IOS XR データシート

目次

新しい要求に応える新しいソフトウェア

従来のネットワーク オペレーティング システム（NOS）は、ネイティブハードウェア環境で実行するように設計されています。NOS は画一的なアプローチで設計されているため柔軟性に欠け、ネットワークデバイスの管理が複雑になり、更新や変更に多くの時間が必要になります。シスコでは、NOS プラットフォームはシンプルかつ最新で、高信頼性が必要であると考えています。NOS は、独自の設定をサポートし、運用の柔軟性を高め、セキュリティを強化できる必要があります。柔軟な NOS がなければ、サービスプロバイダーのエンジニアは、前例のないトラフィックの増加に対処し、サービスプロバイダーの顧客が要求するサービスとパフォーマンスを提供できる、高速で信頼性の高い柔軟なネットワークを効率的に管理、運用するのに苦労します。

接続されているデバイス数の増加とコンテンツ消費量の上昇により、インターネットトラフィックは、過去 5 年間で 30% の複合年間成長率を記録しています。2022 年までに、次のことが予想されています。

- IP トラフィックが 1 か月あたり 396 エクサバイトに増加する。
- インターネットトラフィックの 1/3 が大都市サービスエリアで発生する。
- 280 億台を超えるデバイス/エンドポイントがオンラインになる。
- ピーク時のインターネットトラフィックは、ストリーミングビデオやオンラインゲームの増加により、平均的なインターネットトラフィックよりも急速に増加しています。[1]

この増加を見越して、シスコはネットワーク運用を容易にするために IOS® XR NOS を設計しました。最新のオペレーティングシステムである IOS XR は、次の点でエンジニアを支援するように設計されています。

- ネットワーク全体（エッジ、アグリゲーション、コア）で、維持が容易な単一の NOS パラダイムを提供します。
- 必要な機能に基づいて配信と展開をシンプルにすることで、運用コスト（OpEx）を削減します。
- Linux スタイルのワークフローと標準 Linux ライブラリのサポートを使用して、デバイスのプロビジョニングと管理をシンプルにします。
- 管理 API の統合により業務効率を向上させ、ほぼリアルタイムの実用的なテレメトリデータを提供します。
- 自動化により、よりスムーズな導入とリモートでの設定更新を促進できます。
- ネットワーク内の信頼を検証し、サービスプロバイダーがセキュアな環境を運用できるようにします。

IOS XR のロックステップの進化

IOS XR ネットワーク オペレーティング システムは、これらの技術的移行に対応するために、継続的に進化してきました。IOS XR にはクラス最高レベルのルーティングプロトコルと機能が組み込まれ、セグメントルーティングやイーサネットバーチャル プライベートネットワーク（EVPN）などのインテントベースのトランスポートテクノロジーにも引き続き重点が置かれています。これにより IOS XR は、ネットワークセグメント全体における Web スケールのサービスプロバイダーや大規模サービスプロバイダーにとって最有力の選択肢となっています。

[1] Cisco Visual Networking Index（2017 ~ 2022 年）

また、SP ネットワークが自動運用ワークフローに移行していることを認識することが重要です。この移行により、業界全体のベンダー ネットワーク オペレーティング システムにおいて、拡張可能なオープン ソフトウェア アーキテクチャの導入が促進されています。この移行により、ネットワークスタックのすべてのレイヤーでモデル駆動型 API を使用した運用の拡張性が促進されています。IOS XR の開発は、この移行を補完することに意図的に焦点を当て、多くの重要な変更をもたらしました。

- IOS XR リリース 6.x では、32 ビット QNX オペレーティングシステムから 64 ビット Linux オペレーティングシステムに移行しました。
- プログラムによるプロビジョニングと大規模なリアルタイムのテレメトリデータによる YANG モデルの組み込みサポート。
- カスタムプロトコルとコントローラのスタックの下位層にある高性能なサービスレイヤー API により、IOS XR の機能が大幅に向上し、必要なワークフローやツールと統合できます。
- IOS XR へのゼロタッチ プロビジョニング（ZTP）機能の採用により、Day 0 の導入要件に対応します。
- IOS XR がエンドユーザーへの直接アクセスの基礎となる Linux 環境を開放したため、多数のスクリプト言語（bash、Python、Golang、C++）の統合、設定管理ツール（Ansible、Puppet、Chef など）の使用、およびコンテナ（LXC、Docker）のサポートが可能になりました。

拡張性に優れた 400G 最適化ルータを実現する Cisco® 8000 シリーズ プラットフォームの発表により、IOS XR はサポート対象プラットフォームのポートフォリオを継続的に拡大し、XRd および XRv9000 仮想ルータ、NCS 540/560、NCS 5000/5500/5700、ASR 9000、および認定されたサードパーティ製ハードウェアを使用した VNF ソリューションへの対応を促進します。IOS XR は、業界で最も包括的なプラットフォームとソリューションのポートフォリオを提供し、サービス プロバイダー ネットワークのすべてのセグメントで一貫した運用と機能を実現します。

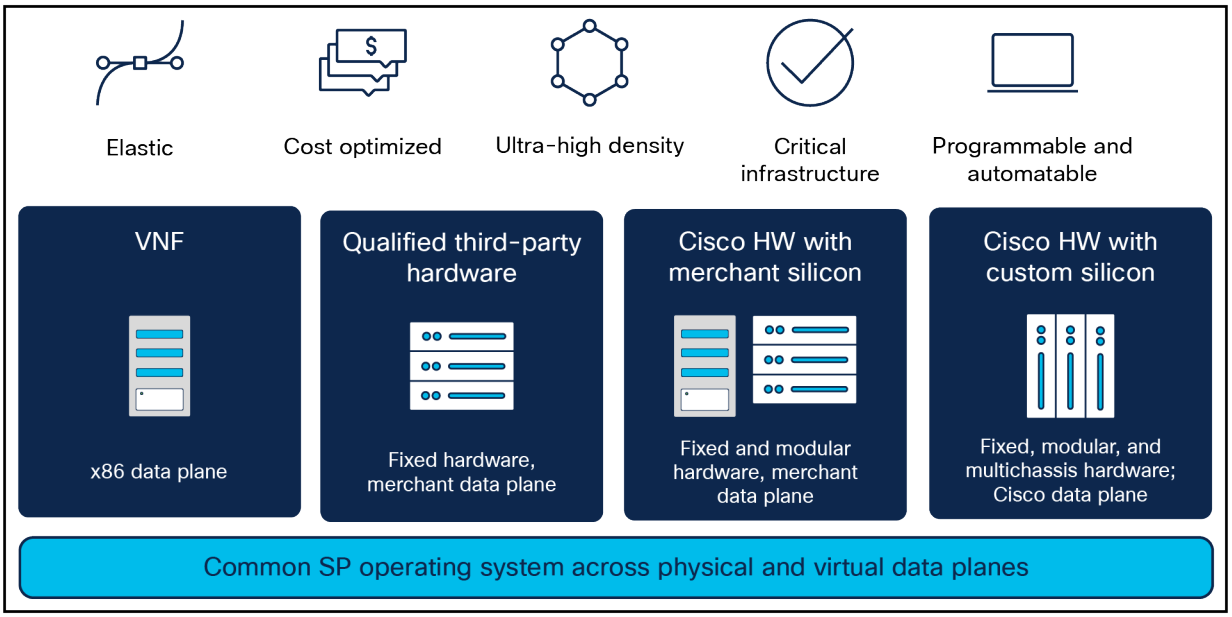

図 1.
IOS XR がサポートするプラットフォーム

IOS XR の概要：シンプル、最新、高信頼性

IOS XR リリース 7 のアーキテクチャは、これらの要件に正面から対処できるように進化しています。IOS XR アーキテクチャでは、次の 3 つの基本原則を重視しています。

