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

1. 日 時：令和元年 12 月 25 日（水）14:00～15:30

2. 場 所：中央合同庁舎 2 号館 10 階　第 1 会議室

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、戸川構成員、徳田構成員、中尾構成員、名和構成員、林構成員、藤本構成員、吉岡構成員、若江構成員

【オブザーバ】

尾崎洸(経済産業省)、上西裕(内閣官房 IT 総合戦略室)、吉川徹志(内閣サイバーセキュリティセンター)、浦船利幸(地方公共団体情報システム機構) 、久保田実(情報通信研究機構)

【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)、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、田島地域情報政策室係長、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 19－1　前回までの御議論と今後の進め方等について（事務局）

資料 19－2　ハードウェアチップ脆弱性検知手法（戸川構成員）

資料 19－3　サイバーセキュリティの今後の研究開発課題について（久保田実(情報通信研究機構)）

席上配布　　サイバーセキュリティタスクフォース第 18 回　議事要旨

5. 議事概要

(1) 開会

(2) 議事

◆　議事（１）前回までの御議論と今後の進め方等について、事務局より、「資料 19－1　前回までの御議論と今後の進め方等について」を説明(省略)

◆　構成員の意見・コメント

齋藤構成員)

「資料 19－1」の 2 ページの Wi-Fi の安全な利用については、5G と一体で考えなければならない。東京 2020 大会の開催までには 5G はまだ普及しないため、Wi-Fi 6 の利用が重要な課題になってくる。新しい規格が出て、セキュリティレベル

が上がっているので、早期に導入できるようにすることが望ましいと考えている。W56 などの 5GHz 帯の周波数を使用している Wi-Fi には、DFS の機能があり、これはレーダーの周波数と重なるので、それを抑制する機能がある反面、チャンネルボンディングにより帯域が大きく取れるというメリットがある。5G が今脚光を浴びているが、Wi-Fi を活用することも重要であり、そのセキュリティも担保されなければならない。新しい規格のものを早く普及させることが課題であるので、そのための施策を実行していく必要がある。

鵜飼構成員)

昨今、ネットワーク機器等に安全保障上懸念されるバックドアが仕込まれていないか調査してほしいという依頼が様々な民間企業から当社に来ているような状況である。ブラックハットでもいろいろな機器からバックドアが見つかったという話が出ている。気にされている民間企業が増えてきていると感じる。そのような部分をどのように担保していくかは議論するのが難しいかもしれないが、IoT・5G セキュリティ総合対策の観点から、１つの軸として考えてみることも重要なことではないかと考えている。バックドアとして騒がれているものの中には、ベンダーのメンテナンス用のものもある。このようなメンテナンス用のものが公表されていないということも問題である。逆に悪用されてネガティブなことになってしまうことも問題である。そういうことを含めて、どのように考えていくかが重要である。

小山構成員)

「資料 19－1」の 8 ページの②情報通信サービス・ネットワークのレイヤー構造について、従来の通信から 5G になると、スライシングやエッジコンピューティングが途中で使われるなど、ノードと通信が一体的になってくるイメージを持っている。どのレイヤーでセキュリティ対策を行うかという議論が始まっているが、一方でスライシングなどまだサービスが始まっていない中で、将来的にどこに影響が出てくるのか、例えば、通信の秘密のような慎重に扱われてきたテーマがどこに、どのように効いてくるのかという議論も必要である。いざサービスが進展してみて振り返ってみたときに、通信の秘密に抵触していて、ビジネスに影響が出るということがあってはならないと思うので、そういうところを見越した対策を進めていくべきではないかと考えている。

岡村構成員)

中長期的な「IoT・5G セキュリティ総合対策」も勿論重要であるが、最近、自治体からの廃棄パソコンがネットオークションで売られていたり、クラウドが障害を起こしてバックアップが一部あるいは全部取られていない状態でデータを復元できなくなる事象が発生した。こういう状況のもとで東京 2020 大会に突入した場合に、どうなってしまうのかという危機感を持っている。あと数ヵ月後を問題なくすごすために、あまり時間がないので、もう少し急いで短期的に速やかに検討すべき課題について、最新の事象を取り入れたうえで、未然にクラウド側あるいは端末側でバックアップがきっちりと取られているのかどうかを確認するといったもう少しベーシックな部分についても、今一度、更に力を入れてもらえるように改めてお願いしたい。

中尾構成員)

「資料 19－1」の 6 ページの中長期的な検討項目について、IoT や 5G で今見えているある１つのセクターやエリアのセキュリティはすごく重要である。それに加えて、IoT も 5G もシステム自身が非常にバラエティに富んでおり、5G のシステムを１つ取っても、スマートシティのシステムを１つ取っても、基本的に、共通のモデルを取ることがなかなか難しくなっている。例えば、スマートシティの場合には、国が先導するスマートシティの話もあれば、グーグルなどの民間が進

