参考資料２

サイバーセキュリティタスクフォース（第 32 回）議事要旨

1. 日 時）令和３年６月３日（木）13：00～15：00

2. 場 所）オンライン

3. 出席者）

【構成員】

後藤座長、安達構成員、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、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】

扇慎太郎（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）、尾崎洸（経済産業省）

【総務省】

田原サイバーセキュリティ統括官、藤野審議官（国際技術、サイバーセキュリティ担当）、中溝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）、佐々木サイバーセキュリティ統括官室統括補佐、横澤田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 32-1　「ICT サイバーセキュリティ総合対策 2021」（案）
参考資料１　「ICT サイバーセキュリティ総合対策 2021」（案）の概要
参考資料２　デジタル社会の実現に向けた改革の基本方針の概要
参考資料３　次期サイバーセキュリティ戦略（骨子）の概要
参考資料４　サイバーセキュリティタスクフォース第 31 回 議事要旨

5. 議事概要

（1）開会

（2）説明

◆議題（１）「「ICT サイバーセキュリティ総合対策 2021」（案）」について、事務局より「資料 32-1　「ICT サイバーセキュリティ総合対策 2021」（案）」を説明。

◆構成員の意見・コメント

後藤座長）

「ICT サイバーセキュリティ総合対策 2021」（案）（以下、「総合対策 2021（案）」とする。）について、中身が豊富かつ、初めて見る方もいるかと思うので、脚注の追加や用語集を記載すると良いと思ったが、そういった予定

はあるか。無いようであれば脚注を少し追加する程度で良いと思うが、幅広い記載があるため、検討いただきたい。

横澤田サイバーセキュリティ統括官室参事官補佐）

特段作業の予定はなかったが、改めて脚注の必要性を検討した上で対応する。

戸川構成員）

全体的なコメントとして、今回 ICT という大きな枠組みの中で IoT・5G セキュリティ総合対策 2020 を全体的に見直し、構成をし直すという立て付けでまとめられており、有意義だと思っている。実際に総合対策 2020 と総合対策 2021（案）を比べながら資料等を拝見したが、例えば、総合対策 2020 における「Ⅲ 具体的施策」が、これまで各項 10 項目であったところを 3 項目にまとめていただくような形で、綺麗に整理されたと理解している。具体的な質問としては、かなりフォーマットが変わっている状態かと思うが、総合対策 2020 で取り上げられたいくつかの施策・課題等の中で今回取り上げられなかったものはあるか。

中尾構成員）

全体の構成に関係する質問をさせていただく。参考資料 1 の 2 ページにある、「Ⅱ 情報通信サービス・ネットワークの個別分野に関する具体的施策」のうち、1、2、3、4 とあるが、3 を拝見するとデジタル改革・DX 推進の基盤となるサービス等のセキュリティ対策の推進とある。そこでは IoT、クラウド、スマートシティが取り上げられており、その 3 つは確かに重要な課題である。しかし、IoT は 5G のエッジで利用され、クラウドは 5G の MEC のセンター（コア）として利用され、またスマートシティの基盤になるという点で、こういったサービス等に関わるセキュリティ対策として、5Gというのを「１．電気通信事業者における安全かつ信頼性の高いネットワークの確保のためのセキュリティ対策の推進」の（3）で挙げられているのだと思うが、その辺り全体のバランスにおいて少し違和感がある。全体の構成の中で、上手く配分または整理していただくことは可能か。

中溝サイバーセキュリティ統括官室参事官）

戸川構成員からのご指摘の点について、昨年の総合対策 2020 から終了した取組を削除することはあり得るが、基本的には踏襲したものとなっている。例えば、一部オリパラ東京大会に向けた施策がもう終わっており、また、人材育成のサイバーコロッセオは既に終了しているため、その言及というのは基本的には他の部分へ、その成果を活用する程度の記載にとどめている。基本的には昨年記載したものの内、特段落としたものはないとご理解いただいて良い。中尾構成員からのご指摘の点については、5G の記載場所は正直、事務局の中でも議論があった部分であった。5G について、主には電気通信事業者が提供するネットワークとしての 5G の安全・信頼性をどのように確保するかというところを 5G のセキュリティ対策の一つの大きい柱として考え、「１．電気通信事業者における安全かつ信頼性の高いネットワークの確保のためのセキュリティ対策の推進」のところに現時点でカテゴライズして入れている。ただ、5G のところで説明した通り、5G は当然、電気通信事業者（提供する側）の対策も必要だが、5G のユーザ側としてもしっかりセキュリティ対策を講じるということも大事である。そのため、その点も付記した形で、メインは電気通信事業者、提供する事業者側のセキュリティ対策、安全・信頼性の確保のための対策ということでⅡ章の配下に置いているが、実際の記述としては、もう少し広くユーザ側の視点も踏まえた記述として書かせていただいている。そのような形でこの部分に入れるということで、どうかと考えている。

