サイバーセキュリティタスクフォース（第 43 回）議事要旨

1. 日 時）令和 5 年 4 月 28 日（金）13：00～15：00

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、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、安田構成員、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

【発表者】

株式会社三菱総合研究所デジタル・イノベーション本部サイバーセキュリティ戦略グループ　小川博久主任研究員
NTT コミュニケーションズ株式会社ビジネスソリューション本部ソリューションサービス部第一マネージドソリューション部門第五グループ　大村優担当課長
国立研究開発法人情報通信研究機構サイバーセキュリティ研究所サイバーセキュリティネクサス　井上大介ネクサス長

4. 配付資料

資料 43－１－1　ISP におけるネットワークセキュリティ技術の導入に関する調査（三菱総合研究所）
資料 43－１－2　悪性 Web サイトの検知技術・共有手法の実装可能性検証に係る調査ご報告（NTT コミュニケーションズ）
資料 43－１－3　トラストサービスの普及に関する取組状況
資料 43－２－1　CRYPTREC の最近の取組
資料 43－２－2　サイバーセキュリティ統合知的・人材育成基盤 CYNEX 2022 年度活動状況報告（NICT）
資料 43－３　「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」の検討状況について
資料 43－２　「ICT サイバーセキュリティ総合対策 2023（仮）」の骨子（案）
参考資料　サイバーセキュリティタスクフォース第 42 回 議事要旨

5. 議事概要

（1）開会

（2）説明

◆議題（１）「情報通信ネットワークの安全性・信頼性の確保に関する取組状況と課題について」について、三菱

総合研究所小川氏より資料 43－1－1、NTT コミュニケーションズ大村氏より資料 43－１－２、事務局より資料 43－１－３を説明。

◆構成員の意見・コメント
【資料 43－1－1 について】

吉岡構成員）

各種認証技術等の普及が進んでいないのは、何か我が国独自の事情などがあるか。また、逆に普及が進んでいる国については何か過去に普及させるための施策があったのか把握されていることがあれば教えていただきたい。

三菱総合研究所小川氏）

私が知っている状況として DNSSEC に関してはアメリカやドイツもかなり普及している。これらの国は、ドメインのなりすましを防ぐという観点で政府が主体的に政府機関で管理しているドメインに DNSSEC を導入していたり、一部金融機関に対して強制的に導入要請をしていた背景がある。DMARC についても同様で、国が主体となって導入している、あるいは金融機関などから強い導入要請があるといった状況である。

JPNIC 木村氏）※質疑対応者として発言

RPKI に関しては、国際的にも導入はまちまちな状況で、導入が進んでいる国についてなぜ進んでいるのかは個別の事情によると思うが、国際的な状況の一つとして AWS や Cloudflare や Google といった事業者はバリデーションの導入を進めており、日本においては 2 年前の情報ではあるが公の場でバリデーションを導入している事業者は NTT コミュニケーションズと IIJ にとどまっている。なぜ普及していかないのかについては、認証技術を導入しても設定を誤ると到達性が失われてしまう点に、事業者が敷居を高く感じているところであるので、本事業では実験環境を設けて一連の動作を行い、先ほどの小川さんの説明にあった①導入しても問題が無いか②不正を避けられるか③不具合に対処できるかの 3 つのポイントについて確証を得ていただくようなコースマテリアルをつくって実施した。

後藤座長）

同じ部分について質問です。各種認証技術の導入をためらっている ISP の属性分類の調査もしているのか。今後の普及のための対策を考える上での参考になるような情報は大体得られているという理解でよいか。例えば技術者の多い大企業は良いが、そうでないところはオペレーションが難しいために事業規模によって普及率が違っているといった分析など、次の施策を考える上での参考情報は得られているか。

三菱総合研究所小川氏）

RPKI と DNSSEC、DMARC はそれぞれ技術分野も導入対象組織も違うため、各々で分析行っている状況だが、端的に言うと ISP が顧客に対してサービスを提供しているか否かの観点がある。例えば、DNSSEC についてはマネージド DNS のような丸抱えでサービス提供している事業者において導入するかどうかといった観点もあるので、提供しているサービス内容や事業規模は影響していると思っている。もう少し細かい分析については今年度の実証で確認する。

