원자력시설등의 사이버보안 훈련 평가방안 개발

김현두*, 김시원
한국원자력통제기술원, 대전광역시 유성구 유성대로 1534
*hdkim@kinac.re.kr

1. 서론

최근 전 세계적 사이버위협 및 공격발생률이 지속적으로 증가하고 있는 가운데, 특히 국가 주요기반시설인 에너지, 교통, 공공설비 등을 대상으로 한 위협 발생이 빠르게 증가하고 있다. 글로벌 IT 기업인 시스코는 13년 10월 기준 전 세계 연간 누적 사이버위협 경보 발생 건수가 12년 대비 14%나 증가했다고 보고하고 있으며, 미국 시장조사업체 포네몬 인스티튜트가 7개국을 대상으로 사이버위협 발생에 따른 피해액 범위를 조사한 결과에 따르면 산업별 연평균 피해액은 에너지 및 공공시설 관련 산업이 1,318만 달러로 가장 큰 것으로 집계되었으며, 피해액 규모가 큰 산업은 에너지, 교통 등 국가 주요기반시설 관련 산업들이 포함되었다고 한다[1][2][3].

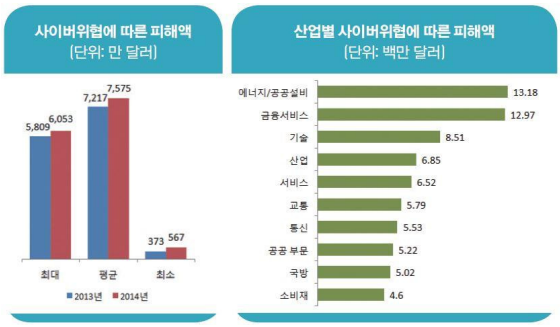

Fig. 1. The Damage of Seven Leading Industrial Nations caused by Cyber Threat[3].

그러나 정부와 기업에서는 증가하는 사이버위협을 적절히 방어·예방하는데 필요한 질적·양적인력과 대응 체계가 부족하다 판단하여, 이에 최근 해외 각국에서는 정부와 국가 주요기반시설의 사업자들은 사이버공격 대응 역량을 향상하기 위해 많은 사이버보안 훈련을 추진하고 있다[1].

2. 본론

2.1 원자력시설의 훈련에 관한 국내 법령

2014년에 개정된 원자력시설 등의 방호 및 방사능 방재 대책법(이하 '방사능방재법'), 시행규칙 및 관련 고시에서는 원자력사업자의 물리적방호(사이버보안 포함) 훈련계획 수립과 훈련의 시행 및 보고에 대해 법제화하고 원자력안전위원회에서는 이를 평가할 수 있도록 기술하고 있다.

2014년 방사능방재법령에서 훈련에 관한 사항이 개정되고 원자력사업자는 준비기간을 거쳐 2016년에 처음으로 방사능방재법령에 따른 사이버보안 훈련을 계획하였고 따라서 원자력사업자의 사이버보안 훈련을 평가하기 위한 평가표 및 평가방안 개발의 필요성이 대두되었다.

2.2 사이버보안 훈련 평가표 개발

2.2.1 평가 목표 설정

사이버보안 훈련의 목표를 훈련참가자의 교육 및 훈련, 사이버보안 비상사건에 대한 대응 기회 제공, 새로운 비상대응체계 및 절차의 필요성 확인과 기존의 비상대응체계 및 절차에 대한 평가로 설정하였다[4].

이에 따른 사이버보안 훈련 평가는 사이버보안 훈련의 목표를 달성 여부를 확인하고, 문제점을 도출하여 도출된 문제점을 체계 및 절차에 반영하고 다음 훈련에서 이를 보완할 수 있는 목표를 다음과 같이 설정하였다.

- 훈련 참가자의 개인임무 및 절차 숙지여부 확인
- 훈련에 필요한 상황/단계별 절차 존재여부 확인
- 훈련 절차의 적절성 확인

'훈련 참가자의 개인임무 및 절차 숙지여부 확인'은 훈련의 참가자가 사이버보안 비상사건 발생 시 적시에 적절한 대응을 할 수 있음을 확인하기 위해 사전에 숙지여부를 평가하고, '상황/단계별 절차 존재 확인' 및 '절차의 적절성 확인'은 사이버위협 또는 공격 시 발생할 수 있는 상황에 대응하고 피해확산방지 또는 사고완화를 하기 위한 대응절차 보유하고 있음을 확인하고 훈련을 통해 대응절차가 사이버위협이나 공격을 대응하기에 적절한지를 확인하여 원자력사업자의 사이버보안 비상사건 대응체계의 유효성을 확인하기 위함이다.

