【ZEUS】EC サイトのセキュリティ対策実施状況報告書_回答フォーム設問内容一覧

【１】脆弱性対策

次の①～⑤について現状の対応状況を回答してください。

原則、全項目対応している必要があります。「対応していない」を選択された場合、対応完了後改めてご報告頂く必要がございます。

※対策の詳細は、以下資料をご参照ください。
1.EC 加盟店におけるセキュリティ対策導入ガイド【附属文書 20】　※P5～8 をご参照ください。
2.EC 加盟店におけるセキュリティ対策導入ガイド【附属文書 20】補足資料　※P12～24 をご参照ください。

※回答内容が不明な場合はシステム担当者様または外注のシステム会社様にご確認ください。

① システム管理画面のアクセス制限と管理者の ID/PW 管理

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。
取得されたアカウントを不正使用されないよう二段階認証または二要素認証を採用する。
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(PCIDSS ver4.0 基準)のログイン失敗でアカウントをロックする。

□対応している
□対応していない
□対応していないが、代替策で対応している
（代替策を記載：　　）

「対応していない」を選択された場合
対応予定月を選択してください。
□2025 年 12 月末
□2026 年 1 月末
□2026 年 2 月末
□2026 年 3 月末
□上記までに対応が難しい

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。)

Web サーバや 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。

□対応している
□対応していない
□対応していないが、代替策で対応している
（代替策を記載：　　）

「対応していない」を選択された場合
対応予定月を選択してください。
□2025 年 12 月末
□2026 年 1 月末
□2026 年 2 月末
□2026 年 3 月末
□上記までに対応が難しい

③ Web アプリケーションの脆弱性対策

脆弱性診断また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。

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　(当該脆弱性が無いものが望ましい) やソフトウェアのバージョンアップを行う。Web アプリケーションを開発また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。

□対応している
□対応していない
□対応していないが、代替策で対応している
（代替策を記載：　　）

「対応していない」を選択された場合
対応予定月を選択してください。
□2025 年 12 月末
□2026 年 1 月末
□2026 年 2 月末
□2026 年 3 月末
□上記までに対応が難しい

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。

□対応している
□対応していない
□対応していないが、代替策で対応している
（代替策を記載：　　）

「対応していない」を選択された場合
対応予定月を選択してください。
□2025 年 12 月末
□2026 年 1 月末
□2026 年 2 月末
□2026 年 3 月末
□上記までに対応が難しい

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・チェックリストに記載の対策を 1 つ以上実施している。

□対応している
□対応していない
□対応していないが、代替策で対応している
（代替策を記載：　　）

「対応していない」を選択された場合
対応予定月を選択してください。
□2025 年 12 月末
□2026 年 1 月末
□2026 年 2 月末
□2026 年 3 月末
□上記までに対応が難しい

【2】不正ログイン対策

下記①～⑦のうち、実施している対策にチェックを入れてください。
いずれか 1 つ以上の対策が必須となります。

※対策の詳細は、以下資料をご参照ください。
1.EC 加盟店におけるセキュリティ対策導入ガイド【附属文書 20】　※P10～16 をご参照ください。
2.EC 加盟店におけるセキュリティ対策導入ガイド【附属文書 20】補足資料　※P25～33 をご参照ください。

※「会員登録」「ログイン認証」「属性情報変更」の各タイミングで最適な対策を網羅的に実施してください。
□① 不審な IP アドレスからのアクセス制限
□② 二要素認証等による本人確認
□③ 会員登録時の個人情報確認（氏名・住所・電話番号・メールアドレス等）
□④ ログイン試行回数の制限強化（アカウントパスワードクラッキングの対応）
□⑤ ログイン時のメールや SMS 通知、スロットリング
□⑥ 不正検知システム（Fraud サービス）
□⑦ デバイスフィンガープリント
□⑧現時点で、上記①～⑦いずれも未対策

上記①～⑦以外に実施している対策があれば、3.EC 加盟店におけるセキュリティ対策一覧[【附属文書 20 別紙 a】の 3.不正ログイン対策（決済前の対策）の中から具体的に記入してください。
（実施している対策：　　）
「⑧現時点で、上記①～⑦いずれも未対策」を選択された場合
対応予定月を選択してください。
□2025 年 12 月末
□2026 年 1 月末
□2026 年 2 月末
□2026 年 3 月末
□上記までに対応が難しい

▼各資料のリンクは下記にございます。
1.EC 加盟店におけるセキュリティ対策導入ガイド【附属文書 20】.pdf
https://www.cardservice.co.jp/info/guide/pdf/securityguide1_csv.pdf

2.EC 加盟店におけるセキュリティ対策導入ガイド【附属文書 20】 補足資料.pdf
https://www.cardservice.co.jp/info/guide/pdf/securityguide2_csv.pdf

3.EC 加盟店におけるセキュリティ対策一覧 【附属文書 20 別紙 a】.pdf
https://www.cardservice.co.jp/info/guide/pdf/securityguide3_csv.pdf

以上