第１回クレジットカード決済システムのセキュリティ対策強化検討会
議事要旨

日時：令和４年８月４日（木）１３時００分～１５時００分

場所：オンライン会議（Teams）

出席委員：
中川座長、池本委員、大河内委員、大野委員、小川委員、篠委員、二村委員、松尾委員、三浦委員、森竹委員
※オブザーバーについては構成員名簿を参照

議題：
１．開会
２．議事
（１）検討会の設置等
（２）クレジットカード決済システムのセキュリティ対策強化に向けた方向性
（３）今後の検討に向けて
（４）自由討議
３．閉会

議事概要：
■事務局より、資料１、２、３に基づき、検討会の趣旨等について説明。
■事務局より、資料４－１、４－２、５に基づき、ご議論いただきたい論点を提示した後、委員による自由討議を実施。

自由討議：
Ⅰ．クレジットカード情報保護対策・漏えい防止
〇加盟店での漏えい対策
・2017 年以降、EC 加盟店でクレジットカード番号の非保持化が浸透した。一方、セキュリティリテラシーの低い EC サイトの開発会社等は、開発ツールの設定不備をつかれて不正侵入されるケースが多い。既知の脆弱性の悪用事案が多く、入り口としての加盟店・EC サイトの開発会社等のセキュリティのリテラシーの均一的な強化、脆弱性対策が必須。
・非保持化対策を通じて加盟店側でセキュリティの関心はかなり上がったが、セキュリティはアップデートしないといけない。セキュリティ対策はプロ集団との戦いであり、加盟店単位で対応していくのは限界ではないか。
・中小加盟店や EC モールもシステムを実装した時点ではセキュリティ対策を考えていたかもしれないが、サイバー攻撃の進化や、IT 環境の進化もあるので、構築、運用開始後は、セキュリティ対策の状況を定期的に確認する運用も大事である。
・セキュリティ対策の強化や運用にはコストもかかる。コストも含めた対応検討ができるとよいのではないか。

○アクワイアラーによる加盟店管理・決済代行業者の管理
・アクワイアラー管理は法律上の制度となっているが、現時点のクレジットカード業界の構造において、アクワイアラーによる管理がどこまで実効的なのか、決済代行の管理が実効性ある実態なのかの確認をした方がよい。場合によっては考え直さないといけないかもしれない。
・決済代行業者等を通じた加盟店管理の在り方について、アクワイアラーの対応というより法第35条の16第1項第4号事業者側の対応として考えないといけないのではないか。
・PSPも含め、ECサイト構築に携わる全てのプレーヤーがセキュリティのレベルを上げていく必要がある。特にセキュリティ対策は、発信されるセキュリティホールなどのセキュリティ情報の数や頻度が多く、情報のキャッチアップ、レベル感を合わせていくことが非常に重要。
・決済代行業者における漏えい対策について、基本的にはPCI DSSの準拠だが、PCI DSSの監査をするQSAによってレベル感が違うところもあるのではないか。一般的にQSAの評価は、PCI DSSの要件書に応じて監査するとはあるが、PCI DSSの要件書はセキュリティ対策について記載があるが、そのレベル感については示唆されておらず、QSAのレベルによって判断される為、PCI DSS要件書だけでいいのか。

○インシデント対応・漏えい防止にかかる情報の横展開
・セキュリティ関連の情報は、日々刻々変わっていく。準拠評価をする立場として、事案が発生した場合には、公開している情報を探し当てて確認している。それぞれの情報発信だけでなく、ここを見れば最新の情報や過去の事案が全て分かるという、集約・情報共有の一元化が必要。
・PCI DSSを準拠しているのにも関わらず漏えいしている事案もある。漏えい事案の対象システムが準拠範囲に含まれていたかどうかは公開情報では不明である。新しくリリースされたPCI DSSのVer.4は、カード情報の取扱範囲の確認も強化されており、今後より一層のPCI DSS準拠の強化が進むのではないか。

