サイバーセキュリティタスクフォース
情報通信ネットワークにおけるサイバーセキュリティ対策分科会（第５回）議事要旨

1. 日 時）令和５年５月18日（木）10：00～12：00

2. 場 所）WEB開催

3. 出席者）

【構成員】
後藤主査、井上構成員、河村構成員、小塚構成員、小山構成員、齋藤構成員、田中構成員、辻構成員、藤本構成員、吉岡構成員

【総務省】
山内サイバーセキュリティ統括官、内藤官房審議官（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（総括担当）、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、廣瀬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. 配付資料
資料５－１　NOTICEステアリングコミッティの設置について
資料５－２　これまでの論点整理等に対する主なご意見
資料５－３　分科会取りまとめ骨子（案）－総合的なIoTボットネット対策の実現に向けて－
参考資料　　情報通信ネットワークにおけるサイバーセキュリティ対策分科会第４回　議事要旨

5. 議事概要
（1）開会

（2）説明
◆議題（１）「NOTICEステアリングコミッティの設置について」について、事務局より資料５－１、議題（２）「取りまとめ骨子（案）について」について、事務局より資料５－2、資料５－3を説明。

◆構成員の意見・コメント
後藤主査）

資料５－３の２ページ目（1）タイトルにある「必要不可欠」の文言について、必要不可欠、すなわち情報通信ネットワークへの依存性が毎年高まる一方であると認識している。この点本文では強調いただきたい。

齋藤構成員）

前回会合でも言及したが、メーカーにおける施策、通信事業者における施策、NOTICEとしての施策それぞれが重要であり、これらの施策を改善し全体としてどのような方向性となるのかを、本文の前段で表現した方が良い。様々な主体が関係している例であれば、マイクロソフトにおけるパソコンのOSの安全性向上や、スマートフォンのオンラインアップデート、加えてクラウドのSaaS事業などにおいてオンラインサービス提供者側が実装における脆弱性の責任をもつといった責任分界点の明確化等の取組がある。IoTに関しても色々な主体が関係して

いるところもあり、どういう方向へ向かうのかをいま挙げた成功事例などを見据えて前段で議論すべき。

後藤主査）

つまり２ページ「(2) 情報通信ネットワークの機能に支障を及ぼし得るサイバー攻撃の現状」には、現状についての記載だけではなく、冒頭に端末やネットワークの在り方を示した上で、これまでにあった取組を示し、IoTの世界でも同様に行うべきということか。

齋藤構成員）

各施策が今後成功するかの見通しを立てるためにも、過去の成功事例について記載をした方が良いかと思う。

後藤主査）

非常に良いご意見だと思って私も賛同である。どう書くかということについては事務局の方も含めてあると思うので、この辺りは最後また改めて議論したい。

辻構成員）

資料５－２に関し、NOTICE の調査範囲について ID・パスワードの設定不備以外の脆弱性もチェックすべきという意見はごもっともだと思う。NOTICE 調査対象のポート範囲は 30 いくつかかと思うが、そこを拡大・拡充していくことで、ネットワーク機器だけに関わらず、外部に公開すべきではないポートが見つけられると思う。公開していたとしてもアクセス元を制限した方が良い、いわゆる管理ポートと言われるようなものである。開いているポートに認証をすることや脆弱性の有無を確認することだけではなく、そもそも外部に公開すべきではないポートについて、それが管理ポートであると NOTICE の取組において実際にアクセスして分かると思うので、そういったものに注意喚起すべきではないか。NOTICE で広く認証や脆弱性対策を行う前にそもそもアクセス制限をきちんとしていれば予防措置として攻撃されないというところに立ち返り、外向きに開いている管理ポートの現状や脅威に気づいていただくためにも、こういった点を注意喚起していくことも視野に入れると良いのではないか。また、C&C サーバ検知に関して、国内で見つかった C&C サーバにどう対処していくか、協力してもらうなども考えるべき。過去に、国家背景と思われる攻撃により沢山の C&C サーバが国内の特定クラウド事業者に偏った事例があるが、攻撃を停止してもらうことができなかったのか、結果的に被害拡大を抑えることができなかった失敗事例もあるので、同じことを繰り返さないよう、C&C サーバ検知後の、対処可能範囲における取組も検討すべき。最後に、今後ノウハウの共有によって C&C サーバ等を検知できる ISP が増えた後になると思うが、C&C サーバの検知に関し得られた情報は ISP や総務省の範囲内だけではなく、他省庁への共有も検討すべきではないか。法的な問題などもあるかと思うが、昨今各省庁が共有・公開というキーワードを打ち出してきていることもあり、情報を共有してもらうだけではなく情報をハンドルする側でも共有を促進させることで、民間から提供される情報だけではなく、総務省側で持っている情報も広く共有し相互に対応能力を上げることも検討すべきではないか。

