Cisco IMC ファームウェア管理

この章は、次の内容で構成されています。

- ファームウェアの概要 （1 ページ）
- シスコからのファームウェアの取得 （3 ページ）
- Cisco IMC セキュア ブートについて （5 ページ）
- Cisco IMC ファームウェアのインストール （8 ページ）
- インストールした CIMC ファームウェアのアクティブ化 （12 ページ）
- BIOS ファームウェアのインストール （14 ページ）
- インストールされている BIOS ファームウェアのアクティブ化 （17 ページ）
- 保留中の BIOS アクティベーションのキャンセル （19 ページ）
- VIC ファームウェアのインストール （20 ページ）
- リモート サーバからの CMC ファームウェアのインストール （23 ページ）
- インストールした CMC ファームウェアのアクティブ化 （25 ページ）
- リモート サーバからの SAS エクスパンダ ファームウェアのインストール （27 ページ）
- インストール済み SAS エクスパンダ ファームウェアの有効化 （29 ページ）

ファームウェアの概要

C シリーズ サーバは、使用する C シリーズ サーバ モデルに特有のシスコ認定ファームウェアを使用します。すべてのサポート対象サーバ モデルのファームウェアの新しいリリースは、Cisco.com からダウンロードできます。

注意 新しい BIOS ファームウェアをインストールするとき、それはサーバで実行されている Cisco IMC ファームウェアと同じソフトウェア リリースに属する必要があります。新しい BIOS ファームウェアのインストールは、必ず一致する Cisco IMC ファームウェアをアクティブにした後に行ってください。そうしないと、サーバはブートしません。

起こりうる問題を避けるため、 Cisco Host Upgrade Utility（HUU）を使用することを強く推奨します。このユーティリティは BIOS、 Cisco IMC、およびその他のファームウェアを互換性のあるレベルにアップグレードします。このユーティリティの詳細については、インストールする Cisco IMC ソフトウェア リリースに付属の HUU のバージョン の *Cisco Host Upgrade Utility Guide* を参照してください。HUU のガイドは次の URL にあります。 http://www.cisco.com/en/US/products/ps10493/products_user_guide_list.html。

ファームウェアを手動で更新する場合は、最初に Cisco IMC ファームウェアを更新する必要があります。Cisco IMC ファームウェアの更新プロセスは、次の段階に分けられます。これは、サーバがオフラインになる時間を最小限にするためです。

- インストール：この段階では、Cisco IMC は選択した非アクティブまたはバックアップの Cisco IMC ファームウェアをサーバのスロットにインストールします。
- アクティベーション：この段階では、Cisco IMC は非アクティブのファームウェア バージョンをアクティブとして設定するため、サービスの中断の原因となります。サーバをリブートすると、新規のアクティブ スロット内のファームウェアが、実行中のバージョンになります。

Cisco IMC ファームウェアをアクティブ化した後は、BIOS ファームウェアを更新できます。BIOS 更新のプロセス全体でサーバの電源をオフにする必要があるため、プロセスは段階に分類されません。その代わり、入力するコマンドは 1 つで済みます。Cisco IMC は BIOS ファームウェアをできる限り迅速にインストールし、更新します。Cisco IMC がリブートを完了すると、サーバの電源をオンにして、サービスに戻すことができます。

（注）

- 古いファームウェア バージョンを新しいものにアップグレードしたり、新しいファームウェア バージョンを古いものにダウングレードしたりできます。
- この手順は、スタンドアロン モードで実行している Cisco UCS C シリーズ サーバにのみ適用されます。Cisco UCS Manager の統合モードで実行している UCS C シリーズのファームウェアをアップグレードするには、Cisco Technical Assistance Center にお問い合わせください。

セキュア モードの Cisco IMC では、ロードおよび実行前のすべてのファームウェア イメージがデジタル的に署名され、信頼性と整合性が確認され、改竄されたソフトウェアの実行からデバイスを確実に保護できます。

シスコからのファームウェアの取得

手順

ステップ 1 http://www.cisco.com を参照します。

ステップ 2 まだログインしていない場合は、ページの右上隅にある [Log In] をクリックし、Cisco.com の資格情報を使用してログインします。

ステップ 3 上部のメニュー バーで、[Support] をクリックします。

ステップ 4 ロール ダウン メニューの [All Downloads] をクリックします。

ステップ 5 使用しているサーバ モデルが [Recently Used Products] リストに表示される場合は、サーバ名をクリックします。表示されない場合は、次の手順を実行します。

a) 左側のボックスの [Products] をクリックします。
b) 中央のボックスで、[Unified Computing and Servers] をクリックします。
c) 右側のボックスで、[Cisco UCS C-Series Rack-Mount Standalone Server Software] をクリックします。
d) 右側のボックスで、ダウンロードするソフトウェアのサーバ モデルをクリックします。

ステップ 6 [Unified Computing System (UCS) Server Firmware] リンクをクリックします。

ステップ 7 （任意） ページの左側のメニュー バーから以前のリリースを選択します。

ステップ 8 選択したリリースのCisco Host Upgrade UtilityISOに関連付けられている [**Download**]ボタンをクリックします。

ステップ 9 [Accept License Agreement] をクリックします。

ステップ 10 ISO ファイルをローカル ドライブに保存します。

Cisco Host Upgrade Utilityを含むこの ISO ファイルを使用して、Cisco IMC とサーバーの BIOS 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。 このユーティリティの詳細については、インストールするCisco IMCソフトウェアリリースに付属の HUU のバージョン の *Cisco Host Upgrade Utility Guide* を参照してください。HUU のガイドは次の URL にあります。 http://www.cisco.com/en/US/products/ps10493/products_user_guide_list.html。

