

AI活用で

ととのう、セキュリティ

—Web資産のリスク管理をラクにする方法とは—

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、新規プロダクト企画・事業開発をリードしながら、各種セミナー・講演への登壇などエバンジェリストとしても活動。



主な著書

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。

脆弱性は年々増加し、米国NISTも全件対応は諦めた

NISTの発表によると…

CVEの申請件数

2020年から2025年の間に

263% 増加



2026年1～3月の提出件数も
昨年同年比で1/3近く増加

NVDの運用を リスクベースストリार्ージへ移行

- (1) CISA KEVカタログに掲載されているCVE
- (2) 連邦政府で使用されているソフトウェアに関するCVE
- (3) 大統領令EO14028で定義される重要ソフトウェアに関するCVE

いずれかに該当するCVEが優先され、該当しないCVEは
詳細スコアや影響情報がすぐ整備されるとは限らなくなる

AI時代に重要性が高まる「自社文脈(コンテキスト)での判断」

これまで

NVD



整備・公表された脆弱性情報を見て判断



これから

脆弱性情報

CVE/CVSS
/NVD

悪用情報

CISA KEV/
脅威情報

自社資産情報

外部公開状況/重
要度/環境



さまざまな情報をもとに自組織で優先順位づけ

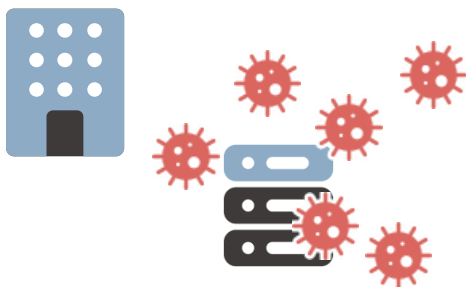
すべての脆弱性を見る時代から、リスクに応じて優先順位をつける時代へ



優先順位づけ（トリアージ）って
どう考えればいい？

では、ここで質問です！

Q. みなさんならどちらの優先度を高くしますか？



1

社内サーバーの
脆弱性100件



2

公開サーバーの
脆弱性1件

では、ここで質問です！

Q. みなさんならどちらの優先度を高くしますか？



1

本番環境だが
VPN配下



2

外部公開された
古い検証環境

正解はない。自社文脈にあわせて、総合的に評価することが重要

脆弱性の深刻度

取り扱う情報の重要度

ビジネス上の重要度

外部公開状況



開発・リリース頻度

しかし、日常的に「全ての資産に対して」リスク（脆弱性）を把握するのは大変

多くの企業で起きていること





**優先度 中～低の資産も含めて
自社資産全体のリスクを把握する**

外部公開資産のリスク管理に必要なこと：ASM (Attack Surface Management)

STEP 1

自社の外部公開資産を一覧化する（棚卸し）

STEP 2

その資産が、何に使われているかを判定する

STEP 3

外部公開状況・利用技術・重要度を整理する

STEP 4

悪用状況や脆弱性情報と突き合わせる

STEP 5

優先順位をつけて、対応・監視につなげる



人手で頑張る
には限界が...



待てよ、**生成AI**とか使えないかな…？

高度な生成AI活用により、効率的かつ信頼性の高い探索が可能



生成AIをASMに活用することで…！

会社名だけで 攻撃面を探索

検索結果に上がってきた
組織名(文字列)を解読



膨大な情報源 から総合的に判定

- ✓ SSL証明書の情報
- ✓ IR情報(Web公開済み) など



発見経路/理由 が分かる

生成AIが攻撃面を見つけるまでに
辿ったルートの説明



生成AIが、Webサイトの属性を自動判定&重要度をランク付け



生成AIをASMに活用することで…！

サイト用途

Medium

- ECサイト
- VPN管理サイト

Low

- 外部SaaSサイト
- テストサイト

保持データ

High

- 個人情報
- クレジットカード情報

利用技術

Low

- WordPress
- EC-CUBE
- 旧式技術
(JSP/PHP/CGIなど)

技術スタックだけでなく「ビジネス上の重要度」をもとに判定

生成AIが、リスクの深刻度を自動で可視化し、わかりやすく解説



生成AIをASMに活用することで…！

既に悪用されている
脆弱性

実際の攻撃で
使われている脆弱性



CVSSスコア／深刻度

脆弱性の技術的な
深刻度・影響範囲

悪用可能性(EPSS)

