KR Maritime Cyber Security

News from KOREAN REGISTER

Vol. 029

September 2020

KR Cyber security Activities

SC Shipmanagement Ltd. signed the contract for KR cyber security compliance certification.

SC Shipmanagement Ltd., Container Company in Paisley, UK, signed a contract for company/ship cyber security compliance certification with Korean Register (KR).

Under the contract, KR verifies its cyber security capabilities in terms of administrative, technical and physical aspects of cyber security management system in SC Shipmanagement's headquarter, and conducts the survey of cyber security compliance certification for 4 container ships.

In particular, as on-site survey by the surveyor is becoming more difficult due to COVID-19, survey for cyber security compliance certification of SC Shipmanagement will be conducted by remote cyber security survey from KR's headquarter.

Remote cyber security surveys is that enables survey by reviewing the data of the electronic file (photograph, video, copy of document, etc.) submitted by the company or the ship owner without the need for direct physical attendance of surveyor to a company or a ship and communicate with the company or the ship in real-time video, if necessary.

With non-face-to-face activities becoming important around the world due to COVID-19, these remote cyber security surveys are expected to enhance traditional on-site survey capabilities by utilizing state-of-the-art digital technologies for survey to improve efficiency.

In order to enhance safety and efficiency in maritime industry, KR plans to present a new option of smart and safe survey for the company and the ship by combining on-site survey and remote cyber security survey.

Carnival Corporation hit by ransomware

Cruise line operator Carnival Corporation has disclosed that one of their brands suffered a ransomware attack over the past month. Carnival Corporation disclosed that one of its brands suffered a ransomware attack "On August 15, 2020, Carnival Corporation and plc detected a ransomware attack that accessed and encrypted a portion of one brand's information technology systems. The unauthorized access also included the download of certain of our data files."

Steve Durbin, managing director of the Information Security Forum, says ransomware is one of the most prevalent threats to an organization's information and is increasingly lucrative for criminals. "To protect against the scale and scope of these threats, an organization will be forced to rethink its defensive model, particularly its business continuity and disaster recovery plans," adds Durbin. "Established plans that rely on employees being able to work from home do not stand up to an attack that removes connectivity or personally targets individuals as a means of dropping ransomware into the corporate infrastructure. Revised plans should cover threats to periods of operational downtime caused by attacks on infrastructure, devices or people."

According to Terence Jackson, Chief Information Security Officer at Thycotic, ransomware has evolved over the years from being something that required someone fairly skilled in writing code to a ransomware-as-a-service (RaaS) offering. Jackson notes, "However, the skills that it takes to launch a ransomware attack have lessened. Exploit kits can be easily purchased off of the web now just like other commercial off-the-shelf software. Phishing is, and will likely continue to be, the preferred method for ransomware. It only takes one employee to open the door. This makes the attackers job much easier and again lowers to technical bar of entry to perpetrate an attack. As long as humans remain the weakest link in the defenses, ransomware attacks will continue to intensify."

Shahrokh Shahidzadeh, CEO at Acceptto, notes that attacks appear to be more successful when leveraging a valid digital credential for planting ransomware and unfortunately, current binary approaches to authentication allow too many cybercriminals into networks, allowing them to effectively plant ransomware attacks. Shahidzadeh adds, "The use of valid digital credentials which have been purchased on the dark web, or stolen out right in a breach, provides the best access for planting ransomware when a targeted organization doesn't have a continuous, behavior-based authentication solution which would catch the inappropriate use of that credential. Ransomware attacks will continue to adapt and evolve, especially with the ease of access to stolen digital credentials and the current deployment of continuous authentication solutions. In short, if your organization doesn't continuously authenticate every digital credential, the likelihood of a ransomware attack being successful goes up exponentially."

