DXの陰に潜む
見えないリスク への対処法

生成AIで実現する網羅的・継続的な脆弱性対策とは

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・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

DX推進により
「見えないリスク」が増加している

DXが進むにつれ、セキュリティリスクは変化・拡大している

Phase 1

情報のデジタル化

＜主なリスク＞

- 人的リスク(漏洩・持出)
- ストレージの安全性
- 不適切な認証・権限設定

データそのもののセキュリティリスクが中心

Phase 2

業務のデジタル化

＜主なリスク＞

- クラウド環境の設定不備
- ネットワークへの攻撃
- 不完全なエンドポイント管理

業務プロセス自体がデジタル化し
インフラ周りのセキュリティが重要に

Phase 3

事業のデジタル化

＜主なリスク＞

- 頻繁なサービスアップデート
- 潜在的なデジタル領域の攻撃面
- サプライチェーンの拡大

サービスそのものがデジタルで
完結するようになると、
リスクはさらに多層化・継続化

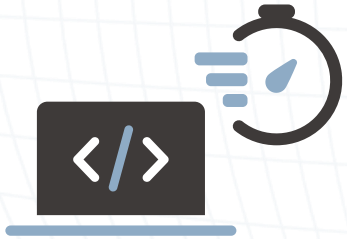
事業のデジタル化（Phase3）は進んでも、セキュリティ対策が追いついていない

セキュリティリスクが拡大する原因

事業のデジタル化を主導しているのは事業部門であり、セキュリティ部門が把握しきれていない。

デジタルサービスは誰でも作れる時代
したがって機動力が求められる。

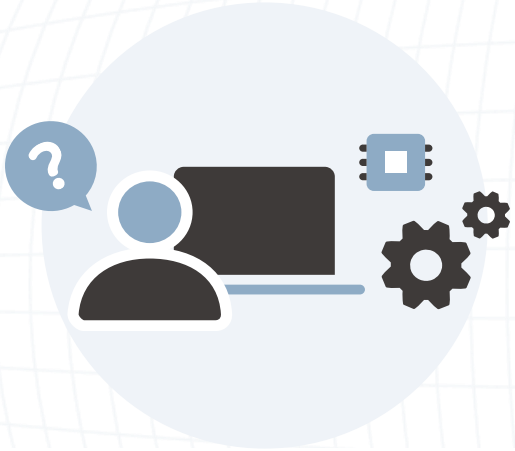
これまでは「ベンダーに丸投げ」だったが、
今後は自社にセキュリティの責任が発生。



そんなことを知らない事業部門は、セキュリティ部門の判断を仰ぐ暇もなく…

「見えないリスク」が増加！

見えないリスクとは？



自社グループが管理すべきデジタルサービスを

「認識できていない」リスク

デジタルサービスのセキュリティ対策状況を

「把握できていない」リスク

自社グループが管理すべきデジタルサービスを「認識できていない」リスクの対処法

「認識できていないリスク」はどこにある？

Phase 1

情報のデジタル化

＜主なリスク＞

- 人的リスク(漏洩・持出)
- ストレージの安全性
- 不適切な認証・権限設定

Phase 2

業務のデジタル化

＜主なリスク＞

- クラウド環境の設定不備
- ネットワークへの攻撃
- 不完全なエンドポイント管理

Phase 3

事業のデジタル化

＜主なリスク＞

- 頻繁なサービスアップデート
- 潜在的なデジタル領域の攻撃面
- サプライチェーンの拡大

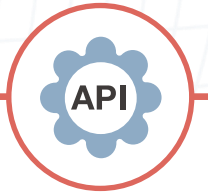
情シス・セキュリティ部門が認識しやすい
社内ITを中心とした「静的」IT資産がほとんど

