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

Pioneering the Future: Japanese Science, Technology and Innovation

Cyber-Security for Critical Infrastructure

Program Director

Atsuhiro Goto

Dean and Professor
Graduate School of Information Security, Institute of Information Security

Profile

Professor Atsuhiro Goto received his PhD from University of Tokyo in 1984. Upon graduation, he joined NTT, where he was assigned to the company's information and communication technology R&D, working for nearly 27 years on information technologies. In 2007, he was named head of the NTT Information Sharing Platform Laboratories, and subsequently named head of the NTT Cyber Space Laboratories in 2010. He has served in his present position since 2011. Professor Goto has various experiences in government-related work as well, serving as member or chair for various councils and committees for the House of Representatives, the Cabinet Secretariat, the Ministry of Internal Affairs and Communications, the Ministry of Education, Culture, Sports, Science and Technology, the Ministry of Economy, Trade and Industry, the Ministry of Defense, and other government ministries.

Creating the Safest, Most Secure Social Infrastructure in the World

The threat of cyber-attacks has been growing in frequency and severity over the past several years. Communications and broadcasting, energy, transportation, and other critical infrastructure are now beginning to be targets of these attacks. As Japan looks forward to the 2020 Tokyo Olympic and Paralympic Games, ensuring the cybersecurity of our nation's critical infrastructure has become a pressing issue. There are significantly rising expectations for cybersecurity technology development, systems design, and human resources development in Japan. Our nation is now engaging in a boldly, quickly, and completely in an all-Japanese program to ensure cybersecurity for critical infrastructure.

Atsuhiro Goto

The Growing Threat of Cybersecurity to Critical Infrastructure

A variety of different social infrastructure supports the lives of our citizens and the economic activity of our nation. Over the past several years, communications and broadcasting, energy, transportation, and other critical infrastructure have become a main target of cyber-attacks. We have seen reports from overseas sources describing several-month-long interruptions of control systems for steel manufacturing plants due to computer worms, six-hour stoppages of railroad operations due to malware in rail operation systems, and other cases of cyber-attack. Consequently cyber-attack countermeasures have become a pressing global issue.

As Japan looks forward to the 2020 Tokyo Olympic and Paralympic Games, our nation has predicted the potential for massive chaos should any cyber-attacks near event stadiums cause power outages, traffic network interruptions, and communications network paralysis.

With the coming popularization of the Internet of Things (IoT), a wide variety of devices will connect to the network, placing a greater load on critical infrastructure. These connected objects will also suffer from the threat of cyber-attack, increasing the range and influence of such attacks. “I believe that one of the most important issues for our nation is to create a safe social foundation built on secure infrastructure. To achieve this, we must revitalize our domestic industries through cybersecurity products and services, as well as provide personnel in Japan who are experts in cybersecurity,” says Atsuhiro Goto, program director for this research and development plan.

Cybersecurity Measures Require Nation-Wide Engagement

Professor Goto, who describes himself as a science nerd interested in both sports and tinkering with electronic gadgets in equal measure, sought his education at the Department of Electronic Engineering, University of Tokyo. In matriculating to graduate school, he immediately became involved with computers, which he had selected as the topic of his graduation thesis. Says Goto, “At the time, there were no such thing as PCs. We would go to Akihabara to search for computer parts, and we even put together the software on our own. I think that sense of being a ‘maker’ was probably what made it most interesting.” After graduation, Goto went to work for Nippon Telegraph and Telephone Public Corporation (now NTT), becoming involved in a national project: The Fifth Generation Computer Systems (FGCS) Project. His role there involved research and development of parallel processing systems. However, Goto points to the advent of the Internet as the turning point in his career.

