サイバーセキュリティタスクフォース（第９回）議事要旨

1. 日 時：平成 30 年 4 月 11 日（水）13:30～15:30

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】

安田座長、鵜飼構成員、岡村構成員、後藤臨時構成員、小山構成員、園田構成員、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

【オブザーバ】

大手英明(内閣サイバーセキュリティセンター)、小柳聡志(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、山碕国際政策課長、布施田技術政策課長、中溝通信規格課長、翁長宇宙通信政策課長、三田地上放送課長、萩原電気通信技術システム課長、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、豊重サイバーセキュリティ課課長補佐

4. 配布資料

資料９－１　IoT セキュリティ総合対策」の取組状況について

資料９－２　「公衆無線 LAN セキュリティ分科会」における検討について

資料９－３　「情報開示分科会」における検討について

5. 議事概要

(1) 開会

(2) 議事

◆ 事務局より、資料９－１　「『IoT セキュリティ総合対策』の取組状況について」を説明 (省略)
◆ 公衆無線 LAN セキュリティ分科会主査を務めている後藤臨時構成員より、資料９－２　「『公衆無線 LAN セキュリティ分科会』における検討について」を説明 (省略)
◆ 情報開示分科会主査を務めている岡村構成員より、資料９－３　「『情報開示分科会』における検討について」を説明 (省略)

◆ **構成員の意見・コメント**

中尾構成員)

資料９－３に関して、情報を開示する対象はセキュリティ対策であると理解したが、セキュリティ対策はふっと沸いて出るものではなく、各組織が、どういう脅威状況や脆弱性状況であるか、それに対するリスク分析を行った結果をもとに、対策が練られる。例えば、開示された結果が、セキュリティ対策だけであると、それがどういう根拠で記載されているかが一般的には分からないので、そのような紐付けがされないと、社内で共有する場合でもあまり意味がなくなるのではないか。そのあたりも含めて、開示対象に入っているかどうか確認したい。

岡村構成員)

事前開示という性格上、状況が移り変わる中で、動的なものとなる。アセスメントが先行するのが本来の姿であるとともに、詳しく手の内を明かすとかえってそれが狙われるリスクがあるという指摘もある。日米の具体的な開示事例の記載例を見ても、例えば、情報セキュリティ基本方針の策定状況や、管理体制では CIO と CISO を分離して設置している、あるいは CSIRT を設置している、教育・人材育成では従業員に対する研修の実施体制として年１回、定期的に研修を行っている、社外との情報共有では ISAC や CSIRT 協議会に加盟している、第三者認証では ISMS や P マークを取得しているといった非常にざっくりした内容が、第三者開示において開示されている。第二者開示では、例えば、サイバーセキュリティ保険に加入することを前提として、保険会社がチェックシートを用いて、聞き取りでセキュリティ対策の状況を確認している。確認内容はある程度各社においてまちまちの部分があるが、第二者開示という性格上、観点がもう少し具体化されたものになっている。

中尾構成員)

例えば、特定の企業の名前は出さないで、これぐらいの規模の組織では、こういう事例で、セキュリティのリスク分析から対策を導出して、それを上手く運用して、現在このような良い結果が出ているといった優良事例を公開していくという方向についても並行して検討していけば、より効果があると考えられる。

岡村構成員)

ベストプラクティスを様々と探しているが、企業側になかなか応じてもらえないという実情がある。継続的にそれが可能であれば、そのような事例の発見や収集に向けて取り組んでいく方向もある。

藤本構成員)

資料９－３に関して、当社も情報セキュリティ報告書を開示している。その関係で幾つかの会社と、どのように作ればよいかという意見交換を行った経験がある。その中で情報開示自体が危ないのではないかという議論があった。担当者が情報セキュリティ報告書の開示をトップに提案したところ、トップから危なくないのかという指摘が入って、その先の第三者開示に進めなくなった会社もあったように記憶している。ガイドラインを作成する際には、このように考えて、こういう形の情報を開示すれば、脆弱性が見えてリスクが増すということもなく、情報提供できるという、担当者がトップに説明する際の参考となる考え方をできれば提示してもらいたい。

岡村構成員)

