Securify Scan

3-SHAKE

10分でわかる！
セキュア開発の取り組み方

目次

01

セキュア開発の取り組みにおける課題

セキュア開発の取り組みにおける課題

Securify Scan

セキュア開発は、ソフトウェア開発のライフサイクルにおいて、
開発の前段階でセキュリティ対策を実施することで、リスクおよびコストを低減でき、
リリーススケジュールを妨げないようにするという考え方によって行われるかと思います。

▶ **このような考え方をシフトレフトと呼びます。**

しかし、実際の開発現場では上述のような流れで対応できているところはあまりなく、
その場しのぎでツールを導入する、
脆弱性診断に対応するといったことが多いのではないでしょうか。

そこでセキュア開発、特にプロダクトセキュリティにおいて、
どのように実施するのが理想かをフレームワークを紹介しながら解説していきます。

01

セキュア開発におけるフレームワークの紹介

セキュア開発におけるフレームワークの紹介

Securify Scan

セキュア開発（プロダクトセキュリティ）に関するフレームワークとして、以下の2つをご紹介します。
これらのフレームワークでは、セキュアなプロダクトを作るために
どのような開発ライフサイクルをとるべきかということが書かれています。

1 NISTが作成した「Secure Software Development Framework（SSDF）」

※NISTとは：National Institute of Standards and Technologyの略で「米国国立標準技術研究所」という機関

（出典：https://csrc.nist.gov/Projects/ssdf）

2 Microsoftが作成した「Microsoft セキュリティ開発ライフサイクル（Microsoft SDL）」

（出典：https://www.microsoft.com/en-us/securityengineering/sdl）

02

セキュア開発の前提となる考え方

セキュア開発の前提となる考え方

Securify Scan

フレームワークについてご紹介しましたが、前提となる考え方があるため、そちらを先に記載いたします。

SSDFには以下の記述があります。

> SSDF のプラクティス、タスク、および実装例は、考慮すべき出発点です。
> それらは、変更およびカスタマイズされ、時間とともに進化することを意図しています。
> **SSDF の意図は、従うべきチェックリストを作成することではなく、**
> **安全なソフトウェア開発プラクティスを採用し、**
> **ソフトウェア開発を継続的に改善するためのリスクベースのアプローチを計画および実装するための**
> **基礎を提供することです。**（筆者訳）

▶ **これは「リスクベース」のアプローチを実施すべきと読み取れます。**

では、リスクベースとは具体的にどのような内容でしょうか。

セキュア開発の前提となる考え方

Securify Scan

リスクベースのアプローチとは
発生し得るリスクを洗い出し、それに基づいてセキュリティ対策を実施することを指します

簡単な流れ

リスク特定	保有している情報資産を調査 情報資産に対する脅威・脆弱性の調査
リスク分析	リスク値の算出を元に優先度を決定
リスク評価	リスク水準と算出したリスクを比較
リスク対応	以下の対策を実施 リスク低減・リスク回避・リスク移転・リスク保有

セキュア開発の前提となる考え方

Securify Scan

ここまでで解説したように、まずはリスクを洗い出し、
リスクへの対策方法を決定するプロセスを踏むことが適切であると読み取れます。

逆に上記のようなリスクベースのアプローチではないケースは
冒頭の「その場しのぎ」の対応であると言えます。

前提となる考え方について触れたところで、
具体的な取り組みの流れについて、フレームワークに沿って簡単に解説をしていきます。

03

セキュア開発の取り組み方の流れ

セキュア開発の取り組み方の流れ(SSDF)

Securify Scan

SSDFでは以下の4つの取り組みをプラクティスとして提供しています。

組織の準備 (PO) :

組織の人員、プロセス、およびテクノロジが、組織レベルで、場合によっては個々の開発グループまたは
プロジェクトで、安全なソフトウェア開発を実行する準備が整っていることを確認します。

ソフトウェアの保護 (PS) :

ソフトウェアのすべてのコンポーネントを改ざんや不正アクセスから保護します。

安全なソフトウェアを作成する(PW):

リリースにおけるセキュリティの脆弱性が最小限に抑えられた、十分に保護されたソフトウェアを作成します。

脆弱性への対応 (RV) :

ソフトウェア リリースに残っている脆弱性を特定し、それらの脆弱性に対処するために適切に対応し、
同様の脆弱性が今後発生するのを防ぎます。

セキュア開発の取り組み方の流れ(SSDF)

Securify Scan

各プラクティスは、次の要素で定義され、具体化されています。

実践:

実践の名前と一意の識別子、それに続く実践とは何か、なぜ有益なのかについての簡単な説明。

タスク:

