

원자력시설 IEMI 위협 취약성 평가를 위한 시나리오 평가 방법론 개발

류진호*, 송등훈*

요 약

원자력시설 등의 방호 및 방사능 방재 대책법에 따라 2018년 개정된 설계기준위협(DBT)은 전자적 침해행위 중 하나로 의도적 전자기파 간섭(IEMI) 위협을 반영하였으며, 이에 따라 원자력시설은 IEMI 위협에 대한 물리적방호시책을 마련하여야 한다. 한국원자력통제기술원(KINAC)은 개정 설계기준위협에 따라 2018년 원자력시설의 고출력 전자기파 방호 심·검사 기준(KINAC/RS-020)을 개정하여 원자력시설의 IEMI 위협에 대한 취약성 평가 방법론을 제시하고 있다. 본 논문은 KINAC/RS-020에 따른 원자력시설 IEMI 위협 취약성 평가를 위해 개발 중인 IEMI 위협에 대한 시나리오 평가 방법론에 대해 소개한다.

I. 서 론

원자력시설 등의 방호 및 방사능 방재 대책법(이하, 방사능방재법)에 따라 정부는 원자력시설의 물리적방호 체제(전자적 침해행위에 대한 대책 포함)를 마련하여야 하며, 원자력시설은 물리적방호체제의 이행과 관련된 방호대책을 수립하도록 요구받고 있다[1]. 갈수록 고도화되고 지능화되는 공격수단의 개발 및 테러리즘의 부상을 대비하기 위해 방사능방재법 시행령 제7조는 원자력시설에 대한 신규 위협을 평가하여 물리적방호체제의 설계·평가의 기준이 되는 설계기준위협(Design Basis Threat, 이하 DBT)을 3년마다 새롭게 설정하도록 하고 있다. 이와 관련하여 최근 원자력시설에는 복핵 이슈를 기점으로 고출력 전자기파(Electromagnetic Pulse, 이하 EMP) 위협에 대한 대책의 필요성이 시급하게 제기된 바 있다. EMP 위협은 방사능방재법상 전자적 침해행위의 유형 중 한 종류로, 원자력사업자는 이와 관련한 방호대책을 마련하여야 한다. 2018년 개정된 사이버보안 분야 DBT는 고출력 전자기파 위협 중 의도적 전자기파 간섭(Intentional Electromagnetic Interference, 이하 IEMI)을 방호 대상 위협으로 설정하였다.

한편 한국원자력통제기술원 사이버보안실에서는 개정 DBT에 따른 원자력사업자의 IEMI 방호 대책 수립

을 지원하고 규제기준을 제시하기 위한 심·검사기준서 『원자력시설의 고출력 전자기파 방호』(KINAC/RS-020)를 2018년 개정하여 IEMI 방호를 위한 기준을 제시하고 원자력시설의 IEMI 위협에 대한 취약성 평가 방법을 제시하였다[2]. 또한 동 부서에서는 DBT 개정에 따른 신규 IEMI 위협에 대한 원자력시설 취약성 평가를 위해 2019년 시나리오 기반 평가를 실시하여 완료할 예정이다. 이에 본고에서는 원자력시설의 IEMI 위협에 대한 취약성 평가에 활용할 수 있는 시나리오 평가 방법론을 소개하고자 한다. 이를 위해, 먼저 시나리오 평가를 통한 시설의 위협에 대한 취약성 평가와 방사능방재법 제4조에 따른 “물리적방호체제의 수립”과의 상관관계를 동법 시행령 제7조와 관련된 위협평가 체계를 통해 살펴볼 필요가 있다.

II. 원자력시설 위협평가 체계

원자력시설의 물리적방호체제(사이버보안분야 포함)의 수립을 위해 가장 중심이 되는 일은 방사능방재법 시행령 제7조에 따른 DBT의 설정이다. 매 3년마다 개정되어야 하는 사이버보안 분야 DBT를 위해 한국원자력통제기술원 사이버보안실에서는 위협 정보를 수집 및

본 연구는 원자력안전위원회의 재원으로 한국원자력안전재단의 지원을 받아 수행한 원자력안전연구사업의 연구결과입니다.

