SIP

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

日本発の科学技術イノベーションが未来を拓く

重要インフラ等におけるサイバーセキュリティの確保

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
情報セキュリティ研究科研究科長
教授

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。

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。

Atsuhiro Goto

重要インフラに迫る サイバーセキュリティの脅威

国民生活や経済活動は、さまざまな社会インフラによって支えられている。近年、通信・放送、エネルギー、交通といった重要インフラに対して、サイバー攻撃の脅威が現実化している。海外では、製鉄所内発電所の制御システムへのワーム感染による数か月の停止、鉄道運行システムのマルウェア感染による鉄道の6時間停止といったサイバー攻撃事例が報告されており、その対策が全世界的に急務となっている。

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とっては、会場の近隣で、万が一、サイバー攻撃による停電、交通網の遮断、通信網麻痺が同時に発生した場合、大混乱となるのは明らかだ。

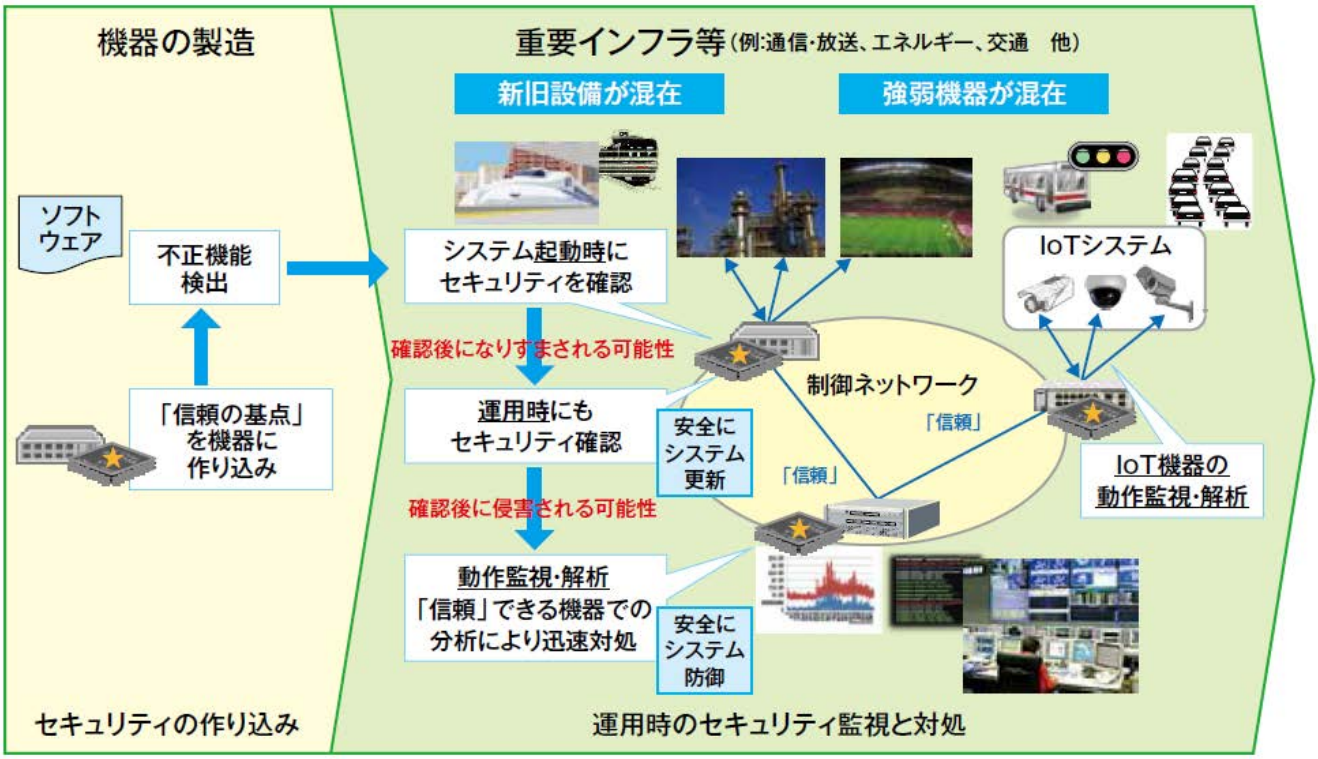
さらに今後、IoT(Internet of Things)の普及により多種多様な機器がネットワークに接続、重要インフラにおいても活用促進が予想されているが、そこでもサイバー攻撃の脅威が生まれ、攻撃の影響が広範に渡ることも懸念されている。「重要インフラ等へのサイバーセキュリティを確保し安全な社会基盤づくりを行うとともに、国産のセキュリティ技術のレベルアップと人材育成によって産業を活性化していくことは、我が国にとって最重要課題であると考えています」と訴えるのは、本研究開発計画のプログラムディレクターを務める後藤厚宏氏だ。

