参考資料１

ICT サイバーセキュリティ政策分科会（第１回）議事要旨

1. 日 時）令和６年２月９日（金）13：00～15：00

2. 場 所）WEB 開催

3. 出席者）

【構成員】

後藤主査、新井構成員、栗原構成員、小山構成員、篠田構成員、蔦構成員、盛合構成員、吉岡構成員

【オブザーバー】

内閣官房内閣サイバーセキュリティセンター、内閣官房サイバー安全保障体制整備準備室、デジタル庁、経済産業省、地方公共団体情報システム機構

【総務省】

山内サイバーセキュリティ統括官、豊嶋大臣官房審議官（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、田畑サイバーセキュリティ統括官室企画官、牧野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】

仲上竜太（一般社団法人日本スマートフォンセキュリティ協会（JSSEC））、加唐寛征（トレンドマイクロ株式会社）

4. 配付資料

資料１－１　「ICT サイバーセキュリティ政策分科会」開催要綱
資料１－２　サイバーセキュリティの最近の状況及び ICT サイバーセキュリティ政策分科会について
資料１－３　スマートフォン/モバイルにおけるセキュリティ課題と JSSEC の取り組み（JSSEC）
資料１－４　サイバー未来図：ウクライナから学び、台湾有事を見据えて（トレンドマイクロ株式会社）（非公開資料）
資料１－５　NTT コミュニケーションズにおけるサイバーセキュリティの取組（NTT コミュニケーションズ）（非公開資料）
資料１－６　ICT-ISAC におけるサイバーセキュリティ対策に関する取組（ICT-ISAC）
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）議題

◆議題（１）「サイバーセキュリティの最近の状況及び ICT サイバーセキュリティ政策分科会について」、事務局より資料１－２、議題（２）「我が国を取り巻くサイバーセキュリティの情勢」について、JSSEC 仲上氏より資料１－３、トレンドマイクロ加唐氏より資料１－４を説明。

◆構成員の意見・コメント

吉岡構成員）

スマートフォンの脅威ということで、スミッシングや不正アプリの大量配布などが知られていると思うが、スマートフォンはいろいろなビジネスで使われているので、より深刻な脅威、企業等を狙ったスパイウェアや APT につながるような事例もあると思うのだが、そういったものを把握・観測する仕組みや取組はあるのか。

蔦構成員）

今回、モバイルエコシステムに関する議論についての言及があったが、今 Android はサードパーティーのものを認めているが、日本も Apple に対してもアプリストアを第三者が作れるようにという法案が出るという報道が出ている。その是非を議論する場ではないと理解しており、あくまでファクトベースの質問だが、もし Apple の方で第三者がアプリストアを経営できるというようになった場合に、こういった不正アプリあるいは不正なアプリストアが出てくる可能性はどれほどあるか、また、そういったものを防ぐため、あるいは減らすためにはどういった取組が必要になってくるか。

