

의료기관 10곳 중 4곳 ‘보안관제 사각 지대’, 환자 안전과 진료 연속성 위한 대책 필요

- 보안관제 필요성 인식(88.2%) 높으나 실제 실시율은 57.0%에 그쳐...필요성에 대한 인식과 실제 대응체계 구축 간 상당한 격차 확인돼
- 종합병원 84.9% 보안인증체계 ‘0개’, 상급종합병원과의 종별 격차 심각...가장 큰 애로사항은 전문인력 및 예산 부족
- 의료기관 평가·인증 제도에 사이버 보안 항목을 단계적으로 반영하고 공동대응체계와 정례적 실태조사 강화 필요

※ 이 글의 내용은 ‘의료기관 사이버 보안 실태조사’ 결과를 토대로 한 저자의 의견이며, 한국보건사회연구원 공식 견해와 다를 수 있음. 또한 활용한 자료는 국가승인통계가 아님을 밝혀둠.

□ 한국보건사회연구원(원장 신영석)은 『보건복지 이슈엔포커스』 제475호 <의료기관 사이버 보안 현황과 정책 과제>를 발간했다. 연구책임자는 재정통계연구실 이기호 부연구위원이다.

○ 이 자료는 대한병원협회에 위탁하여 전국 17개 시도의 상급종합병원(41개소) 및 종합병원(222개소) 총 263개소를 대상으로 실시한 온라인 설문조사 결과를 바탕으로 작성됐다.

※ 보안관제 : 병원의 의료 정보 시스템과 네트워크를 24시간 365일 실시간으로 모니터링하여 사이버 공격이나 보안 위협을 탐지하고 차단하는 예방·대응 체계

□ 실태조사 결과, 국내 의료기관의 보안관제 사각지대가 존재하며 의료기관 종별 보안 역량 격차가 심각한 것으로 나타났다.

○ 상시 모니터링을 위한 핵심 수단인 보안관제의 경우, 전체 응답 기관의 43.0%가 실시하지 않고 있는 것으로 확인되었다. 종별로는 상급종합병원의 실시율이 75.6%인 반면, 종합병원은 53.6%에 그쳤다.

○ 보안인증체계 보유 수준에서도 격차가 뚜렷했다. 보안관제를 실시하는 기관 중에서도 67.3%는 외부 인증을 받은 보안관리체계가 없었다. 특히 종합병원의 84.9%는 보안인증을 전혀 보유하지 않아(0개) 지역 의료체계의 핵심 기능

을 수행함에도 보안 역량이 상대적으로 취약한 상태임이 드러났다.

- 의료기관들은 사이버 보안의 필요성을 강하게 인식하고 있으나, 비용과 인력 등 현실적 장벽에 부딪히고 있는 것으로 분석되었다.
- 보안관제가 필요하다는 응답은 88.2%에 달했으나 실제 실시율은 57.0%에 그쳐, 인식과 실행 사이에 31.2%포인트의 큰 격차가 존재했다.
- 보안관제 도입을 저해하는 가장 큰 요인은 ‘초기 구축 비용 부담’이었으며, 이어서 ‘내부 전문인력 부족’, ‘내부 기술적 지식 부족’ 순으로 나타났다.

