

보건복지 ISSUE & FOCUS

제475호 (2026-16)



발행인 신영석 발행처 한국보건사회연구원 (30147) 세종시 시청대로 370 세종국책연구단지 사회정책동(1~5층)
T 044)287-8000 F 044)287-8052 발행일 2026. 10. 6. ISSN 2092-7117

의료기관 사이버 보안 현황과 정책 과제¹⁾

이기호

재정통계연구실 부연구위원

- 의료기관 사이버 보안은 개인정보 보호나 전산관리 차원을 넘어 환자 안전과 진료 연속성, 국가 의료서비스 체계의 안정성을 좌우하는 핵심 정책 과제임.
- 의료기관은 전자의무기록, 검사, 처방, 수술, 응급진료 등 핵심 기능이 정보시스템과 연계되어 있어 사이버 공격은 진료 차질과 환자 안전 위협으로 이어질 수 있음.
- 실태조사 결과 의료기관의 보안관제 사각지대가 존재하고, 의료기관 종별 보안역량에도 차이가 있는 것으로 나타남. 전체 응답 기관의 43.0%는 보안관제를 실시하지 않았음. 보안관제가 필요하다는 응답은 88.2%였으나 실제 실시율은 57.0%에 그쳐 필요성에 대한 인식과 실제 대응체계 구축 사이에 상당한 격차가 확인됨.
- 이에 의료기관의 규모와 보안역량을 고려한 보안관리 체계를 마련하고, 의료기관 평가인증 제도에 사이버 보안 항목을 단계적으로 반영하는 한편 공동대응체계와 정례적 실태조사를 강화할 필요가 있음.

01. 의료기관 사이버 보안의 필요성 및 의미

◆ 의료기관에 대한 사이버 공격은 단순한 정보 유출을 넘어 진료 중단과 환자 안전까지 위협하고 있으며, 국내외에서 관련 침해사고가 지속적으로 발생하고 있음.

- 2023년 한 해 동안 유럽연합(EU) 국가들의 보건의료 분야에서 309건 이상의 중대한 사이버 보안 사고가 발생하였다고 보고됨. 이는 EU 내 다른 어떤 주요 분야보다 높은 수치임(European Commission, 2025).

1) 이 글은 이기호, 안수인, 이혜정. (2025). 의료기관 사이버 보안 개선을 위한 정책 방안 연구(한국보건사회연구원)의 연구 결과와 이 연구에서 실시한 '의료기관 사이버 보안 실태조사' 결과를 토대로 작성하였음.

- 미국에서 2024년 500건 이상의 의료기록이 유출된 대규모 의료 데이터 유출 사건은 총 725건으로 2023년 747건 대비 2.95% 감소하였으나, 침해된 데이터 건수는 2억 7523만 4065건으로 2023년 1억 6828만 8480건 대비 63.5% 증가한 것으로 보고됨(The HIPAA Journal, 2024).
 - 대규모 의료정보 유출 사고가 발생할 경우 한 번의 침해사고가 미치는 피해 범위가 매우 클 수 있음을 보여 줌.
- 국내에서도 2020년부터 2025년 8월까지 의료기관에서 발생한 진료정보 침해사고는 총 100건으로 나타남. 연도별로는 2020년 13건, 2021년 21건, 2022년 23건, 2023년 23건, 2024년 14건, 2025년 8월까지 6건이 발생함(전진숙 국회의원실 자료; 허유정, 2025).
 - 특히 전체 100건 가운데 랜섬웨어가 91건으로 91.0%를 차지하였는데, 악성코드 3건, 해킹메일 2건, DDoS 공격·계정 탈취·네트워크 침입·정보 노출이 각각 1건으로 나타나 랜섬웨어가 의료기관 진료정보를 위협하는 가장 주요한 공격 유형으로 확인됨.
 - 의료기관 종별로는 의원이 45건으로 가장 많았음. 병원 34건, 종합병원 16건, 상급종합병원 5건으로 나타남. 이는 사이버 침해사고가 대형 의료기관에 국한된 문제가 아니라 의원과 병원을 포함한 의료기관 전반에서 발생하고 있음을 보여 줌.

◆ 의료기관에 대한 사이버 위협은 환자의 생명이나 건강을 위협하는 중대한 위협 요인으로, 디지털 보안 위협은 더욱 복잡하고 초국가적으로 확산되고 있음.

