参考資料１

サイバーセキュリティタスクフォース（第 21 回）議事要旨

1. 日 時：令和 2 年 2 月 20 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、鵜飼構成員、岡村構成員、小山構成員、齋藤構成員、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、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)、桑山耕平(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)、後藤宏昭(TIS)

【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)、塩崎放送技術課長、岩片地域情報政策室係長、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 21－1　地域のセキュリティコミュニティの形成について（事務局、一部構成員限り）

資料 21－2　インシデント演習シナリオ（事務局、構成員限り）

資料 21－3　スマートシティのセキュリティについて（事務局）

資料 21－4　今後重点的に取り組むべき研究開発の推進方策について（事務局）

参考資料 1　サイバーセキュリティタスクフォース第 20 回　議事要旨

5. 議事概要

(1) 開会

(2) 議事

◆　議事（１）地域のセキュリティコミュニティの形成について、事務局より、「資料 21－1　地域のセキュリティコミュニティの形成について」、「資料 21－2　インシデント演習シナリオ」を説明(省略)

◆　構成員の意見・コメント

名和構成員)

「資料 21－2」でサイバー演習のシナリオ案がまとめられているが、演習の実施目的や達成すべき目標について、どのように考えているか。また、1 ページに事件・事故から、何が起きるのかを体験すると記載されているが、今後どのような

進展があるのか気になった。評価マニュアルにおいて達成すべき目標と評価がどのようにリンクしているか、それについての設計がどのようになっているか、あるいは今後の見通しなどについて、教えていただきたい。

大森サイバーセキュリティ統括官室参事官(総括担当))

現在まだそのようなところまで内容が詰まっていない状況である。

名和構成員)

韓国や台湾、米国、EU では、HSEEP（Homeland Security Exercise and. Evaluation Program）のような演習と評価の実施のためのプロセスが無料で公開されている。テンプレートが 200MB の文書になっていて、70 種類のシナリオが収められている。他国の知見が既にあるので、それらを参考にして、それらをベースにグレードアップしていけば、他国よりも良いものが効率よく実施できると思う。

中尾構成員)

基本的に、「資料 21－2」のインシデント演習のシナリオ案の対象は、経営層あるいは戦略マネジメント層であるのか。日本の中で CISO という位置づけの人は経営層の一部や、戦略マネジメントのサイバーセキュリティ担当である。ところが日本の組織体制として、多くの企業では、CISO はかなり経営層に偏っていて、サイバーセキュリティの担当というよりも、それを管理するガバナンスの担当の上の立場の人になっている。そのような人を対象とした演習としては、具体的なサイバー演習を担当している人たちからヒアリングを行い、それを如何にコントロールするかというレベルが非常に重要になるのではないかと考えている。このような演習も有効であるが、対象に経営層などの上の層を加えることができれば、より分かりやすくなると思う。

齋藤構成員)

「資料 21－1」の 11 ページに「自発的な動きがあることを前提に」と記載されているが、これが非常に難しいところではないかと考えている。地域ということもあり、地方自治体等が主体となって、その地域で開催されるイベントのセキュリティ対策や、地域特有の問題点などを事前に提起していくような動きが出ればよいのではないかと考えている。大都市と地方で根本的に異なるのは、セミナーや演習の機会である。地方はそのような機会が非常に少ない。放送局の系列局に話を聞いたところ、福岡でさえ、セミナー等があまり開催されていない状況である。無料、有料を問わず、このような機会が増えるとよいと考えている。セミナーが終わった後に懇親会を開催すれば、地域の繋がりが出来るきっかけになると思う。NISC の分野横断的演習のように、説明会を丁寧に実施して、経営層から実務者までを含めた参加による本番の演習を実施し、その後に反省会を実施して次に繋げていく流れが大切なのではないかと考えている。

コミュニティの維持というところでは、先ほど話があった人事異動がネックになってくる。やはりコアメンバーを決めて、事務局に専任の担当者を置いて、人脈が途切れないような体制を整備することが大切である。放送分野のセプターの事務局は民放連が実施しているが、ここ６～７年は同じ担当者が運営している。インシデントが発生すれば、いつでもその人に報告すれば、総務省や関係各所に連絡できるという安定的な運営体制になっている。平時、有事の信頼関係の構築を含め、信頼できるキーマンの存在が大切なのではないかと考えている。

若江構成員)

