2017 年 6 月 21 日
一般社団法人日本クレジット協会

PCI DSS 準拠にかかる基準及び検証方法等に関する実施要領

1. 位置づけ

本実施要領は、『クレジットカード取引におけるセキュリティ対策の強化に向けた実行計画-2017-』（以下「実行計画」）別紙『1.PCI DSS とは』に基づき PCI DSS 準拠を目指す各主体者における取組方法等について定めるものとする。

なお、「非保持」の考え方、その他 PCI DSS 準拠に関する内容等本実施要領に定めのない事項については実行計画が原則、適用されるものとする。

当協会会員においては、これまで、改訂版「日本におけるクレジットカード情報管理強化に向けた実行計画」を業界指針としてカード情報保護に取組むこととしていたが、今後は実行計画を指針とし、本実施要領は、日本国内における PCI DSS 準拠に取組む際の実行計画の補完内容として取り扱うものとする。

また協会会員以外の実行計画における各主体においても、実行計画の補完内容として本実施要領を参照するものとする。

2. 各主体者の定義、適用レベル及び選定基準等

（1）定義

1）加盟店

物品等の販売や役務の提供等にあたりクレジットカードの取り扱いを行っている全ての事業者

①非対面/EC・EC 以外	・インターネット環境で、顧客と非対面で商品・役務等取引を行う形態 ・電話、FAX 等により注文を受付ける形態
②対面/POS 取引	実際に店舗等で、顧客と対面で商品・役務等取引を行う形態
③対面/スタンドアローン	決済専用端末やインプリンタで、顧客と対面で商品・役務等取引を行う形態

2）クレジットカード会社

①アクワイアラー	加盟店契約会社
②プロセシング業者	決済業務や事務処理等を受託する会社
③イシュアー	クレジットカード発行会社

3）PSP

インターネット上の取引において EC 加盟店にクレジットカード決済スキームを自ら提供し、カード情報を処理する事業者

（2）適用レベルと選定基準

1）加盟店

適用レベル	選定基準
レベル A	国際ブランド 4 社の基準による　※1
レベル B	①非対面/EC・EC 以外 ②対面/POS ：トランザクション件数年間 100 万件以上（レベル A 以外）※2
レベル C	①非対面/EC・EC 以外 ②対面/POS ：トランザクション件数年間 100 万件未満
レベルなし	対面/スタンドアローン ：全て

※1　American Express：250 万件以上、JCB：100 万件以上、VISA、Mastercard：600 万件以上の対象企業のうち、2 ブランド以上の基準に該当した企業。

※2　いずれかの国際ブランド会社において、トランザクション件数が年間 100 万件以上。

2）クレジットカード会社

適用レベル	選定基準
レベル A	①アクワイアラー。ただし、国際ブランドから直接且つ定期的にカード情報保護にかかる取組の状況について報告を求められている先 ②プロセシング業者
レベル B	イシュアー及びレベル A 以外のアクワイアラー

3）PSP

選定基準
全て

3. PCI DSS 準拠方法

各主体適用レベルごとの準拠方法は別紙参照

（1）オンサイトレビュー（年 1 回）

認証セキュリティ評価機関（QSA）等による審査。インタビューやドキュメント確認、サーバーの実機確認、ネットワークなど、オンサイトにて監査を実施。

（2）自己問診（年 1 回）

WEB サーバーのセキュリティ診断､アプリケーション､ネットワークのペネトレーションテストなど、PCI SSC 等が HP 上で公開している問診票の質問項目についてチェックし、全ての項目を対応済とするまで繰り返し実施し、AOC（Attestation Of Compliance）を作成。

4. 実施時期

本実施要領は、2017 年 6 月 21 日より実施する。