

AIが変える脆弱性診断

攻撃の高速化に
「自律的セキュリティ運用」で立ち向かう

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！



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。



「ととのう、セキュリティ」の考え方を動画で紹介しています



「Claude Mythos」の衝撃

2026年4月、Anthropic（アンソロピック）社が発表した最新AI「Claude Mythos」が大きな注目を集めた。

脆弱性の発見

大量のOSSから、数千規模の危険な脆弱性を発見
長年発見されなかったバグ・エラーを検出

Exploit-PoC

攻撃用のコードを構築・修正する能力が飛躍的進化
自律的に攻撃を完遂する（やりきる）チカラ

文脈理解・推論

部分的なコード単体のパターンマッチングに加え
外部仕様や状態遷移を考慮して脆弱性を特定

ハーネスとの連携

Mythos単体の能力だけでなく、制御設計などの
ハーネスによってパフォーマンスを引き出せる

（参考）Anthropic社『Project Glasswing: An initial update』
株式会社リチェルカセキュリティ『Mythos以降のAI脆弱性診断— 内製化のためのハーネスエンジニアリング—』

攻撃者はAIで進化、防御側(企業)は今までと同じ脆弱性対策



攻撃者 × 高性能AI

- ・ 24時間365日の攻撃
- ・ 自律的に探索/攻撃



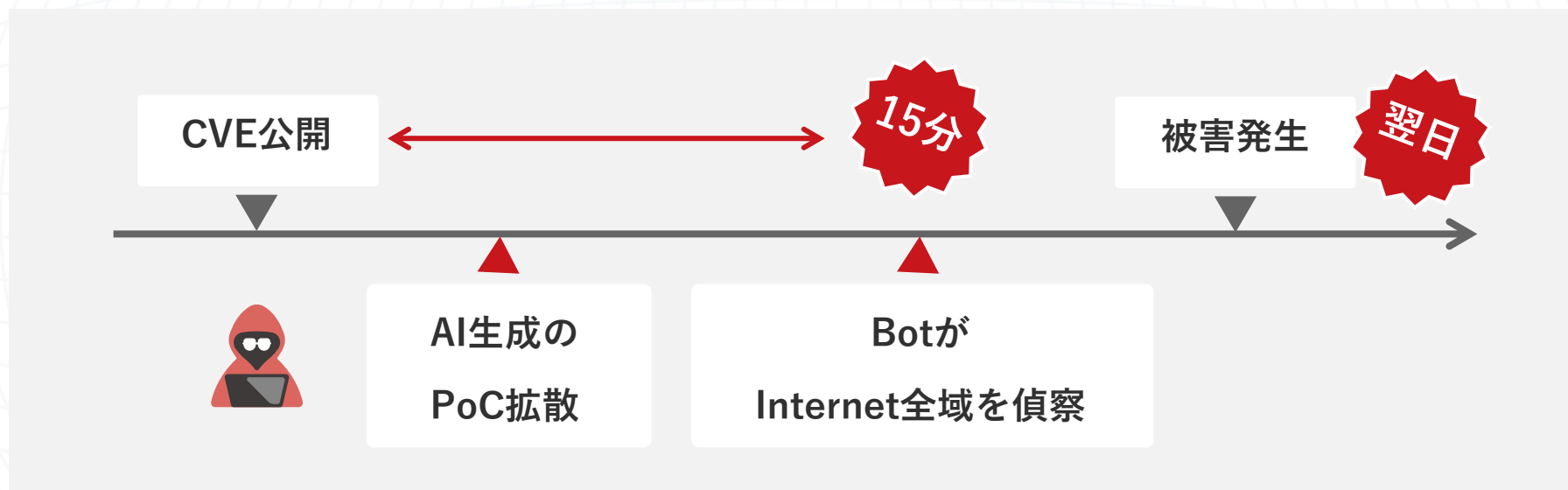
企業 × 継続運用

- ・ 年1、2回の定期診断
- ・ 人力で時間をかけて作業

人力前提のセキュリティ対策は、すでに限界を超えている

今やらなければならない対策（Must）の水準が上昇

セキュリティ対策としてやるべきこと（Should）は、昔から大きく変わっていない。
しかし、最低限必要な対策のレベル（Must）がどんどん上がっている。



2026年の 現実

- スキャン開始時間：CVE公開から「**15分**」以内が常態化 ※1
- 悪用開始までの平均：2024年の56日→2026年は「**10時間**」に短縮 ※2
- 実例：LiteLLM (CVE-2026-42208) 公開から「**36時間**」で実攻撃を確認 ※3

