第２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９月１３日（火）１４時００分～１６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（代理）、篠委員（代理）、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）クレジットカード番号等の漏えい対策
３．閉会

議事概要：
■日本クレジット協会より資料２に基づき、クレジットカード取引セキュリティ対策協議会より資料４に基づき、EC 決済協議会より資料５に基づき、説明。
■事務局より、資料３に基づき、クレジットカード番号等の漏えい対策について御議論いただきたい論点を提示した後、委員による討議を実施。

討議：
１．クレジットカード番号等の漏えい対策の全体像
・中長期的な課題認識として、他のカード会社も不正利用の被害の内訳を調査すると、議論が深まっていくのではないか。
・イシュアーにおける不正検知は、業界全体の水準があるというより、従来より各社でシステム導入されバージョンアップされ、今日に至っているもの。
・不正検知は、不正という確証が持てない中で動いている。実際、正当な理由の決済を止めてしまう場合もあり、どの線で守るかを不正検知の観点だけで見るとうまく機能しない。顧客属性、過去の経験値、情報量・質等を勘案して、個社で対応するしかない状況というのが実態。
・クレジットマスターの手法は、従前から継続的にあるが、業界としては苦慮する手口であり、防ぐことは難しい。不正利用されないよう対策することの方で防ぐしかないのではないか。最近は攻撃者側の技術が進化しているところ、大量のデータが流れたら不正検知して止めにいくという入り口対策が有効なのではないか。

２．EC 加盟店（2 号業者）での漏えい対策
２－１．EC 加盟店側での対応

・EC 加盟店での脆弱性対策を義務づけることに異論はない。公平・平等に加盟店皆が守らなければならないという方向性に進むことに賛成。まずは脆弱性対策を積み上げることが重要。その上で不正アクセスの早期検知があることが望ましい。
・不正アクセスの早期検知については、従前、不正利用対策の方針の１つであるが、技術面、コスト面等から、慎重に検討してほしい。
・EC 加盟店での非保持化は進んでいると認識。一方、EC 加盟店が PSP に接続する間のサービスを利用している場合に、当該サービスに起因した漏えい事案もある。EC 加盟店サイトや加盟店が利用するサービスを含めた脆弱性対策、不正アクセス検知、改ざん検知を求めていく必要がある。セキュリティ対策のための業務負荷や対策運用コストという観点もあるが、不正アクセス検知、改ざん検知は非常に重要。
・加盟店はセキュリティ対策を外部の社に丸投げしている場合が多いが、義務の主体者であるので、脆弱性対策を進めてほしい。
・PCIDSS は非常に有効な手段であるが、PCIDSS を入れて終わりだとすると、落とし穴がたくさんある。
・被害を防ぐという点では、脆弱性対策、適切なアップデートが必要。自社で適切に行われていない現状が課題であるが、まずは、加盟店の社内にセキュリティの担当部署または担当者を設置してほしい。
・EC サイトソフトウェアの脆弱性が発覚すれば周知公表されるはずであり、ソフトウェアを提供する会社含め適切な人に迅速に情報を届けることができる枠組みや連絡手段も検討事項として考えられないか。
・不正アクセスの検知の仕組みとして、クラウド事業者等が提供するセキュリティ対策サービスを加盟店が使うのは好事例。特に小規模な加盟店にとっては解決策の１つではないか。
・越境 EC で商売するのに必要な国際レベルでのセキュリティ対策は必要。加盟店は委託先やウェブサイトの管理会社に対策をお任せしている場合もあり、そうした事業者にチェック項目のひな形を出させて確認できる仕組みがあればよいのではないか。一方、当該項目は狙う側にも参考になる情報であり、細かなところまではすべてオープンにするには別途検討が必要ではないか。
・EC 加盟店側は、各サイトのセキュリティ対策の意識付けが弱い。アクワイアラーの加盟店管理としているが、申告書ベースでチェックしてワークするのか懸念。加盟店の意識が弱い、あるいは能力がなければ、アクワイアラーがチェックするのは実効的ではない。義務を課すことは賛成の立場だが、エンフォースメントとして一律投網をかけるのか。クレジットカードの取引件数といった定量的・第三者認証をとったサービス利用といった定性的なリスクベースの中で優先順位をつけて執行していくのではないか。
・不正アクセスの手段は高度化・巧妙化しているものもある一方、非常に簡単な攻撃で全く対策ができていないところが被害にあうケースも多く二極化している。全ての加盟店に、誰でもがわかるような脆弱性対策の最低限のラインを提示し啓蒙を行い、守ってもらうだけでも、かなり効果があるのではないか。
・事務局資料の加盟店に EC サイトの脆弱性対策を求めるべきという方向性に異論がなかった。他方、誰もがわかるレベルで脆弱性についての理解を広めることから始めるべきという指摘もあった。脆弱性対策の中味・水準について、実効性も確保しつつ制度設計を進めるべき。
・不正アクセスの早期検知等を求めていくことは望ましく、脆弱性対策と両輪ではある。全体にどのように義務づけにいくのか具体的には法制度をどうするかを今後考えていかないといけない。

・セキュリティ投資の必要性を感じないEC加盟店に行動変容を促すため、脆弱性対策リスクが高いビジネスモデルの場合、改善命令をすることも論理的選択肢にはあるが、義務付けには工夫が必要である。

