脆弱性診断はどの方法を選ぶべき？

ツール診断・手動診断の違いと、自社に合った診断手法の見極め方

AeyeSecurityLab

本資料の目的

ビジネス環境や開発体制の変化に伴い、脆弱性診断の実施方法も進化しています。
診断そのものの需要も高まり続ける中で、現場ではどのように実施すれば良いか迷うケースも少なくありません。

「どんな診断方法が自社に合っているのかわからない」「自社の場合、内製化すべきか外部に委託すべきかわからない」
「そもそも、どのような診断方法があるのだろうか？」「内製化するとしても、誰が診断を実施すべき？」
など、脆弱性診断を進めていくにあたっては、さまざま疑問が生じているのではないでしょうか。

本資料では、セキュリティご担当者に向け、脆弱性診断の代表的な実施方法やそれぞれのメリット・課題を詳しく解説。
近年、選択する企業が増えている「ハイブリッド診断」についても取り上げ、
自社に最適な診断方法の選び方から、実践に向けたヒントまでをまとめています。

Webサイトのセキュリティを強化したい方、自社に合った診断手法を知りたい方は、ぜひご一読ください。

代表的な診断方法と大方針

診断方法	特徴	手法	大方針
外部委託	専門業者に依頼	手動診断が多いが 直近では自動診断も登場	お金と時間に余裕があって 「おまかせ」できる場合
ハイブリッド	一部を外部委託するが 残りは自社で診断	複数手法を組み合わせる	お金と時間に限りがあるものの セキュリティを担保したい場合
内製（自社実施）	社内セキュリティ部門や 開発チームが診断	脆弱性診断ツールを 利用することが多い	

手動診断

- ○ きめ細やかな診断
- △ 工数/時間がかかる

自動診断

- ○ おまかせ&スピーディ
- △ 診断範囲が限定的

従来は「おまかせ」状態の企業が多かった

これまで 「外部委託」で「手動診断」を検討することが主流だった

開発を完全に
外部委託している

取引先などから
外部委託を求められる

専門性の高い領域は
専門家に任せたい

**費用と時間はかかるが、外部に診断を「おまかせ」することが
一般的な選択肢だった**

今は「診断スタイルの見極め」が必要に

市場の変化・DXの進展によって、従来の診断方法では追いつかなくなっている

セキュリティ人材の不足

採用・育成の難易度が上がり
委託先でも同じくリソース不足で
診断／リリースが滞る

アジャイル開発の増加

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

ノーコード開発 ローコード開発

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

どのような診断方法を選択・使い分けすべきか、現場で判断に迷うことも…

代表的な診断方法ごとのメリット・課題

診断方法	○ メリット	△ 課題
外部委託	・専門性と社内外への結果の信頼性が高い ・自社での人材育成やツール導入・運用が不要	・ほかの方法と比べ、費用が高額になりやすい ・各調整の負担が大きく、緊急時の対応が困難
ハイブリッド	・外部委託と内製のメリットが両方得られる ・リスクの重要性に沿った効率的な投資が可能	・方法を使い分ける明確な方針策定が必要 ・方法の混在によって管理工数が増加しやすい
内製（自社実施）	・低コストかつ迅速・柔軟な診断が可能 ・自社内でノウハウが蓄積できる	・人材の確保や業務フロー/ルール整備が必要 ・高度な攻撃手法への対応が難しい場合がある