「最低限」の水準が引き上げられている⇒考え方を変える必要がある

これまで

脆弱性診断は年1回でいい

予算がついてから対応しよう

人手が足りないから後回し

重要システムだけ見ればいい

これから

どう定期的に脆弱性診断を実施するか？

どう予算を最適化しながら進めるか？

どう人手不足でも回すか？

どうやって網羅的に見るか？



そうだ、こちら側もAIの力を借りよう！

攻撃者がAIを使うなら、守る側もAIを使って然るべき

政府指針でも、高性能AIを活用したセキュリティ強化の重要性が示されている。

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
(ソフトウェア・ベンダに対する注意喚起)

令和8年5月18日
内閣官房国家サイバー統括室、経済産業省

足下で、ソフトウェア[®]の脆弱性発見について高い能力を有するAI（高性能AI）の開発が進んでいる。こうした高性能AIは、未知の脆弱性の早期発見や是正によりセキュリティ向上に役立つ一方で、仮に悪意ある者に使われた場合には、サイバーセキュリティ上のリスクが一気に高まるおそれがある。

このため、政府全体としては、内閣官房国家サイバー統括室を中心に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関する対策パッケージ「Project YATA-Shield」をとりまとめたところである。経済産業省としても、高性能AIを活用したサイバーセキュリティ産業の育成も重要との観点の下、引き続き、国内のサイバーセキュリティ対策の実装を支える高度な人材育成や、研究開発などサイバーセキュリティ産業の育成・振興等の各種施策の企画・実行を推進していく予定である。

こうした政府の取組も念頭に置きつつ、広く産業界で用いられているソフトウェアを開発・提供・運用する主体（ソフトウェア・ベンダ）の皆様におかれましては、セキュア・バイ・デザインの原則に基づき、以下のとおりソフトウェア開発ライフサイクル（SDLC）全体において高性能AIも活用しながら脆弱性の早期発見・対応に率先して取り組むことをお願いしたい。なお、高性能AIの活用にあたっては、情報漏えいや意図しない学習への流用等のリスクを適切に管理する必要があることに留意されたい。

1. リリース前のソフトウェアについては、高性能AIを積極的に活用し、リリース後の脆弱性発見の可能性を低減させた上で、リリースをする。
2. リリース後のソフトウェアについては、自ら高性能AIを積極的に活用して自らがリリースしたソフトウェアの脆弱性の把握に努めるとともに、脆弱性関連情報の収集・早期把握に努めつつ、脆弱性が発見された場合には（必要に応じ高性能AIも活用して）パッチを早急に作成し、顧客に速やかに提供する。

国家サイバー統括室など

『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
(ソフトウェア・ベンダに対する注意喚起)』

“ソフトウェアを開発・提供・運用する主体は、開発ライフサイクルにおいて**高性能AIも活用しながら**脆弱性の早期発見・対応に率先して取り組むこと”

