IoT社会に対応した サイバー・フィジカル・セキュリティ

Society 5.0を支える強靭なセキュリティ基盤の確立を目指す

産業システムや生活環境等のフィジカル空間に埋め込まれたIoT機器が、多様なネットワークを介してクラウド等のサイバー空間と連結され、高度な知識処理や分析・解析処理との連携により、様々な付加価値を創出しフィジカル空間である経済社会に多大な恩恵をもたらす。一方、IoTの普及・拡大に伴いサイバー攻撃の脅威があらゆる産業活動に潜みつつあり、製品やサービスを製造・流通する過程で不正なプログラムの組込みや改造が行われるサプライチェーンリスクの問題も顕在化している。このため、IoTシステム／サービス及び中小企業を含む大規模サプライチェーン全体を守る『サイバー・フィジカル・セキュリティ対策基盤』の開発を行い、実稼働するサプライチェーンに組み込み実用化することで、サイバー脅威に対するIoT社会の強靭化を図る。

プログラムディレクター

後藤 厚宏

情報セキュリティ大学院大学
学長

Profile

1984年東京大学大学院工学系研究科情報工学専攻博士課程修了。同年日本電信電話公社に入社、約27年間情報技術に関する研究開発に従事。2007年NTT情報流通プラットフォーム研究所長、10年NTTサイバースペース研究所長を歴任。11年より情報セキュリティ大学院大学情報セキュリティ研究科教授、17年より現職。内閣官房、総務省、文部科学省、経済産業省、防衛省などの審議会、委員会等における委員長等および委員を歴任。

研究開発テーマ

IoT機器やサプライチェーンの各構成要素についてセキュリティの確保（信頼の創出）とその確認（信頼の証明）を繰り返し行い、信頼のチェーンを構築・維持することで、IoTシステム／サービス及びサプライチェーン全体のセキュリティを確保する。

(A)「信頼の創出・証明」技術の研究開発

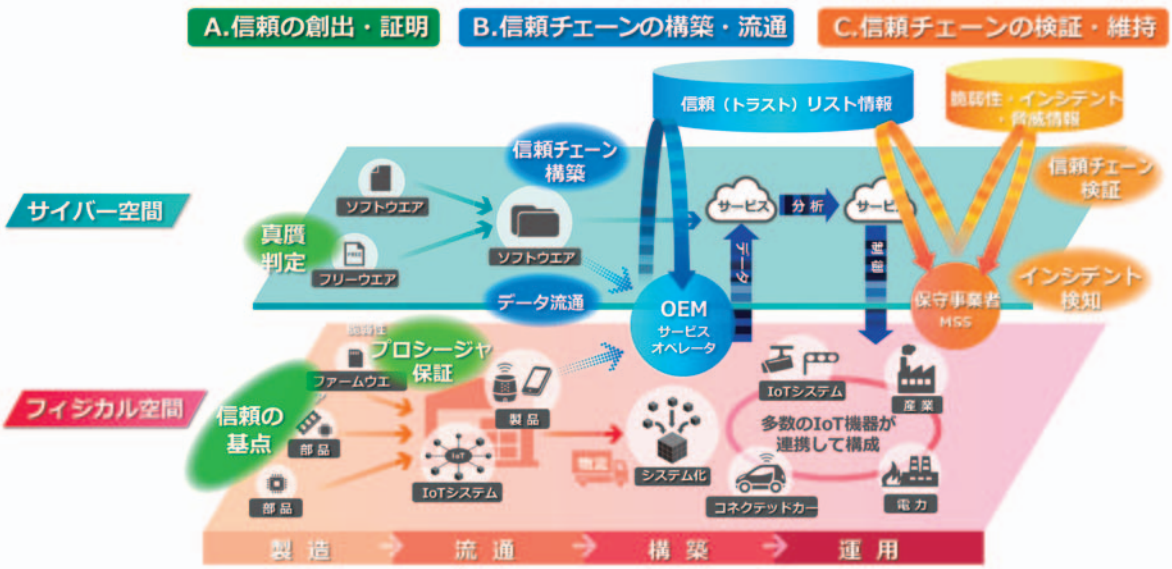
個々のIoT機器やサービスのセキュリティを強化し、多様なIoTシステム／サービスやサプライチェーン全体のセキュリティ確保を実現する上で必要な信頼の創出・証明技術の研究開発を行う。

(B)「信頼チェーンの構築・流通」技術の研究開発

多様な社会インフラやサービス、幅広いサプライチェーンのセキュリティを確保するため、IoTシステム／サービスや調達・構築に関わるサプライチェーンにおいて「信頼チェーン」を構築し、必要な情報をセキュアに流通させる技術を研究開発する。

