参考資料2

**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１回）議事要旨**

1. 日 時）令和５年１月１８日（水）10：00～12：00

2. 場 所）オンライン

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、吉岡構成員

【オブザーバー】

野村至（内閣サイバーセキュリティセンター）、下河大介（経済産業省）

【総務省】

山内サイバーセキュリティ統括官、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】

引地信寛（ICT-ISAC）、沖本彰（KDDI 株式会社）

4. 配付資料

| | |
|---|---|
| 資料１－１ | 「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」開催要綱 |
| 資料１－２ | 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について |
| 資料１－３ | IoT 機器へのサイバー攻撃の現状について（吉岡構成員） |
| 資料１－４－１ | NOTICE の現況 |
| 資料１－４－２ | NOTICE：４年間の取組と成果、課題（井上構成員） |
| 資料１－４－３ | NOTICE における ICT-ISAC の役割と課題認識（ICT-ISAC） |
| 資料１－４－４ | NOTICE サポートセンターの活動と課題（NOTICE サポートセンター） |
| 参考資料 | 「サイバーセキュリティタスクフォース」開催要綱 |

5. 議事概要

（1）開会

（2）説明

◆議題（１）「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について」について、事務局より資料 1-2 を説明、議題（２）「IoT ボットネットの現状について」について、吉岡構成員より資料 1-3 を説明。

◆構成員の意見・コメント

後藤主査）

C&C サーバへイブンや IoT ボットへイブンのような攻撃インフラを構築しやすい箇所があって、その辺りを攻

撃者側のエコシステムが上手く住み着きながら動いている印象だが、そういった傾向は世界的にはだいぶ認識されているものなのか。

吉岡構成員）

ある程度専門の方はどの辺りのクラウドサーバやクラウドサービスに C&C サーバや IoT ボットネットが存在するとか、バレットプルーフと言われるような対策の甘い部分に存在するかお分かりになるのかと思う。さらにそこにビジネスとしてどんどん住み着いている点もご存知の方もいらっしゃると思うが、まだあまり全体像が明らかになっていないと思っており、最後にご紹介したような攻撃者情報把握の取組をこれから行っていきたいと思っている。

河村構成員）

2 点質問があり、1 点目に個人の持っているルータ等が多く感染しているということがデータとして出てきているが、自覚症状というのは全くないと考えていいのか。2 点目に、あるサービスを攻撃するための一道具として感染端末が使われるというイメージだと思うが、消費者個人に関する被害はあるのか。ある場合には攻撃被害全体のうちどのくらいの割合で個人への被害が含まれているのか。

吉岡構成員）

感染端末の悪用のされ方によって違うと思うが、基本的には消費者は非常に気づきにくいと思う。そもそも主にルータ等が攻撃されるのも、ルータは一度設定したらどこにあるかも忘れてしまうようなものであるためで、もしサイバー攻撃をされていても気づかないということは大いにあり得る。ただ、サービス妨害攻撃というのは、大量の通信を行う攻撃に悪用されている時は機器の負荷は上がるので、体感的にネットが遅い、繋がらないというようなことはあるかもしれない。ただ、この図も示すように攻撃のアイドル時間も長く、年中 24 時間ずっと攻撃されているものでもないため、実感としてはあまり感じられないことが多い。加えて例えば私が今着目しているのはプロキシ系といった、他の攻撃に感染端末が悪用されるものが多く、その攻撃に加担してしまっていることはあるにしても、エンドユーザー自身が直接的に被害を受けないケースはやはり多い。一方で、全てが感染に気づきにくいという訳ではなく、例えばルータが乗っ取られた場合、正規の外部サイトにパソコンやスマートフォンでアクセスした際に、正規のサイトでない、不正なサイトに誘導されてしまう可能性がある。そこで ID とパスワードを入力してしまうと利用者の情報を取られるようなことや、不審なスマホのアプリのインストールを促されてしまうなど、そういった過去事例は起きており、エンドユーザーである家庭のパソコンやスマートフォンを使っているユーザへの影響も出てくる。

小塚構成員）

ログインによる侵入は比較的分かりやすいが、ログインせずに攻撃をするというのはどういうことなのか。そして NICT の NOTICE 注意喚起は基本的にログインの疑似攻撃をするということだと理解しているが、これがそうではない攻撃手法が多くなってきたということにとなると、どういう形の対策が考えられるのか。

吉岡構成員）

ログインしない攻撃というのは、そもそも IoT 機器についても機器の管理画面のようなものを表示するためにウェブのようなネットワークサービスが動いている。そこに不備があり、ある種のデータが送られると、特にログインをしなくてもいきなり管理者権限を取られてしまう攻撃が実際に多くあり、その場合にそのままマルウェアが送り込まれて感染してしまうケースが多い。例えば NOTICE 等でこういった不備を突いた攻撃が実際にできるのかどうかを実際に調べようとなると、これもある種の疑似攻撃のようなもので、害のない何らかの任意のプ

