



## 概要

---

この章は、次の項で構成されています。

- [概要, 1 ページ](#)
- [ファームウェア アップグレードをサポートするコンポーネント, 8 ページ](#)
- [ファームウェア バージョンの用語, 9 ページ](#)
- [バージョンをまたがるファームウェアのサポート, 10 ページ](#)
- [サーバパック, 12 ページ](#)
- [軽量アップグレード, 13 ページ](#)
- [FI クラスタ用のファームウェア自動同期, 16 ページ](#)
- [ファームウェア アップグレードのオプション, 17 ページ](#)
- [Cisco UCS 6200 シリーズ ファブリック インターコネクトから Cisco UCS 6300 シリーズ ファブリック インターコネクトへの移行中のファームウェア アップグレード, 24 ページ](#)
- [Cisco UCS Manager リリース 3.2 へのファームウェア アップグレード, 25 ページ](#)
- [マイナーまたはパッチ リリースへのファームウェア アップグレード, 26 ページ](#)
- [ファームウェアのダウングレード, 27 ページ](#)
- [Cisco UCS Central のファームウェア管理, 28 ページ](#)

## 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 ドメイン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 Cisco UCS ドメインのコンポーネントであり、機能するためにはファームウェアが必要です。

このガイドでは、Cisco UCS Manager を使用して、ファームウェアを取得し、Cisco UCS ドメインのエンドポイントをアップグレードする方法について説明します。また、これらのエンドポイントをアップグレードする際に従う必要があるベストプラクティスについても詳しく説明します。

Cisco UCS Manager リリース 3.1(1) 以降、シスコは Cisco UCS Manager の各リリースと併せて、次の各プラットフォーム用のユニファイド Cisco UCS Manager ソフトウェアおよびファームウェアアップグレードをリリースしました。

- Cisco UCS 6300 シリーズ Fabric Interconnect と Cisco UCS B シリーズ、および C シリーズサーバ
- Cisco UCS 6200 シリーズ Fabric Interconnect と Cisco UCS B シリーズ、および C シリーズサーバ

- Cisco UCS 6324 ファブリック インターコネクト (Cisco UCS B シリーズ サーバおよび C シリーズ サーバと接続) (UCS Mini と呼ばれます)

図 1: Cisco UCS 6300 シリーズ ファブリック インターコネクト (Cisco UCS B シリーズおよび C シリーズ サーバと接続)

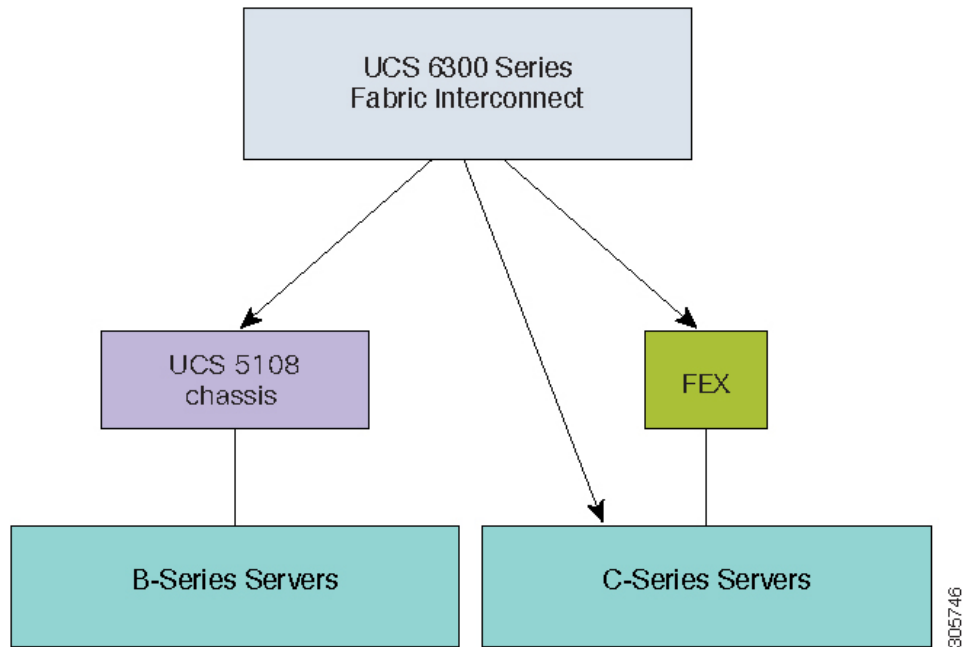


図 2: Cisco UCS 6200 シリーズ Fabric Interconnect と Cisco UCS B シリーズ、および C シリーズ サーバ

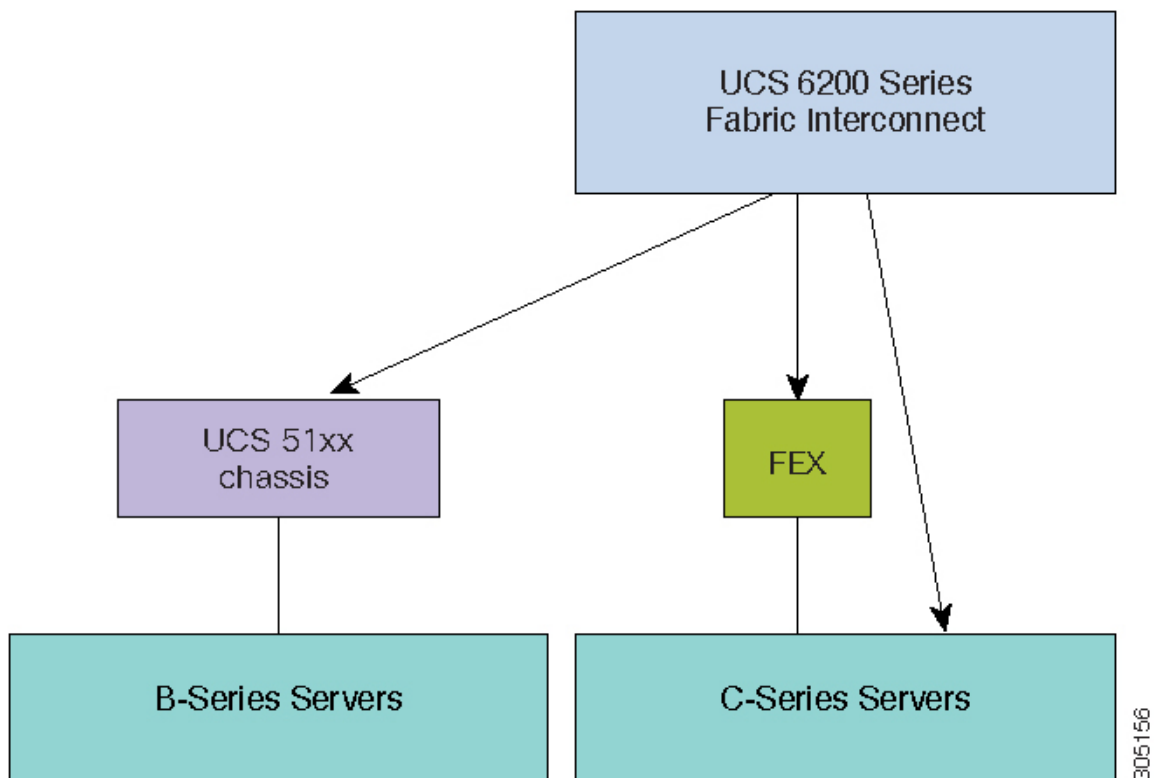
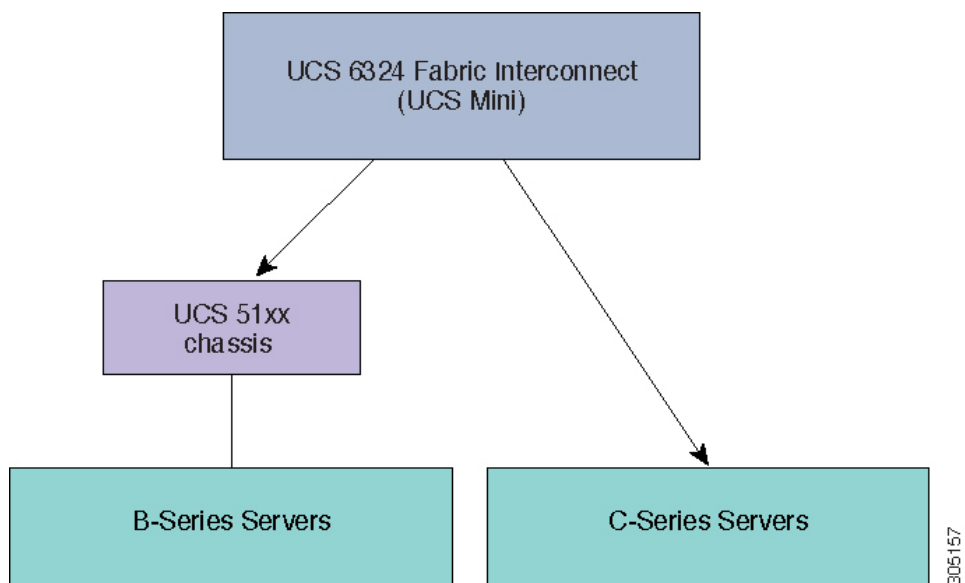


