参考資料４－１

サイバーセキュリティタスクフォース（第３回）議事要旨

１．日 時：平成 29 年３月 27 日（月）15:00～17:00

２．場 所：総務省第１特別会議室（中央合同庁舎２号館８階）

３．出席者：

【構成員】

鵜飼構成員、岡村構成員、戸川構成員、徳田構成員、名和構成員、林構成員、藤本構成員、安田構成員、吉岡構成員

【オブザーバー】

村上企画官(内閣サイバーセキュリティセンター)、小柳課長補佐（経済産業省）

【総務省】

福岡総務審議官、今林政策統括官（情報通信担当)、谷脇情報通信国際戦略局長、吉岡大臣官房審議官、上原サイバーセキュリティ・情報化審議官、吉田情報通信国際戦略局参事官、大森参事官（サイバーセキュリティ戦略担当）、荻原電気通信技術システム課長、湯本消費者行政第二課長、藤田地上放送課長、住友衛星・地域放送課企画官、酒井情報セキュリティ対策室調査官、山田情報セキュリティ対策室課長補佐

４．配布資料

資料３－１ IoT セキュリティ対策の取組方針 ver1.0（案）（事務局）

資料３－２ IoT セキュリティ対策の中長期的課題（ビジネス及びサイバー脅威の変化の見通しから）（名和構成員）

資料３－３ IoT セキュリティ対策の法的側面（岡村構成員）

参考資料３－１ サイバーセキュリティタスクフォース（第２回）議事要旨

５．議事概要

（１）開会

（２）議事

- 事務局より、資料３－１ 「IoT セキュリティ対策の取組方針 ver1.0（案）」を説明
（省略）

◆ **構成員の意見・コメント**

➢ **岡村構成員**

IoT セキュリティ対策の取組方針 ver1.0（案）について、簡潔にまとめられている。書きぶりについて、P3 (3) セキュアゲートウェイの設置について、ICT に詳しくない人でも使えるようにする等の理由が書かれていると説得力が増すのではないか。

- **鵜飼構成員**

いくつかの技術的な対策について記載されているが、対策を進める上で技術的な課題が生じることが予測される。対策の実現性についての確証がないまま進めてもよいのかどうかについて確認したい。

- **事務局**

対策によって温度差はあると考えている。日本独自の技術を活用した対策に挑戦すると言う意味もある。セキュアゲートウェイについては、補正予算で実証実験を行う予定である。企業が提供している商用製品をさらに高度化することを考えている。

- **吉岡構成員**

(1)、(2) に記載されている内容について、緊急性があることが示されている点がよい。これらの課題を短期間で解決することは難しいので、継続的な取り組みを行うことにより価値が出る。継続的な取り組みのための体制や具体的な進め方についての記述があるとよいのではないか。

- **事務局**

体制については検討する。継続的な取り組みを行うことについても想定している。

- **戸川構成員**

P1 (1) ① 重要 IoT 機器の脆弱性調査について、IoT 機器の脆弱性には、ソフトウェアの脆弱性に起因するものとハードウェアの脆弱性に起因するものとの二つの要因がある。

従来の PC では、ソフトウェアの脆弱性が問題であったが、IoT 機器については、ハードウェアの脆弱性が問題となる。

インテルが CPU 内に FPGA を組み込んだシステムを開発した。このシステムは、外部からデータをダウンロードして、ハードウェアを書き換えることができる。

このような、ハードウェアに起因する脆弱性が今後増加する可能性があるので、IoT にどのような影響があるのかについて、継続的な調査研究が必要である。

また、ID／パスワードを適切に設定していたとしても、ハードウェアの脆弱性を悪用した不正行為が行われる可能性があることについても調査する必要がある。

- **安田座長**

方針案には、ハードウェアの脆弱性も記載されているのか？

- **事務局**

関係省庁と協力して検討する。

- **安田座長**

方針案の文書を見直してみた方がよいのではないか。

- **藤本構成員**

国際連携、国際標準化について、機器を開発・製造する側の目線から見ると、日本市場向けと海外市場向けとで標準化が１つのものになっていることが望ましい。それは国外の事業者にとっても同じだと思う。

P2 の２の文章中の、『国外の IoT 機器については』と書かれている部分を、『今後新たに製造される IoT 機器についても』とすれば、両方のニュアンスが入るのでよいのではないか。

- **事務局**

そのように修正する。

- **名和構成員**

記載されている対策について、ガイドラインのような形態で提示すれば、企業が自主的に実施することを前提としているようにみえるが、これまでのような自主的な取り組みが行われることを期待しない方がよい。

強制力をもたせるような形で、もう少し強気な姿勢で臨んだ方が良い。

- **林構成員**

内容的にはよいと考える。

全体的に、どのようなテンポで、どのようにして進めるのかについて、事務局としての心構えがあるとよい。

先日、NATO の Tallinn Manual 2.0 が公開された。国家や専門分野をまたぐ形で整理がされている。ルールの数も 2013 年版では、100 個程度であったが、2017 年版では 150 個に増えている。