「資料 21－2」のインシデント演習のシナリオ案を見ていて、経営層にも受け入れられやすい工夫が必要ではないかと感じた。NCA や JNSA で開催されているゲーム形式の演習に参加したことがある。経営層向けのゲームでは、セキュリティ対策を取らなかったことによって、どれぐらいの損失が発生したかや、対策を講じたことによって、結果的にどのくらい資産を増やしたかといった要素があって、経営層も興味をもちやすい内容になっていた。セキュリティ対策に取り組まないことが、ビジネスリスクに繋がることを体感できる要素があればよいのではないかと思う。コミュニティをどう形成していくかという話もあったが、それについては、ここで記載のあるようなセミナー形式に加えて、例えば、温泉イベントのように地域のコミュニティが主体的に取り組み、互いの関係を築いていけるようなイベントを、総務省が支援するという形で全国に増やしていくことがあってもよいのではないかと考えている。

岡村構成員)

地方から出てきており、かつ中小事業者という立場からやや厳しいことを申し上げるかもしれない。今度、民事訴訟が ICT 化される中で、裁判所は某外資系のソフトを導入する予定である。小規模法律事務所のような中小事業者が困っているのは、専門人材を雇用するのが困難であることである。財務的にも困難である。それでどうするのかについては、アウトソーシングを活用して、リーズナブルな料金の事業者に維持管理を依頼することができないかという考え方になる。そのような考え方しかなかなか成り立たない。現在、中小事業者では、さまざまな費用負担が大きくなってきており、専門人材を雇用するハードルの閾値が上昇している。そのような状況を踏まえて、地域のセキュリティ対策の強化についてのゴールがどこにあるのかということを考えなければならない。例えば、東大阪には多くの中小企業が集積している。大企業の下請けを行い、サプライチェーンの末端でかなり高度な機密等を扱っている。最終的なゴールは、中小企業がアウトソーシングを活用できるように、中小企業を支えるセキュリティベンダーのようなものを育成し、そのようなベンダーを育てるためのコミュニティを作る。そのような考え方を１つの柱にしてもらうことが現実的な対策になるのではないかと考えている。

関西では、関西情報センターなどが講演会等を実施しているが、講演者は地元の有名人と東京から呼ばれる人の 2 種類であるという状態である。数年前までは専門人材が関西にもたくさんいたが、今では、数多くの主要な専門人材が東京に引き抜かれてしまった。そのような意味で今の関西は焼け野原状態になっている。コミュニティを育てるといっても、残った固定メンバーでやりくりをしているというのが現状である。このような状況と中小企業が置かれている厳しい状況を理解していただきたい。関西でさえ厳しい状況であることから、他の地域ではもっと厳しい状況になっているかもしれない。もう少しその先にあるゴールについても検討をお願いしたい。

小山構成員)

「資料 21－1」の 11 ページに「平時・有事における情報共有を可能にする信頼関係はどのように構築されるのか？」という問いかけがある。セキュリティのコミュニティの形成や情報共有に取り組んできた ICT−ISAC の経験から感じているところについて少し話をしたい。有事における情報共有は未だかつて上手くいったことがない。有事になると、自身がインシデントに見舞われたり、社会がある程度騒がしくなっている状況で混乱したりするので、その時点でコミュニティとの情報共有を行おうとしても、本当の情報が出てこない。情報を出すこと自体がリスクになるケースもある。気を遣って何が起きているのかを聞きづらい状況である。むしろ平時の情報共有について、しっかりと取り組むべきであると思う。平時の情報共有についても、演習や情報共有の機会があって、その時に集まってきたメンバーだけでは、なかなか情報共有が進まないのではないかと考えている。お互いのことをよく知らないという観点でしゃべることがリスクであるということを感じるのではないかと思う。地域であれば、商工会議所のように常々集まっていて、セキュリティ以外の信頼関係がしっかりと出来ているところに入っていき、そこでセキュリティの話題を提供して意見交換してもらうという取組が良いのではないかと感じている。その中で会話が進むと、自社と他社のレベルの違いをなんとなく感じることが出来たり、

他社から聞いたことで自社において出来ていないものは、自社に持ち帰り、問題ないかという検討がなされたりする。自社のレベルの高さが分かるので、セキュリティ対策を進めていくうえでの予算を獲得するモチベーションや推進力に繋がる。有事の情報共有は難しいが、平時の情報共有はできると思う。平時は新しいコミュニティを作るよりも、今確立されている信頼関係のあるコミュニティの中にセキュリティ分野の人が入っていく方が良いのではないかと考えている。

