セキュア ブートの構成

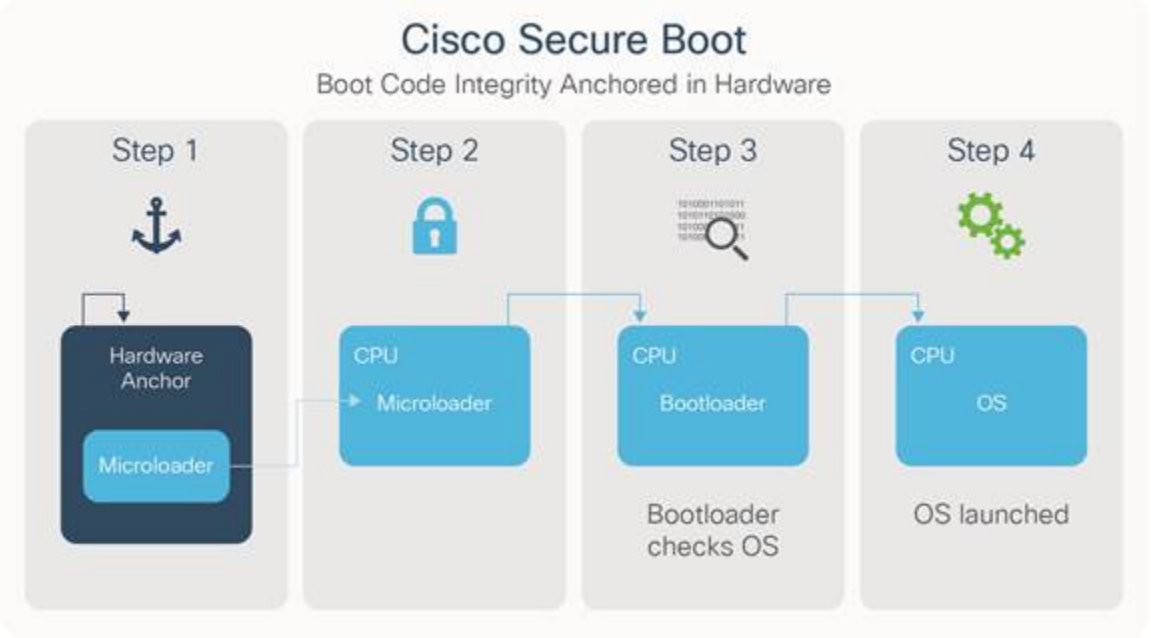
Cisco Secure Boot に関する情報

Cisco Secure Boot サポートは、Cisco MDS NX-OS 8.1(1) 以降のリリースの Cisco MDS 9700 48 ポート 32 Gbps ファイバ チャネル スイッチング モジュール、Cisco MDS 9132T ファイバ チャネル スイッチ、Cisco MDS 9396T ファイバ チャネル スイッチ、および Cisco MDS 9148T ファイバ チャネル スイッチに導入されました。

シスコのセキュアブートは、シスコ製ハードウェア プラットフォーム上で実行される最初のコードが真正であり、改ざん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 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

Cisco MDS NX-OS リリース 8.1（1）から、偽造防止対策が Cisco MDS 9700 48 ポート 32 Gbps ファイバ チャネル スイッチング モジュール、Cisco MDS 9132T ファイバ チャネル スイッチ、Cisco MDS 9396T ファイバ チャネル スイッチ、および Cisco に導入されました。 MDS 9148T ファイバー チャネル スイッチ。

偽造防止対策により、Cisco NX-OS ソフトウェア イメージを備えたシスコ ハードウェア 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 ID が確立されます。

Cisco MDS 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: ACT2 test has failed on module 9 with error : ACT2 authentication failure
```

ACT2 認証失敗について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。

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。