

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6回）議事要旨

1. 日時) 令和5年6月19日(月) 15:00~17:00

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、小山構成員、齋藤構成員、田中構成員、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6-1 「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とりまとめ」(案)

資料6-2 「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とりまとめ」(案)の概要

資料6-3 構成員等からの主なご意見

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5回 議事要旨

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とりまとめ」(案)について、事務局より資料6-1、資料6-2、資料6-3を説明。

◆構成員の意見・コメント

後藤主査)

事務局から、本分科会のとりまとめについて、親会に出した後は、総合対策2023に反映するとあったが、総合対策の中に入れ込んで一つにまとまるという理解でよいか。

佐藤サイバーセキュリティ統括官室企画官)

後藤主査の御認識のとおり、現在親会の方で検討されているICTサイバーセキュリティ総合対策2023の一部としてとりまとめ案を付け、併せてパブコメにかけることを考えている。

小山構成員)

今日の御説明にもあったが、構成員の皆様のコメントや意見を丁寧に取り上げ、それを矛盾なく組み合わせて

資料にまとめていただいております。この表紙にもあるとおり IoT ボットネット対策がいよいよ本格的に始まったかなというように思っている。従来の NOTICE のように、見えたものから順番に対策を行っていくのではなく、更に一步前進してボットネットの全体像を把握して、かつ複数の端末が一つの C&C サーバに命令を受けて C&C サーバがコロコロ変わって、いたちごっこが始まるということではなく、ボットネットを可視化する上で、対策の処方箋を考えていくというようなことが関係者の巻き込みにもつながるので、とても良い対策が始まっていくというように読ませていただいた。個人的な意見として、本気でボットネット対策をやるのであればボットネットに通し番号をつけて、C&C サーバがコロコロ変わっているがこれが「1 番」など、ボットネットの壊滅作戦の実施のためのナンバリングのようなことも含めて取組を進めていきたいと感じている。

井上構成員)

非常にとりまとめをきれいな形でやっていただいております。特に図 9、図 10 の方でステアリングコミティの立ち上げの部分と、将来的にこういった形で NOTICE のプロジェクトが発展していくという図を描いていただいて、NICT だけではなく、総務省や NOTICE に参画する ISP78 社に加え、機器メーカーや SIer、NOTICE サポートセンター、最後は利用者というように、全体的な取組であるということが明示されることは非常に良いと思う。既に参画していただいている各主体、これから参画されるエンティティの方々を含めて NOTICE を日本全体で回していっているという図になっていると思う。この点本当に感謝する。今後の対策案の、特に 18 ページの②利用者への注意喚起等の実効性向上において、1 行目「ホームページの充実等を含め NOTICE の情報発信を強化するとともに」について、NOTICE の取組自体についての情報発信・強化も非常に重要だと思っている。情報発信・強化に関しては、利用者への注意喚起の実効性向上が最終的なアウトプットになるので、それに繋がるということで文言的にはこれで大丈夫だと思うが、NOTICE の取組全体を国民の皆様を知っていただくことが非常に重要と思っている。2019 年の NOTICE の本調査開始の頃にメディア対応の影響でかなり炎上したこともあり、その結果 NOTICE の調査対象が縮減して進められたところもあるので、情報発信力の強化の中にメディア対応等も含めて考えていただければと思っている。

吉岡構成員)

かなり多角的な視点での対策が記載されていて素晴らしい内容だと思った。今後の進め方において国際的な連携も重要であると書いていただいております。本当にそのように思っている。やはり C&C サーバの多くが海外にあり、攻撃も国内外を跨ぐものが多い中、こうした取組が実現されると中々他では見えないものが日本は見えているというようになる可能性もあると思った。是非海外との連携も今後活発にして、日本のこの分野の貢献が更に広がると良いと思った。

後藤主査)

ネットは繋がっているものなので、グローバルな連携が非常に大事な取組だと思っている。完成度の高いとりまとめ案になっているようで、修正・指摘等が出ておらず、タスクフォースの構成員の皆様からは上手く多角的に幅広い視野でまとめたとりまとめ案になっているという評価をいただけた。

◆構成員の挨拶

井上構成員)

