Cisco UCS のリリース 1.3 からリリース 2.1 へのアップグレード

Cisco UCS Release 2.1 へのファームウェア アップグレード 2

ファームウェア アップグレードに関する注意、ガイドライン、および制約事項 2

Cisco UCS リリース 2.1 ファームウェアのダウンロード 10

Cisco UCS Release 2.1 へのファームウェア アップグレード 15

改訂：**June 10, 2015,**

Cisco UCS Release 2.1 へのファームウェア アップグレード

Cisco UCS Release 2.1 へのファームウェア アップグレードは、スタンドアロン ファブリック インターコネクトとサーバのための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、次のデータ トラフィックの中断を想定しておく必要があります。

- クラスタ設定のファブリック インターコネクトについては、正しい手順に従うとデータ トラフィックの中断は最小になります。ファブリック インターコネクト間のフェールオーバーにより、ファブリック インターコネクトと 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 インターコネクトでは、サーバのリブートに必要な最大 1 分間と、ファブリック インターコネクトと I/O モジュールのリブートに必要な約 10 分間、データ トラフィックが中断されます。
- サーバについては、各サーバをアップグレードする場合は、サーバのリブートの間データが中断されます。

シスコでは、ファームウェアを管理および更新するための一連のベスト プラクティスを『Cisco UCS B-Series Firmware Management Guides』と次のテクニカル ノートで保持しています。『Unified Computing System Firmware Management Best Practices』

（注） Cisco UCS 6100 シリーズ ファブリック インターコネクトから、Cisco UCS 6200 シリーズ ファブリック インターコネクトへのアップグレード方法については、『Upgrading Cisco UCS B-Series Hardware』を参照してください。

ファームウェアアップグレードに関する注意、ガイドライン、および制約事項

Cisco UCS ドメインのエンドポイントのファームウェアをアップグレードする前に、次の注意、ガイドライン、および制約事項を考慮してください。

（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。Cisco UCS ドメインに、アップグレード後のリリースでサポートされていないハードウェアが含まれている場合、Cisco UCS Manager GUI では、そのハードウェアのオプションとしてファームウェアが表示されず、アップグレードできません。

設定の変更とアップグレードに影響を与える可能性がある設定

Cisco UCS ドメインの設定に応じて、アップグレード後に設定を変更するには、次の変更が必要な場合があります。障害などの問題を回避するには、必要な変更を行ってからアップグレードすることを推奨します。

Cisco UCS Release 2.1(2) 以降へのアップグレードがサービス プロファイル レベルで定義されているイニシエータ IQN に及ぼす影響

2 つの iSCSI vNIC があり、両方が同じイニシエータ IQN（Cisco UCS Release 2.0(1) でサポート）を使用している場合は、アップグレードすると、単一のサービス プロファイル レベルのイニシエータ IQN が作成され、iSCSI vNIC のイニシエータ IQN はリセットされて値を失います。

Cisco UCS Release 2.0(1) のサービス プロファイル全体において、iSCSI vNIC で同じイニシエータ IQN が使用されている場合は、アップグレードすると、サービス プロファイル レベルの重複したイニシエータ IQN が生成されます。 このような構成では、サービス プロファイル レベルで定義された重複イニシエータ IQN を持つ各 iSCSI vNIC に対してエラーが生成されます。 これらのエラーは、サービス プロファイル レベルの重複イニシエータ IQN を変更すると解消されます。 サービス プロファイル関連の操作（ホスト ファームウェア パッケージのアップデートなど）を実行する前に、これらのエラーを解消する必要があります。

デフォルトのメンテナンス ポリシーの設定を「ユーザ確認応答」にする

デフォルトのメンテナンス ポリシーは、ホスト メンテナンス ポリシーによるサーバ ファームウェアのアップグレードなど、大きな影響を及ぼす変更がサービス プロファイルに加えられた場合にただちにサーバがリブートするように設定されています。 サーバ トラフィックの予期せぬ中断を避けるため、デフォルトのメンテナンス ポリシーのリブート ポリシー設定をユーザ確認応答に変更することを推奨します。

デフォルトのメンテナンス ポリシーのリブート ポリシー設定をユーザ確認応答に変更すると、大きな影響を及ぼす変更のリストが保留中のアクティビティと共に一覧表示されます。 これにより、サーバのリブートを制御することができます。

FCoE VLAN ID とイーサネット VLAN ID のオーバーラップは Cisco UCS Release 2.0 以降では許可されない

⚠

注意 Cisco UCS 1.4 以前のリリースでは、イーサネット VLAN と FCoE VLAN で VLAN ID のオーバーラップが可能でした。 ただし、Cisco UCS Release 2.0 以降では、VLAN ID のオーバーラップは許可されません。 アップグレード中に Cisco UCS Manager で VLAN ID のオーバーラップが検出されると、重大なエラーが生成されます。 VLAN ID を再設定しない場合、Cisco UCS Manager によって重大なエラーが生成され、オーバーラップしている VLAN のイーサネット トラフィックがドロップされます。 このため、イーサネットと FCoE の VLAN ID がオーバーラップしていないことを確認してから、Cisco UCS Release 2.2 にアップグレードすることを推奨します。

