AI活用で成果を最大化する
“戦略的”セキュリティ対策の思考法

AeyeSecurityLab

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。

AeyeSecurityLab

AeyeSecurityLab

誰でも簡単に

プロさながらの高度な

脆弱性診断を

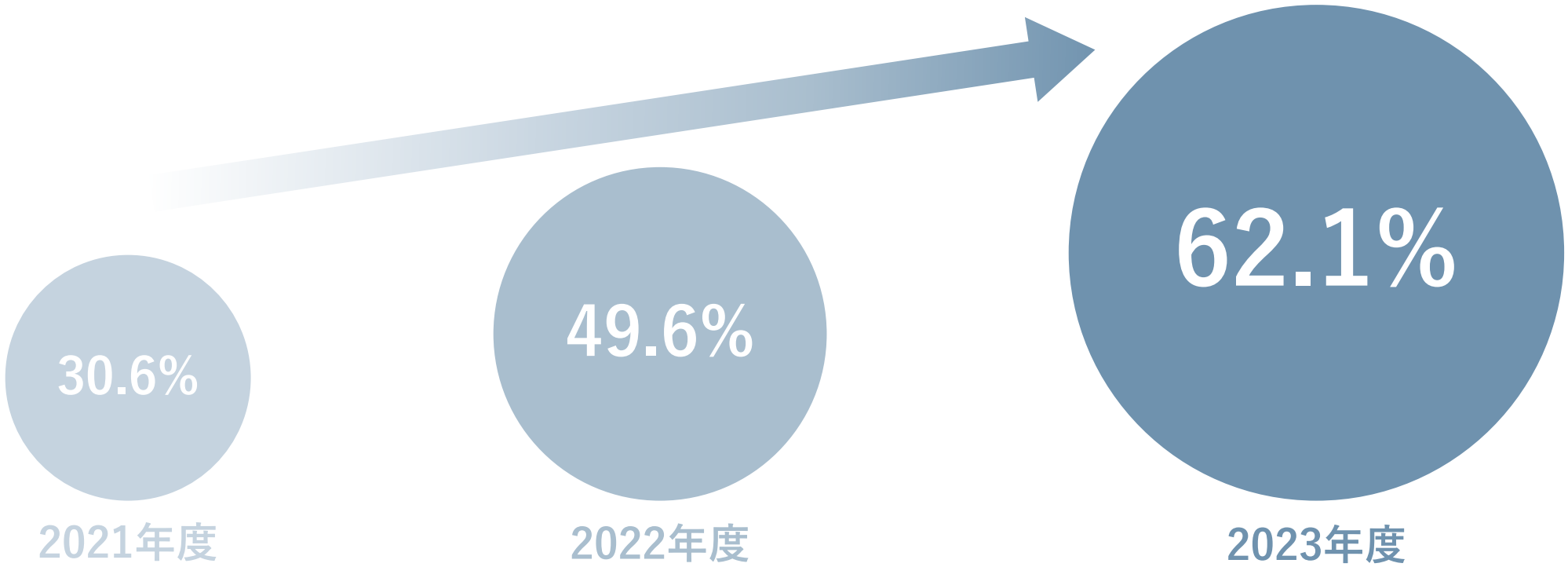
AeyeScan

AI活用で成果を最大化する
“戦略的”セキュリティ対策の思考法

DXは進んでいる…？

やらないと死ぬDX、年々高まる人材需要

DXを推進する人材が「大幅に不足している」



出展：DX 動向 2024 - 深刻化する DX を推進する人材不足と課題　https://www.ipa.go.jp/digital/chousa/discussion-paper/f55m8k00000039kf-att/dx-talent-shortage.pdf

DX に取り組まない/取り組めない理由の約7割が人材不足

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%

出展：DX 動向 2024 - 深刻化する DX を推進する人材不足と課題　https://www.ipa.go.jp/digital/chousa/discussion-paper/f55m8k00000039kf-att/dx-talent-shortage.pdf

