# 第５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１２月２３日（金）１５時３０分～１７時３０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、長谷川委員、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）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報告書（骨子案）
（２）自由討議
３．閉会

議事概要：
■事務局より、資料３に基づき、報告書（骨子案）について説明した後、委員による自由討議を実施。

自由討議：
全体
・基本的考えとして、「消費者保護」というより「消費者利益の保護」の方がよいのではないか。割賦販売法自体は購入者等の利益の保護を目的としている。「消費者利益」の意義には、被害を受けない観点だけでなく、適切なコストでサービスの利便性を享受するという観点もある。セキュリティ対策は効果的・効率的であるべき。
・クレジットカード決済の特殊性として、世界中でどこでも使える点があり、利便性もあるが、それが故のセキュリティ上の課題にもつながる。セキュリティ対策としては、海外の不正事案やセキュリティ情報を踏まえることも有益であるため、これらの情報を持っている国際ブランドと、国が建設的な対話を定期的にできる仕組みがあると良いのではないか。国内の規制とブランドルールとの関係の整合も期待できる。
・クレジットカード取引にはブランドの役割が大きい。割賦販売法の対象にはいないが、重要なステークホルダーとしてブランドにも議論に介在してもらう必要がある。

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）加盟店での漏えい対策の強化
・EC 加盟店における対策の実効性確保として、脆弱性対策とあるが幅広く見える。既知の脆弱性対策としたほうが良いのではないか。

・脆弱性対策の意味合いとして、具体的には脆弱性診断の意味合いが多いのではないか。基本的なセキュリティ対策の徹底を当然ながら行った上で、クレジットカード関連ならではの対策として位置づけたほうがよい。
・WAF は設定が大変であり、WAF を入れても漏えいした事案もあるため、脆弱性対策をしたうえで WAF を導入することが一般的。
・EC 加盟店の適切管理義務の水準引上げに異論はない。但し、EC 加盟店の中にはセキュリティ対策への意識が低いところもあるため、いかに理解させていくかのサポートが重要。JCA の体制強化もその解の一案とも考えられる。
・アクワイアラー等の加盟店管理は実効性がどんどん難しくなってきており、その手法が妥当なのか。アクワイアラー等は、そもそも PSP に対する強制調査の権限はなく、調査対象者の回答に依存せざるを得ない。さしあたりは、アクワイアラー等の加盟店管理の運用の延長で対応するということだろうが、そもそもの加盟店管理の在り方自体を見直すことを強く打ち出すべき。
・クレジットカード業界ではこれまで EC 加盟店に対して非保持化、PCIDSS 準拠等の確認をしていたが、構造的に限界がきている。EC 加盟店での脆弱性対策の義務化の方向性には同意。PSP やアクワイアラー等プレーヤー毎の応分の負担・責務を果たすことによって実効性の担保ができると考える。
・アクワイアラー等側では、既に試行として加盟店契約締結時のセキュリティチェックを始めており、実効性担保の効果等を検証した上で今後議論を進めてほしい。
・アクワイアラー等の加盟店管理として、既存の EC 加盟店数が膨大のため、新規契約締結分は実行に移せるが、既存 EC 加盟店を対象にセキュリティチェックをやっていくのは現実的ハードルが高い。範囲や優先度、時期については実情に合わせた運用設計が求められる。
・利便性の確保の観点と不利益回避の観点があるが、昨今はカード自体の紛失と異なり、利用者本人のあずかり知らないところで漏えいされ、世界中で不正利用されているという問題である。誰がどう負担するかが論点。社会的インフラの決済手段の提供者として、カード会社だけでなく、加盟店、EC モール運営者含め全体でどう負担するかを考えることも必要。
・加盟店管理として調査・管理の範囲を広げようとする方向において、アクワイアラー側の管理体制を人的にもシステム的にも強化する必要があるが、加えて国としても人的にもシステム的にも強化していく必要がある。現実にできる範囲での保護しかしないのであれば本末転倒。国で、リスクベースのうえ一定の優先度をガイドライン等で示すことが現実的ではあるが、アクワイアラー側での管理体制も強化していくという考えの下で進めていくべき。
・EC 加盟店が利用するサービスのセキュリティ対策の底上げも課題であることを明記すべき。例えば、新しい PCIDSS のバージョンでは、EC 加盟店に対しコンテンツセキュリティポリシーの要望が出ているほか、現在のバージョンであっても、クレジットカード番号等の取扱いに関係する利用先に対し、PCIDSS 準拠を求めている。
・加盟店の自己申告に対する実効性対策として、きちんと対応していなさそうな EC 加盟店に対して、国で無作為に EC 加盟店の脆弱性対策チェックをしても良いのではないか。
・セキュリティ対策の表示は、利用者への周知だけでなく、今後キャッシュレス決済を利用する EC 加盟店に対しても、PSP 等実際に加盟店を募集する事業者のセキュリティレベル等を判断材料として提供するためにも必要。

