サイバーセキュリティタスクフォース（第 44 回）議事要旨

1. 日 時）令和 5 年 6 月 29 日（木）10：00～12：00

2. 場 所）総務省第 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、篠田構成員、園田構成員、辻構成員、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】

内閣サイバーセキュリティセンター、デジタル庁、経済産業省、地方公共団体情報システム機構

【総務省】

山内サイバーセキュリティ統括官、内藤官房審議官（国際技術、サイバーセキュリティ担当）、小川サイバーセキュリティ統括官室参事官（総括担当）、酒井サイバーセキュリティ統括官室参事官（政策担当）、佐藤サイバーセキュリティ統括官室企画官、田畑サイバーセキュリティ統括官室企画官、廣瀬サイバーセキュリティ統括官室統括補佐、井上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 44－1　e シールに係る取組について
資料 44－2　「ICT サイバーセキュリティ総合対策 2023」（案）
資料 44－3　「ICT サイバーセキュリティ総合対策 2023」（案）の概要
資料 44－4　「情報通信ネットワークにおけるサイバーセキュリティ対策分科会とりまとめ」（案）の概要
参考資料　　サイバーセキュリティタスクフォース第 43 回 議事要旨

5. 議事概要

（1）開会

（2）説明

◆議題（1）「e シールに係る取組について」について、事務局より資料 44－1 を説明。

◆構成員の意見・コメント

後藤座長）

e シールに係る取組について、今後の有識者会議での検討に非常に期待している。組織等の実在性確認については、簡単ではないと思われるが、おそらく将来はメタバース上の組織等、何をもって存在とするのかが議論になると思うので、この辺りも段階的にいろいろ工夫して、有識者に議論していただくという期待でよいか。

酒井参事官）

そういうことになると思う。現状我々が把握しているところでは、特に金融の領域では、金融機関の ID に関してはかなり厳格に制度運用されている。それ以外については、現在、デジタル庁でデジタル ID の総合的な検討

が進められており、法人については法人登記あるいは gBizID のようなものを活用するという議論がされており、こういった検討と連携をして進めていきたいと思っている。ただ、ユースケースによって ID が必要な範囲も大分変わってくると考えられる。今回はインボイスへの期待がいろいろ寄せられているので、例えばそういったものをユースケースとした場合に、どの程度のものが必要になるのかを具体的に検討していきたいと考えている。

岡村構成員）

EU の eIDAS 規則というものがあるが、それとの互換性などについてはどのようにお考えか。

酒井参事官）

我々も eIDAS の動向は常時把握している。将来的には相互に運用できるようになるのが望ましいと考えているが、相互認証のスキームとなると、検討と実装にかなりの時間を要するだろうと考えている。今回は e シールの普及というものをまず優先に考えたいので、全てを議論し尽くすというよりは、当面のビジネスに必要な領域を早めに特定し、世の中に方針を示していくことを優先したい。eIDAS については引き続き検討していくが、年度末までにアウトプットが出せる論点を優先すると、あまり注力はできないのではないかと思っている。

名和構成員）

e シールに係る指針を別途確認させていただいているが、その中では秘密鍵と PIN コードが漏えいする脅威のシナリオがあまり反映されてない気がする。秘密鍵と PIN コードが漏えいし、不正されたことに気づかずに第三者がそれを悪用した場合に、認証局や監視者などがモニタリングして早期に発見する仕組みがあるか。これを窃取した者が意図的になりすまして認証局に執行要求した場合、それを利用している方に一定の損害を与えることができ、実際に諸外国で当たり前のように発生しているため、秘密鍵と PIN コードに係る最近の脅威を反映するような指針にしていただきたい。

酒井参事官）

現状の指針もとりまとめから 2 年ほど経っており、そういった部分の見直しも必要だと思う。御指摘を踏まえて、脅威についても検討してまいりたい。

藤本構成員）

今後の有識者会議における議論について、制度を導入することによって取引の安全性と高める話と、利活用を推進する話の 2 つ混ざっているように感じる。今後どちらに重きを置かれた議論にするのか、どのように整理されるのかなど伺いたい。

