원자력시설 사이버사건 대응훈련 정책 개선을 위한 규제방안 연구

류진호* 김상우*
*한국원자력통제기술원 사이버보안실
halloyu@kinac.re.kr, kjoey@kinac.re.kr

A Study on the Improvement of Cybersecurity Exercise Policy for the Nuclear Facilities

Jinho Ryu*
*Cyber Security Division, Korea Institute of Nuclear Nonproliferation and Control

요 약

정보처리기술이 발달함에 따라 원자력시설에 대한 사이버침해 가능성이 갈수록 높아지고 있다. 방사능방재법 및 관련 법령에 의거하여 국내 원자력시설은 각 시설 별 사이버사건 비상대응 절차를 수립하고 절차의 유효성 및 비상대응조직의 대응역량을 제고하기 위한 목적의 주기적인 사이버사건 대응훈련을 실시하고 있으며, 규제기관의 독립적인 훈련평가 결과를 통해 많은 개선사항이 도출되고 있다. 본 논문에서는 현행 원자력시설의 사이버사건 대응훈련 체계를 분석하여 사이버사건대응훈련 정책의 개념에 대해, 국내·외 기준에 따른 사이버사건 대응훈련 정책의 요소를 식별하여 이를 개선하기 위한 구체적인 규제방안을 제시한다.

1. 서론

전 세계적인 정보처리기술의 발달은 산업제어시스템을 활용하는 원자력시설 계측 및 제어분야에 대해 디지털화된 기기들의 도입들을 촉발하며 많은 변화를 가져왔다. 이러한 변화가 적시성, 효율성을 증대시킨 반면, 사이버보안의 관점에서는 또 다른 대책이 요구되었다. 2015 년 원자력시설 등의 방호 및 방사능 방재 대책법의 개정으로 원자력시설에 대한 전자적침해행위에 대한 대책이 수립되도록 법령체계가 정비되었다.

2016 년 한국원자력통제기술원에서 발행한 *원자력시설의 컴퓨터 및 정보시스템 보안* 심·검사 기준서[1]는 각 원자력시설별 사이버보안조치 이행의 기준이 되는 "정보시스템 보안규정 (Cyber Security Plan, CSP)"의 지침을 제시하며, 이에 따라 해당 계획의 단계별 이행에 대한 특별검사가 2019 년 완료된 바 있다.

아울러 원자력시설에 발생할 수 있는 사이버사건에 대한 대응체계를 시험하고 대응역량을 제고하기 위한 사이버사건 대응훈련(이하, 사이버보안 훈련)이 관련 법령에 근거하여 2016 년부터 실시되고 있다. 그러나 사이버보안 필수디지털자산 식별, 휴대용 저장매체 통제, 심층방호 적용 등 주요 보안조치들이 앞서 언급한 CSP 에 따라 이행되고 있는 것과는 달리 사이버보안 훈련은 주로 관련 법령 및 고시에 근거하여 수행되고 있다. 이에 따라 원자력시설 사이버보안 이행의 기준이 되는 CSP 와 사이버보안 훈련과의 관계성이 모호하고, 사이버보안 훈련의 내용이 KINAC/RS-015 에 따른 훈련 지침의 내용을 적절히 반영될 수 없는 구조로 생각되고 있다.

이에 본 논문에서는, 원자력시설 사이버보안 훈련의 수준을 제고하기 위해서 CSP 수준의 정책이 개발될 필요가 있음을 관련 문헌조사를 통해 뒷받침하고, 이에 대한 구체적인 방안에 대해 논의하고자 한다.

2. 원자력시설 사이버보안 훈련 규제체계 현황

동법 제 9 조의 3(물리적방호 훈련) 및 원자력안전위원회 고시 제 2017-1 호에 따라 원자력시설은 물리적방호 훈련의 일환으로 사이버보안 훈련을 실시하도록 요구받고 있으며, 이에 따라 국내 원자력시설은 2016 년부터 현재까지 각 시설별로 연 3 회(전체훈련 1 회/부분훈련 2 회)의 훈련을 수행하고 있다. 각 원자력시설은 훈련을 실시하기 위해 연간훈련계획 및 훈련 세부계획을 수립하여 원자력안전위원회의 승인을 받은 뒤 실시하여야 한다. 관련 법령간의 상관관계를 도식화하면 아래 그림과 같다.

