生成AIを活用した
「人手をかけない 脆弱性診断 」で、
DX推進とセキュリティを両立

登壇者紹介

株式会社エーアイセキュリティラボ

代表取締役社長 **青木 歩**（あおき あゆむ）

セキュリティ業界20年以上
サイバー攻撃へのセキュリティ対策分野で活動

2000年よりセキュリティ事業に従事。
大手企業のグループ会社、セキュリティ専門企業にて、
企画、営業・マーケティング等幅広い業務に携わる。
その後、組織立ち上げ、責任者を歴任。

本日お話したいこと

- DXの進展がもたらすセキュリティへの影響
- セキュリティ対策の実行における主要課題の洗い出し
- 生成AIを用いた「AeyeScan」のデモンストレーション
  およびフィンテック領域での活用事例をご紹介

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%

参考：IPA「DX動向2024： https://www.ipa.go.jp/digital/chousa/dx-trend/eid2eo0000002cs5-att/dx-trend-2024.pdf」

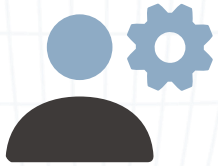
DXを取り巻く状況

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

参考：IPA「DX動向2024： https://www.ipa.go.jp/digital/chousa/dx-trend/eid2eo0000002cs5-att/dx-trend-2024.pdf」

DXの進展がもたらすセキュリティへの影響

自社で管理すべきデジタルサービス・資産の増加に伴い、セキュリティ対策の対象範囲は劇的に拡大し、それに伴い対策の複雑性と実現難易度も一層高まっている。

DX	セキュリティ
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 × 急速な技術の進化	増 → 必要なセキュリティ対策の **対応範囲も広く…** **難易度も高く…**

DXの推進にセキュリティ強化は不可欠だが、その実現には多くの課題が存在

DXの進展によって生じたセキュリティ課題

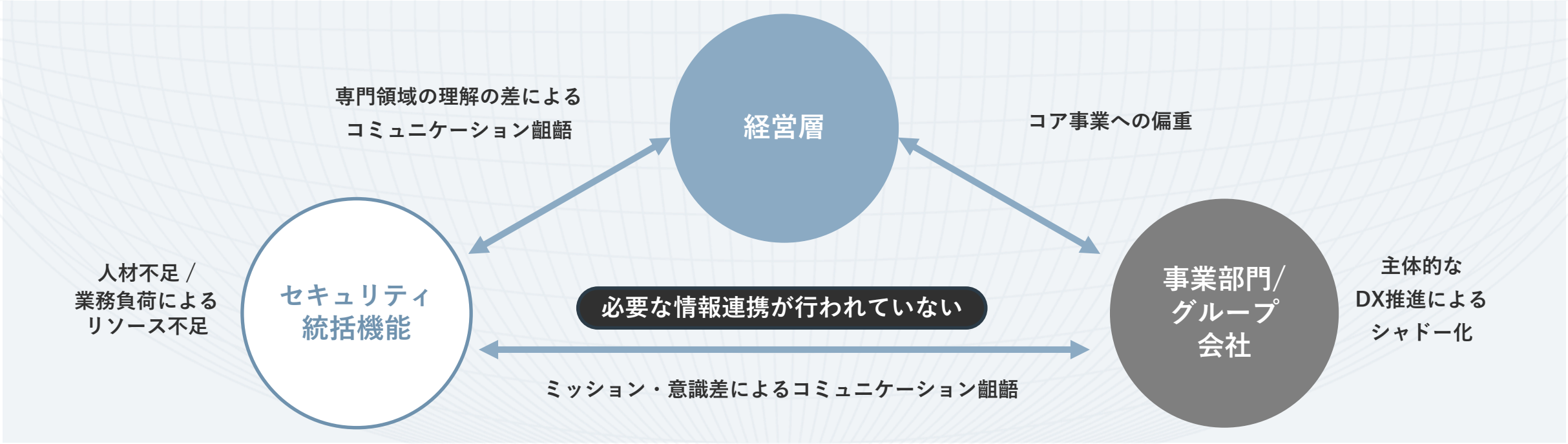
❶ 時間・予算・人材の不足

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の進展によって生じたセキュリティ課題

❷ 部門間での連携の難化

組織全体でセキュリティガバナンスを効かせるために、部門や役割を超えたコミュニケーションが求められる。セキュリティガバナンス強化に向けリソースを効率良く配分する必要がある。



