参考資料 1

# サイバーセキュリティタスクフォース（第 35 回）議事要旨

1. 日 時）令和 4 年 1 月 14 日（金）10：00～12：00

2. 場 所）オンライン

3. 出席者）

【構成員】

後藤座長、鵜飼構成員、宇佐美構成員、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

【オブザーバー】

扇慎太郎（内閣サイバーセキュリティセンター）、鈴木雅也（デジタル庁）、石巻克基（経済産業省）、石川家継（地方公共団体情報システム機構）

【総務省】

巻口サイバーセキュリティ統括官、山内大臣官房審議官（国際技術、サイバーセキュリティ担当）、湯本サイバーセキュリティ・情報化審議官、梅村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）、安藤サイバーセキュリティ統括官室企画官、佐々木サイバーセキュリティ統括官室統括補佐、廣瀬サイバーセキュリティ統括官室参事官補佐、須藤住民制度課デジタル基盤推進室課長補佐（代理出席）

4. 配付資料

資料 35-1　総務省におけるこれまでの取組及び最近のサイバーセキュリティの動向
資料 35-2　令和 3 年度補正予算及び令和 4 年度予算案における総務省サイバーセキュリティ関係事項
資料 35-3　今後検討いただきたい論点（案）
参考資料 1　総務省におけるこれまでの取組
参考資料 2　サイバーセキュリティタスクフォース第 34 回 議事要旨

5. 議事概要

（1）開会

（2）説明

◆議題（1）「総務省におけるこれまでの取組及び最近のサイバーセキュリティの動向」について、事務局より資料 35-1 を説明。議題（2）「令和 3 年度補正予算及び令和 4 年度予算案における総務省サイバーセキュリティ関係事項について」について、事務局より資料 35-2 を説明。議題（3）「今後検討いただきたい論点（案）」について、事務局より資料 35-3 を説明。

◆資料 35-3 についての構成員及び事務局からの意見・コメント

※なお、掲載の便宜上、関連のある項目ごとに意見・コメントを並べ替えている。

**【１】情報通信ネットワークの安全性・信頼性の確保**

岡村構成員）

「今後検討いただきたい論点（案)」の方向性については賛成だが、議論の前提として、資料 35-1 の 22 ページで取り上げられているクラウドサービスの障害は、ユーザ側の設定ミスというよりは、仕様変更に関するユーザ側と事業者側とのコミュニケーション不整合に起因しているもの。本件から得られた教訓として、情報通信全体に関して、仕様変更の際にはコミュニケーションをきちんと取ることによって、そうした不整合を解消していく必要があるのではないか。
また、同じく資料 35-1 の 23 ページでは海外動向が記載されているが、中国の個人情報保護法の課題というのは、越境移転等に本人同意が必要である点も重要だが、主要機器は政府指定のものを使わなければならない点について、日本側に影響は及ばないのかということが大きな課題になってくることを指摘しておきたい。

吉岡構成員）

３ページ中の NOTICE や、明らかに脆弱性があるメーカー保証期間を終えた機器や中古機器を使用しない、使用を中止させる方法といった話題との関連で、IoT 機器等のセキュリティ強化につなげるための、エンドユーザや組織に対するリーチャビリティの向上についてコメントさせていただきたい。これまで様々な形でエンドユーザ等への情報発信や注意喚起がされてきており、テレワークの普及を踏まえれば、その重要性はさらに高くなっていると思うが、簡単な課題ではないと認識している。
前回のタスクフォースで、ウェブサービスのような形で、自身の機器の脆弱性やサービス提供の終了、感染のリスクを確認できるサービスの実証実験を行っている旨を紹介させていただいたが、それとは別に、WarpDrive という NICT からの委託研究も行っている。こちらではセキュリティアプリのようなものを開発し、エンドユーザにパソコンやスマートフォンへインストールしてもらって色々な情報発信や注意喚起をそのアプリ経由で行う仕組みを試行した。NICTER の観測結果なども活用することで、感染している部分をエンドユーザ自身で調べられるようになっており、世界的に技術的な先進性があり、実効性も高いと思っている。また、横浜国立大学の方で同じような仕組みを学内全体に適用してみたところ、脆弱な機器がかなり見つかった。適切に情報提供すると、対策率等の効果も非常に高いことも分かってきている。個人だけでなく組織に対しても、どのように情報提供のリーチャビリティを高め、今までの様々な施策を有効活用していくかという点が重要だと考える。