【資料 43－１－２について】
鵜飼構成員）

フィッシングサイトの件については、大変素晴らしい結果が出ていると思う一方で、Google との結果を比較し

てみると、技術的にまだ全体的に発展途上感のようなものがあるかと思っていて、Google などと比較してアンドをとられているところが思ったよりも少ないのではないのか。この手のフィッシングサイトの検出の取組は従前より官民で色々行ってきているが、この取組結果を踏まえると、対策が被害拡大に追いつきつつあるのか、それとも対策は色々と頑張っているが悪性ウェブサイトのようなものが急速に増加したり、何か攻撃者のアクティビティが拡大したりといった状況で、被害拡大の方が大きくなっているのか、その辺の感触をお聞かせいただきたい。

岡村構成員）

私の意見もフィッシングに関してなのだが、ほとんどが海外から行われており、テイクダウンや摘発などに関してもやはり国際連携をしなければ、なかなか日本国内だけでは収まらない傾向があるためその点注意すべき。

NTT コミュニケーションズ大村氏）

１点目に鵜飼構成員のご質問だが、我々が調査している中でも攻撃キャンペーンないしはターゲットブランドに応じて使い捨ての URL が記載されているメールが大量にばらまかれる事例は観測できているので、そこに対しての対策というのはイタチごっこになると感じている。一方で攻撃調査の中で攻撃者グループの分類を進めることでテイクダウンと絡めて効果的な対策に結びつけられないかを検討しているので、そういった観点で今後事業者連携、国内対策連携を進めていければと思う。２点目に岡村構成員からいただいたご意見について、この調査の中でも国別傾向というのは見ており、圧倒的に海外が多い点も確認しているので、こういった海外サイトのテイクダウンに関しては、先ほどのワーキンググループに参画いただいている専門機関の JPCERT/CC とも連携した上で海外サイトのテイクダウンなども今年度対策施行の観点でトライできればと考えている。

篠田構成員）

JPCERT と一緒に取り組む点について、長期にわたりこのフィッシング対策のテイクダウンのスピードアップについては取り組んでおり、APWG（Anti-Phishing Working Group）というグループでも ICANN のセキュリティ担当者にボードメンバーに加わっていただいているにも関わらず、なかなかコンセンサスが取れず対策の足並みを揃えていくことができないが、こうした日本の独自の活動で具体的な対処結果の数字を示して、日本ではこうした対策を進めていくべき。日本独自のフィルタリングサービスが立ち上がるのかという期待も込めて話しているが、それがあればユーザはそのフィルタリングサービスを使えば、一時的にブロックができて、フェイクドアから守られるというようなことが数字として示して ICANN で話すことができると良い例として世界にも示せるのではないかと思うので、ICANN 等と足並みを揃えて具体的な世界的なガイドラインになっていけば良いと期待している。

NTT コミュニケーションズ大村氏）

先ほどの APWG 含めて国内の優良事例となるべく、関係機関と連携して良い成果が出るように取り組んでいきたい。

【資料 43－1－3 について】
中尾構成員）

資料 43－1－3 の 4 ページ目 e シールの検討の実施については、デジタル庁の「トラストを確保した DX 推進 SWG」で検討して具体的な報告書などが策定されたあと、総務省に戻ってきて e シールに関する調査研究を実施しているのは何か背景があるのか。トラストサービスは資料に挙げている電子署名・タイムスタンプ・e シール・e デリバリーなど色々あると思うが、世界的にみるともう少し幅広の言葉かと思っている。その辺を担保して責

