サイバーセキュリティQ&A

ユーザーマニュアル

その他の質問や回答については、Axisの*FAQ*データベースをご覧ください。

一般的な質問

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慣行には、コンピューター、電子通信システムとサービス、有線/電子通信、保存された情報の可用性、完全性、安全性、真正性、機密性、非否認性を保証するための、損害を防止し、リストアするプロセスが含まれます。

サイバーセキュリティとは、長期にわたってリスクを管理することです。リスクは、完全に排除することはできず、軽減することしかできません。

サイバーセキュリティの管理には、一般的に何が必要ですか?

サイバーセキュリティは製品、人、テクノロジーに関するもので、継続的なプロセスです。

そのため、組織のさまざまな側面を**特定**し、評価する必要があります。これには、装置、システム、ソフトウェア、ファームウェアのインベントリを作成すること、ミッションクリティカルな目標を設定すること、手順とセキュリティポリシーを文書化すること、リスク管理戦略を導入すること、資産に関するリスク評価を継続的に実施することなどが含まれます。

そして、サイバー攻撃に対して優先すべきと判断したデータ、装置、システム、施設を**保護**するためのセキュリティ制御対策を実施する必要があります。

また、サイバー攻撃を**検知**して適時に対策を講じるのに役立つアクティビティの開発と実施も必要です。これにはたとえば、セキュリティ情報イベント管理 (SIEM) システムや、ネットワークデバイスやネットワーク管理ソフトウェアのデータを管理し、異常な行動や潜在的なサイバー攻撃に関するデータを収集し、そのデータを分析してリアルタイムのアラートを提供するSecurity Orchestration, Automation and Response (SOAR) システムが必要になります。Axis装置では、お客様がお使いのSIEMまたはSOARシステムの主要なデータソースであるSYSログとリモートSYSログをサポートしています。

また、サイバーセキュリティ管理には、サイバーセキュリティインシデントが検知された後に**対処**するための手順の開発と実施も必要です。それには、地域の規制や社内ポリシーに加え、サイバーセキュリティインシデントの開示要件も考慮する必要があります。Axisは、サイバーセキュリティ攻撃時にAxis装置が侵害されたかどうかを理解するのに役立つ、『*AXIS OS Forensic Guide*』を提供しています。

レジリエンス計画を維持し、サイバーセキュリティインシデントによって侵害された機能やサービスを**リカバリ**またはリストアするためのアクティビティの開発と実施も重要です。たとえば、*Axisデバイス管理アプリケーション*を使用すると、リストアポイントがサポートされているため、Axisデバイスを簡単にリストアできます。リストアポイントとは、ある時点におけるシステム構成の「スナップショット」を保存したものです。関連するリストアポイントがない場合でも、このツールは、すべての装置をデフォルトの状態に戻し、保存された構成テンプレートをネットワーク経由でプッシュするのに役立ちます。

サイバーセキュリティリスクとは何ですか?

RFC 4949インターネットセキュリティ用語集によると、サイバーセキュリティリスクとは、特定の脅威が特定の脆弱性を悪用し、特定の有害な結果を引き起こす可能性として表される損失の予測値です。

長期的にリスクを十分に低減させるには、明確なシステムポリシーとプロセスを定義することが重要です。推奨される方法は、ISO 27001やNISTなど、明確に規定されたIT保護フレームワークに従って対策を講じることです。小規模の組織にとってこの作業は負担になる場合もありますが、最小限のポリシーとプロセスのドキュメントを用意することは、何も持たないよりはるかに優れています。

リスクを評価し、優先順位を付ける方法については、『*Cybersecurity Reference Guide*』を参照してください。

脅威とは何ですか?

脅威は、資産やリソースを侵害したり、これらに損害を与えたりする可能性があるものと定義できます。一般に、人はサイバー脅威というと、悪意のあるハッカーやマルウェアを連想する傾向があります。しかし実際には、事故や意図しない誤用、ハードウェア障害などが悪影響を及ぼすことも少なくありません。攻撃は日和見的な攻撃と標的型の攻撃に分類できます。現在の攻撃の大多数は、機会があったから攻撃するという日和見的攻撃です。このような攻撃では、フィッシングやプロービングなどの低コストの攻撃方法が使用されます。標準レベルの対策を講じることで、日和見的な攻撃がもたらすほとんどのリスクを軽減することができます。

特定の目標を持ち、特定のシステムを標的とする攻撃者から保護する方が難しくなります。標的型攻撃では、日和見的な攻撃者と同じ低コストの攻撃方法が使用されますが、最初の攻撃が失敗すると、攻撃者は決意を深め、より洗練された方法で目標を達成するために時間とリソースを費やすようになります。彼らにとっては、「どれだけの価値があるか」が重要なのです。

最も一般的な脅威は何ですか? それらの脅威にどう対処できますか?

