平成 29 年 12 月 22 日

平成 29 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．　レンタルサーバ等提供事業者における不正利用対策について

【事業者からの発表】

○（委員）　レンタルサーバの場合、例えば不正なアクセスがどこかのＩＰアドレスからあって、それに対して whois をかけたときに、そこに出てくるアドレスや管理者の名前は、どのようになるのか。

○（事業者）　発表の中で挙げた範囲のものは、全て弊社になる。

○（委員）　つまり、相手から何か反応があれば、御社は必ず把握できるということか。

○（事業者）　そのとおり。

○（委員）　先ほどＳＭＳ認証の話があったが、最近では、フリーＳＭＳというか、ＩＰ電話の番号とかを発信させて、自動的にＳＭＳをクリアするためのツールがサイトに多く載っているが、これらはブラックリスト化されているのか。

○（事業者）　その点は、弊社が利用している上流の電話認証のプロバイダー側に設けられている対策であると考えており、弊社ではその内情はわからない。

○（委員）　つまり、依頼している事業者側に不備があった場合、実際にはＳＭＳ認証が電話のユーザーとして本人確認をされた携帯電話や固定電話の番号の認証としては機能していないにもかかわらず、つながってしまっていることがありうるということか。

○（事業者）　そのとおり。

○（委員）　ＯＳを事業者側が管理できない状態になると、使っているユーザーが全部、セキュリティも含めて管理しなければならなくなるが、以前あった、コントロールパネルの脆弱性が出ると、一気に他のユーザーまで影響を受けるような攻撃を受けるといった場合のように、そもそも使われているソフトウエ

アに脆弱性が発見されときに、ユーザーに対する注意喚起や対策はどうなっているのか。

○（事業者）　ユーザーに管理いただいているものであるため、事業者側としては踏み込んだ注意喚起をしなくてもいいのではないかという意見も歴史的・社内的経緯としては存在していたが、火がつくときは一気に燃えてしまうので、どんどん注意喚起をしなければならないという認識に変わってきている。一方で、どういう流れで注意喚起をするのが良いかは難しいところで、注意喚起の内容によってはユーザーが迷って、コールセンターがパンクしてしまうということもあり、想定される影響の内容やどのくらいの利用があるかの推測のもと、一つ一つ事例を確認しながら注意喚起を実施している。手法としても、ツイッターで流すことから個別にメールを送ることまで、様々である。今後もさらに行っていかなければならないと認識している。

○（委員）　御社は、セキュリティ対策をしっかりと行われていると思うが、業界にはそうでないベンダーもたくさんいる。弱いところを悪用する外部の人と、確信的に利用する利用者、両方を捉える必要があるので、こういうところでやられている内容を周知し、うまく徹底して、故意かどうかはわからないがそのあたりをあまり考慮していないような事業者への策を行っていくことも必要だと思う。

○（委員長）　本人認証というと、例えばネットカフェでは業界団体があるが、横の連携や組織化という点では、他の事業者の情報はどの程度わかっているのか。

○（事業者）　セキュリティ・インシデントが検出された初期の頃は、直接こういう問題に力を入れて対応する必要性の認識が希薄で、社内にも対応する人間が乏しかった。さらに、その後、対策を行っていかなければならないとなったときに、そもそも、入ってくる情報がないという状態であった。業界でどのようなつながりがあるかということも担当レベルでわかっておらず、非常に苦労をした。その後、例えば、ＪＰＣＥＲＴコーディネーションセンターやＪＡＩＰＡ、業界の団体、あるいは中立の団体の方に色々とご紹介をいただくような機会を得て、ホスティング系の事業者も担当レベルでは連絡を取り合う場所がようやくできつつあるが、まだまだ活動の途中であると感じている。

○（委員）　ＩＣＴ－ＩＳＡＣとの関係が重要ではないかと思うが、どのような交流を持っているのか。
○（事業者）　ＩＣＴ－ＩＳＡＣとは、中の方との個人的なやりとりはあるが、個別のホスティング事業者としては、会費のことや、ＩＣＴ－ＩＳＡＣにはキャリアやＩＳＰの回線系の事業者が多くおり、ホスティングサービスの事業者からするとメリットがないこと、さらに、ホスティングの事業者で体力のあるところは非常に限られており、そうでない企業は、外に出すような人がいないとか、予算的にも厳しいといったこと等があり、別な路線で走っているという感じである。

