

単一プラットフォーム フォームのパワー

長期的な価値の創出、サイバーセキュリティ、統合を目的とした設計



Axisネットワーク デバイスの原動力

AXIS OSは、大半のAxisネットワークデバイスに搭載されているLinuxベースのオペレーティングシステムです。これは、顧客サイトに導入されている200超のAxis製品や数千に上るデバイスの心臓部に当たるものです。Axis OSには、イノベーション、信頼性、シームレスな統合への取り組みが反映されています。Axisのソフトウェアにより、当社デバイスの信頼性と優れた画質を実現する能力が可能となります。そして、Axisソフトウェアは、リリースされるたびに改良が重ねられています。実際、当社の研究開発における労力の80%は、ソフトウェア開発を中心とした取り組みに注がれています。

当社は常に新たな機能を追加しながら、既存の機能を改善しているのです。当社はまた、AXIS OSに基づき構築されたデバイスの脆弱性パッチを適用することで、セキュリティを継続的に強化しています。これにより、デバイスが改善され、より安全に対応できるユースケースが増加します。

AXIS OSは、長期的な価値、高水準のサイバーセキュリティ、容易な統合というネットワークデバイスの最も重要な基準を満たせるように特別に設計されています。

Axisデバイス専用の設計

AXIS OS開発組織によってLinuxのYocto/OpenEmbeddedの安定性に基づき構築された

AXIS OSは、カメラ、スピーカー、アクセスコントロール機器といったAxisエッジデバイス固有の条件に合わせて完全に最適化されていることから、これは一般的なビルドとは一線を画します。

長期的な価値

AXIS OSにより、デバイスの常時稼働が実現します。24時間年中無休で稼働するように設計されているため、昼夜を問わず、長期的な用途の条件に対応する一貫した高応答性の性能が実現します。

堅牢なサイバーセキュリティ機能

AXIS OSの中核には、サイバーセキュリティへの取り組みが据えられています。セキュリティアーキテクチャーが組み込まれたAXIS OSにより、組織のデバイスを保護することができます。安全なソフトウェア開発手法と慎重な脆弱性管理によって構築されたAXIS OSを活用することで、新たな脅威に備えてデータとデバイスの回復力を確保することが可能となります。

スムーズな統合

AXIS OSはONVIFなどの規格に準拠し、VAPIXを搭載していることから、Axisネットワークデバイスは多様なエコシステムに容易に統合することができます。この統合性により、ユーザーと開発者はスムーズで相互接続されたエクスペリエンスを得ることが可能です。

数字で見るAXIS OS

開発者数 : 900

コードの行数 : 24,000,000

1日あたりのコードのコミット数 : 4,000

1日あたりの自動テストの回数 : 4,000,000

アクティブトラックがサポートされているAxis製品の数 : 200+

LTS（長期サポート）トラックがサポートされているAxis製品の数 : 500+

年間のアクティブトラックのソフトウェアリリース数 : 6+

ソフトウェアコンポーネント数 : 2000+

オープンソースコンポーネントの数 : 95%以上

エッジ専用の設計
単一のプラットフォーム

Axisデバイス 専用の設計

AXIS OSは、エッジデバイスの性能、統合、セキュリティ、ソフトウェアの品質に特に焦点を当てて設計されています。

LinuxのYocto/OpenEmbeddedの安定性を基盤として構築されたAXIS OSは、すべてのAxisネットワークデバイスに使用できる単一の統合プラットフォームとなります。これにより、さまざまな製品全体で、一貫したエクスペリエンスが実現します。

次ページでは、特別にエッジデバイスに焦点を当てて構築されたオペレーティングシステムの価値、およびこの単一のプラットフォームの能力を詳しくご紹介します。



エッジ専用の設計
単一のプラットフォーム

エッジの卓越性を実現する設計

今日は汎用ソリューションが主流となっていますが、AXIS OSは単なるLinuxオペレーティングシステムの1つではありません。汎用Linuxビルドの慣例を打開したこのOSは、エッジデバイスの特定ニーズに合わせて細かく調整されたソリューションです。この専門化により、Axis製品固有の性能、信頼性、セキュリティが実現するのです。

Linux Yoctoが基盤

LinuxのYocto/OpenEmbeddedの堅牢な基盤により、安定性と効率性が保証されます。LinuxのYocto/OpenEmbeddedでは、開発者は使い慣れた環境で開発に取り組むことができます。これが、Axisネットワークデバイスのスムーズな動作を実現する基盤となります。

チップセットの柔軟性

汎用性がAXIS OSの特徴です。大半のAxisデバイスで、Axis ARTPECチップセットが専用にサポートされています。また、サードパーティ製のチップとも互換性があります。そのため、広範なネットワークデバイスでAXIS OSの能力のメリットを活かすことができます。

長期的な価値を考慮した設計

当社は、末永く正常に動作するデバイスを提供することに取り組んでいます。そのため、AXIS OSは堅牢かつ高い持続可能性を念頭に置いて構築されています。当社はまた、高い透明性を持って、当社デバイスの平均寿命をaxis.comで公開しています。

目的に合わせた厳格なテスト

その特定の目的において優れた性能が発揮されるように、AXIS OSには厳格なテストが実施されています。性能、サイバーセキュリティ、統合に関して期待を上回る成果を実現するため、当社は徹底的なテストを課しています。

ソフトウェアの品質

AXIS OSは、妥協のないソフトウェア品質を追求する当社の姿勢の賜物と言えます。このオペレーティングシステムは、Axisデバイスの長い耐用期間にわたって、高信頼性かつ安全で馴染みあるユーザーエクスペリエンスを実現できる高水準を達成することを念頭に設計されています。

