サイバーセキュリティタスクフォース（第１回）議事要旨

１．日 時：平成 29 年 1 月 30 日（月）10:30～12:30

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、園田構成員、戸川構成員、徳田構成員、中尾構成員、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）

【総務省】

あかま総務副大臣、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、小笠原情報通信政策課長、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）、湯本消費者行政第二課長、萩原電気通信技術システム課長、藤田地上放送課長、住友衛星・地域放送課技術企画官、山田情報セキュリティ対策室課長補佐

４．配布資料

資料１－１「サイバーセキュリティタスクフォース」開催要綱（案）（事務局）
資料１－２　サイバーセキュリティの現状及び総務省の対応について（事務局）
資料１－３　政府におけるサイバーセキュリティ政策の現状について（NISC）
資料１－４　最近のサイバーセキュリティにおける脅威動向について（中尾構成員）
資料１－５　今後の検討課題・スケジュールについて（事務局）

５．議事概要

（１）開会

（２）あかま副大臣挨拶

（省略）

（３）開催要綱について

事務局より、資料１－１「「サイバーセキュリティタスクフォース」開催要綱（案）」について説明(省略)

- **安田構成員**

目的のところに、情報通信分野とあるが、ICT 全体と考えていただきたい。

（４）座長の選出及び座長代理の指名

議事に先立って、座長の選出及び座長代理の指名が行われ、座長に安田構成員が、座長代理に徳田構成員が、それぞれ選任された。

- **安田座長**

  2020 年のオリンピック・パラリンピックは、ICT を駆使した祭典になる。データのスピードも向上し、サイバー攻撃が増加することが予想される。そのような状況に対応し、万全のサイバーセキュリティ対策を実施できるようにしなければならない。本タスクフォースにおいて、皆さまの活発な議論をお願いしたい。

（５）議事

- 事務局より、資料１－２ 「サイバーセキュリティの現状及び総務省の対応について」を説明(省略)

  - **安田座長**

    2020 年までまだ時間があるが、攻撃者は既に準備を開始している。既に日本へのサイバー攻撃のテストが行われているということを考慮していただきたい。

- NISC 山内参事官より、資料１－３ 「政府におけるサイバーセキュリティ政策の現状について」を説明(省略)

- 中尾構成員より、資料１－４ 「最近のサイバーセキュリティにおける脅威動向について」を説明(省略)

- 事務局より、資料１－５ 「今後の検討課題・スケジュールについて」を説明(省略)

- 構成員の意見・コメント

  - **鵜飼構成員**

    全体的にやるべきことが多いため、特定の課題にフォーカスすること難しい。人材や研究開発については、他でも議論されている。2020 年までに残されている時間は少ないので、優先度をつける必要がある。人材が重要な課題であると考えており、ドラスティックに取り組む必要がある。ICT 業界に若いセキュリティエンジニアが目を向けるようなインセンティブが必要である。

    研究開発については、防御技術が重要。世の中に普及させるために、産学官の協力が求められる。

  - **岡村構成員**

    スマートメータや車載システムに対するサイバー攻撃が懸念される。家庭にあるデジタル端末が攻撃されることが問題である。産業用制御システムは、これまでは保守という観点が中心であったが、今後はセキュリティを重要課題として意識改革

すべき。システムの設計段階からセキュリティを考慮する、セキュリティバイデザインが重要になる。

大手教育産業企業で発生した個人情報漏えい事故から得られる教訓として、新たな利便性を有する技術の登場とセキュリティ上の脅威とのトレードオフという課題があり、この傾向は今後も高まるおそれがある。

研究開発面では、今後の高齢化社会を想定すると、高齢者が自ら機器のセキュリティ設定を行うということは考えづらく、セットトップボックスのような形でセキュリティ対策を組み込まないとセキュリティが確保できないのではないかと考えられ、そのような技術の開発が必要になるのではないか。

最近、攻撃対象が、大企業から中小企業へと変化している。金融機関でいえば、メガバンクから地銀・信用金庫へと変化している。このような状況を考えると、ISPにおいてゲートウェイでセキュリティ対策を実施する必要があるのではないか。

