ファームウェア管理

CIMC ファームウェアの概要

UCS E シリーズ M6 サーバーは、使用しているサーバーモデルに固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ー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。

潜在的な問題を回避するには、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、CIMC、BIOS、およびその他のファームウェア コンポーネントを互換性のあるレベルにアップグレードします。

（注） 一致する CIMC ファームウェアをアクティブ化するまでは、新しい BIOS ファームウェアをインストールしないでください。インストールすると、サーバーがブートしなくなります。

CIMC 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、サーバー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、CIMC は、選択した CIMC ファームウェアをサーバーの非アクティブまたはバックアップ 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、CIMC は非アクティブ ファームウェア バージョンをアクティブとして設定してサーバーをリブートします。これにより、サービスが中断さ

れます。サーバーをリブートすると、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。

CIMC 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。サーバーは、BIOS アップデートプロセス全体を通して、電源をオフにする必要があります。CIMC がリブートを完了すると、サーバー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。

ファームウェアのアップグレードのオプション

Cisco Host Upgrade Utility（HUU）を使用して、ファームウェア コンポーネントをアップグレードできます。

HUU：すべてのファームウェア コンポーネントのアップグレードにCIMC、BIOSおよびFPGAファームウェアを含むHUU ISO ファイルを使用することを推奨します。 HUU ISO パッケージを使用してすべての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。

（注） 最新バージョンの CIMC または BIOS ファームウェアを古いバージョンの他のファームウェアとともに使用すると、予期しない動作が発生する可能性があります。

シスコからのソフトウェアの取得

BIOS および CIMC ファームウェアをダウンロードするには、次の手順を使用します。

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。

ロールダウン メニューが表示されます。

ステップ 4 [Downloads]（中央）ペインから、[All Downloads]（右下隅）をクリックします。

[Download Software] ページが表示されます。

ステップ 5 左ペインから、[Products] をクリックします。

ステップ 6 中央ペインから、[Unified Computing and Servers] をクリックします。

ステップ 7 右ペインから、[Cisco UCS E-Series Software] をクリックします。

ステップ 8 右ペインから、ダウンロードするソフトウェアのサーバー モデルの名前をクリックします。

[Download Software] ページは次のカテゴリで表示されます。

- [Unified Computing System (UCSE) Server Firmware]：ホスト アップグレード ユーティリティが含まれています。

ステップ 9 適切なソフトウェア カテゴリ リンクをクリックします。

ステップ 10 ダウンロードするソフトウェア イメージに関連付けられている [Download] ボタンをクリックします。

[End User License Agreement] ダイアログボックスが表示されます。

ステップ 11 （任意）複数のソフトウェア イメージをダウンロードするには、次を実行します。

a) ダウンロードするソフトウェア イメージに関連付けられている [Add to cart] ボタンをクリックします。

b) 右上にある [Download Cart] ボタンをクリックします。

カートに追加したすべてのイメージが表示されます。

c) 右下隅にある [Download All] をクリックして、すべてのイメージをダウンロードします。

[End User License Agreement] ダイアログボックスが表示されます。

ステップ 12 [Accept License Agreement] をクリックします。

ステップ 13 必要に応じて、次のいずれかを実行します。

- ソフトウェア イメージ ファイルをローカル ドライブに保存します。
- ソフトウェア イメージを TFTP サーバーからインストールする場合は、使用する TFTP サーバーにファイルをコピーします。

サーバーは、TFTP サーバー上の宛先フォルダに対する読み取り権限を持っていることが必要です。

次のタスク

ソフトウェア イメージをインストールします。

リモート サーバーからの CIMC ファームウェアのインストール

潜在的な問題を回避するには、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、CIMC、BIOS、およびその他のファームウェア コンポーネントを互換性のあるレベルにアップグレードします。

（注） 一致する CIMC ファームウェアをアクティブ化するまでは、新しい BIOS ファームウェアをインストールしないでください。インストールすると、サーバーがブートしなくなります。

