

第3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6年2月28日(水) 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 葛大輔

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。

【被害者に直接届く注意喚起の実施】

- ・ 幅広い年代が被害者となっていることから、年齢に応じてタッチポイントが異なる点を踏まえ、時期・ターゲットを絞り、動画サイト、デジタルサイネージ等様々な媒体を効果的に活用して注意喚起を実施する必要がある。また、深刻な被害が発生しているインターネットバンキングに係る不正送金においては、売買された金融機関口座が悪用されているところ、若者や外国人が犯罪の認識なく口座を売っている実態がある。出入国在留管理庁と連携した取組について、こうした背景も記載いただきたい。
- ・ 本年2月、警察庁、都道府県警察、消費者庁、国民生活センター、EC加盟店等が連携して、犯罪につながる副業募集についての注意喚起を実施した。社会に対して広く浸透させるため、こうした各組織が連携した注意喚起を、一度だけでなく繰り返し実施することが重要である。
- ・ 犯罪者側によって標的とされるサービスが変化していく中、企業単体での広報等には限界があるため、今後も官民連携による業界横断的な注意喚起等を積極的に実施していただきたい。

【フィッシングサイトにアクセスさせないための方策】

- ・ 一部の金融機関ではフィッシングサイトのテイクダウンを積極的に実施している一方、他の事業者、公的機関等においてテイクダウンの取組が広がっていない状況である。このため、消費者保護に向けて各事業者が自らテイクダウンを実施することが望ましい旨についても報告書に記載いただきたい。また、関係省庁においても、所管事業者に対するフィッシング対策の必要性に関する広報・啓発を推進いただきたい。
- ・ パスキーを普及して広く利用されるようにするため、本報告書に記載を盛り込むことは重要である。他方、全ての利用者がパスキーに完全に移行しない限り、ID・PWによるログインが存在することでフィッシング被害の可能性があるため、利用者自らがID・PWを入力しない仕組み、例えばパスワードマネージャーの利用といったものも、パスキー導入の下地作りも兼ねて推奨するべきではないか。

- ・ パスキーの導入について、特に中小事業者では ID・PW 形式から変更することも負担であり、補助金の活用等を含めて関係省庁と連携して導入を推進していくことも検討すべきではないか。
- ・ JC3 主催のチャレンジカップは非常に有意義な取組であり、今後もこのような取組について積極的に推進していただきたい。

【ID・PW を窃取された場合でも被害に遭わないための方策】

- ・ フィッシングは各フェーズで被害者が異なり、例えば、知的財産権等を侵害される企業、個人情報の窃取や金銭的被害を受けるサービス利用者、不正アクセスを受けるサービス提供事業者、チャージバックによって金銭的被害を受ける EC 加盟店等が挙げられる。これを念頭に、どの場面でどの主体と連携して被害防止対策を推進するか検討すべきではないか。
- ・ EC 事業者等が警察への情報共有が抑止的な理由については、社会的な批判等だけでなく、一般顧客のプライバシーの保護に配慮していることもあるため、その点を踏まえた報告書の記載としていただきたい。
- ・ プライバシーの保護は事業者にとって重要な観点であるところ、昨年作成された「サイバー攻撃被害に係る情報の共有・公表ガイダンス」では、技術情報と被害内容対応情報を切り分けて共有・公表することを整理しているので、参考としていただきたい。
- ・ 不正取引に関する情報について、個人情報保護法上の個人データに直ちに該当しない場合であっても、行動履歴や位置情報といった情報を無制限に共有することには問題があるため、事業者等における負担には留意しつつ、透明性を確保することに重点を置く記載としていただきたい。
- ・ EC サイトが不正取引に関する情報を警察に提供する取組について、警察との連携を犯罪抑止に繋げる趣旨は残しつつ、犯罪が多発しているといった負の印象を与えない表現を検討いただきたい。
- ・ 個人情報保護法の第 27 条第 1 項第 2 号に基づいた情報共有に関する記載については、本人同意がない場合の話なのか、本人同意の有無に関係ない話なのかといった点や、個人又は企業の財産保護に関する話なのか、といった点を可能な限り明確化して記載すべきではないか。
- ・ 個人情報保護委員会のガイドライン等に、警察への情報提供に関する記載を追加することは非常に重要であることから、警察庁において個人情報保護委員会事務局と実現に向けた調整を実施することに期待する旨も報告書に記載いただきたい。
- ・ 不正利用に関する警察との情報共有について、個人情報保護委員会で作成しているガイドライン等に記載があれば、事業者側はより安心して警察との連携を進めることが可能となるため、その点を踏まえて報告書を作成いただきたい。

