サイバーセキュリティタスクフォース（第 38 回）議事要旨

1. 日 時）令和 4 年 5 月 20 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、宇佐美構成員、岡村構成員、金居構成員（代理出席）、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、吉岡構成員

【オブザーバー】

鈴木雅也（デジタル庁）、石巻克基（経済産業省）、鈴木一弘（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、山内官房審議官（国際技術、サイバーセキュリティ担当）、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）、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、高地官房サイバーセキュリティ・情報化審議官、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 38－1　サイバーセキュリティを巡る最近の動向
資料 38－2　ICT サイバーセキュリティ総合対策 2022（仮）」の骨子（案）
参考資料 1　サイバーセキュリティタスクフォース第 37 回 議事要旨

5. 議事概要

（1）開会

（2）説明

◆議題（１）「サイバーセキュリティを巡る最近の動向について」について、事務局より資料 38-1 を説明。議題（２）「「ICT サイバーセキュリティ総合対策 2022（仮）」の骨子案について」について、事務局より資料 38-2 を説明。

◆構成員の意見・コメント

全体について

戸川構成員）

全般的に非常によくまとまっている。構成についても、これまでの議論がベースになっており良い。プログレスレポートの内容を本文に盛り込むことについても賛同する。「ICT サイバーセキュリティ総合対策 2021」の記載の達成度の把握は非常に重要。

後藤座長）
全体の構成については、各構成員から賛同が得られたものと理解した。なお、各項目においては、サイバーセキュリティ戦略の中での位置づけやデジタル社会の実現に向けた重点計画との関連に触れていただくと相互関係が分かりやすくなると思う。

岡村構成員）
構成案について、大枠これに賛成するところだが、今後本文の策定過程で動きもあろうかと思うため、弾力的に座長と事務局にお任せするという方向性で結構である。

「Ⅰ サイバーセキュリティを巡る最近の動向」について

小山構成員）
先般、経済安全保障推進法案が成立したが、その中には基幹インフラにおける事前審査制度のような大きな施策が含まれていたかと思う。そうしたことと、総務省の特に情報通信分野におけるサイバーセキュリティ対策の関連性に触れていただけると良い。

「Ⅱ 情報通信ネットワークの安全性・信頼性の確保」について

中尾構成員）
Ⅱのうち「1 情報通信ネットワークのサイバーセキュリティ対策の推進」で挙げられている８つの論点は、相互に関係する。例えばサプライチェーンは、IoT やクラウドサービスを用いたシステム環境やスマートシティ、放送設備にも関わる。ついては、5 ページの内容に加え、これらの全体像が分かる記載があると良い。

後藤座長）
全体像の追記、記載の順番や項目順の工夫を提案いただいたと理解した。

篠田構成員）
中尾構成員の観点と違うかもしれないが、全体像を把握し、省庁横断的に必要なところへリソース分配されるのが理想的である。

岡村構成員）
5 ページの SBOM について、オープンソースソフトウェアが多用されるライセンスについても十分な分析をした上で、オープンソースソフトウェアを安全に使っていくという方向性が今後求められると思う。現状は開発者任せになっているために、不安感のための躊躇が生じているように思われる。

後藤座長）
サプライチェーンリスクというのは非常に意味が広く、サービス要素としてのサプライチェーンとインフラ設備の部品・装置のサプライチェーンの２種類に分けられると思うので、整理して記載できると良い。

藤本構成員）
6 ページで触れられている NOTICE について、最近の状況等から特に検討したい内容等があれば、是非教えていただきたい。

高村サイバーセキュリティ統括官室参事官）

毎月約 1,500 人に注意喚起し、脆弱性に対処される方が約 500 人、脆弱性が残ってしまう方が約 1,000 人というところ。脆弱性に対処できない方、特に御本人が何等かの被害を受けておらず困っていないケースについてどうすべきかが最大の課題と認識しており、工夫が必要と思っている。

岡村構成員）
6 ページの「トラストサービスの普及」について、SSL 証明書にも様々なものがあるので、SSL 証明書を用いた https 通信であれば必ず安全・安心ということではない旨を記載いただければありがたい。

