METI
Ministry of Economy, Trade and Industry

Cybersecurity Guidelines for Commercial Space Systems Ver 1.1

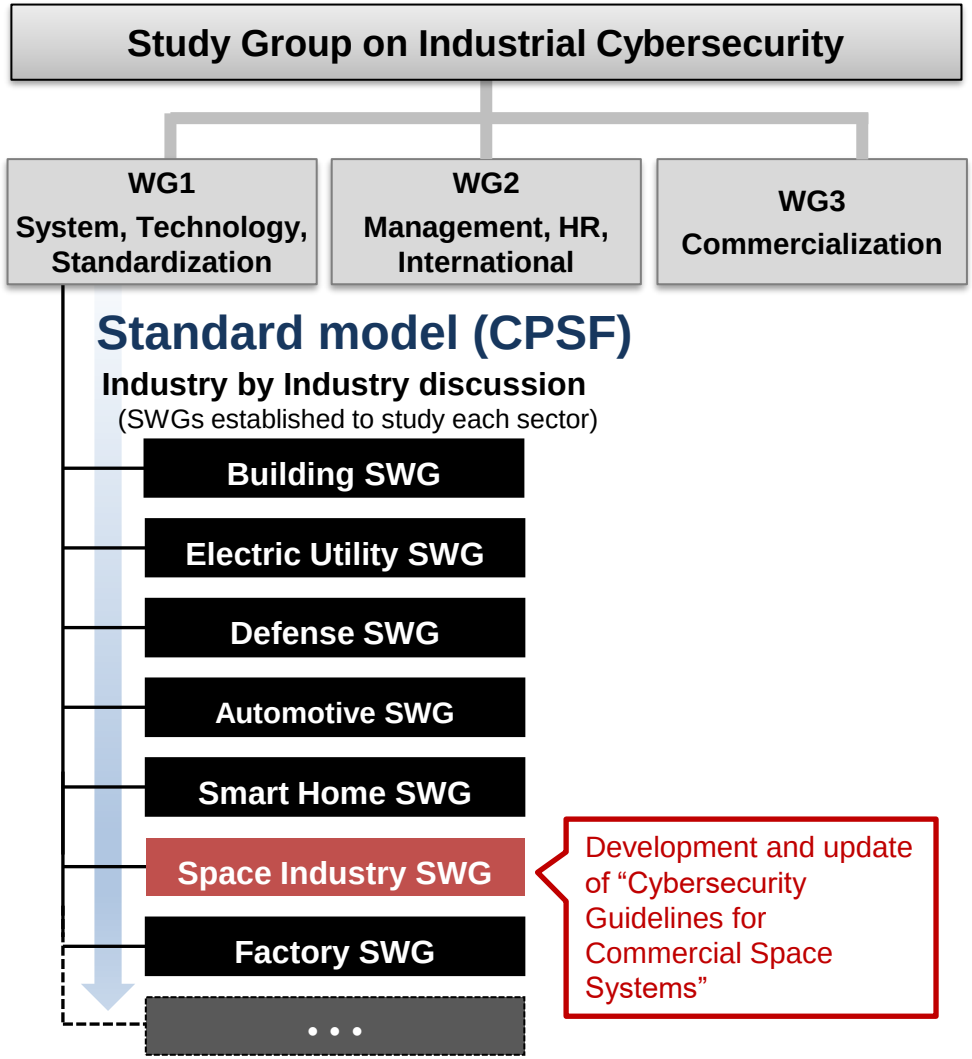
Summary

March, 2023

Space Industry Office,
Manufacturing Industries Bureau,
Ministry of Economy, Trade and Industry

Organization to Promote Cybersecurity of Commercial Space Systems

- METI is promoting cybersecurity measures for each industrial sector under the Study Group on Industrial Cybersecurity.
- The “Space Industry SWG” was established in January 2021.



