

AIのリスクだけ見ていませんか？

生成 AI サービスを

安全に提供するための

Webセキュリティ入門



本資料の目的

今やビジネスのあらゆるシーンで活用が進む生成AI。
Webアプリケーション開発においても、生成AIを取り入れたアプリケーションや開発手法が急速に増加しています。

しかしその一方で、
「生成AIによるセキュリティ考慮不足のコード生成」や
「開発者のスキル不足に起因するセキュリティ対策の不備」など、
新たなリスクも顕在化しており、多くの企業が不安を抱えているのではないのでしょうか。

さらに見落とされがちなのが、Webアプリケーションに対する従来型のセキュリティ対策です。
基本的な脆弱性対策や、安全性を意識した運用が後回しになり、
結果として重大なリスクを招くケースも少なくありません。

本資料では、生成AI時代においても欠かすことのできないWebアプリケーションの脆弱性対策と、
手間をかけずに効率よくリスクを防ぐ方法について、わかりやすく解説します。

これから生成AIを開発に取り入れようとしている方や、セキュリティに不安を感じている方、
脆弱性対策の見直しや自動化を検討している方は、ぜひご一読ください。

生成AIを活用したWebアプリケーションが増加している

生成AI技術の急速な進化と普及により、Webアプリケーション開発のあり方が変化しています。

活用例

アプリケーションの機能として活用

コンシューマー向け

- ・ 占いアプリ
 - ・ 料理レシピ提案サービス
 - ・ 教育・学習支援アプリ
- など

ビジネス・専門分野向け

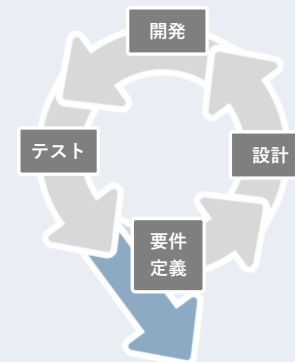
- ・ 全般：議事録作成
 - ・ 営業：活動・データ分析レポート
 - ・ マーケティング：記事・LP作成
- など

ユーザー体験や業務効率を大幅に向上させる
機能が提供できる

開発プロセスにおいて活用

画面デザイン
／UI作成支援

テストコード
自動生成



機能開発
／コード生成支援

ドキュメント化
／コード解析支援

読み込ませる参考データの品質によっては
大幅な開発工数の削減が見込める

生成AIを活用したWebアプリケーションにはこんなリスクが

生成AIのリスク

生成AI固有のリスク



Hallucinationやプロンプト
インジェクションなど

利用する人のリスク
(開発者 / 運用者)



