平成 29 年 10 月 27 日

平成 29 年度サイバーセキュリティ政策会議（第１回）
発言要旨

１．　開会

２．　長官官房サイバーセキュリティ・情報化審議官挨拶

本会議は、情報セキュリティに関する産業界等と政府機関、特に警察との連携のあり方について議論するため、平成 13 年度以降開催してきた生活安全局長主催の私的懇談会である総合セキュリティ対策会議について、サイバーセキュリティに関するより幅広いテーマを取り扱うため、本年度改組したものである。

前身となる総合セキュリティ対策会議におけるこれまでの提言は、例えば平成 18 年度に運用が開始されたインターネットホットラインセンター、平成 26 年に業務が開始された日本版ＮＣＦＴＡであるＪＣ３等、官民が連携した多くの具体的施策に結実しているところであり、新設したサイバーセキュリティ政策会議においてもこの流れを引き継いでいきたいと考えている。

インターネットが国民生活や社会経済活動に不可欠な基盤として定着し、日々新たな技術やそれを活用したサービス等が生まれ、利用される中で、平成 28 年にはＩｏＴ機器を標的とする不正プログラム Mirai に感染したボットネットによる大規模なＤＤｏＳ攻撃が発生し、また本年に入り、ランサムウェアの WannaCry による世界規模での被害のほか、ビットコインを始めとする仮想通貨を利用した手口の犯罪が発生するなど、新たな技術、サービスを犯罪インフラとして悪用したサイバー犯罪、サイバー攻撃が発生しており、サイバー空間の脅威はますます高まっている。

こうした状況を踏まえ、本年度は新たな傾向のサイバー犯罪等に対応するための官民連携の更なる推進をテーマとし、具体的には仮想通貨を利用した犯罪への対策、レンタルサーバを利用した犯罪への対策、ボットネット対策の３つの項目について、官民が連携した対策の今後の方向性を議論いただきたい。

３．　委員長挨拶

このサイバーセキュリティ政策会議の前身となる総合セキュリティ対策会議は、十数年続いてきたものである。テーマはそれぞれの時期で異なるが、十数年前と変わらず、現在も警察のサイバー政策には、民間の力が必要不可欠である。

本会議にお集まりいただいた日本のサイバー世界のトップの皆様方には、是非、日本国民皆様の利益に繋がるような御発言、御力添えをいただければと思う。

４．　平成 29 年度サイバーセキュリティ政策会議のテーマについて

【事務局から、平成 29 年度サイバーセキュリティ政策会議のテーマについて説明】

５．　新たな傾向のサイバー犯罪等の現状と対策

【事務局から、新たな傾向のサイバー犯罪等の現状と対策について説明】

６．　仮想通貨とＩＣＯを巡る問題について

【委員から、仮想通貨とＩＣＯを巡る問題について発表】

○（委員長）　デジタル通貨の保有者の方がリスクや損失に直面する可能性が高いということは、そう簡単に現状が完全に転換して仮想通貨に移っていくことはないということか。

○（委員）　現在、ビットコインの市場流通残高は、ここ半年間の間に約５倍になり、約 10 兆円である。これは、全世界で 10 兆円ということであり、例えば日本銀行券は日本全体で100兆円、日本の個人資産は約1,000兆円にもなる。その意味で、ビットコインは、現在存在しているソブリン通貨、あるいは日本人が保有している金融資産を大きく代替するような存在ではない。

また、現在、ビットコインは家電量販店等で使えると宣伝されているが、実際にはほとんど使われていない。これは、ビットコインの値動きがあまりにも激しく、今日 0.1 ビットコインの製品が、明日は 0.05 ビットコインで買えるということが起こり得るため、今の相場を気にしながら買い物をするより自分が納得するレートで換金をして日本円で買ったほうがより心安らかに買い物がで

きるからである。

では、なぜあれほどビットコインを使えることが議論になるのかというと、ビットコインの値段を引き上げたいと思っているビットコインの仲介業者や取引業者が、ビットコイン取引における 10 分以上の決済承認時間について、その間の価格変動による損失のリスクを負担することで、ビットコインを使ってもらおうとし、また、店側は、ビットコインを使えるようになったことをマスコミに話すと、マスコミが来て報道してくれるので、宣伝効果は非常に大きく、そのため、次々にビットコインを使い始めるからである。そうすると、世の中でビットコインが広く使われているかのように錯覚するが、実際には使われていない。

ビットコインは、ある意味では、富の移転の手段としては使われているが、経済を支えるための決済通貨の代替物としては全く機能していないと言える。

○（委員長）　そのように聞くと、安堵する部分はあるが、他方で、ビットコインの価格の上下により多大な損害を被る人が出てくるといった可能性はある。それをどう救済するかということも、ある意味ではサイバー世界に関連する重要な課題として残っていくのではないかと思う。

○（委員）　ビットコインの分裂について、８月１日に、実際には分裂したけれども、折衷案という形が採用されていたということだが、もし、この部分の折衷案という形になったときには､現状の２つに分かれているビットコインは、そのまま移行するとか、あるいは一緒になるとか、今後どういう形になっていく傾向にあるのか。

