## なぜ定期的な脆弱性診断が必要なの？

# 知っておきたいWebサービスの

# セキュリティ基礎



AeyeSecurityLab

# 本資料の目的

サイバー攻撃による情報漏えいやサービス停止などの事件が世間を賑わせている昨今。

デジタルサービスがビジネスの主流となる中、複数のWebサービスを運営している企業も増え、
セキュリティ対策の強化は急務となっています。

しかし、専門知識が求められるセキュリティに関しては、

「専門人材が社内にいない」
「そもそも、どんな対策を実施すべきかわからない」
「やるべきことが多すぎて、どこから手をつけてよいかわからない」

といったお悩みをお持ちの企業様も多いのではないでしょうか？

本資料では、Webサービスを提供しているすべての企業様に知っていただきたいセキュリティの基礎から、
セキュリティ対策の中でも定期的・継続的な実施が欠かせない
「脆弱性診断」の運用方法まで、幅広くご紹介します。

ぜひご一読ください。

# なぜ、Webサービスには定期的な脆弱性診断が必要なのか

## (1)Webアプリケーションに潜む脆弱性(不具合やミス)を突いた攻撃が脅威となっている

### 情報漏えい・損失

クレジットカードや
個人情報、機密情報が
漏れたり、重要情報が
破損される

### 改ざん・データ破壊

Webサイトが改ざん
されたり、データベース
の情報が破壊・削除
される

### マルウェア感染

ウイルスや
ランサムウェアなどを
仕込まれ、
不正操作される

### なりすまし

正規ユーザーに
なりすまし、
不正操作や情報搾取が
行われる

**サービス停止や企業の社会的イメージ・信用の損失を招くだけでなく、**
**調査・補償のための経済的損失も…！**

# なぜ、Webサービスには定期的な脆弱性診断が必要なのか

## （2）リリースが増加していることで、新たな脆弱性の混入リスクが高まっている

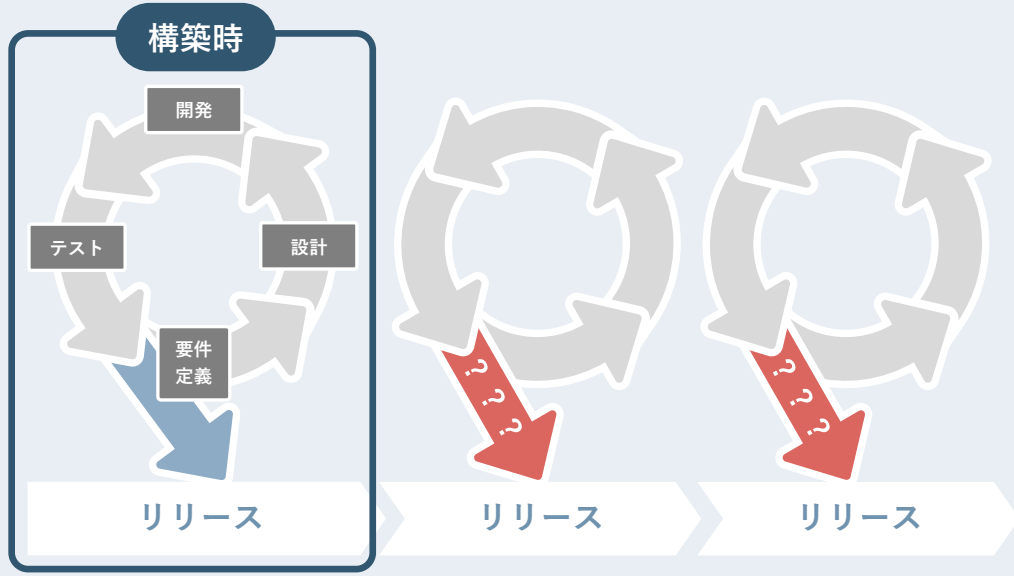
**環境変化**

アジャイルな
開発方式の増加

ノーコード・
ローコードツールの普及