どこで何やってるか
分からない…！

事業のデジタル化によって増える「認識できていないリスク」

PoCで作ってみた
SaaS/IaaS/PaaS上のアプリ

事業部門がアジャイル開発で
構築・運用するWebサイト



スクラップ＆ビルドの連続で
誰も管理できていないAPI

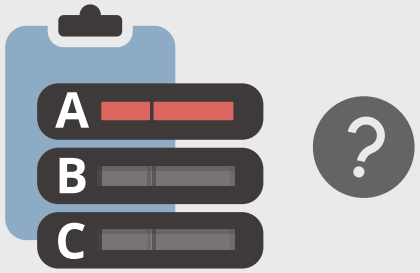
「認識できていないリスク」を認識する難しさ

人力で探索・精査が必要

広範囲から検出することはできるが、
不要なものも多く紛れ込んでおり、
人手による精査が必要。

優先順位付けが困難

対応優先度を決めるのが難しい。
システム観点からだけでなく、
事業観点での優先順位付けが必要。



お客様から伺う「ASMツール」活用のお悩み

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。

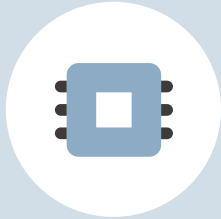
精度がすごい

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。

高度な生成AI活用活用により、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
辿ったルートを説明

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