ステップ 11 （任意） Cisco IMC と BIOS ファームウェアを手動でアップグレードする予定の場合、次の手順を実行します。

リリース 3.0 以降、BIOS および Cisco IMC ファームウェア ファイルは、単独の .zip ファイルとして HUU 内に組み込まれなくなりました。現在、BIOS と Cisco IMC ファームウェアを抽出するには、HUU の GETFW フォルダにある **getfw** ユーティリティを使用する必要があります。BIOS または Cisco IMC ファームウェア ファイルを抽出するには、次の手順を実行します。

（注） この手順を実行するには：

- Openssl をターゲット システムにインストールする必要があります。
- Squashfs カーネル モジュールをターゲット システムにロードする必要があります。

Viewing the GETFW help menu:

```
[root@RHEL65-***** tmp]# cd GETFW/
[root@RHEL65-***** GETFW]# ./getfw -h
Help:
  Usage: getfw {-b -c -C -H -S -V -h} [-s SRC] [-d DEST]
    -b      : Get BIOS Firmware
    -c      : Get CIMC Firmware
    -C      : Get CMC Firmware
    -H      : Get HDD Firmware
    -S      : Get SAS Firmware
    -V      : Get VIC Firmware
    -h      : Display Help
    -s SRC  : Source of HUU ISO image
    -d DEST : Destination to keep Firmware/s
  Note : Default BIOS & CIMC get extracted
```

Extracting the BIOS firmware:

```
[root@RHEL65-***** GETFW]# ./getfw -s /root/Desktop/HUU/ucs-c2xxx-huu-3.0.1c.iso -d
/tmp/HUU
FW/s available at '/tmp/HUUucs-c2xxx-huu-3.0.1c'
[root@RHEL65-***** GETFW]# cd /tmp/HUU/
[root@RHEL65-***** HUU]# cd ucs-c2xxx-huu-3.0.1c/
[root@RHEL65-***** ucs-c2xxx-huu-3.0.1c]# ls
bios  cimc
[root@RHEL65-***** ucs-c2xxx-huu-3.0.1c]# cd bios/
[root@RHEL65-***** bios]# ls
bios.cap
[root@RHEL65-***** bios]#
```

Extracting the CIMC firmware:

```
[root@RHEL65-***** GETFW]# ./getfw -s /root/Desktop/HUU/ucs-c2xxx-huu-3.0.1c.iso -d
/tmp/HUU
FW/s available at '/tmp/HUUucs-c2xxx-huu-3.0.1c'
[root@RHEL65-***** GETFW]# cd /tmp/HUU/
[root@RHEL65-***** HUU]# cd ucs-c2xxx-huu-3.0.1c/
[root@RHEL65-***** ucs-c2xxx-huu-3.0.1c]# ls
bios  cimc
[root@RHEL65-***** ucs-c2xxx-huu-3.0.1c]# cd cimc/
[root@RHEL65-***** cimc]# ls
cimc.cap
[root@RHEL65-***** cimc]#
```

ステップ 12 （任意）リモート サーバーからファームウェアをインストールする予定の場合、そのリモート サーバーに BIOS のインストール用 CAP ファイルと Cisco IMC インストール用 BIN ファイルをコピーします。

リモート サーバーは次のいずれかになります。

- TFTP
- FTP

- SFTP
- SCP
- HTTP

サーバーにはリモート サーバーのコピー先フォルダに対する読み取り権限が必要です。

（注） Cisco UCS C シリーズ サーバでは、リモート サーバからファームウェアを更新する際に、サーバのフィンガープリント確認がサポートされます。このオプションは、リモート サーバのタイプとして SCP または SFTP を選択している場合のみ利用できます。

このアクションを実行する際にリモート サーバのタイプとして SCP または SFTP を選択すると、メッセージ「Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?」が表示されます。サーバのフィンガープリントの真偽に応じて、[y] または [n] をクリックします。

フィンガープリントはホストの公開キーに基づいており、接続先のホストを識別または確認できます。

次のタスク

Cisco Host Upgrade Utility 使用してサーバー上のすべてのファームウェアをアップグレードするか、手動でサーバーに Cisco IMC ファームウェアをインストールします。

Cisco IMC セキュア ブートについて

Cisco IMC のセキュア モードについて

（注） Cisco IMC のセキュア ブート モードは、一部の Cisco UCS C シリーズ サーバでのみデフォルトで有効になっています。

Host Upgrade Utility（HUU）、Web UI または CLI を使用して、Cisco IMC を最新バージョンに更新できます。Cisco IMC をアップグレードするために HUU を使用する場合は、セキュア ブート モードをイネーブルにするよう求めるプロンプトが表示されます。**[Yes]** を選択すると、システムはセキュア モードを開始し、ファームウェアを 2 度インストールします。**[No]** を選択すると、システムは非セキュア モードを開始します。Cisco IMC をアップグレードするために Web UI または CLI を使用する場合は、バージョン 2.0(x) にアップグレードする必要があります。バージョン2.0(x)でシステムを起動した後、システムはデフォルトでは非セキュア モードで起動します。セキュア モードを有効にする必要があります。セキュア モードを有効にすると、自動的にファームウェアが再インストールされます。Web UI では、セキュア モード オプ

ションが Cisco IMC ファームウェア更新ページ内のチェックボックスとして利用できます。CLI では、**update-secure** コマンドを使用してセキュア モードを有効にできます。

