
いま進めるべき

脆弱性対策への生成AI活用

診断からASMまで、セキュリティの現場を変える
「精度アップ」の最新事情

登壇者紹介

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

セキュリティエンジニアとして大手金融機関等の脆弱性診断に従事。その後、Webアプリケーション検査ツール・サポートチームの立ち上げをしつつ、CSIRTや開発現場でのセキュリティを推進。

2020年6月より現職。AeyeScanのカスタマーサクセスチームの責任者として脆弱性診断の内製化を支援。大規模イベントや大手企業での講演に多数登壇。

『セキュリティエンジニアの知識地図』を共著。



コミュニティ
活動など

- 情報セキュリティ10大脅威 選考会メンバー
- OWASP/ISOGJ アジャイル開発におけるセキュリティ | パターン・ランゲージ
- OWASP/ISOGJ Webシステム／Webアプリケーションセキュリティ要件書

「脆弱性診断」界隈で「よく聞くお悩み」

予算が限られている

人員も限られている



対策すべき範囲 **増**

必要な対策の幅 **増**

「脆弱性診断」界隈で「よく聞くお悩み」

特に以下のような企業さまから、「診断のスケジュール調整が困難」「組織全体のWebサイトを把握しきれていない」といったお声を伺います。



複数のWebサイト
やWebサービスを
提供している



Webサイトの
規模が大きい
(100画面以上ある)