後藤座長）

それぞれ全て密に関係するものなので、配置に苦労したのではないかと思うが、少しでも分かりやすい形で工夫いただくということで良いと思う。

岡村構成員）

マクロな議論の後で細かいことだが、総合対策 2021（案）の 10 ページに「NICTER で観測したサイバー攻撃関連通信の約半数が IoT 機器を狙ったものである」という記載が登場する。これは意図的に IoT 機器を標的にしたという読み方になると思うが、裏付けがあるのか。もし、ないのであれば、結果として IoT 機器が対象になったという趣旨になるので IoT 機器が対象となったものであるといった書き方をするというのも一つの手ではないか。

横澤田サイバーセキュリティ統括官室参事官補佐）

記載の根拠としては、総合対策 2021（案）の 13 ページ目にある NICT で運用している NICTER の円グラフになる。外部から飛んでくる攻撃通信の中身を分析した結果を示したもので、IoT 機器を狙った攻撃が 37%を占める。攻撃通信の宛先のポートが何かというところから通常 IoT 機器で使われているポート向けの通信がこれだけを占めているということで、その通信の送り手としても IoT 機器を狙ったものだと解釈をしてこのような記載にしている。

吉岡構成員）

総合対策 2021（案）の研究開発の前の箇所で C&C サーバの検知やフロー分析を行い、対策をしていくという内容も記載されており、これは非常に効果的な手段になり得ると思う。こういった方法で攻撃側が操作している C&C サーバの情報を捕まえていくことは大事だと思うが、フロー分析に加えて、マルウェア解析などから、国内でいわゆる IoC（Indicator of Compromise）の生成や収集を積極的に行うことが大事である。さらにもう一歩進めると、攻撃者や攻撃者グループのふるまい、動向の把握を進めることに意義があるのではないか。その背景にあるエコシステムや攻撃の動機の把握まで出来ると、対策や施策を考える時により実効性が高くなるのではないかと思う。IoT のサイバー攻撃についても、Mirai 等で DoS 攻撃の話が大きくあったが、最近は、NAS の中のファイルを暗号化するようなランサムウェア攻撃が IoT でも発生しており、実際に国内でも被害が出ている。そういった機器の特性も上手く考慮してマネタイズも行われるという傾向も少し出ているように思い、さらに重要な機能や役割を持つ IoT 機器に対して同様の攻撃がある可能性もあると思う。複雑化している攻撃側の行動原理や動機を適宜分析することで、対処療法的に、最終的に出ている攻撃を観測するということに加えて、元凶を絶つという意味合いで攻撃について理解をして、適切に対応するという意味での研究が必要だと思っている。もう一点、NOTICE 等で行われている施策について、それらだけでは十分な効果を得ることは難しいという話があり、その通りだと思う。一方で、これらの施策の効果がどのくらいあったのかをしっかりと評価すること自体も凄く難しい。かなり複雑な要素が絡み合っているので、数字上での単純な増減などの議論は難しいことも多く、施策や対策がどういう効果があったのかということを適切に測ること自体が研究だと思う。そのため、研究の項目の中にそういった定量的な評価のための研究開発というものもあると良いのではないか。

鵜飼構成員）

安全保障という観点での話が、ここ数年とても重要になってきている。この数カ月ほどの間で Tick 関連の話が色々と出てきており、民間のセキュリティベンダにおける意識の向上が見えると思うが、この点を全体的にもう少し入れ込んだ方が良いと思う。顕著に出ている例としては、攻撃された際、今まではどちらかというと、積極的に色々な情報を公開・公表していくというものだったが、これは攻撃者にヒントを与えることにもなりかねな

