware ip verify length maximum max-tcp

n7000(config)# hardware ip verify length maximum max-tcp
```

CHAPTER 6

Cisco NX-OS ソフトウェアのアップグレードまたはダウングレード

この章では、Cisco NX-OS システム ソフトウェアをアップグレードおよびダウングレードするときの Cisco NX-OS ベスト プラクティスについて説明します。Cisco NX-OS システム ソフトウェアをアップグレードまたはダウングレードする方法は 2 つあります。2 台のスーパーバイザ モジュールを取り付けたシャーシで無停止アップグレードを実行する場合は特に、In-Service-Software-Upgrade（ISSU）を使用することを推奨します。ただし、従来の方法はすばやくダウングレードする必要があるラボ環境と実稼動環境に適合するので、この方法についても説明します。

この章で説明する内容は、次のとおりです。

推奨のアップグレード手順（ISSU）

導入：Cisco NX-OS Release 4.0(1)

In-Service-Software-Upgrade（ISSU）では、1 つのコマンドを実行するだけで 2 台のスーパーバイザ モジュールを取り付けた Nexus 7000 をアップグレードまたはダウングレードできます。ブート変数が自動的に変更され、互換性チェックが実行されます。管理者は、結果が期待どおりであることを確認したら続行するように指示されます。処理が始まると、ダウンタイムなしでシステム ソフトウェアがシームレスにアップグレードされます。シャーシは、処理が行われている間も（中断せずに）パケットを転送し続け、その間に各シャーシ コンポーネントはアップグレードされます。アップグレードまたはダウングレードに必要な時間は、シャーシ タイプと取り付けられているモジュールの台数によって異なります（30 ～ 50 分）。処理を完了するには、各スーパーバイザ モジュールの CMP ポートを手動でリロードする必要があります。この手順を手動にすることで、ユーザが CMP ポートから手順をモニタリングしている場合にユーザが切断されないようにします。

最善の結果を得るために、次の推奨事項に従ってください。

- アップグレード全体をモニタリングする場合（モニタリングすることを推奨します）、両方のスーパーバイザ モジュールのコンソールまたは CMP ポートに接続します。
- リンク フラップ、STP 状態の変化などが発生しない安定した環境でのみ、ISSU アップグレードを実行します。
- Session Manager のセッションがアクティブな場合は、ISSU を実行できません。アクティブなセッションに対して、コミット、廃棄、または保存を実行する必要があります。

```
n7000# install all kickstart bootflash:n7000-s1-kickstart.5.1.1.bin system
bootflash:n7000-s1-dk9.5.1.1.bin

n7000# reload cmp module 5
n7000# reload cmp module 6
```

（注）　この手順は、1 台のスーパーバイザ モジュールを取り付けたシャーシについても使用できますが、シャーシはリロードする必要があるので処理中に中断が発生します。

ソフトウェアの互換性の確認（ISSU とシャーシのリロード）

導入：Cisco NX-OS Release 4.0(1)

ソフトウェアをダウングレードする前に、機能を適切に無効にできることを確認するために非互換性があるかどうかを確認します。設定から自動的に削除される機能があるかどうかが管理者に通知されるので、管理者はダウングレードする前に対処できます。このコマンドは、ダウングレードに ISSU を使用する場合も従来の方法を使用する場合も実行する必要があります。

```
n7000# show incompatibility-all system bootflash:n7000-s1-dk9.4.2.4.bin

Checking incompatible configuration(s) for vdc 'n7000':
------------------------------------------------------------

<CLI 出力は省略>

6) Service : otv , Capability : CAP_FEATURE_OTV
Description : Overlay Transport Virtualization
Capability requirement : STRICT
Disable command : no feature otv

7) Service : bfd , Capability : CAP_FEATURE_BFD_V2
Description : Feature bfd is enabled.
Capability requirement : STRICT
Disable command : Disable bfd using"no feature bfd"

<CLI 出力は省略>
```

従来のアップグレードまたはダウングレードの手順（シャーシのリロード）

導入：Cisco NX-OS Release 4.0(1)

従来のアップグレード手順は、特定のシナリオに対する推奨の方法なので、ここで説明します。この手順は、連続稼動が要件に含まれないラボ環境、または稀ですが、実稼動環境でのアップグレードで、タイミングよくダウングレードする必要がある場合に役に立ちます。システムをリロードして新しいソフトウェアをロードする前に、すべての設定を保存し、バックアップしていることを必ず確認することを推奨します。

```
n7000# copy running-config startup-config vdc-all

n7000(config)# boot kickstart bootflash:n7000-s1-kickstart.5.1.1.bin
n7000(config)# boot system bootflash:n7000-s1-dk9.5.1.1.bin

n7000# reload
```

CHAPTER 7

EPLD ソフトウェアのアップグレードまたはダウングレード

この章では、Electronic Programmable Logic Device（EPLD）をアップグレードまたはダウングレードする推奨手順について説明します。EPLD は、ハードウェアを交換することなくアップグレードできる I/O モジュールにある、ASIC などのハードウェア コンポーネントです。EPLD のアップグレードは、通常は不要ですが、新しいシャーシのインストールまたはシャーシの再導入など、一部の場合には、最新の EPLD バージョンにアップグレードし、すべてのアップグレード可能なハードウェア コンポーネントに、最新の機能強化や重大な修正が含まれているようにすることを推奨します。

この章で説明する内容は、次のとおりです。

EPLD アップグレード/ダウングレードの確認

導入：Cisco NX-OS Release 4.2(6)

EPLD のアップグレードを開始する前に、シャーシで検証チェックを実行し、必要な EPLD のアップグレード、および、各アップグレードの影響について、理解する必要があります。これは、アップグレードによって、不要にネットワークが停止される可能性があるような影響が、実稼動トラフィックに及ぼされるかどうかを判断する場合の準備に、役に立ちます。

```
n7000# show install all impact epld bootflash:n7000-s1-epld.5.1.1.img

Compatibility check:
Module  Type  Upgradable        Impact   Reason
------  ----  ----------    ----------   ------
     1    LC         Yes    disruptive   Module Upgradable
     2    LC         Yes    disruptive   Module Upgradable
     4    LC          No          none   Module is not Online
     5   SUP         Yes    disruptive   Module Upgradable
     7    LC         Yes    disruptive   Module Upgradable
     8    LC         Yes    disruptive   Module Upgradable
     9    LC         Yes    disruptive   Module Upgradable
    10    LC         Yes    disruptive   Module Upgradable
     1  Xbar         Yes    disruptive   Module Upgradable
     2  Xbar         Yes    disruptive   Module Upgradable
     3  Xbar         Yes    disruptive   Module Upgradable
     1   FAN         Yes    disruptive   Module Upgradable
     2   FAN         Yes    disruptive   Module Upgradable
     3   FAN         Yes    disruptive   Module Upgradable
     4   FAN         Yes    disruptive   Module Upgradable
```

```
Retrieving EPLD versions... Please wait.

Images will be upgraded according to following table:

Module  Type           EPLD      Running-Version   New-Version  Upg-Required
------  ----  -------------      ---------------   -----------  ------------
     1    LC  Power Manager              4.008       4.008           No
     1    LC  IO                         1.015       1.016           Yes
     1    LC  Forwarding Engine          1.006       1.006           No
     1    LC  FE Bridge(1)             186.005     186.006           Yes
     1    LC  FE Bridge(2)             186.005     186.006           Yes
     1    LC  Linksec Engine(1)          2.006       2.006           No
     1    LC  Linksec Engine(2)          2.006       2.006           No
     1    LC  Linksec Engine(3)          2.006       2.006           No
     1    LC  Linksec Engine(4)          2.006       2.006           No
     1    LC  Linksec Engine(5)          2.006       2.006           No
     1    LC  Linksec Engine(6)          2.006       2.006           No
     1    LC  Linksec Engine(7)          2.006       2.006           No
```

EPLD アップグレードの手順

導入：Cisco NX-OS Release 4.0(1)

この項は、参照の目的で含まれており、必須ではない場合がありますが、読むことを推奨します。最新の EPLD イメージにアップグレードしなくても、Cisco NX-OS ソフトウェアをアップグレードできます。cisco.com にある EPLD のリリース ノートを確認し、新しい機能または重大な修正に基づいて、その EPLD をアップグレードする必要があるかどうかを判断する必要があります。新規インストールを実行する場合は、EPLD を最新バージョンにアップグレードし、EPLD のアップグレードの将来的な必要性を抑制すると効率的です。

EPLD は、**install** コマンドの使用時に、コンポーネントごとにアップグレードされます。アップグレードできるコンポーネントは、一度に 1 つだけです。1 つのコンポーネントをアップグレードすると、ネットワークに対する不要な影響を回避するため、より細かく制御できます。ELPD のアップグレードには、I/O モジュールごとに 30 分間かかります。ダウングレードは、通常は必要ではありませんが、コンポーネントのダウングレードにも、同じ手順を使用できます。

最善の結果を得るために、次の推奨事項に従ってください。

- 実稼動トラフィックを渡さない I/O モジュールで、EPLD のみをアップグレードします（アップグレードの開始前に、トラフィックをリダイレクトします）。
- 時間を節約するために、アップグレードしようとしている I/O モジュールの電源がオフになっていないことを確認してください。モジュールの電源がオフの場合、モジュールの電源はオンになり、モジュールにあるすべてのアップグレード可能なコンポーネントは、アップデートの必要性に関係なく、アップデートされます。この場合、I/O モジュールのアップグレードに、より長い時間を要します。
- シャーシ全体で EPLD のアップグレードを開始するには、**install all epld** コマンドを使用します。この手順は、非実稼動シャーシでのみ使用する必要があります。実稼動シャーシでは、「実稼動」トラフィックは渡されません。
- コンポーネントのアップグレード プロセスは中断しないでください。

