「義務化」時代の新常識！

人手不足でも定期診断を実現する自動化ツールの選び方

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

脆弱性対策の「義務化」、すでに対応済みですか？

2025年3月4日改訂のガイドラインに基づき、EC加盟店の脆弱性対策が義務付けられました。

2. 主な改訂内容

EC加盟店の取り組み

商品・サービス・金額等が掲載され
消費者が閲覧するWebサイトや
LPなどのWebページも対象

クレジットカード情報保護対策

EC加盟店は、これまで実施してきたセキュリティ対策に加え、システムやWebサイトの脆弱性対策を実施する。

カード情報を保持していなくても、脆弱性対策の不備によるカード情報漏えい事案が発生していることから、
ECサイトだけでなく、Webサイトへの「脆弱性対策」の実施が指針対策に追加された。

参考：https://www.meti.go.jp/press/2024/03/20250305002/20250305002.html

なぜ「義務化」への対応は難しいのか？

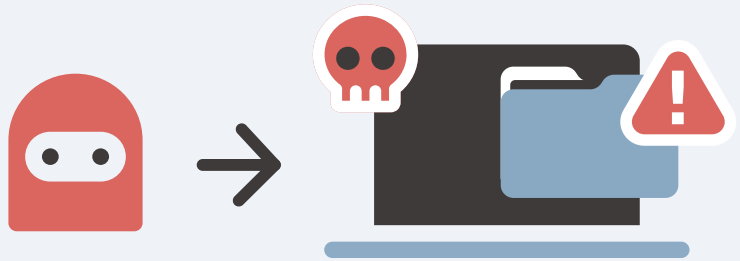
DXの進展やサプライチェーンリスクの拡大により、
企業に求められるセキュリティ対策は高度化・複雑化している

- デジタルサービスの増加により、Web開発そのものが増加
- クラウド、SaaS、APIの活用が進み、システムが複雑化
- 企業規模に関わらずサプライチェーン全体でセキュリティ対策が必須
- アジャイル開発やDevOpsの普及により、リリースサイクルが短縮
- 対応を担うセキュリティ人材が社内にいない

システムの複雑化と高速化が進むなか
人手だけで「義務化」に対応するのは現実的ではありません。

そもそも、脆弱性診断（セキュリティ診断）とは？

脆弱性を突いた攻撃を受けた際に、被害につながる可能性がないか検証すること



システムやアプリケーションに潜む
脆弱性を放置していると、
サイバー攻撃を受けて企業の機密情報や
個人情報が漏えいする危険性が高まる。

脆弱性診断は、Webサイト・サーバ・ネットワークに実施する必要がある。
中でも頻繁に改修がなされ、攻撃対象として狙われやすいWebサイトには定期的な診断が必要。

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

コストとスピードを両立なら
「ハイブリッド」あるいは「内製（自社実施）」がオススメ

AeyeSecurityLab

「ハイブリッド」や「内製」成功のカギは「ツールの活用」にあります

しかし、いざ導入を検討すると、多くの方がその「選定」の難しさに直面します。

多様な診断ツールが存在

特徴が異なる多様なツールがあるものの、専門分野なので、違いの把握が難しい

自社のニーズとの合致が重要

他社にとっての正解が自社にとっての正解とは言い切れない面も

運用を見据えた選定が必要

せっかく導入しても、日々の運用に負荷がかかるとかえってリスクに

脆弱性診断ツール選定時によく検討されるポイント

コスト

ツールの価格は
いくらか

操作性
（工数）

設定や、スキャン実施
からレポート出力までに
どのぐらい時間が
かかるか

診断項目

診断したい項目を
網羅できるか

精度
（誤検知の少なさ）

適切な診断結果を、
安定して得られるか

最近では無料ツールも登場しており、導入を検討したことがある方もいるのでは…？

コストを抑えて導入したとしても、実際に運用するといくつかの課題が…

コスト優先でツールを導入した際に起こりがちな課題

コスト

操作性
(工数)

・設定や準備に時間がかかる
・レポーティングに
手間がかかる

診断項目

ガイドラインに準拠するため
ツールごとの差は少ないが、
自社の基準を満たしているか
確認が必要

精度
(誤検知の少なさ)

・過検知や誤検知が発生
・重複巡回が発生

最も注目したいのは「操作性(工数)」と「精度(誤検知の少なさ)」

脆弱性診断ツールを選ぶ際に、検討すべき観点は４つ

表面的なコストだけでなく、人手をかけずに運用できるよう、
総合的な観点でツールを選ぶことが大切です。

- コスト(ツール価格)
- 操作性(工数)
- 診断項目
- 精度(誤検知の少なさ)