どのような診断方法を選択・使い分けすべきかは、
それぞれのメリットや課題を踏まえて検討するのがおすすめ

近年「ハイブリッド」に移行する企業が増えている

診断対象の増加やアジャイル開発の浸透、リリースサイクルの高速化といった市場の変化を背景に、企業では新たな診断ニーズを抱えることに。

増加するWebサイトに対し網羅的に診断したい

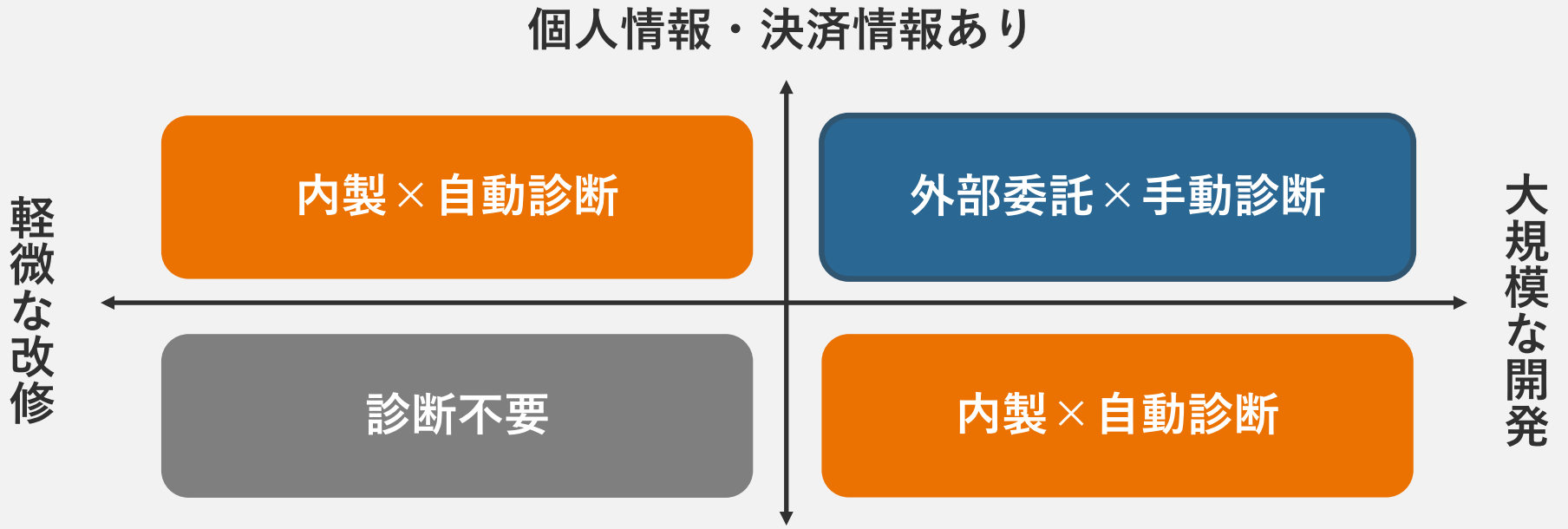
診断にかけるリソースを最適化したい

スピードと専門性のバランスを取りつつ継続的に診断したい

コスト・スピード・専門性のバランスを柔軟に調整できる「ハイブリッド」診断が選ばれている

「ハイブリッド」における外部委託／内製の決め方（例）

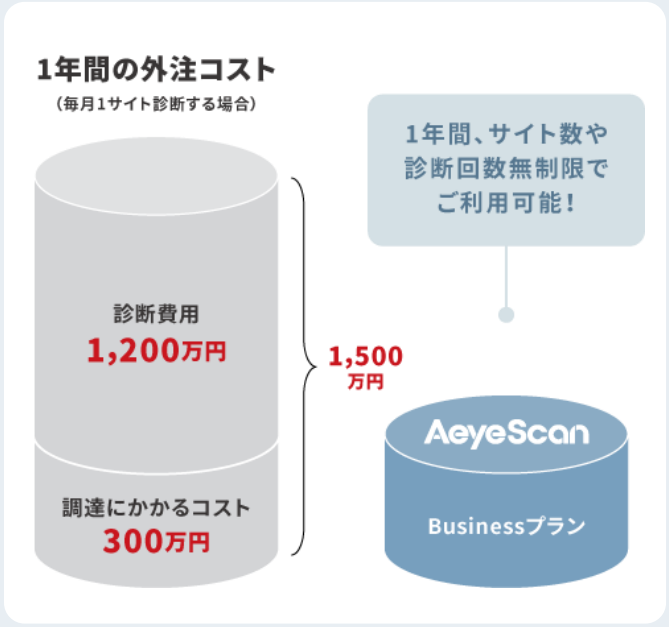
外部委託にするか内製にするかは、**診断対象サイトの重要度**（下図の縦軸）と、**開発規模・頻度・変更範囲**（下図の横軸）を踏まえて決めるとよいでしょう。



