Cybersecurity Guidelines for Commercial Space Systems

Ver. 1.1

March, 2023

Space Industry Office, Manufacturing Industries Bureau,

Ministry of Economy, Trade and Industry (METI)

Table of contents

1. Introduction

1.1 Background and Purpose of the Development of the Guidelines

(1) Background 1: Increasing cybersecurity risks in enterprises

In recent years, with the spread of digital technology such as AI, IoT, and big data, "digital transformation (DX)" initiatives that go beyond utilizing IT for business to bring radical transformation in business models, organizations, operations, corporate culture, and climate to realize customer value based on digital technology, and lead to new growth and enhanced competitiveness, are being promoted on a global level. Under these circumstances, companies are required to rapidly promote DX to maintain and strengthen competitiveness.

However, the impact of damage caused by cyberattacks on physical space is increasing due to the fusion of cyberspace and physical space, resulting from the growing use of and dependence on digital technology. In fact, many cyberattacks on control systems, such as those of power systems, petrochemical and automobile plants, building systems, and on vulnerable IoT devices in physical space have already been identified. Moreover, cyberattacks are taking place through multiple entry points, and a number of cyberattacks targeting weak points in the supply chain have been identified, such as attacks on cloud services, attacks targeting open source software (OSS), which increasingly used by enterprises, and attacks targeting group companies, overseas offices, and business partners. In addition to cases of suspected state involvement, these cyberattacks include many cybercrimes such as theft of information and intellectual property by organizations, groups, and individuals for financial gain, ransom demands (ransomware) through file encryption, information leakage through phishing, and unauthorized mining of cryptographic assets by crypto-jacking, which target all enterprises, including small and medium-sized enterprises.

As described above, the targets and starting points of cyberattacks are expanding with the growing use of digital technology, and their impact is directly linked to the risk of information leakage and theft of intellectual property, such as personal information and trade secrets in cyberspace, as well as to various management risks such as the risk of business shut down due to system downtime in physical space, the risk to human life and safety, risk of damages to assets, and reputation risk, etc. In other words, there is an increasing need for management to consider cybersecurity risks as a company-wide issue and implement measures by demonstrating leadership. In December 2020, the Ministry of Economy, Trade and Industry also issued a caution to management in the wake of recent cyberattacks to encourage the further strengthening of cybersecurity efforts. [1]

[1]Ministry of Economy, Trade and Industry: "Cautions to Corporate Managers Cybersecurity in Light of Situations of Recent Cyberattacks" (December 2020)
https://www.meti.go.jp/press/2020/12/20201218008/20201218008-2.pdf (in Japanese)

(2) Background 2: Growing cybersecurity risks in space systems

In the space sector, more than 90 security incidents occurred both inside and outside Japan between 1986 and 2022. Also, over 6,000 cyberattacks including phishing and malware were detected by the National Aeronautics and Space Administration (NASA) from 2017 to 2020. [2]

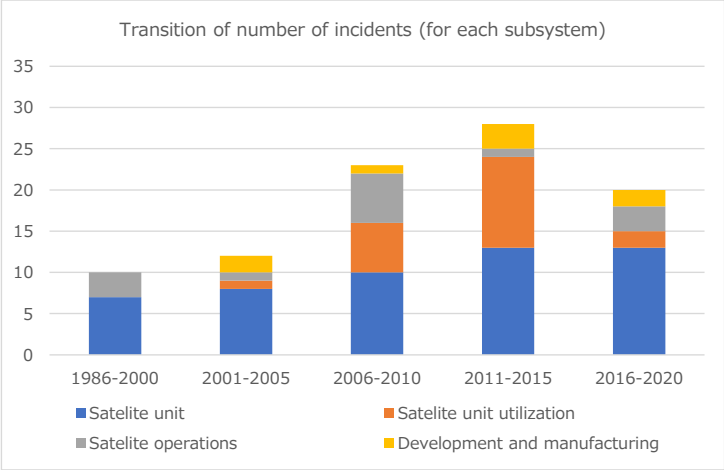


Figure 1-1 Number of domestic and international incidents in the space sector[3]

The following items are the main factors making cybersecurity for space systems critical and challenging:

- Extending roles of space systems in Japan's security, economy, and society
- Spread of digital technology, including unmanned and automated space systems and increased use of cloud services
- Increasing complexity of networks, including an increase in inter-satellite communication and connections between satellites and ground communication networks
- Increase in the number of satellites, ground stations, and data volume due to satellite constellations
- Diversification of stakeholders and complexity of supply chains resulting from the opening-up of technology for space systems to the commercial and incorporation of consumer technology

[2] NASA Office of Inspector General/Office of Audits: "NASA'S CYBERSECURITY READINESS" (May 2021) https://oig.nasa.gov/docs/IG-21-019.pdf
[3] Created based on various public information

(3) Background 3: Major overseas trends related to space system cybersecurity

Under these circumstances, initiatives by the national and commercial sectors on cybersecurity measures for space systems are gaining momentum in the United States and other foreign countries.

Table 1-1 Cybersecurity related initiatives for space systems in the U.S. and other foreign countries

Date	Subject	Initiatives
July 1990	National sector	NSD-42 "National Policy for the Security of National Security Telecommunications and Information Systems", was issued.
July 1990	National sector	The National Security Telecommunications and Information Systems Security Committee (NSTISSC) was established based on NSD-42.
October 2001	National sector	NSTISSC was designated as the Committee on National Security Systems (CNSS) by Executive Order 13231 "Critical Infrastructure Protection in the Information Age". CNSS consists of the Department of Defense (DoD), Central Intelligence Agency (CIA), Defense Intelligence Agency (DIA), Department of Justice (DOJ), Federal Bureau of Investigation (FBI), National Security Agency (NSA) and National Security Council (NSC).
June 2005	National sector	The Department of Defense issued DoDI 8581.01 "Information Assurance (IA) Policy for Space Systems Used by the Department of Defense" (revised June 2010).
March 2007	National sector	In response to NSD-42, CNSS issued CNSSP 12 "National Information Assurance Policy for Space Systems Used to Support National Security Missions". (January 2012 revised, February 2018 revised)
February 2009	National sector	In response to NSD-42, CNSS issued CNSSP 22 "Information Assurance Risk Management Policy for National Security Systems". (Revised January 2012, Revised August 2016, to Cybersecurity Risk Management Policy)
March 2012	National sector	In response to NSD-42, CNSS issued CNSSD 505 "Supply Chain Risk Management (SCRM)" (revised July 26, 2017).
January 2017	Commercial sector	Aerospace Corporation explained how satellite owners should comply with DODI 8581.01 and CNSSP 12, in "NAVIGATING THE POLICY COMPLIANCE ROADMAP FOR SMALL SATELLITE".
August 2018	Commercial sector	The "No Encryption, No Fly" rule was proposed at the American Institute of Aeronautics and Astronautics (AIAA) Small Satellite Conference.
April 2019	National and commercial sectors	Establishment of the Space Information Sharing and Analysis Center (Space ISAC). (Launched by NASA, the US Space Force, and US National Reconnaissance Office.)
April 2019	Commercial sector	The Orbital Security Alliance (OSA) announced "Big Risk in Small Satellites."
February 2020	National sector	Executive Order 13905 "Strengthening National Resilience Through Responsible Use of Positioning, Navigation, and Timing Services", was issued. A document on security profiles related to PNT services (NISTIR 8323) was issued in February 2021.

Date	Subject	Initiatives
May 2020	National sector	UKSA (UK Space Agency) issued “Cybersecurity Toolkit Ver. 2” for space asset owners and suppliers of goods to the space industry.
May 2020	Commercial sector	OSA issued the “Commercial Space System Security Guidelines” led by the commercial sector.
September 2020	National sector	Executive Order SPD-5 “Cybersecurity Principles for Space Systems” (including points such as the necessity for space systems to be designed and developed taking into account attacks by malicious cyber activity; protection of ground systems, operation technology, and information processing systems, etc.) was issued.
May 2021	National sector	The Department of Homeland Security (DHS) established a WG as a trial process to examine whether it is necessary to add space systems to sixteen critical infrastructure sectors.
February 2022	National sector	NIST created NISTIR 8270 (2nd Draft) “Introduction to Cybersecurity for Commercial Satellite Operations”, an introduction to security for commercial satellite operations.
March 2022	National sector	CISA and FBI announced AA22-076A “Alert (AA22-076A) Strengthening Cybersecurity of SATCOM Network Providers and Customers” (a security advisory summarizing mitigation measures and the relevant information on cyber-attack threats against international satellite communication networks).
April 2022	National sector	DHS updated the “DHS Space Policy,” a document describing the space policy with respect to homeland security.
May 2022	National sector	The US Space Force began trials of IA-Pre, “Infrastructure Asset Pre-Approval” (a preliminary security assessment program for commercial satellite communication services procured by the US DoD).
June 2022	National sector	The German Information Security Agency (BSI) announced the “IT-Grundschutz-profil für Weltrauminfrastrukturen” (Baseline cybersecurity measures for satellite systems).
August 2022	National sector	The German Information Security Agency (BSI) announced the “Cybersicherheit für Weltrauminfrastrukturen” (Cybersecurity strategy for space infrastructure).
October 2022	Commercial sector	US Aerospace Corporation announced, “Space Attack Research and Tactic Analysis (SPARTA)” which is an attack framework based on MITRE ATT&CK.
November 2022	National sector	NIST created CSWP 27 “Cybersecurity Profile for Hybrid Satellite Networks (HSN) Cybersecurity, Final Annotated Outline”.
November 2022	National sector	The European Council passed the “NIS2 Directive”, amending the “NIS Directive” (Network and Information Systems Directive). The space sector (operators of ground-based infrastructure, owned, managed, and operated by Member States or by private parties, which support the provision of space-based services, excluding providers of public electronic communications networks) was newly added to the sectors covered under this directive.
December 2022	National sector	NIST created NISTIR 8401 “Satellite Ground Segment: Applying the Cybersecurity Framework to Satellite Command and Control”, a document on security profiles for the satellite ground segment.

(4) Purpose of Creating the Guidelines

As mentioned above, as cybersecurity risks of space systems in enterprises are growing and discussions and initiatives are gaining momentum overseas, it was decided in the "Implementation Plan of the Basic Plan on Space Policy" (December 15, 2022) to develop guidelines for private companies on cybersecurity measures of space systems as part of enhancing the assurance of functionality for all space systems.

Since there are many space systems that are important for people's lives and security in Japan, with commercial operators playing a pivotal role, the guidelines aim to encourage commercial space operators to take voluntary measures for business promotion by summarizing and presenting the followings in an easy format:

- Security risks pertaining to space systems.
- Basic security measures that should be examined by each stakeholder involved in space systems.
- Reference literature that can be used as a reference and existing measures that can be used when examining the measures.

(5) Developing and Updating the Guidelines

The guidelines were developed using the following process:

- Discussions were held by the Space Industry Sub-Working Group (SWG) established under the Study Group for Industrial Cybersecurity WG1 (systems, technologies, and standardization).
- A working group composed of experts was set up under the Space Industry SWG to discuss technical issues.
- The following were used as the basic framework for the discussions.
  - ✓ "Cyber/Physical Security Framework (CPSF) Ver 1.0" (April 2019, Cybersecurity Division, Ministry of Economy, Trade and Industry)
  - ✓ "Security Risk Assessment Guide for Industrial Control Systems" (March 2020, Information-technology Promotion Agency)
  - ✓ The guidelines were developed while keeping in mind harmonization with JAXA, other industries, and overseas initiatives.

In Ver 1.1, a checklist of Requirements and Measures and a table of correspondence between the NIST CSF and countermeasures specific to space systems were added as Attachments 1 and 2, respectively, and other minor revisions were made. The guidelines will continue to be reviewed about once a year to incorporate the latest findings from Japan and overseas. Note that the references cited in the guidelines should be checked for the latest editions.

1.2 Scope of the Guidelines

The space systems covered by the guidelines are satellite systems and ground systems (satellite operation facilities, satellite data utilization facilities, development, and manufacturing facilities) operated by the commercial sector. The guidelines cover the design, development, manufacturing, operation, maintenance, and disposal phases of satellite systems. The guidelines focus mainly on the operation and maintenance phases for ground systems and describe the important points to be noted during each phase from system design to disposal. The launch facility is not covered by the guidelines.

Overall Space System

Space system			Operating entity
Space transportation system	Launch vehicle	Rocket	National sector
Manned system	Space station	Experiment building	National sector
Satellite system	Space probe	Lunar probe and planetary probe	National sector
	Transfer vehicle	Supply transfer vehicle	National sector
	Satellite	Positioning satellite	National sector
		Meteorological satellite	National / commercial sectors
		Communication satellite	National / commercial sectors
		Broadcasting satellite	Commercial sector
		Remote sensing satellite	National / commercial sectors
Ground system	Satellite operation facility	Tracking and control station, receiving station and mission control system, etc.	National / commercial sectors
	Satellite data utilization facility	Data processing systems, observation reception and data distribution processing, etc.	National / commercial sectors
	Launch facility	Launch site, launch control system, etc.	National / commercial sectors
	Development and manufacturing facility	OT system (FA system, etc.)	National / commercial sectors
		IT system (OA system, etc.)	National / commercial sectors

Scope of the Guidelines

Commercial space system		Phase to be covered in the lifecycle			
		Design, development and manufacturing	Launch	Operations and maintenance	Disposal
Satellite	Remote sensing satellite	✓	-	✓	✓
Satellite operation facility	Tracking and control station, receiving station and mission control system, etc.	-	-	✓	✓
Satellite data utilization facility	Data processing systems, observation reception and data distribution processing, etc.	-	-	✓	✓
Launch facility	Launch site, launch control facility, etc.	-	-	-	-
Development and manufacturing facility	OT system (FA system, etc.)	✓	-	✓	✓
	IT system (OA system, etc.)	✓	-	✓	✓

* Design, development and manufacturing phases include transportation, installation adjustment and testing but are not included in the scope of these guidelines.

Figure 1-2 Overall space system and the subject of the guidelines

For reference, the relationship between the satellite system life cycle and stakeholders has been summarized in Figure 1-3.

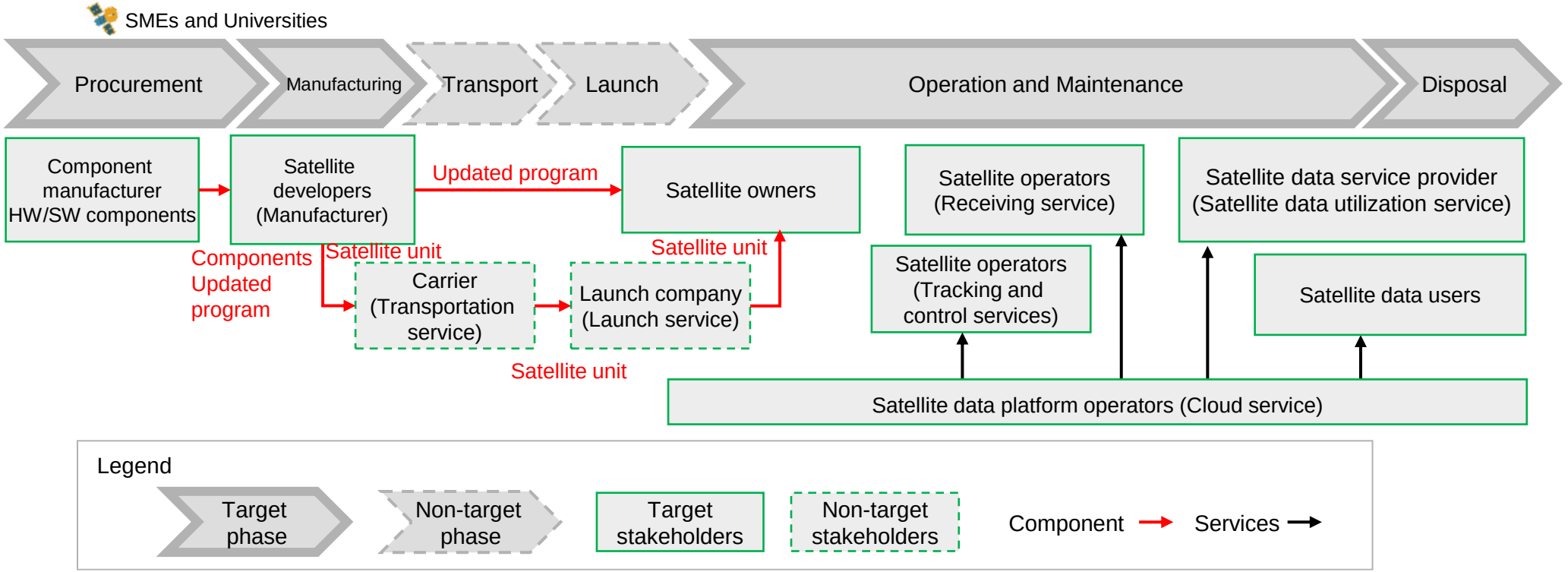


Figure 1-3 Overview of the relationship between satellite life cycle and stakeholders

In the guidelines, the standard model, risk scenarios, and measures for space systems in the commercial sector are organized by setting the operators of remote sensing microsatellites with active new entrants and their supply chains as analysis targets, but the guidelines can also be used when examining security measures for other satellite systems such as meteorological, communication, and broadcasting satellites. The scope of the guidelines shall be updated from time to time.

1.3 Structure of the Guidelines and Intended Readers

Table 1-2 shows the structure of the guidelines and intended readers.

The management of each operator should particularly refer to “1. Introduction” and “2. Cybersecurity Situation of Space Systems.”

Table 1-2 Structure of the guidelines and intended readers

	Satellite owners	Satellite operators*	Satellite data platform operators	Satellite data service providers	Satellite developers
1. Introduction					
1.1 Background and Purpose of the Development of the Guidelines	✔	✔	✔	✔	✔
1.2 Scope of the Guidelines					
1.3 Structure of the Guidelines and Intended Readers					
1.4 How to Use the Guidelines					
2. Cybersecurity Situation of Space Systems					
2.1 Incident Case Studies	✔	✔	✔	✔	✔
2.2 Concept of Cybersecurity Risks in Commercial Space Systems					
3. Key Points of Cybersecurity Measures for Commercial Space Systems					
3.1 Common Measures	✔	✔	✔	✔	✔
3.2 Specific Measures for Space Systems					
3.2.1 Measures Required by Law	✔	✔	✔	✔	✔
3.2.2 Satellite Unit	✔	✔			✔
3.2.3 Satellite Operation Facility		✔	✔		✔
3.2.4 Satellite Data Utilization Facility		✔	✔	✔	
3.2.5 Development and Manufacturing Facility		✔			✔

*: Includes ground station service providers providing tracking and control station services or receiving station services.

In “2. Cybersecurity Situation of Space Systems,” past incidents involving space systems and major security risks anticipated for space systems are summarized.

In “3. Key Points of Cybersecurity Measures for Commercial Space Systems,” Section 3.1 describes general common measures, and Section 3.2 describes security measures required for each subsystem (satellite unit, satellite operation facility, satellite data utilization facility, and development and manufacturing facility) as specific measures.

1.4 How to Use the Guidelines

The guidelines are intended for the following uses:

- Operators of the space industry use the guidelines as a reference for the cybersecurity measures.
- Governments, municipalities, and companies use the guidelines when procuring space systems to confirm whether the operators have taken basic cybersecurity measures.

Since the space systems and business environments vary, when examining measures, it is possible to tailor (custom) the measures described in the guidelines based on the characteristics and importance of the system to be examined, risk evaluation results, and the business environment of the operator. Also, when multiple stakeholders are considering common measures, the tailoring (customization) of the measures must be discussed, agreed upon, and approved by the stakeholders.

Attachment 1 of the guidelines includes a checklist summarizing Requirements and Measures, while Attachment 2 includes a table showing the correlation between the NIST Cybersecurity Framework (NIST CSF) and specific measures for space systems shown in 3.2.2 to 3.2.5 of the guidelines. Each Attachment should be used as a reference when considering the measures.

2. Cybersecurity Situation of Space Systems

2.1 Incident Case Studies

(1) Cybersecurity incidents of Space Systems

Over 90 cybersecurity incidents in the space sector occurred inside and outside Japan between 1986 and 2022. Some cases are shown below.

Table 2-1 Cybersecurity incidents in space systems (excerpts)[4]

Year	Target	Impact	Overview
2008	NASA Terra satellite	Lost control of satellite	Control over Terra, an earth observation satellite of NASA, was lost for several minutes due to interference with the satellite. The incident occurred twice, in June and October 2008. A report to the U.S. Congress indicated that a commercial ground station may have been the intrusion point, but the KSAT company denied the report.
2014	NOAA Meteorological observation NW	Satellite data could not be viewed	A meteorological observation satellite network of the National Oceanic and Atmospheric Administration (NOAA) was the target of a cyberattack through the Internet.
2015	Iridium Communication satellite	Communication contents became visible	A vulnerability was identified in an Iridium communications satellite where the pager communication data was not encrypted. A presentation at the international conference Chaos Communication Camp 2015 revealed how to analyze and decode the pager communication data of an Iridium communications satellite using commercially available antennas (costing about EUR 50) and convert it into plain text.
2018	NASA Jet Propulsion Laboratory (JPL)	Disclosure of mission data	A hacker gained unauthorized entry into the network of JPL using Raspberry Pi installed by a staff member without authorization and moved across several systems. The internal activity was carried out for about 10 months, and 23 files with 500 MB of data were stolen.
2020	Eighteen communication satellites in geostationary orbit	Eavesdropping on Internet communication	A presentation at the international conference BlackHat revealed that when signals from 18 communication satellites in geostationary orbit were received using commercially available antennas (costing about USD 300). The analysis of the communication revealed that communications on all 18 satellites were not encrypted, and sensitive information was visible. Information on hazardous materials and on administrator rights to wind power stations classified personal information (passport numbers and credit card data), and other such information was visible.
2022	Viasat Inc. Communication satellite KA-SAT	Connectivity with satellite broadband service was lost	Tens of thousands of communication modems used for communication satellite service KA-SAT of Viasat were the target of a DoS attack, temporarily disabling the satellite broadband connections from Ukrainian and European organizations using this service. In addition to disrupting the Ukrainian military's chain of command, this attack affected several wind turbines in Germany using the modems, disabling the remote control of more than 7,800 wind turbines managed by several power companies.

[4] Created based on various public information

2022	SpaceX Satellite ground equipment	Stopped the internet connection service	The Starlink service, which is a satellite constellation-based Internet connection service provided by SpaceX, to the Ukrainian government was seen to be a potential attack target by Russia because the location of Starlink's ground facilities can be identified by detecting satellite signals.
2022	ALMA Electron Telescope Computer system	Observation stopped	ALMA telescope's computing system in Chile suffered a cyberattack shutting down scientific observations and the website of the Joint ALMA Observatory in Chile. Computer clusters used for communication and other operations were affected, leading to the suspension of all observations.

(2) Cybersecurity incidents related to space systems

Some security incidents outside of the space sector are also useful references for the space sector. The following are examples that may be relevant to space systems.

Table 2-2 Cybersecurity incidents that may be relevant to space systems[5]

Year	Target	Impact	Overview
2019	Realtime OS VxWorks	Possibility of unauthorized access, etc.	Eleven vulnerabilities were announced in VxWorks of WindRiver, which is used in more than a billion devices in a wide range of industries such as medicine, automobiles, aircraft, defense, etc. Of these, 6 have been classified as fatal vulnerabilities, but many devices are said to be difficult to patch.
2020	Natural gas compression facility	Shutdown of natural gas compression facilities	A natural gas compression facility in the United States suffered a ransomware attack and was forced to shut down for 2 days.
2020	Up to about 18,000 organizations, including NASA	Information leaks, etc.	SolarWinds announced that malware was introduced to the network monitoring software Orion Platform through an official update. Early-stage malware sent information on the affected organization to the C&C server while avoiding detection by security services. The second-stage malware was introduced against targets that the attackers were interested in.
2020	Qualcomm product Snapdragon	Possibility of information leaks, etc.	Over 400 vulnerabilities were discovered in Qualcomm's Snapdragon, a system-on-chip (SoC) used in smartphones. The same SoC was used in some of NASA's early small satellites.
2021	Microsoft Exchange Server	Back door installation, etc.	Microsoft announced the occurrence of an unauthorized access incident that exploited 4 critical zero-day vulnerabilities in the Microsoft Exchange Server. By the time this incident was discovered, hundreds of thousands of organizations around the world were attacked.
2021	Apache Software Foundation Apache Log4j	Possibility of arbitrary command execution, such as information leaks	A remote code execution vulnerability was announced in Apache Log4j provided as open source by the Apache Software Foundation. There is a possibility of a remote third party sending crafted data to execute arbitrary commands.

[5] Created based on various public information

2.2 Concept of Cybersecurity Risks in Commercial Space Systems

(1) Framework for understanding the big picture

As mentioned above, various security incidents have occurred in space systems, and it is not easy to grasp the overall picture of security risks and measures related to space systems. Therefore, it is recommended to organize the concept of security risks and measures in commercial space systems by utilizing the "Cyber/Physical Security Framework (CPSF) Ver. 1.0" (February 2019, Ministry of Economy, Trade and Industry).

The CPSF aims to ensure the security of the entire supply chain in a new industrial society called "Society 5.0" that highly integrates cyberspace and physical space. A major feature of this framework is that, unlike frameworks targeting one organization such as the Information Security Management System (ISMS), this framework takes a multi-stakeholder approach to security measures across the entire supply chain, including affiliated companies and business partners. The CPSF approach is believed to be effective even for space systems because the supply chain is composed of various stakeholders such as satellite developers, satellite operators, ground station operators, and satellite data platform operators.

As shown in Figure 2-1, the CPSF considers the industrial society in three layers and organizes risk sources, required measures, etc. at each layer. An overall picture of security risks and measures can be identified by using this three-layer model for space systems.

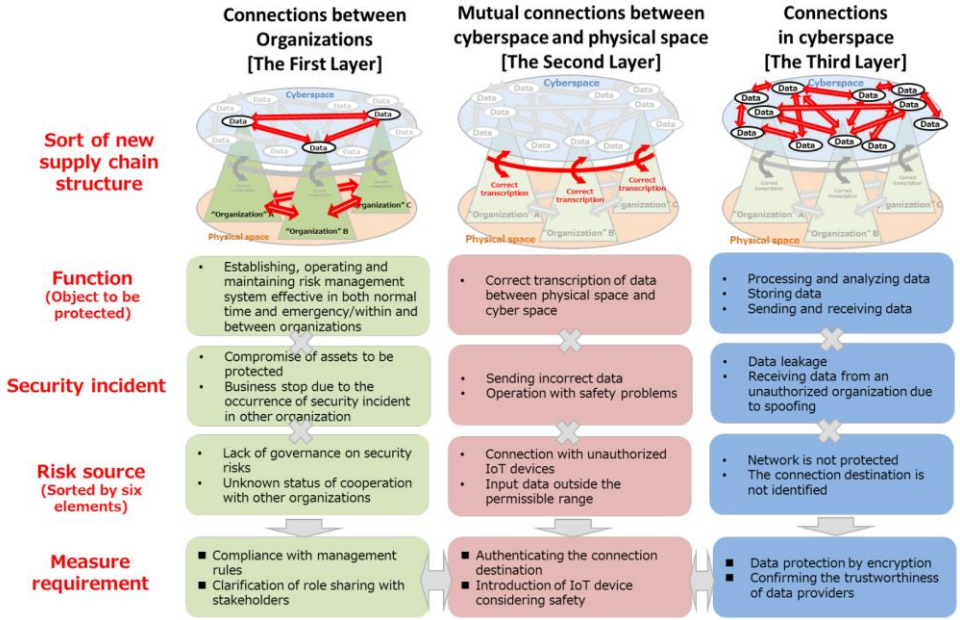


Figure 2-1 Overview of CPSF

(2) Flow of Security Risk Management

Figure 2-2 shows the flow of security risk management presented in the CPSF. In the following section of the guidelines, the targets of analysis are clarified as Step 1 of the CPSF, multiple risk scenarios that may cause serious business damage are examined for analysis as Steps 2 and 3, and approaches to risk management are summarized so as to be able to mitigate risks as Step 4.