- 세계보건기구(WHO) 보고서에 따르면 의료분야 사이버 위협은 금전적 이득이나 사이버 범죄를 위한 개인식별정보(PII) 탈취뿐 아니라 진료 예약이나 수술 취소에 따른 혼란, 의료정보 시스템 마비 등을 통해 환자의 치료를 지연시키는 등 환자의 생명이나 건강에 심각한 영향을 미칠 수 있음(Abed et al, 2024).
- 경제협력개발기구(OECD)는 의료의 디지털화가 가속화되면서 해킹, 시스템 중단, 환자 피해, 사회적 신뢰 저하 등 디지털 보안 위협의 영향이 의료서비스 전반으로 확대되고 있다고 지적함(Sutherland et al., 2023).
- 포네몬(Ponemon) 자료에 따르면 랜섬웨어 공격을 경험한 미국 의료기관 중 68%가 환자 치료에 차질이 있었다고 응답했음. 환자 사망률이 증가했다는 응답도 28%로 나타남(Ponemon Institute, 2023).
 - 이는 의료기관에 대한 사이버 공격이 단순한 개인정보 유출이나 전산장애를 넘어 실제 진료와 환자 안전에 영향을 미칠 수 있음을 보여 줌.

◆ 의료기관의 사이버 보안은 전산 부서만의 문제가 아니라 환자 개인정보와 생명·안전, 진료 연속성을 함께 보호하기 위한 필수 관리 영역임.

- 오늘날 의료서비스 환경은 전자의무기록(EMR), 의료영상저장전송시스템(PACS), 처방전달시스템(OCS), 임상검사정보시스템(LIS), 사물의료기기(IoMT) 등 다양한 정보시스템을 기반으로 운영되고 있음.
- 이러한 정보시스템은 진료 효율성과 의료서비스 질을 높이는 데 기여하지만, 동시에 사이버 공격이 발생할 경우 진료 전 과정에 영향을 줄 수 있는 위험 요인이 되기도 함.

- 특히 랜섬웨어 공격이나 악성코드 감염으로 의료기관의 정보시스템이 마비될 경우 진료 예약 취소, 검사 결과 확인 지연, 수술 일정 차질, 응급환자 이송 등 환자 안전 문제가 발생할 수 있음.

◆ **한국의 의료기관은 사이버 위협에 대한 공동대응체계 참여 수준에서 의료기관 종별 차이가 나타남. 이를 포함한 보안 실태를 체계적으로 파악할 수 있는 실증적 근거도 아직 충분하지 않음.**

- 2024년 말 기준 의료정보보호센터 가입률은 상급종합병원 60.0%, 종합병원 7.1%로 의료기관 종별 차이가 크게 나타남(한국사회보장정보원, 2025).
 - 의료정보보호센터 가입률은 의료기관의 전체 사이버 보안 수준을 직접 나타내는 지표가 아니라 공동보안관제, 위협정보 공유, 침해사고 대응 지원 등 공동대응체계에 대한 참여 수준을 보여 주는 지표임.
 - 특히 종합병원의 가입률이 7.1%에 그친다는 점은 의료기관의 전체 보안 수준과는 별개로, 공동보안관제와 위협정보 공유 등 의료분야 공동대응체계와의 연계가 제한적임을 보여 줌.
- 국내에서는 의료기관의 사이버 보안 실태를 체계적으로 조사·분석하고 정책적 개선 과제로 연결한 실증 연구가 충분하지 않음.
 - 특히 보안관제, 보안인증, 인력·예산, 공동대응체계 등 핵심 요소를 종합적으로 검토한 근거 기반 연구는 아직 미흡한 상황임.

◆ **이 글은 ‘의료기관 사이버 보안 실태 조사’ 결과를 토대로 의료기관 사이버 보안 수준과 한계를 점검하고, 향후 정책 과제를 제시하는 데 목적이 있음.**

- ‘의료기관 사이버 보안 실태조사’는 대한병원협회에 위탁하여 전국 17개 시도의 상급종합병원 및 종합병원을 대상으로 2025년 7월 28일부터 8월 22일까지 총 26일간 온라인 설문조사 방식으로 실시하였음.
 - 종합병원은 설문조사 대상 330개소 중 222개소가 응답하여 응답률 67.3%였으며, 상급종합병원은 설문조사 대상 47개소 중 41개소가 응답하여 응답률 87.2%임.
 - 전체 조사 대상 377개소 중 263개소가 응답하여 전체 응답률은 69.8%임.
- 이 글에서는 ‘의료기관 사이버 보안 실태조사’ 결과 중 보안관제 도입 수준, 보안인증체계 보유 현황, 보안관제 필요성 인식, 도입 저해 요인, 정보보안 업무 애로 사항 등을 중심으로 의료기관의 현황을 살펴본 뒤 의료기관의 사이버 보안 수준과 한계를 점검하고 향후 정책 과제를 제시하고자 함.