始める前に

- admin 権限を持つユーザーとして CIMC にログインします。
- シスコから CIMC ファームウェア ファイルを取得します。

（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。

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**	CIMC 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** *protocol ip-address path*	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**
ステップ 4	Server /cimc # **show detail**	（任意）BIOS 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、ファームウェアをアップデートする例を示します。

```
Server# scope cimc
Server /cimc # scope firmware
Server /cimc/firmware # update tftp 10.20.34.56 test/dnld-ucs-k9-bundle.1.0.2h.bin
```

```
<CR> Press Enter key Firmware update has started.

Please check the status using "show detail"

Server /cimc #
```

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ー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。

（注） アップデートの処理中にアクティブ化を開始すると、アクティブ化に失敗します。

手順

	コマンドまたはアクション	目的
ステップ 1	Server # **scope cimc**	CIMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scope firmware**	CIMC 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 # **activate**	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、サーバーは現在非アクティブのイメージをアクティブにします。

例

この例では、ファームウェアイメージをアクティブ化します。

```
Server /cimc/firmware # show detail
Firmware Image Information:
    Update Stage: NONE
    Update Progress: 0%
    Current FW Version: 4.11(0)73
    FW Image 1 Version: 4.1-suthandy-030223-111138
    FW Image 1 State: BACKUP INACTIVATED
    FW Image 2 Version: 4.11(0)73
    FW Image 2 State: RUNNING ACTIVATED
    Boot-loader Version: 4.11(0)73
    Secure Boot: ENABLED

Server /cimc #
Server /cimc # activate
```

パスワードの保存形式の変更

この手順では、パスワードストレージの形式を変更する方法について説明します。

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 # **change-password-storage**	パスワードストレージの形式を変更します。形式を変更する前にプロンプトが表示されます。

例

次に、形式を変更する例を示します。

```
Server# scope cimc
Server /cimc # change-password-storage

This operation will change the user password storage form to be SHA512 with salt.
Note that, once you start this operation:
1. You cannot change the password storage format back.
2. The IPMI over LAN feature will stop working.
3. You need to change the passwords of all local users to have them stored in the new
format.
Are you sure you want to continue?[y|N]

Press Y to change the format.
```

TFTP サーバーからの BIOS ファームウェアのインストール

潜在的な問題を回避するには、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ーは、CIMC、BIOS、およびその他のファームウェア コンポーネントを互換性のあるレベルにアップグレードします。

HUU を使用する代わりに CIMC および BIOS ファームウェアを手動でアップグレードする場合、まず CIMC ファームウェアを更新してから、BIOS ファームウェアを更新します。一致する CIMC ファームウェアをアクティブ化するまでは、新しい BIOS ファームウェアをインストールしないでください。インストールすると、サーバーがブートしなくなります。

（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。

（注） BIOS ファームウェアを更新する前に、サーバーの電源を切り、モジュールをメンテナンスモードにします。

始める前に

シスコから CIMC ファームウェア ファイルを取得します。

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 # **update protocol** *ip-address path-and-filename*	BIOS ファームウェアのアップデートを開始します。サーバーは、指定の IP アドレスにある TFTP サーバーから、指定のパスとファイル名のアップデート ファームウェアを取得します。
ステップ 3	Server /bios # **show detail**	（オプション）BIOS ファームウェアアップデートの進捗状況を表示します。
ステップ 4	Server /bios # **activate**	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化します。

