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４回）議事要旨

1. 日 時）令和５年４月21日（金）13：00～15：00

2. 場 所）総務省会議室及びWEB併用のハイブリッド開催

3. 出席者）

【構成員】
後藤主査、笠間氏（井上構成員代理）、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

【オブザーバ】
内閣サイバーセキュリティセンター、経済産業省

【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

【発表者】
大村優（NTTコミュニケーションズ株式会社）

4. 配付資料

資料４－１　電気通信事業者によるサイバー攻撃への効果的な対処を通じた安心・安全な情報通信ネットワークの実現に向けて（NTTコミュニケーションズ）
資料４－２　伝えるかたち 伝わるかたち～注意喚起について思うこと～（辻構成員）（非公開資料）
資料４－３　諸外国におけるサイバーセキュリティ対策の取組事例
資料４－４　これまでの論点整理（案）
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３回　議事要旨

5. 議事概要
（1）開会

（2）説明
◆議題（１）「フロー情報分析によるC&Cサーバ検知に関する調査の報告」について、NTTコミュニケーションズ大村氏より資料４－１を説明。

◆構成員の意見・コメント
小山構成員）
資料４－１の９ページにおいてMiraiやEmotetのC&Cサーバが検知できていることが分かり、今後の成果が

期待される。一方で 10 ページでは各社が検知した共通の C&C サーバが少ない点については、過去のマルウェア感染状況を見ても他 ISP とはそれが一致しないことは共通の理解であり、調査対象や調査期間が異なる事が原因だと思われる。今後分析手法等の共有をしていく上では、精度向上及びノウハウ蓄積のためにもある程度調査対象を合わせて、対策を行うべき IoT 機器やボットネットを決定する必要がある。19 ページの将来構想については賛同する。14 ページのようにボットネットを観測して、対策を行った時の効果を視覚的にも確認できると、対策への賛同も増えてくると思われるため、将来構想の一つの成果の確認として使用すると良い。引き続きの取組をお願いする。

吉岡構成員）

専門家が見ても C&C サーバだと言えるものが一定数検知できている点素晴らしい取組だと思う。19 ページの統合分析対策センターも取組において非常に重要と考える。質問だが、9 ページ表に【参考】として記載のある数字の意味を教えていただきたい。bot、Brute force、ssh、tor となっていて、これは表左側の検知した IP アドレスを分母にとって、その中の一部がこれらだという意味か、若しくは C&C サーバとして検知した IP とは別の IP を指しているのか等、それぞれ数字が何を意味しているか簡単にご説明いただきたい。

NTT コミュニケーションズ大村氏）

9 ページのスライドの数字に関しては、表の悪性 IP 数が分母になり、様々な OSINT と突合し、例えば OSINT の bot 感染端末と分析された IP だったり、Brute-force に利用される IP アドレスだったり、ssh のスキャンに利用されたり、あるいは tor の IP アドレスに認識されるようないずれも悪性 IP 数の中の分析の結果として、観測された情報となり、IP アドレスが重複してカウントされるケースもあるため、悪性 IP 数を分母として解析の観点で判明した通信特性として掲載している。悪性度評価を経た C&C サーバに含まれる IP 数ではなく悪性 IP 数の内数の分析結果となる。

吉岡構成員）

その場合表中の悪性 IP 数は C&C サーバのアドレスの他ボット側の IP なども全て含んだものか。

NTT コミュニケーションズ大村氏）

C&C サーバに限定して解析はしているが、どうしても他の特性を持つ IP アドレスが混入して過検知されているとご理解いただきたい。

吉岡構成員）

承知した。C&C サーバを想定し検知したところ末端側の IP も検知された形と理解した。

小塚構成員）

回線が第二種電気通信事業者に貸出されて、第一種電気通信事業者がサービスを提供していると構成もあると思う。今回実証に参加している 3 社は全て第一種電気通信事業者として回線を貸し出す側かと思うが、この取組を拡大する際には、どちらの事業者がどのような形で責任を分担するのか。