システムの意図的または偶発的な誤用

システムに対して正当なアクセス権を持つ人物は、どのシステムにとっても最も一般的な脅威の1つです。彼らは、許可されていないサービスにアクセスできます。彼らがシステムから情報を盗んだり、システムに意図的に損害を加えたりする可能性があります。また、人は間違いを犯すものです。問題を解決しようとして、システムのパフォーマンスを不注意に低下させてしまうこともあります。正当なユーザーに機密情報を流出させようとするソーシャルエンジニアリングの被害者になることもあります。大切なもの (アクセスカード、スマートフォン、ノートパソコン、書類など) を紛失したり、置き忘れたりすることもあります。ユーザーのコンピューターが侵害され、意図せずにシステムにマルウェアが感染する場合もあります。

推奨される対策としては、ユーザーアカウントのポリシーとプロセスを定義する、十分なアクセス認証方式を導入する、ユーザーアカウントと権限を長期的に管理するツールを使用する、露出を減らす、サイバー意識を高めるトレーニングを実施するなどがあります。

Axisは、*ハードニングガイド*と、*デバイスおよびビデオ管理ソフトウェアによって、この脅威への対策をサポートします。*

物理的な改ざん＆妨害

物理的に露出している機器は、いたずら、盗難、接続の切断、向きの変更、ケーブルの切断などの被害に遭う可能性があります。

推奨される対策としては、ネットワーク周辺機器 (サーバーやスイッチなど) を施錠できるエリアに設置する、手が届きにくい場所にカメラを取り付ける、物理的に露出している場合は保護ケーシングを使用する、ケーブルを壁やコンジット内に設置して保護するなどがあります。

Axisは、装置用*保護ハウジング*、いたずら防止ネジ、SDカードデータを暗号化する機能を備えたカメラ、カメラビューに対するいたずらを検知する機能、ケーシングが開けられたことを検知する機能などでこの脅威に対抗できるよう支援いたします。

ソフトウェアの脆弱性の悪用

ソフトウェアベースのすべての製品に、悪用される可能性のある脆弱性 (既知または未知) があります。ほとんどの脆弱性はリスクが低く、悪用するのが非常に難しいか、悪影響の及ぶ範囲が限定的です。まれに、重大な悪影響を及ぼす脆弱性が発見され、悪用されることがあります。MITREは、リスクの軽減に役立てられる共通脆弱性識別子 (CVE: Common Vulnerabilities and Exposures) の大規模なデータベースをホストしています。

推奨される対策としては、システム内の既知の脆弱性の数を最小限に抑えるために継続的なパッチ適用プロセスを導入する、既知の脆弱性の調査と悪用を難しくするためにネットワークの露出を最小限に抑える、欠陥を最小限に抑えるポリシーとプロセスに従って業務を進め、パッチを提供し、発見された重大な脆弱性について透明性を持つ信頼できるサブサプライヤーと連携するなどがあります。

Axisは、Axisソフトウェアにおける悪用可能な脆弱性を最小限に抑えることを目的とした*Axisセキュリティ開発モデル*と、お客様が適切な措置を講じるために認識しておく必要がある脆弱性を特定、修正、公表する*Axis脆弱性管理ポリシー*によって、このような脅威に対処しています。(2021年4月時点において、*AxisはAxis製品の共通脆弱性識別子採番機関*であり、MITRE Corporationの業界標準プロセスに当社のプロセスを適合させることができます。) また、Axisはどのように露出を抑え、管理を追加して悪用のリスクを低減すればよいのかの推奨事項を含む*ハードニングガイド*を提供しています。AxisはAxisデバイスのオペレーティングシステムを最新の状態に保つために、*各種デバイスソフトウェアトラック*をユーザーに提供しています。主なトラックは以下の2つです。

1. アクティブトラックは、新機能や機能性の追加に加え、バグ修正とセキュリティパッチも含むデバイスのソフトウェア更新を提供します。
2. 長期サポート (LTS) トラックは、サードパーティ製システムとの非互換性リスクを最小限に抑えつつ、バグ修正とセキュリティパッチのみをサポートするデバイスのソフトウェア更新を提供します。

サプライチェーン攻撃

サプライチェーン攻撃は、サプライチェーン内の安全性の低い要素を標的にして組織に損害を与えようとするサイバー攻撃です。この攻撃では、ソフトウェア/オペレーティングシステム/製品を侵害し、管理者がそれらをシステムにインストールするように仕向けます。製品はシステム所有者への出荷中に侵害される可能性があります。

推奨される対策としては、信頼できる検証済みの提供元からのソフトウェアのみをインストールするポリシーを導入する、インストールする前にソフトウェアチェックサム (ダイジェスト) とベンダーのチェックサムを比較してソフトウェアの完全性を確認する、納品された製品に改ざんの兆候がないか確認するなどがあります。

Axisは、この脅威にさまざまな方法で対抗しています。Axisは、インストールする前に管理者が完全性を検証できるように、ソフトウェアとチェックサムを公開しています。装置の新しいオペレーティングシステム (OS) を読み込む際、Axisネットワーク装置はAxisによって署名された装置のソフトウェアのみを受け入れます。Axisネットワーク装置での*セキュアブート*も、Axisの署名付きOS以外は装置で実行できないようになっています。また、各装置には一意のAxis装置IDがあり、このIDによって、その装置がAxisの純正品であることをシステムが検証することができます。このようなサイバーセキュリティ機能の詳細については、ホワイトペーパー*Axis Edge Vault*をご覧ください。

脅威の詳細については、Cybersecurity reference guide (サイバーセキュリティリファレンスガイド) を参照してください。

脆弱性とは何ですか?