【事業者からの発表】
○（事務局）　Abuse 対策の話の中で、「同意なくサーバ領域は入れず検知・不正の判断が難しい」とあったが、これは、実際にサーバ内に入っていかなければ、どのようなファイルが設置されているかはわからないということか。
○（事業者）　そのとおり。
○（事務局）　Abuse 対策の中で、「損害賠償請求のリスク」という話があるが、実際、様々な企業が社会的責任を果たそうと、そういった損害賠償請求とかのリスクを承知で思い切った措置をとっていることを考えると、こういったものは少し違う性格のリスクなのではないかと感じる。
○（委員）　インターネット上の本人認証の仕組みがあるといいなというのは、本当にそのとおりだと感じるが、個人認証等の様々な取組が始まってから十何年が経ってもできないのは残念である。
Abuse 案件に対する問い合わせをグループ内で適宜転送しているという話があり、問合せ元に金融ＩＳＡＣが入っていたので気になったのだが、これは、どのＩＰアドレスが Abuse に遭ったかという話であれば、どのホスティング企業が担当かは、分けられると思うが、アプリケーション側でのアタックがありましたよとか、そこに脅威がありますよという問合せが、例えば金融ＩＳＡＣ等から来た場合、その情報はグループのホスティング事業者各社に行くのか、それとも、例えば、別の組織があって、そこに行くのか、その辺の構造はどうなっているのか。また、こういった問合せの対応体制を含め、社内の対策を行

う場合、ＣＳＩＲＴという組織をつくっている会社が多いと思うが、御社にそのような組織は存在するのか。
○（事業者）　後半の質問は、Abuse 案件を懲罰する組織ということか。
○（委員）　ＪＰＣＥＲＴからアドバイスを受け、各業界や各企業で構成されるＣＳＩＲＴ協議会というものがあったり、サイバーセキュリティ基本法でも各企業がＣＳＩＲＴをつくることが望ましいということが書いてあったりすると思うが、しっかりした問合せ窓口をつくって運営しているのであれば、ＣＳＩＲＴと呼ぶかどうかは別として、それに類した組織や機能もあるのではないかと思うが実際のところどのようになっているのかということである。
○（事業者）　正式な組織としては存在しないが、グループ横断で関係各所から中心メンバーが集まって、組織化をしている。そこで、今起こっている問題の共有や、それに対する対策の方針等を協議し、各社に展開している。
○（委員）　前半の質問についてはいかがか。アプリケーション寄りというか、サーバのＩＰアドレスで区切れるような話ではなく、例えば、こういう脆弱性があるということや、Abuse の例があるという話について、ホスティング企業以外のグループ企業にも情報が送られているのか。
○（事業者）　そのとおり。今回の発表はホスティング事業者に絞って書いているが、グループ企業を含めて、全て一括で受けている。
○（委員）　最後に不正利用について言及されていたが、ここで言う不正利用とは、正規利用者が過失により踏み台にされるということなのか、それとも、確信犯で悪いことをしようとしていることなのか、あるいは、それ以外のことなのか、いずれのことを言っているのか。
○（事業者）　どちらもということで差し支えない。
○（委員）　そういった意味では、過失によって、あるいは、幾ら注意してもなかなか直してくれないようなユーザーもいれば、確信犯でやっている人もいると思うが、どちらの問題が大きいと考えているか。
○（事業者）　発生するセキュリティ・インシデントもその時々によって性質が変わるので、温度というのも時々で変わるが、悪意が存在するというところにおいては、後者の確信犯的にやられるほうをまず止めることが重要だと考える。

