第１回　キャッシュレス社会の安全・安心の確保に関する検討会　議事要旨

1　開催概要

(1)　開催日時等

○　開催日時

令和５年 11 月９日（木）午後３時 00 分から午後５時 00 分まで

○　開催場所

ウェブ会議

(2)　出席委員等

○　委員

情報セキュリティ大学院大学教授　藤本正代（委員長）

（株）三菱 UFJ 銀行コンプライアンス統括部組織犯罪対策室調査役　大谷昭彦

（株）メルカリ経営戦略室政策企画マネージャー　岡本洋平

LINE ヤフー（株）CTSO 企画室（兼）渉外安全対策本部
安全対策部　安全政策　上級執行役員付参事　佐川英美

（一財）日本サイバー犯罪対策センター理事　櫻澤健一

（一社）EC ネットワーク理事　沢田登志子

森・濱田松本法律事務所弁護士　蔦大輔

東京都立大学法学部教授　星周一郎

○　事務局

警察庁サイバー警察局長

警察庁長官官房審議官（サイバー警察局担当）

警察庁サイバー警察局サイバー企画課長

警察庁長官官房参事官（サイバー情報担当）

警察庁サイバー警察局サイバー捜査課長

警察庁サイバー警察局情報技術解析課長

○　オブザーバー

内閣官房内閣サイバーセキュリティセンター

個人情報保護委員会事務局

金融庁

消費者庁

総務省

経済産業省

2　議事進行

(1)　開会

※　事務局より開会を宣言

※　事務局より委員長候補として藤本委員を推薦し、委員からの承認を得た。

(2)　議事

○　事務局説明

事務局及び個人情報保護委員会事務局から説明を行った。

○　自由討議

各委員からの主な意見については次のとおり。

【関係機関等との連携による利用者に直接届く効果的な注意喚起について】

・　注意喚起を顧客に知ってもらうこと、また、注意すべき点を正しく理解してもらうことが課題であることから、幅広い関係者で連携して注意喚起することで、話題性を高め、報道機関等に取り上げられるようにしたり、具体的な事例を示すなどサービスの実態や特徴を踏まえた注意喚起とすることが重要ではないか。

・　報道機関等と連携し、犯行手口や資金の流れだけではなく、例えばフィッシングメールの件名や文面等の具体的な犯罪者のアプローチ方法等にも焦点を当てて注意喚起すべきではないか。

・　コンビニや薬局においてコード決済が悪用される事例について、具体的な犯罪手口の情報を店舗に共有することで、店頭での被害の抑止につながるのではないか。

・　店舗における被害に関する捜査には防犯カメラの映像が重要となることから、映像の保存期間を長くすることなどについて事業者の協力を得ることが重要ではないか。

・　事業者が認証等を求めるページにおいて注意喚起や確認メッセージを表示することは、犯罪者の偽サイト作成のコストを増やし作成しづらくする観点からも効果的ではないか。

・　フィッシング被害者に対して利用ブラウザ、メールソフト、セキュリティ対策の有無等について調査を行い、どのプロセスに問題があったか分析し、被害の背景にある事情を踏まえた注意喚起を行うことが必要ではないか。

・　税金の支払時期や事業者が新たなサイトを作成した時期等を狙った巧妙なフィッシングが行われていることから、受信者側が立ち止まることができるような行動変容を促す注意喚起・教育を実施することが必要ではないか。

【フィッシングメールを利用者に届かせない対策について】

・　正規の URL や IP アドレス情報をホワイトリストとしてブラウザに登録し、アドレスバーの色その他の表示により正規サイトであることを示すといった対策はできないか。

・　事業者から送付するメールは委託事業者のアドレスから送付している場合もあり、DMARC 導入時の拒否・隔離のポリシー設定は慎重に行っている実態がある。
・　偽サイトや偽メールの真偽判定は人間の目では難しい点もあることから、例えば DMARC 等の技術的なサポートを取り入れ、機械的な判断を介在させることで、顧客に対して注意喚起・警告が出るという仕組みは効果的である。
・　フィッシングメール対策に加え、スミッシング対策として、SMS を受信するアプリの対策も必要ではないか。
・　偽 EC サイトへの対策として、SNS や検索エンジン事業者が広告を掲載するに当たって厳格な審査を行うことが重要ではないか。

