ICT サイバーセキュリティ政策分科会（第 9 回）議事要旨

１．日　時）令和 6 年 6 月 14 日（金）14：00～16：00

２．場　所）WEB 開催

３．出席者）
【構成員】
後藤主査、新井構成員、上原構成員、小山構成員、篠田構成員、辻構成員、蔦構成員、盛合構成員

【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（統括担当）、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、道方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

【発表者】
井上大介（国立研究開発法人情報通信研究機構（NICT））、

４．配布資料
資料９－１　NICT サイバーセキュリティ研究所の取り組み（NICT）（一部非公開資料）
資料９－２　これまでの論点整理（案）
参考資料１　ICT サイバーセキュリティ政策分科会第 7 回 議事要旨
参考資料２　ICT サイバーセキュリティ政策分科会第 8 回 議事要旨

5. 議事概要
（１）開会

（２）議題
◆議題（１）「CYNEX、CYXROSS 等について」NICT 井上氏より資料９－１を説明

◆構成員の意見・コメント

上原構成員）

CYXROSS Agent の導入拡大について、現在の範囲の見込みはどの程度を想定しているのか。懸念点として中央省庁はもちろんのこと標的型は弱いところを狙った攻撃である点を踏まえると地方支分局が心配である。また、狙う側のインセンティブについて、独法等が保有している情報を狙う方が魅力的であると考える。範囲として独法等に広げることはできないか。
旧帝大から論文が出てこないという御指摘の通り、日本の研究費は旧帝大を中心に供給される構図を考えると、サイバーセキュリティの方向に向いていないという意味となるため非常に問題であると考える。一方、学問の自由があり、恣意的にすることはできないが、1 番の問題点は東大や京大という最も研究費が厚い 2 大大学の基幹ポスト内にセキュリティ分野の講座がないということである。その時点で既にルートが絶たれているため、問題意識を持っていた方が良いと考える。

盛合構成員）

CYXROSS については、各省庁におけるセキュリティ対策を海外製品のみに頼るのではなく、国産の技術で守れる仕組みを、今後は政府全体の端末に導入していけるように各省庁に御理解・御支援をいただきたい。
AI の安全性・セキュリティに関して、これからは国際競争力の強化が重要であるため、MITRE や NIST 等の海外各研究機関との連携を是非進めていただきたい。

新井構成員）

研究用データセットの公開について、サイバーセキュリティの用の AI を使用した課題解決においてデータセットが古いという問題があり、研究者が古いセットを使用して新しいものを作る際、利益喪失が課題となっていた。

従って、NICT がデータセットを公開することにより、AI for Security の領域にカジュアルに参入できることが大きなポイントであると考える。データセットの作成は非常に労力を要するためである。また、機械学習の検知力を知るためには自分でデータセットの作成から始める必要があるため、研究者にとって非常にストレスであり、また、大きな障壁であるが、そこを低減してくれる試みであるため非常に期待している。

辻構成員）

STARDUST で得られた情報について、攻撃手法やツール等のデータ公開はしているか。していなければ公開する予定はあるか。
WarpDrive について、現在のユーザー数や収集情報数について伺いたい。
AI について、現時点で AI 研究の先にはどのような課題解決に繋がっていくのかを伺いたい。

NICT 井上氏）

上原構成員への回答。現在は中央省庁への導入を目標としており、まずは、中央省庁において情報の有効性の検証を行うところから始めている。CYXROSS CORE の体制整備と各省庁への調整が終了次第、順次拡大を考えている。
旧帝大に集まっている非常に優秀な学生にとってセキュリティ分野を選択する機会が限られていることは大きな課題であると考えている。

新井構成員のコメントについて、データセットが古い問題は非常に重要な問題点である。USENIX においても古いデータセットを使用して評価をした論文が多くあったが、最新のデータセットを使用した検証はサイバーセキュリティ分野で非常に重要であるため、データセットの提供だけでなく、リアルタイムのデータを使った検証を行える環境構築を考えている。
Co-Nexus E には現在民間企業のみに参加していただいているが、今後は大学内で作成されたプロトタイプやアルゴリズムを NICT へ持ち込んでいただき、NICT においてリアルタイムでデータの検証を行っていけるように、大学の先生方へ話をしていきたいと考えている。

