

AXが変えるセキュリティの 「あたりまえ」

—脆弱性対策を、組織と業務から変える仕組みとは

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。

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）



フォローお願いします！



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。

誰でも簡単に

プロさながらの高度な
脆弱性診断を



AXが変えるセキュリティの 「あたりまえ」

—脆弱性対策を、組織と業務から変える仕組みとは

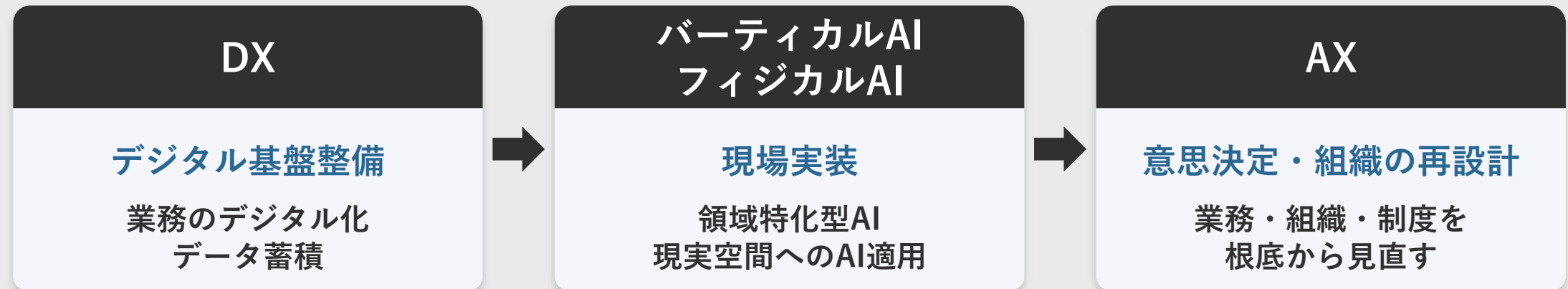
AXってなに？

| AX (AIトランスフォーメーション) って何？

AIを活用して、顧客や社会のニーズを基に、製品やサービス、ビジネスモデルを変革するとともに、業務そのものや、組織、プロセス、企業文化・風土を変革し、競争上の優位性を確立すること。

内閣府『人工知能基本計画』（第Ⅰ期・令和7年12月23日閣議決定）

「あらゆる組織で、AIを前提として意思決定や業務の進め方を根底から見直す」ことがAXの到達点



人工知能基本計画（第Ⅱ期・令和8年7月14日閣議決定）に基づく整理

いまはAIを事業に組み込む「AX時代」へと突入している

DX

ITやクラウド活用による
業務効率化



人間がやっていた定型業務を
システムに代替させる



AX

AIの自律的な動きによる
業務変革



人間ができていないことも含め
AI活用で事業を発展させる

DXとAIは何を変えたか？

| DXが変えたセキュリティの「あたりまえ」

デジタル化の主体

IT部門主導から
事業部主導へ



重点領域

社内IT・インフラから
デジタルサービスへ



IT部門が把握できない**Web資産**が増加している

DXの進展により、Web資産の全体像が見えにくくなっている

AIが変えたセキュリティの「あたりまえ」

企業

人手中心の開発から

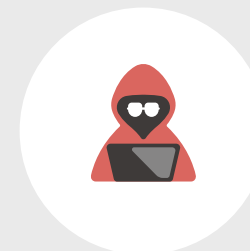
AI協働の高速開発へ



攻撃者

人手中心の攻撃から

AI活用型の高速攻撃へ



セキュリティも、**開発・攻撃のスピード**に追いつかなくてはならない

なかでも、脆弱性対策は“発見と対応のスピード”が問われている

AXを前提としたセキュリティ対策



AX時代を前提に、セキュリティの共通基準づくりが進む

AI活用やサプライチェーンを含め、継続的なリスク管理を促す指針・評価制度が相次いで公表されている。

AI 事業者ガイドライン (第 1.2 版)

