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２回）議事要旨

1. 日 時）令和５年２月 16 日（木）10：00～12：00

2. 場 所）総務省 第２特別会議室(８F)及びオンライン

3. 出席者）

【構成員】

後藤主査、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、藤本構成員、吉岡構成員

【オブザーバー】

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】

松本勝之（ソフトバンク株式会社）

4. 配付資料

資料２－１　サイバーセキュリティ対策の取組みについて（NTT コミュニケーションズ）
資料２－２　KDDI におけるサイバーセキュリティ対策の取組（KDDI）
資料２－３　ネットワークにおけるサイバーセキュリティ対策（ソフトバンク）
資料２－４　ISP における DDoS 攻撃対策の現状（インターネットイニシアティブ）
資料２－５　ICTーISAC におけるサイバーセキュリティ対策に関する取り組み（ICT-ISAC）
参考資料１　第１回会合における構成員からの主なご意見
参考資料２　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１回）議事要旨

5. 議事概要

（1）開会

（2）説明

◆議題（１)「通信事業者によるサイバーセキュリティ対策の取組状況と課題について」について、小山構成員より資料２－1、田中構成員より資料２－２を説明。

◆構成員の意見・コメント

吉岡構成員）

特定の機器の感染による数千台規模の攻撃活動であってもネットワークにこれほど大きなインパクトを与える

ということが改めて実感できた。継続した攻撃観測とベンダとの連携、所有者へのフォローなど、対策活動として今後のモデルとなる事例であると思う。初期の Mirai のように Telnet から多様な機器に感染する、というケースだけでなく、特定機種の脆弱性やセキュリティ不備を狙った攻撃も増えると思うので、当該機器のベンダとの連携の重要度がさらに高くなると思う。フロー情報の解析に関する研究開発の必要性についても完全に同意する。材料であるフロー情報は誰でも利用できるものではないので、研究者がこのようなデータを使用して研究ができるための枠組みがあると良いと思う。

小山構成員）

フロー情報分析については、法的にどこまでできるかについてまだ十分に整理ができていないが、認定協会業務の 2 号業務の一環として取り組める余地がないか民間レベルでは考えており、どういった条件下であれば取り組むことができるか総務省にも検討をお願いしたい。

佐藤企画官）

現在、フロー情報分析による C&C サーバ検知の実証事業を行っている。実証の状況を見ながら、次のステップとして何ができるかをしっかり検討していく。当該実証については、本分科会でも今後状況を報告する予定であるため、その際ご意見・ご議論をいただきたい。

小山構成員）

フロー情報だけ眺めていても何かが分かるわけではないため、他のセキュリティ情報との突合や分析ノウハウの共有といったものが重要。

後藤主査）

小山構成員からあったように、米国ではキャリアがフロー情報分析をサービスとして提供している部分もあり、そういった取組がどの程度有効かの調査があればより参考になると思う。海外では FloCon という会議において、フロー情報分析等について非常に有益そうな議論がされており、日本からの発表はあまりないが注目すべき。また、昨今この議論のベースとなるネットワークのトラフィックなどを研究する若手研究員がだんだん減ってしまって、ネットフローを扱う技術者の高齢化も心配しているが、若手研究者がセキュリティ関連でネットワークトラフィック等を研究し世の中に役立つという空気を盛り上げられればいいと思った。

小塚構成員）

小山構成員及び田中構成員お二人の発表とも、ミニマムであっても端末ユーザーの側の対応が必要な部分があるというご指摘があった。この点、ファームウェア・ソフトウェアのアップデートに留まらず、機器の買い替え・更新が必要となれば金銭的な負担もあるため、ユーザーの対応はどの程度まで必要か質問したい。また関連の意見として、対個人ユーザーの場合には、大変だと思うが必要性を理解してもらえれば最終的には行動を取っていただけるかもしれないが対企業ユーザー、とりわけ中小企業などを考えると、セキュリティ担当者ないしは機器等の更新・買い替え等を判断する担当者の有無などの、社内の仕組みも含めて企業のユーザーの方が実は端末側対策のハードルは高いのではないかと思うので、その点考える必要がある。

小山構成員）

小塚先生のおっしゃったとおりで、個人ユーザーは自分で契約した回線の先に端末機器を設置して、それが踏み台になる構図がほとんど。一方で法人契約の場合は、SIer が間に入るケースでは、回線の契約者と機器設置管理

者が別であることもあり、企業の中の意思決定だけでなく、問題の所在の特定等、対応が難しい面がある。

田中構成員）

小山構成員の話とも重なるが、NOTICE の枠組みで注意喚起しても、是正に至らない利用者は実は法人の方がほとんどという状況。その原因としては、今小山構成員もお話しされたとおり、問題の所在が曖昧である、あるいは注意喚起時には機器を導入した担当者がおらず、その機器管理の意識といったものが個人のお客さまよりも難しいケースがある。