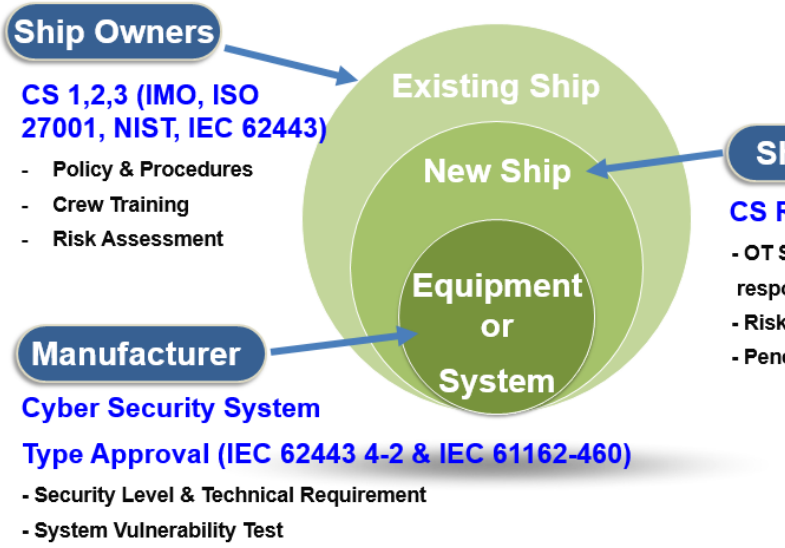
Source : SECURITY Magazine, 2020

Understanding of KR CS-Ready Notation

KR Cyber Security Certification System

KR Maritime Cyber Security Certification applies to the company or the ship with cyber security management system (CSMS). When the company/the ship pass the survey for certification(document review and on-site survey), KR issues cyber security compliance certificates to the company/the existing ship, and cyber security notation (CS-Ready) to the new ship. Cyber security compliance for the company/the existing ship is divided to 3 levels (CS1, CS2 and CS3) in accordance with cyber security maturity, and consists of 35 survey areas and 144 survey items.

- **CS1, CS2, CS3** : Requirements of CSMS for the existing ship **(Shipping company)**
- **CS Ready** : Requirements for establishing integrated cyber security system of new ship **(Shipbuilder)**
- **CS Type Approval** : Requirements of cyber security function of equipment system **(Equipment company)**


Ship Owners
CS 1,2,3 (IMO, ISO 27001, NIST, IEC 62443)
- Policy & Procedures
- Crew Training
- Risk Assessment
Existing Ship
New Ship
Equipment or System
Shipyard
CS Ready
- OT System incident response & recovery
- Risk Assessment
- Penetration Test
Manufacturer
Cyber Security System
Type Approval (IEC 62443 4-2 & IEC 61162-460)
- Security Level & Technical Requirement
- System Vulnerability Test

Need of Cyber Security Notation (CS Ready) for New Ship

As the marine business environment changes, Advanced automation and integrated control system is equipped in ships, and remote access, control and maintenance of the system in ships became possible from the land, which resulted increase of ship cyber risks. Therefore it is very important for maritime safety that construction and verification of an integrated system preventing and responding cyber incidents from the stage of ship building. KR gives 'CS Ready' notation to the new ship with cyber security system. In this newsletter, the requirements will be introduced.

[CS Ready] Understanding of documents : #1 List of Assets

Ship consists of various IT/OT systems. Identification and categorization of each system's cyber assets by list of assets can be seen as the first step in identify cyber attack vectors and efficiently responding to cyber incidents such as damage, falsification and leakage.

- **Asset** : physical or logical object owned by or under the custodial duties of an organization, having either a perceived or actual value to the organization [IEC 62443]
- **Information Technology(IT)** : any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information e.g. router, switch, firewall, server, printer, desktop, laptop, etc.
- **Operation Technology(OT)** : devices, sensors, software and associated networking that monitor and control onboard systems. e.g. ICS, SCADA, DCS, PLC, Data historian, Sensor, Actuator, etc.

