https://doi.org/10.7840/kics.2023.48.11.1525

Improvement Measures for Aviation Security Policies and Security Management System Against Potential Cyber Threats In-Flight

Sanghoon Jeon◆

ABSTRACT

In light of providing in-flight wired and wireless networks, and Internet services, there is a current exposure to potential cyber threats. Given the rapidly evolving ICT technology and aviation services, it is crucial to approach aviation security policies in a balanced and systematic manner. The widening gap between advancing technology and outdated aviation security policies makes it difficult to effectively address unpredictable aviation security threats and ensure the safety of aviation services. Therefore, proactive measures such as revising aviation security policies and regulations and establishing a cyber risk management system are urgently needed. This paper aims to propose improvement measures for responding to potential cyber threats and establishing aviation security policies and management systems to ensure safe aviation operations and navigation.

Key Words : Aviation security, Aviation policy, Wireless network security, Cyber threats, In-flight threats

Ⅰ. Introduction

Common aviation security threats refer to actions taken during flight operations that pose a threat to aircraft safety, such as aircraft terrorism, hijacking, and in-flight disturbances. Accordingly, in the domestic context, the 「Aviation Security Act」 and the 「Aviation Safety Act」 are in place to protect aircraft operations and navigation. Article 1 of the 「Aviation Security Act」 establishes standards, procedures, and obligations to prevent unlawful acts within airport facilities, navigation safety facilities, and inside aircraft, ensuring the security of civil aviation in accordance with international agreements, such as the 「International Civil Aviation Organization」. Additionally, the 「Aviation Safety Act」 regulates methods for ensuring safe and efficient aircraft navigation, along with the obligations of the country, airline operators, and aviation personnel to ensure safety and security against threats. These measures align with physical security policies[1,2].

However, with the rapid advancement of Information and Communications Technology (ICT), wireless networks and Internet services are now provided to general passengers inside the aircraft. Recently, in-flight entertainment systems and Internet services are made available using technologies such as Wi-Fi, Bluetooth, and computer communication technologies such as Gatelink for aircraft-to-ground communication. Moreover, cockpit Electronic Flight Bags (EFBs) operated by pilots and Special Handling Reports (e-SHRs) used by cabin crew are used for aircraft operations[3].

The provision of wireless networks and Internet services on aircrafts has raised concerns about potential cyber threats. However, the reality is that there is a lack of detailed guidelines addressing potential cyber threats that could interfere with aircraft operations and navigation, or lead to illegal in-flight activities. Although efforts are made to follow

◆ First Author : Far East University Department of Hacking & Security, randyjeon@gmail.com, 정회원

논문번호 : 202307-020-0-SE, Received July 25, 2023; Revised August 14, 2023; Accepted August 27, 2023

international standards and recommendations adopted by agreements or annexes under the 「International Civil Aviation Organization」[4], these international standards and recommendations do not provide specific guidelines on dealing with clear cyber threats. Additionally, there are no domestic laws or orders of legal force in this regard. Specific cyber threats and vulnerabilities were addressed using the response guidelines provided by the FAA and ICAO.

Cybersecurity incidents targeting civilian airlines commonly involve breaches targeting the airline's IT infrastructure, and they are protected by laws such as the 「Act on Promotion of Information and Communications Network Utilization and Information Protection」 and the 「Personal Information Protection Act」. However, the current reality is the absence of clear security policies and regulations that effectively protect communication information, operational data, and passengers' personal information within an aircraft and respond to cyber threats. Dealing with active and sometimes passive potential cyber threats is challenging under existing laws owing to ambiguous physical protection measures, such as illegal activities, interference with operations, and restrictions on electronic device usage.

To respond to this ambiguity and uncertainty, a proactive improvement of aviation security policies and security management systems is required. This includes establishing clear criteria for potential cyber threats and security obligations, and defining illegal or violation cases in a timely manner.