後藤座長）

ご指摘の点は、「【１】情報通信ネットワークの安全性・信頼性の確保」だけではなく、「【２】研究開発」や「【５】普及啓発」の辺りにも絡む横軸の話だと理解した。

小山構成員）

昨年 11 月に（「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会　第四次とりまとめ」で）通信の秘密の考え方を整理いただいたことにより、DDoS 攻撃の命令を出す C&C サーバの IP アドレス等の調査ができるようになったことに感謝している。一方で、昨年 10 月頃から、監視カメラを主な踏み台とする DDoS 攻撃が 2016 年の Mirai に相当する規模で盛んに行われているが、攻撃の主なターゲットは海外であり、

海外では大きな被害が出ていると伝え聞くものの、日本としては通信に影響がない。この中で、自分たちのサービスを守る視点で正当業務行為として C&C サーバの通信をブロックすることができるのか、また、多数ある C&C サーバの IP アドレスを全部ブロックしてよいのか、それとも可能な限り短期間で切り替えてブロックするのか等について悩みながら、ネットワークを見ている状況である。
また、製造元の海外メーカーが解散しているので、パッチの提供がほぼ期待できず、注意喚起すらできない状況である。3 ページに記載の保証期間を終えた機器や中古機器だけでなく、既にインターネットに多数ぶら下がっているもののメンテナンスできない機器が、社会で問題を起こしている。攻撃先が海外 ISP であったとしても、お互い依存関係にあるわけなので、1 つのインターネットをどう守るかという観点から、どのようなアクションを打つとこの状況が打開できるかを検討いただきたい。(「【7】情報の開示・共有等」では) ICT-ISAC の役割についても問題提起していただいているが、ICT-ISAC においてもこのような一歩踏み込んだ議論ができるようになったというところもご報告させていただく。

辻構成員)

NOTICE について、NOTICE ウェブサイトで月次のスキャン結果が出るようになってから毎月見ているが、試行パスワードも少し前に増やして、さらに広い範囲で脆弱性が存在する IoT 機器を検出し減らしていく活動をされており、着実に成果も出されていると思う。とはいえ、SSH や telnet というような管理ポートをスキャンして 3 年目になるので、そろそろ飽和するのではないか。SSH や telnet も開いておらず、http、https のみで管理ポートが開いている機器が攻撃者の隠れみのになって悪用され続ける問題が根深く残っているため、http、https への拡大は急務としてご検討いただきたい。また、侵入型のランサムウェア攻撃などでは、昨今のテレワーク普及により持ち出された古い VPN 機器の脆弱性を突かれるケースの問題も根深く、NOTICE の取組でバナー情報ないしはバージョン情報といったものを取得しているのであれば、そういった機器の注意喚起に範囲を拡大するというようなことも今後検討されてはよいのではないかと思った。
それから、3 年間粛々と続けていることは素晴らしいが、世の中に忘れられかけている部分もあるのではないかと思い、取組自体は良いのでもったいないと感じる。昨年の夏頃に政府広報ラジオで効果的な活動をされたかと思うが、そうした取組を、「バズる」と言ったら語弊があるかもしれないが、世間に話題にしてもらうことを検討してはどうか。自分がインターネットを使い続けることで世界的に色々なところに迷惑をかけるが、自分は不利益を被らないというところが IoT の脆弱性対策が進まない 1 つの理由と思われるため、例えば「サザエさん」のような国民的アニメとコラボするなどして、他人に迷惑をかけていることにもう少しアプローチする観点で広報活動をしてみると良いのではないかと思う。
また、(資料 35-1 の 19 ページでは) フィッシングメールの届出件数が非常に増えているとのことだが、ここ 2 年間についての自分の調べでは、届出件数は本当に爆発的に増えており、例えば昨年 11 月の 48,461 件から 12 月は 63,159 件に増加している。しかし、これはフィッシングサイトの URL 数にすると 11 月も 12 月も 7,500 件と 7,400 件であり、届出件数だけを挙げるだけではミスリードになってしまうかもしれない。メディアは大きな数字を取り上げがちかもしれないが、本質的な数字の指し示し方も検討した方がよいのではないか。