開示をしすぎることによってのリスクという点では、セキュリティ管理策の手の内を知られることに繋がるのではないかということが考えられる。それと並んで、ここまで対策しているけれども、万が一インシデントが起きたときには、株主代表訴訟等のターゲットにされないか、法的な損害賠償リスクもあるのではないかと懸念しているということが考えられる。米国の開示事例を見ても、どちらかと言うと、抽象的な記述にとどまっており、米国企業においても様々な制度のもとで苦労している様子が見受けられる。様々な媒体がある中で、各企業はどの媒体で情報開示するのが自然であり、かつマーケットに受け入れられるのかということについて検討することに努力されている。また会社法上、強制力を持ったものもあるので、そういうものも含め、どのように整理していくかについて今後検討しなければいけないと痛感している。

吉岡構成員)

資料９－２に関して、このところ公衆無線 LAN のセキュリティとして重要であると思っているのは、無線 LAN ルーターそのもののセキュリティである。Mirai の大量感染の際に、無線 LAN ルーターも含めて、多くの攻撃を受けていた。無線 LAN ルーターは一般的に、グローバルのインターネットからアクセスできる口と、ローカルな無線 LAN 側にサービスを提供するための口の２つの通信の口を持っている。Mirai はグローバルの口から侵入して攻撃を受けるというタイプのもので、それでも相当の被害があった。無線 LAN ルーターのセキュリティを考えるときに、ローカルな LAN 側の口の方がセキュリティが弱いと考えるのが一般的である。LAN 側から攻撃を受けた場合には、ルーター自体が侵入されて感染する可能性があって、そうすると暗号化を行っているかどうかに関わらず、ルーター自体がやられてしまい、盗聴されたり、有害なサイトに誘導されたりする。分科会における検討において、ルーターそのもののセキュリティについて検討されていないようであれば、そのあたりも詳しく検討した方がよい。昨年度、総務省で IoT 機器の脆弱性調査が行われていたが、これはグローバルから見えるセキュリティの状況を調べているもので、LAN 側からみたときに、ルーターがどうなっているかは調べられていない。内部からの攻撃については、様々事例としては紹介されているが、統計的に有意と言えるほど調べられていないので、検討してもらいたい。

後藤臨時構成員)

分科会の議論としては、一番分かりやすいところ、目立つところとして、暗号化と認証を中心に議論しているが、当然ながら、ルーターそのものにパッチが当たっていないという脆弱性を抱えたままでは、何も対策が活きないため、物理レイヤーからアプリケーションレイヤーまで幅広く対策が必要であるという認識を持っている。その中で、特に提供者側への啓発活動において、無線 LAN ルーターそのもののセキュリティにも取り組んでいくことが大事であると考えている。

名和構成員)

資料９－２に関して、P2 の事例３において、HTTPS による通信であることを確認と記載されているが、官公庁のウェブページの方で HTTPS に対応しているものが少なすぎるので、そのような取組についての議論がされているか。

後藤臨時構成員)

官公庁のウェブページについては議論を行っていないが、総務省から何かあるか。

豊重サイバーセキュリティ課課長補佐)

まだまだ未整備のところがある。公衆無線 LAN 以外のところも含めて、総合的に対策を実施していく必要がある。

名和構成員)

東京オリンピック・パラリンピックや G20 の開催も控えているが、いつまでに実施するかは決まっているか。

澤田サイバーセキュリティ・情報化審議官)

総務省のセキュリティポリシーもあるが、もともとは政府機関等の情報セキュリティ対策のための統一基準群があり、HTTPS 対応は今は推奨基準になっていて、必要な場合は HTTPS 対応を実施することになっている。それが新しい案では遵守基準に格上げされ、基本的にすべて HTTPS 対応することになる。総務省においても、その基準の改定を待っていると遅れることになるので、実はポリシーを改訂を一歩先に実施した。引き続き総務省ホームページをはじめ、できるだけ早く HTTPS 対応を進めていきたい。

名和構成員)

今年の 1 月から 2 月にかけて、アルゼンチンのスターバックスで、Wi-Fi を利用していた人がマルウェアに感染し被害にあった事例があった。また今年の 3 月から今日にかけて、国内のカフェにおけるあまり安全でないフリーWi-Fi を利用していたモバイル PC が感染し、マイニングの被害にあった事例があった。このような事例が増加傾向にある。また、脅威の想定が「個人情報の入力情報の盗聴」となっている印象で、想定脅威の認識が古いような気がする。2019～2020 年に起こりうる脅威（例えば、ARP スプーフィングによる中間者攻撃等）を想定した方がよい。