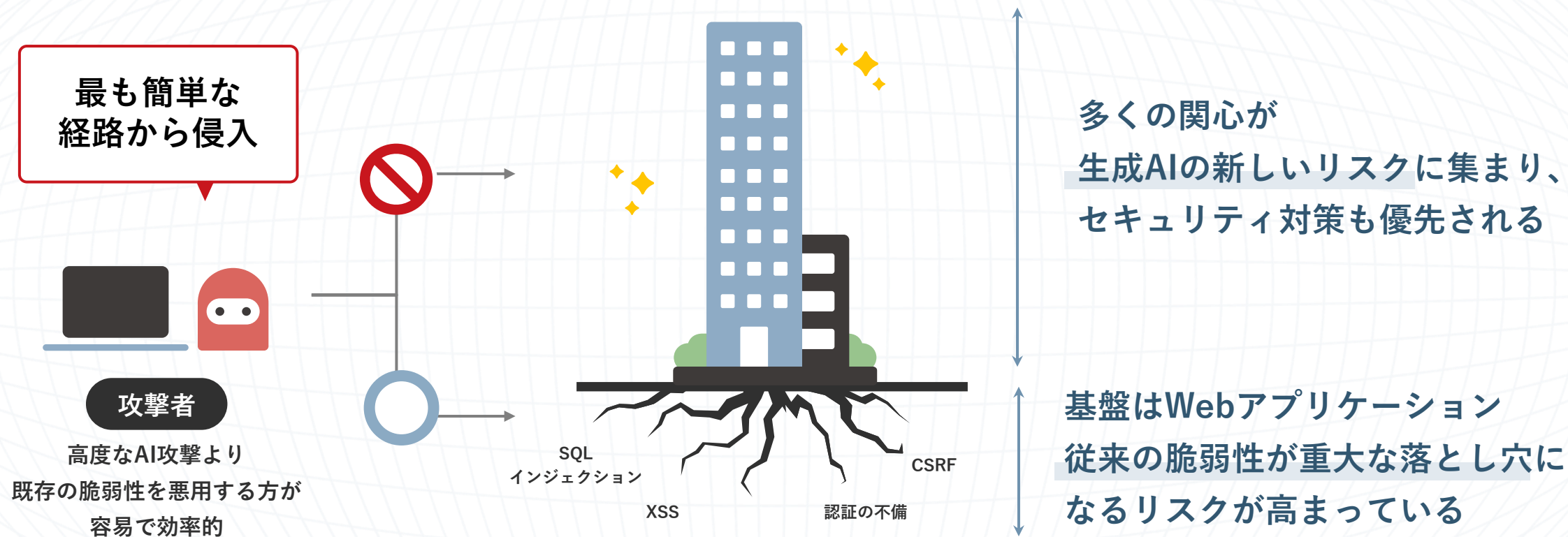
スキル不足による
セキュリティ対策の不備

Webアプリケーション のリスク



SQLインジェクションやクロスサイト
スクリプティング (XSS) など
Webアプリケーションにおける典型的な脆弱性

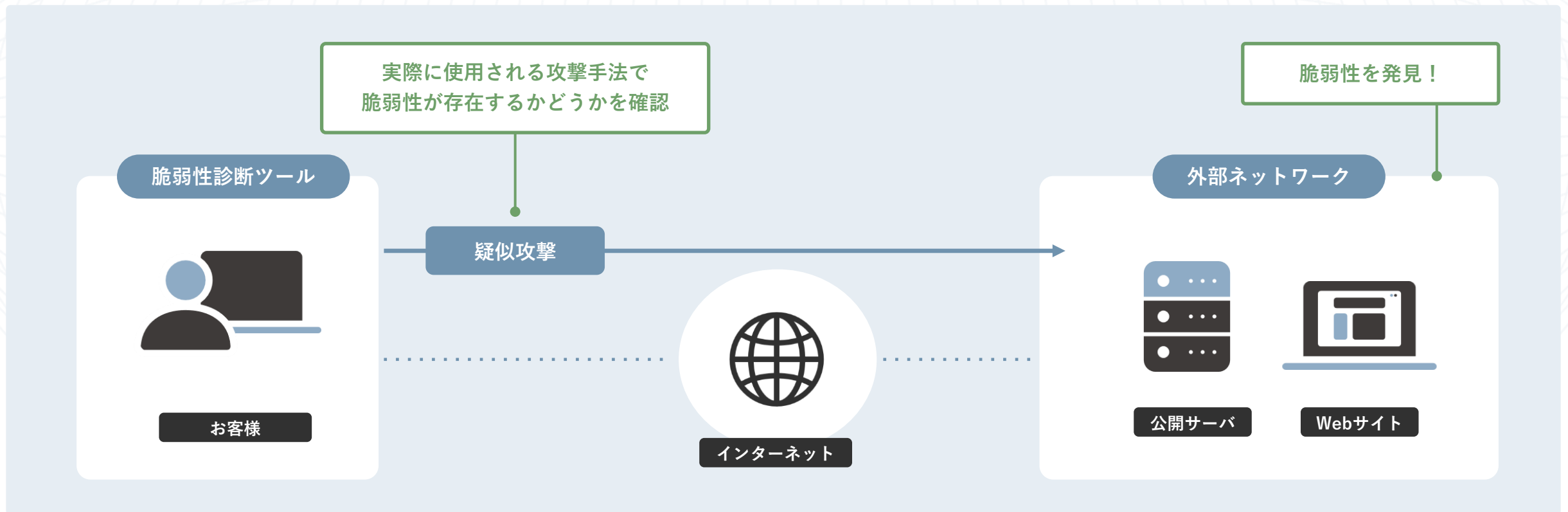
生成AIブームの裏で放置される「既存の脆弱性」



実際に発生しているサイバー攻撃の多くは
依然として「既存の脆弱性」を起点としている

既存の脆弱性に対して必要な「脆弱性診断」とは

脆弱性を突いた攻撃を受けた際に、被害につながる可能性がないか検証すること



定期的に脆弱性診断を実施するにはどうすればよい？

構築時

設計・開発時に
可能な限り脆弱性を解消



IPAによる「安全なウェブサイトの作り方」を参考にすることで、自社開発でも外部委託でも同じ基準でセキュリティ対策が可能

運営時

運用中は定期診断を実施しつつ、リリースや機能改修時も
必ず脆弱性診断を行う



年に1回の
