Cybersecurity reference guide

ユーザーマニュアル

Cybersecurity reference guide

目次

Cybersecurity reference guide

はじめに

はじめに

本ガイドの目的は、共通のベースラインを提供し、Axisが作成するサイバーセキュリティ関連資料の参考資料とすることです。これらは、NIST、SANS、ISO、RSA の各カンファレンスや、サイバーセキュリティコミュニティ内のさまざまな組織の資料に基づく簡略化された説明、モデル、構造です。

Axisの他の資料へのリンク:

- *axis.com/about-axis/cybersecurity*
- *help.axis.com/cybersecurity-qna*
- *axis.com/support/cybersecurity/resources*
- *help.axis.com/axis-security-development-model*
- *axis.com/support/cybersecurity/vulnerability-management*

サイバーセキュリティの定義

NISTの定義の一部に基づいて:

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。

組織の種類

組織によって資産、リソース、露出度、サイバー成熟度は異なります。推奨される実施方法に従う場合、*CISコントロール (旧称: 重要なセキュリティコントロール)*は3つの組織プロファイルを定義しています。

- **SANS実装グループ1 (IG1)**

  ほとんどの場合、IG1企業は中小企業であり、ITやサイバーセキュリティの専門知識が限られているため、IT資産や人員の保護に専念することができません。

- **SANS実装グループ2 (IG2)**

  IG2企業は、ITインフラストラクチャーの管理と保護に責任を持つ個人を雇用しています。このような企業は通常、職務権限や使命に応じてリスクプロファイルが異なる複数の部門をサポートしています。小規模な企業単位では、規制遵守の負担があるかもしれません。

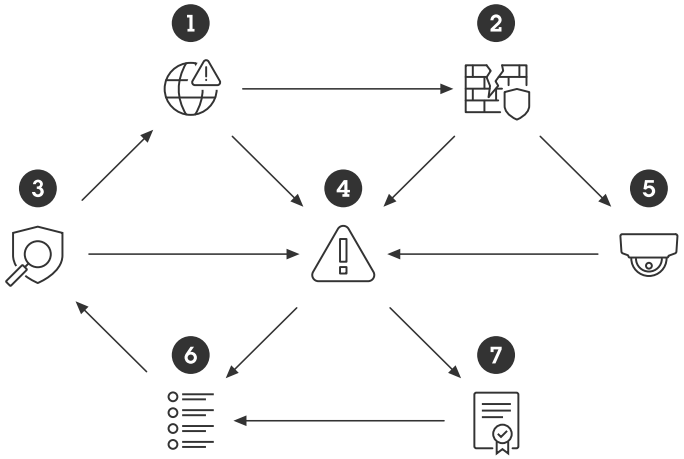
- **SANS実装グループ3 (IG3)**

  IG3企業は一般的に、サイバーセキュリティのさまざまな側面 (リスク管理、侵入テスト、アプリケーションセキュリティなど) を専門とするセキュリティ専門家を雇用しています。IG3資産とデータには、規制やコンプライアンス監視の対象となる機密情報や機能が含まれています。

用語

用語

用語マップは、本ドキュメントで説明する特定のサイバーセキュリティ重要用語の関係を示しています。



- **(2) 脆弱性**が露出している **(5) 資産**と増大する **(4) リスク**を悪用する **(1) 脅威**
- **(4) リスクが**影響する**(7) ポリシー**と**(6) 要件**の提示
- **(6) 要件**は **(3) セキュリティ管理**で解決され、セキュリティ管理は継続的な **(1) 脅威**に直面しながら **(4) リスク**を緩和している

リスク

サイバーセキュリティとは、リスクを長期的に管理することです。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。時々、人々は次のように用語を混同することがあります。リスク、資産、脅威、脆弱性、または悪影響

RFC 4949インターネットセキュリティ用語集では、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もたらす確率として表される損失の予測であると定義しています。

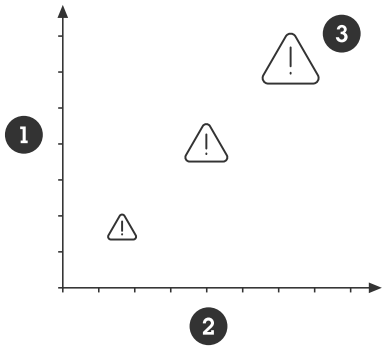
よく使われる省略形は、**リスク = 確率 x 影響**です。

この計算式は、リスクの優先順位付けに使用されます。RFCの定義では、脅威、脆弱性、および有害な結果について「特定の」という用語が使われています。各脅威を個別に検討し、最も信憑性が高く、最も悪影響が大きいものから始める必要があります。

