



概要

この章は、次の内容で構成されています。

- [概要, on page 1](#)
- [このリリースの新規情報および変更情報 \(7 ページ\)](#)
- [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 \(7 ページ\)](#)
- [ファームウェア バージョンの用語, on page 9](#)
- [バージョンをまたがるファームウェアのサポート \(10 ページ\)](#)
- [サーババック \(10 ページ\)](#)
- [軽量アップグレード \(11 ページ\)](#)
- [FI クラスタ用のファームウェア自動同期 \(14 ページ\)](#)
- [ファームウェア アップグレードのオプション, on page 15](#)
- [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 6400 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 \(23 ページ\)](#)
- [Cisco UCS Manager リリース 4.2 へのファームウェア アップグレード \(26 ページ\)](#)
- [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 \(28 ページ\)](#)
- [ファームウェアのダウングレード, on page 29](#)
- [Cisco UCS Central のファームウェア管理 \(31 ページ\)](#)

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 4.1(1) では、Cisco UCS 64108 ファブリック インターコネクタから Cisco UCS 6400 シリーズ ファブリック インターコネクタを導入します。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にそれぞれユニファイド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 Bシリーズ、およびCシリーズサーバーとのCisco UCS 6400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シリーズサーバーとの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シリーズサーバーとのCisco UCS 6200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シリーズサーバーとのCisco UCS 6324ファブリックインターコネクト（別名UCS Mini）

