サイバーセキュリティタスクフォース（第 39 回）議事要旨

1. 日 時）令和 4 年 6 月 10 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、小山構成員、篠田構成員、園田構成員、徳田構成員、中尾構成員、名和構成員、林構成員、藤本構成員、前田氏（鵜飼構成員代理出席）、吉岡構成員、若江構成員

【オブザーバー】

鈴木雅也（内閣サイバーセキュリティセンター）、黒澤健（経済産業省（代理出席））、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 39－1　「ICT サイバーセキュリティ総合対策 2022」（案）
資料 39－2　「ICT サイバーセキュリティ総合対策 2022」（案）の概要
参考資料 1　サイバーセキュリティタスクフォース第 38 回 議事要旨

5. 議事概要

（1）開会

（2）説明

◆議題「「ICT サイバーセキュリティ総合対策 2022」（案）について」について、事務局より資料 39-1、資料 39-2 を説明。

◆構成員の意見・コメント

Ⅰサイバーセキュリティを巡る最近の動向

林構成員）

“Cybersecurity for All”の政府における定訳は、「誰一人取り残さないサイバーセキュリティ」なのか、「誰一人取り残されないサイバーセキュリティ」なのか。

廣瀬サイバーセキュリティ統括官室参事官補佐）

こちらの表現は、持続可能な開発目標（SDGs：Sustainable Development Goals）の「Leave No One Behind」に

由来するものと認識している。「デジタル社会の実現に向けた重点計画」等のデジタル化の文脈では、「誰一人取り残されない」という表現が、「サイバーセキュリティ戦略」のようなサイバーセキュリティの文脈では「誰一人取り残さない（サイバーセキュリティの確保）」という表現が採用されているところ、本案では後者を採用しているが、必ずしも両者で何か意味が違うわけではないと理解している。

岡村構成員）
大変立派な報告書になり感謝する。フィッシング動向については、フィッシング対策協議会が本年６月３日に５月までのフィッシング報告状況を公表している（https://www.antiphishing.jp/report/monthly/202205.html）ので、脚注等で現状に言及いただければと思う。

梅村サイバーセキュリティ統括官室参事官）
岡村構成員から頂いたデータについて勉強させていただき、どのような記載ができるか検討してまいりたい。

高村サイバーセキュリティ統括官室参事官）
フィッシングの新しい報告状況が出ているということなので、最低限、注釈の更新はさせていただく。

篠田構成員）
Anti-Phishing Working Group の調査（https://www.newswire.com/news/apwg-1q-2022-report-phishing-reaches-record-high-apwg-observes-one-21733280?fbclid=IwAR0NhA27GxH7NCl6jGFTubtIz74L97ffbs8-YGRYGiCoAq55Vk3je1p4hy8）では、フィッシングの観測総数が記録的に多かった一方で、大規模にランサムウェアを開発・展開するサイバー犯罪組織の撤退傾向により、ランサムウェア攻撃の観測総数は減少を示している旨を補足する。

Ⅱ１.情報通信ネットワークの安全性・信頼性の確保

林構成員）
分量が多くやや分かりにくいという前回の指摘を踏まえて明快に整理されており、理解しやすくなった。特に、「ア.電気通信事業者による積極的サイバーセキュリティ対策の推進」の「今後の取組」において、通信の秘密とサイバー攻撃対策について、今後法改正も含めて検討していくと示されたということは評価に値する。その上で、（サイバー攻撃対策のために）通信内容そのものを利用することと、メタデータを利用することは性質がかなり異なることに留意いただきたい。また、今回検討対象にしているのは電気通信事業者（におけるサイバー攻撃対策）であるが、インターネット上のプレイヤーは電気通信事業者に限られないため、この点についても横断的に整理が必要な時期が来たのではないかと思っている。

岡村構成員）
大変立派な報告書になり感謝する。その上で林構成員も言及された通信の秘密に係る部分については、「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」（以下「サイバー研」という。）での既存の整理も踏まえ、更なる整理をお願いしたい。

若江構成員）
メタデータの取扱いもプライバシー保護の観点では重要と考えるなど、細かい点は異論があるが、制度改正の検討が急がれるという点については林構成員の問題意識を共有する。電気通信事業者によるサイバー攻撃対策は、これまでサイバー研で個別に法的整理を行ってきたが、サイバー攻撃が巧妙化する中で、解釈を都度整理していくのは即応性に欠けるだけでなく、場合によっては誤った解釈を提示してしまうおそれもある。また、サイバー

研の構成員のうち法律家の方々はサイバー攻撃の実態に詳しい方ばかりだとは思うが、攻撃手法等を詳細に把握しているわけではなく、攻撃対策に必要と説明されればダメとは言えない状況なのではないか。サイバー攻撃対策は重要で迅速な対応が求められるからこそ、法令化の必要が高い。14 ページの記載どおり、なるべく早く検討いただきたい。

