Cyber-security for Critical Infrastructure

Creating the Safest, Most Secure Social Infrastructure in the World

The threat of cyber-attacks has been growing in its frequency and severity over the past several years, and they have also begun to target critical infrastructure, including communications and broadcasting, energy, and transportation. 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 and quickly in an all-Japanese program to ensure cybersecurity for critical infrastructure.

Program Director

Atsuhiro Goto

Institute of Information Security
President

Profile

Atsuhiro Goto received his PhD from the 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 became a professor at the Institute of Information Security's Graduate School of Information Security in 2011, and has served in his present position since 2017. Dr. 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, and the Ministry of Defense.

Research and Development Topics

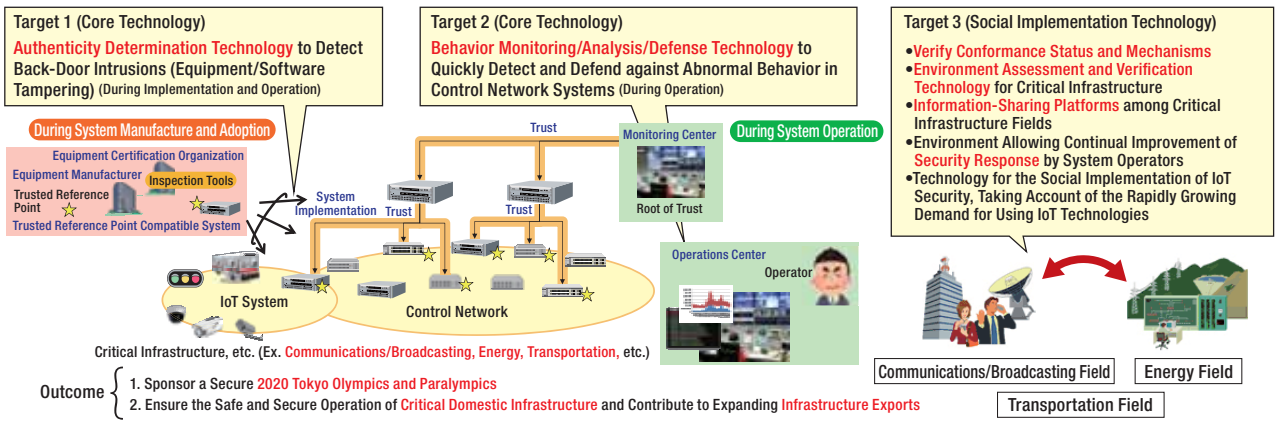
(a) Core Technologies: Develop cybersecurity technologies for control system and communication system equipment and control networks

- Authenticity determination technologies for control and communication systems (technologies to confirm the authenticity and integrity of devices and software).
- Behavior-monitoring and analysis technologies for control systems, communication systems, and related networks.
- Defense technologies for control and communication systems
- Security verification technologies for IoT systems.

(b) Social Implementation Technologies: Create a standard platform for social implementation and cybersecurity capacity-building

- Conformance test methodologies to determine whether developed cybersecurity functions are correctly implemented.
- Information-sharing platform technologies to bridge infrastructure operators.
- Assessment and verification platform technologies for cybersecurity technologies applied to critical infrastructure.
- Foster human resources capable of developing cybersecurity technologies, and capable of developing cybersecurity technologies, and capable of assessing and managing security technologies adopted for critical infrastructure systems.

