サイバーセキュリティタスクフォース（第 24 回）議事要旨

1. 日 時：令和 2 年 5 月 28 日（木）10:00～11:30

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）、吉川徹志（内閣サイバーセキュリティセンター）、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】

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）、森下宇宙通信政策課長、塩崎放送技術課長、中溝消費者行政第二課長、中村電気通信技術システム課長、佐々木サイバーセキュリティ統括官室統括補佐、相川サイバーセキュリティ統括官室参事官補佐、水落地域放送推進室技術企画官（代理出席）

4. 配布資料

資料 24-1　IoT・5G セキュリティ総合対策 2020（案）
参考資料 1　IoT・5G セキュリティ総合対策プログレスレポート 2020
参考資料 2　サイバーセキュリティタスクフォース第 23 回　議事要旨

5. 議事概要

（1）開会

（2）説明

◆IoT・5G セキュリティ総合対策 2020（案）について、事務局より、「資料 24-1　IoT・5G セキュリティ総合対策 2020（案）」を説明。

◆構成員の意見・コメント

岡村構成員）※チャットによるコメント

34 ページにある「テレワーク」に関して私見を述べる。ひとくちに「テレワーク」と言っても、z 指摘どおり、①「三密回避」等の感染症対策を対象とする今回のようなものと、②首都圏や西日本などで近く発生が懸念されている大震災のような大規模災害（他に毎年各地を襲う集中豪雨被害もある）の発生時における事業継続性計画の色彩を有するものと、③我が国が重要課題とする少子高齢化社会の下における老老介護対策のような従来的なテレワークとで、そ

の形態、それに対するセキュリティのありかたについて、対策内容についても、共通部分と異なる部分の双方があるようだ。そのため、どのような射程距離を対象とするかによって、テレワークに関係する検討内容・検討結果が異なるようだ（これと親戚関係とも言うべき「リモート学習」もまた、シチュエーションによって異なるようだ)。また、オフィスの「三密」を回避し、通勤距離を短縮しつつセキュリティを保ち、また、大規模災害発生時には代替機能を営む方法として「サテライト」におけるテレワークの活用も考慮する必要があると考える。いずれにしても、今回の事態を契機として、世界的に情報ネットワークの利活用が質量ともに大きな変化を遂げ、極めて重要となる状態と見られているだけに、思ったよりも大きな課題であると考えている。その中でセキュリティに対する懸念がテレワークに対する障害とならないようにする必要がある（この点は数年前の情報通信白書でも指摘されていたと記憶している)。以上の見地からすると、第１に、いわゆる第二波、第三波到来の懸念を考慮すると短いスパンで当面の対策を公表する 必要がある。第２に、それとは別に、今世紀に入った頃から数年おきに新たなパンデミックが発生し続けていること、米連邦取引委員会などで下記ロイター通信の報道のような国際的動向もあることなどから、長期的に海外の動向も視野に入れて検討を深めるべき課題であると考える。

https://www.reuters.com/article/us-zoom-ftc/u-s-ftc-indicates-it-is-looking-at-zoom-privacywoes-idUSKBN22N2MJ?fbclid=IwAR2TccvZ2bBXDjpfGNeiBacR4mI2WA6aQj8Qoitax0Vw4RaQTGIYtwbOtI

このような次第で、総合対策案の上記項目においては、短期的・長期的の双方から、より踏み込んで検討すべき課題である旨、できれば付加していただければと考えている。

斎藤構成員）

5 ページ、34 ページのテレワークのセキュリティ対策についてだが、我々も今、テレワークを本格化してやっている中でこういったシステムはオンプレミスやクラウド等色々なパターンがあり、業務の内容に応じて適切なシステムを選択し、利用していくということが求められているのではないかと思う。セキュリティ対策もそのパターンに合わせた対応が必要ということをできれば本文に加えた方が良いのではないかと思う。総務省の「テレワークのセキュリティガイドライン第 4 版」でも非常に詳しく解説されていて、特にテレワークの仕組みのパターンにどのようなものがあるのかということについて重点的に書かれているため、業務内容に応じて適切なものを選び、そのセキュリティ対策をやっていくということを改訂版に加えた方がいいと思う。特に今、テレワークを導入するため、急いで社内システムへの VPN 接続を拡大しているところが多いと思う。こういったケースが増えているということは、サイバー攻撃によるセキュリティリスクも高まっているとみて良いので、設定、対策をしっかりやるということが必要である。

