
AIで脆弱性診断を自動化し、デジタル領域を守る！

攻めのDXを実現する 「戦略的」セキュリティ対策

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・海外事業展開など全社横断プロジェクトにも携わる。

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。

誰でも簡単に

プロさながらの高度な
脆弱性診断を



進む「DX」 増える「セキュリティ対策の悩み」

| やらないと死ぬDX、年々高まる人材需要

DXの推進は、多くの組織において取り組むべき重要課題とされている一方、DX人材の不足が慢性化している状況にある。

DXの戦略立案や統括を行う
人材が不足している

69.2%

DXを現場で推進、実行する
人材が不足している

65.4%

DXを取り巻く状況

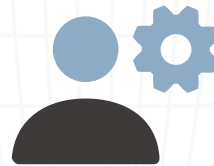
DXの進展に伴い、ITシステムの連携・整備やデータ活用が新たな価値創出の源泉となった結果、デジタルサービス・システムの開発機能の内製化が加速している。

IPAが提言するDXに必要な要素

ビジネス環境の変化に
迅速に対応できる
ITシステムの整備



競争領域を
強化するための
社内外システムの連携



ビジネス上の
ニーズに合致する
データ活用と分析



DXの進展でセキュリティ対策の需要は高まっている



デジタルサービスの開発・提供
自社で管理すべきデジタル資産

増

×

急速な技術の進化

||

必要なセキュリティ対策の

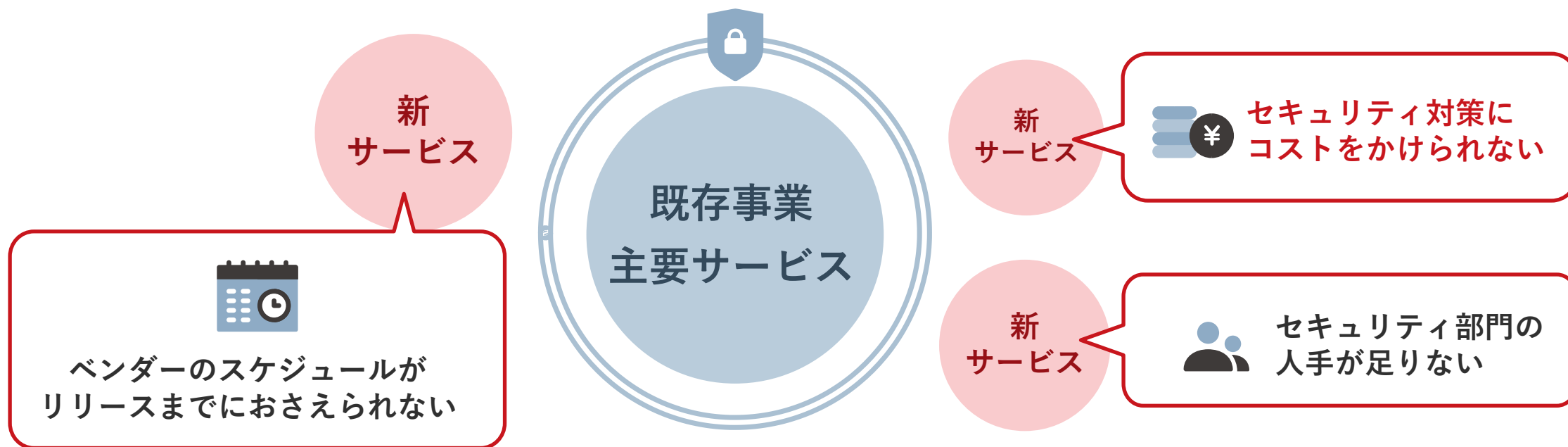
対応範囲は
拡大

難易度は
上昇

DXの進展に伴う「セキュリティ対策の悩み」

① 対応範囲は広がる一方、時間・予算・人材は足りない

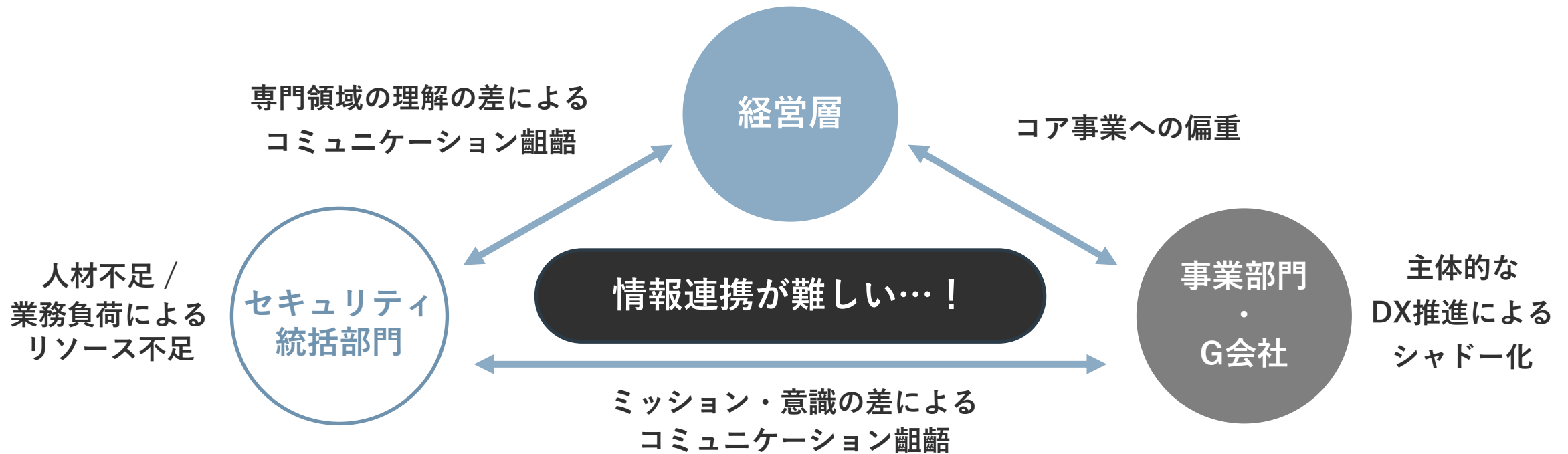
新しいデジタルサービスが次々と生みだされる一方で、事業立ち上げ段階から万全のリソースをかけてセキュリティ対策を行うことは困難であり、事業スピードとの両立が課題化しやすい。



