アクシスコミュニケーションズ・サイバーセキュリティ・マガジン

セキュリティにおけるパートナー

サイバーセキュリティ環境の
インサイト＆インスピレーション

スタート >

AXIS COMMUNICATIONS

概要

堅牢なセキュリティフレームワーク

ご存知かもしれませんが、サイバーセキュリティ対策のための唯一のソリューションというものは存在しません。また、サイバーセキュリティ攻撃を完璧に防ぐ「鋼鉄の鎧」のような機能が組み込まれている製品というものもありません。どちらかと言えば、サイバーセキュリティとは信頼性のあるパートナーシップの問題なのです。つまり、サブサプライヤーから製造業者、設置担当者、インテグレーター、そしてエンドユーザーに至るまでのそれぞれが重要な役割を負っているということです。これは、対策を1回限り講じれば済むというものでもなく、進行形のプロセスです。

責任あるサイバーセキュリティパートナーの1社として、当社は本記事と共にさまざまなヒントやインスピレーションをお届けします。貴社が最新の状態を維持し、セキュリティ対策を講じる上で有効な情報が含まれています。これが貴社のお役に立てば幸いです。

先に進む前に、米国国立標準技術研究所（NIST）のリスク管理フレームワークを簡単にご紹介しておきます。サイバーセキュリティは本質的にリスク管理の問題であることから、リスク管理フレームワークを利用して、事業や組織に対するリスク発生の確率と潜在的な危害レベルをまず評価することが重要となります。さまざまなリスク管理フレームワークが存在しています。

AxisはNISTフレームワークに整合したサイバーセキュリティアプローチを取っています。世界的に使用されているNISTガイドラインは、大企業や大組織だけでなく、中小企業にも適したフレームワークとして高い評価を得ています。貴社が異なるフレームワークを使用している場合でも、NISTフレームワークと一致している要件が多く含まれているかもしれません。

NISTフレームワークは、確認、保護、検知、対応、回復という5つの機能が柱となっています。当社のウェブサイト「www.axis.com/cybersecurity」に、各機能の詳細、サイバーセキュリティパートナーとしての当社の役割、および貴社自身の役割が記載されています。

では、本マガジンをお楽しみください。

目次

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）
- 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。

自社のアセットとリソースに注意

ビデオシステムに関しては、明らかに保護に必要なリソースは、カメラによるビデオフィードとなります。アセットは、ビデオ管理システム（VMS）のビデオ録画です。通常、アクセスはユーザー権限に従って制御されます。考慮すべき他のアセットとして、ユーザーアカウントとパスワード、構成、オペレーティングシステム、ファームウェアとソフトウェア、そしてネットワーク接続を備えたデバイスが挙げられます。

詳しく読む >

注意する必要のある脅威

サイバー脅威対策の第一歩は、自社に発生し得る脅威を把握することです。機密性、整合性、可用性は、ITシステムを保護する上で重要な要素と見なされます。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と悪用される可能性のある脆弱性を見ていきましょう。

映像監視における3つの最も一般的なサイバー脅威

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＆妨害

詳しく読む >

1

思いがけない人的ミス＆不注意な行為

ネットワークを保護するためにどれほど優れたテクノロジーを導入しても、たった1人のスタッフが電子メール内の危険なリンクを攻撃者の意図通りにクリックしてしまえば、その攻撃者はシステムに侵入することができます。そのため、サイバー犯罪者にとってはこれは最も簡単な攻撃手段となります。したがって、これはよく使われる手段です。サイバー攻撃をうっかり引き入れてしまう人的ミスには、以下のような種類があります。

- **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、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。
- **パスワードの誤用：**これには、強力なパスワードを設定していない、パスワードを適切に保管していない、またはパスワードを更新していないなどのケースが含まれます。
- **重要なコンポーネントの管理ミス：**システムへのアクセス許可につながる要素を紛失または置き忘れる場合です。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。
- **不十分なシステム管理：**システムの更新を行っていない、またはセキュリティパッチをインストールしていないというケースです。
- **改善の失敗：**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の要因は、サイバー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です。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、VMSを導入して、ビデオや重要なシステムへのアクセス権を信頼性の高い少数の個人に制限する必要があります。

詳しく読む >

システムの意図的な誤用

2

非常に一般的な別のサイバー脅威の要因として、ビデオシステムへの正当なアクセス権を持つスタッフがビデオ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への不正アクセスと操作
- 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

脆弱性に対処し、システムの意図的な誤用の脅威を軽減するには、ポリシーと長期的なプロセスを実装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と同時に、権限を付与する個人を適切に審査することが重要です。デバイスには管理用と日常操作クライアント（VMS）用に別々のアカウントを設け、メンテナンスとトラブルシューティングには一時的なアカウントを使用する必要があります。これら3つすべてを同じアカウントにすると、パスワードが容易に組織内に知れ渡るようになるため、故意的または偶発的な誤用の機会が発生しやすくなります。

詳しく読む >

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、ITシステムを物理的に保護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。
- 物理的に露出した装置は、盗難に遭う可能性があります。
- 物理的に露出したケーブルは、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

カメラ自体が改ざんされやすいだけでなく、ネットワークケーブルも脅威に曝される可能性があります。これにより、ネットワークが侵害される可能性が発生します。悪用の脅威をもたらす要因となる他の一般的な脆弱な機器として、鍵のかかっていない場所に配置されたサーバーやスイッチ、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カメラ、壁や導管に収められていないケーブルなどが挙げられます。

悪影響に注意

ビデオシステムは金融取引を処理したり顧客データを保管したりするものではありません。こうした情報が入っていないビデオシステムを攻撃しても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。対策費用を値切ると、長期的にはるかに多くのコストがかかる羽目に陥るかもしれません。

優れたサイバー衛生の維持

システムとデバイスのユーザーがシステムの健全性を維持し、オンラインセキュリティを向上させることを目的として、適切な慣行と手順を実行することで、優れたサイバー衛生（サイバーハイジーン）が実現します。多くの場合、サイバー衛生は内部プロセス全体の一環となっています。このようにして優れたサイバー衛生を実現することで、盗難や破損の可能性があるIDや他の情報の安全性を確保することができます。物理的な衛生管理と同様に、サイバー衛生管理を定期的に実施して、自然劣化や一般的な脅威を排除する必要があります。

優れたサイバー衛生のメリット

デバイスとソフトウェアに定期的なサイバー衛生手順を実行することで、メンテナンスとセキュリティという点でメリットがもたらされます。

- メンテナンスを実施することで、デバイスとソフトウェアを継続的に最高の効率で実行できるようになります。断片化されたファイルや旧式プログラムにより、脆弱性のリスクが高まります。メンテナンス手順を確立することで、こうした問題を早期に特定でき、深刻な問題の発生を防止することが可能となります。適切に保守されているシステムは、サイバーセキュリティリスクに対する脆弱性が低下します。
- ハッカーやなりすまし犯罪から、ウイルス、インテリジェントなマルウェアに至るまで、組織は常にリスクに曝されています。脅威を予測し、適切なサイバー衛生慣行を維持することで、早期発見を促進し、リスクへの準備態勢を整え、そしてリスクが現実になるのを防止することができます。

物理的な衛生管理と同様に、サイバー衛生管理は定期的に実施する必要がある

詳しく読む >

強力で一意のパスワードを使用

当たり前のように聞こえるかもしれませんが、サイバー犯罪者がシステムへ不正アクセスするために利用する最も一般的な方法は、弱いパスワードを使用する手段です。ほとんどのIPベースのデバイスは、デフォルトのパスワードと設定で出荷されます。そのため、IT部門や会社のポリシーに従って、これらをすぐに変更することが重要となります。組織は、適切なパスワード管理を実施する必要があります。強力で一意のパスワード（8文字以上）を使用し、パスワードは定期的に変更し、そして拠点間でパスワードを共有しないでください。パスワードポリシーの行使をコンピューターシステムに任せることはできません。組織はパスワードに関する組織のベストプラクティスのトレーニングを従業員に提供し、各自がこれを理解していることを確認する必要があります。証明書を使用して、パスワードとユーザー名を暗号化することも勧められます。

