サイバーセキュリティタスクフォース（第 13 回）議事要旨

1. 日 時：令和元年 5 月 10 日（金）10:00～11:30

2. 場 所：中央合同庁舎 2 号館 9 階　第 3 特別会議室

3. 出席者：

【構成員】

徳田座長代理、鵜飼構成員、岡村構成員、後藤構成員、戸川構成員、中尾構成員、名和構成員、林構成員、藤本構成員

【オブザーバ】

吉川徹志(内閣サイバーセキュリティセンター)、木村隼斗(経済産業省) 、

【総務省】

竹内サイバーセキュリティ統括官、泉審議官(国際技術、サイバーセキュリティ担当)、二宮サイバーセキュリティ・情報化審議官、木村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)、三田地上放送課長、沼田技術政策課技術調査専門官、福島通信規格課企画官、山崎宇宙通信政策課課長補佐、藤田電気通信技術システム課長、中溝消費者行政第二課長、相川サイバーセキュリティ統括官室参事官補佐、篠崎サイバーセキュリティ統括官室統括補佐、豊重サイバーセキュリティ統括官室参事官補佐、後藤サイバーセキュリティ統括官室参事官補佐、橋本サイバーセキュリティ統括官室参事官補佐

4. 配布資料

資料 13－1　「IoT セキュリティ総合対策」の見直しの方向性（事務局作成資料）

資料 13－2　構成員からの御意見のまとめ

資料 13－3　「IoT セキュリティ総合対策」プログレスレポート 2019（5/10 時点版）

参考資料１　「IoT セキュリティ総合対策」

参考資料２　「IoT セキュリティ総合対策」プログレスレポート 2018

5. 議事概要

(1) 開会

(2) 議事

◆　事務局より、資料 13－1　「IoT セキュリティ総合対策」の見直しの方向性（事務局作成資料）を説明しつつ、説明に関連する構成員からの御意見について、資料 13－2　構成員からの御意見のまとめを用いて説明 (省略)

◆　**関係者の意見・コメント**

岡村構成員)

資料 13-1 の 1 ページに関して、脆弱性調査と注意喚起の結果、問題案件のうち少なくとも重大案件については、一定期間を経た後に是正の有無について事後確認を行うことも大切ではないかと思う。注意喚起までで終えると結局放置されたまま何も変わらないということになりかねないので、かつて違法サイトに対して、各省庁が「インターネット・サーフ・デイ」という取組みを行ったが、それと同様の取組みについて検討してほしい。

脆弱性対策の推進において、オープンソースでプロジェクトが消滅しているケースが問題になる。そのような是正のしようがないものや、どこへ注意喚起してよいか分からないものについては、どのように対応していく必要があるか。例えば、使ってもらっては困るものについて公表することなども視野に入れて考えなければいけない問題であると考えられる。

名和構成員)

「資料 13-1」の 4 ページに関して、IoT 機器に対する攻撃が進行中である中で、脆弱性対策の体制整備が一定程度完了したという文章表現に違和感を覚えた。サイバー攻撃の踏み台については、昨年あたりから、外部の組織や外部の機材に向けたものだけではなく、組織の中や組織内の機材に向けたものも出てきている。このようなルーブ・ゴールドバーグ(Rube-Goldberg)型攻撃に対する認識が資料上で確認できない。ルーブ・ゴールドバーグ(Rube-Goldberg)型攻撃については、２つの議論の反映が重要になる。１つ目の議論としては IoT 機器メーカで独自に作っているソフトウェアの領域が徐々に小さくなり、サードパーティのコードやそのライブラリにかなり頼っている中でデビルズアイビィ(Devil's Ivy)という脆弱性に対する認識の反映が足りない。このデビルズアイビィ(Devil's Ivy)は、IoT 機器メーカが開発速度を上げたり、安定性を高めたりする中で使っている数百万以上あるサードパーティのコードを利活用しており、攻撃者がそれを狙ってきている。２つ目の議論としては、IoT 機器メーカがいかに脆弱性対策を実施していても、過去に作ったサードパーティのコードを悪用してアカウントを乗っ取ったり、開発サーバの脆弱性を突いて違うコードを提供したりしていて、これがなかなか見つからない状況となっている。また、脆弱性管理の監視対象が数百万のサードパーティに上るため、実質的には管理が不可能となっている。雑草対策と同じ状況であることから、雑草の植物名に由来したデビルズアイビィ(Devil's Ivy)という名前が付けられている。

中尾構成員)