岡村構成員)

名前が通っているような一流のホテルであっても、備え付けられた利用者用の公衆無線 LAN にアクセスすると、証明書の有効期限が切れているが、大丈夫であるかと聞かれるような状況が見受けられるので、証明書の更新についても、検討の視点として必要であると考えられる。

後藤臨時構成員)

本日の資料では省略されているが、分科会報告書では、公衆無線 LAN 提供者側もそのような認識を深めること、また利用者が提供者側の認証をしっかりできるようにすることが重要であるということが記載されている。

安田座長)

その部分について、総務省としての指導があるか。

豊重サイバーセキュリティ課課長補佐)

分科会において、その部分について今後取り組んでいく必要があることを提言していただいている。

林構成員)

資料９－１に関して、P6 のところで、国際会議の数だけ見ればずいぶんたくさんある。その一方で外務省の取組は、総務省や経済産業省の取組と比べると少し遅いという感じが否めない。大きな柱として、国際ルールの順守、コンフィデンスビルディング、キャパシティビルディングの３つの柱があるが、キャパシティビルディングに相当に精力を集中して取り組むという方向に動かす必要がある。その点を総務省からも強く言ってもらいたい。最近、アジアパシフィックテレコミュニティのコースで、セキュリティの講義を行ったが、それ以外にテレコム支援協議会も様々な国から若手を集めてトレーニングを行っている。そのときに受講者にある特定の国籍の人がいるかどうかは非常にクリティカルである。それによって講義内容を変えるなどの工夫をしている。そういう国のイニシアティブが相当強いので、センターがタイにできるのは喜ばしいが、できれば二国間でもっと実施していくことが必要になる。

資料９－３に関して、情報開示というと第三者開示のことだとばかり思っていたが、ここで第一者開示や第二者開示を入れられたのは、目が覚めるような思いがした。逆に見ると、第一者開示の情報は社内で情報を取得できて、対処できれば終わりであるが、そうではない部分がいっぱいある。また公的な情報がもらえることもあり、何となく開示と共有は、ファンクションが異なるのではないかという漠然とした気持ちが消え去らない。その中で、開示に関して３つを含めて考えた背景として、どのような観点の議論があったかを参考として教えてほしい。

岡村構成員)

様々な観点があると思うが、日本の経営幹部は、あまり ICT に関心がないことが少なくない。ましてや、セキュリティについては、金食い虫のように考えている人が残念ながら少なからずいる。そうした中で、セキュリティを推進するためには、人、モノ、金がかかるのも事実である。また、ICT を経営の刷新に役立てるというのがあるべき姿である。ところがそこに乖離が見られる。経営陣の方できちんとセキュリティを認識してもらい、セキュリティを徹底した企業として社会に受け入れられるように、努力を行うことを経営方針として組織全体に行き渡るように明確化してもらう必要があると考えている。ただ言うは易し、行うは難しという部分があるので、そこは個人の見解になるが、橋渡し的な人材を先ずは利活用することによって、橋渡しを行ったうえで、経営陣が会社の決め事や基本的な経営方針として、しっかりできるような姿になることが相応しいと考えられる。先ずは下位から始めるということで第一者開示を行い、それを複雑に入り組んでいるグループやサプライチェーンの中に広げて、マーケット等に受け入れられるような形で実施するのが、分かりやすい順番ではないかということで、第一者開示、第二者開示、第三者開示という形で整理した。

林構成員)

世間には、セキュリティ疲れのようなものがある気がする。物理的な安全を担当するセクションや、セキュリティを取り込んだ形でリスク管理を担当するセクションなど、様々なセクションがあって、CSR 報告書や内部統制報告書、環境報告書、サステナビリティ報告書など、それぞれの報告書を作成するためのセクションも別になっている。社長からすると、そんなにたくさんのセクションから報告を受けている暇はないと考えられる。もし橋渡し人材が機能していれば、それによって何とか報告をまとめる、あるいは様々なセクションの報告にある共通項や特徴のあるものだけを抜き出してまとめることができる。そのように情報圧縮を試みているような感じを持っている。そういう実態を調べたことがあれば教えてほしい。そうでなければ、私の方で別の機会に試みたい。

岡村構成員)