これらの観点を満たす一例として、
AIを活用したクラウド型Webアプリケーション脆弱性診断ツール

AeyeScanをご紹介させてください！

AeyeSecurityLab

クラウド型Webアプリケーション脆弱性診断ツール「AeyeScan」とは

学習コストゼロ！ 専門知識・トレーニング不要で導入できる

1

最短10分で診断開始

専門知識は不要！
SaaS環境なので24時間放置しておけます。

お客様

1 スキャン登録

3 結果レポート

AeyeScan

2 自動診断

Webサイト

3

診断結果レポートも自動生成

開発担当にすぐ渡せるレポートが簡単に出力できます。

2

画面遷移図を自動作成

AeyeScanがサイトを自動巡回、診断すべき画面を抽出して画面遷移図を生成します！

Demonstration

製品デモ

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

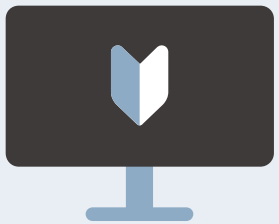
※ 富士キメラ総研調べ「2024 ネットワークセキュリティビジネス調査総覧 市場編」Webアプリケーション脆弱性検査ツール〈クラウド〉2023年度実績
※ITR調べ「ITR Market View：サイバー・セキュリティ対策市場2025」SaaS型Webアプリケーション脆弱性管理市場：ベンダー別売上金額シェア（2022年度実績）

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

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。

AeyeSecurityLab

AeyeScanのポイント

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！

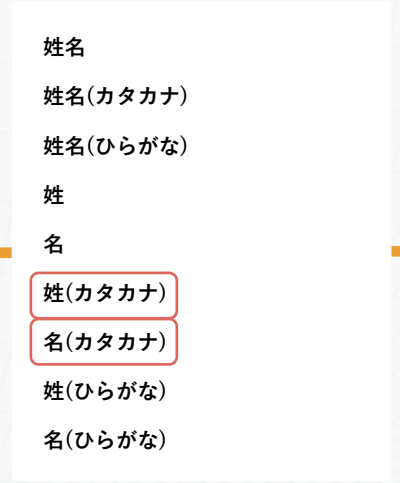
ココがポイント

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

フォームを自動認識しラベル化

自動認識したラベル(赤枠)に応じ
適切な入力値を設定



正常遷移

適切な値を入力

AeyeScanのポイント

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

OWASP アプリケーション
セキュリティ検証標準

IPA 安全なWebサイトの作り方

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、
有識者会議による審査の結果、AeyeScanが選定されました。

AeyeScanのポイント

国内製品ならではの「日本語によるレポート」が自動生成される！

ココがポイント

- どのガイドラインに準拠して検出された項目かがわかる
- どう修正すべきかも記載してあり、そのまま開発者に渡せる
- エグゼクティブサマリも簡単に作成可能

PDF DOC CSV

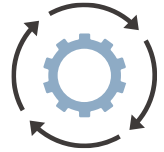
様々な形式でカンタンに
自動生成ができる！

ドメインごとの課金ではなく「定額プラン」での利用も可能

複数のWebサイトを運営していても診断し放題だから…

リリース直前の診断や、
継続的な再診断も
負担なく実施できる

診断を運用サイクルに
組み込みやすく、
チームで取り組める



継続的かつ高頻度な診断により、セキュリティ強化を実現

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
H.O 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
Loyalty Marketing, Inc.

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

エンタメ

イープラス
CAPCOM
とらラボ! TORANOANA LABORATORY

Leverages

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
Classi
COACH A Co.,Ltd.
cybozu
Speee
SecureNavi
DMM Boost
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 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
NHC
Human Interactive Technology Inc.
FUJISOFT
FUJITSU
MACROMILL
MITSUBISHI ELECTRIC 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

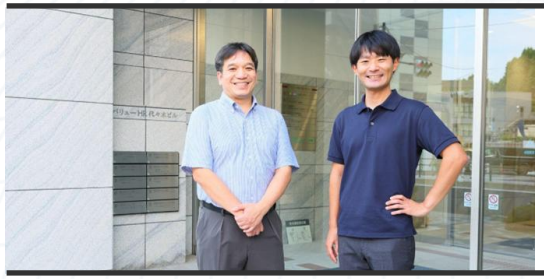
NEC NECセキュリティ
NTT DATA NTTデータ先端技術株式会社
GSX
cybertrust
LAC

社名五十音順（導入いただいた企業様の一部です）

AeyeSecurityLab

導入事例紹介

バリューＨＲ 様



企業名　株式会社バリューＨＲ

事業内容　健康情報のデジタル化サービス・健康管理サービスの提供など

従業員数　680人（2023年12月31日現在）

課題

他社の診断ツールを使っていたが、
多くの時間と工数がかかるほか、
対象範囲をすべてチェックできずにいた

具体的な課題

1. 顧客から求められるセキュリティレベルに応える必要がある
2. 他社ツールでは設定やスキャンに時間がかかり、診断しきれないことも多かった
3. 好きなタイミングでスキャンしたいため、外部委託はできない

機微な個人情報を大量に預かっていることもあり、顧客からも定期的な脆弱性診断の実施状況を問われていた。セキュリティの担保のために他社の診断ツールを導入したものの、時間や工数などの課題が生じ、他のツールを検討することになった。