岡村構成員)

辻構成員御指摘のとおり、フィッシングメールの届出件数というのは、特定の方が膨大な数を届け出ることもあり、件数の増加だけではミスリードになることも事実である。他方で、近年、フィッシングの対象がどんどん移り変わり、これまで経験がなかったようなカード会社等が盛んに狙われていることや、ボットを使ったバルクメールという形で同じ URL から多数のメールが出されるようなこともあるので、その点を指摘したい。

辻構成員）

届出件数の増加だけを示すと、フィッシングサイトの URL 数ではさほど変わっていないという指摘を受ける可能性もあると思うので、いま岡村構成員がお話しされたような現状が伝わる情報発信があった方が良いのではないかと感じた。自分の問題意識は、①適切に知り、正しく怖がる注意喚起と②届出を受ける側の作業効率の 2 つであり、 ①については、過剰に伝わり過ぎるのも考えものであり、メディアが適切に報じるとよいと思うし、②については、報告が増えれば増えるほど今までのオペレーションに無理がでるかもしれないと心配している。

名和構成員）

重要インフラのサイバーセキュリティに係る行動計画を踏まえ、総務省として取組を見直すべき点に関連して、重要インフラの分野の中には行政サービスがあり、また総務省の所管事務には地方自治も含まれるが、今回の資料全般を見ても、地方自治、あるいは行政サービスに関する取組に関する記述がないように感じるが、それについては何か理由があるのかをご教示いただきたい。
また、海外における政策やサイバー攻撃の動向から留意すべきことに関連して、今やサイバー攻撃はいわゆるコンピュータシステム等のネットワークに対する脆弱性を突いた行為だけではなく、人間の脳の脆弱性を突いた行為にも及んでいるところ、NATO が概念として示している Cognitive Warfare（認知戦）のように、計画的に人間に対して特定の情報を浴びせて認知を変化させることで、民主主義国家における考え方を二極化させる影響工作に対する検討や状況認識を進めていく必要がある。

梅村サイバーセキュリティ統括官室参事官）
地方公共団体のセキュリティ確保は、主に自治行政局が担っており、今回の会合にも同局がオブザーバーとして参加している。本タスクフォースの開催目的は情報通信分野におけるサイバーセキュリティ確保の取組の検討であるが、関連するところについては同局とも連携しながら進めていければと考えている。

後藤座長）

IoT 機器に関しては、この 1 ～ 2 週間で、最近は H2 という SQL データベースの OSS にリモートコード実行の脆弱性が見つかったということで北米では大騒ぎになっているようであり、米国ではつい先日もホワイトハウスで OSS のセキュリティに関する議論があった。こうした大規模・広範囲に広がる IoT 機器の不具合につながる OSS の問題等は総務省だけの取組ではなく、IoT 社会の安全性という意味では非常に大きな課題だと認識しており、「【 1 】情報通信ネットワークの安全性・信頼性の確保」で取り上げても良いと思う。

篠田構成員）

「重要インフラのサイバーセキュリティに係る行動計画」について、訓練をやって大丈夫でしたという報告だけではなく、効果のレビューや実際の被害の減少につながる辛辣な意見があって然るべきだと思う。

中尾構成員）

情報通信ネットワークの安全性・信頼性の確保について、世の中の環境、技術的な背景、法令の変化等に関して継続的な検討が必要というのは当然のことであり強く賛同するが、非常に広い表現になっているため、次回以降

具体的な議論を行う前に整理をした方がより分かりやすく、議論が活性化するのではないか。例えば、サイバー攻撃のイベントや挙動の観測・分析・共有と、対策とかソリューションの導出は、国内産業を活性化するという意味で連動して考えなくてはいけないものの、あくまで別軸で考えるべきかと思う。加えて、リスクマネジメントや、総務省が検討会をやっている事業者のガバナンスの強化ということは一つの軸として重要になるかと思っている。また、国内・国際の基準やガイドラインの整備というところにも関係すると思うが、ISO では総務省の IoT 推進コンソーシアムの成果を反映した IoT セキュリティプライバシーガイドラインが出来上がってきている。これらを具体的に「【１】情報通信ネットワークの安全性・信頼性の確保」の議論の際に整理をしていただき、それに加えて人材育成、啓蒙活動や国際連携を議論することが必要になってくるのかと思う。

