ホワイトペーパー

NIS 2

6月 2024

目次

1 はじめに

1.1 NIS 2とは？

NIS 2はEU指令であり、2024年10月17日までにEU各加盟国の国内法に移管されることになっています。NIS 2は、EU全域で高い共通レベルのサイバーセキュリティを達成し、その地域内のセキュリティと経済・社会の効果的な機能に貢献することを目指しています。これは、社会の重要な分野で必要不可欠かつ重要なサービスを提供する事業体に対して、サイバーセキュリティ能力を構築し、ネットワークや情報システムに対する脅威を軽減し、インシデントに直面した際にサービスの継続性を確保し、セキュリティインシデントを関係当局に報告することを要求しています。加盟国には、国家サイバーセキュリティ戦略を採用し、サイバー危機管理当局やコンピューターセキュリティインシデント対応チームを含む当局を設置することを要求しています。そして、サイバーセキュリティのリスク管理策や実施策を概説しています。必要不可欠で重要な事業体がコンプライアンスを守らない場合は、管理チームへの多額の罰金や法的措置が含まれる可能性があります。

詳しくは、*eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555&qid=1713340785613*をご覧ください。

1.2 NIS 2は誰に影響を与えるのか？

NIS 2は、 **必要不可欠な** または **重要な** サービスを欧州の経済と社会に提供するすべての事業体（企業とサプライヤーを含む）に影響します。

1.2.1 直接影響を受ける

必要不可欠な事業体 - エネルギー、運輸、金融機関、健康、飲料水、下水、デジタルインフラ、行政、宇宙

重要な事業体 - 郵便事業、廃棄物管理、化学薬品、食品、製造（医療機器、電気、輸送機器など）、デジタルプロバイダー（オンラインマーケットプレイス、検索エンジン、ソーシャルネットワークなど）、研究組織

国の管轄当局 - 各国の管轄当局は、EU加盟国によって指定され、それぞれの国内におけるNIS 2の実施と施行を監督します。

1.2.2 間接的な影響

ベンダーとサプライヤー - NIS 2は、必要不可欠で重要な事業体に向けて必要不可欠なサービスやデジタルサービスを提供するベンダー、サプライヤー、サードパーティサービスプロバイダーに間接的に影響します。こうした企業は、自社の製品やサービスのセキュリティを確保する必要があり、その顧客からサイバーセキュリティに関する契約上の要求を受けている可能性があります。

必要不可欠なサービスやデジタルサービスのユーザー - 必要不可欠なサービスやデジタルサービスのユーザーは、NIS 2によって直接規制されるわけではありませんが、この指令によって要求されるサイバーセキュリティのプラクティスとインシデント対応能力が向上するという恩恵を受けます。これは間接的に、それらが依存するサービスのセキュリティと信頼性を高めることになります。

2 NIS 2の要件

2.1 必要不可欠で重要な事業体の場合

セキュリティ対策 - リスクを管理し、ネットワークと情報システムのセキュリティを確保するために、適切なセキュリティ対策を実施します。こうした対策は、リスク評価とベストプラクティスに基づく必要があります。

インシデントレポート - ネットワークと情報システムのセキュリティに重大な影響を及ぼしうる重大なインシデントを管轄当局に報告します。対応を調整し、潜在的な被害を軽減するためには、適時に報告することが不可欠です。

リスク管理 - リスクアセスメントを実施し、潜在的な脅威と脆弱性を特定し、それらのリスクを軽減するための対策を講じます。

管轄当局との協力 - EU加盟国が指定する管轄当局と協力します。これには、規制監督やインシデント対応目的のために必要な情報やシステムへのアクセスを提供することも含まれます。

インシデント対応計画 - サイバーセキュリティインシデントに効果的に対応するためのインシデント対応計画を策定・維持します。こうした計画は、インシデントを検知、報告、緩和するための手順を概説する必要があります。

サプライチェーンのセキュリティ - ネットワークと情報システムの全般的な耐久性を確保するため、サードパーティベンダーやサプライヤーも含めてサプライチェーンのセキュリティを確保します。

継続的な監視 - 脅威や脆弱性をリアルタイムで検知・対応するため、ネットワークや情報システムの継続的な監視と監査を実施します。

3 サプライヤーへの影響

サプライヤーは、以下の要件に対応することで、NIS 2事業体をサポートできます。

セキュリティ・バイ・デザイン - IoTデバイスメーカーは、設計段階からデバイスにセキュリティ機能を組み込み、セキュリティが製品の不可欠な要素であることを保証する必要があります。