まずは、脆弱性診断から「AI活用のセキュリティ対策」を始めませんか？

判断基準が明確、かつ運用頻度が高い「脆弱性診断」は、AI活用の仕組み化が効果を発揮しやすい領域です。

脆弱性診断は…

情報処理の量が膨大



脆弱性情報・
資産情報・ログなど
判断材料が膨大

判断の再現性が重要



属人化により
優先度がぶれると
対応品質が安定しない

説明できる判断が必要



対策方針の理由を
言語化できないと
経営の合意が得られない

継続運用が前提



一度きりではなく
日々発生し続けるため
仕組み化が必要

だから、AI活用によって「品質」を維持しながら「効率」を高められる！

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

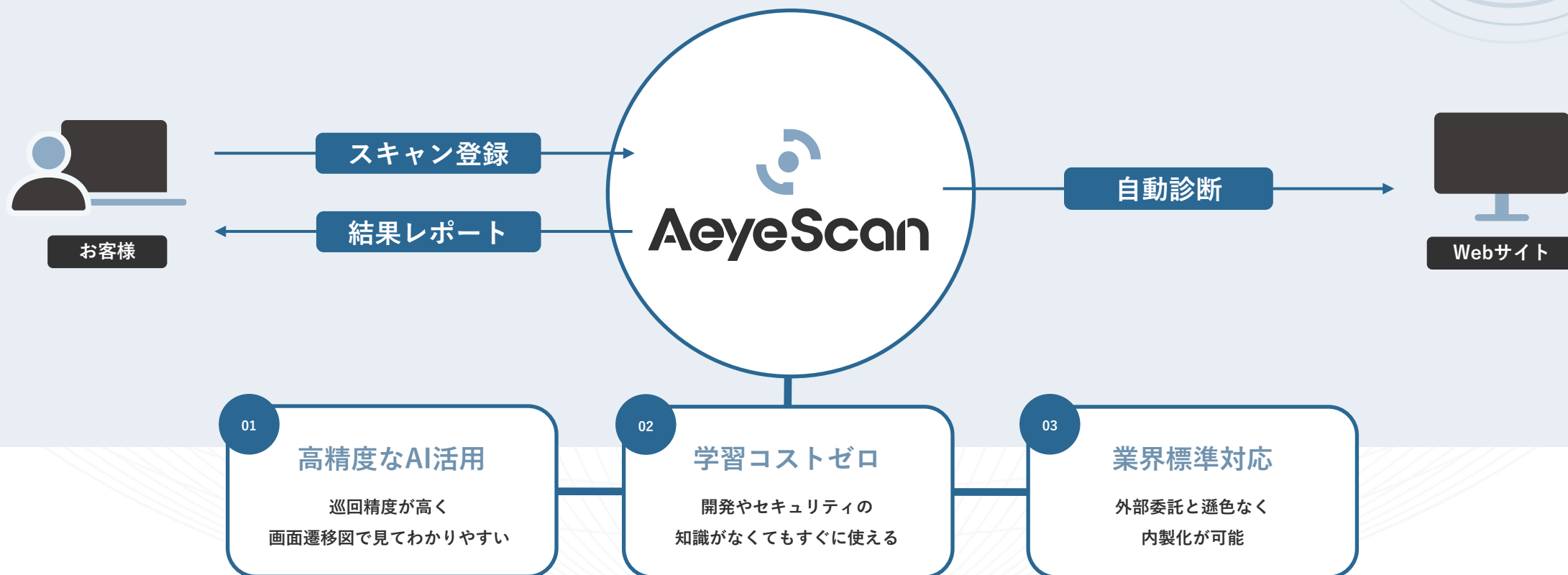
国内市場シェア

No.1※

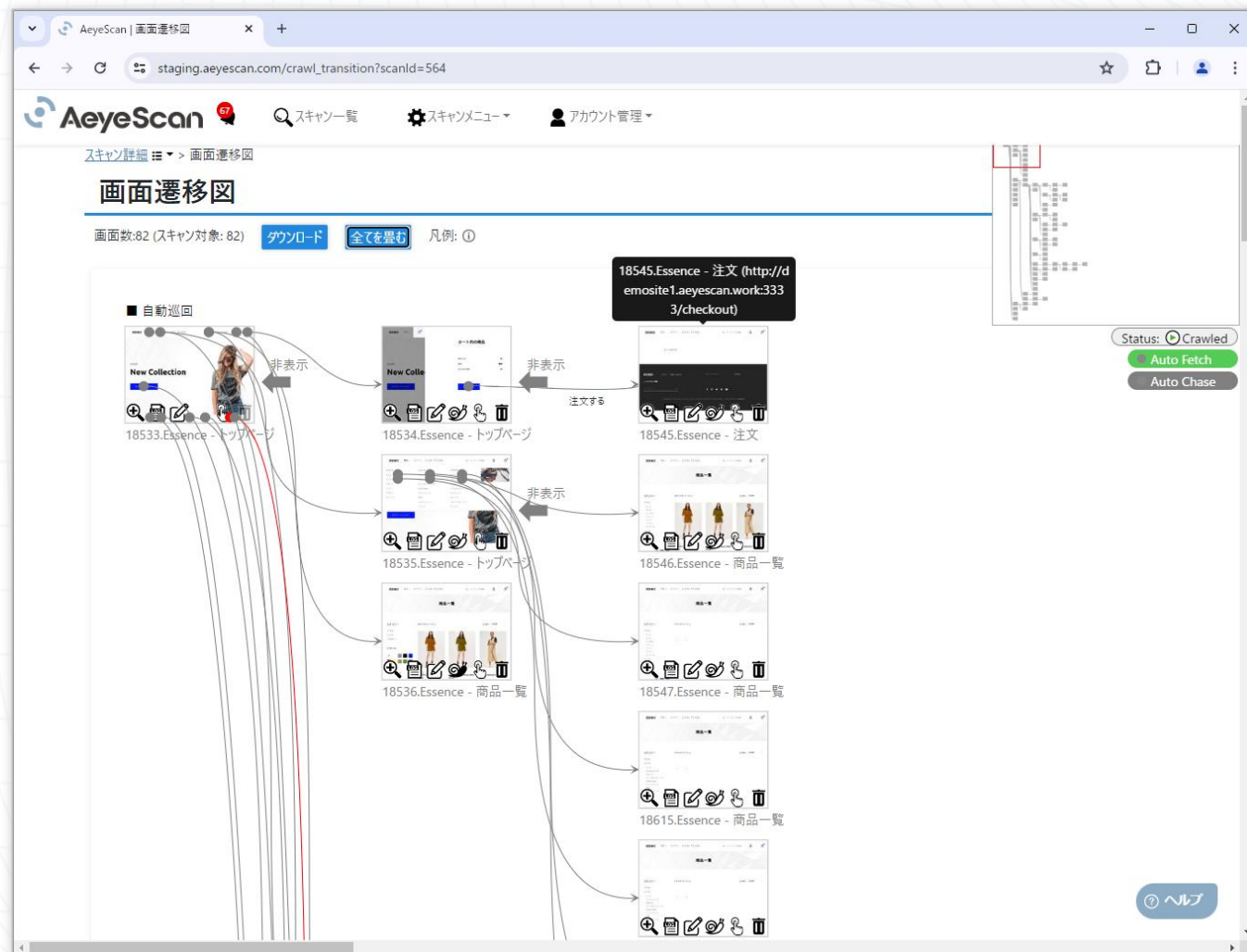
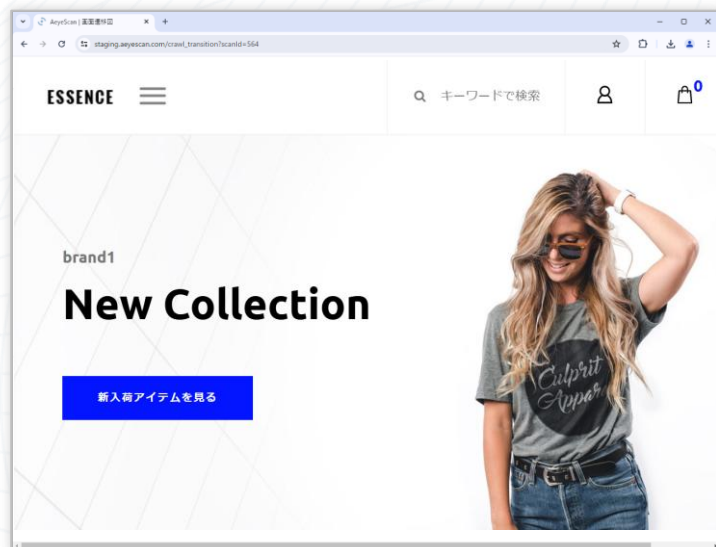
※ 富士キメラ総研調べ「2025 ネットワークセキュリティビジネス調査総覧 市場編」
Webアプリケーション脆弱性検査ツール ベンダーシェア（2024年度実績）