**【２】研究開発**

戸川構成員）

経済安全保障の文脈においてサイバーセキュリティは非常に重要なものと認識しているところ、研究開発においても経済安全保障が重要なキーワードの１つではないか。総務省の政策に直接関わるところとしては、Beyond 5G、6G による情報通信ネットワークがあるが、これに接続される多様な IoT 機器だけでなく、Beyond 5G、6G の情報通信ネットワーク機器あるいは IoT 機器そのものも多様なハードウェア・ソフトウェアから構成されている。特に最近は、FPGA と呼ばれるハードウェアでありながらソフトウェア的な書き込みができる集積回路や、RISC-V と呼ばれるオープンソースのプロセッサにより、専門業者でない方々でも簡単に IoT 機器を構成するハードウェア、ソフトウェアを設計できる状況でおり、これらのセキュリティをどう担保していくかが経済安全保障において非常に重要な点だと思う。こういった文脈も継続して意識しながら進めていくべきではないか。

篠田構成員）

資料は良くできているが、技術的な対策に寄っていることが気になる。他国において、多額の予算をかけても情報漏えいや攻撃が起きているのは、人間が最たる脆弱性となっているからであり、例えば教育・指導をしても行動変容を起こさない等の指摘もある。そこから、他国では人間の脆弱性に対して効果的な研究が始まっており、日本でも人間の脆弱性も加味したより包括的なアプローチを検討してはどうか。

**【３】人材育成**

林構成員）

昨年９月に策定された「サイバーセキュリティ戦略」には経済安全保障に関する記述が非常に多く、また、これまでより緻密になっている印象を受けた。資料 35-1 中 17 ページの図は、それも踏まえて作成したものと推測するが、総務省の主たるターゲットは一番下の「情報の安全確保」あるいは情報ネットワークの安全性・信頼性の確保であることは間違いないと思う。
また、これまで他の構成員がコメントされた技術的な問題解決策は、翻ってみると安全保障に直接、間接に影響を与えるものだと理解しているが、セキュリティのカバーする範囲は広いので、主として安全保障をやっている方は安全保障の観点からこれを見ているし、主として技術をやっている方は技術の説明の方からなされるというのが一般的である。両者をかみ合わせると、もう少し知恵が出てくるのではと強く感じる。例えば、法律を改正した、通信の秘密の解釈を整理した、あるいは技術標準を変えたとかいうことを安全保障の方面の人たちにも分かるような形で説明していく必要があるのではないか。特に最近、戦略マネジメント層の育成等も議論になっていると思うが、こういう方々には両面の知識と経験が必要とされているところであり、総務省が率先して実行すると良いのではないか。

藤本構成員）

総務省としてどのターゲットを重視して人材育成の取組を行うべきかという点で、どの層も非常に重要だが、「誰も取り残さない」という方針が出ている中、戦略マネジメント層・経営層が特に重要ではないか。教育プログラムの提供は、これらの層の方々にサイバーセキュリティへの関心を持っていただく一つのきっかけにはなるかと思うが、引き続き関心を持っていただくためには、これらの層の方々がアップデートされた情報を入手できることが非常に重要になる。教育プログラムの作成時には最新の脅威情報や政策的な取組情報を入れるが、引き続き最新の情報を入手してもらうためには、こういった会議などに参加するとよい、といった情報提供をしてはどうか。加えて、これらの層の方々に NOTICE のような取組をまず知っていただいて、その上で会社が所有する IoT 機器を確認するような動きにつながれば効果も高いと思うので、経営層の方々に最新の情報を提供する活動もご検討いただきたい。

園田構成員）

CYNEX とも関わる話かもしれないが、後藤座長ともご一緒させていただいている、地域で人材育成エコシステムの仕組みをどうやって作っていくかという点について、タスクフォースでも議論を重ねてきたが、なかなかうまく仕組みが続いていない。こういった仕組みを続かせていくにはどうしたら良いか、人材がどんどん拡大再生産される仕組みにしていくにはどうしたら良いかといった論点も加えていただけると良い。

