令和２年 11 月 18 日

令和２年度サイバーセキュリティ政策会議（第２回）
発言要旨

１　開会

２　第一回会議における御発言の整理等について
【事務局から、第一回会議における御発言の整理等について発表】

３　ＰａｙＰａｙの取組と不正利用の実態について
【有識者から、ＰａｙＰａｙの取組と不正利用の実態について発表】

４　ドメインレベルでのセキュリティについて
【有識者から、ドメインレベルでのセキュリティについて発表】

５　サイバー犯罪捜査における犯人の事後追跡可能性の確保について
【事務局から、サイバー犯罪捜査における犯人の事後追跡可能性の確保について発表】

６　質疑

委　　員：　有識者より、ＳＭＳ認証代行による不正なアカウント作成、警察庁より匿名化技術における Proxygate の説明があったが、この様に犯罪に悪用される技術・サービスに対し、先行して対策を行っていくことが、健全なサイバー空間の実現につながっていくと考える。

また、事業者が行っているポイント還元キャンペーンに係るポイントの不正取得は、事業者にとって非常に大きな問題であると考える。報道によると、中国では、2017 年に、羊毛党（ヤンマオダン）と呼ばれるグループが、ＥＣサイトなどの提供する少額のポイント還元キャンペーンを標的に大量のポイントを不正取得したという事例も確認されている。

この様な事案を防ぐためのキャンペーン制度設計に係る対策について、助言できることがあれば、御紹介願う。

事 務 局：　委員の御指摘のとおり、犯罪の実行に際しての匿名化手口の１つとして、Proxygate が悪用されており、対策を検討する必要があると考えている。

一方、例えばウイルスに感染し、知らない間に踏み台にされ、意図せず犯罪に加担してしまうという事例もあることから、対策は関係省

庁や関係団体とともに慎重に検討していきたい。

また、ＳＭＳ認証代行については、埼玉県警において、事業者の規約に反して電子決済アカウントを不正に取得した事案に関連してＳＭＳ認証代行を行う者が摘発されるなど、犯罪に悪用されている実態が明らかとなったところ。

デジタル化が進む中でＳＭＳ認証を利用し、本人確認を強化するという流れもあるところ、本人確認の正確性を毀損する悪用事例があるという点について情報発信を行い、社会全体として対策が講じられるよう働きかけていくべきと考える。

有 識 者：　弊社に限らず、事業者では不正行為により得られる利益が高くならないように制度設計を行っている。具体的には、キャンペーンで付与されるポイントの上限額を抑える、ポイントが付与される回数を制限するなどの対策を実施している。

加えて、モニタリング体制も重要であり、決済の態様から不正を見抜き、ポイントを付与しない取組も実施している。

委　　員：　キャンペーンの制度設計において、ポイントの上限を抑えるということであったが、中国で報告された羊毛党の事例では、少額のポイントをかき集め、収益を上げる手法が取られており、ポイントの上限を抑えるということだけでは、対策は難しいと思うが、この点についてはいかがか。

有 識 者：　御指摘の手法については、日本では現時点であまり見られないが、実際に１件５００円のポイントを不正にかき集めるため、２万枚程度のＳＩＭを使用したという事例も確認されていることから、これに対する有効な対策を引き続き検討することが必要と考える。

委　　員：　有識者の説明において、ＳＭＳ認証による本人確認に関し、ＭＶＮＯ事業者に問題があるという話があったが、具体的にどの程度の問題なのか。

また、ＭＶＮＯ事業者との意見交換や検討の場を設けたことはあるか。

有 識 者：　ＭＶＮＯ事業者については、本人確認を適切に行っていない事業者もあるところ、不正が発生した場合に犯罪者にたどり着きづらいといった問題があるほか、データＳＩＭの入手手続が容易であるため、犯罪者が不正にＳＩＭを入手するハードルも低くなり、犯罪につながりやすくなっているという課題があると認識している。

ＭＶＮＯ事業者との接触は、これからの課題と考えている。

委　　員：　ＰａｙＰａｙにおいて、事業者側としてできる限りのことを全てや

られていると思うが、ユーザーサイドに対して最低限実施してほしい対策があればお伺いしたい。

有 識 者：　まずは、怪しいサイトに自分の情報を入力しないということが、重要だと思う。また、怪しいメールを開かないといった基本的な対策も、被害を防ぐ手段として重要であると考える。

委　　員：　２点申し上げたい。

１点目は、犯罪捜査の障害について。ログの保存義務や本人確認義務の強化等について、規制を強化できれば、犯罪捜査を適切に進めることが出来るといった点もあると思うが、実際に規制強化を実施するとなると、事業者側のコストの問題や、利用者等の利便性が落ちるといった点からの反対も予想されるほか、通信の秘密やプライバシー保護との関係等、様々な主体との間における価値判断の対立が起こると思う。

