



脆弱性診断ツールは

どう選べばいい？

運用で失敗しないための
4つの比較ポイントと選定基準



本資料の目的

脆弱性診断の内製化を検討する上で、ツールの導入は欠かせません。

しかし、脆弱性診断ツールの導入をお考えのお客様の中には、

「どのような観点で比較したらよいのかわからない」

「何を重視して選ぶべきか迷っている」「そもそもツールごとの違いを把握することが難しい」

といったお悩みを抱えるケースも少なくありません。

また、社内にセキュリティ人材が不足している企業も多く、適切なツールを選定することは容易ではありません。

そこで本資料では、こうしたお悩みを解決するため、ツール導入時に検討すべき4つの視点や、

コストを抑えつつ診断業務を効率化するためのツール選定のポイントをまとめました。

どのツールを選べばよいかお悩みの方、脆弱性診断の内製化を目指している方は、ぜひご一読ください。



脆弱性診断ツールを検討するにあたり、 こんなお悩みはありませんか？

やっぱり無料のものから
使ってみるべき？

何を一番重視して
選べばいい？

どれが自分たちの
ニーズを満たしている？

どういう観点で
比較・評価すればいい？

正直、どれも同じに
見える…

なぜ脆弱性診断ツールの選定は難しいの？



多様な
診断ツールが存在

特徴が異なる多様な
ツールがあるものの、
専門分野なので、
違いの把握が難しい



自社のニーズとの
合致が重要

他社にとっての正解が
自社にとっての正解とは
言い切れない面も



運用を見据えた
選定が必要

せっかく導入しても、
日々の運用に負荷が
かかるとかえって
リスクに

脆弱性診断ツール選定時によく検討されるポイント

コスト

ツールの価格は
いくらか

操作性 (工数)

設定や、スキャン実施
からレポート出力までに
どのくらい時間が
かかるか

診断項目

診断したい項目を
網羅できるか

精度 (誤検知の少なさ)

適切な診断結果を、
安定して得られるか

最近では無料ツールも登場しており、導入を検討したことがある方もいるのでは…？

コストを抑えて導入したとしても、実際に運用するといくつかの課題が…

コスト優先でツールを導入した際に起こりがちな課題

コスト



操作性
(工数)

- ・ 設定や準備に時間がかかる
- ・ レポート生成に手間がかかる



診断項目

ガイドラインに準拠するため
ツールごとの差は少ないが、
自社の基準を満たしているか
確認が必要



精度
(誤検知の少なさ)

