参考資料２

サイバーセキュリティタスクフォース（第 30 回）議事要旨

1. 日 時）令和 3 年 4 月 7 日（水）10：00～12：00

2. 場 所）オンライン

3. 出席者）

【構成員】

後藤座長、安達構成員、鵜飼構成員、岡村構成員、小山構成員、篠田構成員、園田構成員、徳田構成員、中尾構成員、名和構成員、林構成員、藤本構成員、吉岡構成員

【オブザーバー】

篠崎美津子（内閣官房情報通信技術（IT）総合戦略室）、尾崎洸（経済産業省）、八島一司（地方公共団体情報システム機構）

【発表者】

木村泰司（一般社団法人日本ネットワークインフォメーションセンター（JPNIC））

【総務省】

田原サイバーセキュリティ統括官、藤野審議官（国際技術、サイバーセキュリティ担当）、箕浦サイバーセキュリティ・情報化審議官、中溝サイバーセキュリティ統括官室参事官（総括担当）、高村サイバーセキュリティ統括官室参事官（政策担当）、海野サイバーセキュリティ統括官室参事官（国際担当）、佐々木サイバーセキュリティ統括官室統括補佐、横澤田サイバーセキュリティ統括官室参事官補佐

4. 配付資料

資料 30-1-1　サイバーセキュリティに関するインターネット利用者の意識調査結果について
資料 30-1-2　無線 LAN セキュリティに関する周知啓発と利用者意識調査について
資料 30-1-3　テレワークセキュリティに関する周知啓発と実態調査について
資料 30-2　クラウドサービス利用時のセキュリティ向上に関する取組について
資料 30-3　情報通信ネットワークの将来像とセキュリティ技術に関する標準化を巡る議論の動向について
資料 30-4　「IoT・5G セキュリティ総合対策 2021（仮称）」の構成（案）について【関係者限り】
参考資料 1　サイバーセキュリティタスクフォース第 29 回 議事要旨

5. 議事概要

（1）開会

（2）説明

◆議題（１）「サイバーセキュリティに関するインターネット利用者の意識調査結果等」について、事務局より「資料 30-1-1　サイバーセキュリティに関するインターネット利用者の意識調査結果について」、「資料 30-1-2

無線 LAN セキュリティに関する周知啓発と利用者意識調査について」、「資料 30-1-3　テレワークセキュリティに関する周知啓発と実態調査について」を説明、議題（2）「クラウドサービス利用時のセキュリティ向上に関する取組」について、事務局より「資料 30-2　クラウドサービス利用時のセキュリティ向上に関する取組について」を説明、議題（3）「情報通信ネットワークの将来像とセキュリティ技術に関する標準化を巡る議論の動向」について、JPNIC 木村様より「資料 30-3　情報通信ネットワークの将来像とセキュリティ技術に関する標準化を巡る議論の動向について」を説明。

◆構成員の意見・コメント

岡村構成員）

フィッシング対策協議会の会長をやっている関係で申し上げると、フィッシングは高止まり状態にある。現在ではこの URL（https://www.antiphishing.jp/report/monthly/202103.html）の月次報告書の中にも記載されている通り、Amazon が約半数で突出している状態。協議会としては、Amazon の日本法人にフィッシング届出窓口の設置をお願いしたという状況。これは日本だけの現象のようで、欧米では Amazon に対するフィッシングが日本ほど問題になっておらず、その理由がはっきりしないところである。かつては、いわゆる 3 メガバンクなどが狙われていたが、この資料の通り、最近はクレジットカード会社が狙われる傾向にあるため、クレジットカード会社の団体に対して、ユーザへの注意喚起など、対策の強化を呼びかけている。このようにフィッシングというのは、かなり増えているということを申し上げる。

後藤座長）

多要素認証、ユーザ認証周りについてはアンドロイド端末・iPhone 関係の端末、マイクロソフトの端末に作り込まれている認証方式が、ユーザの意識に影響を与えていると思う。