エッジ専用の設計
単一のプラットフォーム

単一プラットフォームのパワー

卓越性に対する当社の取り組みは製品カテゴリーを超えて浸透しており、それがこの単一プラットフォームのパワーとして具体化されました。装着式カメラから防爆ソリューション、PTZカメラやサイレン、そしてスピーカー、インターコムに至るまで、200超の製品をサポートするこの統合プラットフォームは、パートナーや顧客にメリットを提供することを目的としています。

一貫性のある動作

AXIS OSは、さまざまな製品に搭載されています。つまり、すべての製品でAPIと動作が共通しているということです。プラットフォームが単一であることから、インテグレーターや開発者は、デバイス固有の複雑なドライバーを使うことなく、新しいAxisデバイスをシステムに組み込むことができます。これにより、統合が高速化されるだけでなく、将来性のあるソリューションをより迅速に開発することが可能となります。その結果、刻々と拡大を続けるAxisエコシステム内で、新製品を迅速に導入することができるのです。これによってエンドユーザーに均一なエクスペリエンスを確実に提供することが可能となります。また、すべての統合ソリューションがすべてのAXIS OSデバイスで動作するため、開発者の時間と費用の節約が実現します。

複雑性を排除した汎用性

単一のプラットフォームには、複雑性を排除しながら1つのプラットフォームで多様性を実現できるというメリットがあります。PTZカメラを監視システムに統合する場合、スピーカーをインテリジェント音声ソリューションに組み込む場合など、そのニーズに関わらず、一貫したプロセスで目的を達成することができます。互換性の枠を超越して拡張したこの汎用性により、調和のとれたエクスペリエンスだけでなく、固有のニーズに合う統合ソリューションを構築できる可能性が高まります。

統合セキュリティ

サイバーセキュリティが最優先される環境において、単一のプラットフォームには、製品範囲全体にわたって統合ソリューションをサポートできるというメリットがあります。製品ごとに難しい課題に対応している場合は、セキュリティを維持することが困難になります。1つの脆弱性を特定してこれに対処すると、その修正がサポートされているすべての製品に適用されます。これにより、セキュリティ管理を合理化できるだけでなく、新たな脅威に容易かつ迅速かつ集団的に対応できるようになります。また、これが時間やリソースの節約につながり、Axisエコシステム全体の回復力も強化されます。



長期的な価値

AXIS OSにより、デバイスのライフサイクル全体を通じて予測可能な価値が創出されます。安定した堅牢なアーキテクチャーにより、ダウンタイムを最小限に抑えることができます。

最新の機能を含め、当社は末永くソフトウェア更新を提供しています。豊富な文書や資料、便利なツール、直感的なインターフェースを備えたAxisデバイスは、使いやすだけでなく、メンテナンスも容易に行うことができます。また、当社は透明性と信頼性の高いリリーススケジュールを提供しているため、各組織のニーズに合わせてメンテナンスを計画することが可能となります。

次ページでは、Axisソフトウェアの品質、AXIS OSライフサイクル管理、ソフトウェアサポートを詳しくご紹介します。

ソフトウェアの品質
デバイスのライフサイクル
ライフサイクルサポート
トラックの選択

ソフトウェアの品質
デバイスのライフサイクル
ライフサイクルサポート
トラックの選択

信頼できる ソフトウェア

当社は、AXIS OSの品質を非常に重視しています。約900人の開発者により、1日あたり4,000行のコードがメインブランチにコミットされているAXIS OSは、市場のニーズに対応するために継続的に変革を続けています。200超の製品ごとに1日あたり2つのビルドということは、年間で18万2,500という驚異的な数のビルドになります。これにより、反復的なテストや付加価値の創出が可能となります。

厳格なテスト

安定性の高いソフトウェアを構築するには、厳格なテストが不可欠となります。実際、当社のシステムでは、1日あたり400万件に上る多様なテストが実行されています。その上、当社は1日あたり4,000行超のコードをコミットし、脆弱性のパッチ適用と品質の向上を図っています。これを年間で考えると、合計10億以上のテストと100万行以上のコードのコミットが行われている計算となります。また、データ共有を通じて、当社は顧客やパートナーからAXIS OSに関する直接的なフィードバックを募っています。

継続的改善

AXIS OSは、静的なものではありません。これは常に動的に改善されています。AXIS OSアクティブトラックを備えたAxisデバイスは、定期的な更新と機能強化を通じて、技術の進歩に合わせて進化しています。つまり、今日購入する製品には今後も新しい機能が追加され、耐用期間を通してその価値が高まるということです。



ソフトウェアの品質
デバイスのライフサイクル
ライフサイクルサポート
トラックの選択

デバイスのライフサイクルのサポート

AXIS OSを使用するメリットの1つとして、インストールからメンテナンスや交換に至るまでのデバイスのライフサイクルをサポートできることが挙げられます。AXIS OSの場合は、Axisデバイスの耐用期間を通して管理および最適化を図る上で有用となるツールとリソースが提供されます。

容易なインストールと構成

AXIS OSにはプロセスを案内するウィザード、テンプレート、プロファイルが備わっているため、Axisデバイスのインストールと構成が簡素化されます。また、AXIS Device Manager (ADM) と AXIS Device Manager Extend (ADMX) を活用することで、複数のデバイスを一度にインストールおよび構成することが可能となります。これにより、時間と労力の節約が実現します。