Figure 1: Cisco UCS BシリーズおよびCシリーズサーバーとのCisco UCS 6400シリーズファブリックインターコネクト

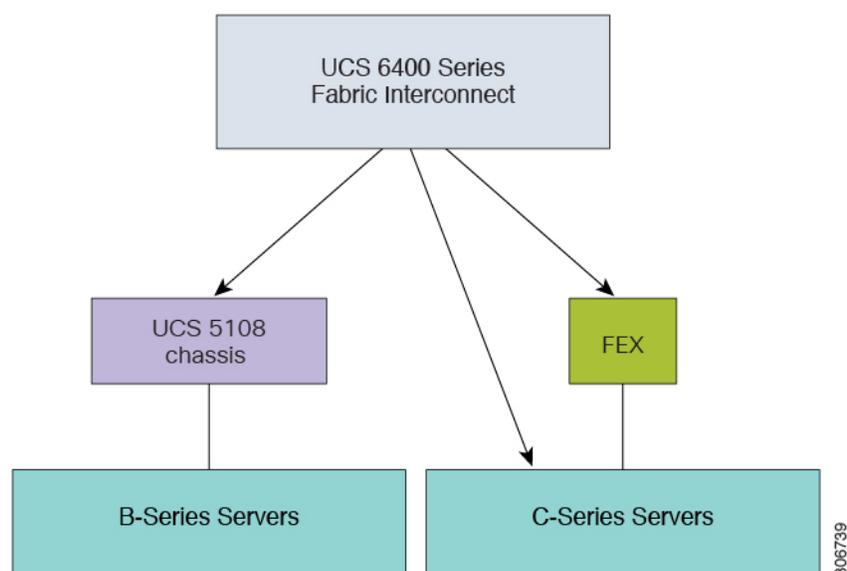


Figure 2: Cisco UCS B シリーズおよび C シリーズサーバーとの Cisco UCS 6300 シリーズ ファブリック インターコネクト

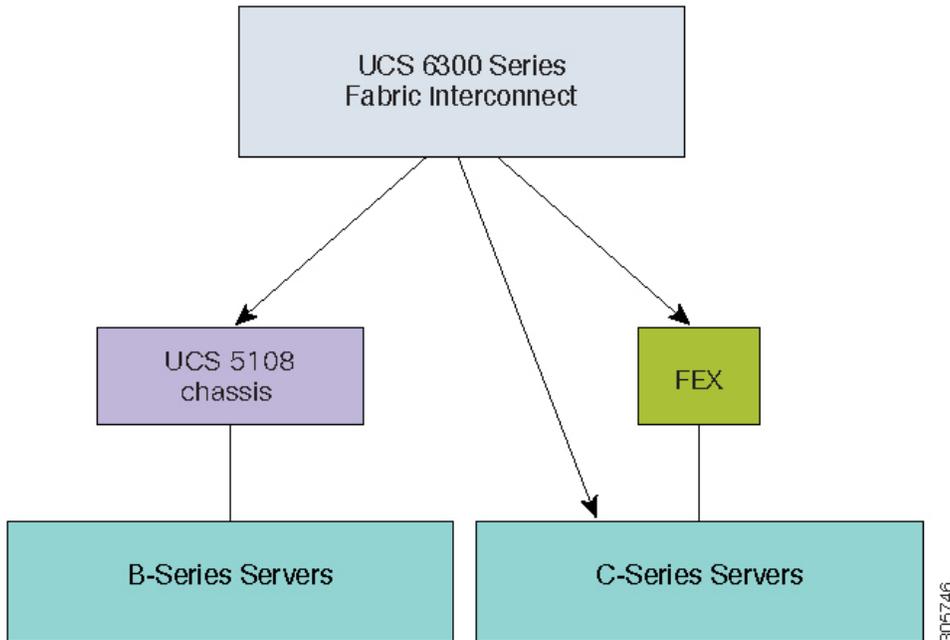


Figure 3: Cisco UCS B シリーズおよび C シリーズサーバーとの Cisco UCS 6200 シリーズ ファブリック インターコネクト

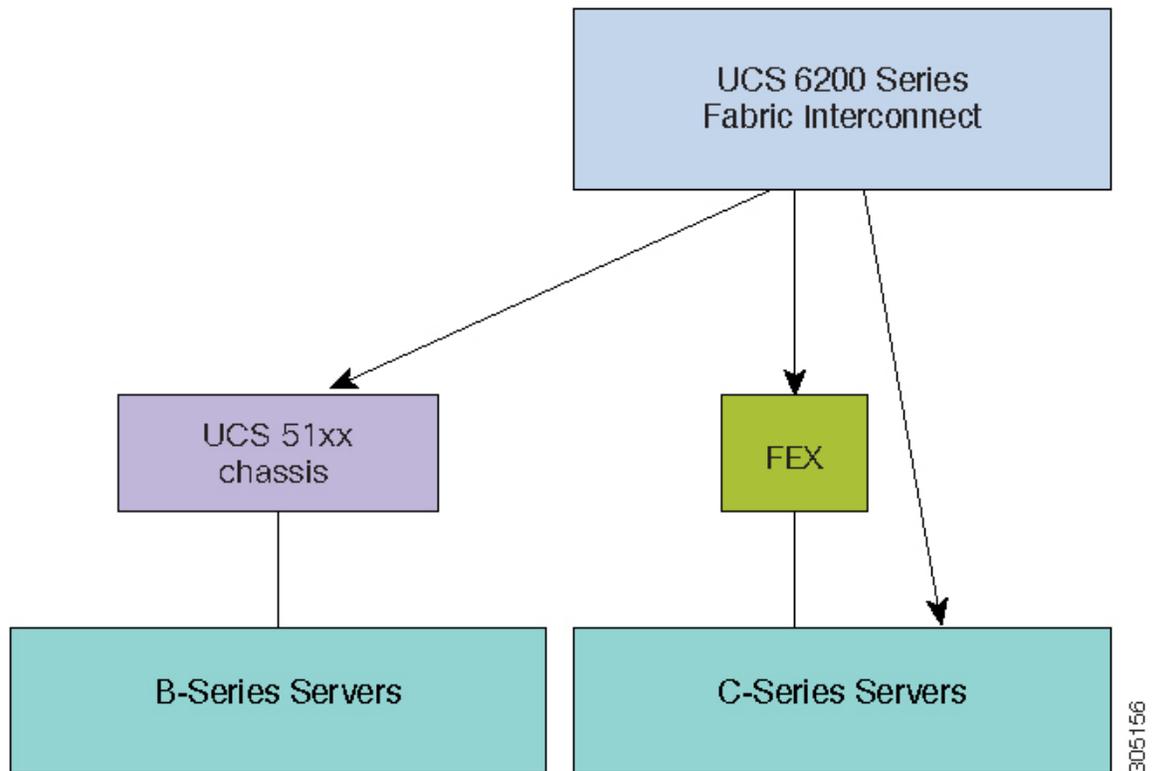
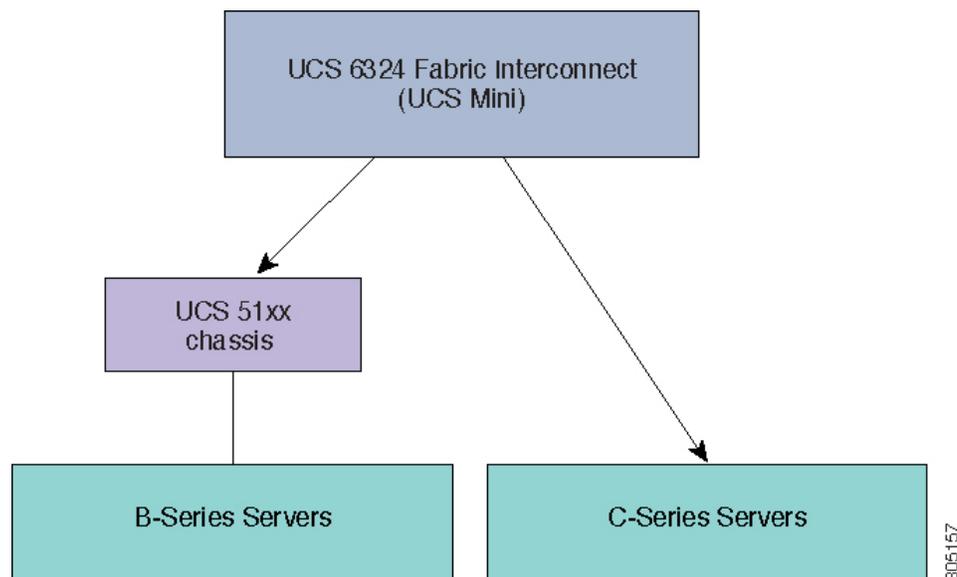