AeyeSecurityLab

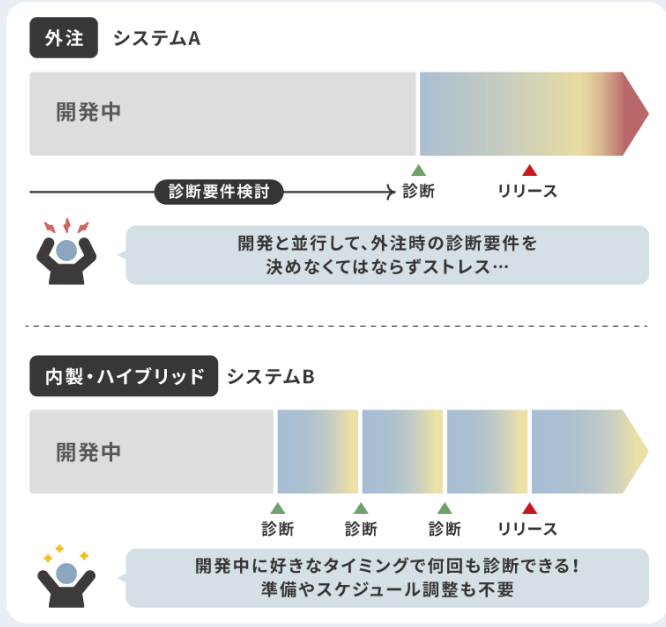
「ハイブリッド」にすると、具体的にどんなメリットがある？

診断コストを、ぐっと抑えられる



すべての診断を
外注するのに比べて、
コストを大幅に
削減できる

ちょっとの変更時も、逃さず診断できる



開発プロセスに診断を
組み込めるので、
修正や機能追加時にも
欠かさず診断できる

外注時の診断要件（対象サイト数・回数など）を決める手間・時間も軽減！

実際に、ハイブリッド診断に移行したお客様の成功事例をご覧ください！

株式会社カプコン 様

100%外部委託の状態から一部を内製化し、高頻度な診断を可能に

お客様の情報を取り扱うサイトや機能のリリース時には外部ベンダーによる手動診断を実施し、
関連するプロモーションサイトなど、セキュリティリスクの低いサイトをAeyeScanで自動診断。
これまで見送っていたサイトへも開発現場が主体となって高頻度に診断を実施する体制が整った。

このスタイルがマッチするケース

- 外注コストを抑えつつ、セキュリティ対策を最適化したい
- 開発プロセスにセキュリティ診断を組み込みたい
- 診断のスピードと頻度を上げたい

詳細はこちら⇒ https://www.aeyescan.jp/case/capcom/

株式会社バトンズ 様

外部委託に加えAeyeScanで毎週土日＋新機能リリース時の自動診断

企業のM&Aに関わるサービスを運営しており、トップレベルの機密情報を扱っているからこそ、サービスの頻繁なアップデート・リリースに合わせた診断を目指してハイブリッドな診断スタイルを構築。成長スピードを落とさず、堅牢なセキュリティを担保している。

