アクシスコミュニケーションズ

サイバーセキュリティ

連携によって優れたサイバー
保護を実現

AXIS COMMUNICATIONS

目次

概要

サイバーインシデントのリスクの軽減

ネットワークにあるデータやシステムを保護する上で、ネットワーク製品やソフトウェアサービスをサイバー脅威から保護することが非常に重要となります。システムが侵害されると、データの機密性や完全性が失われる可能性、および適時にデータの取得やアクセスができなくなる可能性があります。

サイバーセキュリティパートナーとしての責任を果たす任務の一環として、IPベースの物理的セキュリティ製品の安全な調達に有用となる考慮事項とガイドラインをご提供します。貴社が可能な限り安全な方法でAxis製品を使用できるように、当社は安全対策を容易に導入する方法をご案内しています。

本書では、サイバーセキュリティの詳細をご説明します。また、https://www.axis.com/ja-jp/about-axis/cybersecurityには、より優れたサイバー保護を共に確保できる方法が記載されています。

責任の共有

サイバーセキュリティの中核は、製品、人、テクノロジーです。これは継続的に注力すべきプロセスです。また、協力を図りながら、サイバーセキュリティチェーンのすべてのリンクを可能な限り強固なものにする必要があります。サイバーセキュリティは共通の責任です。エンドユーザーを含め、以下のような関係者が協力して取り組む必要があります。

デバイスメーカー

ここがサイバーセキュリティの出発点となります。製品のライフサイクル全体を通じて欠陥リスクを最小限に抑えるため、メーカーは設計、開発、製造、ソフトウェアのメンテナンスにおいてサイバーセキュリティのベストプラクティスを適用する必要があります。自社のサプライチェーンを注意深く管理することが重要となります。製品には、さまざまなセキュリティ制御を実装できる機能が組み込まれている必要があります。また、顧客のセキュリティプロセスやポリシーをサポートするために、効率的なデバイスの構成と管理を実現できるツールも必要となります。また、新たに脆弱性が発見された場合に、それをパートナーや顧客に通知するチャンネルも必要です。

正規ディストリビューター

扱う製品に直接触れることのないディストリビューターの場合は、比較的簡単にサイバーセキュリティに対応することができます。しかし、付加価値の付いた商品を提供するディストリビューターの場合は、インテグレーターや設置担当者と同様の側面を考慮に入れる必要があります。特に、メーカーから機器を購入して、別の(または独自の)ブランドでラベルを付け直す場合は注意が必要です。透明性が鍵となります。機器の元のメーカーを明確に提示してください。

コンサルタント、インテグレーター、設置担当者

こうした職業の担当者は、エンドユーザーのセキュリティ管理の特定、設計、実装を支援し、顧客のネットワークで物理的セキュリティデバイスによる問題が発生しないように顧客を補助する責任を負います。その任務には、パスワード、リモートアクセス管理、ソフトウェアや接続デバイスのメンテナンスなど、戦略の開発が含まれる場合があります。また、設置されている機器に最新の更新が適用されていること、およびシステムがウイルススキャンされていることを確認する役割が含まれる場合があります。多くの場合、OEM/ODM機器を使用することで、サイバーセキュリティの責任の所在が不明確になります。サイバーセキュリティに関する全体的な協議で、この課題について話し合う必要があります。

エンドユーザー

それぞれの組織には固有のサイバーセキュリティニーズがあるため、普遍的なサイバーセキュリティ構成というものは存在しません。しかし、必要なセキュリティの要件範囲を定義するために、一連の情報セキュリティポリシーを設定することが重要となります。デフォルトのアカウントを削除すること、一意の強力なパスワードを作成して安全に保存し、これを定期的に変更すること、差別化された権限を割り当てること、パッチと更新を常に適用することが重要となります。しかし、これらは実行すべき手順のほんの一部に過ぎません。

研究者/調査員

多くの場合、研究者/調査員によりデバイスの脆弱性が発見されます。脆弱性が意図的なものでない場合は、通常、研究者/調査員がメーカーに通知し、その脆弱性が公開される前にメーカーがこれを修正する機会を提供します。しかし、重大な脆弱性に意図的な性質がある場合は、ユーザーの意識を高めるために、多くの場合、こうした脆弱性が一般公開されます。

物理的セキュリティから得られるサイバーセキュリティの教訓

ほとんどの人にとって、物理的セキュリティリスクを理解することはそう難しくありません。ドアに鍵がかかっていなければ、侵入者が入るリスクが高まります。貴重品を目に付く場所に置けば、簡単に盗まれるかもしれません。間違いや事故により、人、財産、物に害が及ぼされる可能性があります。サイバーセキュリティ対策も、物理的セキュリティ対策とほぼ同じように取り組むことができます。

組織で物理的セキュリティを担当しているか、サイバーセキュリティを担当しているかに関わらず、両方に同じ原則を適用する必要があります。

> アセットとリソースを特定して分類する（保護の対象）

> 発生する可能性の高い脅威を特定する（攻撃者と攻撃手法）

> 脅威により損害が発生する可能性の高い脆弱性を特定する（可能性）

> 不良な事態が発生した場合にかかる推定コストを特定する（結果） 多くの場合、リスクレベルは「脅威が発生する確率」と「もたらされる有害な影響」を掛けて計算します。これが判断できたら、悪影響の発生を防止するために取ることができる措置を自問自答する必要があります。

サイバーセキュリティとは？

サイバーセキュリティは、コンピューターのシステムとサービスをサイバー脅威から保護することです。サイバーセキュリティの実践には、コンピューター、電子通信システムやサービス、有線/電子通信、保存されている情報の損傷を防止し、その機密性、完全性、可用性、安全性、信頼性、非否認性を保証するプロセスが含まれます。

注意する必要のある脅威

IT（情報技術）またはOT（制御・運用技術）システムに関して保護すべき重要な要素は、機密性、完全性、可用性、安全性です。このいずれかに悪影響を与えるものはすべて、サイバーセキュリティインシデントと捉えられます。

では、最も一般的なサイバーセキュリティ脅威および悪用され得る脆弱性を見ていきましょう。IPベースの物理的セキュリティシステムが対象となる場合の最も一般的なサイバー脅威として、以下の4つが挙げられます。

1. **思いがけない人的ミス＆不注意な行為**
2. **システムの意図的な誤用**
3. **物理的な改ざんと妨害**
4. **ソフトウェアの脆弱性の悪用**

1 思いがけない人的ミス&不注意な行為

いかに優れたテクノロジーでネットワークを保護していても、セキュリティ侵害の主要因には人的要素が含まれます。

意図せずにサイバー攻撃を引き起こす人的ミスとして、以下が挙げられます。

> **ソーシャルエンジニアリング**
攻撃者の心理的操作にユーザーが騙されてセキュリティミスを犯す場合、または機密情報をうっかり提供してしまう場合があります。ソーシャルエンジニアリングの例として、フィッシングやスケアウェアなどが挙げられます。

> **パスワードの悪用**
これには、強力なパスワードを使用していない場合、またパスワードを適切に保護して更新していない場合が含まれます。

> **重要なコンポーネントの管理ミス**
これには、システムにアクセスするために必要となるものを紛失した場合、または置き忘れた場合が含まれます。例として、アクセスカード、電話、ノートパソコン、書類などが挙げられます。

> **不適切なシステム管理**
これには、システムの更新やセキュリティパッチの適用が適切に行われていない場合が含まれます。

> **改善の失敗**
これには、誰かが不用意に修正しようとして、逆にシステム性能が低下するといった場合が含まれます。

脆弱性&人的ミス

人的ミスによって引き起こされる最も一般的な脆弱性は、サイバーセキュリティに対する意識の低さおよびポリシーやリスクを管理するための長期的なプロセスの欠如に起因します。人的ミスにより発生する脅威を軽減するには、組織内の全員がサイバーセキュリティのベストプラクティスを習得する必要があります。また、ビデオ管理システム(VMS)やデバイスマネージャーを使用して、ネットワーク接続デバイスへのアクセスを少数の信頼できる個人に制限する必要があります。

2 システムの意図的な誤用

非常に一般的な別のサイバー脅威の要因として、システムへの正当なアクセス権を持つスタッフがシステムを意図的に誤用するというケースが挙げられます。

意図的な誤用には、以下のような種類があります。

システムサービスとリソースの操作

データの盗難

システムに対する故意的な危害

脆弱性＆意図的な誤用

ポリシーと長期的なプロセスを実装することで、脆弱性を抑制し、システムが意図的に悪用されるリスクを軽減することが重要となります。機密データへのアクセス権を持つ個人の数を制限すること、および権限を付与する個人を適切に審査することが重要です。

カメラなど、ネットワークに接続されている物理的セキュリティデバイスの管理に使用しているソフトウェアには、独自の認証情報が割り当てられている管理者アカウントを使用する必要があります。一意のアカウントを使用し、これは共有するべきではありません。この場合は、サイト運営者が管理ソフトウェアで個別のアカウントを持つべきです。また、その他の個人が物理的セキュリティデバイスに直接アクセスできない環境を確立する必要があります。個人にアクセスを許可しなければならない状況が発生した場合は、その個人に一時的なアクセス権を付与します。

