Axisセキュリティ開発モデル

はじめに

Axisの安全な開発への取り組み

すべてのAxis開発チームは、Axisセキュリティ開発モデル（ASDM）を遵守することが義務付けられています。ASDMは、開発の開始から廃棄に至るまでのライフサイクル全体を通じて、セキュリティが組み込まれたソフトウェアを構築するためにAxisが使用するプロセスとツールを規定したフレームワークです。

ASDMの目的

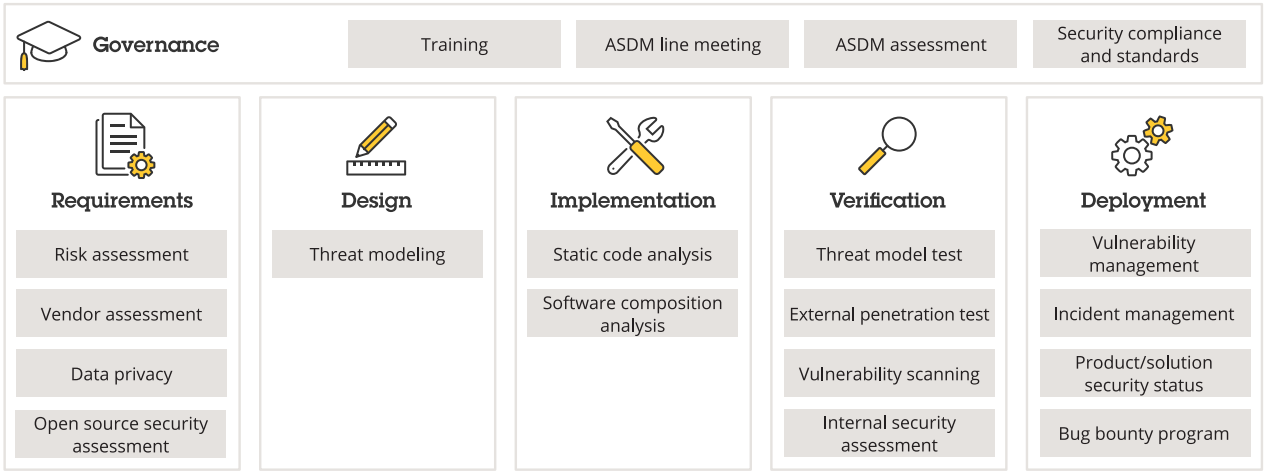
ASDMの取り組みを推進する主な目的は次の通りです。

- Axisソフトウェア開発活動にソフトウェアセキュリティを統合する。
- Axisの顧客のビジネスにおけるセキュリティ関連リスクを軽減する。
- 高まりつつある顧客やパートナーのセキュリティ意識に対応する。
- 問題の早期発見と解決により、コスト削減の可能性を創出する。

ASDMの対象は、Axisの製品とソリューションに含まれるソフトウェアです。

ASDMの概要

ASDMは、開発ライフサイクルの各段階にわたる複数の活動で構成されています。セキュリティ活動は総称してASDMと呼ばれます。最新バージョンは2024.02で、詳細は以下の通りです。



ソフトウェアセキュリティグループ (SSG) は、ASDMを統括し、ツールボックスを継続的に発展させる責任を担います。開発組織全体でASDMの成熟度を高め、活動を実施するためのロードマップと展開プランが用意されています。ロードマップと展開プランはどちらもSSGが管理しますが、開発ライフサイクルに関連する活動などの実際の実施責任は、開発チームに委ねられます。

チームにASDMとその実施の主導権を持たせるということは、マネージャーが活動の導入に責任を持つことを意味します。SSGが中央集約型のASDM展開プランをプッシュする体制から、プル型のアプローチへと移行し、マネージャーが管理する形になりました。

ソフトウェアセキュリティグループ (SSG)

SSGは、安全な開発プラクティスを促進し、組織内でセキュリティ文化を育成する役割を担います。このグループは、ASDMの開発とメンテナンスを担当し、開発中にセキュリティが組み込まれるようにサテライトとチームを指導するセキュリティコーチで構成されています。 SSGは、セキュリティ関連の問題について、開発組織に対する社内での主要な窓口となる組織です。