Cisco IMC バージョン 2.0 への最初のアップグレード時に、機能およびアプリケーションの一部が正しくインストールされておらず、2 回目のアップグレードが必要であることを示す警告メッセージが表示される場合があります。Cisco IMC ファームウェア バージョン 2.0(x) をセキュア モードで正しくインストールするために、セキュア ブート オプションをイネーブルまたは非イネーブルにした状態で2回目のアップグレードを実行することを推奨します。インストールが完了した後、イメージをアクティブ化する必要があります。セキュア ブート オプションをイネーブルにしたままシステムを起動した後は、Cisco IMC はセキュア モードのままとなり、後でディセーブルにできません。このイメージがアクティブになっていない場合や、他のファームウェア イメージを再インストールした場合、Cisco IMC が応答不能になる場合があります。

警告 セキュア ブートの移行でファームウェアをインストールした後は、他の通常のサーバベースのタスクを実行する前にイメージをアクティブにする必要があります。このイメージがアクティブになっていない場合や、他のファームウェア イメージを再インストールした場合、Cisco IMC が応答不能になる場合があります。

セキュア ブートは、ファームウェアのインストールが完了し、イメージがアクティブになった場合にのみイネーブルになります。

（注） Cisco IMC がセキュア モードになっている場合、次のことを意味します。

- 署名済みの Cisco IMC ファームウェア イメージのみがデバイスにインストールされ、起動できます。
- セキュア Cisco IMC モードは後でディセーブルにできません。
- いずれの Cisco IMC バージョンも最新バージョンに直接アップグレードできます。
- Cisco IMC のファームウェア バージョンは、バージョン 1.5(3x) より前のバージョンにインストールまたは起動できません。
- Cisco IMC バージョン 2.0 は、バージョン 1.4(x)、1.5、1.5(2x)、または 1.5(1)、1.5(2) または非セキュアのファームウェア バージョンにダウングレードできません。

最新バージョンからダウングレードする際にサポートされる Cisco IMC バージョン

次の表は、前のバージョンにダウングレードできるセキュア モードの Cisco IMC バージョンを示します。

Cisco IMC バージョンから	目的の Cisco IMC バージョン	可能性
2.0(x)	1.5(1) よりも前	可能性なし

Cisco IMC バージョンから	目的の Cisco IMC バージョン	可能性
2.0(x)	1.5(3x) 以降	可能性あり
2.0(x)	1.5(3x) よりも前	可能性なし

（注） 使用している Cisco IMC のバージョンが非セキュア モードの場合、Cisco IMC を以前のバージョンにダウングレードすることができます。

（注） HUU を使用して 1.5(4) より前のバージョンに Cisco IMC バージョンをダウングレードする場合は、最初に Cisco IMC をダウングレードし、その後に他のファームウェアをダウングレードする必要があります。ファームウェアをアクティブにし、次に BIOS ファームウェアをダウングレードします。

Cisco IMC バージョン 2.0(1) に必要な更新回数

重要 この項は、Cisco IMC バージョン 2.0(1) 以前のリリースに有効です。

最新バージョンにアップグレードする際にサポートされる Cisco IMC バージョン

次の表に、最新バージョンのすべてのアプリケーションを正しくインストールするために Cisco IMC に必要な更新回数を示します。

Cisco IMC バージョンから	非セキュア Cisco IMC バージョン 2.0(x) へ	セキュア Cisco IMC バージョン 2.0(x) へ
1.5(2) よりも前	更新 2 回	更新 2 回
1.5(2)	更新 1 回	更新 2 回
1.5(3)	更新 1 回	更新 2 回
1.5(3x) 以降	更新 1 回	更新 2 回

非セキュア モードでの Cisco IMC の更新

重要 この項は、Cisco IMC バージョン 2.0(1) 以前のリリースに有効です。

すべての最新機能とアプリケーションが正常にインストールされた状態で、非セキュアモードで Cisco IMC を最新バージョンにアップグレードできます。Web UI または CLI を使用して Cisco IMC を最新バージョンにアップグレードするときは、使用しているバージョンによってはファームウェアを手動で2回更新する必要があります。「最新バージョンにアップグレードする際にサポートされる Cisco IMC バージョン」を参照してください。Cisco IMC バージョンにアップグレードするために HUU を使用すると、最新バージョンに自動的にアップグレードされます。

（注） 1.5(2x) よりも前のバージョンの Cisco IMC からインストールする場合は、次のメッセージが表示されます。

警告 「一部の Cisco IMC ファームウェア コンポーネントが正しくインストールされていません。Please reinstall Cisco IMC firmware version 2.0(1) or higher to recover".

（注） （HUUによる）更新の最中は、KVMセッションに再接続して更新の現在

することを推奨します。

Cisco IMC が非セキュア モードで実行している場合は、次を意味します。

- 署名済みまたは未署名の Cisco ファームウェア イメージをデバイスにインストールできます。
- いずれの Cisco IMC バージョンも最新バージョンに直接アップグレードできます。
- Cisco IMC のファームウェア バージョンは以前のバージョンにインストールまたは起動できます。

Cisco IMC ファームウェアのインストール

- フロント パネルの USB デバイスを介して Cisco IMC ファームウェアを更新する場合は、スマート アクセス USB オプションが有効であることを確認します。
- アップデートがすでに処理中であるときにアップデートを開始すると、どちらのアップデートも失敗します。

始める前に

- admin 権限を持つユーザとして Cisco IMC にログインします。

- Cisco.com から Cisco Host Upgrade UtilityISO ファイルを入手し、シスコからのファームウェアの取得 （3 ページ） の説明に従ってファームウェア インストール ファイルを抽出します。

