サイバーセキュリティタスクフォース（第 10 回）議事要旨

1. 日 時：平成 30 年 7 月 2 日（月）16:00～18:00

2. 場 所：中央合同庁舎４号館 12 階　全省庁共用 1208 特別会議室

3. 出席者：

【構成員】

安田座長、鵜飼構成員、岡村構成員、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】

山内智生(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】

谷脇政策統括官(情報セキュリティ担当)、澤田サイバーセキュリティ・情報化審議官、柳島参事官(行政情報セキュリティ担当)、木村サイバーセキュリティ課長、福島サイバーセキュリティ課調査官、沼田サイバーセキュリティ・情報化推進室長、山田技術政策課オリパラ技術革新研究官、根本通信規格課企画官、大村消費者行政第二課長、澤谷サイバーセキュリティ課課長補佐

4. 配布資料

資料 10－１　「サイバーセキュリティタスクフォース」開催要項（改正案）

資料 10－２　IoT セキュリティ総合対策　プログレスレポート 2018（案）

参考資料 10－１　サイバーセキュリティタスクフォース（第９回）議事要旨

5. 議事概要

(1) 開会

(2) 議事

◆　事務局より、資料 10－１　「サイバーセキュリティタスクフォース」開催要項（改正案）を説明 (省略)
◆　事務局より、資料 10－２　IoT セキュリティ総合対策　プログレスレポート 2018（案）を説明 (省略)

◆　構成員の意見・コメント

名和構成員)

10 ページに関して、例えば米国当局における中国電子機器メーカーの機器の利用禁止や部品の輸出禁止により、4 月下旬から一部の中国電子機器メーカーの製品のアップデートが止まり、脆弱性対策が実施できない状況にあるなど、今後の取組または進捗状況において、今起きている状況について触れられていないのはどうしてか。

日本のスマホや家電 IoT に使われている Android について、他国のそれよりアップデートの頻度が少ない。また、オランダでは、Samsung がアップデートが不十分ということで訴訟が起こり、現在係争中となっている報道がある。日本では、オランダのように、セキュリティを重要視する姿勢が希薄である印象を受けており、IoT セキュリティ総合対策の取組が足下から揺らぎかねない状況であると感じている。この部分について、何か記載する予定であるか、また何か検討中のものがあればお聞きしたい。

木村サイバーセキュリティ課長)

我が国において、明確に書き込めるようなものは今の時点では思いつかない。参考として、そういうものを記載できるかどうか検討する。

名和構成員)

今、かなりの頻度で Android のセキュリティパッチが提供されている。それだけ日本の Android 利用者が使っている端末自体の脆弱性が広がってきているので、個人的にはリスクが高まっていると思う。これは現実に起きている事象であるので、官民連携で取り組んでいく必要があり、このレポートの中でも何らかの取組が記載されるとよい。

岡村構成員)

32 ページに記載されている「橋渡し人材」という言葉について、情報開示分科会の主査の立場から、やや時代的にあまり使われなくなったのではないかという指摘をして、親会の方で検討することを進言してきた。それを受けての発言になるが、NISC 等の会議では、「橋渡し人材」ではなく、「戦略マネジメント層」という言葉が使われているので、このレポートでも共通用語として、「戦略的マネジメント層」という言葉を使いたいと考えている。構成員皆様の意見をお伺いしたい。

名和構成員)

「橋渡し人材」は、目指す方がいなかったり、経営層からも意味があるのか、CSIRT の担当者がやればよいという見方をされ、言葉の揺らぎが大きいと思う。中小企業では、マネジメント層が IT 部門に歩み寄り、IT 部門の事業を知ろうとしており、融合の取組が進みつつある。こうした人材育成に向けた取組が上場企業向けであるのか、中小企業を含めた企業全体であるのかをみて、一番多く使われている概念を表す言葉を使うのがよい。

中尾構成員)

「橋渡し人材」は何となく違和感がある。総務省の方で「戦略マネジメント層」という言葉を後押ししてもらえるとよい。

林構成員)

後藤構成員が担当している NISC の普及啓発・人材育成専門調査会でも、同様の改正案を出していたので、問題はないと思う。

安田座長)

構成員からの意見が大体まとまったので、「戦略マネジメント層」という言葉を使う方向にしたいと思う。

鵜飼構成員)

29 ページの AI を活用したサイバー攻撃検知・解析技術の研究開発に関して、資料 19 をセキュリティベンダーの視点でみると、既にいろいろなものが存在しているというように見えてしまいがちである。もう少し新規性のある部分や、今の実社会で解決できていない課題を解決する部分が重要であるので、そのような部分について前段にもう少し記載して、周囲からの批判にも留意する必要がある。

