参考資料１

サイバーセキュリティタスクフォース（第 17 回）議事要旨

1. 日 時：令和元年 11 月 22 日（金）10:30～12:00

2. 場 所：中央合同庁舎 2 号館 8 階　第 1 特別会議室

3. 出席者：

【構成員】

後藤座長、鵜飼構成員、小山構成員、齋藤構成員、園田構成員、戸川構成員、中尾構成員、林構成員、藤本構成員、吉岡構成員、若江構成員

【オブザーバ】

寺岡優(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)、金城賀真(代理) (地方公共団体情報システム機構) 、衛藤将史(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、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、中溝消費者行政第二課長、清水消費者行政第二課企画官、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(室長代理)、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 17－1　今後の検討課題とスケジュールについて

資料 17－2　昨今のサイバー攻撃や注目すべき事象について

資料 17－3　NICT におけるセキュリティ人材育成について

資料 17－4　ISAC を活用する情報共有について

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　サイバーセキュリティタスクフォース第 16 回　議事要旨

参考資料３　日米 ISAC 間の覚書について

参考資料４　「サイバーセキュリティに関する総務大臣奨励賞」の募集開始

5. 議事概要

(1) 開会

(2) 議事

◆ 議事（１）今後の検討課題とスケジュールについて、事務局より、「資料 17－1　今後の検討課題とスケジュールについて」を説明(省略)

◆ 議事（２）IoT のセキュリティ対策について、吉岡構成員より、「資料 17－2　昨今のサイバー攻撃や注目すべき事象について」を説明(省略)

◆ 議事（３）人材育成の推進について、衛藤将史氏より、「資料 17－3　NICT におけるセキュリティ人材育成について」を説明(省略)

◆ 議事（４）情報共有の促進について、中尾構成員より、「資料 17－4　ISAC を活用する情報共有について」を説明(省略)

◆ **構成員の意見・コメント**

鵜飼構成員)

最近、セキュリティベンダーが広域スキャンを実施していそうな雰囲気を感じている。広域スキャンを実施して何か問題がありそうであれば、レポートを作成して販売するということもある。その辺りの実態について何か把握していれば教えてほしい。

吉岡構成員)

広域スキャンの中で、セキュリティベンダーが実施していると思われるものが多数ある。一部のセキュリティベンダーについては、その素性が見えている。

小山構成員)

IP アドレススキャンについて、課題となる事例をご紹介したい。ドメインから企業が持っている IP アドレスを調べて、それらの企業のセキュリティ情報を積み上げて、その評価の結果として報告書を公表したり、販売したりするということを複数の事業者が実施している。企業の評価に使われる場合はビジネスに影響が出る場合も想定され、技術的なセキュリティ対策とは別の側面での注意が必要である。「資料 17－1」に関して、短期的な取組と中長期的な取組に分けて検討を進めることは良い方法であるので、是非とも協力させていただきたい。そのような意味合いにおいて重要 IoT 機器の対策は、短期的に、できれば東京オリンピック・パラリンピック競技大会の開催までに対策を終えたいというものになる。今後の中長期的な取組については、IoT 機器がインターネット接続のためにポートが開いているだけで、将来のリスクに繋がるというメッセージが「資料 17－2」に出ていた。その動的な IP アドレスにぶらさがっている IoT 機器が外からのアクセスを期待してポートを開けるということはまず考えられない。そのような IoT 機器が仮にリスクの根源に近いものであれば、IoT 機器に対する対策を今後どうしていくかということについて制度面も含めて考えていく必要がある。

もう１つ中長期的な取組として、通信事業者の悩みとなっているのは、従来よりマルウェアに感染しているパソコンのユーザに対する注意喚起を行っているが、IoT 機器の場合は機器の数が膨大になり、使用者も当事者意識が希薄であるため、注意喚起の効果が日増しに薄れてきているということである。そのような状況の中で、C&C サーバとの通信のブロックについての合理的な進め方など、制度面も含めて実施できる方向で検討を進めてもらいたい。

人材育成について、セキュリティ人材育成のための新会社を設立した。「資料 17－3」で説明のあった人材育成とは少し異なっている。そもそもセキュリティ人材がいないので、育成しようにも種がない。種を作るために理系の学生に対して、給料を支払って勉強してもらい、セキュリティに目覚めてもらう。そこから育成しようという取組を行うための新会社の設立である。そもそもセキュリティ人材の方向に人を向けていくという入口の部分も必要であると感じている。

後藤座長)

IoT 機器についてはコンシューマ向けだけでなく、インフラ設備にも埋め込まれているという話が出た。それにも関係するが、NICT のセキュリティ人材育成については自治体向けという話も出た。その辺りの関係性も含めて何か意見があれば頂戴したい。