* 한국원자력통제기술원 (halloyu@kinac.re.kr, igiveitashot@kinac.re.kr)

분석하여 신규 DBT 설정안의 기반이 되는 위협평가서를 작성한다. 이를 토대로 신규 DBT(안)이 도출되면 방사능방재법 제6조에 따른 물리적방호협의회 의결을 통해 DBT 개정을 확정한다. DBT가 재설정 되면 개정된 DBT에 따라 원자력시설의 물리적방호체제가 적절한지 여부를 평가하여야 하고 신규 위협수준에 비해 기존의 물리적방호체제가 미흡하다면 보완하여야 한다. 이와 같이 DBT 개정에 따른 기존 물리적방호체제의 유효성을 평가하기 위해 시설의 신규 위협에 대한 취약성 평가를 수행해야 하며, 시나리오 평가 방법론은 그러한 시설 취약성 평가에 활용할 수 있다. 이러한 원자력시설의 3개년에 걸친 위협평가 체계는 아래 그림 1과 같이 요약할 수 있다.



(그림 1) 원자력시설 위협평가 체계 개념도

Ⅲ. 시나리오 기반 IEMI 취약성 평가 방법론

개정 DBT에 따라 IEMI 위협이 원자력시설이 방호해야 할 위협으로 설정되었으며, KINAC/RS-020에 따라 IEMI 위협에 대한 방호기준은 DBT에 정의된 최대 위협세기로 설정되었다. 또한, 동 심·검사기준서에 따라 IEMI 위협을 방호해야 하는 원자력시설은 핵물질을 사용·저장하는 시설로, 여러 종류의 원자력시설 중에서도 특정 원자력시설들에 한해서 IEMI 위협에 대한 취약성 평가가 이루어지게 되었다. 이는 원자력시설별로 유효한 위협이 차등적으로 고려된 결과이다. 이 때, 핵물질이라 함은 방사능방재법 시행령 별표1에 따르는 법령 용어로, 모든 방사성물질이 해당하는 것이 아닌 ²³⁵U, ²³⁸Pu 등 특정 방사성물질에 그 정의가 한정된다.

이상적으로 원자력시설의 신규 DBT에 따른 IEMI 위협에 대한 취약성을 평가하기 위해서는 DBT에 정의된 공격속성을 활용하여 가능한 모든 공격조합에 대해

시나리오를 평가해야 한다. 그러나, 이와 같은 방법을 구현하기란 매우 어려우므로 DBT의 공격속성을 활용하여 발생가능성과 개연성이 비교적 높으며 원자력시설의 방호 대책이 가장 취약한 대상에의 공격을 가정하는 공격시나리오를 통해 취약성을 평가하는 것이 보다 현실적인 방안이다. 이를 위해서 공격시나리오는 단순히 DBT의 공격속성을 이용한 무작위의 대상에 대한 공격이 아닌, 기존의 물리적방호체제를 고려했을 때 가장 취약할 것으로 예상되는 대상을 선정하여야 한다. 또한, 해당 시나리오의 취약성 평가 관점에서 타당성을 입증하기 위해 방호구역에서 공격대상까지의 가장 취약경로를 식별하고 해당 경로 상 배치된 격실의 현황과 건설 자재 적용 현황 등 근거 자료가 문서화 되어야 한다.