後藤主査）

資料 5-2 について、意見を追加してクリアにしていただけたが、今おっしゃった中身はその後の本編にそのまま影響しそうなところなので、またその所でも議論したい。

田中構成員）

10 ページ目の一番下の段落の端末設備の接続に関するガイドラインの部分について、取組は非常に良いと思っ

ているが、感染機器の利用者はある意味で被害者でもあり、接続拒否についてしっかり理解を得られるようガイドラインの中で具現化していく必要がある。そのために広く関係者、ステークホルダーから意見をいただきながら丁寧に議論をして、こうしたガイドラインをまとめていくことが必要かと思う。

後藤主査）

関係するところとして、ガイドラインの対象読者には誰を想定するか。

田中構成員）

端末設備の接続に関するガイドラインとあり、ISP 側が接続拒否できる具体的な要件や手続きの妥当性を示すものとなっているので、ISP 側に示されるガイドラインと認識している。

後藤主査）

その場合は、ISP から見た場合の対象は個人ユーザーか企業ユーザーのいずれであるか。

田中構成員）

両方が含まれるのではないかと理解した。

佐藤企画官）

当該ガイドラインの策定については、接続拒否の制度は慎重に運用すべきであること、実際に接続拒否するかどうかはあくまで ISP の判断に委ねられることの２つの原則を守りながら、丁寧に関係者のご意見を伺いながら引き続き検討していきたい。その際に併せて一般利用者、法人利用者の両方から十分に理解をいただけるように、また、前回の会合で吉岡先生からもご指摘いただいたが、ガイドラインの策定だけではなく制度自体の周知啓発も必要であるので併せて取り組んで行きたい。

小塚構成員）

約款に関するガイドラインは非常に重要だと思う。法律の観点から言うと、約款は一方的に定められる契約であるところ、約款に対する規制がだんだん強くなるとその内容が不当なものである場合には端的に言えば一部無効ということもあり得るという考え方が強くなってきているため、どういった状況であれば接続拒否をしても不当と言われないかの指針を示す点に非常に意味がある。後藤主査が言及していたとおり、対消費者契約と対事業者契約ではこの点規制の強さが違うため、消費者契約の場合は消費者契約法という法律に照らした問題になり、事業者契約の場合には民法の中の定型約款という規定に照らした問題になるという違いが発生する。その点もを踏まえながらこのガイドラインを策定する必要があるかと感じた。資料５－３分科会取りまとめ構成（案）についての感想だが、「２．端末側に対する対策（NOTICE)」という見出しについて、端末側の対策＝NOTICE の運営の在り方と読めてしまうがそれでいいのだろうかと問題意識を持っている。今回取りまとめの趣旨は NOTICE というものを単なる利用者への脆弱性の通知よりも、広く端末側に関する対策の在り方と位置付け、もっと踏み込んだ対策を実施していくということだと理解しておりそれは良い方向だと思うため、その点ははっきりと明確に出た方が良いかと思う。取りまとめを本文に起こすのであればそのあたり分かるようにした方が良いかというように感じた。また、質問があり、現在は脆弱な端末としてルーターが主に挙げられているが、これから IoT 機器が増えると言われている中で、例えば自動車がコネクティッド・カーのようになっていくと、消費者の身近なところに大きな IoT 端末ができることにもなるわけだが、そういったものも同じような危険性を持つのか、それともルーターやカメラといった端末が主として問題なのか。場合によっては近未来に対する見通についても報告