任を持ってトラストサービスを実施するのがデジタル庁かと思っていたので、デマケーションなど、もし整理ができているのであれば伺いたい。

酒井参事官）

デジタル庁とのデマケーションについては、これからも引き続き議論があるところだと思う。現状の私の理解では、もともと総務省では e シールのガイドラインや指針を検討するにあたり電子署名の制度を参考にしており、いわゆる PKI 型で実装していくということを念頭にしていた。その後デジタル庁内での議論の中で、PKI 型以外にも会社の発行証明をする技術が既に事業としていくつか存在していることや、あるいは欧州において eIDAS 規制でよりしっかりした評価基準ができているといった指摘があり、改めて市場動向を踏まえ総務省で調査をすることに至っている。今後デジタル庁がトラストサービス全体をリードするという点については変わりがないと認識しており、総務省の検討結果を踏まえ、追ってデジタル庁にインプットをしてまた然るべく議論が始まる認識でいる。

岡村構成員）

eIDAS 規制は 2016 年 7 月に施行されているが、GDPR と同様に日本と EU の制度の整合性を確保しなければなかなか実効性があるものにしにくいのでその点対応をいただきたい。

◆議題（２）「サイバー攻撃への自律的な対処能力の向上に関する取組状況と課題について」について、事務局より資料 43－２－１、NICT 井上氏より資料 43－2－2 を説明。

◆構成員の意見・コメント
【資料 43－2－1 について】
岡村構成員）

耐量子計算機暗号については、量子暗号技術自体はもとより当然必要であるが、NICT の量子ネットワークホワイトペーパー1.5 版でも指摘されているとおり、かなり鍵が大きくなるので、量子ネットワークや量子鍵配送ネットワークといった多層的なネットワーク化が重要だという意見に私も賛同する。したがって、量子暗号技術とともにそのようなネットワークに対応するための検討作業ということもさらに進めていただきたい。

酒井参事官）

今回説明では量子ネットワークには触れていないが、量子ネットワークは NICT の未来 ICT 研究所がリードして進めている。詳しく説明しなかったが、CRYPTREC は NICT のサイバーセキュリティ研究所が特に耐量子計算機暗号で大きく貢献している。このように耐量子計算機暗号、量子ネットワークそれぞれをリードする 2 つの研究所がともに NICT にある点が大変な強みだと考えているので、これらの連携も含め、この強みを生かして取り組んでまいりたいと考えている。

【資料 43－2－2 について】
名和構成員）

資料 43－2－2 の 4 ページで説明のあった解析者コミュニティ形成について、意見としてはそのコミュニティ形成において多様性を確保していただきたい。性別は当たり前だが、様々なハンディキャップを持っている方や非日本語スピーカー、海外居住者も含まれるだろう。特にハンディキャップを持っている方は身体的ハンディキャップや集団に馴染めない方がかなりいらっしゃるが、その中で非常に長けた解析能力を持っている方もいるため、彼らのチャンスを無くさないようにしていただきたい。また非日本語スピーカーについては、日本人であっても

英語の方が使いやすい場合や、海外で教育を受けた方が長く日本語以外の言語で話している場合もあるため、世界の共通言語である英語でコミュニケーションを取ることも含み入れた方が良いのかと思う。加えて海外居住者あるいはリモートワークを基本としている企業もあるので、そこに所属されている社員の方などが参加する時の格差がないようにしていただきたい。

藤本構成員）

CYNEX の取組は非常に素晴らしいもので、こちらで学習した人材が今後活躍していくのだろうと思うが、質問として、もし CYNEX で学習をして既に社会で活躍されている方がいる場合、どういうところで働いているのかを知りたい。情報セキュリティ人材不足については色々なところから話を聞くため、育成された人材が本当に必要とされている場所で活躍できるようにすることも大事なことかと思うので、今後活躍していただくための仕組みなどについて何か検討があれば教えていただきたい。

戸川構成員）

国産セキュリティ製品に関する実用化支援の取組については非常に強く賛同するのでこうした取組を継続的に進めていただきたい。また 4 つの Co-Nexus があるが、いわゆるテストベッドとして技術者・開発者に対してハードウェアを含めて開発の場を提供すること、それからいわゆるピラミッドの底の方で、人材教育にきちんと取り組むことという両面から、国産の人材教育・研究開発を進めていくことは非常に重要であるため、引き続き取り組んでいただきたい。その上での質問なのだが、説明資料に参画組織数の具体的な数字の記載があるが、こちらの数は予定とおり年々増加しているのかの状況について分かることがあれば教えていただきたい。