Ⅳ. 공격시나리오 작성 및 평가 방법론

4.1. 공격대상 선정 및 평가

방사능방재법에 따라 마련되는 방호대책의 목적은 핵물질의 불법이전(이하, 불법이전)과 원자력시설등의 사보타주(이하, 사보타주)를 방지하는 것이다. 이에 따라 원자력시설의 IEMI 위협에 대한 공격시나리오는 불법이전과 사보타주 각각을 목적으로 하는 공격에 대해 작성되어야 한다. IEMI 위협이 달성하고자 하는 목적에 따라 공격대상이 달라질 수 있다. 불법이전의 경우 공격대상 시스템은 KINAC/RS-020 2.4.2.1.3에 따른 ‘핵물질의 불법이전 방호를 위한 보안기능’을 수행하는 시스템이다. 사보타주의 경우 공격대상 시스템은 KINAC/RS-020 2.4.1.1.1~2.4.2.1.2에 따른 ‘원자로 정지 및 안전정지 상태 유지기능’과 ‘방사성물질 배출 또는 방사선 노출 방호기능’을 수행하는 시스템이다. 공격대상의 선정은 이와 같은 요건을 만족시켜야 하며, 선정의 적절성을 아래 표 1과 같은 항목들을 통해 종합적으로 평가할 수 있다.

(표 1) 공격대상 선정 평가항목

평가항목 대분류	평가항목 소분류
공격대상의 선정	공격 대상 시스템 개요
	물리적 위치
	수행 기능
	H/W 및 필수 S/W 현황
	공격에 따른 악영향

4.2. 공격시나리오 작성 및 평가

IEMI 위협의 공격 대상이 결정되면 공격을 위한 현실적이고 구체적인 시나리오가 작성되어야 한다. 원자력시설 중 핵물질이 있는 시설의 경우 방사능방재법 시행령 별표 2에 따른 방호요건에 따른 방호구역 지정하여 관리한다. IEMI 위협에 대한 취약성 평가를 수행해야 하는 시설은 모두 II등급 또는 III등급 방호구역을 관리하는 시설로, 방호구역에 대한 물리적방호 관점의 접근 통제, 검색, 탐지 및 판정 기준이 적용되고 있다. 따라서, 휴대용 IEMI 장비에 대해서 방호구역 내로 진입하는 공격시나리오는 물리적방호 측면에서의 공격시나리오와 결합하지 않는 한 방호구역 출입 과정에서의 탐지 및 공격 시도가 가장 가능성이 높은 공격시나리오로 간주될 수 있다.

위 사항을 고려하여 작성된 공격시나리오는 아래 표 2와 같은 항목들에 대해 적절성 여부를 평가할 수 있다.

[표 2] 공격시나리오 평가 항목

평가항목 대분류	평가항목 소분류
공격시나리오에 대한 세부사항	공격의 목적
	공격 인원(내·외부자 위협 포함)
	공격까지의 침투 시점, 경로
	공격수단

V. 방호시나리오 작성 및 평가 방법론

5.1. 불법이전 방호시나리오의 작성 및 평가

방호시나리오는 각 공격시나리오에 따라 작성되어야 한다. IEMI 위협은 전자적 침해행위의 한 종류로, 원자력시설에서의 대응은 각 시설의 사이버사건 비상대응계획 지침에 따라 수행하게 된다. 이때, 불법이전 위협에 대해서는 방호구역 외곽에 위치한 공격대상 설비의 위치 특성 상 IEMI 공격을 통해 설비의 영구적 손상을 초래할 수 있음이 고려되어야 한다.

위 사항을 고려하여 작성된 방호시나리오의 적절성 평가는 원자력시설 사이버보안 훈련 평가 방법론의 사항을 준용하여 실시할 수 있다. 사이버보안 훈련 평가는 전자적 침해행위에 대한 원자력사업자의 사이버보안 사전대응지침서에 따른 대응활동을 “예방→탐지→대응→복구”의 4단계로 구분하여, 각 단계별 활동의 적절성

[표 3] 방호시나리오 평가 항목(불법이전)

탐지	- IEMI 위협에 의한 공격 대상 시스템의 피해 상황 기술
	- 공격 대상 시스템의 고장 분석을 통한 IEMI 공격 판정내용 기술
대응	- IEMI 공격에 따른 초동조치 내용 기술
	- IEMI 공격에 따른 대응을 위해 관련 부서 및 유관기관 전파, 비상대응조직 구성에 대한 내용 기술
	- 공격 대상 시스템의 복구 전까지 기능 보안을 위한 대응조치 기술
복구	- 공격 대상 시스템의 기능 복구를 위한 조치 및 대체 품에 대한 기술
	- 복구 완료 후 정상 기능 회복 확인 및 상황전파 내용 기술

여부를 세부 평가항목에 따라 수행하는 활동이다.

