연구보고서 2025-61

의료기관 사이버 보안 개선을 위한 정책 방안 연구

이기호
안수인·이혜정

사람을
생각하는
사람들

KOREA INSTITUTE FOR HEALTH AND SOCIAL AFFAIRS

한국보건사회연구원
KOREA INSTITUTE FOR HEALTH AND SOCIAL AFFAIRS

▌연구진

연구책임자 **이기호** 한국보건사회연구원 부연구위원
공동연구진 **안수인** 한국보건사회연구원 전문연구원
이혜정 한국보건사회연구원 연구위원

연구보고서 2025-61

의료기관 사이버 보안 개선을 위한 정책 방안 연구

발 행 일 2025년 12월
발 행 인 신 영 석
발 행 처 한국보건사회연구원
주 소 [30147]세종특별자치시 시청대로 370
세종국책연구단지 사회정책동(1~5층)
전 화 대표전화: 044)287-8000
홈페이지 http://www.kihasa.re.kr
등 록 1999년 4월 27일(제2015-000007호)
인 쇄 처 (사)공감과어울임 세종인쇄정보

ISBN 979-11-7252-136-3 [93510]
https://doi.org/10.23060/kihasa.a.2025.61

발|간|사

오늘날 우리는 인공지능(AI)이 경제와 사회 전반을 재편하는 이른바 '모두의 AI' 시대를 맞이하고 있다. 정부는 2025년 'AI 3대 강국 도약'을 국가 비전으로 선포하며 전 산업 분야의 디지털 혁신에 박차를 가하고 있으며, 보건의료 분야 또한 이러한 변화의 거센 물결 속에 서 있다. 전자의무기록(EMR)의 보편화를 넘어 인공지능(AI) 기반의 정밀 진단, 원격 모니터링, 그리고 클라우드 기반의 데이터 공유에 이르기까지 의료 서비스의 질적 도약은 눈부시게 전개되고 있다.

그러나 디지털 전환과 인공지능(AI)이 가져온 혁신적 성과의 이면에는 보안과 개인정보 보호라는 구조적 취약점이 공존하고 있다. 의료기관이 보유한 방대한 양의 진료 데이터와 민감정보는 이제 사이버 범죄자들의 핵심 표적이 되고 있다. 최근 발생한 대규모 통신사 서버 해킹 사고에서 목격했듯이, 초연결 사회에서의 사이버 위협은 단일 기업의 피해를 넘어 국가 사회 시스템 전체의 마비를 초래할 수 있다. 특히 의료기관에 대한 사이버 공격은 단순한 정보 유출을 넘어 수술 중단, 진료 지연 등 환자의 생명과 직결되는 치명적인 위협으로 직결된다는 점에서 그 그 사안이 매우 중대하다.

실제로 국내외에서는 랜섬웨어 공격으로 인한 병원 마비와 수십만 건의 개인정보 유출 사고가 끊이지 않고 있다. 하지만 이러한 사이버 위협의 급증에도 불구하고, 우리 의료기관의 대응 체계는 여전히 보완해야 할 점이 많다. 보안 전담 인력의 부족, 낮은 보안관제 서비스 가입률, 그리고 사고 발생 후 통지에 치중된 현행 법령의 한계 등은 디지털 의료 강국으로 나아가기 위해 반드시 해결해야 할 선결과제이다.

이 연구에서는 급변하는 사이버 위협 환경 속에서 국내 의료기관의 사

이버 보안 실태를 객관적으로 진단하고, 실효성 있는 정책 대안을 모색하는 데 주력하였다. 특히, 미국·유럽·일본 등 주요국의 정책 동향과 침해 사례를 면밀히 분석하고, 국내 상급종합병원 및 종합병원을 대상으로 한 실증적인 실태조사를 실시하였습니다. 이를 통해 우리 의료 현장에 적용 가능한 구체적인 정책 방안을 제시하고자 노력하였다.

이 보고서는 이기호 부연구위원의 책임하에 이혜정 연구위원, 안수인 전문연구원이 원내 연구진으로 참여하였다. 모든 연구진의 노고에 감사드린다. 또한 보고서 작성과 관련하여 유익한 의견을 주신 한국사회보장정보원 의료정보보호센터 이성훈 센터장, 김태균 책임, 김혜현 주임, 그리고 의료기관 사이버보안 실태조사에 많은 도움을 주신 대한병원협회 안정호 팀장에게도 감사의 마음을 전한다. 마지막으로, 이 보고서의 내용은 본원의 공식적인 의견이 아님을 밝힌다.

2025년 12월

한국보건사회연구원 원장

신 영 석

목 차

표 목차

그림 목차

요약

1. 연구의 배경 및 목적

인공지능(AI)은 국가 경쟁력과 산업 발전을 좌우하는 핵심 기술로 부상하며 경제·사회 전반의 디지털 혁신을 촉진하고 있다. 이러한 기술 발전은 보건의료 분야에서도 진단·치료 효율성 향상, 환자 맞춤형 의료서비스 확대, 의료데이터 활용 등 다양한 혁신을 가능하게 하고 있으며, 전자의무기록(EMR), 의료영상저장전송시스템(PACS), 처방전달시스템(OCS) 등 의료정보시스템을 기반으로 디지털 헬스케어 서비스가 빠르게 확산되고 있다. 그러나 데이터 중심의 디지털 의료 환경이 확대될수록 보안과 개인정보 보호의 중요성 또한 함께 증가하고 있으며, 최근 발생한 대규모 해킹 사건과 같이 사이버 위협이 사회 전반에 심각한 영향을 미칠 수 있다는 점이 확인되고 있다.

특히 의료기관은 방대한 양의 민감한 개인정보와 의료데이터를 보유하고 있어 사이버 공격의 주요 표적이 되고 있으며, 랜섬웨어 공격이나 해킹으로 인한 데이터 유출과 의료서비스 중단 사례가 국내외에서 지속적으로 발생하고 있다. 의료데이터는 높은 경제적 가치를 가지며, 클라우드 서비스, 원격의료 플랫폼, 의료 IoT 등 다양한 디지털 기술과 연결되면서 사이버 공격 위험이 더욱 확대되고 있다. 정부는 의료기관의 진료정보 침해사고 대응을 위한 법적 근거와 제도를 마련하였지만, 현행 제도는 사후 대응 중심의 구조로 예방적 보안관리체계와 규제 기반이 충분하지 않다는 한계가 지적되고 있다. 또한 의료기관의 보안관제서비스 참여율이 낮고 보안 투자 인식도 부족한 상황에서 의료기관 사이버 보안 실태를 체계적으로 분석한 연구 역시 부족한 실정이며, 이에 대한 실증적 분석과 정책적 대응 방안 마련이 필요한 상황이다.

본 연구의 목적은 의료기관의 사이버 위협 현황과 보안 실태 및 문제점을 종합적으로 파악하고, 이를 토대로 의료기관의 사이버 보안을 강화하기 위한 정책적 대응 방안을 마련하는 데 있다. 이를 위해 국내외 선행연구와 사례분석, 설문조사 등을 수행하여 의료기관이 직면한 사이버 위협과 보안 수준을 진단하고, 예방 및 대응 체계의 한계와 개선점을 도출하고자 한다. 분석 결과는 향후 의료기관의 보안 거버넌스 확립, 실시간 위협 탐지·대응 체계 구축, 인증 인프라 강화, 보안 교육 내실화, 민관·국제 협력 확대 등 구체적인 정책 방향을 제시하는 데 활용하고자 한다.

2. 주요 연구 내용

본 연구의 주요 연구 결과는 다음과 같다.

첫째, 사이버 보안 관련 개념과 의료기관의 사이버 위협 및 취약점과 체계적인 사이버 역량 강화를 위한 국내외 선행연구를 검토하였다. 선행 연구에 따르면 의료기관은 민감한 환자 개인정보와 의료데이터를 보유하고 있어 금전적 이익을 목적으로 한 사이버 공격의 주요 표적이 되고 있으며, 공격자는 데이터 탈취나 정보시스템 마비를 통해 의료서비스를 지연·중단시키는 방식으로 피해를 발생시키고 있다. 특히 의료환경은 정보시스템, 의료기기, 단말기, 센서 등 다양한 장치가 복잡하게 연결된 구조로 이루어져 있어 사이버 공격에 취약하며, 최근 디지털 전환 가속화와 함께 원격의료, 스마트 의료기기, 클라우드 서비스 등 네트워크 기반 의료서비스가 확대되면서 사이버 위협 또한 증가하고 있는 것으로 나타났다.

둘째, 우리나라와 주요 해외 국가들의 의료기관 관련 사이버 보안 정책 동향을 살펴보고, 법·제도 및 정책 추진 현황을 비교·정리하여 개선 사항을 도출하였다. 정보보안 일반법과 보건의료 특별법을 예방-탐지·분석-

대응·복구-사후활동의 전 주기 관리 단계에 따라 분석하였다. 개인정보보호법 등 일반 정보보안 법령은 사고 전 과정에 대한 관리와 제재 체계가 비교적 명확한 반면, 의료법 체계는 예방과 탐지 중심 규정에 치우쳐 대응·복구와 사후평가로 이어지는 관리체계가 상대적으로 미흡한 것으로 나타났다. 또한 의료기관의 보안 거버넌스, 침해사고 신고 기준, 사후 개선 절차 등이 충분히 제도화되지 않았으며, EMR 인증과 ISMS-P 등 기존 제도 역시 의료정보시스템 전체와 의료기관 전반을 포괄하는 데 한계가 확인되었다. 이에 따라 의료기관 사이버 보안 강화를 위해 정보보호 책임자 및 보안조직 의무화, 침해사고 신고 기준 구체화, 의료정보시스템 전반을 포괄하는 인증체계 확대, EMR 인증과 ISMS-P 연계, 사후평가와 재발방지 체계 정례화 등 사고 전 주기를 포괄하는 통합적 보안 거버넌스 구축이 필요함이 정책적 과제로 도출되었다.

셋째, 국내외 의료기관 사이버 보안 침해 사례를 분석하였다. 의료기관의 사이버 보안 침해사고는 의료정보시스템의 고도화와 디지털 의존도가 높아지면서 증가하고 있으며, 주요 공격 대상은 전자의무기록(EMR), 의료영상저장전송시스템(PACS), 처방·검사 시스템 등 핵심 의료정보 인프라로 나타났다. 대부분의 침해사고는 고도의 해킹 기술보다는 패치 미적용, 초기 계정 비밀번호 미변경, 외부 포트 노출, VPN 취약점 방치 등 기본적인 보안 관리 미흡에서 발생하였다. 또한 의료기관 규모에 따라 피해 양상은 다르게 나타났지만 공통적으로 진료 지연, 수술 일정 차질, 데이터 손실 등 환자 안전과 의료서비스 연속성에 직접적인 영향을 미쳤다. 특히 백업 데이터가 동일 네트워크에 저장되어 함께 암호화되는 사례가 많아 복구가 어려웠으며, 이는 피해 확대의 주요 원인으로 지적되었다. 한편 경제적 피해 역시 랜섬 지불 비용을 넘어 진료 중단에 따른 수익 손실, 시스템 복구 비용, 환자 이탈 및 평판 하락 등 다양한 형태로 발생하

였다. 또한 사고 대응 절차와 조직적 대응 역량이 부족한 의료기관에서는 피해가 더욱 확대되는 경향이 확인되었다. 이에 따라 의료기관 사이버 보안은 단순한 기술 문제가 아니라 환자 안전과 병원 운영 안정성을 포함한 복합적 관리 과제로 인식될 필요가 있으며, 기초 보안 수칙 준수, 독립된 백업 관리, 조직적 대응 체계 강화가 중요하다. 아울러 현행 의료법의 사고 통지 중심 규정을 예방 중심의 보안관리체계로 확대하고, 보안책임자 지정, 백업·복구 훈련 의무화, 위협정보 공유체계 구축 등 제도적 보완을 통해 국제 보안 기준과 정합성을 갖춘 의료기관 사이버 보안 체계를 마련할 필요가 있다.

넷째, 상급종합병원 및 종합병원을 대상으로 의료기관 보안관제, 정보보안 예산, 정보시스템 구축 및 유지 보수 현황, 정보보안 조직 및 인력, 정보보안 교육 및 정책, 업무시 애로사항, 보안사고, 정책개선 요구사항, 보안관제 도입 및 활성화 과제 등 사이버 보안 관련 실태 및 문제점, 이슈사항 등 파악하기 위해 의료기관 사이버 보안 실태조사를 실시하였다. 조사결과를 종합하면 다수 기관이 보안예산 확보에 어려움을 겪고 있으며, 전문 인력 채용난, 의료기관 공동보안센터(ISAC) 참여 저조, 공급망 검증 체계 미흡, 교육훈련 부재 등의 문제가 드러났다. 또한 경제적 피해 비용 산정체계가 정형화되지 않아 피해보고의 정확성이 떨어지고 정책 설계의 근거자료 확보에 제약이 발생한다는 점이 확인되었다.

3. 결론 및 시사점

본 연구는 국내외 선행연구 고찰 및 국내외 정책 및 제도 분석, 의료기관을 대상으로 한 사이버 보안 실태조사를 통해 의료분야 사이버 보안의 구조적 취약요인을 분석하고 정책적 개선 방향을 도출하였다.

의료기관의 사이버 보안 역량은 단순한 기술적 보안 장비의 도입만으로 확보될 수 있는 문제가 아니라 조직문화, 예산 우선순위, 인력 역량, 데이터 거버넌스, 협력 네트워크 등 다양한 요소가 결합된 복합적 관리체계의 문제임이 확인되었다. 특히 의료기관은 진료 중심의 운영 구조로 인해 정보보안 투자가 상대적으로 후순위로 밀리는 경향이 있으며, 이는 사이버 침해사고 발생 이후 발생하는 복구 비용과 서비스 중단에 따른 사회적 비용을 고려할 때 비효율적인 구조로 평가된다. 또한 공격자는 기술적 취약점뿐만 아니라 의료기관 종사자의 인적 오류를 악용하는 사회공학 공격을 적극적으로 활용하고 있어 체계적인 보안 교육과 훈련의 정례화가 필수적이며, 이를 제도적으로 의무화할 필요성이 제기된다.

의료데이터의 경제적 가치 상승과 디지털 헬스 기술의 확산 역시 의료기관을 대상으로 한 사이버 공격 위험을 확대시키는 주요 요인으로 나타났다. 특히 의료기기와 사물인터넷(IoT) 기반 장비의 확산은 보안 취약점을 장기간 유지시키는 구조적 문제를 내포하고 있으며, 제조사의 보안 업데이트 정책이 불명확하거나 장비 수명주기 동안 지속적인 보안 관리가 이루어지지 않는 경우 의료기관은 상시적인 사이버 위협에 노출될 수 있다. 이에 따라 의료기기 보안 인증, 소프트웨어 업데이트 관리 기준, 취약점 모니터링 체계 등을 포함한 통합적 보안 생태계 구축이 필요하다. 또한 클라우드 서비스, 외주 개발, 원격 유지보수 등 다양한 제3자 참여가 확대되면서 공급망 보안 위험이 증가하고 있으며, 협력사 보안평가, 계약 기반 보안 요구사항 표준화 등 공급망 관리체계 강화가 요구된다.

거버넌스 측면에서는 의료기관 간 위협정보 공유체계의 강화가 중요한 정책 과제로 확인되었다. 의료기관공동보안관제센터(의료ISAC)은 의료기관 간 사이버 위협정보 공유를 위한 핵심 조직이지만 가입률과 활용도가 낮은 수준에 머물러 있어 가입비 지원, 참여 인센티브 제공, 참여등급

제 도입 등을 통해 참여 확대를 유도할 필요가 있다. 또한 익명화 기반 침해사고 정보 공유체계는 의료기관의 평판 리스크를 완화하면서 보안문화 형성에 긍정적인 영향을 미칠 수 있을 것으로 여겨진다.

기술적 대응 측면에서는 인공지능(AI) 기반 위협탐지 기술의 활용 가능성도 고려할 수 있다. 인공지능(AI) 기반 보안 기술은 의료데이터의 패턴을 분석하여 비정상적인 접근이나 행위를 조기에 탐지할 수 있으며, 의료기관의 보안 인력 부족 문제를 보완할 수 있는 기술적 수단이 될 수 있다. 다만 인공지능(AI) 모델은 개인정보 보호와 학습 데이터 품질 문제를 동반하며, 적대적 공격에 의해 모델의 추론 과정이 교란될 가능성도 존재한다. 따라서 인공지능(AI) 기반 보안 기술의 도입과 함께 설명가능성과 책임성을 포함하는 거버넌스 체계 구축이 병행되어야 한다.

본 연구는 이러한 분석 결과를 바탕으로 의료기관 사이버 보안 정책 추진 방향을 단계적으로 제시하였다. 단기적으로는 의료ISAC 참여 확대, 보안관제 서비스 참여 인센티브 설계, 랜섬웨어 대응 프로토콜 구축 등 실무적 효과가 높은 정책과제가 우선적으로 추진될 필요가 있다. 중기적으로는 의료기기 및 공급망 보안 인증제 구축, 침해사고 자동 신고 플랫폼 구축, 보안 전문인력 양성 프로그램의 제도화가 요구된다. 장기적으로는 예방 중심의 법·제도 체계 확립, 무결성 공격 대응 거버넌스 구축, AI 기반 위협탐지 체계 고도화 등을 통해 국가 차원의 의료 사이버 보안 생태계를 구축해야 할 것이다.

궁극적으로 의료분야 사이버 보안은 국민 생명과 건강 보호, 디지털 헬스케어 산업 발전, 인공지능 기반 의료혁신의 지속가능성을 보장하는 핵심 기반이라는 점에서 국가적 차원의 정책적 관심과 지속적인 투자 확대가 필요하다.

