参考資料3

サイバーセキュリティタスクフォース（第 41 回）議事要旨

1. 日 時）令和 4 年 12 月 13 日（火）10：00～12：00

2. 場 所）オンライン

3. 出席者）

【構成員】

後藤座長、鵜飼構成員、岡村構成員、小山構成員、篠田構成員、園田構成員、辻構成員、徳田構成員、中尾構成員、名和構成員、林構成員、藤本構成員、安田構成員、若江構成員

【オブザーバー】

山田隆裕（内閣サイバーセキュリティセンター）、満塩尚史（デジタル庁）、渡邊貴史（経済産業省）、鈴木一弘（地方公共団体情報システム機構）、髙井祐樹（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、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、田畑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、高地官房サイバーセキュリティ・情報化審議官

【発表者】

井上大介（国立研究開発法人情報通信研究機構）、松尾早苗（日本マイクロソフト株式会社）

4. 配付資料

資料 41－1 「ICT サイバーセキュリティ総合対策 2022」等に基づく取組
資料 41－2 最近の無差別型サイバー攻撃の動向と対策（ＮＩＣＴ）
資料 41－3 国際的なサイバーセキュリティ・ボットネット対策（マイクロソフト）
資料 41－4 サイバーセキュリティタスクフォースの今後の進め方 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）「「ICT サイバーセキュリティ総合対策 2022」等に基づく取組」について、事務局より資料 41-1 を説明。

◆構成員の意見・コメント

岡村構成員）

説明の中で SBOM の話題が出ていたが、本タスクフォース構成員は技術系の方が大変多く、また SBOM に関し

ては ISO やアメリカ大統領令等で状況が変化しているため、本タスクフォースにて今後、適切な方に簡単に SBOM についての説明の機会をいただくようお願いしたい。

◆議題（２）「最近の無差別型サイバー攻撃の動向と対策」について、NICT 井上氏より資料 41-2、議題（３）「国際的なサイバーセキュリティ・ボットネット対策」、について、マイクロソフト松尾氏より資料 41-3 を説明。

◆構成員の意見・コメント
後藤座長）

Digital Crimes Unit（以下 DCU）の活動規模について、技術の専門家や法務部門と一緒に活動しているということだが、大体どのような規模であるのか、機密でなければ教えていただきたい。

マイクロソフト　松尾氏）

DCU 自体はさほど大きい組織ではなく、おそらく 100 人いないくらいと思う。マイクロソフトの法務部門がグローバルで 2000 人ぐらいおり、そのうちコマーシャルリーガル担当や政策渉外担当以外が DCU という組織に含まれる。

中尾構成員）

二点質問がある。一点目に、CT の Crawlers&Emulators の話をされていたが、マイクロソフトはいわゆるエッジ側である、マイクロソフトの色々な製品でほぼ正確な C2 サーバの情報を時間軸でかなり的確に把握されているのではないかと思うが、正しいか。そういった C2 サーバの情報は例えば総務省などの関係機関等にご提供いただけるのか。二点目は、マイクロソフトの Threat Intelligence Center にて様々な取組を行っているのはよく理解したが、ディフェンダーでデータを取ってただそれを解析しても国家の関与は見えにくいのではないかと思うが、どのように判断されているのか。

マイクロソフト　松尾氏）

DCU の観点での回答となるが、もちろんエッジ側で色々な情報の収集はしている。マイクロソフトのディフェンダーが起点となり、(スライド図の)マルウェアのコンフィグレーションという矢印のとおり、DCU が使っている Crawlers&Emulators の方にフィードしている。DCU 側では、ターゲットとしている特定のマルウェアの C2 サーバがあり、組織としてなかなかの投資にもなるので、戦略的優先事項の高い Necurs とか Trikbot のような例については、特定のアクションを取りにいく前提で DCU が使っているクラウド上の仮想空間に感染しているような状況を作って（Emulators）その通信をクロールする形（Crawlers）となっている。技術的なところは私も完全に見えているわけではないが、件数に関してターゲットを結構絞ってアクションを行っている。例えば Necurs だと、それらが使っている特定の暗号 SSH コマンドを分析することで C2 の通信を特定したり、どこにどういった隠れたインフラがあるかを分析するために、マイクロソフトだけでは得られない、色々な通信事業者が持っているフロー解析のようなものも適宜情報共有いただきながら分析しているという理解である。この C2 サーバからの通信に関する情報をお渡しできるかについては、DCU が追っているものに限定して、Necurs への対応時以降可能となった。テイクダウンしきれずに残っている C2 サーバや、今後ターゲットにするため狙いを定めているマルウェアに関しては、C2 サーバからの通信を前述の Emulators 環境に受けているので、CTIP というプログラム等を通じて関係者に共有している。