酒井参事官）

その点も重要な点だと思う。おそらく制度の要否を検討する前にそういった議論が必要だと思う。新しい技術なので、ニワトリと卵のようなところがあるが、いろいろお話を伺うと、アプリケーションによって、あるいは使い方によっては、発信元の確認をそれほど厳格にする必要がないというケースも多くある。むしろそういったものについては、国の制度の枠外でどんどん普及したらいいのではないかという御指摘も頂いている。そういう意味で e シールのレベル分けを行っていき、国による第三者確認が必要な領域をある程度具体的にお示しできればと思っている。結果的に世の中に普及している e シールの大部分は国による認定制度を要さずに、極めて重要なものだけが国が認定する e シールだということもありうると思うが、今後、いろいろ情報を集めて、この報告書の中で何らかの形で表現していきたいと考えている。

中尾構成員）

今後、検討会で議論をしていただくのは非常に良いことだと思う。先ほど名和構成員が言及されたなりすましなど、ケアしなければいけないことがいくつか出てくると思う。例えば技術基準策定の必要性について、e シールの基本技術はデジタル署名の技術をベースにしていると思うが、デジタル庁等で進めているデジタル署名全体の技術的な要件と e シールの話とのデマケーションや連携はどのような状況か。

酒井参事官）

これから制度化を検討する際には、電子署名法が 1 つ参考にすべきものなのだと思うので、制度の強度や深さといったものは電子署名法を参考にある程度レベル感を合わせていくことになると思う。この検討会にはデジタル庁にオブザーバーで参加いただくことになっている。先ほど申したようにデジタル庁では法人 ID を検討しているチームもあり、また電子インボイスのメッセージフォーマットを検討しているチームもあると聞いているので、この検討会の中でデジタル庁ときちんとコミュニケーションをとりながら進めてまいりたい。

◆議題（2）「「ICT サイバーセキュリティ総合対策 2023」（案）」について、事務局より資料 44－ 2、資料 44－ 3、資料 44－ 4 を説明。

◆構成員の意見・コメント
鵜飼構成員）

NOTICE は非常に重要な取組だと思うので、ぜひ続けていただきたいと思う。現在、様々な取組を行っている中で、こういった攻撃スキャン・大規模スキャン技術は、いわゆる安全保障の面でもすごく重要な技術で、ICT を含めて様々な発展的な要素があると思っている。先刻漏えいしたロシアのサイバー兵器に関する文書、バルカンファイルズというものがあるが、これが本物かどうかは分からないが、ロシアでもいわゆる大規模スキャン技術を活用している。こういった技術重要で、継続して開発を続けることが必要。スキャンの技術はそんなに難しくないといったことを言う人もいるが、私もスキャンをずっと作っていたので分かるが、本当に細かい技術の積み重ねのため、1 回開発をやめてしまうと、また最初からとなるので、どんな方法であるにしろずっと続けていただきたいと思っている。今の仕組みや法制度では、グローバルで Shodan のようにスキャンするというのは難しく、指定された IP アドレスが限定されているが、どんな形であれ、引き続き技術の蓄積を行っていただきたい。

名和構成員）

36 ページにある国際連携の推進について、まず全体的に誰が何をやるか確認させていただきたい。特に「積極的」という言葉について、「電気通信事業者が積極的に○○」と書いている。以前にはないような書きぶりで、相当の努力を電気通信事業者に求めるようなところがよくまとまった一方で、36 ページにある総務省として努力していただくところについては、積極的という言葉が極端に少ない感じがする。また今後の取組については、「連携強化のための関係性構築」とのコピペが並びすぎているような気がする。おそらく今後、流動的な国際連携の中で、機動的にいろいろなイベントをつかんでいくのかと思うが、ここで唯一「積極的」と言っているのが、「国際標準化活動への積極的な関与」で、総務省としては、特に大きく考えているという印象を受けたが、国際標準への日本の貢献が少なく、また、タイトルにも「日本の取組の発信及び各国からの提案への対処」とあり、リーダーシップと読めるところが少ないように感じる。また様々な国際標準会議に出ている方の話では、国からの支援が少ない、情報のインプットが少ないということを以前から聞く。できれば、ここで「積極的な国際標準への関与」に資するような施策のアクションアイテムを少し入れ込んでいただくか、あるいは実行上でそれを反映していただくようにしていただきたい。