```
n7000# install module 1 epld bootflash:n7000-s1-epld.5.1.1.img

Retrieving EPLD versions... Please wait.
```

```
Images will be upgraded according to following table:
Module  Type           EPLD      Running-Version   New-Version  Upg-Required
------  ----  -------------      ---------------   -----------  ------------
     1    LC  Power Manager              4.008       4.008           No
     1    LC  IO                         1.015       1.016           Yes
     1    LC  Forwarding Engine          1.006       1.006           No
     1    LC  FE Bridge(1)             186.005     186.006           Yes
     1    LC  FE Bridge(2)             186.005     186.006           Yes
     1    LC  Linksec Engine(1)          2.006       2.006           No
     1    LC  Linksec Engine(2)          2.006       2.006           No
     1    LC  Linksec Engine(3)          2.006       2.006           No
     1    LC  Linksec Engine(4)          2.006       2.006           No
     1    LC  Linksec Engine(5)          2.006       2.006           No
     1    LC  Linksec Engine(6)          2.006       2.006           No
     1    LC  Linksec Engine(7)          2.006       2.006           No
     1    LC  Linksec Engine(8)          2.006       2.006           No

Module 1 will be powered down.
Do you want to continue? (yes/no) [n]:
```

CHAPTER 8

機能の有効化と無効化

導入：Cisco NX-OS Release 4.0(1)

Cisco NX-OS ソフトウェアには、OSPF、PIM などの特定の機能を有効および無効にする機能が用意されています。デフォルトでは、Cisco NX-OS ソフトウェアは、初期ネットワーク接続に必要な機能だけを有効にします。この方法では、必要のない追加のプロセスを実行しないことによってオペレーティング システムを最適化し、アベイラビリティを向上させています。

機能が有効になっていない場合、その機能のプロセスは実行されないので、コンフィギュレーション コマンドと確認コマンド（show）は CLI から実行できません。機能が有効になると、コンフィギュレーション コマンドと確認コマンドを実行できるようになります。機能によっては、機能が設定されるまで（**router ospf 10** など）、プロセスは開始されません。機能を無効のままにしておくか、不要になったときに無効にすることを推奨します。

```
n7000# show process | grep ospf
-     NR         -            1     -  ospf

n7000# show process | grep pim
-     NR         -            0     -  pim


n7000(config)# feature ospf
n7000(config)# router ospf 10

n7000(config)# feature pim


n7000# show feature

Feature Name          Instance  State
--------------------  --------  --------
bfd                   1         disabled
bfd_app               1         disabled
bgp                   1         disabled

<CLI 出力は省略>

ospf                  1         enabled
ospf                  2         enabled (not-running)
ospf                  3         enabled (not-running)
ospf                  4         enabled (not-running)
ospfv3                1         disabled
ospfv3                2         disabled
ospfv3                3         disabled
ospfv3                4         disabled
otv                   1         disabled
pbr                   1         disabled
pim                   1         enabled (not-running)
```

```
pim6                  1         disabled

<CLI 出力は省略>

vrrp                  1         disabled
vtp                   1         disabled
wccp                  1         disabled


n7000# show process | grep ospf
9074      S  775d327b            1     -  ospf
```

CHAPTER 9

IP 管理

この章では、IP 管理プロトコルを設定する場合に Cisco NX-OS が推奨するベスト プラクティスについて説明します。

この章で説明する内容は、次のとおりです。

Network Time Protocol（NTP）

ログのタイムスタンプおよびその他の管理データがすべてのデバイスで同期されるよう、すべてのネットワーク デバイスで NTP を設定することを推奨します。ネットワーク全体で相関しているネットワーク イベントの場合、NTP を使用すると利点があります。Cisco NX-OS では、NTP クライアント モードおよびピア モードでの動作がサポートされます。

冗長 NTP サーバ

導入：Cisco NX-OS Release 4.0(1)

冗長性のために、複数の NTP サーバを設定する必要があります。プライマリ NTP サーバは **prefer** オプションで設定し、VRF インスタンスは、アウトオブバンド接続に管理 VRF インスタンスを使用するよう、VRF インスタンスを設定する必要があります。

```
n7000(config)# ntp server a.a.a.a prefer use-vrf management
n7000(config)# ntp server a.a.a.a use-vrf management

n7000(config)# ntp peer b.b.b.b prefer use-vrf management
n7000(config)# ntp peer b.b.b.b use-vrf management
```

時間帯 / サマー タイム

導入：Cisco NX-OS Release 4.0(1)

デフォルト値が不要の場合、クロックの時間帯およびサマー タイムのパラメータを設定する必要があります。これらの値が設定されていない場合、クロックは、デフォルトで、サマー タイムの調整なしで UTC に設定されます。

```
n7000(config)# clock timezone PST -8 0
n7000(config)# clock summer-time PST
```

NTP 送信元インターフェイス /IP アドレス

導入：Cisco NX-OS Release 4.1(3)

管理 VRF インスタンス以外の VRF インスタンスを使用する場合は、NTP 送信元インターフェイスまたは IP アドレスを指定することを推奨します。これによって、ファイアウォールなどのセキュリティデバイスが、NTP パケットの送信元を特定できます。送信元インターフェイスまたは IP アドレスが指定されない場合、元の（アウトバンド）インターフェイスのプライマリ IP アドレスが使用されます。NTP トラフィックが管理 VRF インスタンスに関連付けられている場合、mgmt0 インターフェイスの IP アドレスが選択されます。NTP インターフェイスと IP 送信元アドレスを同時に設定することはできません。

```
n7000(config)# ntp source-interface ethernet 2/1

n7000(config)# ntp source x.x.x.x
```

NTP ロギング

導入：Cisco NX-OS Release 5.0(2a)

NTP ロギングはデフォルトでディセーブルになっています。NTP 同期の問題のトラブルシューティングを行う場合、NTP メッセージを記録してトラブルシューティングの参考にできます。

```
n7000(config)# ntp logging
```

MD5 認証

導入：Cisco NX-OS Release 5.0(2a)

デバイスで、そのクロックがルージュ NTP サーバまたはピアから同期されないようにするため、MD5 認証をイネーブルにする必要があります。NTP クライアント、ピア、サーバには、同じ信頼済み認証キーを設定する必要があります。異なる認証キーを使用して NTP サーバまたはピアから NTP メッセージを受信する場合、NTP クライアントではそのクロックと同期されません。

```
n7000(config)# ntp server a.a.a.a use-vrf management key 1
n7000(config)# ntp peer b.b.b.b use-vrf management key 1

n7000(config)# ntp authentication-key 1 md5 <password>
n7000(config)# ntp trusted-key 1
n7000(config)# ntp authenticate
```

アクセス コントロール リスト

導入：Cisco NX-OS Release 5.0(2a)

セキュリティを強化するには、特定の NTP ピアまたはサーバへのアクセスを制限して、Access Control List（ACL; アクセス コントロール リスト）を設定する必要があります。**statistics per-entry** での ACL 統計の収集はオプションですが、特定の NTP ピアまたはサーバから受信しているパケットの確認には効果的です。

```
n7000(config)# ntp server a.a.a.a use-vrf management
n7000(config)# ntp peer b.b.b.b use-vrf management
```

```
n7000(config)# ntp source x.x.x.x
n7000(config)# ntp access-group peer ntp-peers

n7000(config)# ip access-list ntp-peers
n7000(config-acl)# statistics per-entry
n7000(config-acl)# permit udp a.a.a.a/32 x.x.x.x/32 eq ntp
n7000(config-acl)# permit udp b.b.b.b/32 x.x.x.x/32 eq ntp
```

簡易ネットワーク管理プロトコル（SNMP）

Cisco NX-OS では、SNMP v1、v2c、および v3 がサポートされます。SNMPv3 では、ユーザ名、パスワード、およびペイロード データに対する認証機能および暗号化機能があるため、セキュリティを強化するには、SNMPv3 の使用を推奨します。

基本設定（連絡先 / 場所）

導入：Cisco NX-OS Release 4.0(1)

SNMP 管理デバイスからポーリングされているときにデバイスが識別されるよう、連絡先および場所の情報を指定します。

