第４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１１月１５日（火）１０時００分～１２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、長谷川委員、松尾委員、三浦委員、森竹委員
※オブザーバー、プレゼンターについては構成員名簿を参照

議題：
１．開会
２．議事
（１－１）クレジットの安全・安心な利用に関する犯罪の抑止（フィッシング対策）
（１－２）クレジットの安全・安心な利用に関する犯罪の抑止（警察等との連携）
（２）クレジットカード番号等の漏えい対策（インシデント対応・漏えい防止にかかる利用者保護）
（３）クレジットの安全・安心な利用に関する周知
３．閉会

議事概要：
■第４回検討会は非公開での開催とされた。
■フィッシング対策協議会より資料２に基づき、警察庁より資料３及び資料４に基づき、日本サイバー犯罪対策センターより資料５に基づき説明。
■事務局より、資料６に基づき、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．クレジットの安全・安心な利用に関する犯罪の抑止
１－１.フィッシング対策
イシュアーでの対応（DMARC）：
・業界として、一定の効果があることは認識しており、対応できるカード会社から対応している。
・フィッシングメールが届かないような対策があるのであれば、国としてフィッシング対策を進めてほしい。
・DMARC の有用性は疑いなく、積極的に導入してほしい。他方、クレジットカード事業者だけの問題ではなく、メールを発信する各事業者の問題。政府をあげて推奨いただくために積極的に官民連携をはかってほしい。

・導入の義務化や推奨をするのであれば、法令の義務付けではなく、自主規制ではないか。本件は、会員と接点を持つ側であるカード発行会社の問題であり、マンスリークリアも対象になるが、２月超を対象にしている割賦販売法との整合を考慮すると、自主規制による導入の推奨になるのではないか。しかしながら、自主規制だと、業界団体で実施状況のモニタリングをしていくのは荷が重いのではないか。今後の実行体制も含めて慎重な検討が必要である。
・DMARC の重要性を理解。自主規制では現状からあまり飛躍的に変わらず、実効性が不十分なので、これまでの漏えい防止・不正利用という概念を越えて、何らかの形での義務化も排除しないでもう少し検討したほうがよいのではないか。DMARC 導入は経済コストの問題かと思っていたが、導入した後の実行に時間がかかることは意外だった。一定程度義務づけた上で体制を早く作る、実効性を確保するために割販法で位置づけることも検討したほうがよいのではないか。

イシュアーでの対応（その他自衛策）：
・フィッシングの自衛対策が欠けているという認識に同意。加盟店である事業者内の部門間の整理がつかず、連携がうまくいっていない。
・偽サイトのテイクダウンやブラウザ事業者への通報を個社ごとに対応している。
・フィッシングの場合は、漏えい事案と異なり、業界関係者全てが被害者にあたると考える。レピュテーションリスクがあるので自衛をやることはよいが、結果的に犯罪を防ぐことに繋がっておらず、自衛のみでは不十分ではないか。犯罪組織を潰していくように国として舵をきってほしい。また、最終的にはフィッシングメールやサイトをなくすこと、カードホルダーのリテラシーを上げていくことがあるのではないか。
・偽サイトのホスティング対応事業者は海外が多く、テイクダウンの要請にスピーディーに対応してくれない傾向の国もある。ブラウザ事業者への通報も先方事業者の都合による優先順位もあり、単一企業からの通報には限界を感じている。業界として組織的な対応により何らか効果を高められないかと考えている。
・同じ IP アドレスで複数のカード会社になりすましてフィッシングメールを送っている事例が多くあることから、組織的に攻撃者の情報連携をすると対策が取れるのではないか。
・EC サイトのなりすましは、クレジットカード会社の個社でテイクダウンする対応が出来ない場合もあるため、業界をまたいで要請する策が考えられないか。
・テイクダウンして終わりでなく、警察又は JPCERT はテイクダウン後にプロバイダから契約者を明らかにして、契約者を調査してほしい。また、海外からのフィッシングの抑止も考えないといけないのではないか。
・フィッシング対応についての義務化によるレベル感については意見があったが、前提として、起きてしまったことに対する顧客対応と事故対策は異なり、どうやって今後未然防止するかという観点が重要である。クレジットカードシステムを守るため、DMARC 対応含め事業者自らが対策を進めるべきであるという部分は共通した意見であった。