めるスマートシティの話もあれば、地方自治体が進めるスマートシティの話もある。それぞれ目的やターゲットが異なっている。単純にセキュリティと言っても、なかなか統一したようなセキュリティ対策を取りにくい。総務省として、どこをターゲットして、このような話を持っていくのかは中長期的な検討項目であるので、もう少し議論されることになると考えている。そのあたりのスコープをクリアにしないと多分言葉だけになってしまい、もったいないという気がする。

パッシブディフェンスという受身で防御するという考え方があり、NICT が実施しているダークネットやハニーポットはパッシブディフェンスである。そこから得られた情報をもとに、ファイアウォールの設定を変更したり、攻撃者の情報を活用したりしている。その次にグレーゾーンと呼ばれているアクティブディフェンスという考え方があり、さらにオフェンシブサイバーメジャーという考え方があり、ハッキングされたらハッキングし返すというハックバックはオフェンシブサイバーメジャーである。それは日本ではなかなか実施できないが、アクティブディフェンスについて考えた場合に、研究開発の流れの中で、相手の攻撃者を追いかけていくという話をどこまで実施してよいのか、場合によっては研究倫理に引っかかってしまう話になるかもしれないが、そのような部分を総務省の視点で整理していくことが中長期的にできれば、非常にクリアになって、日本のサイバーセキュリティの研究開発がより進むような気がする。そのようなメジャーはいろいろあると思う。

名和構成員)

「資料 19－1」の 3 ページに中小企業に対する支援施策の検討の話が出ているが、方針や達成レベルが示されていないような印象を受ける。既に警察や経済産業省において取組を始めているものがあり、この中に通信・放送事業者を対象とする取組も含まれているケースがある。地方に呼ばれて出向いたときに、重要インフラ領域の中小企業の方から、最初は警察、次に経済産業省、そして総務省の順で施策が積み重なっているという声が聞かれる。「資料 19－1」の 7 ページの関係主体との連携をしつつ、既に施策が推進されている他の省庁の取組を少し配慮した形で、現場が求める施策支援を行うことができれば、困惑させずに有用なものになると考える。

吉岡構成員)

IoT については、多くの施策において、想定される脅威のモデルが Mirai 等にフォーカスされている。多くの機器が乗っ取られて、大量のデータを送り付ける DoS 攻撃が脅威モデルになっており、2016 年から脅威モデルとしては同じである。本当に今はそれだけなのかが分からなくて研究しているところであるが、脅威モデルがだんだん見えにくくなってきている。そういう意味では先ほど話が出たアクティブなセキュリティ対策として、攻撃側のモニタリングに関する研究が始まっており、いろいろと見えてきているものがある。パッシブに見ているだけでは分からない話がとても多い。そういう部分について、どこまで研究として実施できるのか、実施してよいのかを整理しつつ進める必要があると考えている。攻撃者側の視点がないといろいろと変遷する脅威に対して追随することができないのは分かり切っていることであるが、そのように思う。例えば、最近、EMOTET が出てきているが、これは元々存在した攻撃のパターンを組み合わせれば出来てしまうものである。少し工夫しただけでこれだけ被害が増える。これも攻撃者側の視点があれば先読みできたのではないかと思っており、研究者としては残念に感じる。攻撃者側の視点を持った研究やいろいろな活動が、IoT の領域においても非 IoT の領域においても大事であると考えている。

藤本構成員)

IoT や 5G の利活用が多岐にわたることに伴って、リスクも多岐にわたるため、利用者の参加が不可欠になるのではないかと考えている。利用者自身に、自ら自分たちで安全・安心を作っていく一員になるという意識を持ってもらわないとい

けない。そうでなければ提供する側が安全なものを提供するという形にはなりにくい。中長期的にそのような意識をどのように醸成していくのかを併せて検討してほしい。

◆ 議事（２）研究開発の推進について、戸川構成員より、「資料 19－2　ハードウェアチップ脆弱性検知手法」を、久保田実氏より、「資料 19－3　サイバーセキュリティの今後の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**

若江構成員)

研究開発においてデータはとても重要である。ハードウェアトロイが日本で発現した例はあまりなく、データがほとんどないと思うが、データは Trust-HUB 等から共有してもらっているのではないかと思う。国内でデータが不足して困ったことや、こうすればデータを確保できてよいということがあれば、教えてほしい。

戸川構成員)

学習させるためのデータやテストのためのデータをいかにして集めるかが大きな問題である。現状は、Trust-HUB のサイトや回路設計で日常使われているような幾つかのサイトからデータを持ってきてトライアルを行っている。最近は、日本国内のハードウェア・ソフトウェアベンダーが設計したデータを使って検証を行っている。ただハードウェアトロイと呼ばれているものは、国内の実例として誰かに仕込まれたものとしては見つかっていない。どのようなシナリオがあって、どのようなものを作ることが考えられるのかというデータについては、研究開発のレベルでデータを作っている。

