AeyeSecurityLab

# サイバー攻撃から自社サイトを守る

# 失敗しない 脆弱性診断のススメ

# Webサイトの脆弱性診断、こんな風に考えていませんか？

立ち上げ時に脆弱性診断を
したので大丈夫。
それ以降行っていない。

コストと時間がかかるので、
画面を絞って
脆弱性診断をしている。

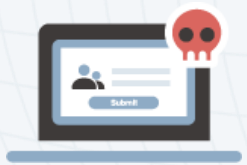
クレジットカード番号は
非保持なので、脆弱性診断は
していない。

ひとつでも当てはまったら危険！
今すぐ脆弱性診断の見直しと改善をおすすめします！

# Webサイトの脆弱性診断、こんな風に考えていませんか？

### ✕ 立ち上げ時に脆弱性診断をしたので大丈夫。それ以降行っていない。

サイバー攻撃の新たな手法、
新たな脆弱性に対応できていない
可能性があります。



サイバー攻撃は日々進化しています。過去に診断した画面でも、定期的なセキュリティチェックは欠かせません。また、新たにリリースした機能や、既存の改修時にも診断が必要です。

### ✕ コストと時間がかかるので、画面を絞って脆弱性診断をしている。

重要な画面だけ診断すればよかったのは
昔のこと。今は全ての画面が
攻撃対象になり得ます。

あまり使われていない機能であっても、サイバー攻撃の対象になり得る時代。毎年診断していても、重要な画面だけでは不十分です。画面を絞る場合も、対象の見直しが必要です。

### ✕ クレジットカード番号は非保持なので、脆弱性診断はしていない。

クレジットカード番号を取り扱って
いないECサイトであっても、
診断は必要です。

最近では、非保持化を達成した サイトからもカード情報が窃取されている傾向に。カード情報の保持・非保持にかかわらず、定期的な診断・点検と、必要に応じた対策が必要です。

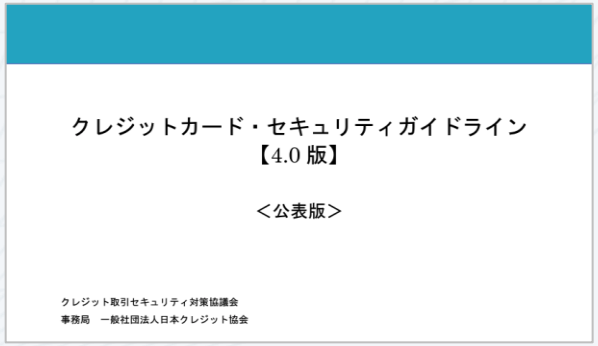
# 進化するサイバー攻撃の手法

## クレジットカード番号非保持化の限界

特にオープンソースにより構築され、適切なアップデートを行わないなど、十分なセキュリティ対策を講じていないECサイトの脆弱性を狙った攻撃が増加。クレジットカード番号等を保持していなくとも、ECサイト自体が改ざんされることで不正ファイルの設置や偽の決済サイトへの誘導が行われ、クレジットカード番号等が流出。


【出典】経済産業省　商務・サービスグループ 商取引監督課 「最近の主な漏洩事案」

上記のような現状を踏まえ、一般社団法人日本クレジット協会による「クレジットカード・セキュリティガイドライン【 4.0版 】 でも、クレジットカード番号の保持・非保持にかかわらず、定期的な点検、および必要に応じた追加対策の導入を推奨。


クレジットカード・セキュリティガイドライン
【4.0 版】

＜公表版＞

クレジット取引セキュリティ対策協議会
事務局　一般社団法人日本クレジット協会

【参考】一般社団法人日本クレジット協会 「クレジットカード・セキュリティガイドライン【4.0版】」

# 進化するサイバー攻撃の手法

## フィッシングのターゲットは30%がEC系ブランド

フィッシング対策協議会による「フィッシングレポート2023」によると、昨今のフィッシングは、基本的にはクレジットカード情報狙いであるが、EC 系ブランドをかたるフィッシングも継続に行われており、その割合は全体の約 30.0%であった。