シンプル

さまざまなワークフローのより容易なプロビジョニング、自動化、および統合を実現します。

1. **よりシンプルでリーンなアーキテクチャ：**IOS XR 上の新しいハードウェアプラットフォームでは、管理プレーンとシステムコンテナが存在しないため、既製のツールとスクリプトソリューションを使用してシステムをこれまでになく容易に管理できます。

2. **よりシンプルな運用：**Linux スタイルのワークフローと統合により、拡張性に優れた設定管理ツール（Ansible、Puppet、Chef）の使用と、標準 Linux アプリケーションのバイナリまたはコンテナ（LXC、Docker）としてのオンボックスでのサポートが実現されます。

3. **よりシンプルでセキュアな Day 0 ロールアウト：**RFC 8572 に基づく強力でセキュアなゼロタッチ機能により、IOS XR ルータとブートストラップサーバーの間の YANG モデルトランザクションに基づいたテンプレート駆動型 ZTP スクリプトによるセキュアなデバイスオンボーディングを実現できます。

4. **よりシンプルなソフトウェアの配信と展開：**「ゴールデン ISO」（GISO）と呼ばれるアーティファクトにより、カスタムスクリプト、アプリケーション、パッケージ、およびファイルが展開可能な ISO アーティファクトに結合されます。個々の IOS XR コンポーネントおよびパッチは、RPM を介して配信されます。

5. **IOS XR インストールの強力な新しい設計：**DNF（Dandified YUM）をベースに構築され、モジュラーシャーシシステムと YANG モデル API をサポートするように拡張された IOS XR インストールにより、オペレータは、インストールプロセスのリアルタイムテレメトリ通知をサポートしながら、IOS XR RPM、ネイティブ Linux RPM、およびゴールデン ISO（GISO）インストールのライフサイクルを管理できます。

最新

スタックのすべてのレイヤーにモデル駆動型 API があります。トランスポートテクノロジーに関して業界をリードするサポートを提供します。

1. **YANG モデルの管理レイヤー API：**デバイスのプロビジョニングと管理が自動化されます。これらのモデルには、ネイティブ IOS XR YANG モデルと OpenConfig モデルが含まれます。

2. **ストリーミングテレメトリ機能：**ケイデンスベースのモニタリングまたはイベント駆動型のモニタリングにより、管理レイヤーの YANG モデルパスから派生したデータを gRPC、TCP、または UDP を介してトランスポートとしてモニターできます。

3. **サービスレイヤー（SL）API およびオープン フォワーディング アブストラクション（OFA）API：**サービスレイヤー API は IOS XR の共通ネットワーク インフラストラクチャ レイヤー（RIB、ラベルスイッチ データベース、BFD、L2 など）の高性能な API です。この API により、コントローラやカスタムプロトコルは、たとえば IOS XR RIB でルートを操作したり、ラベルスイッチドパスをオンザフライで作成したりできます。OFA API は、ハードウェアプラットフォームの ASIC SDK 上にあるモデル駆動型 API です。この API により、ネットワークスタックの最下位レイヤーへの直接、または P4 ランタイムなどのモデル化された抽象化を介した、高性能アクセスが可能になります。

4. **セグメントルーティングと EVPN：**セグメントルーティングと EVPN は、シンプルさ、規模、およびプログラムによる拡張性を重視する IOS XR ベースのトランスポート展開の中核です。IOS XR では、SR Flex-Algo、SRV6 などのサポートの追加により、これらのテクノロジーが引き続き重視されています。EVPN は、レイヤー 2 VPN サービスとレイヤー 3 VPN サービスを含むあらゆるサービスタイプに関して統一されたコントロールプレーン プロトコル（BGP）を提供することで、さらに高度なシンプルさを実現します。

5. **ゼロタッチ API：**Day 0 自動化を実現するゼロタッチプロビジョニング用の包括的な API。これには、bash および Python ライブラリをオンボックスで使用する CLI 自動化 API が含まれます。また、IOS XR により、オペレータは、ZTP Python ライブラリのオンボックス NETCONF クライアントを使用し、YANG モデル XML 入力を介してシステムを起動することもできます。これはさらに、準備が整えばネットワークチームが CLI から YANG モデルにシステムを移行することを可能にします。

高信頼性

信頼できるセキュアなワークフローの実現には、高信頼性ネットワークデバイス上で実行される高信頼性 NOS が不可欠です。IOS XR では、次を可能にすることで、これを実現します。

1. **ハードウェアから始まる信頼：**改ざんできないセキュアなトラストアンカーモジュール（TAm）には、ハードウェアコンポーネントの既知の適正な値と、シスコをルートとするキーおよび証明書が格納されます。これらは、BIOS ブート時にハードウェアのコンポーネントを検証するために使用されます。

2. **セキュアブート：**セキュアブートプロセスを通じてネットワーク OS（IOS XR）の一部を検証することにより、信頼性が強化されます。これは、OS を起動する前に、ブートローダーとカーネルモジュールの署名を TAm のキーに対して検証することで実現されます。

3. **実行時の信頼性：**すべてのランタイムプロセスに対して IMA（整合性測定アーキテクチャ）評価チェックを適用し、それらの実行可能ファイルを TAm で維持されている整合性リストと比較することで、実行時の信頼性を維持します。すべての不一致はログに記録され、管理者はアクションを実行できます。

4. **署名付き RPM：**TAm のキーに基づいて、すべての IOS XR RPM およびサードパーティアプリケーション RPM の署名をインストール前に確認することにより、それらの RPM の信頼性が強化されます。

5. **信頼性に関する可視化およびレポート：**デバイスのライフサイクル中にシステムによって実行されるすべての信頼性検証操作を、リモート構成証明機能を使用して可視化およびレポートできます。

