重要インフラ等における サイバーセキュリティの確保

世界で最も安心・安全な社会基盤の確立を目指して

近年、サイバーセキュリティ攻撃の脅威はますます深刻化しており、その矛先も通信・放送、エネルギー、交通といった社会を支える重要インフラに向けられ始めている。2020年東京オリンピック・パラリンピック競技大会を迎える我が国においても、重要インフラにおけるサイバーセキュリティの確保は緊急の課題であり、その技術開発と制度の設計、そして人材育成に大きな期待が寄せられている。重要インフラ等におけるサイバーセキュリティの確保では、オールジャパン体制で迅速かつ大胆に推進する。

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。情報基礎研究部に配属され、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。衆議院、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

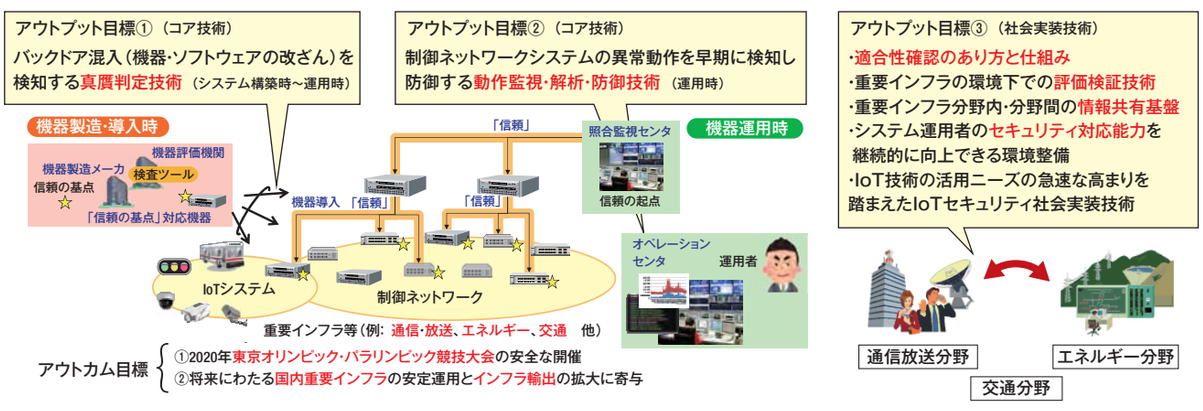
(a) コア技術の開発: 制御・通信機器と制御ネットワークのセキュリティ対策技術の開発

- 制御・通信機器の真贋判定技術(機器やソフトウェアの真正性・完全性を確認する技術)を開発する。
- 制御・通信機器および制御ネットワークの動作監視・解析技術を開発する。
- 制御・通信機器およびシステムの防御技術を開発する。
- IoTのセキュリティを支える暗号実装技術を開発する。

(b) 社会実装技術の開発: 社会実装向け共通プラットフォームの実現と、セキュリティ人材の育成

- 開発されたセキュリティ機能が正しく実装されていることを確認するための適合性確認のあり方と仕組みを検討する。
- インフラ事業者間をまたがる情報共有プラットフォーム技術を開発する。
- 重要インフラにセキュリティ技術を適用するうえでの評価検証プラットフォーム技術を開発する。
- セキュリティ技術の開発に加え、重要インフラシステムに導入するセキュリティ技術の評価と運用が可能な人材を育成する。