単一の一般的な単語や名称を当てたパスワードは、その長さに関係なく、数秒で解読される可能性がある

IT部門の方針やセキュリティネットワークポリシーに従ってデバイスを展開＆インストール

デバイスを展開する際は、使用しないサービスを有効のままにしないでください。こうすることで、サイバー犯罪者は容易に攻撃して、悪意のあるアプリケーションをインストールできるようになります。使用しないサービスを無効化し、信頼できるアプリケーションのみをインストールすることで、システムの脆弱性が攻撃者に悪用される確率が低下します。また、物理的にデバイスを適切に設置し、ネットワークポートとSDカードポートに一般の人がアクセスできないようにすることも重要です。

詳しく読む >

明確な役割と所有権の定義

担当領域に適切なアクセス権が適切な従業員に確実に提供されるように、明確なルールと手順を確立する必要があります。組織は「最小権限のユーザーアカウント」の原則に従う必要があります。つまり、従業員が業務を遂行する上で必要なリソース以外にはアクセスできないようにすることです。デフォルトのアカウントは絶対に使用しないでください。メンテナンス目的で一時アカウントを使用する場合は、タスク完了時にそのアカウントを必ず削除してください。

デバイスのデフォルト設定、特にデフォルトのパスワードは使用しないでください。一般的なデバイスのデフォルトの管理者アカウントIDやパスワードは、単純なGoogle検索で簡単に見つけることができるため、ハッカーが容易に侵入することが可能となります。デフォルト設定はデモ目的でのみ使用します。必ずデバイス保護サービスを有効化および構成してください。

61%
自分自身のデバイスで個人的なタスクと業務の両方を行う労働者の割合

80%
未承認のSaaS（Software-as-a-Service）アプリケーションを仕事で使用していることを認めた従業員の割合

75%
ネットワーク侵入件数全体の中で、脆弱な認証情報や認証情報の盗難によりネットワークが悪用された事例の割合

詳しく読む >

適切な最新ファームウェアの使用

デバイスを常に最新のファームウェアで更新していますか？システムやデバイスにバグや欠陥があると、攻撃に対する組織の脆弱性が高まり、サーバーの秘密鍵やユーザーパスワードがハッカーに盗まれる可能性があります。ソフトウェア/ファームウェアの更新管理計画を良好に文書化して、ネットワークデバイスに最新のファームウェアとセキュリティ更新が適用されていることを常に確認することが重要となります。

リスク分析の実施

組織は資産保護にどれほど支出する必要があるのでしょうか？潜在的な内外部の脅威および主要資産の損害または喪失が発生した場合の影響を分析することで、保護対策の取り組みに優先順位を付けることができます。米国国立標準技術研究所のサイバーセキュリティフレームワークといったリスク管理フレームワークが存在しています。リスク管理のプロセスとガイドラインを確立する上で、こうしたフレームワークが有用となります。

2019年、報告された侵害件数が2018年の3倍超となる

85億件以上

に激増*

* システム保護と潜在的な脅威に関する「IBM X-Force脅威インテリジェンス・インデックス2020」のデータに基づいています。

詳しく読む >

サプライチェーンの安全性の度合い

サプライチェーン全体と緊密に連携を図ることで、ネットワークおよび接続されたデバイスに発生し得る脅威をより良く把握することができます。今日、多くのITメーカーは、ネットワークにつながっているデバイスを強化するためのベストプラクティスに関する文書やガイド、また安全なサプライチェーンに関する資料を提供しています。こうした資料を入手できない場合は、メーカーに直接相談するか、他のユーザーが公開している文書を参考にすることが重要となります。個々のデバイスかシステム全体かに関わらず、デバイスはITポリシーに準拠して使用する必要があります。

常に暗号化された接続を使用

業界に関係なく、すべてのデータは暗号化により保護する必要があります。ローカルネットワークや「社内」ネットワークも含め、すべてのネットワークで暗号化された接続を使用する必要があります。ハッカーは、悪意のあるコードにより、暗号化されていない送信を「リッスン」します。そのため、認証プロトコルにより、情報がネットワーク経由で送信される前に暗号化されることを確認することで、攻撃の可能性を効果的に削減することができます。

安全性に関するプロトコル

- HTTPダイジェスト（アクセス）認証は、有用な方法の1つです。これにより、ユーザー名やパスワードといった認証情報とユーザーのIDがウェブサーバーで確認されます。
- HTTPS（HyperText Transfer Protocol Secure）は、最も一般的なデータ暗号化プロトコルです。HTTPSとHTTPは両方ともプロトコルの1つですが、HTTPSでは転送されるデータがSSL（Secure Sockets Layer）またはTLS（Transport Layer Security）を使用してさらに暗号化される点で異なります。
- SRTP（Secure Real-Time Transport Protocol）により、ビデオストリームが暗号化されるため、ビデオ自体の保護が強化されます。ビデオのローカルストレージとしてVMSやSDカードを使用する場合は、これらも暗号化されていることを確認してください。

詳しく読む >

システム全体の健全性を維持する上で、システムに適切なメンテナンスを実施することが重要となる

ネットワーク境界の保護

ファイアウォールとフィルターを理解していますか？ネットワークをバックボーンから保護することで、サイバーセキュリティのベストプラクティスを実装する他の対策をより適切にサポートすることができます。物理セキュリティデバイスでVLAN（バーチャル・ローカル・エリア・ネットワーク）などのネットワークセグメンテーションを使用することで、スヌーピングによる機密情報の漏洩および個々のサーバーやネットワークデバイスへの攻撃リスクを削減することができます。また、ACL（アクセスコントロールリスト）により、ネットワーク上の悪意ある動きを制御することが可能です。新しいデバイスに投資する前に、ソリューションがネットワーク全体で機能することを確認するため、ベンダーにネットワークポートのリストの提供を依頼してください。

システムとプロセスのメンテナンス

システム全体の健全性を維持する上で、システムに適切なメンテナンスを実施することが重要となります。デバイスやシステムログを定期的に監視して、不正アクセスの試みを検出する必要があります。高速なペースでテクノロジーが進化する今日の世界では、更新、新機能、ベストプラクティスが常に生成されています。そのため、全員がプロセスを理解できるように、メンテナンス手順を文書化する必要があります。

AXIS Device Managerなどのデバイス管理ソフトウェアを利用することで、組織はネットワークに接続されているすべてのデバイスとソフトウェア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。ネットワーク全体をスキャンし、モデル番号、IPアドレスとMACアドレス、ファームウェアバージョン、証明書のステータスなど、すべての重要情報を取得してください。

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

よく言われるように、ネットワークはそれに接続されているデバイスが安全でなければ安全ではありません。ネットワークを保護するために、組織は積極的に階層化された保護対策の実装に取り組んでいますが、物理資産のライフサイクルを効果的に管理する対策も講じる必要があります。しかし、多くの場合、新しいファームウェアがリリースされても、組織はソフトウェアの更新を怠ります。これは通常、ネットワーク上のすべてのテクノロジーのオーバービューを完全に把握していないためです。

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2つのタイプがある

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。より効率的な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。ネットワークと重要なデータを注意深く監視し、脅威対策や脆弱性の保護が完全に確立されていることを確認できるように、組織はネットワークに展開されているすべてのテクノロジーのオーバービューを明確に把握する必要があります。

