Cross-ministerial Strategic Innovation Promotion Program (SIP)

Cybersecurity for Critical Infrastructure

Goal of R&D

To establish the world's safest and most secure social infrastructure by maintaining robust cyber security against cyber attacks to critical infrastructures or other systems that support the daily lives of people and socio-economic activities.

Background of the R&D

◆ The threat of cyber attacks has surfaced against the control network systems of critical infrastructures or other systems.

In Ukraine, a power outage affected 1.4 million households, which required six hours for recovery.

◆ Critical infrastructures would be most targeted in Japan where Olympics and Paralympics games will be held in 2020.

Characteristics of Control Network Systems

◆ Service continuity FIRST

Focus more on availability and integrity than on confidentiality.
Tend to minimize the application of security patches or other updates.

◆ Device life cycle are dozens of years

Old and new devices introduced in different years coexist.

Situation of Control Network Systems

◆Same risks as in information networks

- Connection with information networks through a variety of routes
- Data and information exchanged online as well as offline
- Use of generic devices and open standard protocols

◆ No effective measures against existing risks

- Replacement of devices/software by malicious insiders during manufacturing through installation (supply-chain risk) and during maintenance and operation

◆ Following of technology trends

- Adoption of an explosive number of (powerless) IoT devices
- Use of virtualization technology

◆ Advancement and sophistication of cyber attacks

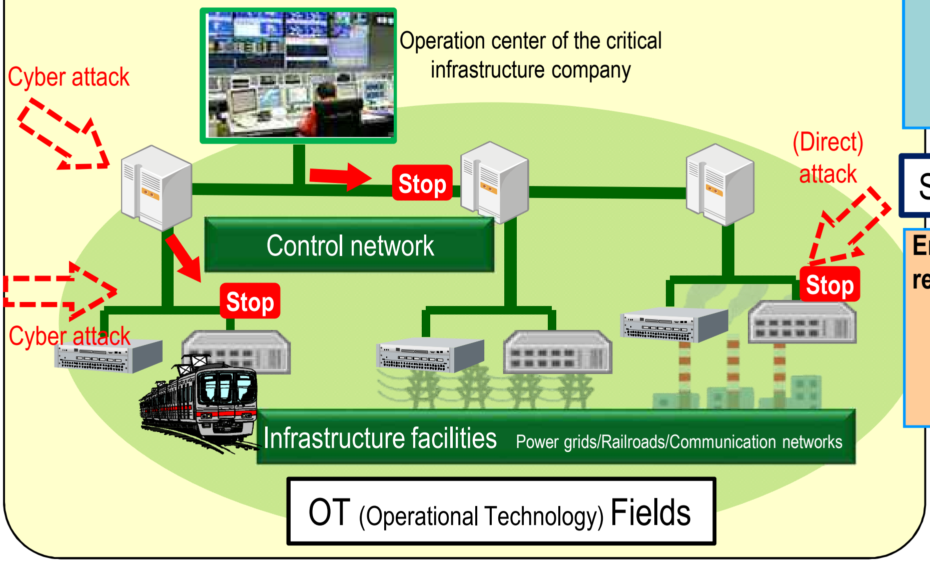
- Information-sharing among critical infrastructure fields
- Development of human resources capable of assessing and managing security technologies adopted for critical infrastructure systems

Initiatives in SIP

Measures in accordance with the characteristics of critical infrastructure facilities: long life; old and new facilities mixed; large scale and wide area

Immunity in system — **Technology enhancing the security resistance inside the facilities**

Organizing ability — **System and human resources that can use immune technologies on their own**



Operation center of the critical infrastructure company
Cyber attack
Stop
(Direct) attack
Control network
Stop
Cyber attack
Stop
Infrastructure facilities Power grids/Railroads/Communication networks
OT (Operational Technology) Fields

Core technologies

Enhancement of "system immunity"

Authenticity determination technology
Operation monitoring and analysis/Defense technology
Encryption implementation technologies for IoT

Social implementation technologies

Enhancement of organizational capacity to respond to issues

Information-sharing platform
Human resources development for security
Conformance Verification