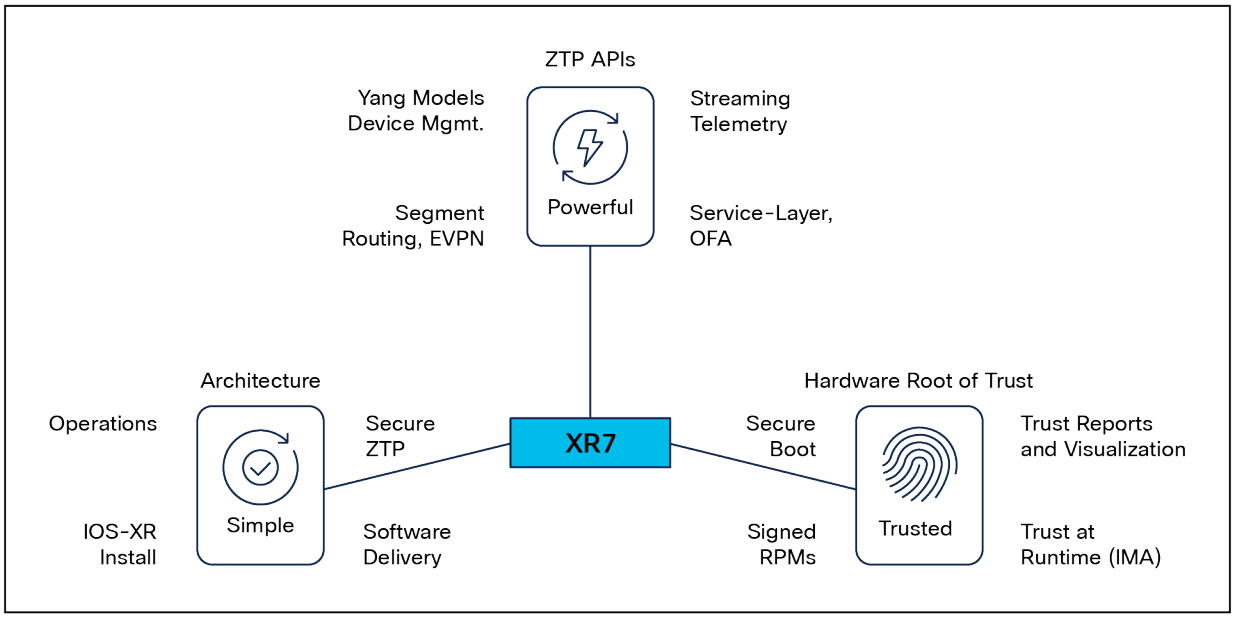

図 2.
高信頼性ネットワークデバイスで実行されている高信頼性 NOS

これらの概念についてさらに詳しく説明することで、将来の課題に対処しようとするサービスプロバイダーのニーズを満たすために IOS XR が進化しつづけることを明らかにします。

IOS XR：シンプル

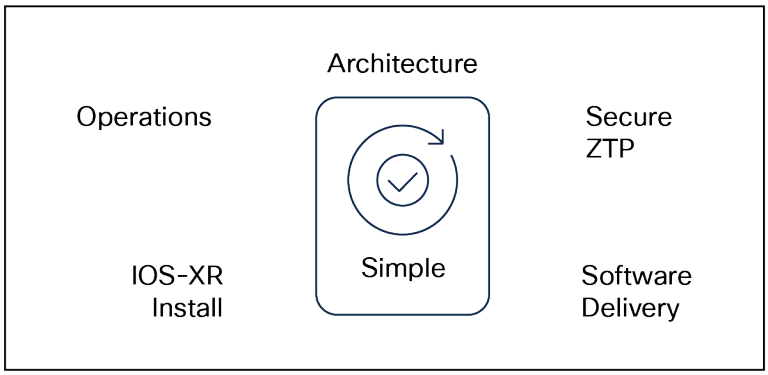

図 3.
IOS XR：シンプル

将来を見据えたシンプルなアーキテクチャ

シンプルさと使いやすさは IOS XR の背後にある基本原則の 1 部です。これらの原則はさまざまな形式で表されます。その 1 つは、Linux カーネルバージョン 4.8.28 を使用して配布できるように、IOS XR が WindRiver Linux 9 (WRL9) 上に構築されていることです。

IOS XR 6.X と比較した場合の IOS XR の主要な変更点の 1 つは、新しいハードウェアプラットフォームにおける管理プレーンの完全な廃止です。これは、IOS XR 6.X でサポートされていた、分離された XR コントロールプレーンと管理プレーンコンテナのセットアップが不要になったことを意味します。その結果、XR ソフトウェアアーキテクチャは次のようになっています。

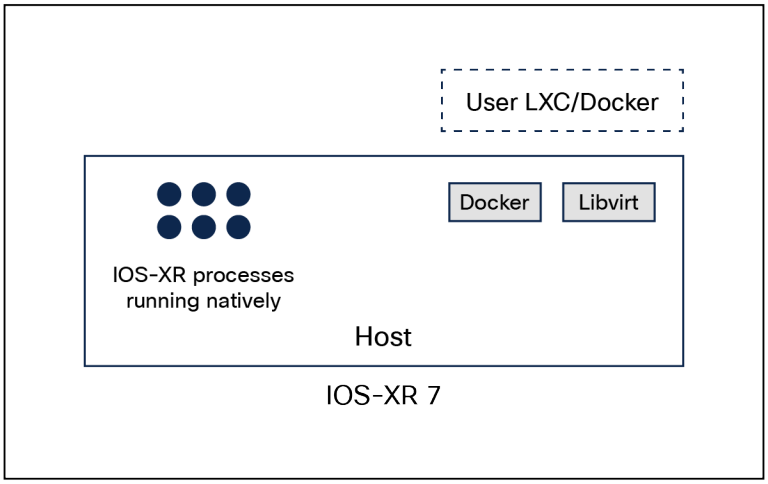

図 4.
IOS XR ソフトウェアアーキテクチャ

- IOS XR コントロール プレーン プロセスは、ホスト上でネイティブに実行されます。
- システム全体（ホストレイヤー）に対して単一の Linux シェルが存在します。
- Libvirt デーモンと Docker デーモンは、それぞれの virsh および docker クライアントとともに、すべて同じ環境（ホストシェル）で実行されます。
- 管理プレーンが排除されたことで、すべてのシステムレベルおよび環境レベルの設定とアクション機能が XR に移行されます。

Linux ワークフローのサポート

過去 10 年間で、SP のネットワーク運用は、サーバーの世界で生まれた Linux コミュニティ自動化ワークフローインストール手法を使用するように進化しました。この進化は Web スケールのサービス プロバイダー ネットワークで始まりました。そこでは、手動での操作をほとんど必要とせず、コミュニティ主導の自動化ツールまたは自社開発の自動化ツールを使用してプロビジョニング、管理、および操作するネットワークの作成に重点が置かれていました。