アップリンク トランクの設定で VLAN ID 1 がネイティブ VLAN として定義および設定されている場合、イーサネット VLAN 1 ID を別の値に変更すると、ファブリック インターコネクトでネットワークの中断やフラッピングが生じ、その結果、HA イベントが発生して、大量のトラフィックが取り込まれ、サービスを一時的に使用できなくなります。

Cisco UCS 1.4 以前のリリースでは、VSAN の FCoE VLAN ID を明示的に設定しなかった場合、Cisco UCS Manager は、デフォルトの VSAN のデフォルト FCoE VLAN として VLAN 1 を割り当てました（デフォルトの VSAN ID 1 を使用）。 これらのリリースでは、VLAN 1 は、イーサネット トラフィックのデフォルト VLAN としても使用されました。 このため、FCoE VLAN および 1 つ以上のイーサネット VLAN のデフォルト VLAN ID を受け入れた場合は、VSAN の FCoE VLAN またはイーサネット VLAN の VLAN ID を再設定する必要があります。

Cisco UCS Release 2.2 の新規インストールでは、デフォルトの VLAN ID は次のようになります。

- デフォルトのイーサネット VLAN ID は 1 です。
- デフォルトの FCoE VLAN ID は 4048 です。

FCoE ストレージ ポートのネイティブ VLAN に VLAN ID 4048 が使用されていた Cisco UCS Release 1.4 からリリース 2.0 にアップグレードした後、デフォルトの VLAN ID は次のようになります。

- デフォルトのイーサネット VLAN ID は 1 です。
- 現在のデフォルトの FCoE VLAN ID が保持されます。 競合するイーサネット VLAN がある場合、Cisco UCS Manager によって重大なエラーが生成されます。 1 つの VLAN ID を、使用または予約されていない VLAN ID に変更する必要があります。

（注） Cisco UCS ドメインでデフォルト VLAN ID の 1 つが使用されているため VLAN のオーバーラップが発生している場合は、1 つ以上のデフォルト VLAN ID を、使用または予約されていない VLAN ID に変更します。 リリース 2.0 以降では ID が 3968 ～ 4047 の VLAN は予約されます。

予約済み範囲の ID を持つ VSAN は正常に動作しない

予約範囲の ID を持つ VSAN は、アップグレード後に正常に動作しません。 次を実行して、Cisco UCS Manager で設定されている VSAN が予約済み範囲に含まれないようにします。

- Cisco UCS ドメイン FC スイッチ モードを使用する予定の場合は、ID が 3040 ～ 4078 の範囲にある VSAN を設定しないでください。
- Cisco UCS ドメイン FC エンドホスト モードを使用する予定の場合は、ID が 3840 ～ 4079 の範囲にある VSAN を設定しないでください。

VSAN に予約済み範囲の ID がある場合は、その VSAN ID を、使用または予約されていない VSAN ID に変更します。

リリース 1.3 からのアップグレードにおける組織名の制限事項

Cisco UCS Manager Release 1.3 よりも前のリリースで、名前にスペースを含む組織を作成し、その後、Cisco UCS Manager をリリース 1.3.x にアップグレードすると、スペースがアンダースコアに自動的に置き換えられました。 ただし、その後、Cisco UCS Manager を 1.4.x 以降のリリースにアップグレードすると、スペースがアンダースコアに変換されず、スペースを含む以前の組織名が再表示されます。 名前にスペースを含む組織のすべてのオブジェクト（サービス プロファイル、ポリシー、テンプレートなど）は削除されます。

この問題を回避するには、1.3.x リリースから 1.4.x 以降のリリースにアップグレードする前に、次の操作を行います。

1. アンダースコアおよびスペースを削除することにより、名前にアンダースコアを含む組織の説明フィールドを変更し、その組織がデータベースで保持されるようにします。
2. アップグレードする前に、[All Configuration] オプションを使用してバックアップを作成します。 アップグレード後に問題が発生する場合は、バックアップ ファイルを使用して設定を復元します。 設定ファイルをインポートした後、すべてのブレードに VIF の状態を復元するように再認識させます。

vNIC フェールオーバーと NIC チーミングの両方がイネーブルになっている場合、アップグレード時にすべての接続が失われる可能性がある

ホスト オペレーティング システム レベルで、1 つ以上の vNIC で [Enable Failover] を設定し、同時に NIC チーミング/ボンディングを設定した場合は、ファームウェアのアップグレード時にすべての接続が失われる可能性があります。いずれかの方法を使用して可用性を設計します。両方は使用しないでください。