DXの進展に伴う「セキュリティ対策の悩み」

② ステークホルダーが増え、連携が難しくなった

セキュリティガバナンス実現のため、部門や役割を超えたコミュニケーションが求められる。



セキュリティ対策の悩みを克服する 「戦略的」思考とは

セキュリティ対策の「戦略的」思考

「戦略的な」セキュリティ対策とは・・・

濃淡をつける・取捨選択する・選択と集中

手間と時間をかけて
専門家が対応する

人的リソースを最小化
しつつ対応する

濃

淡

戦略的なセキュリティ対策を実行する上での課題

手間と時間をかけて
専門家が対応する

濃

淡

人的リソースを最小化
しつつ対応する

課題①

専門人材は限られているが、技術的に人間が対応しなければならない範囲が広い

課題②

継続的・網羅的に対応する必要があるが、割ける人的・金銭的リソースは限定的

▼
AIを活用した「自動化・内製化」で解決できないか？

個別のセキュリティ対策・施策から「まずAIを使ってみる」



法令遵守

- デジタル関連法令対応
- コンプライアンス対応
- 業界のセキュリティガイドラインへの準拠

...etc



ミスができない領域
人が考えて対応すべき



ガバナンス強化

- 事業特性に応じたセキュリティポリシーやガイドライン作成
- セキュリティ対応マニュアルの整備と実行管理

...etc



関係者が多く影響範囲が広い
人の精緻な設計が必要



具体的な対策

- セキュリティ製品やサービスの導入
- システム面のサイバー攻撃対策
- 脆弱性診断

...etc



目的と方法を決めれば
対策にAIを組み込める

AIと相性の良いセキュリティ対策：脆弱性診断

継続的・永続的に対策が必要



人力では生産性が上がらない

網羅的に診断することが望ましい



網羅性を高めると費用も増える

AIによる自動化・内製化ができれば
業務の効率化・費用の最適化につながりやすい

AIを活用した 脆弱性診断の自動化・内製化

脆弱性診断を自動化・内製化するときに考えること

「内製化できればいいんだけどな…」



?