に記載しても良いかと思う。

後藤主査）

NOTICE の取組だけの議論ではないという趣旨が非常に大事なポイントである。現状について齋藤構成員からも言及があったように、本来何を目指しているかを明らかにして、それに向かっての取組として NOTICE の中で上手く対応していく意図かと思うので記載は是非工夫していくべき。小塚構成員のご質問については、私から仮に申し上げると、自動車メーカーがしっかり作っていると期待できる一方で、将来的にホームルーターのようにネットワークに接続されるものをユーザー自らが車に接続してしまうということが全くないわけではないため、その意味では同じようなリスクが広まっていく可能性は十分にあると思う。ただあまり自動車とホームルーターは一緒に議論するレベルではないと思われるので、ご専門の方や事務局の意見等、また別途で伺いたいと思う。

小山構成員）

資料５－１と資料５－３の NOTICE について関係者へのお願いと質問がある。資料５－１のように NOTICE のステアリングコッミティを設置し資料５－３の 11 ページに書かれているような今後の取組を推進していくかと思うが、NOTICE の活動自体が従前からの注意喚起に頼った対策から脱却することが必要かと考えており、そのためにはメーカーや SIer の方々との連携が重要である。全体的にバランスの良い取組を推進するため、過去の注意喚起から脱却するための取組と理解しており、注意喚起が活動の中心にならないように関係者の皆様にご留意いただきたい。その上での質問だが、同 11 ページではメーカーや SIer との連携が重要とあるが、これらのプレイヤーの中で IoT 機器メーカーや SIer を NOTICE の取組に巻き込んでいくミッションを担っていくのは誰を想定しているのかというところが知りたい。私も NTT コミュニケーションズの立場と ICT-ISAC の立場の両面でを活動をしているが、過去 NOTICE の取組あるいは ICT-ISAC の取組では IoT 機器メーカーや SIer を巻き込むことができず、力任せに注意喚起をし続けてきた結果、注意喚起疲れのようなことが起きているので、そこにメーカーを巻き込む、SIer を巻き込むことをミッションとして是非しっかり設けていただきたく、その点どのように考えているのかについて質問したい。

酒井参事官）

メーカーや SIer を巻き込んでいく点について小山構成員のご認識のところは私も同様に考えており、現状のメーカーとの接点については、ネットワーク機器の業界団体である DLPA と定期的な会合をもって状況の共有をしているケースや、NICT が個別調査の中で見つけた脆弱性について個別メーカーと連絡を取り、ある種脆弱性ハンドリングの作業のような形を取っているケース、あるいは経済産業省で行われている IoT 機器のセキュリティ認証基準策定業務の担当部門と総務省とが連携して、IoT 機器を製造している、あるいは利用している業界団体の方との接点を持つケース等色々な形がある。NOTICE もこれまでの調査で脆弱であると検知した機器のうち機種特定できたものは一定のメーカーに偏る傾向があるので、今後 ICT-ISAC、NICT、総務省がどのようにして主要なメーカー等とのコミュニケーションをとるかということは一つポイントになってくるだろう。現時点ではすぐ取り組むべきタスクが明確ではないが、述べたような問題意識の中で誰がどのように取り組むのかということも含め、このステアリングコッミティの中で議論していきたい。ユーザー機器については DLPA のようなまとまった業界団体があるが、法人ルーターに関してはかなりバラバラで業界団体というものがあるわけではないようなので、ここへのアプローチはお知恵をいただきながら引き続き議論したい。

