資料３

第１１回 技術戦略専門委員会での
グランドチャレンジ検討WGに関する意見に基づく事務局メモ

【背景（社会環境）の変化について】

・団塊の世代にはパソコン等に慣れている人が多いので、今後ますます高齢者が IT 機器を使いこなすようになり、利用者の年齢層が広がる。

・あるリスクへの対策が、別のリスクの原因になる「リスク対リスク」の時代になりつつある。

・国民もネットワークの先はブラックボックスだと考えるのではなく、リスクを理解して、整理して取り組む必要がある。

・情報家電に加えて、携帯電話、モバイル端末、RFID なども普及しており、それらのセキュリティ対策にも取り組むべき。

【グランドチャレンジの研究開発テーマについて】

・基盤としての IT の強化の例として、電子申請があると考える。しかし、今の認証の仕組みはガチガチなので、サービスの内容を分析し、要求されるセキュリティのレベルの仕分けをしていく必要がある。

・（かつて韓国であったように）インターネットが止まってしまうなどの「相当悪い状況」が起こるという想定を行なって、テーマを立てる必要もあるだろう。

・今は顧客情報が入ったＰＣを紛失すると記者会見などをして報告しないといけないが、あるレベル以上のセキュリティ対策をしたＰＣならば（実際には情報が漏洩しないはずなので）、報告しなくとも良いはず。こういうレベルの条件を整理するのがグランドチャレンジになるのではないか。

・例えば、リスクのプライオリティ付けをするツールを活用することで、セキュリティ対策を効率的かつ合理的に実施する取組みもグランドチャレンジになり得るのでは。

・高齢化などの社会の世代構成変化に対応する技術開発も研究としてやっておく必要ある。操作や認知のミスなどに対応できるセキュリティに今から取り組んでいかないといけない。

・（自動車などの）組込み系といった日本の得意分野のセキュリティを高めることで、日本の強みとしていく。そのために社会としてどのような活動をすべきか。そして、どのような体制で取り組むべきかを考えることは重要。（＝ 攻めのセキュリティ）

・情報家電などファームウェアをアップデートできる機器の対策はパソコンと同様な方法でよいか。あるいはパソコンとは利用者層が異なる等の理由から別に扱うべきか。（参考）利用者のアップデートの了解の要否及びその取得方法、アップデートが成功しなかった場合のリスクへの対応など、パソコンと異なる留意点が考えられる。

・ アップデートできない組込みソフトのセキュリティをどのように確保すべきか。（古

いバージョンの製品を徐々に使えなくしていく自動的な仕組みなど）

・新技術の利活用と、セキュリティの脅威への対策の間の「タイムラグ」を短くするには、システムの動作を常にチェックする仕掛けがいるだろう。新しい情報技術の利活用と信頼性の確保とを並行して進めるために、一定レベルの情報セキュリティを担保できる設計開発手法が有効ではないか。

・新技術は、それを運用する体制まで考えた上でセキュリティ対策も一緒に開発すべき。

・新技術を、何もない０から開発し、製品化まで持っていくのに、どれだけのコストがかかるか？　どういう体制で進めればセキュリティ対策を組み込めるか、ということを実際にやってみるのも、グランドチャレンジになり得るのでは。

・フェイルセーフのための技術開発や、自覚や十分な知識のない利用者（永遠のビギナー）を技術面で補うことを考える必要があるのではないか。

・情報セキュリティ対策のレベルの合理性や効率を判断するために、技術仕様の表記の共通化や、リスクの形式的な記述方式、リスクの定性的・定量的な評価方式が有用と考えられるが、それらの合意（広い意味の標準化）などは可能か。

【プロジェクト管理関係】

・不十分な研究分野の発見や早い段階での成果の利用ができるよう、国が支援するプロジェクトの内容および実施状況の公開をもっと促進すべきではないか。

以上