林構成員のところでそういう機会を今後作るのであれば、ぜひ役立てさせていただくことができたらありがたい。法律実務家として日頃から感じているところでは、どちらかと言うと、規模がある程度大きくない企業の場合には、良きに計らえ型の経営者が多いのが現状。ややこしい事を言われても、よく分からないから、担当者たるあなたに任せるので間違いがないようにやりなさいというように、そういうところで、残念ながら終わっている。

徳田構成員)

資料９－２に関して、先ほど吉岡構成員から、ルーター機器の LAN 側の方の口のセキュリティも問題であるという意見があったが、IoT をサポートするような、様々な IoT ホームゲートウェイやルーター等が新しい名称で出てきている。そうすると、通常のプロトコルに加えて、例えば MQTT のような新しいプロトコルがサポートされて、プロトコルスタックがリッチになっているが、その実装がきちんと出来ていない怪しいものがたくさんある。そういう意味で言うと、LAN 側の口と WAN 側の口をチェックするのも重要であるが、実装されているプロトコルスタックを検証できるツールが本当はオープンソースソフトウェアで出来ていて、ベンダーやサービス事業者が設置する前に自主的にツールを使ってチェックできるように、ツールセットが公開されているとよい。安かろう悪かろうで様々なプロトコルが売り出されてしまうが、実際に様々な攻撃を受けると、穴があってやられてしまうということが報告されており、検証ツール自体のカタログ等がまだ国内に整備されていないので、長期的には NICT の SecHack365 で育ってきた方々が日本独自の様々な検証ツールやモニタリングツールを開発できるようになればよいが、それには数年かかる。検証ツールの整備も大事である。

資料９－１の P6 に関して、セキュリティ人材の育成支援で ASEAN 各国向けの取組が記載されているが、東京オリンピック・パラリンピックを目標にすると、ASEAN だけでなく、欧州とも連携していく必要がある。特にトップノッチレベルの方々のトレーニングには、英国政府から英国の拠点と日本の研究者との連携を取りたいという話や、米国からも様々様々なトレーニングを使ってほしいという話が来ている。特に心配されるのは、英語でのコミュニケーション力である。一国で全部守りきれない状況が明らかになってきているので、連携しながら実施しようとすると、英語でのコミュニケーション力が高いセキュリティエンジニアを育てていく必要がある。そのあたりを付け加えてもらいたい。

木村サイバーセキュリティ課長)

サイバーセキュリティ関連の外務省の取組には、様々な取組がある。例えば、二国間であれば、外務省が中心となって、そこに関係省庁がぶら下がる形で、様々な国とサイバー協議を実際に行っている。人材育成についても、タイのキャパシティビルディングセンターの財源について、外務省の承諾を得て、JAIF（日 ASEAN 統合基金）を活用させてもらっている。今後４年間、様々な取組を推進する計画である。一般的な ODA についても、JICA の取組のような、ASEAN 諸国を中心とする途上国向けの人材育成の取組や、技術協力プロジェクトに対して、総務省も協力を行っている。また、日本での集団研修の中で、サイバーセキュリティの研修も実施してきている。そのあたりを含めて、関係省庁が連携を取り、お互いが補完し合いながら、キャパシティビルディングといった取組にさらに力を入れていくことができればよいと考えている。東京オリンピック・パラリンピックに向けて、日本と先進国がお互い協力しあう、また、ロンドンオリンピック・パラリンピックを経験した英国から教えを請う立場からの取組を、組織委員会と共にしっかり行っていく必要があると考えている。

徳田構成員)

検査ツールについては、NICT の中でも、サイバー空間上のモニタリングツールを始めとして、様々なツールを開発している。高度なツールキットはかなりライセンスフィーの高いものが多く、NICT では予算的な圧迫も強いので、日本のコ

ミュニティでそういうオープンソースソフトウェアを開発して、良いものを様々なところで使えるような形にしていくことができればよいと考えている。

小山構成員)

