サイバーセキュリティタスクフォース（第 26 回）議事要旨

1. 日 時：令和 2 年 10 月 12 日（月）16:00～17:45

2. 場 所：オンライン

3. 出席者：

【構成員】

後藤座長、鵜飼構成員、岡村構成員、小山構成員、斎藤構成員、篠田構成員、園田構成員、戸川構成員、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、若江構成員

【オブザーバー】

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

【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、安達地域情報政策室課長補佐（代理出席）

4. 配付資料

資料 26-1　テレワークのセキュリティについて
資料 26-2　スマートシティセキュリティガイドライン（第 1.0 版）の概要
資料 26-3　NOTICE の実施状況及び実施計画の変更について
資料 26-4　電子署名を用いた電子契約サービスに関する整理について
資料 26-5　令和３年度総務省サイバーセキュリティ関連予算概算要求について
参考資料 1　IoT・5G セキュリティ総合対策 2020
参考資料 2-1　中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）（初版）
参考資料 2-2　設定解説資料（Cisco WebEx Meetings／Microsoft Teams／Zoom）
参考資料 3　スマートシティセキュリティガイドライン（第 1.0 版）
参考資料 4-1　電子契約サービスに関するＱ＆Ａ（電子署名法第２条１項関係）
参考資料 4-2　電子契約サービスに関するＱ＆Ａ（電子署名法第３条関係）
参考資料 4-3　押印についてのＱ＆Ａ

5. 議事概要

（1）開会

（2）議事

◆議事１　「IoT・5G セキュリティ総合対策 2020 を踏まえた最近の取組状況」について、事務局より、「資料 26-1、資料 26-2、資料 26-4、資料 26-5」を説明。NICT より「資料 26-3」を説明。

◆構成員の意見・コメント

徳田構成員）

一つ目はスマートシティについて、セキュリティだけではなく、セーフティというキーワードが入っているのが非常に大事。データの改ざんや、その影響が物理的な環境に反映される。例えば降水量だったり、避難措置にクリティカルなデータ等も公開されたり共有されるようになってきているので、そのデータが意思決定のベースになる。そういうものが悪意を持った方たちに改ざんされると人命にも直結してくるので、非常に大事だと思っており、分科会の名前にセーフティと入れていただいたのが非常に良かったと思う。二つ目は、NICT の予算の説明でいろいろと NICT の施策の事をご説明いただいたが、今回の SecHack365、サイバーコロッセオ、CYDER、三つとも事業が順調に進んでいるが、サイバーコロッセオは東京オリンピック・パラリンピックに向けて役割を終焉するという理解。また、一つ目の人材育成で新たに予算をつけていただいているが、これは日本にとっても非常に大事だと思っている。一つのカギはセキュリティ教育のクオリティで、大学院レベルでは後藤座長の情報セキュリティ大学院大学が実践されているが、クオリティをどう担保していくかという課題があるので、サーティファイされた教材など、質の保証が今後大事になってくるのではないかと理解している。

斎藤構成員）

まず資料 26－1 の 2 ページ目にある「テレワークセキュリティガイドライン」が 2020 年度内に改定予定という点に関してであるが、多要素認証については、詳しく解説するべきではないかと思う。それから会議ツールについて、マニュアルを作ることは非常に重要であると思うが、仕様変更が頻繁になる箇所もあるので、マニュアルも追従して更新していくことが重要になると思う。あとはツールだが、最近はバーチャルオフィスツールなどで国産ツールも出てきており、利用シーンにおいて選べるほどバリエーションも多い。しかし、ツールを全部網羅するというのは中々難しいところもあるので、メインをアプリケーションで利用、他はブラウザで利用するなど区別することで運用、セキュリティレベルを維持していくことも必要なのではないか。実際にセキュリティの業務を担当している立場から感じている。

篠田構成員）

まず、ガイドラインが非常に良くできていて、すばらしいと思った。全く手引きがない状態で、手探りでやるよりは随分楽であるし、担当者の方も早急にやらなければならないので、早く対応するにはガイドラインは非常に助けになると思う。多要素認証の部分だけ触れてあげると良いと思うし、既にラック社が専門家として対応しており、テキストで分からない場合はラック社にエスカレートできるというところまで出来ているので、申し分ないと思う。あとは、テレワークをきっかけとしてさまざまな中小企業のセキュリティがアップできれば良いと思う。