**実態**

構築時の診断のみで、
全てのリリース
タイミングでは
診断できていない




**脆弱性診断のサイクルが適切でないと脆弱性リスクも高まる**

# そもそも、Webサービスに必要なセキュリティ対策とは

IPAによる「安全なウェブサイトの運用管理に向けての20ヶ条」に、
Webサイトを安全に運用するために必要なセキュリティ対策の指針が掲げられている。

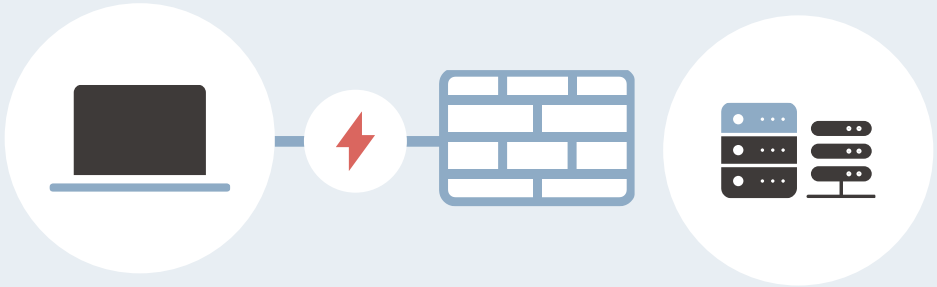
## Webサイトのセキュリティ対策のチェックポイント

**CHECK 01**

Webアプリケーションの
セキュリティ対策

**CHECK 02**

Webアプリケーションが稼働
しているウェブサーバの
セキュリティ対策



**CHECK 03**

Webサーバが設置されている
ネットワーク(ルータやファイア
ウォール)のセキュリティ対策

**CHECK 04**

その他のセキュリティ対策

引用：安全なウェブサイトの運用管理に向けての20ヶ条 ～セキュリティ対策のチェックポイント～（IPA）

AeyeSecurityLab

# Webサイトに必要なセキュリティ対策20ケ条

| Webアプリケーションのセキュリティ対策 | Webサーバのセキュリティ対策 | ネットワークのセキュリティ対策 | その他のセキュリティ対策 |
|---|---|---|---|
| ① ファイルの公開設定 | ⑨ バージョンアップ | ⑮ 不要な通信の遮断 | ⑲ クラウドサービスのセキュリティ対策 |
| ② Webページの公開設定 | ⑩ 不要なサービス・アプリケーションの停止 | ⑯ 通信のフィルタリング | |
| ③ 脆弱性への対策 | ⑪ 不要なアカウントの削除 | ⑰ 不正な通信の検知・遮断 | ⑳ 脆弱性診断 |
| ④ ソフトウェアの脆弱性対策 | ⑫ 安全なパスワードの設定 | ⑱ ログ管理 | |
| ⑤ エラーメッセージ | ⑬ アクセス制御 | | |
| ⑥ ログ管理 | ⑭ ログ管理 | | |
| ⑦ 暗号化 | | | |
| ⑧ 不正ログインへの対策 | | | |

