

「知る」から始める サイバーレジリエンス

—生成AIを活用して“デジタル資産”を可視化する方法とは—

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CXチームでの活動に加え、新規プロダクト企画や各地での講演・エバンジェリスト活動にも携わる。

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。

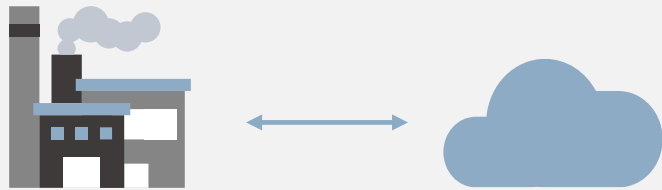
そして、サイバーセキュリティの進化を通して、
人は、人にしかできない、創造性を活かした仕事に注力できる、
社会の進化にも貢献していきます。

DXとAIが変えた サイバーセキュリティの「前提」

| DXの進展・AIの進化により「攻撃される前提」でのリスク管理が重要に

DXの進展

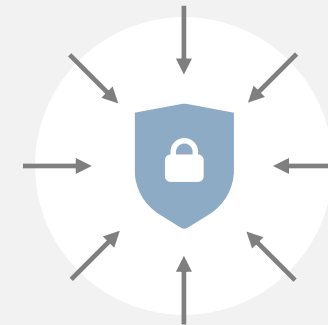
ITとOTが融合し、
ビジネスとデジタルが直結



**サイバー攻撃は
事業存続のリスクに**

AIの進化

サイバー攻撃のコモディティ化



**攻撃されるのが
当たり前の世界へ**

攻撃される前提のセキュリティ対策：サイバーレジリエンス

攻撃されても、業務やサービスを継続し、被害を最小化しながら素早く復旧できる体制とは？

NIST CSF 2.0のモデルと、対応する対策・ソリューション

← ガバナンス（Govern）：経営層と戦略の統合 →

特定

資産とリスクの
可視化

ASM、脆弱性管理
ID/アクセス管理

防御

権威の
侵入・拡散を阻止

EPP/EDR、DLP
ネットワーク
セキュリティ

検知

脅威の早期発見
分析

SIEM
脅威インテリジェンス

対応

インシデントの
迅速な封じ込め

SOAR
インシデント
レスポンスサービス

復旧

事業継続の
確保

｜ 今やるべきは「特定」：資産とリスクの可視化

攻撃される前提で考えた時に、資産とリスクを可視化していることが重要



「見えないものは守れない」

攻撃対象を特定（把握）することが、サイバーレジリエンス強化の第一歩

「静的」IT資産とはひと味違う「デジタル資産管理」の難しさ

攻撃者に狙われやすいにもかかわらず、シャドーITやガバナンスの整備が追いつかない状況。

可視化が難しい



誰が/何を/どこで/どのように
使っているか把握できない

攻撃対象になりやすい



デジタル資産は誰でもアクセス可能
常に攻撃にさらされている

ガバナンスが追いつかない



社内ルールやガバナンスが
導入スピードに追いつかない

｜ 孫子も「己を知ることの大切さ」を説いている

敵を知り、己を知れば、百戦殆(あやう)からず

敵を知る = 脆弱性診断

攻撃者がどのように攻めてくるか予め知っておき、
それに備えられるよう訓練しておく

己を知る = ASM

自分たちの資産(城砦、兵糧、武器…)を予め把握し、
弱いところ・守るべきところを押さえておく



| お客様から伺う「脆弱性診断」のお悩み

公開するWebサイトや
提供するWebサービス
が増えている



開発規模・サイト規模
が大きくなっている
(100画面以上ある)