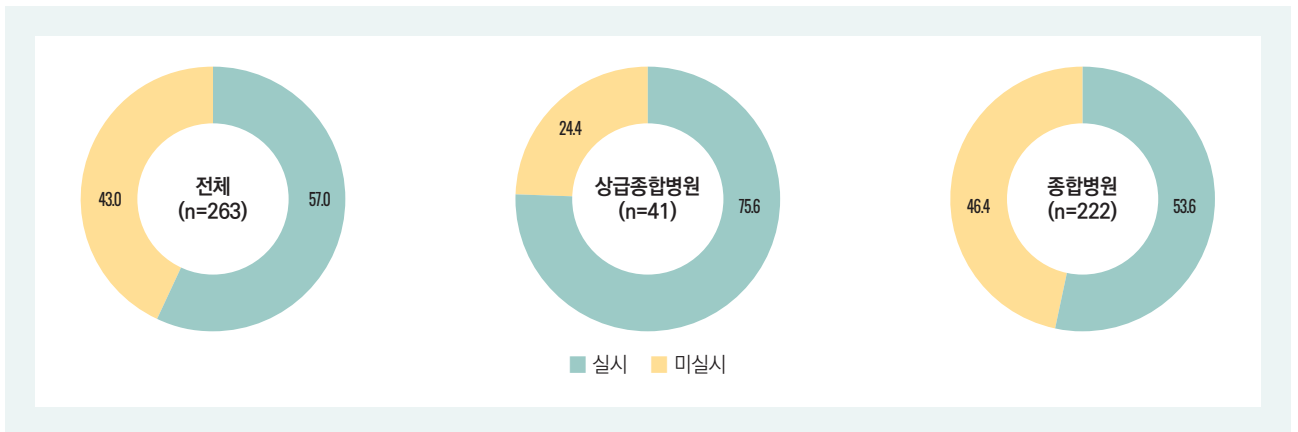
02. 의료기관 사이버 보안 실태조사 결과

◆ **보안관제는 의료기관 사이버 보안의 기본 대응체계에 해당하지만, 여전히 충분히 확산되지 못했으며, 상급종합병원과 종합병원 간 도입 수준에도 차이가 나타남.**

- 보안관제는 악성코드 감염, 비정상 접속, 랜섬웨어 공격 징후 등을 상시 모니터링하고 이상행위를 조기에 탐지하기 위한 핵심 수단임.
 - 의료기관은 24시간 진료체계를 유지하고, 전자의무기록·검사·처방·수술 등 핵심 기능이 정보시스템과 연계되어 있다는 점에서 보안관제는 단순한 정보기술(IT) 운영 수단이 아니라 진료 연속성을 유지하기 위한 최소한의 안전장치임.
- 실태조사 결과 전체 응답 기관 263개소 중 보안관제를 실시하는 의료기관은 57.0%(150개소), 실시하지 않는 의료기관은 43.0%(113개소)로 나타남.
 - 이는 전체 응답 의료기관 10곳 중 4곳 이상이 사이버 위협을 상시 탐지할 수 있는 보안관제 체계를 운영하지 않고 있음을 의미함.
 - 종별로는 상급종합병원의 보안관제 실시율은 75.6%였으나, 종합병원은 53.6%에 그쳐 의료기관 종별 보안관제 도입 수준 차이가 확인됨.
- 의료기관의 시스템 장애는 진료 지연, 검사·처방 차질, 응급환자 대응 지연 등으로 이어질 수 있으므로 보안관제 미실시는 진료 연속성과 환자 안전을 위협할 수 있는 중요한 취약 요인임.

[그림 1] 보안관제 실시 여부

(단위: %)



출처: “의료기관 사이버 보안 개선을 위한 정책 방안 연구”, 이기호 외, 2025, 한국보건사회연구원, p. 188, 저자 재작성.

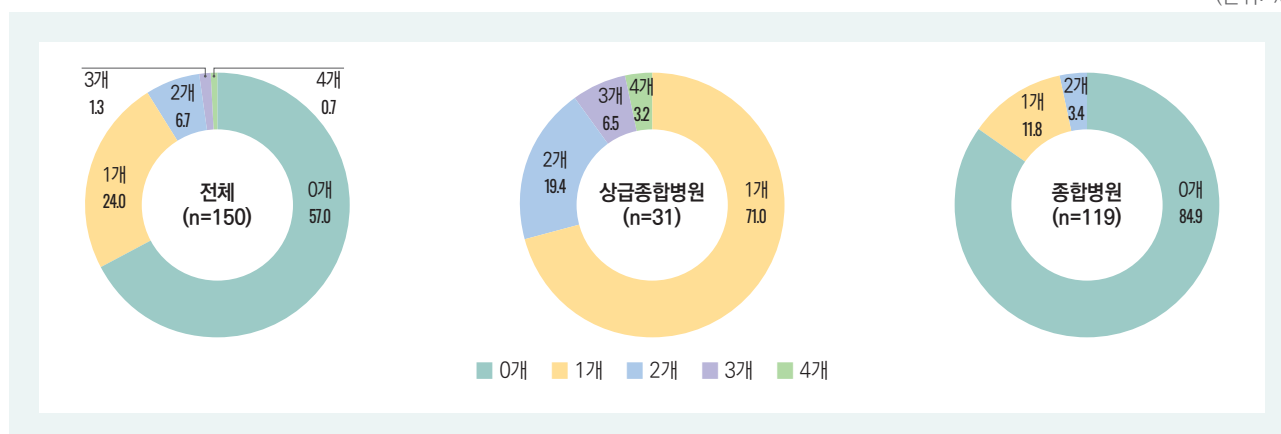
◆ 보안인증체계 보유 수준에서도 의료기관 종별 격차가 뚜렷하게 나타남.

