セキュア開発ライフサイクル

シスコ製品の強化

シスコ セキュア開発ライフサイクル(SDL)は、シスコ製品のレジリエンシーと信頼性を高めるために設計された、反復可能かつ測定可能なプロセスです。開発ライフサイクル中に導入されたツール、プロセス、営業活動やトレーニングの組み合わせにより、多層防御を促進し、製品のレジリエンシーに対する包括的なアプローチが可能になり、セキュリティアウェアネスの文化を確立します。

シスコの SDL は、業界トップクラスの事例と技術を適用し、フィールドで検出される製品のセキュリティインシデントが少ない Trustworthy ソリューションを構築します。

シスコの SDL は、次のような複合的な要素を調べることでさらにその成り立ちが明確になります。

- 製品のセキュリティ要件
- サードパーティのセキュリティ
- セキュア設計
- セキュアなコーディング
- セキュアな分析
- 脆弱性テスト

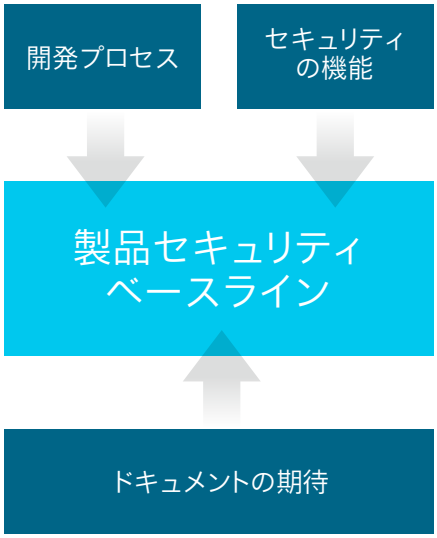
製品のセキュリティ要件

製品セキュリティ要件では、シスコ製品の内部および市場ベースの標準を定義します。要件は、既知のリスク、お客様の期待、業界のベストプラクティスに基づいて内部および外部のソースから構成されます。製品は、2 種類の製品のセキュリティ要件に対応する必要があります。

- **シスコの内部要件:** シスコの製品セキュリティベースライン(PSB:Product Security Baseline)によって定義される
- **市場ベースの要件:** 製品が展開される業界または場所によって示される

シスコの内部要件

シスコの PSB は、シスコ製品ポートフォリオのセキュリティ関連の機能、開発プロセス、ドキュメントの期待を定義する要件の主体です。PSB は、クレデンシャル、キー管理、暗号化標準、スプーフィング防止機能、整合性と耐タンパー性、およびセッション/データ/ストリーム管理などの重要なセキュリティコンポーネントに重点を置いています。レジリエンシーと堅牢性、機密データの廃棄、ロギングに関するガイダンスも PSB に示されています。この重要な要件は、進化する脅威に対する固有の保護の構築を目的として、新しい技術と標準を組み込むために継続的に強化されます。



市場ベースの要件

金融、政府/自治体、医療のような市場および業界は、多くの場合、シスコのお客様にセキュリティ要件を追加しています。これらの要件は PSB によって示されたものを超える場合がありますが、シスコは業界の要求を満たすか、または上回るように努めています。
要求される製品の認定には次のものが含まれます。

- コモンクライテリア認定
- 暗号化機能を含む製品の暗号化の検証
- IPv6 認定
- 国防総省(DoD)の統合機能認定製品リスト
- NERC-CIP(North American Electric Reliability Corporation - Critical Infrastructure Protection)

サードパーティのセキュリティ

一般的な業界では、商用とオープンソースのサードパーティ製ソフトウェアを両方とも製品に組み込むのが普通です。そのため、サードパーティの脆弱性が発見された場合、製品とお客様は影響を受ける可能性があります。その影響を最小限に抑えるために、シスコは次のように統合ツールを使用して、サードパーティ製ソフトウェアの潜在的なセキュリティ脅威を可視化します。

