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

1. 日 時：令和 2 年 4 月 16 日（木）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、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、吉岡構成員、若江構成員

【オブザーバー】

尾崎洸（経済産業省）、鮫島清豪（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）

【発表者】

井上大介（NICT）、衛藤将史（NICT）

【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）、安達地域情報政策室課長補佐（代理出席）

4. 配布資料

資料 23-1　セキュリティ情報の自給に向けたサイバーセキュリティ知的基盤構想
資料 23-2　人材育成オープンプラットフォームの研究開発と活用コミュニティの慫慂
資料 23-3　無線 LAN 及びテレワークにおけるセキュリティ対策の強化について
資料 23-4　取りまとめの方向性について
参考資料 1　サイバーセキュリティタスクフォース（第 22 回）議事要旨

5. 議事概要

（1）開会

（2）議事

◆議事２（１）情報集約・分析基盤の構築について、NICT 井上氏より、「資料 23-1　セキュリティ情報の自給に向けたサイバーセキュリティ知的基盤構想」、議事２（２）人材育成基盤の構築について、NICT 衛藤氏より、「資料 23-2 人材育成オープンプラットフォームの研究開発と活用コミュニティの慫慂」をそれぞれ説明。

◆構成員の意見・コメント

小山構成員）

一点目は、基盤構築を進める際に、データ提供や蓄積について通信事業者への期待があれば教えていただきたい。私も長く Telecom-ISAC や ICT-ISAC 等の通信業界のセキュリティ対策を進めていくということに取り組んできているが、なかなか通信事業者自体が自分でデータを使うことや提供するということについては難しい面がある。研究の視点からでも結構なのでコメントをいただきたい。二点目は、こういった基盤を使ってどのようなセキュリティサービスが企業に提供できるのか具体的なイメージがあると進みやすいと思うので、少しかみ砕いた事例などを教えていただきたい。

NICT 井上氏）

一点目の通信事業者様への期待ということだが、これまでも NICT は ICT-ISAC 様と情報共有を様々な形でさせて頂いており、通信事業者の中での様々なデータの出し方の難しさは体感している。その中で無理に情報を出して下さいとお願いしても継続しない部分も多いと思う。通信事業者様への期待としては今 ICT-ISAC の中で NICT も部分的に関わっている情報共有の仕組みがいくつかありますが、その活動をそのまま継続させていただいて、例えば DoS 攻撃の情報の迅速なシェアリング、あるいは ICT-ISAC の方でされている日本国内に対するスキャンの情報の共有、そのあたりの情報をこれまで通り共有をさせていただければ十分と考えている。
二点目のご質問の企業へのサービスの具体的な事例だが、こちらは有償サービスにするか無償サービスにするか様々なオプションがあり得ると思うが、一つはやはり国産の IoC (Indicator of Compromise)、きちんと出所が分かる explainable な IoC というのを作って、それを順次提供して、例えば生の C&C サーバの情報もしくは C&C サーバ情報にブラックリストから外すべきといった付加価値を付け加えたような新しい国産 IoC 情報の提供、あるいは STARDUST を活用した標的型攻撃の情報、これはかなり具体的な標的型攻撃の情報が取れるが、その標的型攻撃に使われているツールやプロセスといった生の情報を迅速に共有できれば良いと考えている。
もう一つのサービスはセキュリティ製品の運用、検証ということで、今 NICT の中で、海外製品のみでセキュリティアプライアンスを約 20 種類くらい揃え、テストベット的なものを構築しているので、その中にさらに新しく作られた国産プロトタイプ的な製品を入れていただき、NICT の CSIRT による長期運用ということをさせていただければと思う。そういった 20 種類くらいのアプライアンスが並んでいる環境は世界的にも珍しい環境なので、一気にアプライアンス製品を触れる環境が出来上がっており、それを使って on-the-job で高度な人材育成サービスというのも企業向けには提供できるのではないかと考えている。

