2025年3月改定！

クレジットカード・セキュリティガイドラインに新たに追加された“5つの脆弱性対策”

人手とコストをかけずに脆弱性診断を実現する方法

AeyeSecurityLab

本資料の目的

2025年3月、クレジットカード取引に関わる事業者が実施すべきセキュリティ対策を定めた
「クレジットカード・セキュリティガイドライン」が【6.0版】に改訂されました。
主な改訂内容の1つに、 カード情報保護対策として、EC加盟店のシステム及びWebサイトの「脆弱性対策」を実施することが指針対策に追加されています。
つまり、定期的な脆弱性診断の実施が、セキュリティ対策義務の「実務上の指針」として位置づけられたことになります。

しかし、具体的な方法がわからない方も多いのではないでしょうか。
また、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。

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

- クレジットカード番号等の非保持化に対応していても、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する事案が発生している
- オープンソースにより構築されている、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サイトが特に攻撃の対象となっている

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」

IPAが中小企業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

出典：ECサイト構築・運用セキュリティガイドライン

クレジットカードの不正利用被害額は年々増加

2024年のカード不正利用被害額は、
前年比2.6割増の555億円に

↓

そのうち92.5%がクレジットカード番号の
盗用による被害

クレジットカード不正利用被害の発生状況

（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
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%
2022年(1月～12月)	436.7	1.7	0.4%	411.7	94.3%	23.3	5.3%
2023年(1月～12月)	540.9	3.1	0.6%	504.7	93.3%	33.1	6.1
2024年(1月～12月)	**555.0**	5.9	1.1%	513.5	**92.5%**	35.6	6.4%

出典：クレジットカード不正利用被害の発生状況

「クレジットカード・セキュリティガイドライン【 6.0版 】」では
EC加盟店のシステム及びWebサイトにおけるウイルス対策、管理者の権限の管理、デバイス管理等の脆弱性対策の不備を原因としたカード情報漏えいの防止のため、具体的な「脆弱性対策」を講じることを追加

出典：ECサイト構築・運用セキュリティガイドライン

EC加盟店が取るべき対策とは

クレジットカード・セキュリティガイドライン【 6.0版 】において、
「EC 加盟店のシステム及び Web サイトの「脆弱性対策」を講じる。」という記述が追加されました

非保持化

- カード情報保護のための取組として「非保持化」を推進

PCI DSS 準拠

- 業態、システム・ネットワーク構成に適した要求事項に対応

NEW 脆弱性対策

- 既存・新規を問わず、全てのEC加盟店は、5つの具体的な脆弱性対策をすべて実施

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、
EC加盟店のシステム及びWebサイトの「脆弱性対策」の実施が追加指針対策となっています。

クレジットカード・セキュリティガイドライン【 6.0版 】で示された５つの脆弱性対策を
ご紹介するとともに、継続対応のポイントをご説明いたします。

クレジットカードの情報漏えいを防ぐ5つの対策

1. システム管理画面のアクセス制限と管理者のID／パスワード管理
2. データディレクトリの露見に伴う設定不備への対策
3. Webアプリケーションの脆弱性対策
4. マルウェア対策としてのウイルス対策ソフトの導入、運用
5. 悪質な有効性確認、クレジットマスターへの対策

【出展】クレジットカード・セキュリティガイドライン【6.0版】改訂ポイント

クレジットカードの情報漏えいを防ぐ5つの「脆弱性対策」

1 システム管理画面のアクセス制限と管理者のID/パスワード管理

IPアドレスを制限

- システム管理画面のアクセス可能なIPアドレスを制限する。
- IPアドレスを制限できない場合は管理画面にベーシック認証等のアクセス制限を設ける。

2段階認証または多要素認証を採用

- 取得されたアカウントを不正使用されないよう2段階認証又は多要素認証（2要素認証）を採用する。

アカウントロック機能を有効にする

- システム管理画面のログインフォームでは、アカウントロック機能を有効にし、10回以下(PCI DSS ver4.0.1基準)のログイン失敗でアカウントをロックする。