NICT 井上氏）

まず名和構成員からの解析者コミュニティ形成における多様性を確保すべきというご意見については、おっしゃるとおりであり、Co-Nexus A の取組は基本的にフルリモートで行えるようになっており物理的なロケーションというのはあまり関係ないような形でできるようになっている。また常時情報共有の環境も整備して、常にチャットツールを使いながら情報交換を行っている。使用言語についても、現在は日本語中心だが、日本語話者ではない方、英語話者の方が入ってこられる場合には当然英語でのコミュニケーションも取っていきたいと思っている。また、ジェンダーについても、Co-Nexus A のアナリストチームは女性が年々増えてきており、解析チームの中で女性と男性の割合が半々ぐらいになっているが、参加企業の方にどんどん女性の参画を進めていただけるような居心地の良い環境をつくっていきたい。次に藤本構成員のご質問だが、この Co-Nexus S の教育コースは今 5 年間の 2 年目がちょうど終わった時点で、昨年から受講期間が半年間のオンラインコースを開始しており、1 期生が 6 名、2 期生が 8 名となっている。参加者の所属については、セキュリティベンダや半分程度は政府官公庁系から参加いただいている。ベンダにはどういったモチベーションを持ってコースに参加したかを聞いており、もともとセキュリティエンジニアだったという人も半分以上いるが、その他にも、セキュリティ営業職で技術がよく分からないまま製品の営業を行っていたため知識を身につけたいという方や、還暦近い方が所属会社でセキュリティビジネスを牽引する担当となったため参加した方もいらっしゃる。この 2 人については半年間のかなりハードなプログラムを修了した。モチベーションは様々だが、それぞれセキュリティの分野で既に活躍をしていると理解している。次に戸川構成員からのご質問で、CYNEX への参画組織数が予定とおりに増加しているかについては予定を上回る数で参画組織数が増えている。この組織数は今後むやみに増やしていくというよりも、参画していただいた組織とさらに関係を深めながら、各分析や教育プログラムを深めていくようなフェーズに入ろうとしているところだが、年々ありがたいことに参画希望組織が増加している。

名和構成員）※チャット欄より抜粋

既存のコミュニティから外れている優秀な方々に、このコミュニティの存在が伝わるように配慮していただければと思う。

後藤座長）

12 ページのタイムラインについて、今後は組織に参画してもらうフェーズからアライアンスによる自走組織化と記載があるが、この大きな違いはどのあたりにあるのか。また、NICT 以外の、IPA や JPCERT など他のセキュリティ関連組織との連携等共同して取り組んでいる点などについて教えていただきたい。

NICT 井上氏）

この CYNEX の事業は国費による 5 年間の事業であるが、今後ある程度の自走化を図るためアライアンス化するにあたって、各組織から参画費用をいただくことを予定しており、事業の中のサービスなどをもっと拡充していくことや外向きの情報発信等をさらに強化をしていく想定をしている。JPCERT や IPA との連携に関しては、実はもう既に CYNEX に入っていただき情報共有の取組などに既に参画していただいている。それ以外にも常日頃から我々の CYNEX の解析チームと JPCERT、IPA は様々なところで情報共有を行っており、ある意味この CYNEX が中核拠点になって、そちらとの関係もさらに太くしていこうという状況である。