3 物理的な改ざんまたは妨害

サイバーセキュリティという観点から、物理的な保護体制を確立することが非常に重要となります。

> 物理的に露出している装置は、改ざんされる可能性があります。

> 物理的に露出しているデバイスは、盗難に遭う可能性があります。

> 物理的に露出しているケーブルは、切断や再配線される可能性があります。

脆弱性＆物理的な脅威

一般的に悪用の脅威が発生する要因として、サーバーやスイッチなどのネットワーク機器が鍵のかかっていない場所に配置されている状況、カメラが保護ケースで保護されていないために簡単にアクセスできる状況、ケーブルが壁や導管に収められていない状況などが挙げられます。ネットワーク接続デバイスにより、同じネットワークの他の資産が公開される可能性があります。

悪影響に注意

ビデオ、音声、アクセスコントロールシステムでは、金融取引が処理されることも、顧客データが保存されることもありません。こうしたシステムは攻撃したところでほぼ収益化できないため、サイバー犯罪組織にとってはあまり価値がありません。しかし、侵害されたシステムは他のシステムに対する脅威となる可能性があります。

したがって、コストを見積もるのは容易ではありません。残念ながら、間違いを犯してから教訓を学ぶ組織が多いのが現状です。脅威対策は品質と同じです。つまり「安かろう悪かろう」というわけです。製品ライフサイクル全体を通じてサイバーセキュリティを考慮に入れていないサプライヤーから安価なシステムを購入してしまうと、長期的にはるかに高いコストがかかる可能性があります。

4 ソフトウェアの脆弱性の悪用

ソフトウェア開発には、バグやコーディングの誤りなど、攻撃に悪用され得るセキュリティ脆弱性が発生するというリスクが存在します。製品に存在するソフトウェアの脆弱性が多いほど、攻撃に曝されるリスクが高くなります。理想的には、メーカーは製品を発売する前に、ソフトウェア開発モデルを構築することで、ソフトウェア開発のすべての段階を通じて脆弱性のリスクを最小限に抑えるプロセスとツールを組み込む必要があります。

この業界において、まったくエラーのないソフトウェアのリリースは稀ですが、セキュリティリスクをもたらすバグやその他の不適切な実装を特定および修正し、製品メーカーから顧客に通知する必要があります。そのため、メーカーは高い透明性を持って、新たに発見されたソフトウェア脆弱性を公開し、適時に顧客に解決策を提供する必要があります。また、セキュリティパッチやバグ修正が含まれているソフトウェア更新が製品メーカーから提供されたら、顧客はそれを確実かつ継続的に実装することが重要となります。

リスクを軽減するためにエンドユーザーが念頭に置くべき考慮事項

サイバーセキュリティを念頭に置いて物理的セキュリティ製品を購入する場合に、まず検討すべき点がいくつかあります。

第一に、物理的セキュリティサプライヤーのサイバーセキュリティアプローチをチェックする必要があります。その会社がサイバーセキュリティを管理する企業ポリシーを制定していること、およびそのポリシーに基づいて自社の資産を継続的に特定および評価していること、さらに資産に関連するリスク評価を実施していることを確認してください。また、サプライヤーがサプライチェーンとどのように連携を図っているかを把握することも重要となります。さらに、製品の設計と製造にサイバーセキュリティ機能とサポートが組み込み込まれているかどうかを確認する必要もあります。

ネットワーク製品のライフサイクル全体を通じてサイバーセキュリティをサポートするために、どのような対策が提供されているか、システムが攻撃を受けた場合はどうなるか、サプライヤーの製品に関連するサイバーセキュリティインシデントが発生した場合の対応に関するガイドラインが提供されているかどうかも確認してください。

上記は考慮すべき事柄のほんの一部にすぎません。以降のページにさらに詳しい情報が記載されています。

監視製品のサプライヤーおよびサプライヤーの下請け業者について知っておくべき事柄

セキュリティ脅威がなくなることはありません。継続的に新たな脅威が発生し、いつ何時その性質が変化するか分かりません。組織は、多くの場合、こうしたリスクをサプライヤーがどのように評価して対処するかのみに焦点を当てています。そのサプライヤーの下請け業者はどうでしょうか？ サプライヤーがどのようにサプライチェーン全体を管理および維持し、コンポーネントレベルから完成品に至るまでのすべての工程が安全であることを確認しているかご存じですか？

サプライヤーはセキュリティリスクを最小限に抑制することに重点を置いていますか？

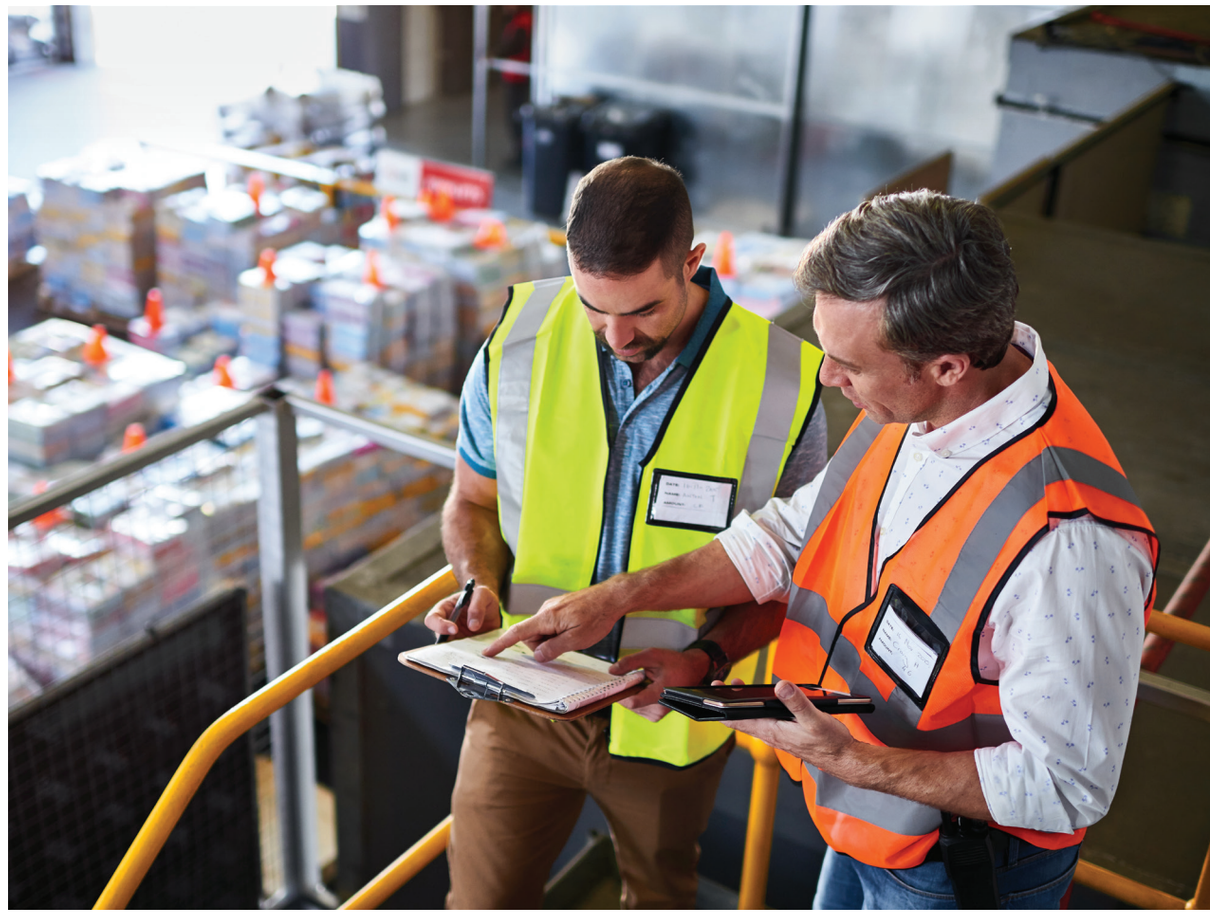
> サプライヤーはコンポーネントレベルから完成品までのサプライチェーン全体を管理していますか？

> サプライヤーの会社では、セキュリティ上の考慮事項を中核に据えたソフトウェア開発モデルが確立されていますか？

> サプライヤーは、保護機能が組み込まれた製品を設計および製造していますか？

> サプライヤーは、保護対策の導入に関する知識とツールを共有していますか？

> ソフトウェアの脆弱性が新たに発見された場合に、サプライヤーは迅速に対応し、無料アップグレードを提供していますか？



サプライチェーンパートナー

サプライチェーンのセキュリティは、厳格な評価プロセスを通じて適切なサプライチェーンパートナーを選択することから始まります。評価プロセスには、各社の品質と持続可能性の管理プロセスの分析を含める必要があります。少なくとも、ISO 9001認証またはIATF 16949認証を取得するなど、第三者組織の審査に合格している企業を選択してください。