○（委員）　悪意を持って入って来る人を止めるために、最初の入り口である程度止めようということか。
○（事業者）　そのとおり。
○（委員）　逆に、過失とか意識の低い人に対して、教育や指導等の何か上手い手段は持っているのか。
○（事業者）　メールやメディアを使った定期的な啓蒙や、あるいは、乗っ取られにくい環境をいかに提供するかも重要だと思っていることから、一定のパスワードの強度を申し込みのときに強制させるといった対策を講じている。
○（委員）　損害賠償請求のリスクや免責という話が出ていたが、損害賠償責任をどういう場合に負わなければならないのか、詰めて検討をしているのか。契約上の責任の場合は当然、約款で一定の免責ができると考えており、そのときに、免責できるかどうかは、当該事業者の行為に過失がなければいいと思っており、注意義務を尽くし、他の利用者を守るために行った行為について、どこまで本当に損害賠償の責任が追求されるのかは、きちんと法律的に構成を考えた上で、約款でどこまで消費者契約法に基づく免責ができるのかということを詰めたときに、それほど大きなリスクはないのではないかと個人的には考えている。免責というのも、どういう法律的な責任で、どういう場合に免責がなければならないと考えているのかを少し詳しく説明いただきたい。
○（事業者）　具体例を示すと、最近、様々なものをつなぎ込んで、自分の銀行口座にアクセスを許可しているアプリケーションがたくさんあるが、その事業者が例えば弊社のサーバを使っていた場合、１日に何回もＡＰＩが走っているので、複数回アクセスがあり、それを、不正な本人のアクセスではないと判断して、止めてくださいという依頼があった場合、そのアプリケーション事業者のサーバを止めると、数万人、数百万人の方が利用できなくなってしまうということで、通知の上で止めることも難しく、実際に止めてくださいと言われたときに、止められないという状況は多々ある。利用規約に記載はしているものの、具体的なところまで記載しておらず、適用できるケースが現在は非常に少ない。また、約款への記載が今後どうなるかという法改正もあり、その点は非常に事業者として難しいと考えている。
○（委員）　今の話だと、止めた場合のリスクがある一方、止めてほしいと言

われているのに止めなかった場合のリスクが顕在化することはやむを得ないと判断しているということか。
○（事業者）　実際には、契約者の方に、このような連絡が来ていますけれども、止めてもいいですかと意見照会をしており、ここは前後の状況もあるが、真っ当な契約者であれば、すぐ調べていただけるので、連絡がとれないという状況になれば、止めるということもやっている。つまり、一切やっていないということではなく、その連絡をせずに、今やられているので止めてくださいと言われた場合に、瞬間的に対応できるかどうかということである。
○（委員）　リスク判断をして、個別のケースでは対応されているという理解でよいか。
○（事業者）　そのとおり。実際に止めているケースもある。
○（委員）　サーバやインフラというものを貸し出す、箱を提供するといったビジネスモデルの場合、完全にAbuseを防ぐことは難しく、何かしら残存リスクがあると思うが、そこに対して、一部、リスク移転しなければならない部分もあると思う。ここまでこうなったら手に負えないので、例えば、セキュリティベンダーに任せるとか、法執行機関に相談するとか、あるいは、何かあったらサイバー保険を活用するとか、そういったリスク移転という観点で何か行っていることや検討していることはあるか。
○（事業者）　最終的にはサーバを運営する事業者の責任を問われることが多いので、難しいところではあるが、保険への加入や、外部のセキュリティベンダーとの協力といったことは、日々、その範囲を広げながら、模索しながら行っているところである。
○（委員）　例えば、不正利用され、セキュリティベンダー等から悪用されたサーバ上のデータやログ、ハードディスクのイメージが欲しいと言われたときに、事業者側は、早く調べてもらいたいとか、事情は色々あると思うが、そのあたりをスムーズに進める方法等は何かあるか。というのも、御社の同業で、弊社側から連絡するとはね返されることが結構あり、しかるべき手順を踏んで、令状がないのであればと来ないでくれとか、１本数百万するハードディスクを買い取ってくれ等と言われるが、このようなことを言っていては、なかなか悪事はなくならないと思っており、日本を代表するサービスプロバイダーとして、

工夫されていることや、経験的なものがあるのではないかと思っている。
○（事業者）　明らかに不正な使われ方をしている場合や、利用者の許可・合意が得られた場合は、割と踏み込んで対応ができるものになっており、実際、弊社では、ハードディスクを買い取ってくださいであるとか、そういった対応は行っておらず、できるだけ協力して対応できるようにしている。