利用者による対応：
・送信メールやフィッシングサイトの巧妙化のため、カード会社としてできる範囲でやっているが限界を感じている。利用者にとって、フィッシングの判別が難しいほか、スマホではメール発信者のドメインや偽サイトの URL の目視が難しいほか、SMS によるスミッシングもある。

・消費者は不正利用事案が生じてから調べることが多いが、クレジットカードの利用前に一度立ち止まってから申し込むように周知してほしい。
・利用者は注意喚起されても対応が難しいのではないか。例えば、海外からの電話は受け取らないような仕組みの構築やメールを受信しない設定で対応できないか。
・利用者にはサービスを選ぶ権利がある。DMARC 対応など安全なサービスを提供している事業者を選んでいってほしいと利用者に伝えていきたい。
・フィッシング対策は、クレジットカード業界だけの問題ではない。全体の問題の一部として、クレジットカード事業者がどのくらい早く対応するかという位置づけ。

１－２．警察等との連携
・クレジットカード業界の現状の活動として、クレジットカード犯罪対策協会では警察への捜査支援、情報連携等をしている。また、捜査員にカードビジネスや犯罪傾向の説明や研修をしている。しかし、非対面取引では不正利用の検知が難しいと認識。①業界として捜査進展につながる体制の継続（捜査員の知識のボトムアップ、不正利用情報の当局への提供)、②不正利用される可能性の高いクレジットカード番号等のスピード感をもったクレジットカード会社への提供、③カード番号や個人情報が売買される海外の SNS への取締りを取締当局の対応として期待。
・PSP としては、警察との連携は日々行っており、警察にはサイバー攻撃に対して積極的に対応してもらっているという印象がある。PSP としては、そもそも不正利用をされない環境、不正で得たカードを使えないようにする環境の構築に今後力を入れたい。カード会社の啓発もあるが、PSP としても啓発して意識づくりを進めていきたい。
・警察の捜査に資する情報がどういうものか教えてもらえると、フォレンジック調査会社も協力できる。
・クレジットマスターの犯罪は、PSP・アクワイアラー側の協力によって防げるのではないか。
・チャージバックが多い利用者への対応にはイシュアー・アクワイアラー・PSP 全体の協力も必要。
・警察としても、現場の警察への届出の対応には、現場でしっかり対応できるよう対策を講じていきたい。
・警察庁でもサイバー警察局が立ち上がり、国際捜査のための体制を整えていくことにしたところ。捜査・検挙は一番効果のある対策であり、今後とも引き続き対応･捜査を進めていきたい。
・警察等との連携については、加盟店側に捜査の流れを誤解のないよう伝えることが最初の出発点だろう。

２．クレジットカード番号等の漏えい対策
（１）国への早期報告：
・加盟店の漏えい事案では、アクワイアラーは早期に地方の経済産業局に速報ベースで報告しているものと認識。加盟店も早期に個人情報保護委員会へ報告できていると理解。既に早期に報告する運用はできあがっているため、国の報告義務の明示は不要。
・行政で法制化または基準を策定して管理してもらったほうが実務としては非常に運用しやすい。個別事案で対応が変わることから、対応や範囲などについては関係各所の意見を元に検討すべき。

・漏えい事案は深刻化していることから、国に早期に漏えい事案の報告をして、国で対策を考えてほしい。
・カード情報の漏えいという事態は悪意をもって不正利用されるおそれが極めて高い事態になり得ることである。安全分野のリコール情報など原因不明でもまずは公表して利用者に警戒してもらう考え方が法制度として位置づけられていることから考えると、漏えい事案についても直ちに行政に報告、行政から注意喚起するまたは利用者に直接通知することは必須であろう。
・国への報告義務は、被害拡大防止または再発防止のためか、その趣旨は両方あり得るだろうが、その意味で報告義務を明確にしたほうがよいのではないか。

