サイバーセキュリティタスクフォース（第 46 回）議事要旨

1. 日 時）令和 6 年 1 月 24 日（水）15：00～17：00

2. 場 所）オンライン

3. 出席者）

【構成員】
後藤座長、井上氏（小山構成員代理出席）、鵜飼構成員、岡村構成員、栗原構成員、篠田構成員、園田構成員、辻構成員、戸川構成員、名和構成員、林構成員、藤本構成員、吉岡構成員、若江構成員

【オブザーバー】
内閣サイバーセキュリティセンター、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】
盛合志帆（国立研究開発法人情報通信研究機構（NICT））、新井悠（株式会社 NTT データグループ）

4. 配付資料
資料 46－1　「ICT サイバーセキュリティ総合対策 2023」に基づく取組
資料 46－2　NICT における最新の取組状況（NICT）※非公開資料
資料 46－3　生成 AI 普及の先にある未来線を予測する（NTT データグループ新井氏）※非公開資料
資料 46－4　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）議題
◆議題（1）「「ICT サイバーセキュリティ総合対策 2023」に基づく取組状況」について、事務局より資料 46－1 を説明。

◆構成員の意見・コメント
鵜飼構成員）

C&C サーバの検知について少しずつ成果が出ているのはとてもよいと思うが、出口をどのように考えているか。C&C サーバが検知できれば、例えば、未観測のソフト事業者や我々のようなマルウェア対策の仕組みを作っているベンダをうまく活用して、日本全体でマルウェア脅威を減らせるのではないかと思うが、何か出口プランや

活用方法などについて具体案が決まっていれば共有いただきたい。

佐藤企画官）

ご質問いただいた C&C サーバの利活用については、ICT-ISAC が中心となり新たにワーキングを立ち上げて検討している。様々な利活用方策が議論されているが、例えばインテリジェンスとしての活用や注意喚起の他、C&C サーバの遮断やテイクダウンなどは制度面との関係も出てくるが、そういった方策も含めて議論が進められている。ある程度整理できた段階で、来年度から試行的なアクションを実施することなども含めて検討を行っている状況。ただし、利活用までに至る課題も多く、例えば C&C サーバの在処はすぐに変わってしまうため、情報の新鮮度が非常に大きな課題になっている。C&C サーバを検知してからリストを共有するに当たり、どれほど悪性度が高いかの評価も含めどういった情報を付加すべきかの検討や、一連のオペレーションの迅速化などをしっかり行わなければいけない。まだ様々課題がある状況だが、利活用方策についても具体化すべく取組を進めていきたいと考えている。

吉岡構成員）

2 点質問があり、C&C サーバの検知について、事業者間で検知した C&C サーバの重なりが少ないという話があったと思うが、この意味を確認したい。事業者 A で検知した C&C サーバの情報を使って、事業者 B や C で保管する機器や C&C サーバを検知するのに役に立ちにくいという意味か、あるいは重複がないということはそれぞれ脅威が独立しているという意味なのか、そうではないのかというところをお聞きしたい。もう 1 点は 14 枚目のスライドの政府端末情報を活用したサイバーセキュリティ情報の収集・分析に係る実証事業について、情報を収集・分析するということが記載されているが、この取組は分析までなのか、それとも最終的には分析を活かして実際に防御することに活用するという対策まで行うことが目標なのか。

佐藤企画官）

まず、事業者間で重なりが少ない理由に対する御質問について、資料 7 ページ目の「昨年度末までの成果」の中央の図のとおり、事業者 A・B・C で重なりがあった C&C サーバが実質 6 個であり、今年度その理由についても深掘りをして分析を進めている。各社の検知をするためのツールの違いや、ネットワークの特性の違いなども理由として考えられる。今年度の実証では共通のシード情報を使って分析を深めていき、重なりが少ない理由についても更に明らかにしていきたいと考えている。

吉岡構成員）

重複の有無の判定は検知された C&C サーバの IP アドレスなど、C&C サーバそのもの自体の重複を確認していたということか。

佐藤企画官）

御指摘のとおりで、IP アドレスベースで重複があるかないかを判断している。

吉岡構成員）

検知した IP アドレスを各事業者のネットワークにマッチングした上で検知されるかどうか見ると、検知される C&C サーバが重複しているかだけではなく、得られたリストを各 ISP に適用した時にどれくらい適用されるかを見ることで相互に利用ができると思うが、そういった分析は行っているか。