Cisco UCS ドメインの 1 つ以上の vNIC に対してフェールオーバーをイネーブルにしているかどうかを確認するには、サーバに関連付けられている各サービス プロファイル内で vNIC の設定を確認します。 詳細については、実行しているリリースの Cisco UCS Manager コンフィギュレーション ガイドを参照してください。

ファームウェア アップグレードに関するハードウェア関連の注意事項および制限事項

Cisco UCS ドメインのハードウェアはアップグレード方法に影響を与えることがあります。エンドポイントをアップグレードする前に、次の注意事項および制約事項を考慮してください。

サーバまたはシャーシのメンテナンスなし

⚠

注意 更新が完了するまで、エンドポイントがあるハードウェアを取り外したり、メンテナンス作業を実行しないでください。 ハードウェアが取り外されたり、その他のメンテナンス作業により使用できない場合、ファームウェアの更新は失敗します。 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場合があります。 バックアップ パーティションが破損しているエンドポイントではファームウェアを更新できません。

アップグレードの実施前や実施中に RAID 構成ハードディスクを交換しない

Cisco UCS インフラストラクチャやサーバ ファームウェアのアップグレードの実施前および実施中は、以下を順守してください。

- サーバのローカル ストレージ（ハード ディスクや SSD）の取り外し、挿入、交換を行わない。
- リビルド、アソシエーション、コピーバック、 BGI など、ストレージ操作が実行されていないことを確認する。

常にホスト ファームウェア パッケージを使用して Cisco UCS Gen-2 アダプタをアップグレードする

Cisco UCS Gen-2 アダプタは、エンドポイントで直接アップグレードすることはできません。 このようなアダプタのファームウェアは、ホスト ファームウェア パッケージを使用してアップグレードする必要があります。

Cisco UCS 82598KR-CI 10-Gigabit Ethernet Adapter はアップグレードできない

Intel ベースのアダプタ カードである Cisco UCS 82598KR-CI 10-Gigabit Ethernet Adapter（N20-AI0002）のファームウェアは、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。

（注） NX-OS の内部電源シーケンサ ファームウェアが Cisco UCS アップグレード プロセスの一部として更新された場合、ファブリック インターコネクトはローダ プロンプトを表示します。 続行するには、ファブリック インターコネクトをパワーサイクルします。

アップグレードのファームウェアおよびソフトウェアに関する注意事項および制約事項

エンドポイントをアップグレードする前に、次の注意事項および制約事項を考慮してください。

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 ドメインの設定によって、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。

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 リリースやパッチには依存関係があるため、ファームウェアの更新を正常に実行す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、当該のリリースやパッチに付属のリリース ノートを参照してください。

アダプタおよび I/O モジュールの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 [スタートアップバージョンのみを設定する] 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 [スタートアップバージョンのみを設定する] 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 状態のままになります。 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またはリセットして、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 [スタートアップバージョンのみを設定する] 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、[スタートアップバージョンのみを設定する] 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。 また、Cisco UCS Manager がファブリック インターコネクトと I/O モジュールの間の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した場合、Cisco UCS Manager は、ファブリック インターコネクトのファームウェアに一致するファームウェア バージョンを使用して I/O モジュールを自動的に更新し、ファームウェアをアクティブ化して、I/O モジュールを再度リブートします。

不要なアラートを回避するためのアップグレード前の Call Home のディセーブル化（任意）

Cisco UCS ドメインをアップグレードすると、Cisco UCS Manager によってコンポーネントが再起動され、アップグレード プロセスが完了します。 この再起動によって、サービスの中断およびコンポーネントの障害と同じイベントが発生し、Call Home アラートの送信がトリガーされます。 アップグレードの開始前に Call Home をディセーブルにしない場合は、アップグレードに関連したコンポーネントの再起動によって生成されるアラートを無視してください。

自動インストールによるアップグレードに関する注意、ガイドライン、および制約事項

自動インストールを使用して Cisco UCS ドメインのエンドポイントのファームウェアをアップグレードする前に、次の注意、ガイドライン、および制約事項を考慮してください。

（注） 次の注意事項は自動インストールに固有の事項であり、ファームウェア アップグレードに関する注意、ガイドライン、および制約事項, （2 ページ）の項目と併せて考慮する必要があります。

エンドポイントの状態

アップグレードを開始する前に、影響を受けるすべてのエンドポイントが次の状態であることが必要です。

- 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、両方が稼働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。
- アップグレードするすべてのエンドポイントについて、動作可能な状態にあることを確認します。
- アップグレードするすべてのサーバについて、すべてのサーバが検出され、検出が失敗しないことを確認します。いずれかのサーバエンドポイントをアップグレードできないと、サーバ ファームウェアのインストールの処理は失敗します。