주요 용어: 사이버보안, 사이버위협, 사이버공격, 침해사고

제1장

서론

제 1 장 서론

제1절 연구의 배경 및 목적

1. 연구 배경

2025년 8월 13일 대통령 직속 국정기획위원회가 발표한 국정운영 5개년 계획(안)에서는 국가 비전 및 국정 목표 달성을 위한 23대 추진 전략 중 하나로 “AI 3대 강국 도약”을 선정하였다(국정기획위원회, 2025, p.25). 인공지능(Artificial Intelligence, AI)은 자료 분석·관리 등 업무 보조를 넘어 소통·창작 등 인간의 사고·행동까지 대체하며 경제·사회 전 분야에 영향을 미치는 범용 기술로 자리매김하였다. 또한 국가 전략 자산이라는 인식이 확산되면서 글로벌 인공지능(AI) 패권 경쟁 하에서 독자적인 인공지능(AI) 생태계 확보가 국가 경제와 산업 경쟁력 강화의 핵심 과제로 부상하였다(국정기획위원회, 2025, p. 192).

이와 같은 인공지능(AI) 기반 디지털 혁신은 보건의료 분야에서도 빠르게 확산되고 있다. 진단·치료 효율성 향상, 환자 맞춤형 서비스 제공, 의료 데이터 활용 확대 등 다양한 영역에서 새로운 가능성이 열리고 있으며, 전자의무기록(EMR), 의료영상저장전송시스템(PACS), 처방전달시스템(OCS) 등 의료정보시스템을 중심으로 의료 서비스의 디지털 전환이 가속화되고 있다. 최근에는 인공지능(AI)을 활용한 영상 판독 및 질병 예측, 원격진료 서비스, 환자 모니터링 웨어러블 기기 등 디지털 헬스케어 서비스가 빠르게 확산되고 있다.

그러나 이러한 데이터 기반 디지털 혁신의 확대는 동시에 보안과 개인

정보 보호 측면에서 새로운 위험을 초래하고 있다. 특히 의료기관은 개인 식별번호, 진료기록, 결제 정보 등 민감한 개인정보를 대규모로 보유하고 있어 사이버 공격의 주요 표적이 되고 있다. 의료데이터는 다크웹(dark web)에서 금융 정보보다 10~20배 높은 가치를 가진 것으로 평가되며(Ponemon Institute, 2023, p.7), 의료기관 내부망과 외부 클라우드 서비스, 원격진료 플랫폼, 협력 기관 시스템이 상호 연결되면서 공급망 공격과 의료 IoT(Internet of Things) 해킹 위험도 증가하고 있다(ENISA, 2023, p.15).

최근 사이버 위협은 실제 의료서비스 중단과 환자 안전 위협으로 이어지는 사례도 증가하고 있다. 국내에서는 2021년 서울대학교병원이 북한 연계 해킹조직의 공격을 받아 약 83만 건의 환자·직원 개인정보가 유출되었으며(박은주, 2023.05.10), 최근 3년 반 동안 총 74건의 의료기관 해킹 피해가 보고되었다(김병규, 2023.09.14). 해외에서도 유사한 사례가 지속적으로 발생하고 있다. 미국에서는 2021년 랜섬웨어 공격으로 스크립스 헬스(Scripps Health)가 운영하는 5개 병원의 정보시스템이 마비되어 환자데이터가 유출되었으며(California Department of Public Health, 2021, p.3), 영국에서는 2017년 노후화된 정보시스템과 패치가 적용되지 않은 윈도우 운영체계를 대상으로 한 WannaCry 랜섬웨어 공격으로 인해 NHS(National Health Services)의 운영 중단이 발생하였다(National Audit Office, 2018, p.6). 이러한 사례는 사이버 공격이 의료서비스 중단과 막대한 경제적 손실을 초래할 수 있음을 보여준다.

실제로 의료기관을 대상으로 한 사이버 공격은 단순한 정보 탈취를 넘어 의료서비스 중단, 치료 지연, 응급환자 전원 등 환자의 생명과 건강을 위협하는 심각한 범죄행위로 이어질 수 있다. 2024년 세계보건기구(WHO)의 사이버 보안 보고서에 따르면 코로나19 팬데믹 기간 동안 의료

기관 대상 사이버 위협이 크게 증가하였으며, 이는 금전적 이득을 위한 개인식별번호 탈취뿐만 아니라 진료 예약 및 수술 취소, 의료정보시스템 마비로 인한 치료 지연 등 환자 안전에 직접적인 영향을 미친 것으로 나타났다(Abed et al., 2024). 또한 OECD Health 워킹 페이퍼에서는 글로벌 보건의료 환경에서 디지털 보안 위협이 더욱 복잡하고 초국가적으로 확산되고 있으며, 코로나19 이후 의료 디지털화가 가속화되면서 해킹, 시스템 중단, 환자 피해, 사회적 신뢰 저하 등이 현실화되고 있다고 보고하고 있다(Sutherland et al., 2023).

이러한 사이버 보안 위협은 의료기관에 국한된 문제가 아니라 국가 전체 디지털 인프라의 취약성과도 연결될 수 있다. 2025년 4월 발생한 SK텔레콤 홈 가입자 서버(Home Subscriber Server, HSS) 해킹 사건에서는 약 2,695만 명 가입자의 핵심 인증 정보(IMSI, IMEI, 유심 인증키 등)가 유출되었으며, 이로 인해 복제폰 제작과 금융 사기 등 2차 피해 우려가 제기되었다. 금융권에서는 SK텔레콤을 통한 신원 인증을 일시적으로 중단하는 등 사회 전반에 혼란이 발생하였다. 이러한 사례는 통신·금융·의료 등 다양한 디지털 서비스가 상호 연결된 환경에서 보안 취약점이 다른 분야로 확산될 수 있음을 보여준다.

정부 역시 이러한 사이버 위협에 대응하기 위해 국가 차원의 보안 정책을 추진하고 있다. 정부는 '안전과 책임 기반의 AI 기본 사회 실현(국정과제 23번)'과 '국민이 안심할 수 있는 개인정보 보호 체계 확립(국정과제 25번)'을 주요 국정과제로 선정하여 인공지능(AI) 시대의 안전한 디지털 환경 구축을 추진하고 있다. 보건복지부 또한 의료기관 사이버 보안 강화를 위해 관련 법제도를 정비하고 있으며, 의료법에는 진료 정보 침해사고의 통지(의료법 제23조의3), 진료 정보 침해사고의 예방 및 대응(의료법 제23조의4), 진료 정보 침해사고의 범위(의료법 시행령 제24조의3), 의

료정보보호센터를 통한 침해사고 대응 업무 위탁(의료법 시행규칙 제16조의4) 등의 규정을 마련하였다.

그러나 현행 제도는 침해사고 발생 이후의 통지 의무 중심으로 구성되어 있어 의료기관의 사전 예방조치와 보안 관리 체계 구축을 의무화하는 규정은 충분하지 않다는 지적이 있다. 또한 진료 정보 침해사고의 범위가 협의적으로 규정되어 있으며, 사고 조사 및 재발 방지 명령, 과태료 부과 등 보건복지부의 행정 권한 근거가 명확하지 않고 위반 시 명시적 제재 규정도 부족한 상황이다.

한편 국내 의료기관의 사이버 보안에 대한 인식 역시 아직 충분하지 않은 것으로 나타난다. 의료기관 보안을 지원하기 위해 운영되고 있는 의료정보보호센터의 보안관제서비스 가입률은 상급종합병원 45개 중 27개(60.0%), 종합병원 267개 중 19개(7.1%)에 불과하다(한국사회보장정보원, 2025). 의료기관에서 침해사고가 발생할 경우 탐지·조사·복구 비용과 데이터 손실, 업무 중단 등 막대한 피해가 발생할 수 있음에도 불구하고 보안 투자와 관리 수준은 여전히 제한적인 상황이다.

의료기관의 디지털 전환이 빠르게 진행되는 가운데 사이버 위협 또한 증가하고 있음에도 불구하고, 국내에서는 의료기관의 사이버 보안 실태를 체계적으로 분석하고 정책적 개선 방향을 제시하기 위한 실증 연구가 충분히 이루어지지 않고 있다.

2. 연구 목적

본 연구의 목적은 의료기관의 사이버 위협 현황과 보안 실태 및 문제점을 종합적으로 파악하고, 이를 토대로 의료기관의 사이버 보안을 강화하기 위한 정책적 대응 방안을 마련하는 데 있다. 이를 위해 국내외 선행연

구와 사례분석, 설문조사 등을 수행하여 의료기관이 직면한 사이버 위협과 보안 수준을 진단하고, 예방 및 대응 체계의 한계와 개선점을 도출하고자 한다. 분석 결과는 향후 의료기관의 보안 거버넌스 확립, 실시간 위협 탐지·대응 체계 구축, 인증 인프라 강화, 보안 교육 내실화, 민관·국제 협력 확대 등 구체적인 정책 방향을 제시하는 데 활용하고자 한다.

특히 보건의료 데이터 집적과 교류 확대, AI·원격의료 등 신기술 확산 추세 속에서, OECD 권고 사항을 국내 실정에 맞게 반영하여 기술 발전 속도에 부합하는 보안 체계와 법·제도적 기반을 마련하는 것이 필요하다. 궁극적으로 "모두의 AI" 시대가 국민 생활의 질 향상과 신뢰받는 의료 혁신으로 이어지기 위해서는 보안과 데이터 보호를 서비스 혁신과 동등한 수준의 정책 의제로 설정하고, 균형적이고 선제적으로 대응해야 할 필요가 있다. 본 연구는 이러한 대응 전략 수립을 위한 기초 자료를 제공하고자 한다.

제2절 연구의 내용 및 추진 방법

본 연구는 앞 절에 제시한 연구 목적을 달성하기 위해 총 6개의 장으로 구성하여 전개하였다.

제1장 '서론'에서는 의료기관 사이버 보안 개선을 위한 정책 연구의 배경과 본 연구의 목적을 기술하였으며, 아울러 이를 위해 본 보고서를 구성하고 있는 연구 내용과 방법을 기술하였다.

제2장 '이론적 배경'에서는 문헌고찰을 통해 사이버 보안, 사이버 공격, 사이버 위협, 사이버 침해사고 등 관련 개념과 선행 연구 검토 결과를 기술하였다.

제3장 '의료기관 사이버 보안 정책 검토'에서는 문헌고찰, 전문가 자문 등을 통해 우리나라와 주요 해외 국가들의 의료기관 관련 사이버 보안 정책 동향을 살펴보고, 법·제도 및 정책 추진 현황을 비교·정리하여 개선사항을 도출하였다.

제4장 '의료기관 사이버 보안 침해 사례'에서는 문헌고찰, 전문가 자문 등을 통해 의료기관 사이버 침해 사례를 분석하였다. 미국, 일본, 유럽 등 주요 해외 의료기관의 사이버 위협 사례를 분석하여 위협의 유형, 발생 원인, 대응 방안 및 시사점을 도출하고, 동일한 분석 틀을 국내 의료기관 사례에도 적용하여 비교·검토함으로써 의료기관이 직면한 주요 사이버 위협의 특징과 공통점을 파악하여 시사점을 도출하였다.

제5장 '의료기관 사이버 보안 실태조사'에서는 문헌고찰, 전문가 자문을 통해 설문지를 개발하고 상급종합병원, 종합병원을 대상으로 사이버 보안 인식 및 정책, 사이버 보안 실태 및 문제점, 이슈 사항 등을 설문조사 및 데이터를 분석하였다.

제6장 '결론 및 정책 개선 방안'에서는 국내외 사례 분석과 실태조사

결과를 종합하여 의료기관의 사이버 보안 역량 강화를 위한 핵심 과제를 설정하고, 보안관제서비스 확대 전략 및 정책 개선 방향을 제시하였다. 이 과정에서 현행 정책의 한계와 향후 과제를 함께 제시함으로써, 지속 가능한 사이버 보안 거버넌스 확립과 실효성 있는 대응 방안을 마련하는 데 필요한 기초 자료를 제공한다. 특히 국내 의료기관을 대상으로 한 실태조사와 사례분석을 통해 구체적이고 검증 가능한 데이터를 제공하여, 향후 관련 학술연구의 이론적 토대와 경험적 근거를 확충하는 데 도움을 줄 수 있을 것으로 기대한다.

연구 내용 및 추진 방법을 요약하면 [그림 1-1]과 같다.

〔그림 1-1〕 연구 내용 및 추진 방법

출처: 저자 작성

제2장

이론적 배경

제 2 장 이론적 배경

제1절 사이버 보안의 개념 및 최신 동향

사이버 보안(cyber security)의 개념은 정보시스템에서 처리하는 정보의 기밀성과 안전한 관리에 초점을 둔 정보보안(information security)에서 비롯되었다. 1983년 미국 국방부가 기밀 및 민감정보(classified/sensitive information)를 처리하는 컴퓨터에 대해 보안 수준을 평가하고 표준화된 기준을 제시한 '신뢰할 수 있는 컴퓨터 시스템 평가 기준(Trusted Computer System Evaluation Criteria, TCSEC)'을 발표하였는데, 이는 현대 정보보안 개념의 시초가 되었다(NIST, 2018, pp. 10-12).

1990년대 인터넷이 상용화되면서 '네트워크 보안'(network security) 개념이 대두되었다. 1988년 미국 코델대학교 대학원생 로버트 태판 모리스(Robert Tappan Morris)가 유발한 세계 최초의 대규모 인터넷 웜 공격 사건인 모리스 웜(Morris Worm)은 네트워크를 통한 대규모 사이버 피해의 가능성을 보여주었으며, 방화벽과 침입탐지시스템(Intrusion Detection System, IDS) 등 네트워크 보안 기술의 필요성을 인식하게 하는 계기가 되었다 (Cheswick et al., 1994, pp. 45-47).

2000년대 들어 금융·산업·보건 등 민간 영역이 사이버 공격의 주요 표적이 되면서, 사이버 보안은 기술적 방어를 넘어 사회·경제적 안정성 차원의 과제로 확장되었다. 특히 2010년대 이후 국가 차원의 사이버 안보 전략이 수립되며 '사이버 보안(cyber security)'이 국제 표준 용어로 정착하였다. 다만 사이버 보안의 개념은 국제기구나 연구자의 관점에 따라

다양하게 정의되고 있다. 〈표 2-1〉은 주요 국제 기관 및 연구자들이 정의한 사이버 보안의 개념이다.

〈표 2-1〉 국제기구의 사이버 보안 개념

구분		설명
국제기구	ITU (2008)	- 사이버 환경과 조직 및 사용자의 자산을 보호하는 데 사용할 수 있는 도구, 정책, 보안 개념, 보호 장치, 위험 관리 접근 방식, 조치, 교육, 모범 사례, 보증 및 기술의 집합
	UN (2010)	- 사이버 공간에서 정보와 정보시스템의 가용성, 무결성, 기밀성을 보장하기 위한 조치
	ISO/IEC (2012)	- 사이버 공간에서 정보의 기밀성, 무결성 및 가용성을 보존하는 것
	ISO/IEC (2016)	- 보건정보보안(Health information security)은 ISO/IEC 27002를 보건 분야에 적용하여 보건정보의 기밀성, 무결성 및 가용성을 보장하는 것
	NIST (2018)	- 사이버 공격으로부터 사이버 공간을 보호하거나 방어하는 능력
	OECD (2019)	- 디지털 보안(digital security)은 기술 뿐만 아니라 ICT 사용과 관련된 경제적, 사회적 위험을 관리하는 것
	WHO (2021)	- 보건 분야의 사이버 보안은 디지털 건강 보안의 필수 구성 요소로, 보건 데이터의 기밀성, 무결성 및 가용성을 보장
	ENISA (2022a)	- 네트워크 및 정보시스템, 사용자 및 영향을 받는 사람들을 사이버 위협으로부터 보호하는 모든 조치를 포함
학술연구	Shackelford (2012)	- 사이버 공간에서 정보, 시스템, 네트워크의 파괴나 중단으로부터 보호하는 것
	Von Solms & Van Niekerk (2013)	- 단순한 정보보안 보다 넓은 개념으로, 사이버 공간의 시스템, 인간, 프로세스를 포괄
	Craigen etl al.(2014)	- 사이버 공간과 관련된 시스템을 보호하기 위해 활용되는 자원, 프로세스, 구조의 조직과 집합
	Borky& Bradley (2018)	- 알려진 또는 잠재적 위협으로부터 시스템을 보호하면서 동시에 시스템 기능 유지 간 균형을 잡는 행위
	Bada & Nurse (2019)	- 시스템, 네트워크, 프로그램을 디지털 공격으로부터 보호하는 것
	Craigen, Diakun-Thibault, & Purse (2021)	- 기밀성, 무결성, 가용성의 유지 뿐만 아니라, 인간 요인(human factor)과 완벽한 보안의 불가능성을 인정하는 것
	Schiliro (2023)	- 인력 및 인프라, 구조와 프로세스를 포함한 자원을 모아, 네트워크 및 사이버 공간에 활성화컴퓨터 시스템의 무결성을 훼손하거나 재산권을 침해하는 사건으로부터 보호하기 위한 것

국제기구에서 정의하는 사이버 보안의 개념은 '정보나 정보시스템의 기밀성, 무결성, 가용성을 보장하는 활동'이라는 정보보안 개념을 확장한 것이라는 점에서 공통점을 갖고 있으나 각 국제기구의 활동 목적이나 관심 영역에 따라 사이버 보안의 개념 및 범위가 다소 차이가 있음을 알 수 있다. 또한 사이버 보안의 개념은 초기에는 단순히 정보나 정보시스템 보호에 주목한 협의의 개념(UN, 2010; ISO/IEC, 2012)이었다면, 최근에는 사회적·경제적 위험 관리를 포함(OECD, 2019)하거나 사용자 및 사회적 영향까지를 포함(ENISA, 2022a)하는 광의의 개념으로 확장되고 있으며, 특정 분야에서는 해당 분야에 적합하게 사이버 보안의 개념을 재정의(ISO/IEC, 2016; WHO, 2021)하고 있다.