Therefore, this study proposes improvement measures for aviation security policies and related laws concerning the provision of wireless networks and Internet services on aircrafts as well as enhancements to aviation security management systems to effectively address cyber threats. Technical explanations are not included within the scope of this study.

Ⅱ. Related

2.1 Current Status of Domestic Aviation Security Policies

As shown in Table 1, there have been consecutive incidents and accidents occurring in domestic airports, navigation safety facilities, and inside aircraft during the first half of 2023[5]. Actions that disrupt aircraft operations, interfere with navigation, or pose threats to safety are subject to domestic laws such as the 「Aviation Security Act」 and the 「Aviation Safety Act」, providing a legal basis for addressing these unlawful activities. On the other hand, security incidents like personal data breaches are comprehensive breaches occurring in airline IT infrastructures, and they are governed by legal frameworks such as the 「Personal Information Protection Act」, the 「Act on Promotion of Information and Communications Network Utilization and Information Protection」, and the 「Act on Information and Communication Network-Based Services Promotion and Information Protection」.

However, at present, there is a lack of clear laws, regulations, and guidelines concerning cyber security threats that could potentially occur inside aircraft. The urgency lies in the need for aviation security policies, standards, and management systems to ensure the safety and security of aircraft operations.

While the use of electronic devices is controlled during takeoff and landing in aircraft that support information technology, there is no control over the use of computers like laptops and tablets during flight. Furthermore, in certain aircraft models, the provision of in-flight wireless networks and internet services has

Table 1. Cases of domestic aviation security accidents in 2023.

Date of the incident	Security incident details	Location of occurrence
'21.3.8	Airline customer personal information leakage incident	Airline
'23.3.26	A Kazakhstani person who was denied entry crossed the fence	Airport
'23.4.3	U.S. citizen found carrying live ammunition	Aircraft
'23.4.6	Chinese passenger passes security check with a concealed weapon	Airport
'23.6.19	Disruptive behavior on board aircraft, forced illegal opening of emergency exit	Aircraft
'23.6.21	Attempted emergency exit opening by a drug-positive teenager	Aircraft

raised concerns about potential threats, where unauthorized access to aircraft systems by unidentified passengers has been reported[6,7]. Current physical security control regulations such as restrictions on illegal activities like interference with radio signals and electronic device usage limitations do not adequately address proactive responses to cyber security threats that may not be visible within the aircraft. There is a need for improvements in existing laws, regulations, and protective measures by introducing clear guidelines and provisions.

2.2 Limitations of International Civil Aviation Agreements and Standards

Aviation security-related laws, including the 「Aviation Security Act」 and the 「Aviation Safety Act」, mandate adherence to international civil aviation agreements. The international agreements listed in Table 2 require the enactment of laws within domestic jurisdictions to establish basic legal authority for conducting aviation security activities within the country's territory. These laws grant authority to designated authorities responsible for aviation security in the country, including the power to enforce aviation security rules, regulations, and procedures, which may include the designation of security restricted areas and the authority to screen passengers. The International Civil Aviation Organization (ICAO) recommends that contracting states protect the confidentiality, integrity, and availability of critical systems and data, including risk assessments performed by respective national entities, encompassing supply chain security, network segregation, protection of remote access capabilities, and limitations.

However, concerning cyber security threats and incidents, ICAO advises compliance with standards and guidelines from organizations such as International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) and National Institute of Standards and Technology (NIST) [8]. Private airlines cannot be compelled by public or specific agencies to collect and analyze proprietary assets and information, as there is a lack of relevant legislation. Therefore, ICAO recommends that airlines voluntarily establish systems. International standards and guidelines serve as recommendations rather than legally binding obligations, which limits their effectiveness in enhancing safety and security measures within the international civil aviation community.

Table 2. International legal instruments.