定期的な更新とパッチ - メーカーは、IoTデバイスの脆弱性に対処するため、定期的なセキュリティ更新とパッチを提供する必要があります。

認証と認可 - IoTデバイスは、不正アクセスを防止するため、強力な認証メカニズムと適切な認可制御（authorization controls）を採用する必要があります。

データの暗号化 - IoTデバイスによるデータの伝送とストレージは、機密情報が傍受されたり、権限のない第三者によってアクセスされたりするのを防ぐために暗号化される必要があります。

インシデントレポート - メーカーは、IoTデバイスに関連する重大なセキュリティインシデントや侵害があれば、関係当局に報告し、可能性として消費者や顧客も報告する必要があります。

プライバシーへの配慮 - 個人データを処理するIoTデバイスは、NIS 2に加えてGDPR（一般データ保護規則）などのデータ保護規制にも準拠する必要があります。

サプライチェーンのセキュリティ - コンポーネントサプライヤーから顧客に至るサプライチェーン全体のセキュリティを確保することは、製造プロセスのあらゆる時点でセキュリティの脆弱性が入り込む可能性を防ぐために必要なことです。

4 Axisの対応

以下では、AxisがサプライヤーとしてNIS 2事業体の要件を満たすかを説明します。

4.1 セキュリティ・バイ・デザイン

セキュリティ・バイ・デザインとは、製品の設計・開発の不可欠な部分としてセキュリティに関する配慮と活動を確実に実施し、脆弱性のリスクを軽減し、製品に対してロバスト性の高いセキュリティ設定がデフォルトで行われるようにするためにとられるアプローチです。Axisでは、セキュリティ・バイ・デザインの原則がソフトウェアとハードウェアに適用され、次の主な要素によって網羅されています。

- *Axis Security Development Model（ASDM）*：ASDMは、定義されたプロセスとツールのフレームワークであり、セキュリティへの配慮がソフトウェア開発の不可欠な要素であることを保証します。活動には、リスク評価、脅威モデリング、侵入テスト、脆弱性スキャン、インシデント管理、バグ報奨金プログラムの実施などが含まれます。Axisソフトウェア開発者はASDMを使用して、ソフトウェア開発にセキュリティが組み込まれていることを確認し、脆弱性のあるソフトウェアをリリースするリスクを軽減します。
- *バグバウンティプログラム*：Axisは、ほとんどのAxis製品を動かしているLinuxベースのオペレーティングシステムであるAXIS OSの脆弱性を積極的に特定し、パッチを適用し、開示するという当社の取り組みを強化するプライベートバグバウンティプログラム（脆弱性報奨金制度）をサポートしています。これにより、外部のセキュリティ研究者や倫理的ハッカーとの専門的な関係を構築するというAxisの取り組みが強化されます。
- *ソフトウェア部品表（SBOM）*：Axisは、ほとんどのAxisデバイスで使用されるLinuxベースのオペレーティングシステムであるAXIS OSにSBOMを提供します。これにより、セキュリティ研究者、当局、および顧客に、AXIS OSを構成するソフトウェアコンポーネントに関する洞察が提供されます。これは、脆弱性評価と脅威分析を専門とする人々にとって特に役立ち、サイバーセキュリティの透明性に対するAxisの取り組みを示すものです。
- *AXIS OSデフォルトセキュリティ設定*：最新のAXIS OSバージョンを実行しているデバイスは、工場出荷時の状態で次のように設定されています。デフォルトパスワードなし、HTTPとHTTPSが有効、IEEE 802.1X/802.1AR/802.1AEによるセキュアなオンボーディングと通信がデフォルトで有効、セキュアでないプロトコルは無効。デフォルト保護制御の詳細については、*こちら*をご覧ください。
- *Axis Edge Vault*：Axisデバイスに内蔵されたAxis Edge Vaultは、ハードウェアベースのセキュリティプラットフォームであり、Axisネットワーク製品の完全性を保護する機能や、暗号キーに基づく安全な動作を有効にする機能を備えています。セキュアブートと署名付きOSによるサプライチェーン保護、デバイスの出所を証明する内蔵Axisデバイス固有IDによる信頼できるデバイス識別、暗号情報の改ざん防止ストレージのための安全なキーストレージ、署名付きビデオによるビデオ改ざん検知を提供します。

