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

１．日 時：平成 29 年３月８日（水）10:30～12:00

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、小山構成員、戸川構成員、名和構成員、徳田構成員、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】

山内参事官(内閣サイバーセキュリティセンター)、土屋企画官（経済産業省）

【総務省】

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、今川情報流通振興課長、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、玉田衛星・地域放送課長、山田情報セキュリティ対策室課長補佐

４．配布資料

資料２－１ IoT セキュリティ対策の論点及び方向性（案）について（事務局）
資料２－２ IoT セキュリティ対策について（鵜飼構成員）
資料２－３ サイバー攻撃対策としての IoT セキュリティについて（小山構成員）
資料２－４ IoT のセキュリティ向上に向けて（吉岡構成員）
参考資料２－１ サイバーセキュリティタスクフォース（第１回）議事要旨

５．議事概要

（１）開会

（２）議事

- 鵜飼構成員より、資料２－２ 「IoT セキュリティ対策についてについて」を説明（省略）
- 吉岡構成員より、資料２－４ 「IoT のセキュリティ向上に向けてについて」を説明（省略）
- 小山構成員より、資料２－３ 「サイバー攻撃対策としての IoT セキュリティについて」を説明（省略）
- 事務局より、資料２－１ 「IoT セキュリティ対策の論点及び方向性（案）について」を説明（省略）

◆ **構成員の意見・コメント**

- 事務局より、欠席の中尾構成員の資料２－１に対するコメントが紹介された。
  - ✓ 設計・製造段階について、セキュリティバイデザインが重要であり、デバイスの製造者に対する適切かつ具体的なガイドラインを提供するべきではないか。各セクターごとにガイドラインがあるとよい。
  - ✓ 販売段階については、セキュアな IoT 機器であることを認定する制度が必要である。認定の管理番号を発行してはどうか。また、セキュアなシステム構築について、メーカーやベンダへの啓発を行うための活動を行う必要がある。
  - ✓ 将来にわたって、IoT 機器のセキュリティを確保する上では、定期的な認定やソフトウェアのアップデートを行う必要がある。
    ネットワーク全体のセキュリティの観点では、情報共有・分析を目的として ICT ISAC が設立されているが、定常的にセキュリティマネジメントプロセスをまわすことが必要である。

- **名和構成員**

方向性について、国内・海外の切り分けが明確になっていない。論点の (2) ①～④および、視点のうちの事業者の視点について、国内・海外で切り分けて議論する必要がある。

民間企業については、意識啓発の効果が低下してきているので、何らかのインセンティブが必要である。

Web カメラの映像がインターネット上に公開された事件については、マスコミが調査報道したことにより、メーカーが対処したという状況である。

セキュリティバイデザインについては、人間の行動原理に合ったものとする必要がある。

- **林構成員**

個人情報保護法の法人版の法人情報保護法があるかというと、法人にはプライバシーがないので、ないということになる。整理が必要であるが、うまくいかない。

効率的なマネジメントシステムでまわすことができればよいが、社会的にどのような貢献ができるのかがよくみえていない。

CSMS の理念はわかるが、インプリのところで有効性が低下している。

民法については、有体物を対象としたものであるため、情報に適用することが難しい。政府が音頭をとらないと情報への適用は難しいのではないか。

コンピュータに記録されている情報については、電磁的記録という概念を適用することにより、法律において扱うことができるようにしたが、それでも通信中のデータには適用できない。

規律が情報であれば、規律の手段も情報でなければならない。

- **岡村構成員**

営業秘密は、やるべきことをやっていれば保護されるというものであるので、他人に迷惑をかけないように義務を課するという取り組みへのインセンティブが働きにくい。

車検制度と同様に、重要機器については検査制度が必要であるが、その場合のコストはユーザが負担することになる。

時間軸の観点では、数年に一回検査を業務づけることも必要と考えるが、何についてどこまでということを規定することは難しい。

製品の欠陥という概念を IoT に適用し、メーカーに責任を負わせることも必要。

国際動向への対応という点では、SBD 規格の国際展開をしてはどうか。

IoT 機能が組み込まれている製品から IoT をネット切断しても、製品として使うことができるようにすることも必要。

多重防御の考え方も必要である。メーカーは、SBD により安全な製品を製造する。ユーザは、家庭用のセットトップボックスによりセキュリティを確保する。ISP は、セキュリティゲートウェイを設置することにより、付加的なサービスとしてネットワークセキュリティを提供する。通信の秘密については、ユーザの同意を得ることにより回避できる。

脆弱性情報については、NICT、IPA、JPCERT が保有している情報の共有・交換が求められる。

NISC がとりまとめるということも考えられるが、情報の扱いにはゼロデイ攻撃の道具にならぬよう注意が必要である。

- **安田座長**

時間軸という話があったが、オリンピック・パラリンピックまでに何ができるのかということを考える必要がある。

- **小山構成員**

社会に混乱をもたらす可能性があるものに優先的に対処する必要がある。

得られた成果を製品の製造にどのように反映するか。

セキュリティを確保するための検査制度については、輸入品に対して適用することは難しいのではないか。

事務局資料の P4 ④ にあるように、ユーザの意識啓発も必要である。

米国では、製品の選択に際して、コンシューマレポートを参考にする人がいる。日本では、Kakaku.com を参考にする人が多いので、Kakaku.com の評価項目にセキュリティをどのようにして入れるか。どの Recommendation を見ても、セキュリティに関する内容が記載されているようになるとよい。

ID／パスワード の適切な設定やファームウェアのアップデートが確実に実行できれば、セキュリティインシデントの 99% は防ぐことができるのではないかと考えている。