小山構成員）

IoC を提供する考え方として、例えば企業が実際に通信に使っている IP アドレスの情報を NICT に提供すると、その IP アドレスがもう既に乗っ取られて通信に使われている、汚染されている等の情報も逆に引き出せるのではないかと考えている。企業の立場からすると IoC をもらってこれでブロックしなさいと言われるよりも、もう既にあなたの IP アドレスは使われているとダイレクトの情報をもらったほうがアクションに繋がりやすいかなと思うが、そういったサービスはいかがだろうか。

NICT 井上氏）

企業の方から今使っている IP アドレスの情報を提供いただければ我々の NICTER や DoS 攻撃の観測データもあるの

で、その中で実際に使われている IP アドレスのマッチングをかけ、ここは危険ですというのは結構簡単にお返しできると思うので、そのような情報の流れができるのであれば十分に考えられるサービスである。

小山構成員）

セキュリティベンダー１社では太刀打ちできない大規模なネットワーク情報を持っているということで、そのようなサービスが民間ビジネスへの圧迫といったネガティブな意見が出るかもしれないが、是非ともそのようなところに進んでいただきたい。

名和構成員）

産業領域において営利が追求できる仕組みがないと尻すぼみになってしまう恐れがあると思っている。私自身、今現在、複数の国でディレクターとして経営を行っているが、きちんとしたデータを自分なりに、あるいは官・学から頂いて回している状況である。その仕組みは地域によって違うが、NICT の観点から、産業領域に営利を追求できる仕組みの構築のアイディアとして、どのような施策が考えられるか伺いたい。

鵜飼構成員）

データ不足という点は同意するが、他方で、高度技術の研究開発をしていく上で常に困るのは正常系のデータである。例えば、正常系のデータを実際に使えるものとして作るとなると過検知の抑制や競合を防止するための開発がエンジンの開発よりもかなり大きいところがあり、正常系データや正常系テスト環境も大きく足らない状況にある。今現在は海外のセキュリティベンダーからそういったデータを獲得している状況があるので、正常系のデータに関しても国内で作ることについて協調できればと思うが、何か取り組みについて考えられている所があればお聞かせいただきたい。

戸川構成員）

産官学の連携という話で、NICT の皆様方から見て大学にどのような役割を期待しているのか伺いたい。学会等でセキュリティに関するセッションは活発化しており、同時に大学内においてもセキュリティに関して興味を持っている学生が多いという印象であり、それを活用しない手はないと思う。その上で、改めて大学と NICT、産業界も含めてどのような連携が可能なのか、どのような連携の仕方をイメージしているのかお聞かせいただきたい。

吉岡構成員）

なかなか大学が産学官連携で役割を果たせていないと思う。海外ではかなりの先生が産業界と連携し、私の周りでお付き合いのある先生もほとんどご自身の企業を持っている方がとても多い。そこで事業として自分でもデータをとりつつ、研究にもフィードバックするというような流れができているので、大学としても大学に閉じこもっているのではなく、出来るだけ外に出ていく必要があるだろうと思う。その中で我々は NICT 等との密な連携を前提とした研究をいくつもさせて頂いているので、他大学も含めてそのような連携が広がれば良いと考えている。また、私がなかなかリソースを割けていないということもり、大学の中にある CSIRT との連携ができていないが、意外に大学の中にもデータがあるため、大学の中でももう少しオペレーション部隊と研究部隊で連携し、両方が Win-Win となる関係のモデルケースのようなものができると良いとも考えている。