定期診断

+

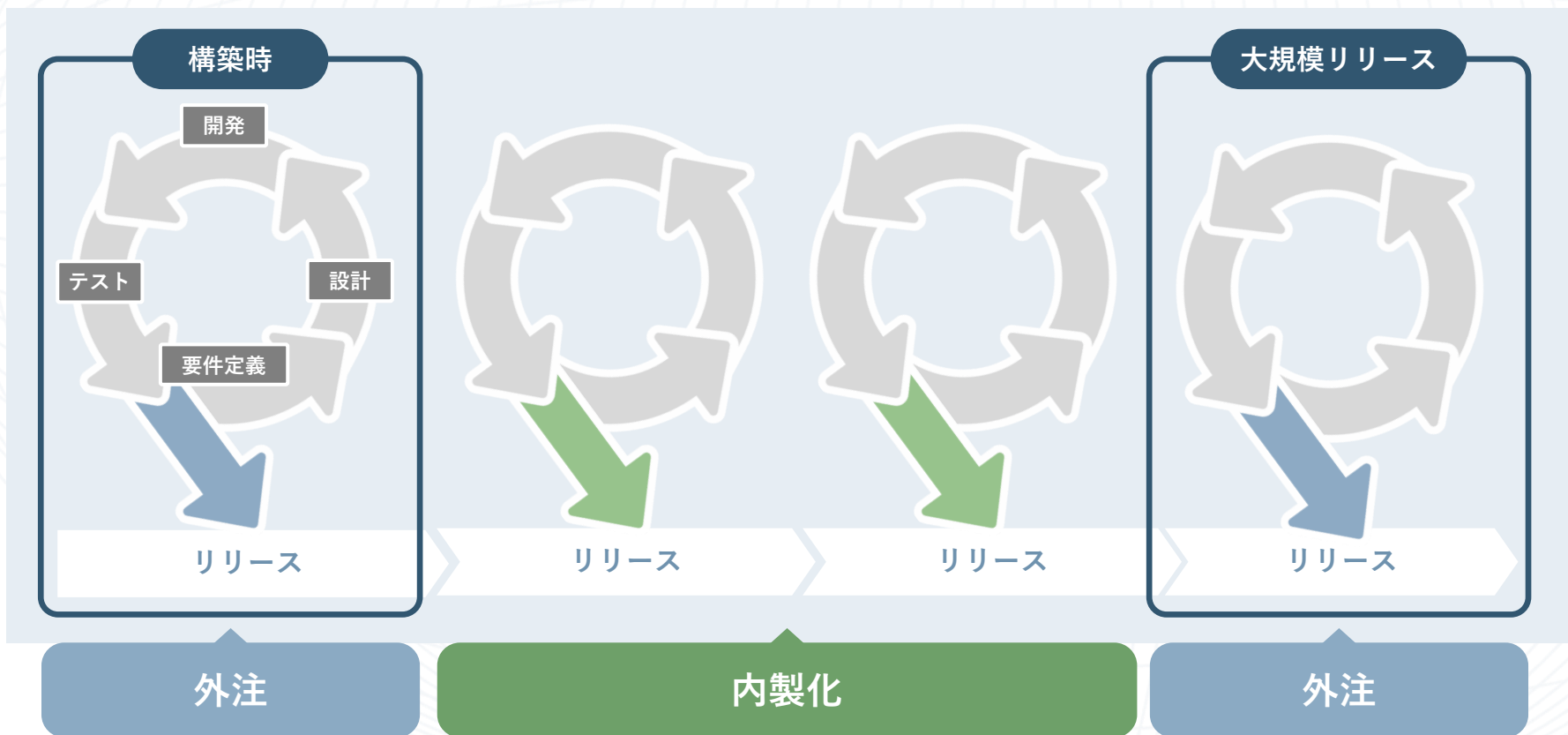


リリースや
機能改修時

Webサイトで扱う情報の重要度を踏まえて頻度の検討を！

| そんなに頻繁に脆弱性診断を外注していたらコストが…

そこでおすすめしたいのが、脆弱性診断を外注するだけでなく、社内でも実施するハイブリッド型の運用。



大規模リリースは
外部に任せ、日々の
小さな更新は社内で。

状況に応じた
診断体制で、継続的な
セキュリティを実現。

| 専門家でもないのに、脆弱性診断を自分たちでできるの？

誰でも簡単に、プロさながらの脆弱性診断ができるツールの導入がおすすめ！

 **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「2024 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〈クラウド〉2023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

