

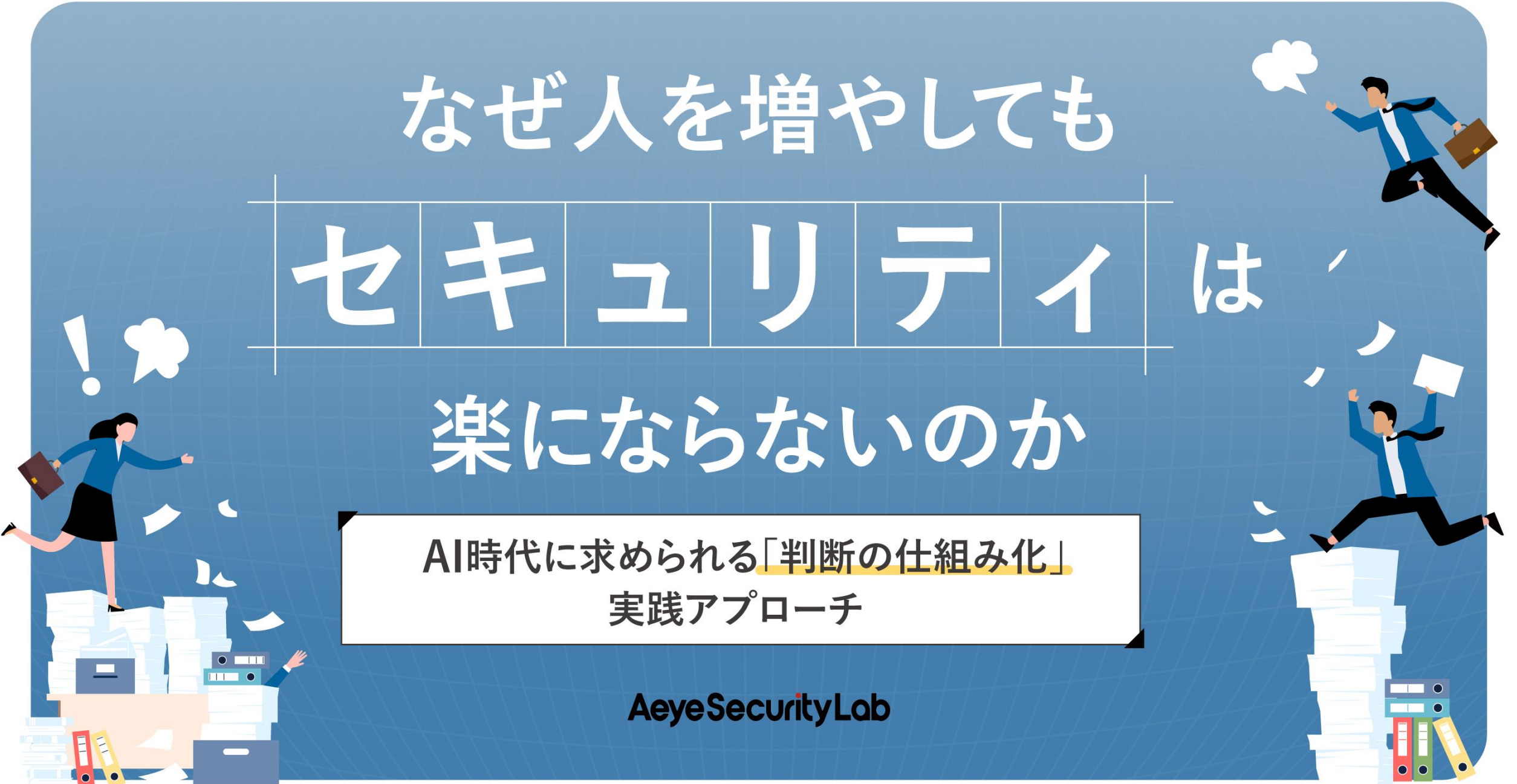
なぜ人を増やしても

セキュリティは

楽にならないのか

AI時代に求められる「判断の仕組み化」
実践アプローチ

AeyeSecurityLab



本資料の目的

サイバー攻撃の高度化とシステムの複雑化により、
企業に求められるセキュリティ対策の範囲と難易度は急速に拡大しています。

こうした状況の中で、セキュリティ対策が継続的に回らないケースも増えているのではないのでしょうか。
その要因は「人手不足」として語られがちですが、実際には、判断の複雑さや属人化といった構造的な問題にあります。

本資料では、セキュリティ運用が抱える本質的な課題を整理した上で、
「人手」に依存しない新たなアプローチとして、
判断を標準化・再現可能にする“仕組み化”の考え方を解説します。