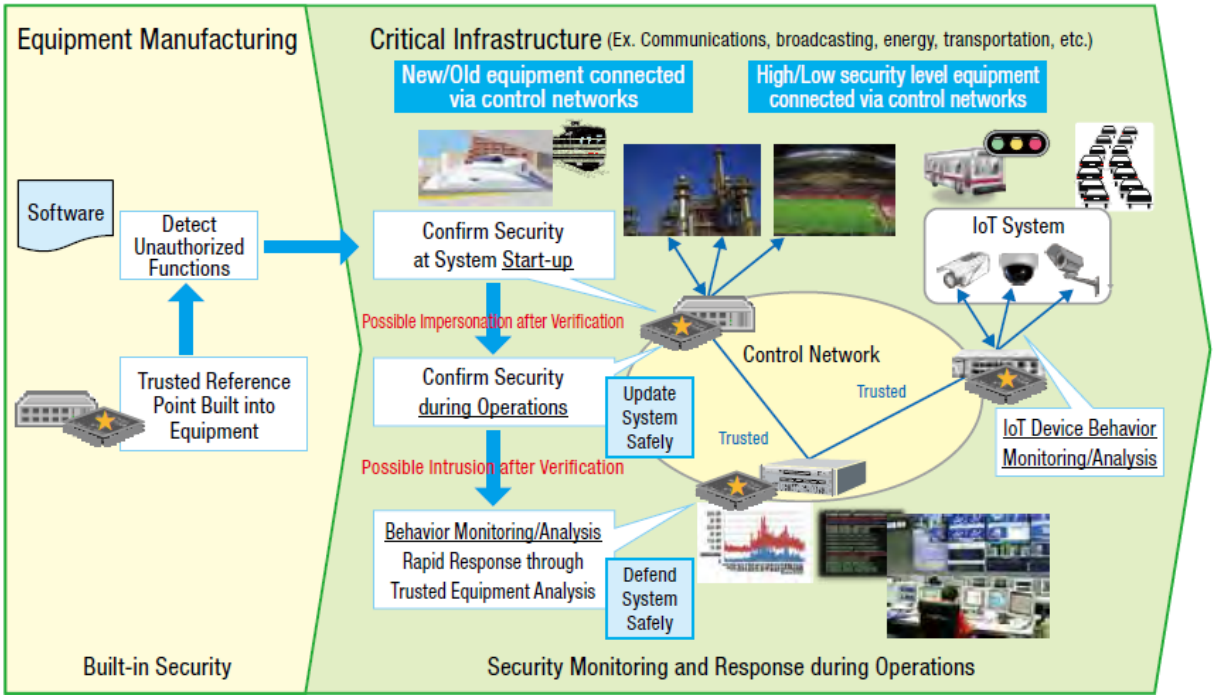
“I became involved in research related to commercialization of the Internet, which was still in its very earliest stages at the time. From there, I branched out into cybersecurity as well.”

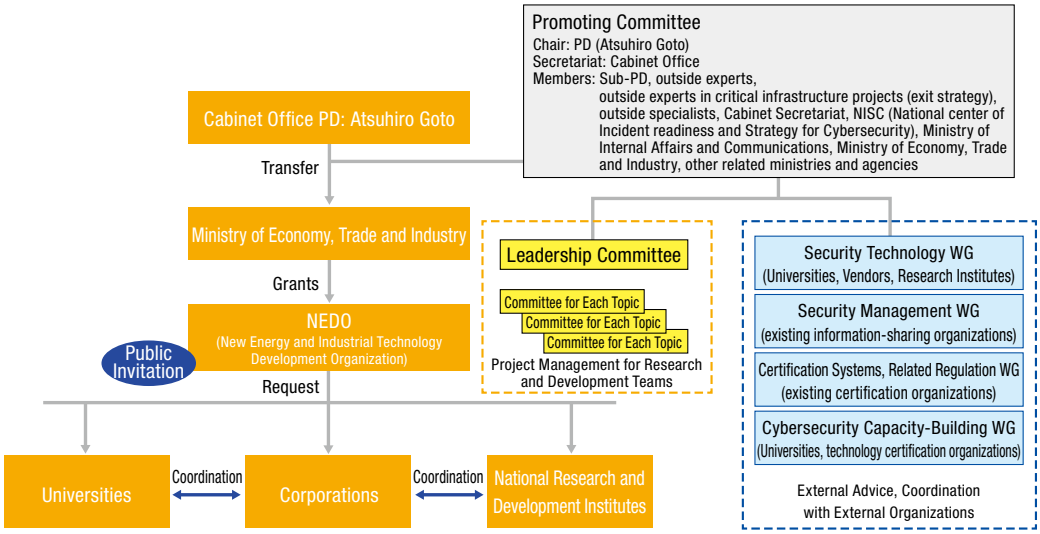
Ever since, Professor Goto has spent many years researching the Internet and cybersecurity, coming to feel a great sense of urgency about the need for national-level measures against threats to cybersecurity. This threat has now evolved into a major social issue as well.

Goto asserts, “Cybersecurity is a nation-wide issue for Japan. We have to create a cooperative structure through coordinated industry-academy-government efforts if we are to produce wide-ranging measures to address this threat.”