Experts	Affiliation (as of January 2023)	Space Industry SWG	Space Industry SWG Working Committee
Osamu Kashimura	Japan Space Systems (JSS)	✓	
Hiroshi Koyama	Mitsubishi Electric Corporation	✓	
Haruhiko Kataoka	IHI Corporation	✓	
Megumi Kinoshita	Security Center, Information-technology Promotion Agency, Japan (IPA)	✓	✓
Toshinori Kuwahara	Department of Aerospace Engineering, School of Engineering, Tohoku University	✓	
Tetsuya Sakashita	Japan Institute for Promotion of Digital Economy and Community (JIPDEC)	✓	
Hiroshi Sasaki	Fortinet Japan G.K.	✓	✓
Toshio Nawa	Cyber Defense Institute, Inc.	✓	
Mitsuhiko Maruyama	PwC Consulting LLC, JP	✓	
Takuho Mitsunaga	Department of Information Networking for Innovation and Design, Toyo University	✓	
Kenzo Yoshimatsu	Control System Security Center (CSSC)	✓	✓
Takanori Awatsu	Skygate Technologies Corporation		✓
Kenji Uesugi	PwC Consulting LLC, JP		✓
Ryuichi Kokubo	Axelspace Corporation		✓
Yusuke Koide	Synspective Inc.		✓
Ryo Suzumoto	ArkEdge Space Inc.		✓
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		✓

Table of Contents of the Guideline

Background and Purpose

Section 1.1 of the guidelines

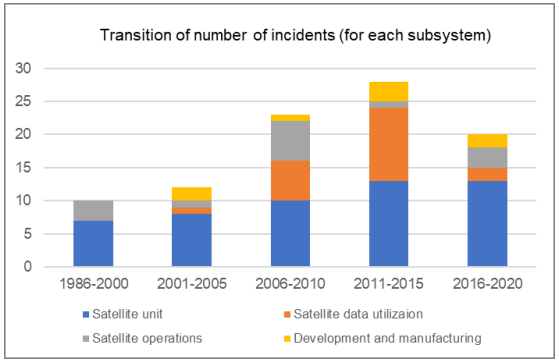
- While the role of commercial space systems is extending in national security and economic society in Japan, there are growing concerns about cybersecurity of commercial space systems.
- The guidelines encourage to implement cybersecurity measures by space companies.

●Factors that make securing space systems both important and difficult

- **Extending role of space systems** in security and the economic society of Japan
- **Spread of digital technology**, including unmanned and automated space systems and increased use of cloud services
- **Advancing 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

● Increase in incidents of space systems

- 1986-2020:
  More than 90 incidents occurred both inside and outside Japan.
- 2017-2020:
  Over 6,000 cases of cyberattacks, including phishing and malware, have been detected by the National Aeronautics and Space Administration (NASA).



● Cybersecurity measures implemented by Europe and the United States for space systems

- April 2019, United States: Space ISAC was established by public and private sector partnership [Private sector, NASA, United States Space Force and National Reconnaissance Office].
- May 2020, United Kingdom: “Cybersecurity Toolkit Ver. 2” was published for product suppliers to the space industry [UK Space Agency].
- September 2020, United States: **Executive Order SPD-5 , “Cybersecurity Principles for Space Systems”, was published.**
- February 2022, United States: **Introduction to Cybersecurity for Commercial Satellite Operations (NISTIR 8270, 2nd Draft) was published. [NIST]**
- December 2022, United States: **Satellite Ground Segment: Applying the Cybersecurity Framework to Satellite Command and Control (NISTIR 8401) was published. [NIST]**

● Purpose of development of the guidelines

The purpose of the guidelines is to encourage businesses to take voluntary cybersecurity measures, by summarizing and presenting the following in an easy-to-understand format, from **the perspective of business promotion of space operators in the commercial and mitigation of management risks posed to these operators, such as bankruptcy due to cyberattacks**:

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

Scope of the Guidelines

Section 1.2 of the guidelines

- The guidelines cover satellite systems (earth observation satellites) and ground systems (satellite operation facilities, satellite data utilization facilities, development and manufacturing facilities) operated by commercial companies.
- The guidelines cover the design, development, manufacturing, operation, maintenance, and disposal phases of satellite systems.
- The guidelines focus mainly on ground system operation and maintenance phases and describe the important points to be noted during each phase, from system design to disposal.

Scope of 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 the guidelines.

Structure of the Guidelines and Intended Readers

Section 1.3 of the guidelines

- Past incidents involving space systems and significant cybersecurity risks anticipated for space systems are summarized in “2. Cybersecurity Situation of Space Systems”.
- Measures common to all organizations associated with space systems and measures unique to space systems are summarized under “3. Key Points of Security Measures for Commercial Space Systems”.