【出典】フィッシング対策協議会「フィッシングレポート2023」


## 進行する「犯罪のビジネス化」でサイバー攻撃が容易に

IPA（独立行政法人 情報処理推進機構）が毎年発表している「情報セキュリティ10大脅威 2024」に、犯罪のビジネス化（アンダーグラウンドサービス）が2年連続でランクイン。

【出典】IPA（独立行政法人 情報処理推進機構）「情報セキュリティ10大脅威 2024」

AeyeSecurityLab

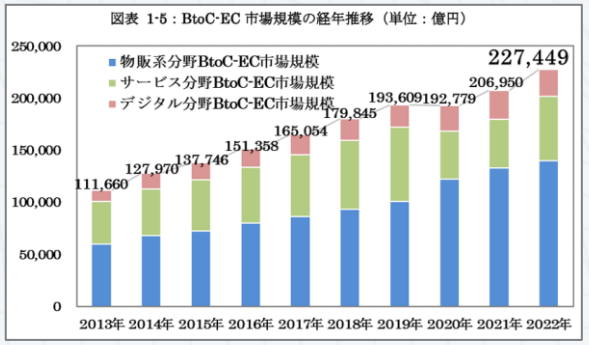
# 数字で見る、脆弱性診断の現状

## EC市場規模の拡大

**BtoC ECの市場規模は拡大傾向。**
**デジタルサービスも増加。**

コロナ禍も影響し、販路の軸がWEBサイトに移行傾向。
それに伴い、脆弱性診断の対象となるデジタルサービスも増加傾向にある。

引用：経済産業省 令和４年度
電子商取引に関する市場調査 報告書

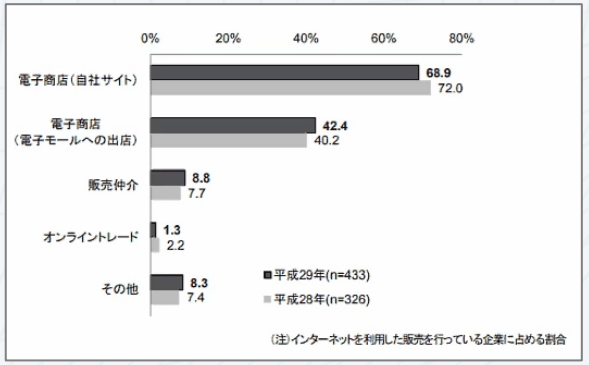



## 自社EC強化の傾向

**約5割の企業が電子商取引を実施。**
**中でもBtoC ECの実施割合は約2割で、自社EC比率は約7割。**

電子商取引を行っている企業の割合は49.0%あり、「消費者への販売」は18.3%を占める。電子商取引に「自社サイト」を利用している企業の割合は68.9%。

引用：総務省「平成29年通信利用動向調査」




**EC市場の拡大により、脆弱性診断数の必要性は増加**

AeyeSecurityLab

# 数字で見る、脆弱性診断の現状

## カード不正利用による被害額の増加

被害額は前年比3割増の437億に。
94%がクレジットカード番号の盗用による被害。

国内のECサイトにおける個人情報とクレジットカード情報の漏えい事故と、
それに伴うクレジットカードの不正利用被害の発生が後を絶たない状況。

PDFはこちら

クレジットカード不正利用の被害額

（単位：億円、%）

| 期　間 | クレジットカード不正利用被害額 | クレジットカード不正利用被害額の内訳 | | | | | |
|---|---|---|---|---|---|---|---|
| | | 偽造カード被害額 | | 番号盗用被害額 | | その他不正利用被害額 | |
| | | 被害額 | 構成比 | 被害額 | 構成比 | 被害額 | 構成比 |
| 2014年(1月～12月) | 114.5 | 19.5 | 17.0% | 67.3 | 58.8% | 27.7 | 24.2% |
| 2015年(1月～12月) | 120.9 | 23.1 | 19.1% | 72.2 | 59.7% | 25.6 | 21.2% |
| 2016年(1月～12月) | 142.0 | 30.6 | 21.6% | 88.9 | 62.6% | 22.5 | 15.8% |
| 2017年(1月～12月) | 236.4 | 31.7 | 13.4% | 176.7 | 74.8% | 28.0 | 11.8% |
| 2018年(1月～12月) | 235.4 | 16.0 | 6.8% | 187.6 | 79.7% | 31.8 | 13.5% |