手順

	コマンドまたはアクション	目的
ステップ 1	server# **scope cimc**	Cisco IMC コマンド モードを開始します。
ステップ 2	server /cimc # **scope firmware**	Cisco IMC ファームウェア コマンド モードを開始します。
ステップ 3	server /cimc /firmware # **update** プロトコル *IP* アドレス パス	プロトコル、リモート サーバーの IP アドレス、サーバー上のファームウェア ファイルへのファイル パスを指定します。プロトコルは次のいずれかになります。 • TFTP • FTP • SFTP • SCP • HTTP

	コマンドまたはアクション	目的
		（注） Cisco UCS C シリーズ サーバーでは、リモート サーバーからファームウェアを更新したときの、サーバーのフィンガープリントの確認をサポートするようになりました。このオプションは、リモート サーバのタイプとして SCP または SFTP を選択している場合のみ利用できます。 このアクションを実行する際にリモート サーバのタイプとして SCP または SFTP を選択すると、メッセージ「Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?」が表示されます。サーバのフィンガープリントの真偽に応じて、[y] または [n] をクリックします。 フィンガープリントはホストの公開キーに基づいており、接続先のホストを識別または確認できます。
ステップ 4	server /cimc/firmware # **update usb** パスとファームウェア ファイル名	接続されている USB から Cisco IMC ファームウェアを更新します。
ステップ 5	（任意） server /cimc /firmware # **update-secure** プロトコル *IP* アドレス パス	Cisco IMC のセキュア ブート オプションに移行します。移行は次のことを意味します。 • 署名済された Cisco IMC ファームウェア イメーにのみをサーバ上でインストールおよびブートできます。 • バージョン 1.5(3x) 以前の Cisco IMC ファームウェアはインストールまたはブートできません。

	コマンドまたはアクション	目的
		• セキュア ブートを後でディセーブルにすることができません。 **重要** このアクションは、Cisco IMC 2.0(1) バージョンにのみ使用できます。以降のバージョンでは、デフォルトで有効になっています。 **警告** セキュア ブートの移行でファームウェアをインストールした後は、他の通常のサーバベースのタスクを実行する前にイメージをアクティブにする必要があります。このイメージがアクティブになっていない場合や、他のファームウェア イメージを再インストールした場合、Cisco IMC が応答不能になる場合があります。 Cisco IMC バージョン 2.0(1) の場合、セキュア ブートは、ファームウェアのインストールが完了し、イメージがアクティブになっている場合にのみイネーブルになります。
ステップ 6	（任意） server /cimc /firmware # **show detail**	ファームウェア アップデートの進捗状況を表示します。

例

次に、Cisco IMC ファームウェアを更新し、非セキュア ブートから Cisco IMC バージョン 2.0 のセキュア ブートに Cisco IMC を移行する例を示します。

```
server# scope cimc
server /cimc # scope firmware
server /cimc /firmware # update ftp 192.0.20.34 //test/dnld-ucs-k9-bundle.1.0.2h.bin
Firmware update has started.
Please check the status using "show detail"
Server /cimc /firmware # update-secure tftp 1.1.1.1 /cimc-pkg.bin
Migrating to Cisco IMC Secure Boot option implies:
-You can install and boot only signed Cisco IMC firmware images on the server.
-You cannot install and boot Cisco IMC firmware versions prior than 1.5(3x).
```

```
-You cannot disable Secure Boot later on.

After installing the firmware with the Secure Boot migration, you must
activate the image before performing any other regular server-based tasks.
The Secure Boot option is enabled only when the firmware installation
is complete and you have activated the image.

Continue?[y|N]y
Update to Secure Boot selected, proceed with update.
Firmware update initialized.
Please check the status using "show detail".
server /cimc /firmware # show detail
Firmware Image Information:
    Update Stage: DOWNLOAD
    Update Progress: 5
    Current FW Version: 2.0(0.29)
    FW Image 1 Version: 2.0(0.28)
    FW Image 1 State: BACKUP INACTIVATED
    FW Image 2 Version: 2.0(0.29)
    FW Image 2 State: RUNNING ACTIVATED
    Boot-loader Version: 2.0(0.9).35
    Secure Boot: DISABLED

*+--------------------------------------------------------------------------+
 + Some of the Cisco IMC firmware components are not installed properly! +
 + Please reinstall Cisco IMC firmware version 2.0 or higher to recover. +
 +--------------------------------------------------------------------------+
server /cimc /firmware #
```

次に、Cisco IMC ファームウェアを更新する例を示します。

次のタスク

新しいファームウェアをアクティブにします。

インストールした CIMC ファームウェアのアクティブ化

始める前に

CIMC ファームウェアをサーバにインストールします。

重要 アクティブ化の進行中は、次のことを行わないでください。

- サーバーのリセット、電源切断、シャットダウン。
- CIMC をリブートまたはリセットします。
- 他のすべてのファームウェアをアクティブ化します。
- テクニカル サポート データまたは設定データをエクスポートします。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope cimc**	CIMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scope firmware**	ファームウェア コマンド モードを開始します。
ステップ 3	Server /cimc/firmware # **show detail**	使用可能なファームウェア イメージおよびステータスを表示します。
ステップ 4	Server /cimc/firmware # **activate** [**1** | **2**]	選択したイメージをアクティブにします。イメージ番号が指定されていない場合、サーバは現在非アクティブのイメージをアクティブにします。
ステップ 5	プロンプトで **y** と入力し、選択したファームウェア イメージをアクティブ化します。	BMC がリブートし、リブートが完了するまですべての CLI セッションと GUI セッションが終了します。
ステップ 6	（任意） CLI にログインし、手順 1 ～ 3 を繰り返してアクティブ化されたことを確認します。	

