BIOS 保護

コントローラでの BIOS 保護

BIOS 保護を使用すると、Intel ベースのプラットフォームの BIOS フラッシュを保護し、安全に更新することができます。BIOS 保護が使用されていない場合、Intel プラットフォームの BIOS を保存するフラッシュ ユーティリティは書き込み保護されません。そのため、BIOS の更新が適用されると、悪意のあるコードも適用されてしまいます。

デフォルトでは、BIOSイメージが含まれているフラッシュをバンドルし、BIOSフラッシュでの書き込みを可能にする BIOS カプセルを介してのみアップデートを受け入れることによって、BIOS 保護が機能します。

BIOS 保護を使用した BIOS または ROMMON のアップグレード

BIOSまたはROMMONをアップグレードするには、次のようにBIOS保護機能を使用します。

1. ROMMON バイナリと一緒にバンドルされている新しい BIOS イメージ カプセルが、ROMMON アップグレード スクリプトによってシスコ デバイスのメディアに挿入されます。
2. その後、シスコ デバイスは、新しい BIOS/ROMMON のアップグレードが行えるようにリセットされます。
3. リセット時に、元の BIOS によって更新されたカプセルが検出され、更新された BIOS が使用可能かどうかが判定されます。
4. その後、元の BIOS によって BIOS カプセルのデジタル署名が検証されます。署名が有効な場合は、元の BIOS によってフラッシュ ユーティリティから書き込み保護が削除され、

SPI フラッシュが新しい BIOS イメージに更新されます。BIOS カプセルが無効な場合は、SPI フラッシュは更新されません。

5. 新しい BIOS/ROMMON イメージが SPI フラッシュに書き込まれた後、SPI フラッシュの必要な領域が再び書き込み保護されます。
6. カードがリセットされると、更新された BIOS がリブートされます。
7. カプセルが BIOS によって削除されます。

BIOS のアップグレード

手順

BIOS カプセルを更新するには、**upgrade rom-monitor filename** コマンドを使用します。

例：

```
upgrade rom-monitor filename bootflash:capsule.pkg <slot>
```

例

次に、BIOS 保護のアップグレードを確認する例を示します。

```
Device# upgrade rom-monitor filename bootflash:qwlc-rommon-capsule-p106.pkg all
Verifying the code signature of the ROMMON package...
Chassis model AIR-CT5540-K9 has a single rom-monitor.

Upgrade rom-monitor

Target copying rom-monitor image file

Secure update of the ROMMON image will occur after a reload.

8388608+0 records in
8388608+0 records out
8388608 bytes (8.4 MB, 8.0 MiB) copied, 11.9671 s, 701 kB/s
131072+0 records in
131072+0 records out
131072 bytes (131 kB, 128 KiB) copied, 0.414327 s, 316 kB/s
Copying ROMMON environment
8388608+0 records in
8388608+0 records out
8388608 bytes (8.4 MB, 8.0 MiB) copied, 31.1199 s, 270 kB/s
131072+0 records in
131072+0 records out
131072 bytes (131 kB, 128 KiB) copied, 2.44015 s, 53.7 kB/s
131072+0 records in
131072+0 records out
131072 bytes (131 kB, 128 KiB) copied, 2.43394 s, 53.9 kB/s
ROMMON upgrade complete.
```

```
To make the new ROMMON permanent, you must restart the RP.
Device#reload
```