図 3 : Cisco UCS B シリーズ サーバおよび C シリーズ サーバ向け Cisco UCS 6324 ファブリック インターコネクト



次の図に、Cisco UCS Manager リリース 3.2 でサポートされる各種プラットフォームとファームウェア バンドルを示します。

各リリースには、次のファームウェア バンドルがあります。

- インフラストラクチャソフトウェアバンドル：このバンドルはAバンドルとも呼ばれます。このバンドルには、ファブリック インターコネクタ、IO モジュール、および Cisco UCS Manager が機能するために必要なファームウェア イメージが含まれています。  
Cisco UCS Manager 3.2 以降のリリースには、3 つの個別のインフラストラクチャ バンドルが含まれています。
  - Cisco UCS 6200 シリーズ ファブリック インターコネクタ：  
ucs-k9-bundle-infra.3.2.x.xxx.A.bin
  - Cisco UCS 6300 シリーズ ファブリック インターコネクタ：  
ucs-6300-k9-bundle-infra.3.2.x.xxx.A.bin
  - Cisco UCS 6324 ファブリック インターコネクタ：  
ucs-mini-k9-bundle-infra.3.2.x.xxx.A.bin
- B シリーズサーバソフトウェアバンドル：Bバンドルとも呼ばれます。このバンドルには、B シリーズ ブレードサーバが機能するために必要なファームウェア イメージ（アダプタ、BIOS、CIMC、ボードコントローラ ファームウェアなど）が含まれています。『*Release Bundle Contents for Cisco UCS Manager, Release 3.2*』には、B シリーズサーバソフトウェアバンドルの内容の詳細が掲載されています。



---

(注) Cisco UCS Manager リリース 3.1(2) から、ローカルディスクのように、B シリーズと C シリーズの両方のサーバソフトウェアバンドルに共通するエンドポイント用のファームウェアは、B シリーズと C シリーズの両方のサーバソフトウェアバンドルで入手できます。

---

- C シリーズサーバソフトウェアバンドル：Cバンドルとも呼ばれます。このバンドルには、C シリーズ ラック マウントサーバが機能するために必要なファームウェア イメージ（アダプタ、BIOS、CIMC、ボードコントローラ ファームウェアなど）が含まれています。C バンドルには、Cisco UCS S3260 ストレージサーバ用のファームウェア イメージも含まれています。『*Release Bundle Contents for Cisco UCS Manager, Release 3.2*』には、C シリーズサーバソフトウェアバンドルの内容の詳細が掲載されています。



---

(注) Cisco UCS Manager リリース 3.1(2) から、ローカルディスクのように、B シリーズと C シリーズの両方のサーバソフトウェアバンドルに共通するエンドポイント用のファームウェアは、B シリーズと C シリーズの両方のサーバソフトウェアバンドルで入手できます。

---

- 機能カタログソフトウェアバンドル：Tバンドルとも呼ばれます。このバンドルには、実装固有の調整可能なパラメータ、ハードウェア仕様、および機能制限が指定されます。

Cisco UCS Manager は機能カタログを使用して、新しく承認された DIMM やディスク ドライブなどのサーバコンポーネントの表示と設定可能性を更新します。Cisco UCS Manager 機能カタログは単一のイメージですが、Cisco UCS Manager ソフトウェアにも組み込まれています。Cisco UCS Manager リリース 3.2 以降のリリースは、任意の 3.2 カタログファイルを使用

ですが、3.1 カタログバージョンは使用できません。サーバコンポーネントが特定の BIOS バージョンに依存していない場合、それを使用したり、Cisco UCS Manager に認識させたりすることは、主にカタログバージョンの機能になります。機能カタログは、UCS インフラストラクチャリリースにバンドルされるのに加えて、スタンドアロンイメージとしてリリースされる場合もあります。

Cisco UCS ドメインのエンドポイントのアップグレード順序は、アップグレードパスによって異なります。

Cisco UCS ドメインのエンドポイントをアップグレードする適切な順序を確認するには、アップグレードパスに必要な手順の順序を参照してください。

シスコでは、このマニュアルおよびテクニカルノート『[Unified Computing System Firmware Management Best Practices](#)』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を管理するための一連のベストプラクティスを保持しています。

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。

- 更新：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。
- アクティブ化：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。



(注) 機能カタログのアップグレードの場合は、更新とアクティブ化が同時に行われます。このようなアップグレードについては、アップデートまたはアクティブ化のいずれかのみを実行する必要があります。両方の手順を実行する必要はありません。

## Cisco UCS Manager ユーザマニュアル

Cisco UCS Manager では、次の表に示す、使用例を基本とした従来よりもコンパクトな新しいマニュアルが用意されています。

ガイド	説明
<a href="#">『Cisco UCS Manager Getting Started Guide』</a>	Cisco UCS アーキテクチャのほか、Cisco UCS Manager の初期設定や構成のベストプラクティスなど、稼働前に必要な操作について説明しています。

ガイド	説明
『Cisco UCS Manager Administration Guide』	パスワード管理、ロールベースアクセスの設定、リモート認証、通信サービス、CIMC セッション管理、組織、バックアップと復元、スケジューリング オプション、BIOS トークン、および遅延展開について説明しています。
『Cisco UCS Manager Infrastructure Management Guide』	Cisco UCS Manager によって使用および管理される物理および仮想インフラストラクチャ コンポーネントについて説明しています。
『Cisco UCS Manager Firmware Management Guide』	ファームウェアのダウンロードと管理、自動インストールによるアップグレード、サービス プロファイルによるアップグレード、ファームウェアの自動同期によるエンドポイントでの直接アップグレード、機能カタログの管理、展開シナリオ、およびトラブルシューティングについて説明しています。
『Cisco UCS Manager Server Management Guide』	新しいライセンス、Cisco UCS Central への Cisco UCS ドメインの登録、電力制限、サーバのブート、サーバプロファイルおよびサーバ関連ポリシーについて説明しています。
『Cisco UCS Manager Storage Management Guide』	Cisco UCS Manager の SAN や VSAN など、ストレージ管理のあらゆる側面について説明しています。
『Cisco UCS Manager Network Management Guide』	Cisco UCS Manager の LAN や VLAN 接続など、ネットワーク管理のあらゆる側面について説明しています。
『Cisco UCS Manager System Monitoring Guide』	Cisco UCS Manager における、システム統計を含むシステムおよびヘルス モニタリングのあらゆる側面について説明しています。
Cisco UCS S3260 サーバと Cisco UCS Manager との統合	Cisco UCS Manager を使用して管理している UCS S シリーズ サーバの管理のあらゆる側面について説明しています。