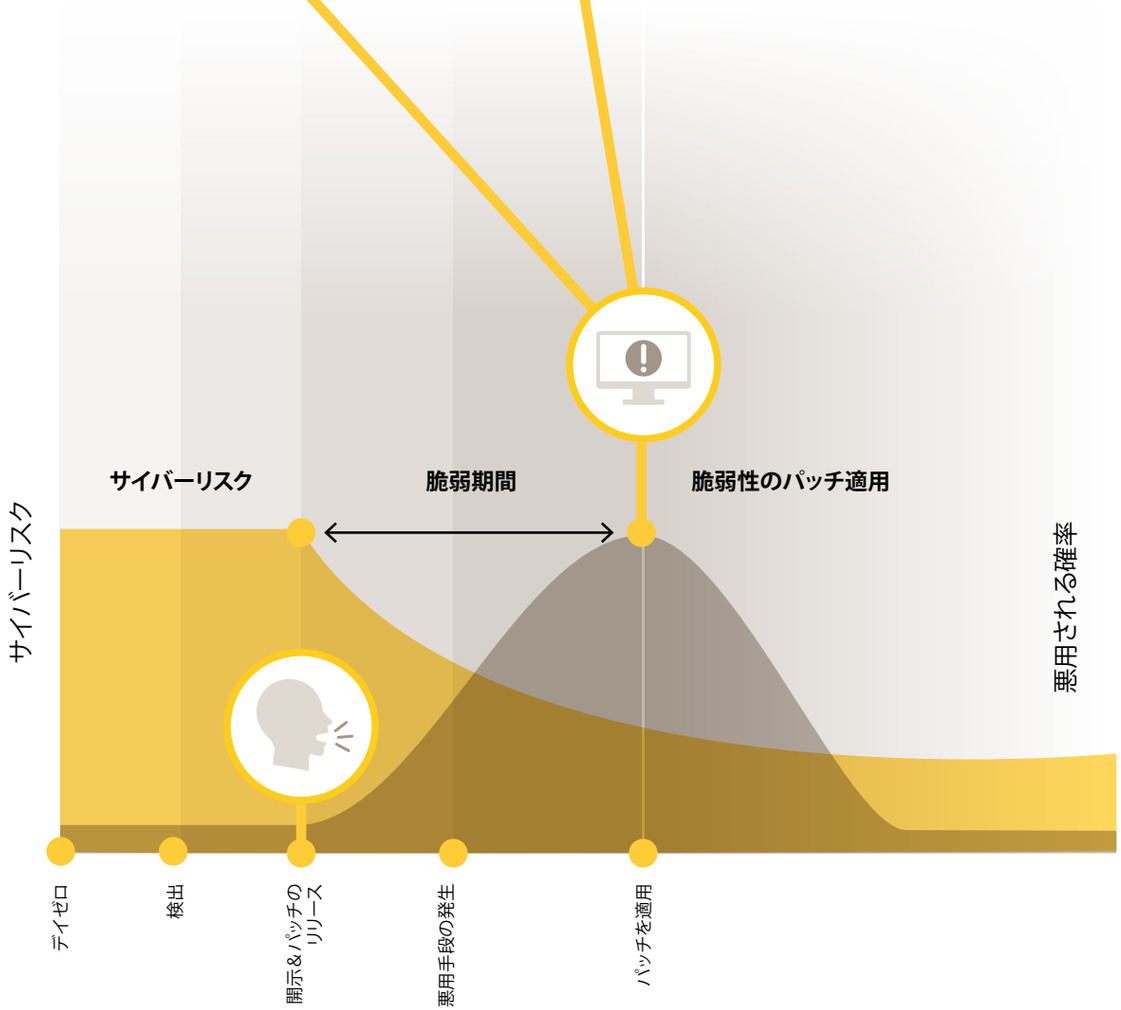
英国個人情報保護監督機関（ICO）のコメント

「侵害の脆弱性の60%は、パッチがリリースされているのに、ユーザーがそれを適用していないことが要因で発生しています」

詳しく読む >

「希望」は「無計画」と同義語

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、特定時点ですべてのテクノロジーデバイスを更新してパッチを適用する必要があります。



サイバーセキュリティ対策を改善する上で、更新とパッチは最善策となりますが、旧式のテクノロジーには適用できない場合があります。メーカーがサポートを停止したケースなどがこれに当てはまります。また、サイバーセキュリティの観点からは、パッチが適用されていない旧式のテクノロジーはリスクの最大要因となります。組織が脅威の発生を常に把握し、常に最新のサイバーセキュリティのベストプラクティスに従うことが非常に重要となるのです。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。

脅威に遅れを取らない対策

効果的なライフサイクル管理により、組織はビジネスを安全に維持できるだけでなく、将来に向けてより優れた準備態勢を整えることが可能となります。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、悲惨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。

物理デバイスも更新する必要あり

脆弱性への対処やバグ修正、また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、メーカーはファームウェア更新やセキュリティパッチを定期的にリリースしています。組織はオペレーティングシステムとアプリケーションにパッチを適用することの重要性は理解していますが、ハードウェアを制御するファームウェアの更新を怠ることがよくあります。これにより、こうしたデバイスにおけるサイバー攻撃の脆弱性が高まり、貴重な顧客データを損失する、またはコンプライアンス違反のせいで規制当局に多額の罰金を支払う羽目に陥るなど、さまざまな悪影響がもたらされる可能性があります。

詳しく読む >

ライフサイクル管理の合理化

構造化されたライフサイクル管理プログラムを確立することで、組織は将来に向けて適切な計画を策定することができます。最も適切かつ高度なテクノロジーを使用することで、セキュリティの脅威と脆弱性が最小限に抑えられます。AXIS Device Managerといったデバイス管理ソフトウェアにより、組織はこのタスクを自動化して、資産を効果的に管理できるようになります。

時間と労力の節約

サイバーセキュリティリスクの管理に関しては、デバイス管理ソフトウェアを活用することで、組織はかなりの時間を節約し、ストレスも緩和することができます。システムのメンテナンスにこのタイプのソフトウェアを利用することで、以下のような事柄が可能となります。

- システムの変更、ファームウェアの更新、新しい証明書をすべての適切なデバイスに同時に適用することができます。
- セキュリティ設定を容易に行い、または再構成して、ネットワーク全体に適用することができます。これにより、すべてのデバイスが最新のセキュリティポリシーと慣行に準拠していることを確認することが可能となります。
- 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ことができます。
- ネットワーク全体のユーザー特権レベルを管理し、変更を構成することが可能です。

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、ファームウェアバージョン、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。

完全なオーバービュー

ネットワークエコシステム全体の非常に詳細なオーバービューを把握することで、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。

詳しく読む >

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、どのデバイスに最新のパッチ、ファームウェア更新、証明書が適用されているかを確認することが可能です。また、メーカーがサポートを停止したデバイスに削除のフラグが付けられているかどうかをチェックすることも可能です。マルウェアがデバイスに感染する可能性があるかどうかを判断する上で、この情報は非常に貴重となります。ネットワークが危険に曝される前に、その他多くの脆弱性の問題を解決するために必要なすべての情報を得ることができます。

先を見越したエコシステムセキュリティ対策

デバイス管理プロセスを自動化することで、脅威や脆弱性からネットワークを保護することができます。しかし、組織は関係者全員が有意義なサイバーセキュリティポリシーとベストプラクティスに準拠していることを確認する必要もあります。たとえば、以下のような質問を自問自答してみてください。組織にパスワード強度に関するポリシーが制定されていますか？どのくらいの頻度でユーザーはパスワードを変更する必要がありますか？潜在的な攻撃面を削減するために、使用していないサービスをオフにすることがベストプラクティスとして定着していますか？デバイスの脆弱性はどのくらいの頻度でチェックされていますか？メーカーが既知の攻撃や脆弱性を公表した際に自社のリスクレベルを判断する手順は整っていますか？上記は、先を見越したネットワークエコシステム対策を特定して実装できるようにする上で自問自答するべき質問の例です。

ゼロトラストネットワークとは？

ネットワークの脆弱性はますます高まっています。高度なサイバー攻撃が増えているだけでなく、攻撃の基点となるネットワークエンドポイントに関係する接続デバイスが指数関数的に増加していることで、ネットワークがますます脅威に曝されるようになりました。この結果として、「ゼロトラスト」の概念が出現し、これに伴いゼロトラストネットワークとゼロトラストアーキテクチャーが登場しました。Axisを含め、ハードウェアメーカーにとってはゼロトラストの未来に備えることが不可欠となっています。この未来は、考えられているよりも早く現実のものとなるでしょう。

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。それらがどこに存在するか、どのように接続されているかは関係ありません。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。

アクセスを必要最小限に制限

ネットワークに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しか付与しません。

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。

詳しく読む >

ファイアウォールでは不十分な3つの理由

従来は、組織は企業のファイアウォールを可能な限り堅牢にすればそれで安心できましたが、多くの理由から、このアプローチに対する懸念が高まっています。

1 損失を受ける可能性が高い

ファイアウォールによりネットワークアクセスのセキュリティが確保されているように見えますが、ファイアウォールさえ破ってしまえば、侵入者はネットワーク内をかなり自由に移動することが可能となります。

2 もはやファイアウォールだけでは十分ではない

ネットワークに接続されているデバイスの数が非常に多い場合は、単一のソリューションでネットワーク境界を保護することはもはや不可能です。

3 より「透過的」なネットワークによりメリットがもたらされる

ネットワークを超えたクラウドベースのサービスが登場したこと、およびシステムを顧客とサプライヤーにシームレスに接続することでメリットがもたらされるということから、ネットワークセキュリティの性質が変化しました。

