AeyeSecurityLab

DX時代の人手をかけない Webセキュリティマネジメント実践

― 失敗しない脆弱性診断内製化の進め方 ―

AeyeSecurityLab

登壇者紹介

株式会社エーアイセキュリティラボ

事業企画部 ディレクター **阿部 一真**（あべ かずま）

新卒でNTTデータに入社し、Salesforceビジネス推進部門で
コンサルティングセールス・カスタマーサクセスを経験。
その後、AIベンチャー企業・SaaSスタートアップ企業にてCS責任者
およびプロダクトマネージャー・事業統括責任者を歴任し、エーアイ
セキュリティラボに入社。
現在はCXチームでの活動に加え、新規プロダクト企画・海外事業
展開など全社横断プロジェクトにも携わる。

あらたな答えを、つぎつぎと。

変化の激しいサイバーセキュリティの世界。

私たちは、未知の課題が生まれるたび、培った知見と経験・実績をもとに、
「あらたな答え」を世の中に提供し続けていきます。

世界も驚くような、技術の力で。

そして、サイバーセキュリティの進化を通して、
人は、人にしかできない、創造性を活かした仕事に注力できる、
社会の進化にも貢献していきます。

AeyeSecurityLab

AeyeSecurityLab

誰でも簡単に

プロさながらの高度な
脆弱性診断を

AeyeScan

そのセキュリティ対策で
DX時代を乗り超えられるか？

DXの進展でセキュリティ対策の需要は高まっている

デジタルサービスの開発・提供
自社で管理すべきデジタル資産
増

×

急速な技術の進化

＝

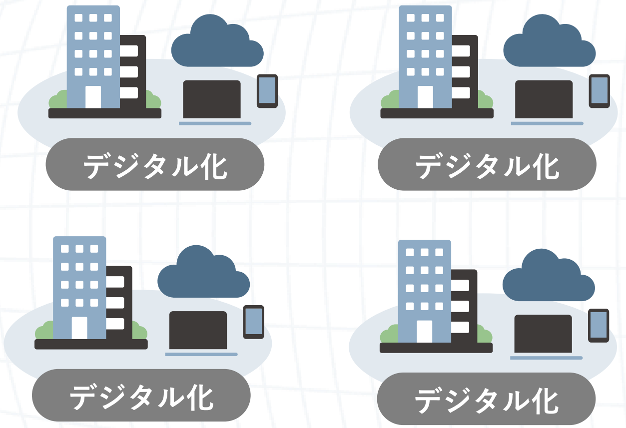
必要なセキュリティ対策の

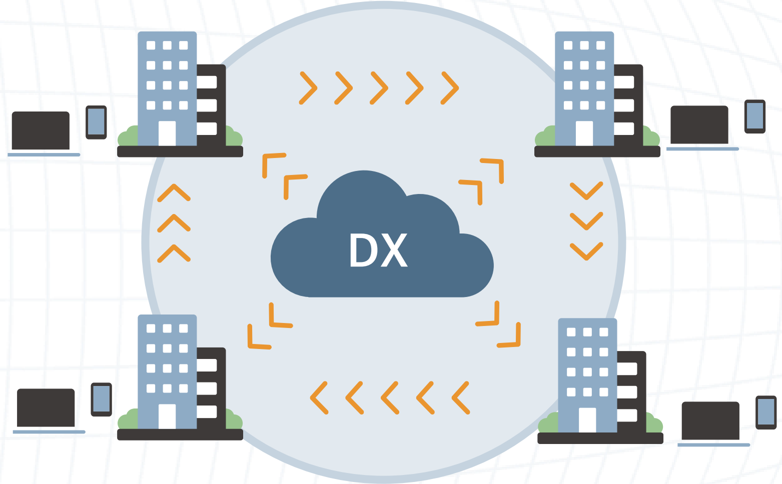
対応範囲は拡大

難易度は上昇

DX時代のセキュリティ強化における問題

① 対応範囲の拡大：サプライチェーンリスクの増大





DX初期：社内業務のデジタル化

セキュリティ対策が不十分な
「即席デジタル」の乱立

DX中期：企業間連携のデジタル化

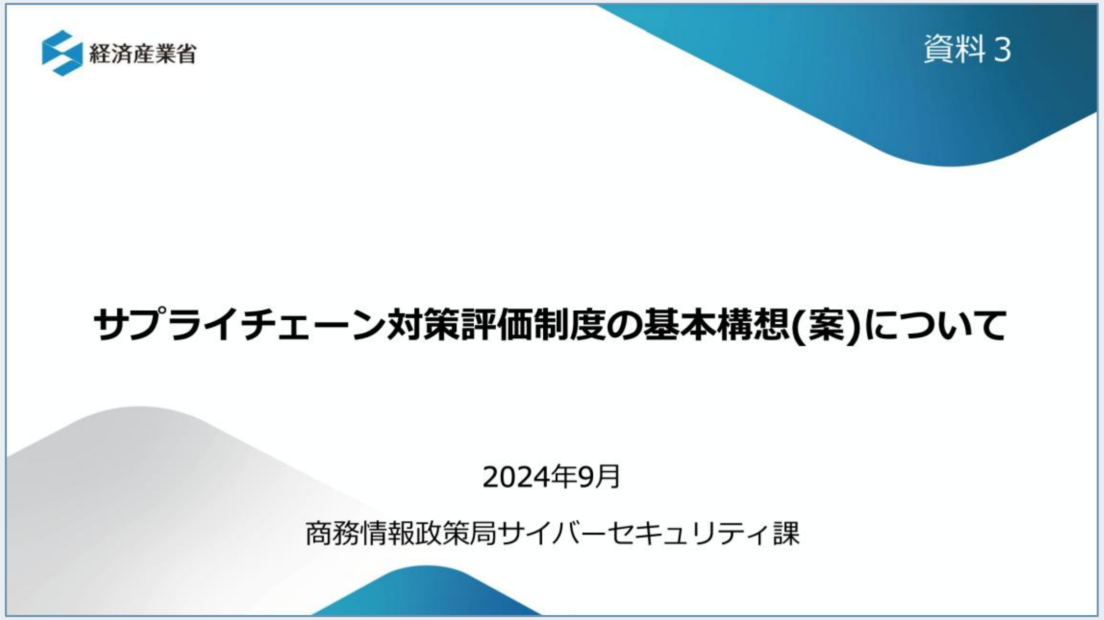