# ファームウェア アップグレードをサポートするコンポーネント

Cisco UCS Manager でサポートされているさまざまなプラットフォームは、ファームウェア アップグレードをサポートするさまざまなコンポーネントを搭載しています。

- ファブリック インターコネクト :

- Cisco UCS 6332
- Cisco UCS 6332-16 UP
- Cisco UCS 6248 UP
- Cisco UCS 6296 UP
- Cisco UCS 6324

- シャーシ コンポーネント :

- ブレード サーバ シャーシ :

- I/O モジュール



---

(注) I/O モジュールは、プライマリ Cisco UCS Mini シャーシではサポートされません。ただし、セカンダリ Cisco UCS Mini シャーシでサポートされます。

---

- 電源装置

- Cisco UCS S3260 シャーシ :

- シャーシ管理コントローラ (CMC)
- シャーシアダプタ
- SAS エクспанダ
- ボードコントローラ

- サーバ コンポーネント :

- ブレードおよびラック サーバ :

- アダプタ
- Cisco Integrated Management Controller (CIMC)
- BIOS
- ストレージコントローラ



(注) ストレージコントローラは、Cisco UCS Mini ではサポートされるサーバコンポーネントではありません。

- ボードコントローラ
- Cisco UCS S3260 ストレージサーバノード
  - Cisco Integrated Management Controller (CIMC)
  - BIOS
  - ボードコントローラ
  - ストレージコントローラ

## ファームウェアバージョンの用語

使用されるファームウェアバージョンの用語は、次のようなエンドポイントのタイプによって異なります。

### CIMC、I/O モジュール、BIOS、CIMC、および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、BIOS、CIMC、およびシスコのアダプタには、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。

#### Running Version

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。

#### Startup Version

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。

### バックアップバージョン

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、または最近アクティブ化されたバージ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 インターコネクトおよび 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 インターコネクトのファームウェアとファブリック インターコネクト上の Cisco UCS Manager だけです。すべてのイメージがファブリック インターコネクトに保存されるため、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 インターコネクトイメージは、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 インターコネクトイメージは、ファブリック インターコネクト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。

## バージョンをまたがるファームウェアのサポート

Cisco UCS Manager の A バンドル ソフトウェア (Cisco UCS Manager、Cisco NX-OS、IOM、FEX ファームウェア) は、サーバ上で以前のリリースの B バンドルまたは C バンドル (ホストファームウェア (FW)、BIOS、Cisco IMC、アダプタ FW およびドライバ) と同時に使用できます。

次の表に、Cisco UCS 6200 および 6300 ファブリック インターコネクトでサポートされる A、B、および C バンドルの混在バージョンを示します。

表 1: Cisco UCS 6200 および 6300 ファブリック インターコネクトでサポートされる混在 Cisco UCS リリース

		インフラストラクチャのバージョン (A バンドル)			
ホスト FW のバージョン (B または C バンドル)	2.2(8)	3.1(1)	3.1(2)	3.1(3)	3.2(1)
2.2(8)	6200	6200	6200	6200	6200

		インフラストラクチャのバージョン (Aバンドル)			
3.1(1)	-	6200、6332、6332-16UP	6200、6332、6332-16UP	6200、6332、6332-16UP	6200、6332、6332-16UP
3.1(2)	-	6200、6332、6332-16UP	6200、6332、6332-16UP	6200、6332、6332-16UP	6200、6332、6332-16UP
3.1(3)	-	6200、6332、6332-16UP	6200、6332、6332-16UP	6200、6332、6332-16UP	6200、6332、6332-16UP
3.2(1)	—	—	—	—	6200、6332、6332-16UP

次の表に、Cisco UCS Mini ファブリック インターコネクでサポートされる A、B、および C の混在バンドルバージョンを示します。

表 2: Cisco UCS Mini ファブリック インターコネクでサポートされる混在 Cisco UCS リリース

		インフラストラクチャのバージョン (Aバンドル)			
ホスト FW のバージョン (B または C バンドル)		3.1(1)	3.1(2)	3.1(3)	3.2(1)
3.1(1)		6324	6324	6324	6324
3.1(2)		6324	6324	6324	6324
3.1(3)		6324	6324	6324	6324
3.2(1)		—	—	—	6324

次の表に、3.2 バンドルを備えたすべてのプラットフォームでサポートされる、B および C バンドルの混在バージョンを示します。

表 3: 3.2(1)A バンドルを備えたすべてのプラットフォームでサポートされる、B、C バンドルの混在バージョン

		インフラストラクチャのバージョン (Aバンドル)		
Host FW Versions (B, C Bundles)		3.2(1)		
		6200	6300	6324
		ucs-k9-bundle-infra32xxxxAbin	ucs-6300-k9-bundle-infra32xxxxAbin	ucs-mini-k9-bundle-infra32xxxxAbin

	インフラストラクチャのバージョン (Aバンドル)		
2.2(8) (B、Cバンドル)	Yes	—	—
3.1(1) (B、Cバンドル)	Yes	Yes	Yes
3.1(2) (B、Cバンドル)	Yes	Yes	Yes
3.1(3) (B、Cバンドル)	Yes	Yes	Yes
3.2(1) (B、Cバンドル)	Yes	Yes	Yes



**重要** バージョンをまたがるファームウェアを設定する場合は、サーバのエンドポイントのファームウェアのバージョンが Cisco UCS ドメイン の設定に対応するようにする必要があります。

## サーバパック

サーバパックを使用すると、完全なサーバアップグレードを必要とせずに、既存のインフラストラクチャで新しいサーバプラットフォーム<sup>1</sup>を動的にサポートすることができます。このサポートは、Cisco UCS Manager カタログイメージによって提供されます。このモデルにより、新しいサーバを有効化する新しい B シリーズ、または C シリーズ サーババンドルが既存のインフラストラクチャ A バンドルでサポートされます。

たとえば、リリース 3.1(1) より後のリリースの B または C サーババンドルは、リリース 3.1(1) のインフラストラクチャ A バンドルでサポートされます。ただし、リリース 3.1(1) 以降のリリースの B または C サーババンドルは、リリース 3.1(1) よりも前のすべてのリリースのインフラストラクチャ A バンドルでサポートされていません。

特定のリリースの『*Release Notes for Cisco UCS Manager*』には、そのリリースでのバージョンにまたがるファームウェアサポートの完全なマトリックスが記載されています。B または C サーババンドルに追加された新機能は、インフラストラクチャ A バンドルを該当するバージョンにアップグレードした後にのみ使用できるようになります。

現在以下のサーバがサーバパックをサポートしています。

<sup>1</sup> この機能は特定のサーバプラットフォームに適用されます。

- B シリーズ サーバ : UCS B200 M4、B260 M4、B420 M4、B460 M4、B200 M5
- C シリーズ サーバ : UCS C220 M4、C240 M4、C460 M4、C220 M5、C240 M5

既存のインフラストラクチャバンドルで周辺機器がサポートされていない場合、サーバパック機能によってサポートされません。この周辺機器をサポートするためには、インフラストラクチャバンドルをアップグレードする必要があります。たとえば、既存のインフラストラクチャバンドルでサポートされていない新しいアダプタを使用してサーバがインストールされている場合、これらのアダプタのサポートには、インフラストラクチャバンドルへのアップグレードが必要です。これらのアダプタは、サーバパック機能を通じてサポートすることはできません。