クレジットカードの情報漏えいを防ぐ5つの「脆弱性対策」

2 データディレクトリの露見に伴う設定不備への対策

公開ディレクトリには、重要なファイルを配置しない

- 特定のディレクトリを非公開にする。公開ディレクトリ以外に重要なファイルを配置する。

アップロード可能な拡張子やファイルを制限する

- WebサーバーやWebアプリケーションによりアップロード可能な拡張子やファイルを制限する等の設定を行う。

クレジットカードの情報漏えいを防ぐ5つの「脆弱性対策」

3 Webアプリケーションの脆弱性対策

脆弱性診断又はペネトレーションテストを定期的に実施

- 脆弱性診断又はペネトレーションテストを定期的に実施し、必要な修正対応を行う。

最新のプラグインの使用やソフトウェアのバージョンアップを行う

- SQLインジェクションの脆弱性やクロスサイト・スクリプティングの脆弱性対策として、最新のプラグインの使用やソフトウェアのバージョンアップを行う。

入力フォームの入力値チェック

- Webアプリケーションを開発又はカスタマイズされている場合には、セキュアコーディング済みであるか、ソースコードレビューを行い確認する。その際は、入力フォームの入力値チェックも行う。

クレジットカードの情報漏えいを防ぐ5つの対策

4 マルウェア対策としてのウイルス対策ソフトの導入、運用

マルウェア検知/除去などの対策としてウイルス対策ソフトを導入して、
シグネチャーの更新や定期的なフルスキャンなどを行う。

クレジットカードの情報漏えいを防ぐ5つの「脆弱性対策」

5 悪質な有効性確認、クレジットマスターへの対策

悪質な有効性確認、クレジットマスターに対して、「セキュリティ対策導入ガイド【附属文書20】」別紙a「1.脆弱性対策」⑤に記載の対策を1つ以上実施する。

不審なIPアドレスからのアクセス制限

- 「不審なIPアドレスからのアクセス制限」を行う。
- 特に海外からの攻撃が非常に多いため、海外からのアクセスが不要な場合は遮断を行う。

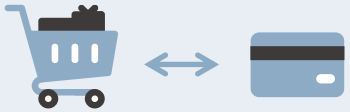
有効なカード会員データの漏えい対策

- 同一アカウントからの入力制限を行う。
- オーソリ拒否時に、エラー内容が分からないようにエラー内容を非表示にする。

本人認証

- EMV3-Dセキュアや SMS通知など本人認証ができる対策を行う。

有効性確認の回数制限



- 有効性確認の回数制限を設けるなどの対策を行う。

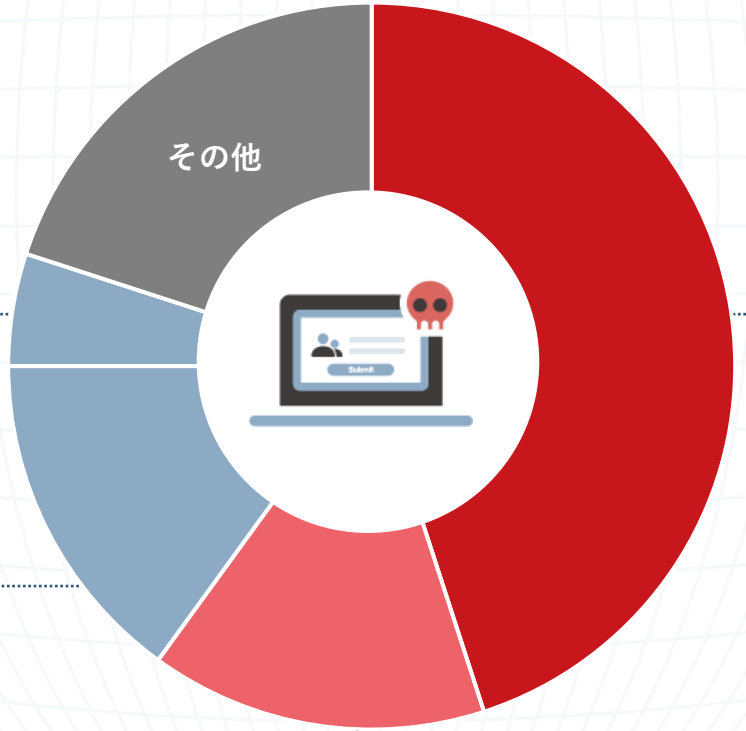
【出展】EC加盟店におけるセキュリティ対策一覧1.0版（附属文書20 別紙a）

定期的な脆弱性診断を阻む要因のほとんどは「人材不足」と「コスト」

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%

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

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**

出典：ECサイト構築・運用セキュリティガイドライン

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

専門人材がいない

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をご紹介させてください！

他社はこうやって解決している　タイガー魔法瓶 様

コストを抑えて、時短、簡単、高精度な診断が実現できた

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。

他社はこうやって解決している　テモナ 様

AeyeScanへのツール移行で診断の実行時間が短縮。社内で高頻度に診断できる体制も確立

課題

従来使っていた診断ツールでは
想定以上の時間を要することがあり、
リリーススケジュール全体に影響が出ていた

具体的な課題

1. 他社の診断ツールはシナリオ登録にも診断実行自体にも時間がかかる
2. 自社のセキュリティ基準上、診断の質を落とすことや、診断せずにリリースすることはできない
3. 脆弱性診断が、リリースサイクル短縮化のボトルネックとなっていた

自社で定めるセキュリティ基準を満たすため、定期的に脆弱性診断を実施していた。その際、診断全体で時間がかかり、リリースサイクルを短縮化できないという課題があった。そのため高精度な診断をスピーディーに実現するために、ツールの乗り換えを検討し始めた。