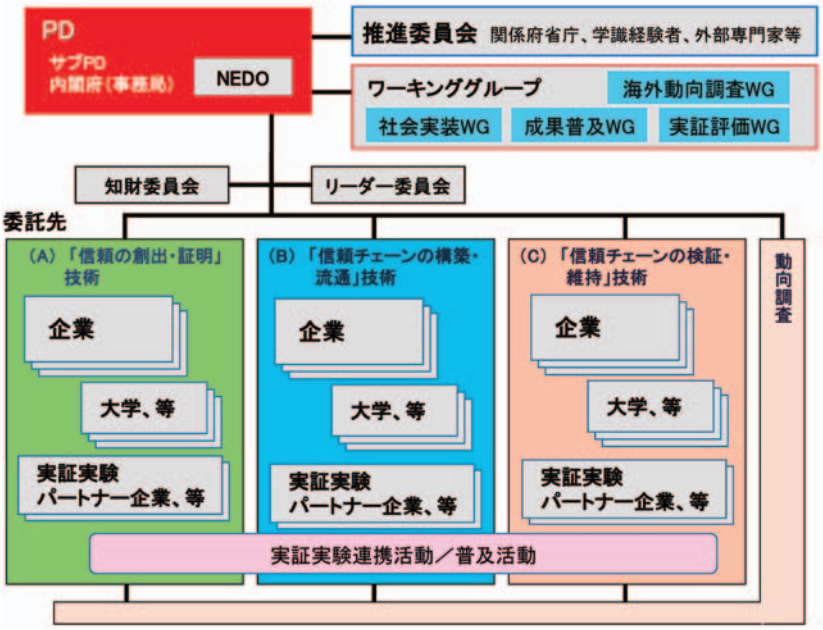
(C)「信頼チェーンの検証・維持」技術の研究開発

「信頼チェーン」を構築したIoTシステム／サービス及びサプライチェーンにおいて、「信頼チェーン」が安全に運用されていることを検証し、維持することを可能とする技術を研究開発する。加えて、技術成果の社会実装に必要な導入・運用マニュアルや組織・人材開発の取組みも併せて行う。



実施体制

プログラムディレクター（PD）のもと、関係府省庁、学識経験者、外部専門家等が参加する推進委員会を設置し、プロジェクトを推進するとともに、実証評価や成果普及等の横断的な課題についてはワーキンググループ（WG）により解決を図る。また、研究開発の成果を主体的に実用化・事業化できる企業を中心に、先進技術を有する大学等を含むプロジェクト実施体制を構築する。さらに、技術成果の社会実装に向けた実証実験において、実フィールドをもち課題認識のある事業者やベンダが主体的に取組めるように、社会実装の観点からの要求事項を共有できる体制を構築する。



出口戦略

実証実験から社会実装へ

研究開発した技術の実証実験と、その結果のフィードバックを繰り返すことで、早期の社会実装を目指すとともに、中小企業を含むサプライチェーン全体での本基盤の活用を促し、日本発の高いセキュリティ品質を備えた製品・サービス・システムの普及を目指す。

参画企業が主体的に製品化・事業化

参画企業が主体となって製品化を進め、各産業分野への導入を推進する。一部の成果は、関連するベンダにライセンス供与することで、その普及を目指す。

欧米の基準と整合性を取り、府省による制度整備と連携

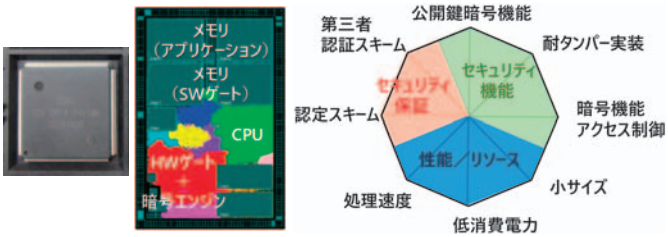
関係省庁等で検討しているIoT機器やサプライチェーン全体に関する政府施策と連携し、米国や欧州のサイバーセキュリティフレームワーク整備と伍することができる制度作りに貢献する。特に、本プロジェクトの取組や成果が、欧米で加速しているサイバーセキュリティのフレームワークの動きと整合しているかの検証を行い、国際競争力が確保されることを確認しつつ研究開発を進める。

これまでの成果・期待される成果

各研究テーマは2020年度に基本技術の開発を完了し、プロトタイプシステムを用いて、社会実装を目指した実証実験に順次着手している。

2021年度は各テーマの社会実装責任者の元、インフラ、ビルサービス、自治体等への実証実験を加速させる。

本プロジェクトが終了する2022年までに、実証実験を行った産業分野について、実証実験の結果を踏まえ確認等を行う機関、トラストリストの構築・管理をする機関、脆弱性・インシデント・脅威等の情報管理をする機関の体制検討を完了し、サプライチェーン全体のセキュリティ確保を実施可能な体制を構築する。

本プロジェクトでは、『サイバー・フィジカル・セキュリティ対策基盤』の実現により、Society5.0の実現がもたらす価値創出を支えるとともに、グローバルなサプライチェーンに参画する要件となるセキュリティ確保を適切なコストで実現して日本の製品・サービスの国際競争力を強化する。

● 信頼の基点となるセキュア暗号ユニット（SCU、Secure Cryptographic Unit）と実装イメージ