



BIOS 保護

- [BIOS 保護の概要 \(1 ページ\)](#)
- [ROMMON アップグレード \(1 ページ\)](#)
- [BIOS 保護の機能履歴 \(3 ページ\)](#)

BIOS 保護の概要

BIOS 保護機能により、ゴールデン ROMMON イメージの書き込み保護とセキュアアップグレードが有効になります。ROMMON は、デバイスの電源を投入または再起動したときに、ハードウェアを初期化して Cisco IOS XE ソフトウェアイメージをブートするブートストラッププログラムです。ファームウェア障害を解決するか、新しい機能をサポートするには、ROMMON のアップグレードが必要になることがあります。通常、ROM モニターのアップグレードはまれで、Cisco IOS XE ソフトウェアのアップグレードごとには必要ありません。

BIOS 保護機能がないと、ソフトウェアのアップグレード中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。

ROMMON アップグレード

ROMMON イメージは、プライマリ ROMMON およびゴールデン ROMMON として SPI フラッシュデバイスに保存されます。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起動します。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起動します。デバイスがプライマリ ROMMON から起動すると、ゴールデン ROMMON はロックされます。BIOS 保護を使用すると、ゴールデン ROMMON は書き込み保護され、フラッシュユーティリティの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ができません。アクセスポリシーは、FPGA ファームウェアによって管理されます。FPGA は、ゴールデン ROMMON SPI フラッシュデバイスで許可されていない操作（書き込み、消去など）をブロックします。



(注) ゴールデン ROMMON アップグレードは、セキュアブート FPGA アップグレードなしでは有効になりません。

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、デバイスの起動時に自動的にアップグレードされます。ゴールデン ROMMON は、カプセルアップグレードを使用してのみアップグレードできます。

アップグレードプロセスはスタンドアロンシステムと高可用性システムで異なり、以下で説明します。

スタンドアロンシステム

スタンドアロンデバイスでは、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、デバイスの起動時にプライマリ ROMMON が自動的にアップグレードされます。ゴールデン ROMMON は、カプセルアップグレードを使用してアップグレードできます。

高可用性および StackWise Virtual システム

高可用性設定のデバイスでは、In-Service Software Upgrade (ISSU) を実行することを推奨します。FPGA のアップグレードは、ISSU の一部として行われます。

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を実行する場合は、両方のスーパーバイザを同時にリロードしないでください。スタンバイスーパーバイザを ROMMON 状態にして、アクティブスーパーバイザを起動します。各スーパーバイザで ROMMON アップグレードが完了すると、FPGA およびソフトウェアイメージがアップグレードされます。

スタンバイスーパーバイザを起動し、スタンバイスーパーバイザがアップグレードしてスタンバイホット状態になるようにします。

カプセルアップグレード

カプセルアップグレードでは、ゴールデン ROMMON をアップグレードするため、認証後にプライマリ ROMMON によって使用されるセキュアな更新カプセルが作成され、署名されます。セキュアな更新カプセルには、セキュアなフラッシュ証明書が必要です。セキュアなフラッシュ証明書はプロダクトキーを使用して作成され、プライマリ ROMMON イメージに追加されて更新カプセルの真正性が検証されます。カプセルは、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、署名されます。

デバイスが起動すると、プライマリ ROMMON がゴールデン ROMMON のカプセルアップグレードをトリガーします。ゴールデン ROMMON のカプセルアップグレードを実行するには、特権 EXEC モードで **upgrade rom-monitor capsule golden switch** コマンドを使用します。

カプセルアップグレードでは、次のプロセスが実行されます。

- 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。有効でない場合、プロセスは終了します。

- 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。有効でない場合は、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。
- 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、IOS はセキュアな更新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。
- デバイスが再起動すると、アップグレードを実行するためにセキュアな更新カプセルが選択されます。

BIOS 保護の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Gibraltar 16.12.1	BIOS 保護	BIOS 保護機能により、ゴールデン ROMMON イメージの書き込み保護とセキュアアップグレードが有効になります。
Cisco IOS XE Amsterdam 17.1.1	カプセルアップグレード	upgrade rom-monitor capsule switch active コマンドを使用したゴールデン ROMMON のカプセルアップグレードのサポートが有効になりました。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> からアクセスします。

