원자력시설, 위협에 대비하고 있나
핵안보의 현황과 과제

포커스

2014년 12월, 'Who am I'라고 밝힌 한 해커(또는 그룹)가 원자력발전소를 해킹했다며 100억 달러를 요구했다. 원자력발전소(원전)를 운영하는 한국수력원자력(이하 한수원)은 업무용 네트워크에 해킹 시도가 있었던 것이라고 밝혔지만, 국민들은 원자력발전소 가동을 조작할 수도 있지 않을까 우려했다. 한수원의 설명 후에도 해커는 원자력발전소의 설계 도면까지 공개하면서 원전 제어시스템을 파괴하겠다고 협박해 국민들의 불안감을 부추겼다. 우리 정부와 관련기관들은 상황을 확인하고 원전 제어시스템에 대한 공격은 불가능하다고 판단했지만, 만에 하나 있을지 모르는 공격에 대비하면서 비상대기 태세를 유지했고, 그 해 12월은 악몽이 되었다. 대한민국의 12월을 발칵 뒤집어 놓은 원전 해킹 사건은 3개월 후 정부합동수사단의 발표로 전모가 밝혀지며 막을 내렸다.

정부합동수사단은 이 원전 해킹 사건이 사회불안을 야기하고 국민들의 불안심리를 자극하기 위한 사건이라고 판단했다. 유출됐다고 공개된 자료는 교육용 자료나 오래 전 문서로 원전 관리에 있어 중요한 자료는 아니라고 밝혔다. 한수원의 협력업체 등 관계자 이메일에 보관되어 있던 자료였고, 이메일을 통한 악성코드로 인해 자료유출이 이루어 졌다는 것이 확인되었다. 제어시스템 해킹은 없었고 원전은 안정적으로 운영되었으나 이 사건으로 원자력시설 사이버보안에 대한 경각심이 높아졌다. 이에 사이버보안 분야 인력과 예산과 확충되고 사이버보안 강화가 이루어졌다. 그로부터 수년이 흐른 2020년, 원자력 사이버보안은 어떤 수준일까?

해킹 사건 이후 본격적으로 사이버보안 강화

해킹 사건 이전에도 원자력안전위원회와 한국원자력통제기술원(KINAC)은 사이버보안의 중요성을 인지하고 있었다. KINAC은 2011년 말부터 일부 원자력시설을 대상으로 선제적으로 사이버보안 검사를 시행했다. 원자력안전위원회(원안위)는 2013년과 2014년에 걸쳐 관련 법령을 개정함으로써 원자력시설 사이버보안 규제에 대한 근거를 마련했다. 원안위와 KINAC은 2015년부터 사이버보안 규제를 본격적으로 추진했다.

KINAC은 검사를 통해 원전의 사이버보안 현황을 확인한다.
출처: KINAC.

선제적인 조치는 이미 전 세계적으로 사이버보안의 중요성이 높아지고 있었기 때문에 시행한 것이다. 또한 원전처럼 인터넷망과 분리되어 폐쇄적으로 운영되는 산업제어시스템에 대해서도 보안을 강화해야 한다는 분위기가 형성되어 있었다. 계기는 2010년대 초에 발생한 스턱스넷 사건이다. 이란의 나탄즈 우라늄 농축 시설이 악성코드 '스턱스넷'에 감염돼 1,000여대의 원심분리기가 파괴된 것이다. 이로서 폐쇄망도 공격받을 수 있고, 사이버공격으로 물리적인 파괴가 가능하다는 것이 확인되었다.

이후 전 세계적으로 국가기반시설과 산업제어시스템까지 사이버보안을 굳건히 해야 한다는 경각심이 높아졌다. 국제원자력기구(IAEA)는 사이버보안 지침서를 발행하고 원자력시설에 사이버보안을 이행해야 한다고 밝혔다. 특히 규제기관은 원자력 사업자가 사이버보안에 관련한 법적 의무 사항을 정확하게 이해하고 이행할 수 있는 수단으로 기준과 지침 등을 제공해야 한다고 권고했다.

국가기반시설인 원자력발전소는 높은 수준의 사이버보안을 요구한다. KINAC은 원자력시설의 사건, 사고 등 방사선적 영향을 초래하는 것을 방지하기 위해 제어·감시 설비에 대한 사이버보안 수준을 정의하고 기술기준을 제시했다. 이에 따라 각 원자력시설은 스스로의 환경에 적합한 사이버보안 강화 계획을 수립했다. 해당 계획은 2015년 4월 KINAC 검토를 거쳐 원안위 승인을 받았다.