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 # update 10.20.34.56 //test/dnld-ucs-k9-bundle.1.0.2h.bin
<CR> Press Enter key
Firmware update has started.
Please check the status using "show detail"
Server /bios #
```

UCS E シリーズ M6 サーバーアクセス問題のトラブルシューティング

E シリーズ M6 サーバーへのアクセスに問題がある場合は、CIMC ファームウェアイメージが破損しているか、ファイルシステムが破損しているか、CIMC ファームウェアのインストールが正常に完了しなかった可能性があります。必要に応じて、次のいずれかを実行します。

- CIMC ファームウェア イメージが破損している場合は、破損した CIMC ファームウェア イメージからの回復 （8 ページ）を参照してください。
- ファイル システムが破損している場合は、破損ファイル システムの回復 （10 ページ）を参照してください。
- CIMC ファームウェアのインストールが正常に終了しなかった場合は、CIMC ファームウェアを再インストールします。

重要 セキュリティ上の観点から、**boot backup** コマンドはディセーブルです。

破損した CIMC ファームウェア イメージからの回復

始める前に

- サーバを PC に接続します。シリアルケーブルの一端を E シリーズ サーバーのシリアル ポートに接続し、もう一端を PC に接続します。
- ユーザが指定したインターフェイス オプションに応じて、次のいずれかを実行します。
  - 専用：イーサネットケーブルを E シリーズ M6 サーバーの管理（専用）ポートに接続します。
  - Shared-Lom-GE2：イーサネットケーブルを E シリーズ M6 サーバーの外部 GE2 インターフェイスに接続します。

- Shared-Lom-Console：Cisco IOS CLI を使用して、E シリーズ M6 サーバーの内部コンソールインターフェイスを設定します。

- シリアル出力を表示するには、Minicom を起動します。
- 通信設定は、9600 ボー、8 ビット、パリティなし、および 1 ストップ ビットに設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	Router # **hw-module subslot** *slot* **stop**	指定した E シリーズ M6 サーバーへの電源をシャットダウンします。
ステップ 2	Router # **hw-module subslot** *slot* **start**	指定した E シリーズ M6 サーバーの電源を再起動します。
ステップ 3	***	Minicom から、*** コマンドを入力してブートローダプロンプトを入力します。
ステップ 4	ucse-cimc > boot current recovery	現在のイメージから E シリーズ M6 サーバーをブートします。
ステップ 5	Recovery-shell # **interface** [**dedicated** | **shared-lom-console** | **shared-lom-ge1** | **shared-lom-ge2** | **shared-lom-ge3**] *interface-ip-address* **netmask** *gateway-ip-address*	指定したインターフェイスの IP アドレス、サブネットマスク、ゲートウェイ IP アドレスを指定します。
ステップ 6	Recovery-shell # **ping** *tftp-ip-address*	CIMC ファームウェアが保存されているリモートの TFTP サーバーに ping を送信し、ネットワーク接続を確認します。
ステップ 7	Recovery-shell # **update** *tftp-ip-address image-filename*	CIMC ファームウェアイメージをインストールします。このイメージはリモートの TFTP サーバーに保存されています。
ステップ 8	Recovery-shell # **reboot**	CIMC をリブートします。

例

この例では、E シリーズ M6 サーバーの CIMC ファームウェアイメージを回復します。

```
Router# hw-module subslot 2/0 stop
Router# hw-module subslot 2/0 start

***

ucse-cimc > boot current recovery
recovery-shell# interface shared-lom-ge2 192.168.0.138 255.255.255.0 192.168.0.1
Network configuration:
```

```
IP config: addr: 192.168.0.138 Mask: 255.255.255.0
Gateway: 192.168.0.1
recovery-shell# ping 10.20.34.56
PING 10.20.34.56 (10.20.34.56): 56 data bytes
64 bytes from 10.20.34.56: seq=0 ttl=60 time=10.000 ms
64 bytes from 10.20.34.56: seq=1 ttl=60 time=0.000 ms
--- 10.20.34.56 ping statistics ---
10 packets transmitted, 10 packets received, 0% packet loss round-trip min/avg/max =
0.000/1.000/10.000 ms
recovery-shell# update 10.20.34.56 update_pkg-cimc.combined.bin
downloading firmware image "update_pkg-cimc.combined.bin" from " 10.20.34.56 "
download firmware image done, size in bytes: 22384144
installing firmware image, please wait ... activating installed image
done
Stage: NONE
Status: SUCCESS

Error: Success
recovery-shell# reboot
```

破損ファイル システムの回復

この手順は、CIMC ブート ログ ファイルに次のエラー メッセージが表示された場合に使用します。

