ICT サイバーセキュリティ政策分科会（第 10 回）議事要旨

１．日　時）令和 6 年 6 月 24 日（月）14：00～16：00

２．場　所）WEB 開催

３．出席者）
【構成員】
後藤主査、新井構成員、上原構成員、栗原構成員、小山構成員、篠田構成員、蔦構成員、吉岡構成員、盛合構成員

【オブザーバー】
内閣官房内閣サイバーセキュリティセンター、内閣官房サイバー安全保障体制整備準備室、デジタル庁、経済産業省、地方公共団体情報システム機構

【総務省】
山内サイバーセキュリティ統括官、豊嶋大臣官房審議官（国際技術、サイバーセキュリティ担当）、小川サイバーセキュリティ統括官室参事官（統括担当）、酒井サイバーセキュリティ統括官室参事官（政策担当）、佐藤サイバーセキュリティ統括官室企画官、道方サイバーセキュリティ統括官室企画官、牧野サイバーセキュリティ統括官室統括補佐、井上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 10－１　「ICT サイバーセキュリティ政策の中期重点方針」（案）
資料 10－２　「ICT サイバーセキュリティ政策の中期重点方針」（案）の概要

5．議事概要
（１）開会

（２）議題
◆議題「ICT サイバーセキュリティ政策の中期重点方針」（案）」事務局より資料 10－１を説明。

◆構成員の意見・コメント

蔦構成員）

15 ページについて、経済安全保障推進法については今年改正法が成立し、基幹インフラ分野として港湾運送が追加されているはずである。施行はまだではあるが、脚注などで触れておいた方が良いのではないか。
21 ページについて、新 NOTICE の取組の重要性は言うまでもないが、新 NOTICE に加えて事前の対策として、IoT 機器のセキュリティ基準の在り方を不断に検討していくという記載がある。近時、セキュア・バイ・デザインやセキュア・バイ・デフォルトの重要性が高まってきており、シフトレフトという単語を聞く機会もだいぶ増えてきたため、その辺りを記述に加えたほうが良いのではないか。44 ページ脚注 40 に、AI セキュリティ情報発信ポータルのアドレスがあるが、民間企業のアドレスであり役所から出すドキュメントに説明なく出てくるのは違和感がある。委託事業だと思うが、総務省が行っていることが分かるようにしておく方が良いのではないか。読売新聞の報道で NISC が省庁独法の脆弱性を 24 時間体制でチェックするという記事が出ていた。機器の脆弱性をリアルタイムで監視するという観点は、新 NOTICE や CYXROSS の取組にも関連しているため、報道レベルだが記述を加える必要があるかどうか検討いただければ。

上原構成員）

18～19 ページについて、新 NOTICE の第一義的なターゲットは IoT ボットネットとなっているが、被害状況が大きく変化していく中で、ルータ脆弱性を突いた被害が増えていることも問題であるため、脆弱性をターゲットとする活動に関して、IoT ボットネットに限らない広範な活動となっていることを打ち出していくべきである。また、19 ページについて、IoT 機器メーカーや Sier 等との連携について、ここの協力なしには進まない事態となってきているので、強力に進めていただきたい。
24 ページのネットワークセキュリティ認証技術の導入促進について、DMARC、DNSSEC 等のネットワーク認証が進まないと、メールを起点としたフィッシングや標的型攻撃は減少しない。単に DMARC の導入や DNS の強化だけではなく、更に一歩進んで、その結果をうまくユーザーに見せる、管理者へ可視化の推進を行うなどを行うべき。例えば DMARC を導入するのであれば、そのポリシーについて少しずつレベルを引き上げていくという活動とセットになるべきであろうと考えており、ガイドラインを策定する中でより強力に推進していくことが

重要である。
29 ページについて、自治体に関しての今後の取組の方向性に「セキュリティポリシーガイドラインに基づくセキュリティ対策を着実に推進する」とあるが、自治体のセキュリティがうまく機能していない主な原因は、どうしても業者任せとなっており、依然として LG.JP への移行が進まず、変なドメイン名を使用している関係で偽サイトなどに使用される被害が発生しており、根本的な解決がいつまでも進まないといったことが起きているため、現在の状況でポリシーに書かれていることを確実にどうかの再確認を進めることも重要であると考える。