令和 8 年 3 月 31 日

総務省 経済産業省

総務省・経済産業省
「AI事業者ガイドライン」

経済産業省 国家サイバー統括室
National Cybersecurity Office

サプライチェーン強化に向けたセキュリティ対策評価制度 に関する制度構築方針(案)

令和 7 年 12 月

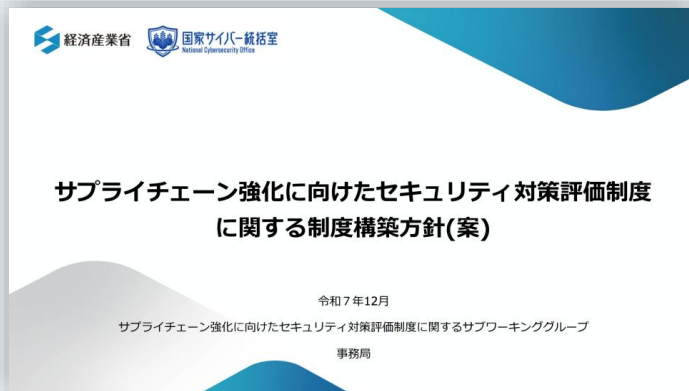
サプライチェーン強化に向けたセキュリティ対策評価制度に関するサブワーキンググループ
事務局

経済産業省・国家サイバー統括室
「サプライチェーン対策評価制度」

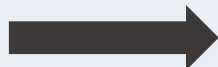
2026年度中の制度開始予定「サプライチェーン対策評価制度」

サプライチェーン全体の強靱性の確保と、対策要求の共通化による対策適正化・確認の効率化が目的。

★3、★4は2026年度下半期の運用開始想定。



セキュリティ対策の
成熟度を3段階で評価



	★3	★4	★5
想定脅威	一般的な サイバー攻撃	供給停止・情報漏洩 など大きな影響を もたらす攻撃	未知の攻撃も含めた 高度なサイバー攻撃
対策の基本的な 考え方	全てのサプライ チェーン企業が 最低限 実装すべき対策	サプライチェーン 企業等が標準的に 目指すべき対策	サプライチェーン 企業等が到達点と して目指すべき対策
評価スキーム	自己評価	第三者評価	第三者評価