- 보안인증체계는 의료기관의 전반적 보안관리 수준을 객관적으로 확인하는 기준임.
 - 보안인증체계는 보안관제 도입 여부뿐 아니라 정보보호 거버넌스, 접근통제, 개인정보 보호, 침해사고 대응, 백업·복구, 교육훈련, 외주·공급망 관리 등 보안관리체계가 적절하게 운영되고 있는지를 점검하는 수단임.
 - 특히 단순히 보안장비 보유 여부를 확인하는 것이 아니라 의료기관이 일정 수준 이상의 정보보호 관리체계와 운영 역량을 갖추고 있는지를 확인하는 기준이라는 점에서 의미가 있음.
- 실태조사 결과 보안관제를 실시한다고 응답한 의료기관 150개소 중 보안인증체계를 보유한 기관은 32.7%(49개소), 보유하지 않은 기관은 67.3%(101개소)로 나타남.

- 보안관제를 운영하고 있더라도 외부 인증을 통해 보안관리체계를 객관적으로 확인받은 의료기관의 비율은 높지 않음을 보여 줌.
- 이는 보안관제 도입과 함께 조직 차원의 보안관리체계를 지속적으로 관리·점검하는 것이 중요함을 보여 줌.
- 의료기관 종별로는 상급종합병원은 대부분 1개 이상의 보안인증체계를 보유한 반면 종합병원은 84.9%가 인증을 전혀 보유하지 않은 것으로 나타남.
 - 의료기관 간 격차가 보안관제 도입 여부에만 그치는 것이 아니라 보안관리체계의 제도화 수준에서도 뚜렷하게 나타남.
 - 특히 종합병원은 지역 의료체계에서 입원·수술·응급진료 등 핵심 기능을 수행하고 있음에도 보안인증과 보안관리체계 측면에서는 상대적으로 취약한 상태임.
 - 다만 보안인증체계 보유 여부만으로 의료기관 전체의 사이버 보안 수준을 단정하기보다는 인증 취득에 필요한 인력·예산 및 제도적 적용 여건을 함께 고려할 필요가 있음.

[그림 2] 보안인증체계 보유 여부 및 개수

(단위: %)



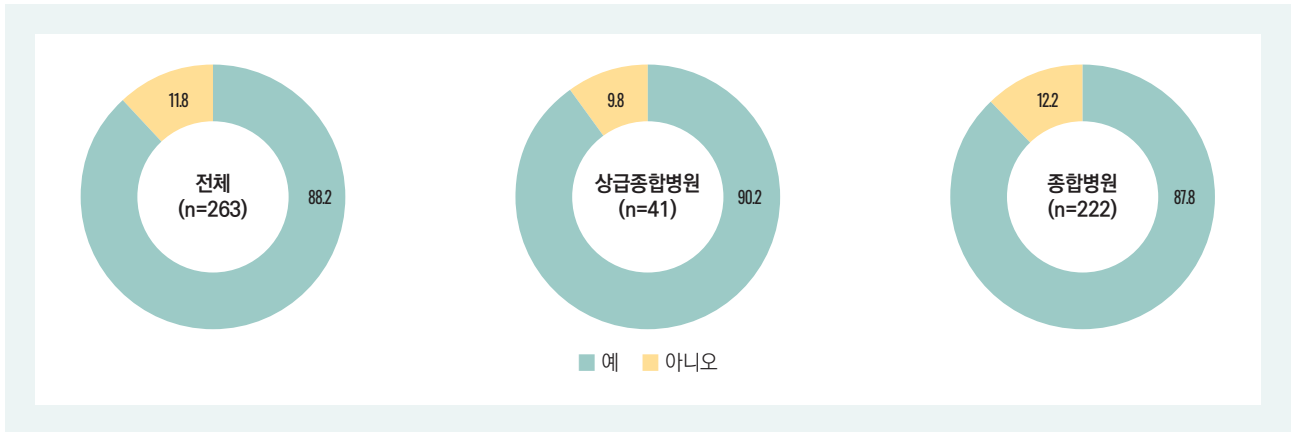
출처: "의료기관 사이버 보안 개선을 위한 정책 방안 연구", 이기호 외, 2025, 한국보건사회연구원, p. 192, 저자 재작성.

