クレジットカード決済システムの更なるセキュリティ対策強化に向けた主な取組のポイント

キャッシュレス決済及びEC取引の普及に伴い、クレジットカード決済市場の規模が増加する一方、サイバー攻撃やフィッシング詐欺の増加等を背景に、クレジットカードの不正利用被害額が増加傾向。こうした中で、非対面取引におけるクレジットカード決済の更なるセキュリティ対策強化を図るため、クレジットカード決済網に関わる多様なプレーヤーによる多面的・重層的なセキュリティ対策の取組を整理。

Ⅰ．漏えい防止（クレジットカード番号等の適切管理の強化）

（１）EC加盟店･アクワイアラー等

◆EC加盟店

- 従前の**非保持化**等の対策に加え、クレジットカード番号等の適切管理義務の水準を引き上げるべく、**ECサイト自体の脆弱性対策**を必須化（システム上の設定不備改善、脆弱性診断、ウイルス対策等）【セキュリティ対策GL改定】
  ※引き続き、漏えい事案が多発しているOSS（オープン・ソース・ソフトウェア）を利用したサイトの運用の対策（2019年国から注意喚起）も継続強化
- アクワイアラー等からの調査に基づき、ECサイトの脆弱性対策の実施状況を申告
  ※昨年10月～試行的運用開始
- **「ECサイト構築･運用セキュリティガイドライン」**（IPA：今年度末策定）等を踏まえた自主的取組の充実 ※対策の例：WAF（Webアプリケーションファイアウォール）の導入等

◆アクワイアラー等

- 加盟店管理（セキュリティチェック）における**EC加盟店調査事項の対象拡大**【セキュリティ対策GL】
  ※昨年10月～試行的運用開始(再掲)、2025年度～法的義務化
  ←調査の頻度やシステム整備等、実務的に運用可能な加盟店管理手法となるよう要検討

＜継続的検討事項（更なる制度的措置の必要性）＞

- 加盟店管理の実効性担保に向けた国の監督の関与の在り方
  ※他、トークナイゼーションの技術の利用等、将来的な課題も存在

（２）決済代行業者等

＜継続的検討事項（更なる制度的措置の必要性）＞

- PSPの実態整理を踏まえた監督の在り方、EC決済システム提供者の範囲の明確化

（３）クレジットカード番号等取扱業者

◆イシュアー等

- 最新の国際セキュリティ基準「**PCI DSS v4.0**」準拠への移行（～2024年３月末）

＜継続的検討事項（更なる制度的措置の必要性）＞

- EC加盟店を含む、クレジットカード番号等取扱業者でのセキュリティ対策の表示等

（４）漏えい時のインシデント対応の強化

◆EC加盟店･決済代行業者等

- 漏えい時の**利用者への連絡･公表の早期化**等【業界マニュアル改定】
  ※「サイバー攻撃被害に係る情報の共有・公表ガイダンス検討会」（NISC等）でのガイダンスも参照

◆日本クレジット協会（認定割賦販売協会）

- クレジットカード業界のセキュリティ対策に関する**体制強化**（セキュリティ問題の原因･分析等）

＜継続的検討事項（更なる制度的措置の必要性）＞

- 漏えい時の国への報告、被害拡大防止･利用者保護に向けたクレジットカード決済サービスの即時停止･再開の判断の明確化

Ⅱ．不正利用防止

（１）利用者本人の適切な確認の強化

◆イシュアー・EC加盟店

- 不正利用防止措置として、利用者本人しか知り得ない･持ち得ない情報（ワンタイムパスワード･生体認証等）による利用者の適切な確認**（本人認証）**の仕組みを順次導入（～2024年度末）【セキュリティ対策GL改定】
  ※アカウントの紐付け時の確認等、運用については更なる検討が必要
- 原則全てのEC加盟店で、国際的な本人認証手法「**EMV 3DS**」**の導入**【セキュリティ対策GL改定】
- 利用者の適切な確認の実効性を担保するため、イシュアーの**リスクベース認証**の精度の向上（利用者の行動分析、AI等を活用した利用者の行動分析等）
  ※リスクや取引規模が大きい加盟店での更なる不正利用防止措置の運用検討

＜継続的検討事項（更なる制度的措置の必要性）＞

- 不正利用防止措置の主体の整理、利用者本人の適切な確認の実効性担保に向けたモニタリング等

（２）不正利用情報の共有化と活用

◆業界横断的な取組

- **イシュアー間の不正利用情報の共有**に向けた枠組みの検討･連携の促進

Ⅲ．犯罪抑止･広報周知

（１）フィッシング対策

◆イシュアー

- サイトのテイクダウンや送信メールのドメイン管理**（DMARC）**等によるフィッシング詐欺への自衛･推奨

（２）警察等との連携による犯罪抑止

◆国･イシュアー･EC加盟店

- **警察庁サイバー警察局や都道府県警等の連携強化**による犯罪抑止【業界マニュアルへの反映等】
  ※「サイバー事案の被害の潜在化防止に向けた検討会」（警察庁）を踏まえて今後具体化（今年度末）

（３）利用者への広報周知

◆日本クレジット協会･イシュアー･国

- クレジットの安全･安心な利用に関する利用者への被害防止のための措置の**広報･周知**（利用明細の確認、EMV3DSのワンタイムパスワード設定等）

※「世界一安全な日本」創造戦略（2022年12月改定）においても、クレジットカード等の決済の本人認証や不正検知の強化、フィッシング対策の推進等が必要とされている。
※セキュリティ対策GL：クレジットカード・セキュリティガイドライン（クレジット取引セキュリティ対策協議会）