Also, it is recommended to refer to the "Security Risk Assessment Guide for Industrial Control Systems" (March 2020) for a practical work-level procedure for Steps 1 to 4. This guide can be used when each company performs individual and detailed risk analysis.

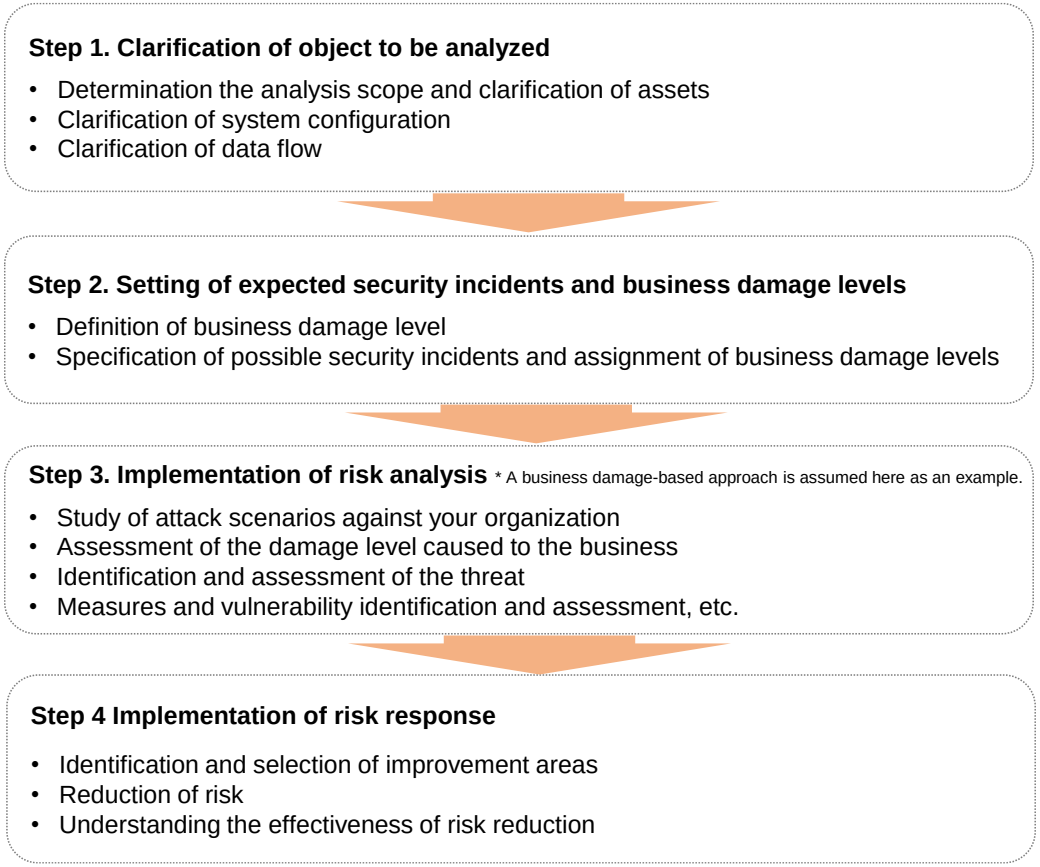
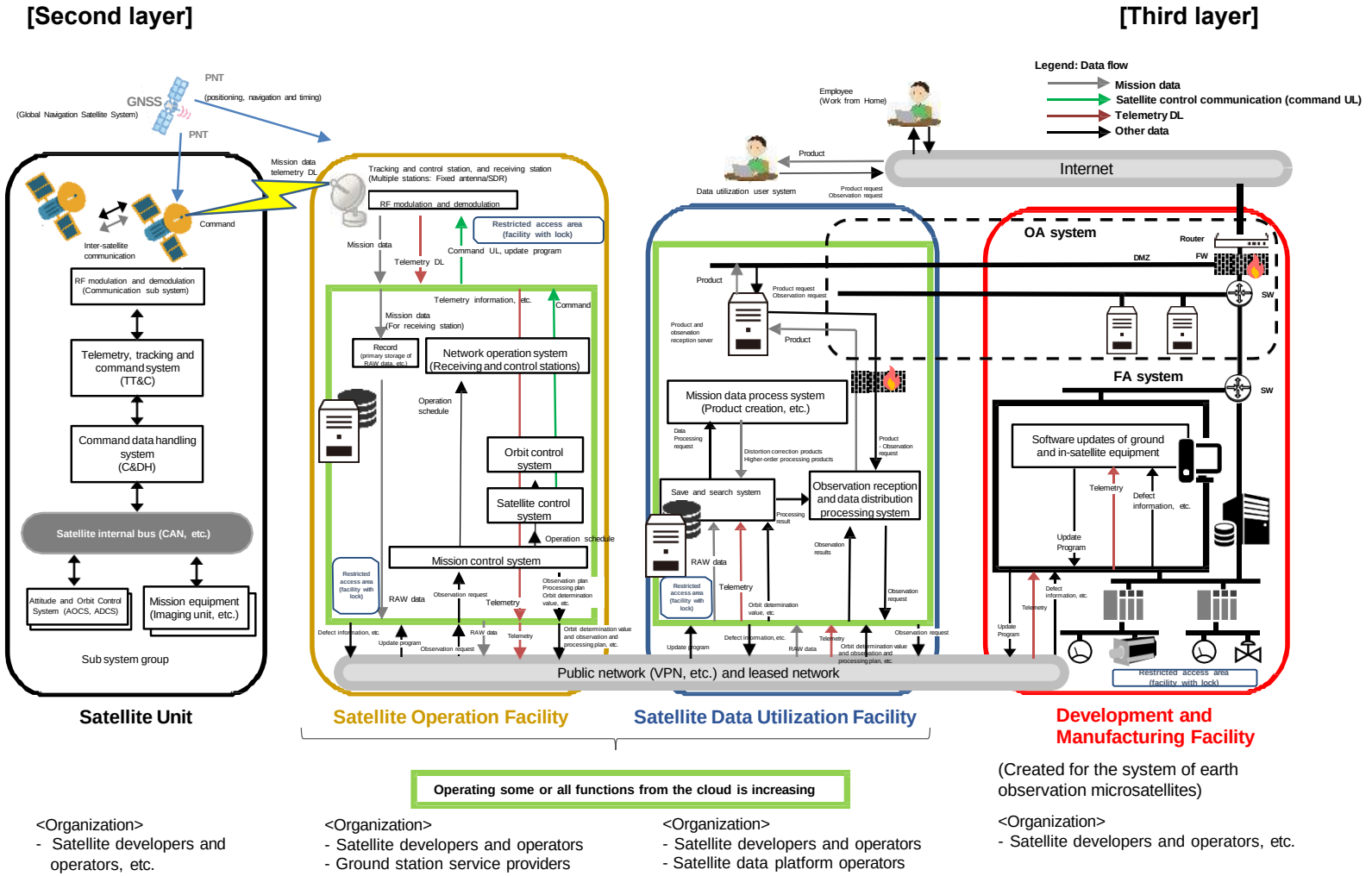


Figure 2-2 Flow of security risk management as presented in CPSF

(3) Standard models of commercial space systems

While utilizing the three-layer structure of the CPSF, the following standard model was created to clarify the targets of analysis by organizing the overall image of commercial space systems and stakeholder relationships, with remote sensing microsatellites as the analysis target.



(Created for the system of earth observation microsatellites)

<Organization>
- Satellite developers and operators, etc.

<Organization>
- Satellite developers and operators
- Ground station service providers

<Organization>
- Satellite developers and operators
- Satellite data platform operators
- Satellite data service providers, etc.

<Organization>
- Satellite developers and operators, etc.

Figure 2-3 Standard model of a space system

Column: Consequence-Driven Cyber-informed Engineering (CCE)

Competence-Driven Cyber-Informed Engineering (CCE) developed at the Idaho National Laboratory (INL) under the U.S. Department of Energy (DOE), is a security risk management methodology developed for use by control system engineers during development and system upgrades of critical infrastructure systems such as power facilities and plants.

CCE is broadly divided into four examination steps.

- In the 1st Quad, "events we don't want to occur" in the target system are identified and prioritized for the response. In this step, events that we do not want to occur are simply examined without considering cybersecurity. Such as "satellite shutdown," "sensitive satellite data leakage", in the case of space systems.
- In the 2nd Quad, related systems and subsystems that cause these events are identified.
- In the 3rd Quad, the kind cyberattacks that can cause the events of the 1st Quad using the systems of 2nd Quad are examined
- In the 4th Quad, security measures to respond to the cyberattacks of the 3rd Quad are examined.

Each Quad corresponds to the analysis in Steps 1 to 4 of the CPSF in the previous section.

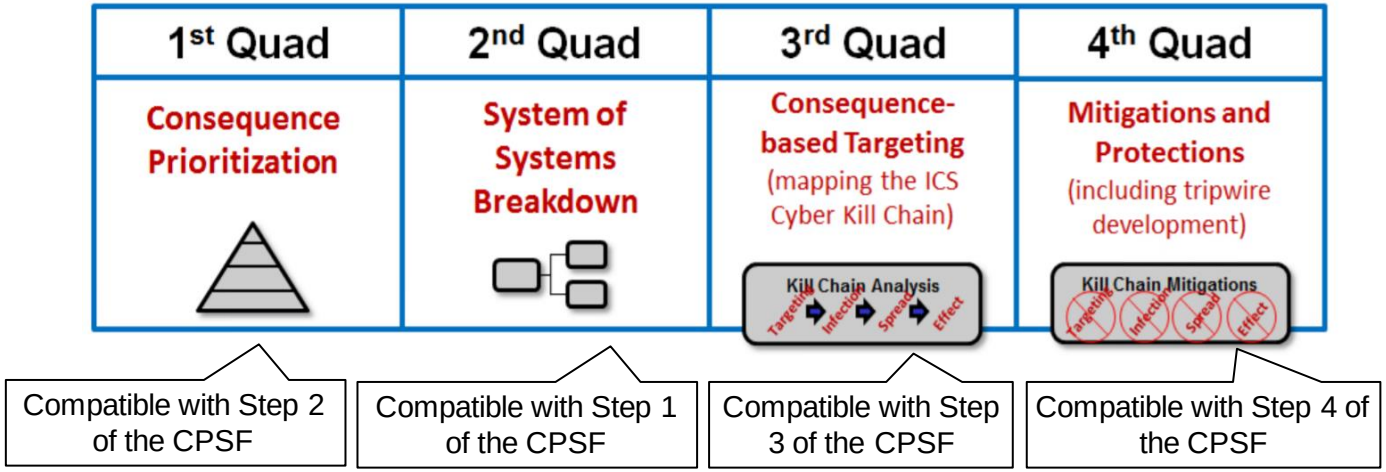


Figure 2-4 Four steps of CCE

(4) Examples of unwanted events

Examples of unwanted events in space systems are shown in the figure below. The next section examines multiple possible risk scenarios that can cause these events.

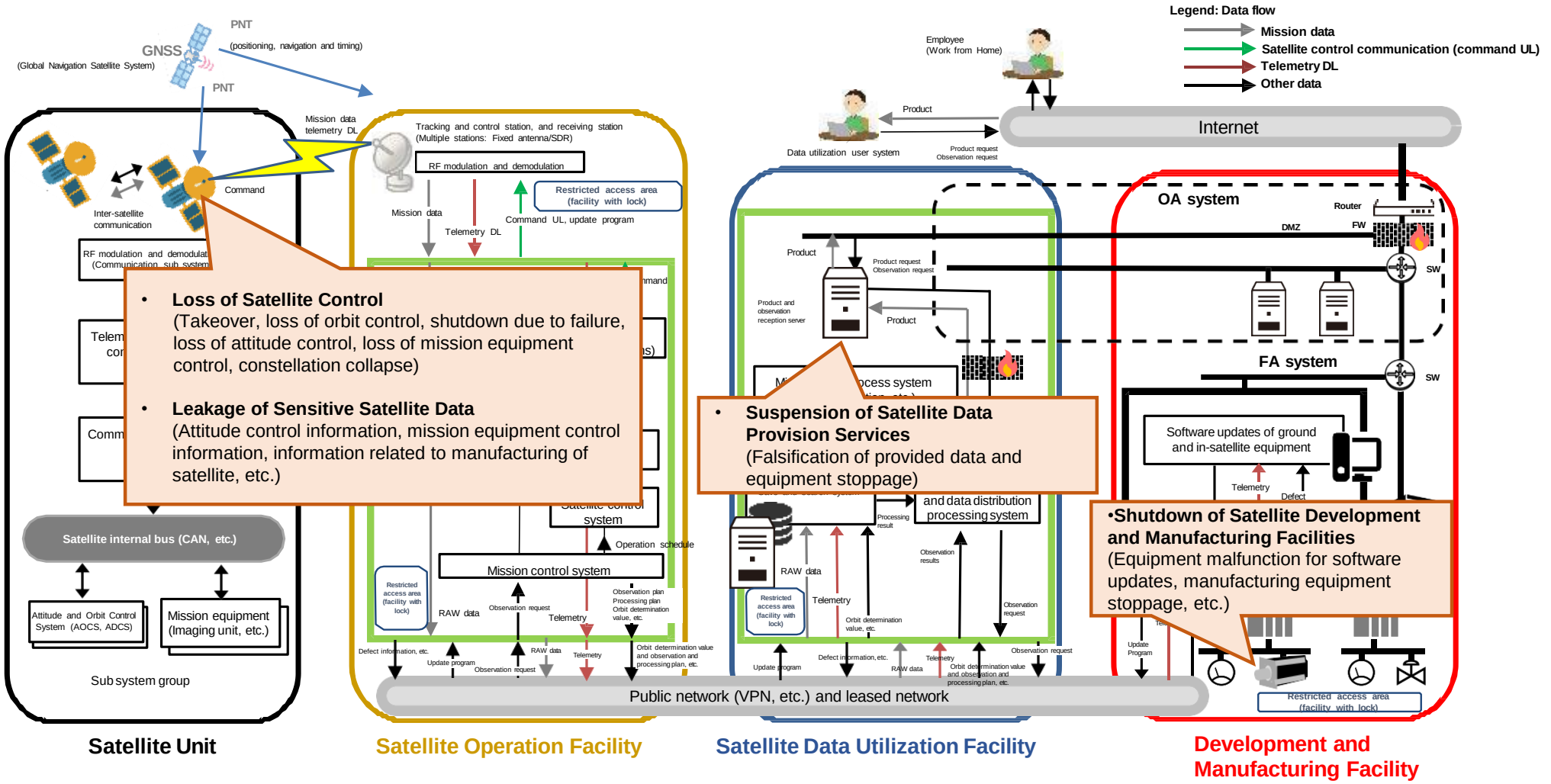
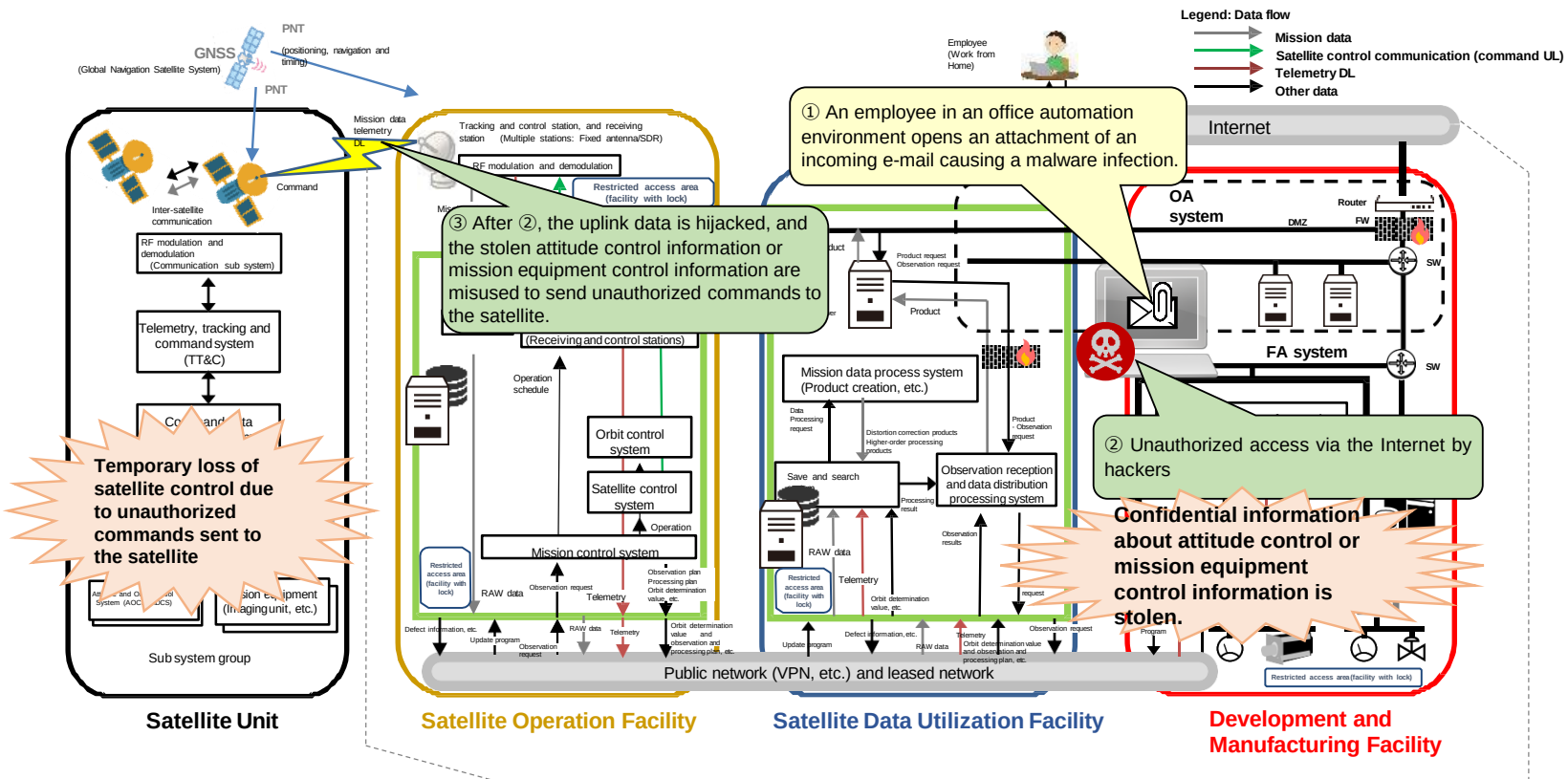


Figure 2-5 Examples of unwanted events

(5) Examples of possible risk scenarios

The guidelines include the following seven examples of risk scenarios that can cause serious business damage. In the following, an outline of each risk scenario is illustrated based on a standard model of a space system.

- Risk scenario 1: Loss of satellite orbit control due to a targeted email attack
- Risk scenario 2: Loss of satellite and mission equipment control due to malware infection of development and manufacturing terminals
- Risk scenario 3: Loss of satellite control due to a cyberattack on a satellite data utilization facility
- Risk scenario 4: Unable to provide services due to unauthorized access to the observation reception server
- Risk scenario 5: Disclosure of company secrets due to an email attack in a work from home environment
- Risk scenario 6: Suspension of operation due to unauthorized use of USB flash drives
- Risk scenario 7: Constellation collapse crisis due to acceptance of unauthorized satellite instruments



Entry point

Communication between satellite and ground stations

Internet

Method of attack

- Spoofing and replay attacks

<Carelessness activities>
- Malware infection due to opening email attachments

<Malicious activities>
- CNE (Intelligence and manipulation activities)

Source of threat

③

Intelligence agency or industrial espionage

①

Employees with low security awareness

+

②

Intelligence agency or industrial espionage

Figure 2-6 Risk scenario 1: Loss of satellite orbit control due to a targeted email attack

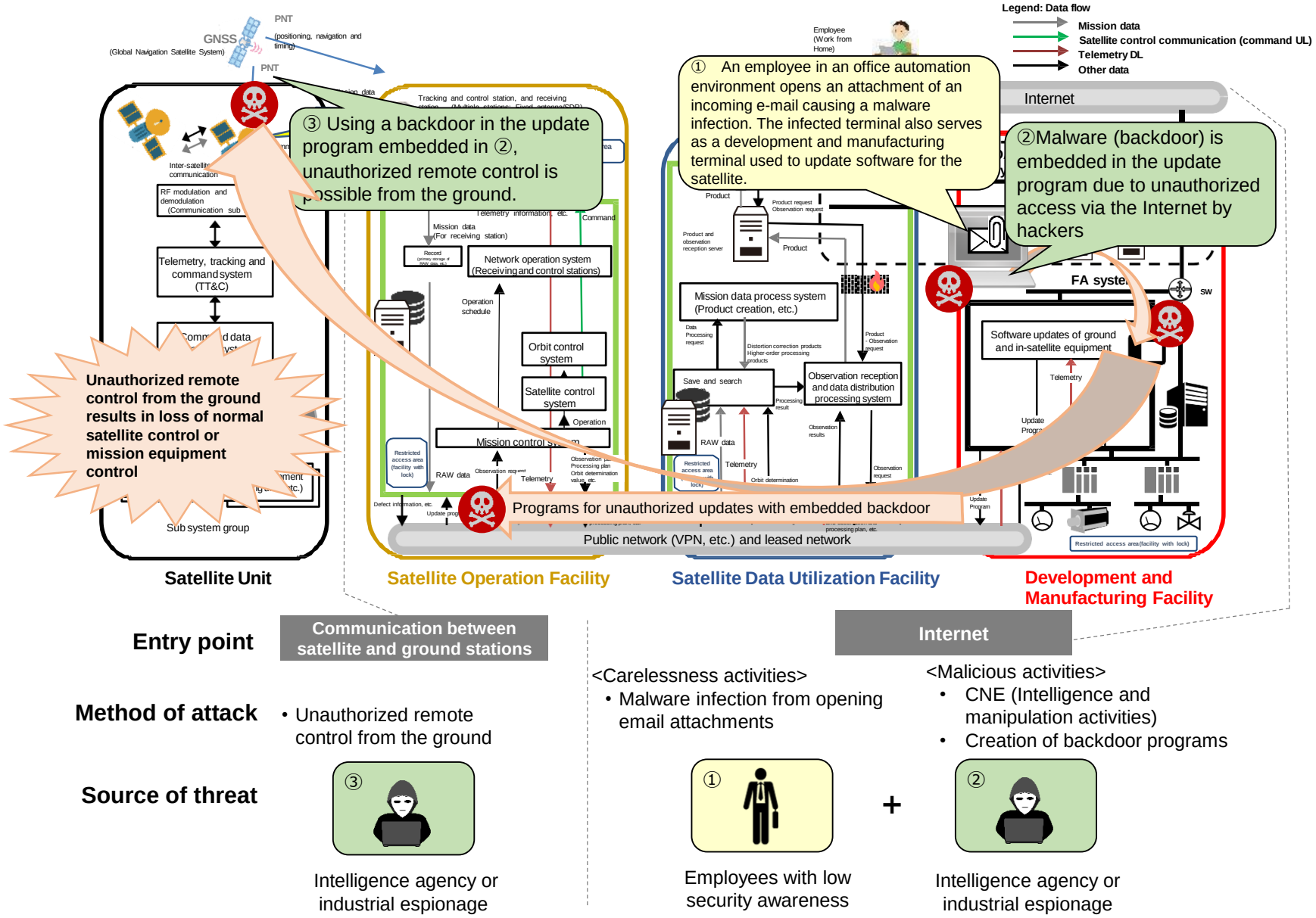
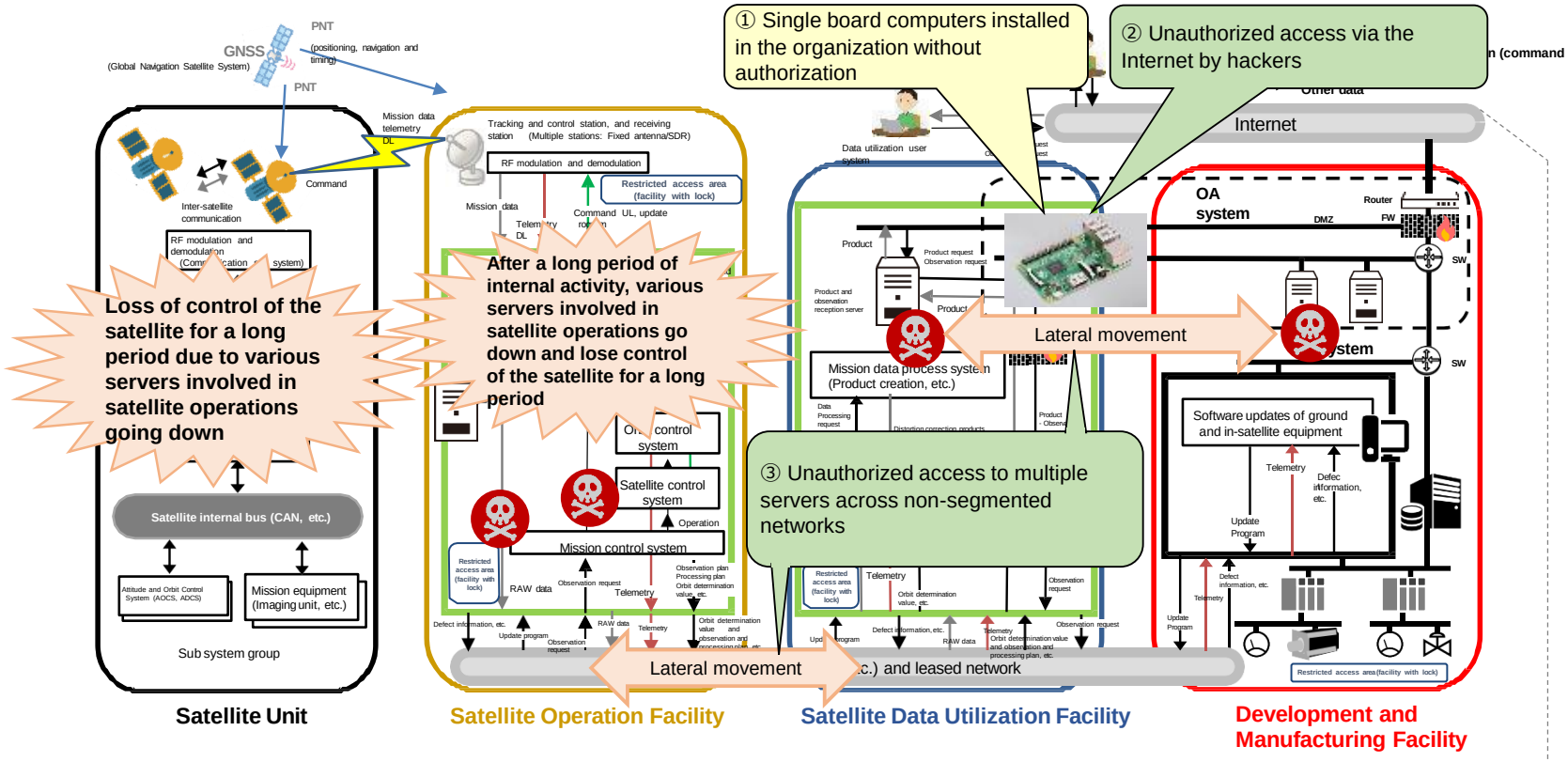


Figure 2-7 Risk scenario 2: Loss of satellite and mission equipment control due to malware infection of development and manufacturing terminals