Date	Agreement content	Related document
1963.09.14	Tokyo Convention on Offenses and Certain Other Acts Committed on Board Aircraft (Tokyo Convention)	Doc 8364
1970.12.16	Hague Convention for the Suppression of Unlawful Seizure of Aircraft (Hague Convention)	Doc 8920
1979.09.23	Montreal Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (Montreal Convention)	Doc 8966
1971.09.23	Protocol Supplementary to the Montreal Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, signed on 24 February 1988 in Montreal (Montreal Protocol)	Doc 9518
1991.03.01	Convention on the Marking of Plastic Explosives for the Purpose of Detection, signed in Montreal (MEX Convention)	Doc 9571
2010.09.10	Beijing Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation, signed in Beijing (Beijing Convention)	Doc 9960
2010.09.10	Protocol Supplementary to the Beijing Convention for the Suppression of Unlawful Seizure of Aircraft, signed in Beijing (Beijing Protocol)	Doc 9959
2014.04.04	Protocol Amending the Convention on Offenses and Certain Other Acts Committed on Board Aircraft, adopted in Montreal (Montreal Protocol 2014)	Doc 10034

2.3 Potential Cyber Threats to Aircraft

Aircraft rely on the TCP/IP (Transmission Control Protocol/Internet Protocol) for communication between the on-board systems and ground systems, ensuring the control, navigation, operation, maintenance, and management of the aircraft. Real-time monitoring of aircraft status information is conducted, and data is continuously recorded in management systems to maintain information currency.

Aircraft on-board systems, such as the Aircraft Control System, Airline Information System, and In-flight Entertainment & Communication System, are interconnected and operated using firmware and software with network operation and control capabilities. Messages are exchanged between Air Traffic Control (ATC) centers using Controller Pilot Data Communications (CPDLC) and text transmissions via the Aircraft Communications, Addressing, and Reporting System (ACARS), enabling two-way data communication. For communication with ground terminals at airports, specific aircraft may adopt and operate access systems using wireless networks for information exchange between the ground and aircraft. In this way, computer communication technology is integrated into aircraft, providing various services[9-11].

However, aviation security guidelines and annexes provide general guidance on responding to cyber security threats and incidents. Nevertheless, they do not include detailed instructions on threat prevention activities like cyber penetration testing and evaluation or specific guidelines on software verification processes, vulnerability and security operation testing, and airworthiness assessment testing for confidentiality, integrity, and availability.

At the present stage, there is a need for updated and specific legal regulations and guidelines that protect comprehensive information and data operated within aircraft systems, and enable effective responses to cyber security threats. These should clearly define lawful violations and unlawful activities, along with the corresponding penalty criteria.

Ⅲ. The Necessity for Improvements in Current Aviation Security Policies and Related Laws

3.1 Limitations in Response Potential Cyber Threats

Electronic intrusions, as defined in Article 2 of the「Information and Communications Network Protection Act」[12], refer to methods such as hacking, computer viruses, logic bombs, service denials, or high-power electromagnetic waves used to attack electronic control and management systems.

Airports are protected under the「Airport Facilities Act」 and「Guidelines for the Protection of Major Information and Communications Infrastructure」, while airline IT infrastructures are governed by legal bases such as the「Information and Communications Network Protection Act」,「Act on Promotion of Information and Communications Network Utilization and Information Protection」, and the「Personal Information Protection Act」[13-17].

However, there is a problem with the existing「Aviation Security Act」,「Aviation Safety Act」, and related regulations and guidelines, as they lack response policies and related laws to address threats like electronic intrusions into in-flight information and communication systems. Article 23 of the「Aviation Security Act」 (Passenger Cooperation Obligations) stipulates that the use of electronic devices on board the aircraft that violates Article 73 of the「Aviation Safety Act」 (Restrictions on the Use of Electronic Devices) can be restricted. Electronic devices may be limited in use to prevent interference with in-flight navigation and communication equipment due to electromagnetic interference. Article 214 of the「Enforcement Rules of the Aviation Safety Act」 also restricts the use of portable electronic devices recognized not to cause electronic interference according to recommendations from aircraft manufacturers, except for devices such as portable voice recorders, hearing aids, cardiac pacemakers, electric razors, and others.