知的財産の中央リポジトリ: シスコは、一元的に管理されるリポジトリを通じてサードパーティ製ソフトウェアを使用し、製品を内部的に追跡します。この単一の参照ポイントでは、社外に配布されるサードパーティコードに関連付けられているメタデータのエントリが必要であり、脆弱性が見つかった場合は、影響を受けたすべてのシスコ製品を迅速に特定できます。

サードパーティの脆弱性に対する正確性と迅速な対応を促進するツール:

- **サードパーティ製ソフトウェアの脅威および脆弱性の通知:** シスコは、継続的に更新される既知のサードパーティ製ソフトウェアの脅威および脆弱性のリストから製品チームに自動的にアラートを送信し、迅速な調査と脅威および脆弱性の軽減を可能にします。
- **スキャンと分析:** シスコは、サードパーティのリポジトリの正確性と完全性を向上するために、ソースコードとイメージを検査するツールを採用しています。

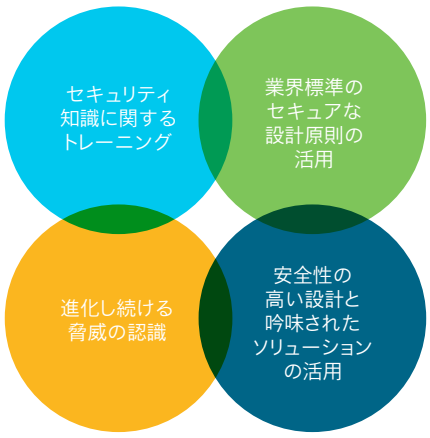
セキュア設計

製品セキュリティ要件では、シスコ製品の内部および市場ベースの標準を定義します。要件は、既知のリスク、お客様の期待、業界のベストプラクティスに基づいて内部および外部のソースから構成されます。製品は、2 種類の製品のセキュリティ要件に対応する必要があります。

- セキュリティを念頭に置いた設計
- 脅威モデリングによる設計上のセキュリティの検証

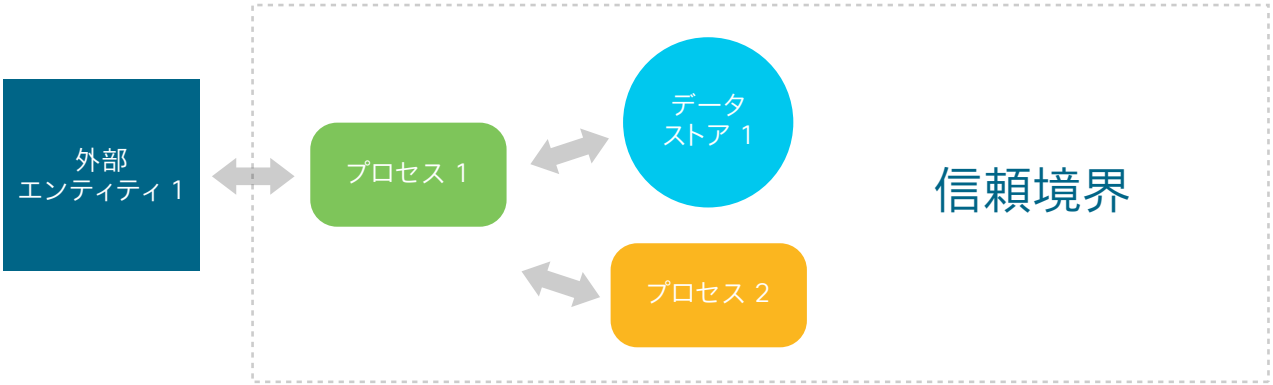
セキュリティを念頭に置いた設計

セキュア設計では、個人向けおよびプロフェッショナル向けの継続的な改善に取り組む必要があります。社内のセキュリティ トレーニング プログラムにより、すべての従業員のセキュリティ認識を強化し、開発チームとテストチームには詳細なセキュリティ学習を奨励します。進化し続ける脅威を認識し、業界標準の原則と安全性の高い吟味されたソリューションを活用することで、シスコはよりセキュアな製品の設計と作成に努めています。