新しいカタログイメージはハードウェアおよびソフトウェアコンポーネントを中断せずに使用できるため、サーバパックを使用すれば、ドメイン全体でのファームウェアアップグレードの運用オーバーヘッドを負担せずに、新しいサーバプラットフォームをアクティブなUCSドメインにより柔軟に追加できるようになります。

## 軽量アップグレード

Cisco UCS Manager リリース 3.1(3) までは、特定のコンポーネントのみが変更された場合でも、ファームウェアをパッチリリースにアップグレードするには、ファームウェアバンドル全体をダウンロードしてアクティブ化する必要がありました。一部のコンポーネントに修正が加えられていなくても、すべてのコンポーネントのファームウェアバージョンが変更されていました。これにより、そのコンポーネントファームウェアの不要な更新がトリガーされていました。

システムへのセキュリティ更新もパッチによって提供され、ファブリックインターコネクとダウンタイムの再起動につながっていました。

Cisco UCS Manager リリース 3.1(3) では、軽量アップグレードが導入され、次のような方法でファームウェアアップグレードが向上しています。

- コンポーネントのファームウェアバージョンは、変更された場合にのみ更新されます。
- セキュリティ更新はサービスパックを通じて提供されます。リリース 3.1(3) では、軽量アップグレードはセキュリティ更新のみをサポートしています。
- サービスパック内では、更新は特定のコンポーネントにのみ適用される場合があります。これらのコンポーネントは、ファブリックインターコネクの再起動なしで時々アップグレードされることがあります。
- インフラストラクチャおよびサーバコンポーネントの更新は、共通のサービスパックバンドルを通じて提供されます。サーバコンポーネントについては、変更したファームウェアイメージのみがサービスパックバンドルの一部となります。これにより、従来の B シリーズおよび C シリーズのバンドルと比較して、サービスパックのバンドルが小さくなりました。

## サービスパック

サービスパックは、Cisco UCS Manager インフラストラクチャとサーバコンポーネントにセキュリティ更新を適用するパッチです。サービスパックは、基本リリースに固有のもので、基本リリースにサービスパックを適用することはできませんが、個別にサービスパックをインストールすることはできません。

サービスパックは、インフラストラクチャコンポーネントとサーバコンポーネント用の単一バンドルとして提供されます。インフラストラクチャおよびサーバの自動インストールを使用してサービスパックを適用することで、関連するインフラストラクチャコンポーネントおよびサーバコンポーネントをすべて更新できます。Cisco UCS Manager リリース 3.1(3) では、サービスパックのバンドルによって、インフラストラクチャコンポーネントに対してのみ中断不要な更新が提供されます。インフラストラクチャコンポーネントの中でも、ファブリックインターコネクットのサービスパックへの更新の場合、OpenSSL の修正などの特定のシナリオにおいては、ファブリックインターコネクットの再起動が必要になる可能性があります。サーバコンポーネントの更新が中断され、アプリケーションのダウンタイムが伴います。

サービスパックはメンテナンスリリース用に累積されます。最新のサービスパックには、特定のメンテナンスリリースの際にリリースされた以前のサービスパックからのすべての修正が含まれています。

以前に適用されたサービスパックは、Cisco UCS Manager GUI と Cisco UCS Manager CLI を介して削除または更新できます。その結果、コンポーネントのファームウェアバージョンは、基本のリリースバンドルに由来します。

サービスパックは、Cisco UCS Manager リリース 3.1(3) より前のメンテナンスリリースには適用されません。

## サービスパックのバージョン

サービスパックのバージョンには、次のガイドラインが適用されます。

- サービスパックは基本のバンドルにのみ適用できます。たとえば、サービスパック 3.1(3)SP2 は 3.1(3) リリースにのみ適用できます。3.1(4) リリースとは互換性がないため、適用できません。
- 個別のメンテナンスリリースのサービスパックのバージョンの番号付けに関連はありません。たとえば、サービスパック 3.1(3)SP2 と 3.1(4)SP2 は別個のもので関連はありません。
- 個別のサービスパックを使用して、メンテナンスリリースごとに同じ修正を適用できます。たとえば、3.1(3)SP2 および 3.1(4)SP3 で同じ修正を適用できます。
- サービスパックではこれまでの修正内容が累積されています。同じメンテナンスリリースであれば、どのパッチバージョンでも最新のサービスパックを適用できます。たとえば、3.1(3)SP3 には、3.1(3)SP2 および 3.1(3)SP1 に行われたすべての修正が含まれます。任意の 3.1(3) リリースに 3.1(3)SP3 を適用できます。

- メンテナンス リリースのサービス パックを、デフォルトのサービス パックのバージョンより下のバージョンにダウングレードすることはできません。
- サービス パックのアップグレードまたはダウングレードが失敗すると、そのメンテナンス リリースのデフォルトのサービス パックのバージョンが実行中のサービス パックのバージョンになります。次に例を示します。

基本バンドルのバージョン : 3.1(3b)

デフォルトのサービス パックのバージョン : 3.1(3)SP2 (デフォルト)

実行中のサービス パックのバージョン : 3.1(3)SP3

3.1(3)SP3 から 3.1(3)SP4 へのアップグレード中に、アップグレードが失敗すると、表示される実行中のサービス パックのバージョンは 3.1(3)SP2 (デフォルト) となります。

次の表に、サービス パックが適用されるさまざまな状況で表示されるリリースバージョンと実行バージョンを示します。

リリースバージョン	表示される実行バージョン
3.1(3a)	基本バンドルのバージョン : 3.1(3a) サービス パックのバージョン : 3.1(3)SP0 (デフォルト)
3.1(3)SP1	基本バンドルのバージョン : 3.1(3a) サービス パックのバージョン : 3.1(3)SP1
3.1(3)SP2	基本バンドルのバージョン : 3.1(3a) サービス パックのバージョン : 3.1(3)SP2
3.1(3b)	基本バンドルのバージョン : 3.1(3b) サービス パックのバージョン : 3.1(3)SP2 (デフォルト)
3.1(3)SP3	基本バンドルのバージョン : 3.1(3b) サービス パックのバージョン : 3.1(3)SP3

## サービス パックのロールバック

基本リリースに適用されたサービス パックをロールバックできます。次の項では、さまざまなロールバックシナリオ中にバンドルのバージョンおよびサービス パックのバージョンに加えられの変更について説明します。

## サービスパックの削除

バンドルのバージョン	サービスパックのバージョン
バンドルのバージョンは変更されません。	サービスパックは、バンドルに付属するデフォルトのバージョンです。

## 以前のメンテナンス リリースへのインフラストラクチャバンドルのダウングレード

バンドルのバージョン	サービスパックのバージョン
インフラストラクチャバンドルは、以前のメンテナンス リリースのバージョンに変更されません。	サービスパックは、以前のメンテナンスリリースでは有効ではないため、削除されます。

## 同じメンテナンスリリース内にあるが以前のサービスパックのバージョンであるインフラストラクチャバンドルのダウングレード

バンドルのバージョン	サービスパックのバージョン
インフラストラクチャバンドルは、メンテナンス リリースパッチのバージョンに変更されません。	自動インストール中に対応するサービスパックのバージョンが指定されていない場合、インフラストラクチャのアップグレードまたはダウングレード中にサービスパックが削除されます。

## サービスパックに関するガイドラインと制約事項

- FIの再起動が必要なサービスパックからFIの再起動が必要な別のサービスパックにアップグレードすると、FIは2回再起動されます。
- サーバ自動同期ポリシーは、サービスパックではサポートされていません。
- 下位のFIがリリース3.1(3)より前のリリースで実行されている場合、サービスパックの自動同期はサポートされません。

