令和３年２月８日

令和２年度サイバーセキュリティ政策会議（第４回）
発言要旨

１　開会

２　金融庁発表「資金移動業者等を通じた銀行口座不正出金事案を踏まえた対応について」

【金融庁から、「資金移動業者等を通じた銀行口座不正出金事案を踏まえた対応について」の発表後、質疑応答】

委　　員：資料において、「資金移動業者のアカウントと銀行口座を連携して口座振替を行うプロセスに脆弱性がないか確認する」とあるが、銀行側（ＡＰＩ提供側）、フィンテック企業側（ＡＰＩ利用側）の双方に課題があり、難しい領域であると考える。

以前調査したところ、銀行側が個人情報等をそのままＡＰＩで提供してしまうことがあったり、フィンテック企業側も、ＡＰＩに対するＤＤｏＳ攻撃の被害を受けたり、暗号化されていないプロトコルを使用したため攻撃者に情報が窃取されるなどの問題があったかと思われるが、資料中の脆弱性がないか確認するという点について、具体的な確認の手順等を通知等することは検討されているのか。

金 融 庁：資金移動業者と銀行間の連携サービスについては、双方共に相手方が十分にセキュリティを確保しているという想定の下、連携サービスを提供していたことが問題であった。今後は、連携してサービスを提供する以上、自らが提供しているサービスに係る部分のみならず、相手方のセキュリティ状況も含めてしっかり確認することが顧客保護の観点から重要であると考えており、必要であれば具体的な手順等についても検討してまいりたい。

委　　員：資料のｅＫＹＣの説明において、「資金移動業者と銀行間において本人確認情報の照合を行うことを検討」との御発言があったが、安全性の部分や、情報の取扱い等に関して、犯収法をはじめとした関連法規の改正等が必要かお伺いしたい。

金 融 庁：現在も口座振替契約を締結する際に、銀行、資金移動業者双方において、本人確認情報の照合を実施しているところ、今後は自主規制団体が定めるガイドライン等により照合する項目を増やすようお願いをしている状況であり、犯収法を改正することは現時点では検討していない。

委　　員：本人確認のタイミングについて、決済単位で実施するなど、現状よりも厳

しくすることを考えているか。

金 融 庁： 現状、被害が発生した資金移動業者の本人確認方法は、当該事業者自らが本人確認をするのではなく、銀行において本人確認済みか否かを確認するものであった。すなわち、銀行が口座振替契約に関して行う認証と、資金移動業者が行う認証が同一のものとなり、かつ、その認証をキャッシュカードの暗証番号で実施していたことに問題があったと認識している。そのため、当庁としては、銀行の認証強化に加え、資金移動業者において公的個人認証やｅＫＹＣ等により自ら本人確認を行うこと等の不正防止策を実施することをお願いしている。

さらに、預金口座と資金移動業者のアカウントが紐付いた後についても、認証した端末と異なる端末からアクセスされた場合に、改めて認証を実施すること等も重要と認識している。

委　　員： 資料記載の業界指針について、不正防止策の実施に係る「リスクの検証」とは、システム構築時における、脅威分析とセキュリティ・バイ・デザインということになると思う。また、本人確認と不正モニタリングという点について、金融庁監督下の事業者にとどまらず、同様のシステムを抱えている業界に対して広く適用できるものと考える。

金融庁は、関係省庁と連携し、預金者向けに注意喚起を実施していると思うが、インターネットバンキングの利用者に対し、入出金等の取引がなされた際にメールで通知するサービスを銀行等の事業者に推奨しないのか。

金 融 庁： 預金者が不正な取引があった際に気付いていただくことは非常に重要であると認識。まず口座連携を行う際には、資金移動業者又は銀行から、銀行に登録されている顧客の連絡先に通知することが重要と考えている。その上で、個別の取引についても、可能な範囲で通知をお願いしている。

委　　員： 資金移動業者関連事案の被害者側の立場からすると、金融庁の呼びかけは大変ありがたい。これまで、複数の事業者が連携してサービスを提供する場合、どの事業者に問い合わせるべきか被害者には分かりづらかった。そのため、ともすると、銀行と資金移動業者の間でたらい回しにされるケースも多々あったかと思う。連携してサービスを提供する場合、サービス全体のリスクを検証し、責任分担についても連携する事業者間でよく話し合うよう呼びかけをして頂いたことは、大変ありがたい。

他方、事業者のいずれが負担するかに関わらず、被害者は補償が行われた段階で満足してしまい、根本的な原因である犯人の存在に思いが及ばないという問題もある。金融庁から、犯人の検挙のために、警察に対して情報提供を積極的に行うよう事業者側に依頼しているか。

金 融 庁： 今までの事案についても、警察としっかり連携を取り、対応させていた

だいているところ。

資金移動業者等に対しても、警察に速やかに情報提供を行い、協力するようにお願いをしている。今後ともしっかり連携していきたい。

委 員 長： キャッシュレス決済サービスの不正利用事案の発生状況は如何か。

事 務 局： 当該事案と同様の手口は、今のところ収まっている。事案発生時は、早い段階から金融庁と相談し、資金移動業者においても非常に前向きな捜査への協力を頂いた。