リスクについて議論する際の課題は、確率係数です。物事は起こるかもしれないし、起こらないかもしれません。敵対者が脆弱性を悪用する確率は、多くの場合、脆弱性の悪用がいかに容易であるか (暴露の度合い) と、敵対者が脆弱性を悪用することで得られる潜在的な利益によって決まります。

次の2つの次元でリスクをプロットすることができます。リスクが発生する確率を1つの軸として使用し、リスクが発生した場合のリスクの影響を別の軸に使用します。これにより、各リスクの潜在的な影響と優先順位が明確に表示されます。

用語



*1 **確率**昇順*
*2 **ネガティブな影響**昇順*
*3 **リスクレベル**昇順*

攻撃価値 = 攻撃の利点 – 攻撃コスト

保護を追加すると攻撃コストが増加するため、確率が低下します。攻撃コストは、攻撃を成功させるために必要な時間、リソース、スキル、洗練度に関係します。捕まるリスクやその他の悪影響も攻撃コストの一部です。

サイバー空間におけるリスクを分析するプロセスであるリスク評価は、物理的な保護と同じです。検討すべき質問は以下の通りです

1. 何を守りたいですか?
2. 誰から守りたいですか?
3. 悪影響が出る確率は?
4. 失敗した場合、どの程度の影響がありますか?
5. リスクを軽減するために、どのような戦略を実行すべきですか?

どのような種類の保護対策やセキュリティコントロールを実施するにしても、何らかのコストが発生します。どの組織も財源には限りがあります。リスクが何であるかがわからなければ、保護のための予算を見積もることは困難です。リスクを受け入れることは常に必要ですが、その決断はリスクに基づいた意図的なものでなければなりません。

各資産タイプへの潜在的なマイナスの影響を見積もるのは難しく、複雑です。多くの場合、見積もりは主観的で、影響分析は過小評価されがちです。ISO 27000の影響モデルと指定タイプ (限定的、深刻、深刻、壊滅的など) を使用すると、優先順位をつけるための概要をすばやく把握することができます。つまり、マイナスの影響から回復するのにかかる時間を見積もることで、より正確な値を設定する簡単な方法を提供します。

- **制限付き** = 数時間から数日まで
- **深刻** = 数日から数週間
- **重大** = 数週間から数か月
- **壊滅的 =** 数か月から数年 (仮にあった場合)

資産

物理的保護が人や対象、物体の保護に重点を置いているのに対し、サイバーセキュリティ保護はデータ資産やコンピューターリソースの保護に重点を置いています。主に次の3つの領域があります。

- **機密性**: 情報やリソースの開示

用語

- **完全性**: 情報やリソースの破壊または改変
- **可用性**: 情報やリソースへのアクセス

これらの領域はCIAトライアドとも呼ばれています。オペレーションテクノロジー (OT) はユーザビリティを優先し、インフォメーションテクノロジー (IT) はセキュリティを優先します。機密性、完全性、可用性の適切なバランスを見つけるのは、しばしば困難です。

適切な保護レベルを決定するためには、資産やリソースを分類する必要があります。すべてのデータ資産やコンピューターリソースがマイナスの影響という点では同等であるとは限りません。これらは、多くの場合、次のように分類されます。

- **パブリック**: その資産は一般消費者をターゲットにしています。または、一般に開示された場合、その悪影響は限定的です。
- **プライベート**: 資産に特定の/選択されたグループの特権があります。通常、悪影響は会社や家族など特定の組織内に限られます。
- **制限付き**: 資産は、組織内の選ばれた個人に特権が与えられます。

ビデオシステムのライブビデオは、一般公衆と組織内の公衆の両方を指すパブリックに分類されます。しかし、ほとんどの場合、ライブビデオはプライベートに分類され、特定の組織単位でしかアクセスできません。一方、録画ビデオは、ほとんどの場合、非常にデリケートなシーンがある可能性があるため、制限付きに分類されます。認証情報と設定も制限付きとして分類する必要があります。

脅威

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。

攻撃はどこからともなく起こるものではありません。システムや資産を危険にさらす動機は常に存在します。攻撃には、日和見的なものと標的型のものがあります。サイバーセキュリティでは、攻撃者は悪意を持った敵対者とも呼ばれます。

今日の攻撃の大部分は日和見的な攻撃です。つまり、隙があるところで攻撃が発生します。多くの場合、外部の日和見的攻撃者は、被害者が誰であるかさえ知りません。このような攻撃者は、フィッシングやプロービングといった低コストの攻撃ベクトルを使用します。このような場合、彼らは失敗した攻撃に時間とリソースを費やす決意はなく、すばやく次の試みに移ります。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。標的型攻撃、つまり特定のシステムを特定の目的で狙う攻撃者から守るのはより困難です。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。

一般的な敵対者 (脅威アクター)