	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 for tracking and control station services or receiving station services.

Intended Use of the Guidelines

Section 1.4 of the guidelines

Users:

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

Notes:

- When considering the measures described in the guidelines may be tailored (customized) based on the characteristics and importance of the target systems, risk assessment results and business environment of the operators, etc.
- When multiple stakeholders are considering common measures, tailoring (customization) of the measures must be discussed, agreed upon, and approved by the stakeholders.
- Attachment 1 includes a checklist summarizing Requirements and Measures, while Attachment 2 shows 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.

Incident Case Studies of Space Systems

Section 2.1 of the guidelines

- Over 90 cybersecurity incidents related to the space sector occurred inside and outside Japan between 1986 and 2022.
- Typical examples of recent incidents that came to light in countries other than Japan are listed below.

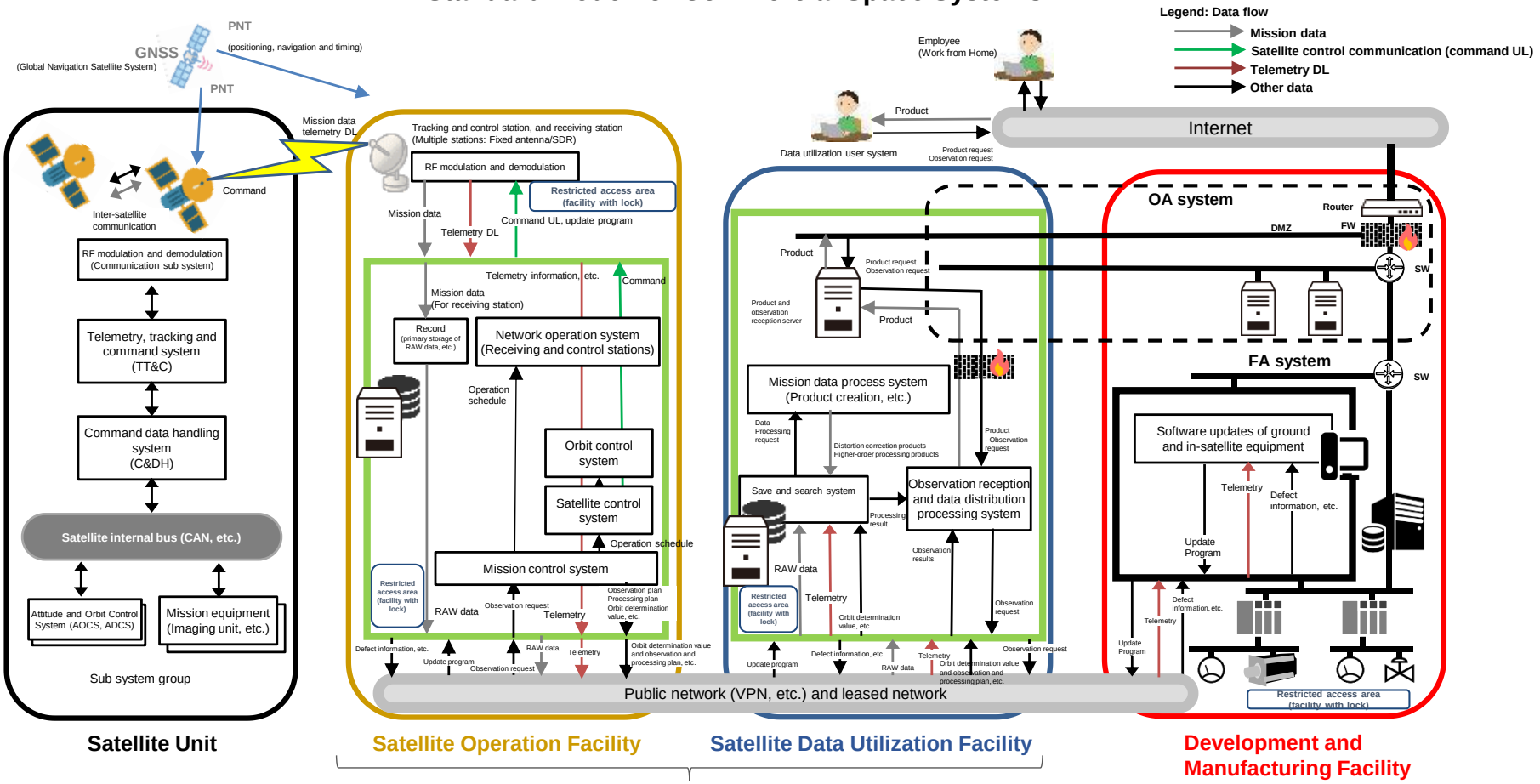
Year	Target	Impact	Overview
2014	NOAA Meteorological observation NW	Satellite data could not be viewed	A meteorological observation satellite network of the National Oceanic and Atmospheric Administration (NOAA) was the target of a cyberattack through the Internet.
2015	Iridium Communication satellite	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 a total of about 50 euros) and convert it into clear text information (plain text).
2018	NASA Jet Propulsion Laboratory (JPL)	Disclosure of mission data	A hacker gained unauthorized entry into JPL's network using Raspberry Pi installed by a staff member without authorization and moved across several systems. The internal activity was carried out for about ten 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 a total of about 300 dollars). The analysis of the communication revealed that communications on all the 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, credit card data, etc.), 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 Viasat's communication satellite service "KA-SAT" 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 remote control of more than 7,800 wind turbines managed by several power companies.
2022	Space X Satellite ground equipment	Stopped the internet connection service	The Starlink service, which is a satellite constellation- based Internet connection service provided by US 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 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 suspension of all observations.