これらのワークフローは、Day 0 ロールアウトにも広がりました。これらの Linux の自動化により、数週間かかる可能性がある手動のデバイスオンボーディング プロセスを、Day 0 の自動化レベルに基づいて数時間で完了できるプロセスに変換できます。これらのワークフローは、ZTP（ゼロタッチプロビジョニング）のカテゴリに分類されます。これについては、後の項で詳しく説明します。

SP が使用するツールについては、Telnet の expect 形式の CLI ベーススクリプトからより確定的なモデル駆動型の SSH ベースの設定管理ツールへの大幅な変更が見られました。これらのツールは、拡張性と信頼性を向上させ、多くの場合、マルチベンダー互換性を持ちます。

効果的でありつづけるために常に進化してきた IOS XR は、アプリケーション ホスティング機能およびパケット/ IO 機能を提供します。これらの機能により、Linux のアプリケーションとツールをネイティブバイナリまたはコンテナ（LXC/Docker）としてオンボックスで実行し、それらのアプリケーションが固定シャーシプラットフォームまたはモジュラ シャーシ プラットフォームで動作中にトラフィックを送受信できるようになります。さらに、Linux 環境が機能しているために、ZTP、gRPC ベース API（サービスレイヤー、YANG モデル API）、テレメトリなどの機能が有効になりました。

ゴールデン ISO（GISO）

IOS XR を使用すると、ネットワークオペレータの運用上のニーズに合わせて、ソフトウェアをさまざまな形式で配信できます。その発想は、サーバー群で使用されている Linux ディストリビューションの基本バイナリアーティファクト（ISO）を取得して開き、すべてのサーバーでベースとして使用されるパッケージおよび設定ファイルを追加して、その組み合わせから新しい ISO を作成するというものでした。この組み合わされた ISO は、サーバーマシンに使用される「ゴールデン」設定を表すため、「ゴールデン ISO」と呼ばれます。ゴールデン ISO の作成後、設定管理ツールが引き継いで、新しくブートされるデバイスでロールベースの環境をセットアップするまでは、サーバーは PXE ブートされ、そのすべてが基本「ゴールデン」状態になります。

IOS XR には、ゴールデン ISO ビルドプロセスに導入されるいくつかの新機能があります。GISO プロセスの進化を以下に示します。

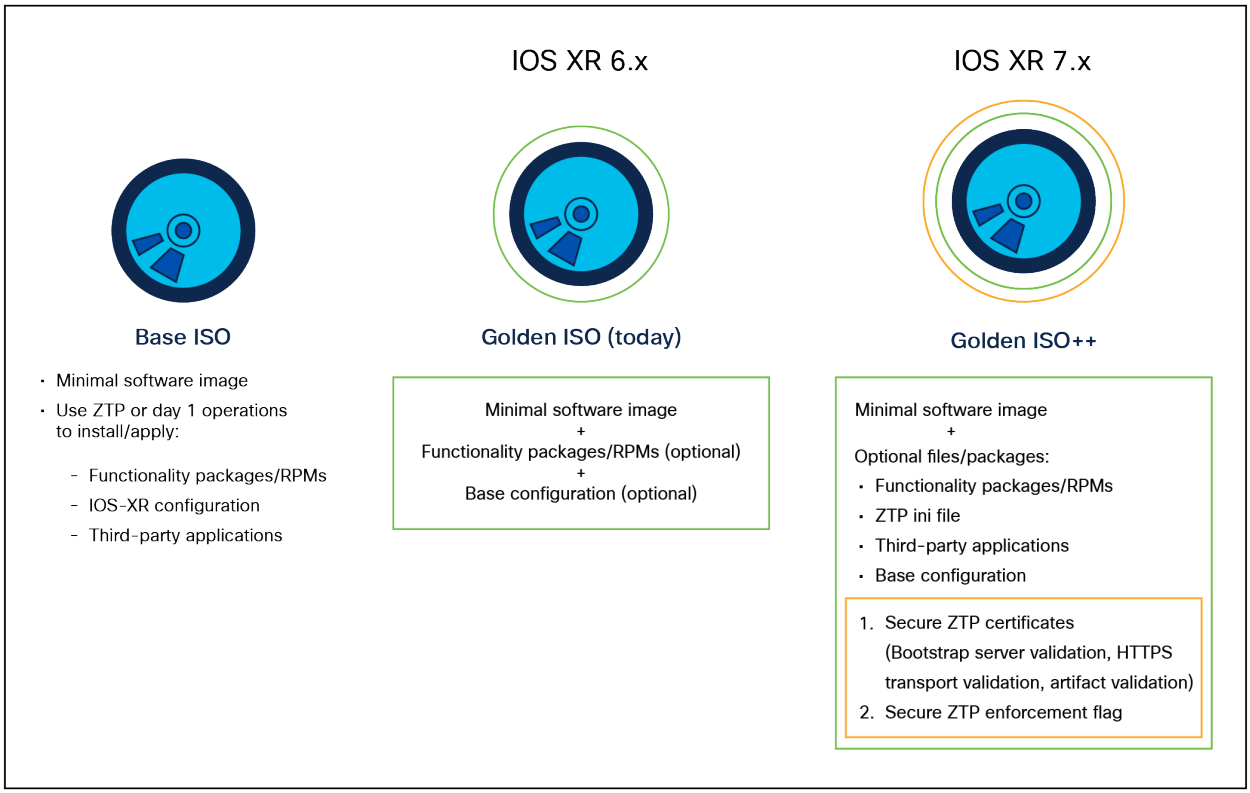

図 5.
ゴールデン ISO ビルドプロセスの進化

IOS XR では、GISO ビルドプロセスにより、次のアーティファクトを基本 ISO に追加できます。

1. **IOS XR 機能 RPM：**BGP、OSPF、ISIS、Telnet などの、IOS XR のさまざまなオプションコンポーネントの RPM です。

2. **基本設定：**有効な IOS XR 構成ファイルをゴールデン ISO に追加できます。

3. **ztp.ini ファイル：**IOS XR では、IOS XR ZTP ワークフロー用に新しいタイプのファイルが導入されます。ztp.ini ファイルは、特定のデフォルト設定を ZTP プロセス用に設定できるようにすることを目的としています。これによりユーザーは、サポートされているノブを介して ZTP ステートマシンに影響を与えることができます。

4. **サードパーティ アプリケーション RPM：**サードパーティの Linux アプリケーションは、IOS XR のゴールデン ISO ビルドプロセスでサポートされます。このために Linux アプリケーションを、基盤となる WindRiver Linux 9（WRL9）ディストリビューション用にコンパイルして RPM にパッケージ化し、「その RPM に署名して」、IOS XR インストールプロセスがブート後に RPM をインストールできるようにする必要があります。

