【情シス部門・開発責任者向け】

Webサイトの網羅的な脆弱性診断を実現するには？

ー「いつでも・だれでも」診断できる環境・体制づくりー

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、新規プロダクト企画にも携わる傍ら、各種セミナー・講演へ
の登壇などエバンジェリストとしても活動。

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）

フォローお願いします！

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

脆弱性診断を取り巻く現状（外部要因）

攻撃増加

診断義務化

委託費用高騰

限られた予算で、一部のサイト・アプリを外部診断するケースが多い

脆弱性診断を取り巻く現状（内部要因）

セキュリティ人材や予算の不足

採用・育成は難易度が上昇し
外注先でも同じくリソース不足で
診断できない／リリースできない

アジャイル開発（開発の高速化）

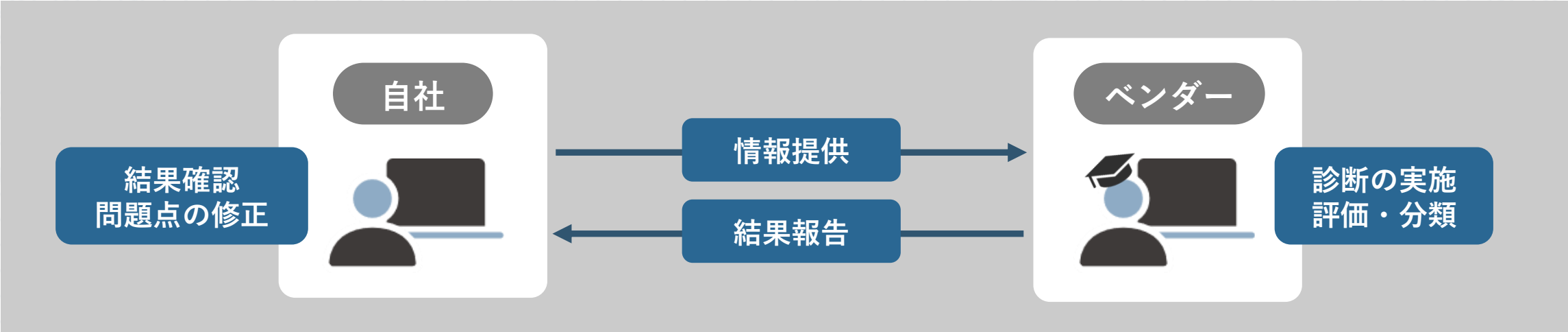
従来型の診断フロー・期間では
2～4週間のリリースサイクルに
柔軟に対応できない