河村構成員）

資料５－３の 10 ページの「②利用者への注意喚起の実効性向上」一つ目のポツだが、最後に「安全な機器やサ

ービスを選ぶといった利用者に求められる役割」と記載があり、もちろんそのとおりだと思うが、どう選べば良いのか、どうしてそれを選ばなければいけないのか等、利用者が安全なものを選ぶことができるための情報が豊富にあることが大前提となり非常に重要である。もう一点、今回の資料ではメーカーという言葉だけ出てくるが、以前の議論でベンダーという言葉に言及があったように、例えばルーターやネットワークカメラはほとんどインターネットで買っている利用者が多いと思われるところ、そういった場合に、デジタルプラットフォームを運営している事業者やネットショッピングの場を提供している事業者、あるいは電気製品の量販店などもステークホルダーに含めるべきではないか。機器の売場や購入ページに、何らかのセキュリティ対策をしている機器であること、あるいはセキュリティ対策をしている機器を選ばないと社会に弊害があるというようなことを認識して初めて利用者は正しいものを選ばなければとなるので、製品そのものへの表示だけではなく、売場や Web サイトへの表示も考えていくことが遥かに効果的かと思うため、ステークホルダーの中にそういった事業者も含めた方が良い。その際に、ネットワークカメラは攻撃するためのボットネットのために侵入されるのだろうが、理屈で言うと侵入されることによりプライバシーの侵害が起こりうるかもしれない。そのようなことをわざわざしているのかは分からないが、そういった点を強調して、侵入されうることを自分事として考えさせ、利用者が安かろう悪かろうの製品を購入しないようにすべき。加えてもう一点、懸案となっている資料５－３の６ページ四つ目のポツの接続拒否について、例えば銀行 ATM の暗証番号の変更を喚起される等は、基本的にパスワードなどの脆弱性は自分が被害にあわないためにという理屈から言われていて、それに応じないということはある程度自己責任になるわけで認識しやすいが、他方でパスワードに脆弱性があることが社会に悪影響をもたらすからという理屈については認識していないと思うので、これからはサービスやモノを買うときに脆弱なパスワードが社会に影響をもたらすという認識を持たせる機会を設け、消費者がその理屈を理解した上での接続拒否ということかと思う。あとは接続拒否の条件として、累次にわたって注意喚起に応じない場合とあったが、そういうときは注意喚起に応じていないのではなくて、注意喚起自体を読んでいないなど、全く届いてない場合もある気がするので、そういった点も検討しながら接続拒否に関しては十分な慎重性をもって検討していただきたい。

藤本構成員）

NOTICE 注意喚起については資料５－３の 9 ページ等色々なところに出てくるが、注意喚起を実際に届けるためにはホームページの役割は結構大きくなってくるかと思う。注意喚起の認知度が上がって、何か対応しなければと思った時にアクセスするのはホームページかと思われるところ、資料５－１にあるように NOTICE サポートセンターがホームページの運用等の広報を担当されるとのこと、特に記載の変更をお願いするものではないが、今後広報におけるホームページの拡充というのが非常に重要になってくるかと思うので対応いただきたい。

酒井参事官）

藤本構成員ご指摘の広報について我々も非常に重要だと考えており、現在ステアリングコッミティの中で、訴求対象ごとにどういうことを伝えれば良いのかのポイントを整理していくような広報戦略の検討に着手している。具体的には、河村構成員からご指摘があったように、一般ユーザーに脆弱な機器が公衆のネットワークにも被害を及ぼし得るということや、特に中小企業のユーザにネットワーク機器を設置した場合には外的な脅威の変化に応じて継続的なセキュリティ対策が必要であると理解していただくことが必要。またメーカーに対しては機器の運用を開始する際にどういったところに気を付けて初期設定をすべきか、外部に提供すべきサービスやそうでないサービスにどういったものがあるかといったインストラクションを付けられないかということや、あるいは SIer に対し事業者からシステム構築の依頼があった場合に、仮に仕様書の中にネットワーク機器の保守項目が含まれていない場合には、そういった項目を逆に提案していただくことなども考えられる。ルーター設置に関わる方、消費者、設置業者、管理者といった方それぞれに注意喚起を出すチャンスがあると思われるため、それぞれの方に対しルーター設置の際に伝えていただきたい注意点を記載した簡単なフライヤーのようなものを作る事ができれば、各々の立場で問題の所在や具体的な対処法についてご認識いただくことが強化できるのではないか。