辻構成員への回答。
STARDUST で得られた情報を詳細にまとめたレポートを Co-Nexus A 内で共有しているが、現状外部への公開は行っておらず、情報公開をするためのエフォートが足りていないことが課題となっている。現在今年度中の公開へ向けて準備中である。
WarpDrive のユーザー数はモバイルと PC 合わせて約 2 万人であり、収集情報数は 1 回 Web へアクセスすることを 1 と数えると 100 万 URL アクセス／日であったが、第 2 ・ 3 弾アップデート後は 700 万 URL アクセス／日となった。
NICT における AI 研究について、リアルタイムでのデータ解析はまだまだ難しさがあり、リアルタイムに動く機械学習技術を作ることが大きな課題である。例えば、自然言語翻訳をサイバーセキュリティ分野に適合させることにより、翻訳精度が高くないロシア語や中国語などを綺麗に翻訳することで、今まで見えてなかった情報がリアルタイムに翻訳され、解析者に渡すことが可能となり得ることが AI for Security の一つである。Security for AI に関しては、LLM を使用し、セキュリティ情報を要約して一般のユーザーへ分かりやすく伝えるという話があるが、現在公開されている LLM を使用して要約してみたところ、精度的にアクショナブルな情報として使用するにはまだまだであった。作る際・使う際のリスク、AI を使用する際にやはり気にしないといけないことを日本の中で共有できるような研究開発を行うことが AI for Security だと考えている。

小山構成員）

アクティブサイバーディフェンスの検討が進んでいるが、欧米並みの法制度が整った前提で、NICT の研究開発や人材育成の方向性や可能性について伺いたい。

蔦構成員）

CYXROSS Agent の今後の導入範囲について、独立行政法人の他に、サイバーセキュリティ基本法に規定する指定法人（J-LIS、年金機構等）や、行政機関以外にも国会・裁判所などの官の方面への展開が必要であり、また、民の方面への展開も視野に入れても良いのではないかと考える。
AI のセキュリティに関する検討についても NICT を中心に進めていただきたい。

篠田構成員）

今までサイバーセキュリティ領域においてデータセット等の情報共有が出来なかった理由は何故か。
省庁からの情報収集について、端末から得られたデータセットのみでは狭い意味での脅威情報データとなるため、

それを磨き上げて使える状態になった情報を収集されるという認識で良いか。

コメント
自給率を上げていくことにリスクがあったが、そのリスクを下げるという取組に賛成する。
北米にサイバーセキュリティ拠点を作ることについては大賛成である。色々なプランニングがされる場に日本人がいることを望んでいる。

NICT 井上氏）

小山構成員への回答。アクティブサイバーディフェンスについて、NICT としてどういった貢献ができるのかはこれから検討していかないといけないと思っており、慎重に考えないといけない。アクティブサイバーディフェンスを行うためには、相当なアトリビューション能力やエビデンスが必要である。まずは STARDUST などの取組を通じて、人間の攻撃者が背後にいる攻撃をしっかりと観測して、アトリビューションできるケイパビリティを日本に蓄えることが、アクティブサイバーディフェンスにも繋がる第一歩ではないかと考えており、総務省とも連携をしながらどういった形で貢献していくべきかについて慎重に検討していきたい。

蔦構成員への回答。CYXROSS のガバレッジについて、日本全国の政府関係機関に導入することが目標である。中央省庁への導入で得られた情報を元に経験を積み、範囲の拡大を計る。独法の国研については国研協という協力体制があり、そちらへ色々なアラートデータの提供を始めている。様々なアプローチから国全体を守る取組を進めて行く必要がある。

篠田構成員への回答。データセットの公開について、NICT のセキュリティポリシーで規定されているため外部公開ができなかった。こういった問題を解消していくことも課題である。
CYXROSS の情報について、エンドポイントで収集された情報を NICT 内の収集情報と照らし合わせ、ポリッシュされたアクショナブルな情報、よりエンリッチされた情報として省庁に提供する。

後藤主査）

データ収集について、他の組織や海外からなどの複数のデータから新しい知見を得ようとする際の事例や問題点はあるか。

NICT 井上氏）

CURE というデータを集めるリポジトリーでデータマッチングを行っている。CURE の中で複数のデータの繋ぎ合わせを行っているが、データの種類は増加していくと同時に、繋ぎ合わせのマッチング方法や AI を使った自然言語処理など、かなり工夫が必要であることが分かってきた。その辺りも大きな研究課題として引き続き取り組んでいく。

なお、上原構成員は 15 時 00 分、議題（１）の自由討論終了後に途中退席された。

◆議題（２）「論点整理（案）について」、事務局より資料９－２を説明

◆構成員の意見・コメント

原主査）

上原構成員より事前にいただいたコメントを代読。
「全般によくまとめていただきましてありがとうございます。
おおむね問題はございませんが、1 点だけ、NOTICE の役割についてご意見いたします。
役割を再定義するにあたっては IoT 機器のセキュリティ向上を通じ、サイバー攻撃の発生を防ぐとなっていますから総合的な IoT セキュリティ対策のために活用する方向を強く打ち出すことで、今後の取り組みの方向性を、IoT ボットネット対策に閉じることなく幅広に取り組みを行うような書きぶりにできないでしょうか。
例えば喫緊の課題としては、VPN ルータの脆弱性検出と通知にも活用するなども可能なのではないかと思います。以上です。」