佐藤企画官）

投影されているスライドについては、まだそこまでは実施していない段階の結果である。その結果を踏まえて、現在、見つかった C&C サーバについて共有トライアルを実施している。実際にフロー情報を分析し、C&C サーバを検知しているのは 3 社だが、この 3 社に 9 社加えた合計 12 社で、検知した C&C サーバのリストを共有し、各社のネットワーク上の情報と照合してみることで、どういうことが見えてくるのか検証している。この共有トライアルも 1 回だけでなく、複数回実施している。成果についても現在精査をしているところで、どこかの段階で御説明できればと考えているが、現時点では、それほど重なりがないということが分かっている。一方で、数としては少ないものの、色々な事業者から活動状況が見えていると C&C サーバもあるので、どう評価するかなども含めて分析を行っている。

酒井参事官）

14 ページの CYXROSS について、こちらの目標が情報収集・分析までなのか、あるいはそれを活用することまでなのかという御質問について、当面の目標は情報の収集と分析ということになる。現在エージェントの開発が終了し、一部政府システムで実証を開始している。ここで収集したデータをもとにこれから NICT で分析作業をトライアルしようと思っている。おそらくこれにしばらくは時間がかかるだろうと思う。ただ将来的に分析結果をどう活用するかは当然意識しており、政府のシステムの防護に役立てていきたいということも考えている。ただ現時点で政府のシステム防護はシステムを調達した各省庁の役割、それから政府の共通システムを開発しているデジタル庁の役割、政府のシステム全体を防護している内閣サイバーセキュリティセンターの役割、それぞれに役割があるので、この情報をそれぞれがどのように活かすことができるか、また連携するときにどのような体制が望ましいのかといった点については、実証を通じて評価を行い、改めて計画を作っていくことを検討している。

戸川構成員）

NOTICE について、無事に継続できることになったが、継続していくことが非常に重要だと認識している。その上でもう一歩踏み込んだ話として IoT セキュリティを強化、担保することにおいては、ネットワークを通じたセキュリティと同時にイントラネットの中で、非常に多種多様な IoT デバイスがある場合に、どのようにセキュリティを担保するかも考えていく必要がある。NOTICE の取組が前提だが、そういったものを考えていく必要があり、そのためには後半の方で説明があった教育の話とも通じるかと思う。利用者の意識や教育、イントラの中でのセキュリティの担保に関する研究開発も進めていく必要がある。そういった仕組みづくりを含めて総合的に IoT のセキュリティの強化を図っていただけると幸い。

藤本構成員）

19 ページの説明について、国際連携の中で非常に多くの方々が一堂に会する形で演習に参加されているのは素晴らしいと思った。。私どもも、大学院で教育をするなかで、情報セキュリティに関する学習は、短期間では終わらないという観点から、卒業された方々が交流する場というのが非常に大事だと考えており、セキュリティの知識やノウハウをアップデートするためにも、参加された方々が引き続き交流していけるような取組も重要だと考える。そのような取組があれば、教えていただきたい。また、これからということであれば、参加された方々の交流を支援するような仕組みがあれば良いと思った。

田畑企画官）

19 ページの AJCCBC について、この研修に参加した卒業生同士で交流する場を設けたりといった取組も本取組と併せて行っている。

辻構成員）

C&C を検知した情報について、テイクダウンだけではなく悪用の確認を、民間含む多くの様々な方ができるようになんらかの形での情報公開、提供などは行うのか。探せば見つかるような既知のものであったとしても総務省から注意喚起などの形をとることで広く伝えることができれば、リーチしやすく響きやすいのではないかと思う。色々な機器の情報などでも発信することによって伝わり方が変わってくるので、そういったところの活用をもう少し考慮いただければ嬉しいと思っている。

名和構成員）

スライド番号 9 に記載のあるソースコードについて、令和 4 年度行政事業レビューシートにおける評価においては、挙動に関する技術分析など、と慎重に言葉を選んで表記している。特に、ソースコードについてはプログラムまたは開発者の方において著作権または特許権で守られているはず。このアプリ⇒ソースコードのこのソースの意味は何か。もう一つコメントとしては、ユーザ情報が「？」との記載があり、アプリから出るものに加えて、そこから不適切な展開や共有、漏洩しないかといった考察やオープンソースデータを含めた情報分析も必要だと思った。