However, there are no restrictions on using laptops or tablets inside the aircraft, except during takeoff and landing. Furthermore, certain aircraft models provide in-flight wireless networks and internet services. As mentioned in Section 2.3, the absence of recognition of potential threats or electronic intrusions that may gain unauthorized access to interconnected in-flight operation, control, and management systems in aviation security and safety-related laws and regulations is evident. Current aviation services and ICT integration technologies are not adequately reflected in related laws, highlighting existing issues. While the aviation sector possesses mature physical security systems for handling aviation terrorism, detection, search, and surveillance, there is a demand for improvement in aviation security policies and the establishment of response strategies, which should include addressing cyber security threats.

3.2 The Need for Establishing and Improving Aviation Security System

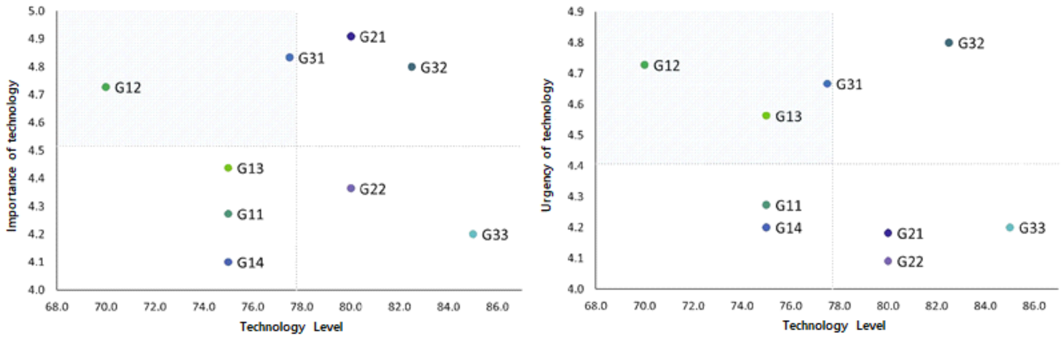
With the rapid development of ICT convergence technology, it is becoming integrated with the aviation industry. In order to ensure safe aviation, the aviation security management system must establish a comprehensive cybersecurity strategy, including measures to address cyber threats and responses.

In certain modern aircraft models, such as the A321, wired and wireless network services are provided through interface devices that offer computer communication capabilities, creating a reality where safety cannot be guaranteed against potential cyber threats. Both ground airports and onboard systems manage sensitive information critical for aviation operation and navigation. Therefore, it is essential to establish an aviation security management system that defines and addresses cyber intrusions, intentional or illegal data tampering, system disruption, unauthorized access, and service denial, among other cyber threats, as violations of regulations and related laws.

Given the paramount importance of aviation safety, air craft must adopt a proactive approach to cyber threats. This entails constant monitoring of potential threats and implementing a real-time management system capable of responding to cyber intrusions and threats, ensuring the safety of aviation operations.

3.3 The Urgency of Aviation Operation, Navigation Safety, and Security Technologies

When examining the report on the importance of domestic aviation technology and the urgency of technology acquisition, as shown in Fig. 1, the fields of aviation operation and safety (G32) and aviation traffic system and maintenance (G33) demonstrate high levels of (left) technological significance and (right) urgency for technology acquisition. However, as indicated in Table 3, there are shortages in basic research resources and manpower, and insufficient research in navigation safety facilities, aviation operation and safety, and aviation traffic systems[18].



G11:Fixed-wing aircraft design/manufacturing/certification, G12: Rotary-wing aircraft design/manufacturing/certification, G13: Unmanned aircraft design/manufacturing/certification, G14: Aircraft maintenance/modification/powerplants/components, G21: Airport facilities, G22: Navigational safety facilities, G31: Navigation (CNS, etc.), G32: Aviation operation/safety, G33: Aviation traffic systems and maintenance

※ Note-2021 Comprehensive Report on Analysis of Technology Levels in Transportation and Land Development.