機能改修や
サービス追加など、
リリース頻度が高い



課題解消のカギを握るのは、「脆弱性診断ツールの精度」

| ① 脆弱性診断ツールの精度が低いと、結果の信ぴょう性に欠ける

精度が低いツールでは類似ページの判断ができず、同じ画面を多数巡回／診断してしまう



診断結果の出力まで
かなりの時間がかかる



誤検知の割合が高まる

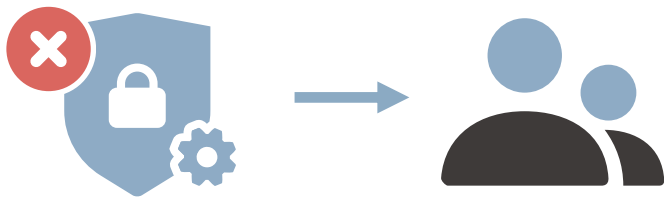


② 脆弱性診断ツールの精度が低いと、人的コストが膨らむ

精度の低さによる弊害はツールのチューニングによる回避が可能だが、
専門知識をもった人材による設定が必要



結局人手をかけなければ
ならない事態に



専門知識をもつ貴重な人材の
時間が取られてしまう



「精度」の課題は 生成AIで解決できる

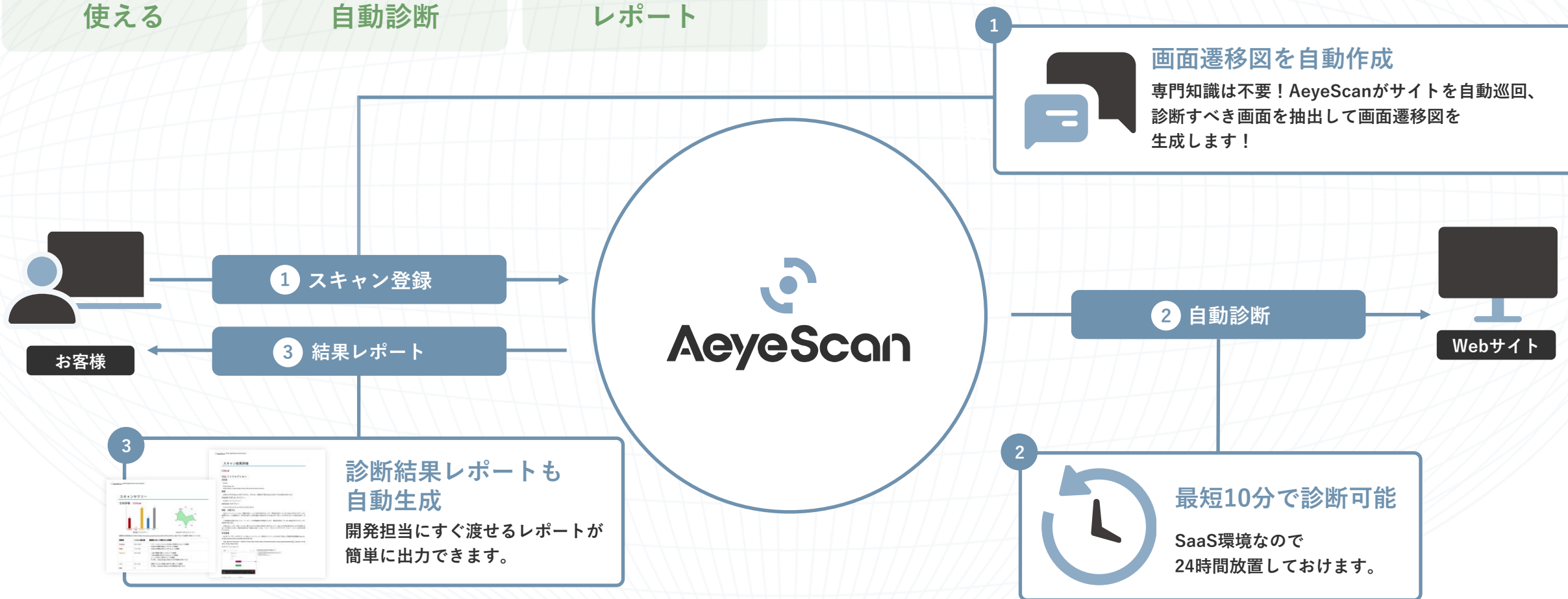
生成AI活用により、自動化の精度を向上させることが可能
人手をかけずにセキュリティを強化できる

生成AIを活用した脆弱性診断ツールなら、高精度な診断が簡単にできる

誰でも簡単に
使える

AIによる
自動診断

わかりやすい
レポート



AI活用のレベルが高いため、巡回が高精度で範囲が広い

例：AIによるフォーム入力値の判断処理

課題

フォーム入力は正しい値を入力する必要がある。
間違えると、**入力エラーとなり遷移できず診断が進まない...**

AeyeScanなら、
正確に入力値を推測して巡回！

！ココがポイント

名前や住所など決まった項目だけでなく、
どんな項目にも対応！



クレジットカード

例えば



画像アップロード

フォームを自動認識しラベル化

登録フォーム

姓名	
郵便番号	
住所	
電話番号	
メールアドレス	

確認する →

自動認識したラベル(赤枠)に応じ
適切な入力値を設定

姓名
姓名(カタカナ)
姓名(ひらがな)
姓
名
姓(カタカナ)
名(カタカナ)
姓(ひらがな)
名(ひらがな)

正常遷移

適切な値を入力

登録フォーム

姓名	巡回 太郎
郵便番号	000-0000
住所	東京都 江東区...
電話番号	03-0000-0000
メールアドレス	taro@example.com

確定 →

生成AIを使えば、巡回はここまで進化できる

認識AIができること

画面上の入力フォームのラベル（氏名など）を
認識AIが判断することでフォームに入力する



生成AIができること

生成AIを使うことで、人が画面を見るように
「これは商品画面」「これはお知らせ画面」と
判断できる！



これまで手動でしか診断できなかった項目にも対応

生成AI機能

認可の不備の脆弱性

検出手順

- 1 サイト巡回時に「どの画面が管理者機能であるか」をChatGPTに推測させる
- 2 一般ユーザ権限でログインした際に「推測した画面へのボタンやリンクがない」場合に管理者機能であると判定する
- 3 スキャン時に、一般ユーザで管理者メニューを表示できるか検証する



