



## **Cisco UCS の Release 1.0(2) から Release 1.3(1) へのアップグレード**

### **Upgrading Cisco UCS from Release 1.0(2) to Release 1.3(1)**

初版: 2010 年 05 月 18 日

Text Part Number: OL-22854-01-J

**【注意】** シスコ製品をご使用になる前に、安全上の注意（[www.cisco.com/jp/go/safety\\_warning/](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。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。シスコシステムズ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、シスコシステムズ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システムズ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 of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at <http://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. (1005R)

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。

Copyright © 2010 Cisco Systems, Inc. All rights reserved.

Copyright © 2010-2011 シスコシステムズ合同会社. All rights reserved.



## 目次

### はじめに v

対象読者 v

マニュアルの構成 v

表記法 vi

関連資料 vii

マニュアルの入手方法およびテクニカル サポート vii

### Release 1.0(2) から Release 1.3(1) へのアップグレードの概要 1

ファームウェアの概要 1

Cisco UCS Release 1.3(1) へのファームウェア アップグレード 2

Release 1.0(2) からのアップグレード時に必要な手順 3

Cisco UCS Release 1.3(1) へのアップグレードのガイドラインと注意 3

ファームウェア バージョン 6

エンドポイントでの直接のファームウェアのアップグレード 7

直接のファームウェア アップグレードのステージ 7

直接のファームウェア アップグレードの停止の影響 9

サービス プロファイル によるファームウェア アップグレード 10

ホストファームウェア パッケージ 11

管理ファームウェア パッケージ 12

サービス プロファイル によるファームウェア アップグレードのステージ 12

ファームウェアのダウングレード 13

### ファームウェアのアップグレードの前提条件の実行 15

ファームウェアのアップグレードとダウングレードの前提条件 15

すべてのコンフィギュレーション バックアップ ファイルの作成 16

ファブリック インターコネクトの全体のステータスの確認 18

クラスタ設定の高可用性ステータスとロールの確認 18

I/O モジュールのステータスの確認 19

サーバのステータスの確認	20
シャーシのサーバのアダプタのステータスの確認	21
<b>Release 1.3(1) ファームウェア イメージのダウンロード</b>	<b>23</b>
シスコからの Cisco UCS Release 1.3(1) イメージバンドルの入手	23
ファブリック インターコネクต์へのファームウェア パッケージのダウンロード	24
ファームウェア パッケージの内容の判断	26
イメージダウンロードのキャンセル	26
ファブリック インターコネクットの空き領域のチェック	27
ファブリック インターコネクต์からのファームウェアの削除	27
<b>Release 1.0(2) から Release 1.3(1) へのファームウェアのアップグレード</b>	<b>29</b>
Release 1.0(2) からのアップグレード時に必要な手順	29
アダプタ、BMC、IOM のファームウェアの Release 1.3(1) へのアップデート	30
アダプタ、BMC、IOM のファームウェアの Release 1.3(1) へのアクティベーション	31
Cisco UCS Manager ソフトウェアの Release 1.3(1) へのアクティベーション	33
クラスタのファブリック インターコネクต์ファームウェアのアクティベーション設定	34
下位ファブリック インターコネクットのファームウェアの Release 1.3(1) へのアクティベーション	34
プライマリ ファブリック インターコネクットのファームウェアの Release 1.3(1) へのアクティベーション	35
スタンドアロンファブリック インターコネクットのファームウェアの Release 1.3(1) へのアクティベーション	36
ホストファームウェア パッケージの Release 1.3(1) へのアップデート	37



## はじめに

---

この前書きの内容は次のとおりです。

- [対象読者](#), [v ページ](#)
- [マニュアルの構成](#), [v ページ](#)
- [表記法](#), [vi ページ](#)
- [関連資料](#), [vii ページ](#)
- [マニュアルの入手方法およびテクニカル サポート](#), [vii ページ](#)

## 対象読者

このガイドは、主に既存の Cisco Unified Computing System (Cisco UCS) インスタンスをアップグレードする必要があるユーザを対象にしています。

## マニュアルの構成

このマニュアルの構成は、次のとおりです。

章	タイトル	説明
第 1 章	概要	UCS Manager GUI を使用して、Cisco Unified Computing System (Cisco UCS) を、指定したリリースにアップグレードする概要を説明します。開始する前に知っておく必要があるアップグレード手順やその他の情報などが含まれます。
第 2 章	前提条件の実行	アップグレードの前提条件について説明します。

章	タイトル	説明
第 3 章	ファームウェアのダウンロード	アップグレードに必要なファームウェアがある場所と、それを Cisco UCS Manager にダウンロードする方法について説明します。
第 4 章	ファームウェアのアップグレード	アップグレードを実行するために必要な順序で従う必要がある手順について説明します。

## 表記法

このマニュアルでは、次の表記法を使用しています。

表記法	意味
<b>bold</b> フォント	コマンド、キーワード、GUI 要素、およびユーザが入力したテキストは <b>bold</b> フォントで表示されます。
<i>italic</i> フォント	マニュアルのタイトル、新規用語または重要な用語、値を指定すべき引数は <i>italic</i> のフォントで表示されます。
[ ]	角カッコの中の要素は、省略可能です。
{x y z}	必須の代替キーワードは、波カッコ内にグループ化され、垂直バーで区切られます。
[x y z]	どれか1つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
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。
courier フォント	ターミナルセッションおよびシステムから表示される情報は、courier フォントで表示されます。
<>	パスワードのように出力されない文字は、山カッコで囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!, #	コードの先頭に感嘆符 (!) またはポンド記号 (#) がある場合には、コメント行であることを示します。



(注) 「注釈」です。



ヒント 「問題解決に役立つ情報」です。



注意

「要注意」の意味です。この状況では、機器の損傷やデータの損失につながるような操作をする可能性があります。



ワンポイントアドバイス

ここで説明されている操作により時間を短縮できることを意味します。この段落で説明する操作を実行すると、時間を節約することができます。



警告

読者に対する警告を意味します。この状況では、身体に対する傷害につながるような操作をする可能性があります。

## 関連資料

Cisco Unified Computing System (Cisco UCS) に関するすべてのマニュアルの一覧を示すロードマップは、次の URL から入手できます。

<http://www.cisco.com/go/unifiedcomputing/b-series-doc>

## 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。







# 第 1 章

## Release 1.0(2) から Release 1.3(1) へのアップグレードの概要

---

この章の構成は、次のとおりです。

- [ファームウェアの概要, 1 ページ](#)
- [Cisco UCS Release 1.3\(1\) へのファームウェアアップグレード, 2 ページ](#)
- [ファームウェアのダウングレード, 13 ページ](#)

### ファームウェアの概要

Cisco UCS では、シスコから取得し、シスコによって認定されたファームウェアを使用して、Cisco UCS インスタンスのエンドポイントをサポートします。各エンドポイントは、ファームウェアが機能するために必要なインスタンスのコンポーネントです。Cisco UCS インスタンスには、次のファームウェアエンドポイントが含まれ、ファームウェアのアップグレード時にアップグレードする必要があります。

- BIOS、ストレージコントローラ（RAID コントローラ）、Cisco Integrated Management Controller (CIMC) など、サーバ上に物理的に存在するエンドポイント
- NIC および HBA ファームウェアなどのアダプタ上に物理的に存在するエンドポイントおよび Option ROM（該当する場合）
- I/O モジュール
- ファブリック インターコネクト
- Cisco UCS Manager



(注) Release 1.3(1) では、BMC の名前が CIMC Controller に変更されました。このリリースにアップグレード後、Cisco UCS Manager では BMC という用語が使われなくなります。このマニュアルでは、Release 1.3(1) を対象にしているため、BMC ではなく CIMC の用語を使うことがあります。

シスコでは、このマニュアルおよび次のテクニカルノートにおいて、ファームウェアイメージおよびファームウェアアップデート管理の一連のベストプラクティスを保持しています。『[Unified Computing System Firmware Management Best Practices](#)』

このマニュアルでは、ファームウェアの管理について、次の定義を使用しています。

<b>アップグレード</b>	エンドポイントで実行しているファームウェアを、リリースやパッチなどの他のイメージに変更します。アップグレードには、アップデートとアクティベーションが含まれます。
<b>アップデート</b>	ファームウェア イメージをエンドポイントのバックアップパーティションにコピーします。
<b>アクティブ化</b>	バックアップパーティションのファームウェアをエンドポイントのアクティブなファームウェアバージョンとして設定します。アクティベーションには、エンドポイントのリブートが必要な場合やリブートが発生する場合があります。

## Cisco UCS Release 1.3(1) へのファームウェア アップグレード

Cisco UCS Release 1.0(1) および 1.0(2) から Release 1.3(1) へのファームウェア アップグレードは、予定されたメンテナンス ウィンドウで計画する必要があります。このファームウェア アップグレードでは、次のことを想定しておく必要があります。

- クラスタ設定では、最大 1 分間のデータ トラフィックの中断。ファブリック インターコネクタ間のフェールオーバーにより、ファブリック インターコネクタと I/O モジュールのリブートに必要な長時間の中断が避けられます。
- スタンドアロン ファブリック インターコネクタでは、サーバのリブートに必要な最大 1 分間、およびファブリック インターコネクタと I/O モジュールのリブートに必要な約 10 分間のデータ トラフィックの中断。

このファームウェアのアップグレードでは、次の方法を組み合わせる必要があります。

- エンドポイントでの直接のアップグレード。2つのファブリック インターコネクタによるクラスタ設定の場合、直接のアップグレードによって、データ トラフィックの中断を最小限にすることができます。ただし、Cisco UCS インスタンスに、直接アップグレードするエンドポイントのファームウェア ポリシーをインクルードしないようにします。ファブリック イ

