

フ ロ ン テ ィ ア A I で、

脆弱性診断はどう変わる？

進化する攻撃に追従する、
これからの防御アプローチ

AeyeSecurityLab



本資料の目的

フロンティアAIの進化により、
サイバー攻撃はこれまで以上に高速化・自動化しつつあります。
一方で、「攻撃側がAIを使うなら、防御側もフロンティアAIで対抗すればよい」という単純な構図では、
システム全体を漏れなく守ることはできません。

本書では、フロンティアAIを脆弱性診断に活用する際の限界を整理したうえで、
AI時代だからこそ重要になる「既知の脆弱性を残さない」という基本対策と、
攻撃の進化に追従するための網羅性・再現性・継続性を備えた診断体制について解説します。

さらに、こうした防御を人手やコストを抑えながら継続するための、
セキュリティ専用AIによる自動診断のアプローチもご紹介します。

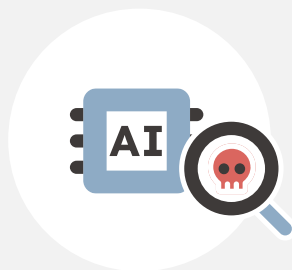
フロンティアAI時代における脆弱性対策の考え方を整理し、
自社に必要な防御体制を見直すために、ぜひご一読ください。