NOTICE のプロジェクトは、稼動している既存の IoT 機器を遠隔から脆弱性を確認して、脆弱性のある機器の保有者に対しアラートを通知し是正してもらうようにしている。NICT としては、デビルズアイビィ(Devil's Ivy)を含め標的型攻撃や内部犯行等に使われるような検体を STARDUST の中で動かして評価している。デビルズアイビィ(Devil's Ivy)だけでなく、いろいろな APT のキャンペーンを含めて、実施しなければいけないことはたくさんある。そのあたりを「IoT セキュリティ総合対策」の中でどのように書き込んでいくかがポイントになり、無視はできない。

「資料 13-1」は、構成員の意見を取り込んで、網羅的な内容になっているが、整理が不十分であるという気がしている。例えば、現在のサイバーセキュリティの環境で IoT がベースになっているが、IoT の世界はエッジ部分には 5G、その裏の部分にはベースとなるクラウドがあって、その中には AI 等のテクノロジーがあり、全体としてみるとスマートシティが形成されており、それらのセキュリティを検討する１つの領域がある。他方、それらのコンポーネントを含めて、基盤の部分のセキュリティについて、暗号危殆化やハードウェアセキュリティ・チップセキュリティ等を検討する領域がある。また、広域ネットワークスキャンを行うことによって、いろいろな基礎データを収集する日本版 SHODAN のような基盤的な活動について検討する領域がある。それに関連して、NOTICE に関しては、アクセスコントロールや PW 設定等の端末接続の技術基準を作っているが、そのような基準やガイドライン、国際標準について検討する領域もある。そこに米英仏独が、IoT 機器のセキュリティガイドラインをコンシューマ向けにリバイズするために、リクワイヤメントのような形で出してきている。それを受けて、日本としては、設備に対する技術基準の中に盛り込むのか、「「IoT セキュリティ総合対策」」の中で適切なガイドラインづくりを行っていくのかという部分が１つの戦略になってくる。前述したようなア

プリケーション領域、基盤領域、基準やガイドラインを国際標準に持っていく領域、人材育成の領域という４つの大きな柱があって、現在「資料 13-1」に書かれているものを再整理するともう少し分かりやすくなるのではないかと思う。

戸川構成員)

総務省以外でも、IoT セキュリティのさまざまなレポートが出てきていると認識している。「IoT セキュリティ総合対策」では、５つの柱から構成されているが、別の省庁からは別の観点で、または IPA のような別の組織からさまざまなレポートが出ている。どこが何をカバーしているかという全体の俯瞰ができると、「IoT セキュリティ総合対策」プログレスレポートの位置づけがより明確に分かりやすくなると考えている。欧米を含め世界中でどういったセキュリティ対策がどのレベルで出ていて、それが我が国の「IoT セキュリティ総合対策プログレスレポート」とどういう関連性があって、整合性が取れているのかどうかが見えると議論が分かりやすくなると思う。

藤本構成員)

「資料 13-1」の 13 ページに関して、情報共有が今後重要になると考えられる。言うは易し行うは難しで情報を出してもらうことがなかなか難しいので、閉じた世界で情報を共有したり、同じ業界などの信頼できる企業間で情報を共有したりすることによって、より深い情報が出てくることはある。それに加えて、そのような情報が集まってくる総務省等においても情報をサマライズして、傾向を見て、どこの話であるか分からない形で情報をオープンにするような工夫をしてほしい。情報共有の効果がより一層高まると考えられる。

鵜飼構成員)

小規模事業者に対するサイバーセキュリティ対策をどうしていくかという部分で、地域のセキュリティ人材の育成やセキュリティ人材のシェアリング、人材エコシステムの形成が記載されているが、そもそも現状としてこういったことを出来る人がいないので、このような取組みを行っていくことは重要な試みである。一方で、そうは言っても小規模事業者の圧倒的大多数はそもそも関心がないという状況であるので、育成された人材が、どのようにして関心がない小規模事業者に対してリーチをしていくかが重要であると考えているので、今後そのような議論を行ってほしい。

人材が育成されても、現実的には小規模事業者はお金がない状況である。セキュリティベンダーにおいては、このような小規模事業者に対して安価に提供できる何らかのサービスを考えていかないといけないと考えているが、その一方で関心がない小規模事業者に対してサービスを作って安価に提供しても赤字覚悟になってしまう。このようなリスクと潜在的な必要性のギャップを埋めていくような何らかの施策があると人材が育成された後の対策が進むのではないかと考えている。このような施策について今後検討してほしい。

数多くの防御ソフトが提供されているが、総合力のレベルを示していく必要があるのではないかという議論がこれまでにあったが、どれが良いのか悪いのかが分からない、またそれを検証するのにも専門的な知識が必要になってくる。よほど専門的な人材がいる大企業でなければ、現実的には比較検討は難しいのが現状である。マルウェア対策１つ取っても、検証する対象やその母数、取得するタイミングの違いで評価結果が大きく変わる。また時期によっても、防御ソフトの優劣が大きく変わる。一方でカタログに書かれているスペックが本当に適切に実装されているのかということも重要であり、そういったことを見ていく必要があると考えている。

