Cisco UCS C シリーズ サーバのファームウェアの更新

この章では、次の事項について説明します。

HUU を使用した Cisco UCS C シリーズ サーバのファームウェアの更新

重要 Cisco IMC ファームウェアをアップグレードしたら、互換性マトリクスをチェックして、アップグレードされたバージョンの Cisco IMC にドライバが準拠しているかどうか確認する必要があります。ドライバのバージョンが準拠していない場合、Cisco IMC のバージョンに一致するようにドライバのバージョンをアップグレードする必要があります。

「ハードウェアとソフトウェアの相互互換性マトリックス」については次を参照してください。

http://www.cisco.com/en/US/products/ps10477/prod_technical_reference_list.html

HUU ISO を使用すると、書き込み可能なディスク（DVD または CD）によりホストからローカルで、または HUU ISO を仮想デバイスとしてマウントすることによりリモートで、サーバのコンポーネントをアップグレードできます。次の手順では、HUU を使用してファームウェアをアップグレードする方法について説明します。

アップグレードのための ISO のダウンロードと準備

ステップ 1 HUU ISO ファイルをダウンロードします。

a) http://www.cisco.com/cisco/software/navigator.html にアクセスします。

b) 中央のカラムで、[Servers – Unified Computing] をクリックします。
c) 右側のカラムで、[Cisco UCS C-Series Rack-Mount Standalone Server Software] をクリックします。
d) 右側のカラムでサーバのモデル名を選択します。
e) [Unified Computing System (UCS)Server Firmware] をクリックします。
f) リリース番号を選択します。
g) [Download] をクリックして、ucs-*server platform*-huu-*version_number*.iso ファイルをダウンロードします。
h) ログイン画面で資格情報を入力します。
i) 次の画面に進んでライセンス契約に同意し、このファイルを保存する場所を参照します。
j) [Download] をクリックします。
ISO バンドルは選択した場所にダウンロードされます。

ステップ 2 ローカル アップグレード用に ISO を準備する場合は、このステップを完了するか、**ステップ 3** に進みます。

a) 書き込み可能なディスク（CD）に ISO イメージを書き込みます。
b) VGA モニタと USB キーボードを Cisco C シリーズ サーバに接続します。
c) ディスクを Cisco C シリーズ サーバの USB DVD ドライブに挿入します。
d) アップグレードするファームウェア コンポーネントに応じて、次のいずれかのファームウェア更新手順を実行します。

ステップ 3 **KVM コンソール**を使用してリモート アップグレードのために ISO を準備します。

a) ブラウザを使用して、アップグレードするサーバ上の Cisco IMC GUI ソフトウェアに接続します。
b) ブラウザのアドレス フィールドにサーバの Cisco IMC IP アドレスを入力し、次にユーザ名とパスワードを入力します。
c) ツールバー上の**[Launch KVM Console]** をクリックして、 **KVM コンソール** を起動します。

（注） HUU を起動するサーバ ノードを選択します。

d) **KVM コンソール**で、[Virtual Media] をクリックします。
e) [Add Image] をクリックし、ucs-*server-name*-huu-*version_number*.iso ファイルをクリックします。
f) [Client View] 領域の [Mapped] カラムで、追加する ISO ファイルのチェックボックスをオンにし、マッピングが完了するまで待機します。
g) ISO ファイルがマッピングされたリモート デバイスとして表示されたら、アップグレードするファームウェア コンポーネントに応じて次のいずれかの手順を実行します。

[Update All] オプションを使用したファームウェアの更新

ステップ 1 サーバを起動し、[Boot Menu] 画面を開くよう求められたら、F6 を押します。
ステップ 2 [Boot Menu] 画面で、準備された ISO を選択します。

- ローカル アップグレードの場合は、物理または外部接続された CD/DVD デバイスを選択してから、[Enter] を押します。
- リモート アップグレードの場合は、[Cisco vKVM-Mapped vDVD1.22] を選択し、[Enter] を押します。