AIの進化がもたらす「セキュリティ常識」の変革

「Claude Mythos Preview」をはじめとするフロンティアAI（自律型AI）の登場により、AIの性能は急速に進化しています。

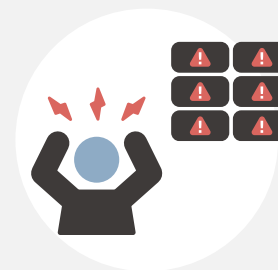
フロンティアAIの進化がもたらす脅威

脆弱性発見から攻撃までの
スピードが劇的にアップ



最新の攻撃手法（ゼロデイ/Nデイ）を取り込み、人間を遥かに凌駕する速度で次々と脆弱性を突き、悪用する能力を持つ。

従来の人間中心の対策では
対応困難な時代へ



少ない工数で攻撃の成否を判断できるため、攻撃サイクルが超高速化。脆弱性を放置できる猶予はゼロに。

攻撃と防御の圧倒的な非対称性が課題に

攻撃側はフロンティアAIを使って一箇所の穴を見つけてきますが、防御側は一箇所の穴が致命傷になるため、「全体」を網羅し続ける必要があります。

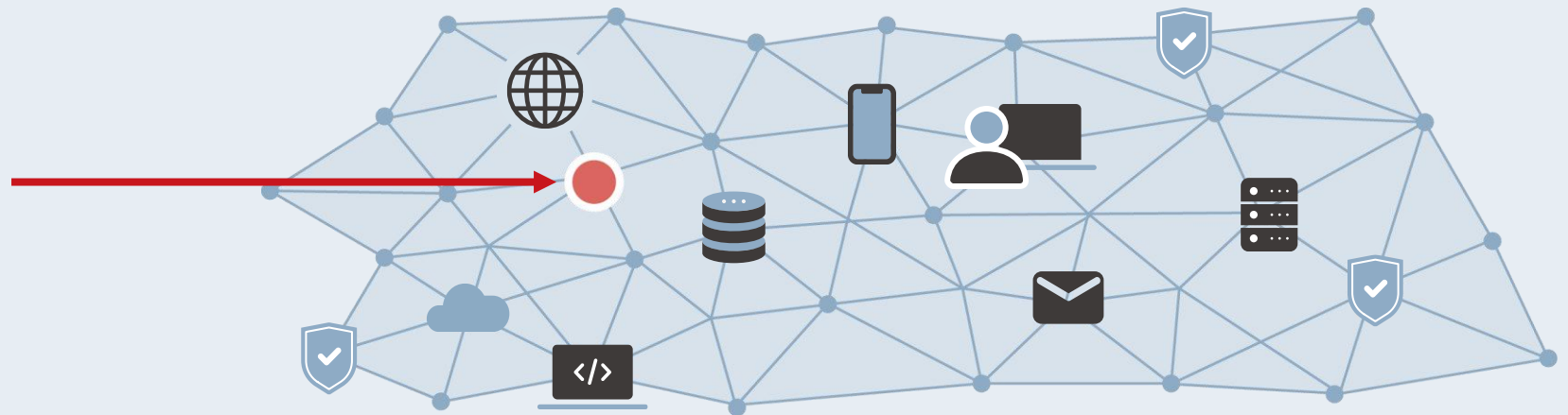
攻撃側

「点（脆弱性）」を
ピンポイントで突き抜ける
能力が高度化



防御側

「面（システム全体）」を常に取り守り続けなければならない



この「網羅性の欠如」こそが、フロンティアAI時代における防御の最大の弱点となっています。



では、防御側も
フロンティアAIを使えばいいのでは？

フロンティアAIで高性能な防御ができるという誤解

フロンティアAIは脆弱性検知を高速化しますが、「網羅性の向上（穴をゼロにする）」は構造上難しいのが現状。

誤解 1



脆弱性がなくなるまで
全自動で診断してくれる？

フロンティアAIが知っているのは、
世界で公開済みの脆弱性や攻撃手法のみ。
自ら全自動で脆弱性がなくなるまで
診断計画を立ててはくれない。

※「AIが未知の脆弱性を発見」というニュースは、AIを駆使して「専門家が」発見しています。

誤解 2



フロンティアAIモデルが
進化すれば網羅性も高まる？

システム全体の「網羅性」は学習で
強化できず、“AIモデルの進化”とは
無関係。AIが進化しても、
診断の網羅性は100%にならない。

米国の主要なセキュリティ研究※の
結果から見ても、フロンティアAI
単体で「穴をゼロ」にするのは困難

※LLMを用いた自動脆弱性診断の評価テスト等

脆弱性発見率 約50～70%
→ 3～5割は見落とす可能性

誤検知（偽陽性）も多く発生
→ 人による確認・仕分けが必要

フロンティアAIによる脆弱性診断の限界

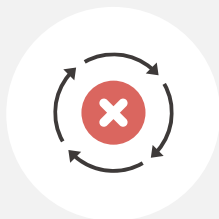
フロンティアAIのベースである大規模言語モデル（LLM）は、「ふさわしいテキストを確率で選んで返す」仕組みであるため、診断の正しさを担保する上でも限界があります。

