サイバーセキュリティタスクフォース（第 12 回）議事要旨

1. 日 時：平成 31 年 3 月 26 日（火）14:00～15:30

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】

徳田座長代理、岡村構成員、後藤構成員、小山構成員（代理：則武）、林構成員、藤本構成員

【オブザーバ】

吉川徹志(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】

竹内サイバーセキュリティ統括官、泉審議官(国際技術、サイバーセキュリティ担当)、木村参事官(総括担当)、赤阪参事官（政策担当）、三田地上放送課長、高地国際政策課長、坂中技術政策課長、田沼通信規格課長、影井電気通信技術システム課課長補佐、相川サイバーセキュリティ統括官室参事官補佐、豊重サイバーセキュリティ統括官室参事官補佐、後藤サイバーセキュリティ統括官室参事官補佐

4. 配布資料

資料 12－１　IoT セキュリティ総合対策の主な取組の進捗状況等について

資料 12－２　総合対策策定後の状況変化と今後の方向性について

資料 12－３　構成員からの御意見

参考資料１　 IoT セキュリティ総合対策

参考資料２　 IoT セキュリティ総合対策プログレスレポート 2018

参考資料３　2018 年「深刻な影響を発生させたサイバー攻撃」及び現実的な対策(事態対処態勢)

5. 議事概要

(1) 開会

(2) 議事

◆　事務局より、資料 12－１「IoT セキュリティ総合対策の主な取組の進捗状況等について」を説明 (省略)

◆　**関係者の意見・コメント**

中尾構成員)

大きな流れとしてはよい。確認だが、日本で技術基準の中にコモンクライテリアの注意書きがある。国際的な流れで、アメリカではセキュリティ的な基準をレベル化して製品を作っていくというのがある。イギリスではセキュリティガイドラ

インを１０数点定めており、日本よりも多い。制度化はＩｏＴ推進コンソーシアムで検討されているが、コンシューマデバイスのガイドラインが基準化していて、ＩｏＴ対策の中の技術基準を、国際的にどう認知させていくかというのは検討していく必要がある。

竹内統括官)

今回紹介したのは初期状態のセキュリティレベルを規定したもの。これを上回るものについては認証マーク等、メンテナンスまでベンダーがやっていくか、どう運用していくのかを、民間の動きを踏まえてどうフォローしてくか、これから書いていく。国際的な認知は、「ＮＯＴＩＣＥ」や「ＣＣＤＳ」での検討内容も含め、セミナー等の国際的枠組の中で取り組んでいきたい。

岡村構成員)

今、モバイルファーストが定着しているが、国際的にモバイル端末のあり方について議論されている。電波となると、すでに国際的な枠組があるので、これからは日本発の標準化のセキュリティの枠組をつくっていくのが望ましいのではないか。

中尾構成員)

トラストについて、トラストサービスのイメージは、誰に対するトラストか。「資料 12-1」の 10 ページの図を見ると、ネットワーク利用者が誰とやるか、どこが作成したか、送信先、送信元の保証などのイメージだが、よくイメージされるトラストは定義がより広いのではないか。例えば組織間やサプライチェーンのトラスト。今回は、こういったある程度はっきり技術的に対応できるものが多いが、まずはここからやっていくのか。もしくはこれからスコープを広げていくのか。

竹内統括官)

「資料 12-1」の 10 ページの５つの要素は、サービスとしてトラストで求められる機能を切り出していった時にどうなるかを示したもの。機能とサービスに必要な仕組みを検討し、それをベースにサービスプロバイダがサービスを提供するように、取り組んでいく。

岡村構成員)

地域における人材育成について、日本全国でセキュリティに限らず人材不足の状況。社会保険料高騰の関係で新規に人を入れるのも中小事業者には厳しい。取引先の末端に属する中小のセキュリティ基準を引き上げるという観点からすれば、サポート隊のような、比較的リーズナブルな条件で必要に応じて事業者を助けるものを進めてほしい。一般的な人材育成では、法・制度面、マネジメント面に明るい人材が不足している。今後は技術者を育てるとともに、統括できる人間を育てる場所が必要ではないか。大企業では海外からそういった人材を誘致している例もあるが、国内でそういった人材を供給できる方が望ましい。社会人の大学教育等含め、考えていただければ。

林構成員)

全体としてみると、昔は企業のトップの理解が得づらく、そちらの解決に注力していたが、それは必要なくなってきたという点で進展していると思う。ＩｏＴ分野ではゼロから専門的なセキュリティ人材を育てるより、既に当該分野で働いている人材にさらに付け加える形で、セキュリティの技能を習得させていくという育て方が望ましいのではないか。

◆　事務局より、資料 12－２　「総合対策策定後の状況変化と今後の方向性について」を説明 (省略)
◆　事務局より、資料 12－３　「構成員からの御意見」を説明 (省略)

◆　**関係者の意見・コメント**

小山構成員（代理：則武））

１点目、踏み台になるＩｏＴ機器については対策がされてきたところだが、2017 年に重要ＩｏＴ機器の課題が挙げられているので取り組むべき。２点目、「ＮＯＴＩＣＥ」は国内中心だが、攻撃はグローバルで行われる。国により法・制度が異なるため、「ＮＯＴＩＣＥ」をそのまま拡大することは困難だが、できるところから日本の先進モデルとして展開することを考えて欲しい。３点目、ＩＳＰと議論していると、情報をどう使っていいのかわからない、事例集があるとやりやすいという意見を聞くので、情報共有や対策の事例集があればよい。

岡村構成員）

通信の秘密については憲法の改正が必要なので難しいということを前提にしてほしい。通信の秘密とセキュリティの関係について報告書が総務省から出ているので、どんどんこれを進めていただいて、ここまではして大丈夫というラインを示してほしい。

中尾構成員）

今まで色々な方の意見があったが、これをどうまとめていくのか。それぞれ重なっている部分も反対の部分もあり、全体的な流れのなかで何をやるべきなのか整理していかなければならない。総合政策の中に、具体的にこれを実現するためのプランが盛り込まれ、来年、再来年とフォローアップをしていく構想ではないかと考えているが、是非まとめていただき、議論させていただきたい。

徳田座長代理）

安田先生の方から、人材育成は「かなり進んできたので国が率先して進める必要はない」というご意見があったが、セキュリティ人材のピラミッドの一番上にあるマスターレベルの人材を、国際連携を意識した Ph.D. in cybersecurity というプログラムがあるが、日本では Advanced Degree の人材が国を越えて海外の研究機関と連携するような取組は遅れている。組織間の連携を意識していくと、より高度な人材が育成できるのではないか。また、ＮＩＣＴが行っているＣＹＤＥＲ等を進めつつ、よりよい人材育成の仕組み作りを行っていただければよい。

以上