A Focus on Core Technologies and Social Implementation Technologies

There are two basic components defined under this research and development plan:





●Implementation Structure

(1) Development of Core Technologies (development of cybersecurity technologies for control system and communication system equipment and control networks); and (2) Development of Social Implementation Technologies (creation of a shared platform for social implementation and cybersecurity capacity-building).

With respect to developing core technologies under (1) above, this national project will engage in developing technologies to verify the security of devices and equipment that make up critical infrastructure control system networks both in procurement and during system operations. As well, this part of the project will create conformance test technologies and verification functions during operations for devices based on the technologies developed. The project will continue forward to develop systems defense technologies for control systems and security verification technologies for IoT devices. Professor Goto explains, "In particular, we assume that critical infrastructure equipment will be used for 10 years or even longer. This means that we have to be able to introduce new cybersecurity technologies in stages for infrastructure systems that incorporate older equipment. We also think it is important to incorporate effective measures for devices, such as IoT sensors, that have limited implementation of security functions."

The second imperative under this project, as mentioned under (2) above, is developing social implementation technologies. Here, this program intends to design certification systems to verify whether correct functions are implemented for cybersecurity technologies and devices. This includes structuring platforms capable of sharing information flexibly within and between industries. This program also intends to secure platform technologies for evaluation and verification core technologies and to develop critical infrastructure system engineers for cybersecurity.

Says Professor Goto, "In advancing this research and development, we need a mechanism to facilitate seamless coordination between the differing infrastructure systems of each industry. We are actively seeking the opinions and participation of not only security vendors, but also universities, research institutes, infrastructure vendors, related groups, and certification bodies, as well as seeking requirements and suggestions from those working on the front lines of critical infrastructure operations."

Stronger Security Creates a Driving Force for Industrial Competitiveness

Professor Goto has set interim goals to ensure the safe and secure operation of the 2020 Tokyo Olympic and Paralympic Games. He aims to incorporate the research and development outcomes of this project into communications, broadcast, energy, transportation, and other critical infrastructure. Goto hopes that this research and development ultimately contributes to stronger competitiveness for Japanese industry. More secure technologies, systems, and trained personnel can generate more value for critical infrastructure industries, leading to improved competitiveness. This will further contribute to an increase in infrastructure exports as a Japanese specialty industry. Professor Goto has the following to say about the advancement of research and development under this project.

"Since my days involved in research at NTT, I have had a strong commitment to deliverable results for technology development and activities that can be used to benefit industry. Stronger cybersecurity measures in Japan is a critical issue that should be addressed immediately. At the same time, these measures should be leveraged to improve the competitive advantage of our industries. We hope to proceed in an all-Japanese structure incorporating industry-academy-government resources while expanding beyond traditional industrial fences."

Research and Development Topics

1. Develop Core Technologies: Develop cybersecurity technologies for control system and communication system equipment and control networks

- Develop cybersecurity verification technologies for control and communication devices.
- Develop behavior-monitoring and analysis technologies for control systems, communication systems, and related networks.
- Develop defense technologies for control systems.
- Develop security verification technologies for IoT systems.

2. Develop Social Implementation Technologies: Create a shared platform for social implementation and cybersecurity capacity-building

- Design certification programs to verify whether developed cybersecurity functions are correctly implemented.
- Develop information-sharing platform technologies to bridge infrastructure vendors.
- Develop assessment and verification platform technologies for cybersecurity technologies applied to critical infrastructure.
- Develop cybersecurity capacity-building for security technologies, products, and for fully utilizing them in critical infrastructure fields.

Exit Strategies

☑ Ensure social implementation of research and development outcomes

Advance research and development for adopting critical infrastructure for the 2020 Tokyo Olympic and Paralympic Games. Structure a research and development program that results in the shortest path from research and development to social implementation.

☑ Develop measures to advance the spread of cybersecurity

Develop strong cybersecurity functions to incorporate into critical infrastructure across Japan. Encourage the creation of standards, specifications, safety evaluation methods and other certifications tailored to each industry. Promote the use of development outcomes. Contribute to global business by exporting technologies, products, and evaluation and verification services utilizing the results of this research and development.

We will conduct this project using an all-Japanese approach of industry-academy-government relationships, breaking through traditional fences in industry categories.

Driving industrial competitiveness through stronger cybersecurity capability

内閣府
Cabinet Office

Issued by: Director General for Science, Technology and Innovation
Date: December 2015