「即席デジタル」との連携で
サプライチェーン全体が脆弱化

AeyeSecurityLab

サプライチェーン対策評価制度の基本構想(案)

制度の目的

- サプライチェーン企業、ひいてはサプライチェーン全体の強靭性(事業継続性に加えてデータ保護を含む)の確保
- 対策要求の共通化を通じたサプライチェーン対策の重複排除、対策状況の可視化による確認の効率化


経済産業省

資料３

サプライチェーン対策評価制度の基本構想(案)について

2024年9月

商務情報政策局サイバーセキュリティ課

セキュリティ対策を３段階で評価

取引先のセキュリティ対策レベルを可視化

自社のセキュリティ対策水準と目標を明確化

参考：サプライチェーン対策評価制度の基本構想(案)について https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_supply_chain/pdf/002_03_00.pdf

DX時代のセキュリティ強化における問題

② 難易度の上昇：セキュリティ対策項目は増え、より深い技術知見が必要

Webアプリケーションのセキュリティ対策

① ファイルの公開設定
② Webページの公開設定
③ 脆弱性への対策
④ ソフトウェアの脆弱性対策
⑤ エラーメッセージの設定
⑥ ログ管理
⑦ 暗号化
⑧ 不正ログインへの対策

Webサーバのセキュリティ対策

⑨バージョンアップを行う
⑩ 不要なサービス・アプリケーションの停止
⑪ 不要なアカウントの削除
⑫ 安全なパスワードの設定
⑬ アクセス制御
⑭ ログ管理

ネットワークのセキュリティ対策

⑮ 不要な通信の遮断
⑯ 通信のフィルタリング
⑰ 不正な通信の検知・遮断
⑱ ログ管理

その他のセキュリティ対策

⑲ クラウドサービスへのセキュリティ対策
⑳ Webアプリケーション・Webサーバ・ネットワークへの定期的な脆弱性診断

正直、全部やるのは無理…

引用元：https://www.ipa.go.jp/security/vuln/websecurity/sitecheck.html 安全なウェブサイトの運用管理に向けての20ヶ条 ～セキュリティ対策のチェックポイント～