- **身近な存在**: あなたの私生活を詮索したがる人たち
- **従業員**: または、偶然または故意の誤用により、システムに合法的にアクセスした人
- **いたずら者**: コンピューターシステムに干渉することが楽しいと感じる人
- **ハクティビスト**: 政治的またはイデオロギー的な動機で組織を攻撃しようとする人々
- **サイバー犯罪者**: 詐欺や価値ある情報の販売で金儲けをしようとする人
- **産業界の競争相手**: 企業や組織の経済的優位性を獲得することに関心のある実体
- **サイバーテロリスト**: 多くの場合、イデオロギー的または政治的な理由からアラームやパニックを引き起こすことを目的とした攻撃を行う人やエンティティ
- **国家**: 経済的利益や政治的利益を得るため、または重要な情報システムに損害を与えるために行動する外国諜報機関の諜報員

- **個人**: 動機が上記と異なる可能性のある、特定の個人またはグループが独自に行動する場合。これは、調査ジャーナリスト、ホワイトハットハッカー、または同様のものである可能性があります。ホワイトハットハッカー (別名、倫理的ハッカー) は、あなたが欠陥を修正するよりもむしろ欠陥を隠すことを優先する場合、脅威となる可能性があります。

脆弱性

すべてのシステムに脆弱性があります。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。欠陥、露出、特性、人為的なミスに起因することもあります。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、システム設定の不備、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

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、セキュリティコントロール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、被害者にはシステムを保護する時間がないため、ゼロデイ悪用が成功するリスクが高まります。

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) レポートには、CVSS番号が記載されていることがよくあります。

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。

ポリシー

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。

セキュリティコントロール

セキュリティコントロールとは、物的財産、情報、コンピューターシステム、その他の資産に対するセキュリティリスクを回避、検知、対策、最小化するために採用される保護措置または対策です。セキュリティコントロールを導入するプロセスは、しばしば強化と呼ばれます。

補償的セキュリティコントロールは、望ましいセキュリティコントロールを適用することができない場合、望ましいコントロールが利用できない場合、またはコストがかかりすぎる場合に使用できる代替的な保護手段です。

セキュリティコントロールは、長期にわたる脅威、価値、脆弱性、露出の変化に応じて継続的に監視および更新する必要があります。これには、ポリシーとプロセスを定め、それに従うことが必要です。

SANS Instituteは、*CISコントロールのリスト*を発表しました。これは、優先順位付けされたサイバー防御のベストプラクティスの推奨セットです。セキュリティコントロールの多様性を示すために、ここにリストの全容を示します。

- CISコントロール#1: 企業資産のインベントリとコントロール
- CISコントロール#2: ソフトウェア資産のインベントリとコントロール
- CISコントロール#3: データ保護
- CISコントロール#4: 企業資産とソフトウェアの安全な設定

用語

- CISコントロール#5: アカウント管理
- CISコントロール#6: アクセスコントロールの管理
- CISコントロール#7: 継続的な脆弱性の管理
- CISコントロール#8: 監査ログの管理
- CISコントロール#9: 電子メールおよびWebブラウザーの保護
- CISコントロール#10: マルウェアの防御
- CISコントロール#11: データの復元
- CISコントロール#12: ネットワークインフラストラクチャーの管理
- CISコントロール#13: ネットワークの監視と防御
- CISコントロール#14: セキュリティ意識と技能のトレーニング
- CISコントロール#15: サービスプロバイダーの管理
- CISコントロール#16: アプリケーションソフトウェアのセキュリティ
- CISコントロール#17: インシデント対応の管理
- CISコントロール#18: 侵入テスト

*AXIS OS強化ガイド*はCISに基づいています。

一般的な脅威に対する保護手段

一般的な脅威に対する保護手段

一般的な脅威を理解し、それに対抗することで、リスクの大部分を軽減することができます。

故意または過失によるシステムの誤用

システムの使い勝手とセキュリティのバランスと取るのは容易ではありません。多くのシステムは、セキュリティではなく、利便性の観点から強化されています。このため、故意または偶発的な誤用が発生する可能性があります。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。

一般的な脅威の例:

- 個人は、許可されていないサービス (ライブまたは録画ビデオなど) にアクセスする可能性があります。
- 個人は過ちを犯します
- システムのパフォーマンスを低下させるような修正を個人が試みることがあります
- 不満を持つ個人が故意にシステムに損害を与える可能性があります
- 個人はソーシャルエンジニアリングの影響を受けやすい
- 個人が盗む
- 個人は、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。
- 個人のコンピューターが侵害され、意図せずにシステムがマルウェアに感染する場合もあります

一般的な推奨される保護手段は次のとおりです。

- 定義済みのユーザーアカウントポリシーとプロセス
- 十分なアクセス認証方式
- ユーザーアカウントと権限を長期的に管理するツール
- 露出の低減
- サイバー意識向上トレーニング

Axisがこの脅威に対抗している方法:

