



Cisco Nexus 7000 シリーズ NX-OS ハイアベイラビリティおよび冗長性ガイド

2011 年 10 月

【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。

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、すべてユーザー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。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. 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。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、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、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

Cisco Nexus 7000 シリーズ NX-OS ハイアベイラビリティおよび冗長性ガイド
Copyright © 2008-2011 Cisco Systems, Inc.
All rights reserved.

Copyright © 2008–2012, シスコシステムズ合同会社.
All rights reserved.



CONTENTS

新機能および変更された機能に関する情報 vii

はじめに ix

対象読者 ix

マニュアルの構成 ix

表記法 x

関連資料 xi

マニュアルの入手方法およびテクニカル サポート xii

CHAPTER 1

概要 1-1

ハイ アベイラビリティについて 1-1

サービスレベル ハイ アベイラビリティ 1-1

プロセスの分離 1-2

プロセスの再起動性 1-2

システムレベルのハイ アベイラビリティ 1-2

物理的な冗長性 1-2

ISSU 1-3

仮想デバイス コンテキスト (VDC) 1-3

ネットワークレベル ハイ アベイラビリティ 1-4

レイヤ 2 HA 機能 1-4

レイヤ 3 HA 機能 1-4

可用性のためのその他の管理ツール 1-4

汎用オンライン診断 (GOLD) 1-5

組み込みイベント マネージャ (EEM) 1-5

Smart Call Home 1-5

CHAPTER 2

サービスレベル ハイ アベイラビリティの理解 2-1

Cisco NX-OS サービスの再起動について 2-1

仮想化のサポート 2-1

ライセンス要件 2-2

再起動性インフラストラクチャ 2-2

システム マネージャ 2-2

永続ストレージ サービス 2-2

メッセージおよびトランザクション サービス 2-3

- HA ポリシー 2-3
- プロセスの再起動性 2-3
 - プロセス再起動の種類 2-4
- スタンバイ スーパーバイザ サービスの再起動 2-5
- スイッチング モジュール サービスの再起動 2-6
- VDC 内サービスの再起動 2-6
- 再起動のトラブルシューティング 2-6
- その他の関連資料 2-7
 - 関連資料 2-7
 - 標準 2-7
 - 管理情報ベース (MIB) 2-7
 - RFC 2-7
 - シスコのテクニカル サポート 2-8

CHAPTER 3

- ネットワーク レベル ハイ アベイラビリティの理解 3-1
 - ネットワーク レベル ハイ アベイラビリティに関する情報 3-1
 - 仮想化のサポート 3-1
 - ライセンス要件 3-1
 - スパニング ツリー プロトコル 3-2
 - 仮想ポート チャネル 3-2
 - ファーストホップ冗長プロトコル 3-3
 - ルーティング プロトコルにおけるノンストップ フォワーディング 3-4
 - OSPFv2 のステートレスな再起動 3-4
 - スイッチオーバーの OSPFv2 グレースフル リスタート 3-4
 - OSPFv2 プロセス障害発生時の OSPFv2 グレースフル リスタート 3-4
 - その他の関連資料 3-5
 - 関連資料 3-5
 - 標準 3-5
 - 管理情報ベース (MIB) 3-5
 - RFC 3-5
 - シスコのテクニカル サポート 3-6

CHAPTER 4

- システム レベル ハイ アベイラビリティの理解 4-1
 - Cisco NX-OS システム レベル ハイ アベイラビリティについて 4-1
 - 仮想化のサポート 4-2
 - ライセンス要件 4-2
 - 物理的な冗長性 4-2
 - 電源装置の冗長構成 4-2

ファントレイの冗長性	4-3
スイッチファブリックの冗長性	4-4
スーパーバイザモジュールの冗長性	4-4
スーパーバイザの再起動とスイッチオーバー	4-4
シングルスーパーバイザでの再起動	4-4
デュアルスーパーバイザでの再起動	4-5
デュアルスーパーバイザでのスイッチオーバー	4-5
デュアルスーパーバイザシステムでのアクティブスーパーバイザモジュールの交換	4-8
デュアルスーパーバイザシステムでのスタンバイスーパーバイザモジュールの交換	4-9
HAステータス情報の表示	4-10
VDCハイアベイラビリティ	4-12
その他の関連資料	4-13
関連資料	4-13
標準	4-13
管理情報ベース (MIB)	4-13
RFC	4-13
シスコのテクニカルサポート	4-14

CHAPTER 5

In-Service Software Upgrade の理解 5-1

ISSU について	5-1
仮想化のサポート	5-1
ライセンス要件	5-2
注意事項および制約事項	5-2
ISSU の動作原理	5-2
ISSU の設定	5-3
ISSU の互換性の判断	5-3
その他の関連資料	5-3
関連資料	5-3
標準	5-3
管理情報ベース (MIB)	5-4
RFC	5-4
シスコのテクニカルサポート	5-4

INDEX



新機能および変更された機能に関する情報

このドキュメントには、『Cisco Nexus 7000 シリーズNX-OS ハイアベイラビリティおよび冗長性ガイド』の新機能と変更された機能についてのリリース固有の情報を記載しています。

表 1-1 には、『Cisco Nexus 7000 シリーズNX-OS ハイアベイラビリティおよび冗長性ガイド』で説明されている新機能と変更された機能およびそれらの記載箇所をまとめています。この表には、各新機能の簡単な説明と変更が行われたリリースも記載しています。

表 1-1 新機能および変更された機能に関する情報

機能	説明	変更されたリリース	参照先
リリース 4.1(4) 以降 変更なし。	—	—	—
仮想ポート チャネ ル	2 つのシステム間に、論理 シングルリンクとして動 作する物理冗長リンクを作 成します。	NX-OS 4.1(4)	第 3 章「ネットワーク レ ベルハイアベイラビリ ティの理解」



はじめに

ここでは、『Cisco Nexus 7000 シリーズ NX-OS ハイアベイラビリティおよび冗長性ガイド』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。

この章では、次の内容について説明します。

- 「対象読者」 (P.ix)
- 「マニュアルの構成」 (P.ix)
- 「表記法」 (P.x)
- 「関連資料」 (P.xi)
- 「マニュアルの入手方法およびテクニカル サポート」 (P.xii)

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

このガイドの構成は次のとおりです。

章とタイトル	説明
第 1 章「概要」	ハイ アベイラビリティ機能を概説します。
第 2 章「サービスレベル ハイ アベイラビリティの理解」	サービス レベル HA を実現する Cisco NX-OS サービスの再起動性について説明します。
第 3 章「ネットワーク レベル ハイ アベイラビリティの理解」	Cisco NX-OS のネットワーク レベル ハイ アベイラビリティについて説明します。
第 4 章「システム レベル ハイ アベイラビリティの理解」	Cisco NX-OS のシステム レベル ハイ アベイラビリティについて説明します。
第 5 章「In-Service Software Upgrade の理解」	In-Service Software Upgrade (ISSU) 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。



(注)

「注釈」を意味します。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。



ヒント

「問題解決に役立つ情報」です。

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。
[]	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	スイッチに表示され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 <i>screen</i> 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。
<>	パスワードなどの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 (!) または番号記号 (#) がある場合は、コメント行であることを示します。

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 6.x』

NX-OS コンフィギュレーション ガイド

『Cisco Nexus 7000 Series NX-OS Configuration Examples, Release 5.x』

『Configuring the Cisco Nexus 2000 Series Fabric Extender』

『Cisco Nexus 7000 Series NX-OS FabricPath Configuration Guide』

『Configuring Feature Set for FabricPath』

『Cisco NX-OS FCoE Configuration Guide for Cisco Nexus 7000 and Cisco MDS 9500』

『Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide, Release 6.x』

『Cisco Nexus 7000 シリーズ NX-OS ハイアベイラビリティおよび冗長性ガイド』

『Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 6.x』

『Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide』

『Cisco Nexus 7000 Series NX-OS LISP Configuration Guide』

『Cisco Nexus 7000 Series NX-OS MPLS Configuration Guide』

『Cisco Nexus 7000 Series NX-OS Multicast Routing Configuration Guide』

『Cisco Nexus 7000 Series NX-OS Software Configuration Guide』

『Cisco Nexus 7000 Series OTV Quick Start Guide』

『Cisco Nexus 7000 Series NX-OS Quality of Service Configuration Guide, Release 6.x』

『Cisco Nexus 7000 Series NX-OS SAN Switching Configuration Guide』

『Cisco Nexus 7000 Series NX-OS Security Configuration Guide, Release 6.x』

『Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x』

『Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 6.x』

『Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide』

『Cisco Nexus 7000 Series NX-OS Virtual Device Context Quick Start』

NX-OS コマンド リファレンス

『Cisco Nexus 7000 Series NX-OS Command Reference Master Index』

『Cisco Nexus 7000 Series NX-OS FabricPath Command Reference』

『Cisco NX-OS FCoE Command Reference for Cisco Nexus 7000 and Cisco MDS 9500』

『Cisco Nexus 7000 Series NX-OS Fundamentals Command Reference』

『Cisco Nexus 7000 Series NX-OS High Availability Command Reference』

『Cisco Nexus 7000 Series NX-OS Interfaces Command Reference』

『Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference』

- 『Cisco Nexus 7000 Series NX-OS LISP Command Reference』
- 『Cisco Nexus 7000 Series NX-OS MPLS Command Reference』
- 『Cisco Nexus 7000 Series NX-OS Multicast Routing Command Reference』
- 『Cisco Nexus 7000 Series NX-OS OTV Command Reference』
- 『Cisco Nexus 7000 Series NX-OS Quality of Service Command Reference』
- 『Cisco Nexus 7000 Series NX-OS SAN Switching Command Reference』
- 『Cisco Nexus 7000 Series NX-OS Security Command Reference』
- 『Cisco Nexus 7000 Series NX-OS System Management Command Reference』
- 『Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference』
- 『Cisco Nexus 7000 Series NX-OS Virtual Device Context Command Reference』

その他のソフトウェアのマニュアル

- 『Cisco NX-OS Licensing Guide』
- 『Cisco Nexus 7000 Series NX-OS MIB Quick Reference』
- 『Cisco Nexus 7000 Series NX-OS Software Upgrade and Downgrade Guide, Release 6.x』
- 『Cisco NX-OS System Messages Reference』
- 『Cisco Nexus 7000 Series NX-OS Troubleshooting Guide』
- 『Cisco NX-OS XML Interface User Guide』

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

Cisco NX-OS は、ネットワーク、システム、プロセスの各レベルにおけるハイ アベイラビリティを実現するために特別に設計された回復性の高いオペレーティング システムです。

この章では、ハイ アベイラビリティ (HA) の概念と Cisco NX-OS デバイスの機能について説明します。この章の構成は次のとおりです。

ハイ アベイラビリティについて

Cisco NX-OS は、ハードウェアまたはソフトウェア障害発生時のトラフィックの中断を防ぐ、または最小限に抑えるため、次の 3 つの機能を備えています。

- 冗長性：Cisco NX-OS HA では、物理的および環境的側面、電源、システム ソフトウェアなどあらゆるコンポーネント レベルにおいて、ハードウェアおよびソフトウェアの冗長性を実現しています。
- 各プレーンおよび各プロセスの分離：Cisco NX-OS HA では、デバイス内の各コントロール転送プレーンと各データ転送プレーン、および各ソフトウェア コンポーネントが分離されているため、あるプレーンで障害が発生しても他のプレーンが中断されることはありません。
- 再起動性：ほとんどのシステム機能およびサービスが分離されているため、エラーが発生しても、他のサービスは実行され続けている中で独立して再起動が可能。さらに、ほとんどのシステム サービスはステートフルな再起動を実行するため、その他のサービスに対して透過的に稼働を再開できます。
- スーパーバイザの SSO：Nexus 7000 シリーズは、アクティブおよびスタンバイのデュアル スーパーバイザ構成をサポートしています。2 つのスーパーバイザ モジュール間で状態と設定が常に同期された状態に維持されるため、スーパーバイザ モジュールの障害発生時にシームレスかつステートフルなスイッチオーバーが可能です。
- 中断なしのアップグレード：Cisco NX-OS では、In-Service Software Upgrade (ISSU) 機能をサポートしています。これにより、スイッチのトラフィック転送動作を継続しながら、デバイス ソフトウェアをアップグレードできます。ISSU を使用すると、ソフトウェアのアップグレードによるダウンタイムを短縮するかゼロにすることができます。