각 원자력시설은 승인된 계획에 따라 사이버보안 체계를 정비했다. KINAC은 시설별 사이버보안 이행 현황을 점검하기 위해 2015년 9월부터 2019년말까지 7단계에 걸쳐 단계적으로 특별검사를 시행했다. 운영 조직과 분리된 독립적 사이버보안 전담 조직 구성, 디지털자산 평가, 보안등급별 보안전략, 보안조치 이행 등 세부사항을 점검했다. 특별검사 결과 미흡한 사항이 있을 경우 원안위가 시정조치를 요구하여 개선토록 하였다. 2020년 현재 특별검사에 따른 조치 결과를 확인중이며 2021년까지 개선조치를 완료할 예정이다.

사이버보안 체계 구축과 점검을 통해 충분한 보안 수준을 유지하도록 하는 한편, 위협이 발생할 경우에 대비해 훈련을 시행하고 있다. KINAC은 주기적인 훈련 평가를 통해 개선사항을 도출하고 비상시 대응 능력을 강화해 나가고 있다. 그 결과 국제원자력기구(IAEA)로부터 사이버보안 국제 교육훈련과정을 주관할 역량을 갖춘 국가(기관)로 인정받았다. 실제로 KINAC은 2019년 11월 세계 20개국의 규제기관, 원자력 시설, 정부 관계자를 대상으로 국제훈련과정을 성공적으로 개최한 바 있다. 또한 우리나라의 사이버보안 훈련평가 프로그램은 IAEA에서 우수사례로 꼽으며 국제사회에서 선도적인 것으로 평가받고 있다.

사이버보안의 최신 과제, EMP 대응

최근 사이버보안 분야의 이슈는 EMP(Electro Magnetic Pulse) 대응이다. EMP는 높은 상공에서의 핵폭발 또는 전자기 발생장치에 의해 발생되는 순간적인 고출력 전자기파로 전자장비의 정지나 오작동을 유발할 수 있다. 이에 우리나라도 EMP 공격으로부터 원전의 안전을 지키는 것을 목표로 EMP 방호 규제를 추진하고 있다.

KINAC은 원자력안전위원회와 함께 2015년 12월부터 EMP 방호 규제의 법적 근거를 마련하였고, 국내 원전에 방호대책 마련을 요청했다. 이에 한수원은 우선 EMP로 인한 원전의 영향을 평가하여 그 결과를 KINAC에 제출하였다. KINAC은 평가 결과에 대한 검증을 진행 중이며 2021년까지 완료할 예정이다. 또한 EMP 방호 대책의 적합성을 평가하여 EMP 공격 시에도 원전의 안전기능을 보장할 수 있도록 규제할 계획이다.

EMP 공격을 보여주는 가상 이미지. 출처: PapaLegba 유튜브

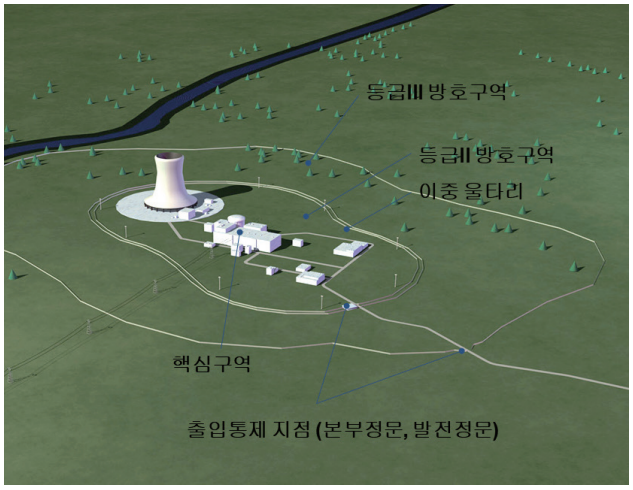
이에 앞서 2017년 KINAC은 원전의 EMP 방호 기술기준을 제정하고, 원전 외 연구용 원자로, 방사성폐기물 처분 시설 등 기타 원자력시설에 대해서도 심사·검사 시 EMP 방호 규제를 포함하도록 기술기준을 개정했다. 또한 원자력시설의 EMP 방호 규제 방법론 개발을 위한 연구를 수행하고 있다. 이와 더불어 위협·대응 시나리오 평가 결과에 따른 시정조치를 통해 시설별로 보완하면서 EMP 방호 규제 체계를 완성해 나가고 있다.