セキュリティ対策の課題を克服する「戦略的」思考

セキュリティ対策の「戦略的」思考

「戦略的な」セキュリティ対策とは・・・

濃淡をつける・取捨選択する・選択と集中

手間と時間をかけて
専門家が対応する

人的リソースを最小化
しつつ対応する

濃 ⟷ 淡

戦略的なセキュリティ対策を実行する上での課題

手間と時間をかけて
専門家が対応する

濃 ⟷ 淡

人的リソースを最小化
しつつ対応する

課題①

専門人材は限られているが、技術的に人間が
対応しなければいけない範囲が広い

課題②

継続的・網羅的に対応する必要があるが、
割ける人的・金銭的リソースは限定的

AIを活用した「自動化・内製化」で解決できないか？

個別のセキュリティ対策・施策から「まずAIを使ってみる」

法令遵守

- デジタル関連法令対応
- コンプライアンス対応
- 業界のセキュリティガイドラインへの準拠

…etc

ミスができない領域
人が考えて対応すべき

ガバナンス強化

- 事業特性に応じたセキュリティポリシーやガイドライン作成
- セキュリティ対応マニュアルの整備と実行管理

…etc

関係者が多く影響範囲が広い
人の精緻な設計が必要

具体的な対策

- セキュリティ製品やサービスの導入
- システム面のサイバー攻撃対策
- 脆弱性診断

…etc

目的と方法を決めれば
対策にAIを組み込める

AIと相性の良いセキュリティ対策：脆弱性診断

継続的・永続的に対策が必要	⟷	人力では生産性が上がらない
網羅的に診断することが望ましい	⟷	網羅性を高めると費用も増える

AIによる自動化・内製化ができれば

業務の効率化・費用の最適化につながりやすい

AIを活用した
脆弱性診断の内製化

脆弱性診断を自動化・内製化するときに考えること

「内製化できればいいんだけどな…」

?

診断の**品質を維持**

できるだろうか？

?

コスト(費用・時間)

を抑えられるか？

?

