改訂日：2025 年 2 月 28 日

Cisco Nexus Hyperfabric シリーズ：セキュアブート

Cisco Secure Boot に関する情報

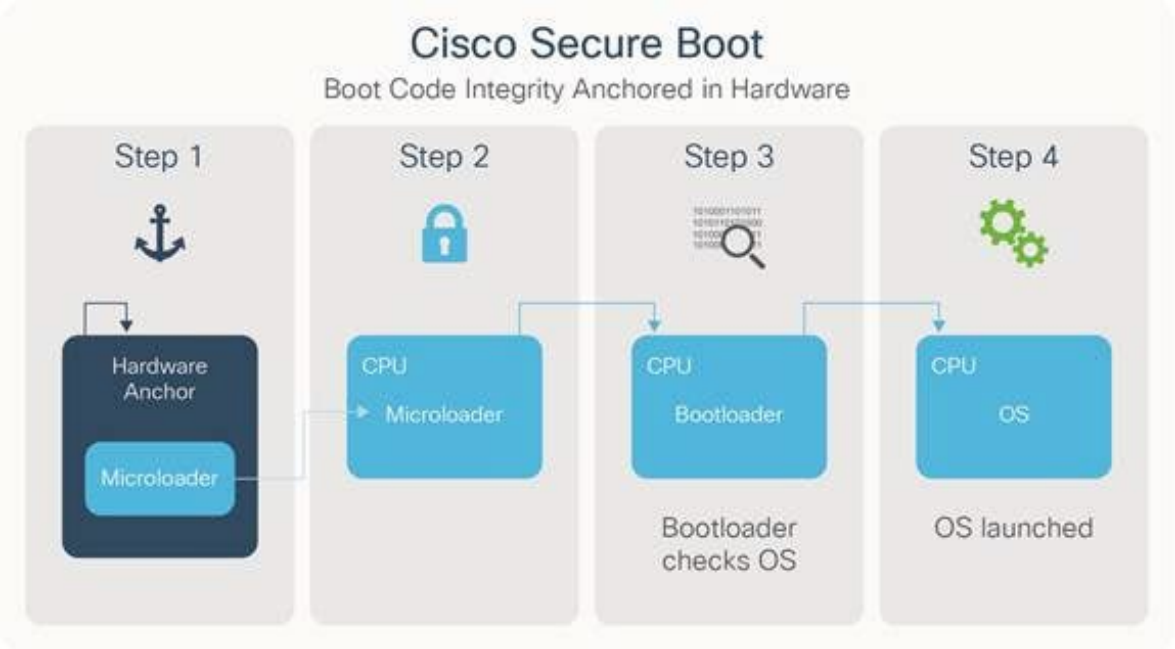
シスコ セキュア ブートのサポートは、Cisco Nexus Hyperfabric OS を使用する Cisco 6000 シリーズ スイッチ（HF6100-60L4D および HF6100-32D）に導入されています。

シスコのセキュアブートは、Cisco 6000 シリーズ スイッチ上で実行される最初のコードが真正であり、変更されていないこと確認します。シスコ セキュア ブートはマイクロローダーをミュート不可ハードウェアにアンカーリングし、信頼の起点を確立して、シスコのネットワークデバイスが、改ざんされたネットワークソフトウェアを実行するのを防止します。ハードウェアのブート コードを保護し、イメージ ハッシュを表示し、デバイスの セキュア ユニーク デバイス ID（SUDI）証明書を提供します。起動プロセス中にセキュア キーの認証に失敗すると、ラインカード モジュールは起動が機能不全になり、BIOS の改ざんを防ぎます。セキュアブートはデフォルトで有効になっています。

ソフトウェア認証に関して、シスコはハードウェアによるセキュアブートプロセスを実装することによって差別化され、優れた堅牢性を備えたセキュリティを実現します。ハッカーがデバイスを物理的に所有している場合でも、ハードウェアの変更は難しく、コストがかかり、隠蔽も容易ではないため、堅牢です。

シスコのセキュアブートのワークフロー

図 1：Cisco 6000 シリーズ スイッチのブートコードの整合性とセキュリティに関するワークフロー



1. 本物ハードウェアアンカーリングされたセキュアブートの場合により、CPU 上で実行される最初の命令は、変更できないハードウェア内に保存されます。
2. デバイスが起動すると、マイクロローダーは、次の一連の指示がシスコからのものかどうかを、その一連の指示にあるシスコのデジタル署名を検証することによって確認します。
3. ブートローダは、オペレーティング システムがシスコによってデジタル署名されているかどうかを確認することにより、オペレーティング システムがシスコからのものであることを検証します。
4. すべてのチェックに合格すると、オペレーティング システムが起動します。デジタル署名チェックが何らかの失敗をした場合、シスコデバイスはそのソフトウェアを起動させず、悪意のあるコードがデバイスに実行されないように確認します。

偽造防止対策について

偽造防止対策が Cisco 6000 シリーズ スイッチ（HF6100-60L4D および HF6100-32D）に導入されています。

偽造防止対策により、シスコのソフトウェア イメージを備えた Cisco 6000 シリーズ スイッチ プラットフォームが本物であり、変更されていないことが保証されます。これにより、ハードウェア レベルの信頼のルートと、システムを構築するための不変のデバイス アイデンティティが確立されます。

Cisco 6000 シリーズ スイッチは、ACT2 対応の ASIC で構築されています。これにより、対応する SUDI X.509v3 証明書がハードウェアに埋め込まれます。SUDI 証明書、関連付けられたキーペア、その証明書チェーン全体が改ざん防止 Cisco トラストアンカー チップに保存されます。キー ペアは特定のチップにバインドされ、秘密キーはエクスポートされません。この機能により、アイデンティティ 情報のクローニングやスプーフィングを不可能にします。

SUDI はトラスト アンカー モジュール（TAm）に恒久的にプログラムされていて、クローズで、セキュリティ保護され、そして監査されたシスコの製造プロセスにおいてシスコによって記録されます。このプログラミングは強力なサプライ チェーン セキュリティを提供します。これは、ルータやスイッチなどの組み込みシステムにとって重要です。

ACT2 認証が失敗すると、エラー メッセージが表示されます：

`ACT2_AUTH_FAIL`：モジュール `9` での `ACT2` テストがエラー：「`ACT2 authentication failure`」で失敗しました

支援が必要な場合は、Cisco Technical Assistance Center（TAC）にお問い合わせください。