管理者メニュー



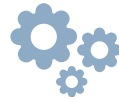
一般ユーザーメニュー

生成AIの活用による高度な自動化を実現

生成AI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

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



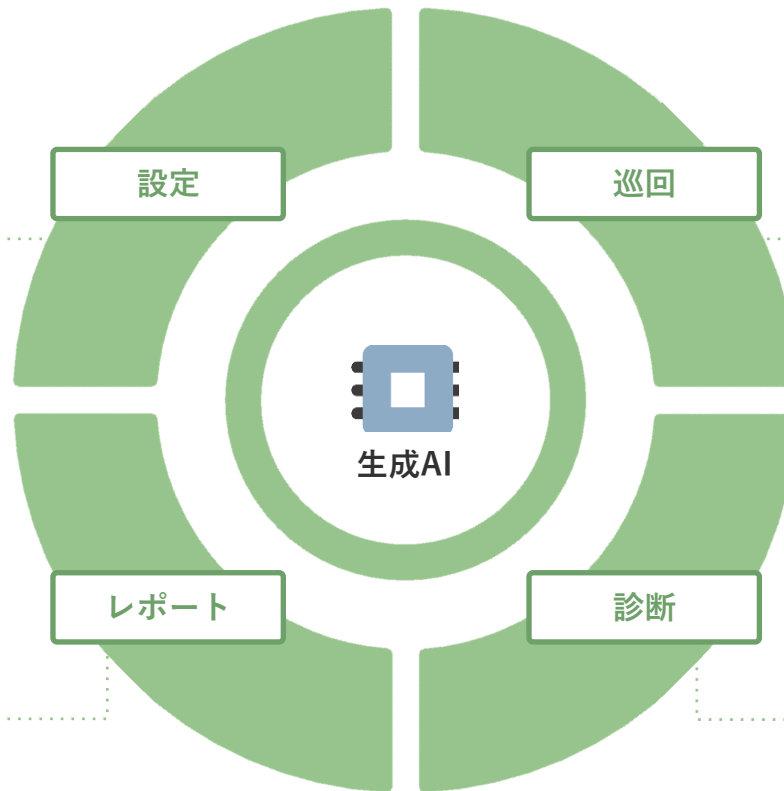
特許 第7320211号

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



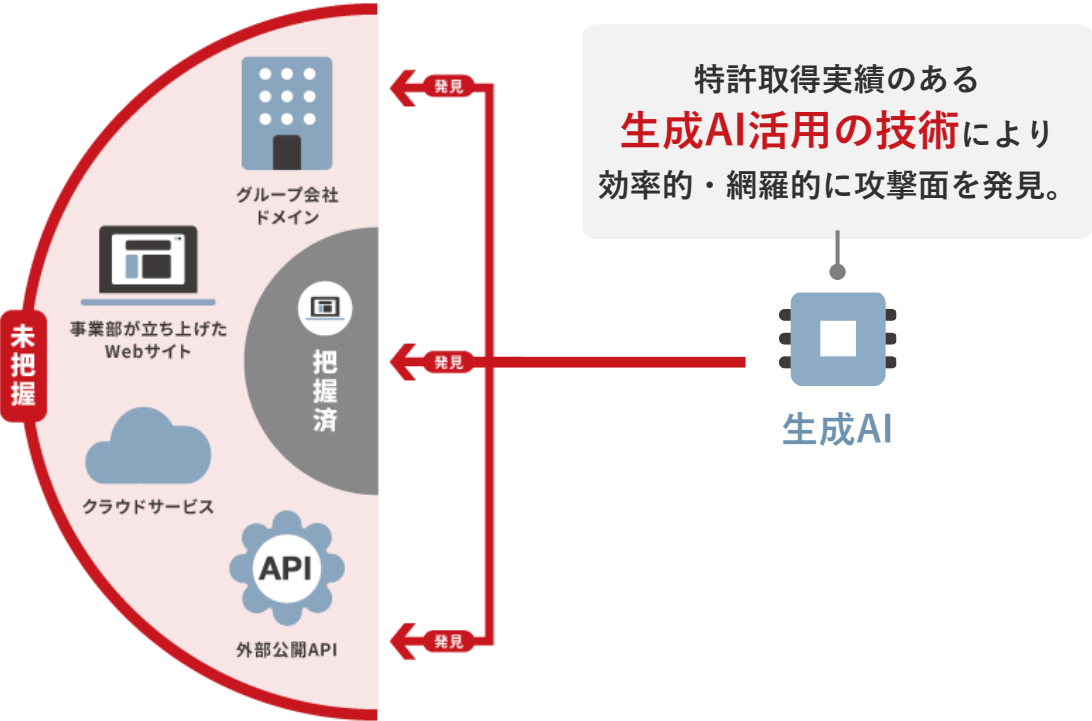
生成AI活用で、工数をかけずにWeb-ASMを実現

 Web-ASM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



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！

ASMツールの精度が低いと、結局人が精査する必要がある



ASMの抽出アルゴリズムの関係で、不正確な情報を検知してしまい、人手をかけて精査する必要がある出てくる。

例：不正確な情報の検知



自社で管理していないサイトが発見される



誤った情報が報告される

生成AI活用により、攻撃面を高精度で発見できる

Web-ASM機能