デフォルトのホスト ファームウェア ポリシーに関する推奨事項

Cisco UCS Manager をアップグレードすると、「default」という名前の新しいホスト ファームウェア ポリシーが作成され、まだホスト ファームウェア ポリシーが含まれていないすべてのサービス プロファイルに割り当てられます。 デフォルトのホスト ファームウェア ポリシーは空白です。 いかなるコンポーネントのいかなるファームウェア エントリも含まれていません。 このデフォルトのポリシーは、ユーザの確認応答を受けてからサーバをリブートするのではなく、即時にリブートするように設定することもできます。

サーバ ファームウェアのアップグレード時に、Cisco UCS ドメインのブレード サーバやラック マウント サーバのファームウェアをデフォルトのホスト ファームウェア ポリシーに追加できます。 アップグレードを完了するには、すべてのサーバをリブートする必要があります。

デフォルトのホスト ファームウェア ポリシーが割り当てられている各サービス プロファイルは、そこに含まれているメンテナンス ポリシーに従って、関連付けられているサーバをリブートします。 メンテナンス ポリシーが即時リブートに設定されている場合は、[Install Server Firmware] ウィザードでの設定の完了後に、アップグレードをキャンセルしたり、サーバのリブートを阻止することはできません。 これらのサービス プロファイルに関連付けられているメンテナンス ポリシーを検証して、時限リブートまたはユーザ確認応答のいずれが設定されているかを確認することを推奨します。

（注） 2.1(2a) より前のリリースからアップグレードする場合は、CSCup57496 の影響を受ける可能性があります。 手動で CIMC をアップグレードしてサービス プロファイルを関連付けたら、管理ファームウェア パックを削除して CIMC のファームウェアをアクティブにします。 詳細については、https://tools.cisco.com/bugsearch/bug/CSCup57496を参照してください。

ファブリック インターコネクトの時刻、日付、およびタイム ゾーンを同一にする

クラスタ構成内のファブリック インターコネクトを確実に同期させるには、それらが同じ日付、時刻、タイム ゾーンに設定されていることを確認する必要があります。 両方のファブリック インターコネクトに NTP サーバと正しいタイム ゾーンを設定することを推奨します。 ファブリック インターコネクトの日付、時刻、タイム ゾーンが同期していないと、自動インストールでエラーが発生することがあります。

インフラストラクチャとサーバのファームウェアを同時にアップグレードすることは不可能

インフラストラクチャ ファームウェアをサーバ ファームウェアと同時にアップグレードすることはできません。 インフラストラクチャ ファームウェアを先にアップグレードし、次にサーバ ファームウェアをアップグレードすることを推奨します。 インフラストラクチャ ファームウェアのアップグレードが完了するまで、サーバ ファームウェアのアップグレードは開始しないでください。

必要な権限

自動インストールを使用してエンドポイントをアップグレードするには、次の権限が必要です。

権限	実行できるアップグレード作業
admin	• インフラストラクチャファームウェアのインストール の実行 • サーバ ファームウェアのインストール の実行 • ホスト ファームウェア パッケージの追加、削除、および変更
サービス プロファイルの計算（ls-compute）	サーバ ファームウェアのインストール の実行
サービス プロファイルのサーバ ポリシー（ls-server-policy）	ホスト ファームウェア パッケージの追加、削除、および変更
サービスプロファイルの設定ポリシー（ls-config-policy）	ホスト ファームウェア パッケージの追加、削除、および変更

サーバ ファームウェアのインストールに対するホスト ファームウェア パッケージと管理ファームウェア パッケージの影響

サーバ ファームウェアのインストールでは、ホスト 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するため、Cisco UCS ドメインのすべてのサーバを同じファームウェア バージョンにアップグレードする必要はありません。 ただし、関連するサービス プロファイルにサーバ ファームウェアのインストールを設定したときに選択したホスト ファームウェア パッケージが含まれるサーバは、すべて指定したソフトウェア バンドルのファームウェア バージョンにアップグレードされます。

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 パッケージだけでなく管理ファームウェア パッケージも含まれている場合は、サーバ ファームウェアのインストールでは、管理ファームウェア パッケージのファームウェア バージョンを使用して、サーバの CIMC をアップグレードします。 CIMC は、ホスト ファームウェア パッケージの CIMC の方が管理ファームウェア パッケージの CIMC より新しいバージョンの場合でも、ホスト ファームウェア パッケージのファームウェア バージョンにはアップグレードされません。 ホスト ファームウェア パッケージを使用してサーバの CIMC をアップグレードする場合は、関連付けられたサービス プロファイルから管理ファームウェア パッケージを削除する必要があります。

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ていないサーバに対してサーバ ファームウェアのインストールを使用した場合の影響

サーバに関連付けられたサービス 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ていない場合、このサーバのエンドポイントのアップグレードにサーバ ファームウェアのインストールを使用すると、サーバ ファームウェアのインストールではデフォルトのホスト 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します。 サーバ ファームウェアのインストールでは、デフォルトのホスト ファームウェア パッケージのみ更新できます。