これまでの取組で管理の甘い危険なルーターの利用実態や、危険な運用形態になっている原因が分かりはじめているところなので、その辺りを踏まえて訴求対象別の広報戦略をこれから年度末に向けて検討していきたい。

佐藤企画官）

続いて河村構成員のご意見について、利用者に安全な製品を選んでいただくためには、十分な情報があることが前提であることはご指摘のとおりと思うので、そういった点も分かるようにとりまとめに盛り込んでいきたいと考えている。また販売店、いわゆる流通業者についても当然ステークホルダーに含まれると思うためしっかり連携できるようにしていきたい。さらに注意喚起については自らの機器が踏み台となることだけではなく、例えばパスワードの甘い機器から情報が盗み取られプライバシーの侵害になり得るかもしれない等、利用者が自分事のように捉えていただけるような注意喚起に工夫して取り組んでいきたい。接続拒否についてはご指摘のとおり極めて慎重に運用すべきであると考えており、そのための条件として、注意喚起がしっかり届いていることが前提であると思うので、そういった前提も含めどういった場合に接続拒否ができ得るのかを慎重に検討していきたい。

井上構成員）

NICT で調査を実施している側からのコメントだが、辻構成員からも言及があった、新しい脆弱性や開いてはいけないポート番号の調査を行って広報していく取組は非常に重要だと思っている。それを実施するにあたっては、現状の NOTICE では調査対象のポート番号を追加したり、特に ID とパスワードの追加だったり、そういった特定アクセス行為に関する部分に関しては実施計画の改訂をしなければならないが、総務大臣認可を得るプロセスにおいて数か月ほどかかることもある。そのため、危険なポート番号が判明しても即時対応できる形には制度上なっていないという課題があるので、そういう意味では、この調査の柔軟性や機動性を確保する仕組みが必要であると思う。メディア対応については、2019 年の NOTICE 開始時にメディアで取り上げられた際に炎上したこともあり、かなり慎重な実施に舵を切ったという経緯がある。次期 NOTICE を検討するにあたっては、こういった分科会の形で検討したり検討資料も公開されていたりと、高い透明性をもって検討を進めていると理解している。NOTICE 開始時は NICT 法の改正をした後に調査を実際に行うタイミングで報道が始まったため、そのときの反省を踏まえ、もう少し前からこういった NICT 法の検討を行っていることについて、メディアとコミュニケーションを取りながら十分な情報展開及び広報活動をしていく必要がある。最後に、人員確保について NICT からのコメントも様々記載していただいている。この NOTICE の活動の検討段階から NICT に通信事業者や機器ベンダー等の企業から人員を投入していただき、一緒になって調査システムを作っていただいたり、通信事業者との情報連携を行っていただいたりし、その結果プロジェクト全体の意思疎通が図れたため心より感謝している。NOTICE は継続していく方向性になっているところ、次の NOTICE のプロジェクトにおいてもそういった人員の協力やリエゾン的な部分については協力をお願いしたい。

吉岡構成員）

私が am I infected?等の活動をして感じていることは、どういった状況になった際に注意喚起対象とするかのラインを引くかが難しいという点である。NOTICE の場合は Telnet でログインできる場合や、マルウェアに感染していると NICTER 観測結果で分かった場合などのケースになると思う。am I infected?で観測していると、設定不備のある可能性があるなど、例えば何か機器の管理画面が外から見えていると確認はできるが、意図的なのかそうでないのか微妙であるグレーなケースがかなり多く、am I infected?はそういうものを含めた検査依頼を受けてするものであるため少し幅広く注意喚起やお知らせが出来る。こういうものが見えているが大丈夫かと少し幅広に確認することができても、依頼を受けて検査するものではない場合に、どこまで踏み込んで注意喚起をするかのラインの決め方は難しいとは思うが、外から見て問題があるのを確認できるケースばかりではないと認識しているので、今後はその辺りも技術的に考えていかなければならない。また、エンドユーザーに様々な注意