さらに、AIを活用した具体的な実現方法として、脆弱性診断を起点とした実践的な取り組みをご紹介します。

セキュリティ対策を“属人化した作業”から“継続的に回るプロセス”へと転換するためのヒントとして、
ぜひ本資料をご活用ください。

| 守り手が疲弊する、終わりのない苦行

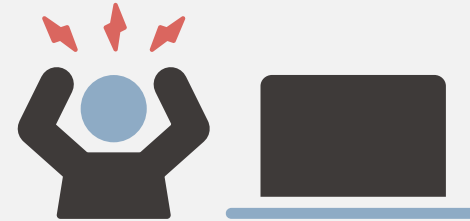
攻撃者は「AI」で武装し、低コストで無限に襲いかかる。対する私たちは、限られた「人手」で、増え続ける穴を塞ぎ続ける。——この「圧倒的な非対称性」のなかで、従来型の防御は限界を迎えています。

攻撃者



AIによる攻撃の
「自動化・高度化」

企業



リソース不足と
「対応範囲の肥大化」

脆弱性対策の継続的な運用はますます困難な状況に
しかし、人手・予算はなかなか増えない

現場を襲う、終わりのない「判断」

アラート対応

どこまで無視していい？

脆弱性対応

自社環境で本当に危ない？

優先順位づけ

どこまでやれば合格？

説明責任

「安全です」と言えるか？



事業継続

サービス止めてまで直す？

次から次へと、正解のない判断を迫られている

問題の本質は、「人手不足」ではなく「スキル不足」…？

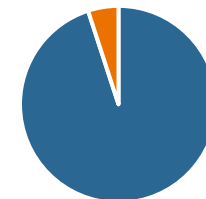
セキュリティ対策で語られがちな量的な不足以上に、現場を追い詰めているのは「スキルの高度化」です。

ISC2：2025年版「サイバーセキュリティ人材調査」



何らかのスキル不足を抱えている

→ **Yes.** 世界の回答者の **95%**



内、自組織でスキル不足に起因する
重大インシデントを少なくとも1回経験

88%

では、解決策は「スキルの補充/スキルを持った人材の補充」なのか…？

「スキルの補充」では解決しない3つの理由

処理能力の限界

判断に必要な情報が多すぎて
人間が処理しきれない



人員を増やしても情報処理の
「複雑さ」は解消されない

個人の能力には
物理的な限界がある

属人化

高度なセキュリティ判断は
ベテランの頭の中にしかない



訪れるのは
“質のバラつき”と“教育コスト”

属人化は、組織としての
新たな脆弱性を生む

戦略の不在

目の前の現場対応に追われ
中長期的な設計が後回しに



スキルを磨くほど職人技に依存し
仕組み化から遠ざかる

実務（How）を極めても
構造は変えられない

「スキルの補充」ではなく「誰でも判断・対応できる仕組みづくり」を

「人の努力」でカバーし続ける運用は、もはや持続可能な取り組みとは言えません。
必要なのは、個人のスキルに依存しない「設計されたプロセス」への転換です。

これまで		これから
人が判断する	>>	判断を構造化する
経験に頼る	>>	ルールと根拠に落とす
属人化	>>	再現可能にする
人が処理する	>>	機械に任せる部分を増やす

セキュリティ判断を「作業」から「仕組み」に変える **発想の転換** が必要

| 仕組みへの転換を加速させる「AIと人間の協働」

「判断の仕組み化」のために必要なのは、以下の3つのステップです。



仕組み化の土台となる「経験の蓄積」には、膨大な工数を要する
効率的な仕組み化には、**AIとの協働が不可欠**

AIとの協働で「判断を仕組み化する」ための具体的な取り組み

例) 脆弱性管理のプロセスを仕組み化する場合

判断を「分解」する

「この脆弱性は危険か？」ではなく、
構成要素に分解する

- 悪用可能性 (Exploit)
- 到達可能性 (Exposure)
- 事業影響 (Impact)