Medium

- ECサイト
- VPN管理サイト

Low

- 外部SaaSサイト
- テストサイト

保持データ

High

- 個人情報
- クレジットカード情報

利用技術

Low

- WordPress
- EC-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

デジタルサービスのセキュリティ対策状況を

「把握できていない」リスクの対処法

IT資産を認識できても、対策状況を「把握できないリスク」が…

情報連携の困難さにより、セキュリティ部門で進捗や対応状況が管理しきれなくなっている

定められたルール通りに診断できてる？

スコープ漏れなく診断できてる？

スケジュール通りに実行できてる？

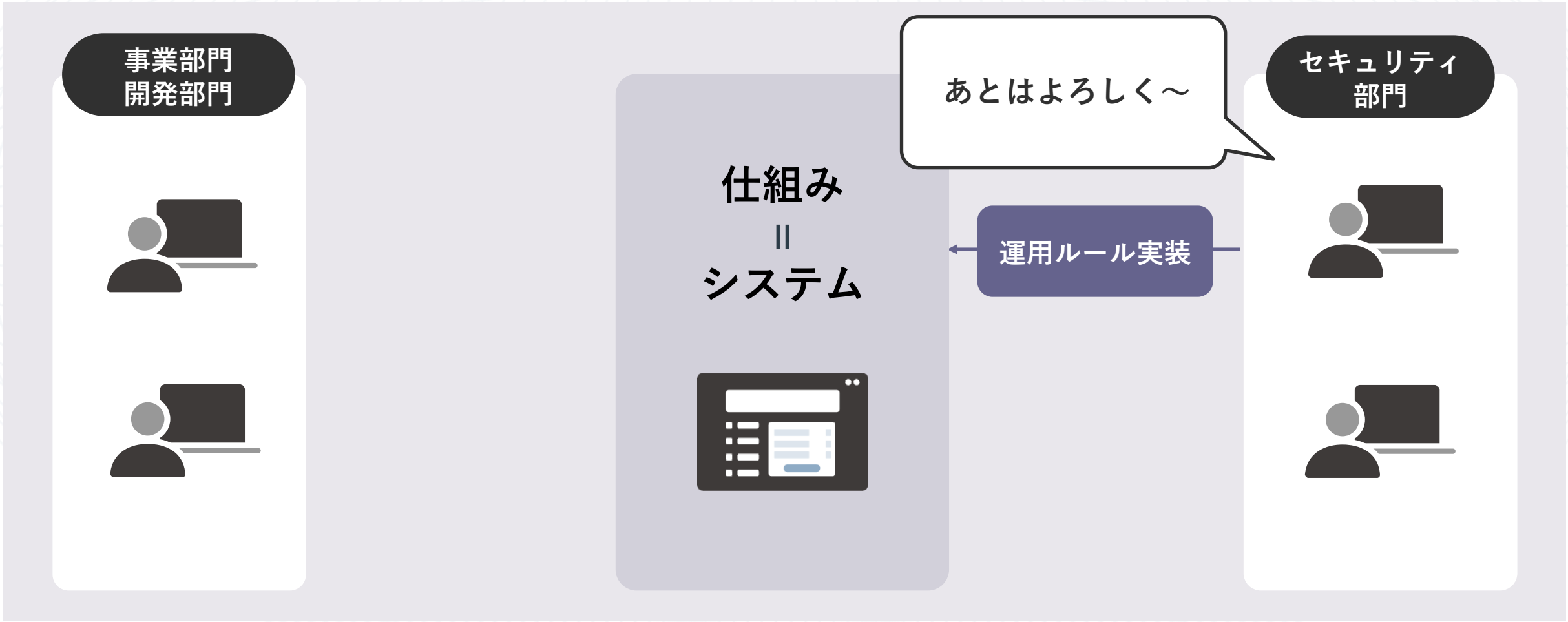
見つかった脆弱性はきちんと修正できてる？

遅延や抜け漏れが生じ、十分に対応できない可能性も！

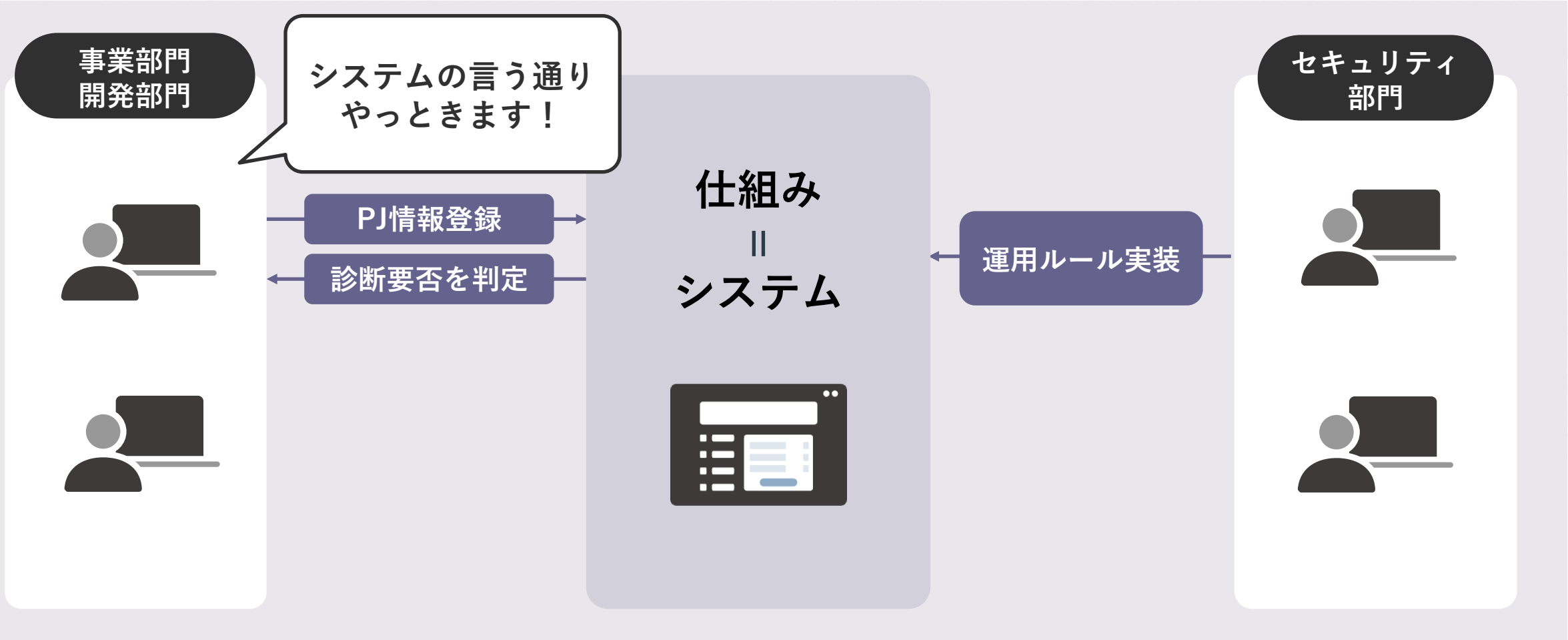
人が頑張る／人に任せるのは限界があるな…

それなら、システムに任せてしまおう！

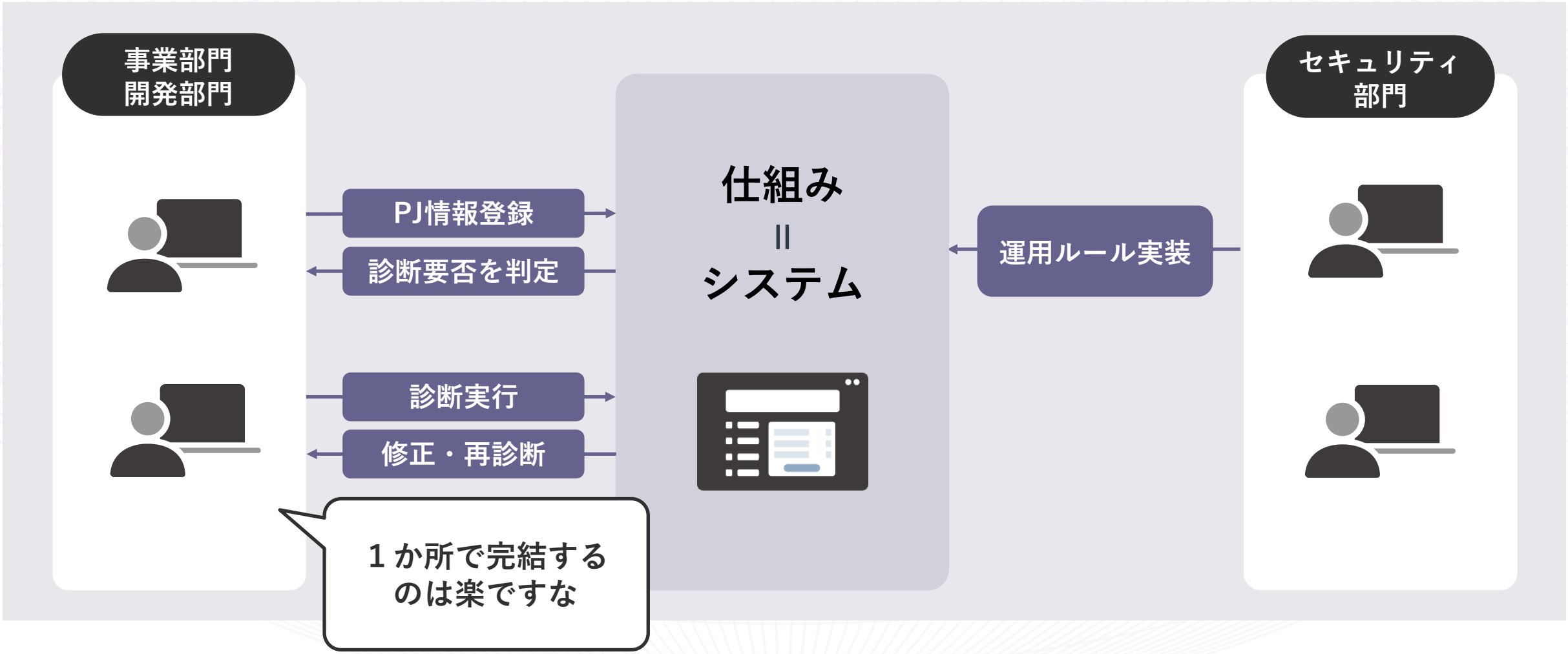
セキュリティ対策の状況を把握し、運用するための「仕組み」づくり