後藤座長）

テレワーク関係は非常に大事なポイントだと思う。

中尾構成員）

基本的に IoT・5G セキュリティ総合対策 2020（案）は全般的に網羅されていてよく書けているのではないかと思う。その中で言葉として気になる点として、リスク、脅威、脆弱性という言葉が出てきているが、脅威というのはマルウェアが侵入する等、何らかの発生する事象によって影響を与えるものを指す。一般的に脅威の情報というのは共通で共有したり認識したりすることに意味がある。脆弱性はシステム、コンピューター、ソフトウェア、ハードウェアに内在

する仕組みの欠陥で weakness よりも少し強いということになるので、これも基本的には共有したりそれに対する対策を取るということが重要になる。しかし、リスクという言葉は一般用語として少し曖昧で、こういった総務省が発行する IoT・5G セキュリティ総合対策 2020（案）の中のリスクという言葉と、一般人が使うリスクというのは少し異なる。一般人がリスクというと簡単に脅威といった話になるが、ここで使われているのは正式なリスクという意味だと思うので、基本的にはリスクというのは脅威や脆弱性等それなりのリスクの源となるようなものから算定された組織やある企業に対する損害を受ける可能性、想定される可能性を言う。そのため、例えばページ 4 ①に「5G の開始に伴う新たなリスク」とあり、これは悪くはないかもしれないが、「5G の開始に伴う新たなセキュリティ課題」とされた方がより正確である。もう一つ 25 ページをご覧いただくと 5G のリスク情報と脅威情報の共有の枠組みの構築とあるが、ここはリスク情報というのを脆弱性情報に変えていただいた方が、正確かと思う。サプライチェーンリスクとあるが、これは後藤先生の SIP（戦略的イノベーション創造プログラム）でも使われていて一般的な言葉になっているので、いわゆるテンプレートとしてのサプライチェーンリスクなのでこれは問題ないと思う。したがって、リスクという言葉の使い方を全般的にチェックしていただいた方が良いのかなと思った。

後藤座長）

この辺りの用語は非常に大事なので、事務局の方で全体を見直していただきたい。

若江構成員）

一点気になったのが 22 ページの NOTICE のところで、先日ネットメディアで赤阪参事官の対談の記事を読んだが、ここには、実は NOTICE で問題が見つかって注意喚起の対象となっているルーターは個人用ではなく、ほとんどが法人用のルーターだと書いてあった。これまでは脆弱なルーターの大半は個人用のルーターだと思っていたら個人用は結構安全だったということが分かり、驚いたが、これまでの啓発活動が効果を発揮してユーザのリテラシーが向上した、あるいはルーターメーカーの意識が向上して、新しい製品がセキュアになったということかもしれず、これまでの努力が実を結んだ成果として評価されるところだ。ただ、そうすると法人向けルーターの対策こそ急がなければならないと思う。しかし、（NOTICE の）公式ウェブサイトを見ても注意喚起の大半が法人用であるというような記載は見つかっておらず、IoT・5G セキュリティ総合対策 2020（案）でもその辺りの記載が見当たらない。むしろ「専用のサポートセンターを設置して行政相談窓口や消費生活センターと連携して、利用者に適切な IoT セキュリティ対策を案内する」等と書いてあるのは個人ユーザを念頭に入れているように見えるので、法人向けルーターの対策を講じるような記載があっても良いのではないかと思った。特に対談のところでも指摘されていたが、法人向けルーターの場合、メンテナンスなどで外部からアクセスする必要があるのでポートを開けておかなければならないため、パスワードがしっかりしなければならないが、かなり甘いものがたくさんある一方で、NOTICE での注意喚起が難しいということだった。NOTICE で今リーチできるのはルーターを所有している法人であるが、法人はその設定を SIer に丸投げしていて自分たちはよく分からず、SIer がやってくれているはずだと思い、SIer の方はメーカー、あるいは法人がやるはずだと思っている構造が少なくないということだったので、もう少し法人対策のところについても注意喚起を行っていく、あるいは実態調査を行っていく等の方向性が打ち出されていても良いのではないかなと思った。