JSSEC　仲上氏）

１点目の御質問について、不正アプリの調査の観点で分析されているのか、脅威が深掘りされていないのではないかというような御質問だと理解しているが、不正アプリの調査については、JSSEC としては中々取り組めていない。もしかしたら御説明いただけるのかもしれないが、総務省においてアプリストア上のアプリケーションを調査する取組を進めていると伺っている。このような取組は非常に重要と考えており、特に多くの方が利用するアプリケーションには当然悪意を持って入れているというケースは少ないかもしれないが、例えば、適切なプライバシーポリシーがアプリケーション上は適用されていても、組み込んでいるライブラリは別のところに送ってしまっているというようなケースもあるので、こういった調査は非常に重要かつ国民にとっても知るべき情報が含まれた形にはなると思っている。一方で、深掘りの観点での非常に難しい課題として、動的解析も静的解析も、非常にハイレベルな知見を持ったエンジニアが個々に対処していく必要があり、例えばアプリケーションのストアでは、当然多くの場合、問題のない純粋な目的を果たすアプリケーションが大量に投稿されていく中で、すべてを確認しながら不正アプリを見つけていくのは非常に難しい作業であると思う。そのため、不正アプリを見つけていくための技術の進化の点では、これまでは公式アプリストアがやるべき仕事ということで中々事業化されることはなかった領域だと思うが、こういった不正アプリを見つけていくような取組やエンジニアの育成についてこれから考えていくべき課題になってくる。蔦構成員から頂いているアプリストア、モバイルエコシステムの議論について。まず、不正なアプリストアが出てくるかどうかという点については、基本的には表立ってたくさんのアプリストアが出てくるわけではないと思う。また、不正なアプリの流通を減らすための取組としては、先ほどの不正アプリをどのように見つけていくかという難しさに直面せざるをえないと考えているが、当初は当然新しいアプリストアが出ても、一般からアプリケーションを募集するというより、自分たちの企業体や自分たちのグループの中でのアプリケーションを配布するためにストアを作るといった目的のために出てくるものだと思う。その辺りは少し一般の一ユーザがアプリをアップロードして配布できるような公式アプリストアとは違う特性で制限も可能かと思う。とはいえ、先ほど申し上げたようなアプリケーションの中に含まれるライブラリが知らない間に情報を勝手に送信しているといったことに対して、できる範囲での調査、それからユーザからこの動作は不正でないのかというように指摘された場合の取り下げの取組といったところについては整備が必要だと思うので、そういったことについては、諸外国の動向を参考にしつつ、JSSEC としても方針を示したいと考えている。

新井構成員）※チャット欄より抜粋
スマホアプリについて、御説明いただいた不正アクセスやフィッシングの助長につながるアプリ以外にも、表向きは「家族や友人間でのファイル共有のためのアプリ」を標榜しつつ、実態は児童ポルノの温床になってしまっているものもあると聞くが、そういった表向きは正当な利用を標榜しているアプリについてどのような対処をすべきかお考えがあれば伺いたい。

仲上氏）※チャット欄より抜粋
位置情報の追跡やカメラをのぞき見するようなスパイアプリも表向きはセーフティや関係向上を謳って配布されているものも多い。DDoS サービスが負荷テストサービスとして販売されているように、一義的には使い方に責任の所在があると考えるが、被害者になりうる一般利用者側にそのような悪用が存在すること、事例があること、注意すべきことを啓発すべきである。モノを探すためのタグデバイスなども悪用が簡単に可能であり、技術進歩に伴う新技術の悪用とその対策を周知することがすぐできる取組だと考える。

新井構成員）

今般、米国において Volt Typhoon と呼称される国家支援背景のグループが同国の重要インフラに長期間にわたって潜伏していて、それを抑止したというような報道がある。こういった活動は、先ほど加唐氏から御説明があったような、事前にロシアに協力的なサイバー攻撃者がウクライナのインフラに対して攻撃し、サイバー攻撃による影響を与えることができる場所を事前に確保した上で、実際に攻撃を行っていることがロシアの侵攻発生の直後に起こっている状況があるということなので、いわば平時にそういったものを獲得しておいて、有事に攻撃を発生させるというようなことが実際に起きているということだと思う。実際にそういった報道が米国においても行われているような状況で、対策として、事前に潜行しているスパイのような方々がいるので、それに対してはクリアランスで対応することが重要であろうとご示唆いただいたが、それ以外にもこうした潜在化している脅威、サイバーセキュリティの世界だとスレットハンティング、脅威ハンティングと呼ばれているが、事前に何らかの形で進行しているかもしれない活動を通じて積極的に発見したり止めていくという活動は有効なのか。

盛合構成員）

インフルエンス・オペレーションのところで、一部の国ではこういうコミュニティが存在するということだったが、このようなコミュニティはどこが主導してやられているか、いくつか事例をお聞かせいただきたい。そして日本で、もしこういうものを立ち上げるとすると、どういうところが旗を振るとうまくいくと考えるかも併せて教えていただきたい。

蔦構成員）

いわゆるアトリビューションについて質問したい。主要な APT グループの話で、加唐氏のスライドの 7 ページくらいに APT29 や 28 など載っていたが、この辺りは日本の方でもいろいろとアトリビューションに関する取組を警察庁を中心にやっているという理解であり、具体的にどこまで本当に特定できるものなのか相場感を知りたい。また、特定することによって民間事業者にとってはどういう利点があるのかについてもコメントいただきたい。