診断の品質を維持
できるだろうか？

?

コスト(費用・時間)
を抑えられるか？

?

社内メンバーで対応
できるだろうか？

脆弱性診断を自動化・内製化するときに考えること

?

診断の品質を維持
できるだろうか？

?

コスト(費用・時間)
を抑えられるか？

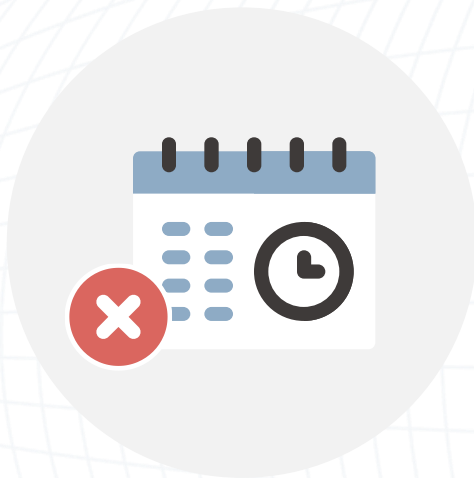
?

社内メンバーで対応
できるだろうか？

+

事業部門・開発部門に内製化の協力を得られるか？

実際に事業部門と向き合う中で直面する「壁」



課題 1

稼働を割きたくない

診断に時間を取られたくない
スケジュール調整したくない
なるべく対応したくない



課題 2

コストをかけたくない

計画にセキュリティコストを含めていない
診断環境を用意したくない



課題 3

セキュリティ意識が低い

診断とは何をするものなのかがわからない
セキュリティを意識しようと思っていない

脆弱性診断の自動化・内製化に必要な要素とは？

① 脆弱性診断のプロセスに
事業部門を巻き込む

② AIを活用した脆弱性診断
ツールの導入

脆弱性診断の自動化・内製化に必要な要素とは？

① 脆弱性診断のプロセスに事業部門を巻き込む

事業部門とセキュリティ部門で一緒に脆弱性診断を行うことのメリットを訴求

早期に脆弱性を発見することで
開発終盤での手戻りを最小化できる
(シフトレフト)

業務やサービス仕様に詳しいチームが
診断に参加することで
診断の精度・網羅性が上がりやすい

脆弱性診断の自動化・内製化に必要な要素とは？

② 脆弱性診断ツールの導入

事業部門を巻き込む前提で考えた場合、ツール選定に必要なポイントは…

1 誰でも使える操作性



2 利用範囲に制限がない



3 結果がわかりやすい



ほんとに自動化・内製化できるの…？

| アイフル様の場合

内製化前の状況

- 外注していたWebアプリ開発を内製開発に移行していた
- 一方、脆弱性診断の外部に診断を委託していた
- 委託コストと、ベンダー調整工数が大きな悩みの種

不安ポイント

社内・開発チームでも使いこなせるかどうか



内製化にあたっての不安・懸念

- Webアプリ開発エンジニアが、自社Webアプリの脆弱性診断を行うことはできるのか…？
- 診断まではできたとして、脆弱性の修正まで自分たちで完了できるのか…？