徳田座長代理)

国が実施するべきか、民間や業界団体が自主的に実施するべきか、さまざまな位置づけが考えられる。国が実施するよりも、民間が実施した方がタイムリーにレポートがアップデートされると思われる。

後藤構成員)

それぞれの取組み案や取組み項目の依存関係、政策チェーンのようなものについて、先ず時間軸を考えた方がよい。量子分野のように将来必要となる基盤技術がある一方で、IoT 機器の脆弱性対策のように現在の製品をチェックし、それを見ながら製造中の機器に対して評価を行うものもある。更にその先に向けては構成要素であるソフトウェアや部品のそもそもの素性をチェックするものもある。そういう形のものが依存関係を構成していて、現在取り組んでいるものが、将来役に立つためには、別に実施しているこの取組みとこの取組みが出来て、その先になるといった時間軸上の展開案をしっかりと見極め、併せて検討していく必要がある。そうなると意義が整理しやすくなる。

名和構成員)

「資料 13-1」の 9 ページに関して、内閣府の宇宙開発戦略推進事務局が進めている「みちびき」は 4 基が稼動していて、将来的に更に 3 基が打ち上げられる予定である。このような公共専用サービスのセキュリティに対する支援やその検討は工程表の中で考えられているのか。

現在、公共専用サービスを運用している事業者においては、官からの支援が少ないということで困っている。このまま行くと、公共専用サービスを使う可能性がある防衛省や警察庁、海上保安庁等がセキュリティの弱いものを使い始めてしまう可能性がある。衛星通信におけるセキュリティ技術の研究開発の時間軸が、2018 年度から 5 年間に設定されているが、それだと間に合わないと考えている。途中経過からでもセキュリティ技術をインプットし支援してほしい。

徳田座長代理)

宿題という形で引き取らせていただきたい。NICT の中にセキュリティ技術を開発しているチームがある。そこでの成果を総務省と共有して書き込める部分があれば記載する。

岡村構成員)

セキュリティ製品の優劣比較については、景品表示法の有利誤認という制度があり、それとの関連で比較広告のガイドラインが策定されている。ただし ICT を対象としたものになっていないので、省庁連携のような形で、総務省の制度として、NICT の力を借りながら、製品の優劣比較をサポートできるようにすることも 1 つの方法としてあり得ると考えられる。

林構成員)

オリンピック競技のチケットを購入する際にもインターネットを使うような時代になってきている。IoT 機器についても使わなければ今後生活ができなくなる。さまざまな施策を検討する中で、それらが段々と細かくなってきている一方で、簡潔に説明できるようにすることも求められる。その中に個人という目線がなかなか入れられないが、個人という目線については忘れてはいけない。

中尾構成員)

IoT セキュリティ対策については、先出しじゃんけんのような状態になっていて、クリアなリボケーションがあんまりない。英国は昨年、デバイスベンダーや製造者に対して、コンシューマ用デバイスに関する行動指針を出している。それは日本の設備に関する技術基準に非常に近いものとなっている。例えば、原則として初期 PW は設定しない、脆弱性に関する情報は公開してほしい、ソフトウェアは定期的に更新する、認証情報は安全な形で送受信する、通信そのものを安全にするなど、全部で 13 項目について書かれている。他方、米国は IoT デバイスをカテゴリーに分けてレベル分け・レイティングを行い、それぞれについて厳格なセキュリティのコントロールをリスト化している。双方の形態はかなりオーバーラップしつつ表現は大分違っている。IoT 推進コンソーシアムの取組みをベースに、日本の中でもそういうものの出し方について検討していかないといけない。国際標準化は進めているが、そういうものを見ながら方向性を考えていく必要がある。

岡村構成員)

PW を定期的に変更するべきであるとする国もあれば、みだりに PW を変更すべきではないとする国もある。後者については、米国の巨大 ICT ベンダーでそれに追従するような見解が出されている。PW を変更しなくてもよいというのは、単純で脆弱な PW は使ってはいけないということや、PW の使い回しは行わないということが前提にあってはじめてそのような話になる。消費者はどちらを信じてよいのか分からなくなっている。そういう部分について目配りを行うことが必要であると考えている。

中尾構成員)

英国は初期 PW を設定しないと言っているだけで、PW を頻繁に変えなさいとは一言も言っていない。それについては、欧米はあまり言っていないような気がしている。一方、日本は PW を頻繁に変えなさいと言っているところが案外多く、文化が違うのかもしれない。日本は E メールを送るときに暗号化したり、圧縮したりする際の PW を、同じ E メールで送ったりしているが、欧米はそのようなことをしない。日本独特の環境がある。

徳田座長代理)