●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研究開発概念図



出口戦略

☑ 出口指向の研究開発を推進

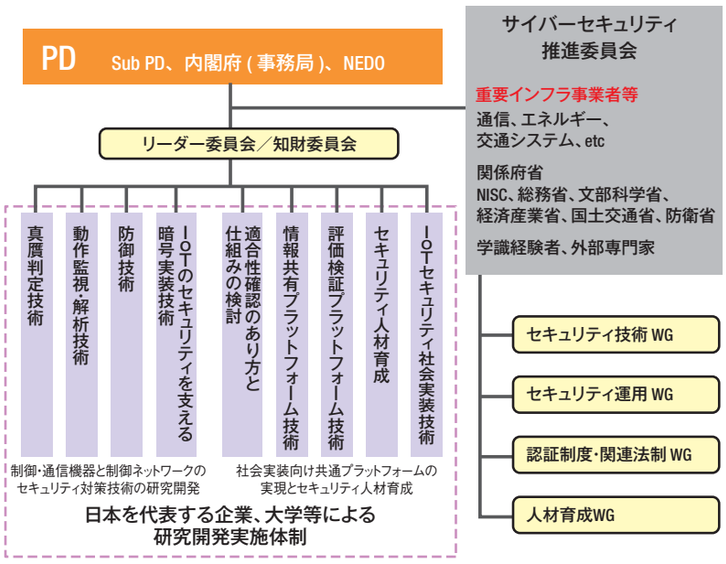
2020年東京オリンピック・パラリンピック競技大会に向けて先行すべき重要インフラを皮切りに、順次、重要インフラへの導入を目標とした研究開発を推進するとともに、研究開発段階から社会実装を最短で実現する研究開発体制を構築する。

☑ サイバーセキュリティ普及推進のための方策を展開

強靭なセキュリティ機能を日本全体の重要インフラへ順次展開。利用される分野に応じ、標準化・規格化・安全評価手法やその認定手法のあり方と仕組みを検討し、開発成果の利用を促進する。また、本研究開発の成果を活用した認証評価サービスや、技術、製品の輸出展開によりグローバルビジネスに貢献する。

実施体制

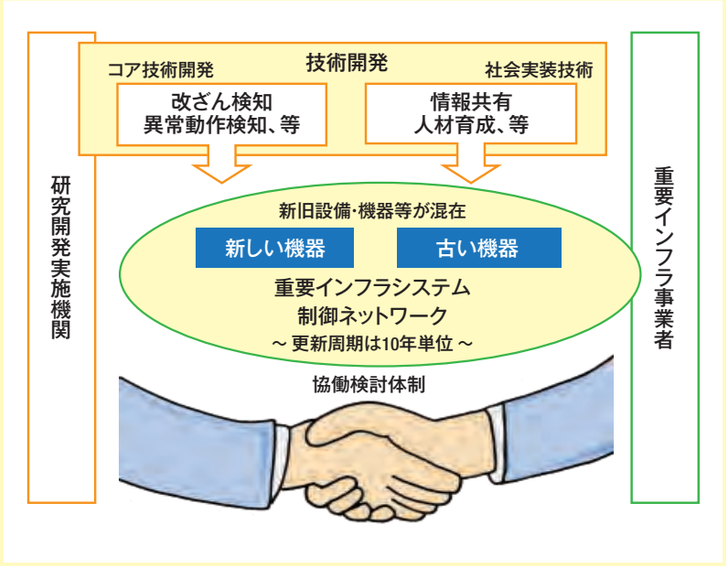
プログラムディレクター（PD）と、サブPD、および、関係府省、内閣サイバーセキュリティセンター（NISC）、学識経験者、外部専門家、さらには重要インフラ事業者が参加するサイバーセキュリティ推進委員会のもと、各研究主体が、コア技術、および社会実装技術の開発を実施する。さらに、主要な研究課題に対応した4つのワーキンググループ（WG）を組織し、研究開発実施者、重要インフラ事業者、有識者の密な連携による課題の意識合わせやニーズの抽出を実施し、より現場の要望に即した技術開発が行えるような体制が整備されている。



これまでの成果

重要インフラ事業者との実検証を推進

「優先度の高い対策の早期導入」「事業者側の検証環境での評価」といった重要インフラ事業者からの要望に基づき、先行して実装可能な一部技術の実検証を推進している。その一例が動作監視・解析技術で、旧式の設備と新型の設備が混在する重要インフラ制御システムに対して、効果的な監視や解析、およびセキュリティ攻撃を検知可能な技術の検証を2016年末から進めている。また、人材育成についても重要インフラ事業者との協働のもと、実業務に即した教育カリキュラムの策定が進められている。