| 2019年(1月～12月) | 274.1 | 17.8 | 6.5% | 222.9 | 81.3% | 33.4 | 12.2% |
| 2020年(1月～12月) | 253.0 | 8.0 | 3.2% | 223.6 | 88.4% | 21.4 | 8.5% |
| 2021年(1月～12月) | 330.1 | 1.5 | 0.5% | 311.7 | 94.4% | 16.9 | 5.1% |
| （1月～3月） | 73.7 | 0.7 | 0.9% | 68.7 | 93.2% | 4.3 | 5.8% |
| （4月～6月） | 81.9 | 0.3 | 0.4% | 78.1 | 95.4% | 3.5 | 4.2% |
| （7月～9月） | 81.3 | 0.2 | 0.2% | 77.1 | 94.8% | 4.0 | 4.9% |
| （10月～12月） | 93.2 | 0.3 | 0.3% | 87.8 | 94.2% | 5.1 | 5.5% |
| 2022年(1月～12月) | 436.7 | 1.7 | 0.4% | 411.7 | 94.3% | 23.3 | 5.3% |
| （1月～3月） | 100.1 | 0.2 | 0.2% | 94.6 | 94.5% | 5.3 | 5.3% |
| （4月～6月） | 106.2 | 0.2 | 0.2% | 100.6 | 94.7% | 5.4 | 5.1% |
| （7月～9月） | 102.7 | 0.7 | 0.7% | 95.9 | 93.4% | 6.1 | 5.9% |
| （10月～12月） | 127.7 | 0.6 | 0.5% | 120.6 | 94.4% | 6.5 | 5.1% |

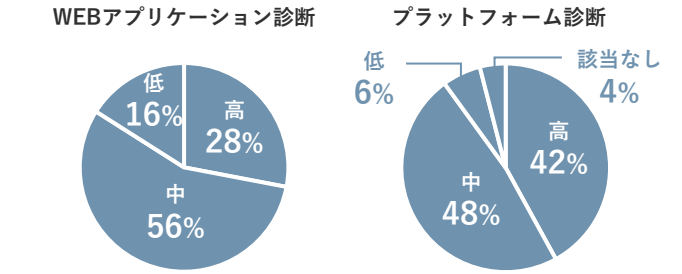
## セキュリティ対策の軽視は危険

ECサイトの52%が、
サイバー攻撃に遭う可能性あり。

IPAが50社のECサイトを対象に脆弱性診断を実施した結果、全体の
52%で危険度の高い脆弱性が検出されるという結果に。

PDFはこちら

診断対象企業50社における危険度の最高位別にみた企業の割合




ECサイトにおけるサイバー攻撃・フィッシング対策は急務

# なぜ、ECサイトが攻撃対象として狙われるのか？

## ECサイトのサイバー被害が増えている背景としては、以下の3つが挙げられます。

### 背景01


ECパッケージやSaaSサービスを使って
**簡単にECサイトを構築**
できるようになった

### 背景02

サイバー被害を受けたECサイトの97%が
**自社構築サイト※に集中**
している

### 背景03

自社構築サイトの中には
**セキュリティ対策を考えていない**、
または、セキュリティ対策に
**十分な費用をかけていない**サイトが多く、
そのようなECサイトを狙った攻撃が増加

※ECパッケージ、または、スクラッチで自社サイトを構築することを、「自社構築サイト」と定義しています。SaaSサービスをカスタマイズせずそのまま利用している場合は除きます。