鵜飼構成員)

当方、サイバーセキュリティを始めたのは 20 数年前になる。セキュリティコミュニティに育ててもらったと感じている。セキュリティコミュニティの中にずっといた人間からみると、「資料 21－1」の 11 ページに「セキュリティコミュニティが自発的に立ち上がるためにどのような要素が必要か？」という問いかけがあるが、やりたい人が勝手にどんどん進めていって、参加したい人がそれについてくる、それに尽きると思う。そういう意味合いでは人に大きく依存する。そのような人がいなければ立ち上がらない。反対にそのような人がいれば立ち上がる。政府が支援できることを考えたときに、コミュニティの中に入っていって、何かをコントロールするということになると、コミュニティによって色があるので、あまり得策ではない。その一方でこのようなコミュニティがあることを宣伝するプロモーションとしての役割は有難いのではないかと思う。情報発信に課題を抱えるコミュニティが多いので、非常に助かると思う。そういう意味合いでは、自立的な在り方を損なわないという部分は大事である。横から暖かく見守るプロモーションにしっかりと取り組むのがよいのではないかと考えている。

◆ 議事（2）スマートシティのセキュリティについて、事務局より、「資料 21－3　スマートシティのセキュリティについて」を説明(省略)

◆ **構成員の意見・コメント**

藤本構成員)

「資料 21－3」の 14 ページのスマートシティのガバナンスやマネジメントについて、「産官学などの様々な主体による共同での運営や運用」と記載されているが、その通りであると思う。様々な主体で、リスクマネジメントプロセスを適切に回していってもらいたいということは言うまでもないが、スマートシティ全体で見て、それぞれのリスク対策について、誰が責任をもって実行するのかという責任所在が決まっていなければ、なかなか実効性を持たせられないと思う。スマートシティのプロジェクトは未知の部分が多いため、最初から責任所在を明確にすることは難しい。しかしながら、多くの人がリスクに気が付いていたにも関わらず、そのリスクに対する対策が実施されておらず、事故や事件に繋がってしまうことは避けたいため、全体のプロジェクトが進む中で、関係者が集まるなどして気が付いたリスクを出し合って、どう対応するかを話し合うような場を何回か設けるということを検討してほしい。その場では責任所在が決まらなくても、誰かがそれを実施しなければならないということが共通に理解されることにもつながると思う。

後藤座長)

それぞれのステークホルダーの取組を共有し合うということになるか。

藤本構成員)

はい。それも大切であると思う。全員がどこかに集まって、リスクアセスメントを実施してみる。そういう場もあるとよいのではないかと考えている。

小山構成員)

スマートシティのセキュリティの固有の問題ではないかもしれないが、5G のセキュリティをどのように保てばよいのかを考えているが、おそらくスマートシティのような取組が、5G の１つのユースケースとして有望であり、そこから出てくる具体的なテーマ等を深堀りしていく方がリアリティのある検討が出来るのではないかと考えている。「資料 21－3」を見ていると、5G というキーワードが出てこない。一世代前の WiFi やスマートフォンをベースとした取組の事例が下敷きになっている。むしろ 5G のユースケースの１つとしてのスマートシティとして捉え、その時の課題が何であるかを議論できれば、今後検討の広がりに繋がるのではないかと思う。

戸川構成員)

スマートシティ特有のセキュリティを考えた場合に、もう少し一般化した話を考えた方がよいと思う。人材育成を含めた地域のセキュリティの話と、5G や IoT のセキュリティの話を深堀りすることが、スマートシティのセキュリティに繋がるのではないかと思う。地域のセキュリティを考えた場合には、「資料 21－1」や「資料 21－3」に記載されていたように、大学の役割が各地域でセキュリティに関しても大きいのではないかと感じている。東京に比べ、地方は人材が少ないということがあるかもしれないが、各地域には大学があるので、大学にいる情報セキュリティの専門家を上手く活用することで、地域が活性化し、セキュリティ人材も上手く育ててもらうことで、スマートシティのセキュリティが担保できるようになると考えている。5G や IoT、地域のセキュリティ全体を高度化していくこと、そのものによって、「資料 21－3」の 14 ページに記載されているスマートシティのセキュリティの課題への対応を底上げすることができるのではないか。そのうえで、「資料 21－3」の 14 ページに記載されている個別の課題にトライしていくことが重要であると考えている。そのためには、学だけでなく、その地域に根差した企業や官も含めて、産官学の強い結びつきが非常に重要であると思う。