（2）決済代行事業者等における漏えい対策の強化

・アクワイアラーだけでなくPSPもセキュリティ対策やECシステムの構築のプロではなく、PSPの管理にも限界がある。セキュリティの義務の主体は本来EC加盟店であるため、加盟店管理の中味として現実的な制度設計が必要。
・PSPの登録については、加盟店管理の観点では、アクワイアラーとPSPの業務整理、すなわち責任と役割の線引きが課題。アクワイアラーの統制強化を軸とした見直しはどうか。
・PSP・ECモールの運営者がどういう役割を果たしているか、EC加盟店はPSPに何を期待しているかを早急に実態把握すべき。漏えい対策や不正利用対策において同等の役割を果たしている者または期待されている者に対しては、アクワイアラー・PSPに関わらず、等しい規制を課していくべき。
・PSPの実態把握は視野を広げて把握してほしい。例えば、ECモールの運営事業者は取引の場も決済手段も提供する。ECモール運営事業者は多数のEC加盟店を抱えており、加盟店契約の実質的な締結権限を握っているはず。従来の概念でいえば、加盟店契約締結業者として登録すべき対象になっているように思えるが、現在の法制では、決済ルートのなかで誰か一者が登録していればよいとして必ずしも登録されていない。加盟店契約を締結する事業者側として誰が責任を負っているのかがわかりにくくなってきている。多数のEC加盟店を一定数以上受け入れている事業者にはセキュリティリスクもあるはずであり、いわゆる決済代行業者だけではなくECモールの運営業者も含めて、様々な形で加盟店を抱えているところの実態の把握が必要。現実にEC加盟店をコントロールできる主体の観点からは、従来のアクワイアラーの概念だけでは十分ではなくなってきているのではないか。狭義のアクワイアラーが監督できる状況にあるのか、誰が責任をもって加盟店を調査することが実効的か、視野を広くして調査してほしい。

（３）クレジットカード番号等取扱業者での漏えい対策の強化
・ECサイト上でのセキュリティ対策の表示の表記の仕方には、セキュリティリスクへの配慮が必要。
・セキュリティ対策の見える化の表示をすることによって狙われないようにはした方が良い。また、どこがセキュリティ上よいサイトか消費者にわかりにくいというのももっともだが、EMV3DSが義務化された後はそもそも表示の必要はなくなるのではないか。

（４）漏えい時のインシデント対応の強化
・加盟店での漏えい事案の公表の早期化に向けて、利用者保護の趣旨の整理が必要。関心を持たない利用者もいるのではないか。
・現状、漏えいしたクレジットカード番号の範囲が確定してから利用者へ伝えられているが、その間に不正利用される危険性がある。一方、その範囲が確定していない段階で、例えばクレジットカード番号を切り替えたら、漏えいしたEC加盟店にカード切り替え費用を請求できない場合もある。公表と同時に、あるべきステップでどのような対策を取っていくかという標準的な対応を示さないと、利用者やクレジットカード会社へ混乱をもたらすのではないか。
・決済システムのインフラでの被害をトータルで最小化するため、負荷は少し増えるかもしれないが、各段階の当事者のセキュリティ体制として、漏えい時の利用者への個別通知・公表をしてほしい。製品安全の分野では、製品に不具合がある場合はリコールをかけることになっているが、原因や範囲が調査中だからという理由で国へ報告をしなかったらリコール隠しという社会的な批判を受け、消費生活用製品安全法では特に重大な事故の場合にはまずは公表して注意喚起する。クレジットカード決済でも同様に、一定の重大性がある場合、重大な漏えい事故の場合は、

