サイバーセキュリティタスクフォース（第 14 回）議事要旨

1. 日 時：令和元年 6 月 14 日（金）10:00～11:30

2. 場 所：中央合同庁舎 2 号館 8 階　第 1 特別会議室

3. 出席者：

【構成員】

徳田座長代理、鵜飼構成員(代理:金居)、岡村構成員、後藤構成員、小山構成員(代理:大田)、園田構成員、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】

吉川徹志(内閣サイバーセキュリティセンター)、木村隼斗(経済産業省) 、矢野博之(情報通信研究機構)

【総務省】

竹内サイバーセキュリティ統括官、泉審議官(国際技術、サイバーセキュリティ担当)、二宮サイバーセキュリティ・情報化審議官、木村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)、三田地上放送課長、坂中技術政策課長、福島通信規格課企画官、中溝消費者行政第二課長、井手電気通信技術システム課認証分析官、相川サイバーセキュリティ統括官室参事官補佐、篠崎サイバーセキュリティ統括官室統括補佐、豊重サイバーセキュリティ統括官室参事官補佐、横澤田サイバーセキュリティ統括官室参事官補佐

4. 配布資料

資料 14－1　IoT セキュリティ総合対策改定版（仮称）（案）について（事務局作成資料）

資料 14－2　IoT セキュリティ総合対策改定版（仮称）（案）【メイン・随行のみ】

資料 14－3　「サイバーセキュリティ戦略」における各施策の位置づけ

資料 14－4　「サイバーセキュリティ人材育成分科会」第 1 次取りまとめ

参考資料１　IoT セキュリティ総合対策（平成 29 年 10 月）

参考資料２　IoT セキュリティ総合対策プログレスレポート 2019（令和元年 5 月）

参考資料３　G20 貿易・デジタル経済大臣会合閣僚声明（仮訳）

5. 議事概要

(1) 開会

(2) 議事

◆ 議事（１）IoT セキュリティ総合対策改定版（仮称）（案）について、事務局より、資料 14－1　IoT セキュリティ総合対策改定版（仮称）（案）について（事務局作成資料）、資料 14－2　IoT セキュリティ総合対策改定版（仮称）（案）【メイン・随行のみ】、資料 14－3　「サイバーセキュリティ戦略」における各施策の位置づけ、資料 14－4　「サイバーセキュリティ人材育成分科会」第 1 次取りまとめを説明(省略)

◆ 議論終了後、竹内サイバーセキュリティ統括官より、参考資料３について補足説明。

◆　関係者の意見・コメント

（１）IoT セキュリティ総合対策改定版（仮称）（案）について

名和構成員)

「資料 14-1」の 5 ページに関して、最低限のセキュリティ対策を行うという説明があったが、最低限の定義や決め方はどのようになっているか。

木村サイバーセキュリティ統括官室参事官(総括担当))

これから新しく製造される IoT 機器に関して、規則を改正して技術的基準を盛り込んでいる。例えば、ID・パスワードの初期設定を変更したり、ファームウェアのアップデートを行ったりするような基準を最低限のものとして規則に盛り込んでいる。来年 4 月から施行する予定で現在準備期間の段階にある。

名和構成員)

最低限を決める根拠については、透明性が確保されているか。チームを組んで合意形成しながら決めるのか。原子力分野では、DBT という設計基礎脅威を定めており、そのような脅威に基づいて妥当性を確保しながら決めている例もある。解釈に揺らぎがないようにしてほしい。

木村サイバーセキュリティ統括官室参事官(総括担当))

規則の改正については、別の審議会で議論を重ね、その議論に基づいてパブコメを行い、省令改正を行うという流れになっている。規則の内容については、解釈が明確になるように運用上のガイドラインを作成し、今年 4 月に公表しているところである。

名和構成員)

審議会に集まった有識者の方々の知見と能力に基づく議論によって決まるという認識になる。

竹内サイバーセキュリティ統括官)