この様な価値判断の対立の中で、どの様にバランスを取っていくかという点は、省庁単位で縦割りにせず、国民に見えるところで、オープンに議論を行い、知見を結集し、適切に進めていただきたいと考える。

２点目は、海外対策について。サービスがグローバル化する中で、国内法の整備だけでは、捜査や法執行の場面で、国境を越えることが難しいという実態は理解できる。この様な状況では、国際協調が重要となるが、現状のサイバー犯罪条約等がどの程度有効に機能しているのかお伺いしたい。

委 員 長：　御指摘があった点は非常に重要。事後追跡を可能にして、不正利用をいかに抑止するかという面と表現の自由といった観点は昔から対立がありながらも、ログの保存の議論等バランスをとりながら少しずつ進んできた。今後、日本が世界から見て遅れているデジタル化を進めるという流れにおいて、国民が安心して使える様になるセキュリティの確保は最大の課題であり、バランスをとりつつもしっかりと対応してほしい。

事 務 局：　サイバー犯罪条約については、成立から長い時間が経ち、その間にも、サイバー犯罪をめぐる国際情勢は、深刻化している。各国の関係機関と協力し、現在の条約に加え、より良い国際的な協調体制をどう整備していくか議論を行っている。

他方、サイバー犯罪条約の成立以後、例えば個人情報保護におけるヨーロッパとその他の国との間に見られる様に、意見の隔たりがあるという状況もある。日本では、外務省を中心に議論を進めており、警

察庁としても関係省庁と連携して、議論に参画していく。

委　　員：　今回の説明等を受けて、本人確認をどの様にすべきかという点が非常に重要であるという事が改めて理解できた。一方、「本人確認」という概念は身元確認と当人認証の２つに分けて考えることが必要である。ＰａｙＰａｙでは、身元確認まで実施しているのか、それとも当人認証のみで良いとしているのか、その考え方も含めてお伺いしたい。また、本人確認をする上で、電子メールに関してはＳ／ＭＩＭＥを導入すれば、詐欺等が、減少していくと思うが、なかなか普及しない。

Ｓ／ＭＩＭＥを普及させるために、警察庁において、ＰＲしていく、あるいは、サポートしていくということは考えられないか。

有 識 者：　決済事業者としては、決済サービスのアカウントを持っている当人と、そのアカウントに結びつけられている銀行口座、クレジットカードを持っている当人が、同一の人物なのかどうかというところが確認できればよいことから、身元確認までは実施せず、当人認証としている。

事 務 局：　Ｓ／ＭＩＭＥの普及も含めて、暗号化技術の普及・活用にはユーザーの利便性を確保することが重要であると認識している。

経済産業省や関係機関等が、これまでユーザーへの推奨等広報啓発を行ってきたと承知しているが、警察庁もタイアップすることを検討していきたい。

委　　員：　金融機関や決済事業者では、犯収法（犯罪による収益の移転防止に関する法律）に基づき、口座作成時やユーザー登録時に本人確認を実施されているが、将来的には、例えば、高額な決済が発生する場合にリアルタイムの本人確認を求めるといったこともあり得ると思うが、御意見をお伺いしたい。

有 識 者：　当社では、犯収法に基づき、アカウントに銀行口座を結びつける際に、本人確認を実施しているほか、一定の条件に該当する場合には、当社で改めてｅＫＹＣを実施している。

御質問のあった取引時における本人確認については、安全性の観点から選択肢の１つとして考えられるが、ｅＫＹＣを実施する際に数分程度を要するなど利便性の問題もある。ユーザーの利便性を図りながら、その様な仕組みをどのように組み込むかという点は今後の課題として認識している。

事 務 局：　本人確認制度は、金融機関に係るマネロン対策から始まったものであるが、対象が金融機関のみならず、他業界にも拡大したことを踏ま

え、犯収法として警察庁所管となった。

同法は、国際的な枠組みに基づくものであることから、国際的な情勢を踏まえる必要があるほか、リスクベース・アプローチといった考え方、産業界の動向等も踏まえながら対応を検討する必要があると考える。

委　　員：　リスクベース・アプローチを実施することを期待したい。複数の事業者間で連携できる仕組みがあれば、利用者や各金融機関の負担も軽減できると考えている。

事 務 局：　有識者より、ドメインレベルでのセキュリティについて発表いただいた。警察でも、ドメインネームサーバの機能不全により行政機関を含むWebサイトの閲覧障害が生じた事例を認知しているほか、サイバー攻撃やサイバー犯罪の捜査を進めていく上でも、匿名のドメインサービスが、事後追跡の障壁となるケースを何度も経験している。

また、社会的認知度のあるドメインが第三者に登録される、あるいは金融機関や非常に著名な組織と誤認識させる様な紛らわしいドメインを登録され、フィッシングサイト、詐欺サイト等に悪用される事例も増加しており、サイバー空間の脅威の一類型となっているところ。ドメインのセキュリティについても、議論していく価値が大いにあると考えている。この点について、委員の先生の御知見を頂戴したい。

