

サイバーセキュリティタスクフォース（第18回）議事要旨

1. 日 時：令和元年 12 月 5 日（木） 14:00～15:30
2. 場 所：中央合同庁舎 2 号館 8 階 第 1 特別会議室
3. 出席者：

【構成員】

後藤座長、岡村構成員、小山構成員、齋藤構成員(大関代理)、篠田構成員、園田構成員、徳田構成員、林構成員、藤本構成員、若江構成員

【オブザーバ】

尾崎洸(経済産業省)、神谷征彦(内閣官房 IT 総合戦略室)、吉川徹志(内閣サイバーセキュリティセンター)、浦船利幸(地方公共団体情報システム機構)、小松直人(無線 LAN ビジネス推進連絡会)、田中俊昭(KDDI)

【総務省】

竹内サイバーセキュリティ統括官、二宮審議官(国際技術、サイバーセキュリティ担当)、岡崎サイバーセキュリティ・情報化審議官、大森サイバーセキュリティ統括官室参事官(総括担当)、赤阪サイバーセキュリティ統括官室参事官(政策担当)、近藤サイバーセキュリティ統括官室参事官(国際担当)、渡邊放送技術課課長補佐(代理)、水落地域放送推進室技術企画官、神門地域情報政策室長、相川サイバーセキュリティ統括官室参事官補佐、佐々木サイバーセキュリティ統括官室統括補佐

4. 配布資料

- 資料 18-1 前回までの御議論について（事務局）
- 資料 18-2 公衆無線 LAN のセキュリティに関して（無線 LAN ビジネス推進連絡会）
- 資料 18-3 電気通信・放送・地方自治体分野のサイバーセキュリティ対策について（事務局、関係者限り）
- 資料 18-4 サイバーセキュリティタスクフォース 検討資料（KDDI 株式会社、関係者限り）
- 資料 18-5 地上波放送局の現状と課題（株式会社テレビ東京、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 17 回 議事要旨

5. 議事概要

(1) 開会

(2) 議事

- ◆ 議事（1）前回までの御議論について、事務局より、「資料 18-1 前回までの御議論について」を説明(省略)
- ◆ 議事（2）Wi-Fi のセキュリティ対策について、小松直人氏より、「資料 18-2 公衆無線 LAN のセキュリティに関して」を説明(省略)

◆ 構成員の意見・コメント

岡村構成員)

頻繁に新幹線で大阪－東京間を往復しているが、車内で PC を接続しようとする安全に接続できないという警告がでる。次の日に用事がある場合は日本を代表するシティホテルに宿泊しているが、ホテル内で PC を接続しようすると、本当に接続してよいのかという警告画面が頻発して飛んでくる。そのような状態であるので、果たして、「資料 18-2」の 12 ページの中に示されているような（公衆無線 LAN に対する）不安を感じているかどうかという状況であるが本日も指摘があったこと以前の問題が不安にさせている原因ではないかと考えている。

「資料 18-1」について、東京 2020 大会の開催までに間に合うように実施してもらいたい取組がたくさん出てくる。それはそれで実施しなければいけないということは、はっきりしている。アドホックに対応していても訳が分からない状況になるので、総務省が採るべきとりまとめの具体的なアクションについて、早期に用意するための声明やそのとりまとめを行うことが重要ではないかと考えている。何を実施すればよいのかということは、まとまっているようでまとまっていない状態であると思う。

小松オブザーバ)

Caution は、必ず利用許諾を取ったり、認証を入れたりしているところから出る。おそらく先ほどの Caution は、http サイトに飛ぼうとしているときにログインエラーを出すところで、エラーが発生していると考えられる。その部分は構造的な問題であり、解決しなければいけない問題である。当然ながら、その時点で危ないと言われると不安になるというのはご指摘のとおりであると思う。

徳田構成員)

東京 2020 大会の開催が近づいてきているため、今までに開催されたサイバーセキュリティタスクフォースの議論の中でいろいろなアイデアがまとめられてきているが、既に前もって出来るものはリストアップして整理して、実際にどこまで協調が出来ているか、対策が進んでいるかというある種のチェックリストを作成した方がよいと考えている。どこまで大会に向けて出来るかどうかについても、最終まで出来るのを待っていると時間が過ぎてしまうので、スナップショット的に、中間とりまとめとして、すぐに実施出来る対策の一覧表を作成することが非常に役に立つのではないかと考えている。

藤本構成員)

東京 2020 大会の開催までの期間があと僅かである。人材について、育成が大事なことはいうまでもないが、今確保されている人材をどのように有効に、かつ効果的に活用して対応するのかという考え方で取り組む時機に差し掛かっていると考えている。諸外国に比べて日本の場合は、情報セキュリティ人材が圧倒的に少ない。そのような現状を考慮して、今どこにどれぐらいどんなスキルを持った人材がいるのかということ踏まえて、短期に出来る対応を検討する必要があるのではないかと考えている。

後藤座長)