社内メンバーで対応

できるだろうか？

AeyeSecurityLab

脆弱性診断を自動化・内製化するときに考えること

?
診断の**品質を維持**
できるだろうか？

?
コスト（費用・時間）
を抑えられるか？

?
社内メンバーで対応
できるだろうか？

＋

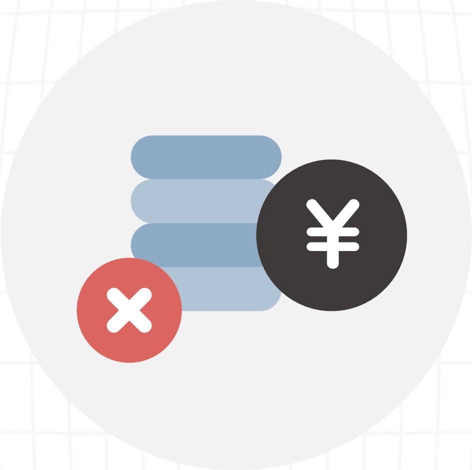
事業部門・開発部門に内製化の協力を得られるか？

実際に事業部門と向き合う中で直面する「壁」

課題 1

稼働を割きたくない

診断に時間を取られたくない
スケジュール調整したくない
なるべく対応したくない



課題 2

コストをかけたくない

計画にセキュリティコストを含めていない
診断環境を用意したくない

課題 3

セキュリティ意識が低い

診断とは何をするものなのかがわからない
セキュリティを意識しようと思っていない

脆弱性診断の自動化・内製化に必要な要素とは？

① 脆弱性診断のプロセスに
事業部門を巻き込む

② AIを活用した脆弱性診断
ツールの導入

脆弱性診断の自動化・内製化に必要な要素とは？

① 脆弱性診断のプロセスに事業部門を巻き込む

事業部門とセキュリティ部門で一緒に脆弱性診断を行うことのメリットを訴求

早期に脆弱性を発見することで
開発終盤での手戻りを最小化できる
（シフトレフト）

業務やサービス仕様に詳しいチームが
診断に参加することで
診断の精度・網羅性が上がりやすい

AeyeSecurityLab

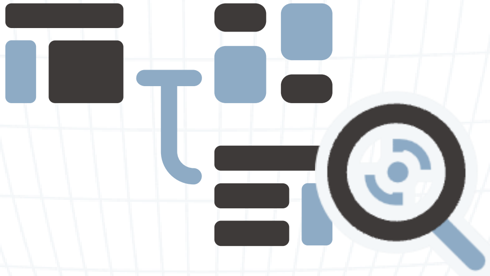
脆弱性診断の自動化・内製化に必要な要素とは？

② 脆弱性診断ツールの導入

事業部門を巻き込む前提で考えた場合、ツール選定に必要なポイントは…

1 誰でも使える操作性

2 利用範囲に制限がない



3 結果がわかりやすい

AeyeSecurityLab

脆弱性診断の内製化を進める具体的なステップ

脆弱性診断内製化のポイント

脆弱性診断の内製化は、STEP 0～5の段階に分けて考えることができます。

STEP 0		運用体制の構築・役割分担
STEP 1	情報収集	情報収集・対象の把握
STEP 2	検討	診断の必要性や優先順位を評価、対応方針の検討
STEP 3	実行	診断計画の立案と実行・進捗の全体管理
STEP 4	修正	検出された脆弱性の評価と対応
STEP 5	運用	診断状況の報告・方針の見直しと全社最適

AeyeSecurityLab

脆弱性診断内製化のポイント

脆弱性診断の内製化は、STEP 0～5の段階に分けて考えることができます。

STEP 0		運用体制の構築・役割分担
STEP 1	情報収集	情報収集・対象の把握
STEP 2	検討	診断の必要性や優先順位を評価、対応方針の検討
STEP 3	実行	診断計画の立案と実行・進捗の全体管理
STEP 4	修正	検出された脆弱性の評価と対応
STEP 5	運用	診断状況の報告・方針の見直しと全社最適

STEP 0 運用体制の構築・役割分担

従来の運用体制

セキュリティ部門が
まとめて診断

事業部門 → 依頼 → セキュリティ部門
開発部門 → 依頼 → セキュリティ部門
セキュリティ部門 → 診断

これからの運用体制

事業部門・開発部門が
脆弱性診断を実施できる
体制を構築

セキュリティ部門 → 支援 → 事業部門 → 診断
セキュリティ部門 → 支援 → 開発部門 → 診断

メリット

- シフトレフトの実現
- 診断対象の的確な把握
- セキュリティ意識の醸成

AeyeSecurityLab

脆弱性診断内製化のポイント

脆弱性診断の内製化は、STEP 0〜5の段階に分けて考えることができます。

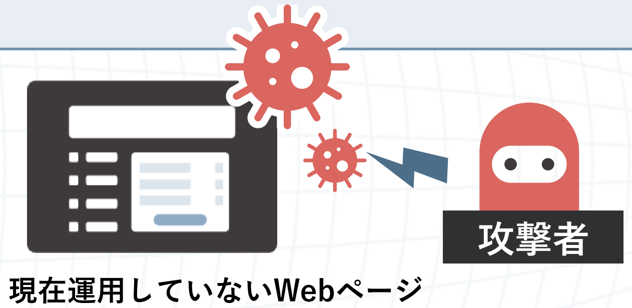
STEP 0		運用体制の構築・役割分担
STEP 1	情報収集	情報収集・対象の把握
STEP 2	検討	診断の必要性や優先順位を評価、対応方針の検討
STEP 3	実行	診断計画の立案と実行・進捗の全体管理
STEP 4	修正	検出された脆弱性の評価と対応
STEP 5	運用	診断状況の報告・方針の見直しと全社最適

STEP 1 情報収集・対象の把握

必要に応じてASMツールも活用しながら、診断対象の全体把握が重要

某大手ハウスメーカー（A社）さまの事例

某日、A社が運営サイトのアクセスが急増し、高負荷状況に…
調査した結果、過去に3年程度オープンしていたWebサイトの現在は運用していないページが攻撃を受けていたことが判明



ページが公開されていたこと、アクセス可能であることは認識されていたのか？

気付いたら「さくっと」Webサイトができている…	開発後・リリース後も検証環境やテスト環境がひっそり残っている…

脆弱性診断内製化のポイント

脆弱性診断の内製化は、STEP 0〜5の段階に分けて考えることができます。

STEP 0		運用体制の構築・役割分担
STEP 1	情報収集	情報収集・対象の把握
STEP 2	検討	診断の必要性や優先順位を評価、対応方針の検討
STEP 3	実行	診断計画の立案と実行・進捗の全体管理
STEP 4	修正	検出された脆弱性の評価と対応
STEP 5	運用	診断状況の報告・方針の見直しと全社最適

AeyeSecurityLab

STEP 2 診断の必要性や優先順位を評価、対応方針の検討

スコープを明確にし、**優先順位・必要を評価して対策の濃淡をつける**ことが重要

診断対象の棚卸し

→

診断の必要性を評価

- 取り扱っている情報の重要度
- ビジネス上の重要度
- 監督官庁・業界団体のガイドライン
- リリース・アップデート頻度(開発体制)