トレンドマイクロ　加唐氏）

最初の御質問について、スレットハンティングがワイパーなどの攻撃に対しても有効かということだが、これは有効な事例がある。最初のサボタージュの事案のページで、1 番下に Industroyer2 というのを記載したが、その

事例では、その組織にマイクロソフトやESETのソリューションが入っていて、ある程度きちんとブロックして、攻撃の進行が深刻化しないようになったということが報告されている。そのため、あらかじめきちんとスレットハンティングをしておいて、弊社のようなものなど、セキュリティソリューションできちんと検知対応しておくと、たとえ入られたとしてもその後に使われるツールなどがもし検知可能であれば本当に深刻な被害までつながらずに済む可能性があり、おっしゃるとおりスレットハンティングはとても有効だと思う。次の御質問で、インフルエンス・オペレーションの対策のコミュニティはどこが主導しているかについて、私が知っている限りは、大きく進んでいる地域はバルト諸国と聞いている。ロシアからのインフルエンス・オペレーションをずっと昔から受けていて、古くからコミュニティが存在しており、どこが主催しているかは分からないが、ここには一部の弊社のメンバーも入っており、法執行機関や SNS などのプラットフォーマーも入っていて、お互いに協力し合っている。日本では現在おそらく内閣府が主導してインフルエンス・オペレーションのリサーチ、対策をやっていると思うので、省庁だけではなく、例えばXやMetaなどの一般のリサーチャーやプラットフォーマーも巻き込む形でやっていくと、何が広まっているかという事実のみではなく、誰が広めているかというアトリビューションというところまで行く可能性もある。そこまで行くと、より相手のモチベーションというのが分かって、対策に結びつきやすくなるので、もちろん政府主導でやりつつ、民間やプラットフォーマーが参画することが重要と思う。アトリビューションがどこまでできるかについての御質問に関して、まず民間企業の目線から言うと、ツールや攻撃基盤、被害者傾向などのクラスタリングが基本的な限界である。クラスタリングの結果が今表示しているスライドであるような APT29 や 28 など、いわゆる APT グループや intrusion set などといわれるものになっている。ただ一部の民間レベルでも例えばウイルストータルへのサブミッションの情報などから攻撃者が意図せずに自分の情報が漏れてしまうような情報をアップロードしていたりすることもあり、例外的に個人の名前レベルで特定できることもあるが、基本的にはツールなどのクラスタリングが限界点になっている。加えてそういった情報を法執行機関などに提供し、捜査という形で役立ていただくのが民間でやることかと思う。特定することによって民間事業者にとってどういう利点があるかについては、誰がどういう意図を持ってどこに対してどういう情報を用いて攻撃しているかという、攻撃のすべてをきちんと明らかにしておくことによって、将来どこに攻撃が起こる可能性があるか、どういう手法で攻撃が起こる可能性があるかの知見や予測につながるので、攻撃が発生したらどういう意図を持っているかというモチベーション分析がすごく重要だと思う。そのモチベーション分析にはもちろん誰がやっているかということが分かった方がより正確にできると思うので、アトリビューションの観点では、誰がやっているか、例えば法執行機関のように逮捕するという目的でなくてもきちんとできる限り分析しておくというのが重要かと思う。

トレンドマイクロ飯田氏）※チャット欄より抜粋
新井構成員の御質問に対する回答の補足として、潜伏する脅威に対する発見手法については、セキュリティ対策の基本だが定期的な検査がやはり有効だと考えている。ペネトレーションテストの再定義とカバレッジの変更が必要になるかもしれないが、潜伏している脅威を念頭に定期的に検査していくことが、見つける手段の一つになると考えている。