選択したデバイスからサーバがブートします。

ステップ 3 HUU をブートすると、[Cisco End User License Agreement（EULA）] が表示されるので、EULA を読み、

- [I Agree] をクリックしてライセンス契約書に同意し、更新を進めます。
- キャンセルする場合は [I Disagree] をクリックします。

（注） [I Disagree] を選択すると、アップグレードがキャンセルされ、ホストが再起動されます。

EULA に同意すると、[Cisco Host Upgrade Utility] ウィンドウが表示され、更新が利用可能なすべてのコンポーネントのリストが表示されます。

ステップ 4 リストされたすべてのコンポーネントを更新する場合は、[Update all] をクリックします。

- [Enabling Cisco IMC Secure Boot] 確認ダイアログボックスが表示されます。

（注） セキュア ブートがまだ有効になってない場合に限り、M3 サーバに対してのみこのメッセージが表示されます。

ステップ 5 確認ボックスの内容を注意深く読み、先に進んでファームウェアを更新し Cisco IMC セキュア ブートをイネーブルにする場合は、[Yes] をクリックします。

（注）
- バージョン 2.0(x) 以前から 2.0(x) に更新する場合、[Yes] をクリックすると、Cisco IMC のアクティブなバージョンとバックアップ バージョンの両方が 2.0(x) に更新されます。
- 更新中に KVM 接続が切断されるため、更新の進行状況を表示するには再接続する必要があります。

Cisco IMC セキュア ブートの詳細については、Cisco UCS C シリーズ サーバの統合管理コントローラ GUI の構成ガイド、リリース 2.0(1)『*Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide, Release 2.0(1)*』の「**Introduction to Cisco IMC Secure Boot**」の項を参照してください。

ステップ 6 サーバを再起動してファームウェアの変更を適用します。

特定のコンポーネントのファームウェア更新

次の手順では、個々のコンポーネントのファームウェア更新方法について説明します。

ステップ 1 リストの特定のコンポーネントを更新する場合は、更新するコンポーネントを選択します。

セキュアなアダプタの更新ファームウェアをダウングレードする場合は、後続のステップ **2** から **4** を実行します。または、ステップ **5** に進みます。

ステップ 2 セキュアなアダプタの更新ファームウェアをダウングレードするには、HUU をマッピングして HUU からの起動を可能にします。

ステップ 3 仮想 **KVM コンソール**で、HUU 起動時に「Loading firmware tools」メッセージが表示されるのを待ちます。

ステップ 4 「Loading firmware tools」メッセージが表示されたら、[enable-security-version-check] を無効にします。

a) Cisco IMC のコマンドライン インターフェイスから、**scope cimc->scope adapter-secure-update->enable-security-version-check yes/no/status** コマンドを実行します。

b) Cisco IMC Web UI から、[Utilities] タブにログインします。

c) XML API から次のデータを入力します。

要求:

```
<configConfMo cookie='1458615470/be0d9210-2e9a-1e9a-8004-816d1e1b0ff4'
 inHierarchical='false' dn='sys/rack-unit-1'>
  <inConfig>
    <computeRackUnit dn='sys/rack-unit-1' adaptorSecureUpdate='Disabled'/>
  </inConfig>
</configConfMo><IP>/nuova
```

応答：

```
<configConfMo dn="sys/rack-unit-1" cookie="1474315600/b51b2682-3ce2-1ce2-8038-c4ae729d8b18"
 response="yes">
 <outConfig>
  <computeRackUnit dn="sys/rack-unit-1" adminPower="policy" availableMemory="196608"
   model="UCSC-C240-M4L" memorySpeed="1866" name="UCS C240 M4L" numOfAdaptors="1"
   numOfCores="12" numOfCoresEnabled="12" numOfCpus="2" numOfEthHostIfs="2" numOfFcHostIfs="2"

   numOfThreads="24" operPower="on" originalUuid="0CA8BC15-2499-46F2-BFFE-686B224AB52E"
   presence="equipped" serverId="1" serial="FCH1927V0FC" totalMemory="196608" usrLbl=""
   uuid="0CA8BC15-2499-46F2-BFFE-686B224AB52E" vendor="Cisco Systems Inc"
   cimcResetReason="ac-cycle" adaptorSecureUpdate="Disabled" status="modified" >
    </computeRackUnit>
 </outConfig>
</configConfMo>
```