近い将来
悪用される可能性

悪用観測(KEV)

公的機関などが
悪用を確認済みと
公開している情報

検出したWebサイトで使用されているミドルウェアやライブラリにおける
最新の「脅威インテリジェンス」と自動で突合・可視化

生成AIを活用した

Web資産の優先順位づけ・リスク管理は
AeyeScanにお任せください！

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

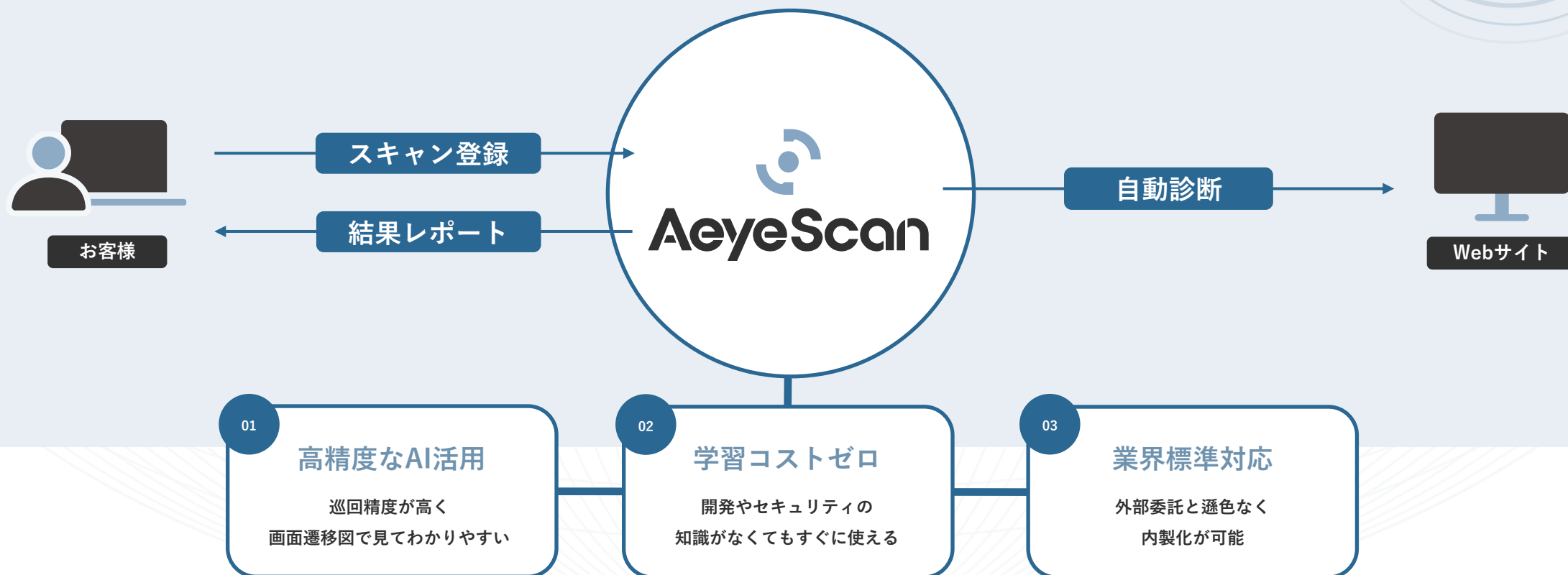
国内市場シェア

No.1※

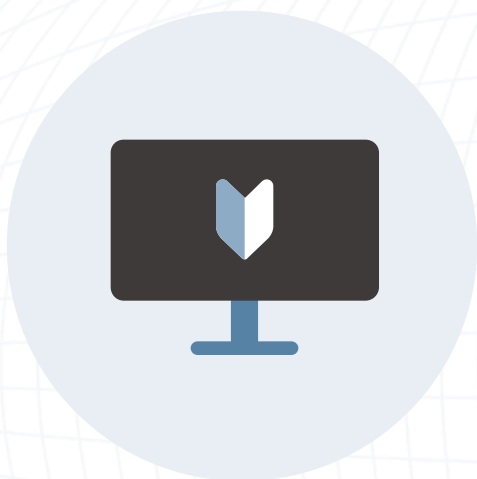
※ 富士キメラ総研調べ「2025 ネットワークセキュリティビジネス調査総覧 市場編」
Webアプリケーション脆弱性検査ツール ベンダーシェア（2024年度実績）