後藤座長）

この件はテレワークのための法人の環境にも関係するところなのでホットなトピックだと思う。

赤阪サイバーセキュリティ統括官室参事官（政策担当））

確かにこちら記述が入っておりませんでしたので、追記をさせて頂きたいと思う。取組の実態としては、法人向けの注意喚起が課題だ。例えば ISP に集まって頂いて意見交換を行った上で法人営業を活用して、法人窓口に対して注意喚起をしていくというような注意喚起のベストプラクティスに関する意見交換をおこなったり、SIer に任せている法人も多いと思われるので、ユーザに注意喚起するだけではなくて、SIer も巻き込んで対策を打っていかないと有効な取組には繋がっていかないのではないかということで、我々も SIer に働きかけを行っていくために業界団体にも今、話をしていったりとそういった取組を進めている。そういった取組についても、この記述の中に盛り込むということで検討させていただきたいと思う。テレワークのセキュリティについては、今回コロナ対策ということで補正予算を使って緊急に対策を取り進めているところで、新しくテレワークを導入する中小企業向けにチェックリストの策定等を行うわけだが、それに合わせて実態調査も行うことにしているので、そういったところでどういった使われ方、どういった利用の形態があるかということを十分に把握した上で、その利用の実態に合わせた対策というものも内容を充実させていきたいと思っている。そちらも追記するような形で見直しをさせて頂きたいと思っている。

林構成員）

今回、電気通信事業者のアクティブな対策ということで、随所に色々な新しい提案をされているということを大変嬉しく思う。どんな点かというと、今までネットワークと端末は別々の所管に属するのでそれぞれが努力しなさい、というのが原則だったと思うが、ネットワークを介して通信がなされるのでもう少し通信事業者がアクティブな対策を取るべきじゃないかということ、データ負けしてしまっている、戦いに勝てないというようなこと等、基本的なそういった論点を精査していただいて、通信事業者がもっと頑張れと書いているのは私としては大変嬉しい。問題は、このテーマについては政策課題に関する部分と具体的施策に関する部分でそれぞれについて書いてあるわけだが、内容についてはかなり重複が見られるような気がして、事の重要性に鑑みて重複があっても必要なことは書いていただくというような意味では私もこの方法でいいと思うが、これを世間にドキュメントとして発表した時の訴求力という点ではエグゼクティブサマリーのようなものを付けて頂いて、もう一工夫していただくと分かりやすくなるのではないかと思う。併せてサイバーセキュリティ基本法第 6 条、第 7 条に関係するということを述べているのも今までの検討に比べれば一歩踏み出されたのではないかと思う。米国における 2015 年サイバーセキュリティ情報共有法においてネットワーク及びシステムの管理者はそのシステムがきちんと機能しているかモニタリングしなさい、といった権限と責任を明確化しているわけだが、それになるべく近づけるような努力は今後も必要だと思うので、全体としては非常に前進しているというのを歓迎すると同時に、これを具体化するためにどういうことが望ましいか、もう少し詳細を詰めるところでは、私も何らかのご提案を申し上げたいと思っている。

名和構成員）

私は地方で講演依頼を受け、講演をよく行っているが、総務省の総合対策がかなり引き合いに出されており、読まれている印象がある。その観点でのコメントだが、47 ページのパラグラフ 3 つ目の「また地域においてはセキュリティに関する」という部分だが、主語を地域の民間企業というふうに読み解くとメリットがない。押し付け的に書いているような印象があり、これは地域のセキュリティを推進しているようなところが増えている中で、率直に言うと不快に思う。せっかく地方自治体が企業に寄り添った形で表現や取組を強化している中で、中小企業におけるメリットを書かないということはあまり良くないのではないかと思いコメントさせていただく。この姿勢のようなものが 6 ペー

ジにも表れているようで、6 ページの下の方、最後の 2 行目から「中小企業等におけるテレワークの環境化でのセキュリティ対策を強化していくために」とあるが、この強化していくという主語が簡単に読むと総務省になってしまうため、中小企業にやらせるという押し付け的な表現になってしまっている印象。今、どこの県も自治体も、主語を大事にして「して頂く」や「するように促進する」のような表現で揃えているが、中央省庁からこういった書きぶりになると少し残念な気持ちになる。この表現のところを一言でも良いので変えていただくと、円滑さが出てくると思った。