例

この例では、ファームウェア イメージ 1 をアクティブ化し、BMC がリブートした後でアクティブ化されたことを確認します。

```
Server# scope cimc
Server /cimc # scope firmware
Server /cimc/firmware # show detail
Firmware Image Information:
    Update Stage: NONE
    Update Progress: 100
    Current FW Version: 1.3(3a)
    FW Image 1 Version: 1.4(3j)
    FW Image 1 State: BACKUP INACTIVATED
    FW Image 2 Version: 1.3(3a)
    FW Image 2 State: RUNNING ACTIVATED
    Boot-loader Version: 1.4(3.21).18

Server /cimc/firmware # activate 1
This operation will activate firmware 1 and reboot the BMC.
Continue?[y|N]y
.
.
 -- BMC reboot --
.
.
-- Log into CLI as Admin --

Server# scope cimc
Server /cimc # scope firmware
```

```
Server /cimc/firmware # show detail
Firmware Image Information:
    Update Stage: NONE
    Update Progress: 100
    Current FW Version: 1.4(3j)
    FW Image 1 Version: 1.4(3j)
    FW Image 1 State: RUNNING ACTIVATED
    FW Image 2 Version: 1.3(3a)
    FW Image 2 State: BACKUP INACTIVATED
    Boot-loader Version: 1.4(3.21).18
```

BIOS ファームウェアのインストール

（注） この手順は、一部のサーバでは使用できません。他の BIOS インストール方法については、次の URL で入手可能な *Cisco UCS C-Series Rack-Mount Server BIOS Upgrade Guide* を参照してください。
http://www.cisco.com/en/US/docs/unified_computing/ucs/c/sw/bios/b_Upgrading_BIOS_Firmware.html

始める前に

- admin 権限を持つユーザとして Cisco IMC にログインします。
- インストールした CIMC ファームウェアのアクティブ化 （12 ページ）の説明に従って、インストールする BIOS バージョンに対応する Cisco IMC ファームウェアをアクティブにします。
- サーバの電源を切ります。

（注）
- アップデートがすでに処理中であるときにアップデートを開始すると、どちらのアップデートも失敗します。
- フロントパネルのUSBデバイスを介してBIOSファームウェアを更新する場合は、スマート アクセス USB オプションが有効であることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope cimc**	Cisco IMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scope firmware**	ファームウェア コマンド モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	Server /cimc/firmware # **show detail**	使用可能なファームウェア イメージおよびステータスを表示します。
ステップ 4	[現在のファームウェア バージョン（Current FW Version）] フィールドに表示されるファームウェアバージョンが、インストールするBIOSファームウェアバージョンと一致するかどうか確認します。	**重要** Cisco IMC ファームウェアバージョンが一致しない場合は、この手順を続行する前に Cisco IMC ファームウェアをアクティブ化します。そうしないとサーバがブートしません。詳細については、インストールした CIMC ファームウェアのアクティブ化（12 ページ）を参照してください。
ステップ 5	Server /cimc/firmware # **top**	サーバのルート レベルに戻ります。
ステップ 6	Server# **scope bios**	BIOS コマンド モードを開始します。
ステップ 7	Server /bios # **update** プロトコル *IP* アドレス パス	次の情報を指定します。 • プロトコル。TFTP、FTP、SFTP、SCP、または HTTP が使用できます。

	コマンドまたはアクション	目的
		（注） Cisco UCS C シリーズ サーバーでは、リモート サーバーからファームウェアを更新したときの、サーバーのフィンガープリントの確認をサポートするようになりました。このオプションは、リモート サーバのタイプとして SCP または SFTP を選択している場合のみ利用できます。 このアクションを実行する際にリモート サーバのタイプとして SCP または SFTP を選択すると、メッセージ「Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?」が表示されます。サーバのフィンガープリントの真偽に応じて、[y] または [n] をクリックします。 フィンガープリントはホストの公開キーに基づいており、接続先のホストを識別または確認できます。 • リモート サーバの IPv4 アドレスまたは IPv6 アドレス、あるいはホスト名。 • リモート サーバ上の BIOS ファームウェア ファイルへのファイル パス。
ステップ 8	Server /bios # **update usb** パスとファームウェア ファイル名	接続されている USB から BIOS ファームウェアを更新します。

例

次に、BIOS ファームウェアをアップデートする例を示します。

```
Server# scope bios
Server /bios# show detail
BIOS:
    BIOS Version: CxxMx.2.0.3.0.080720142114
    Backup BIOS Version: CxxMx.2.0.2.68.073120141827
    Boot Order: (none)
    Boot Override Priority:
    FW Update/Recovery Status: None, OK
    UEFI Secure Boot: disabled
    Configured Boot Mode: None
    Actual Boot Mode: Unknown
    Last Configured Boot Order Source: UNKNOWN
Server /bios # update ftp 10.10.10.10 //upgrade_bios_files/Cxx-BIOS-1-4-3j-0.CAP
 <CR>  Press Enter key
Firmware update has started.
Please check the status using "show detail"

For updating the BIOS using the front panel USB:

Server /bios # update usb CxxMx-BIOS-3-1-0-289.cap
 User Options:USB Path[Cxxmx-BIOS-3-1-0-289.cap]
<CR> Press Enter key
Firmware update has started.
Please check the status using "show detail"
Server /bios # show detail
BIOS:
BIOS Version: CxxMx.3.1.0.289.0530172308
Boot Order: (none)
FW Update Status: None, OK
UEFI Secure Boot: disabled
Configured Boot Mode: Legacy
Actual Boot Mode: Legacy
Last Configured Boot Order Source: BIOS
One time boot device: (none)
Server /bios #
```

