高性能AI時代のサイバーセキュリティ

人力運用から AI活用型防御 への転換

AeyeSecurityLab

本資料の目的

いま、ビジネスにおけるAIの性能は急速に進化しています。
一方で、高性能AIがサイバー攻撃に悪用されることで、
システムの脆弱性が発見されてから攻撃に至るまでの時間は劇的に短縮され、
従来の人力中心のセキュリティ対策では対応が極めて困難な状況に陥りつつあります。
攻撃者による高度化・高速化した脅威に対抗するためには、
人力中心の運用だけではもはや限界を迎えているといわざるをえません。

いま、企業に強く求められているのは、
継続的な脆弱性管理・リスク評価・修正対応をプロセスとして回し続けること、
そして防御側もまた「AI」を組み込んだセキュリティ体制へと転換することです。

そこで本資料では、高性能AIによって激変するサイバー攻撃の最新現状と、
AI時代に企業が備えるべき新たなセキュリティ対策の思考法、
さらにAIの脅威に対抗するための具体的な「AI活用型防御」について解説します。
貴社のセキュリティ戦略をアップデートする一助として、ぜひ最後までご一読ください。

「Claude Mythos Preview」の衝撃

セキュリティ業界だけでなくビジネス界全体で、Anthropic（アンソロピック）社が発表した最新AI「Claude Mythos Preview（クロード・ミュトス・プレビュー）」が大きな注目を集めています。

「Claude Mythos Preview」の概要

目的

未知の脆弱性発見を人力からAI主体へ転換

従来は人間のスキルと長時間の手動検証が必要だった

従来のAIとの違い

生成AIから、“自律型サイバーAI”へ進化

人間の指示待ちではなく、自ら探索・判断・検証を行う

性能

人間を凌駕する速度で発見・検証

何十年も潜んでいた未知の脆弱性（ゼロデイ）を高速・自律的に見つける

高性能AIによって、サイバー攻撃は大きく変化する

高性能AIを悪用した攻撃は、過去の「延長線」にある

AIを使って脆弱性を発見する取り組みは数年前から存在しており、「AIを悪用したサイバー攻撃」も過去から着実に進化を続けてきた歴史の延長線にあります。

Phase1

AI＝効率化ツール

- フィッシングメール自動作成
- マルウェア量産
- ディープフェイク詐欺

攻撃作業の自動化

Phase2

AI＝探索支援

- 脆弱性候補の洗い出し
- コード解析支援
- 攻撃シナリオ生成

攻撃判断の高速化

Phase3

自律型サイバーAI

- AIによる自律的な探索
- 脆弱性の発見/検証
- 攻撃まで高速実行

攻撃そのものの自律化

高性能AI時代、セキュリティは「継続運用」が前提に

高性能 AI が攻撃者に悪用されることにより、脆弱性の発見から悪用までの時間は急速に短縮。
企業には継続運用を前提とした防御体制が求められています。

攻撃者×高性能AI

- 脆弱性発見が高速化
- 悪用までの時間が短縮
- 同時多発的な攻撃が増加

AIにより攻撃サイクルが高速化

企業×継続運用

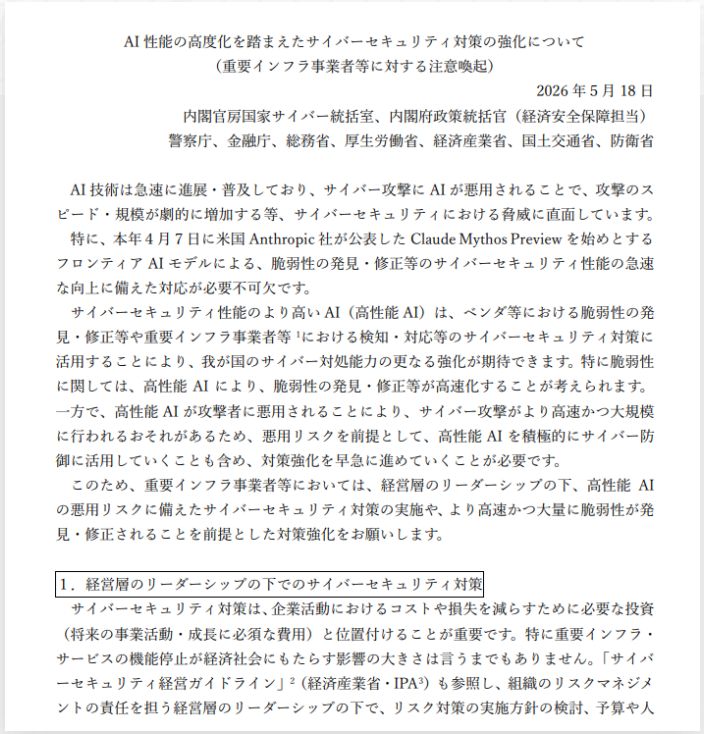
- 継続的な資産管理
- 脆弱性情報の収集
- リスク評価
- 優先順位付け
- 継続的な修正対応

