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

GOTO Atsuhiro

President

Institute of Information Security

* The affiliation and title of PD shall be as of the end of the 1st period (the end of FY2018).

Profile

GOTO Atsuhiro 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

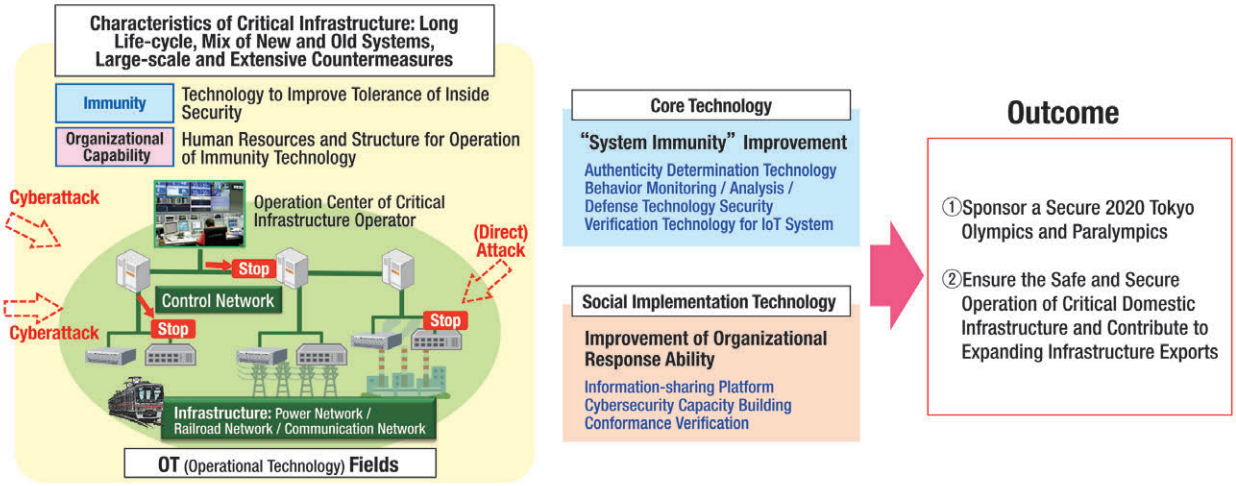
(a) Core Technologies: Develop cybersecurity technologies for control system and communication system equipment and control networks

- 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

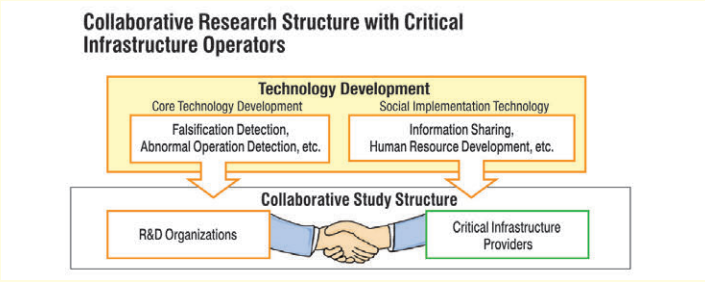
- Conformance test methodologies to promote spreading cybersecurity technologies.
- Information-sharing platform technologies to bridge infrastructure operators.
- Assessment and verification platform technologies for cybersecurity technologies applied to critical infrastructure.
- Foster human resources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

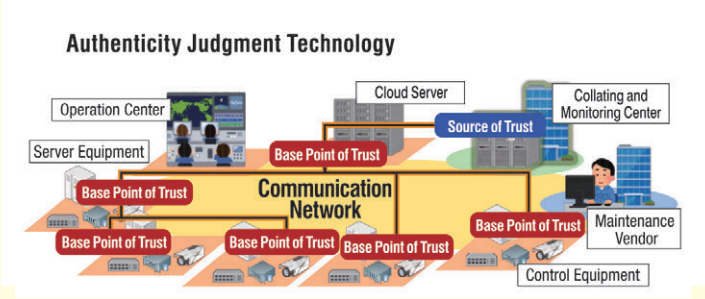
•Cybersecurity for Critical Infrastructure: Target and Overview of Research and Development



Early achievement of social implementation in critical infrastructure: genuineness determination technology and operation monitoring/analysis technology

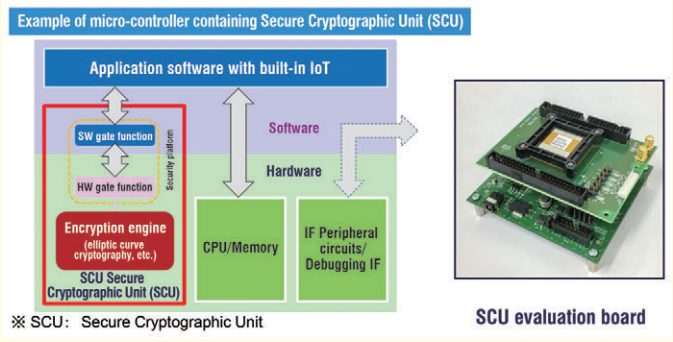
From the beginning of the project, we constructed a co-operative examination system through R&D institutes and critical infrastructure providers at the very outset and had many discussions. Then we conducted technology development being aware of operation after implementation. We promoted actual verification of some technologies that can be implemented antecedently based on demands from critical infrastructure providers such as "early introduction of high-priority measures" and "assessment in the verification environment of providers". One example of this is operation monitoring/analysis technology we confirmed the effectiveness of the technology to effectively detect security attacks in a critical infrastructure control system where old and new facilities are mixed, and it was commercialized at the end of 2017. We also verified improvement of security making use of the authenticity judgment technology and active monitoring/analysis technology not only in a verification environment but also in an actual operation environment, and implemented it at critical infrastructure facilities that would support the opening of a safe Tokyo Olympic and Paralympic Games.





Establishment of cryptographic implementation technology ensuring IoT security

We developed a Secure Cryptographic Unit (SCU) implementing the latest public key encryption function to utilize public key encryption freely and ensure security even at a terminal node with little resource considering future IoT-ization of critical infrastructure at an early stage. We have already achieved the performance targets (world's smallest, lowest power consumption and fastest) and established the technologies that enable production of a very small Secure Cryptographic Unit compared with security chips available in global markets. We will create guidance documents to promote popularization of these technologies to continuously broaden their implementation base.



Human resource development for fostering practical skills for critical infrastructures

As for human resource development related to cyber security, together with the critical infrastructure providers, we examined what educational menus are really needed for the people in charge of operating critical infrastructures in actual fields, and designed more practical curriculums and developed educational materials. By using the developed educational materials, the learners will be able to clearly picture actual situations on site based on the examples of actual incidents. We distributed the educational materials to many critical infrastructure providers as a trial and improved them by offering educational courses using them and receiving continuous feedbacks from the providers. We established the system to constantly update the educational materials, aiming at them being used at employee training courses of companies or human resource development courses of business organizations so that the lessons learned are socially implemented even after completion of the project.