セーフガードにより
診断が制限される



攻撃と判定される処理は、
モデルによっては拒否・
制限される場合がある。

再現性がなく
精度が担保できない



診断手法が正しいかを検証
してはならず、診断のたびに
手法がブレる。

コンテキストに
誤りが蓄積する



指示修正が追記で行われる
ため、必要な記憶が抜け、
結果に影響を及ぼす。

情報収集（巡回）に
限界がある

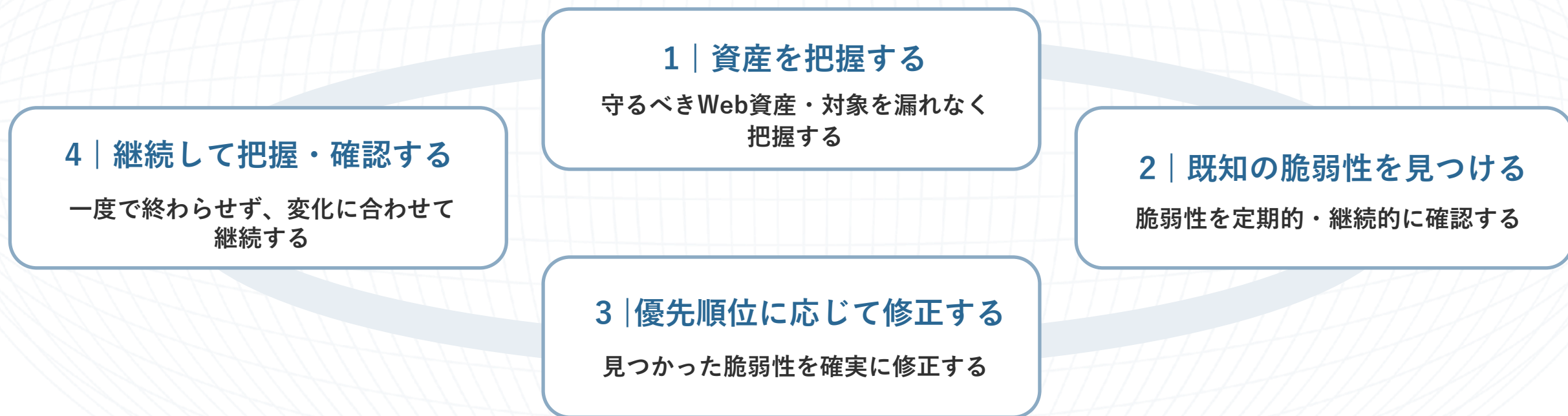


確率任せなので、巡回が速す
ぎる切り上げ（見落とし）や
堂々巡り（時間切れ）に
陥りやすい。

無理に現場で使おうとすると、かえって専門家の補完＝属人化が発生

フロンティアAI時代だからこそ立ち返るべき「基本の徹底」

新しい攻撃手法への対応や高度な防御策に目を奪われがちですが、まず重要なのは、すでに分かっている脆弱性を確実に残さないという「当たり前の対策」です。



新しい攻撃手法を追いかける前に、まずは既知のリスクを残さない仕組みづくりを

必要な防御とは、「網羅的で地道な継続診断」

これから防御に必要なのは、フロンティアAIモデルの進化ではなく、システム全体を網羅的に潰す地道で継続的な診断だと言えます。

網羅性

全画面・全サイトを
網羅的に診断



認証後の画面も含め、
診断対象を漏れなく確認

再現性

同じ基準で
繰り返し診断



担当者や実施タイミングによらず、
一定の基準で実施

継続性

低コスト・低工数で
継続



人に依存せず、必要なタイミングで
繰り返し実施

「網羅性・再現性・継続性」のある診断を、攻撃に追従させる仕組みが必要

診断対象の拡大による「コスト増」への対抗策

攻撃が高速化・自動化するAI時代においては、「すべてのサイト・すべての画面」を網羅的に診断する（面で対策する）ことが必須となり、それだけセキュリティコストや手間が嵩む時代に突入しています。

AI時代に備えた「セキュリティ体制・予算」をつくる

「かかる費用の理解」とコストの最適化

AI活用による自動化で
脆弱性診断のコストと工数を抑える



予算や人材には限りがあるため、既存対策である
「脆弱性診断」は自動化し、コストを最適化

限られた予算と人材を
未知のリスクへの備えに集中投資



脆弱性診断のコストを抑えることで、限られた
予算と人材を本当に必要なところに回す

【結論】 防御に必要なのは、セキュリティ専用AI

フロンティアAI時代の防御に必要なのは、汎用的なフロンティアAIで対抗することではなく、Web巡回・脆弱性診断に特化し、「網羅性・再現性・継続性」を仕組みで担保できるセキュリティ専用AIです。