い側面もあるため、安全保障の観点で考えると公開する内容については慎重にしていかないといけない。場合によっては、安全保障上公表しないという対応も有り得る。情報共有についても今までの議論では、技術情報の話がメインになっていて、実際に攻撃者や営業情報に関連するような話、具体的には今回 Tick が色々とセキュリティベンダの製品を買いあさるという話もあったが、もう少し一歩踏み込んだ話を安全保障という観点でやっていかなければいけないのかと思う。クラウドについても同様で、足元で色々なクラウドサービス、本来であれば中身を解析されないはずの製品を無理やり調達されて中身を解析されたりしている。また国内産業も安全保障上大変重要だが、技術というところにどうしてもフォーカスがいっており、国内産業をさらに大きくしていくというところだけでなく、普及策のようなものがまだまだ議論するべきところだと思っている。いずれにしても全体的に安全保障として、ICT に関する施策、サイバーセキュリティに関する戦略をどうすべきかについて、今後も各論の中で議論ができればと思う。

後藤座長）

安全保障に関し、参考資料 3 の次期サイバーセキュリティ戦略の骨子案でも既にいくつか出ている議論が多いかと思うが、その辺りとのすり合わせを今後もしていくということで良いか。

中溝サイバーセキュリティ統括官室参事官）

サイバーセキュリティ戦略本部における次期戦略の議論でも安全保障に関する言及も色々あるかと思うので、そちらの議論も踏まえて検討する。

林構成員）

一つはミクロの細かい点だが、目次「II 情報通信サービス・ネットワークの個別分野に関する具体的施策」の中、「4 その他の具体的施策」、また「III 横断的施策」の「2 その他の横断的施策」とあるが、「その他」という表記では、重要度が弱い印象を受けた。「II 情報通信サービス・ネットワークの個別分野に関する具体的施策」の「個別分野」という表記を取り、II、IIIそれぞれに「個別分野の具体的施策」という表記をした方がよいのではないか。もう一つの方はもう少し大きな話だが、現在、科学技術政策や科学技術社会論に関わる方々が作ろうとしている「日本の科学技術」という本のうち、「デジタル社会」という部分で、私も編者の一人ということで参画している。そこで 2010 年から 2021 年までの科学史を振り返る部分を担当するにあたり、やはりこの時代は DX が一番の特徴かと思い、DX についての色々な本を読み、作成した素案を他の章の担当者の前で発表したところ、DX がよく分からないという声が非常に強かった。一流の科学者、技術者が集まっていてもそのような声が多く驚いた。コンセプトとして DX というのはカバーする範囲が非常に広いので、分かりにくいのではないかと思う。今までのセキュリティは DX という概念とあまり接点がないままにセキュリティ・プロパーで議論して良かったが、これからは DX とセキュリティという表裏一体みたいな形で議論することになると思う。そのため、例えばコラムという形で解説を入れる、あるいは先ほど出てきた国民のためのサイトに記載するなど、このドキュメントが一般の方々に読まれるような工夫というのが、より必要になってきたのではないか。

後藤座長）

その他の要望については工夫いただくこととし、DX については参考資料 3 の次期戦略にもある言葉なので、解説を少し追加すると良いかもしれない。

若江構成員）

総合対策 2021（案）の 20 ページ、IoT のセキュリティ対策に関して、①に安全な設計、製造、販売のことが記

載されていて、②に安全でないものに対する注意喚起ということが、対策として記載されているが、その間にユーザに対する安全な設定や使い方に関する啓発があっても良いのではないか。無線 LAN のセキュリティの関係ではガイドラインを利用者や提供者向けに作って、周知・徹底をしていた。IoT については、最後の方に少しだけ記載されているだけだ。パスワードをきちんとつける、インターネット側に認証画面を公開しないなど、基本的な安全な使い方や設定が、意外と知られていない。今後も法人ユーザや SIer に対する働きかけというのはあると思うが、SIer でもあまり意識できていないところがあると聞いている。ユーザ側が安全な設定をして利用するというようなことへの注意喚起があると、注意喚起のリーチが難しいという問題の改善に役立つのではないか。

後藤座長）

販売側もユーザに啓発する必要があり、ユーザ側も購入後に注意が必要だが、この辺りは一言付け加える形か。

中溝サイバーセキュリティ統括官室参事官）

付け加える方向で検討したい。このタスクフォースの提言案の中に記載はしていないが、総務省では重要 IoT 機器の調査をしており、実際に IoT 機器をモニター出来る画面をネット上で見る事が可能であった場合があり、そこを調査して、実際に直接注意喚起や対策を呼びかけるといった取組などもこれまでやってきている。いずれにしても趣旨を踏まえて、記載ぶりを検討したい。