インターコネクが 1 つだけの Cisco UCS インスタンスでは、トラフィックの中断が避けられません。

- ホスト ファームウェア パッケージまたは管理ファームウェア パッケージ、またはその両方を含む サービス プロファイルによって、サーバエンドポイントをアップグレードします。この方法はデータ トラフィックを中断させるため、メンテナンス ウィンドウ時に実行する必要があります。



(注) 直接のアップグレードは、サーバ BIOS、ストレージコントローラ、HBA ファームウェア、HBA オプション ROM など、すべてのエンドポイントで利用できるわけではありません。これらのエンドポイントは、サーバに関連付けられているサービス プロファイルに含まれているホスト ファームウェア パッケージによって、アップグレードする必要があります。

## Release 1.0(2) からのアップグレード時に必要な手順

Cisco UCS Release 1.0(2) からアップグレードする場合、次の順序でコンポーネントをアップグレードします。この順序に従わないと、ファームウェアのアップグレードが失敗し、サーバで Cisco UCS Manager の通信に問題が発生することがあります。さらに、このマニュアルの手順と推奨されるオプションによって、データ トラフィックの中断を最小限にします。

- 1 アダプタ (インターフェイスカード) : アダプタを直接アップグレードする場合、この手順を最初に実行します。ただし、希望に応じて、この手順を省略し、ホスト ファームウェア パッケージの最後の手順としてアダプタをアップグレードできます。
- 2 BMC : ホスト ファームウェア パッケージのアダプタをアップグレードする場合、この手順を最初に実行します。
- 3 I/O モジュール。
- 4 Cisco UCS Manager。
- 5 ファブリック インターコネク。
- 6 ホスト ファームウェア パッケージ : アップグレードプロセスの最後の手順にする必要があります。サーバの追加のリポートを避けるため、この手順中に、ボードコントローラ ファームウェアをアップグレードすることをお勧めします。ホストファームウェアパッケージの BIOS とストレージコントローラのファームウェアをアップグレードする必要があります。

## Cisco UCS Release 1.3(1) へのアップグレードのガイドラインと注意

Cisco UCS インスタンスの任意のエンドポイントのファームウェアをアップデートする前に、次のガイドラインと注意を考慮してください。

## BMC の CIMC への名前の変更



(注) Release 1.3(1) では、BMC の名前が CIMC Controller に変更されました。このアップグレードの完了後、Cisco UCS Manager では BMC という用語が使われなくなります。このマニュアルでは、Release 1.3(1) を対象にしているため、BMC ではなく CIMC の用語を使用することがあります。

### 各エンドポイントの適切なタイプのファームウェア アップグレードの決定

アダプタやサーバ CIMC などの一部のエンドポイントは、直接のファームウェア アップグレードか、またはサービスプロファイルに含まれるファームウェアパッケージによって、アップグレードできます。Cisco UCS インスタンスの設定によって、これらのエンドポイントのアップグレード方法が決まります。サーバに関連付けられているサービスプロファイルに、ホストファームウェアパッケージが含まれる場合、ファームウェアパッケージによって、それらのサーバのアダプタをアップグレードします。同様に、サーバに関連付けられているサービスプロファイルに管理ファームウェアパッケージが含まれる場合、ファームウェアパッケージによって、それらのサーバの CIMC をアップグレードします。

管理ファームウェア パッケージによる CIMC のアップグレードまたは、サーバに関連付けられたサービスプロファイル内のファームウェアパッケージによるアダプタのアップグレードは、直接のファームウェア アップグレードより優先されます。サーバに関連付けられたサービスプロファイルにファームウェアパッケージが含まれる場合、エンドポイントを直接アップグレードすることはできません。直接のアップグレードを実行するには、サービス プロファイルからファームウェア パッケージを削除する必要があります。

### 部分アップグレードなし

Cisco UCS インスタンスのすべてのエンドポイントを、同じファームウェア リリースにアップデートすることをお勧めします。あるエンドポイントのファームウェア リリース内の新しい機能および修正プログラムは、別のエンドポイント内の同じ機能および修正プログラムと依存関係があることがあります。そのため、ファームウェア リリースを混在させると、通常の使用時に、パフォーマンスの問題やその他の問題を引き起こしたり、アップデートが失敗したりする可能性があります。

### サーバまたはシャーシのメンテナンスなし



注意

アップデートプロセスが完了するまで、エンドポイントを含むハードウェアの削除やメンテナンスを実行しないでください。ハードウェアが削除されるか、メンテナンスのために使用できない場合、ファームウェアのアップデートが失敗します。この失敗により、バックアップパーティションが破損することがあります。バックアップパーティションが破損したエンドポイントのファームウェアはアップデートできません。

## ファブリック インターコネク ト数

2つのファブリック インターコネク トのあるクラスタ設定の場合、ファブリック インターコネク ト間のフェールオーバーを利用して、データ トラフィックを中断せずに、エンドポイントの直接のファームウェア アップグレードを実行できます。ただし、ホストまたは管理ファームウェア パッケージによってアップグレードする必要があるエンドポイントの場合は、データ トラフィックの中断が避けられません。

単一のファブリック インターコネク トのスタンドアロン設定の場合、エンドポイントの直接のファームウェア アップグレードを実行すると、データ トラフィックの中断を最小にできます。ただし、アップグレードを完了するために、ファブリック インターコネク トをリブートする必要があるため、トラフィックの中断は避けられません。

## Cisco UCS Manager GUI ですべてのエンドポイントを同時にアクティブにしない

Cisco UCS Manager GUI を使用して、ファームウェアをアップデートする場合、[Activate Firmware] ダイアログボックスの [Filter] ドロップダウンリストで [ALL] を選択して、すべてのエンドポイントを同時にアクティブにしないでください。多くのファームウェア リリースとパッチには依存関係があり、ファームウェアのアップデートを成功させるために、エンドポイントを特定の順序でアクティブにする必要があります。この順序は、リリースやパッチの内容によって異なることがあります。すべてのエンドポイントをアクティブにすると、必要な順序でアップデートが行われることが保証されず、エンドポイント、ファブリック インターコネク ト、および Cisco UCS Manager 間の通信が中断することがあります。特定のリリースやパッチの依存関係については、リリースまたはパッチに付属するリリース ノートを参照してください。

## アクティベーションの影響

直接のアップグレード時に、アダプタに [Set Startup Version Only] を設定する必要があります。この設定では、アクティブ化されたファームウェアが pending-next-boot 状態に移行し、サーバがすぐにリブートしません。アクティブ化されたファームウェアは、サーバがリブートされるまで、アダプタで実行されているバージョンのファームウェアになりません。ホスト ファームウェア パッケージのアダプタに [Set Startup Version Only] を設定することはできません。

サーバがサービス プロファイルに関連付けられていない場合、アクティブ化されたファームウェアは pending-next-boot 状態に移行します。Cisco UCS Manager は、サーバがサービス プロファイルに関連付けられるまで、エンドポイントをリブートせず、ファームウェアをアクティブにしません。必要に応じて、関連付けられていないサーバを手動でリブートして、ファームウェアをアクティブにできます。

I/O モジュールに対して [Set Startup Version Only] を設定した場合、そのデータパス内のファブリック インターコネク トがリブートされると、I/O モジュールがリブートされます。I/O モジュールに対して、[Set Startup Version Only] を設定しない場合、I/O モジュールがリブートし、トラフィックが中断します。さらに、Cisco UCS Manager は I/O モジュールとの間でプロトコルとファームウェア バージョンの不一致を検出すると、自動的に、一致するファームウェア バージョンで I/O モジュールをアップデートし、ファームウェアをアクティブにして、再度 I/O モジュールをリブートします。

### Cisco UCS 82598KR-CI 10-Gigabit Ethernet Adapter はアップグレード不可

Cisco UCS 82598KR-CI 10-Gigabit Ethernet Adapter のファームウェア (N20-AI0002) は、製造元でハードウェアに書き込まれます。このアダプタのファームウェアはアップグレードできません。

## ファームウェアバージョン

エンドポイントのファームウェアバージョンはエンドポイントのタイプによって異なります。ファブリック インターコネクタに物理的に存在するエンドポイントのバージョンは、サーバまたは I/O モジュールに物理的に存在するバージョンと異なります。

### CIMC、I/O モジュール、アダプタのファームウェアバージョン

各 CIMC、I/O モジュール、アダプタには、フラッシュにファームウェア用の 2 つのスロットがあります。各スロットに 1 つのバージョンのファームウェアを装着します。1 つのスロットはアクティブで、他方のスロットはバックアップスロットです。コンポーネントは、アクティブとして指定されているスロットからブートします。

Cisco UCS Manager では次のファームウェアバージョンの用語が使われます。

<b>実行されているバージョン</b>	実行されているバージョンは、アクティブで、エンドポイントで使用されているファームウェアです。
<b>スタートアップバージョン</b>	スタートアップバージョンは、エンドポイントの次のブート時に使用されるファームウェアです。Cisco UCS Manager はアクティベーション操作によって、スタートアップバージョンを変更します。
<b>バックアップバージョン</b>	バックアップバージョンは、他方のスロットのファームウェアで、エンドポイントによって使用されていません。このバージョンは、エンドポイントをアップデートしたが、まだアクティブにしていないファームウェアか、または最後のアクティベーションによって交換された古いファームウェアバージョンなどです。Cisco UCS Manager はアップデート操作によって、バックアップスロットのイメージを置き換えます。