※ 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）

有償契約
300社以上



| 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。

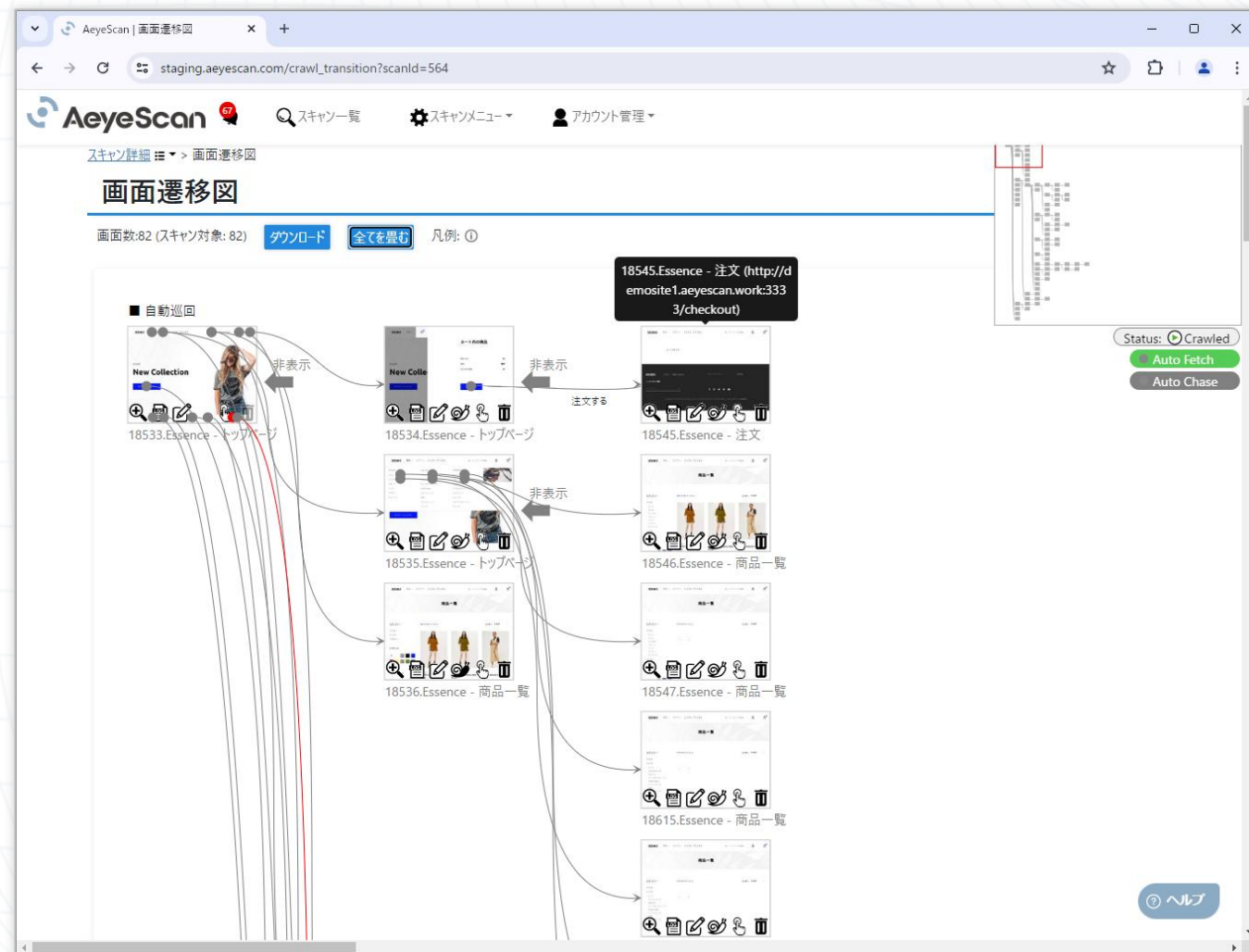
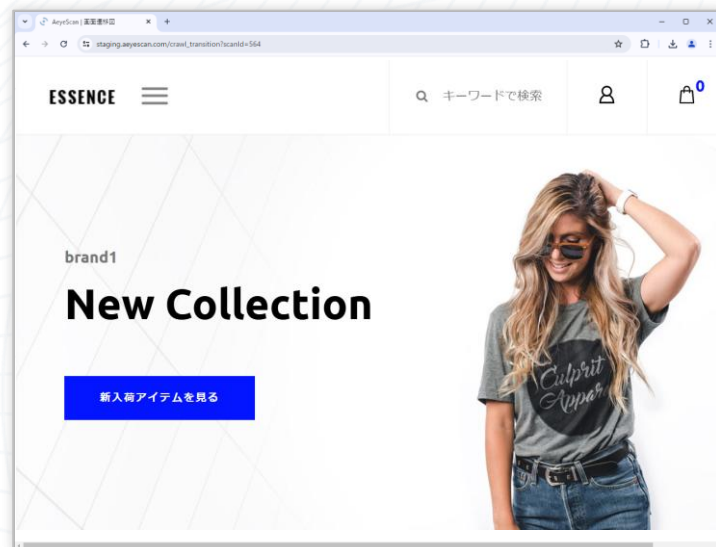


