提出必須

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

申告日

本申告書は、クレジット取引セキュリティ対策協議会が策定した「クレジットカード・セキュリティガイドライン」に基づく対応であり、全てのEC加盟店はご加盟時に自らのセキュリティ対策の措置状況を申告する必要があります。

【ご参考】クレジットカード・セキュリティガイドライン

1. 申告内容のご記入

≪申告前にお読みください≫
・システム未構築の場合は、各セキュリティ対策のチェック項目について、構築完了した時点で充足することを前提に申告してください。
・新規加盟店契約時のみならず、契約後においても継続的に対策を維持することを前提に申告してください。
・各対策の詳細は、クレジット取引セキュリティ対策協議会作成の「セキュリティ・チェックリスト」をご確認ください。下表に「該当頁」を記載しています。
【ご参考】セキュリティ・チェックリスト
・ECサイトの開発を委託し、そのECシステムを提供する会社（7号事業者）が「セキュリティ・ガイドライン」で求めるセキュリティ対策を実施していることを確認の上、申告してください。

（1）申告者および委託先情報　※セキュリティ対策を委託先等が実施している場合は委託先情報についても記入してください。

申告者情報	
事業者名	
ECサイト名	
URL	https://

委託先情報 ※複数の組み合わせがある場合、「(2)①②/A社」「(2)③/B社」等書き分けてください。	
委託先企業名	
ASPカート事業者名	株式会社ハンズ
PCI DSS準拠済み	QSA:

（2）カード会員データの漏えい等対策

重点対策項目	該当頁	すべてに「○」か「×」を記入
①管理者画面のアクセス制限と管理者のID/PW管理		
管理者のアクセス可能な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。設定①	13 14	○
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。設定②		○
管理者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。		○
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。）	15 16	○
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。		○
③Web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。	17 18	○
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。	19 20 21 22	○
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。		○
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。	23	○
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。	24	○

（3）不正ログイン対策　※貴社サイトが対象となります

（3つの場面：カード会員が操作をする場面）

不正ログイン対策項目		該当頁	すべてに「○」か「×」を 3つの場面 A 会員登録時	B ログイン認証時	C 属性変更時
①	不審なIP アドレスからのアクセス制限	27 28 29	○	○	○
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）		×	対象外	対象外
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）		対象外	○	対象外
⑤	ログイン時のメールやSMS 通知、スロットリング等		対象外	×	対象外
⑥	不正検知システム（Fraud サービス）		×	対象外	×
⑦	デバイスフィンガープリント等		対象外	×	×

確認結果

	A	B	C
【不正ログイン対策】 ※自動計算 A、B、Cの各場面ごと（縦列）に最低1つ以上「○」がつかない場合「×」となります。	○	○	○

【カード会員データの漏えい等対策】 ※自動計算
重点対策項目のうち全て対応できていれば「○」、1つでもできていない項目があれば「×」となります。 ○

確認結果が全て「○」＝提出可能です。

確認結果のいずれかに「×」がある。
＝以下に代替策を記入の上、提出してください。
※記入いただけない場合契約できません。

各種対策未充足時における代替策　例）WAF（Web Application Firewall）の導入等

受付会社使用欄

設定①と設定②を「〇」で申請するためには、
カートＳ管理画面にて、ショップ様ご自身での
設定が必要となります。
設定①と設定②以外の項目につきましては、
上記記入例通りにご入力いただければ問題ございません。

設定①：アクセス可能なIPアドレスを制限する設定

▼参照マニュアル：
https://cart.e-shops.jp/manual/02-iplimit/

設定②：二要素認証の設定

▼参照マニュアル：
https://cart.e-shops.jp/manual/02-two-factor/