このスタイルがマッチするケース

- 急成長中でリリースサイクルが短い
- 情報資産の機密性が高く、強固なセキュリティが求められる
- リリース前に高品質な診断を徹底したい

詳細はこちら⇒ https://www.aeyescan.jp/case/batonz/

とはいえ、診断の内製化ってどうやるの・・・？

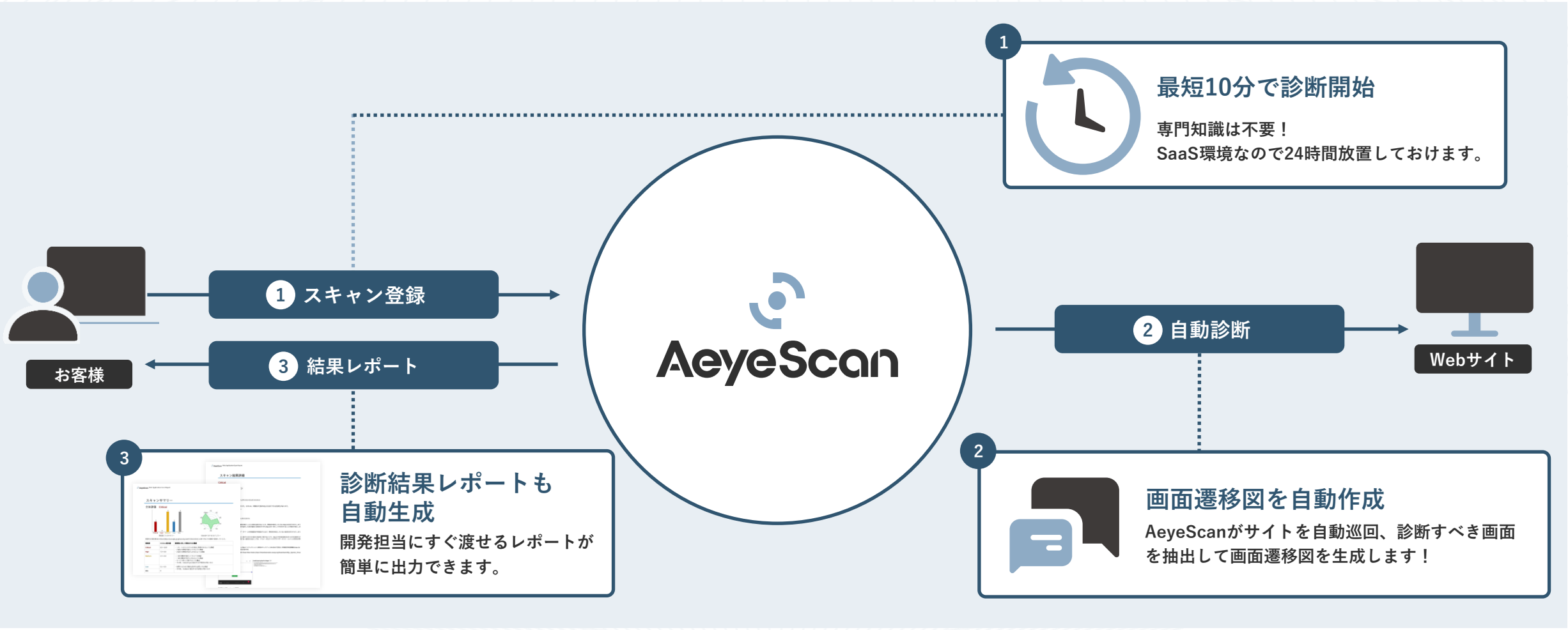
内製を含むハイブリッド診断は、人材・知識不足や管理工数が課題となりやすい

診断方法	○ メリット	△ 課題
外部委託	・専門性と社内外への結果の信頼性が高い ・自社での人材育成やツール導入・運用が不要	・ほかの方法と比べ、費用が高額になりやすい ・各調整の負担が大きく、緊急時の対応が困難
ハイブリッド	・外部委託と内製のメリットが両方得られる ・リスクの重要性に沿った効率的な投資が可能	・方法を使い分ける明確な方針策定が必要 ・方法の混在によって管理工数が増加しやすい
内製（自社実施）	・低コストかつ迅速・柔軟な診断が可能 ・自社内でノウハウが蓄積できる	・人材の確保や業務フロー/ルール整備が必要 ・高度な攻撃手法への対応が難しい場合がある