資料９－３に関して、自分が情報を取り扱ってきた経験からの意見になるが、情報共有と開示を並べると違和感がある。共有はギブ&テイクになるが、開示になると、開示請求のように堅い感じがある。第二者開示と第三者開示は理解できるが、第一者開示の情報共有になると理解が難しいと感じた。情報共有の観点から考えると、情報を発信したい人と情報を収集したい人がいて、情報を発信したい人のコミュニティをどのように作っていくかが重要になってくる。そう考えると、もう１つ情報発信を伴う関係者間の情報共有のようなものがあった方がしっくりきて、理解されやすいと考えられる。第三者開示がなかなか上手く出来ていない。大規模インシデントの際に、それに対する落ち着いた情報の出し方が非常に難しい。攻撃の手法を開示し、教えることで、対策を考えてもらうということは実施したいが、そうすると攻撃者側において、いたずらに被害を拡大させてしまうことが考えられる。社会に対する情報発信を、どのように安全にしていくかとうところについて、広い意味で今後議論が必要であると考えている。その理由として、もはや Microsoft やアンチウイルスソフトベンダーが、Windows 等の定期的なパッチを当ててくれる時代は終わったので、関係者がしっかりと情報共有をしていかないと、自分の身を守れないということがある。重要なテーマであるので、何とかしていきたい。

岡村構成員)

脆弱性情報の開示・共有に関して、今の経済産業省のフレームワークにおいては、攻撃者側に悪用されないように、先ずは IPA に届出を行い、IPA が JPCERT/CC に報告し、JPCERT/CC がベンダーと交渉し、それが完了するとパッチが準備される。準備が整い、配布する際にそれを公表するという形になっており、対応体制が前進した。一方でさまざまな課題もあり、例えば、オープンソースの場合にはプロジェクト自体が終わりを迎えていて、連絡がつかないから、それを使わないように公表すると JPCERT/CC 等が判断したことがある。そのような問題に対しては、昔から苦労しながら何が合理的であるかを考えて、少しずつ対応を進めているような状態である。大きなゴールで考えると、今、サイバーセキュリティ基本法の改正案が国会に上がっている。そこでは守秘義務を課したうえで重要インフラ分野ごとにもう少しセプター活動を推進できるようにし、情報共有を図っていくという新たなフレームワークが出来つつある。電気通信事業者の場合も、電気通信事業法改正の中の１つの柱として、そういうものが入ってくる。法制度自体の整備が進んできているものの、断片的であったり、これらを集めると上手くいくようなものが出来ていないので、NISC の方でしっかり取り組んでほしい。

小山構成員)

脆弱性情報について具体的な話をすると、パッチが出来て公表するという今までの手続論については全く否定するものではない。ただ今の IoT 時代になって、そもそもパッチが出ない、アップデートの方法もない中で、攻撃の情報だけが広まっている。リスクを治めていく手段について無策な状況にある。それについて情報開示という視点でどのようにアプローチすればよいかという部分が重要なテーマではないかと考えている。

岡村構成員)

大変重要な指摘である。

中尾構成員)

NICT のテストベットの中で、今、IoT 系の検証モジュールや API を組み込んでテストベットを作っている。それをどうオープンソース化するかという問題はあるかもしれないが、徐々には進んでいるという状況である。先ほどの情報公開の議論の中で、今回の検討は組織が対象となり、そこで考えられているセキュリティの対策をどのように公開していくかという流れになっている。そのようなスタートポイントも重要だが、それに加えて、情報開示のパターンとして、例えば、クラウドサービスのような組織が提供する様々なサービスという見え方で、どのように情報を公開していくかという方向も重要である。クラウドサービスの場合は、クラウドサービスを提供する側とクラウドを使うユーザ側がいて、ユーザは提供側のサービスプロバイダーがどのようなセキュリティのケイパビリティを持っているかというリクエストを投げる。サービスプロバイダーはそれをもらって、サービスとして、このようなことをやるという情報を公開する。また、IoT を考えたときに、IoT のサービスという視点で、ISO においても、どのようにセキュリティの対策を見せていくのかという議論を行っているが、IoT の機器を作る側と IoT サービスを提供する側、IoT サービスを使うユーザ側がいて、サプライチェーンのようにどのように責任分担の関係を整理して、どのように情報を共有・公開していくのかという方向についても今後情報開示分科会の中で議論してほしい。

国際連携については、様々な組織との連携が必要になるが、例えば、英国ではサイバーUK という大きなイベントを年に１回実施している。日本からは誰も参加していない。そういう中で英国がどのような戦略で、国外に向かってどのような情報発信を行っているかが参考になる。英国のような情報発信に積極的な国と、日本は二国間あるいは米国も入れた連携の形で、どういう内容を、どういう方向で、情報共有して連携をして、それをどう活用しているかという検証を含めて、日本もそういうステップを踏んでいかないといけない。単純にアグリーメントを結んで頑張るだけでは、なかなか進まないというのが実際のところである。国際連携の全体像を見極めて、どの部分について、どのように連携して効果を上げていくかという議論を行ってほしい。