2.2.2 훈련 단계별 평가 주안점

사이버보안 훈련의 단계는 탐지, 초동대응, 비상대응조직 구성, 상황전파, 증거수집, 분석 및 제거/복구로 설정하였다[4]. 사이버보안 훈련 평가 시에는 각 단계별 적시 보고/지시 및 보고/지시 절차를 확인하기 위한 항목을 추가적으로 설정하였으며 각 평가 항목에서 반드시 확인해야 할 주안점을 아래와 같이 도출하였다.

Table 1. The keynote of exercise evaluation

훈련단계	훈련평가 주안점
탐지	적시 탐지를 위한 절차
초동대응	네트워크 격리
비상대응 조직구성	신속한 조직구성
상황전파	상황전파 기관 및 내용
증거수집	휘발성/비휘발성 데이터 수집 절차 및 도구
분석	분석의뢰 또는 분석 절차
제거/복구	피해목록 및 우선순위 선정
보고/지시	적시 보고/적절하고 명확한 지시

2.2.3 훈련 대상시스템 및 시나리오 평가

방사능방재법에 따른 사이버보안 훈련의 대상시스템은 필수디지털자산(CDA, Critical Digital Asset)으로 분류되는 제어시스템, 보안시스템 그리고 비상대응시스템에서 선정될 수 있으며 시나리오는 2015년 12월에 재설정된 설계기준위협(DBT, Design Basis Threat)내에서 작성이 되어야 한다.

이를 평가하기 위해서는 우선, 훈련 대상시스템으로 선정된 설비가 사이버위협으로 인해 발전소 운전이나 운영을 방해할 수 있는지, 단순 운전원의 혼란만을 유발하는 것인지를 확인하고 시나리오가 설계기준위협 내에서 작성이 되고 현실성이 있는지 그리고 선정된 사이버위협과 대상시스템으로 인한 사고완화와 확산방지를 위한 필요한 인원 및 조직이 모두 시나리오에 반영되었는지를 평가해야 한다.

2.2.4 실제훈련 vs 도상훈련

훈련의 목적을 최대로 달성하기 위해서는 가능한 범위 내에서 훈련의 많은 부분이 실제훈련으로 수행되고 지향되어야 하나 훈련의 여건과 상황 등을 고려하여 불가피한 경우는 일부 도상으로 진행할 수 있다.

그러나 훈련참여자의 편의 및 훈련의 간결함을 위하여 실제훈련을 수행할 수 있음에도 도상훈련으로 진행되어서는 안되므로 이를 충분히 확인하고 평가해야 한다.

3. 결론

방사능방재법에 따른 2016년 사이버보안 훈련은 방사능방재법에 의거한 최초의 사이버보안 훈련으로 원자력사업자와 많은 훈련참여자들이 사이버보안 비상대응에 대한 인식제고를 하고 미흡한 사항을 도출하는 의미있는 훈련이었다.

현재 원자력사업자는 사이버보안계획(CSP, Cyber Security Plan) 3단계에 의거하여 비상대응 절차 및 체계 구축을 진행하고 있으며, 이를 바탕으로 향후에는 설정된 훈련 평가방안 및 평가표를 개선하고 최종적으로 훈련 평가체계를 구축하여 원자력사업자가 훈련의 목표를 충분히 달성하고 사이버위협 발생 시 적시에 적절한 대응을 하여 사고를 완화하고 피해확산을 방지할 수 있도록 수준 높은 훈련을 설계하기 위한 기반이 되어야 할 것 이다.

4. 참고문헌

[1] 한국인터넷진흥원, “일본·유럽 정부, 주요 기반시설 대상 사이버보안 훈련 실시”, (2014).

[2] Cisco, “Cisco 2014 Annual Security Report”, (2014).

[3] Ponemon Institute, 2014 Global Report on the Cost of Cyber Crime, (2014).

[4] H.D.Kim, “Development on Guidance of Cyber Security Exercise for the Nuclear Facilities”, KNS, (2016).