→

対策方針の検討

診断方法

- 外部委託
- 社内診断(内製化)

診断タイミング

- 新規リリース
- 改修・追加開発
- 定期診断

脆弱性診断内製化のポイント

脆弱性診断の内製化は、STEP 0～5の段階に分けて考えることができます。

STEP 0		運用体制の構築・役割分担
STEP 1	情報収集	情報収集・対象の把握
STEP 2	検討	診断の必要性や優先順位を評価、対応方針の検討
STEP 3	実行	診断計画の立案と実行・進捗の全体管理
STEP 4	修正	検出された脆弱性の評価と対応
STEP 5	運用	診断状況の報告・方針の見直しと全社最適

AeyeSecurityLab

STEP 3 診断計画の立案と実行・進捗の全体管理

Webサイト・Webアプリを**開発している部門との情報連携・協業**が「ミソ」

診断計画を立てる

リリース前の診断

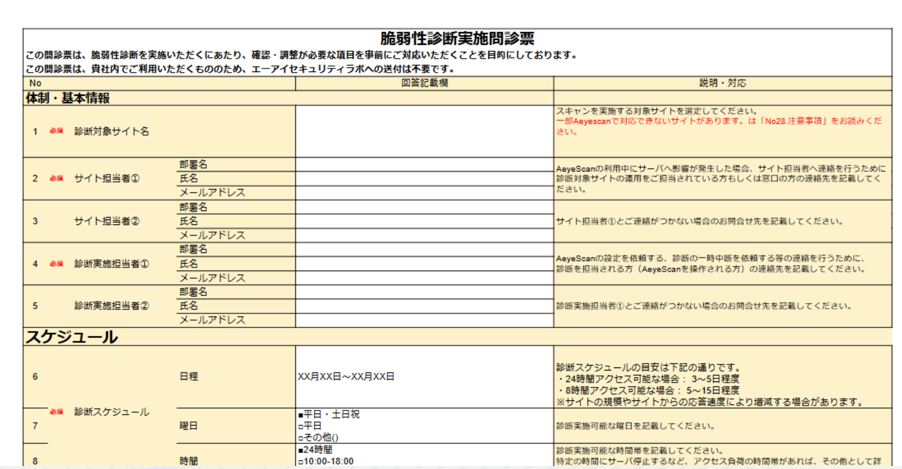
開発プロジェクトのキックオフ等に参加し、スケジュールを事前に確認しておく

定期診断

実施時期を各プロジェクトと事前に調整しておく

診断の実施準備をする

開発部門と情報連携し、診断要件を確認する



脆弱性診断実施問診票

この問診票は、脆弱性診断を実施いただくにあたり、確認・調整が必要な項目を事前にご対応いただくことを目的にしております。
この問診票は、貴社内でご利用いただくもののため、エーアイセキュリティラボへの送付は不要です。

No				回答記載欄	説明・対応
体制・基本情報					
1	必須	診断対象サイト名			スキャンを実施する対象サイトを選定してください。 一部Aeyescanで対応できないサイトがあります。は「No28.注意事項」をお読みください。
2	必須	サイト担当者①	部署名 氏名 メールアドレス		AeyeScanの利用中にサーバへ影響が発生した場合、サイト担当者へ連絡を行うために診断対象サイトの運用をご担当されている方もしくは窓口の方の連絡先を記載してください。
3		サイト担当者②	部署名 氏名 メールアドレス		サイト担当者①とご連絡がつかない場合のお問合せ先を記載してください。
4	必須	診断実施担当者①	部署名 氏名 メールアドレス		AeyeScanの設定を依頼する、診断の一時中断を依頼する等の連絡を行うために、診断を担当される方（AeyeScanを操作される方）の連絡先を記載してください。
5		診断実施担当者②	部署名 氏名 メールアドレス		診断実施担当者①とご連絡がつかない場合のお問合せ先を記載してください。
スケジュール					
6	必須	診断スケジュール	日程	XX月XX日～XX月XX日	診断スケジュールの目安は下記の通りです。 ・24時間アクセス可能な場合： 3~5日程度 ・8時間アクセス可能な場合： 5~15日程度 ※サイトの規模やサイトからの応答速度により増減する場合があります。
7			曜日	■平日・土日祝 □平日 □その他()	診断実施可能な曜日を記載してください。
8			時間	■24時間 □10:00-18:00	診断実施可能な時間帯を記載してください。 特定の時間にサーバ停止するなど、アクセス負荷の時間帯があれば、その他として詳

