Cross-ministerial Strategic Innovation Promotion Program (SIP)
Cyber-security for Critical Infrastructure

Goal of R&D:
Ensuring strong cybersecurity against the threats of cyber-attacks on critical infrastructure that support the lives of citizens and socio-economic activity creates the safest and most secure social infrastructure in the world.

Background of R&D

- Threats of cyber-attacks on control network systems of critical infrastructure have manifested
  - In the Ukraine, it took 6 hours to have power restored after a blackout
    - 1.4 million households were affected
  - Critical infrastructure is the target of cyber-attacks in Japan where the 2020 Olympics/Paralympics are held

Characteristics of Control Network Systems

- Emphasis on service continuity
  - More emphasis on Availability and Integrity than Confidentiality
  - Security patches are minimal
- Life cycle measured in tens of years
  - New and old devices that were installed at different times are used together

Current State Surrounding Control Network Systems

- Same risks as in information networks
  - Connection with information networks through a variety of routes
  - Data and information exchanged online
  - Use of generic devices and standard protocols
- Current risks for which there are no effective countermeasures
  - Device/software replacements caused by or internal crime and the like during manufacturing and construction (supply chain link) or during maintenance or operation

Initiatives in SIP

Security countermeasure technologies of control network systems

- Authentication determination
- Behavior monitoring analysis/defense

- Measures for replacing devices/software (1-1)
- Use of new and old devices together, virtualization technologies (1-2a, 1-2b)
- Guaranteeing availability even in the event of a cyber-attack (1-3)
- Strengthening of security of dynamic map (database) infrastructure
- Coordination between SIP programs (additional topic)

⇒ Can also handle new cyber-attacks by utilizing the latest AI technologies

Security countermeasure technologies preceding the spread and expansion of IoT systems

- The use of new and old devices together, the explosive increase in IoT devices (2-1)
- Defenseless IoT devices (2-2), (2-3)

Social implementation technologies for assuring the cybersecurity of critical infrastructure

- Forms of checking compatibility for promoting the social implementation of research and development results (3-1)
- Mechanism for promoting information sharing (3-2)
- Development of human resources for cybersecurity (3-3)

Contribution Roadmap to Social Infrastructure

Contributions toward Society 5.0:
A human-centered society for economic development and solving social problems, through the high-precision fusion of cyberspace and physical spaces

Source: “Comprehensive Strategies on Science, Technology, and Innovation for 2016” (decided by the Cabinet on May 24, 2016)
Roadmap of Market Development

With contributions to the Olympic Games as a opportunity, this program will provide a platform that supports the improvement of cybersecurity inside Japan, with a focus on operators of critical infrastructure. The aim will be to spread this platform to corporations and places outside of Japan in the future.

- **Trusted Operational Platform for Cybersecurity (TOP)**
  - **Global Reach**
  - **2020**
  - **2025**
  - **2030 and on**
  - **Y**
  - **(1) Energy, transportation, telecommunications**
  - **(2) Energy, transportation, telecommunications**
    - (select operators)
  - **(3) Critical infrastructure operators (13 fields)**
  - **(4) Corporations**
  - **(5) Abroad**

**The Plan (planned from January 2016–2019)**

**Core technologies**
- Authenticity determination technology
- Behavior monitoring/analysis/defense technologies
- Encryption implementation technologies for IoT

**Social Implementation Technologies**
- Forms of checking compatibility
- Information sharing
- Evaluation verification
- HR development

**Cross-ministerial Strategic Innovation Promotion Program (SIP)**

**Cyber-security for Critical Infrastructure**

- **Global Reach**
  - **Trusted Operational Platform for Cybersecurity (TOP)**
  - Provides all the stages from technology, deployment, operation procedures, to staff for cybersecurity as a set
  - Provides a framework capable of being an outlet for excellent security technology and knowhow inside and outside Japan

**Authenticity determination technology**
**Behavior monitoring/analysis/defense technologies**
**Encryption implementation technologies for IoT**
**Forms of checking compatibility**
**Information sharing**
**Evaluation verification**
**HR development**