한편, 대부분의 연구자들도 국제기구와 마찬가지로 사이버 보안이 '정보나 정보시스템의 기밀성, 무결성, 가용성을 보장하는 활동'이라는 정보보안의 기본 개념을 확장하고 있다는 점에서 공통점을 갖고 있다. 다만 연구자들이 제시한 사이버 보안 개념의 차이점을 살펴보면, Shackelford (2012)는 사이버 보안이 사이버 공격에 대한 단순한 차단뿐만 아니라 시스템의 운영 지속성까지를 포함한다고 보았으며, Von Solms & Van Niekerk(2013)는 사이버 위협이 단순히 기술적 문제뿐만 아니라 사용자의 행동, 사회적 네트워크, 프로세스 운영 등을 통해 발생할 수 있기 때문에 사이버 보안을 인간과 프로세스를 포함하는 확장된 개념으로 설명하였다. Craigen, Diakun-Thibault , & Purse(2014)는 방화벽과 같은 단순한 기술적 사이버 보안뿐만 아니라 조직 구조, 인적 자원, 업무 프로세스 등 조직 관리 및 운영까지를 사이버 보안에 포함한 개념으로 설명하고 있으며, Borky & Bradley(2018)는 사이버 보안과 시스템 운영 효율성 간의 균형을 강조하였고, Schiliro(2023)는 사이버 보안을 재산권적 보호까지 확장하였다.

국제기구나 연구자의 사이버 보안 개념을 종합하면, 사이버 보안은 사이버 공간에서 발생하는 다양한 위협으로부터 정보와 시스템, 네트워크, 사람을 보호하기 위한 기술적 조치에 그치지 않고 조직과 사회 차원의 위험관리, 법·제도·정책적 지원, 인권과 프라이버시 보호, 경제·사회적 연속성 확보, 그리고 안전과 신뢰 보장을 포함하는 종합적 활동으로 이해할 수 있다.

본 연구에서는 이러한 논의를 바탕으로 사이버 보안을 사이버 공간에서 발생하는 다양한 위협으로부터 정보, 시스템, 네트워크 및 인간을 보호하기 위한 기술적·관리적·정책적 활동을 포괄하는 개념으로 정의한다.

1. 사이버 위협/사이버 공격/사이버 침해사고

사이버 위협(cyber threat)은 "조직의 운영, 자산 또는 개인에게 정보시스템을 통해 무단 접근, 파괴, 공개, 정보 수정 및 서비스 거부를 일으켜 악영향을 줄 수 있는 모든 상황이나 사건"을 의미한다(NIST, 2025). 반면 사이버 공격(cyber attack)은 "네트워크, 시스템 또는 장비의 기능에 무단으로 영향을 미치는 행위 또는 정보에 무단으로 접근, 사용, 공개, 파괴, 수정 또는 탈취하는 행위"를 의미한다(NIST, 2025).

사이버 위협과 사이버 공격의 의미를 비교하면, 사이버 위협은 정보시스템에 해를 끼칠 수 있는 잠재적인 모든 상황, 사건 또는 행위를 의미하는 추상적이고 포괄적인 개념인 반면, 사이버 공격은 사이버 위협이 현실에서 실행된 구체적이고 직접적인 행위를 의미한다. 따라서 사이버 위협은 잠재적인 위협 요소이고, 사이버 공격은 그 위험이 현실화 된 것을 의미한다.

한편, 사이버 침해사고(security incident)는 "정보시스템 또는 그 정

보가 처리·저장·전송되는 과정에서 기밀성, 무결성, 가용성이 위협받거나 보안 정책/절차 위반이 이루어지는 사건 또는 위협 가능성이 있는 사건"을 의미한다. 즉 사이버 침해사고는 사이버 공격이나 오류로 인해 정보시스템의 기밀성, 무결성, 가용성이 위협받거나 손상된 사건으로 대응이 요구되는 경우를 의미한다.

종합하면 사이버 위협은 잠재적 위험을 의미하고, 사이버 공격은 그 위험이 실제로 실행된 행위이며, 사이버 침해사고는 그러한 공격이나 오류로 인해 정보시스템의 기밀성·무결성·가용성이 침해된 결과적 사건을 의미한다.

2. 사이버 위협 유형 및 최신 동향

가. 랜섬웨어(ransomware)

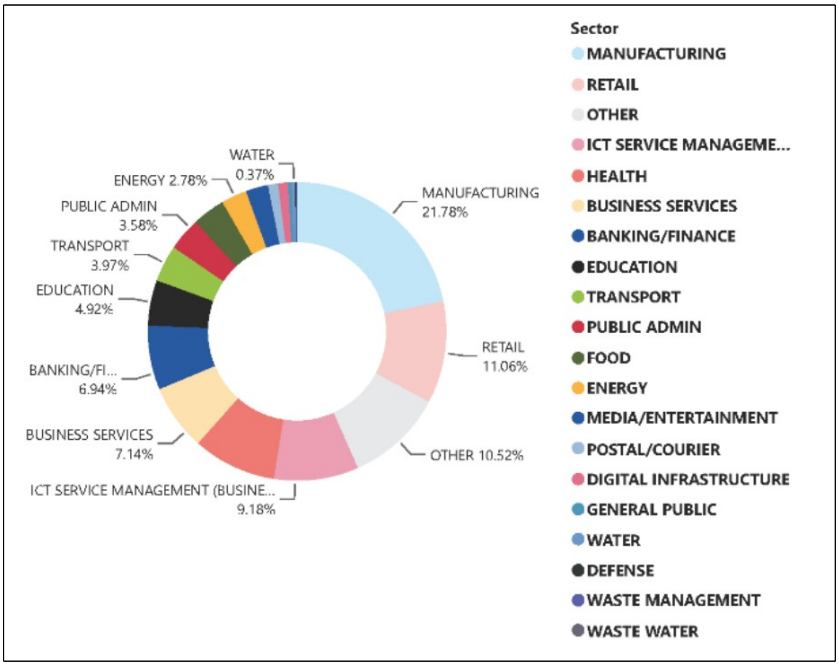
랜섬웨어(ransomware)는 위협 행위자(공격자)가 대상의 자산을 장악하고 자산의 가용성을 반환하는 대가로 몸값을 요구하는 공격 유형으로 특정 행위 방식(action)에 국한되지 않고 변화하는 랜섬웨어 위협 환경과 다중 갈취(multiple extortion) 기법의 확산, 그리고 순수한 금전적 이익 외에도 다양한 목표를 가진 공격자들의 행위를 포괄한다(ENISA, 2024, p.7).

랜섬웨어(ransomware)는 'LEDS'라고도 불리는 잠금(Lock), 암호화(Encrypt), 삭제(Delete), 탈취(Steal)라는 4가지 핵심 동작을 통해 실행될 수 있다(ENISA, 2022b, p.8). 즉 랜섬웨어는 화면 잠금이나 특정 애플리케이션 접근 차단 등을 통해 자산 접근을 차단할 수 있으며, 자산을 암호화하여 대상 사용자가 사용할 수 없도록 만들 수도 있고, 자산을 도

용하여 가용성을 침해하고 궁극적으로 기밀성을 손상시킬 수도 있으며, 자산을 삭제하여 영구적으로 사용할 수 없도록 만들 수도 있다(ENISA, 2022b, p.8).

랜섬웨어(ransomware)는 현재 가장 심각한 사이버 위협 중 하나로 최근에도 특정 산업에 국한되지 않고 다양한 분야를 무차별적으로 공격하고 있다. ENISA 보고서(ENISA, 2024)에 따르면 특히 제조 및 산업 부문이 가장 빈번하고 큰 피해를 입은 것으로 나타났으며, 다음으로 소매업과 디지털 서비스 제공업체 등이 피해를 입은 것으로 나타났다.

[그림 2-1] 유럽연합(EU)의 랜섬웨어 피해 분야



출처: ENISA. (2024). ENISA THREAT LANDSCAPE 2024. p.47

유럽연합(EU)의 경우 ENISA 보고서(ENISA, 2024)에 따르면 이중 갈취(double extortion)빈도가 증가하고 있다. 사이버 범죄자들은 고도화된 전술을 활용해 기관을 다시 공격하며, 주로 과거 공격에서 확보한 취약점이나 계정 정보를 이용한다. 또한 일부 랜섬웨어 그룹은 첫 번째 공격 이후 탈취 데이터를 다크웹 마켓(dark web market)에서 재판매하거나 동일한 피해자를 자신들의 유출 사이트(leak sites)에서 재활용하기도 하며, 이 과정에서 운영자들은 피해자의 압박을 극대화하기 위해 탈취 데이터의 규모를 부풀리거나 침해 사실을 허위로 주장하기도 한다(ENISA, 2024).

유럽연합(EU)의 랜섬웨어 관련 대표적인 사례를 살펴보면 2023년 사이버 범죄 조직인 클롭(Clop) 그룹이 수행한 MOVEit Transfer 취약점 공격을 통해 랜섬웨어의 파괴력이 다시 한번 확인되었으며, 이 공격은 제로데이 취약점을 이용해 수백 개의 글로벌 기업과 공공기관의 데이터를 유출했고 영국 방송 공사(BBC), 브리티시에어웨이(British Airways), 쉘(Shell) 등 세계적 기업들이 직접적인 피해를 입었다. 특히 이 범죄 조직은 암호화가 아닌 단순 데이터 탈취와 공개 협박만으로 금전을 요구하는 새로운 유형의 갈취 방식을 사용하였다. 또 다른 사이버 범죄 조직인 Hive 랜섬웨어 그룹은 의료기관과 중소기업을 대상으로 활발히 활동했으나 2023년 초 미국 연방수사국(FBI)과 유럽연합(EU) 법집행협력청(Europol)의 합동 작전에 의해 인프라가 해체되었다. 한편, 록빗(LockBit)은 여전히 전 세계적으로 가장 활동적인 랜섬웨어 조직으로, 병원, 정부기관, 제조업체를 공격하며, 피해자 포털에 데이터 경매 기능을 도입하는 등 한층 정교한 협박 방식을 도입하고 있다.

우리나라의 경우 2025년 상반기 보고된 랜섬웨어 공격은 총 82건이었으며 대표적인 사례로는 2025년 6월 9일 국내 최대 규모의 온라인 서점

YES24의 랜섬웨어 감염으로 도서 판매, 전자책 서비스, 공연 예매 등 모든 서비스가 약 5일 동안 중단되었다. 이로 인해 국민들의 일상생활에 피해가 발생했으며 기업의 금전적 피해는 약 100억 원 규모의 손실이 발생한 것으로 추산되고 약 2,000만 명의 전체 회원 정보도 유출됐을 가능성이 있다(한국인터넷진흥원, 2025a).

나. 악성코드(malware)

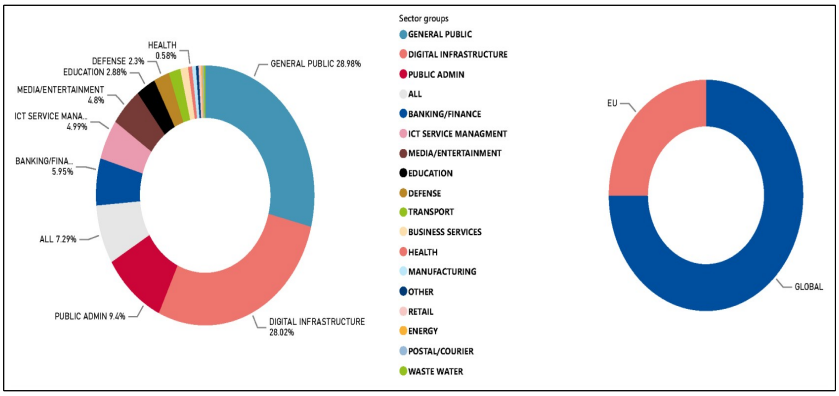
악성코드(malware) 또는 악성로직(malicious logic)은 시스템의 기밀성, 무결성 또는 가용성에 부정적인 영향을 미치는 무단 프로세스를 수행하도록 설계된 모든 소프트웨어 또는 펌웨어(firmware)를 설명하는 데 사용되는 포괄적인 용어이다. 대표적인 예로는 바이러스(virus), 웜(worm), 트로이 목마(trojan horse) 등 숙주를 감염시키는 코드 기반 개체가 있으며, 공격자는 이러한 악성코드를 직접 제작하거나 구매하여 디지털 공격을 수행하고 운영을 지원하며 자산에 대한 통제권을 확보 및 유지하고 방어 체계를 회피하며 침해 이후(post-compromise) 행위를 수행한다(ENISA, 2024, p.62).

사이버 위협 행위자의 목표에 따라 악성코드는 보넷(botnet)과 같이 시스템 및 네트워크를 제어하는 경우도 있고 정보 탈취(information stealing)와 같이 데이터를 탈취하는 경우도 있으며 DoS(Denial of Service)와 같이 시스템 및 네트워크를 완전히 무력화하는 방식으로 실행되는 등 다양한 형태로 나타난다(ENISA, 2024, p.62).

기존에는 불특정 다수의 시스템을 대상으로 무차별적으로 감염시키는 방식이 일반적이었으나 최근에는 특정 시스템을 겨냥한 표적형 악성코드(targeted malware)로 진화하고 있다.

ENISA(2024)의 보고서에 따르면 악성코드는 특히 일반 대중과 디지털 인프라 분야에 큰 피해를 입힌 것으로 나타났으며 최근 가장 빈번히 발견된 유형은 정보 탈취형 악성코드로 암호화폐 지갑, 온라인 뱅킹 정보, 기업 네트워크 침투 등에 광범위하게 활용되고 있다.

[그림 2-2] 유럽연합(EU)의 악성코드 피해 분야



출처: ENISA. (2024). ENISA THREAT LANDSCAPE 2024. p.57

유럽연합(EU)에서 발생한 악성코드의 대표적인 사례를 살펴보면 다음과 같다.

이스라엘의 백도어 전문 제작사인 NSO 그룹이 개발한 Pegasus 스파이웨어는 제로 클릭 방식으로 iMessage나 WhatsApp 취약점을 악용해 피해자의 개입 없이 설치되며, 정치인, 언론인, 인권운동가 등을 대상으로 한 감시 활동에 사용되었다. 2021년 폭로된 Pegasus Project는 스파이웨어의 위험성을 국제사회에 크게 각인시켰다.

RedLine Stealer와 Raccoon Stealer와 같은 정보 탈취형 악성코드는 피싱 이메일과 악성 광고를 통해 확산되며 로그인 정보와 암호화폐 지갑 정보를 대규모로 수집하였다. 특히 Raccoon은 다크웹(dark web)에

서 구독 서비스 형태로 판매되어 사이버 위협의 상업화를 보여주는 사례로 평가된다.

러시아의 샌드웜(Sandworm) 해커그룹은 우크라이나 에너지 인프라를 겨냥하여 HermeticWiper, WhisperGate와 같은 데이터 파괴형 와이퍼 악성코드를 배포했으며, 이는 단순한 금전적 범죄가 아닌 국가 차원의 전략적 사이버 공격 사례로 평가된다.

우리나라의 경우 2025년 상반기 보고된 악성코드 공격은 총 33건이었으며 같은 기간 역대 국내 침해사고 중 가장 큰 규모의 정보 유출 사고로 평가되는 SK텔레콤 유심 정보 유출 사고가 발생하였다. SK텔레콤은 공식적으로 이번 사고가 "신원 미상의 해커가 네트워크에 침입해 악성코드를 설치하고 홈 가입자 인증 서버(Home Subscriber Server)에 저장된 유심 정보들을 외부로 전송한 것"이라는 설명을 공지하였으며, 과학기술정보통신부 등 조사 당국의 발표에 따르면 SK텔레콤 감염 서버 28대에서 BPFDoor 27종, 타이니쉘(TinyShell) 3종, 웹쉘 1종 등 총 33종의 악성코드가 확인되었으며 이로 인해 유심 정보 25종(9.82GB)과 가입자 식별번호(IMSI) 약 2,696만 건이 유출된 것으로 나타났다(과학기술정보통신부, 2025).

다. 사회공학(social engineering)

사회공학(social engineering)은 대상에게 특정 정보를 공개하도록 유도하거나 부당한 이유로 특정 행동을 수행하도록 유도하는 모든 기법으로 공격자는 정보보안 체인에서 가장 약한 고리로 간주되는 인적 요소를 악의적인 목적으로 악용한다(ENISA, 2024, p.69).

사회공학의 대표적인 유형으로는 피싱(phishing), 스피어피싱(spear-

phishing), 스미싱(smishing), 비싱(vishing), 프리텍스팅(pre-texting), 비즈니스 이메일 침해(Business Email Compromise, BEC) 등이 있다.

피싱(phishing)은 수신자를 속여 비밀번호, 신용카드 번호, 개인정보와 같은 민감한 정보를 입력하도록 유도하는 것을 목표로 하며, 공격자는 합법적인 것처럼 보이는 사기성 이메일, 메시지 또는 웹사이트 링크를 사용한다(ENISA, 2024, p.62).

스피어피싱(spear-phishing)은 피싱과 유사하지만 매우 구체적인 타깃을 가지고 있으며 더욱 설득력 있게 보이기 위해 공격자는 조직이나 특정 대상에 대한 정보를 기반으로 메시지를 맞춤 설정하고 종종 공개정보 수집(open-source intelligence, OSINT)을 활용하여 대상을 조사하기도 한다(ENISA, 2024, p.62).