中尾構成員）

IoT のボットネット対策という言葉が多く使われている。もちろんボットネットを構成する C&C サーバをディテクトして、それに対するミティゲーションを考えるというのは、ボットネット対策だと思うが、NOTICE に絡むようなエッジ側のデバイスの脆弱性などのアラーティングや、ある程度脆弱性があるのがはっきり分かっている IoT 機器に対して、ISP が行うウォールド・ガーデン等の対処を検討するのは、どちらかというと IoT ボットネット対策ではなく、IoT セキュリティ対策ではないかという気がする。また、SIer という言葉が数多く出ており、私も日本にいると問題なく使っているが、ISO27400 について議論した際、SIer と言っても外国人は誰も分からなかった。システムインテグレーターとするのか、または、ISO27400 の規格においては SIer を IoT のサービス提供者のように考えていたので、SIer という用語を使う際、それがシステムインテグレーターだと外国人の方が分かるようにノートを付けていただいた方がよいと感じた。具体的な IoT に関わる検討は非常に体系的に進めていただいており、NOTICE のステアリングコミッティを作り推進するのは非常にいいと思う。日本の中で総務省が NOTICE・NICTER などの IoT 機器の脆弱性を狙ったものへの対処などを推進しているのは非常にいい。一方で IoT 機器の適合性評価制度のような話は別の省庁で進んでいるが、これを実際にやっているシンガポールは、NOTICE の方にもすごく興味があるようで、IoT セキュリティに関する総務省を中心とした体系的な取組がもっと世の中に伝わった方がいいのではないかと思う。セキュリティ対策としての体系的な表現が響くと非常にアピール力が上がると思う。そして、名和構成員のコメントでもあるが、日・ASEAN について、ASEAN 諸国、例えばシンガポールやタイやマレーシアといった人たちと話すと、どうやら技術的に彼らの方が進んでいる認識を持っている方が非常に多い。実際進んでいるところがあるが、多くの ASEAN 諸国の人は、いろいろな連携をするためのリーダーシップを日本にとって欲しいと言っている。正確に総合対策の 1 文 1 文をチェックさせていただいてはいないので何とも言えないが、その辺りが響くような表現を埋め込んでいただくと、非常にありがたい。

戸川構成員）

全体的には現状分析に基づいて、差分を上手く取り入れた形で適切な対策ができているのではないかと思う。その中で先ほどボットネットという言葉が適切かどうかという話があったが、総合的な IoT ボットネット対策の推進は非常に重要だと思っており、先ほど鵜飼構成員からコメントがあったとおり、NOTICE の延長・拡充は、ぜひ進めていただきたい。NOTICE をいつまで延長できるのかというところが、非常に気になっている。その上で、持続的に研究開発を進めていくことは非常に重要なことだと思う。今回の資料の中で特出している点を進めることは言うまでもないが、昨今の世界情勢や将来的な脅威をにらんだ上で、研究開発に関しては比較的幅広に捉えて、きちんと考慮することを総合対策等で示すことも重要ではないかと思う。もう 1 点、サイバー攻撃への自律的な対処能力の向上について、SecHack365 のような比較的あまり慣れていないような方々やこれから取り組んでいこうといった方々が、こういった催しや取組を通じて、セキュリティに関する能力を向上させていく取組は非常に重要だと思う。正しく脅威を認識して正しく対応することができることが非常に重要だと思うので、これが総合対策の中に記述されている点は、私としては非常に評価できるところなのではないかと思う。

佐藤企画官）

まず鵜飼構成員からコメント頂いた NOTICE に関する NICT 側の観測能力の維持強化という点は、御指摘のとおりで、分科会のとりまとめでは、来年度以降も継続的に取り組むという方針をお示ししている。NOTICE の今後の在り方を検討するに当たっては、現在の NOTICE の課題として、注意喚起のためにどういう観測ができるかが前提になっていた。今回の分科会での検討を踏まえて、まず国内にどういった脅威があるのかをしっかり観測をすることが重要であろうということ、そして、その観測で明らかになった脅威を踏まえどういった対処を行

