



## **Cisco NX-OS のハイアベイラビリティおよび 冗長性ガイド**

Release 4.0

June 2008

**【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/](http://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。  
米国サイト掲載ドキュメントとの差異が生じる場合があるため、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。

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

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

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

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0805R)

このマニュアルで使用している IP アドレスは、実際のアドレス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、および図は、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 NX-OS のハイアベイラビリティおよび冗長性ガイド*

Copyright © 2008 Cisco Systems, Inc.

All rights reserved.

Copyright © 2008, シスコシステムズ合同会社 .

All rights reserved.



## CONTENTS

<b>はじめに</b>	vii
対象読者	vii
マニュアルの構成	vii
表記法	viii
関連資料	ix
マニュアルの入手方法および Service Request ツールの使用方法	x
Japan TAC Web サイト	x

---

### CHAPTER 1

<b>概要</b>	1-1
ハイ アベイラビリティについて	1-2
サービス レベル ハイ アベイラビリティ	1-3
プロセスの分離	1-3
プロセスの再起動性	1-3
サービス レベル ハイ アベイラビリティ	1-4
物理的な冗長性	1-4
ISSU	1-5
VDC	1-5
ネットワーク レベル ハイ アベイラビリティ	1-6
レイヤ 2 HA 機能	1-6
レイヤ 3 HA 機能	1-6
可用性のためのその他の管理ツール	1-7
GOLD	1-7
EEM	1-7
Smart Call Home	1-7

---

### CHAPTER 2

<b>サービス レベル ハイ アベイラビリティの理解</b>	2-1
NX-OS サービスの再起動について	2-2
バーチャライゼーションのサポート	2-2
ライセンス要件	2-2
再起動性インフラストラクチャ	2-3
システム マネージャ	2-3
永続ストレージ サービス	2-3
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	2-4
プロセスの再起動性	2-5
プロセス再起動の種類	2-5
ステートフルな再起動	2-6
ステートレスな再起動	2-6
スイッチオーバー	2-7
スタンバイ スーパーバイザ サービスの再起動	2-7
スイッチング モジュール サービスの再起動	2-7
VDC 内サービスの再起動	2-7
再起動のトラブルシューティング	2-8
参考文献	2-9
関連資料	2-9
標準	2-9
MIB	2-9
RFC	2-9
技術サポート	2-10

CHAPTER 3

<b>システム レベル ハイ アベイラビリティの理解</b>	<b>3-1</b>
NX-OS システム レベル ハイ アベイラビリティについて	3-2
バーチャライゼーションのサポート	3-2
ライセンス要件	3-3
物理的な冗長性	3-3
電源の冗長性	3-3
電源モード	3-3
ファントレイの冗長性	3-4
スイッチ ファブリックの冗長性	3-4
スーパーバイザ モジュールの冗長性	3-5
スーパーバイザの再起動とスイッチオーバー	3-6
シングル スーパーバイザでの再起動	3-6
デュアル スーパーバイザでの再起動	3-6
デュアル スーパーバイザでのスイッチオーバー	3-6
スイッチオーバーの特性	3-6
スイッチオーバーのメカニズム	3-7
スイッチオーバーの失敗	3-7
スイッチオーバーの手動による起動	3-7
スイッチオーバーに関する注意事項	3-7
スイッチオーバーが可能かどうかの確認	3-8
HA ステータス情報の表示	3-9
VDC ハイ アベイラビリティ	3-11

参考文献	3-12
関連資料	3-12
標準	3-12
MIB	3-12
RFC	3-12
技術サポート	3-13

## CHAPTER 4

<b>ネットワーク レベル ハイ アベイラビリティの理解</b>	<b>4-1</b>
ネットワーク レベル ハイ アベイラビリティについて	4-2
バーチャライゼーションのサポート	4-2
ライセンス要件	4-2
スパニングツリー プロトコル	4-3
ファーストホップ冗長プロトコル	4-4
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	4-5
OSPFv2 のステートレスな再起動	4-5
スイッチオーバーの OSPFv2 グレースフル リスタート	4-5
OSFPv2 プロセス障害発生時の OSPFv2 グレースフル リスタート	4-5
参考文献	4-6
関連資料	4-6
標準	4-6
MIB	4-6
RFC	4-6
技術サポート	4-6

## CHAPTER 5

<b>インサービス ソフトウェア アップグレードの理解</b>	<b>5-1</b>
ISSU について	5-2
バーチャライゼーションのサポート	5-2
ライセンス要件	5-2
注意事項と制約事項	5-3
ISSU の動作原理	5-3
ISSU の設定	5-3
参考文献	5-4
関連資料	5-4
標準	5-4
MIB	5-4
RFC	5-4
技術サポート	5-4