> **“一旦悪質な要素がネットワーク内に入ると、データの損失により取り返しのつかない損害が発生し得るという実際のリスクがあるだけでなく、検出されるまで数週間から数ヵ月間も悪質な要素がその中で活動を続けることが可能となります（これが存在する場合）。**
>
> ウェイン・ドリス（Wayne Dorris）氏、アクシスコミュニケーションズ、地域担当アーキテクト＆エンジニアリング・マネージャー

詳しく読む >

ゼロトラストの仕組み

ゼロトラストでは、きめ細かいネットワーク境界セキュリティやネットワークのマイクロセグメンテーションなどの手法が活用されます。前者はユーザーとデバイスに基づいています。物理的な場所やその他の識別データを使用して、そのネットワークアクセスの認証情報が信用できるかどうかを判断します。後者の場合は、より重要なデータが存在するネットワークの特定部分にさまざまなレベルのセキュリティ機能を適用します。

セキュリティの追加レイヤー

個人にその業務を遂行する上で必要となる一部のネットワークとデータにしかアクセス権を付与しないという方法を取ることで、明らかなセキュリティ上のメリットが得られます。また、異常な動作がこうしたIDに関連付けられた際にフラグを立てることで、セキュリティのレベルを向上させることができます。たとえば、ネットワーク管理者は、R & Dや財務サーバーのメンテナンスのために広範なネットワークアクセス権を持っている場合があります。

セキュリティの危険信号

たとえば、深夜に特定の重要ファイルやデータをダウンロードして、ネットワーク外部に送信するために同じネットワーク管理者の認証情報が使用された場合は、これはセキュリティの危険信号になります。ゼロトラストネットワークを構築するには、追加の認証が必要なように設定するか、または異常な活動にはリアルタイムでフラグが付けられ、調査のためにセキュリティオペレーションセンターに通知されるような構造を設ける必要があります。

異常な動作が発生するということは、セキュリティ認証情報の盗難、不満を持った従業員による仕業、または何かを窃盗しようと探している企業スパイがその要因である可能性があります。

詳しく読む >

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とそのコンテキスト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

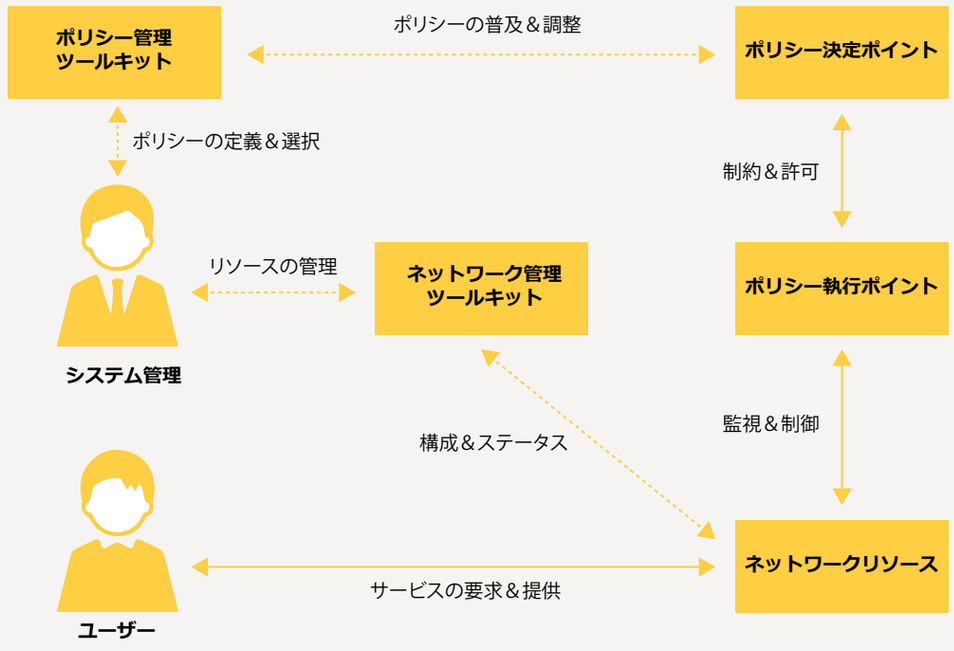
ポリシーエンジンが正常に機能するようにするには、次世代ファイアウォール（NGFW）、電子メールとクラウドのセキュリティゲートウェイ、データ損失防止（DLP）ソフトウェアなど、組織は主要なセキュリティ制御機能のルールとポリシーを慎重に定義する必要があります。こうした制御機能を組み合わせることで、ホスティングモデルや場所を超えたネットワークのマイクロセグメンテーションを実現することができます。

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。

- ルールを作成する
- ルールを監視する
- ルールを執行する

ポリシーエンジンの概要



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。

詳しく読む >

ゼロトラストネットワーク＆映像監視

ネットワークに接続するエンティティにはもちろん人も含まれますが、今日最も多いのは、デバイスからのネットワーク接続です。これには、ネットワーク監視カメラや関連付けられたネットワーク接続デバイスが含まれます。組織がゼロトラストネットワークアーキテクチャーに移行するのに伴い、「決して信用せず、常に検証する」という原則に従ってネットワークデバイスを利用することが不可欠となってきました。

皮肉な顛末

組織の物理的な安全性を維持するように設計された監視カメラがサイバーセキュリティの脆弱性につながるとしたら、これは皮肉なことではないでしょうか？繰り返しになりますが、従来型の形式のデバイスセキュリティではもはや十分ではありません。悪質な要素により従業員のアクセス認証情報が盗まれるのと同じように、デバイスのセキュリティ証明書が危険に曝される可能性があります。ゼロトラストネットワークを構築するには、デバイスでネットワークの信頼性が証明できるような新しいアプローチが必要となります。

やや意外な解決策

接続されたハードウェアデバイスで不変の信頼の基点（Root of Trust）を構築できるテクノロジーの1つとして、ブロックチェーン技術が挙げられます。ブロックチェーンという名称を聞くと、多少悪いイメージのある暗号通貨に関連付ける方が多いかもしれません。しかし、ブロックチェーン自体は、2つの当事者間の取引を効率的かつ検証可能で恒久的な方法で記録することができるオープンな分散型台帳です。組織は、プライベートブロックチェーンを採用してハードウェアの信頼の起点を築き、デバイス内に不変のトラストキーを確立することができます。

予測：使用されるIoTデバイスの数

2025年までに
750億
台に増加

ブロックチェーン技術が優れている理由

ブロックチェーンの構造により、鎖（チェーン）に生成されたデータ取引は、すべて暗号的にリンクされている先行の全取引のコンセンサスノードの演算をすべてやり直さない限り変更することはできません。そのため、ハードウェアデバイスの識別可能な部分のトラストキーがブロックチェーンに組み込まれていれば、デバイス自体の不変の認証情報が確立するのです。

サイバースペースで始まっている熾烈なAI競争

テクノロジーの進歩に伴い、悪意のある攻撃者もこれを利用して犯罪を成功させる可能性を検討していることは間違いありません。新しいテクノロジーにより、ランサムウェア攻撃や金融情報の盗難を計画しているサイバー犯罪者、または敵対国の重要なインフラストラクチャーの破壊やそれ以上の危害を加えることを狙う国家ぐるみの犯罪組織もその武器を強化することができるのです。

こうした犯罪組織は、他の合法的な事業と同様に十分な資金を備えています。犯罪組織は、人工知能（AI）、機械学習（ML）、深層学習（DL）といった新しいテクノロジーにより革新を図っています。しかも、犯罪者は国内や国際的な法規制、道徳、倫理的規範に縛られることがありません。

テクノロジーを利用して、犯罪目的を達成できる機会を検討するだけです。

AIなどの新テクノロジーは、常に犯罪者により悪用されます。**幸いなことに、標的となり得る組織もこれを防御対策として利用できるのです。**

詳しく読む >

目に見えない攻撃者

攻撃を高度化するために人工知能を使用するネットワーク侵入者がますます増えています。DDoS（大規模な分散型サービス拒否）攻撃により、人気のウェブサイトやオンラインサービスが無効化されたというニュースが一面に登場することがよくあります。なぜこのような事態が発生するのでしょうか？

ほとんどのサイバー犯罪者の主要目的は、可能な限り長時間、検出されないままで密かに悪事を働くことができる状況を作ることです。本質的に、家に入るコソ泥のようなものです。部屋から部屋へと移動し、カメラやアラームを注意深く回避しながら、貴重品を探して、侵入したときと同じようにこっそりと立ち去ります。同様に、サイバー犯罪者も検知されることなくネットワークに侵入し、動き回った後、ネットワークから密かに抜け出すことを企んでいます。