スタートアップバージョンからエンドポイントをブートできない場合、バックアップバージョンからブートします。

### ファブリック インターコネクタおよび Cisco UCS Manager のファームウェアバージョン

アクティブにできるのは、ファブリック インターコネクタのファームウェアとファブリック インターコネクタ上の Cisco UCS Manager だけです。すべてのイメージがファブリック インターコネクタに保存されるため、ファブリック インターコネクタおよび Cisco UCS Manager ファームウェアにはバックアップバージョンがありません。その結果、ブート可能ファブリック インターコネクタ イメージは、サーバ CIMC とアダプタのように、2 つに制限されません。代わりに、ブート可能ファブリック インターコネクタ イメージは、ファブリック インターコネクタのメモリの空き領域と、そこに保存されるイメージの数によって制限されます。

ファブリック インターコネクトおよび Cisco UCS Manager ファームウェアには、カーネル ファームウェアとシステムファームウェアの実行されているバージョンとスタートアップバージョンがあります。カーネル ファームウェアとシステム ファームウェアは、同じバージョンのファームウェアを実行している必要があります。

## エンドポイントでの直接のファームウェアのアップグレード

正しい手順に従って、正しい順序でアップグレードを適用すれば、エンドポイントの直接のファームウェアアップグレードと新しいファームウェアバージョンのアクティベーションによって、Cisco UCS インスタンスのトラフィックの中断が最小限になります。

次のエンドポイントのファームウェアを直接アップグレードできます。

- アダプタ
- CIMC
- I/O モジュール
- ボード コントローラ
- Cisco UCS Manager
- ファブリック インターコネクト

アダプタおよびボードコントローラファームウェアも、サービスプロファイル内のホストファームウェアパッケージによってアップグレードできます。ホストファームウェアパッケージを使用して、このファームウェアをアップグレードする場合、ファームウェアのアップグレードプロセス中に、サーバをリブートする必要がある回数を削減できます。



(注) 管理ファームウェアパッケージによる CIMC のアップグレードまたは、サーバに関連付けられたサービスプロファイル内のファームウェアパッケージによるアダプタのアップグレードは、直接のファームウェアアップグレードより優先されます。サーバに関連付けられたサービスプロファイルにファームウェアパッケージが含まれる場合、エンドポイントを直接アップグレードすることはできません。直接のアップグレードを実行するには、サービスプロファイルからファームウェアパッケージを削除する必要があります。

## 直接のファームウェアアップグレードのステージ

Cisco UCS Manager は直接アップグレードのプロセスを2つのステージに分け、サーバやその他のエンドポイントのアップタイムに影響を与えずに、システムの実行中にエンドポイントにファームウェアをプッシュできるようにします。

### アップデート

このステージでは、選択したファームウェアバージョンがプライマリ ファブリック インターコネクトから、エンドポイントのバックアップパーティションにコピーされ、ファームウェアイ

メージが破損していないことが確認されます。アップデートプロセスでは、常にバックアップスロットのファームウェアが上書きされます。

アップデート ステージは、次のエンドポイントにのみ適用されます。

- アダプタ
- CIMC
- I/O モジュール

アップデートを [Startup Version Only] と設定し、エンドポイントがすぐにリブートしないようにすることができます。これにより、いつでもアップデートを実行して、メンテナンス期間にアクティブにしてリブートできます。



#### 注意

アップデートプロセスが完了するまで、エンドポイントを含むハードウェアの削除やメンテナンスを実行しないでください。ハードウェアが削除されるか、メンテナンスのために使用できない場合、ファームウェアのアップデートが失敗します。この失敗により、バックアップパーティションが破損することがあります。バックアップパーティションが破損したエンドポイントのファームウェアはアップデートできません。

#### アクティベーション

このステージでは、指定したイメージバージョン（通常はバックアップバージョン）がスタートアップバージョンとして設定され、[Set Startup Version Only] を指定していない場合、エンドポイントがただちにリブートされます。エンドポイントがリブートされると、バックアップパーティションがアクティブなパーティションになり、アクティブなパーティションがバックアップパーティションになります。新しいアクティブなパーティションのファームウェアはスタートアップバージョンおよび実行されているバージョンになります。

指定したファームウェアイメージがすでにエンドポイントに存在するため、次のエンドポイントのみアクティベーションが必要です。

- Cisco UCS Manager
- ファブリック インターコネクト
- それらをサポートするサーバ上のボード コントローラ

ファームウェアをアクティブにすると、エンドポイントがリブートされ、新しいファームウェアがアクティブなカーネルバージョンおよびシステムバージョンになります。スタートアップファームウェアからエンドポイントをブートできない場合、デフォルトがバックアップバージョンに設定され、エラーが生成されます。



**注意**

I/O モジュールに対して [Set Startup Version Only] を設定した場合、そのデータパス内のファブリック インターコネク트가リブートされると、I/O モジュールがリブートされます。I/O モジュールに対して、[Set Startup Version Only] を設定しない場合、I/O モジュールがリブートし、トラフィックが中断します。さらに、Cisco UCS Manager は I/O モジュールとの間でプロトコルとファームウェアバージョンの不一致を検出すると、自動的に、一致するファームウェアバージョンで I/O モジュールをアップデートし、ファームウェアをアクティブにして、再度 I/O モジュールをリブートします。

## 直接のファームウェアアップグレードの停止の影響

エンドポイントで、直接のファームウェアアップグレードを実行する場合、Cisco UCS インスタンスで、1 つ以上のエンドポイントでトラフィックの中断や、停止が発生することがあります。

### ファブリック インターコネク ト ファームウェア アップグレードの停止の影響

ファブリック インターコネク トのファームウェアをアップグレードする場合、次の停止の影響や中断が発生します。

- ファブリック インターコネク トがリブートします。
- 対応する I/O モジュールがリブートします。

### Cisco UCS Manager ファームウェア アップグレードの停止の影響

Cisco UCS Manager へのファームウェア アップグレードにより、次の中断が発生します。

#### Cisco UCS Manager GUI

- Cisco UCS Manager GUI にログインしているすべてのユーザがログアウトされ、それらのセッションが終了します。
- 実行中の保存されていない作業が失われます。

#### Cisco UCS Manager CLI

telnet によってログインしているすべてのユーザがログアウトされ、それらのセッションが終了します。コンソールセッションは終了しません。

### I/O モジュール ファームウェア アップグレードの停止の影響

I/O モジュールのファームウェアをアップグレードする場合、次の停止の影響と中断が発生します。

- 単一のファブリック インターコネク トのスタンドアロン設定の場合、I/O モジュールのリブート時にデータトラフィックが中断されます。2 つのファブリック インターコネク トのクラスタ設定の場合、データトラフィックは他方の I/O モジュールおよびそのデータパス内のファブリック インターコネク トにフェールオーバーします。

- 新しいファームウェアをスタートアップバージョンとしてのみアクティブにした場合、対応するファブリックインターコネク트가リブートされると、I/Oモジュールがリブートします。
- 新しいファームウェアを実行されているバージョンおよびスタートアップバージョンとしてアクティブにした場合、I/Oモジュールがただちにリブートします。
- ファームウェアのアップグレード後に、I/Oモジュールを使用できるようになるまで最大10分かかります。

### CIMC ファームウェアアップグレードの停止の影響

サーバの CIMC のファームウェアをアップグレードした場合、CIMC と内部プロセスのみが影響を受けます。サーバトラフィックは中断しません。このファームウェアアップグレードにより、CIMC に次の停止の影響と中断が発生します。

- KVM コンソールおよび vMedia によってサーバで実行されているすべてのアクティビティが中断されます。
- すべてのモニタリングおよび IPMI ポーリングが中断されます。

### アダプタ ファームウェアアップグレードの停止の影響

アダプタのファームウェアをアクティブにし、[Set Startup Version Only] オプションを設定していない場合、次の停止の影響と中断が発生します。

- サーバがリブートします。
- サーバトラフィックが中断します。

## サービス プロファイルによるファームウェアアップグレード

サービスプロファイルを使用して、サーバの BIOS を含む、サーバおよびアダプタファームウェアをアップグレードできます。次のポリシーを定義し、それらをサーバに関連付けられているサービスプロファイルにインクルードします。

- ホストファームウェアパッケージポリシー
- 管理ファームウェアパッケージポリシー



(注) サービスプロファイルによって、I/Oモジュール、ファブリックインターコネクタ、または Cisco UCS Manager のファームウェアをアップグレードすることはできません。それらのエンドポイントのファームウェアは直接アップグレードする必要があります。

## ホスト ファームウェア パッケージ

このポリシーでは、ホスト ファームウェア パッケージ (ホスト ファームウェア パックとも呼ばれる) を構成するファームウェアバージョンのセットを指定することができます。ホストファームウェアには次のサーバおよびアダプタ エンドポイントのファームウェアが含まれます。

- アダプタ ファームウェア パッケージ
- ストレージコントローラ ファームウェア パッケージ
- ファイバチャネルアダプタ ファームウェア パッケージ
- BIOS ファームウェア パッケージ
- HBA オプション ROM パッケージ
- ボードコントローラ パッケージ



### ヒント

同じホスト ファームウェア パッケージに、複数のタイプのファームウェアを含めることができます。たとえば、ホスト ファームウェア パッケージに、BIOS ファームウェアとストレージコントローラ ファームウェアの両方を含めたり、2つの異なるモデルのアダプタのアダプタファームウェアを含めたりすることができます。ただし、同じタイプ、ベンダー、モデル番号の1つのファームウェアバージョンだけを使用できます。システムによって、エンドポイントに必要なファームウェアバージョンが認識され、他のすべてのファームウェアバージョンが無視されます。