サブサプライヤーの評価

サプライヤーは、サブサプライヤー（サプライヤーの下請け業者）のリスク管理プロセス、およびその生産設備とプロセスを評価する必要があります。現場訪問とフォローアップの現場監査を実施することで、その施設が認定ベンダーとしての資格要件と基準を満たしているかどうかを評価する必要があります。潜在的な新しいサプライチェーンパートナーの評価の一環として、サブサプライヤーの財務状況と所有構造の詳細な分析を実施する必要があります。

戦略的サブサプライヤー

重要なコンポーネントのサプライヤーや製造パートナーの場合は、こうした組織の関係者との関係が特に緊密かつ長期的なものとなる傾向があります。こうした組織は、自社のサプライヤーが共同プロジェクトと開発を推進し、目標を設定し、そして長期的な相互の取り組みと計画を策定している戦略的なサブサプライヤーという位置付けとなります。サプライヤーの製品に組み込まれる重要なコンポーネントはすべて、戦略的なサブサプライヤーから直接調達し、社内で保管する必要があります。それほど重要でないコンポーネントは製造パートナーから調達しても構いませんが、承認ベンダーに認定されているサプライヤー以外からは調達しないでください。

サプライヤーの生産製品の安全性評価

> サプライヤーは、製造プロセスを定義および監視していますか？

> サプライヤーは、重要な生産設備を開発および生産していますか？

> サプライヤーは、生産過程でコンポーネント、モジュール、製品をテストするシステム、およびソフトウェア、テストコンピューター、その他のITハードウェアインフラストラクチャーを提供していますか？

> サプライヤーは、リアルタイムのデータ分析、潜在的なセキュリティリスクの評価、緩和計画の実施が可能となるように、24時間年中無休で生産データを収集していますか？

指定された要件にサブサプライヤーが準拠していることをサプライヤーが確認する最良の方法として、毎年または隔年に定期的な現場監査を実施する手段が挙げられます。こうした監査では、プロセスのコンプライアンス、品質管理、トレーサビリティ記録といった重要な側面を幅広く評価する必要があります。また、工場内における物理的な取り扱い、在庫の取り扱い、生産設備の評価もこれに含める必要があります。

四半期ごとに事業評価を実施して、期待値と実際の業務状況を照会するのも良策です。戦略的なサブサプライヤーの場合は、上級幹部がこうした評価を実施することが勧められます。

物理的セキュリティ

コンポーネントサプライヤーから流通センターに至るまで、サプライチェーン内のすべての拠点/施設が、高いセキュリティ要件を満たしている必要があります。たとえば、出入口を確実かつ継続的に警備し、アクセスコントロールと訪問者の登録を記録および保存することが重要となります。また、スキャン装置を使用して、望ましくない物体や物質の存在を検知する必要があります。輸送については、認識されている有名な運送事業者を手配する必要があります。厳格なセキュリティ規制と管理を実践している輸送会社のみを選択してください。さらに、カメラを使用して、商品の入出荷を監視して記録することが推奨されます。

ゼロトラストネットワーク

ネットワークの脆弱性はますます高まっています。接続デバイスが急増している現状に伴い、ネットワークエンドポイントを狙う攻撃が増えています。サイバー攻撃は、その数が増加しているだけでなく、その手段がより巧妙化しています。これに伴い、「ゼロトラスト」という概念が登場しました。

どのようなトラフィックも信用しないというアプローチ

その名称通り、ゼロトラストネットワークの概念は、人間かマシンかに関わらず、ネットワークに接続されているエンティティやネットワーク内に存在するエンティティは絶対に信用できないという考え方です。これは、エンティティがどこにあるか、またどのように接続されているかには関係ありません。ゼロトラストネットワークの最も重要な哲学は、「決して信用せず、常に検証する」ということになります。

ゼロトラストネットワークの概念は、人間かマシンかに関わらず、ネットワークに接続されているエンティティやネットワーク内に存在するエンティティは絶対に信用できないという考え方です。

アクセスを必要最小限に制限

アクセスしているエンティティやネットワーク内に存在するエンティティは、その動作やネットワークでそれがアクセスしている特定データの機密性に応じて、さまざまな方法でそのIDを複数回検証する必要があります。本質的に、エンティティには、そのタスクを完了するために必要最小限のアクセス権のみを付与します。

ゼロトラストネットワークとアーキテクチャー

サイバーセキュリティ強化の必要性に対する顧客の意識が高まるのに伴い、HTTPSやより精巧なIEEE 802.1X標準など、ゼロトラストネットワークとアーキテクチャーが実装されるようになってきました。こうした認証プロトコルを活用することで、認証デバイスのネットワークへの参加を自動的に許可し、認証されていないデバイスをブロックすることができます。ネットワークデバイスメーカーにとっては、ネットワークをサポートするテクノロジーやインターフェースを組み込むことで、こうした要件を満たすことが不可欠な条件となっています。

ポリシーエンジン を使用

すべてのゼロトラストネットワークの中核となるのがポリシーエンジンです。ポリシーエンジンはソフトウェアで、これにより、組織がデータとネットワークリソースにアクセスする方法に関するルールを作成、監視、適用することができます。ポリシーエンジンではネットワーク分析とプログラムされたルールの組み合わせが使用され、これによりいくつかの要因に基づいて役割ベースのアクセス許可が付与されます。

すべての要求に対する「許可」または「拒否」を判断

簡単に述べると、ポリシーエンジンにより、すべてのネットワークアクセス要求がポリシーと比較され、その要求を許可するか拒否するかがエンフォーサーに通知されます。ゼロトラストネットワークでは、ポリシーエンジンにより、ホスティングモデル、場所、ユーザー、デバイス全体におけるデータセキュリティとアクセスポリシーが定義および適用されます。

ルールの定義と適用

ポリシーエンジンが正常に機能するようにするには、次世代ファイアウォール（NGFW）、電子メールとクラウドのセキュリティゲートウェイ、データ損失防止（DLP）ソフトウェアなど、組織は主要なセキュリティ制御機能のルールとポリシーを慎重に定義する必要があります。こうした制御機能を組み合わせることで、ホスティングモデルや場所を超えたネットワークのマイクロセグメンテーションを実現することができます。

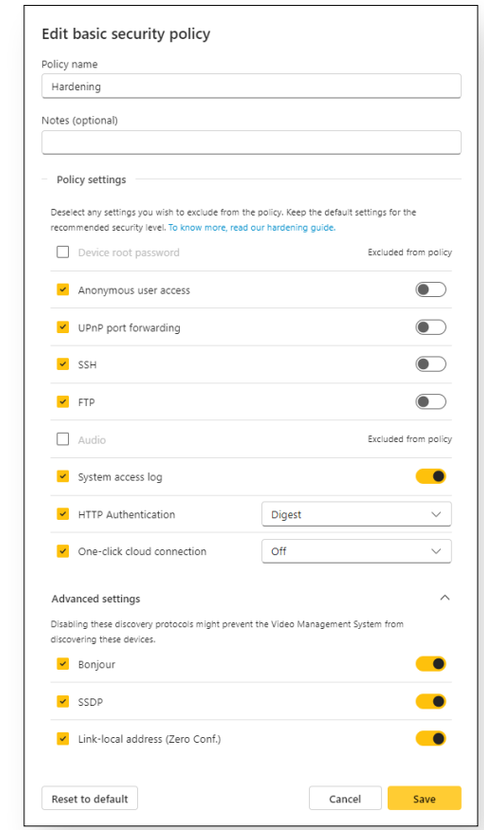
データとネットワークリソースにアクセスする方法

ポリシーエンジンにより、以下が可能となります。

> ルールの作成
> ルールの監視
> ルールの強制

現在だけでなく、将来性に優れたポリシーエンジン

今のところ、各ソリューションの管理コンソールにポリシーを設定する必要がありますが、製品全体のポリシーを自動的に定義および更新できる統合コンソールも増えています。IAM（アイデンティティ/アクセス管理）、多要素認証、プッシュ通知、ファイルアクセス許可、暗号化、セキュリティオーケストレーションはすべて、ゼロトラストネットワークアーキテクチャーの設計において重要な役割を果たす要素です。



ポリシーエンジンの設定

効果的なライフサイクル管理を実装することが重要である理由

脅威に遅れを取らない対策

ライフサイクルを効果的に管理することで、組織はその事業を安全に維持し、将来に向けてより適切な準備態勢を整えることができます。リスクのある箇所を把握し、悪用される可能性のある領域を最新の状態に保つ必要があります。ネットワーク監視カメラがダウンしてしまうと、重大な結果がもたらされる可能性があるため、これはセキュリティシステムにとって特に重要となります。

ネットワーク接続デバイスの更新の重要性

既知の脆弱性を悪用する攻撃者を撃退し、既存の対策の弱体化を回避するためには、ネットワークカメラやVMSなど、すべてのネットワーク接続デバイスを更新してパッチを適用する必要があります。

脆弱性への対処やバグ修正、その他の性能の問題を解決することで、安定した安全なシステムを確保できるように、メーカーはデバイスソフトウェアの更新とセキュリティパッチを定期的にリリースしています。しかし、組織はハードウェアが動作するファームウェアやオペレーティングシステムの更新を怠ることがよくあります。

これは通常、ネットワークにあるすべてのサービスの全体像を完全に把握していないためです。また、全体像を把握していても、すべてのデバイスを更新するのは面倒で時間のかかる作業となり得ます。

