Microsoft Secure Boot証明書の有効期限の緩和

はじめに

このドキュメントでは、Cisco UCS環境に関係するセキュアブート証明書の期限切れを緩和する方法について説明します。

バックグラウンド情報

セキュアブートは、最新のサーバおよびPCのUnified Extensible Firmware Interface(UEFI)に組み込まれている基本的なセキュリティ機能です。デジタル署名および検証済みのソフトウェア（ブートローダ、オペレーティングシステムカーネル、およびUEFIドライバ）のみが実行可能であることを保証することで、ブートプロセス中に信頼のチェーンが確立されます。このメカニズムは、ブートキット、ルートキット、およびその他の低レベルのマルウェア脅威からシステムを保護します。

セキュアブートの中心には、Microsoftによって発行された暗号証明書のセットがあります。これらの証明書は、Cisco UCS(Unified Computing System)サーバを含め、過去10年間に出荷された事実上すべてのサーバおよびPCのUEFIファームウェアに組み込まれています。ブートタイムソフトウェアの一部が正当であるかどうかを検証するトラストアンカーとして機能します。

Microsoftは、2つの重要なセキュアブート証明書(Microsoft Windows Production PCA 2011およびMicrosoft UEFI CA 2011)の有効期限が2026年10月19日に切れる予定であることを公開しました。この期限はハードウェアエコシステム全体に影響を与えます。シスコはUCSサーバポートフォリオへの影響をCisco Bug ID CSCwr45526で確認しています

問題

有効期限が切れる証明書

この問題の中心にある2つの証明書は次のとおりです。

証明書	ロール	有効期限
Microsoft Windows製品PCA 2011	Microsoft Windowsブートローダの署名と検証	2026年10月19日
Microsoft UEFI CA	サードパーティのUEFIドライバ、オプションROM、および	2026年

証明書	ロール	有効期限
2011	Windows以外のブートローダに署名し、検証します。	10月19日

これらの証明書は、UEFIファームウェアのセキュアブートキーストアに保存されます。

- db（シグニチャデータベース）：ブートタイムバイナリの検証に使用される信頼できる証明書が含まれています。
- KEK(Key Exchange Key)：シグニチャデータベースのアップデートを承認します。
- PK（プラットフォームキー）：通常はOEMが所有する信頼のルート（例：Cisco）。

Cisco UCSサーバの問題の理由

Bシリーズ（ブレード）、Cシリーズ（ラック）、Xシリーズ（モジュラ）プラットフォームを含むCisco UCSサーバは、UEFI BIOSファームウェアにプリロードされたこれらのMicrosoft 2011証明書とともに出荷されます。セキュアブートを有効にすると、BIOSはブートサイクルごとに次の証明書を使用して検証します。

1. Windows Serverブートローダ(たとえば、`bootmgfw.efi`):Windows製品PCA 2011によって署名されました。
2. 次のようなサードパーティ製UEFIコンポーネント

   - Cisco VIC（仮想インターフェイスカード）オプションROM
   - ストレージコントローラ(RAID)UEFIドライバ
   - ネットワークアダプタPXEブートROM
   - POST中にロードされた他のPCIeデバイスファームウェア

   これらは通常、Microsoft UEFI CA 2011によって署名されます。

何もアクションを実行しないと、どうなりますか。

証明書の有効期限が切れると、Cisco UCSサーバで次の障害シナリオが発生する可能性があります。

- Windowsサーバのブートに失敗する:UEFIファームウェアがWindowsブートローダを検証できないため、セキュアブートによってOSのロードがブロックされます。これは、Windows Server 2016、2019、2022、および2025に影響します。

- UEFIドライバとオプションROMが拒否される：期限切れ証明書で署名されたUEFIドライバに依存するハードウェアコンポーネントは、POST中に初期化に失敗する場合があります。その結果、RAIDボリュームへのアクセスが失われたり、PXEブート中にネットワーク接続が切断されたり、その他の重要なハードウェア機能が失われる可能性があります。
- システムがセキュリティで保護されていない状態に陥る：管理者が回避策としてセキュアブートを無効にしようとする可能性があります。これにより、ファームウェアレベルのセキュリティの重要なレイヤが排除され、組織のコンプライアンスポリシー（NIST、PCI-DSS、HIPAAなど）に違反する可能性があります。
- 大規模な運用中断：数百または数千のUCSサーバがあるエンタープライズ環境では、ブート障害イベントの調整により、データセンター全体で重大なダウンタイムが発生する可能性があります。