```
UNEXPECTED INCONSISTENCY; RUN fsck MANUALLY
```

始める前に

- サーバを PC に接続します。シリアルケーブルの一端を E シリーズ サーバーのシリアル ポートに接続し、もう一端を PC に接続します。
- ユーザが指定したインターフェイス オプションに応じて、次のいずれかを実行します。
  - 専用：イーサネットケーブルを E シリーズ M6 サーバーの管理（専用）ポートに接続します。
  - Shared-Lom-GE2：イーサネットケーブルを E シリーズ M6 サーバーの外部 GE2 インターフェイスに接続します。
  - Shared-Lom-Console：Cisco IOS CLI を使用して、E シリーズ M6 サーバーの内部コンソールインターフェイスを設定します。
- シリアル出力を表示するには、Minicom を起動します。
- 通信設定は、9600 ボー、8 ビット、パリティなし、および 1 ストップ ビットに設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	Router # **hw-module subslot** *slot* **stop**	指定した E シリーズ M6 サーバーへの電源をシャットダウンします。

	コマンドまたはアクション	目的
ステップ 2	Router # **hw-module subslot** *slot* **start**	指定したEシリーズM6サーバーの電源を再起動します。
ステップ 3	***	Minicomから、*** コマンドを入力してブートローダプロンプトを入力します。
ステップ 4	ucse-cimc > boot current recovery	現在のイメージからEシリーズM6サーバーをブートします。
ステップ 5	Recovery-shell # **fs-check** [**p3** | **p4**]	特定のパーティションのファイルシステムをチェックし、破損したファイルシステムを復元します。 （注） このコマンドでは、p3 および p4 パーティションだけを使用できます。このコマンドは破損したパーティションで使用します。破損したパーティションは、CIMC ブート アップ時に**run fsk** エラーメッセージを表示するパーティションです。 • コマンド出力に **clean** が表示される場合は、破損したファイルが回復されていることを示します。**reboot** コマンドを入力して、CIMC を再起動します。以降の手順を省略します。 • コマンド出力に **clean** が表示されない場合は、ステップ 6 に進みます。
ステップ 6	Recovery-shell # **reboot**	（任意）破損したファイルシステムが **fs-check [p3 | p4]** コマンドによって復元されず、出力に **clean** が表示されない場合は、**reboot** コマンドを入力してパーティションをフォーマットします。 以降の手順を省略します。 （注） p3 パーティションをフォーマットすると、CIMC 設定は失われます。
ステップ 7	Recovery-shell # **interface** [**dedicated** | **shared-lom-console** | **shared-lom-ge1** | **shared-lom-ge2** | **shared-lom-ge3**] *interface-ip-address* **netmask** *gateway-ip-address*	指定したインターフェイスのIPアドレス、サブネットマスク、ゲートウェイIPアドレスを指定します。
ステップ 8	Recovery-shell # **ping** *tftp-ip-address*	CIMCファームウェアが保存されているリモートのTFTPサーバーにpingを送信し、ネットワーク接続を確認します。

	コマンドまたはアクション	目的
ステップ 9	Recovery-shell # **update** *tftp-ip-address image-filename*	CIMC ファームウェアイメージをインストールします。このイメージはリモートの TFTP サーバーに保存されています。
ステップ 10	Recovery-shell # **reboot**	CIMC をリブートします。

例

この例は、E シリーズ M6 サーバーで **fs-check p3** コマンドを使用して、現在のイメージから CIMC ファームウェアを回復します。