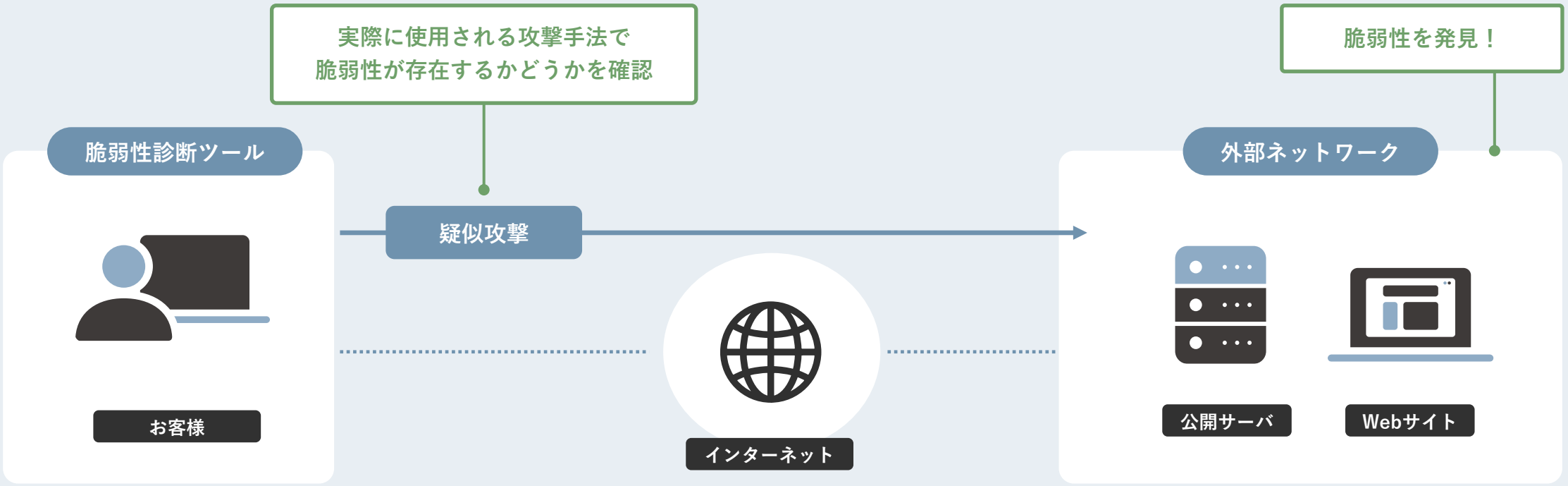
「安全なウェブサイトの運用管理に向けての20ヶ条」で提示されているセキュリティ対策のほとんどが、