文字列を解読するほか、SSL証明書の情報やWeb公開済みのIR情報など膨大な情報源から総合的に判定。さらに発見経路・理由も提示。

例

山田自動車と、山田自動車部品の膨大な検索結果



膨大なWebの検索結果

帳票振り分けAI

山田自動車



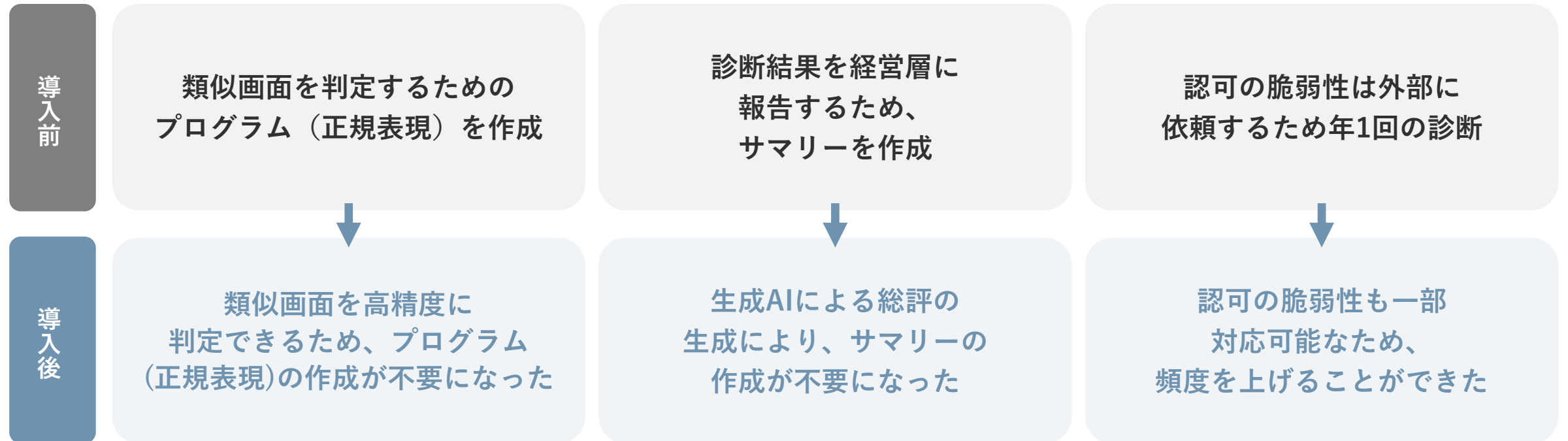
山田自動車部品



組織外のサイト



生成AI機能を導入したA社さまの事例



脆弱性診断への生成AI活用で、セキュリティ担当者の工数を削減しよう
そして空いた時間は、より高度なプロジェクトや業務に充てよう

 **AeyeScan** (エーアイスキャン) により
セキュリティ対策にかかる **コストを削減!**



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※



有償契約
200社以上

※ 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）

プロが認める品質・精度

セキュリティベンダーやSIerでも
顧客向けサービスとして活用



ブラウザ上での直感的な操作

専任エンジニア不要、情シスや開発部門でも
安定した運用が可能

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



エンタメ



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





AeyeScan

セキュリティに、確かな答えを。