※★1、★2に関しては、先行する自己評価制度の仕組みである「[SECURITY ACTION](#)」にて制度化

★3の取得も大変！でも、取引先は「普通に」求めてくることに…

AX時代に必要なセキュリティ対策のポイント

事業変革に合わせた

組織変革

事業部門が主体的に実践し
IT部門が支援する体制へ

セキュリティ部門

支援

事業部門

診断



支援

開発部門

診断



組織変革に合わせた

業務変革

「自分で自分の身を守る」ために
脆弱性診断を日常業務へ

要件
定義

設計

開発

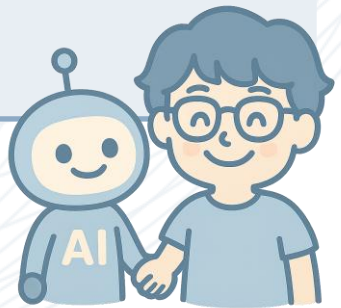
テスト

運用



専門知識や人手に依存せず

現場部門が自ら、脆弱性対策を実践できるよう
我々が強力にバックアップします！



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

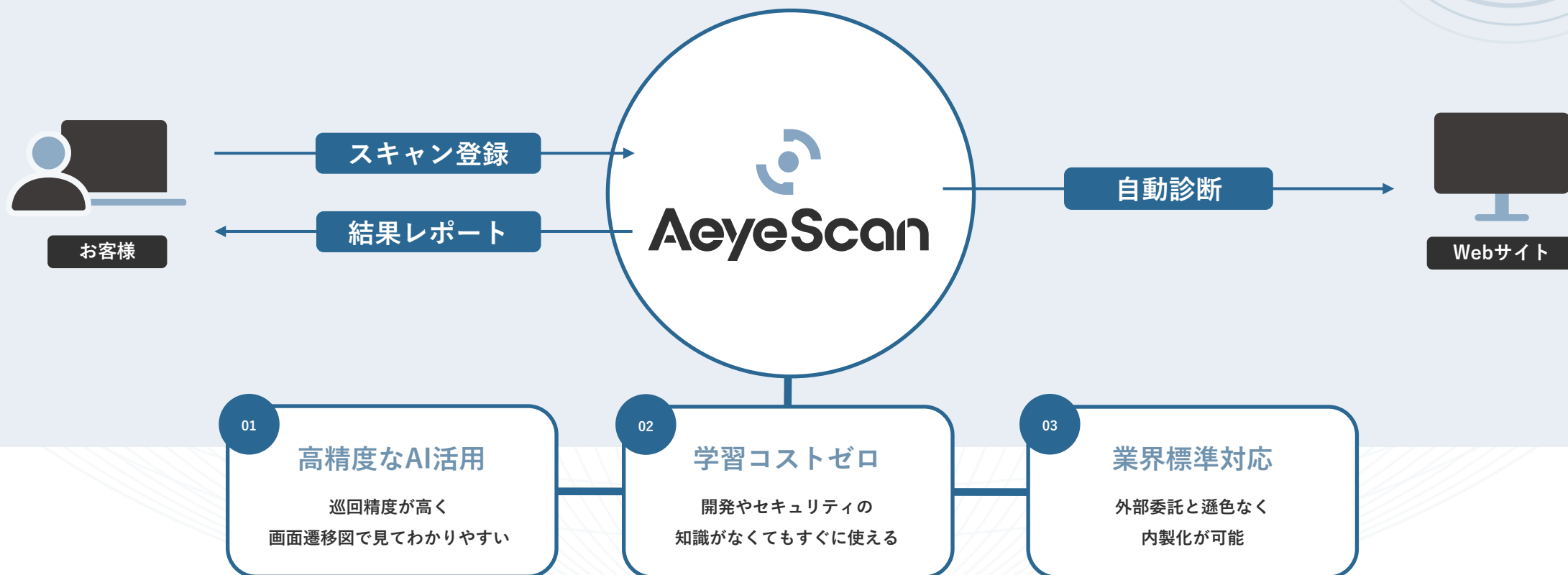
国内市場シェア

No.1※

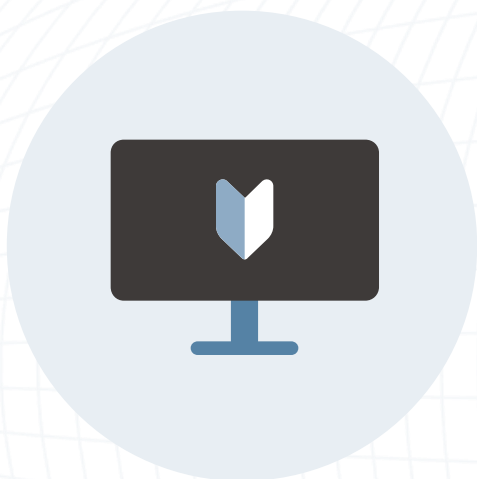
※ 富士キメラ総研調べ「2025 ネットワークセキュリティビジネス調査総覧 市場編」
Webアプリケーション脆弱性検査ツール ベンダーシェア（2024年度実績）