1

これを行う1つの方法として、人間かデバイスかに関わらず、ネットワーク内の正当ユーザーのように振る舞うという手段が挙げられます。この場合、AIと機械学習が新しい貴重な武器として活躍します。これにより、サイバー犯罪者は人やデバイスのネットワーク動作を学習し、新しいマルウェアやフィッシング戦略を迅速に開発し、そしてこれを大規模に展開できるのです。

2

しかし、ネットワークに不正アクセスする最も簡単な方法は、正当ユーザーを騙してリンクをクリックさせ、侵入口を作る方法です。また、口調や文調を本物とほとんど区別できないほどに似せて作成した偽の電子メールを、あたかも上司から送信されているように見せかけて送るという方法は最も効果的な手段の1つです。

AIとは、コンピューターに操作の結果を保存および分析させる一連のアルゴリズムです。その後、コンピューターは同様の要求が発生した際に、それに応じてその操作を調整できるようになります。数百から数千に上る要求を学習させることで、コンピューターの応答と動作が徐々に最適化されます。

詳しく読む >

すべての道はローマに通ず

サイバー犯罪者は、攻撃のライフサイクルを通じて多数のAIツールを使用します。これには、偽のソーシャルメディアプロファイルを介して従業員に働きかける「チャットボット」から、ニューラルネットワークを使用することで最も価値の高いデータを特定して抽出する方法に至るまで、さまざまな手段が含まれます。

ネットワークに侵入した後に、横方向への移動により侵入先を広げるラテラルムーブメントはこうした手法の1つです。遠隔地に設置され、セキュリティで保護されていないデバイスなどのネットワークのエントリポイントが、侵入者の最終目的地であることはめったにありません。

侵入者は移動の途中でユーザーの認証情報、特にネットワークアクセスの主キーを獲得できるネットワーク管理者といった特権ユーザーの認証情報を収集しながら、ネットワーク内の機密性の高い領域を目指して進行します。

詳しく読む >

ITとOTの間の危険なリンク

さまざまな「モノ」がインターネットに接続される「モノのインターネット（IoT）」が世界中に拡大していますが、これにより情報技術（IT）ネットワークがオペレーショナルテクノロジー（OT）環境とより緊密に統合されることから、リスクが急速に増大します。

簡単に述べれば、デジタル情報の流れを管理するのがITネットワークです。対照的に、ビジネスや特定の場所の物理的なプロセス、機械、物理的な資産の運用を管理するのがOTとなります。窃盗目的ではなく、破壊や崩壊を目的とする攻撃者にとっては、OTにアクセスすることが不可欠となります。発電所や石油精製所、または病院内の機械に攻撃者がアクセスした場合に発生し得る損害や被害の規模は想像に難くありません。

詳しく読む >

探偵を活用

サイバー犯罪者がAIを使用したらと考えるだけで、身も凍るような思いがします。しかし、ネットワークを侵入から保護することを目的とするユーザーも、その同じテクノロジーを活用することができるのです。しかも、多くの点で、攻撃者よりも防御する側のほうが有利です。

多くの点で、攻撃者よりも防御する側のほうが有利です。

DARKTRACE

ダークトレース（Darktrace）社は、サイバーセキュリティでAIに焦点を当てた世界有数の企業として認識されています。ご想像の通り、同社は犯罪組織によるAI使用が増加している現状に関する豊富な専門知識も備えています。同社は、犯罪者よりも高い優位性を維持するためにAIと機械学習を継続的に革新しています。

詳しく読む >

攻撃に利用されるAIは防御ツールとしても利用可能

ダークトレース社、ジェフ・コーネリアス氏のインタビュー

ダークトレース社のエグゼクティブ・バイス・プレジデントを務めるジェフ・コーネリアス（Jeff　Cornelius）氏に、サイバー犯罪者よりも高い優位性を維持するために同社がどのようにAIと機械学習を活用しているかについてお話を伺いました。数ページにわたり、同氏のインタビューをご紹介します。

Q　事態はどれほど悪化していますか？

「第一に、皆さんが報道からどのような印象を抱いているか分かりませんが、AIと機械学習は簡単に開発できるものではありません。サイバー攻撃を企む犯罪組織や国家という強力な敵が存在してはいるものの、多くの側面でこちら側が有利です」

「主な優位性として、顧客からアクセス権が提供されれば、当社はネットワーク活動全体を確認できるということが挙げられます。これにより、すべてのデバイスとユーザーの動作を理解します。対照的に、犯罪者は限られた活動しか見ることができず、それに頼る以外に手はありません。犯罪者は侵入した環境をほぼ探り足で進まなければなりませんが、当社側はその環境全体を理解しているという強みがあります」

「最終的に、犯罪者の活動の中には、普通の企業や組織ならまず行わない行動が含まれています。当社の主要目的は、ネットワーク内のこうした異常な動作を特定し、それに対処することです。敵が出現する時期や場所、また敵が利用する新しい手法やその目標が分からないため、当社は広範な視野を備えておく必要があります」

詳しく読む >

模倣に関する興味深い洞察

ダークトレース社、ジェフ・コーネリアス氏のインタビュー

Q

詳しくご説明いただけますか？

「たとえば、家の外から某人物の日常的な行動を日々観察していれば、その人物が毎日出勤する時間、通勤路、昼食を取る場所など、その人物の習慣をかなり詳細に把握することができます。観察者はおそらくその人物の日常生活の一部を非常にうまく模倣できるようになるでしょう」

「しかし、奥まった部屋でその人物が取る行動は外からは見えません。したがって、たとえば朝食時にその人物を模倣しようとしても、間違いなく間違いを犯し、親しい家族にその異常に気付かれてしまいます。通常、インターネットにはかなり適切な情報が掲載されているため、これを基に個人を標的にした巧妙なスピアフィッシングメールを作成することはできますが、一旦侵入した後は、当社の土俵だということです」

詳しく読む >

教師あり機械学習

ダークトレース社、ジェフ・コーネリアス氏のインタビュー

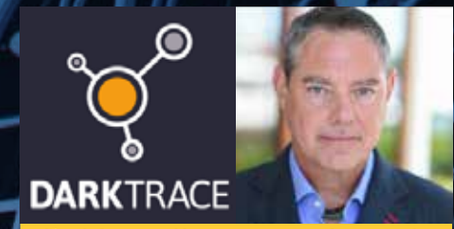
Q 機械学習についてお伺いできますか？

「機械学習の『教師あり学習』と『教師なし学習』には重要な違いがあります。教師あり学習の場合は、コンピューターに一連の既知のデータを与えて学習させます。常にこうしたデータが参照され、記録された結果が期待通りのものであるかどうかが確認されます」

「サイバーセキュリティの場合は、学習モデルが既知のマルウェアに基づいて構築されます。犯罪者とサイバーセキュリティ企業の勝負はここが決め手となります。犯罪者は機械学習を使用してマルウェアの新バージョンを作成しています。こうした事例は指数関数的に増加しています。サイバーセキュリティ企業は、教師あり機械学習を用いて新しい防御モデルを構築することで、犯罪者よりも優位に立つことに取り組んでいます。これは、新しい単語や言語が毎日出現している世界で、スペルチェックすることで遅れを取らないようにする努力と少し似ています。しかし、遅れを取らないように努力することは不可能ではないにしても、ますます困難になってきています」

詳しく読む >

…対教師なし機械学習



ダークトレース社、ジェフ・コーネリアス氏のインタビュー

Q

他に手段はありますか？

「あります。対照的に、教師なし機械学習アルゴリズムにより、過去の脅威の知識に依存するのでなく、データを個別に分類し、説得力のあるパターンを検出することができます。この場合は、大規模なネットワークデータが分析され、既知の証拠のみに基づいて何十億もの確率ベースの計算が行われます。そして、デバイスやユーザー、またはいずれかのエンティティのグループに関連する特定ネットワーク全体の『通常』の動作に対する理解が形成されます。次に、この進化する『パターン』からの逸脱の検出が可能となります。逸脱は、脅威発生の兆候であり得ます。この早期警告システムにより、サイバー犯罪者や悪意のある人物の先手を打つことができるのです」