後藤座長）

この辺りは細かいところかもしれませんが、もう一度事務局の方で全体の再チェックをお願いしたい。

徳田構成員）

トラストサービスに関してですが、今回の COVID-19 の関係で皆さんがサイバー空間上で働き方であったり教育だったり医療でシフトしてきている。実はこのトラストサービスに対する制度や枠組みの早急な改善が必要だと思っていて、この中にタイムスタンプ、e シール、リモート署名の３つの例がある。まず問題なのはタイムスタンプの場合には民間がずっとやっていて NICT も協力しているが、2020 年度中に国による認定制度を整備する。トラステッド・ルートと同じようにルートのところは国が基準などを認定し、その後民間でスケールするようにするという方向性で私は良いと思う。しかし、問題は 3 番目のリモート署名や e シールが 2021 年度となっているので、これは是非 2020 年度中にやらないと国にとっては非常にダメージが大きくなると思う。次に書いてあるようにわざわざ請求書に押印等が必要とされている中小企業等がある中で、今回テレワークまではシフトしたので、ぜひ次のステップまで早くやるということにプライオリティを上げて頂きたい。２つ目は是非皆様の知見をお聞きしたいが、ZOOM などのテレワーク環境で利用されるツールが数千万人規模から数億人規模に拡大し、好むと好まざるに関わらず使われるようになり、そういったテレワークのツールの安全性というのが上手く一般の人達に伝わってないので、その辺を上手く伝えられる仕組みがあると良い。トラストサービスの枠組みとも少し似ているが、どういった仕組みを作っていったら一般の人達が色々使っているテレワークのツールをより安全な形に持っていけるかを考える必要があるのではないかと思う。

中尾構成員）

ICT-ISAC では総務省と共に色々やっているが、テレワークを安全に使っていくためのガイドラインを様々な ISAC（金融 ISAC、交通 ISAC 等）と連携して作っているので、恐らくそういったところも総務省と連携して活用していただけると思う。

藤本構成員）

総合対策案を読みますとやはりセキュリティ上の課題が山積しているということがよく分かる。このような情報を、ICT 利活用を推進する方々や今後使っていく方々に届け、セキュリティへの関心を持っていただかないといけないと思っている。せっかくこのようにまとめられて色々な取組が推進されているので、その情報の中で必要なことを、セキュリティの専門家以外の方々にも届ける何らかの取組というのも始めていった方が良いと思っている。それによって安全性を確保しながら ICT 利活用を推進する人材も育成されていくと思うので、そのようなこともご検討いただければと思っている。

後藤座長）

徳田構成員からの 2021 年度では遅いのではないか、前倒しすべきではないかという意見については総務省から何かコメントはあるか。

赤阪サイバーセキュリティ統括官室参事官（政策担当））

このトラストサービスについては昨年度以来検討してきたところだが、ご指摘の通り今般のコロナ影響でより必要性や社会的な要請も高まっていると思うので、我々としても可能な限り前倒しをして取組を進めていきたいというふうに思っている。特に e シールについては、昨日閣議決定されたが、今回の二次補正予算でこの e シールに関する実証調査を行って、制度化を前倒ししていくというような予算も含まれているところなので、こういったものも活用しながら、民間の仕組みということもあるので、是非民間企業にもご協力いただきながら、できるだけ早く仕組みの構築というものを進めていきたいと思っている。またリモート署名についても今、規制改革の会議等でも論点として取り上げられているところなので、経産省、法務省とも協働の上ということになるが、すみやかに電子署名法との位置づけについて整理していくということで進めたいと思っている。

小山構成員）

今回取り上げられたような内容を活用した C&C サーバ探索の高度化を、どんどん進めていただきたい。それが実際に、事業者や民間でも使えるようにするため、法制度的な手当てが重要だと思う。時間のかかることであるため、そろそろスケジュール化を吟味し、取り組んでいただきたい。

