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

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

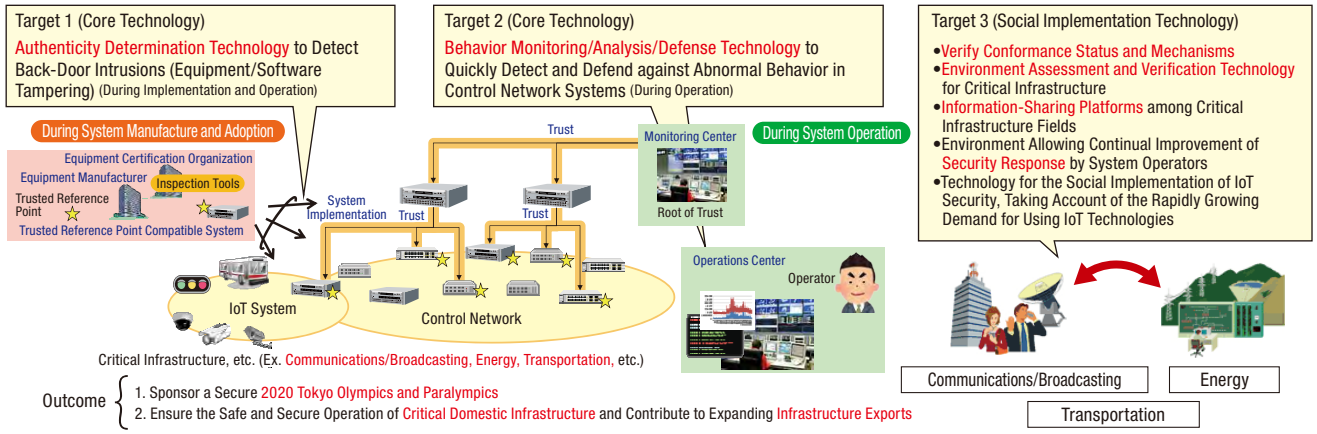
(a) Core Technologies: Develop cybersecurity technologies for control system and communication system equipment and control networks

- 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

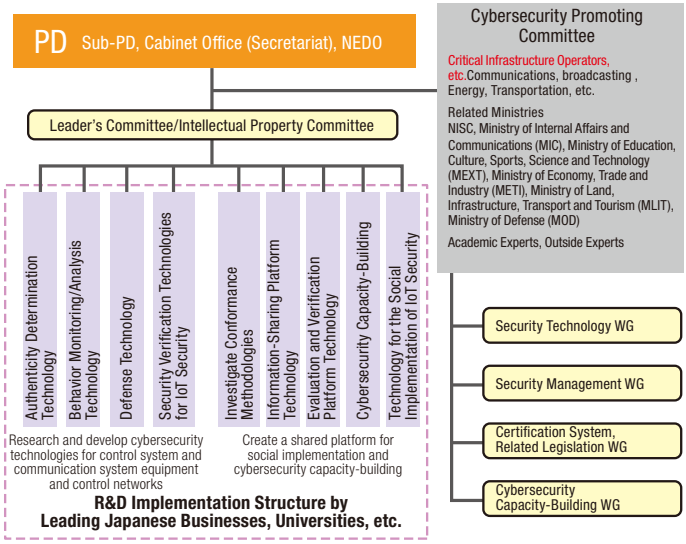
- Conformance test methodologies to promote spreading cybersecurity technologies.
- Information-sharing platform technologies to bridge infrastructure operators.
- Assessment and verification platform technologies for cybersecurity technologies applied to critical infrastructure.
- Foster human resources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

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



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.



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.

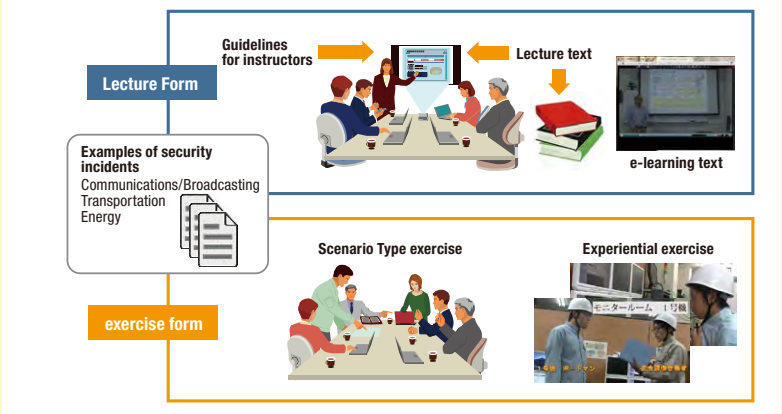
Develop strategies to deploy cybersecurity measures

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 and products utilizing the results of this research and development.

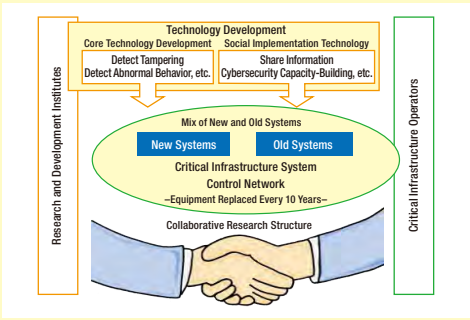
Progress to Date

Realize Early Productization through Validation Tests with Critical Infrastructure Operators

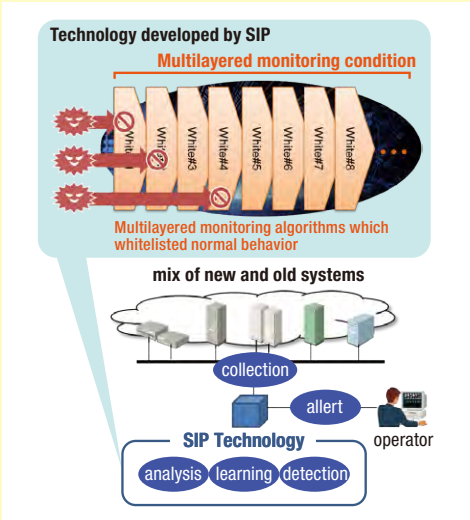
Critical infrastructure operators have made requests for the early adoption of high-priority measures and evaluations within operator test environments. Based on these requests, validation for certain implementable technologies have been promoted. One example relates to behavior monitoring and analysis technology. 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 is working in close coordination with critical infrastructure operators on human resources development. The program evaluates and improves the training curriculum formulated in line with actual work conditions.



•Human Skill Development for Critical Infrastructure operators



•Collaborative Research Structure with Critical Infrastructure Operators



•Enhanced Security Tolerance under Mix of New and Old System