酒井参事官）

こちらにあるソースコードというものは、ソースコードが直接事業者から享受できるものではないので、いわゆる調査目的でのリバースエンジニアリングの範囲内で行うということになる。今回の調査においては、ツール等を活用した静的な分析、それから通信を活用する動的な分析それぞれを行っているが、いずれも調査・分析目的で合法的な範囲内ということで、法律の有識者のコメントもいただきながら進めている。

岡村構成員）

著作権法改正で非享受目的の分析などは適法になったので、その点だけ伝えさせていただく。

篠田構成員）※チャットより抜粋
P18 について、CYDER と CYNEX には今後も期待している。Global Certification のような国際的なレベルを示せれば、ユーザーの能力比較も容易になるだろう。P20 について、日 ASEAN での能力構築が充実してきていると感じる。しかし、トレーニングの内容や CTF 問題の作成に苦労しているという話も聞く。以前お伝えしたとおり、国内外に協力できる専門家がいることを再度お伝えする。また、米国や英国などの有志国が提供する研修プログラムと書いているが、英語での提供ということで適切だった等、理由は気になった。英語だけであれば SecurityCamp が他国と共同で提供している東アジア・ASEAN 諸国のトレーナー達は英語で提供できているので、候補として考えられると思う。P24 について、多くの演習や CTF の開催、全国的な展開は素晴らしいと思う。SECCON が開催する地方 CTF や SecurityCamp が開催する地方ミニキャンプ等からセキュリティ関連業務に就職する若者も少なくない。これらの継続と改善が P23 での現状と課題の解決につながると信じている。 ※参考までに、EU 政府主催の CTF「ECSC」は、CTF とトレーニングを通じて若者の能力開発、そして副次的効果として国家間の関係強化が図られている。ICC のアジア予選 ACSC では昨年オンライン CTF に 1,400 名が参加するなど規模は大きいが、EU のようなトレーニング提供までは至っていない。攻防戦ではアジアチームが優勝するなど潜在的にアジアの若者は能力が高い。ASEAN 地域の意向を尊重することが大切だが、世界のそうした試みと協力すれば、より多くの人にリーチし、能力開発やエコシステム構築に繋がると思う。

佐藤企画官）

篠田構成員の御指摘は 3 点ともそのとおりで、活動を充実させるべくしっかりと対応してまいりたい。特に AJCCBC について、取組を広げていくためにはより多くの関係者を巻き込んでいく必要があると認識している。

名和構成員）※チャットより抜粋
スライド番号 9 について、リバースエンジニアリングは、日本を含め多くの国々において特定の条件下で合法とされていることは承知している。これを尊重して、エンドユーザーライセンス契約（EULA）においても、「リバースエンジアリングの制限は、適用法令と矛盾する場合には適用されません」などの表現が追加されるようになってきている。しかし、一部において、適用法令の存在を尊重しない EULA が存在している。そのようなところに慎重かつ丁寧に対応にしていく姿勢が必要であると思う。個人的に懸念しているのは、係争までいかなくとも、外国から「不必要な」または「他の目的で」抗議が発生すること。特に、ネット上に広く公開される資料には、他国や他国の特定企業を刺激しない配慮も必要ではないか。以上、外国でデジタルフォレンジックの実務経験からの意見である。

佐藤企画官）

御指摘の点を踏まえて進めてまいりたい。

◆議題（２）「最近のサイバー攻撃の動向と対策」について、NICT 盛合氏より資料 46－２、NTT データグループ新井悠氏（より資料 46－３を説明。

◆構成員の意見・コメント
井上氏）

説明の中で調査スキャンが増えているという話があったが、スキャンが増えていることの社会的な受け止めを御存知であれば教えていただきたい。増えていることによってある程度はネットを使う時は仕方ないという認識が増えているのか。長期的にも増えているかと思うが、以前であればモバイルに繋がっているものは課金パケットに繋がるので絶対そのようなものは製造できないという雰囲気であったが、最近の変化を御存知であれば教えていただきたい。

NICT　盛合氏）

社会には一般ユーザや機器の提供者など様々な意識があり、利用ユーザの認識の変化についてのアンケートといったものは実施していないが、調査スキャンが増加している時代ならではの対策のアプローチとして、守る側の意識としては、御紹介した ASM という考え方から、自組織のセキュリティの脆弱性の状況を収集・把握することもできるようになってきている。