DXの進展によって生じたセキュリティ課題

❸ セキュリティ対策の必要量も急増

例えばWebサイトのセキュリティ対策を例にとっても、求められる対策の量は膨大であり、
あらゆる項目をすべての対象に徹底して実施することは容易ではない。

Webアプリケーションのセキュリティ対策

① ファイルの公開設定
② Webページの公開設定
③ 脆弱性への対策
④ ソフトウェアの脆弱性対策
⑤ エラーメッセージの設定
⑥ ログ管理
⑦ 暗号化
⑧ 不正ログインへの対策

Webサーバのセキュリティ対策

⑨バージョンアップを行う
⑩ 不要なサービス・アプリケーションの停止
⑪ 不要なアカウントの削除
⑫ 安全なパスワードの設定
⑬ アクセス制御
⑭ ログ管理

ネットワークのセキュリティ対策

⑮ 不要な通信の遮断
⑯ 通信のフィルタリング
⑰ 不正な通信の検知・遮断
⑱ ログ管理

その他のセキュリティ対策

⑲ クラウドサービスへのセキュリティ対策
⑳ Webアプリケーション・Webサーバ・ネットワークへの定期的な脆弱性診断

では、どうするべきか…？

DXとセキュリティを両輪で進めるために必要な「AI活用」

人手やコスト・時間が限られる中でセキュリティを担保するためには、対応に濃淡をつけつつ、
リソースを効率良く配分する方法を考える必要がある。その方法のひとつが、AI活用といえる。

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

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いけない範囲が広い

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」も必要

セキュリティ領域におけるAI活用

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活用と相性のよい、デジタルサービス領域の脆弱性診断

Webサイトを狙うサイバー攻撃が増加する中、日々新たな脆弱性が明らかになっており、
対策もアップデートし続けなければならない。

継続的・永続的に対策が必要となる	⟷ 人間が対応していると継続的・永続的に工数を取られて生産性が上がらない
自社Webサイト・Webサービスを網羅的に診断することが望ましい	⟷ Webサイト・Webサービスが増える度に、必要な費用も増えてしまう

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**つながりやすいと言える**

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

脆弱性診断のプロセスに事業部門を巻き込むためのポイント

1

ファーストステップは限りなくシンプルに

可能な限り新しいタスクは
増やさず、最初の１歩目を
無意識に踏み出せる

2

事業部門・開発部門にメリットがある

事業部門・開発部門の
日常業務に組み込むことで
彼ら自身の業務を効率化

3

支援の姿勢を示す

困った時に
気軽にコミュニケーションが
とれる状態にしておく

事業部門を巻き込む前提で考えた場合のツール選定ポイント

1 誰でも使える操作性

ツール習得コストがかからず
事業部でも簡単に利用できる

2 利用範囲に制限がない

画面数やサイト数に制限がなく
いつでも・いくらでも使える

3 結果がわかりやすい

エンジニアでも、問題箇所や
リスク、修正方法がわかる

情報集約・管理が円滑になることで
戦略策定や人材育成などの業務に人手を割ける

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

01
高精度なAI活用
巡回精度が高く
画面遷移図で見てわかりやすい

02
学習コストゼロ
開発やセキュリティの
知識がなくてもすぐに使える

03
業界標準対応
外部委託と遜色なく
内製化が可能

AeyeSecurityLab

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

AISIN
KOSÉ
SAKI
TIGER
Mizuno
ユーグレナ

インフラ

HIS
近鉄情報システム株式会社
dmm グループ
Suzuyo
NTT東日本
HITOWA GROUP
Looop

金融

アイフル
JOBPAY
SOMPOひまわり生命
DMM FinTech
Tokyo Century

メディア

集英社
中日新聞
NIKKEI

エンタメ

e+ イープラス
CAPCOM
とらラボ!

SaaS

estie
エムティーアイ
OZ INTERNATIONAL
COACH A Co.,Ltd.
cybozu
JINSOKEN
Schoo
Speee
ZENKIGEN
Direct Sourcing
TAL
TEMONA
NAVITIME
KNOCK ON THE DOOR
BATONZ
VALUE HR
hokan
Money Forward
RUN.EDGE
RVSTA
Rescuenow

SI・IT企業

Rworks
アクモス株式会社
AVANT GROUP
CTC
Insight Edge
Infcurion
SB Technology
SBWorks
NTT DATA
NTTビジネスソリューションズ
Globalway
circlace
さくら情報システム
CEC
tdi
Simplex Inc.
777WORKS
SOFT CREATE
SOLTEC
電通総研
TOPPAN
JOPS
NI+C
Human Interactive Technology Inc.
FUJISOFT
FUJITSU
YONA
リピスト