- ・ 過検知や誤検知が発生
- ・ 重複巡回が発生

最も注目したいのは「操作性(工数)」と「精度(誤検知の少なさ)」

操作性（工数）における課題

ツール選定に失敗するとこんなところで手間・工数が発生してしまいます

導入

- ツール操作の学習
（個々の担当者ごと）



設定準備

- テストシナリオの作成
- パラメータやセッションの
引き継ぎ



スキャン

- 重複巡回によってスキャン
が非効率化



レポート

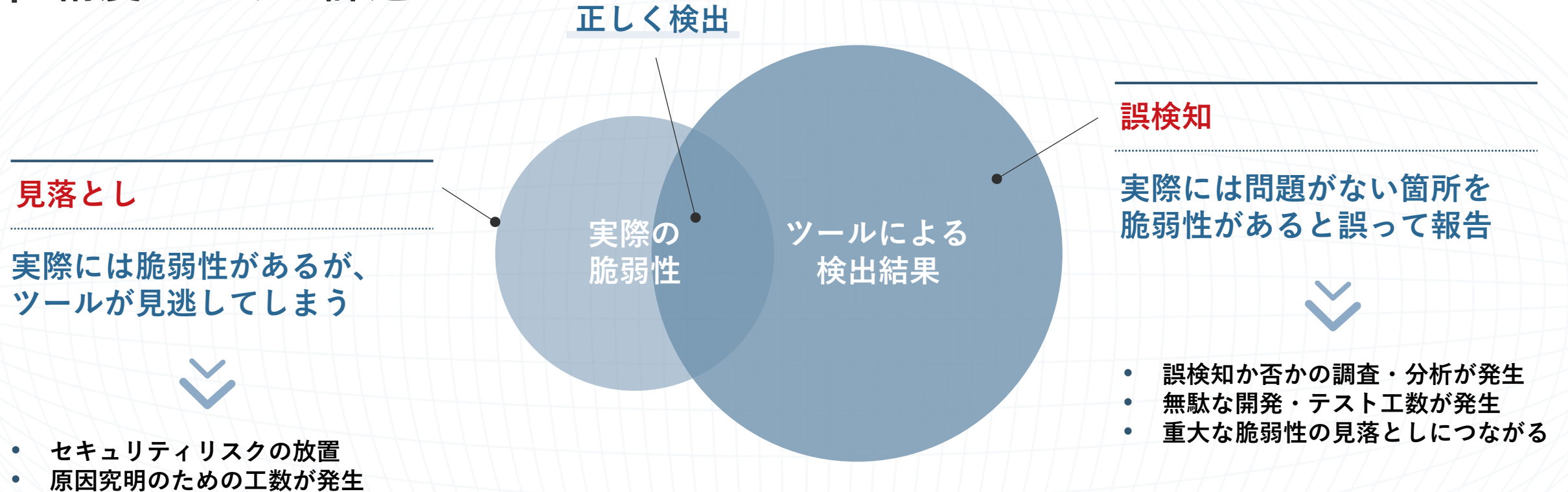
- 開発者向けのレポート作成
- 経営者への報告サマリ作成



自動化で業務効率化を図るはずが

トータルの工数がさほど削減できないリスクが

精度における課題



見落としのリスクと、
 専門知識を持った人による検証が必要になるリスクが

脆弱性診断ツールを選ぶ際に、検討すべき観点は4つ

コストを抑えてツールを導入しても、**操作性(工数)**と**精度**を軽視すると運用コストが膨らんでしまいます。人手をかけずに運用できるよう、総合的な観点でツールを選ぶことが大切です。

コスト(ツール価格)

操作性(工数)

診断項目

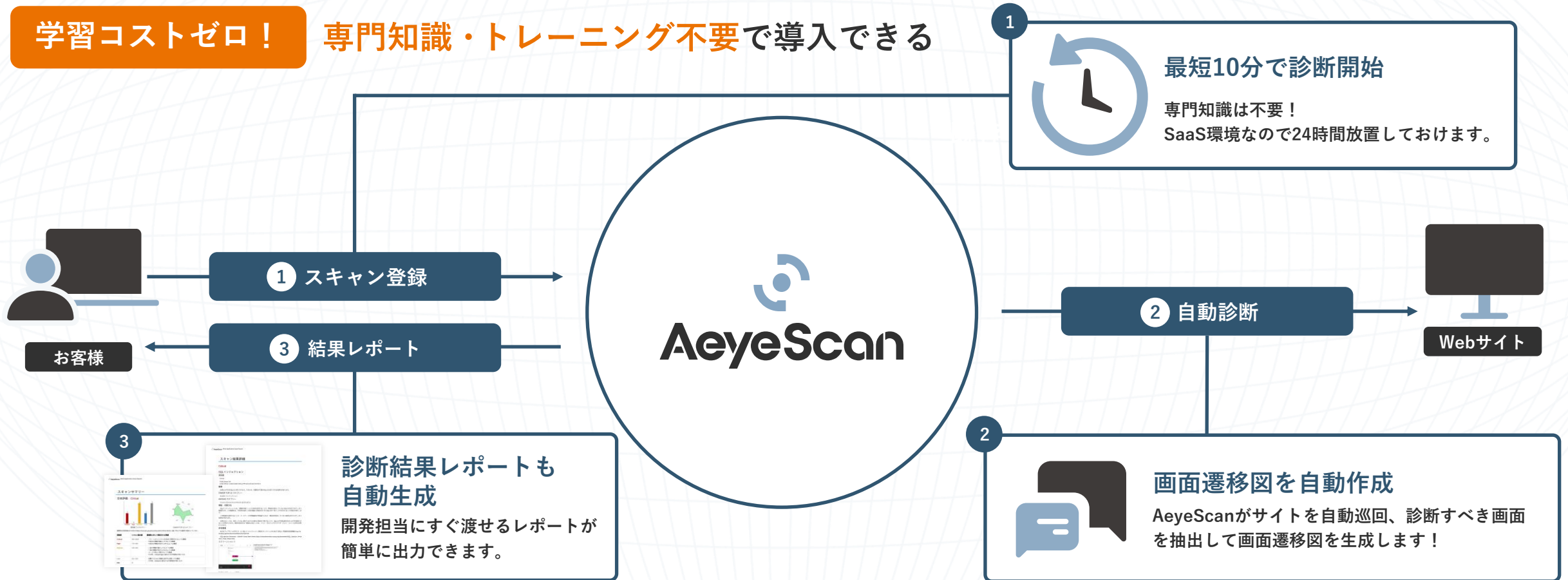
精度(誤検知の少なさ)

これらの観点を満たす一例として、
AIを活用したクラウド型Webアプリケーション脆弱性診断ツール

AeyeScan をご紹介させていただきます!