SSGを配置する理由は次の通りです。

- Axisの製品およびソリューションのセキュリティ向上に向けた体系的なアプローチを確立する
- Axisブランドのすべての製品およびソリューションでASDMが動作することを確認する
- 開発チーム間でASDMの運用を調整する
- ASDMのステータスを明確にし、透明性を確保する
- ベストプラクティスを含む知識の共有を促進する

サテライト

サテライトは開発組織のメンバーであり、その時間の一部をソフトウェアのセキュリティ面に関する作業の推進に充てます。サテライトを配置する理由は次の通りです。

- 大規模な中央SSGを構築することなくASDMを拡張する
- 開発チームに近い場所でASDMサポートを提供する
- ベストプラクティスを含む知識の共有を促進する

サテライトは、開発チームのサブセットにおいて、新しい活動の実施やASDMの維持管理をサポートします。

役割と責任

ASDMを構成する主要なエンティティと役割がいくつかあります。下の表は、ASDMに関連する役割や責任をまとめたものです。

役割/エンティティ	の一員	責任	コメント
セキュリティコーチ	SSG	ASDMを管理し、発展させます。サテライトやチームにASDMの使い方を指導し、マネージャーにはASDMのステータスを活用して組織を推進する方法を指導します。	100% SSGに従事
衛星	開発ライン	SSGによるASDM導入の支援、チームの指導、トレーニングの実施に加え、チームがSSGから独立して日常業務の一環としてツールボックスを継続的に使用できるようサポートします。	ソフトウェアセキュリティに関心を持ち、熱意を持って取り組むことのできる開発者、アーキテクト、テスター、およびそれに類する役割を担う人々。サテライトは、少なくとも20%の時間をASDM関連の業務に割り当てます。 サテライトの総数を制限するためには、複数のチームによる横断的な責任が求められます。
管理者	開発ライン	ASDMプラクティスの実施に必要なリソースを確保します。ASDMの進捗とカバレッジの追跡および報告を推進します。チームがトレーニングを受けており、サテライトをサポートできる体制が整っていることを確認します。	セキュリティは、ソフトウェアがセキュリティを考慮して開発されるようにするために、マネージャーが優先すべき事項です。 「マネージャー」とは、ラインマネージャーとディレクターの両方を指します。
開発チーム	開発ライン	サテライトとSSGのサポートを得て、ASDMのツールを使用します。	開発チームは、開発者やテスターなど、何らかの形でソフトウェアの開発に携わる人々で構成されます。テスターは、開発者や開発組織から独立しています。

製品セキュリティチーム	製品管理	インシデントや脆弱性管理に関する外部とのコミュニケーションに対応し、セキュリティ機能に関する業務を推進します。	製品管理は、製品オーナーと製品スペシャリストで構成されます。
AXIS OS R&Dステアリンググループおよび CTO	R&D管理	セキュリティ戦略を決定し、SSGのメインステークホルダーとして活動します。	SSGは、ステータスとASDMロードマップを定期的にAXIS OS R&Dステアリンググループ とCTOに報告します。

ASDM活動の展開

開発チームへのASDM活動の展開は、以下のように段階的に行われます。

1. チームはトレーニングを受けて新しい活動に取り組みます。
2. SSGはチームと協力し、チームが管理するシステムの特定の部分に対して、リスクアセスメントや脅威モデリングなどの活動を実施します。
3. チームのワークフローへのツールボックスの統合に関する次の活動は、SSGの直接的な関与なしに独立して作業する準備ができた時点で、マネージャー、チーム、サテライトに引き継がれます。

活動の変更や追加を含むASDMの新しいバージョンがリリースされた場合は、この展開が繰り返されます。SSGがチームと関わる時間は、活動の内容やコードの複雑さに大きく左右されます。チームへの引き継ぎを成功させるための重要な要素は、チームと共にASDMの作業を継続できるサテライトの存在です。SSGは、活動の展開と並行して、サテライトの育成と配置を推進します。

以下の図は、展開方法の概要を示しています。



SSGにおける引き継ぎの「完了」の定義は以下の通りです。

- トレーニングが完了した
- サテライトの割り当てが完了した
- チームがASDMの活動を実施する準備ができている
- ラインマネージャー、QAマネージャー、サテライト、SSGメンバーとの定期的なASDMステータス会議が設けられた。