○対策に向けた規制の在り方・視点
・クレジットカードは国際的な決済ツールであり、国際的スタンダードに沿った基準を採用すべき。
・技術的側面が大きいため、規制の方向性としては柔軟に規制内容を作り変えられる方法が必要。エンフォースメントとして、現状は損失分担ルールが第一の発想だが、自分のところで損失を抱えればいいのではないか、となってしまうので法律の裏付けが必要。柔軟性という点からは、法律とガイドラインの民間ルールとの組み合わせが必要である。一方、実際のチェックについては、行政の監督だけでなく、民間認証機関等を活用することを制度に含めるべき。各事業者のプレーヤーごとに委ねると、事業者にはそれぞれ力関係が出てくる。
・カード漏えいだけではなく、カード情報含めた個人情報の漏えいもあり、ウェブセキュリティ全般を視野にいれた議論ができればよい。通販だと越境ECも見据えた国際的なレベル感を踏まえて、ホームページのセキュリティ最低基準をガイドライン等で出していただけるとありがたい。加盟店の業界団体では、毎年セキュリティのセミナーを主催しているが、関心をもって参加する会社は少ない。

Ⅱ．不正利用防止
○不正利用に関する実態把握

・不正利用として、番号盗用の被害額が多いのが現状。被害の手口を知ることで、不正利用対策の優先づけや方向性がわかるのではないか。想定される内訳としては、クレジットマスター、情報漏えい、フィッシングか。どのくらいの割合で漏えいしているかは把握出来るとよい。
・不正利用に使われる商材・サービスはどうなっているのか。以前調べたときは４、５つの換金しやすい分野等に偏っていた。今もそうなのか。
・不正利用はどこかで漏えいした番号が使われ、消費者が気付かないうちに引き落とされることも水面下でもあるかもしれないが、まずは消費者が心当たりがないとカード会社に申し出をするはず。不正利用の 330 億円の不正利用はどういう契機で顕在化していくのか。
・不正利用の 330 億円の金額は、日本クレジット協会の会員会社に調査を実施し、結果を取りまとめたもの。国際ブランドカードを発行している会社を対象、回答社数は４１社。フランチャイジーやブラザーカンパニーもあり、各社の下に何十社とぶらさがっているため、全体のクレジット決済の相当のシェアが対象として把握できていると認識。

〇決済時の取引認証（EMV3DS）の導入
・クレジットカードの IC 化は一定の効果が出たが、非対面利用での不正が止まらないことについては、ここまで大量の不正取引があるという実態を鑑みると、加盟店の商材に応じた４方策（本人認証、券面認証、配達先のチェック、リスクベース認証）だけでなく、更なる対策として本人確認の義務化のような議論が必要なのではないか。
・従来、3DS が導入されていると購入手続きが面倒だったが、リスクベース認証で、かごオチリスクが解消されたのであれば、素晴らしいという印象を受けた。そうすると、EMV3DS の導入のハードルがわからない。加盟店にとって、導入の経済的負担の問題なのか、かごオチの利用率の問題なのか。先駆的に導入されている事業者はどういう場合なのか。導入の費用対効果の面も含めて加盟店が導入を躊躇する理由の率直な議論が必要。
・EC モール、EC システムは PSP のカテゴリーに含まれているが、企業・業種・団体によってまちまちなので、全般的に網羅しながら議論できたらよい。
・かごオチが 3DS 導入の妨げになるというのは確かに感じるが、経済的負担も導入の妨げとしてはあると思う。自分の知る通販事業者 20-30 社うち４，５社程度しか導入していなかった。
・現状、既存の 3DS を利用している加盟店は、国際ブランドとの関係で、新しい EMV3DS のバージョンへ 10 月までに切り替える真っ最中。今後は、EMV3DS を利用する加盟店の拡大、クレジットカード会員側の登録の推進も必要。全ての加盟店に一斉に導入は厳しいが、導入に向けた時間軸・規模等の優先順位を議論していくことが必要。
・PSP としては EMV3DS を加盟店に導入してもらうための準備は終えていて、これから加盟店へ導入拡大する段階である。導入負荷は高く、中小事業者にとっては大きい投資になるため、加盟店に導入メリットをしっかり啓発し理解してもらった上で導入してもらうる必要がある。一律の導入は非常に難しく、時間軸・ルールなどしっかり議論して現実的な形で決めていくことが必要。
・最低限、これだけは守らなければならないということを専門家の方に決めていただいて、これを守らなければカード決済ができないとなると、事業者が一並びで公平・平等で導入すれば加盟店としても納得しやすい。導入している事業者側の好事例の収集も必要であるが、本人確認の義務化も必要。大手企業だけが導入に伴い、顧客にパスワード変更等のメールをしつこくするとかえって顧客に危惧される反応にもなる。大手企業だけでなく、公平・平等な取組が必要。
・一律の対応が求められている状態でないと困るという指摘は印象的。セキュリティの方策にもよるが、段階的とするのかきめ細かく考えていきたい。