Entry point — Internet

Method of attack

<Carelessness activities>
- Unauthorized intrusion due to connection of unauthorized terminals

<Malicious activities>
- CNE (Intelligence and manipulation activities)

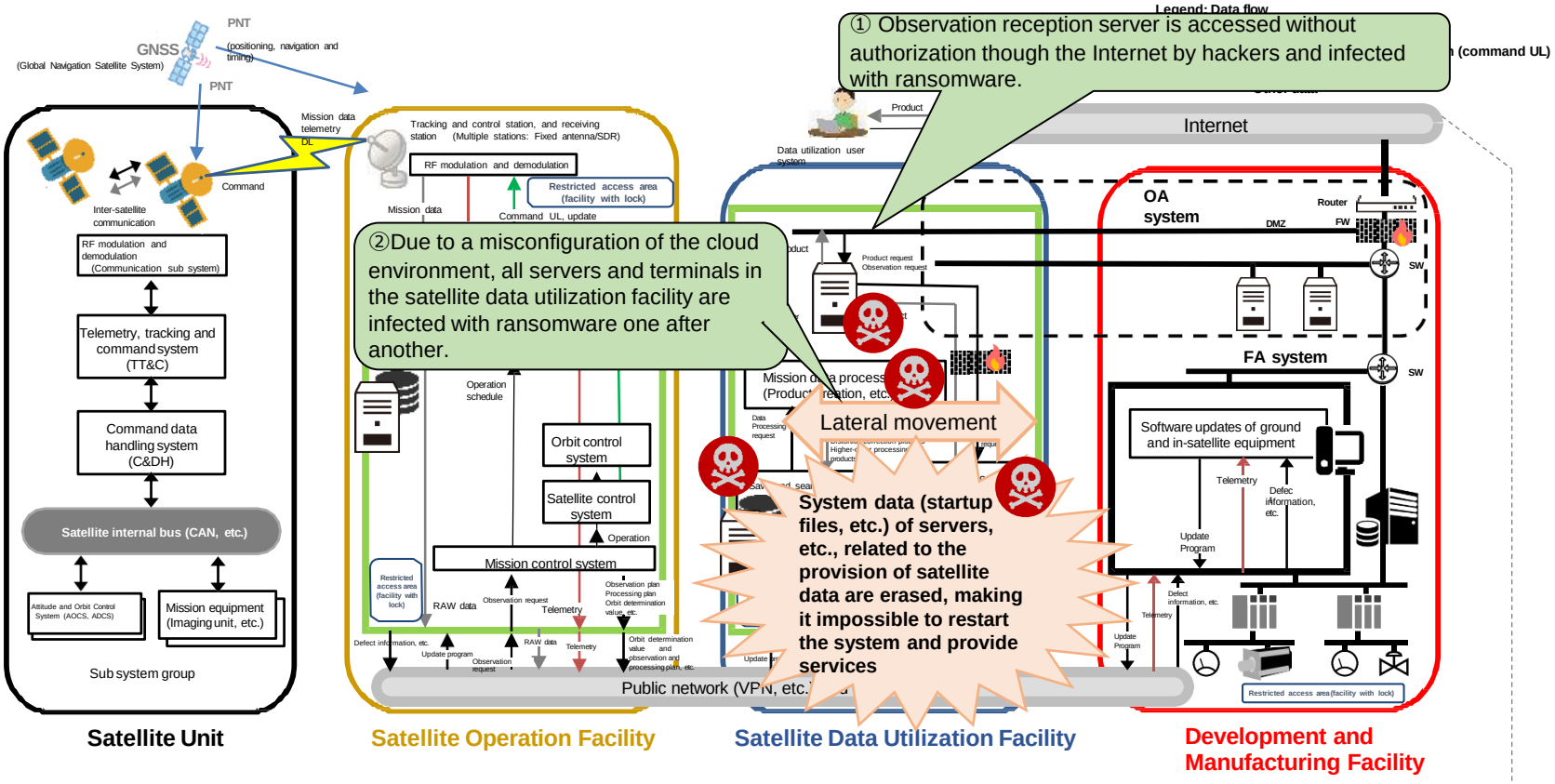
Source of threat

① + ② ③

Employees with low security awareness

Intelligence agency or industrial espionage

Figure 2-8 Risk scenario 3: Loss of satellite control due to a cyberattack on a satellite data utilization facility



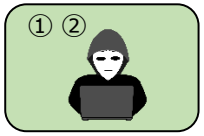
Entry point

Internet

Method of attack

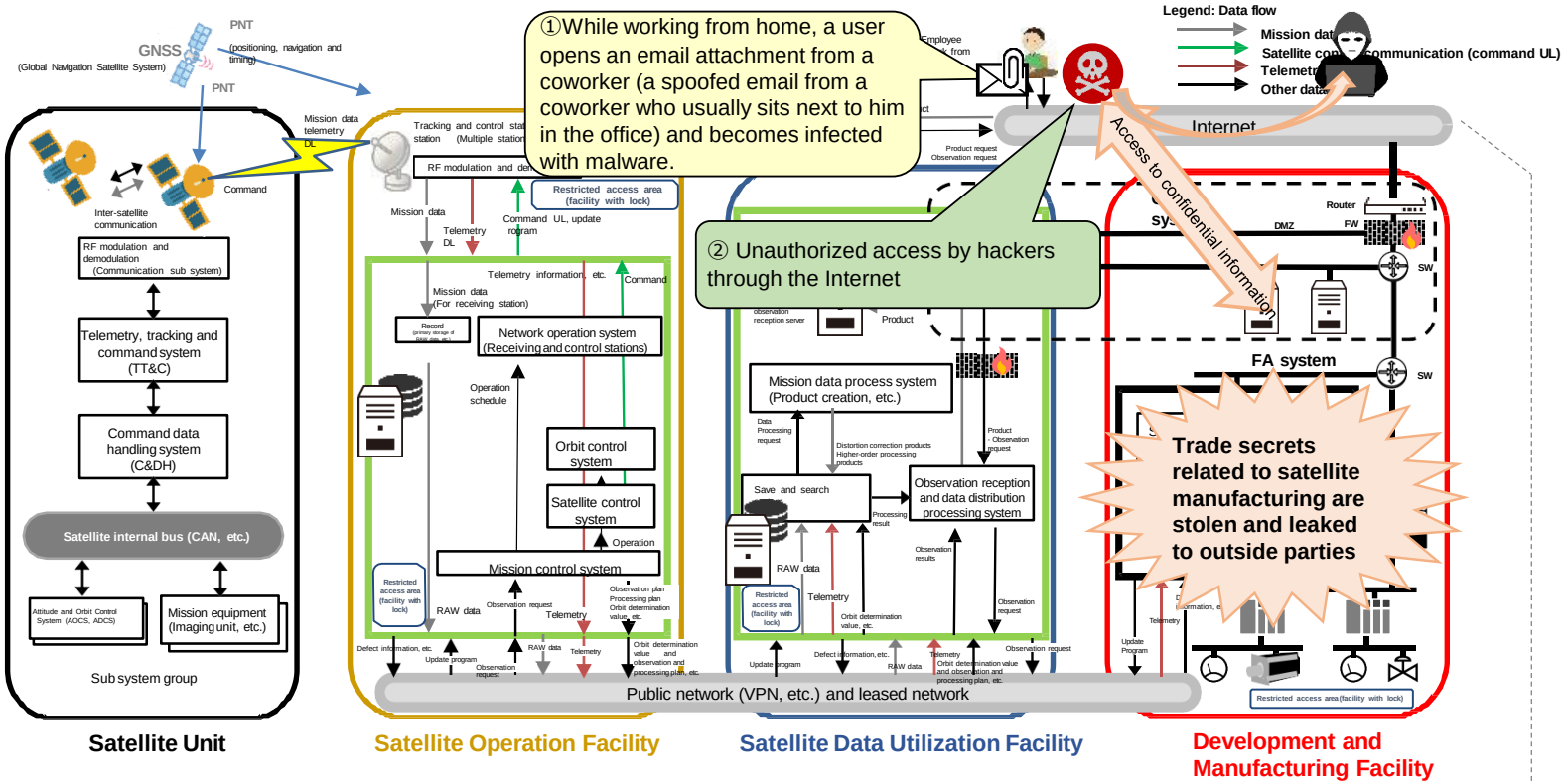
- Attacks on web applications (SQL injection attacks, malicious file upload attacks, etc.)

Source of threat



Intelligence agency or industrial espionage

Figure 2-9 Risk scenario 4: Unable to provide services due to unauthorized access to the observation reception server



Entry point — Internet

Method of attack

<Carelessness activities>
- Malware infection due to opening email attachments

<Malicious activities>
- CNE (Intelligence and manipulation activities)

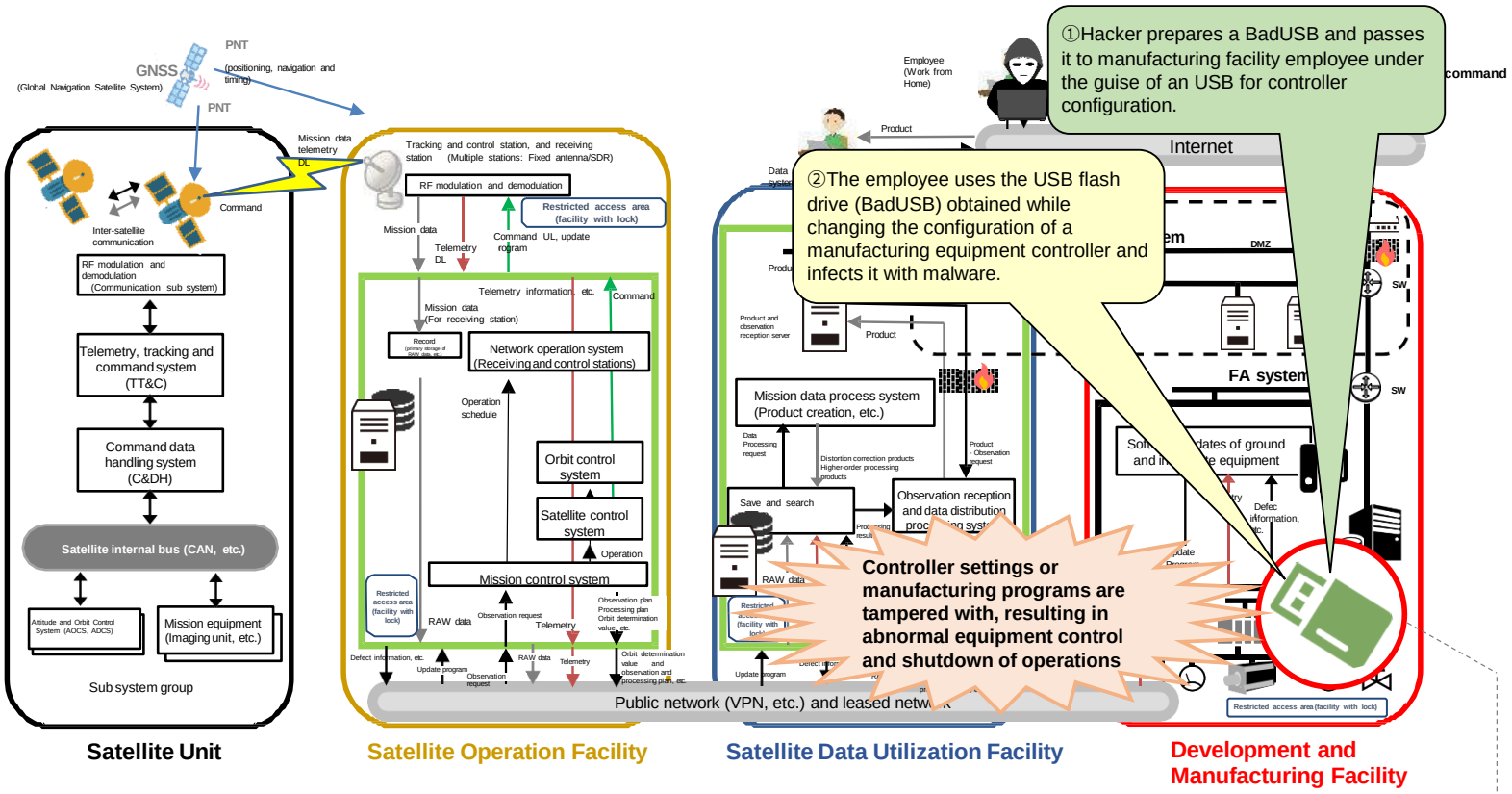
Source of threat

① Employees with low security awareness

+

② Intelligence agency or industrial espionage

Figure 2-10 Risk scenario 5: Disclosure of company secrets due to an email attack in a work from home environment



Entry point

External recording media in closed environments

Method of attack

<Carelessness activities>
- Malware infection due to the use of personal USB flash drives other than the USB flash drives prescribed for operations

<Malicious activities>
- Production and transport of BadUSB*

*USB flash drive prepared by planting malware in the firmware

Source of threat

② + ①

Employees with low security awareness

Intelligence agency or industrial espionage

Figure 2-11 Risk scenario 6: Suspension of operation due to unauthorized use of USB flash drives

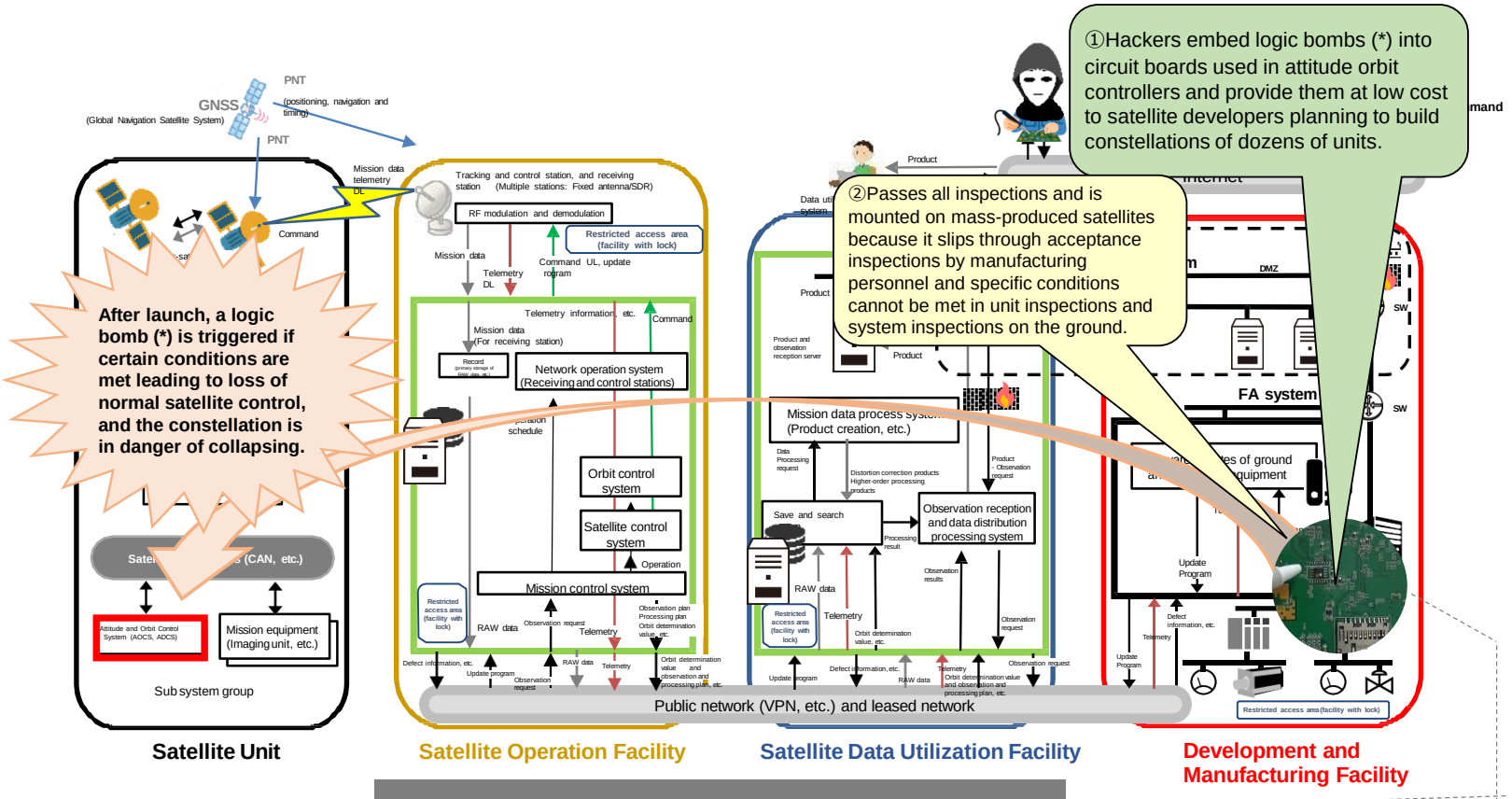
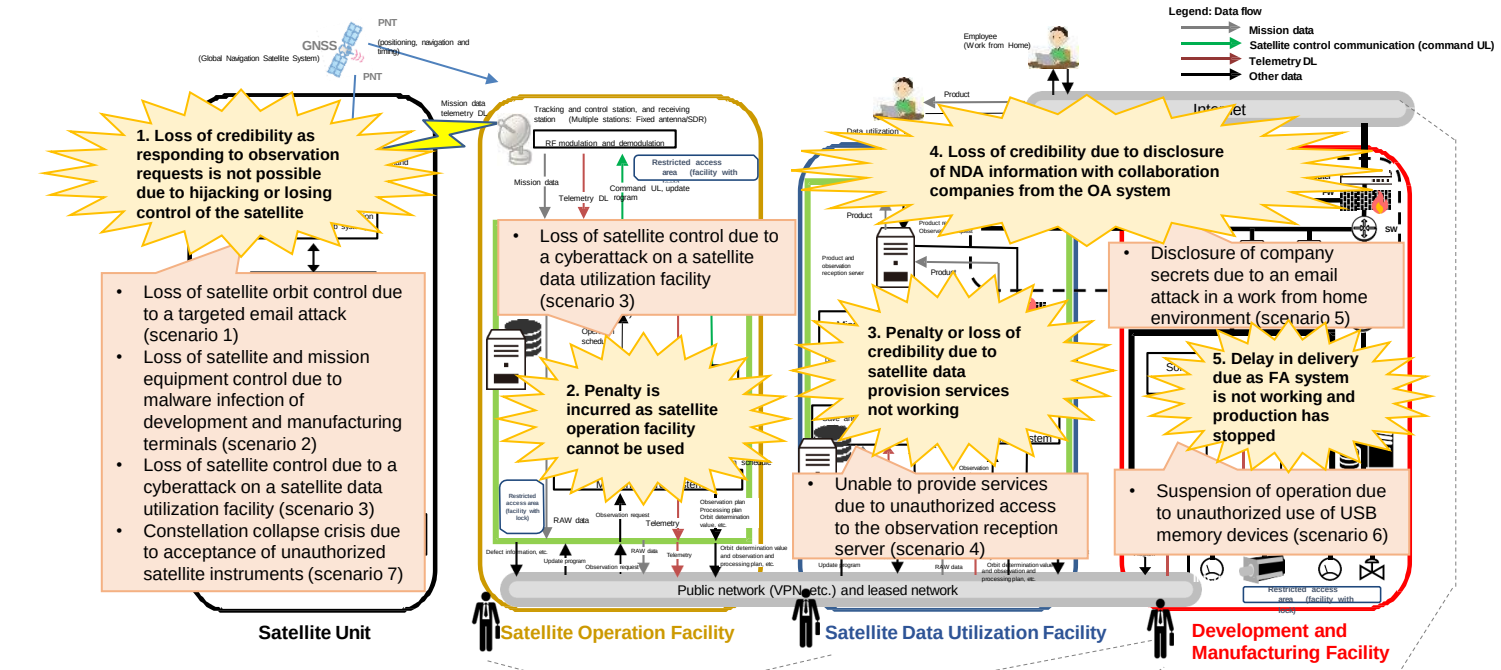


Figure 2-12 Risk scenario 7: Constellation collapse crisis due to acceptance of unauthorized satellite instruments

The following figure shows the seven risk scenarios described so far, organized based on the standard model.



Example of entry points

Communication between satellite and ground stations	Employees and contractors who enter and leave	Supply chain risk	Internet

Example of attack methods

- Communication between satellite and ground stations
  - Interception of communications
  - Spoofing
  - Replay attack
  - Jamming, etc.
- Employees and contractors who enter and leave
  - <Malicious activities>
  - Taking out plans for design by USB
  - <Carelessness activities>
  - Unauthorized intrusion due to connection of unauthorized terminals, etc.
- Supply chain risk
  - <Malicious activities>
  - Tampering with unauthorized HW/SW, etc.
  - <Carelessness activities>
  - Attacks due to OSS vulnerabilities, etc.
- Internet
  - Targeted email attack
  - Attacks on Web services you provide
  - Attacks on the Web services you use
  - Attacks on empty ports, etc.

Example of threat sources

Foreign intelligence agencies; Industrial spies; Organizations and individuals seeking money; Employees with resentment; Employees with low consciousness of security

No.	Satellite owners	Satellite operators	Ground station service providers	Satellite data platform operators	Satellite data service providers	Satellite developers
	Satellite Unit	Satellite Operation Facility		Satellite Data Utilization Facility (OA system)		Development and Manufacturing Facility (OA system)
1	✔	✔	✔	✔	✔	✔
2	✔	✔	✔	✔	✔	✔
3	—	—	—	✔	✔	—
4	—	—	—	—	—	✔
5	—	—	—	—	—	✔

✔: Businesses affected by a chain of damages from 1 to 5 above

Figure 2-13 Examples of serious business damage, attack methods, etc. pertaining to each stakeholder

(6) Main measures for each subsystem

The table below shows the results of organizing the main measures required for each subsystem based on the 7 risk scenarios described above. Measures related to organizational management corresponding to the first layer of the CPSF are described in Section 3.1, and technical measures for each subsystem corresponding to the second and third layers of the CPSF are described in Section 3.2.

Table 2-3 Main measures required for each subsystem based on anticipated risk scenarios

No.	Example of a risk scenario that will lead to a major business damage	Primary measures				
		Satellite unit	Satellite operation facility	Satellite Data Utilization Facility	OA System	Development and manufacturing facility
Scenario 1	A terminal of an employee in the OA environment was infected with malware after a targeted email attack. Confidential information related to attitude control and mission equipment control was stolen by remote access through the Internet. The uplink data of the satellite unit was subsequently hijacked, and unauthorized commands were sent to the satellite using the stolen information, resulting in a temporary loss of satellite orbit control.	・ Integrity and encryption of data sent and received in RF communications	・ Integrity and encryption of data sent and received in RF communications	-	・ Cybersecurity education and training for employees	-
Scenario 2	The development and manufacturing terminals used for updating the software of the satellite unit (combined use with OA) were infected with malware and a malicious program (back door) was embedded in the update program, and the satellite or mission equipment could not be controlled normally by remote operations from the ground.	・ Prior verification of update program and measures for protection from vulnerabilities* (*Since the risk is after launch, it is verified with the development and manufacturing equipment)	-	-	・ Cybersecurity education and training for employees	・ Separation of information and control systems
Scenario 3	An unauthorized terminal installed in the satellite data utilization facilities was subject to a cyberattack through the Internet and became the origin for attacks from the Internet inside the equipment, resulting in various servers not working, including the ground infrastructure system for satellite operation, and in loss of satellite control for a long period.	・ Ensuring multiple secure communication paths	・ Facility vulnerability protection	・ Facility vulnerability protection	・ Measures to prevent the use of shadow IT ・ IT asset management, configuration management and patch management for information systems	-
Scenario 4	The observation reception server was infected with ransomware after unauthorized access through the Internet. Subsequently, all servers and terminals in the facility were infected due to defective settings of the server environment, and the system data needed for the startup was erased, which disabled to reboot of the system and providing services.	-	-	・ Implementation of secure development ・ Use of external services such as cloud services	・ Technical protection of servers used for critical operations ・ Incident response	-

No.	Example of a risk scenario that will lead to a major business damage	Primary measures				
		Satellite unit	Satellite operation facility	Satellite Data Utilization Facility	OA System	Development and manufacturing facility
Scenario 5	While working from home, the computer of an employee was infected with malware on opening an email attachment from a colleague (it was a spoofed email from a sender posing as a colleague who usually sits next to him in the office). Trade secrets concerning satellite manufacturing were stolen by remote access via the Internet and disclosed externally.	-	-	-	・ Cybersecurity education and training for employees ・ Collection and analysis of terminal and network logs	-
Scenario 6	An unauthorized personal USB flash drive was used to change the settings of the manufacturing equipment controller, and malware in the USB flash drive altered the settings and programs, causing abnormalities in controlling the equipment, and operations were suspended.	-	-	-	-	・ Prohibition of using unauthorized USB flash drives ・ Malware measures with whitelist type
Scenario 7	When procuring satellite instruments, an unauthorized board was accepted and installed in the satellite group without identifying that the device was malicious. A logic bomb was initiated when certain conditions were met after the satellite was launched, and the constellation faced the danger of disruption.	-	-	-	-	・ Inspection of parts that are accepted
Summary of primary measures for each subsystem		・ Integrity and encryption of data sent and received in RF communications (3.2.2) ・ Prior verification of update program and measures for protection from vulnerabilities (3.2.2) ・ Ensuring multiple secure communication paths (3.2.2)	・ Integrity and encryption of data sent and received in RF communications (3.2.3) ・ Facility vulnerability protection measures (3.2.3)	・ Facility vulnerability protection (3.2.4) ・ Implementation of secure development (3.2.4) ・ Use of external services (3.1.2, 3.2.1)	・ Common cybersecurity measures (3.1) ・ Reporting incidents (3.1.5)	・ Measures for supply chains (3.2.2) ・ Common control system cybersecurity measures (3.2.5)

3. Key Points of Cybersecurity Measures for Commercial Space Systems

This section describes the key points of security measures for commercial space systems based on the concept of security risk pertaining to commercial space systems analyzed in the previous section. Measures common to all organizations involved in space systems are described in Section 3.1, and specific measures for each subsystem are described in Section 3.2.