デバイスソフトウェアの更新を怠ると、デバイスがサイバー攻撃に対して脆弱になる可能性があるだけでなく、その結果として、動作不能になる場合やコンプライアンス違反により規制当局から多額の罰金が科せられる場合があります。

よく言われるように、ネットワークの安全性はそれに接続されているデバイスの安全性にかかっています。そのため、ネットワークに接続された物理資産のライフサイクルを効果的に管理することが重要となるのです。

1つのデバイス – 2つのライフタイム

ソフトウェアベースのデバイスのライフサイクルには、以下のように2つのタイプがあります。

1)デバイスの機能寿命またはデバイスが正常に動作および機能する期間。たとえば、ネットワークカメラの機能寿命は通常10〜15年です。

2)デバイスの経済的ライフサイクル。新テクノロジーを導入するコストよりも、デバイスの維持にかかるコストが高くなるまでの期間です。IPカメラは15年間機能すると考えられていますが、サイバーセキュリティの状況が急速に変化しているため、実際の耐用期間はこれよりも短くなります。

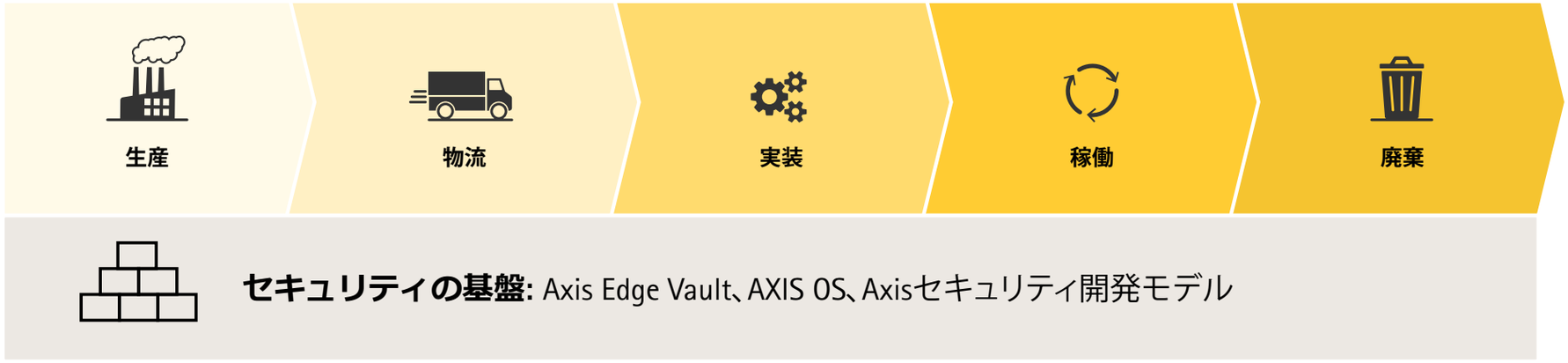
資産の積極的な管理

ライフサイクル管理とは、物理的資産の機能的ライフサイクルと経済的ライフサイクルの両方を効果的に管理することです。組織は、ネットワークに展開されているすべてのデバイスの全体像を明確に把握して、デバイスを脅威から保護する必要があります。

Axisのサイバーセキュリティアプローチ

Axisは、高レベルのサイバーセキュリティサポートを実現することに取り組んでいます。当社は、継続的にサービスとサイバーセキュリティプロセスの改善に注力しています。当社は、事業とサプライチェーンの保護、脆弱性のリスクを軽減するためのソフトウェア開発、新たに発見された脆弱性の管理、製品にセキュリティを組み込むことでライフサイクルを通じてサイバーセキュリティ全体をサポートすることについて、当社がどのような措置を講じているかを高い透明性をもって伝達することが重要であると考えています。

以降のページで、セキュリティ基盤として当社が講じている対策、およびリスクを軽減してAxisのセキュリティを確保することを目的として、製品の生産から実装、稼働、廃止に至るまでの製品ライフサイクルの各段階を通じて当社が取っているアプローチや措置について詳しくご説明します。



セキュリティの基盤

内部セキュリティに対する構造的かつ体系的なアプローチ

セキュリティに対する協力的なアプローチを推進するAxisでは、全従業員が内部セキュリティの継続的な改善を促進しています。ISO 27001 認定を取得している当社の情報セキュリティ管理システム（ISMS）が、当社のサイバーセキュリティフレームワークの基盤となっています。ISMSの一環として、当社はサイバーセキュリティ管理体制を導入することで、ITインフラストラクチャー、ソフトウェア開発プラットフォーム、コネクテッドサービスの管理において確実にベストプラクティスに準拠できる環境を整えています。

構造的かつ体系的なアプローチに従うことで、当社は資産の機密性、完全性、可用性を保護しています。Axisはまた、デバイスのAXIS OSポートフォリオをサイバーセキュリティ規格「ETSI EN 303 645」に準拠させるなど、さまざまな規制要件を満たし、戦略的に選択したフレームワークや規格を遵守しています。しかし、当社は規制や認証だけを目安にしているわけではありません。多数の認証を取得することが、必ずしもサイバーセキュリティの向上につながるとは限らないためです。

詳細情報：Axisにおけるコンプライアンス

RI. SE

CERTIFIKAT

ISO/IEC 27001

Härmed intygas att/This is to certify that

Axis Communications AB

Gränden 1, 223 69 LUND, SWEDEN

har ett ledningssystem för informationssäkerhet som uppfyller kraven enligt ISO/IEC 27001:2022 vad gäller
has an information security management system that fulfils the requirements of ISO/IEC 27001:2022 with respect to

Product management, utveckling och drift inom IT-infrastrukturtjänster och Axis Connected Services
Allt i enlighet med uttalande om tillämplighet fastställt 2023-11-14

Product management, development and operations within IT infrastructure services and Axis Connected Services
All in accordance with Statement of Applicability established 2023-11-14

Ursprungligen utfärdat/Originally issued	2019-02-27
Giltigt till och med/Expiry date	2025-02-26
Beslutsdatum/Decision date	2023-12-07

Jonas Madsen

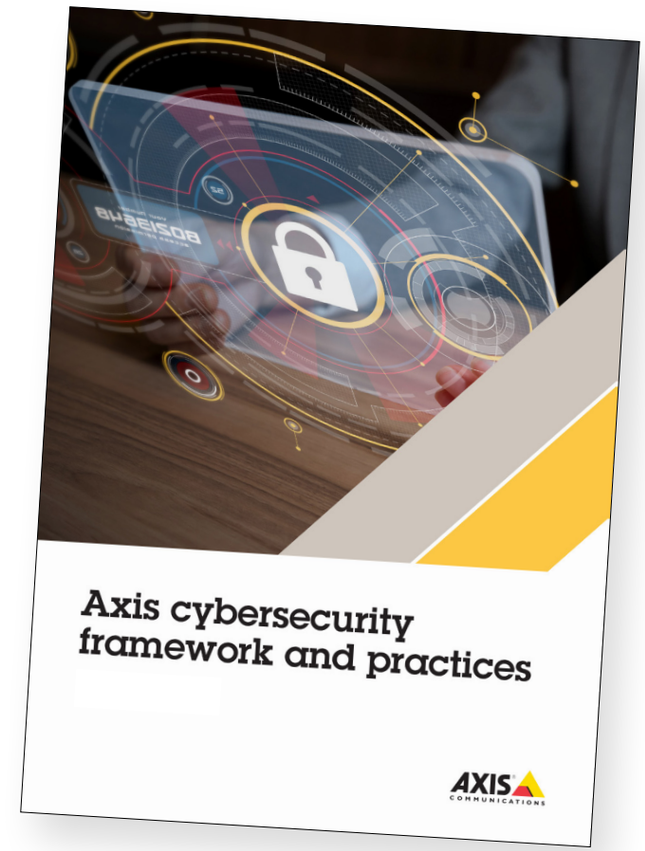
RISE Research Institutes of Sweden AB | Certification
Box 857, SE-501 15 Borås, Sweden
+46 10-516 50 00
certifiering@ri.se | www.ri.se

SP

Certifikat/Certificate 6134 | | version/issue 5 | 2023-12-07

This document is the property of RISE and may not be reproduced other than in full, except with the prior written approval by RISE.