5. **セキュア ZTP アーティファクト：**セキュア ZTP アーティファクトについては、この後の項で詳しく説明します。セキュア ZTP が機能するための基本要件は、ブート時にボックスに所有者（顧客/ネットワークオペレータ）の証明書をインストールすることです。TLS クライアント証明書（オプション）を、セキュア ZTP で必要なワークフローに基づいてパッケージ化することもできます。セキュア ZTP 強制フラグは、ZTP プロセスのステートマシンを変更するためにユーザーが指定できる設定です。これにより、セキュア ZTP を強制するか、下位互換性のあるクラシック ZTP ワークフローを有効にできます。

IOS XR のゴールデン ISO のビルドツールはオープンソースであり、次の場所にあります：
https://github.com/IOSXR/gisobuild

ゼロタッチプロビジョニング（ZTP）

IOS XR では XR のゼロタッチプロビジョニング（ZTP）が拡張され、RFC 8572（https://tools.ietf.org/html/rfc8572）に示されている要件（「セキュア ZTP」と呼ばれます）をサポートします。前述のように、ゼロタッチプロビジョニングは、今日使用されている SME およびステージング施設に関連する OpEx を削減するためにルータの Day 0 プロビジョニングを自動化しようとしているほとんどのサービスプロバイダーにとって重要なパズルのピースです。

ほとんどのアクセス展開では、ネットワークオペレータは、購入したルータを受け取り、通常、最初の「トラック」ロールアウトの一環として、それらを事前ステージング施設に渡します。事前ステージング施設では、デバイスが、通常、SME の助けを借りて手動で設定され、それらにブートストラップ設定が適用されます。これらの事前設定済みのボックスは、その後、インストールサイトに送られます。このような事前設定済みのデバイスは、多くの場合、サードパーティのインストーラを使用して簡単にセットアップし、電源を入れることができます。これが 2 番目の「トラック」ロールアウトに該当します。これは、すべてのネットワークオペレータの正確なワークフローとは言えないかもしれませんが、それらの大部分で使用されているワークフローは、ほぼこのようなものです。

事前ステージング施設での有能な SME の確保、複数のトラックロールアウト、インストール後のロールアウト、およびブートストラップ設定にエラーがあった場合の修正により、ほとんどの大規模サービスプロバイダーで OpEx が継続的に増加しています。これらの展開におけるデバイスの数が、消費者の需要と新しい 5G アーキテクチャに対応するために増えつづけていることから、OpEx を最大限に削減できる手法を見つけることが不可欠になっています。

IOS XR ZTP は、次の要件に対処できるように設計されています。

1) **ツリーベースのビルドアウト：**トポロジに依存しないようにするには、ツリーベースのビルドアウトが必要です。使用するアウトオブバンド管理ネットワークがないため、ネットワーク内のすべてのデバイスが DHCP サーバーへの L2 接続を備えているわけではありません。そこで、すでにプロビジョニングされたデバイスがツリー内の次のデバイスの DHCP リレーとして機能する必要があります。

2) **セキュリティの重要性：**アクセスデバイスは、通常、セキュアではない場所に移動するため、オンボーディングプロセス中に信頼性を確立する必要があります。大まかに言うと、これは次の要件に変換されます。

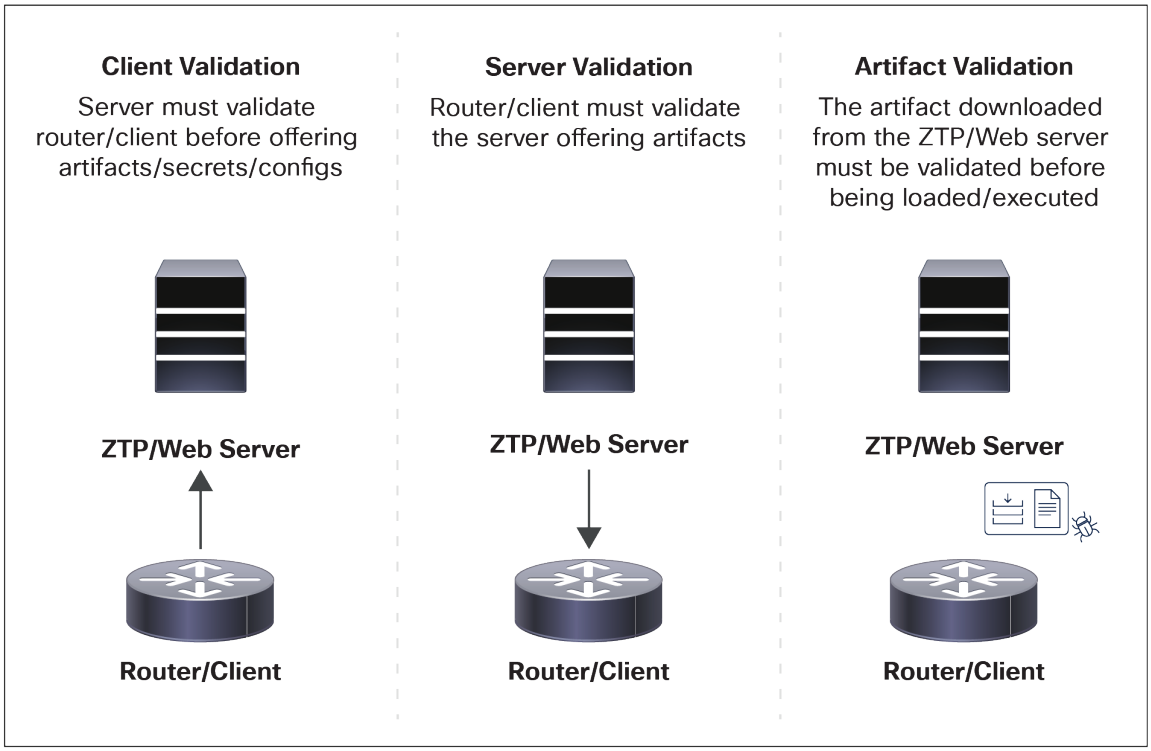

図 6.
IOS XR ZTP と信頼の確立

3) **VLAN 検出による L2 到達可能性：**多くの場合、DHCP サーバーや Web サーバーなどの初期到達可能性サービスは、レイヤー 2 メトロイーサネットクラウドを介してのみ到達可能であることがあります。アウトオブバンド管理ネットワークがないため、これらのネットワークの ZTP にはデータ（実稼働）ポートを使用する必要があります。これらのことから、レイヤー 2 クラウド全体で使用中の VLAN を検出し、正しい VLAN で DHCP 要求を適切にタグ付けする（これにより、検出後に ZTP で処理が進められる）VLAN 検出手法が IOS XR ZTP によって実装されます。

上記の目標を考慮して、IOS XR では、RFC-8572 の概念が実装され、IOS XR でセキュア ZTP 機能が実現されます。このサポートは次の 3 つで構成されます。