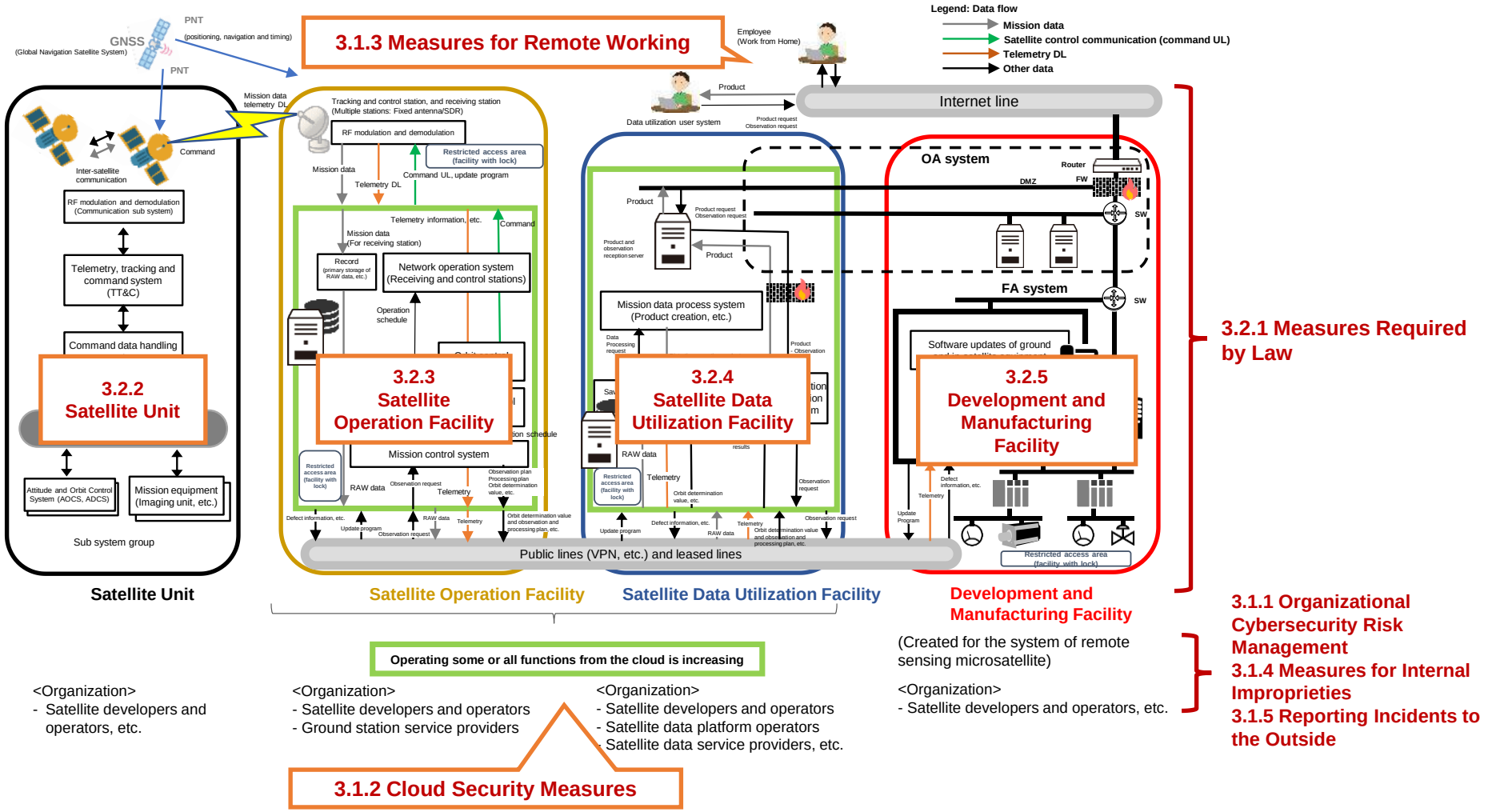


Figure 3-1 Overview of space systems and the corresponding points

Security measures that each stakeholder involved in commercial space systems should consider and work on, and the information that can be used as a reference when considering the measures are classified under three items, “Requirements,” “Basic measures”, and “Details”, as shown below.

Requirements
indicate cybersecurity measures to be considered and addressed by each stakeholder.

[Basic Measures]
indicate examples of widespread practices and measures that are recommended to be addressed to meet the requirements. Cases of advanced practices and measures that are difficult to implement without a certain budget and organizational structure and personnel, although further cybersecurity enhancements are expected, are indicated with the condition “when a high-security level is required.”

(Details)
indicate additional and reference information concerning Requirements and corresponding Basic measures.

The purpose of the guidelines is to encourage voluntary measures by commercial operators, and the “Requirements” shown here are positioned as guidelines for cybersecurity measures that stakeholders with some kind of involvement in each subsystem should jointly consider. When considering specific security measures, it is recommended to consult with consultants, system integrators, and vendors who possess the necessary knowledge, while taking into account the details of the measures described in the “Basic measures” and the reference guidelines. Since cyberattacks are constantly evolving, and new products and services are launched in response, it is important to always consult with organizations and experts who possess information and knowledge at the forefront of security.

The required measures for each stakeholder are summarized in Tables 3-1 and 3-2. Also, a checklist organizing requirements for measures is included in Attachment 1. This checklist, which shows requirements and basic measures necessary for space systems, should be used as a reference when implementing measures.

Table 3-1 Correspondence between each stakeholder and Requirements and Basic Measures 1/2

Category	Sec.	Item Name	Requirements	Basic Measures/ Basic measures when a high security level is required	Stakeholders				
					Satellite owners	Satellite operators*	Satellite data platform operators	Satellite data service providers	Satellite developers
Common Measures	3.1.1	Organizational Cybersecurity Risk Management	**[Requirements]** Establish a cybersecurity risk management system under the management's leadership to implement measures, which include identification, prevention, detection, response, and recovery, against the company's cybersecurity risks.	**[Basic Measures]** (1) When identifying the cybersecurity risks to the company and implementing measures while establishing a cybersecurity risk management system, it is preferred that existing standards and frameworks, including (a) to (e) given below, are used from the perspective of ensuring the effectiveness of the measures and preventing oversight. (a) Cybersecurity Management Guidelines Ver. 3.0 (METI, IPA) (b) Information Security Measure Guidelines for Small and Medium-sized Enterprises, third edition (IPA) (c) ISO/IEC 27001 (Information Security Management System) (d) Cybersecurity Framework Ver1.1 (NIST) (e) SP 800-171 (NIST)	✓	✓	✓	✓	✓
	3.1.2	Cloud Cybersecurity Measures	**[Requirements]** When utilizing external services, select services that meet the security requirements and service level agreements (SLAs) appropriate to the laws, regulations, and mission, etc.	**[Basic Measures]** (1) The principal laws and regulations concerning external services for the space industry are as given below, and services should be selected after confirming that the external service providers comply with the laws and regulations. (a) Regulation for Enforcement of the Act on Ensuring Appropriate Handling of Satellite Remote Sensing Data	✓	✓	✓	✓	✓
				[Basic Measures] (2) The principal certifications concerning external services for the space industry include (a) to (c) given below, and services with an appropriate security level should be selected. (a) ISO/IEC 27017 Code of practice for information security controls based on ISO/IEC 27002 for cloud services (ISO/IEC) (b) Information System Security Management and Assessment Program (ISMAP) (Cabinet Secretariat, MIC, METI) (c) The Federal Risk and Authorization Management Program (FedRAMP)	✓	✓	✓	✓	✓
	3.1.3	Cybersecurity Measures for Remote Working	**[Requirements]** When remote working, maintain the environment and organize the regulations for performing safe operations.	**[Basic Measures]** (1) Existing guidelines, including the (a) and (b) given below are preferred to be used for safe remote working operations. (a) Telework Security Guidelines (fifth edition) (MIC) (b) Telework Security Guidelines for SMEs (Checklist), third edition (MIC)	✓	✓	✓	✓	✓
	3.1.4	Measures for Internal malpractice	**[Requirements]** Consider measures for the prevention and early detection of internal improprieties.	**[Basic Measures]** (1) Using the existing standards, including (a) given below to address internal improprieties is preferred. (a) Guidelines for the Prevention of Internal Improprieties in Organizations (fifth edition) (IPA)	✓	✓	✓	✓	✓
	3.1.5	Reporting Incidents to the Outside	**[Requirements]** Report incidents including defects to the external authorities, as necessary.	**[Basic Measures]** (1) When an incident occurs in the space system, notifying the competent ministries and agencies, affected organizations, and individuals may be required in accordance with laws, regulations, and rules. For this reason, it is preferred that the stakeholders to whom a report is to be submitted when an incident occurs are identified, and the communication flow is organized.	✓	✓	✓	✓	✓

*: Includes ground station service providers providing tracking and control station services or receiving station services.

Table 3-2 Correspondence between each stakeholder and Requirements and Basic Measures 2/2

Category	Sec.	Item Name	Requirements	Basic Measures/ Basic measures when a high security level is required	Stakeholders				
					Satellite owners	Satellite operators*	Satellite data platform operators	Satellite data service providers	Satellite developers
Specific Measures for Space Systems	3.2.1	Measures Required by Law	**[Requirements]** Comply with the relevant laws and regulations and provide appropriate responses throughout the lifecycle. Comply with the following key laws and regulations (a) to (c) related to the space industry to promote the safe usage of space: (a) Act on Launching of Spacecraft, etc. and Control of Spacecraft (b) Act on Ensuring Appropriate Handling of Satellite Remote Sensing Data (c) Foreign Exchange and Foreign Trade Act	-	✓	✓	✓	✓	✓
	3.2.2	Satellite Unit	**[Requirements]** Implement cybersecurity measures in the satellite system (main satellite unit and RF communication).	**[Basic measures when a high-level of security is required]** (1) When a high security level is required, implementation of the following measures (a) to (f) is preferred. (a) RF communication protection (b) Jamming protection measures of RF communication (c) Prior verification of functions implemented in satellites (d) Measures for protection of satellite instruments from vulnerabilities (e) Ensuring the integrity of data sent and received (f) Measures for supply chains	✓	✓	-	-	✓
	3.2.3	Satellite Operating Facility	**[Requirements]** Implement cybersecurity measures for satellite operation facilities (tracking and control station, receiving station, network operation system, and mission control system (including satellite control system and orbit control system)).	**[Basic measures when a high-level of security is required]** (1) When a high security level is required, implementation of the following measures (a) to (h) is preferred. (a) Equipment protection (b) Communication protection (c) Jamming protection measures (d) Data protection (e) Facility inspection and vulnerability protection measures (f) Ensuring the integrity of data sent and received (g) Use of external services (h) Secure coding	-	✓	✓	-	✓
	3.2.4	Satellite Data Utilization Facility	**[Requirements]** Implement cybersecurity measures for satellite data utilization facilities.	**[Basic measures when a high-level of security is required]** (1) When a high security level is required, implementation of the following measures (a) to (f) is preferred. (a) Equipment protection (b) Data protection (c) Facility inspection and vulnerability protection measures (d) Ensuring the integrity of data received (e) Use of external services (f) Secure coding	-	-	✓	✓	✓
	3.2.5	Development and Manufacturing Facilities	**[Requirements]** Implement cybersecurity measures for satellite development and manufacturing facilities.	**[Basic Measures]** (1) When handling satellite development and manufacturing equipment, using the existing standards, including (a) given below is preferred. (a) The Cyber/Physical Security Framework for Factory Systems (METI)	-	✓**	-	-	✓

*: Includes ground station service providers providing tracking and control station services or receiving station services.

**: Ground station service providers are excluded.

3.1 Common Measures

3.1.1 Organizational Cybersecurity Risk Management

Requirements

Establish a cybersecurity risk management system under the management's leadership to implement measures, which include identification, prevention, detection, response, and recovery, against the company's cybersecurity risks.

[Basic Measures]

(1) When identifying the cybersecurity risks to the company and implementing measures while establishing a cybersecurity risk management system, it is preferred that existing standards and frameworks, including (a) to (e) given below, are used from the perspective of ensuring the effectiveness of the measures and preventing oversight.

(a) Cybersecurity Management Guidelines Ver 3.0 (METI, IPA)
(b) Information Security Measure Guidelines for Small and Medium-sized Enterprises, third edition (IPA)
(c) ISO/IEC 27001 (Information Security Management System)
(d) Cybersecurity Framework Ver1.1 (NIST)
(e) SP 800-171 (NIST)

(Details)

● Basic measures (1) (a) "Cybersecurity Management Guidelines Ver 3.0 (METI, IPA)"

① Target

Large, medium, and small enterprises (excluding small businesses)

② Overview

The basic measures summarize "three principles" of which the management needs to be aware for protecting companies from cyberattacks, and "ten important items" regarding which the management should instruct executives (CISO, etc.) responsible for implementing information security measures.[6]

The three principles mentioned in the guidelines of which management should be aware are as follows.

[6] Ministry of Economy, Trade and Industry: "Cybersecurity Management Guidelines Ver 3.0" (March 2023)
https://www.meti.go.jp/policy/netsecurity/mng_guide.html (in Japanese)
The English version of the previous version can be accessed https://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v2.0_en.pdf

- Management must recognize that cybersecurity risk is a key issue in their company's risk management and take measures under their own leadership.
- For management to fulfill its responsibility to ensure cybersecurity, it is necessary to pay attention to cybersecurity measures not only for the company itself but also for the entire supply chain, including domestic and overseas offices, business partners, and contractors.
- Proactive communication with relevant parties is necessary to implement cybersecurity measures in both normal times and emergencies.

Figure 3-2 shows an outline of the "ten important items" of which management should instruct CISO and other officers.

Build a structure or process for cybersecurity risk management	**Direction 1** Recognize cybersecurity risk and develop a company-wide policy **Direction 2** Build a management system for cybersecurity risk **Direction 3** Secure resources (budget, workforce etc.) for cybersecurity measures
Identify cybersecurity risks and implement measures	**Direction 4** Identify cybersecurity risks and develop plans to address them **Direction 5** Establish systems to effectively address cybersecurity risks **Direction 6** Implement a PDCA cycle for cybersecurity measures
Establish a system to prepare for the occurrence of incidents	**Direction 7** Develop a cybersecurity incident response team and relevant procedures **Direction 8** Develop a recovery team and relevant procedures in preparation for damage due to cyber incidents
Drive security measures in the supply chain	**Direction 9** Understand cybersecurity status and measures in the entire supply chain including business partners and outsourcing companies
Drive communication with stakeholders and other relevant parties	**Direction 10** Gather, utilize and provide cybersecurity related information through information sharing activities

Figure 3-2 Overview of the "Ten Important Items" of Which Management Should Instruct CISOs, etc.

It is possible to visualize the status of your company's efforts for the "ten important items," using the "Cybersecurity management guidelines implementation status visualization tool" (for enterprises and organizations with 300 or more employees). [7]

The tool can be used by officials to evaluate the status of measures taken by their own company and report the response results to management, thereby visualizing the status of measures taken within the company and disclosing the same to stakeholders such as business partners. There are 40 specific question items as shown in Table 3-3, and for each item, the status of measures taken is selected on a 5-point scale.

[7]Information-Technology Promotion Agency, Security Center: "Cybersecurity Management Visualization Tool" (March 2023)
https://www.ipa.go.jp/security/economics/checktool/index.html (in Japanese)

Table 3-3 Items of “Cybersecurity management guidelines implementation status visualization tool”

Directions	#		Item
Direction 1 Recognize cybersecurity risk and develop a company-wide policy	1	1-1	Recognize cybersecurity risks as one of the management risks.
	2	1-2	Formulate and declares basic policies that consider cybersecurity risks for the organization as a whole.
	3	1-3	Understand the requirements of laws, contracts, guidelines, etc., and reflect them in basic policies, etc.
Direction 2 Build a management system for cybersecurity risk	4	2-1	Establish a cybersecurity risk management system consisting of CISO, etc. based on the basic policies of the organization.
	5	2-2	Clarify the roles and responsibilities of each party with respect to the management of cybersecurity risks.
	6	2-3	Clarify the relationship between governance, internal controls, and risk management systems related to business continuity and cybersecurity risk management systems within the organization.
Direction 3 Secure resources (budget, workforce etc.) for cybersecurity measures	7	3-1	Management and other parties discuss and clarify cybersecurity measures and the resources (budget, human resources, etc.) to implement them.
	8	3-2	Appropriately separate the parts of cybersecurity measures to be handled by the organization and the parts to be outsourced.
	9	3-3	Clarify the system required for its own organization, systematically securing, and training cybersecurity personnel, and considering appropriate treatment of such personnel.
	10	3-4	Implement cybersecurity knowledge and skill acquisition for personnel responsible for “plus security.”
	11	3-5	Regarding the part to be outsourced, select, and utilize appropriate external resources in consideration of its own issues, budget, location, etc.
Direction 4 Identify cybersecurity risks and develop plans to address them	12	4-1	Identify digital environments, services, and information to be protected and prioritizes countermeasures based on location, business value, etc. of the assets.
	13	4-2	Identify cyber threats and vulnerabilities to the digital environment, services, and information to be protected, and understand how cybersecurity risks from these threats impact the company's business.
	14	4-3	Develop a risk response plan based on the results of the risk assessment and the degree of impact of cybersecurity risks.
Direction 5 Establish systems to effectively address cybersecurity risks	15	5-1	Perform asset management, configuration management, and patch management for critical systems.
	16	5-2	Measure to prevent the use of shadow IT within the organization.
	17	5-3	Conduct a risk assessment at the time of system design, and necessary security functions are specified and implemented during development.
	18	5-4	Implement multiple technical measures for terminals, servers, etc. used for important operations.
	19	5-5	Implement multiple technical measures in the network for important operations.
	20	5-6	Establish and implement vulnerability countermeasure plans, such as periodic vulnerability assessments, continuous patching, and other mitigation measures for systems, etc.
	21	5-7	Collect and analyze logs from terminals and networks.
	22	5-8	Implement incident response mechanisms, such as blocking communications when a cyberattack is detected.
	23	5-9	Implement an incident management system.

Directions	#		Item
	24	5-10	Conduct cybersecurity trainings and exercises for employees.
Direction 6 Implement a PDCA cycle for cybersecurity measures	25	6-1	Define KPIs for cybersecurity operations management.
	26	6-2	Management regularly receives reports on the implementation status of cybersecurity measures, discusses them, and instructs measures to be taken.
	27	6-3	Conduct cybersecurity audits and reviewing cybersecurity measures based on the results in a timely manner.
	28	6-4	Communicate with stakeholders on the status of cybersecurity risk countermeasures.
Direction 7 Develop a cybersecurity incident response team and relevant procedures	29	7-1	Define an incident response plan that considers the entire supply chain.
	30	7-2	Implement a dedicated team (CSIRT, etc.) that can respond to incidents.
	31	7-3	Define the content and timing of information to be shared, reported, and disclosed outside the organization.
	32	7-4	Regularly conduct emergency response exercises in the event of an incident.
	33	7-5	Define an implementation plan to promptly analyze and investigate logs in the event of an incident, and to identify the scope of impact.
Direction 8 Develop a recovery team and relevant procedures in preparation for damage due to cyber incidents	34	8-1	Develop a plan for restoring operations that considers the entire supply chain in the event of damage.
	35	8-2	Conduct periodic recovery response exercises.
Direction 9 Understand cybersecurity status and measures in the entire supply chain including business partners and outsourcing companies	36	9-1	Understand the status of countermeasures against cybersecurity risks in transactions and cooperation with group companies.
	37	9-2	Confirm that appropriate measures are taken based on the roles and responsibilities related to cybersecurity risks agreed upon in contracts with contractors and other business partners.
	38	9-3	Ensure that cybersecurity risks do not exceed acceptable levels throughout the supply chain that affects the company's business.
Direction 10 Gather, utilize and provide cybersecurity related information through information sharing activities	39	10-1	Share information by obtaining alert information provided by related organizations and participating in industry security communities, etc., and apply the information to its own measures.
	40	10-2	Share information to related organizations and communities when incidents of malware infection, unauthorized access, etc. occur, and provide through appropriate public announcements, etc.

In addition, the following appendices are provided in the Cybersecurity Management Guidelines. [8]

- Appendix A Check sheet of cybersecurity management

[8]Ministry of Economy, Trade and Industry: "Cybersecurity Management Guidelines Ver 3.0" (March 2023)
https://www.meti.go.jp/policy/netsecurity/mng_guide.html (in Japanese)
The English version of the previous version can be accessed https://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v2.0_en.pdf

- Appendix B Reference information on cybersecurity
- Appendix C Items to organize within the organization for the occurrence of incidents
- Appendix D In relation to standards, frameworks, etc.
- Appendix E Definition of terms
- Appendix F Guidebook for establishing cybersecurity systems and securing necessary human resources

● **Basic measures (1)(b) "Information Security Measure Guidelines for Small and Medium-sized Enterprises, third edition (IPA)"**

① Target

Small and medium enterprises and small businesses (including corporations, sole proprietors, and various organizations)

② Overview

This is a summary of guidelines that management should be aware of and implement when working on information security measures, as well as the procedures and methods for implementing measures within the company. As shown in Table 3-4, the guidelines consist of the Management Edition and the Practice Edition.[9]

Table 3-4 Structure of the Information Security Measure Guidelines for Small and Medium-sized Enterprises, Third Edition (IPA)

Structure		Overview
Main part	Part 1 Management Edition	Explains matters that management should know and think about at their own risk.
	Part 2 Practice Edition	For those who practice information security measures, this section provides a detailed step-by-step explanation on how to proceed with the measures.
Appendix	Appendix 1 Five Articles on Information Security	The important measures that must be implemented regardless of the size of the organization are summarized and explained in five articles.
	Appendix 2 Information Security Policy (Sample)	A sample of a basic policy of an organization on information security.
	Appendix 3 Five-Minute Information Security Self-Diagnosis.	A 25-item checklist that can be effectively executed without much expense.
	Appendix 4 Information Security Handbook (Template)	A template of a handbook created for dissemination of measures to employees.
	Appendix 5 Information Security Related Regulations (Sample)	A sample document of internal rules on information security.
	Appendix 6 Guidance for Safe Use of Cloud Services by Small and Medium-Sized Enterprises	A guide to using cloud services safely. A 15-item checklist is attached.

[9] Information-Technology Promotion Agency, Security Center: "Information Security Measure Guidelines for Small and Medium-sized Enterprises" (March 2021) https://www.ipa.go.jp/security/keihatsu/sme/guideline/ (in Japanese)

Structure		Overview
	Appendix 7 Risk Analysis Sheet	The possibility of damage (risk) can be examined based on information assets, and status of threats and measures.

＜Part 1: Management Edition＞

The contents are consistent with the Cybersecurity Management Guidelines. For example, as shown in Table 3-5, the Management Edition describes the "three principles" that management needs to recognize, and the "seven important initiatives" that need instructions from management for implementation.

Table 3-5 Three Principles and Seven Important Initiatives of the Information Security Measure Guidelines for Small and Medium-sized Enterprises, Third Edition (IPA)

"Three principles" that management needs to recognize	"Seven important initiatives" to be implemented
Promote information security measures under management leadership.	Establish an organization-wide response policy related to information security.
	Secure budgets, human resources, etc. for information security measures.
	Have the necessary measures examined and give instructions on their execution.
	Instruct a review of the information security measures as appropriate.
	Establish systems for emergency response and recovery.
Consider the information security measures of outsourcing companies as well.	Clarify security responsibilities when outsourcing or using outside services.
Always communicate with stakeholders about information security.	Gather the latest trends related to information security.

＜Part 2 Practice Edition＞

It is explained in a structure to allow leveling up step-by-step according to the level of the enterprise.

③ Key points for utilization

One of the targets of utilization is to get a perfect score in the "Step 2: in-house assessment of information security." By utilizing the "Information Security Related Regulations" (see Table 3-6) in the appendix, one's own security-related regulations can be formulated relatively easily.

Table 3-6 Structure of Appendix 5: Information Security Related Regulations (Sample)

	Name	Overview
1	Organizational measures	Establish rules for the construction and inspection of management systems and information sharing for information security.

	Name	Overview
2	Personnel security	Establish rules for responsibilities and training of the director and employees, and human resource development.
3	Information asset management	Establish rules for managing, taking out, backing up, and destroying information assets.
4	Access control and authentication	Establish access control policies and authentication rules for information assets.
5	Physical security	Establish rules such as settings for security area and precautions within the area.
6	Use of IT equipment	Establish rules for the use of IT equipment and software, etc.
7	IT infrastructure operation management	Establish rules for IT infrastructure such as servers and networks.
8	System development and maintenance	Establish rules for information systems developed and maintained independently.
9	Outsourcing management	Establish rules for selection, contracts, and evaluation for outsourcing. Examples of clauses relating to confidentiality in outsourcing agreements and samples of outsourcing checklists are attached.
10	Information security incident response and business continuity management	Establish rules for incident response and business continuity management related to information security.
11	Handling of individual numbers and specific personal information	Establish rules for the handling of My Numbers.

● **Basic measures (1)(c) "ISO/IEC 27001 (Information Security Management System)"**

① Target

The scope of application can be freely determined by organizational units, business units, physical units, etc.

② Overview

ISO/IEC 27001 (Japan standard JIS Q 27001) is a standard that defines the requirements for information security management systems (ISMS). The standard has been created to provide requirements for organizations to establish, implement, maintain, and continuously improve ISMS.

In order for a company to obtain ISMS certification in which a third-party certification body examines and certifies whether an information security management system is appropriately operated and managed based on ISO/IEC 27001, the company is required to apply to the ISMS certification body and undergo an examination. An interim examination (surveillance review) is required at least once a year and a full examination (recertification review) every three years even after the initial examination to maintain certification. [10]

[10] ISMS Accreditation Center (ISMS-AC): "What is ISMS (Information Security Management System)?"
https://isms.jp/isms/index.html
ISMS Accreditation Center (ISMS-AC): "List of ISMS certificated organizations" (July 2021)
https://isms.jp/lst/isr/

③ Key points for utilization

Although obtaining certification is not necessary when utilizing ISO/IEC 27001, ISMS certification is an objective proof of trust as the company has been audited by a third party.

● **Basic measures (1)(d) "Cybersecurity Framework Ver1.1 (NIST)"**

① Target

Although designed for critical infrastructure, organizations in any field can use the standard.

② Overview

In response to Executive Order 13636 "Improving Critical Infrastructure Cybersecurity" (February 2013), Ver 1.0 was developed in 2014, and updated to Ver 1.1 in 2018. The framework consists of three elements: Framework Core, Framework Implementation Tiers, and Framework Profiles. [11]

The "Framework Core" is a set of specific cybersecurity measures that are common to all industries and critical infrastructures, and consists of five core functions (Identify, Protect, Detect, Respond, and Recover) and 23 categories. The "Framework Implementation Tiers" is a set of four tiers, showing standards for evaluating at what stage an organization's cybersecurity measures are. The "Framework profiles" describes the "current state (As-Is)" and "what it should be (To-Be)" of the organization's cybersecurity measures.

③ Key points for utilization

NISTIR 8270 (2nd Draft) "Introduction to Cybersecurity for Commercial Satellite Operations," an introduction to security for commercial satellite operations, provides a practical example of a Cybersecurity framework for low earth orbit small satellite platforms (see Table 3-7).[12]

Table 3-7 Practical example of a cybersecurity framework for low earth orbit small satellite platforms

Seven steps to Implementing NIST CSF	Case study (low earth orbit small satellite vehicle)
STEP 1: Establish Scope and Priorities	Assumed that the enterprise owns and manages only the operations part of a satellite platform. Ultimately, various products and services used outside of the space sector will be compared using the target profile (cybersecurity requirements for the company's satellite platform) to be created.
STEP 2: Orient	List cybersecurity events caused by potential threats and their business impact (original p14 Table 1).

[11]NIST: "Framework for Improving Critical Infrastructure Cybersecurity Version 1.1" https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf
[12]NIST Computer Security Resource Center: "Introduction to Cybersecurity for Commercial Satellite Operations (2nd Draft)" (February 2022)
https://csrc.nist.gov/publications/detail/nistir/8270/draft

Seven steps to Implementing NIST CSF	Case study (low earth orbit small satellite vehicle)
STEP 3: Create a current profile	Review the NIST CSF subcategories and select the ones currently implemented. Create a list of subcategories that have been implemented (current profile).
STEP 4: Conduct a risk assessment	Consult with organizations such as DHS and DoD and join industry ISACs, which act as a forum for sharing/receiving high-priority information on risk. Prepare to establish a risk response system in a cost-effective manner referring to NIST SP 800-30, etc.
STEP 5: Create a target profile	Create a target profile (original p25 Table 5) consisting of expected outcomes, required subcategory items, etc.
STEP 6: Determine, analyze, and prioritize gaps.	Identify gaps between current and target profiles and add/update the action plan.
STEP 7: Implement action plan	The security department manager presents the action plan to key stakeholders for approval. Present the business case and resource requirements to executives for approval of the action plan. The monitoring and review process for the implementation of the action plan will ensure that the actions sufficiently address the risks in the satellite operations, and that the current and target profiles can be updated in the future and surveillance on external service providers can be maintained.

Attachment 2 of the guidelines summarizes the correlation between the NIST CSF subcategories and specific measures for space systems of Sections 3.2.2 to 3.2.5. It is recommended to use this attachment as a reference when implementing the measures.