42 ページに記載されている未来のサイバーセキュリティ研究者・起業家の創出や、資料 29 に関して、研究開発に割りと偏っているふしがある。起業家を育成する取組に関する書きぶりが薄く、起業家を育成する心積もりが感じられないという批判が出る可能性があるので、書きぶりをもう少し厚くする必要がある。

中尾構成員)

AI を活用したサイバー攻撃検知・解析技術の研究開発は、NICT で現在取り組んでいる話である。AI については、どのような問題があるか、またどういうコリレーションのメカニズムを導くのに、どういうデータを集めて解析しなければいけないかといった根本に立ち返った議論を行っている。現在の文章において、もう少しその部分が分かるように記載してもらいたい。修正提案の文章を送らせていただいてもよいと思っている。もっと本質的な AI のテクノロジーを使ったコリレーション分析と、ディープラーニングを行っているので、そのあたりを追記した方がよい。

安田座長)

取り組んでいるが、成果が出ているとは言い難いので、プログレスレポートとしては難しいところである。修正提案の文章をいただくことにしたい。

戸川構成員)

このレポートは、非常に網羅的でよくまとまっていると思う。AI の書きぶりの指摘や用語の使い方の指摘など、そのような点が浮き彫りになるという意味で、IoT セキュリティ総合対策が策定されて、かつプログレスレポートで定期的に見ていくことは非常に重要であると思う。IoT のセキュリティに関しては、コストや機能安全、セキュリティの話がある中で、政府による何らかの指針、指標というものが役に立つが、プログレスレポートでは、今、政府が何を考えて、どのような対策をとろうとしているのかということが、細かく１つ１つの要素についてきっちり見えてくるという意味で非常によかったと思う。

1 ページのはじめにで記載があるが、サイバーセキュリティは非常に重要な案件になっているので、いろいろな省庁等で、いろいろな対策を打ち出してきている。それらがどういう位置づけにあって、どう整合していくのか、その対応づけについて常に意識しておくことが重要である。

木村サイバーセキュリティ課長)

政府全体の戦略との関係については、NISC の方で取りまとめられようとしているサイバーセキュリティ戦略があり、この中で総務省として、政府の一員として、いかに貢献していくかという部分の関係性を示すために、資料 3 をまとめた。こういう形のものは、新しい取組がでれば、そういうものとの対比をしっかり明示できるように引き続き進めていきたいと思う。

中尾構成員)

今後の取組のところの書きぶりになるが、心配事が何点かある。1 点目は、例えば、脆弱性のある IoT 機器を特定して、それに対して必要な対応をとるという総務省の施策は、日本中の IoT に関係するシステムやデバイスが何らかのマルウェアに感染して攻撃に加担するのを避けたいという狙いである。オリパラを控えて、ゲートウェイを上手く使う方法もあるが、IoT のシステムはコンフィグレーションが山のようにあり、簡単にゲートウェイを設置すればよいという問題ではなかった。このような日本の上手く対応した経験を海外に適用していくという視点が、あまり記載されていないので、どこかに記載した方がより網羅的な対策になると思う。

2 点目は、国際標準化の議論の中で、ドイツからアップデートの機能を適正に実装して運用するところについて、きちんと深堀りするべきであるという意見が出ている。一方、日本の IoT 推進コンソーシアムが公表するガイドラインには、そこまでの内容が書かれていない。IETF や ITU-T でもソフトウェアのアップデートに取り組んでいる。車のソフトウェアアップデートは JASPAR が JAMA と連携して取り組んでいる。このような流れがある中で、総務省の IoT セキュリティ総合対策の視点としても、ソフトウェアのアップデートが非常に重要になってくるので、このレポートの中で上手い書き方をしてもらいたい。

3 点目は、第 1 期の SIP の成果が、第 2 期の SIP にどう繋がっているのかが見えにくいので、総務省側でこのレポートの中に上手く溶け込ませることのできる知見を把握しているのであれば、教えてほしい。

4 点目は、IoT だけでなく、スマートシティやインダストリー4.0 などさまざまなコネクテッド環境が出てきて、いろいろなセキュリティ対策について考えていく必要がある中で、それを具現化する際にはユースケースを潰さないといけないという意見が専門家から出ている。そのような意見はフランスやドイツからも出ている。6 ページに記載されている IoT セキュアゲートウェイについては、ユースケースとして、カーモビリティ分野、スマートホーム分野、エデュケーション分野の 3 分野が採り上げられているが、この施策の今後の取組の中で、具体的なユースケースを絞り込むことを考えているかどうかを聞きたい。

木村サイバーセキュリティ課長)

