資料 2-1

分野・領域に係るこれまでの議論（第 1 回、第 2 回会合を終えて）

1. 領域のまとまりの整理

・海外のカンファレンスにしか存在しない領域もある。

→留意しつつ専門調査会資料（検討の素材）掲載の整理例②で議論を進めてはどうか。

2. 日本の強み

（現在の強み）

・強みをどのように測るか。カンファレンスでの発表件数もある。
・日本が世界と戦えているか。戦えていないなら、その理由の分析も必要。

（ポテンシャル）

・日本で研究を実施する上で法制度的に有利・不利なこともある。
・品質や実運用に配慮する細やかさは日本の強みになるのでは。
・日本の暗号の強みを活かせるとよいのだが。
・攻撃のローカライゼーションが進展し、日本でしか観測できない攻撃がある。攻撃解析の粒度も自国の方が高くなる。

（産業界との関係）

・スマホ、CPU、OS、ファジングツールなど、日本は産業として弱い面があり、どうしても研究領域でも弱くなってしまう。

→資料 2-2

3. 日本の強みと重点的な強化の関係

・弱いところでも、どうするか考えるべき分野があるのでは。
・将来的にどの分野で強くなりたいかも考える必要。
・自国で自給自足すべき分野もある。
・日本の独自性を創出しようとした結果、本当にインパクトある研究テーマから逸れてしまっている事例があるので注意すべき。日本特有の事情・環境に特化した技術では市場が日本にしかなく難しい。

→上記の点に留意しつつ重点的な強化を検討

4. 重点的な強化

・大規模投資の前の段階にある斬新な研究分野をつくる・見つけることも重要。
・短期で成果を出す実践的研究と長期で出す基礎研究の両方を意識すべき。（前者はセキュリティだけを切り出すのは難しいことがあるが、後者ではセキュリティ全体を見る長期的な基礎研究もある。）

→専門調査会資料（議論の素材）（第 1 回資料 1-6）のｐ2 を参照しつつ、当面、「真ん中」の議論を進めてはどうか。

（新興領域への対応）

・重要なイベントやインシデントが発生したとき、世界の研究者の動きはとても早い。いつの間にか一つのジャンルになっている。

（産業界との関係）

・企業のニーズなどを考慮して検討すべき。
・HCI 分野など、日本が強い分野と連係して設計段階から一緒にセキュリティを検討する方法がありうる。

→全体として更に議論が必要。一つの議論促進として資料 2-3　　**以上**