継続的な脆弱性管理体制が必要

参考：「AI 性能の高度化を踏まえたサイバーセキュリティ対策の強化について」https://www.cyber.go.jp/pdf/press/20260518_AI_CS_Critical_Infrastructure.pdf

政府も高性能AI時代への前提変更を始めている

内閣官房の「国家サイバー統括室」は、 Anthropic社の「Claude Mythos Preview」の登場を念頭に、政府全体の対策パッケージ『Project YATA-Shield』を取りまとめました。



AI 性能の高度化を踏まえたサイバーセキュリティ対策の強化について
（重要インフラ事業者等に対する注意喚起）

2026 年 5 月 18 日
内閣官房国家サイバー統括室、内閣府政策統括官（経済安全保障担当）
警察庁、金融庁、総務省、厚生労働省、経済産業省、国土交通省、防衛省

AI 技術は急速に進展・普及しており、サイバー攻撃に AI が悪用されることで、攻撃のスピード・規模が劇的に増加する等、サイバーセキュリティにおける脅威に直面しています。
特に、本年 4 月 7 日に米国 Anthropic 社が公表した Claude Mythos Preview を始めとするフロンティア AI モデルによる、脆弱性の発見・修正等のサイバーセキュリティ性能の急速な向上に備えた対応が必要不可欠です。
サイバーセキュリティ性能のより高い AI（高性能 AI）は、ベンダ等における脆弱性の発見・修正等や重要インフラ事業者等[1]における検知・対応等のサイバーセキュリティ対策に活用することにより、我が国のサイバー対処能力の更なる強化が期待できます。特に脆弱性に関しては、高性能 AI により、脆弱性の発見・修正等が高速化することが考えられます。
一方で、高性能 AI が攻撃者に悪用されることにより、サイバー攻撃がより高速かつ大規模に行われるおそれがあるため、悪用リスクを前提として、高性能 AI を積極的にサイバー防御に活用していくことも含め、対策強化を早急に進めていくことが必要です。
このため、重要インフラ事業者等においては、経営層のリーダーシップの下、高性能 AI の悪用リスクに備えたサイバーセキュリティ対策の実施や、より高速かつ大量に脆弱性が発見・修正されることを前提とした対策強化をお願いします。

1．経営層のリーダーシップの下でのサイバーセキュリティ対策
サイバーセキュリティ対策は、企業活動におけるコストや損失を減らすために必要な投資（将来の事業活動・成長に必須な費用）と位置付けることが重要です。特に重要インフラ・サービスの機能停止が経済社会にもたらす影響の大きさは言うまでもありません。「サイバーセキュリティ経営ガイドライン」[2]（経済産業省・IPA[3]）も参照し、組織のリスクマネジメントの責任を担う経営層のリーダーシップの下で、リスク対策の実施方針の検討、予算や人

ポイント

1. **経営層のリーダーシップの下でのサイバーセキュリティ対策**
   セキュリティを必要投資と捉え、予算・人材確保・リスク管理を実施
2. **基本的なサイバーセキュリティ対策の確実な実施及び更なる対策の強化**
   基本対策に加え、ゼロトラスト・脅威検知・AI活用など対策を強化
3. **高性能AIにより高速化する脆弱性の発見・修正等への対応**
   継続的な脆弱性対応と資産管理、リスク評価・優先順位付けを実施

参考：「AI 性能の高度化を踏まえたサイバーセキュリティ対策の強化について」https://www.cyber.go.jp/pdf/press/20260518_AI_CS_Critical_Infrastructure.pdf

攻撃者がAIを使うなら、守る側もAIを使うのは「当然の前提」

人間の手作業や、年1～2回の定期的な脆弱性診断（手動）だけで、24時間365日休みなく進化・巡回し続ける攻撃者に対抗することは、物理的に不可能です。

攻撃者×高性能AI

- 24時間365日の攻撃
- 自律的に探索/攻撃

企業×継続運用

- 年1、2回の定期診断
- 人力で時間をかけて作業

人力前提の防御は、すでに限界を超えている

では、汎用AIによる社内診断で防御はできるのか

防御側も、AIを使わなければ太刀打ちできなくなっていはいるものの、汎用AI（LLM）を使った社内診断だけでWebアプリケーションを守ることは不可能といえます。

汎用AIによる社内診断の限界

静的ソースコードしかレビューできない

実際の攻撃は動的環境で行われるが、静的なソースコードしか見れない

嘘や誤検知・見落としがある

安全でも危険と判断したり隠された脆弱性を見落とすことがある

プロンプトスキルが属人化する

精度の高い回答を引き出すためには専門家のチューニングが必要

認証・画面巡回に壁がある

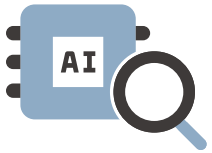
ログインや認証が必要な画面を自律的に巡回・診断できない

汎用AIではなく、Web巡回・診断に特化したセキュリティ専用AIによる「AI活用型防御」が必要

高性能AI攻撃時代に求められる「AI活用型防御」

高性能AIを悪用した攻撃が増加する時代に必要なのは、単なる生成AIでなく、Web巡回・診断・継続運用まで実行できるセキュリティ専用AIです。これにより「AI vs AI」のセキュリティ体制を構築できます。