セキュリティ対策の状況を把握し、運用するための「仕組み」づくり

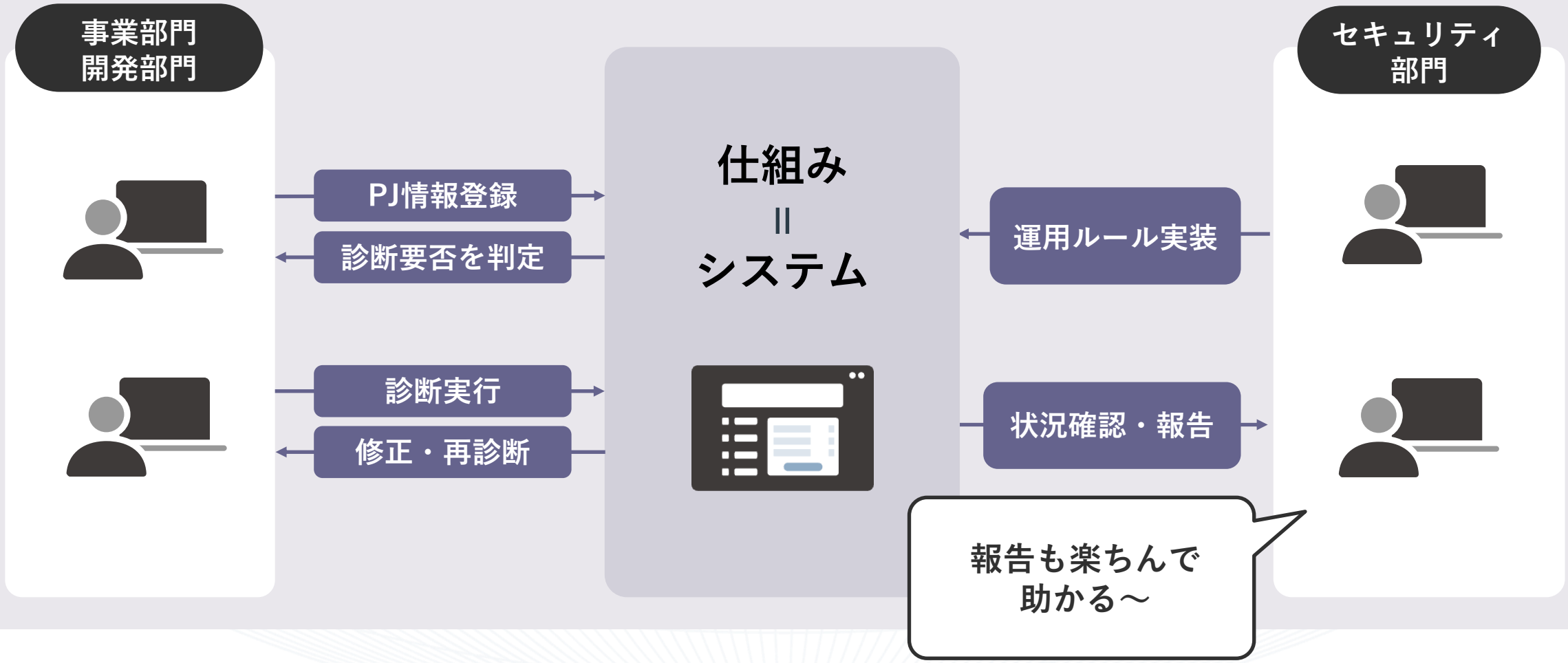


セキュリティ対策の状況を把握し、運用するための「仕組み」づくり

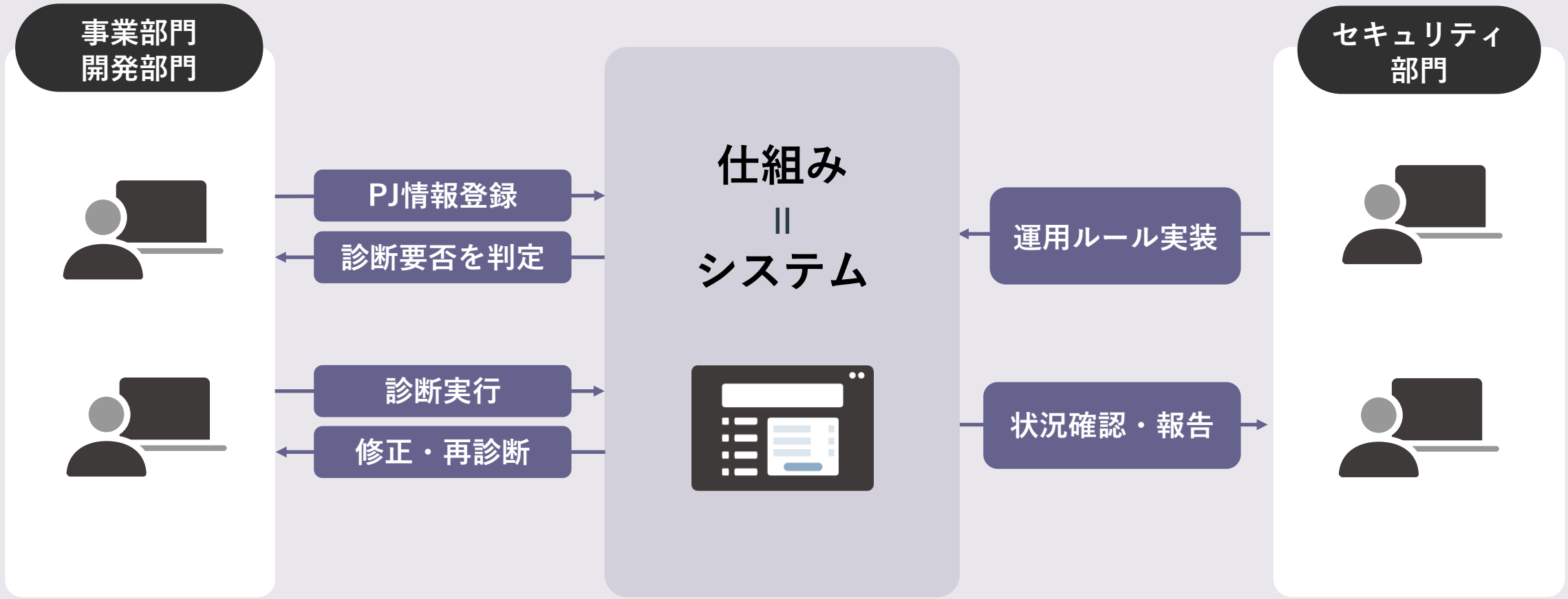


AeyeSecurityLab

セキュリティ対策の状況を把握し、運用するための「仕組み」づくり



セキュリティ対策の状況を把握し、運用するための「仕組み」づくり



セキュリティマネジメント：目指す姿（チラ見せ）

経営層

セキュリティ関連施策の
投資判断

全社情報セキュリティの
リスクマネジメント

戦略目標の定義
リソース配分

定期報告
施策検討・上申

セキュリティ部門
情報システム部門

具体的な施策の決定
ルール策定・運用設計

セキュリティ対策関連の
情報集約・対応検討

ルール周知
技術サポート
実行管理

プロジェクトや
対策状況の共有

事業部門・開発部門
グループ会会社

全社ポリシーに則った
セキュリティ対策

セキュアな開発
セキュアなサービス提供

AeyeSecurityLab

デジタル領域の見えないリスクには・・・

1. 生成AIで効率的に
   未把握のWebサイトを把握

Web-ASMの実施

2. 情報が自ずと集約される
   仕組みをつくる