| アイフル様の場合

内製化に一步を踏み出せた理由

簡単 & 学習コストが低い

操作ガイド、FAQ、サポートが充実
アプリ開発のエンジニアも自力で習得

自力で修正まで完了できる

エンジニアも理解できる診断結果レポートで
毎回セキュリティ部門が支援しなくてもいい

開発部門側でいつでも・だれでも脆弱性診断ができる状態を実現
安心安全なサービス開発ができ始めている

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

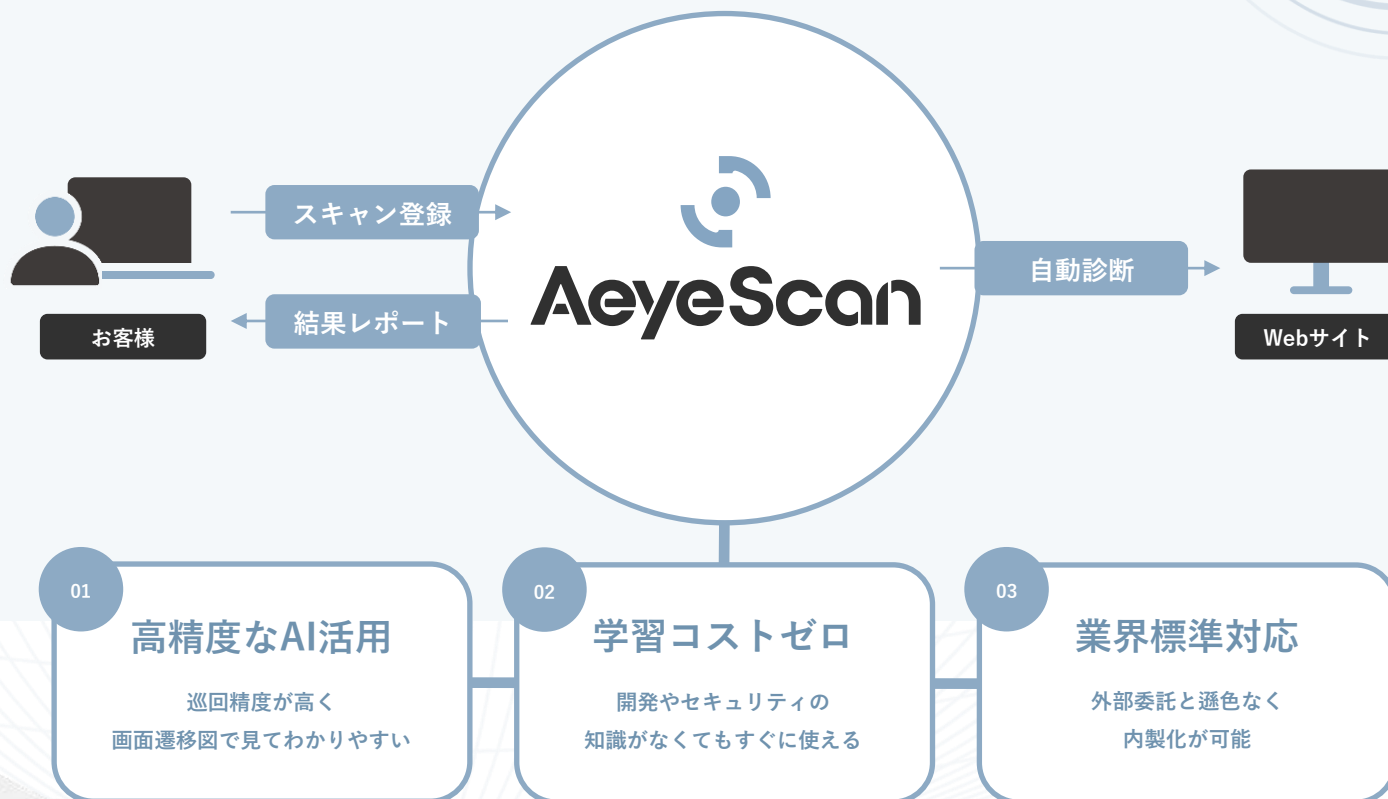
国内市場シェア

No.1※

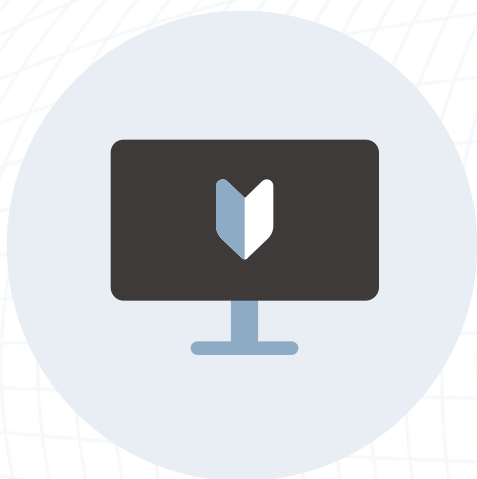
※富士キメラ総研調べ「2023ネットワークセキュリティビジネス調査総覧 市場編」
(Webアプリケーション脆弱性検査ツール(クラウド)2022年度実績)

※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)