1 点目については、書きぶりを検討させていただく。2 点目については、アップデート機能の実装というものの重要性をどう捉えるかの問題である。

中尾構成員)

最新の IETF や ITU-T の議論と、車の議論をまとめているので、共有する。それを見ていただいたうえで、書きぶりについて見極めていただきたいと思う。

木村サイバーセキュリティ課長)

どう書き込むかを含めて検討させていただく。4 点目については、IoT セキュアゲートウェイを実際に実装していくうえで、ユースケースごとに見ていく必要があるという観点から実証実験に取り組んでいたのが実態である。社会実装していくうえでのユースケースづくりは必要であると思う。今年度、そのような実証実験を実施するかどうかを含めて、実サービスに向けた取組の重要性を認識しており、また今回の実証実験で課題も明らかになっているので、そのような課題を解決しながら、必要があれば、新しいユースケース分野で実証実験を行うことも考えられるのではないかと思っている。

柳島参事官(行政情報セキュリティ担当))

3 点目については、第２期の研究開発計画についてパブコメが終了したところで、SIP 事務局が研究開発計画の最終的な取りまとめを行っている段階である。SIP の中で、第１期と第２期の時期が被っているのは、サイバーセキュリティの案件だけで、同じような中身にならないようにすると共に、全く異なる中身でもないようにするという難しさがある。そのような中で、第１期は主に重要インフラ事業者のサーバー等を対象としたサイバーセキュリティの取組、第２期はどちらかというと IoT 機器にターゲットを置いた形の取組という違いを出しつつ、またそれらの橋渡しも行うという視点を盛り込み、研究開発計画を取りまとめているところである。このレポートの中で、SIP との連携や SIP の成果を活かすという形での書きぶりができると思うので、後藤構成員とも相談して、書きぶりを検討したいと思う。

山内智生(内閣サイバーセキュリティセンター))

資料 3 でまとめられている内容について、今月中に決まる新しいサイバーセキュリティ戦略の中で、今後はこれに紐づく年次計画を、総務省等の各省庁の施策を中心にまとめることになる。また、IoT の関係は日々変化が起きるので、年に１回に限らず、連携していきたいと考えている。このような形で、年次計画に基づいて取組を進めていきたい。

「戦略マネジメント層」という言葉は、現在、サイバーセキュリティ戦略の中でも使われているので、「橋渡し人材」という言葉に対して、気にする必要はない。

我が国の対策をモデルにして海外に展開するという議論は、サイバーセキュリティ戦略本部でも全く同じ議論があった。サイバークリーンセンターを東南アジアに展開し、成功した事例もあるので、このレポートの中に、総務省と相談して、今後の取組として一言入れさせていただきたい。IoT の関係だけではないが、ボットなどについては、米国を含め諸外国でも気にしていて、いろいろな対策を進めている。そういう国と連携して、我が国のモデルを展開していくということはレポートの中で少し表現があってもいいと思う。

安田座長)

全体像としては、正しいと思うが、省庁対応になると、多少制限が出てくる可能性もあるので、そのあたりは全体でもう少し議論させていただきたいと思う。

藤本構成員)

網羅的で分かりやすい内容のレポートに仕上がっていると思う。10 ページから 12 ページに関して、IoT 機器による脅威は、何か検査を行い、安全な機器しか市場に出さないという動きだけだと、相当なコストがかかってくるので、利用者により安全な機器を選んでもらうといった形で、利用者も参加して、小さくしていくことが必須ではないかと思う。11 ペー

ジに記載されている脆弱な IoT 機器を特定した場合の所有者等に対する注意喚起について、所有者等においてどういうリアクションであったか、注意喚起によりどのような良さが生まれたか、そこで発見されたことが次の施策に対して、どのような示唆を与えて反映されていったかという一連の流れが見えてくると、効果を反映した参加型の新しい施策の展開の仕方が見えてくるのではないかと思う。そのような意味合いで、４）に記載されている課題は重要なことが書かれていて、今後のいろいろな具体的な施策に繋がっていくと思う。プログレスレポートの中でもそのような流れが見えると、すごく良くなると思う。

林構成員)

個別の話を１件、全体の話を２件申し上げたいと思う。個別の方は、電気通信事業法の改正と NICT 法の改正を成立させていただいて、非常に大きな今後のステップになると評価している。またここから出てきたプログレスレポートについても大変うれしく思う。ただ、それで終わりではなく、また時代がいろいろと変化するので、このステップがまた次のステップに繋がればうれしく思う。