Zone	Asset	Manufacturer	Software	OS	Port	Location	PIC
Enterprise System	Mail Server	HP	PMS	Windows Server 2016	USB : 3 LAN : 2	Accomm.	2nd officer
	PCs	HP	PMS	Window 10	USB : 3 LAN : 2	Accomm.	2nd officer
	Printers	HP	-	-	USB : 2 LAN : 2	Accomm.	2nd officer
	Router	CISCO	CISCO	-	USB : 1 LAN : 20	Accomm.	2nd officer
DMZ	Firewall	CISCO	CISCO	-	USB : 1 LAN : 20	W/H	2nd officer
	Event Log	Advantech	-	Windows Server 2016	USB : 4 LAN : 2	W/H	2nd officer
	Anti-virus	HP	-	Windows Server 2016	USB : 4 LAN : 2	W/H	2nd officer
Control System	No.1 O/S	HP	KC 600	Windows Embedded	USB : 5 LAN : 3	ECR	1st engineer
	No.2 O/S	HP	KC 600	Windows Embedded	USB : 5 LAN : 3	ECR	1st engineer
	OS Switch	Moxa	Phoenex	-	-	ECR	1st engineer
	Firewall	Fortinet	Forti	-	USB : 1 LAN : 20	ECR	1st engineer
Wireless	A.P.	CISCO	CISCO		USB : 1 LAN : 4	W/H	2nd officer
Remote System	Vsat Rack	Intellian	-	-	USB : 3 LAN : 10	W/H	2nd officer
	Router	CISCO	CISCO	-	USB : 1 LAN : 20	W/H	2nd officer
	Firewall	CISCO	CISCO	-	USB : 1 LAN : 20	W/H	2nd officer
Navigation and Communication System	No.1/2 ECDIS	JRC	-	Windows Embedded	USB : 3 LAN : 4	W/H	2nd officer
	No.1/2 Radar	JRC	-	Windows Embedded	USB : 3 LAN : 4	W/H	2nd officer
	Firewall	Fortinet	Forti	-	USB : 1 LAN : 20	W/H	2nd officer

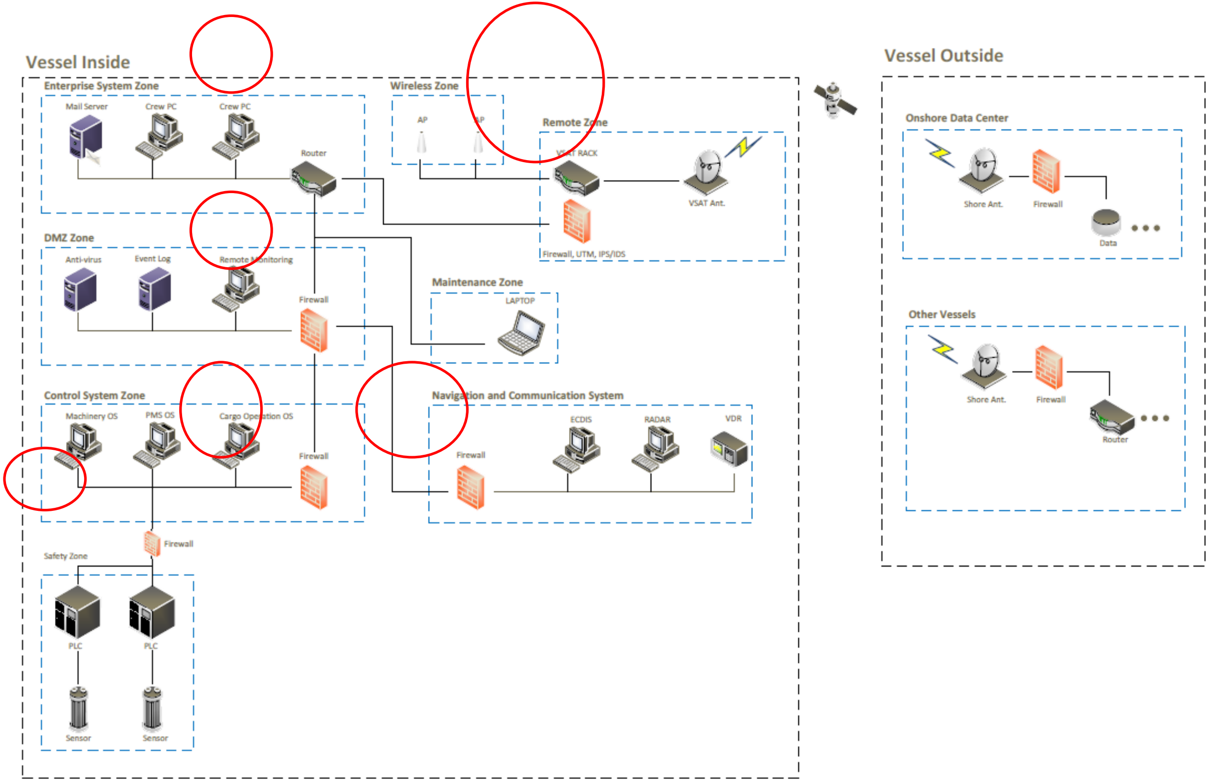
[CS Ready] Understanding of documents : #2 Network configuration of the ship

The network configuration of the ship allows us to identify zones, communication routes, perimeter protection devices (gateway, router, firewall, VPN, etc.) of cyber assets and data flows (one-way, two-way). The configuration diagram (example) of the ship's network referring to this is as follows:

- **Zone** : grouping of units that represent the partition of a system based on functional, logical, and physical (including location) relationships. See IEC 62443 3-2 Standard for criteria for separating zones.
- **Conduit** : Logical grouping of communication channels connecting two or more zones that share common security requirements. E.g. switch, router, firewalls, UTM, IPS/IDS, etc.