有償契約
200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。

| 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



エンタメ



SaaS



SI・IT企業



セキュリティ企業



生成AIの活用による高度な自動化を実現

オプション機能

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

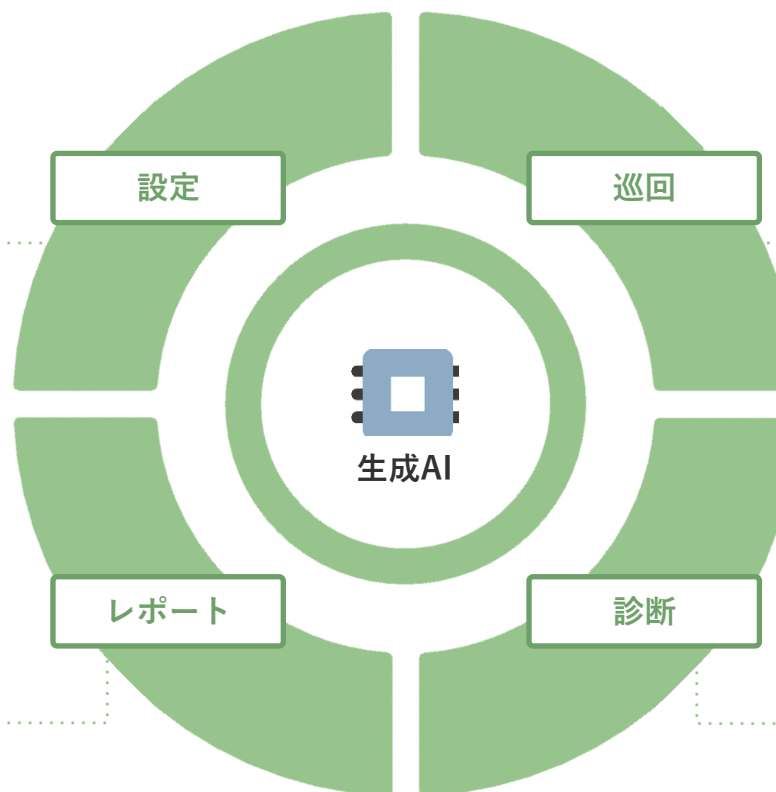
- ・多言語対応
- ・フリーフォーマットでの指示
- ・画面の自動類似判定



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



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

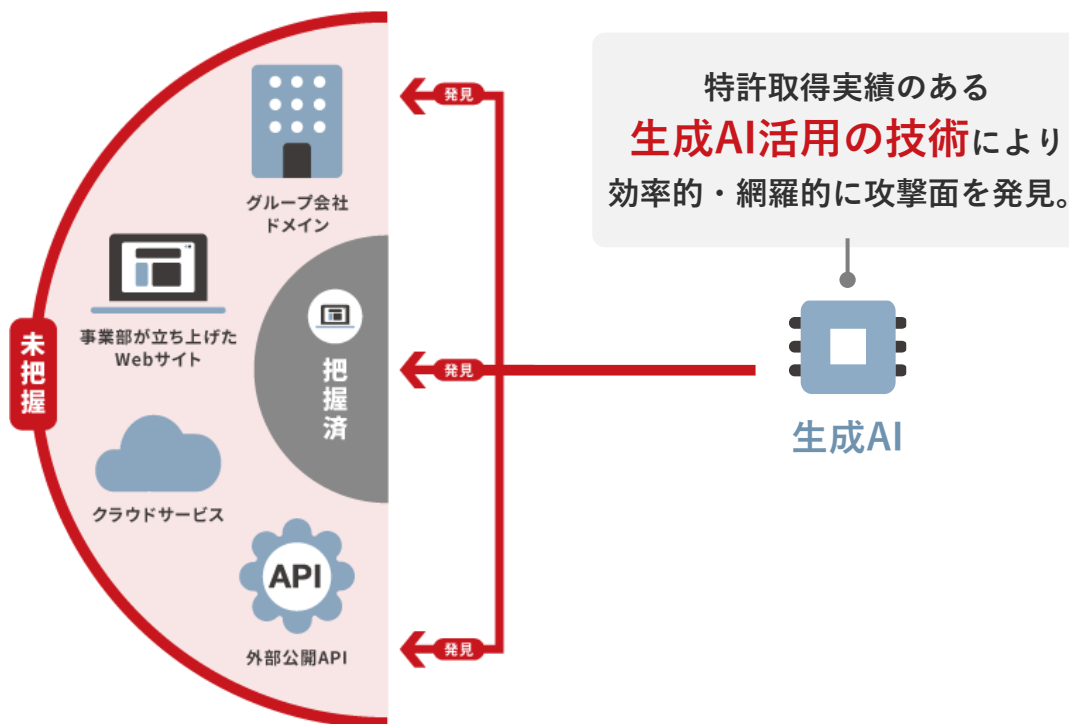
生成AI活用で、工数をかけずにWeb-ASMを実現