岡村構成員）

１点目に井上さんのご発表に関して 26 ページの国産セキュリティ製品の運用・検証については、大変強く期待しているので、今後更にお進めいただくようお願いしたい。２点目には松尾さんに対する質問で、資料 41-３の１ページ目の右側に民事訴訟とあるが、差し支えない範囲でどういうケースを想定されているのかということを教えていただきたいことと、日本の法律で欠けているもの、こういうものがあればもう少し実効性が確保できるのではないかということがあれば教えていただきたい。

NICT　井上氏）

国産セキュリティ製品の運用・検証については、現在、6 企業で主にどちらかというとベンチャー企業が多く、是非この製品検証を通じて国内あるいは国外にも通用する製品を出していけるよう引き続き努力していきたい。

マイクロソフト　松尾氏）

ご紹介したようなテイクダウンにあたり、民事訴訟という手法を用いているのは世界の中でもアメリカのみである。一次的には、被害者はマルウェアに感染したコンピュータのユーザであるが、マイクロソフトが知的財産権を有する Windows に対する攻撃であるという法的整理を行い、マイクロソフトとサイバー犯罪者との間に争いがあるという主張をしている。その際どのような理屈を使っているかについては、いくつか実際に訴状が公開をされている。例えば、日本でいう商標法に当たるランハムアクト上の侵害行為や著作権法違反、契約に関する不当な介入等、いくつかの法的な理論を使って、まずはマイクロソフトとサイバー犯罪者の間に法的な争いがあるという主張をしている。ランハムアクトの例では、マルウェアを仕込む際に小さいファイルのようなものを書き込んだりすることがあり、そのファイルをクリックするとマイクロソフトのロゴが表示されたりするので、マイクロソフトが商標を取得しているものが許諾なく勝手に使われた、という主張をした。著作権法の例として Trikbot の時は、サイバー犯罪者がマルウェアを仕込む際に、通常マイクロソフトの Windows 上で、合法的なアプリケーションが動作するために使用されるべき SDK（System Development Kid）というツールを悪用していた。本来であれば、マイクロソフトとの契約に基づいて、アプリケーションの開発者が Windows 上で SDK を使用して、アプリケーションを Windows 上で動作させるという状況になる。そこで、有害な目的を持って SDK を使ってマルウェアを Windows 上で動作させるということ自体が SDK をマイクロソフトの許諾なしに勝手に使うことであるので、マイクロソフトの著作権を侵害しているという主張をした。契約に関する不当な介入の例では、マイクロソフトとお客様の間に Windows を使用することでサービスを提供しているという契約関係があるところに不当に介入しているなど、アメリカ法の理屈に基づいていくつか並べている。このようなケースで民事訴訟の手法を使う場合のマイクロソフト側の利点として、サイバー犯罪者が法廷に現れることはまずないので、著作権法違反にあたるかどうか、法廷の場で細かい主張を繰り広げることにはならない。裁判所も、これは明らかに有害な行為が行われていて、マイクロソフトの主張もそれほど珍奇なものでもなく、もっともだと判断した場合に、Ex ParteTRO(仮処分のようなもの）を出してそのサイバー犯罪者の犯罪インフラを潰す。最終的にはサイバー犯罪者は法廷に現れず、デフォルトジャッジメントでそのまま決定が最終化される。法律の仕組みが異なるため、日本ではなかなか使えない手法である。