● **Basic measures (1) "SP 800-171 (NIST)"**

① Target

The U.S. DoD, in its DFARS (252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting), requires that contracts containing controlled unclassified information (CUI) include cybersecurity measures equivalent to NIST SP 800-171 (Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations). The consignee determines whether the information necessary for the work of the subcontractor is CUI, and requests protection based on DFARS Clause 252.204-7012 when applicable.

② Overview

SP 800-171 consists of the following 14 families (categories) and 110 items.

- Access control: Restricting the users/functions that can access the systems
- Awareness and training: Adhering to security policies
- Audit and accountability: Ability to audit the systems and pursue accountability

- Configuration management: Establishing the security configuration settings required for the devices constituting the systems
- Identification and authentication: Identifying system users and devices
- Incident response: Ability to track and report incidents
- Maintenance: Performing maintenance of an organization's systems
- Media protection: Securely storing CUI and limiting who can access it
- Personnel security: Screening individuals who access the systems
- Physical protection: Limiting physical access to an organization's systems, devices, etc.
- Risk assessment: Appropriately evaluating the risk to information assets
- Security assessment: Evaluating security control measures on a regular basis
- System and communications protection: monitoring, Monitoring, controlling, and safeguarding the systems' key communications
- System and information integrity: Identifying information and system flows in a timely manner

③ Key points for utilization

Consideration should be given to the fact that direct contracts with DoD and contracts with DoD contractors are subject to this regulation.

Column: CMMC (Cybersecurity Maturity Model Certification)

The US DoD Office of the Under Secretary of Defense (OUSD) for Acquisition and Sustainment developed CMMC, which is a new certification system framework using a 5-stage maturity model, based on the recognition that uniformly requiring SP 800-171 for all supply chains, including SMEs, made compliance impractical. Ver. 1.0 was established in January 2020. Ver. 2.0 was released in November 2021, and the 5-stage maturity model was revised to a 3-stage maturity model.

CMMC is designed such that each business including SMEs can receive certification from certified third-party assessment organizations (C3PAO) for the ability to appropriately safeguard information at each level (Level 1 to 3) commensurate with risk, considering the flow down to subcontractors in the supply chain. Level 1 (foundational) requires 17 federal contract information (FCI) protection measures as stipulated in Federal Acquisition Regulation 48 CFR 52.204-21, level 2 (advanced) requires 110 measures equivalent to NIST SP 800-171, and level 3 (expert) requires measures equivalent to SP 800-172 (targeted attack countermeasures). The latest information on CMMC is provided by DoD OUSD[13].

[13]DoD Office of the Under Secretary of Defense for Acquisition and Sustainment: "Cybersecurity Maturity Model Certification" (December 2020) https://www.acq.osd.mil/cmmc/index.html

3.1.2 Cloud Security Measures

Requirements

When utilizing external services, select services that meet the security requirements and service level agreements (SLAs) appropriate to the laws, regulations, and mission, etc.

[Basic Measures]

(1) The principal laws and regulations concerning external services for the space industry are as given below, and services should be selected after confirming that the external service providers comply with the laws and regulations.

(a) Regulation for Enforcement of the Act on Ensuring Appropriate Handling of Satellite Remote Sensing Data

(2) The principal certifications concerning external services for the space industry include (a) to (c) given below, and services with an appropriate security level should be selected.

(a) ISO/IEC 27017 Code of practice for information security controls based on ISO/IEC 27002 for cloud services (ISO/IEC)

(b) Information System Security Management and Assessment Program (ISMAP) (Cabinet Secretariat, MIC, METI)

(c) The Federal Risk and Authorization Management Program (FedRAMP)

(Details)

● **Basic measures(1)(a) "Regulation for Enforcement of the Act on Ensuring Appropriate Handling of Satellite Remote Sensing Data"**

As for the part relevant to the external services under the "Regulation for Enforcement of the Act on Ensuring Appropriate Handling of Satellite Remote Sensing Data," it is necessary to pay attention to the restrictions on countries or regions where records are stored, as shown in Table 3-8. As countries or regions subject to restrictions change depending on the international situation, it is necessary to check on a case-by-case basis. For the required security requirements regardless of cloud, refer to "3.2.1 Measures Required by Law".

Table 3-8 Regulation for Enforcement of the Act on Ensuring Appropriate Handling of Satellite Remote Sensing Data

Article 7 (2) If a Satellite Remote Sensing Instruments User and Satellite Remote Sensing Data Holder manages the business of handling of Satellite Remote Sensing Data, in whole or part, by the use of external storage service through telecommunication lines, it must expressly provide for the following matters in a contract with the business providing the service (hereinafter referred to as a "service provider" in this paragraph) relating to the use of the service. (ii) that Satellite Remote Sensing Data is not to be stored on a computer located in any of the following countries or regions:

(a) the regions specified in Appended Table 3-2 or 4 of the Export Order; or
(b) the countries or regions determined by a resolution of the United Nations General Assembly or Security Council as being responsible for the occurrence of situations threatening the peace and security of the international community;

Table 3-9 Regions listed in Appended Table 3-2 of the Export Order

Afghanistan, Democratic Republic of the Congo, Cote d'Ivoire, Eritrea, Iraq, Lebanon, Liberia, North Korea, Sierra Leone, Somalia, and Sudan

*As of January 23, 2023

Table 3-10 Regions listed in Appended Table 4 of the Export Order

Iran, Iraq, North Korea

*As of January 23, 2023

● **Basic Measures(2)(a) "ISO/IEC 27017 Code of practice for information security controls based on ISO/IEC 27002 for cloud services (ISO/IEC)"**

① Target

Cloud services

② Overview

ISMS cloud security certification certifies that the ISMS (information security management system) conforming to JIS Q 27001:2014 (ISO/IEC 27001:2013), has implemented the management measures specific to cloud services stipulated in ISO/IEC 27017:2015, an international standard for cloud services, for the provision or use of cloud services included within the scope of the system. As shown in Figure 3-3, the prerequisite for obtaining ISMS cloud security certification is to obtain ISO/IEC 27001:2013, and it is necessary that ISO/IEC 27017:2015 is properly implemented as a management measure specific to cloud services[14].

Please also refer to 3.1.1(c)ISO/IEC 27001 (Information Security Management System).

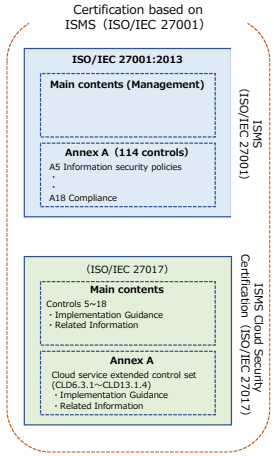


Figure 3-3 Relationship between ISMS (ISO/IEC 27001) and Cloud Security certification (ISO/IEC 27017)[1]

[14]JIPDEC ISMS Accreditation Center: "ISMS Conformity Assessment Scheme (ISMS Cloud Security Certification Based on ISO/IEC 27017:2015)" (August 2016) https://isms.jp/isms-cls/about-cls.pdf (in Japanese)

● **Basic Measures(2)(b) "Information System Security Management and Assessment Program (ISMAP) (Cabinet Secretariat, MIC, METI)"**

① Target

Cloud service

② Overview

It is a certification standard for promoting the use of cloud services in government information systems, in which the uniform standard for information security measures for government agencies, etc. and security requirements of NIST SP 800-53 (Moderate) have been supplemented based on ISO/IEC 27001 (the domestic standard is JIS Q 27001), etc.

● **Basic Measures(2)(1)(c) "The Federal Risk and Authorization Management Program (FedRAMP)"**

① Target

US Cloud Services

② Overview

The Federal Risk and Authorization Management Program (FedRAMP) is a US government-wide program that provides a standard approach to security assessment, certification, and continuous monitoring of cloud products and services. It is based on the security controls of NIST SP 800-53 and has Low, Moderate, and High baselines. When it comes to national security, there is a more stringent program called FedRAMP+.

3.1.3 Measures for Remote Working

Requirements
When remote working, maintain the environment and organize the regulations for performing safe operations.

[Basic Measures]

(1) Existing guidelines, including the (a) and (b) given below are preferred to be used for safe remote working operations.

(a) Telework Security Guidelines (fifth edition) (MIC)

(b) Telework Security Guidelines for SMEs (Checklist), third edition (MIC)

(Details)

● **About basic measures(1)(a) "Telework Security Guidelines (fifth edition) (MIC)"**

① Target

Businesses implementing or considering remote working (including corporations, sole proprietors, and various organizations)

② Overview

The measures provide ideas and examples of security measures for introducing remote working ("teleworking" is also used for the same meaning in Japan), as a guideline to eliminate security concerns when enterprises implement remote work, and to introduce and use remote working with peace of mind. Table 3-11 shows the structure of the security guidelines.[15]

Table 3-11 Structure of Telework Security Guidelines (fifth edition) (MIC)

Chapters	Overview
Chapter 1. Introduction	Describes the background and purpose of these guidelines, forms of telework, intended audience, etc.
Chapter 2 Points to Consider when Telework	Describes in detail the need to implement measures with a good balance of "rules," "people," and "technology," and the importance of appropriate division of roles between "managers," "system security managers," and "people working from home" and the roles of each position, when promoting security measures in telework. Also, describes the ideas for the use of cloud

[15] Office of the Director-General for Cybersecurity in the Ministry of Internal Affairs and Communications of Japan: "Telework Security Guidelines (fifth edition)" (May 2021) https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/ (in Japanese)
The English version of the previous edition can be accessed https://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/COVID-19/pdf/telework-security-guidelines.pdf

Chapters	Overview
	services and zero trust security, considering the recent changes in the environment surrounding telework and security trends.
Chapter 3 Description of Telework Methods	Organizes telework methods into seven types, and in addition to the basic configuration, shows the derivative configurations for each method, and security considerations specific to each method. (Security measures common to each method are described in Chapter 4 and Chapter 5). The chapter also provides a flowchart and a table comparing the characteristics of each method that can be used as a reference when selecting a suitable method based on the content of the work to be realized through telework, the ease of security control, etc.
Chapter 4 List of Security Measures for Telework	Gives a list of "basic measures" for the positions of "manager," "system security manager," and "person working from home," which are generally prevalent as security measures for telework and are required to be essentially implemented, and "advanced measures" that are difficult to implement unless a certain budget and organizational structure are in place but are expected to further improve security through implementation. Also organizes each security measure into 13 categories.
Chapter 5 Description of Security Measures for Telework	Gives a detailed description of each security measure described in Chapter 4.
Chapter 6 Examples of Problems and Measures for Telework	Describes security considerations and which security measures in the guidelines are effective, after introducing specific examples of security-related problems in telework.

③ Key points for utilization

In the guidelines, security measures are organized into 13 categories shown in Table 3-12. Furthermore, security measures are classified into basic measures and advanced measures, as a reference for prioritization (degree of difficulty in implementation). In addition, measures to be implemented by managers, system security managers, and people working from home are shown, and each measure is explained. This makes it possible for companies to formulate their own security regulations for telework relatively easily.

Table 3-12 Categories for Organizing Security Measures

	Measure category	Description
A	Governance and risk management	Measures related to risk management and the establishment of information security regulations (rules), etc., when implementing telework.
B	Asset and configuration management	Measures related to identification of assets such as hardware and software used for teleworking and management thereof.
C	Vulnerability management	Measures related to elimination of known vulnerabilities by implementing software updates, etc.
D	Privilege management	Measures to protect system administrator rights in case of unauthorized access, etc.

	Measure category	Description
E	Data protection	Measures related to identification of information (data) to be protected and ensuring the confidentiality and availability of stored data.
F	Malware prevention	Measures related to prevention and detection of malware infection and endpoint security.
G	Protection and encryption of communications	Measures to ensure the confidentiality and availability of data in communications.
H	Account and authentication management	Measures related to account management and authentication methods for accessing information systems.
I	Access control and authorization	Measures related to restricting access to data and services only to those with the minimum necessary and valid rights.
J	Incident response and log management	Measures related to quick response to security incidents and logging and investigation.
K	Physical security	Measures related to protection from information leakage etc. by physical means.
L	Threat intelligence	Measures related to the collection of information on threat trends, attack methods, vulnerabilities, etc.
M	Training	Measures to raise the understanding and awareness of security among those working from home.

Column: Concept of Zero Trust Security

In recent years, as cyberattacks are becoming more sophisticated, a new approach to security, "zero trust security," has been attracting attention.

Telework Security Guidelines (fifth edition) (MIC) describes "zero trust security" as follows.

Zero trust security indicates the concept of enhancing security for units of data and devices, based on the idea that there is a limit to the protection provided by the boundary (boundary-based security) between the external network (Internet) and the internal network (LAN), and that threats can also exist within the internal network.

If the premise of the traditional boundary-based security is "trust, but verify," then, in contrast, the premise of zero trust security is "never trust, always verify."

Although there are various theories on the requirements for achieving zero trust security according to the reference literature [16], the following concepts are characteristic of all the theories.

- Consider security in terms of the smallest units of data, devices, etc., without distinguishing between the inside and outside of a network
- Implement strong user authentication and strict access control
- Place no environmental constraints (such as location, terminal) when it comes to security measures

[16] Literature, etc. citing the concept of zero trust security
1) NIST: "NIST Special Publication 800-27 Zero Trust Architecture" (August 2020) https://csrc.nist.gov/publications/detail/sp/800-207/final
2) Google: "Beyond Corp"
3) Forrester: "Zero Trust eXtended (ZTX) Ecosystem Providers"
4) Discussion Paper: "Approach to Zero Trust deployment in Japanese Government Information System" (June 2020) https://cio.go.jp/node/2714/index.html (in Japanese)

● **Basic Measures(1)(b) "Telework Security Guidelines for SMEs (Checklist), third edition (MIC)"**

① Target

Persons in charge of SMEs etc. where budgets, security systems, etc. are not necessarily sufficient

② Overview

As a supplement to "Telework Security Guidelines (fifth edition) (MIC)", this manual provides specific security measures that are easy to implement and should be implemented on a priority basis even by SMEs. The structure of this manual is shown in Table 3-13. In addition, the manual organizes teleworking methods into eight methods and describes the corresponding measures. [17]

Table 3-13 Structure of Telework Security Guidelines for SMEs (Checklist), Third Edition (MIC)

Structure	Overview
Quick reference index	This section shows the pages of this manual addressing the teleworking security-related questions.
Table of contents	A detailed table of contents of this manual.
Introduction	After clarifying the purpose and intended audience of this manual, this section describes its overall and how to use it.
Part 1	
1. Forms of telework	This section shows the classification of work styles according to the location where work is carried out.
2. What is your method of telework?	Assuming a teleworking usage scenario, the method of teleworking that has been (or is planned to be) introduced can be confirmed using a flowchart.
3. Overview of telework methods	This section gives an overview of the methods of teleworking handled in this manual.
4. Description of telework methods	This section describes in detail each method of teleworking handled in this manual.
Part 2	
1. Checklist of telework security measures	Security measures that should be implemented for each method of teleworking are shown in the form of a "checklist."
2. List of examples of settings for the measures in the checklist	This section introduces a "document to explain settings" that explains how to configure and use products often used for teleworking.
3. List of security measures	In addition to the "checklist" presented in a list format, details of anticipated threats for each security measure are also provided.
References	
1. Threats targeting teleworking environments	This section describes anticipated threats in a teleworking environment.

[17] Office of the Director-General for Cybersecurity in the Ministry of Internal Affairs and Communications of Japan: "Telework Security Guidelines for SMEs (Checklist) (second edition) (May 2021)" https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/ (in Japanese)

Structure	Overview
2. Effective security measures for teleworking	This section describes effective security measures for avoiding threats in a teleworking environment.
3. Keywords you should know	Important keywords for security measures appearing in the checklist of security measures for teleworking are explained in detail using illustrations.
4. Glossary	Explanation of the main terms used in this manual.
5. Links	Links to documents, websites, etc. that can be used as references when utilizing the checklist of measures.
Appendix (attached sheet)	
Employee handbook	Contains information that employees working from home should always repeat and be aware of, as well as contact information in case of emergency. Employees working from home are required to use this handbook distributed to them.
Emergency response card (sticker)	Describes what actions should be taken by employees working from home with a top priority in the event of a problem. The card is distributed to employees working from home, and they are asked to make use of this card by affixing on devices used while working from home, such as their PCs.

③ Key points for utilization

If the contents of measures corresponding to the eight methods (Method (1) company-provided device, VPN/remote desktop method; Method (2) company-provided device, cloud service method; Method (3) company-provided device, standalone method; Method (4) company-provided device, secure browser method, Method (5) personally owned device, VPN/remote desktop method; Method (6) personally owned device, cloud service method; Method (7) personally owned device, standalone method; and Method (8) personally owned device, secure browser method) are utilized based on priority, it is relatively easy to implement teleworking measures in the company.

3.1.4 Measures for Internal Improprieties

Requirements
Consider measures for the prevention and early detection of internal improprieties.

[Basic Measures]

(1) Using the existing standards including (a) given below to address internal improprieties is preferred.

(a) Guidelines for the Prevention of Internal Improprieties in Organizations (fifth edition) (IPA)

(Details)

● **Basic Measures (1)(a) "Guidelines for the Prevention of Internal Improprieties in Organizations (fifth edition) (IPA)"**

① Target

All organizations

② Overview

The guidelines focus on preventing internal improprieties in an organization, from the perspective of early detection and prevention of subsequent expansion.

③ Key points for utilization

Appendix VI: Utilizing 5 basic principles and 25 categories (see Table 3-14) for prevention of internal improprieties makes it relatively easy for a company to formulate its own rules for the preventing internal improprieties. Also, utilizing the internal improprieties check sheet (see Table 3-15) makes it possible to grasp the status of measures against internal improprieties in one's own organization.

Table 3-14 Appendix VI: Five basic policies and twenty-five classifications to prevent internal improprieties

5 basic principles and 25 classifications	Examples of measures	Main measures
Make crimes difficult (make harder to attempt): Strength countermeasures to make criminal activities difficult to conduct.		
Strength countermeasures	Access control, password policy setting, revocation of resignees' IDs, fixing PCs with security wires	(5)(6)(7)(9) (14)(21)
Restrict entering/exiting facilities	Restriction of outsiders entrance, entrance/exit control	(8)
Check at exit points	Checks for taking out of laptop PCs, etc., monitoring e-mails and networks	(8)(10)(17)(18)
Block criminals	Restriction of entrance/exit based on physical levels	(8)
Restrict information devices and networks	Prohibition against unauthorized bringing-in of PCs/USB storages, Restriction of uses of SNSs, uses of wireless LANs in hotels and public wireless LANs	(11)(12)(15)
Raise risks to be caught (detected if committed): Strength management and surveillance to raise risks to be caught.		
Strength monitoring	Monitoring of access logs, working environment with multiple workers, information devices inventory, mobile devices management, monitoring of entrance/exit records	(6)(8)(9)(10) (17)(18)(30)
Support natural surveillance	Development of reporting system	(29)
Reduce anonymity	ID management, Removal of shared accounts, property management based on ledgers	(7)(9)(10)
Implement operational managers	Restriction of one-man works	(26)
Strength physical surveillance system	Setting up of surveillance cameras, Implementation of mechanical security systems	(8)
Reduce rewards from crimes (not worth doing): Hide or remove targets, or make it unprofitable to prevent crimes.		
Hide targets (Unknown whereabouts)	Authorization of access rights, mobile devices storage with locks, application of privacy protection films	(5)(6)(9)(15)
Eliminate targets (Eradicate existences)	Complete data deletion, physical destruction of record media, etc., disposal /deletion of information provided to persons involved	(4)(9)(13)(21)

5 basic principles and 25 classifications		Examples of measures	Main measures
	Specify properties	Property management for information devices and record media	(9)
	Decimate the market	Immediate reporting to police, (compliance to legal systems)	(27)
	Make it unprofitable	Encryption of electronic files, hard disks, telecommunications	(12)(13)(14)(15)
Reduce seduction of crimes (not to motivate): Deter crimes by dampening enthusiasm to commit crimes.			
	Reduce discontent or stress	Promotion of impartial personnel evaluations, appropriate working environment, smooth communication	(24)(25)
	Avoid conflict	Promotion of impartial personnel evaluations, appropriate working environment, smooth communication	(24)(25) (29)
	Control emotions	Promotion of impartial personnel evaluations, appropriate working environment, smooth communication	(24)(25)
	Mitigate pressure from co-workers	Promotion of impartial personnel evaluations, appropriate working environment, smooth communication	(25)
	Block copycat crimes	Recurrence prevention measures (Being careful to disclose the ways of incidents)	(28)
Not allow justification of crimes (not allow to excuse): Get rid of reasonings for criminals' self-justification of their activities.			
	Decide rules	Development of basic policies, management and operation methods, services contracts, employment regulations	(1)(2)(16)(20) (22)(27)
	Post instructions	Posting of basic policies inside and outside organizations, education about the policies for employees	(1)(2)(19)
	Appeal to conscience	Indication of management levels, signing of pledges, posters for ban on bringing in personal devices	(3)(4)(11)(19) (20)(23)
	Support compliance	Education of compliance items and related laws	(19)(22)(23)
	Regulate drug, alcohol	(Ban on drinking alcohol in workplaces, restriction of alcohol when holding important information)	-

Table 3-15 Internal Impropriety Check Sheet

No.	Content
Basic Policies	
1-1	Has the top manager formulated “basic policies” and disseminated these to officers and employees, for the purpose of showing within and outside the organization that internal impropriety countermeasures are the responsibility of the top manager? (See Appendix IV for examples of basic policies.)
1-2	Has the top manager made necessary decision and instruction to secure resources for implementing measures based on “basic policies”?
2-1	Has the top manager appointed a Supervising Manager for internal impropriety countermeasures, and is the top manager conducting approvals for management systems and implementation measures? (However, if the organization is one in which the top manager has a view of the entire organization and implements internal impropriety countermeasures on his or her own, it may not be necessary to construct management systems.)
2-2	Has the Supervising Manager constructed cross-organizational management systems in accordance with the basic principles, and formulated implementation measures?
Designation as Confidential	
3	Does the organization assess important information, assign it rating categories according to degree of importance, and set the scope of insiders allowed to handle the information?
4-1	Do creators of important information select an established rating category for the information, and obtain confirmation of the selection from superiors, etc.?
4-2	Are confidentiality marks, etc. understandable by insiders displayed on electronic documents containing important information?
Designation of Access Rights	
5-1	Do persons in charge of administering and operating information systems do so with procedures established for registration, change, deletion, and other settings concerning user IDs and access rights?
5-2	Do persons in charge of administering and operating information systems promptly delete user IDs and access rights that have become unnecessary due to transfer or retirement?
6	When there are multiple system administrators, does the organization assign an appropriate scope of rights for each system administrator ID and enable information system administrators to monitor each other? In addition, when only one person in the organization is in charge of the system administrator, does the organization monitor the administrator' operations through logs etc.?
7	Does the organization perform authentication using individual passwords, IC cards, etc. for individual users and system administrators, without using shared IDs, shared passwords or shared IC cards, etc.?
Physical Management	
8	Does the organization physically protect locations where important information is stored, handled, etc. with walls and entry/exit management measures?
9-1	Does the organization manage and protect information devices such as PCs and portable storage media such as USB storage to prevent theft, improper removal from the premises, etc.?
9-2	When disposing of information devices or storage media, does the organization confirm that important information has been completely deleted?
10	When mobile devices and portable storage media are taken from the premises, does the organization manage the approval, recording, etc. of the removal?
11	Does the organization restrict employees' bringing in and using personal mobile devices and storage media for work?

	Technological and Operational Management
12	Does the organization restrict the use of file sharing software, SNS, external online storage, etc. on its networks, to prevent improper removal of important information?
13-1	Does the organization manage the transfer of important information to contractors or other parties concerned, at all steps from transfer to disposal?
13-2	Does the organization take into account the mistaken transfer of important information to persons other than the parties concerned via the Internet or otherwise outside the organization, and protect the important information using encryption, etc.?
14	Does the organization limit the important information that can be used and handled outside the organization, and protect important information and information devices?
15	Does the organization take into account the surrounding environment, network environment, etc. when performing work using important information outside the organization?
16	Does the organization confirm and agree the security measures according to the services to be entrusted prior to the contract agreement, and make sure whether the security measures are practiced as specified in the agreement during the contract period?
	Securing Evidence
17	Does the organization safely protect logs and trails for a fixed period, including the history of access to important information and users' operation history?
18	Does the organization not only record and store logs and trails of the access history, operation history, etc. of system administrators, but also have the content of these periodically checked by persons other than system administrators?
	Human Management
19-1	Does the organization provide education for all the officers and employees, and disseminate policies concerning the organization's internal impropriety countermeasures, procedures for handling important information, etc.?
19-2	Does the organization periodically repeat its education, and periodically review and update its content?
20	At the conclusion of employment, does the organization require employees to submit written pledges imposing confidentiality obligations? (recommended)
21	At the conclusion of officers and employees employment and termination of work contracts with contractors, does the organization have them return or completely delete all information assets which were entrusted to handle, and does the organization delete their user IDs and privileges from information systems?
	Compliance
22	Has the organization prepared rules of employment and other internal rules, and made provisions for official disciplinary proceedings?
23	In order to make obligations to protect important information understood by officers and employees, does the organization request them to submit written pledges of confidentiality etc.?
	Workplace Environments
24	Does the organization promote impartial and objective personnel and performance evaluations as well as provide opportunities to explain how evaluation is carried out in personnel and performance evaluations? (recommended)
25	Does the organization as a whole promote environments that maintain good communication throughout the workplace, such as by preparing systems for promoting mutual work support and environments facilitating consultation, while also preparing suitable work environments through means such as normalization of workloads and working hours? (recommended)
26	Does the organization restrict independent work apart from other employees in environments that disallow mutual monitoring, and has the organization set necessary procedures for prior approval for independent work? (recommended)

	Follow-up Measures
27	In order to identify the scope of the effects of internal improprieties, organizations must assess the concrete status of incidents and must implement measures to minimize damage and prevent the spread of effects. In addition, organizations must secure systems for cooperation with parties concerned inside and outside the organization, as required. Does the organization do so?
28	Has the organization considered punishment for perpetrators of international improprieties, and has the organization considered providing notification of cases of internal improprieties within the organization?
	Organizational Management
29	Has the organization prepared whistleblower systems for the occurrence of incidents suspected of involving internal improprieties, has it established multiple points of contact, and does it secure anonymity for whistleblowers, as required?
30	Does the organization identify internal impropriety countermeasure items, regularly and irregularly conduct checks (including internal and other audits), report the checked results to the top manager, and conduct reviews of countermeasures, as required?

3.1.5 Reporting Incidents to the Outside

Requirements
Report incidents including defects to the external authorities, as necessary.

[Basic Measures]

(1) When an incident occurs in the space system, notifying the competent ministries and agencies, affected organizations, and individuals may be required in accordance with laws, regulations, and rules. For this reason, it is preferred that the stakeholders to whom a report is to be submitted when an incident occurs are identified, and the communication flow is organized.