NICT 井上氏）

事業継続のための仕組みを考えた方が良いのではというご質問はまさにその通りだと思う。その一方で、なかなかデータ共有あるいはデータをシェアして分析しようという取組にお金を払って参加してくださいということは難しいと思うので、最初のスタートとしてはやはり国の資金でこのような知的基盤を立ち上げ、その中からクオリティの高い情報を出せるようにして情報の提供サービスをつくる、あるいはこの基盤の中で人材育成の仕組みを構築する中で、今日のナショナルトレーニングの話にもなるが、そのトレーニングの部分を上手く商用化していくことはあり得る。あるいはセキュリティの機器を持ち込んで色々検証するところでも上手く仕組みが回り始めれば、それを商用サービス化する営利化の仕組みを順次考えていかないといけない。ひとまずは国の資産を活用し、体制を回す仕組みをつくるところからやりたいと考えている。
正常系のデータの重要性の指摘はその通りで、NICT で作成しているセキュリティのテストベットは NICT のネットワーク自身をデータとして使っており、ほとんどが正常系データであるため、正常系のデータを使えるような仕組みを作りたい。データ自身を外に出せるかというところは検討が必要かと思うが、正常系データの重要性を改めて認識したため、その点も検討を進めたいと考えている。
産学官連携の中でも学への期待は非常に大きく、NICT でも様々な大学との連携を進めており、一つは分析等を一緒に実施できる方々に是非参加して頂きたいと考えている。今、NICT の中ではリサーチアシスタントという仕組みを作って、学生の方々に一般のアルバイトとは違って、我々の研究の中に入って一緒にデータ解析したり、観測をする機会を設けている。興味がある学生さんにはこの仕組みに参加して頂き、on-the-job で給料を受け取りながら力をつけ、セキュリティ業界の中で長く働いて頂ける仕組みとなっている。
もう一つが、大学にも非常に大量なデータがあるので、各大学が持っているデータで観測網をつくり、そこで得られた情報を更に集約するという観測網的な役割も大学の方に大きく期待しており、そのように大学から出てきた新しい技術が国内でも使われるような環境を作っていくために、今回提案させていただいた構想を活用していただきたい。

若江構成員）※チャットによるコメント

SINET (Science Information NETwork)のデータは連係して活用できないのか。

NICT 井上氏）※チャットによるコメント

NII-SOCS (NII Security Operation Collaboration Services)で SINET データを集めているが、データの利用に関してはかなり厳しい制約が課されているそうで、現状で外部機関がそれを利用することは不可能とのことである。

小山構成員）

衛藤氏の発表内容に賛同した上で、それを実現するためには前段階としてお膳立てが必要と考えている。つまり IT 構築や運用を外注している多くの企業には IT 業務自体が無く、セキュリティ人材育成を進めるためには、まずそのような企業における IT 系業務の内製化を進めなければセキュリティ人材も育成できない。今後クラウドデフォルトでデジタルトランスフォーメーション等を進めるためにはまず IT の内製化が必要で、その延長線上でセキュリティ対策を行っていく必要があり、どこの会社にもある経理部や財務部などの専門職を参考とし、社内に専門組織を持ちつつ、各職場にも経理担当者等を配置するような形が理想であり、このようにセキュリティの種を蒔いていくことで遠回りだが人材育成が始まると思う。

藤本構成員）

衛藤氏提案の人材育成プラットフォームに強く賛同する。その中で戦略マネジメント層人材育成には、マネジメントや基礎的な技術、法制度等、多岐にわたる知識が必要とされるのでコンテンツの開発がとても大変だと思う。そのようなものを共同で開発、展開することによって加速できればとても良いと思う。どのように推進するかについて、NICTの役割としてすでにお考えの具体的な活動などがあれば、ご紹介いただきたい。

園田構成員）※上記質問に関するチャットによるコメント

戦略マネジメント層人材育成に関するコンテンツとしては、棲み分け等も考慮した最初の取組として、第一に、既存のシナリオを活かしつつ CYDER やサイバーコロッセオのシナリオを生かした戦略マネジメント層向けコンテンツを開発する。第二にサイバー攻撃を経営リスクとして扱う演習の開発構築等を考えている。

齋藤構成員）

人材育成について、パソコン黎明期の 80 年代前半に企業に就職した方は現在退職期を迎え、企業のセキュリティ部門に再就職されているような方も結構いる。講師人材の拡大という意味で言えば、こうした経験豊富な方々を積極的に登用することも考えてはどうかと思う。