PD

プログラムディレクター　後藤 厚宏 インタビュー

オリ・パラ後も見据えた、安全・安心・高セキュリティな重要インフラの実現を目指す

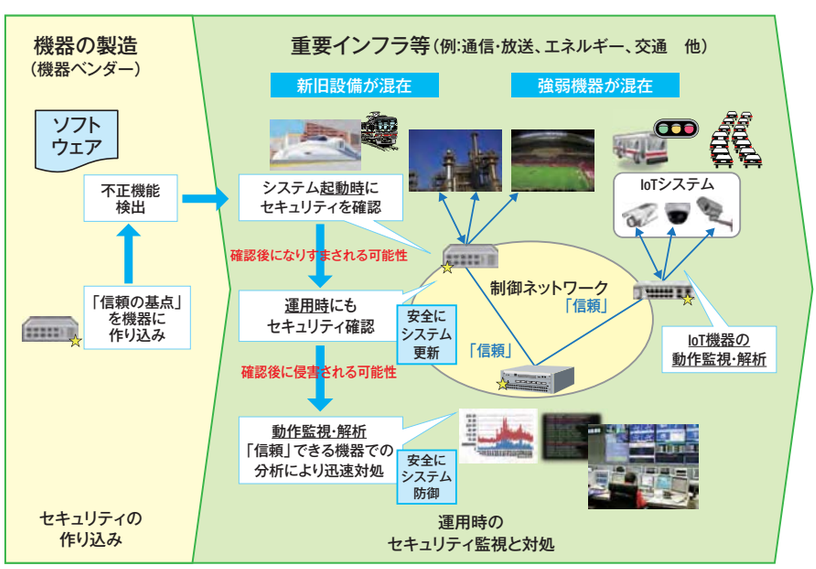
社会を支える重要インフラがサイバー攻撃の脅威にさらされる中で、サイバーセキュリティ確保に向けた取り組みは、重要インフラ事業者との密な連携をはじめとしたオールジャパンの体制により、着実にそのあゆみを進めている。

オリンピック・パラリンピックを目前に、サイバーセキュリティの確保に邁進

通信・放送、エネルギー、交通といった社会インフラに対するサイバー攻撃の脅威は現実化しており、重要インフラ等におけるサイバーセキュリティの確保が、世界的にも急務となっている。2017年度で3年目を迎えた本プログラムを統括する後藤厚宏氏は、次のように決意を新たにする。

「重要インフラに対するサイバー攻撃の事例が世界的に報告されていますが、2017年5月にはランサムウェア（身代金要求型ウィルス）による大規模な攻撃により100ヶ国以上で被害が出るなど、2020年の東京オリンピック・パラリンピック競技大会を前に、ますます本プログラムの重要性を認識しています。また、サイバーセキュリティの確保は、コア技術の研究開発と社会実装技術が一体となることで、はじめて実現されます。そのためにも、産学連携をさらに推し進め、一丸となってプログラムに邁進していかなければなりません。」

●サイバーセキュリティを確保するための仕組み



重要インフラ事業者との密な連携で、いち早い実装・検証を実施

そうした中で、後藤氏が「一つの大きな成果」として強調するのが、2016年度から実施している社会実装の加速に向けた重要インフラ事業者との協働である。後藤氏は、「多くのインフラ事業者の方々に参加してもらえたことで、現場からの具体的な要望や提案に基づいた、研究開発が行える体制を整えられました。」と話す。実際に大学や研究機関、産業界、そして重要インフラ事業者を交えた推進委員会をはじめ、ワーキンググループによる課題の意識合わせと要望の抽出、さらには各研究開発テーマを跨った技術の一体化・システム化に際してのテーマ間の連携など、いち早い社会実装に向け、有機的な活動が可能な組織体制が整備できているという。