**確実なロジックで
脆弱性診断を自動化**

攻撃速度に追従し
自ら探索・診断・判断できる



**URLを設定するだけで
自動巡回**

Web巡回・認証突破・動的診断に
対応した知識と機能を持つ



**専門知識や
プロンプトスキル不要**

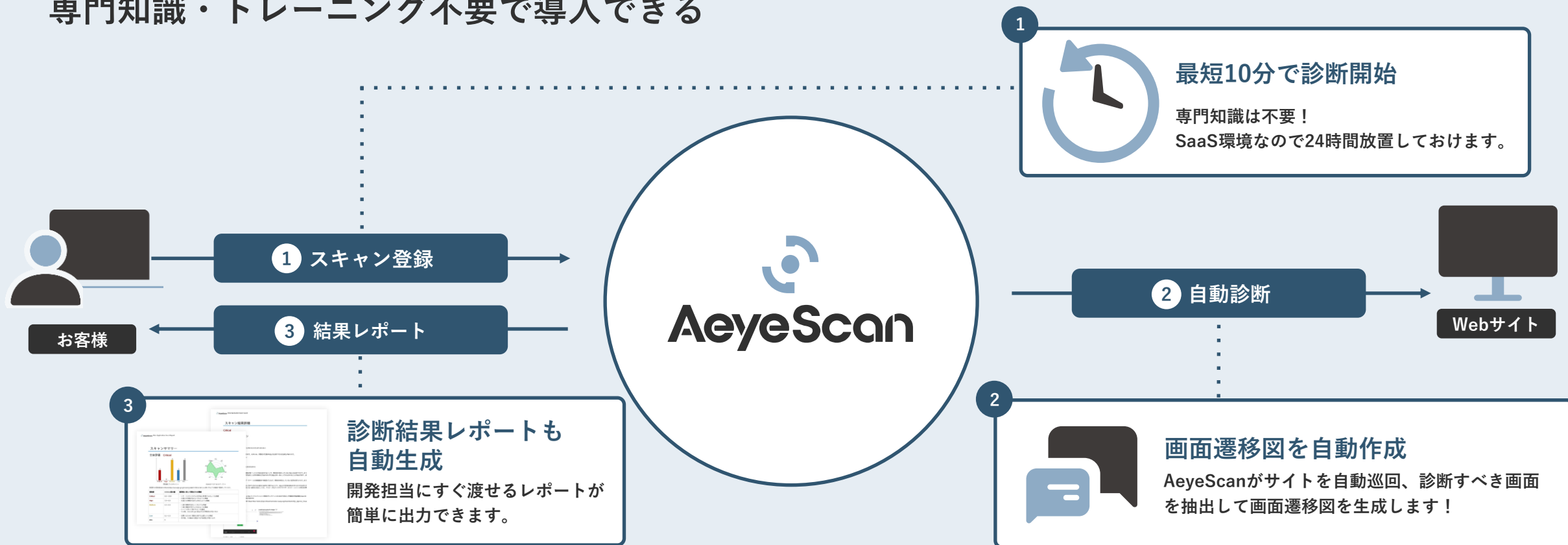
学習コストゼロで現場で使え
継続運用できる

基本の対策を自動化することで、コストの最適化ができる

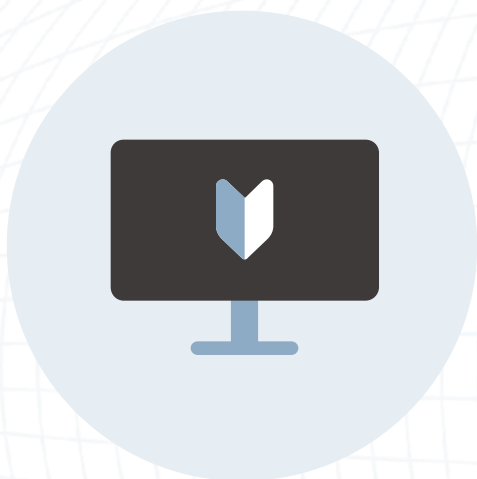
セキュリティ専用AIなら クラウド型Webアプリケーション脆弱性診断ツール「AeyeScan」

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。

 **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
500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2026」SaaS型Webアプリケーション脆弱性診断・管理市場: ベンダー別売上金額シェア (2024年度実績)

プロが認める品質・精度



ブラウザ上での直感的な操作

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

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

インフラ※



エンタメ



メディア



製造



金融



人材・教育



SaaS



SI・IT企業



セキュリティ企業



※公共および社会・生活基盤までを包含

社名五十音順（導入いただいた企業様の一部です）会社名及びロゴは各社の商標または登録商標です

フロンティアAI時代に必要な「面」の防御を、迅速かつ低コストで実施

専門家品質の高精度な脆弱性診断を、仕組みとして自動化。

フロンティアAIでは難しい網羅的・再現性のある自動診断が、社内に必要なタイミングに実施できます。

網羅的な「面」の
防御ができる



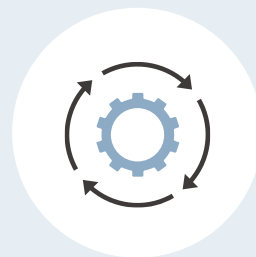
認証機能のある画面も
自動巡回して網羅性を担保

属人化せず、現場で
運用できる



非エンジニアでも
簡単な操作で実施できる

仕組み化で
無理なく継続できる



開発プロセスに組み込み
自然に実行される仕組みへ

コストと工数を
最適化できる



外注による診断と比較して
コスト・工数を削減

導入事例紹介

日本経済新聞社 様



企業名 株式会社日本経済新聞社

事業内容 新聞を中核とするメディア・情報サービス事業

従業員数 3,023名 (2025年12月31日現在)

課題

プロダクトの内製化により
リリースサイクルが高速化し
定期診断だけでは追いつけない状況だった

具体的な課題

- ① 内製化・アジャイル開発により、リリースや更新の頻度が高まっていた
- ② 年1回の定期診断では、リリース間のセキュリティチェックに限界があった
- ③ 外注では調整・再診断の負担が大きい

プロダクトの内製化に伴い、開発スピードが高まり、短いサイクルでリリース・更新するプロダクトも増加。従来の年1回の定期診断や外部委託による診断では、こうしたスピードに対応しきれないことが課題となっていた。

導入

標準に基づく網羅的な診断と
全プロダクトに適用しやすい点を評価し
AeyeScanの導入を決定

導入の背景

- ① 言語やフレームワークに依存せず、幅広いプロダクトに適用できる
- ② 除外範囲を細かく設定でき、実サービスに影響を与えにくい
- ③ 標準に基づき、網羅的に検証できる