徳田構成員）

一点目のコメントとして、私たちは日頃このようなキーワードに慣れているが、先ほどの後藤先生、林先生のコメントと同様に、もう少し消化しやすい形に工夫されるのが良いかと思う。二点目は各論に入るが、「II デジタル改革・DX 推進の基礎となるサービス等のセキュリティ対策の推進」の「(3) スマートシティのセキュリティ対策」について、ある程度は触れられていると思う。まず一つに情報共有として、イギリスの英国アカデミーやロイヤルソサイエティが COP26 に向け、温暖化対策に ICT を様々使うということがある。そのなかには様々な項目があるが、様々なセンサーを使って温暖化の状況をモニタリングし、それを基にフィードバックをかけていくというものがある。その際、データの改ざん等があるといけないので、infrastructure with trust ということで、社会インフラを作る上でのサイバーセキュリティの重要性が記載されている。今回の総合対策の印象が DX ということで、これからの社会を支える社会基盤をどう守っていくかということにつき、Ⅰ、II、Ⅲと挙げてあるが、あらゆる産業セグメントが with trust の infrastructure に依存してくるという社会の変容をもう少し強調されるのも良いのではないか。また、スマートシティセキュリティガイドライン（第 2.0 版）のパブコメを今やっている最中かもしれないが、「Ⅲ 横断的施策」の「２．その他の横断的施策 （1）国際連携の推進」という、国際標準化に向けてスマート IoT のガイドラインに関しては、かなり順調に ITU-T 等のキーワードが入ってきている。スマートシティセキュリティガイドラインに関してもどういう形で国際標準にプッシュしていくかというのを少し触れていただけると良いのではないか。次に研究開発の推進のところで、特に IoT の関係機器の NOTICE が進められているが、様々な施策の効果を評価して検証できるような指標を作っていく必要があると思う。さらに様々な IoT 機器の場合にはソフトウェアでコントロールされているので、効率良く様々なことが分析、チェック、または検証できるツールセットのようなものがパブリックにもっとできていくことが必要ではないかと思った。最後に、AI×セキュリティというキーワードがあまり触れられなくなっている部分があり、AI バックグラウンドの人を新しいセキュリティ人材として引き込む意味でも、セキュリティドメインでも機能的な方法で新しい知見が得られるということは、非常に大事なキーワードになってくるので、AI×セキュリティも非常に重要な分野だと思う。

中溝サイバーセキュリティ統括官室参事官）

スマートシティセキュリティガイドライン（第 2.0 版）の意見募集の期間は終了しており、現在提出意見の精査中でそれが終わり次第、公表というスケジュールを予定している。いずれにしても、それを踏まえて今後、国内のみならず、国外にも色々と情報共有等をして認識を広めていきたいというような思いを持っている。

藤本構成員）

私も最近ＤＸのセキュリティの話をすると、それは一体何かというような質問を受けることが多くなっていて、やはりなかなか分かりにくいのかと感じている。そういった中で、総合対策 2021（案）を拝見すると、社会全体のデジタル改革と DX というのが、セットで文書中に何箇所か出てくる。これを自分なりに読み解いてみると、社会で起きている様々なことをデジタルデータとして捉えることにより、新しいことができるという形で DX を捉えていると理解した。しかしそのように読み替えるのが正しいかよく分からないため、共通理解を得られるような説明が付加されると良い。

小山構成員）

一点目は、研究開発に関し、吉岡構成員の考えに賛同するので、我々通信事業者も協力したい。二点目は、総合対策 2021（案）の 31 ページ目、サイバー攻撃の被害情報の適切な共有及び公表の促進については、被害組織が情報提供をためらう、または提供するにも色々課題がある点記載している通りと思う。民間企業が国の支援を受けたような、攻撃者に対抗しうる最大の武器というのは情報の共有だったり発信だったりするが、被害を受けてみると本当に難しいのは被害者自身から情報を提供することなので、ここは引き続き検討をお願いしたい。

安達構成員）

以前、このタスクフォースでも発言したが、通信事業者のネットワークはインフラのベースになっていると思うので、我々放送事業者にとっても、またその他の事業者にとっても、通信事業者ネットワークは重要な位置づけである。そのためここに記載があるように、小山構成員から秘匿性がというお話があったが、それを超えてサイバー攻撃が排除されたクリアなネットワークが構築できることが理想である。やはり通信事業者だけでは、その構築は厳しいと思うので、その他セキュリティベンダや ISP とも連携することで可能になるのかと考えている。