３．　仮想通貨交換業者における不正利用対策について

【事業者からの発表】
○（委員）　捜査関係事項照会について、年間何件ぐらいあるのか。というのも、２年前に前身となる会議で、捜査関係事項照会書の対応ということについて議論しており、弊社では全世界で大体 10 万件の捜査関係事項照会書を、例えば、ＦＢＩやニューヨーク市警、フランスの警察からいただき、９万 9,000 件は電子メールで、残りの 1,000 件は日本から郵便で来ているという状況で、ヤフーであれば１万 8,000 件、先ほど発表のあった企業も 400 件、つまり、毎日１通の郵便が来ているということであるが、そういう関係で何通かということを伺いたい。
　また、各県警に対する情報共有という話があったが、警察庁と各県警との情報共有というのは上手くいっているところもある。例えば、捜査関係事項照会書を各県警から受け取るに当たって、我々も幾つかのルールがあり、数年前、一時期、捜査関係事項照会書の宛て先がばらばらであったが、送り先を統一するよう警察庁から各県警に伝えてもらったところ、それ以降は統一されているので、そういう連絡の体制はとれていると感じている。
○（事業者）　捜査関係事項照会の件数について、正確な数字は今すぐ答えられないが、感覚的には、そこまで大きくはなく、１日に１件から数件といった感じである。実際の照会の流れは、まず、メールか電話で依頼が来て、その後、捜査対象のアドレス等が記載された書類が送られてくるといったフローである。大体の場合は、該当がないが、該当がある場合には、個人情報を渡すといったフローになっている。
○（委員）　御社では比較的最近、不正送金の事案が報道されたかと思う。仮想通貨交換業というのは、例えば東京証券取引所といったように、正に場の提

供をしている部分も確かにあると思うが、それ以上に、銀行のように顧客の資産を左右するための秘密鍵を預かっていて、その秘密鍵を、ユーザーに対して渡したＩＤとパスワード、さらに、最近ではワンタイムパスワードによって、ユーザーからの指示に基づいて出し入れしているという意味では、交換所であると同時に、交換所の取引をするための言わば銀行の機能を果たしていると思っている。この場合、不正送金事案というのは正にインターネットバンキングの不正送金事案と似ていると思っており、銀行でも二要素認証というのが完全には徹底されていないが、御社は対応されているということである。以前あった事件のときには、二要素認証自体を使っていないとか、知らないとか、そういう被害者側の証言だったと記憶しているが、二要素認証の導入の経緯や今の普及状況等はどのようになっているのか。

○（事業者）　現在、送付時の二要素認証は必須化しているが、以前は必須化しておらず、当該事件の際は導入していたが、告知が十分でなかったと言われている。当然、告知も今では行っており、かなりセキュリティレベルは担保されると思っている。

　また、金融機関では、大体の場合、地銀や信金がまず突破されて、そこから連続で不正が行われるので、全体としてセキュリティが強化されるといいなと思っている。

○（委員）　現在、御社で預かっている部分を預かり資産とすると、大体幾らぐらいになるのか。

○（事業者）　公開はしていないが、かなり大きいと思う。

○（委員）　その場合、利用者保護という観点で言うと、銀行並みにやらなくてはならない。スマホのアプリだけであれば、かなり堅牢性を担保できると思うが、パソコンとなるとかなり危険である。パソコンでも取引できるようなインターフェースになっているのか。

○（事業者）　パソコンでも取引できる。

○（委員）　パソコンでは使用したことがなかったが、先日、スマホアプリを使ってみたところ、本人確認ができないと言って返ってきて、かなり本人確認は厳密だと感じた。しかし、パソコンでも使えるとなると危険かもしれない。パソコンでもスマホでもできるとなると、ユーザーはスマホしか使っていなく

て、パソコン側で別の人が何かやってしまうということも起こり得る。この点、銀行等でかなり進んでいる部分もあると思うが、なりすましの対策等は何かあるのか。

○（事業者）　スマホとＰＣを比べると、おそらくＰＣのほうが不正は多いと思われる。一般的なマルウェアと言われるものがＯＳレベルで入ってしまうのは、ＰＣのほうが可能性は高い。当然、スマホも同じようにウイルスが入る可能性はあるが、現状、可能性としては低い。弊社としては、マルウェアが入ったパソコンで操作されると、当然、キーのログもとられていて、行動はとられているので、これは、仮想通貨に限らず、全ての取引、ありとあらゆる金融取引が筒抜けになってしまうという意味では、何かしら対策が必要だと思っている。その上で、二段階認証というのは非常に強力で、ネットバンキングでも、二経路認証であったり、三経路であったり、いろいろな施策がなされている。二段階認証を導入した後は不正ログインが非常に減っているので、パソコンとスマホの両方が必要であるというところで対策は行っており、当然、これで終わりではないが、マルウェアが入っている、あるいはフィッシングサイトに飛ぶといったところは、当局と協力して、フィッシングサイトを発見したら、当然、そのドメインを止める措置があるので、それをお願いし、マルウェアが入った場合は、そういったものを使わないように注意喚起をするといったところで対応をしている状況である。