```
n7000(config)# snmp contact Cisco Systems
n7000(config)# snmp location San Jose, CA
```

ユーザ（バージョン 3）

導入：Cisco NX-OS Release 4.0(1)

追加のセキュリティ認証および暗号メカニズムのため、SNMPv3 が SNMP の推奨バージョンです。デフォルトでは、ローカル データベースにあるすべてのユーザ アカウントは、SNMPv3 要求を認証する場合に SNMP サーバが使用できる SNMP ユーザに同期されます。SNMP ポーリングおよび SNMP インフォーム通知の送信用に、追加のユーザ アカウント /SNMP ユーザ アカウントを作成できます。次の例では、デフォルトの「admin」ユーザが表示され、「snmp-user」という名前の別の SNMP ユーザが作成されます。v3 通知を送信するには、SNMP ユーザに対してエンジン ID のみを設定する必要があります（エンジン ID の値は、SNMP 通知サーバのエンジン ID に基づいています）。

```
n7000# show run snmp

snmp-server user admin network-admin auth md5 0x272298231264cbf31dbd423455345253 priv
aes-128 0x272298231264cbf31dbd423455345253 localizedkey

n7000(config)# snmp-server user snmp-user auth md5 <password> priv aes-128 <password>
engineID 80:00:00:09:03:00:0C:29:13:92:B9
```

コミュニティ ストリング（バージョン 1 および 2c）

導入：Cisco NX-OS Release 4.0(1)

SNMPv3 対応の管理サーバが使用できない場合、**snmp-server community** コマンドを使用して SNMP バージョン 1 および 2c をイネーブルにできます。SNMP v2c では、SNMPv1 以上の追加機能が提供されます。SNMP は、読み取り専用アクセスまたは読み取り / 書き込みアクセスに設定できます。セキュリティを強化するには、読み取り専用（ネットワーク オペレータ）アクセスのみをイネーブルにします。

```
n7000(config)# snmp-server community <password> group network-operator

n7000(config)# snmp-server community <password> group network-admin
```

（注）　**snmp-server community <password> ro** コマンドは、**snmp-server community <password> group network-operator** コマンドに自動的に変換されます。**snmp-server community <password> rw** コマンドは、**snmp-server <password> group network-admin** コマンドに自動的に変換されます。

通知 / トラップ受信機

導入：Cisco NX-OS Release 4.0(1)

ネットワーク イベントについて SNMP ネットワーク管理サーバに通知するには、SNMP 通知受信機を設定する必要があります。受信機は、特定の VRF インスタンスの SNMPv1、SNMPv2c、および SNMPv3 に対して設定できます。追加認証機能と暗号化機能のため、SNMP v3 を推奨します。SNMPv3 では、SNMP 受信者エンジン ID で設定された SNMP ユーザが必要です。

バージョン 3（推奨）

```
n7000(config)# snmp-server host x.x.x.x version 3 priv snmp-user
n7000(config)# snmp-server host x.x.x.x use-vrf management
```

バージョン 2c

```
n7000(config)# snmp-server host x.x.x.x traps version 2c <password>
n7000(config)# snmp-server host x.x.x.x informs version 2c <password>
n7000(config)# snmp-server host x.x.x.x use-vrf management
```

バージョン 1

```
n7000(config)# snmp-server host x.x.x.x traps version 1 <password>
n7000(config)# snmp-server host x.x.x.x use-vrf management
```

通知 / トラップ イベント

導入：Cisco NX-OS Release 4.0(1)

重要なイベントについて SNMP ネットワーク管理サーバに通知するには、SNMP 通知またはトラップを設定する必要があります。すべての SNMP 通知 / トラップをイネーブルにするか、または、イネーブルな機能に関連する特定の通知 / トラップをイネーブルにします。一部の通知 / トラップはデフォルトでイネーブルになっています。イネーブルになっているトラップを確認するには、**show snmp-server trap** コマンドを使用します。SNMP ホスト受信者の設定方法によって、SNMP 通知またはトラップが送信されます。

すべての通知 / トラップをイネーブルにする

```
n7000(config)# snmp-server enable traps
```

個々の通知 / トラップをイネーブルにする

```
n7000(config)# snmp-server enable traps feature-control
n7000(config)# snmp-server enable traps callhome smtp-send-fail
n7000(config)# snmp-server enable traps snmp authentication
```

インターフェイス リンク ステータス トラップ

導入：Cisco NX-OS Release 4.0(1)

SNMP インターフェイス リンク ステータス トラップは、デフォルトでイネーブルになっています。SNMP リンク ステータス トラップは、インターフェイスごとにディセーブルにできます。特定の環境では、インターフェイス トラップをディセーブルにすることは効果的です。ただし、重要なインフラストラクチャまたはサーバ インターフェイスでは、インターフェイス トラップをイネーブルにすることを常に推奨します。

```
n7000(config)# interface ethernet 1/1
n7000(config-if)# no snmp trap link-status
```

コミュニティ ストリングのアクセス コントロール リスト

導入：Cisco NX-OS Release 4.2(1)

特定の送信元 IP アドレスまたは宛先 IP アドレスへのアクセスを制限するには、Access Control List（ACL; アクセス コントロール リスト）をコミュニティ ストリング（SNMP v1 および v2c）に常に適用する必要があります。

```
n7000(config)# ip access-list snmp-acl
n7000(config-acl)# permit udp host x.x.x.x host x.x.x.x eq snmp

n7000(config)# snmp-server community <password> group network-operator
n7000(config)# snmp-server community <password> use-acl snmp-acl
```

送信元インターフェイス

導入：Cisco NX-OS Release 4.2(1)

管理 VRF インスタンスが使用中ではない場合、**通知**および**トラップ**の送信元インターフェイスを指定します。これによって、ファイアウォールなどのセキュリティ デバイスが、SNMP パケットの送信元を特定できます。送信元インターフェイスまたは IP アドレスが指定されない場合、元の（アウトバンド）インターフェイスのプライマリ IP アドレスが選択されます。**通知**機能は、SNMP v2c および v3 にのみ適用されます。すべての SNMP ホストにグローバルに、または、SNMP ホストごとに、送信元インターフェイスを設定できます。

グローバルに設定：

```
n7000(config)# snmp source-interface informs loopback0
n7000(config)# snmp source-interface traps loopback0
```

サーバごとに設定：

```
n7000(config)# snmp-server host a.a.a.a source-interface loopback0
```

SNMP のディセーブル化

導入：Cisco NX-OS Release 4.2(1)

SNMP はデフォルトでイネーブルになっています。ただし、コミュニティ ストリングが設定されていない場合、SNMP v1 および v2c は SNMP 要求には応答しません。SNMPv3 対応のサーバが Cisco Nexus 7000 シリーズ デバイスをポーリングする場合、SNMPv3 は SNMP 要求に応答します（SNMP ユーザ「admin」がデフォルトで設定されています）。SNMP が必須ではない場合、次のコマンドを使用してディセーブルにし、セキュリティを強化する必要があります。

```
n7000(config)# no snmp-server protocol enable
```

システム メッセージ ロギング

Cisco NX-OS ソフトウェアでは、DRAM にあるローカル ログ ファイル（log:messages）にシステム メッセージが保存されます（最新の 100 個の重大度 0、1、または 2 のメッセージは、NVRAM に保存されます）。Cisco NX-OS ソフトウェアでは、logflash: にもシステム メッセージが記録されます。logflash: は、システムのリロード後にも、一貫性のあるデータを提供します（logflash://sup-local/logs/messages）。

Syslog サーバ

導入：Cisco NX-OS Release 4.0(1)

最大 3 台の Syslog サーバを設定し、システム メッセージを受信できます。トラフィックを分離するために管理 VRF インスタンスを使用し、冗長性を保つ目的で少なくとも 2 台の Syslog サーバを設定することを推奨します。ログ メッセージの重大度は、サーバごとに指定できます。次に、重大度 5 を指定することによって、各サーバにメッセージ 0（Emergency）から 5（Notification）までを記録する例を示します。

```
n7000(config)# logging server a.a.a.a 5 use-vrf management
n7000(config)# logging server b.b.b.b 5 use-vrf management
```

送信元インターフェイス

導入：Cisco NX-OS Release 4.0(1)

デフォルト VRF インスタンスを使用して Syslog サーバに到達する場合、ループバック インターフェイスを送信元 IP アドレスとして指定できます。これによって、ファイアウォールなどのセキュリティ デバイスが、Syslog パケットの送信元を特定できます。送信元インターフェイスが指定されない場合、元の（アウトバンド）インターフェイスのプライマリ IP アドレスが選択されます。

```
n7000(config)# logging source-interface loopback 0
```

リンク ステータス イベント

導入：Cisco NX-OS Release 4.0(1)

すべてのインターフェイス リンク ステータス（Up/Down）メッセージが、デフォルトで記録されます。リンク ステータス イベントは、グローバルに、または、インターフェイスごとに、設定できます。次のグローバル コマンドによって、すべてのインターフェイスのリンク ステータス ロギング メッセージがディセーブルにされます。インターフェイス コマンドによって、特定のインターフェイスのリンク ステータス ロギング メッセージがイネーブルにされます。このシナリオは、ミッション クリティカルなインフラストラクチャまたはサーバ インターフェイスを除き、過度なメッセージをフィルタ処理する場合に便利です。

```
n7000(config)# no logging event link-status default

n7000(config)# interface ethernet x/x
n7000(config-if)# logging event port link-status
```

タイムスタンプ

導入：Cisco NX-OS Release 4.0(1)

システム メッセージ ロギングは、デフォルトで、1 秒単位で記録されます。より精度を高めるために、タイムスタンプをミリ秒単位およびマイクロ秒単位に設定できます。時間が重要な問題についてトラブルシューティングする場合は、ミリ秒単位またはマイクロ秒単位でタイムスタンプを使用することを推奨します。

