원전 사이버 보안 강화를 위한 선행 요건

손재영
한국원자력통제기술원 원장

· 서울대 원자핵공학과 학사, 석사
· 과학기술처 원자력실 사무관, 우주항공기술과장
· 과학기술부 장관 비서관
· 외교통상부 주영 한국대사관 과학관
· 교육과학기술부 기초연구과장, 연구정책과장
· 대구경북과학기술원 건설추진단장
· 국제과학비즈니스벨트 기획단장
· 교육과학기술부 원자력안전국장
· 원자력안전위원회 사무처장

작년 연말에 발생한 소위 '원전반대그룹'의 사이버 위협이 지금까지도 계속되고 있다. 이들은 한국수력원자력의 자료를 비롯하여 각종 유관 기관들의 자료를 인터넷에 공개하며 금전적 요구를 하는 등 사이버 공간을 배경으로 국민의 불안감을 조성하고 있다.

이들이 위협의 도구로 사용하고 있는 사이버 기술은 시간과 공간의 제약을 받지 않으며 수행자의 익명성 또한 쉽게 보장하는 특성이 있다. 때문에 원전을 비롯하여 각종 중요 보안 시설과 금융 거래 시스템 등 사회 기반 시설에 사이버 테러가 발생하면 범인을 잡아내기도 힘들고 그 피해 규모 또한 쉽게 상상하기 힘들다. 우리나라를 비롯한 세계 각국이 최대 안보 위협 중 하나를 사이버 테러로 규정하고 이에 효과적으로 대응하기 위한 새로운 방안 마련에 고심하고 있는 것도 바로 이 때문이다.

원전 사이버 보안을 위한 적극적 대응

우리나라는 원전 사이버 보안이라는 측면에서 보았을 때 사이버 위협에 대한 대응책이 잘 갖추어진 국가에 속한다. 다른 분야와 달리 원전 제어 시스템은 외부 인터넷과 물리적으로 완전히 분리되어 있기 때문에 외부 접속을 통한 해킹 가능성은 사실상 희박하다.

그러나 일반적 업무 처리를 위한 시스템은 외부와 연결되어 있기 때문에 이를 통해 중요한 자료가 유출될 수 있는 가능성은 존재한다. 지금도 계속되고 있는 원전 사이버 위협이 외부 해킹에 의한 것인지는 아직도 확실하게 규명되지 않았지만 일반망 해킹을 통한 자료 유출은 가능한 것으로 드러난 만큼 이

에 대한 철저한 대비가 필요하다.

현재 원전 사이버 보안을 위한 다양한 방안들이 논의되고 있거나 이미 시행되고 있다. 관련 업무를 위탁받아 수행중인 한국원자력통제기술원은 이미 올 4월부터 발전소 현장의 사이버 규제 업무를 수행하고 있으며, 효과적인 규제 업무 수행을 위한 전담 조직 신설 및 인력 확충도 조만간 이루어질 예정이다.

이와 같은 정부의 적극적 대응은 향후 원전 사이버 위협의 재발을 막고 우리나라의 핵안보 수준을 강화할 수 있는 계기가 될 것으로 기대되고 있다.

원전 시설 관계자의 사이버 보안 의식 제고 필요

그러나 진정한 원전 사이버 보안 강화를 위해서는 이와 같은 제도적 노력 이전에 선행되어야 할 요건이 있다. 바로 원전 시설 관계자들의 철저한 사이버 보안 인식 제고다.

원전 사이버 공격의 대표적인 사례로 꼽히는 2010년 이란 나탄즈 원전의 스턱스넷 사건도 외부를 통한 해킹이 아니라 내부를 통해 제어 시스템에 악성코드가 감염되면서 발생한 사건이었다. 이 때문에 이란은 나탄즈 원전을 1년 가량 가동 중지했고 우라늄 농축 시설 원심분리기 또한 1천대 이상 교체하는 큰 피해를 입었다.

2014년 일본 몬주 원전에서 발생한 악성 코드 감염 사건도 내부 직원이 동영상 재생 소프트웨어를 업데이트한 것이 문제의 발단이었다. 이를 통해 직원들의 개인 정보와 훈련 기록 등 4만여개 이상의 문서가 유출된 것으로 알려지고 있다.

두 사건 모두 제도적 미비가 아니라 내부 직원들의 보안 인식 부재로 인해 발생한 사건이라는 공통점이 있다.

이와 같은 사건이 외국의 일만은 아니다. 우리나라도 원전 근무자가 업무의 효율성만을 중시하여 접속 자격이 없는 근무자에게 중요한 전산 기기의 아이디와 패스워드를 유출한 사건이 있었다. 다행히 직접적인 피해로 연결되지는 않았지만 해킹 등의 추가 피해를 야기할 수 있는 위험한 행위였다.

결국 제아무리 첨단의 방화벽을 설치하고 제도적 관리 방안을 마련해도 직접 업무에 종사하는 직원의 보안 의식이 없다면 갈수록 고도화되어가는 사이버 위협에 효과적으로 대응할 수 없는 것이 사실이다. 최종 운영은 결국 사람이 하는 일인 만큼 종사자들의 인식 제고가 무엇보다 선행되어야 하는 것도 바로 이 때문이다.

국제핵안보교육훈련센터(INSA)를 통한 교육 훈련

물론 사이버 보안 대응 태세 확립이 원전 종사자들의 개인적 노력만으로 확립되기는 힘들다. 지금까지 큰 문제가 없었다는 인식 때문에 상대적으로 다른 업무에 비해 우선 순위에서 밀려나 있던 관련 업무의 위상을 제도로 정립해 나가는 노력 또한 필요하다. 현재 정부에서는 이를 위해 원전 종사자의 사이버 보안 문화 정착 및 맞춤형 교육 훈련 프로그램을 추진하고 있는데 KINAC은 핵비확산 및 핵안보 인력 교육 전문 기관인 국제핵안보교육훈련센터(INSA)를 통해 이를 적극적으로 시행하여 관련 인력의 전문성 향상 및 인식 제고 노력을 지속적으로 수행해 나갈 예정이다.

이제 원전을 대상으로 한 사이버 위협은 영화나 드라마에서 자주 나오던 단골 소재에서 벗어나 언제든 우리에게 일어날 수 있는 또 하나의 현실적인 위협으로 자리잡았다. 전 세계적으로 이에 대한 대응책 마련에 부심하고 있는 지금, 이를 방지하기 위한 제도적 노력과 함께 관계자 모두의 인식과 역량 또한 제고하여 핵비확산 및 핵안보 선진국으로서의 대한민국 역량을 또 한 단계 높이는 계기가 되기를 기원한다.