脆弱性診断内製化のポイント

脆弱性診断の内製化は、STEP 0～5の段階に分けて考えることができます。

STEP 0		運用体制の構築・役割分担
STEP 1	情報収集	情報収集・対象の把握
STEP 2	検討	診断の必要性や優先順位を評価、対応方針の検討
STEP 3	実行	診断計画の立案と実行・進捗の全体管理
STEP 4	**修正**	**検出された脆弱性の評価と対応**
STEP 5	運用	診断状況の報告・方針の見直しと全社最適

STEP 4 検出された脆弱性の評価と対応

評価の理由・根拠(特に対応不要とした場合)と、**対応履歴を残しておく**のが大事

診断結果の確認

→

修正対応の必要性を評価

- CVSS等の深刻度
- 発生しうる被害・リスクの大きさ
- 修正にかかるコスト(工数・費用)
- リリースまでに残された時間

など

→

対策方針の検討

- リリース前に必ず修正する
- 次回リリースまでに必ず修正する
- 大規模修正で修正
- 現時点では対応不要

脆弱性診断内製化のポイント

脆弱性診断の内製化は、STEP 0～5の段階に分けて考えることができます。

STEP 0		運用体制の構築・役割分担
STEP 1	情報収集	情報収集・対象の把握
STEP 2	検討	診断の必要性や優先順位を評価、対応方針の検討
STEP 3	実行	診断計画の立案と実行・進捗の全体管理
STEP 4	修正	検出された脆弱性の評価と対応
STEP 5	運用	診断状況の報告・方針の見直しと全社最適

AeyeSecurityLab

STEP 5 診断状況の報告・方針の見直しと全社最適

診断の予実と診断結果をもとに、**次年度以降の方針を見直し**、**最適化**するのが大事

経営層

セキュリティ関連施策の投資判断

全社情報セキュリティのリスクマネジメント

セキュリティ部門
情報システム部門

具体的な施策の決定
ルール策定・運用設計

セキュリティ対策関連の情報収集・集約

事業部門・開発部門
グループ会社

全社ポリシーに則ったセキュリティ対策

セキュアな開発
セキュアなサービス提供

経営層 → セキュリティ部門：戦略目標の定義 / リソース配分

セキュリティ部門 → 事業部門：ルール周知 / 技術サポート / 実行管理

事業部門 → セキュリティ部門：プロジェクトや対策状況の共有

セキュリティ部門 → 経営層：定期報告 / 施策検討・上申

脆弱性診断内製化のポイント

脆弱性診断の内製化は、STEP 0～5の段階に分けて考えることができます。

STEP 0		運用体制の構築・役割分担
STEP 1	情報収集	情報収集・対象の把握
STEP 2	検討	診断の必要性や優先順位を評価、対応方針の検討
STEP 3	実行	診断計画の立案と実行・進捗の全体管理
STEP 4	修正	検出された脆弱性の評価と対応
STEP 5	運用	診断状況の報告・方針の見直しと全社最適

自分たちだけで内製化するのは大変

でも AeyeScan なら…！

AeyeSecurityLab

生成AI時代の脆弱性診断なら AeyeScan

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※

※ 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2024」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）

有償契約
200社以上

お客様 → スキャン登録 → AeyeScan → 自動診断 → Webサイト

AeyeScan → 結果レポート → お客様

01 高精度なAI活用
巡回精度が高く
画面遷移図で見てわかりやすい

02 学習コストゼロ
開発やセキュリティの
知識がなくてもすぐに使える

03 業界標準対応
外部委託と遜色なく
内製化が可能

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。

AeyeScanが選ばれている理由

プロが認める機能・性能 × 誰でも使える操作性

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
AISIN / KOSÉ / saki / TIGER / Mizuno / ユーグレナ

インフラ
HIS / H₂O RETAILING / odakyu / 近鉄情報システム株式会社 / J.union / 水ing Swing Corporation / Suzuyo / NTT東日本 / HITOWA GROUP / Y MEDIA / Looop