シフトレフトやDevSecOpsの推進に向け、開発プロセスの中でセキュリティチェックを行う仕組みを整備。AeyeScanは、標準に基づく網羅的な診断や、幅広いプロダクトへの適用しやすさを評価して導入した。

効果

開発チームが
自律的に診断できる体制を整え
社内のセキュリティ文化の醸成を後押し

具体的な効果

- ① 月1回の定期診断により、リリース間のチェックを強化
- ② 開発者が自ら脆弱性を見つけ、修正につなげられるようになった
- ③ 診断・修正・共有のプロセスを改善

AeyeScanの導入により、開発チームが月1回のペースで診断を実施できる体制を構築。診断手順の整備や勉強会なども進め、開発者にセキュリティ文化を根付かせる一助となっている。

導入事例紹介

ゲオホールディングス 様



企業名 株式会社ゲオホールディングス

事業内容 メディア事業・リユース事業・オフプライス事業・モバイル事業など

従業員数 連結6,512名 (2025年8月時点)

課題

事業が成長していくスピードに
合わせた診断が困難に

具体的な課題

- 1 診断対象のWebアプリケーション数が拡大
- 2 外注では調整やコストの面が課題に
- 3 セキュリティ室が社内で診断するのは業務負荷がかかる

全国2,000を超える「ゲオ」店舗での販売を支えるシステムや、オンライン販売を行うWeb・スマホアプリが拡大し、アタックサーフェイスも増加。診断は外注していたが、事業成長のスピードに追いつかなくなっていた。

導入

開発チームでも使いこなせる
使い勝手の良さを評価

導入の背景

- 1 グラフィカルな画面遷移図で、どこにどんな脆弱性があるかわかりやすい
- 2 マニュアルがなくても操作できる
- 3 SaaS形式で容易に導入できる

複数ツールを比較し「安価だが診断内容がシンプルすぎる」「昔ながらのインターフェイスで開発者が使いづらい」など、決め手に欠けていた。そのような中、AeyeScanの操作性の良さを高く評価し、導入を決定。

効果

開発者主導の診断体制を確立し
コスパよくスピーディーな診断を実現

具体的な効果

- 1 開発チームが最小の工数で診断できる
- 2 短期間での開発・リリース案件でも間に合うスピーディーな診断を実現
- 3 開発者とのコミュニケーション補助ツールとしても活躍

導入当初はセキュリティ室がメインで診断を行い、徐々に開発チームへと展開を進めていった。外注時と比較して、コスパよくスピーディーに診断が行えることに加え、社内のセキュリティ意識も向上している。

導入事例紹介

ベルーナ様



企業名 株式会社ベルーナ

事業内容 アパレル・雑貨事業、プロパティ・ホテル事業など

従業員数 連結 3,884名 (2025年3月31日現在)

課題

事業の多角化で増加する
数十ものWebサイトに対し
均質な診断を実施するのが難しい

具体的な課題

- 1 外部委託ではコストがかさみ、診断範囲を限定せざるを得ないことも
- 2 全体で一定水準以上の品質を保ちたい
- 3 毎回異なる事業者に依頼しており調整の手間もかかる

多様な事業を展開する中、Webサイトは重要な顧客接点だが、増え続けるWebサイト全体に同一レベルの対策ができていなかった。内製のほうがコスト効率がよく、セキュリティ面でもよい選択ができると考えた。

導入

サブスクリプション形式で
使い勝手や診断品質にも優れた
AeyeScanを採用

導入の背景

- 1 シナリオ作成から診断の実施、レポート作成まで簡単にできる
- 2 画面遷移図で診断中の箇所やスキャン結果がわかりやすく示される
- 3 診断品質も十分なレベルに達している

AIを活用した他の診断ツールも試した上で、設定の簡単さなど、使いやすさを評価。トライアルを行い、以前受けたベストエフォート型診断サービスと比較しても診断品質が十分だと判断し、AeyeScanを採用。

効果

すべての事業に均質な診断を実現
診断回数を増やししながら
コストが半減

具体的な効果

- 1 網羅的な定期診断と、改修時のスポット診断を内製で実現
- 2 修正、再診断までのスピードが向上
- 3 セキュリティを標準化しつつ、費用、時間、工数の最適化が実現

導入後は、事業全体で横断的な診断が可能に。分かりやすいレポートにより改修スピードが向上し、診断回数を増やしつつ、コストは半分以下に削減。セキュリティの標準化とリソース最適化を実現できた。

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

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	70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





AeyeScan

セキュリティに、確かな答えを。