스미싱(smishing)은 평판이 좋은 회사나 신뢰할 수 있는 행위자를 사칭하여 모바일 문자 메시지를 사용하는 공격으로 단문 메시지 서비스(Short Message Service, SMS)와 피싱(phishing)의 합성어이다.

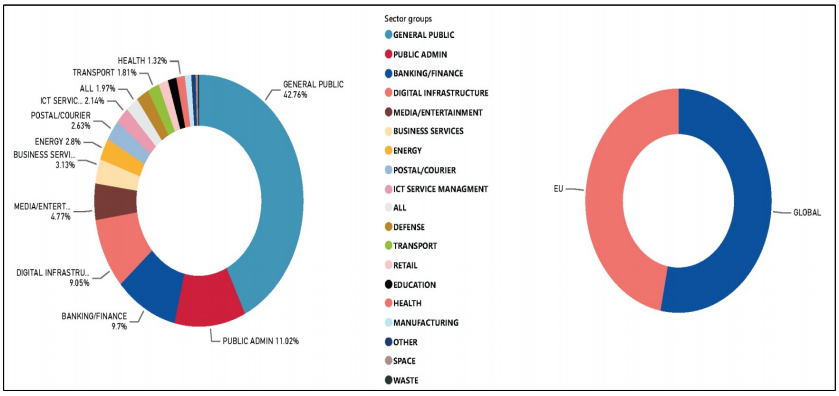
비싱(vishing)은 음성 통신, 특히 전화 통화를 통해 발생하는 피싱의 한 형태로 공격자가 신뢰할 수 있는 기관을 사칭하여 피해자에게 민감한 정보를 공개하도록 유도하는 방식이며 최근에는 인공지능(AI)의 등장으로 기존 음성 녹음 파일을 기반으로 오디오를 생성하는 것이 훨씬 용이해졌다(ENISA, 2024, p.62).

프리텍스팅(pretexting)은 악의적인 공격자가 정보를 얻기 위해 조작된 시나리오를 만들어 온라인이나 오프라인에서 다른 사람인 척하며 신뢰를 얻고 표적을 조종하여 기밀 정보를 공개하거나 특정 행동을 취하도록 유도하는 수법이다(ENISA, 2024, p.62).

비즈니스 이메일 침해(BEC)는 기존 이메일 체인을 활용하여 피해자가 특정 행동을 취하도록 유도하는 프리텍스팅 기법을 사용하기도 하며 비

즈니스 이메일 침해(BEC)의 하위 유형인 CEO 사기는 기업의 CEO 또는 고위 임원을 사칭하여 다른 직원, 파트너 또는 협력업체를 속여 금전을 편취하는 방식으로 이루어진다(ENISA, 2024, p.62).

[그림 2-3] 유럽연합(EU)의 사회공학 피해 분야



출처: ENISA. (2024). ENISA THREAT LANDSCAPE 2024. p.63.

최근에는 인공지능(AI)을 활용해 작성된 고도화된 피싱 메시지와 딥페이크 음성 또는 화상회의를 활용한 새로운 사회공학 기법이 빠르게 확산되고 있다. ENISA(2024)의 보고서에 따르면 사회공학(social engineering)은 특히 일반 대중과 공공행정 분야에 큰 피해를 입힌 것으로 나타났다.

유럽연합(EU)의 대표적 사례를 살펴보면 다음과 같다.

비즈니스 이메일 침해(BEC) 사례로 2023년 유럽의 한 대기업 회계팀이 CEO를 사칭한 공격자의 이메일에 속아 거액을 송금했으며 이 과정에서 공격자는 단순한 이메일 위조를 넘어 딥페이크 음성을 활용해 신뢰를 조작하였다. 또 다른 사례로는 2022년부터 확산된 콜백 피싱이 있다. 이는 이메일에 악성 파일 대신 고객센터 번호를 남겨 피해자가 직접 전화를

걸도록 유도한 후, 공격자가 원격제어 프로그램을 설치하게 만드는 방식으로 기존의 악성 첨부파일 중심 공격보다 탐지를 회피하기 쉽다는 점에서 급속히 확산되었다. 최근에는 SVG 파일과 OneNote 문서를 악용한 피싱 공격도 등장했는데, 겉으로는 무해해 보이는 파일이지만 열람 시 자동으로 악성코드를 다운로드하거나 매크로를 실행하여 감염을 유발했다.

우리나라의 경우에도 피싱(phishing), 스피어피싱(spear-phishing), 스미싱(smishing), 비즈니스 이메일 침해(BEC) 등이 빈번하게 발생하고 있다.

한국인터넷진흥원에 따르면 피싱(phishing) 사이트 차단 건수는 지속적으로 증가하고 있으며 2025년 상반기 피싱 사이트 차단 건수는 9,251건으로 나타났다. 이를 연간으로 환산하면 약 18,000건으로 2024년 13,324건 대비 약 35% 증가할 것으로 예상된다(한국인터넷진흥원, 2025b). 한편 카카오뱅크가 발표한 통계에 따르면 2025년 상반기 'AI 스미싱 문자 확인' 서비스를 통해 6개월 동안 수집된 약 37,000건의 스미싱(smishing) 데이터를 분석한 결과 가장 많이 발생한 스미싱 문구 유형은 개인정보 유출·수집 사칭으로 전체의 37%를 차지해 1위를 기록했으며 금융기관 사칭 19%, 기업 및 광고 사칭 18%, 청첩·부고 등 지인 사칭 12%, 과태료·범칙금 등 단속 사칭 10%, 기타 4% 순으로 나타났다(뉴시스, 2025.7.9.). 또한 기업 타깃형 스피어피싱(spear-phishing) 사례도 보고되고 있다. 중소기업을 대상으로 비즈니스 메일 계정을 탈취하거나 유사 도메인을 활용해 거래처를 속이고, 송금 계좌를 자신이 관리하는 계좌로 변경하여 금전을 편취하는 사례가 보고되어 이에 대한 대응 방안을 마련하고 있다(한국인터넷진흥원, 2025c).

라. 데이터에 대한 위협(threats against data)

데이터에 대한 위협(threats against data)은 데이터에 대한 접근을 차단하거나 시스템 동작을 방해하기 위해 데이터를 조작하는 것을 목표로 하며, 주로 데이터 침해(data breach), 데이터 유출(data leak), 데이터 조작(data manipulation) 등으로 분류될 수 있다(ENISA, 2024, p.69).

데이터 침해(data breach)는 사이버 범죄자가 민감하거나 기밀이거나 보호되는 데이터에 대한 무단 접근 권한을 얻기 위해 실행하는 고의적인 사이버 공격을 의미하며 시스템이나 조직에 대한 고의적이고 강제적인 침입을 통해 데이터를 탈취하는 행위를 의미한다(ENISA, 2024, p.69).

데이터 유출(data leak)은 데이터 노출(data exposure)이라고도 하며 구성 오류, 취약성 또는 인적 오류 등으로 민감하거나 기밀이거나 보호되는 데이터의 의도치 않은 손실 또는 노출을 유발할 수 있는 사건이다(ENISA, 2024, p.69).

한편 새로운 분산 시스템 및 의사결정의 핵심 기술인 머신러닝(ML)/인공지능(AI) 모델의 도입 증가와 최근 대규모 언어 모델(LLM) 및 생성형 인공지능(AI)의 확산으로 인해 데이터 조작(data manipulation)이 새로운 위협으로 주목받고 있다(ENISA, 2024, p.69). 데이터 조작(data manipulation)은 신뢰할 수 있는 데이터를 의도적으로 왜곡하거나 변조하여 머신러닝(ML)/인공지능(AI)의 정확도와 성능, 그리고 사람들의 현실 인식을 표적으로 삼는 공격 유형으로 데이터 포이즈닝(data poisoning), 적대적 공격(adversarial attacks), 정보 조작(information manipulation) 등이 포함된다(ENISA, 2024, p.69).

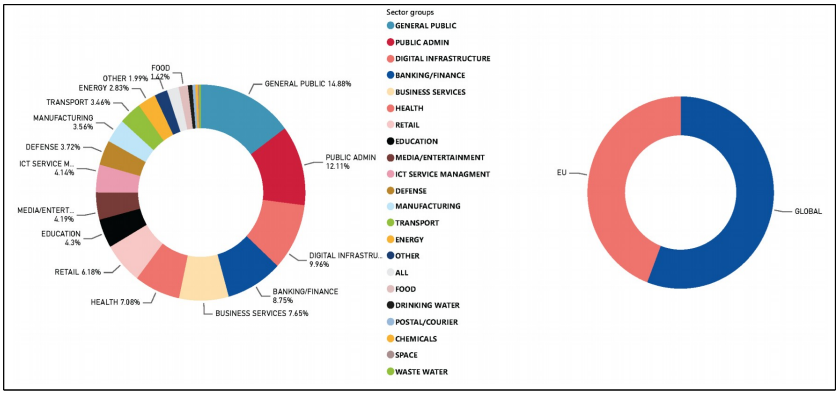
데이터 포이즈닝(data poisoning)은 훈련된 모델의 정확도를 떨어뜨

리거나 추론 시점에 특정 데이터 포인트의 오분류를 유발하기 위해 훈련 데이터를 조작하는 ****훈련 단계 공격(training-time attack)****이며 적대적 공격(adversarial attacks)은 추론 단계에서 특별히 제작된 데이터 포인트를 머신러닝(ML) 모델에 입력하여 잘못된 추론(오분류)을 유발하는 공격이다. 또한 정보 조작(information manipulation)은 특정 사건에 대한 사람들의 인식을 표적으로 삼아 거짓 또는 오해의 소지가 있는 정보를 생성하거나 확산시키는 고의적인 공격이다(ENISA, 2024, p.69). 최근에는 단순한 데이터 유출을 넘어 데이터 무결성을 훼손하는 공격, 나아가 사회적 신뢰를 저해하기 위한 공격으로까지 진화하고 있다.

데이터에 대한 위협은 일반대중, 공공행정, 디지털 인프라 분야 순으로 나타났다.

데이터에 대한 위협의 대표적인 사례로는 러시아-우크라이나 전쟁 과정에서 러시아 측이 허위 이미지와 왜곡된 정보를 대규모로 배포하여 국제 여론을 조작하고 사회적 혼란을 조성하려 시도한 사례가 있다.이는 데이터 무결성뿐만 아니라 사회적 신뢰 자체를 겨냥한 공격으로 평가된다.

[그림 2-4] 유럽연합(EU)의 데이터에 대한 위협 피해 분야



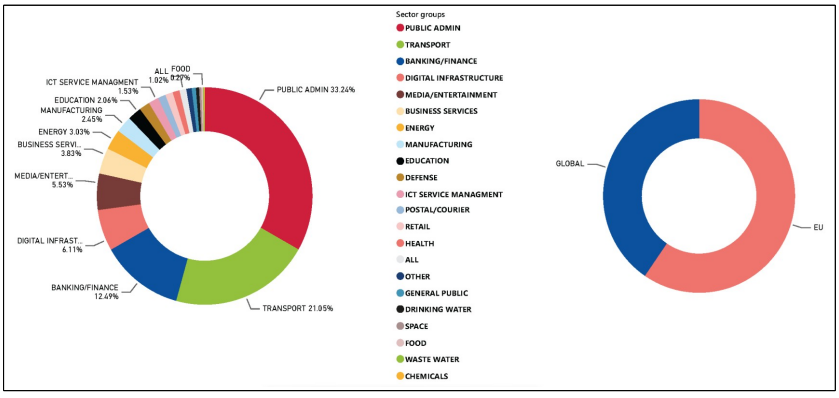
출처: ENISA. (2024). ENISA THREAT LANDSCAPE 2024. p.71.

마. 가용성에 대한 위협(threats against availability: DDoS)

가용성은 수많은 사이버 위협과 공격의 표적이 되며 그중에서도 분산 서비스 거부(Distributed Denial of Service, DDoS) 공격이 두드러진다. 분산 서비스 거부(DDoS)는 시스템 및 데이터의 가용성을 표적으로 삼으며 새로운 위협은 아니지만 현재의 사이버 보안 위협 환경에서 중요한 공격 유형 중 하나로 자리 잡고 있다. 분산 서비스 거부(DDoS) 공격은 시스템 또는 서비스의 리소스를 고갈시키거나 네트워크 인프라에 과부하를 발생시켜 서비스의 정상적인 운영을 방해함으로써 공격 목적을 달성한다(ENISA, 2024, p.78).

분산 서비스 거부(DDoS) 공격은 금전적 이익을 위해 개인이나 기업 등을 대상으로 하였으나, 최근에는 정치적 동기에 의한 공격과 국가의 중요 기반시설을 대상으로 한 공격이 증가하고 있다(ENISA, 2024, p.78). 최근 공격자들은 산 서비스 거부(DDoS)를 주요 공격 이전의 전술적 교란 수단으로 사용하거나 랜섬웨어와 결합하는 형태로 진화하고 있다.

[그림 2-5] 유럽연합(EU)의 가용성에 대한 위협 피해 분야



출처: ENISA. (2024). ENISA THREAT LANDSCAPE 2024. p.80.

유럽연합(EU)의 가용성에 대한 위협의 대표적인 사례를 살펴보면 다음과 같다.

우크라이나 전쟁 이후 친러시아 핵티비스트(hacktivist) 그룹인 Killnet은 유럽 각국의 정부 웹사이트와 금융기관을 대상으로 정치적 메시지를 담은 초당 수백 기가비트(Gbps)에서 수 테라비트(Tbps)에 달하는 대규모 DDoS 공격을 감행하였다. 또 다른 사례로 2023년 이스라엘-하마스 분쟁 발발 직후에도 유사한 패턴이 관찰되었는데, 양측을 지지하는 해커 그룹들이 서로의 공항, 정부기관, 통신사를 상대로 연속적인 분산 서비스 거부(DDoS) 공격을 수행하였다. 특히 이스라엘의 공항 예약 시스템이 일시적으로 마비되면서 국제적 혼란을 초래한 사건은 분산 서비스 거부(DDoS)의 사회적 파급력을 보여준 사례로 평가하고 있다. 최근에는 다크웹(dark web)에서 구독형으로 제공되는 DDoS-for-Hire 서비스가 확산되면서 일정 비용만 지불하면 타인의 웹사이트나 서버를 마비시키는 DDoS 공격 대행이 가능해져 소규모 공격자들도 손쉽게 대규모 공격을 수행할 수 있게 되었으며, ENISA는 이러한 현상을 “위협의 민주화(democratisation of threats)”로 규정하였다.

우리나라에서는 2025년 상반기 분산 서비스 거부(DDoS) 공격이 238건으로 2024년 상반기 대비 55.5% 증가한 것으로 나타났으며 이 중 DNS 서버에 과부하를 유발하는 DNS Query Flooding 공격 유형(71%)이 높은 비중을 차지하는 것으로 확인되었다. 또한 공격 대상 업종의 대부분은 정보통신업에 해당되었다(한국인터넷진흥원, 2025a).

바. 정보 조작 및 간섭(Information Manipulation and Interference)

외국 정보 조작 및 간섭(Foreign Information Manipulation and Interference, FIMI)은 대체로 불법 행위로 분류되지는 않지만 가치, 절차 및 정치적 과정을 위협하거나 부정적인 영향을 미칠 잠재력을 지닌 행동 패턴을 의미한다. 이러한 활동은 의도적이고 조정된 방식으로 수행되며, 국가 행위자(state actors)뿐만 아니라 비국가 행위자(non-state actors)와 그들의 대리인(proxies)에 의해 해당 국가 내외에서 실행될 수 있다(ENISA, 2024, p.91).

ENISA는 '허위정보/오정보(disinformation/misinformation)' 대신 '정보 조작(information manipulation)'이라는 용어를 사용하고 있는데 이는 전달되는 콘텐츠의 진실성 여부보다는 정보를 조작하는 행위 자체에 초점을 두기 위함이다. 또한 ENISA는 정보보안 모델의 세 가지 핵심 요소 중 최소한 하나인 무결성(integrity)에 직접적인 영향을 미치며, 진위(authenticity), 책임성(accountability) 등 다른 사이버 보안 원칙에도 위협이 되기 때문에 사이버 보안 위협으로 간주되어야 한다고 주장하고 있다(ENISA, 2024, p.91).

정보 조작은 의도적이고 조직적으로 수행되는 조작적 성격을 가지며 최근 국제 정세의 변화와 함께 증가하는 경향을 보이고 있다. 최근 정보 조작 사건의 동향을 사례 중심으로 살펴보면 정보 조작은 러시아의 우크라이나 침략 전쟁에서 여전히 핵심 요소로 활용되고 있으며 콘텐츠의 현지화를 강화하는 동시에 러시아의 영향력을 세계적으로 확대하려는 시도가 관찰되고 있다. 또한 특정 뉴스와 관련된 정보 조작이 증가한 것으로 나타나는데, 이는 2024년에 선거를 비롯한 여러 주요 사건이 발생했기 때문인 것으로 분석된다.

정보 조작은 광범위한 디지털 네트워크를 통해 지속적으로 확산되고 있으며 가짜 계정과 허위 웹사이트의 활용 사례가 다수 확인되고 있다. 최근 인공지능(AI)을 활용한 정보 조작 사례도 관찰되고 있으나 아직까지는 제한적인 규모로 평가되고 있다. 다만 우리나라의 경우 아직까지 정보 조작이나 간섭을 사이버 보안 위협의 영역으로 체계적으로 분류하거나 관리하고 있지는 않은 것으로 보인다.