## FI クラスタ用のファームウェア自動同期

クラスタを構成するために、セカンダリファブリックインターコネクトを交換、またはスタンバイからHAへの変換として追加するには、インフラストラクチャバンドルのファームウェアのバージョンが一致する必要があります。管理者は現在、交換FIを適切なバージョンに手動でアップグレードまたはダウングレードしてからクラスタに接続しています。ファームウェア自動同期を使

用すると、交換 FI がスタンバイとして HA に追加されるときに、そのインフラストラクチャバンドルを存続 FI と同じバージョンに自動的にアップグレードまたはダウングレードできます。ソフトウェアパッケージは、FI に存在する UCS ソフトウェアまたはファームウェアです。

#### ソフトウェアおよびハードウェアの要件

存続 FI 上のソフトウェアパッケージは、Cisco UCS リリース 1.4 以降である必要があります。ファブリックインターコネクットのモデル番号も同様です。たとえば、ファームウェア自動同期は、HA 用に設定されている 62XX および 63XX FI モデルの組み合わせの場合はトリガーされません。

#### 実装

以前の実装では、ソフトウェアパッケージのバージョンに不一致が存在する場合、交換 FI を強制的にスタンダロンモードとして設定します。交換 FI は、通常のアップグレードまたはダウングレードプロセスで、存続 FI 上のソフトウェアパッケージと同じバージョンに手動でアップグレードまたはダウングレードされます。次に、交換 FI がクラスタに追加されます。これは、交換 FI のアップグレードまたはダウングレードは手動プロセスであるからです。

現在のオプションに加えて、交換 FI のソフトウェアパッケージを存続 FI と同期するためのオプションが追加されました。ユーザがファームウェアを自動同期する場合、存続 FI のソフトウェアパッケージが交換 FI にコピーされます。次に、交換 FI のソフトウェアパッケージがアクティブになり、交換 FI がクラスタに追加されます。Cisco UCSM データベースと設定の同期は、HA クラスタが正常に構成されると通常のプロセスによって発生します。

#### ファームウェア自動同期の利点

UCS クラスタ内の 1 つのファブリック インターコネクで障害が発生した場合、自動同期の機能により、交換 FI のソフトウェアパッケージのリビジョンが存続 FI と同じになります。このプロセスでは、エンドユーザは最小限の対話で、明確かつ簡潔なフィードバックを得ることができます。

## ファームウェアアップグレードのオプション

Cisco UCS ファームウェアは、次の複数の方式によってアップグレードできます。



- (注) 1 つ以上の Cisco UCS ドメインを以降のリリースにアップグレードするために必要な手順については、該当する [Cisco UCS アップグレードガイド](#) を参照してください。アップグレードガイドが提供されていない場合は、[Cisco Technical Assistance Center](#) にお問い合わせください。そのリリースからの直接アップグレードはサポートされていない場合があります。

#### Cisco UCS Manager による Cisco UCS ドメインのアップグレード

そのドメインの Cisco UCS Manager を使用して Cisco UCS ドメインをアップグレードする場合は、次のいずれかのアップグレードオプションを選択できます。

- 自動インストールによるインフラストラクチャとサーバのアップグレード：このオプションでは、自動インストールを使用してアップグレードの最初の段階ですべてのインフラストラクチャコンポーネントをアップグレードできます。次の段階で、ホストファームウェアパッケージを使用してすべてのサーバエンドポイントをアップグレードできます。
- サービス プロファイルのファームウェア パッケージを使用してサーバをアップグレード：このオプションを使用すると 1 回のステップですべてのサーバのエンドポイントをアップグレードできるため、サーバのリブートによる中断時間を短くすることができます。サービス プロファイルの更新の延期導入とこのオプションを組み合わせると、スケジュールされたメンテナンス ウィンドウ時にサーバのリブートが行われるようにすることができます。
- インフラストラクチャおよびサーバのエンドポイントの直接アップグレード：このオプションでは、ファブリック インターコネクタ、I/O モジュール、アダプタ、ボードコントローラなど、多数のインフラストラクチャとサーバのエンドポイントを直接アップグレードできます。ただし、直接アップグレードは、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、ローカル ディスクなど、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。そ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。
- シャーシ プロファイルのシャーシ ファームウェア パッケージを介したシャーシのアップグレード：このオプションにより、1 つの手順ですべての S3260 シャーシ エンドポイントをアップグレードできます。



(注) シャーシ プロファイルとシャーシ ファームウェア パッケージは、S3260 シャーシのみに適用されます。

### Cisco UCS Manager を通じた Cisco UCS ドメイン 内の S3X60 サーバ ノード のアップグレード

Cisco UCS Manager を通じて S3260 シャーシ とサーバを含む Cisco UCS ドメインを次のようにアップグレードできます。

- 自動インストールによるインフラストラクチャ コンポーネントのアップグレード：自動インストールを使用することで 1 つの手順で Cisco UCS Manager ソフトウェアおよびファブリック インターコネクタなどのインフラストラクチャ コンポーネントをアップグレードできます。
- シャーシ プロファイルのシャーシ ファームウェア パッケージを介したシャーシのアップグレード：このオプションにより、1 つの手順ですべてのシャーシ エンドポイントをアップグレードできます。

『Cisco UCS S3260 Server Integration with Cisco UCS Manager』には、シャーシ プロファイルとシャーシ ファームウェア パッケージに関する詳細情報が記載されています。

- サービス プロファイルのファームウェア パッケージを使用してサーバをアップグレード：このオプションを使用すると 1 回のステップですべてのサーバのエンドポイントをアップグレードできるため、サーバのリブートによる中断時間を短くすることができます。サービス

プロファイルの更新の延期導入とこのオプションを組み合わせると、スケジュールされたメンテナンス時間中にサーバのリブートが行われるようにすることができます。

また、各インフラストラクチャ、シャーシとサーバエンドポイントでファームウェアを直接アップグレードすることもできます。このオプションにより、ファブリック インターコネクタ、SAS エクスパンダ、CMC、シャーシアダプタ、ストレージコントローラ、ボードコントローラを含む、多くのインフラストラクチャ、シャーシ、サーバエンドポイントを直接アップグレードできます。ただし、直接アップグレードは、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、ローカル ディスクなど、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。

『Cisco UCS S3260 Server Integration with Cisco UCS Manager』には、S3X60 サーバノードのファームウェア管理についての詳細情報が記載されています。

### Cisco UCS Central による Cisco UCS ドメインのアップグレード

1 つ以上の Cisco UCS ドメインを Cisco UCS Central に登録している場合は、Cisco UCS Central を使用してそれらのドメイン内のすべてのファームウェアのコンポーネントを管理およびアップグレードできます。このオプションを使用すると、ファームウェアアップグレードの制御を集中化して、データセンターのすべての Cisco UCS ドメインを必要なレベルにすることができます。

Cisco UCS Central を使用すると、グローバルなファームウェア管理向けに設定されたすべての登録済み Cisco UCS ドメインの機能カタログ、インフラストラクチャ、およびサーバのエンドポイントをアップグレードできます。