ローコード開発（コモディティ化）

PaaS/IaaS/SaaSの普及により
開発のハードルが下がったことで
診断対象サイトが急増している

診断対象・診断回数が増え、外部診断だけでは到底カバーできない…

外部委託中心運用の限界



委託先との連携に

余計な工数がかかる

診断タイミングを

柔軟に調整できない

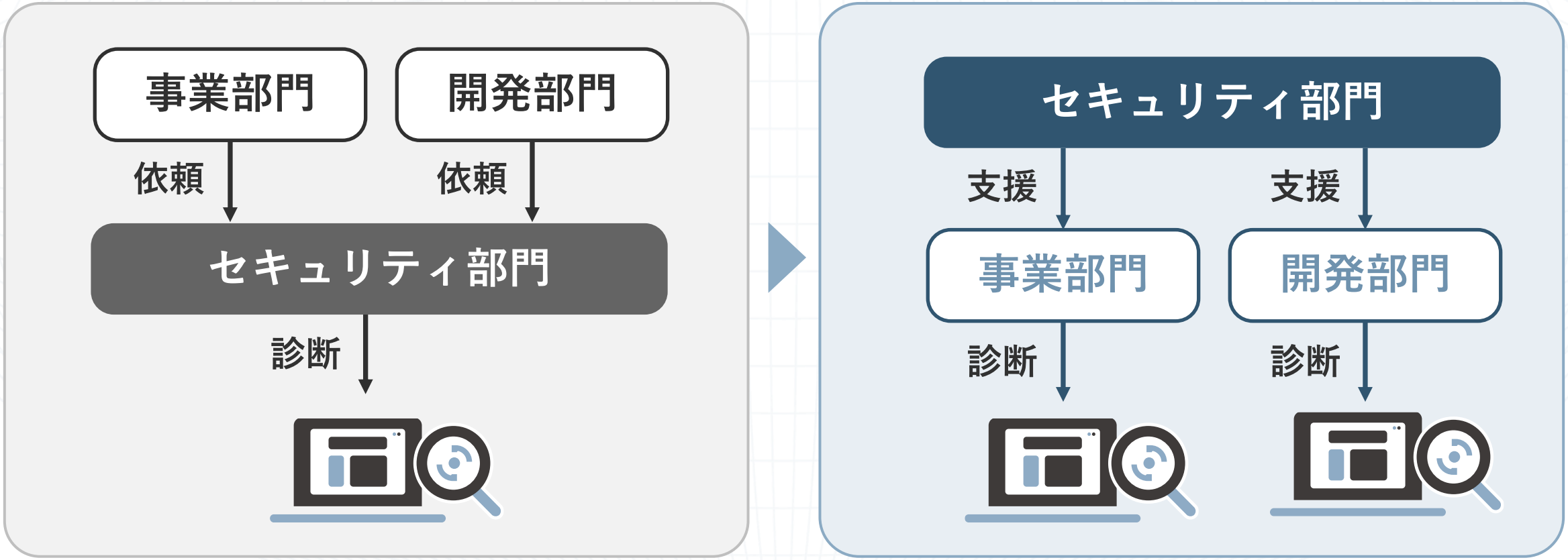
追加の依頼ができず

リスクを潰しきれない

脆弱性診断って社内でできるの？

診断内製化を進めるポイント

➡ セキュリティ部門が「支援・管理する」体制への移行◎



事業部門・開発部門が、自分たちで診断をするようになると…

業務・サービス・アプリに
詳しい担当者が「直接」
診断できれば…

セキュリティ部門だけでは
受けきれなかった診断も
各部門で診断できれば…

開発プロセスの中で
早め・小まめに診断して
手戻りを防げれば…

⌄⌄

精度が上がる

網羅性が上がる

納期に間に合う

セキュアなサービス開発・運用・提供

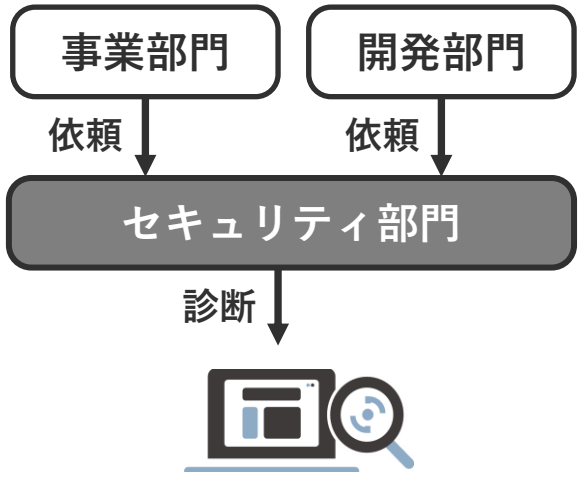
健全な開発体制・PJ

AeyeSecurityLab

「いつでも・だれでも・好きなだけ診断」大作戦！

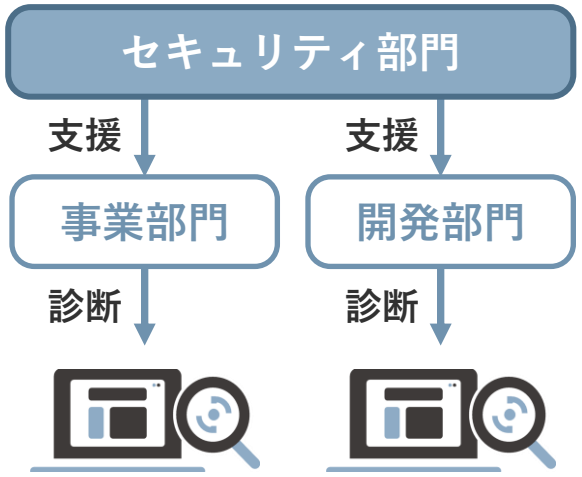
従来の運用体制

セキュリティ部門が
まとめて診断



これからの運用体制

事業部門・開発部門が脆弱性診断を
自ら実施できる体制を構築



- シフトレフトの実現
- 診断対象の的確な把握
- セキュリティ意識の醸成

脆弱性診断の「内製化」部分について考える