ログラムを端末上で操作してそれが動いたかどうかを確認するなどの方法で、本当にその攻撃が成立するかどうかを調べることになるが、その手法もかなり検討が必要なものではないかと思う。間接的に攻撃が成立するかを調べる方法としては、各機器のファームウェアのバージョンのようなものが通信の特徴から分かる場合があり脆弱性の有無を確かめる方法もある。バージョンアップするとこういう脆弱性が直っていく場合もあるが、このバージョンのファームウェアであれば脆弱性があるということが分かるものについては、疑似攻撃をしなくてもファームウェアのバージョンから当該脆弱性が残っているのではないかと推定することは出来るため、横浜国立大学の am I infected?というサービスで、間接的に推測してお伝えするというやり方をとっている。

小山構成員）

am I infected?のような、IoT 機器の感染状況を調査する仕掛けとして公開されているのは大変素晴らしいことです。このサイトの存在を感染の疑いのある人にどんどん周知すべきと感じた。例えば機器メーカーがユーザからセキュリティ対策について問い合わせを受けた場合など、am I infected?で一回健康診断的に機器の状況を見ていただき、その上でメーカーに相談するなど具体的な対策につながる活用方法が考えられる。どんどん周知普及していくべき。現在、どういう形で広報活動をされているのかを教えていただきたい。

吉岡構成員）

広報活動については大学でプレスリリースをすることが時々ある程度で、あとは NHK やいくつかのメディアで取り上げていただいた。NHK で報道された際にはインパクトが大きくユーザ数は急増した一方、急増しすぎてサービスが止まってしまったこともあったが、これまでそのようなワンショットで周知するだけであったためご協力いただけることがあれば是非お願いしたい。

小山構成員）

今後 IoT のセキュリティガイドラインを更新する機会をとらえて、「事業者がユーザに IoT 機器を提供する際には、保守運用の一つのお作法として、定期的に am I infected?のような診断サイトで感染状況を確認することを推奨する」など、強制力はないかもしれないがガイドラインを活用して普及啓発を進めていきたい。

田中構成員）
am I infected?では比較的リテラシーが高いユーザからの問い合わせが多いと思われるところ、それでも対応困難なケースが多いとのことだが、問い合わせをする意識の高さと技術的に是正ができることというのは必ずしもマッチしないということか

吉岡構成員）仰る通り関心があることと技術的に理解できることとはかなり差があると感じている。問い合わせは色々いただくが初歩的な質問が多い。例えばグローバル IP を元に注意喚起しているが家庭内のプライベート IP アドレスと違うといったものが多い。問い合わせいただいて一般にはこういう風に思うのかと学習してどう利用者に対処の方法を伝えれば良いかを考えている。

小山構成員）※チャットより抜粋
（事務局に対し）C2 サーバも攻撃先も海外にある一方で、攻撃している IoT 機器は国内にあるパターンの想定がされがちだが、攻撃先が意図的に日本に向けられた場合の対応が十分かを、安全保障の観点で検討すべき。キルネットの事例をみると、攻撃に慣れていない日本のサイトが狙われたとき、社会の反応は過剰になるため、あらかじめの検討が必要。

◆議題（３）「NOTICE の取組状況について」について、事務局より資料 1- 4 -1、井上構成員より資料 1-4-2、ICT-ISAC の引地氏より資料 1-4-3、NOTICE サポートセンターの沖本氏より資料 1-4-4 を説明。

◆構成員の意見・コメント
小山構成員）

NOTICE の取り組みを振り返ると、過去に脅威が顕在化した Mirai に対して注意喚起可能な機器を調査しながら対応されてきたと理解している。一方で通信事業者の立場でネットワークを見ていると、今国内で被害が出ている IoT ボットネットの一部である DVR 機器等で起きている大規模な DoS 攻撃が注意喚起の対象になっていないようである。今後は現在のリスクの高いボットネットから対策を進める方法も取り入れたらどうか。可能であれば、通信フロー分析などでボットネットの全体像を把握しつつ、注意喚起に加えてメーカーと連携した am I infected?の取組みや、サーバの通信を一旦切断するなどの対応と並行して、テイクダウンを行うという複合技で、ひとつひとつのボットネットの塊を確実に小さくし、効果を測定するというようなことをやってはどうか。

