Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.29, NO.5, Oct. 2019 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2019.29.5.1077

원전디지털자산 사이버보안 규제 요건 개발을 위한 보안조치 적용 방안에 대한 분석*

김 인 경,† 변 예 은, 권 국 희‡
한국원자력통제기술원

Analysis of the Application Method of Cyber Security Control to Develop Regulatory Requirement for Digital Assets in NPP*

In-kyung Kim,† Ye-eun Byun, Kook-heui Kwon‡
Korea Institute of Nuclear nonproliferation And Control

요 약

원자력 발전소의 사이버위협이 현실화되면서 국제사회 및 국내에서는 사이버보안 규제지침 마련을 통해 필수디지털자산에 대한 적절한 보안조치를 적용하도록 요구하고 있다. 그러나 각 필수디지털자산에 대해 일괄적으로 동일한 사이버 보안조치 적용에 대해 규제 대상 내에서도 원전의 비상정지를 일으키고, 노심 손상을 유발할 수 있는 사고와 직접적으로 관련된 디지털자산에 단계적 접근방식을 적용한 규제 효과성 제고가 필요하다. 이에 본 연구에서는 원전 사고와 직접 관련된 디지털자산에 대하여 단계적 접근방식의 규제요건 개발을 위한 보안조치 적용 방안을 제시하였다. 단계적 접근방식의 기본적 고려사항인 규제 대상 설비의 침해영향도(Consequence)를 기반으로 한 규제 요건 적용을 위해 기존의 필수디지털자산에 요구되고 있는 보안조치를 보다 강화하거나 추가적인 보안조치를 개발하여 원전 사고와 직접 관련된 디지털자산에 요구하는 방식과 기존의 보안조치를 재분석하여 원전 사고와 직접 관련되지 않는 필수디지털자산에 대해서는 최소한의 보안조치를 요구하는 방식으로 크게 나누고 각 방안 별 세부적 사항을 기술하였다.

ABSTRACT

As the cyber threats of nuclear power plants become more necessary to systematically prepare against the cyber attack, the international community and the domestic government are urged to apply proper security controls for Critical Digital Assets (CDA) through cyber security regulatory guidelines. In this study, we suggests the application of security controls to develop the regulatory requirements of the graded approach through the analysis of domestic and foreign cyber security regulation guidelines and best practices for digital assets directly related to nuclear accidents. In order to apply the regulatory requirements based on the consequence(impact of infringement) of the regulated facility, which is a basic consideration of the graded approach, we will classify two methods and describe details of each method. By reanalyzing existing security controls, it is introduced that the method of demanding digital assets directly related to accident to enhance security controls required for existing CDA or develop additional security controls and requiring minimum security controls for CDA that are not directly related to accident.

Keywords: Nuclear digital assets, cyber security, Regulation

Received(04. 23. 2019), Modified(08. 31. 2019), Accepted(09. 01. 2019)

* 본 연구는 원자력안전위원회의 재원으로 한국원자력안전재단의 지원을 받아 수행한 원자력안전연구사업의 연구결과입니다. (No. 1605007).

† 주저자, ikkim0106@gmail.com

‡ 교신저자, vivacita@kinac.re.kr(Corresponding author)

I. 서 론

2014년 한국수력원자력의 상업용 네트워크 침투를 통한 데이터 유출, 2010년 이란 원자력시설에 악성코드 스턱스넷(Stuxnet) 감염을 통한 원심분리기 1,000여개 파괴, 2016년 독일 그룬트레밍엔 원전 내 일부 시스템이 외부로부터의 악성코드에 감염과 같이 원자력시설에 대한 사이버보안 중요성이 높아짐에 따라 사이버공격에 대한 더욱 체계적인 대비가 필요한 실정이다.

이에 IAEA 등 국제사회는 물리적방호체제 내에서 사이버보안 강화를 위해 원자력시설 사이버보안 기술지침(NSS No. 17) 및 계측제어시스템 사이버보안 기술지침(NST No. 33-T) 등의 발행을 통해 사이버공격에 의한 원전 사고 예방을 촉구하고, 안전-안보 연계를 고려한 보안체계의 수립을 권고하고 있다. 또한, 세계 각국에서는 원전에 대한 사이버보안 체계를 강화하고자 법령과 규제지침을 제정하였다. 미국의 경우, 원자력규제위원회(NRC)에서 사이버보안 연방법령(10 CFR 73.54)과 사이버보안 규제지침(RG 5.71)을 제정하여 공표한 바 있으며, 해당 법령과 규제지침에서 제시하는 사이버보안 규제요건을 사업자들이 준수하도록 요구하고 있는 상황이다.

국내에서도 원자력시설 등의 방호 및 방사능 방재 대책법(이하, 방사능방재법) 및 관련 원자력안전위원회 고시와 한국원자력통제기술원(KINAC)의 “원자력시설 등의 컴퓨터 및 정보시스템 보안 기술기준”(KINAC/RS-015)에 따라, 각 시설에서 정보시스템 보안규정을 마련하고 원자력시설의 안전(Safety-related 및 Important-to-Safety), 보안(Security), 비상대응(Emergency Preparedness) 기능을 수행하거나 침해 시 해당 기능에 악영향을 줄 수 있는 디지털기기를 필수디지털자산으로 식별하도록 요구하고 있으며, 각 필수디지털자산에 대해 적절한 보안조치를 적용하도록 규제하고 있으나 필수디지털자산에 대해 일괄적으로 동일한 사이버 보안조치 적용에 대한 보안조치 관리에 어려움이 있다. 따라서 규제 대상 내에서도 원전의 비상정지를 일으키고, 노심 손상을 유발할 수 있는 디지털자산을 분석하고 관련된 자산에 단계적 접근방식을 적용한 보안대책 및 규제방향 제시를 통한 효과성 제고가 필요하다. 이에 본 연구에서는 사이버 위협으로 발생할 수 있는 원전 사고와 직접 관련된 디지털자산에 대하여 국내외 원전 사이버보안 규제지침 및 최적관행 분석을 통해 단계적 접근방식의 규제요건 도출을 위한 보안조치 적용 방안을 제시하고자 한다.