脆弱性は、システムを攻撃したり、システムにアクセスしたりする機会を敵対者に与えます。脆弱性は、欠陥、機能、人的ミスなどに起因します。攻撃者は既知の脆弱性を悪用しようとし、その多くは複数の脆弱性を組み合わせて使用します。成功した侵害の大半は、人的ミス、システム構成の不備、システムメンテナンスの不備によるもので、多くの場合、適切なポリシーの欠如、責任の所在があいまい、組織の意識の低さなどが原因です。

ソフトウェアの脆弱性とは何ですか?

装置のAPI (アプリケーションプログラミングインターフェース) とソフトウェアサービスには、攻撃で悪用される可能性のある欠陥や機能がある場合があります。製品に欠陥がないことを保証できるベンダーは存在しません。欠陥が分かっていれば、セキュリティ制御対策を講じてリスクを軽減することができます。一方、攻撃者が新たな未知の欠陥を発見した場合は、被害者がシステムを保護する時間がないので、リスクが増大します。

共通脆弱性評価システム (CVSS) とは何ですか?

共通脆弱性評価システム (CVSS) は、ソフトウェアの脆弱性の深刻度を分類する方法の1つです。この方法では、脆弱性がどの程度悪用されやすいかと、どのような悪影響があるかに注目します。

スコアは0~10の値で付けられ、10が最も深刻です。公開されている共通脆弱性識別子 (CVE) レポートの多くに、CVSS値が記載されています。

Axisでは、ソフトウェア/製品で識別された脆弱性がどの程度重大であるかを判断する手段の1つとして、CVSSを使用しています。

Axisに関するご質問

サイバーセキュリティの詳細と、サイバーインシデントから製品やサービスをより確実に保護するためにできることを理解するのに役立つトレーニングとガイドを教えてください。

リソースのWebページから、ハードニングガイド (*AXIS OS Hardening Guide*、 *AXIS Camera Station Pro System Hardening Guide* 、 *Axis Network Switches Hardening Guide*など)、ポリシードキュメントなどにアクセスできます。Axisでは、サイバーセキュリティに関するeラーニングコースも提供しています。

装置の最新のオペレーティングシステムは、どこで見つけることができますか?

「*装置のソフトウェア*」で、お使いの製品を検索してください。

装置のオペレーティングシステムを簡単にアップグレードする方法を教えてください。

デバイスソフトウェアは、*Axisビデオまたはデバイス管理ソフトウェア*を使用してアップグレードできます。

Axisのサービスに障害が発生した場合、どのように連絡が来ますか?

*status.axis.com*にアクセスしてください。

発見された脆弱性に関する通知はどうすれば受け取れますか?

*Axis Security Notification Service*にお申し込みください。

Axisは脆弱性をどのようにして管理していますか?

*Axis脆弱性管理*を参照してください。

Axisはどのようにしてソフトウェアの脆弱性を最小限に抑えているのですか?

記事「*Making cybersecurity integral to Axis software development*」をお読みください。

Axisでは、装置のライフサイクル全体でサイバーセキュリティをどのようにサポートしていますか?

「*サイバーセキュリティへのライフサイクルアプローチ*」をご覧ください。

Axis製品にはどのようなサイバーセキュリティ機能が組み込まれていますか?

以下をご覧ください:

- *Axis Edge Vault*
- *AXIS OS*
- *デバイスのライフサイクルを通じてサイバーセキュリティをサポート*

AxisはISO認証を取得していますか? また、そのほかにどのようなサイバーセキュリティ関連の規制に準拠していますか?

はい。Axisは*ISO/IEC 27001:2023*の認証を取得しており、ソフトウェア、クラウドサービス、ITインフラストラクチャーの開発および運用に関する要件を満たす情報セキュリティマネジメントシステム (ISMS) を設置しています。

Axis Communications UK Ltd.は、Cyber Essentials (証明書番号：IASME-CE-017710) およびCyber Essentials Plus (IASME-CEP-004245) の認証を取得しています。

*AXIS OS 11*以降を実行するAxisデバイスは、*ETSI EN 303 645*サイバーセキュリティ規格の認証を取得しています。また、AXIS OSネットワーク製品には、ドイツ連邦情報セキュリティ庁 (*BSI - Bundesamt für Sicherheit in der Informationstechnik*) が発行したITセキュリティラベル (IT-Sicherheitskennzeichen) が付いています。

Axisのサイバーセキュリティコンプライアンスと認証に関する最新情報について詳しくは、*Axis Trust Center*をご覧ください。

私の会社でのNIS 2への準拠についてAxisはどのようなサポートを提供していますか?

*NIS 2*に関する記事をご覧ください。

T10189380_ja

2025-09 (M5.2)