Figure 4: Cisco UCS B シリーズ サーバーおよび C シリーズ サーバーとの Cisco UCS 6324 ファブリック インターコネク



次の図に、Cisco UCS Manager リリース 4.1 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、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 4.1 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 6400 シリーズ ファブリック インターコネクト：
ucs-6400-k9-bundle-infra.4.x.x.xxx.A.bin
 - Cisco UCS 6300 シリーズ ファブリック インターコネクト：
ucs-6300-k9-bundle-infra.4.x.x.xxx.A.bin
 - Cisco UCS 6200 シリーズ ファブリック インターコネクト：
ucs-k9-bundle-infra.4.x.x.xxx.A.bin
 - Cisco UCS 6324 ファブリック インターコネクト：
ucs-mini-k9-bundle-infra.4.x.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。各 4.x リリースに対応する『*Release Bundle Contents for Cisco UCS Manager*』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。



Note 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 C3260 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。4.1 以降のリリースに対応する『*Release Bundle Contents for Cisco UCS Manager*』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。



Note 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 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 4.1 以降のリリースは、任意の 4.1 カタログファイルを使用できますが、4.0 または 3.2 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の順序は、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決定するアップグレードパスについては、ステップの決められた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。アクティブ化には、エンドポイントのリポートが必要な場合やリポートが発生する場合があります。



Note 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 ドキュメント

Cisco UCS Manager 次の表に記載する、細分化されたユースケース ベースの新しいドキュメントが用意されています。

ガイド	説明
Cisco UCS Manager クイック スタート ガイド	Cisco UCS のアーキテクチャと初回操作について説明しています。これには Cisco UCS Manager 初期構成と構成のベストプラクティスも含まれます。
Cisco UCS Manager アドミニストレーションガイド	パスワード管理、ロールベースのアクセス構成、リモート認証、通信サービス、CIMC セッションの管理、組織、バックアップと復元、スケジュール設定オプションに、BIOS トークン、遅延導入について説明しています。
Cisco UCS Manager インフラストラクチャ管理ガイド	Cisco UCS Manager で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』	自動インストールを使用したファームウェアのダウンロード、管理、アップグレード、サービスプロファイルを使用したファームウェアのアップグレード、ファームウェア自動同期を使用したエンドポイントでの直接ファームウェアアップグレード、機能カタログの管理、導入シナリオ、トラブルシューティングについて説明しています。