II. 원전 사이버보안 규제 현황

2.1 국외 현황

2000년대에 들어 원자력시설을 목표로 한 사이버공격에 대한 대비가 필요하다는 인식이 점차 늘어났으며, 이를 바탕으로 실질적인 사이버공격 대비를 위한 원전 사이버보안 규제 체계가 마련되기 시작했다. 먼저, IAEA 등 국제사회에서는 원자력시설에 대한 사이버보안 강화를 위해, 기존의 물리적방호체제 내에서 사이버보안 이슈에 대하여 2011년 핵물질 및 원자력시설 물리적방호 기술지침(NSS No. 13)(INFCIRC/225/Rev.5)에서 ‘물리적방호, 원자력안전 및 핵물질계량관리 기능을 수행하는 전산시스템은 위협평가나 설계기준위협에 따라 사이버공격, 임의조작, 위조와 같은 위해로부터 보호되어야 함’을 새롭게 명시함으로써, 사이버보안 요건을 추가하였다. 또한, 같은 해에 제정된 원자력시설 사이버보안 기술지침(NSS No. 17)을 통해 핵안보 및 안전기능을 수행하는 컴퓨터기반 시스템에 사이버공격으로 인한, 핵물질의 불법이전(Unauthorized Removal) 및 방사선적 사보타주(Radiological Sabotage) 발생을 예방, 탐지 및 대응하는 것이 원자력시설 사이버보안의 목적임을 발표하고, NSS No. 17에서는 원자력시설의 디지털시스템을 보호하기 위한 사이버보안 프로그램(CSP) 수립방법과 사이버보안을 위한 관리 및 이행 사항에 대해 조직, 자산 분석, 단계적 접근(Level, Zone), 위험관리, 보안설계, 공급망 통제에 대한 세부적인 내용을 제시하였다. 추가적으로 원자력시설 계측제어시스템에 특화된 사이버보안 가이드를 제공하기 위한 계측제어시스템 사이버보안 기술지침(NST No. 33-T) 등의 발행을 통해 사이버공격에 의한 원전 사고 예방을 촉구하고, 안전-안보 연계를 고려한 보안체계의 수립을 권고하고 있다.

세계 각국에서는 이러한 국제사회의 흐름과 더불어 국가별 원자력시설 사이버보안 규제 체계를 갖추기 시작하였으며, 이에 대한 흐름도는 Fig 1과 같다. 미국의 원자력규제위원회(NRC)는 2009년에 사이버보안 연방법령(10 CFR 73.54)을 제정하여 원전 디지털 컴퓨터, 통신시스템, 네트워크를 보호하도

록 요구하고 있으며, 10 CFR 73.54에서의 원전 별로 보호될 디지털자산 확인, 심층방호(Defense-in-Depth) 전략 및 자산별 보안조치 적용 등의 내용을 포함한 사이버보안계획(CSP)을 마련하여 NRC의 검토 및 승인을 받도록 하고 있다. 또한, 2010년 사이버보안 규제지침(RG 5.71)을 제정하여 악의적인 사이버공격으로부터 디지털설비를 보호하기 위한 보안요건을 기술하고 원전의 사이버보안 조직(CST), 대상 분석, 심층방호, 보안조치, 위험평가 등을 통해 일반적인 디지털 시스템을 위한 사이버보안 지침인 NIST 800-53을 기반으로 조정된 보안조치 147개를 각각의 디지털자산 별로 고려하도록 규제지침을 제시하였다. 2010년과 2012년에 NRC는 각각 사업자의 사이버보안 지침(NEI 08-09, Rev.6)과 필수디지털자산 식별 지침(NEI 10-04, Rev.2)을 배서(Endorsed)하였으며, 이를 기반으로 작성된 사업자의 사이버보안계획(CSP)과 해당 계획을 8개 단계로 나누어 이행하는 단계별(Milestones) 이행계획을 2012년 승인 완료하였다. 2013~2015년 NRC는 사업자의 사이버보안계획 1~7단계 이행결과에 대한 중간검사(Interim Inspection)를 수행하였으며, 2016~2017년 중간검사 경험공유 및 사업자 협의를 거쳐 사업자 사이버보안조치 평가 지침(NEI 13-10)을 배서하였다. 2018년부터는 사업자의 사이버보안계획 8단계에 대한 전체검사(Full Inspection)를 수행 중에 있으며, 해당 검사는 2020년에 완료될 예정이다.