◆ **의료기관의 88.2%가 보안관제의 필요성을 인식하고 있으나 실제 실시율은 57.0%에 그쳐 인식과 실행 사이에 31.2포인트의 격차가 나타남.**

- 의료기관 전반에서 보안관제 필요성에 대한 인식은 높은 수준임.
 - 전체 응답 기관 263개소 중 보안관제 체계 도입이 필요하다고 응답한 비율은 88.2%(232개소)로 나타남.
 - 의료기관 종별로는 상급종합병원 90.2%, 종합병원 87.8%가 필요하다고 응답함.
- 이러한 격차는 의료기관이 보안관제의 필요성을 인식하고 있음에도 실제 도입을 가능하게 하는 비용·인력·기술적 여건이 충분하지 않음을 보여 줌.
 - 보안관제 도입 저해 요인으로는 '초기 구축 비용 부담'이 가장 높게 나타났으며, 다음으로 '내부 전문인력 부족', '내부 기술적 지식 부족', '보안관제 필요성에 대한 경영진의 인식 부족' 순으로 조사됨.
 - 특히 초기 구축 비용과 전문인력 부족이 상위 저해 요인으로 나타난 것은 의료기관 사이버 보안 정책이 인식 개선을 넘어 실제 구축·운영 여건을 개선하는 방향으로 추진될 필요가 있음을 시사함.

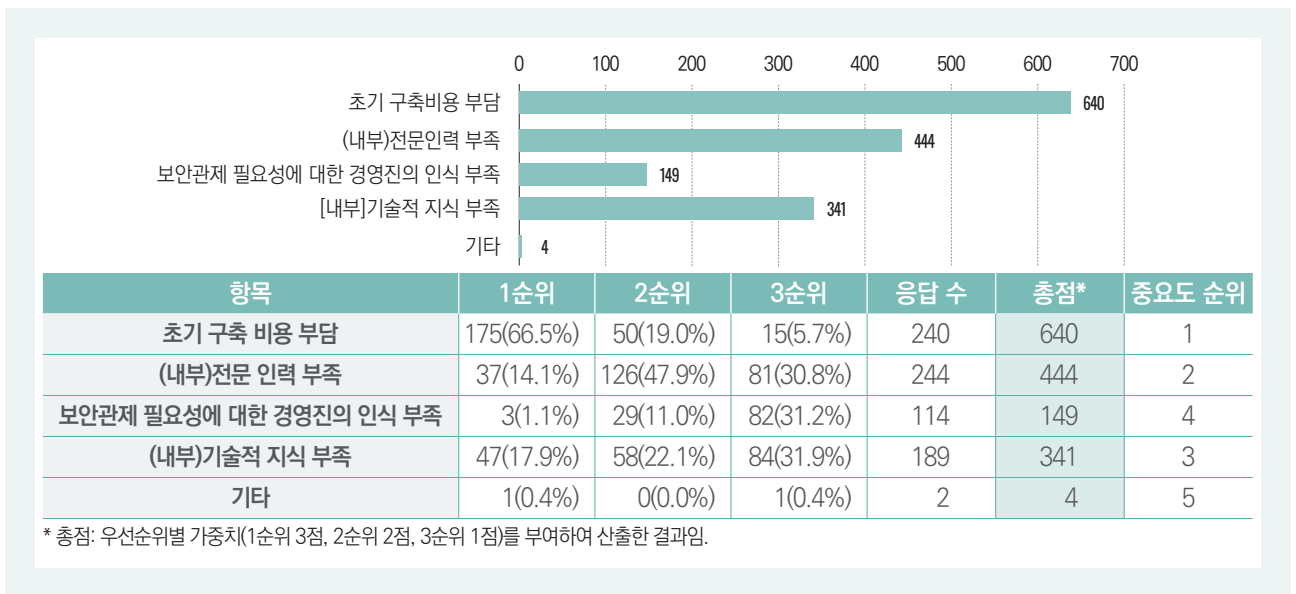
[그림 3] 보안관제체계 도입 필요성 여부

(단위: %)



출처: “의료기관 사이버 보안 개선을 위한 정책 방안 연구”, 이기호 외, 2025, 한국보건사회연구원, p. 394, 저자 재작성.