セキュリティ対策の推進には 国をあげた取り組みが不可欠

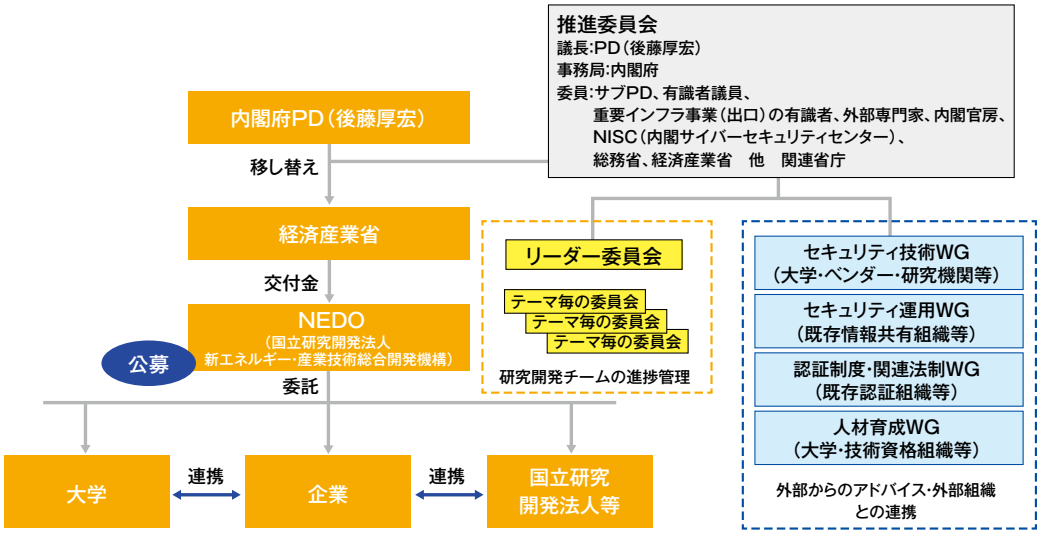
「スポーツを好む一方で、電子部品をいじることにも熱中した理系少年でした」と語る後藤氏は、東京大学工学部電子工学科の門を叩く。そして大学院への進学を目前に出会ったのが、卒業論文のテーマとして選んだコンピュータだったという。「当時はPCなんてなかった時代。秋葉原で部品を集めて自分で一から組み立て、ソフトウェアも自分で組む。そうした手作り感が面白かったのかもしれませんね」と後藤氏は振り返る。その後、日本電信電話公社(現NTT)に入社、当時の国家プロジェクトである「第五世代コンピュータ」の開発計画へ参加しコンピュータの並列処理の研究開発に携わっていたが、転機となったのがインターネットの登場だった。

「当時、黎明期にあったインターネットの実用化に関する研究を担当することとなり、そこからサイバーセキュリティにも触れるようになったのです」と後藤氏は語る。

以後、長らくインターネットおよびサイバーセキュリティの研究に携わってきた後藤氏だが、サイバーセキュリティの脅威が重大な社会的問題となって



●研究開発概念図



●実施体制

いく中で、国をあげての対策が急務であると危機感を募らせていたという。

「サイバーセキュリティは我が国全体の課題であり、広範囲にわたるその対策の実現には、産学官の連携による協力体制が不可欠です」と後藤氏は訴える。

コア技術と社会実装技術の開発に注力

本研究開発計画の基本テーマとして掲げられているのは、①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、②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、である。

まず、①のコア技術の開発では、重要インフラの制御ネットワークを構成する機器装置のセキュリティを調達時とシステム運用時に確認できる技術を開発し、その技術に基づく機器の適合性試験技術と運用時の照合機能を実現していく。加えて、制御・通信機器およびシステムの防御技術、IoT向けセキュリティ確認技術についても開発していく。「特に重要インフラの設備では10年以上の利用が前提のため、旧式の設備が残っているインフラシステムにおいても新しいセキュリティ技術を段階的に導入できるようにすること、また、IoTのセンサーのようにセキュリティ機能の実装が限られる機器にも有効な対策を施していくことが重要と考えています」と後藤氏は説明する。

続く②の社会実装技術の開発では、セキュリティ技術や機器に対して、正しく機能が実装されているか確認するための認証制度の設計をはじめ、各業界および業界間で柔軟な情報共有が可能なプラットフォームの構築、そして、コア技術を評価検証するためのプラットフォーム技術の確立、そして重要インフラを支えるセキュリティ人材の育成を進めていく。

「本研究開発の推進にあたっては、分野ごとに異なるインフラシステム間を円滑に連携可能な仕組みが必要であり、ベンダーのみならず大学・研究機関、インフラ事業者や関連団体、さらには認証団体にも参加してもらい、現場からの要望や提案も含め、広く意見を募りながら、プロジェクトを展開していきたいと考えています」と後藤氏は語る。

セキュリティ強化が産業競争力向上の推進力に

後藤氏は、まずは2020年東京オリンピック・パラリンピック競技大会の安定運営の実現を中間目標として定め、通信・放送、エネルギー、交通等の重要インフラに対して本研究開発成果を実装していくことを目指す。そして、最終的には本研究開発により、日本の産業の競争力向上にも寄与していきたいという。技術、制度、人材を含めたサイバーセキュリティの強化は、重要インフラの付加価値となって競争力を促進、ひいては日本の得意産業としてインフラ輸出の拡大に貢献すると期待される。後藤氏は、本研究開発の推進にあたり、次のように思いを語る。

「NTTの研究所に在籍していた頃から、私は技術開発の成果や活動そのものが社会や産業の役に立てるような“出口指向”を強く意識していました。我が国のサイバーセキュリティ対策の強靭化は、即時行動すべき緊急課題であると同時に、産業競争力強化の『レバレッジ(梃)』となるものです。産学官、そして業界の垣根も超えたオールジャパンの体制で取り組んでいきたいと考えています」

研究開発テーマ

1. 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･通信機器のセキュリティ確認技術を開発する。
●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向けセキュリティ確認技術を開発する。

2. 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認証制度を設計する。
●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、製品の開発、およびその評価が可能な人材を育成する。

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策定を推進し、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。

産学官、そして業界の垣根も超えた
“オールジャパン体制”で取り組んでいきます

サイバーセキュリティ強化で
産業競争力の向上を推進

内閣府

発　行：内閣府政策統括官（科学技術･イノベーション担当）
発行日：平成27年12月