2.2 국내 현황

국내에서는 2013~2014년 관련 법령 개정을 통해 사이버보안 규제요건을 마련하고 2015년부터 본격적으로 사이버보안 규제를 이행하고 있다. 2013년 12월, 원자력시설 등의 방호 및 방사능 방재 대책법(이하, 방사능방재법), 시행령 및 시행규칙의 개정을 통해 원자력시설 사이버보안 체계 구축을 위한 규제자와 사업자의 의무를 제시하였다. 이러한 의무에는 사이버위협을 포함한 설계기준위협의 설정, 위협 평가, 정보시스템 보안규정 수립, 이행 및 심·검사, 사이버보안 훈련 수행 및 평가 등이 포함되어 있으며, 방사능방재법 시행규칙에서는 필수디지털자산 보안을 위한 항목들로 조직, 필수디지털자산 분석, 단계적 보안전략, 보안조치, 감시 및 평가, 사건대응을 제시하고 있다. 2014년 10월, 방사능방재법 관련 고시의 개정을 통해 정보시스템 보안규정 작성에 대한 세부기준, 사이버보안 관련 검사 및 훈련에 대한 규정을 수립하였으며, 같은 시기에 원자력시설 컴퓨터 및 정보시스템 보안 기술기준(KINAC/RS-015, Rev.1)이 발행되어 방사능방재법, 시행령, 시행규칙 및 고시에 따른 원전 사이버보안 이행기준 및 정보시스템 보안규정 표준양식을 제시하였다. 이러한 사이버보안 관련 원자력안전위원회 고시와 한국원자력통제기술원(KINAC)의 규제기준(KINAC/RS-015)을 통해, 각 원자력시설에서 정보시스템 보안규정을 마련하고 원자력시설의 안전(Safety-related 및 Important-to-Safety), 보안(Security), 비상대응(Emergency Preparedness) 기능을 수행하거나 침해시 해당 기능에 악영향을 줄 수 있는 디지털기기를 필수디지털자산으로 식별하도록 요구하고 있으며, 각 필수디지털자산에 대해 취약점 분석 및 평가를 수행하고 이를 기반으로 적절한 보안조치를 적용하도록 규제하고 있다. 국내 원자력사업자는 방사능방재법령에 따라 시설별 정보시스템 보안규정을 마련하여 2015년 4월에 원자력안전위원회로부터 승인을 받았으며, 같은 해 8월에 정보시스템 보안규정을 7개의 단계로 나누어 2018년까지 이행하기 위한 7단계 이행계획도 승인받게 된다. 사업자는 2015년 10월 사이버보안 조직 구성(1단계)에 대한 이행결과 제출을 시작으로 현재 운영적·관리적 보안조치(6~7단계) 이행결과까지 제출한 상태이며, 원자력안전위원회와 한국원자력통제기술원에서는 사업자의 단계별 이행결과의 적절성에 대해 특별검사를 수행하여 확인하고 있다. 현재는 운영적/관리적 보안조치(6단계) 이행결과에 대한 특별검사를 수행하는 중이며, 2019년까지 최종 7단계 특별검사가 완료될 예정으로, 그 이후에는 정기검사를 통해 사업자의 사이버보안 체계가 지속 확인될 것이다.

III. 보안조치 적용 방안

원전디지털자산을 대상으로 하는 사이버보안 규제활동은 규제기준에서의 100여가지의 보안조치 항목을 통제하는 방식으로 사이버 위협에 대응하는 체계로, 보안통제 적용 대상이 되는 필수디지털자산에 대해 일괄적으로 동일한 사이버 보안조치를 적용하는 것에 대한 실효성 제고가 필요하다. 이에 본 연구에서는 원자력시설 사이버보안 규제 대상 내에서도 사고와 직접 관련된 필수디지털자산의 집합으로 이루어

진 디지털자산에 대해서는 더 많은 자원을 투입하는 규제 요건 도출을 위해 단계적 접근방식(Graded Approach)의 보안조치 적용 방안을 제시하고자 한다. 단계적 접근방식은 규제 대상 설비의 침해영향도(Consequence)를 분석하여, 높은 침해영향도를 갖는 설비에 대해 보다 높은 수준의 보안조치를 적용하는 것을 기본으로 한다. 이를 적용하기 위한 방안은 기존에 필수디지털자산에 요구되고 있는 보안조치를 보다 강화하거나 추가적인 보안조치를 개발하여 원전 사고와 직접 관련된 디지털자산에 요구하는 방식과 기존의 보안조치를 재분석하여 원전 사고와 직접 관련되지 않는 필수디지털자산에 대해서는 최소한의 보안조치를 요구하는 방식으로 크게 나눌 수 있어 본 장에서는 각각의 방식에 대해 세부적으로 구체화한 방안을 기술한다.

3.1 현 보안체계 내에서의 요건 강화 방안

3.1.1 심층방호 전략 요건 강화

현재 국내외 규제기준에서는 원자력발전소에 심층방호 전략을 적용하여 설계기준위협에서 정한 사이버 공격으로부터 보호를 요구하고 있으며, 사이버보안 심층방호 구조는 사이버보안 경계로 구분된 N가지의 사이버보안 등급으로 구성된다. 그리고 각 경계에서의 디지털 통신은 감시 및 통제되며 높은 사이버보안성이 요구되는 시스템일수록 높은 등급의 구역에

Fig. 2. Example of defense-in-depth for cyber security separated into 6 levels

배치된다. R.G. 5.71 및 KINAC/RS-015 에서는 심층방호 구조를 4가지 등급으로 분류하여 필수디지털자산 중 안전 관련 기능(Safety function) 기능을 등급4에 배치하는 Fig 2의 예시를 통해 SSEP 기능을 기준으로 하는 심층방호 전략을 제시하였다. 본 연구에서는 SSEP 기능 기준을 적용한 심층방호 등급 분류에서 나아가 사고와 직접 연관된 디지털자산은 추가로 더 높은 등급에 배치하여 현행 요건을 강화시키는 방안을 제시한다. 즉, 기존의 필수디지털자산 규제기준에서 적용된 심층방호의 N개의 등급을 $N+1$개로 분리하고, 사고와 직접적으로 연관된 디지털자산을 등급$N+1$에 배치하여 기존의 등급N에 해당하는 안전, 보안기능을 수행하는 필수디지털자산과 격리하여 보안조치를 적용하는 방안을 통해 현행 보안조치를 강화할 수 있다. 즉, 등급$N+1$에