```
n7000(config)# logging timestamp milliseconds
```

機能ごとの重大度レベル

導入：Cisco NX-OS Release 4.0(1)

Cisco NX-OS ソフトウェアでは、機能ごとに設定された重大度レベルがサポートされます。ネットワークで管理可能なより高度なレベルが必要な機能については、重大度レベルを設定することを推奨します。次に、NTP の設定および確認のコマンドの例を示します。すべての機能の現在の重大度レベルを変更するには、**logging level all <severity #>** コマンドを使用できます。

```
n7000(config)# logging level ntp 7

n7000# show logging level ntp
Facility        Default Severity        Current Session Severity
--------        ----------------        ------------------------
ntp                     2                       7

0(emergencies)          1(alerts)       2(critical)
3(errors)               4(warnings)     5(notifications)
6(information)          7(debugging)

n7000(config)# logging level all 5
```

ログ ファイルの内容の表示

導入：Cisco NX-OS Release 4.0(1)

次の **show logging** コマンドは、システム メッセージ ログ ファイルの表示および管理に役に立ちます。

```
n7000# show logging logfile  <-  Displays the contents of the default log file.

n7000# show logging last 10  <-  Displays the last # of lines of the default log file.

n7000# show logging NVRAM   <- Displays contents of the log file stored in NVRAM.

n7000# show file logflash://sup-local/log/messages <- Displays contents in logflash.
```

ログ ファイルの内容の削除

導入：Cisco NX-OS Release 4.0(1)

次の **clear** コマンドは、システム メッセージ ログ ファイルの内容を削除が必要な場合に、役に立ちます。

```
n7000# clear logging logfile  <- Clears the contents of the default log file.
```

```
n7000# clear logging nvram    <- Clears the contents of the default log file stored in
NVRAM.
```

Smart Call Home

Smart Call Home では、Network Operation Center（NOC）、特定のエンジニア、または Cisco TAC などの受信者に対して、標準的なテキスト電子メールまたは XML 通知を送信し、TAC ケースを自動生成する、自動的な方法が提供されます。問題の解決を早めるには、内部受信者と Cisco TAC 受信者の両方に対して Call Home をイネーブルにすることを推奨します。

内部受信者と Cisco TAC 受信者（宛先プロファイル）

導入：Cisco NX-OS Release 4.0(1)

Smart Call は Cisco NX-OS Release 4.0(1) で導入されましたが、次の例は Cisco NX-OS Release 5.0(2a) CLI の構文に基づいています。例：トラフィックを分離する管理 VRF インスタンスを使用して、冗長性の目的で 2 台の異なる電子メール サーバにフル テキスト電子メールを送信するよう、Call Home が設定されます。宛先プロファイル「Internal-NOC」では、プライオリティがより低いため、メール サーバ a.a.a.a が優先されます。応答がない場合は、メール サーバ b.b.b.b が使用されます。

```
n7000(config)# callhome

n7000(config-callhome)# contract-id Cisco-Contract-#
n7000(config-callhome)# customer-id xyz.com

n7000(config-callhome)# site-id n7000-Kirkland-DC
n7000(config-callhome)# streetaddress 12345 Street NE, Kirkland, WA
n7000(config-callhome)# email-contact Cisco-Customer@xyz.com
n7000(config-callhome)# phone-contact +1-800-123-4567

n7000(config-callhome)# destination-profile Internal-NOC
n7000(config-callhome)# destination-profile Internal-NOC format full-txt
n7000(config-callhome)# destination-profile Internal-NOC email-addr call-home-noc@xyz.com
n7000(config-callhome)# destination-profile Internal-NOC alert-group all

n7000(config-callhome)# destination-profile CiscoTAC-1 email-addr callhome@cisco.com

n7000(config-callhome)# transport email mail-server a.a.a.a priority 10 use-vrf management
n7000(config-callhome)# transport email mail-server b.b.b.b use-vrf management

n7000(config-callhome)# transport email from call-home@xyz.com
n7000(config-callhome)# transport email reply-to call-home@xy.com
```

（注）　**transport email snmp-server** コマンドは、Cisco NX-OS Release 4.x および NX-OS Release 5.x ソフトウェアでサポートされている元のコマンドです。複数のサーバおよびプライオリティへのサポートを追加するため、NX-OS Release 5.0(2a) で **transport email mail-server** コマンドが導入されました。

Call Home 受信者のテスト

導入：Cisco NX-OS Release 4.0(1)

Call Home の初期設定時に Call Home 受信者についてテストし、Call Home が想定どおりに動作することを確認します。

```
n7000# callhome test
```

CHAPTER 10

使いやすくするための管理ツール

この章では、デバイスの管理に推奨する Cisco NX-OS ソフトウェアについて説明します。設定の変更、スーパーバイザ モジュール ステータスの確認、またはハードウェアの交換についても説明します。

この章で説明する内容は、次のとおりです。

設定の変更

ここでは、Cisco NX-OS の設定を変更する場合に推奨される手順面でのベスト プラクティスについて説明します。

設定のロールバック

導入：Cisco NX-OS Release 4.0(1)

設定のロールバック機能を使用すると、管理者は、新しい設定への変更が想定どおりに動作しなかった場合に設定を簡単にロールバックできるようにするための、設定チェックポイントを作成できます。実稼動ネットワークで変更制御手順によって変更を行う前に、設定のチェックポイントを作成するための設定ロールバック機能を使用することを推奨します。これによって、予見できない問題が発生した場合に、1 つのコマンドで元の設定を再適用できます。Cisco NX-OS Release 4.2(1) から、（手動またはライセンスの期限切れによって）機能がディセーブルの場合に、自動チェックポイントが作成されます。ライセンスの期限切れによる VDC の削除では、自動チェックポイントは生成されません。Cisco NX-OS Release 4.2(1) チェックポイントから、**checkpoint file** コマンドを使用して作成しない場合に、チェックポイントがスタンバイ スーパーバイザに保存されます。次に、基本的なチェックポイントおよびロールバックの動作に関する例を示します。

```
n7000# checkpoint ospf-change-control
.....Done

n7000(config)# interface ethernet x/x
n7000(config-if)# ip address x.x.x.x/xx
```

```
n7000(config-if)# ip router ospf 10 area 0
n7000(config-if)# no shutdown

n7000# show run interface ethernet x/x

interface Ethernetx/x
  ip address x.x.x.x/xx
  ip router ospf 10 area 0.0.0.0
  no shutdown

n7000# rollback running-config checkpoint ospf-change-control
Note: Applying config parallelly may fail Rollback verification
Collecting Running-Config
Generating Rollback Patch
Executing Rollback Patch
Generating Running-config for verification
Generating Patch for verification

n7000# show run interface ethernet x/x
```

Session Manager

導入：Cisco NX-OS Release 4.0(1)

Session Manager を使用すると、ACL および QoS の設定を、バッチ モードで実行コンフィギュレーションに設定できます。これは、設定を適用する前に、TCAM スペースなどのハードウェア リソースが使用可能かどうかを確認する場合に役に立ちます。ACL を適用する場合か、QoS を設定する場合には、Session Manager を常に使用する必要があります。次に、インターフェイスに対して ACL を設定、確認、および適用する処理について説明します。

```
n7000# configure session apply-acl
Config Session started, Session ID is 1
Enter configuration commands, one per line.  End with CNTL/Z.
n7000(config-s)# ip access-list inbound-acl
n7000(config-s-acl)# deny ip 10.0.0.0/8 any
n7000(config-s-acl)# deny ip 172.16.0.0/12 any
n7000(config-s-acl)# deny ip 192.168.0.0/16 any
n7000(config-s-acl)# interface ethernet x/x
n7000(config-s-if)# ip access-group inbound-acl in
n7000(config-s-if)# verify
Verification Successful
n7000(config-s)# commit
Commit Successful
```

スーパーバイザ冗長性

ハイ アベイラビリティを使用するには、シャーシごとに 2 つのスーパーバイザ モジュールを取り付けることを推奨します。ここでは、冗長スーパーバイザ モジュールのステータスを確認し、必要な場合に手動でスーパーバイザ スイッチオーバーを実行する場合の情報について、説明します。

スーパーバイザ ステータスの確認

導入：Cisco NX-OS Release 4.0(1)

2 つのスーパーバイザ モジュールがある場合、スイッチの通常の動作中には、1 つのスーパーバイザ モジュールは「Active with HA standby」状態で、もう 1 つのスーパーバイザ モジュールは「HA Standby」状態である必要があります。

```
n7000# show system redundancy status

Redundancy mode
---------------
      administrative:    HA
         operational:    HA

This supervisor (sup-1)
-----------------------
    Redundancy state:    Active
    Supervisor state:    Active
    Internal state:      Active with HA standby