岡村構成員）

質問に関連して、日本でも著作権法でフィッシングサイトを潰した事例はある。アメリカ法の理屈に基づいてということなので少々一般化しにくいところがあるが、日米の知的財産法制度の違いというよりは、広く普及している Windows の SDK に関する権利者たるマイクロソフトさんだからこそ可能な方法であると思った。

小山構成員）

NICT の井上さんとマイクロソフトの松尾さんに関係する ICT-ISAC の取組をご紹介したい。前身の Telecom-ISAC 時代から NICT はもちろんだが、マイクロソフトとは非常に密に連携させていただいている。その中でもマルウェア対策、昔々のファイル共有ソフトの Winny に感染する Antinny が日本中を混乱に陥れた時も通信事業者と連携していただいてマイクロソフトの MSRT という、アップデートする時にマルウェアを駆除するツールを使って根こそぎ削除していただくような取組を行ったり、通信事業者からの注意喚起によるマルウェア感染数の減少をマイクロソフトから情報をいただいたりしていた。さらにサイバークリーンセンターというボットネット対策の取組においてはマイクロソフトと同じような形で連携し、ボットネットタスクフォースという、グローバルを巻き込んだマイクロソフトのボットネット対策の取組にも関わってきた。今般、総務省の第 4 次とりまとめにより、C2 サーバの通信フロー分析ができるようになったので、フロー分析の取組とマイクロソフトの説明にもあった全世界を網羅している端末のセキュリティ対策と連携ができないか検討をしており、来週にはマイクロソフトと ICT-ISAC で議論の場を設け、通信事業者あるいは放送といったインフラ事業者とマイクロソフトで何かできないかディスカッションする予定です。この検討結果は本会議に共有させていただきたいと考えており、総合実証の中で出てきた C2 等の IoC データを NICT に更に共有するようなことが、将来の認定協会業務の中でできれば、セキュリティ対策に広がりが出てくると思う。引き続き関係者の皆様と連携させていただきたい。

名和構成員）

松尾様へのご質問です。今日説明いただいた国家アクターは、米国と価値観を共有しない国や地域の支援する攻撃グループのことを指していると思う。具体的には日本の防衛白書にある通り、ロシア、中国、北朝鮮、イラン、一部確か韓国も入っていたかと思う。少し気になるのが、私の観点として、日本企業が海外拠点に多数ある中で現在米国あるいはイギリス等が行っているサイバーオペレーションあるいは国家のアクターに関する観測をされているのか、あるいは観測と分析の結果を日本の国益のために企業や政府に共有いただけることはあるのか。

マイクロソフト　松尾氏）

マイクロソフトが追跡している国家アクターに関して、マイクロソフトが得られる最大の情報は、マイクロソフトのインターネットにおけるサービス上のもの、すなわちクラウドサービス上で観測できる国家アクターからの攻撃ということになる。ウクライナにおいては破壊的な攻撃、ワイパーのような攻撃があったが、これまで国家アクターが関与している攻撃というのは、諜報活動が主流であるため、メールシステムが狙われることになる。クラウド上であれば、我々は、パスワードスプレー攻撃などを用いて、お客様のアカウントを乗っ取ろうとする試みを相当量把握することができる。逆にクラウドではなくてオンプレだと、基本的には状況が分からない。マイクロソフトのデジタルディフェンスレポートで、ロシアの国家アクターによる攻撃や北朝鮮が行っているような暗号資産を狙う攻撃などかなり詳細に紹介している。このレポートは、クラウドから得られるインサイトに相当依存している。また、こうした情報を政府に共有しているかということだが、まずマイクロソフトが最初に通知するのは攻撃を受けたお客様である。MSTIC チームが追跡しているとある国家アクターからのパスワードスプレー攻撃があったことや、実際にアカウントが乗っ取られて入られたことなど、そのお客様に対して通知している。アカウントが乗っ取られ、システム内に入られる前に通知をすることを目指しているが、残念ながら一部入られたりするようなケースもある。いずれにしても攻撃が判明したらすぐに直接そのお客様に通知をするというのが基本スタンスである。その後、お客様との間の守秘義務の関係から、より一般化されたデジタルディフェンスレポートのような形で我々のインサイトを公のものにするということになっているので、政府の皆様にどのお客様が攻撃をされたということを我々が直接お伝えすることはないが、政府が我々のお客様だったとして、攻撃を受けていれば、直接通知を行うということになる。

