Cisco Trustworthy 技術データシート

製品概要

Trustworthy ソリューションには、現在の脅威から保護するための多層セキュリティを備えた製品およびソリューションを提供するというシスコの取り組みが含まれています。Trustworthy 技術は、シスコのソリューション ポートフォリオ全体のセキュリティとレジリエンシー（復元力）の基盤となります。イメージ署名、セキュアブート、シスコのトラストアンカーモジュール（TAm）、ランタイムディフェンスなどの Trustworthy 技術は、Cisco ハードウェア プラットフォームで実行されるコードが真正であり、変更されておらず、意図したとおりに動作していることを確認するのに役立ちます。ハードウェアレベルの信頼の起点、一意のデバイス ID、スタートアップ時のすべてのレベルのソフトウェア検証により、システムの信頼のチェーンが確立されます。

Trustworthy 技術はシスコソリューションのセキュリティをどのように強化しているか？

今日の高度なサイバー攻撃は、ルータやスイッチのようなデバイスを攻撃することで、ネットワーク インフラストラクチャをさらに侵害しようとしています。攻撃者はそうして機密通信を傍受し、データを盗んだり操作したりしてネットワークの他の部分に対する攻撃を開始します。これには、ネットワークデバイスのハードウェアまたはソフトウェアを変更する APT(Advanced Persistent Threat) が含まれます。これらの脅威は、数ヵ月、場合によっては数年間見落とされる可能性があり、壊滅的な損害を与える可能性があります。

シスコの Trustworthy 技術は、製品保証機能とシスコのソリューションのセキュリティとレジリエンシーを強化する基盤となるセキュリティ機能を提供します。デバイスの偽造やハードウェアとソフトウェアへの悪意のある攻撃から保護するために、シスコはデジタル署名付きソフトウェアイメージ、ハードウェアアンカー セキュアブート、セキュアユニークデバイス識別子 (SUDI)、その他の Trustworthy 技術を使用して、ソリューションの真正性と完全性を検証します。特に、Trustworthy 技術はハードウェアとソフトウェアの完全性の自動チェックを実行し、侵害が検出された場合にはブートプロセスをシャットダウンすることができます。シスコのトラストアンカーモジュールは、セキュアユニークデバイス識別子、安全性の高いストレージ、ランダムビットジェネレータ、セキュアな鍵管理を備えています。これらのセキュリティの追加レイヤによって偽造やソフトウェアの変更から保護され、セキュアで暗号化された通信が可能になり、シスコのネットワークデバイスが意図したとおりに動作していることが検証されます。

シスコを選択する理由

シスコのセキュリティへの取り組み範囲は、業界では比類のないものです。シスコの Trustworthy ソリューションは、セキュリティに重点を置いた開発プロセスと標準ベースのテクノロジーから始まり、セキュアでレジリエンシーの高いネットワーキング ソリューションを可能にするセキュリティ機能を加えます。セキュリティ機能は、スタートアッププロセスのプロアクティブなモニタリングを含む、システムクリティカルな機能とセキュリティ機能の両方を実行します。

シスコは、ソリューションのセキュリティとレジリエンシーの継続的な強化に努めています。署名付きイメージとトラストアンカーモジュールのセキュアブートなどの Trustworthy 技術を備えた、Cisco ハードウェアおよびソフトウェア プラットフォームの真正性と完全性を検証することでリスクを軽減し、今日の脅威から保護します。

シスコには、シスコ製品開発チームと協力してシスコ製品ライン全体にセキュリティを組み込む専任のエンジニア チームおよびセキュリティマネージャがいます。シスコは、自社のグローバル エンタープライズ ネットワークの防御を通じて得られたセキュリティの専門知識を活用し、ビジネスとソリューションのセキュリティを継続的に強化しています。

シスコ Trustworthy 技術の基本概念

イメージ署名：イメージ署名では、2 段階のプロセスを経て、特定のコードブロックに一意のデジタル署名を作成します。まず、チェックサムに似たハッシュアルゴリズムを使用して、コードブロックのハッシュ値を計算します。その後、ハッシュをシスコの秘密キーで暗号化してデジタル署名を作成し、それを追加したイメージを提供します。署名付きイメージは、ソフトウェアが変更されていないことを検証するために、実行時に検証される場合があります。