※ 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）

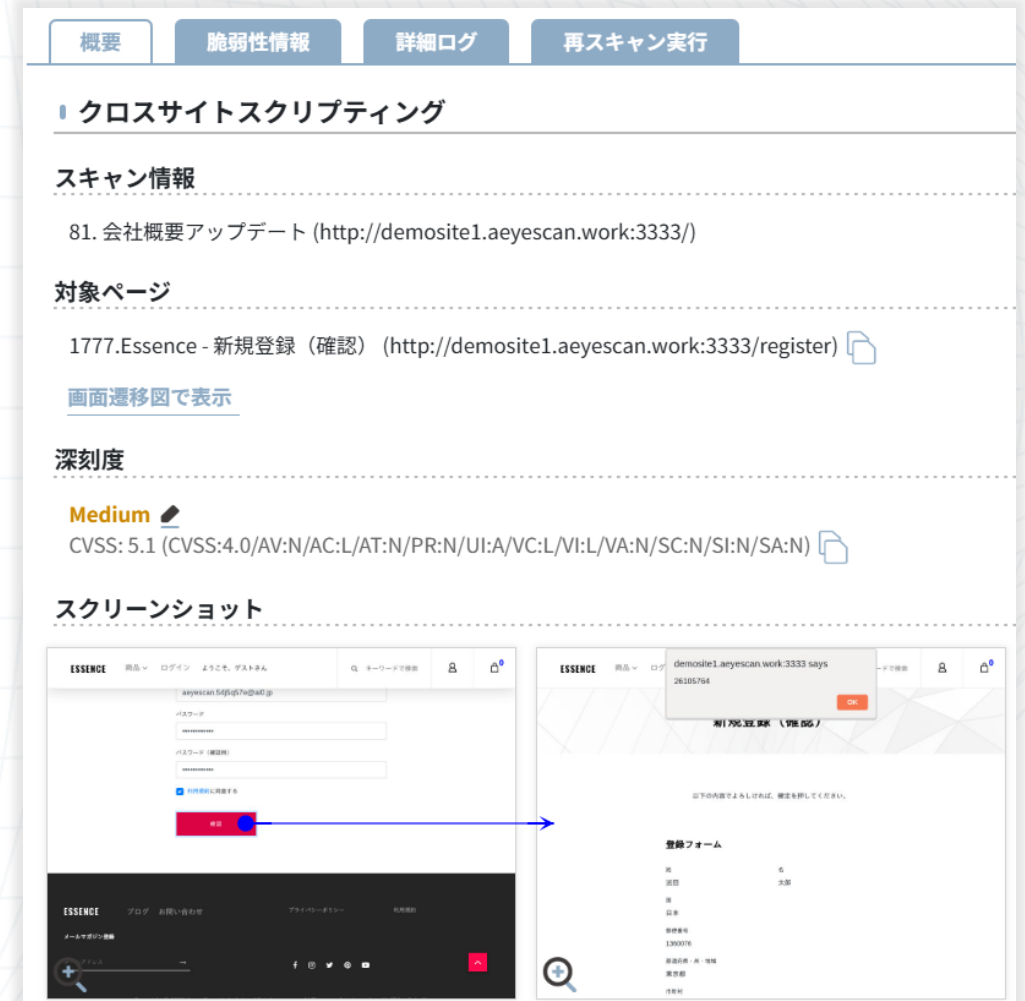
有償契約
300社以上



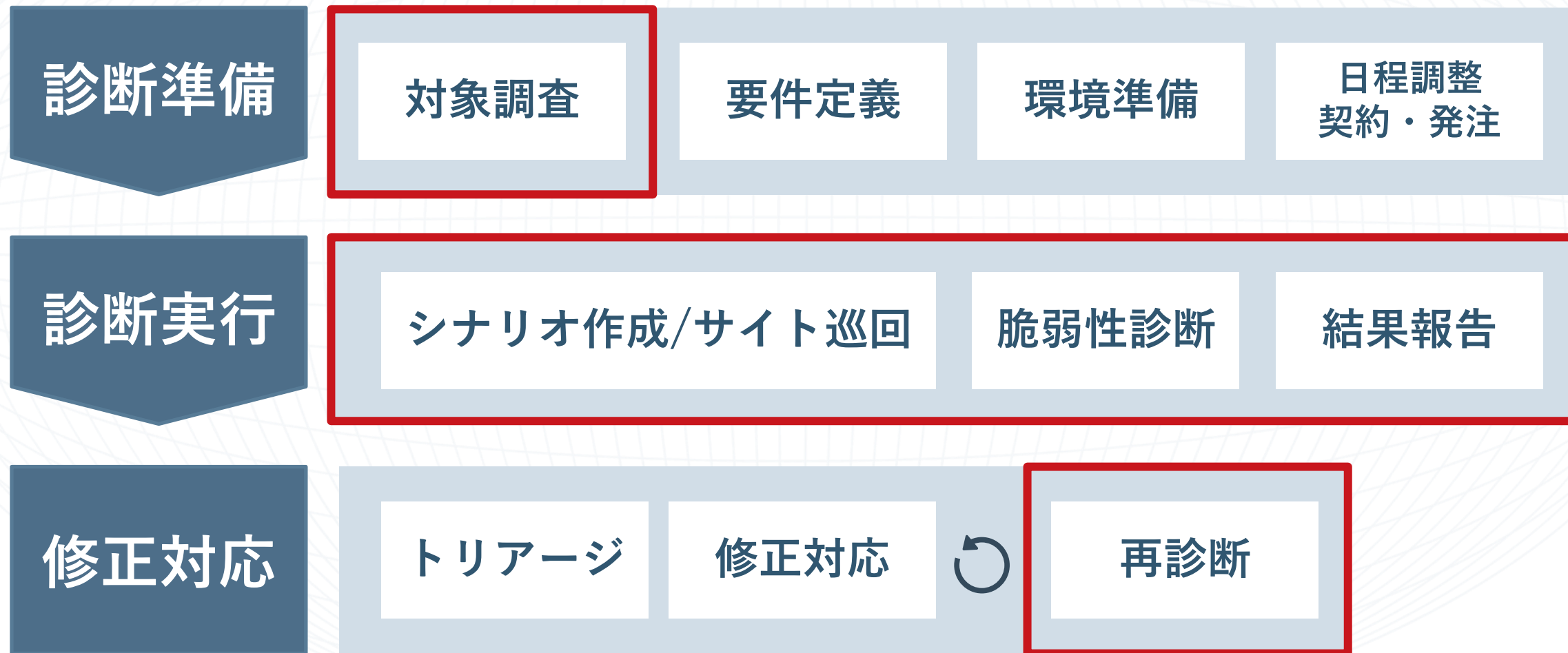
巡回時に、自動で画面遷移図を生成



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

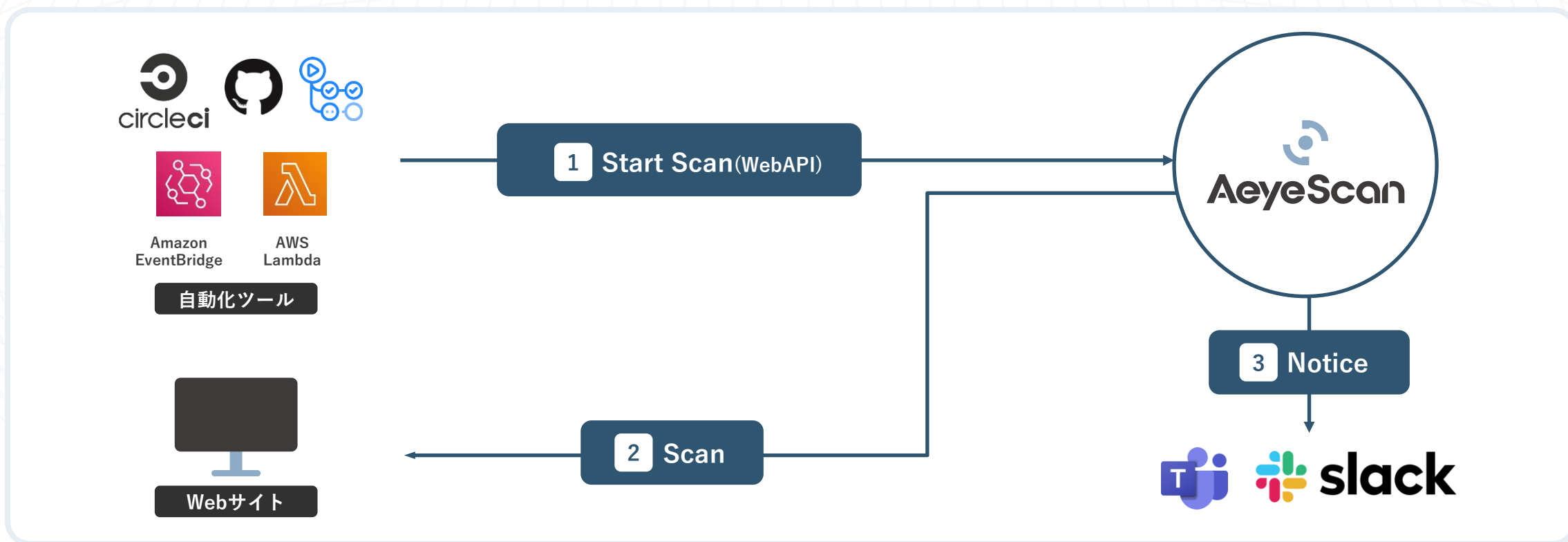


脆弱性診断プロセスの大部分を省力化できる



｜ アジャイル開発・高頻度リリースでも漏れなく診断

CI/CDに組み込むことで、リリースのたびに自動で診断が実行される仕組みづくりが可能に。