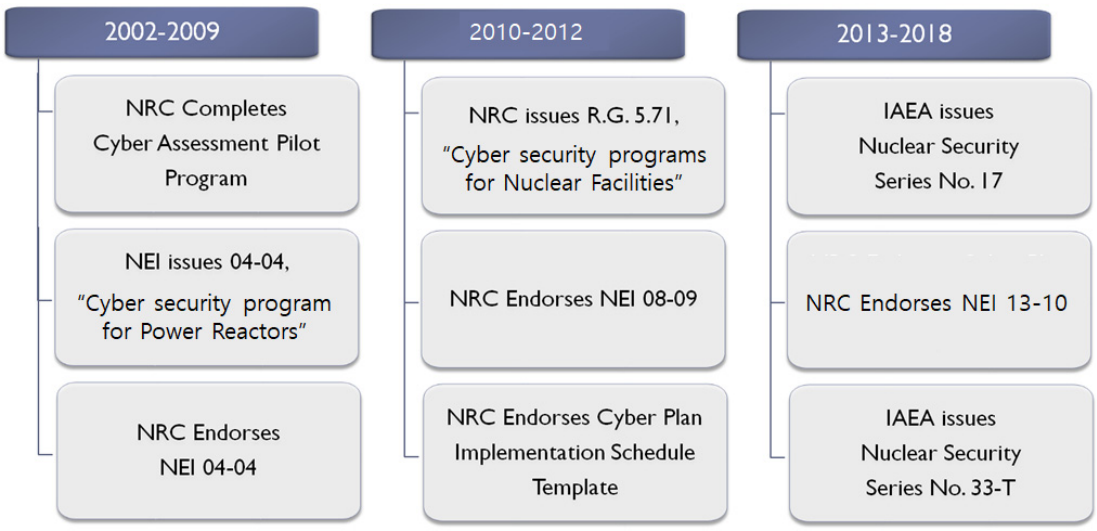


Fig. 1. History of Cyber Security Regulatory policy for international nuclear cyber security

서 등급N 및 등급N에서 등급N-1로의 통신은 물리적으로 단방향이 되도록 구성하고, 등급$N+1$인 핵심디지털자산 간에만 양방향 통신을 사용하도록 제한하여, 등급$N+1$에 있는 네트워크, 시스템 및 핵심디지털자산으로의 핸드쉐이킹, 프로토콜을 포함한 어떠한 종류의 정보도 전송 불가하게 구성하는 것이다.

3.1.2 보안조치 요건 강화

현 원자력시설의 사이버보안 규제요건 내에는 필요한 문서화, 상세한 보안 요건, 주기적 검토의 최소단위, 조치 수행의 범위, 조치 적용이 어려울 때의 대안적 조치 수행 등의 100여 가지의 보안조치를 명시하고 있다[1]. 완화실패로 노심 손상을 유발할 수 있는 사고와 관련된 디지털자산은 기존의 보안조치 중 Table 1에서 제시하는 일부 항목에 대해서는 더 구체적이고 엄격한 보안조치가 필요할 것이며, 이에 현 규제체계 내에서의 사이버 보안조치를 기준으로 세부적 내용에 대한 변경, 조정, 추가 등을 통해 현 보안조치를 강화할 수 있는 요소를 다음의 3가지 유형으로 도출할 수 있으며, 각 유형 별로 관련한 보안요건 예시는 Table 2과 같다.

1) 주기 변경

사이버 보안조치 중에 사용 및 변경 여부에 대한 검토, 목록 갱신, 사용 불가 조치, 분석 및 검증, 감사 등 주기성을 부여하고 있는 항목에 대해 필수디지털자산에 적용하는 최소한의 주기보다 빈번하게 수행되도록 주기를 단축할 수 있다.

2) 범위 조정

사이버 보안조치 중에 보안 조치를 적용하기 위한 방법과 적용 대상에 대한 범위를 정의 및 구체화하거나, 항목과 관련한 상세한 요건이 명시되어 있는 기준 지침 문서를 제시함으로써, 세부적이면서 강화된 보안 조치 적용이 가능할 수 있다.

3) 구체적 요건 추가

기존의 사이버 보안조치 중에 자동화된 도구 사용, 문서화, 보안 기능 등 세부적 항목 추가를 통해 기존 보안조치를 구체화하거나 강화, 대안적 대책 수행 등의 보안 조치를 수행할 수 있다.

Table. 1. List of required Security Control Reinforcing

No.	Security Control
1	Account Management
2	Access Enforcement
3	Information Flow Enforcement
4	Seperation of Functions
5	System Use Notification
6	Session Lock
7	Permitted Actions without Identification or Authentication
8	Insecure and Rogue Connections
9	Access Control for Portable and Mobile Devices
10	Auditable Events
11	Content of Audit Records
12	Audit Review, Analysis, and Reporting
13	Time Stamps
14	Protection of Audit Information
15	Audit Record Retention
16	Transmission Integrity
17	Heterogeneity/Diversity
18	Device Identification and Authentication
19	Authenticator Feedback
20	Hardware Configuration

3.1.3 보안조치 요건 추가

현 사이버 보안조치 내 명시되지 않은 기술적, 운영적, 관리적 보안요건을 추가하여 핵심디지털자산만을 대상으로 한 보안조치 요건을 수행 할 수 있다.

기술적 보안조치

기술적 보안조치는 일반적으로 인적 개입을 요구하지 않고, 자동적이거나 전자적으로 정책들이 수행되는 조치들로, 하드웨어, 펌웨어, 운영체제, 응용프로그램 등의 메커니즘에 의해 수행된다. 이에 소프트웨어, 프로토콜 및 통신, 접근통제, 보안기능 및 장비 등의 보안성이 요구되며 다음과 같은 예시의 추가적 보안조치를 적용할 수 있다.