戸川構成員）

まず、今回の手引き、チェックリストは非常に良くできていると思うし、非常にタイムリーなものになっていると思っている。このテレワークのセキュリティだが、今回のデータにあった通り、3 月、4 月のコロナ禍という状況において、皆さんテレワークを始めたというところがあったと思うが、現状のコロナ禍だけではなく、これからもテレワークは重要な位置づけになるのではないかと思う。いわゆる新しい生活様式というものが提唱されているが、これが主

要な活動になるのではないかと思う。そのような状況の中、ツール等の内容の変更や様々な脆弱性等も指摘されてくると思うので、定期的なアップデートが必要だと思う。また、せっかく作ったとしても、多くの方々に見ていただかないと非常にもったいないと思うので、いかにこういったチェックリスト等を普及させていくのかという点も非常に重要と思っている。

吉岡構成員）

ガイドラインの更新とチェックリストの検討委員会に入り、少しご協力させていただいたが、非常に短期間でやったということで、事務局含め、とりまとめていただいた関係者の皆様に感謝している。正直なところ、時間がすごく限られていたので、攻撃が実際にテレワークの環境でどのように起きるのかというところの実態把握という意味ではまだまだだと思っており、それをしっかりと情報収集し、どのようなことが起きているのかということも把握した上で、更に良い対策にするための更新が必要と思っている。

鵜飼構成員）

この短期間でガイドラインをまとめていただき、非常に感謝を申し上げる。今回の調査で副次的というか、思いの外いろいろな課題があるというのが逆に見えてきてしまったところが正直あるのではないかと思う。WindowsXP や 7、8 を全部足すとおそらく MacOS より数が多く、結構衝撃的な数が出ていると思った。このように新たに見えてきた問題に対して、今後この手引きまたはガイドラインだけで対応していくのか、それとも別に何かやるのか等、改めて検討をしていかないといけないのではと思った。

園田構成員）

私の方からはデザインについて言及させていただく。この手の資料を読むときに、個別の方々の事情に応じて、それぞれ必要な情報が限られてくるため、全員が全部読む必要はないという部分があると思う。それに早く到達するためにもっとデザイン上の工夫が必要かなと思う。総じて言えるのが、見やすくするところとその情報を渡りやすくするという意味で、もっと色々なアイコンを使ったり、色を分けたり、色のポリシーを考えたりすれば良くなるのではないかと思った。中身が非常に良いだけに、その工夫がもう一つあるとさらに良くなるのではないかと思う。

名和構成員）

質問ではなくコメントを申し上げる。想定脅威の項目があり、そこにマルウェア感染、不正アクセスと一言しかない。読み方（解釈の仕方）は色々あると思うので、他の省庁あるいは業界団体が出している同じようなドキュメント等とリンクするようにしたほうが良いと思った。そこで、公的機関が出している何かしらのサイバー脅威の分類を利用したり、あるいは MITRE 社の ATT＆CK は米国のセキュリティプロダクトの方でよく参照することが考えられる。そうすれば、大手企業が米国企業のセキュリティ対策ソフトをプロダクトに入れているので、親和性が良くなるのかと思った。

岡村構成員）

テレワークセキュリティは自治行政局の会議でも議論したが、本ガイドラインは中小企業が相手ということで、例えば自宅からウェブ会議に参加した社員の横で子供の泣き声が聞こえる等の状態である。それがテレワークの実態だということに鑑みると、社外からウェブ会議に参加するときは、せめて周囲に会議内容が半ば聞き取れないようにマイク付きイヤホン、ヘッドホンを使うといった、基本的な対策も実際には要るのではないかと思う。