サービスレベル ハイ アベイラビリティ

Cisco NX-OS では、各コンポーネントを区分けするモジュラ方式のアーキテクチャを採用することにより、障害の分離、冗長性、リソースの効率利用を実現しています。

サービスレベル HA の詳細については、[第 2 章「サービスレベル ハイ アベイラビリティの理解」](#)を参照してください。

ここでは、次の内容について説明します。

プロセスの分離

Cisco NX-OS ソフトウェアでは、サービスと呼ばれる独立したプロセスが、サブシステムまたはフィーチャセットの機能またはフィーチャセットを実行します。各サービスおよびサービス インスタンスは、独立した保護プロセスとして実行されます。このアプローチにより、高いフォールトトレラントを備えたソフトウェア インフラストラクチャとサービス間での障害の分離を実現できます。あるサービス インスタンス（802.1Q など）で障害が発生しても、その時点で実行されている他のサービス（Link Aggregation Control Protocol (LACP) など）に影響が及ぶことはありません。また、サービスの各インスタンスは独立したプロセスとして実行できるため、同じルーティング プロトコルの 2 つのインスタンス（たとえば、Open Shortest Path First (OSPF) プロトコルの 2 つのインスタンス）を別々のプロセスとして実行できます。

プロセスの再起動性

Cisco NX-OS のプロセスは、保護メモリ領域内で互いに独立に、またカーネルとも独立に動作します。このようにプロセスが分離されているため、障害が閉じこめられ、迅速な再起動が可能になります。プロセスの再起動性により、プロセスレベルの障害によってシステム全体に障害が及ぶのを防ぐことができます。また、大半のサービスはステートフルな再起動を実行できます。これにより、プラットフォーム内の他のサービス、およびネットワーク内の隣接デバイスへ透過的に、障害の発生したサービスを再起動し、動作を再開できます。

システムレベルのハイ アベイラビリティ

Nexus 7000 シリーズは、冗長なハードウェア コンポーネントとハイ アベイラビリティ ソフトウェア フレームワークによってシステム障害から保護されています。

システム レベル HA 機能の詳細については、[第 4 章「システム レベル ハイ アベイラビリティの理解」](#)を参照してください。

ここでは、次の内容について説明します。

物理的な冗長性

Nexus 7000 シリーズは、次の物理的な冗長性を備えています。

- 電源の冗長性：Cisco Nexus 7000 シリーズ シャーシは、電源モジュールを Cisco Nexus 7010 スイッチで 3 つまで、Cisco Nexus 7018 スイッチで 4 つまで搭載できます。各モジュールは内部的に分離された 2 つの電源ユニットで構成されているため、電源モジュールごとに 2 つの電源経路が、フル装備ではシャーシ全体で 6 つの電源経路が確保されます。
- ファントレイの冗長性：Cisco Nexus 7010 のシャーシには、入出力モジュールの冷却用に 2 つの冗長なシステム ファントレイが備えられており、さらにスイッチ ファブリック モジュールの冷却用に 2 つの冗長なファントレイが備えられています。各ペアのファントレイのどちらか一方が動作していれば、システムは十分に冷却できます。故障した Cisco Nexus 7010 ファントレイを交換する時間制限はありませんが、十分な通気を確保するため、障害が発生したファントレイをそのままにします。

Cisco Nexus 7018 のシャーシには2つのファントレイが備えられています。各トレイは、シャーシ内のモジュールを冷却するために必要です。上部のファントレイはスロット1～9、およびファブリックモジュールを冷却します。下側のファントレイはスロット10～18を冷却します。これらのファントレイはそれぞれホットスワップ可能ですが、取り外し作業を3分以内に完了しないと、スイッチがシャットダウンされます。

- **ファブリックの冗長性**：Cisco NX-OS は、冗長なスイッチファブリックモジュールによってスイッチングファブリックの可用性を実現しています。1台のCisco Nexus 7000シリーズに1～5枚のスイッチファブリックカードを装着して、容量と冗長性を高めることができます。システムに装着された各入出力モジュールは、スイッチファブリックモジュールに自動的に接続され、それらの機能を利用できます。いずれかのスイッチファブリックモジュールで障害が発生すると、残りのアクティブなスイッチファブリックモジュール間で、自動的にトラフィックの再割り当てと均等化が行われます。故障したスイッチファブリックモジュールを置換すると、これとは逆のプロセスが実行されます。新しいファブリックモジュールを装着してオンラインにすると、装着されたすべてのファブリックモジュール間でトラフィックが再配分され、元の冗長性が復元されます。
- **スーパーバイザモジュールの冗長性**：Cisco Nexus 7000シリーズシャーシでは、プレーンの制御および管理機能の冗長性を実現するために、スーパーバイザモジュールを2台搭載できます。デュアルスーパーバイザ構成は、アクティブ/スタンバイ構成で動作します。常に、どちらか一方のスーパーバイザモジュールだけがアクティブ状態にあり、もう一方のモジュールはスタンバイバックアップとして機能します。2つのスーパーバイザモジュール間で状態と設定が常に同期された状態に維持されるため、アクティブなスーパーバイザモジュールの障害発生時にステートフルなスイッチオーバーが可能です。

Nexus 7000シリーズの物理的な冗長性の詳細については、[第4章「システムレベルハイアベイラビリティの理解」](#)を参照してください。

ISSU

Cisco NX-OS を使用すると、In-Service Software Upgrade (ISSU) を実行できます (ISSU は中断なしのアップグレードとも呼ばれます)。Cisco NX-OS では、モジュラ方式のソフトウェアアーキテクチャによって、サービスおよびフィーチャをプラグインベースでサポートしています。これにより、スーパーバイザおよびスイッチングモジュールのイメージの完全なアップグレードを、他のモジュールにほとんど、あるいはまったく影響を与えずに実行できます。この設計によって、データフォワーディングプレーンに影響を及ぼさずに Cisco NX-OS を中断なしにアップグレードができるため、フルバージョンアップのときでも、アップグレード中にフォワーディングを中断せずに済みます。

ISSUの詳細については、[第5章「In-Service Software Upgradeの理解」](#)を参照してください。

仮想デバイスコンテキスト (VDC)

Cisco NX-OS は、デバイスレベルでの論理的な仮想化を実装しています。これにより、物理的に同じスイッチ上で、1つのデバイスで複数のインスタンスを同時に実行できます。こうした論理的な動作環境を仮想デバイスコンテキスト (VDC) と呼びます。VDC では、論理的に切り離されたデバイス環境によって、設定および管理が個別にできます。この高い分離性によって、セキュリティ上および管理上の利点が得られるだけでなく、障害を分離することができます。手動による操作ミスや設定に起因する障害は、所定の仮想デバイス内に隔離されます。仮想デバイスコンテキストは元来、ハイアベイラビリティ機能ではありませんが、障害ドメインが機能的に独立しているため、可用性が向上し、デバイスの設定に関連するサービスの停止を防ぐことができます。

VDCの詳細については、『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.1*』を参照してください。

ネットワークレベル ハイ アベイラビリティ

ネットワーク コンバージェンスは、フェールオーバーとフェールバックを透過的かつ高速にするツールや機能によって最適化されています。

ネットワーク レベル HA 機能の詳細については、[第 3 章「ネットワーク レベル ハイ アベイラビリティの理解」](#)を参照してください。

ここでは、次の内容について説明します。

レイヤ 2 HA 機能

Cisco NX-OS は、次のレイヤ 2 HA 機能を提供しています。

- ブリッジ プロトコル データ ユニット (BPDU) ガード、ループ ガード、ルート ガード、BPDU フィルタ、Bridge Assurance などのスパニング ツリー プロトコル (STP) の改良により、STP コントロール プレーンのヘルス状態を保証
- 単一方向リンク検出 (UDLD) プロトコル
- IEEE 802.3ad リンク アグリゲーション



(注)

Cisco NX-OS Release 4.1(3) 以降のリリースでは、仮想ポート チャネル (vPC) によって、論理シングルリンクとして動作する 2 つのシステム間に物理冗長リンクを作成できます。

レイヤ 3 HA 機能

Cisco NX-OS は、次のレイヤ 3 HA 機能を提供しています。

- ノンストップ フォワーディング (NSF) グレースフル リスタートによるルーティング プロトコルの拡張
OSPFv2、OSPFv3、Intermediate System to Intermediate System (IS-IS)、Enhanced Interior Gateway Routing Protocol (EIGRP)、および Border Gateway Protocol (BGP) は、基本プロトコルに対してグレースフル リスタート拡張を適用して、それぞれの環境で、ノンストップ フォワーディングと中断を最小限にするルーティング リカバリを実現します。
- 最短パス優先 (SPF) の最適化。リンクステートアドバタイズメント (LSA) ペーシングや SPF の増大など。
- プロトコル ベースの定期リフレッシュ
- ホットスタンバイ ルータ プロトコル (HSRP)、ゲートウェイ ロード バランシング プロトコル (GLBP)、仮想ルータ冗長プロトコル (VRRP) などのファーストホップ冗長プロトコル (FHRP) 用のタイマー (ミリ秒)。

可用性のためのその他の管理ツール

Cisco NX-OS には、システム可用性イベントのモニタリングと通知を行うシスコのシステム管理ツールがいくつか組み込まれています。

ここでは、次の内容について説明します。

汎用オンライン診断 (GOLD)

汎用オンライン診断 (GOLD) サブシステムとスーパーバイザ上の追加のモニタリング プロセスによって、回復不可能な重大な障害、サービス再起動エラー、カーネル エラー、ハードウェア障害が検出されると、冗長なスーパーバイザへのステートフル フェールオーバーの起動が容易になります。

GOLD の設定の詳細については、『*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x*』を参照してください。

組み込みイベント マネージャ (EEM)

Cisco Embedded Event Manager (EEM; 組み込みイベント マネージャ) は、Event Detector (イベントディテクタ)、Event Manager (イベント マネージャ)、Event Manager Policy Engine (イベント マネージャ ポリシー エンジン) で構成されます。EEM を使用すると、システム ソフトがイベントディテクタを介して特定のイベントを察知したときに、特定のアクションを実行するポリシーを定義できます。これにより、多数のネットワーク管理タスクを自動化し、Cisco NX-OS の動作を管理して可用性の向上、情報の収集、重要なイベントの外部システムまたは個人への通知が柔軟に行える、ツールセットが実現します。

EEM の設定の詳細については、『*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x*』を参照してください。

Smart Call Home

Cisco GOLD および Cisco EEM の機能を組み合わせた Smart Call Home は、重要なシステム イベントを E メールで通知するためのツールです。メッセージ形式には、ポケットベル サービス、標準の E メール、または XML ベースの自動解析アプリケーションと互換性があります。この機能を使用して、ネットワーク サポート エンジニアをポケットベルで呼び出したり、ネットワーク オペレーション センターに E メールで通知したりできます。また、Cisco Smart Call Home のサービスを使用すると、Cisco Technical Assistance Center (TAC) に自動的に障害を報告できます。