ガイド	説明
Cisco UCS Manager サーバ管理ガイド	新しいランセンス、Cisco UCS Central への Cisco UCS ドメインの登録、パワー キャッピング、サーバブート、サーバプロファイル、サーバ関連のポリシーについて説明しています。
Cisco UCS Manager ストレージ管理ガイド	Cisco UCS Manager での SUN、VSAN などのストレージ管理のすべての側面について説明しています。
Cisco UCS Manager ネットワーク管理ガイド	Cisco UCS Manager での LAN、VLAN などのネットワーク管理のすべての側面について説明しています。
Cisco UCS Manager システム モニタリング ガイド	Cisco UCS Manager でのシステム統計を含め、システムおよびヘルスマニタリングのすべての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 による UCS S シリーズサーバ管理のすべての側面について説明しています。

このリリースの新規情報および変更情報

ここでは、Cisco UCS Manager リリース 4.2 の新機能および変更された動作について説明します。

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 64108 ファブリック インターコネクト
 - Cisco UCS 6454
 - 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 C3260 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 エクスパンダ
 - 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 C3260 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。

実行されているバージョン

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。

スタートアップバージョン

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。

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、6300 および 6400 シリーズ 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。

次の表に、Cisco UCS Mini 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 の混在バンドルバージョンを示します。

次の表に、4.2(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 および C バンドルの混在バージョンを示します。



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¹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) 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) 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。

¹ 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 サーバー : UCS B200 M4、B260 M4、B420 M4、B460 M4、B200 M5、B480 M5、B200 M6
- C シリーズ サーバー : UCS C220 M4、C240 M4、C460 M4、C220 M5、C240 M5、C480 M5、C220 M6、C240 M6、C225 M6、および C245 M6

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、シャーシ、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、シャーシ、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る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す。	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す。	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(各サービスパックにつき1回)。
- 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を強制的にスタンドアロンモードとして構成します。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。ユーザー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メカニズム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ト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。



Note 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、シャーシ、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。その後、シャーシファームウェア パッケージを介してすべてのシャーシ コンポーネントをアップグレードし、ホストファームウェア パッケージを介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、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。
- 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。



Note 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 インターコネクト、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、およびホストファームウェアをアップグレードできます。

各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はできません。Cisco UCS Central では、グローバルサービスプロファイル内でホストファームウェアポリシーを使用して、ホストファームウェアコンポーネントをアップグレードする必要があります。

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
- シャーシ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