Table 2 . Example for applicable Requirement by R.G. 5.71

	Example		Description
1) Cycle Change	Req.	**B.1.2 Account Management** 〔Licensee/Applicant〕 is responsible for the following : • reviewing CDA accounts in a manner consistent with the access control list provided in the [design control package, access control program, cyber security procedures] and initiating required actions on CDA accounts [no less frequently than once every 30 days],	
	〔no less frequently than once every 30 days〕 → At least once every 30 days, Immediately when administrators and users are changed		▸ Change existing cycle(at least once a quarter) more frequently, In addition, by changing the requirements for immediate changes in administrators and users, such as personnel transfers, it is possible to reduce the likelihood that unauthorized accounts will be used for unauthorized access and strengthen control requirements to prevent unauthorized or unintended use,
2) Range Adjust	Req.	**B.1.3 Access Enforcement** 〔Licensee/Applicant〕 is responsible for the following: • requiring dual authorization for critical privileged functions and the creation of any privileged access for users, and	
	dual authorization → Approve by dual authentication methods (In addition to administrative procedures, technical and physical authentication mechanisms could be applied)		▸ By changing the range of the approval method from the existing standards(dual authorization), it is possible to apply the multiple or various access control through comparison and analysis of the advantage and disadvantage of the authentication method such as passwords, tokens, biometrics, location-based authentication by giving technical and physical diversity to the mechanisms.
3) Add detailed require ment	Req.	**B.1.19 Access Control for Portable and Mobile Devices** 〔Licensee/Applicant〕 is responsible for the following : • enforcing and documenting that mobile devices are only used in one security level and that mobile devices are not moved between security levels.	
	(Add) → Enforcing and documenting that mobile devices connected to VDA maintain the same level of integrity as CDA		▸ Portable media and mobile devices are the main attack vectors in malicious attacks. So, they connected to VDA should be managed by the same security level as VDA. Thereby, it could strengthen the control of unauthorized access and data movement.

공개적으로 접근 가능한 요소 사항에 대해 다음을 보장
- 공개적으로 접근할 수 있는 시스템에 정보를 게시할 수 있는 권한을 제한적으로 부여
- 공개적으로 접근할 수 있는 시스템에 SSEP 기능에 악영향을 미치거나 공격 수행에 영향을 줄 수 있는 정보를 포함하여 게시하지 않도록 권한을 부여받은 사람의 교육 필요

▸ 본 항목의 보안 목적은 SSEP 기능에 악영향을 미칠 수 있거나 악의적인 공격을 수행하는데 도울 수 있는 정보가 공개되지 않도록 보장하기 위한 것으로 공격 수행에 도움을 줄 수 있는 정보를 식별하고 식별된 정보를 보호하기 위한 보호 메커니즘 개발과 구현이 필요하며 정보에 접근할 수 있는 담당자는 정보의 민감한 특성에 대해 통보받고 해당 보안 조치에 대한 지침 제공이 필요

운영적 보안조치

운영적 보안조치는 사람에 의한 사이버보안 활동 및 정책 환경에 의한 조치로 원자력 시설 및 계약업체의 책임 등에 대해 문서화하여야 한다. 이에 계정 관리, 인증 관리, 물리적 및 환경적 보호, 유지보수 등의 보안성이 요구되며 다음과 같은 예시의 추가적 보안조치를 적용할 수 있다.

예상되는 실패에 대한 응답에 대해 다음을 보장
- 기술 사양, 예방 유지 프로그램, 유지보수 프로그램, 보안 계획, 비상 계획, 시정조치 프로그램의 준수를 통해 핵심디지털자산의 가용성 보호
- 프로그램의 적용이 어려울 경우 다음과 같은 방법으로 핵심디지털자산의 가용성 제공
- 필요한 경우 구성요소의 대체, 구성요소의 대체 기능 및 교환가능 활동에 대한 메커니즘 활용
- 특정 운영환경에서의 구성요소에 대한 평균고장시간 고려

▸ 본 항목의 보안 목적은 핵심디지털자산 가용성을 보장하기 위한 것으로 예상되는 실패에 대해 적절한 대응 활동이 계획되고 실행될 수 있도록 핵심디지털자산을 분석하고 핵심디지털자산의 기술 사양, 유지보수 프로그램, 비상 계획 및 시정조치 프로그램 등에서 다루지 않는 사항에 대한 적절한 정책과 절차 개발이 필요

관리적 보안조치

관리적 보안조치는 위험 관리에 필요한 활동에 의한 조치로 사이버보안 정책 환경을 위한 문서화된 정책 및 계획 수립이 필요하다. 이에 시스템 개발, 구매 시의 보안성이 요구되며 다음과 같은 예시의 추가적 보안조치를 적용할 수 있다.

공급 및 구매 시 정보 출력 처리 및 보존에 대해 다음을 보장
- 민감한 정보가 권한이 있는 개인에게만 공개되도록 보존
- 권한이 없는 개인에게 정보의 출력이 노출되지 않도록 처리

▸ 본 항목의 보안 목적은 핵심디지털자산에서 얻은 민감한 정보가 적절히 처리되고 허가되지 않은 개인에게 공개되지 않도록 보장하는 것으로 보호되어야 하는 정보의 분류 및 해당 정보에 대한 접근 권한을 가진 개인의 명확성이 필요

3.2 현 보안체계 내에서의 대안조치 적용 방안

기존의 필수디지털자산은 침해영향도를 고려하지 않고 원전 내의 안전, 보안, 비상대응 기능과 관련된 디지털자산을 식별해 동일한 보안조치를 적용하였다. 그러나 높은 침해영향도를 갖는 사고와 직접 연관된 디지털자산을 추가적으로 식별하게 되면, 사고와의 연계성이 적은 필수디지털자산은 낮은 침해영향도를 갖는다는 것을 자동적으로 확인할 수 있게 되므로, 기존의 보안조치보다 낮은 수준의 보안조치를 적용하는 방안도 고려해 볼 수 있다. 이와 관련해 NEI 13-10에서도 이러한 침해영향별 차등적 보안조치 적용 방안과 유사한 개념을 도입하고 있으며, 세부적인 내용은 다음과 같다.