Smart Call Home の設定の詳細については、『*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x*』を参照してください。



CHAPTER 2

サービスレベルハイ アベイラビリティの理解

この章では、サービス レベル ハイ アベイラビリティ (HA) を実現する Cisco NX-OS サービスの再起動性について説明します。この章の構成は次のとおりです。

Cisco NX-OS サービスの再起動について

Cisco NX-OS サービス再起動機能では、スーパーバイザを再起動せずに障害の発生したサービスを再起動することによって、プロセス レベルの障害がシステム レベルの障害に拡大するのを防ぐことができます。サービスは、現在のエラー、障害状況、サービスのハイ アベイラビリティ ポリシーに基づいて再起動できます。サービスの再起動には、ステートフルな再起動とステートレスな再起動があります。Cisco NX-OS では、サービスが実行時の状態情報とメッセージを保存することで、ステートフルな再起動を実現しています。ステートフルな再起動では、サービスが保存されていた状態情報を取り出して、直前のチェックポイント サービス状態から動作を再開します。ステートレスな再起動では、サービスは、初めて起動するときのように、初期化および実行されます。

すべてのサービスがステートフルな再起動が可能のように設計されているわけではありません。たとえば、Cisco NX-OS は、3 層ルーティング プロトコル (Open Shortest Path First (OSPF) や Routing Information Protocol (RIP) など) の実行時の状態情報を保存しません。これらのプロトコルは、再起動のあとも設定は維持されますが、動作状態については隣接するルータから情報を取得して再構築するように設計されています。3 層プロトコルのハイ アベイラビリティ機能の詳細は、[第 3 章「ネットワーク レベル ハイ アベイラビリティの理解」](#)を参照してください。

仮想化のサポート

仮想デバイス コンテキスト (VDC) におけるサービス レベル ハイ アベイラビリティの詳細は、「VDC 内サービスの再起動」(P.2-6) を参照してください。



(注) およびリソースの割り当ての詳細については、『Cisco DCNM Virtual Device Context Configuration Guide』を参照してください。



(注) VDC の詳細については、『Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.1』を参照してください。

ライセンス要件

次の表に、サービス レベル ハイ アベイラビリティ機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	サービス レベル HA 機能にライセンスは必要ありません。ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。
VDC	VDC にはアドバンスド サービス ライセンスが必要です。

Cisco NX-OS のライセンス スキームの詳細は、『Cisco NX-OS Licensing Guide』を参照してください。

再起動性インフラストラクチャ

Cisco NX-OS では、大部分のプロセスおよびサービスのステートフルな再起動が可能です。プラットフォーム内のプロセス、サービス、アプリケーションのバックエンドでの管理および調整は、このセクションで説明する一連の高レベルのシステム コントロール サービスによって実行されます。

ここでは、次の内容について説明します。

システム マネージャ

システム マネージャは、あらゆるシステム機能、システム管理、システム ヘルス モニタリングの実行を制御し、ハイ アベイラビリティ ポリシーを実施します。システム マネージャは、サービスの起動、停止、モニタリング、再起動を担当し、サービス ステートとスーパーバイザ ステートの同期を管理および起動して SSO を実現します。

永続ストレージ サービス

Cisco NX-OS サービスは、永続ストレージ サービス (PSS) を使用して、運用の実行時情報を保存および管理します。PSS コンポーネントは、システム サービスを使用して、サービス再起動時に状態を回復します。PSS は状態および実行時情報のデータベースとして機能します。これにより、各サービスは、必要なときにいつでも、サービス自体の状態情報のチェックポイントを作成できます。サービスを再起動すると、障害が発生する直前の既知の動作状態を回復できるので、ステートフルな再起動が可能になります。

PSS を使用する各サービスは、保存された情報をプライベート情報 (当サービスだけ読み取り可能) または共有情報 (他のサービスも読み取り可能) として定義できます。情報を共有する場合は、ローカル (同一スーパーバイザ上のサービスだけ読み取り可能) またはグローバル (スーパーバイザまたはモジュール上のサービスが読み取り可能) のどちらかを指定できます。たとえば、アクティブなスーパーバイザ上で実行されているサービスの PSS 情報を共有かつグローバルとして定義すると、他のモジュール上のサービスは、その PSS 情報と同期することができます。

メッセージおよびトランザクション サービス

メッセージおよびトランザクション サービス (MTS) は、ハイ アベイラビリティ セマンティクスに特化した高パフォーマンス プロセス間通信 (IPC) メッセージ ブローカです。MTS は、モジュール内とモジュール間、およびスーパーバイザ間でメッセージのルーティングとキューイングを行います。また、イベント通知や同期などのメッセージ交換を容易にし、システム サービス間およびシステム コンポーネント間のメッセージ永続性を促進します。MTS では、永続メッセージおよびログ メッセージをキュー内に保管できるため、サービスの再起動後もそれらのメッセージにアクセスできます。

HA ポリシー

Cisco NX-OS では、各サービスに、障害の発生したサービスの再起動方法を定義する一連の内部 HA ポリシーのセットを作成できます。サービスごとに4つの定義済みポリシーを用意できます。つまり、スーパーバイザが2つの場合のプライマリ ポリシーとセカンダリ ポリシー、スーパーバイザが1つだけの場合のプライマリ ポリシーとセカンダリ ポリシーです。HA ポリシーが定義されていないサービスでは、サービスの障害発生時に実行されるデフォルトの HA ポリシーは、スーパーバイザが2つの場合はスイッチオーバー、スーパーバイザが1つの場合はスーパーバイザのリセットとなります。

HA ポリシーには、次の3つのパラメータを指定します。

- システム マネージャによって実行されるアクション：
 - ステートフルな再起動
 - ステートレスな再起動
 - スーパーバイザのスイッチオーバー (または再起動)
- 最大再試行回数：システム マネージャによって実行される再起動試行回数を指定します。再試行をその回数行ってもサービスが正常に再起動しない場合、その HA ポリシーは失敗したものと見なされ、定義されている次の HA ポリシーが使用されます。他の HA ポリシーが定義されていない場合はデフォルトのポリシーが適用されます。つまり、スーパーバイザのスイッチオーバーまたは再起動が実行されます。
- 最小ライフタイム：再起動の試行のあとに、実行する必要があるサービス時間を指定します。最小ライフタイムは最低でも4分です。

プロセスの再起動性

プロセスの再起動性により、データ プレーンやその他のサービスを中断せずに、障害の発生したサービスを回復し動作を再開することができます。システム マネージャは、サービスの HA ポリシー、前回の再起動の失敗、同じスーパーバイザ上で実行されているその他のサービスのヘルス状態に応じて、サービスの障害発生時に実行するアクションを決定します。

表 2-1 に、さまざまな障害発生時にシステム マネージャによって実行されるアクションを示します。

表 2-1 さまざまな障害におけるシステム マネージャのアクション

障害	アクション
サービス/プロセスの例外	サービスの再起動
サービス/プロセスのクラッシュ	サービスの再起動
サービス/プロセスの応答がない	サービスの再起動

表 2-1 さまざまな障害におけるシステムマネージャのアクション (続き)

障害	アクション
サービスの障害が繰り返される	スーパーバイザのリセット (シングルスーパーバイザの場合) またはスイッチオーバー (デュアルスーパーバイザの場合)
システムマネージャからの応答がない	スーパーバイザのリセット (シングルスーパーバイザの場合) またはスイッチオーバー (デュアルスーパーバイザの場合)
スーパーバイザのハードウェア障害	スーパーバイザのリセット (シングルスーパーバイザの場合) またはスイッチオーバー (デュアルスーパーバイザの場合)
カーネル障害	スーパーバイザのリセット (シングルスーパーバイザの場合) またはスイッチオーバー (デュアルスーパーバイザの場合)
ウォッチドッグタイムアウト	スーパーバイザのリセット (シングルスーパーバイザの場合) またはスイッチオーバー (デュアルスーパーバイザの場合)

ここでは、次の内容について説明します。

プロセス再起動の種類

障害の発生したサービスは、HAの実装およびHAポリシーに応じて、ここで説明するいずれかの方法で再起動されます。

ここでは、次の内容について説明します。

ステートフルな再起動

再起動可能なサービスで障害が発生すると、サービスは同じスーパーバイザ上で再起動されます。サービスの新しいインスタンスは、以前のインスタンスがオペレーティングシステムによって異常終了させられたと判断した場合、永続コンテキストがあるかどうかを確認します。新しいインスタンスは初期化時に永続コンテキストを読み込んで、実行時コンテキストを構築します。この結果、新しいインスタンスは障害発生前のインスタンスと同じ状態になります。初期化が完了すると、サービスは、停止したときに実行していたタスクを再開します。新しいインスタンスが再起動および初期化されている間、他のサービスは、そのような障害が発生していることを認識していません。他のサービスから障害が発生したサービスに送信されたメッセージは、サービスが再開された時点でMTSから取得できます。

新しいインスタンスでステートフルな初期化を完了できるかどうかは、前のインスタンスの障害の原因に依存します。サービスで再起動を数回実行できない場合、そのサービスの再起動は失敗したと見なされます。その場合、システムマネージャは、再起動に失敗したサービスのHAポリシーに指定されたアクション (ステートレスな再起動、再起動しない、スーパーバイザのスイッチオーバーまたはリセットのいずれか) を実行します。

ステートフルな再起動に成功した場合、システムが矛盾のない状態に到達するまでに遅延が発生することはありません。ステートフルな再起動により、障害発生後の回復に要する時間が短縮されます。

ステートフルな再起動の前後および最中に発生するイベントは次のとおりです。

1. 実行中のサービスが、実行時状態情報のチェックポイントをPSSに作成します。
2. システムマネージャが、ハートビートを使用している実行中サービスのヘルス状態を監視します。

3. システム マネージャが、クラッシュまたはハングしたサービスを即座に再起動します。
4. 再起動のあとに、サービスは、PSS から状態情報を回復し、保留中のすべてのトランザクションを再開します。
5. 何度か再起動してもサービスの動作が安定しない場合、システム マネージャはスーパーバイザのリセットまたはスイッチオーバーを開始します。
6. Cisco NX-OS はプロセス スタックとコアをデバッグ用に収集します。また、オプションでコア ファイルをリモートに転送します。

ステートフルな再起動が発生すると、Cisco NX-OS がレベル LOG_ERR の Syslog メッセージを送信します。SNMP トラップがイネーブルになっている場合は、SNMP エージェントがトラップを送信します。Smart Call Home サービスがイネーブルになっている場合は、サービスがイベント メッセージを送信します。

ステートレスな再起動

Cisco NX-OS インフラストラクチャ コンポーネントは、ステートレスな再起動を管理します。ステートレスな再起動中、システム マネージャは、障害の発生したプロセスを特定し、新しいプロセスに置き換えます。障害の発生したサービスは再起動時に実行時状態を保持していません。実行中のコンフィギュレーションから実行時状態を構築するか、必要なら、他のサービスと情報を交換して実行時状態を構築します。

ステートレスな再起動が発生すると、Cisco NX-OS がレベル LOG_ERR の Syslog メッセージを送信します。SNMP トラップがイネーブルになっている場合は、SNMP エージェントがトラップを送信します。Smart Call Home サービスがイネーブルになっている場合は、サービスがイベント メッセージを送信します。

