산업통상자원부 MINISTRY OF TRADE, INDUSTRY & ENERGY	**공 동 보도자료**	원자력안전위원회 NUCLEAR SAFETY AND SECURITY COMMISSION
배포 즉시 보도하여 주시기 바랍니다.		
담당 부서	산업부 원전산업관리과 김영규 과장(044-203-5321), 김종연 사무관(5313)	원안위 방재환경과 이순종 과장(02-397-7354), 김성길 서기관(7352)

원전 사이버 공격, 원전 안전에는 영향 없어

- 12.22~23일 정부기관 합동으로 원전 보안 상황 정밀 재점검 -

□ 원자력 안전에 영향을 주는 원전 제어망은 사내 업무망이나 사외 인터넷 망과 완전히 분리된 단독 폐쇄망으로 구성되어 사이버 공격이 원천적으로 불가능함

○ 원전제어망은 단방향 통신으로 구성되어 인터넷망으로부터 네트워크를 통해 절대 접속할 수 없음(붙임 참고)

□ 지난 12.17일 '한수원 직원 개인정보 유출' 건 직후 한수원 자체 보안점검 결과에서도 원전 운영 안전과 관련한 문제점은 발견되지 않았음

○ 또한, 지금까지 공개된 자료는 핵심기술이 아닌 일반적 기술자료로서 원전 안전에 미치는 영향은 없는 것으로 확인된 바 있음

□ 정부는 금번 사태를 엄중하게 보고, 국가 최상급 중요 시설인 원전에 대해 이루어진 사이버 공격에 대해 검찰 차원에서 엄정한 조사와 수사가 진행 중이며,

○ 산업부, 원안위 등 관계부처 간 긴밀한 협조를 통해 대응하고 있음

① 정부는 12.19일 12시부로 사이버 위기 '관심' 경보를 발령하고, 각급기관 및 보안관제센터의 비상근무태세를 유지토록 하였으며,

* 사이버위기경보 : 국가사이버안전관리규정 제11조에 의거 사이버 공격에 대한 대응을 목적으로 '정상→관심→주의→경계→심각' 의 5단계로 발령

② 산업부는 12.20일(토) 장관이 직접 한수원과 한전기술 본사를 방문하여 사이버 공격 비상대응체제 점검 후, 한수원을 비롯한 전체 에너지 공기업들에 대해 대책회의를 통해 사이버 보안 현황을 점검하고 철저한 보안관리를 지시하였으며,

- "산업부-한수원 사이버 공격 대응 TFT(팀장:원전산업정책관)"를 구성하여 비상근무 및 세부적인 대응체제·방안을 점검하고 있음.

③ 한수원은 원안위의 유출자료 안전성 검토에 적극 협조하는 한편, 사내 모든 PC 대상 바이러스 체크와 USB 포트 봉인 등 만일의 사태에 대비한 사내 사이버 보안 경계를 강화하였음

④ 원안위는 본부, 지역사무소 및 원자력통제기술원이 비상근무 중이며, 현장확인 등을 통해 안전성을 지속적으로 확인해 나가고 있음

□ 정부는 원전 안전에는 문제가 없다는 점을 한수원의 자체점검을 통해 확인하였으나,

○ 국민들의 우려와 불안감을 없애기 위해 원안위-산업부-원자력안전기술원-원자력통제기술원-한국인터넷진흥원 등 관계부처 및 전문기관 합동으로 12.22~23 일간 고리와 월성본부에 대해 자료유출과 관련된 업무망의 보안현황 및 자료유출이 원전안전에 미치는 영향

등에 대해 전반적으로 점검할 계획임

□ 추가로 한수원은 12.22~23일간 울진(한울원전), 영광(한빛원전)을 포함한 4개 본부 전 원전을 대상으로 사이버 공격 대비 모의 훈련을 추진할 예정

○ 또한, 모의 훈련 설비를 활용하여, 실제로는 불가능할지라도 만약의 경우 원전 운전용 제어컴퓨터의 USB포트를 통한 접속이 있다할지라도 복구·회복이 가능함을 시험을 통해 재확인할 계획임

□ 정부는 엄정한 수사·조사와 함께 관계부처 합동 정밀 점검 등을 통해 추가적인 사이버 공격 가능성에 대비하고 원전 안전에 문제가 없음을 확실히 함으로써 국민들이 불안해하지 않도록 만전을 기하겠음

<붙임자료> 원자력발전소 전산시스템 망 구성도

OPEN 공공누리 공공저작물 자유이용허락

이 보도자료와 관련하여 보다 자세한 내용이나 취재를 원하시면 산업통상자원부 원전산업관리과 김종연 사무관(☎ 044-203-5313), 원자력안전위원회 방재환경과 김성길 서기관(☎ 02-397-7352)에게 연락주시기 바랍니다.