Standard Model for Commercial Space Systems

Section 2.2 of the guidelines

- The following standard model was developed by creating an overall image of commercial space systems by analyzing a remote sensing microsatellite.

Standard Model for Commercial Space Systems



Operating some or all functions from the cloud is increasing

<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.

(Created for the system of earth observation microsatellites)

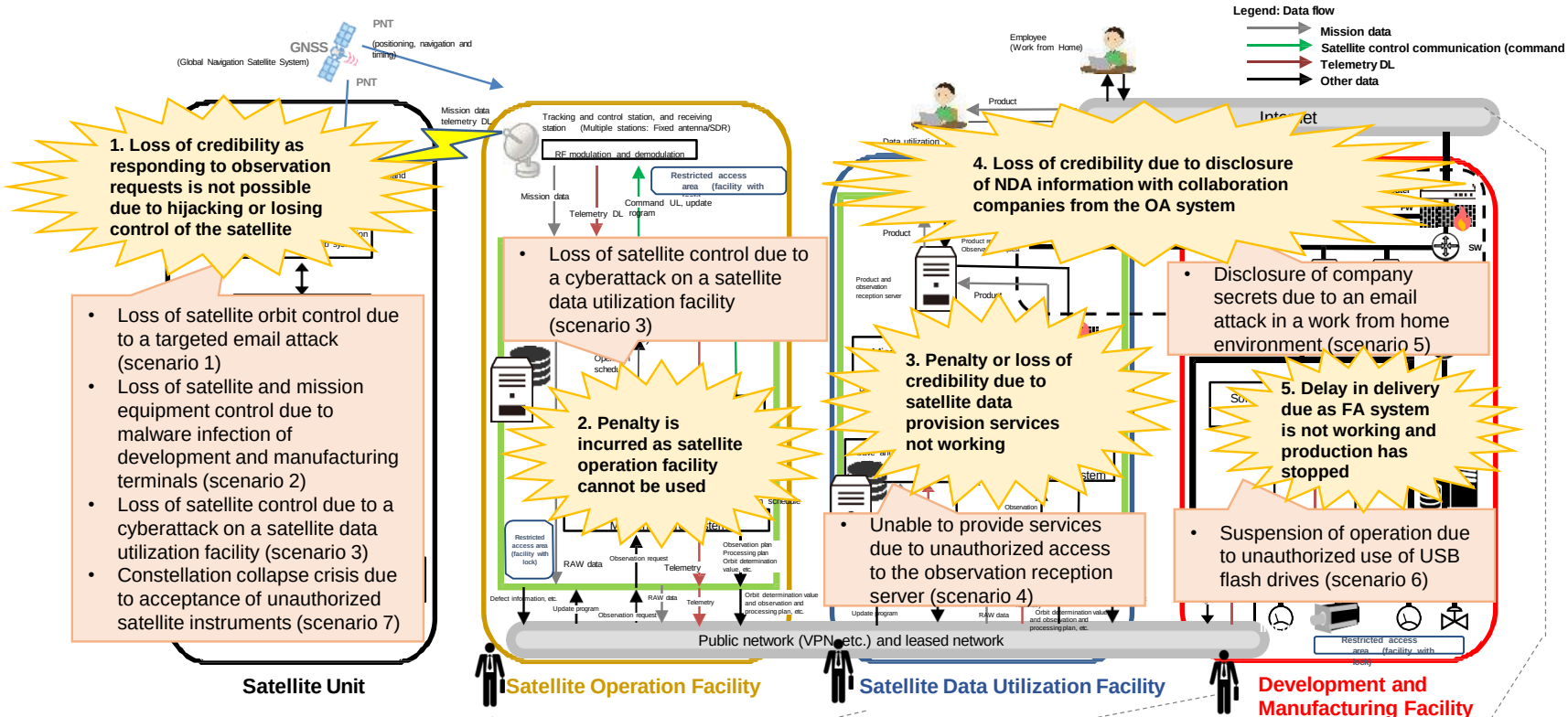
<Organization>
- Satellite developers and operators, etc.