喚起をしても効果がはっきり見えず○○疲れとなっているというご指摘については、本当にそのとおりだと思っており、対処療法的なアプローチは、やはり効果も見えにくくてそういった状況にもなる。一方で攻撃の発生原因を追究する方針で、攻撃が起こる前に状況を把握することや事前に通知が出来ると良いと思うが、実際の脆弱性の多くは個々の機器の脆弱性にとどまらず、根本原因が機器のハードウェアやチップなどの、ベンダーが出しているBSPと呼ばれるボードサポートパッケージといったものやSDK、オープンソースソフトウェアに起因している場合も多くある。その場合はNOTICEでは本来起こり得る脅威の氷山の一角しか見ていないという状況に過ぎず、そのまま終わってしまうのが非常にもったいない。個々の機器以外の脆弱性についてもしっかりと分析し、根本的にはどれくらい大きな問題でどれくらいの製品に影響があり得る問題であるかを調べると凄く底が深いところもあると思うが、そういった調査ができるとそのような状況を世界的に発信できるなど、日本の活動として注意喚起の価値が凄く高くなると思う。

辻構成員）

公的な問題などもあると思うのだが、こちら側の情報共有をしないと、もらってばかりというのもどうかと思うし、省庁間の情報共有にも課題があると私は強く思っているので、その辺りもこういったの取組をきっかけに考えていただきたい。（以下チャット欄より抜粋）「○○疲れ」は難しいところで情報共有疲れもあるが、これまでのNOTICEではISP側への負担もあったので、どちらも加味しバランスを取りつつ双方からアプローチする必要がある。またWebサイトの拡充は大切で、コンテンツとしての充実も根幹であり大切だが、様々な方々に関心を持ってもらうためのリーチの手法も大切。美味しいお店でも店構えが悪い場合や、知られなければ食べようと思ってもらえないのと同様に、Web サイトの拡充の際には多くの人に知ってもらうためのバズりを目指せるといい。

小山構成員）

資料5－3の13ページ四ポツ目の最後の部分について、ISP3社がフロー分析をした結果を比較しているが、グラフマイニング及び機械学習といったC&Cサーバの調査手法に基づく違いが確認された。従来からマルウェア感染事案においても、ISP毎のIPアドレスレンジによる違いがあることが知られていた。今回のフロー分析においてもISP毎に分析結果に違いが出ることを再度確認できたと理解している。今回このように正当業務行為としてC&Cサーバを検知するところまでは法的整理の上認められているが、どのように得られた情報を共有していけば良いかは課題であり整理すべき事項として検討を行っている。仮に検知したC&Cサーバの情報共有が許された場合も、C&CサーバのIPアドレスを1個もらってアクションにつながるわけではないので、このC&Cサーバ調査プロジェクトの営みと今後行われるNOTICEステアリングコッミティを中心とした取組が上手くすり合っていくように、情報共有をどのように進めるかをこれから私自身検討していきたい。

田中構成員）

同資料15ページのIoTボットネットの全体像の可視化については、これまでの会合でも議論されているとおり、非常に大事な取組で強く賛同する。とはいえ可視化は一つの手段であって目的ではないので、資料では可視化を進めることで最終的にボットネットの縮小などに取り組むというところまで記載を進めて良いのではないか。

佐藤企画官）

小山構成員のご指摘のとおりであり、例えばC&Cサーバは居場所がすぐに変わるので、効果的な情報共有の在り方や迅速に共有できる枠組み、どういった情報を共有すべきかなど色々課題があり、ICT-ISACでも検討しているところであり総務省としても議論に参画して、しっかりと効果的な対策につなげられるように取り組んでまいりたい。また田中構成員の可視化は手段であるというご指摘もそのとおりであり、可視化した後に、その先の

対策に繋げていくことが重要である。ただその対策もどういったアクションを取っていくかは今後議論をしなければならない点が多くあるので、しっかりと対策に繋げて IoT ボットネットの縮小することも含めて読めるようとりまとめに記載したい。