属人化を排除し、誰が開発しても一定のセキュリティを担保できる。



生成AIで、自動診断の対象領域を拡張

格納型XSSや権限昇格など、アプリケーションの文脈理解が必要な診断にも対応。

従来の自動診断

入力して反応を見る診断が中心
反射型XSSやSQLインジェクションなど
パターン化しやすい脆弱性に対応



生成AIによる自動診断

アプリケーションの文脈まで理解
格納型XSSや権限昇格の脆弱性など
複雑な診断の自動化を支援



| 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

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



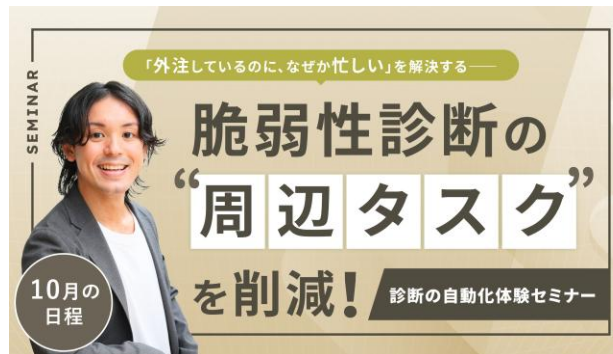
定期開催中！

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

AeyeScanがどんなものか知りたい方に、
デモを交えてわかりやすくご紹介。
まずは気軽に使い勝手をチェック！

デミセミナーの日程を確認

AeyeScanの操作を
体験してみたい方へ

実際の操作を通して、一連の機能を体感。
導入前の不安や疑問をまるごと解消。
“わからないまま”をなくすセミナーです。

ハンスオンセミナーの日程を確認

セキュリティ対策に
お悩みの方へ

最新の事例や対策ノウハウをテーマ別に紹介。
月替わりで学べる無料ウェビナーを開催中。
お気軽にご視聴いただけます！

ウェビナーの日程を確認





AeyeScan

セキュリティに、確かな答えを。