中尾構成員）

ICT-ISAC の立場としてコメントすると、テレワークに関して、例えば家庭内で安全・快適に在宅勤務を行うためのリファレンスガイドを ICT-ISAC において、総務省と連携しつつ、作成・公開している。また、無線 LAN のセキュリティ強化についても、積極的に協力させていただいている。クラウドに関して様々な事案が発生しているというのは確かだと思う。その中で、実は ITU-T（X.1631）と ISO（ISO/IEC 27017）において、クラウドサービスプロバイダとクラウドの利用者がどのようなセキュリティをやらなくてはいけないかという Code of practice が定められている。その中で、今日ご指摘いただいている利用者側への教育、啓蒙というのもきちんとやらなくてはいけない、とある。例えば、クラウドサービス利用者は、クラウドサービスビジネスマネージャやクラウドサービス管理者、サービスのインテグレータ、従業員などのクラウドユーザ向けの意識啓発や教育などのトレーニングプログラムを構築しなくてはいけない。その文書では、サービスを使うための手順や標準、リスクを認識すること、それに対する法的なレギュレーションに関することの考慮など、様々なことが記載されている。エンドユーザがいわゆるクラウドサービスプロバイダが提供するようなツールあるいはアプリケーションの設定や使い方に関する啓蒙認識を増やすことが重要だが、X.1631 では、ハイレベルなことしか書いていないので、具体的にどういうことに注意して設定をしなくてはいけないかというのが抜けている。そういったところに深く入り込むことによって、設定のミスの軽減ができるのではないかと思う。具体的にそれを前に進めるにあたって、サポーティブではあるが、もう少し深いガイドラインとしてベストプラクティスが必要だと思った。

鵜飼構成員）

クラウドサービスの設定ミス防止・軽減に向けた取組の検討について、サービス利用者としてのクラウドサービス事業者の対策を促す取組、セキュリティベンダによるアセスメントの利用等と書いてあって、確かにユーザー

やクラウドサービスの提供者からすると、正直よく分からないという所もあって、セキュリティベンダにアセスメントを安価に頼めるような仕組みがあると、大分違うと思う。こういった取組というのはぜひ進めていただきたいと思っている。一方で、今の段階だと様々なクラウドサービスがあり、そのアップデートによる変化が激しいため、セキュリティベンダは、全てをキャッチアップするというのは大変な中でサービスの立て付けを検討している。そういう意味で、今後どのような形でこういったサービスのセキュリティベンダによるアセスメントの利用普及が見込まれるのかが見えていると、各セキュリティベンダも思い切って投資できるところがあるので、そういった情報を表に出していくことができればと思っている。割と急いでやらなければならない内容だと思うので、ぜひ進めていただきたい。

藤本構成員）

無線 LAN の使用に関して、資料 30-1-2 の中で SSID や暗号化有無の確認方法が分からないという回答が多いという説明があったが、このような回答が出るということは、アンケートの回答者は確認しようとしているが、そのハードルを越えられていないということかもしれない。書いた人は気づかないが、読んだ方によっては分かりにくい部分があるのかもしれない。一度、対象読者にサンプル的にでも読んでいただいて、どこで引っかかっているのかを確認するなどをしていくと、この辺の数字が下がってくるのではないか。

吉岡構成員）

無線 LAN ルータのファームウェア更新の話が出ていたと思うが、古い機器についてはファームウェアの更新手順もかなり複雑で、中々難しい面があるかもしれない。また、そもそも単価が高くない無線 LAN のルータについて、メーカがいつまでサポートするのかという点も難しい問題だと思っている。エンドオブサービスやエンドオブサポート、いわゆる EOS について、無線 LAN ルータでも考えていく必要があると思っている。一方で、様々なメーカとお話しさせていただくと、大規模なマルウェア感染や大きな問題があった場合は、サポート外だからといって完全に無視するというのは、現状の利用者の期待を考えると中々難しいというところもあり、実際にはかなり古い機器であっても対応しなければならないということも現実的にはある。つまり EOS をきっちり決めて、その間だけ守るということも難しいという話も聞いている。もう 1 つの観点は、こういった攻撃が今後、ますます増えてくるのか、そうでないのかについてである。Mirai 等の IoT のマルウェアが出てきて少し経つが、大規模なインシデントが今後も出るのかどうかという情報が無いため、EOS について議論をするのが難しく、どちらにするとも決めかねているという話を聞いた。そういった方向性をメーカが主導して考えていくというのが本筋かもしれないが、重要な事項については何らかの方向性を国が示すといった考え方もあるかもしれないということを申し上げたい。どうすれば良いという意見を言えるほど状況が分かっていないが、そういった問題意識があるということだけ共有させていただく。

