資料４

技術戦略専門委員会
第２６回会合　議事要旨

１　日時
平成 26 年 12 月 19 日(金) 16:00～17:50

２　場所
内閣府庁舎別館９階大会議室

３　出席者（敬称略）

（委員長）	後藤 滋樹	早稲田大学理工学術院教授
（委員）	上野 裕子	三菱 UFJ リサーチ&コンサルティング株式会社 政策研究事業本部 経済・社会政策部 主任研究員
	小松 文子	独立行政法人 情報処理推進機構 情報セキュリティ分析ラボラトリー長
	小山 覚	NTT コミュニケーションズ株式会社 経営企画部 マネージドセキュリティサービス推進室 担当部長
	新 誠一	電気通信大学 教授
	神成 淳司	慶應義塾大学 准教授
	名和 利男	株式会社サイバーディフェンス研究所 理事／上級分析官
	松原 実穂子	株式会社日立システムズ シニアサイバーセキュリティアナリスト
（事務局）	髙見澤 將林	内閣官房副長官補
	藤山 雄治	内閣審議官
	谷脇 康彦	内閣審議官
	佐々木 良一	情報セキュリティ補佐官
	三角 育生	内閣参事官

（オブザーバー）　内閣府
総務省
文部科学省
経済産業省
防衛省

4 議事概要

（1）開会

（2）技術戦略専門委員会について

事務局から、資料 1、資料 2、資料 3 に沿って説明。

その後、後藤委員を委員長に互選。

（3）技術戦略専門委員会における検討方針（案）について

事務局から、資料 4 に沿って説明。

（4）情報セキュリティ研究開発施策の状況について

総務省から資料 6-1 に沿って、経済産業省から資料 6-2 に沿って説明。

その後、自由討議が行われ、委員等からは以下のような意見が述べられた。

＜自由討議＞

○IoT では、農業、医療、ビルといった、従来の IT の範囲外の分野も対象となってくる。これらの分野を管轄している省庁も、この委員会にオブザーバーとして参加してもらうべきではないか。

○農業分野では、農業機械の自動運転や UAV（無人航空機）の活用等の研究開発が既に進んでいる。管轄省庁とも連携し、ガイドラインを制定するなど、セキュリティ対策を進めることが急務である。

○上流工程からのセキュリティ確保について、配布資料ではニーズ側からのアプローチをまず進めることが提案されているが、並行してシーズ側からも連携していく必要があるのではないか。

○国際的に利用されるセキュリティ技術となるためには、その技術単独でなく、魅力ある新しいシステムにセキュリティを備えた形で提示していく必要があるのではないか。

○IoT が普及すると、従来の IT に慣れていない一般の方も利用者となる。そのような利用者でもあまり意識せずに使えるよう、海外で取り組まれているような、人間の行動原理に基づくセキュリティ研究が必要ではないか。

○IoT 利用の進展は、攻撃側が容易に対象機器を入手・分析でき、脅威が拡大することにもつながることも認識しておくべき。例えば、スマートメーターの脆弱性を探すことにより、数千万世帯に攻撃できる可能性がある。

○配布資料にある、研究・開発・企画段階からのセキュリティ組込確認というのは、旧来の手法に縛られている印象を受ける。全ての攻撃を未然に防ぐことはもはやできないので、今の日本に欠けている、例えばハードウェアに組み込まれた不正な機能を見つけ出すような技術が、少なくとも重要なところでは必要。

○多くの中小企業がセキュリティ対策をまだ余計な負担と認識していたり、大企業においてもセキュリティ人材の社外流出を警戒していたりする状況の下、業界内・企業間でセキュリティ情報をいきなり共有することは厳しい。現場の状況をよく把握した上で、必ず成功するプロセスと目標を設定すべき。

○IoT のデバイスは、10 年以上使われることが想定される。その長期間セキュリティを確保できるアーキテクチャが必要ではないか。また、多くのデバイスが管理者不在となる恐れがあるので、それらはプライベートネットワーク下に置いて通信を一か所のゲートウェイに集めるなど、面から点へ、常に管理下に収めるセキュリティ対策手法を検討すべき。国でガイドラインを作る等して進めて欲しい。また、世界に先駆けた手法として、デバイスの仮想化技術をセキュリティに応用することもできるのではないか。

○IoT の普及により攻撃の対象範囲が拡大していく中、全ての攻撃を未然に防ぐことは不可能。各組織において、受容できるリスクの水準を見極めておく必要がある。

○例えば、企業の役員が個人所有のパソコンで扱った重要情報が漏えいした場合、企業がその端末を調べることは、個人情報及びプライバシー保護の観点などから難しい。また、その際に個人が利用できるサービスも日本にはほとんど存在しない。今後の IoT の拡大を鑑み、個人を対象とするインシデント対応等のサービスも確立していく必要がある。

○現在、政府で行われているサイバーセキュリティ演習は、官公庁や重要インフラ企業が主な対象者であるが、最近のエンターテインメント系企業へのサイバー攻撃の事例から考えると、演習に招く対象範囲を広げていく必要がある。

○セキュリティ技術の研究開発に国費を投入する際には、企画段階から産業界側と一緒になって社会実装や産業化を見据えた上で、国際標準化等のオープン・クローズ戦略も含めた研究開発戦略を立て、進めることが重要。

○IoT は、運用、システム、デバイスの 3 層全体でのセキュリティを視野に入れて技術開発しなくてはならない。国としてこの枠組みを決め、そこに各企業の技術を当てはめていくような形で進めることができるとよい。

○リスク受容については、どのようなリスクに対して誰が受容するのかを対象ごとに決める必要がある。これと、先ほどあった、通信を一か所に集めるなどの点のセキュリティ対策を結びつけることが必要。

○リスク受容に必要なリスクの定量化は現状では難しい。リスクが見えるネットワーク構成を考えるなど、観点を変える必要がある。ぜひ大学等の研究者の方で検討してもらいたい。一方、企業の方には、実用的な情報を大学等の研究者の方に提供してもらえるとよい。

○現在のコンピュータやインターネットには、性質上、攻撃を受けても気づきにくい、攻撃者が捕まりづらいといった課題がある。システムの本質的な作りを見直す必要があるかもしれない。

○セキュリティの基準は、現場を見て、ユーザビリティやコストも勘案して設定していかないと、守られないものとなる。絶対に守るべき部分と、接続の確保や状況報告がされればよいといった最低限のことでよい部分に分け、この委員会で議論ができるとよい。

○セキュリティ対策を進める上での最大の課題は、人材不足。例えば、現在制御システムと情報システムの両方を理解している人材がほとんどいない。セキュリティは各分野に渡る知識が必要であり習得が大変である。育成と待遇改善のための施策を国として進めてほしい。また、育成した人材が攻撃側に回らないよう、倫理教育と待遇改善の面も考慮してほしい。

（5）閉会

以　上