全体の方は、プログレスレポートは良く出来ているが、何かを訴求する相手によっては、絵というのはすごく効果があると思う。プログレスレポートに関して、どういう方を対象に、どのように出されるかということによって、文字と絵のどちらを主にするか、選択肢について考えることが重要である。オバマ政権においても、規制改革を分かりやすさとパラレルにして実践していたり、行動経済学の学者がシンボリックな言葉を使って、分かりやすさを感性に訴えていたりすることからみても、ある部分では当たっているところがある。プログレスレポートで絵を取り入れて上手くやれば、成功しそうな気がする。

もう１つは、計量化が難しい中で、そういうことをすることによって、どれぐらい対策が進んだかが分かってくるのではないかと思う。そういうことが間接的にせよ訴えられるようになるのではないかという感じを持った。

安田座長)

今回のプログレスレポートには、数字的な部分は全部入っており、分かりやすくなっていると思う。これを絵にできるかどうかはなかなか難しい問題であるので、次回以降で検討するということにしたい。

木村サイバーセキュリティ課長)

正確性を求めると、どうしてもこのような文章の方がより的確になるので、本日の会合に向けては文章という形でまとめさせていただいた。ただこれを最終的に決定していただいた後、世の中にしっかり認識していただく段階においては、絵といったものを考えなければいけないと思っており、そういったものを準備できないか作業を開始したところである。

藤本構成員から指摘をいただいた点について、まさに今回、脆弱性調査を先行的に実施して取り組んでみたところである。現時点では、明確な形でフォローアップできていない。ただ今回法改正もありましたので、今後これを継続的に実施していく中では、当然、例えば注意喚起した結果として、どのような効果が出たか、全体としてどれぐらい減っていったかといったところはしっかり確認しながら、注意喚起の実効性をチェックしていく必要があると考えている。将来的にそのような方向で取り組んでいけるようにしたいと思う。

岡村構成員)

先ほど「橋渡し人材」について、名称の問題を取り上げたが、もう少し大きな視点での問題を提起させていただきたいと思う。最近、サイト証明が乱用されている事態と、ブラウザ最大手の仕様変更でブラウザ上でサイト証明を表示する方法が右側の上に短く表示される形態になったことが悪い意味でうまく被ってしまった状態になっている。国際標準化の推進においては、総務省において何が問題になっているかということを最新の情勢を把握して、こういう問題が起きて大問題になりかけているから、何とかしなさいと、デジュールスタンダードだけでなく、やはりもう１回デファクトスタンダードを獲得している大手の海外ベンダーに対しても、働きかけができるようなスタイルにしておかないといけないと思う。

先般あるセキュリティベンダーが刑法のウイルス罪の適用があるかどうかということでいろいろと問題になった。これだけ複雑怪奇にセキュリティの法制度が入り組んでくると、人材育成の中で、腑分けや解体新書のように、ある程度どの制度が今どうなっているかという概要ぐらいは知っている人を育てないと妙なところでトラブルに巻き込まれたりする時代になってきている。また何か起きたときにどう対応していいかというときに、技術的な対応と制度的な対応の両方が必要であるはずである。そのような観点で、今後の人材育成において、法律面についての知識を獲得する必要があることを記載していただきたい。

林構成員)

情報セキュリティ六法のようなものがあってもいいのではないかと思う。そういう編集ができないかといろいろと考えているところであり、基礎資料には着手している。人材育成の中の何分の一かは法制度の知識が必要になると思うので、今後の人材育成に役に立つような貢献がしたいと考えている。

安田座長)

IoT 家電やネットワーク家電のようなものが、このレポートの中のどこに入ってくるのかが気になる。IoT 機器に関するものではあるが、IoT 機器というと、一般の人にはサーバーや電話がイメージされてしまう。冷蔵庫やテレビなど、身近にある家電がすべてネットワークに繋がって、その部分で大変危険な状態になるということをどこかに記載した方がよい。別途相談させていただこうと思う。

大分意見が出たので、これらの意見をまとめていただき、その後相談するということしたいと思う。このレポートは、いつ頃公表する予定であるか。

木村サイバーセキュリティ課長)

政府のサイバーセキュリティ戦略策定の動きがあるので、そちらとの整合を図り、タイミングを見極めながら、公表に繋げたいと考えているところである。

安田座長)

もう１回ぐらい会合を開催する時間があるかどうかは分からない。議論が煮詰まってくれば早めに公表する可能性もあるので、本日の意見を調整させていただくこと、やりとりをさせていただくことになるが最終的には座長に一任していただくことでよろしいですか。

全構成員)

結構です。

谷脇政策統括官(情報セキュリティ担当))

突貫工事でプログレスレポートの取りまとめを行ってきたので、まだまだ抜けのあるところや表現がつたないところがあると思うので、お気づきの点があれば、事務局の方にメールなりでお寄せいただきたい。

以上