「資料 18-1」の説明においても、地方の人材の問題、自治体の人材の問題が出ていた。そういう部分が大事であると思う。

- ◆ 議事（3）総務省所管分野のサイバーセキュリティ対策について、事務局より、「資料 18-3 電気通信・放送・地方自治体分野のサイバーセキュリティ対策について」、田中俊昭氏より、「資料 18-4 サイバーセキュリティタスクフォース 検討資料」、大関 潔氏より、「資料 18-5 地上波放送局の現状と課題」を説明(省略)

◆ 構成員の意見・コメント

○情報共有について、ICT-ISAC を始めとして、さまざまな ISAC が先進的な取組を実施してきているが、そのような取組について知らない人がいることも事実である。「資料 18-1」の 4 ページでは国内の ISAC 間の連携を支援するという善意を示しただけの書きぶりになっているが、もう少し PR を実施してもよいのではないかと考えている。

○インシデント情報を共有することが大変大事であるが、この分野について、2016 年に諸外国・先進国の例を米国型、EU 型、英国型の 3 つのパターンに分けて考えてはどうかということで調べたことがある。英国型はインテリジェンス機関を中心に構成するという方法であり、現に **National Cyber Security Centre** が英国政府通信本部(GCHQ)の中に設立されている。英国型は真似できる点はなさそうである。EU 型は、報告制度を義務付けており、通信や放送の分野できちんと実施されている。他のインフラ事業ではどこまで、どのように実施しているかどうかは分からないが、そのようなところに働きかけを行うのであれば、横並びで調べて、ここはこうした方がお互いの共有がもっとスムーズになるのよという提案が役に立つのではないかと考えている。その際にどの情報を共有するかという情報だけに着目しているが、EU 型では **Single Contact Point (SCP)** という形で窓口を統一して、一括して情報共有を行う担当者を決めている。この EU 型の例は参考になるのではないかと考えている。顔見知りの人との間での情報共有は非常に実施しやすいからである。米国は、経済学で捉えて、情報共有を進めるにはインセンティブを与えないといけないと考えているところがあり、インセンティブというよりも、法律的に訴訟に持ち込まれたり、何らかの刑事罰が課されたりすることがないということを保証するという免責規定でもって、それが十分機能するものと考えている。日本の場合は、防護措置を取らなければならないと記載されているが、米国の場合は、防護措置を取ったとしても責任を問われることはないという書き方になる。それらは裏と表の関係で言っていることは同じである。

○電気通信事業法の第 6 条の利用の公平では、原則的な部分しか記載されておらず、例外条項が設けられていない。郵便法には、郵便禁制品が規定されていて、取扱い拒否を行う範囲が決まっている。電気通信事業法には、それに該当する条項はない。何かしら免責条項について工夫してもらい、特に事業用電気通信設備規則の第 6 条をもう少し拘束力の強いような規定の方に移してもらえばよいのではないかと考えている。

○地方自治体分野では、三層の対策によるセキュリティ強化はこの時点で有効なものであると考えているが、同時に組織の活力や生産性の向上、働き方改革、デジタルトランスフォーメーションの可能性も併せて分断してしまうものでもあるという点について懸念している。最新のセキュリティ対策を随時導入するということ为例えば 3 年間で定期的に見直すということも含めて義務付けていかないとかえって地方自治体の方々の仕事をスポイルすることにならないかという危惧をしている。このことは地方自治体だけでなく、事業者にも当てはまることである。数年単位での最新のセキュリティ対策の適用を定期的に見直すという文化を醸成していくことができればよいと考えている。

○今の指摘の趣旨についてはよく分かる。保護と利活用のバランスをもう少し再構成できないかという点について、例えば、クラウドにある程度乗せることを部分的にもできないか検討を要する。他方で視野に入れないといけないのは、例えば、個人番号利用事務系であれば、今春の通常国会で成立した戸籍法の改正によって、戸籍にマイナンバーが付くように

なった。従って、市区町村レベルがその事務をハンドリングすることになる。ある自治体の場合、担当者が1人でLGWANも、住民基本台帳も、マイナンバーも、防災無線も担当しており、人口数万人の都市で5人ぐらいしか担当者がいないというような実情があると聞いている。人、モノ、お金について、どのようにバランスを取っていくかとともに、戸籍などの事務が追加され、負担が重たくなっていくという実情が聞かれるので整理が難航し、簡単には片付きそうもない問題であるという気がする。

後藤座長)

本日時間の関係等があって、ご披露いただけなかった意見については、明日までの事務局に連絡していただきたい。前回からの議論でいろいろな課題が出てきている。これらの課題について、早めに議論を行い、とりまとめてもよいのではないかという意見も出た。大事な点であると思うので、今後の進め方について、事務局と相談しながら検討させていただく。とりまとめの考え方についても検討したいと思う。

相川サイバーセキュリティ統括官室参事官補佐)

次回以降のサイバーセキュリティタスクフォースの日程について、第19回会合は12月25日(水)の14時～を予定している。具体的な議事と開催場所については、後ほど事務局から連絡させていただく。構成員の方々には個別の相談をさせていただくこともあるので、引き続き協力をお願いしたい。

以上