２－２．アクワイアラー側での対応
・加盟店からの申告に基づくセキュリティ対策の実施状況の確認を、アクワイアラーやPSPに義務として課す場合、アクワイアラーやPSPの業務量が増えると想定されるので、非保持化の対応の前例を踏まえ、うまく進めてほしい。
・加盟店のセキュリティレベルについてチェックリストで確認する場合、加盟店のセルフチェック形式であり、アクワイアラーやPSPの業務負荷としては、申告書として受け止める形。どの程度実態に即しており抑止効果があるのか、試行期間に判断していく。
・セキュリティ対策の申告については、アクワイアラーやPSPが定期的に加盟店調査を実施して管理していく形となるものであるが、アクワイアラーやPSPの負荷もあると想像されるため、年１回など配慮が必要ではないか。
・アクワイアラーにおける実効性の課題として、脆弱性診断について知見を有している人材がいないところもある。より専門的な論点が入るので、どのような対策が有効かまとめていきたい。
・アクワイアラー側での対応については、方向性としては、現在の法制度上、将来的にアクワイアラーの管理でみていくという事務局資料に異論がなかった。但し、実効性という観点からはうまくやらないといけない。

３－１．PSP（4号・7号業者）での漏えい対策
・昨今の漏えい事案も踏まえると、PSP間でも対応に差があるということだろう。組織のセキュリティ意識、対策水準の底上げ、組織の文化、人的資源、セキュリティ対策費用等が必要であり、そのためにも経営層の強いリーダーシップが必要ではないか。監督上の観点で明示して確認していくことが必要ではないか。
・基本的なセキュリティ対策は、一般的には、本来、PCIDSSの要件に入るものがほとんどではないか。PCIDSSの準拠については、QSAのレベルにより、運用まで見ているのか、仕組みとして入っていればよしとするのか、QSAによって観点や深堀りのレベルが違うのではないか。PSPのセキュリティの体制は非常に必要なもの。PSPに求めるレベルをQSA同士でも話し合ったほうがよいのではないか。
・基本的なセキュリティ対策はPCIDSSテスト手順に含まれているが、QSAのPCIDSS準拠の審査にあたり、業務フローを確認し、カード会員データがどこにあるか確認する段階で顧客から正確な情報をもらえない場合には、準拠を確認できないことになる。年間４回分の脆弱性スキャンの実施を確認したり、顧客の状況を深堀りをする、診断対象や方法の適切性の確認などにより、脆弱性診断結果そのものをしっかり確認することである程度の改ざんは見つけることができると思うが、当該結果自体も改ざんされていると虚偽を見抜くことは難しい現実もある。
・PCIDSSに準拠してないものもあるが、脆弱性が公表されてから短期間で狙われるゼロデイ攻撃の場合もあり得るのではないか。総じて言えばPSP自体の漏えい件数は加盟店ほどは多くはなく年に１件くらいの程度ではないか。
・PSPがしっかり実施できているかは、アクワイアラーの負担が増えるかもしれないが、アクワイアラーがPSPに対し、調査・指導権限を持つことが有効ではないか。

・クレジットカード番号等の適切管理義務として、基本的なセキュリティ対策などを監督上明記いただくことは賛成。
・アクワイアラーが PSP の調査・指導をすると、カード事業の範囲に限定されかねず、組織・業務運営体制まで調査するには限界があるので、行政の監督上の観点としていれてほしい。業界団体の自主規制の機能強化も期待したい。
・PSP の７社で構成する業界団体として、セキュリティだけではなく、不良加盟店の排除なども議論している。網羅的な業界の底上げや国内 PSP200 社も参加するようになると、現状の枠組みでは実質議論が困難になると認識。PSP 全社が参画する別組織を立ち上げるという方策もある
・本当に信頼できるセキュリティレベルをきちんと確保できる PSP を利用することで安全管理措置を確保することが現実的な選択肢のように思う。アクワイアラーが PSP を調査・指導するといってもどこまで排除できるか、そもそもの入り口で選別審査があるかどうかという点では、国が事前に一定程度審査して登録制にしたほうがよいのではないか。
・加盟店が契約しているので、加盟店に申告させることがいいのではないか。PSP、アクワイアラーに申告してもその先に行かない可能性もあるので、事業者として認識できるような組織体が必要ではないか。
・PSP の中でも既に登録されている場合もある。行政としては、PSP に対し登録性にしたほうがよいのではないか。
・意図的にセキュリティの対応をしない PSP がいた場合、登録制により自己規律の度合いが上がっていくという期待程度かもしれない。４号業者のうち一定レベルの事業者は第三者認証を必ず受けてその結果を公表するという＋αの規範を入れるなど何か方法を考えないと機能しないのではないか。
・PCIDSS の実質的な準拠の体制は当然必要という方向性は固まったが、どのように見るか実務的に難しいのではないかという指摘もあり、具体策が課題。一方、国の事前監督や登録制度があれば、セキュリティ体制も多くの場合は自ずと効果があるのではないかという指摘もあり、事前の参入規制の形を踏まえながら、登録の取消や業務停止も含めた実効化の選択肢があるかもしれない。

３－２．加盟店向け決済システム提供事業者（7 号業者）での漏えい対策
・クレジットカード会員データのセキュリティに影響を与えるサービスについて、７号業者に該当するのであれば、代表的なものは、図などで表記して明示化してはどうか。
・７号業者向けや PSP 向けに漏えいマニュアルが策定されると、７号業者向けに長期に啓発ができるのではないか。
・事務局資料にあるように、７号業者の該当性については特段の異論はなかった。