Sida/Page 1(1)



製品の完全性の保護＆ソフトウェアの脆弱性のリスク削減

内部セキュリティから製品セキュリティに移行しましょう。以下の要素は、Axisのハードウェアとソフトウェアのセキュリティ基盤を形成するものであると同時に、当社の透明性の基本原則を反映するものです。

Axis Edge Vaultサイバーセキュリティプラットフォーム

Axisデバイスに組み込まれているこのハードウェアベースのプラットフォームには、Axisデバイスの完全性を保護する機能が含まれています。これにより、デバイスの安全な起動と統合が実現するだけでなく、暗号キーなどの機密データを不正アクセスから確実に保護することができます。

詳細情報：Axis Edge Vault

Axisセキュリティ開発モデル（ASDM）

ASDMは、ソフトウェアに脆弱性が存在する製品がリリースされるリスクを低減するために、Axisで適用されている開発方法論です。これにより、ソフトウェア開発にセキュリティへの考慮が確実に組み込まれ、リスク評価、脅威モデリング、コード分析、侵入テスト、バグバウンティプログラム（脆弱性報奨金制度）、脆弱性スキャンと管理といったエリアに確実に対応することができます。ASDMにより、開発のあらゆる段階における問題を迅速に検知して解決できるため、顧客のセキュリティ関連リスクが削減されます。

詳細情報：ASDM

AXIS OS

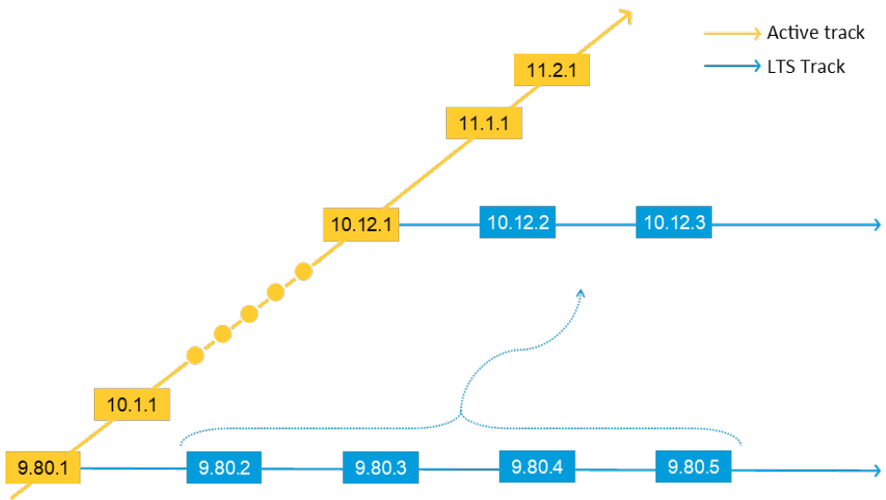
AXIS OS は、Linuxベースのエッジデバイス向けオペレーティングシステムです。オープン性、透明性、サイバーセキュリティを重視して構築されたこの強力なオペレーティングシステムは、Axisデバイス向けのさまざまなトラックを備えています。これにより、Axisは多数の製品全体のソフトウェアセキュリティ機能とパッチを迅速にリリースすることができます。これは、リスクを軽減し、Axisの製品とサービスを最新の状態に維持して保護できるように設計されています。多くの製品のサポート終了日はAxisのWebサイトに記載されているため、顧客は製品の廃止や交換を適時に計画することができます。

詳細情報：AXIS OS

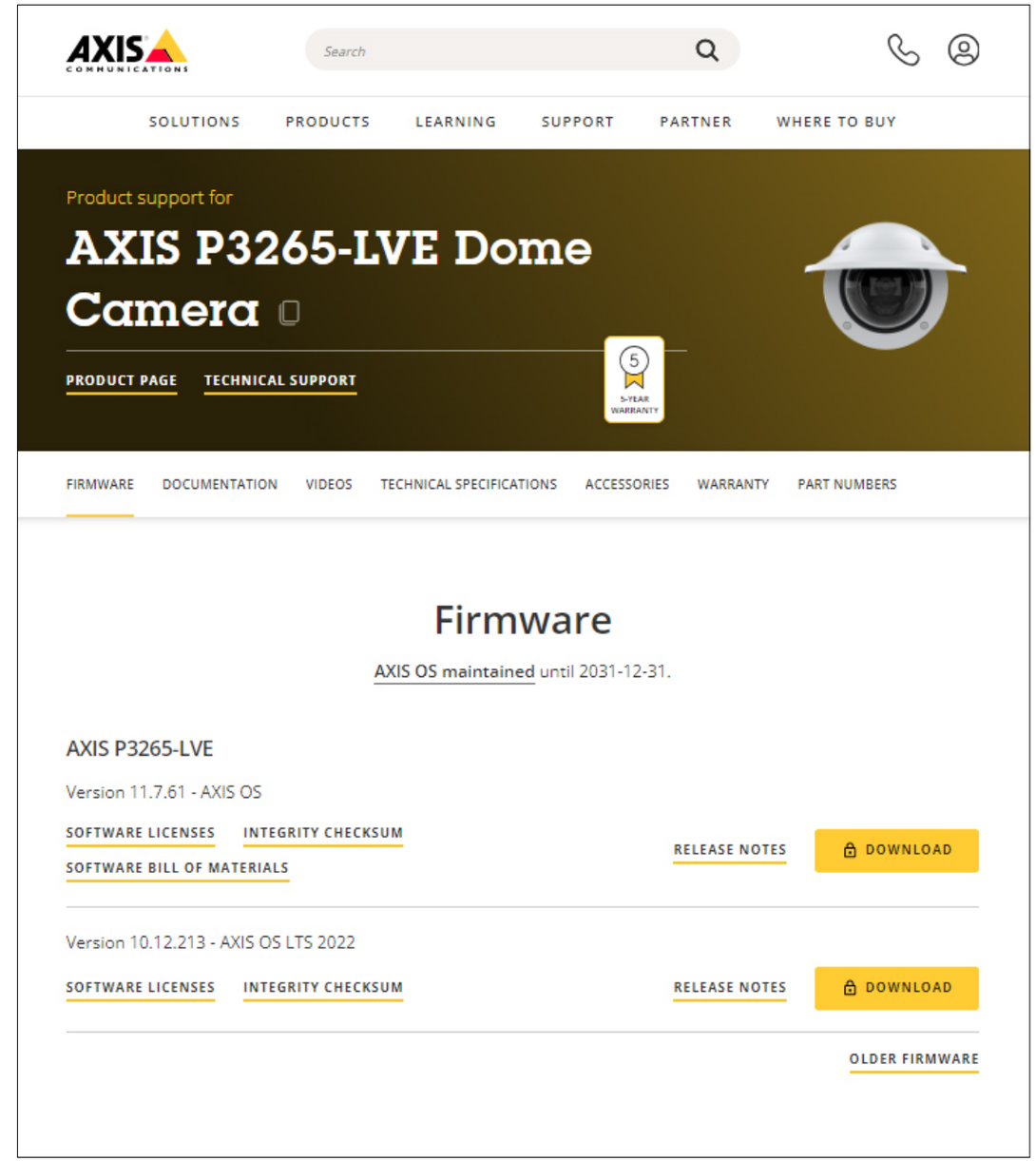
ソフトウェア部品表（SBOM）

当社はサイバーセキュリティに重点を置き、顧客、セキュリティ研究者、当局に対する透明性を向上させながら、AXIS OSのソフトウェア部品表を発行しています。ソフトウェア部品表には、Axisデバイスのオペレーティングシステム構築に使用されるコンポーネントの広範かつ詳細なリストが記載されています。これにより、サプライヤーは適用するサイバーセキュリティのベストプラクティスに関する洞察を得ることができます。また、部品表には、脆弱性評価、脅威分析、修復計画を専門とするサードパーティにとっても貴重な情報が含まれています。

詳細情報：ソフトウェア部品表



AXIS OSトラック



新たに発見された脆弱性の管理

CVE（共通脆弱性識別子）プログラムにおけるCVE採番機関（CNA）のメンバーであるAxisは、顧客が適切かつ適時に措置を講じられるように、脆弱性を公開して関係者に通知しています。Axisは外部の研究者と協力を図りながら、高い透明性と責任をもって、調整されたプロセスで脆弱性と危険性を開示しています。Axisは、影響を受けるデバイス、ソフトウェア、サービスにパッチを提供し、必要なすべての情報を**Axis Webサイト**および一般公開されているCVEプログラムの脆弱性データベースを通じて提供しています。また、当社はセキュリティ通知サービスも提供しています。これにサインアップすることで、脆弱性や他のセキュリティ関連事項に関する情報を受け取ることができます。最新のセキュリティパッチが確実に適用されるように、Axisはインストールされている製品のオペレーティングシステムを最新の状態に保つことの重要性を強調しています。

詳細情報：Axis脆弱性管理ポリシー

バグバウンティプログラム

当社は、透明性の高い脆弱性管理戦略の一環として、バグバウンティプログラムを運用しています。大手クラウドソーシングサイバーセキュリティ企業のBugcrowdとの提携により、このプログラムが実現しました。当社は、外部のセキュリティ研究者やホワイトハッカー（倫理的ハッカー）と専門的な関係を構築することに取り組んでいます。このプログラムの一環として、当社はAXIS OSベースの製品の脆弱性を発見した研究者に「報奨金」を提供しています。こうして発見された脆弱性などをAxisは透明性の高い方法で外部に公開し、影響を受ける製品にパッチを提供します。

生産

物流

ハードウェアとソフトウェアコンポーネントの侵害リスクの軽減

サプライチェーンのセキュリティ

他すべての製品と同様に、物理的セキュリティ製品も、完全性を維持しながら、設計・意図通りに機能するものでなければなりません。サプライチェーンの工程で、製品のハードウェアとオペレーティングシステムに不正な変更や操作が加えられないように適切な保護対策を実施することで、これを実現することができます。