NTT コミュニケーションズ大村氏）

その点今後の ICT-ISAC におけるワーキンググループの中でも整理が必要な部分と理解しており、現時点で一種事業者が分析を行うべきか二種事業者が分析を行うべきかの明確な回答は持ち合わせていないため、今後の検討

事項としたい。

後藤主査）

6 ページに関して。今回は実証参加 3 社がフロー情報を自社独自の方法で分析し、その結果を C&C サーバリストとしてまとめ、さらにその C&C サーバリスト全体をまとめた評価を実施するという 2 段階の評価になっている。これは、機微な情報であるフロー情報の取扱いに注意しているため仕組みであると理解している。また 2 段階めで統合している C&C サーバリストについても十分機微な情報だが、もしフロー情報を最初から全部まとめて分析でき、かつ分析手法も全て試せるとなった場合に、悪性リストの分析結果について大きな進展があり得るのかどうかについての感触等があったら教えていただきたい。例えば現在金融機関ではマネーロンダリング対策のために金融機関毎に口座情報を分析している。もし複数の金融機関の口座について、取引情報全体をまとめて分析できれば、マネーロンダリング対策としては有効であると思われるが、各社の口座情報を勝手に共有することはできない。そのため、現在は研究中ではあるが、プライバシー・インフォーシング・テクノロジーズ (PETs)、例えば、秘密分散、秘密計算といった技術を使ってプライバシー問題がない形で共有することでマネーロンダリング対策効果を高めることを期待する取組がある。同様の発想で、フロー情報に対しても何か画期的な良い技術により問題のない形で情報の共有かつ、悪性サイトに関するデータ抽出が可能となると良いと考えるが、何かご見解があれば伺いたい。

NTT コミュニケーションズ大村氏）

仰るとおり、各社での分析手法の共有及びフロー情報分析事業者の拡大がより進むと、今回の調査における課題である各社の検知情報の差異や精度の向上といったところが更に進展することが想定される。ただしフロー情報で共有できる情報自体は IP アドレスとポート番号の 2 つに限定されている点で分析における限界もあるので、共有出来る情報を広げることが実現できれば、非常に高精度に悪性の C&C サーバを検知する可能性も劇的に高まるのではないかと考える。

齋藤構成員）

10 ページに関し C&C サーバ検知結果が通信事業者によって異なる点について、これは各事業者が個別に自社網のフロー情報を持ち寄ってネットワーク全体を見ることも一つの手法かもしれないが、通信の秘密を守る意味で困難と思われるところ、各事業者が自社網の状況を自社で確認し、その総和をもって日本全体のネットワークの状況を把握する試みの方が現実的ではないか。一点、検知手法の共有は言葉としては入っているが、具体的な活動は見られなかったようで、その点何か知的財産等の障壁があるのではないかと想像したが具体的な方針などがあるのか。おそらく各通信事業者ともネットフローの取得はネットワークの運用のために行っており、それをマルウェアの活動や C&C サーバへの通信の分析のためには使用できていないと思うが、分析手法の共有についてどの程度検討しているか教えていただきたい。

NTT コミュニケーションズ大村氏）

分析手法の共有に関して、各社で知的財産・R&D 的な要素に関する部分の共有は難しいと思っているが、特徴量や分析に利用するシード情報を持ち寄って、今年度各社共通的な手法で調査を実施できないかについては検討スコープに入っており、今年度そういった部分での取組も進めていく予定である。

齋藤構成員）

そうするとその結果を合わせることで日本のネットワークの全体像を描いていくと思うが、検知用のプロジェク

トにおいて進めていいのか、ある程度信頼関係のある業界団体のようなところで進めていった方がいいのかといった具体的なイメージはあるか。

NTT コミュニケーションズ大村氏）

当面は今回実証参加の通信事業者 3 社及び ICT-ISAC 加盟の通信事業者に限定し、その活動の中で今年度実証を展開していくことを考えており、今後の展開に関しては事業者の拡大も視野にとは思う。