## サービスパックの更新のオプション

次のいずれかの方法で Cisco UCS ファームウェアをサービスパックにアップグレードできます。

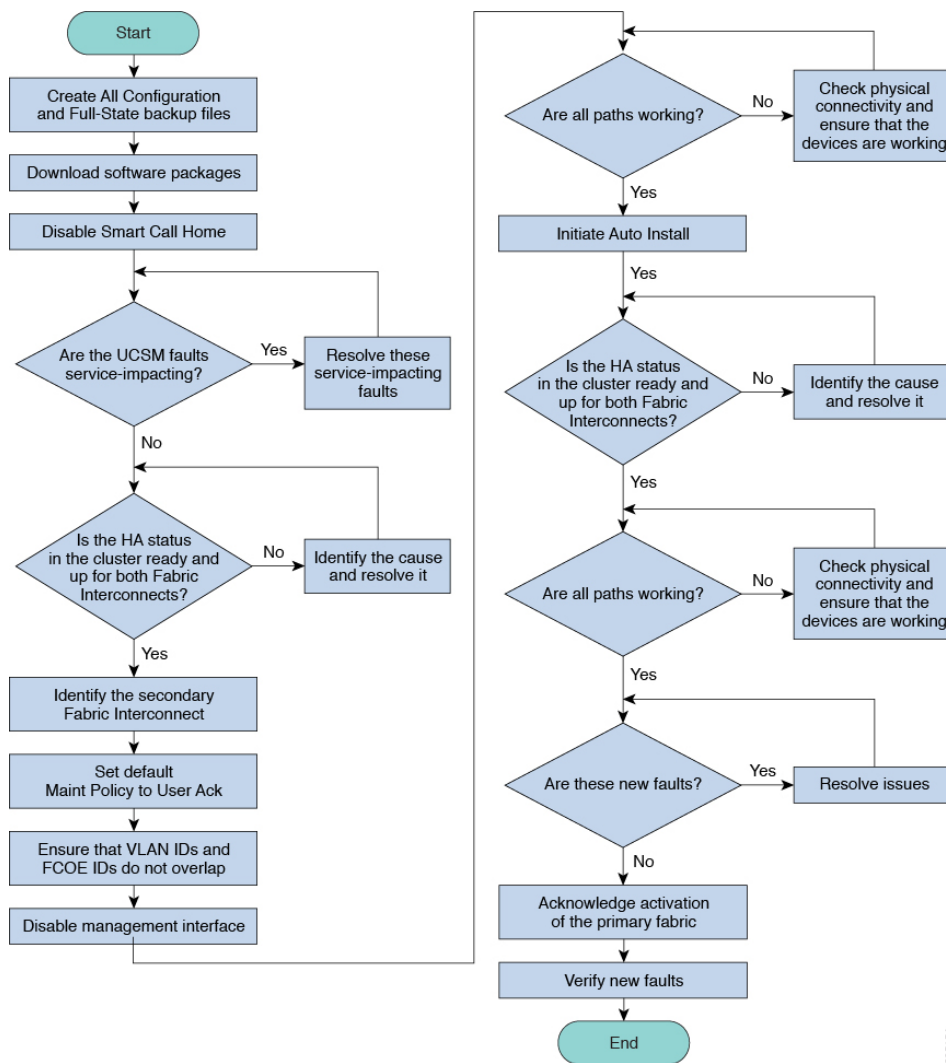
- インフラストラクチャの自動インストールを介してサービスパックにアップグレードする
- サーバの自動インストールを介してサービスパックにアップグレードする
- サービスプロファイルのファームウェアパッケージを介してサービスパックにアップグレードする
- シャーシプロファイルのシャーシファームウェアパッケージを介してサービスパックにアップグレードする
- 基本のメンテナンス リリースで Cisco UCS Manager サービスパックを直接アクティブにする
- 基本のメンテナンス リリースでファブリック インターコネクタのサービスパックを直接アクティブにする

## 自動インストールによるファームウェアアップグレード

自動インストールでは、次の 2 つの段階によって、Cisco UCS ドメインを 1 つのパッケージに含まれるファームウェアバージョンに自動的にアップグレードすることができます。

- インストールインフラストラクチャファームウェア：Cisco UCS インフラストラクチャソフトウェアバンドルを使用して、ファブリックインターコネクト、I/Oモジュール、Cisco UCS Manager などのインフラストラクチャコンポーネントをアップグレードすることができます。図4：インフラストラクチャファームウェアの自動インストールのプロセスフロー、（20ページ）に、インフラストラクチャファームウェアを自動的にインストールするための推奨プロセスフローを示します。

図4：インフラストラクチャファームウェアの自動インストールのプロセスフロー



- インストールサーバファームウェア：必要に応じて、Cisco UCS B シリーズブレードサーバソフトウェアバンドルを使用してCisco UCS ドメインのすべてのブレードサーバをアップグレードしたり、またCisco UCS C シリーズラックマウント UCS 管理対象サーバソフトウェアバンドルを使用してすべてのラックサーバをアップグレードすることができます。

この2つの段階は独立したものであり、異なる時刻に実行することや、実行されるようにスケジュールすることができます。

自動インストールを使用して、インフラストラクチャ コンポーネントを Cisco UCS のあるバージョンにアップグレードし、サーバコンポーネントを異なるバージョンにアップグレードすることができます。

シスコは、自動インストールを使用して Cisco UCS ドメイン をアップグレードすることを強く推奨します。

## サービス プロファイルのファームウェア パッケージによるファームウェアアップグレード

サーバファームウェアおよび BIOS のバージョンは、複数のサーバにわたって定期的に更新する必要があります。これを手動で行う場合は、連続的に行う必要があり、長いダウンタイムが必要となります。

更新テンプレートであるサービス プロファイル テンプレートの属性としてホスト ファームウェア ポリシーを定義することにより、ホスト ファームウェア パッケージを使用できます。サービス プロファイル テンプレートに加えたすべての変更は、そのインスタンス化されたサービス プロファイルに自動的に反映されます。その後、サービス プロファイルに関連付けられているサーバもファームウェア バージョンと同時にアップグレードされます。

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 インターコネクト、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。