辻構成員）※一部チャットより抜粋

Shodan、Censys、ZoomEye といったような公開されているような行為のためにやるものもいくつかあるかと思うが、Mirai で見たところの国別の偏りなどはあるか。また、防弾ホスティングについて、スキャンの特徴から同一かつ定期的にスキャンをしてきている、攻撃のためにスキャンをして、負荷脆弱性で攻撃するリスクをつくっているような活動などをもし分析をされているようであれば追加情報を教えていただきたい。

（以下チャット欄より抜粋）管理用 UI の公開については、CISA の BOD 23-02 でも取り扱いについて言及され

ているが、認証云々の前に不用意に公開しないことが推奨される。そちらのまとめなどもあるか。もし、ないのであれば認証、脆弱性の前に行うべきセオリーとも言えるものであるため把握と対処についての注意喚起があるといいと思う。

岡村構成員）

Mirai の感染ホスト数の話について、Mirai は御存知のとおりソースコードがオープンにされていて、今も感染数が増えているという認識だが、これだけまだ Mirai の対応が出来ていないということはベンダの認識が薄いのか。Mirai がまだ感染燃え盛っていることを世間に向かって明確化しなければならないと思うが、御意見を伺いたい。

若江構成員）

岡村構成員の質問と少し似ているが、22 ページの対策は何年も前から言われている基本的なことで、ユーザ側が注意することでリスクを緩和できるのにもかかわらず、それができていないために攻撃者にとって入れ食いのような状態を作り出していることも改めて分かった。やはり啓発の課題、届けられるべき人に情報が届いていない問題を痛感し、NOTICE の活動はベンダや設置業者、利用者ごとに適した啓発の強化とセットでやることが不可欠ではないかと感じた。NICTER Blog や X でのポストには色々な情報が入っているが、例えば特定の機種など、注意しなければいけないような問題が出た時に、それをお伝えするような専門のアカウントを作っても良いのではないかとも思った。警告するだけのアカウントがあると皆フォローするのではないかと思う。

吉岡構成員）

これだけの分析をされるのは大変なことだと思う。私も同じような研究をしている意味で素晴らしい内容だと思った。また、データに基づいてここまで調べ、それが対策にも繋がっているということで素晴らしいと思った。最後 AI の話についても同じように地に足を付いた活動を期待している。

NICT　盛合氏）

辻構成員からの国別の分類の御質問について、この 90 の調査スキャン組織の中には横浜国大などセキュリティ研究をしっかりしている研究室、あるいは組織もある一方で、怪しいところもあれば、実体を伴っていないところもある。先ほど防弾ホスティングについてお話ししたが、法規制を受けない国にサーバを置くことでサイトを保護しているところもある。例えば海外に置かれているサーバには日本の著作権法や法律が適用されないということで、置かれやすいサイトとしてはオランダや旧ソ連の地域といったところがある。そういう意味ではそういったところに偏りがある。それ以外には研究や調査などカテゴリごとに分布が違う。岡村構成員からの Mirai の感染が増えているという御指摘について、しっかりとユーザ及び IoT 機器の製造者に意識を高めていただくことが必要というのはまさにおっしゃるとおりで、やはりそこが対策されていないので、Mirai、攻撃者によって脆弱な侵入口を見つけられて Mirai に感染してしまい、ホスト数が増えるということになっている。NOTICE について来年度も継続的に調査・対策を行うことになったが、これまでと違う点として、IoT 機器の製造事業者とも連携して対策を促すことを今後強化していく必要があると考えているので、そういった活動を通じて Mirai に感染するホスト数の削減に寄与できれば良いと考えている。続いて、若江構成員からの御指摘について、22 ページで対策をいくつか述べたが、これらも十分に周知されていないところがあると思うので、こういったところも周知活動していき、具体的なアクションへつなげられるような動きを行っていきたい。吉岡構成員からもコメントありがとうございます。NICT にもこういう解析を行うチームのメンバーを一人ずつ増やしていって定期的に分析

した結果を、速報性が求められるのはXを使ったり、定期的に四半期ごとにNICTER Blogという形で出したり、年間まとめてNICTER観測レポートを出したりと、様々な形で発信しているので今後も続けていきたい。

※チャットより抜粋
辻構成員、調査スキャナの国別のパケット数のデータはこちら。
https://blog.nicter.jp/2023/10/nicter_statistics_2023_3q/#%E8%AA%BF%E6%9F%BB%E3%82%B9%E3%82%AD%E3%83%A3%E3%83%8A%E3%81%AB%E3%81%A4%E3%81%84%E3%81%A6