•Cyber-security for Critical Infrastructure: Research and Development Structure



Exit Strategies

Ensure social implementation of research and development outcomes

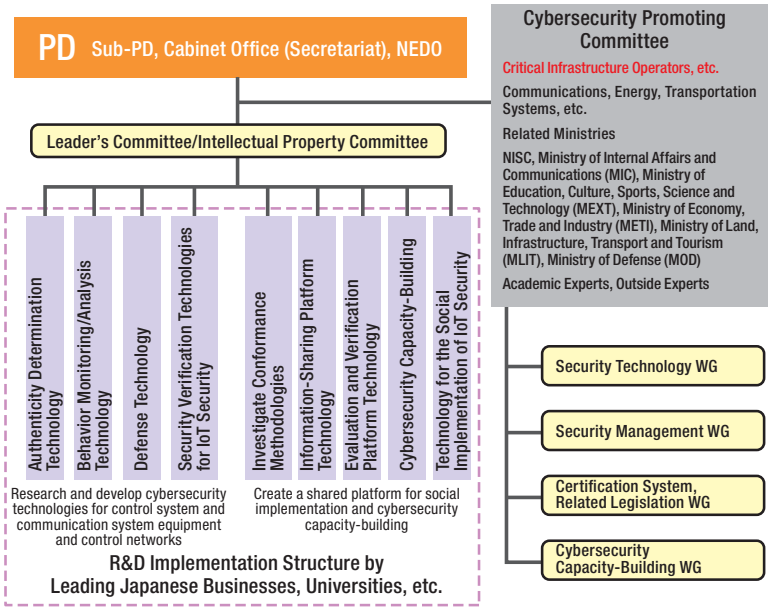
Advance research and development for adopting critical infrastructure for the 2020 Tokyo Olympic and Paralympic Games. Structure a research and development program that results in the shortest path from research and development to social implementation.

Develop strategies to deploy cybersecurity measures

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 sector. 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.

Implementation Structure

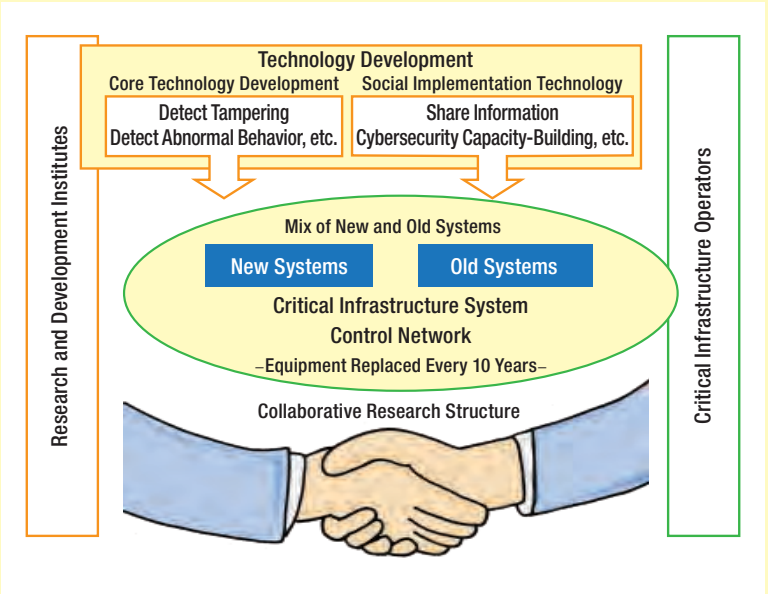
Research organizations engage in the development of core technologies and social implementation technologies under the guidance of the Cybersecurity Promoting Committee. The Committee consists of the Program Director (PD), Sub-PD, related ministries including the National center of Incident readiness and Strategy for Cybersecurity (NISC), academics, outside experts, and critical infrastructure operators. Four working groups (WGs) have been established for each of the research topics. In each working group, researcher and development professionals work closely with experts and representatives from critical infrastructure operators to establish a shared outlook and to better identify needs. This framework ensures that technical development conforms to the actual needs on the front lines.



Progress to Date

Promote Validation Tests with Critical Infrastructure Operators

Critical infrastructure operators have made requests for the early adoption of high-priority measures and evaluations within operator test environments. Based on these requests, validation for certain implementable technologies have been promoted. One example relates to behavior monitoring and analysis technology. Since late 2016, the program has promoted validation of effective monitoring and analysis within a critical infrastructure control system featuring a mix of old and new systems. These tests have also included technology capable of detecting cyber-attacks. The program is working in close coordination with critical infrastructure operators on human resources development. The agenda here is to establish a training curriculum attuned to actual work conditions.