- *AXIS OS Hardening Guide*では、装置の一般的な脅威に対する一般的なセキュリティコントロールについて説明しています
- *AXIS Camera Station Hardening Guide*では、ビデオシステムの一般的なセキュリティコントロールについて説明しています
- *AXIS Device Manager*と*AXIS Device Manager Extend*は、一般的なセキュリティコントロールの管理に役立ちます

物理的ないたずらや妨害行為

ITシステムの物理的保護は、サイバーセキュリティの観点から非常に重要です。

一般的な脅威の例:

- 物理的に露出した機器がいたずらされる可能性があります
- 物理的に露出したギアが盗まれる可能性があります

- 物理的に露出したケーブルが、外される、方向転換される、切断される可能性があります

一般的な推奨される保護手段は次のとおりです。

- ネットワーク機器 (サーバーやスイッチなど) を鍵のかかる場所に設置する
- 手の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
- 壁やコンジットのケーブルを保護する

Axisがこの脅威に対抗している方法:

- 暗号化されたSDカードにより、権限のないユーザーがSDカードを取り出すことができてもビデオを再生できないようにする
- カメラビューに対するいたずらの検知
- ケーシング開放検知

既知のソフトウェア脆弱性の悪用

すべてのソフトウェアベースの製品には、悪用される可能性のある脆弱性があります。これらは既知のものと未知のものに分類されます。すべての未知の脆弱性はいずれ明らかになります。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。時折、悪用可能で重大な悪影響を及ぼす可能性がある脆弱性が発見されます。MITREは、人々がリスクを軽減するのに役立つCVE (共通脆弱性識別子) の大規模なデータベースをホストしています。

一般的な推奨される保護手段は次のとおりです。

- 継続的なパッチ適用プロセスは、システム内の既知の脆弱性の数を最小限に抑えるのに役立ちます。
- ネットワークの露出を最小限に抑え、既知の脆弱性の探索や悪用をより困難にします。
- 欠陥を最小限に抑えるポリシーとプロセスに従って作業し、パッチを提供するプロセスを持ち、重大な脆弱性が発見されたときに開示を行う、信頼できるサブサプライヤーと協力します。

Axisのサポート:

- *Axisセキュリティ開発モデル*は、ソフトウェアの脆弱性を含む製品をリリースするリスクを低減するためにAxisが使用するプロセスとツールを定義するフレームワークです。
- *Axis脆弱性管理ポリシー*では、お客様が適切な対応を取るために認識する必要がある脆弱性の特定、修正、および開示を行っています。2021年4月以降、AxisはAxis製品のCVE (共通脆弱性識別子) 番号付与機関 (CNA) として承認され、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るようになりました。その結果、より良い方法でお客様をサポートすることができます。
- *AXIS OS Hardening Guide*などの*Axis強化ガイド*は、ソフトウェア欠陥の悪用のリスクを低減するために、暴露を低減し、補完コントロールを追加する方法に関する推奨事項を提供しています。
- LTS (長期サポート) ファームウェアバージョンにより、お客様はAxis装置のオペレーティングシステムにパッチを適用することができ、サードパーティのビデオ管理システムとの非互換性問題のリスクを最小限に抑えることができます。

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。これは主に、他の攻撃手段 (ソーシャルエンジニアリング、フィッシング攻撃、インターフェースプロービングなど) が、システムの保護レベルが高いために失敗した場合に使用されます。この攻撃では、ソフトウェア/ファームウェア/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

一般的な脅威に対する保護手段

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。サプライチェーン攻撃を成功させるには、スキル、時間、リソースが必要です。

一般的な推奨される保護手段は次のとおりです。

- 信頼され、検証されたソース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設定します。
- インストール前に、ソフトウェアのチェックサム (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します。
- 配信時に、パッケージまたは製品に改ざんの形跡がないか確認します。

Axisがこの脅威に対抗している方法:

- Axisのソフトウェアはチェックサム付きで公開されているため、管理者はインストール前にソフトウェアの整合性を確認することができます。
- Axis装置内で署名されたファームウェアを使用することで、インストールされているAXIS OSがAxisによる純粋なものであること、および装置にダウンロードしてインストールされる新しいファームウェアもAxisによる署名付きであることが保証されます。
- Axis装置のセキュアブートでは、ファームウェアにAxis署名があることを装置が確認できます。ファームウェアが不正なものであったり、変更されていたりすると、ブートプロセスは中断されます。
- IEEE 802.1AR準拠のAxis装置IDは、装置固有のAxisベンダー証明書であり、ケーシング内のハードウェアがAxisのものであることをシステムが確認する方法を提供します。
- SDカードの暗号化とファイルシステムの暗号化により、カードや装置の盗難時に保存データの抽出を防止します。

ユーザーマニュアル
Cybersecurity reference guide

バージョン M3.2
日付: 2023年11月
製品番号 T10201166