サイバーセキュリティ脅威の削減に向けた協力体制

たった1人で、企業や組織、重要なインフラストラクチャー、そして都市を保護することはできません。特効薬や単一のソリューションというものは存在しません。許容可能なレベルのサイバーセキュリティを正常に維持するには、エンドユーザーを含め、多くの利害関係者が献身的に共同作業を行う必要があります。

サイバーセキュリティ文化の構築

一丸となって協力することが鍵となります。組織内のすべての個人をサイバーセキュリティチームの一員と見なす必要があるのです。以下の事柄を考慮してください。

- 従業員のサイバーセキュリティトレーニングに投資する。
- 入社時に従業員を教育する。
- 上級幹部にサイバーセキュリティポリシーを執行することを奨励する。
- 継続的に情報を提供し、サイバー脅威の発生時にはその詳細を伝達する。
- 新しいネットワーク機器を選択する際は、要件としてサイバーセキュリティを考慮に入れる。
- BYOD（個人所有デバイスの持ち込み）ポリシーを制定する。
- サイバーセキュリティインシデント対応戦略を構築して適用する。

組織全体をサイバーセキュリティ計画に関与させることで、組織のネットワークとデバイスのセキュリティをより良く確保できる環境を構築することができます。

詳しく読む >

責任の共有

サイバーセキュリティは製品、人、技術に関するもので、これは継続的なプロセスです。そして、協力しあい、サイバーセキュリティチェーンの全てのリンクを可能な限り強固なものにする必要があることは明らかです。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。

インテグレーター＆設置担当者

設置されているすべての機器に最新の更新が適用され、高度なウイルススキャナーが実行されていることを確認する必要があります。また、他の関係者と共同で、パスワード、リモートアクセスの管理、ソフトウェアと接続デバイスの長期的なメンテナンスに関する堅牢な戦略を確実に実施することに取り組む必要があります。

ディストリビューター

扱う製品に直接触れ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してい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

システムの指定を支援し、適切なライフタイムメンテナンスも補助する必要があります。潜在的な関連コストについては、高い透明性をもって説明してください。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、この課題も話し合う必要があります。

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。メーカーは、欠陥のリスクを最小限に抑えるために、設計、開発、テスト段階で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。組み込みのセキュリティ機能、自社開発のチップ、自社のサプライチェーンを慎重に管理することも重要です。手頃で自動化されたデバイス管理ツールを提供し、既知の脆弱性についてチャンネルやパートナーに通知することも重要となります。

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、これを一般公開することがよくあります。

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。

詳しく読む >

セキュリティパートナー

全員が協力してこそ、絶えず進化するサイバーセキュリティ脅威に対処する準備を整え、脅威が顕在化した場合もこれに迅速に対応できる環境を構築することができるのです。デバイス製造からシステムの設計とインストール、そしてメンテナンスとデバイス管理に至るまで、実装したサイバーセキュリティソリューションのあらゆる側面が正しく機能するようにするためには、関係者すべてが各自の役割の責任を果たす必要があります。このように警戒を怠らないことが大切です。

エッジに移行することで高まるサイバーセキュリティ脅威

エッジに向かう世界

2021年、エンドユーザーに近い「エッジ」コンピューティングに向けた勢いが増しています。数十億ものIoTデバイスがすでにネットワークに接続されており、この数が**急速に増加**しているという現状は周知の事実です。しかし、こうしたデバイスの性質と要件により、サイバーセキュリティに深刻な影響が及ぼされます。

IoT

IoT（モノのインターネット）とは、さまざまなデバイスがインターネットに接続され、相互に「通信」できるネットワークの仕組みを指しています。これには、スマートフォンやウェアラブルデバイスといったテクノロジーガジェット、スマートメーターなどのスマートホームデバイス、スマートマシンなどの産業用デバイスが含まれます。IoTデバイスにより、センサーやプロセッサーを使用して環境から取得したデータが収集および分析され、それに応じてアクションが実行されます。

急増

2025年までに、接続された750億を超えるIoTデバイスが使用されることになると予測されています。この数値は、2019年のIoTインストールベースのほぼ3倍に当たります。

詳しく読む >

エッジに向かう世界

> カメラ内で実施されるデータ処理と分析が増加傾向にあります。

簡単に述べれば、ネットワークに接続されている「モノ」の多くは、現状を即座に感知し、取る措置を決定し、そして行動する能力を備えていることが要件となります。または、こうした能力によるメリットを受けています。

自動運転車は明らかな例

外部環境との通信に関連する機器（例：信号機）か、リスクを検知するセンサー（例：車の前に突然出現した物体の検知）かに関わらず、決定は瞬時に下される必要があります。データセンターでの処理・分析のためにデータがネットワーク経由で車両から送信されてから、実行する措置の決定が返信されるまでの遅延は許されるものではありません。

映像監視も同様

受動的ではなく積極的な対策に移行する場合、つまり事後対応ではなく、事態の防止を目的とする場合は、カメラ内で実施されるデータ処理と分析が増加します。しかし、エッジに配置するデバイスが増加し、安全性とセキュリティにおいてこうしたデバイスがより重要な役割を果たすようになると、必然的に多くの影響がもたらされます。これについては、次ページをご覧ください。

詳しく読む >

専用デバイスによる専有のパワー

エッジコンピューティングのレベルを向上させるためには、特定のアプリケーション向けに設計され、最適化された専用のハードウェアとソフトウェアが不可欠となります。接続するデバイスには、より高い演算能力が必要となります。また、こうしたデバイスは、サイバーセキュリティを念頭に置いて、シリコンから目的に合わせて設計および製造する必要があります。

ここで、専有の統合処理チップが重要となります。たとえば、Axisのデバイスは、社内設計の「システムオンチップ」を搭載しています。これにより「バックドア」を作成する不正かつ悪質な「ファームウェア」アップグレードといったサイバー攻撃からデバイスが保護されます。最新の「ARTPEC-7」プロセッサは、セキュリティを第一に考えて、現在だけでなく、将来的な映像監視のニーズに対応できるように特別に設計されています。

映像監視用に特別に設計された最新のAxis ARTPEC-7チップは、第1世代製品の50倍以上の性能を備えています。当社独自のチップを設計・製造することで、Axisは顧客ニーズを満たす最適な製品を製造でき、サイバーセキュリティ脅威といった外部要因の変化に対応することができます。

> **ARTPEC-7により、当社は非常に高い画質、高性能、優れた帯域幅の効率、エッジで分析を実行する機能を備えたネットワークカメラを提供することが可能となりました。**
>
> ステファン・ランドバーグ（Stefan Lundberg）氏、
> アクシスコミュニケーションズ、エキスパート・エンジニア

詳しく読む >

信頼できるエッジに向けて

「信頼性」にはさまざま種類があります。

- **組織が責任を持ってデータを収集および使用することに対する信頼**
- **デバイスとデータがサイバー犯罪者から安全に守られていることに対する信頼**
- **データが正確であり、テクノロジーが設計通りに機能することに対する信頼**

こうした信頼性を維持できるか、裏切ることになるかはエッジにかかっています。

サプライチェーン全体で信頼性を確立することが不可欠となります。ハードウェア自体にスパイチップを埋め込むことは比較的困難です。しかし、ファームウェアのアップグレードを通じて、デバイスにスパイ「バックドア」を作成することは、製造時点で不正チップを埋め込むよりも比較的簡単と言えます。

詳しく読む >

信頼できるエッジに向けて

個人のプライバシーに関する問題は、継続的に世界中で議論の種となっています。動的な匿名化機能やマスキングといったテクノロジーをエッジで使用してプライバシーを保護することはできるものの、プライバシーに対する姿勢や規制は地域や国によって異なります。監視部門の企業に国際的な法的枠組みを制定する必要性は継続的に話題に上がっています。

これまで以上にサイバーセキュリティが重要

デバイス内でデータの処理や分析が行われる機会が増加していることで、サイバーセキュリティがますます重要となってきました。高度なサイバー攻撃が増加している現状の中でも、最も基本的なファームウェアのアップグレードすら怠っている組織が多く存在します。安全なシステムの基本は、ハードウェア、ソフトウェア、ユーザーに関する明確なポリシーを通して、個々のデバイス管理と監視ソリューション全体の包括的なライフサイクル管理の両方を実施することです。

コンプライアンス違反の脅威

近年、ブリティッシュ・エアウェイズやマリオット・インターナショナルなどの組織が、規制違反により多額の罰金を科されました。罰則への恐怖から、ビジネスコミュニティには衝撃が走りましたが、これは組織がサイバーセキュリティ予算を改めて検討する有意義な機会ともなりました。