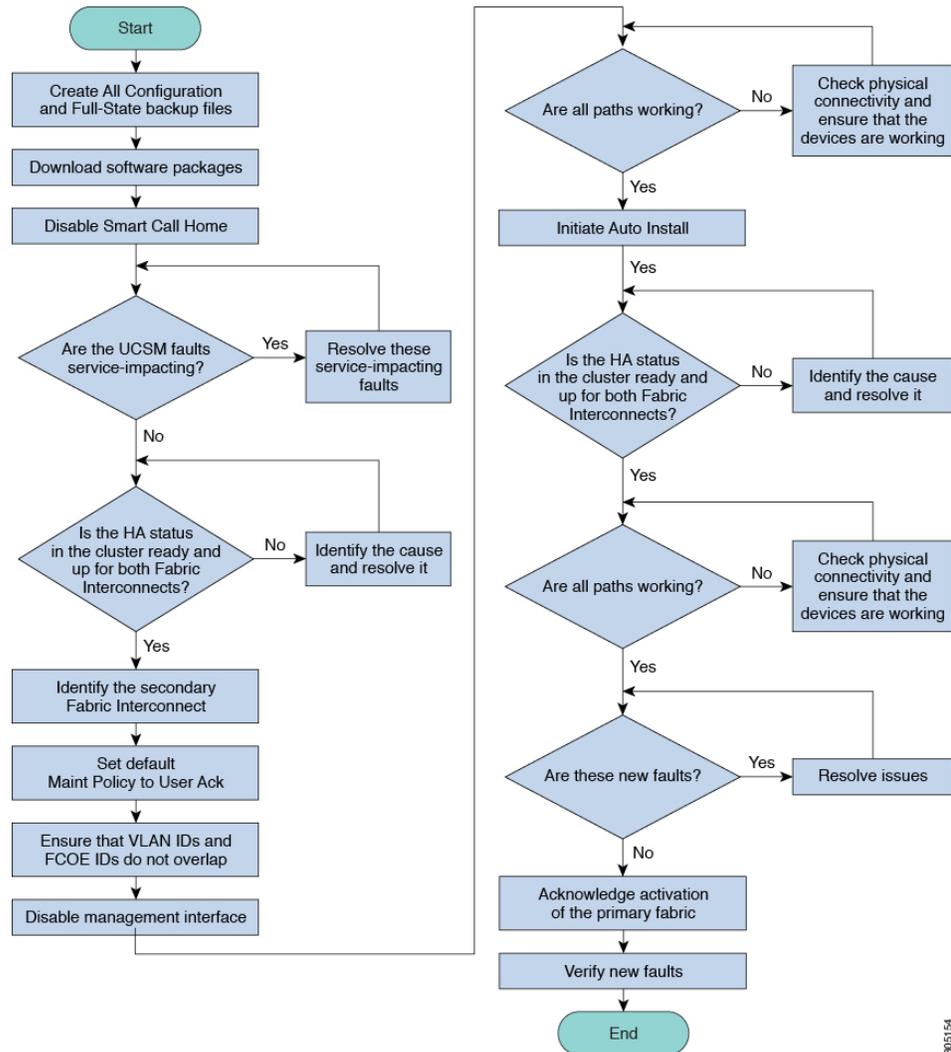
- 基本のメンテナンス リリースで Cisco UCS Manager サービス パックを直接アクティブにする
- 基本のメンテナンス リリースでファブリック インターコネクットのサービス パックを直接アクティブにする

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 インターコネクット、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 5: 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 \(19 ページ\)](#)、では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推奨されるプロセス フローを説明しています。

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



305154

- [Install Chassis Firmware]: 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シャーシコンポーネントをアップグレードします。
- 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 のバージョンにアップグレードし、シャーシと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、自動インストールと Fabric Evacuation 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。