機能改修・追加など
リリース頻度が高く
間隔も短くなっている



でも…

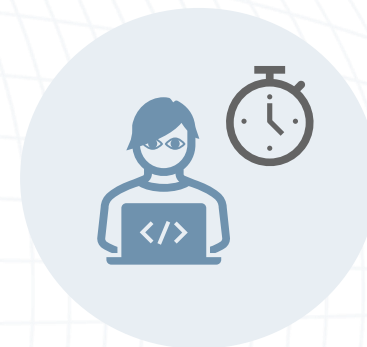
予算が限られている

人員も限られている

| お客様から伺う「ASM」のお悩み

探索のためにはヒントが必要

把握できていない攻撃面を知りたいが、手がかりがない。
だからASMを使って探索したいのに…ヒントが必要って…



本当に自社の資産なのか怪しい

類似する他社のWebサイトが紛れ込むし、発見経路や
検出理由もわからない。精査するのに手間と時間が…





待てよ、**生成AI**とか使えないかな…？

生成AIが「スゴイ」時代になってきた

スピードがすごい

わずか数秒・数分で
処理完了。



調査、文章生成、コード生成
など、多くの業務が圧倒的に
高速化されている。

精度がすごい

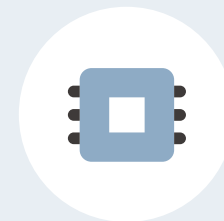
驚くほどの理解力と
分析力。



文脈理解・論理展開・目的把握
ができるため、精度の高い
提案やレポート生成が可能に。

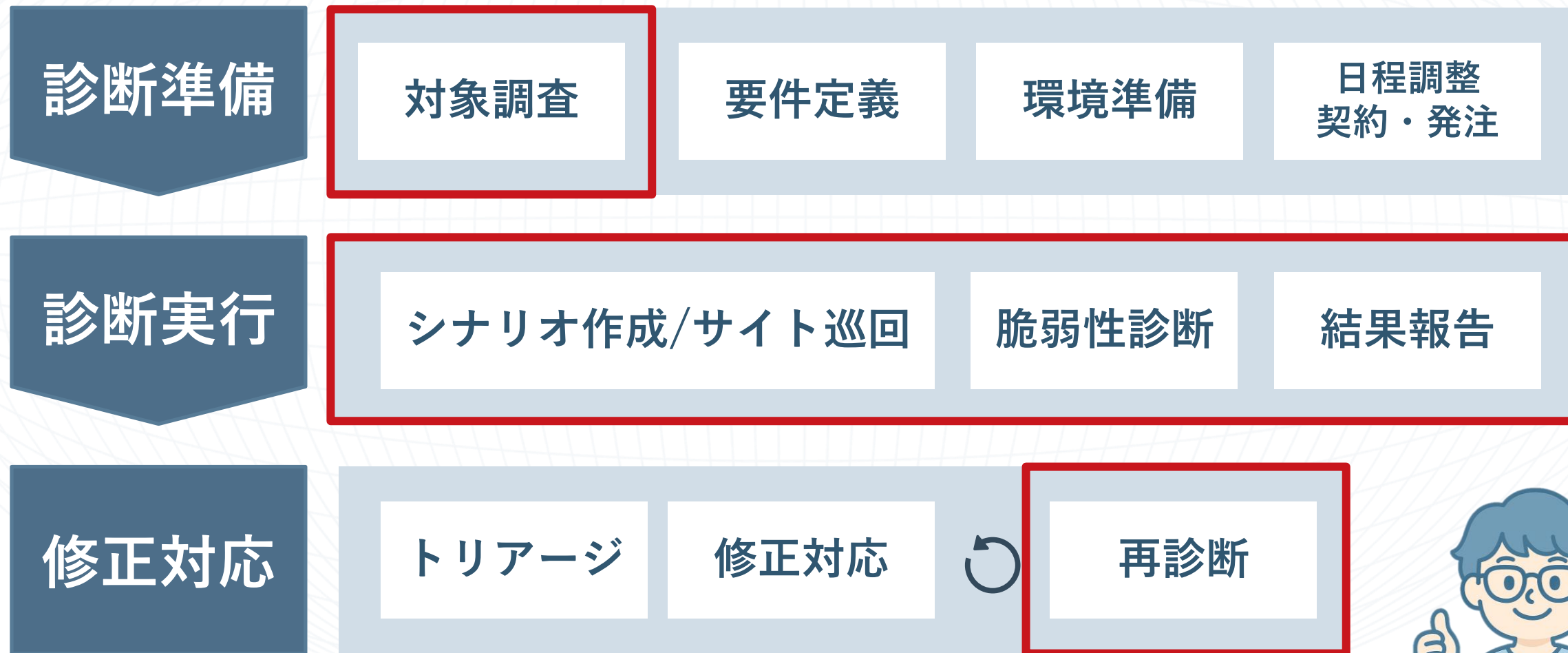
性能がすごい

膨大なデータを瞬時
に読み解く。



学習済みの膨大な知識に加えて、
構造化されていない情報も
文脈で判断可能。

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