**マネジメント
プラットフォームの活用**

我々と一緒に解決しましょう！

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）

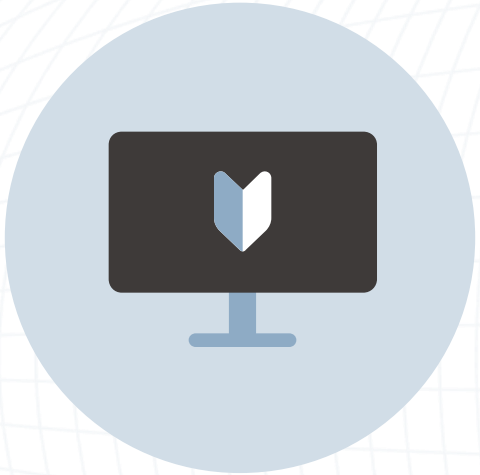
有償契約
300社以上

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

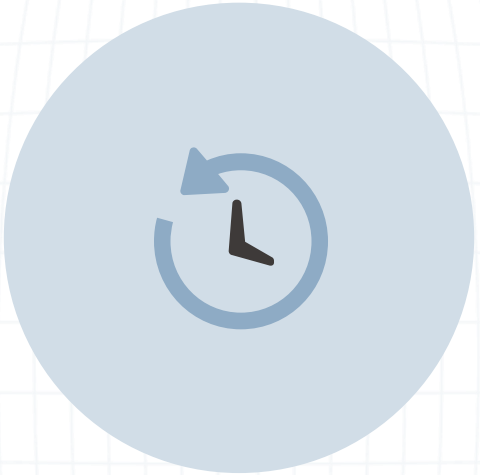
03
業界標準対応
外部委託と遜色なく
内製化が可能

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。



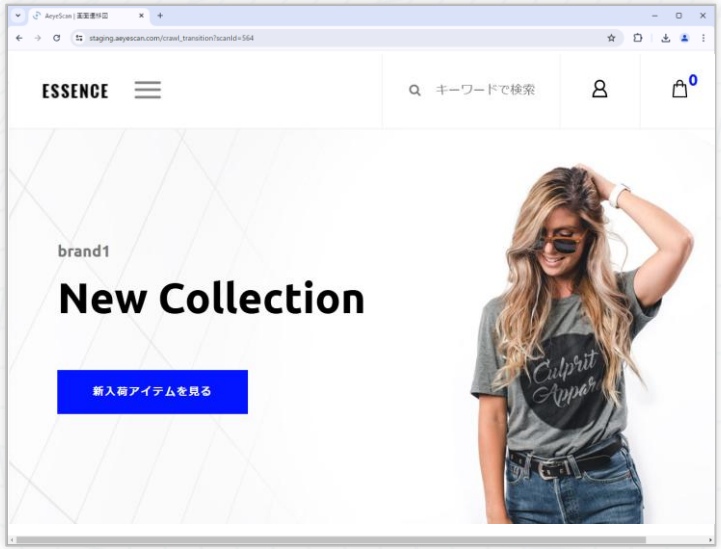
AIによる自動診断

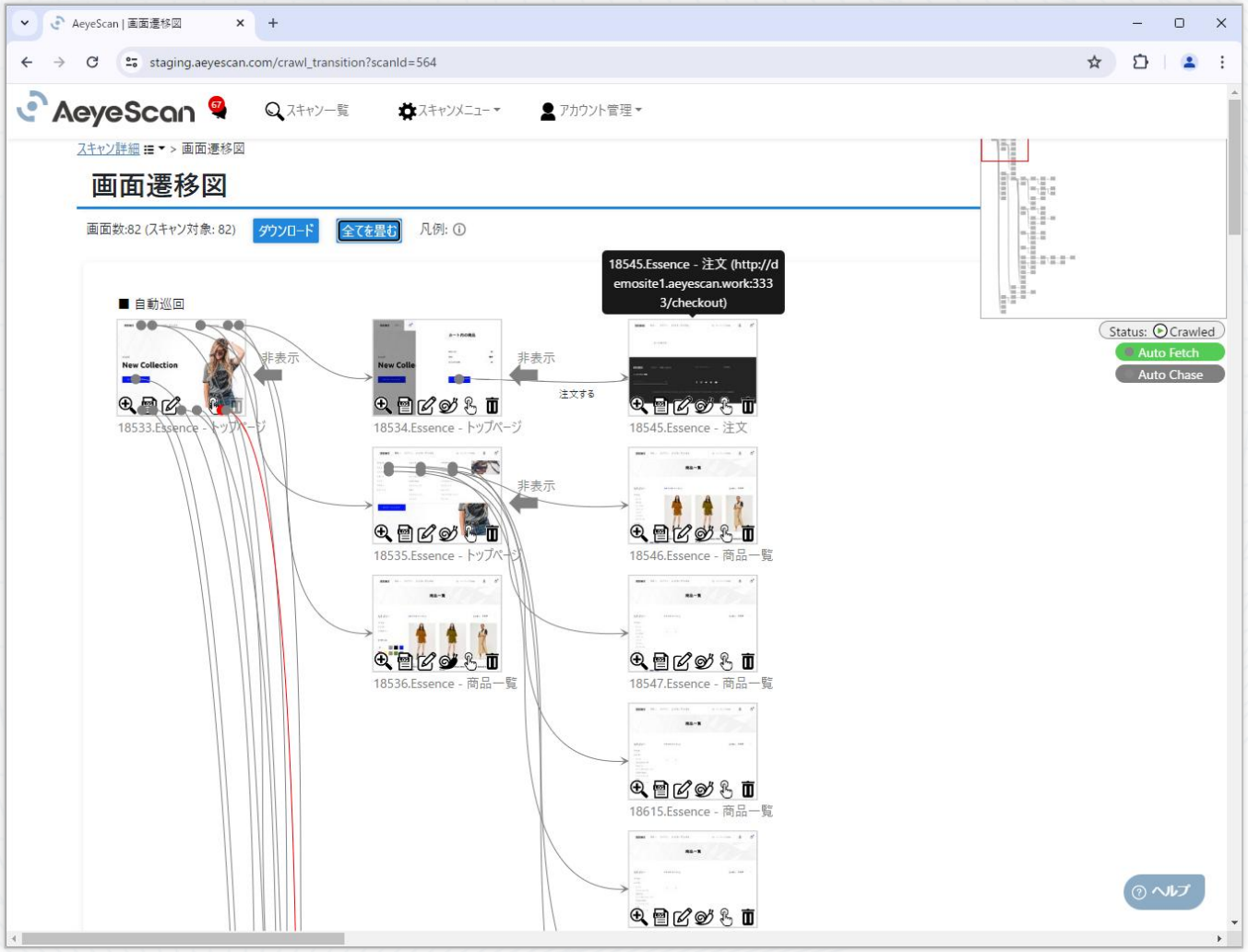
圧倒的な巡回精度で
24時間自動で診断。
画面遷移図で状況を可視化。

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

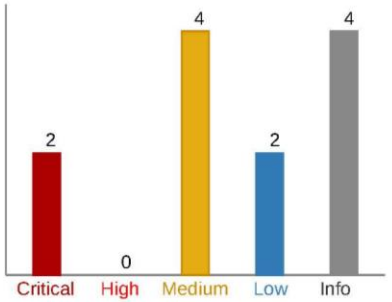




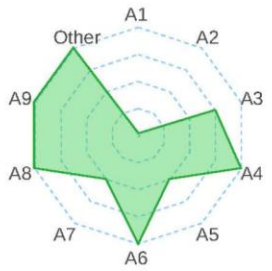
結果がわかりやすく、すぐさま修正作業に取り組めるレポート