うかということの、2 つの機能をしっかり切り離して、今後 NOTICE を運営すべきではないかと考えている。国内に脆弱性等のある機器又は感染している機器がどれほどあるかを観測していく能力を維持強化していくことが大変重要だと考えており、NOTICE の今後の大方針の 1 つとして、観測の維持強化を打ち出した。これを踏まえ、継続的に取組が行われるよう、しっかり支援していきたいと思っている。次に、中尾構成員から頂いた IoT ボットネット・IoT セキュリティの用語について、どういった形で記載をさせていただくかを工夫してみたいと思うが、一方で似たような言葉が乱立すると、分かりづらくなるということもあると思うので、ここで示している IoT ボットネットとは何かを脚注で説明を加えるなど検討してみたい。また SIer について、68 ページでは SIer の脚注で定義を書かせているが、こちらも中尾構成員から頂いた御指摘を踏まえて、どういった書き方が適切か改めて検討したい。

小川参事官）

名和構成員、中尾構成員から国際連携の話について御指摘いただき、ありがとうございます。「積極的」という表現については、書いてないから積極的にやらないということではなく、しっかり取り組んでまいりたいと考えており、特に 38 ページにも記載があるとおり、今年 10 月に京都で開催予定の IGF は日本で始めての開催である。IGF でもサイバーセキュリティについて非常に関心が高いので、しっかりとホストとしても参画をしていく。QUAD においては、サイバーセキュリティに関して様々な議論があるので連携をしていく。また、日・ASEAN の関係で中尾構成員からも御指摘いただいたが、日本に対してリーダーシップを発揮してほしいといった期待が当然あるので、50 周年を迎える日・ASEAN について、特に同志国を含めて、連携強化のための関係性構築に取り組むことが重要だと記載させていただいている。ASEAN 各国と諸国の ISP との間も含めて信頼醸成のためのイベントを実施することなど、サイバーセキュリティに関する脅威情報の共有を促進できるような検討を進める旨 39 ページにおいても記載している。さらに、41 ページのとおり、ASEAN 諸国との間からも評判が非常に高い AJCCBC を広げるにあたり、アメリカやオーストラリアなど同志国とも連携して、実際にプログラムを提供していくことに非常に力を入れている。また、御指摘のとおり国際標準化は非常に重要で、5G のセキュリティの関係でも 43 ページにもあるように積極的な対処のための連携強化に向けて継続的に取り組むことが必要であり、標準化活動にはノウハウも必要となるため、引き続き方策を検討して参画していく。貴重な御指摘を踏まえてしっかりと活動していきたい。

酒井参事官）

戸川先生からの研究開発に関する御指摘について、報告書の 27 ページや 28 ページに今後研究開発を進めていくと記載されているが、御指摘を伺って改めて見てみると、27 ページのア「CRYPTREC の取組の推進」の次のイが「その他の取組の推進」となっており、「その他」の中にも NICT の良い取り組みが多く記載されているが、目立ちにくいと改めて感じた。書きぶりについて、検討させていただきたい。

小山構成員）

86 ページの 3 行目の「様々な情報を重ね合わせていくことで」について、様々な情報を重ね合わせていくということは、ボットネットを可視化するという文脈において、例えば参加する ISP を増やすことによって、量的な面で可視化をしっかりと進めていく、解像度を上げていくとともに、ボットネットの通信先が特定のサーバに集中している点を海外等のインテリジェンスと重ね合わせることで特定するなど、情報の質を増やすことによって、ボットネットの可視化の解像度を更に上げていくといった取組を行うことになるのだと思う。一方で、「情報を重ね合わせていくということで」の文言を一般の方が見ると、プライバシーの侵害などが行われるのではないかという懸念も生じると思う。しかし、今回の分析手法は、ISP がユーザー特定を行うことなく、ボットネットの可視化を行う手法だと思うので、プライバシーの十分な配慮が行われていることなどに言及すべきではないかと