Potential Risk Scenarios

Section 2.2 of the guidelines

- Seven example scenarios that can cause serious harm to businesses were summarized based on the Standard Model for Commercial Space Systems.

Seven Risk Scenarios Associated with Commercial Space Systems and the Impact



	Communication between satellite and ground stations	Employees and contractors who enter and leave	Supply chain risk	Internet
Example of entry points				
Example of attack methods	• Interception of communications • Spoofing • Replay attack • Jamming, etc.	<Malicious activities> • Taking out plans for design by USB <Carelessness activities> • Unauthorized intrusion due to connection of unauthorized terminals, etc.	<Malicious activities> • Tampering with unauthorized HW/SW, etc. <Carelessness activities> • Attacks due to OSS vulnerabilities, etc.	• 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

Primary Measures Needed for Each Subsystem (1)

Section 2.2 of the guidelines

- Primary measures needed for each subsystem are summarized based on the 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	–

Primary Measures Needed for Each Subsystem (2)

Section 2.2 of the guidelines

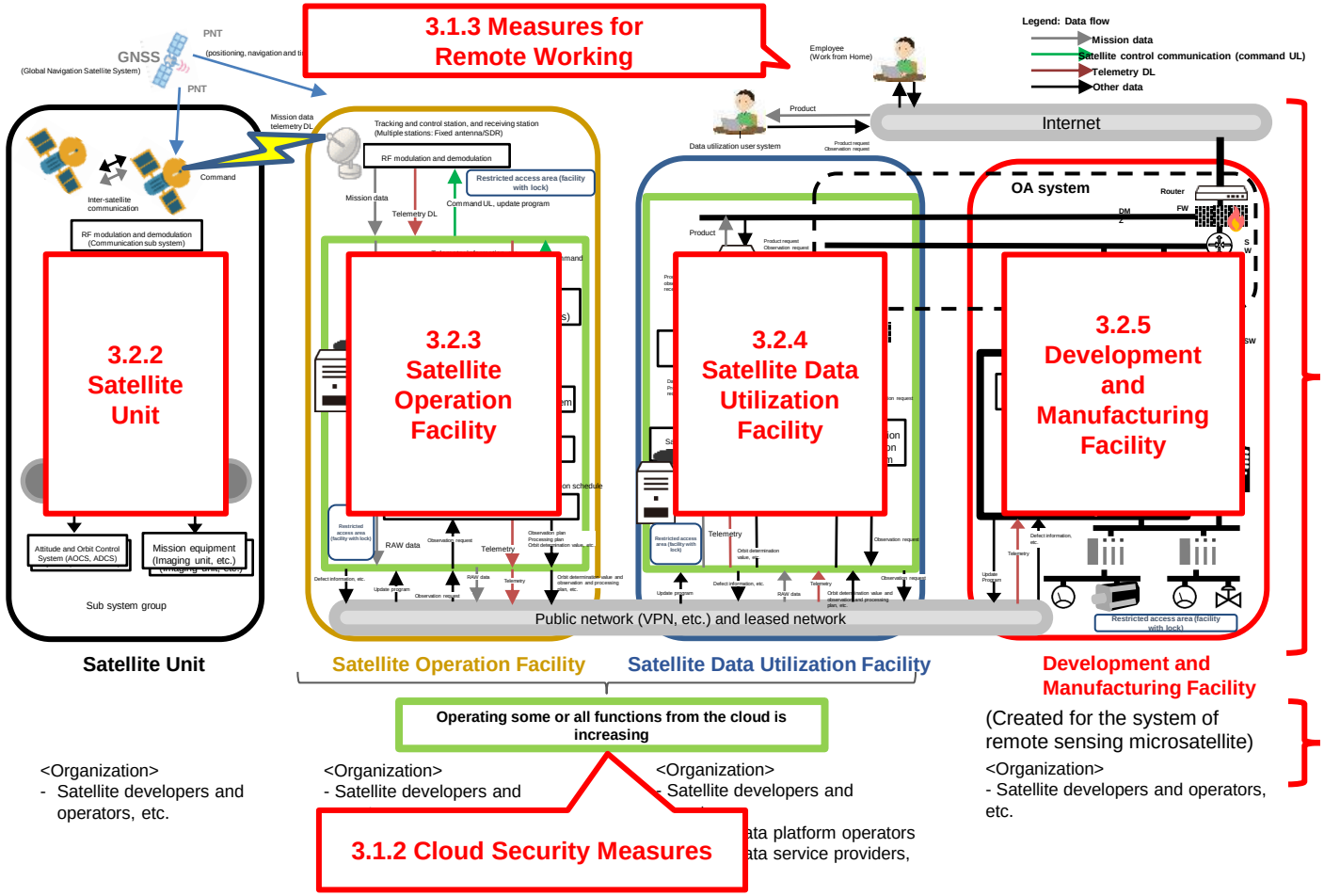
No.	Example of a risk scenario that will lead to a major business damage	Primary measures				
		Satellite unit	Satellite operation facility	Satellite data utilization facility	OA system	Development and manufacturing facility
Scenario 5	While working from home, the computer of an employee was infected 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)