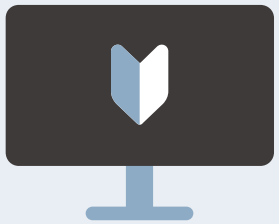
それを解決するのが AeyeScan です！

AeyeScanとは？

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。

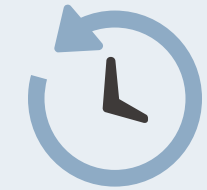


AeyeScanが選ばれている理由



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。

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

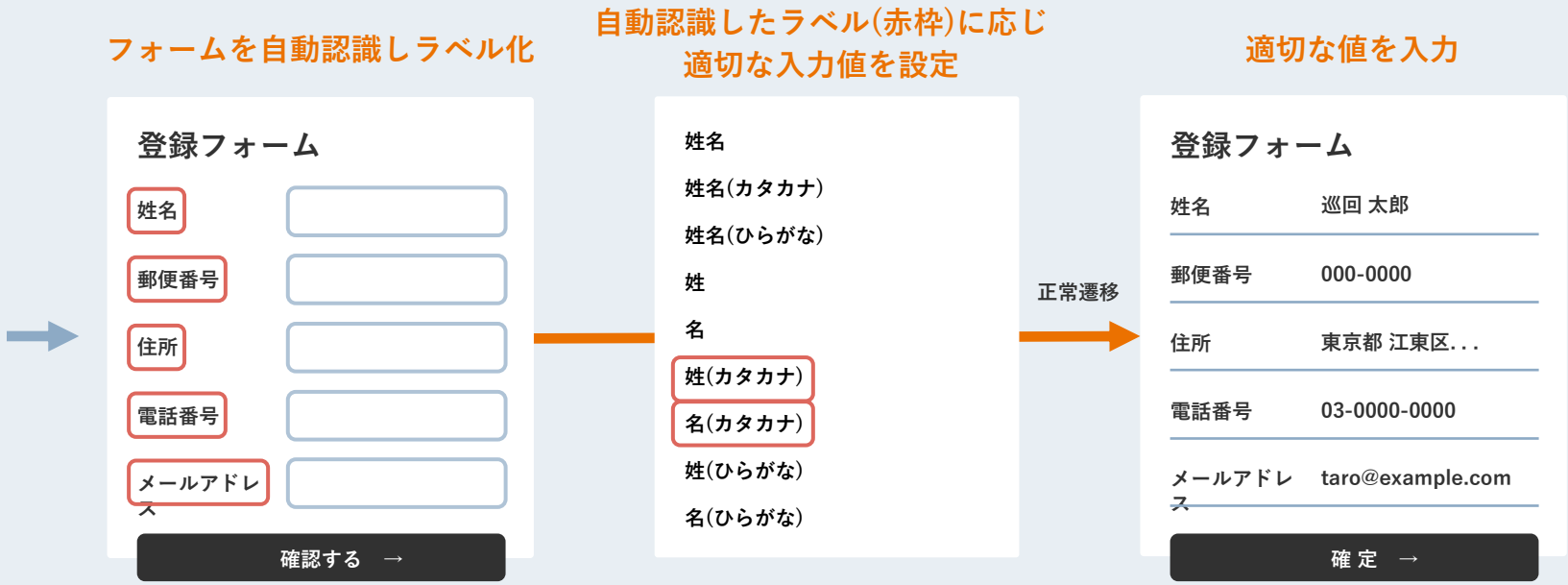
フォーム入力は正しい値を入力する必要がある。
間違えると、**入力エラーとなり遷移できず診断が進まない…**

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



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

OHSAWA 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
JARMeC 日本動物高度医療センター
HITOWA GROUP
BOOK・OFF
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
エアアドエムネット株式会社
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 KDDI Agile Development Center
circlace
さくら情報システム
SUNDAY SYSTEMS
CEC
GA TECHNOLOGIES
Simplex Inc.
777WORKS
SOFT CREATE
SOLTEC
高千穂交易株式会社
TDI
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
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
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

セキュリティベンダーにも選ばれています

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）

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

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

×

プロが認める品質・精度

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

AeyeSecurityLab

方針策定・ルール整備に向け、運用面のアドバイスも行っています

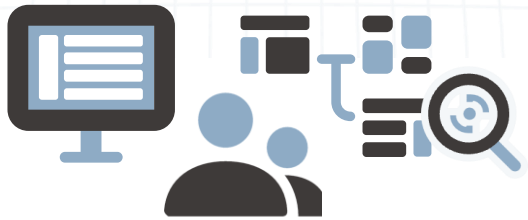
STEP 1 ：使える

（目安）　1～3カ月目

- 操作学習支援（Webセミナー）
- AeyeScanスタートガイド

STEP 2 ：運用できる

3～6カ月目



- AeyeScan運用検討のご支援
- 他社運用事例のご紹介

STEP 3 ：成果を出す

6～9カ月目

- 全社利用・G会社展開のご支援
- 診断プロセス全体設計のご支援

- キックオフ＆定期ミーティング（AeyeScan導入計画の策定と、進捗に応じた各種ご相談・ご支援）
- テクニカルサポート窓口(メール対応) ／ FAQ (サポートポータル)

※本資料に記載の内容は現時点の最新情報であり、今後変更となる可能性があります。予めご了承ください。

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

会社概要

商号	株式会社 エーアイセキュリティラボ	
役員	代表取締役社長	青木 歩
	取締役副社長	安西 真人
	取締役	杉山 俊春　角田 茜
	執行役員 CTO	浅井 健
	執行役員	関根 鉄平
事業内容	情報セキュリティ関連事業（調査・コンサルティング） セキュリティ診断クラウドサービス「AeyeScan」提供	
設立	2019年4月	
拠点	東京都千代田区神田錦町2-2-1 KANDA SQUARE 11F WeWork内	
資本金	1億円	
社員数	57名	
Webサイト	https://www.aeyesec.jp/	
取得認証	情報セキュリティマネジメントシステム（ISMS） ISMSクラウドセキュリティ認証（ISO27017） 情報セキュリティサービス基準適合サービスリスト	

AeyeSecurityLab

セキュリティに
「あらたな答え」を提供し続ける
プロ集団

IS 752963 / ISO 27001

CLOUD 790050 / ISO 27017

023-0026-20

セキュリティに、確かな答えを。