Fig. 1. (Left) Technological Importance of Aviation Transportation (Right) Urgency to Secure Aviation Transportation Tech.

Table 3. Analysis of Transportation Tech Level in 2021

Middle Category	Subcategory	Infrastructure	Lack of R&D Investment	Insufficient Basic Research	Inadequate Business Support	Shortage of Human Resources	Need for Legal and Regulatory Improvement
Aircraft	Fixed-Wing Aircraft Design/Manufacturing/Certification		◎	○			
	Rotary-Wing Aircraft Design/Manufacturing/Certification	○	◎			○	
	Unmanned Aircraft Design/Manufacturing/Certification	·	◎	·	○		·
	Aircraft Maintenance/Conversion/Power/Components	○	◎		·		
Aviation Infrastructure	Airport Facilities		◎		◎		◎
	Navigation and Safety Facilities		○	·	◎	·	
Aviation Traffic Management	Navigation (CNS, etc.)		○	◎	○		
	Aviation Operations and Safety		◎	◎		○	
	Aviation Traffic Management Systems and Maintenance				○	◎	

※ Note-2021 Comprehensive Report on Analysis of Technology Levels in Transportation and Land Development.

To improve and enhance domestic technological capabilities, it is necessary to identify and invest in R&D projects for navigation systems, communication technologies, etc., which are currently reliant on foreign technologies. Developing international standard technologies to bridge the technological gap, prioritizing the establishment and support of aviation operation, navigation safety, and aviation security management systems, and revising and updating policies and relevant laws are deemed to be the most urgent tasks. The convergence of aviation technology based on excellent domestic information and communication technology is expected to have a significant impact.

Ⅳ. Improvement Measures for Aviation Sector Cybersecurity Policies and Management Systems

4.1 Improvement Measures for Aviation Sector Cybersecurity Policies and Management Systems

In the aviation industry, there is a close relationship between comprehensive information related to the operation and navigation of aircraft and aviation services. This paper emphasizes the need to establish a comprehensive information and data-based aviation security policy and management system to address potential cyber threats to onboard wireless and wired networks and internet services from unidentified passengers.

The information and data for the operation, control, navigation, operation, and maintenance of aircraft in section 2.3 are communicated through information and communication devices, linking various systems within the aircraft such as aircraft systems, airline information systems, and in-flight entertainment systems used for passenger services. Comprehensive information and data security management are required for aviation operation, navigation, and services. The aircraft system is considered an information and communication system that utilizes computer and computer technology for data collection, processing, storage, retrieval, transmission, and reception, similar to the definition in Article 2, Clause 2 of the Basic Telecommunications Act. Therefore, it is necessary to revise and establish aviation security management guidelines. Table 4 represents the current regulations and guidelines.

Table 4. List of Aviation Security Level Management Guidelines.

Regulations	Relevant laws
Domestic laws and regulations	· Aviation Security Act · Aviation Industry Act, Aviation Safety Act, Airport Facilities Act · Guidelines for the Management of National Security Facilities and Protection Equipment · National Aviation Security Plan · National Aviation Security Contingency Plan · Guidelines for Airport Construction, Maintenance, and Repair · Guidelines for Education and Training · Regulations on the Duties of Aviation Security Supervisors · Types, Performance, and Operational Standards of Aviation Security Equipment · Standard Operating Guidelines for Aircraft Security · Commercial Air Cargo Security Standards · Liquid, Aerosol, Gel Security Control Guidelines
ICAO annexes and related regulations	· ICAO Annex 17 · ICAO Publication - Emergency Measures for Protecting Civil Aviation against Acts of Unlawful Interference · ICAO Publication-Emergency Measures

However, comprehensive protection measures and response guidelines related to cyber threats are currently nonexistent. Therefore, in the current aviation security laws and guidelines, the scope of (restrictions on electronic devices) should be expanded to include a comprehensive information protection management system that can control the illegal use of information and communication devices, including portable information and communication devices, for data collection, processing, storage, retrieval, transmission, and reception.