(그림 1) 방사능방재법에 따른 사이버보안 훈련 관련 법령

3. 원자력시설 사이버보안 훈련 정책 현황

3.1 원자력시설 사이버보안 훈련 정책의 정의

행정학사전[2]에 따르면 정책이란 "공공문제를 해결고자 정부에 의해 결정된 행동방침을 말하며, 법률·정부방침·정책지침·결의와 같이 여러 형태로 표현" 되며 "합법적 강제력을 수반하는 권위가 부여되고 이에 따르지 않을 경우 벌금·제재 등의 조치"를 받는 것을 의미한다.

방사능방재법 제 9 조(물리적방호에 대한 원자력사업자의 책임)에 따라 원자력사업자는 CSP 를 수립하여 이를 원자력안전위원회(정부)의 승인을 받아야 한다. 승인받은 CSP 를 위반하였을 경우 동법 제 12 조(검사) 제2항에 따라 정부는 시정을 명할 수 있다. 마지막으로 동법 제 50 조(벌칙)에 따라 정부는 검사에 따른 시정 명령을 위반할 경우 1년 이하의 징역 또는 1천만원 이하의 벌금을 부과할 수 있다.

이러한 법률구조를 종합할 때, 원자력시설의 CSP 는 행정학사전에서 정의하는 정책의 조건을 충족한다고 볼 수 있다.

3.2 원자력시설 사이버보안 훈련 정책 현황

원자력안전위원회 고시 제 2017-51 호(물리적방호규정 등의 작성내용의 항목별 세부작성기준) 별표 4(정보시스템 보안규정의 세부작성기준)은 원자력사업자의 CSP 가 작성되어야 할 세부기준을 제시한다. 동 고시의 “전자적 침해행위에 대한 원자력시설 컴퓨터 및 정보시스템 대응조치계획에 관한 사항”에서는 본 논문에서 다루고자 하는 사이버사건 대응과 관련한 교육 및 훈련에 관한 사항을 기술하도록 명시하고 있다.

이러한 요건은 KINAC/RS-015 부록 2 에 근거하여 수립된 원자력시설별 CSP 에 반영되어 있다. 따라서 현재 원자력시설은 사이버사건 대응을 위한 최소한의 정책이 존재한다고 볼 수 있다. 원자력시설별 CSP 수립 시 참조된 KINAC/RS-015 의 해당 대목은 아래와 같다.

3.3 교육 및 훈련에 관한 사항

3.3.1 교육 및 훈련

3.3.1.1 비상사건 대응 훈련

(원자력사업자)는 비상사건대응 교육 및 훈련과 관련하여 다음을 이행한다

가. 사이버공격 비상사건대응 인력에 대하여 주기적으로 교육 제공

나. 개발된 비상사건대응 절차 및 가상 시나리오를 기반으로 원자력시설 운영에 영향을 주지 않은 범위 내에서 주기적인(최소 년 1 회 이상) 모의 훈련 실시(비공지 훈련 포함)

다. 교육훈련 결과에 대한 문서화

3.3.1.2 비상 복구계획 점검 및 훈련

(원자력사업자)는 다음이 수행되도록 보장한다.

가. 비상복구계획에 대한 주기적 점검 및 훈련(최소 년 1 회 이상)을 통해 효과성 입증

나. 훈련을 실제 백업될 장소에서 수행하여 관련자로 하여금 그러한 상황에 익숙해 질 수 있도록 하며, 해당 장소가 비상 복구계획을 지원할 능력을 갖추었는지 확인

다. 훈련은 미리 설정된 실제 발생될 수 있는 현실적인 시나리오를 기반으로 수행

라. 훈련 시 필수디지털자산에 대한 복구 및 재구성 포함

마. 점검 및 훈련 결과를 검토하여 보완사항에 대한 적절한 조치 이행 및 비상 복구계획 개정

바. 비상 복구계획 훈련이 필수디지털자산 본래의 SSEP 기능 성능 및 신뢰성에 악영향을 미쳐 수행이 불가할 경우에는 다른 대안적인 대책 수립

사. 계획예방정비 기간 등을 활용하여 비상 복구계획에 대한 점검 및 훈련 수행 가능

(그림 2) KINAC/RS-015 의 전자적 침해행위에 대한 원자력시설 컴퓨터 및 정보시스템 대응조치계획에 관한 사항 중 사이버사건대응 교육 및 훈련에 관한 사항