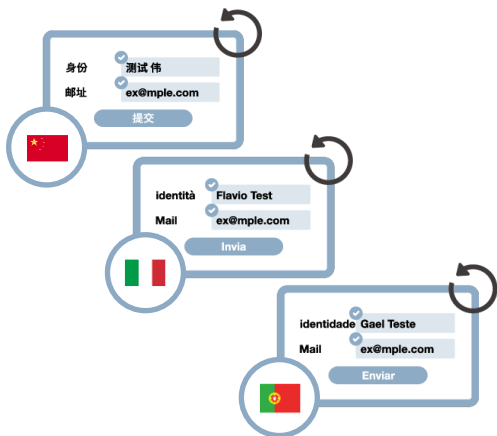


| 生成AIを組み込むことで、多様なWebサイト・多様な脆弱性に対応

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

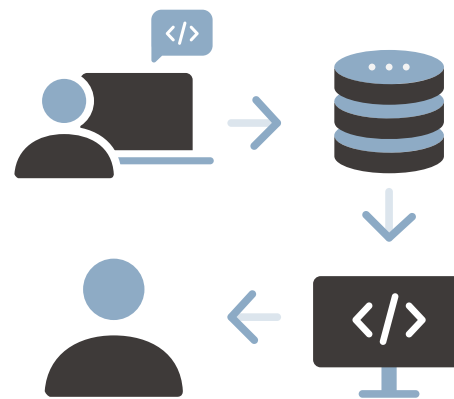


日本語	ポーランド語
英語	スペイン語
フランス語	ポルトガル語
中国語	ロシア語
韓国語	スウェーデン語
オランダ語	アラビア語
ドイツ語	...
イタリア語	

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



生成AIが、Webサイトの属性を自動判定し&重要度をランク付け

サイト用途		保持データ	利用技術
Medium	Low	High	Low
<ul style="list-style-type: none">ECサイトVPN管理サイト	<ul style="list-style-type: none">外部SaaSサイトテストサイト	<ul style="list-style-type: none">個人情報クレジットカード情報	<ul style="list-style-type: none">WordPressEC-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」をもとに判定することで