スキャンサマリー

全体評価　Critical



深刻度ごとのサマリー



OWASP TOP 10 カテゴリー

脆弱性の深刻度は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。

深刻度	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	

スキャン結果詳細

Critical

SQLインジェクション

深刻度

Critical

CVSS Score: 9.8
CVSS Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

概要

危険な文字列をSQL文に挿入できます。そのため、攻撃者が任意のSQL文を実行できる危険性があります。

OWASP TOP 10 カテゴリー

A1:2017-インジェクション

ASVS4.0 カテゴリー

5.1.2,5.1.3,5.1.4,5.3.1,5.3.4,5.3.5,13.2.2,13.3.1

解説・対策方法

SQLインジェクションとは、攻撃者が細工した入力値を送信することで、開発者の想定していないSQL文を実行できてしまう脆弱性です。この脆弱性は、利用者の送信した値が適切に前処理されずにSQL文の一部として利用されることが原因で発生します。

この脆弱性を悪用することで、データベースの情報漏洩や情報改ざんなど、開発者の想定していない処理を実行されてしまう危険性があります。

対策方法としては、想定していない値が入力された場合に処理を中断することや、SQL文で特殊な意味を持つ文字を無害化することが挙げられます。後者を実現する一般的な方法としては、パラメータ化クエリやプリペアードステートメントの利用が挙げられます。

参考情報

安全なウェブサイトの作り方 - 1.1 SQLインジェクション | 情報セキュリティ | IPA 独立行政法人 情報処理推進機構 (https://w

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

AISIN
KOSÉ
SAKI
TIGER
TEIJIN
Mizuno
ユーグレナ

インフラ

HIS
H2O RETAILING
odakyu
近鉄情報システム株式会社
水ing Swing Corporation
Suzuyo
NTT東日本
HITOWA GROUP
grow up together MEDIA
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

人材・教育

Junion
JINSOKEN
Schoo
ZENKIGEN
Direct Sourcing
PERSOL
Leverages

エンタメ

イープラス
CAPCOM
とらラボ!