至上命題となった「DX」を支える「セキュリティ」

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
増

×

急速な技術の進化

＝

必要なセキュリティ対策の
対応範囲も広く…
難易度も高く…

今後、より重視される「デジタルサービス」のセキュリティ対策

業務のデジタル化

社内IT資産 増

今まで情シスが管理していたので

攻撃面を把握しやすい

DX

デジタルサービスの増加

Web接点 増

事業部が独自に構築・運用するので

攻撃面を把握しにくい

直近の事例

某大手ハウスメーカー（A社）さまの事例

概要

過去、3年間に渡って使用していた、**現在は運用していないページ**でセキュリティ設定に不備があったことがわかった。

そのページが**データベースを操作するための言語を用いたサイバー攻撃**を受けたことにより、当該サイトのデータベースから情報が漏えいしたことが判明した。

（漏洩した情報）

- お客様のメールアドレス・ログイン ID・パスワード
- A社グループ従業員等のメールアドレス
- A社システムへのログイン時に使用するパスワード

現在は運用していないページ

このページにアクセス可能であることは認識されていた？

データベースを操作するための言語を用いたサイバー攻撃

一般的な脆弱性診断を実施すれば検知できていた可能性が高い

「うちのセキュリティ大丈夫？」

A社がサイバー攻撃されたけど、当社のWebサイトは問題ないよね？

今年度の脆弱性対策は、ばっちりなんだよね？

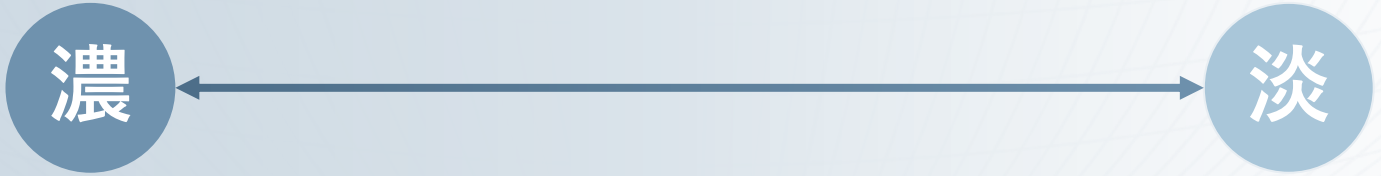
どのような戦略でセキュリティ対策を行うのか？

「戦略的な」セキュリティ対策とは何か・・・？

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



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