## INDEX

## 索引





## はじめに

ここでは、このマニュアル「Cisco NX-OS のハイアベイラビリティおよび冗長性ガイド Release 4.0」の対象読者、構成、表記法について説明します。関連資料の取得方法に関する情報も提供します。

この章の構成は次のとおりです。

- [対象読者 \(p.vii\)](#)
- [マニュアルの構成 \(p.vii\)](#)
- [表記法 \(p.viii\)](#)
- [関連資料 \(p.ix\)](#)
- [マニュアルの入手方法および Service Request ツールの使用方法 \(p.x\)](#)

## 対象読者

このマニュアルは、NX-OS デバイスの設定と保守を担当する、経験を積んだネットワーク管理者向けです。

## 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 NX-OS サービスの再起動性について説明します。
第 3 章「システムレベルハイアベイラビリティの理解」	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 4 章「ネットワークレベルハイアベイラビリティの理解」	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 5 章「インサービスソフトウェアアップグレードの理解」	インサービスソフトウェアアップグレード (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」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。



**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	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。
ストリング	引用符を付けない一組の文字。ストリングの前後には引用符を使用しません。引用符を使用すると、その引用符も含めてストリングとみなされます。

出力例では、次の表記法を使用しています。

screen font	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。
<b>boldface screen font</b>	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、かぎカッコ(<>)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(#)がある場合には、コメント行であることを示します。

## 関連資料

Cisco NX-OS のマニュアルは、次の URL から入手できます。

[http://www.cisco.com/en/US/products/ps9372/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps9372/tsd_products_support_series_home.html)

Cisco NX-OS のマニュアル セットには、次の資料が含まれます。

## リリース ノート

『Cisco NX-OS Release Notes』 Release 4.0

## NX-OS コンフィギュレーション ガイド

『Cisco NX-OS Getting Started with Virtual Device Contexts』 Release 4.0

『Cisco NX-OS Fundamentals Configuration Guide』 Release 4.0

『Cisco NX-OS Interfaces Configuration Guide』 Release 4.0

『Cisco NX-OS Layer 2 Switching Configuration Guide』 Release 4.0

『Cisco NX-OS Quality of Service Configuration Guide』 Release 4.0

『Cisco NX-OS Unicast Routing Configuration Guide』 Release 4.0

『Cisco NX-OS Multicast Routing Configuration Guide』 Release 4.0

『Cisco NX-OS Security Configuration Guide』 Release 4.0

『Cisco NX-OS Virtual Device Context Configuration Guide』 Release 4.0

『Cisco NX-OS Software Upgrade Guide』 Release 4.0

『Cisco NX-OS Licensing Guide』 Release 4.0

『Cisco NX-OS High Availability and Redundancy Guide』 Release 4.0

『Cisco NX-OS System Management Configuration Guide』 Release 4.0

『Cisco NX-OS XML Management Interface User Guide』 Release 4.0

『Cisco NX-OS System Messages Reference』

『Cisco NX-OS MIB Quick Reference』

## NX-OS コマンド リファレンス

『Cisco NX-OS Command Reference Master Index』 Release 4.0

『Cisco NX-OS Fundamentals Command Reference』 Release 4.0

『Cisco NX-OS Interfaces Command Reference』 Release 4.0

『Cisco NX-OS Layer 2 Switching Command Reference』 Release 4.0

『Cisco NX-OS Quality of Service Command Reference』 Release 4.0

『Cisco NX-OS Unicast Routing Command Reference』 Release 4.0

『Cisco NX-OS Multicast Routing Command Reference』 Release 4.0

『Cisco NX-OS Security Command Reference』 Release 4.0

『Cisco NX-OS Virtual Device Context Command Reference』 Release 4.0

『Cisco NX-OS High Availability and Redundancy Command Reference』 Release 4.0

『Cisco NX-OS System Management Command Reference』 Release 4.0

## その他のソフトウェアのマニュアル

『Cisco NX-OS Troubleshooting Guide』 Release 4.0

## マニュアルの入手方法および Service Request ツールの使用方法

マニュアルの入手方法、Service Request ツールの使用方法、および追加情報の収集方法については、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。『What's New in Cisco Product Documentation』には、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>

Really Simple Syndication (RSS) フィードとして『What's New in Cisco Product Documentation』に登録し、リーダ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します。RSS フィードは無料サービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。