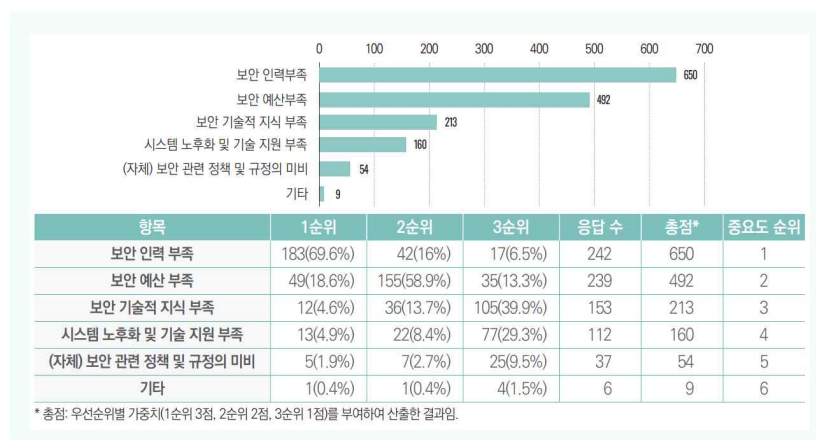
[그림 4] 보안관제체계 도입 저해 요인



출처: “의료기관 사이버 보안 개선을 위한 정책 방안 연구”, 이기호 외, 2025, 한국보건사회연구원, p. 398, 저자 재작성.

- 정보보호 업무 전반에 대한 애로사항 역시 ‘보안 인력 부족’과 ‘보안 예산 부족’이 압도적인 비중을 차지하여, 지속적인 보안관리를 수행할 수 있는 기반이 미흡함을 보여주었다.

[그림 5] 정보보안 업무 관련 애로 사항



출처: “의료기관 사이버 보안 개선을 위한 정책 방안 연구”, 이기호 외, 2025, 한국보건사회연구원, p. 344, 저자 재작성.

- 국내외 의료기관을 겨냥한 사이버 공격은 단순한 정보 유출을 넘어 환자의 생명과 진료 중단으로 이어지는 중대한 위협으로 부각되고 있다.
 - 국내의 경우 2020년부터 2025년 8월까지 총 100건의 진료정보 침해사고가 발생했으며, 이 중 랜섬웨어 공격이 91.0%(91건)로 가장 치명적인 유형으로 확인되었다. 종별로는 의원(45건)과 병원(34건) 등 대형병원뿐 아니라 의료기관 전반에서 사고가 지속되고 있다.
 - 미국 포네몬 연구소 자료에 따르면, 랜섬웨어 공격을 받은 의료기관의 68%가 진료 차질을 겪었으며, 68% 중 28%는 환자 사망률이 증가했다고 답해 사이버 보안이 환자의 안전과 직결됨을 방증했다.

- 이기호 부연구위원은 의료기관의 사이버 복원력을 높이기 위해 다음과 같은 정책 과제를 제안했다.
 - 실태조사에서 확인된 의료기관 간 보안 격차를 줄이기 위해 의료기관 규모와 보안역량에 따른 차등화된 지원과 의료기관 자체의 보안역량 강화
 - 개별 의료기관의 자체 대응 한계 보완을 위해 의료정보보호센터를 중심으로 공동대응체계를 강화하고, 의료기관의 실질적인 참여 확대
 - 의료기관 사이버 보안 실태를 정기적으로 파악하고 사이버 침해사고에 따른 경제적 피해를 객관적으로 제시할 수 있는 근거 기반 강화
 - 의료기관 사이버 보안은 궁극적으로 국민의 민감한 진료정보와 환자 안전 보호, 사이버 위협 상황에서도 의료서비스의 연속성을 확보하기 위한 과제이므로 정부의 제도적·재정적 지원과 의료기관 간 공동대응체계 강화

- 이 부연구위원은 “의료기관은 전자의무기록, 검사, 처방, 수술, 응급진료 등 핵심기능이 정보시스템과 연계돼 있어 사이버 공격은 진료 차질과 환자 안전 위협으로 이어질 수 있다.”고 말했다.

- 이어서 그는 “의료기관 사이버 보안의 궁극적 목표는 공격의 완벽한 차단을 넘어, 침해사고 발생 시에도 진료가 멈추지 않고 환자가 필요한 의료서비스를 지속적으로 받도록 하는 '사이버 복원력'을 확보하는 것”이라고 강조했다.

※ 이슈엔포커스 제475호 원문 보기

<https://www.kihasa.re.kr/publish/regular/focus/view?seq=77093>