ファームウェアパッケージは、このポリシーをインクルードしているサービスプロファイルと関連付けられたサーバすべてにプッシュされます。

このポリシーにより、同じポリシーを使用しているサービスプロファイルと関連付けられているすべてのサーバでホスト ファームウェアが同一になります。したがって、サービスプロファイルのあるサーバから別のサーバに移動した場合でも、ファームウェアのバージョンはそのまま変わりません。さらに、ファームウェアパッケージのエンドポイントのファームウェアバージョンを変更した場合、同時にその影響を受けるサービスプロファイルすべてに新しいバージョンが適用されます。また、この結果、サーバがリブートされることがあります。

このポリシーはサービスプロファイルにインクルードする必要があります。また、そのサービスプロファイルを有効にするには、サーバと関連付ける必要があります。

### 前提条件

このポリシーは他のどのポリシーにも依存していません。しかし、ファブリックインターコネクタに適切なファームウェアがダウンロードされていることを確認する必要があります。サービスプロファイルがあるサーバと Cisco UCS Manager とのアソシエーションを形成しようとしているときに、このファームウェアイメージが使用できない場合、Cisco UCS Manager はファームウェアのアップグレードを無視して、アソシエーションの形成を完了します。

## 管理ファームウェア パッケージ

このポリシーでは、管理ファームウェアパッケージ（管理ファームウェアパックとも呼ばれる）を構成するファームウェアバージョンのセットを指定することができます。管理ファームウェアパッケージには、サーバの Cisco Integrated Management Controller (CIMC) が含まれます。CIMC を直接アップグレードする場合は、このパッケージを使用する必要はありません。

ファームウェアパッケージは、このポリシーをインクルードしているサービスプロファイルと関連付けられたサーバすべてにプッシュされます。このポリシーにより、同じポリシーを使用しているサービスプロファイルと関連付けられているすべてのサーバで CIMC ファームウェアが同一になります。したがって、サービスプロファイルをあるサーバから別のサーバに移動した場合でも、ファームウェアのバージョンはそのまま変わりません。

このポリシーはサービスプロファイルにインクルードする必要があります。また、そのサービスプロファイルを有効にするには、サーバと関連付ける必要があります。

このポリシーは他のどのポリシーにも依存していません。しかし、ファブリックインターコネクタに適切なファームウェアがダウンロードされていることを確認する必要があります。

## サービス プロファイルによるファームウェア アップグレードのステージ

サービスプロファイルのホストおよび管理ファームウェアパッケージポリシーを使用して、サーバおよびアダプタ ファームウェアをアップグレードできます。



### 注意

エンドポイントを追加するか、既存のエンドポイントのファームウェア バージョンを変更することによって、ホスト ファームウェア パッケージを変更した場合、変更を保存するとすぐに、Cisco UCS Manager によって、エンドポイントがアップグレードされ、そのファームウェア パッケージに関連付けられているすべてのサーバがリブートされるため、サーバ間のデータ トラフィックが中断します。

### 新しいサービス プロファイル

新しいサービス プロファイルの場合、このアップグレードは次のステージで行われます。

**ファームウェア パッケージ ポリシーの作成** このステージでは、ホストおよび管理ファームウェア パッケージを作成し、それらを適切なファームウェア ポリシーに含めます。

**サービス プロファイルの関連付け** このステージでは、サービスプロファイルにファームウェアパッケージを含め、サービス プロファイルとサーバとのアソシエーションを形成します。システムによって、選択したファームウェア バージョンがエンドポイントにプッシュされます。ホスト ファームウェア パッケージの場合、サーバがリブートされ、エンドポイントで、ファームウェアパッケージに指定されたバージョンが確実に実行されます。

### 既存のサービス プロファイル

サービス プロファイルがすでにサーバに関連付けられている場合、ホスト ファームウェア パッケージの変更を保存するとすぐに、Cisco UCS Manager によってファームウェアがアップグレードされます。ホスト ファームウェア パッケージの場合、変更を保存するとすぐに、Cisco UCS Manager によってサーバがリブートされます。

## ファームウェアのダウングレード

Cisco UCS インスタンスのファームウェアを、アップグレードと同じ方法でダウングレードします。ファームウェアのアップデート時に選択したパッケージまたはバージョンによって、アップグレードを実行するか、ダウングレードを実行するかが決まります。

■ ファームウェアのダウングレード



## 第 2 章

# ファームウェアのアップグレードの前提条件の実行

この章の構成は、次のとおりです。

- [ファームウェアのアップグレードとダウングレードの前提条件, 15 ページ](#)
- [すべてのコンフィギュレーションバックアップファイルの作成, 16 ページ](#)
- [ファブリック インターコネクットの全体のステータスの確認, 18 ページ](#)
- [クラスタ設定の高可用性ステータスとロールの確認, 18 ページ](#)
- [I/O モジュールのステータスの確認, 19 ページ](#)
- [サーバのステータスの確認, 20 ページ](#)
- [シャーシのサーバのアダプタのステータスの確認, 21 ページ](#)

## ファームウェアのアップグレードとダウングレードの前提条件

Cisco UCS インスタンスのすべてのエンドポイントが完全に機能し、それらのエンドポイントのファームウェアのアップグレードまたはダウングレードを開始する前に、すべてのプロセスが完了している必要があります。機能状態でないエンドポイントはアップグレードまたはダウングレードすることはできません。たとえば、検出されていないサーバのファームウェアはアップグレードまたはダウングレードできません。最大回数の再試行後に失敗した FSM などの未完了のプロセスによって、エンドポイントのアップグレードやダウングレードが失敗する可能性があります。FSM が実行中の場合、Cisco UCS Manager によって、アップデートとアクティベーションがキューに入れられ、FSM が正常に完了すると、それらが実行されます。

[Equipment] タブのコンポーネントの周囲の色付けされたボックスは、そのコンポーネントのエンドポイントがアップグレードまたはダウングレードできないことを示していることがあります。

エンドポイントのアップグレードを試みる前に、そのコンポーネントのステータスを確認してください。



(注) Cisco UCS Manager GUI の [Installed Firmware] タブでは、これらの前提条件を実行するための十分な情報が得られません。

Cisco UCS インスタンスのファームウェアをアップグレードまたはダウングレードする前に、次の前提条件を実行します。

- 設定を All Configuration バックアップ ファイルにバックアップします。
- クラスタ設定の場合、ファブリックインターコネクトの高可用性ステータスに、両方が稼動中であると示されていることを確認します。
- スタンドアロン設定の場合、ファブリック インターコネクトの [Overall Status] が [Operable] であることを確認します。
- すべてのサーバ、I/O モジュール、アダプタが完全に機能することを確認します。動作不能なサーバはアップグレードできません。
- すべてのサーバが検出されていることを確認します。それらの電源が入っていることや、サービス プロファイル と関連付けられていることは必要ありません。

## すべてのコンフィギュレーションバックアップファイルの作成

この手順は、All Configuration バックアップファイルの既存のバックアップ操作がないことを前提としています。

Cisco UCS インスタンスのバックアップの詳細については、『Cisco UCS Manager GUI Configuration Guide』および『Cisco UCS Manager CLI Configuration Guide』を参照してください。

### 操作を行う前に

バックアップ サーバの IP アドレスおよび資格情報を取得します。

### 手順

- ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。
- ステップ 2 [All] ノードをクリックします。
- ステップ 3 [Work] ペインの [General] タブをクリックします。
- ステップ 4 [Actions] 領域の [Backup Configuration] をクリックします。
- ステップ 5 [Backup Configuration] ダイアログ ボックスで、[Create Backup Operation] をクリックします。
- ステップ 6 [Create Backup Operation] ダイアログボックスで、次の操作を実行します。



a) 次のフィールドに入力します。

- **[Admin State]** フィールド： **[enabled]** オプション ボタンをクリックすると、**[OK]** をクリックしてすぐに、バックアップ操作が実行されます。

- **[Type]** フィールド： **[All configuration]** オプション ボタンをクリックすると、すべてのシステムおよび論理設定情報を含む XML バックアップ ファイルが作成されます。

- **[Preserve Identities]** チェックボックス： Cisco UCS インスタンスに、プールから取得され、保存する必要がある ID が含まれる場合、このチェックボックスをオンにします。

MAC アドレス、WWNN、WWPN、UUIDS などの ID は実行時に割り当てられます。バックアップファイルのインポート後に、これらの ID を変更しない場合は、このチェックボックスをオンにする必要があります。このチェックボックスをオンにしない場合、インポートおよび PXE ブートや SAN ブートなどの操作が機能しなくなると、これらの ID が変更されることがあります。

- **[Protocol]** フィールド： ファイルをバックアップ サーバに転送するために使用するプロトコルを指示する場合に、次のいずれかのオプション ボタンをクリックします。

- **[FTP]**

- **[TFTP]**

- **[SCP]**

- **[SFTP]**

- **[Hostname]** フィールド： バックアップ ファイルを格納する場所の IP アドレスまたはホスト名を入力します。これは、サーバ、ストレージレイ、ローカル ドライブ、またはファブリック インターコネクタがネットワーク経由でアクセス可能な任意の読み取り/書き込みメディアなどがあります。ホスト名を使用する場合、Cisco UCS Manager で DNS サーバを使用するように設定する必要があります。

- **[Remote File]** フィールド： バックアップ コンフィギュレーション ファイルのフルパスを入力します。このフィールドには、ファイル名とパスを含めることができます。ファイル名を省略すると、バックアップ手順によって、ファイルに名前が割り当てられます。

- **[User]** フィールド： Cisco UCS Manager がバックアップ場所へのログインに使用する必要のあるユーザ名を入力します。プロトコルに TFTP を選択した場合は、このフィールドに入力する必要はありません。