4. 국내·외 기준에 따른 사이버 훈련 정책 요구사항

4.1 KINAC/RS-015 비상사건 대응에 관한 사항

KINAC/RS-015 2.3(비상사건 대응 및 복구)에 따르면 원자력사업자는 비상사건에 대응하기 위한 목적, 범위, 역할, 책임 및 관리적인 사항을 기술하는 비상사건 대응 정책을 개발해야 한다. 이는 사이버 비상사건에 대한 훈련에 관한 사항을 포함하기 때문에 사이버보안 훈련에 대한 원자력사업자의 상위 문서에 해당한다. 따라서, 이러한 요구사항은 훈련에 관한 정책의 필요성을 언급하고 있는 것으로 간주될 수 있다.

4.2 美 국립표준기술연구소(NIST) SP 800-84

미 국립표준기술연구소 표준문서인 NIST SP 800-84 [3]는 기관의 사이버사건대응을 위한 IT 전략 계획에 대한 가이드를 제공하는 문서이다. 본 문서에서는 종합적인 교육 및 훈련에 대한 정책을 개발할 것을 명시하고 있으며, 정책 항목으로 제안하는 사항은 아래와 같다.

- 목적
- 유효일자

- 달성하고자 하는 목표들
- 적용 대상 및 범위
- 관련 법령 및 규제요건
- 책임 조직 및 담당자
- 훈련 정책 요구사항
- 훈련 정책에 대한 검토 및 승인

4.3 美 국토안보부의 훈련 평가 프로그램(HSEEP)

미국 국토안보부(DHS)의 국토안보훈련 및 평가 프로그램(Homeland Security and Evaluation Program, HSEEP)[4]는 미국의 9.11 테러 이후 발간된 지침 및 가이드 성격의 문서로 다양한 비상대응분야(재난, 테러, 사이버공격 등)에서 적용 가능한 훈련 설계, 실시 및 평가에 대한 기준을 제시한다.

HSEEP 는 가장 먼저 훈련 프로그램 관리(program management)에 관한 사항을 다룬다. 여기서 "프로그램"이라 함은 특정 장기목표에 대한 체계화된 행동/조치들을 의미하며, 따라서 훈련 프로그램은 훈련의 계획, 수행 및 평가에 대한 일관된 접근방법을 뜻한다.

훈련 프로그램 관리는 훈련 프로그램 중점사항(priorities)들이 달성되도록 중점사항 그 자체를 식별하고, 필요한 자원을 배분하고, 훈련이 지속되기 위한 조직/부처/기관을 통합하는 활동을 의미한다. 이를 통해 일련의 훈련활동을 지속적으로 감독하고 중점사항을 일관성 있게 추구해 나가는 것을 보장한다. 이에 따라 훈련 프로그램 중점사항 역시 훈련의 정책에 반영되어야 할 중요한 요소로 간주될 수 있다.

또한, HSEEP 를 통해 제시되는 훈련의 유형에 관한 정의는 대표적으로 훈련 정책에 포함되어야 할 요소로 볼 수 있다. 현행 사이버보안 훈련의 경우, 훈련을 실시하는 방법 및 종류에 대한 기준이 모호한 반면, HSEEP 에 근거한 훈련 유형 분류체계는 향후 훈련의 실시 목적에 적합한 형태의 훈련을 수행할 수 있는 근거로 활용될 수 있을 것이다.

NIST SP 800-84 와 HSEEP 에 따른 훈련의 유형 분류 체계를 종합하면 아래 그림과 같이 표현할 수 있다.