IoT 機器については、製造物責任法が適用される場合があるが、法律の適用される期間が、現行の 10 年でよいのかという課題がある。

個人情報や機密情報の漏えいについては、全ての情報に対して一律に対策を実施するのではなく、情報がもつ価値に応じて、対策に軽重をつけるべきではないか。サイバーセキュリティ基本法の制定、改正の意義は多大だが、具体化や課題の検討が重要。

人材については、ICT に詳しい経営者が少ないので、ICT に詳しい経営者の育成が必要である。

- **園田構成員**

不足している人材が、どのような人材なのかを明確にする必要がある。現状では、製造業におけるセキュリティ人材が不足している。関係する方に、人材が不足していることに関心を持ってもらう必要がある。

イノベーションを起こす人にインセンティブを用意することも重要である。人材育成を支援する仕組みについて議論したいと考えている。

- **戸川構成員**

IoT のセキュリティについて、PC・スマートフォン等、計算を行うためのリソースがあるものと組み込み機器のように、リソースのないものがある。8 bit・16 bit で計算を行うような機器については、別の観点からセキュリティを考える必要がある。

物理レイヤでは、不正な部品が入り込まないようにする必要がある。製造段階でハードウェアに混入するトロイの木馬の脅威を想定しなければならない。米国で

は、2000 年代後半、ハードウェアに混入するトロイの木馬についての研究開発が行われている。

- **林構成員**

若い人に何をやってほしいか。インターネットには、変数と定数がある。定数は、事故が発生した場合に、誰が責任を負うのかというようなことを規定する法律を指している。AI を使用して法律を作るとどうなるのか。

製造物責任法について、ソフトウェアは対象外となっているが、IoT が普及した場合にそのようなことでよいのか。

製造物を対象とした法律をそのまま情報社会に適用することができるのかということについて、議論が必要ではないか。

- **藤本構成員**

セキュリティに対する組織的な取り組みについて

一般的に機器は、製造時に検査を行い、安全面のチェックをして出荷する。IoT 機器は、ネットワークに接続されるため、出荷後にリスクが明らかになるということに注意を払う必要がある。そのようなリスクに対処するためには、今までと異なる組織体制が必要であり、新たに IoT ビジネスを始める企業等は、組織を変えていく必要がある。組織変革のあり方についての支援も考えたほうがよいのではないか。

セキュリティを考える主体が、個々の企業から、複数の企業により構成されるグループへと変化する。そのような状況においては、グループ内での、あるいは情報通信事業者との間でのリスク情報の共有が必要である。さらに、ユーザにもリスクを理解してもらう必要があるので、リスクコミュニケーションが重要となる。

イノベーションを阻害しないような、リスクコミュニケーションを行うことが大切である。

- **吉岡構成員**

ルータやカメラなどのデジタル機器のマルウェア感染が多く注目されているが、重要なシステムのアクセス制御の不備の問題もある(例：病院の水処理システムに誰でもアクセス可能であった事例が報道されている)。このような状況は氷山の一角であり、全体像を把握するためには、フィールド調査を行う必要があるが、コストがかかる。

運用面では、VPN を使用して接続しなければならないところが、そのままインターネットに接続しているというようなケースがある。

産業構造と運用状況を把握することが必要である。

攻撃者は、IoT への攻撃方法を考えている段階である。IoT を対象とするマルウェアは進化のスピードが早いので、先行して調査を行う必要がある。

- **徳田構成員**

人材育成について、セキュリティだけではなく、ICT 人材も不足している。全ての人がセキュリティを意識するようになることが必要である。

オリンピック・パラリンピックに向けては、特別チームを設置する必要がある。

IoT セキュリティ全般については、海外から、日本の製造業のブランドを活かして欲しいという声をいただいている。

RSA 暗号の開発者の一人である、Shamir 博士が、インターネットを経由することなく、P to P で、スマートランプに使用される Zigbee プロトコルを改ざんできることを示したという例もある。

IoT セキュリティガイドラインを分野別に応用する必要がある。

重要インフラについては、野良 IoT(管理されていない IoT 機器)の対策が必要である。

情報保護の面では、セキュリティバイデザイン、プライバシーバイデザインの実践が重要である。

つながることによるメリットとリスクを明らかにすることも必要。

スピード感を持って議論していただきたい。

- **安田座長**

セキュリティ対策の実施においては、PDCA という概念があるが、このタスクフォースでは、CAPD という考え方でやっていただきたい。

以上