ホワイトペーパー

サイバーセキュリティ

コンセプトおよび用語

目次

1. はじめに

本ドキュメントでは、サイバーセキュリティのコンセプトおよび用語に関する概要を説明しています。内容は簡潔な定義、モデルおよび構造に基づいています。物理セキュリティシステムに重点を置き、サイバーセキュリティの基本を理解したい個人および組織のお客様を対象に作成されています。本ドキュメントは、アクシスのその他のサイバーセキュリティ関連ドキュメント向けの用語集および定義参考資料です。

2. サイバーセキュリティ

サイバーセキュリティにはいくつかの定義がありますが、ウィキペディアの「コンピューターセキュリティ」(英語版) では以下のように定義づけられています。

> *サイバーセキュリティまたはITセキュリティとも呼ばれるコンピューターセキュリティは、ハードウェア、ソフトウェアまたはそれらに保存された情報を盗難や破損から保護するとともに、こういった不正行為がもたらすサービスの停止または誤用から保護するコンピューターシステムのことである。*

オンライン上での安全性を常に確保できる唯一の方法は存在しません。デジタルセキュリティで重要なのはどのツールを使用するかではなく、直面する脅威とその脅威への対策方法を理解することです。セキュリティを向上するためには、保護する必要のある資産とその資産を誰から保護すべきなのかを判断しなくてはなりません。脅威は貴社の場所、業務内容、共に働くスタッフにより変わる場合があります。そのため、貴社にとって最適なソリューションを選択するには、脅威モデル評価を実施する必要があります。

3. リスクアセスメント

サイバースペースにおけるリスク分析のプロセスは、物理的な保護におけるリスク分析と類似しています。一般的に物理的世界で保護が必要となるのは物体、建物および人物ですが、サイバースペースでは情報/データ、リソースおよびサービスが資産となります。物理的な侵害、盗難、破損はサイバースペースに比べて発見しやすいと言えます。

リスクアセスメントを実施する際の5つの基本的な質問：

1. 保護したい資産は何か？
2. 誰から資産を守りたいか？
3. 資産を保護しなければならなくなる可能性はどの程度か？
4. 保護できなかった場合、被害はどの程度か？
5. 資産を保護するためにどの程度の努力ができるか？

情報保護に関するISO 27000規格では、資産の**機密性、可用性**および**完全性** (CIA 3要素) について説明しています。

データやサービスにアクセスできなかった場合、データが破壊された場合またはアクセス権のない第三者にデータが流出した場合、どのような影響があるでしょうか？データの種類に応じて価値が異なる場合があるため、影響を評価するためにはデータを分類する必要があります。

ISOでは、データおよびサービスを**機密情報、私的情報**および**公共情報**に分類しています。例えば、1つの映像システムでは映像システムのリソースを次のように分類できます。

> ライブ映像は公共情報に分類されます。一般的な民間または組織内のスタッフなどがデータの利用者となります。ライブ映像が一般に公開される場合、危険性は限定されます。

> 録画は**私的情報**に分類できます。録画されたインシデントの一部は機密情報を含んでいる可能性があるため、特定の組織にのみアクセス権が与えられます。

> システム設定、アカウントおよびパスワードは**機密情報**に分類されます。組織内の特定の個人のみにアクセス権が与えられます。

4. 脅威の全体像

何者かが脆弱性を悪用しシステムを攻撃する場合は、常に根本的な理由が存在します。攻撃は日和見型または標的型のいずれかに分類できます。サイバーセキュリティでは、攻撃者は**アドバーサリー**とも呼ばれ、悪意がある人物と無意識に(または誤って)資産に危害を加える人物とがいます。

今日の攻撃の大半は、ある種の欠陥を利用して攻撃を試みる日和見型攻撃です。多くの場合、日和見型攻撃者は標的と面識がありません。こういった攻撃者はオープンネットワーク、サービスまたはポートのスキャニング、デフォルトの、または一般的なパスワードの試行、パッチが適用されていないサービスの検索、フィッシングメールの送信など、低コストの攻撃方法を使用します。攻撃に失敗した場合、日和見型攻撃者は時間やリソースを投資しようという強い意志は持たず、次の標的に移ります。日和見型攻撃に関連するほとんどのリスクは、標準的なレベルの保護を適用することで低減できます。