(그림 3) NIST SP 800-84 및 DHS HSEEP 에 따른 사이버보안 훈련 유형분류 체계[5]

5. 상세 규제방안

5.1 CSP 개정을 통한 사이버보안 훈련 정책 개선

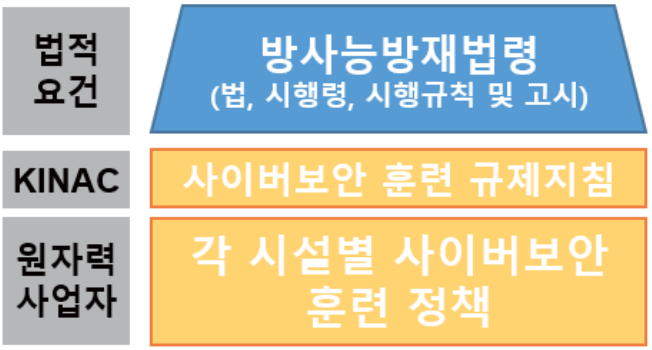
원자력사업자의 사이버보안 이행 활동의 최상위 문서가 되는 CSP 개정을 통해 훈련 정책을 수립할 수 있다. 물리적방호의 관점에서 원자력시설 규정 중 방사능방재법상 CSP 에 상응하는 규정인 "원자력시설 등의 물리적방호를 위한 규정"에 따르면 물리적방호 교육 및 훈련과 관한 사항의 기술이 관련 훈련 고시와 연동되어 전체훈련 및 부분훈련의 실시에 관하여 적시되어 있다.

이러한 사례를 참조할 때, CSP 의 "전자적 침해행위에 대한 원자력시설 컴퓨터 및 정보시스템 대응조치계획에 관한 사항" 에 따른 교육 및 훈련에 관한 사항에서도, 해당 훈련이 방사능방재법 및 관련 고시에 따라 수행한다는 기술이 필요하다.

또한, 해당 규제요건을 만족시키기 위한 훈련의 실시 유형에 대하여 본 논문에서 제시한 바와 같이 NIST SP 800-84 및 HSEEP 에 따른 다양한 형태의 훈련 형태에 대해 정의하는 것이 필요하다.

기타 NIST SP 800-84 및 HSEEP 에 따른 훈련 정책의 주요 요소(정책 수립 과정에서 중견 간부의 참여 보장, 훈련의 중점사항(priorities) 등)에 대해서도 CSP 에 반영되어야 할 것이다.

이러한 CSP 의 개정방안은 결국 개정방향과 그 내용에 대한 규제지침을 제공하는 사이버보안 훈련 규제지침의 필요성을 역설한다. 규제기관은 현행 관련 규제요건 및 KINAC/RS-015 의 내용을 보다 상세화 및 보충하는 수준의 규제지침을 개발하여 본 논문에서 제안하는 바와 같이 국내·외 기준에 따른 사이버보안 훈련에 관한 정책을 수립하는 기준을 제시해야 할 것이다. 관련 법령체계와 연계된 규제 개선방안은 아래 그림과 같이 도식화 할 수 있다.

