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 cyber security 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 communications and broadcasting, energy, and transportation infrastructure. Ensuring cybersecurity for critical infrastructure is an urgent issue not only in Japan, but also across the world. Professor Atsuhiro Goto, now in his second year overseeing the program, explains his new resolve.

"We see reports of cyber attacks on critical infrastructure from all over the world. One such attack caused a major power outage in Ukraine at the end of 2015. 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."

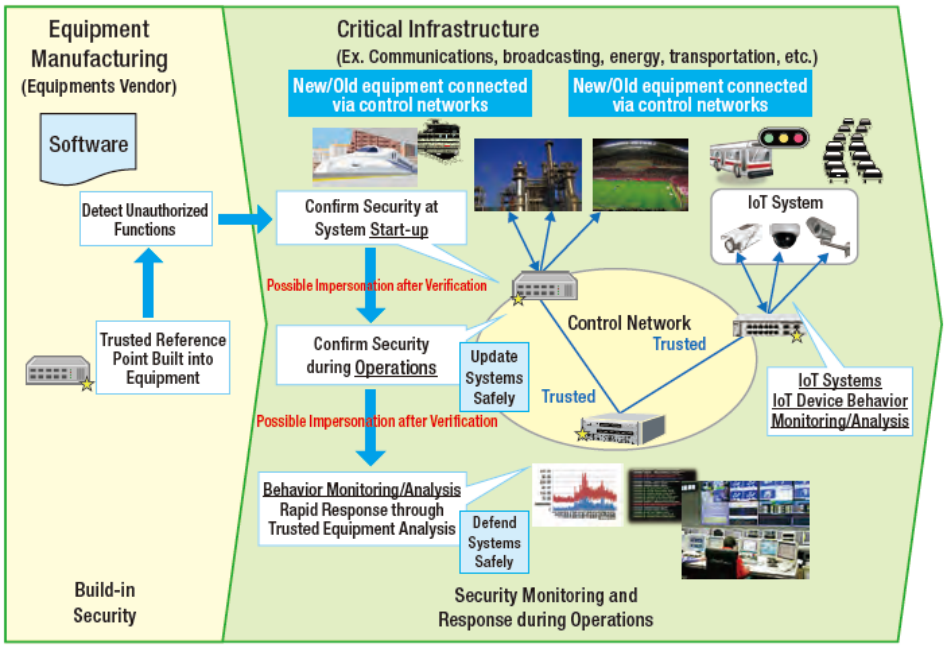
Implementation and Validation through Close Collaboration with Critical Infrastructure Operators

Prof. Goto stresses that one major success of the program has been speeding social implementation with the cooperation of critical infrastructure operators. 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 evaluations within operators test environments. 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 are scheduled for late 2016 to validate the soundness of critical infrastructure control systems that combine both old and new systems. At the same time, the program will work 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. Prof. Goto adds, "We plan to develop a security information sharing platform beginning in 2017

•Research and Development Concept Overview



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, Prof. 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 on to produce real-world curriculum.

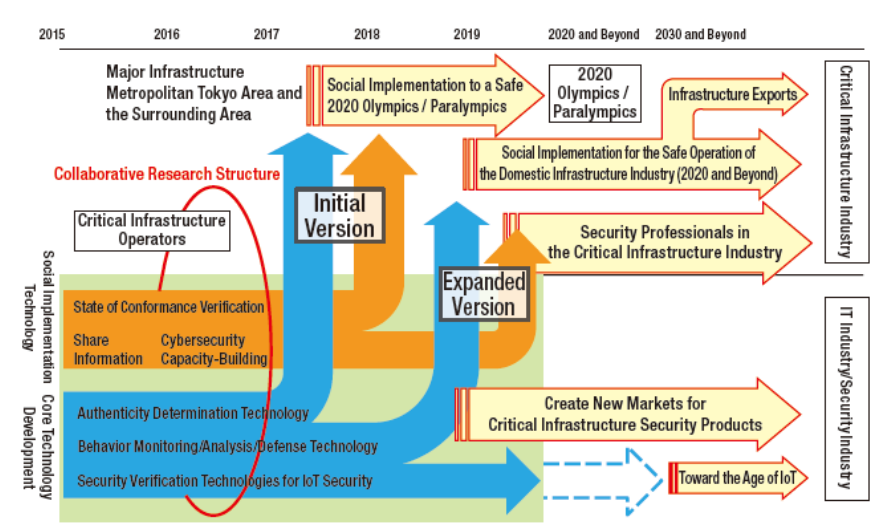
Says Goto, "Our first order of business is implementing practical cyber security for the rapidly approaching the 2020 Tokyo Olympic and Paralympic Games. However, security technology is also important for supporting the upcoming Society 5.0. It is not enough to develop technologies that solve our immediate 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, Prof. 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 the security as the added value of security to these critical infrastructures. We also hope to see the country export Japanese security technology, as well as the resulting 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 enhance the added value and 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.