齋藤構成員）

中立的な場所で日本の全体像を描いていただいた方が色々な応用が利くと思う。

辻構成員）

事業者間の相関性の表と図を見ると、事業者ごとに検知しているものの系統が異なっていると見えているので、検知ポイントを増やせば、もっと全体像が見えてくるというお話があったと思う。他事業者がこれに参画するときに、システムの構成、検知手法や今後ブラッシュアップしていくというお話もあったが、そういったものをできるだけクリアに共有いただくという形をとっていただきたい。また質問だが、1 点目に資料中今後検討とあった、検知した C&C サーバリストについて具体的にどういった範囲で何のためにどのように活用していくかという現時点での想定はあるか。こうすればブロックできるのではないか、被害者を減らすことができるのではないかといった想定の部分である。2 点目にボットネットの可視化のスライドにおいて、10 日間でボットネットの規模が増えて、それが更に 10 日後に規模が縮小していた図があったかと思うが、これは何が影響してこういうサイクルになっていたか分かっているのか。特に、減っている理由の方を伺いたい。また 10 日間というのはよくあるサイクルか。

NTT コミュニケーションズ大村氏）

質問への回答として 1 点目については、今後の具体的な利活用に関しては、まさに ICT-ISAC の中でも特定の事象、国内の電気通信事業者が協調対処すべきような非常に影響度の高いボットネットをユースケースとして捉えて、それらの対策に繋がるような C&C サーバを共有することで、具体的な対策効果のシミュレーションや効果測定できると非常に今後の有効活用での評価にも繋がるのではないかと考えている。2 点目については、フロー情報分析から明確に具体的な事象として何が起こって減ったかというのは特定が難しい部分はあるが、攻撃者の傾向やボットネットの活動の変遷の一環でこういった拡大縮小が行われている。現時点でフロー分析から得られる情報としてはそういったところまでかと思う。またボットネット増減のサイクルについてはボットネットの種類に応じて大きな開きがあるかと思う。

辻構成員）

サイクルが短かければ短いほど、検知してから共有して対策というようにもっていく間に減っている、情報が行き届いた頃には C&C サーバが止まって違うところに行っていることになると、せっかく検知をしたのに間に合わなかったということになるので、検知することも凄く大事なことだが、それを有効に活用するためにこういったサイクルがどれくらいなのかに照らし合わせて、共有の仕方、対策の実施の仕方を検討していく必要があると感じた。

後藤主査）

C&C サーバではないが、私の大学で悪性サイトの寿命を調査した研究があった。その調査では、悪性サイトは非

常に早いサイクルで姿を変え、アトリビューションを避けようとするという報告があるので、辻構成員のお話にもあったように、いわゆる検知結果をいかに素早く活用するかということは非常に大事だと思った。

笠間氏）

一点質問があり、13 ページで C&C サーバの所在地として海外が多いという話だったが、一定数日本のアドレスも今回の手法で検知されており、これが自社網の中だったのかもしくは外だったのかという点と、検知されたものについては、アドレスが具体的に何だったのかを追跡しやすいパターンかと思うが、他社の場合も含めて何かアドレスの素性を確認するというアクションをされたのか、何かあれば教えていただきたい。

NTT コミュニケーションズ大村氏）

これに関しては事業者 B のパターンでいうと Japan と書いてあるところはその事業者外のアドレスになる。具体的な IP に紐づくサービスの深掘りまでは実施出来ていないので、今後そういった国内にある C&C サーバに関しては、詳細に関しても分析を進めていきたい。

笠間氏）

情報共有に関する法的整理は既にできているということなので、このような事例は上手く情報共有して C&C サーバを特定して対処するというところに繋ぎやすい事例かと思った。

◆議題（２）「効果的な利用者への周知啓発について」について、辻構成員より資料４－２を説明。

◆構成員の意見・コメント
小塚構成員）　※チャットより抜粋

「伝えるべき人に」「伝えるべき内容を」伝達するという辻様のご意見には賛成する。その際には、通信事業者が対応する方が効率的な範囲と、一般ユーザに対処してもらうことに効果がある範囲とを見きわめていくことが重要ではないかと思う。