3.2.1 NEI 13-10에서의 단계적 보안 조치

NEI 13-10에서는 각 디지털자산별로 사이버공격 시 예상되는 침해영향에 따라 등급을 분류하고, 해당 영향의 정도에 따라 각 디지털자산에 차등적으로 사이버 보안조치를 적용함을 기본으로 하여 사이버 보안조치 평가를 수행하도록 요구하고 있다. 사이버공격으로 인한 결과가 안전 또는 보안 기능에 악영향을 미칠 수 있는 디지털자산은 높은 침해영향도를 갖는 것으로 간주하여 직접(Direct) 필수디지털자산으로 분류하고, 안전 및 보안 기능에 악영향을 미칠 수 없는 디지털자산은 낮은 침해영향도를 갖는 것으로 간주하여 비직접(Non-direct) 필수디지털자산으로 분류한다. 그리고 Fig 3과 같이 직접 필수디지털자산에 대해서는 규제

Table 3. Characteristic by type of Direct CDA

Characteristic of CDA		A.1	A.2	A.3	B.1	B.2	B.3
Change and inject program code	Factory installed by manufacturer	×	○	○	○	○	○
	Installed in the field	×	×	×	×	×	○
Have HMI		×	○	○	○	○	○
Changing the operating parameters	Device for Management /Test	○	N/A	N/A	N/A	N/A	N/A
	Internal HMI	×	○	○	○	○	○
Change configuration setting	Using a maintenance tool	○	○	○	○	○	○
	Built-in HMI	×	×	○	○	○	○
	By taking the CDA out of service	○	○	○	○	○	○
	By a console port, USB, serial communication channel	×	×	×	×	×	△
HMI access control	Exist functions	×	×	○	○	○	○
	Support multi-users and individual authentication for users	×	×	×	×	×	×
	Log storage	×	×	×	×	×	△
Firmware updates		×	×	×	×	×	○
Communicatio n software	Contains functionality	×	×	×	△	○	○
	Configuration of the CDA	N/A	N/A	N/A	×	×	○
Exist consol port or external interface		×	×	×	△	△	○
Contains a maintenance and configuration port		×	○	○	○	○	○
Storage for data	Contain bulk storage for data	N/A	○	○	○	○	○
	Support external access	N/A	×	×	×	×	○
Employ a physical access protection mechanism such as a key or fob		×	×	○	○	○	○
Communication Capability	Using either an RS-232, 422, 485	×	×	×	○	○	○
	Using vendor-proprietary hardware interface	×	×	×	×	×	○
	Change for program by communication function	×	×	×	×	○	○

※ Description Symbol
(O : Providing functions, △ : Providing limited functions, × : No functions, N/A : Not applicable)

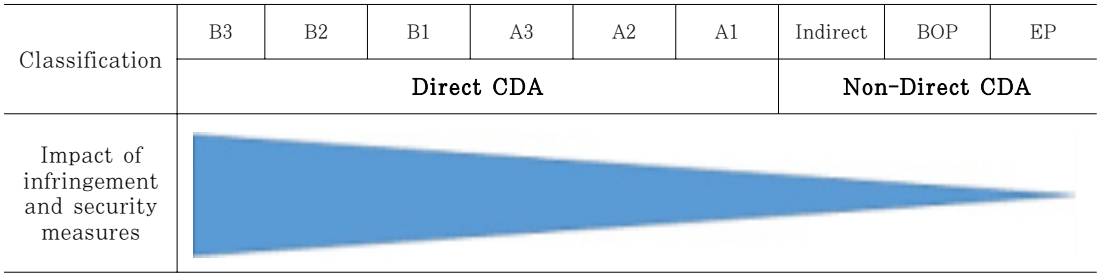


Fig. 3. Concept of Graded Approach in NEI

기준에서 제시하는 100여개의 사이버 보안조치를 평가하고, 비직접 필수디지털자산에 대해서는 기존의 보안조치와 관련된 공격벡터를 모두 막기 위한 기본적인 보안조치(Baseline Cyber Security Controls)를 기술적 보안조치(RS-015, 부록 2.1의 62개 보안조치)에 대한 대안조치를 적용하도록 하고 있다. 비직접 필수디지털자산은 수행 기능과 침해영향에 따라 비상대응, Balance of Plant(BOP), 간접(Indirect) 필수디지털자산과 같이 세부적으로 분류되고, 일반적으로 물리적접근 통제, 무선통신 통제, 네트워크 접근 통제, 매체 통제, 형상 관리, 주기적인 기능 점검 및 보안조치 감시를 기본 보안조치로 요구하고 있다. 직접 필수디지털자산에 대해서는 설비의 소프트웨어 및 하드웨어 특성 등에 따라 유형을 분류하고, 유형별로 각 기술적 보안조치마다 적용 가능 여부와 대안조치에 대해서 사전에 평가하여 보안조치 적용 방안을 표준화한 후, 유형별로 일관된 보안조치를 적용하는 것을 기본으로 하고 있다. 이는 필수디지털자산에 대한 보안조치 적용 프로세스를 최적화하여, 규제 기준에서 요구하는 보안 수준을 효율적이고 효과적으로 달성하는 것을 목적으로 하고 있다.

