AIと進める

“開発を止めない” シフトレフト

―品質向上が競争力を加速する―

登壇者紹介

株式会社エーアイセキュリティラボ

執行役員兼CX本部長　**関根 鉄平**　CISSP

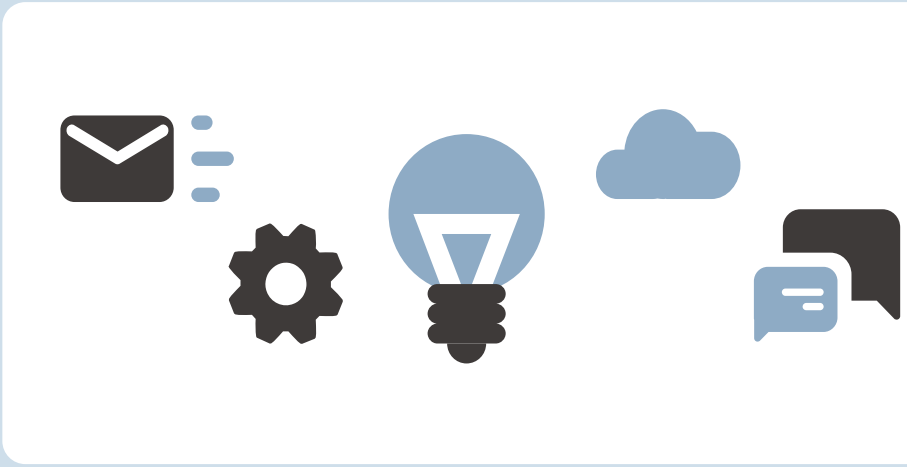
セキュリティエンジニアとして大手金融機関等の脆弱性診断に従事。その後、Webアプリケーション検査ツール・サポートチームの立ち上げをしつつ、CSIRTや開発現場でのセキュリティを推進。
2020年6月より現職。AeyeScanのカスタマーサクセスチームの責任者として脆弱性診断の内製化を支援。大規模イベントや大手企業での講演に多数登壇している。
『セキュリティエンジニアの知識地図』を共著。

コミュニティ活動など

- 日本セキュリティオペレーション事業者協議会（ISOG-J）、OWASP Japan 共同ワーキンググループ
- 公益社団法人日本通信販売協会（JADMA）Web・セキュリティ専門部会
- 情報セキュリティ10大脅威 選考会メンバー

DXの進展でセキュリティ対策の需要は高まっている

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
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