後藤座長）

テレワークのガイドラインとチェックリストに関しては、期待が大きい分たくさんのご意見が出たが、なにか事務局から回答はあるか。

高村サイバーセキュリティ統括官室参事官（政策担当））

まず、斎藤構成員、篠田構成員から話があった多段階認証について、配付している参考資料 2-1 の 34 ページ目に二重丸で 9-1 認証というセクションがあるが、現時点だとここでは長く複雑なパスワードを求めるところで止めている。本当は二要素認証、二段階認証をかけた方がいいが、これを書いてしまうと中小企業がどのようにしたらいいのかわからない、もしくはコストが高すぎて対応できないという問題があるので、あえて無視しているところがある。二段階認証等をかけることに越したことがないので、もし構成員の先生方で、安くて、もしくは導入や運用がそれなりに簡単なものがあれば、是非お知らせいただけると有難い。ちなみに Google Authenticator はきちんと使うのはあまりにも難しいので、無理だと思っている。そういったレベルで廉価かつ簡単なものを是非ご紹介いただければと思う。また斎藤構成員から頂戴した件について、今回テレカンシステムだけ出しているが、個別なアプリケーションに関する詳細解説書は、私たちとしても頑張りますとしか言いようがなく、頑張っていきたいと思う。逆に今回テレカンシステムだけ作っているが、他のものも作るべきだというお話があれば、そこはまた先生方からご提起いただければ頑張りたいと思っている。また、チェックリストのアップデートについても、とりあえず年度内はやっていきたいと思っているが、そこで一回落ち着いたあとは当然セキュリティの情勢というのがどんどん変わっていくかと思うので、年に二回、三回の見直しは難しいが、そこにあわせて適宜のタイミングで見直しを加えていきたいと思っている。また普及の部分も大事だというお話だが、今回は補正予算として確保しているが、ガイドラインやチェックリストの存在自体が全く知られていないため、スケジュールの最終調整をしているところだが、Yahoo、Google を使ったネット広告、専門の新聞、専門の雑誌など、中小企業が読んでいそうな新聞雑誌に広告を打つ予定。これで、相談窓口の存在やチェックリストの存在というのを広く知っていただきたいと思う。また吉岡先生からいただいた実態把握の件については、今回第一弾の調査をやってみて思いもよらないことがたくさん出てきたということもあるため、ここの部分については第二弾の調査で更なる深掘り、もしくは実態把握に努めていきたいと思っている。それに加えて鵜飼構成員から話があった古い OS については、実は設問が悪かった可能性もあると思っている。具体的には、使っている端末は何ですかとしか聞いていないので、実はネットに繋がっていない、あるいは管理だけしている、といったものが紛れている可能性もある。そこの部分は第二弾で深掘りしたいと思っている。ただ、いずれにしても対策そのものは NISC と連携しながら行っていく予定なので、アップデートできないものの排除というのは進めていきたいと思う。また園田構成員からいただいたお話で、青くて下線が引いてあり、リンクのように見えるというのは、私自身としては新発見だった。今後気を付けたいと思う。いずれにしても今回かなり突貫で作ったところと、専門家が書いてくるものはきちんとしているが普通の人は読んでも分からないということがあり、ここをどのように通訳するのかというところにかなり労力を割いたため、次のバージョンではもう少し頑張りたい。次のバージョンは検索すらできない人もターゲットにしていかなければならないと思っているので、引き続きご指導いただければ。また名和構成員からいただい

た公的ドキュメントや専門家が使うツールに飛ばして紹介すると良いのではないか、もしくは他のものと表現を合わせたら良いのではないかというお話があったが、実は最初はそうなっていたものを全部削った。これは対象読者像がプロではないという前提なので、やはりなるべく簡単なものにしたいことと、他の方からこれでも量が多いという話があり、私たちとしても、一項目を見開きで済ませたかったが、結局収まらなかった。もう少しシンプルなものを志向していきたいと思っており、チェックリストだとそこは難しいが、ガイドラインではやりたいと思っている。また岡村構成員から最後にご指摘いただいた、聞き耳を立てている人対策だが、覗き見対策と通信盗聴対策は入れていたが、聞き耳対策は盲点だったので、是非次回に入れたいと思う。

藤本構成員）

スマートシティガイドラインについて、素晴らしいガイドラインをお作りいただいたので、是非とも広く使っていただければと思っている。このガイドラインを有効に活用するためにはマルチステークホルダー、いわゆる参加組織のどの部門にこれを読んで有効に使うようなセキュリティ人材がいれば良いのかというのを考えていく必要があると思っている。また、現状どういうところに人材がいて、どのように育てていけばいいのか等、その辺の議論も併せてしていくと良いのではないかと思っているので、もし現状の調査をされているようであれば教えていただきたい。