みんなを巻き込む前提で考えると、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

「いつでも・だれでも・好きなだけ診断」できる環境づくり

でも、実際には…難しいですよね？

課題 1

どう業務フローを組めばいい？

課題 2

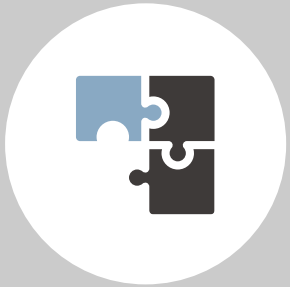
どうやって運用ルールを作る？

課題 3

どこから手を付ければいい？

AeyeScanなら、内製化をバッチリご支援します

脆弱性診断におけるよくある課題 #1



ツールを導入したけど

具体的にどう進めたら良い？

業務フローの整理や

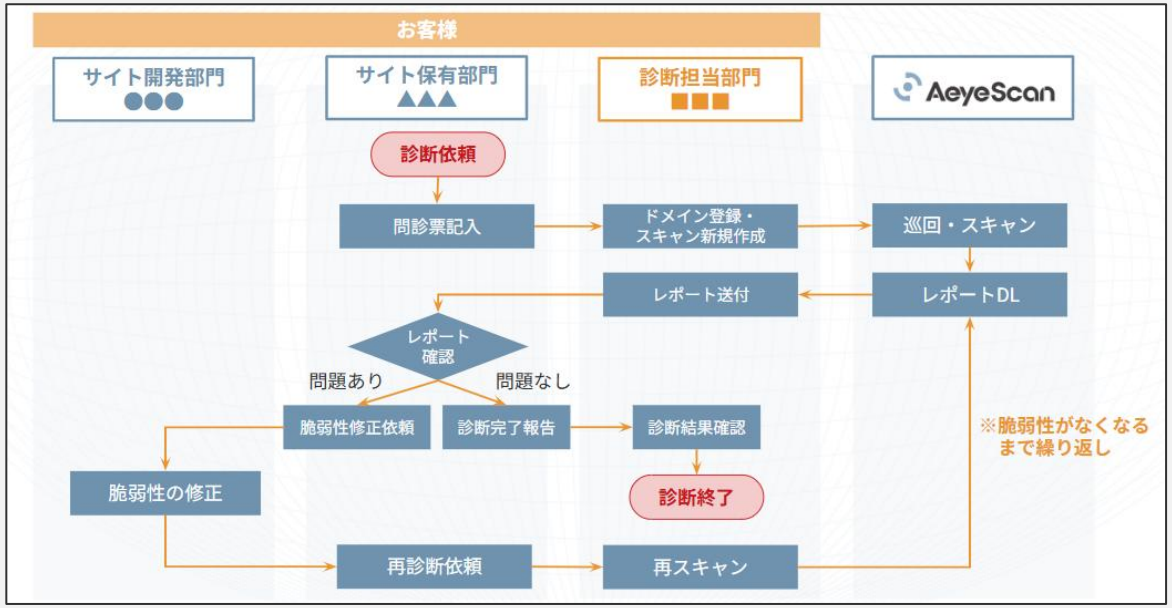
役割分担はどうすればいい？

AeyeSecurityLab

脆弱性診断に特化した業務フロー検討支援

「誰が」「いつ」「なにを」するのか、あらかじめ明確にすることで
ボトルネックや解決策のシミュレーションができます！

貴社と同様のフローの企業が
どのような悩みを持っていたのか？
どうやって解消してきたのか？など
他社事例も踏まえたご提案を
させていただきます。



脆弱性診断におけるよくある課題 #2

脆弱性診断をどの範囲に対して
どのタイミングで
実施すればよいか悩んでいる。

サイト保有部門が脆弱性診断に
応じてくれない。
必要性を理解してくれない。

AeyeSecurityLab

脆弱性診断ルールの策定

多くの企業で策定している項目（ベストプラクティス）に沿って、
貴社のご状況に合わせた独自のルール作成をご支援いたします。
同業種・同規模の他社事例の情報提供も可能です。