「セキュリティもやる前提」の開発現場が直面する課題

リソースが限られていて
セキュリティ対応まで
手が回らない

セキュリティ人材不足で
専門知識が
チーム内で不足している

脆弱性管理・対応が
属人化しており
共通の基準が持てない

PMは限られたリソースでセキュリティ対策もしなければいけない
開発スピードとの両立も難しい…

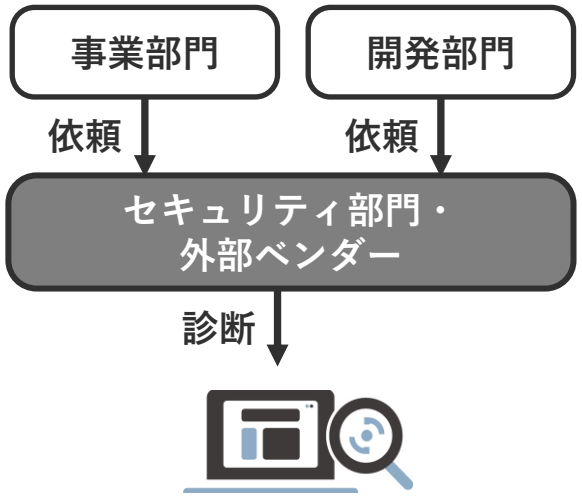
AeyeSecurityLab

開発とセキュリティを両立するために、運用体制を見直す

セキュリティを開発の中に組み込むことで、スピードアップが実現する。

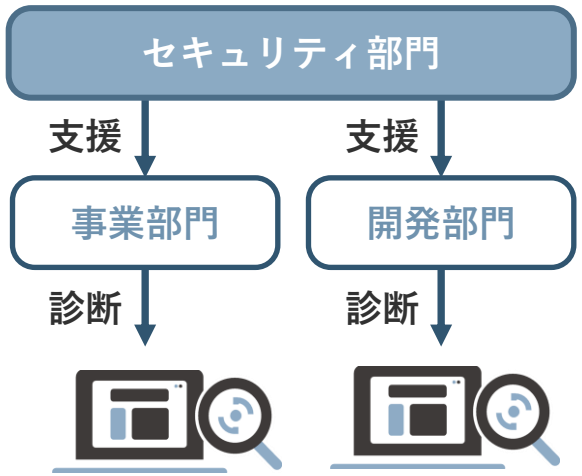
従来の運用体制

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
脆弱性診断を実施できる
体制**を構築

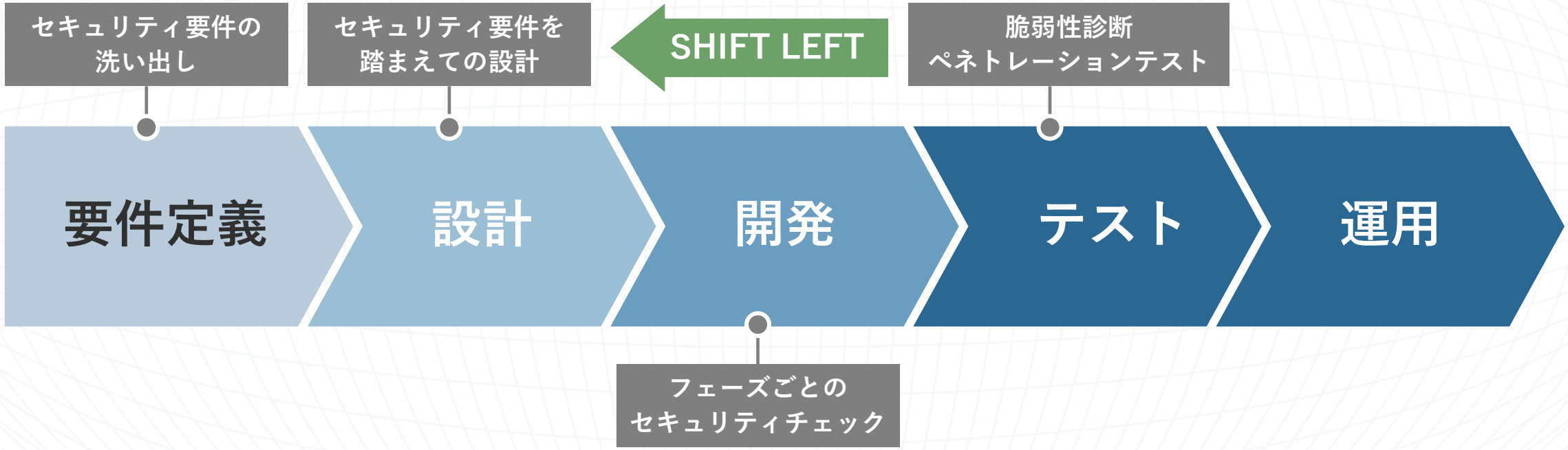


実現したいこと

- 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

PMの負担を減らしながら、品質を高めるシフトレフト