◆議題（3）「分科会の検討状況について」について、事務局より資料 43－3、議題（4）「総合対策骨子（案）について」について、事務局より資料 43－4 を説明。

◆構成員の意見・コメント
【資料 43－3 について】
林構成員）

分科会のアウトプットについて、資料 43―3 の 7 ページの課題として、サイバー攻撃に効果的に対処していくためには、脆弱性のある IoT 機器、ボットネット、C&C サーバ等全体を俯瞰した対応が必要で、それら様々な情報を重ね合わせていくことで精度を上げながら全体像を把握していくことが重要というまとめがある。この点大変重要であり、部分を詰めていくことも大事だが、取組全体をどうやってみるかというのはもっと大切である。その対策として今後統合分析対策センター（仮称）を立ち上げる方向性は自然な流れかと思うが、当該ページに記載のある方向性だけではなく、もっと幅広い指摘として、例えば色々な施策についての法的根拠については電気通信事業法における設備規制の部分が基になると思う。だがこの部分はサイバーに特化していない条文であるため、サイバーの観点ではその部分をもう少し一般化した方が良いのではないかといった問題も考えられる。センター立ち上げの根拠だけではなく、もう少し幅広い対応を想定しこれを見ていくという必要がある。また 3 ページ記載のサイバー攻撃に悪用される恐れがある端末の接続拒否については、一般の接続規制にそのまま持ち込むことはできず、サイバーの特性から説明していくことになると思われるが、かなり一般的な規律にならざるを得ないので、その辺のバランスを取る必要があるだろう。そういうような視点から出てきた論点というのを非常に大きな目で見ていくというために役立つのではないかと思った。

若江構成員）

資料 43―3 の 7 ページの林構成員の意見に賛同する。色々な施策を進める上での法的根拠が、今のままの電気通信事業法では十分に見いだせなくなっていくのではないか。センターを立ち上げるだけではなくこれを機に総合的対応をみすえた電気通信事業法の見直しを検討すべきではないか。これまでのように対処の必要性が発生する度にサイバー研などに法的な違法性阻却事由について確認するのでは、時間もかかるし、解釈にも無理が生じる恐れがある。2 点質問だが、1 点目に資料 43－3 の 2 ページ、ID・パスワード以外の脆弱性のある IoT 機器

についても対処を可能とするというのは、具体的にはどういった取組を検討するのか。2点目に5ページの利用者への注意喚起のみに依存せず、柔軟な対処を進めるとあるが、これも具体的にはどういうことが検討されているのか。

徳田構成員）

NOTICEについて林構成員のコメントとも関係するが、NICTの現場では特定の方がきちんとレジスターされた形でNOTICE調査を行っている。この点、NOTICEを実際に動かすための人的リソースも、開始当初は関連企業の方にもNICTに来ていただくといった協力関係があったが、年が経つごとに人員も大変になってきており、ISPの方にとっても業務負担が大きいこともあるため、実際の運営フロー全体を見直す良い機会かと思う。また、先ほどもNOTICEに関し、ネットワーク上に古いIoTデバイスが残っている点が課題であるという説明があったと思うが、一方で今後製造され、ConnectedXという形でネットワークに接続される新しい製品に対するファームウェアのチェックであったり、セキュリティレベリングという視点で今後接続される機器に対しても、もう少しオートマティックにチェックできる環境であったり、レベリングを出すような取組など、民間や国などが今後新しくネットワークに接続されるデバイスについても考えないといけないのではないか。