田中構成員）

辻構成員の発表は非常に面白く、まさに伝わるプレゼンだったと思う。セキュリティの重要性や何が求められているのかが伝わりにくい層に働きかけていくことがプロジェクトの目的になってくると思うので、各層に届くアプローチの仕方というものをしっかり考えないと空振りになってしまうのではないかと思った。先日、銀行 ATM の前で還付金詐欺への注意喚起を車から放送している場面に出くわしたが、SNS 等とは別に住宅街で放送を流すことで救われた高齢者や主婦の方々もかなりの数いたのではないかと思う。我々が続けている NOTICE プロジェクトも、辻構成員がおっしゃったような観点をしっかりと取り入れていくべきだと感じた。

藤本構成員）

辻構成員のプレゼンに色々共感するところがあって考えさせられた。最近、注意喚起について私自身感じていることなのだが、注意喚起を装ったフィッシングメールが非常に多くなっていると思う。メールで注意喚起を受けた際にそのメールがフィッシングメールかもしれないと思ってしまうと、きちんとしたメールでも URL をクリックできないところがある。それで、注意喚起の送付元サイトから直接確認しようとしても、目的の箇所になかなか到達できないというような経験があり、メールでの注意喚起にあたっては考える必要があると思っている。やはり注意喚起をするというのは、伝えた相手にリアクションしてもらうということが大事だと考え

ており、辻構成員の発表のとおり、伝わるような伝え方をすることが非常に重要なポイントかと思うが、さらにその人がどういうようにリアクションをするかについても研究をして情報を届ける工夫も必要になってきていると思う。もう 1 点、情報を伝える時に考えなければならないのはタイミングかと思っていて、辻構成員のプレゼンの中にも Web や SNS、セミナーに来てくれない人にどうやって伝えるのかが非常に重要かと考える時、情報が伝わりづらい人たちに、どういうタイミングであれば話を聞いてもらえるきっかけを掴めるのかを考え、どういう形の伝え方があるのかという作戦というか、戦略的な思考も必要だと思った。

辻構成員）

確かにおっしゃるとおりで、色々な脅威や事件事故に対して、こうすれば良いという銀の弾丸みたいなものはないが、例えば振込み詐欺等でコンビニの店員の制止を振り切ってまで振り込もうとした人など、情報不足により詐欺に遭いそうになった人もいたりする。そういった人達に対する情報提供についてもっと考える必要があり、例えば区で高齢者向けスマホ活用もやっている例もあるが、そういった人達がどこから情報を入手して、どういったコミュニティに参加しているのか知る必要がある。私が関わった事例では、スマホに初めて触れるような高齢者の方々に対して動画サイトに詐欺に関する注意喚起の広告を出した例があったが、そもそもスマホを始めて触った人は動画サイトを見ないのではないかと思ったので、高齢者の方をターゲットにした注意喚起を行うのであれば、極端な表現だが、たとえば、朝 4 時くらいの暴れん坊将軍の再放送の時間の CM に松平健が振り込め詐欺成敗などやった方がうけるのではないかとコメントをしたこともある。

小山構成員）

スライドの 12 ページに書かれていたとおり、伝えるべき人に伝えるというのは重要なポイントかと思う。IoT 機器の注意喚起の報告がこの分科会でも過去にあったのだが、対策しても動かないのは法人が設置したものだということである。つまり注意喚起の対象となるのは回線契約者しか特定できないので、機器設置者や IoT を実際に使っている人に対する効果的な注意喚起の方法などアドバイスがあれば伺いたい。

辻構成員）

注意喚起対象がどの程度の規模の組織なのかを考えると、例えば商工会議所のようなところが開催しているイベントに参加する形で話をするであるとか、そういった人達は横のつながりが強い場合もあるので、そういった人達のコミュニティにリーチするというのが一つの方法ではないのかと思う。

◆議題（3）「諸外国におけるサイバーセキュリティ対策の取組事例」について、事務局より資料 4－3、議題（4）「論点整理」について、事務局より資料 4－4 を説明。