効率的なリソース配分・戦略的セキュリティ対策を実現

｜サイバーレジリエンス強化は「知る」ことから始めよ！

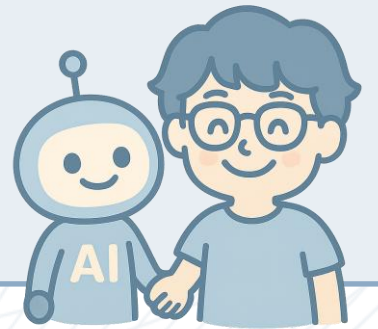
脆弱性診断で「敵」を知り
ASMで「己」を知る

×

生成AIを活用して
継続的・網羅的な対策を実現

AIと

継続的かつ網羅的に
サイバーレジリエンスを強化！



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

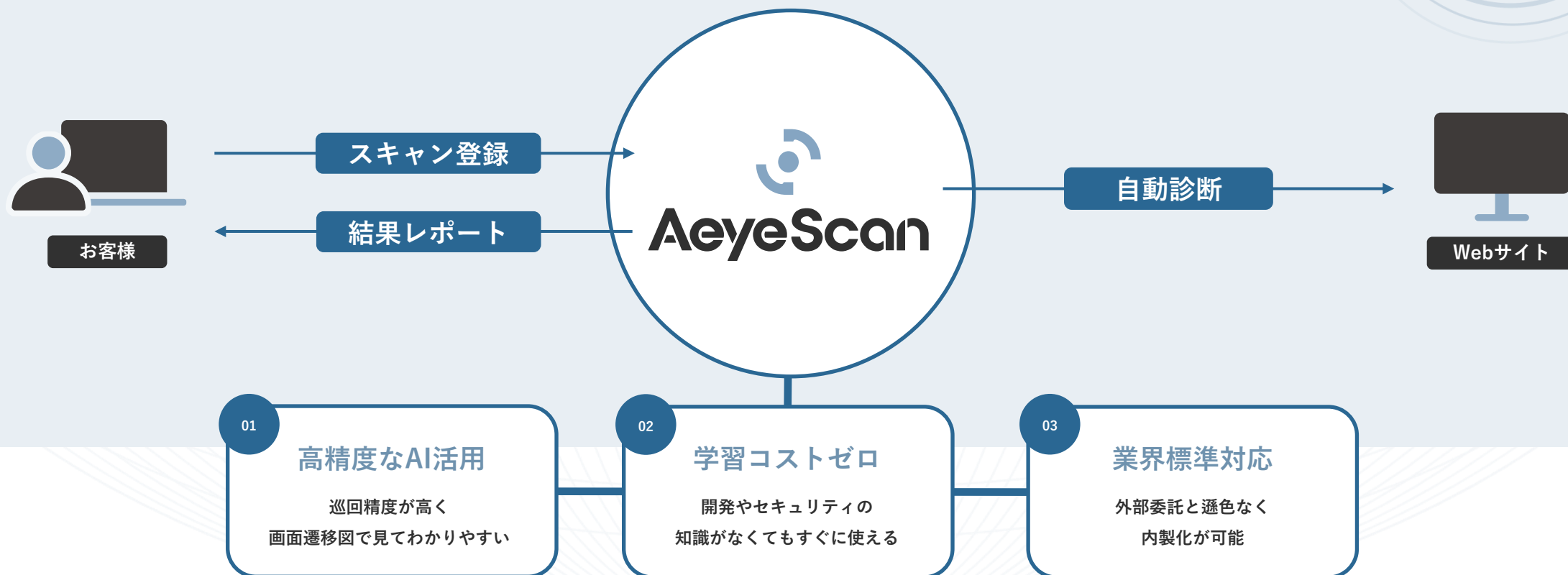
国内市場シェア

No.1※

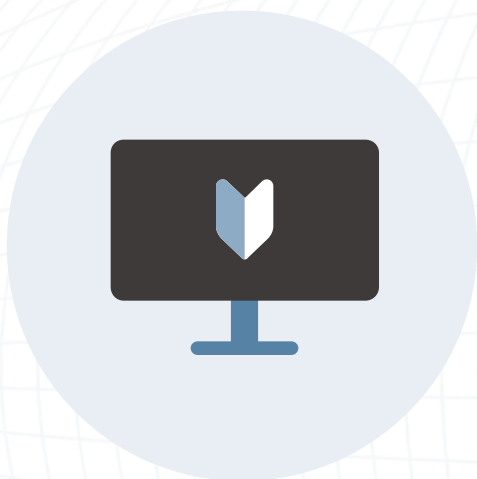
※ 富士キメラ総研調べ「2024 ネットワークセキュリティビジネス調査総覧 市場編」
Webアプリケーション脆弱性検査ツール〈クラウド〉2023年度実績

※ 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（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。

