サイバーセキュリティタスクフォース（第47回）議事要旨

１．日　時）令和７年９月１日（月）13：00～15：00

２．場　所）WEB開催

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、鈴木構成員、園田構成員、辻構成員、遠山構成員、戸川構成員、徳田構成員、中尾構成員、中島構成員、名和構成員、林構成員、森構成員

【オブザーバー】

内閣官房国家サイバー統括室、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】

三田サイバーセキュリティ統括官、赤阪大臣官房サイバーセキュリティ・情報化審議官、水間サイバーセキュリティ統括官室参事官（総括担当）、道方サイバーセキュリティ統括官室参事官（政策担当）、成瀬サイバーセキュリティ統括官室サイバー・経済安全保障情報分析官、神谷サイバーセキュリティ統括官室企画官、梅城サイバーセキュリティ統括官室企画官、鮫島サイバーセキュリティ統括官室統括補佐、中村サイバーセキュリティ統括官室参事官補佐

【発表者】

庄司周平（内閣官房国家サイバー統括室参事官）、新井悠（株式会社NTTデータグループ）

４．配布資料

資料47－１　「ICT サイバーセキュリティ政策の中期重点方針」に基づく取組状況
資料47－２　サイバー対処能力強化法及び同整備法について(国家サイバー統括室)
資料47－３　サイバーセキュリティ領域における AI の趨勢・動向
(NTTデータグループ新井氏)(非公開資料)
資料47－４　AIセキュリティに関する検討について
参考資料１　「サイバーセキュリティタスクフォース」開催要綱
参考資料２　「ICTサイバーセキュリティ政策の中期重点方針」(本文)

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政策の中期重点方針」に基づく取組状況」について、事務局から資料47－１を説明。

◆構成員の意見・コメント

遠山構成員）コメント

放送事業は、サイバーセキュリティ基本法における重要インフラに指定されており、あらゆる状況下でも放送を継続させることが重要な業務である。現状は専用機器や専用回線を使ったスタンドアローンのマスター設備を使用しているが、今後放送設備の IP 化やクラウド化が進むことを踏まえると、セキュリティ対策もより一層重要になる。ICT-ISAC の放送設備サイバー攻撃対策ワーキンググループでは、放送設備の IP 化やクラウド化を踏まえたセキュリティ対策の強化や従業員のセキュリティ意識の向上を図るため、放送設備サイバー攻撃対策ガイドラインの改定作業や、放送事業者を対象とした放送設備のリスクアセスメントに関する勉強会の開催検討を行っている。こうした取組により、放送分野全体の安全性・信頼性が確保されればと考えている。

戸川構成員）コメント

ICT サイバーセキュリティ政策の中長期重点方針に基づいた取組を、こうした場で適宜報告いただくことは、サイバーセキュリティタスクフォースの構成員にとっても有益であり、また、政府が実施している内容を確認するという意味においても、非常に重要であるため、引き続きお願いしたい。
また、「２．サイバー攻撃対処能力の向上と新技術への対応」については、AI とセキュリティをうまく利用する取組に対して、実務面においても研究開発面においても注力していく必要がある。
また、AI for Security の文脈において、レッドチーミング等を考慮した最先端セキュリティ技術の活用や、AI 同士が連携して検知を高度化する研究開発も含め、一歩踏み込んで実施することが非常に重要であり、継続的に実施いただきたい。
加えて、NOTICE は非常に重要な取組であるため、引き続き実施いただきたい。

中尾構成員）コメント

放送分野におけるクラウド化及び IP 化は、2028 年を目途にその導入が検討されているが、こうした取組を進めるにあたっては、安全性の確保が不可欠であるところ、クラウドの利用においては、クラウドサービスを提供する側と利用する側の両面から対策を講じなければならない。クラウドサービスを提供する側への対策については、内閣府が中心に進めている ISMAP や総務省の検討内容を参考に、安全にクラウドサービスを提供できる事業者を選定すべきである。また、ユーザー側も、総務省のガイドラインに適合する運用を行う必要がある。
また、放送設備の集中化にはリスクがある。放送設備を一箇所に集約すると、サイバー攻撃等を受けた際に、システム全体に影響が及ぶ可能性がある。そのため、完全に一点集中化するのではなく、バックアップや二重化といった対策を講じ、様々なインシデントを想定した設計にすべき。

