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

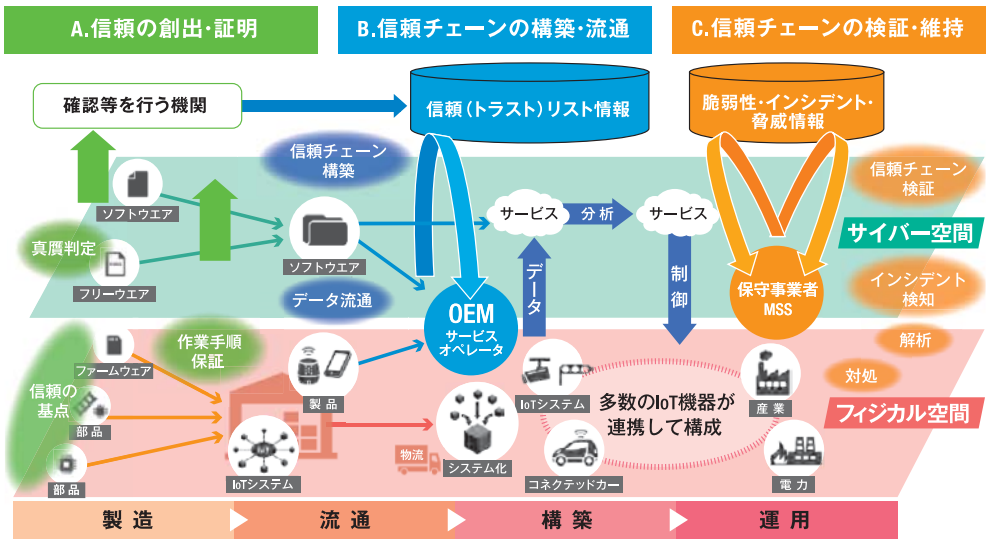
個々のIoT機器やサービスのセキュリティを強化し、多様なIoTシステム／サービスやサプライチェーン全体のセキュリティ確保を実現する上で必要な信頼の創出・証明技術の研究開発を行う。

(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。

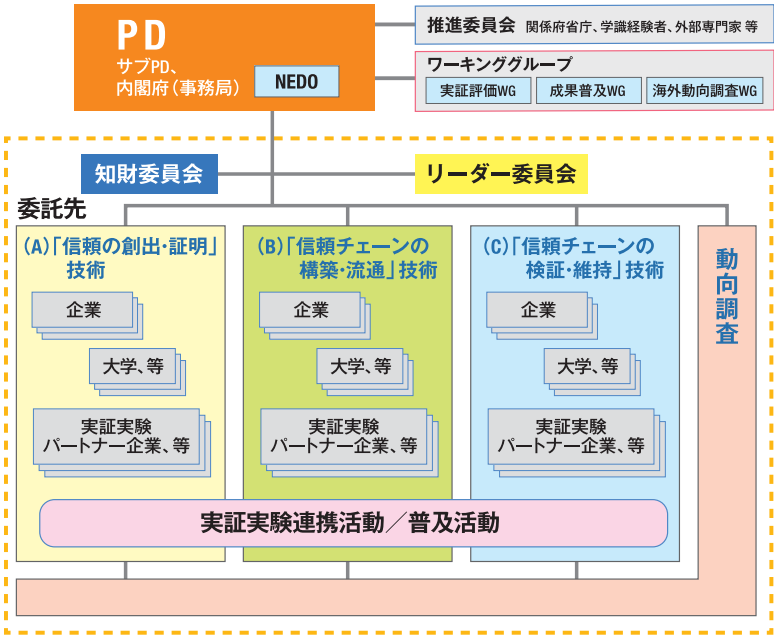
(C)「信頼チェーンの検証・維持」技術の研究開発

「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。

期待される成果

2020年を目途に、特定分野の実証実験パートナー環境でのIoTシステム／サービスまたはサプライチェーンにおける『サイバー・フィジカル・セキュリティ対策基盤』の社会実装を目指した実証実験に順次着手し、その他大規模なサプライチェーンを保有している社会インフラ産業への応用展開を図る。

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、IoT社会を強靭化してサイバー犯罪による経済損失を回避することで、Society 5.0の実現がもたらす約90兆円の価値創出を支える。さら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することにより、輸出主体の製造業の参入機会を確保して日本の製品・サービスの国際競争力を強化する。

PD Interview

プログラムディレクター　インタビュー

後藤 厚宏

情報セキュリティ大学院大学
学長

IoT社会をサイバー攻撃の脅威から守りたい。

Society 5.0を支えるセキュアなIoTサプライチェーンの実現を目指して。

様々な機器がインターネットでつながっているIoT社会。その恩恵と背中合わせにあるのが、悪意あるサイバー攻撃の脅威です。「サイバー・フィジカル・セキュリティ対策基盤」を世界に先駆けて整備することで、IoT社会の強靭化を図る本プログラムについて、後藤 厚宏PDにインタビューしました。

「つながって便利になれば、当然リスクも増えてきます」

Q－IoT社会になって、サイバーとフィジカル。両面のセキュリティが必要ということですね。

PD－**サイバーはいわゆるIT、今、DX（デジタルトランスフォーメーション）と言ったほうがいいのかもしれません。それらを、人間社会がどんどん使いこなして新たな価値を享受しようとするに従って、リスクも増えてくるという問題があります。**

今回、IoTとサプライチェーンに着目して取り組んでいます。デバイスとしてのIoTだけではなく、例えばスマホから取りだした情報をクラウドに上げて、分析して、またそれを戻すことによって、ナビゲーションのサービスを受けられます。こういったIoTの使い方は、まさにサイバー・フィジカルな典型です。