1) **セキュア ZTP YANG モデルのサポート：**これによりルータと RESTCONF ベース ZTP サーバーの間の相互作用が実装されて、アーティファクト（設定、スクリプト）がダウンロードされ、ルータが自動的にプロビジョニングされます。
2) **セキュアゴールデン ISO のサポート：**これにより、所有者証明書（ネットワークオペレータに関連付けられた）をパッケージ化し、ダウンロードされたアーティファクトの署名を検証して、デバイスが ZTP サーバーからの応答に基づいて参加しようとしているネットワークドメインを検証できるようになります。セキュア GISO は、オプションの TLS クライアント証明書の追加にも役立ちます。これにより ZTP サーバーへの TLS 接続を確立して、後続のやり取りを保護および暗号化することが容易になります。
3) **改ざんされないセキュア固有識別子（SUDI）を中継するオンボックス インフラストラクチャ：**これは、証明書とシリアル番号の組み合わせを ZTP サーバーに中継し、所有者の証明書とキーを保存するためのルータ上のセキュアな場所を提供するオンボックス インフラストラクチャです。

IOS XR：最新

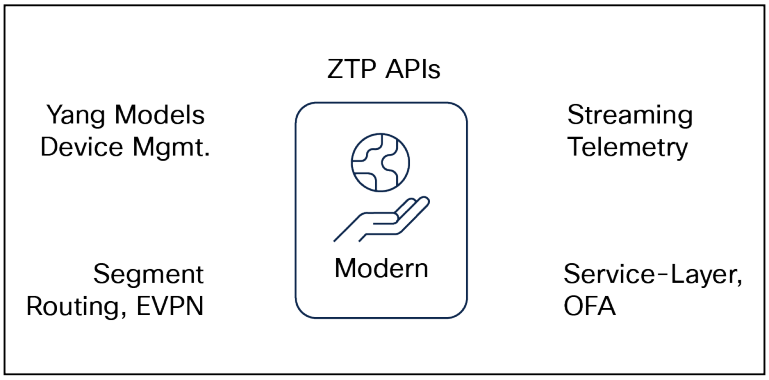

図 7.
IOS XR：最新

IOS XR では、スタック内でのプログラムおよびモデル駆動型の相互作用ポイントの構築が一貫して重視されていて、ネットワークデバイスの展開と管理を容易にする自動化可能なインターフェイスが提供されます。この設計により、外部ツール、アプリケーション、およびコントローラとの強力な統合によって IOS XR の機能を容易に拡張できます。

ただし、これらの機能の説明を API に関する話題だけで完結させることは困難です。セグメントルーティングや EVPN などのテクノロジーが進化したことで、ネットワークオペレータは、それらを活用して、従来のトランスポートネットワークを、プロトコル中心の展開（MPLS、RSVP-TE、レイヤー 2 およびレイヤー 3 VPN 展開）からこれらのテクノロジーに基づいた、よりシンプルでリーンなソリューション（多くの場合、外部コントローラおよびプランニングツールを併用）に移行させました。

そのため、進化するネットワーク運用の文脈でこれらの機能を理解することが重要です。通常、ネットワーク運用は次の 3 つのカテゴリに分類できます。

- **Day 0**：デバイスの最初のロールアウト、ZTP による自動展開、Day 1 管理およびモニターソリューションへの登録。ここでは、ゼロタッチプロビジョニング API およびインフラストラクチャが重要な役割を果たします。
- **Day 1**：ネットワークでのロールベースのデバイス設定、一元管理ソリューションおよびコントローラの立ち上げ、拡張可能な設定管理ツールと自動化を使用したアプリケーションとポリシーの大規模展開。デバイスプロビジョニングのためのモデル駆動型 YANG ベース API、デバイスモニタリングのためのモデル駆動型テレメトリ機能、サービスとポリシーをネットワークに展開するためのセグメントルーティングおよび EVPN ソリューションは、Day 1 運用で利用される重要な要素です。
- **Day N**：リアルタイムのネットワークおよびアプリケーション情報を使用してネットワーク内の状態を操作し、ネットワークの劣化の問題を修正し、アラームを発生させてメンテナンス時間をスケジュールし、ネットワークのテレメトリデータおよびパターンを分析してネットワーク設計を進化させることで将来の課題に対応します。サービスレイヤーおよびオープン フォワーディング アブストラクション（OFA）API などのハイパフォーマンスの下位レイヤー API、テレメトリを介して実装されるフィードバックループ、および YANG に基づくデバイスプロビジョニング API を活用してネットワークやアプリケーションのイベントに応答するカスタムコントローラ/アプリケーションは、Day N ソリューションの革新を促進する一般的なコンポーネントです。

上記のような API およびテクノロジーとさまざまな運用パラダイムとの対応をふまえて、これらの機能の所在を理解するために、IOS XR のネットワークスタックについて詳しく説明します。