問題を早期に発見・修正することで手戻りが減り、スピードアップと品質向上を両立。



さらに、対策を講じるべき対象を的確に把握できる。
また、セキュリティ意識の醸成にもつながる。

シフトレフトを進める上で立ちはだかる「内製化」の壁

セキュリティ対策を内製化する第一歩として、脆弱性診断ツールの選定があるが、
そこでつまづきがちです。

まずは無料のものから
使ってみるべき？

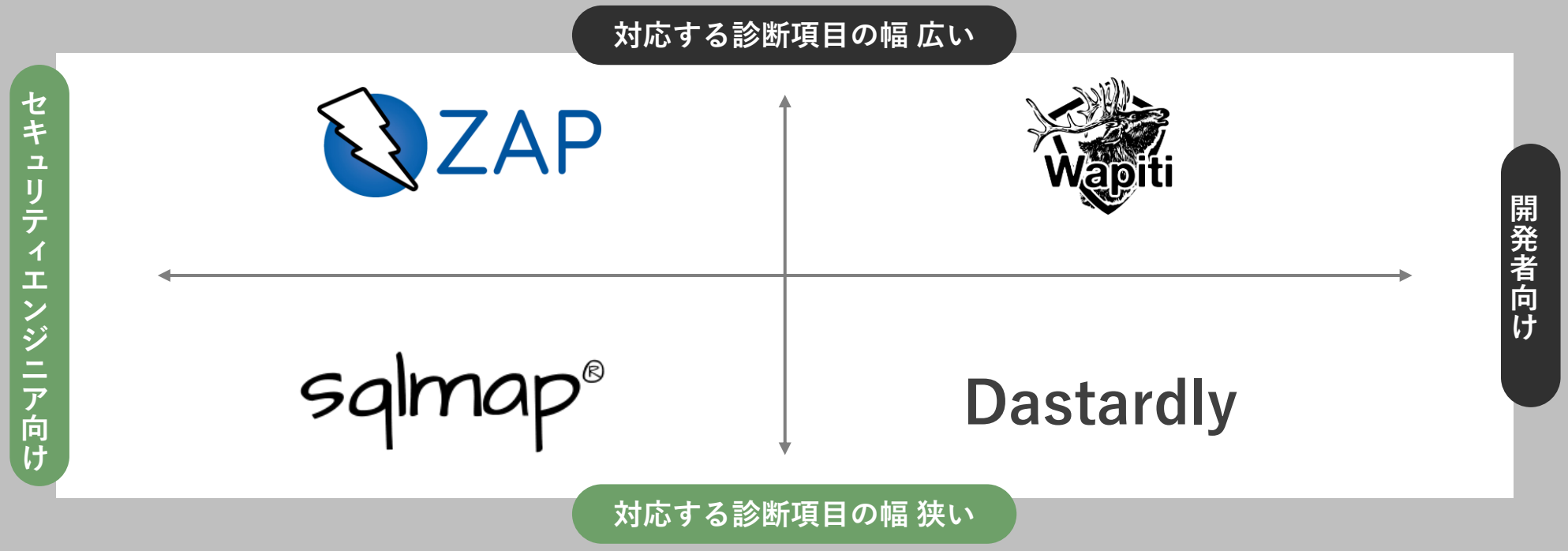
どれが自分たちのニーズを
満たしている？

正直、どれも同じに
見える…

そもそも、内製化のために有償ツールを導入するのはハードルが高い…

内製化の第一歩として選ばれがちな「無料ツール」

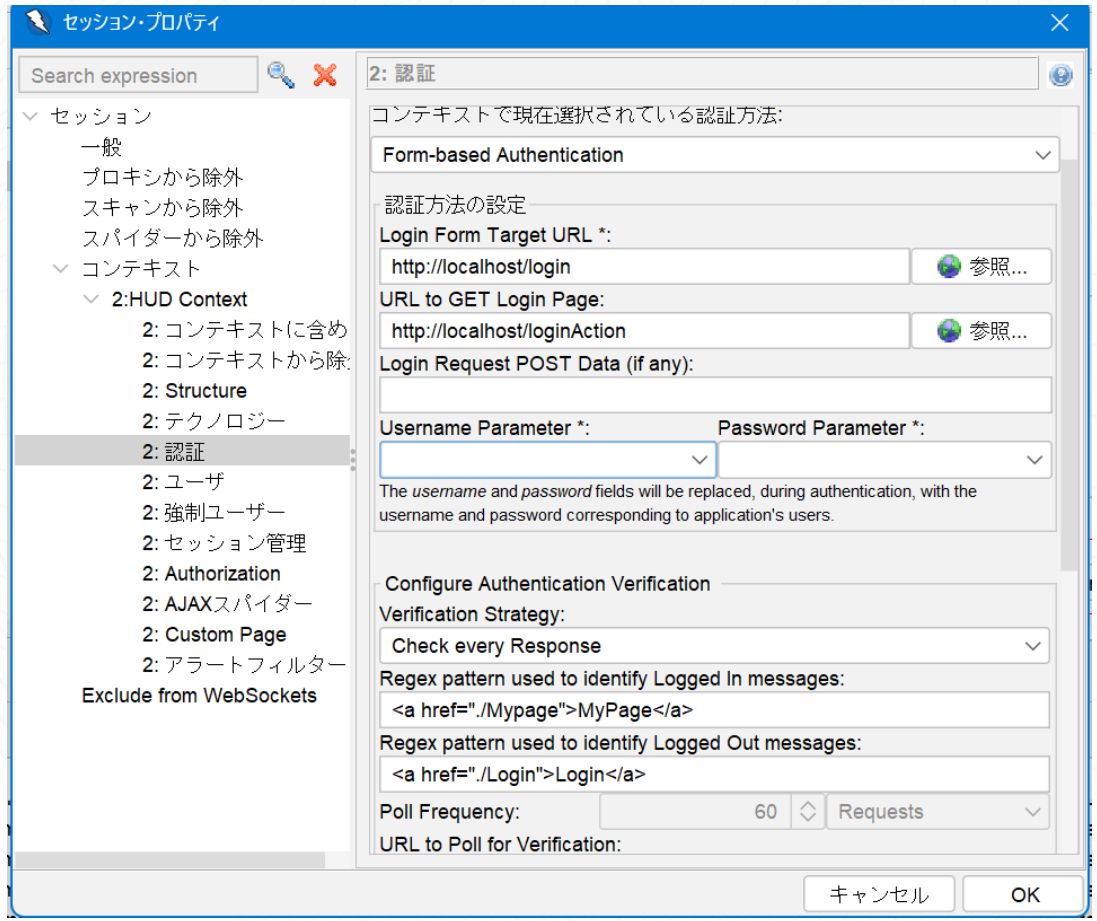
脆弱性診断ツールの一例

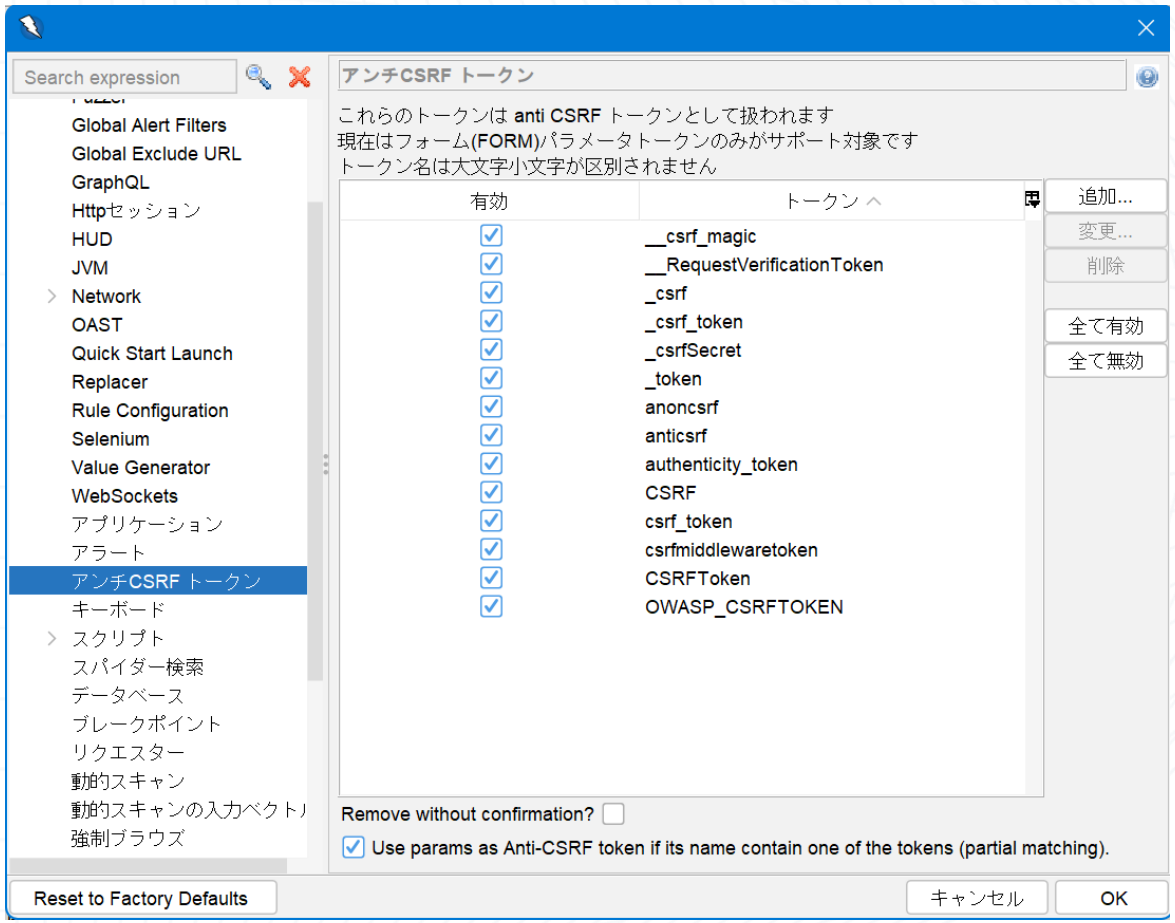


設定さえ行えば、無料ツールでも脆弱性診断を行うことは可能。

→　実際の画面をご覧ください！

OWASP ZAP 実際の画面





無料ツールを導入しても、逆に工数がかかっては意味がない

Webサイトの数が増え、それぞれ診断頻度が高まると、人力での対応に限界が…

診断対象の増加

並行して開発されている