（2）利用者への個別通知・公表
・利用者への個別通知・公表は、情報漏えいのフォレンジック調査中は、中途半端な公表により消費者に対して混乱が起きないよう、カード会社は加盟店と調整している。但し、加盟店の希望によりカード番号特定前でも早期の申し出があった場合には、現在、業界として公表文のひな形を用意している状況。個人情報保護法により速やかな通知・公表が求められているため、業界として基本的になるべく早期に公表できるよう対応している状況。
・加盟店は、HP での公表や顧客への個別通知を実施しているという印象。
・現状、利用者の混乱を避けるため、状況が見えた段階で初めて通知・公表をしてきたと理解。利用者への通知・公表の目的は利用者側が身構えてもらうことのためだとすると、疑わしい場合にも利用者に身構えてもらうために、より早期の通知・公表が必要ではないか。
・公表を持続させる期間や方法も課題であり、解決すべき。サイト上見つけにくい場所での公表や、公表後に割と早期に消されることが見受けられる。漏えい事業者がレピュテーションリスクを気にすることはわかるが、公表してもその後見つけられないという状況にすることは、適切な行動ではないのではないか。
・自分のクレジットカード番号等が漏えいした可能性があるということなので、不正利用がないか把握するため、利用者には早期に通知してほしい。段階的にわかった状況を公表してほしい。
・フォレンジック調査に時間がかかったり、漏えい期間の認識あわせや、フォレンジック調査の結果グレー判定の際の判定に苦慮することがあり、時間を要していることがあるので、このあたりがルール化されるとスピーディーになる。
・加盟店としては顧客との関係から個別通知等していると認識しているが、やるべき事業者がいてやらずに問題になったのであれば義務化が必要なのではないか。
・国への報告が義務化されるのであれば、被害拡大防止として行政が公表することもあり得る。国への報告と公表を併せて考えた場合に、どのような公表のあり方が適切か考える必要があるのではないか。

（3）漏えいした場合のクレジットカード決済サービスの停止
・PSP としては、漏えいした加盟店に決済停止を案内し、現状ほとんどの加盟店に即日停止してもらっている。カード決済以外も含めて止めている場合もある。
・利用者のカードの不正利用発覚時にカード会社に決済停止を依頼すると、今のところは割と柔軟に対応してもらっている。今後も柔軟に対応してほしい。

・加盟店から既に対応したとの申出により、フォレンジック調査前でも、カード決済の即日停止を拒否されることはある。アクワイアラーとしては、漏えい原因や再発防止策が明らかになり確認できるまでの間の決済停止に対し、強制力を持たせる方向性については同意。
・PSP のような大規模な漏えい事案では強制力が必要だが、税金等継続課金で払っているときに決済を止めることについては注意が必要ではないか。
・必要な対応であり、現状、民間事業者の段階で一定程度やっているという認識。法制度で担保するのであれば、国際ブランドルールとの関係含め、実情把握の上、国が踏み込むべき要件等を整理すべき。

（４）対策の強化に向けた各プレイヤーの役割
・海外の特定の IP アドレスからの不正侵入による改ざん等のケースが多い。こうした IP アドレスのモニタリングや共有情報の連携などにより、個別の加盟店や PSP だけでなく、業界全体として、なりすまし対策を進めるのがよいのではないか。
・セキュリティ対策協議会は非常に努力を重ねてきているが、自主的な集まりの位置づけであり、行政のより強い関与も視野にいれていく時期に来ているのではないか。
・国・行政がもう少し関わっていくべき。事業者も再発防止という観点では、行政、各プレイヤーそのものが責任をもってやるという考え方を明確にしていくということか。

３．クレジットの安全・安心な利用に関する周知
・日本クレジット協会の注意喚起の動画は短くわかりやすかった。一方、業界団体のサイトに見にいく人は少ないだろうから、政府広報やドキュメンタリー、若い人向けに動画サイトやニュースサイトの広告に流す等の広報に力を入れたらよいのではないか。
・成年年齢の引き下げ時に、中学校の教科書に記載したり、教育現場にオンラインセミナーで周知していた。利用者の手前の方にも周知する視点も必要ではないか。
・利用者への効果的な周知は難しいが、利用者の行動変容のため試行錯誤を続けていくしかない。