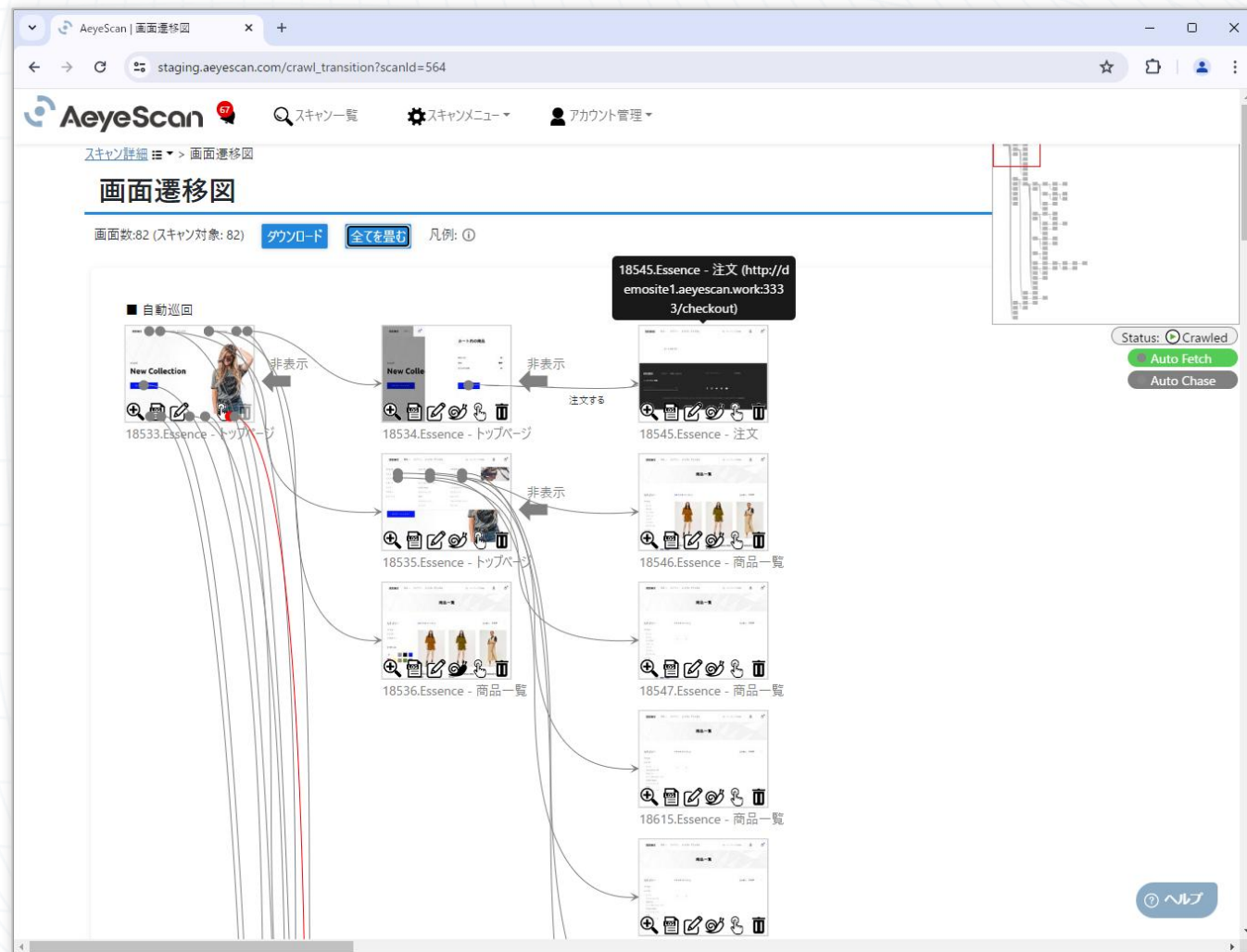
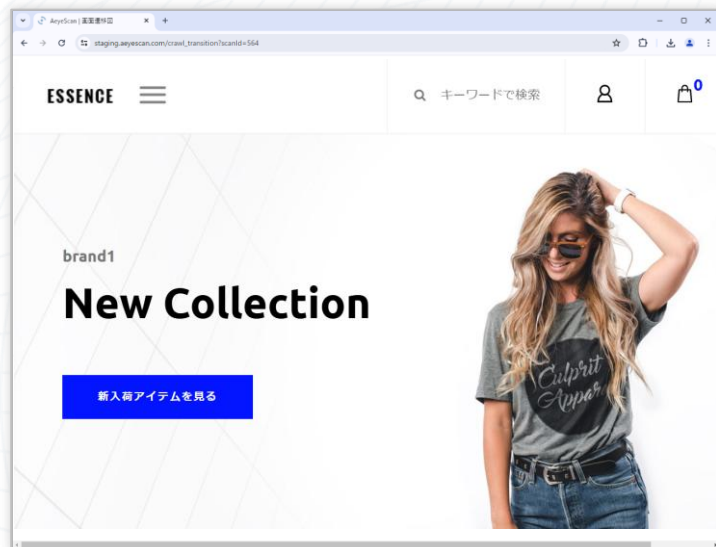