導入

短時間でスキャンできて使いやすく、
設定も楽なことから導入を決定

導入の背景

1. 以前使っていたツールと比較して設定が簡単
2. スキャン時間が短縮でき、使いやすい
3. OWASP TOP 10に沿って出されるレポートがわかりやすい

普段から付き合いのあるベンダーからの紹介も含め、いくつかの候補を検討する中、短時間でスキャンでき、使いやすいことを重視してAeyeScanを選定。中でも、ユーザーIDやパスワードの仕様を調べて設定する必要がなく、楽だと感じた。

効果

診断にかかる時間・工数が短縮できたほか、
見込み客からのセキュリティに関する質問にも
迅速に回答できるようになった

具体的な効果

1. サービス導入前にセキュリティについて回答することで、営業もしやすくなった
2. 画面遷移図により、自社サービスの構成が把握できるようになった
3. 数日かけても終わらなかった診断が、1日で終わるようになった

AeyeScanの導入で、スケジュールを組んでおけば自動的にスキャンが実施されるようになった。工数や時間が削減できたのはもちろん、導入前にセキュリティ実施状況を伝えられるようになったことで、営業担当者にもメリットが生まれた。

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。

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

AeyeScanにご興味をお持ちいただいた方へ、トライアルをご用意しています

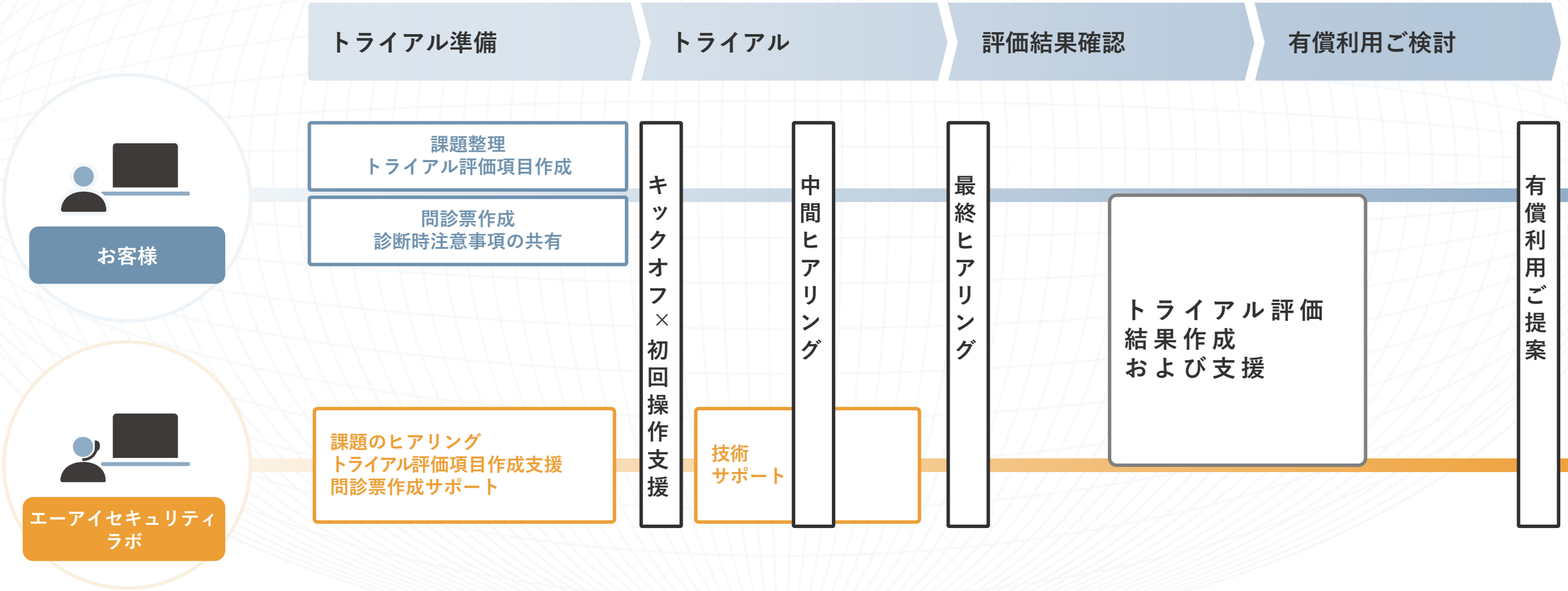
トライアルとは？

「AeyeScanで自社のWebサイトを適切に診断できそうか」を検証いただくための取り組みです。

- いざ導入を決めたものの診断できない箇所があり、すぐに導入できなかったケースがございます。
  →検討初期段階であっても、まずはトライアルをお試しいただくことを推奨しています。
- トライアルでは、操作支援などのサポートも行います。
- トライアル開始に必要なのは以下の3点のみ。お気軽にお申し込みください！
  - 検証するサイトの選定
  - AeyeScanのIPアドレス許可設定
  - 問診表のご一読と社内周知

Businessプランをご検討のお客様向け トライアルスケジュール

キックオフを行った後、弊社で各種サポートを行います。



AeyeScanを実際に操作してみませんか？

お申込みはこちら

アンケート

アンケートにご回答いただいた方へ、
講演資料をプレゼントいたします。
ぜひ、ご協力よろしくお願いいたします！

セキュリティに、確かな答えを。