わかりやすいレポート

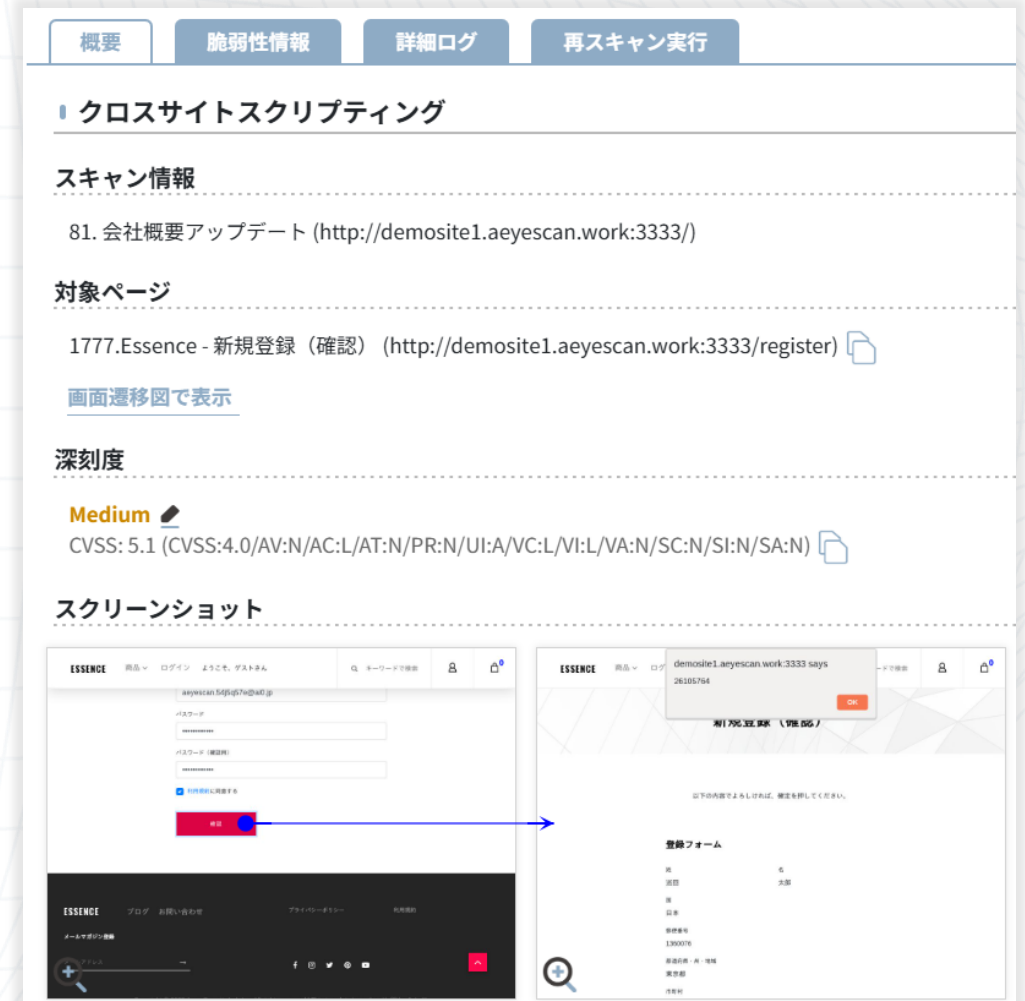


各種ガイドラインに準拠した
プロ仕様のレポート出力、
日本語と英語に対応。

巡回時に、自動で画面遷移図を生成



結果がわかりやすく、すぐさま修正作業に取り組めるレポート

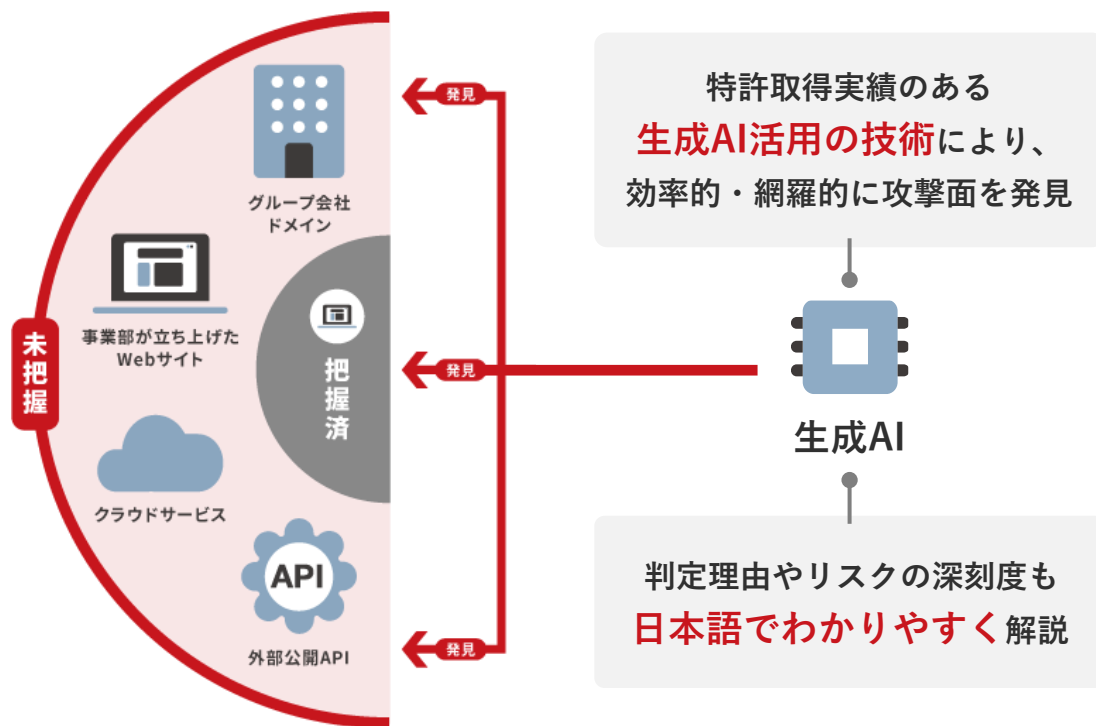


生成AI活用で、工数をかけずにWeb-ASMを実現

オプション機能

Web-ASMとは？

把握していないWeb資産（攻撃面）の継続的な発見・リスク評価



Web-ASMの実施ステップ

1

攻撃面の
発見



自社が保有している
ドメイン一覧を抽出

2

攻撃面の
情報収集



属性やミドルウェア・
ライブラリの情報を収集

3

攻撃面の
リスク評価



資産の重要度と
リスクの深刻度を提示

AeyeScan Web-ASM機能が、これらの作業を自動化

【新機能】資産の探索からプラットフォーム診断までワンストップ！

探索・発見

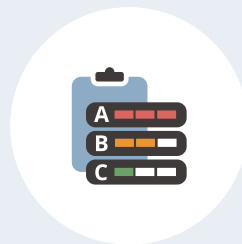