感じた。

吉岡構成員）

私も NOTICE やフローデータの分析など、様々な観点での情報の取得と、それを適切なステークホルダーに提供して対策を進めるという構想が必要だと依前から思っていたところ、そのような内容が書かれており、本当に感動した。他の構成員からもあったように、攻撃スキャン技術は応用の幅が非常に広い技術だと思う。現在は、IoT 機器の脆弱性を探すことが主眼かもしれないが、例えば VPN サーバ等の脆弱性を見つければ、それは企業への侵入口を探すという企業のセキュリティ対策にもなり、テレワークセキュリティとも関係する。重要な施設の機器の脆弱性が発見されることもあると思うが、それはインフラのセキュリティにもつながるかもしれない。クラウドの領域をスキャンするとクラウド側でも脆弱性が見つかる場合もあるので、応用の幅はかなり多岐にわたっている。今後、例えばコネクテッドカーやスマートシティ、医療やヘルスケアなど、ネットワークに接続されているものは基本的に全て関係してくると思うので、特定の施策というよりも、多くの施策の横串となる基盤的な技術になり得ると思っている。一方で、注意喚起まで含めたパッケージで行うと、かなり実施者の負担が大きいという御説明もあったと思うが、全てを注意喚起対象とするよりも、まずは観測技術の研究開発を継続し、何が本当に問題になっていて、何が注意喚起を含めたアクションを取らなければならないのかという状況把握をすることが重要だと考えた。また、基本的に NOTICE 等のスキャンはグローバルなインターネットに対する取組であり、組織内や家庭内のローカルネットワークの状況は、当然見えては困るという面もあるが、見えにくいところだと思う。本会議でも確かローカルネットワーク内への IoT 関係の攻撃が進展したという事例の紹介があったように、ランサムウェアや企業のネットワークということを考えると、当然組織内のセキュリティも大事になってくる。今後そういった脅威の拡大がどういう状況になっているのかということを注視し、必要に応じてその辺りについても観測技術の検討を行うとよいと思う。

徳田構成員）

2 点コメントする。1 点目は 81 ページの NOTICE ステアリングコミッティについて、この体制を作っていただいたことが、NOTICE のアクティビティの持続的な発展維持につながると考えており、今は 4 者だが、ステークホルダーを可能な限り取り込めるような柔軟な体制で運営していただけると、他の委員からの御指摘のように様々なあらゆる分野で脆弱性の可視化や把握、分析が進むと思う。こういう形で作っていただいたということを非常に感謝している。2 点目は、26 ページに CYXROSS に関して、今後、長期的には、データドリブンのアプローチとしてサイバー攻撃や防御の技術に様々な AI ツールが使われてくる。いかに自国でどのような攻撃があるかないかということを把握するデータを取得することが非常に大事。「導入府省庁のみでなく、政府全体のサイバーセキュリティを統括する NISC・行政各部の情報システムの監視・分析を担う GSOC 及び・・・」とあるが、何らかの形で輪を広げて、特定のところだけではなくて、全体に情報が行くとよいと思う。サブコメントが 2 つある。1 つはエディトリアルな点だが、目次において 1 章の中で(1)総合的な IoT ボット対策の推進、その後、(3)トラストサービスの普及になっているが、(2)は消えたのか。単にこれはエディトリアルなエラーと理解してよろしいか。2 つ目として、昨日、松本大臣が NICT を訪問されて、サイバーセキュリティの研究所で NICTER や DAEDALUS を見ていただいた。DAEDALUS というのは、非常に古く 2010 年代から使われていて、地方自治体に対してアラートを出す仕組みだが、大臣が、地震対策というのは年何回かキチッと各組織でやられており、非常に大きいクリティカルなインシデントが地方自治体で起きてない、サイバーセキュリティについても DAEDALUS のようなツールがあるので、活用していただければいいとコメントされていた。そして、CYDER とも関係して、国家公務員、国の機関の方については非常に履修率が高くなりほぼカバーされているが、地方公務員の方たちは中々お忙しくて、土壇場でキャンセルされてしまうケースなどがあるので、DAEDALUS と CYDER の演習を一括に地方自治体の方たちにコメント頂けるとよいと思う。