## Japan TAC Web サイト

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

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

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

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

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



## 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 \(p.1-2\)](#)
- [サービス レベル ハイ アベイラビリティ \(p.1-3\)](#)
- [サービス レベル ハイ アベイラビリティ \(p.1-4\)](#)
- [ネットワーク レベル ハイ アベイラビリティ \(p.1-6\)](#)
- [可用性のためのその他の管理ツール \(p.1-7\)](#)

## 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 システムのほとんどの機能およびサービスは分離されているため、他のサービスを稼働し続けたまま、障害の発生したサービスだけを再起動できます。また、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できるため、他のサービスへ透過的に動作を再開できます。
- スーパーバイザの SSO Nexus 7000 シリーズは、アクティブ/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、インサービスソフトウェアアップグレード (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別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 \(p.1-3\)](#)
- [プロセスの再起動性 \(p.1-3\)](#)

### 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機能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、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。

## サービス レベル 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3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 \(p.1-4\)](#)
- [ISSU \(p.1-5\)](#)
- [VDC \(p.1-5\)](#)

### 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3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 7000 シリーズ シャーシは、I/O 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 Switch Fabric Module ( SFM; 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、システムは充分冷却できます。ファントレイで障害が発生しても、代替のファントレイが用意できるまで、故障したファンを装着したままにして、正常なエアフローを確保する必要があります。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。
- **ファブリックの冗長性** Cisco NX-OS は、冗長な SFM によってスイッチング ファブリックの可用性を提供しています。1 台の Cisco Nexus 7000 シリーズ シャーシに1 ~ 5 枚の Switch Fabric Card ( SFC; 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 I/O モジュールは、正しく装着されたすべての SFM 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 SFM で障害が発生すると、残りのアクティブな SFM 間で、自動的なトラフィックの再割り当てと均等化が実行されます。故障した SFM 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3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、インサービス ソフトウェア アップグレード (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)。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ることなく実行できます。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 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「インサービスソフトウェアアップグレードの理解」](#)を参照してください。

## 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 NX-OS Virtual Device Context Configuration Guide*』 Release 4.0 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ォ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4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 \(p.1-6\)](#)
- [レイヤ 3 HA 機能 \(p.1-6\)](#)

### レイヤ 2 HA 機能

Cisco NX-OS レイヤ 2 HA 機能

- Bridge Protocol Data Unit (BPDU; ブリッジ プロトコル データ ユニット) 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 Spanning Tree Protocol (STP; スパニング ツリー プロトコル) 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
- UniDirectional Link Detection (UDLD; 単一方向リンク検出) プロトコル
- Shortest Path First (SPF; 最短パス優先) の最適化。Link-State Advertisement (LSA; リンクステートアドパタイズメント) ペーシングや SPF の増大など。
- IEEE 802.3ad リンク アグリゲーション

### 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。
- プロトコル ベースの定期リフレッシュ
- Hot Standby Router Protocol (HSRP; ホットスタンバイ ルータ プロトコル)、Gateway Load Balancing Protocol (GLBP; ゲートウェイ ロード バランシング プロトコル)、Virtual Router Redundancy Protocol (VRRP; 仮想ルータ冗長プロトコル) などの First-Hop Redundancy Protocol (FHRP; ファーストホップ冗長プロトコル) 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。

- [GOLD \(p.1-7\)](#)
- [EEM \(p.1-7\)](#)
- [Smart Call Home \(p.1-7\)](#)

### GOLD

Cisco Generic On-Line Diagnostics (GOLD; 汎用オンライン診断) 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 NX-OS System Management Configuration Guide*』Release 4.0 を参照してください。

### 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 NX-OS System Management Configuration Guide*』Release 4.0 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 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 NX-OS System Management Configuration Guide*』Release 4.0 を参照してください。





# 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 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。

- [NX-OS サービスの再起動について \(p.2-2\)](#)
- [ライセンス要件 \(p.2-2\)](#)
- [再起動性インフラストラクチャ \(p.2-3\)](#)
- [プロセスの再起動性 \(p.2-5\)](#)
- [スタンバイ スーパーバイザ サービスの再起動 \(p.2-7\)](#)
- [スイッチング モジュール サービスの再起動 \(p.2-7\)](#)
- [VDC 内サービスの再起動 \(p.2-7\)](#)
- [再起動のトラブルシューティング \(p.2-8\)](#)
- [参考文献 \(p.2-9\)](#)

## 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ない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 (OSPF や 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4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。

## バーチャライゼーションのサポート

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.2-7) を参照してください。



(注) VDC の詳細については、『Cisco NX-OS Virtual Device Context Configuration Guide』Release 4.0 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。