藤本構成員）

セキュリティの話を利用者に聞いてもらう一番のタイミングとしては、法人であれ個人であれ、機器を購入する際であり、後になってセキュリティについて伝えようと思っても、聞きに来ていただけない利用者には伝えられる術がない。広報活動やマーケティング活動において機器メーカと協力するのが有効とのこと、そのような取組は何かあるのか。

小山構成員）

広報の考え方では対個人ユーザーと対法人ユーザーの 2 通りあり、まず個人ユーザーの場合は、例えば端末機器等を買うときに注意点が 3 つなどの分かりやすいメッセージを出していく必要がある。一方で法人ユーザーは購入者と使用者が異なる側面もあり、悩ましい事例として、全てのポートが開いている脆弱な機器を発見し、メーカーにその旨問い合わせたところ、そもそもその端末はインターネット接続を想定しておらず、Sler が容易に設定できるよう全ポートを開けた状態で販売しているということがあった。この事例では利用環境によってはそれでも良いのかもしれないが、そもそもそういうことをメーカー自身が考えていないことが問題になった事例もあった。

後藤主査）

まさにセキュリティ・バイ・デザインの考えであり、IoT 機器関係では、イギリスで、機器出荷段階でポートを閉じたりパスワードを設定したりするといった誓約を作る動きがスタートし盛り上がっていることと同じだろう。

◆議題（1）「通信事業者によるサイバーセキュリティ対策の取組状況と課題について」について、ソフトバンク松本氏より資料２－３、齋藤構成員より資料２－４、小山構成員より資料２－５を説明。

◆構成員の意見・コメント
後藤主査）

資料２－４の 1 ページ目右側に世界地図でセキュリティ対策機能を置いている場所の話があったが、セキュリティ機能を IX といった上位のティアに集約すると対策効率が良くなることは考えられるか。

齋藤構成員）

IX でセキュリティ機能を提供しているようなケースもあるかとは思うが、現在の技術では通信の方向の制御や、実際に守る宛先が決まっていない通信に対する適切な対処がしにくいため、IX の分野でセキュリティ事業として成立するのは難しいのではないか。常にネットワークを俯瞰し異常と思われる通信を止めることは難しく、決まっている攻撃から守るべき宛先について、普段の正常な状況と比べることで異常を判断しているのが現状で、

直感的にはそういった意味では IX のような中間者が適宜通信を止めるのは少し難しいのではないかと思う。

河村構成員）

資料２－３の 21 ページの、より上流工程での対策についてはそのとおりで、機器の設計段階でセキュリティの対処をすべきであると考える。また資料２－４の６ページ目にも観点は違うが脆弱性を持った IoT 機器を放置することは良くないとして、ネットワークの上流での対策について言及されており、まったくそのとおりだと思う。前回分科会でも申し上げたように、個々の消費者によるセキュリティ対策を徹底するのは難しい。質問として、資料２－４の発表では、パソコンやスマートフォンについて言及がないが、これらは充分なセキュリティ対策がなされているためにセキュリティ対策の対象として名前が登場していないという理解で正しいか。結局技術やコストを端末側にかければ、消費者から見ると機器の値段が高くなることになると思うが、IoT 機器についてもこれから世に出る機器は、安全にすることは可能だが、そうすると値段が高くなるという意味なのか、それとも安全にすること自体が難しいことなのか。

後藤主査）

私の理解で申し上げると、値段は少し上がるかもしれないが、IoT 機器を技術的に相当安全なものにすることは可能であると思っている。一方、現実社会では自由に商売が出来て、安くてセキュリティ品質の悪い IoT 機器も販売できる環境であるため、利用者が店で買う IoT デバイスを全てセキュリティ対策がきちんとしたものにするには、それを規制する何か制度的な仕組みがないと難しい認識でいるが、この点補足あるか。

佐藤企画官）

補足として総務省の取組を紹介すると、ネットワークに接続される利用者側の端末設備については、初期パスワードを使用しないなどのセキュリティの要件を定めた技術基準を 2020 年に新たに設けたため、基本的にはその基準に合致したものがネットワークに接続されている。NOTICE の取組で現在脆弱性が発見されているのは前述の技術基準施行前に発売された古い機器であるケースが多い。これから発売される機器については、こうした一定の基準を満たした安全なものが多くなると思うが、当然いたちごっこの世界であるので、新しい機器についても不断に対策の検討を行う必要があると考えている。また古い機器への対処についても NOTICE 注意喚起の効果向上という観点で引き続き改善する必要がある。

後藤主査）

補足すると、パソコンやスマホはおおよそ 4、5 年で買い替えているが、IoT 機器のライフサイクルは、監視カメラになると 10 年 15 年、自動車などは数十年であり、古い機器が残ってしまう。ソフトバンクの松本様からの、より上流工程でセキュリティ対策をすべきという話も、齋藤構成員からの今ある IoT 機器に総当たりで対処しなければならないというご指摘も、両方大事な課題と認識した。