後藤座長）

Wi-Fi に関しては、買取型とレンタル型という議論も前にあったと思う。通信サービス事業者によるレンタルサービス等では、サービス事業者主導のメンテナンスが期待できるので、その辺りも議論できればと思う。

篠田構成員）

周知啓発について、テレビやラジオが媒体として出ているが、面白みを加える取組として、リーチしづらい子どもたち、若い人を使うという方法が台湾で成功している。例えばインスタグラムなどのアカウントを総務省はまだ持っていないと思うが、インスタグラムなどで詐欺アプリのこういったものが良くないというのを写真で見せるだけでも面白くなると思うし、文章は読まれないが、絵だとインパクトがある。そこに絵とメッセージが書いてあるだけで、全然良いと思う。あとは、SMS のメッセージの詐欺などもたくさんあるが、そういったものにつ

いても文章ではなくて、絵と軽いメッセージがあるだけで、大分インパクトがある。要は、みんなインスタントなメッセージが欲しており、文字で読まなければいけないものはあまり読まない。Twitter でさえも離れ気味と聞いているので、少しだけ面白みというか、インスタグラムを利用するなどの工夫をしても良いと思った。

園田構成員）

ウェブのアンケートという所で、そもそもリーチしている人たちが、ある一定以上のリテラシーをお持ちの方々というところがある。それにリーチできないような方々への啓発というのが気になる。そういった人たちに向けて何が効果的かというと、旧来のメディアと位置づけられるかもしれないが、テレビやラジオ、新聞、雑誌等も良い。また、面白みという点で言うならば、若者に色々流行っている動画系のメディアなど、そういったものに上手く乗っかってバズってもらえるようなコンテンツ作りなどの工夫が必要かと思う。

安達構成員）

資料 30-1-1 に注意喚起情報の伝達手法について書いてあったが、そこの回答欄にテレビやメディアが一切含まれていなかったが、そういった取組も必要かと思う。もう 1 つ考えられるのが、メディアはその他に含まれているのかという点で、パーセンテージが低かったので、ポイント的にどうなのかと思った。それと 1 点質問で、資料 30-1-1 の調査対象者の属性の職業について、日本の全体の職業構成と同じようなバランスでの割合となっているか。

中溝サイバーセキュリティ統括官室参事官）

職業については、属性に合わせてというところは必ずしもそれを反映している形にはなっていない。

安達構成員）

今回のアンケートは約半分、会社員の方が含まれているので、割とそういった方面に精通している方がご回答されているという印象を受けたので確認させていただいた。

名和構成員）

今回の意識調査で、ネット利用の機器がスマートフォンの方がパソコンの倍という数字が出ている。これはつまり、スマートフォンによるセキュリティのインシデントに当たる確率が高くなると感じている。他方、最近はスマートフォンのアプリに関する問題が新聞報道で騒がれている。インターネットのアクセスについては、アプリが必須になってきているが、そのアプリに関する意識調査という点が今回の報告書の中では見えていない。アプリを除いたということは何か意味があるのか。または別に行うのか。

中溝サイバーセキュリティ統括官室参事官）

アンケートを実施する段階では、スマートフォン利用とパソコン利用、その他の媒体の利用の割合がどのくらいかというのは見えない段階だったので、スマートフォンに特化した質問は検討していなかった。ある程度スマートフォンの利用は多いだろうということは、もちろん予測できたところではあるが、その点は今回の調査で明らかとなったし、調査の中でスマートフォンを利用する際の、様々な対策の必要性や課題が見えてきているので、そこをもう 1 回さらに洗い出した上で、ご指摘があったようなアプリに関する課題のさらなる深掘りを引き続き検討していけたらと思っている。