対応しなければいけない範囲が広い

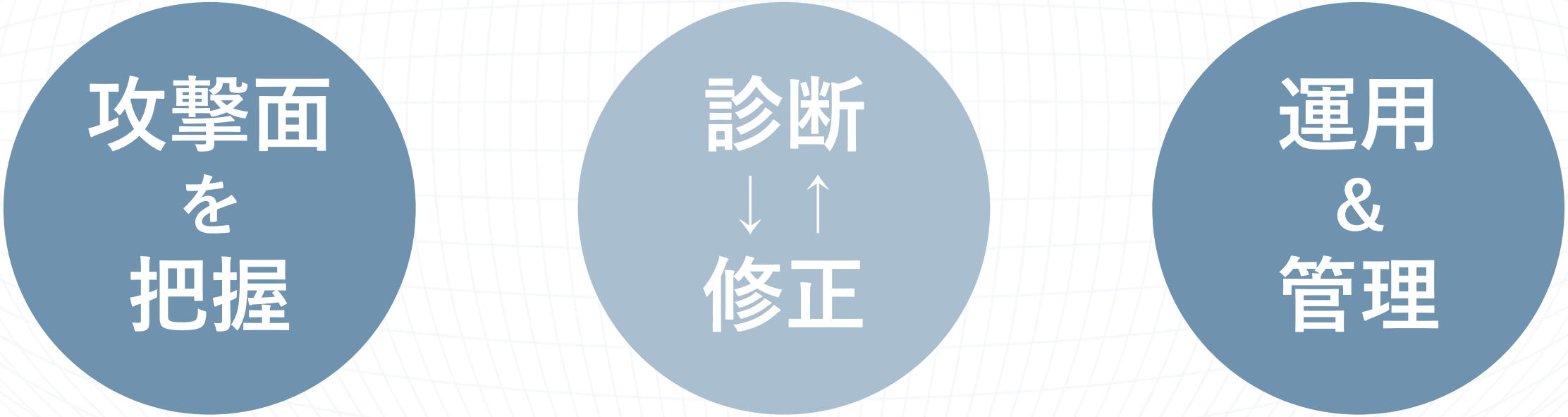
課題②

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

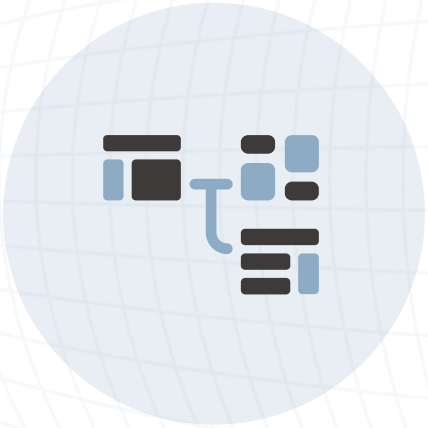
AIを活用した「自動化・内製化」で解決できないか？

戦略的セキュリティ対策には何が必要か

戦略的セキュリティ対策に必要な３要素

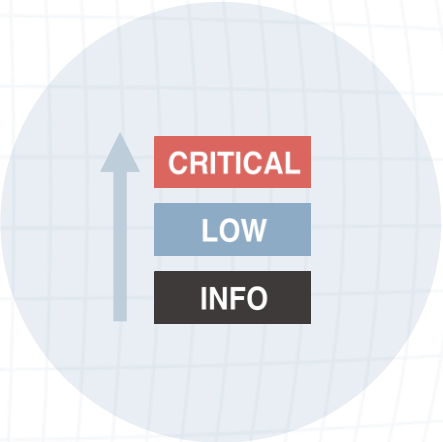


脆弱性診断と言われて思い浮かぶのは…？

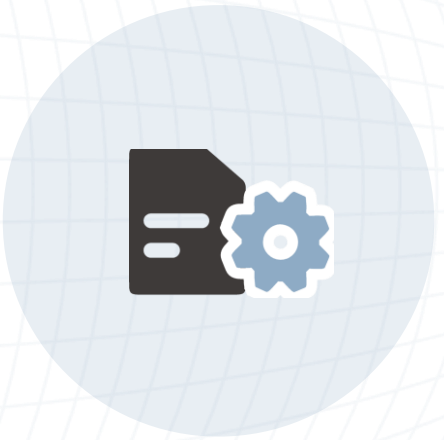


脆弱性情報の収集

脆弱性の評価



優先度付け



脆弱性の修正

戦略的セキュリティ対策に必要な３要素

攻撃面
を
把握

診断
↓ ↑
修正

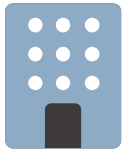
運用
&
管理

「攻撃面」を網羅的に把握できているか？

ECサイト

コーポレートサイト

会員向けサイト



企業向けサイト

キャンペーンサイト

社内Webシステム

- どんな会社でも、様々なIT資産やWebサイトを保有・運営している
- 一方、Webサイトについては、そのすべてを把握できているケースは少ない

ASM(Attack Surface Management)とは？

外部からアクセス可能な IT 資産を発見し、 それらに存在する脆弱性などのリスクを継続的に検出・評価する一連のプロセスのこと

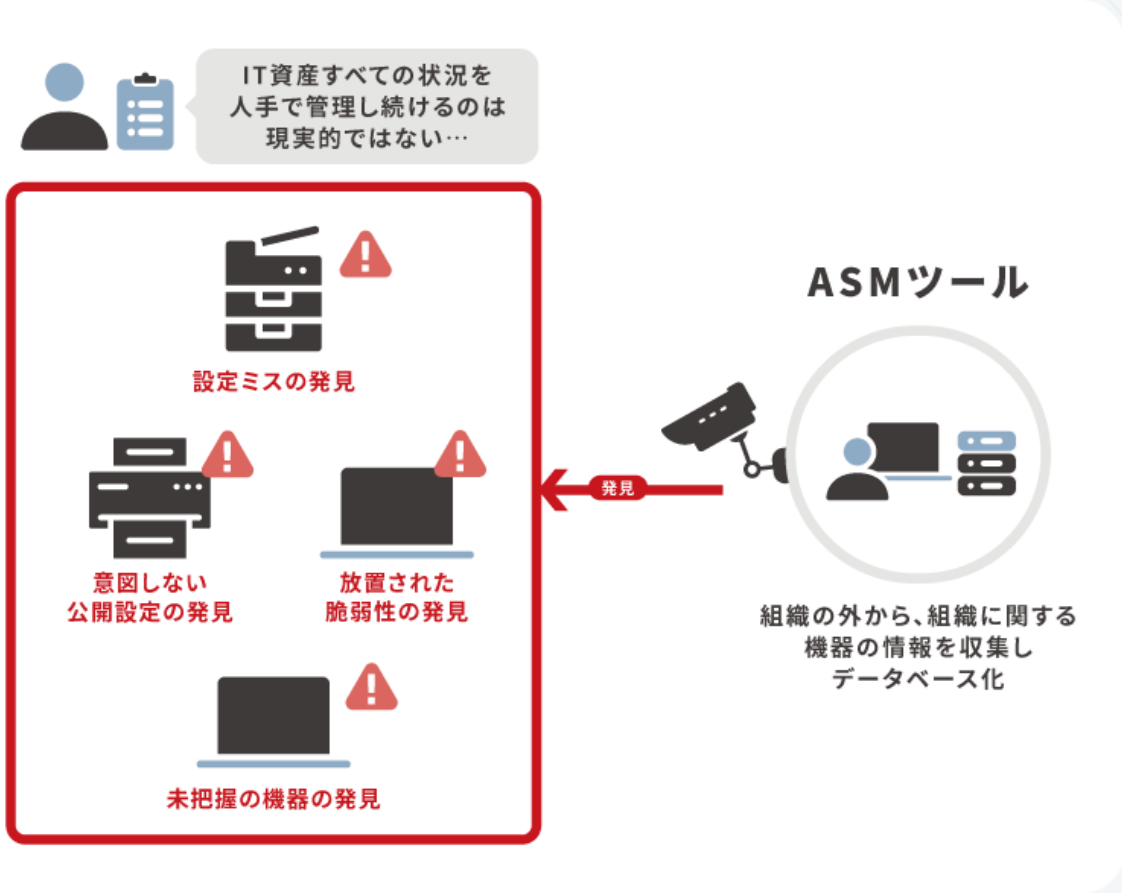
攻撃面の発見

↓

攻撃面の情報収集

↓

攻撃面のリスク評価



参考：経済産業省　「ASM（Attack Surface Management） 導入ガイダンス」https://www.meti.go.jp/press/2023/05/20230529001/20230529001-a.pdf