品質管理

Axisはサプライヤーや製造パートナーと協力を図りながら、大規模な品質管理を実施することで、製品の完全性を維持および保護しています。コンポーネントは、常にAxis仕様の部品表に従って、承認ベンダーに認定されているサプライヤーから調達しています。Axisの許可なしに、サプライヤーが仕様、作業指示、品質検査文書を変更することはできません。承認された変更はすべて文書化して、記録する必要があります。

トレーサビリティ

マテリアルハンドリングプロセスにより、常に材料のステータスを保証し、品質を損なう可能性のある逸脱を検知することができます。入荷材料から完成部品に至るまでの生産バッチのトレーサビリティを確保するため、サプライヤーと製造パートナーは、トレーサビリティシステムを維持する必要があります。製造段階で、物理的なコンポーネントには複数のテストと適合性の検証を行い、逸脱があればこれを確実に発見します。

偽造部品の検出

自動光学検査（AOI）を利用することで、偽造部品が含まれていないことを確認することができます。Axisは、重要な生産設備だけでなく、生産の異なる段階でコンポーネント、モジュール、製品をテストするためのシステムを開発および生産しています。このプロセスにより、改ざんのリスクが削減されます。追加のセキュリティ管理として、年を通してすべてのテストデータがAxisと共有されるため、不正な変更を即座に特定できる体制が確立しています。

詳細情報：
Axisサプライチェーンのセキュリティ

流通関連の脅威への対処

Axisデバイスにはサイバーセキュリティ機能が内蔵されていること、およびデバイスを工場出荷時のデフォルト設定にすることで、当社は出荷中のソフトウェアの不正変更を防止しています。Axis Edge Vaultでサポートされている機能（詳細については次ページ参照）により、デバイスに入っている機密情報を保護し、デバイスで正規のAxisオペレーティングシステムが実行されていることを保証することができます。

ベンダーのリスク評価を行い、組織にもたらされ得るリスクの軽減措置をそのベンダーが講じているかどうかを判断する上で、サプライチェーンのセキュリティを理解することが必要となります。

サイバーセキュリティ機能内蔵

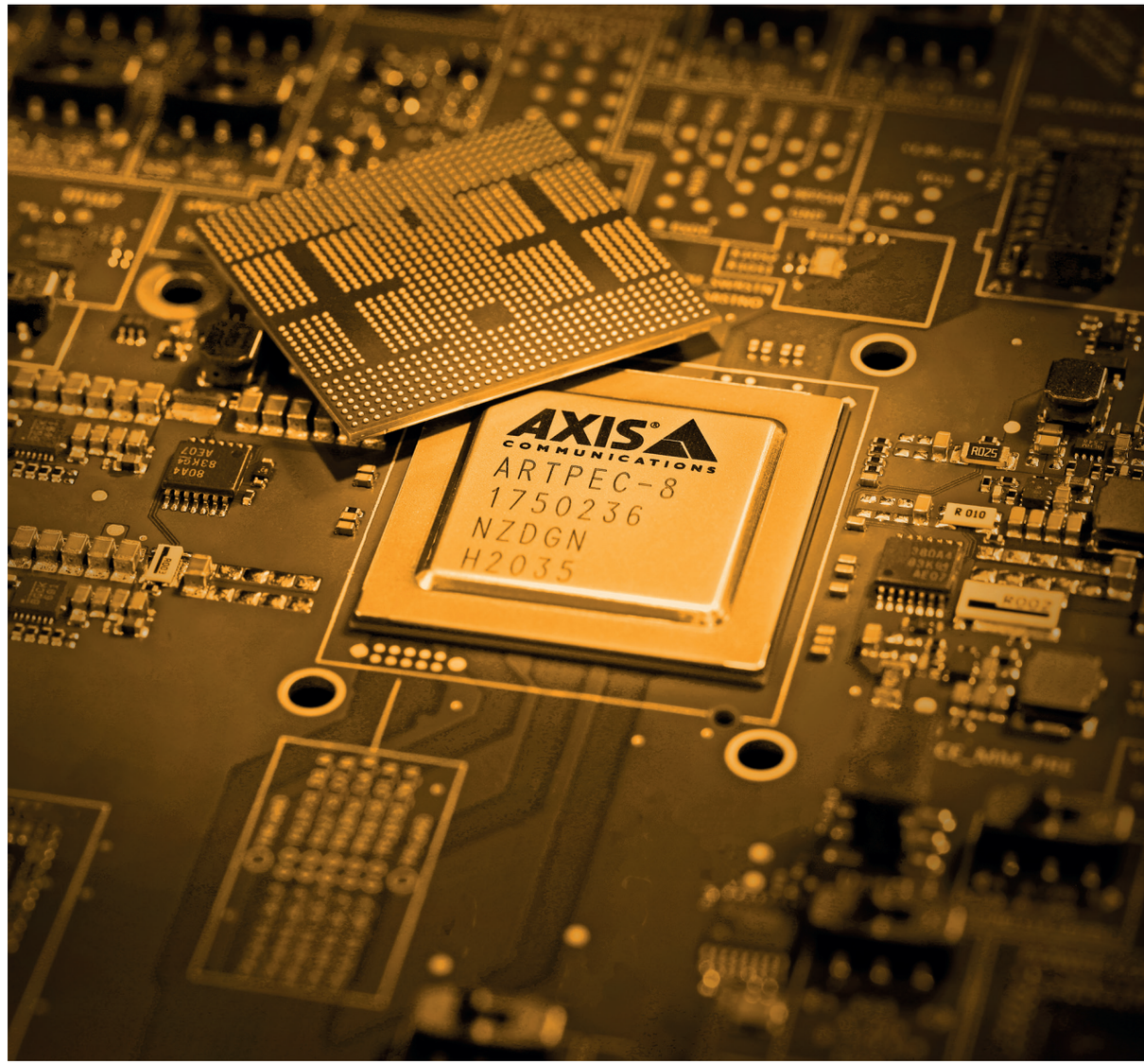
Axisデバイスに内蔵されているセキュリティ機能により、安全な起動とオンボーディングが可能となるだけでなく、機密情報を確実に保護することができます。

Axis Edge Vaultサイバーセキュリティプラットフォーム
こ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が、ネットワーク内におけるAxisデバイスの信頼性を保証する強固な基盤となります。Axis Edge Vaultには、以下のような機能*が含まれています。

- **セキュアなキーストア**：これには、暗号キーを安全に保管できる暗号コンピューティングモジュールが含まれています。これにより、デバイスが侵害された場合でも、デバイスのIDやその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。暗号化コンピューティングモジュールには、Axisシステムオンチップ（SoC）に組み込まれているTEE（Trusted Execution Environment）が含まれます。これには、マザーボードの別個チップであるセキュアエレメントやTPM（Trusted Platform Module）も含まれます。Axisデバイスは、こうした3つのモジュールのいずれかまたは任意の組み合わせを使用して構築されています。
- **署名付きファームウェア＆セキュアブート**：これにより、デバイスで正規のAxisオペレーティングシステム（AXIS OS）以外はダウンロードおよび実行することができません。
- **Axisデバイス ID**：IEEE 802.1ARに準拠したこのIDにより、安全なデバイスの特定とネットワークでのオンボーディングが実現します。
- **FS（暗号化ファイルシステム）**：これにより、システムインテグレーターから最終顧客への転送時など、デバイスの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のを防止することができます。
- **署名付きビデオ**：これにより、ユーザーはキャプチャ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。

** 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 プロダクトセレクターで、製品でサポートされている機能を確認してください。*

詳細情報：Axis Edge Vault



デフォルト設定

製品のセキュリティ機能に加え、Axisデバイスは事前定義されたデフォルトの保護設定で提供されます。

認証情報＆ネットワークプロトコル

Axisデバイスは、ユーザー名とパスワードを含めてアカウントを設定するまで動作しません。これを設定した後は、その認証情報が適切に提供された場合にのみ、管理機能やビデオストリームにアクセスできるようになります。

また、デバイスインターフェースへのアクセスについてはHTTPとHTTPS、ビデオと音声ストリーミングにはRTSPとRTP、サードパーティ製アプリケーションによるAxisデバイス検出にはUPnPやBonjourなど、Axisデバイスではデフォルトで最小限のネットワークプロトコルとサービスのみが有効化されています。

顧客のゼロトラストネットワークへの対応

Axisは、独自のAxisデバイスID、HTTPSプロトコルのサポート、IEEE 802.1X標準への準拠、IEEE 802.1ARに準拠したデバイス認証、IEE 802.1AE MACsecに対応した自動データ暗号化をサポートする製品を生産することで、ゼロトラスト要件に対応しています。

HTTPSはデフォルトで有効化されているため、デバイスのパスワードを安全に設定することができます。また、これにより、HTTPSを使用するビデオ管理ソフトウェアで、信頼できるCA署名付きSSL証明書を検証できるようになります。これは、新しい製品のAxisデバイスIDでサポートされています。

Axis製品でデフォルトで有効化されているIEEE 802.1X、IEEE 802.1AR、IEEE 802.1AEのサポートにより、デバイスの自動オンボーディング、認証、エンドツーエンドの暗号化が可能となります。これにより、ITプロフェッショナルは標準メカニズムを使用して、IEEE 802.1Xをサポートし、Axisデバイスを企業ネットワークに効率的かつ安全に統合できるようになります。Arubaネットワークでデバイスを使用している顧客は、統合ガイドをダウンロードすることができます。これには、Axisデバイスの安全なオンボーディングと管理に関するベストプラクティスの構成の概要が記載されています。