NICT 衛藤氏）

【資料 23-2】2 ページ目で IT 構築における課題を取り上げており、民間の教育事業者のところで IT を支える環境構築開発者層のセキュリティ知識の不足を指摘しているが、ご指摘の通り内製化不足の背景がこういった課題に繋がっていると改めて理解した。IT 構築運用部門を内製化していくことは社会的に非常に必要なことであり、そういった声も最近多く聞くようになっているため、その流れをうまく作っていければと考えている。しかしながら、NICT が旗振り役として先導することも限界があるため、報告では「コミュニティの慫慂」とさせていただいたが、色々な事業者やユーザー組織の方々と議論をしながら、どのような社会的な体制づくりが必要なのかということを議論させていただきたい、そのような場として既存のコミュニティに NICT が参画していくという議論も含め、推進していければと考えている。大変参考となるご意見に感謝する。
続いて戦略マネジメント層の人材育成に関して、必要となるスキルや知識が多岐に渡り、法制度も必要ということで非常に難しい領域ではあるが、幸いにして戦略マネジメント層人材の育成という観点では既に NISC の方で戦略マネジメント人材に必要なスキルセットというものが定義されている。また、IPA 等においても戦略マネジメント層人材向けのセキュリティ育成コンテンツが作られ、そのようなプログラムが既に動いている状況にある。そのような中で NICT が果たす役割として求められているのが、特に地方自治体における戦略マネジメント層人材の育成というところである。我々は CYDER という、地方自治体の方々を一番多く含む年間 3000 人の方々に CSIRT の要員育成をやっているが、特に町村というような小規模自治体の方々のお話を聞くと、CSIRT の要員も足りていないが、その上位層にいる戦略マネジメント人材についても教育や育成を考える以前に決定的に不足しているという声が上がっている。そのため、既存の戦略マネジメント人材向けの教育などを実施している NISC や IPA 等の組織ともうまく連携しながら、地方自治体向けの戦略マネジメント人材を育成するコンテンツをつくっていきたい。
現在セキュリティ業界では「プラス人材」という言葉があるが、これは、既に業界の様々な分野で技術者として活動している方々にセキュリティの知識や技術をプラスアルファとして持っていただき、それぞれのキャリアを生かしなが

らセキュリティに携わって頂くという概念である。我々自身で推進していく人材育成事業においても、また、コミュニティの中で民間大学等の教育機関を含めて進めていく中でも、既にある程度のキャリアを持った方々にセキュリティの教育をしていくという方向性が社会的にも効率的だと思うため、今後のコミュニティの議論の中でそういった点についても挙げていきたいと思う。

吉岡構成員）※チャットによるコメント

演習のタイプにもよると思うが、演習時に演習実施者が演習環境において、どのような操作を行ったかというログは、収集・蓄積されているのか。そのデータ自体が研究の題材となり得ると思ったため、教えていただきたい。もしログがあるとすると、そのデータを研究に利用する際に障害はあるのか。（演習実施者の許諾などの観点で）

NICT 衛藤氏）

既に 3000 人の CYDER の受講者の方々の受講時のマウスの動きやキー入力等を記録・収集し、サイバーセキュリティの対応能力に優れているかどうかの評価ができるような取組を行っている。このログデータに関しては、プライバシー情報にもあたるので取扱いが難しいが、制度を作り、データの活用という面でコミュニティの活動の中で考えていければと思っている。

篠田構成員）※チャットによるコメント

ご経験の深い、鵜飼さん、小山さんの意見に同意する。そして、（セキュリティ情報）自給率の高い国は、政府が顧客ということが多くある。ベンチャー企業もそれで育つ。自給率を高めるため、セキュリティ教育を盛んに行い、就職先がなく、一部が Black に流れるというのは聞く。セキュリティ教育は育成内容次第だが、彼らが学んだ後の出口を心配している。