## 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ブ化による、Cisco UCS ドメインのトラフィックの中断を最小限に留めることができます。

使用するターゲット シャーシに応じて、各種コンポーネントでファームウェアを直接アップグレードすることができます。

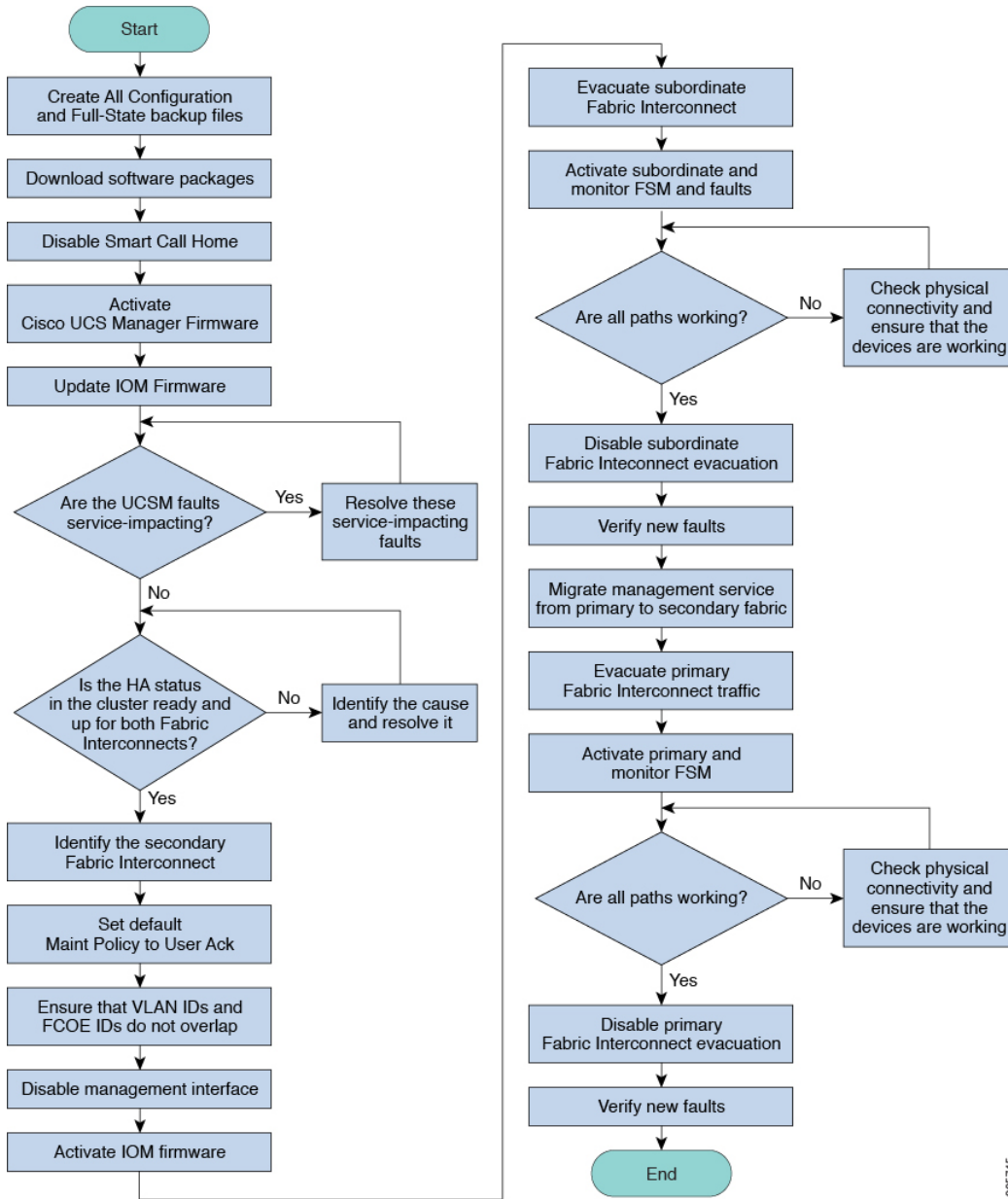
インフラストラクチャ	UCS 5108 シャーシ	UCS ラックサーバ	Cisco UCS S3260 シャーシ
<ul style="list-style-type: none"> <li>• ファブリックインターコネクト</li> <li>• Cisco UCS Manager</li> </ul>	<ul style="list-style-type: none"> <li>• I/O モジュール</li> <li>• 電源装置</li> <li>• サーバ：               <ul style="list-style-type: none"> <li>◦ アダプタ</li> <li>◦ CIMC</li> <li>◦ BIOS</li> <li>◦ ストレージコントローラ</li> <li>◦ ボードコントローラ</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• アダプタ</li> <li>• CIMC</li> <li>• BIOS</li> <li>• ストレージコントローラ</li> <li>• ボードコントローラ</li> </ul>	<ul style="list-style-type: none"> <li>• CMC</li> <li>• シャーシアダプタ</li> <li>• SAS エクスパンダ</li> <li>• シャーシボードコントローラ</li> <li>• サーバ：               <ul style="list-style-type: none"> <li>◦ CIMC</li> <li>◦ BIOS</li> <li>◦ ボードコントローラ</li> <li>◦ ストレージコントローラ</li> </ul> </li> </ul>



(注) サーバエンドポイント上でのファームウェアの直接アップグレードは、検出され、関連付けられていないサーバとシスコアダプタでのみ可能です。

図 5 : インフラストラクチャ ファームウェアの手動インストールのプロセス フロー, (23 ページ) は推奨されるプロセス フローを示しています。

図 5 : インフラストラクチャ ファームウェアの手動インストールのプロセス フロー



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) 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。

## Cisco UCS 6200 シリーズ ファブリック インターコネクタから Cisco UCS 6300 シリーズ ファブリック インターコネクタへの移行中のファームウェア アップグレード

移行中は次のガイドラインに従う必要があります。

- Cisco UCS 6200 シリーズ ファブリック インターコネクタは、Cisco UCS Manager リリース 3.1(1) 以降のリリースにアップグレードする必要があります。
- Cisco UCS 6300 シリーズ ファブリック インターコネクタには、アップグレード元の Cisco UCS 6200 シリーズ ファブリック インターコネクタと同じビルドバージョンをロードする必要があります。
- Cisco UCS 6200 シリーズ ファブリック インターコネクタと Cisco UCS 6300 シリーズ ファブリック インターコネクタ間でのみ移行できます。Cisco UCS 6248 UP と Cisco UCS 6296 UP ファブリック インターコネクタ間、または Cisco UCS 6332 と Cisco UCS 6332 16UP ファブリック インターコネクタ間では移行できません。
- すべてのファブリック インターコネクタには、同じバージョンのキックスタート、システム、および UCSM イメージが必要です。
- ファブリック インターコネクタのアップグレードは、新しい FEX または仮想インターフェイス カードにアップグレードする前に実行する必要があります。
- クラスタ設定の場合、両方のファブリック インターコネクタに、ファブリック インターコネクタと FEX 間の対称接続トポロジが必要です。
- スタンドアロンインストールでは、ダウンタイムを想定する必要があります。ファブリック インターコネクタのアップグレードでは、本質的にトラフィックの中断が発生します。
- ベストプラクティスは、このハードウェア アップグレードを実行する前に、設定およびソフトウェアのフルバックアップを実行することです。

# Cisco UCS Manager リリース 3.2 へのファームウェアアップグレード

## Cisco UCS Manager リリース 3.2 へのアップグレード条件

- Cisco UCS Manager リリース 3.2 にアップグレードする前に、既存のインフラストラクチャおよびサーババンドルのリリースバージョンが Cisco UCS Manager 2.2(x) 以降であることを確認してください。



### 重要

Cisco UCS Manager リリース 2.2(1a) より前のインフラストラクチャバンドルからのアップグレードはサポートされません。ただし、クラスタ内の FI を Cisco UCS Manager リリース 2.1(2) 以降のリリースで実行される FI に置き換えてから、自動同期機能を使用することで、この FI を直接 3.x(x) リリースにアップグレードできます。このようなシナリオでは、2.2(x) にまずアップグレードしてから 3.x(x) リリースにアップグレードする必要はありません。

- Cisco UCS Manager リリース 3.2 にアップグレードする前に、以下を実行して、使用中のキーリングが 2048 ビット以上のモジュラス サイズを備えているか確認してください。

- 1 次のコマンドを使用して、使用中のキーリングのモジュラス サイズを確認します。

```
UCS-A# scope security
UCS-A /security # scope keyring keyring-name
UCS-A /security/keyring # show detail
```

- 2 デフォルトのキーリングを使用しており、モジュラスサイズが 2048 ビット未満である場合は、モジュラスサイズを 2048 ビット以上に再構成し、次のコマンドを使って証明書を再生成します。

```
UCS-A# scope security
UCS-A /security # scope keyring default
UCS-A /security/keyring # set modulus mod2048
UCS-A /security/keyring # set regenerate yes
UCS-A /security/keyring # commit-buffer
UCS-A /security/keyring # show detail
```

- 3 デフォルトとは異なるキーリングを使用しており、モジュラスサイズが 2048 ビット未満である場合は、既存のキーリングを削除して、モジュラス値が 2048 以上の新たなキーリングを作成する必要があります。



(注) 使用中のキーリングは削除できません。使用中のキーリングを削除するには、まず別のキーリングを使用するよう HTTPS を設定する必要があります。

Cisco UCS Manager リリース 3.1 以降のリリースでは、モジュラスサイズが 2048 ビット未満であるキーリングをサポートしていません。

### Cisco UCS Manager リリース 3.2 へのアップグレードが失敗する条件

次のシナリオでは、以前のリリースから Cisco UCS Manager リリース 3.2 へのアップグレードが失敗し、Cisco UCS Manager は以前のバージョンにロールバックします。

- ファブリック インターコネクットのパーティションに十分な空き領域がない状態でのアップグレード
  - /var/sysmgr の空き容量が 20 % 未満
  - /mnt/pss の空き容量が 30 % 未満
  - /bootflash の空き容量が 20 % 未満
- 誤設定による Cisco UCS Manager の検証エラー