○（委員）　先日、これは本当かどうかわからないが、御社の数値を見ていたある事業者が、瞬間的に、合法的だがおかしな取引をしたことがあったと聞いている。こういったものは、それを見ている方が悪いと思うが、例えば、偽の買いを入れていって、価格を故意に動かすといった組織的な犯罪等に関して、モニターやその他の手を打ったりしているのか。

○（事業者）　まず、御指摘の事例に関しては、弊社はその事業者と契約関係がなく、また、もし仮にこの件が事実だとすると、当社の利用規約違反になる。我々の価格を参照して何かサービスをするということは、業法に抵触する可能性がある。さらに、利用規約で明確に禁止をしており、弊社としては困っているという状況である。価格を不用意に動かすとか、意図する価格形成がされないということについては、もちろん、明らかに相場操縦をするといったものは、

監視をしている。しかし、この点については、法律、自主規制といったところで、ガイドラインが定まっていないということも事実であり、今後、自主規制団体や金融庁で、不正な取引といったものもルール作りをし、運用する必要があると思っている。

○（委員）　相場操縦に関して、基本的に、資金決済法にはそもそも、相場操縦やインサイダー取引を違法であるとする、いわゆる金融商品取引法的な規制はない。したがって、通常の意味での相場操縦やインサイダー取引が仮にあったとしても、民事であれば話は別だが、少なくともそれは資金決済法上の罪には問えないという理屈になると思われる。この点については、昨日、米国のＧＤＡＸとコインベースが大量のビットコインユーザーから訴追を受けており、これは、インサイダー取引あるいは相場操縦的なことがあり、これに取引所の内部の人間が加担したのではないかということで訴訟事件になっている。これも 33 年法や 34 年法という米国の法律の直接の対象にはなっていないはずで、もちろん本件は民事の訴訟であるが、基本的に罪には問えないという形になっていると理解している。

これに関連して、似たような不正送金あるいは不正引き出しが社会的な問題になったという意味では、2003 年から 2004 年頃に偽造カード事件というものが大きく騒がれたときがあったが、そのときは結局、国会で預貯金者保護法と言われる法律が制定され、銀行側が補償するという内容になった。その議論の際、最も有効だった対策は、例えば、預金引出は 50 万円までとか、あるいは、送金は 300 万円までというような送金の上限を隠した、あるいは出金の上限を隠したということであった。しかし、現在の仮想通貨の場合は、通常の送金的な意味での送金と、銀行送金的な送金と、それとは別に、例えば株の取引をするような、取引所の売買、資産の運用の売買みたいなものと両方があり、また、何億円単位で売買している人がいるはずなので、上限額を隠してしまうといったことは、技術的、ビジネス的に難しいのではないかと思うが、この点で、こういう人は幾らまでとか、資産の何％までといった形で移動を抑制するような、何らかの対策のとりようはあるのか。

○（事業者）　まず、取引制限は技術的には可能である。実際にアメリカでは、本人確認の程度によって、入出金に制限がある。日本はそうではなく、犯収法

の要件を満たせば、入金、出金が制限なくできるということになっている。弊社は、それに加え、大きい金額の入出金は自主的にモニターしている。例えば、突然、１億円の出金があった場合には、サスピシャス・アクティビティーということで本人に確認をするといった措置をとっている。

ビジネス的に厳しいかと言われると、業界ルールが統一されており、皆が同じルールでやっているのであれば、そんなに反対する方はいないと思うが、仮に、１社だけがやるという他社がそろっていない状況の場合は、何かしら業界でそろえる必要はあると思っている。