佐藤企画官）

まずは林構成員と若江構成員からいただいた、取組全体の様々な情報を収集して俯瞰的に対応することが必要であるというご意見については、分科会でも構成員の方々からご指摘をいただいたこともあり、課題として挙げている。その対応の方向性として「統合分析対策センター（仮称）」の立ち上げだけではないのではないかという点についても、どういった対策・対応の方向性があり得るのかについて改めて分科会の方でも検討したい。また、若江構成員からご質問いただいたファームウェアの脆弱性については、メーカー側でファームウェアのアップデートを行い最新バージョンをリリースしても、利用者側でファームウェアがアップデートされずに古いままになっていることにより、それを突いたサイバー攻撃が実際に起きている。この点、NOTICE調査の過程でファームウェアのバージョンが古いかどうかが分かる場合があり、ID・パスワードの脆弱性と同様に対応ができないかという方向で検討している。次に5ページの柔軟な対処については、利用者への注意喚起が基本的な対処になるが、例えばISPによっては機器のレンタルサービスを行っており、その際は利用者への対応を求めなくともISPで一括してファームウェアのアップデートやID・パスワードの変更等の対応ができるケースもある。またメーカーとの連携も選択肢としており、4ページ記載のメーカーへの対応については、NOTICEでID・パスワードに脆弱性がある場合に、機種特定まで行っている関係で、例えばあるメーカーの製品について脆弱性が見つかった場合はメーカーにファームウェアの改修をしてもらったり、新製品発売の際にはそのセキュリティ機能改善のためのコミュニケーションを取ったりなどの対応をしている。また、法人ユーザの場合は機器の設置・管理にSIerが間に入るケースもあり、その場合には利用者ではなくSIerとコミュニケーションを取って対処を促すなどケースバイケースで対応をしていくような、もう少し柔軟な取組を行っていければと考えている。最後に徳田構成員からのコメントについて、まず、運営に係るリソースについては前回の分科会でもご指摘をいただいており、我々としてもNOTICEがしっかり継続できるよう柔軟な運営に配慮しつつ取り組んでいきたい。また古い機器への対応だけではなく、新しい機器への対応も必要というところもまさにご指摘のとおりで、NOTICEで何ができるかというところも含めて検討してまいりたい。

後藤座長）

私は分科会の主査も務めているが、佐藤企画官からの説明のとおりで、特に運営について最後の徳田構成員のお話について、現状のNOTICE運営が人的にISPの方の頑張りに依存している点が課題であるため運営の効率化について議論したい。

中尾構成員）

分科会で議論した内容について、NOTICE を前提とした、現在ネットワーク上で動作している脆弱な IoT 機器を特定していく試みは、世界でもそれほどない非常に特異な試みで面白いと思うし、仕組み全体だけではなく、利用者やメーカー、NOTICE の運営側という様々な視点から整理されたことは非常に良い検討と思う。その中で徳田構成員のご発言にあった、現状使用されている IoT 機器だけではなく、今後出回る IoT 機器に対する検討について、世界的には後者をかなり重要視していると認識している。アメリカやヨーロッパの関係者の話では、機器メーカーが製品を製造する際に、製品のセキュリティレベルを特定できるような基準や仕組みをつくることにより、例えば適切なパスワード管理やアップデート機能といった基準をクリアすることで、一定レベルのセキュアな IoT 機器で一定サービスに耐えられることをある程度保証する流れになっているようだ。この点アメリカやヨーロッパだけでなくシンガポールなども ETSI の EN 303 645 （IoT 機器のセキュリティ規格）という基準をかなり重視している。アメリカなどはメーカーが製造した IoT 機器をテストラボというところで一回動作させそのセキュリティレベルを検証する取組がある。検証するセキュリティレベルがより上の製品にはペネトレーションテストも実施する評価環境があり、NICT の井上さんの発表と繋がり、重要な点であると思う。またアメリカは、一度テストを行った製品でも新しい攻撃手法に対しては脆弱性も出てくるため、先ほどの話にあった統合分析対策センターのようなところで、全体を見据えた評価を行いたいとのことで、現在はその構想を練っていると言っていた。そう考えると、総務省で今進められている取組の全体図を見据えることによって、日本でも全体的で包括的な対策にきちんと乗り出せる気がしており、一部 IoT 機器の適合性評価やラベリングについては経済産業省と連携をすべきではないかと思う。

後藤座長）

中尾構成員からのコメントは非常に大事なポイントである。私も経済産業省の取組について認識しているが、日本全体としては新製品と運用中の製品の両方が全体としてカバーされるような取組が必要だと認識している。