※ 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）

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。

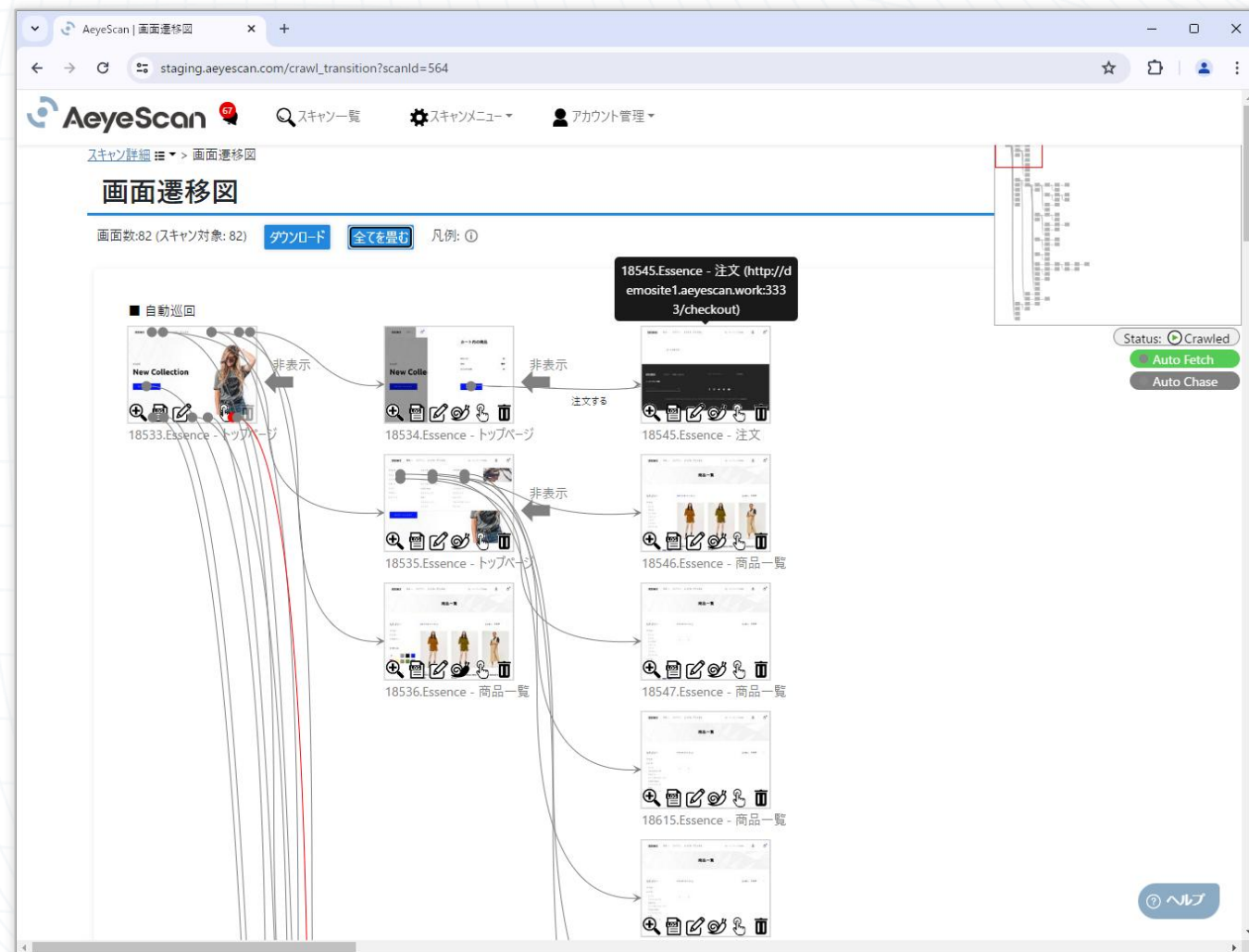
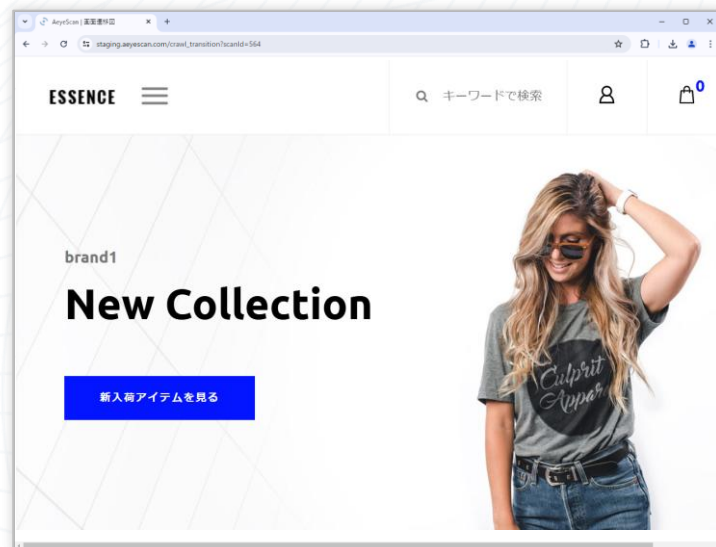