サーバに関連付けられているサービス プロファイルが以前にサーバ ファームウェアのインストールのデフォルトのホスト ファームウェア パッケージによって更新されている場合、このサーバの CIMC またはアダプタをアップグレードするには、次のいずれかの方法を使用する必要があります。

- サーバ ファームウェアのインストールを使用してデフォルトのホスト ファームウェア パッケージを変更し、次にサーバ ファームウェアのインストールを使用してサーバをアップグレードする。
- 新しいホスト ファームウェア パッケージ ポリシーを作成し、これをサーバに関連付けられたサービス プロファイルに割り当て、そのホスト ファームウェア パッケージ ポリシーを使用してサーバをアップグレードする。
- サービス プロファイルをサービス プロファイルの関連付けから解除し、次にサーバのエンドポイントを直接アップグレードする。

新たに追加されたサーバのサーバ ファームウェアのアップグレード

サーバ ファームウェアのインストールを実行した後、Cisco UCS ドメインにサーバを追加すると、新しいサーバのファームウェアはサーバ ファームウェアのインストールによって自動的にアップグレードされません。 新しく追加したサーバのファームウェアを、最後にサーバ ファームウェアのインストールを実行したときに使用したファームウェア バージョンにアップグレードする場合は、エンドポイントを手動でアップグレードしてそのサーバ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。 サーバ ファームウェアのインストールには、ファームウェア バージョンの変更が毎回必要です。 サーバを同じファームウェア バージョンにアップグレードするためにサーバ ファームウェアのインストールを再実行することはできません。

（注） リリース 2.2 へのアップグレードが終了すると、Cisco UCS Manager で [Firmware Auto Sync Server] ポリシーを使用して、新たに検出されたサーバを自動的に更新できます。 詳細については、該当する『*Cisco UCS B* シリーズ ファームウェア管理ガイド』を参照してください。

Cisco UCS リリース 2.1 ファームウェアのダウンロード

このセクションには、Cisco UCS リリース 2.1 ファームウェアを入手してファブリック インターコネクトへダウンロードする方法に関する情報が記載されています。

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

Cisco UCS ドメイン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。

[機器] 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 [インストールされたファームウェア] 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 ドメイン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。

- リリース ノートの内容を確認します。
- 適切なハードウェアおよびソフトウェア相互運用性の表を参照し、すべてのサーバのオペレーティング システム ドライバのレベルが、アップグレード予定の Cisco UCS のリリースに対して正しいレベルになっていることを確認します。
- 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、両方が稼働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 [全体のステータス] が [操作可能] であることを確認します。
- データ パスが稼働中であることを確認します。 詳細については、『Firmware Management Guide』の「Verifying that the Data Path is Ready」の項を参照してください。
- 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。
- Cisco UCS ドメインに致命的または重大な障害がないことを確認します。 このような障害がある場合は解決してから、システムをアップグレードしてください。 致命的または重大な障害があると、アップグレードが失敗する可能性があります。
- すべてのサーバが検出されていることを確認します。 サーバの電源を入れる必要はありません。また、サーバをサービス プロファイルと関連付ける必要もありません。
- ラックマウント サーバを Cisco UCS ドメインに統合する場合、Cisco UCS Manager で管理するシステムにラックマウント サーバをインストールし、統合する方法については、該当する C シリーズ ラックマウント サーバのインストール ガイドの指示に従います。

シスコからのソフトウェア バンドルの入手

はじめる前に

Cisco UCS ドメインをアップデートするために、次のどのソフトウェア バンドルが必要なのかを判定します。

- Cisco UCS インフラストラクチャ ソフトウェア バンドル：すべての Cisco UCS ドメインで必要です。
- Cisco UCS B シリーズ ブレード サーバ ソフトウェア バンドル：ブレード サーバが含まれるすべての Cisco UCS ドメインで必要です。
- 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：統合されたラックマウント サーバが含まれる Cisco UCS ドメインのみで必要です。 このバンドルには、Cisco UCS Manager がそれらのサーバ

を管理できるようにするためのファームウェアが含まれており、スタンドアロン C シリーズ ラックマウント サーバには適用されません。

手順

ステップ 1 Web ブラウザで、 Cisco.com を参照します。

ステップ 2 [Support] で [All Downloads] をクリックします。

ステップ 3 中央のペインで、[Servers - Unified Computing] をクリックします。

ステップ 4 入力を求められたら、Cisco.com の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 右側のペインで、次のように必要なソフトウェア バンドルのリンクをクリックします。