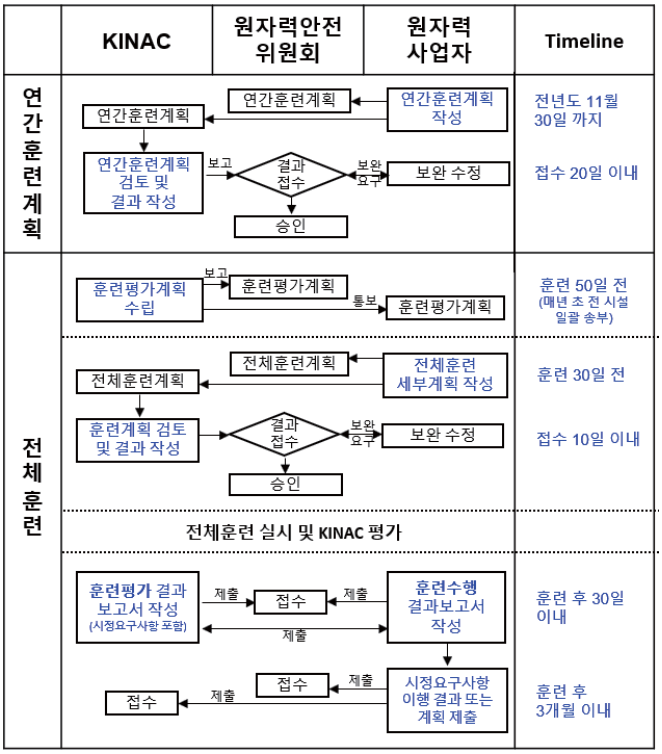


(그림 4) 사이버보안 훈련 규제요건에 따른 규제지침 및 시설 별 사이버보안 훈련 정책의 관계도

5.2 연간훈련계획 심사를 통한 사업자 정책 수립 유도

사이버보안 훈련 정책의 요소 중 시설 규정에 반영되기 어려운 수준의 정책이 존재할 수 있다. 예를 들어 정기 인사를 통해 바뀔 수 있는 정책 담당자, 또는 보다 단기간에 달성하고자 하는 정책 등의 경우에는 관련 규제기관의 승인을 받아야하는 사업자 규정이 아닌 주기적으로 갱신되는 문서를 통해 구현하는 것이 바람직할 것이다.

현 사이버보안 훈련 규제 체계에는 이러한 성격의 문서로 사이버보안 연간훈련계획이 존재한다. 연간훈련계획은 전년도 11 월 말까지 관련 규제기관에 제출되어 심사 및 승인을 받는 원자력시설의 당해년도 훈련계획에 관한 사항으로 매년 변동될 수 있는 성격의 정책을 기술하기에 적합하다. 연간훈련계획을 통해 구현된 정책은 각 부분/전체훈련 세부계획 심사 및 훈련 평가를 통해 그 이행여부가 점검될 것이다. 이러한 사이버보안 훈련 수행과 관련된 규제 절차는 사무편람[1]에 기술되어 있으며, 이를 도식화하면 아래 그림과 같다



(그림 5) 원자력시설별 연간훈련계획 및 전체훈련 세부계획에 대한 심사 및 훈련평가 절차도

6. 결론

정보보안 및 사이버보안에 있어서 정책을 수립하고 이를 이행하는 것은 조직의 보안 관점에서의 목표를 지속적으로 달성하는데 중요한 요소이다. 본 논문에서는 원자력시설 사이버보안 훈련 분야에 대해서 기존 규제체계하에서 수행된 노력들을 살펴보고, 훈련 정책의 개선이 필요함을 진단하였으며, 그 개선방안으로 정보시스템 보안규정(CSP) 차원의 훈련 정책 및 연간훈련계획의 보완을 통한 정책의 수립을 제시하였다. 또한, 수립될 훈련 정책에 들어갈 요소들에 대해서도 국내·외 기준을 근거로 열거하였다.

사이버보안 사건대응훈련은 일반적인 조직에서 사이버사건대응 계획의 일환으로 사건대응조직 구성원의 역량을 제고하기 위해 실시되는 활동이다. 이에 따라, 사이버보안 훈련 정책은 결과적으로 사이버사건대응 정책의 한 부분으로 자리잡을 수 있으며, 이는 실제 KINAC/RS-015 에서 제시하는 바와 일치한다. 본 논문에서 제시하는 사이버보안 훈련 정책의 개선 활동은 연관된 사이버보안분야 정책의 수립 및 개선에 파급되어 전반적인 원자력시설 사이버보안 체계가 개선되는 것이 바람직 할 것이다.

참고문헌

[1] "원자력시설의 컴퓨터 및 정보시스템 보안 (KINAC/RS-015)", 한국원자력통제기술원, 2016.

[2] 하동석 외 1 인, “이해하기 쉽게 쓴 행정학용어사전”, 새정보미디어, 2010.

[3] Tim Grance et al., “Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities”, NIST, 2006

[4] "Homeland Security Exercise and Evaluation Program (HSEEP)." US Department of Homeland Security, 2013.

[5] T. Aoyama et al., "On the complexity of Cybersecurity Exercises Proportional to Preparedness", Journal of Disaster Research, Vol. 12, No.3, 1081, 2017.

[6] "원자력시설등의 물리적방호 관련 사무편람", 한국원자력통제기술원, pp.22-26, 2016.