For example, in-flight 'cyber attacks' refer to any illegal actions, including hacking, computer viruses, logic bombs, mail bombs, denial-of-service attacks, or any other electronic means, aimed at intruding, disrupting, paralyzing, or destroying information communication networks of aircraft, airport facilities, or systems, as well as any actions or provisions that involve the interception or tampering of information. It is clearly specified as illegal actions, and amendments to aviation security-related laws and guidelines are made accordingly.

4.2 Establishment of Cybersecurity and Threat Management System in the Aviation Sector

To manage and respond to cybersecurity threats in the aviation sector, it is essential to establish an aviation cyber security threat management system. Along with the enhancement of relevant laws and regulations in Section 4.1, the establishment of an integrated cooperative system among government agencies, airport facilities, air traffic management, and domestic and international airlines in the aviation sector is a prerequisite for effective management. With the provision of wireless networks and internet services on board, aviation has evolved to the point where previously isolated aircraft can no longer guarantee the safety of their onboard systems against cyber threats.

Therefore, the establishment and operation of aviation sector cybersecurity monitoring centers are required to ensure the security of comprehensive information for airport facilities and aircraft operations. The key tasks to be provided are as follows:

- *Establishment and Implementation of Cybersecurity Measures*: Formulation and enforcement of safety measures for aviation information and communication networks and comprehensive information protection, along with supervision and guidance.
- *Installation and Operation of Cybersecurity Monitoring Center*: Policy formulation, operation, collection, analysis, and dissemination of cyber threat related information, incident investigation, recovery support, and domestic and international cooperation on cyber threat-related information.
- *Incident Investigation and Handling*: Analysis and investigation of incidents arising from cyber attacks.
- *Workforce Development and Education & Promotion*: Acquiring and fostering skilled

personnel for the establishment of aviation sector cyber security infrastructure and enhancing security awareness, through professional workforce recruitment, training, education, and promotion.

· *Cyber Threat Response Training*: Regular cyber threat response training and establishment of a cooperative system among relevant agencies.

· *Aircraft airworthiness Cyber Attack Test*: Periodic vulnerability assessment and cyber attack testing on aircraft onboard systems and wireless network interface devices.

4.3 Management of Cyber Threats in Aircraft Cabins

Aircraft cabins are composed of control systems, airline information systems, and in-flight entertainment systems, among others, and operate wireless and wired network interfaces and communication systems.

To respond to cyber threats within the aircraft cabin, a continuous monitoring system is required for in-flight systems, wireless and wired network interfaces, and information communication networks, both during take-off and landing, and throughout the flight.

During the flight, detection and prevention systems, as well as monitoring systems, are necessary to prevent and block misuse, unauthorized access, and illegal activities of authenticated wireless network services and internet users. While it is challenging to detect acts that may cause system malfunctions or illegal activities in advance, proactive measures and accident prevention become feasible by detecting suspicious computer and device usage, software, etc., through cabin crew members. The most critical aspect of managing cyber threats in the aircraft cabin is the proactive response of cabin crew members in identifying and controlling illegal activities in advance. By utilizing the roles of cabin crew, private companies are evaluating 'preventive measures' as the most intuitive and practical alternative for security management.

Therefore, it is essential to enhance the security awareness of cabin crew members and provide them with education on how to respond to suspicious device usage and cyber illegal activities. This is an urgent task and the most proactive method for accident prevention. The key tasks for managing cyber threats in the aircraft cabin are as follows:

· *Continuous Monitoring System Operation*: Perform checks for malicious code and vulnerabilities before and after take-off and landing, and when connecting to airport communication systems. Conduct system log checks.

· *Cabin Crew Security and Response Training*: Provide education on identifying and responding to suspicious device usage and illegal activities.

· *Emergency Response System Operation*: Conduct ongoing threat level assessments and carry out cyber simulation exercises.

· *Incident Handling and Reporting*: Handle incidents during flight and conduct cause analysis investigations.