ステップ 5 [Update] をクリックして、更新プロセスに戻ります。

（注）
- あるコンポーネントのファームウェアを特に更新する場合を除き、[Update all] オプションを使用してすべてのコンポーネントのファームウェアを更新することを推奨します。
- 3 つのコンポーネント（BMC、BIOS、または CMC）のいずれかのファームウェアを更新する場合は、他の 2 つのコンポーネントのファームウェアも更新することをお勧めします。
- BMC ファームウェアを更新する場合は、[Exit] をクリックしてから [OK] をクリックして BMC ファームウェアをアクティブにします。
- BMC と他のコンポーネントを一緒に更新することを選択し、BIOS を選択していない場合は、終了時に**シャーシ ファームウェア**を更新するよう求めるプロンプトが表示されるので、確認ダイアログボックスで [Yes] をクリックしてシャーシ ファームウェアを更新します。

重要 S3260 サーバでは、[Update] または [Update all] をクリックして CMC1 と CMC2 のシャーシ コンポーネントを同時に更新すると、2 番目のコンポーネントの更新によるサーバ コンポーネントのトリガーがスキップされ、以降のコンポーネントが更新されます。

これにより更新が開始され、更新のステータスが [Update Status] カラムに表示されます。また、ファームウェアの更新中は、関連する一連のアクティビティとステータスの詳細なログが [Execution Logs] セクションに表示されます。

ステップ 6 HUU を終了する場合は、[Exit] をクリックします。

（注） [Exit] をクリックしたら、サーバの電源が自動的に投入されて更新の完了が示され、新しいファームウェアが有効化されるまで、数分間待機する必要があります。

（注） BMC を更新し、BIOS は更新していない場合は、[Exit] をクリックすると BMC がアクティブになり、BMC と KVM への接続が切断されます。

HDD ファームウェアの更新

次の手順では、HDD ファームウェアの更新手順を示します。

ステップ 1 サーバのハードディスクのファームウェアを更新する場合は、[Update HDD Firmware] をクリックします。ウィンドウに新しいファームウェアをサポートするサーバのハードディスク ドライブのリストが表示されます。ファームウェアのアップグレードをサポートしていないハードディスク ドライブは表示されません。

重要 ハードディスク ドライブのファームウェアを更新すると、データ損失が発生する可能性があります。ファームウェアを更新する前に完全なシステム バックアップを作成することをお勧めします。

a) すべてのハードディスクのファームウェアを更新するには、[Update All] をクリックします。

このオプションでは、最新のファームウェアがインストールされた HDD は更新されません。

b) 特定の HDD を更新するには、HDD を選択し、[Update] をクリックします。

ステップ 2 サーバを再起動してファームウェアの変更を適用します。

更新ステータスの確認とログの保存

次の手順では、最後の更新を確認し、ログを保存する手順を示します。

ステップ 1 ファームウェアを更新したら、サーバを起動して HUU ISO に戻し、[Last Update Verify] をクリックします。

このアクションは、各コンポーネントで、以前 HUU を使用して更新されたファームウェアのバージョンと、コンポーネントのファームウェアの現在のバージョンを比較し、更新のステータスを表示します。

ステップ 2 更新ステータスのログ ファイルを後で使用できるように保存する場合は、[Save Logs] をクリックします。

更新の詳細なステータスを含むログ ファイルは、サーバに物理的または KVM vMedia 経由で接続されている外部 USB デバイスに保存されます。

（注） ファームウェアの更新中にエラーが発生すると、エラー ログを保存するよう求められます。接続された外部 USB にログを保存する場合は、[Save Logs] をクリックします。このログは、エラーの原因の特定とトラブルシューティングに使用できます。