4.2 定期的な更新とパッチ

Axisでは、ハードウェアおよびソフトウェア製品で新たに発見されたセキュリティ上の脆弱性に対処するため、ソフトウェアの更新を提供しています。またAxisでは、顧客がAxisデバイスソフトウェアを最新の状態に保ちやすくするためのデバイス管理ツールも提供しています。接続デバイス向けの新しいAXIS OSリリースは、Axis Companion、AXIS Camera Station、パートナービデオ管理ソフトウェア（Milestone XProtect®やGenetec™ Security Centerなど）、およびAxisデバイス管理ツールで紹介されています。さらにAxisでは、誰でも加入できるセキュリティ通知サービスを提供しています。詳しい情報は以下で説明されています。

- *AXIS OS*：Axisでは、デバイスソフトウェアを最新の状態に保つため、アクティブトラックと長期サポート（LTS）トラックという2つの主な選択肢を提供しています。アクティブトラックでは、バグ修正やセキュリティパッチに加えて、最新機能や性能を利用することができます。長期サポート（LTS）トラックを利用したソフトウェアは、サードパーティシステムとの良好な統合を維持することに重点を置くため、バグ修正とセキュリティパッチのみを提供して安定性を最大限に高めます。
- デバイス管理ツール：*AXIS Device Manager*および*AXIS Device Manager Extendは*、顧客が最新のセキュリティパッチやバグ修正でAxisデバイスソフトウェアを簡単に更新できるようにするツールです。

  Axisデバイスをローカルで効率的に設定および管理するために、AXIS Device Managerは、デバイス認証情報の管理、証明書の導入、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のセキュリティタスクのバッチ処理を有効にします。

  AXIS Device Manager Extendは、すべてのデバイスとサイトに関する情報を使いやすい単一のアプリケーションに集約したダッシュボードを提供します。デバイスソフトウェアのアップグレードが可能になると通知され、一括アップグレードやその他のタスクを大規模に実行できます。また、交換用製品に関する推奨も受けられます。こうしたアクティビティは完全に追跡可能であり、レポートまたは監査の目的ですべてのシステムデバイス情報をエクスポートすることができます。
- *Axisセキュリティ通知サービス*：Axisがサインアップを奨励しているこのサービスは、加入者にセキュリティインシデントや脆弱性をタイムリーに通知します。

4.3 認証と認可

不正アクセスを防止し、Axisデバイスの全般的なセキュリティを高めるために、Axisでは以下をサポートしています。

- 役割ベースのアクセスデバイス管理アクセス権限（管理者/オペレーター/閲覧者）と、AxisデバイスをIT標準の *Active Directory Federation Service*（ADFS）統合に接続することで、認証/認可を一元化することが可能です。（ADFSは、Windowsサーバーオペレーティングシステム上のユーザーにシングルサインオン（SSO）認証サービスを提供するためにMicrosoftによって開発されたソフトウェアコンポーネントです。ADFSは、組織の境界を越えてユーザーが単一のログイン認証情報を使用してWindowsサーバーオペレーティングシステム上のアプリケーションにアクセスすることを可能にします）
- *ゼロトラストネットワーキング*を容易にする技術。 AXIS OSの最新リリースでは、それらのテクノロジーがIEEE 802.1AR準拠のAxisデバイスIDを併せてIEEE 802.1Xを含み、IEEE 802.1Xネットワークへのデバイスの自動的でセキュアなオンボーディング、およびデータ通信の自動暗号化のためのIEEE 802.1AE（MACsec）を対象としています。

4.4 データの暗号化

機密情報が傍受されたり、権限のない第三者によってアクセスされたりするのを防ぐため、Axis製品では以下をサポートしています。

- すべてのデータ通信がTLS 1.2またはそれ以降の規格をサポートするHTTPS。AXIS Camera Stationビデオ管理ソフトウェアサーバーとクライアント間のビデオストリーム接続がAES-256で暗号化されていること。
- *IEEE 802.1AE（MACsec）*による自動データ通信暗号化。
- SRTP/RTSPSとも呼ばれるRTP経由のセキュアビデオストリーミング (AXIS OS 7.40以降）。SRTP/RTSPSは、セキュアなエンドツーエンドの暗号化転送方法を使用して、許可されたクライアントのみがAxisデバイスからビデオストリームを受信できる。
- *エッジストレージ暗号化*（SDカード）
- AXIS OS 10.10から開始された*エッジ録画のパスワード暗号化エクスポート*（SDカード、ネットワーク共有）。これにより、パスワード暗号化された録画をエクスポートできるようになり、エクスポートした録画を手作業で暗号化しなくても、機密性の高いビデオデータを安全に共有でき機能が追加された。

