【参考情報③】内閣府 戦略的イノベーション創造プログラム（SIP）

SIP新課題：重要インフラ等におけるサイバーセキュリティの確保

H27（2015）年度～H31（2019）年度（予定）、H27年度予算：5億円

経緯

H27年6月18日（第10回CSTI）　新課題候補「重要インフラ等におけるサイバーセキュリティの確保」の承認
8月6日　情報セキュリティ大学院大学・後藤厚宏教授の内閣府政策参与への任命
9月15日～10月5日　研究開発計画案パブリックコメントの実施
11月10日（第12回CSTI：持ち回り）実施方針の決定
H28年1月22日　委託先決定

達成目標

- 悪意のある機能を“持ち込ませない”、悪意のある動作を“いち早く発見する” システムの実現
- 国産セキュリティ技術を確立。重要インフラ産業の競争力強化、安全な社会基盤実現に貢献

⇒ 2020年五輪大会の安心安全な開催

PD

情報セキュリティ大学院大学教授
後藤　厚宏

研究開発計画案概要

SIP 戦略的イノベーション創造プログラム
Cross-ministerial Strategic Innovation Promotion Program

【参考情報④】第5期科学技術基本計画における「サイバーセキュリティの確保」(抜粋)

第２章　未来の産業創造と社会変革に向けた新たな価値創出の取組
（２）世界に先駆けた「超スマート社会」の実現（Society 5.0）
超スマート社会の姿
：中略
一方、**超スマート社会では、サイバー空間と現実世界とが高度に融合した社会となり**、サイバー攻撃を通じて、現実世界にもたらされる被害が深刻化し、国民生活や経済・社会活動に重大な被害を生じさせる可能性がある。このため、より高いレベルの**セキュリティ品質を実現していくことが求められ、こうした取組が企業価値や国際競争力の源泉となる。**

実現に必要となる取組
：中略
その際、**システム全体の企画・設計段階からセキュリティの確保を盛り込むセキュリティ・バイ・デザインの考え方に基づき推進することが必要**である。
：中略
総合科学技術・イノベーション会議は、健康・医療戦略推進本部との連携・協力を進めるとともに、**ＩＣＴ関連の司令塔である高度情報通信ネットワーク社会推進戦略本部及びサイバーセキュリティ戦略本部との連携を進める**。

（３）「超スマート社会」の競争力向上と基盤技術の強化
② 基盤技術の戦略的強化

ⅰ）超スマート社会サービスプラットフォームの構築に必要となる基盤技術
：中略
・**設計から廃棄までのライフサイクルが長いといったＩｏＴの特徴も踏まえた、**安全な情報通信を支える**「サイバーセキュリティ技術」**

ⅲ）基盤技術の強化の在り方
：中略
加えて、世界中から優れた人材、知識、資金を取り入れて研究開発及び人材育成を進めるとともに、ＡＩ技術や**セキュリティ技術の領域などでは、人文社会科学及び自然科学の研究者が積極的に連携・融合した研究開発を行い、技術の進展がもたらす社会への影響や人間及び社会の在り方に対する洞察を深めることも重要**である。

第３章 経済・社会的課題への対応
（２）国及び国民の安全・安心の確保と豊かで質の高い生活の実現
③ サイバーセキュリティの確保
：中略
このため、サイバーセキュリティの確保の重要性に関する社会的認知の向上や、サイバーセキュリティに対する国民のリテラシーの向上、質的にも量的にも不足している人材の育成のための取組を推進しつつ、**日々進化するサイバー攻撃の脅威に対処して、サイバー攻撃から国民生活や経済・社会活動を守るための技術開発に取り組む**。
具体的には、サイバー攻撃の検知・防御技術、認証技術、制御システムセキュリティ技術、暗号技術、ＩｏＴ分野でのセキュリティ技術、ハードウェアの真正性を確認する技術、重要インフラのシステム構築時及び運用時にシステムとして健全な状態であることを監視・確認できる技術等の開発及び社会実装を推進する。

内閣サイバーセキュリティセンター

National center of Incident readiness and Strategy for Cybersecurity