篠田構成員）

地域 SECUNITY の取組は、地道に継続していくことが重要だと考えられる。また、各地域ではプログラミング教室や競技オリンピックなどさまざまな活動が推進されており、プログラミング講習の一環としてセキュリティ教育を取り入れることで、参加者が集まりやすくなる等の傾向はあるならば検討いただきたい。
一方、国内外ではたとえば競技オリンピックの世界大会やアジア大会、今年度 NCO が実施している国際 CTF 競技大会「International Cybersecurity Challenge (ICC)」やアジア大会のような国際的取り組みもあり、地域レベルの活動と併せてこうした機会を活用することが、より幅広い人材育成につながる可能性もあると思う。

神谷企画官）

地域 SECUNITY のイベントは、広範な参加を得るため、連携や周知を工夫して行うことが重要である。地域型 CTF（Capture The Flag）等も、広く参加可能なものとして、周知を徹底した上で参加拡大を図ることが重要だと考える。

辻構成員）※チャットより一部修正の上抜粋

総合的な IoT ボットネット対策のうち、C&C サーバへの対処について、C&C サーバの生存時間が短く、C&C サーバを検知・共有するまでの間に、別の C&C サーバに移る場合もあるかと思う。共有については、サイバー攻撃に係る痕跡を調査するための IoC 情報として活用すると思われる一方で、遮断においてはいたちごっこになってしまうように思うが、実際の感触はどうか。
また、様々な人材育成のアプローチは素晴らしいと思うが、目的・目標に対してどのような結果であったか。望むべき人材は育成され、課題等が解消されたのかといった効果測定に関する結果はあるのか。

神谷企画官）

C&C サーバへの対処について、ご指摘のとおり、C&C サーバの生存時間が短く、検知から共有までに別の C&C サーバに移っている場合があり、いたちごっこになる可能性もあるため、こうした取組だけで全ての C&C サーバについて適時に把握・共有できるわけではないと思っている。しかし、検知した C&C サーバのうち、早期に検知されているものも相当程度あり、その有用な活用方法について検討すべきだと考える。なお、本実証では通信遮断は行っていない。

道方参事官）

ご指摘の人材育成の取組については、いくつかのプログラムがある。国の行政機関や地方公共団体向けの「CYDER」は、インシデント対応能力の訓練を通じて、インシデント対応のリーダーやそのチームの一員となる人材を育成している。また、25 歳以下の若手人材を育成する「SecHack365」は、その卒業生が、起業したり、アカデミアにおいて論文をトップカンファレンスへ出す等の成果を出している。その他、万博向けサイバー防御演習である「CIDLE」も成果を上げており、プログラムに応じてそれぞれの目的に沿った成果が出ているところ。

◆議題「（２）サイバー対処能力強化法及び同整備法について」について、内閣官房国家サイバー統括室庄司参事官から資料 47－２を説明。

◆構成員の意見・コメント

中尾構成員）

国家サイバー統括室からの説明について、サイバー攻撃の守る対象に政府や自治体が含まれていることを確認した。重要インフラ企業等で発生したインシデントを政府機関と共有し、官民連携の下、分析・対応する試みは素晴らしいと思う。しかし、政府がサイバー攻撃を受けた場合に、その攻撃情報がどのような経路で分析をされ、民へ共有されるのか見えない部分がある。その点について、簡単に補足説明いただきたい。