NICT 井上氏）※篠田構成員の上記コメントに関するチャットによるコメント

国産セキュリティ製品の最大のユーザーは国であるべきだと思う。そういう意味で、官は非常に重要なステークホルダーだと考えている。

徳田構成員）

NICT は従来 JGN (Japan Gigabit Network)あるいは JGN-X 等ネットワークレイヤのテストベットを提供して役に立てていただいたというイメージはあるかと思うが、次の次期中長期に向けてはセキュリティや AI 等の様々なデータレイヤに関して、NICT という中立機関だからこそ取れるものも、セキュリティ、プライバシーに配慮した形で積極的にオープンにしていきたいと思っているので、このようなデータドリブンでの新しいサービスやビジネスセグメントにつながるようなビジネスコーディネーターといった方々にもご協力いただきたい。
また、NICT では学部生も含める形でリサーチアシスタント制度を再構築して頂いた。通常であれば博士課程の方たちが来られていたが、それではとても追い付かないので優秀な学部生の方もリサーチアシスタントとして受け入れているので、是非大学の方たちともタイトな連携ができればと思っている。
最後に、NICT がどのような形で持続可能なトレーニングプログラムをオファーしていくかというと、一つは研究部隊がいるので非常に先端的な、また最新のスクリプト等が利用できるので、持続可能な形のトレーニングコンテンツ、

または教材コンテンツを外部のステークホルダーの方たちと連携しながら作っていく。個々の演習は民間の方がやられるが、その中にあるコアの部分のアップデートについては、マザーマシーンとして NICT のナショナルトレーニングセンターが役割を持って協業していくことができればと思っている。

◆議事２（３）無線 LAN 及びテレワークにおけるセキュリティ対策の強化について、事務局より、「資料 23－３　無線 LAN 及びテレワークにおけるセキュリティ対策の強化について」を説明（省略）

◆構成員の意見・コメント

齋藤構成員）
個人的な感想になってしまうかもしれないが、ユーザーの意識調査を見ると意識は高いのではと感じている。やはり設置側が重要で、安全に提供するという点を重視していかなければいけないと思う。もちろんユーザーのリテラシーを上げていくことも重要だが、設置側が安全に提供することを考えなければいけない。加えて、チェックリストの件だが、放送設備のセキュリティ対策でもチェックリストを設けており、省令も改正されている中で、改訂も含めた新たな取組を考えている。構成としては単純に項目を並べるだけではなく、これは必ずやる必要があるもの、できる限りやっていくものと、ある程度ランク付けしたほうが良いのではと思う。

赤阪サイバーセキュリティ統括官室参事官（政策担当））

Wi-Fi については、設置側でしっかり対策していただくというのはご指摘の通りだと思う。提供側のガイドライン・手引きの見直しについて、先ほど説明した通り、関係省庁等のご協力を頂きながら、必要なところには配布し、周知していきたいと考えている。テレワークのチェックリストについては、ご指摘の通り一律にリスト化するのではなくて、必須のもの、推奨のものといったレベル感の分け方、あるいは、機器、ネットワーク環境や使い方に応じてどういった対策が必要か、企業の立場に応じて提示していきたいと考えている。

名和構成員）

このガイドラインはすばらしいと思うが、受け身の姿勢が多すぎる印象がある。例えば、ドローンと同じように、悪意のある Wi－Fi アクセスポイントを設置させないような取り組みは総務省にあるのか。

赤阪サイバーセキュリティ統括官室参事官（政策担当））

具体的にそこまで突っ込んだ検討はまだできていないが、今回、このガイドラインを作るにあたり、Wi-Biz（無線 LAN ビジネス推進連絡会）という事業者の団体と色々ご相談し、事業者としても紛らわしいものへの対策をどうしていくかお考えいただいている。技術的なものや制度的なもの等、すぐには難しいかもしれないが、何らかの対応ができないかということについて、事業者サイドとも連絡を取り、考えていきたいと思っている。