いま企業に有効なAI活用型防御とは

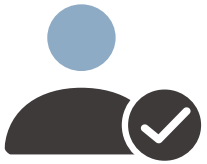


高性能かつ自律型

攻撃速度に追従し
自ら探索・診断・判断できる

セキュリティ専用

Web巡回・認証突破・動的診断に
対応した知識と機能を持つ



専門知識が不要

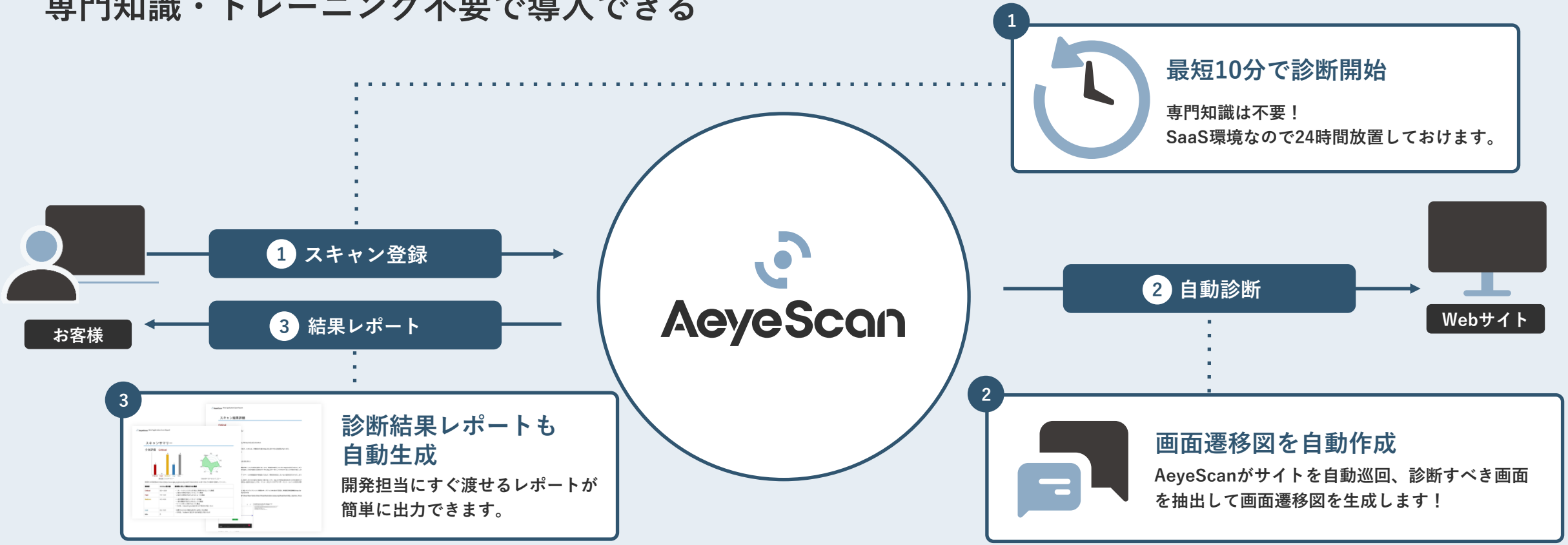
高度なプロンプト技術なしで
継続運用できる

AeyeSecurityLab

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（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

AeyeSecurityLab

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※

EPARK / AIRE / HIS / H2O RETAILING / NTT EAST / odakyu / 近鉄情報システム株式会社 / GEO / SymEnergy シン・エナジー / 水ing Swing Corporation / Suzuyo / TOYOTA HOME / NANKAI 南海システムソリューションズ / 日本調剤 / JARMeC 日本動物高度医療センター / HITOWA GROUP / BOOK・OFF / ベルーナ / grow up together MEDIA / Looop / Loyalty Marketing, Inc.