Other supervisor (sup-2)
------------------------
    Redundancy state:    Standby
    Supervisor state:    HA standby
```

手動スイッチオーバー

導入：Cisco NX-OS Release 4.0(1)

この項は、参考のために記載しており、必要のない場合があります。

スーパーバイザ スイッチオーバーは、2 つのスーパーバイザ モジュールがある場合に、シャーシを使用して手動で起動できます。スイッチオーバーが実行されると、前のアクティブなスーパーバイザ モジュールはリロードされ、スタンバイ スーパーバイザとしてオンライン状態に戻ります。スタンバイ スーパーバイザが「HA standby」ではない場合、スイッチオーバーを手動で実行することはできません。

```
n7000# system switchover
```

ロケータ LED

導入：Cisco NX-OS Release 4.0(1)

Cisco NX-OS ソフトウェアでは、イーサネット I/O モジュール上でハードウェア コンポーネント（シャーシ、ファン、ファブリック、モジュール、電源）およびポートを識別する場合に役に立つ、ロケータ LED 機能がサポートされます。ハードウェアの交換またはイーサネット ポートに関する作業（追加、移動など）の物理的な作業を担当する、リモート サポート チームとともに作業を行う場合には、ロケータ LED 機能を使用する必要があります。シャーシ コンポーネントまたはインターフェイスのロケータ LED をディセーブルにするには、**no locator-led** コマンドを使用します。

```
n7000# locator-led chassis
n7000# locator-led fan 1
n7000# locator-led module 1
n7000# locator-led powersupply 1
n7000# locator-led xbar 1

n7000(config)# interface ethernet 1/1
```

```
n7000(config-if)# beacon

n7000# show locator-led status
Component        Locator LED Status
-------------------------------------
Chassis          ON
Module  1        ON
Module  2        off
Module  5        off
Xbar  1          ON
Xbar  2          off
Xbar  3          off
PowerSupply  1   ON
PowerSupply  2   off
PowerSupply  3   off
Fan  1           ON
Fan  2           off
Fan  3           off
```

（注）　Cisco NX-OS CLI の構文は、Cisco NX-OS Release 4.1(2) で変更されました。**locator-led** コマンドが、廃止予定の **blink** コマンドに置き換わりました。I/O モジュールのイーサネット ポートのステータスは、**show locator-led status** コマンドの出力には表示されません。ポート ロケータ LED（ビーコン）がイネーブルかディセーブル化を判断するには、**show interface** コマンドを使用するか、または実行コンフィギュレーションを表示します。

Ethanalyzer

導入：Cisco NX-OS Release 4.0(1)

コントロール プレーン プロトコルおよび CPU の使用率が高い場合にトラブルシューティングを行うには、イーサネット アナライザを使用します。イーサネット アナライザを使用すると、管理者は、スーパーバイザ モジュール CPU へ、およびスーパーバイザ モジュール CPU から、送信されるパケットを記録できます。CLI を使用して、パケットごとの簡略情報または詳細情報を記録して表示するか、または、Wireshark などのプロトコル アナライザにエクスポートできます。トラブルシューティングをする場合、対象パケットを特定するには簡略な記録を実行し、対象パケットをより詳細に分析するには詳細な記録を実行する必要があります。記録は、**write** または **>** オプションを使用してファイルにリダイレクトし、ローカルに保存できます。イーサネット アナライザでは、デフォルトで 10 フレームが記録されます。フレーム数を増加するには、**limit-captured-frames <0- 2147483647>** オプションを使用できます。値 **0** は、制限がないことを意味し、10MB の循環バッファが作成されます。

簡略記録：

```
n7000# ethanalyzer local interface inband
Capturing on inband
2010-06-02 20:44:40.327808 192.168.20.1 -> 224.0.0.5    OSPF Hello Packet
2010-06-02 20:44:41.480658 192.168.20.2 -> 207.68.169.104 DNS Standard query A
print.cisco.com
2010-06-02 20:44:41.730633 192.168.20.2 -> 207.68.169.104 DNS Standard query A
print.cisco.com
2010-06-02 20:44:41.730638 192.168.20.2 -> 65.54.238.85 DNS Standard query A
print.cisco.com
2010-06-02 20:44:42.480586 192.168.20.2 -> 65.54.238.85 DNS Standard query A
print.cisco.com

<テキストは省略>
```

詳細記録：

```
n7000# ethanalyzer local interface inband limit-captured-frames 100 detail
Capturing on inband
Capturing on inband
Frame 1 (60 bytes on wire, 60 bytes captured)
    Arrival Time: Oct  2, 2010 22:07:57.150394000
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    Frame Length: 60 bytes
    Capture Length: 60 bytes
    [Frame is marked: False]
    [Protocols in frame: eth:llc:stp]
IEEE 802.3 Ethernet
    Destination: 01:80:c2:00:00:00 (01:80:c2:00:00:00)
        Address: 01:80:c2:00:00:00 (01:80:c2:00:00:00)

<テキストは省略>
```

簡略記録のファイルへの書き込み：

```
n7000# ethanalyzer local interface inband write bootflash:cpu.
```

記録ファイルの読み取り：

```
n7000# ethanalyzer local read bootflash:cpu.txt
```

詳細記録のファイルへのリダイレクト：

```
n7000# ethanalyzer local interface detail > cpu-1.txt
```

記録ファイルの読み取り：

```
n7000# show file bootflash:cpu-1.txt
```

（注） **inband** オプションでは、I/O モジュールのパケットが記録され、**mgmt** オプションでは、スーパーバイザ モジュール mgmt0 ポートが記録されます。

（注） CLI の構文は、Cisco NX-OS Release 4.x から Release 5.x で、少し変更されました。この CLI の出力は、NX-OS Release 5.1(1) から記録されます。

スイッチド ポート アナライザ

導入：Cisco NX-OS Release 4.0(1)

Intrusion Prevention Systems（IPS; 侵入防御システム）などのネットワーク サービスでトラブルシューティングまたはデータの提供を行う場合、Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）を使用して、送信元から宛先へトラフィックをミラーできます。このマニュアルでは、SPAN の詳細については説明しませんが、トラブルシューティング後にアクティブにする必要がない場合には、ローカル セッションおよび ERSPAN セッションで **shut** コマンドを使用してディセーブルにすることを推奨します。これによって、ハードウェア リソースで、ファブリック全体に不要なトラフィックが充満することを防ぐことができます。ERSPAN 機能が、Cisco NX-OS Release 5.1(1) で導入されました。

ローカル SPAN：

```
n7000(config)# monitor session 1
n7000(config-monitor)# shut
```

Encapsulated Remote（ERSPAN; カプセル化リモート）：

```
n7000(config)# monitor session 1 type erspan-source
n7000(config-erspan-src)# shut

n7000(config)# monitor session 1 type erspan-destination
n7000(config-erspan-dst)# shut
```

デバッグの実行

ここでは、デバッグを実行する場合の Cisco NX-OS 推奨のベスト プラクティスについて説明します。ネットワークのパフォーマンスに影響が及ぼされる可能性があるため、デバッグ コマンドの実行時には、常に注意を払ってください。

ファイルへの出力のリダイレクト

導入：Cisco NX-OS Release 4.0(1)

デバッグの出力は、デフォルトで、コンソール セッションおよびモニタリング セッション（SSH/Telnet）に記録されます。これは、ネットワーク パフォーマンスに影響を及ぼす可能性があります。デバッグの実行時には、スーパーバイザ モジュール CPU での処理のオーバーヘッドを抑制するには、出力を、コンソール セッションまたはターミナル セッションではなく、ファイルにリダイレクトする必要があります。次に、分析のためにデバッグの出力がファイルにリダイレクトされる例を示します。リダイレクトされたデバッグの出力は、log: ディレクトリに保存されます。デバッグの出力がファイルにリダイレクトされると、リモートの宛先に出力を表示するか、または、コピーできます。pipe オプションを使用すると、ログ ファイルを解析できます。**show debug** コマンドによって現在のデバッグ ステータスが表示され、**no debug all** コマンドによってすべてのデバッグがディセーブルになります。

（注） 必要ではない、意図しないデバッグを実行したままにしないでください。

```
n7000# debug logfile cdp-debug
n7000# debug cdp all
n7000# no debug cdp all

n7000# dir log:cdp-debug
      14560    Nov 01 22:05:18 2010  cdp-debug

n7000# show debug logfile cdp-debug
2010 Nov  1 22:02:02.948577 cdp: Going to send CDP version 2 pkt on Ethernet7/3
2010 Nov  1 22:02:02.948662 cdp: Sent CDP packet untagged on interface 0x1a30200
0
2010 Nov  1 22:02:02.948696 cdp: Going to send CDP version 2 pkt on Ethernet10/1
8

<テキストは省略>

n7000# show debug logfile cdp-debug | include Ethernet10/1
```

CHAPTER 11

ハードウェアの診断の確認とロギング

この章では、ハードウェアの障害を管理およびトラブルシューティングするときの Cisco NX-OS の推奨機能と手順について説明します。

この章で説明する内容は、次のとおりです。

オンライン診断

Generic Online Diagnostics（GOLD）には、ハードウェア障害の検出に役立つハードウェア テスト検証が用意されています。障害が検出された場合、ネットワークが停止する可能性を低減するために障害を軽減する是正措置が行われます。GOLD テストは、シャーシの電源を入れたときに Online Insertion and Removal（OIR; 活性挿抜）イベントに対して実行されます。ヘルス チェックは、バックグラウンドで（連続テスト）、CLI からの要求に応じて実行されます。

GOLD の有効化

導入：Cisco NX-OS Release 4.0(1)

Generic Online Diagnostics は、デフォルトで有効になっています（オンライン診断を無効にすることは推奨しません）。イベント オンライン診断が無効になっている場合、次のコマンドを使用して有効にできます。