継続的な監視と診断

顧客の同意の下、AXIS OSではログ、レポート、アラートによってヘルスマonitoringデータが収集され、Axisデバイスの性能とステータスが監視および分析されます。これは、問題を特定して解決する上で有益となります。また、これにより、当社はリリースごとにソフトウェアを改善していくことができます。

長期的なサポートと互換性

AXIS OSでは、定期的なセキュリティパッチとバグ修正により、Axisデバイスの長期サポートが提供されます。当社は長期サポートにより、変更や中断を最小限に抑えることで、Axisデバイスとアプリケーションの互換性を維持しています。通常、AXIS OSを実行するデバイスの耐用期間は約10年超となります。状況に応じて、当社は最長で13年間サポートを提供します。

信頼性と献身性

AXIS OSは、信頼性と品質を重視する顧客の期待とニーズを満たすように設計されています。各製品においてAXIS OSの明確な耐用期間が高い透明性を持って設定されており、可能な限りその予定に沿って製品が維持されます。可能な限り最高のサービスとサポートを提供するAxisは、顧客と長期的な関係を築いています。

AXIS OSベータ版

製品を正式にリリースする前に、AXIS OSの最新機能をテストおよび評価することを望む開発者やインテグレーターにとって、AXIS OSベータ版は非常に有益です。AXIS OSベータ版を活用することで、特定のデバイスで早期互換性テストを実行すること、今後のセキュリティ更新を確認すること、そして今後の機能にアクセスすることが可能となります。

AXIS OSベータ版を活用することでもたらされるメリットの例:

- > エッジ分析、IoT接続、プラットフォームのモジュール化など、将来的にAXIS OSに搭載される新機能や改良された機能を内覧できる。
- > AXIS OSの開発と改善に有用となるフィードバックや提案をAxisに提供できる。
- > 今後のAXIS OSの変更や更新に合わせてアプリケーションとシステムを準備および適応させることで、潜在的な問題を回避できる。

こちらで、AXIS OSベータ版の詳細をご覧ください。



ソフトウェアの品質
デバイスのライフサイクル
ライフサイクルサポート
トラックの選択

AXIS OSライフサイクルソフトウェアのサポート

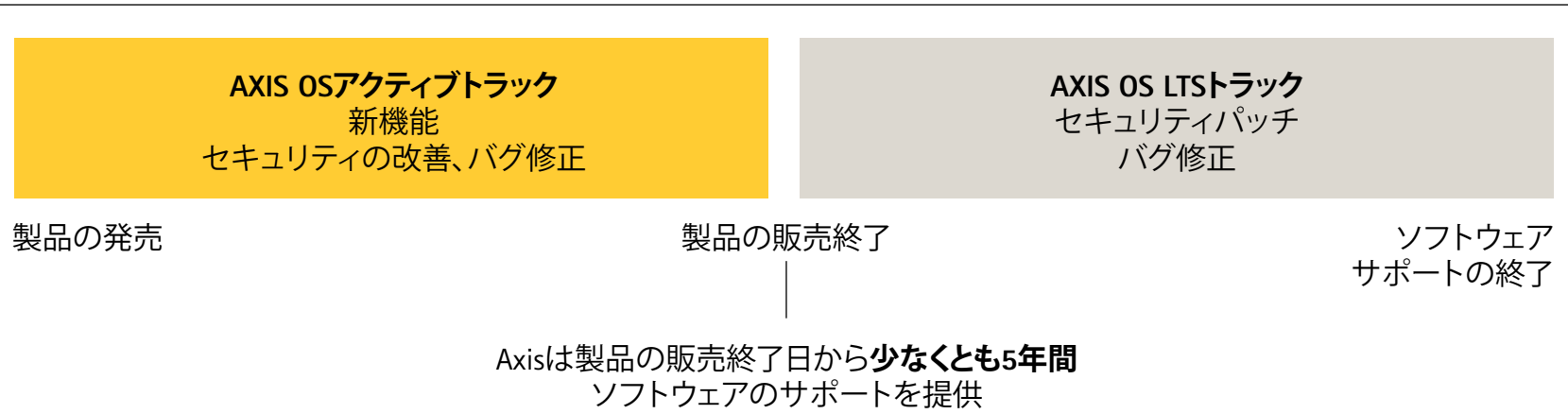
AXIS OSライフサイクルサポートは、さまざまなトラックで構成されています。積極的かつ長期的なサポートがメイントラックとなります。個々の製品ライフサイクルに対応するPSS（製品固有のサポートトラック）も提供されています。

Axisデバイスの耐用期間は、最小の期間でも業界の平均を上回っています。堅牢な5年間のハードウェア保証は、長年にわたるAXIS OSソフトウェアのサポートによって補完されます。大半のデバイスのAXIS OSの耐用期間は8～12年となります。

仕組み:

1. Axisがリリースした新規デバイスには、AXIS OSアクティブトラックのみが適用されます。リリース後の最初の期間は、新機能を含め、継続的な更新と改善が提供されます。
2. 製品のリリースから2年以内に、アクティブトラックの代替としてLTS（長期サポート）トラックが提供されます。この時点で、アクティブトラックかLTSトラックのいずれかを選択することができます。LTSトラックが適用された製品のサポートは、パッチとバグ修正のみとなります。
3. リリースから2～4年後にデバイスの製造・販売が中止されると、そのデバイスのアクティブトラックも同様に廃止されます。この時点で、すべてのデバイスが自動的にLTSトラックに移行され、最低5年間にわたってパッチとバグ修正のサポートが提供されます。