「Ⅲ サイバー攻撃への自律的な対処能力の向上」について

吉岡構成員）
7 ページの「大学や民間企業における研究開発の支援等」という見出しと、中身の CRYPTREC 暗号リスト改定等の関係性が少し分かりにくい。文脈を説明いただきたい。

高村サイバーセキュリティ統括官室参事官）
IoT マルウェアの無害化・無機能化の技術に関する研究開発等の記載が漏れていたため、改めて明記させていただければと思う。

中尾構成員）
総務省施策として進めている大学や民間企業が実施している研究開発を追記いただくのは良いと思うが、例えば CYNEX の産学官連携を視野に入れつつ、最先端のマルウェア解析や、セキュリティ対策の新規導出といった研究開発を推進するといったフレーズもあるとなお良い。

吉岡構成員）
同感である。

徳田構成員）
7 ページの「NICT における研究開発」について、耐量子計算機暗号（PQC: Post-Quantum Cryptography）は QKD ネットワーク（Quantum Key Distribution Network）と相互補完的に医療や金融の分野で使われているので、QKD ネットワークの技術についても触れるとバランスが良くなると思う。「大学や民間企業における研究開発の支援等」については、吉岡構成員をはじめ大学の先生方の活動を追記し、産学官連携を強化するような方向性を示せると良いのではないか。

高村サイバーセキュリティ統括官室参事官）
QKD ネットワークは暗号そのものではないのでどう書くか難しいが、検討させていただく。

後藤座長）
「研究開発の推進」の柱書で、Beyond 5G 等の中長期的な技術トレンド云々という記載と「大学や民間企業における研究開発の支援等」の記載がぴったりこない印象があり、工夫いただけると良い。

戸川構成員）
研究開発と人材育成は両輪で進めつつ、長期的な目標も掲げながら取り組むことが非常に重要である。特に、人材育成という点では、 8 ページの SecHack365 を含め若手の人材育成に力を入れていただきたい。

篠田構成員）
8 ページの「地域人材エコシステムの形成」について、モデル対象地域というのは都道府県レベルなのか、高専・大学レベルなのか。

高村サイバーセキュリティ統括官室参事官）
学校では仕事の提供まで行うのは難しいため、沖縄県にある第三セクターが、都道府県レベルで、自ら後継者を育成できるレベルまでの人材育成と、人材維持のための仕事のオーダーと地元企業のマッチングをセットで行っている。

「Ⅳ 国際連携の推進」について

中尾構成員）
9 ページの「⑤国際標準化」について、「『自由、公正かつ安全なサイバー空間』という我が国の基本的理念に必ずしも整合的でない動きに積極的な対処ができるよう」な「連携体制」とはどういうことなのか確認させていただきたい。また、この記載はサマライズされたものかもしれないが、標準化の対象は「IoT セキュリティガイドライン」に限られないので、もう少し幅広な表現にしていただけると助かる。

安藤サイバーセキュリティ統括官室企画官）
現在開催中の ITU-T　SG17 は、中尾構成員をはじめとする情報通信技術委員会(TTC)の皆様に御協力いただき、つつがなく進んでいる状況。その他、英国や米国といった有志国からも情報を頂きながら、まさに積極的に対処しているが、特に何か規定に基づく組織を立ち上げるということでもないので、「連携の強化」と改めさせていただければと思う。表現を幅広にする点についても御指摘のとおりであり、再考して提示させていただきたい。

徳田構成員）
前回も話題に出たが、サイバーセキュリティ分野の若手研究者のプレゼンス向上や長期的な信頼関係を築けるコミュニティの形成が不可欠と考えるところ、Ⅲ又はⅣのどこに記載するかはお任せするが、研究開発・人材育成における国際連携も推進いただきたい。

篠田構成員）
①から⑥の全ての取組について継続を期待するところであるが、これらはすべて政府同士又は ISAC 間同士の連携なのか。例えば、国内外の大学間や一定のレベルのコミュニティ間における連携支援等も含まれるのか。