[그림 4] 보안관제체계 도입 저해 요인



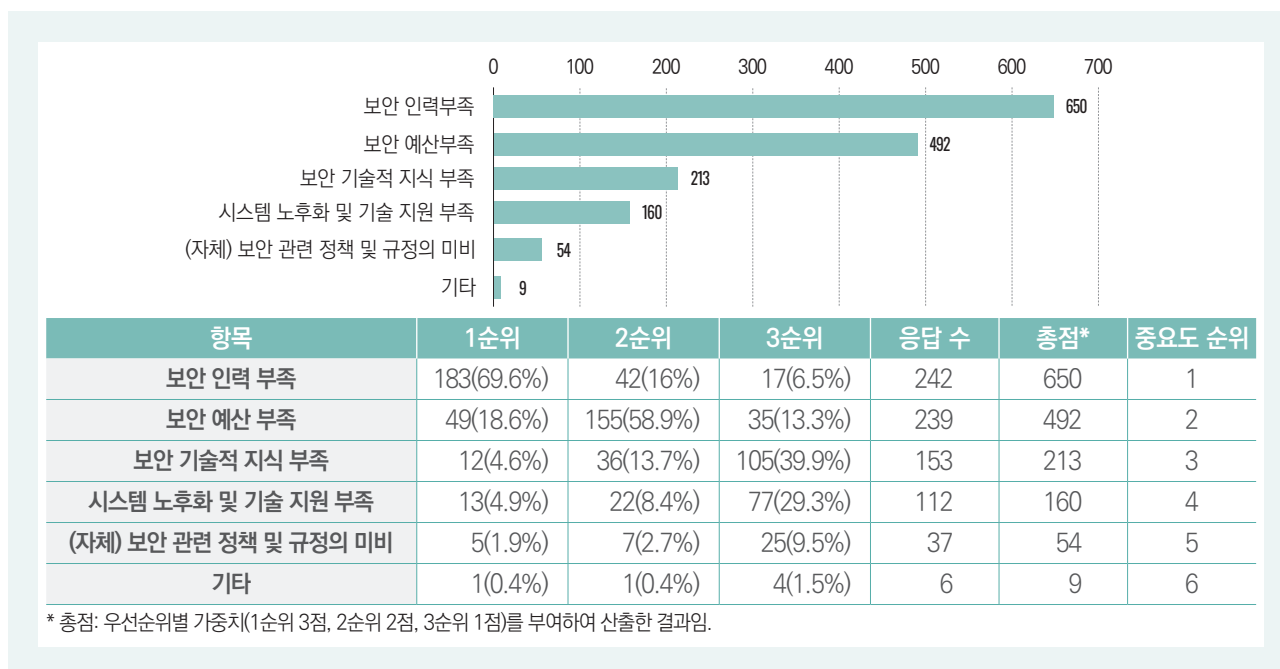
출처: “의료기관 사이버 보안 개선을 위한 정책 방안 연구”, 이기호 외, 2025, 한국보건사회연구원, p. 398, 저자 재작성.

◆ 의료기관 보안 업무의 가장 큰 제약 요인은 전문인력과 예산 부족으로, 지속적인 보안관리 기반이 충분하지 않음.

- 정보보안 업무 관련 애로 사항으로는 ‘보안 인력 부족’이 가장 높게 나타났으며, 다음으로 ‘보안 예산 부족’, ‘보안 기술적 지식 부족’, ‘시스템 노후화 및 기술지원 부족’ 순으로 나타남.
 - 전담 인력과 전문성이 부족할 경우 보안관제, 침해사고 대응, 취약점 점검, 교육훈련, 의료기기 보안점검 등 핵심 보안활동을 지속적으로 수행하기 어려울 수 있음.
 - 보안 예산 부족 역시 대부분의 보안활동을 제약하는 핵심 요인으로 보안관제 도입, 보안인증체계 획득, 전문인력 충원, 모의훈련, 백업·복구체계 구축, 의료기기 보안관리 등은 모두 일정 수준의 예산 투입을 전제로 함.

- 이러한 결과는 의료기관 사이버 보안역량이 보안장비 도입뿐 아니라 전문인력과 지속적인 운영예산 확보의 영향을 받고 있음을 보여 줌.

[그림 5] 정보보안 업무 관련 애로 사항



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

03. 의료기관 사이버 보안 강화를 위한 정책 과제

◆ 실태조사에서 확인된 의료기관 간 보안 격차를 줄이기 위해 의료기관의 규모와 보안역량에 따른 차등화된 지원과 함께 의료기관 자체의 기본 보안역량 강화가 병행되어야 함.

- 상급종합병원의 보안관제 실시율은 75.6%인 반면 종합병원에는 53.6%로 22.0%포인트의 차이가 나타났으며, 보안인증체계 보유 수준에서도 의료기관 종별 격차가 확인됨.
 - 이러한 결과는 의료기관의 규모와 인적·재정적 여건에 따라 사이버 보안 대응역량에도 차이가 있을 수 있음을 보여 줌.
- 따라서 모든 의료기관에 동일한 수준의 관리 기준과 지원을 적용하기보다 의료기관의 규모·기능·보안 역량을 고려한 단계적 접근이 필요함.
 - 상급종합병원 등 국가 및 지역 의료체계에서 중요한 역할을 수행하는 의료기관에는 보안관제, 정보보안 전담 인력, 침해사고 대응, 백업·복구 등 상대적으로 높은 수준의 보안관리 기준을 적용할 필요가 있음.
 - 보안인력과 예산이 상대적으로 부족한 의료기관에는 공동보안관제, 기술·재정지원, 교육·컨설팅 등을 연계하여 실제 대응역량을 높이는 방식으로 지원할 필요가 있음.

