BIOS 保護

BIOS 保護

BIOS 保護機能によって、ゴールデン ROMMON イメージに対する書き込み保護が提供され、そのイメージへのアップグレードが安全に行われるようになります。

BIOS 保護機能がないと、ソフトウェアアップグレード時に悪意のあるコードによってゴールデン ROMMON が破損する可能性があります。

プライマリ ROMMON とゴールデン ROMMON

ROMMON イメージは、プライマリ ROMMON およびゴールデン ROMMON の両方として SPI フラッシュデバイスに格納されます。

プライマリ ROMMON は、デバイスの電源がオンになるか再起動されるたびに、デバイスをブートするために使用されます。プライマリ ROMMON が破損した場合、デバイスはゴールデン ROMMON を使用して IOS XE ソフトウェアイメージをブートします。

デバイスがプライマリ ROMMON からブートした場合、ゴールデン ROMMON はロックされたままです。

BIOS 保護機能が有効になっていると、ゴールデン ROMMON は書き込み保護されるため、フラッシュユーティリティの標準アップグレードメカニズムを使用してアップグレードすることはできません。ゴールデン ROMMON のアクセスポリシーは、FPGA ファームウェアによって適用され、ゴールデン ROMMON SPI フラッシュデバイスでの書き込みおよび消去コマンドなどの不正な操作がブロックされます。

（注） ゴールデンROMMONのアップグレードは、セキュアブートFPGAがアップグレードされた後にのみ利用可能になります。

スタンドアロンデバイス、高可用性デバイス、およびSVLデバイスでのアップグレード

アップグレードプロセスは、スタンドアロン、高可用性、および SVL デバイスごとに異なります。アップグレードプロセスの仕組みを次の表に説明します。

表 *1:* スタンドアロンデバイス、高可用性デバイス、および *SVL* デバイスでのアップグレード

デバイス設定	アップグレード プロセス
スタンドアロンデバイス	デバイスをインストールモードでアップグレードすると、デバイスのブート時にプライマリ ROMMON が自動的にアップグレードされます。ゴールデンROMMONをアップグレードするには、カプセルアップグレードプロセスを使用します。
高可用性デバイスおよび StackWise Virtual デバイス	高可用性セットアップでは、デバイスに対して In-Service Software Upgrade（ISSU）を行います。この ISSU プロセスには FPGA のアップグレードが含まれます。 リロードを使用してインストールモードでアップグレードする場合は、一度に1つのスーパバイザをリロードします。スタンバイスーパバイザを ROMMON 状態にして、アクティブなスーパバイザを最初にブートします。アクティブなスーパバイザで ROMMON のアップグレードが完了したら、FPGAおよびソフトウェアイメージもアップグレードします。

カプセルアップグレード

プライマリROMMON、プライマリFPGA、およびゴールデンFPGA（セキュアブートFPGA）は、デバイスのブート時に自動的にアップグレードされます。対照的に、ゴールデンROMMONをアップグレードできるのはカプセルアップグレード プロセスを使用する場合のみであるため、重要なブートコンポーネントに対するセキュリティが強化されます。

カプセルアップグレードでは、セキュアなアップデートカプセルが作成されてデジタル署名され、プライマリROMMONによってそのカプセルが使用されて、認証後にゴールデンROMMONがアップグレードされます。このプロセスにはセキュアなフラッシュ証明書が必要であり、それはプロダクトキーおよびアップデートカプセルの真正性を確認するためにプライマリ ROMMON イメージに含まれている ID を使用して生成されます。カプセル自体は、セキュア

なフラッシュ証明書とセキュアブート 16 MB フラッシュイメージを使用して作成され、アップグレードの完全性と真正性を保証するために署名されます。

デバイスがブートすると、プライマリ ROMMON によってゴールデン ROMMON のカプセルアップグレードが開始されます。ゴールデン ROMMON のカプセルアップグレードを手動で行うには、スイッチで **upgrade rom-monitor capsule golden** コマンドを使用するか、スイッチスタックで **upgrade rom-monitor capsule golden switch** コマンドを特権 EXEC モードで使用します。

カプセルアップグレードの仕組み

process_workflow

ここでは、カプセルアップグレード時の動作について説明します。

1. デバイスは、セキュアブート FPGA アップグレードが有効になっているかどうかを確認します。セキュアブート FPGA アップグレードが有効になっていない場合は、アップグレードが停止します。
2. デバイスは、ブートローダー保護が有効になっているかどうかを確認します。ブートローダー保護が有効になっていない場合は、プライマリ ROMMON、ゴールデン ROMMON、およびプライマリ FPGA のワンタイムアップグレードが開始されます。
3. ブートローダー保護がすでにアクティブになっている場合は、Cisco IOS XE がセキュアなアップデートカプセルをブートフラッシュにコピーし、デバイスを再起動します。
4. デバイスが再起動すると、セキュアなアップデートカプセルが選択されて、アップグレードが実行されます。

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。