戸川構成員）

全体的な感想・コメントであるが、喫緊の課題含め、非常に網羅的かつポイントを押さえて、資料をまとめていただいている。文書そのものは長いので、可能ならば、冒頭にエグゼクティブサマリーのようなものがあると、読むほうにとって分かりやすいと思う。指摘をさせていただくのであれば、24 ページ、または再掲で 40 ページにある通り、5G セキュリティにおいては、ハード、ソフト、双方に関するセキュリティ・バイ・デザインの概念が非常に重要だと思う。特に、現在開発が進んでいる、あるいは、もう開発が終わって、その次の Beyond5G まで進んでいるが、5G のネットワークコアの部分では、仮想化が進み、ソフトウェア化が進む一方、DSP（信号処理用のプロセッサー）のような、ハードウェアもキーコンポーネントになっていると思う。この 5G のセキュリティ対策として、「脆弱性の検証手法等の確立と体制整備」は大変重要な政策だと思うので、是非継続して進めていただきたい。

吉岡構成員）

テレワークのセキュリティが重要になるであろうというのは皆様もお考えの通りであると思う。少なくともどういう観点があるかということを、少しだけ述べさせていただきたい。ユーザが狙われるというケース、これは、皆様、急に使うようになり、色々と分からないことが多いとか、テレビ会議のファイル共有とか、ちょっとした操作の間違えで、非常に重大なことが起きてしまうが、使うことに慣れていないことで、操作の誤りや、騙されてしまうことが非常に

増えており、実際にそういう攻撃も増えているようだ。2つ目は、ツールやサービスも攻撃の対象になることがある。テレビ会議システムのバックエンドに対して DoS 攻撃を行うということもあり得ると思う。実は最近、DoS 攻撃を観測するシステムを大学で動かしているが、実際、テレビ会議システムのバックエンドへの攻撃は、この COVID-19 の前と比べてかなり増えている。したがって、そういったところも重要になると思う。3つ目は、そういったサービスは便利なものも色々あるが、海外製も非常に多い、むしろほとんどそうだと思う。先ほど徳田先生からのご意見にもあったが、運用の仕方、データの流れ、どこへどう保持されているか、というのが見えにくいので、本当に安全なのか、安全ではない前提ではどう使えばいいのかという辺りが今後重要になってくると思う。

園田構成員）

家庭のセキュリティのレベルと、色々なものが非常に近くなってしまうと言うか、企業という枠組みを外れ、家庭に仕事が戻ってきてしまったので、そういうことを考えるならば、やはり、家庭のセキュリティをどう上げていくかが大事なのかなと思う。

後藤座長）

確かに、私も今、自宅であるので、非常に大事なポイントだと思う。

鵜飼構成員）

NOTICE で色々な取組をやってきていて、今までにない取組ができるようになったのは非常に大きなポイントだと思う。どんどん成果も出てきているが、注意喚起をしても対応してくれないケースが多く出てきているのではないかと思う。今後 IoT、5G がどんどん普及していくと、家庭のルーターだけでなく、検査しないといけない対象が爆発的に増えていくと思う。そうなったときに、注意喚起をしても対応しないケースはもっと想定されるので、ここから更に一歩先に進んだような、攻撃パケットだけをフィルタリングしてしまうといった取組ができないだろうか。また、先ほど小山構成員の話にもあった通信の秘密について、本来、通信の秘密が担保されなければいけない理由はいくつかあると思うが、これに関しては、もっと積極的にやらないといけないと思う。ある意味、通信の秘密をきちんと担保するということでもある。法制度の話もあるので、今後、5 年以内くらいにはかなり大きな問題の一つになると思うので、このことを今後の検討課題の一つに入れるべきではないかと思う。

後藤座長）

鵜飼構成員の言うフィルタリングとは、バックボーン等、キャリアレベルでのフィルタリングという意味か。

鵜飼構成員）

おっしゃる通り、キャリアレベルでのフィルタリングをしていくということである。

小山構成員）

過去、私も、中尾構成員とともに ICT-ISAC 等で、こういった取組・課題に直面して議論をさせていただいた。確かにフィルタリング等で通信を緊急避難的に止めていく必要性を感じたことは、ここ 10 年くらいの間で何度かあった。どう進めるかというのは、技術的な取組と法制度の取組がセットかと思う。鵜飼構成員からも、今、応援コメントを頂けたので、こういった取組を是非推進していただければと考える。