직접 필수디지털자산의 유형별 특성은 Table3과 같으며, 비직접 필수디지털자산을 위한 기본적인 (Baseline) 보안조치는 다음과 같다.

- a : 필수디지털자산을 방호구역에 위치시키거나, 정보시스템 보안규정에 적시된 물리적 및 환경적 보호 관련 보안조치를 모두 적용
- b : 필수디지털자산 및 필수디지털자산과 연결된 자산에 무선통신 기능이 없어야 함
- c : 필수디지털자산 및 필수디지털자산과 연결된 자산은 다른 네트워크와 물리적으로 단절(Air-gapped)되거나 결정적(Deterministic) 격리장치에 의해 격리되어야 함
- d : 휴대용 매체 및 모바일 장치(PMMD)는 NEI 08-09 D.1.19의 PMMD 접근 통제 보안조치에 따라 통제되어야 함
- e : 해당 필수디지털자산에 대한 변경은 다음 사항을 보장하기 위해 이행 전에 평가 및 문서화되어야 함
  · 기본적인 보안조치가 유지되고, 새로운 공격경로/취약점이 생기지 않았으며, 필수디지털자산에 대한 변경이 해당 필수디지털자산을 직접 필수디지털자산으로 만들지 않음
- f : 해당 필수디지털자산, 또는 해당 필수디지털자산과 상호 연결되고 필수디지털자산의 침해로 영향 받는 설비가 의도한 기능을 수행할 수 있는지를 확인하기 위해 주기적으로 점검*되어야 함

* 점검 주기는 사이버 공격으로 인해 안전, 보안 및 비상대응 기능에 악영향을 미치기 전에 사이버 공격을 탐지하고 완화하기에 충분해야 함

- g : 기본적인 보안조치가 그대로 유지되는지 확인함으로써 필수디지털자산의 보안 상태가 유지되도록 지속적인 모니터링과 평가를 수행

3.2.2 단계적 보안 조치 적용 방안

NEI 13-10의 보안조치 적용 프로세스를 핵심디지털자산에 그대로 옮겨와 적용하게 된다면, 사고와 직접 관련된 디지털자산에 대해서는 기존의 보안조치 모두를 적용하고 그 밖의 디지털자산에는 공격벡터를 모두 막기 위한 기본적인 보안조치를 적용하는 방안을 고려해 볼 수 있다. 하지만 사고와 직접 관련된 디지털자산은 노심 손상과 같은 중대사고를 유발할 수 있는 설비이므로 안전 및 보안 기능에 악영향을 미칠 수 있는 설비인 직접 필수디지털자산에 포함될 수 있다. 이렇듯 사고와 직접 관련된 디지털자산과 직접 필수디지털자산이 정확히 일치하지 않고 직접

필수디지털자산 중에 사고와 관련이 적은 디지털자산이 있을 수 있으므로 이러한 자산에 대해서는 기본적인 보안조치를 적용할 것인지 기존의 보안조치 전부를 적용할 것인지에 대한 결정이 필요하다. 이 중에서 보안 기능을 수행하는 필수디지털자산의 경우, 원자로정지를 유발할 수 있는 물리적 공격과 핵물질의 불법이전을 방지한다는 측면에서 사고와 직접 관련된 디지털자산과 동일하게 기존의 보안조치를 모두 적용할 필요가 있다. 다만 NEI 13-10에서 제시한 바와 같이 직접-필수디지털자산 유형 중 어디에 해당하느냐에 따라 유형별로 사전에 도출된 보안조치를 적용하는 것은 가능하다. 그 외에 사고와 관련이 적은 필수디지털자산에 대해서는 직접 필수디지털자산이지만 중대사고를 유발 할 수 없으므로 공격벡터 제거를 위한 기본적인 보안조치를 적용하는 것으로 보안 수준을 조정하는 방안도 생각해 볼 수 있다. 마지막으로 남은 비직접 필수디지털자산에 대해서는 NEI 13-10과 동일하게 기본적인 보안조치를 적용하여 요구되는 보안 수준을 만족하도록 한다.

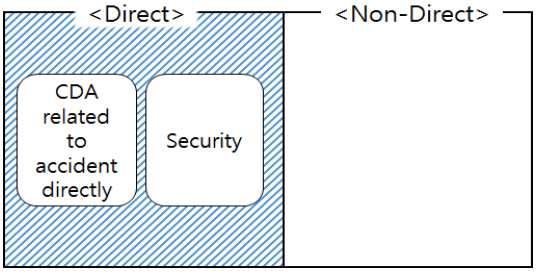


Fig. 4. Relation diagram between CDA related to accident directly and general CDA

Table 4. Application of security controls considering CDA related to accident directly

Asset Types (Impact of Infringement)		Application of security measures
Direct CDA	CDA related to accident directly (Very High)	Apply about 100 security controls after evaluating each controls
	CDA related to security (High)	Apply baseline technical security controls as NEI 13-10 and all operational/ management security controls
	CDA related to safety (Normal)	Apply alternative controls and all operational/ management security controls to remove attack vectors
Non-Direct CDA (Low)		

아래의 Fig 4는 사고와 직접 관련된 디지털자산과 필수디지털자산 간의 관계를 도식화하여 보여주고 있으며, 빗금으로 표시된 부분이 NEI 13-10의 보안조치 적용 방안과 차이가 나는 부분이다.

본 연구에서 제시된 규제 방향을 정리해보면 최종적으로 Table 4와 같은 보안조치 적용 방안을 도출할 수 있다.