若干補足する。説明上、事務局が最低限という言葉を使ったが、理解していただくために使った言葉になっている。何が最低限であるかということを求めて、深く議論した訳ではない。趣旨としては、ネットワークを保護するために端末・機器に対し、どのような機能を求めるかということを電気通信事業法の省令で規定している。必要な機能を持っていることが定められ、サイバーセキュリティの観点ではアクセス制御機能、パスワード変更を促す機能、ファームウェアのアップデート機能という 3 つの機能を持っていることが、今回追加する内容として妥当であるとし、省令改正した。言葉としての最低限に、絶対的な意義がある訳ではない。

名和構成員)

安心した。原子力施設防護で類似の取り組みがあった。最低限を決める取り組みで 5 年間議論が停滞した。その後、DBT という設計基礎脅威を定めて、ようやく議論が動き出したという経緯があるので気になった。

岡村構成員)

「資料 14-4」の 3 ページに関して、サイバーセキュリティ人材の中央への偏在が、ものすごいスピードで進んでいるということを身にしみて感じているところである。その背景を別の面からみると、かつて人材のブリーダーであった大学では、自前でサーバーを構えていたが、外部のクラウドを使うようになってきている。サーバーの管理に携わり、現場でセキュリティの知見を育んでいたが、いまやせいぜい端末の管理が中心になっており、新たな育ちがなくなっている。そのような取り巻く環境変化についても指摘しておきたい。そうなると能動的に人材づくりについて高専等を含めて実施していかないといけない。そこに人を持っていくやり方として、初等・中等教育でプログラミング教育の必要性が指摘されているが、同時に中等教育ぐらいで正式なカリキュラムでなくても、セキュリティの重要性・必要性を説くような形のものが入るとよい。

中尾構成員)

「資料 14-1」に関して、前回のタスクフォースにおいて、「IoT セキュリティ総合対策プログレスレポート」の中にばらばらにいろいろな事が記載されていたが、今回の改定の中では、それらが十分整理されて分かりやすくなっていると思う。

2 ページに関して、策定後の状況変化として 6 点が記載されているが、「①5G のサービス開始」、「②サプライチェーンリスクの重要性」という見出しは言葉が足りていない。おそらく②はリスク管理の重要性とした方がよい。「③ Society5.0 の実現に向けたデータの流通・管理の重要性」についても、①や②が相互に絡んでいると思う。説明を聞いた感じだと分けて書いてもよいという気がした。「⑤大規模な量子コンピュータの実用化の可能性」については、実用化されていると断言はしていないが、裏返して考えた方がよい。私見になるが、さまざまな学会に出席していると、実用化が進んでいると言う人もいるが、実用化はまだ大分先であると言う人も結構いる。そういう状況を踏まえると、例えば、⑤の大項目では、新たな推奨暗号の研究開発の必要性ということを言って、その裏に大規模な量子コンピュータの実用化を視野に入れるということを入れておくことについて検討してもらいたい。

4 ページに関して、具体的施策に IoT、5G、クラウド、スマートシティのセキュリティが記載されているが、研究開発にはそれらの研究開発が記載されていない。また研究開発に記載されている内容は、6 ページの横断的施策の「①基礎的・基盤的な研究開発等の推進」を指していると思われるが、サイバーセキュリティの考え方からみると、予兆を見つけるための観測技術や予兆の分析技術などの重要な技術がたくさんあり、それらが抜け落ちている。「①基礎的・基盤的な研究開発等の推進」に入っているということであればよいのかもしれないが、網羅的ではない。これらが「IoT セキュリティ総合対策改定版（仮称）（案）」の中に文章として記載されているとよい。

5 ページに関して、「（５）トラストサービスの在り方の検討について」は、WG で何回か議論され、今年度中に成果物が出るという説明を受けたが、どういうレベルで成果物が出てくるイメージであるか。例えば、いろいろな議論があって、トラストサービスを考えたときに、何をトラストアンカーにするか。トラストアンカーをハードウェアに置くのか、ハードウェアに載るソフトウェアの中に置くのか。そのような考え方を整理するか。どのようなレベルになるか説明してほしい。