中尾構成員）

鵜飼構成員からもあった NOTICE に関して、総務省より、感染端末の把握、それに対するユーザにアラートをあげて改善していただくなど、取組としては非常に効果が出てきつつあると思う。その中で、ユーザがどのくらい対応してくれるか、あるいは総務省の別の取組で、これはユーザの挙動ではないが、感染後の攻撃挙動を無害化・無効機能化する活動も始められているということで、国内的な IoT のセキュリティ対策は、総合的に意味があるものになってきており、非常に評価できると思う。何度か申し上げているが、IoT 自身の感染している機器は日本だけでなく海外にもたくさんある。海外からの IoT を用いた攻撃は、非常に増加しつつあり、DoS だけでなく、マルウェアへのインジェクションを含めて色々な脅威が想定できる。そのため、せっかく総務省でこういった国内の IoT のセキュリティの活動を良い形でまとめていらっしゃるので、国際連携の活動の一環として、この現状の活動をベストプラクティスとして策定していただき、具体的に海外の主要国にそれを共有し、上手く連携をすることで、海外でも同様な対策を少しでも推進していただけるような国際連携があっても良いのでは思う。それが海外からの攻撃の回避につながるのではないかと思う。今の総合対策の中で、ここまで記載するのが難しいのであれば、今後の進め方の中でちょっと触れていただくということでも良い。

後藤座長）

確かに緊急時のテレワークという環境から、これからは長期的な平常時のテレワークになるので、ますます長期的に海外との連携が重要になるかと思うが、国際連携について総務省から何かコメントはあるか。

近藤サイバーセキュリティ統括官室参事官（国際担当））

NOTICE 等の取組については、総務省としても、海外に展開すべきベストプラクティスと捉えており、昨年度も、日米サイバー対話や日英サイバー対話等数々の二国間協議が行われた中で、NOTICE をはじめとした日本の取組をアピールしている。ご指摘のようにこういったものをさらに海外に発信していくことは重要なので、しっかり対応して参りたい。

吉岡構成員）

NOTICE の通知対象で一般のエンドユーザが少ない件について、長年攻撃を観測している感触から申し上げると、確かに日本は Mirai 等の感染台数は他国に比べて少ないと思う。一方、これだけ Mirai にずっと攻撃され続けていても Telnet が見えている状況は、逆に Mirai に感染しない、侵入されても内部の構成上感染しないという事情のものが残っているという見方もできる。その意味で、攻撃が変わると、エンドユーザ側が弱いということも事実であり、そちらへ

の攻撃も増えるということも考えると、引き続き、エンドユーザへの通知、注意喚起も重要であろうと考える。

岡村構成員）

こちらが観測しているところでは、やはりフィッシングが非常に多い。昔風のサイバー攻撃もさることながら、やはり、テレワーク等では、家庭内で、そういうものが来た場合に開いてしまうケースが多い。できればどこかでその点にも触れていただきたい。

後藤座長）

テレワークに関係して、フィッシング問題がまた増えているのではないか、ということでよろしいか。

岡村構成員）

ずっと多い状態が高止まりで続いている。特に家庭の場合には、専用端末を配布したところで、そういうものがやって来る可能性があるので、注意喚起をいただきたい。

後藤座長）

テレワークというのは企業と家庭が繋がるので、両方に対する注意喚起が必要だというご提案、先ほど若江構成員の議論にあったところと同じかなと思う。

岡村構成員）

特に家庭での端末使用に際してということである。

後藤座長）

今回 COVID-19 問題等で、大きくテレワークが取り上げられ、先ほどのトラストサービスを含めて、一気にデジタル化、いわゆる DX が半分強制的に進められてしまっているが、1 つは、それを良い機会として前向きに捉えようという話に加え、それに伴う、企業と家庭の両面にわたるセキュリティ強化、この両方が重要だというのが今回強調されたポイントかと思う。その関係で、将来、研究開発等に関し、クラウドとの関係も含めて、ゼロトラストアーキテクチャという言葉もあるが、そういう研究開発のところで、先ほどの 5G セキュリティに加えて、何かコメントいただきたい。

中尾構成員）

今、後藤先生がおっしゃたことは非常に重要だと思う。例えば、5G や Beyond5G もバックエンド側に、MEC（Mobile

Edge Computing）も含めて、必ずクラウドが存在する。そこでのクラウドの使い方は、一般的なクラウドユーザとクラウドプロバイダーの構成になっていない場合が多い。ただ、脆弱性はかなり引きずっており、ハイパーバイザーに近いものは当然存在して仮想化の中に作られるので、クラウドなどのバックエンドのユーザに IoT 利用者がいるが、5G とクラウド、利用者の全体を見据えて相互に連携する課題や問題点、またはそのための解決が今後出てくると想定している。