- **[Password]** フィールド： ユーザ名に関連付けられたパスワードを入力します。プロトコルに TFTP を選択した場合は、このフィールドに入力する必要はありません。

b) **[OK]** をクリックします。

**ステップ 7** Cisco UCS Manager に確認ダイアログボックスが表示されたら、**[OK]** をクリックします。

**[Admin State]** フィールドをイネーブルに設定すると、Cisco UCS Manager によって、選択した設定タイプのスナップショットが取得され、ファイルがネットワークの場所にエクスポートされま

す。[Backup Configuration] ダイアログボックスの [Backup Operations] テーブルに、バックアップ操作が表示されます。

**ステップ 8** (オプション) バックアップ操作の進行状況を表示するには、次の操作を実行します。

a) [Properties] 領域に操作が表示されない場合、[Backup Operations] テーブルの操作をクリックします。

b) [Properties] 領域で、[FSM Details] バーの下矢印をクリックします。

[FSM Details] 領域が展開され、操作のステータスが表示されます。

**ステップ 9** [OK] をクリックし、[Backup Configuration] ダイアログボックスを閉じます。

バックアップ操作は完了するまで実行し続けます。進捗を表示するには、[Backup Configuration] ダイアログボックスを再度開きます。

## ファブリック インターコネクットの全体のステータスの確認

### 手順

**ステップ 1** [Navigation] ペインの [Equipment] タブをクリックします。

**ステップ 2** [Equipment] タブの [Equipment] ► [Fabric Interconnects] を展開します。

**ステップ 3** 確認するファブリック インターコネクットのノードをクリックします。

**ステップ 4** [Work] ペインの [General] タブをクリックします。

**ステップ 5** [Status] 領域で、[Overall Status] が [operable] であることを確認します。

ステータスが [operable] でない場合は、**show tech-support** コマンドを実行して、シスコのテクニカルサポートに問い合わせてください。ファームウェアアップグレードに進まないでください。**show tech-support** コマンドの詳細については、『Cisco UCS Troubleshooting Guide』を参照してください。

## クラスタ設定の高可用性ステータスとロールの確認

高可用性ステータスは、クラスタ設定の両方のファブリック インターコネクットで同じです。

手順

- ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。
- ステップ 2 [Equipment] タブの [Equipment] ▶ [Fabric Interconnects] を展開します。
- ステップ 3 クラスターのいずれかのファブリック インターコネクットのノードをクリックします。
- ステップ 4 [Work] ペインの [General] タブをクリックします。
- ステップ 5 [High Availability Details] 領域のフィールドが表示されていない場合は、見出しの右側の [Expand] アイコンをクリックします。
- ステップ 6 次のフィールドに次の値が表示されることを確認します。

フィールド名	必要な値
[Ready] フィールド	[Yes]
[State] フィールド	[Up]

値が異なる場合は、**show tech-support** コマンドを実行して、シスコのテクニカル サポートに問い合わせてください。ファームウェア アップグレードに進まないでください。

- ステップ 7 [Leadership] フィールドの値に注意して、ファブリック インターコネクットがプライマリであるか、下位であるかを判断します。  
この情報は、ファブリック インターコネクットのファームウェアをアップグレードするために知っておく必要があります。

## I/O モジュールのステータスの確認

手順

- ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。
- ステップ 2 [Equipment] タブの [Equipment] ▶ [Chassis] を展開します。
- ステップ 3 I/O モジュールのステータスを確認するシャーシをクリックします。
- ステップ 4 [Work] ペインの [IO Modules] タブをクリックします。
- ステップ 5 各 I/O モジュールについて、次のカラムに次の値が表示されることを確認します。

フィールド名	必要な値
[Overall Status] カラム	[ok]
[Operability] カラム	[operable]

値が異なる場合は、**show tech-support** コマンドを実行して、シスコのテクニカルサポートに問い合わせてください。ファームウェア アップグレードに進まないでください。

**ステップ 6** 手順 3 から 5 を繰り返して、各シャーシの I/O モジュールのステータスを確認します。

## サーバのステータスの確認

サーバが操作不可能な場合、Cisco UCS インスタンスの他のサーバのアップグレードに進むことができます。ただし、操作不可能なサーバはアップグレードできません。

### 手順

**ステップ 1** [Navigation] ペインの [Equipment] タブをクリックします。

**ステップ 2** [Equipment] タブの [Equipment] をクリックします。

**ステップ 3** [Work] ペインの [Servers] タブをクリックして、すべてのシャーシのすべてのサーバのリストを表示します。

**ステップ 4** 各サーバについて、次のカラムに次の値が表示されることを確認します。

フィールド名	必要な値
[Overall Status] カラム	[ok]、[unassociated]、または障害を示していないすべての値  値が、[discovery-failed] などの障害を示している場合、そのサーバのエンドポイントをアップグレードできません。
[Operability] カラム	[operable]

**ステップ 5** サーバが検出されていることを確認する必要がある場合、次の手順を実行します。

- a) 検出のステータスを確認するサーバを右クリックし、[Show Navigator] を選択します。
- b) [General] タブの [Status Details] 領域で、[Discovery State] フィールドによって、[complete] の値が表示されていることを確認します。  
[Status Details] 領域のフィールドが表示されない場合は、見出しの右側の [Expand] アイコンをクリックします。

## シャーシのサーバのアダプタのステータスの確認

### 手順

- ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。
- ステップ 2 [Equipment] タブの [Equipment] ▶ [Chassis] ▶ [Chassis Number] ▶ [Servers] を展開します。
- ステップ 3 アダプタのステータスを確認するサーバをクリックします。
- ステップ 4 [Work] ペインの [Inventory] タブをクリックします。
- ステップ 5 [Inventory] ペインの [Interface Cards] サブタブをクリックします。
- ステップ 6 各アダプタについて、次のカラムに次の値が表示されることを確認します。

フィールド名	必要な値
[Overall Status] カラム	[ok]
[Operability] カラム	[operable]

フィールドに異なる値が表示され、アダプタが操作不可能な場合、Cisco UCS インスタンスのサーバの他のアダプタのアップグレードに進むことができます。ただし、操作不可能なアダプタはアップグレードできません。





## 第 3 章

# Release 1.3(1) ファームウェア イメージのダウンロード

---

この章の構成は、次のとおりです。

- シスコからの Cisco UCS Release 1.3(1) イメージバンドルの入手, 23 ページ
- ファブリック インターコネクต์へのファームウェア パッケージのダウンロード, 24 ページ
- ファームウェア パッケージの内容の判断, 26 ページ
- イメージダウンロードのキャンセル, 26 ページ
- ファブリック インターコネクットの空き領域のチェック, 27 ページ
- ファブリック インターコネクต์からのファームウェアの削除, 27 ページ

## シスコからの Cisco UCS Release 1.3(1) イメージバンドルの入手

### 手順

---

- ステップ 1 Web ブラウザで、<http://www.cisco.com> にナビゲートします。
- ステップ 2 [Support] の下で、[Download Software] をクリックします。
- ステップ 3 [Unified Computing] をクリックします。
- ステップ 4 Cisco.com ユーザ名およびパスワードを入力して、ログインします。
- ステップ 5 [Cisco Unified Computing System] をクリックします。
- ステップ 6 [Unified Computing System (UCS) Complete Software Bundle] をクリックします。
- ステップ 7 [Latest Releases] フォルダの下での最新の 1.3(1) リリースのリンクをクリックします。

[Latest Releases] フォルダに、Cisco UCS Release 1.3(1) が表示されない場合は、[All Releases] ▶ [1.3] を展開します。

**ステップ 8** [Release Notes] リンクをクリックして、リリース ノートの最新バージョンをダウンロードします。

**ステップ 9** 次のいずれかのボタンをクリックして、表示される指示に従います。

- [Download Now] : ファームウェア イメージをすぐにダウンロードできます。
- [Add to Cart] : 後でダウンロードするファームウェア イメージをカートに追加します。

**ステップ 10** プロンプトに従って、イメージのダウンロードを実行します。

**ステップ 11** Cisco UCS をアップグレードする前にリリース ノートをお読みください。

### 次の手順

ファームウェア イメージをファブリック インターコネク トにダウンロードします。

## ファブリック インターコネク トへのファームウェア パッケージのダウンロード

同じ手順で、1つのファームウェア イメージをファブリック インターコネク トにダウンロードできます。



(注)

クラスター セットアップでは、ダウンロードの開始に使用されたファブリック インターコネク トに関係なく、ファームウェア パッケージは自動的に両方のファブリック インターコネク トにダウンロードされます。Cisco UCS Manager により、両方のファブリック インターコネク トのすべてのパッケージおよびイメージの同期状態が保たれます。ファブリック インターコネク トの1つがダウンした場合でも、ダウンロードは正常に終了します。オンラインに復帰したときに、イメージがもう片方のファブリック インターコネク トに同期されます。

### 操作を行う前に

シスコからファームウェア パッケージまたはイメージを取得します。



## 手順

- ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。
- ステップ 2 [Equipment] ノードをクリックします。
- ステップ 3 [Work] ペインの [Firmware Management] タブをクリックします。
- ステップ 4 [Installed Firmware] タブをクリックします。
- ステップ 5 [Download Firmware] をクリックします。
- ステップ 6 [Download Firmware] ダイアログボックスで、次の操作を実行します。