これまでのASMによくある課題

❶ 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…

❷ 本当に自社の資産なのか？

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…

生成AIの活用で、簡単に・網羅的に・効率的に攻撃面を発見できる！

生成AIをWeb-ASMと組み合わせて…

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

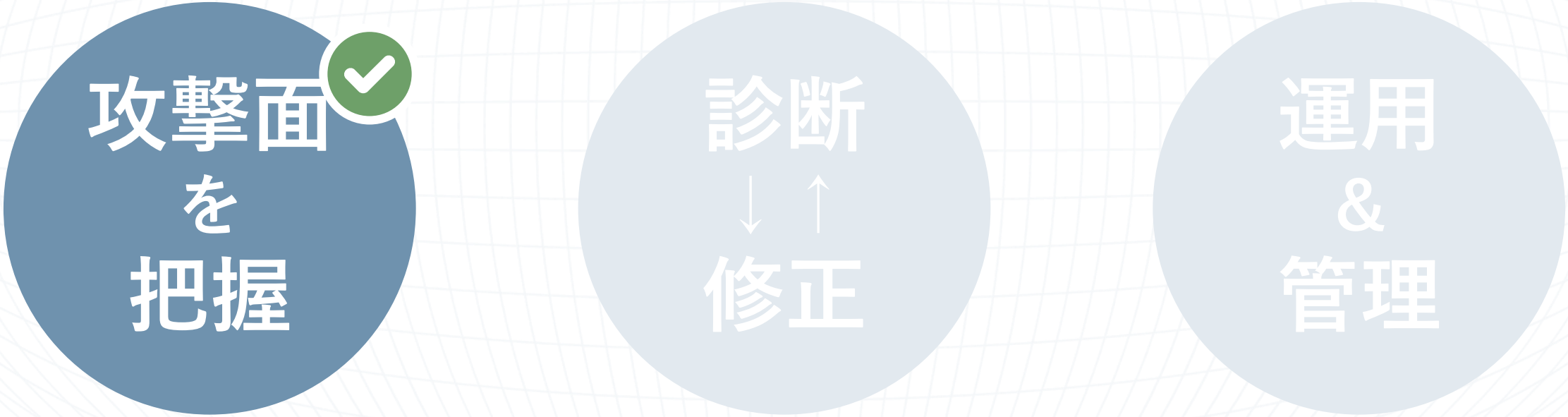
膨大な情報源
から総合的に判定

- SSL証明書の情報
- IR情報(Web公開済み)　など

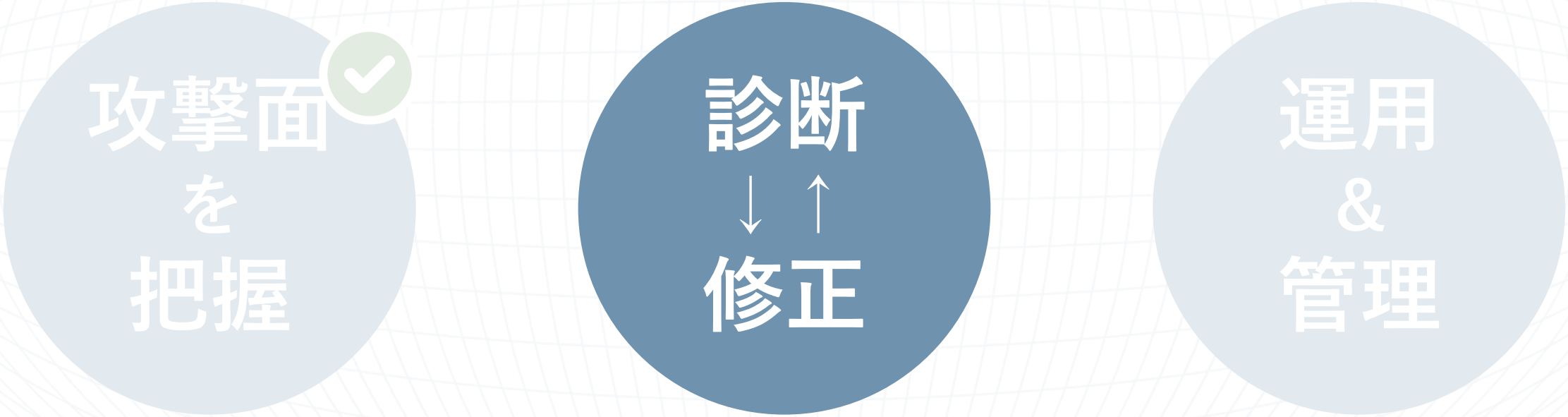
発見経路/理由
が分かる

生成AIが攻撃面を見つけるまでに
辿ったルートを説明

戦略的セキュリティ対策に必要な３要素



戦略的セキュリティ対策に必要な３要素



特に、対応が後回しになりがちな「手薄な」領域で工夫が必要

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
対応しなければいけない範囲が広い

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

➡「自動化・内製化」で解決できるかも！