セキュリティ企業

NEC NECセキュリティ
cybertrust
LAC

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

AeyeSecurityLab

AeyeScanが選ばれている理由

プロが認める機能・性能

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

×

誰でも使える操作性

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

AeyeSecurityLab

AI活用のレベルが高いので、自動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…**

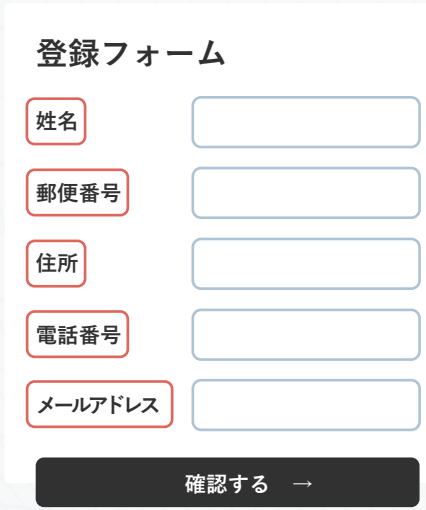
AeyeScanなら、
正確に入力値を推測して巡回！

ココがポイント

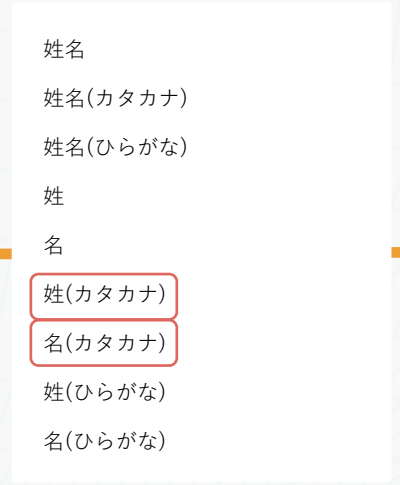
名前や住所など決まった項目だけでなく、
どんな項目にも対応！

例えば
- クレジットカード
- 画像アップロード

フォームを自動認識しラベル化



自動認識したラベル(赤枠)に応じ
適切な入力値を設定



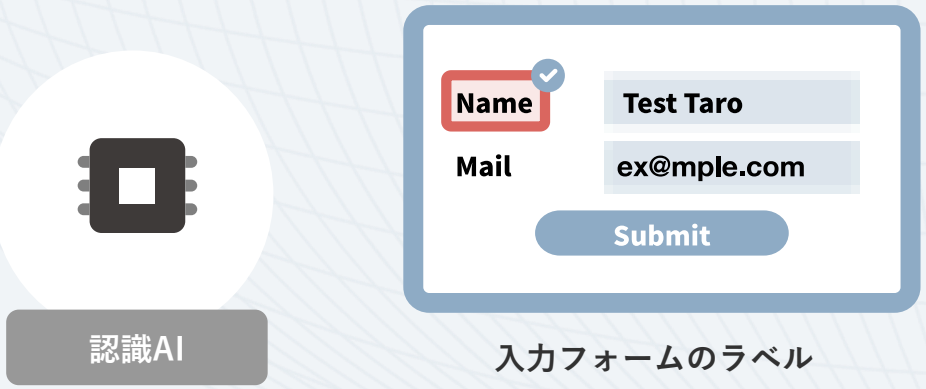
正常遷移

適切な値を入力

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！

AeyeSecurityLab

これまで手動でしか診断できなかった項目も診断が可能に

セカンドオーダーインジェクションによる クロスサイトスクリプティング（XSS）

検出手順

1. 登録/更新した値が表示されそうな画面を生成AI（ChatGPT）に推測させる
2. 値が表示されているか、巡回データを基に判定する
3. 判定結果がTrueの場合、セカンドオーダーインジェクションによるXSSスキャンの対象として診断を実施する

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」を生成AI（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

