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 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

President

Institute of Information Security

Profile

Atsuhiro Goto received his PhD from the University of Tokyo in 1984. Upon graduation, he joined NTT, 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 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

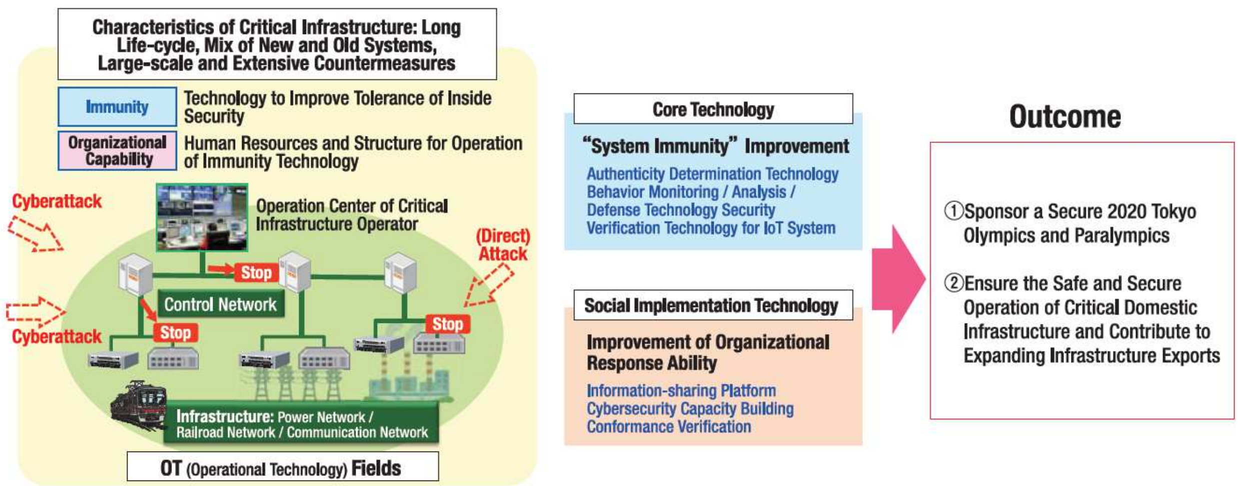
(a) Core Technologies: Develop cybersecurity technologies for control system and communication system equipment and control networks

- 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

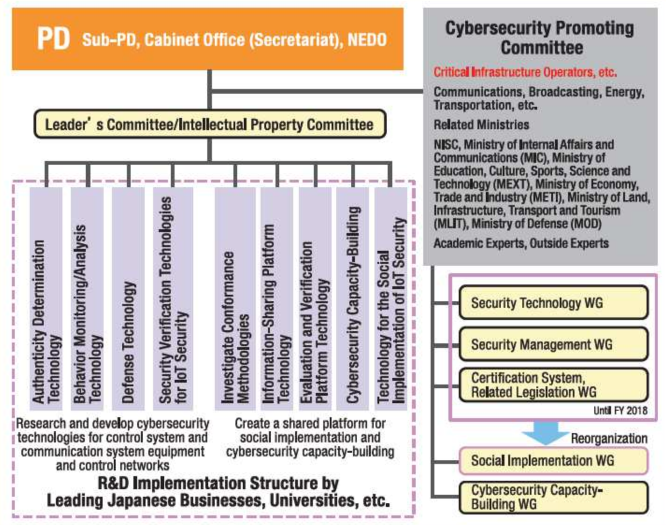
- Conformance test methodologies to promote spreading cybersecurity technologies.
- Information-sharing platform technologies to bridge infrastructure operators.
- Assessment and verification platform technologies for cybersecurity technologies applied to critical infrastructure.
- Foster human resources capable of developing cybersecurity technologies, and capable of assessing and managing security technologies adopted for critical infrastructure systems.

•Cybersecurity for Critical Infrastructure: Target and Overview of 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. 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.

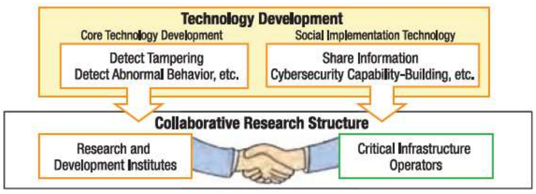


Progress to Date

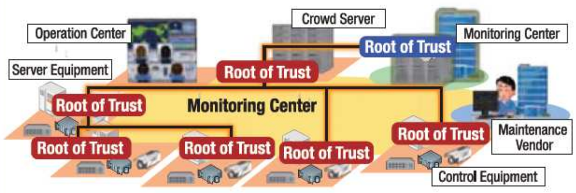
Realize Early Social Implementation through Collaborative Research Structure with Critical Infrastructure Operators

The project is based on a collaborative research structure established between research and development institutes and critical infrastructure operators. When the project started, there were detailed discussions about the development of relevant technologies with respect to their operation after implementation. 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. The program confirmed the effectiveness of technology that can detect security attacks within a critical infrastructure control system featuring a mix of old and new systems. The program productized the technology at the end of 2017.The program verifies security improvement by using authenticity determination technology and behavior monitoring and analysis technology under a test environment and in actual work conditions. The program is accelerating the implementation of relevant technology in critical infrastructure required to organize the 2020 Tokyo Olympic and Paralympic Games, safely.

•Collaborative Research Structure with Critical Infrastructure Operators



•Authenticity Determination Technology



Human skill development for critical infrastructure operators

On the topic of training professionals in cybersecurity, the program has formulated training and education curricula for people who work on the front lines of infrastructure operations. The program is working with critical infrastructure operators to produce real-world curricula and develop teaching materials. With the teaching materials, it is possible to gain concrete images of potential events at each workplace based on actual cases. Developed materials are distributed to many critical infrastructure operators for trial and provide educational courses using them to receive feedback from operators on a continuous basis and brash up curricula. The program aims for the social implementation of the curricula through their use in company employee training courses and human skill development courses of industrial organizations even after the completion of the project, and is currently considering the creation of a system for continuous update of teaching materials.