(Details)

● **Basic Measures (1) "Stakeholders to whom a report is to be submitted when an incident occurs"**

Table 3-16 Examples of whom to report and contact in the event of an incident

Case	Notifier	Notification destination	Laws, regulations, etc. that serve as the basis	Remarks and reference URL
[Required] When, due to a failure of the satellite remote sensing equipment or the Earth-orbiting satellite carrying the satellite remote sensing equipment, or other circumstances, it is no longer possible to use the satellite remote sensing equipment without taking termination measures, and there is no prospect of recovery.	Satellite remote sensing device users	Prime Minister (Cabinet Office)	Act on Ensuring Appropriate Handling of Satellite Remote Sensing Data Article 11 (Measures to be Taken in Case of Fault)	Cabinet Office: "Applying for a License pertaining to Use of Satellite Remote Sensing Instruments and a Certification of Persons Handling Satellite Remote Sensing Data" https://www8.cao.go.jp/space/english/rs/application.html
[Required] When, due to a collision of the satellite with another object, or another accident, the satellite cannot be managed without taking termination	Satellite managers	Prime Minister (Cabinet Office)	Act on Launching of Spacecraft, etc. and Control of Spacecraft Article 25 ((Measures in Case of Accident)	Cabinet Office: "Applying for a Permission Related to the Launching of Spacecraft, etc. and License Related to the Control of Spacecraft" https://www8.cao.go.jp/space/english/activity/application.html

Case	Notifier	Notification destination	Laws, regulations, etc. that serve as the basis	Remarks and reference URL
measures pertaining to the permission under the same paragraph, and there is no prospect of recovery.				
[Required] When a part of telecommunications service is suspended, when communication secrets are leaked, or other serious accidents occur in connection with telecommunications service.	Telecommunications carrier	Minister of Internal Affairs (Ministry of Internal Affairs and Communications)	Telecommunications Business Act Article 28 (Reporting on the Suspension of Telecommunications Operations and on Serious Accidents) Regulations for Enforcement of the Telecommunications Business Law Article 58 (Significant Accidents Requiring Reporting)	Ministry of Internal Affairs and Communications: "Reporting Serious Accidents" https://www.soumu.go.jp/menu_seisaku/ictseisaku/net_anzen/jiko/judai.html (in Japanese)
[Required] When critical infrastructure services are disrupted due to space-related services.	Critical infrastructure operators	Related Ministries * See the link on the right for details	* See the link on the right for details	Cabinet Secretariat, Cabinet Cybersecurity Center: "Guidelines for Establishing Safety Principles for Ensuring Information Security in Critical Infrastructure (fifth edition)" (May 2019) https://www.nisc.go.jp/eng/pdf/principles_ci_eng_v5.pdf
[Required] When there is a contractual reporting obligation, etc.	Affected organization	Contract counterparty	Contracts	-
[Required] When specific personal information (My Number, etc.) is leaked.	Person in charge of affairs using the individual numbers, person in charge of affairs related to the individual	Personal Information Protection Commission, etc.	Response in the event of a leakage, etc. of specific personal information (Specific Personal Information Protection Commission Notice No. 2 of 2015)	Personal Information Protection Commission: "Response in the event of a leakage, etc. of specific personal information" (March 2021) https://www.ppc.go.jp/legal/rouei/ (in Japanese)

Case	Notifier	Notification destination	Laws, regulations, etc. that serve as the basis	Remarks and reference URL
	numbers, etc.			
[Reasonable endeavors] When an incident such as leakage of personal information is discovered.	Business handling personal information	Personal Information Protection Commission, etc.	Response in the event of an incident such as a leakage of personal data (Personal Information Protection Commission Notice No. 1 of 2017)	Personal Information Protection Commission: "Response to leakage, etc. (personal information)" https://www.ppc.go.jp/personalinfo/legal/leakAction/ (in Japanese)
[Optional] When an information security incident occurs at a higher education institution.	General Affairs Department, etc.	Ministry of Education, Culture, Sports, Science and Technology	Sample regulations for information security measures in higher education institutions (2019 edition supplement)	Research Organization of Information and Systems, National Institute of Informatics, Information Security Policy Promotion Working Group at Higher Education Institutions: "Formulation of Information Security Policies for Higher Education Institutions" https://www.nii.ac.jp/service/sp/ (in Japanese)
[Optional] When being a potential cybercrime victim.	Affected organization	Cybercrime consultation desk at each prefectural police headquarters	-	National Police Agency's Cybercrime Countermeasures Project: "List of Cybercrime Consultation Desks at Prefectural Police Headquarters" https://www.npa.go.jp/cyber/soudan.html (in Japanese)
[Optional] When there is a concern about information leakage of sensitive technology (e.g., technology subject to export control under the Foreign Exchange and Foreign Trade Law).	Affected organization	Ministry of Economy, Trade and Industry (Cybersecurity Division or Space Industry Office)	Cautions to Corporate Managers Cybersecurity in Light of Situations of Recent Cyberattacks (Ministry of Economy, Trade and Industry)	Ministry of Economy, Trade and Industry: "Cautions to Corporate Managers Cybersecurity in Light of Situations of Recent Cyberattacks" (December 2020) https://www.meti.go.jp/press/2020/12/20201218008/20201218008-2.pdf (in Japanese) Ministry of Economy, Trade and Industry: "Recognition of the current cybersecurity situation surrounding the industry and the direction of future efforts based on the results of the report on "Caution and Request for Report in the wake of Recent Cyber-Attack Cases" and the project report on the "Pilot Project to Support Reactive Cybersecurity Measures for SMEs (so-called "cybersecurity help team")" (June 2020) https://www.meti.go.jp/press/2020/06/20200612004/20200612004-2.pdf (in Japanese)
[Optional] When there is a threat of a targeted cyberattack.	Affected organization	IPA Security Center (Cyber	-	Information-Technology Promotion Agency, Security Center: "J-CRAT/Targeted Cyberattack special Consultation Desk" (August 2021)

Case	Notifier	Notification destination	Laws, regulations, etc. that serve as the basis	Remarks and reference URL
		Rescue Team (J-CRAT))		https://www.ipa.go.jp/security/tokubetsu/ (in Japanese) Information-Technology Promotion Agency: "J-CSIP & J-CRAT" https://www.ipa.go.jp/english/about/about_1_1.html https://www.ipa.go.jp/security/J-CRAT/index.html
[Optional] When being a victim of a computer virus or unauthorized access.	Affected organization	IPA Security Center	Computer Virus Countermeasures Standard (Ministry of Economy, Trade and Industry) Unauthorized Computer Access Countermeasures Standard (Ministry of Economy, Trade and Industry)	Information-Technology Promotion Agency, Security Center: "Notification of Computer Viruses and Unauthorized Access" (August 2021) https://www.ipa.go.jp/security/outline/todokede-j.html (in Japanese) Information-Technology Promotion Agency, Security Center: "Worry-free Information Security Consultation Service" https://www.ipa.go.jp/security/anshin/ (in Japanese)
[Optional] When vulnerability-related information on software products, etc. is discovered.	Discoverer of vulnerability-related information	IPA Security Center	Rules for Handling Software Vulnerability Information and Others (Ministry of Economy, Trade and Industry Directive)	Information-Technology Promotion Agency: "IPA/ISEC : Information Security Early Warning Partnership" https://www.ipa.go.jp/security/english/about_partnership.html
[Optional] When wishing to obtain support and consultation on incident response.	Affected organization	JPCERT/CC	-	JPCERT Coordination Center.: "Incident Report" https://www.jpcert.or.jp/english/ir/form.html
[Optional] When vendor services, insurance, etc. can be used.	Affected organization	Contract counterparty	Contracts	-

3.2 Specific Measures for Space Systems

3.2.1 Measures Required by Law

Satellite owners	Satellite operators	Ground station service providers	Satellite data platform operators	Satellite data service providers	Satellite developers

Requirements

(1) Comply with the relevant laws and regulations and provide appropriate response throughout the lifecycle. Compliance with the following key laws and regulations (a) to (c), related to the space industry is required to promote the safe usage of space.

(a) Act on Launching of Spacecraft, etc. and Control of Spacecraft

(b) Act on Ensuring Appropriate Handling of Satellite Remote Sensing Data

(c) Foreign Exchange and Foreign Trade Act

(Details)

● **Requirements (1)(a) "Act on Launching of Spacecraft, etc. and Control of Spacecraft"**

① Target

Operation and management of satellites and their launch vehicles

② Overview

From the viewpoint of compliance with space treaties and development of commercial space activities, as shown in Figure 3-4, it is stipulated in this Act that it is necessary to obtain permission for launching satellites, type certification for satellite launch vehicles, compliance certification for launch facilities, permission for the management of satellites, and approval for measures ensuring compensation for damages, etc.

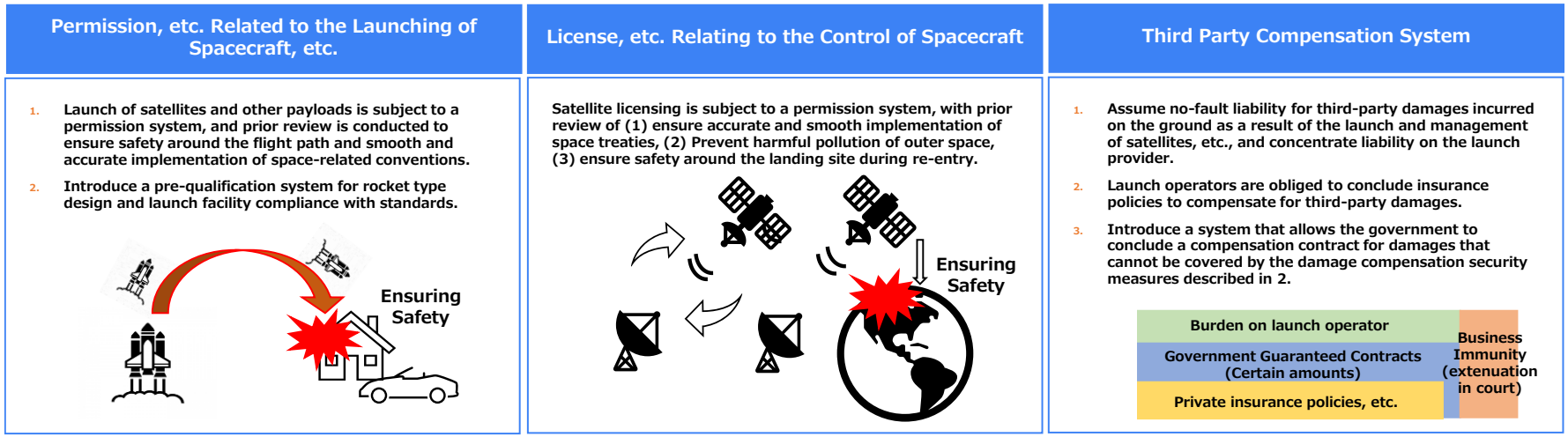


Figure 3-4 Main contents of the Act on Launching of Spacecraft, etc. and Control of Spacecraft[18]

Compliance with laws and enforcement regulations and specific requirements are described in the Appended Table of "Review Standards and Standard Period of Time for Process Relating to Procedures under the Act on Launching of Spacecraft, etc. and Control of Spacecraft."

[18] Space Development Strategy Promotion Secretariat, Cabinet Office: "Space Policy Committee 65th Meeting" (December 2017)
https://www8.cao.go.jp/space/comittee/dai65/gijisidai.html

● **Requirements (1)(b) "Act on Ensuring Appropriate Handling of Satellite Remote Sensing Data"**

① Target

Satellite remote sensing instrument users and satellite remote sensing data holders

② Overview

In order to ensure appropriate handling of satellite remote sensing data, as shown in Figure 3-5, necessary matters such as the license for the use of satellite remote sensing instrument, obligations of satellite remote sensing data holders, and certification for persons handling satellite remote sensing data, are stipulated in this Act. The legal system for each requirement is organized as shown in Figure 3-6. [19]

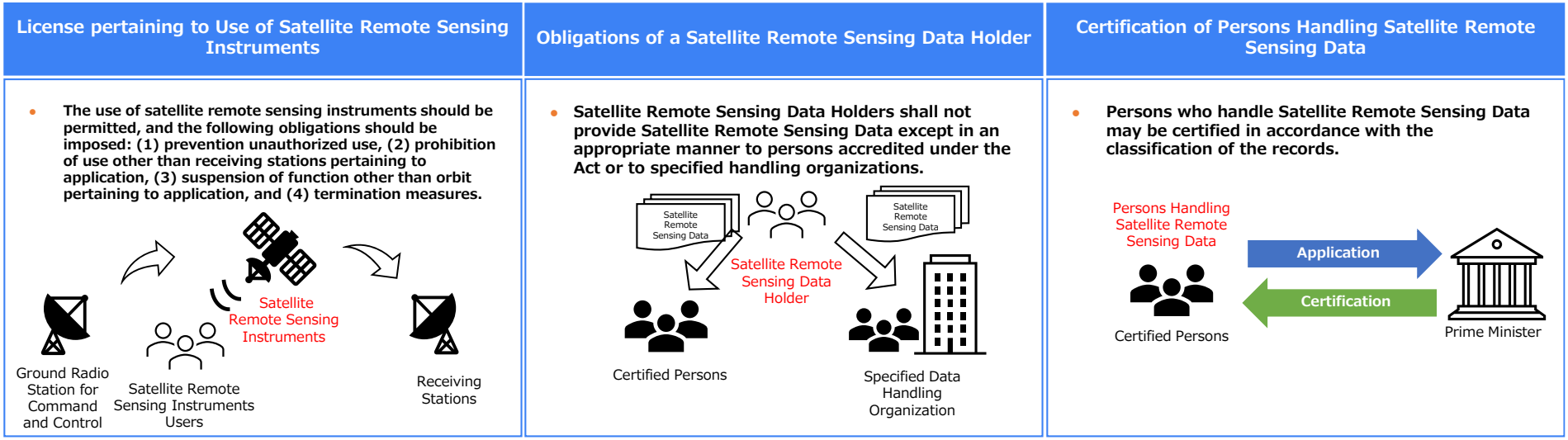


Figure 3-5 Main contents of the Act on Ensuring Appropriate Handling of Satellite Remote Sensing Data[20]

[19] Space Development Strategy Promotion Secretariat, Cabinet Office: "Accepting Applications for 'License for the Use of Satellite Remote Sensing Equipment' and 'Certification for Handling Satellite Remote Sensing Data'
https://www8.cao.go.jp/space/application/rs/application.html

[20] Space Development Strategy Promotion Secretariat, Cabinet Office: "Space Policy Committee 65th Meeting" (December 2017)
https://www8.cao.go.jp/space/comittee/dai65/gijisidai.html

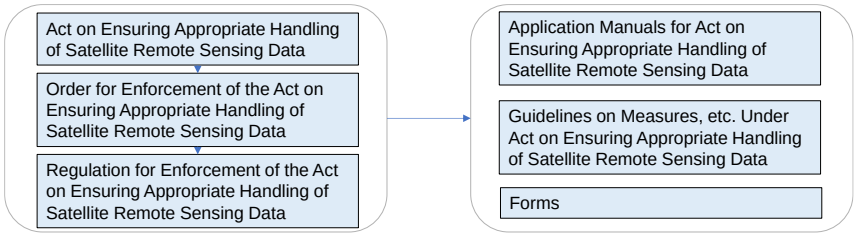


Figure 3-6 Legal system for requirements (1) (b)

The enforcement regulations stipulate that it is necessary to meet the security requirements of Table 3-17 when handling satellite remote sensing data.

Table 3-17 Relevant Articles for the Regulations for Enforcement of the Act on Ensuring Appropriate Handling of Satellite Remote Sensing Data

Article 7 (1) The measures specified by Cabinet Office Order, as referred to in Article 6, item (ii) and Article 20 of the Act, are as specified in the lower column of the following table, in accordance with the categories of Satellite Remote Sensing Data respectively specified in the upper column of the table.
(a) Organizational safety management measures (1) that a basic policy for safety management of the Satellite Remote Sensing Data is established. (2) that the responsibilities and authorities as well as businesses of person in charge of handling Satellite Remote Sensing Data are made clear. (3) that an organization for handling business in case of divulgence, loss or damage of Satellite Remote Sensing Data is established. (4) that regulations on safety management measures have been established and implemented, and operation of such regulations is being assessed and improved.
(b) Human safety management measures (1) that confirmation is made that the person in charge of handling Satellite Remote Sensing Data does not fall under any of Article 5, items (i) to (iv) and Article 21, paragraph (3), item (i)(a) to (d) of the Act. (2) that a person in charge of handling Satellite Remote Sensing Data has taken has taken measures to ensure that information on Satellite Remote Sensing Data handled by such person in the course of business and any other special confidential information (meaning unpublished information which such person may learn in the course of business) will not be used for any purpose other than for the ensuring of appropriate operation of such business or any other purpose found to be necessary. (3) that necessary education and training are provided to a person in charge of handling Satellite Remote Sensing Data.
(c) Physical safety management measures (1) that facilities for handling Satellite Remote Sensing Data are clearly distinguished. (2) that measures have been taken to restrict entry into and bringing any device into facilities for handling Satellite Remote Sensing Data. (3) that for a computer and portable memory device (meaning a portable media or device capable of being inserted into or connected to a computer or its peripheral equipment to store information; hereinafter the same applies in this paragraph), in order to prevent theft, loss or any other accident, fixing the edge of a computer with a wire or any other necessary physical measures have been taken.

(d) Technical safety management measures
(1) that appropriate measures have been taken for facilities for handling Satellite Remote Sensing Data so as to prevent unauthorized access (meaning unauthorized access as provided in Article 2, paragraph (4) of the Act on Prohibition of Unauthorized Computer Access (Act No. 128 of 1999).
(2) that measures have been taken to restrict a portable memory device from being connected with a computer or its peripheral equipment.
(3) that operations of computers and terminals relating to the handling of Satellite Remote Sensing Data have been recorded.
(4) that for transfer or telecommunication transmission of Satellite Remote Sensing Data, encryption or any other necessary measures for the appropriate protection of Satellite Remote Sensing Data have been taken.
(5) that for processing of Satellite Remote Sensing Data, necessary measures have been taken to ensure that such processing is implemented in an appropriate manner.

● **Requirement (1)(c) "Foreign Exchange and Foreign Trade Act"**

① Target

Those dealing with technology requiring permission under the provisions of Article 25, Paragraph 1 of the Foreign Exchange and Foreign Trade Act (see Table 3-18) and Article 17, Paragraph 2 of the Foreign Exchange Order.

② Overview

The Act stipulates that it is necessary to obtain permission when the specified technology stipulated by laws and regulations is managed at overseas bases, etc., or when the purpose is to provide such technology within Japan to non-residents from the specified state.

Table 3-18 Relevant provisions in the Foreign Exchange and Foreign Trade Act

Article 25 Paragraph 1 (1) When a resident or a non-resident intends to carry out transactions designed to provide technology pertaining to the design, manufacture or use of specific kinds of goods, which is specified by Cabinet Order as being considered to undermine the maintenance of international peace and security (hereinafter referred to as the "specified technology") in the specified foreign state (hereinafter referred to as the "specified state"), or when a resident intends to carry out transactions designed to provide a non-resident from the specified state with the specified technology, he/she shall obtain, pursuant to the provisions of Cabinet Order, permission from the Minister of Economy, Trade and Industry with regard to the transactions.

The following are some examples of technologies in the space industry that may fall under the specified technology. When handling these technologies, procedures shall be carried out as necessary after fully considering the contents of this Act from the operation design stage.

・ Attitude and orbit control

- Command and telemetry data handling
- Optical sensors and SARs for mounting on satellites
- Programs designed for the above uses

3.2.2 Satellite Unit

Satellite owners	Satellite operators	Ground station service providers	Satellite data platform operators	Satellite data service providers	Satellite developers

Requirements
Implement cybersecurity measures in the satellite system (main unit and RF communication)

[Basic Measures]

(1) When a high security level is required, implementation of the following measures of (a) to (e) is preferred.

(a) Protection of RF communication
(b) Anti-jamming measures for RF communication
(c) Prior verification of functions implemented in satellites
(d) Measures against vulnerabilities in devices mounted on the satellite
(e) Ensuring the integrity of Data Sent and Received
(f) Measures for supply chains

(Details)

● **Basic Measures(1)(a) "Protection of Protection of RF communication"**

If RF communication parameters are known, anyone can intercept RF communication information, but if measures such as encryption and electronic signatures are implemented, leakage and falsification of information can be prevented. Additionally, when a high level of security is required, information leakage prevention measures combining encryption with spectrum spread technology may be used. When encryption of RF communication is difficult due to the use of amateur radio bands or resource limitations of the satellite unit, there are measures such as incorporating electronic signatures, message authentication, etc. that detect falsification of communication.

To ensure the availability of communication environment between the satellite and the ground station, one or more of the following measures can be taken - preparing multiple uplink and downlink paths, multiple access points, and backup stations, and making it possible to use multiple command frequencies.

Key management is important when using encryption technology. Among cryptographic key methods, the key delivery method is an issue, especially for common key cryptography (also called secret key cryptography or symmetric key cryptography). For example, when communicating with multiple partners during

constellation operation, public key cryptography is assumed to be used as a method for securely sharing a single cryptographic key, because the common key cryptography has limitations in terms of managing multiple keys. However, many conventional space-mission-scenarios involve point-to-point communication and limited partners; therefore, the use of common key cryptography is recommended in terms of processing speed[21].

"CCSDS CRYPTOGRAPHIC ALGORITHMS" [22, 23], a standard specification recommended by the CCSDS (Consultative Committee for Space Data Systems), provides reference information on encryption for the space sector. Also, "SYMMETRIC KEY MANAGEMENT" [24], a standard specification recommended by the CCSDS, provides reference information on cryptographic key management.

[21]CCSDS: "SYMMETRIC KEY MANAGEMENT (DRAFT RECOMMENDED PRACTICE), CCSDS 354.0-R-1" (June 2018)
https://public.ccsds.org/Lists/CCSDS%203540R1/354x0r1.pdf
[22] CCSDS: "CCSDS CRYPTOGRAPHIC ALGORITHMS (INFORMATIONAL REPORT), CCSDS 350.9-G-1" (December 2014)
https://public.ccsds.org/Pubs/350x9g1.pdf
[23] CCSDS: "CCSDS CRYPTOGRAPHIC ALGORITHMS (RECOMMENDED STANDARD), CCSDS 352.0-B-2" (August 2019)
https://public.ccsds.org/Pubs/352x0b2.pdf
[24]CCSDS: "SYMMETRIC KEY MANAGEMENT (DRAFT RECOMMENDED PRACTICE), CCSDS 354.0-R-1" (June 2018)
https://public.ccsds.org/Lists/CCSDS%203540R1/354x0r1.pdf

[Reference 3.2.2-1] Standard Specification Recommended by the CCSDS

The CCSDS is an international standardization review committee for space data communication systems, established in 1982 by space agencies of various countries, which is working to define, and develop a standard for, space data communication systems. Documents (Recommended Standard and Recommended Practice) prepared by the CCSDS are not binding, but since the CCSDS serves as a subcommittee of the ISO (International Organization for Standardization) in the space data communications field, these documents, after publication, are automatically transferred to review and procedures for approval as ISO documents.

Documents prepared by the CCSDS are classified into 9 book colors according to the type of document and the stage of review, as shown in Fig. 3-7

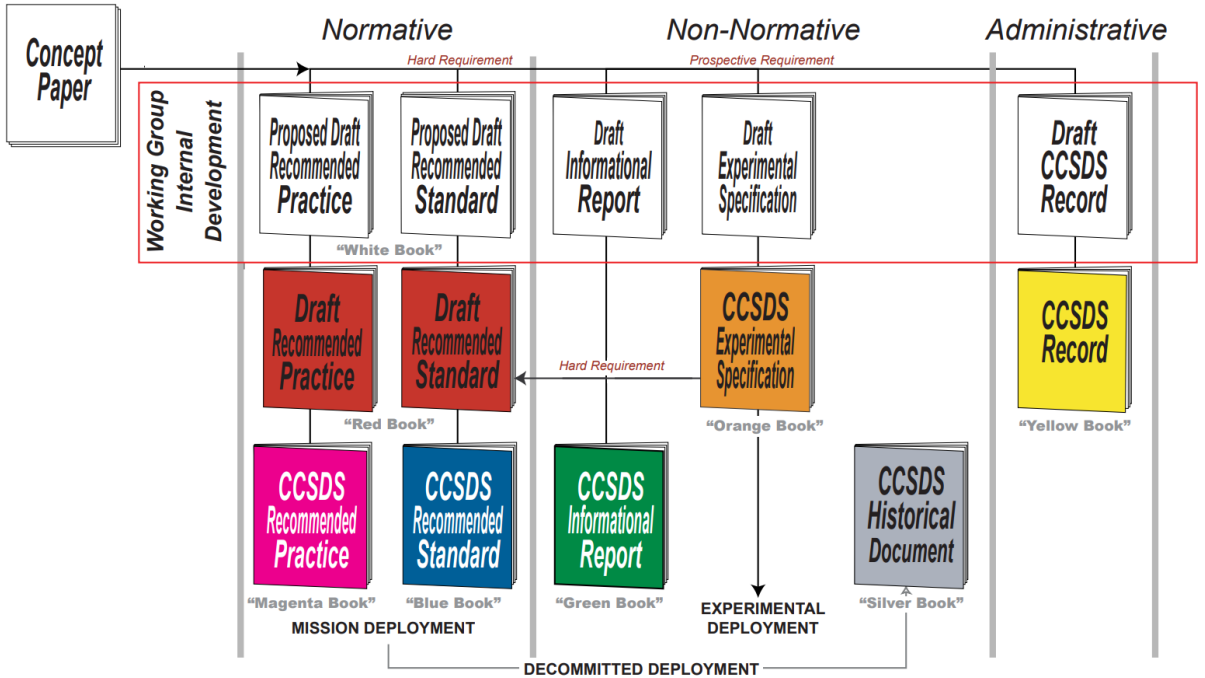


Figure 3-7 CCSDS Document Classification[25, 26]

[25] JAXA-CCSDS Secretariat, Japan Aerospace Exploration Agency: "Consultative Committee for Space Data Systems (CCSDS) 'About CCSDS Documents'" https://stage.tksc.jaxa.jp/ccsds/docs/booktop.html (in Japanese)

[26] CCSDS: "ORGANIZATION AND PROCESSES FOR THE CONSULTATIVE COMMITTEE FOR SPACE DATA SYSTEMS (CCSDS RECORD), CCSDS A02.1-Y-4" (April 2014) https://public.ccsds.org/Pubs/A02x1y4c2.pdf

"CCSDS CRYPTOGRAPHIC ALGORITHMS"[27] recommends the use of AES (Advanced Encryption Standard), which is a single common key block cipher, to ensure confidentiality. AES is the only symmetric cryptographic algorithm recommended for use in all CCSDS mission and ground systems, recommending a specific mode of operation for the algorithm (counter mode) and a minimum key length (128 bits).

"CCSDS CRYPTOGRAPHIC ALGORITHMS (RECOMMENDED STANDARD), [28] CCSDS 352.0-B-2" provides recommendations on CCSDS cryptographic security algorithms for authenticated encryption and authentication, and states that adoption of standard algorithms which are properly implemented will enable secure interoperability as well as reduce costs for missions utilizing security services. However, CCSDS does not specify at which layer of the OSI (Open Systems Interconnection) model the encryption algorithm should be used. As shown in "THE APPLICATION OF CCSDS PROTOCOLS TO SECURE SYSTEMS"[29], in the space communications layering model, there are multiple layers that can adopt cryptographic algorithms, and it is left to individual mission planners to implement these algorithms depending on the mission environment (based on the mission security requirements and the results of the mission risk analysis, without specifying how, when, or where these algorithms should be implemented or used). Also, it is recommended to prepare multiple authentication/integrity algorithms.

- **Basic Measures (1) (b) "Anti-Jamming Measures for RF Communication"**

Unlike wired communication, RF communication between the satellite and the ground station may be interrupted (jamming or interference) by a device that emits the same (or nearby) frequency at a higher power level. When the frequency being used is jammed, communications over the RF link are interrupted, telemetry and commands cannot be sent and received between the satellite and the ground station, and data collection from the satellite becomes impossible. As a result, data that could not be transmitted or received is completely lost, and there is a possibility that it cannot be recovered.

The inability to receive housekeeping data on the ground may also result in the loss of the satellite because of the inability to respond in an emergency situation requiring immediate action against the satellite. Similarly, even if telemetry can be received, the satellite may be lost if the command uplink is jammed.