AXIS OSライフサイクルソフトウェアのサポート ソフトウェアのサポート（8～12年）



ソフトウェアの品質
デバイスのライフサイクル
ライフサイクルサポート
トラックの選択

適したソフトウェア サポートトラック の選択

アクティブトラックとLTSトラックの両方が利用可能な状態になった時点で、顧客はAxisのガイドランスに従って、そのニーズに最も適したトラックを選択することができます。

アクティブトラック

AXIS OSアクティブトラックにより、AXIS OSの最新かつ機能豊富なエクスペリエンスが得られます。これは新しくリリースされたデバイスで利用できる唯一のトラックで、最新の機能や拡張機能を直ちに利用することで得られるメリットを欲している顧客向けに構成されています。これにより、ユーザーは進化するデバイス機能を常に利用できるようになります。このトラックを利用すること

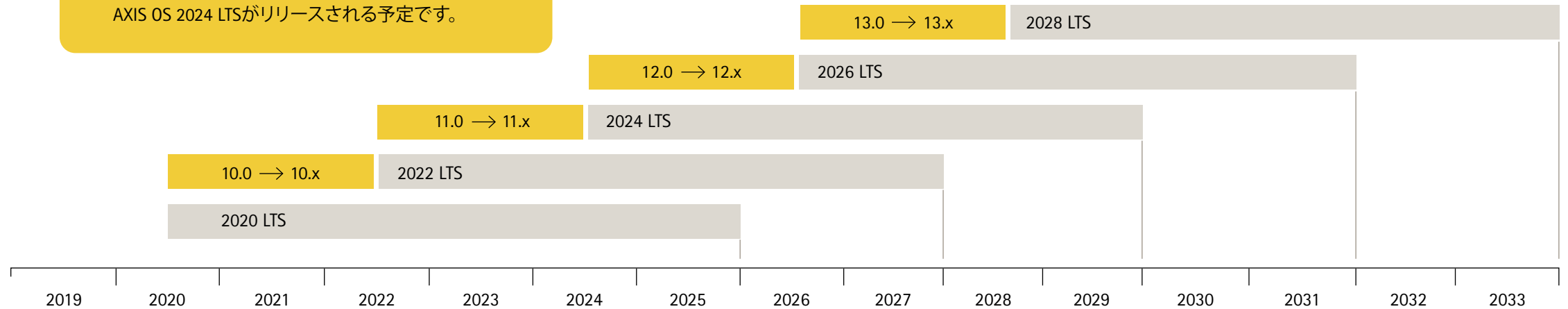
で、新規サイバーセキュリティ機能が追加され、より安全な操作が可能となるだけでなく、既存の機能も継続的に強化されます。AXIS OSアクティブトラックをデバイスに適用することで、購入後何年経っても追加費用なしで製品を最大限に活用することができます。互換性に依存していない場合は、これが最適なトラックと言えます。

LTSトラック

APIの一貫性と互換性が必要な場合は、LTS（長期サポート）トラックが利用可能な時点でこれを選択することが勧められます。下位互換性に重点が置かれているLTSトラックでは、定期的なセキュリティパッチとバグ修正が提供

されます。新しいセキュリティ機能は提供されませんが、これによってサイバーセキュリティを維持することができます。このトラックの場合は、新しい機能を追加することではなく、中断の抑制を目的として変更を最小限に抑えることに焦点が当てられています。LTSトラックは、信頼性と品質を重視し、適切に統合されたサードパーティシステムが必要な顧客に適しています。それぞれのLTSトラックは5年間のサポートで、定期的なアクティブトラックの発表に基づいて24カ月ごとにリリースされます。製造・販売が中止されたデバイスはすべて、自動的にLTSトラックに移行されます。

AXIS OSのアクティブトラックとLTSトラックの年表が示されている下図をご覧ください。ほぼ24カ月ごとに、新しいAXIS OSメジャーバージョンが発表され、新たなLTSトラックがリリースされています。たとえば、2024年にオペレーティングシステムが現在のAXIS OS 11からAXIS OS 12に切り替えられ、新たなAXIS OS 2024 LTSがリリースされる予定です。



サイバーセキュリティへのフォーカス

AXIS OSは、設計段階でセキュリティを組み込んでデバイスを開発するという一貫したアプローチにより誕生したオペレーティングシステムです。

開発プロセスとツールを定義する当社のAxisセキュリティ開発モデル（ASDM）により、ソフトウェア開発時とそれ以降の脆弱性のリスクを軽減することができます。

当社のハードウェアベースのサイバーセキュリティプラットフォーム「Axis Edge Vault」には、顧客がロードした暗号化キーの耐タンパー性ストレージとセキュアブート機能が備わっています。AXIS OSコアソフトウェアは、十分にテストされたオープンソースのコンポーネントで構成されています。また、すべてのリリースに伴うソフトウェア部品表（SBOM）により、AXIS OSが最新の状態であること、および既知の脆弱性のパッチが適用されていることを確認することができます。

AXIS OSは、特にエッジデバイスのセキュリティに焦点が当てられているETSI EN 303 645に準拠し、この規格の認証を取得しています。また、FIPS 140に準拠していることで、NIST（米国国立標準技術研究所）が発行している最新の暗号化標準規格にAXIS OSが準拠していることが保証されます。さらに、CVE採番機関（CNA）の認証を取得している当社は、脆弱性の特定、管理、開示に関するベストプラクティスに従っています。