◆構成員の意見・コメント
【資料 4 － 3 について】
辻構成員）

資料 4 － 3 の 3 ページについて Walled Garden はどういった原理で実現しているのか。日本で法律的に実施可能なものなのか、どうすれば実施出来るのかということが気になった。あとは 2 ページの NCSC の取組の脆弱性のスキャンについても法的な問題等の懸念もあるので、そういったことをどうクリアにして実施しているかが気になる。加えて、NOTICE では機器特定や機器のバージョンも分かるという点で、いわゆる SHODAN のようなこともやろうと思えばできるのか。詳細を公開するかは別にして、国内にどれだけ脆弱な機器があるという情報を添えるだけで注意喚起の効果も上がると思うし、メディアも取り上げてくれやすくなるかと思ったので、そういった取組が実現できればいいと思った。

吉岡構成員）

Walled Garden については NICT と我々（横浜国立大学）とデルフト工科大学で KPN というオランダの ISP の協力を得て行った研究で、基本的には NICT のダークネットと横浜国立大学のハニーポットで、まず攻撃を常に観測し、この中で KPN の IP アドレスからの攻撃があったときにデルフト工科大学を経由して KPN に情報を提供する。KPN はそこから感染端末を持つユーザを特定して、そのユーザを Walled Garden に隔離するのだが、具体的には基本的にほぼ全ての外からユーザに届く通信のブロックとユーザから外に出ていく通信もホワイトリストを除いてブロックするという形になっている。そうするとインターネットがつながらなくなるので、ユーザがブラウザを立ち上げてどこかにアクセスしようとすると、そこをリダイレクトして注意喚起のページに誘導するようにしている。その注意喚起ページには、なぜ当該利用者が隔離されているのかという説明と、要請する対応の内容、及び Mirai 等のマルウェアに感染している事実をウェブベースで伝える形になっている。対応してくれたら再度インターネットに繋がる趣旨のことも記載しているようで、再度インターネットに繋げるために対応が必要になるので、非常に効果は高いのだが、かなり強制力のある強い方法になるかと思う。

佐藤企画官）

このプロジェクトが日本で可能かどうかについては、どういった条件で行うかによって当然ケースバイケースだと思うが、仮に実施しようとすると通信の遮断という強い措置になるため、事前に利用者からの同意が必要になるのではないかと思う。

河村構成員）

私もこの Walled Garden の試みは興味がある。通信の遮断を伴うという説明について、これは感染端末を持つユーザがブラウザを立ち上げると注意書きページに誘導されるということだが、質問として、例えば PC の OS のバージョンアップを促す画面のように、無視することも可能なのか。全くインターネットに繋がらなくさせるというよりは、複数回しつこく画面が出るということも可能なのか。また、インターネット不通を解決するためには対応を要請すると記載があるが、この場合の対応を、消費者がする場合はパスワードを変えるなどそういうことを指しているのか。

吉岡構成員）

ユーザの対応は今おっしゃっていただいたとおりで、この場合は実験当時主に Mirai というマルウェアの感染が中心だったので、ルーターの再起動やフォームウェアの更新等の一般的な対応リストをお伝えしていた。実は実験の中では、ユーザへの注意喚起の方法として、非常に平易な分かりやすい方法の記載と、専門的な方法の記載とで、効果にどれくらい差があるかについても実験をしたのだが、先ほどまでの議論でもあったとおり、できるだけ平易に誰でも理解できるレベルの記載の方が効果が高いという結果も得られている。また、通信遮断するのではなくて、注意喚起だけを出してみるというお話もあったのだが、それも一つのアプローチではないかと思った。もともとこの施策を行った際には、基本的には外部に攻撃をしているという事実が確認されている状況だったので、これ以上感染が広げるのを止めるという意味もあって、外への通信の遮断をせざるを得ないという緊急的な対応だと思うのだが、それ以外の対応で注意喚起のメッセージを伝えるというアプローチもあるのかと個人的に思った。