小山構成員）

まずこのセキュリティガイドラインは大変意欲的な取組で素晴らしいと思う。ガイドラインの中で認証のことについて何箇所か触れられているが、スマートシティというものを考えた場合に、今までの IT 分野と違う大きいもの同士がいきなり相互接続していくということで考えると、生まれた時からゼロトラストアーキテクチャのようなものをしっかりと取り入れていかないとセキュリティ対策が行き届かないと思っている。どんなに良い対策をしても、デバイスや ID 管理の重要性が見直される瞬間が来ているのではないかと考えている。今の IT ネットワークにおいては、人が使うデバイスをどう認証するかといったことは、もともと手元にあるデバイスが大半なので、しっかりと出来てきたかというと、それでも意外と出来てこなかった面が多いと思う。今後は最初からどこにあるか分からないネットワークや都市 OS の上で、色々なサービスが相互に繋がっていくことを考えると、モノの管理の基本を始める必要があるのではないかと思う。モノを特定して管理する、ベースをしっかりするということをセキュリティ対策の基本とするべきと考えており、その点について指摘させていただいた。

岡村構成員）

漏えい等が問題になる具体的なケースでは、例えば大手金融機関が合併したが、片方は 5 年保存、もう片方は 6 年保存でどちらのルールに従っていいか分からない、廃棄したのは良いけれど、廃棄のルールも矛盾するので果たして正規に廃棄できたのか、それとも紛失したのか分からないといったインシデントが多く続いてきた。おそらく今回も様々な利害関係者が入ってくるため、それぞれの個別ルール自体が不整合であるがゆえの色々なインシデントまがいなことが起こるのではないかということが一点。それから、それぞれフォーマットが違うので他の利害関係者とデータのやり取りができない、外字等のフォントが未だに不整合だというような問題、更にはワタナベのナベという字だけでも山ほどあるので、データマッチングをしようと思ってもできないという完全性や可用性に関する問題もあるので、そういう点も更に深掘りしていく必要があるのではないかと考えている。

若江構成員）

スマートシティリファレンスアーキテクチャを読んでみると、多少パーソナルデータの扱いという項目もあるが、プライバシーの観点が少し弱いと思っている。スマートシティ官民連携プラットフォームの分科会の内容を見ると、もし扱うとすれば総務省がやる分科会で扱う以外ないというところもあり、セキュリティガイドラインにおいては個人情報を守るための検討をしていると思うが、更にデータの取り扱いそのものに対するルールの検討も今後 2.0 版で厚めにしていただけるといいと思う。

後藤座長）

スマートシティではマルチステークホルダーが関与するため、横方向では様々な事業者が繋がり、縦方向ではメインの事業者から一人一人の個人、市民というエンドユーザーまである。そのような縦横がある中、スマートシティの見方がスマートシティの内側を見ている感じがあった。実際に情報やプライバシーデータの流れを考えると、スマートシティの外側との関係も大きくなるので、最初どのあたりから固めていって、どう展開していくのかという大きなスケジュールが見えてくると良い。

中溝サイバーセキュリティ統括官室参事官（総括担当））

質問にお答えにするというよりは、いろいろご意見として賜って引き続き検討を深めてまいりたいということではあるが、お答えできる範囲でコメントする。まず藤本構成員からご指摘があった今のスマートシティのステークホルダーの現状というところでいうと、正直、我々もこの検討を始めたばかりということもあり、今後は現状を聞きながらセキュリティの在り方を考えていくことを予定しており、その過程でまたご意見いただけたら有難い。また、小山構成員からご指摘があった認証が大事という点は非常に認識しており、ID 管理あるいは認証の強化と理解しているが、そこもしっかりガイドライン第 2 版をこれから来年春へ向けて作っていく中で、念頭に置いて取り組んで参りたいと思う。それから岡村構成員からご指摘があったデータの保存のルール、あるいはフォントの不整合のルール等の点も重要と認識した。今回セキュリティガイドラインということで検討しているが、実はこのスマートシティのリファレンスアーキテクチャの検討の場の中で、データ連携の在り方の検討が行われているし、内閣府の別の場でもデータ連携基盤というような取組があって、フォーマットの統一の議論も行われている。いずれにせよ、そういった議論と並行してセキュリティをしっかり検討していくというのは大事だと思うので、十分留意して参りたい。若江構成員からご指摘があったプライバシーの点は、私どもとしても同じような問題意識を持っており、スマートシティについては色々な報告書、ドキュメント、ガイドライン等があるが、実はセキュリティに特化したものは諸外国を見ても全く見当たらない、プライバシーについても見当たらないというような状況である。今回セキュリティに視点をおいてガイドラインを作っているが、プライバシーの視点も少し 2.0 版へ向けて入れていく必要があると思っている。一方で、別のスマートシティの連携の検討の場でもプライバシーの部分は色々検討が行われる見込みになっているので、そことも連携を取りながら検討を深めて参りたい。最後の後藤座長のご指摘の点の対象者ということだが、これは参考資料 3 の本文 4 ページ目に想定読者の記載がある。想定読者を読み上げると、①としてスマートシティ全体を統括するサービスオーナー・推進主体、具体的には地方公共団体や事業者等。②としてスマートシティ事業に関わる事業者および利用者、ということでクラウド基盤、都市 OS 等のシステム提供者、IoT 機器、ネットワーク機器等の機器メーカー、ソフトウェア、アプリケーション等のサービス提供者、センサーデータ、フィールドデータ等のデータ提供者等と書いている。非常に野心的かもしれないが、要は関係者の対象を幅広くしたいと考えている。後藤座長のご指摘では、これを実際に使うユーザー、いわゆる消費者といった方々も念頭にということと受け取っている。いずれにしても私どもとしては、まずは今申し上げた読者を対象にこれを守って頂きたく、周知して参りたいと思っているが、ステー