- 의료기관 평가·인증 체계에도 정보보호 거버넌스, 보안관제, 침해사고 대응, 백업·복구, 의료기기 보안 등 사이버 보안 관련 항목을 단계적으로 반영하여 예방적 보안관리 수준을 높일 필요가 있음.
- 의료기관 역시 정부 지원을 기다리는 수동적 주체가 아니라 스스로 기본적인 사이버 보안 수준을 관리하는 주체가 되어야 함.
 - 경영진과 종사자를 대상으로 사이버 위협과 침해사고의 심각성을 지속적으로 교육하고, 침해사고 대응 절차와 자체 보안 규정을 정기적으로 점검할 필요가 있음.
 - 백업·복구 체계 점검, 계정 및 접근권한 관리, 취약점 점검, 모의훈련 등 의료기관이 자체적으로 수행할 수 있는 기본 보안활동을 일상적인 관리체계로 정착시킬 필요가 있음. 내부 전문성이 부족한 경우 외부 보안 컨설팅을 적극 활용할 수 있음.
- 중장기적으로는 「의료법」 등 관련 법령에서 의료기관의 사이버 침해사고 예방 및 정보시스템 안전성 확보에 관한 책임을 보다 명확히 하는 방안도 검토할 필요가 있음.

◆ 개별 의료기관의 자체 대응 한계를 보완하기 위해 의료정보보호센터를 중심으로 공동대응체계를 강화하고, 의료기관의 실질적인 참여를 확대할 필요가 있음.

- 실태조사에서는 보안관제가 필요하다고 응답한 의료기관이 88.2%였으나 실제 실시율은 57.0%에 그쳐 필요성에 대한 인식과 실제 대응체계 구축 사이에 상당한 차이가 나타남.
 - 특히 초기 구축 비용과 전문인력 부족이 보안관제 도입을 제약하는 주요 요인으로 나타나 모든 의료기관이 자체적으로 보안관제와 침해사고 대응역량을 확보하는 데는 현실적인 한계가 있음.
- 의료정보보호센터는 공동보안관제, 위협정보 공유, 침해사고 대응지원 등을 통해 개별 의료기관의 보안역량을 보완할 수 있는 공동대응체계임.
 - 2024년 말 기준 의료정보보호센터 가입률은 상급종합병원 60.0%, 종합병원 7.1%로 의료기관 종별 참여 수준에 큰 차이가 나타남.
 - 특히 종합병원 가입률이 7.1%에 그친다는 점은 전체 사이버 보안 수준과는 별개로 공동보안관제와 위협정보 공유 등 공동대응체계와의 연계가 매우 제한적임을 보여 줌.
- 따라서 향후 정책의 초점은 의료정보보호센터의 기능을 단순히 확대하는 것뿐 아니라 의료기관이 실제 공동대응체계에 참여하도록 만드는 데 둘 필요가 있음.
 - 보안관제 비용 부담 완화, 기술지원, 보안 컨설팅, 교육훈련, 의료기관 평가·인증제도와의 연계 등 의료기관이 체감할 수 있는 구체적인 참여 유인 방안을 마련할 필요가 있음.

◆ 의료기관 사이버 보안 실태를 정기적으로 파악하고 사이버 침해사고에 따른 경제적 피해를 객관적으로 제시할 수 있는 근거 기반을 강화할 필요가 있음.

- 현재 의료기관의 보안인력, 예산, 보안관제, 침해사고 대응, 의료기기 보안 등 사이버 보안 수준을 지속적으로 파악할 수 있는 자료는 충분하지 않음.

- 이번 실태조사는 상급종합병원과 종합병원을 대상으로 의료기관 사이버 보안 현황을 파악하였다는 점에서 의미가 있으나, 의료기관 유형별 차이와 정책 효과를 지속적으로 파악하기 위해서는 병원 및 의원 등을 포함한 전체 의료기관을 대상으로 정기적인 자료 축적이 필요함.
- 의료기관 사이버 보안 실태조사를 정례화하고, 향후 병원 및 의원급 의료기관까지 조사 대상을 단계적으로 확대하여 의료기관 유형별 취약 영역과 정책 지원 필요성을 파악할 필요가 있음.
 - 조사 결과는 의료기관 평가인증체계 개선, 재정·기술 지원의 우선순위 설정, 공동대응체계 개선 및 정책성과 평가를 위한 기초 자료로 활용할 수 있음.
- 의료기관의 사이버 침해사고는 정보시스템 복구비용뿐 아니라 진료 중단, 진료 지연, 환자 이송, 업무 중단 등 의료기관 특유의 직간접 피해를 초래할 수 있음.
 - 그러나 피해 규모가 구체적인 비용으로 제시되지 않으면 의료기관 경영진이 사이버 위협을 투자 우선순위로 인식하기 어렵고, 정부 역시 어느 영역에 어느 수준의 지원이 필요한지 판단하는 데 한계가 있음.
- 따라서 의료기관 특성을 반영한 경제적 피해 산정 모델을 마련하여 ‘사이버 침해사고가 의료기관에 실제로 어느 정도의 경제적 피해를 발생시키는가’를 객관적으로 제시할 필요가 있음.
 - 이를 의료기관의 예방적 보안 투자와 정부의 재정·기술지원 및 정책지원 우선순위 설정을 위한 근거 자료로 활용할 필요가 있음.