河村構成員）

先ほどの辻構成員の発表でも意味のある注意喚起についてのお話があったが、製品安全や事故など一般的な注意喚起でも言えると思うが、この場合、実際に感染しているユーザに向けてあなたは感染しているという注意喚起がブラウザを立ち上げる度に出るというのは、通信を遮断しなくても相当効果があると思った。また加えて、ブラウザを立ち上げた際の注意喚起については該当するデバイスが感染している場合のケースに限られるのか。それとも同じルーターを通じて使っている別の機器に感染があったときにもブラウザを立ち上げると注意喚起が出てくるものなのか教えていただきたい。

吉岡構成員）

基本的には先のご説明のとおり、私たちが行った実験では攻撃通信がその利用者の IP アドレスから出ていることを確認したときに通知がいく方法をとったため、脆弱性があるというだけでは注意喚起はされないと思う。先ほどルーターと限定的に言ってしまったが、より厳密に言うとその利用者の IP アドレスから攻撃が届いていることを確認しているので、多くの場合はルーターと思うが、感染しているのが必ずしもルーターだけとは限らず、利用者が使用しているデバイスの別の何かが感染している場合もあるため、注意喚起をするときにはルーターとは確か言い切らず、お使いのデバイスといった広い言い方をしていたと思う。さらにこの研究は続きがあり、オランダのデルフト工科大学が独自か、少なくとも私たちは入らない形で行ったのだが、そのように ISP から通知があった時に、ユーザがどこまで理解ができているのか電話をかけて細かく聞いたという研究もしていた。そもそも今のような注意喚起をした時にどのデバイスについてのことを指しているのか分かったか、インストラクションの提示した対策の意味が分かったかなどをかなり詳しく聞いて、対策ができないというときにどこに問題があるかということを調べたような研究もある。その研究でも色々な結果が出ているが、意外にデバイスを完全に特定した形で注意喚起をしなくても一定の効果はあったということもあって、多くの場合はルーターだったのでルーターについて対策をしたということなのかもしれないが、そういうような結果も出ていた。
補足として、Walled Garden について追加の情報として、これは実験的にやったものなのか、オランダの ISP は定常的にこういった取組を行っているのかという質問を受けたことがあったのだが、確認したところいくつかの ISP は基本的な対策として実行しているとのことである。つまり研究目的の実証実験だけではなく、通常の対応としてこういうことを行っているということである。ただ一方で、ヨーロッパ中心にそれがスタンダードな対応かというと必ずしもそうではないという状況だと聞いている。

【資料４－４について】

吉岡構成員）

資料４－４についてのコメントだが、まず全体をとおして非常に素晴らしい内容のとりまとめをいただき、基本的に全ての内容について同意する。特に 2 ページ、私も分科会でプレゼンしたが、IoT を狙う攻撃の脅威が多様化していて、脆弱性を狙う攻撃が主流になっていると考えており、やはり NOTICE の効果を維持するためにも脆弱性等のある IoT 機器への対応というのも是非ご検討いただきたい。また 4 ページの接続拒否の問題について、利用者が注意喚起に応じない場合の最終的な対処の手段として有効なものであるとは考えているが、先ほどからもあるように慎重に行う必要があり、顧客である利用者の理解をなかなか得にくいところもあると思う。先日の KDDI からのプレゼン等でもあったかと思うが、慎重さは絶対に必要であるものの、利用者へそもそもこういった問題があることの注意喚起・啓発と併せて、どのように接続拒否のような仕組みをこれから適用していく可能性があるのかということ、要件や手続き等を明確化していくところからでもスタートしていくことで、NOTICE の取組が少しでも加速すれば良いというように感じた。最後に、脅威がかなり多様化していることもあり、13 ページのところで、総合的な対策が必要である点も常日頃から私も思っていることで、資料４－１で統合分析対策センターについては、まさにこういった体制が必要だと思っていた。やはり多様化した脅威は例えばハニーポットやダークネット等だけでは全て検知できないけれども、説明もあったフローデータの分析によって判