製品名	ライセンス要件
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。

NX-OS のライセンス スキームの詳細は、『Cisco NX-OS Licensing Guide』Release 4.0 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 (p.2-3)
- 永続ストレージ サービス (p.2-3)
- メッセージおよびトランザクション サービス (p.2-3)
- HA ポリシー (p.2-4)

### 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、Persistent Storage Service (PSS; 永続ストレージ サービス) を使用して、運用の実行時情報とプラットフォーム サービスの設定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ステートを回復します。PSS はステート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、自身のステート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(当サービスのみ読み取り可能)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のみ読み取り可能)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

Message and Transaction Service (MTS; メッセージおよびトランザクション サービス) は、ハイ アベイラビリティに特化した高パフォーマンス プロセス間通信メッセージ 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、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 コンポーネント間における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。すなわち、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、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。この回数だけ再試行を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みなされ、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。すなわち、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 / プロセスからの応答がない	サービスの再起動
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 \(p.2-5\)](#)

## 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 \(p.2-6\)](#)
- [ステートレスな再起動 \(p.2-6\)](#)
- [スイッチオーバー \(p.2-7\)](#)

## 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、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ことを認識すると、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、障害発生前のインスタンスと同じ状態にします。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がステートフルな初期化を無事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よって決まります。サービスが数回で再起動の試みを成功できない場合、そのサービスの再起動は失敗したとみなされます。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が安定した動作を再開しない場合、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起動します。
6. 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、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ないため、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。

ステートフルな再起動が発生すると、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、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みなされるからです。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、回復不可能とみなされます。

スーパーバイザのスイッチオーバーおよびリセットの詳細については、第3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 モードから一時的に抜けます。再起動不可能なサービスで障害が発生すると、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、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、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 NX-OS Virtual Device Context Configuration Guide』Release 4.0 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とき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残されています。
- 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` コマンドを入力します。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; 簡易ファイル転送プロトコル)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 NX-OS Troubleshooting Guide*』 Release 4.0 を参照してください。

## 参考文献

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 (p.2-9)
- 標準 (p.2-9)
- MIB (p.2-9)
- RFC (p.2-9)
- 技術サポート (p.2-10)

## 関連資料

関連トピック	マニュアル名
仮想デバイス コンテキスト (VDC)	『Cisco NX-OS Virtual Device Context Configuration Guide』Release 4.0
スーパーバイザ スイッチオーバー トラブルシューティング	第3章「システム レベル ハイ アベイラビリティの理解」 『Cisco NX-OS Troubleshooting Guide』 Release 4.0
NX-OS の基礎	『Cisco NX-OS Fundamentals Configuration Guide』 Release 4.0
ライセンス	『Cisco NX-OS Licensing Guide』 Release 4.0

## 標準

標準	タイトル
この機能によってサポートされるようになった新規の標準 または変更された標準はありません。また、サポートされ ている既存の標準は、この機能でもサポートされます。	—

## MIB

MIB	MIB 関連のリンク
<ul style="list-style-type: none"> <li>• CISCO-SYSTEM-EXT-MIB : ciscoHaGroup、 cseSwCoresTable、cseHaRestartNotify、 cseShutDownNotify、cseFailSwCoreNotify、 cseFailSwCoreNotifyExtended</li> <li>• CISCO-PROCESS-MIB</li> <li>• CISCO-RF-MIB</li> </ul>	<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><a href="http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a></p>

## RFC

RFC	タイトル
この機能によって実装されている RFC はありません。	—

## 技術サポート

説明	リンク
TAC のホームページには、製品、テクノロジー、ソリューション、テクニカルティップス、ツールへのリンクを含め、30,000 ページに及ぶ検索可能な技術コンテンツが含まれています。Cisco.com の登録済みユーザは、このページからログインして、さらに広範なコンテンツにアクセスできます。	<a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a>



# 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、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。

- [NX-OS システム レベル ハイ アベイラビリティについて \(p.3-2\)](#)
- [ライセンス要件 \(p.3-3\)](#)
- [物理的な冗長性 \(p.3-3\)](#)
- [スーパーバイザの再起動とスイッチオーバー \(p.3-6\)](#)
- [HA ステータス情報の表示 \(p.3-9\)](#)
- [VDC ハイ アベイラビリティ \(p.3-11\)](#)
- [参考文献 \(p.3-12\)](#)