제2절 의료 분야 정보 공유·분석센터(ISAC)

1. ISAC의 개념

정보 공유·분석센터(Information Sharing & Analysis Center, ISAC)의 개념을 최초 정립한 국가는 미국이다. 1998년 미국의 빌 클린턴 대통령이 발표한 '대통령 결정 지침 63호(Presidential Decision Directive 63, PDD-63)'에 따라 미국의 중요 인프라시설을 사이버 및 물리적 보안 위협과 기타 위험으로부터 보호하기 위해 실행 가능한 위협 정보를 수집·분석하여 이를 회원들에게 공유하고 위험을 완화하며 복원력을 강화할 수 있는 도구를 제공하는 기관을 설립할 것을 권고하였으며 이에 따라 설립된 것이 정보 공유·분석센터(ISAC)이다(NCI, 2025). 이에 1998년 미국 연방정부는 각 주요 인프라시설 분야에서 위협과 취약성에 대한 정보를 공유하기 위한 분야별 정보 공유·분석센터(ISAC)를 설립하도록 요청하였으며 2025년 9월 기준 총 28개 분야의 정보 공유·분석센터(ISAC)가 설립되어 운영되고 있다(표 2-2 참조).

〈표 2-2〉 미국의 정보 공유·분석센터(ISAC)

구분	주요 회원	역할
American Chemistry Council	화학 관련 기업들	- 회원 기업을 위한 옹호 활동, 정보 공유, 과학 연구, IT/보안 이슈 대응 등 지원
Automotive ISAC	자동차 제조업체, 부품업체, 운송사 등	- 자동차 산업 전반의 사이버 위협, 취약성, 모범사례 등 공유 및 협업 플랫폼 제공
Aviation ISAC	민간 및 상업 항공사, 항공 관련 기업	- 항공산업 보안 위협 정보를 분석·공유하고 대응 역량을 강화하는 기능 제공
Communications ISAC	통신사, 인터넷 서비스 제공자, 방송사 등	- 통신 인프라의 위협·침입·이상 징후를 수집, 분석, 경고·전파; 통신 인프라의 안정성 유지

구분	주요 회원	역할
Downstream Natural Gas ISAC	가스 배급 회사, 천연가스 유틸리티	- 위협 정보 배포, 분석, 정부 및 전력 부문과의 협업 조정 역할 수행
Elections Infrastructure ISAC	선거 관리 기관, 기술 공급업체, 보안 전문가 등	- 미국 선거 인프라의 보안 강화, 위협 정보 공유, 교육 및 기술 통제 지원
Electricity ISAC	전력 및 천연가스 설비 운영 기관 등	- 전력망 및 연계 인프라의 사이버/물리 위협 대응을 위한 분석, 경고, 정보 공유 기능 수행
Emergency Management & Response ISAC	응급 서비스 부문 기관들	- 응급 서비스 섹터 관련 위협·위험 정보를 수집·분석·전파하며 대응 역량 강화
Financial Services ISAC	은행, 증권사, 금융기관 등	- 금융 인프라의 지속성 유지, 위협 정보 교환, 대응 훈련, 회원 간 협업 증진
Food & Agriculture ISAC	식품, 농업 기업 및 관련 조직	- 식품·농업 분야의 위협 인텔리전스 제공, 보안 관행 공유, 사고 대응 지원
Healthcare Ready	의료 공급망 관련 기관, 공공 보건	- 의료 공급 안정성 강화, 재난 전후 협업, 보건 부문 복원력 강화
Health ISAC	병원, 의료기술 업체, 제약사, 실험실 등	- 보건 분야의 사이버 및 물리적 위협에 대한 신속한 정보 공유, 대응 체계 구축
Information Technology ISAC	IT 기업들, 기술 인프라 운영자	- 위협 인텔리전스 공유, 분석, 자동화된 공유 플랫폼 운영, 보안 정책 조율
Maritime ISAC	해운 회사, 항만 시설, 물류업체 등	- 해양 및 해운 분야의 보안 이슈 대응, 정부 및 업계 간 연결 및 정보 공유
Maritime Transportation System ISAC	해운 커뮤니티, 항만·터미널 등	- 해양 운송 사이버 보안 공유, 위협 식별, 회원 간 협업 강화
Media & Entertainment ISAC	영화사, 방송사, 출판사, 콘텐츠 제작/배포자 등	- 미디어/엔터테인먼트 산업의 데이터 유출, 사이버 공격, 콘텐츠 보호 등을 위한 정보 공유 플랫폼 제공
Multi-State ISAC	미국 주, 지방정부, 부족 정부 등	- 지방정부 수준의 사이버 위협 감시, 실시간 모니터링, 취약점 식별 및 대응 지원
National Defense ISAC	국방 관련 기업, 방위 산업체, 전략적 파트너 등	- 방위 산업 보안 강화, 위협 공유, 방위 기반 산업에 특화된 대응 체계 구축
Oil & Natural Energy ISAC	석유, 천연가스 산업 전반의 기업	- 탐사, 생산, 정유, 운송 등 석유 에너지 산업의 사이버 위협 대응 및 인텔리전스 공유

구분	주요 회원	역할
Public Transportation & Over-the-Road Bus ISAC	대중교통 운영사, 버스 운송사 등	- 교통 운송 부문의 물리/사이버 위협 정보 공유, 분석 및 대응 지원
Real Estate ISAC	상업용 부동산 운영사, 건물주, 리조트, 쇼핑몰 등	- 테러 위협, 침입, 취약성 등에 대한 정보 공유 및 대응 계획 지원
Research & Education Networks ISAC	대학, 연구기관, 교육 네트워크	- 교육/연구기관 대상 사이버 위협 분석 및 공유, 모니터링, 보안 역량 강화 지원
Retail & Hospitality ISAC	소매 기업, 호텔, 여행업, 소비자 서비스 업체 등	- 소비자 연계 산업의 보안 위협 공유, 모범사례 개발, 협업 강화
Small Broadband Provider ISAC	중소 인터넷 서비스 사업자, 통신망 운영자	- 중소 통신업자가 직면한 위협 인지 및 대응, 정보 공유 및 기술 지원 제공
Space ISAC	우주 산업체, 위성 기업, 연구소 등	- 우주 시스템의 물리·사이버 위협 공유, 사고 대응, 커뮤니케이션 역할 수행
Surface Transportation ISAC	철도, 트럭 운송, 화물 운송업체 등	- 육상 운송 및 물류 분야의 사이버/물리 위협 대응 역량 강화 및 정보 공유
Tribal ISAC	미국 부족 정부 및 부족 운영 조직	- 부족(종족) 정부 간 위협 정보 공유, 보안 역량 강화, 정부-업계 협업 촉진
Water ISAC	상·하수도 유틸리티, 물 관리 기관	- 수처리 및 상하수도 시스템의 사이버/물리 위협 경고, 복원력 강화, 보안 정보 제공

출처: 미국 정보 공유·분석센터(ISAC) 국가협의회 홈페이지.
https://www.nationalisacs.org/members

미국의 정보 공유·분석센터(ISAC)는 분야별로 제공되는 서비스에 다소 차이가 있으나 일반적으로 중요 인프라 시설의 소유자 및 운영자가 물리적 및 사이버 위협과 이에 대한 완화 방안에 관한 정보를 공유하고 우수 사례를 확산하기 위한 설립 취지에 따라 위험 완화, 사고 대응, 정보 공유 등 중요 인프라 시설 보호를 위한 다양한 서비스를 제공하고 있다(NCI, 2025).

한편 우리나라는 「정보통신기반 보호법」 제16조 제1항에 따라 금융·

통신 등 분야별 정보통신기반시설을 보호하기 위해 취약점 및 침해 요인과 그 대응 방안에 관한 정보 제공과 침해사고 발생 시 실시간 경보 및 분석 체계 운영 등의 업무를 수행하는 정보 공유·분석센터(ISAC)를 구축·운영하고 있다(정보통신기반 보호법, 2025).

〈표 2-3〉 정보 공유·분석센터(ISAC) 구축 및 운영 근거

정보통신기반 보호법
제16조(정보공유·분석센터) ① 금융·통신 등 분야별 정보통신기반시설을 보호하기 위하여 다음 각호의 업무를 수행하고자 하는 자는 정보공유·분석센터를 구축·운영할 수 있다. 1. 취약점 및 침해요인과 그 대응방안에 관한 정보 제공 2. 침해사고가 발생하는 경우 실시간 경보·분석체계 운영 ② 삭제 〈2015. 12. 22.〉 ③ 삭제 〈2015. 12. 22.〉 ④ 정부는 제1항 각호의 업무를 수행하는 정보공유·분석센터의 구축을 장려하고 그에 대한 재정적·기술적 지원을 할 수 있다. 〈개정 2015. 12. 22.〉 ⑤ 삭제 〈2015. 12. 22.〉

출처: 정보통신기반 보호법. (법률 제20068호. 2024. 1. 23., 일부개정)

우리나라의 경우 2002년에 설립된 정보통신 분야 정보 공유·분석센터(ISAC)를 시작으로 2025년 9월 기준 정보통신, 금융, 지자체, 의료 등 4개 분야의 정보 공유·분석센터(ISAC)를 운영하고 있다.

〈표 2-4〉 우리나라 정보 공유·분석센터(ISAC)

구분	주요 회원	역할
금융 ISAC	은행, 증권사, 보험사 및 전자금융업 등	- 금융권 통합보안관제 구축 및 운영 - 사이버 위협 정보 공유 - 침해 행위 탐지 및 분석 최신탐지기법 개발 및 적용
정보통신 ISAC	정보통신사업자	- 통신사 간 위협 정보 수집 및 공유, 침, 사이버 위협 경보 - 통신 기반시설 침해사고 분석 및 복구지원, 초기 대응 체계 강화, 침해사고 경보 - 회원사 취약점 분석 및 평가
지자체 ISAC	지방자치단체	- 지자체 간 위협 정보 수집 및 상황 공유, 취약점 대응 방안 제공 - 주요 기반시설 대상 침해사고 대응 훈련, 복구계획 지원, 회원사 간 실시간 위협정보 공유

구분	주요 회원	역할
의료 ISAC	상급종합병원, 종합병원	- 의료기관 간 위협 정보 수집 및 공유보안 취약점 경고 - 의료기관 침해사고 신고·점수 초기 대응 및 복구 지원 - 의료기관 취약점 점검 및 분석

출처: 금융보안원 홈페이지(https://www.fsec.or.kr/bbs/101)

2. 한국: 의료정보보호센터

앞서 설명한 바와 같이 우리나라는 「정보통신기반 보호법」 제16조에 따라 의료 분야 정보보호 강화를 위하여 2018년 의료기관공동보안관제센터를 설립하였으며, 2023년 진료정보침해대응센터와 의료기관공동보안관제센터를 통합하여 의료정보보호센터를 신설하였다.

〈표 2-5〉 의료법에서 규정하고 있는 의료 ISAC의 업무 및 위탁운영 등

의료법
제23조의3(진료정보 침해사고의 통지) ① 의료인 또는 의료기관 개설자는 전자의무기록에 대한 전자적 침해행위로 진료정보가 유출되거나 의료기관의 업무가 교란·마비되는 등 대통령령으로 정하는 사고(이하 "진료정보 침해사고"라 한다)가 발생한 때에는 보건복지부장관에게 즉시 그 사실을 통지하여야 한다. ② 보건복지부장관은 제1항에 따라 진료정보 침해사고의 통지를 받거나 진료정보 침해사고가 발생한 사실을 알게 되면 이를 관계 행정기관에 통보하여야 한다. **제23조의4(진료정보 침해사고의 예방 및 대응 등)** ① 보건복지부장관은 진료정보 침해사고의 예방 및 대응을 위하여 다음 각 호의 업무를 수행한다. 1. 진료정보 침해사고에 관한 정보의 수집·전파 2. 진료정보 침해사고의 예보·경보 3. 진료정보 침해사고에 대한 긴급조치 4. 전자의무기록에 대한 전자적 침해행위의 탐지·분석 5. 그 밖에 진료정보 침해사고 예방 및 대응을 위하여 대통령령으로 정하는 사항 ② 보건복지부장관은 제1항에 따른 업무의 전부 또는 일부를 전문기관에 위탁할 수 있다. ③ 제1항에 따른 업무를 수행하는 데 필요한 절차 및 방법, 제2항에 따른 업무의 위탁 절차 등에 필요한 사항은 보건복지부령으로 정한다.
의료법 시행규칙
제16조의4(진료정보 침해사고의 예방 및 대응을 위한 업무의 위탁) 보건복지부장관은 법 제23조의4제2항에 따라 같은 조 제1항 각 호에 따른 진료정보 침해사고의 예방 및 대응을 위한 업무를 「사회보장급여의 이용·제공 및 수급권자 발굴에 관한 법률」 제29조에 따른 한국사회보장정보원에 위탁한다.

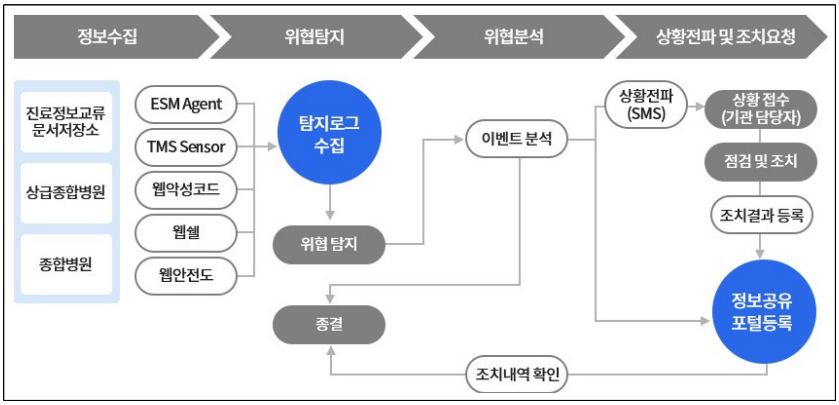
출처: 의료법, 법률 제18289호 (2025); 의료법 시행규칙, 보건복지부령 제970호 (2025).

우리나라의 의료 분야 정보 공유·분석센터(ISAC)인 의료정보보호센터의 업무는 「의료법」 제23조의3과 제23조의4에 규정되어 있으며 「의료법 시행규칙」 제16조의4에 따라 한국사회보장정보원이 위탁받아 운영하고 있다(표 2-5 참조).

의료정보보호센터의 주요 업무는 보안관제, 정보 공유, 침해 대응, 교육 및 훈련 등 4가지로 구분할 수 있다.

첫째, 보안관제는 회원이 보유한 시스템과 네트워크 자원의 손상을 방지하기 위하여 실시간으로 사이버 위협을 모니터링하고, 즉각적으로 대응 및 관리하기 위한 일련의 모든 활동을 말한다(의료정보보호센터, 2025). 의료정보보호센터는 회원(의료기관)의 정보시스템에 대한 24시간 365일 사이버 침해 대응 보안관제 서비스를 제공하고 있으며, 보안관제를 통해 탐지된 이벤트 중 침해 행위로 의심되는 건에 대해 분석을 수행하고 점검 또는 조치를 요청하거나 권고하고 있다(의료정보보호센터, 2025).

[그림 2-6] 의료 ISAC 보안관제 절차



출처: 의료정보보호센터. (2025). 의료정보보호센터 홈페이지. https://www.hisc.or.kr/page/subPage.do?page=sub4_1&muNo=6&muGpNo=5&muPrNo=5

정보 공유 업무는 국내외에서 발생하거나 생성되는 사이버 위협 정보를 산업 분야 간 또는 동일 산업 내에서 상호 공유하는 서비스로 의료정보보호센터는 다양한 채널로부터 수집·분석한 위협 정보를 의료 분야 희망 기관에 무상으로 제공하고 있다(의료정보보호센터, 2025).

〈표 2-6〉 의료 ISAC 정보 공유 유형

구분	설명
사이버 위협정보	- 보안관제에서 탐지된 사이버 위협(악성코드 분석 등) 정보 - 공격시도 IP 차단 요청 - C&C(Command & Control) IP·도메인 차단 요청
보안이슈	- 랜섬웨어 확산 - 주요시설 대상 DDoS 발생
보안권고	- 아파치 스트럿츠(Apache Struts) 취약점 및 업데이트 권고 - 워드프레스 취약점 및 업데이트 권고
보안뉴스	- 의료보안 뉴스클리핑
보안동향·기술정보	- 월간 공격 서비스(포트) 동향 및 분석

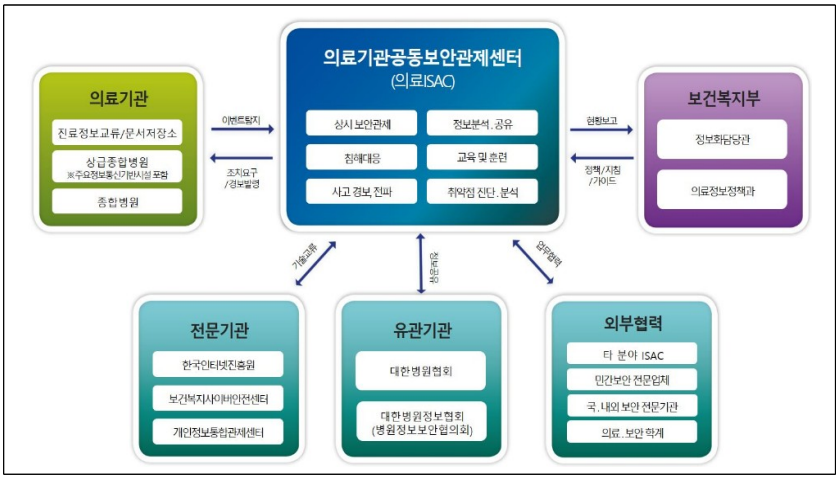
침해 대응 업무는 침해사고 예방 업무와 침해 대응 업무로 구분할 수 있다. 의료정보보호센터의 침해사고 예방 업무는 대내외 위협 상황 발생 시 회원기관에 위기 단계별(관심 → 주의 → 경계 → 심각) 경보를 발령하고 대처 요령을 전파하는 것이다. 한편 의료기관 정보시스템을 대상으로 사이버 침해사고가 발생할 경우 ① 침해사고 신고 접수, ② 초기 대응 지원 및 필요 시 현장 조사를 통한 사고 원인 분석 및 조치 지원, ③ 의료기관의 데이터 및 시스템 복구를 위한 계획 수립 지원, ④ 침해사고 확산 또는 재발 방지를 위한 대책 수립 지원 등 침해 대응 업무를 수행한다.