先ほども申し上げたとおり、次期 NOTICE に向けて非常に有意義な検討がなされたと思う。特に最初の NOTICE は NICT が調査を行って注意喚起を ISP に依頼し、そこで非常にコストがかかるユーザー特定を行い、最後に注意喚起を促すというモデルから始まったものではあるが、次期 NOTICE に関しては更に枠組みを広げて、様々

なエンティティの方々が参画をして日本全体を安全にしていこうという大きなプロジェクトと整理され、非常に心強く思っている。我々も注意喚起の精度や脆弱性に対する取組の精度を高くしていく所存なので、引き続きご協力のほどよろしくお願ひしたい。

河村構成員)

消費者の立場でここに出ているので、利用者への注意喚起のことについて一番意見を述べてきたところだが、色々反映していただいて感謝している。今後について、ID・パスワードに脆弱性がある IoT 機器があると繰り返し述べられているわけだが、効果的な注意喚起について、何回か前の会合でも、どうすれば実効性があるかというような発表があったかと思う。実際に利用者として読むと、ID・パスワードに脆弱性がない、つまり買った時から個別の ID やキーが付いているものは直さなくていいのではないかと感じる。大手メーカーの推奨機器というものだと思うが、真面目な人ほど買った時から一度も変えていないと心配するといったように、消費者の方が無駄に心配をしたりしないよう、まずは対応の必要がない人が分かる方法が必要だと思っている。それは実はそれほど簡単に分からない。今回、私はこれに参加してから色々なことが分かったが、私は使っているルーターのパスワードを変えたことなどないが、調べてみると大手メーカーで個別のパスワードが設定されているらしいということも分かった。ID・パスワードと繰り返し書かれているが、製品において「パスワード」という言葉は私が知る限りでは見たことがない。大体ここでパスワードに位置するものはキーと書かれており、ID も少し違う SSID と言われているなど、その言葉が何を指しているか分からない。注意喚起されている点が自分の製品のどの情報が分からないだけで、消費者の対処がストップしてしまったり、無駄な時間がとてもかかったりする。そのため、注意喚起の効果を高めるためには、製品にはこういう言葉も使われていますと書くなど、分かりやすくする必要があると思う。

小山構成員)

IoT ボットネットというのは、やはり DDoS 攻撃に悪用されうる身近な脅威である。2014 年くらいにも大規模なボットネットとしてホームルーターが踏み台となった犯罪基盤などが摘発されたようなこともあったが、あの頃から IoT 機器を何とかしなければいけないということで、当時の Telecom-ISAC を引継ぐ形で ICT-ISAC としても取り込ませていただいた。IoT ボットネットなどを可視化していく取組が始まったということが今回大きな前進に繋がっていくと嬉しく思っている。引き続きこの対策に力を尽くしていきたいと思う。皆さんとともに進められたらと思っているのでよろしくお願ひしたい。

齋藤構成員)

非常に素晴らしいとりまとめをいただき感謝している。期間中私の方はふわっとした発言をすることが多く、色々苦労させてしまったのではないかとと思うが、しっかり私の意見も拾っていただいた。今の小山構成員の話と重なるが、我々通信事業者としては今そこにボットネットを使った実際の機器が日々発生していて、これを何とかしないとイケないというモチベーションをもって今までも活動してきたわけだが、ここに示されたように今後実施しなければいけないことが明確になったので、それをまずは真摯にやっていきたいと思う。それだけではなく、将来のこととして、全体の像の中のどこかの切片だけ頑張れば対処すれば良いというものではないと思うので、この事象そのものの撲滅に向けて皆様と協力しながら今後も進めていきたいと思う。

田中構成員)

今回の分科会について、端末からネットワークに至るまで非常に多岐にわたる課題を議論し、そちらの結果を事務局の方で上手くまとめていただき本当に感謝している。報告書の中でも整理されているが、今回のプロジェクトは非常に多くの関係者が協調してやっていかなければいけない。特に利用者も含めて整理いただいたが、今回

上手くまとめていただいた取組を関係者一同で共有、啓発していくことが非常に重要だと改めて思っている。冒頭、事務局の方からもあったが、サイバーセキュリティを取り巻く脅威は非常に高まっている中、今回のまとめていただいた取組を関係者各位で着実に取り組んでいくことが解決に向けた近道かと思っている。是非引き続きよろしくお願ひしたい。