オプション機能

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のスク্যানによる



Web-ASMの実施ステップ

1

攻撃面の
発見

Web-ASM機能

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

自動巡回

未把握のドメインを
巡回対象に追加

3

攻撃面の
リスク評価

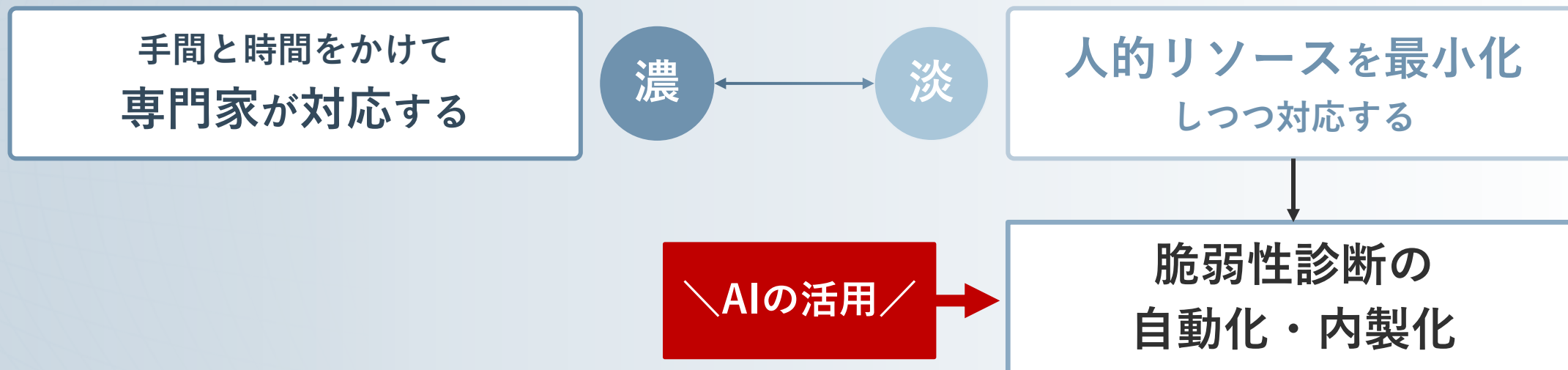
脆弱性診断

管理対象の全ドメインに
脆弱性診断を実施**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！

本日のまとめ

AIで実現する戦略的なセキュリティ対策



AIを活用して「攻め」と「守り」を両立しましょう！

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 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。