교육 및 훈련 업무로는 정보보호 책임자를 대상으로 의료 분야를 포함한 다양한 산업 분야의 최신 정보보호 동향 및 신규 위협 정보에 대한 교육, 의료기관 정보보호 담당자를 대상으로 한 침해사고 대응 능력 향상을 위한 정보보호 전문 기술 교육, 그리고 사이버 위기 발생 시 대응 역량 강

화를 위한 모의 침투 등 위기 대응 모의훈련을 실시하고 있다.

의료정보보호센터의 주요 업무 구성도는 〔그림 2-7〕과 같다.

〔그림 2-7〕 의료 ISAC 업무 구성도



출처: 한국사회보장정보원. (2025). 한국사회보장정보원 홈페이지. 2025.11.2. 인출. https://www.ssis.or.kr/lay1/S1T748C1588/contents.do

의료정보보호센터의 회원 구성은 상급종합병원과 종합병원이며, 2024년 말 기준 상급종합병원 45개 중 27개(60.0%), 종합병원 267개 중 19개(7.1%)가 회원으로 가입되어 있다.

3. 미국: Health-ISAC

미국의 의료 분야 정보 공유·분석센터(ISAC)인 Health-ISAC은 앞서 설명한 바와 같이 미국의 28개 분야별로 설립된 정보 공유·분석센터(ISAC) 중 하나로 비영리 민간 부문 회원 중심 조직으로서 사이버 및 물리적 보안 사건을 예방·탐지·대응할 수 있도록 글로벌 건강 부문에서 신

뢰할 수 있는 협력 관계를 강화하여 회원들이 생명을 구하는 데 집중하도록 지원하고 있다(Health-ISAC, 2025a).

Health-ISAC의 목적은 건강 부문에 대한 사이버 및 물리적 보안 위협에 대한 상황 인식(situational awareness)을 제공하는 데 있으며, 이를 통해 회사들이 운영상의 회복력을 보장하기 위해 위협을 감지·완화·대응할 수 있도록 지원하는 것이다. 또한 전 세계 수천 명의 건강 보안 전문가를 연결하여 신뢰할 수 있는 협력 환경에서 동료의 통찰력, 실시간 알림 및 모범 사례를 공유하도록 지원하고 있다(Health-ISAC, 2025a).

Health-ISAC의 주요 업무는 위협 정보 공유, 교육 및 프로그램, 사이버 위협 경보 시스템, 보안 컨설팅 등 4가지로 구분할 수 있다.

위협 정보 공유 업무는 의료산업과 관련된 사이버 위협 정보를 수집·분석하여 회원사에게 실시간으로 제공함으로써 잠재적 위협에 대한 신속한 대응을 지원하는 활동이다.

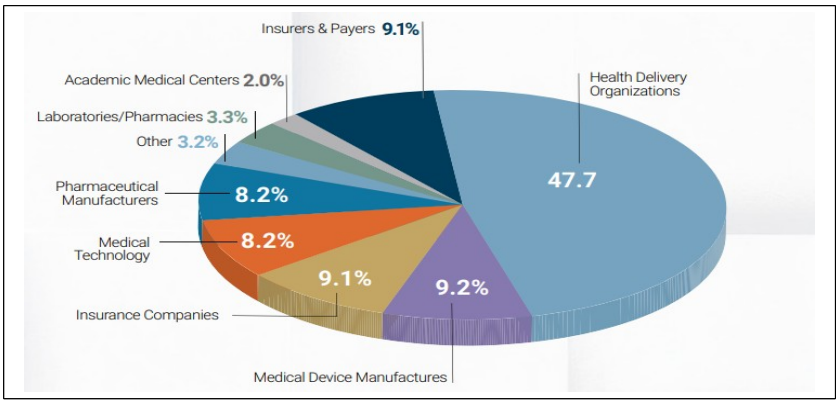
교육 및 프로그램 업무는 회원사들의 보안 인식을 높이기 위해 정기적인 교육 세션과 훈련 프로그램을 운영하여 최신 보안 동향과 대응 방안을 공유하는 활동이다.

사이버 위협 경보 시스템 업무는 새로운 위협이 발견되면 즉각적인 경보를 발령하여 회원사들이 신속하게 대응할 수 있도록 지원하는 활동이다.

보안 컨설팅은 회원사들의 보안 취약점을 평가하고 개선 방안을 제시하는 맞춤형 보안 컨설팅 서비스이다.

Health-ISAC의 회원 구성은 의료서비스 제공자, 의료기기 제조업체, 보험사, 제약회사 및 의료 기술 회사 등이며, 2024년 기준 전 세계 140개국 이상에 분포해 있으며 약 12,000명의 보안 전문가가 Health-ISAC 네트워크에 포함되어 있다(Health-ISAC, 2025b, p.3).

[그림 2-8] Health-ISAC 회원구성 비율



출처: Health-ISAC. (2025b). Health-ISAC. 2024 Annual Report. p.5

4. 유럽: ENISA, EH-ISAC[1)]

유럽연합 사이버 보안청(European Union Agency for Cybersecurity, ENISA)은 유럽 전역에 걸쳐 높은 수준의 사이버 보안을 공통적으로 달성하기 위해 설립된 유럽연합(EU) 산하 기관으로, 2004년 '유럽 의회 및 이사회 규정 Regulation (EC) No 460/2004'에 따라 임시 조직으로 설립되었으나, 2019년 '유럽 의회 및 이사회 규정 2019/881(Regulation (EU) 2019/881)'에 따라 영구적인 조직으로 목표, 역할과 임무를 재정립하였다. 동 법에서는 유럽연합의 사이버 보안 정책 및 법률의 개발 및 이행(제5조), 회원국의 사이버 보안 역량 강화 지원(제6조), 유럽연합 차원의 운영 협력(제7조), 사이버 보안 인증 및 표준화(제8조), 사이버 보안완 관련 지식 및 정보 제공(제9조), 사이버 보안 인식 제고 및 교육(제10조), 사이버 보안 연구 및 혁신(제11조), 국제협력(제12조)을 유럽연합 사이버

1) ENISA 공식 홈페이지 및 EU 사이버보안법(Regulation (EU) 2019/881) 기반 작성

보안청(ENISA)의 과업으로 규정하고 있다.

유럽연합 사이버 보안청(ENISA) 주요 업무를 구체적으로 살펴보면 다음과 같다.

첫째, 유럽연합 집행위원회(European Commission, EC), 의회(European Parliament, EP) 및 회원국의 사이버 보안 정책 및 법령 수립을 지원하고 있다.

둘째, 사이버 보안과 관련하여 현장 대응 조직인 컴퓨터 긴급 대응팀(Computer Emergency Response Team, CERT)과 컴퓨터 보안사고 대응팀(Computer Security Incident Response Teams, CSIRT)을 지원하고, 사고 대응 절차 마련 및 가이드라인 제공 등 기술적·운영적 지원을 수행하고 있다.

셋째, 유럽연합의 공통 사이버 보안 인증 체계(ENISA Certification Framework)를 개발·관리하는 등 사이버 보안 관련 인증 및 표준화 업무를 수행하고 있다.

넷째, 사이버 보안 전문 인력 양성, 국가별 역량 평가, 연합훈련(Cyber Europe) 운영 등 사이버 보안 역량 강화와 교육·훈련을 수행하고 있다.

다섯째, 산업계, 학계, 정부 간 위협 정보, 모범사례, 관련 통계 공유 등 정보 허브 및 국제협력을 지원하고 있다.

종합하면 유럽연합 사이버 보안청(ENISA)은 유럽연합 전역의 사이버 보안 관련 정책, 인증, 역량 강화 및 조정 등을 목적으로 정책, 기술, 산업 그리고 회원국 간의 협력 허브로서 유럽의 대표적인 사이버 보안 실행기관의 역할을 수행하고 있다.

EH-ISAC(European Health Information Sharing & Analyses Center)은 유럽 의료기관, 국가 및 부문별 컴퓨터 보안사고 대응팀(CSIRT), 유럽연합 사이버 보안청(ENISA)이 함께 참여하는 협의체로 유

럽연합(EU) 전역의 보건 분야에서 사이버 보안과 복원력을 개선하는 데 주력하고 있다. 유럽연합 사이버 보안청(ENISA)이 법률에 의해 설립된 유럽연합(EU)의 사이버 보안을 전담하는 공공기관인 반면, EH-ISAC는 건강 분야에 특화된 비영리 정보 공유 조직으로 강제적 권한이 없고, 회원 자율 참여를 기반으로 운영되고 있다. 이에 EH-ISAC과 유럽연합 사이버 보안청(ENISA)는 유럽 의료 부문의 사이버 보안 강화를 목표로 협력하는 관계이며, EH-ISAC의 회원 구성은 2025년 9월 현재 12개국 20개 기관, 총 32명으로 구성되어 있다.

5. 일본: Health ISAC Japan

일본은 의료 분야에서 정보보안의 중요성을 계발하기 위해, 2013년에 설립된 메디컬 IT 보안 포럼(MITSF)을 전신으로 하여, 2019년 10월에 '의료 ISAC(医療ISAC)'로 개칭하였으며, 2025년 9월부터는 'Health ISAC Japan'으로서 새로운 체제로 활동하고 있다(Health ISAC Japan, 2025).

Health ISAC Japan는 비영리 일반사단법인으로 운영되고 있다. 동 기관의 정관 제3조에 따르면 Health ISAC Japan은 의료·헬스케어 영역에서 IT 보안의 계발 활동을 수행하고, 이 분야에 종사하는 사람들과 관련 단체의 리터러시를 향상시키는 것을 목표로 하며, 그 목적에 기여하기 위해 Health ISAC Japan의 역할과 관련된 7가지 사업을 명시하고 있다(Health ISAC Japan, 2025). 즉, Health ISAC Japan의 주요 업무는 IT 보안에 관한 세미나 개최(제1호), IT 보안에 관한 조사 연구, 정보 수집, 정보 제공 및 컨설팅(제2호), IT 보안에 관한 정부 기관 등에 대한 제안 및 요청(제3호), IT 보안에 관한 간행물의 발행 및 판매(제4호), IT 보

안 관련 시스템, 소프트웨어, 네트워크 등의 개발 및 운영(제5호), IT 보안 관련 제품 및 서비스의 성능 테스트 및 인증(제6호), 전 각 호에 부대 관련되는 일체의 사업(제7호) 등이다.

Health ISAC Japan은 2019년 미국의 Health ISAC과의 제휴를 통해 보건의료 사이버 보안 관련 콘텐츠를 일본에 제공하는 활동을 수행하고 있다. 예를 들어 전 세계 Health ISAC 커뮤니티의 일일 보고서, 보건의료 해킹 관련 블로그(Hacking Healthcare blog), 위협 인텔리전스 알림 등의 일본어 번역 및 제공 서비스를 수행하고 있다. 또한 사이버 보안 관련 정기 세미나 및 워크숍, 보안 교육 프로그램을 운영하고 있으며, 보건의료 현장의 사이버 보안 과제에 대한 정책 개발 및 제언, 의료기기 및 의료기관 관련 가이드라인 개발, 의료기관 등을 대상으로 한 사이버 보안 관련 각종 조사를 수행하고 있다(Health ISAC Japan, 2025).

6. 호주: 보건사이버공유네트워크(HCSN)

보건사이버공유네트워크(Health Cyber Sharing Network, HCSN)는 '2023-2030 호주 사이버 안보 전략(2023-2030 Australian Cyber Security Strategy)'의 일환으로 호주 내무부(Australian Department of Home Affairs)의 자금 지원을 받아 CI-ISAC(Critical Infrastructure Information Sharing & Analysis Center)가 운영하는 시범 사업으로 2025년부터 2027년까지 3년간 운영될 계획이다.

보건사이버공유네트워크(HCSN) 시범 사업의 목적은 보건 부문 내 협업, 정보 공유, 사이버 위협 대응 역량 및 모범 사이버 보안 관행을 개선하고, 산업 내·산업 간·정부와의 사이버 위협 인텔리전스(CTI)를 공유할 수 있는 대안적 메커니즘을 구축하며, 보조금 지원 기간 종료 이후에도

지속 가능한 자립형 ISAC을 구축하는 데 있다.

보건사이버공유네트워크(HCSN)의 연도별 목표 및 역량 구축 로드맵은 〈표 2-7〉과 같다.

〈표 2-7〉 호주 보건사이버공유네트워크(HCSN) 연도별 목표 및 로드맵

구분	2025년	2026년	2027년
보건 부문 내 협업, 정보 공유, 사이버 위협 대응 역량 및 모범 사이버 관행 개선	- 20~30개 의료기관 대상으로 시범 운영 완료 - 공동 설계 단계 완료 - 사이버 지식 기반	- 사이버 훈련(Cyber Exercising) 역량 강화 - 사이버 교육(Cyber Training)	- 추가 사이버 자원 및 역량 확충
산업 내/산업 간/정부와의 사이버 위협 인텔리전스(CTI)를 공유할 수 있는 대안적 메커니즘	- TISN, DHA, 산업 그룹 통합 - 보건 특화 인텔리전스 통합	- '대규모 공유' 개시 - 추가 협업 기회 마련	- 공격표면(attack surface) 모니터링 - 유출 자격 증명(leaked credential) 모니터링
보조금 지원 기간 종료 시 자립형 ISAC 설립			- 보건 부문 전반으로 채택 확대

출처: HCSN. (2025). Collective Defence for Health Critical Infrastructure. https://ci-isac.org.au/wp-content/uploads/2025/02/HCSN-Information-Pack.pdf

호주의 보건사이버공유네트워크(HCSN)은 설립 후 본격적으로 업무를 수행하는 초기 단계로, 아직은 주요 업무에 대한 실적 보고가 충분하지 않은 상황이다.

제3절 선행 연구 검토

1. 의료기관의 사이버 공격 동기

의료기관의 의료데이터는 환자의 질병정보 및 건강 정보 등 민감한 개인정보를 포함하고 있어 다크웹(dark web)에서 금융 데이터보다 높은 가치를 지니며 사이버 범죄자들에게 매력적인 표적이 되고 있다.

Wasserman, & Wasserman(2022)는 구조화된 문헌검색을 통해 의료기관 사이버 공격의 동기를 재정적 목적, 정치적 목적, 서비스 중단, 화이트햇 액터 등 4가지로 세분화하여 설명하고 있다.

첫째, 재정적 목적은 사이버 공격자의 가장 흔한 동기인 금전적 이득으로 의료기관을 대상으로 탈취한 데이터의 몸값을 요구하거나 다른 범죄 목적을 위해 제3자에게 데이터를 판매할 수 있다(Wasserman, & Wasserman, 2022).

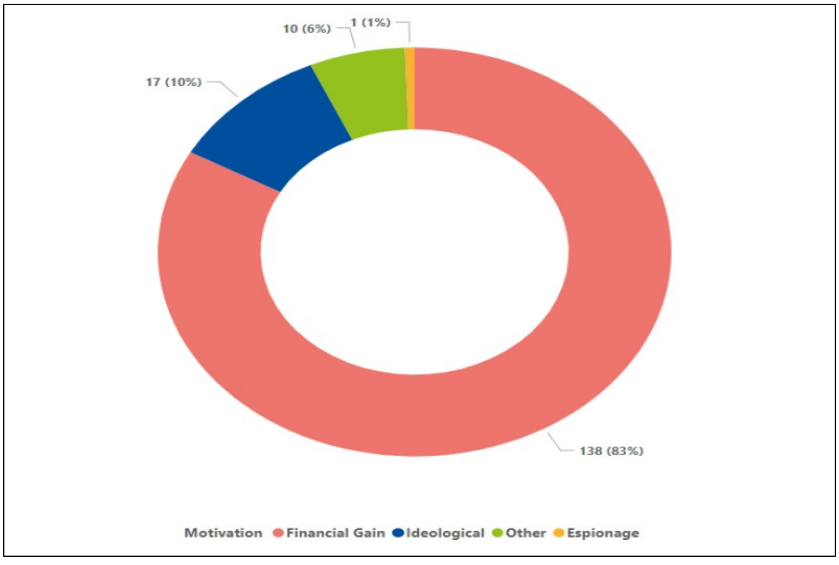
둘째, 정치적 목적은 국제 전쟁 중에 상대 국가가 국민에게 의료서비스를 제공하는 것을 방해하거나 의료기기 작동을 변경하여 상대 국가의 국민에게 해를 끼칠 수도 있고, 기밀정보를 폭로하려고 시도할 수도 있다(Wasserman, & Wasserman, 2022). 또한 국내 정치적 동기를 가진 공격 사례도 존재한다. 2014년 보스턴 어린이 병원에서 발생한 사건은 자녀 양육권 사건 처리 방식에 대한 불만을 표출하기 위해 공격자가 주도한 사례이다(Wasserman, & Wasserman, 2022).

셋째, 서비스 중단은 사이버 범죄자가 의료서비스의 운영을 방해할 목적으로 수행하는 공격으로 개인적인 즐거움을 위해 수행될 수도 있으며, 병원이나 의사의 대응에 대한 불만이나 보복의 성격을 가질 수도 있다(Wasserman, & Wasserman, 2022).