## 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 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
  - 電源モジュール
  - 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：
  - インサーブिस ソフトウェア アップグレード (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「インサーブिस ソフトウェア アップグレードの理解」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 NX-OS Unicast Routing Configuration Guide』 Release 4.0 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 NX-OS Virtual Device Context Configuration Guide』 Release 4.0 を参照してください。
  - Generic Online Diagnostic (GOLD; 汎用オンライン診断) GOLD の設定については、『Cisco NX-OS System Management Configuration Guide』 Release 4.0 を参照してください。
  - Embedded Event Manager (EEM; 組み込みイベント マネージャ) EEM の設定については、『Cisco NX-OS System Management Configuration Guide』 Release 4.0 を参照してください。
  - Smart Call Home Smart Call Home の設定については、『Cisco NX-OS System Management Configuration Guide』 Release 4.0 を参照してください。

### バーチャライゼーションのサポート

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.3-11) を参照してください。



(注) VDC の詳細については、『Cisco NX-OS Virtual Device Context Configuration Guide』 Release 4.0 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。

製品名	ライセンス要件
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。

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』 Release 4.0 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。

- [電源の冗長性 \(p.3-3\)](#)
- [ファントレイの冗長性 \(p.3-4\)](#)
- [スイッチ ファブリックの冗長性 \(p.3-4\)](#)
- [スーパーバイザ モジュールの冗長性 \(p.3-5\)](#)

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。

## 電源の冗長性

Nexus 7000 シリーズでは、電源モジュールを 3 台まで搭載できます。各電源モジュールは、入力数と入力電圧に応じて、6.0 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 つに分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 NX-OS Fundamentals Configuration Guide』 Release 4.0 の「システム管理」の章を参照してください。

[表 3-1](#) 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 3-1 電源の冗長モード

冗長モード	説明
合計電源（非冗長）	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。
電源ユニット冗長性（N+1）	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。
入力電源回路網冗長性	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。
完全冗長性	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 SFM 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後、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。



### 注意

ファントレイで障害が発生しても、代替のファントレイが用意できるまで、故障したファンを装着したままにして、正常なエアフローを確保する必要があります。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 SFM 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 Switch Fabric Card (SFC; 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、SFM 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 SFM で障害が発生すると、残りのアクティブな SFM 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 SFM 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 / 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 Generic On-Line Diagnostics ( GOLD; 汎用オンライン診断 ) 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、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、稼働中で、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 スイッチオーバー 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.3-6) 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 (p.3-6)
- デュアル スーパーバイザでの再起動 (p.3-6)
- デュアル スーパーバイザでのスイッチオーバー (p.3-6)
- スwitchオーバーの特性 (p.3-6)
- スwitchオーバーのメカニズム (p.3-7)
- スwitchオーバーの失敗 (p.3-7)
- スwitchオーバーの手動による起動 (p.3-7)
- スwitchオーバーに関する注意事項 (p.3-7)
- スwitchオーバーが可能かどうかの確認 (p.3-8)

### 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、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witch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witch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witchング モジュールがリセットされない。

## 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 プロセスを開始することはできません。

## 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、Spanning Tree Protocol (STP; スパニング ツリー プロトコル) 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` コマンドを入力します。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 プロセスを開始することはできません。



(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されません。

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` コマンドを入力します。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実行するには次の注意事項に留意してください。

- スwitchオーバーを手動で開始すると、2 つのスーパーバイザ モジュールが存在することを示すシステム メッセージが表示されます。
- スwitchオーバーは、2 つのスーパーバイザ モジュールがスイッチ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イッチ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。

- システムがスイッチ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.3-9)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以下に示します。

```
switch# show module
Mod  Ports  Module-Type                               Model                               Status
----  -
2    8       IP Storage Services Module              DS-X9308-SMIP                       ok
5    0       Supervisor/Fabric-1                     DS-X9530-SF1-K9                     active *
6    0       Supervisor/Fabric-1                     DS-X9530-SF1-K9                     ha-standby
8    0       Caching Services Module                 DS-X9560-SMAP                       ok
9    32      1/2 Gbps FC Module                      DS-X9032                             ok

Mod  Sw                Hw                World-Wide-Name(s) (WWN)
----  -
2    1.3(0.106a)      0.206            20:41:00:05:30:00:00:00 to 20:48:00:05:30:00:00:00
5    1.3(0.106a)      0.602            --
6    1.3(0.106a)      0.602            --
8    1.3(0.106a)      0.702            --
9    1.3(0.106a)      0.3              22:01:00:05:30:00:00:00 to 22:20:00:05:30:00:00:00

Mod  MAC-Address(es)                               Serial-Num
----  -
2    00-05-30-00-9d-d2 to 00-05-30-00-9d-de  JAB064605a2
5    00-05-30-00-64-be to 00-05-30-00-64-c2  JAB06350B1R
6    00-d0-97-38-b3-f9 to 00-d0-97-38-b3-fd  JAB06350B1R
8    00-05-30-01-37-7a to 00-05-30-01-37-fe  JAB072705ja
9    00-05-30-00-2d-e2 to 00-05-30-00-2d-e6  JAB06280ae9
```