わかりやすいレポート



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。

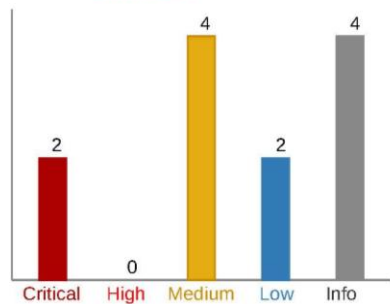
巡回時に、自動で画面遷移図を生成



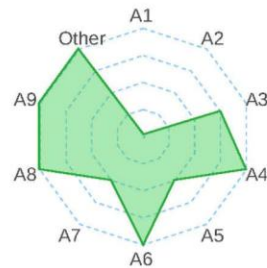
結果がわかりやすく、すぐさま修正作業に取り組めるレポート

スキャンサマリー

全体評価 **Critical**



深さごとのサマリー



OWASP TOP 10 カテゴリー

脆弱性の深さはCVSSv3 (<https://www.ipa.go.jp/security/vuln/CVSSv3.html>) に基づき以下の基準で設定しています。

深さ	CVSSv3基本値	脆弱性に対して想定される脅威
Critical	9.0～10.0	・ リモートからシステムを完全に制御されるような脅威 ・ 大部分の情報が漏えいするような脅威 ・ 大部分の情報が改ざんされるような脅威
High	7.0～8.9	
Medium	4.0～6.9	・ 一部の情報が漏えいするような脅威 ・ 一部の情報が改ざんされるような脅威 ・ サービス停止に繋がるような脅威 ・ その他、Critical/Highに該当するが再現性が低いもの
Low	0.1～3.9	・ 攻撃するために複雑な条件を必要とする脅威 ・ その他、Mediumに該当するが再現性が低いもの
Info	0	

クロスサイトスクリプティング

スキャン情報

948. スキャン結果 ブランドECサイト (<http://demosite2.aeyescan.work:3333/>)

対象ページ

36846.Essence - 登録情報編集 (確認) (<http://demosite2.aeyescan.work:3333/my-page/user-edit>)

[画面遷移図で表示](#)

深刻度

Medium

CVSS: 6.1 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)

スクリーンショット



| 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

製造



インフラ



金融



メディア



人材・教育



エンタメ



Leverages



SaaS



SI・IT企業



セキュリティ企業



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！

デモ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。

ハンズ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



オフラインイベントも是非お申込みください！

AeyeSecurityLab

触って試して専門家に相談できる！

脆弱性診断ツール 比較・体験セミナー

参加
無料

2025
11.13

会場: 神田スクエア
木 15:30-17:00

株式会社エーアイセキュリティラボ
執行役員 兼 CX本部長
関根 鉄平 CISSP

株式会社エーアイセキュリティラボ
CX本部プリセールスリーダー
高橋 貴弘





AeyeScan

セキュリティに、確かな答えを。