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. Critical infrastructure including communications and broadcasting, energy, transportation, and so on has become 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.

Program Director

Atsuhiro Goto

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

Research and Development Topics

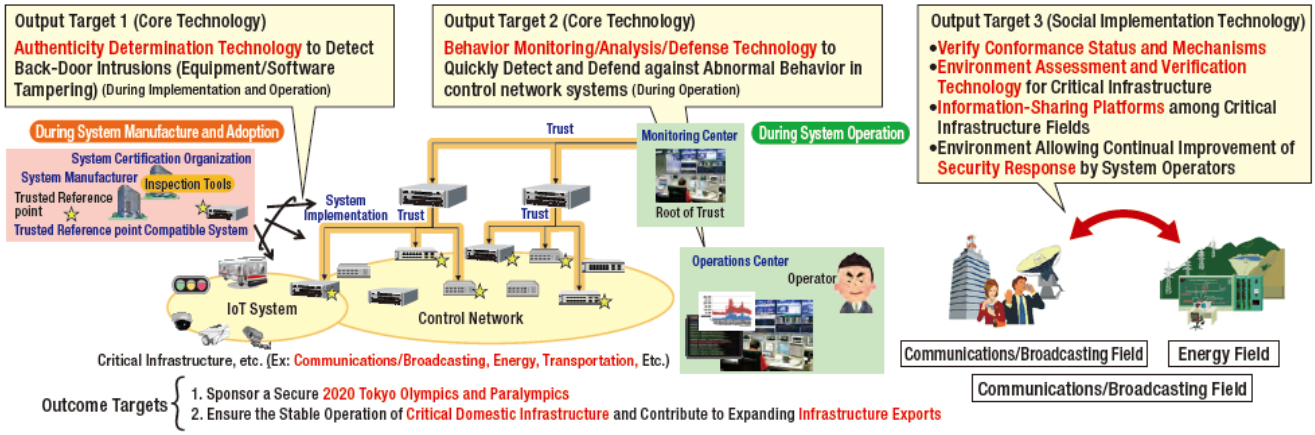
(a) Develop Core Technologies: Develop cybersecurity technologies for control system and communication system equipment and control networks

- Develop authenticity determination technologies for control and communication systems (technologies to confirm the authenticity and integrity of devices and software).
- 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.

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

- Investigate conformance status and mechanisms to determine whether developed cybersecurity functions are correctly implemented.
- Develop information-sharing platform technologies to bridge infrastructure operators.
- Develop assessment and verification platform technologies for cybersecurity technologies applied to critical infrastructure.
- Foster human resources 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

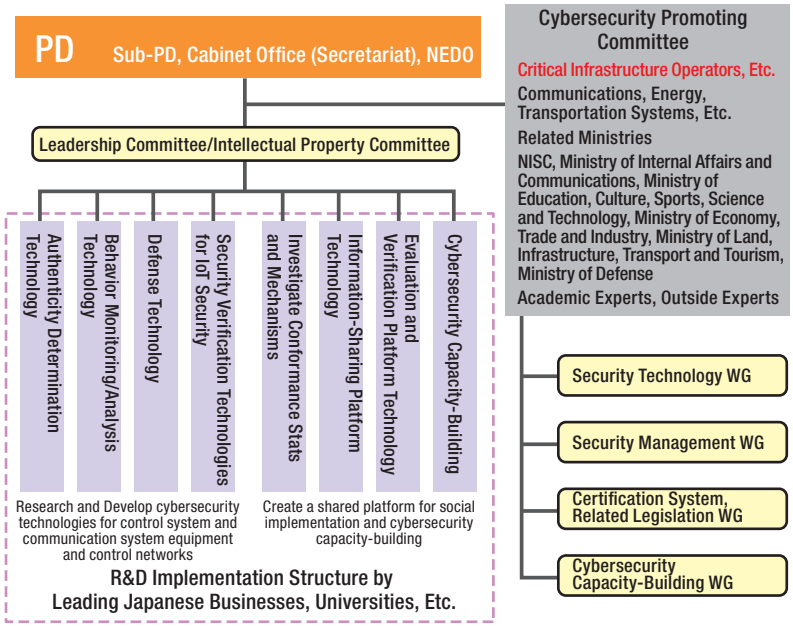
Advance research and development for adopting critical infrastructure for the 2020 Tokyo Olympic and Paralympic Games. Structure a research and development program that results in the shortest path from research and development to social implementation.

Develop 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 sectors. 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-directors (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 (WG) have been established for each of the research topics. In each working group, researcher and development professionals work closely with representatives from critical infrastructure operators and experts 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

Begin 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 fast-tracked. One example relates to behavior monitoring and analysis technology. The program plans to validate [technologies including] effective monitoring and analysis within a critical infrastructure control system featuring a mix of old and new systems. These tests will also include technology capable of detecting cyber attacks. These tests are scheduled to begin in late 2016. The program will work 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.