次ページでは、Axisセキュリティ開発モデル、Axis Edge Vault、脆弱性管理、統合セキュリティの概念を詳しくご紹介します。

ASDM
内蔵サイバーセキュリティ
脆弱性管理
オールインワン

ASDM

内蔵サイバーセキュリティ

脆弱性管理

オールインワン

セキュリティを念頭に置いた開発アプローチ

Axisセキュリティ開発モデル(ASDM)に従うことで、サイバーセキュリティをソフトウェア開発ライフサイクルに効果的に統合することが可能となります。これには、ソフトウェア開発段階で考慮すべきセキュリティに関する説明が含まれています。これは、サイバーセキュリティのベースラインを確立し、ガイダンスを提供することで、脆弱性と開発コストを削減することを目的とするものです。

Axis独自のASDM

Axisセキュリティ開発モデルは、標準的な「既製」フレームワークではありません。当社は、ISO 27001、IEC 62443、NIST、BSIMM、CMMCなど、多くのサイバーセキュリティ規格やフレームワークをチェックしています。こうした規格や標準に見られる共通点として、開発段階からセキュリティが組み込まれていることが挙げられます。当社はこれを起点として、当社の企業文化、開発慣行、提供する製品の種類に合わせて独自のモデルを構築したのです。

ASDMツールボックス

ASDMツールボックスには、異なるセキュリティ問題に対処するさまざまな措置が規定されています。数例として、リスク評価、脅威モデリング、脅威モデルテスト、静的コード解析、脆弱性スキャン、ベンダー評価などが挙げられます。開発するソフトウェアの種類に応じて、開発部門は焦点を当てる措置を選択します。単にプロセスに準拠することではなく、サイバーセキュリティを向上させることが目標となります。

外部の専門知識によるメリットの向上

安全なソフトウェア開発の重要課題に主に対処しているのは、Axisの研究開発部門とソフトウェアエンジニアです。しかし、外部組織の経験や専門知識が有益に働く場合もあることを当社は認識しています。そのため、当社は侵入テストを専門企業に委託しています。当社はまた、AXIS OSのバグバウンティプログラム(脆弱性報奨金制度)により、脆弱性の特定に貢献したセキュリティ研究者に金銭的な報酬を提供しています。



ガバナンス

トレーニング

ASDMラインミーティング

ASDMの評価

セキュリティのコンプライアンスと標準

要件	設計	実装	検証	導入
リスク評価 ベンダー評価 データプライバシー オープンソースのセキュリティ評価	脅威モデリング	静的コード解析 ソフトウェアコンポジション解析	脅威モデルテスト 外部侵入テスト 脆弱性スキャン 内部セキュリティ評価	脆弱性管理 インシデント管理 製品/ソリューションセキュリティステータス バグバウンティプログラム

ASDM
内蔵サイバーセキュリティ
脆弱性管理
オールインワン

内蔵サイバーセキュリティ

徹底的な保護

Axis Edge Vaultは、ハードウェアベースのサイバーセキュリティプラットフォームです。これは、ネットワークにおけるAxisデバイスの信頼性を保証する強固な基盤となるものです。しかし、このように強力なハードウェアベースの基盤があっても、その可能性を最大限に引き出すオペレーティングシステムがなければ何ものなりません。Edge Vaultプラットフォームから最大の能力を引き出すAXIS OSがあれば、より強力なエッジセキュリティがあらゆるユースケースで実現します。

Edge Vaultの機能:

安全なキーストレージ

セキュアキーストアには、暗号化キーの安全な保管と計算を実現する暗号コンピューティングモジュールが含まれます。これにより、デバイスが侵害された場合でも、デバイスIDや他の機密情報を不正アクセスから保護することができます。搭載されている暗号コンピューティングモジュールは、SoC(システムオンチップ)に組み込まれたTEE(Trusted Execution Environment)およびプリント基板(PCB)に別個に配置されたチップである専用セキュアエレメントまたはTPM 2.0(Trusted Platform Module 2.0)です。

署名付きOSとセキュアブート

署名付きOSとは、デバイスソフトウェアイメージにコード署名が施されたOSを指しています。署名付きOSとセキュアブートの組み合わせにより、正規のAXIS OSシステム以外ではデバイスをダウンロードまたは実行することができなくなります。これにより、ソフトウェアとハードウェアのサプライチェーンにおける改ざんを防止する保護層が追加されます。

AxisデバイスID

IEEE 802.1ARに準拠したAxisデバイスIDにより、ネットワークにおける安全なデバイスの特定とオンボーディングが可能となります。これは、製造されたAxisデバイスすべてのパスポートとしての役割を果たします。

EFS(暗号化ファイルシステム)

ファイルシステムを暗号化することで、システムインテグレーターからエンドユーザーへの転送中など、デバイス未使用時にファイルシステムのデータが抽出または改ざんされるリスクを排除することができます。

署名付きビデオ

署名付きビデオにより、ユーザーはキャプチャーしたビデオの真正性を検証し、改ざんされていないことを確認することができます。



Axis Edge Vaultサイバーセキュリティプラットフォーム

暗号コンピューティングモジュール	機能	ユースケース
セキュアエレメント TPM 2.0 SoCセキュリティ(TEE)	セキュアブート 署名付きOS AxisデバイスID セキュアキーストア 署名付きビデオ EFS(暗号化ファイルシステム)	高信頼性のデバイスID 安全なキーストレージ ビデオの改ざん検知 サプライチェーンの保護

* 注意: すべてのデバイスモジュールがすべてのAxis Edge Vault機能でサポートされているわけではありません。データシートまたはAxis製品セレクトターを使用して、特定の製品でサポートされている機能を確認してください。