넷째, 화이트햇 액터(White Hat Actor)는 선한 의도를 가지고 사이버 보안 활동을 수행하는 전문가를 의미하며, 악의적 의도가 없는 해커가 병원 네트워크의 취약점을 발견하여 악의적인 해커가 이를 악용하기 전에 문제를 해결하려는 경우를 말한다.

한편 ENISA(2023) 보고서에서는 2021년 1월부터 2023년 3월까지 유럽연합(EU)의 의료기관을 대상으로 한 사이버 공격의 동기를 '금전적 이득', '이념적 행위', '기타 행위', '알 수 없음' 등 4가지로 세분화하여 설명하고 있다. '금전적 이득'은 사이버 공격의 근간이 분명히 금전적 이득에 있는 경우로 83%를 차지하였으며, '이념적 행위'는 공격이 핵티비스트 활동과 연관되어 있고 공격자가 공격 목적을 명확히 밝힌 경우로 10%를 차지하였다. 또한 '기타 행위'는 사고가 의도치 않은 경우로 6%, 동기에 대한 명확한 결론을 내릴 수 없는 '알 수 없음'의 경우 1%로 나타났다.

[그림 2-9] 유럽연합(EU) 의료기관을 대상으로 한 사이버 공격 동기



출처: ENISA. (2023). ENISA Threat LANDSCAPE: HEALTH SECTOR. p.19.

의료기관을 대상으로 한 사이버 공격의 가장 큰 동기는 금전적 이득을 얻기 위한 것이다. 다만 최근에는 정치적·이념적 목적, 개인적인 보복이나 자기만족을 위한 서비스 중단, 그리고 이유를 알 수 없는 공격 등도 사이버 공격의 동기로 나타나고 있다.

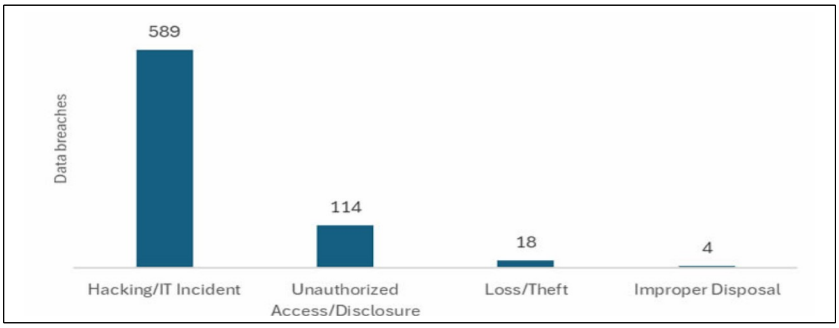
2. 의료기관의 사이버 침해사고 현황

유럽집행위원회(EC)는 2023년 한 해 동안 유럽연합(EU) 국가들이 의료 분야를 대상으로 한 중대한 사이버 보안 사고 309건을 보고하였으며, 이는 다른 어떤 중요 분야보다도 많은 수치였다고 발표하였다(European Commission, 2025). 의료서비스 제공자들이 디지털 건강 기록(digital health records)을 점점 더 많이 사용함에 따라 데이터 관련 위협의 위험도 계속 증가하고 있으며, 이로 인해 전자 건강 기록, 병원 워크플로우 시스템, 의료기기를 포함한 많은 시스템이 영향을 받을 수 있고 환자 치료를 위협하며 심지어 생명을 위험에 빠뜨릴 수도 있다(European Commission, 2025).

미국의 경우 2024년에 보건복지부(Department of Health and Human Services, HHS) 시민권국(Office for Civil Rights, OCR)에 보고된 500건 이상의 기록이 유출된 대규모 의료 데이터 유출 사건은 총 725건으로 2023년 747건 대비 2.95% 감소하였으나, 침해된 데이터 건수는 275,234,065건으로 2023년 168,288,480건 대비 63.5% 증가한 것으로 보고되었다(The HIPAA Journal, 2024). 대규모 의료데이터 유출의 가장 흔한 원인은 해킹 및 기타 IT 사고로, 589건의 데이터 유출이 발생하여 전체의 81.2%를 차지하였으며 침해된 데이터도 259,037,984건으로 전체의 94.1%를 차지한 것으로 나타났다.

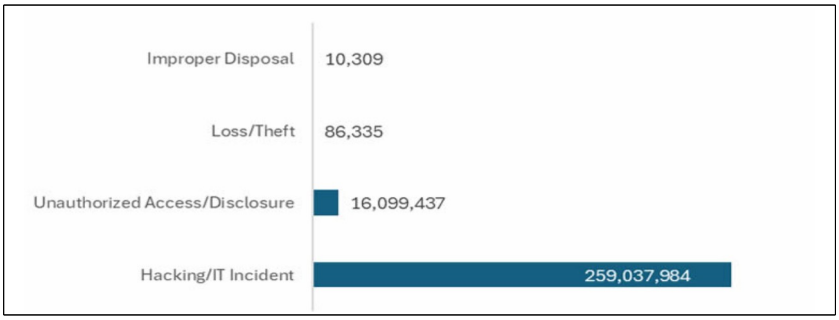
우리나라의 경우 2020년 이후 총 91건의 진료정보 침해사고가 발생한 것으로 보고되었으며, 진료정보 이외의 침해사고도 129건에 달하는 것으로 보고되었다(이승덕, 2024).

[그림 2-10] 2024년 유출 원인별 대규모 의료데이터 유출 건수(미국)



출처: The HIPAA Journal. (2024). 2024 healthcare data breach report.

[그림 2-11] 2024년 유출 원인별 침해된 의료데이터 건수(미국)



출처: The HIPAA Journal. (2024). 2024 healthcare data breach report.

정부 부처 및 관련 기관에 공식적으로 보고된 국내외 사이버 침해사고 현황을 살펴보면, 유럽연합(EU) 국가들은 침해사고 건수가 크게 증가하였고, 미국은 침해사고 건수는 전년 대비 비슷한 수준이었으나 침해된 데

이터는 크게 증가하였으며, 우리나라의 경우 최근 3년간 비슷한 수준을 유지하는 것으로 나타났다.

〈표 2-8〉 우리나라 사이버 침해사고 현황

구분		발생유형	
		랜섬웨어	기타
계	91	84	7
2020년(2월-12월)	13	12	1
2021년	21	21	-
2022년	23	19	4
2023년	23	22	1
2024년(1-8월)	11	10	1

출처: 이승덕. (2024, 10월 3일). 의료기관 해킹 등 사이버 침해사고 200건 넘어. 의학신문.

하지만 다양한 원인으로 미보고된 사이버 침해사고가 보고된 사이버 침해사고보다 훨씬 많을 수 있다는 점을 간과해서는 안 된다.

미국의 경우 500건 이상의 기록이 유출된 대규모 침해사고에 대해서만 공개를 의무화하고 있어 소규모 침해사고는 미보고 상태로 남을 가능성이 높으며 실제 침해사고 건수는 보고된 침해사고 건수보다 많을 수밖에 없다는 점이 지적되고 있다.

ENISA(2023)는 의료기관이 사이버 침해사고 발생 사실을 공개적으로 인정할 경우 법적 책임 및 제재를 피하기 어렵다는 우려와 환자로부터 신뢰를 잃어 경영에 치명적인 영향을 줄 수 있다는 이유로 사이버 침해사고 신고를 꺼리거나 이를 은폐·축소하려는 경향이 있다고 설명하고 있다.

한편 Sangari, Dallal, & Whitman(2022)은 사이버 보험 청구 데이터를 사용하여 보고된 사이버 사고 데이터베이스의 미신고율을 모델링하고 정량화한 결과 전체 사이버 사고 중 약 3%만이 보고되었으며, 97%는 미보고되었다는 연구 결과를 제시하였다. 비록 이 연구는 사이버 사고 데

이터베이스를 활용하였기 때문에 의료 분야 또는 의료기관의 사이버 침해사고의 미신고율을 설명하기에는 적합하지 않으나 공식적으로 신고된 사이버 침해사고보다 미신고된 사이버 침해사고가 훨씬 더 많을 수 있음을 시사하고 있다.

우리나라의 경우 의료기관 사이버 침해사고 미신고와 관련한 연구가 부재하여 미신고 이유나 미신고율을 파악할 수는 없었으나 외국의 선행연구 결과와 크게 다르지 않을 것으로 여겨진다.

3. 의료기관의 사이버 보안 문제점과 대책

Appari, & Johnson(2010)은 전자의무기록의 도입, 정보보안 규제 강화, 의료 제공자 통합, 그리고 환자·의료 제공자·보험사 간 정보 교류의 증가에 따라 정보보안이 의료기관의 핵심 문제로 부각되었으며, 이에 의료 분야의 정보보안 및 개인정보보호에 관한 기존 연구 문헌과 정보시스템, 보건 정보학, 공중보건학, 법학, 의학 등 다양한 학문 분야의 연구 문헌과 미디어 간행물 및 보고서까지 광범위하게 문헌을 수집하여 비판적 문헌조사를 수행하였다. 이 연구에서는 의료 분야 정보보안 및 개인정보보호 문제가 기술적·조직적·법적 측면에서 복잡하게 얽혀 있는 다면적인 문제임에도 불구하고, 기존 연구들이 특정 기술이나 법적 규제에 치우치는 연구 편향성이 심하다는 점을 비판하였으며 향후 의료기관의 성공적인 전자의무기록 활용과 정보보안을 위해서는 총체적인 시스템 관점의 정보보안 접근 방식이 필요하다고 주장하였다. 한편 이 연구는 의료기관의 정보보안을 기술적 조치 또는 법적 규제라는 단면적 과제로 접근하는 기존 연구와 달리 법·제도, 조직·문화, 기술적 조치 등 다면적 관점에서 접근하였다는 점에서 의미가 있으나 새로운 보안 문제로 등장한 사이버

위협을 다루지 못했다는 점이 연구의 한계로 여겨진다.

Jalali, & Kaiser(2018)은 미국의 병원을 대상으로 한 사이버 공격이 증가함에 따라 환자 안전과 개인정보 보호를 위협하는 중요한 문제로 대두되면서 병원의 사이버 보안 역량이 조직 내부의 역동성을 통해 어떻게 발전하는지를 체계적으로 분석하고, 병원 조직과 시스템 차원에서의 사이버 보안 역량 구축 메커니즘을 규명하는 연구를 수행하였다. 이 연구에서는 병원 IT 및 보안 전문가(CIO, CISO 등)를 대상으로 한 인터뷰를 통해 수집한 데이터를 기반으로 병원의 사이버 보안 역량 형성을 설명하는 핵심 변수로 자원 가용성의 불확실성, 외부 압력, 엔드포인트 복잡성, 내부 이해관계자 조정, 사이버범죄 활동 등 다섯 가지를 발견하였으며, 이 중 병원의 사이버 보안 역량에 가장 큰 영향을 미치는 요인은 엔드포인트 복잡성이었으며, 다음은 내부 이해관계자 조정으로 나타나 사이버 보안 역량 향상을 위해 무작정 자원을 늘리기 보다 이 두 가지 요인을 개선하는 것이 더욱 효과적이라고 주장했다. 한편, 개별 병원뿐 아니라 국가 전체의 병원 시스템 보안 수준은 가장 취약한 병원에 의해 좌우될 수 있으며, 일부 병원이 낮은 자원 수준에 머물면 전체 인프라의 취약성을 야기할 수 있기 때문에 국가 차원에서 병원 간 자원 불균형을 완화하여 전체 의료 인프라의 사이버 취약성을 줄이는 것이 중요하다고 주장했다. 이 연구는 병원들의 실제 운영데이터나 공격사례를 직접 분석한 것이 아니라 병원 IT 및 보안 전문가(CIO, CISO 등) 인터뷰에서 수집된 질적 정보를 기반으로 하여 주관성이 포함되어 있고, 기존 연구에서 다루던 암호화, 접근통제 등 기술적 요인을 분석에서 제외함으로 기술적 요인이 충분히 반영되지 못했다는 한계가 있다. 다만 이 연구는 자원을 늘리는 것보다 구조적, 조직적 접근이 더욱 효과적일 수 있다는 점과 국가 차원에서 병원의 사이버 취약성을 줄이기 위해서는 병원 간 자원 불균형을 완화할 필

요가 있다는 점에서 시사하는 바가 크다.

McLeod, & Dolezel(2018)은 의료기관 데이터 침해사고의 급증으로 환자 개인정보 노출과 금전적 피해 등 심각한 문제가 발생함에 따라 2009년부터 2018년까지 미국 보건복지부(DHHS)의 의료데이터 신고 데이터를 수집하여 의료기관의 데이터 유출 현황과 관련 요인을 체계적으로 분석하고, 데이터 유출 발생 위험을 예측할 수 있는 모델을 개발하는 것을 목적으로 연구를 수행했다. 이 연구에서 의료기관의 데이터 침해의 가장 위험한 위협은 해킹이며 가장 취약한 지점은 네트워크 서버이기에 정보보안 투자와 전략에 있어서 이들을 우선적으로 다룰 것으로 권고하였으며, 기술적 보안 대책과 더불어 직원의 사이버 보안 인식 개선 및 교육을 강화해야 한다고 주장했다. 이 연구는 연구 시점이 다소 경과함에 따라 최신 사이버 위협 트렌드를 충분히 반영하지 못했다는 한계가 있으나, 데이터 침해 예방을 위한 위협 요인과 취약 지점을 분석하여 구체적인 사이버 보안 정책과 실무적 대응책을 제시하였다는 데 그 의미가 크다.

Sardi et al.(2020)은 체계적이고 접근 방식을 통해 의료 부문의 사이버 위험에 대한 기존 문헌을 분석하여 이 주제에 대한 실제 연구 현황을 파악한 분석 결과, 미국을 제외한 다른 국가에서는 이 주제에 대한 학계의 관심이 매우 부족한 것으로 나타났으며, 사이버 위험을 실증적으로 조사하고 의료 시설에 실질적인 해결책을 제시할 필요성을 강조했다. 다만 이 연구는 “건강(Health)”이라는 키워드와 관련한 분석함에 따라 연구의 범위를 지나치게 좁힌 것이 연구의 한계라고 밝히고 있으나 이로 인해 기존 문헌의 지식 격차를 파악하고 사이버 위험 연구에 대한 향후 연구 기회를 제시하였다는 점에서 의미가 있다.

Alodaynan, & Alanazi(2021)은 기존 문헌조사를 통해 의료시스템의 사이버 보안 취약점을 체계적으로 조사하여, 병원 서버 및 응용프로그램

에 대한 무단 접근과 해킹이 환자데이터 안전과 시스템 기능에 미치는 위협을 이해하고 데이터 및 시스템의 안정성 확보와 환자 개인정보보호 수준 향상을 위한 연구를 수행했다. 이 연구에서 의료시스템이 사이버 공격의 주요 대상인 이유는 민감한 데이터의 높은 금전적 가치와 의료 IoT, 공개된 네트워크, 직원들의 단말기 등 공격자가 악용할 수 있는 다양한 엔트리포인트(entry point)로 비인가 접근 가능성이 높기 때문이며, 주요 취약점 및 위협으로는 최신 보안패치 및 기능이 적용되지 못한 레거시 시스템과 직원들의 낮은 보안 의식에서 비롯된다고 설명하고 있다. 의료시스템은 복잡성과 상호 연결성 때문에 다양한 취약점에 노출되어 있으며, 의료용 사물인터넷(IoMT) 기기와 인적 요소에 대한 맞춤형 보안 전략이 시급함을 강조하며, 이를 위한 해결책으로 다계층 보안 도입, 직원 대상의 정기적 보안 교육을 통한 인적 오류 최소화, 의료용 사물인터넷(IoMT) 장치에 특화된 경량 암호화 프로토콜 및 인증 메커니즘 개발 및 적용을 제시하였다. 특히 이 연구에서는 의료기관의 정보보안을 단순히 정보기술(IT) 문제로 볼 것이 아니라 조직 전체의 위험관리 및 환자 안전의 관점에서 접근해야 한다고 제언하였다. 다만 이 연구는 문헌 기반의 조사이기에 실제 시스템의 복잡성을 충분히 반영하지 못했을 수도 있다는 것이 연구의 한계이다.

Husain, Tyagi, Khan, & Komakula(2023)는 국제표준인 ISO 27001 인증이 의료기관의 사이버 보안 태세를 강화하는 데 어떻게 기여할 수 있는지 분석하고, 그 효과를 제시하고자 문헌 검토를 수행하였다. 그 결과 ISO 27001 인증이 의료기관의 정보보안을 체계적으로 관리하는 데 매우 효과적이며, ISO 27001의 요구사항은 리스크관리, 보안 정책 수립, 직원 교육, 기술적 통제 등 조직 전체의 정보보안을 포괄적으로 다루기 때문에, 단순한 기술적 방어를 넘어선 총체적인 보안 환경을 조성하는

데 도움되는 것을 확인하였다. 다만 실제 의료기관의 데이터를 기반으로 한 실증적 분석이 아니기에 ISO27001 인증을 획득한 의료기관의 보안 수준이 실제로 얼마나 향상되었는지에 대한 정량적, 객관적 증거를 제시하지는 못하였으며, ISO 27001 구현 과정에서 발생하는 실제 조직적, 재정적, 기술적 어려움이나, 의료 특유의 복잡한 시스템에 표준을 적용하는 구체적인 도전 과제에 대한 심층적인 논의가 상대적으로 부족한 것이 연구의 한계이다.