AIと人間が協働して
判断材料を集約する

判断を「形式知化」する

CVSS (数値) だけでなく、
業務文脈をルール化する

- ビジネス観点の重要度は？
- システム停止時の影響範囲は？
- 業務継続の代替手段はある？

判断の「観点」をルール化し
組織の判断能力を「複製」する

判断を「仕組み化」する

AIと役割分担し、
人は設計と例外処理に注力する

AI	人間
• 情報収集	• 例外処理
• 情報整理	• 経営判断
• 反復作業	• 仕組みの設計

人を「作業」から解放し
本来の「戦略」に注力させる

まずは、脆弱性診断から「判断の仕組み化」に着手しませんか？

判断基準が明確、かつ運用頻度が高い「脆弱性診断」は、AI活用の仕組み化が効果を発揮しやすい領域です。

脆弱性診断は…

情報処理の量が膨大



脆弱性情報・
資産情報・ログなど
判断材料が膨大

判断の再現性が重要



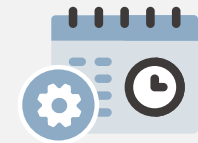
属人化により
優先度がぶれると
対応品質が安定しない

説明できる判断が必要



対策方針の理由を
言語化できないと
経営の合意が得られない

継続運用が前提

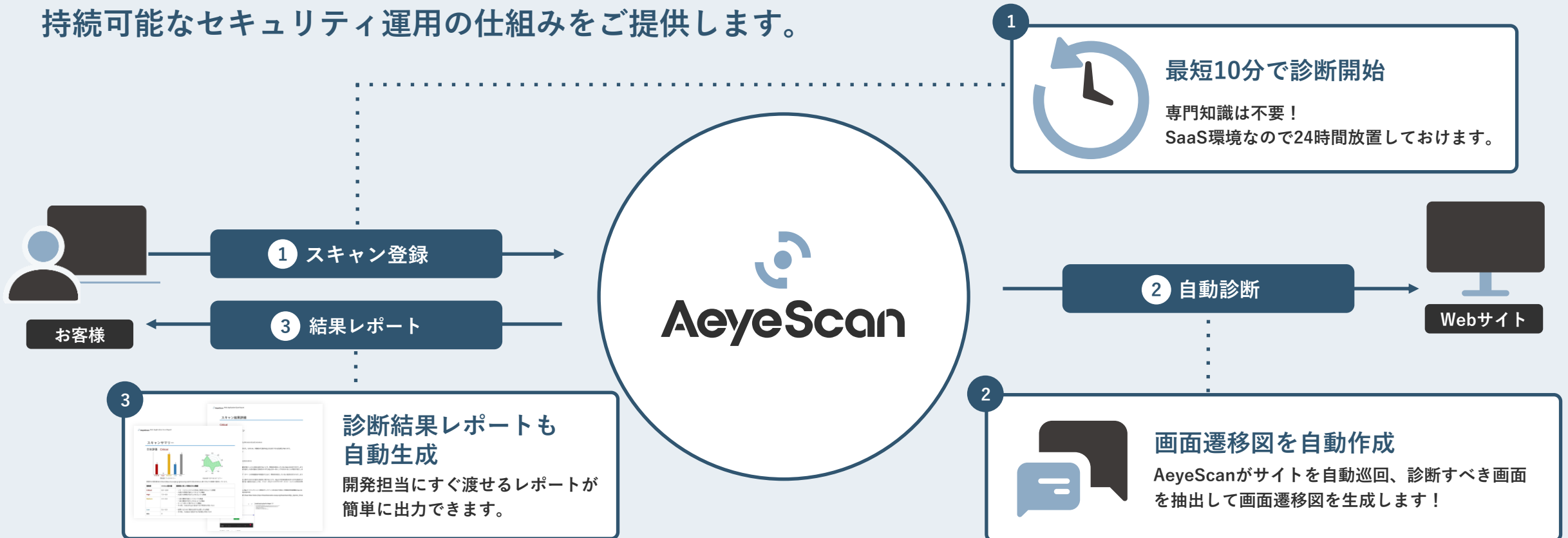


一度きりではなく
日々発生し続けるため
仕組み化が必要

だから、AI活用によって「品質」を維持しながら「効率」を高められる！

AIとの協働で「判断の仕組み化」を実装する クラウド型Webアプリケーション脆弱性診断ツール「AeyeScan」

属人的な「作業」をAIが担う「仕組み」へ。
持続可能なセキュリティ運用の仕組みをご提供します。



 **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 (2023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

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



| AeyeScanが選ばれている理由



誰でもかんたん操作



開発やセキュリティの知識がなくても、
トレーニングなしで診断可能。



AIによる自動診断



圧倒的な巡回精度で
24時間自動で診断。
画面遷移図で状況を可視化。



わかりやすいレポート



各種ガイドラインに準拠した
プロ仕様のレポート出力、
日本語と英語に対応。

導入事例紹介

エイチ・アイ・エス 様



企業名 株式会社エイチ・アイ・エス

事業内容 総合旅行会社

従業員数 10,849名 (2023年6月時点)

課題

セキュリティの内製化が困難。
診断の外注コストを削減したい

具体的な課題

- 1 社内からの診断依頼が増え続けていた
- 2 診断対象が多く外部委託せざるを得ない
- 3 外注による診断コスト増

内製・外製含め100を超えるWebアプリケーションがあり、内部の体制だけでは全ての診断実施に対応できず、一部を外部に委託。コスト削減と体制整備が課題だった。

導入

情報処理推進機構（IPA）の検証結果と
「7割以上自動化」という点が決め手

導入の背景

- 1 手動の診断では対応が追いつかず自動化を検討していた
- 2 自動化できても性能が落ちない製品を探していた

手動作業を伴う診断では対応が困難になり、診断の自動化を検討。AeyeScanは、IPAの検証結果が高評価だったことと、「7割以上の自動化が可能」という点が決め手で導入。

効果

診断・レポート作成工数を大幅に削減。
さらなる内製化比率の向上を目指す

具体的な効果

- 1 診断の大部分を自動化し工数を削減
- 2 レポート機能により大幅に時間を短縮
- 3 リリース前に診断と脆弱性改修が完了

「脆弱性が発覚しても、リリースまでに修正が間に合わない」という悩みも解消され、脆弱性を潰してからアプリをリリースできるように。

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 61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。