蔦構成員）

サイバー安全保障分野での対応能力の向上に向けた有識者会議において、能動的サイバー防御という文脈で通信の秘密との関係やインフラ関係事業者における官民連携などがテーマになっているということで、本分科会とテーマが重複する部分もあるのではないかと思っている。それを踏まえて、サイバーセキュリティ戦略本部の重要インフラ制度と経済安保推進法の基幹インフラの取組などとどう連携していくかという点も可能な限り明確に

した方がいいのではないか。
クラウドセキュリティ・トラストサービスは非常に重要なサービスであるが、それ自体は重要インフラというわけではないため、重要インフラに関する記述に出てくるのはやや唐突感もある。影響範囲も考慮し、重要インフラに準ずる重要性がある旨を報告書内に明記しても良いのではないか。

篠田構成員）

SecHack365 等の取り組みでサイバーセキュリティ人材体制強化を進めている部分や、地域セキュニティなどを通じて省庁を超えて横断的に協力していることをもう少し記載しても良いかと考える。
国際連携について、東南アジアや ASEAN には講師となる強い人材が多くいるため、そういった人材が AJCCBC に協力、参入できる体制作りを継続して進め、様々な協力関係の構築により政策の強化に繋がると考える。

小山構成員）

C2 サーバの検知・対処の推進について、フロー情報分析事業者の検出共通性は高くないというデータが出ている。この「多くの事業者が参画することで、より多くの C２サーバが検知できる可能性。」の意味は「多くの事業者が持つフロー情報を統合的に分析することに価値がある」と認識をしているが、もしそういうことであればそう書いていただいた方が今後の取組に繋がるような具体的な方向感が出てくるのでないか。

盛合構成員）

AI とセキュリティの「関係省庁・機関と連携しつつ」という記載について、AI の安全性（AI Safety や AI Security）に関して各国で色々なガイドラインやフレームワークが出来つつあるところであるので、「各国の関係機関」という表現も入れてはどうかと思った。

後藤主査）コメント

幅広い分野でサイバーセキュリティの取組が増えてきた中で、AI、PQC 等のホットな話題もあれば、重要インフラの取組のようにしっかり国を支えていかないといけない取組もある。それと同時にクラウドの使い方に関するガイドラインも非常に重要であり、また、地域セキュニティや普及啓発なども有効である。特に昨今のセキュリティの事案を見ると、最先端の話も大事であるが、昔から地道にやっていくべきであったところが漏れていて、抜けていて大きな事故になってしまったものもあるということで、総務省の役割が増えてきたという印象がある。そういう意味で今後も全体の取組を拡大していただければと思う。

佐藤企画官）

上原構成員への回答。
NOTICE をより幅広い取組にできないかという点について、NOTICE は IoT ボットネット対策を主眼として取り組んでいるプロジェクトであるが、その上で VPN ルータの脆弱性が見つかった場合には対応を行っていくことで役立てるようにしていきたい。

蔦構成員への回答。
ACD 等の安保関係について、有識者会議が立ち上がって検討が開始されたが、具体的な検討は始まったばかりであるため、現時点で本分科会と連携することは難しい状況である。ただし、平時から対策を行うことは日本のサイバー安保能力の向上に繋がると考え、今回取りまとめた４つの取り組みがサイバー安保に貢献するというメッセージを取りまとめにおいてしっかりと打ち出していきたい。
データ流通基盤に関しては、ご指摘の通り取りまとめの段階において、重要性をしっかりと記述し、唐突感が無いように記載していく。

篠田構成員へ回答。
人材育成については、求められる人材のレベルが様々であるため、記載ぶりを工夫したい。地域セキュニティについて、政府機関だけでなく地域において普及啓発を行っている民間の機関との連携を行うことで相乗効果を図ることが非常に大切であると考えている。
国際連携について、AJCCBC についても活動を拡大しており、有志国等の関係者が増加している。そうした状況の中で、様々な関係者が参画し内容を充実させることで、地域に貢献できるような活動にしていくことを我々も目指しているので、しっかりと取り組んで行きたいと考えている。

小山構成員への回答。
現在は各社で分析した C2 サーバリストを、ICT-ISAC で深掘り分析を行っているが、更に統合的に分析を行えるようにすれば更なる有益なアウトプットが出る可能性があるため、取りまとめ案に記載していきたい。

盛合構成員への回答。
国内の関係機関や関係省庁、AISI 等との連携に加えて、諸外国の様々な取組やガイドラインとの連携は必要不可欠であるため、その旨取りまとめ案に記載していきたい。

後藤主査への回答。
新しい話も大切であるが、地域セキュニティ等、地に足のついた取組を継続して行っていくことも非常に重要であり、取りまとめ案ではもう少し明確に記載をしたい。

(3)閉会

以上