木村サイバーセキュリティ統括官室参事官(総括担当))

研究開発の部分は、従来から取り組んでいるいろいろなセキュリティに関する研究開発があり、①基礎的・基盤的な研究開発等の推進の中に盛り込んでいる。その部分は継続して重視している。

竹内サイバーセキュリティ統括官)

「資料 14-1」の 4 ページに関して、AI による予兆分析のようなものが柱立てとして入っているのかどうかという指摘であるが、6 ページの「⑥AI を活用したサイバー攻撃検知・解析技術の研究開発」の中に内容としては入っており、しっかりと研究開発を実施していく。4 ページは何を目標として、個別施策と横断的施策がどういう位置づけになるかを模式図的に、絵で示しているものになる。考えられるすべての施策を書くという位置づけにはなっていない。個々の重要な施策が漏れていないかどうかや、位置づけが違っていないかどうかを、5 ページ以降の各施策の項目立てと、「資料 14-2」の中に記載しているので、会合後でもよいので確認してもらいたい。

トラストサービスについても、「資料 14-2」の中に記載しており、内容としては、電子署名について署名をクラウドに預けてリモートから署名できるようにすること、またタイムスタンプについては民間の認定制度しかないので不足する点もあるという指摘をもらっており、国としての認証制度について WG で検討している。さらに欧州で実施されている e シールについて、法人が発行する領収書・請求書や、ソフトウェアのアップデートのファイルが、この会社から提供されたものであることを証明できるようにすることや、どういうサービスの場合に、そのような認証・証明行為が必要であるか、どのような手続や位置づけが望ましいかについて WG で検討している。詳細は「資料 14-2」の中に記載している。

後藤構成員)

「資料 14-1」の 3 ページに関して、「時間軸を意識した施策展開」、「政策バリューチェーン」というキーワードが入っているが、これらはキーポイントである。サイバーセキュリティ人材づくりについて広い取組みが必要という意見が出たが、文科省の施策や NISC の取組みがある中で、今回は地域のセキュリティ人材育成に総務省が手を挙げているということになる。他の施策を見渡しながら、総務省における役割を示し、地域における問題解決を実施していくと訴えていくことが重要である。政策バリューチェーンを意識して取り組んでもらえるとよい。

国の動きは年度単位になっているが、人材育成は年度で切れるものではない。年度間にまたがって継続的な取組みをしてほしい。時間軸を意識した施策展開については、今回のように状況変化に対してどのように対応していくかという条件変化を捉える視点は大事である。変化のスピードは事象によってまちまちである。変化の仕方についても、労働人口の変化のように将来が見えていて、徐々に減るという予測に基づいて対応するものもあれば、AI の技術の進歩のように時々技術レベルの階段が上がり、一方向に変化するものに対応するものもある。さらに、昨今の国際情勢のように、突然変化が起きるものに対応するものもあり、セキュリティ業界では、インシデントレスポンスがその一般的な例であり、そういうものは政策面でも個々の政策を見るというよりは、省庁間で横連携して全体をみて議論できるような体制ができるとよい。IoT セキュリティについても、そのような観点からのチェックの仕組みについて年度間をまたがって継続的に進められるようになることを期待している。

林構成員)

「資料 14-3」に関して、吹き出しの枠線の色と各戦略の色で、同じ色を使っているものがあり、分かりにくいので色使いを変更してほしい。

「資料 14-2」の 4 ページにあるⅠ　背景の「（2）サイバーセキュリティリスクの増大」について、タイトル中の増大ですべてを表しているとは思うが、サイバーセキュリティ戦略では高度化、複雑化、深層化などいろいろな議論があって、もう少し重たいということを強く打ち出している。増大だと少し軽すぎる気がする。タイトルにそのような要素を盛り込んでほしい。4 ページ以降の中身で記載していることはそのままでよい。