한편 원전 운영 시 사이버 공격으로 인한 영향을 검증하고 사고로의 확산을 막기 위해 다양한 시험이 필요하다. 그러나 원전에 직접 시험할 수 없으므로 KINAC은 테스트베드를 구축해 그 영향을 평가하고자 한다. KINAC은 2021년부터 2022년까지 사이버보안 테스트베드를 원전 사이버 공격 예방을 위한 규제요건과 검증기술을 개발할 예정이다.

핵물질과 원자력시설 위협에 대응하는 모든 조치, 물리적방호

원자력시설에 대한 위협은 물리적으로도 존재한다. 영화에서 흔히 등장하는 핵무기 탈취와 테러처럼, 원자력시설이 보유한 핵물질을 탈취해 핵 테러를 일으킬 가능성도 있다. 따라서 이러한 위험을 초래하지 않도록 원자력시설과 핵물질을 방호할 필요가 있다.

예를 들어 테러 조직은 핵물질을 불법으로 탈취해 직접 핵무기를 만드는 것뿐만 아니라, 원자력시설을 공격해 방사성 물질을 유출시켜 인명, 재산, 환경에 악영향을 끼칠 수 있다. 이런 위험한 상황이 발생하지 않도록 사전에 방지하고, 위험 상황이 이미 발생했다면 이를 신속하게 탐지해 적절한 행동을 취하는 모든 조치를 물리적방호라고 한다.



원자력발전소의 물리적 방호구역 예시. 출처: KINAC

원자력발전소는 이러한 위험을 우려해 엄격한 물리적방호 체계를 갖춰야 한다. 예를 들어 핵연료는 물리적방호의 대상이 되는 중요한 핵물질로, 개인/집단에 의해 탈취되는 것을 막기 위해 관리된다. 원자력발전소 각 구역은 중요도에 따라 방호등급이 나누어지고, 등급별로 적합한 방호 수준이 설정된다. 그리고 수준에 맞게 방호울타리, CCTV, 센서 등 물리적방호 장비와 인력을 배치하고 운영한다.

물리적방호는 국가(원안위), 규제전문기관(KINAC), 원자력 사업자의 유기적 협력으로 이루어지고 있다. 사업자는 물리적방호 설비를 갖추고 인력을 배치하는 등 실질적인 역할을 하고, KINAC과 원안위는 정기적인 검사를 통해 물리적방호 수준을 만족시키는지 판단하며 필요시 시정조치를 취하도록 한다. 특히 KINAC은 물리적방호 심사 및 검사, 훈련평가 등을 이행하며 원안위의 규제 업무를 지원하고 있다. 물리적방호 수준과 대응 기준을 부여하고, 물리적방호 시설 및 설비의 성능이 적정하게 유지되고 있는지 검사하고, 시설별로 비상조직의 대응 조치 훈련을 평가하며, 물리적방호 종사자에 대한 법정교육도 담당하고 있다. 이를 통해 방호 시설 및 설비의 성능을 최상의 상태로 유지하고, 사전 예방과 비상시 적시 대응을 할 수 있도록 돕고 있는 것이다.

드론 위협에 대비하는 물리적방호 규제

KINAC은 원안위와 함께 안팎의 다양한 위협으로부터 원자력시설을 방호하기 위해 지속적으로 노력하고 있다. 최근 전 세계적으로 주목받고 있는 이슈는 드론이다. 2019년 9월 15일 사우디아라비아 정유시설에 발생한 드론 테러 이후 여론의 관심이 증가했다. 국내 원전 주변에 드론이 출몰한 경우는 2016년 1회, 2017년 2회, 2018년 0회에 그쳤으나 2019년에는 15회로 급증했다. 취미용 드론인 것으로 추정되지만

공격 수단이 될 경우를 대비하는 것이 중요하다. KINAC과 원안위는 2015년부터 드론을 신종 위협 수단으로 평가하고 불법드론에 대응하기 위한 새로운 규제를 추진하고 있다.

KINAC과 원안위는 원자력 사업자에게 물리적방호 체제 구축 시 드론 대비 조치를 포함할 것을 요구했다. 특히 드론을 탐지하고 차단하는 것이 중요함을 강조했다. 이에 사업자는 드론 발견 시 행동 요령을 수립해 드론 탐지 시 지역 군부대, 경찰서 등과 협력하고 있다. 또한 드론을 탐지하기 위한 고성능 감시장비를 설치하였고, 대응 장비를 단계적으로 도입할 계획이다. 또한 원전 상공은 항공안전법에 근거한 비행금지 구역임을 알려 실수에 의한 위반 행위가 발생하지 않도록 하고 있다.

