Transactions of the Korean Nuclear Society Spring Meeting
Jeju, Korea, May 19-20, 2022

Suggestion of a Cyber Security Incident Report Framework for Nuclear Facilities in ROK based on Foreign Cases

In-hyo Lee[*]
Korea Institute of Nuclear Nonproliferation and Control, 1418 Yuseong-daero, Daejeon, Republic of Korea 34101
[*]*Corresponding author: lih9103@kinac.re.kr*

1. Introduction

It is necessary to develop a cyber security incident report system to respond to cyber threat or cyber-attack in a timely manner. To establish this system, it is necessary to improve related law and have standard cyber threat information sharing system. This paper analyzed the cyber security incident report system of EU/US and cyber threat information sharing cases of US. Based on this analysis, the cyber security incident report framework for nuclear facilities in ROK was suggested which contains the improvement of related domestic law and cyber threat information sharing system establishment.

2. Cyber Security Incident Report System of EU and US

2.1 Cyber Security Incident Report System of EU

EU has been establishing information sharing system to deal with cyber security incidents occurred in various nations. European Network and Information Security Agency (ENISA) receive report from related organization when cyber security incident occurs. There are several security articles about that such as Framework Directive, e-Privacy Directive, Data Protection Regulation, e-Sig and e-ID Regulation. The relationship among the security articles is followed in Fig.1.

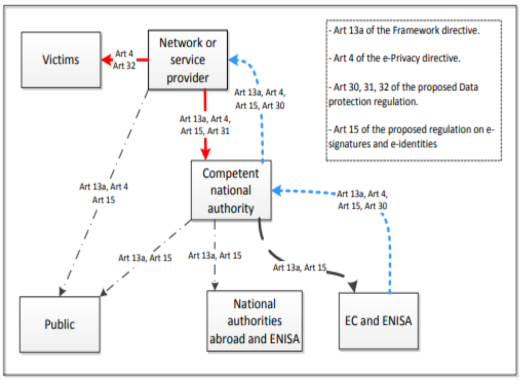
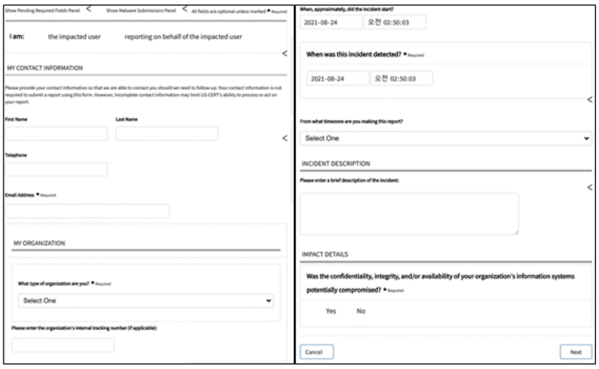

Victims
Art 4
Art 32
Network or service provider
Art 13a, Art 4, Art 15, Art 30
Art 13a, Art 4, Art 15, Art 31
Competent national authority
Art 13a, Art 4, Art 15, Art 30
Art 13a, Art 4
Art 15
Art 13a, Art 15
Art 13a, Art 15
Art 13a, Art 15
Public
National authorities abroad and ENISA
EC and ENISA
- Art 13a of the Framework directive.
- Art 4 of the e-Privacy directive.
- Art 30, 31, 32 of the proposed Data protection regulation.
- Art 15 of the proposed regulation on e-signatures and e-identities

Fig. 1. Similarities and differences among the security articles [1]

2.2 US ICS Cyber Security Incident Report System

Cybersecurity and Industrial Security Agency (CISA) under the Department of Homeland Security (DHS) was established in 2018 by integrating US-Computer Emergency Readiness Team (US-CERT) and Industrial Control Systems-Cyber Emergency Response Team (ICS-CERT). The legal base of CISA is CISA Act of 2018 (CISA ACT) which was revised from Homeland Security Act of 2002. CISA provides cyber incident reporting system via its website. It also provides guidance of cyber incident report which contains requirement and process.


Show Pending Required Fields Panel
Show Malware Submissions Panel
All fields are optional unless marked * Required

I am: the impacted user reporting on behalf of the impacted user

MY CONTACT INFORMATION

Please provide your contact information so that we are able to contact you should we need to follow-up. Your contact information is not required to submit a report using this form. However, incomplete contact information may limit US-CERT's ability to process or act on your report.

First Name
Last Name
Telephone
Email Address * Required

MY ORGANIZATION

What type of organization are you? * Required
Select One

Please enter the organization's internal tracking number (if applicable):

When, approximately, did the incident start?
2021-08-24 오전 02:50:03

When was this incident detected? * Required
2021-08-24 오전 02:50:03

From what timezone are you making this report?
Select One

INCIDENT DESCRIPTION

Please enter a brief description of the incident:

IMPACT DETAILS

Was the confidentiality, integrity, and/or availability of your organization's information systems potentially compromised? * Required
Yes No

Fig. 2. CISA incident reporting system [2]

3. Analysis of US Cyber Threat Information Sharing Cases

It is important to share threat information always for ensuring speediness and correctness of the reported contents.