IV. 결 론

사이버공격으로 인한 원전 사고를 예방하기 위해서는 사고와 직접적으로 연관된 디지털자산 도출과 이에 대한 보안대책 적용이 요구된다. 현재의 원자력시설 사이버보안 규제에서는 안전, 보안, 비상대응 기능과 관련된 디지털자산(필수디지털자산)에 대해 100여개의 보안조치 항목을 통제하는 방식을 사용하고 있으나, 모든 규제 대상 자산에 일괄적으로 동일한 보안조치를 적용했을 시 보안조치 관리의 어려움을 야기한다. 이에 사이버보안 규제 대상 내에서도 단계적 접근방식을 적용하여 높은 침해영향도를 갖는 디지털자산에 대해서는 높은 수준의 보안조치를 적용하고, 낮은 침해영향도를 갖는 나머지 필수디지털자산에 대해서는 낮은 수준의 보안조치를 적용하여 규제 효율성을 높일 필요가 있다.

본 연구에서는 단계적 접근방식을 고려하여 사고와 직접적으로 연관된 디지털자산을 대상으로 기존에 필수디지털자산에 요구되고 있는 보안조치를 보다 강화하거나 추가적인 보안조치를 개발하여 하는 방안 및 현행 사이버 보안조치를 그대로 적용하고, 사고와의 연관성이 낮은 디지털자산에는 기존 보안조치를 대안적으로 만족시킬 수 있는 대안조치를 적용하는 방안을 제시하였다. 본 연구에서의 결과는 기존의 사이버보안 규제 대상 자산보다 높은 보안성을 가질 수 있는 규제 요건을 마련하는 기반이 될 것이며, 나아가 사고와 직접적으로 관련된 원전디지털자산 규제 방안을 마련함으로써 원전의 보안성을 강화할 수 있을 것으로 기대된다.

References

[1] Korea Institute of Nuclear Nonproliferation And Control(KINAC), KINAC/RS-015, "Regulatory Standard on Computer Security of Nuclear Facilities", 2016.

[2] Korea Institute of Nuclear Nonproliferation And Control(KINAC), KINAC/RS-019, "Regulatory Standard on Critical Digital Assets of Nuclear Facilities", 2015.

[3] U,S.Nuclear Regulatory commissio(U.S.NRC), Regulatory Guide 5.71(R.G 5.71), "Cyber Security Programs for Nuclear Facilities", 2010.

[4] U,S.Nuclear Regulatory commissio(U.S.NRC), Regulatory Guide(R.G) 1.152 (Rev.2), "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants", 2006.

[5] U,S.Nuclear Regulatory commissio(U.S.NRC), 10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks", 2009.

[6] Nuclear Energy Institute(NEI), NEI 10-09(rev.0) "Addressing Cyber Security Controls for Nuclear Power Reactors", 2011.

[7] Nuclear Energy Institute(NEI), NEI 08-09(rev.6) "Cyber Security Plan for Nuclear Power Reactors.", 2010.

[8] Nuclear Energy Institute(NEI), NEI 10-04(rev.2) "Identifying Systems and Assets Subject to the Cyber Security Rule", 2012.

[9] Nuclear Energy Institute(NEI), NEI 13-10(rev.6) "Cyber Security Control Assessments.", 2017.

[10] International Atomic Energy Agency(IAEA), Nuclear Security Series No. 13, "Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities" (INFCIRC/225/Revision 5), 2011.

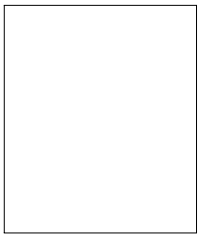
[11] International Atomic Energy Agency(IAEA), "Nuclear Security Series No. 17, Computer Security at Nuclear Facilities", 2011.

[12] International Atomic Energy Agency(IAEA), "Nuclear Security Series No. 13-T, Computer Security of Instrumentation and Control Systems at Nuclear Facilities", 2018.

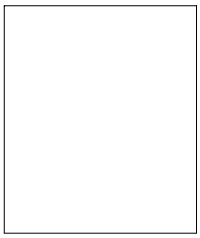
[13] National Institute of Standards Technology(NIST), 800-53(rev3) "Recommended Security Controls for Federal Information Systems and Organizations", 2015.

[14] National Institute of Standards Technology(NIST), 800-82(rev2) "Guide to Industrial Control Systems (ICS) Security", 2015. hash protocols," CS-2006-20, Computer Science Department, University of Virginia, 2006.

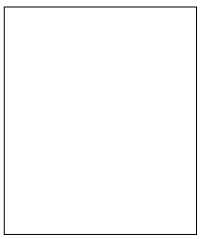
〈저자소개〉



김 인 경 (In-Kyung Kim) 정회원
2015년 2월: 고려대학교 수학과 석사
2017년 5월~현재: 한국원자력통제기술원 사이버보안실 전문연구원



변 예 은 (Ye-Eun Byun) 정회원
2012년 2월: 경북대학교 수학과 학사
2014년 8월: 한국과학기술원 수리과학과 석사
2015년 8월~현재: 한국원자력통제기술원 연구원
〈관심분야〉 정보보안, 기반시설 보안



권 국 희 (Kook-Heui Kwon) 정회원
2008년 2월: 경북대학교 컴퓨터공학과 학사
2012년 9월: 아주대 정보전산학과 석사
2018년 8월: 충남대 컴퓨터통신 및 보안 박사과정 수료
2007년 11월~2011년 8월: 한국전력기술 원자력계측제어실 선임기술원
2011년 9월~현재: 한국원자력통제기술원 사이버보안실 선임연구원/실장
〈관심분야〉 정보보안, ICS 보안, 개발단계 보안, Risk 평가