クホルダーやさらにそれ以上のことも念頭に置き、検討を深めていけたらと思っている。

徳田構成員）

一つは私たちの実体験の話で、スマイルクーポンというサービスを日本の藤沢市で実験をしたことがあり、それをスペインのサンタンデールに持って行き、実験しようとした。どのようなサービスかというと、スマイルをディスプレイの前で作ると自分の顔写真が映るわけだが、100%スマイルか 80%スマイルかというスマイルの度合いとその時の天気の状況などのコンテキストに応じてパーソナライズされたディスカウントクーポンがスマートフォンで獲得できるものをつくった。スペインに持って行き、実験をしようとしたら、EU の GDPR で、12 歳以下の方が自分の顔をパビリックディスプレイに表示する行為が許されていないため、親の承諾があるかというボタンでまず確認しなければいけなかった。今のガイドラインの中でいうとマルチステークホルダーでサービスを多国間で流通させようと思っている場合に、実は GDPR などのデータ保護規定が違うとそこに壁があるというのが一点。もう一点はこれもサービスのマルチステークホルダー問題だが、藤沢市の中にパナソニック等がサステーナブルスマートタウン（SST）というのを作って、600 戸ぐらいの住宅を売り、全部ネットワーク的に繋がっているという素晴らしいモデルを作ったが、そこの豪雨を検知・予測するセンサーシステムと藤沢市が自治体として出している退避避難を予測するサービスにコンフリクトがあった。SST ではこの雨なら全然安全だからここにいてくださいというが、自治体の方は避難して下さいというような状況があった。色々なサービスが出てくると、マルチステークホルダー間でのコンフリクト問題も起きる。それはセキュリティの問題かと言われると微妙なところだが、マルチステークホルダーの問題というのが、データに関しても非常にセンシティブである。各ステークホルダーは相手のステークホルダーがどういうポリシーでシステムをつくっているかが分からないので、いろいろ事実例でトラブルが起こりうるという報告である。

戸川構成員）

NOTICE のご説明について、非常に広範囲にわたるところで、よく理解できた。今回実施内容の変更についてご報告があったが、この実施内容の変更は、今後どういった指針によって変更があるのか、もし決まっていること、あるいはお考えがあればお聞かせ願いたい。

吉岡構成員）

資料 26-3 の 4 ページ目に NOTICE 注意喚起の取組結果というグラフがあり、最近の５ヶ月分のところは色が二つに分かれており、色が濃くなっているところは前年度に検知されている IP アドレスと理解しているが、あまり数が変わっていない、むしろ増えているような感じになっており、このデータをどう読むのかというのをまずお聞きしたい。こういうものを見つけて検知をして注意喚起をした効果がどう見えているのかということと、もしこれが毎月同じものが見えていることだとすると、どうしてそうなっているのかというあたり、もし情報があれば教えていただきたい。