Bundle	ナビゲーション パス
Cisco UCS インフラストラクチャ ソフトウェア バンドル	[Cisco UCS Infrastructure and UCS Manager Software] > [Unified Computing System (UCS) Infrastructure Software Bundle] をクリックします。
Cisco UCS B シリーズ ブレード サーバ ソフトウェア バンドル	[Cisco UCS B-Series Blade Server Software] > [Unified Computing System (UCS) Server Software Bundle] をクリックします。
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	[Cisco UCS C-Series Rack-Mount UCS-Managed Server Software] > [Unified Computing System (UCS) Server Software Bundle] をクリックします。

ヒント これらのパスからアクセスできる Unified Computing System (UCS) Documentation Roadmap Bundle は、Cisco UCS のすべてのドキュメントのダウンロード可能な ISO イメージです。

ステップ 6 ソフトウェア バンドルをダウンロードする最初のページで、[Release Notes] リンクをクリックしてリリース ノートの最新版をダウンロードします。

ステップ 7 ダウンロードする各ソフトウェア バンドルについて、次の手順を実行します。

a) 最新リリース 2.2 ソフトウェア バンドルのリンクをクリックします。
リリース番号の後には、数字と文字が括弧内に続きます。 数字はメンテナンス リリース レベルを表し、文字はそのメンテナンス リリースのパッチを区別します。 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、最新版のリース ノートを参照してください。

b) 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]：ソフトウェア バンドル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ソフトウェア バンドルをカートに追加します。

c) メッセージに従ってソフトウェア バンドルのダウンロードを完了します。

ステップ 8 Cisco UCS ドメインをアップグレードする前に、リリース ノートを参照してください。

次の作業

ソフトウェア バンドルをファブリック 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 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 バンドルのイメージ ファイルは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 は、両方のファブリック インターコネクトにあるすべてのファームウェア パッケージとイメージを同期状態にします。 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。

はじめる前に

必要なファームウェア バンドルをシスコから入手します。

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
[プロトコル] フィールド	リモート サーバとの通信時に使用するプロトコル。 次のいずれかになります。 • [FTP] • [TFTP] • [SCP] • [SFTP] （注） TFTP ではファイル サイズが 32 MB に制限されます。 ファームウェア バンドルはそれよりも大幅にサイズが大きい可能性があるため、ファームウェアのダウンロードに TFTP を選択しないことを推奨します。

名前	説明
[Server] フィールド	ファイルがリモート サーバのファイルである場合は、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。 ファイルがローカル ソースのファイルである場合、このフィールドには「local」が表示されます。 （注） IPv4 または IPv6 アドレスではなくホスト名を使用する場合、で DNS サーバを設定する必要があります。 Cisco UCS ドメインが Cisco UCS Central に登録されていないか、DNS 管理が [ローカル] に設定されている場合は、Cisco UCS Manager で DNS サーバを設定します。 Cisco UCS ドメイン Cisco UCS Central に登録されていないか、DNS 管理が [グローバル] に設定されている場合は、Cisco UCS Central で DNS サーバを設定します。
[Filename] フィールド	ファームウェア ファイルの名前。
[Path] フィールド	リモート サーバ上のファイルへの絶対パス。 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 フォルダにあれば、リモート パスを指定する必要はありません。 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。
[ユーザ] 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。 このフィールドは、プロトコルが TFTP の場合は適用されません。
[パスワード] フィールド	リモート サーバのユーザ名のパスワード。 このフィールドは、プロトコルが TFTP の場合は適用されません。

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 （任意） [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。

次の作業

ファームウェア バンドルのイメージ ファイルが完全にダウンロードされたら、エンドポイント上でファームウェアを更新します。

Cisco UCS Release 2.1 へのファームウェア アップグレード

ここでは、Cisco UCS ドメインを Cisco UCS Release 2.1 にアップグレードするために従う必要がある手順に関する情報が含まれます。

Cisco UCS Release 2.1 へのファームウェア アップグレードのオプション

Cisco UCS Release 2.1 では、Cisco UCS ドメインでファームウェアをアップグレードするための次のオプションがあります。

- 自動インストールでのアップグレード：このアップグレード パスでは、Cisco UCS ドメインのファームウェアのアップグレード前のレベルが、そのリリースで最新のファームウェア バージョンである必要があります。 このアップグレード オプションを使用するには、Cisco UCS Manager を Cisco UCS Release 2.1 の最新バージョンにアップグレードし、自動インストールを使用して残り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必要があります。 このオプションは、すべてのサーバエンドポイントをアップグレードするために、ホスト ファームウェア パッケージを使用します。
- 手動アップグレード：このアップグレード パスでは、アップグレード前のファームウェア レベルがそのリリースの特定のレベルである必要はありません。 アダプタなどの一部のサーバ エンドポイントを、手動でアップグレードすることを選択できます。

自動インストールを部分的に利用したリリース 1.3 からのアップグレード手順の概要

（注） 次の一連の手順では、ホスト ファームウェア パッケージをすべてのサーバのサービス プロファイルに含めていると仮定します。 適切な手順の詳細については、Cisco UCS B シリーズのファームウェアの管理ガイドを参照してください。