Cross-ministerial Strategic Innovation Promotion Program(SIP)

Cybersecurity for Critical Infrastructure

Initiatives by SIP

1. Enhancement of the Security (Immunity) of the Control Network Systems

Authenticity determination technologies	1-1 Protection of Critical Infrastructures by Continuous Monitoring of Unauthorized Changes to the Server Devices - Continuous Monitoring of unauthorized changes to the systems prevents abnormal behavior, such as backdoor communications	NTT
Operation monitoring and analysis technologies	1-2 Minimize Impact on Businesses by Revealing Intrinsic Threats in Early Stages - Support highly skilled operations that reveal, in early stages, intrinsic threats slipped through the existing security measures and monitor and analyze such threats.	Fujitsu
	1-3 Enhancement of Security Resistance of the Control System by Early Detection of Intrusion/Attacks - Detects unauthorized operation that is hard to detect in the control system where availability is considered important.	Hitachi
	1-4 System Defense Technologies That Enables Safe Operational Continuity Even When an Abnormality is Detected - Protects the entire control system from hard-to-detect sophisticated attacks for safe operational continuity.	ALAXALA CSSC

2. Technologies for Security Measures Ahead of the Growth of IoT Systems

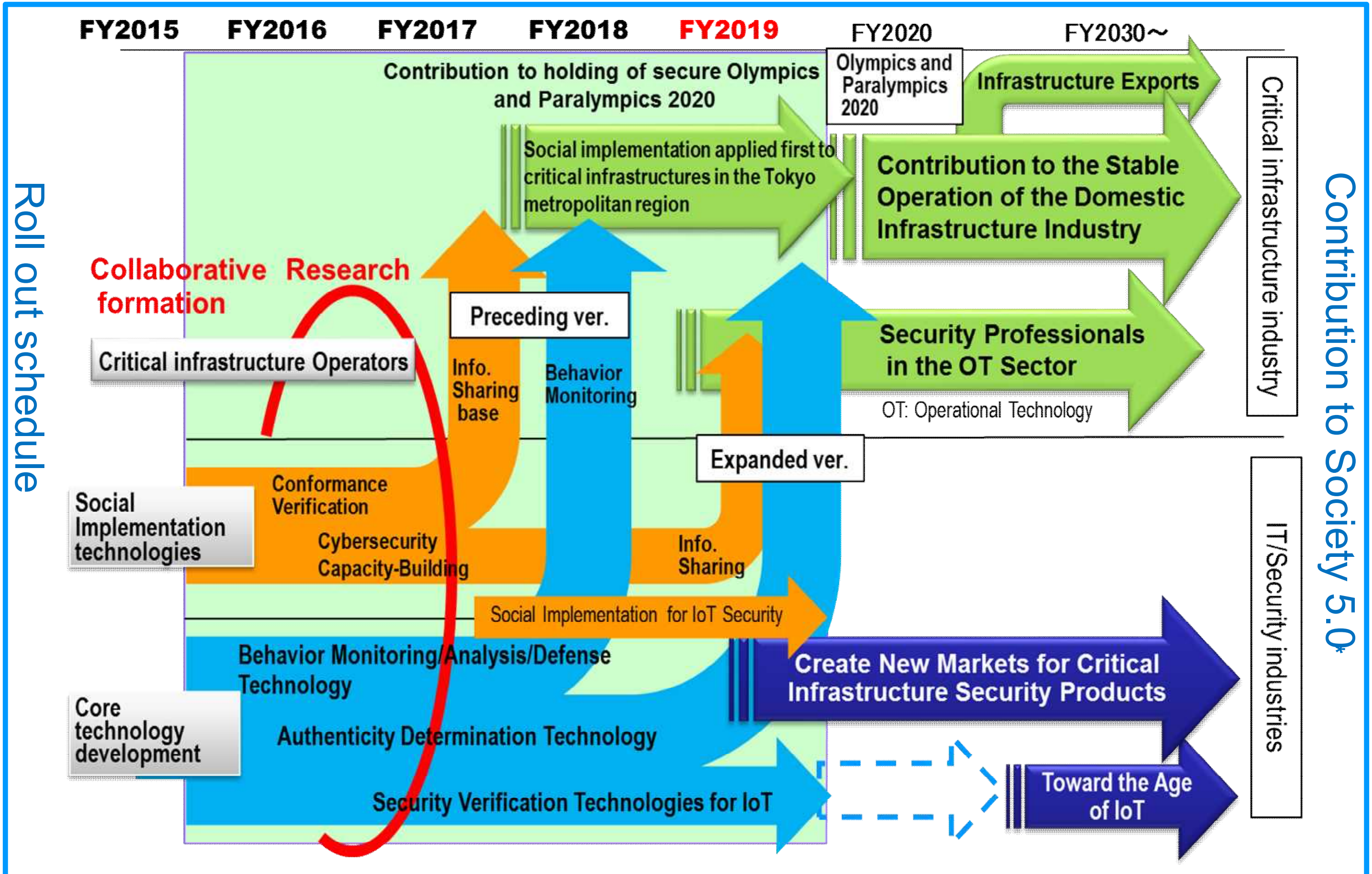
Technologies for IoT	2-1 Security Monitoring Equipment for IoT Systems - Automatic adjustment to a variety of IoT devices to monitor and analyze operations of them for detecting security anomalies	Mitsubishi Electric NTT
	2-2 Implementation Technologies of Ultra-Low Power Public-Key Cryptography That Achieves IoT Security - Public-key cryptography anywhere! Secure Cryptographic Unit	ECSEC Renesas Electronics
	2-3 Total Cyber Security With *Defense*, *Detection*, and *Measures* for Protecting End Points - Secure cryptographic/authentication function achieved by generating cryptographic/authentication key from seeds with less risk of being guessed within IoT devices	Panasonic

