サイバーセキュリティタスクフォース（第 20 回）議事要旨

1. 日 時：令和 2 年 1 月 27 日（月）14:00～15:30

2. 場 所：中央合同庁舎 2 号館 7 階　省議室

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、齋藤構成員、園田構成員、徳田構成員、中尾構成員、
名和構成員、林構成員、藤本構成員、若江構成員

【オブザーバ】

入江奨(経済産業省)、上西裕(内閣官房 IT 総合戦略室)、鮫島 清豪(内閣サイバーセキュリティセンター)、
田中俊明(KDDI) 、齋藤衛(インターネットイニシアティブ)

【総務省】

竹内サイバーセキュリティ統括官、二宮審議官(国際技術、サイバーセキュリティ担当)、
岡崎サイバーセキュリティ・情報化審議官、大森サイバーセキュリティ統括官室参事官(総括担当)、
赤阪サイバーセキュリティ統括官室参事官(政策担当)、近藤サイバーセキュリティ統括官室参事官(国際担当)、
塩崎放送技術課長、水落地域放送推進室技術企画官、中村電気通信技術システム課長、
安達地域情報政策室課長補佐、相川サイバーセキュリティ統括官室参事官補佐、
佐々木サイバーセキュリティ統括官室統括補佐

4. 配布資料

資料 20－1　我が国のサイバーセキュリティ強化に向けた緊急提言（案）（事務局）

資料 20－2　我が国のサイバーセキュリティ強化に向けた緊急提言（案）概要（事務局）

資料 20－3　今後重点的に取り組むべき研究開発課題について（事務局）

資料 20－4　「サイバーセキュリティタスクフォース」ヒアリング資料（小山構成員、関係者限り）

資料 20－5　サイバーセキュリティタスクフォースヒアリング資料（田中俊昭氏(KDDI)、関係者限り）

資料 20－6　サイバーセキュリティタスクフォースヒアリング資料（齋藤衛氏(インターネットイニシアティブ)、関係者限り）

参考資料 1　サイバーセキュリティタスクフォース第 19 回　議事要旨

5. 議事概要

(1) 開会

(2) 議事

◆ 議事（１）我が国のサイバーセキュリティ強化に向け速やかに取り組むべき事項[緊急提言]（案）について、事務局より、「資料 20－1　我が国のサイバーセキュリティ強化に向けた緊急提言（案）」、「資料 20－2　我が国のサイバーセキュリティ強化に向けた緊急提言（案）概要（事務局）」を説明(省略)

◆　構成員の意見・コメント

齋藤構成員)

「資料 20－1」の 8 ページの⑤について、民間企業によって参照されているという文言がある。事業者及び民間企業によって参照されているという文言に修正することを提案させていただきたい。民間企業と言うと、どうしてもメーカーやベンダーというイメージになってしまう。

「資料 20－1」の 6 ページの公衆無線 LAN のとるべき対策の②について、通信経路が暗号化されていない状況で ID・パスワードを入力しないという文言があるが、これはなかなか一般の人への周知が難しい。総務省が実施している「国民のための情報セキュリティサイト」にも同じような内容が記載されており、これらを上手く活用していくべきではないかと考えている。

名和構成員)

「資料 20－1」の 7 ページの公衆無線 LAN のとるべき対策の③について、2020 東京大会に向けて多くの利用が見込まれるホテル・観光関係機関という文言があるが、これに対応して新たに、思いやりの視点からの多言語への対応について記載しておくべきではないかと考えている。多言語への対応についてもサイバー攻撃から守るべき対象になり得る。

岡村構成員)

「資料 20－1」の 8 ページのとるべき対策の③について、当方は地方公共団体における情報セキュリティポリシーに関するガイドラインの改訂作業に携わっているところである。「資料 20－1」の説明の中に、リース契約の問題が出てきたが、現象面としては、地方公共団体において起きていることであるが、実際のファイナンスリースの場合には賃貸借契約でリース期間が満了すれば返却しなければならない点では、民間企業においても全く同じことが当てはまる。総務省から地方公共団体の庁舎内におけるリース終了品については、物理的または磁気的な破壊を、職員立ち合いのもので行うという形のリリースが出されている。ファイナンスリースに限れば、民間企業が知らないうちに、いろいろなところから情報が洩れている可能性があり、数量的にみても多い可能性がある。地方公共団体分野以外に、民間企業のファイナンスリースにおけるデータ消去に関する制度と実態が合っていない部分があるので、これについても制度的に検討すべき課題であると考えている。それについても、官民問わず、重要データをどのようにクリーンに復元できない形でリース終了品のデータを消去できるのかといった視点での検討が必要になると考えている。データの消去という関係では、さらにクラウド化において、本当にデータを消去してくれているのだろうかということと裏腹の関係にあることも留意されたい。