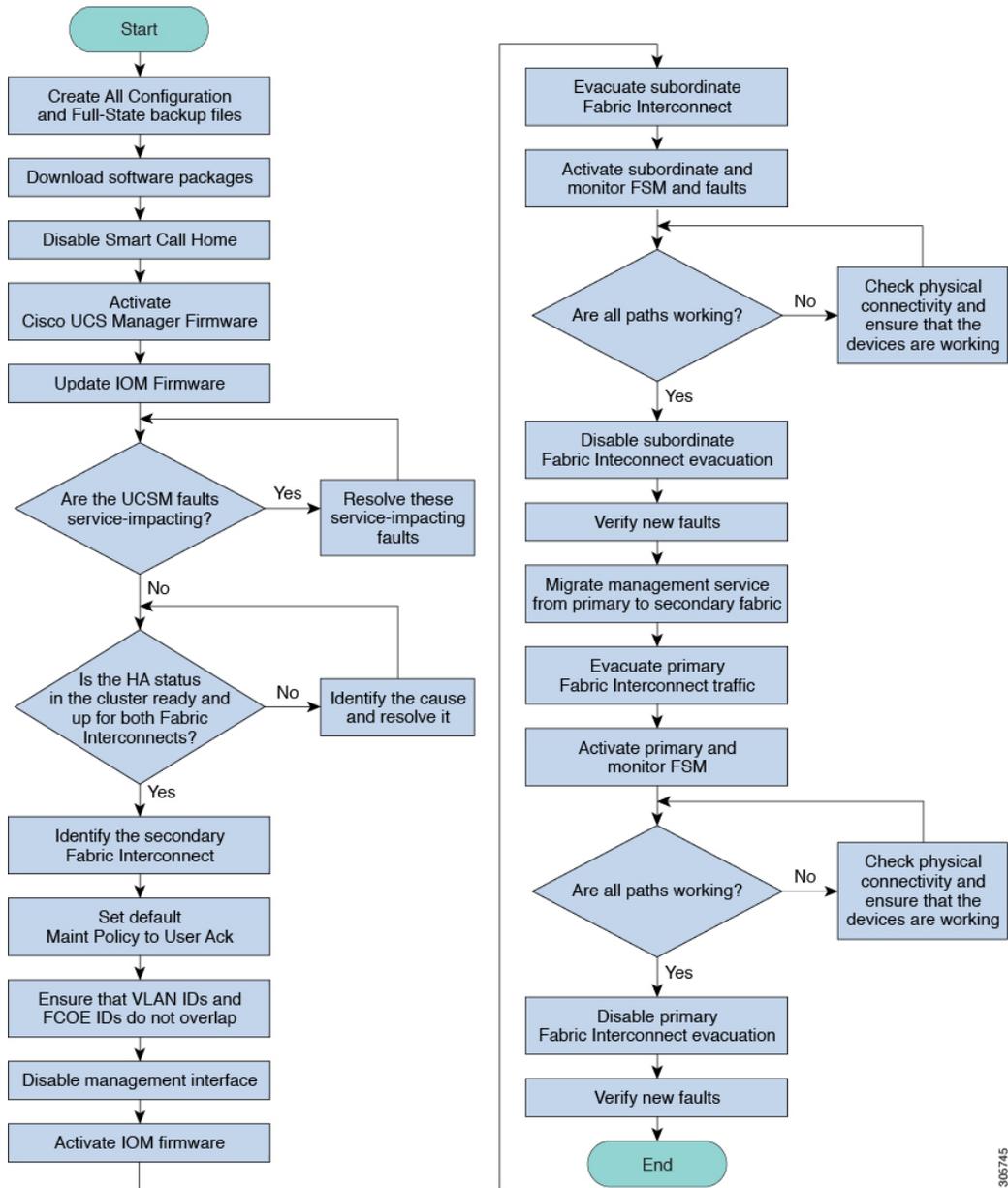
インフラストラクチャ	UCS 5108 シャーシ	UCS ラックサーバ	Cisco UCS C3260 シャーシ
<ul style="list-style-type: none"> • Cisco UCS Manager • ファブリック インターコネクト <p>必ず Cisco UCS Manager をアップグレードしてからファブリック インターコネクトをアップグレードしてください。</p>	<ul style="list-style-type: none"> • I/O モジュール • 電源装置 • サーバ： <ul style="list-style-type: none"> • アダプタ • CIMC • BIOS • ストレージコントローラ • ボードコントローラ 	<ul style="list-style-type: none"> • アダプタ • CIMC • BIOS • ストレージコントローラ • ボードコントローラ 	<ul style="list-style-type: none"> • CMC • シャーシアダプタ • SAS エクспанダ • シャーシボードコントローラ • サーバ： <ul style="list-style-type: none"> • CIMC • BIOS • ボードコントローラ • ストレージコントローラ



Note 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。

Figure 6: 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, on page 22は推奨されるプロセスフローを示しています。

Figure 6: 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



305745

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。



Note 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 6400 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 4.1(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 6400 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 インターコネクタから Cisco UCS 6400 ファブリック インターコネクタに移行できますが、Cisco UCS 6400 ファブリック インターコネクタから Cisco UCS 6200 シリーズ ファブリック インターコネクタには移行できません。次の間では移行できません。
 - Cisco UCS 6332 および Cisco UCS 6332 16UP ファブリック インターコネクタ
 - Cisco UCS 6332 および Cisco UCS 6454 ファブリック インターコネクタ
 - Cisco UCS 6332 および Cisco UCS 64108 ファブリック インターコネクタ
 - Cisco UCS 6332 16UP および Cisco UCS 6454 ファブリック インターコネクタ
 - Cisco UCS 6332 16UP および Cisco UCS 64108 ファブリック インターコネクタ
- 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。



(注) UCS 6400 シリーズ ファブリック インターコネクタには統一されたイメージがあります - キックスタート イメージとシステム イメージはもはや分離されていません。

- ファブリック インターコネク ト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 トに、ファブリック インターコネク トと 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 ト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 6400 シリーズ ファブリック インターコネク ト上のソフトウェア機能設定

Cisco UCS Manager リリース 4.0 (1) および 4.0 (2) では、Cisco UCS 6454 ファブリック インターコネク トのさまざまなソフトウェア機能のサポートが導入されました。Cisco UCS Manager リリース 4.1 では、Cisco UCS 64108 ファブリック インターコネク トでのこれらの機能のサポートが拡張されています。これらのソフトウェア機能は次のとおりです。