3. Enhancement of Organizational Ability and Creation of Framework for Ensuring the Security of Critical Infrastructures

Social Implementation technologies	3-1 R&D on How to Check the Conformance for Promoting Social Implementation of R&D Technologies - Consideration of the framework for conformance checking with which social implementation can be achieved more effectively and rapidly than ever before	AIST
	3-2 Protection for Critical Infrastructure Companies by Rapidly Distributing Information on a Very Urgent Threat - Rapid distribution of threat information in a standard format which enables machine-processing ; Development of an information sharing system to protect critical infrastructure companies as early as possible	Hitachi
	3-3 Developing Security Human Resources for Acquiring Practical Skills in Critical Infrastructures 3-4 Programs of Human Resource Development for Improving Organizational Incident Response Ability	Keio University Nagoya Institute of Technology

Cross-ministerial Strategic Innovation Promotion Program (SIP)

Cybersecurity for Critical Infrastructure



Roll out schedule

FY2015 FY2016 FY2017 FY2018 FY2019 FY2020 FY2030～

Collaborative Research formation

Critical infrastructure Operators

Social Implementation technologies

Core technology development

Contribution to holding of secure Olympics and Paralympics 2020

Social implementation applied first to critical infrastructures in the Tokyo metropolitan region

Preceding ver.

Info. Sharing base

Behavior Monitoring

Conformance Verification

Cybersecurity Capacity-Building

Expanded ver.

Info. Sharing

Social Implementation for IoT Security

Behavior Monitoring/Analysis/Defense Technology

Authenticity Determination Technology

Security Verification Technologies for IoT

Olympics and Paralympics 2020

Infrastructure Exports

Contribution to the Stable Operation of the Domestic Infrastructure Industry

Security Professionals in the OT Sector

OT: Operational Technology

Create New Markets for Critical Infrastructure Security Products

Toward the Age of IoT

Critical infrastructure industry

IT/Security industries

Contribution to Society 5.0*

*Society 5.0: A human-centric society that balances economic advancement with the resolution of social problems by realizing the advanced fusion of cyberspace and physical space
From the *5th Science and Technology Basic Plan* (Approved by the cabinet on January 22, 2016)