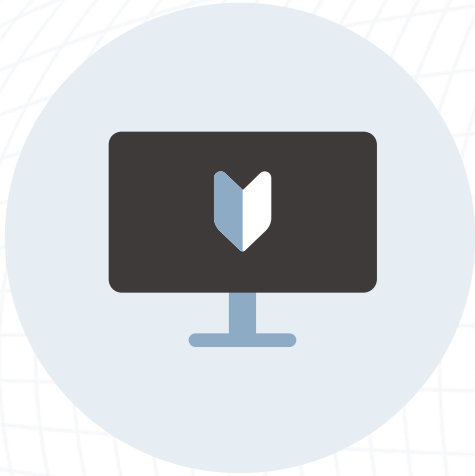
セキュリティベンダーやSIerでも
顧客向けサービスとして活用



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

| 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。



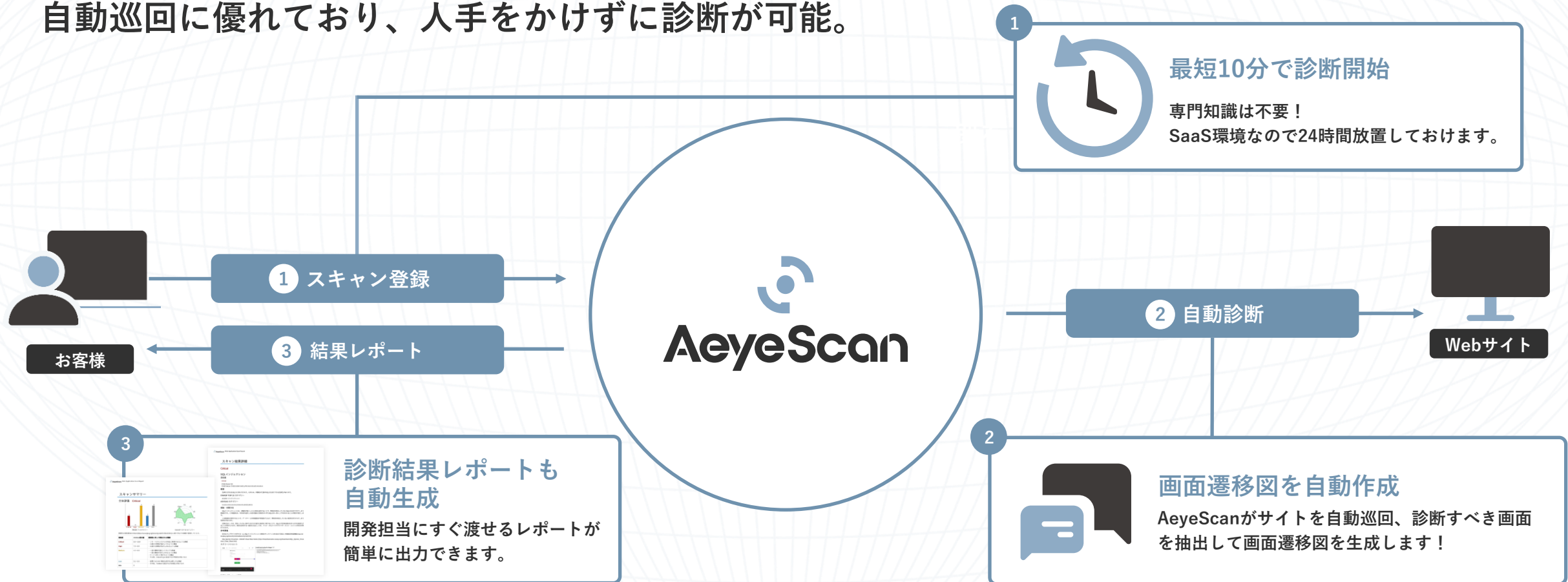
わかりやすいレポート



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。

そもそもAeyeScanとは？

AI・RPAの活用により、脆弱性診断を自動化するクラウド型Webアプリケーション診断ツール。
自動巡回に優れており、人手をかけずに診断が可能。



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

製造



インフラ



金融



メディア



人材・教育



エンタメ



Leverages



SaaS



SI・IT企業



セキュリティ企業



導入事例紹介

バトンズ 様



企業名 株式会社バトンズ

事業内容 M&A総合プラットフォームの企画・開発・運用

従業員数 122名 (2025年2月時点)