名和構成員）

米国やイギリス、NATO、ドイツなどにいる国家アクターの攻撃のレポートが見当たらないが、それに対して見つかった場合は日本の企業に教えていただけるのか。

マイクロソフト　松尾氏）

基本的方針としてはそのとおりと聞いている。ただ、例えばアメリカの国家アクターがターゲットにしているような国を想定した場合、例えばイランの場合には、我々がその国でのサービスオペレーターではないという状況がある。マイクロソフトはクラウド上から得られるインサイトをもとに分析を行っているので、我々がクラウドサービスを提供していない国々に対して、アメリカやイギリス、NATO 加盟国等が行っている攻撃というのは我々には分からないということに基本的にはなると思う。

藤本構成員）

資料 41-２、13 ページにあるようにユーザの努力で対策することが困難というのは非常によくわかるが、一方でユーザの方々のセキュリティへの関心も以前に比べて高まっていると感じている。しかし、セキュリティの専門家の方々が一生懸命説明してくれるけれども使っている言葉がわからないというような話もよく聞く。ユーザも一緒にセキュリティ対策に取り組んでいくことを考えると、先ほど松尾様のプレゼンの最後にもあったように、例えば販売代理店に確認をしていただく形で少しでも適切な機器が接続されるような試みは行われているのか。また、そういったことは可能か。

NICT　井上氏）

一般ユーザにどうやってリーチしていくのかというのも非常に重要な課題である。実はこの DVR/NVR の件に関しては、国内の販売店、代理店の方とも実際の脆弱性があるという話からファームウェアを新しく作成し、展開してほしいというところまで話をしていて、一部の機器に関しては最新のファームウェアを出していただき、それを更新すれば大丈夫というところまで対応している。加えて、脆弱性届出についても実は NOTICE の活動の一環で 100 件以上の脆弱性届出をしており、CV になっているのが 24 件くらいある。そうした形で脆弱性を潰しながら代理店にも話をして、ファームウェアをアップデートしていただくところまで対処している。ただ、資料でベンダーに更に協力してほしいと書いているのは、やはり一部協力的ではないというか、ほとんど協力してくれないベンダーや代理店もあるので、一緒に努力していただくような取組を今後も進めていきたい。

辻構成員）

３点質問したい。１点目に STARDUST で得られた攻撃情報（主に IoC 情報）はどのような活用がされているのか。何かしらの形でメンバーではない方でも入手可能な方法が現在はあるのか。ないのであれば今後予定はされているか。２点目に am I infected?は、とても良い取組だと思うが、恥ずかしながら最近知った。利用回数を見てもまだまだ少なく感じるので、何かしらプロモーションをしたほうがいいように思う。また、そもそもで申し訳ないがネーミングが一般的に分かりにくい印象。３点目に NOTICE で得られた情報は今後、別の活用方法は検討されているか。また、別の活用を念頭に置き NOTICE の仕組みを応用するといったことは検討されているか。何かしらの方法で収集できた情報についても集計し注意喚起に利用することがよいと思う。

NICT　井上氏）

１点目に STARDUST の情報だが、今のところ Co-Nexus A の中のメンバー間で情報共有をしていて、どういった攻撃が最近見られているか、あるいは環境を作るにあたってどういうところを気にして作らないといけないか

