

2024年義務化対応にお悩みの方へ

# ECサイトの脆弱性診断は

## こう解決する



AeyeSecurityLab



# 本資料の目的

経済産業省によるクレジットカード決済システムのセキュリティ対策強化検討会報告書にて、**脆弱性診断を含めたセキュリティ対策の必須化**を、2024年度末までにクレジットカード・セキュリティガイドラインに記載することが求められています。定期的な脆弱性診断の実施が、今後ますます重要になると考えられます。

しかし、対策の必要性は理解していても、具体的な方法がわからない方も多いのではないのでしょうか。また、対策を一度実施すれば良いわけではなく、安全性を保つには、継続的に対策を実施する必要があります。

本資料では、経営者・担当者に向けて、ECサイトの脆弱性診断が義務化となった背景～企業がやるべき対策を、この1冊で学べるようにわかりやすくまとめました。

2024年度の脆弱性診断義務化対応にお悩みの方は、ぜひご一読ください。

# クレジットカード・セキュリティを取り巻く状況

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【5.0版】」において、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。

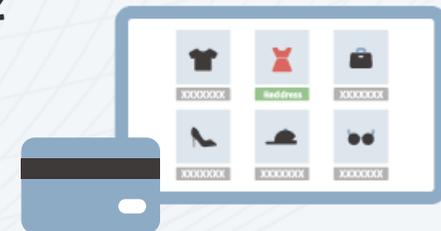
【参考】[一般社団法人日本クレジット協会「クレジットカード・セキュリティガイドライン【5.0版】」](#)

クレジットカード・セキュリティガイドライン  
【5.0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

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」](#)



# 過半数のECサイトがサイバー攻撃の危険に晒されている

2023年のカード不正利用被害額は、前年比2割増の541億円に。  
そのうち93%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。

【出典】日本のクレジット統計 2023年度

## 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%

IPAが50社のECサイトを対象に脆弱性診断を実施したところ、  
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

# クレジットカード情報漏洩からECサイトを守るために



これまで実施が義務付けられてきたクレジットカード情報の非保持化等の対策に加え、  
2024年末までにECサイト自体の脆弱性対策を必須化する方向で検討が進められています。

クレジットカード情報漏えい対策として、定期的な脆弱性診断の実施は今後ますます重要に。

# クレジットカードの情報漏えいを防ぐ3つの対策

## クレジットカード・セキュリティ ガイドラインの順守

対策は、大きく以下の3つ。特にECサイトを運営している事業者の場合、「情報保護対策」と「非対面取引における不正利用対策」の2つがメインとなる。

- 1 情報保護対策
- 2 対面取引における不正利用対策
- 3 非対面取引における不正利用対策

## セキュリティ・チェックリスト の申告

ECサイト事業者が新たに決済代行会社と契約を結ぶ際には、「セキュリティ・チェックリストに基づく対策措置状況申告書」の提出が求められる。

チェックリストにはアクセス制御や脆弱性診断など、顧客情報の漏えいを防ぐために実施すべき対策項目が記載されている。

## 定期的な脆弱性診断の実施

ECサイトにおける脆弱性の有無と危険度をチェックし、危険度の評価と対策提示を受けられるのが脆弱性診断。

ECサイトの脆弱性を利用したサイバー攻撃による不正アクセスを防げるので、クレジットカード情報の漏えい予防に有効。

### 🚨 ココがポイント

ECサイト運用において、定期的な脆弱性診断が占めるウェイトが大きくなっている

# 定期的な脆弱性診断の実施を阻む要因のほとんどは「属人化」

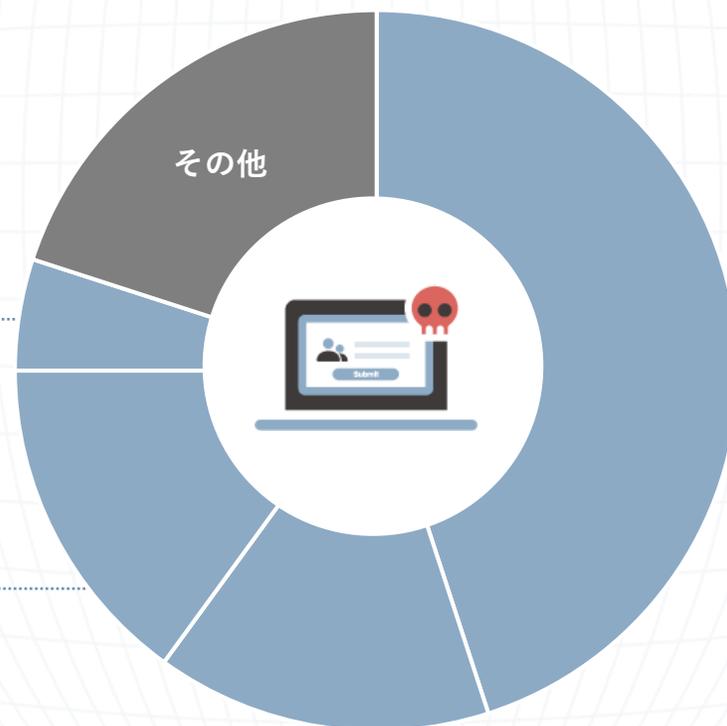
ECサイトへの継続的なセキュリティ対策が実施できない理由として、以下のような意見が挙げられています。