불법이전의 경우 공격대상 설비에 영구적인 피해를 주는 것이 가능하기 때문에 “탐지 → 대응 → 복구” 단계에 평가의 주안을 둔다. 이에 대한 세부 평가항목은 아래의 표 3과 같다.

5.2. 사보타주 방호시나리오의 작성 및 평가

사보타주 위협에 대해서는 휴대용 IEMI 장비가 출입통제 과정에서 탐지되어 공격대상과 IEMI 장비 간 이격거리를 가능한 먼 상태로 유지하는데 주안점을 두어야 한다. 사보타주의 경우 물리적방호체제를 통해 방호구역 출입통제 과정에서 휴대용 IEMI 장비를 탐지하

[표 4] 방호시나리오 평가 항목(사보타주)

예방	- 방호구역 출입구에서 최취약지점에 위치한 공격 대상 시스템까지의 IEMI 방호 현황
	- 방호구역 진입 전 IEMI 위협을 차단하기 위한 물리적방호체제의 구축 현황
탐지	- 공격자가 IEMI 장비를 소지한 채 방호구역 통과 시도 시 검문검색에 대한 상세 내용
	- 물리적방호 담당 인력의 검문검색을 통해 IEMI 장비를 탐지한 내용에 대한 기술
	- IEMI 장비에 대한 탐지 이후 공격자가 IEMI 장비를 작동시킨 상황에 대한 탐지 여부 확인
대응	- 공격 대상 시스템에 대한 IEMI 공격에 따른 초동조치 기술
	- IEMI 공격에 따른 대응을 위해 관련 부서 및 유관기관 전파, 비상대응조직 구성에 대한 내용 기술
	- 공격 대상 시스템에 대한 정상 동작여부 확인 및 상황 전파내용 기술

는 것을 목표로 “예방 → 탐지 → 대응”의 단계에 주안점을 둔다. 이와 같이 사보타주 위협에 대한 방호시나리오의 평가는 아래 표 4와 같이 요약할 수 있다.

VI. 결 론

전자적 침해행위에 대한 원자력시설의 취약성 평가는 시설의 규모와 시설을 구성하는 계통·기기의 복잡도가 높아 고려해야할 요소들이 매우 많은 문제이다. 본고에서는 방사능방재법에 따른 원자력시설의 전자적 침해행위에 대한 방호와 관련하여 IEMI 위협에 대한 원자력시설의 취약성 평가를 위해 활용할 수 있는 시나리오 기반 취약성 평가 방법론을 소개하였다. 본 방호를 통해 원자력시설의 IEMI 위협에 대한 방호 능력의 적절성과 방호에 추가적으로 필요한 대책 적용여부를 가늠할 수 있을 것으로 기대한다.

참 고 문 헌

- [1] 한국원자력통제기술원, “원자력시설 등의 방호 및 방사능 방재 대책 법령집”, pp. 2-6, 2017.
- [2] 한국원자력통제기술원 “원자력시설의 고출력 전자기파 방호(KINAC/RS-020)” pp. 13, 2018.

<저 자 소 개 >

류 진 호 (Jinho Ryu)

정회원

2015년 8월 : 서울대학교 원자핵공학과 졸업

2017년 8월 : 서울대학교 에너지시스템공학부 석사

2017년 8월~현재 : 한국원자력통제기술원 사이버보안실 연구원



<관심분야> 해체원전 사이버보안, EMP 방호

송 동 훈 (SONG DONG HOON)

정회원

2012년 2월 : 부산대학교 전자전기공학부 졸업

2012년 1월~2015년 8월 : 한국전력기술 기술원

2015년 8월~현재 : 한국원자력통제기술원 사이버보안실 선임연구원



<관심분야> 사이버보안, EMP 방호