吉岡構成員）

偽アクセスポイントが懸念され始めているという話があったが、実際に把握する仕組みや試みがあれば教えていただきたい。

赤阪サイバーセキュリティ統括官室参事官（政策担当））

定量的に把握できていない状況なので、このことについて調査できるかどうかについては、検討させていただきたい。

吉岡構成員）

研究要素があるのかという意味でもお聞きした。勉強になった。

◆議事６（４）取りまとめの方向性について、事務局より、「資料 23－４　取りまとめの方向性について」を説明（省略）

◆構成員の意見・コメント

中尾構成員）※チャットによるコメント

５G セキュリティの推進は積極的に推進すべき点、全く同意する。ただ、記載の「脆弱性」に関しては脆弱性の検証だけでは意味がないと考える。それは、セキュリティに関連する場合、脆弱性が発見されても、それが攻撃やセキュリティ事象につながらない場合は、単なる脆弱性で問題にならないためであり、脆弱性に関連しないセキュリティ脅威も多く存在するためである。従って、脆弱性に加え、それに関連する脅威の分析の視点をきちんと組み入れる必要があり、それらの脅威に加え、５G システムや利用者に対するインパクト分析を実施することが重要となる。それらの総合的な検討を踏まえた上で、有効なセキュリティ対策、対策施行のための優先度分析などが実施できるものと考える。P6 については、適切なご修正をいただければ幸いである。

園田構成員）※チャットによるコメント

今実際に脆弱性の評価をシステムで行う仕組みや、脆弱性を発見する仕組みも研究開発の端緒にあるので、世界に遅れずにその流れをフォローして脅威分析や評価というところに繋げていく必要があると思う。

林構成員）

Active Network Security という新しい概念を設けて、そこで色々な方向性を探っていこうという案に賛成する。ただ、今のインターネットは昔の通信ネットワークとは違って自律システムの相互接続で成り立っているので、システムセキュリティという面も色濃く残している。日頃からやっておられると思うが、経産省との連携をさらに強化していただき、Autonomous System（AS）をいかにしてセキュリティとして担保するのかという視点で議論いただければありがたい。
問題提起をした責任もあるので、通信の秘密とサイバーセキュリティ対策の関係について、今の自律システム管理責任という観点から新しい提案ができないかということで論文を準備中である。もう 1 件若干宣伝めくが、サイバーセキュリティ関係法令 Q&A ハンドブックという、A5 版で 300 ページに及ぶ意ドキュメントを作ったので紹介させていただきたい。法律は大体事例より遅れてくるもので、時に法務部に相談をすると、面倒くさいことになり、かえって損をしてしまったという噂も聞かないわけではない。ただ、セキュリティと法律をやっている方はかなり開明的になっ

てきており、そのことをまとめた資料があると今日議論になった人材育成の教材などでも有効だと思い、岡村構成員から提案があったものを NISC で取り上げ、岡村構成員が副主査、私が主査をさせていただいたので、何らかの形でご参照いただければ幸いである。

小山構成員）

Active Network Security の定義にもよるが、資料 12 ページを見ると、「C&C サーバの検知について AI などを活用して高度化を図る」と書かれている。AI を使うかどうかは別にしても、こういった取り組みは、アメリカなどではインターネットのフロー情報を分析して、C&C サーバを調査する取り組みが以前から行われている。皆様もご存じの通り、FBI 等海外の法執行機関と連携して C&C サーバのテイクダウンが行われたこともあるが、ネットワーク上での対策で言うと、残念ながら日本は海外との協調対処ができていない。資料にもあるが、インターネットは世界中で 1 つなので、やはり、海外の動向を調査し、日本が国際連携するための課題を明らかにした上で、一つ一つ解決していく取組を行うこと、解決できていない課題は何なのかということを関係者で共有していただきたい。林構成員もおっしゃった通信の秘密に関しては、私も以前から取り組んできているが道半ばの状態が続いている。インターネットの安定運用のための議論をし、しっかりと世論を作っていくことも重要だと考える。