特定の目的を持って特定のシステムを狙う標的型攻撃からの保護は、より難易度が高くなります。標的型攻撃も日和見型攻撃と同様に、最初は低コストの攻撃方法を使用します。しかしこういった攻撃者はより強い意志を持ち、最初の攻撃でアクセスに失敗した場合でも侵入に成功した場合に予測される価値に応じて、より多くの時間とリソースを投資し、さらに高度な手段を使用します。標的型攻撃者は、高度なソーシャルエンジニアリングやスピアフィッシング(特定の受信者を標的として巧妙に作成されたEメール)を使用してシステムへのアクセスを得ることが多くあります。この試みに失敗すると、攻撃者はシステムやソフトウェア、プロセスなどを分析し、代わりとなる悪用可能な脆弱性を探ります。

5. 攻撃者と攻撃者の動機

どちらのタイプの攻撃者から攻撃を受ける可能性が高いかをある程度把握することで、その攻撃者の予測される動機、投資する時間やリソース、意思の強さ、そして攻撃者に標的にされやすい脆弱性に関する洞察を得ることができます。

> **身近な人物**。オーナーの私生活を詮索したい場合など。

> **従業員**または正当なアクセス権を持つ人物。偶発的または意図的な悪用を行う。

> **迷惑行為を行う人物**。コンピューターシステムにいたずらをするのを楽しむ。

> **ハクティビスト**。政治的またはイデオロギー的な理由により組織を攻撃する。

> **サイバー犯罪者**。詐欺行為または重要な情報の販売によって金銭を稼ぐことを目的とする。

> **競合社**。自分たちの会社のために経済的な優位性を得ようとする。

> **サイバーテロリスト**。イデオロギー的または政治的な目的で、混乱やパニックを起こすための攻撃をしかける。

> **国家** (対外情報庁)。経済的利益や政治的利益を得る、または極めて重要な情報システムに被害を与えることを目的とする。

> **個人**。単独で活動する特定の人物またはグループ。上記に記載された動機とは異なる動機を持つ。例としては調査活動中のジャーナリストやホワイトハットハッカーなどが挙げられる。ホワイトハットハッカー (エシカルハッカー) は、オーナーが所有するシステムの欠陥や脆弱性を修正するのではなく、隠すことにリソースを投資した場合などに脅威を与えることがある。

6. 攻撃の利益とコスト

攻撃の価値は、攻撃にかかるコストに対して、侵入に成功した場合にどれだけの利益を得られるかに応じて異なります。サイバーセキュリティの目標は、攻撃にかかるコストが利益を上回るようにする、つまり攻撃の価値を下げることです (価値 = 利益 - コスト)。適切な保護レベルを適用する (攻撃のコストを明確にする) ためには、可能性の高い脅威を把握することが重要です。すべてのシステムはあらゆる脅威や標的の対象となり得ますが、一部の脅威はその他の脅威に比べて可能性が高いと言えます。可能性がより高い脅威を把握することで、重点的にセキュリティ手段を講じる場所 (悪用される可能性の高い脆弱性) を特定しやすくなります。

7. 一般的な組織タイプと脅威

一般的に、攻撃による悪影響は標的となる組織のタイプに応じて異なります。

組織のタイプ	**例**	**可能性の高い攻撃者**	**影響**
小規模組織	> 消費者 > 家族経営ビジネス > 非営利組織	> 身近な人物 > 迷惑行為を行う人物 > 日和見型ハッカー	**個人**レベル > プライバシー > 完全性
企業組織	> 製造業 > 企業 > 小売店舗	上記に加えて： > 従業員 > ハクティビスト > 組織的犯罪者 > 競合社	**ビジネス**レベル > 金銭的損失 > ダウンタイム > 信用 > 知的財産 > 競争力
重要なインフラ施設	> エネルギー施設/水処理施設 > 金融機関 > 通信事業 > 交通機関 > 医療機関 > 警察/軍事施設	上記に加えて： > 国家 > サイバーテロリスト	**公的**レベル > 安全性 > 供給品 > パニック