手順の順序は、データ トラフィックの中断を最小限に抑えるように設計されています。 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。

1. 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, （10 ページ） で説明されているすべての前提条件の手順を実行します。
2. Cisco.com から Cisco UCS インフラストラクチャ ソフトウェア バンドル のファームウェア イメージを入手して、それをファブリック インターコネクトにダウンロードします。インフラストラクチャのアップグレードを完了するには、このファームウェア イメージをステップ 5 でもう 1 回ダウンロードする必要があります。 この余分なダウンロードは、Cisco UCS リリース 1.3 が別のサーバとインフラストラクチャ バンドルをサポートしないために必要です。
3. （オプション）Call Home の無効化：Cisco UCS ドメインに Call Home または Smart Call Home が含まれている場合は、Call Home を無効にして、Cisco UCS Manager がコンポーネントを再起動するときに不要なアラートを受信しないようにします。 詳細については、「Call Home の無効化」を参照してください。
4. Cisco UCS Managerのアクティブ化：この手順を実行するときに [Skip Validation] を選択します。 詳細については、「Cisco UCS Manager ソフトウェアのアクティブ化」を参照してください。

5 次のファームウェア イメージを Cisco.com から入手し、それらをファブリック インターコネクトにダウンロードします。 詳細については、Cisco UCS リリース 2.1 ファームウェアのダウンロード, （10 ページ）を参照してください。

- Cisco UCS インフラストラクチャ ソフトウェア バンドル：すべての Cisco UCS ドメインで必要です。
- Cisco UCS B シリーズ ブレード サーバ ソフトウェア バンドル：ブレード サーバが含まれるすべての Cisco UCS ドメインで必要です。
- 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：統合されたラックマウント サーバが含まれる Cisco UCS ドメインのみで必要です。 このバンドルには、Cisco UCS Manager がそれらのサーバを管理できるようにするためのファームウェアが含まれており、スタンドアロン C シリーズ ラックマウント サーバには適用されません。

6 インフラストラクチャ ファームウェアのアップグレード：Cisco UCS Manager で、[機器] > [ファームウェアの管理] >[ファームウェアの自動インストール] を選択し、[インフラストラクチャ ファームウェアのインストール] をクリックして、フィールドに値を入力し、インフラストラクチャをアップグレードします。 詳細については、「自動インストールを使用したインフラストラクチャ ファームウェアのアップグレード」を参照してください。

7 データ パスが復元されたことを確認します。 詳細については、「データ パスの準備完了の確認」を参照してください。

⚠

注意 アップグレード時の中断を最小限に抑えるには、次のことを確認する必要があります。

- ファブリック インターコネクトとサービス プロファイルの両方がフェールオーバー用に設定されていることを確認します。
- プライマリ ファブリック インターコネクトのリブートを承認する前に、セカンダリ ファブリック インターコネクトからデータ パスが正常に復元されていることを確認します。

8 [保留中のアクティビティ] ダイアログボックスの [ユーザ承認アクティビティ] タブで、プライマリ ファブリック インターコネクトのリブートを承認します。 [保留中のアクティビティ] アイコンをクリックしてダイアログボックスを開きます。 詳細については、「プライマリ ファブリック インターコネクトのリブートの承認」を参照してください。

9 サーバ ファームウェアのアップグレード：[サーバ ファームウェアのインストール] ウィザードで次の手順を実行します。 詳細については、「自動インストールを使用したサーバ ファームウェアのアップグレード」を参照してください。

a Cisco UCS Manager で、[機器] > [ファームウェアの管理] > [ファームウェアの自動インストール] を選択し、[サーバ ファームウェアのインストール] をクリックします。

b ファブリック インターコネクトにダウンロードしたファームウェア バンドルを選択します。

c ホスト ファームウェア パッケージのルートをクリックし、サービス プロファイルが関連付けられていないサーバを含むすべてのサーバをアップグレードします。

d [影響を受けるエンドポイント サマリー] ページで、このアップグレードによってリセットされるサーバのリストを確認します。

e Cisco UCS ドメイン内のすべてのサーバのアップグレードが完了するまで待機します。

10 （オプション）Call Home の有効化：ファームウェアをアップグレードする前に Call Home を無効にした場合は、Call Home を有効にします。 詳細については、「Call Home の有効化」を参照してください。

リリース 1.3 からの手動アップグレード手順の概要

（注） 次の一連の手順では、ホスト ファームウェア パッケージをすべてのサーバのサービス プロファイルに含めていると仮定します。 適切な手順の詳細については、Cisco UCS B シリーズのファームウェアの管理ガイドを参照してください。

手順の順序は、データ トラフィックの中断を最小限に抑えるように設計されています。 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。

1 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, （10 ページ） で説明されているすべての前提条件の手順を実行します。