課題

M&A・事業承継に関わる機密情報を
万全のセキュリティで守るため、
診断の高頻度化が必要に

具体的な課題

- 1 外部ベンダーによる脆弱性診断はコストがかかる
- 2 診断範囲の調整も入ることから、準備にかなりの工数を要する

プラットフォームの企画・開発・運用を行う中で、企業の極めて重要な機密事項を取り扱うことから、診断頻度を見直すことに。限られた予算やリソースの中で高頻度化を目指すべく、内製化を検討。

導入

外部の専門家に依頼するときと
同レベルの診断クオリティを評価

導入の背景

- 1 業界標準のセキュリティ基準に準拠している
- 2 自動巡回の精度が他社ツールより高い
- 3 自動で画面遷移図が生成され、非エンジニアでもわかりやすい

経産省が示すセキュリティ基準や、OWASPアプリケーションセキュリティ検証標準を満たしている上、自動巡回の精度が高いことからAeyeScanを採用。効率的に診断が実施できるわかりやすさも評価。

効果

週1の定期診断と
新機能リリース時の即日診断を実現し、
サービスへの信頼度も向上

具体的な効果

- 1 診断の高頻度化を実現
- 2 脆弱性を検知した場合も即座に対応できるようになった
- 3 お客さまにサービスの安全性を客観的に示せるようになった

外注時は年に1回の診断だったが、毎週土日の定期診断と、新機能リリース時の即日診断が可能に。金融機関などのお客様にセキュリティ対策の実施状況も説明しやすくなり、サービスへの信頼度向上を実感。

導入事例紹介

ミズノ 様



企業名 ミズノ株式会社

事業内容 スポーツ用品の開発・販売ほか

従業員数 3,584人(2024年3月31日現在)

課題

国内だけでも約20 Webサイトを運営する中、
定期的な脆弱性診断ができていなかった

具体的な課題

- 1 サイト立ち上げ時や大規模改修時だけしか診断ができていない
- 2 外部ベンダーによる脆弱性診断だと多額のコストがかかる
- 3 内部の人材のスキル不足・業務負荷が高くなる

グローバル全体でセキュリティポリシーを見直し、その中に定期的な脆弱性対策を含めたものの、外部ベンダーによる脆弱性診断だとコストがかかる。内製化を検討するもスキル不足や業務過多といった課題があることから、自分たちでも使える診断ツールの導入を検討。

導入

定額で複数サイトに外部ベンダーによる
脆弱性診断と変わらないクオリティの診断が
できると評価

導入の背景

- 1 専門知識を持たなくても簡単に操作できる
- 2 サイト数に比例して費用が増加しない
- 3 外部ベンダーによる脆弱性診断と同等の品質で診断できる

AeyeScanのトライアルを行い、簡単に操作できることを実感。また、同一サイトに対して、外部ベンダーによる脆弱性診断による診断とAeyeScanによるスキャンを並行して行いレポートを比較。AeyeScanの方が同レベル以上・検知項目が多かったことから、導入を決めた。

効果

定期的な診断が可能な体制が整った。
時間短縮により、
診断後の対策、チェックもスムーズに

具体的な効果

- 1 内製化により、診断にかかる時間が数ヶ月単位から数週間に短縮
- 2 診断、対策、チェックの運用がきれいに回せている
- 3 開発ベンダーとのコミュニケーションもスムーズになった

外部ベンダーによる脆弱性診断では脆弱性への対応も含めて数ヶ月単位の時間がかかっていたが、数週間で診断を終えてすばやく対策できるようになった。レポートに具体的な修正方針も示されるため、開発ベンダーとのコミュニケーションもとれ、対策もスムーズになった。

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

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

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	田中 大介
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		
従業員数	43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		





AeyeScan

セキュリティに、確かな答えを。