名前	説明
[Protocol] フィールド	<p>リモートサーバとの通信時に使用するプロトコル。ここに指定できる値は次のとおりです。</p> <ul style="list-style-type: none"> <li>• [FTP]</li> <li>• [TFTP]</li> <li>• [SCP]</li> <li>• [SFTP]</li> </ul> <p>(注) TFTP には、32 MB のファイル サイズ制限があります。ファームウェア バンドルは、はるかに大きくなることもあるため、ファームウェアのダウンロードには、TFTP を選択しないことをお勧めします。</p>
[Server] フィールド	<p>ファイルが存在するリモート サーバの IP アドレスまたはホスト名。</p> <p>(注) IP アドレスではなくホスト名を使用する場合、Cisco UCS Manager で DNS サーバを設定する必要があります。</p>
[Filename] フィールド	ダウンロードするファームウェア実行可能ファイルの名前。
[Remote Path] フィールド	<p>必要に応じて、リモートサーバ上のファイルの絶対パスを指定します。</p> <p>SCP を使用する場合、絶対パスは常に必要です。他のプロトコルを使用する場合は、ファイルがデフォルトのダウンロードフォルダに存在すれば、リモートパスを指定する必要がありません。ファイルサーバの設定方法の詳細については、システム管理者に問い合わせてください。</p>
[User] フィールド	システムがリモートサーバへのログインに使用する必要のあるユーザ名。プロトコルが TFTP の場合、このフィールドは適用されません。

名前	説明
[Password] フィールド	リモート サーバのユーザ名のパスワード。プロトコルが TFTP の場合、このフィールドは適用されません。

Cisco UCS Manager GUI によって、ファームウェア バンドルのファブリック インターコネク トへのダウンロードが開始されます。

**ステップ 7** [OK] をクリックします。

**ステップ 8** (オプション) [Download Tasks] タブで、イメージダウンロードのステータスをモニタします。  
 (注) Cisco UCS Manager によって、ブートフラッシュの領域が不足していることが報告された場合は、古いイメージを削除して、領域を解放します。ブートフラッシュの空き領域を表示するには、[Equipment] タブのファブリック インターコネク トにナビゲートし、[General] タブの [Local Storage Information] 領域を展開します。

#### 次の手順

エンドポイントのファームウェアをアップデートします。

## ファームウェア パッケージの内容の判断

#### 手順

**ステップ 1** [Navigation] ペインの [Equipment] タブをクリックします。

**ステップ 2** [Admin] タブの [Equipment] ノードをクリックします。

**ステップ 3** [Work] ペインの [Firmware Management] タブをクリックします。

**ステップ 4** [Packages] サブタブで、パッケージの内容を表示するには、パッケージの横の [+] アイコンをクリックします。

**ステップ 5** パッケージの内容のスナップショットを取得するには、次の手順を実行します。

- a) イメージ名とその内容を含む行を強調表示します。
- b) 右クリックし、[Copy] を選択します。
- c) クリップボードの内容をテキスト ファイルまたはその他のドキュメントに貼り付けます。

## イメージ ダウンロードのキャンセル

イメージのダウンロードは実行中にのみキャンセルできます。イメージのダウンロードの完了後に、ダウンロード タスクを削除しても、ダウンロード済みのイメージは削除されません。

## 手順

- ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。
- ステップ 2 [Equipment] ノードを展開します。
- ステップ 3 [Work] ペインの [Firmware Management] タブを選択します。
- ステップ 4 [Download Tasks] タブで、キャンセルするタスクを右クリックし、[Delete] を選択します。

# ファブリック インターコネクットの空き領域のチェック

イメージのダウンロードが失敗したら、Cisco UCS でファブリック インターコネクットのブートフラッシュに十分な空き領域があるかどうかをチェックします。

## 手順

- ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。
- ステップ 2 [Equipment] タブの [Equipment] ► [Fabric Interconnects] を展開します。
- ステップ 3 空き領域をチェックするファブリック インターコネクットをクリックします。
- ステップ 4 [Work] ペインの [General] タブをクリックします。
- ステップ 5 [Local Storage Information] 領域を展開します。  
ファームウェアイメージバンドルをダウンロードする場合、ファブリック インターコネクットに、ファームウェア イメージバンドルのサイズの少なくとも 2 倍の空き領域が必要です。ブートフラッシュに十分な領域がない場合は、ファブリック インターコネクットから、古いファームウェア、コア ファイル、その他の不要なオブジェクトを削除してください。

# ファブリック インターコネクットからのファームウェアの削除

Cisco UCS Release 1.3(1) 以前のリリースでは、[Packages] タブからファームウェア パッケージを削除できません。パッケージからすべてのイメージを削除すると、Cisco UCS Manager によってパッケージが削除されます。

## 操作を行う前に

ファームウェア パッケージとその内容を削除する前に、パッケージの内容を判断することをお勧めします。

## 手順

---

- ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。
  - ステップ 2 [Equipment] タブの [Equipment] ノードを展開します。
  - ステップ 3 [Work] ペインの [Firmware Management] タブをクリックします。
  - ステップ 4 [Firmware Management] タブで、[Images] タブをクリックします。
  - ステップ 5 表で、削除するイメージをクリックします。  
Shift キーまたは Ctrl キーを使用して、複数のエントリを選択できます。
  - ステップ 6 強調表示されたイメージを右クリックし、[Delete] を選択します。
  - ステップ 7 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。
-



## 第 4 章

# Release 1.0(2) から Release 1.3(1) へのファームウェアのアップグレード

この章の構成は、次のとおりです。

- [Release 1.0\(2\) からのアップグレード時に必要な手順, 29 ページ](#)
- [アダプタ、BMC、IOM のファームウェアの Release 1.3\(1\) へのアップデート, 30 ページ](#)
- [アダプタ、BMC、IOM のファームウェアの Release 1.3\(1\) へのアクティベーション, 31 ページ](#)
- [Cisco UCS Manager ソフトウェアの Release 1.3\(1\) へのアクティベーション, 33 ページ](#)
- [クラスタのファブリック インターコネクト ファームウェアのアクティベーション設定, 34 ページ](#)
- [スタンドアロン ファブリック インターコネクトのファームウェアの Release 1.3\(1\) へのアクティベーション, 36 ページ](#)
- [ホストファームウェアパッケージの Release 1.3\(1\) へのアップデート, 37 ページ](#)

## Release 1.0(2) からのアップグレード時に必要な手順

Cisco UCS Release 1.0(2) からアップグレードする場合、次の順序でコンポーネントをアップグレードします。この順序に従わないと、ファームウェアのアップグレードが失敗し、サーバで Cisco UCS Manager の通信に問題が発生することがあります。さらに、このマニュアルの手順と推奨されるオプションによって、データトラフィックの中断を最小限にします。

- 1 アダプタ（インターフェイスカード）：アダプタを直接アップグレードする場合、この手順を最初に実行します。ただし、希望に応じて、この手順を省略し、ホストファームウェアパッケージの最後の手順としてアダプタをアップグレードできます。
- 2 BMC：ホストファームウェアパッケージのアダプタをアップグレードする場合、この手順を最初に実行します。

- 3 I/O モジュール。
- 4 Cisco UCS Manager。
- 5 ファブリック インターコネクト。
- 6 ホストファームウェアパッケージ：アップグレードプロセスの最後の手順にする必要があります。サーバの追加のリポートを避けるため、この手順中に、ボードコントローラファームウェアをアップグレードすることをお勧めします。ホストファームウェアパッケージの BIOS とストレージコントローラのファームウェアをアップグレードする必要があります。

## アダプタ、BMC、IOM のファームウェアの Release 1.3(1) へのアップデート



### 注意

アップデートプロセスが完了するまで、エンドポイントを含むハードウェアの削除やメンテナンスを実行しないでください。ハードウェアが削除されるか、メンテナンスのために使用できない場合、ファームウェアのアップデートが失敗します。この失敗により、バックアップパーティションが破損することがあります。バックアップパーティションが破損したエンドポイントのファームウェアはアップデートできません。

### 手順

- ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。
- ステップ 2 [Equipment] タブの [Equipment] ノードを展開します。
- ステップ 3 [Work] ペインの [Firmware Management] タブをクリックします。
- ステップ 4 [Installed Firmware] サブタブの [Update Firmware] をクリックします。  
Cisco UCS Manager GUI によって、[Update Firmware] ダイアログボックスが開き、Cisco UCS インスタンスのすべてのエンドポイントのファームウェアバージョンが確認されます。この手順は、シャーシとサーバの数によって、数分かかることがあります。
- ステップ 5 [Update Firmware] ダイアログボックスで、次の操作を実行します。
  - a) メニューバーの [Filter] ドロップダウンリストから、[ALL] を選択します。  
特定のタイプのエンドポイントを一度にアップデートする場合は、[Filter] ドロップダウンリストからそのエンドポイントを選択します。
  - b) メニューバーの [Set Version] ドロップダウンリストから、Release 1.3(1) ファームウェアバンドルに含まれるファームウェアバージョンを選択します。
  - c) [OK] をクリックします。  
サーバのサービスプロファイルにホストファームウェアパッケージが含まれる場合、Cisco UCS Manager はそのサーバのアダプタファームウェアをアップデートできません。通知メッセージの確認をすると、Cisco UCS Manager によって、ホストファームウェアパッケージが関連付けられていないサーバのその他のすべてのエンドポイントのファームウェアがアップデー

トされます。サーバのアダプタ ファームウェアを直接アップデートする場合、関連付けられたサービス プロファイルからすべてのホスト ファームウェア パッケージを削除する必要があります。ホスト ファームウェア パッケージからアダプタ ファームウェアを削除しても、アダプタを直接アップデートできるようにするために十分ではありません。