藤本構成員)

攻撃が成功した場合にどのような事態になるのかというところがあまりイメージ出来ていない。リスクマネジメントには、未然防止を図るものと、事故が起きてしまった場合に適切に対処できるための準備というものがある。今までの話は、未然防止が中心ではないかと思う。事故に対し素早く適切に必要なプロフェッショナル人材を投入して、被害の拡大を防ぐという部分に対して、どのような準備が必要になるのかという視点も、特に重要インフラや重要インフラの１つである自治体においては重要になるのではないかと考えている。

若江構成員)

サイバー攻撃を防ぐための論点も重要であるが、大規模災害で障害が発生した場合の迅速な復旧についても非常に重要ではないかと考えている。特に IoT が広く普及した社会で、大規模な事故が発生した場合の通信の影響が今まで十分想定されていないのではないか。そういう部分に不安を感じている。大規模停電が発生して、その後復電したときに IoT 機器が一斉に起動し、一斉にセッション要求が発生することになるため、DDoS 攻撃のようになってしまう場合がある。そうなると１回復旧しても障害が継続してしまうという話を事業者から聞いたことがある。そのような場合にどのように対応するのか、遠隔で復旧の順番をコントロールするといったことを実施している事業者もあると思うが、IoT の場合はコストが安くなっているところもあり、十分対応できていない部分があるのではないかと考えている。今まで IoT がこれほど普及した状況での事故が起きていないということもあり、どういうことが起きるのかを想定する必要があるのではないかと考えている。

中尾構成員)

当然ながら事故を未然に防ぐことを検討するのは重要であるが、例えば、重要インフラ分野の ISAC を含めて、どういう情報が共有されているかと言うと、脅威情報だけでなくて、何かインパクトがあったときに、どのようにリカバリーしているのかという情報も共有されている。IoT の探索や研究は、インパクトがどこまであるかという部分には踏み込めない。そのため、実際に起きたインシデントから、それをどのようにリカバリーしたかという情報は非常に重要になってきており、そのような情報のシェアリングを行っているのは確かである。例えば、ヘルスケア分野においてもランサムウェアが発生して、病院のカルテシステムなどが停止した。それをどのようにリカバリーしたか、復旧に長い時間がかかったので、それに対してはこのように対処した方がよいという議論が行われている。NICT の人材育成の中でもいろいろな演習が行われており、何かを発見するというものもあるが、演習の中の１つのプロセスとして、機器が乗っ取られて何かが起きたときにどれをどのようにリカバリーするかというものも含まれている。インシデントのリカバリーという部分が全部抜けているという訳ではないという気がするが、他部分より注目が少ないという印象は受ける。その理由としては、インシデントのインパクト分析は攻撃を受けた組織しか実行ができないため、組織の状況に依存するリカバリー処理を共有しにくいということも影響していると考える。

後藤構成員)

共有されたインシデント情報を自社に当てはめて、自社においてどのような被害が起こり得るかというシミュレーションまで実施することが非常に重要である。

戸川構成員)

IoT セキュリティ対策を考えたときに、トップに近い戦略マネジメント層の方々がどこまでセキュリティのことを考えているのかについて非常に気になるところである。例えば、パスワードがデフォルトのままであるといったようなところは、ある程度そういうところに気を付けるという意識があれば、未然に防げるところが多分にあると思う。それに対して、戦略マネジメント層の方々がどういったところまでそのような意識を持っているのかという点が重要な問題である。一方で、人材育成の観点からの話を申し上げると、理工系の組織にいる者として、ある程度はセキュリティに関するマインドは育成されつつあるのではないかという印象を受けているが、ただセキュリティの意識が高まってきている若手の方々が戦略マネジメント層になるまでには少し時間がかかる。 IoT の普及を考えると、現状で早急に採るべき対策としては、戦略マネジメント層を含め、社会全体でセキュリティを意識していない方々が、セキュリティを意識していくことが重要であると考えている。

齋藤構成員)

NICT が実施している「CYDER」の演習に放送事業者も参加している。先ほど企業や自治体の戦略マネジメント層の意識について話が出たが、「CYDER」の演習は開催回数や開催地域が細かく設定されているにも関わらず、自治体の中には、まだ参加していないところもあるということであった。リーダーの方々の人材育成が重要であるという意識を高めて、参加を促す体制を整備しなければならないと考えている。放送事業者は重要インフラ事業者の取組として NISC の「分野横断的演習」にも参加している。どちらかと言うと「分野横断的演習」は手順重視の演習であり、「CYDER」は技術面で有効な演習である。「CYDER」は民間放送事業者や重要インフラ事業者が参加するには費用がかかり、参加が鈍っているところがある。この点については政策的にフォローしてもらいたい。