岡村構成員）

一点目に、総合対策 2021（案）の 41 ページ目、利用者への普及啓発案だが、高齢者のデジタル格差は、かなり古くから言われてきた問題であり、今回のコロナワクチン接種のネット予約で改めて浮き彫りになった。共助という記載にデジタル格差を含めているとは思うが、高齢者のデジタル格差の縮小のための啓発活動は、セキュリティ面でも必要かつ重要である旨を改めて文字として明確化した記載ぶりにしていただきたい。もう一点は、40 ページ、41 ページの辺りで、デジタル社会形成基本法に基づいた記載としても良いが、社会全体のデジタル化、また、かねてより言われているサプライチェーン全体の推進向上という観点から、中小企業においては高度な人材だけではなくて、よりベーシックなことができるような人材の確保にも非常に難儀している状態であるので、そうした中小企業向けのセキュリティ人材の育成などについても明記していただくということを是非お願いしたい。

中尾構成員）

本文最後、今後の進め方の部分について、総務省としては今後この提言を踏まえて、自由、公正、かつ安全なサイバー空間の実現を下支えする ICT インフラ・サービスのサイバーセキュリティの確保を図る観点から、各施策を具体的に推進していくことを期待するものであると記載している。ここについて、もう少し総務省が推し進め

る意味合いを含めて記載できないか。具体的な事項が記載されている総合対策なので、総務省はこういった対策をハイレベルかもしれないが、ご提言いただきつつ、最後の進め方の部分をもう少し、前向きな記載としていただきたい。

中溝サイバーセキュリティ統括官室参事官）

あくまでも本総合対策は、本タスクフォースの有識者の皆様から総務省に対するご提言として、事務局でとりまとめているものだが、いただいたご趣旨は表現ぶりのニュアンスの問題だけだと思うので、大枠は変えづらいが検討する。

岡村構成員）

参考資料 3 にも関わることだが、オリパラの準備は完了したと理解しており、次に大規模国家的イベントとして万博がある。これからの問題でもあり、大量の攻撃を受ける可能性があるので、出来れば触れていただきたい。

高村サイバーセキュリティ統括官室参事官）

万博については、政府全体の中でオリパラと同じようにテロ対策及びサイバー対策のタスクフォースがそれぞれ立っている。そもそも万博については、ICT を何に使うか決まっていない状態で、オリンピックであれば招致した際にいわゆる国際放送センター（IBC）から公式映像と公式音が放送されるということが分かっていたが、それに対して万博の場合はチケット販売サイトが立つ以上の情報がない。そのため何を記載するのかという問題になるので、現段階で何をすべきだという提言できるものがないと理解していただきたい。話が具現化した際には、その部分は当然先生方にも相談しながら、記載することになると思う。

中尾構成員）

一点目は総合対策 2021（案）の 12 ページで PDCA サイクルと記載されていることについて、PDCA は Plan Do Check Act のことで、日本でしか使われていない言葉になっている。今は Plan の前に Identify としてビジネスの状況やリスク分析などがあり、これは Plan の中に入っていない。もし、この PDCA を使わざるを得ないのであれば、仕方ないが、リスク管理サイクルといったような言葉に置き換えた方が良いと思う。もう一点は、これも非常に細かい点だが、34 ページに国際的な ISAC 間連携とある。これは非常に重要だが、ISAC を持っていない国が非常に多くあるため、ISAC 間連携だけというよりも、最後の方にこのような脅威情報等の共有、分析のための取組を国際的に拡大することも重要である、というような記載の方が良いのではないか。

篠田構成員）

生まれたときから eID や Email アドレスを持つような、デジタル・ネイティブが 100%に近くなる時代までは、年齢、国籍、障害、といったさまざまな要因から格差はあり続けるため、アナログ処理も並行して持ち続けることになると思う。先日も話したが、高い技術を持つ人材教育と合わせて、社会に足りないピースとしての人材教育もあわせて今後考えていけたらと思う。AI の部分について、数年前から AI の方々にアプローチしているが、人類の課題解決の方が先であり、AI はセキュリティまでは手が回らず、優先度、順番があれば、ずっと後になるだろうと言われる。リサーチャーに任せていたら難しいということで、優先度を上げるからには何か手を打たないと扱ってもらえないという印象を持っている。

後藤座長）

前向きなアドバイスや用語の追加等をコメントいただいたが、全体として良くまとまって、カバーされている戦略になっているのではないかというコメントが多かったと思う。

（3）閉会

以上