ユーザの意識啓発、セキュリティバイデザイン、製品の検査制度を組み合わせた、包括的な対策が必要ではないか。

- **名和構成員**

IoT 製品のメーカーに対して、セキュリティバイデザインの支援を行う必要がある。たとえば、日本では、Fuzzing Tool に関する国家的な支援がされていない。米国では、FDA(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ている。

日本では、メーカーに丸投げされているので支援が必要である。

検査制度は、製品のセキュリティ確保という点では、順序が逆である。

- **安田座長**

今の意見を、論点及び方向性の資料のどこかに入れていただきたい。

脆弱性情報の共有について、NISC は統括することができるのか。2020 年までに何かアウトプットがでるのか？

- **山内オブザーバー**

脆弱性情報の共有の際に対策をどうするかという部分は、関係機関と相談して検討する。サイバーセキュリティ戦略本部の中で IoT 機器のセキュリティ対策について議論しており、夏の時点までに方向性を出す予定なので、この場での議論もそこに入れたい。

- **藤本構成員**

既に流通している機器の話と今後市場に出てくる機器の話という分類の仕方はわかりやすい。機器について、脆弱性を見つけて、それを連絡する手段を整備した後、製造者に伝えたとして、どのようにアクションを起こすのかということが重要である。

セキュリティバイデザインは、メーカーの努力に依存する面が大きい。組織として実施できるような体制が必要だが、その有り様によって、脆弱性の連絡手段も変わるのではないか。

ユーザが、セキュリティ上の配慮がされた製品を選択できるようにすることも大切だと思う。

安全性の確保は、製造者が考え実践しなければ実現は難しい。ガイドラインは助けにはなるが、製造者がセキュリティ意識を持つ必要がある。

製品の認証については、タイムスケジュールを考え、認証取得プロセスにおいて、長い待ち時間が発生しないような工夫があるとよい。

- **事務局**

製品の認証制度については、経済産業省や製造業者と協力して取り組みを進める。

- **戸川構成員**

小さい IoT として、計算リソースが少ない機器があるが、そのような機器は、パスワードによるセキュリティ対策が採りにくい。

重要インフラを構成する機器に対する認証が必要である一方、Pocket WiFi のようなものが街中に大量に存在するので、それらへの対応も必要である。

ISP におけるゲートウェイの設置は一つの方法である。

セキュリティバイデザインについては、意識啓発が必要。製品を構成する回路部品等がセキュアでなければ、製品としてもセキュアではない。従って、出自がクリーンな回路部品等を使用するという意識啓発が必要である。

米国において、サイバーセキュリティ上の理由から、特定の国の ICT 関連製品の使用を禁止するという政府の報告書が出されている。

- **安田座長**

事務局資料の 3. (3) ③ にセキュアゲートウェイに関する記述があるが、どのようにして推進するのか。

- **事務局**

ゲートウェイの機能等について、実証実験を行う予定である。

- **安田座長**

東京オリンピック・パラリンピック時等において海外で製造されたスマートフォンが、日本に持ち込まれるケースについてはどのように対処するのか。

- **事務局**

国内の基準で、セキュリティを守ることができればよいが、セキュアではない製品の使用を防ぐことができない場合も出てくる。現時点では国際的なルールに則して対応を考えていかないといけない。

- **安田座長**

戸川構成員の意見を、論点及び方向性の資料のどこかに入れていただきたい。

- **徳田構成員**

前回のタスクフォースで述べたが、Shamir 博士が、Philips 社のスマートランプに対して、P to P で攻撃を行うことが可能であることを示した。

IoT 製品の中には、P to P で攻撃を行うことが可能な製品があるということで、攻撃が見えない、攻撃に気付かない、攻撃されたかどうかがわからないという事態が懸念される。

建物の CO2 濃度を表示する装置のように、IoT 機器に脆弱性がどの程度残存しているのかを表示するソフトウェアがあるとよい。

機器のセキュリティ認証マークについては、ゆるい基準に基づいたマークでもよいので、早くユーザに知ってもらう事が重要である。

ユーザが自らマークを取得するというような形態があってもよい。

メーカーとエンドユーザの責任の切り分けについては、製品開発がイノベーションの源泉であることを考えて、バランスをとることが重要である。

海外との関係では、日本製の製品を使用したいという声を多く聞いているので、これまでに築いた日本製の製品のブランドをより高めるためのアプローチがよい。

たとえば、セキュリティバイデザインやプライバシーバイデザインに従って製品の開発・製造を行っていることをアピールする。

- **岡村構成員**

セキュアな製品を普及させる上でのインセンティブとして、たとえば、基準に適合する製品を対象として、税の優遇措置を適用することが考えられる。

セキュリティ人材の育成については、企業において、セキュアコーディングのトレーニングセンターを整備することが考えられる。

学校教育のカリキュラムの中でも情報セキュリティ教育を実施していくことが必要である。

- **名和構成員**

製品のセキュリティについて、海外で製造された Voice over IP 機器にバックドアが仕掛けられていたという報道がある。このようなケースは、問題を発見することが難しい。

防災・危機管理分野において IoT 製品が使用される場合があり、製品の脆弱性が大きな影響を及ぼす可能性がある。日本の同盟国の情報機関が、日本でよく使われているデバイスのハッキングツールを使用していたという情報が公開されている。

このような問題については、国が適切な対応を行う必要があると考えている。

- **安田座長**

P3 3 (1) ① 対策を取るべき IoT 機器の種類・範囲について、オリンピック・パラリンピックに向けて考えなければならない。

事務局において、本日出された意見を反映した上で、方向性を検討していただきたい。

以上