後藤座長)

「資料 20－1」について頂いたコメントについては、この後、事務局の方で修正案を作っていただきたい。修正内容については、座長一任とさせていただきたいが、それでよいか。

全構成員)

異議なし。

後藤座長)

「資料 20－1」については、事務局と座長で修正内容の検討を行い、その後公表する。なるべく早期に取組を進めていただけるようにしたいと思う。

◆ 議事（２）研究開発の推進について、事務局より、「資料 20－3　今後重点的に取り組むべき研究開発課題について」を説明(省略)

◆ 構成員の意見・コメント

中尾構成員)

「資料 20－3」の説明の中に、情報通信研究機構関係の研究開発がたくさん出てきた。今後重点的に進めていく研究開発に関する取組ということで取りまとめられているが、これらの研究開発について、エンドユーザ、研究機関のどちらを見ているか、ターゲットが分かりにくいという印象を受ける。いろいろな攻撃の解析を行なったり、防御を行ったりする際に、どのようなターゲットを攻撃者が狙っているのか、または攻撃者が狙っているターゲットのリスクが何で、そのインパクトがどの程度であるのかといったことを把握しなければ、対応ができない。一般的な研究開発の場合、ある組織がスペシフィックに実施してきたものに対して防御しようとしているのか、一般的な防御のインフラを広く開発しようとしているのかが分かりにくいので、確認したい。

最近の攻撃の手法はコンビネーションになってきていると認識している。これまでの攻撃手法が組み合わされるだけではなく、現在、基本的なパッシブディフェンスのファイアーウオールや IDS やアンチウイルスソフト等をかいくぐったり、観測網であるハニーポットやダークネット等を回避したりしていくようなところに発展してきていると認識している。このため、攻撃のノウハウを知り得るということが重要になってきているが、なかなか日本の研究開発の環境では、攻撃のツール等を作ってこなかったという背景もあり、情報通信研究機構では、STARDUST に攻撃のシナリオをホワイトハッカーのレベルで組み込んでビヘイビアを見ていくことを考えている。そのあたりの方向性が「資料 20－3」の方向性と合っているのかを確認したい。攻撃シナリオという言葉はいろいろなところで使われている。サイバー演習のコンテンツでもいろいろな攻撃シナリオのパターンを作っている。攻撃シナリオを見ていくことも重要であるが、新たな攻撃を模索しながら、ある環境に入れてそれを評価する。攻撃側と防御側を戦わせるといったことになると、なかなか一筋縄ではいかないという印象を受ける。

いろいろな情報の共有やその仕組みが今後出てくる。集めた情報は研究の基本になり宝であるが、情報通信研究機構の視点で言えば、それらの情報を全部使ってくださいと差し出すことにはならない。情報通信研究機構が保有する情報を使っていただけるのは、情報通信研究機構とトラストリレーションシップを結んだ研究機関となり、そのような研究機関と連携しながら使っていくという体制で実施することは十分あり得る。そのような道は上手く作っていく必要がある。

サプライチェーンに関係する話として、5G や IoT の話が出ている。サプライチェーンにおいては、いろいろなモジュールが繋がっていて、そこに発生するリスクがサプライチェーンリスクであると認識している。もう少し一般的にみれば、バックエンドにクラウドがあったり、ビッグデータのアナリティクスがあったり、エンドユーザには IoT デバイスがあったりする。そのような環境であるため、攻撃の機会が、非常に広範囲になる。総務省の重点的な取組の中で、IoT の部分は捉えられているが、車や５G のネットワークといった具体的な部分をもう少し深堀りしていくような研究も、研究の課題にされないのかということについて確認したい。

近藤サイバーセキュリティ統括官室参事官(国際担当))