Techniques for counteracting jamming include spectrum spread technology and frequency hopping technology, but when anti-jamming technology cannot be mounted due to reasons such as satellite application, scale, resource limitations, etc., measures such as preparing backup stations and backup communication

[27] CCSDS: "CCSDS CRYPTOGRAPHIC ALGORITHMS (INFORMATIONAL REPORT), CCSDS 350.9-G-1" (December 2014)
https://public.ccsds.org/Pubs/350x9g1.pdf
[28]CCSDS: "CCSDS CRYPTOGRAPHIC ALGORITHMS RECOMMENDED STANDARD (RECOMMENDED STANDARD), CCSDS 352.0-B-2" (August 2019)
https://public.ccsds.org/Pubs/352x0b2.pdf
[29]CCSDS: "THE APPLICATION OF SECURITY TO CCSDS PROTOCOLS (INFORMATIONAL REPORT), CCSDS 350.0-G-3" (March 2019)
https://public.ccsds.org/Pubs/350x0g3.pdf

channels (that can be implemented within the satellite resource limitations and are operated by appropriate switching) can be considered.

● **Basic Measures (1) (c) "Prior Verification of Functions Implemented in Satellites"**

If an unintended function (any situation or event that may damage the system in the form of interference with satellite operation, harmful modification of mission data, service disturbance, etc.) is incorporated into the satellite, not only will it be difficult to carry out the mission, but there is a possibility that the satellite will be lost. In other words, it can be said that the software development process of embedded systems itself includes potential vulnerabilities. For example, malicious code may be inserted during the development process to introduce vulnerabilities such as backdoors to the control system. Also, software developers often introduce trap doors in the code so that they can re-invade the system and perform specific functions. These potential issues, risks, and vulnerabilities in the software development processes are briefly described in "SECURITY THREATS AGAINST SPACE MISSIONS"[30]. Prior verification methods from the viewpoints of hardware and software are introduced below.

- Preventing the incorporation of contaminated hardware components (e.g., hidden malicious functions, system instability, damage to the system, undesirable impact on the system) can be addressed by security mechanisms such as supply chain reliability verification, vetted hardware suppliers, inspected hardware production, hardware reliability verification, hardware functionality analysis, etc.
- For software threats embedded in the system (e.g., undesirable events, damage to the system, activation of other threats), available security mechanisms may include acceptance testing, independent verification & validation (IV&V), code walk-through, automated code analysis, run-time security monitoring, software partitioning (trusted computing base), and supply chain reliability verification. "IV&V Guidebook [Introduction]" (JAXA) [31]is a reference book on IV&V.

For OSS (open source software), there are reference books such as "Collection of Use Case Examples Compiled Regarding Management Methods for Utilizing Open Source Software and Ensuring Its Security" (Ministry of Economy, Trade and Industry) [32]and "Overview of CVE (Common Vulnerabilities and Exposures) Identifiers" (IPA)[33], which are explained below.

---

[30]CCSDS: "SECURITY THREATS AGAINST SPACE MISSSIONS (INFORMATIONAL REPORT), CCSDS 350.1-G-2" (December 2015)
https://public.ccsds.org/Pubs/350x1g2.pdf
[31]Japan Aerospace Exploration Agency: "IV&V Guidebook (Introduction) V ER2.1" (June 2018)
https://stage.tksc.jaxa.jp/jedi/devel/ivv_project/guidebook/file/ivv_guidebook_1.pdf (in Japanese)
[32]Cybersecurity Division, Commerce and Information Policy Bureau, Ministry of Economy, Trade and Industry: "Collection of Use Case Examples Regarding Management Methods for Utilizing Open Source Software and Ensuring Its Security" (April 2021)
https://www.meti.go.jp/policy/netsecurity/wg1/CollectionOfUseCaseExamplesForUtilizingOSS.pdf
[33] Information-Technology Promotion Agency, Security Center: "Overview of CVE (Common Vulnerabilities and Exposures) Identifiers"
https://www.ipa.go.jp/security/english/vuln/CVE_en.html

The "Collection of Use Case Examples Compiled Regarding Management Methods for Utilizing Open Source Software and Ensuring Its Security" summarizes issues related to the utilization of OSS from the perspectives of selection evaluation, licensing, vulnerability handling, maintenance and quality assurance, supply chain management, individual capabilities and education, organizational structure, community activities, etc., based on a survey conducted through interviews with companies that are implementing helpful initiatives in light of the current situation where many companies have issues related to software management methods and vulnerability handling including OSS. When a vulnerability involving OSS is discovered, it is very important to respond to the vulnerability quickly and appropriately in order to maintain security. "Information Security Early Warning Partnership" and "JVN (Japan Vulnerability Notes)" operated by IPA (Information-Technology Promotion Agency) and JPCERT/CC (JPCERT Coordination Center) provide users with necessary information for performing these series of responses. Also refer to "3.1.5 Reporting Incidents to the Outside".

The CVE (Common Vulnerabilities and Exposures) identifiers introduced in the "Overview of CVE (Common Vulnerabilities and Exposures) Identifiers" cover vulnerabilities in individual products and are numbered by MITRE, a non-profit organization that has received support from the US government. Most vulnerability inspection tools and services providing vulnerability countermeasure information use CVE. By assigning unique identification numbers, "CVE-IDs" to vulnerabilities in individual products, it is possible to determine that vulnerability countermeasure information issued by organization A and that issued by organization X address the same vulnerability, and the IDs can be used for cross-referencing and association between countermeasure information.

● Basic Measures (1) (d) "Measures against Vulnerabilities in Devices Mounted on the Satellite"

As cyberspace and physical space become highly integrated, the risk of devices scattered around physical space becoming new targets of cyberattacks has become apparent. In fact, in 2016, routers and webcams in fixed configurations were infected with the malware "Mirai", and infected devices became the source of a large-scale DDoS attack. There have been many other cases where malware such as variants of Bashlite, BrickerBot, and variants of Mirai threaten the security of IoT devices, not only causing direct damage to their users, but also affecting other devices connected to the network, via malware-infected devices. The impact is not limited to cyberspace, but may also extend to physical space.

It is necessary to check the vulnerabilities of devices mounted on satellites in orbit as well. Therefore, it is necessary to conduct vulnerability diagnosis on the ground for equipment equivalent to that in flight, and if the results confirm a fatal vulnerability affecting satellite services, appropriate measures such as software updates must be taken via satellite communication.

Methods for confirming the presence of vulnerabilities that can lead to security threats and the validity of security measures are explained below from the viewpoints of security verification for devices and security verification for embedded software.

- Security verification is effective to check the presence of vulnerabilities and take security measures for devices. The "Guide for Security Verification to Ensure Cybersecurity of Devices" (Ministry of Economy, Trade and Industry) [34] is a reference book. The Main Guide, Separate Volume 1, and Separate Volume 2 focus on the "verification" phase of the equipment development process, and organize matters that verification service providers should implement in verification and matters that equipment manufacturers should prepare for verification requests. Additionally, in Separate Volume 1 and Separate Volume 2, threat analysis methods for equipment are also shown[35].
- If, as a result of security verification [36] of the embedded software in a device mounted on the satellite, a fatal vulnerability or security hole affecting satellite services is confirmed in a program embedded in the device, it is necessary to apply the latest security patch, etc. "How to Effectively Proceed with Vulnerability Countermeasures, Tool Utilization Edition" (IPA)[37] provides reference information on vulnerability countermeasures, and explains procedures, etc. for vulnerability countermeasures utilizing the open source software, Vuls (Vulnerability Scanner). Vuls is compatible with OS such as Ubuntu, Debian, CentOS, Amazon Linux, and RHEL, and can scan approximately 370 software types in a few minutes (as verified by IPA), thus reducing the time required to collect vulnerability-related information on a daily basis.

Various software is installed on satellites and mission equipment, and it is necessary to take required vulnerability countermeasures by referring to the countermeasure flow shown in Figure 3-8. To properly implement vulnerability countermeasures, it is necessary to accurately identify the software installed in the satellite and mission equipment, and at a minimum, manage the items shown in Table 3-19 in a list.

[34]Cybersecurity Division, Commerce and Information Policy Bureau, Ministry of Economy, Trade and Industry: "Guide for Security Verification to Ensure Cybersecurity of Devices" (April 2021) https://www.meti.go.jp/press/2021/04/20210419003/20210419003-1.pdf (in Japanese)
[35] Same as 34
[36] Information-Technology Promotion Agency: "How to Effectively Proceed with Vulnerability Countermeasures, Tool Utilization Edition" https://www.ipa.go.jp/topic/isec-technicalwatch-201902.html (in Japanese)
[37] Information-Technology Promotion Agency, Security Center: "How to Effectively Proceed with Vulnerability Countermeasures, Tool Utilization Edition - Vulnerability Countermeasures Using Vulnerability Detection Tool Vuls -" https://www.ipa.go.jp/files/000071584.pdf (in Japanese)

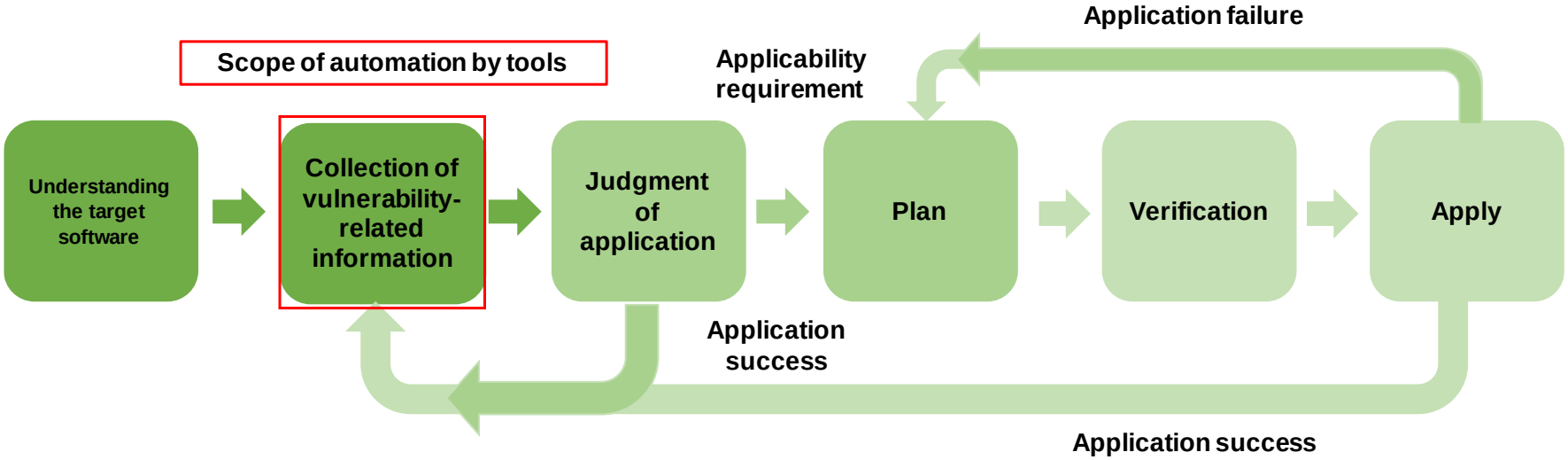


Figure 3-8 Vulnerability Countermeasures Flow (Example)[38]

Table 3-19 Control items for target software[39]

#	Item	Remarks
1	Software name	-
2	Software version	-
3	How to install the software = How to install the latest version	[For Linux servers] yum, rpm, compile from source code, etc. [For Windows servers] Deployment of installers, executable files, etc.
4	Site providing the latest version (URL)	To be used to check the latest version, not necessary if the software installation method in #3 can be used for substitution

[38] Same as 37
[39] Same as 37

● **Basic Measures (1) (e) "Ensuring the integrity of Data Sent and Received"[40, 41]**

There are two types of threats to space missions: active and passive. Active threats are those where the source of the threat initiates a series of events and actively interferes with the system and tries to exploit a vulnerability. Active threats include the following, which may attack satellites, ground systems, and communication systems.

- Interference with communication systems (disruption resulting in unserviceability, loss of availability and data integrity)
- Attempt to gain unauthorized access to an access-controlled system
- Playing back recorded legitimate communication traffic later, to send unauthorized data
- Spoofing an authorized entity to gain access
- Exploiting software vulnerabilities
- Unauthorized modification or corruption of data
- Malicious software such as viruses, worms, distributed denial-of-service (DDoS) agents, keyloggers, rootkits, and trojan horses

Passive threats, on the other hand, are intended to misuse systems that already exist and are in use, rather than actively interfering with the target system, and include the following threats

- Loss of confidentiality through eavesdropping on communication links (wirelines, RF, networks)
- Traffic analysis to determine which entities are communicating with each other

Against such active and passive threats, the following security measures, etc. can be considered to ensure the integrity of data (telemetry data, commands, update programs, mission data, etc.) sent and received between the satellite and ground stations.

- For protection from unauthorized commands, an authentication function is provided for identifying unauthorized commands and unauthorized update programs uplinked from the Earth station (antenna facility) to prevent them from being executed.
- An authentication function for identifying the correct counterpart or command is provided to protect against "spoofing" from unintended transmission sources, such as attackers. However, even when a complex identifier is used, this alone is not effective against a replay attack where communication is

[40] CCSDS: "SPACE DATA LINK SECURITY PROTOCOL (RECOMMENDED STANDARD), CCSDS 355.0-B-2" (July 2022)
https://public.ccsds.org/Pubs/355x0b2.pdf
[41] CCSDS: "SECURITY THREATS AGAINST SPACE MISSIONS（INFORMATIONAL REPORT）,CCSDS 350.1-G-3" (February 2022)
https://public.ccsds.org/Pubs/350x1g3.pdf

intercepted and reused; therefore, one or more of the countermeasures, such as adding a timestamp or an authenticated message counter to the command, encrypting the time of transmission, etc., are applied.

- To detect that data sent from the legitimate counterpart has been falsified along the way, measures such as including self-signed data when sending data are implemented.
- Measures such as defining the timeline of commands (scheduled and in-context) are implemented so that commands are not executed outside of the defined timeline, except when responding to an abnormality after launch or responding to an emergency.

● **Basic Measures (1) (f) "Measures for Supply Chains"**

In recent years, there are concerns about new security risks affecting supply chains. Today, the global division of labor, called the global value chain, can be seen in many fields. The advantage of this division of labor is that various products can be produced at low cost, but on the other hand, since many companies in various regions are involved in production, etc., it can also be a source of new risks. The "10 Major Threats to Information Security 2023"[42]also cites "the increase in attacks exploiting weaknesses in the supply chain" as the second most common threat to companies. Also, in the "IoT/5G Security Comprehensive Measures" [43] formulated in 2019, incorporation of unauthorized programs and firmware and tampering have been cited as examples of such risks in the process of manufacturing and distributing ICT products and services, and it has also been mentioned that among parties involved in contractual relationships, such as outsourcing, those who have inadequate cybersecurity measures may be used as a steppingstone. [44]

In light of this situation, the space industry too needs to take security measures for supply chain risks in the lifecycle of satellites from procurement to disposal, by identifying the location of cybersecurity risks in each phase of the lifecycle, including not only one's own company, but also business partners and contractors[45]. In order to build partnerships with business partners to improve cybersecurity of the entire supply chain, the Ministry of Economy, Trade and Industry (METI) and the Japan Fair Trade Commission (JFTC) have organized measures to support cybersecurity measures by SMEs and the application of related laws and

[42]Information-Technology Promotion Agency, "Information Security (10 Major Threats to Information Security 2023)" (January 25, 2023) https://www.ipa.go.jp/security/vuln/10threats2023.html (in Japanese)

[43] Ministry of Internal Affairs and Communications, Cybersecurity Task Force "IoT/5G Security Comprehensive Measures" (August 2019) https://www.soumu.go.jp/main_content/000641510.pdf (in Japanese)

[44] Ministry of Internal Affairs and Communications, "2020 White Paper Information and Communications in Japan (ICT White Paper) - Digital Transformation and New Lifestyles Promoted by 5G" https://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/whitepaper/2020/pdf/contents.pdf

[45] Cybersecurity Division, Commerce and Information Policy Bureau, Ministry of Economy, Trade and Industry: "Cybersecurity Management Guidelines Ver 2.0" (November 2017) https://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v2.0_en.pdf

regulations to support and request business partners to take such measures[46]. In this arrangement, it is considered that the enhancement of security measures for the entire ply chain is an important initiative, and that a business entity that places an order does not immediately become a problem under the Antimonopoly Law if it requests its counterparty to implement cybersecurity measures. However, depending on the method and content of the request, it may become a problem as abuse of a superior position under the Antimonopoly Law, and examples of such cases are provided.

The supply chain cyber-risk guidelines include "Cybersecurity Management Guidelines Ver 3.0" introduced in 3.1.1, which include "Drive security measures in the supply chain" as one of the three principles that management should be aware of, and "Understand cybersecurity status and measures in the entire supply chain including business partners and outsourcing companies" as one of the ten important items for cybersecurity management.

A list of main guidelines on supply chain risks issued in and outside Japan for procurement activities (mainly outsourcing) in the critical infrastructure industry and of large companies can be found in the JCIC (Japan Cybersecurity Innovation Committee) Column [47].

The lifecycle of a satellite from procurement to disposal and security requirements for suppliers at the time of procurement are organized in Fig. 3-9.

[46] Ministry of Economy, Trade and Industry and the Japan Fair Trade Commission: "Toward building partnerships with suppliers to improve cybersecurity throughout the supply chain" (October 2022) https://www.jftc.go.jp/dk/guideline/unyoukijun/cyber_security.html (in Japanese)

[47] Japan Cybersecurity Innovation Committee: "JCIC Column Supply chain Cyber-risk Guidelines" (January 2020) https://www.j-cic.com/column/scr.html (in Japanese)

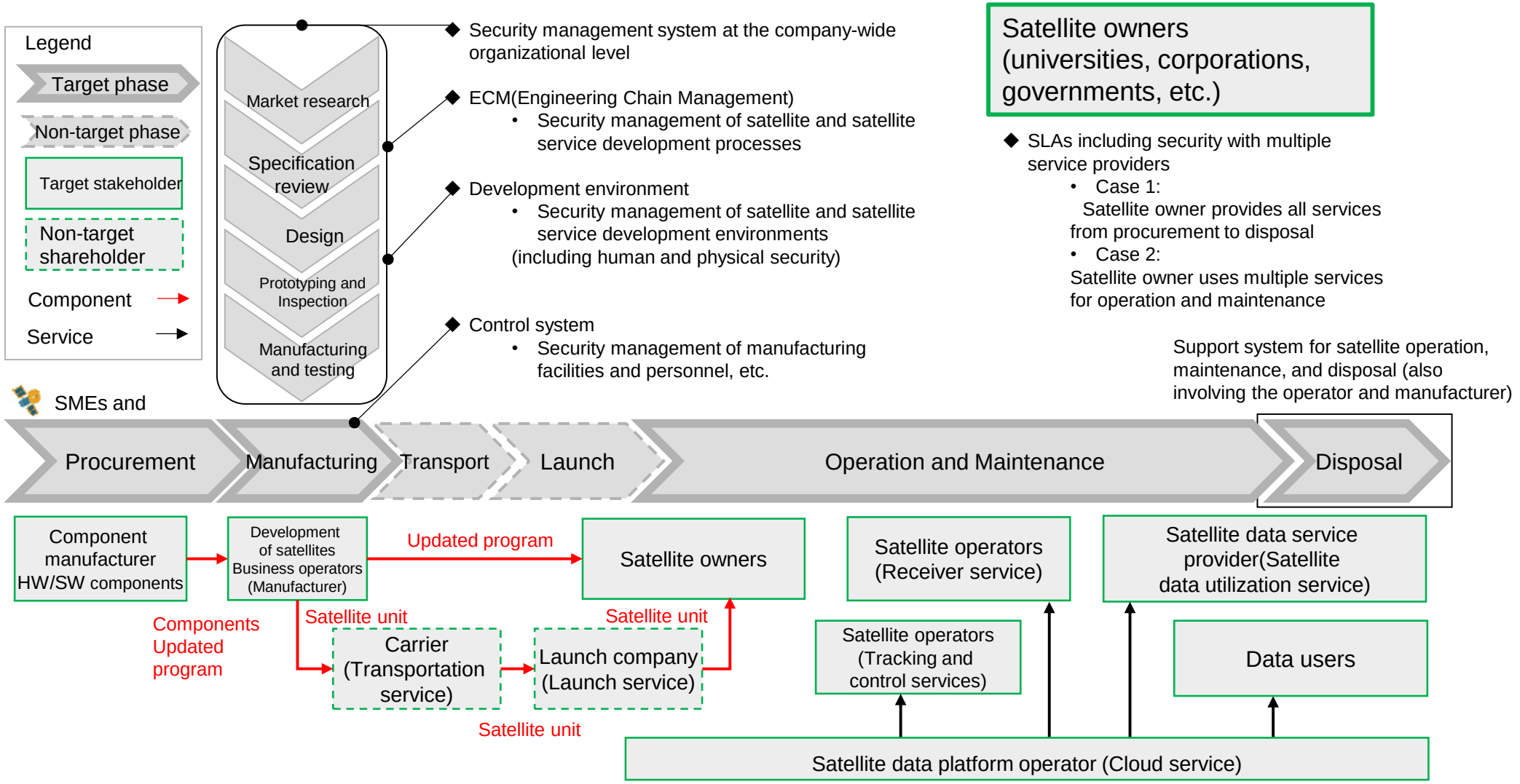


Figure 3-9 Satellite Lifecycle and Supplier Security Requirements Mapping During Procurement

Note: The transportation and launch phases of a satellite are outside the scope of these guidelines, but when attacks such as tampering on the satellite unit or devices mounted on the satellite, etc. are anticipated during satellite transportation, adoption of tamper-resistant technology, etc. to detect attacks such as tampering is recommended.

3.2.3 Satellite Operation Facility

Satellite owners	Satellite operators	Ground station service providers	Satellite data platform operators	Satellite data service providers	Satellite developers

Requirements

Implement cybersecurity measures for satellite operation facilities (tracking and control station, receiving station, network operation system, mission control system (including satellite control system and orbit control system)).

[Basic Measures]

(1) When a high-security level is required, implementation of the following measures (a) to (h) is preferred.

(a) Equipment protection
(b) Communication protection
(c) Anti-jamming measures
(d) Data protection
(e) Facility inspection and vulnerability protection measures
(f) Ensuring the integrity of data sent and received
(g) Use of external services
(h) Secure coding

(Details)

● **Basic measures (1) (a) "Equipment Protection"**

Control station	Network operation system	Receiving station	Mission control system

If facilities that carry out satellite mission control, etc. are attacked by hostile organizations (terrorists, criminals, foreign intelligence agencies, saboteurs, political activists, computer hackers, commercial competitors, etc.) or malicious insiders (dissatisfied staff, dishonest maintenance personnel, dishonest system personnel, internal collaborators influenced by external threat actors on SNS, etc.), or if facilities used to control the satellite are overrun without technically attacking the system, not only would the facilities be lost, but the mission operations and the services provided could be directly affected.

The loss of ground systems (particularly facilities that carry out satellite mission control) can lead not only to loss of data and loss of timely access to data, but also to the loss of the entire mission. The following measures can be used against such physical attacks on ground facilities. [48]

- Deploying security guards
- Installation of gates
- Access control to facilities (restricting the information handled and the area handled)
- Setting up a backup site in case of an attack

One or more of the following measures can be taken in preparation against intrusion by suspicious persons from the outside, unauthorized personnel, etc.

- Restricted access to facilities or areas that perform tracking, control, and reception, among satellite operation facilities
- Restricted access to facilities or areas that perform satellite operation tasks such as network operations and mission control
- Measures such as locking, entrance/exit records, or entry detection to prevent unauthorized use of satellite operation facilities
- When a satellite operation facility is located as part of another facility, measures to check and maintain communication means and systems with the manager of the said facility
- Restriction on areas and information systems handling network operation tasks, to prevent leakage or tampering of operations information on domestic and overseas ground station (tracking and control station and receiving station) networks
- Measures to implement encryption functions for communication pathways and communication information with domestic and overseas ground stations, and for the stored data

In addition, measures to prevent damage due to environmental factors (fires, power outages, other natural disasters, etc.) (formulating a plan in case satellite operation support is required during an emergency), etc. can be taken.

● **Basic Measures (1) (b) "Communication Protection"**

Control station	Receiving station	Mission control system

As explained in 3.2.2 Basic Measures (1) (a) "Protection of RF Communication", when performing satellite tracking and control, and receiving and recording

[48] CCSDS: "SECURITY THREATS AGAINST SPACE MISSIONS (INFORMATIONAL REPORT), CCSDS 350.1-G-2" (December 2015)
https://public.ccsds.org/Pubs/350x1g2.pdf

mission data, etc. encryption of RF communication with satellites and encryption of keys used for encryption are performed from the viewpoint of preventing tampering and eavesdropping. Also, in mission control systems that track and control satellites and send commands, in addition to encryption, there are measures such as limiting the number of employees who can use the system. Furthermore, in inter-site communication, measures such as using dedicated lines or encrypted networks are implemented from the viewpoint of preventing tampering and eavesdropping.

"Communication protection" for satellite operation facilities includes, as shown below, "protection of RF communication" between the satellites and the ground stations and "protection of inter-site communication" for satellite operation facilities. Regarding "protection of RF communication" between satellites and ground stations, refer to the explanation of 3.2.2 Basic Measures(1)(a) "Protection of RF communication".

The following measures can be taken for "protection of inter-site communication" for satellite operation facilities.

- From the viewpoint of preventing tampering and eavesdropping, use a dedicated line or encrypted network (VPN (Virtual Private Network) with mutual authentication and TLS (Transport Layer Security)), etc.
- Design the network such that unnecessary or unexpected communication does not occur in inter-site communication
- Divide the network into segments and control communication using firewalls
- When using external services, etc. described in Basic Measures (1)(g) below, clearly define the boundaries between trusted and untrusted zones, and ensure that only the minimum necessary communication is possible with the outside

The following measures can be taken for mission control systems that perform satellite tracking and control and send commands.

- In order to limit the number of employees who can use the system, restrict the access to the system through authentication mechanisms such as login, IP address restrictions, etc.
- Keep a record of operations
- Implement encryption functions for communication pathways and communication information with related facilities and systems, and for the stored data

● Basic Measures (1) (c) "Anti-Jamming Measures"

Control station	Receiving station

To prepare against the possibility of interruption, such as jamming or interference, in RF communication between the satellite and the ground station (tracking, control, and reception), refer to 3.2.2 Basic Measures (1)(b) "Anti-Jamming Measures for RF communication".

● **Basic measures (1) (d) "Data Protection"**

Control station	Receiving station	Mission control system

Destruction, tampering or leakage of critical data related to satellite and ground station operations may cause problems in satellite operations. This may also affect the satellite data utilization facility and provided services as described below.

Given below is an explanation from the viewpoint of information to which access should be restricted and measures, in order to protect usage records, housekeeping data, mission data, mission control system logs, etc. of satellite operation facilities and radio stations (receiving stations).

- One of the measures would be to store information such as satellite housekeeping data and satellite mission data acquired through downlinks, in a storage with limited access. Another measure is to store and protect records related to satellite operation, such as usage records of the satellite operation facility, radio station usage records, login, and command transmission histories of mission control systems, etc., from the viewpoint of incident response.
- If necessary, measures to protect data by storage encryption or file encryption may also be considered.

● **Basic Measures (1) (e) "Facility inspection and vulnerability protection measures"**

Control station	Network operation system	Receiving station	Mission control system

If an unintended function is implemented in a system in the satellite operation facility, not only will the mission be difficult to execute, but the satellite may be lost.

When an unintended function that may adversely affect satellite control or a vulnerability or security hole leading to information leakage, tampering, etc. are identified, it is necessary to apply the latest security patches, etc. and implement measures such as eliminating vulnerabilities in the systems in the satellite operation facilities. References for such measures are as follows.