8. リスク

「リスク」の定義は人により異なる場合がありますが、「RFC 2828インターネットセキュリティ小辞典」では以下のように定義づけています。

特定の脅威が特定の脆弱性を攻略し、特定の有害な結果をもたらす確率として表明される損失の期待値。

略式としてよく使用されるのが「リスク = *発生確率 x 影響度*」という数式です。この数式は、脅威のさまざまなタイプの優先順位を決めるために使用されます。RFCの定義では、「脅威」、「脆弱性」および「有害な危害」に対する表現に「特定」という言葉が含まれています。すべての脅威は個々に検証する必要があり、最も発生する可能性が高く、最も悪影響を及ぼすものから始めます。

各保護タイプ (機密性、可用性および完全性) に関しては、脅威の悪影響をある程度理解しておくことが重要です。この作業は難しく、予測が主観的であるケースや、影響を過小評価しているケースが多くみられます。ISO 27000が定義づけている影響度のタイプ (**限定的、深刻、危機的**または**致命的**) を使用することで、優先順位を決めるための概要をつかみやすくなります。攻撃から回復するまでにかかる時間に基づいて影響度タイプを考慮することができます (限定的 = 数時間/数日、深刻 = 数週間、危機的 = 数か月、致命的 = 数年など)。

9. セキュリティコントロール

セキュリティコントロールを追加するプロセスは「強化」と呼ばれます。セキュリティコントロールとは、物理的なプロパティ、情報、コンピューターシステムまたはその他の資産に対するセキュリティリスクを回避、検出、防止または最小限に軽減する予防対策や防衛手段です。補償コントロールとは、望ましいセキュリティコントロールを適用できない場合や、希望する保護の費用が高すぎる場合などに導入可能な代替予防対策です。

アクセス制限と露出の低減は、システムを使いづらくさせます。システムの使い勝手とシステムの保護とのバランスを取るには、システムユーザーのニーズとシステムを保護する担当者のニーズ間における難しい妥協が求められることが多くあります。制限が厳しすぎればユーザーは適用された保護をバイパスする方法を見つけ出し、結果的に新たな脆弱性をもたらす可能性があります。使い勝手と保護の間における望ましいバランスは、システムオーナーが判断しなければなりません。

10. 脆弱性と露出

脆弱性は攻撃者に対しシステムへ不正アクセスを行う機会を与えます。この脆弱性は欠陥、特性またはユーザーエラーによって生じる場合があります。攻撃者はこういったあらゆる機会を利用しようとし、多くの場合1つまたは複数の機会を組み合わせて目的の達成を試みます。

調査によると、達成される侵害全体の95%以上は3つの要因、つまり人的ミス、システムの不適切な設定、システムの不適切なメンテナンスによるものです。こういった状況は、一般的に適切な方針や責任の所在がしっかりと定められていないことにより生じます。

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)およびソフトウェアサービスには、攻撃に悪用可能な欠陥が含まれていることがあります。自社の製品に欠陥がないと保証できるベンダーは存在しません。既知の欠陥である場合は、補償セキュリティコントロールでリスクを低減できることがあります。一方、攻撃者が未知の欠陥を見つけ出した場合は、標的にシステムを保護する時間を一切与えないゼロデイエクスプロイトが生じる可能性があります。

危機的ではない脆弱性とは、影響度が低い、または潜在的な影響度は深刻であるものの悪用が困難な脆弱性のいずれかを指します。重大な欠陥を悪用するには、ネットワークへのアクセスやネットワークが提供するリソースへのアクセスの取得など、多数の条件を満たす必要があります。

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1つの手段です。このシステムは対象の脆弱性がいかに悪用しやすいか、そしてどういった悪影響が生じるかを検証する数式を使用します。スコアは0～10の数値で示され、10が最も深刻です。多くの場合、CVSS番号は公開されているCommon Vulnerability and Exposure (CVE) レポートに記載されています。アクシスは、ソフトウェアや製品に含まれる既知の脆弱性の深刻度を予測する複数の手段の1つとしてCVSSを使用しています。

露出もまた、脆弱性のリスクを判断する一因になります。攻撃者がその脆弱性を悪用しやすいかどうかは、インフラ、サービスの露出および日常業務に応じて異なります。
例えば、エンタープライズビジネスポータルを提供する公共ウェブサーバーで、脆弱性のリスクが危機的と分類されたとします。しかし同じ脆弱性でも、保護されたローカルネットワーク上のカメラで使用される場合は、限定的と分類できる可能性があります。