クラウド型Webアプリケーション脆弱性診断ツール「AeyeScan」とは

学習コストゼロ！ 専門知識・トレーニング不要で導入できる



 **AeyeScan** (エーアイスキャン) により
セキュリティ対策にかかる **コストを削減!**



クラウド型Webアプリケーション
脆弱性検査ツール

国内市場シェア

No.1※



有償契約
300社以上

※富士キメラ総研調べ「2025 ネットワークセキュリティビジネス調査総覧 市場編」Webアプリケーション脆弱性検査ツール ベンダーシェア (2024年度実績)
※ITR調べ「ITR Market View : サイバー・セキュリティ対策市場2025」SaaS型Webアプリケーション脆弱性管理市場：ベンダー別売上金額シェア (2022年度実績)

プロが認める品質・精度

セキュリティベンダーやSIerでも
顧客向けサービスとして活用



ブラウザ上での直感的な操作

専任エンジニア不要、情シスや開発部門でも
安定した運用が可能

| AeyeScanのポイント

テストシナリオの作成が不要で、設定は最短10分で完了

従来のツール

URLの設定

パラメータ・セッションの手動設定

テストシナリオの手動作成

AeyeScan

URLを入力するだけ！



1週間かかっていた準備が3、4時間で
終わるようになったというお声も！

| AeyeScanのポイント

AI活用のレベルが高いため、自動巡回が高精度で範囲が広い

例：AIによるフォーム入力値の判断処理

課題

フォーム入力は正しい値を入力する必要がある。
間違えると、入力エラーとなり遷移できず診断が進まない…

AeyeScanなら、
正確に入力値を推測して巡回！

！ココがポイント

名前や住所など決まった項目だけでなく、
どんな項目にも対応！

 クレジットカード

例えば

 画像アップロード

フォームを自動認識しラベル化

登録フォーム

姓名	<input type="text"/>
郵便番号	<input type="text"/>
住所	<input type="text"/>
電話番号	<input type="text"/>
メールアドレス	<input type="text"/>

確認する →

自動認識したラベル(赤枠)に応じ
適切な入力値を設定

姓名
姓名(カタカナ)
姓名(ひらがな)
姓
名
姓(カタカナ)
名(カタカナ)
姓(ひらがな)
名(ひらがな)

正常遷移

適切な値を入力

登録フォーム

姓名	巡回 太郎
郵便番号	000-0000
住所	東京都 江東区...
電話番号	03-0000-0000
メールアドレス	taro@example.com

確定 →

| AeyeScanのポイント

各種セキュリティガイドラインの**自動化可能な項目**に対応



OWASP TOP10



OWASP アプリケーション
セキュリティ検証標準



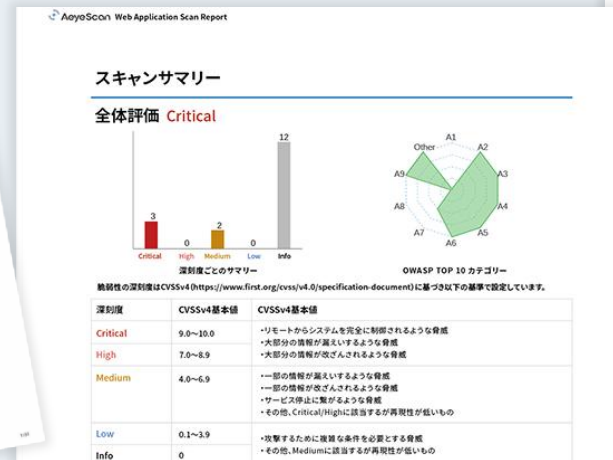
IPA 安全なWebサイトの作り方

! ココがポイント

独立行政法人情報処理推進機構（IPA）が実施した2021年度セキュリティ製品の有効性検証において、有識者会議による審査の結果、AeyeScanが選定されました。

AeyeScanのポイント

国内製品ならではの「日本語によるレポート」が自動生成される！



スキャン結果詳細

Critical

SQLインジェクション

深刻度

Critical

CVSS Score: 9.3
CVSS Vector: CVSS4.0(AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VA:H/SC:N/SI:N/SAN)