NICT 久保田所長）

実施計画の変更の今後については、現状の実施計画の ID パスワードの組み合わせは現時点で最良と思われれるものに更新したため、しばらくはこの組み合わせで調査を実施することになると思う。ただし、ご承知の通りマルウェアの攻撃は日々変化していて、NOTICE の調査の過程で新たに ID パスワードの追加が必要になる可能性は否定できない。

なので今後も状況を調べながら、時代に追従していく必要があると思っている。また、吉岡構成員の質問だが、おっしゃる通り前の月から同じ IP が見えているケースというのが半分くらいある。これは時間が経つとだんだん減ってはいくが、必ずしもユーザーに警告が伝わっていない、ユーザーがきちんと認識していないといった可能性がある。まず、インターネットサービスプロバイダーがユーザーにアラートを出すが、メールで出した場合、スパムメールと思われたり、ユーザーが真面目に読まなかったりといったケースがあるということで、ISP によっては手紙や電話でコンタクトするケースもあると聞いているが、これはかなり ISP にとっては負担になる。つまり、必ずしも全ての ISP で出来ているわけではないということで、今後もそういった状況への対応は検討する必要があると思っている。

高村サイバーセキュリティ統括官室参事官（政策担当））

補足をさせていただく。まず、実施計画の変更の関係だが、そこは久保田センター長がおっしゃった通りで ID パスワードを増やしていくケースはあると思っている。その一方で、この NOTICE という取組は、配付資料 26-3 の 1 ページ目にあるように、令和 5 年度末までの 5 年間の時限立法ということでやっている。令和 5 年度までに、全く新しい攻撃に今回の NOTICE の法律の仕組みで対応できるかどうかという部分もあるが、おそらく淡々と ID パスワードを増やすだけだと思っている。これ以上の対応が必要なものが出てくるようであれば、時限措置の延長もしくは単なる延長ではなく、やる内容を増やした法律をつくっていくという可能性もあると思う。いずれにしても、この 5 年間で NOTICE の取組を続けなくていい、きれいなネットワーク環境というものを作れたら有難いと思っている。その観点からいくと、吉岡構成員からいただいている話だが、実はこの根雪のようにいつまでも対応してくれない人よりも、我々からするときれいにしたはずなのに、何故か毎月 150 件くらい新規がでてくる方が深刻な問題で、これが何なのかという原因は突き止めて対応していきたいと思っている。おそらく新たに設置する VPN 機器があって、その管理を請け負っている事業者が管理が面倒だからといって統一的なパスワードを入れているとった推察はしているが、ISP の直接のお客様ではないので中々ここにたどり着かない。なので、ここをもう一段踏み込んで ISP と連携しながらやっていきたいと思っている。

斎藤構成員）

現状、放送事業者では主に早期警戒情報をいただいている。IoT・5G セキュリティ総合対策 2020 にも記載のある通り、令和 2 年 3 月の省令改正を受けて免許申請におけるサイバーセキュリティの対策というものが求められる状況になっている。脆弱性の情報の分析や必要な対策を取る上でも、情報共有が非常に重要になっているので、来年度もこの体制は維持していきたいと思う。

鵜飼構成員）
資料 26-5 の 2 ページ目に、国産のサイバーセキュリティ製品市場の活性化が一つの目的でもあるというご説明をいただいたが、NICT が IoC 情報等の分析を実施し、製品ベンダーがそれを使ってお客様にサービスを提供し、その製品の価値の向上に資するといった取組ができるのか。単純にそういうことがもしできるのであれば、メーカーとしてやったほうがいいと思った。

名和構成員）

資料 26-5 の 3 ページ目のナショナルサイバートレーニングセンターの強化の SecHack365 について、25 歳以下の若

手セキュリティ人材の育成だが、応募から選定して受講者を選ぶということだと思うが、これに対しての個人の信頼性確認を予算として割り当てているのかという点をお聞きしたい。割り当てていなくて、今いる人員で個人の信頼確認の専門性を持っていない方がやった場合、リスクが残るのではないかと思う。