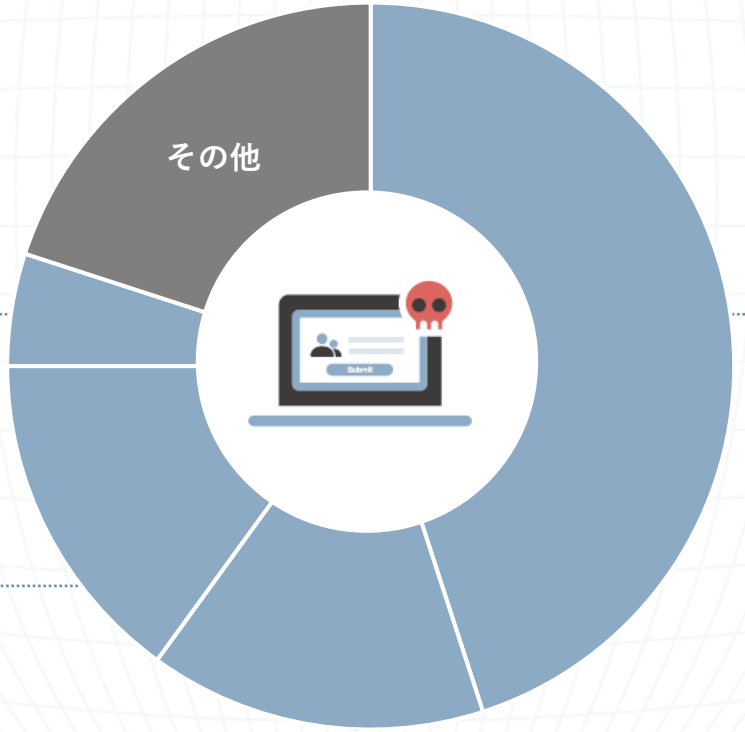
AeyeSecurityLab

# 構築時や運用時にセキュリティ対策が実施できていない理由

ECサイトへの継続的なセキュリティ対策が実施できない理由として、
以下のような意見が挙げられています。

**5%**

前任者が退職し、後任者における
セキュリティ対策の引継ぎや知見の
キャッチアップが不十分であった




**45%**

EC サイトの運営で主に
セキュリティ対策の必要性を認識
している人員がいなかった

**15%**

事業全体の売上高に比較して、EC事
業による売上高の割合が低い(5%以
下)ため、費用を掛けられなかった

**15%**

外部委託先にセキュリティ対策を
依頼しているつもりであったが、
外部委託先では認識されていなかった

AeyeSecurityLab

# ECサイト構築・運用時のセキュリティ要件

## 必須要件だけでも、多くの項目を継続的に実施しなければならない状況。

| 構築時 | | 運用時 | |
|---|---|---|---|
| 設計 | 構築中 / 完成 | 運用開始時 | 運用開始後 / 定期対応 |
| 「安全なウェブサイトの作り方」「セキュリティ実装チェックリスト」の準拠 | サーバ及び管理端末等で利用しているソフトウェアを最新の状態に | | 共通要件 継続対応が必要！ |
| 「クレジットカード・セキュリティガイドライン」の遵守 | 脆弱性診断の実施と、見つかった脆弱性に対する対策 | | |
| サイト利用者情報への不正ログイン対策 | 管理者画面や管理用ソフトウェアへ接続する端末を制限 | 重要なファイルの定期的な差分チェックと、改ざん検知ツールによる監視 | |
| サイト利用者の個人情報に安全管理措置 | 管理者画面や管理用ソフトウェアへ接続する端末のセキュリティ対策 | | |
| ドメイン名の正当性証明とTLSの利用 | | | |

**しかし、需要に対して<u>セキュリティ人材は不足</u>している。**
**外注にも採用にも<u>コストと時間</u>がかかる。**

日本のセキュリティ人材数

480,659(+23.8%)