名和構成員)

先ほど説明があったハードウェアチップの脆弱性の研究については、工場出荷時から実用に至るまでの話であると理解した。実用段階になって、ハードウェアベンダーがアップデートした後に、ハードウェアトロイが仕込まれる事例の研究や状況を耳にしたことがあれば、教えてほしい。

戸川構成員)

アップデートについては、研究レベルでは盛んであり、注目されている。今回説明した話は、半導体チップを作る設計工程・製造工程の話である。半導体チップが市場に出てアップデートする際のデータをいかにセキュアに担保するかという話は、どういう取組にするべきであるかという部分も含めて、こうすればよいという明確な答えが出ていない。まさにその部分が研究開発の対象となってくる。どういうフローで、誰が、いつ、どのタイミングでそれに対して安全性を担保するのかというところを含めて考えていかなければならない。

名和構成員)

攻撃者になったと仮定したときに、アップデートでこういう攻撃が可能になるというものがあるか。

戸川構成員)

いたちごっこになると思うが、なんとかなりそうな印象である。

吉岡構成員)

ハードウェアトロイについて、実際の攻撃のデータが限られている。当然ながら、サイバー攻撃と比べて、攻撃の頻度がすごく低く、なかなか攻撃のデータを集めて、そこから学ぶという研究のスタイルを採ることが難しいという話を伺っている。そうすると、情報共有を行ってもデータが足りないという状況になるので、攻撃の考えを持った研究者が必要であり、研究者も強力なハードウェアトロイをどのように作るかを積極的に考えて、それでも守れるように両方の視点で研究を実施しなくてはならない。特にこの分野はそのような傾向が強いのではないかと思う。

この問題を違う切り口から見るとサプライチェーンのセキュリティの問題になると考えられる。どこで不正な回路のデザインが入り込む余地があるのかということを産業的な観点で分析することがどこまで出来ているのか。出来ていないのであれば、そういう部分について研究することができるのではないかと考えている。

「資料 19－3」については、オペレーションの自動化が今後決定的に重要になると考えている。常にマルウェア対策が必要と言われるが、マルウェアとは何かと言えば、攻撃者が自動化作業を行った結果であると考えている。攻撃者が自分たちで全部実施するのが困難であるため、プログラム化している背景がありそれがマルウェアになっていると考えると、攻撃者は常に自動化していろいろなことを実施しようとしている。それに対して守る側がどこまで自動化できているのかを考えると、なかなか実施できていないことが多い。非対称性があるので、AI を含めて、いかに効率的に自動化について考えるかということが 1 つキーになるのではないかと考えている。

鵜飼構成員)

バックドアの問題はここ数年、非常に大きな問題になっているが、この問題について全体像が上手く整理されたものがない。ソフトウェアレベルのバックドアやファームウェアレベルのバックドアに加えて、先ほど説明があったハードウェアレベルのバックドアもあり、幾つかの種類がある。それぞれのバックドアに利点や欠点がある。ソフトウェアレベルのバックドアは、これらの中でまだサンプル数が多いと言われているが、それでも非常に数が少ない。データを集めるのが難しいのが現状である。これがファームウェア、ハードウェアとレイヤーが下がれば、さらにデータを集めるのが難しくなってくる。ハードウェアの PGA でビット数を改ざんするという話になると、見つけるのが非常に大変であり、バックドアを仕掛ける観点からみるとレイヤーが下に行けば行くほどレベルが上がり、発見が難しくなる。バックドアの問題にどのように対処していくかは、いろいろな意味で多角的にアプローチしていかないといけない。現実的にサンプル数が少ない中で、普通に実施しようとすると、回路をリバースエンジニアリングして地道に見ていく、それによってデータを積み上げることが足元の対処としては適切ではないかという感触を受けるが、もう少し解析を簡単にできるようにしたり、リバースエンジニアリングを効率的に実施できるようにする部分にフォーカスしているような研究があれば、教えてほしい。

戸川構成員)

事例が少ないのはそのとおりであり、大きな問題であると考えている。リバースエンジニアリングを行うことによって、解析を実施している研究者は存在するが、日本国内に限るとほとんどいないというレベルになっている。攻撃側がどのような事を考えて、攻撃しようとしているかという部分は、なかなか例がないところである。一番重要なのは、このような問題があるということを広く周知し、みんなが知るという状態になり、コミュニティが広がっていくことであると考えて

いる。そのうえでこのような可能性がある、このような場合があるため、このように対処していこうという議論を行っていくことが重要であると考えている。

小山構成員)