スイッチオーバー

スタンバイ スーパーバイザが使用可能な場合で、複数の障害が同時に発生したときには、Cisco NX-OS は常に、スーパーバイザの再起動ではなくスーパーバイザのスイッチオーバーを実行します。こうしたケースは、同一スーパーバイザ上では回復不可能と見なされるからです。たとえば、複数の HA アプリケーションで障害が発生すると、回復不可能と見なされます。

スーパーバイザのスイッチオーバーおよび再起動の詳細については、第4章「システム レベルハイ アベイラビリティの理解」を参照してください。

スタンバイ スーパーバイザ サービスの再起動

スタンバイ状態のスーパーバイザ上のサービスで障害が発生した場合、システム マネージャは HA ポリシーを適用せず、30 秒待ってからサービスを再起動します。30 秒待つことで、スタンバイ サービスの障害と同期化が繰り返されたとき、アクティブなスーパーバイザが対応しきれなくなるのを避けることができます。再起動されるサービスをアクティブなスーパーバイザ上のサービスと同期させる必要がある場合、スタンバイ スーパーバイザは、当該サービスの再起動と同期化が完了するまでホットスタンバイ モードではなくなります。サービスが再起動不可能な場合は、スタンバイ スーパーバイザがリセットされます。

スタンバイ サービスの再起動が発生すると、Cisco NX-OS はレベル LOG_ERR の Syslog メッセージを送信します。SNMP トラップがイネーブルになっている場合は、SNMP エージェントがトラップを送信します。Smart Call Home サービスがイネーブルになっている場合は、サービスがイベント メッセージを送信します。

スイッチング モジュール サービスの再起動

スイッチング モジュールまたは別の非スーパーバイザ モジュール上でサービスの障害が発生した場合は、それらのサービスの HA ポリシーによって回復アクションが決まります。非スーパーバイザ モジュール上でサービスの障害が発生した場合は、スーパーバイザのスイッチオーバーは必要ないため、回復方法は、ステートフルな再起動、ステートレスな再起動、モジュールのリセットのいずれかになります。中断なしにアップグレード可能なモジュールは、中断なしに再起動も可能です。

モジュール サービスの中断なしの再起動が発生すると、Cisco NX-OS はレベル LOG_ERR の Syslog メッセージを送信します。SNMP トラップがイネーブルになっている場合は、SNMP エージェントがトラップを送信します。Smart Call Home サービスがイネーブルになっている場合は、サービスがイベント メッセージを送信します。

VDC 内サービスの再起動

サービスで障害が発生し、すべての HA ポリシーでサービスの再起動が失敗に終わった場合、次に実行されるアクションは、通常、スーパーバイザの再起動またはスイッチオーバーです。しかし、VDC 内で実行されているサービスの場合は、スーパーバイザの再起動またはスイッチオーバーを実行する前に VDC の再起動を試行するよう、VDC ポリシーに指定できます。

VDC の詳細については、『Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.1』を参照してください。

再起動のトラブルシューティング

サービスで障害が発生すると、システムは障害の原因を判定するために使用できる情報を生成します。次の情報ソースが使用可能です。

- サービスの再起動によって、LOG_ERR レベルの Syslog メッセージが生成されます。
- Smart Call Home サービスがイネーブルになっている場合は、サービスの再起動によって Smart Call Home イベントが生成されます。
- SNMP トラップがイネーブルになっている場合は、サービスが再起動されると、SNMP エージェントがトラップを送信します。
- サービスの障害がローカル モジュール上で発生した場合は、そのモジュール内で **show processes log** コマンドを入力することで、イベントのログを表示できます。プロセスのログは、スーパーバイザのスイッチオーバーまたはリセット後も保持されます。
- サービスの障害が発生すると、システムのコア イメージファイルが生成されます。最新のコア イメージを表示するには、アクティブなスーパーバイザ上で **show cores** コマンドを使用します。コア ファイルはスーパーバイザのスイッチオーバーまたはリセット後は削除されますが、Trivial File Transfer Protocol (TFTP) などのファイル転送ユーティリティを使用してコア ファイルを外部サーバにエクスポートするようにシステムを設定することもできます。
- CISCO-SYSTEM-MIB には、コアのテーブルが含まれています (cseSwCoresTable)。

サービスの障害に関する情報を収集および使用についての詳細は、『Cisco Nexus 7000 Series NX-OS Troubleshooting Guide』を参照してください。

その他の関連資料

サービスレベルの HA 機能の実装に関する詳細は、次の各セクションを参照してください。

関連資料

関連項目	参照先
仮想デバイス コンテキスト (VDC)	『Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.1』
スーパーバイザ スイッチオーバー	第 4 章 「システム レベル ハイ アベイラビリティの理解」
トラブルシューティング	『Cisco Nexus 7000 Series NX-OS Troubleshooting Guide』
Cisco NX-OS の基礎	『Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide, Release 6.x』
ライセンス	『Cisco NX-OS Licensing Guide』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

管理情報ベース (MIB)

MIB	MIB のリンク
<ul style="list-style-type: none"> CISCO-SYSTEM-EXT-MIB : ciscoHaGroup、cseSwCoresTable、cseHaRestartNotify、cseShutDownNotify、cseFailSwCoreNotify、cseFailSwCoreNotifyExtended CISCO-PROCESS-MIB CISCO-RF-MIB 	<p>MIB を検索およびダウンロードするには、次の URL にアクセスしてください。</p> <p>http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</p>

RFC

RFC	タイトル
この機能によってサポートされている RFC はありません。	—

シスコのテクニカル サポート

説明	リンク
TAC のホームページには、3 万ページに及ぶ検索可能な技術情報があります。製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクもあります。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/cisco/web/support/index.html



CHAPTER 3

ネットワーク レベルハイ アベイラビリティの理解

この章では、Cisco NX-OS ネットワークのハイ アベイラビリティについて説明します。この章の構成は次のとおりです。

ネットワーク レベルハイ アベイラビリティに関する情報

Cisco NX-OS のネットワーク レベルハイ アベイラビリティ (HA) は、フェールオーバーおよびフォールバックを透過的かつ迅速に行うツールや機能によって最適化されています。この章で説明する機能によって、ネットワーク レベルのハイ アベイラビリティが保証されます。

仮想化のサポート

システム内の各仮想デバイス コンテキスト (VDC) は、それぞれ別個のスパニング ツリー プロトコル (STP) を実行します。VDC には、バーチャライゼーション サポートの拡張も含まれています。各 VDC は、ルーティング プロトコルの 1 つ以上のインスタンスを実行することもできます。この章で説明するネットワーク レベル HA 機能は、システムの障害や再起動と同じように、VDC の障害や再起動に使用されます。



(注) VDC の詳細については、『Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.1』を参照してください。

ライセンス要件

次の表に、ネットワーク レベルハイ アベイラビリティ機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	ネットワーク レベル HA 機能にライセンスは必要ありません。ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。
VDC	VDC にはアドバンスド サービス ライセンスが必要です。
BGP	ボーダー ゲートウェイ プロトコル (BGP) には、エンタープライズ サービス ライセンスが必要です。

Cisco NX-OS のライセンス スキームとライセンスの取得および適用方法の詳細は、『Cisco NX-OS Licensing Guide』を参照してください。

スパニング ツリー プロトコル



(注)

スパニング ツリー プロトコル (STP) は、IEEE 802.1w および IEEE 802.1s 規格に準拠しているものを指します。このマニュアルで IEEE 802.1D STP を指す場合は、802.1D と明記します。

耐障害性のあるネットワーク接続を実現するには、ネットワーク内のすべてのノード間のパスでループが発生しないようにする必要があります。端末間に複数のアクティブなパスが存在すると、ネットワーク内でループが発生し、その結果、各ネットワーク デバイスが複数のレイヤ 2 LAN ポート上の端末 MAC アドレスを学習します。そうした状態になるとブロードキャスト ストームが発生し、ネットワークの状態が不安定になります。

STP は、レイヤ 2 レベルで、ループのないネットワークを実現します。レイヤ 2 LAN ポートは STP フレーム (Bridge Protocol Data Unit (BPDU; ブリッジ プロトコル データ ユニット)) を一定の時間間隔で送受信します。ネットワーク デバイスはこれらのフレームを転送せず、これらのフレームを使用してネットワーク トポロジを決定し、そのトポロジ内でループのないパスを形成します。スパニング ツリー トポロジを使用することで、STP は、冗長なデータ パスをブロックされた状態にします。スパニング ツリーのネットワーク セグメントに障害が発生した場合、冗長パスがあると、STP アルゴリズムにより、スパニング ツリー トポロジが再計算され、ブロックされたパスがアクティブになります。

Cisco NX-OS は、多重スパニング ツリー プロトコル (MSTP) もサポートしています。MSTP によって実現される複数の独立したスパニング ツリー トポロジは、データ トラフィック用に複数の転送パスを提供し、ロード バランシングを有効化して、多数の VLAN をサポートするために必要な STP インスタンスの数を軽減します。

MST には、高速スパニング ツリー プロトコル (RSTP) が組み込まれています。これにより、高速なコンバージェンスが可能になります。MST では、1 つのインスタンス (フォワーディング パス) での障害が他のインスタンス (フォワーディング パス) に影響しないため、ネットワークの耐障害性が向上します。



(注)

スパニング ツリーの各パラメータはレイヤ 2 インターフェイスに対してだけ設定できます。レイヤ 3 インターフェイスに対してスパニング ツリーの設定を行うことはできません。レイヤ 2 インターフェイスの作成方法の詳細については、『Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 6.x』を参照してください。

STP の動作と設定の詳細については、『Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide』を参照してください。

仮想ポート チャネル

従来のポート チャネル通信においては、ポート チャネルが 2 つのデバイス間でしか動作しないという大きな制約があります。大規模なネットワークでは、何らかの形でハードウェア障害の代替パスを確保するために、設計上複数のデバイスを同時にサポートする必要がある場合があります。この代替パスは、ループを形成するように接続され、ポート チャネル テクノロジーの長所を単一パスに制限することがあります。この制限に対処するために、Cisco NX-OS は、仮想ポート チャネル (vPC) というテクノロジーを備えています。vPC ピア エンドポイントとして機能する 1 組のスイッチは、ポートチャ

ネル接続デバイスへの単一の論理エンティティのように見えますが、論理ポート チャネル エンドポイントとして動作する 2 つのデバイスは 2 つの個別のデバイスです。この環境はハードウェアの冗長性の利点とポート チャネル ループ管理の利点を組み合わせます。

vPC の詳細については、『Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 6.x』を参照してください。

ファーストホップ冗長プロトコル

2 台以上のルータ グループ内では、ファーストホップ冗長プロトコル (FHRP) によって、ファーストホップ IP ルータの透過的なフェールオーバーを実現できます。Cisco NX-OS では、次の FHRP をサポートしています。

- ホットスタンバイ ルータ プロトコル (HSRP) : HSRP は、デフォルト ゲートウェイ IP アドレスが設定されたイーサネット ネットワーク上の各 IP ホストに対し、ファーストホップ ルーティング 冗長性を実現します。2 つ以上のルータで構成される HSRP ルータ グループの中から、アクティブ ゲートウェイとスタンバイ ゲートウェイが選択されます。アクティブ ゲートウェイがパケットのルーティングを行います。スタンバイ ゲートウェイは、アクティブ ゲートウェイで障害が発生するまで、あるいは事前の条件が一致すると、アイドル状態を維持します。