SSGは、各チームからの入力を基に、上級管理職向けのステータスレポートを作成します。

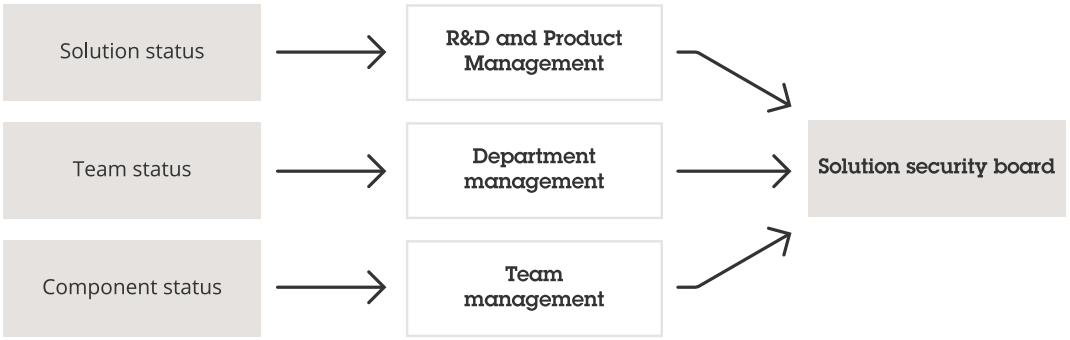
ASDMガバナンス

ASDMステータス構造

ASDMのステータス構造には2つの視点があります。1つはチーム中心で、チームが作成したコンポーネントに焦点を当て、チームと部門の構造を模倣したもの。もう1つはソリューション中心で、当社が市場に提供するソリューションに焦点を当てたものです。この2つの視点は、モデルを継続させ、セキュリティ業務が確実に実施されるようにするために不可欠です。

組織内のセキュリティ体制を検証するために、この2つの視点は、さまざまなR&Dマネージャーで構成されるソリューションセキュリティ委員会に集約されます。セキュリティステータスが委員会に報告されるようにすることは、管理者の責任です。

以下の図は、ASDMのステータス構造を示しています。



コンポーネントステータス

プラットフォーム内のLinuxデーモン、サーバーソフトウェア、クラウドサービスなど、あらゆる種類のアーキテクチャエンティティを網羅する必要があるため、コンポーネントの定義は広範に設定されています。各チームは、新しいコンポーネントとレガシーコンポーネントの両方を含め、すべての高リスクなコンポーネントを明確に把握する必要があります。ソリューションについては、すべての構成要素のセキュリティステータスを把握することが重要です。

まず、コンポーネントのセキュリティ状況が既知か未知かを判断するために、そのコンポーネントがセキュリティ分析を受けているかどうかを把握する必要があります。これを確実にするために、各コンポーネントは、セキュリティ分析の範囲に応じて、完了、未完了、進行中のいずれかに分類されます。

コンポーネントのセキュリティ品質を把握するために使用するメトリクスは、そのコンポーネントに紐づけられたバックログのセキュリティ作業項目に基づいています。これには、未実装の対策、未実行のテストケース、未対応のセキュリティバグなどが含まれます。

コンポーネントカバレッジは、ASDMラインミーティングの活動の一部です。

チームステータス

チームのステータスには、ASDMの熟練度評価、セキュリティ分析活動に関連するメトリクス、そして担当するコンポーネントのセキュリティステータスの集計が含まれます。これらはすべてASDMラインミーティングで議論されます。

チームの成熟度は、チームが実施している活動に関連しています。ASDMを使い始めたばかりのチームでは実施する活動が少ないと予想されますが、セキュリティ業務に熟練したチームは、より多くの活動を実施し、モデルにフィードバックを提供すると予想されます。

ソリューションステータス

ソリューションステータスは、ソリューションを構成する各コンポーネントのセキュリティステータスを一元的に示します。

ソリューションステータスの最初の部分は、コンポーネントの分析の適用範囲です。これは、ソリューションオーナーが、ソリューションのセキュリティステータスを把握できているか、それとも不明であるかを理解するのに役立ちます。また、一つの視点として、見落とされている部分の特定にも役立ちます。

ソリューションステータスの残りの部分には、ソリューションのセキュリティ品質を評価するためのメトリクスが含まれています。これは、ソリューション内のコンポーネントにリンクされているセキュリティ作業項目を調べることによって行われます。