藤本構成員)

簡潔に分かりやすく取りまとめていただいている。私からは利用者への注意喚起について主にコメントをさせていただいたが、やはり注意喚起を受けて私たち利用者の認識や行動が変わらなければいけないというところが重要なポイントだと思っており、そういう行動が変わる伝え方というのはどういうものなのか私たち研究者も色々な研究の余地がある部分だと思っている。引き続きよろしくお願ひしたい。

吉岡構成員)

これだけのとりまとめをいただきまして改めて感謝申し上げる。様々な観点で非常に適切なこれからの活動の方針が述べられていると思っている。特に総合分析対策センターというものでIoTポットネットの活動の実態が見えてくること、それに基づく対策が進むことを期待している。今回のとりまとめのその先のことについて個人的に思っていることとして、こういった活動で攻撃の実態が分かってきて対策が進むということは素晴らしい。一方で、私も研究でこういうことをやっていると、毎日どうしてこのように絶えず攻撃がくるのかと今更ながら思うわけだが、攻撃は自然に起こるものではなく、攻撃者がいてモチベーションがあるからこそこれだけのことが起きているのだろうと思っている。よく言われるのは攻撃がビジネス化されているということで、どこかで稼いでいる人がいる、または稼いでいなくてもハクティビズムといったような形で何かを主張したい人がいるといったように、どうして攻撃が起こっているのかという背景や攻撃者のモチベーションに私自身は今すごく興味を持っており、そういう仕組みが分かるとどこで対策をすると攻撃者にとってのメリットが減る、例えば稼ぎにくくなる、住みにくくなるなどということを考えられる。まずは現状を把握することが大事だと思うが、その先にそういったこともあると漠然と思っているということだけ一言述べさせていただきます。

後藤主査)

皆様から非常に有益なご意見をいただいた。本分科会は構成員の皆様がステークホルダーを代表する方であったこともあるが、加えてISPの方、ベンダーの方から直接幅広くお話を伺えたため、分かりやすく、地に足がついたとりまとめになったのだと思っている。これからも継続的な取組が必要になると思うが、現場の方の本音というものをしっかり収集して取り組んでいくという姿勢が大事だと思っている。今後は親会のタスクフォースにて、総合対策のとりまとめになるが、そういう視点を大事にしてもらえればと思っている。

山内サイバーセキュリティ統括官)

今、後藤主査の方からもお話をいただいたが、1月から毎月1回ずつ5ヶ月間にわたって、集中的に色々議論いただいた。後藤主査、それから構成員の皆様には本当に忌憚のない御意見いただき感謝申し上げます。我々の今までのNOTICEで何ができたのか、できていなかったのかということも含めて、忌憚のない意見、ある種厳しい御意見をいただけたと思っている。それは私たちにとっては非常に意味のあることで、関係者の方、特にNOTICEにおいて実際に調査をするNICTの方々、注意喚起をしていただくISPの方々に加えて、SIerやベンダーとどのように協業するかについて、我々の資源をどう配分するかも含めて考えていく必要があると改めて思った。我々の目指すところについて述べると、ネットワークの安全性・信頼性の向上、それを妨げる要因になっているIoTポットネットの撲滅、そして、その構成要素になっている脆弱性をもつ端末や感染をしてしまった端末をいかに

減らすかということが我々の目標になると思っている。したがって、IoT ボットネットの可視化やそれをどう置き換えていくか、訴求をするかが、先ほど御指摘があったように一般の利用者に十分に伝わっていないのではないということも意識してこれから取り組んでいかないといけないと思っている。調べるための手段として NOTICE、NICT 法という不正アクセス禁止法の除外の規定を持っていて、これをどのようにするかということをするべき国会の場でも御議論いただいて、私たちもツールを備えた上で取り組んでいきたいと思っている。恐らく取り組んでいる最中にまた色々なことが分かってくると思うので、その節には構成員をはじめとする皆様の御協力、忌憚のない御意見をまた頂戴できればと思う。

(3) 閉会

以上