この資料の作成プロセスが、IoT セキュリティの標準化等に対して、どの程度適用されるのかということを考えてみる必要があるのではないか。IoT のセキュリティについても、難しさは、国家レベルでのサイバーセキュリティと同程度ではないかと考えているからである。

その意味で、国際的な場を設定して、各国に働きかける必要があるのではないか。達成するレベルとして、どの程度を目指すのか？

- **事務局**

Tallinn Manual 2.0 は、内容的には、特に新規性があるものではないと認識しているが、関係者の範囲が拡大している点と、各分野の行政と直接関わるサイバーセキュリティの部分に踏み込んでいる点が前のバージョンと異なる。

体制については、政府側だけでなく、構成員を始めとしてさまざまな関係者と常時対話をしながら対策を練り、採っていく体制が必要になる。タスクフォースは、対策を取りまとめる実行の司令塔でもあるので、ぜひその責任を共有していただきたい。

- **名和構成員**

1 (2) ⑤ の ISP による C&C サーバとの通信制御の実施について、実施する上で ISP との協議が必要であるので、そのような記述にした方がよい。

他国の最新のサイバー攻撃動向からみると、C&C サーバとの通信制御は、対策としては少し古い認識のように感じる。公的機関のサーバや SNS のサーバが乗っ取られて、C&C サーバ利用されている場合があり、このような場合に ISP が通信を遮断してしまうと、業務継続性が確保できなくなる。

- **安田座長**

通信制御を実施する部分について、倫理教育や法制度改革が必要になるが、いずれ、これらについても触れることになると考えられる。

- **事務局**

方針としては、実施の検討と考えていただきたい。通信の遮断については、通信の秘密に関する整理を行った上で ACTIVE という取組みの中で実施している。これと同じように、IoT の場合にもあてはまる議論があるかもしれない。

IoT セキュリティ対策の緊急方針としてまとめているが、今後、人材育成や情報教育についても、議論が必要であると考えている。

- **徳田座長代理**

(2) ③について、より積極的にステークホルダー間での情報共有できる仕組みを整備し、基礎を作っていく必要がある。IPA は、情報共有をシステマティックに実施しているので、仕組みが参考になるのではないか。

書きぶりとして、さまざまな関係者が情報にアウトリーチできるようなニュアンスにするべきではないか。

2（5）について、ユーザにもある程度分担してもらう必要がある。IoT セキュリティガイドラインでは、ルールセットが記載されていた。一般利用者のための啓もうを含めた形で上手くニュアンスが伝わるように表現を工夫する必要がある。

➢ **岡村構成員**

通信の秘密との関連については、通信当事者の同意や緊急行為が要件となるが、包括的な事前同意は認められないというのが伝統的な判断となっている。

総務省の過去の研究会の成果として、『電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会報告書』があり、わかりやすい形でまとめられている。

ガイドライン等の文書は、わかりやすくまとめないと活用されないので、本タスクフォースの成果についても、かなり個別の論点まで立ち入った検討の結果をわかりやすい形で示す必要がある。

➢ **安田座長**

次回以降に議論したい。P4 の 3. まとめ に記載されている内容について、現在の体制で実施可能なのか？『必要な体制を構築し』という文章を追加するべきではないか？

- 名和構成員より、資料３－２ IoT セキュリティ対策の中長期的課題（ビジネス及びサイバー脅威の変化の見通しから）を説明（省略）

- 岡村構成員より、資料３－３ IoT セキュリティ対策の法的側面を説明（省略）

◆ **構成員の意見・コメント**

➢ **藤本構成員**

例えば、IoT 機能を有する冷蔵庫を購入したにも係わらず、普通の冷蔵庫として、やむを得ずネットワーク接続をしない状態で使用することになった場合、諦めるしかないのか？そのあたりについて、法律の整備が必要ではないか。

➢ **岡村構成員**

自動車における車検と対比して考えると、定期メンテナンスを義務的にするのか、それともユーザ側がコストを負担して IoT 機能を保有し、メンテナンスを専門事業者に任せるのか、それとも IoT 機能が不要なユーザは IoT 機能のスイッチを切って使うのか等々を考えたうえで、制度を検討する必要がある。

PC の場合でも、ハードウェア的に無線 LAN 機能を切れるような状態にした方が安全である。利便性と速さとリスクはトレードオフの関係であるということをユーザに理解してもらう必要がある。

- **安田座長**

車がネットワークに接続した場合、自動的に修正してくれるのか？

- **岡村構成員**

できるものとできないものがある。ソフトウェアの脆弱性はパッチで対応可能であるが、バッテリーが経年劣化しているような場合については、対応できない。

事業者とユーザのいずれが負担するのかについて、線引きが必要。

- **安田座長**

PC の不具合については、リコールしてもらいたいと考えている。

- **岡村構成員**

古い OS が搭載された PC を 10 年間使用している場合もあるが、そのような OS には、マルウェアが対応していないので、却って危険は少ないのではないかという話もある。