ASDM

内蔵サイバーセキュリティ

脆弱性管理

オールインワン

脆弱性管理

顧客が危険に曝されるリスクを最小限に抑えることを目的として、当社は業界のベストプラクティスに従い、高い透明性を持って脆弱性の管理と対応を実施しています。

業界最高の脆弱性管理

Axisが提供する製品やサービスに脆弱性が皆無であることを保証することはできません。これは当社に限ったことではなく、すべてのソフトウェアやサービスに共通する課題です。しかし、当社はあらゆる段階で潜在的な脆弱性を特定して軽減することで、顧客環境でAxisの製品とサー

ビスを展開する際に発生し得るリスクを抑制することに全社を挙げて取り組んでいます。

CVE採番機関

Axisは、CNA (CVE [Common Vulnerability and Exposures] Numbering Authority) 採番機関として認定を受けています。CVEプログラムに参加している当社は、志を同じくする企業と協力を図りながら、脆弱性管理の改善に取り組んでいます。当社は、CVEを管理する非営利団体 (MITRE) による国際的なフレームワークや公的な脆弱性管理ポリシーに合わせて脆弱性の処理、開示、パッチの適用方法を調整しています。

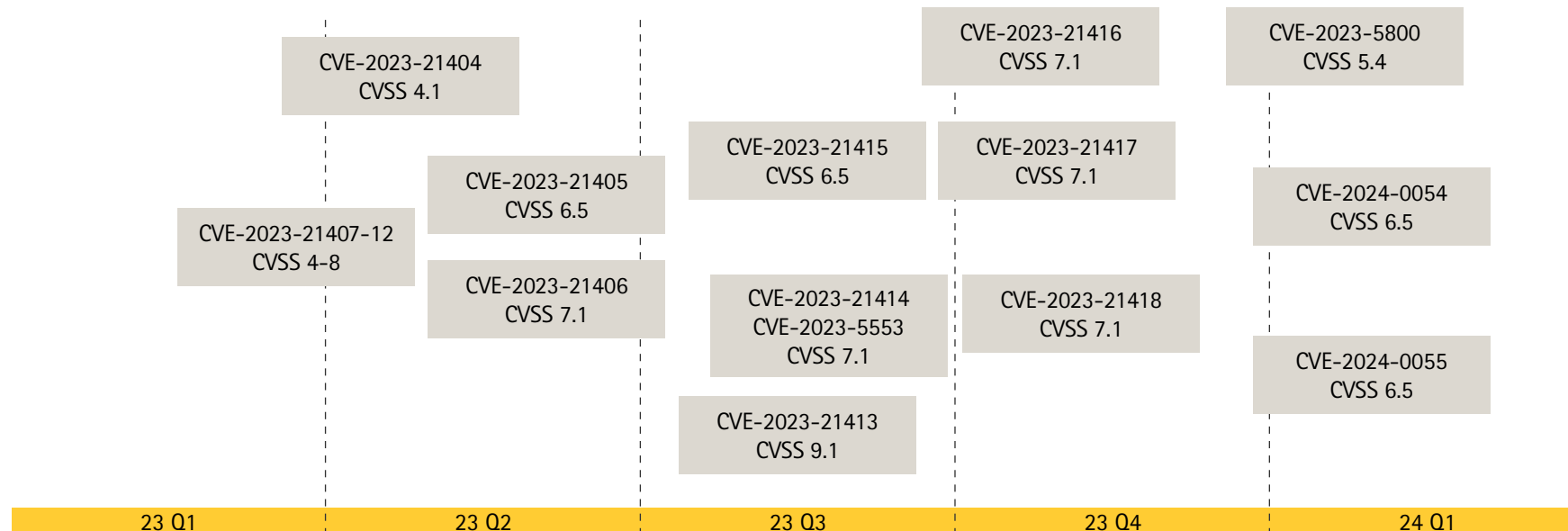
透明性の高い高信頼性の管理

Axisは、よく知られているCVSS (共通脆弱性評価システム) を使用して、Axisが開発したコードやサードパーティのオープンソースコードに関連する脆弱性を評価しています。また、ベストプラクティスの推奨事項を適用する場合に、当社製品との関連性の高さに応じて、そのオープンソースコードの脆弱性を評価しています。Axisセキュリティ通知サービスに登録すると、Axis製品の脆弱性などのセキュリティに関する情報を受け取ることができます。

セキュリティ研究者や組織とのパートナーシップ

当社は、脆弱性を当社に報告してくれる個人のセキュリティ研究者やセキュリティ研究組織の意見を貴重なものと捉え、感謝の気持ちを持って受け入れています。そして、その脆弱性を躊躇なく公開し、パッチを適用しています。脆弱性が明らかになった経緯に関わらず、責任ある倫理的な開示プロセスを通して、高い透明性を持ってその脆弱性を適切に処理することが重要なのです。

AXIS OSの脆弱性



Axisが公開した
AXIS OSの脆弱性

ASDM
内蔵サイバーセキュリティ
脆弱性管理
オールインワン

オールインワンのセキュリティ措置

AXIS OSを搭載したネットワークデバイスでは、ハードウェアコンポーネントとソフトウェアコンポーネントが連携して機能するため、顧客は安全にデバイス、サービス、接続先のシステムを使用することができます。包括的な保護層は、セキュリティ基盤とハードウェアベースのセキュリティプラットフォームを根底に、ソフトウェアまで保護層が続く形態で構成されています。AXIS OSを搭載したデバイスは、多層防御のサイバーセキュリティアプローチによって保護されます。これにより、データ、アプリケーション、プロセスのセキュリティが累積的に強化されるという仕組みです。

