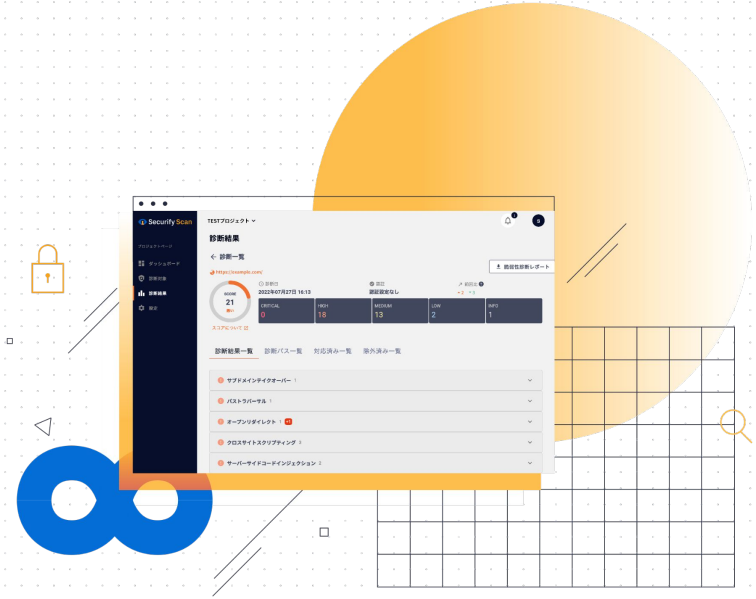
Securify Scan

DX時代における脆弱性診断のハイブリッド運用のススメ

～脆弱性診断サービスとツールを徹底比較～



3-SHAKE

目次

DX時代における開発とセキュリティについて

Securify Scan

デジタルトランスフォーメーション（DX）時代と呼ばれる今、社会は大きく変化しています。
企業間のビジネスも従来とは比較にならないほど迅速に取り交わされるようになり、ビジネスモデルも目まぐるしく変わっています。
その結果、ビジネスモデルに追随するかたちで開発にもスピードが求められ、アジャイル開発等を用いた高速開発を導入する企業が増えています。

特にWebアプリケーション脆弱性診断については以下の課題が顕在化しています。

- セキュリティエンジニアの慢性的な不足
- 手動診断のスピードが開発スピードに追いつかないことによるシステムリリース遅延
- Webアプリケーションの複雑化や案件増加に伴う診断コストの増加

上記の課題の解決策の一つとして、脆弱性診断の内製化が注目されています。

内製化とは、診断ツールを自社で運用することです。
内製化することで、開発と並走して診断を実施できるため、
診断コストやスケジュール調整工数の低減や開発スピードと並行した脆弱性対策の実施が可能となります。
しかし、脆弱性診断を内製化すれば、全てが解決するわけではありません。

ではどのようにすればいいのか、見ていきましょう。

Webアプリケーション脆弱性診断には、
大きく分けて「手動診断」と「ツール診断」の2つがあります。

手動診断

サイバーセキュリティの専門知識を持つ診断員（セキュリティエンジニア）が
診断対象のWebアプリケーションを手動で検査する方法です。
検査にはツールを用いますが、攻撃者の目線でどのように攻撃できるかを
セキュリティエンジニアの知見を活かして、診断します。
※お客様個別の検査観点を診断する高度な攻撃内容を想定しております

ツール診断

一般的によく見られる攻撃パターンによる影響確認や既知の脆弱性の確認を自動的に行い検査する方法です。
診断対象であるWebアプリケーションの設定等を自身で行う必要性はありますが、
診断自体はツールによって自動で診断します。

脆弱性診断の種類毎の特徴

Securify Scan

「手動診断」と「ツール診断」の一般的な特徴をまとめると以下になります。

	手動診断	ツール
メリット	● 知見を持ったセキュリティエンジニアによる精度の高い診断が可能 ● **仕様上のミスに起因する脆弱性**(ビジネスロジック診断)を検査できる ● **ページ、APIの依存関係が存在する**(事前もしくは事後条件が存在する)場合に発生する脆弱性を検査できる ● **権限**に起因する脆弱性を検査できる	● **定常的・複数回**の脆弱性診断を**低コスト**で実施することが可能。 ● **自社**で脆弱性診断を実施することが可能。
デメリット	● 特定の期間のみの脆弱性の把握になり、**常時ではない。** ● 診断準備・実施までの期間がかかる ● **値段が高額**	● 自身で設定する必要がある ● 手動診断と比較して、**検出精度が低い** ● 対応できない認証方式が多い ● 手動診断の左記メリットで挙げられた検査は対応していない
診断対象例	● ECサイト ● 複雑な構成や個人情報、機密情報を扱っているWebアプリケーション	● コーポレートサイトなどの静的なサイト ● シンプルな構成のWebアプリケーション

手動診断と脆弱性診断ツールの比較①

Securify Scan

「手動診断」と「脆弱性診断ツール※」の特徴をまとめると以下になります。

	手動診断	ツール
診断対象レイヤー	Webアプリケーション	Webアプリケーション ネットワーク（ポートスキャン）
静的なサイト ※コーポレートサイト等	○	○ ※手動診断と大きな差はない
SPA	○	○
対応認証方式	○	△ ※cookieを利用したForm認証、Basic認証、JWT認証に対応（順次拡大予定）