委　　員： 資料にもリスクの検証とあるが、リスクアセスメントをしっかりやっていくことが重要であると認識。単独の不正に係るリスクは比較的容易に評価できる一方、高度・複雑な攻撃に対するリスク評価はなかなか難しいと思う。リスク評価の実施手法などを含めて、注意喚起していく必要があると考えている。

委 員 長： 各省庁においても様々なレベル・観点から対応する様心がけていかなければならないと考えている。

３　令和２年度サイバーセキュリティ政策会議報告書（案）について

【事務局から、令和２年度サイバーセキュリティ政策会議報告書（案）について発表後、質疑応答】

委　　員： 報告書内のスミッシングに係る解説をより分かりやすくお願いしたい。

また、テレワークに係る記載について、テレワークをされる方がすべからくリモートデスクトップ機能を用いて行っている印象を受ける文章となっており、実情と異なることから表現の修正をお願いしたい。

委　　員： 報告書における公共空間という語についてコメントしたい。サイバー空間やインターネットは、物理空間における公園や公道といった公共空間とは若干異なっていると感じている。私道の様な私的な設備の集合体がサイバー空間を形成しているのではないかと思う。

そういった理解の上においてなお、サイバー空間が公共的な非常に重要な役割を担っているというのが今回の報告書の記載の趣旨と理解しているが、何らかの追記をして頂いた方が良いのではないか。

委　　員： 本日の金融庁発表の本人確認については非常に有用な内容でもあったことから、報告書に追記頂いた方が良いのではないか。また、今回、報告書で得られた知見を役立てていくため、社会に発信していく枠組みが有れば良いと考えるので検討頂きたい。

事 務 局：　警察として情報発信を行うことは重要と認識。報告書の内容等を踏まえ、警察庁としてどのような対応をすべきか検討してまいりたい。

委　　員：報告書に関しては、意見はないが、むしろ、報告書を踏まえてこれからどう取組を実行していくかが重要である。特に今回のテーマにもなっている官民連携の推進について、具体的な方針があればぜひお伺いしたい。

委 員 長：報告書の作成で終わるのではなく、次の展望を見据えながら取組を継続していくことが重要であると思う。委員からの御指摘については、次回、事務局から説明頂ければと思う。

委　　員：報告書全体についての感想として、サイバー空間をどのようなものと認識していくか、共通の認識を持つことが非常に重要と思う。

その中で情報提供について一言。本法人においても、情報発信、情報提供を一般国民の方に向けて実施しているところ、警察でなければ難しい情報発信、情報提供もあると認識している。

報告書中に刑訴法４７条を踏まえた情報発信の強化についての記載があるところ、一般国民に向けた情報発信であるのか、あるいは対象となる業種等を絞って発信するのかなどにより事情は異なると思うが、情報発信の必要性が認められる場合、相手方の適切な情報管理の前提の下、積極的に発信していくことが重要と考える。本法人においても、警察と連携し対応できればと考えている。

事 務 局：サイバー空間の脅威に対応していく上では、まず情報共有と適切な情報発信というものが不可欠の要素だと考えている。刑訴法４７条の規定も踏まえつつ、今後、的確に情報共有・発信を進めていくべきだと思う。

他方、まだ我が国では情報を共有する、特に機密性がある程度高い情報を共有する土台となるような情報管理の仕組みが十分整備されていない現状があり、これも課題であると認識していることから引き続き検討を進めていくべきと考えている。

また、委員の御指摘のとおり、サイバー犯罪の被害に遭った方々が警察への相談、情報提供等を躊躇する状況もあるため、より相談しやすい環境を整備し、警察が的確に情報を得られるような仕組みを構築することについても併せて取り組んでまいりたい。

委　　員：　サイバー空間は、私的な領域の集積としての空間である一方、公共空間としての機能を果たしているとも言える。実社会であれば、交通検問や防犯カメラの設置により監視できるが、サイバー空間で同様のことができないという現状も、私的領域の集積としての性質故であると思うが、この部分はサイバー空間上の捜査活動における１つの隘路になっているのではないかと考えている。こういった中でも、サイバー空間に対する攻撃が不特定多数に影響を及ぼすという現状を鑑みれば、対応を考えていかなければならないと思う。

委 員 長： これまで様々な議論をしていただいたが、特に警察庁が重く受け止めるべきことは、委員から御指摘があったように、国民の常識的な感覚からしても、真に問題があるのは被害にあったサービスを提供していた事業者ではなく、犯罪を犯した犯人であり、これを捕捉しなければならないという点であると思う。

今回の報告書においても、アトリビューションの強化を掲げているが警察においては組織全体を挙げて犯人を探求し、それにより国民の期待に応えていくことが必要である。

４　閉会