・法令を導入したとすると、エンフォースメントとして、どのような形になるだろうか。従前どおりの損失負担のルールまでか、行政処分までか。アクワイアラーに課すのか、加盟店まで課すのか。
・カード会社と加盟店の契約の中で、一定のセキュリティレベルがとれていなければ、情報漏えい・不正利用の損害は加盟店が負担するべきという議論があった。これが今どのくらい普及して適用されているだろうか。

〇カード会社（イシュアー）間での不正利用データの共有
・セキュリティ情報だけでなく、不正利用情報事案の共有も必要。個人情報保護法との整合性の関係もあり、法令上の裏付けが必要であろう。

Ⅲ．クレジットの安全・安心な利用に関する周知・犯罪の抑止
・フィッシングについては大きな課題感を持っている。従前はオンラインバンキングが狙われていたが、現状は個人情報とクレジットカード番号を取る手口が多い。サイト自体のテイクダウンといった取組の強化も今後必要。
・インターネット上で既に流出しているクレジットカード番号をカード会社で活用できると良い。

Ⅳ．その他
〇今後の検討に向けた全体論
・法律上は、セキュリティ対策は割賦販売法にも形の上では求められており、例えばPCI DSSについてはガイドラインにより最新のものを守ることが実質上の義務になっているにもかかわらず、漏えいする。不正利用対策についても、ネット決済のところは決定打が欠けているが、法律上若干の裏付けがあるとは言える。今の制度のどこに課題があったかを分析しておかないと、有効打を打つことが難しい。例えばセキュリティ対策のアップデートや対応をしていない加盟店が多いまたは対策したつもりになっているが十分ではない、認証機関の質に問題があるのではないかといった指摘があるが、これらを取りまとめて、次回以降事務局にご提示いただきたい。
・クレジットカード決済はネット決済の主要なツールとして、今後も伸びていくので有効な方策が必要。他方、規制をやりすぎると利用者負担が増えてネット決済自体が伸びていかない。リスクに見合わない規制は控え、リスクベースでの規制が大事。利用者・購入者が受ける被害だけで考えると、300億円、400億円の数は大きいが、70兆円の中のわずかな部分ともいえる。しかし、犯罪者集団にお金が流れているという点では、単なる経済的損失だけではないところを着目していくべき。
・330億円のリスクの認識について、犯罪集団に資金が流れているが、加盟店やサイト構築者に自分の問題と考えてもらえているだろうか。損失分担ルールが機能していないのではないかという指摘があったが、保険でなんとかなるとか、リスクはあるが私は大丈夫との心理が働いて、自分の周りで実際に困ったことが起きていないという認識なのかもしれない。330億円がいかに大変なリスクかという説明がもう少し必要。

〇クレジット取引セキュリティ対策協議会での取組
・クレジット取引セキュリティ対策協議会は、2016年以降、セキュリティ対策を2020年までにグローバルなレベルに引き上げようと期限付きで活動し、実行計画を策定していった。2020年以

降は、クレジットカード・セキュリティガイドラインを策定し、割賦販売法の具体的な実行指針となった。来年度の不正被害は 400 億円を超えるのではないかと言われる大変な不正被害が起きており、実効性のある対策を具体的に検討しているところ。次回以降、協議会が検討しているセキュリティ対策を提示したい。
・クレジット取引のセキュリティ対策は、従来はクレジットカード業界の色が強かったという認識だが、昨今色々なプレーヤーがこの業界に参画して、キャッシュレス決済が成り立っている。一定の業界だけが頑張れば防げるわけではない。セキュリティ対策協議会でも、マルチステークホルダーとともに、実効性のある取組・施策をまとめていけるようにしていきたい。