断できるといった、総合的に情報を見ていかないとこの多様な脅威に立ち向かえないという状況になりつつあるように思うので、この取組についても非常に意義があると感じた。

田中構成員）

これまでの議論を綺麗に整理してまとめていただいたと思う。全体的な話となるが、今回、端末側の部分、ネットワーク側の部分に分けた上で、課題を 6 つに整理いただいたと思うが、可能であれば全体の方向性のような、端末側とネットワーク側の計 6 つの課題の対処を進めていく中で、どこを到達点とするのかが示せると良い。途切れのない不断の取組だと思うので、ゴールや KPI のようなものは設定しにくいかもしれないが、これら 6 つの取組が総合的に全体として目指していく部分を 1 枚で示し、その部分についてコンセンサスを得て進めた方が、各取組がバラバラにならず良いのではないかと思う。

小山構成員）

過去の議論がカテゴライズされてうまくまとめていただいていると感じた。その上で 13 ページの今後形成されるであろう統合分析対策センターには大変期待している。最も期待している点としては、資料にも記載のとおり IoT ボットネット全体像の可視化である。ボットネットの C&C サーバがコロコロ変わっていくという点についてはそのとおりだと思うが、ボットネット自体の場所は変わらず、感染端末は次々と違う C&C サーバから指令を受けて悪さをされている。ボットネットがどう変遷していくのかを可視化して、その上で対策の効果を確認するということが重要なのかと思う。そう考えると、11 ページの C&C サーバの検知精度の向上というのは、学術的にとても重要なことだと思いつつ、実際の IoT ボットネットの対策を進めていく上では、C&C サーバの検知の精度の向上に加え、C&C サーバを含んだボットネットの追跡性を高めるという視点もある方が全体の効果にも繋がる思うので、ボットネットの追跡性を高めるという概念を少し持ちながら、検知精度を高めるという取組をすべきだというように思った。

齋藤構成員）

先ほど田中構成員のご指摘にもあったが、今現在 IoT 機器のセキュリティが非常に重要な課題であることは事実であり、それに対応する施策がこれまで活発に行われて、今後それぞれが活性化し、引き続き実施されていくと点は非常に良いことだと思う。私もこれら施策に関係していてどんどん世の中が良くなっていけるという実感もあるのだが、それぞれの事業者が全部の対策を全力で取り組まなければならないのか、それともお互いに補完し合うような面があるのか。特にコスト負担や作業量といった点で、エンドユーザ、通信事業者及び製造に関わる方がそれぞれどれだけのことを実施するかという点が、最終的にはある程度バランスのとれた施策にしていただきたいと思う。資料 4 － 4 のような論点整理から提言もまとまっていくかと思うが、我々としてどういう状態を目指していくのかに関して、ある程度共通の目標を掲げていただいた方がいいのではないか。

笠間氏）

色々な論点があり、端末側・ベンダー側・ユーザ、そして調査をしている我々NICT、あとは注意喚起の伝え方等色々な対策の方面があって、恐らくどこかが欠けてもうまくいかないというように思うため、こういったとりまとめによって対処がきちんと可視化されていくと良い。9 ページの NOTICE の運営についてコメントだが、我々NICT はこの調査を 4 年ほど続けており、当初は Telnet と SSH のポート 23 番、2323、あと 22 番で、オリジナルの Mirai が狙っていた部分にフォーカスをして調査をしてきたのだが、その後、別のポートや HTTP 等の別のプロトコルの問題にも調査を拡大していって、その結果 1 万数千台などのレベルで脆弱性な機器が見つかっている。そういった調査対象の拡大をしながら続けてきたわけだが、吉岡構成員のお話であったように最近増