```
n7000(config)# diagnostic bootup level complete
```

診断内容の理解（モジュール別）

導入：Cisco NX-OS Release 4.0(1)

show diagnostic content コマンドを実行すると、モジュールに使用できるテストと、各テストの関連する属性が表示されます。これは、On-Demand テストを実行する前にモジュールに使用できるテストを確認し、そのテストで中断が発生するかどうかを確認できるので便利です。

```
n7000# show diagnostic content module 1

Module 1: 10/100/1000 Mbps Ethernet Module

Diagnostics test suite attributes:
B/C/* - Bypass bootup level test / Complete bootup level test / NA
```

```
P/*   - Per port test / NA
M/S/* - Only applicable to active / standby unit / NA
D/N/* - Disruptive test / Non-disruptive test / NA
H/*   - Always enabled monitoring test / NA
F/*   - Fixed monitoring interval test / NA
X/*   - Not a health monitoring test / NA
E/*   - Sup to line card test / NA
L/*   - Exclusively run this test / NA
T/*   - Not an ondemand test / NA
A/I/* - Monitoring is active / Monitoring is inactive / NA

                                                    Testing Interval
ID     Name                                Attributes      (hh:mm:ss)
____   __________________________________  ____________    _________________
 1)    EOBCPortLoopback--------------->     C**N**X**T*     -NA-
 2)    ASICRegisterCheck-------------->     ***N******A     00:01:00
 3)    PrimaryBootROM----------------->     ***N******A     00:30:00
 4)    SecondaryBootROM--------------->     ***N******A     00:30:00
 5)    PortLoopback------------------->     CP*N***E**A     00:15:00
```

On-Demand テスト

導入：Cisco NX-OS Release 4.0(1)

On-Demand テストは、ハードウェアに障害があると考えられる場合は必ず実行する必要があります。On-Demand テストは、Exec モードから実行します。GOLD テストでは、中断が発生する場合と発生しない場合があります。このため、ネットワークが停止しないように注意する必要があります。GOLD テストで中断が発生する場合は、続行を確認するプロンプトが管理者に表示されます。

```
n7000# diagnostic start module 1 test 6 port 1
```

GOLD テスト結果の確認（モジュールごと）

導入：Cisco NX-OS Release 4.0(1)

次のコマンドでは、モジュール 1 に関する GOLD テストの結果を確認します。**detail** オプションを指定すると、各テストのタイムスタンプ情報が表示されます。これは、テストに合格した可能性がある日時またはテストに不合格になった可能性がある日時の確認に役立ちます。

```
n7000# show diagnostic result module 1

Current bootup diagnostic level: complete
Module 1: 10/100/1000 Mbps Ethernet Module

        Test results: (. = Pass, F = Fail, I = Incomplete,
        U = Untested, A = Abort, E = Error disabled)

         1) EOBCPortLoopback--------------> .
         2) ASICRegisterCheck-------------> .
         3) PrimaryBootROM----------------> .
         4) SecondaryBootROM--------------> .
         5) PortLoopback:

          Port   1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16
          -------------------------------------------------
                 U  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U

          Port  17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32
          -------------------------------------------------
                 U  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
```

```
Port  33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48
------------------------------------------------
```

オンボード障害ロギング

Onboard Failure Logging（OBFL; オンボード障害ロギング）は、トラブルシューティング時に役立つ詳細情報を含んでいるモジュールごとの永続的なイベント ロギングを提供します。OBFL は、デフォルトで有効になっています。OBFL は無効にしないでください。一部の OBFL ログのデータは理解するのが難しい可能性がありますが、このログは Cisco TAC がハードウェアの問題を診断するときに役立ちます。

OBFL の有効化と無効化

導入：Cisco NX-OS Release 4.0(1)

この項は、参考のために記載しており、必要のない場合があります。

OBFL ログは、システム単位またはモジュール単位で無効にできます。次の例では、以前に無効にしたモジュールごとの OBFL ログを有効にする方法を示しています。このログはデフォルトで有効になっているので、この作業は通常は必要ありません。

```
n7000(config)# hw-module logging onboard module 1 environmental-history
    Module:  1   Enabling environmental-history ... was successful.
```

ログの内容の確認

導入：Cisco NX-OS Release 4.0(1)

OBFL ログは、システムごと（すべてのログ）、すべてのモジュールのログ タイプごと（例：環境に関する履歴）、モジュール/ログ タイプごとに確認できます。内容をリモートの宛先に送信する必要がある場合は、「|」オプションを使用して、出力をファイルにリダイレクトできます。ログは永続的なので、大量のデータを含んでいる可能性があります。

```
n7000# show logging onboard  module 1 environmental-history
----------------------------
    Module:  1
----------------------------
========== Sensor Temperature History Log ==========
-------------------------------------------------
Fri Apr  9 11:20:24 2010 sensor 13 temperature 53
Fri Apr  9 11:36:25 2010 sensor 14 temperature 54

<テキストは省略>
```

ログの内容の消去

導入：Cisco NX-OS Release 4.0(1)

次の **clear log onboard** コマンドを使用して、すべてのログ、すべてのモジュールの 1 つのログ タイプ、または指定したモジュールの特定のログ タイプの内容を消去できます。

```
n7000# clear log onboard ?
  <CR>
```

```
counter-stats          Clear OBFL counter statistics
environmental-history  Clear OBFL environmental history
error-stats            Clear OBFL error statistics
exception-log          Clear OBFL exception log
fex                    Clear OBFL information for FEX
internal               Clear Logging Onboard Internal
interrupt-stats        Clear OBFL interrupt statistics
module                 Clear OBFL information for Module
obfl-logs              Clear OBFL (boot-uptime/device-version/obfl-history).
stack-trace            Clear OBFL stack trace
```

CHAPTER 12

ハードウェア リソース使用率の管理

この章では、CPU、メモリ、I/O モジュール TCAM テーブルの各使用率など、ハードウェア リソースの使用率を管理するときの Cisco NX-OS の推奨手順について説明します。

この章で説明する内容は、次のとおりです。

CPU プロセス

この項では、スーパーバイザ モジュールの CPU 使用率を確認する方法について説明します。

使用率

導入：Cisco NX-OS Release 4.0(1)

show system resources コマンドを実行すると、スーパーバイザ モジュールの全体的な CPU 使用率が表示されます。sort オプションを指定して **show process cpu** コマンドを実行すると、プロセスごとに最も CPU 使用率が高い順に並べ替えられて、すべてのプロセスが表示されます。**show process cpu history** コマンドを実行すると、60 秒、60 分、72 時間の 3 つの単位で CPU 履歴が表示されます。CPU 履歴の確認は、ネットワーク イベントと過去の CPU 使用率を関連付けるときに役立ちます。**show process cpu** コマンドの sort オプションと history オプションは、Cisco NX-OS Release 4.2(1) で導入されました。

Cisco NX-OS はプリエンプティブ CPU マルチタスクを利用するので、プロセスはアイドル状態の CPU を使用してタスクをより速く完了できます。このため、問題とならない可能性がある CPU スパイクが history オプションによって報告されることがあります。CPU の平均使用率が 100 % に近いままの場合は、追加の調査を実施する必要があります。

```
n7000# show system resources
Load average:   1 minute: 0.06   5 minutes: 0.04   15 minutes: 0.00
```

```
Processes   :   310 total, 1 running
CPU states  :   0.0% user,   0.5% kernel,   99.5% idle
Memory usage:   4135780K total,   1180900K used,   2954880K free
                      0K buffers,  759580K cache

n7000# show process cpu sort

PID    Runtime(ms)  Invoked   uSecs  1Sec    Process
-----  -----------  --------  -----  ------  -----------
 3102         1692    371648      4    2.0%  platform
    1          162     49364      3    0.0%  init

<テキストは省略>


n7000# show process cpu history

                    1    1                   1                       1
    151 2    1  176 6112 2212    1   21  511 1  2    31 151 1 10
100
 90
 80
 70
 60
 50
 40
 30
 20                #                       #
 10  #            ## #  #                  #                #     #
    0....5....1....1....2....2....3....3....4....4....5....5....
               0    5    0    5    0    5    0    5    0    5
```

プロセスの再起動

導入：Cisco NX-OS Release 4.0(1)

この項は、参考のために記載しており、必要のない場合があります。

一部の Cisco NX-OS プロセスは、**restart** コマンドを使用して再起動できます。プロセスでは手動再起動を要求すべきではないですが、要求する場合、プロトコルを再設定したり、シャーシをリロードしたりせずにプロセスを再起動できます。プロセスを再起動すると中断が発生する場合があるので、この機能は注意して使用する必要があります。