◆ **궁극적으로 의료기관 사이버 보안은 정보시스템을 보호하는 데 그치지 않고, 국민의 민감한 진료정보와 환자 안전을 보호하며 사이버 위협 상황에서도 의료서비스의 연속성을 확보하기 위한 과제임.**

- 개인의 진료정보에는 질병, 검사 결과, 치료 내용 등 민감한 개인정보가 포함되어 있어 사이버 침해로 유출될 경우 개인정보 및 사생활 침해와 2차 피해로 이어질 수 있음. 또한 의료정보시스템 장애는 검사·처방·수술·응급진료 등의 지연이나 중단으로 이어져 국민이 필요한 의료서비스를 적시에 제공받는 데 영향을 미칠 수 있음.
- 결국 의료기관 사이버 보안의 목표는 사이버 공격을 완전히 차단하는 것만이 아니라 사이버 공격이 발생하더라도 진료가 멈추지 않고 환자가 필요한 의료서비스를 계속 받을 수 있도록 하는 데 있음.
 - 이를 위해 의료기관의 예방·대응·복구 역량과 정부의 제도적·재정적 지원, 의료기관 간 공동대응체계를 함께 강화하여 의료체계의 사이버 복원력을 높일 필요가 있음.

참고문헌

- 이기호, 안수인, 이혜정. (2025). **의료기관 사이버 보안 개선을 위한 정책 방안 연구**. 한국보건사회연구원.
- 허유정. (2025. 9. 24.). 진료정보도 ‘해킹 안전지대’ 아냐... 사이버 침해 사고 6년간 100건. **한국일보**.
- 한국사회보장정보원. (2025). **의료정보보호센터 내부 자료**.
- Abed, S. F., Allain-loos, S., & Shindo, N. (2024, January 26). *Examining the threat of cyber-attack on health care during the COVID-19 pandemic* (WHO Cyber-security Report). World Health Organization. <https://iris.who.int/server/api/core/bitstreams/65e5a0a9-74fd-46f6-947e-ec910dabb47a/content>
- European Commission. (2025, January 15). *Bolstering the cybersecurity of the healthcare sector*. https://commission.europa.eu/news-and-media/news/bolstering-cybersecurity-healthcare-sector-2025-01-15_en
- Ponemon Institute. (2023). *Cost of a Data Breach Report 2023: Healthcare Industry Findings*. IBM Security.
- Sutherland, E., Keelara, R., Eiszele, S., & Haugrud, J. (2023). *Fast-Track on digital security in health* (OECD Health Working Papers, No. 164). OECD Publishing. <https://doi.org/10.1787/c3357f9f-en>
- The HIPAA Journal. (2024). *2024 healthcare data breach report*.

용어 설명

- **사이버 위협(cyber threat)**: 정보시스템에 무단 접근하여 데이터를 파괴·공개·변조하거나 서비스 거부를 일으켜 조직 운영과 자산에 손실을 입히거나 개인에게 악영향을 줄 수 있는 모든 상황이나 사건.
- **사이버 공격(cyber attack)**: 네트워크, 시스템 또는 장비의 기능에 무단으로 영향을 미치는 행위 또는 정보에 무단으로 접근하여 사용, 공개, 파괴, 수정 또는 탈취하는 행위.
- **사이버 침해사고(security incident)**: 정보시스템 또는 그 정보가 처리·저장·전송되는 과정에서 기밀성, 무결성, 가용성이 위협받거나 보안 정책·절차 위반이 이루어지는 사건 또는 위협 가능성이 있는 사건.
- **사이버 위협·사이버 공격·사이버 침해사고 관계 설명**: 사이버 위협은 잠재적 위험을 의미하고, 사이버 공격은 그 위험이 실제로 실행된 행위를 의미하며, 사이버 침해사고는 그러한 공격이나 오류로 인해 정보시스템의 기밀성·무결성·가용성이 침해된 결과적 사건을 의미.
- **사이버 복원력(Cyber Resilience)**: 사이버 위협이나 침해사고가 발생하더라도 핵심 기능과 서비스의 중단을 최소화하고, 침해사고에 대응·복구하여 신속하게 정상적인 운영 상태로 회복할 수 있는 역량.