委　　員：　かつては、当事者同士のドメインネームの紛争処理が大きな課題で、それは不正競争防止法の関係で一定程度解決されている。ただ、ドメインは、ある種の公共財であるが、サイバーセキュリティとの関係で、その登録が簡単にできることの課題については、これから重視していかなければいけないと改めて実感した。

一つ質問であるが、ドメインに関してはＩＣＡＮＮにより一括してドメインの資源管理が行われているということであるが、ドメインネームが適切に配分できているかということだけでなく、適正に使われているかということについては、一切関知しないスタンスなのか。

このようなドメイン管理構造の中に、ドメインの適正な管理という要素を落とし込む余地があれば、御教示いただきたい。

有 識 者：　ドメインは、ＩＣＡＮＮを主とした分配構造があるが、他の知的財産と違い、各国法がない。ＩＣＡＮＮに専門家や技術者が集まり、ポリシーを作成し、これに準じてドメインを使用していくという形で対応しているところ。

もともと、ＩＣＡＮＮ設立時の目的が、ドメインを分配して、経済を活性化する、ドメインを広く一般に広めてインターネットの通信を

活性化するという目的もあったことから、比較的簡単に、誰でも安価に取れるような仕組みになっている状況。

そのため、第三者がドメインを取得することも違法ではなく、転売することも違法ではない。しかし、それが原因となり、様々な問題が発生していることは事実。

ドメインの不正取得を阻止する方法として新ｇＴＬＤというものがある。各会社が独自のドメインを設定し、自分たちのドメインを特定の人だけに登録をさせることができるという仕組みである。これにより第三者の使用を防ぐことが可能となる。

委　　員：　会社や組織が変わり、ドメイン名を廃棄したところ、それを不正に使用されたといった例があるところ、その対応としては、ドメイン名を廃棄することなく一定期間保有し続ける方法が現実的と思う。

この様な危険性と対応手法を啓発する仕組み、あるいはＰＲ活動などは実施されているか。

有 識 者：　ＰＲ活動は、世間一般にはしていないが法人に対するドメインの管理方法のＰＲは行っている。

また、弊社では、どの程度アクセス数があるかを確認して、ドメインを廃棄することが適切か否かを説明するといったこともしている。

委　　員：　有識者の発表の中で、不正利用の検出に関して人と機械を併用して行っているという説明があったが、不正利用をどの程度事前に阻止できているのか。

また、事後追跡について、通信匿名化技術が悪用された場合、犯罪者の特定のハードルはかなり高くなると思う。警察としてどこまで、何ができるかということを含め、多角的に整理をし、検討する必要があると考える。

例えば、事業者側でアクティブフィンガープリンティング（ブラウザ上で Javascript 等を実行し、端末の情報等を収集する技術）を利用してもらうということも含めて検討しても良いと考える。

有 識 者：　当社としては、一定の閾値を設け、システム上で不正な取引を検知し、取引を遮断している。その割合は出していないが相当数の不正な取引を止めることが出来ている。

事 務 局：　事後追跡可能性について、委員御指摘のとおり様々な技術があることから、今後も情報収集・議論をしていきたい。

委　　員：　フィッシングについては、先ほど有識者からお答えいただいたように利用者側がやるべき事をやるということがまず必要であると考える

が、実際にはフィッシングが非常に多く発生していることから分かるように対策がとられていない状況である。利用者側にやるべき事をやらせるためにはどの様な活動をすれば良いのか、また、そのための研究・検討は行われているのか、お伺いしたい。

事 務 局：　御指摘のとおり、やるべき事をやっていただくためにどの様な働きかけをするのかという点は課題と認識しており、現在はフィッシング対策協議会等と連携して検討を行っている。

また、効果的な広報啓発については、事業者のサービスの中で対応いただけること等を総合的に考えて、粘り強く行っていくことが必要と考える。

委　　員：　本協議会としても、警察庁と連携するとともに、民間の技術者等からフィッシングサイトの報告をいただいて、セキュリティベンダー等に情報提供を行うことで被害拡大を防止する点に力を入れて、活動を行っている。

委 員 長：　これまでの議論を見るに、これからのデジタル化社会に向け、サイバー空間について、公共空間としての安全性を確保していくということの重要性は確実に高まっていく。この点は委員の皆様にも共有いただけたと思う。今後、12 月に第３回の会議を行い、１月には報告書のたたき台を考えていく必要があるが、ここからさらに具体的な議論を進めるための柱として、各委員から様々御指摘頂いたことを踏まえ、「犯行主体の特定を通じた犯罪対策・安全保障」、「サイバー空間の健全性確保」、「サイバー空間の安全を確保するための技術的・物理的措置」の３点があると考える。

この３点を軸に、第３回会議において、報告書のイメージをまとめて事務局から説明するようお願いする。

７　閉会