概要

危険な文字列をSQL文に挿入できます。そのため、攻撃者が任意のSQL文を実行できる危険性があります。

OWASP TOP 10 カテゴリー

A1:2017-インジェクション

ASVS4.0 カテゴリー

5.1.2, 5.1.3, 5.1.4, 5.3.1, 5.3.4, 5.3.5, 13.2.2, 13.3.1

解説・対策方法

SQLインジェクションとは、攻撃者が細工した入力値を送信することで、開発者の想定していないSQL文を実行できてしまう脆弱性です。この脆弱性は、利用者の送信した値が適切に前処理されずにSQL文の一部として利用されることが原因で発生します。この脆弱性を悪用することで、データベースの情報漏えいや情報改ざんなど、開発者の想定していない処理を実行されてしまう危険性があります。

対策方法としては、想定していない値が入力された場合に処理を中断することや、SQL文で特殊な意味を持つ文字を無効化することが挙げられます。脆弱性を実装する一般的な方法としては、パラメータ化クエリやプレアドステートメントの利用が挙げられます。

参考情報

安全なウェブサイトの作り方 - 11 SQLインジェクション | 情報セキュリティ | IPA 独立行政法人 情報処理推進機構 (<https://www.ipa.go.jp/security/vuln/websecurity/sql.html>)

SQL Injection Prevention - OWASP Cheat Sheet Series (https://cheatsheetsseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html)

スクリーンショット



ココがポイント

- どのガイドラインに準拠して検出された項目かがわかる
- どう修正すべきかも記載しており、そのまま開発者に渡せる
- エグゼクティブサマリーも簡単に作成可能



様々な形式でカンタンに
自動生成ができる！

ドメインごとの課金ではなく「定額プラン」での利用も可能



複数のWebサイトを運営していても診断し放題だから…

リリース直前の診断や、
継続的な再診断も
負担なく実施できる



診断を運用サイクルに
組み込みやすく、
チームで取り組める



継続的かつ高頻度な診断により、セキュリティ強化を実現

さまざまな企業さまに導入いただいております

ユーザー企業

人材・教育



メディア



インフラ



製造



SaaS



金融



エンタメ



SI・IT企業

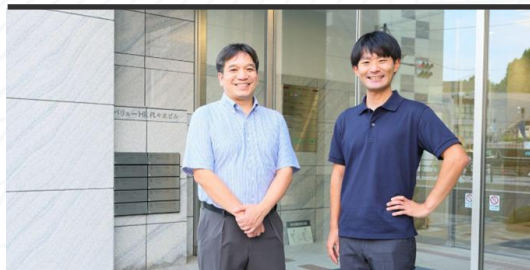


セキュリティ企業



導入事例紹介

バリューHR様



企業名 株式会社バリューHR

事業内容 健康情報のデジタル化サービス・健康管理サービスの提供など

従業員数 680名 (2023年12月31日現在)

課題

他社の診断ツールを使っていたが、多くの時間と工数がかかるほか、対象範囲をすべてチェックできずにいた

具体的な課題

- 1 顧客から求められるセキュリティレベルに応える必要がある
- 2 他社ツールでは設定やスキャンに時間がかかり、診断しきれないことも多かった
- 3 好きなタイミングでスキャンしたいため、外部委託はできない

機微な個人情報を大量に預かっていることもあり、顧客からも定期的な脆弱性診断の実施状況を問われていた。セキュリティの担保のために他社の診断ツールを導入したものの、時間や工数などの課題が生じ、他のツールを検討することになった。

導入

短時間でスキャンできて使いやすく、設定も楽なことから導入を決定

導入の背景

- 1 以前使っていたツールと比較して設定が簡単
- 2 スキャン時間が短縮でき、使いやすい
- 3 OWASP TOP 10に沿って出されるレポートがわかりやすい