セキュリティステータスの重要な側面は、ソリューションオーナーによって定義されるバグ基準(バグバー) です。ソリューションオーナーは、自身のソリューションに適したセキュリティレベルを定める必要があります。例えば、これはソリューションが市場にリリースされる際に、未解決のクリティカルまたは高深刻度の作業項目が残っていないことを意味します。

これは、ASDMの製品／ソリューションセキュリティステータスの活動でカバーされています。

ASDM活動

トレーニング

Axisでソフトウェア開発に携わるすべての人が、その業務を遂行できるようにする必要があります。そのための一つの重要な側面は、必要な知識を身に付けることです。トレーニングの目的は、セキュリティの重要性を強調し、分散型オーナーシップを促進するとともに、Axisでのソフトウェア開発に伴うASDM活動や責任について理解を深めてもらうことです。

これらのトレーニングは、デジタル形式のコースからディスカッションベースのセッションまで多岐にわたります。

ASDMラインミーティング

定期的にフォローアップ会議を行う目的は、継続的な改善プロセスに不可欠な、フィードバックループを確保することです。これらの会議では、マネージャー、サテライト、およびSSGが集まり、以下のトピックについて話し合います。

- ASDMを扱うための組織としての能力
- ASDM活動の遂行
- コンポーネントのセキュリティステータス

ASDMアセスメント

ASDMモデルとその各活動の有効性は、定期的に評価されます。目的は、活動、手法、ツールにおけるギャップを特定することです。この評価は、外部侵入テストやバグバウンティプログラム (脆弱性報奨金制度) による外部ソースからのフィードバックだけでなく、社内での振り返り (レトロスペクティブ) からのフィードバックにも基づいています。

セキュリティのコンプライアンスと標準

目標は、開発チームがASDMに従うだけで済むようにすることです。この方針に従い、SSGはセキュリティ関連のさまざまな標準を定期的に評価し、それらをASDMにマッピングします。これは、ASDMの継続的な評価と改善に向けた多数のインプットの1つとして活用されます。

リスクアセスメント

ASDMの主要な目的は、開発の遅延を避けるために、チーム内のセキュリティ活動の効率を最適化することです。リスクアセスメントは、コンテクスト要因や、新しい、または古いコードに関連する固有のリスクに基づき、セキュリティ対策の適切なレベルを判断するための基本的な手法です。

リスクアセスメントでは、新製品や既存製品に追加・変更された機能によって、リスクの露出が増加するかどうかを判断します。これには、データプライバシーの観点やコンプライアンス要件も含まれます。リスクに影響を与える変更の例としては、新しいAPIの導入、承認要件の変更、新しいミドルウェアの追加などがあります。

ベンダーアセスメント

AxisがAxisブランドの製品で使用する目的でベンダーからコード (またはコードを含む製品) を購入する場合、ベンダーがセキュリティ活動をどのように実施しているかを評価する必要があります。 ベンダーアセスメントは、ベンダーの既存のセキュリティ慣行を理解し、改善点を特定するとともに、開発プロセスへのセキュリティ活動の統合を推進するためのツールとして機能します。

以下は、Axisがサードパーティ製ソフトウェアのサプライヤーを評価する際に考慮する事項です。

- サードパーティのコードに脆弱性があり、それが悪用された場合のAxisブランドへの影響
- 開発環境／ITセキュリティ

- 安全なソフトウェア開発活動
- 脆弱性およびインシデント管理

データプライバシー

信頼はAxisにとって重要な重点分野であり、当社の製品、ソリューション、サービスによって収集された個人データを取り扱う際には、ベストプラクティスに従うことが不可欠です。

データプライバシーに関するAxisの取り組みの範囲は、次のことを実現できるように定義されています。

- 法的義務を履行する
- 契約上の義務を履行する
- 顧客が義務を履行できるようサポートする

当社では、**データプライバシー**に関する活動を、次の2つのサブ活動に分けています。

- データプライバシーの評価
  - **リスクアセスメント**の際に実施する
  - データプライバシーの分析が必要かどうかを判断する
- データプライバシーの分析
  - 必要に応じて、**脅威モデリング**の際に実施する
  - 個人データと個人データに対する脅威を特定する
  - プライバシー要件を明確にする