```
n7000# restart ospf 10
```

メモリ

この項では、スーパーバイザ モジュールの DRAM とフラッシュ メモリの使用率を確認する方法について説明します。

DRAM 使用率

導入：Cisco NX-OS Release 4.0(1)

シャーシのスーパーバイザ モジュールのメモリ使用率は、次のコマンドでモニタリングできます。**show system resources** コマンドを実行すると、スーパーバイザ モジュールの全体でのメモリ使用率が表示されます。**show process memory** コマンドを実行すると、VDC ごとの 1 プロセスあたりのメモリ使用率が表示されます。

```
n7000# show system resources
Load average:   1 minute: 0.06   5 minutes: 0.04   15 minutes: 0.00
Processes   :   310 total, 1 running
CPU states  :   0.0% user,   0.5% kernel,   99.5% idle
Memory usage:   4135780K total,   1180900K used,   2954880K free
                      0K buffers,  759580K cache

n7000# show process memory

PID    MemAlloc  MemLimit    MemUsed     StackBase/Ptr      Process
-----  --------  ----------  ----------  -----------------  ----------------

<テキストは省略>

11849   2994176  329981836   127692800   bffff5e0/bfffc820  nfm
12019  13029376  334518976   115449856   bfffe1c0/bfffde30  ospf
12266    155648  0           1712128     bfffe800/bfffe5cc  more
12267   1118208  0           48463872    bffff670/bfff9c08  vsh
12268         0  0           0           bfffe410/bfffdd28  ps

<テキストは省略>
```

フラッシュ使用率

導入：Cisco NX-OS Release 4.0(1)

フラッシュ ファイル システムの容量は、スーパーバイザ モジュールごとに確認できます。次の例では、スロット 5 に 1 台のスーパーバイザ モジュールを取り付けています。bootflash: は、2 GB のオンボード フラッシュを指しています。logflash、slot0 は、スーパーバイザ モジュールの外付けコンパクト フラッシュ用スロットを指しています。**dir** コマンドを実行すると、フラッシュ メモリのタイプごとに内容が表示されます（ここでは、出力を記載していません）。

```
n7000# show hardware capacity | begin flash
         5       bootflash     1767480     1055144     40
         5       logflash      7997912     7555672      5
         5       slot0         1996928     1652944     17

n7000# dir bootflash:
n7000# dir logflash:
n7000# dir slot0:
```

MAC アドレス TCAM テーブル

この項では、MAC アドレス TCAM テーブルの使用率を確認し、必要な場合はエージン タイムを変更する方法について説明します。

使用率

導入：Cisco NX-OS Release 4.0(1)

Cisco Nexus 7000 シリーズでは、分散フォワーディング アーキテクチャを採用しています。このアーキテクチャでは、各イーサネット M シリーズ モジュールにパケット転送を担当するフォワーディング エンジンが搭載されます。M シリーズ モジュール上のフォワーディング エンジンは、128,000 個の MAC アドレス エントリを格納できます。MAC アドレス テーブルは、同じ Virtual Device Context（VDC; 仮想デバイス コンテキスト）で設定されたポートを持つイーサネット M シリーズ モジュール間で同期されます。次のコマンドは、シャーシ内のすべてのモジュールの MAC アドレス テーブルの容量を確認するときに役立ちます。

```
n7000# show hardware capacity forwarding | begin L2

L2 Forwarding Resources
-----------------------
  L2 entries: Module   total    used   mcast   ucast   lines   lines_full
              1       131072       6       1       5    8192            0
              2       131072       6       1       5    8192            0

<テキストは省略>
```

エージング タイム

導入：Cisco NX-OS Release 4.0(1)

この項は、参考のために記載しており、必要のない場合があります。

デフォルトの MAC アドレス テーブルのエージング タイムは 1,800 秒（30 分）です。エージング タイムを変更して、おおよそのアグレッシブ タイムアウト値に設定できます。MAC アドレスのエージング タイムは、スイッチド ドメイン内のすべてのデバイスに対して整合している必要があります。

```
n7000(config)# mac address-table aging-time ?
  <0-0>         0 disables aging
  <120-918000>  Aging time in seconds.
```

ユニキャストまたはマルチキャスト TCAM テーブル

この項では、ユニキャストまたはマルチキャスト TCAM テーブルの使用率を確認する方法について説明します。

使用率

導入：Cisco NX-OS Release 4.0(1)

Cisco Nexus 7000 シリーズでは、分散フォワーディング アーキテクチャを採用しています。このアーキテクチャでは、各イーサネット M シリーズ モジュールにパケット転送を担当するフォワーディング エンジンが搭載されます。M シリーズ モジュール上のフォワーディング エンジンは、128,000 個の IPv4/IPv6 ルーティング エントリまたは、Scalable-Feature ライセンスがインストールされた XL モジュールの場合は、1,000,000 個のエントリを格納できます。IPv4/IPv6 ユニキャスト/マルチキャスト テーブルは、同じ Virtual Device Context（VDC; 仮想デバイス コンテキスト）で設定されたポートを持つイーサネット M シリーズ モジュール間で同期されます。次の例では、非 XL モジュールのデフォ

ルトの TCAM 割り当てを表示します。Cisco NX-OS Release 4.2(1) より、Cisco NX-OS では動的 TCAM 割り当てをサポートしています。これにより、イベントおよび追加のエントリを必要とするアドレス ファミリ（つまり、IPv6 ユニキャスト）でのリソース使用率を向上させることができます。

```
n7000# show hardware capacity forwarding | begin TCAM

Key: Log/Phys = Logical entries / Physical entries
Note: IPv4 Multicast/IPv6 Unicast entries share one FIB TCAM entry pool

Module 1 usage:
Route Type            Used      %Used      Free      %Free      Total
                   (Log/Phys)             (Log/Phys)           (Log/Phys)
------------------------------------------------------------------------------
IPv4 Unicast:        19/19         0    57325/57325     99    57344/57344
IPv4 Multicast:       4/8          0    16380/32760     99    16384/32768
IPv6 Unicast:         9/18         0    16375/32750     99    16384/32768
IPv6 Multicast:       5/20         0     2043/8172      99     2048/8192
```

NetFow TCAM テーブル

この項では、NetFlow TCAM テーブルの使用率を確認する方法について説明します。

使用率

導入：Cisco NX-OS Release 4.0(1)

Cisco Nexus 7000 シリーズでは、分散フォワーディング アーキテクチャを採用しています。このアーキテクチャでは、各イーサネット M シリーズ モジュールにパケット転送を担当するフォワーディング エンジンが搭載されます。M シリーズ モジュール上のフォワーディング エンジンは、512,000 個の NetFlow エントリを格納できます。この値は、XL M シリーズ モジュールでも非 XL M シリーズ モジュールでも同じです。

```
n7000# show hardware capacity forwarding | begin Netflow

n7000# show hardware capacity forwarding | begin Netflow
Netflow Resources
-----------------
Flow Table Usage:  Module  Util    Used    Free    Fail
                   1       0.00%   0       515090  0
                   2       0.00%   0       515090  0
ICAM Usage:        Module  Util    Used    Free
                   1       0.00%   0       16
                   2       0.00%   0       16
IPv4 Mask Usage:   Module  Util    Used    Free
                   1       0.00%   0       32
                   2       0.00%   0       32
IPv6 Mask Usage:   Module  Util    Used    Free
                   1       0.00%   0       32
                   2       0.00%   0       32
```

ACL または QoS TCAM テーブル

この項では、ACL または QoS TCAM テーブルの使用率を確認し、必要な場合は ACL TCAM チェーニングを有効にする方法について説明します。

使用率

導入：Cisco NX-OS Release 4.0(1)

Cisco Nexus 7000 シリーズでは、分散フォワーディング アーキテクチャを採用しています。このアーキテクチャでは、各イーサネット M シリーズ モジュールにパケット転送を担当するフォワーディング エンジンが搭載されます。M シリーズ モジュール上のフォワーディング エンジンは、64,000 個（非 XL モジュールの場合）または 128,000 個（Scalable Feature ライセンスがインストールされた XL モジュールの場合）の ACL QoS エントリを格納できます。

```
n7000# show hardware capacity | begin ACL
         ACL Hardware Resource Utilization (Module 1)
         ---------------------------------------------
                           Used    Free    Percent
                                           Utilization
-----------------------------------------------------
Tcam 0, Bank 0             1       16383   0.00
Tcam 0, Bank 1             2       16382   0.01
Tcam 1, Bank 0             1       16383   0.00
Tcam 1, Bank 1             2       16382   0.01

LOU                        0       104     0.00
Both LOU Operands          0
Single LOU Operands        0
LOU L4 src port:           0
LOU L4 dst port:           0
LOU L3 packet len:         0
LOU IP tos:                0
LOU IP dscp:               0
LOU ip precedence:         0
TCP Flags                  0       16      0.00

Protocol CAM               0       7       0.00
Mac Etype/Proto CAM        0       14      0.00