◆議題（3）「通信分野におけるサイバーセキュリティ対策の取組について」、小山構成員より資料１－５及び資料１－６を説明。

◆構成員の意見・コメント
後藤主査）
最後の 15 ページにおいて、ICT-ISAC がこれまで歴史的に取り組んできた関係各所からのいろいろな幅広い情

報を、他の重要インフラに提供するという役割まで説明いただいた。得られる情報の範囲は、現在はいわゆるサイバーセキュリティ、ネットワークセキュリティに近いところで得られたものだと思うが、先ほどのトレンドマイクロの話にもあったように、ネットワークではなく各所で地政学的に怪しげな動きなど、幅広い脅威情報にまで拡張していくことは可能か。

小山構成員）

例えばもう少し具体に想定してお答えすると、もしウクライナにワイパー攻撃が仕掛けられたときに、某国の IP アドレスを踏み台に攻撃したという情報があったとする。そういう IP アドレスの情報さえあれば、日本の通信で同様の IP アドレスから攻撃らしき通信があったかどうかを調べることができる。調べた上で、何時何分に某電力会社のインフラにも同様の通信があったという具体的な情報としてお渡しすることができる。従来は皆さん気をつけてください、この IP アドレスです、調べてくださいとアラートを出す方法が中心だったと思うが、今後は具体的にあなたはここで通信していましたといったところまで踏み込んだ情報発信・注意喚起が可能だと思う。そのため、重要インフラだけではなく、重要インフラを対象に海外のリスク事案に紐付いた情報をさらに具体化して届けていくような取組ができれば良いという意味で書かせていただいた。

蔦構成員）

最近 ISAC がたくさん増えていることをこの図だけを見ても思うところであり、そうなってくると ISAC 間の情報連携といったものも重要性が増してくるのだろうと思っている。かつては業界が違えば必要な情報が違うからあまり連携する意味はないといった話もあったかもしれないが、今日では、共有すべき情報というものは一定程度あるということでよろしいだろうか。また、そういった ISAC 間連携をしていくということになると、先ほど国際連携のところに記載されていたが、アメリカの方だと National Council of ISACs というか、とりまとめ機関的なところがあると思っているが、日本でも同じような機関はあった方がいいのかどうかというところについて、ご意見いただきたい。

小山構成員）

まず国内 ISAC 間で共有すべき情報があるかということに関しては、フィッシングなどそれぞれ業界特有の優れた取り組みが行われており、現状ではお互いの対策手法などをお互いどうやっているのか、情報共有させていただいている。主に 2 ヶ月に 1 回程度国内 ISAC の集まりがあり、ICT-ISAC がとりまとめをやらせていただいてきた。米国の National Council of ISACs のような専門のとりまとめの団体が日本で必要かというと、ISAC の数も多くないこともあり、そこまでの必要性は感じていない。むしろ共有する情報を具体的に流すことで輪が生まれて、その輪を回していくことで、事務局のミッションもはっきりしたものになってくると思うので、組織を作る前にこういった連携する具体的な動作を開始したいと考えている。

後藤主査）

先日の能登地震のときは通信インフラも被害を受けたが、フィジカルな災害とサイバーに係る問題が重なる可能性は十分あると思われる。今回能登半島地震の場合は分からないが、フィジカルな災害のときに、サイバーの面から ISAC 間の連携は貢献できるか、それとも自然災害などは別扱いの方がよいのかに関して、感覚的なことで結構だが伺いたい。

小山構成員）

現在の災害対策情勢において、フィジカルとサイバーの体制は厳密には連携していない。地震・台風等の災害で

は、通信事業者間でも共同復旧や、そのための事業者間調整を行うというのは日頃からやっており、ワークしていると思う。一方でサイバーに係る問題においても、災害対策時に連携が可能かということに関しては、サイバー攻撃が発生してしまうとインシデント対応しながら情報発信を行うことは相当難易度が高くワークしない可能性が高い。ICT-ISAC の取組としては、日頃の情報共有ツールとして攻撃観測のシステムを会員間で共有しながら、自分だけが攻撃を受けているのではなく、他も同時に受けていたというような裏取り情報を得ることで、お互いが動きやすくするという取組は行っている。きちんとした答えになっていないが、サイバーとフィジカルの情報共有を業界横断でしていくというのはまだ難しい、欧米でもできていないのではないかと思っている。

（3）閉会

以上