小山構成員）

52 ページの「国家安全保障戦略等」の「等」に現在動き出した ACD に関する有識者会議のアウトプットも含まれてくるのかどうかについて、これらを加味した動きとする方が良いと考える。可能であれば有識者会議で議論されている内容を踏まえて、この中期重点方針の見直しや新たな取組の追加等を行なった方が来年度以降の具体的な政策に繋げられるのではないか。

吉岡構成員）コメント

20 ページの IoT ボットネットの脅威について効果的な対応が必要である。IoT 機器の脆弱性以外の問題も発生しており、今後も表出する可能性があるため、NOTICE で得られた知見は、非常に高度な分析情報の提供となり、より幅広い分野で活用できると考える。例えば、ランサムウェア攻撃についても VPN 経由が多く、また、現在アタックサーフェイスマネージメントが重要視されている中、様々な組織等の防御という観点でも役に立つということが記載されており問題ないが、その一方で、それぞれの対策は関係者の多大な努力で成り立っているため、実際に活動を行う場合には相当なリソースが必要である。

佐藤企画官）

蔦構成員への回答。
改正経済安全保障推進法について、ご指摘の通り脚注で記述できるように工夫したい。
IoT セキュリティ基準の在り方について、ご指摘の通りセキュア・バイ・デザインやセキュア・バイ・デフォルトが重要であることは事実であるため、この文章の中に入れていけるように記載を工夫したいと考えている。
AI 関係のポータルサイトについて、ご指摘の通り委託事業で行ったものであり、委託先事業者のドメインであるため、総務省とのコラボレーションプロジェクトであることがわかるように記載したい。
NISC による国・独法のサイバー攻撃の 24 時間体制チェックについて、現時点では具体的な中身が検討されている段階であると認識をしている。その上で一般論として、NICT の取組が貢献できる部分は非常に大きいと考えている。ご指摘のような動きも踏まえながら、貢献できるところについてはしっかり貢献していきたいと考えている。

上原構成員への回答。
新 NOTICE について、ご指摘のとおり、ターゲットは IoT ボットネットであるが、NOTICE で見つかった脆弱性については、DDoS 攻撃に限らず様々な攻撃に利用される可能性があるため、こうした観点から、不正侵入等の脆弱性については、同じ脆弱性であっても様々な攻撃に使用されるということを念頭に置きながら取組を進めていきたい。多様な関係者との連携について、注意喚起のみによらない対処を進めなければならないというところは我々も認識しており、実際に NOTICE プロジェクトの下に会議体を新たに設けて、るメーカーと連携して対策を進めようとしており、この取組を更に拡大していきたい。
ネットワーク認証技術について、ご指摘のとおり、導入率を上げるためには単なる普及啓発だけではなく、ISP をはじめとするそれぞれの企業の対策状況の可視化を進めていくことも必要と考えており、こうした観点を意識して記載している。地方公共団体におけるドメインの問題について、LG.JP が進まない点に関しては、今後ご指摘を踏まえて、関係部局と連携をしながら、対策を検討していく。

小山構成員への回答。
ACD に関する有識者会議は現在議論をしているところであり、具体的なことはまだ何も決まっていないため現時点での記載は難しいという状況であるが、「おわりに」の意図としては、これから出てくるであろう政府の方針を踏まえて取組を進めていくことを踏まえた形で記載をしている。従って、新たな方針が出た際は、必要に応じて中期重点方針を見直していく、もしくは更に充実させていく対応を考えている。

吉岡構成員へのコメント。
新 NOTICE によって得られた知見・ノウハウを活用して、幅広くセキュリティ対策に活用していく点はご指摘のとおりであり、そういった内容を含めて記載している。一方、リソースが必要という点については、41 ページの NICT の研究開発等の取組や事業推進体制の強化を行っていくという観点から記載している。取組を広げていくためには、それに対応したリソースが必要ということはご指摘のとおりであるので、そういった点にも対応していく。