In-flight emergency response systems are essential and also of utmost importance. These emergency response systems must operate seamlessly within the aircraft, and proactive responses from cabin crew are required for accident prevention and threat management.

Ⅴ. Conclusions

Safety has always been a top priority in aircraft operation. However, safety and security have become interconnected with the advancement and convergence of Information and Communication Technology (ICT) in the aviation industry.

From a safety perspective, the focus is on mitigating the impact of aircraft system failures on flight safety through the design, operation, and maintenance of systems, ensuring safety, and reducing the risk of malfunctions.

From a security perspective, cyber threats pose another potential threat to the safety domain, which must protect the operation of an aircraft. Unauthorized and systemic interference or disruptions can compromise the cyber-airworthiness of aircraft systems, potentially leading to errors and malfunctions that undermine safety. To ensure the safe operation of aircrafts, physical security measures such as detection, screening, and surveillance have been implemented to address physical threats such as aviation terrorism and unlawful acts. However, with the convergence of aviation services and ICT, the provision of wireless and Internet services onboard introduces previously unseen and emerging threats that challenge aviation safety.

It is crucial to adopt a balanced and systematic approach to aviation security policies in response to rapidly evolving ICT and aviation services. The gap between advancing technology and outdated aviation security policies leaves us vulnerable to unpredictable aviation security threats that jeopardize the safety of aviation services.

Therefore, as outlined in this paper, it is imperative to revise and update aviation policies, laws, and regulations and establish an integrated cyber threat management system to proactively address potential aviation security threats and ensure safety.

References

[1] Aviation Security Act, 2022.

[2] Aviation Safety Act, 2023.

[3] Kang, "*Both flight attendants and pilots use tablets instead of paper*," (https://www.chosun.com/economy/industry-company/2023/04/05/C6IY2KEHHRDHVI3S3D6DTLJ7WA/I)

[4] Annex17, Aviation Security, ICAO.

[5] Lee, "*In the first half of 2023, what incidents of in-flight security occurred*," (https://www.boannews.com/media/view.asp?idx=119600&page=2&mkind=5&kind=1)

[6] Lee, "*Strengthening in-flight cybersecurity re sponse is necessary*," (https://www.boannews.com/media/view.asp?idx=119624&page=1&mkind=5&kind=2)

[7] Special Conditions: Boeing Model 777-200, -300, and -300ER Series Airplanes; Aircraft Electronic System Security Protection From Unauthorized External Access.

[8] Aviation Security Manual, Doc 8973, ICAO.

[9] AMC 20-170 Integrated modular avionics (IMA) ED Decision 2018/008/R Annex IV AMC 20-170.

[10] Air Traffic Control, *FAA Needs a More Comprehensive Approach to Address Cybersecurity As Agency Transitions to NextGen*, United States Government Accountability Office, Apr. 2015.

[11] Aeronautical Radio, Incorporated (ARINC), Aviation security, 2012. (http://www.arinc.com/products/security/aviation_security.html)

[12] Information and Communications Network Protection Act, 2022.

[13] Airport Facility Act, 2023.

[14] Guidelines for the Protection of Key Information and Communications Network Facilities, 2017.

[15] Information and Communications Network Protection Act, 2022.

[16] Act on Promotion of Information and Communications Network Utilization and Information Protection, 2023.

[17] Personal Information Protection Act, 2020.

[18] *Analysis of Technology Level in Land, Infrastructure, and Transport - Comprehensive Report*, Ministry of Land, Infrastructure and Transport, 2021.

Sanghoon Jeon

Apr. 2021~Current : Professor, Far East University, Department of Hacking & Security.

Dec. 2010~Current : ISO/IEC JTC1/SC27 WG4, Head of Delegate-Korea

Feb. 2019~Current : IUT-T SG17 (Security) Delegate

<Research Interests> Information Security, Aviation Security, Network Security, Entity Authentication

[ORCID:0000-0002-5365-3174]