若江構成員)

「資料 21－3」の 14 ページに記載されている「セキュリティ対策の促進に向けて政策的にとり得る手段は何か？」という部分では、スマートシティのセキュリティにおいて、どう脆弱性をハンドリングしていくかが気になっている。脆弱性を見つけて報告する側のマナーは大分理解が進んできているように思うが、他方で、報告される側のアレルギーのようなものがまだまだ解消されていないのではないかと考えている。脆弱性があることを隠すのではなく、むしろ見つけてもらって、攻撃される前に修正するという姿勢が重要なのはいうまでもない。そうした姿勢は、長年、セキュリティの問題に向き合ってきた ICT ベンダーの間では浸透していると思うが、これからスマートシティで大きな役割を担うことになるメーカーなどはどうだろうか。メーカーに対して、脆弱性が報告された場合に対応するための啓発や意識改革を進める方向で、政策を推進してもらいたいと思う。

名和構成員)

スマートシティのような仮想空間を積極的利用する町には、放火するなど悪い事をする人、つまりサイバー犯罪者が出現すると思う。サイバー版のポリスや火消し組のようなものを作ることが必要である。現在、CSIRT や ISAC 等があるが、

町レベルになると、町全体のガバナンスを効かせることは厳しい。今、物理的にあるレスポンスオーガナイゼーションと呼ばれている交番や消防署のようなものを、スマートシティの中に組み込んでいかなければならない。大規模にインシデントが発生するという部分の抑制が効かない。そういう部分の政策が必要であると考えている。

徳田構成員)

「資料 21－3」の 14 ページの「セキュリティに配慮したスマートシティの普及のための政策」について、大学時代に、EU-Japan でスマートシティのプロジェクトを実施していたが、実際に自治体の職員と協働していると、一番問題であるのは、情報セキュリティだけでなく、情報化を推進する部門の人が少なすぎることである。今でも人材が不足しており、NICT では CYDER というサイバー演習を実施しているが、自治体職員の受講者数は国家公務員の受講者数と比較し、３年間で残念ながらそれほど増えていない。担当者が受講のため休んでしまうと現場が回らなくなってしまうということがその理由となっている。明らかに人手不足である。首長に相談した方がよいかもしれないが、都市の機能が着々とスマート化し、5G やローカル 5G、IoT のセグメントが増えていった際、情報インフラや組織のインフラを管理する担当者がいない限り、脆弱性のポテンシャルの高いところが増えることになる。今までの地震や水害の時にどうするかについては、物理的な空間の場合なので慣れている。職員が現地へ出向いて行き、水が道路に溜まっているところではどう対応すべきかがマニュアル化されている。実際にサイバー空間上でトラブルが起きたときには、まだまだ経験値が足りないので、スマートシティに行く前に、地道にシティ、セミスマートシティ、スマートシティという段階を踏まなければならない。そうしなければ、非常に高度なサービスを開始し、脆弱性を突かれたときに、対応が進まなくなる。ぜひサイバー演習も促進していただきたい。Society5.0 に向けて自治体もインフラが変わってきているので、首長には、もう少し人的リソースの割り当てを変えていってもらわなければならない。

中尾構成員)

スマートシティというコンテキストの中でいろいろと考える必要のあることが多いような気がしている。標準化の団体である ITU-T へも参加しており、ITU-T には SG20 があって、そこではスマートシティが IoT やセキュリティを含めて議論されている。ただ現状は、まだ標準化の土俵に、「資料 21－3」の 14 ページのスマートシティのセキュリティに関する論点も含めてスマートシティそのものが上がってきていない状態である。その理由について、いろいろな人と話をしてみると、スマートシティやスマート化というものを検討するときに、いろいろなステークホルダーが集まって、どのようなリクワイヤメントがあるか、何をしたいかによって、グランドデザインを描いて、そのグランドデザインに従って、システムをいろいろなステークホルダーと一緒に構築していく。そうなったときに、例えば、交通を始めとして、犯罪の防止、インフラの整備、廃棄物の処理、車の関係、医療の関係、金融の関係など非常に多岐に渡ったサービスのうち、グランドデザインの中に何を入れるかを設計していくことになる。その部分が多岐に渡っているので、共通のセキュリティの検討がなかなか実施しにくい。その中で IoT が１つのキーになっており、IoT の利活用ということでスマートシティをどのように扱うかという議論が大分出てきている。ただなかなか難しいのは、様々な個々のスマートシティに関するアーキテクチャ、システムの構成、要件、サービス提供の内容が異なってくるので、スマートシティで扱える共通の基盤がかなり限られていることである。共通の基盤はデータを吸い取って、それを格納するクラウドの環境であったりする。そこで問題になるのは、プライバシーに関係して、どのようにデータを扱っていくのかというところである。こういう部分が共通のセキュリティのイシューとして大きいと考えられる。