No.	Requirements	Description
ZCR 3.2	Separation of business systems and control system assets	Control system is separated from business system.
ZCR 3.3	Separation of SIS asset	Safety system is separated from non-safety system.
ZCR 3.4	Separation of temporary connection equipment	Temporary connection equipment(laptop, USB, etc.) is separated from control system.
ZCR 3.5	Separation of radio communication equipment	Wireless communication is separated into areas separated from wired communication.
ZCR 3.6	Separation of external network connection equipment	emote access is physically separated.

[IEC 62443 3-2 Requirement of division of zones and communication routes]



[Example of ship network configuration]

Guideline for Type Approval of Maritime Cyber Security

Understanding Guideline for Type Approval of Maritime Cyber Security

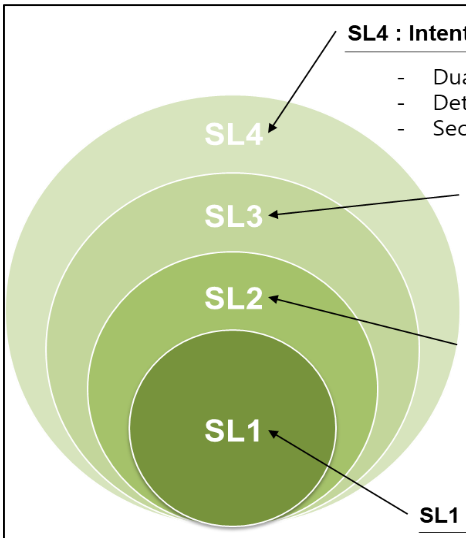
Type approval is to certify for the manufacturers of equipment for marine use that equipment comply with the provisions for the type approved products in the Guidance, where deemed satisfactory by the Society as the results of carrying out the examination, tests and inspection specified in the Guidance before installation on board. The cyber security type approval has been developed based on international standards such as ISA 62443 4-2, IEC 61162-460, and inspect cyber security level and function of cyber systems including remote access equipment, integrated control and monitoring systems on board the ship. The security requirements and their levels are verified on 12 categories and 124 requirements.

< Composition of KR Cyber Security Type Approval Guidelines >

Section 1 General	Section 5 Data Confidentiality	Section 9 Software Application Requirements
Sections 2 Identification and Authentication	Section 6 Restricted Data Flow	Section 10 Embedded Device Requirements
Section 3 Use Control	Section 7 Timely Response to Events	Section 11 Host Device Requirements
Section 4 System Integrity	Section 8 Resource Availability	Section 12 Network Device Requirements

Source : http://www.krs.co.kr/KRRules/KRRules2019/data/data_other/ENGLISH/gc31e000.pdf

Understanding Security Level (SL)



SL4 : Intentional violation, sophisticated means with extended resources

- Dual Approval
- Detect unauthorized alteration
- Security functionality and operation verification

SL3 : Intentional violation, sophisticated means with moderate resources

- Security mechanism based on hardware
- Concurrent session control

SL2 : Intentional violation, simple means with low resources

- Protect against unauthorized use of test interface
- Protect from installation and execution of unauthorized software
- Device, communication data identification and authentication