徳田構成員）

賛成する。人材育成のフェーズ論とも言うべきところかもしれない。

後藤座長）

人材育成のフェーズ論については、自らも当事者であり、次回以降議論できればと思う。

**【４】「統合知的・人材育成基盤（CYNEX）」の構築**

鵜飼構成員）

CYNEX について、産学官のしっかりした結節点を作っていただけるととても良いと思うが、産学官はお互いの理解や向いている方向性が違うところもあり、ぼんやりしている状態で進んでしまうと、よく分からないまま月日が経って終わってしまうということにもなりがちである。記載されているシステム基盤構築や運営環境整備のように、実際に何をやるかということだけではなく、その前提として、CYNEX で実現していく内容のすり合わせ、ゴールの共有などをしっかり時間を取って議論ができる場がほしい。

徳田構成員）

NICT では、SecHack365 や、CYDER やサイバーコロッセオという形で国家公務員や地方公務員等を対象として様々なレベルのセキュリティ人材の育成を実施している。
SecHack365 については、やっと年間 50 名程度、5 年間で 250 名程度ではあるが、IPA の未踏事業と同じように、引き続き、若い方を中心にベストオブベストを作るべく精力的に継続していくことが非常に大事ではないかと思っている。特にセキュリティの専門家ではなかった参加者たちが修了後に起業したり、色々な分野で活躍することで、幅広く社会の中にアドバンスドな知識を持った方たちがイノベーターやクリエイターとして入ってい

くので、将来に向けての早期投資という意味では、他の研究開発にかけている国費に比べても、コストパフォーマンスが良いと理解している。
CYNEX は、新しく NICT の中に作る統合知的・人材育成基盤で、サイバーセキュリティ研究所を中心に立ち上げ作業を進めている。情報共有の例として、NICT は多言語音声翻訳のために総務省と一緒に翻訳バンクという仕組みを作っているが、例えば製薬会社の方に和文英文の翻訳ペアを 100 万文提供していただくと、そのデータを元に多言語音声翻訳のエンジンがドメインに特化されて、”study”を「勉強する」ではなく「治験する」とするようなより精度の高い翻訳結果が出てくるといったウィンウィンの関係ができている。製薬会社が厚生労働省に治験を出すための英文資料の翻訳で、例えばアストラゼネカ社が 4 週間かけていたのが、このドメインに特化した精度の高い翻訳により 2 週間で済んでしまう。
セキュリティの情報は、今のところあまりこれと同じようにスムーズに共有できておらず、大学の方も産業界の方もイライラしている部分があるが、できるだけそのイライラを解消し、共有のデータ基盤で、共通にお話しし、協創できる場を作っていきたいと思っているので、是非ご要望があれば言っていただければと思っている。

**【5】普及啓発**

篠田構成員）

防御策の普及啓発については多くの施策があるが、起きてしまった後どうするのかという点の普及啓発についてはどうなのか。例えばフィッシングサイトの報告も日本では警察に電話しなければならず、（メール報告の）フォームも分かりづらい。窓口も各県警にぶら下がっていたりして分かりづらいので、その辺りももう少し自動化できないかと思う。報告の質・量が上がれば、セーフブラウジングへのインプットも考慮できるのではないか。

岡村構成員）

フィッシング対策にあたっては、セーフブラウジングだけでなく、国際的な CERT 間の連携によるフィッシングサイトのテイクダウンを進めることも重要である。

篠田構成員）

フィッシング対策の国際団体である APWG（Anti-Phishing Working Group）と仕事をしており、国際 CERT 間の連携によるテイクダウンについてはずっと努力しているものの、時間がかかるために、より早く効果的なブラウザによるブロッキングにシフトしようとしている。現状ブロッキングの反映はブラウザ企業のクライテリアに依存しているため、攻撃データベースを集めてブラウザ企業にプッシュしているが、これを仕組み化できないかということで ICANN その他にロビイングのようなことをしている。日本政府としてデータベース等が集まっているのであれば、それをブラウザ企業に提供してプッシュするのも一案だと思う。