篠田構成員）

まず総合対策のレポートが非常に良くできている。その上で、地域 SECUNITY については、私も東北で御協力させていただいたが、その際、意外に学校の先生の参加が多いと感じた。初学者向けの簡単なウェブハッキングの演習後、学生たちを講師に招いてパネルディスカッションをしたが、学校の先生が言うには、彼らもセキュリティに関しては素人なので、もっと知りたいということで、演習環境を求めて参加したということだった。今後おそらく演習環境や教材など CYDER の仕組みが広く共有されていくと思うが、そういった方がいるので、引き続き演習環境や教材が様々なそういう教員の方々に提供されていくことを期待している。さらに地元の方からは、単発でやるのではなく、シーズナルに、年に 1 回この時期にここでやるというよな継続性が大事だという声があったので、継続的に行っていただくことを期待する。もう 1 点が国際連携の AJCCBC について、今年の 3 月から拡充されるのは良いことだと思う。私が関与している ICC という国際 CTF（Capture The Flag）大会は、EU の ENISA が発起人として作ったもので、第 1 回はギリシャで開催し、今年は第 2 回をアメリカで開催する。70 数ヶ国が世界から参加しており、昨年は ENISA が主催、今年はアメリカの民間団体とアメリカ政府が共同で開催し、来年は UAE 政府が主催する予定。AJCCBC 自体は ASEAN の試みだが、選ばれた子たちがそういう ICC に参加するという仕組みはありえるのだろうかという思いを巡らせた。

辻構成員）

NOTICE を継続的に続けていくことが大事だということは、鵜飼構成員からもコメントがあったが、現在 NOTICE は主に脆弱な IoT 機器で、ある特定のポートに弱い ID・パスワードが使われているものを検出し、それに対処していくという範疇で行われていると思うが、それだけではなく、継続的に続けていくに当たっては、国内にあるサーバ、ネットワーク機器などインターネットにつながっているようなものに関して、機器の特定とバージョンを把握した上で、どういった脅威があるのかを自分事のように感じていただけるよう注意喚起を活用していただきたいと思っている。

若江構成員）

C&C サーバの検知について、早期発見の成果も上がっているとのことなので、今後、利活用が進むと予想される。また、様々な通信に関する情報を収集、分析し、対策のためにステークホルダーで共有するという仕組みはとても重要で、適切な管理・運営のもとで利活用することが期待されていると思う。利活用が今後進んでいくのであれば、その運用に対する説明責任や外部からのチェック体制をどのように構築すれば、セキュリティを強靱にしつつ、他の権利侵害などの支障を最小限に抑えた形で進めることができるのかについて、考えていく時期にも来ているという気がしている。例えば、フロー情報の分析なども、先ほど小山構成員からプライバシーに配慮してやっているとの御発言もあったが、そうであるなら、どのようにプライバシーに配慮して行っていくのかを具体的に外部にも分かりやすいように説明する仕組みが必要になってくるのではないかと思う。加えて内部のコミュニティではなくて、外部の研究者や技術者のような人もチェックできるような情報開示の仕組みを考える時期に来ていると思っており、課題として利活用の点だけではなく、そういう仕組みの構築のようなものを盛り込んではどうか。ステアリングコミッティの中に、そういったステークホルダーを入れることも考えられるが、そういうことも検討していただけるといいと思う。

佐藤企画官）

前段で頂いた構成員からの御意見のうち、中尾構成員の NOTICE の情報発信についての御指摘は非常に重要である。NOTICE の情報発信は国内だけでなく、海外に対してもしっかり発信をしていく必要がある。当然、国際連携も念頭に置きながら取り組んでいくことになると思う。御指摘いただいた点を踏まえてやっていきたい。次に小山構成員から頂いたプライバシーへの配慮について記載すべきではないかという点についても御指摘のと

おりだと思っている。どこに記載するかに関しては、座長とも相談しながら修正をしていきたい。また、吉岡構成員からのローカルのネットワークに関する御指摘について、NOTICE 等をはじめとする観測・調査については、御指摘のとおりグローバル IP アドレスを対象としているので、中は見ていないという状況である。そういった中で、現在のサイバー攻撃の状況を見ながら、我々も今の観測の範囲が適切かどうかも継続して検討していきたい。次に徳田構成員からの御指摘について、1 点目のステアリングコミッティ等の多様なステークホルダーを巻き込んだ取組にしていく点は、我々が目指している方向性と同じである。本文の 82 ページにあるように、今後、メーカーや SI にも NOTICE に参画をいただいて、総合的に対処を行っていきたいと考えている。辻構成員から御指摘のあった脆弱性が発見された際の注意喚起の活用についても御指摘のとおりだと思っている。個別の利用者に注意喚起を行うだけではなく、マクロで見たときにどういった脆弱性があるのかというところも含めて情報発信していくことも大変重要で、NOTICE の今後の取組の一環としてしっかりやっていきたい。若江構成員の外部のチェックや分かりやすい情報開示についての御指摘は、C&C サーバの検知に関してだと思うが、これも小山構成員の御指摘と同様、こういった点に配慮することは、非常に重要なことだと思っている。現在もこれまでの有識者会議のとりまとめに基づいて、C&C サーバに関する情報や通信トラフィック・フロー情報の取扱いを極めて慎重に行いながら、実証を進めている。現在、こういった情報の利活用をどうすべきかを ICT-ISAC を中心に検討いただいている。同時に適切な情報管理も大変重要になってくると考えている。そういった点を含めて検討を継続して進めていきたい。