詳細情報：エンタープライズIT向けのAxisソリューション

実装

実装時のサイバーセキュリティ

Axisデバイスは、ノートパソコン、デスクトップコンピューター、モバイルデバイスなどと同様のネットワークエンドポイントです。しかし、ノートパソコンとは異なり、ユーザーがAxisデバイスで有害であり得るWebサイトにアクセスすること、悪質な電子メールの添付ファイルを開くこと、信頼性の低いアプリケーションをインストールすることはありません。それでも、ネットワークビデオ、音声、アクセスコントロール製品には、接続されているシステムにリスクをもたらし得るインターフェースが備わっています。

Axis製品に関するハードニングガイドには、サイバーリスクへの曝露を軽減する上で有用となる推奨事項が記載されています。以下の基本的な推奨事項をご覧ください。たとえば、デバイスを構成する前に工場出荷時のデフォルト設定を実行して、不要なソフトウェアや構成が含まれていないことを確認することが勧められます。

また、デバイスで最新のAXIS OSが実行されていることを確認してください。これには、特定のデバイスの最新のセキュリティパッチやバグ修正が含まれています。

強力なパスワードを設定すること、デバイスのWebインターフェースへの直接アクセスを制限すること、HTTPS（クライアントとデバイス間のデータトラフィックが暗号化される）のみが使用されるようにデバイスを構成すること、未使用のサービスと機能を無効化することで、不要なリスクを軽減する必要があります。また、デバイスの日付と時刻を正しく設定することで、正確なシステムログを保持し、HTTPSやIEEE 802.1Xなどのサービスで重要となるデジタル証明書を検証および使用できる状態を維持することも重要となります。

Axisデバイスを効率的にローカルで構成および管理できるAxisツールとして、AXIS Device Managerが挙げられます。これにより、デバイスの認証情報の管理、デジタル証明書の展開、使用されていないサービスの無効化、AXIS OSのアップグレードなど、インストールおよびセキュリティタスクのバッチ処理が可能となります。デバイス管理ソフトウェアの詳細については、次ページをご覧ください。

AXIS OSベースのデバイスの完全かつ拡張されたハードニングに関する推奨事項については、AXIS OSハードニングガイドをご覧ください。Axisビデオ管理ソフトウェアとネットワークスイッチのハードニングガイドは、サイバーセキュリティのリソースページからアクセスすることができます。Axisデバイスは、エンタープライズITインフラストラクチャーとネットワークにシームレスに統合することができます。この詳細については、エンタープライズIT向けのAxisソリューションを参照してください。

Axisは、リスクを軽減し、Axis製品とサービスを最新の状態に維持して保護する上で有益となるツール、文書や資料、トレーニングを提供しています。**当社のサイバーセキュリティのリソースをご覧ください。**

稼働

稼働中のデバイスのサイバーセキュリティ

サイバーセキュリティを維持する上で、デバイスの稼働時に注意すべき最も重要な事柄として、デバイスのファームウェアまたはオペレーティングシステム(AXIS OS)を必ず最新の状態に維持することが挙げられます。こうすることで、デバイスに最新のセキュリティパッチとバグ修正が確実に適用されます。署名付きファームウェアやセキュアブートなどのAxisデバイスの機能により、正規のAXIS OS以外はインストールすることも実行することもできません。無料で提供されるAXIS OSバージョンは、アクティブトラックかLTS(長期サポート)トラックのいずれかとなります。アクティブトラックのAXIS OSバージョンでは新機能がサポートされていますが、互換性問題のリスクを最小限に抑えるために、LTSトラックではこれがサポートされていません。しかし、セキュリティパッチとバグ修正は両方のトラックに含まれています。Axisセキュリティ通知サービスにサインアップすると、新たに発見された脆弱性を常に確認することができます。脆弱性に関する通知には、影響を受ける製品を新しいデバイスソフトウェアで修正する方法の説明が記載されています。

多数のデバイスのオペレーティングシステムをより簡単かつ効率的に更新できるように、AxisはAXIS Device ManagerやAXIS Device Manager Extendなどのデバイス管理ソフトウェアを提供しています。

デバイス管理ソフトウェアの機能と仕組み

デバイス管理ソフトウェアを利用することで、ネットワークに接続されているすべてのカメラ、エンコーダ、アクセスコントロール、音声機器、その他のデバイスの完全なインベントリをリアルタイムで迅速に収集することができます。これにより、ネットワーク全体をスキャンし、新しいデバイスや更新されたデバイスが検知されたら、そのモデル番号、IPアドレスとMACアドレス、デバイスソフトウェアバージョン、証明書のステータスなど、すべての重要な情報を取得することが可能です。

全体像の完全な把握

ネットワークエコシステムの全体像を非常に詳細に把握することで、容易にすべてのデバイスに一貫したライフサイクル管理ポリシーと慣行を実装し、すべての主要なインストール、展開、構成、セキュリティ、メンテナンスタスクを安全に管理することが可能となります。

サイバーセキュリティポリシーやデバイス管理のベストプラクティスに関する文書を作成することで、パスワードの強度やユーザーがパスワードを変更するべき頻度、また攻撃対象領域(アタックサーフェス)を削減するために未使用のサービスをオフにする必要性などを明確化する必要があります。

デバイスの脆弱性をスキャンする頻度、およびメーカーが既知のエクスプロイトを公開した際にリスクレベルを評価する手順を定めることも重要です。

時間と労力の節約

デバイス管理ソフトウェアを活用することで、組織はサイバーセキュリティリスクを管理する上でかかる時間や労力を節約することができます。

これにより、以下が可能となります。

> システムの変更、デバイスソフトウェアの更新、新しいデジタル証明書を該当するデバイスすべてに同時に実行する。

> 簡単にセキュリティ設定を作成または再構成してネットワーク全体に適用し、すべてのデバイスが最新のセキュリティポリシーとセキュリティ対策を満たしていることを確認する。

> すべてのデバイスで最も安全な最新のファームウェアバージョンが実行されていることを確認する。

> ネットワーク全体のユーザー特権レベルを管理し、変更を構成する。

リアルタイムの洞察の取得

デバイス管理ツールを利用することで、組織はエコシステムの状態に関するリアルタイムの洞察を得ることができます。たとえば、最新のソフトウェアや証明書で更新する必要があるデバイスを把握すること、また製品の製造中止やサポート終了日に関する情報を取得して、デバイスの交換時期を計画することができます。

Axisのデバイス管理ツール

当社のデバイス管理ソフトウェア「AXIS Device Manager」と「AXIS Device Manager Extend」を活用することで、Axisデバイスを効率的に管理することができます。AXIS Device ManagerとAXIS Device Manager Extendは相互に補完させて使用できるように設計されています。

AXIS Device Manager

AXIS Device Managerにより、新しいデバイスのインストールと構成を迅速かつ簡単に行うことができます。このオンプレミスツールでは、ソフトウェアアップグレードやアプリケーションのインストールなど、すべての主要なインストール、セキュリティ、運用タスクがサポートされています。これにより、Axisデバイスにバックアップや復元の設定を構成すること、また保証ステータスを表示することが可能となります。また、HTTPSやIEEE 802.1X証明書など、サイバーセキュリティ制御を適用することもできます。

詳細情報：AXIS Device Manager

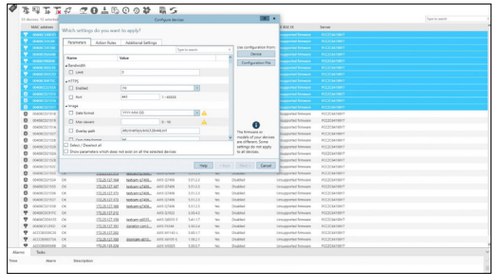
AXIS Device Manager Extend

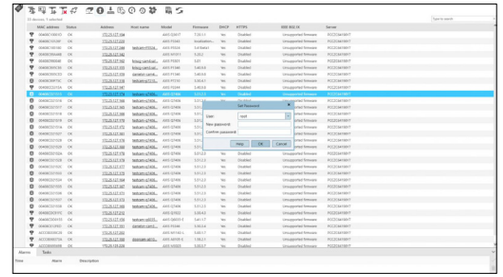
複数の拠点を持つ組織に最適なAXIS Device Manager Extendを利用することで、すべてのサイトの資産をリモートで管理することができます。この使いやすいアプリケーションにより、AXIS OSのアップグレード、セキュリティポリシーの定義付け・適用・実施、アプリケーションの管理など、重要なメンテナンス作業が簡素化されます。ライブダッシュボードが備わっているため、オフラインのデバイスや保証期間を過ぎたデバイスなど、システムに潜在的に存在する問題に関する状況認識を高め、より迅速にトラブルシューティング行うことができます。また、セキュリティ脅威を最小限に抑え、脆弱性を軽減する上で有用となるデバイス設定の推奨事項も含まれています。セキュリティポリシーをすべてのAxisデバイスに同時に定義、適用、強制することができます。