\* this terminal session

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以下に示します。

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

## 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 3-2 および 3-4 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 3-2 に、冗長ステートのとり得る値を示します。

表 3-2 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 <code>failed</code> (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。この状態が続く場合は、TAC に連絡してください。

表 3-3 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 3-3 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 3-4 に、内部冗長ステートのとり得る値を示します。

表 3-4 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 (「 <a href="#">スイッチオーバーの手動による起動</a> 」 [p.3-7] を参照)。
Active with no standby	スイッチオーバーが可能です。
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	システムが HA スイッチオーバー メカニズムに移行中です。
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。
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、インサービス ソフトウェア アップグレード (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。これらのハイ アベイラビリティ機能はすべて、VDC をサポートしています。

VDC で回復不可能なエラーが発生した場合、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。

- 停止 (Bringdown) VDC を障害ステートに移行します。障害ステートから回復するには、当該 VDC を削除してから再作成する必要があります。
- 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 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 NX-OS デバイスの場合は、リロードを実行します。
- 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 NX-OS Virtual Device Context Configuration Guide*』 Release 4.0 を参照してください。

## 参考文献

システム 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 \(p.3-12\)](#)
- [標準 \(p.3-12\)](#)
- [MIB \(p.3-12\)](#)
- [RFC \(p.3-12\)](#)
- [技術サポート \(p.3-13\)](#)

## 関連資料

関連トピック	マニュアル名
仮想デバイス コンテキスト (VDC)	『Cisco NX-OS Virtual Device Context Configuration Guide』Release 4.0
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 NX-OS の基礎	『Cisco NX-OS Fundamentals Configuration Guide』 Release 4.0
ノンストップ フォワーディング (NFS)	『Cisco NX-OS Unicast Routing Configuration Guide』 Release 4.0
インサービス ソフトウェア アップグレード (ISSU)	<a href="#">第5章「インサービス ソフトウェア アップグレードの理解」</a>
GOLD、EEM、および Smart Call Home	『Cisco NX-OS System Management Configuration Guide』 Release 4.0
ライセンス	『Cisco NX-OS Licensing Guide』 Release 4.0

## 標準

標準	タイトル
この機能によってサポートされるようになった新規の標準または変更された標準はありません。また、サポートされている既存の標準は、この機能でもサポートされます。	—

## MIB

MIB	MIB 関連のリンク
<ul style="list-style-type: none"> <li>• CISCO-XXXXXX-MIB</li> </ul>	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。 <a href="http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a>

## RFC

RFC	タイトル
この機能によって実装されている RFC はありません。	—

## 技術サポート

説明	リンク
TAC のホームページには、製品、テクノロジー、ソリューション、テクニカルティップス、ツールへのリンクを含め、30,000 ページに及ぶ検索可能な技術コンテンツが含まれています。Cisco.com の登録済みユーザは、このページからログインして、さらに広範なコンテンツにアクセスできます。	<a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a>





# 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、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ついて \(p.4-2\)](#)
- [ライセンス要件 \(p.4-2\)](#)
- [スパニングツリー プロトコル \(p.4-3\)](#)
- [ファーストホップ冗長プロトコル \(p.4-4\)](#)
- [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 \(p.4-5\)](#)
- [参考文献 \(p.4-6\)](#)

## ネットワーク レベルハイ アベイラビリティについて

Cisco NX-OS のネットワーク レベル 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。

### バーチャライゼーションのサポート

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 Spanning Tree Protocol (STP; スパニング ツリー プロトコル) 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 NX-OS Virtual Device Context Configuration Guide』Release 4.0 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。

製品名	ライセンス要件
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	Border Gateway Protocol (BGP; ボーダー ゲートウェイ プロトコル) には、エンタープライズ サービス ライセンスが必要です。

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』Release 4.0 を参照してください。

## スパンニングツリー プロトコル



(注)

Spanning Tree Protocol (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。

フォールトトレラントなインターネットネットワークを作成する場合、ネットワーク上のすべてのノード間にループフリーパスを形成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。スパンニングツリー 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。スパンニングツリーの 1 つのネットワーク セグメントで障害が発生し、冗長パスが存在する場合、STP アルゴリズムはスパンニングツリー トポロジを再計算し、ブロックされたパスをアクティブにします。