自社に紐づくと思われる
Web資産を、生成AIが探索



ドメイン・Webサイト等の
発見経路／判定理由も説明
→ブラックボックス化を防止

精査・評価

資産情報の収集、資産の精査
リスク評価・優先度付を支援



CVSS/EPSS/KEV等の指標
＋ビジネス観点の重要度
→多角的な精査・評価を楽に

検査・監視



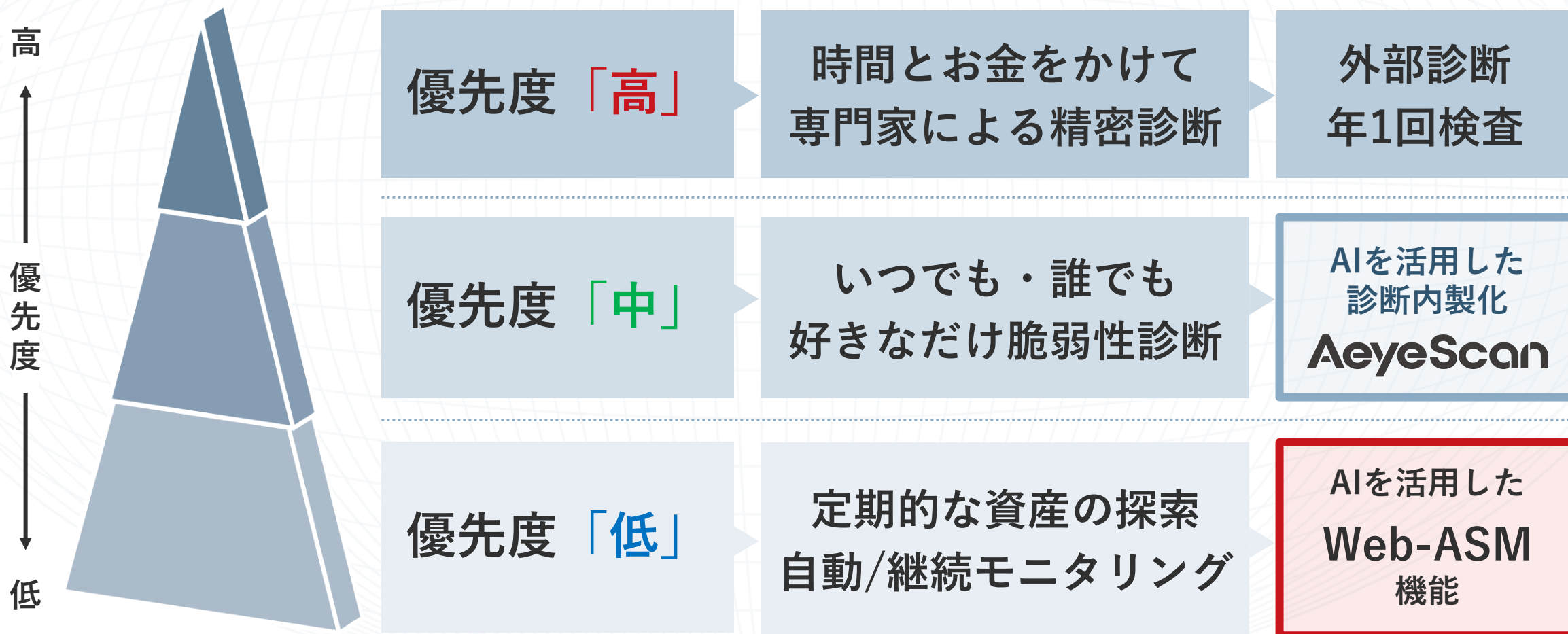
プラットフォーム ネットワーク

PF診断やNW診断を含む
自社資産の定期的なスキャン



ポートスキャン/NWスキャン
での潜在的リスクチェック
→全資産のモニタリングも

網羅的な「セキュリティ診断」を実現するなら **AeyeScan**



| AeyeScanが選ばれている理由

誰でも使える操作性

×

プロが認める機能・性能

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

ととのう、セキュリティ

私たちは、AIの力でセキュリティ対策が無理なく回り続ける仕組みを提供し、専門部門だけに頼らず、チームで安全を支えられる状態をつくります。

本来の業務に集中しながら、事業が前に進み続ける世界を実現していきます。



脆弱性対策まるわかり月間

8月限定

1週間ごとに学べる動画を公開! いつでも視聴可能!

Week 1

担当サービスを守る

8/ 3月～7金

開発・事業部門
の方向け

Week 2

最新トレンドを知る

8/ 10月～14金

情報収集したい
方向け

Week 3

自社全体を守る

8/ 17月～21金

情シス・セキュリティ部門
の方向け

Week 4

診断ツールを知る

8/ 24月～28金

ツールをご検討中
の方向け

夏休みの情報収集は、ぜひ自席からお好きなタイミングで!

詳細はこちらから



セキュリティ診断のお悩み・お困りごとをお聞かせください！

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 に関する 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





AeyeScan

セキュリティに、確かな答えを。