など、攻撃者が見ているかなり深いところまで情報としてみえるようになっているので、そういった情報を Co-Nexus A の中で共有している。外向きにも情報を出していきたいと考えていて、今年度末か来年度頭ぐらいにホワイトペーパーのような形で、STARDUST で得られた情報や観測のノウハウなど、そういったところをまとめて情報を出していきたいと考えている。2 点目に、am I infected?に関しては、横浜国立大学が主体でやられていて、ネーミングが分かりにくいということは吉岡先生に言っておくが、これも総務省から予算を出されているミティゲートからも成果として出ているものなので、何らかの形で更にプロモーションしていった方が良いとは私も思う。そのあたり、タスクフォースで出たご意見として吉岡先生に事務局からもお伝えいただければと思う。3 点目に、NOTICE で得られた情報の今後の活用について、特定アクセスでログイン試行して得られた情報というのは我々の中でも最高度の秘密情報として扱っているので、それ自身を外に出すということは NICT 法上もできない。NICT 職員のみしかアクセスできないという建付になっているので、特定アクセス情報自身は使えないが、それ以外の周辺情報に関しては、先ほどの色々な代理店にお話をしたり、ベンダーとお話ししたりという情報として使っていたり、アカデミックなペーパーを書く情報としても中で使っていたりする。更にこういう使い方をしたいという議論については、NOTICE を 5 年後どうするかという論点も含めて今後議論したいと思うので、辻構成員からもこういった使い方をした方がいいのではないかといった色々なご意見をいただければと考えている。

鵜飼構成員）

NOTICE、NICTER の取組だが、状況が可視化されて注意喚起ができるといった運用が確立できたのは非常に大きな貢献かと思う。今後 Mirai 系のボットだけではなくランサムウェアなどでも問題になっている VPN が大きな社会課題になっているが、こういったところについても有用な基盤になったのではないかと思う。是非今後はこういったところに注意喚起の幅を広げていただければと思っている。一方で、先ほど少し話があったが、注意喚起がなんとなくこれだけでは限界もあるかと思っていて、対策については更に一歩踏み込んだ施策を検討していく必要があるのではないか。具体的にはメーカーのファームウェアの更新とユーザへの周知を促していくというのも重要だと思う一方で、メーカーもコスト的な課題もあるので、なかなかそういったことも難しい。コストがなかなか価格に転嫁できないといった問題もあると思うので、なにか今後その点有用な施策も検討していかれるのもよいのではないか。

NICT　井上氏）

実は NOTICE というか NICT の中の法律と実施計画で、この ID とパスワードの入力、つまり特定アクセスと呼んでいるものに加え、付帯業務で脆弱性をもった機器の調査等もやっている。例えばリフレクターとして使えるような機器の日本の中での調査や、先ほどもお話にでた VPN 機器の調査は行っていて、本当にまずいものに関しては、ものによっては例えばある ISP の中で特定の機器が相当数接続されていて、そこに対応していただく形で脆弱性を持つ機器の数を数千台規模で減らしたりしている。公表されているグラフは注意喚起の取組結果を示す一つのグラフだけだが、その裏で色々な付帯業務を行っている。そういった業務を更に深めていくことと、行っていること自体も外向きにアピールしていきたいとは思っているが、そのあたりは総務省とも連携しながら、どういった出し方していくというのは議論していきたい。

篠田構成員）

人材育成オープンプラットフォームについて、資料 41-2 の 27 ページに「NICE Framework に基づいた演習教材の段階的整備」とあるが、セキュリティコースをすでに持っているような高校・専門学校・大学・大学院といった教育機関のカリキュラムの一部になることを想定しているか。また、例えば日本の工業大学・工科大学等でセキュリティコースを設置したいが、リソース/手がかりがないといったところも、NICT に相談の余地があるの

か。

NICT　井上氏）

これは両方ある。既にセキュリティコースを持ちその一部のカリキュラムという形でやっている教育機関もある。長崎県立大学ではセキュリティコースが既にあり、その中で授業の一環としてこういった演習環境を使って高校生向けに感染のデモなどを行っているが、学生がこの CYROP を使って学んでいるということで、既にコースがある学校で演習を実施するというパターンがある。あとはご相談を受けながら教育教材を一緒に作成しているところというのは、実は他に全くリソースがなく、学科で一人の先生が授業や演習をしてくださいと言われているようなところと連携をして、その先生が簡単に使えるような教育コンテンツなどをお話しながら作っているという両方のパターンがある。

若江構成員）※チャット欄より抜粋

VPN の脆弱性調査を既に実施していると聞いて驚いた。ランサムウェア攻撃被害などの状況を考えても重要なことだと思うが、調査の結果をどのように活用しているのか今度教えていただきたい。

◆議題（４）「サイバーセキュリティタスクフォースの今後の進め方」について、事務局より資料 41-4 を説明。

（3）閉会

以上