詳細情報：AXIS Device Manager Extend

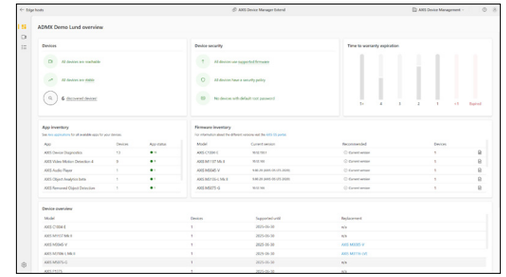
セキュリティ侵害が発生した場合

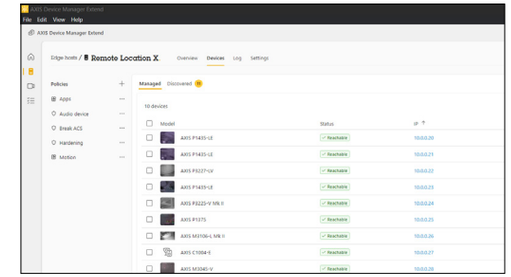
ネットワークでセキュリティ侵害が発生した場合に備えて、Axisは、Axisネットワークデバイスのフォレンジック分析の実施に有用となる AXIS OS フォレンジックガイドを提供しています。





AXIS Device Managerインターフェースのスナップショット





AXIS Device Manager Extendインターフェースのスナップショット

廃棄

廃棄

更新とパッチは製品のサイバーセキュリティを維持するための最善策となりますが、サポートが終了している古い製品の場合は、更新とパッチを入手できなくなる可能性があります。サイバーセキュリティという観点から、パッチが適用されていない古い製品は大きなリスクとなります。1つでも見逃したデバイスがあれば、これが攻撃の侵入口となる可能性があります。

サポートが終了し、パッチが適用されていない可能性のあるデバイスを実行することで発生するリスクを回避するため、製品の廃止を計画することも非常に重要となります。Axisは製品のオペレーティングシステムのサポート終了日を公開しているため、デバイスの廃止や交換の準備を適時に整えることができます。また、AXIS Device Manager Extendを活用している場合は、システムにおけるすべてのデバイスの保証、製品製造中止、サポート終了に関する情報を取得することができます。

廃止されたデバイスに入っているデータを削除することも重要な作業です。工場出荷時のデフォルト設定を実行すると、デバイスからすべての設定とデータが直ちに消去されます。製品廃止に関する詳細については、AXIS OS ポータルにアクセスしてください。

コンプライアンス

さまざまな国でサイバーセキュリティ関連の法規制がますます多く制定されています。企業は事業を展開する国の法規制を遵守しなければなりません。同様に、製品やサービスの認証など、業界や組織により準拠が義務付けられる基準や規格も増えています。法規制を確実に遵守し、ビジネスプロセス関連のガイドラインや仕様を実装することは、すべての利害関係者の責任となります。

ベースラインとしてのサイバーセキュリティコンプライアンス

サイバーセキュリティコンプライアンスとは、当局によって定義された基準や規制要件に従うことを指します。また、規格や認証が重要であることは言うまでもありませんが、これは全体像の一部にすぎません。

規格や認証に準拠することが「価値判断を伴わない官僚主義的な確認手続き」になってしまうリスクは常に存在します。

サイバーセキュリティコンプライアンスの状況は継続的に変化しており、かつては「あれば便利」だった要素が急速に「必須要素」になりつつある現状を認識することが重要です。

そのため、組織は標準や認証をベースラインとして、つまり目標ではなく最小要件として捉える必要があります。可能な限り最も安全な方法で使用・運用できる製品とサービスをサプライヤーが提供することが真の目標です。また、顧客が継続的にサイバーセキュリティを維持できるように、そのニーズをサポートできるガイダンスを高い透明性をもって顧客に提供することが重要となります。

規制

サイバーセキュリティ規制は、組織にシステムと情報を保護させること、および組織が提供する製品とサービスについて最低限のセキュリティを確保させることを目的とするものです。いくつかの重要な規制とその適用例を挙げてみましょう。

2023年にNIS2指令が発効し、EU（欧州連合）加盟国は2024年10月までにこれを国内法に反映させる必要があります。この指令により、重要分野で事業を展開するすべてのEU企業に、高水準の共通レベルのサイバーセキュリティ対策を構築することが義務付けられます。企業がサイバーセキュリティの義務を怠ると、たとえそれがサプライヤーに起因する結果であったとしても、企業側が罰せられる可能性があります。

そのため、今後はベンダー評価とサプライチェーンのセキュリティがさらに重要になると考えられます。この指令により、間接的にメーカー、輸入業者、ディストリビューターに義務が課されるため、こうした企業は製品のライフサイクル全体を通して注意義務を確実に履行する必要があります。

2023年12月には、デジタル要素を備えたハードウェアとソフトウェア製品の共通サイバーセキュリティ標準を定義する新規制「サイバーレジリエンス法（CRA）」が欧州理事会と欧州議会で暫定合意に達しました。これには、IoTデバイスなど、別のデバイスやネットワークに直接または間接的に接続される製品が含まれます。同法案は、透明性を高め、データ保護を確実に強化しながら、サイバーセキュリティインシデントを削減することを目的としたものです。英国でも、英国製品セキュリティおよび電気通信インフラストラクチャー（PSTI）法と呼ばれる同様の法案が可決されており、2024年4月に施行されます。

組織が米国政府と取引する場合、その欧州企業はCMMC（サイバーセキュリティ成熟度モデル認証）などの認証を取得する必要があります。CMMCの場合は、サイバーセキュリティ対策の内部管理に基づいて監査認証を取得しなければなりません。

サイバーセキュリティを確保するには、継続的な警戒とメンテナンスが必要です。

規格/標準＆認証/認定

大半の規格や認証では、機能、対策、プロセスに焦点が当てられています。これにより、セキュリティが不可欠な要素として配置されていることを確認することが目的です。こうした認証は、ソフトウェアの脆弱性を発見するための侵入テストやバグバウンティプログラムなど、第三者企業による試験によって補完することができます。

製品認証を取得することで、顧客や政府の安心感は高まりますが、一般的にこうした認証の有効期限は1年で、期限が来れば製品の再認証が必要となります。市場では、新規テクノロジーや機能が速い速度で絶えず開発および公開されていることで、その規格や認証が後手に回る可能性があります。

また、規格に準拠することでサイバーセキュリティ体制が向上するとしても、これによってサイバーセキュリティインシデントを完璧に防止できるという保証はないことに注意してください。組織は、自主的に脅威とセキュリティポリシーを継続的に確認していく必要があります。

Axisを選ぶ理由

サイバーセキュリティの推進

Axisでは、サイバーセキュリティを不可欠な要素として企業の中核に据えています。当社はこのサイバーセキュリティを基盤として、内部情報セキュリティシステム、サプライチェーン管理、製品とサービスの開発、ソフトウェアの脆弱性の管理を実施しています。当社にとってサイバーセキュリティは、透明性が鍵となる共有の継続的責任となっています。顧客が当社の製品を可能な限り最も安全な方法で使用できるようにすることを当社は目指しています。そのため、当社の製品はサイバーセキュリティ機能と保護機能の役割を果たすデフォルト設定を組み込んで設計および製造されています。当社がハードニングガイドを提供しているのも、この当社の目標を達成するためです。当社は継続的に脅威を監視し、セキュリティを向上させる方法を検討しています。CVE採番機関（CNA）の認定を受けている当社は、新たに脆弱性が発見された場合にはそれを公開してパッチを提供することで、顧客が適切かつ適時に措置を講じられるよう取り計らっています。また、製品設置後も引き続きAxisデバイスのセキュリティを強化できるように、ソフトウェアアップグレードを提供しています。

さらに、AXIS Device Manager や AXIS Device Manager Extendといったツールを提供することで、Axisデバイスの管理を簡素化し、ライフサイクル全体を通じてサイバーセキュリティのリスクを軽減することに努めています。

Axisを選ぶべきその他の理由

> **品質を重視するAxisの取り組み：**
顧客の安心感を高めるために、当社の製品はすべて、広範な試験に合格しています。

> **革新的なテクノロジー：**
テクノロジーと人間の想像力を融合することで、性能とユーザビリティ両方の改善に取り組んでいます。オープンな業界標準に基づいて構築されているため、高い柔軟性と拡張性を備え、容易に統合することができます。

> **全レベルでサステナビリティを考慮に入れた製品：**
環境に優しい開発に継続的に取り組み、その姿勢で高い評価を受けているAxisは、持続可能な材料を使用しています。2022年に発売されたAxisのカメラとエンコーダの約90%がPVCフリーの製品です。

> **地域的な専門知識を備えてグローバルに展開：**
Axisは、ネットワークビデオ製品における世界最大の導入実績を誇り、50か国以上に従業員を擁しています。当社は洞察と経験を共有しながら、常に開発状況を最先端に維持しています。

> **パートナーシップのパワー：**
パートナーとの関係構築を重視する当社の取り組みにより、Axisは市場で最も統合されたカメラブランドに成長しました。

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。