**脆弱性診断により問題発見できる！**

引用：安全なウェブサイトの運用管理に向けての20ヶ条 ～セキュリティ対策のチェックポイント～（IPA）

# 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



# 定期的に脆弱性診断を実施するにはどうすればよい？

## 構築時

### 設計・開発時に
### 可能な限り脆弱性を解消


IPAによる「安全なウェブサイトの作り方」を参考にすることで、
自社開発でも外部委託でも同じ基準で
セキュリティ対策が可能

## 運営時

### 運用中は定期診断を実施しつつ、リリースや機能改修時も
### 必ず脆弱性診断を行う

年に1回の
定期診断

＋

リリースや
機能改修時

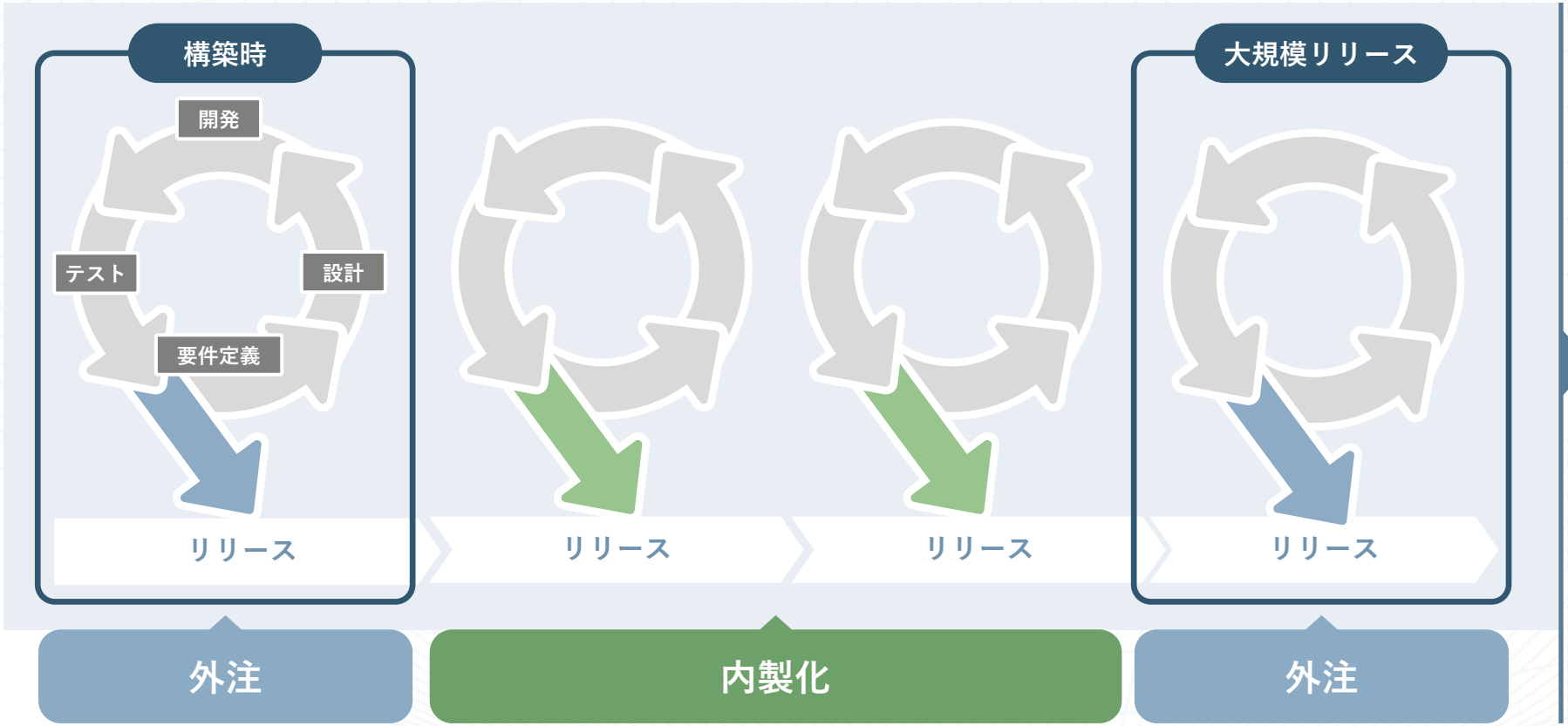
**Webサイトで扱う情報の重要度を踏まえて頻度の検討を！**

引用：安全なウェブサイトの作り方（IPA）

AeyeSecurityLab

# そんなに頻繁に脆弱性診断を外注していたらコストが…

そこでおすすめしたいのが、脆弱性診断を外注するだけでなく、
社内でも実施するハイブリッド型の運用。




大規模リリースは
外部に任せ、日々の
小さな更新は社内で。

状況に応じた
診断体制で、継続的な
セキュリティを実現。

# 専門家でもないのに、脆弱性診断を自分たちでできるの？

## 誰でも簡単に、プロさながらの脆弱性診断ができるツールの導入がおすすめ！

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

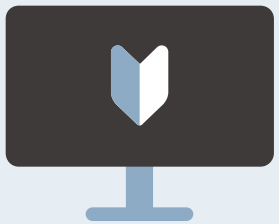
※ 富士キメラ総研調べ「2024 ネットワークセキュリティビジネス調査総覧 市場編」Webアプリケーション脆弱性検査ツール〈クラウド〉2023年度実績
※ITR調べ「ITR Market View：サイバー・セキュリティ対策市場2025」SaaS型Webアプリケーション脆弱性管理市場：ベンダー別売上金額シェア（2023年度実績）

## 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

# 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。

# そもそもAeyeScanとは？

AI・RPAの活用により、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。
自動巡回に優れており、人手をかけずに診断が可能。