○（委員）　ビットコインの分裂について追加で説明をさせていただく。

先程、ビットコインの手数料が実は安いとお話しした。例えばニューヨークからメキシコに何十ドル、何百ドルもかからず送金できるので、移民の人が家族に送金するのに使うといったニーズがあった。しかし、現在はビットコインを送金するのには、最低でも 15 ドルぐらいかかるというのが実態である。

これはなぜかというと、ビットコイン取引を記録するブロックのサイズが上限に張りついてしまい、これ以上追加でビットコイン取引を記録しようとしても、その箱の中に入らないので、送金をしようとしても、手数料を一銭も払わない場合には、その取引は箱の中に入れてもらえないからである。この解決策

として箱そのものを大きくする、すなわちブロックサイズを引き上げるという案と、SegWit というビットコインの取引情報の中に含まれる冗長な署名データを削減し、今の１メガバイトの箱の大きさを維持するという案の２つの案が出た。ニューヨークを中心とするコアの開発者たちは後者を、中国人を中心とするマイナー、すなわち発掘者側は前者を主張していた。

しかし、このまま対立が続くと、どこかでブロックチェーンが勝手に分岐してしまい、どちらの分岐が正しいのかがわからなくなってしまって、一方の分岐で取引をしていた人の過去の取引があるときに全部なくなってしまうといったことが起こりかねないというのが、資料にあるＵＡＳＦ（User Activated Soft Fork）と言われる現象である。これが８月１日に起こるかもしれないということで、ビットコイン分裂か、ビットコイン暴落か、などと報じられたのである。

ところが、その直前、SegWit2x というものによって関係者がほぼ合意し、８月１日の分裂は実質的には避けられた。これは、このタイミングでＵＡＳＦを実施すると、本当にビットコインが暴落し、ビットコイン保有者が損をしてしまうため、それを避けるために決定を先延ばしするというもので、ニューヨーク・アグリーメントと呼ばれる。しかし、一部の者が別のコインをつくり、勝手に分派してしまったのがビットコインキャッシュである。

８月１日にビットコインからビットコインキャッシュが分かれた後、ビットコインキャッシュは一時期全体で２兆円ぐらいになり、去年の今ごろのビットコイン全体と同じぐらいの価値を持つ別の通貨に成長した。一方、ビットコインは６兆円とか８兆円ぐらいの規模に拡大していった。

そして、今年の 11 月にニューヨーク・アグリーメントの期限が来る。そうすると、今度はビットコインが、箱の大きさが２メガバイトの上限の別のビットコインに分裂するとされており、これはニューヨーク・アグリーメントの結果成立した延長によって、再度引き起こされる分裂である。ニューヨーク・アグリーメントに納得していないニューヨークのコア派の人たちが、ビットコインを１メガバイトの箱の大きさのままやり続けるかもしれず、そうすると、ビットコインとビットコインの SegWit2X によって分派したＢ２Ｘというものの２つができる可能性がある。さらに、ビットコインキャッシュと同じように、最近ビットコインゴールドというものが分裂したので、近々、かつてはビットコ

インと呼ばれていたものが４つに分裂した形になる可能性がある。

分裂していても、それぞれの価値は全て保たれており、実際には分裂する前と比べて、価値がどのビットコインも何倍にもなっているので、その意味では、あまり誰も損しておらず、文句を言う人はいない。ただ、この状態が長く続き、結局ビットコインの希少性がないのではないかということになると、そのうちどれかが暴落するのではないかとか、いずれかが実質的に詐欺だということで価値を失うのではないかということが、いろいろなところで噂されているが、現状ではそこは何とも言えないという状況である。

○（委員）　お話を伺うに、ビットコインにそれほど犯罪に悪用されるような瑕疵があるようには聞こえず、むしろ、ＩＤとパスワードを盗まれて悪用されるといった、周辺の問題のほうが大きいのではないかと思う。

現在は使われていないと思うが、昔テレフォンカードというものがあり、当時は高額のテレフォンカードが犯罪に悪用されていた。そのときの対策として、テレフォンカードの上限を 1,000 円に変えて、犯罪者のうま味をなくすということをした。悪用される方のうま味をなくすことで、一気に魅力を失って、結果として悪用されなくなった。

同様に、ビットコインにも、悪さをしようとする人にとってうま味をなくすような仕組みをつくれるのではないかと思うが、どのようなものが考え得るか。

○（委員）　テレフォンカードの犯罪対策、あるいはその後の例えば偽造カード事件における銀行のＡＴＭ間の引き出し限度額の引き下げといった犯罪のインセンティブをそぐ方向というのは極めて有効であると思う。

しかし、問題は、テレフォンカードであれば当時のＮＴＴが、そして例えば銀行のＡＴＭの引き出しであれば各銀行が、それぞれ自分たちで管理して、判断して、決定することができる仕組みである一方、残念ながら、ビットコインは、ディセントラライズという言葉で表されるように、中央を持っていないということである。誰も意思決定をしておらず、できないのである。ガバナンスの仕組みをある目的のために変えたいというとき、例えば、まさにビットコインの箱の上限に達してしまったため、変えなければならないというとき、現にこれほどもめていることからわかるとおり、ビットコインは決められない、変えられないシステムなのである。したがって、実際にこういう状態を見ている