そのため、Axisデバイスの用途に関わらず、保護と安全な通信が実現することから、安心してサードパーティシステムに適切かつ安全に統合することができます。

アクセスコントロール

アクセスコントロールの管理

複雑なパスワードのインジケータによるローカルユーザーデバイス管理
OpenID Connect (RFC6749, 1.3.1 認可コード)に基づくユーザーデバイスのフェデレーション管理により、ADFS統合が可能となり、パスワードの複雑化を強制する機能、ローテーション、自動アカウントロックアウト、多要素認証 (MFA)、MicrosoftのADエンタイトルメント管理といった機能が実現

特徴

アプリケーションのセキュリティ

TLSベースのアプリケーションセキュリティ (MQTT, SFTP, NTS, HTTPS, WebRTC)
ビデオストリーミングの暗号化 (RTSPS/SRTP, HTTPS)、安全なリモートSyslog

オペレーティングシステム

暗号化とデータ保護

OpenSSL 1.1.1 & 3.0
公開鍵基盤 (PKI) 規格のX.509デジタル証明書
TLS 1.2/TLS 1.3 (Transport Layer Security)
SDカード暗号化 (AES-XTS-Plain64 256ビット)
EFS (暗号化ファイルシステム) (AES-XTS-Plain64 256ビット)
署名付きビデオ

デフォルトのセキュリティ

デフォルトでHTTPS対応
遅延をもたらす総当たり攻撃の防御
ホストベースのファイアウォール
NTS (Network Time Security)
危険なTLSバージョンの無効化
UART/デバッグポートの無効化

プライバシー

診断データの使用
顧客固有のデータ保存に対するミニマリズム的アプローチ

エンタープライズネットワークセキュリティ

IEEE 802.1X (ネットワークアクセスコントロール)
IEEE 802.1AR (安全なデバイスID)
IEEE 802.1AE (MACセキュリティ、MACSec)

AXIS OS

OpenSSL, Apache, Curlなどの業界標準のオープンソースソフトウェアコンポーネントを95%以上備えた一般的なLinuxベースのオペレーティングシステム
機能拡張に焦点を当てたアクティブトラック & サードパーティ統合と下位互換性のユースケース向けの5年間のLTS (長期サポート)トラック

シリコンによるセキュリティ強化 (チップ)

ハードウェアのRoT (信頼の基点)

ARMベースのSoC (システムオンチップ) セキュリティ
TEE/OP-TEE (Trusted Execution Environment)
TPM 2.0 (Trusted Platform Module 2.0)、セキュアエレメント

安全なキーストレージ

顧客がアップロードした秘密鍵、ビデオ署名キー、AxisデバイスIDなどの暗号化キーの耐タンパー性ストレージと操作

セキュリティの基盤

Axisセキュリティ開発モデル

Axisセキュリティ開発モデル (ASDM)
サードパーティによる侵入テスト
Bugcrowdとの提携によるバグバウンティプログラム
ソフトウェア部品表 (SBOM)

コンプライアンス

コモンクライテリアの評価保証レベル (EAL)
FIPS 140
ETSI EN 303 645

高信頼性のデバイスID

Axis Edge Vaultサイバーセキュリティプラットフォーム
署名付きOSによるセキュアブート (コード署名)
AxisデバイスID (IEEE 802.1AR)

AXISのメリット
ACAP
自動化

世界最高級の 統合

Axis製品において、統合は極めて重要な役割を果たしています。当社は、多様かつ広範なアプリケーションに簡単に統合できる堅牢かつ一貫したAPIの構築に取り組んでいます。

そのため、Axisデバイスの機能すべてが活かされた包括的なソリューションを設計することが可能となります。

次ページでは、VAPIX（当社独自のAPI）、ONVIFの推進、IoTへの取り組み、ACAPによるプラットフォームのモジュール化、ネットワーク統合の自動化を詳しくご紹介します。

VAPIX、ONVIF、IoT、クラウド 統合におけるAxisの優位性

監視と接続の動的な環境において、アクシスコミュニケーションズは業界標準の既成概念を一変する一連の統合ソリューションを提供しています。

VAPIX:歴史に残る拡張性

当社のオープンAPIフレームワーク「VAPIX」は、当社のイノベーションへの取り組みを実証するものです。JSONとXML形式の他、HTTP GETとPOST呼び出しがサポートされているこのフレームワークにより、開発者はカスタマイズされたソリューションを容易に構築できるようになります。市場で最も広範かつ一貫性のあるライブラリを備えたVAPIXは、ONVIFを立ち上げる以前にAxisネットワーク製品におけるオープン統合の草分けとなったAPIです。

ONVIF:協調的な業界規格標準化

Axisはオープン規格業界フォーラム「ONVIF」と協力を図りながら、業界を前進させる協力の精神を育み、包括的で相互運用可能なソリューションをユーザーに提供することに取り組んでいます。ONVIFは、IPベースの物理セキュリティ製品における効果的な相互運用性を追求することを目的として、インターフェースの標準化を促進する業界フォーラムです。これにより、パートナーの統

合が簡素化され、Axisデバイスをさまざまなシステムとシームレスに連携させることが可能となります。

IoT:未来の形成

IoT(モノのインターネット)によって接続性が再構築される中、Axisデバイスはこの進化するエコシステムの推進に一役買っています。Axis製品では、IoTイノベーションにつながるMQTTなどのプロトコルがサポートされています。Axis製品を活用すれば、デバイスを接続できるだけでなく、そのデバイスが進化を続けるIoT環境の一部になります。