梅村サイバーセキュリティ統括官室参事官）
御指摘を踏まえつつ、今後引き続き検討を進めたい。

名和構成員）
本案における「必要」と「重要」の語はどのように使い分けているのか。11 ページ「（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」のリード文では、「…これらを横断する課題としてのサプライチェーンリスク対策などの取組を強化することが必要」と記載している一方、16 ページ「(5G セキュリティガイドラインの普及等)」の「今後の取組」では、「今後も NICT や我が国の産業界において活用がなされるよう、検討を進めていくことが重要」と記載しており、サプライチェーンリスク対策は 5G セキュリティガイドラインの普及より低いレベルに置かれている印象があるので、文言を再考いただいた方が良いのではないか。

梅村サイバーセキュリティ統括官室参事官）
「必要」と「重要」で重要度のレベル感に差異を付けたつもりはない。むしろ具体的な対応が見えていたりするものについては、喫緊性を表すために「必要」と書いている。全体を見てどうかというのは少し眺めてみたい。

名和構成員）※チャット
一部の読み手は、この種の文書を丁寧に読みこんで社内施策の優先度を組み立てているので、できる限り読み手に寄り添った書き振りに配慮してもらうと良い。

篠田構成員）
Log4j の事案は氷山の一角であるとの認識から、オープンソフトウェアの保守作業が数名のボランティアに依存している実態を反省して、ホワイトハウスとオープンソースソフトウェアの団体が議論を重ねた結果、米国ではオープンソースセキュリティ強化の流れが進んでいる。SBOM 導入の検討についても大切だが、日本でもオープンソースソフトウェアの開発活動を官民で協力して行う方向を模索してはどうか。

高村サイバーセキュリティ統括官室参事官）
オープンソースソフトウェアのコミュニティ支援については、経産省所管の独法である IPA が設立したオープンソフトウェア・センターの人材育成ワーキンググループにおいて行う旨が過去に整理されており、ソフトウェアそのものということもあって総務省としては手を出しづらいところがある。また、2008 年に同センターにおいて自ら策定した「OSS モデルカリキュラム v1」に基づく人材育成に取り組んだが、多くの人材が外資企業に流れたという苦い経験もあり、（政府全体としても）手を出しづらい領域であるというのを御理解いただけるとありがたい。

小山構成員）
19 ページで「ソフトウェア脆弱性等を有する IoT 機器」に「直接的な注意喚起を行う手法について検討を進める」とあるが、これは製造事業者や販売事業者、輸入事業者から利用者に対して注意喚起を行うということか。ISP では同意なしに脆弱性を調査することは難しく、現行の NOTICE の取組でも直接的な注意喚起はできていいない。一方で、製造事業者等では販売先を記録しないのが一般的な商習慣であるため、利用者へのリーチが難

しいという課題が出てくる。この点、具体的にどのようにお考えかお聞かせ願いたい。

高村サイバーセキュリティ統括官室参事官）
ソフトウェア脆弱性等を有する IoT 機器については、周知啓発だけで足りるのかという問題意識を持っている。現時点で具体的な案があるわけではなく、どうやればよいかという点も含め今後検討するという趣旨で御理解いただければと思う。

岡村構成員）※チャット
直接的な注意喚起における「一般的な周知広報等」が、ゼロデイ攻撃を招くものであると誤解されないよう、書きぶりを工夫いただきたい。

中尾構成員）
「エ.クラウドサービスにおけるサイバーセキュリティの確保」について、「セキュリティリスク『による影響』の小さい業務・情報を扱う」としてはどうか。また、ISMAP は現在、政府機関が利用するクラウドサービスの評価制度であるが、地方自治体にまで利用主体を広げていくメッセージが含まれると良いと思った。

廣瀬サイバーセキュリティ統括官室参事官補佐）
最初の御指摘についてはおっしゃる通りなので修正させていただく。一方、地方自治体については ISMAP の範疇を超えるため、政府機関と並列して記載するのは難しいかと思うが、検討すべき論点であることは間違いないので、検討させていただきたい。

前田氏（鵜飼構成員代理））
スマートシティのセキュリティについてはセキュリティ関係者のみで議論されていて、私自身が「スマートシティセキュリティガイドライン」第 2.0 版のレビューに参加した際に、都市 OS ベンダーや API 連携に関わる事業者の参画が少ない、参画していてもほとんど意見が出ないと感じた。セキュリティ関係者と規格設計・実装を行う人々が協働しないと新しい取組は進まないと思っており、この点についての言及があっても良いと思った。

廣瀬サイバーセキュリティ統括官室参事官補佐）
問題意識は共有しており、地方自治体や都市 OS ベンダー等の関係者ともよく意見交換をしながら、一層の普及啓発や必要な見直しを進めていきたい。

宇佐美構成員）
「キ.放送設備におけるサイバーセキュリティ対策」では、放送の可用性についても言及いただき、バランスの取れた記述になっているので、特に異存はない。

中尾構成員）
「ク.Beyond 5G・6G に向けたサイバーセキュリティの検討」について、例えば ITU-T のフォーカスグループが発出している文書「Network 2030」においては、インターネットに代わる次のネットワークを含む Beyond 5G に係る言及がされているところ、「今後の取組」に日本として Beyond 5G の議論にもっと積極的に関与・貢献していく方向性を明記した方が良い。