インストールされている BIOS ファームウェアのアクティブ化

（注）

- リリース 4.0(1) から、サーバがオンの場合に BIOS をアクティベートすることができます。サーバがオンのときに、ファームウェアをアクティブにすると、アクティベーションが保留状態で、ファームウェアは次のサーバが再起動した後にアクティベーションされます。
- [Activate BIOS Firmware]（アクティブ化）オプションを使用できるのは一部の C シリーズサーバだけです。このオプションがないサーバでは、サーバをリブートしてインストールされている BIOS ファームウェアをアクティブにします。

始める前に

- BIOS ファームウェアをサーバにインストールします。
- ホストの電源を切ります。

重要 アクティブ化の進行中は、次のことを行わないでください。

- サーバのリセット、電源切断、シャットダウン。
- Cisco IMCCisco IMC のリブートまたはリセット。
- 他のすべてのファームウェアをアクティブ化します。
- テクニカル サポート データまたは設定データをエクスポートします。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope bios**	BIOS コマンド モードを開始します。
ステップ 2	Server /bios # **show detail**	使用可能なファームウェア イメージおよびステータスを表示します。
ステップ 3	Server /bios # **activate**	現在非アクティブになっているイメージをアクティブにします。
ステップ 4	プロンプトで **y** と入力し、選択したファームウェア イメージをアクティブ化します。	

例

次に、ファームウェアをアクティブにしてから、アクティベーションを確認する例を示します。

```
Server# scope bios
Server /bios # show detail
BIOS
    Version: C240M4.2.0.2.67.072320142231
    Backup BIOS Version: C240M4.2.0.2.66.071820142034
    Boot Order: (none)
    Boot Override Priority:
    FW Update/Recovery Status: None, OK
    UEFI Secure Boot: disabled
    Configured Boot Mode: None
    Actual Boot Mode: Legacy
    Last Configured Boot Order Source: BIOS

Server /bios # activate
```

```
This operation will activate "C240M4.2.0.2.66.071820142034" after next host power off
Continue?[y|N]

Server# scope bios
Server /bios # show detail
BIOS
    Version: C240M4.2.0.2.66.071820142034
    Backup BIOS Version: C240M4.2.0.2.67.072320142231
    Boot Order: (none)
    Boot Override Priority:
    FW Update/Recovery Status: None, OK
    UEFI Secure Boot: disabled
    Configured Boot Mode: None
    Actual Boot Mode: Legacy
    Last Configured Boot Order Source: BIOS
 Server /bios #
```

```
Server# scope bios
Server /bios # show detail
BIOS:
    BIOS Version: Cxxx.4.0.0.19.0528180450
    Backup BIOS Version: Cxxx.4.0.0.23.0612180433
    Boot Order: (none)
    FW Update Status: Done, OK
    UEFI Secure Boot: disabled
    Actual Boot Mode: Uefi
    Last Configured Boot Order Source: BIOS
    One time boot device: (none)
Server /bios # activateSystem is powered-on. This operation will activate backup BIOS
version
"C125.4.0.0.23.0612180433" during next boot.
Continue?[y|N]y
Server# scope bios
Server /bios # show detail
BIOS:
    BIOS Version: Cxx.4.0.0.19.0528180450
    Backup BIOS Version: Cxxx.4.0.0.23.0612180433
    Boot Order: (none)
    FW Update Status: Done, Activation pending
    UEFI Secure Boot: disabled
    Actual Boot Mode: Uefi
    Last Configured Boot Order Source: BIOS
    One time boot device: (none)
Server /bios #
```

保留中の BIOS アクティベーションのキャンセル

始める前に

BIOS ファームウェアが保留状態になければなりません。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope bios**	BIOS コマンド モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	Server /bios # **show detail**	使用可能なファームウェア イメージおよびステータスを表示します。
ステップ 3	Server /bios # **cancel-activate**	（注） BIOS ファームウェアが保留状態でなければなりません。 保留中の BIOS のアクティブ化をキャンセルします。
ステップ 4	プロンプトで、**y**を入力してアクティブ化をキャンセルします。	

例

この例では、保留中の BIOSファームウェアのアクティブ化をキャンセルします。

```
Server# scope bios
Server /bios # show detail
 BIOS:
    BIOS Version: Cxxx.4.0.0.19.0528180450
    Backup BIOS Version: Cxxx.4.0.0.23.0612180433
    Boot Order: (none)
    FW Update Status: Done, Activation pending
    UEFI Secure Boot: disabled
    Actual Boot Mode: Uefi
    Last Configured Boot Order Source: BIOS
    One time boot device: (none)
Server /bios # cancel-activate
This will cancel Pending BIOS activation[y|N]y
Server /bios # show detail
BIOS:
    BIOS Version: Cxxx.4.0.0.19.0528180450
    Backup BIOS Version: Cxxx.4.0.0.23.0612180433
    Boot Order: (none)
    FW Update Status: None, OK
    UEFI Secure Boot: disabled
    Actual Boot Mode: Uefi
    Last Configured Boot Order Source: BIOS
    One time boot device: (none)
Server /bios #
```

VIC ファームウェアのインストール

始める前に

- 管理者権限を持つユーザとしてログインします。

- フロント パネルの USB デバイスから VIC ファームウェアを更新する場合は、スマート USB オプションが有効で、有効な VIC ファームウェアが USB デバイスで利用可能であることを確認します。
- アップデートがすでに処理中であるときに新たにアップデートを開始すると、どちらのアップデートも失敗します。