高村サイバーセキュリティ統括官室参事官（政策担当））

鵜飼構成員と名和構成員のご意見にまずは回答させていただく。まず、資料 26-5 の 2 ページ目、サイバーセキュリティ統合知的・人材育成基盤の構築という部分だが、資料の左半分にサイバー攻撃分析環境というのがある。これは NICT がつくっている STARDUST 等々含めて実際には民間企業の方々、その他諸々の方々にもご活用いただいているが、こういった形のものを広く皆さんに開放できるものを作っていきたいと思っている。ただ最後は運営費を含めて改正する形にならざる得ないところはあるかもしれないが、日本の分析をする方々のインナーサークルを作っていけると嬉しいと思う。是非こういうところに鵜飼構成員、名和構成員にもご参画いただけると有難いと思う。加えてここで単に分析してもしょうがないので、セキュリティ機器テスト環境という形になっているが、ここで得られた知見というのは、こういった新たな攻撃などに自分のところの製品が対応できるのかというような意味でのテスト環境というところへなるべく早期に反映できる。理想的には自動的に反映できるものが作れれば嬉しいと思っている。例えば、新しいタイプのウイルス（ランサムウェア）が出てきて騒ぎになったときに、セキュリティベンダーが自社のサービスを使っていればこのランサムウェアに対処できると、エビデンス込みでアピールできるような環境が作れれば嬉しいと思っている。いずれにしても、どうすれば作れるのかという部分を含めて色々研究課題はあるとは思っているので、是非皆さま方のご指導を賜れればと思う。名和構成員から頂戴した Vetting の関係について、指導を含めたアトリビュートの話だが、基本的に現状ではやっていない。そもそも論ではあるが、日本の国の制度の原則として、科研費などの競争的資金には実施地の限定、国内でやることという限定をかけているケースが多く、そこに国籍要項や指導要項は入っていないので、そこを今のところ先陣を切ってやるのが結構難しい状況にあることをご理解いただければと思う。ただその一方で、本当にそれでいいのかという部分は統合イノベーション戦略全般の中でも議論されているので、そこの中でやっていいという話、もしくはやるべきだという話になるのであれば、当然ここについても予算を付けてやらせていただきたい。ここの部分はこの国の現状はこうですというご説明しかできないので、その点でご容赦いただければと思う。

中溝サイバーセキュリティ統括官室参事官（総括担当））

放送分野については、令和 2 年 3 月の省令改正で報告事項とサイバーセキュリティインシデントに関する事項の採用を盛り込むような改正をさせていただいたところで、サイバーセキュリティの強化を放送分野でも進めていただきたい。情報共有が大変大事だということも承知しているので、放送分野における情報共有の体制の整備について我々としても必要な支援等をして参りたいと思っている。

吉岡構成員）

先ほどのお話の流れの中で、新しい IP が毎月見えるという話があったが、真に新しい機器なのか、同じ機器の IP アドレスが動的割り当てで変わっているのか、については確認した方がいいと思った。全体数があまり変わってないところを見ると、いわゆる IP チャーム、いわゆる攪拌で変わったように見えているだけかもしれないと感じたため、コメントした。

徳田構成員）

SecHack365 をやらせていただいている NICT からのコメントということで、名和構成員がおっしゃるように、また先ほど高村参事官が言われたように、申請される方のアトリビュートをオフィシャルに書き込むことはできないので、選ぶ段階でベストエフォートでやっているのが現状である。入口の部分より、私たちが心配しているのは卒業した後で、１年かけて育った方たちがダークサイドに行かないように卒業生一人一人に対して SecHack365 リターンズというイベントをやっており、卒業した人がまた SecHack365 を次の世代の学生諸君たち、若い人たちの教育にチューターとして戻ってきてくれたり、または他の明るい側の職を考えて下さったり、そのあたりのバランスが重要である。非常に優秀な方が育ってきているので、今おっしゃったような入口のチェックも大事だが、実は出口、卒業した後にダークサイドに行かないように皆さん気を付けてくださっていると思う。

岡村構成員）

ハンコ廃止が提唱されているが、振り返ってみると自身でもこの一週間、ネット通販で買い物したり、あるいはコンビニでスマホのバーコード決済で買い物をしたりということで、一切ハンコを使っていない状況である。結局のところ実はハンコそのものはあまり関係がなくて、紙ということが妨げになっている。民間部門では紙なしで何万円もするものを買えるため、むしろ紙からの脱却と、それに伴う認証の問題が本質だと思っており、ICT の時代は視点を変えた方がいいのではないかということを申し上げる。

後藤座長）

意見も出尽くしたようなので、意見交換は以上とさせていただく。本日も自由闊達なご意見をいただけたことに感謝申し上げる。

（3）閉会