安田座長)

公衆無線 LAN について、公衆ということで何らかのチェックを受けるのか。

後藤臨時構成員)

今回の方針では、例えば暗号化に対して、これでやりなさいという決めつけのチェックは、利用者を制限することに繋がるので適切ではなく、あくまで公衆無線 LAN はお客様や訪日外国人により広く、気持ちよく使ってもらうことを前提にした上で、それを安全にするにはどうすればよいのかという方針で検討している。こういうものであれば、このような組み合わせで、工夫するとよいという形で安全性を高めていき、それを優良事例という具体的な形で示していくという考え方で活動している。

安田座長)

セキュリティに限らず、サービス時間のようなものを保証するということはあるのか。要するに、故障を起こして、何時間も利用停止するようなことはあるのか。

後藤臨時構成員)

そのようなサービスを出す大規模な公衆無線 LAN キャリアもあり、そういうキャリアがそれを売りにしてもらえるとよい。利用者もそれを理解して、大事な仕事のときはそのようなサービスを使うというように誘導できるとよい。

安田座長)

そうなると契約の問題になる。

戸川構成員)

資料９－１に関して、IoT セキュリティ総合対策の項目の履行を網羅的に検証していただいていて、進んでいると理解しているが、項目にある程度濃淡があるのではないかと思う。まとめている中で、この項目が弱いという気づきがあれば教えてほしい。

木村サイバーセキュリティ課長)

例えば、予算施策について、既に IoT セキュリティ総合対策を取りまとめた時点で予算が確保されているものについては、概ね実施している。平成 30 年度予算で、こういう施策を実施したいと考えているものについては、平成 30 年度が始まったばかりであるので、予算を使って成果を上げるという意味合いでは実質的には取り組めていないに等しい。人材育成施策について既存の取組しか資料に記載していないが、更に拡張することができないかという点など、そういう意味での濃淡はある。今回は現時点での報告になっているが、次回のタイミングでは、個別の取組の出来栄えや、今回触れていないが追加的にできるようになったものも含めて説明できるように工夫してみたい。

戸川構成員)

IoT セキュリティ総合対策は IoT セキュリティという観点から対策を取りまとめたものであるので、IoT 機器に多少特化した話がより鮮明になっている方がよい。先ほど LAN 側、WAN 側の口のセキュリティについて、LAN 側から攻撃されるという話があったが、これが通常の PC だけの話であったとすると、今の PC はウイルス対策もされていて、なかなか LAN 側からの攻撃は少なくなるように感じる。IoT 機器であるから、様々な脆弱性があって、それに対する攻撃がある。Microsoft 等からセキュリティアップデートがあって、通常の PC の場合はそれが確実にできるが、IoT 機器の場合はどういうことが起きるか、ただ当てるだけでよいのか、何か方策があるのかというのは今後考えていかないといけない視点である。

鵜飼構成員)

資料９－２に関して、様々な無線 LAN があって、今後、東京オリンピック・パラリンピックを迎えるにあたって、基本的には訪日外国人が来て、公衆無線 LAN を快適に安全に使えるようになるとよいという発想に立っているが、そのようなユーザのほとんどが、IT について詳しいわけではない一般の方が対象となる。暗号化についても、現状でも暗号化されているもの、そうでないものの両方がある。公衆無線 LAN が安全に使えるかどうかは、暗号化の有無もあるが、通信プロトコルに HTTPS が適正に利用されているかどうか、ほぼその１点に尽きると考えられる。暗号化されていても、WEP で 01234 というような簡単なパスワードを設定しているところがたくさんある。今さらそういうものの対策を行うのは現実的にみても大変であるので、そのサービスの通信プロトコルに HTTPS が使われているかどうかをユーザにおいて分かるようにすることが一番の対策になる。その点に集約される話である。ウェブサイトを閲覧する場合に、HTTPS が使われていれば安全であると表示する、またユーザが公衆無線 LAN を使う場合にほとんどがアプリを使うので、そのような

アプリに HTTPS による通信が適切に実装されているかどうかを表示するといったような、暗号化の有無に関わらずユーザに分かりやすい情報発信を行うことが一番のポイントになると考えられる。