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？

？

診断員を**育成・確保**できるだろうか？

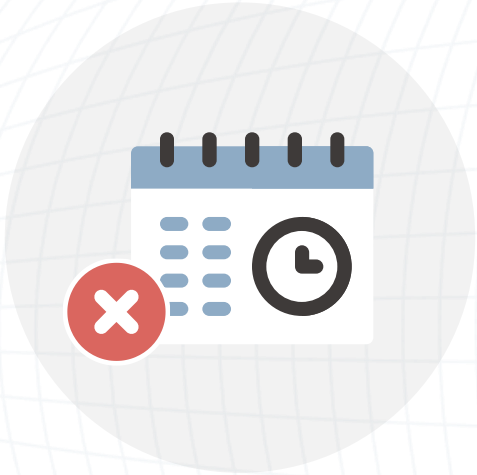
？

コスト（費用・時間）を削減できるか？

＋

事業部門・開発部門に内製化の協力を得られるか？

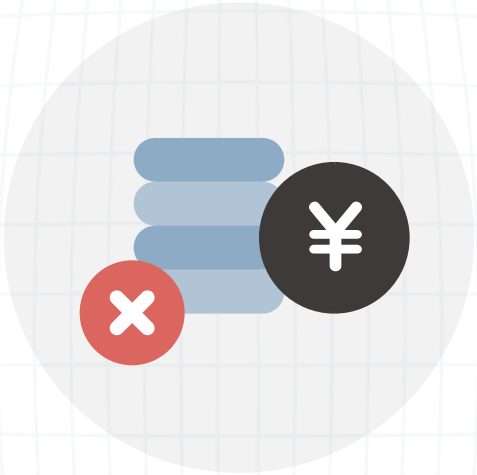
実際に事業部門と向き合う中で直面する「壁」



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

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

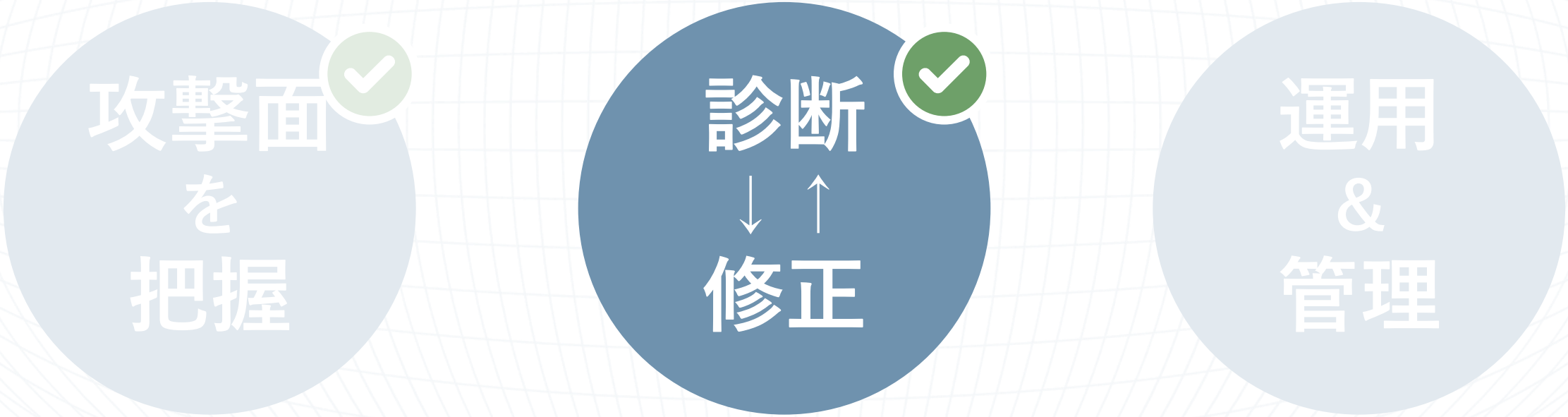
2 利用範囲に制限がない

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

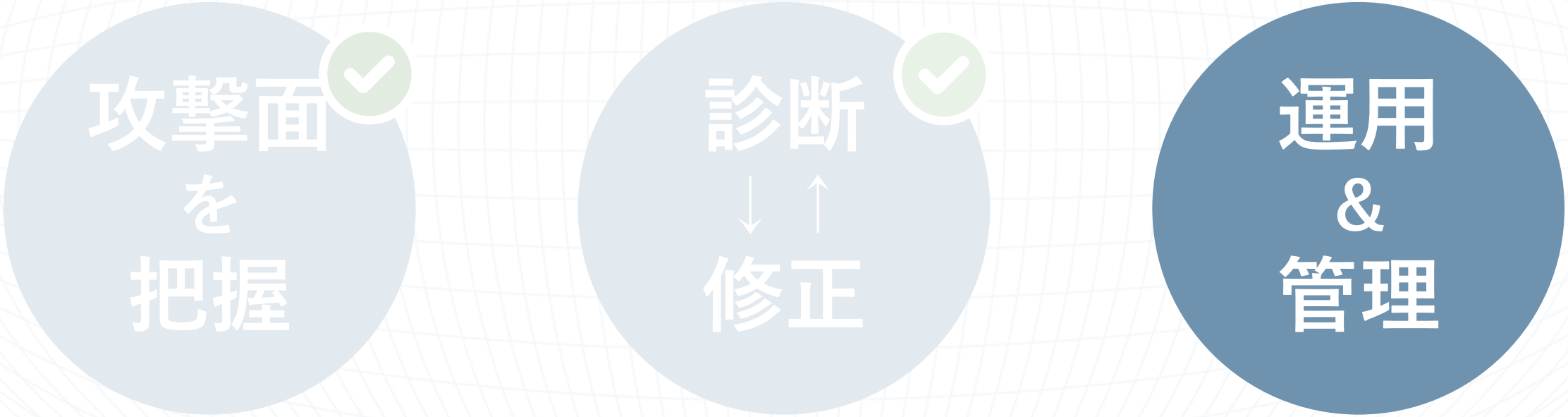
エンジニアでも、問題箇所や
リスク、修正方法がわかる

戦略的セキュリティ対策に必要な３要素

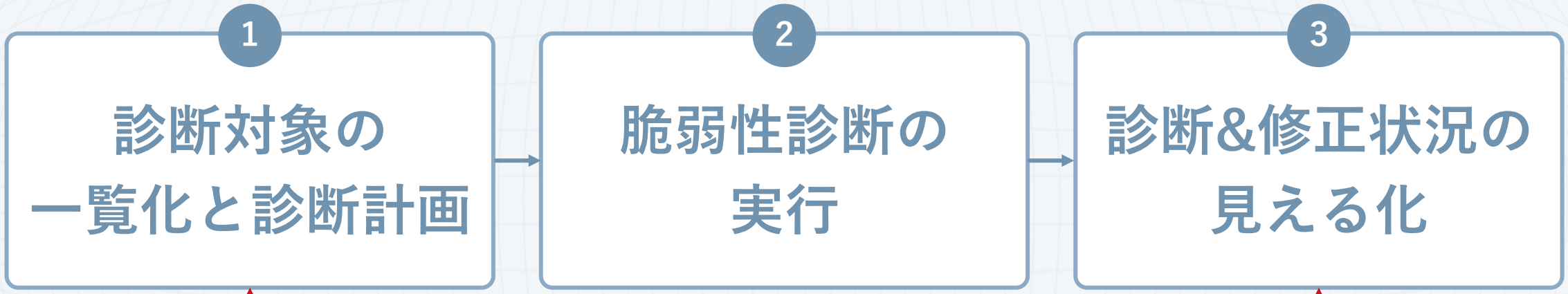


AeyeSecurityLab

戦略的セキュリティ対策に必要な３要素



脆弱性対策における運用＆管理の全体像



人がアナログに頑張るのは