小川参事官）

徳田構成員から頂いた CYCROSS についての御指摘を頂いた。26 ページのところに記載があるが、一部の導入省庁だけではなくて、政府全体の NISC や GSOC、デジタル庁にも共有して、全部で進むと良いというのは御指摘のとおりで、そういう形になるように進めてまいりたい。加えて、地方自治体の CYDER などの受講の話についても御指摘いただき、地方自治体に受講いただくことが非常に重要で、CYDER の受講促進を行うとともに、DAEDALUS についても地方公共団体に向けて引き続き推奨していく。32 ページに記載のオンラインの入門コースには昨年度 700 人が受講している。集合演習に来るのが難しい方でもオンラインで受講できるものもあるので、これも組み合わせてしっかりと幅広い方に受講いただけるようにしていく。また 33 ページにもあるが、病院など重要インフラ事業者がサイバー攻撃を受けるということもあるので、重要インフラ事業者の方にも CYDER を受講いただくようにしていく。さらに、国家安全保障戦略においてもサイバー安全保障分野での対応能力の向上として、政府内外の人材の育成活用の促進を引き続き図るとされており、CYDER は非常に実績もあるので、サイバー安全保障分野における人材育成にも知見を活用することを視野に入れて、関係省庁とも連携していく。そして、篠田構成員からも御指摘があった地域 SECUNITY についても本当に様々なプログラムを各地域でいろいろな方の知見を頂きながら工夫しており、若年層向けの CTF や演習なども行っているので、引き続きしっかりとやっていくと認識している。また、AJCCBC の関係について、こちらでも CTF を取組の一環としてすでに提供しているところなので、御指摘頂いたような機関との連携というのも、もし可能であればぜひ御相談できればと思う。

酒井参事官）

補足的に私からもコメントさせていただく。NOTICE の取組の透明性を高めていくことは、非常に重要だと思っている。現状は管理の甘いユーザー側の IoT 機器、主にルータということで、なるべく知識の乏しい方も含めて分かっていただけるように、シンプルにあなたの機器が危ないのでこの対策をしてくださいとだけ伝えるという形になっていたが、このやり方では、そもそもなぜそれが分かったのか、国は何を観測していて何を観測していないのか、それはどういうやり方でやっているのかといったことに対しての情報提供が、これまで不十分なところがあったという意識をしている。この辺りはステアリングコミッティの方で、きちんと内容を開示していく。可能であれば、第三者へオープンにしていくといくことをその次の段階として検討していくべきなのだろうと考

えている。またこうやっていくことによって、国への安心感・信頼感が高まれば、新しくスキャンを行っていくということについての理解も高まっていくと思うので、おそらく観測の拡大と世の中への情報開示は、両輪で進めるべきことなのだろうと認識している。SECUNITY で CYDER の取組の拡大、活用をできればよいという点について、CYDER のプロジェクトでは教材の民間利用の拡大を検討しており、CYROP という民間展開の別のシステムを作っている。現にこのシステムを大学の授業等で活用いただいている例も出てきている。SECUNITY において、これと同様の取組が拡大できる余地があるようであれば、ぜひ積極的に検討していきたいと思う。

佐藤企画官）

徳田構成員から御指摘頂いた本文のタイプミスについては、目次において(2)が抜けていたので、修正させていただく。

吉岡構成員）

AI の技術の発展は、サイバーセキュリティにまったく影響がないということはなく、どれくらいの影響があるか悪用と利活用の両面でこれから見定めていく必要があると思っており、ここに書いてあるのはごく一例であるが、ありとあらゆる所で関係してくると思うので、何らかの形で注視、ウォッチしておくべき動向だと考えている。