オープンソースのセキュリティ評価

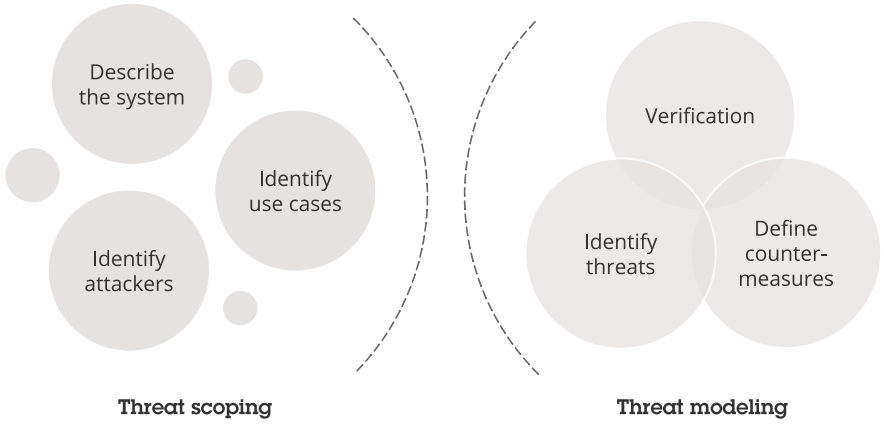
オープンソースセキュリティ評価とは、オープンソースプロジェクトがセキュリティ活動をどのように実施しているかを評価するとともに、プロジェクトに関連する潜在的なリスクを軽減するための戦略を策定することを指します。 サードパーティ製ソフトウェアのリスクは、それに依存するアプリケーションやシステムに直接的な影響を与える可能性があります。

以下は、Axisがオープンソースのソフトウェアコンポーネントを使用する前に評価する際に考慮する事項です。

- 貢献者
- 更新の頻度
- 脆弱性の管理

脅威モデリング

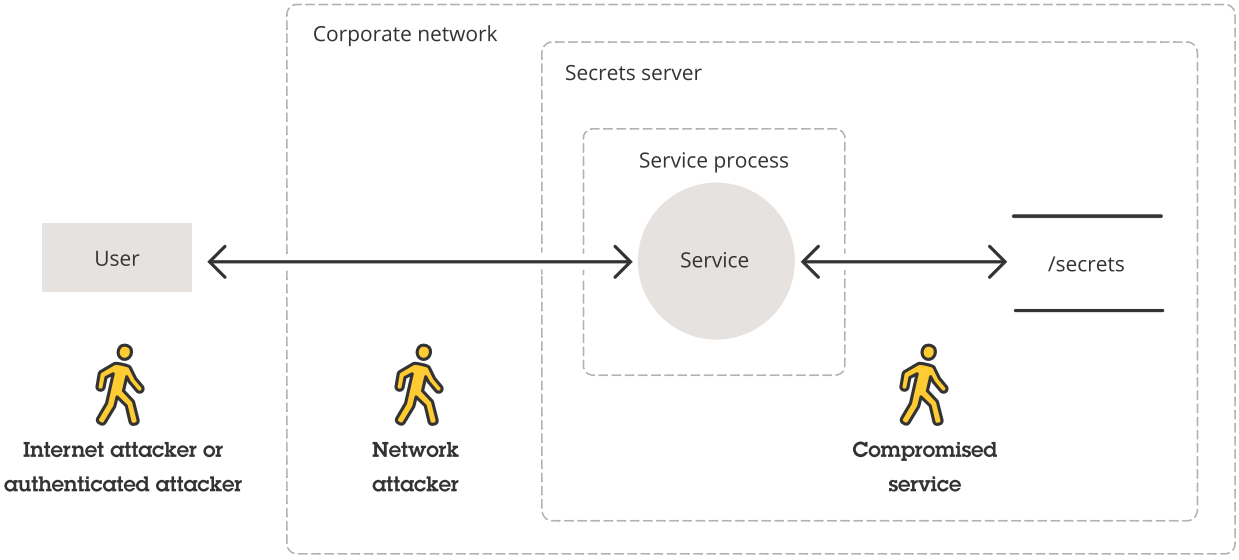
脅威モデリングは、開発プロセスの初期段階で脅威を特定し、対策を定義し、検証計画を立てるための体系的なアプローチです。 ただし、脅威を特定する前に、脅威モデルの対象範囲を決定する必要があります。範囲を明確にする方法の一つは、考慮すべき攻撃者を記述することです。このアプローチにより、分析に含めるべき高レベルのアタックサーフェス（攻撃対象領域）を特定することもできます。