また、重要インフラ事業者からは「優先度の高い対策を早期に導入したい。」「実際に現場で検証を行い、評価を行いたい。」との要望も寄せられており、研究開発中のコア技術について、いち早い実装も行われようとしている。その一例が、動作監視・解析技術の領域だ。新旧機器が混在する重要インフラの制御システムの健全性を確認しつつ、攻撃を検知する技術について、重要インフラ事業者との協働による検証が、2016年度末から開始されている。

一方、社会実装向け共通プラットフォームの実現や、セキュリティ人材の育成といった社会実装技術の開発も進展が見られている。後藤氏は、「重要インフラ事業者間を跨いだ、セキュリティ情報の共有プラットフォームについても、重要インフラ事業者に利用してもらいながら都度、機能の強化と改善を図っていきたいと考えており、2017年から徐々に稼働を開始する計画です。」と話す。

重要インフラ等におけるサイバーセキュリティの確保

日本発のセキュリティ技術を重要インフラの新しい付加価値に

また、サイバーセキュリティに関する人材育成では、実際の現場でオペレーションを担う人員にとって、どのような教育メニューが本当に必要なのか、重要インフラ事業者と共に検証を行い、より実地に即したカリキュラムを策定していくという。

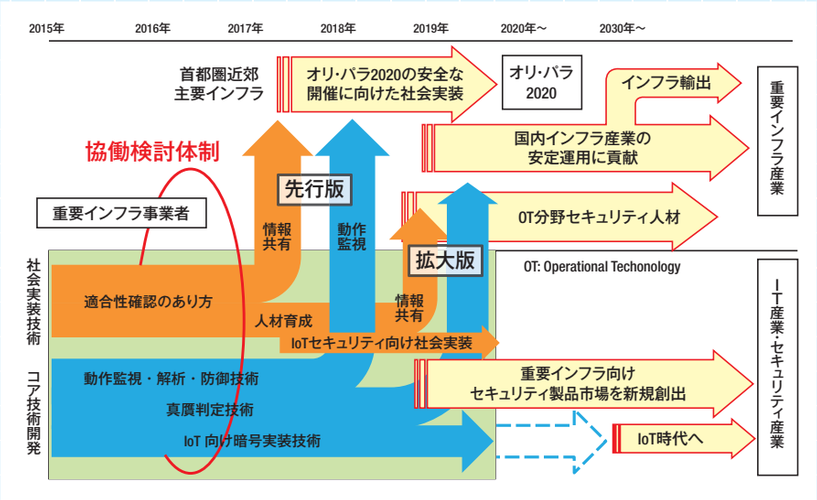
後藤氏は、「まずは2020年の東京オリンピック・パラリンピック競技大会に向けて地に足の着いた社会実装を目指します。その一方で、セキュリティは来たるべき『Society 5.0』を支える重要な技術でもあることから、目の前の課題を解決する技術の開発だけでなく、プログラム終了後の10年後、20年後を見据えた研究開発も並行して進めていきます。」と強調する。

そのためにも、新たなサイバー攻撃の手法やセキュリティの脆弱性への対策を継続して行うとともに、AIやビッグデータの活用により、セキュリティ技術をさらに進化させていく構えだ。最後に後藤氏は、次のように将来展望を語った。

「日本のエネルギーの安定運用、通信・交通網の信頼性といった強みに、さらにセキュリティという付加価値を、本プログラムを通じて提供していきます。そして、日本発のセキュリティ技術、ひいては安全・安心な重要インフラを世界に発信していきたいと考えています。」

今後の予定

東京オリンピック・パラリンピック競技大会が開催される2020年に向け、産学、および重要インフラ事業者との密な連携により社会実装に向けた確実な成果を上げていくとともに、2020年以後も重要インフラ全体の付加価値・競争力向上のための研究開発を継続して実施していく。



セキュリティという付加価値を実装することで、安全・安心で定評のある日本の重要インフラ産業の競争力をさらに向上させていきます。