Cisco UCS Manager によって、選択したファームウェア イメージがバックアップ メモリ パーティションにコピーされ、そのイメージが破損していないことが確認されます。イメージは、明示的にアクティブにするまで、バックアップ バージョンとして残されます。Cisco UCS Manager はすべてのアップデートを同時に開始します。ただし、アップデートによって、完了する時間が異なることがあります。

[Update Firmware] ダイアログボックスで、すべてのアップデート済みエンドポイントについて、[Update Status] カラムに [ready] と表示されると、アップデートは完了です。

**ステップ 6** (オプション) 特定のエンドポイントのアップデートの進捗をモニタするには、エンドポイントを右クリックし、[Show Navigator] を選択します。

Cisco UCS Manager によって、[General] タブの [Update Status] 領域に進捗が表示されます。ナビゲータに [FSM] タブがある場合は、そこでも進捗をモニタできます。[Retry #] フィールドのエントリに、アップデートが失敗したことが示されないことがあります。再試行回数には、Cisco UCS Manager がアップデート ステータスを取得するときに、発生する再試行も含まれます。

#### 次の手順

ファームウェアをアクティブにします。

## アダプタ、BMC、IOM のファームウェアの Release 1.3(1) へのアクティベーション

この手順により、これらのエンドポイントのファームウェアのアクティベーションで、データトラフィックの中断を最小限に抑えることができます。正しいオプションを設定した次の順序でエンドポイントをアクティブにしないと、エンドポイントがリポートし、データトラフィックが一時的に中断する可能性があります。



#### 注意

[Activate Firmware] ダイアログボックスの [Filter] ドロップダウンリストで [ALL] を選択して、すべてのエンドポイントを同時にアクティブにしないでください。多くのファームウェア リリースとパッチには依存関係があり、ファームウェアのアップデートを成功させるために、エンドポイントを特定の順序でアクティブにする必要があります。この順序は、リリースやパッチの内容によって異なることがあります。すべてのエンドポイントをアクティブにすると、必要な順序でアップデートが行われることが保証されず、エンドポイント、ファブリック インターコネクタ、および Cisco UCS Manager 間の通信が中断することがあります。特定のリリースやパッチの依存関係については、リリースまたはパッチに付属するリリース ノートを参照してください。

この手順は、[アダプタ、BMC、IOM のファームウェアの Release 1.3\(1\) へのアップデート](#), 30 ページから直接続いており、[Firmware Management] タブを表示していることを前提としています。

## 手順

- ステップ 1** [Installed Firmware] タブの [Activate Firmware] をクリックします。  
1 つ以上の選択したエンドポイントが、バックアップバージョンとして目的のバージョンで設定されていない場合、Cisco UCS Manager GUI によって、[Set Version] ドロップダウンリストにそのバージョンが表示されません。各エンドポイントについて、[Startup Version] カラムからバージョンを選択する必要があります。
- ステップ 2** アダプタ ファームウェアが、サービス プロファイルのホスト ファームウェア パッケージによってアップデートされていない場合は、[Activate Firmware] ダイアログボックスで、次の手順を実行して、アダプタ ファームウェアをアクティブにします。
- [Filter] ドロップダウン リストから、[Interface Cards] を選択します。
  - [Set Version] ドロップダウン リストから、Release 1.3(1) ファームウェア バンドルに含まれるファームウェア バージョンを選択します。
  - [Ignore Compatibility Check] チェックボックスをオンにします。  
このリリースのファームウェアは以前のリリースと互換性がありません。そのため、アクティベーションを成功させるために、[Ignore Compatibility Check] チェックボックスをオンにする必要があります。
  - [Set Startup Version Only] チェックボックスをオンにします。  
(注) 直接のアップグレード時に、アダプタに [Set Startup Version Only] を設定する必要があります。この設定では、アクティブ化されたファームウェアが `pending-next-boot` 状態に移行し、サーバがすぐにリブートしません。アクティブ化されたファームウェアは、サーバがリブートされるまで、アダプタで実行されているバージョンのファームウェアになりません。ホストファームウェアパッケージのアダプタに [Set Startup Version Only] を設定することはできません。
  - [Apply] をクリックします。  
すべてのアダプタの [Activate Status] カラムに `pending-next-boot` または `ready` が表示されている場合は、ステップ 3 に進みます。
- ステップ 3** BMC ファームウェアが、サービス プロファイルの管理ファームウェア パッケージによってアップデートされていない場合は、[Activate Firmware] ダイアログボックスで、次の手順を実行して、BMC ファームウェアをアクティブにします。
- [Filter] ドロップダウン リストから、[BMC] を選択します。
  - [Set Version] ドロップダウン リストから、Release 1.3(1) ファームウェア バンドルに含まれるファームウェア バージョンを選択します。  
1 つ以上の選択したエンドポイントが、バックアップバージョンとして目的のバージョンで設定されていない場合、Cisco UCS Manager GUI によって、[Set Version] ドロップダウン リストにそのバージョンが表示されません。各エンドポイントについて、[Startup Version] カラムからバージョンを選択する必要があります。
  - [Ignore Compatibility Check] チェックボックスをオンにします。



- d) [Apply] をクリックします。  
BMC のファームウェアのアクティベーションによって、データトラフィックは中断しません。ただし、すべての KVM セッションに割り込み、サーバに接続しているすべての vMedia が切断されます。

すべての BMC コンポーネントの [Activate Status] カラムに [ready] が表示されている場合は、ステップ 4 に進みます。

**ステップ 4** IOM ファームウェアをアクティブにするには、[Activate Firmware] ダイアログボックスで、次の手順を実行します。

- a) [Filter] ドロップダウンリストから、[IO Modules] を選択します。
- b) [Set Version] ドロップダウンリストから、Release 1.3(1) ファームウェア バンドルに含まれるファームウェアバージョンを選択します。
- c) [Ignore Compatibility Check] チェックボックスをオンにします。
- d) [Set Startup Version Only] チェックボックスをオンにします。

**重要** I/O モジュールに対して [Set Startup Version Only] を設定した場合、そのデータパス内のファブリック インターコネクタがリブートされると、I/O モジュールがリブートされます。I/O モジュールに対して、[Set Startup Version Only] を設定しない場合、I/O モジュールがリブートし、トラフィックが中断します。さらに、Cisco UCS Manager は I/O モジュールとの間でプロトコルとファームウェアバージョンの不一致を検出すると、自動的に、一致するファームウェアバージョンで I/O モジュールをアップデートし、ファームウェアをアクティブにして、再度 I/O モジュールをリブートします。

- e) [Apply] をクリックします。  
すべての IOM の [Activate Status] カラムに [pending-next-boot] または [ready] が表示されている場合は、ステップ 5 に進みます。

**ステップ 5** [OK] をクリックします。

## Cisco UCS Manager ソフトウェアの Release 1.3(1) へのアクティベーション

この手順は、前の手順から直接続いており、[Firmware Management] タブを表示していることを前提としています。

### 手順

**ステップ 1** [Installed Firmware] サブタブの [Activate Firmware] をクリックします。

Cisco UCS Manager GUI によって、[Update Firmware] ダイアログボックスが開き、Cisco UCS インスタンスのすべてのエンドポイントのファームウェアバージョンが確認されます。この手順は、シャーシとサーバの数によって、数分かかることがあります。

- ステップ 2** [Filter] ドロップダウン リストから、[UCS Manager] を選択します。
- ステップ 3** [Activate Firmware] ダイアログ ボックスの [UCS Manager] 行で、次の手順を実行します。
- [Startup Version] カラムのドロップダウン リストから、Release 1.3(1) ファームウェア バンドルに含まれているファームウェア バージョンを選択します。
  - [Ignore Compatibility Check] チェックボックスをオンにします。
- ステップ 4** [OK] をクリックします。
- Cisco UCS Manager はすべてのアクティブなセッションを切断し、すべてのユーザをログアウトさせて、ソフトウェアをアクティブにします。アップグレードが完了すると、再度ログインするように求められます。
- 

## クラスタのファブリック インターコネクット ファームウェアのアクティベーション設定

### 下位ファブリック インターコネクットのファームウェアの Release 1.3(1) へのアクティベーション

#### 操作を行う前に

クラスタの下位ファブリック インターコネクットであるファブリック インターコネクットを特定します。詳細については、[クラスタ設定の高可用性ステータスとロールの確認](#)を参照してください。

#### 手順

---

- ステップ 1** [Navigation] ペインの [Equipment] タブをクリックします。
- ステップ 2** [Equipment] タブの [Equipment] ノードを展開します。
- ステップ 3** [Work] ペインの [Firmware Management] タブをクリックします。
- ステップ 4** [Installed Firmware] サブタブの [Activate Firmware] をクリックします。
- Cisco UCS Manager GUI によって、[Update Firmware] ダイアログ ボックスが開き、Cisco UCS インスタンスのすべてのエンドポイントのファームウェアバージョンが確認されます。この手順は、シャーシとサーバの数によって、数分かかることがあります。
- ステップ 5** メニューバーの [Filter] ドロップダウン リストから、[Fabric Interconnects] を選択します。
- ステップ 6** メニューバーで、[Ignore Compatibility Check] チェックボックスをオンにします。
- ステップ 7** 下位ファブリック インターコネクットの [Activate Firmware] ダイアログ ボックスの行で、次の手順を実行します。
- [Kernel] 行で、[Startup Version] カラムのドロップダウン リストから、Release 1.3(1) ファームウェア バンドルに含まれるファームウェア バージョンを選択します。

- b) [System] 行で、[Startup Version] カラムのドロップダウン リストから、Release 1.3(1) ファームウェア バンドルに含まれるファームウェア バージョンを選択します。