後藤主査）

情報共有の重要性と課題については皆さん理解しているが、例えば専門家同士、ISP 同士、ISP とメーカー間での情報共有などがある中で、データのオープン化のように広く周知すると広報にもつながるかもしれないが、他方で機微な情報も含んでいると非常に難しい部分もあり課題も多いと思う。海外との共有になるとさらに難しいところもあると思うが、課題意識として情報の共有の仕方や中身をどう考えていくかに関して何か意見はあるか。

小塚構成員）

後藤主査がおっしゃっていた国際的な情報共有については私もその問題意識をもっていた。C&C サーバのプレゼンでも主にそういったサーバは海外で発見されているという話もあり、そうすると取得した情報を国際的にも共有した上でさらに連携ということがその先にあるかと思うところ、検知の仕方などの技術あるいは取得する情報自体も始めから海外の取組とある程度同じようにしていく必要もあるのではないかと感じた。

吉岡構成員）

運用者、システム構築者に対する情報発信が重要である点、強く同意する。小塚構成員の指摘に関連して、海外でも同様の観測をしていることがあると思うが、逆の観点でそういったデータを取り込み活用する可能性はあるのか。ハニーポットも海外に多くあり、攻撃スキャンについても有名な Shodan や Censys などの活用はあるか質問したい。

佐藤企画官）

現在でも C&C のサーバの検知にあたっては様々な情報と組み合わせて総合的に分析しつつ精度を高めていく取り組みを行っている。その中で吉岡先生からご指摘をいただいた海外情報の活用も行っているが、今後更に取り組む必要があると思う。小塚先生からご指摘いただいた海外との連携については、まずは国内においてしっかり分析して C&C サーバを見つけていく取組を確立していく必要があるかと思う。海外との連携もその先の課題かとは思うが非常に重要な視点であり、既に見つかっている C&C サーバと思われるものも海外にあることが多いことも分かっているため、そういったところも念頭に置きながらどういった連携があり得るのか、C&C サーバの利活用の在り方とも関連する論点なのでしっかり検討を進めていきたい。

後藤主査）

すぐではなくても将来を見越して今から情報共有フォーマット等準備しておくのは大事かと思った。それでは全体を振り返って、先ほど最初に齋藤構成員の話もあった、そもそものこれら取組の狙いをどう書き込んでいくかも含め全体として意見等はあるか。先述のマイクロソフト社の件は苦労した歴史かもしれないが、過去の関連する成功事例と上手く対応させていくことで、この取組でもしっかり将来の成果が期待できることが主張できればということだと思う。

佐藤企画官）

齋藤構成員からいただいたご意見は非常に重要なご指摘である。資料５－３の３ページ目三ポツの部分に、IoT 機器に、開発・製造といった段階で適切なセキュリティ対策が講じられることが望ましいことを記載しているが、

その部分にご指摘をいただいたマイクロソフトやクラウドのような事例を記載しつつ、望ましい形を工夫して書かせていただきたいと考えている。

齋藤構成員）

今言及いただいた方向性のあとに、10 ページのユーザーが安全な機器やサービスを選択することが必要であるという部分については、これに追加して、現状の注意喚起に対してやはりアクションをきちんと取っていただくということで対策の精度を上げていくためにご協力いただけるように、他の販売店や SIer 等の役割や利用者側の役割等、期待する役割などの項目でくくって、他のステークホルダーに関しても期待する対応を記載するのはどうか。

辻構成員）

（以下チャット欄より抜粋）ダメな状態を指摘するときは、脆弱性だけでなく、何が危ないのか、どういった不利益があるのか、どういった対応が必要かもセオリーとしてセットで伝えることで、ユーザーへの動機付けを強めることも大切。

田中構成員）

色々な議論をまとめていただきまとまりが出てきたと思うが、端末とネットワークの対策と、先ほど申し上げたような IoT ボットネット可視化により最終的にボットネット縮小を目指していくといった全体像を絵のような形で示していただいた方が、本施策全体に対する関係者の理解も深まるかと思っている。現状、文字のみの報告書案となっているので、次回以降、その部分などを構成に追加するとより読みやすいかと感じた。

（3）閉会

以上