2019년 원자력발전소에 15번의 드론이 출몰하면서 드론에 대한 우려가 높아지고 있다. 출처: shutterstock

드론에 대응하는 방법은 여러 가지가 있으나 가장 현실성 있는 방법은 전파 차단으로 알려져 있다. 원전에서 전파를 발생시키는 것은 불법인 상황이었으나 올해 전파법이 개정되면서 드론 대응용 전파 발생장치를 설치할 수 있게 되었다. 그러나 전파가 원전의 안전성에 영향을 미치지 않는지 검증이 필요하다. 이에 한수원은 드론 탐지 및 대응 설비의 원전 영향 분석을 연구하고 있으며 이후 KINAC과 원안위가 검증할 예정이다. 이와 별개로 대응 장비를 사용할 경우 대응의 범위, 권한, 배상 등에 대한 검토도 필요하다.

2020년 KINAC은 전 원전 본부에서 드론 대응을 위한 물리적방호 훈련을 실시하도록 했다. 완벽한 장비가 갖춰지기 이전이라도 드론 탐지 및 대응이 가능하도록 노력하고 있는 것이다. 한편 KINAC은 2016년과 2017년에 걸쳐 KAIST와 협력해 드론 대응방안을 연구한 바 있으며, 사업자의 이해를 돕기 위해 2017년 사업자를 대상으로 드론 비행 시연 등 드론 대응을 위한 기초 교육을 시행하기도 했다. KINAC은 앞으로도 드론 대응 능력 제고를 위해 규제와 교육을 추진해 나갈 계획이다.

사이버보안과 물리적방호를 아우르는 핵안보라는 개념은 원자력의 평화적 이용(Atoms for peace)이 장려되던 1960년대에 이미 등장했다. 핵연료로 쓰일 핵물질의 국제적인 이동이 활발해지자 이동 중인 핵물질의 불법 탈취 등의 예방조치가 강조되면서 핵안보의 중요성이 대두된 것이다. 그러나 최근 과학기술이 발달하고 변화하면서 사이버 테러와 EMP, 드론 공격 등 핵안보에 새로운 위협들이 등장하고 있다. 이러한 환경을 반영하여 KINAC은 유관기관과 협력하면서 빠르게 해당 이슈들에 대해 대처하며 핵안보를 더욱 더 강화해 나갈 것이다.

글 / 오혜진 칼럼니스트

핵안보의 중심

사이버보안과 물리적방호의 최신 이슈 대응

핵안보의 중요성 강화

- 원자력 시설 사보타주, 방사성 물질 오염, 핵 밀수, 사이버 테러 등 핵 테러 개념 확장
- 핵물질 및 방사성물질, 관련 시설에 대한 위협에 대응하기 위해 핵안보 강화

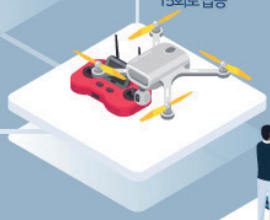
물리적방호와 사이버보안으로 핵안보 체계 구축

물리적방호

- 핵물질과 원자력시설 위협을 사전에 방지하고 위협이 발생한 경우, 이에 대응하는 모든 조치
- KINAC은 위협을 분석하고 원자력 시설이 최적의 상태를 유지하도록 심사, 검사, 훈련평가를 시행

물리적방호 최신 이슈

- 드론 위협의 현실화
- 국내 원전 인근 드론 출현 '16년 1회, '17년 2회, '18년 0회에 그쳤던 횟수가 '19년에는 15회로 급증



사이버보안

- 사이버테러로부터 원자력시설의 시스템을 보호
- KINAC은 원전 제어시스템의 보안을 위해 2015년부터 본격적으로 사이버보안 규제 시행

KINAC, 최상의 물리적방호를 위하여

- 드론 설계기준 위협 반영
- 원자력사업자 드론 대응 조치 훈련 및 평가
- 드론 대응 장비 도입에 따른 규정 변경 심사
- 장비 성능 및 안전성 영향 평가

사이버보안 최신 이슈

- 고출력 전자기 펄스(EMP) 대응
- 전자장비를 정지/오작동시키는 EMP 방호가 원전 안전과 직결

KINAC, 사이버보안 강화를 위하여

- EMP 방호 규제 법적 근거 마련
- 원자력시설의 EMP 방호 심·검사 기준 제정
- EMP 방호 규제 방법론 연구 수행
- EMP 영향평가 분석 및 대응을 위한 체계 검사
- 사이버공격에 따른 영향 분석, 사이버보안 검증 테스트베드 구축