齋藤構成員）

パソコンやスマートフォンはマイクロソフトや Google、Apple といったいくつかの大きな企業による寡占の状況があるが、一方で IoT 機器を作っているメーカーは現状たくさんあり、「上流工程で機器をセキュアにすることで下流工程において利用者が困らない」というメッセージを伝える先である製造者が非常に多い点が大きな課題と認識している。資料２－１及び資料２－４でも指摘しているが、監視カメラや DVR 機器の感染が分かったとしても、どの機種のどのバージョンにどのような問題があるかを、個別のコンタクトでいかに利用者に伝えるか、各社各様に整理しないと今後も効果的な対策にはならないのではないか。

河村構成員）

既存の古い機器への対処に人海戦術的な対応が必要であるのも非常に理解できるが、今後発売されるものに対し今ある基準よりも更に高いセキュリティ基準を設けることで、十年、二十年と使うような機器も安全にすることができる。つまり危険な機器が次々流通することを仕方がないことにすべきでない。一方で対策を打った結果機器の価格が高くなることには消費者団体として積極的な賛成はできないが、納得できる範囲の価格上昇であれば許容するということと、前述の新しい技術基準については、パスワード設定程度では少し優しすぎる基準と直感的に思う。新しい基準の策定まで視野に入れるべきではないか。

後藤主査）

大変貴重なご提言で、今後の分科会の課題・議題だと認識している。今回 5 人の方の発表の共通点として ISP キャリアも対策・手間がかかっている点が挙げられていたが、例えば注意喚起について 1 件当たりのコストを数字で表現することは可能か。大まかでいいと思うが、どの程度コストが掛かっているかを共有すると、議論がしやすいだろう。

小山構成員）

以前、注意喚起を行うための、ログ分析によるユーザー特定から注意喚起文面作成・送付の一連の流れに対し、いくら掛かるかを測定したことがあるが、相当な金額が掛かる一方、生産性があまり高くない業務であるため、経営上売り上げにつながる方向にしたい。

齋藤構成員）

恐らく対応にかかるのは 1 件数百円のレベルだったと記憶しているが、郵送での注意喚起を行うと 1,000 円を超えたかと思う。

小山構成員）

注意喚起をした利用者に対策を行っていただくまでサポートを行うと、更に上がって数千円の単位になっていたと思うので（※）、1 回注意喚起を行うと新たな IoT 機器を買えてしまうくらいのコストが ISP 側で発生していると私は理解している。

※会合後、ICT-ISAC 会員事業者への調査を行ったところ、注意喚起 1 件あたりのコストは手法により差異があるものの、平均で 3,000 円/件程度であった。

後藤主査）

一般的なコールセンターでも 1 件 5,000 円～2 万円ほどかかると聞いたことがある。他にも、IoT デバイスについて、ボットネットを抑え込むような根本的で規模の大きい対策も必要とのご指摘があった。この点に関しては、OSINT 情報やいわゆるサイバースレッドインテリジェンスと呼ばれている情報が役立つだろうが、ボットネット対処には詳細で深いインテリジェンス情報が必要なのか、それとも、OSINT 情報でしっかり対応することで対処できるのかについて何か意見はあるか。

齋藤構成員）

資料２－４でも言及したが、現在総務省のフロー情報分析による C&C サーバ検知のプロジェクトに関し実装のためのワーキンググループを ISAC で立ち上げている。まだ実証実験に入ってないという認識で具体的に今回のワーキンググループの活動がどういう成果を上げるかは分からないが、一般論として、セキュリティベンダ等が

提供しているインテリジェンス情報を入手しても、自社網で検知したマルウェアの活動とはその情報が合致しないことが経験則として分かっている。自社網でのマルウェアの活動は各 ISP がそれぞれ観測しなければならないというのが意見であるところ、世界中の情報を一挙に集める必要はなくとも、自社網においてどういう攻撃が行われているのかについては、フロー情報分析等何らかの手法で常時見つけるような活動が必要ではないか。

後藤主査）

外から得られるような情報ではなく、ISP やキャリア自らが得られる深い情報の調査、収集、分析が重要と理解した。

小塚構成員）

少し関連して人材について、そういった取組に対応できる人材がどこにいるのが 1 番良いのか。通信業界だけでなく、メーカー、金融や交通、電力など、アプリケーションを持つ業界のうち、どこにセキュリティに対応できる人材がいることが、大規模な対策を行っていく上で理想であり、現実はどうなのか。

小山構成員）

人材が必要なのは全ての段階で、セキュリティ・バイ・デザインという言葉があるとおり、高度なスキルを持った関係者が 1 ヶ所にいるというより、各段階で人材教育をして、レベルの高いものでなくても、基本的なコーディングや導入前のテストにおいて機能だけでなくセキュリティ面のテストも行うといった各所の薄く広い育成がまずは重要ではないか。後藤主査からもご指摘があったように、深いインテリジェンスは専門的な領域になってくるため、現場のデータに研究者が触れることができる環境も作りながら人材育成を行う取組が必要。

後藤主査）

理想はそうであるとしても、現状はまだそこに達していないか。

小山構成員）

そのとおりである。そのため、セキュリティ・バイ・デザインについては人材育成だけに頼るよりは、ガイドラインの作成及びそれに沿った機器の製造といった合わせ技が必要と思う。

（3）閉会

以上