- スイッチング モード : Cisco UCS 6400 シリーズ ファブリック インターコネク トはイーサネットまたは FC スイッチング モードをサポートしていません。
- MAC セキュリティ : Cisco UCS 6400 シリーズ ファブリック インターコネク トで MAC セキュリティをサポートしていません。
- ブレークアウト アップリンク ポート : サポートされたブレークアウト ケーブルを使用して、1 つの QSFP ポートを 4 つの 10/25G ポートに分割をサポートします。これらのポートは、イーサネット アップリンクまたは FCoE アップリンク ポートの 10/25 G スイッチに接続するとしてのみ使用できます。これらは、サーバポート、FCoE ストレージポート、アプライアンス ポートまたはモニタリング ポートとして設定できません。
- MTU 設定 : Cisco UCS 64108 ファブリック インターコネク トは QOS ドロップ クラス ポリシーの mtu 設定をサポートします。

Cisco UCS 6400 シリーズ ファブリック インターコネク ト次のソフトウェア機能をサポートしません。

- 非ポート チャネル モードでのシャーシ ディスカバリ ポリシー : Cisco UCS 6400 シリーズ ファブリック インターコネク トはポート チャネル モードのみをサポートします。
- 非ポート チャネル モードでのシャーシ接続ポリシー : Cisco UCS 6400 シリーズ ファブリック インターコネク トはポート チャネル モードのみをサポートします。
- マルチキャスト ハードウェア ハッシュ : Cisco UCS 6400 シリーズ ファブリック インターコネク トはマルチキャスト ハードウェア ハッシュをサポートしていません。
- ダイナミック vNICS でのサービス プロファイル : Cisco UCS 6400 シリーズ ファブリック インターコネク トはダイナミック vNIC 接続ポリシーをサポートしていません。

- マルチキャスト最適化：Cisco UCS 6400 シリーズ ファブリック インターコネク トは QoS 用のマルチキャスト最適化をサポートしていません。
- NetFlow—Cisco UCS 6400 シリーズ ファブリック インターコネク トは Netflow に関連する構成をサポートしていません。
- ポート プロファイルと DVS 関連の設定：Cisco UCS 6400 シリーズ ファブリック インターコネク トはポート プロファイルおよび分散型仮想スイッチ（DVS）に関連する設定をサポートしていません。

Cisco UCS 6400 シリーズ ファブリック インターコネク トの次のソフトウェア機能の構成が変更されました。

- ユニファイドポート: Cisco UCS 6400 シリーズ ファブリック インターコネク トは、最大 16 つのユニファイドポートをサポートします。これらは FC として設定できます。これらのポートはモジュールの先頭にあります。
- VLAN の最適化: Cisco UCS 6400 シリーズ ファブリック インターコネク トでは、PV カウントが 16000 を超えるとポート VLAN (VP) グルーピングを利用して VLAN ポート カウント数の最適化を設定できます。次の表は、Cisco UCS 6400 シリーズ ファブリック インターコネク ト、Cisco UCS 6300 シリーズ ファブリック インターコネク ト、および Cisco UCS 6200 シリーズ ファブリック インターコネク トで有効および無効にされた VLAN ポート数の最適化による PV カウントを示しています。

	6200 シリーズ FI	6300 シリーズ FI	6400 シリーズ FI
VLAN ポート カウントの最適化が無効にされた PV カウント	32000	16000	16000
VLAN ポート カウントの最適化が有効にされた PV カウント	64000	64000	64000

Cisco UCS 6400 シリーズ ファブリック インターコネク トがイーサネット スイッチング モードのとき:

- Fabric Interconnect (FI) をサポートしません **VLAN ポート数の最適化有効**
- Fabric Interconnect (FI) 16000 PVs と同様に **VLAN ポート数最適化 Disabled** に設定すると、EHM モードをサポートしています
- VLAN の制限：Cisco UCS 6400 シリーズ ファブリック インターコネク トは、システムで利用するために 128 個の VLAN を予約します。