大部分のホストの実装では、ダイナミックなルータ ディスカバリ メカニズムをサポートしていませんが、デフォルトのルータを設定することはできます。すべてのホスト上でダイナミックなルータ ディスカバリ メカニズムを実行するのは、管理上のオーバーヘッド、処理上のオーバーヘッド、セキュリティ上の問題など、さまざまな理由で適切ではありません。HSRP は、そうしたホスト上にフェールオーバー サービスを提供します。

- 仮想ルータ冗長プロトコル (VRRP) : VRRP は、1 つ以上の仮想ルータの役割を LAN 上の VRRP ルータにダイナミックに割り当てます。これにより、マルチアクセス リンク上の複数のルータが同じ仮想 IP アドレスを使用できるようになります。VRRP ルータは、LAN に接続された 1 つ以上の他のルータと連係して VRRP を実行するように構成できます。1 台のルータが仮想ルータ マスターとして選択され、残りのルータは仮想ルータ マスターで障害が発生したときのバックアップとして動作します。
- ゲートウェイ ロード バランシング プロトコル (GLBP) : GLBP は、冗長なゲートウェイ間でプロトコルとメディア アクセス コントロール (MAC) アドレスを共有することで、IP のパス冗長性を実現します。また、GLBP を使用すると、レイヤ 3 ルータ グループで、LAN 上のデフォルト ゲートウェイの負荷を分担できます。GLBP ルータは、グループ内の別のルータで障害が発生したとき、そのルータのフォワーディング機能を自動的に引き継ぎます。

GLBP は HSRP および VRRP とほぼ同じ機能を実行します。つまり、複数のルータが、仮想 IP アドレスの設定された仮想グループに参加できます。ただし、GLBP は、HSRP および VRRP が提供していないロード バランシング機能も実行します。GLBP では、グループ内のすべてのルータ間でフォワーディングの負荷を分担します。アイドル状態のルータが他に存在しているにもかかわらず 1 台のルータにすべてのフォワーディング負荷を処理させることはありません。HSRP と VRRP では、1 台のメンバーをアクティブなルータとして選択し、グループの仮想 IP アドレスにパケットをフォワーディングします。グループ内の他のルータは、アクティブ ルータで障害が発生するまでは冗長ルータです。

FHRP の設定の詳細については、『Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 6.x』を参照してください。

ルーティング プロトコルにおけるノンストップ フォワーディング

Nexus 7000 シリーズ では、Open Shortest Path First バージョン 2 (OSPFv2)、Enhanced Interior Gateway Routing Protocol (Enhanced IGRP)、Border Gateway Protocol (BGP; ボーダー ゲートウェイ プロトコル) をサポートしています。これらの各プロトコルには、ネットワーク レベルの HA メカニズムが組み込まれており、プロセスの再起動やスーパーバイザのスイッチオーバーに起因するネットワークの停止を最小限に抑えます。

ここでは、例として、OSPFv2 の HA 機能について説明します。OSPFv2、EIGRP、および BGP の HA 設定の詳細については、『Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 6.x』の「High Availability and Graceful Restart」の章を参照してください。

ここでは、次の内容について説明します。

OSPFv2 のステートレスな再起動

OSPFv2 を実行している Cisco NX-OS システムがコールドリブートされると、ネットワークは、そのシステムへのトラフィックの転送を停止して、ネットワーク トポロジからそのシステムを除外します。このシナリオでは、OSPFv2 はステートレスな再起動を実行し、ローカル システム上のネイバールータとの隣接関係をすべて削除します。Cisco NX-OS は、スタートアップ コンフィギュレーションを適用し、OSPFv2 はネイバーを再検出して、隣接関係を再確立します。

スイッチオーバーの OSPFv2 グレースフル リスタート

スーパーバイザのスイッチオーバーが開始されると、OSPFv2 は、自身が一時的に使用不能になることを知らせて、グレースフル リスタートまたはノンストップ フォワーディング (NSF) を起動します。スイッチオーバーの間も、各ネイバードバイスはトラフィックを転送し続け、システムはネットワーク トポロジ内に存続したままです。スイッチオーバーが完了すると、Cisco NX-OS は実行コンフィギュレーションを適用し、OSPFv2 は自身が再度使用可能になったことをネイバーに通知します。ネイバーは隣接関係の再確立を補助します。

OSPFv2 プロセス障害発生時の OSPFv2 グレースフル リスタート

OSPFv2 は、プロセスで問題が発生すると、自動的に再起動します。再起動のあとに、OSPFv2 は、プラットフォームがネットワーク トポロジから除外されないように、グレースフル リスタートを起動します。OSPF を手動で再起動した場合は、グレースフル リスタートが実行されます。これは、機能的には SSO と同じです。どちらの場合も、実行コンフィギュレーションが適用されます。グレースフル リスタートによって、OSPFv2 は、プロセスの再起動中でもデータ フォワーディング パス内に存在し続けます。



(注)

再起動中の OSPFv2 インターフェイスが猶予期間の終了前に復旧しない場合、またはネットワークのトポロジが変更された場合は、OSPFv2 ネイバーは再起動中の OSPFv2 との隣接関係を切断し、通常の OSPFv2 の再起動として処理します。

その他の関連資料

ネットワーク レベルの HA 機能の実装に関する詳細は、次のセクションを参照してください。

関連資料

関連項目	参照先
仮想デバイス コンテキスト (VDC)	『Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.1』
グレースフル リスタート	『Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 6.x』の「High Availability and Graceful Restart」の章
In-service Software Upgrade (ISSU)	第 5 章「In-Service Software Upgrade の理解」
ライセンス	『Cisco NX-OS Licensing Guide』

標準

標準	タイトル
IEEE 802.1Q-2006 (旧称 IEEE 802.1s)、IEEE 802.1D-2004 (旧称 IEEE 802.1w)、IEEE 802.1D、IEEE 802.1t	—

管理情報ベース (MIB)

MIB	MIB のリンク
<ul style="list-style-type: none"> CISCO-SYSTEM-EXT-MIB : ciscoHaGroup、cseSwCoresTable、cseHaRestartNotify、cseShutDownNotify、cseFailSwCoreNotify、cseFailSwCoreNotifyExtended CISCO-STP-EXTENSION-MIB CISCO-PROCESS-MIB CISCO-RF-MIB 	<p>MIB を検索およびダウンロードするには、次の URL にアクセスしてください。</p> <p>http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</p>

RFC

RFC	タイトル
この機能によってサポートされている RFC はありません。	—

シスコのテクニカル サポート

説明	リンク
TAC のホームページには、3 万ページに及ぶ検索可能な技術情報があります。製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクもあります。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/cisco/web/support/index.html



CHAPTER 4

システム レベル ハイ アベイラビリティの理解

この章では、Cisco NX-OS HA システムおよびアプリケーションの再起動操作について説明します。この章の構成は次のとおりです。

Cisco NX-OS システム レベル ハイ アベイラビリティについて

Cisco NX-OS システム レベル ハイ アベイラビリティ (HA) は、ハードウェアおよびソフトウェア障害の影響を軽減します。サポートされている機能は次のとおりです。

- 冗長なハードウェア コンポーネント :

- スーパーバイザ
- スイッチ ファブリック
- 電源装置
- ファントレイ

物理要件および冗長なハードウェア コンポーネントの詳細については、それぞれ、『Cisco Nexus 7000 Series Site Preparation Guide』および『Cisco Nexus 7000 Series Hardware Installation and Reference Guide』を参照してください。

- HA ソフトウェア機能 :

- In-Service Software Upgrade (ISSU) : 中断なしのアップグレードのコンフィギュレーションと実行については、第 5 章「[In-Service Software Upgrade の理解](#)」を参照してください。
- ノンストップ フォワーディング (NSF) : ノンストップ フォワーディング (別名 グレースフル リスタート) については、『Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 6.x』を参照してください。
- 仮想デバイス コンテキスト (VDC) : VDC と HA については、『Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.1』を参照してください。
- 汎用オンライン診断 (GOLD) : GOLD の設定については、『Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x』を参照してください。
- 組み込みイベント マネージャ (EEM) : EEM の設定については、『Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x』を参照してください。
- Smart Call Home : Smart Call Home の設定については、『Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x』を参照してください。

仮想化のサポート

仮想デバイス コンテキスト (VDC) におけるシステム レベル ハイ アベイラビリティの詳細は、「[VDC ハイ アベイラビリティ](#)」(P.4-12) を参照してください。



(注) VDC の詳細については、『[Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.1](#)』を参照してください。

ライセンス要件

次の表に、システム レベル ハイ アベイラビリティ機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	VDC と Smart Call Home を除き、システム レベル ハイ アベイラビリティ機能にライセンスは必要ありません。ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。
VDC	VDC にはアドバンスド サービス ライセンスが必要です。
Smart Call Home	Smart Call Home は、Cisco SMARTnet Service および Cisco SP Base Service を介して利用できます。

Cisco NX-OS ライセンス方式、およびライセンスの取得方法と適用方法の詳細については、『[Cisco NX-OS Licensing Guide](#)』を参照してください。

物理的な冗長性

Nexus 7000 シリーズは、次の物理的な冗長性を備えています。

物理的な冗長性の詳細については、『[Cisco Nexus 7000 Series Site Preparation Guide](#)』および『[Cisco Nexus 7000 Series Hardware Installation and Reference Guide](#)』を参照してください。

電源装置の冗長構成

Nexus 7000 シリーズ は、電源モジュールを Cisco Nexus 7010 スイッチで 3 つまで、Cisco Nexus 7018 スイッチで 4 つまで搭載できます。各電源モジュールは、入力数と入力電圧に応じて、7.5 KW まで出力できます。2 つまたは 3 つの電源モジュールを装着することで、いずれか 1 つのモジュールで障害が発生してもシステムの動作が停止することはありません。障害の発生した電源モジュールはシステムを稼働させたまま交換できます。電源モジュールの装着と交換については、『[Cisco Nexus 7000 Series Hardware Installation and Reference Guide](#)』を参照してください。

冗長性を高めるため、各電源モジュールは内部が 2 つにわかれた電源ユニットで構成されています。これにより、電源モジュールごとに 2 つの電源経路が、フル装備ではシャーシ全体で 6 つの電源経路が確保されます。また、電源サブシステムにより、3 つの電源装置を、4 つのうちいずれかの冗長モードで構成できます。

電源モード

4つの電源冗長モードはそれぞれ、異なる電力バジェットと割り当てモデルを使用しており、使用可能な出力と容量も異なります。電力バジェット、使用可能な容量、要件計画、冗長構成の詳細については、『*Cisco Nexus 7000 Series Hardware Installation and Reference Guide*』を参照してください。

表 4-1 に、使用可能な電源装置冗長モードについて説明します。

表 4-1 電源の冗長モード

冗長モード	説明
複合	このモードは電源の冗長性を提供しません。使用可能な電力は、すべての電源装置の電力の合計です。
insrc-redundant	このモードでは2つの電気回路網を使用します。1つの回路網で各電源の半分のモジュールに電力を供給します。一方の電源回路網がダウンしても、各電源装置が残りの半分のモジュールから電力の供給を受けて動作し続けます。使用可能な電力は、2つの回路網のうち電力の少ないほうの回路網に接続された電源装置から供給される電力の合計です。
ps-redundant	このモードは、アクティブな電源がダウンしたときに備えて予備の電源装置を1台追加したものです。最大の電力を供給できる電源がスタンバイモードで動作します。残りの1台または2台の電源装置がアクティブになります。使用可能な電力は、アクティブな電源ユニットによって供給される電力の合計です。
redundant	このモードは、電源の冗長性と入力電源回路網の冗長性を組み合わせたものです。つまり、シャーシは予備の電源装置を1台備えており、各電源装置の半分が1つの電源回路網に接続され、残りの半分がもう1つの電源回路網に接続されます。使用可能な電力は、電源装置モードと入力電源モードのうち使用可能電力が小さいほうです。