Cisco NX-OS は、Multiple Spanning Tree Protocol (MSTP; 多重スパンニングツリー プロトコル) 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ンニングツリー 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、Rapid Spanning Tree Protocol (RSTP; 高速スパンニングツリー プロトコル) 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 (転送パス) で障害が発生しても他のインスタンス (転送パス) に影響しないため、ネットワークのフォールトトレランスが向上します。



(注)

スパン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のみ設定できます。レイヤ 3 インターフェイスに対してスパン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 NX-OS Interfaces Configuration Guide』Release 4.0 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 NX-OS Layer 2 Switching Configuration Guide』Release 4.0 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、First-Hop Redundancy Protocol (FHRP; ファーストホップ冗長プロトコル) 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。

- Hot Standby Router Protocol (HSRP; ホットスタンバイ ルータ プロトコル) 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。

- Virtual Router Redundancy Protocol (VRRP; 仮想ルータ冗長プロトコル) 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。
- Gateway Load Balancing Protocol (GLBP; ゲートウェイ ロード バランシング プロトコル) GLBP は、冗長なゲートウェイ間でプロトコルと Media Access Control (MAC; メディア アクセス制御) 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。すなわち、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。グループ内の残りのルータは、アクティブなルータで障害が発生するまで冗長なルータとなります。

FHRP の設定の詳細については、『Cisco NX-OS Unicast Routing Configuration Guide』 Release 4.0 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 NX-OS Unicast Routing Configuration Guide』Release 4.0 の「ハイアベイラビリティとグレースフル リスタート」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 \(p.4-5\)](#)
- [スイッチオーバーの OSPFv2 グレースフル リスタート \(p.4-5\)](#)
- [OSPFv2 プロセス障害発生時の OSPFv2 グレースフル リスタート \(p.4-5\)](#)

### 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 デ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せん。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。

## 参考文献

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 (p.4-6)
- 標準 (p.4-6)
- MIB (p.4-6)
- RFC (p.4-6)
- 技術サポート (p.4-6)

## 関連資料

関連トピック	マニュアル名
仮想デバイス コンテキスト (VDC)	『Cisco NX-OS Virtual Device Context Configuration Guide』Release 4.0
グレースフル リスタート	『Cisco NX-OS Unicast Routing Configuration Guide』Release 4.0 の「ハイ アベイラビリティとグレースフル リスタート」の章
インサービス ソフトウェア アップグレード (ISSU)	<a href="#">第5章「インサービス ソフトウェア アップグレードの理解」</a>
ライセンス	『Cisco NX-OS Licensing Guide』 Release 4.0

## 標準

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

## MIB

MIB	MIB 関連のリンク
<ul style="list-style-type: none"> <li>• CISCO-XXXXXX-MIB</li> </ul>	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。 <a href="http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a>

## RFC

RFC	タイトル
この機能によって実装されている RFC はありません。	—

## 技術サポート

説明	リンク
TAC のホームページには、製品、テクノロジー、ソリューション、テクニカル ティップス、ツールへのリンクを含め、30,000 ページに及ぶ検索可能な技術コンテンツが含まれています。Cisco.com の登録済みユーザは、このページからログインして、さらに広範なコンテンツにアクセスできます。	<a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a>



# インサーブス ソフトウェア アップグレードの理解

---

この章では、インサーブス ソフトウェア アップグレード (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 \(p.5-2\)](#)
- [ライセンス要件 \(p.5-2\)](#)
- [注意事項と制約事項 \(p.5-3\)](#)
- [ISSU の動作原理 \(p.5-3\)](#)
- [ISSU の設定 \(p.5-3\)](#)
- [参考文献 \(p.5-4\)](#)

## 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、インサーブिसソフトウェアアップグレード (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 CLI (コマンドライン インターフェイス) 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
- Connectivity Management Processor (CMP; 接続管理プロセッサ) 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。

## バーチャライゼーションのサポート

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バーチ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を実行することはできません。



(注) VDC の詳細については、『Cisco NX-OS Virtual Device Context Configuration Guide』Release 4.0 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。

製品名	ライセンス要件
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。

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』Release 4.0 を参照してください。

## 注意事項と制約事項

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。

## 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` コマンドを入力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 NX-OS Fundamentals Configuration Guide』Release 4.0 の「ソフトウェア イメージ」を参照してください。

## 参考文献

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 (p.5-4)
- 標準 (p.5-4)
- MIB (p.5-4)
- RFC (p.5-4)
- 技術サポート (p.5-4)