脅威の範囲設定の際の焦点は、システムの高レベルな説明を使用して、対処すべき攻撃者を特定し、分類することにあります。脅威モデルの作成時に使用される、より詳細なユースケースの記述との関連付けがしやすくなるため、記述はデータフロー図 (DFD) として視覚化することが推奨されます。

これは、特定したすべての攻撃者を考慮しなければならないという意味ではありません。単に、脅威モデルで対処する攻撃者について、明確かつ一貫性があることを意味します。基本的に、考慮する攻撃者によって、評価対象となるシステムのセキュリティレベルが決まります。

攻撃者の記述には、攻撃者の能力や動機は含まれていないことに注意してください。当社では、脅威モデルを可能な限り簡素化し、効率化するために、このアプローチを選択しました。



脅威モデリングには、チームが適宜繰り返し実施することのできる、次の3つのステップがあります。

1. DFDのセットを使用してシステムを記述する
2. DFDを使用して脅威を特定し、Abuseケース形式で記述する
3. 脅威に対する対策を定義し、その対策が効果的かどうかを検証する

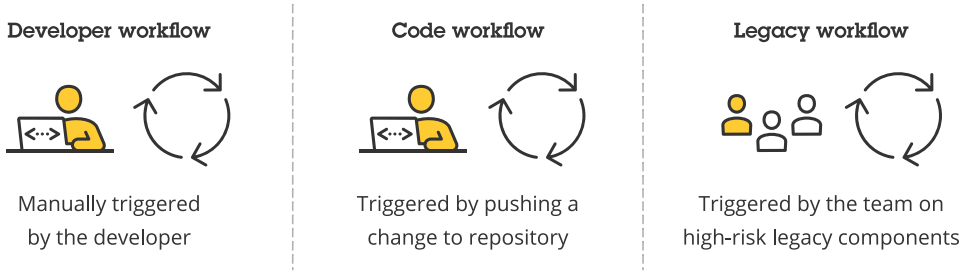
脅威モデリング活動の結果として、優先順位付けされた脅威と対策を含む脅威モデルが作成されます。対策に必要な開発作業は、対策の実装と検証の両方のチケットを作成することで管理されます。チームは脅威モデルをレビューにかけることもできます。

静的コード解析

静的コード解析は、一部のセキュリティバグクラスを自動的に検出し、手動によるコードレビューの作業負荷を軽減します。

ASDMでは、チームは静的コード解析を次の3つの方法で使用することができます。

- 開発者ワークフロー: 開発者が作業中のコードを分析する
- コードワークフロー: 開発者がコードレビューシステムでフィードバックを受け取る
- レガシーワークフロー: チームが高リスクのレガシーコンポーネントを分析する



ソフトウェアコンポジション解析

ソフトウェア構成分析は、ソフトウェアシステム内のオープンソースコンポーネントを特定し、これらのコンポーネントに関連する既知のセキュリティ脆弱性を検出するための継続的なプロセスを提供し、プロアクティブなリスク軽減を実現します。 信頼と透明性を促進するためには、使用されているコンポーネントとそれに関連する脆弱性について、オープンで透明性のあるコミュニケーションが不可欠です。すべてのAxisソフトウェアには、ソフトウェア部品表が付属しています。

脅威モデルテスト

脅威モデルに基づいてテストを作成するには、具体的なテストケースを作成し、対策の有効性を検証するとともに、潜在的な攻撃に耐えるシステムの能力を評価する必要があります。 対策の検証の重要性を強調するため、脅威モデルテストは脅威モデリングと組み合わせて行われますが、独立したアクティビティとして扱われます。

外部侵入テスト

場合によっては、Axisのハードウェア製品やソフトウェア製品に対してサードパーティによる侵入テストが実施されます。これらのテストを実施する主な目的は、特定の時点および特定の範囲におけるプラットフォームのセキュリティに関する洞察と保証を提供することです。