若江構成員）

32ページの解析をどのように行うのか詳しく伺いたい。

NICT　盛合氏）

この文字以上のところの詳しいところは、今日は準備できていないため、これに関連する論文をお送りする。

※チャットより抜粋
p.32だが、こちらで発表している。国立台湾大学との共同研究です。通信事業者の力を借りるのではなく、ユーザの機器等に蓄積されているアクセスログの分析を行う。
https://ieeexplore.ieee.org/abstract/document/9838653/

後藤座長）

NOTICEの件も含め、同じような取組を海外に協力を求めて展開するという活動というのは構想にあるか。

NICT　盛合氏）

吉岡先生と一緒に、デルフト工科大学やインターネットサービスプロバイダと提携してIoT機器のセキュリティを向上する取組についてエコシステムをどのように回すかを一緒に調査してまとめた論文がトップカンファレンスで採択されたりしている。海外でもまだそれほど数は多くなく、日本のIoT機器調査の取組は珍しく、そこまで出来ている国々が少ないと聞いており、発表すると非常に関心高く質問等を受ける。

園田構成員）

先日新井さんと直接議論させていただいた点だが、フィルタレスの生成AIというのは相手方が使いだしている現状において、制度上何かを担保しながらでも、生成AIを使った研究をできる仕組みを整えておかなければ攻撃者側に先行されるばかりだと思う。

（以下チャット欄より抜粋）悪意あるフィルタレス生成AIと同等のものをこしらえて、既存の例えばフィッシングフィルターをすり抜けるような手口サンプルが出た際に類似のものを多数生成するような体制を作っておけば（そしてその生成データをフィッシングフィルター側にフィードバックできる仕組みを構築できれば）、特に和文の場合、犯罪的な試みの可能性をかなり潰せるのではないかと思う。そのために社会制度などで何か担保できれば世の中の役に立ちそうな気がする。ジェイルブレイクプロンプトもフィルタレス生成AIに生成させて可能性を潰すのもよいかもしれない。

吉岡構成員）

規制や倫理規制について、その倫理性の自体の是非もあるのだが、そもそも規制しようと思ってもできるのか、

アライメントなどが本当にできるのかというところが土台ではないか。

NTT データ　新井氏）

規制について、いわゆる法律による規制があるが、法令の規制の強さもあると思うが、どれほど効果的なのかも考える必要がある。今のところ諸外国の法令を見てもそこまで踏み込んでいる例はなく、EU の AI 規制は民間事業者が開発している AI を対象にしていて、そもそもサイバー犯罪者がつくっているものは規制の対象外だったりするので、現在の法の枠組みそのものや法の枠組みを考える上での議論そのものが各国まだ出来ていない状況なので、先んじて考える領域ではないかと思っている。

吉岡構成員）

技術的な点から Jailbreak の話について、確かに ChatGPT なども不適切なものをブロックしていると思うが、本当に止められるのか。何を答えていいのか、何を答えてはいけないかというのを AI に学ばせて規制する際、本当に規制の意図したとおりに技術的にコントロールできるのかという興味から質問した。

NTT データ　新井氏）

完全にブロックするのは無理だと思う。何らかの形で漏れてしまうものが出てくると思われる。現状では自然言語だけで質問する形式だがマルチモーダルといって、複数の入力が可能になる生成 AI も登場しつつあり、自然言語に加えて、たとえば画像を入力して画像に対する問いを答えなさいという生成 AI の場合、画像に対してはキーワードによるフィルタリングが中々かけられないため規制できないはずだ、という研究もされ始めている。今後そうした課題に対する研究を重ねられていく領域であると思う。

後藤座長）

今、御提示いただいた課題は今日の委員会だけで議論しきれるものではなく、この後の今後のタスクフォースの進め方で今後取り上げていくものである。大事な問題提起をまとめていただいた。

◆議題（３）「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 46－４を説明。

◆構成員の意見・コメント
若江構成員）※チャット欄より抜粋

議題１とも関係するが、総務省におけるサイバーセキュリティ関連予算の中で、生成ＡＩの脅威対策に関連する予算はどのようなものがあるのか（偽情報対策を除いて）教えていただけると助かる。

佐藤企画官）

現時点においては、生成ＡＩの脅威対策に関する予算は含まれていない。今後新たに立ち上げる分科会での議論も踏まえながら、政府として取り組むべき施策について生成 AI の関係も含めてしっかり検討を行ってまいりたい。

（3）閉会

以上