名和構成員）

最近有名なスマホでも、プライバシーポリシに関して法に備えた隔離をしなかったり、近隣諸国で非常に評判の高いアプリの、開発者のアカウントが乗っ取られ、正規のアプリから情報が流出したという事案が発生しており、何をもってアプリが安全かということはないと思っている。誰かが国民がよく使っているアプリを継続的に監視していかないと甚大な被害が発生し得るということを感じている。

徳田構成員）

資料 30-3 の 22 ページに調査内容として、日本からの標準化への関与活性化に向けた課題ということで、詳しく整理していただいてある点について、1 つ目の質問は、日本のベンダーや NICT のような公的機関において、どのくらいの年齢の方たちが ITU や ITU-R などの会合に出ていっているか、または興味があるかについてである。IETF・ITU・IEEE などがあるが、各ベンダで自分たちがビジネスをしていく上で、どのくらい重要と思っているか、技術をこれから作っていく企業側や公的機関側でどのくらい積極的に標準化に関与しく必要があると思っているかに関する意識調査のデータはあるか。もう 1 点は将来のネットワークに関してで、今回まとめていただいたデータは、インターネットをベースに議論されていたと思うが、実は私たちのような公的機関でやっているテーマの 1 つに、Beyond5G、5G の次の社会インフラを支える標準化がある。実際に ITU-R では、ビジョン勧告などに向けてスタートしており、ITU-R に NICT も投稿し、オールジャパンとしての投稿が出てくると思うが、次の 2030 年代のネットワークアーキテクチャというのは、インターネットももちろん残っていくが、Beyond 5G のネットワークアーキテクチャの議論もあるし、量子ネットワークの技術がたくさん出てきているので、少し未来志向で準備していく必要がある。このように、セキュアな通信ネットワークが量子暗号を使ったネットワークの利用など、標準に対してカバーをしていくエリアというのが広がっていると私は理解しているが、その辺はどうか。

JPNIC 木村様）

まず 1 点目の企業からの参加の重要性に関する意識の調査に関しては、意識調査そのものはできていない。この調査で分かってきていることは、実は標準化の対応については、ITU のように組織として参加できる所に関しては重要性の認知が広がっているが、ETSI のように個別に相互運用性実験などに参加しなければならない場合には、企業から重要性の認知がされていないので、継続的に参加しにくい。IETF でも、そんな声が聞かれているという状況。企業の中での認知度に関して、さらに深く調査する余地が残っていると言える。量子の技術を使った 2030 年に向けた検討は、広がってきていると思う。IETF での講演の話題としても挙がってきており、具体的には鍵の共有や通信そのものなど扱ってる所は各々別々だが、広がってきていると考えている。

徳田構成員）

Beyond 5G に関しては、総務省からも非常にたくさんの財政的支援をされていて、Beyond 5G に向けての標準化を日本の関係者で 10 パーセントくらい取っていこうというような国の戦略もあるが、本日の資料でも記載があるように組織的なサポートが必要であったり、経験者が不足しているという状況がある。私も ITU 協会の表彰の委員を仰せつかってお手伝いしているが、多くの方たちがどんどんシニアの方たちになってきており、若手が中々オンザジョブトレーニング的に参加する機会を頂けないような場合もある。Beyond 5G に向けては産官学が、この標準化に向けて連携を強めていかないといけないという危機感を持っている。

中尾構成員）

標準化に若手が参加しづらいという状況が実は非常に多くなっているが、中国では若い参加者が多く参加し、多くの提案を出してきている。それは中国では色々な戦略を考えていて、中国自身が国としてどういうような方向