複数の製品に診断が必要

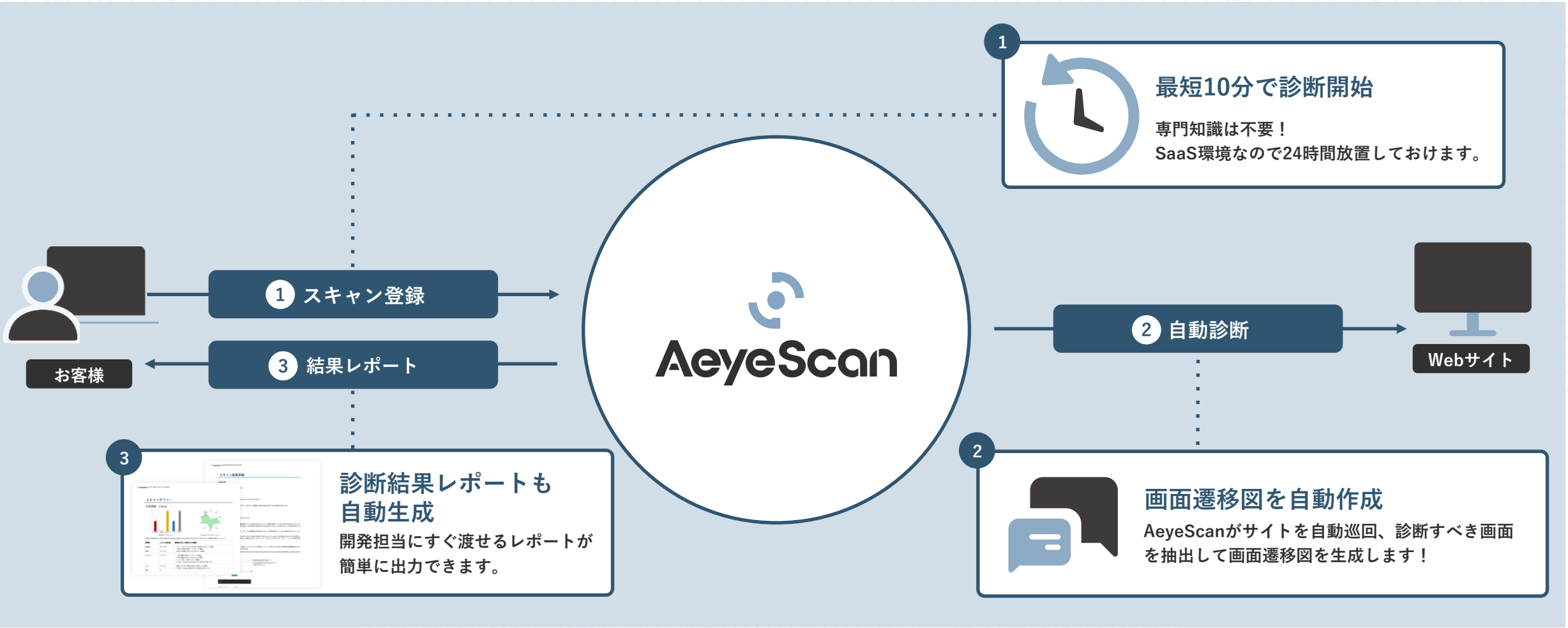
リソース不足

各製品に割ける人員や
スケジュールに限りがある

そこでご紹介したいのが、AI活用により**診断を自動化**するツール

AeyeScanとは：診断の全工程を圧倒的に自動化

AI・RPA活用により、脆弱性診断を自動化するクラウド型Webアプリケーション診断ツールです。

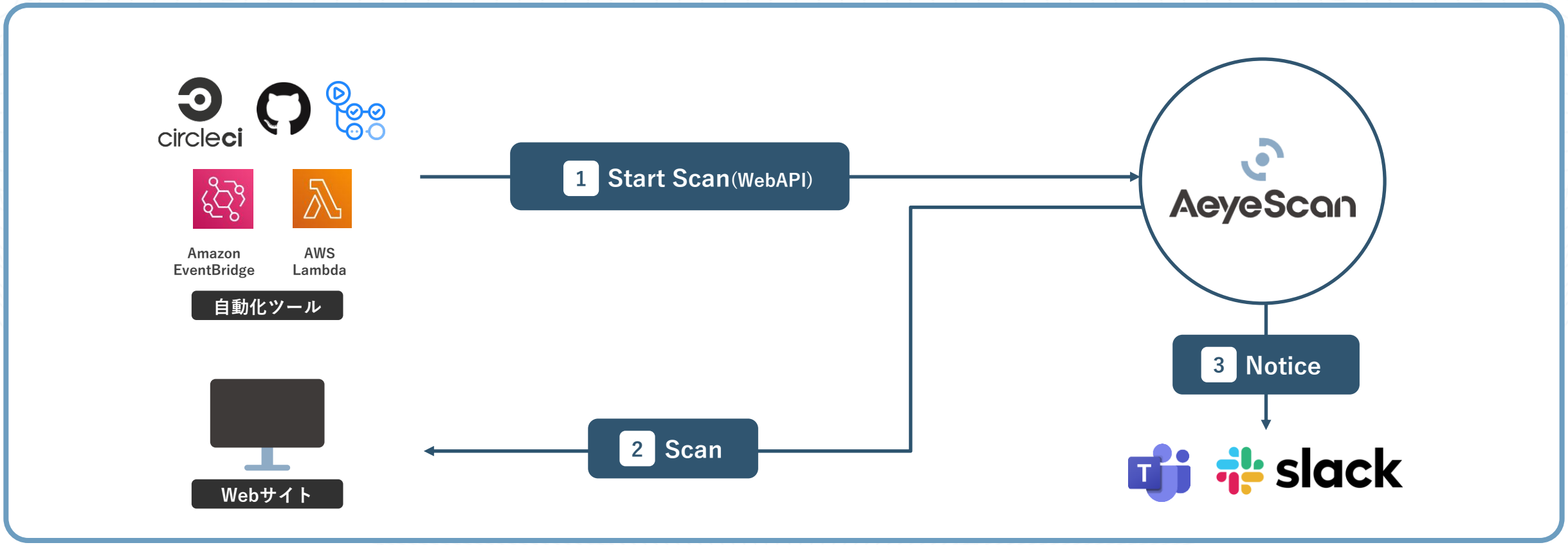


Demonstration

デモ

CI/CD連携でアジャイル開発・高頻度リリースでも漏れなく診断

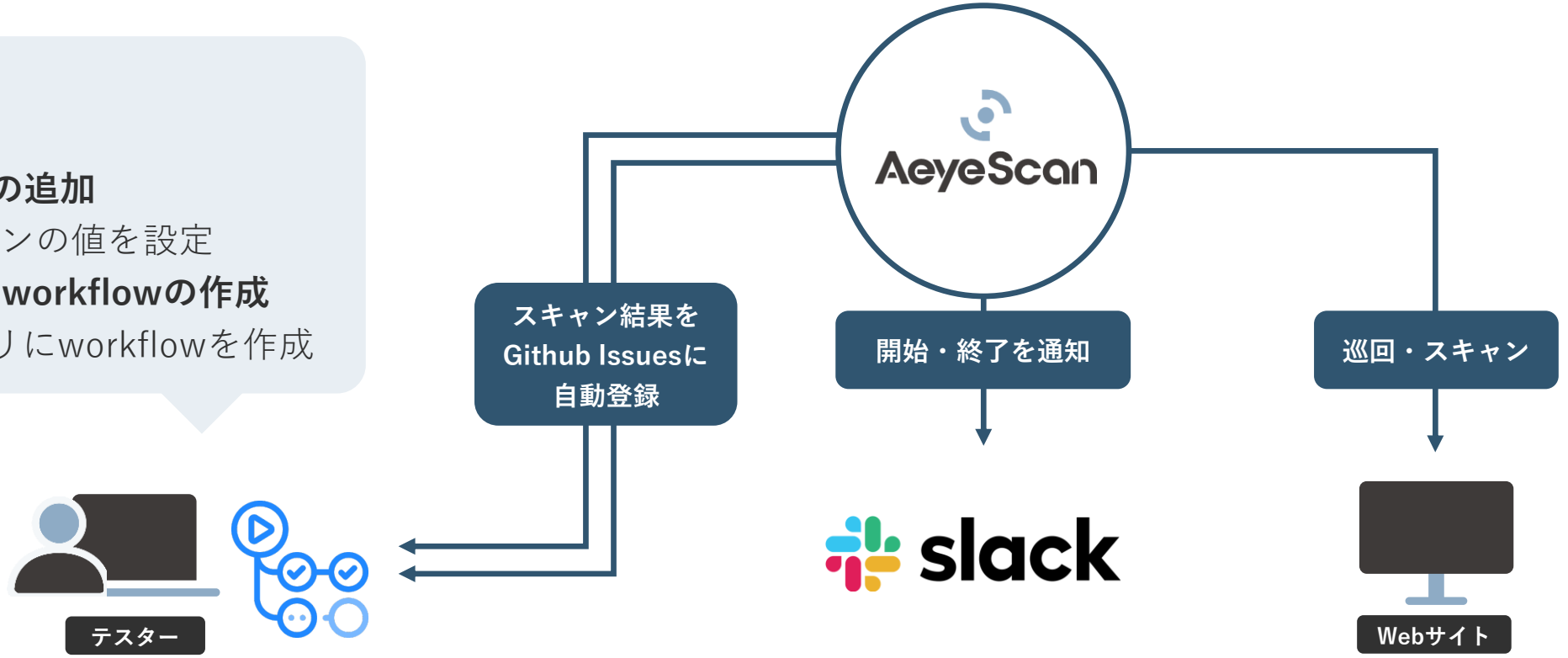
CI/CDに組み込むことで、リリースのたびに自動で診断が実行される仕組みづくりが可能に。
診断を開発プロセスに組み込み標準化できるので、大幅な効率化とセキュリティ強化を両立。



仕組みづくりと効率化の事例

Github Actionsを使い、診断を自動化。結果も一元管理

1. **スキャン作成**
2. **APIキー作成**
3. **GitHub secretsの追加**
   APIキーとトークンの値を設定
4. **GitHub Actions workflowの作成**