初回診断“前”に必要

診断対象・範囲

- 社外公開有無
- 重要情報の取り扱い有無
- 動的サイト/静的サイト有無

診断タイミング・頻度

- 随時診断の実施有無と頻度
  （新規リリース/機能追加・改修）
- 定期診断の実施有無と頻度

初回診断“後”に検討

診断対象の棚卸

- 棚卸の頻度
- 棚卸の方法

診断手法の棲み分け

- AeyeScanのみ/
  手動診断・外部委託と併用
- （併用の場合）切り分けの基準

脆弱性の修正基準（トリアージ）

- 修正対象の基準
- 修正期限

脆弱性診断実施状況の監査・確認

- ルールに基づいた
  診断および修正状況の確認
- 確認方法

脆弱性診断におけるよくある課題 #3

診断対象サイトは複数あるが
どこから着手すべきか悩んでいる。

診断の事前準備に時間がかかって
スケジュール通りに実施できない。

AeyeSecurityLab

診断スケジュール作成支援

診断対象サイトへの診断計画を策定することで、
効率よく・円滑に診断していくことができます。

診断計画が決まっていない場合は、弊社で**計画策定をご支援**いたします。

おすすめの進め方

- 初回診断対象の棚卸
- 診断の優先度を定義・評価

まずは診断業務が問題なく回せるかどうかの検証も含め、

向こう３ヶ月の診断計画を立ててみましょう！

診断優先度の決定とスケジュール化

診断対象サイトの優先度が決まったら、以下に基づいてスケジュール化します。

優先順位の付け方

難易度＞重要度＞緊急度

難易度が低いものから先に実施し、
その間に難易度が高い＝事前調整が必要なサイトへ調整を進めておきます。

難易度：低のサイト → 事前準備 → 診断 → 事後対応

難易度：高のサイト → 事前準備 → 診断 → 事後対応

：

いきなり全て内製化は厳しいので…