ICT のスマートシティ用のインフラを作っていくときに、出てくるセキュリティ要件については当然個々のシステムを作っていく中で、個々のシステムにとって必要なリスク分析を実施していかなければならない。構成するスマートシティの内容によって、想定する脅威や必要となる対応は一言では言えないような気がする。人材もかなり限られている中で、世界中でスマートシティが検討されており、英国のブリストルが英国政府からスマートシティの指定都市に認定されて、知人の英国ブリストル大学のサイバーセキュリティの先生に予算がついた。この先生はスマートシティのサイバーセキュリ

ティ担当としてリードしている。突然、セキュリティについて具体的に検討すると言っても何も分からないので、ブリストルのスマートシティにおいて何を作っていくのかというところから議論に入っていった。非常に大変であると言っている。そこは大学と上手く連携しているということなので、面白いのではないかと考え、NICT との間でも連携しようとしている。そういったいろいろな背景や議論があるので、この論点の中に書かれていることは非常に重要なポイントであるが、１つ１つについて、おそらくこうであるという断言ができないところが多々あるという気がする。データの扱いやインフラのクラウド構築については、おそらく共通になってくるという気がする。

後藤座長)

「資料 21－3」の 1 ページのスマートシティの意義のところで、データ利活用型スマートシティによる課題解決を目指している。たくさんの要素があるスマートシティの中でそれにフォーカスした場合、どういう論点になるのかという 14 ページに記載されている論点が、データ利活用型スマートシティと独立して一般的な概念として書かれてしまっている。データ利活用型スマートシティに絞ると、議論しやすいと思う。データ利活用によって付加価値が高まったスマートシティをどうやってセキュアにしていくのかという方向が定まるのではないかという気がする。

逆の発想で、安全な町は付加価値が高いという話が先ほど出たが、セキュアであることがスマート化の要件や魅力になるような方向、つまり Security for smart city あるいは、Security by smart city あるいは、Security with smart city という物理的なセキュリティを含めてセキュリティを高めることが価値になるという議論もほしいという気がする。

鵜飼構成員)

この手の施策を打ち出すと何が起きるかというと、Black Hat で日本のスマートシティの脆弱性を発見したという研究発表があって、自分自身がその発表のレビューを行うようなことがあるのではないかと想像できてしまう。同じような話が Black Hat で上がってきている。そういう意味合いで、セキュリティのブランドは非常に重要ではあるが、概ね研究者と名乗る人が出てきて、こういうことをするというのが次に見えることである。こういう研究発表という名の暴露が出たときに、どう対応するかという体制をしっかりと作っておく必要がある。Black Hat に研究発表が出るようなときは、結構話が７～８割盛られている。そこまで大したことではないので、そこでしっかりと反論しなければならない。そういうことができる体制を作っておく必要がある。

一方で簡単なセキュリティ上の問題が、次々と暴露されることも問題であると思うので、アセスメントをしっかりと実施すべきであると思う。先ほど話が出たがアプリケーションやサービス等が個別のシステムに結構依存すると思われるため、ブリストル大学の先生のように全部要件を見ていかないと非常に不安であるという印象がある。この中の一部のサービスで致命的なまずい問題があれば、スマートシティがやられたという話になってしまうので、ある程度の然るべき機関や人が全体の要件を分担して見ていく必要がある。「資料 21－3」の 11 ページの標準 API と記載されているところは、ここで何かしらの Open API があって、サービスの認証が行われたりすると思うが、ここはアセスメントを集中的に実施できるところであるので、しっかりと実施しておくべきである。いずれにしても一度走り始めたあとに脆弱性が多数出てくると思われるため、継続的に自分たちのサービスをアセスメントしていくような体制、何か暴露が出たときに反論していくような体制を同時に作っていく必要があると考えている。

◆ 議事（３）研究開発の推進について、事務局より、「資料 21－4　今後重点的に取り組むべき研究開発の推進方策について」を説明(省略)。

構成員の意見・コメント

林構成員)