プラクティスを実行するために必要なアクション。

概念的な実装例:

タスクの実装を支援するために使用できるツール、プロセス、またはその他の方法の種類の概念的な例。
例や例の組み合わせは必須ではなく、記載されている例だけが実行可能なオプションではありません。

リファレンス:

確立された安全な開発プラクティスドキュメントへのポインターと、特定のタスクへのそのマッピング。

セキュア開発の取り組み方の流れ（SSDF）

Securify Scan

少し噛み砕いて説明します。

プラクティス	概要	実施内容
組織の準備 (PO)	セキュアな開発をするための 組織的な体制を構築する	・リスクの洗い出しと評価 ・セキュリティ要件の定義 ・役割と責任の定義 ・開発におけるツール導入支援
ソフトウェアの保護 (PS)	リリースしたソフトウェアを守る 仕組みを構築する	・デプロイしたソフトウェアの改ざんからの保護 ・デプロイモジュールのアーカイブ
安全なソフトウェアを作成する (PW)	脆弱性の混入を可能な限り防ぐ 開発をする	・セキュリティ要件を満たした設計 ・セキュアコーディング ・セキュリティソフトによる脆弱性特定と修正
脆弱性への対応 (RV)	脆弱性が発見された際に対応する	・脆弱性の継続的な把握と確認 ・脆弱性の評価と修正

セキュア開発の取り組み方の流れ（Microsoft SDL）

Securify Scan

Microsoft SDLでは以下の12をプラクティスを順番に実施するべきということが記述されている

プラクティス　1：トレーニングを提供する

プラクティス　2：セキュリティ要件を定義する

プラクティス　3：指標とコンプライアンス レポートを定義する

プラクティス　4：脅威モデリングの実行

プラクティス　5：設計要件を確立する

プラクティス　6：暗号化標準の定義と使用

プラクティス　7：サードパーティ コンポーネントを使用するセキュリティリスクを管理する

プラクティス　8：承認されたツールを使用する

プラクティス　9：静的分析セキュリティ テスト (SAST) を実行する

プラクティス 10：動的分析セキュリティ テスト (DAST) を実行する

プラクティス 11：侵入テストを実行する

プラクティス 12：標準的なインシデント対応プロセスを確立する

セキュア開発の取り組み方の流れ（Microsoft SDL）

Securify Scan

各プラクティスの詳細は割愛しますが、SSDFと同様の流れとなっていると考えられます。
以下が各プラクティスを大まかに分類した内容になります。

教育・啓蒙：

セキュリティについて全員が基礎的な内容を理解する

要件定義：

1、セキュリティ品質の最低許容レベルを定義し、KPIを設定する

2、脅威分析をして、リスクを特定し、適切な対応方針を設定する

3、セキュリティを考慮した設計をする

セキュリティテスト：

SASTやDASTで、セキュリティテストを実施する

脆弱性対応：

インシデントが発生した際の対応計画を設定する

セキュア開発の取り組み方の流れ（まとめ）

Securify Scan

- いずれのフレームワークにおいても以下の共通点があります

  - プロダクトに対するセキュリティ要件を定義すること
  - 脅威分析をして、リスクベースアプローチをすること
  - 開発者に一定のセキュリティ知識が必要であること
  - セキュリティテストを実施すること

- これらのことから考えられることとして、「どんな情報資産」を「誰の」「どんな攻撃」から「どうやって守り担保する」かを検討することが重要であると読み取れます。

- 紹介したフレームワークを活用することで、「その場しのぎ」ではない、リスクベースアプローチによる本質的なセキュア開発を実施することが可能であると考えられます。

- 本紙で記載はできていないが、セキュリティテストについては自動化できる範囲は自動化することを推奨しています。

次ページで紹介する、**スリーシェイクが提供している「SecurifyScan」**を利用することで、SSDFの「十分に保護されたソフトウェアを作成する(PW)」やMicrosoftSDLの「プラクティス10 - 動的分析セキュリティテスト (DAST) を実行する」の一部を自動化が可能ですので、ぜひお試しください。

Securify Scan（セキュリファイ スキャン）とは

Securify Scan

Webアプリケーションの
継続的セキュリティを簡単に実現

Securify Scan

Securify Scan（セキュリファイスキャン）は自社のプロダクトに対して、**手軽に、何度でも**脆弱性診断の実施を可能にし、セキュリティレベルを可視化: DevSecOpsへの取り組みをサポートします。

▸ **まずは2週間の無料トライアルでお試しいただけます！**

Thank you.