例えば、単品のマルウェアを作るコストと比較し、ファームウェアを改ざんしてバックドアを作るコストは、相当高いものになると思う。さらにハードウェアの設計段階から、バックドアを仕込むことになると、さらに指数関数的にコストが上がっていくことになるのではないかと考えている。仮に、国家レベルでの取組として、コストを度外視することもあるかもしれないが、どれぐらいのコストが掛かるのかという部分と、今後、どのような対策を採り得るかという部分の双方を見ながらのも必要になるのではないか。感覚的なものでよいので、コストについて教えてほしい。

戸川構成員)

ハードウェアレベルで実際にマルウェアを組み込む場合のコストについては、例えばトランジスタやマスクのレベルで組み込むことを考えると、非常に大きなコストが掛かる。これまでに作成した設計情報を製造現場に確保したまま、発現させたい機能だけを上手く埋め込むことは、専門的な知識が必要で、かつ場合によっては工場の中に入り込むことが必要になるため、かなり難しく、非常に大きなコストが掛かる。一方で設計段階においては、通常、ハードウェア記述言語を使って設計を行う場合がほとんどであるが、ハードウェア記述言語は簡単に言うとテキストファイルである。そこに非常に簡単な不正回路を記述しようとすると、おそらく５行ぐらいのコードで書ける。５行ぐらいのものを、数万～数十万行あるコードの中に埋め込むことになるため、一度テキストファイルを入手できれば、その中に書き込むことは容易である。

岡村構成員)

ハードウェアマルウェアを組み込むという形になると、日本の現行刑法上も「不正指令電磁的記録に関する罪」の構成要件に、故意であれば該当する。意図しようがしまいが、ユーザの意図に反する動きを行い、それに危険性が伴えば、ハードウェアであるため、PL 法の対象になる場合があり得る。このような整理を自分なりに行ってきた。例えば、テレビや家庭用レコーダーはネット家電としてイーサネットに繋げられるような形になっている。メーカ側は、チップを入れていて、どのような番組をどう視聴したかといった情報を集めて売っている。ユーザの意図に反しているような場合が多いと考えられるが、どこまでをアウトにし、どこまでをセーフにするのかは、ユーザが意図していると言いながらも、どこかで線を引かなければならない。かなり難しい場合があると思うが、そのあたりについて、どのように考えているか教えてほしい。

戸川構成員)

ハードウェアトロイは、何をもって、意図している、意図していないと考えるかは難しい問題である。現状においては明確な定義がなく、議論されている状況である。一つ言えることは、組み込まれた機能を使って、例えばハードウェアの中身を見ることができたり、ハードウェアの中から情報を引き出すことができたりすることができるかどうかは、１つの線引きになる。それが意図しているか、意図していないかは別問題になる。仮にそれが意図しているものであれば、そのような機能が見つかったときに仕様通りであるという話になる。反対に意図していないものが見つかった場合には、これは何だという話になる。意図しているかどうかが分からないので、おそらく技術的に解決できることは、ハードウェアの中身を見る、ハードウェアの中から情報を引き出すといった何かしらの特定の機能を持っているか、持っていないかについ

て見ることである。人間の心の問題にもなるので、それが故意であるかどうかを判別することは技術では解決することはできない。そこから先は、実際にそれをどう使っていくかという話になるのではないかと考えている。

後藤座長)

「資料 19－3」の 6 ページに次世代ネットワークセキュリティの全体の図があり、そこにたくさんの赤い爆弾が描かれている。ハードウェアレベルやソフトウェアレベル、アプライアンスレベルのものがあり得る。それに加えて、サプライチェーン上のどこで入れられるかという議論や、ライフサイクル上のいつアップロードされるかという時間軸の議論があった。さらにハードウェアチップ脆弱性検知手法の議論があり、３次元ぐらいの組み合わせが出来ており、これらの中でどこをどうしていくかについて次回の会合で取りまとめていく必要があると感じる。課題の範囲が広いということを再認識したところである。

徳田構成員)

「資料 19－3」の内容について補足したい。NICT の中で推進している AI 技術を使ったセキュリティは世界的なトレンドになっており、ダイナミックに研究が動いている。フランスやドイツ、米国、MITRE 社と NICT はマルウェアの情報を共有している。既に脳情報分野の NICT の CiNet はオープン化されているが、AI 技術を使ったセキュリティのデータプラットフォームについても国内に設置して国際的に連携できるようにすることが重要である。どこまでの情報をオープンにすることができるかはチャレンジになるが、研究者がセキュリティオペレーションの自動化や高度な検出技術などの領域で次の次元に進むためには、このようなデータプラットフォームが大事になる。NICT としては、しっかりと国際連携しながらこのようなデータプラットフォームを作っていきたいと考えている。

後藤座長)

本日ご披露いただけなかった意見については、明日までに事務局に連絡いただきたい。

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 20 回については、年明けの開催を予定している。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