## 関連資料

関連トピック	マニュアル名
ISSU の設定	『Cisco NX-OS Fundamentals Configuration Guide』Release 4.0 の「ソフトウェアイメージ」の章
仮想デバイス コンテキスト (VDC)	『Cisco NX-OS Virtual Device Context Configuration Guide』Release 4.0
ライセンス	『Cisco NX-OS Licensing Guide』Release 4.0

## 標準

標準	タイトル
この機能によってサポートされるようになった新規の標準または変更された標準はありません。また、サポートされている既存の標準は、この機能でもサポートされます。	—

## MIB

MIB	MIB 関連のリンク
<ul style="list-style-type: none"> <li>• CISCO-XXXXX-MIB</li> </ul>	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。 <a href="http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a>

## RFC

RFC	タイトル
この機能によって実装されている RFC はありません。	—

## 技術サポート

説明	リンク
TAC のホームページには、製品、テクノロジー、ソリューション、テクニカルティップス、ツールへのリンクを含め、30,000 ページに及ぶ検索可能な技術コンテンツが含まれています。Cisco.com の登録済みユーザは、このページからログインして、さらに広範なコンテンツにアクセスできます。	<a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a>



## INDEX

E		O	
E メール通知		OSPF プロトコル。OSPFv2 を参照	
Smart Call Home	1-7	OSPFv2	
		再起動	4-5
F		P	
FHRP		PSS	
説明	4-4	グローバルおよびローカル同期	2-3
タイマー	1-6	説明	2-3
		プライベートおよび共有	2-3
G		R	
GLBP		RSTP	
説明	4-4	説明	4-3
H		S	
HA ポリシー		Smart Call Home	
最小ライフタイム	2-4	説明	1-7
最大再試行回数	2-4	STP	
説明	2-4	改良	1-6
HSRP		説明	4-3
説明	4-4	バーチャライゼーションの拡張	4-2
I		V	
IEEE 802.3ad		VDC	
リンク アグリゲーション	1-6	STP 拡張	4-2
ISSU		再起動	2-7
手順	5-3	システム レベル HA	3-11
M		VRRP	
MSTP		説明	4-4
説明	4-3		
MTS			
説明	2-3		

- え
- 追加資料 ix
- 永続ストレージ サービス。PSS を参照
- か
- 仮想デバイス コンテキスト。VDC を参照  
仮想ルータ冗長プロトコル。VRRP を参照  
関連資料 ix
- く
- グレースフル リスタート  
説明 4-5
- け
- ゲートウェイ ロード バランシング プロトコル。GLBP  
を参照
- こ
- 高速スパンニングツリー プロトコル。RSTP を参照
- さ
- サービス  
再起動性 2-5
- 再起動  
VDC 内 2-7  
ステートフル、説明 2-6  
ステートレス、説明 2-6
- 最小ライフタイム。HA ポリシーを参照  
最大再試行回数。HA ポリシーを参照
- し
- システム マネージャ 2-3  
説明 2-3
- 自動同期化  
条件 3-9
- 冗長ステート  
値の説明 3-9
- 資料  
関連資料 viii
- す
- スイッチオーバー  
失敗 3-7  
手動による起動 3-7  
注意事項 3-7  
特性 3-6
- スーパーバイザ モジュール  
アクティブ ステート 3-10  
手動によるスイッチオーバー 3-7  
スイッチオーバーのメカニズム 3-7  
スタンバイ ステート 3-10  
ステートの説明 3-10
- ステートフルな再起動  
説明 2-6
- ステートレスな再起動  
説明 2-6
- スパンニングツリー プロトコル。STP を参照
- そ
- ソフトウェア アップグレード  
中断 5-3
- た
- 多重スパンニングツリー プロトコル。MSTP を参照
- な
- 内部スイッチ ステート  
説明 3-10
- は
- バーチャライゼーション  
STP 拡張 4-2
- ハイ アベイラビリティ  
スイッチオーバーの特性 3-6  
スーパーバイザ モジュールのスイッチオーバー  
メカニズム 3-7  
ステータスの表示 3-9  
説明 1-2

## ふ

ファーストホップ冗長プロトコル。FHRP を参照  
プロセス  
再起動性 2-5

## ほ

ホットスタンバイ ルータ プロトコル。HSRP を参照  
ポリシー。HA ポリシーを参照

## め

メッセージおよびトランザクション サービス。MTS を  
参照

## ら

## ライセンス

BGP 4-2  
ISSU 5-2  
Smart Call Home 3-3  
VDC 3-3  
サービス レベル HA 2-2  
システム レベル HA 3-3  
ネットワーク レベル HA 4-2