11. 脆弱性スキャン

脆弱性スキャンとはソフトウェアや製品の自動検査または手動検査で、複数のスキャンツールが市販されています。脆弱性スキャンは、既知の脆弱性を含むサービスの特定を試みます。このようなサービスは攻撃者に露出された場合、悪用される可能性があります。

脆弱性スキャンは既知の脆弱性しか発見できません。この結果は製品の安全性を示す指標としては適していません。明日、重大な脆弱性が新たに発見される可能性もあります。脆弱性スキャンは、侵入テストと混同されることがあります。侵入テストでは能動的にセキュリティコントロールのバイパスを試みます。脆弱性スキャンは潜在的な脆弱性のみを検出します。

12. IPフィルタリング

IPフィルタリングは、カメラでローカルファイアウォールのような働きをします。プロフェッショナル向け映像システムでは、ビデオ管理システム (VMS) がシステムの中核です。ビデオクライアントがカメラから直接映像へアクセスすることはなく、ライブ映像および録画は、VMSサービスを介してクライアントに提供されます。つまり通常運転時は、コンピューター/サーバーのみがカメラへアクセスします。非ビデオクライアントがカメラへのネットワークアクセスを持つ、隔離されていないネットワーク上に映像システムがある場合は、追加の保護としてIPフィルタリングを適用できます。IPフィルタリングを使用すると、カメラはホワイトリストに登録されていないIPアドレスからの要求に応答しなくなります。ホワイトリストにはVMSサーバー、AXIS Camera Management (ACM) サーバー、およびトラブルシューティングやメンテナンスに使用されるその他のPC(使用している場合) が含まれている必要があります。

13. ネットワークの隔離 (ネットワークセグメンテーション)

ネットワークの隔離とは、極めて重要なネットワークリソースを互いに分離することにより、いずれかのリソースが別のリソースに悪影響を及ぼすリスクを低減する方法です。隔離は、相互に情報をやり取りする必要のない (またはやり取りするべきではない) リソースに特に関係します。ネットワークセグメンテーションは仮想化が可能で、この場合はマネージドスイッチのインフラが必要です。また、異なる配線とネットワークギアを使用してネットワークを隔離することもできます。使用するセグメンテーションのタイプはコスト、インフラ、ポリシーに応じて異なります。

総合的な保護を高めるには、物理的なセキュリティネットワークをその他の (ドメイン) ネットワークリソースから隔離します。あるネットワーク上のビデオクライアントが別のセグメント上のVMSサーバーにアクセスする必要がある場合は、2つのセグメント間にファイアウォールを追加できます。ファイアウォールは、クライアントとVMSサーバー間の通信のみを通過させ、カメラへの通信は阻止します。

14. ネットワークの暗号化 – HTTPS

ネットワークの暗号化は、クライアント、VMS、カメラ間の通信を保護します。ネットワークトラフィックのスニッフィングにより情報が抽出されたり、送信中にデータが改ざんされたりするのを防止します。ネットワークの暗号化は必ずしもカメラ、VMSまたはクライアントに対する保護を高めるとは限りません。

アクシスのカメラはHTTPS (安全なSSL/TLSトンネルを介したHTTP) に対応しています。クライアント (VMSなど) もHTTPSに対応している必要があります。HTTPSはすべての管理トラフィック (通常のHTTPトラフィック) を暗号化しますが、映像はRTSP (リアルタイム・ストリーミング・プロトコル) を介して転送されるため、必ずしも暗号化されるとは限りません。映像を暗号化するには、VMSが暗号化されたTLSトンネルを介してトンネリングされたRTSPの要求にも対応している必要があります。すべてのVMSが対応しているわけではないため、VMSのベンダーに確認してください。HTTPSを確立するには、カメラに証明書 (自己署名またはCAによる署名) があり、HTTPSポリシーが設定されている必要があります。

15. 認定局 (CA)

自己署名証明書を使用してもCA署名証明書を使用しても、暗号化レベルは同じです。違いは、自己署名証明書はネットワークスプーフィング (攻撃者のコンピューターが正当なクライアントまたはサーバーになりすます行為) に対する保護を提供しないことです。CA署名証明書は、クライアントが信頼できるカメラにアクセスしていることを認証するためのトラストポイントを追加します。CA署名証明書は、HTTPS (**サーバー証明書**) および802.1x (**クライアント証明書**) の両方で使用されます。