SL1 : Casual or coincidental violation

- Authorization
- Backup and restore
- Human user authentication

Source : IEC 62443

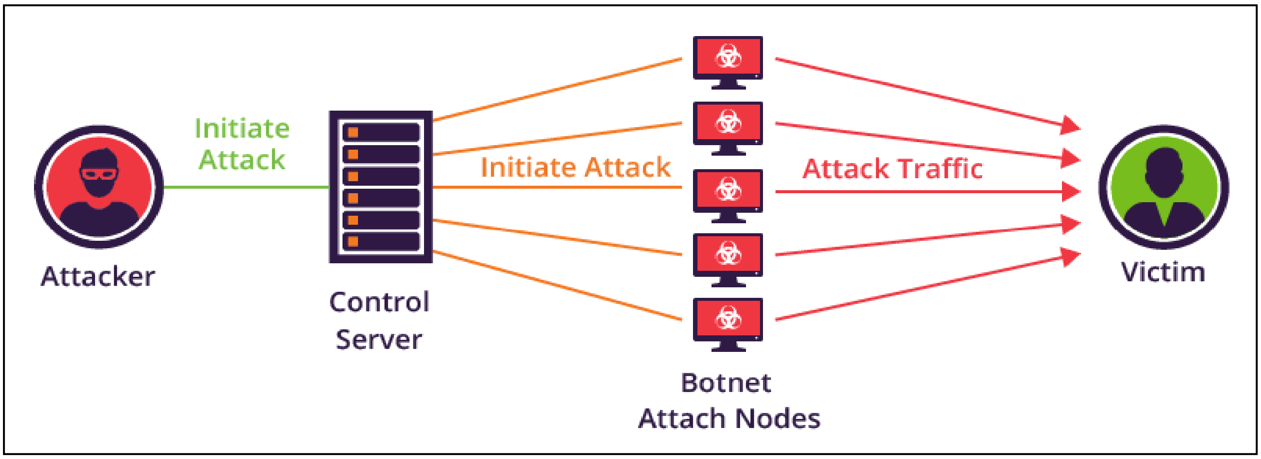
KR Type Approval of Maritime Cybersecurity Inspection Items

Resource Availability - Denial of service(DoS) protection (801)

1. Components should provide the capability to maintain essential functions when operating in a degraded mode as the result of a DoS event. (SL 1)
2. Components should provide the capability to mitigate the effects of information and/or message flooding types of DoS events. (SL 2,3,4)

Denial of service protection

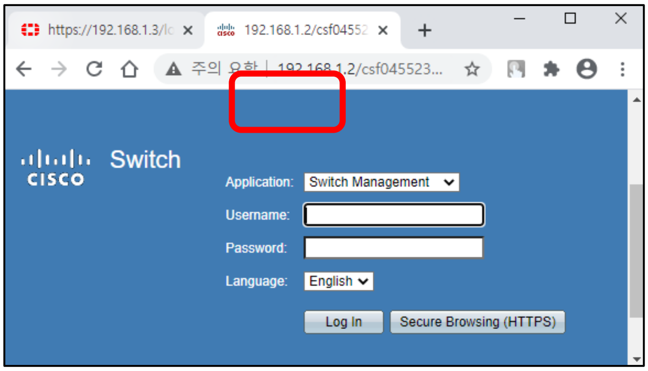
DoS, the abbreviation for Denial of Service, refers to an attack that maliciously attacks the system, resulting in a lack of resources in the system, thus preventing it from being used for its intended purpose. An example of this is that a large amount of traffic is generated on the server of a specific website, causing an overload condition, which makes it impossible to provide smooth service to customers. Security measures came out, and hackers created a more advanced Dos attack. The DDoS attack, called Distributed Denial of Service, uses an advanced attack technique from the existing web server. It uses a more advanced method than the method of directly attacking the existing web server. It's a way to use a zombie PC, but the principle is simpler than you think. First, it distributes a specific malicious code program and infects random PCs in large quantities. Infected zombie PCs do not perform any actions until a hacker's command is given, so owners of infected zombie PCs may not be aware of the infection. The hacker checks that a certain level or higher PC is infected, and the hacker orders zombie PCs to attack targets at once through the Control Server. Compared to the existing DoS attacks that could be solved simply by blocking specific IPs, DDoS attacks are random and come from a large number of locations, and even the target of attack is the victim, not the hacker.



