International Trend for the Insider Threat Mitigation at Nuclear Facilities and its Domestic Countermeasures

Jong-Uk Lee, Chan Kim, In Seon Back, Seung Sik Yu, Heejun Chung
Korea Institute of Nuclear Nonproliferation & Control(KINAC)
1418, Yuseong-daero, Yuseong, Daejeon, 34054, Republic of Korea
julee@kinac.re.kr

1. Introduction

Nowadays insider threats at nuclear facilities have been alarmingly increasing worldwide because the threat would cause tremendous damages to them in unpredictable ways associated with sophisticated technical systems. Therefore, international communities including the International Atomic Energy Agency (IAEA) have paid close attention to malicious threats and made an effort to effectively protect against them.

As a part of coping with the threats at domestic nuclear facilities, this paper reviews the international investigation of the insider threat mitigation(ITM) including the results of the 2019 ITM symposium. In so doing, we suggest effective domestic counter-measures for this issue in the near future.

2. Current Status of International and Domestic Measures

In this section, international measures including the IAEA, the United States and Japan are described in terms of the ITM. In addition, domestic preventive status for the ITM is reviewed in detail.

2.1 Status of International Atomic Energy Agency

IAEA updated Nuclear Security Series No.8, Preventive and Protective Measures against Insider Threats, to Nuclear Security Series No. 8-G(Rev.1) in 2020, to better align and add further detail on certain topics based on the experience of the IAEA and Member States in using the IAEA Series No. 8 published in 2008. Its major revision includes identification of insider threats, implementing measures against them, and the additional evaluation of measures against collusion between insiders, against protracted theft and against sabotage, and etc. This guidance recommends that insider access to a facility should include a physical access to locations and material, internal or authorized remote computer or networks, and access to sensitive information about the facility, pursuant to the definition of insiders[1,2].

Therefore, the implementing measures against potential insider threats should mitigate or minimize the malicious acts by limiting access, authority and knowledge of them, and consider the steps for using preventive and protective measures against them as shown in Fig.1[2,3,4].

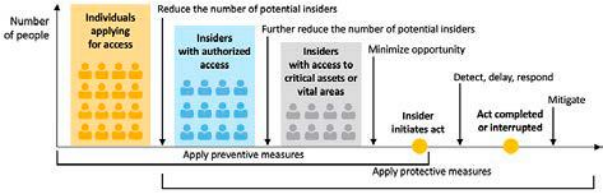

Fig.1. Steps for using preventive and protective measures against potential insider threats.

In addition to this guidance, the IAEA has published INFCIRC 908, titled 'Joint Statement on Mitigating Insider Threat' in 2017, pursuant to the request of the Permanent Mission of the United States of America. Its goal is to make the Member States establish and implement national-level measures to mitigate the insider threat[5].

2.2 Status of the United States

Nuclear Regulatory Commission(NRC) program for the ITM is so similar to the implementing method for international guideline of INFCIRC/225/rev.5[6,7]. Its implementing method consists of five components and they complement each other as shown in Fig.2[8,9]. In particular, access authorization and fitness for duty program are applied as a discrete program to mitigate the insiders even if physical protection program includes them. In addition, NRC has been inspecting and overseeing all the nuclear facilities by NRC inspectors and then feeding each of them back to verify the ITM in terms of 'Defense-in-depth'.

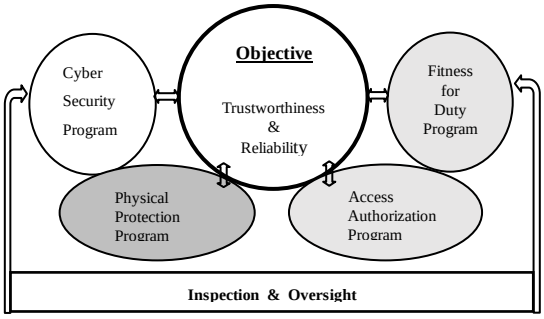

Fig.2. Integration of NRC Required Insider Mitigation Components.