吉岡構成員）

小山構成員のご意見に完全に同意する。IoT ボットネットによる DDoS 攻撃は攻撃者の操作一つでいつでも国内に向けることができるため、安心できる状況ではなく、対策は継続的に必要。一方、異なる観点からの意見としては、NOTICE の活動は素晴らしく、それぞれのコンポーネントでそれぞれのご担当がしっかりと対応していただいたおかげで、きっちりとした注意喚起の枠組みが出来上がってこれだけのことが出来ていると思っている。せっかくここまでできた、多くのサイバー脅威に対して使えるシナリオの活用の幅を上手く広げられるような、全体としての活動の位置付けができると更に素晴らしい。最近サイバー攻撃のエコシステムに注意して色々な分析や観測をしているが、IoT に限らないところも含めて言うと、例えばランサムウェアは非常に問題になっているが、色々な組織からリークした情報がリークデータマーケットやランサム攻撃グループのコミュニティ・サイト等で出回っていて、その中に国内のものもかなりあると認識しており、これも注意喚起の対象にもなるかもしれない。情報の信頼性の問題などをどのように連絡していくかといった解決すべき課題があるとは思うが、少し幅広に活動を見ると相当にポテンシャルがある枠組ではないか。

齋藤構成員）

NOTICE 参加プロバイダーとしては現状で対応の限界にきているというように感じている。コールセンターの役割を良くしていく、ないしは新しい注意喚起の報告方法を検討しながら増やしていかないと、今の枠組の上に新しいインシデントに関する対応を追加するのはかなり難しい。一方で井上構成員のプレゼンで一点確認したいのだが、調査対象の識別符号を増やして注意喚起対象が一気に増えたタイミングが一箇所あったと思うが、これは一度しか行っていないのか。あるボットが問題となったタイミングでそれに対処したいという時にはおそらく常に新しい調査対象を追加していかなければいけないのではないかという気がするが、そうしたことを行っていないのは何か理由があるのか。

井上構成員）

識別符号の精錬は引き続き行っており、例えば調査対象の識別符号を 100 種から 600 種に増やした際も、IoT 機器のマニュアルを 2000 本程度読み込んでその中からデフォルトの識別符号を引っ張り出したり、ハニーポットで検出した今使われている識別符号等を使ったりして作成したものであり、今見ている限りでは ID・パスワードに関してはかなり良いリストができている。そのため今大きく識別符号を追加したからといって結果が大きく

変わるものではないと理解している。新しく出てきたDVR系機器もスキャンを行うものに関してはNICTER注意喚起に含まれるはずかつ、全てではないがNOTICE注意喚起の中にもDVR系機器も含まれているものもあるので、そういった意味では、識別符号が十分なのか、まだ外しているものがあるのかというのは、検討はしながら実施している。一点、建付けの問題として、識別符号をまた新たに増やすとした際に、総務大臣の認可が必要な実施計画書の変更が必要で、その手続に大体半年ぐらい時間がかかり、タイムリーな新しい対応をするときの一つのハードルでもある。（以下チャットより抜粋）また、調査実施機関のNICTとしては、調査体制の維持、人員確保も大きな課題となっている。

河村構成員）

一人一人のユーザが関わっていく部分に関し一消費者団体の立場から発言すると、現在古い機種も含めてたくさんのIoT機器があるなかで大変なご苦労をされていて、有意義な取組だと思う。今後国をあげてのDXだと言われていて、家庭でインターネットを使おうと思えばルータが必ず家にある上、家電もネットに繋がるものが増えていくだろう。例えば冷蔵庫使うのに専門知識は要らないはずだが、ネットに繋げると便利ですよと言われて繋げてみたら、脆弱性があると言われてしまうといったことが起こり、いたちごっこになってしまう。消費者の方で対処しなければいけない行為がだんだん少なくなるだろうというご発表だったが、機器メーカー側で対処する方向の中でも、やはり何らかのユーザの対処も必要であるとすれば、老若男女の国民がネットに繋がる機器をたくさん持つようになる状況では、リスクを下げる方法は極めて分かりやすいものであるべきで、直感的で分かりやすいパスワードの変更方法とか、そういったやり方を標準化するなど、誰にでもできる簡単な形にするということが必要。今後に向けて、消費者を巻き込むところについては、是非メーカーも巻き込んでの対処、機器に関するところは消費者がそれほど思い悩まなくても済むような仕組み、それが自動的なセキュリティパッチなのかファームウェアの自動的な更新なのかは分からないが、できるだけ今後に向けてはそういう方向を目指さないと、利用者に注意喚起するとしても限度があると思う。

後藤主査）

全ての課題の真ん中にある非常に大事なポイントだと思う。色々考えるところが多く、次回以降で皆さんのご意見をいただきたいのは、国境の問題というか、日本の中で考えても収まらない部分がたくさんある。ISP事業者やベンダも国内のサービスだけでなく海外サービスも一緒にやっているところもあり、ユーザもどこにいるか分からない状況では、国という単位では解決しない部分は増えていく。フロー情報の扱いやダークウェブの話はその典型かもしれない。そういうところに関して、何が制約になっていて、どのような解決手段があるのか、こういうところも次回以降、ぜひ議論できたらと思っている。

（3）閉会

以上