パブリック vs. プライベートCA

Comodo社やSymantec社 (前Verisign社) など、公的に信頼されたCAは、一般的に公共ウェブサイトやEメールサーバーなどの公共サービスに使用されます。公的に信頼されたCA用のCAルート証明書は、ほとんどのオペレーティングシステム (Windows、Linux、Mac) やブラウザにあらかじめインストールされています。

プライベートCAは、内部/プライベートネットワークサービス向けのトラストポイントです。プライベートCAは、すべての内部クライアントおよびサーバー用の証明書を発行するために使用されるソフトウェア/サーバー (通常はActive Directory / Certificate Service) です。プライベートCAルート証明書は、プライベートリソースにアクセスするすべてのクライアントにインストールする必要があります。証明書の展開は、利用可能なツールおよびインフラに応じて手動または自動で行うことができます。

16. ネットワークアクセスコントロール – 802.1X

IEEE 802.1Xは、認証されていないネットワーク装置がローカルネットワークにアクセスするのを防止することを目的として定められた規格です。装置がネットワーク (およびネットワークのリソース) へアクセスする許可を得るには、装置自体が正当であることを証明する必要があります。MACアドレス (MACフィルタリング)、ユーザー/パスワード、またはクライアント証明書など、さまざまな認証方法があります。システムのオーナーは脅威、リスク、コストに応じて最適な方法を選択します。

802.1Xのインフラの運用は投資です。マネージドスイッチと追加のサーバー、通常はRADIUS (Remote Authentication Dial-In User Service) が必要です。クライアント証明書を使用するには、クライアント証明書を発行できるCA (プライベートまたはパブリック) が必要です。ほとんどの場合、このインフラにはインフラのメンテナンスと監視を行うスタッフが必要です。エンドユーザーが802.1Xのインフラを使用していない場合、ネットワークビデオ/セキュリティシステムを追加する際にこのインフラを追加する可能性は低いと言えます。さまざまな重要なネットワークリソースの露出を減らすために、802.1Xに代わる方法を提供できる補償コントロールは、ネットワークの分離です。

17. SNMP

SNMP(簡易ネットワーク管理プロトコル)は、IPネットワーク上のマネージドデバイスに関する情報の収集と整理に使用されます。カメラのモニタリングにSNMPを使用することにより、カメラの誤動作や攻撃の可能性を示す切断を検出しやすくなる場合があります。

18. Syslogサーバー

すべてのカメラには、カメラ内の全操作を記録する内部ログがあります。このログは、侵入攻撃が成功したときにカメラが再起動された場合、または攻撃者が消去や変更を行った場合に失われる可能性があります。リモートSyslogサーバーは、日々の稼働中にすべてのカメラログメッセージを収集できます。リモートSyslogサーバーでログを保護することにより、トラブルシューティングや現場検証調査を簡素化し、異常や侵入の痕跡を見つけることができます。

19. 詳細情報:

www.axis.com/support/product-security

> Axis 脆弱性ポリシー

> Axis 強化ガイド (Hardening Guide)

> セキュリティ情報 (CVE)

> ホワイトペーパー

www.axis.com/learning/online-courses

> サイバーセキュリティに関するAXIS Academyのトレーニング

www.axis.com/blog/secure-insights/category/cyber-security

> サイバーセキュリティに関するさまざまなトピック

71009/JA/R1/1708

Axis Communicationsについて

アクシスは、インテリジェントなセキュリティソリューションを通じて、よりスマートで安全な環境の実現を目指しています。ネットワークビデオ市場をけん引するリーダーとして、アクシスはオープンプラットフォームを基盤とした革新的なネットワーク機器を次々と開発し、製品化しています。また、パートナーとのグローバルな連携体制を通じて、お客様に付加価値の高い製品をお届けします。アクシスでは、長年にわたってパートナーと協力関係を築いてきました。アクシスはこうしたパートナーに向け、蓄積された知見と、既存および新規市場における画期的なネットワーク製品を提供しています。

アクシスは全世界50ヶ国以上に2,700人を超える熱意にあふれた従業員を擁し、90,000以上のグローバルパートナーから成る連携体制に支えられています。スウェーデンに本社を置くアクシスは1984年に設立され、NASDAQ Stockholm（ティッカーシンボルAXIS)に株式上場しています。

より詳しい情報はwww.axis.comをご覧ください。

AXIS COMMUNICATIONS