※脆弱性診断ツールは弊社提供 SaaS「SecurifyScan」の内容となります

手動診断と脆弱性診断ツール（SecurifyScan）の比較②

Securify Scan

「手動診断」と「脆弱性診断ツール※」の特徴をまとめると以下になります。

	手動診断	ツール
既知のCVE検査	○	○
SQLインジェクション等の 代表的な脆弱性の診断	○	○
権限診断	○	✕
仕様上のミスに 起因する診断	○	✕
ページ、API間の依存関係が 存在する診断	○	✕

※脆弱性診断ツールは弊社提供 SaaS「SecurifyScan」の内容となります

手動脆弱性診断の補足・注意点

Securify Scan

- 手動診断を行っても何も見つからないケースも存在する
- 発見された脆弱性の危険度のレビューや対応方法のサポートを受けられる
- 仕様上のミスに起因するような脆弱性（前ページのビジネスロジック診断）を検査できる

> **例**
> ECサイトのショッピングカートに1個1,000円の商品Aを2個、1個2,000円の商品Bを
> マイナス1個追加し、合計金額0円で決済ができてしまう

- ページ、APIの依存関係が存在する（事前もしくは事後条件が存在する）場合に発生する脆弱性を検査できる

> **例**
> ECサイト上で商品を一覧で表示する→ショッピングカートに追加する→対象商品を決済する
> 上記のように**一定のプロセスを踏まないとチェックできない内容**

- 権限周りの脆弱性を検査できる

> **例**
> ユーザAの権限しか参照できないページが別権限のユーザBも参照できてしまう

脆弱性診断ツールの補足・注意点

Securify Scan

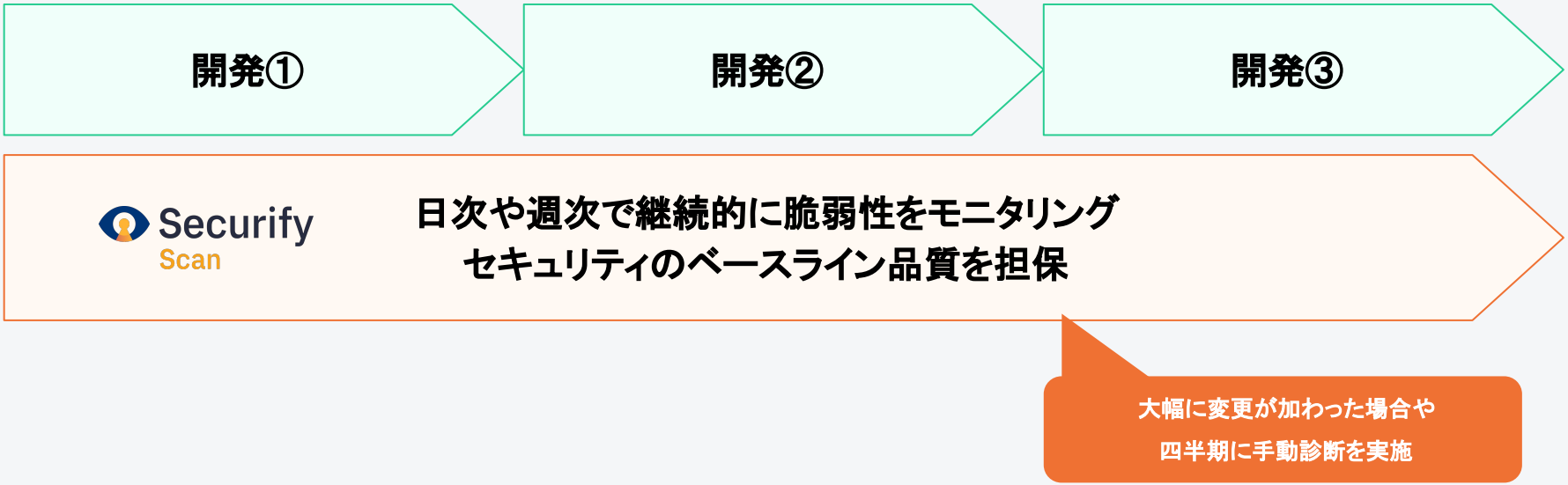
- SaaSでの提供であるため、導入が容易である
- 診断における複雑な設定は不要である
- 運用負荷が低い
- 検出された脆弱性に対する解説や修正方法を記載している
- 認証が必要なWebアプリケーションの診断の場合、診断中にセッション情報がexpireしてしまうと、診断が空振りになる可能性がある
- クローラによって診断対象を洗い出すため、深いページまでたどり着けない可能性がある
- 多要素認証等の複雑な認証方式に対応していない
- 診断対象に対して、パターン化された擬似的な攻撃リクエストを送信しており、場合によって発見された脆弱性が誤検知となることもある
- API単体の診断はできない（対応予定）

※脆弱性診断ツールは弊社提供 SaaS「SecurifyScan」の内容となります

推奨活用方法

Securify Scan

手動脆弱性診断も脆弱性診断ツールもそれぞれメリットとデメリットが存在し、
どちらか一方を実施すれば良いというものではありません。
手動脆弱性診断と脆弱性診断ツールを**ハイブリッドで利用すること**を推奨します。



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.