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

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



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%

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

## 定期的な脆弱性診断を継続していくために

脆弱性診断を外部委託する



コストが高い  
自社にノウハウが残らない

脆弱性診断を内製化する



専門人材がない  
どのツールを選べばいいかわからない

コストを抑えられる、誰でもできる脆弱性診断をお探しなら

**AeyeScan** をご紹介させていただきます！

他社はこうやって解決している

## コストを抑えて、時短、簡単、高精度な診断が実現できた

タイガー魔法瓶 様



### 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。

 **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

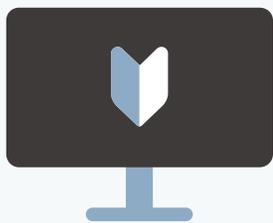
×

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

# | 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。



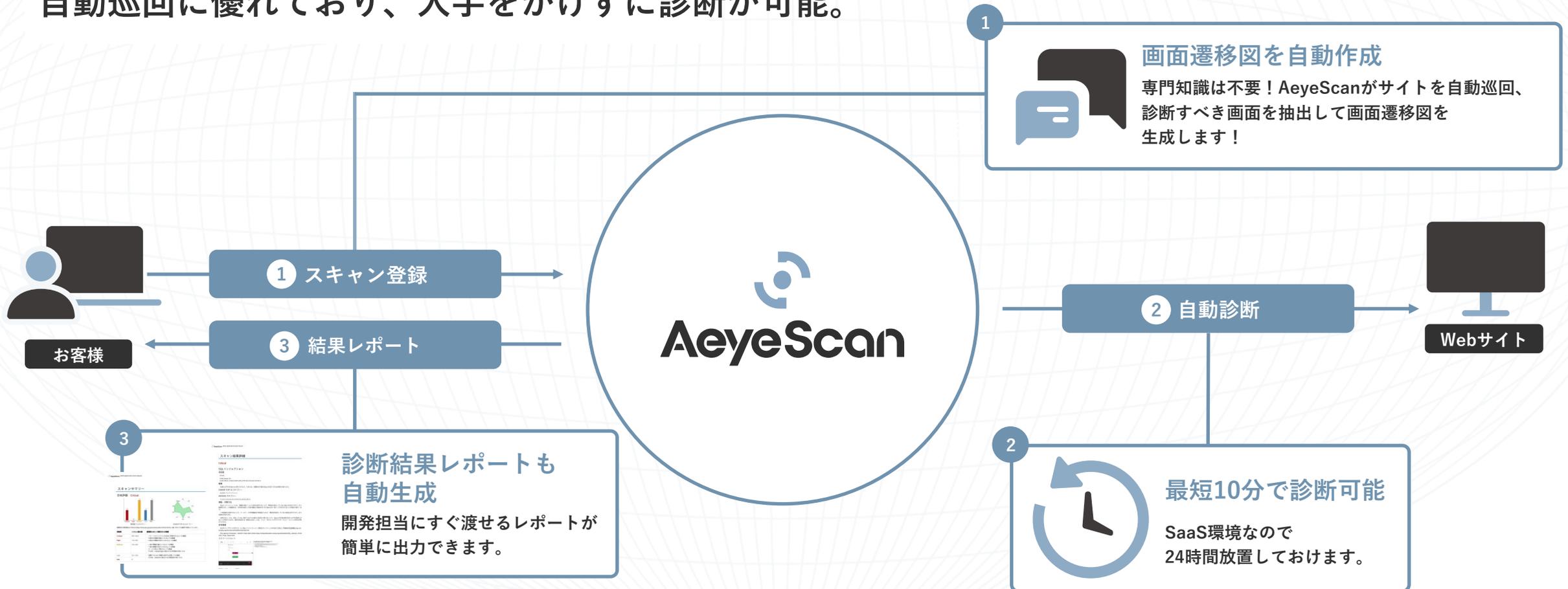
## わかりやすいレポート



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 zu 優れており、人手をかけずに診断が可能。



# 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



### インフラ



### 金融



### 出版メディア



### エンタメ



### SaaS



## SI・IT企業



## セキュリティ企業



# 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か？  
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） 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	33名		
Webサイト	<a href="https://www.aeyesec.jp/">https://www.aeyesec.jp/</a>		
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



**AeyeScan**

セキュリティに、確かな答えを。