

---

貴社のECサイトは大丈夫？

**脆弱性対策** **義務化**

対応度チェックシート

---

# EC加盟店を対象とした脆弱性診断は、ついに「義務化」がスタート

2025年3月4日、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」が改訂。

EC 加盟店のシステム及び Web サイトへの「脆弱性対策」が指針に追加された。

## 2. 主な改訂内容

### EC加盟店の取り組み

#### 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。

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

# ECサイトのセキュリティ対策実施状況報告書の提出が必要

この改訂に伴い、EC 加盟店には、クレジットカード保持／非保持に関わらず、**「ECサイトのセキュリティ対策実施状況申告書」**の提出が求められる。

## 実施状況報告が必要なセキュリティ対策

### 脆弱性対策

全5項目(小分類では17項目)。  
すべて導入されていることが  
求められている。

カード会社・PSPによる  
加盟店調査が年1回あるため、  
継続対応が必要。

### 不正ログイン対策

9つある推奨対策のうち、  
どれか1つ以上対応していればよい。

不審なIPアドレスからのアクセス制  
御(WAF)や、ログイン情報変更時  
のメール通知などの一般的な内容。  
年1回調査あり。

### EMV 3-Dセキュア

すでに対応済みのサイトがほとんど。

クレジットカード・セキュリティガ  
イドライン[5.0版]には、「2025年3  
月末時点でEC利用会員ベースで  
80%の登録率を目指す」と記載。

要件が厳しい脆弱性対策。貴社のECサイトが満たしているかチェック！

チェックシート

# 脆弱性対策の対応状況を、項目ごとにチェック！

	対策項目	対策詳細	対応	チェック欄	備考	AeyeScan 対応状況
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アドレス制限もしくはベーシック制限	両方またはいずれか必須		対応状況を容易に確認可能	-
		推測困難なログインURL及びID/パスワードの設定とadminフォルダ削除			推測されやすいものになっていないか、専門的なチェックが必要	○
		2段階認証	いずれか必須		対応状況を容易に確認可能	-
		多要素認証(2要素認証)				-
		ログイン試行回数の制限(10回)	必須			-
②	サイト設定の不備対策	特定ディレクトリの非公開	必須		意図しないディレクトリの露出がないか、専門的なチェックが必要	○
		アップロード可能な拡張子・ファイルの制限	必須		不正なファイルのアップロードができないように制御されているか、専門的なチェックが必要	○
③	脆弱性の確認	脆弱性診断	いずれか必須		脆弱性診断ツールなどによる専門的なチェックが必要	○
		ペネトレーションテスト			攻撃シナリオに基づく専門的なチェックが必要	-
③-2	SQLインジェクション/ クロスサイト・スクリプティング対策	最新プラグインの使用/ソフトウェアのバージョンアップ	必須		既知の脆弱性がないソフトウェアやプラグインを利用しているか、定期的なチェックが必要	○
		ソースコードレビューによるセキュアコーディング有無の確認	必須		入力フォームの入力値チェックを中心に、専門的なレビューが必要	※
④	マルウェア対策	ウィルス対策ソフト導入と定期的な更新・フルスキャン	必須		ウィルス対策ソフトの導入および定期的な更新・フルスキャンができていれば、対応済と判断して良い	-
⑤	悪質な有効性確認、クレジットマスター対策	不審なIPアドレスからのアクセス制限	いずれか必須		カード情報の有効性を確認する際にEMV 3-Dセキュアが適用されていれば、対応済と判断して良い	-
		有効なカード会員データの漏えい対策				-
		本人認証				-
		有効性確認の回数制限				-

AeyeScanなら、専門的なチェックを必要とする対策にも対応

※EC加盟店におけるセキュリティ対策一覧 1.0版に例示されている、入力フォームの入力値を利用したSQLインジェクション・クロスサイト・スクリプティング対策であれば、AeyeScanで対応可能