組織は、ランサムウェア、マルウェア、フィッシングなど、さまざまな標的型攻撃の脅威に曝されています。これにより、システムのシャットダウン、データの損失、運用の中断、評判の低下、顧客の損失、収益の低下が発生する可能性があります。

コンプライアンスとは？

コンプライアンスとは、政府の規制や国際規格への準拠を指していると思われがちです。しかし、これはそのほんの一部に過ぎません。組織は内部統制とベストプラクティスを実装し、これに準拠して運営するだけでなく、取引先のパートナーもこれらに準拠していることを確認する必要があります。

今日では、組織は顧客データが適切に保護されていることを確認する責任も負っています。

考慮すべき3つの領域：

1. **規制遵守**
   欧州のGDPR（EU一般データ保護規則）などの政府規制およびISOやNISTなどの国際規格とフレームワーク
2. **社内コンプライアンス**
   社内ポリシーとベストプラクティス
3. **社外コンプライアンス**
   サプライチェーン内のコンプライアンス

詳しく読む >

法律を遵守する義務

欧州のGDPR（EU一般データ保護規則）といったデータ保護法は、組織、企業、政府による消費者の個人情報の使用方法を管理することを目的としています。サイバーセキュリティに関して言えば、多くの場合、こうした法律は組織が実施しているセキュリティソリューションと密接に関連しています。

GDPRは欧州の法律ですが、ほとんどのグローバル組織は同法律に何らかの方法で対処する必要があります。たとえば、欧州連合にデータを保存している米国企業は、GDPRに準拠する必要があります。同様に、組織がデータを処理する第三者企業と契約を結んでいる場合は、その第三者企業もGDPRに準拠する必要があります。米国では、50州それぞれがデータ保護に関する個別の規制を制定しています。そのため、州をまたがる作業の管理が困難で時間がかかります。

内部ガバナンスへの高価な投資

ハッカーは規制や規格に準拠した組織はハッキングしません。ハッカーは企業を観察し、その特定の脆弱性および曝されているリスクを判断します。組織は予算すべてをサイバーセキュリティに費やすことができますが、　目標は十分な対策を講じることで、イノベーションを妨げることではありません。組織のリスク選好度に応じて、このバランスを取る必要があります。一部の組織は、法律で定められているよりも強力な管理体制を実施しています。これは、万が一サイバーセキュリティ違反が発生した場合に、組織はビジネスを保護するために適切な措置を講じていたことを証明する必要があるためです。

サプライチェーン内のコンプライアンス

サプライチェーンが複雑な組織には、他のコンプライアンス要件があります。たとえば、欧州に拠点を置く組織が米国政府と取引する場合、この欧州企業は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、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ます。場合によっては、第三者企業（サプライヤーなど）もコンプライアンス違反の責任を部分的に負わなければない可能性があります。つまり、一定割合の罰金が科されるということです。

社外の規則・規制に準拠することは重要ですが、組織の社内ポリシーは外部規則よりも厳格に制定することが勧められます。これは、結局のところ、コンプライアンスを徹底し、すべての侵害からデータを確実に保護する責任は組織にあるためです。

詳しく読む >

自社に適用される法規制を把握

コンプライアンスを常に最良の状態で管理するには、永続的な取り組みが必要です。組織に適用されるサイバーセキュリティやデータ管理の規制は、通常、所属する業界によって異なりますが、 複数の業界や国で共通する規制もいくつか存在します。

組織は、法制化され得る条項などを案内する最新のガイドラインや変更事項を絶えず確認する必要があります。現在発生している脅威や攻撃を調査し、制定されているコンプライアンス関連の法規制を理解することで、組織は加える必要のある変更を判断し、新しいコンプライアンスチェックに合格できる環境を確立することができます。

サイバーセキュリティ監査

自社に適用される法規制を特定できたら、全体的なコンプライアンスの状態を検査する必要があります。内部サイバーセキュリティ監査を実施することで、組織のITセキュリティガバナンスのプロセスを評価することができます。一般的には、サイバーセキュリティ監査は年次に実施すればよいと考えられていますが、 すべての統制を継続的に監視することで、統制上の不備や欠陥が生じた場合に適時に修正できる体制を整えることが勧められます。また、組織は継続的なセキュリティ管理の評価を定期的に文書化することが奨励されています。これは、将来的な監査にも使用することができます。

サイバーセキュリティ監査について考慮すべき事柄：

- **リスク管理：** 規制遵守に関連するリスクを特定および管理するために、貴社はどのようなプロセスを制定していますか？たとえば、リスクの伝達方法やリスク評価を確実に実施するためのプロセスなどです。
- **内部監査プロセス：** 組織は、コンプライアンスを継続的に監視するために、内部監査プロセスを確立する必要があります。たとえば、サイバーセキュリティ慣行に加えられた変更を特定、評価、管理するために、貴社はどのようなプロセスを実施していますか？
- **セキュリティとプライバシーのトレーニング：** 貴社は従業員に権限を付与し、ITセキュリティニーズに適合しない不備や欠陥を特定するために必要なトレーニングを提供していますか？たとえば、電子メールフィッシングの処理方法に関するトレーニングプログラムなどです。こうしたトレーニングプログラムは、組織が実施すべき事柄のほんの一部に過ぎません。内部統制により、トレーニングの効果を決定します。組織にとってリスクが高い部門や部署は、年次ではなく四半期ごとにチェックを実施することが勧められます。

詳しく読む >

コンプライアンスの監視

内部監査の結果を利用して、コンプライアンス監視計画を策定することができます。この計画に従って、組織の全体的なコンプライアンスの取り組みを継続的に評価し、監査中に特定されたすべてのリスクに対処します。組織に最大の脅威をもたらすリスクを優先する必要があります。組織が実施しているコンプライアンス管理体制を評価することで、サイバーセキュリティ管理において規制に適合しない不備や欠陥が発生した場合にそれを特定することができます。

サイバーセキュリティリスクの監視責任者を決定する際は、必要な専門知識に基づいて役割を割り当てる必要があります。必要なスキルセットを備えている従業員や組み合わせることができるリスク監視活動を検討することで、適切な割り当てを実施することができます。

最新の状態を維持

メーカーは通常、脆弱性に対処するために、定期的にファームウェアを更新します。また、新しい法律が制定された際にも、更新します。しかし、すべてのデバイスの概要とそのライフサイクルのステータスを明確に把握して、製品がサポートされなくなった際の準備を常に整えておくことも重要です。AXIS Device Managerといったデバイス管理ツールを利用することで、製品が最新状態に維持されていること、および法規制に準拠していることを確認することができます。こうしたツールからは、ライセンス登録の更新、メンテナンス時期、承認に関する通知が送信されるため、これにより、組織はコンプライアンス要件が満たされていること、常に最新の状態が維持されていることを確認することが可能となります。また、監査に書類が必要な場合も、こうしたツールを利用して、必要な文書を取得することができます。

コンプライアンスの実証

多くの場合、デバイスメーカーは顧客から、サイバーセキュリティのレベルに関するアンケート調査の依頼を受けます。組織は継続計画、認定の取得、ネットワークのデータの保護方法に関する質問に答える必要があります。すべての情報を提出する準備を整えておけば、組織はデューデリジェンスの実施に関する情報などを速やかに提出できるため、顧客の安心感を高めることが可能となります。

2008年以降、米国の銀行に科された罰金の合計額
2,430億ドル

コンプライアンス関連の運用コストの2008年からの増加率
60%

従業員1人あたりの規制リスクのコスト
1万ドル

> **“コンプライアンス違反の代償は高く付きます。コンプライアンスの維持にかかる費用に不満を感じている組織は、一度規制違反をしてみてください。**
>
> 米国のポール・マクナルティ（Paul McNulty）副司法長官
> https://youattest.com/

詳しく読む >

一に文書化、二に文書化

規制遵守を実証するには、文書化が不可欠となります。社内ポリシーには、以下のような内容を含めることができます。

- 記録する内容とその理由。
- 監視機能が稼働されていることを一般に知らせる標識の有無。
- 監視システムにより個人が特定される可能性。（これは個人のプライバシーに影響を与えるため、検討して文書化する必要があります） 映像にアクセスできる人物。
- データの保存方法と保存期間。物理的およびサイバーセキュリティの観点からのデータストレージの安全性。古い映像の削除方法とその確認方法。