Overview of Cybersecurity Measures for the Commercial Space Systems

Section 3 of the guidelines

- The measures of the guidelines are summarized based on the standard model for commercial space systems.
- Section 3.1 of the guidelines describes measures common to all organizations, while section 3.2 describes specific measures for each subsystem.

Outline of Common Measures for Commercial Space Systems and Specific Measures to Each Subsystem



Description of Measures in the Guidelines

Section 3 of the guidelines

- The cybersecurity measures that each stakeholder should consider and work on and the information that can be used as a reference when considering the measures are classified under 3 items: “Requirements”, “Basic measures” and “Details”.
- When examining specific measures, it is important to consider the measures described under “Basic measures”, contents of the referenced guidelines, etc., and “Details”.

Three items of cybersecurity measures in the guidelines

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 “**Basic measures when a high-security level is required**”.

Details
indicate additional and reference information concerning requirements and corresponding basic measures.

Correspondence of Each Stakeholder and the Cybersecurity Measures in the Guidelines (1)

Section 3 of the guidelines

- Requirements indicate items to be considered and addressed by each stakeholder specified clearly.
- Basic measures indicate examples of widespread practices and measures 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 "Basic measures when a high-security level is required".

Category	Ch. and 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)	✓	✓	✓	✓	✓

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

Correspondence of Each Stakeholder and the Cybersecurity Measures in the Guidelines (2)

Section 3 of the guidelines

- Requirements indicate items to be considered and addressed by each stakeholder specified clearly.
- Basic measures indicate examples of widespread practices and measures 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 "Basic measures when a high-security level is required".

Category	Ch. and 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	3.1.3	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.

Correspondence of Each Stakeholder and the Cybersecurity Measures in the Guidelines (3)

Section 3 of the guidelines

- Requirements indicate items to be considered and addressed by each stakeholder specified clearly.
- Basic measures indicate examples of widespread practices and measures 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 "Basic measures when a high-security level is required".

Category	Ch. and 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 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	✓	✓	-	-	✓

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

Correspondence of Each Stakeholder and the Cybersecurity Measures in the Guidelines (4)

Section 3 of the guidelines

- Requirements indicate items to be considered and addressed by each stakeholder specified clearly.
- Basic measures indicate examples of widespread practices and measures 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 "Basic measures when a high-security level is required".

Category	Ch. and 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	3.2.3	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.