**ステップ 8** [Apply] をクリックします。

Cisco UCS Manager はファームウェアをアップデートし、アクティブにして、ファブリック インターコネクットと、そのファブリック インターコネクットへのデータ パス内のすべての I/O モジュールをリブートするため、そのファブリック インターコネクット間のデータ トラフィックが中断します。ただし、Cisco UCS インスタンスがトラフィックおよびポート フェールオーバーを許可するように設定されていることを前提とすると、データ トラフィックはプライマリ ファブリック インターコネクットにフェールオーバーし、中断しません。

**ステップ 9** 下位ファブリック インターコネクットの高可用性ステータスを確認します。

(注) ファブリック インターコネクットの [High Availability Status] 領域に次の値が表示されない場合は、シスコのテクニカル サポートに問い合わせてください。プライマリ ファブリック インターコネクットのアップデートに進まないでください。

フィールド名	必要な値
[Ready] フィールド	[Yes]
[State] フィールド	[Up]

#### 次の手順

下位のファブリック インターコネクットの高可用性状態に、必要な値が含まれている場合、プライマリ ファブリック インターコネクットをアップデートし、アクティブにします。

## プライマリファブリックインターコネクットのファームウェアのRelease 1.3(1) へのアクティベーション

この手順は、[下位ファブリック インターコネクットのファームウェアの Release 1.3\(1\) へのアクティベーション, 34 ページ](#) から直接続いており、[Firmware Management] タブを表示していることを前提としています。

#### 操作を行う前に

下位のファブリック インターコネクットをアクティブにします。

#### 手順

**ステップ 1** [Installed Firmware] サブタブの [Activate Firmware] をクリックします。

Cisco UCS Manager GUI によって、[Update Firmware] ダイアログ ボックスが開き、Cisco UCS インスタンスのすべてのエンドポイントのファームウェアバージョンが確認されます。この手順は、シャーシとサーバの数によって、数分かかることがあります。

## スタンドアロンファブリック インターコネクットのファームウェアの Release 1.3(1) へのアクティベーション

- ステップ 2** メニュー バーの [Filter] ドロップダウン リストから、[Fabric Interconnects] を選択します。
- ステップ 3** メニュー バーで、[Ignore Compatibility Check] チェックボックスをオンにします。
- ステップ 4** 下位ファブリック インターコネクットの [Activate Firmware] ダイアログ ボックスの行で、次の手順を実行します。
- [Kernel] 行で、[Startup Version] カラムのドロップダウン リストから、Release 1.3(1) ファームウェア バンドルに含まれるファームウェア バージョンを選択します。
  - [System] 行で、[Startup Version] カラムのドロップダウン リストから、Release 1.3(1) ファームウェア バンドルに含まれるファームウェア バージョンを選択します。
- ステップ 5** [Apply] をクリックします。
- Cisco UCS Manager はファームウェアをアップデートし、アクティブにして、ファブリック インターコネクットと、そのファブリック インターコネクットへのデータ パス内のすべての I/O モジュールをリブートするため、そのファブリック インターコネクット間のデータトラフィックが中断します。ただし、Cisco UCS インスタンスが、トラフィックおよびポート フェールオーバーを許可するように設定されていることを前提とすると、データトラフィックは、他のファブリック インターコネクットにフェールオーバーし、そのファブリック インターコネクットがプライマリになります。インターコネクットが復帰すると、このファブリック インターコネクットは従属ファブリック インターコネクットになります。
- ステップ 6** ファブリック インターコネクットの高可用性ステータスを確認します。
- (注) ファブリック インターコネクットの [High Availability Status] 領域に次の値が表示されない場合は、シスコのテクニカル サポートに問い合わせてください。

フィールド名	必要な値
[Ready] フィールド	[Yes]
[State] フィールド	[Up]

## スタンドアロンファブリック インターコネクットのファームウェアの Release 1.3(1) へのアクティベーション

単一のファブリック インターコネクットのスタンドアロン設定の場合、エンドポイントの直接のファームウェア アップグレードを実行すると、データトラフィックの中断を最小にできます。ただし、アップグレードを完了するために、ファブリック インターコネクットをリブートする必要があるため、トラフィックの中断は避けられません。

## 手順

- ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。
- ステップ 2 [Equipment] タブの [Equipment] ノードを展開します。
- ステップ 3 [Work] ペインの [Firmware Management] タブをクリックします。
- ステップ 4 [Installed Firmware] サブタブの [Activate Firmware] をクリックします。  
Cisco UCS Manager GUI によって、[Update Firmware] ダイアログボックスが開き、Cisco UCS インスタンスのすべてのエンドポイントのファームウェアバージョンが確認されます。この手順は、シャーシとサーバの数によって、数分かかることがあります。
- ステップ 5 [Filter] ドロップダウン リストから、[Fabric Interconnects] を選択します。
- ステップ 6 メニュー バーで、[Ignore Compatibility Check] チェックボックスをオンにします。
- ステップ 7 ファブリック インターコネクットの [Activate Firmware] ダイアログボックスの行で、次の手順を実行します。
  - a) [Kernel] 行で、[Startup Version] カラムのドロップダウン リストから、Release 1.3(1) ファームウェア バンドルに含まれるファームウェア バージョンを選択します。
  - b) [System] 行で、[Startup Version] カラムのドロップダウン リストから、Release 1.3(1) ファームウェア バンドルに含まれるファームウェア バージョンを選択します。
- ステップ 8 [OK] をクリックします。

Cisco UCS Manager はファームウェアをアクティブにして、ファブリック インターコネクットと、そのファブリック インターコネクットへのデータパス内のすべての I/O モジュールをリブートします。スタンドアロンファブリック インターコネクットでは、これにより、Cisco UCS インスタンスのすべてのデータトラフィックが中断します。

# ホスト ファームウェア パッケージの Release 1.3(1) へのアップデート

Release 1.3(1) にアップグレードする場合、ホスト ファームウェア パッケージによって BIOS とストレージコントローラのファームウェアをアップグレードする必要があります。それらのパッケージをアップグレードしないと、サーバで、Cisco UCS Manager および BMC の通信に問題が発生することがあります。



### 注意

ポリシーが、サーバに関連付けられている 1 つまたは複数のサービス プロファイルにインクルードされている場合、ホスト ファームウェア パッケージ ポリシーを保存するとすぐに、Cisco UCS Manager によって、サーバおよびアダプタのファームウェアが新しいバージョンでアップデートされ、アクティブにされて、サーバがリブートされます。

この手順では、ホストファームウェアパッケージがすでに存在することを前提としています。ホストファームウェアパッケージの作成方法については、『Cisco UCS Manager GUI Configuration Guide』または『Cisco UCS Manager CLI Configuration Guide』を参照してください。

### 操作を行う前に

ホストファームウェアパッケージをアップデートする前に、次の手順を実行します。

- Cisco UCS Manager およびファブリック インターコネクトをアップグレードします。
- 適切なメンテナンス ウィンドウを判断し、サーバのリブート時のデータ トラフィックの中断の影響を緩和します。
- サーバの 1.3(1) ファームウェア バージョンとモデル番号 (PID) を知っていることを確認します。

### 手順

- 
- ステップ 1** [Navigation] ペインの [Servers] タブをクリックします。
- ステップ 2** [Servers] タブの [Servers] ► [Policies] を展開します。
- ステップ 3** アップデートするポリシーを含む組織のノードを展開します。  
システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。
- ステップ 4** [Host Firmware Packages] を展開し、アップデートするポリシーを選択します。
- ステップ 5** 右側の表で、次の手順を実行して、アップデートするファームウェアの既存のエントリを削除します。
- a) 表の、変更するファームウェア バージョンの行を選択します。
  - b) 右クリックし、[Delete] を選択します。
  - c) [Yes] をクリックして、そのエントリを削除することを確認します。
- ステップ 6** [General] タブで、下矢印をクリックして、左側の 1 つ以上の次のセクションを展開します。
- アダプタ ファームウェア パッケージ
  - ストレージ コントローラ ファームウェア パッケージ
  - ファイバチャネルアダプタ ファームウェア パッケージ
  - BIOS ファームウェア パッケージ
  - HBA オプション ROM パッケージ
  - ボード コントローラ パッケージ
- ステップ 7** パッケージにファームウェアを含めるエンドポイントの各セクションで、次の手順を実行します。
- a) 表の、パックを追加するファームウェア バージョンの行を選択します。  
デフォルトで、エントリがベンダー名でソートされます。エントリをソートするには、カラム見出しをクリックします。
  - b) 行を右側の表にドラッグします。

ファームウェアバージョンは、このファームウェアパックに関連付けられているサーバのモデル番号 (PID) と一致している必要があります。誤ったモデル番号のファームウェアバージョンを選択した場合、Cisco UCS Manager によってファームウェアアップデートをインストールできません。

c) [Yes] をクリックして、正しいバージョンを選択したことを確認します。

**ステップ 8** この管理ファームウェアパッケージに、別のモデル番号 (PID) のサーバのファームウェアアップデートを含める必要がある場合は、ステップ 6 と 7 を繰り返します。

**ステップ 9** [Save Changes] をクリックします。

Cisco UCS Manager によって、このポリシーをインクルードしているサービスプロファイルに関連付けられているすべてのサーバに照らして、モデル番号とベンダーが検証されます。モデル番号とベンダーが、ポリシーのファームウェアバージョンと一致していれば、Cisco UCS Manager によってファームウェアがアップデートされます。

---

### 次の手順

ホストファームウェアパッケージに含まれるエンドポイントのファームウェアが Release 1.3(1) にアップデートされたことを確認します。ファームウェアがアップデートされていない場合は、ホストファームウェアパッケージのモデル番号とベンダーをアップデートされたエンドポイントのそれらと照らして確認します。