脅威モデリングによる設計上のセキュリティの検証

脅威モデリングは組織的で反復可能なプロセスであり、システムのセキュリティリスクの把握と優先順位付けを目的として設計されました。脅威をモデル化する際に、シスコのエンジニアはシステムを通じてデータのフローを追跡し、データが侵害される可能性のある信頼境界と変曲点を特定します。潜在的な脆弱性および脅威が特定されると、リスクを最小限に抑えるための緩和策を実施できます。シスコの脅威モデリングツールは、データフローと信頼境界の開発者向けの図に基づいて該当する脅威を公開することで、プロセスを促進します。



セキュアコーディング

セキュアコーディング標準

シスコのコーディング標準は、プログラマがプロジェクトと組織の要件によって定められた一連の統一ルールおよびガイドラインに従うことを促進します。ベテランの開発者は、コーディングと実装のエラーが潜在的なセキュリティの脆弱性を引き起こす可能性があることを把握しています。この知識は経験とトレーニングから得られますが、シスコのすべての開発者は、脅威に強いコードにするためのベストプラクティスに従う必要があります。セキュリティトレーニングにより、開発者はセキュアなコーディングガイドラインとベストプラクティスを学ぶことができます。

共通のセキュリティモジュール

セキュアなコーディングのベストプラクティスを補完するために、シスコは、吟味された共通のセキュリティモジュールを増やし、それを活用しています。シスコが管理するライブラリは、セキュリティの問題を減らすように設計されており、エンジニアが自信をもってセキュリティ機能を導入できるようにします。CiscoSafeC、CiscoSSL、およびその他のライブラリは、セキュア通信、コーディング、情報の保存に重点を置いています。

静的分析

シスコの SDL は、静的分析(SA)ツールの主要なセキュリティチェッカーを特定し、C および Java ソースコードの両方でソースコードの脆弱性を検出します。内部分析、フィールドトライアル、限られたビジネスユニットにより、一連のチェッカーによる検証が行われ、セキュリティ問題の検出を最大化します。潜在的なバッファオーバーフロー、汚染された入力、整数オーバーフローが対象となり、誤検出が最小化されます。シスコの開発チームは、セキュリティチェックを有効にした状態で静的分析を実行し、生成された警告を確認して優先度の高い問題を修正します。

脆弱性テスト

脆弱性テストにより、シスコ製品がセキュリティ欠陥のテストを受けるようにします。
分析は、最初に次の内容を特定することで製品ごとにカスタマイズされます。

- 製品に実装されているすべてのプロトコル
- デフォルトで有効になっているポートおよびサービス
- 一般的なお客様の設定に使用されるプロトコル、ポート、サービス

次に製品を評価し、最低 3 つのシスコ SDL の脆弱性テストで、プローブと攻撃に耐える能力を判定します。

- プロトコルの堅牢性テスト
- 一般的なオープンソースツールと商用のハッカーツールによる一般的な攻撃およびスキャン
- Web アプリケーションスキャン

効果的なセキュリティテスト計画を実行するには、複数のソースからさまざまなセキュリティツールを使用する必要があります。シスコのセキュリティテスト パッケージではこれらのすべてを簡単にインストールできる 1 つのツール群に統合しています。これにより、シスコのエンジニアは一貫性があり、反復可能な方法でセキュリティ欠陥をテストできます。また、製品チームは標準のセキュリティテストスイートを補完するカスタムテストを構築します。

侵入テストとセキュリティリスク評価を担当する熱心なエンジニアにより、潜在的なセキュリティの弱点をさらに特定し解決することもできます。テスト中に見つかった脆弱性は、製品チームによってトリアージされ、シスコの PSIRT(Product Security Incident Response Team)によって確認されます。