Non L4op labels, Tcam 0    0       6143    0.00
Non L4op labels, Tcam 1    0       6143    0.00
L4 op labels, Tcam 0       0       2047    0.00
L4 op labels, Tcam 1       0       2047    0.00
```

ACL リソース ポーリング

導入：Cisco NX-OS Release 4.2(1)

この項は、参考のために記載しており、必要のない場合があります。

ACL TCAM は、現在の M シリーズ フォワーディング エンジンでは 4 つのバンク（非 XL モジュールの場合、1 バンクあたり 16K、XL モジュールの場合、1 バンクあたり 32K）に分割されています。Cisco NX-OS Release 4.2(1) よりも前のリリースでは、1 つの ACL に、1 バンク分のエントリ（モジュール タイプに応じて 16K または 32K エントリ）しか格納できませんでした。Cisco NX-OS Release 4.2(1) より、1 つの ACL を複数のバンクに対してプログラミングできるようになり、非 XL モジュールでは 1 つの ACL に最大 64, 000 個のエントリ、XL モジュールでは最大 132,000 個のエントリを格納できます。この機能は、16,000 個より多くのエントリを格納する ACL が必要なシステムでのみ有効にする必要があります。この機能は、すべての VDC についてデフォルトの VDC（1）で設定します。

```
n7000(config)# hardware access-list resource pooling module 1

n7000# show hardware access-list resource pooling
  Module 1 enabled
```

ファブリック使用率

ファブリック使用率をモニタリングして、入力と出力の帯域使用率を確認できます。**show hardware fabric-utilization** コマンドは、全体的な使用率と使用率の詳細を確認するときに役立ちます。**show hardware capacity fabric-utilization** は、ピーク使用率の履歴を確認するときに役立ちます。

```
n7000# show hardware fabric-utilization
-----------------------------------------------
Slot        Total Fabric        Utilization
            Bandwidth      Ingress % Egress %
-----------------------------------------------
1             138 Gbps          0.0       0.0
2             138 Gbps          0.0       0.0
4             138 Gbps          0.0       0.0
5              69 Gbps          0.0       0.0
7             138 Gbps          0.0       0.0
8             138 Gbps          0.0       0.0
9             138 Gbps          0.0       0.0
10            138 Gbps          0.0       0.0

n7000# show hardware fabric-utilization detail
-------------------------------------------------------------------------
Fabric Planes:
A -- Unicast fabric interface
B -- Multicast/Multidestination fabric interface
-------------------------------------------------------------------------
Unidirectional Fabric Bandwidth per Fab Link is 23 Ggps (A+B)
-------------------------------------------------------------------------
I/O   Fab  Fab  Fab  Fab  Fab        Fabric Utilization
Slot  Mod  Ins  Chnl Link Plane    Ingress%     Egress%
-------------------------------------------------------------------------
1     1    1    5    0     A          0            0
1     1    1    5    0     B          0            0
1     1    1    3    1     A          0            0
1     1    1    3    1     B          0            0
1     2    1    5    2     A          0            0
1     2    1    5    2     B          0            0
1     2    1    3    3     A          0            0
1     2    1    3    3     B          0            0
1     3    1    5    4     A          0            0
1     3    1    5    4     B          0            0
1     3    1    3    5     A          0            0
1     3    1    3    5     B          0            0

<テキストは省略>

n7000# show hardware capacity fabric-utilization
-------------------------------------------------------------------------
Fabric Planes:
A -- Unicast fabric interface
B -- Multicast/Multidestination fabric interface
-------------------------PEAK FABRIC UTILIZATION-------------------------
I/O  |-----FABRIC----|       Ingress           |       Egress
Slot |Mod Inst  Plane| Util           Time     | Util          Time
-------------------------------------------------------------------------
1     1     1     A      0%     11-01@23:09:42    0%     11-01@23:09:42
1     1     1     B      0%     11-01@23:09:42    0%     11-01@23:09:42
1     1     1     A      0%     11-01@23:09:42    0%     11-01@23:09:42
1     1     1     B      0%     11-01@23:09:42    0%     11-01@23:09:42
1     2     1     A      0%     11-01@23:09:42    0%     11-01@23:09:42
1     2     1     B      0%     11-01@23:09:42    0%     11-01@23:09:42
```

```
1     2     1     A      0%     11-01@23:09:42    0%     11-01@23:09:42
1     2     1     B      0%     11-01@23:09:42    0%     11-01@23:09:42
1     3     1     A      0%     11-01@23:09:42    0%     11-01@23:09:42
```

VDC リソース使用率

導入：Cisco NX-OS Release 4.0(1)

グローバル VDC リソースは、**show vdc resource** コマンドで確認できます。VDC はメモリ、SPAN セッションなどの共通のリソースを求めて競合する可能性があるので、知っておくと役に立ちます。

```
n7000# show vdc resource

  vlan                16 used    48 unused  16368 free  16320 avail  16384 total

  monitor-session      0 used     0 unused      2 free      2 avail      2 total

  monitor-session-erspan-dst      0 used     0 unused     23 free     23 avail  23 total

  vrf                  8 used     0 unused    992 free    992 avail   1000 total

  port-channel         0 used     0 unused    768 free    768 avail    768 total

  u4route-mem        120 used     0 unused    396 free    396 avail    516 total

  u6route-mem         36 used     0 unused    172 free    172 avail    208 total

  m4route-mem         82 used     0 unused    118 free    118 avail    200 total
```

CHAPTER 13

Cisco TAC に送信するデータの収集

問題を迅速に解決するためには、TAC ケースのオープン時にトラブルシューティング情報とログを前もって添付しておくことが重要です。この章では、TAC ケースに添付するトラブルシューティング情報を収集するときの推奨手順について説明します。Cisco TAC エンジニアは、追加のデータの提出を依頼することがあります。次の作業を行っておけば、エンジニアにデータが提供されるのでエンジニアはすぐに調査を開始できます。これにより、問題解決にかかる時間を短縮できる可能性があります。

この章で説明する内容は、次のとおりです。

Show Tech-Support 情報の収集

導入：Cisco NX-OS Release 4.0(1)

show tech–support コマンドは、問題の可能性がある事象を診断したり、Cisco TAC ケースに添付する情報を収集するときに役立ちます。**show tech-support** の内容は、通常、非常にサイズが大きく、サイズはシステムを起動していた時間によって異なります。**show tech-support** コマンドでは、**hsrp**、**ospf** などの機能オプションをサポートしています。これは、トラブルシューティングするときに特定の機能に関する情報だけを収集する場合に便利です。

特定の機能に対して **show tech-support** を実行すると、デフォルトでは詳細情報が収集されます。**brief** オプションを指定して、機能に関して収集するデータを少なくすることができます。ただし、このオプションの使用は、通常は推奨しません。すべての機能に対して **show tech-support** を実行するときに、追加のデータを収集する必要がある場合は、**details** オプションを指定する必要があります。

最初の例では、**space-optimized** オプションを使用してすべての機能に関する詳細情報を取得します。2 番目の例では、**ospf** に関する詳細情報を取得し、その情報をフラッシュ（bootflash:）内のファイルにリダイレクトします。

```
n7000# show tech-support details space-optimized

n7000# show tech-support ospf > show-tech-ospf
```

TAC-PAC の生成

導入：Cisco NX-OS Release 4.0(1)

TAC ケースのオープン時には必ず、**tac-pac** を生成してそのファイルを添付します。こうすることで、Cisco TAC エンジニアは、**show tech-support** の出力を依頼しなくても、問題に関する情報を入手できます。**tac-pac** では、役立つ情報が収集され、その情報は圧縮ファイルに保存されます。このため、圧縮ファイルにリダイレクトする **show tech-support** よりも簡単に転送できます。次の例では、圧縮ファイルをフラッシュ（Slot0:）に保存します。

```
n7000# tac-pac slot0:tac-pac-for-tac
```

複数のファイルのアーカイブまたは圧縮

導入：Cisco NX-OS Release 4.0(1)

リモートの宛先にデータを保存するときに複数のファイルをアーカイブおよび圧縮して、転送処理を簡単にすることができます。

```
n7000# show tech hsrp > hsrp-detail.txt
n7000# show tech ospf > ospf-detail.txt

n7000# dir bootflash: | grep detail
    9855855    Nov 02 21:07:40 2010  hsrp-detail.txt
       2703    Nov 02 21:08:11 2010  ospf-detail.txt

n7000# tar create bootflash:tac-info gz-compress bootflash:hsrp-detail.txt
bootflash:ospf-detail.txt

n7000# dir bootflash:tac-info.tar.gz
     860311    Nov 02 21:12:51 2010  tac-info.tar.gz
```

コア ファイルの確認と収集

導入：Cisco NX-OS Release 4.0(1)

プロセスで予期しない再起動またはエラーが発生した場合、Cisco NX-OS によって、イベントに関する詳細情報を含んだコア ファイルが保存されます。コア ファイルの内容は、Cisco TAC エンジニアとソフトウェア開発者がプロセスのエラーを診断するときに役立ちます。コア ファイルはコピーして、TAC ケースに添付する必要があります。次のコマンドでは、コア ファイルがあるかどうかを確認し、リモートの宛先にコピーします。この例では SCP を使用していますが、SFTP、FTP、TFTP などの他のトランスポート プロトコルも使用できます。

```
n7000# show cores

VDC No Module-num       Process-name      PID     Core-create-time

------ ----------       ------------      ---     ---------------
1   8         acltcam     285     Oct 27 09:32


n7000# copy core://8/285 scp://username@x.x.x.x/acltcam-core
```