庄司参事官）

政府は、民間事業者や今回新たに設置する協議会の構成員、外国政府等から得たインシデント情

報等を分析し、各機関に提供するという形を考えている。
各機関へ提供する情報には、機密情報や通信の秘密に該当する情報も含まれるため、こうした情報を「総合整理分析情報」や「提供用総合整理分析情報」、「周知等用総合整理分析情報」といった形で分類し、各主体へ提供する予定である。

中尾構成員）

当方の質問は、政府がサイバー攻撃を受けた場合においても民間と連携できる枠組みになっているのかという趣旨である。アメリカでは、政府だけではサイバー攻撃に関する情報の分析が難しいため、ネットワーク事業者等とも連携し、政府が受けたサイバー攻撃に関する情報を民間と共有し、分析しているとのことだが、今回の仕組みもそのような対応を含んでいるかという確認である。

庄司参事官）

政府へのサイバー攻撃に関する情報は、その性質によって提供のあり方が変わる。国家や特定のグループによるサイバー攻撃なのか等、個別の事案に応じて、政府が検討することになる。

小山構成員）

アクセス・無害化措置について、国内の IoT 機器等がアクセス・無害化の対象となり得る場合、どのようなステップで当該措置を進めていくのか、現状話せる範囲で教えていただきたい。

庄司参事官）

国内の IoT 機器等へのアクセス・無害化については、当該機器等がサイバー攻撃又はその疑いがある通信等を行っていることが認められ、そのまま放置すれば、人の生命、身体又は財産に対する重大な危害が発生するおそれがある、こうした緊急の必要がある場合に、基本的には独立機関の承認を得た上で、警察等が措置を取ることになっている。当該措置の内容は、サーバ等の管理者に対して停止等を命令することや、サーバ等に対して直接措置を取るということが考えられる。

岡村構成員）

サイバー対処能力強化法第 9 章に規定のある協議会は、従前のサイバーセキュリティ基本法に基づく協議会と、どのような点で違うのか教えていただきたい。

庄司参事官）

今回の協議会は新設することとしており、改正前のサイバーセキュリティ基本法に基づく協議会は廃止することとしている。サイバー対処能力強化法に基づく協議会とサイバーセキュリティ基本法に基づく協議会との差異については、前者の協議会は、政府が収集整理・分析した情報を政府から協議会の構成員に対し共有することが法に規定されるとともに、サイバー対処能力強化法に基づき守秘義務の違反に対する罰則を引き上げた上で、同意の下加入いただき、加入いただいた事業者へは秘匿性の高い情報も共有されることを想定している。

◆議題「（３）サイバーセキュリティ領域における AI の趨勢・動向」について、新井氏から資料 47－３を説明。

◆構成員の意見・コメント

岡村構成員）

従前の脆弱性の届出制度等と同様に、法制度によって今のご発表にあったような欠点を補うことはできるのか。

NTT データグループ新井氏）

法的観点から対応することができることはあると考えている。例えば、不正アクセス禁止法の中で、生成 AI を通じて攻撃されるものも適用内であることを改めて示してもらうことや、経済産業省が実施しているソフトウェア等の脆弱性関連情報に関する届出制度における届出対象に、AI に関するものも含まれることを改めて周知してもらうこと等。特に後者について実施することで、脆弱性が修正され、攻撃を防ぐことは、必要な手立てではないかと考える。

小山構成員）※チャットより一部修正の上抜粋

当社の CSIRT 業務では生成 AI と自動化を徐々に導入している。AI は 24 時間無休で働くため、CSIRT 業務の自動化に効果が大きく、OSINT モニタリング等の輪番体制でも有効性を感じている。しかし、人の輪番の引き継ぎが不要になる反面、人へのスキル伝承や新人の技術力向上が難しくなる課題があり、アクセル全開での AI 導入に抵抗感がある。AI が動かない原始時代に戻った場合でも、人が手でリカバリできる状態を維持しつつ AI 導入を進められるようなガイダンスがあれば良い。AI 停止時の細かい手作業手順書を AI に書かせる等、課題解決に MCP の活用も可能性を感じた。良い事例があれば紹介していただきたい。