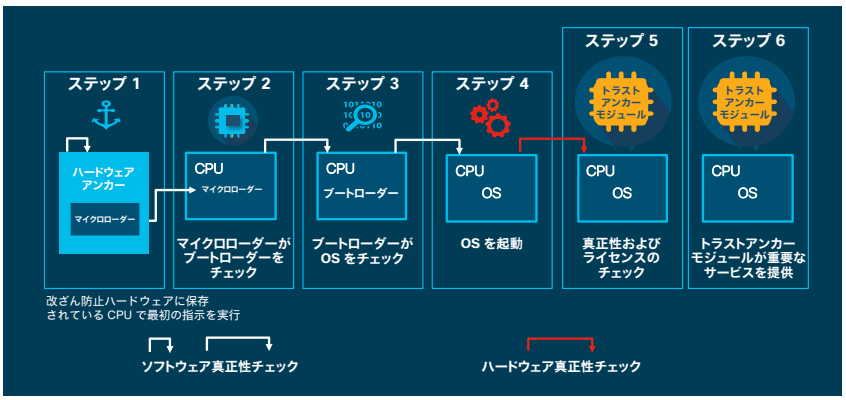
セキュアブート：シスコのセキュアブートは、Cisco ハードウェア プラットフォーム上で実行されるコードが改ざんされていない正規のものであるという確証の助けになります。シスコのハードウェアアンカー セキュアブートは、改ざん防止ハードウェアのマイクローダー（起動する最初のコード）を保護し、シスコのネットワークデバイスが、汚染されたネットワークソフトウェアを実行するのを防止する信頼の起点を確立します。

信頼のチェーン：コードの実行が許可される前に、システムにおけるコードの各要素の完全性が検証されると信頼のチェーンが成立します。信頼のチェーンは、信頼要素の起点から始まります。信頼の起点がチェーン内の次の要素（通常はファームウェア）を検証してから、開始が許可されます。署名と信頼できる要素を使用することで、システムをセキュアに起動し、シスコのソフトウェアの完全性を検証する信頼のチェーンを作成できます。図 1 を参照してください。

トラストアンカーモジュール（TAm）：この独自の改ざん防止チップは、多くのシスコ製品に内蔵されており、不揮発性セキュアストレージやセキュアユニークデバイス識別子、乱数生成（RNG）、セキュアストレージ、鍵管理などの暗号化サービス、実行中の OS およびアプリケーションへの暗号化サービスを備えています。

ランタイムディフェンス（RTD）：ランタイムディフェンスは、実行中のソフトウェアへの悪意のあるコードのインジェクション攻撃を標的にします。シスコのランタイムディフェンスには、アドレス空間レイアウトランダム化（ASLR）、組み込みオブジェクトサイズチェック（BOSC）、X スペースが含まれます。ランタイムディフェンスは補完的なものです。

図 1. ハードウェアアンカー セキュアブートと TAm によるハードウェアとソフトウェアの完全性の検証



一般的な質問

ハードウェアとソフトウェアが正規のシスコ製品であることと、起動前または起動時にシステムソフトウェアが変更されていないことを確認するにはどうすればよいですか？

Trustworthy 技術は、ご使用の製品が正規のシスコ製品であるという確信をお届けします。シスコのセキュアブートは、ハードウェアのブートコードを保護し、デジタル署名付きイメージのチェックを使用して、変更されていない真正なコードがシスコのデバイスで起動していることを検証します。トラストアンカーモジュールの SUDI は、ハードウェアが正規のシスコ製品であることを検証します。

デバイスがシスコの Trustworthy 技術を実装していることを確認するにはどうすればよいですか？

現在、多くのシスコのソリューションで Trustworthy 技術が利用可能になっています。シスコの製品チームは、デバイスのユースケースに基づいて製品にセキュリティテクノロジーを設計しています。この機能は、シスコのルーティング、スイッチング、ワイヤレス、サーバ、セキュリティ製品の多くで利用でき、追加のプラットフォームにも組み込まれています。脅威の状況が進化するに従い、シスコ製品のセキュリティ要件も絶えず見直され変更されます。シスコは、高度なセキュリティ調査に取り組み、新しい Trustworthy 技術の導入や開発を続けており、それらが利用可能になった時点で実装しています。デバイスのセキュリティプロファイルについては、アカウントマネージャまたはセールスエンジニアまでお問い合わせください。