今回のターゲットが研究機関であるのか、日本全体であるのかという点については、先ずはどのような研究開発を国として、あるいは情報通信研究機構として、また民間企業や大学等として取り組んでいくのかという研究開発課題をリストすることを目的としてヒアリングを行ってきた。その中で研究環境や人材育成に関するコメントを多々頂いた。例えば、先ほど話が出た STARDUST のようなものを使わせてほしいというコメントや、攻撃側と防御側を戦わせるようなインフラに関するコメントも頂いた。結果的には研究機関と日本全体の両側から見ているものが入っている。これに伴い、必要なインフラ整備を行っていくということも課題としてとらえている。

STARDUST と「資料 20－3」に記載している構築したい研究環境が合っているかという点については、まさに STARDUST のようなものを推進している。ヒアリングの中でもっと STARDUST を使いたいというコメントや、情報通信研究機構と研究契約を結ぶのが大変であるというコメントを頂いた。先ほど話が出たようにそもそも研究契約を結ばなければ STARDUST を使えない一方で、より活用していくためのバランスをどのように取っていけばよいのかということを課題として記載している。

サプライチェーンやクラウドの課題は多岐にわたるため、どこに注力していくかが重要である。5G 関係の課題については既に研究開発に着手しているものもあり、それ以外の重要な課題についても、ご指摘のとおり深堀りしていくことはあると考えている。

名和構成員)

「資料 20－3」の 3 ページの AI（2）の（4）フォレンジックについて、いろいろな研究が米国や欧州で実施されている中で、それらとの比較でログに注力しているのは正しいが、証跡に関連するものがない。ログと証跡の両方があってはじめて、係争状態や民事裁判でも勝てる。裁判や係争状態において、バスの監視カメラのデジタルデータが扱われる場合に、信用できるデバイスであるかどうかについて国内では裁判官、裁判員の自由心証に基づいて、過去の判例から推定できるが、米国では e ディスカバリーという確立された制度が、欧州でもそれに相当する制度が存在する。（4）の文章中にある、信用できるデバイスを車中に置く必要があるという部分について、何をもって信用を担保するかはもちろんテクニカルに対応するところもあるが、米国や欧州のような日本と違うところでの観点が必要になると考えている。

小山構成員)

AI について、「資料 20－3」においても、AI で守るということが記載され、そういう話をいろいろなところで聞く。確かにそのような世界があるのかもしれないが、ここでしっかりと押さえておきたいのは、攻撃では AI を使いやすいかもしれないが、守るということは脆弱性をつぶすといった基本的な対策を行ってこその防御になるということである。基本的な対策がおろそかになってはいけないという情報発信や啓発を継続的に実施しつつ、防御にも AI を導入するという考え方を普及させていく必要があるのではないかと考えている。

AI を攻めるということに関して、サイバーセキュリティの分野では、どこまで広がりを見せることになるのか。「資料 20－3」の 3 ページの AI（2）の（3）では、データポイゾニングや敵対的サンプル攻撃など幾つか挙げられているが、例えば、サイバー攻撃の対象物や目的は金銭であったり、それが情報に代わってきたりしている。選挙妨害やフェイクニュースのように人の心を操作するところまでサイバー攻撃が発展してきている。そういう分野への AI の適用や AI 騙しのような研究開発についても必要ではないかと考えている。

林構成員)

「資料 20－3」は技術のことが中心でよいが、今、人文社会科学的な研究がサイバーセキュリティの世界では比較的役に立つ要素になってきている。先ほど話があったソーシャルエンジニアリングや、e ディスカバリーのようないろいろな制度が、組織に絡んだり、心理学に絡んだりしている。今後、ヒアリングを続けられる際には、人文社会科学的な研究に期待するものがあるか、それは具体的に何かといったことを聞いてもらいたい。法律に携わっている人にセキュリティについて関心を持ってもらうのは難しいので、技術者からそのように水を向けてもらえるとありがたい。

鵜飼構成員)

民間企業として、サイバーセキュリティ技術の研究開発に取り組んでおり、それを事業に結び付けている。そのような視点から考えたときに、全体的な研究開発を進めていき、その成果が世の中に普及していかないといけない。普及という観点で考えたときには、サイバーセキュリティ対策としてのマーケットが出来上がって、そこに産業が生まれて、それが民間の行動力によって産業に浸透していくという姿が本来のあるべき姿である。そういう研究開発と、国が率先して取り組んでいく研究開発がある。後者は国がお金をつけてしっかりと取り組んでいくことが重要である。前者は最終的には産業の中でしっかりと回っていくことが重要であると考えている。民間でも同じような研究開発があり、例えば、AI を使った攻撃に対する研究等を行ったり、いろいろな研究開発に AI を使ったりしている。産業と一体になって進めていけるような分野は、産と官が一体となって共同研究開発を進めていくことができるとよいと考えている。