   Githubリポジトリにworkflowを作成



内製と外注を併用する「ハイブリッド型」の運用がおすすめ

脆弱性診断のベストな頻度

1 Webサイト構築時

まず、Webサイトの設計・開発時に
可能な限り脆弱性を解消しておく。

2 Webサイト運用時

運用中に発生する問題に対応し、
Webサイトの安全性を維持する。

自社のセキュリティポリシーに適した運用を。推奨は…

年に1回の
定期診断

＋

リリースや
機能改修時

**ツールだけで全てをまかなおうとせず、
大規模改修などの際は外注も視野に入れ、濃淡をつけた対応を！**

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名（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（エーアイスキャン）により
セキュリティ対策にかかる **コストを削減！**

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※

有償契約
300社以上

※ 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）

プロが認める品質・精度 ＋ ブラウザ上での直感的な操作

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

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

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

Junion
JINSOKEN
ZENKIGEN
Direct Sourcing
PERSOL
Leverages
workport

インフラ

EPARK
AIRE
HIS
NTT EAST
odakyu
近鉄情報システム株式会社
SymEnergy
水ing
Suzuyo
NANKAI
日本調剤
HITOWA GROUP
grow up together MEDIA
Looop
Loyalty Marketing, Inc.

金融

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
KOSÉ
SAKI
TIGER
TEIJIN
Denkei
House
Mizuno
ユーグレナ

エンタメ

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

SaaS

Advanced Media, Inc.
Lexica
estie
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
Finovo
freee
porters
hokan
Money Forward
RUN.EDGE
RVSTA
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 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
SUNDAY SYSTEMS
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
JAST
NHC
PCNET
Human Interactive Technology inc.
FUJISOFT
FUJITSU
MACROMILL
YONA
リピスト

セキュリティ企業

NEC
NECセキュリティ
NTT DATA
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

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。