「資料 13-1」の 17 ページに関して、もう少し国際的に貢献できる項目を増やしてもよいのではないかと思う。我が国は、SDGs に向けて、どのような貢献ができるか検討しているが、例えば、サイバークリーンセンターが稼動していた頃、アジア諸国に対して積極的な連携を行っていたように、アジア諸国における汚染の状態やどれぐらいサイバー空間がヘルシーであるかという部分の可視化を行っていくことも考えられる。マイクロソフトリサーチなどいろいろなものが出ているが、今後アジア諸国の人たちがサイバー空間上でビジネスを行う際において、公衆衛生のパラダイムに近いものとして、それらを経年的に見られるものができると、その計測を国内だけではなく、アジア諸国でも行うことができる。そのあたりについて日本が積極的にリードして、ツールや情報発信を外に向けてもう少し強くしていった方がよい。IoT 推進コンソーシアムの取組みをもとに国際標準にシフトしているところだが、その戦略を含めて世界にもう少し貢献できるのではないかと考えている。

国際連携を進めていくうえで、トラステッドなコミュニティをみんなでどのように作っていくかが重要になる。仏独が、日本をはじめ、GAFA と中国に比べて AI の開発等で遅れてしまったため、連携を進めたり、セキュリティについて連携したりしている。基本的な価値観を共有する国々で、トラステッドなコミュニティをどのように作っていくかというキーワ

ードで戦略的に日本がアジア諸国でリーダーシップを取って、そのようなコミュニティを広げていく。その際にセキュリティはツールになると考えられ、前向きにみていろいろな形で貢献できるとよい。

林構成員)

詐欺やうそ、フェイクニュースなどが世の中に蔓延しており、それに対してどう取り組むかということを真剣に考えなくてはいけない。それについては行動経済学的な観点からのいろいろな施策がある。それらはナレッジという塊で米国や英国は取り組んでいる。交通信号のやり方など世の中にはいろいろな規制があって、それがみんなのために上手く機能するかが重要な要素になる。サイバーセキュリティにおいても、そのような要素がたくさんある。それらを事例として一度情報を集めて、施策レベルで何ができるか検討した方がよい。いろいろなことが分かってくると思うので、一度それらの大まとめをしなければいけない時期に来ているのではないかと思う。

岡村構成員)

全体が見えにくいという指摘が出ている。振り返って、OECD のセキュリティガイドラインを改訂した際に、カルチャー・オブ・セキュリティというキャッチフレーズを出したことがかつてあった。IoT セキュリティ文化の実現に向けて、現在の状況を一言で言い表す何らかのキャッチフレーズを副題として付けられないかと思う。その点について検討してほしい。

徳田座長代理)

たくさんのことが書いてあるけれど、キャッチーな形、分かりやすい形にした方がよいというのは重要なポイントであると思う。

鵜飼構成員)

国際連携に関して、ASEAN を中心にさまざまな活動が行われているが、当社も独仏蘭のコミュニティに参加して、さまざまな活動を行っている。北米よりも、独仏蘭は日本に近いカルチャーがある。EU 諸国は産官学の連携が密であり、日本においては、まだまだプレゼンスが足りていない部分があるという気がしている。今後、このような EU 諸国のコミュニティ活動に積極的に参加できるようにする施策が実現されるとよい。

竹内サイバーセキュリティ統括官)

私どもが気づかなかった点について、重要な意見を頂き、御礼申し上げたい。２年前にまとめた「IoT セキュリティ総合対策」の柱立てをドラスティックに変えてしまうと読者のフォローができなくなるので、議論の出発点としては、柱立てを変えない形で示させていただいた。「IoT セキュリティ総合対策」は脆弱性対策の推進を大きな柱にして、施策の塊を当面の施策から将来の施策までパッケージ化している。それ以外のところについては、切り口で整理している。それに加えて、施策によっては全体を通して見られるようなまとめの方法もあり得ると感じた。特に 5G のような今後の広がりのあるものについて、IoT と同じように、ある程度塊でまとめていくのも１つのアイデアであると思う。

政府全体の施策との紐付けや、全体の俯瞰の中で位置づけを示すことについては、NISC においてまとめているような戦略や各府省がまとめているよう年度の施策の中で、この部分に取り組んでいるということを紐付けしてビジュアルに示す

ことはできると思う。「IoT セキュリティ総合対策」の進捗状況がどのようになっていて、今後何を目指すのか、そこで研究開発や国際連携等を含めてどのように連携してしっかりと進めていくのかという点について、全体としてきちんと分かり、伝わるようにしていきたい。「資料 13-2」で拾えていない意見も多々あり、汲み取り方が足りない点も多々あると思うので、本日頂いた意見も含めて反映して、より良いものにしていきたいと思う。また追加の意見も歓迎である。それらに前向きに対応していきたいと思う。

以上