その仕組みを創り出すサプライチェーンはどうかというと、工場などは既にIoTが幅広く採用されています。そのため、IoTとサプライチェーンのセキュリティ確保は同時に取り組む必要があります。

Q－IoTは、いつのまにか社会全般に広がっていますね。

PD－IoTを3つの領域に分類したときに、1番目が、いわゆる重要インフラにおけるIoT。例えば、電力システムや鉄道システムを制御しているようなIoT。2番目が、産業用IoT。工場の中や流通システムで活用されているIoT。3番目が、コンシューマー向けのIoT。家庭用のゲーム機であり、スマート家電もIoTに含まれます。大体その3つに分類しているのですが、第1期は重要インフラのIoTを、**第2期は産業用の工場とか物流とかに直結するサプライチェーンのIoTに重点を置いています。**　＊図1参照

「そこで重要になってくるのが信頼と信頼の結びつきです」

Q－「信頼の創出・証明」「信頼チェーンの構築・流通」「信頼チェーンの検証・維持」という研究内容を少し詳しくお聞かせいただきたいと思います。

PD－例えばサプライチェーンの場合、取引会社同士は「契約」でつながっているわけです。それが成り立っているのは、互いに「信頼」をしているからですね。

その「信頼」の崩し方として、サイバー上の、マルウェアやウイルスで、うその発注書やうその設計図を出したりして、サプライチェーンを成り立たなくする。

例えば実社会で銀行口座を開こうとすると、写真付きの免許証を持って窓口に行って、本人の確認が出来れば銀行口座を開けます。免許証が信頼の基になっているわけです。それに相当するものをIoTやサプライチェーンの中で創り出すのが、「信頼の創出・証明」のプロセス。免許証を使って銀行口座を開いたら、プラスしてクレジットカードも取得して信頼のチェーンが広がり、それを使って買い物ができるようになる。それが「信頼のチェーンの構築・流通」になります。

Q－そして、「信頼のチェーンの検証・維持」では、インシデントの検知などを行うわけですね。

PD－**まさに、その一連の仕組みを創り出すというのが今回の取り組みです。現状では、サプライチェーンの「信頼」を確認するのは大変だし、手間もかかります。それを先進的な技術を使って、いつでも低コストで確認できるようにする。**

例えば、何がいいですかね。このペットボトルのお茶。お茶は、

ペットボトルは誰が作ったものかを瞬時にさかのぼって安全が常に確認できるトレーサビリティを可能にしようという考え方です。

Q－この研究開発を実装するために克服すべきところは、なんでしょうか？

PD－**情報のやりとりや確認する手間がかかるともちろんコストは上がりますが、それ以上のメリットがあれば導入が進みます。**

お客様に代わって流通を追跡するサービスだとか、その評判をチェックするサービスなど、新しいビジネスが生まれてくるかもしれない。

サイバー・フィジカルのセキュリティレベルを上げることによって、新しいビジネスが生まれ、そこから新しい付加サービスが出てくることが成功事例になると思います。

Q－幅広いサプライチェーンに「サイバー・フィジカル・セキュリティ対策基盤」を組み込むのは、大変なことだと思います。

「信頼を証明する仕組みは日本がリーダーシップをとりたい」

PD－製造プロセスを全て管理するのは非常に困難なことです。今回、どういう製造プロセスによって作られたかという、手続きとか、発注書に従って、きちんと作りましたよというのが証明できるようにしておく。これによって意図しない製品を排除する。そういうこともやろうとしているので、幅広い産業で使えるようにしたいですね。

サプライチェーンは世界に広がっています。日本がリーダーシップをとって、信頼の創出や証明する仕組みを創ろうとしている姿勢を早く示したいと思います。

Q－府省庁の連携とか、産学官の連携メリットを少し、お聞かせいただければ。

PD－セキュリティは、分野とか、事業とか、学問だけで語れない世界です。経産省の中小企業向けのセキュリティもあれば、総務省の通信向けのセキュリティもある。セキュリティは多くの分野や省庁に関わるので連携は当然必要です。

また、産業界だけの話ではなく、十分高度なアカデミックな知見が求められる世界でもあります。そういう意味で「学」の協力というのは、必須になりますし、「官」の応援も必要になります。不正アクセス禁止法などの法律はありますけど、まだ法律の整備が十分ではないのは確かですね。

Q－PDご自身がお考えになっている、セキュアなSociety 5.0とは

PD－Society 5.0によって、様々なものがつながり、新たな価値が生まれます。そこを悪用されたら意味がないので、悪用されるリスクを極力減らしていくというところが大事だと思います。

様々なものがつながるからこそ影響も大きくなる Society 5.0の世界において、社会を守れる「サイバー・フィジカル・セキュリティ対策基盤」を、様々な角度から整備するのが第２期のプログラムの目標です。

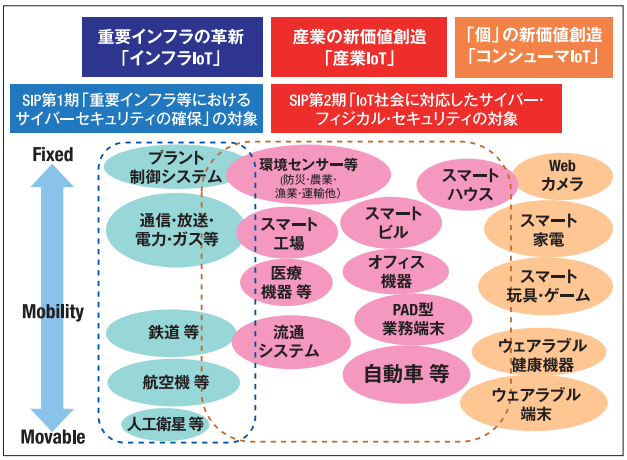


図1