結構しんどい・・・

診断対象の一覧化と診断計画（例）

診断計画

保存　削除　開始

名前　2024年度上半期

期間　2024/04/01 ～ 2024/10/30

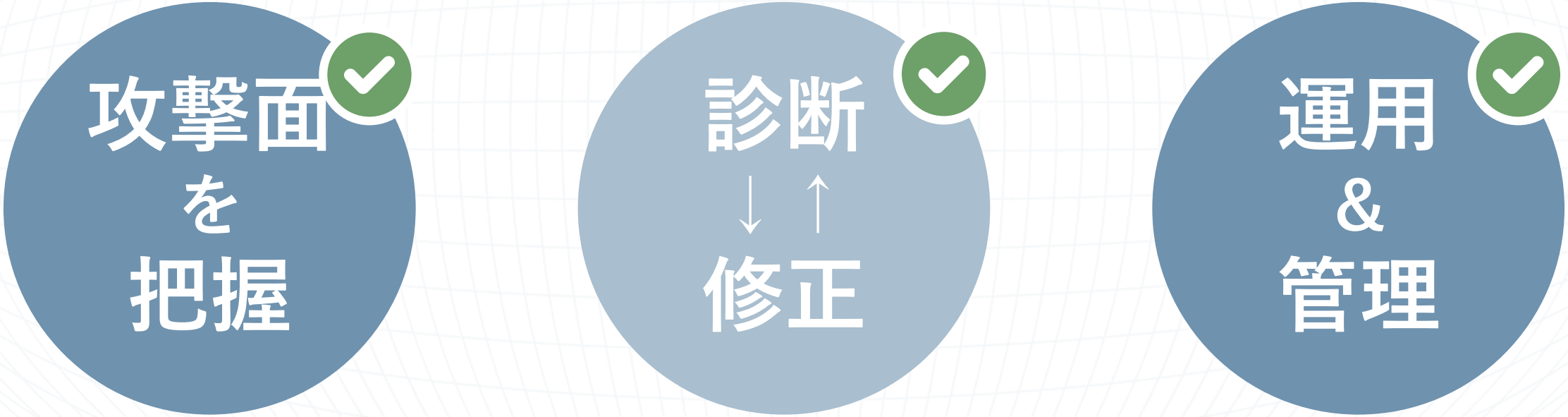
対象サイトの選択（10 / 30）

対象	ID	サイト名	トップURL	重要度	所属グループ	最後の診断期間
☐	1	公式HP	https://www.aeyesecu...	低	広報部	2024/3/10
☑	2	採用サイト	https://www.recruit.ae...	中	人事部	2024/3/21
☐	3	サービスサイト	https://www.aeyescan...	低	マーケティング部	2023/10/5
☑	4	取引先ポータル	https://www.customer...	高	営業部	2024/9/19
☑	5	ECサイト	https://www.aeye-sho...	高	マーケティング部	2024/10/8

診断＆修正状況の見える化（例）

AeyeSecurityLab

戦略的セキュリティ対策に必要な３要素



本日のまとめ

スケーラブルなセキュリティ対策 ＝ 濃淡をつける

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

人材不足の状況でも
AIを活用して実現！

- 攻撃面を把握
- 診断 ↓↑ 修正
- 運用 & 管理

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)

有償契約
100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

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

AeyeScanが選ばれている理由

プロが認める機能・性能 × 誰でも使える操作性

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
Suzuyo
HITOWA GROUP
NTT東日本
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

イープラス
CAPCOM
とらラボ!

SaaS

estie
エムティーアイ
OZINTERNATIONAL
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 情報技術開発株式会社
Simplex Inc.
777WORKS
SOFT CREATE
SOLTEC
電通総研
TOPPAN
JOPS
NHC
Human Interactive Technology inc.
FUJISOFT
FUJITSU
MITSUBISHI ELECTRIC
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