日本のセキュリティ人材の需要に対する不足数

110,254(+97.6%)

引用：https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf

AeyeSecurityLab

# 脆弱性診断は内製化がおすすめ

セキュリティ対策を見直すにしても、業務負荷やコストの問題はどうしよう？

「クラウド型(SaaS)ツール」で、脆弱性診断を**内製化**するのがおすすめ！

AeyeScan

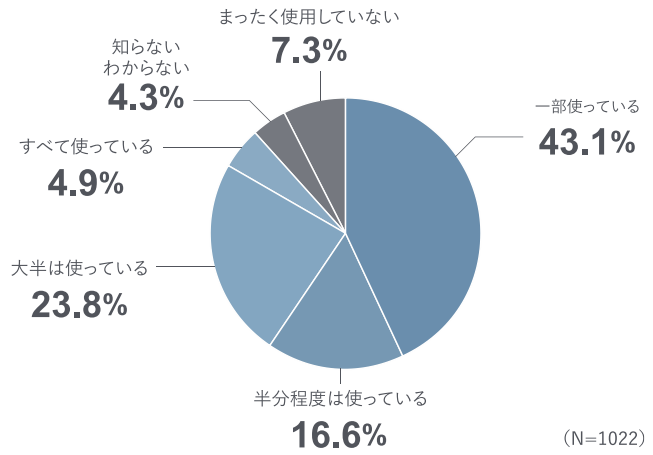
1. **コストダウン**
   脆弱性診断を内製化・効率化することで、コストカットを実現
2. **スピードアップ**
   開発・リリースの高速化にも対応可。開発プロセスに組み込める
3. **トレーニング不要**
   SaaS型のため、導入後たった10分で使え、トレーニングも専任者の採用も不要
4. **専門知識不要**
   サイトを自動巡回して画面を洗い出し、診断対象を抽出してテストシナリオを生成
5. **高精度な診断**
   AI活用により自動巡回の精度が高い。自動でクオリティの高い診断が可能