後藤臨時構成員)

ご指摘のとおりで、そのような議論を分科会でも行ってきた。

園田構成員)

資料９－３に関して、P2 で橋渡し人材のことがさらっと記載されているが、これは重いテーマではないかと思う。このような人材のスキルの具体化や教育コンテンツの開発・普及といった検討の取組が挙げられているが、橋渡し人材はキャリアパスのゴールではないのではないかと思う。その先にどのような人材になっていくのか、CTO 等を見据えていくのかといったところを踏まえて、コンテンツを検討されるとよいのではないかと思う。

脆弱性を探索するツールなどの話があったが、先日、人材育成のプログラムの成果発表を行った際に、既存のツールを改良するという形で、脆弱性探索ツールの成果を発表した参加者が実際にいた。今年度も新たなプログラムを開発していくが、そういった先人の成果を踏まえて、大学の研究室のような形で、継続性のある研究や開発を推進することを心がけていきたいと思う。

後藤臨時構成員)

資料９－３に関して、先ほどどういうサービスであるかを開示することが大事であるという話があったが、総務省の別の委員会でも議論している。そこでは、IoT の場合には IoT 機器側の話とクラウド側の話があって、片側の事業者から情報を共有するというよりも、両方の側の事業者から情報を出し合い、お互いの差を埋めるような会話に近いものが大事ではないかという議論をしている。このような視点が重要である。

また先ほど検証ツールやノウハウを試せるような場が重要であるという話があったが、大学の方で IoT の検証ツールをいろいろと試している経験からそのとおりであると思う。検証ツールの使い方が違うものや、IoT 機器ごとにプロトコルが違うものがあって、簡単に扱うことができない部分がある。そういう検証ツールを出きるだけ広く集めて、また機器を作っている人が一番詳しいので、そういう人にノウハウを出し合ってもらって、そういうものをみんなが使えるような場を作っていくことができると有効であると考えられる。タスクフォースでこれを推進できるとよい。

安田座長)

資料９－１に関して、ここで記載されていることは正しいと思うが、IoT のセキュリティということが国の最も重要事項であり、これが上手くいかないと施策が効かない、産業が育たないという根本的な認識を前書きで触れて追記してほしい。

また P4 にコネクテッド・インダストリー税制の創設が記載されていて、大変良いことを省庁が連携して行っているのは素晴らしいと思う。どんどん推進してもらいたいと思う。促進策がたくさん出ているが、それに取り組むと何かよいことがあるのかが意識として弱いという感じがある。情報開示を行っても、それを褒めてもらえたり、インセンティブがないと情報を出してもらえない。インセンティブの付け方について総合的に考える必要がある。

経団連に後押しをして、デフコンの優勝者に 5000 万円の賞金を出す等の取組をすると影響力がある。若い人がそういうものに目を向けるようになり、大きな動きになっていく。省庁の方から働きかけをしてほしい。そういうことが IoT セキュリティ総合対策に少し盛り込まれるとよい。

各分科会においては、今日の意見を踏まえて、また少し報告をまとめてほしいが、お願いしてよろしいか。

木村サイバーセキュリティ課長)

公衆無線 LAN 分科会は、3 月 22 日に分科会としての報告はまとまっている。情報開示分科会は、今後報告書案のパブコメを行って、もう 1 回それをブラッシュアップして、分科会で報告をまとめる流れになっている。いずれにしても、分科会での取組は、本タスクフォースでしっかりとフォローアップするという意味では同じである。また追加的な取組や内容面について、随時報告を行っていくことでよいのではないかと考えている。

安田座長)

各分科会の主査は、IoT セキュリティ総合対策の中に盛り込めるものをプッシュしてほしい。

谷脇政策統括官(情報セキュリティ担当))

そもそも IoT セキュリティ総合対策について、半年に一度点検することになっている。次回はプログレスレポートという形でまとめて、その中で残っている課題の洗い出しを行ってほしい。セキュアゲートウェイや IoT 機器の認証のように、個別に施策を実施する際には、施策間の役割分担について、どのように切り分けを行うかという問題が出てくる。また、脆弱性情報を共有する際にも、ハードウェア脆弱性とソフトウェア脆弱性、システム脆弱性の関係をどのように整理するかという問題が出てくる。そのあたりを整理して、プログレスレポートの案として提示し議論していただきたいと考えている。

以上