その範囲・ルート原因がはっきりしなくても公表して注意喚起をすべき。利用者側では、利用明細で心当たりのない引き落としがないかを確認するという行動を促すことが不可欠ではないか。
・ある相談事案では決済代行業者での漏えいを９ヶ月後のイシュアーからの連絡で気付き、翌月に不正利用されたという相談事例があった。不正利用のおそれがあるとわかった段階で、広めに利用者へ公表すると被害が防げるのではないか。
・漏えいの連絡を受けた消費者の行動パターンは、様々だとは想定されるが、多くの場合は利用明細を見て不正利用されていないか確認するであろうことから、漏えい事案が早期に公表された場合は、それまで利用明細の確認をしなかった消費者も不正利用がないか確認をすると思われるので、早期に公表してほしい。
・漏えいの利用者への周知・公表の問題は、消費者への公表の仕方・文案の問題と認識。漏えい範囲はまだ不確定であるけれども、直近の利用明細をよく見てほしいといった、消費者側の自衛策となる行動をアナウンスして公表すると良いのではないか。消費者安全法または消費生活用製品安全法の運用が参考となる。

Ⅱ．不正利用防止
（１）利用者本人の適切な確認の強化
・すべての取引における本人認証の義務化については、法人カード・継続的取引など個別考慮が必要なケースもあることに留意。また、システムの安定稼働のための準備も必要となる。
・EMV3DS は、現時点での有効な手法の１つであり、多面的、重層的な対策は引き続き継続することが必要。
・一方、EMV3DS は取引時にコストが発生するため、不正利用被害削減とコストとのバランス、優先順位、取引形態、対象範囲は継続的に慎重に議論を進めるべき。普及にあたっては、EC 加盟店への理解度を高めるとともに、中小 EC 加盟店の負担低減策として政府のコスト支援も必要ではないか。
・EMV3DS はアカウントの紐付けがあれば、その後の個別決済時には省略してもいいのではないかという意見に対しては、アカウントごとの乗っ取りの被害も踏まえると、ログイン後の個々の決済時にも EMV3DS による本人認証を必要とする慎重さもあってもよいのではないか。
・PSP として対策を進めることに違和感はない。2022 年 10 月にて 3DS1.0 から EMV3DS に切り替えは終わり、EC 加盟店の導入対応をしているが、システムの安定度の課題がみられる。イシュアーもブランドも EMV3DS システムの安定度を改善しないと、EC 加盟店でのかご落ちにつながってしまう。
・すべての事業者での義務化ついては、今後の細かい議論として調整させてほしい。

（２）不正利用情報の共有化と活用
・現在、監督官庁は不正利用の額は把握しているが、具体的な不正利用の状況・類型・割合が把握していないということであった。今後、国がモニタリングを適切に実施するとして、国として効果の有無を検証する必要がある。もし国際ブランドが参考となる情報を持っているのであれば、同等の情報が監督官庁にも提供されるような仕組みをつくるべきではないか。
・不正利用対策は段階的な導入が現実的という点に同意。一方、不正利用対策には終わりがなく、「これを入れたから安心」とはならない。監督官庁と業界団体も、継続的に不正利用の状況の研究が必要。

・セキュリティの対策費用がコストに跳ね返ることを鑑みると、キャッシュレス促進のための加盟店手数料低下の動きも求められる環境のなかで、どのようにコストを捻出するか、ポイントの切り下げも含む利用者への価格転嫁をどうしていくかという論点も出てくる。どこまで対策するかの現実解を見定めるにあたり、リスクの正確な判定、これを踏まえた行政指導や業界団体のガイドライン策定も大事。リスクの判定のために個社でもっているデータを出していくことが必要であり、国及び JCA での研究に活かされたい。

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

（１）フィッシング対策

・自衛している事業者が自ら行うフィッシング対策は、フィッシングの未然防止の位置づけで捉えるべきである

・フィッシング対策はイシュアーだけでなく EC 加盟店も行うと良いのではないか。

（２）警察等との連携による犯罪抑止

・フィッシング対策について EC 加盟店に割賦販売法上求めていくのは、難しいかもしれない。経済産業省だけでなく、行政全体としてどのように対策していくか、問題提起をしてはどうか。

（３）利用者への周知

・利用者への周知は業界団体・民間事業者だけでは不十分。国としての実施も強く希望。