ファントレイの冗長性

Cisco Nexus 7000 シリーズ シャーシは、入出力モジュールの冷却用に2つの冗長なシステム ファントレイを備えており、さらにスイッチ ファブリック モジュールの冷却用に2つのファントレイを備えています。各ペアのファントレイのどちらか一方が動作していれば、システムを冷却できます。

ファンの回転速度は可変であり、16段階のいずれかに自動的に調整されます。これにより、システム全体の騒音と消費電力を最小限に抑えながら、システムの冷却効果を最適化します。特定のファントレイ内のファンに故障が検出されると、残りのファンの回転速度が速くなり、故障したファンによって失われた冷却能力を補います。ファントレイ全体を取り外したあと、置換していないことが検出されると、3分間の警告期間が経過したあと、システムのシャットダウンが開始されます。

Cisco NX-OS Release 5.0(2a) 以降の10スロット シャーシのファン シャットダウン ポリシーは次のとおりです。

- システム ファンが取り外された場合：以前のリリースでは、3分以内に他のファンの電源を切断しました。新しいポリシーでは、テーブル マッピングに基づいて他のファンの速度を高めます。
- ファブリック ファンが取り外された場合：以前のリリースでは、3分以内に他のファンの電源を切断しました。新しいポリシーでは、他のファンの速度を最大限に高めます。

**注意**

ファントレイの障害の場合、Nexus 7009 または Nexus 7018 デバイスで、交換が使用可能になるまで十分な通気を確保するように、障害が発生した装置をそのままにします。ファントレイはホットスワップ可能ですが、取り外しおよび取り付け作業を3分以内に完了しないと、システムが自動的にシャットダウンされます。

スイッチ ファブリックの冗長性

Cisco NX-OS は、冗長なスイッチ ファブリック モジュールによってスイッチング ファブリックの可用性を実現しています。1 台の Nexus 7000 シリーズに 1 ~ 5 枚のスイッチ ファブリック カード (SFC) を装着して、容量と冗長性を高めることができます。システムに装着された各入出力モジュールは、スイッチ ファブリック モジュールに自動的に接続され、それらの機能を利用できます。いずれかのスイッチ ファブリック モジュールで障害が発生すると、残りのアクティブなスイッチ ファブリック モジュール間で、自動的にトラフィックの再割り当てと均等化が行われます。故障したファブリック モジュールを置換すると、これとは逆のプロセスが実行されます。新しいファブリック モジュールを装着してオンラインにすると、装着されたすべてのファブリック モジュール間でトラフィックが再配分され、元の冗長性が復元されます。

スーパーバイザ モジュールの冗長性

Nexus 7000 シリーズでは、デュアル スーパーバイザ モジュールによって、プレーンの制御および管理機能において 1+1 の冗長性を実現しています。デュアル スーパーバイザ構成は、アクティブまたはスタンバイ構成で動作します。常に、どちらか一方のスーパーバイザ モジュールだけがアクティブ状態にあり、もう一方のモジュールはスタンバイ バックアップとして機能します。2 つのスーパーバイザ モジュール間で状態とコンフィギュレーションが常に同期された状態に維持されるため、アクティブなスーパーバイザ モジュールの障害発生時にステートフルなスイッチオーバーが可能です。

Cisco NX-OS の汎用オンライン診断 (GOLD) サブシステムとスーパーバイザ上の追加のモニタリング プロセスは、回復不可能な重大な障害、サービス再起動エラー、カーネルエラー、またはハードウェア障害が検出されると、冗長なスーパーバイザへのステートフル フェールオーバーを起動します。

スーパーバイザ レベルの回復不能な障害が発生すると、稼動中で、障害を起こしたスーパーバイザが、スイッチオーバーを起動します。すると、スタンバイ スーパーバイザが新しくアクティブなスーパーバイザとなり、同期された状態およびコンフィギュレーションを使用し、一方で障害の発生したスーパーバイザはリロードされます。リロードが完了し自己診断に合格すると、初期化され、新たなスタンバイ スーパーバイザとなり、新しくアクティブになったユニットと動作状態を同期させます。

スーパーバイザ スwitchオーバーの詳細については「[スーパーバイザの再起動とスイッチオーバー](#)」(P.4-4) を参照してください。

スーパーバイザの再起動とスイッチオーバー

ここでは、次の内容について説明します。

シングル スーパーバイザでの再起動

スーパーバイザが 1 台だけ搭載されたシステムでは、すべての HA ポリシーがサービスの再起動に失敗すると、スーパーバイザが再起動されます。その場合、スーパーバイザとすべてのサービスがリセットされ、以前の状態情報なしで起動されます。

デュアル スーパーバイザでの再起動

スーパーバイザが2台搭載されたシステムでスーパーバイザ レベルの障害が発生すると、システム マネージャは、ステートフルな動作を維持するため、再起動ではなくスイッチオーバーを実行します。ただし、障害発生時にスイッチオーバーが実行できない場合があります。たとえば、スタンバイ スーパーバイザ モジュールが安定したスタンバイ状態にない場合は、スイッチオーバーではなく再起動が実行されます。

デュアル スーパーバイザでのスイッチオーバー

デュアル スーパーバイザ構成では、スーパーバイザ レベルの障害が発生したとき、ステートフル スイッチオーバー (SSO) によるノンストップ フォワーディング (NSF) が可能です。2台のスーパーバイザは、アクティブ/スタンバイ構成で動作します。常に、どちらか一方のスーパーバイザ モジュールだけがアクティブ状態にあり、もう一方のモジュールはスタンバイ バックアップとして機能します。2台のスーパーバイザは常に状態とコンフィギュレーションが同期された状態を維持します。これにより、アクティブなスーパーバイザ モジュールで障害が発生したとき、大半のサービスでシームレスかつステートフルなスイッチオーバーを実行できます。

スイッチオーバーの特性

HA スイッチオーバーには次のような特性があります。

- コントロール トラフィックが影響を受けないため、ステートフル (中断なし) である。
- スイッチング モジュールが影響を受けないため、データ トラフィックが中断されない。
- スイッチング モジュールがリセットされない。
- 接続管理プロセッサ (CMP) がリロードされない。

スイッチオーバーのメカニズム

スイッチオーバーは、次のどちらかのメカニズムによって発生します。

- アクティブ スーパーバイザ モジュールで障害が発生し、スタンバイ スーパーバイザ モジュールが自動的に処理を引き継ぐ。
- アクティブ スーパーバイザ モジュールからスタンバイ スーパーバイザ モジュールへのスイッチオーバーをユーザが手動で起動する。

いったんスイッチオーバー プロセスが開始されると、スタンバイ スーパーバイザ モジュールが安定して使用可能になるまで、同じスイッチ上で別のスイッチオーバー プロセスを開始できません。

スイッチオーバーの失敗

スイッチオーバーが28秒以内に正常に終了しないと、スーパーバイザがリセットされます。リセットにより、スイッチオーバー処理中にネットワーク トポロジが変更されていた場合でも、レイヤ2 ネットワークでループが発生することがなくなります。この回復機能で最適なパフォーマンスが得られるように、スパニング ツリー プロトコル (STP) のデフォルト タイマーは変更しないようにしてください。

20秒以内にシステム起動のスイッチオーバーが3回発生すると、スイッチオーバーが無限に繰り返されるのを防ぐため、すべての非スーパーバイザ モジュールがシャットダウンされます。スーパーバイザは動作を継続するため、スイッチをリセットする前にシステム ログを収集できます。

スイッチオーバーの手動による起動

アクティブ スーパーバイザ モジュールからスタンバイ スーパーバイザ モジュールへのスイッチオーバーを手動で起動するには、**system switchover** コマンドを使用します。いったんこのコマンドを入力すると、スタンバイ スーパーバイザ モジュールが安定して使用可能になるまで、同じシステム上で別のスイッチオーバー プロセスを開始できません。



(注)

スタンバイ スーパーバイザ モジュールが安定したスタンバイ状態 (ha-standby 状態) にない場合は、手動によるスイッチオーバーは実行しません。

HA スwitchオーバーが実行可能かどうかを確認するには、**show system redundancy status** コマンドまたは **show module** コマンドを使用します。コマンドの出力にスタンバイ スーパーバイザ モジュールの状態として ha-standby が表示されたら、手動でスイッチオーバーを開始できます。

スイッチオーバーに関する注意事項

スイッチオーバーを手動で開始すると、すぐに処理が引き継がれます。スイッチオーバーを実行する際には次の注意事項に留意してください。

- スwitchオーバーは、2 つのスーパーバイザ モジュールがスitch内で動作している場合に限り実行できます。
- シャーシ内の各モジュールは正常に機能していなければなりません。

スイッチオーバーが可能かどうかの確認

ここでは、スイッチオーバーの前のスitchとモジュールのステータスを確認する方法を説明します。

- システムがスitchオーバーを実行できる状態かどうかを確認するには、**show system redundancy status** コマンドを使用します。**show system redundancy status** コマンドの詳細については、「[HA ステータス情報の表示](#)」(P.4-10) を参照してください。

- 任意の時点のモジュールのステータス（存在）を確認するには、**show module** コマンドを使用します。**show module** コマンドの出力例を次に示します。

```
switch# show module
Mod  Ports  Module-Type                      Model                      Status
----  -
1    0       Supervisor module-1X             N7K-SUP1                   active *
2    0       Supervisor module-1X             N7K-SUP1                   ha-standby
3    32      1/10 Gbps Ethernet Module       N7K-D132XP-15             ok
4    48      1/10 Gbps Ethernet Module       N7K-F248XP-24             ok
5    48      10/100/1000 Mbps Ethernet XL Module N7K-M148GT-11L           ok
6    32      1/10 Gbps Ethernet Module       N7K-F132XP-15             ok
9    32      1/10 Gbps Ethernet Module       N7K-F132XP-15             ok

Mod  Sw                Hw
---  -
1    6.0(1)            1.8
2    6.0(1)            1.1
3    6.0(1)            0.405
4    6.0(1)            0.500
5    6.0(1)            1.0
6    6.0(1)            0.617
9    6.0(1)            0.616

Mod  MAC-Address (es)                Serial-Num
---  -
1    f0-25-72-ab-a3-f8 to f0-25-72-ab-a4-00 JAF1446BMRR
2    00-22-55-77-bc-48 to 00-22-55-77-bc-50 JAB122901WK
3    00-24-f7-1b-69-70 to 00-24-f7-1b-69-b4 JAF1321ARLQ
4    40-55-39-25-c8-00 to 40-55-39-25-c8-34 JAF1530AAAF
5    e8-b7-48-00-03-60 to e8-b7-48-00-03-94 JAF1513BPCH
6    f8-66-f2-02-a1-f8 to f8-66-f2-02-a2-3c JAF1427DETN
9    a8-b1-d4-57-bc-bc to a8-b1-d4-57-bd-00 JAF1424CFMH

Mod  Online Diag Status
---  -
1    Pass
2    Pass
3    Pass
4    Pass
5    Pass
6    Pass
9    Pass

Xbar  Ports  Module-Type                      Model                      Status
----  -
2    0       Fabric Module 2                  N7K-C7009-FAB-2           ok
4    0       Fabric Module 2                  N7K-C7009-FAB-2           ok
5    0       Fabric Module 2                  N7K-C7009-FAB-2           ok

Xbar  Sw                Hw
---  -
2    NA                0.201
4    NA                0.203
5    NA                0.201

Xbar  MAC-Address (es)                Serial-Num
---  -
2    NA                JAF1406ATRH
4    NA                JAF1422AHCP
5    NA                JAF1406ATRQ
```

```
* this terminal session
switch#
```