クラウド統合:雲の上でのイノベーション

Axisはデジタル接続の分野において、Microsoft AzureやAWS(アマゾン ウェブ サービス)といった主要プラットフォームとのスムーズな通信を念頭に置いて設計されたAPIとのクラウド統合を模索しています。技術の進化に応じて、MQTT経由のメッセージングサービスやWebRTC経由のビデオ・音声ストリーミングなど、当社は一段と多くのクラウド技術をサポートしていく構えです。ユーザーがクラウド技術を最大限に活用できる環境を構築することが当社の目標です。

ACAPによるプラットフォームのモジュール化

AXIS OSにより、AXIS Camera Application Platform (ACAP)を通じてプラットフォームのモジュール化が可能となります。これがこのオペレーティングシステムの重要な機能の1つです。フレームワーク「ACAP」を活用することで、ビデオ分析機能や音声分析機能、またビジネス要件を満たせるようにカスタム調整した他の拡張機能など、開発者はアプリケーションとサービスを構築および展開することができます。ACAPアプリケーションはAXIS OSのコア機能から独立しており、システムの他の部分に影響を与えずにインストール、更新、削除することができます。ACAPアプリケーションは、標準プロトコルやAPI経由で相互通信を図ること、また外部システムと通信を図ることができるように設計されています。

拡張性と性能

ACAPでは、Axisデバイスに搭載されているオペレーティングシステムのマイクロサービスアーキテクチャーが活用されます。需要と負荷に応じて、各サービスを個別にスケールアップまたはスケールダウンすることができます。これにより、システム全体の性能と可用性が向上し、リソースの効率的な使用と割り当てが実現します。

適応性とカスタマイズ性

ACAPを活用することで、さまざまなタイプの統合、分析、デバイスをサポートできるため、Axisデバイスの汎用性、適応性、カスタマイズ性が向上します。また、ACAPにより、カップリングを削減し、プラットフォームの結合力が高まります。これは、各アプリケーションがAXIS OSと疎結合し、それ自体の結合力が高まるためです。

保守性と信頼性

各サービスをそれぞれに分離してテスト、監視、デバッグを行うことができます。これにより、トラブルシューティングと診断が簡素化されるだけでなく、システムの回復力と障害に対する耐性が強化されます。また、ソフトウェアの品質という点で、AXIS OSが傑出した存在となります。



IT部門に最適なAXIS OS

適切に自動化とITインフラストラクチャーへの統合を図ることで、確実に適切なセキュリティ制御を実施して、時間やコストを節約することができます。また、不必要なシステムの複雑性を最小限に抑えることが可能となります。AxisデバイスとソフトウェアをエンタープライズITインフラストラクチャーに統合することで、以下のようなメリットがもたらされます。

- > 専用物理デバイスのステージングネットワークを排除することで、システムの複雑性を最小限に抑えることができます。
- > 自動化されたオンボーディングプロセスとデバイス管理を追加することで、コストの削減が実現します。
- > IEEE 802.1XやIEEE 802.1ARなど、ゼロトラストネットワークのセキュリティ制御が実現します。
- > IEEE 802.1AE MACsecに準拠したデータ暗号化を基盤として導入することで、ネットワーク全体のセキュリティが強化されます。これにより、ネットワークセキュリティなどにAxisデバイスを活かすことができます。
- > リモートSyslogなどの標準プロトコル経由でAxisデバイスを監視することで、ログの監視やヘルスマonitoringなどを行うことができます。

ゼロトラストの原則に基づく安全なネットワーク
単独で動作する孤立したシステムを排除するには、ゼロトラストの原則に基づいて集約された安全なネットワークを構築することが重要となります。明確に定義されたオープンネットワークプロトコルと標準規格を使用して、AxisデバイスをエンタープライズITインフラストラクチャーに統合することで、セキュリティの向上、構成とメンテナンスのコストの削減、ITポリシー主導の運用を実現することができます。

IT部門にもたらされるメリット

IT部門は、ITネットワークセキュリティを確保する責任を担っています。そのため、IT部門にとってAxisデバイスは有益に働きます。汎用性の高いAxisデバイスは、オープン標準のIEEEやIETFに準拠したネットワークプロトコルや共有設計によって定義されているITソリューションによく似ています。そのため、統合、メンテナンス、運用を容易に行うことができます。言うなれば、Axisデバイスはセキュリティ向上に貢献する顧客ネットワークの「信頼できる市民」なのです。



ご相談の 受け付け

AXIS OSという存在があるからこそ、Axisデバイスは顧客から信頼される地位を維持できるのです。非常に優れた画質や音声品質などが実現するのは、このOSのお陰です。

AXIS OSは、長期的な価値、高水準のサイバーセキュリティ、容易な統合というネットワークデバイスの最も重要な基準を満たせるように特別に設計されています。

ぜひ当社までご連絡ください。Axisデバイスにより、それぞれのビジネスや組織にもたらされる価値についてご説明します。

今すぐご連絡ください

また、axis.comで当社のデバイスをご覧ください



Axis Communications(について

Axisは、セキュリティとビジネスパフォーマンスを向上させるソリューションを生み出すことで、よりスマートでより安全な世界の実現を目指しています。ネットワークテクノロジー企業として、また業界をけん引するリーダーとして、Axisは映像監視、アクセスコントロール、インターコム、音声システムなどに関連するソリューションを提供しています。これらのソリューションは、インテリジェントアプリケーションによって強化され、質の高いトレーニングによってサポートされています。

Axisは50ヶ国以上に4,000人を超える熱意にあふれた従業員を擁し、世界中のテクノロジーパートナーやシステムインテグレーションパートナーと連携することで、カスタマーソリューションをお届けしています。Axisは1984年に創業し、本社はスウェーデン・ルンドにあります。