園田構成員)

個別の IoT 機器そのもののクオリティをアップしていくに際しては、サプライチェーンの問題やメーカーの問題など様々な問題があり、短期的な改善は求められない。息の長い対策にどうしてもならざるを得ない。即効性のある対策も一方で必要なのではないかという印象を受ける。情報を集約して脅威検知を行う仕組みや、相手のリストを陳腐化するような技術など、おそらくそういうものが必要になってくると思う。相手のリストを陳腐化するのはインターネットの根幹に関わるものであるため、技術的な開発や研究を含めてかなり難易度が高いものであるが、情報を集約して脅威を検知し対抗する仕組みについては、もう少し短いスパンで実現できるのではないかという印象である。リバースアプローチ的にみて登録された機器に対して、一時的に脅威を検知する仕組みをアドオンしてもらう。そうすると機器を導入しても登録さえすればよいということになる。そういうサービスが民間でも提供されているので、そういう方向性について検討し、制度にするのか、強制するのかを検討できれば、もう少し即効性のある対策が採れるのではないかと思う。

後藤座長)

「資料 17－1」に短期的な取組の例と中長期的な取組の例について事務局から示されているが、人材育成にしても技術開発にしても、両方の面がある。次回以降に向けて、何かヒントになるようなコメントを含めて意見を頂きたい。今の話は技術開発についても、短期的な取組があるのではないかという意見であったが、中長期的な取組も必要であると思う。ま

た、人材育成についても、若手からじっくりと戦略マネジメント層を育成するという話もあれば、１日２日の演習であれば、幅広く全自治体に参加してもらうためにはどうしたらよいかという話もあった。

吉岡構成員)

今後の議論にどれほど繋がるか分からないが、以前から問題意識を持っているものがある。標的型攻撃やランサムウェア、フィッシングなど以前からあるが、未だに非常に大きくなっている問題がある。結局、セキュリティは情報を集めて、どのように対策を講じるかという話になってきて、どこに脅威の情報や攻撃の情報が集まってくるかということを考えると、どうしても避けて通れないのが、巨大 IT 企業であり、そこにそのような情報が集まらざるを得ない状況になっているのではないかと考えている。例えば、標的型攻撃のメールを検知する際に、各企業が独自に実施することは、どう考えても無理がある。横浜国立大学のメールシステムにはマイクロソフトの Office365 を導入しているが、事実上、マイクロソフトに守られていることになっている。それはある意味リーズナブルである。マイクロソフトはそのようなサービスを広く提供しているので、いろいろなところで脅威情報や攻撃情報が自然と集まってきており、強みを持っている。そのように考えると、従来から ISP が通信インフラの観点でそのような情報を持っていて、様々な対策に貢献している。そのような状況は今後も続くと思われるが、一方で上位のレイヤーで多様に貯まってくる情報が対策に重要になると考えている。その部分の情報がかなり抜けてしまっている。どこでどのように情報を集めて、どう有効活用するかという観点が必要なのではないかと考えている。ただ回答がない問題意識で、どうすればよいかという解がない状況になっている。最近、ヤフーと LINE の経営統合の話があるが、国内でもたくさんのユーザを持っていて、いろいろな情報が集まるという方法が出てくるか分からないが、どこに脅威情報や攻撃情報が集まるかを意識して考えていく必要がある。

後藤座長)

自治体への人材育成の普及や、IoT は自治体が管理するケースが多いので注意しなければいけないということを考えると重要インフラのセキュリティということが話題になった。また政府や自治体の調達については、クラウド調達のセキュリティが議論されているが、幅広く IoT も含めて出てくるとなると、考えるべきことが非常に多い。そういう部分について、次回のタスクフォースは重要インフラのセキュリティの話もあるため、次回以降に議論させていただきたい。本日の会合の中で披露できなかった意見については、本日中までに事務局まで連絡していただきたい。

相川サイバーセキュリティ統括官室参事官補佐)

次回以降のサイバーセキュリティタスクフォースの日程について、第 18 回会合は 12 月 5 日（木）の 14 時～、第 19 回会合は 12 月 25 日（水）の 14 時～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。

「参考資料４　サイバーセキュリティに関する総務大臣奨励賞の募集について」は、本日 14 時公表を予定している資料になっている。本奨励賞は平成 29 年度より実施している。サイバーセキュリティ対応の現場において、優れた功績を挙げられ、今後も更なる活躍が期待されている個人の方又は団体の方を表彰したうえで広く周知することで、我が国におけるサイバーセキュリティ意識の向上を図り、サイバーセキュリティに確保につなげることを目的に実施させていただいているものになる。本日から 12 月 27 日まで自薦、他薦の方を受け付けており、積極的な推薦をお願いしたい。

以上