手順

	コマンドまたはアクション	目的
ステップ 1	server # **scope chassis**	シャーシ コマンド モードを開始します
ステップ 2	server /chassis # **update-adapter-fw** ｐ プロトコル リモート サーバ アドレス 画像ファイル パス**activate|no-activate***PCI* スロット番号	VIC ファームウェアは、指定した IPv4 または IPv6 アドレス、あるいはホスト名のリモート サーバに、指定したパスとファイル名で保存されます。リモート サーバは次のいずれかのタイプになります。 • TFTP • FTP • SFTP • SCP • HTTP

	コマンドまたはアクション	目的
		（注） Cisco UCS C シリーズ サーバーでは、リモート サーバーからファームウェアを更新したときの、サーバーのフィンガープリントの確認をサポートするようになりました。このオプションは、リモート サーバのタイプとして SCP または SFTP を選択している場合のみ利用できます。 このアクションを実行する際にリモート サーバのタイプとして SCP または SFTP を選択すると、メッセージ「Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?」が表示されます。サーバのフィンガープリントの真偽に応じて、[y] または [n] をクリックします。 フィンガープリントはホストの公開キーに基づいており、接続先のホストを識別または確認できます。
ステップ 3	server/chassis # **update-adapter-fw usb** イメージファイル パス **activate|no-activate** *PCI* スロット番号	USB デバイスのイメージ ファイルのパス、VIC PCI スロット番号を指定します。
ステップ 4	（任意） server /cimc # **show adapter detail**	ファームウェア アップデートの進捗状況を表示します。

例

次に、VIC ファームウェアを更新する例を示します。

```
Server# scope chassis
Server /chassis # update-adapter-fw update ftp 10.10.10.10 cruzfw_new.bin activate MLOM
Adapter firmware update has started.
Please check the status using "show adapter detail".
You have chosen to automatically activate the new firmware
image.  Please restart your host after the update finish.
```

```
Server /chassis # show adapter detail
PCI Slot MLOM:
    Product Name: UCS VIC 1387
    Serial Number: FCH2102J8SU
    Product ID: UCSC-MLOM-C40Q-03
    Adapter Hardware Revision: 3
    Current FW Version: 4.1(3.143)
    VNTAG: Disabled
    FIP: Enabled
    LLDP: Enabled
    Configuration Pending: no
    Cisco IMC Management Enabled: yes
    VID: V03
    Vendor: Cisco Systems Inc
    Description:
    Bootloader Version: 4.1(2d)
    FW Image 1 Version: 4.1(3.143)
    FW Image 1 State: RUNNING ACTIVATED
    FW Image 2 Version: N/A
    FW Image 2 State: N/A
    FW Update Status: Update in progress
    FW Update Error: No error
    FW Update Stage: Erasing (12%)
    FW Update Overall Progress: 19%
Server /chassis #
```

リモートサーバからのCMCファームウェアのインストール

始める前に

- admin 権限を持つユーザとして Cisco IMC にログインします。
- Cisco.com から Cisco Host Upgrade UtilityISO ファイルを入手し、シスコからのファームウェアの取得 （3 ページ） の説明に従ってファームウェア インストール ファイルを抽出します。
- このアクションを使用できるのは一部の C シリーズ サーバだけです。

（注） アップデートがすでに処理中であるときにアップデートを開始すると、どちらのアップデートも失敗します。

手順

	コマンドまたはアクション	目的
ステップ 1	server # **scope chassis**	シャーシ コマンド モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	server /chassis # **scope cmc** *1|2*	選択した SIOC コントローラ コマンド モードの CMC を開始します。
ステップ 3	server /chassis/cmc # **update** プロトコル *IP* アドレス パス	プロトコル、リモート サーバーの IP アドレス、サーバー上のファームウェア ファイルへのファイル パスを指定します。プロトコルは次のいずれかになります。 • TFTP • FTP • SFTP • SCP • HTTP （注） Cisco UCS C シリーズ サーバーでは、リモート サーバーからファームウェアを更新したときの、サーバーのフィンガープリントの確認をサポートするようになりました。このオプションは、リモート サーバのタイプとして SCP または SFTP を選択している場合のみ利用できます。 このアクションを実行する際にリモート サーバのタイプとして SCP または SFTP を選択すると、メッセージ「Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?」が表示されます。サーバのフィンガープリントの真偽に応じて、[y] または [n] をクリックします。 フィンガープリントはホストの公開キーに基づいており、接続先のホストを識別または確認できます。

	コマンドまたはアクション	目的
ステップ 4	（任意） server /chassis/cmc # **show detail**	ファームウェア アップデートの進捗状況を表示します。

例

次に、CMC ファームウェアを更新する例を示します。

```
server # scope chassis
server /chassis # scope cmc 1
server /chassis/cmc # update  http 10.104.236.99 colusa_cmc.2.0.2a.img
CMC Firmware update initialized.
Please check the status using "show detail"
Server /chassis/cmc # show detail
Firmware Image Information:
    Name: CMC1
    Update Stage: DOWNLOAD
    Update Progress: 25
    Current FW Version: 2.0(2a)
    FW Image 1 Version: 2.0(2a)
    FW Image 1 State: RUNNING ACTIVATED
    FW Image 2 Version: 2.0(2a)
    FW Image 2 State: BACKUP INACTIVATED
server /chassis/cmc #
```