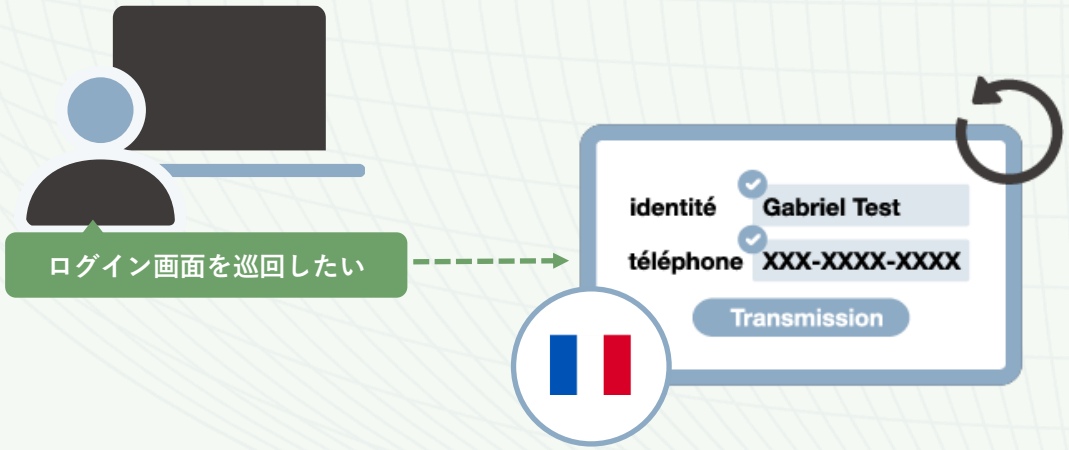
一般ユーザーメニュー

AeyeSecurityLab

自然言語での指示や多言語対応など、生成AIの得意分野も活用

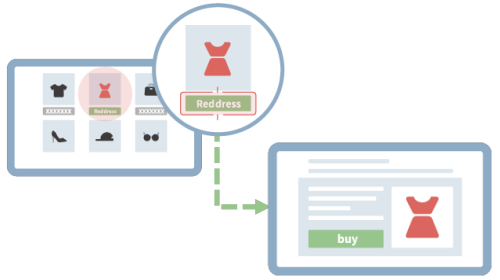
巡回も自然言語での指示が可能に

巡回してほしい画面の機能などを入力すると
指示した箇所のみ巡回



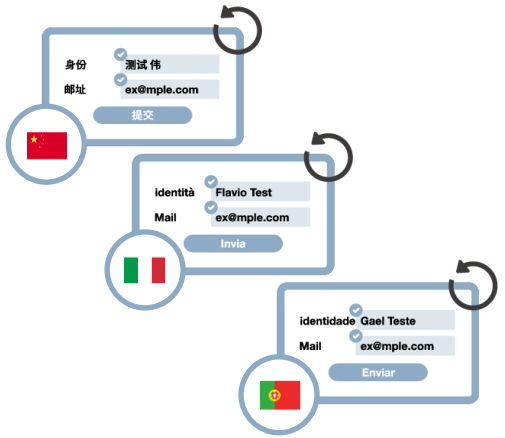
多言語対応により、
日本語以外のWebサイトも幅広く巡回

多言語サイトの把握が可能



日本語サイトと同じように
ボタンやリンクを認識して遷移

フォーム入力も多言語に対応



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

生成AIの活用による高度な自動化を実現

1 診断設定がさらにカンタンに

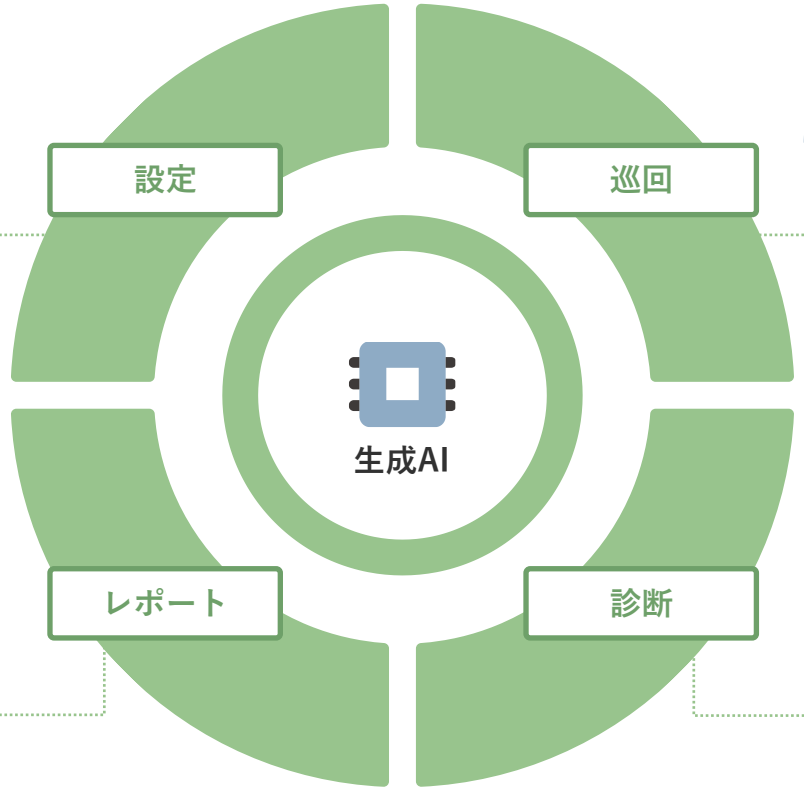
- フリーフォーマットでの指示

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



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

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

導入事例紹介

マネーフォワード様

企業名　株式会社マネーフォワード

事業内容　PFMサービスおよびクラウドサービスの開発・提供

従業員数　2,400人（2024年5月末日現在）

課題

事業が拡大しプロダクトが増えるにつれ、
脆弱性診断の間隔が空いてしまうことが
懸念材料だった

具体的な課題

1. 外注だとナレッジが蓄積されない
2. 外注だと画面数に応じた料金体系で網羅的な診断を受けづらい
3. 開発が遅れた場合、ベンダーとのスケジュール調整が困難

新機能の追加や大規模な改修の際には脆弱性診断を実施していたが、それ以外はプロダクト側の判断に委ねていた。小さな改修のたびに診断を外注するのではなく、内部で迅速に診断する選択肢も持ちたかった。

導入

診断ツールを導入し
継続できなかった経験から、
使いやすさを重視

導入の背景

1. 自動巡回のカバー率が高く、主要な脆弱性を確実に検出できる
2. グループ会社のプロダクトも診断できるライセンス体系
3. API診断が可能