側としては、例えばフィアットカレンシーと同じぐらいの価値を持つようにしたらどうかとか、高額の送金はできないようにしたらどうかといったアイデアはあるが、それをビットコインの特性として組み込むのはなかなか難しい。

あえて言えば、ビットコインの国内の取引所にそれを要請することは考えられる。例えば一定金額以上の取引は必ず申請するようにとか、止めるようにといったことを言うことは、既にある程度行われていると思うが、問題は、日本だけでやっても駄目だということである。ビットコインは全世界共通で使われているため、日本だけでそういうルールをつくったとしても、それを嫌がる人たちが、例えばジンバブエの取引所やロシアの取引所を使うと、結局日本のルールから逸脱することができてしまうことになる。

それでは、グローバルのルールを決める仕組みが何かあるのかというと、それもなかなかないのが現状である。例えば中国は今、完全にビットコインを国内から追い出して、取引所も全部閉鎖させているが、多分、規制当局側がそういうかなり強権的なやり方をしなければ、国際的に相互運用性を持ってしまったものは、なかなかコントロールできないというのが、今の現実ではないかと思う。

７．　ボットネットについて

【委員から、ボットネットについて発表】

○（委員）　ボットネットの話は、犯罪者の観点で見たときに、２つのフェーズに分かれているのではないかと感じている。

１つ目は、ボットを感染させて、ボットネットという１つの大きなネットワークをつくり上げること。２つ目は、でき上がったボットネットを、ダークウェブ等でサービスとして貸し出し、そのサービスを借りた人が金融業界等に対して実行することである。ボットネットをつくり上げる人たちへのアプローチと、つくり上げられたボットネットを活用する人たちへのアプローチは、違うものではないかと感じている。

前者は先ほど発表いただいたところであるが、後者のでき上がったボットネットを悪用する人たちに対してのアプローチは、例えばアンダーグラウンドマーケットのモニタリングや、海外でよく聞くような、インターネット上でのお

とり捜査のようなものの必要性が出てくるかもしれない。

また、先日あるメディアの記事に、日本のマルウェア開発者へのインタビューが掲載されていたが、こういったものも１つのヒントになるのではないかと思っている。最近では、組織としてマルウェアをつくっている人たちもおり、例えば某国では、オープンソースでボットネットをつくり上げたりしているという傾向があったりする。こういったことを踏まえ、マルウェアの開発段階で、動き出す前にどうアプローチするのかを考える必要がある。これについても、つくる側の観点と、でき上がったものを借りる側の観点で、それぞれ犯罪者が動き出す前のアプローチが必要であると感じている。

○（委員）　確かに、ボットネットはつくる人と、使う人の分業化が進んでいる。つくる側は、公開されたソースコードをもとに開発したり、あるいはある程度のコミュニティで開発していたりするという事実もあると思われるので、いろいろな側面から対策を行っていくことが必要だと思う。

また、サービスを買って使う側を見ると、目的とその被害者には何らかの関連があると思われるので、そういった観点でのアプローチや、技術的な側面から、そのインフラをどうやってたたき潰すかという観点でのアプローチ、その両面から考えることが有効な手段だと思う。

○（委員）　Ｃ２サーバについて、海外の事例では、インシデントレスポンスする人が調査のためにＣ２サーバに侵入するといったことをやっている事例がある。簡単に日本でできることではないが、そういった前提条件をつけて、ディスカッションを始めても良いのではないかと考えている。

○（委員）　カメラ等のインターネットに接続可能なＩｏＴ機器が、ネット上で安く販売されている。中国製のものは非常に安く購入可能で、そういった機器は、マニュアルも中途半端な日本語で書かれており、ユーザーはどのような機器を購入したのか分からずに使用することになる。

それがボットに感染するような脆弱な機器で、これが広がっていくような場合を考え、機器側の品質を上げていくとか、ボットに感染しづらいようなものにしていくとか、そういった動きはあるのか。また、その機器側の対策は具体的にどのようなものか。

○（委員）　いろいろなところで最近議論がなされている。例えば、報道等に

よれば、インターネットにつながる接続基準みたいなもので品質を上げていくという動きがあると聞いている。また、技術的な面では、機器の自動バージョンアップ等をやっていくためのフレームワークを、ＩＴＦ等の団体でつくっていくという動きがあると聞いている。

ただ、そのように品質向上に取り組むのはまともな会社なので、中国の安い機器がそういう動きに乗るかといえば正直難しいのではないかと思う。そういう意味では、機器のところだけというよりは、通信事業者によって接続を強制的に切断するようなサービス、機能、あるいは、ユーザー側の管理責任違反のような自己責任との両輪でやっていかなければ、短期的には、国内の事業者のコスト増に結びつくのではないかと危惧をしている。

８．　閉会