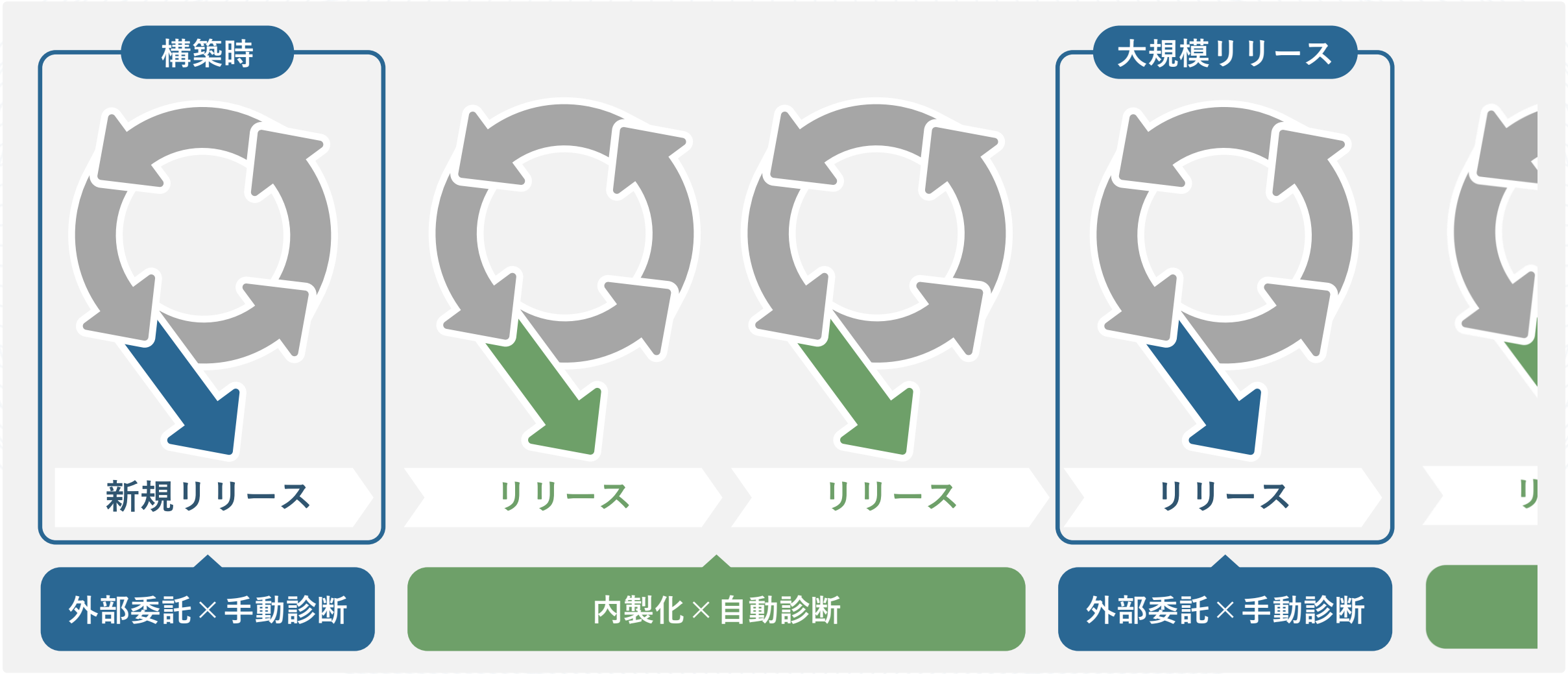
ハイブリッド型・脆弱性診断の手引き

代表的な診断スタイルと、大方針の考え方

お金と時間に余裕があって
「おまかせ」したい場合

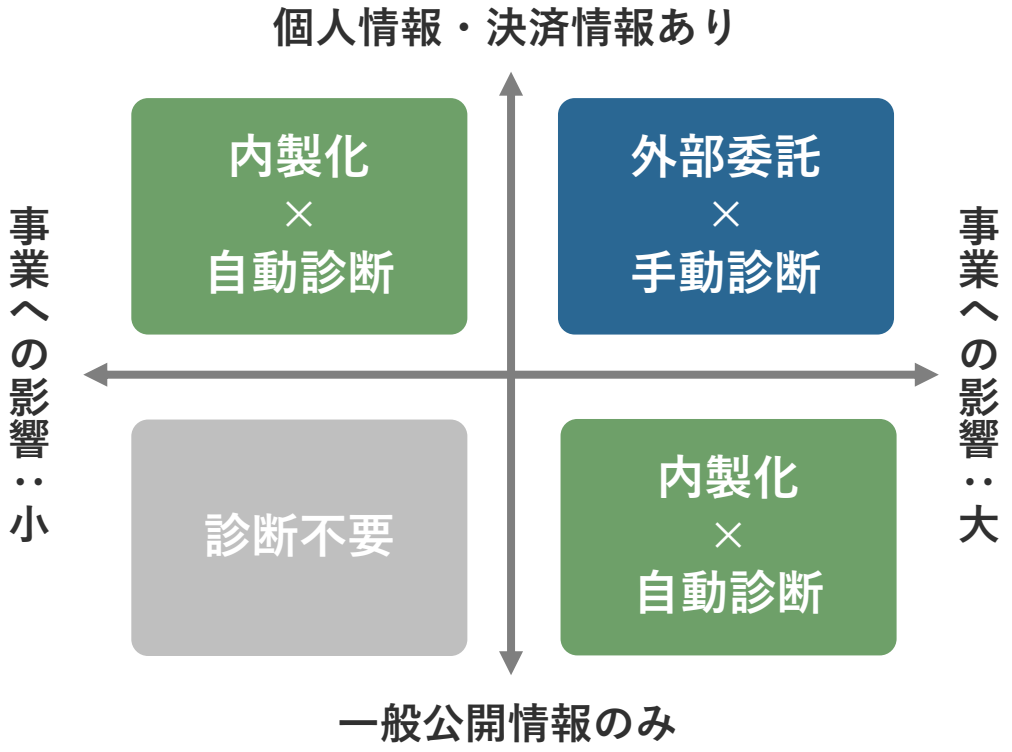
お金と時間に限りがあるが
それでも何とかしたい場合

色々な「ハイブリッド型運用」の類型（サイト単位）

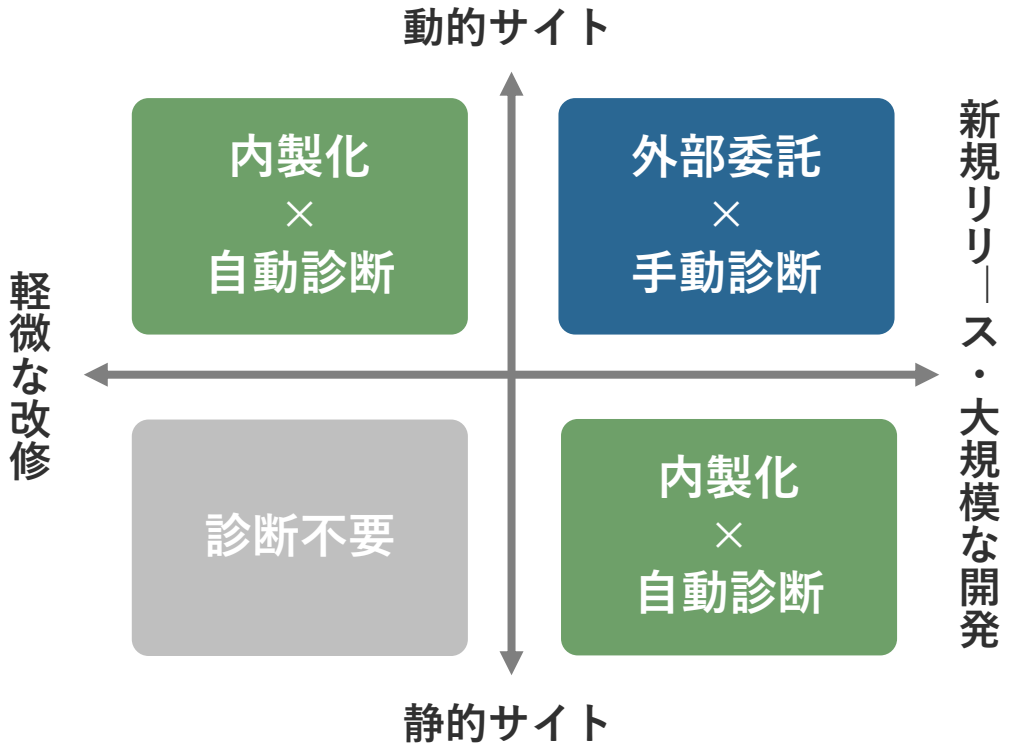


色々な「ハイブリッド型運用」の類型（診断単位）

定期診断



リリース前診断



まとめ：脆弱性診断「内製化」のポイント

失敗例

- 外部委託の要件をそのまま適用
- 最初から全社一斉に利用開始
- 現場だけで内製化を進めようとする（上位層を巻き込めていない）

成功例

- 外部診断／内製診断を使い分ける
- 優先順位を付けて、
  クイック＆スモールに始める
- 内製化の目的や意義を上位層と
  合意し、段階的に進めていく

外注×内製のハイブリッド体制を実現する

AeyeScan のご紹介

生成AI時代の脆弱性診断なら AeyeScan

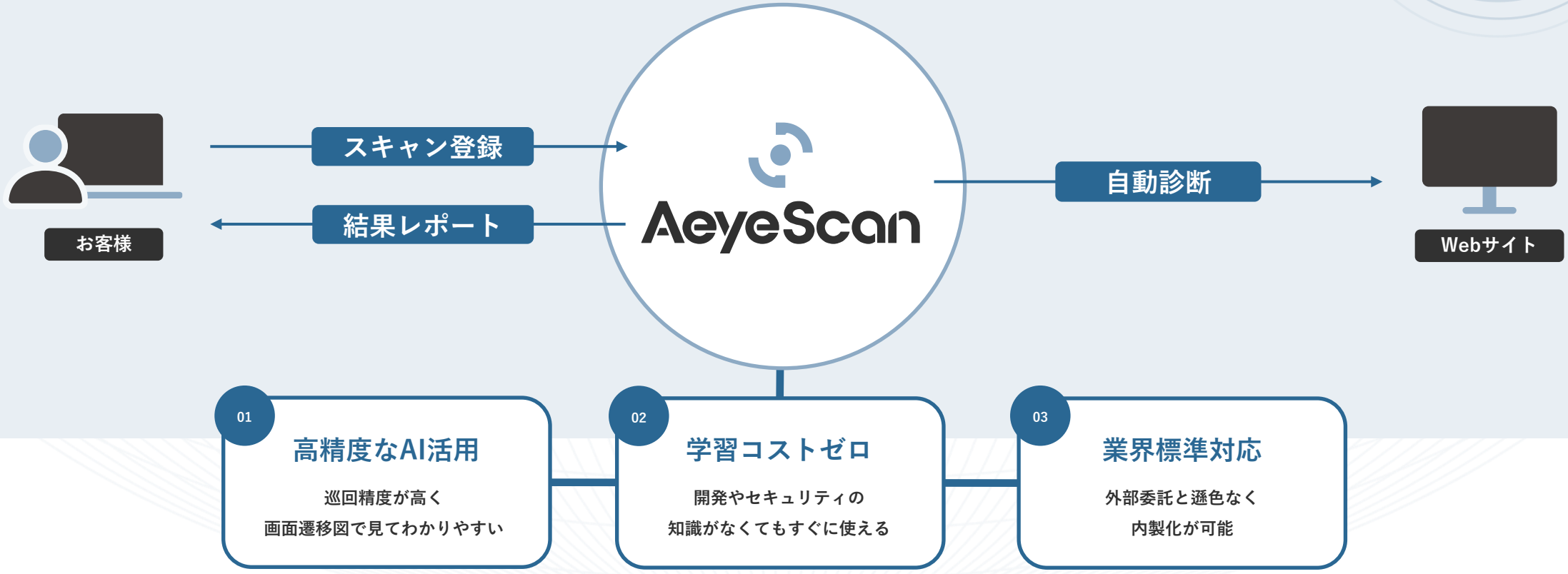
クラウド型Webアプリケーション
脆弱性検査ツール

国内市場シェア
No.1※

※ 富士キメラ総研調べ「2025 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 ベンダーシェア（2024年度実績）

※ITR調べ「ITR Market View：サイバー・セキュリティ対策市場2025」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（2023年度実績）