藤本構成員)

世の中で IT の利活用が進展するのでセキュリティをしっかりと守らないといけないということは十分分かるが、さらに踏み込んで、セキュリティに積極的に取り組むことが、新しい時代を作ることになるというニュアンスが入っているとよい。AI を使った研究開発のような、セキュリティとしてできることがあって始めて、新しい Society5.0 が現実のものになると思う。セキュリティに携わる人間も、自分たちが新しい時代を作る中で重要な役割を果たしていることになり、関心を高めてもらえるようになるのではないかと思う。

吉岡構成員)

「資料 14-2」の 13 ページに関して、「NOTICE」で得られた情報を上手く共有していくことについて重要であると考えている。それに加えて、事業者の中での情報共有という観点と、「NOTICE」の活動を理解してもらうことも含めて、エンドユーザーにどうやってこの現状を正しく理解してもらえるかという観点の２つの観点が重要である。「NOTICE」で得られた情報をエンドユーザーに伝えるときに、伝えるという部分もテクニカルに難しい。そのような部分で効果を高める方法も大事になってくる。

「資料 14-2」の 21 ページに関して、IoT 機器の脆弱性についてどのように対応していくか考えるときに、ルーターのベンダーと話をしていると、脆弱性に対するアップデートをいつまで実施するかという部分に非常に苦労されている。セキュリティアップデートのエンドオブサービスについて、どのように考えるか、やめたくても周りが対応している中で自分たちだけなかなかやめられないというジレンマがあると聞いている。IoT 機器のベンダーとして、いつまで、どのレベルのサービスを提供していくかということに関して、さまざまな IoT 機器が存在するなかで、何らかの考え方の検討ができるとよい。

徳田座長代理)

米国のファンディングエージェンシーである NSF のプロジェクトで、ハワイ大学を中心に持続可能なエネルギーの研究を行っている現場を見に行ったことがある。同じファンディングで、NPO 法人がもらっている資金の中に、なぜ再生可能エネルギーが大事であるかを高校生に教えるための教材を作る予算が含まれていた。地域のセキュリティ人材育成においても、長期的にみると、「SecHack365」で作っている教材を地方でも使えるような形にし、初等・中等教育でプログラミング教育が入ってくるので、それと同じところでやさしいセキュリティに対するリテラシーを高めるために活用し実践すれば、効率良くセキュリティを認識してもらえるようになると考えられる。

セキュリティ人材の偏在、セキュリティに対するアウェアネスの偏在という話が出たが、セキュリティ人材がどうしても首都圏に偏ってくるのはそこで需要が生まれるからである。SME（Small & Medium Enterprise）ではなかなか現場の緊迫感はないと思うが、東京オリパラやラグビーW 杯などの大きなイベントがあると、全国規模でフィッシングなどいろいろな事が起きるので、コマースの観点からも自分たちのビジネスに直結してくることを認識できるとよい。地域レベルでのアウェアネスが高まるムーブメントがあれば、イベントと掛け合わせて、そういうことが議論されるようになるとよい。

事務局の方で、構成員から頂いた意見を整理してもらう。この場で言い足りない意見があれば、明日までに事務局に連絡してほしい。「IoT セキュリティ総合対策改定版（仮称）（案）」は、構成員から頂いた意見をもとに修正を行った後、パブリックコメントにかける予定である。その修正については、座長に一任していただきたい。

全構成員)

異議なし。

相川サイバーセキュリティ統括官室参事官補佐)

次回の会合の具体的な日程、場所、議題については、後日、事務局から連絡する。構成員の方々に個別に相談させていただくこともあるので、引き続きご協力を御願いたい。IoT セキュリティ総合対策改定版（仮称）（案）について、本日頂いた意見を踏まえて、事務局で反映して、座長と相談して、パブコメにかけたいと思う。それについて連絡をさせていただく。

以上