出力の Status 列に、スイッチング モジュールの場合は OK、スーパーバイザ モジュールの場合は active または ha-standby と表示されている必要があります。

- auto-copy 機能の設定、およびスタンバイ スーパーバイザ モジュールへの auto-copy が進行中かどうかを確認するには、**show boot auto-copy** コマンドを使用します。**show boot auto-copy** コマンドの出力例を次に示します。

```
switch# show boot auto-copy
Auto-copy feature is enabled
switch# show boot auto-copy list
No file currently being auto-copied
```

デュアル スーパーバイザ システムでのアクティブ スーパーバイザ モジュールの交換

デュアル スーパーバイザ システムで中断なしにアクティブ スーパーバイザ モジュールを交換できます。

アクティブ スーパーバイザ モジュールを交換するには、次の手順を実行します。

-
- ステップ 1** スタンバイ スーパーバイザへのスイッチオーバーを手動で起動します。

```
switch# system switchover
Raw time read from Hardware Clock: Y=2009 M=2 D=2 07:35:48
writing reset reason 7,

NX7 SUP Ver 3.17.0
Serial Port Parameters from CMOS
PMCON_1: 0x200
PMCON_2: 0x0
PMCON_3: 0x3a
PM1_STS: 0x1
Performing Memory Detection and Testing
Testing 1 DRAM Patterns
Total mem found : 4096 MB
Memory test complete.
NumCpus = 2.
Status 61: PCI DEVICES Enumeration Started
Status 62: PCI DEVICES Enumeration Ended
Status 9F: Dispatching Drivers
Status 9E: IOFPGA Found
Status 9A: Booting From Primary ROM
Status 98: Found Cisco IDE
Status 98: Found Cisco IDE
Status 90: Loading Boot Loader
Reset Reason Registers: 0x1 0x10
Filesystem type is ext2fs, partition type 0x83
Filesystem type is ext2fs, partition type 0x83

GNU GRUB version 0.97

Loader Version 3.17.0

current standby sup
```



```

switch(standby)# 2009 Feb  2 07:35:46 switch %$ VDC-1 %$ %KERN-2-SYSTEM_MSG: Switchover
started by redundancy driver - kernel
2009 Feb  2 07:35:47 switch %$ VDC-1 %$ %SYSMGR-2-HASWITCHOVER_PRE_START: This supervisor
is becoming active (pre-start phase).
2009 Feb  2 07:35:47 switch %$ VDC-1 %$ %SYSMGR-2-HASWITCHOVER_START: This supervisor is
becoming active.
2009 Feb  2 07:35:48 switch %$ VDC-1 %$ %SYSMGR-2-SWITCHOVER_OVER: Switchover completed.

```



(注) スイッチオーバーが完了するまで待つと、スタンバイ スーパーバイザがアクティブになります。

ステップ 2 交換中のスーパーバイザ モジュールの電源を切ります。

```
switch# out-of-service module 6
```

ステップ 3 スーパーバイザ モジュールを交換します。スーパーバイザ モジュールの交換については、『Cisco Nexus 7000 Series Hardware Installation and Reference Guide』を参照してください。



(注) 挿入してから 6 分後に、アクティブ スーパーバイザ モジュールから交換用スーパーバイザ モジュールを起動します。6 分間待ちたくない場合は、**reload module slot-number force** コマンドを使用して交換用スーパーバイザをすぐに起動します。

ステップ 4 アクティブ スーパーバイザ モジュールからスタンバイ スーパーバイザ モジュールへキックスタート イメージをコピーします。

```
switch# copy bootflash:n7000-s1-kickstart.6.0.1.gbin.S30
bootflash://sup-remote/n7000-s1-kickstart.6.0.1.gbin.S30
```

ステップ 5 アクティブ スーパーバイザ モジュールからスタンバイ スーパーバイザ モジュールへシステム イメージをコピーします。

```
switch# copy bootflash:n7000-s1-dk9.6.0.1.gbin.S30
bootflash://sup-remote/n7000-s1-dk9.6.0.1.gbin.S30
```

ステップ 6 スタンバイ スーパーバイザの BOOT 環境変数を構成します。

```
switch# config t
switch# boot kickstart bootflash://sup-remote/n7000-s1-kickstart.6.0.1.gbin.S30
switch# boot system bootflash://sup-remote/n7000-s1-dk9.6.0.1.gbin.S30
```

ステップ 7 これらの変更をスタートアップ コンフィギュレーションに保存します。

```
switch# copy running-config startup-config
```

デュアル スーパーバイザ システムでのスタンバイ スーパーバイザ モジュールの交換

デュアル スーパーバイザ システムで中断なしにスタンバイ スーパーバイザ モジュールを交換できます。

スタンバイ スーパーバイザ モジュールを交換するには、次の手順を実行します。

HA ステータス情報の表示

ステップ 1 スタンバイ スーパーバイザ モジュールの電源を切ります。

```
switch# out-of-service module 6
```

ステップ 2 スーパーバイザ モジュールを交換します。スーパーバイザ モジュールの交換については、『Cisco Nexus 7000 Series Hardware Installation and Reference Guide』を参照してください。



(注) 挿入してから 6 分後に、アクティブ スーパーバイザ モジュールから交換用スーパーバイザ モジュールを起動します。6 分間待ちたくない場合は、**reload module slot-number force** コマンドを使用して交換用スーパーバイザをすぐに起動します。

ステップ 3 アクティブ スーパーバイザ モジュールからスタンバイ スーパーバイザ モジュールへキックスタート イメージをコピーします。

```
switch# copy bootflash:n7000-s1-kickstart.6.0.1.bin
bootflash://sup-remote/n7000-s1-kickstart.6.0.1.bin
```

ステップ 4 アクティブ スーパーバイザ モジュールからスタンバイ スーパーバイザ モジュールへシステム イメージをコピーします。

```
switch# copy bootflash:n7000-s1-dk9.6.0.1.bin
bootflash://sup-remote/n7000-s1-dk9.6.0.1.bin
```

ステップ 5 スタンバイ スーパーバイザの BOOT 環境変数を構成します。

```
switch# config t
switch# boot kickstart bootflash://sup-remote/n7000-s1-kickstart.6.0.1.bin
switch# boot system bootflash://sup-remote/n7000-s1-dk9.6.0.1.bin
```

ステップ 6 これらの変更をスタートアップ コンフィギュレーションに保存します。

```
switch# copy running-config startup-config
```

HA ステータス情報の表示

システムの HA ステータスを表示するには、**show system redundancy status** コマンドを使用します。表 4-2 および表 4-4 に、冗長性、スーパーバイザ、内部状態のとり得る出力値を示します。

```
switch# 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
      Internal state:   HA standby
```

次の条件によって、自動同期化が可能かどうかを判断できます。

- 一方のスーパーバイザ モジュールの内部ステートが **Active with HA standby**、もう一方のスーパーバイザ モジュールのステートが **ha-standby** のとき、システムは HA 状態で動作しており、自動同期化を実行できます。
- どちらか一方のスーパーバイザ モジュールの内部ステートが **none** であるとき、システムは自動同期化を実行できません。

表 4-2 に、冗長ステートのとり得る値を示します。

表 4-2 冗長ステート

ステート	説明
Not present	スーパーバイザ モジュールが存在しないか、シャーシに装着されていません。
Initializing	診断に合格し、コンフィギュレーションをダウンロード中です。
Active	アクティブなスーパーバイザ モジュールとスイッチの構成準備ができました。
Standby	スイッチオーバーが可能です。
Failed	システムがスーパーバイザ モジュールの初期化中に障害を検出し、そのモジュールの電源の投入と切断を 3 回自動的に試行しましたが、依然として failed (障害ステート) と表示されています。
Offline	スーパーバイザ モジュールがデバッグのため意図的にシャットダウンされました。
At BIOS	システムがスイッチオーバーと接続を確立し、スーパーバイザ モジュールが診断を実行しています。
Unknown	システムが無効なステートです。このステートが続く場合は、TAC に連絡してください。

表 4-3 に、スーパーバイザ モジュール ステートのとり得る値を示します。

表 4-3 スーパーバイザ ステート

ステート	説明
Active	スイッチ内のアクティブなスーパーバイザ モジュールの構成準備ができました。
HA standby	スイッチオーバーが可能です。
Offline	システムがデバッグのため意図的にシャットダウンされました。
Unknown	システムが無効なステートです。TAC に連絡してサポートを依頼してください。

表 4-4 に、内部冗長ステートのとり得る値を示します。

表 4-4 内部ステート

ステート	説明
HA standby	スタンバイ スーパーバイザ モジュールの HA スイッチオーバー メカニズムが有効です (「 スイッチオーバーの手動による起動 」(P.4-6) を参照)。
Active with no standby	スイッチオーバーすることはできません。

表 4-4 内部ステート (続き)

ステート	説明
Active with HA standby	スイッチ内のアクティブなスーパーバイザ モジュールの構成準備ができました。スタンバイ スーパーバイザ モジュールは ha-standby ステートです。
Shutting down	システムをシャットダウンしています。
HA switchover in progress	システムはアクティブ状態を開始しています。
Offline	システムがデバッグのため意図的にシャットダウンされました。
HA synchronization in progress	スタンバイ スーパーバイザ モジュールが、アクティブ スーパーバイザ モジュールとステートを同期させています。
Standby (failed)	スタンバイ スーパーバイザ モジュールが機能していません。
Active with failed standby	アクティブ スーパーバイザ モジュールとセカンダリ スーパーバイザ モジュールが存在していますが、セカンダリ スーパーバイザ モジュールが機能していません。
Other	システムが移行過渡ステートです。このステートが続く場合は、TAC に連絡してください。

VDC ハイ アベイラビリティ

Cisco NX-OS ソフトウェアには、コントロールプレーンで障害やスイッチオーバーが発生した場合の影響を最小限に抑えるハイ アベイラビリティ (HA) 機能が組み込まれています。サービス再起動、スーパーバイザ モジュールのステートフルなスイッチオーバー、In-Service Software Upgrade (ISSU) など、さまざまな HA サービス レベルによってデータプレーンの保護が実現されます。これらのすべてのハイ アベイラビリティ (HA) 機能は、VDC をサポートします。

VDC で回復不可能なエラーが発生した場合、Cisco NX-OS ソフトウェアでは、VDC ごとに指定できる HA ポリシーによって処理できます。HA ポリシーに指定できる対処方法は次のとおりです。

- **bringdown** : VDC を障害状態に移行します。障害状態から復旧するには、物理デバイスをリロードする必要があります。これは、デフォルトの VDC の動作です。デフォルト以外の VDC の動作に関しては、物理デバイスをリロードする必要はありません。
- **リセット (Reset)** : 2 台のスーパーバイザ モジュールを搭載した Cisco NX-OS デバイスの場合は、スーパーバイザ モジュール スwitchオーバーを起動します。スーパーバイザ モジュールを 1 台しか搭載していない Cisco NX-OS デバイスの場合は、リロードを実行します。
- **再起動 (Restart)** : VDC を削除し、スタートアップ コンフィギュレーションを使用して再作成します。

VDC と HA の詳細については、『Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.1』を参照してください。