特定の状況に関する文書も含める必要があります。たとえば、侵入が発生した場合、その際に取る措置、データを管理する者、制定されているプロセスなどです。また、内部監査で特定された不備や欠陥、またその問題を解消するために組織が講じている措置を、規制委員会に常に通知することが勧められます。

コンプライアンスは動く目標

法律や規制は絶えず改正・変更されているため、どれほど厳格なコンプライアンス監視計画を策定していても、罰金につながる規制違反が発生し得ることを認識する必要があります。組織は遵守状況を継続的に監視し、コンプライアンスを完全に実証できるような態勢を整えておく必要があります。

今こそ行動すべき時

コンプライアンスがサイバーセキュリティにおける重要な要素であることは間違いありません。しかも、コンプライアンスに対する懸念は浸透しています。組織と消費者は脅威を身近に感じており、迅速に行動しなければ、システムとデータが攻撃に対して脆弱になることに気付いているのです。組織は安心してイノベーションと成長を追求したいと考えてはいますが、サイバー犯罪によってもたらされるリスクを最小限に抑える必要性にも迫られています。一方、消費者はデータが安全に維持されることを望んでおり、取引先の組織が確実な対策を講じて、これを実現することを期待しています。ベンダー、メーカー、エンドユーザーそれぞれがサイバーセキュリティを有効に実装することに責任を持つ共同アプローチを取らなければ、政府の規制を満たすことはできません。こうすることで、最終的に、損害をもたらし得る違反リスクを最小限に抑えることができるのです。

コンプライアンスがサイバーセキュリティにおける重要な要素であることは間違いありません。しかも、コンプライアンスに対する懸念は浸透しています。

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、システムサプライヤーがこうしたリスクを継続的に評価し、対策を講じていることを確認する必要があります。サプライヤーだけでなく、そのサプライヤーの下請け業者についても同様です。

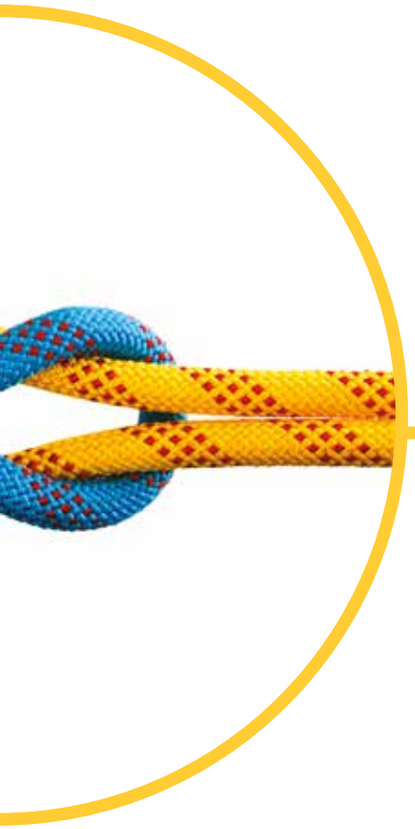
組織は、サプライヤーが講じているサイバーセキュリティ対策にのみ焦点を当てる傾向がありますが、 そのサプライヤーの下請け業者はどうでしょうか？サプライヤーがどのようにサプライチェーン全体を管理および維持し、コンポーネントレベルから完成品までのすべての工程が安全であることを確認しているかご存じですか？

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？

- 保護機能が組み込まれた安全な製品を設計および製造していますか？
- 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？
- 脆弱性が新たに発見された場合、迅速に対応し、無料アップグレードを提供していますか？
- 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？

「サプライヤーはサプライチェーン全体をどのように管理および維持していますか？」

詳しく読む >



適切なパートナーの選択

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。生産拠点を視察してから現場の監査を実施することで、設定されている承認ベンダー資格の要件と基準が満たされているかどうかを評価する必要があります。潜在的な新サプライチェーンパートナーの場合は、サプライヤーはその評価の一環として、組織の財政状況と所有構造を詳細に分析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。そのため、毎日のようにコラボレーションやコミュニケーションを緊密に図り、現場訪問も頻繁になります。

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？

詳しく読む >

サプライヤーの監査

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ことが挙げられます。

監査により、さまざまな重要側面をカバーする必要がある

- プロセスのコンプライアンス（文書）
- 施設のセキュリティ
- 工場内での物理的な取り扱い
- 在庫の取り扱い
- 製造設備
- 品質管理
- トレーサビリティ記録

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。

- 出入口は継続的に監視し、アクセスコントロールにより、訪問者の登録を記録して保存する必要があります。施設とその周辺に警備員を配置している場合でも、一部のエリアは継続的な監視が必要になる場合があります。
- スキャン装置を使用して、望ましくない物体や要素を検知する必要があります。
- 輸送は、認識されている有名な運送事業者に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。集荷時と配達時に、運転手とトラックが安全規制に準拠しているかどうかをチェックします。
- 航空貨物はすべて、X線検査を行う必要があります。また、密かに物が混入されないように、各貨物は出荷時点で封印する手順も一般的に導入されています。
- 多くの場合、入荷品と出庫品は、CCTVカメラを使用して監視および文書化します。

詳しく読む >

データ転送＆情報セキュリティ

サプライチェーンネットワークにおけるデータ転送は、暗号化方式と認証を利用して、セキュリティプロトコルで保護する必要があります。サブサプライヤーとパートナーは、高レベルの情報セキュリティを維持することで、サプライチェーンで不備や欠陥が発生するリスクを削減する必要があります。

サプライヤーは、企業の機密情報を特定・管理する体系的なアプローチを採用する必要があります。このアプローチのシステムには、人、プロセス、ITシステム、物理的な場所を含め、ISO 27001認証とGDPR（EU一般データ保護規則）に準拠する必要があります。これにより、関係者の意識が高まり、効果的なリスク管理が実現します。

人的セキュリティ

教育、能力、実務経験の観点からだけでなく、セキュリティの観点からも、採用する人員を見極めることが重要となります。たとえば、Axisの場合は、採用プロセスにおいては質とセキュリティに重点を置いており、採用プロセスとして、雇用を決定する前に本人確認、信用照会、身辺調査を実施しています。会社の知的財産やその他の機密情報を保護するために、新たに入社する従業員とコンサルタントには秘密保持契約（NDA）への署名を要求します。この契約内容は、雇用中だけでなく、退職後にも適用されます。

従業員のエンパワーメントとリスク削減

Axisは、従業員が情報セキュリティに対して高い意識を維持できる環境を整えています。従業員に権限を付与する際は、自身が実施する必要のある事柄および存在するリスクを十分に理解するために必要な情報を提供しています。Axisの従業員はそれぞれ、真のセキュリティと信頼性の構築に向けた責任を遂行しています。すべての従業員が情報セキュリティの認識に関する教育とトレーニングを受け、注意と警戒を怠らない姿勢で業務に臨んでいます。情報、システム、リソースへのアクセスは制限されており、特定タスクを実行するために必要な従業員のみが利用できる仕組みになっています。同様に、サプライヤーと製造パートナーの従業員も、情報、システム、リソースをAxisと共有しています。

詳しく読む >

製品の完全性

他すべての製品と同様に、監視製品も、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ファームウェア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。

Axisを選ぶ理由は?

よりスマートで安全な世界を実現するためのソリューション

品質は当社の中核：顧客の安心感を高めるため、すべての製品に広範なテストを実施しています。

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。たとえば、Axisのカメラとエンコーダの80%はPVCフリーです。

サイバーセキュリティの推進：当社は脅威と結果を継続的に監視し、迅速かつ断固とした対応を心掛けています。機器の設置後も、アップグレード、更新、インストールを通して、継続的にデバイスのサイバーセキュリティ強化を図っています。

地域的な専門知識を備えてグローバルに展開：ネットワークビデオ製品において世界最大の導入実績を誇るAxisは、50カ国以上に従業員が拠点を置いています。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：他社との提携に取り組むAxisは、市場で最も統合されているカメラのブランドに成長しました。

Axis Communicationsについて

Axisは、セキュリティの向上とビジネスの新しい推進方法に関する洞察を提供するネットワーク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。ネットワークビデオ業界をけん引するリーダーとして、Axisは映像監視、インテリジェントアプリケーション、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製品とサービスを提供しています。Axisは50ヶ国以上に3,800人を超える熱意にあふれた従業員を擁し、世界中の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、スウェーデン・ルンドに本社を構えています。

より詳しい情報は www.axis.com をご覧ください。