セキュリティ対策状況申請届

ご契約者様情報

ご提出日	年　月　日	会社名 (個人の場合は代表者名)	
法人番号 (個人契約者様は記入不要)			
ご連絡先	部署名	担当者名	印
	TEL	(　　)	
加盟店番号			
加盟店名			

下記内容について変更があった場合、□に✔印をお付けのうえ、該当事項を記入してください。

クレジットカード情報の保持状況（店舗販売・通信販売共通）

機器、ネットワークにおけるクレジットカード情報保持状況（カード情報保護対策）について、ご記入ください。
また、EC加盟店の場合は、脆弱性対策の実施状況もご記入ください。

①カード情報非保持

□非保持化済　□カード情報非保持化同等/相当の対応を行っている

□カード情報を保持している　→　②カード情報保持の設問にご回答ください。

②カード情報保持　　③脆弱性対策（EC加盟店のみ）

□ⓐPCIDSS準拠済　□裏面に記載の脆弱性対策①～⑤を全て実施済み

端末機の設置状況（店舗販売のみ）

クレジットカード処理端末機の設置状況(不正使用対策)について、ご記入ください。

□IC対応端末設置済　（端末識別番号 □□□□□－□□□－□□□□□）

不正利用対策状況（通信販売のみ）

通信販売における不正利用対策の導入状況について、ご記入ください。

□EMV-3Dセキュア	○導入	○廃止
□券面認証（セキュリティコード）	○導入	○廃止
□不正配送先情報活用（Fdec等）	○導入	○廃止
□属性・行動分析による不正検知サービス	○導入	○廃止
□不正ログイン対策（裏面に記載の対策の内、1つ以上）	○導入	○廃止
裏面に記載の①～⑧の対策の内、導入または廃止した番号（①～⑧）を右枠内にご記入ください		
□その他（　　）	○導入	○廃止

脆弱性対策　下記①～⑤が全て導入されていることを確認してください。	
①	システム管理画面のアクセス制限と管理者のID/パスワード管理
	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2段階認証または多要素認証（2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 ver4.0.1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。） 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。
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。
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。
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、「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つ以上実施している。

不正ログイン対策　実態に合わせ、以下の中から１つ以上の対策実施が必要です。	
適用場面（会員登録時／会員ログイン時／属性情報変更時の各場面を考慮した適切な対策を実施）	
①	不審なIP アドレスからのアクセス制限
②	2段階認証または多要素認証（2要素認証）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）、スロットリング
⑤	会員ログイン時/属性情報変更時のメールやSMS通知
⑥	属性・行動分析
⑦	デバイスフィンガープリント
⑧	その他の対策（別紙の「導入ガイド【附属文書20】」別紙a_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）