わかりやすいレポート

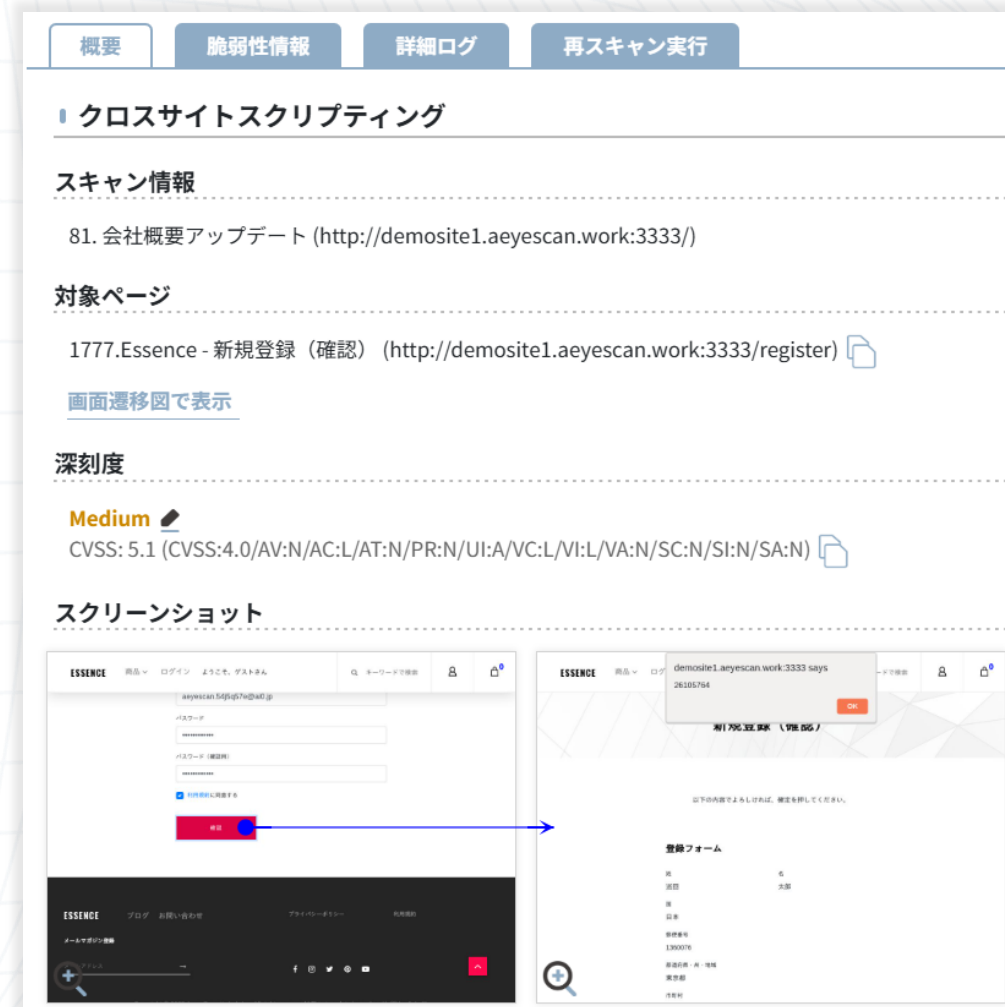


各種ガイドラインに準拠した
プロ仕様のレポート出力、
日本語と英語に対応。

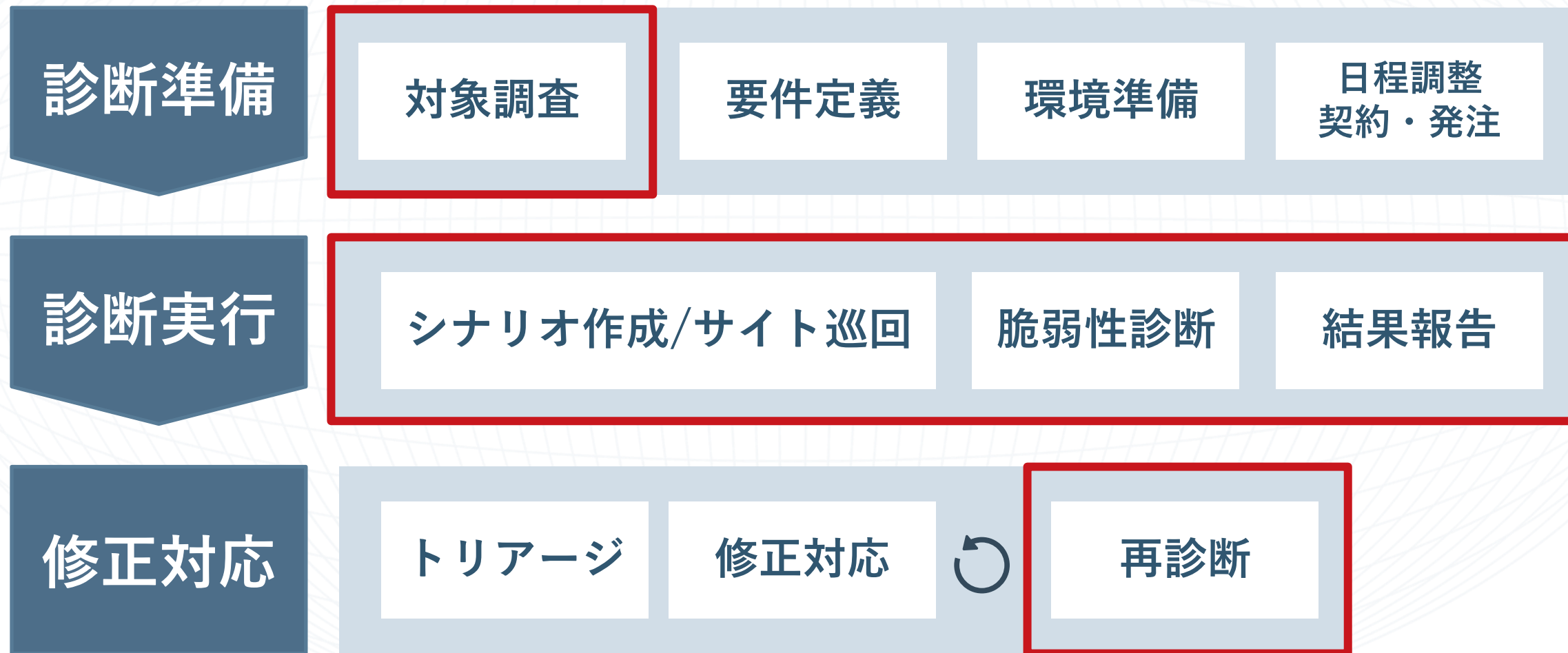
巡回時に、自動で画面遷移図を生成



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



AI活用で、脆弱性診断プロセスの大部分を自動化・省力化できる

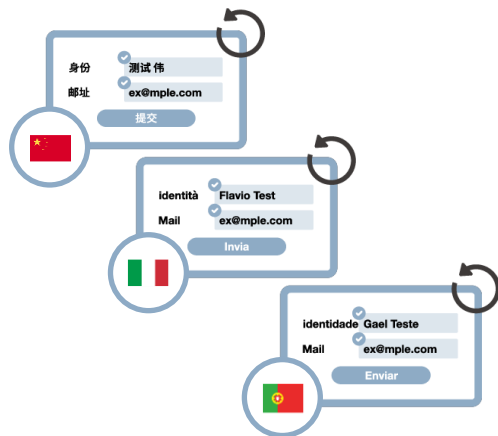


| 生成AIを組み込むことで、多様なWebサイト・多様な脆弱性に対応

多言語対応

日英以外のWebサイトも幅広く巡回・診断

多言語でのフォーム入力

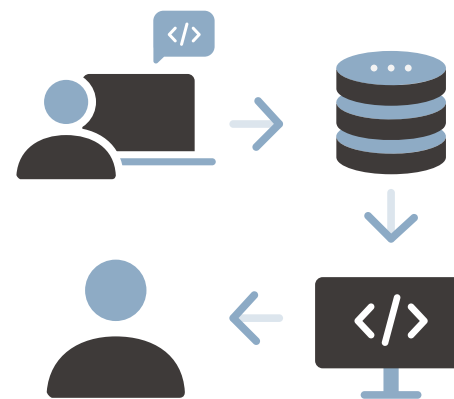


日本語	ポーランド語
英語	スペイン語
フランス語	ポルトガル語
中国語	ロシア語
韓国語	スウェーデン語
オランダ語	アラビア語
ドイツ語	...
イタリア語	

診断項目の拡張

人間しか診断できなかった脆弱性も検出

セカンドオーダー系XXS



認可の不備・権限昇格