外国籍エンジニアも多く在籍するため、英語にも対応していること、Slackをはじめとする外部サービスとの連携性も要件だった。複数のツールの比較検討を進め、いくつかのプロダクトを対象に検証を実施した上で選定。

効果

約60プロダクトに診断を実施できた
今後、最低年1回の診断を計画

具体的な効果

1. 画面遷移図により、CISO室がプロダクトの画面を把握できるように
2. 開発者のセキュリティ意識が高まった
3. グループ統一のセキュリティスタンダード適用にも活用予定

ほぼすべてのサービスを内製で開発する中、「セキュリティスペシャリストの活動をAeyeScanがサポートしてくれている」とCISOも評価。セキュリティエンジニア以外に、QAチームでも使用を開始している。

AeyeScanひとつで、デジタル領域のセキュリティをトータルサポート

Webサイト全体の把握 → **脆弱性診断によるリスク評価**

AeyeScan

- Web-ASM
- 自動巡回
- 脆弱性診断

まとめ

DXとセキュリティは両輪で進められる

AIに任せられる業務は任せて
人は人にしかできないことに注力しよう！

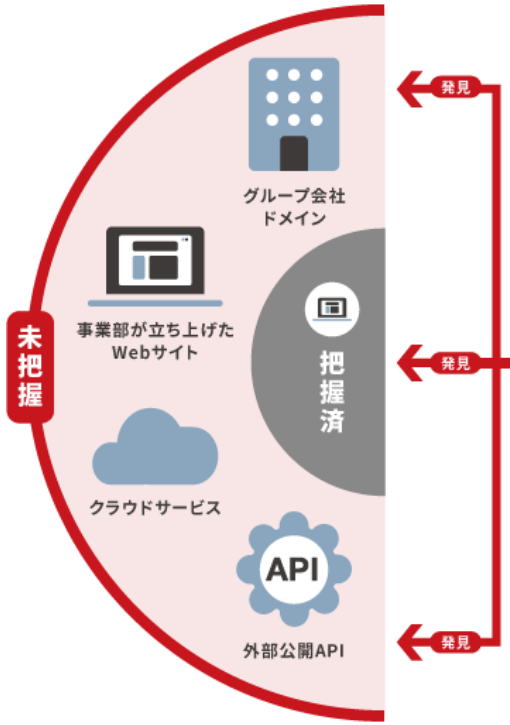
AeyeSecurityLab

生成AI活用で、工数をかけずにWeb-ASMを実現

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



特許取得実績のある
生成AI活用の技術により、
効率的・網羅的に攻撃面を発見。

生成AI

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！

AeyeSecurityLab

期間限定

Web-ASM機能オプション 利用料金50%OFFキャンペーン

内容	Web-ASM機能オプション利用料金を初回契約分50%OFFでご提供いたします。
適用対象	○ 2025年3月31日(月)までに株式会社エーアイセキュリティラボにご発注いただいたものが対象です。 ○ AeyeScan Businessライセンスをご契約中または2025年3月31日（月）までに新規で利用開始いただいていることが前提となります。
申込方法	「Web-ASM機能」お問い合わせフォームまたは弊社担当までご相談ください。

▶ お問い合わせフォームはこちら　https://www.aeyescan.jp/form/web-asm/

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

セキュリティに、確かな答えを。