名和構成員）

先ほど NICT から頂いた、クラウドに関する研究開発についてのコメントであるが、ここ数か月間、クラウドのキャパシティを増やす、あるいは機能を増やすために、コンテナをむやみやたらに入れることで、機能上の障害やインシデントが相次いで発生している。昨年、米国 NIST が、「アプリケーションコンテナに関するサイバーセキュリティのガイドライン」を出したが、この内容に、コンテナのイメージに対するセキュリティチェックあるいは脆弱性検査を専用ツールを使ってやりなさい、とある。一方、ガートナーなどの調査報告を眺めると、米国製とかイスラエル製などのコンテナセキュリティ専門会社が並んでいる。NICT 等の公的機関でアプリケーションコンテナのセキュリティの技術開発を進めて頂き、無償で提供いただくなどをすると、今後のクラウドの安全な利活用に資するのではないかと思う。

後藤座長）

ありがとうございます。徳田構成員からもソフトウェアの検証が重要とのコメントを頂いている。ここで時間となったので、質疑・応答・自由討議の時間は以上で、終わりとさせていただきたい。本日の会合でご披露できなかったご意見等は、明日までに事務局にご連絡いただきたい。構成員の皆様の貴重なご意見に感謝する。全体として、非常にポジティブなコメント、更に頑張るべきではないかというコメント双方を頂いた。今後、IoT・5G セキュリティ総合対策 2020 の策定に向け、総務省で意見公募をやっていただけるようであるが、本日のご議論いただいた内容やご意見を踏まえて、意見公募に向けての事務局の修正案を進めていただきたい。本日のご意見を反映させた意見公募用総合対策の修正案については、座長の私に一任いただければと思うがよろしいか。

全員）

全員賛同。

後藤座長）

それでは、本日の議論はここまでとさせていただきたい。この後、高市大臣より閉会にあたってのご挨拶が予定されている。

※以下チャットでのやりとり

若江構成員）

吉岡先生、先ほどの NOTICE の話について、法人が SIer 任せになっている側面がある反面、リーチできるのは法人である。どうしたら注意喚起がうまくいくかアイデアがあったら教えていただきたい。

吉岡構成員）

若江様、エンドユーザへの注意喚起については、おっしゃる通りなかなか効果が上がり辛いことが課題である。過去の CCC（Cyber Clean Center）等の活動では、メールでの通知から封書も用いることでユーザの対応率が上がったという報告があったと思う。また、海外プロバイダ(オランダ)を巻き込んで行った国際共同研究では、一種の検疫環境に感染ユーザを移動し、Web アクセスを注意喚起サイトに誘導することで、かなりユーザ対応率が上がるという結果も出ている。しかし、ここまで強行な対応を国内で出来るかは疑問である。これ以外にも、例えば SNS アプリなど多くのユーザが既に利用しており、馴染みのあるチャネルを利用して注意喚起を行うといったことが出来ると効果があがるのではないかと思うが、実現には技術的にも他の観点でも様々な課題がある。

徳田構成員）

Beyond5G となると、より仮想化が進み、HW/SW の役割のうち、SW の検証の重要性が高まると思う。 もちろん、戸川先生たちの chip level の検証も重要であるが。

篠田構成員）

5G に関しては Fake News とも言えないが、健康問題が取り上げられる。Google 検索でも 53 万件ヒットする。総務省も検査している結果があるはずなので、5G は安全であるから導入することを、もう少し紹介していくのも良いことかと思う。

テレワークは、ゼロトラストネットワークが当たり前、クラウド前提、のセキュリティガイドライン、が出せるとユーザ企業は楽だと思う。

園田構成員）

注意喚起として最も効き目があるのは、使えなくしてしまうこと（止めてしまうこと、サービスダウンすること）ではないか。 SW の脆弱性探索技術とかの研究開発がますます重要になりそうだ。

岡村構成員）

オフィスや集合住宅における無線 LAN の輻輳問題も、可用性等の関係で考慮願いたい。

（4）高市総務大臣御挨拶

（5）閉会