有償契約
300社以上



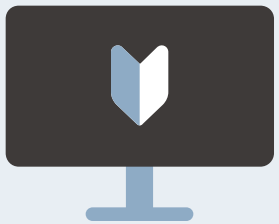
01
高精度なAI活用
巡回精度が高く
画面遷移図で見てわかりやすい

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

AeyeSecurityLab

AeyeScanが選ばれている理由 ① 社内メンバーでも診断ができる！



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。

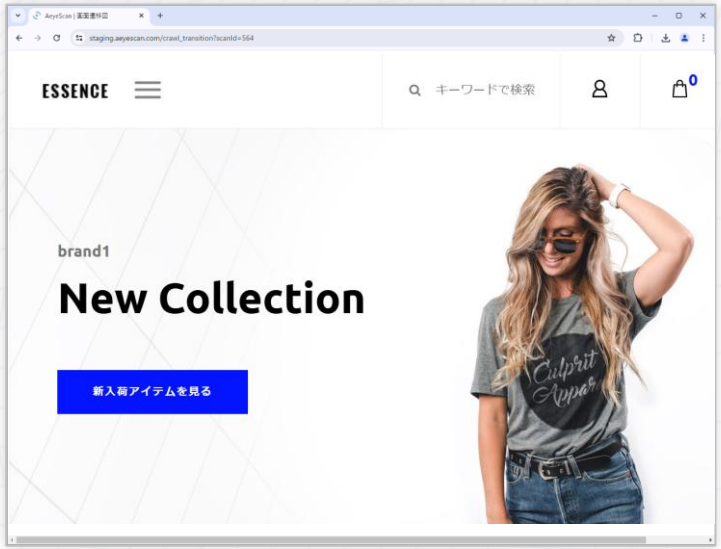
AIによる自動診断

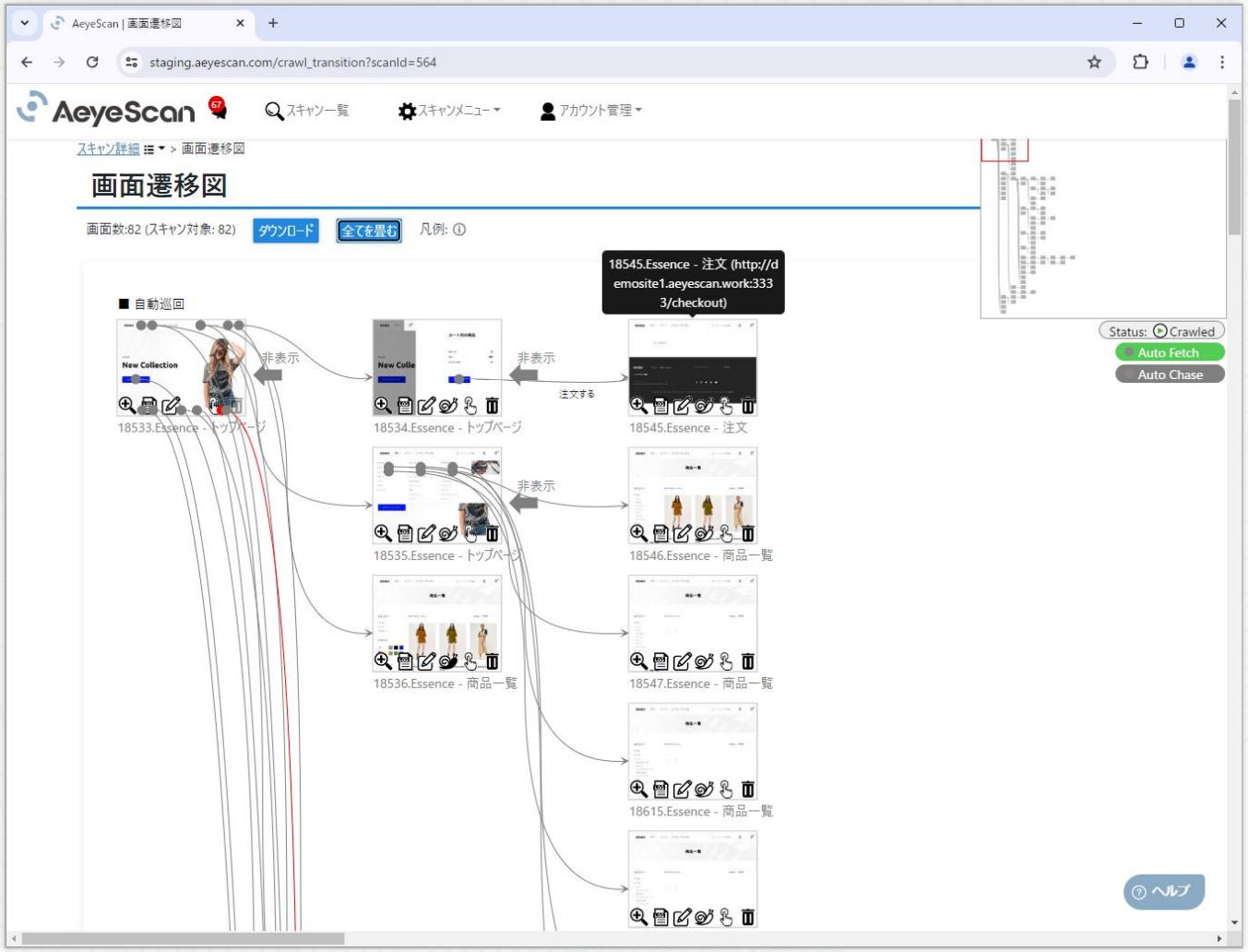
圧倒的な巡回精度で
24時間自動で診断。
画面遷移図で状況を可視化。

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





AeyeSecurityLab

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

AeyeScanが選ばれている理由 ② プロ級の品質・性能・機能

各種セキュリティガイドラインの自動化可能な項目に対応

OWASP TOP10

日本語版PDFはこちら

OWASP アプリケーション
セキュリティ検証標準

OWASP github

IPA
安全なWebサイトの作り方

PDFはこちら

ココがポイント

独立行政法人情報処理推進機構（IPA）が実施した
2021年度セキュリティ製品の有効性検証においてもAeyeScanが選定されている

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

人材・教育

HSAWA DRIVING SCHOOL
河合塾
Junion
JINSOKEN
ZENKIGEN
Direct Sourcing
PERSOL
Leverages
workport

インフラ

EPARK
AIRE
HIS
H.O RETAILING
NTT EAST
odakyu
近鉄情報システム株式会社
SymEnergy
水ing Swing Corporation
Suzuyo
NANKAI 南海システムソリューションズ
日本調剤
HITOWA GROUP
ベルーナ
grow up together MEDIA
Looop
Loyalty Marketing, Inc.

金融

アイフル
MS&AD MS&ADインターリスク総研
JOBPAY
SOMPOひまわり生命
DMM FinTech
Tokyo Century
Net Protections

メディア

集英社
中日新聞
NIKKEI
Media Do

製造

AICA
AISIN
KITZ 株式会社キッツ
KOSÉ
SAKI
TIGER
TEIJIN
Denkei
House
Mizuno
ユーグレナ

エンタメ

e+ イープラス
CAPCOM
GungHo Online Entertainment, Inc.
とらラボ! TORANOANA LABORATORY
BookLive

SaaS

Advanced Media, Inc. 株式会社アドバンスト・メディア
Lexica E-Retailing Platform
estie
エアアンドエムマット株式会社
M-aid
エムティーアイ
OZ INTERNATIONAL
Classi
COACH A Co.,Ltd.
cybozu
Speee
SecureNavi
Diamond head
DMM Boost
TAL
Digital Garage
TEMONA