えている特定の脆弱性を狙うようなパターンも適切にフォローアップ及び調査の拡大をしていき、日本のネットワークが現在どういう状況になっているのかを見ていくことは非常に大事だと思っている。Emotet の時も海外から感染端末のリストをもらって対処をしており、それも対処としては非常に重要だと思うが、先ほどの可視化といった、やはり日本としてネットワークの状況がどうなっているのかをきちんと把握・追跡していくところが一つ重要である。また、ボットネットに注目すると、実は NOTICE で見つかっている ID・パスワードが脆弱な機器の多くは NICTER 観測では見えていない、つまり、Mirai 亜種には感染していないことがわかっている。ただし、それらの ID・パスワードが脆弱な機器が感染しえないのかというと決してそうではなく、その機器に応じた感染手法を用いるとマルウェア感染まで出来てしまう。そのためやはり感染済みの機器だけではなくて、脆弱性や ID・パスワード設定の不備がある機器というのが潜在的なリスクであるというのは、調査を実施している立場から凄く感じているところなので、きちんと観測していくことが重要かと思っている。加えて、以前井上からもコメントもさせていただいたが、我々としては調査を拡大していくとなるとリソースの問題もあり、やはり調査の手法を拡大していくにあたって人員や体制をできる限り柔軟にできるようにするための制度や支援というのをお願いしたい。また、我々が調査しているデータはプロジェクト関係者も含めて積極的に公表することはしていないが、例えば国内にある機種がどのくらいいて、古いバージョンのものがどの程度あるといったデータも集まってきているので、こういったデータを上手く活用し国内のインターネット状況の可視化であるとか、関係団体を含めた協調に繋げられると良い。

河村構成員）

とりまとめについて全体の感想だが、以前も一人一人の消費者が実際に何か対処をすることに頼るのはなかなか難しい上、負担でもあるということを申し上げたが、そういう意味でもなるべくルーター等機器の設計仕様として脆弱性を無くしていく、利用者が意識しなくても安全なものになる方がいいという意見は変わらない。また今回前半で C&C サーバについてご説明いただいたが、C&C サーバ検知の精度を上げていくことやそのリストを共有するといった取組はあるのだが、今一つ見えなかったのが C&C サーバへの対策である。C&C サーバが判明した時に何をするか書いてあるのだが、その際にできるだけ大元のところで何か効果的な行動が取れるのであれば、遮断や利用者への注意喚起などをするまでもなく、なるべく大元で何ができるのかということを考えるといいと思う。凄く難しいことはお聞きしているが、製品安全の考え方を援用するとしても上流で対処することで消費者はあまり意識しなくても安全になるという方が良いのではないか。

後藤主査）

全体の印象として、まず論点整理の最初にあるように、NOTICE が着実に効果を出していることを踏まえると、しっかりこの後も継続していくべきという点に賛成する。ただ田中構成員、齋藤構成員からもあったように、施策全体を大きく見る、俯瞰的に見るという視点が一番大事ではないかと考える。その意味でも、そもそも何のために NOTICE を行っているのかという点、つまり、田中構成員もおっしゃっており、ID・パスワード脆弱性のある機器を見つけて注意喚起するのは手段として行っているものであり、本来の狙いは、ネットワークサービスをきちんと国民が安全安心に使えること、その上で IoT 機器を使いこなせること、と再認識し、それを達成する手段の一つとして NOTICE の取組がある。そういった観点で全体を見極め、この NOTICE がどうあるべきなのかを検討する必要があると思う。また、可視化という言葉が C&C サーバ検知の取組の説明であったが、全体の効果を可視化しながら、皆で協議しつつこの取組がどういう効果をあげているのかをチェックして取組を進めていく姿勢が大事である。その点先ほどの注意喚起の効果測定の話が辻構成員からあったが、C&C サーバ検知に限らず色々な場面で、どういう効果があったのかを見ながら、多数のステークホルダーと互いに協議して知恵を出し合って取組を進めていくのだと思う。特に河村構成員からあったようにメーカー等と協力しつつ進めることが大事だろうと思う。いずれにしても NOTICE の運営を見ると NICT と ICT-ISAC 加盟 ISP の有志で使命感の

高い人の献身的な取組に頼っている部分がある。我々はそれに依存していいのかと一国民として思い、先ほどの笠間氏からの人的リソースの大変さやISPからの注意喚起のための手間の大きさの話もあったが、そういった点に関しても、一部の方に苦労が偏ってしまわないように全体としてのバランスの良い取組とすることが大事である。先ほど田中構成員がおっしゃったように、このとりまとめの最初に、そもそもこれらの取組全体が何を目指しているのかを示して、その中でNOTICEの役割を今後どう継続拡張するべきなのか、役割を噛み砕いていくというのは良いアイデアだと思う。

（3）閉会

以上