若江構成員）

12 ページの構成員からの意見についてだが、1 番上の「サイバーセキュリティと通信の秘密の違法性阻却の考え方について議論が必要だ」は全くその通りだと思い、議論を進めるべきだと考える。他方で、1 番下の「サービスが進展して振り返ってみたときに、通信の秘密に抵触していて、ビジネスに影響が出るということがあってはならないと思うので、そのようなところを見越した対策を進めていくべき」という過去の構成員の意見については、この表現のままだと、常に通信の秘密よりビジネスのほうが重要であるという読み方ができてしまい、「通信の秘密とセキュリティ」という重要な問題にかこつけて、通信の秘密にかかわる情報のビジネス利用にまで拡大して議論しようとしているのではないかと受け止められかねないと思う。過去の会合で構成員からこのような意見が出ているのは事実であるが、もしこのような記載を残すのであれば、それに対する、反論もあったということも入れていただけないか。

小山構成員）※チャットによるコメント

P12 の構成員の意見「サービスが進展して・・・通信の秘密に抵触して・・・見越した対策を進めるべき」は、私（小山）が発言したものと自覚している。ご指摘の通りこの文脈では誤解を与えると思うので発言の背景等の補足説明が必要だと思うが、説明するとかなり長くなってしまう。

中尾構成員）※チャットによるコメント

Active Network Security は誤解を呼ぶ可能性がある。一般的には IDS・FW を動的に高度化する技術を指しているように見えるが、今回はネットワーク側での対策に重点を置いているので、これは IoT だけに閉じた話ではなく、ネットワーク上での観測、分析と連動するべき話となり、そのための法的整備が必要となるという理解である。しかし、ネットワーク事業者だけで全てできるか難しい可能性もあり、IoT－GW などに仕掛ける分析エンジンとの連携などが必要になる可能性もあると考える。従って、「電気通信事業者によるアクティブディフェンス技術」といった名称の方が良いと考える。

中尾構成員）

現在、総務省/経済産業省主導の「クラウドサービスの安全性評価に関する検討会」において、政府調達系のクラウド評価基準化、認定化などの議論を進めているが、本日の議論は、上記の検討会だけでは不十分で、テレワークなどの視点から、追加的に施策や検討を実施すべきということを指しているのか。推進されている検討会とのデマケを十分に行う必要があると思う。

戸川構成員）

先程の徳田構成員や井上室長の回答にあった NICT のリサーチアシスタントも、このようなところに携わることのできる非常に良い取り組みだと思う。大学側ではどうしても計算機環境や演習システムが不足しているところがあるので、ぜひ連携させていただきたく思う。実際にこのようなプラットフォームを促進するための何か起爆剤のようなものがあると良い。大学側としても、こちらにいらっしゃる吉岡構成員や私なら徳田構成員などに何とかお願いすることも可能かとは思うが、通常の大学の方々においては、いかにしてその仕組みを活用するのかが必ずしも明確ではなく、迷っているのではないか。セキュリティ系は現在、学生の関心が高いと思うので、うまくそれを活用できる起爆剤のような仕組みがあると良い。その点で「④ 共創的研究開発/人材育成基盤の構築」は非常に良い取り組みであり、一層こういった仕組みを促進していただければと思う。

名和構成員）

６ページ目で脆弱性に関する事項がいくつも出ており、「検証手法の確立検証」「体制の構築」「情報共有の促進」で大丈夫になるという記載だが、諸外国と比べると、果たして本当かと思う。意図的に残しているもので脆弱性のあるものが出てくるという認識をされていると思うが、検証体制の構築で見つかるというところが少し甘いと思う。

名和構成員)※チャットによるコメント

P6 の「脆弱性」の定義が曖昧で、説明や回答の都度に概念領域が変動したり、主題がずれることがある印象なので、可能であれば、この資料における「脆弱性」の定義を示したほうが良いのではないか。特に、5G という概念領域における「脆弱性」には、”意図的に残されているバグのようなもの”という報告が目立っているので、経産省や IPA で定義されているものとは異なるところがあると思う。

徳田構成員）

総合対策の改定にあたって、スライド２をみると「背景」と書いてあるが、これは COVID－19 前に書かれているものなので、（０）として今の状況、我々が直面している課題をどう克服していくかを明示的に書いたほうが良い。デジタルトランスフォーメーションや ICT リテラシーの高くない企業の方々や全くデジタル化などには興味の無かった方々が、好むと好まずに関わらず社会的な要請でテレワークに移行した。ネットワークに関係のなかった方々が突如、ネットワークや端末を使ってテレワークに入っているので、Privacy-aware や Security-aware な状態での働き方改革になっていない場合が多い。したがって、このまとめの前に、好むと好まざるとに関わらずサイバーシフトしてしまった人へ明示的にメッセージを少し書くべきではないか。