金融
アイフル / JOBPAY / SOMPOひまわり生命 / DMM FinTech / Tokyo Century

メディア
集英社 / 中日新聞 / NIKKEI

エンタメ
イープラス / CAPCOM / とらラボ! TORANOANA LABORATORY

SaaS
estie / M-aid / エムティーアイ / OZ INTERNATIONAL / COACH A Co., Ltd. / cybozu / JINSOKEN / Schoo / Speee / SecureNavi / ZENKIGEN / Direct Sourcing / TAL / TEMONA / NAVITIME / KNOCK ON THE DOOR / BATONZ / VALUE HR / freee / porters / hokan / Money Forward / RUN.EDGE / RVSTA 株式会社リバスタ / rescuenow

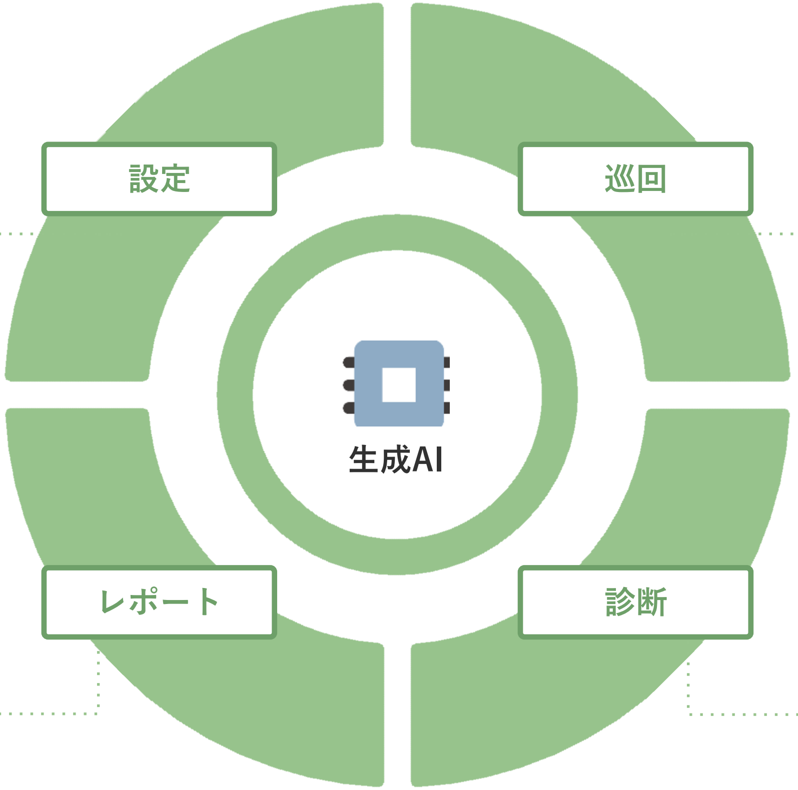
SI・IT企業
Rworks / アクモス株式会社 / AVANT GROUP / CTC / Insight Edge / Infcurion / 80&Co. / SB Technology / SBWorks / NTT AT / NTT DATA / NTTビジネスソリューションズ / Globalway / circlace / さくら情報システム / CEC / tcdi 情報技術開発株式会社 / Simplex Inc. / 777WORKS 株式会社スリーセブンワークス / SOFT CREATE / SOLTEC / 電通総研 / TOPPAN / JOPS / NI+C 日本情報通信株式会社 / Human Interactive Technology Inc. / FUJISOFT / FUJITSU / MITSUBISHI ELECTRIC 三菱電機インフォメーションネットワーク株式会社 / YONA / リピスト / XL

