

한준호 의원
"LGU+ 침해 흔적 사라지면 피해 규모 어떻게 확인하나"

- LG유플러스, 침해 서버 증거보존 부실에 이중화 구조 KISA 사전 미고지까지
- 서버 데이터 동기화 이유로 한쪽 서버만 분석해도 된다고 판단… KISA "해커 침입 흔적까지 동일하게 복제되지는 않아"
- 한준호 의원 "증거 소실로 피해 확인 못 하면 피해는 국민 몫… 제도적 맹점 보완해야"

LG유플러스가 침해사고 조사 과정에서 이중화된 서버 구조를 조사기관에 사전에 알리지 않고, 침해 서버의 디지털 증거를 충분히 확보하지 않은 채 운영체제(OS)를 재설치한 사실이 국정감사에서 도마 위에 올랐다.

국회 과학기술정보방송통신위원회 소속 한준호 간사는 국정감사에서 LG유플러스가 서버의 이중화 구조를 한국인터넷진흥원(KISA)에 사전에 알리지 않은 경위와 침해 서버의 OS 재설치에 따른 증거 훼손 가능성을 집중 추궁했다.

한 의원이 LG유플러스로부터 제출받은 서면답변에 따르면, LG유플러스는 "두 서버가 이중화된 구조로 동기화되는 관계이기 때문에 당시에는 둘 중 하나를 이미징하면 분석이 이루어질 수 있을 것으로 판단했다"고 설명했다.

그러나 한 의원은 서버 간 데이터 동기화와 디지털 포렌식 증거의 동일성은 별개의 문제라고 지적했다. 실제 한 의원이 KISA 관계자에게 "서버 데이터가 동기화됐다고 해서 해커 침입 흔적까지 똑같이 복제되느냐"고 질의하자, KISA 관계자는 "그렇지 않습니다"라고 답변했다.

특히 LG유플러스는 침해 서버의 이미지를 확보하지 않은 상태에서 OS를 재설치한 것으로 드러났다. OS 재설치 과정에서 메모리 정보와 운영체제 기록, 악성코드 파일 등 침해 원인 규명에 필요한 핵심 증거가 소실될 수 있다는 점에서 논란이 제기됐다.

이에 한 의원은 중앙 로그의 별도 저장이나 백업 등 충분한 증거보존 조치 없이 OS를 재설치한 것은 침해 경로와 피해 규모를 규명할 핵심 증거를 훼손했을 가능성이 있다며, 이 같은 대응으로 피해 사실을 제대로 확인하지 못하게 된 것 아니냐는 의혹을 제기했다.

아울러 한 의원은 회사 귀책사유가 인정될 경우 해지 고객에 대한 위약금 면제 및 소급 환급 등 실질적인 이용자 보호조치도 요구했다. 이에 LG유플러스 대표이사는 사법당국의 판단에 따라 필요한 고객 보호조치를 이행하겠다는 입장을 밝혔으나, 구체적인 위약금 면제 및 환급 여부에 대해서는 확답하지 않았다.

한준호 의원은 “이중화된 서버의 데이터가 동기화된다는 이유로 침해 흔적까지 동일하게 보존된다고 판단하는 것은 납득하기 어렵다“며 “감염된 서버의 이미지를 확보하지 않고 OS를 재설치해 핵심 증거가 사라졌다면 침해 원인과 피해 규모를 어떻게 확인할 수 있겠느냐“고 지적했다.

이어 “증거보존 부실로 피해 사실조차 확인하지 못한다면 그 피해는 고스란히 국민들에게 돌아갈 수밖에 없다“며 “정부는 침해사고 조사 과정의 증거보존과 조사기관 협조체계에 대한 제도적 맹점을 보완하고, 이번 사안도 끝까지 점검해야 한다“고 강조했다. 〈끝〉