2.3 Status of Japan

Nuclear Material Control Center(NMCC) had carried out the special investigation for the ITM from 1996 to 2000 to establish the first 'Design Basis Threat (DBT)' in Japan. It includes international measures, domestic status and effective countermeasures against the insiders at that time. In 2019, Japan Atomic Energy Agency(JAEA) had hold the international training course on the ITM under the auspice of the IAEA, to reestablish the substantial measures in near future. After that, JAEA has developed domestic training programs on the ITM and has been annually running five types of courses for nuclear operators in Japan[10].

2.4 Domestic Status

Korea government established the first DBT in 2009 pursuant to 'Physical Protection Law' entered into force in 2004. The current fourth DBT revised in 2018, however, would need to reflect the identification of insider threats, which is one of the major concerns for DBT. It means not only that it is undefined in the legal system but also that the categories of insiders and identification of potential insider threats are not regulated distinctly in the DBT.

As mentioned above, international community has emphasized the importance of insider threat detection so that the Member States may take the effective measures against insider threats of nuclear facilities. Therefore, in the context of substantially implementing the ITM, the domestic legal and institutional countermeasures should be reviewed in detail and reestablish to protect defense in depth against the fatal threat of nuclear facilities.

3. Considerations on Results of the 2019 ITM Symposium

The symposium was held in Belgium in March 2019, hosted by the United States department of Energy National Nuclear Security Administration and the Belgium Federal Agency for Nuclear Control. The objective of the symposium was to discuss the substantial countermeasures for the ITM as well as to encourage the Member States to implement INFCIRC 908, with the participation of their experts.

The main agenda of the symposium consisted of five issues on nuclear security culture, cyber security, trustworthiness programs, and technical measures for the ITM and national policy and regulatory frameworks. Discussions at the symposium yielded following results : to reestablish legal system for the ITM as a part of national-level measure, to strengthen nuclear security culture, and to establish and continuously implement overall preventive and protective measures through strengthening link with cyber security, and etc.[10]. These results had been submitted to the 2020 International Conference on Nuclear Security(ICONS) in this February and during the ICONS, the IAEA including the Member States again emphasized to make the unsigned countries effectively implement the ITM as well as to make them sign INFCIRC 908.

4. Conclusions and Future Countermeasures

The domestic countermeasures for the ITM in the near future are summarized as follows.

In terms of legal system, it is necessary for competent authority to revise the DBT as well as to carry out threat assessment based on the realistic investigation for the insiders including their attributes, categories and identification of potential insiders, etc. in near future.

In institutional aspects of nuclear security implementation, nuclear operator should develop a threat scenario and a response scenario respectively, based on the current characteristics of insiders at each nuclear facility as soon as possible. In addition, the hands-on training exercise at each facility is recommended pursuant to the scenarios.

From the technical point of view, the measures for the ITM should be discussed in close relation with cyber security issue. A naturalized technical guideline and standards should be also made through an in-depth review on this issue. In addition, the technical measures should be continuously supplemented by revision through the close cooperation with related organizations.

REFERENCES

[1] IAEA Nuclear Security Series No. 8, Implementing Guide, Preventive and Protective Measures against Insider Threats, 2008.
[2] IAEA Nuclear Security Series No. 8-G(Rev.1), Implementing Guide, Preventive and Protective Measures against Insider Threats, 2020.
[3] INFCIRC/225/Rev.5, Implementing Guide, "The Physical Protection of Nuclear Material and Nuclear Facilities, 2018.
[4] Matthew Bunn, Harvard University & Scott Sagan, Stanford University, 'Insider Threat', Jan. 2017.
[5] INFCIRC/908, Communication dated 22 December 2016 received from the Permanent Mission of the United States of America concerning a Joint Statement on Mitigating Insider Threats, Jan. 2017.
[6] 10 CFR section 73.55, "Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors against Radiological Sabotage". US-NRC, Mar. 2010.
[7] Regulatory Guide 5.77, Insider Mitigation Program, US-NRC, Mar. 2009.
[8] SECY-17-0095, Review and Approval of Proposed Revision to Regulatory Guide 5.77, "Insider Mitigation Program", US-NRC, Sep. 2017.
[9] Regulatory Guide 5.84, Fitness-for-Duty Programs at New Reactor Construction Sites, US-NRC, Jul. 2015.
[10] Jong-Uk Lee, KINAC/OT-007/2019, Oversea Report on 2019 International Symposium on Insider Threat Mitigation, Mar. 2019.