IOS XR スタックのさまざまなレイヤーと、識別される対応機能を次に示します。

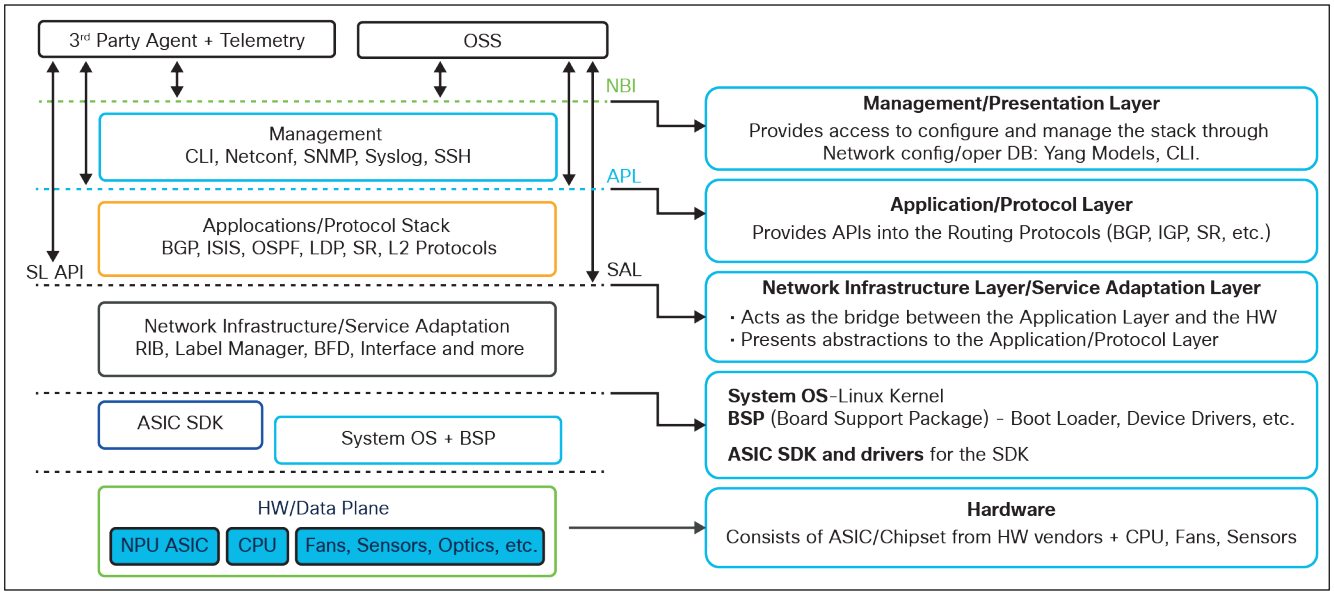

図 8.
IOS XR スタックおよび対応する機能

- **管理性レイヤー：**このレイヤーには、ネットワーク アプリケーションレイヤーの機能やプロトコルに対するコマンドライン インターフェイス（CLI）および YANG モデル API があります。これらの YANG モデルは、デバイスプロビジョニングおよびストリーミングテレメトリに使用されます。ZTP API は、このレイヤーの CLI および YANG API の上に構築されます。このレイヤーでは、「SysDB」と呼ばれる IOS XR 内の内部「データベース」が活用されます。
- **ネットワーク アプリケーション/プロトコルレイヤー：**このレイヤーには、BGP、ISIS、OSPF などのプロトコルと L2VPN、L3VPN などの機能が含まれます。このレイヤーは SYSDB とやり取りして、プロトコルや機能の動作および設定状態を保存します。セグメントルーティングと EVPN の上位レイヤーコンポーネントは、このレイヤーに分類されます。
- **ネットワーク インフラストラクチャ/サービス適応レイヤー：**通常、RIB、ラベルスイッチデータベース、BFD、ネットワーク インターフェイス ハンドラ、コントローラ/エージェント用 API などのコンポーネントで構成されます。このレイヤーの上でエンドユーザー向けに提供される API は「サービスレイヤー API」と呼ばれます。すべての XR コントロール プレーン プロトコル（BGP、ISIS、OSPF など）、セグメントルーティング、および EVPN のインフラストラクチャ コンポーネントは、このレイヤーにマッピングされます。
- **ハードウェア アブストラクション レイヤー（OFA）：**このレイヤーは ASIC SDK（ASIC ベンダーが提供）とやり取りし、RIB の状態や LSD（ラベルスイッチデータベース）の状態などに基づいてデータプレーンのプログラミングを処理します。オープン フォワーディング アブストラクション（OFA）API は、外部アプリケーション向けにこのレイヤーの機能を抽象化します。
- **プラットフォーム統合レイヤー：**通常、ファン、LED、センサーなどのデバイス用のカーネルやユーザー側ドライバで構成されます。これらのデバイス固有ドライバとソフトウェアスタックの上位レイヤーの統合は、このレイヤーで行われます。ソフトウェアスタックがセンサーから情報（温度など）を抽出し、コンポーネントの状態（ファン速度など）に影響を与えることを可能にしているのは、このレイヤーです。

IOS XR：高信頼性

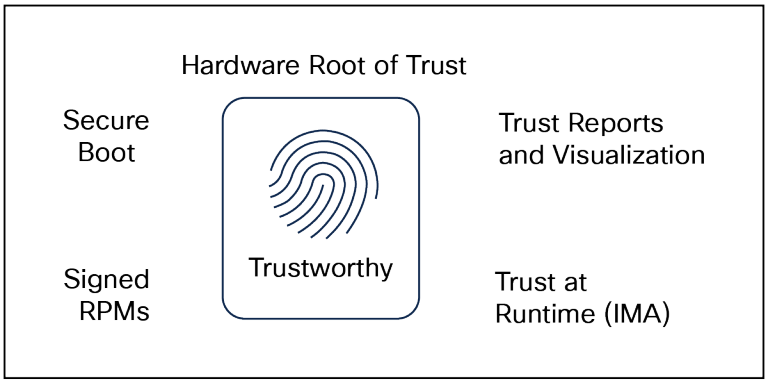

図 9.
IOS XR：高信頼性

IOS XR では、信頼性の概念が、デバイスまたは NOS セキュリティに関するあらゆる議論のテーマとなっています。IOS XR とその互換ハードウェアの目標は、デバイスと OS の整合性がセキュリティの概念と同様に重要視された「高信頼性プラットフォーム」を構築することです。実際には、そもそもセキュアであると見なせるデバイスは存在しないと認識することが重要です。これは理想的な状態ですが、必ずしも達成できるとはかぎりません。信頼性のレベルは、測定、検証、監査できます。

ネットワークデバイスのセキュリティに関連する主要な懸念事項を明確にすることが重要です。

- オペレータは、ルータが意図されたソフトウェアのみを実行していることを、どのようにして確認できますか。
- シスコが構築したルータがその後に物理的に変更されていないことを、どのようにして確認すればよいでしょうか。

署名されたソフトウェアのみのインストールと実行を許可する、ハードウェアコンポーネントの適正な値を事前に把握しておき、ブート中にそれと照合して検証する、といったセキュリティ制御をただちに構築することで、これらの懸念事項に対処できます。さらに一歩踏み込んで、証明書およびキーと検証に使用する既知の適正な値を保存する、改ざん防止機能を備えたハードウェアによってセキュリティ制御が支援されるようにすることで、完全な検証の実現が容易になります。構成証明機能を使用すると、検証結果を可視化してレポートできます。これにより、コンポーネントとネットワークが信頼できることを証明できます。

これらの懸念事項に対処するとともに、IOS XR およびその関連プラットフォーム内の信頼性パラダイムを理解するには、一般的なネットワークデバイスの信頼性のチェーンを理解する必要があります。

ハードウェアの信頼ルート

この概念はシンプルです。ブートプロセスをトレースバックする場合、信頼ルートを可能なかぎり後方にプッシュすることで、システムにおいて最高レベルの信頼性が確保されます。