徳田構成員)

先ほど話が出たが、人が守っている部分がまだまだたくさんあるので、ディフェンダーのムーブメントを加速する仕組みづくりが重要である。「資料 20－3」を読むと、個々の研究グループが独立して、黙々と研究開発テーマをつぶしていけばよいというメッセージが少し伝わってくる。もう少し国として、全体を加速させるようなイメージが必要ではないかと考えている。例えば、情報通信研究機構では、総務省と一緒になって、翻訳バンクという仕組みを作った。医療分野における専門性の非常に高い文書の英語と日本語がペアとなっている文書を 100 万文書頂くと、AI による翻訳の精度が 10 ポイント上がった。先ほど話が出たデータを利活用する部分も、個々が頑張ってもなかなか上手くいかない。もう少し機械学習に使うようなデータを国レベルでシェアできるように、セキュリティ研究のためのデータプラットフォームを作って、それを使うことによって、研究成果に対してフィードバックをかけて加速できるような仕組みづくりが必要であると考えている。現在、情報通信研究機構では、アンドロイドのマルウェアのデータを公開しているが、オープン、クローズド、セミクローズドといったいろいろなレベルのポリシーがあるかもしれないが、もう少しシステマティックに、全体としてデータを提供するようなインフラが欠けているので、研究成果に対してフィードバックをかけて加速できるような仕組みづくりが必要であると考えている。

AI については、ディープラーニングや伝統的な機械学習など、いろいろな方法論がある。理化学研究所の AIP センターには、AI をコアに研究している人たちがいる。データドリブンでディープラーニングを行うときにフェイルしたときの説明性がなかなか付かないので、企業も含めて、説明可能な AI について研究開発を行っている。米国の DARPA においても 5 か年計画で取り組んでおり、３年目が終わったところである。このような AI プロパーで研究を行っている人たちが大分増えてきているので、出来れば、AI に取り組んでいる人たちをもう少し巻き込む仕組を作って、その人たちをメインにして、どのような新しい研究ができるのか考えてもらうべきである。サイバーセキュリティについて研究を行っている人たちには限りがあるので、AI プロパーで研究を行っている人たちを巻き込んで、その人たちにデータを提供して、考えてもらう方が効率的ではないかと考えている。

後藤座長)

「資料 20－3」については、本日いろいろなご意見を頂いた。引き続き検討していきたいと思う。

竹内サイバーセキュリティ統括官)

本日議論いただいた緊急提言（案）については、修正すべき点は速やかに修正したうえで、明日以降速やかに公表し、出来るだけ早く実施に移していけるように対応を進めていきたいと考えている。アクティブディフェンスをサイバーセキュリティ対策として、どのように考えるかについては、施策によっては通信の秘密の再整理が必要になってくるという問題がある。基本的な問題意識としては、通信の秘密ということに懸念があるため、本来実施すべきサイバーセキュリティ対策に踏み込めていないこともあるのではないか。そういうものがあるのであれば、必要な問題意識や課題についてきちんと出していただき、こういう対策を、このように実施していきたいということや、そのうえで検討すべき課題をどのように解いていくか、どういう対策が採り得るか、制度をどう変えるかということを、必要な場で議論していけばよいと考えている。そのような観点から事業者の問題意識として、どのようなことがハードルになっているか、どうしていきたいのかについて、先ずは議論のきっかけとして出していただいた。本日の意見を踏まえて、今後の議論の進め方については、よく相談して進めていきたいと考えている。引き続きお願いしたい。

相川サイバーセキュリティ統括官室参事官補佐)

サイバーセキュリティタスクフォース第 21 回については、2 月 20 日の 14 時から、第 22 回については、3 月 18 日の 16 時からを予定している。具体的な議事と開催場所については、後日事務局から連絡させていただく。構成員の方々には個別の相談をさせていただくこともあるため、引き続き協力をお願いしたい。

以上