4.5 インシデントレポート

Axisでは、当社の製品やサービスで発見されたセキュリティインシデントや脆弱性のインシデントレポートを提供しています。

- Axisは、共通脆弱性識別子 (CVE) 採番機関です。すなわち、Axisが業界のベストプラクティスに従い、当社の製品やサービスにおいて発見された脆弱性を管理し、透明性をもって対応することで、顧客が晒されるリスクを最小限に抑えられることを意味します。Axisはまた、新たに発見された脆弱性にCVE番号を割り当てることができ、それらをWebサイト「*www.cve.org*」で報告します。Axisの*脆弱性管理ポリシー*はaxis.comで公開されています。
- Axisからのセキュリティ通知をご希望の場合は、誰でも*ここから*登録できます。
- AXIS OSの新しいバージョンにおいて、セキュリティパッチとバグ修正が提供されています。また、AXIS Companion、AXIS Camera Station、AXIS Device Manager、AXIS Device Manager Extend、およびサードパーティ製VMS（Milestone XProtect、Genetec Security Centerなど）でも、更新されたデバイスソフトウェアを利用できることが強調されています。
- Axisは、会社に関連するサイバー攻撃に関する透明性の確保に努めており、スウェーデンの関連当局が提供するガイドラインに従ってこうしたインシデントを報告します。

4.6 プライバシーへの配慮

Axisは、どの個人データが収集され（たとえば、My Axisのオンラインアカウントから）、どのように使用されるかを概説する*プライバシーポリシー*と通知をオンラインで公開しています。

Axisはまた、ISO/IEC 27001認証を取得した情報セキュリティ管理システムに関する*サイバーセキュリティのフレームワークとプラクティス*を公開しています。AxisのISO/IEC 27001認証の範囲は、社内のITインフラストラクチャーとサービスの開発と運用を対象とし

ています。ISO 27001は、効果的なリスク管理を通じて組織の情報を保護・管理する方法に関するガイダンスを提供する国際的に認められた規格です。

*ISO/IEC 27001*に準拠しているということは、Axisが国際的に認められたプロセスとベストプラクティスを使用して、顧客とパートナーにサービスとサポートを提供する内部情報インフラストラクチャーとシステムを良好に管理しているという意味です。

Axisはまた、ビデオや音声のキャプチャーに関して、監視におけるプライバシーの問題にも顧客が対処できるよう支援しています。ソリューションには以下が含まれます。

- Axisカメラの静的プライバシーマスキング、および*AXIS Live Privacy Shield*ソフトウェアアプリケーションによる動的プライバシーマスキング
- *AXIS People Counter*アプリケーションや*AXIS P8815-2 3D People Counter*のようなエッジベースのインテリジェント機能（統計的数値データのキャプチャーと保存のみで、個人を特定できる情報は処理されない）
- *サーマルカメラ*
- *レーダー製品*
- *AXIS Camera Station*のビデオ再編集ツールでは、対象外のオブジェクトやエリアにマスキングが可能
- Axisビデオ監視製品では*デフォルトで音声機能を無効化*

プライバシーソリューションの詳細については、 *axis.com/solutions/privacy-in-surveillance*をご覧ください。

4.7 サプライチェーンのセキュリティ

コンポーネントサプライヤーから顧客に至るサプライチェーンのセキュリティを保護することは、セキュリティの脆弱性が入り込む可能性を防ぐために必要なことです。

Axisはサイバーセキュリティに取り組む際に、製品*ライフサイクルアプローチ*を採用しています。当社は、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通じてだけでなく、流通や導入の段階、さらには保守や廃止の段階においても、リスクの軽減に取り組んでいます。

Axisがサプライチェーンセキュリティに取り組むいくつかの方法を以下に説明します。

- Axisは重要なコンポーネントを戦略的サプライヤーから直接調達しています。当社は製造パートナーと緊密に協力しています。生産工程を監視し、24時間年中無休でAxisとデータを共有することで、リアルタイムの分析と透明性が実現します。*Axisサプライチェーンセキュリティについてお読みください*。
- Axis Edge Vaultによる内蔵型のデバイスセキュリティは、以下の機能により、Axisデバイスの完全性を保護します。
  - **署名付きOS**：インストールしたAXIS OSがAxisの正規品であることを保証します。また、デバイスにインストールするための新しいAXIS OSも、Axisによる署名付きであることを確認します。
  - **セキュアブート**：オペレーティングシステムにAxis署名があることをデバイスがチェックできるようにします。不正なOSや改ざんされたOSを検出すると、起動プロセスが中止され、デバイスの動作が停止します。署名付きOS、セキュアブート、そ