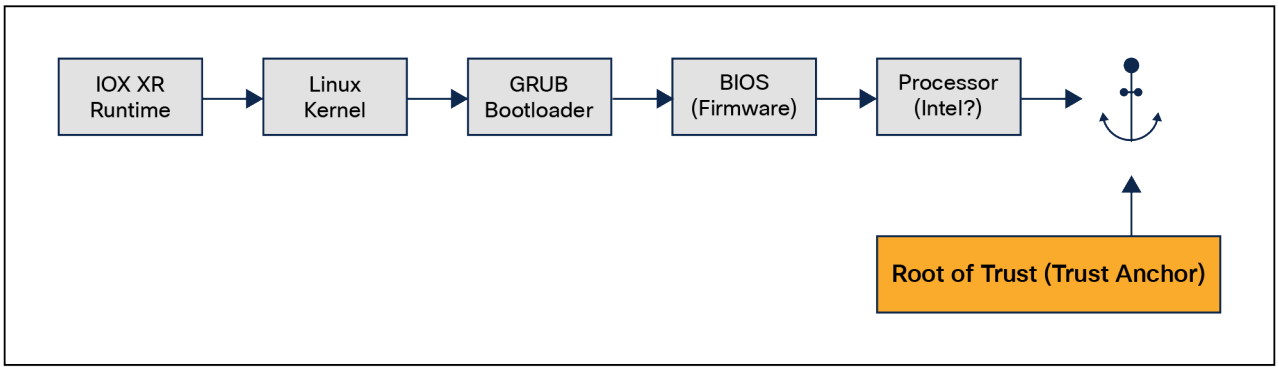

図 10.
ハードウェアの信頼ルート

ランタイム OS、カーネル、およびブートローダー（GRUB）が侵害される既知の攻撃や脆弱性が存在します。UEFI 仕様 2.3.1 では概念としてのセキュアブートが規定されています。この仕様では、BIOS 段階で信頼性が開始され、その後に、ブートローダー、カーネル、OS がチェックされることが想定されています。しかし、BIOS を侵害する可能性のある UEFI ルートキットの出現が確認されていて、セキュアブートプロセスが危険にさらされています。さらに、いずれも Intel ハードウェア上の BIOS 拡張機能である Intel ME および AMT に関するセキュリティ問題の範囲が大幅に拡大しつつあります。UEFI ファームウェアエコシステムの問題や、インプラント/ルートキットの配信およびインストールが比較的簡単であることについては、すでに研究が発表されています。

つまり、ブートプロセスを適切に保護するには、BIOS がブートする前であっても、ブートサイクルの非常に早い段階で検証チェックを開始する必要があります。IOS XR プラットフォームでは、まさにそれが行われます。シスコのハードウェア プラットフォームでは、「ハードウェアアンカー セキュアブート」と呼ばれるものが実行されます。

シスコのセキュアブートと UEFI セキュアブート

シスコのセキュアブートは、セキュアブートプロセスをハードウェアに固定することで差別化され、これにより非常に堅牢なセキュリティを提供します。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、セキュリティ体勢が強化されています。

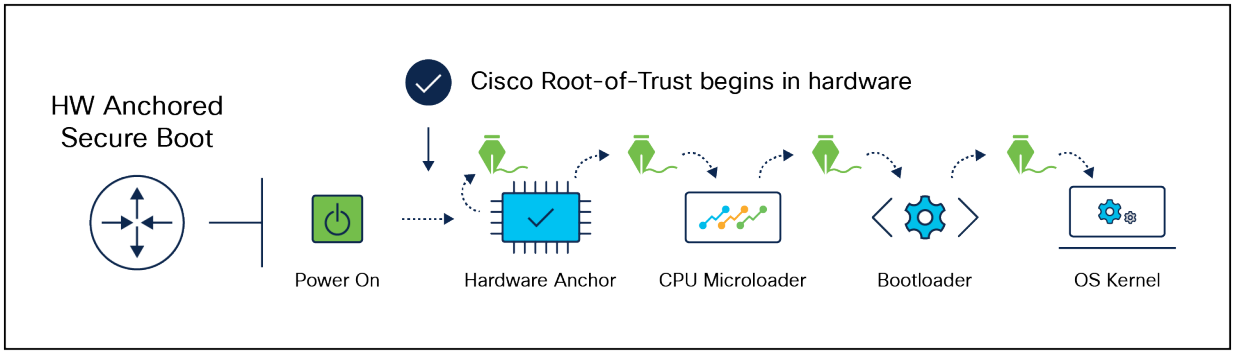

図 11.
シスコのセキュアブート

このプロセスにより、マイクロローダーからブートローダーを介してオペレーティングシステムへの「信頼のチェーン」が作成され、ソフトウェアの真正性が確保されます。デジタル署名のチェックに成功しないと、シスコのデバイスはそのソフトウェアを起動させないため、悪意のあるコードは実行されません。

シスコのトラストアンカーモジュール（TAm）と業界標準の TPM

シスコのハードウェアアンカー セキュアブートにより、ソフトウェアがシスコの正規ソフトウェアとして認証されると、オペレーティングシステムは、TAm に照会してハードウェアが本物であることを確認します。これは、TAm 内のセキュア固有デバイス識別子（SUDI）を暗号的に検証することで、シスコが提供したものであることを確認しています。

SUDI は 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特に重要です。

これに対し、業界標準の TPM は TAm と同様の機能を備えていますが、製造時に固有デバイス識別子（UDI）で永続的にプログラムされることはありません。このインスタンスでの SUDI の構築はエンドユーザーに任されており、ユーザーの操作と開発が必要です。これにより柔軟性は得られますが、不正なサプライチェーンの変更を特定できないリスクが高まります。

シスコの環境保全への取り組み

シスコの企業の社会的責任（CSR）レポートの「環境保全」セクションでは、製品、ソリューション、運用・拡張運用、サプライチェーンに対する、シスコの環境保全ポリシーとイニシアチブを掲載しています。

次の表に、環境保全に関する主要なトピック（CSR レポートの「環境保全」セクションに記載）への参照リンクを示します。

持続可能性に関するトピック	参照先
製品の材料に関する法律および規制に関する情報	材料
製品、バッテリ、パッケージを含む電子廃棄物法規制に関する情報	WEEE 適合性

シスコでは、パッケージデータを情報共有目的でのみ提供しています。これらの情報は最新の法規制を反映していない可能性があります。シスコは、情報が完全、正確、または最新のものであることを表明、保証、または確約しません。これらの情報は予告なしに変更されることがあります。

Cisco Capital

目的達成に役立つ柔軟な支払いソリューション

Cisco Capital により、目標を達成するための適切なテクノロジーを簡単に取得し、ビジネス変革を実現し、競争力を維持できます。総所有コスト（TCO）の削減、資金の節約、成長の促進に役立ちます。100 ヵ国あまりの国々では、ハードウェア、ソフトウェア、サービス、および他社製製品を購入するのに、シスコの柔軟な支払いソリューションを利用して、簡単かつ計画的に支払うことができます。詳細はこちらをご覧ください。

文書の変更履歴

新規トピックまたは改訂されたトピック	説明箇所	日付
一貫性を保つために IOS XR の名所を更新	すべてのセクション	2024 年 4 月

米国本社
カリフォルニア州サンノゼ

アジア太平洋本社
シンガポール

ヨーロッパ本社
アムステルダム（オランダ）

シスコは世界各国に約 400 のオフィスを開設しています。オフィスの住所、電話番号、FAX 番号は当社の Web サイト（www.cisco.com/jp/go/offices）をご覧ください。

Printed in USA C78-743014-02 05/24