NTT データグループ新井氏）

従前からある科学技術やコンピュータサイエンスの価値そのものが、AI によって奪われることはないと思う。トラブルシューティングのようなことについては、その希少性が AI によって翻って手堅いものになり、こうしたことを学習していた人が活躍できるという点が際立ってくるのではないか。

園田構成員）※チャットより一部修正の上抜粋

コードエディターのような生成 AI の活用が進む中で、エキスパートの生産性は劇的に向上する一方、エキスパート以外は仕事を失うリスクが大きくなると感じる。また、入門者が生成 AI に依存することで思考力が低下するという研究結果もあり、人材育成面で懸念を感じている。この点に関して何か知見があれば聞きたい。

NTT データグループ新井氏）

夏に渡米した際、ジュニアと呼ばれる若い人の仕事が AI によって奪われたり、就職が妨げられたりするのではないかという意見を耳にした。こうした事態を防ぐために、政府として若者の採用を支えるための政策を打ち出すことで、新卒採用が控えられるような就職氷河期が再び訪れないようにする必要がある。実際には、AI を利活用する時代が到来するとは思うが、一時的に新卒採用を控えることがあったとしても、AI の利活用が失敗に終わったときに人材が存在しないという最悪の結末にならないように、人材育成が継続的に推進される体制を作っておく等の準備が必要だと考える。

鵜飼構成員）

AI の利活用は作業効率の急速な上昇をもたらすため、研究開発機関や民間のベンダにおいてその実装を進めているが、変化が激しいため標準化に苦労しているのが現状である。インシデントレスポンスやSoCをやっているベンダでも同様の苦労があるのではないかと思うが、AIを利活用していく上での足元の課題や問題意識について、知見があれば伺いたい。

NTTデータグループ新井氏）

AI は毎回結果が変わるため、脆弱性をチェックする手順も毎回異なる。従って、網羅性に問題があるため、脆弱性をチェックする一定の手順を仕様書のように書いて追えるかについて確認するということが一つの標準化の方法だと思う。毎回結果が変わるという AI の性質をどう捉え、品質の精度や統一性をどう担保していくかが、それぞれの企業や組織がこれから考えるべきことであり、ある意味ビジネスになると考える。

森構成員）

生成 AI が悪用されてしまうことについて考える必要がある。関連して、AI による脆弱性発見が可能になっているという話があった。こうした脆弱性発見をはじめとするセキュリティ目的での生成AIの利活用が可能になるのであれば良いが、悪用されると非常に困る。生成AIの能力が悪用されることに関して、何か良い手立てがあるか聞きたい。

NTTデータグループ新井氏）

脆弱性の発見について、商用で販売されている一般的な生成 AI を使って脆弱性を探す場合、倫理的な問題があるとして回答を拒否するため、基本的には、生成 AI は悪用できないと認識している。その一方で、バグバウンティのような例外的に許可されている行為を AI に理解させることができれば、脆弱性を発見することができる仕組みとなっている。そのため、正しい形での脆弱性発見にも障壁があり、悪用に関しても同様の障壁があるため、脆弱性の発見という点ではかなりハードルが高い状況にある。

辻構成員）

診断や監視、インシデントレスポンス等、これまで人力で行ってきたことを AI が担うことができるようになっていることをについて便利だと感じたり、そのような製品が海外の展示会で多く出てきていると思う。こうしたことを踏まえると、セキュリティ人材の育成にも影響が出てくると感じている。どのような領域やレイヤーを捨てて、どこに注力していくべきか。その領域やレイヤーの大小も含めて、整理があれば伺いたい。