次のタスク

新しいファームウェアをアクティブにします。

インストールした CMC ファームウェアのアクティブ化

（注） CMC は 1 つをアクティブな状態にし、他はバックアップとして機能するように設定されています。バックアップ CMC をアクティブにすると、それまでアクティブだった CMC が、バックアップ CMC に変わり、もう一方がアクティブになります。

始める前に

CMC ファームウェアをサーバにインストールします。

重要 アクティブ化の進行中は、次のことを行わないでください。

- サーバのリセット、電源切断、シャットダウン。
- Cisco IMCCisco IMC のリブートまたはリセット。
- 他のすべてのファームウェアをアクティブ化します。
- テクニカル サポート データまたは設定データをエクスポートします。

- CMC-1 アクティベーションによって Cisco IMC ネットワーク接続が中断されます。

手順

	コマンドまたはアクション	目的
ステップ 1	server # **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server # **scope cmc***1*|*2*	選択した SIOC スロット コマンド モードの CMC を開始します。
ステップ 3	Server /cmc # **activate**	選択した CMC に対して選択したイメージをアクティブにします。
ステップ 4	プロンプトで **y** と入力し、選択したファームウェア イメージをアクティブ化します。	CMC-1 がリブートし、そのリブートが完了するまではすべての CLI セッションと GUI セッションが終了しますが、CMC-2 リブートがアクティブなセッションに影響を与えることはありません。

例

次に、SIOC スロット 1 上の CMC ファームウェアをアクティブにする例を示します。

```
Server # scope chassis
Server /chassis # scope cmc 1
Server /chassis/cmc #  activate
Warning: The CMC will be rebooted immediately to complete the activation.
The network may go down temporarily till CMC boots up again
Continue?[y|N]y
```

リモート サーバからの SAS エクスパンダ ファームウェアのインストール

始める前に

- このアクションを実行するには、admin としてログオンする必要があります。
- サーバの電源をオンにする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **scope sas-expander {1 | 2}**	SAS エクスパンダ コマンド モードを開始します。
ステップ 3	Server /chassis/sas-expander # **show detail**	使用可能なファームウェア イメージおよびステータスを表示します。
ステップ 4	Server /chassis/sas-expander # **update** *protocol IP_Address path*	次の情報を指定します。 • プロトコル。TFTP、FTP、SFTP、SCP、または HTTP が使用できます。

	コマンドまたはアクション	目的
		（注） Cisco UCS C シリーズ サーバーでは、リモート サーバーからファームウェアを更新したときの、サーバーのフィンガープリントの確認をサポートするようになりました。このオプションは、リモート サーバのタイプとして SCP または SFTP を選択している場合のみ利用できます。 このアクションを実行する際にリモート サーバのタイプとして SCP または SFTP を選択すると、メッセージ「Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?」が表示されます。サーバのフィンガープリントの真偽に応じて、[y] または [n] をクリックします。 フィンガープリントはホストの公開キーに基づいており、接続先のホストを識別または確認できます。 • リモート サーバの IPv4 アドレスまたは IPv6 アドレス、あるいはホスト名。 • リモート サーバ上の SAS エクスパンダ ファームウェア ファイルへのファイル パス。

例

次に、SAS エクスパンダ ファームウェアをアップデートする例を示します。

```
Server# scope chassis
Server /chassis # scope sas-expander 1
Server /chassis/sas-expander # show detail
Firmware Image Information:
    ID: 1
    Name: SASEXP1
    Update Stage: NONE
    Update Progress: 0
    Current FW Version: 65103900
    FW Image 1 Version: 65103900
    FW Image 1 State: RUNNING ACTIVATED
    FW Image 2 Version: 65103900
    FW Image 2 State: BACKUP INACTIVATED
Server /chassis/sas-expander # update ftp 192.0.20.34
//upgrade_sas_expander_files/sas-expander-2-0-12a.fw
 <CR>  Press Enter key
Firmware update has started.
Please check the status using "show detail"
Server /chassis/sas-expander #
```

インストール済みSASエクスパンダ ファームウェアの有効化

始める前に

- このアクションを実行するには、admin としてログオンする必要があります。
- ファームウェアをエクスパンダにインストールします。
- ホストの電源をオンにする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **scope sas-expander {1 | 2}**	SAS エクスパンダ コマンド モードを開始します。
ステップ 3	Server /chassis/sas-expander # **activate**	現在非アクティブになっているイメージをアクティブにします。

	コマンドまたはアクション	目的
ステップ 4	プロンプトで **y** と入力し、選択したファームウェア イメージをアクティブ化します。	

例

次に、ファームウェアをアクティブにしてから、アクティベーションを確認する例を示します。

```
Server# scope chassis
Server /chassis # scope sas-expander 1
Server /chassis/sas-expander # show detail
 ID: 1
    Name: SASEXP1
    Update Stage: NONE
    Update Progress: 0
    Current FW Version: 65103900
    FW Image 1 Version: 65103900
    FW Image 1 State: RUNNING INACTIVATED
    FW Image 2 Version: 65103900
    FW Image 2 State: BACKUP INACTIVATED

Server /chassis/sas-expander # activate
This operation will activate "65103900" after next host power off
Continue?[y|N] y

Server /chassis/sas-expander # show detail
ID: 1
    Name: SASEXP1
    Update Stage: NONE
    Update Progress: 0
    Current FW Version: 65103900
    FW Image 1 Version: 65103900
    FW Image 1 State: RUNNING ACTIVATED
    FW Image 2 Version: 65103900
    FW Image 2 State: BACKUP INACTIVATED
Server /chassis/sas-expander #
```

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。