エンタメ

イープラス / CAPCOM / GungHo Online Entertainment, Inc. / とらラボ! TORANOANA LABORATORY / BookLive

メディア

集英社 / 中日新聞 / 東海テレビ / NIKKEI / Media Do

製造

AICA / AISIN / KITZ 株式会社キッツ / KOSÉ / SAKI / TIGER / TEIJIN / Denkei / House / Mizuno / ユーグレナ

金融

アイフル / UPSIDER / MS&AD / MS&ADインターリスク総研 / JOBPAY / SOMPOひまわり生命 / DMM FinTech / Tokyo Century / Net Protections

人材・教育

OHSAWA DRIVING SCHOOL / 河合塾 / Junion / JINSOKEN / ZENKIGEN / Direct Sourcing / PERSOL / 立教大学 / Leverages / workport

SaaS

Advanced Media, Inc. 株式会社アドバンスト・メディア / Lexica E-Retailing Platform / エフアンドエムネット株式会社 / M-aid / エムティーアイ / OZ INTER NATIONAL / giftee* / Classi / COACH A Co.,Ltd. / cybozu / Speee / SecureNavi / Diamond head / DMM Boost / TAL / Digital Garage / TEMONA / NAVITIME / KNOCK ON THE DOOR / BATONZ / VALUE HR / freee / vector / porters / hokan / Money Forward / RUN.EDGE / RVSTA 株式会社リバスタ / Rescuenow

SI・IT企業

Rworks / アクモス株式会社 / AVANT GROUP / Insight Edge / Infcurion / 80&Co. / SBWorks / NTT Integration / NTT DATA / NTTビジネスソリューションズ / OMRON / Globalway / KDDI Agile Development Center / circlace / さくら情報システム / SUNDAY SYSTEMS / CEC / GA TECHNOLOGIES / Simplex Inc. / 777WORKS / SOFT CREATE / SOLTEC / 高千穂交易株式会社 / TDI / 電通総研 / TOPPAN / JOPS / JAST / PCNET / Human Interactive Technology Inc. / FUJISOFT / FUJITSU / MACROMILL / MITSUBISHI ELECTRIC / YONA / リピスト

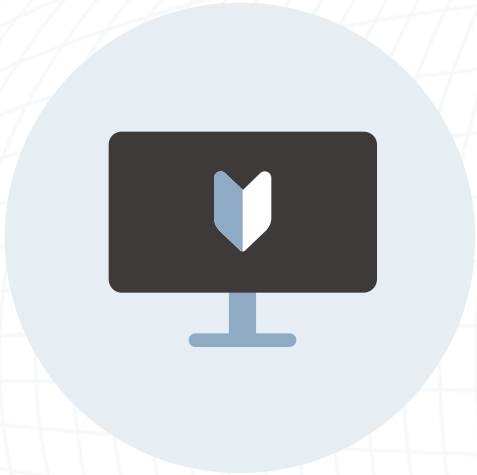
セキュリティ企業

NEC NECセキュリティ / NTT DATA / GSX / cybertrust / LAC

※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

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。

AeyeSecurityLab

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付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

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

TOPPANデジタル 様

企業名　TOPPANデジタル株式会社

事業内容　TOPPANグループ全体のDX事業戦略策定、DX事業の創出・推進等

従業員数　811名（2024年4月1日現在）

課題

開発チームごとに
脆弱性診断の体制が異なり、
手戻りが発生していた

具体的な課題

1. チーム間で診断の運用にばらつきがあった
2. ホールディングスによる診断で脆弱性が発見され、手戻りが発生
3. 修正後の再診断が順番待ちになり、リリーススケジュールが見直しになることも

新たなWebアプリやサービスは、ホールディングス情報セキュリティ本部による診断を経なければリリースできないルールになっている。しかし、開発チームごとに運用のばらつきがあることで、手戻りが発生していた。

導入

直感的なGUI、診断精度の高さ、
SPA対応などを総合評価し採用

導入の背景

1. 診断結果が見やすく、対策方針が明確
2. 診断精度や自動化機能が他のサービスと比較して優れていた
3. チーム・ドメインごとに閲覧権限を制御できる

脆弱性を含んだサイトでのトライアルをはじめ、複数の診断ツールを比較検討。SPAへの対応や診断精度、自動化機能、UI、日本語対応、コスト、運用性の観点で総合的に高評価だったAeyeScanを採用した。

効果

脆弱性診断を全社標準化し、
手戻りを解消
グループの出荷前診断工数も75%削減

具体的な効果

1. 最長で1ヶ月かかっていた診断が、数日で完了するようになった
2. 自分たちのペースで実施可能なので、スケジュール調整が不要になった
3. 診断結果を共有することで、ホールディングス側の出荷前診断の工数も削減

導入後は、開発チームにもスムーズに浸透し、それまで脆弱性診断を実施してこなかったチームを中心に活用が進んだ。チーム単位の効率化はもちろん、ホールディングスと連携し、グループ全体の工数削減にも貢献。

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なの？
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	66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

セキュリティに、確かな答えを。