第２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 12 月 22 日（金）午前 10 時 00 分から午後 11 時 45 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

(2)　議事

○　事務局説明

事務局及び欧州サイバー犯罪センター（ＥＣ３）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。

【生成 AI 等の活用によるフィッシング対策の高度化・効率化】

・　生成ＡＩを活用してフィッシングサイトを検知することは有効な対策である。通報のあったフィッシングサイトを生成ＡＩで自動判定するほかにも、事業者等において、フィッシングサイトのソースコードを取得して他のフィッシングサイトの自動判定を行うことや、フィッシングサイトに流用されやすい要素に着目した自動検知も考えられる。また、フィッシングサイトはクローキングによって対策者側からアクセスできないようにされる場合もある点に留意する必要がある。

・　フィッシングサイト情報の提供を受けるフィルタリング事業者等においては、実施する対策に応じて必要となる情報の精度が異なるため、フィッシングサイトの検知に生成ＡＩの活用を開始する際には、判定の精度に関する情報が付加されていると有用ではないか。また、提供される事業者側で使いやすいデータ形式についても検討していくべきではないか。

・　生成ＡＩによってフィッシングサイトを判別した際、誤判定によって正規のサイトに対して警告表示が行われた場合に、サイト運営者等から是正申告を受け付ける連絡先を警告表示の中に示すなどの救済策を準備することが必要ではないか。

・　ＪＣ３等の民間が保有するフィッシングの検知・分析に関するノウハウを、フィッシングサイト対策に活用できるのではないか。

・　既にＡＩを活用して対策を実施しているブラウザ事業者等に対して、警察や各事業者が把握・研究した手口等を学習用データ等として提供することで、ブラウザにおけるフィッシング対策の高度化に役立つのではないか。

・　犯罪者側が生成ＡＩを悪用することにより、フィッシングサイトの増加やフィッシングに係る手口の巧妙化の懸念があるところ、関連団体や民間事業者と連携して先端技術を活用した攻撃手法の研究を行うことが必要ではないか。

【被害企業等との情報共有による捜査の推進】

・　事業者においては、社会的な批判等を懸念して、利用規約等で第三者提供について同意を得ている場合であっても、個人情報保護法第 27 条第 1 項に該当する場合等に限って、警察に対して最小限の情報提供を行うとするところもあると考えられるところ、財産の保護のために情報提供をする蓋然性が高いケースについて、考え方が整理されていることが望ましいのではないか。

・　ＥＣ事業者等から警察への情報提供について、個人情報保護委員会の Q&A やガイドライン通則編に、個人情報保護法上の整理を明記することが望ましいのではないか。

・　規模やサービスが異なる中で、全ての事業者に適用可能なガイドラインを作成することは時間を要すると考えられるため、まずは個別の事業者等と連携して、どのようなケースであれば情報共有できるのか整理することも重要ではないか。

・　１件の被害額は小さくとも、サービスを横断して組織的に不正行為が行われるケースがあるため、警察において情報を集約・分析して捜査に活用することが重要ではないか。

・　ガイドラインの検討には時間を要するので、個別ケースを進めるのと並行して早めに始めるのが良い。国際動向も踏まえる必要があり、まずは、諸外国において、セキュリティ上の理由等で同意を必要とせずに個人情報等の共有が法令上認められている例について研究を実施するべきではないか。

・　民間事業者が保有する犯罪者の特定に資する情報の選別や、民間事業者から警察に提供する際の効率的・効果的な手段の検索、提供された不正に関する情報の分析等についても、AI 等を活用して高度化すべきではないか。

【国内外の関係機関等との連携強化】

・　ＥＣ３が関係団体と連携してフィッシングサイトのテイクダウンを進めているところ、ＪＣ３でもフィッシングサイトの通報支援ツール「プレデター」を学生ボランティア等に提供しテイクダウンの取組を推進している。abuse 通報はボランティア等の民間でも安全に実施できるので、参画者を増やしていくべき。また、フィッシングサイトの被害事業者に対しても、フィッシング対策協議会や JPCERT/CC への通報に加えてプレデターの活用という新たな選択肢を示せることは有効ではないか。

・　民間事業者からブラウザ事業者等にフィッシングサイトの情報を提供しても、審査に時間を要して、フィルタリング等に迅速に反映されない実態があるため、ブラウザ事業者等と警察等の公的機関が連携して、公的機関が被害事業者等から把握した情報をブラウザ事業者等に提供し、優先的に審査を行いフィルタリング等に反映してもらう枠組みを設ける必要があるのではないか。

【捜査等により得られた情報の活用推進】

・　クレジットカード番号だけでも提供側にとっての個人情報に該当することに留意が必要である。クレジットカード番号等を国際ブランドに提供する場合、国際ブランドが海外の第三者ということであれば、個人情報保護法第 71 条の保有個人情報の越境移転に関する規定が適用される可能性があるが、利用目的の範囲内であれば特段の規制等なく提供可能であると考えられる。

・　侵害された可能性のあるクレジットカード情報について、クレジットカード会社（イシュア）が警察等から情報提供を受けた際の対応方針について、経済産業省等と連携しながら明確にするべきではないか。

・　これまで国際ブランドやイシュア間でやりとりしている情報は、悪用されたことが事業者側において明確なものであるところ、警察から漏洩した可能性のある情報が提供されることは有効な対策であると考えられる。他方、既に事業者側で把握している情報とも重複が生じる可能性がある点には、留意が必要である。

・　警察が把握したクレジットカード情報の国際ブランドへの提供については、日本法人のリソースの面から対応が難しい可能性もあると考えられる。警察が把握した情報をセキュアな環境に保管し、各イシュアが確認できるような環境を構築することも有効ではないか。

【その他】

・　サイバー空間でのフィッシングやクレジットカードの不正利用等は、現実世界における通貨偽造にも相当するような性格の犯罪とでもいうべきであり、それへの対応が十分にできていないのであれば、サイトブロック、強制力のあるテイクダウン等、現代の社会状況に対応した刑事手続の在り方についても、長期的には検討していくべきではないか。

・　EC 3 の説明にあったとおり、事業者が講じる技術的な防御策をすり抜けて、電話、なりすましメール等で利用者を騙そうとする攻撃によって被害が発生していることから、利用者への啓発等の対応も継続して実施していくべきではないか。

・　海外の関係機関と連携する際には、各国の制度を踏まえて対応する必要があることから、国際動向も踏まえた対応を検討することが長期的な課題ではないか。

(3)　閉会