シスコはこの問題を以下のサイトで正式に追跡しました。 Cisco Bug ID CSCwr45526 .この不具合では、次の点を確認します。

- UCSサーバのBIOSファームウェアには、期限が切れるMicrosoft 2011 Secure Boot証明書が含まれています。
- 置換証明書（Microsoft 2023証明書）をUEFIキーストアに導入するには、BIOSのアップデートが必要です。
- 修復を行わないと、セキュアブートが有効になっているUCSサーバは、有効期限後にブート障害が発生するリスクがあります。

ソリューション

この問題に対処するには、調整された2方面からのアプローチ(Cisco UCSファームウェア(BIOS)とMicrosoft Windowsオペレーティングシステムの両方をアップデートする)が必要です。どちらのアップデートも単独では十分ではなく、Secure Bootトラストチェーンの両側を最新化する必要があります。

1. Cisco UCS BIOS/ファームウェアアップデートの適用

新しいMicrosoft Secure Boot証明書を含む、該当するUCSプラットフォームのBIOSファームウェアをアップデート。

新しい証明書	交換品
Microsoft Windows UEFI CA 2023	Microsoft Windows製品PCA 2011
Microsoft UEFI CA 2023	Microsoft UEFI CA 2011

アクションの手順：

- モニタCisco Bug ID CSCwr45526 Cisco Bug Search Toolで、修正済みファームウェアバージョンとリリースタイムラインを検索できます。
- 特定のUCSプラットフォーム（Bシリーズ、Cシリーズ、Xシリーズ）で利用可能な場合は、更新されたBIOSをダウンロードして導入します。
- 導入にシスコの管理ツールを使用:
  - Cisco Intersight：クラウドマネージ型環境では、Intersightファームウェア管理ポリシーを使用して、規模に応じてアップデートを調整します。
  - Cisco UCS Manager(UCSM)：ドメイン管理されたBシリーズおよびCシリーズサーバ向け。
  - Cisco IMC(Integrated Management Controller)：スタンドアロンCシリーズラックサーバ向け。

2. Microsoft Windowsの更新プログラムを適用する

Microsoftは、Windows Updateを通じてセキュアブート証明書の更新を段階的に展開しています。

フェーズ	説明	スケジュール
フェーズ1：準備	新しい2023証明書がセキュアブートdbに追加されます。古い2011証明書は信頼された状態を維持します。新旧両方の証明書が共存します。	現在利用可能
フェーズ2：移行	2023証明書で署名された新しいブートマネージャが展開されます。システムは新しい信頼のチェーンを使用し始めます。	段階的な展開（2025 ~ 2026年）
フェーズ3：適用	古い2011証明書はDBX(Forbidden Signature Database)に追加され、事実上、無効になります。新しい証明書だけが信頼されます。	期限切れ後

アクションの手順：

- Windows Serverを実行しているすべてのUCSサーバに、最新の累積的なアップデートがインストールされていることを確認します。
- Microsoftリリースノートのセキュアブート関連のアップデートに特に注意してください。
- Phase 1とPhase 2のアップデートをスキップしないでください。これらは、スムーズな移行のための前提条件です。

3. 環境の検証

ファームウェアとOSの両方のアップデートを適用した後、各サーバでセキュアブートの状態を確認します。

Windows PowerShellから：

powershell
コードのコピー

```
# Confirm Secure Boot is active
Confirm-SecureBootUEFI

# Review Secure Boot certificate details
Get-SecureBootUEFI -Name db | Format-List
```

Cisco IMC/Intersightから：

- BIOSバージョンがアップデートされたファームウェアを反映していることを確認します。
- セキュアブートがBIOSポリシーで有効のままであることを確認します。

4. 推奨される修復スケジュール

期間	アクション	Priority
現在：2026年第2四半期	セキュアブートが有効になっているすべてのUCSサーバのインベントリを作成します。Cisco Bug ID CSCwr45526のアップデートに登録する 🔍.	高
2026年第2四半期～第3四半期	ラボ/ステージング環境でアップデートされたBIOSファームウェアをテストします。WindowsのPhase 1およびPhase 2アップデートを適用します。	高
2026年第3四半期	BIOSアップデートとWindowsアップデートをUCS全体に対して実稼働導入します。	高
2026年10月19日以前	すべての更新を完了します。すべてのサーバでセキュアブートの状態を検証します。	Critical
有効期限の終了後	フェーズ3の実施を監視します。システムが失われていないことを確認します。	中間

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。