【資料 43－ 4 について】
吉岡構成員）

IoT 機器の対策について先ほどの中尾構成員のご意見にもあったとおり、「ICT サイバーセキュリティ総合対策 2023（仮)」の骨子（案）として II の 1．総合的な IoT ボットネット対策の推進とあるが、最近 IoT 機器の脅威としてボットネットではないものも少しずつ顕在化しており、例えばルーターの VPN 機能を悪用して踏み台化し、他の重要なサイバー攻撃に悪用することも少し顕在化していると思う。したがって、脅威というものがどんどん変性することも踏まえると、AI の利用や悪用も今後サイバーセキュリティに与える影響が凄く大きくなるかと思っている。そういったトピックがかなり急激に出てきて脅威の動向も凄く変わっていくと思うので、統合分析対策センター（仮称）の設置や時間のかかる大規模な取組だけではなく、ある程度柔軟性をもった、先行的に対応できるような研究開発も併せて必要であるように感じた。III の 2．研究開発の推進というところで CRYPTREC の推進等と書かれており、この「等」に様々取組が含まれていると思うのだが、そういった新たな脅威への対抗ができるような取組も含まれると良い。

中尾構成員）

吉岡構成員の話はまさにそのとおりかと思うので、可能であればそういった新たな脅威に関する内容・骨子案を総合対策本文に反映する際にもう少し項目立てた方が分かりやすくなるかという気がした。その文脈でいくと、II 情報通信ネットワークの安全性・信頼性の確保の 2 に 5G セキュリティや SBOM 等と書かれており、これはサプライチェーンリスク対策に関して括弧書きしてある内容だが、SBOM についてはサプライチェーンを構成

している組織が持っているソフトウェア用の資産に対する全体的な管理を行う非常に分かりやすい内容だが、単体としても重要な項目であると思われる 5G セキュリティをサプライチェーンリスク対策の中に含めてしまって良いのかという気がしている。総務省の 1 つの大きな軸になる項目かと思うため、5G だけではなく、活発な議論が始まっている Beyond 5G の辺りは骨子案の中で見える化をすると良い。

徳田構成員）

1 点目に中尾構成員が話をされたところに関し II の 2．その他の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の推進について、総務省は Beyond 5G の研究開発に多く投資しているおり、5G や Beyond 5G や 6G に向けてのセキュリティ対策もかなり重点的なポイントのため書き方を工夫すべきではないか。もう 1 点は IV の国際連携の推進について、NICT で進めている CYNEX にも関わるが、様々な自然言語処理ができる AI ツールが多く利用可能となってきているため、国際連携の部分で国内のインテリジェンス情報だけではなく、もう少し積極的に有志国間でインテリジェンス情報であったりマルウェアの情報であったり、人手を介さずに様々なデータ連携を蓄積・収集・解析できるようなインフラを今から準備するのが良いかと思う。ちなみに NICT ではこの間、米国の MITRE（The MITRE Corporation）と MOU（覚書）を結んでいるが、あちらのセキュリティ担当者は 1500 人おり、NICT 全員で 1300 人なので、NICT 全員よりも多くの人数がセキュリティ担当である。MITRE のセキュリティ担当部署にはガバメントとプライベートセクターとのコラボレーションを専門に扱っている部署があるなど、非常に豊富なデータをもっているので、DFFT のような、そういったデータが人手を介さずに行き来できるようなインフラ整備を始めておいた方が良いのではないか。

後藤座長）

今回の骨子案 I.サイバーセキュリティを巡る最近の動向として新たな国家安全保障戦略の策定等と記載がある。広い意味でのナショナルセキュリティの観点から今回の ICT サイバーセキュリティ総合対策 2023（仮）がまとめられると考え、II.は情報通信ネットワークというインフラの安全性・信頼性確保の観点、III はサイバー攻撃対処の自律性・自給自足の観点で広く捉えると、全ての内容を書き下すことはできないと思うので、I の部分で全体の方向性を示した上で、例えば CYNEX などに今回は注力して項目立てしているというスタンスが見える形が良い。その中で先ほど吉岡構成員、中尾構成員、徳田構成員から意見のあった II の 5G セキュリティの観点や III の AI やセキュリティの関係などの観点も適宜触れるのはどうか。それから IV 国際連携については、G7 だけではなく、QUAD、インド太平洋地域が非常に注目されており、その観点についても全体のイントロが I の部分で書かれると良い。

（3）閉会

以上