Program Director **Atsuhiro Goto** Interview

Keeping Critical Infrastructure Safe and Secure During the Olympics/Paralympics and Beyond

Cyber-attacks threaten critical infrastructure that supports society. This program is engaged in an all-Japanese format to ensure cybersecurity for our nation, working closely with critical infrastructure operators.

Cybersecurity on the Eve of the Olympics and Paralympics

Cyber-attacks represent a real threat to social infrastructure, including communications and broadcasting, energy and transportation. Ensuring cybersecurity for critical infrastructure is an urgent issue not only in Japan, but also across the world. Dr. Atsuhiro Goto oversees this program, which marked its third year in fiscal 2017, and explains his new resolve.

"We see reports of cyber-attacks on critical infrastructure from all over the world. One example is the massive attack by Ransomware which caused damage in more than 100 countries in May 2017. On the eve of the 2020 Tokyo Olympics and Paralympic Games, we are increasingly aware of the need for this program. We can only achieve true cybersecurity when the core technology R&D has been integrated with social implementation technology. To achieve this goal, we must work hand-in-hand with industry and academia to push the program forward."

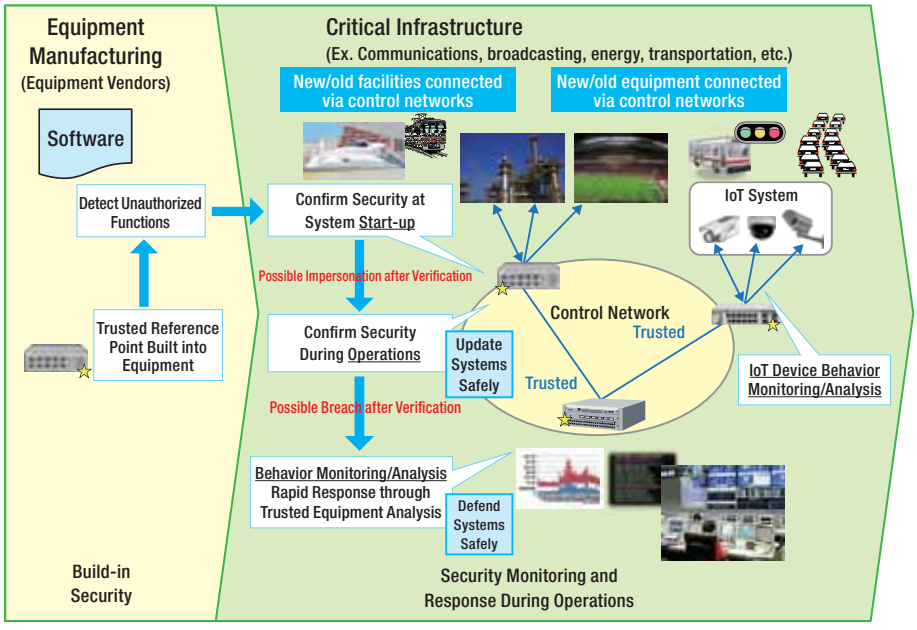
Implementation and Validation through Close Collaboration with Critical Infrastructure Operators

Dr. Goto stresses that one major success of the program has been collaboration with critical infrastructure operators to speed up social implementation, an endeavor that was begun in fiscal 2016. Says Goto, "By involving numerous infrastructure operators, we have set up a framework for R&D that tracks specific requests and suggestions from those on the front lines." This program has created an implementation structure capable of well-coordinated activities. The Promoting Committee consists of representatives from universities, research institutes, industry, and critical infrastructure operators. Working groups provide a mechanism to share issues, identify needs, and provide coordination to integrate technologies and systems across each research and development topic. Combined, this structure works toward social implementation for constituent technologies as quickly as possible.