ASDMの主な目標の1つは透明性であり、当社ではお客様に当社製品に対する外部侵入テストの実施を推奨しています。テストに対する適切なパラメーターの設定や結果の解釈については、協力を惜しまず対応いたします。

外部侵入テストで発見されたすべての脆弱性にはCVE IDが割り当てられ、公開されます。

脆弱性スキャン

定期的な脆弱性スキャンにより、開発チームは製品が一般にリリースされる前にソフトウェアの脆弱性を特定し、パッチを適用することで、顧客が製品やサービスを展開する際のリスクを軽減することができます。スキャンは、オープンソースと市販の脆弱性スキャンパッケージの両方を使用して、各リリースの前 (ハードウェア、ソフトウェア)、または実行中のスケジュールに従って (サービス) 実行されます。

スキャンの結果は、バグ追跡プラットフォームでチケットを生成するために使用され、開発チームによる優先順位付けのために、明確なタグが付けられます。すべての脆弱性スキャンとチケットは、トレーサビリティおよび監査の目的で一元的に保存されます。

クリティカルな脆弱性は、リリース前に解決するか、または特別なサービスリリースで他の重大ではない脆弱性とともに解決し、ソフトウェアのリリースサイクルに合わせて追跡および解決する必要があります。脆弱性の評価方法と管理方法について詳しくは、を参照してください。

内部セキュリティ評価

内部セキュリティ評価の目的は、各チームに対してセキュリティ業務に関するフィードバックを提供し、特定の取り組みを通じてセキュリティに関する知識を広めることです。これは、通常チーム内で実施される、より詳細なセキュリティテストです。この活動はチーム単独で実施するのではなく、評価対象のコンポーネントやシステムに対する別の視点を得るため、チーム外の人物とともに実施されます。

内部セキュリティ評価の結果は、以下の活動へのインプットとして利用されます。

- 評価対象のコンポーネントやシステムのセキュリティ水準を向上させる
- チームのASDM活動の有効性に関するフィードバックを提供する
- ASDMの改善の可能性についてSSGにフィードバックを提供する
- 内部セキュリティ評価の手法に関するフィードバックを提供する

脆弱性の管理

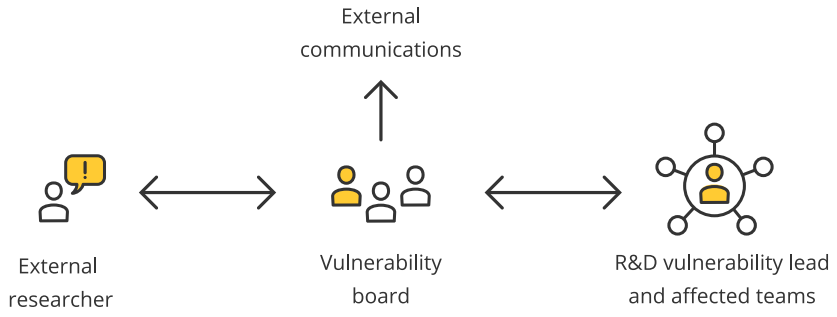
2021年以降、AxisはCVE採番機関 (CNA) として登録されているため、標準的なCVEレポートをMITREのデータベースに公開し、サードパーティ製の脆弱性スキャナーやその他のツールで利用できるようにすることが可能です。

脆弱性委員会は、外部の研究者によって発見された脆弱性に関するAxis社内の窓口です。発見された脆弱性の報告とその後の修復計画は、電子メールアドレス を通じて伝達されます。

脆弱性委員会の主な責任は、以下の点に基づいて、報告された脆弱性をビジネスの観点から分析し、優先順位を付けることです。

- SSGによって提供される技術的分類
- Axisデバイスが動作する環境におけるエンドユーザーの潜在的なリスク
- 代償となるセキュリティ対策 (パッチを適用しない代替的なリスク軽減策) の利用可能性

脆弱性委員会はCVE番号を登録し、報告者と協力してその脆弱性に共通脆弱性評価システム (CVSS) スコアを割り当てます。また、Axisのセキュリティ通知サービスやプレスリリース、ニュース記事を通じて、パートナーや顧客への外部コミュニケーションも促進しています。詳しくは、 *Axis脆弱性管理ポリシー*をご覧ください。