```
Router# hw-module subslot 1/0 stop
Router# hw-module subslot 1/0 start

***

ucse-cimc > boot current recovery
recovery-shell# fs-check p3
e2fsck 1.41.14 (22-Dec-2010)
/dev/mmcblk0p3: recovering journal
/dev/mmcblk0p3: clean, 429/7840 files, 3331/31296 blocks
recovery-shell# fs-check p4
e2fsck 1.41.14 (22-Dec-2010)
/dev/mmcblk0p4: clean, 51/506912 files, 1880262/2025296 blocks
recovery-shell# reboot
```

Recovery Shell コマンド

Recovery Shell コマンド	**Description**
Recovery-shell # **dedicated-interface** *interface-ip-address netmask gateway-ip-address*	専用インターフェイスの IP アドレス、サブネットマスク、ゲートウェイ IP アドレスを指定します。
Recovery-shell # **dedicated-interface (DEPRECATED)**	専用ポートの現在の設定を表示します。
Recovery-shell # **interface [dedicated | shared-lom-console | shared-lom-ge1 | shared-lom-ge2 | shared-lom-ge3]** *interface-ip-address netmask gateway-ip-address*	指定したインターフェイスの IP アドレス、サブネットマスク、ゲートウェイ IP アドレスを指定します。
Recovery-shell # **interface**	インターフェイスの設定を表示します。
Recovery-shell # **ping** *tftp-ip-address*	CIMC ファームウェアが保存されているリモートの TFTP サーバーに ping を送信し、ネットワーク接続を確認します。

Recovery-shell # **update** *tftp-ip-address image-filename*	CIMC ファームウェアイメージをインストールします。このイメージはリモートの TFTP サーバーに保存されています。
Recovery-shell # **fs-check [p3 | p4]**	特定のパーティションのファイル システムをチェックし、破損したファイル システムを復元します。
Recovery-shell # **active image**	CIMC が実行されている現在のアクティブなイメージを表示します（イメージ 1 またはイメージ 2）。
Recovery-shell # **active image [1 | 2]**	アクティブなイメージを 1 または 2 に変更します。指定したイメージがすでにアクティブになっている場合は、メッセージが表示されます。それ以外の場合は、指定したイメージがアクティブになります。 active image コマンドを使用した後は、**reboot** コマンドを使用して、新たに設定したイメージを有効にします。
Recovery-shell # **reboot**	CIMC ファームウェアをリブートします。

パスワードの復旧

始める前に

- サーバを PC に接続します。シリアルケーブルの一端を E シリーズ サーバーのシリアル ポートに接続し、もう一端を PC に接続します。
- ユーザが指定したインターフェイス オプションに応じて、次のいずれかを実行します。
  - 専用：イーサネットケーブルを E シリーズ M6 サーバーの管理（専用）ポートに接続します。
  - Shared-Lom-GE2：イーサネットケーブルを E シリーズ M6 サーバーの外部 GE2 インターフェイスに接続します。
  - Shared-Lom-Console：Cisco IOS CLI を使用して、E シリーズ M6 サーバーの内部コンソール インターフェイスを設定します。
- シリアル出力を表示するには、Minicom を起動します。
- 通信設定は、9600 ボー、8 ビット、パリティなし、および 1 ストップ ビットに設定します。

ステップ 1 Router # **hw-module subslot** *1/0* **oir power-cycle**

E シリーズ M6 サーバーの電源が再投入されます。

ステップ 2 「***」と入力して Autoboot: 0 を停止します

プロンプトの後に「****」と入力します。

ステップ 3 ucse-cimc > **boot current recovery**

boot current recovery と入力して、リカバリモードで起動します。

ステップ 4 Recovery-shell #

```
Recovery-shell は、メニュー方式の限定機能インターフェイスです。

主なオプション：

1. configure interface
   2. show interfaces
   3. ping
   4. cimc image options
   5. emmc options
   6. admin password reset
   7. enter debug shell
   8. exit and reboot
```

ステップ 5 Recovery-shell（選択内容を入力）# **emmc format p3**

パスワードを含む設定をクリアする EMMC カードの p3 パーティションをフォーマットします。

（注） EMMC をパーティション分割すると、CIMC 設定、ISO ファイル、パスワードなどの EMMC カードの内容が失われるか、クリアされます。

```
ACT2 リセットが完了しました。システムを再起動し、デフォルトのパスワードでログインしてください。Recovery-shell は、
メニュー方式の限定機能インターフェイスのメインオプションです：

1. configure interface
  2. show interfaces
  3. ping
  4. cimc image options
  5. emmc options
  6. admin password reset
  7. enter debug shell
  8. exit and reboot
```

ステップ 6 Recovery-shell（選択内容を入力）# **8**

8 を押して終了し、デバイスを再起動します。

例

この例では、CMIC パスワードを覚えていない場合にパスワードを回復します。

```
server # login: admin
Password:
****************WARNING!*****************
```

```
Default credentials were used for login.
   Administrator password needs to be
     changed for security purposes.
**************************************
Enter current password: password
Please change the password...
Enter new password: <strong-password>
Re-enter new password: <strong-password>
Updating password...
Password updated successfully.
```

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。