### アップグレード中の SNMP の自動的な無効化

以前のリリースから Cisco UCS Manager リリース 3.2 にアップグレードするときに、SNMP が自動的に無効になります（有効化されていた場合）。SNMP の状態は、両方のファブリック インターコネクットのアップグレードの完了後に復元されます。アップグレード中、SNMP が自動的に無効になると、すべての SNMP 操作が一時停止します。シスコでは、両方のファブリック インターコネクットのアップグレードが完了してから SNMP 操作を再開することを推奨します。



**重要** SNMP の状態は Cisco UCS Manager のアップグレード後に復元されますが、SNMP 操作は両方のファブリック インターコネクットのアップグレードの完了後にのみ実行できます。

## マイナーまたはパッチリリースへのファームウェアアップグレード

Cisco UCS Manager ソフトウェアのリリース番号は、メジャーリリース識別番号、マイナーリリース識別番号、およびパッチリリース識別番号で構成されます。マイナーリリース識別番号とパッチリリース識別番号は、カッコ内に列挙されます。たとえば、ソフトウェアバージョン番号が **3.2(2a)** の場合は、次の構成になります。

- **3.2** はメジャー リリース識別番号
- **2** はマイナー リリース識別番号
- **a** はパッチ リリース識別番号

つまり、これらは **3.2** リリース トレインの **first** のマイナー リリースの **a** パッチを示しています。メジャーリリース内でのメンテナンスリリースとパッチへのファームウェアアップグレードは、メジャーリリースと同じ方法で行います。

各メンテナンスリリースとパッチの内容の詳細については、最新版のリリースノートを参照してください。

## ファームウェアのダウングレード

Cisco UCS ドメインのファームウェアは、アップグレードと同じ方法でダウングレードできます。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。



(注) Cisco UCS Manager GUI では、リリースでサポートされていないオプションを選択できません。ダウングレードするリリースでサポートされていないハードウェアが Cisco UCS ドメインに含まれている場合は、Cisco UCS Manager GUI にそのハードウェアのオプションとしてそのファームウェアが表示されないか、ダウングレードできません。

### UCS M5 サーバがある Cisco UCS ドメイン

UCS M5 サーバがある Cisco UCS ドメインでは、Cisco UCS Manager リリース 3.2(1) からそれよりも前のリリースにダウングレードする場合は UCS M5 サーバの使用を中止する必要があります。これは、UCS M5 サーバが、Cisco UCS Manager リリース 3.2(1) 以降でのみサポートされているためです。

UCS M5 サーバの使用を停止せずに Cisco UCS Manager リリース 3.2(1) からそれよりも前のリリースにダウングレードすると、アップグレードの検証に失敗し、Cisco UCS Manager からダウングレード操作を続行する前にサーバを停止するよう求められます。

### ブレードサーバのボードコントローラ ファームウェア



#### 重要

- ボードコントローラ ファームウェアをダウングレードする必要はありません。

Cisco UCS B シリーズブレードサーバのボードコントローラ ファームウェアは、ダウングレードするように設計されていません。システム全体のファームウェアダウングレード操作を実行する際、「Error: Update failed: Server does not support board controller downgrade」というエラーメッセージが表示された場合は、このエラーメッセージを無視して、システムファームウェアのダウングレードを続行しても問題ありません。Cisco UCS Manager は、ボードコントローラ ファームウェアを自動的にスキップして、他のファームウェアコンポーネントのダウングレードを続行します。

- ブレードサーバのボードコントローラ ファームウェアバージョンが、インストール済みソフトウェアバンドルと同じか、または新しいバージョンである必要があります。ボードコントローラ ファームウェアのバージョンが、既存の Cisco UCS 環境で実行されているバージョンよりも新しい場合でも、ソフトウェアマトリックスまたは TAC のサポート範囲には違反しません。

### サポートされていない機能はダウングレードの前に設定解除が必要

Cisco UCS ドメイン を以前のリリースにダウングレードする場合は、まず、以前のリリースではサポートされていない機能を現在のバージョンからすべて設定解除して、機能しない設定をすべて修正する必要があります。サポートされていない機能の設定を解除せずに B または C のサーババンドルをダウングレードすると、その機能はダウングレードされたリリースで動作しない場合があります。たとえば、[On Next Reboot] メンテナンス ポリシーは、3.1 の B バンドルと C バンドルでサポートされます。任意のサーババンドルをダウングレードすると、このメンテナンスポリシー オプションは対応するサーバでは動作しません。

以前のリリースでサポートされていないすべての機能を設定解除せずにインフラストラクチャバンドルをダウングレードしようとする、ダウングレードに失敗する場合があります。

### SNMP をダウングレードの前に無効化

Cisco UCS Manager リリース 3.2 からそれよりも前のリリースにダウングレードする前に、SNMP を無効にする必要があります。ダウングレードプロセスは、SNMP が無効にされるまで開始されません。

### ファームウェアのダウングレードの推奨手順

ファームウェアを以前のリリースにダウングレードする必要がある場合は、次の順序で実行することを推奨します。

- 1 ダウングレード先のリリースから設定のバックアップを取得します。これは、現在のリリースにアップグレードしたときに作成したバックアップです。
- 2 ダウングレード先のリリースでサポートされていない機能を設定解除します。
- 3 Full State バックアップ ファイルと All Configuration バックアップ ファイルを作成します。
- 4 Cisco UCS Manager をダウングレードします。
- 5 erase-config を実行します。
- 6 ダウングレード先のリリースから設定のバックアップをインポートします。



(注) ステップ 5 および 6 は任意です。これらのステップは、既存の設定が使用不能になった場合のみ実行します。この場合、ステップ 1 またはステップ 3 からコンフィギュレーションバックアップをインポートします。

## Cisco UCS Central のファームウェア管理

Cisco UCS Central を使用すると、登録されているすべての Cisco UCS ドメインのすべてのファームウェア コンポーネントを管理することができます。



- (注) Cisco UCS Central から Cisco UCS ドメインのファームウェアを管理するには、Cisco UCS Manager でグローバルファームウェア管理オプションをイネーブルにする必要があります。グローバルファームウェア管理オプションは、Cisco UCS Manager を Cisco UCS Central に登録するときにイネーブルにできます。また、管理要件に基づいてグローバル管理オプションのオン/オフを切り替えることもできます。



**重要** Cisco UCS Central から Cisco UCS ドメインの登録を解除しないでください。

Cisco UCS ドメインは、Cisco UCS Central のドメイングループに管理目的で分類されます。ファームウェアは、ドメイングループレベルで各ドメイングループごとに別個に管理することも、ドメイングループのルートからドメイングループ全体に対して管理することもできます。Cisco UCS Central には、次の Cisco UCS ドメインのファームウェアパッケージを管理するオプションがあります。

- **機能カタログ**：ドメイングループごとに機能カタログを1つ使用します。特定のドメイングループに登録されたすべての Cisco UCS ドメインによって、ドメイングループで定義された機能カタログが使用されます。
- **インフラストラクチャファームウェア**：ドメイングループごとにインフラストラクチャファームウェアポリシーを1つ使用します。特定のドメイングループに登録されたすべての Cisco UCS ドメインによって、ドメイングループで定義された同じインフラストラクチャファームウェアバージョンが使用されます。
- **ホストファームウェア**：ドメイングループ内のさまざまなホストファームウェアコンポーネントに対して、複数のホストファームウェアポリシーを設定できます。ドメイングループに登録されている Cisco UCS ドメインでは、グループに定義されているホストファームウェアポリシーを選択できます。Cisco UCS Central には、ドメイングループのすべての Cisco UCS ドメインにホストファームウェアを同時にグローバルにアップグレードするオプションがあります。



- (注) Cisco UCS Central のファームウェア管理の詳細については、『*Cisco UCS Central Administration Guide*』および『*Cisco UCS Central CLI Reference Manual*』の「Firmware Management」の章を参照してください。