- **林構成員**

法的側面については、ケース分けが必要で、分類学の話になる。セキュリティは、企業と個人に共通する課題であるが、共通の認識を持つことが難しい。プラント等におけるセキュリティを扱う安全工学会の会誌において、サイバーセキュリティに関する特集を組んだが、サイバーセキュリティに対する共通認識が深まったとは言い難い。

安全工学会におけるセキュリティは、生命に関わるものであり、なにか起きた場合には、まず停止することが必要で、オペレーションは専門の技術者のみが行う。一方、情報セキュリティは、生命に直接関わるケースが少ない一方、専門家だけではなく、全員に関わるものである。

ある制度に対する過剰反応は、制度が一般の人にとってわかりやすいものとなっていない場合に起こり易い。かつて、Google が普及し始めた頃、日本においては、著作権侵害の懸念が過剰に意識された結果、他国に比べて普及が進まなかったということがある。

- **岡村構成員**

類似した基準やガイドラインが多過ぎて混乱している企業はないか？

➢ **名和構成員**

真面目に取り組んでいる企業は混乱しているが、そのような企業は少ない。

➢ **安田座長**

ハードウェアは出荷時に検査が行われているが、ソフトウェアについては行われていない。ハードウェアの検査が行われなくなったら大変な事になる。

➢ **名和構成員**

前回、米国の Food and Drug Administration)が、Fuzzing Test 機能を有するサイバーセキュリティラボを設立したという話をしたが、そこで使用されている Fuzzing Tool は、Codenomicon という企業の製品で、米国の元サイバーセキュリティ特別補佐官のハワード・A.シュミットが推薦したものである。

同製品は、Connected Car 関連の事業を行う大手企業においても導入が検討されている。

➢ **戸川構成員**

現在の製品やサービスに関する問題と、今後普及することが見込まれる IoT 製品特有の問題とを分けて考える必要がある。不具合が発生した場合、誰が責任を負うのか？

自動車がハッキングされた場合、ハッキングされたソフトウェアだけでなく、自動車全体に影響が生じる。IoT とセキュリティについての議論が必要。

➢ **安田座長**

自動車の運転には、免許が必要であるが、携帯電話・スマートフォンを使用するのに免許は不要である。自動車と携帯電話・スマートフォンが一体化した場合、どうなるのか？免許性にするべきではないかと考えるが、国際的にはどのような流れになっているか。

➢ **名和構成員**

液化プロパンガスを扱う業務・施設を対象とする法律は、10 個以上ある。

医療分野におけるセキュリティガイドラインについては、国内においては、以下がある。

- 厚生労働省 ： 医療情報システムの安全管理に関するガイドライン
- 総務省 ： ASP・SaaS 事業者が医療情報を取り扱う際の安全管理に関するガイドライン

・　　経済産業省 ： 医療情報を受託管理する情報処理事業者向けガイドライン

観点によって、責任分界点が決まることになる。

- **岡村構成員**

エンドユーザにサービスを提供するパッケージに製品やソフトウェアが組み込まれていれば、製品やソフトウェアを製造・開発した事業者が責任を負うことになる。

パッケージ内部での責任の分担は、パッケージの手足である製品やソフトウェアを製造・開発した事業者間での話になる。誰の誰に対する責任か？Connected Car サービスのパッケージがあれば、そこに全責任が転嫁される。

- **名和構成員**

石油プラント、浄水場、火力発電所等において、IoT を導入する動きがあるが、事業法に準拠することが優先されている。また、IoT 導入主体が情報システム部門からお金を稼ぐ利用部門へプレイヤーが変わってきている点についても注意する必要がある。

- **安田座長**

今後の議論の中で詰めたい。2020 年のオリンピック・パラリンピック開催時には、海外から大量のスマートフォンが入ってくる。インシデントが発生した場合、海外のユーザの責任を問うことはできるのか？

- **岡村構成員**

何でも持ち込めるわけではない。どこかで線引きをする必要がある。One Time SIM のようなものを使用して、端末を特定できるようにすることが考えられる。

- **徳田座長代理**

たとえば、モバイルアプリケーションの脆弱性に関するチェックを１つの組織がチェックしているから大丈夫ということにするのは難しいのではないか。さまざまな組織がチェックした結果を共有できる仕組みを作ることも必要である。加害者の立場になる可能性があることを啓もうしていく活動が必要である。

- **安田座長**

次回会合以降、いろいろな立場でもっと議論をしなければいけないと思う。構成員の方々は御意見をまとめておいてもらいたい。

- **事務局**

第４回会合は４月下旬の開催を予定している。議題については、情報共有や国際連携を考えている。

以上