導入

診断時間や工数はもちろん、
レポートのわかりやすさや
ドメイン登録数が無制限であることが決め手に

導入の背景

1. トライアルを実施し、AeyeScanであれば診断の質を落とさずに工数を大きく削減できると判断
2. そのままエンジニアに共有できるほど詳細なレポートが魅力
3. ドメイン登録可能数が無制限のため、診断対象が多いテモナには費用対効果が高い

最初に40社ほどリストアップした中から、3社に絞って同じページを試験して違いを比較。時間や工数の他に、出力されるレポートの内容や料金体系などさまざまなポイントからAeyeScanを採用。レポートは検出された脆弱性の項目名だけでなく、対応方法まで書かれていることが魅力だった。

効果

診断時間の大幅な短縮に成功し、
高頻度で診断できるようになった。
クラウド型ならではのメリットも享受

具体的な効果

1. 平均4、5日かかっていたプロダクトの診断が、2、3日でできるようになった
2. マイナーアップデートの際も気軽に診断できるようになり、診断数は全体で3倍に増えた
3. クラウド型なのでアップデートの手間もかからず、社内レクチャーも1、2時間で可能に

診断時間が大幅に短縮できたことで、より頻繁に診断できるようになり、セキュリティリスクの軽減させることができている。また、以前のツールはオンプレ型だったためPCのセッティング等が引き継ぎのボトルネックになっていたが、その手間がかからなくなったことも大きい。

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「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）

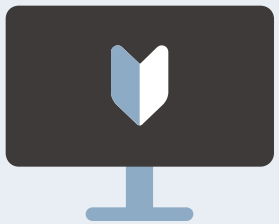
プロが認める品質・精度 ＋ ブラウザ上での直感的な操作

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

AeyeSecurityLab

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

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

人材・教育

HSAWA DRIVING SCHOOL / 河合塾 / Junion / JINSOKEN / ZENKIGEN / Direct Sourcing / PERSOL / Leverages / workport

インフラ

EPARK / AIRE / HIS / H2O RETAILING / NTT EAST / odakyu / 近鉄情報システム株式会社 / 東急 / 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 / HITOWA GROUP / 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 / estie / エアアドエムマット株式会社 / 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 / 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 / JAST / PCNET 株式会社パシフィックネット / Human Interactive Technology inc. / FUJISOFT / FUJITSU / MACROMILL / 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 株式会社NTTデータ先端技術 / GSX GLOBAL SECURITY EXPERTS / 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
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） クラウド型Web診断サービス「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	55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。