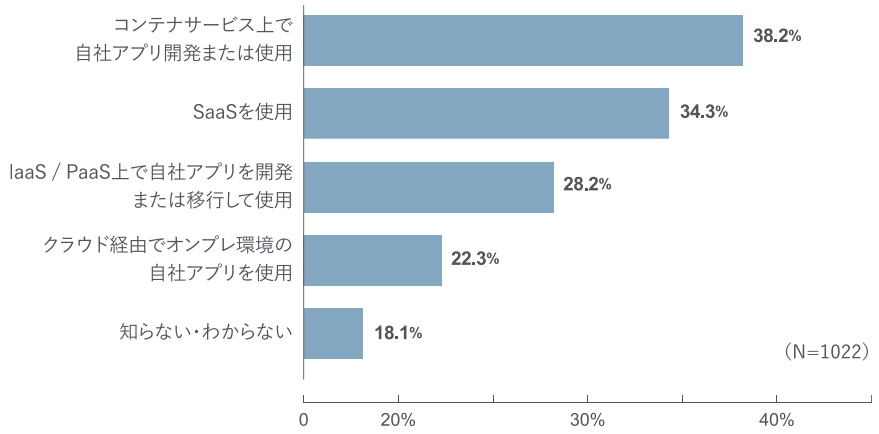
AeyeSecurityLab

# クラウドサービス(SaaS)利用状況

## DX推進の一環としても、クラウドサービス(SaaS)導入は一般的になっている。

### クラウドサービス利用状況（2023年）




半分以上クラウドサービスを利用している比率は
約5割に近づいており、
クラウドサービスの利用は増加している。

コンテナサービス上での開発の比率がトップで、
SaaSの利用が続いており、
IaaS/PaaS上の開発・移行の比率が低くなっている。

出典：株式会社アイ・ティ・アール「クラウド時代のセキュリティ認証・インボイス制度・DXへの取組みー企業IT利活用同行調査2023報告ー

# 導入事例紹介

## タイガー魔法瓶 様


企業名　タイガー魔法瓶株式会社

事業内容　生活用品総合メーカー

従業員数　769人（2023年6月時点）

### 課題

診断を外注していたが、コストと
スケジュール調整が負担になり、内製化を検討

#### 具体的な課題

1. セキュリティ人材の確保が困難
2. 外注コストの膨張
3. 診断調整の負担増

脆弱性診断には専門的なスキルやノウハウが必要となるが、社内での人材確保は難しく、外注せざるを得なかった。1サイトの 診断に数百万円単位のコストがかかる上に、診断実施までの調整コストも膨らんでいた。

### 導入

自動巡回の精度や脆弱性の検知率等で比較。
最も信頼できるAeyeScanに導入決定

#### 導入の背景

1. 脆弱性診断の「内製化」を目指したい
2. 過検知・誤検知が少ない製品を探していた
3. コストを削減したい

自分たちで使いこなせるかを重視しつつ、自動巡回の精度、検知率等を定量的に比較。AeyeScanで特に評価したのは「自動巡回機能」と「診断精度」だが、大幅にコスト削減できる点も導入の決め手。

### 効果

年1回の定期診断を実施。
自動巡回機能で大半の作業を自動化。
大幅な負荷軽減に

#### 具体的な効果

1. 作業の自動化による担当者の負荷軽減
2. セキュリティレベルの担保に有用
3. GUIが使いやすく、教育も容易

「自動巡回機能」により、大半の作業を自動化。直感的に作られたGUIは使いやすく、使い方の共有もしやすい。クラウドサービスならではの、こまめな機能改善も好印象。

AeyeSecurityLab

# 導入事例紹介

## エイチ・アイ・エス 様


企業名　株式会社エイチ・アイ・エス

事業内容　総合旅行会社

従業員数　10,849人（2023年6月時点）

### 課題

セキュリティの内製化が困難。
診断の外注コストを削減したい

#### 具体的な課題

1. 社内からの診断依頼が増え続けていた
2. 診断対象が多く外部委託せざるを得ない
3. 外注による診断コスト増

内製・外製含め100を超えるWebアプリケーションがあり、内部の体制だけでは全ての診断実施に対応できず、一部を外部に委託。コスト削減と体制整備が課題だった。

### 導入

情報処理推進機構（IPA）の検証結果と
「7割以上自動化」という点が決め手

#### 導入の背景

1. 手動の診断では対応が追い付かず自動化を検討していた
2. 自動化できても性能が落ちない製品を探していた

手動作業を伴う診断では対応が困難になり、診断の自動化を検討。AeyeScanは、IPAの検証結果が高評価だったことと、「7割以上の自動化が可能」という点が決め手で導入。

### 効果

診断・レポート作成工数を大幅に削減。
さらなる内製化比率の向上を目指す

#### 具体的な効果

1. 診断の大部分を自動化し工数を削減
2. レポート機能により大幅に時間を短縮
3. リリース前に診断と脆弱性改修が完了

「脆弱性が発覚しても、リリースまでに修正が間に合わない」という悩みも解消され、脆弱性を潰してからアプリをリリースできるように。

AeyeSecurityLab

# 導入事例紹介

## 富士ソフト 様


企業名　富士ソフト株式会社

事業内容　システム開発

従業員数　8,991人（2023年6月時点）

## 課題

セキュア開発ルール＋運用円滑化のため
簡易で低コストの診断方法が必要な状況に

### 具体的な課題

1. セキュア開発対応にばらつきがあった
2. ルール徹底にはコスト増が避けられない
3. 開発競争力の維持にはコスト抑制が必須

セキュア開発に関するルールを策定していたが、各プロジェクトに遵守させるためには簡易かつ低コストで診断できる方法が必要な状況だった。

## 導入

幅広い言語や開発環境に対応しているのが
AeyeScan導入の決め手の1つ

### 導入の背景

1. 簡易かつ低コストな製品を探していた
2. 運用の前提条件は過検知の少なさ
3. 幅広い言語や開発環境への対応が必須

一定のセキュリティベースラインを設けたいという狙いに、AeyeScanが合致。幅広い言語や開発環境に対応しているだけでなく、脆弱性診断の経験がなくても、診断できると感じた。