NTTデータグループ新井氏）

注力すべき人材育成のレイヤーについて、コンピュータサイエンスという普遍的な領域そのものに注力すべきというのは変わらないと考えている。AI に代替されるからこそ、コンピュータサイエンスを知らない人が増えると考えるので、こうした知識を持っている人材は希少性が高まっていくため、希少性の高い人材の育成に注力することは、変わらずやっていくべきだと考える。

鈴木構成員）

AI が偽誤情報の拡散に悪用されるという懸念は 2021 年頃から報告されている。また、今年辺りから、AI エージェントにパーソナリティを付与して、AI エージェント同士で各パーソナリティに応じた説得コミュニケーションをさせるといった研究が増えており、AI が人間に影響を及ぼす可能性が今後増えていくと考える。この場合、ご発表の中であった入出力段階における対策では、その影響は止められないのではないかと考えており、こうした課題もセキュリティ課題の一つとして捉えるべきかどうかについて伺いたい。

NTT データグループ新井氏）

AI がパーソナリティに近いものを持ち、個別に、その人にとってコンフォータブルな回答を返してくるものが悪用され、AI との会話によって被害が生まれる可能性がある。個人的見解だが、プラットフォーマーに対して、AI を偽情報の拡散行為や詐欺行為に悪用するするアカウントの取得を規制する等、制限をかけていく方法があると考える。当然、表現の自由とのバランスもあるため、法的観点からも慎重に検討した上で、議論すべきだと考えている。

徳田構成員）コメント

日本には国立研究開発法人が 26 組織あり、様々な生成 AI を活用して研究開発業務を加速させようとしているが、ISMAP の枠組みがあるため、機微なデータが含まれていない研究データが、行政に関わるデータと同様に扱われ、先端的な生成 AI サービスに対して自由に入力できないという問題がある。こうした問題は、日本の研究開発力をスローダウンさせる可能性がある。ISMAP の枠組みでは、申請に時間がかかり、また、大手の Big Tech は申請しないかもしれないという悩ましい課題があることを共有したい。

中島構成員）※チャットより一部修正の上抜粋

AI ファイアーウォールのような悪用防止対策に、国家や政府、あるいは国際組織などが関与する余地はあるのか。

NTT データグループ新井氏）

コンピュータセキュリティの中の脆弱性やソフトウェアの欠陥に関連した問題である。生成 AI を様々な製品・サービスに組み込む事業者が今後増えていくことが予想されるため、こうした事業者が脆弱性を生み出さないためのガイドラインが必要であると考える。個別のソフトウェアに関しては、その安全性を確保するための手引きは従前から存在しているが、生成 AI も対象としたガイドラインは存在しない。そのため、生成 AI を組み込んだ製品・サービスの安全な作成方法を提示し、生成 AI を組み込んでいる製品やサービスが悪用される芽を摘むという、従前から実施してきた方法を生成 AI という領域においても行うことが必要なのではないか。

◆議題「(４)AI セキュリティに関する検討について」事務局から資料 47－４を説明。

◆構成員の意見・コメント

徳田構成員）コメント

２ページの３ポツ目に、「『不正操作による機密情報の漏えい、AI システムの意図せぬ変更または停止が生じないような状態』に対する脅威への対策について中心的に取り扱う。」という記載があるところ、当該記載は、攻撃者が AI を停止させることを想定していると思われるが、逆に

AI システムを停止させないような攻撃も考えられる。現行の記載の場合、自律性を持った AI システムに対する攻撃の一方しか考慮されていないように思われる。多くの人にとっては、AI システムを止められなくなる攻撃の方が怖いのではないか。

中尾構成員）コメント

NICT は、ISO 及び ITT で標準化を行っており、ISO/IEC の 27090 というセキュリティに対応するためのガイダンスがある。このガイダンスは現時点では DIS の段階だが、様々な脅威がそのインパクトとともにリストアップされている。検討の中で、既に脅威を把握していると思うが、参考に見ていただければと思う。必要であれば、DIS を総務省にも提供することができる。

(3)閉会

以上