後藤主査）

26 ページのサプライチェーンの課題について、セキュア・バイ・デフォルトは非常に広い概念であるため、SBOM のような最初の設計段階から実施するものと関連させて加筆するとほうが良いと考える。
29 ページの自治体の今後の取組について、ISMAP は非常に重要であるが、現状の ISMAP は自治体が使用したい便利なサービス、特に SaaS 系のサービスにはなかなかフィットしないところがある。ISMAP の在り方について、LIU 登録の増加に加えて、複数の自治体が便利に安心して使える SaaS サービスを増やしていくといった取組が重要であると考えるため、この辺りもご検討いただきたい。

盛合構成員）

13 ページの脚注 14 で引用されている参照文献は相当古いものであるため、修正いただきたい。また、内容に対しての参考文献とするのは適切ではないため、もう少し新しい、例えば CRYPTREC 暗号技術ガイドライン（耐量子計算機暗号）などから引用するほうが良いのではないかと考える。
また、11 ページの脚注 12 について、閉じ括弧が脱字となっている。

佐藤企画官）

後藤主査への回答。
セキュア・バイ・デフォルトについて、SBOM との連携についてはご指摘のとおりであり、取りまとめ案への反映を検討したい。
ISMAP と自治体について、現在総務省では関係省庁と連携をしながら、ご指摘のような制度改善に取り組んでいる。その中で、自治体の視点に立った ISMAP－LIU の取組を進めることにより、自治体が安心してクラウドサービスを利用できる環境整備を進めることが非常に重要であると考えている。そういった点も分かる形で記載をさせていただく。
盛合構成員への回答。ご指摘の脚注と脱字についてはしっかりと修正したい。

新井構成員）

本分科会の目的は、2030 年までに総務省が取り組むべきサイバーセキュリティ施策を考えていくことであるが、6 年というスパンで見ると、生成 AI の変化速度は非常に早く、その時々のスナップショットを拾っていかなければならないと考えている。従って、動向等の随時把握や進展の早いものに対してもキャッチアップしていくという趣旨の内容も盛り込んでいただきたい。

佐藤企画官）

AI については、ご指摘のとおり、変化の早い動きを継続的に把握することについては、我々も同じような認識であるが、この点については取りまとめ案にもう少し明確に記載ができないかを検討する。

後藤主査）

CYNEX・CYCROSS・NOTICE など、一次データを自ら収集し、そのデータに基づき分析を行い、新しい技術へという流れを作っていくことは、サイバーセキュリティにとっては必須であると考えている。これらが着実に出来てきており、今後も強化をしていくというメッセージは非常に良い。同時に偽・誤情報のように別の観点でも議論になっているトピックや、AI に関してもサイバーセキュリティ分野のみでなく別の観点でも議論になっていることがある。そういった他の取組に対しても、複合的な検討・分析が必要であり、NICT 等で集めたデータはこれらの様々な観点で使用・活用ができる領域が多いと考えるので、積極的・主体性に連携を行い、新たな分野にも拡充し、課題の解決に活用していくことを最後の方で強調されているとより良いのではないか。

栗原構成員）

放送に関しては記載のとおりに行っていくしかないと考える。CYDER や地域 SECUNITY 等への支援策について、今後、特に地方局等でそういった政策を打っていただけると大変助かるのではないか

篠田構成員）

国際連携に関しては過不足なく記載されている。

佐藤企画官）

後藤主査への回答。

データを収集し、様々な課題の解決に活用していくことは、まさにご指摘のとおりであるため、書きぶりについてご相談させていただきたい。
栗原構成員への回答。
特にローカル局での人材育成と普及啓発の支援策について、関係団体や事業者の方と連携をしながら取り組みを進めたいと考えている。

◆山内サイバーセキュリティ統括官より挨拶

(3)閉会

以上