宇佐美構成員）

弊社もテレワークの中で自宅の機器のセキュリティを非常に気にしており、IP アドレスを調べて入力し、脆弱性を調べましょうといった取組を展開しているが、IP アドレスを調べてもらう時点で大変な困難を感じており、ほぼやってくれる人はいないと思いながらやるような感じになってしまった。また、フィッシングメール訓練のようなこともやっており、そこで引っかかった人を集めて昨日講習会を開催したが、こうやれば通常のメールとフィッシングメールを区別できるということがはっきりと言えないので、一般的に気をつけましょうといった精神論で終わってしまうところが非常に難しいと痛感した。技術的あるいは概念的にできることと、現場に落とせて

実用化できることは若干違うと思うので、実用化できる対策や教育を考えられたらよい。

名和構成員）

他省庁や民間の取組との連携について、普及啓発の現場で支援する立場として、中央省庁でまとめられた知識体系が、省庁を分断してバラバラに出ている状況があると認識している。これを 1 つの知識体系にして、双方向のプラットフォームとしてポータルサイト化し、現場の近くで普及啓発するところへ提供したり、あるいは双方向の助言等を行えるようにすると良いのではないか。最善策の例としては、米国の HSIN（Homeland Security Information Network）や英国の CiSP（Cyber Security Information Sharing Partnership）等があるかと思う。これと同じものではなく、ライトウェイトでいいと思うが、現在総務省が運営している「国民のための情報セキュリティサイト」は一方通行で、国民からの声をリアルタイムに拾っていないような印象であるので、改善を検討できると良い。

**【6】国際連携**

鵜飼構成員）

ビジネスの海外展開は、ある程度市場がありそうな北米やヨーロッパでも相当大変であり、市場がこれからのアジアだと本当に大変で、正直なかなか実にならない。そのような状況でもやらないといつまでたっても前進しないので、政府として進めていくのは非常に重要だと思う。ただ、経済安全保障という話題が非常に大きくなり、環境が変わってきていると思うので、国際連携については、経済安全保障という観点で戦略を練り直し、そこで特に地域や領域を絞っていくというのが良いと思う。経済安全保障を議論する場が、政府の中にも色々できているので、そういったところときちんとすり合わせをして議論していくことが重要である。

篠田構成員）

日本で実施している 1 週間のセキュリティキャンプでの教育を国際版にして、アジア 8 ヶ国と協力して実施する GCC（Global Cybersecurity Camp）や、ENISA の依頼で行っている ICC（International Cybersecurity Challenge）という CTF（Capture The Flag）を実施した経験から申し上げると、ENISA では参加者の選定など運営側の自由に組織運営をさせているのに対し、総務省が関わっている ASEAN 地域では、各国政府が戦略的にピックアップした人材が参加しているので、地域のコミュニティと分断されている。国によってはハッカーコミュニティと政府がつながっておらず敵対関係にあったりする部分も見て取れるが、ヨーロッパでは CCC(Cybersecurity Certification Conference)のリーダーが議員になったり、米国でもジェフ・モスがハッカーコミュニティからホワイトハウスのアドバイザーになるなどしており、政界とセキュリティ分野の架け橋となるような人材をコミュニティからつないでいくというのは大事だと思うところ、日本がリーダーシップを取って各国で多様な人材の募集等を支援できたら良いと思う。

**【7】情報の開示・共有等**

中尾構成員）

情報共有についての話が出てきたが、観測・分析した情報を適正な形で共有する重要性は皆さんご認識のとおり。これまで ICT-ISAC も含めて色々な議論をしているが、米国 AIS(Automated Indicator Sharing)から飛んでくるデータを活用できる人材を育成するというのは当然必要であるものの、どのように活用するかという視点をあま

り持たずに情報を共有しても、せっかくの共有の意味がなくなってしまう。タスクフォースにおける議論の中でも、各種の取組を通じて色々な共有すべき情報が出てくると思うが、具体的な活用についてピュアなエキスパートだけではなく一般の人々にもリーチできる、例えば藤本構成員がおっしゃったように経営層にもリーチできるような情報形態で活用を誘発するというのが非常に重要かと思うため、論点に加えていただければと思う。

後藤座長）

専門家向け、経営層向け、高齢者向け等受け取り側の立場で考えることは非常に大事だと思う。

（3）閉会

以上