インシデント管理

インシデントとは、システムの弱点が悪用されている状態を指します。インシデントに対処し、管理するための組織的なアプローチをインシデント管理と呼びます。インシデント管理の目的は、単に解決策を提供するだけでなく、損害を最小限に抑え、復旧にかかる時間とコストを削減する方法で状況に対処することです。インシデント管理は、システム内にアクティブな攻撃者が侵入している可能性があるため、脆弱性管理とは異なります。

各チームにはインシデント管理のための独自のプレイブックがあります。 プレイブックの目的は、インシデントに迅速に対応し、解決するための手順を文書化することです。 プレイブックは、チームがインシデント発生時に意思決定を行えるようにするだけでなく、インシデント管理はインシデントそのものだけにとどまらないということを再認識させる役割も果たします。

製品/ソリューションセキュリティステータス

リリースのワークフローにセキュリティを組み込むには、プロジェクトマネージャー、製品マネージャー、QAマネージャー、開発マネージャーなど、リリースの意思決定に関わるすべての人が参加する必要があります。さらに、サテライトとSSGのメンバーは、リリースプロセスにおけるセキュリティ対策をサポートするため、アドバイザーとして参加することができます。

製品やソリューションのセキュリティステータスについて定期的に議論することで、次のことが可能になります。

- 当社の製品とソリューションのセキュリティについて、十分な情報に基づいた意思決定を行う
- 開発ラインとプロダクトマネージメントが、当社の製品とソリューションのセキュリティ体制に一致していることを確認する
- セキュリティステータスを完全かつ透明性をもって把握できるようにする

バグバウンティプログラム

バグバウンティプログラム (脆弱性報奨金制度) とは、独立系セキュリティ研究者にAxis製品の脆弱性を発見して報告するように奨励する、クラウドソーシングの仕組みを指します。この活動は、ASDMの取り組みについて外部からのフィードバックを求める成熟したチームによって活用されます。

バグバウンティプログラム (脆弱性報奨金制度)は、脆弱性を積極的に特定し、パッチを適用して公開するというAxisの取り組みを強化するものです。 バグバウンティプログラムを通じて発見されたすべての脆弱性にはCVE IDが割り当てられ、公開されます。

ASDM活動履歴

ASDMは一般的なベストプラクティスを基に作成されましたが、企業文化や製品ポートフォリオといった、*アクシスコミュニケーションズ固有のコンテキストに合わせて特別に調整されています*。したがって、Axisは、すでに確立されているセキュリティ開発ライフサイクルや他の業界の標準に従うのではなく、ASDMを当社の状況に合わせて調整し、最適化することができます。

オリジナルのASDMバージョン (2018.01) は、設計上、活動が少ない構成となっていました。Axisの開発チームがセキュリティ業務において成熟するにつれて、より多くの活動が追加されてきました。 一部の活動、特に焦点が限られている活動は発展しています。チームと組織が成熟するにつれて、SSGの活動も拡大しました。 一部の活動は、その内容をより明確に示すために名称が変更されています。

Axisでは、次のASDMバージョンを定義しています。

ASDMバージョン	活動内容
2018.01	意識向上トレーニング、役割別トレーニング、ステータスのフォローアップ、リスクアセスメント、サードパーティアセスメント、脅威モデリング、脅威モデルコードのレビュー、脅威モデルテスト、脆弱性管理を追加。
2018.11	静的コード解析を追加。
2019.05	データプライバシーとASDM評価を追加。
2019.12	ソフトウェアコンポジション解析を追加。
2020.04	外部侵入テストを追加。
2021.07	脆弱性スキャン、インシデント対応訓練、製品/ソリューションのセキュリティステータスを追加。
2022.02	ASDM監査を追加。
2022.05	オープンソースのセキュリティ評価を追加。
2022.10	バグバウンティプログラム (脆弱性報奨金制度) を追加。サードパーティアセスメントの名称をベンダーアセスメントに変更。
2023.02	セキュリティのコンプライアンスと標準を追加。脅威モデルの統合: コードレビューを脅威モデリングに統合。
2023.07	インシデント対応訓練をインシデント管理に拡張。
2023.08	ASDM監査を内部セキュリティ評価に拡張。外部侵入テストの名称をペンテストからペネトレーションテストに変更。
2024.02	意識向上トレーニングと役割別トレーニングをトレーニングに統合。ステータスフォローアップの名称をASDMラインミーティングに変更。