セキュリティ企業
NEC NECセキュリティ / NTT DATA NTTデータ先端技術株式会社 / GSX / cybertrust / LAC

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

生成AIの活用による高度な自動化を実現

オプション機能



1 診断設定がさらにカンタンに

- フリーフォーマットでの指示

特許 第7320211号

2 巡回がより柔軟に進化

- 多言語対応
- フリーフォーマットでの指示
- 画面の自動類似判定

特許 第7348698号

3 手動で診断していた項目にも対応

- パラメータの用途を推測
- セッションIDの規則性を解析

特許 第7344614号

4 高度なレポート出力も可能に

- 診断結果を元に総評を生成

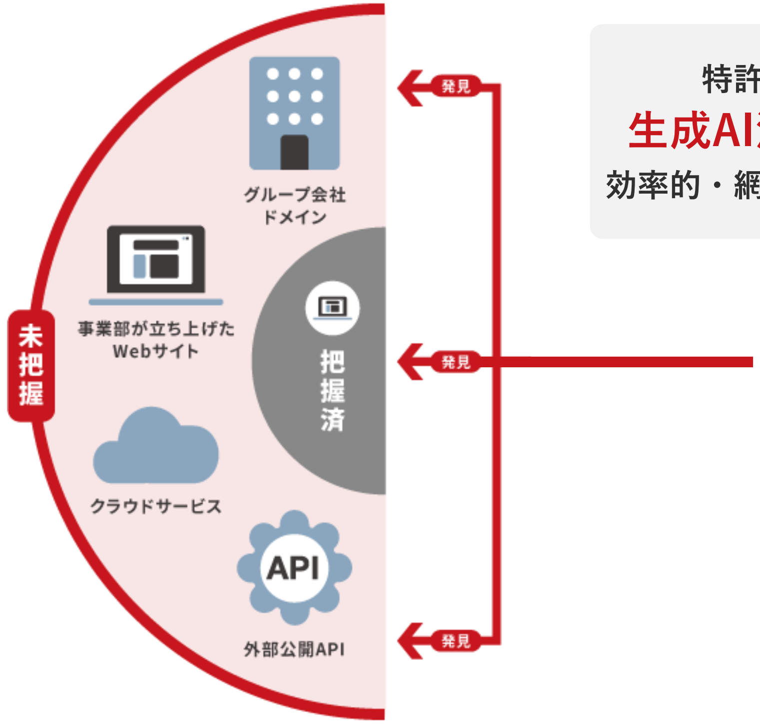
生成AI活用で、工数をかけずにWeb-ASMを実現

オプション機能

Web-ASMとは？

未把握な攻撃面の継続的な発見・リスク評価※

※リスク評価：AeyeScanのスキャンによる



特許取得実績のある
生成AI活用の技術により
効率的・網羅的に攻撃面を発見。

生成AI

Web-ASMの実施ステップ

1	2	3
攻撃面の 発見	攻撃面の 情報収集	攻撃面の リスク評価
Web-ASM機能	**自動巡回**	**脆弱性診断**
自社が保有している ドメイン一覧を抽出	未把握のドメインを 巡回対象に追加	管理対象の全ドメインに 脆弱性診断を実施

AeyeScan ひとつで、
より網羅的な脆弱性診断とリスクマネジメントが可能に！

AeyeSecurityLab

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人（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。

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人（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。

「脆弱性診断」ができるのは分かったけど

内製化には「管理・運用」が大変よね…

AeyeSecurityLab

AeyeScan＋AeyeCopilotの合わせ技で、トータルサポート

4月リリース決定！ AeyeCopilotとは？

関連部門の「情報とコミュニケーション」をつなぐプラットフォーム

診断・対策の全体管理や、セキュリティ対策に関する**最適な意思決定**を支援

ポイント①　脆弱性診断の全体進捗を可視化できる

陥りがちな状況

対応がバラバラ

どこまで対策できているのか
わからない…

サイトA	サイトB	サイトC
後回しでできていない	一部のサイトで診断	新規開発時のみ診断

AeyeCopilotの導入で実現できること

すべての診断の状況を可視化

		期限	状態
サイトA	重要度 高	4月1日	完了
サイトB	重要度 高	6月1日	対応中
サイトC	重要度 低い	5月1日	診断見送り

ポイント②　現場で脆弱性診断の対応優先度が判断できる

共通チェックリスト

AeyeColipot

AeyeCopilotを介した
コミュニケーションも可能

重要度	診断	状況	
重要度 高	診断必須	未着手	対応が遅れている！
重要度 高	診断必須	対応中	予定通り進んでいる！
重要度 低	診断任意	見送り	

現場

対応チェックリストを
もとに優先度が分かる

セキュリティ部門

状況が見えるからこそ
必要なフォローが行える

本日のまとめ

AIを活用してWebセキュリティを強化するキモは「マネジメントの仕組み化」

STEP 1	情報収集	情報収集・対象の把握	AeyeScan
STEP 2	検討	診断の必要性や優先順位を評価、対応方針の検討	AeyeCopilot
STEP 3	実行	診断計画の立案と実行・進捗の全体管理	AeyeCopilot
STEP 4	修正	検出された脆弱性の評価と対応	AeyeCopilot
STEP 5	運用	診断状況の報告・方針の見直しと全社最適	AeyeCopilot

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

AeyeSecurityLab

AeyeScan

セキュリティに、確かな答えを。