その他の関連資料

システムレベルの HA 機能の実装に関する詳細については、次の各セクションを参照してください。

関連資料

関連項目	参照先
仮想デバイス コンテキスト (VDC)	『Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.1』
冗長なハードウェア	『Cisco Nexus 7000 Series Site Preparation Guide』および『Cisco Nexus 7000 Series Hardware Installation and Reference Guide』
電源モードの設定と Cisco NX-OS の基礎	『Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide, Release 6.x』
ノンストップ フォワーディング (NSF)	『Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 6.x』
In-service Software Upgrade (ISSU)	第 5 章 「In-Service Software Upgrade の理解」
GOLD、EEM、および Smart Call Home	『Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x』
ライセンス	『Cisco NX-OS Licensing Guide』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

管理情報ベース (MIB)

MIB	MIB のリンク
<ul style="list-style-type: none"> CISCO-SYSTEM-EXT-MIB : ciscoHaGroup、cseSwCoresTable、cseHaRestartNotify、cseShutDownNotify、cseFailSwCoreNotify、cseFailSwCoreNotifyExtended CISCO-PROCESS-MIB CISCO-RF-MIB 	<p>MIB を検索およびダウンロードするには、次の URL にアクセスしてください。</p> <p>http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</p>

RFC

RFC	タイトル
この機能によってサポートされている RFC はありません。	—

シスコのテクニカル サポート

説明	リンク
TAC のホームページには、3 万ページに及ぶ検索可能な技術情報があります。製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクもあります。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/cisco/web/support/index.html



CHAPTER 5

In-Service Software Upgrade の理解

この章では、Cisco NX-OS In-Service Software Upgrade (ISSU) について説明します。この章の構成は次のとおりです。

ISSU について

2 台のスーパーバイザを搭載した Nexus 7000 シリーズ シャーシでは、In-Service Software Upgrade (ISSU) 機能を使用して、トラフィック転送動作を継続しながら、システムソフトウェアをアップグレードできます。ISSU はノンストップ フォワーディング (NFS) の既存の機能とステートフル スイッチオーバー (SSO) を使用して、システムのダウンタイムを発生させずにソフトウェアアップグレードを実行します。

ISSU は、管理者がコマンドライン インターフェイス (CLI) で起動します。ISSU が起動すると、システム上の次のコンポーネントが (必要に応じて) アップデートされます。

- スーパーバイザ BIOS、キックスタート イメージ、システム イメージ
- モジュール BIOS とイメージ
- 接続管理プロセッサ (CMP) BIOS とイメージ

スーパーバイザを 2 台搭載した冗長なシステムでは、一方のスーパーバイザがアクティブとなり、もう一方のスーパーバイザがスタンバイ モードで動作します。ISSU の動作中、アクティブなスーパーバイザが古いソフトウェアを使用して動作し続けている間に、スタンバイ スーパーバイザに新しいソフトウェアがロードされます。アップグレード処理の一部として、アクティブ スーパーバイザとスタンバイ スーパーバイザの間でスイッチオーバーが発生し、スタンバイ スーパーバイザがアクティブとなり、新しいソフトウェアの実行を開始します。スイッチオーバーのあとに、新しいソフトウェアがスタンバイ (旧アクティブ) スーパーバイザ上にロードされます。

仮想化のサポート

ISSU ベースのアップグレードはシステム全体のアップグレードであり、すべての設定済みの仮想デバイス コンテキスト (VDC) を含む、同じイメージとバージョンがシステム全体に適用されます。VDC は主に、コントロールプレーンとユーザ インターフェイスのパーティシャライゼーションであり、仮想リソースごとに独立したバージョンのイメージは実行できません。



(注)

VDC の詳細については、『Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.1』を参照してください。

ライセンス要件

次の表に、システム レベル ハイ アベイラビリティ機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	ISSU 機能にライセンスは必要ありません。ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。
VDC	VDC にはアドバンスド サービス ライセンスが必要です。

Cisco NX-OS ライセンス方式、およびライセンスの取得方法と適用方法の詳細については、『Cisco NX-OS Licensing Guide』を参照してください。

注意事項および制約事項

ISSU には、次のような制約事項があります。

- アップグレード中に設定やネットワーク接続を変更しないでください。ネットワークの設定を変更するとアップグレードが中断する可能性があります。
- 場合によっては、ソフトウェア アップグレードが中断することがあります。そうした例外的なケースが発生するのは、次のような場合です。
 - たとえ 1 つのスーパーバイザ システムでも、キックスタート イメージまたはシステム イメージを変更した場合。
 - デュアル スーパーバイザ システムで、互換性のないシステム ソフトウェア イメージを使用した場合。
- コンフィギュレーション モードは、変更を防ぐために ISSU 中にブロックされています。

互換性のあるアップグレードおよびダウングレードの詳細については、『Cisco Nexus 7000 Series NX-OS Release Notes, Release 6.x』を参照してください。

ISSU の動作原理

2 台のスーパーバイザを備えた Nexus 7000 シリーズの場合、ISSU プロセスは次の手順を実行します。

1. 管理者が **install all** コマンドを使用するとアップグレードが開始されます。
2. 新しいソフトウェア イメージ ファイルの場所と整合性を確認します。
3. 2 台のスーパーバイザとすべてのスイッチング モジュールについて、動作ステータスと現在のソフトウェア バージョンを確認し、システムが ISSU を実行可能であることを確認します。
4. 新しいソフトウェア イメージをスタンバイ スーパーバイザにロードし、HA ready ステートにします。
5. スーパーバイザのスイッチオーバーを実行します。
6. 新しいソフトウェア イメージをスタンバイ (旧アクティブ) スーパーバイザにロードし、HA ready ステートにします。
7. 各スイッチング モジュールに対して、順次、中断なしのアップグレードを実行します。
8. CMP をアップグレードします。

アップグレードプロセス中、システムは、コンソールに詳細なステータス情報を表示し、重要な手順を実行する際には管理者に確認を求めます。

ISSU の設定

ISSU の設定の詳細については、『*Cisco Nexus 7000 Series NX-OS Software Upgrade and Downgrade Guide, Release 5.x*』を参照してください。

ISSU の互換性の判断

新しいソフトウェア イメージでサポートされていない機能を設定すると、ISSU が中断することがあります。ISSU の互換性を判断するには、**show incompatibility system** コマンドを使用します。

次の例では、ISSU の互換性を判断する方法を示します。

```
switch# show incompatibility system bootflash:n7000-s1-dk9.4.1.4.bin
The following configurations on active are incompatible with the system image
1) Service : vpc , Capability : CAP_FEATURE_VPC_ENABLED
Description : vPC feature is enabled
Capability requirement : STRICT
Disable command : Disable vPC using "no feature vpc"

2) Service : copp , Capability : CAP_FEATURE_COPP_DISTRIBUTED_POLICING
Description : Distributed policing for copp is enabled.
Capability requirement : STRICT
Disable command : Disable distributed policing using "no copp distributed-policing enable"
```

その他の関連資料

ISSU の実装に関する詳細は、次の各セクションを参照してください。

関連資料

関連項目	参照先
ISSU の設定	『 <i>Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide, Release 6.x</i> 』の「Software Images」の章
仮想デバイス コンテキスト (VDC)	『 <i>Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.1</i> 』
ライセンス	『 <i>Cisco NX-OS Licensing Guide</i> 』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

管理情報ベース (MIB)

MIB	MIB のリンク
<ul style="list-style-type: none"> CISCO-SYSTEM-EXT-MIB : ciscoHaGroup、cseSwCoresTable、cseHaRestartNotify、cseShutDownNotify、cseFailSwCoreNotify、cseFailSwCoreNotifyExtended CISCO-PROCESS-MIB CISCO-RF-MIB 	<p>MIB を検索およびダウンロードするには、次の URL にアクセスしてください。</p> <p>http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</p>

RFC

RFC	タイトル
この機能によってサポートされている RFC はありません。	—

シスコのテクニカル サポート

説明	リンク
TAC のホームページには、3 万ページに及ぶ検索可能な技術情報があります。製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクもあります。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/cisco/web/support/index.html



INDEX

E

E メール通知

Smart Call Home から [1-5](#)

F

FHRP

説明 [3-3](#)

タイマー [1-4](#)

「FHRP」を参照

G

Gateway Load Balancing Protocol。

GLBP

説明 [3-3](#)

「GLBP」を参照

H

HA ポリシー

最小ライフタイム [2-3](#)

最大再試行回数 [2-3](#)

説明 [2-3](#)

「HA ポリシー」を参照

HSRP

説明 [3-3](#)

「HSRP」を参照

I

IEEE 802.3ad

リンク アグリゲーション [1-4](#)

ISSU

手順 [5-2](#)

M

MSTP

説明 [3-2](#)

「MSTP」を参照

MTS

説明 [2-3](#)

「MTS」を参照

O

Open Shortest Path First プロトコル。

OSPFv2

再起動 [3-4](#)

「OSPFv2」を参照

P

PSS

グローバルおよびローカル同期 [2-2](#)

説明 [2-2](#)

プライベートおよび共有 [2-2](#)

「PSS」を参照

R

RSTP

説明 [3-2](#)

「RSTP」を参照

S

Smart Call Home

説明 [1-5](#)

STP

拡張 [1-4](#)説明 [3-2](#)バーチャライゼーションの拡張 [3-1](#)

「STP」を参照

V

VDC

STP 拡張 [3-1](#)再起動 [2-6](#)システム レベル HA [4-12](#)

「VDC」を参照

VRRP

説明 [3-3](#)

「VRRP」を参照

え

永続ストレージ サービス。

か

仮想デバイス コンテキスト。

仮想ルータ冗長プロトコル。

関連資料 [1-xi](#)

く

グレースフル リスタート

説明 [3-4](#)

こ

高速スパニング ツリー プロトコル。

さ

サービス

再起動性 [2-3](#)

再起動

VDC 内 [2-6](#)ステートフル、説明 [2-4](#)ステートレス、説明 [2-5](#)

最小ライフタイム。

最大再試行回数。

し
システム マネージャ [2-2](#)説明 [2-2](#)

自動同期化

状態 [4-11](#)

冗長ステート

値の説明 [4-11](#)

す

スイッチオーバー

失敗 [4-5](#)手動による起動 [4-6](#)注意事項 [4-6](#)特性 [4-5](#)

スーパーバイザ モジュール

アクティブ状態 [4-12](#)

アクティブ スーパーバイザの交換 [4-8](#)
 手動によるスイッチオーバー [4-6](#)
 スイッチオーバー メカニズム [4-5](#)
 スタンバイ状態 [4-11](#)
 スタンバイ スーパーバイザの置き換え [4-9](#)
 ステートの説明 [4-11](#)

ステートフルな再起動

説明 [2-4](#)

ステートレスな再起動

説明 [2-5](#)

スパニング ツリー プロトコル。

そ

ソフトウェア アップグレード

中断 [5-2](#)

た

多重スパニング ツリー プロトコル。

な

内部スイッチ ステート

説明 [4-11](#)

は

バーチャライゼーション

STP 拡張 [3-1](#)

ハイ アベイラビリティ

状態の表示 [4-10](#)

スイッチオーバーの特性 [4-5](#)

スーパーバイザ モジュール スイッチオーバー メカニズム [4-5](#)

説明 [1-1](#)

ふ

ファーストホップ冗長プロトコル。

プロセス

再起動性 [2-3](#)

ほ

ホット スタンバイ ルータ プロトコル。

ポリシー。

ま

マニュアル

関連資料 [x](#)

追加資料 [1-xi](#)

め

メッセージおよびトランザクション サービス。

ら

ライセンス

BGP [3-1](#)

ISSU [5-2](#)

Smart Call Home [4-2](#)

VDC [4-2](#)

サービス レベル HA [2-2](#)

システム レベル HA [4-2](#)

ネットワーク レベル HA [3-1](#)