普段から付き合いのあるベンダーからの紹介も含め、いくつかの候補を検討する中、短時間でスキャンでき、使いやすいことを重視してAeyeScanを選定。中でも、ユーザーIDやパスワードの仕様を調べて設定する必要がなく、楽だと感じた。

効果

診断にかかる時間・工数が短縮できたほか、見込み客からのセキュリティに関する質問にも迅速に回答できるようになった

具体的な効果

- 1 サービス導入前にセキュリティについて回答することで、営業もしやすくなった
- 2 画面遷移図により、自社サービスの構成が把握できるようになった
- 3 数日かけても終わらなかった診断が、1日で終わるようになった

AeyeScanの導入で、スケジュールを組んでおけば自動的にスキャンが実施されるようになった。工数や時間が削減できたのはもちろん、導入前にセキュリティ実施状況を伝えられるようになったことで、営業担当者にもメリットが生まれた。

導入事例紹介

マネーフォワード 様



企業名 株式会社マネーフォワード

事業内容 PFMサービスおよびクラウドサービスの開発・提供

従業員数 2,400名 (2024年5月末日現在)

課題

事業が拡大しプロダクトが増えるにつれ、脆弱性診断の間隔が空いてしまうことが懸念材料だった

具体的な課題

- 1 外注だとナレッジが蓄積されない
- 2 外注だと画面数に応じた料金体系で網羅的な診断を受けづらい
- 3 開発が遅れた場合、ベンダーとのスケジュール調整が困難

新機能の追加や大規模な改修の際には脆弱性診断を実施していたが、それ以外はプロダクト側の判断に委ねていた。小さな改修のたびに診断を外注するのではなく、内部で迅速に診断する選択肢も持ちたかった。

導入

診断ツールを導入し
継続できなかった経験から、
使いやすさを重視

導入の背景

- 1 自動巡回のカバー率が高く、主要な脆弱性を確実に検出できる
- 2 グループ会社のプロダクトも診断できるライセンス体系
- 3 API診断が可能

外国籍エンジニアも多く在籍するため、英語にも対応していること、Slackをはじめとする外部サービスとの連携性も要件だった。複数のツールの比較検討を進め、いくつかのプロダクトを対象に検証を実施した上で選定。

効果

約60プロダクトに診断を実施できた
今後、最低年1回の診断を計画

具体的な効果

- 1 画面遷移図により、CISO室がプロダクトの画面を把握できるように
- 2 開発者のセキュリティ意識が高まった
- 3 グループ統一のセキュリティスタンダード適用にも活用予定

ほぼすべてのサービスを内製で開発する中、「セキュリティスペシャリストの活動をAeyeScanがサポートしてくれている」とCISOも評価。セキュリティエンジニア以外に、QAチームでも使用を開始している。

AeyeScanの導入を検討してみませんか？

操作性の確認、実際に利用してみたい方へ

AeyeScanの 無料トライアル

トライアルにかかる費用は不要。実際の操作性はどうか？
またどのように脆弱性が発見されるのか？
などの疑問は無料トライアルで解消しましょう。

無料トライアルの申し込み



お見積りの希望・導入をご検討している方へ

AeyeScanへの お問い合わせ

お見積りの希望・導入をご検討してくださっている方は
お問い合わせフォームよりご連絡ください。
当日もしくは遅くとも翌営業日にはご連絡を差し上げます。

お問い合わせフォーム



会社概要

商号	株式会社 エーアイセキュリティラボ		
役員	代表取締役社長	青木 歩	
	取締役副社長	安西 真人	
	取締役	杉山 俊春	角田 茜
	執行役員 CTO	浅井 健	
	執行役員	関根 鉄平	
事業内容	情報セキュリティ関連事業（調査・コンサルティング） セキュリティ診断クラウドサービス「AeyeScan」提供		
設立	2019年4月		
拠点	東京都千代田区神田錦町2-2-1 KANDA SQUARE 11F WeWork内		
資本金	1億円		
社員数	57名		
Webサイト	https://www.aeyesec.jp/		
取得認証	情報セキュリティマネジメントシステム（ISMS） ISMSクラウドセキュリティ認証（ISO27017） 情報セキュリティサービス基準適合サービスリスト		

AeyeSecurityLab

セキュリティに
「あらたな答え」を提供し続ける
プロ集団



IS 752963 /
ISO 27001

CLOUD 790050 /
ISO 27017 023-0026-20



AeyeScan

セキュリティに、確かな答えを。