シスコのセキュアブート

この付録では、シスコのセキュアブートプロセスと、それがイメージの命名規則に与える影響について簡単に説明します。

ここで説明する内容は、次のとおりです。

基本的な概念

デジタル署名では、ソフトウェアコードなどの特定のデータブロックに関して一意のデジタル署名を作成します（多くの場合、コードまたはイメージ署名と呼ばれます）。署名は、チェックサムに似たハッシュアルゴリズムを使用して作成されます。ソフトウェアコードにこの方法で署名し、実行時にチェックして、変更されていないことを検証できます。通常、コードはコード所有者によって計算された署名を取得し、その署名はコードとともにシステムに保存されます。コードが後で実行されると、同じアルゴリズムを使用して独自の署名を作成し、事前に計算され保存された署名と比較することで自己検証できます。または、他のシステム要素がこの署名の計算とチェックを実行できます。

システムソフトウェアの範囲内の信頼要素は、本物であることがわかっているコードの一部です。信頼できるコードは、変更できない（変更を防ぐ方法で保存されている）か、真正性を保証するための十分な検証メカニズムが用意されているかのいずれかです。

Root of Trust は、保証された信頼要素が存在するシステムの最下位層です。システムで実行される最初のコードが変更不能である場合、それはそのシステムの Root of Trust になります。

信頼チェーンは一連の信頼要素であり、チェーン内の各要素は、その前の要素によって「信頼できる」と検証されます。信頼チェーンは Root of Trust 要素から始まり、チェーン内の連続する要素を検証していきます。

セキュアブートの概要

シスコのセキュアブートは、Root of Trust を変更できない回路カード上のハードウェアチップデバイスにこれを配置します。電源投入直後に実行される最初のコード（マイクロローダ）は、シスコからの正規のコードであり、システムの製造時にプログラムされたものであることが保証されています。また、ソフトウェアイメージはすべて、ロード/実行の前に変更されていないか暗号で検証できます。

シスコのセキュアブートテクノロジーの目的は、保護されていないブートコードに関連する潜在的な問題に対処することです。

コードの一部が検証されると、そのコードは信頼され、プロセッサを制御することができます。ブートシーケンスの各ステップでは、コード署名されたモジュール（信頼チェーン）を介してブートモジュールの次のステップを検証します。

MIO2 によるセキュアブートのサポート

ASR 5500 MIO2 は、リリースキーを持つデジタル署名されたイメージを使用したセキュアブートをサポートします。実稼働環境の MIO2 カードには、リリースキーサフィックス **.SPA** で署名されたイメージファイル名が必要です。例：asr5500-21.0.0.bin.SPA

重要 MIO、DPC、および DPC2 カードにもデジタル署名されたブートイメージがありますが、署名は無視されます。

イメージの命名規則

署名されたイメージと署名されていないイメージを区別するために、リリースエンジニアリングは、署名されたイメージのビルド名にサフィックスを追加します。たとえば、asr5500-20.0.0.bin などです。**SPA** は、お客様のネットワークに展開可能と署名されたリリースキーを示します。

真正性の検証

EXEC モードの **show software authenticateity** コマンドは、starfile イメージの信頼チェーンおよび認証プロセスに関する情報を表示します。

このコマンドのシンタックスは次のとおりです。

show software authenticity { file *url* **[validate] | keys | running }**

注：

- **file** *url* **[validate]** は、フラッシュ上またはネットワーク上の starfile イメージの真正性情報を示しています。**検証** オプションは、イメージのデジタル署名検証を実行します。
- **keys** は、各キーストレージリージョン（プライマリ、バックアップ）の StarOS 公開キー情報と、ロールオーバーキー情報を示しています。
- **running** は、実行中のすべてのソフトウェアイメージ（StarOS、CFE（ブートストラップ）、BIOS/UEFI（Unified Extensible Firmware Interface）、およびマイクロローダー）の信頼チェーンに関する情報を示しています。

このコマンドの詳細については、『*Command Line Interface Reference*』を参照してください。

シスコのセキュアブート

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。