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



リスク対応の優先順位付けに必要な情報を自動判別

Web資産の重要度

各Web資産の属性

(サイト用途、保持データなど)

リスクの深刻度

NEW

ミドルウェアやライブラリの悪用観測脆弱性※

※既にサイバー攻撃で悪用が確認された脆弱性





製品情報サイト

重要度：中

2件

→

ミドルウェアA

CVE-xx

深刻度：高

ミドルウェアA

CVE-xx

深刻度：中



ECサイト

クレジットカード
情報保持

重要度：高

1件

→

ライブラリB

CVE-xx

深刻度：低



ヘルプサイト

WordPress使用

重要度：低

10件

→

ミドルウェアC

CVE-xx

深刻度：高

ライブラリD

CVE-xx

深刻度：高

:

【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

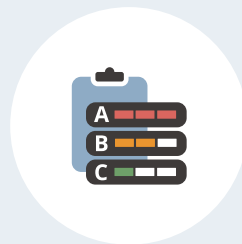
自社に紐づくと思われる
Web資産を、生成AIが探索



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

| 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

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。

トライアル



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



定期開催中！

AeyeScanがよく分かるデモ動画・セミナー

AeyeScanを
検討してみたい方へ

開発を止めない

脆弱性診断

内製化を強力にサポートする

AeyeScan デモ動画

AeyeScanがどんなものか、
デモでわかりやすく紹介！AeyeScanの操作を
体験してみたい方へ

「外注しているのに、なぜか忙しい」を解決する——

9月の
日程

脆弱性診断の “周辺タスク”を 削減！

診断の自動化体験セミナー

操作体験で不安や疑問を解消。
その場で納得できる
セミナー！セキュリティ対策に
お悩みの方へ

最新セキュリティ情報をお届け

ウェビナー

毎月開催

気軽に学べる
無料セミナーです！

事例と対策ノウハウを紹介。
毎月学べるウェビナー
無料配信中！



AeyeScan

セキュリティに、確かな答えを。