NAVITIME
KNOCK ON THE DOOR
BATONZ
VALUE HR
freee
vector
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.
SBWorks
NTT Integration
NTT DATA
NTT ビジネスソリューションズ
OMRON
Globalway
KDDI Agile Development Center
circlace
さくら情報システム
SUNDAY SYSTEMS
CEC
GA TECHNOLOGIES
tdi 情報技術開発株式会社
Simplex Inc.
777WORKS 株式会社スリーセブンワークス
SOFT CREATE
SOLTEC
高千穂交易株式会社
電通総研
TOPPAN
JOPS
JAST
PCNET 株式会社パシフィックネット
Human Interactive Technology Inc.
FUJISOFT
FUJITSU
MACROMILL
三菱電機デジタルイノベーション株式会社
YONA
リピスト

セキュリティ企業

NEC NECセキュリティ
NTT DATA 株式会社NTTデータ先端技術
GSX GLOBAL SECURITY EXPERTS
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 ③ コスト・時間の削減効果

圧倒的コストパフォーマンス

診断サイト数

診断画面数

診断回数

→ 無制限

AeyeScanを導入したお客様から お伺いした診断スピードの変化

	外注時	AeyeScan
G社	2週間	4-5日
A社	最長 1か月	最短 4日
C社	開始まで 1か月	2-3日

AeyeSecurityLab

導入事例紹介

メディアグループ ホールディングス 様

企業名	メディアグループホールディングス株式会社
事業内容	グループ統括／経営企画／管理 歯科ICT事業（メディア株式会社）、AI画像処理事業（アイテック株式会社）
従業員数	連結278名／単体30名（2024年10月時点）

課題

30以上のドメインに水準感を合わせた診断を行うにはコスト・工数面の課題があった

具体的な課題

1. 外部ベンダーによる手動診断では、費用や準備時間が課題になっていた
2. グループ全体でページ数も多く、ドメイン毎のリスク診断の水準感等にバラツキがあった。

歯科ICソリューションやAI画像ソリューションなどを提供してきた同社グループ。全社統一的な水準での脆弱性診断が実施出来ていない状況だった。

導入

複数ドメインに追加コストが不要な料金体系が決め手に

導入の背景

1. 診断対象とするドメイン数が無制限
2. OWASPアプリケーションセキュリティ検証標準に準拠している
3. Cookieやカスタムヘッダーのチューニングが行えるなど自由度が高い

比較検討を進める中で、ドメイン数無制限の料金体系がAeyeScan導入の決め手に。巡回精度のほか、自動生成される画面遷移図も使い勝手が良いと評価。また、レポート作成の工数が削減できる点もメリットだと感じた。

効果

統一的な水準・頻度で一定品質を備えた脆弱性診断を、コストや工数を抑えて実施。より万全なセキュリティ体制の基盤を構築

具体的な効果

1. すべてのサイトに同一基準で脆弱性診断が行えるようになった
2. 各サイトへの診断実施のハードルが下がるとともに、担当者のセキュリティ意識も向上
3. サービスの安全性を客観的に示せる

診断の準備に1～2ヶ月かかることもあったのに対し、現在はドメイン登録後、即診断が行えるようになった。AeyeScanの分かりやすいレポート機能により、検知から対処までがスムーズに行えるようになった。