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。

導入事例紹介

エイチ・アイ・エス 様

企業名　株式会社エイチ・アイ・エス

事業内容　総合旅行会社

従業員数　10,849人（2023年6月時点）

課題

セキュリティの内製化が困難。
診断の外注コストを削減したい

具体的な課題

1. 社内からの診断依頼が増え続けていた
2. 診断対象が多く外部委託せざるを得ない
3. 外注による診断コスト増

内製・外製含め100を超えるWebアプリケーションがあり、内部の体制だけではすべての診断実施に対応できず、一部を外部に委託。コスト削減と体制整備が課題だった。

導入

情報処理推進機構（IPA）の検証結果と
「7割以上自動化」という点が決め手

導入の背景

1. 手動の診断では対応が追い付かず自動化を検討していた
2. 自動化できても性能が落ちない製品を探していた

手動作業を伴う診断では対応が困難になり、診断の自動化を検討。AeyeScanは、IPAの検証結果が高評価だったことと、「7割以上の自動化が可能」という点が決め手で導入。

効果

診断・レポート作成工数を大幅に削減。
さらなる内製化比率の向上を目指す

具体的な効果

1. 診断の大部分を自動化し工数を削減
2. レポート機能により大幅に時間を短縮
3. リリース前に診断と脆弱性改修が完了

「脆弱性が発覚しても、リリースまでに修正が間に合わない」という悩みも解消され、脆弱性を潰してからアプリをリリースできるように。

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

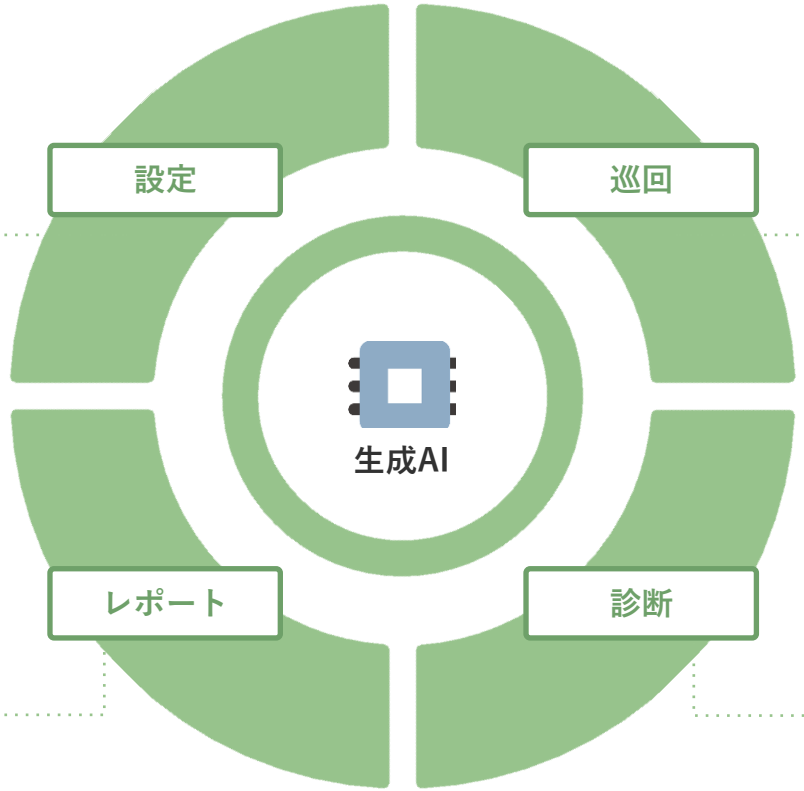
- フリーフォーマットでの指示

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



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

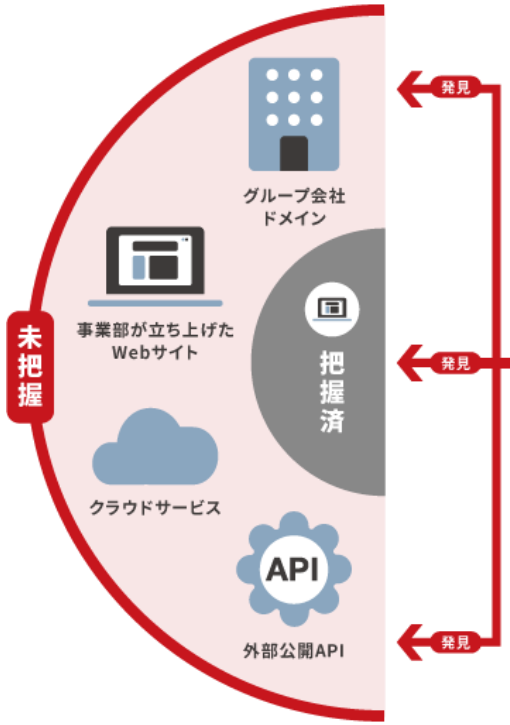
生成AI活用で、工数をかけずにWeb-ASMを実現

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。

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！

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。