してデバイスの工場出荷時設定へのリセットを組み合わせることで、デバイスの出荷中に行われる改造の試みに対する保護を提供します。

- **Axisデバイス IDは**IEEE 802.1ARに準拠しており、ネットワーク上でセキュアなデバイス識別とオンボーディングを可能にします。AxisデバイスIDは、デバイスのセキュアキーストア（セキュアエレメント、TPM、TEE）に保存されます。
- **暗号化ファイルシステム**は、システムインテグレーターから顧客への輸送中など、デバイスが使用されていない間に、ファイルシステムに保存されている顧客固有の設定や情報が抜き取られたり改ざんされたりしないように保護します。
- さらに、Axisは**署名付きビデオ**をサポートし、閲覧者はデバイスからエクスポートされたビデオが改ざんされているかどうかを検証できます。これは、捜査や起訴において特に重要です。詳しくは、*axis.com/solutions/edge-vault*をご覧ください。

- チェックサムはaxis.comからソフトウェアをダウンロードする際に提供されます。このチェックサムにより、ファイルの完全性を確認できます。
- ETSI認証：AXIS OS 11以降を搭載した150を超えるAxis製品は、*ETSI EN 303 645サイバーセキュリティ規格*の認証を受けています。ETSIはEuropean Telecommunications Standards Institute（欧州電気通信標準化機構）の略です。この要件には、安全なキーストレージといったハードウェアベースのセキュリティ機能、デフォルトでのHTTPS対応やデフォルトパスワードの排除といったデフォルトのセキュリティ機能のサポートなど、デバイス自体に関する要件が含まれます。別の側面として、デバイスセキュリティ更新のサポート期間の定義など、ライフサイクル管理に関する要件も含まれています。その他としては、ソフトウェア開発における脆弱性のリスクを軽減するための方法論、透明性の高い脆弱性管理ポリシーの策定、個人データの処理におけるベストプラクティスのサポートなどが挙げられます。こうした要件は、業界のベストプラクティスを考慮して策定されています。つまり、セキュリティに関して、ライフサイクル全体を通じて認定製品の最低限のベースラインレベルを維持することが目的なのです。この規格は、EUサイバーセキュリティレジリエンス法、EU無線機器指令、その他世界中の規格や法律と密接に連携しています。

4.8 トレーニングとガイダンス

Axisでは、スタッフ、パートナー、顧客にサイバーセキュリティのベストプラクティスに関する情報とトレーニングを提供しています。これらを以下に示します。

- 社内セキュリティ意識向上とトレーニング：Axisでは、組織に対するセキュリティの脅威を回避し、軽減するために、従業員を継続的に訓練するセキュリティ意識向上プログラムを開発しています。この意識向上トレーニングは、Axisの全人員に義務付けられています。個人の組織的な役割と責任に応じて、開発者とシステム所有者には追加のセキュリティトレーニングが提供されます。
- *Axis Academyトレーニング*顧客向けのトレーニングコースには、サイバーセキュリティのオンラインコースおよび*Axis approach to the topic*があります。
- オンラインで利用できる*強化ガイド*
  - *AXIS OS*
  - *AXIS Camera Station*
  - *Axisネットワークスイッチ*

- *AXIS OSセキュリティスキャナーガイド*：Axisでは、Axisデバイスのセキュリティスキャンを実行して、脆弱性や設定の不備による影響を受けていないか確認することを推奨しています。AXIS OSセキュリティスキャナーガイドでは、スキャナーからの特定の通知を解決する方法に関する推奨事項と、一般的な「誤検知」の概要について説明しています。
- *AXIS OSフォレンジックガイド*：このガイドは、Axisデバイスが設置されている周辺ネットワークやITインフラに対するサイバーセキュリティ攻撃が発生した場合に、Axisデバイスのフォレンジック分析を行う方に向けた技術的アドバイスを提供します。

Axisとサイバーセキュリティの詳細については、*Axisサイバーセキュリティポータル*をご覧ください。

T10210486/ja/M3.3/2406

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、 また業界のリーダーとして、Axisはビデオ監視、 アクセスコントロール、インターコム、音声システムなどの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 インテリジェントな分析アプリケーションによって強化され、高品質のトレーニングに支えられています。

Axisは50ヶ国以上に約4,000人の熱意にあふれた従業員を擁し、 世界中のテクノロジーおよび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年に設立され、本社は スウェーデンのルンドにあります。