US operates Information Sharing Analysis Center (ISAC) in several industrial areas such as IT, chemical, communication, energy, financial service, and so on.

Because of the variety of information and sources, it is necessary to formulate standard information sharing system and analysis method. DHS started to develop a standard in 2012 and published Trusted Automated eXchange of Indicator Information (TAXII) 1.0 which is a threat information transmission standard in April, 2013 and The Structured Threat Information eXpression (STIX) 1.0.1 which is a threat information expression standard in October, 2013, respectively.

TAXII provides 4 services such as information alert, information subscription management, contents reception and contents request. Also, it supports the HTTP and HTTPs protocols. STIX contains 8 elements to analyze threat information consistently and automatically. The 8 elements are cyber-attack activities, attackers, attack methods, detection indicators, observation indicators, incident, measures and targets. If a specific organization detects cyber threat, the cyber threat information transformed to STIX and it is transmitted to participated organization automatically by TAXII.

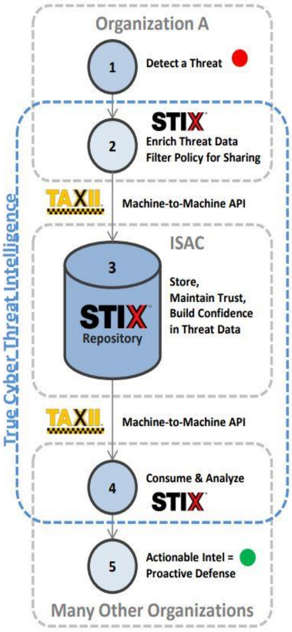


Fig. 3. Structure of STIX/TAXII system [2]

4. Proposal of Establishing a Cyber Security Incident Report Framework for Nuclear Facilities in ROK

4.1 Improvement Method of Cyber Security Incident Report Law

As discussed in chapter 2, EU and US have unified reporting system for cyber security incident. However, in case of ROK, nuclear facilities are subjected to "Enforcement Decree of the Act on Physical Protection and Radiological" and "Act on the Protection of Information and Communications Infrastructure" and they report related administerial agencies by relevant laws. If a nuclear facility is designated to national infrastructure, it is subjected to "Act on the Protection of Information and Communications Infrastructure" and report to NIS or ICT. Then, technical support can be provided by National Intelligence Service (NIS) or Ministry of Science and ICT (MSIT). However, if a nuclear facility isn't designated to national infrastructure, it will report to Nuclear Safety and Security Commission (NSSC) but appropriate technical support may not be assured. The reason why is cooperation of NSSC and administrative agency (NIS, MSIT) may not be assured because there is any link between "Enforcement Decree of the Act on Physical Protection and Radiological" and "Act on the Protection of Information and Communications Infrastructure".

In case of US, cooperation of US NRC, DHS, federal law enforcement agencies and intelligence community is defined in 10 CFR 73.77 [3] and R.G. 5.83 [4]. So, it is necessary to fill the legal hiatus of "Enforcement Decree of the Act on Physical Protection and Radiological" and "Act on the Protection of Information and Communications Infrastructure" by establishing NSSC bulletin and revising KINAC regulation standard (KINAC/RS-015) [5].

4.2 Proposal for Cyber Threat Information Sharing System of Nuclear Facilities

US developed STIX/TAXII for sharing cyber threat information as discussed in chapter 3. In case of ROK, Cyber-Threat EXpression (C-TEX) was developed by Korea Internet and Security Agency (KISA) referring to STIX [6]. However, C-TEX is not used widely over the various fields in comparison with STIX.

Administrative agency provides cyber threat information to national infrastructure based on "Act on the Protection of Information and Communications Infrastructure". In case of nuclear facilities which are not designated to national infrastructure, cyber threat information is provided by relevant organizations based on the KINAC/RS-015 requirements. Because the threat information sources are scattered, it may difficult to deal it effectively. To solve this problem, it is important to establish unified cyber threat information sharing system which utilize standard threat information expression like C-TEX.

5. Conclusions

In order to respond cyber threat or cyber-attack in timely manner, cyber incident should be reported precisely. To work it, systemic reporting method and standard cyber threat information sharing system should be prepared parallelly. In conclusion, by achieving completeness of law, systemic cyber security incident report will be possible. By using the standard cyber threat information expression and establishing information sharing system, furthermore, framework of cyber security incident report could be accomplished.

REFERENCES

[1] ENISA, Cyber Incident Reporting in the EU, 2012.
[2] CISA, US-CERT Federal Incident Notification Guidelines, 2017.
[3] US NRC, Cyber Security Event Notifications (10 CFR 73.77), 2015.
[4] US NRC, Cyber Security Event Notifications (Regulatory Guide 5.83), 2015.
[5] KINAC, Security for Computer and Information System of Nuclear Facilities (KINAC/RS-015), 2016.
[6] NIS et al, 2021 National Cybersecurity White Paper, 2021.