Critical infrastructure operators have made requests for the early adoption of high-priority measures and for validation and evaluation to be conducted on the front lines. Based on these requests, validation for core technologies under development have been fast-tracked. One such example is in the field of behavior monitoring and analysis technology. Tests began in late 2016 to validate the soundness of critical infrastructure control systems that combine both old and new systems. At the same time, the program is working with critical infrastructure operators to validate attack-detection technologies.

Meanwhile, the program is advancing development of social implementation technologies, including a common social implementation platform and education for security professionals. Dr. Goto adds, "We plan to develop a security information sharing platform beginning in 2017

•System for Ensuring Cybersecurity



that spans critical infrastructure operators. As they use this platform, any needs or functions will be addressed promptly, leading to a gradual transition over time."

Japanese-made Security Technology: New Added Value for Critical Infrastructure

On the topic of training professionals in cybersecurity, Dr. Goto responded that the program is currently examining different training and education curricula for people who work on the front lines of this field. The program is working with critical infrastructure operators to produce real-world curricula.

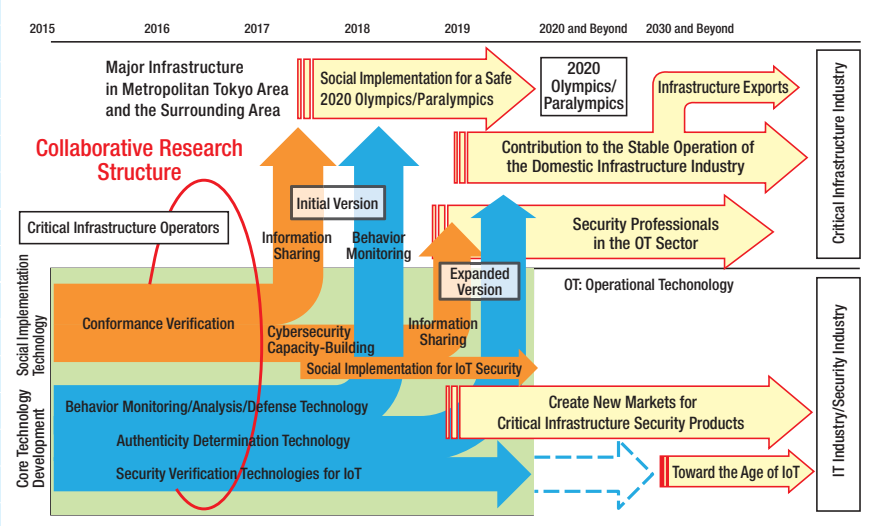
Says Goto, "Our first order of business is implementing practical cybersecurity for the rapidly approaching 2020 Tokyo Olympic and Paralympic Games. However, security technology is also important for supporting the upcoming Society 5.0. It is not enough to develop technologies that solve our immediate problems. We are also engaged in R&D that anticipates conditions 10 or 20 years after the program ends."

For that reason, the program will continue to respond to new forms of cyber-attacks and security vulnerabilities, preparing to further advance security technologies using AI and Big Data. Finally, Dr. Goto shared his outlook for the future.

"Japan's strengths lie in stable operations in the energy sector and reliable communication and transportation networks. Through this program, we plan to provide security as an added value to these critical infrastructures. We also hope to see the country export Japanese security technology, and by extension, safe and secure critical infrastructure, to the rest of the world."

Future Plans

In the run-up to the 2020 Tokyo Olympic and Paralympic Games, the program intends to leverage close ties between industry, academia, and critical infrastructure operators to produce results that lead to social implementation. The program will continue R&D activities to add value and enhance the competitiveness of critical infrastructure as a whole far beyond the year 2020.



By developing security as an added value, we will build a reputation of safety and security in Japan's critical infrastructure industry, strengthening the competitive posture of our nation.