## 効果

AeyeScanとセキュア開発ルール整備との
両輪でほぼ手放しでの運用が可能に

### 具体的な効果

1. 簡単に使えるのでほぼ手放しで運用可能
2. セキュア開発に関する知識と意識が向上
3. 好きなタイミングでの診断を実現

ルール整備との両輪でAeyeScanを導入した結果、診断未実施のまま納品する状況から脱却。「好きなタイミングで診断をする」という形が整った。

# 導入事例紹介

## ラック 様

企業名　株式会社ラック

事業内容　トータルITソリューションベンダー

従業員数　2,172人（2023年6月時点）

### 課題

診断ニーズの高まりと
Webサイト全体への網羅的な診断要望に
対応しきれなかった

#### 具体的な課題

1. 特定時期に診断依頼が集中してしまう
2. スケジュールやコスト面で顧客要望に応えられないケースが増加
3. 全ページを網羅的に診断したいという要望への対応

専門家が深く丁寧にみるサービスの特性上、全ページを網羅的にチェックしてほしいという要望への対応が難しかった。スケジュールやコストがネックで、顧客の要望に応えられないことも。

### 導入

「AeyeScan」はセキュリティ診断を内製化したい企業から高評価、AeyeScanを活用した「Quick WATCH」のサービス開始

#### 導入の背景

1. 技術評価の依頼を受けて検証を実施
2. 日本製ならではの使いやすさと高品質な結果を評価
3. セキュリティ専門家だけでなく内製化にも利用可能と判断

手軽に使えて自社のセキュリティ診断を内製化し、設計や開発の初期段階からセキュリティを組み込むシフトレフトに取り組みたいと考える企業でも使いこなせると判断。

### 効果

コストや時間、リソースによって
やむを得ず対象外としてきた
ページの診断が可能に

#### 具体的な効果

1. 2021年11月に「Quick WATCH」サービスの提供を開始
2. 自動巡回をで見積コストを大幅削減
3. 急ぎのニーズにも対応可能に

2021年11月に「Quick WATCH」の提供を開始し、網羅性と手厚い支援の両方を提供可能になった。また、人材不足で診断を内製化できなかった企業への提案も可能に。

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
100社以上

※富士キメラ総研調べ「2023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)2022年度実績）
※ITR調べ「ITR Market View：サイバー・セキュリティ対策市場2024」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

# 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
ユーグレナ

### インフラ

HIS
ぱかいぐループ
Suzuyo
NTT東日本
Looop

### 金融

アイフル
JOBPAY
SOMPOひまわり生命
DMM FinTech
Tokyo Century

### 出版メディア

集英社
中日新聞
NIKKEI

### エンタメ

CAPCOM
とらラボ!

### SaaS

estie
エムティーアイ
OZINTERNATIONAL
COACH A Co.,Ltd.
cybozu
JINSOKEN
Schoo
Speee
ZENKIGEN
Direct Sourcing
TAL
TEMONA
NAVITIME
KNOCK ON THE DOOR
BATONZ
VALUE HR
hokan
Money Forward
RUN.EDGE
RVSTA

## SI・IT企業

Rworks
AVANT GROUP
CTC
Infcurion
SB Technology
SBWorks
NTT DATA
NTTビジネスソリューションズ
Globalway
circlace
さくら情報システム
CEC
tdi 情報技術開発株式会社
Simplex Inc.
777WORKS
SOFT CREATE
SOLTEC
電通総研
TOPPAN
JOPS
NHC
Human Interactive Technology inc.
FUJISOFT
FUJITSU
MITSUBISHI ELECTRIC
YONA
リピスト

## セキュリティ企業

NEC
NECセキュリティ
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

# 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 | 31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。