注意、ガイドライン、および制約事項

この章は、次の項で構成されています。

- 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，1 ページ
- Cisco UCS Central のファームウェア管理に関する注意、ガイドライン、および制約事項，10 ページ

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 CLI では、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をアップグレードできません。Cisco UCS Manager CLI では、サポートされていないリリースにハードウェアをアップグレードしようとすると、エラー メッセージが表示されます。

ファームウェアをアップグレードする前に、すべてのエラーを解消してください。

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 リリース 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 リリース 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 リリース 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 リリース 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 リリース 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 リリース 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 リリース 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 に対して VLAN ID 4048 が使用されている場合に、Cisco UCS リリース 1.4 からリリース 2.0 にアップグレードすると、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 は保持されます。競合するイーサネット VLAN がある場合は、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。

ファームウェアアップグレードのハードウェアに関する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。

サポートされていないハードウェアは検出されない

新しいサーバまたはアダプタを、それらのサーバ/アダプタ未対応の Cisco UCS Manager リリースを使用している既存の Cisco UCS システムに追加した場合、そのシステムは検出されません。そのサーバまたはアダプタが現在の UCS ファームウェア バージョンでサポートされていないというエラー メッセージが FSM に表示されます。この問題を解決するには、次のいずれかを実行します。

- 互換性のある最新リリースに機能カタログを更新する。
- 新しいハードウェアに必要なバージョンに Cisco UCS Manager のインフラストラクチャ ファームウェアをアップグレードする。リリース ノートのハードウェア サポート マトリックスに互換性情報が詳細に記載されています。

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しても、更新が目的の順序で実行される保証はなく、エンドポイント、ファブリック インターコネクト、Cisco UCS Manager の間での通信が損なわれる可能性があります。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 [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 状態を維持します。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 [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。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, （1 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、インストール サーバ ファームウェア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のファームウェアをサーバの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のファームウェアを先にアップグレードし、次にサーバの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のファームウェアのアップグレードが完了するまで、サーバの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	• インストールインフラストラクチャ ファームウェアの実行 • インストール サーバ ファームウェアの実行 • 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）	インストール サーバ ファームウェアの実行
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

インストール サーバ ファームウェアに対するホスト 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

インストール サーバ ファームウェアでは、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 プロファイルにインストール サーバ ファームウェア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、インストール サーバ ファームウェアでは、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インストール サーバ ファームウェア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インストール サーバ ファームウェアを使用すると、インストール サーバ ファームウェア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。インストール サーバ ファームウェアでは、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 インストール サーバ ファームウェア 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。

- インストール サーバ ファームウェア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、次にインストールサーバファームウェア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バ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

インストール サーバ ファームウェアを実行した後、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インストールサーバファームウェア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、最後にインストールサーバファームウェア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、エンドポイントをそのサーバのファームウェアに手動でアップグレードする必要があります。インストール サーバ ファームウェアには、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インストール サーバ ファームウェア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 Central のファームウェア管理に関する注意、ガイドライン、および制約事項

Cisco UCS Central から Cisco UCS Manager のファームウェアの管理を開始する前に、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。

- ドメイン グループに定義したファームウェア ポリシーは、このドメイン グループに追加されるすべての新しい Cisco UCS ドメインに適用されます。ドメイン グループでファームウェア ポリシーが定義されていない場合、Cisco UCS ドメインは親ドメイン グループからポリシーを継承します。
- グローバル ポリシーは、Cisco UCS Manager が Cisco UCS Central との接続を失った場合でも Cisco UCS Manager にグローバルに残ります。Cisco UCS Manager でグローバルなポリシーの

いずれかに変更を適用するには、所有権をグローバルからローカルに変更する必要があります。

- ホスト ファームウェア パッケージを Cisco UCS Central から作成した場合は、これをサービス プロファイルに関連付けて、Cisco UCS ドメインにアップデートを展開する必要があります。
- Cisco UCS Central でホスト ファームウェア パッケージを変更すると、その変更はホスト ファームウェア アップデートに関連付けられた次のメンテナンス スケジュールの際に Cisco UCS ドメインに適用されます。
- Cisco UCS Central で定義したホスト ファームウェア メンテナンス ポリシーは、Cisco UCS ドメインの org-root に適用されます。Cisco UCS Central から Cisco UCS ドメインのサブ組織に対して別のホスト メンテナンス ポリシーを定義することはできません。
- サービス プロファイルとの関連付けを持たないサーバは、ホスト ファームウェア パックのデフォルト バージョンにアップグレードされます。これらのサーバにはメンテナンス ポリシーがないため、ただちにリブートされます。
- Cisco UCS Central でメンテナンス ポリシーを指定してユーザの確認応答をイネーブルにし、スケジュールを指定しない場合は、Cisco UCS Manager からのみ保留中のタスクに確認応答できます。Cisco UCS Central から保留中のアクティビティに確認応答するには、グローバルなスケジューラを使用してメンテナンスをスケジュールし、ユーザの確認応答をイネーブルにする必要があります。
- Cisco UCS Central でメンテナンス ポリシーをスケジュールし、ユーザの確認応答をイネーブルにすると、このタスクは保留中のアクティビティ タブにスケジュールで指定した時刻で表示されます。
- メンテナンス ポリシーの保留中のアクティビティは、ドメイン グループのセクションからのみ表示できます。
- 任意のファームウェアのスケジュールに対するユーザの確認応答をイネーブルにして、Cisco UCS ドメインでの予期せぬリブートを避けるようにしてください。