<Examples of distributed denial of service attack>

Denial of service protection

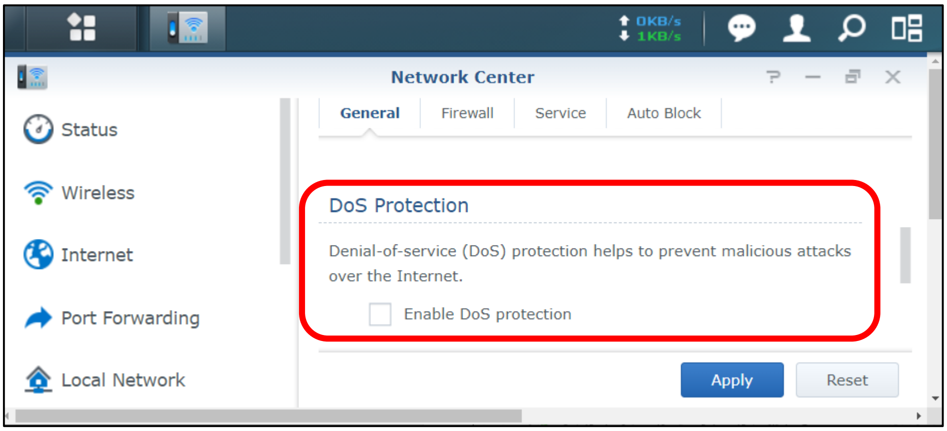
If the service is delayed or becomes impossible as a result of the DoS attack, this causes a problem in availability. Therefore, the cyber security type approval is required to provide a protection function for this. DoS and DDoS attacks have been in progress for a long time, and fortunately, various network devices, such as firewalls and routers, often provide protection for them as basic functions. The picture below is an example of the DoS protection function provided by the router.



Application: Switch Management
Username:
Password:
Language: English

<Example of network device setting page>

First, in order to use the setting generally provided by a network device, enter the address of the device in a web browser such as Internet Explorer or Chrome. The relevant address is often described in the device provider's manual, etc. If there is no special setting, the 192.168.0.1 address is often used. After logging in by entering your ID and password at the corresponding address, you can set up security.



DoS Protection

Denial-of-service (DoS) protection helps to prevent malicious attacks over the Internet.

□ Enable DoS protection

<Example of DoS prevention function>

Many commercial network devices provide the DoS protection function as a basic function, and the default setting is often disabled. Therefore, you can satisfy the requirement by activating it in the setting menu.

Explanation of Term

Remote cyber security survey

survey by reviewing the data of the electronic file (photograph, video, copy of document, etc.) submitted by the Owner of the company or the ships without the need for direct physical attendance of surveyor to a company or a ship and communicate with the company or the ship, if necessary.

Source : KR Guidance for Maritime Cyber Security System 2020

Ransomware

Malicious software that infects your computer and prompts you to pay for the system to work again.

Source : Kaspersky

DoS Attack

A malicious attack that overwhelms the target or surrounding infrastructure with a flood of Internet traffic, disrupting normal traffic on target servers, services, and networks.

Source : CLOUDFLARE

Intrusion Detection System (IDS)

Systems that monitor and alert network traffic when suspicious activity is found

Source : GeeksforGeeks

Intrusion Protection System (IPS)

A network security application that monitors network or system activity. The primary function of the intrusion prevention system is to identify malicious activity, collect information about it, report it, and block or stop it.

Source : GeeksforGeeks

Introduction of Maritime Cyber Security Training

KR Cyber Security Training

According to IMO Resolution MSC.428(98) Maritime Cyber Risk Management in Safety Management Systems, administrations such as Marshall Islands ask the ship owner and ship managers to appropriately addressed in safety management systems no later than the first annual verification of the company's Document of Compliance after 1 January 2021. Therefore, the demand for maritime cyber security training that can help to understand maritime cyber security and establish proper cyber security management system has increased.

KR is providing cyber security training to domestic and overseas shipping companies, shipbuilders, equipment companies, service providers from 2015. In particular, in March, KR received approval from Singapore MPA for the training course named as the understanding of maritime cyber security and provided cyber security training to shipping companies in Singapore through the Maritime Cluster Fund (MCF).

KR provides maritime cyber security e-learning course in cooperation with Orange Security, a cyber security consulting company, for clients who have difficulty in collective training due to COVID-19. Maritime cyber security e-learning course consist of 'Understanding of Maritime cyber Security' and 'Practice of Maritime Cyber Security.' While the former was developed for cyber security awareness of all employees and includes overview of maritime cyber security, examples of maritime cyber incident, etc., the latter is for hands-on staff and consists of implementation of cyber risk management, etc. Currently, the clients in Korea can apply this course through the maritime cyber security e-learning system of Orange Security (http://edu.orangecq.com), the e-learning program for overseas clients is being prepared. The samples of these courses can be founded on YouTube: 'Understanding Maritime Cybersecurity (https://youtu.be/fSIDLMj4gho)' and 'Management Office of Maritime Cybersecurity (https://youtu.be/67t0ckrNtiA)'