中尾構成員）

皆さんおっしゃっていたように NOTICE のステアリングコミッティというのが非常に有効ではないかと私も思っている。昨日アメリカからメディカルデバイスインフォメーションシェアリングカウンセルの説明があった。それは医療関係のデバイス、IoT のデバイスも含めて、そこに存在する脆弱性について関係者、彼らはデバイスマニファクチャラーズと呼んでいたけれども、それと迅速にシェアする。それだけでなく、ファーム等の SBOM の情報をいかに管理するかというのが重要であり、かなり強力にそういう仕組みを作っていると言っていた。先ほど酒井参事官からも御説明があったが、現在の NOTICE のステアリングコミッティの構成をもう少し拡大して、例えば機器ベンダーとマニファクチャラーを積極的に参加いただき、ステアリングコミッティ等で確認できた新しい脆弱性を適切なベンダーに共有するような仕組みというのが拡張的にできるとさらに素晴らしいという気がした。

後藤座長）

今中尾構成員が御紹介された IoT の機器メーカーの取組は、今後 1 番強化していきたいところで、それが SBOM の取組などにも関係してくる。私の理解としては、中尾構成員から言及のあったメディカル系のものは、おそらく米国だけではなく、ヨーロッパにおいて、サイバーレジリエンス法案という EU の法律の動きが業界で非常に話題になっているが、そこではメディカル系は別扱いくらいで特に強化するという言い方をしている。そういうところの取組も含めて、日本としてどうしていくかについて、この NOTICE ステアリングコミッティ、又はその先の構想、総合対処センターなどにおいて積極的に考えるものであるだろうと思っている。この総合対策 2023 をまとめ、次のステップに向けてぜひ動いていただきたい。

酒井参事官）

御指摘の点は、すごく重要な点で、今後、取り組むべきところだと考えている。ただ一方で NOTICE の方は、元々のミッションが通信サービスの安全性を確保するために、ユーザーサイドに設置された機器をきちんと対処していきましょうということが出発点になっており、そういう意味では、幅広く IoT 機器メーカー全部というよりは、攻撃に悪用されがちなルータのメーカーの優先順位が高いという認識で今は取り組んでいる。そういったメーカーの方と議論する際には、当然、SBOM といった話や機器認証の話がスコープに入ると思うので、NOTICE

ではネットワークの保護という観点で、認証制度の在り方について検討できれば、ある意味、分野の先行事例にできるのではないかと考えている。医療等他分野での取組については、NOTICE よりも幅広い枠組みで検討を要する課題だと認識している。

後藤座長）
今回のとりまとめ案について、全体としてはもっと遠慮せずに積極的に PR した方がいいのではないかという非常に前向きな御意見が多かったと思う。また、実際の実行に移す段階で、今後こういうことを期待したいという御意見を数多く頂けた。

◆ご挨拶
山内統括官）

昨年の 12 月から本日までの 4 回、また、分科会においては年明けから先日まで 6 回にわたって、非常に熱心な御議論をいただいた。我々は総務省として、当然サイバーセキュリティの中で何を担当するかある程度決まっている一方、AI を含めて環境が変わり、我々を取り巻くサイバーセキュリティリスクは変わってきているということを念頭に様々な取組を行ってきた。外部との連携、それから関係機関との連携も意識をしなくてはいけない。これまで中々見えづらいということも含めて可視化して、それからどう持続性を持っていくか、特に篠田構成員からの御指摘のとおり、どのように地域に向けて継続的に周知啓発を進めていくか、また、こういうことも含めて透明性や客観視をどう持っていくかを常に意識しなくてはいけないということを非常に意識させられた。その意味で NOTICE に関しては御存知のとおり、当初、プロジェクトの最初に若干不幸な出来事があり、どうも抑制的に議論を進めていたところがあったようにも思う。積極的な説明により説明責任を果たしながらステークホルダーの皆さんと連携、役割分担し、我々の持てる資源をしっかり配分をしていきたい。後藤座長と頂いた意見を踏まえた上で、しっかりパブリックコメントをしていきたいというように思っている。どうぞ引き続き御指導・御助言を頂ければと思う。

（3）閉会

以上