前回の会合で意見を述べた内容について早速取り上げていただいたことに、御礼申し上げたい。

鵜飼構成員)

「資料 21－4」の 3 ページの「ハードウェアチップの脆弱性検知手法の開発」について、現在、足下で問題になっているのは、調達する機器に問題がないのか、今後 5G のチップを使っていこうと思っているが問題ないのかといったところではないかと推測している。現実的にそういったものやソフトウェアのバックドアを検出・調査する技術は、もう少し足下の技術ではないかと考えており、ここに記載されている技術はもう少し先の将来のアドバンストな技術である。足下の技術についてもまだ十分確立されている訳ではないので、確立していく動きがあってもよいのではないかと考えている。足下の技術をどのように考えているかについて気になる。

近藤サイバーセキュリティ統括官室参事官(国際担当))

ご指摘いただいた通りであると考えている。今後重点的に取り組むべき研究開発課題をとりまとめているところであるが、脆弱性の検査・調査に関わる足下の技術についても抜けがないように、しっかりと取り組むよう建付けを工夫したいと思う。

小山構成員)

ハードウェアチップやその脆弱性の話が出ているが、それに関連して、通信事業者においては、どのような機器を調達すればよいのかというサプライチェーンリスクが現実の課題になっている。例えば、中国の特定のメーカーの製品は購入しないように、同盟国の方が発言してきている。今後どのような製品を調達していけばよいのかという指針に繋がるような研究開発に取り組むことが出来れば、非常に助かると考えている。先日、NISC の会議でも、同じ趣旨の発言を行っており、重複するかもしれないが、脆弱性検知手法を開発したときに、いろいろなテストを実施すると思うので、是非そのテスト結果についての情報共有をお願いしたい。調達する際の調達仕様書の書き方においても、参考になると思う。サプライチェーンリスクの回避という視点を、今後重点的に取り組むべき研究開発課題に入れてほしい。

後藤座長)

インシデントの情報共有だけではなく、ホワイトリストのような製品の情報共有も実施していく必要があるという意見であった。

徳田構成員)

足下のテーマと 5 年先を見越したテーマがあるが、総務省の予算の付け方の関係で、情報理論に基づき安全性を担保するような量子通信と、伝統的な耐量子計算機暗号のハイブリッドなスキームなどが使われていくと考えている。予算の建付け上、テーマごとに予算が切られている。衛星通信を使って、秘密鍵だけ分配するようなハイブリッドなソリューションがあって、コストに応じて、いろいろな手法が採られるようになる。「資料 21－4」の 3 ページの下の部分に、「新技術・新たな攻撃に機動的に対応するための研究開発」を入れていただいたことは非常に良かったと考えている。全部量子通信だけで実施しようとすると、まだまだコストがかかるので、工程表に縛られすぎると、新しいハイブリッドスキームなどが経済的な理由で立ち行かなくなる。産業界のいろいろなセグメントが、各セグメントに応じたコストで導入していくことができるように、いろいろな形で柔軟に対応できるようにした方がよいと考えられる。「資料 21－4」の 4 ページにも「新たな脅威に対抗できる暗号技術の確立」が記載されているが、5 年先を見越すと攻撃手法も防御手法も変わっていくので、こういう形で記載していることはよいと思う。

後藤座長)

もう少し柔軟に新しいものを見ていくという話と、新しい技術に乗り換える部分をスムーズにするハイブリッドスキームの話があって、後者のハイブリッドの作り方自体も研究ではないかという提案であった。

岡村構成員)

現在、コロナウイルス騒ぎでテレワーキングが脚光を浴びている。2000 年以降、5 年に 1 回の頻度でウイルスの感染爆発が起きているが、今後もまた同じことが起きることが残念ながら予想される。しかしながら、テレワーキングのセキュリティの要件については、これまで議論がされてきたが、どこかのラインで引かないといけないものが、ぼんやりとしているような状況である。今後の日本社会における大きなテーマとして、テレワーキングにおけるセキュリティの実装という観点についても、今後の課題として検討していただきたい。

後藤座長)

スマートシティのセキュリティや 5G のセキュリティの環境にも近い話である。ぜひ検討していただきたい。

相川サイバーセキュリティ統括官室参事官補佐)

サイバーセキュリティタスクフォース第 22 回会合については、3 月 18 日の 16 時からを予定している。具体的な議事と開催場所については、後日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ため、引き続き協力をお願いしたい。

以上