2 Cisco.com から Cisco UCS インフラストラクチャ ソフトウェア バンドル のファームウェア イメージを入手して、それをファブリック インターコネクトにダウンロードします。インフラストラクチャのアップグレードを完了するには、このファームウェア イメージをステップ 5 でもう 1 回ダウンロードする必要があります。 この余分なダウンロードは、Cisco UCS リリース 1.3 が別のサーバとインフラストラクチャ バンドルをサポートしないために必要です。

3 （オプション）Call Home の無効化：Cisco UCS ドメインに Call Home または Smart Call Home が含まれている場合は、Call Home を無効にして、Cisco UCS Manager がコンポーネントを再起動するときに不要なアラートを受信しないようにします。 詳細については、「Call Home の無効化」を参照してください。

4 I/O モジュールの更新 詳細については、「」または「」を参照してください。

5 I/O モジュールのアクティブ化：この手順を実行するときに [互換性チェックを無視する] と [スタートアップバージョンのみを設定する] を選択します。 詳細については、「IOM のファームウェアのアクティブ化」を参照してください。

6 Cisco UCS Managerのアクティブ化：この手順を実行するときに [Skip Validation] を選択します。 詳細については、「Cisco UCS Manager ソフトウェアのアクティブ化」を参照してください。

7 次のファームウェア イメージを Cisco.com から入手し、それらをファブリック インターコネクトにダウンロードします。 詳細については、Cisco UCS リリース 2.1 ファームウェアのダウンロード, （10 ページ） を参照してください。

- Cisco UCS インフラストラクチャ ソフトウェア バンドル：すべての Cisco UCS ドメインで必要です。
- Cisco UCS B シリーズ ブレード サーバ ソフトウェア バンドル：ブレード サーバが含まれるすべての Cisco UCS ドメインで必要です。
- 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：統合されたラックマウント サーバが含まれる Cisco UCS ドメインのみで必要です。 このバンドルには、Cisco UCS Manager がそれらの

サーバを管理できるようにするためのファームウェアが含まれており、スタンドアロンCシリーズラックマウント サーバには適用されません。

8 下位のファブリック インターコネクトをアクティブにします。 詳細については、「従属ファブリック インターコネクトのファームウェアのアクティブ化」を参照してください。

9 コントロール プレーンの中断を避けるために、プライマリ ファブリック インターコネクトをアップグレード済みのファブリック インターコネクトに手動でフェールオーバーします。 詳細については、「ファブリック インターコネクトの強制フェールオーバー」を参照してください。

10 データ パスが復元されたことを確認します。 詳細については、「データ パスの準備完了の確認」を参照してください。

注意 アップグレード時の中断を最小限に抑えるには、次のことを確認する必要があります。

- ファブリック インターコネクトとサービス プロファイルの両方がフェールオーバー用に設定されていることを確認します。
- プライマリ ファブリック インターコネクトをリブートする前に、セカンダリ ファブリック インターコネクトからデータ パスが正常に復元されていることを確認します。

11 プライマリ ファブリック インターコネクトをアクティブ化します。 詳細については、「プライマリ ファブリック インターコネクトのファームウェアのアクティブ化」を参照してください。

12 サーバのホスト ファームウェア パッケージの更新：アップグレードする最後のファームウェアであることが必要です。 そのファームウェアを使用したサーバの追加のリブートを避けるため、この手順の実行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。 詳細については、「ホスト ファームウェア パッケージの更新」を参照してください。 ホスト ファームウェア パッケージ内の次のファームウェアをアップグレードすることができます。

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

  Cisco UCS は、新しい管理ファームウェア パッケージの作成をサポートしなくなりました。 管理ファームウェア パッケージをすべてのサービス プロファイルから削除し、ホスト ファームウェア パッケージを使用してサーバ上の CIMC を更新することをお勧めします。

（注） ボード コントローラ ファームウェアのアップグレードでは電源の再投入が必要です。アップグレードの実行時に、この操作を行うように促されます。

13 （オプション）Call Home の有効化：ファームウェアをアップグレードする前に Call Home を無効にした場合は、Call Home を有効にします。 詳細については、「Call Home の有効化」を参照してください。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。 このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。 このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。 添付されていない場合には、代理店にご連絡ください。

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

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。 シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

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

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

© 2012-2015 Cisco Systems, Inc. All rights reserved.

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

©2008 Cisco Systems, Inc. All rights reserved.
Cisco、Cisco Systems、およびCisco Systemsロゴは、Cisco Systems, Inc.またはその関連会社の米国およびその他の一定の国における登録商標または商標です。
本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。
「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(0809R)
この資料の記載内容は2008年10月現在のものです。
この資料に記載された仕様は予告なく変更する場合があります。

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255（フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00〜12:00、13:00〜17:00
http://www.cisco.com/jp/go/contactcenter/