- Refer to 3.2.2 Basic Measures (1) (c) "Prior verification of functions implemented in satellites" for measures to confirm that unintended functions have not been implemented in the system
- Refer to 3.2.2 Basic Measures (1) (d) "Measures against vulnerabilities in devices mounted on the satellite" for reference books, etc.

● **Basic measures (1) (f) "Ensuring the Integrity of Data Sent and Received"**

Control station	Receiving station

If information sent and received by a system in the satellite operation facility is leaked, it could be misused by a malicious attacker, making it difficult to execute the mission. Also, if mission data is tampered in a system in the satellite operation facility, the operation of the satellite data utilization facilities described below may be adversely affected.

Given below is an explanation from the perspectives of preventing the transmission of unauthorized commands and up-linking of unauthorized update programs from the Earth station (antenna facility) and preventing leakage and tampering of received data (e.g., mission data), etc., as measures to ensure the integrity of data sent and received (e.g., telemetry data, commands, update programs) and the integrity of received data (e.g., mission data) and mission data sent to an external recording device via a network.

The following measures can be taken to prevent transmission of unauthorized commands and up-linking of unauthorized update programs from the Earth station.

- Measures such as defining the timeline of commands (scheduled and in-context) so that commands are not executed outside of the defined timeline, except when responding to an emergency, and confirming that unintended functions that may adversely affect satellite control have not been implemented in systems in the satellite operation facility (Refer to 3.2.2 Basic Measures (1) (c)).
- Measures such as re-evaluation of the command plan and implementing checks using a check tool (simulator, etc.) before sending commands
- Measures such as using the HMI (human machine interface) that is designed to reduce the possibility of errors in operation based on lessons learned from the past
- Measures such as requiring approval through a special approval flow (workflow application, multiple approvers, written instructions, etc.) when executing important operations
- Measures such as carrying out control operation by two or more persons when sending important commands, update programs, etc.

The following measures can be taken to prevent leakage and tampering of received data (mission data, etc.)

- Measures such as using dedicated lines or encrypted networks for transmission to external recording devices to prevent leakage and tampering of mission data
- Measures to store and regularly monitor the usage status (login records, access logs, etc.) of information systems that handle mission data, etc. and

monitor access status (including operation details) to mission data, etc. in order to prevent leakage and tampering of mission data, etc. recorded in the receiving station facilities

Note: Self-signature is the basic measure against tampering, etc. For measures to include self-signed data in transmitted data, etc., refer to Basic Measures (1)(e).

● **Basic Measures (1) (g) "Use of External Services"**

Control station	Network operation system	Receiving station	Mission control system

Cybersecurity incidents targeting external service organizations have been reported as explained in 3.2.2 Basic Measures (1) (f) "Security Measures for Supply Chains". When using an external service, it is necessary to take measures such as checking whether the service provider has implemented security measures, etc., equivalent to the Basic Measures (1) (a) to (f) described above.

The use of external services is assumed to include the use of satellite operation facility services, public clouds, and ground station services, as shown below.

- Use of satellite operation facility services

  One of the measures taken when using a service to operate all or part of the satellite operation facility is to, when concluding a service agreement with the provider of the said service, include measures equivalent to the safety management measures provided for in "Article 7, Paragraph 2 of the Regulations for Enforcement of the Act on Ensuring Appropriate Handling of Satellite Remote Sensing Data", and an agreement relating to "Article 25 of the Foreign Exchange and Foreign Trade Act" that the service provider shall not store the satellite operation information on computers located in the specified state, etc., in the SLA (Service Level Agreement) with the contract counterparty. For reference information, etc., refer to 3.2.1Measures Required by Law.

- Use of public clouds

  One of the measures taken when using, as part of the satellite operation facilities, external services such as public clouds to store all or part of the data or to configure or operate all or part of the software systems is to check the implementation status of security measures, etc. described in the Basic Measures (a) to (f) by the contract counterparty, or status of certifications equivalent to FedRAMP Moderate Level or ISMAP Level 2.

  - The means that can be used by public cloud users to confirm the measures include conclusion of an SLA, etc., as well as referring to SOC reports and other IT compliance reports submitted by the public cloud service providers, etc.

- Measures to protect mission data include encryption of the public cloud storage as well as additional measures one may take voluntarily as necessary, such as encryption of files.

- Use of ground station services

  Measures when using, as part of the satellite operation facilities, external ground station services for all or part of the radio stations that track and control satellites or receive and record mission data, etc. include checking the implementation status of security measures, etc. described in Basic Measures (a) to (f) by the contract counterparty.

  - One may voluntarily use confidential information, such as cryptographic keys for RF communication and authentication information for encrypted networks such as VPNs, as additional protective measures that can be used securely within these ground station services.
  - When bringing in your own device, such as servers, network devices, modems, etc. to use the services, measures such as locking the front panel, closing unnecessary ports, and encrypting the storage can be taken in advance.

● **Basic Measures (1) (h) "Secure Coding"**

Control station	Network operation system	Receiving station	Mission control system

Web applications are frequently used during system maintenance and software updates for satellites and ground system facilities, etc., and since they can be accessed remotely from the outside, it is necessary to take appropriate security measures. When developing a commercial space system including web applications, it is necessary to consider secure coding paying attention to security, and to clarify the extent to which warranty should be provided prior to executing a contract. Reference books include "Information Security IPA Secure Programming Course[49]", "Guidelines for Preparing Security Specifications for Information System Development Agreements[50]", etc.

[49]Information-Technology Promotion Agency, Security Center: "Information Security IPA Secure Programming Course" (September 2017)
https://www.ipa.go.jp/security/awareness/vendor/programming/ (in Japanese)
[50]Software Association of Japan, Software-ISAC: "Guidelines for Preparing Security Specifications for Information System Development Agreements" (November 2020)
https://www.softwareisac.jp/ipa/index.php (in Japanese)

3.2.4 Satellite Data Utilization Facility

Satellite owners	Satellite operators	Ground station service providers	Satellite data platform operators	Satellite data service providers	Satellite developers

Requirements

Implement cybersecurity measures for satellite data utilization facilities.

[Basic Measures]

(1) When a high-security level is required, implementation of the following measures (a) to(f) is preferred.

(a) Equipment protection

(b) Data protection

(c) Facility inspection and vulnerability protection measures

(d) Ensuring the integrity of data received

(e) Use of external services

(f) Secure coding

(Details)

Reference books on ensuring confidentiality, integrity, and availability of the satellite data utilization facility include, for example, ISO 9001, ISO/IEC 27001 for quality management, and data security sub-categories of the NIST Cybersecurity Framework, for data protection.

● **Basic Measures (1) (a) "Equipment Protection"**

Although there are no specific measures for space systems, refer to 3.2.3 Basic Measures (1)(a) "Equipment Protection" to ensure confidentiality, integrity, and availability of the satellite data utilization facility.

● **Basic Measures (1) (b) "Data Protection"**

Although there are no specific measures for space systems, refer to 3.2.3 Basic Measures (1)(d) "Data Protection" to ensure confidentiality and integrity of the

satellite data utilization facility.

- **Basic Measures (1) (c) "Facility inspection and vulnerability protection measures"**

Although there are no specific measures for space systems, refer to 3.2.3 Basic Measures (1)(e) "Facility inspection and vulnerability protection measures" to ensure confidentiality, integrity, and availability at the satellite data utilization facility.

- **Basic Measures (1) (d) "Ensuring the Integrity of Data Received"**

Although there are no specific measures for space systems, refer to 3.2.2 Basic Measures (1)(e) "Ensuring the integrity of Data Sent and Received" and 3.2.3 Basic Measures (1)(f) "Ensuring the Integrity of Data Sent and Received" to ensure confidentiality, integrity, and availability of the satellite data utilization facility.

- **Basic Measures (1) (e) "Use of External Services"**

Refer to 3.2.3 Basic Measures (1)(g) "Use of External Services", when developing and operating a satellite data utilization facility.

- **Basic Measures (1) (f) "Secure Coding"**

Refer to 3.2.3 Basic Measures (1)(h) "Secure Coding", when developing and operating a satellite data utilization facility.

3.2.5 Development and Manufacturing Facility

Satellite owners	Satellite operators	Ground station service providers	Satellite data platform operators	Satellite data service providers	Satellite developers

Requirements

Implement cybersecurity measures for satellite development and manufacturing facilities.

[Basic Measures]

(1) When handling satellite development and manufacturing facilities, using the existing standards including (a) given below is preferred.

(a) Cyber/Physical Security Framework for Factory Systems (METI)

(Details)

● **Basic Measures(1)(a) "Cyber/Physical Security Guidelines for Factory Systems (Ministry of Economy, Trade and Industry)"**

① Target

Industrial control systems in factories

② Overview

The "Cyber/Physical Security Guidelines for Factory Systems" [51] provide a guide of concepts and steps to be referred when planning and executing measures for factories on your own, and also specify the minimum necessary measures, from technical measures against threats to operational and management measures. Specifically, the guidelines present steps for planning and introducing security measures based on the three steps of "collecting and organizing information," "planning security measures," and "building a system for execution and management of security measures". The guidelines also state that since the scale of factories, equipment and systems vary widely, and measures to be implemented differ by industry and sector, it is necessary to organize and define the concepts suitable for each individual company and industry at each step.

Related reference books include "Control System Security Risks as a Major Management Issue, Third Edition"[52] provided by IPA and "Check List for Industrial

[51] Ministry of Economy, Trade and Industry: "Cyber/Physical Security Guidelines for Factory Systems" (November 2022) https://www.meti.go.jp/policy/netsecurity/wg1/factorysystems_guideline_ver1.0.pdf (in Japanese)

[52] Information-Technology Promotion Agency: "Control System Security Risks as a Major Management Issue, Third Edition" (March 2017) https://www.ipa.go.jp/files/000058489.pdf (in Japanese)

Control Systems of Japan (J-CLICS)" [53] provided by JPCERT/CC.

[53] JPCERT Coordination Center: "Check List for Industrial Control Systems of Japan (J-CLICS)" (April 2017)
https://www.jpcert.or.jp/english/cs/J-CLICS_STEP1_guide_en.pdf

Column: Facilities in a General Factory's Manufacturing Environment (Hiroshi Sasaki, Fortinet Japan LLC, Member of Space Industry SWG)

Facilities in a general factory's manufacturing environment are broadly classified into 3 levels according to its role in production.

- Control information network
  There is a server for production management and status monitoring of the factory.
- Control network
  There are control devices such as PLC (Programmable Logic Controller), DCS (Distributed Control System), etc.
- Field network
  There are field devices such as motors and sensors controlled by control devices.

These factory facilities are often connected to the office within the factory building via a network isolation layer called DMZ (Demilitarized Zone). However, sometimes the DMZ does not exist. Systems within the factory facilities generally have the following characteristics.

- There are often PCs with OS that is no longer supported by the manufacturer.
- The protocols used for communication are different from those of information systems. There are many control-specific protocols unique to control device vendors, making network security products for ordinary information systems less effective.
- The facilities are under the management of the production engineering department and not the information systems department, and often there is no dedicated security organization or person in charge.

Therefore, security measures for factory facilities often lag behind compared to those for information systems, and risks are not sufficiently reduced.

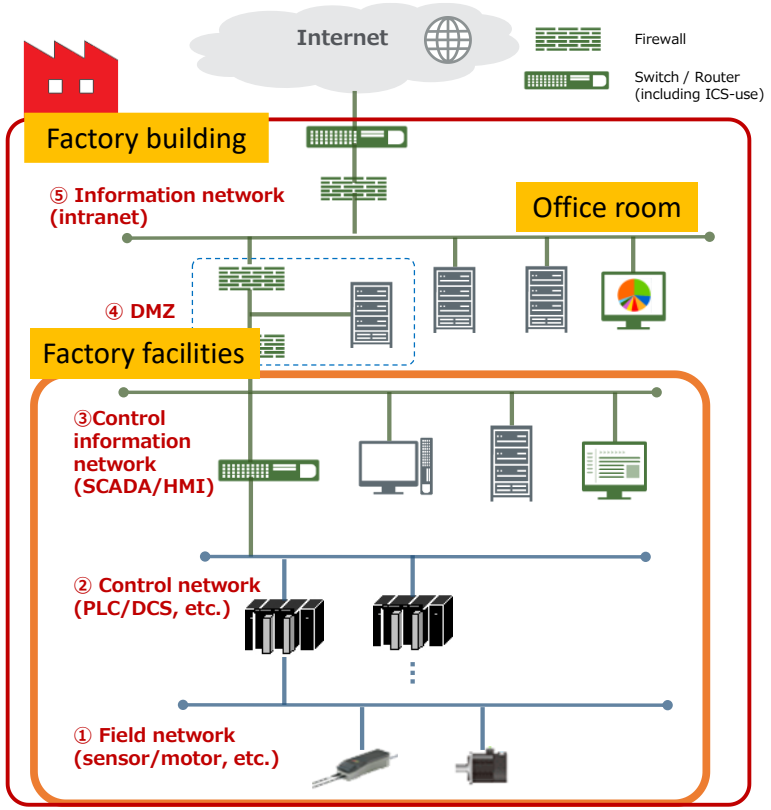


Figure 3-10 Network diagram of a factory's general manufacturing equipment

On the other hand, with the advancement of DX, security risks have increased due to the introduction of IT technology and increased connections to the outside for the purpose of improving production efficiency, remote maintenance, etc. In fact, there are security incidents where, for example, ransomware targeting information systems has spread to factory facility systems, resulting in production shutdown.

To reduce supply chain risks, regulations and guidelines stipulating security requirements for suppliers and their procured goods have been established, mainly overseas, which are also applicable to factory facilities.

Due to such changes in the business environment, the importance of security measures for factory facilities has increased, and many manufacturers in Japan have begun to take security measures for their factory facilities.

Security measures for factory facilities are broadly classified into the following three categories.

- Establishment of organizational structure
  Establishment of an organization responsible for factory security measures, cooperation with the information systems department, human resource development related to factory security, training of field personnel, etc.
- Formulation of operation procedures
  Management of cyber assets in factory facilities, implementation of risk analysis of factory facilities, formulation of security policies, formulation of BCP and incident response procedures involving cybersecurity factors, etc.
- Introduction of technical measures
  Network boundary protection with information systems, monitoring of plant facility network, introduction of anti-virus measures to terminals, etc.

In factory facilities, it is sometimes difficult to introduce technical measures because it is necessary to operate terminals for which support has ended or security patches cannot be applied for reasons of availability, and therefore, it is essential to reduce risks in conjunction with the establishment of organizational structure and operational procedures. Therefore, implementation of comprehensive security measures after understanding the risks of your organization's factory facilities is required, but the reality is that there is a shortage of human resources to promote such measures.

Please refer to the "Core Human Resource Development Program," "Program for Managers," "Program for Practitioners", and "Program for Supervisors", etc. offered by the "Industrial Cybersecurity Center of Excellence (ICSCoE)" of the Information-Technology Promotion Agency (IPA) for the development of security personnel for control systems.

URL: https://www.ipa.go.jp/icscoe/

Column: Security of Development Environment (Kenzo Yoshimatsu, Control System Security Center, Member of Space Industry SWG)

There are situations where the development environment established during the product or system development process needs to be reconstructed in order to address defects, etc.

The following points must be kept in mind when reconstructing the development environment.

- The period during which the development environment may need to be reconstructed spans a long period of time that exceeds the useful life of the product or system.
- The security status can be greatly affected by the slightest difference in the development environment.

While taking these points into consideration, the 3 items that should be kept in mind regarding the development environment:

- Compiler
  Even with the same source, different [54] compilers generate different binary code. In a security product or system, if the binary code differs even slightly, the possibility of an impact on the security status of the product increases. When fixing product defects, the possibility of degradation can be reduced by using the same compiler used during development.
- Third party tools
  Third party tools that install specific software on specific hardware allow software upgrades but may not allow downgrades. For example, for active automated testing tools like fuzzing, the version of the software may change while the tool is used in various development and testing processes. As a result, when attempting to reconstruct the development environment, the version of the software used at the time of development cannot be installed.
  When using third party tools, it is necessary to carefully check whether or not software downgrades may be required when reconstructing the development environment, and whether it is possible to downgrade the tool used when software downgrade is necessary.
- Proprietary tools
  When developing and using a proprietary tool for the development environment, configuration management must be performed for the design documents of the tool, and the tool itself must also be stored. However, when the need to reconstruct the development environment arises long after development has been completed, the proprietary tool may not work well or the tool itself may not be found. In this case, the tool is created again based on the tool design documents, but the parts from that time may not be available. If parts with guaranteed compatibility are not available, a new tool design is required. Considering that such a situation may arise, when developing a proprietary tool, it is desirable to maintain a document describing the required specifications that the tool must satisfy, as a configuration document, as in the case of product design.

[54] Includes compilers with different versions

4. Appendix

4.1 Definitions of Terms

Terms	Definition in these guidelines
Backdoor	A connection window for remote control that is secretly planted as part of a software or system without the knowledge of the administrator or user.
C&C server	A server computer responsible for controlling and sending commands to computers compromised during a cyber-attack using a computer hijacked by an outside invader.
Constellation	A type of satellite operation, in which multiple satellites, either of the same or different types, collaborate and cooperate to execute a common mission.
Data users	Corporate or individual users who utilize satellite data to achieve business or research objectives.
DDoS	An attack method where a large number of devices on the Internet simultaneously overload a specific network or computer, causing it to malfunction.
Development and manufacturing facility	A generic term for such as facilities, equipment, systems, for satellite and ground system development, including such as OT systems (FA systems), IT systems (OA systems, etc.), inspection equipment.
Facility	Facility functions for satellite operation, satellite data utilization, and satellite development and utilization, and each facility has systems and subsystems. Facility > System > Subsystem
Fuzzing	A method of detecting vulnerabilities by sending a large amount of test data that is likely to cause problems in software and other products and monitoring their responses and behavior.
Ground station service provider	A business operator providing tracking and control services or reception services by maintaining tracking and control stations or reception stations necessary for satellite operations.
Ground system	A generic term for facilities and systems installed on the ground for launch, operation, data utilization, development, and manufacturing of satellite systems, including such as rocket launch facilities, satellite operation facilities, satellite data utilization facilities, and development and manufacturing facilities.
Housekeeping data	Data indicating the status of a spacecraft in orbit, such as power, temperature, position, and location, of the satellite.
Jamming	Interference with normal communications, such as sending out radio waves same in frequency band as the radio waves for radar and communications, causing radio interference.
Keylogger	Software that records a user's keyboard operation regardless of the user's intention.
Lateral movement	An attack method in which malware invades the network of an enterprise or organization and exploits the legitimate functions to perform internal reconnaissance and steal credentials.

Terms	Definition in these guidelines
Malware	Software that interferes with the normal use of a computer and performs actions that are harmful to users and computers.
Ransomware	A virus that renders data on PCs and other terminals and servers unusable by encryption or other means and displays a threatening message urging the user to pay a ransom in exchange for recovering the data.
Reception service	A service that maintains a receiving station and receives data sent from a satellite on your behalf.
Replay attack	An attack method in which the transmission and reception of authentication data used to verify a user is eavesdropped, and the obtained data is used as it is to spoof that user.
Rootkit	Software packaged with malicious software such as attack tools and eavesdropping tools.
Satellite data platform operator	A business entity that provides such as satellite data storage and analysis functions and enable cross-sectional data linkage and analysis. Includes businesses that provide services in the form of a cloud.
Satellite data service provider	A service provider that maintains such as mission data processing systems, storage and retrieval systems, observation reception and data distribution processing systems, and provides services to facilitate the use of satellite data by data users.
Satellite data utilization facility	A generic term for facilities that such as perform data storage, data processing, observation reception, and data distribution.
Satellite developer	A business entity that plans, develops, and manufactures satellite systems.
Satellite developer and operator	A business entity that develops, manufactures, operates, and disposes of satellites. The entity may also be the satellite owner.
Satellite operation facility	A generic term for facilities that operate satellites, such as tracking and control stations, receiving station, and such as mission control systems, etc.
Satellite operator	A business entity that maintains ground stations (tracking and control station and receiving station) or operates satellites in orbit using ground station service providers.
Satellite owner	A person who procures a satellite and is responsible for the satellite unit. In some cases, satellite development and manufacturing, satellite operation, satellite data utilization, and disposal are all carried out by the satellite owner, while in other cases, such as satellite operation is outsourced to such as a satellite operator.
Satellite system	A generic term for scientific satellites and other space probe, supply spacecraft that send supplies and astronauts to the International Space Station, and such as artificial satellites that perform positioning, communications and broadcasting, weather observation, and Earth observation.
Satellite unit	Individual satellites in a satellite system that perform positioning, communications and broadcasting, weather observation, and Earth observation. The guidelines focus particularly on microsatellites and small satellites.

Terms	Definition in these guidelines
Spoofing	Pretending to be a specific person other than yourself and acting on behalf of that person.
SQL injection attacks	An attack where an unauthorized access to a database is gained by directly inputting a string of SQL commands into the input screen of such as an Internet website, to obtain information, destroy the database, or falsify the web page.
Tracking and control service	A service that maintains the tracking and control stations necessary for satellite operations and performs satellite tracking and control on your behalf.
Trojan horse	Software that is introduced under the guise of a useful software that the user is prompted to install and execute, and once activated, secretly performs harmful operations such as data leakage or remote control without the knowledge of the user.
Vulnerability	A security weakness in such as software.
Worm	Software that invades a computer through such as the Internet, and further attempts to replicate itself on other computers and performs harmful operations.
Zero-day vulnerability	A vulnerability for which no countermeasures or fixes, have been provided by the software or device developer.

4.2 Abbreviations

Abbreviation	Term
ADCS	Attitude Determination and Control Subsystem
AIAA	American Institute of Aeronautics and Astronautics
AOCS	Attitude and Orbit Control Subsystem
ASAT	Anti-satellite Weapon
C&DH	Command and Data Handling
CAN	Controller Area Network
CCCS	Canadian Center for Cybersecurity
CCSDS	Consultative Committee for Space Data System
CDI	Contexts and Dependency Injection
CI	Classified Information
CIA	Central Intelligence Agency
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
CNE	Computer Network Exploitation
CMMC	Cybersecurity Maturity Model Certification
CNSS	Committee on National Security Systems
CPSF	Cyber/Physical Security Framework
CRYPTREC	Cryptography Research and Evaluation Committees
CSEC	Communications Security Establishment
CSF	Cybersecurity Framework
CUI	Controlled Unclassified Information
DFARS	Defense Federal Acquisition Regulation Supplement
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DL	Downlink
DMZ	Demilitarized Zone
DoD	Department of Defense
DoDI	Department of Defense INSTRUCTION

Abbreviation	Term
DOJ	Department of Justice
DSN	Deep Space Network
ECM	Engineering Chain Management
ESA	European Space Agency
FA	Factory Automation
FBI	Federal Bureau of Investigation
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act Federal Information Security Modernization Act
FW	Firewall
GNSS	Global Navigation Satellite System
HW	Hardware
IaaS	Infrastructure as a Service
ID	Identification
IEC	International Electrotechnical Commission
IoT	Internet of Things
IPA	Information-technology Promotion Agency, Japan
ISAC	Information Sharing and Analysis Center
ISMAP	Information System Security Management and Assessment Program
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
IV&V	Independent Verification & Validation
JAXA	Japan Aerospace Exploration Agency
J-CRAT	Cyber Rescue and Advice Team against targeted attack of Japan
JPCERT/CC	Japan Computer Emergency Response Team Coordination Center
NASA	National Aeronautics and Space Administration
NIST	National Institute of Standards and Technology
NRO	National Reconnaissance Office

Abbreviation	Term
NSA	National Security Agency
NSC	National Security Council
NSD	National Security Directive
NSTISSC	National Security Telecommunications and Information Systems Security Committee
OA	Office Automation
OS	Operating System
OSA	Orbital Security Alliance
OSS	Open Source Software
OT	Operational Technology
PaaS	Platform as a Service
PC	Personal Computer
PNT	Positioning, Navigation and Timing
RF	Radio Frequency
SaaS	Software as a Service
SDR	Software-Defined Radio
SLA	Service Level Agreement
SP	Special Publication
SPD	Space Policy Directive
SW	Switch
SW	Software
SWG	Sub Working Group
TT&C	Telemetry, Tracking and Command
UL	Uplink
USSF	United States Space Force
VPN	Virtual Private Network
VSAT	Very Small Aperture Terminal
WG	Working Group

4.3 Development of the Guidelines

The guidelines were compiled through discussions by the following expert groups based on the results of the Ministry of Economy, Trade and Industry's projects implemented between FY2020 and FY2022.

Relevant Expert Study Groups

	Name of the expert study group	Working period
a	Space Industry SWG	Since January 14, 2021
b	Space Industry SWG Working Committee Core Member Meeting	Since February 15, 2021
c	Space Industry SWG Working Committee	Since February 15, 2021

As of January 2023

List of Expert Study Group Members

Name of the expert	Affiliation (As of January 2023)	Participating Group (a to c in the table above)		
		a	b	c
Osamu Kashimura	Japan Space Systems (JSS)	●		
Hiroshi Koyama	Mitsubishi Electric Corporation	●		
Haruhiko Kataoka	IHI Corporation (former Chief of Staff of the Japan Air Self-Defense Force)	●		
Megumi Kinoshita	Information-technology Promotion Agency, Japan (IPA)	●	●	●
Toshinori Kuwahara	Tohoku University University Space Engineering Consortium (UNISEC)	●		
Tetsuya Sakashita	Japan Institute for Promotion of Digital Economy and Community (JIPDEC)	●		
Hiroshi Sasaki	Fortinet Japan LLC	●	●	●
Toshio Nawa	Cyber Defense Institute, Inc.	●		
Mitsuhiko Maruyama	PwC Consulting LLC	●		
Takuho Mitsunaga	Toyo University ICSCoE, Information-Technology Promotion Agency (IPA)	●		
Kenzo Yoshimatsu	Control System Security Center (CSSC)	●	●	●
Takanori Awatsu	Skygate Technologies Co., Ltd.		●	●
Kenji Uesugi	PwC Consulting LLC		●	●
Ryuichi Kokubo	Axelspace Corporation		●	●
Yusuke Koide	Synspective Inc.		●	●
Suzumoto Ryo	ArkEdge Space Inc.		●	●

Name of the expert	Affiliation (As of January 2023)	Participating Group (a to c in the table above)		
		a	b	c
Yasuo Takahashi	Mitsui Bussan Secure Directions, Inc.		●	●
Hiroshi Tanaka	Mitsubishi Electric Corporation		●	●
Tomomi Nio	Japan Aerospace Exploration Agency (JAXA)		●	●
Toshifumi Hiramatsu	Pasco Corporation		●	●
Tomoyoshi Goda	NEC Corporation		●	●
Regarding "Space Industry SWG Working Committee," the following stakeholders participated in addition to the members mentioned above: Remote Sensing Technology Center of Japan; Space Engineering Development Co., Ltd.; Astroscale Holdings Co., Ltd.; ALE Co., Ltd.; Hitachi Solutions, Ltd.; Canon Electronics Inc.; SAKURA Internet Inc.; SKY Perfect JSAT Corporation; Japan Space Imaging Corporation; Fujitsu Limited; McAfee, LLC				
Observers	Cabinet Office Space Development Strategy Promotion Office Cabinet Secretariat, National Center of Incident Readiness and Strategy for Cybersecurity Cabinet Secretariat, Cabinet Satellite Intelligence Center Ministry of Internal Affairs Ministry of Education, Culture, Sports, Science and Technology Ministry of Defense Japan Aerospace Exploration Agency			
Secretariat	Space Industry Office, Manufacturing Industry Bureau, Ministry of Economy, Trade and Industry Mitsui Bussan Secure Directions, Inc. (FY 2020, FY 2021) Mitsubishi Research Institute, Inc. (FY 2022)			

As of January 2023