梅村サイバーセキュリティ統括官室参事官）
頂いたご指摘を踏まえて、検討してみたい。

Ⅱ２.サイバー攻撃への自律的な対処能力の向上

吉岡構成員）
フィッシングや Emotet 等が流行する原因に共通する要素としては、人間が騙されているという点があり、対策においては、ヒューマンファクターの理解の重要性が高まっていると感じる。例えば CYNEX の活動の中でもそのような観点の研究も行われていると認識しているが、本文の例えば 28 ページにおいて、そのことがより明確に記載されると良い。

梅村サイバーセキュリティ統括官室参事官）
吉岡構成員の御指摘について、「ア. 電気通信事業者による積極的サイバーセキュリティ対策の推進」において、フィッシングサイト等の悪性 Web サイトを検知する技術の実証や DMARC 等の導入実証といった、人間の判断をサポートする取組の記載は既にしている。

高村サイバーセキュリティ統括官室参事官）
追記を試みるが、全体の流れに上手くはまるか分からないので、書ききれない場合は御容赦いただければと思う。

園田構成員）※チャット
吉岡構成員の指摘に賛成する。「ユーザブルセキュリティに関する研究促進」のように表現すると良いかもしれない。

徳田構成員）
NOTICE においても注意喚起対象者の行動変容がいかに起こるかというヒューマンファクターのところを考えていかなければいけないと認識しており、吉岡構成員・園田構成員のコメントに賛成する。

宇佐美構成員）
フィッシングメールは、もはや人が注意能力を上げて気づくのは非常に難しい領域に来ている。被害組織が出す注意喚起の在り方も含め、様々な対策が考えられるかと思う。

中尾構成員）
「(大学と民間企業における研究開発の支援等)」の「今後の取組」の最終パラグラフについては、具体の施策の道行きに加え、「新たな研究開発事業の探索」のような中長期的な方向性を指し示す一文があった方が落ち着く気がした。

高村サイバーセキュリティ統括官室参事官）
探索的研究等を NICT で行っていただくのは歓迎する一方、NICT の新しい業務を書くとなると、中長期目標を変更しなければならないため、本案への追記については御容赦いただければと思う。本件は宿題として承る。

Ⅱ４.普及啓発の推進

藤本構成員）
本文書の注目度は高く、これを用いて勉強したいという学生も多くいる。「イ. 地域セキュリティコミュニティの強化」についてだが、イベントに参加された 1,400 人の属性を明記することにより、読んだ学生が「学生でも参加できるんだ」と知るなどして参加者のすそ野拡大につながるかと思う。また、先行的に若年層向けのイベントを行った旨の記載があったが、他にも戦略的に参加が期待されるところがあるのであれば、追記いただきたい。

廣瀬サイバーセキュリティ統括官室参事官補佐）
藤本構成員からの御指摘について、現状はセミナーやインシデント対応演習には企業の担当者や戦略マネジメント層に、CTF には高専生や高校生に参加いただいているが、引き続きそうした方々に幅広く参加いただきたいと思っているので、そのメッセージを追記する。

岡村構成員）
高専での人材育成には力を入れていただきたい。

若江構成員）
あくまで次回策定時に向けた提言としてだが、「地方自治体や教育委員会への普及啓発」という項目を設け、そこで学校におけるセキュリティ対策支援を位置づけられないか。「教育情報セキュリティポリシーに関するガイドライン」を参照し、各教育委員会が手探りでセキュリティ対策を行っている実態が取材からうかがえるところ、セキュリティに知見の蓄積がある総務省において支援できるとよい。

梅村サイバーセキュリティ統括官室参事官）
文科省は「教育情報セキュリティポリシーに関するガイドライン」を作成しており、GIGA スクールに係るセキュリティ確保については、基本的には文科省が主管で取り組むべきものと思う。。一方、学校教育における情報活用能力育成の重要性が 2020 年改定の学習指導要領でも大きく位置づけられ、力が入れられているが、こうした学校における情報教育に対し、情報通信分野等の企業・団体と総務省・文部科学省、マルチメディア振興センターが協力して、学校現場での無料出前講座を行うのが e-ネットキャラバンの取組である。こういったところで総務省が側面的に文科省の情報教育をサポートしていくことは重要と考える。

Ⅲ今後の進め方

中尾構成員）
最終パラグラフの文末が「望ましい」というのは弱いので、総務省の意思を表現した方がいいのではないか。

梅村サイバーセキュリティ統括官室参事官）
御指摘いただいた通り、ステークホルダー間での共有を踏まえた取組の強化については、より強く書いた方が良いことは理解した。例えば「図っていくべきである」のように修正する方向で考えたい。

その他

徳田構成員）
脚注でガイドライン等の URL が記載されているが、可能であれば、付録 3 として重要なガイドラインの一覧を URL でクリックできるような形にしておいていただけると、読み手が実際にそのガイドラインにアクセスしやすいし、（今後もアップデートを続ければ）どこが変わったのかも分かりやすい。

梅村サイバーセキュリティ統括官室参事官）
大変良いアイデアかと思う。どういう形で記載するかを含めて検討させていただきたい。

（3）閉会
◆巻口サイバーセキュリティ統括官より挨拶。

以上