【ID・PW を窃取された場合でも被害に遭わない対策について】
・　多要素認証の活用について、ユーザーの利便性に配慮しながら推進すべきではないか。
・　生体認証が、他の認証方法と比較して安全性が高いという点について周知していくべきではないか。
・　個人データの提供について、個人情報保護法第 27 条第 1 項第 4 号に加え、同項第 1 号（捜査関係事項照会を前提に）・第 2 号についても活用できるのではないか。
・　個人データの提供に関する指針や個人情報保護法上の解釈について、「防災分野における個人情報の取扱いに関する指針」（令和 5 年 3 月内閣府（防災担当））を参考に、個人情報保護委員会事務局の確認の下、個人データの提供に関する例外について具体的にケースを挙げてガイドラインとして示すことで、企業における情報共有の促進や犯罪抑止対策の強化につながるのではないか。
・　サービスの利用規約において、「一定の条件を満たせば警察に情報提供する」ことを示して同意を取ることで、個人情報保護法における第三者提供に関する同意取得義務の例外事由に完全に当てはまらなくとも、本人同意を根拠に情報共有が可能になるのではないか。
・　利用規約において同意を得る手法については、同意前に取得した個人データの第三者提供は難しいと思料されるものの、今後のために利用規約で情報提供の同意を取ることは有効であり、企業に対して「ビジネスを進める上で個人データの提供に関する規定を設けることが重要である」と発信することは効果的である。
・　割賦販売法に規定されている指定信用情報機関と同様に、法改正等によって JC3 等で情報集約等を行うことを可能とすることも考えられるのではないか。
・　各企業が個人情報保護に重点を置いて対応することはコンプライアンスの観点から重要である一方、不正利用に関しては、出来るだけ早い段階で正確で具体的な情報を警察や他の事業者に共有することが犯罪抑止の上で極めて重要ではないか。
・　個人情報保護法第 27 条第 5 項第 3 号に規定される個人データの共同利用の枠組みを活用した企業間の万引き対策の取組があり、議論の参考になるのではないか。

・　前述の取組は、犯罪の疑いのある情報を事業者間で共有し、更に確度が高い情報については第三者提供の制限の例外として警察に情報提供する仕組みとなっており、EC 事業者間の情報共有についても、JC 3 も含めて共同利用の枠組みを設定し、警察への第三者提供について JC 3 の協力も得ながら判断していくという形式がよいのではないか。
・　警察への提供と同様に JC3 への情報提供を想定している場合、個人情報保護法第 27 条第 1 項第 4 号に基づいて実施することは難しいので、同項第 1 号・第 2 号又はサービス利用者からの同意を活用すべきではないか。
・　個人情報保護法第 27 条に規定される例外への該当性の判断において、実質的な要素として、提供の公益性及び本人の権利利益への侵害の程度も判断要素として加えることはできないか。
・　銀行間の送金については不正送金対策が進展しているところ、暗号資産口座に対する送金についても対策を推進するよう銀行側と連携することが重要ではないか。

【その他】
・　メールを送付する際にリンクを貼らないことをビジネス上の慣行とすることも、有効なフィッシング対策となるのではないか。
・　フィッシングサイトを ISP 等に情報提供する取組を行っている各機関、ボランティア等の活動を拡大するための取組を検討するべきではないか。
・　フィッシングサイトをなくす取組は重要である一方、フィッシングサイト通報の枠組みが競合事業者への妨害に悪用されないようにすることが必要ではないか。
・　多様なアプリストアが認められることで、不正なアプリのダウンロードが増加する可能性があることから、今後の動向を踏まえた注意喚起等についても検討すべきではないか。

(3)　閉会