Cisco UCS Manager リリース 4.2 へのファームウェア アップグレード

Cisco UCS Manager リリース 4.2 へのファームウェア アップグレードのシナリオ

リリース 4.2(x) へのアップグレード:

- 4.2(2)A にアップグレードする場合は、4.1(3h)A 以降のリリースからアップグレードします。
- 4.1(3h) より前のパッチからアップグレードする場合は、リリース 4.1(3h)A バンドルにアップグレードしてアクティブ化します。



(注) リリース 4.1(3h)A をアクティブ化する前に、リリース 4.2(2)A バンドルをダウンロードしないでください。

リリース 4.2(2)A をダウンロードしてアップグレードします。

Cisco UCS Mini では、Cisco UCS Manager リリース 4.2 (x) へのインフラストラクチャ ソフトウェアバンドル (A バンドル) の直接アップグレードは、リリース 3.2(3) 以降のリリースからサポートされています。

『[Cisco UCS Manager Upgrade/Downgrade Support Matrix](#)』には、さまざまな Cisco UCS Manager リリースでサポートされているアップグレードリリースバージョンと推奨されるアップグレードパスがリストされています。



(注) リリースアップグレードを開始する前に、各バージョンの[ファームウェア管理ガイド](#)を参照して、制限事項とアップグレードを実行するための正しいパスを理解してください。



重要 [Cisco UCS B シリーズ M5 サーバーをリリース 4.2(2) にアップグレードする (Upgrade Cisco UCS B-Series M5 servers to Release 4.2(2))] : Cisco UCS B シリーズ M5 サーバを 4.0 (4m) またはそれ以前のリリースからアップグレードする場合は、2 段階のアップグレードを実行します。

1. まず、サーバーを 4.1 リリースバージョンにアップグレードします。シスコでは、最新の 4.1(3) パッチバージョンを推奨しています。
2. サーバーが 4.1 リリースバージョンで実行されたら、4.2(2) リリースにアップグレードします。

Cisco UCS Manager リリース 4.2 へのアップグレード条件

- Cisco UCS Manager リリース 4.2 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とサーババンドルが次の Cisco UCS Manager リリースのいずれかであることを確認してください。

- Cisco UCS Manager リリース 3.2(3) 以降のリリース

Cisco UCS Mini の場合、任意のリリース 3.2(x) または 4.0(x) リリースから、Cisco UCS Manager リリース 4.2 にアップグレードできます。

- Cisco UCS Manager リリース 4.2 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 3.2 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 4.2 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 4.2 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 4.2 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 **4.2(1d)** の場合は、次の構成になります。

- **4.2** はメジャー リリース識別番号
- **1** はマイナー リリース識別番号
- **d** はパッチ リリース識別番号

つまり、これらは **4.2** リリーストレインの **first** マイナー リリースの **d** 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。



Note 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。

Cisco UCS Manager リリース 4.2 からのダウングレード

Cisco UCS 64108 ファブリック インターコネクトを搭載したシステムでは、Cisco UCS Manager リリース 4.1 からダウングレードできません。

MD5 SNMPv3 ユーザ認証

リリースにダウングレードするとよりも前Cisco UCS Managerリリース 3.2(3)、SNMPv3 ユーザの md5 認証は配置されません。このようなユーザを展開するには、次のいずれかの操作を行います。

- **[Auth Type]** フィールドを **[SHA]** に変更します。
- ユーザを削除し、それを再作成します。

SNMPv3 ユーザの AES プライバシー プロトコル

Cisco UCS Manager リリース 3.2(3) 以降のリリースでは、AES 暗号化なしの SNMPv3 ユーザはサポートされていません。したがって、Cisco UCS Manager リリース 3.2(3) より前のリリースにダウングレードすると、AES 暗号化を使用していない SNMPv3 ユーザは配置されません。このようなユーザを展開するには、次のいずれかの操作を行います。

- **AES-128** 暗号化を有効にする
- ユーザを削除し、それを再作成します。

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



Important

- 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 は自動的にボードコントローラ ファームウェアをスキップし、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けます。

- 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。



Note 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できます。



- (注) Cisco UCS CentralからCisco UCS ドメイン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有効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 に登録するときに有効にできます。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 ドメインを登録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

での 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。

翻訳について

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