- ・ 個人情報保護委員会のガイドライン等に関する記載について、民間研究所等の協力を得て一般顧客の権利を不当に侵害しないデータ共有の在り方を検討することも考えられるのではないかと。
- ・ 警察に情報共有を実施しているからとあって、事業者における被害防止対策が不要となる訳ではないため、経済産業省から導入必須化の方針が示されている EMV3-D セキュア等、事業者側での不正決済防止に向けた取組の必要性も記載した方が良いのではないかと。
- ・ 本年2月、金融庁と警察庁で連携して、暗号資産交換業者の不正送金について要請がなされているところ、暗号資産が各種事案に悪用されている状況においてこうした取組は非常に重要である。要請事項が形骸化することのないよう各都道府県警察が地方の金融機関と連携するなど、警察庁や金融庁、全国銀行協会等が協力し、全ての金融機関で取組を実施することが求められる。
- ・ 実空間における被害防止対策として、コンビニ等の店舗における対策は非常に重要である。「渋谷書店万引き対策共同プロジェクト」が実施している、個人情報保護法第27条第5項第3号に規定される枠組みを活用した個人データの共同利用等の取組を参考に検討していただきたい。

【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】

- ・ 犯罪者側が AI を悪用するといった観点や、具体的な事例は不要であるが警察も対抗して AI を活用し始めているといった観点についても報告書に盛り込んでいただきたい。

【被害企業等との情報共有による捜査の推進】

- ・ 個別事業者における被害は小さくとも、社会全体として大きな被害が発生している可能性があるため、警察に情報共有して捜査及び被害防止対策により犯罪者集団の排除につなげることが重要である。
- ・ 警察における捜査に向けた被害企業からの情報共有が十分でない理由として、プライバシー保護等に加えて、令和4年度に開催した「サイバー事案の被害の潜在化に向けた検討会」で議論されたとおり、警察側の対応に問題があるケースもあると思料されるため、その点も御承知いただきたい。

【国内外の関係機関等との連携強化】

- ・ フィッシングサイト等に係る公的機関からの情報提供について、ブラウザ、SNS サービス等を提供するプラットフォーム事業者側においても積極的に受領して活用することが期待される旨の記載を追加いただきたい。
- ・ フィッシングサイトを立ち上げにくくする環境作りも国際的に進めていくべきであり、ドメインの不正利用対策等を国際機関と連携して検討することを記載いただきたい。

- ・ 総務省でも、「不適正利用対策に関するワーキンググループ」が発足しているところ、同WGとも連携して取組を推進する旨を記載していただきたい。

【捜査等により得られた情報の活用推進】

- ・ 警察が保有している捜査情報は事業者では得がたいものであり、事業者における被害防止対策に大いに活用できる可能性がある。このため、警察からフィードバックを受けられることは、事業者から警察への情報共有のメリットにもなり得るので、警察からの情報提供に向けて検討を進める旨が報告書に記載されていることは重要である。他方、提供する情報の具体的な内容や配慮すべき点については今後更に検討していく必要がある。
- ・ 捜査等で把握したクレジットカード番号等の情報共有による被害防止対策について、知見を有する経済産業省とも連携して推進いただきたい。

【その他】

- ・ 警察に対してフィッシングサイトをテイクダウンする権限を付与する記載について、「将来的な法制度のあり方を検討する」といった記載としてもよいのではないか。

(3) 閉会