竹内サイバーセキュリティ統括官）※チャットによるコメント

背景の追記、施策の記載順序含めて、見直しを行えればと思う。

大森サイバーセキュリティ統括官室参事官（総括担当））

今日の段階では取りまとめの方向性の案ということで、ご議論いただいた内容を改定という形で文章にまとめていく。今日頂いたご意見を踏まえながら事務局のほうで作業をしていく。

後藤座長）

遠隔ながら活発な議論ができた。只今ご議論いただいた内容を踏まえつつ、IoT・5G セキュリティ総合対策の改定に向けて事務局で検討を進めていただき、次回以降、また皆さまの御意見をいただきたいと思う。

（3）閉会

なお、会合終了後に岡村構成員から意見（別紙）が提出された。

【別紙】

会合終了後に岡村構成員から寄せられた文書による意見

現在要請されているテレワーク関連のセキュリティについて、最新の情勢を踏まえて「実践的な内容のチェックリスト」を策定することは急務であり、大きな意義があるものと考える。 参考のため、上記策定の際、留意すべき点に関する私見は次だ。

1. テレワーク用ソフトの選定

・ネット会議用アプリその他のテレワーク用ソフトの中にはセキュリティ、プライバシー上の問題大きいものがある。また、脆弱性が判明したものもある。このため、貴省その他の関連省庁において、それらの情報を集約して、所管の官民部門に係る組織に対し適切かつ迅速に情報の周知に努めるようお願いしたい。

・不慣れな企業のため、先進企業等におけるユースケースの収集・公表も可能な限りお願いしたい。

2. テレワーク用ソフトの職員向け使用訓練等

・扱い慣れないテレワーク用ソフトの設定ミスがないよう、勤務先たる当該組織（以下「勤務先」という）において、その社員・職員（以下「社員等」という）に対し事前にテストを行い、社員等向けに勤務先内サポート窓口（専用ダイヤル・専用アドレス等による）を設けることが望ましい。

3. 社員等に対する注意事項の周知・啓発

・テレワークは、社員等の自前端末ではなく、勤務先が貸与した端末（以下「勤務先貸与端末」という）に限定して使用すること、勤務先貸与端末を持ち帰る際には不要なファイル等が記憶媒体に入っていないかチェックして消去することが求められる。

・勤務先貸与端末には、セキュリティソフトをインストールするとともに、勤務先指定ソフト以外のインストールを事前許可制にする（可能であれば勤務先貸与端末の設定変更に技術的制限を設ける）。なお、禁止ではなく事前許可制にするのは、外部組織との会議に別のテレワーク用ソフトを用いるべき場合があるからである。

・外部組織との会議に自宅等からテレワークする必要がある場合には、「なりすまし」に注意する。

・ネット会議用ソフトを使用する際、カメラから背景等から自己の個人情報が漏れるおそれがないよう留意する。例えば、背景である窓の外の風景から自宅所在地等が推測されるおそれがある。机上に置いた書類内容が映り込んで漏れないよう注意する。そのため、カメラの角度に留意しつつ、無地の壁を背景にする、ソフトの設定で可能であれば背景に一般的な風景写真を用いること、家族の声や画像が入り込まないよう居間以外の別の部屋での使用を心掛ける。また、ネット会議の相手方音声が周囲に漏れないよう、なるべく端末スピーカーに代えマイク付きイヤホンを用いる。

・同様の理由で、みだりに位置情報が外部漏洩しないよう、設定に留意する（可能であれば勤務先貸与端末の設定変更に技術的制限を設ける）。

・使用していた勤務先貸与端末を、出社して社内LAN に接続する際、セキュリティチェックする。

以上