また、明確な出金の金額を公開はしていない。公開してしまうと、例えば、100 万円と言うと、99 万円を複数に分けるといった形で対応されてしまう。

【事業者からの発表】

○（委員）　今月 19 日に韓国の仮想通貨取引所ユービットが破産手続を行った。北朝鮮の労働党、39 号室というキーワードが出ており、取引所の従業員の端末が乗っ取られたと聞いているが、こういった事案に鑑み、例えば、御社の従業員について、普段と違う操作しているとか、業務のやり方が変わったとか、そういったところをモニタリングしたり、これから何かやろうとしていたりといったことはあるか。

○（事業者）　弊社は、事業部とは別の独立した内部監査部門を持っており、従業員の操作自体がどうなのかということをパソコンの個体のログから内部監査室のほうで確認をし、問題があるかないかということを判断している。

○（委員）　６月に、一部の仮想通貨交換業者で不正送金の補償のルールを導入したと新聞報道されたかと思うが、これは、補償する場合に、例えば保険会社などを利用しているのか。それとも、自社の内部のファンドで補償するという仕組みなのか。

○（事業者）　弊社の場合、保険会社に、弊社に対して補償をつけていただいている。基本的に、ＩＤとパスワード、二段階認証を設定していれば、不正送金されることはないため、その中で不正送金が発生した場合、弊社がユーザーに対して補償をしており、弊社が支払った分を保険会社に補償していただくという形である。

○（委員）　その場合、マン・イン・ザ・ブラウザ攻撃のようなものは想定しないという前提か。ブラウザの中にマルウェアが入っていて、二段階認証の内容を書き換え、例えばマルウェアが指定する口座にビットコインを送ってしまうというような攻撃は、実際に国内でも発生した事例があったと記憶しており、この場合、二段階認証を突破してしまうわけだが、こういったケースは想定しないという前提か。

○（事業者）　そういう二段階認証を突破する場合に、弊社で補償をするということである。

○（委員）　そういった場合は、保険会社が補償をしてくれる、逆に言うと、そういうケースがなければ、一般に損害は発生しないであろうということか。

○（事業者）　そのとおり。弊社の過去のデータをもとに行っている。

○（委員）　不正利用対策に関しては、リスクベース認証のところも含めて、かなり熱心に行っていると思うが、これは、どこかの業界のものを参考にしてベンチマークにしているのか。あるいは、完全に独自で考えているのか。

○（事業者）　弊社は、基本的には、ネットバンクのようなものだと思っているので、そういったところを参照している。例えば、不正送金関係のチームを仕切っているマネージャーは、元々ネットバンクで不正送金の関係を行っていた人を採用しており、過去にこういう事案が起きたというところを予め学び、全部、内規の方で実施したりしている。

○（委員）　不正な取引のチェックは、最後は人で見ているということであったが、その際、これは不正だなとなる割合はどの程度のものなのか。

○（事業者）　不正に入ってきているもので、ストップさせているものは結構あるという印象である。そういう意味では、ここのオペレーションコストが大変上がっているが、人数を増やしながら、24 時間体制で行っている。

○（委員長）　警察との連携という点では、警視庁と連携しているということであったが、それは警視庁生活安全部サイバー犯罪対策課ということか。

○（事業者）　そのとおり。警視庁生活安全部サイバー犯罪対策課と協定を結び、連携している。

　また、これは弊社の要望になるが、警察庁とか、全銀協では、過去に起こったことについて、弊社以上に経験があり、多くのことを知っていると思うので、

可能であれば、そういったことを意見交換して、未然防止に役立てたいと思っている。データベースについても、現在、弊社が使えるものであれば、例えば、暴力団追放センターのデータベースがあったりするが、これは、飽くまでも暴力団かどうかしかわからないので、もう少し広範に犯罪者のリストだったりというものと照合可能であれば、アカウントをつくる前段階ではじくこともできると思っており、そういうことは協力してやっていければと思っている。

○（委員）　内部で不正な動きがあったときに全部ログをとっているという話があったが、従業員の採用時に、セキュリティ・チェックは行っているのか。

○（事業者）　基本的に、採用時には、バックグラウンド調査を行っており、過去の裁判で立件されているものがあるかどうかや、何かのトラブルに巻き込まれていないかどうかといったことをチェックし、問題ない人だけを採用している。

４．　閉会