SaaS

Advanced Media, Inc. 株式会社アドバンスト・メディア
estie
M-aid
エムティーアイ
OZ INTERNATIONAL
COACH A Co.,Ltd.
cybozu
Speee
SecureNavi
TAL
TEMONA
NAVITIME
KNOCK ON THE DOOR
BATONZ
VALUE HR
Finovo
freee
porters
hokan
Money Forward
RUN.EDGE
RVSTA 株式会社リバスタ
Rescuenow

SI・IT企業

Rworks
アクモス 株式会社
AVANT GROUP
Insight Edge
Infcurion
80&Co.
SB Technology
SBWorks
NTT AT
NTT DATA
NTTビジネスソリューションズ
OMRON
Globalway
circlace
さくら情報システム
CEC
GA TECHNOLOGIES
tdi 情報技術開発株式会社
Simplex Inc.
777WORKS
SOFT CREATE
SOLTEC
高千穂交易株式会社
電通総研
TOPPAN
JOPS
NHC
Human Interactive Technology inc.
FUJISOFT
FUJITSU
MACROMILL
MITSUBISHI ELECTRIC
YONA
リピスト

セキュリティ企業

NEC NECセキュリティ
NTT DATA NTTデータ先端技術株式会社
GSX
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

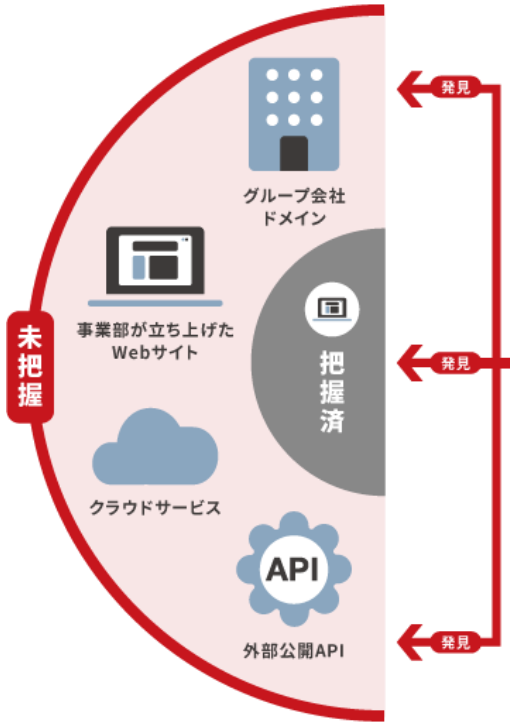
生成AIを活用し、常に自社Webサイト・ドメインを網羅的に把握

オプション機能

Web-ASMとは？

未把握の攻撃面を含めた、自社が管理すべきWebサイト（ドメイン）の継続的＆網羅的な発見・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！

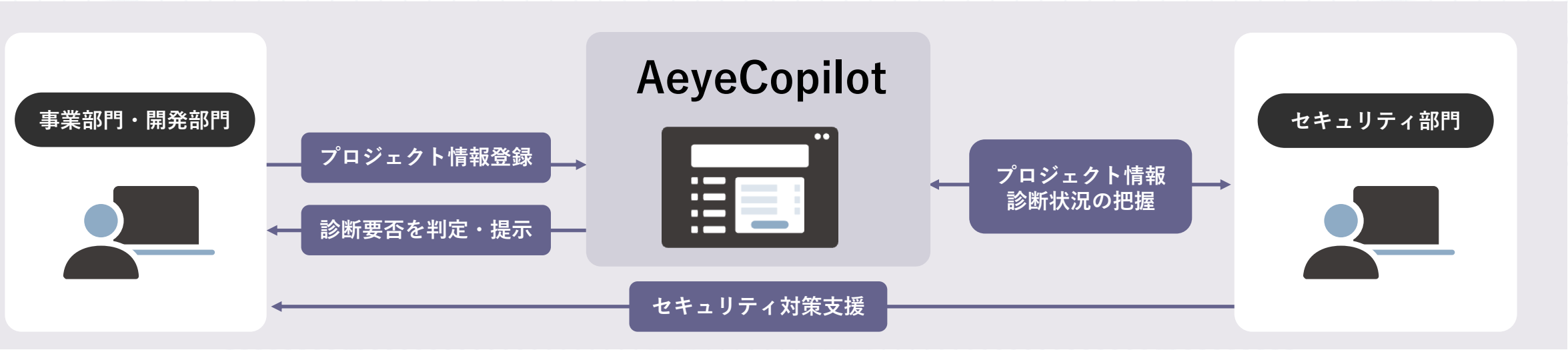
AeyeSecurityLab

全社セキュリティ対策全体を可視化し、運用ルールの徹底を支援

オプション機能

AeyeCopilotとは？

関連部門の「情報とコミュニケーション」が自ずと集約される仕組みで
診断・対策の全体管理や、セキュリティ対策に関する最適な意思決定を支援



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。