シスコの Trustworthy 技術を実装しないことのリスクは何ですか？

ハードウェアアンカーの信頼起点の欠如は、ハッキングを招きます。第三者が、BIOS、ブートローダ、ROM モニタ（ROMMON）ブートコードを改ざんし、変更されたソフトウェアイメージ、バイパスハードウェア、認証、ライセンスチェックをロードしたり、悪意ある意図で追加の機能を実行したりする可能性があります。改ざんされたコードは、データ操作やデータの盗難にもつながり、サービス妨害（DoS）などの攻撃を開始するプラットフォームとなる可能性があります。シスコの Trustworthy 技術により、これらの潜在的なセキュリティギャップを埋めることができます。

またシスコは、バリューチェーン セキュリティ プログラムを通じてサプライチェーンのリスクに対応するために、サプライヤ、製造パートナー、流通パートナーと連携しています。このプログラムは、フィジカル セキュリティ プラクティス、論理的なセキュリティプロセス、セキュリティテクノロジーを使用して、知的財産の侵害、偽造、誤用に対処する多層型のセキュリティアプローチを採用しています。シスコの包括的なプログラムは、ソリューションのライフサイクル全体のセキュリティを継続的に評価、監視、および改善しています。シスコは一貫して、セキュリティ強化とお客様の信頼の獲得に努めています。

不変な機器の ID：SUDI

セキュアユニークデバイス識別子、つまり SUDI は、製品 ID とシリアル番号を保持する X.509v3 証明書です。ID は製造時に実装され、公的に識別可能なルート認証局につながれます。SUDI は、設定、セキュリティ、監査、管理のための不変な機器の ID として使用できます。

トラストアンカーモジュールの SUDI クレデンシャルには、RSA または楕円曲線デジタル署名アルゴリズム（楕円曲線 DSA）ベースのいずれかで使用できます。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機能を持つトラストアンカー モジュール チップに保存されます。さらに、キーペアは特定のトラストアンカーチップに暗号化されており、秘密鍵が取り出されることはありません。この機能により、ID 情報の複製（クローニング）やなりすまし（スプーフィング）が事実上不可能になります。

セキュアキーを使用した保存データの暗号化および暗号解読機能

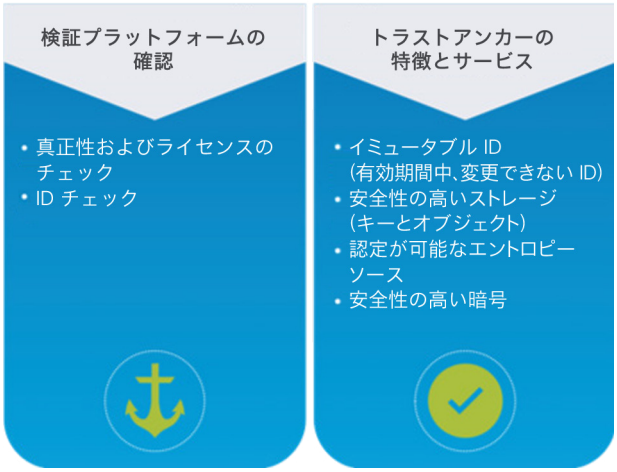
またシスコのトラストアンカーは、一般的に、ローカルで有効な証明書（LSC または LDevID; ローカルデバイス ID）と呼ばれる、お客様が管理する証明書に使用できるキーペアを生成することもできます。

トラストアンカーでサポートされる顧客 ID 機能には次のようなものがあります。

- LDevID RSA 公開キーの取得
- LSC 登録前の認証局 (CA) での認証
- ゼロタッチプロビジョニング認証
- セキュアブートのポスチャアセスメント

SUDI は、暗号化、復号化、署名、操作対象のデータの通過を許可する検証などの非対称鍵操作に使用できます。この機能により、デバイスのリモート認証が可能になります。そうすることで、シスコ製品の正確で一貫性のある電子的な識別を、資産管理、プロビジョニング、バージョンの可視性、サービス権利、品質フィードバック、インベントリ管理に使用できるようになります（図 2 参照）。

図 2. SUDI 不変デバイス ID



安全性の高いストレージ

シスコのトラストアンカーモジュールは、暗号鍵、パスワード、お客様のログイン情報、デバイスに関するその他の重要なセキュリティ情報のために安全性の高いストレージを備えています。このモジュールの利点の 1 つは、秘密鍵とパスワードを保存して、より高いセキュリティを実現できることです。トラストアンカーモジュールの外部にセキュアなストレージを割り当てることも可能です。