に持っていくかというベースがあって、そこから提案が色々出てきている。もう 1 つ、最近よくあるのが、海外にある中国の Huawei などの子会社の方で、英語が完全にフラットな方が Huawei の所属として出てきており、非常に戦略的に振る舞っている。そういった点を踏まえると、基本的にボランティアベースで、色々なことをやらなくてはいけないという日本の場合、参加者の大きな減少等につながると思う。高齢化については、国際標準化の手続きや進め方、内容の整理など、経験が必要な場合が多いが、海外では標準化に関わる人が企業から出ているというよりもセキュリティのベンダが国際標準の専門でやっているところに委託して、その人たちが出てきているというケースが多い。つまりボランティアではなくて、お金をもらって実はやっているケースが多い。こういった環境の中で、日本の国際の標準化という視点では、ITU-R の場合は違うが、国として推進すべき案件や個々の組織が提案していくべき案件という観点で整理すると、組織の提案というのは費用的・人的な負担もあり、また効果が不透明という観点からも減ってきているというのが現状。先ほどご紹介したように、中国の場合は国として標準化を推進しているところもあるため、日本においても Beyond 5G や New IP の話も含めて、国として推進すべきことを総務省が中心になって整理をされて、その方向で進めていくというのが活性化につながるのではないかと思う。

吉岡構成員）

資料 30-3 の DNS やルーティングに関してお聞きしたい。ルーティングと DNS の 2 つの話があり、ルーティングの方は、経路の詐称や脅威の存在もスライドでご説明いただいて、普及が必要ということで進んでいると理解した。一方、DNSSEC については相当前からあるにも関わらず、普及に時間がかかっており、日本では普及率がかなり低いということだったが、アメリカの方を見ても、25%とそこまで高くない。全体で見ると、あまり高くないという感じだと思うが、DNSSEC の普及とサイバー攻撃の頻度や被害がどういう関係にあるかということが分析されているようなものがあるか。DNSSEC で防げる脅威とそうでない脅威があるとは思うが、普及した場合にセキュリティの観点でこういうものの改善に期待されるといったようなことがあれば教えていただきたい。

JPNIC 木村様）

実際に起きたインシデントに対して、DNSSEC がどの範囲で守れるのかについては、技術的な仕様としての守れる範囲に関しては明らかではあるが、実際に発生したことに対して、どれくらい守ることができているかについては、当センターでも注目したい所ではあるが、DNSOPS（日本 DNS オペレーターズグループ）や日本国内でのオペレータコミュニティなどでも、中々情報交換がされていない。ここは、RPKI も共通した話題だが、実際に発生しているインシデントに対して、その技術でどのくらい守ることができたのかということに関しては、データとして少ない。それが見えてこないことには、実際に導入効果という所が見えてこないというのはご指摘の通りである。

岡村構成員）

ご紹介いただいた IaaS・PaaS・SaaS の関係で問題が起こっていることは承知している。それだけではなくて、SaaS 自体の設定不備でも様々な問題が起こっている。昨日も NISC が Twitter 上で注意喚起した案件もあった。また本年 2 月にも、ある弁護士がグーグルグループの設定ミスをして倒産処理の情報が公開状態にあったという事案も発生している。したがって、IaaS・PaaS・SaaS の関係を精査をする必要がある一方で、SaaS 自体の設定に関して設定ミスがないようにという点ついても、エンドユーザーへの啓発が必要となる。

篠田構成員）

ユーザーの行動変容を促すような周知徹底もあるが、これに限界があるというのは長年やって感じており、仕組みという所で大本を止めることが 1 番有効。フィッシングはブラウザから入ることが多いのでブロッキングは非

常に有効であり、その対応をスピードアップするために我々も努力している。しかし、今現在訴えてはいるが中々動かないので、モバイルアプリの企業やユーザー企業やセキュリティ企業の人たちを集めて、ブラウザ企業を同じテーブルにつけるよう努力をしている。こういった活動を米国や他の国も巻き込んでやっているが、日本からもう少し積極的に参加すべきである。

後藤座長）

以上で議事3の意見交換を終了する。議事4は非公開のため、傍聴の音声はここまでとさせていただく。

◆議題（4）「「IoT・5Gセキュリティ総合対策2021（仮称）」の構成（案）」について、事務局より「資料30-4「IoT・5Gセキュリティ総合対策2021（仮称）」の構成（案）について」を説明し、質疑応答、意見交換を実施（非公開）。

以上