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！

# 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

## バトンズ 様


企業名　株式会社バトンズ

事業内容　M&A総合プラットフォームの企画・開発・運用

従業員数　122名（2025年2月時点）

### 課題

M&A・事業承継に関わる機密情報を
万全のセキュリティで守るため、
診断の高頻度化が必要に

#### 具体的な課題

1. 外部ベンダーによる脆弱性診断はコストがかかる
2. 診断範囲の調整も入ることから、準備にかなりの工数を要する

プラットフォームの企画・開発・運用を行う中で、企業の極めて重要な機密事項を取り扱うことから、診断頻度を見直すことに。限られた予算やリソースの中で高頻度化を目指すべく、内製化を検討。

### 導入

外部の専門家に依頼するときと
同レベルの診断クオリティを評価

#### 導入の背景

1. 業界標準のセキュリティ基準に準拠している
2. 自動巡回の精度が他社ツールより高い
3. 自動で画面遷移図が生成され、非エンジニアでもわかりやすい

経産省が示すセキュリティ基準や、OWASPアプリケーションセキュリティ検証標準を満たしている上、自動巡回の精度が高いことからAeyeScanを採用。効率的に診断が実施できるわかりやすさも評価。

### 効果

週1の定期診断と
新機能リリース時の即日診断を実現し、
サービスへの信頼度も向上

#### 具体的な効果

1. 診断の高頻度化を実現
2. 脆弱性を検知した場合も即座に対応できるようになった
3. お客さまにサービスの安全性を客観的に示せるようになった

外注時は年に1回の診断だったが、毎週土日の定期診断と、新機能リリース時の即日診断が可能に。金融機関などのお客様にセキュリティ対策の実施状況も説明しやすくなり、サービスへの信頼度向上を実感。

# 導入事例紹介

## ミズノ 様


企業名　ミズノ株式会社

事業内容　スポーツ用品の開発・販売ほか

従業員数　3,584人（2024年3月31日現在）

### 課題

国内だけでも約20 Webサイトを運営する中、
定期的な脆弱性診断ができていなかった

#### 具体的な課題

1. サイト立ち上げ時や大規模改修時だけしか診断ができていない
2. 外部ベンダーによる脆弱性診断だと多額のコストがかかる
3. 内部の人材のスキル不足・業務負荷が高くなる

グローバル全体でセキュリティポリシーを見直し、その中に定期的な脆弱性対策を含めたものの、外部ベンダーによる脆弱性診断だとコストがかかる。内製化を検討するもスキル不足や業務過多といった課題があることから、自分たちでも使える診断ツールの導入を検討。

### 導入

定額で複数サイトに外部ベンダーによる
脆弱性診断と変わらないクオリティの診断が
できると評価

#### 導入の背景

1. 専門知識を持たなくても簡単に操作できる
2. サイト数に比例して費用が増加しない
3. 外部ベンダーによる脆弱性診断と同等の品質で診断できる

AeyeScanのトライアルを行い、簡単に操作できることを実感。また、同一サイトに対して、外部ベンダーによる脆弱性診断による診断とAeyeScanによるスキャンを並行して行いレポートを比較。AeyeScanの方が同レベル以上・検知項目が多かったことから、導入を決めた。

### 効果

定期的な診断が可能な体制が整った。
時間短縮により、
診断後の対策、チェックもスムーズに

#### 具体的な効果

1. 内製化により、診断にかかる時間が数ヶ月単位から数週間に短縮
2. 診断、対策、チェックの運用がきれいに回せている
3. 開発ベンダーとのコミュニケーションもスムーズになった

外部ベンダーによる脆弱性診断では脆弱性への対応も含めて数ヶ月単位の時間がかかっていたが、数週間で診断を終えてすばやく対策できるようになった。レポートに具体的な修正方針も示されるため、開発ベンダーとのコミュニケーションもとれ、対策もスムーズになった。

# 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 | 田中 大介 |
| 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）<br>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 | | |
| 従業員数 | 43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）<br>ISMSクラウドセキュリティ認証（ISO27017）<br>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。