乱数生成とエントロピーソース

強力な乱数生成（RNG）は暗号化の中核をなしていますが、弱い RNG は暗号化システム全体をの強度を損なう可能性があります。乱数生成器は、暗号鍵の作成、ユーザと Web サイト間における安全性の高い通信の確立、電子メールアカウントのパスワードのリセットにおいて、重要な役割を果たします。確実なランダム性がなければ、攻撃者はシステムが生成しようとするものを予測し、アルゴリズムを弱体化させることができます。シスコのトラストアンカーモジュールは、NIST の仕様に準拠しており、トラストアンカー内の真のランダムソースからエントロピーを抽出する NIST SP 800-90A および B の認定が可能な RNG を備えています。

特徴	説明	利点
Trustworthy 技術	偽造およびソフトウェアの変更から保護し、シスコ製品が意図したとおりに動作していることを検証する、シスコのネットワーキングデバイスに設計されたセキュリティテクノロジーは進化し続けています。Trustworthy 技術には、乱数生成（RNG）および暗号化サポート、セキュアストレージ、セキュアユニークデバイス識別子（SUDI）などのトラストアンカーモジュールのセキュリティ機能に加えて、イメージ署名、セキュアブート、ランタイムディフェンスが含まれます。	• ハードウェアが正規のシスコ製品であることを検証 • 偽造およびソフトウェアの変更から保護 • セキュアで暗号化された通信をサポート • デバイス認証とゼロタッチプロビジョニングを有効にし、導入コストを削減
イメージ署名	イメージ署名では、2 段階のプロセスを経て、特定のコードブロックに一意のデジタル署名を作成します。まず、チェックサムに似たハッシュアルゴリズムを使用して、コードブロックのハッシュ値を計算します。その後、ハッシュをシスコの秘密キーで暗号化してデジタル署名を作成し、それを追加したイメージを提供します。署名付きイメージは、ソフトウェアが変更されていないことを検証するために、実行時に検証される場合があります。	暗号化された署名付きイメージ： • ファームウェア、BIOS、およびその他のソフトウェアが正規のものであり、変更されていないことを確認 • 改ざんされていない正規のソフトウェアのみをシスコ製デバイスで起動可能にする重要なチェック機能の提供 • 執拗な攻撃を効果的に軽減
セキュアブート	シスコのセキュアブートは、シスコ製のハードウェア プラットフォームで実行されるコードが正規のものであり、改ざんされていないこと確認します。シスコのハードウェアアンカー セキュアブートは、改ざん防止ハードウェアのマイクロローダー（起動する最初のコード）を保護し、シスコのネットワークデバイスが、汚染されたネットワークソフトウェアを実行するのを防止する信頼の起点を確立します。	• 起動時のソフトウェア完全性の自動チェック • スタートアッププロセスをモニタし、侵害が検出された場合にはブートプロセスをシャットダウン • 改ざんされていない正規のソフトウェアのみがシスコのプラットフォームで起動可能
トラストアンカーモジュール（TAm）	この独自の改ざん防止チップは、多くのシスコ製品に内蔵されており、不揮発性セキュアストレージ、や SUDI、RNG、キーストア、暗号化エンジンなどの暗号化サービスを備えています。	• 製造時にインストールされる X.509 SUDI 証明書により一意のデバイス ID を提供 • SUDI により、認証とリモートプロビジョニングに加え偽造防止チェックが可能 • セキュアなオンボードストレージ • セキュア通信をサポートする RNG や暗号化サービス
ハードウェア真正性チェック	トラストアンカーモジュールにインストールされている X.509 SUDI 証明書を使用して、Cisco ハードウェアが正規のものである（シスコによって製造された）ことを検証するプロセスです。ハードウェア真正性チェックは、セキュアブートプロセスが完了し、ソフトウェアが信頼できると検証された後にのみ実行されます。	• ハードウェアの真正性を検証 • 偽造から保護
ランタイムディフェンス	ランタイムディフェンスは、実行中のソフトウェアへの悪意のあるコードのインジェクション攻撃を標的にします。シスコのランタイムディフェンスには、アドレス空間レイアウトランダム化（ASLR）、組み込みオブジェクトサイズチェック（BOSC）、X スペースが相補的に含まれています。	• 攻撃者が、実行中のソフトウェアの脆弱性を悪用することを困難または不可能に • ランタイムディフェンスは補完的で、これらを個別に実装することも複数のランタイムディフェンスを一緒に導入することも可能

詳細については、以下にアクセスしてください。

シスコ Trustworthy 技術の詳細については、Trust Center にアクセスするか、ask-trustworthy@cisco.com までお問い合わせください。