導入事例紹介

ゲオホールディングス 様

企業名　株式会社ゲオホールディングス

事業内容　メディア事業・リユース事業・オフプライス事業・モバイル事業など

従業員数　連結6,512名（2025年8月時点）

課題

事業が成長していくスピードに
合わせた診断が困難に

具体的な課題

1. 診断対象のWebアプリケーション数が拡大
2. 外注では調整やコストの面が課題に
3. セキュリティ室が社内で診断するのは業務負荷がかかる

全国2,000を超える「ゲオ」店舗での販売を支えるシステムや、オンライン販売を行うWeb・スマホアプリが拡大し、アタックサーフェイスも増加。診断は外注していたが、事業成長のスピードに追いつかなくなっていた。

導入

開発チームでも使いこなせる
使い勝手の良さを評価

導入の背景

1. グラフィカルな画面遷移図で、どこにどんな脆弱性があるかわかりやすい
2. マニュアルがなくても操作できる
3. SaaS形式で容易に導入できる

複数ツールを比較し「安価だが診断内容がシンプルすぎる」「昔ながらのインターフェイスで開発者が使いづらい」など、決め手に欠けていた。そのような中、AeyeScanの操作性の良さを高く評価し、導入を決定。

効果

開発者主導の診断体制を確立し
コスパよくスピーディーな診断を実現

具体的な効果

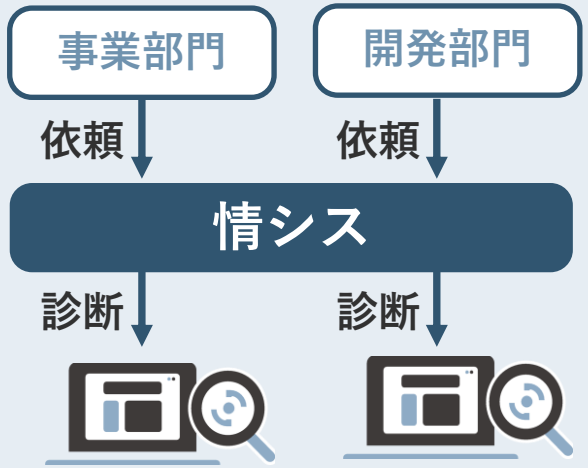
1. 開発チームが最小の工数で診断できる
2. 短期間での開発・リリース案件でも間に合うスピーディーな診断を実現
3. 開発者とのコミュニケーション補助ツールとしても活躍

導入当初はセキュリティ室がメインで診断を行い、徐々に開発チームへと展開を進めていった。外注時と比較して、コスパよくスピーディーに診断が行えることに加え、社内のセキュリティ意識も向上している。

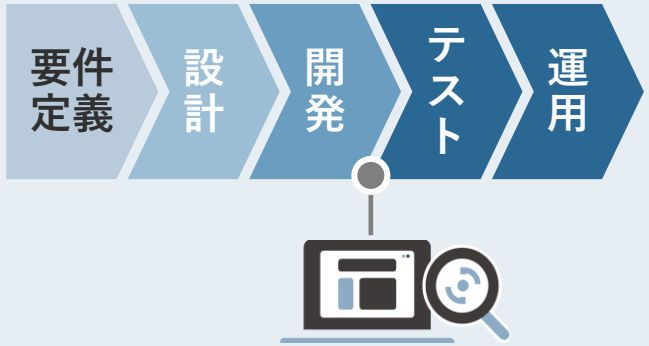
AeyeSecurityLab

運用体制・活用パターン

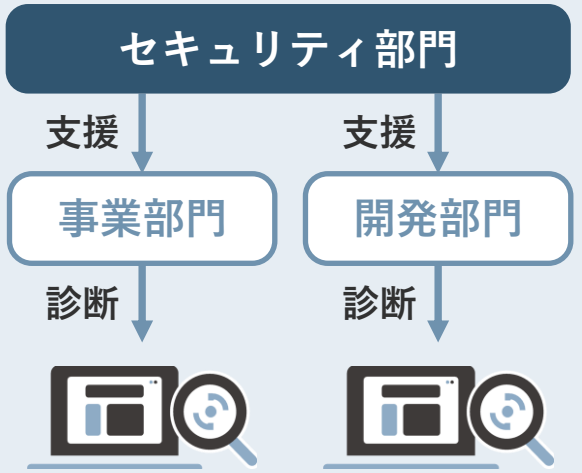
情シス主導型



開発組み込み型



部門分散型



自社の体制に合った活用方法で、クイック＆スモールにスタート

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

AeyeSecurityLab

定期開催中！ AeyeScanがよく分かるデモ動画・セミナー

AeyeScanを検討してみたい方へ

AeyeScanがどんなものか知りたい方向けに、
デモを交えてわかりやすくご紹介。
まずは気軽に使い勝手をチェック！

AeyeScanデモ動画を視聴

AeyeScanの操作を体験してみたい方へ

実際の操作を通して、一連の機能を体感。
導入前の不安や疑問をまるごと解消。
“わからないまま”をなくすセミナーです。

ハンズオンセミナーの日程を確認

セキュリティ対策にお悩みの方へ

最新の事例や対策ノウハウをテーマ別に紹介。
月替わりで学べる無料ウェビナーを開催中。
お気軽にご視聴いただけます！

ウェビナーの日程を確認

AeyeScanを実際に操作してみませんか？

セキュリティに、確かな答えを。