安藤サイバーセキュリティ統括官室企画官）
④の「AJCCBC が実施する研修参加者のすそ野拡大」は、ASEAN のハブとして整備した AJCCBC をアカデミアの方々の日 ASEAN 交流の場にできないかという検討状況を踏まえて記載したもの。こちらの進捗についてはまた別途御報告させていただければと思う。

後藤座長）
国際連携の取組でリソースが確保されている場合は必ずしも多くないと思う。施策においては、ボランティアに期待となってしまわないように、リソースの裏付けも合わせて検討いただきたい。

「Ⅴ 普及啓発の推進」について

小山構成員）
10 ページの「サイバー攻撃被害に係る情報の共有・公表の適切な推進」は大変良い取組と思う。ガイダンスなので、強制力を伴わない参考資料という形からのスタートで良いと思うが、被害組織に公表する意思があっても公表すると批判されるという実態の解決に向けどう取り組むべきかという課題感も可能であれば記載いただきたい。

梅村サイバーセキュリティ統括官室参事官）
頂いた指摘も踏まえ、関係省庁と議論・検討していきたい。

藤本構成員）
10 ページの「サイバーセキュリティ対策情報開示の手引き」について、更新の際は、投資家を含むステークホルダーからの情報開示要望等について、2019 年の公表後の社会環境の変化があれば、それを踏まえていただければと思う。

岡村構成員）
2019 年の公表後以降、情報開示を巡る社会環境に大きな変化はないのではないか。一方で、被害情報を公表すると誹謗中傷の集中砲火を受けることがあるという実態はぜひ検討していただきたいと思う。また、今年の 4 月に ENISA が「EU における協調的脆弱性開示政策についての報告書」を公表しており、その中に我が国についての言及もあるので、Ⅳの国際連携の推進という観点から掘り下げていただくということも重要と思う。

名和構成員）
11 ページの「無線 LAN におけるサイバーセキュリティの確保」の各種ガイドラインについて、プライバシーに関する懸念を強調して示した方が良い。また、記載には及ばないと思うが、「Wi-Fi 利用者向け簡易マニュアル」においては、古い国産 Wi-Fi ルータで、非表示の SSID や MAC フィルタ設定がプライバシー上の懸念になっていること等の周知を行うべきではないか。

篠田構成員）

「個人向けの普及啓発」には、インシデント予防だけでなく発生時の分かりやすい対応方法という観点も加えていただきたい。また、disinformation（偽情報）等については、情報化社会において脆弱な方々を守る上でも非常に重要である一方、人材が不足しているので、重点課題の 1 つとして検討していただけたらと思う。

中尾構成員）

篠田構成員の指摘は重要だと思う。

名和構成員）
e-ネットキャラバンについて、学校は何万とあるので、どの程度の規模で実施されるのかが肝になる。病院内の教育施設等の様々な教育機関も含め、網羅率を拡大する方向で本事業の検討をしていただきたい。また、児童に対するセキュリティ普及啓発においては、教師への支援も必要と思うが、文科省との役割分担も気になる。高齢者関連では、最近大手の携帯電話販売会社が設定サービスを有償化したり、数百単位での店舗削減を行ったりする動きがある。これは高齢者に対するセキュリティの普及を低下させかねないが、このような現状の改善策についても考慮していただければと思っている。

後藤座長）
これまで携帯ショップの役割は大きく、大事なポイントかと思う。

梅村サイバーセキュリティ統括官室参事官）
文科省が新しい小学校の学習指導要領を 2020 年度に開始し、情報活用能力の育成をより重視する方針となっている。こうした状況も踏まえ、学校教育に引き続き協力すべく、情報通信分野の民間企業等の協力を得て、学校等に無料の出前講座を行っているのが e-ネットキャラバンという取組であり、コロナ禍以前は年間 3,000 ほどの講座を希望に応じて実施していたと記憶している。今後はこちらの取組にサイバーセキュリティの内容を少し付加できればということで検討して参りたい。

以上