Kumari, Pattanaik, & Khan(2024)은 의료 부문의 디지털 전환은 운영 효율성과 환자 치료에 혁신적인 개선을 이루었지만 동시에 의료기관을 전례 없는 사이버 보안 위험에 노출시킴에 따라 의료 분야의 사이버 보안 조치가 현재와 미래에 미치는 영향을 포괄적으로 분석하고 의료기관이 사이버 위협에 효과적으로 대응하기 위한 전략을 수립하는 데 도움을 주고자 다양한 학술 논문, 보고서, 사례 연구 등을 종합하여 현재의 보안 조치와 미래의 위협 및 기술 동향을 검토하였다. 연구 결과 사물인터넷(IoT), 블록체인, 인공지능(AI) 등 신기술이 보안을 강화하는 데 긍정적인 역할을 할 수 있지만, 동시에 새로운 위협을 가져올 수 있음을 확인하였다. 한편, 블록체인은 데이터의 무결성과 보안을 강화하는 데 유용하며, 인공지능(AI)은 위협 탐지 및 대응에 혁신적인 솔루션을 제공할 수 있을 것으로 기대하지만, 이러한 신기술의 도입은 새로운 취약점을 초래할 수 있으므로 신중한 접근이 필요하다고 제언하였다. 다만 이 연구에서 논의된 새로운 기술의 이론적인 잠재력과 의료환경에서 실제 적용 가능성은 차이가 있을 것으로 여겨진다.

Vilakazi, & Adebesin(2023)은 의료데이터에 대한 사이버 위협을 완화하는 데 사용될 수 있는 효과적인 전략을 체계적 문헌 고찰을 통해 정책 입안자, 기술 개발자, 의료기관 관리자에게 사이버 보안 강화에 대한

실질적인 지침을 제공하고자 하였다. 이를 위해 주요 학술 데이터베이스에서 41편의 연구논문을 수집하여 분석하고, 신기술 동향, 사이버 보안 과제, 완화 전략으로 분류하여 종합적으로 검토하였다. 이 연구에서는 의료기관의 사이버 위협을 완화하려면 기술적 방어(시스템 암호화, 접근 제어 등) 뿐만 아니라, 사람(직원 교육, 보안 인식) 및 규정 준수(법규 및 표준 이행)를 모두 포괄하는 총체적인 접근이 필수적이며, 이는 정책 입안자, 의료 기술 공급업체/설계자, 의료기관 관리자 모두에게 중요한 함의를 갖고 있다. 이 연구는 의료기관이 단순히 기술적 방어를 넘어, 보안 정책을 준수하고 직원의 인식을 개선하는 조직적 거버넌스를 강화하는 데 투자해야 하며, 이는 진화하는 사이버 공격에 대한 사이버 복원력을 높이는 핵심이라는 점을 설명하고 있다. 다만 이 연구는 문헌 고찰 연구로 사이버 공격 데이터나 사이버 위협을 완화하기 위한 특정 전략의 정량적 효과에 대한 실증적 분석이 부족하다는 것이 연구의 한계로 여겨진다.

Ewoh & Vartiainen(2024)은 의료정보 유출 및 의료기기 기술과 네트워크를 둘러싼 취약성 문제가 기하급수적으로 증가함에 따라 의료시스템 사이버 보안에 관한 문헌을 조사하기 위해 체계적 문헌 검토를 수행했다. 이 연구에서는 의료시스템이 사이버 공격에 취약한 이유로 인적 오류, 투자 부족, 복잡한 네트워크 연결 최종 사용자 장치, 오래된 레거시 시스템, 기술 발전(디지털화) 등 5개 주제를 제시하고 새로운 사회 기술적 관점에서 각각의 주제별 개입 방법을 제안하였다. 또한 이 연구에서는 의료기관의 발전을 위해서는 사이버 보안 기술, 의료기기, 네트워크, 의료 전문가, 사이버 보안 전문가 등 의료시스템에 대한 투자가 매우 중요하다는 점, 의료 전문가와 의료기관이 사이버 보안 취약점의 복잡성을 건설적으로 헤쳐나가기 위해서는 최신 지식과 기술을 제공하는 사이버 보안 교육 및 훈련 프로그램에 대한 투자가 필수적이라는 점과 나아가 정부

는 의료시스템의 사이버 보안 지속가능성을 확보하기 위해 의료기관에 추가적인 재정적 유인을 제공해야 한다는 점을 강조하였다.

최근 의료 분야의 사이버 위협이 증가함에 따라 의료기관 간 협력 기반의 위협 정보 공유 체계인 Health-ISAC이 중요한 보안 대응 전략으로 주목받고 있다. Health-ISAC은 의료 분야 조직 간 사이버 및 물리적 보안 위협 정보를 공유하기 위해 설립된 비영리 협력 네트워크로, 의료기관이 직면한 위협에 대한 상황 인식을 강화하고 대응 역량을 높이는 역할을 수행한다. Health-ISAC은 회원기관에 침해 지표(Indicators of Compromise), 공격 전술·기술·절차(Tactics, Techniques, and Procedures), 취약점 정보 및 경보 등을 제공하여 의료기관이 랜섬웨어, 피싱 등 다양한 사이버 공격에 신속하게 대응할 수 있도록 지원하고 있다. 또한 이러한 정보 공유 체계는 의료기관이 위협 정보를 사전에 인지하고 대응 전략을 수립할 수 있도록 하여 보건의료 분야 전반의 보안 회복력(resilience)을 강화하는 데 기여한다. 특히 Health-ISAC의 Threat Operations Center는 회원기관을 대상으로 위협 인텔리전스 분석, 취약점 보고, 경보 발령, 월간 위협 브리핑 등을 제공하며 의료기관이 위협에 대해 신속하게 대응할 수 있도록 지원하고 있다. 이러한 협력 기반의 정보 공유 모델은 단일 기관의 보안 대응을 넘어 의료 생태계 전반의 사이버 보안 역량을 강화하는 중요한 메커니즘으로 평가되고 있다(Health-ISAC, 2024).

이러한 선행연구를 종합하면 의료기관의 사이버 보안 문제는 단순한 기술적 취약성의 문제가 아니라 조직적 역량, 정책·제도, 인적 요소, 그리고 기관 간 협력 체계가 복합적으로 작용하는 구조적 문제임을 확인할 수 있다.

제4절 소결

제2장에서는 사이버 보안의 개념 및 최신 동향, 의료 분야 정보 공유·분석센터(ISAC), 의료기관 사이버 보안 관련 선행 연구를 검토하였다.

사이버 보안의 개념은 정보시스템의 기밀 보호를 위한 정보보안에서 비롯되었으나, 인터넷의 상용화로 네트워크 보안이라는 개념이 대두되었고, 현재는 사이버 공간에서 발생하는 다양한 위협으로부터 정보와 시스템, 네트워크, 사람을 보호하는 기술적 조치, 조직과 사회 차원에서의 위험 관리, 법·제도·정책적 지원, 인권과 프라이버시 보호, 경제·사회적 연속성 확보, 그리고 안전과 신뢰 보장을 포함하는 종합적 활동으로 그 의미가 확장되었다.

한편 사이버 보안 관련 용어인 사이버 위협, 사이버 공격, 사이버 침해사고의 개념을 살펴보았다. 사이버 위협과 사이버 공격은 많은 사람들이 혼용하여 사용하는 경향이 있는데, 사이버 위협은 정보시스템에 해를 끼칠 수 있는 잠재적인 모든 상황, 사건 또는 행위를 의미하는 추상적이고 포괄적인 개념인 반면, 사이버 공격은 사이버 위협이 현실에서 실행된 구체적이고 직접적인 행위를 의미한다. 사이버 침해사고는 사이버 공격이나 오류로 인해 정보시스템의 기밀성, 무결성, 가용성이 위협받거나 손상된 사건으로 대응이 요구되는 경우를 의미한다.

사이버 위협 유형 분류와 관련한 일의적으로 합의된 기준은 없다. 다만 본 보고서에서는 유럽연합 사이버 보안국(ENISA)의 기준에 따라 랜섬웨어, 악성코드, 사회공학, 데이터에 대한 위협, 가용성에 대한 위협, 정보조작 및 간섭 등으로 구분하고 그 개념과 최신 동향을 살펴보았다. 전 세계적으로 사이버 위협은 크게 증가하고 있으며, 사이버 범죄 조직에 의해 전문화되고 있다. 또한 사이버 위협이 과거에는 금전적 이익을 위해 개인

이나 기업 등을 대상으로 하였으나, 최근에는 정치적 동기에 의한 공격과 국가의 중요 기반 시설에 대한 공격이 증가하고 있다.

다음으로 정보 공유·분석센터(ISAC)의 개념과 우리나라 및 주요 외국의 의료기관 정보 공유·분석 센터(ISAC) 현황을 살펴보았다. 정보 공유·분석센터(ISAC)는 국가의 중요 인프라 시설을 사이버 및 물리적 보안 위협으로부터 보호할 수 있도록 실행 가능한 위협 정보를 수집 및 분석하여 이를 회원들에게 배포하고, 위험을 완화하고 복원력을 강화할 수 있는 도구를 회원에게 제공하기 위해 설립되었으며, 우리나라의 의료정보보호센터, 미국의 Health-ISAC, 유럽연합의 ENISA 및 EH-ISAC, 일본의 Health ISAC Japan, 호주의 보건사이버공유네트워크(HCSN) 등 보건의료 분야 정보 공유·분석센터(ISAC)의 설립 개요, 주요 업무 및 운영 현황을 살펴보았다.

마지막으로 의료기관의 사이버 보안 관련 국내외 선행 연구를 검토하였다. 선행 연구는 의료기관의 사이버 위협 및 취약점, 그리고 체계적인 사이버 역량 강화를 위한 연구를 중점적으로 검토하였다. 의료기관을 대상으로 한 사이버 공격은 의료기관이 보유하고 있는 민감한 환자의 개인정보를 탈취하거나 정보시스템의 기능을 마비시키거나 지연시켜 금전적 이득을 얻기 위해 이루어지고 있다. 한편 의료서비스 환경의 특성상 정보시스템-의료기기-단말기-센서 등 복잡하게 연결된 엔드포인트로 인해 사이버 공격에 취약하며, 최근에는 디지털 전환의 가속화와 원격의료, 스마트 의료기기, 클라우드 서비스 등 네트워크 기반의 새로운 의료서비스 도입이 사이버 공격의 증가에 영향을 미치고 있다. 의료기관의 사이버 위협은 정보시스템에 대한 기술적 대책만으로 해결할 수 있는 문제가 아니며, 의료기관의 조직, 문화, 경영진 및 직원 등의 정보보안 역량 강화를 다차원적 과제로 보아야 함을 공통적으로 강조하고 있다.

제3장

의료기관 사이버 보안 정책 검토

제 3 장 의료기관 사이버 보안 정책 검토

제1절 국내 법·제도 현황

본 절에서는 국내 의료기관의 사이버 보안 관련 법·제도 현황을 체계적으로 분석하였다. 검토의 틀은 정보보안과 보건의료 영역으로 구분하여, 각 분야에서 운영 중인 주요 법률과 제도적 기반을 중심으로 구성하였다.

정보보안 영역에서는 「개인정보 보호법」, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 '정보통신망법'), 「정보통신기반 보호법」을 중심으로 의료기관을 규율하는 「의료법」과의 비교·분석을 수행하였다. 이를 통해 각 법률이 규정하는 정보보호 체계와 그에 대응하는 제도(예: 인증 제도, 침해사고 대응 및 재발 방지 조치, 사고 보고 및 이행 확인 절차 등)를 종합적으로 검토하였다. 이러한 비교를 통해 법률별 규제 목적과 적용 범위, 제도적 운영 방식의 차이를 파악하고, 의료기관 사이버 보안 관련 법제 간 연계성과 보완의 필요성을 도출하고자 하였다.

Nelson et al.(2024)에 따르면, 미국 국립표준기술연구소(NIST)는 사이버 사고 대응 생애주기를 준비–탐지·분석–대응·복구–사후활동의 네 단계로 구분한다. 이 모델은 사고의 예방에서부터 복구 및 재발 방지까지 전 과정을 포괄적으로 관리할 수 있는 국제적인 표준 프레임워크로 활용되고 있다. 국내의 경우 정보보안 분야에서는 관련 법률과 제도가 비교적 체계적으로 마련되어 각 단계별 대응 체계가 제도화되어 있는 반면, 보건의료 분야에서는 의료기관 또는 의료기기 보안 관련 일부 지침과 규정이 존재하나 사고 대응 생애주기 전체를 포괄하는 법적·제도적 기반은 아직 미흡한 수준으로 평가된다.

본 연구에서 검토한 법령은 다음과 같다.

- 「의료법」 및 「의료법 시행령·시행규칙」
- 「전자의무기록의 안전성·신뢰성 확보에 관한 고시」
- 「개인정보 보호법」 및 「시행령」(2025)
- 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」
- 「정보통신기반 보호법」

이상의 법령을 바탕으로 본 절에서는 정보보안과 보건의료 두 축을 중심으로 미국 국립표준기술연구소(NIST)가 제시한 사고 대응 생애주기의 네 단계를 교차 적용한 2×4 분석 틀을 활용하여 의료기관 사이버 보안 관련 국내 법·제도 현황을 검토한다. 이를 통해 현행 제도의 보완 필요성과 법적 사각지대를 진단하고, 의료정보 보호 및 보안 강화를 위한 정책적 시사점과 개선 과제를 도출하고자 한다.

〈표 3-1〉 NIST 사이버 보안 생애주기와 보건·의료 분야 대응 비교

단계	NIST 사이버 보안 생애주기	보건·의료 분야
예방 (Preparation)	- 보호조치 수립 - 자산 식별 - 위험평가 및 예방조치 - 보안인력 훈련 및 예산 확보 - 사고 발생에 대비한 정책·절차 수립 - 거버넌스 체계 확립 - 담당조직(CISO 등) 구성	- 의료기관 정보보호 책임자 (CISO) 지정 - 보안조직 및 예산 확보 - 진료정보 시스템 취약점 점검 - 정기 모의훈련 실시 - 진료정보 시스템 위험평가 수행 - 의료기기·정보시스템 보안수준 평가.
탐지 및 분석 (Detection & Analysis)	- 보안 로그 및 침입탐지시스템 운영 - 이상징후 모니터링 - 사고 식별 및 영향 범위 분석 - 증거 확보 및 로그 관리 체계 강화	- EMR·OCS 등 주요 시스템의 접근로그 분석 및 이상 접근 탐지 - 침해사고 발생 여부 판별 및 영향 범위 파악 - 이상행위 탐지 - 통합보안관제 운영 - 의료기기 이상 탐지 및 보고 - 유지보수업체 연계 모니터링

단계	NIST 사이버 보안 생애주기	보건·의료 분야
대응 및 복구 (Containment/ Eradication/ Recovery)	- 사고 식별 후 격리·차단·복구 조치 수행 - 사고 원인 분석 - 서비스 재가동 및 피해 최소화 - 서비스 연속성 확보 및 백업·복원 관리 - 위기 커뮤니케이션 및 외부 협력	- 의료정보 유출 시 즉각적 차단 - 데이터(환자정보) 백업·복원 - 침해시스템 격리 및 복구조치 - 환자 치료 영향 최소화 - 의료서비스 연속성 확보 업무연속성계획(BCP) 가동 - 의료기기 패치관리 및 SBOM (소프트웨어 부품표) 확인.
이후 활동 (Post-Event Activity)	- 사고 경과 보고 및 사후평가 - 교훈 도출 - 재발 방지 대책 수립 - 보안정책 개선, 교육 및 훈련 강화 - 교육 및 프로세스 개선 - 복원력(Cyber Resilience) 지표 관리	- 의료정보보호센터(ISAC)에 사고 보고 - 관계기관 통보 - 원인 분석 결과 반영 - 재발방지대책 수립 - 정기 보안교육 및 보안훈련 실시 - 의료기기·정보시스템 보안 개선 이행확인.

출처: U.S. Department of Health and Human Services (HHS) (2023; 2024), National Institute of Standards and Technology (NIST) (2010; 2024a; 2024b), 보건복지부·한국사회보장정보원 (2020), 식품의약품안전처 (2025), 한국인터넷진흥원 (2024a; 2024b; 2025), 의료법 제23조의2 등을 Open AI(ChatGPT)의 문서 요약 기능을 참고하여 작성하였음.

〈표 3-2〉는 정보보안 및 보건의료 분야의 주요 법률을 중심으로, 정보보안 침해사고 대응 생애주기의 각 단계(예방-탐지·분석-대응·복구-사후활동)에 따라 관련 제도와 조항을 정리한 것이다.

의료정보 보호 관련 법제는 「개인정보 보호법」, 「정보통신망법」, 「정보통신기반 보호법」 등 일반 정보보호 법령을 상위 체계로 하고, 「의료법」은 이들을 보완·구체화하는 특별법으로 기능한다. 따라서 의료정보 보호 체계는 일반법의 보편적 원칙과 관리 기준을 기반으로 하되, 의료법을 통해 진료정보의 특수성과 의료기관의 관리·운영 여건을 반영하도록 설계되어 있다.

각 법률의 적용 대상이자 보호하고자 하는 정보의 범위는 법률별로 다음과 같다. 「개인정보 보호법」은 개인을 식별할 수 있는 개인정보를, 「정보통신망법」은 정보통신망을, 「정보통신기반 보호법」은 주요 정보통신기

반시설을 각각 보호 대상으로 규정하고 있다. 한편, 「의료법」은 진료기록부 등 진료정보를 보호 대상으로 하며, 진료기록부 등은 진료기록부·조산기록부·간호기록부 및 그 밖의 진료에 관한 기록으로 정의된다.

'그 밖의 진료에 관한 기록'의 구체적 범위는 「휴·폐업 의료기관의 진료기록 이관 및 진료기록 보관시스템 운영에 관한 고시」 제4조(진료기록 보관시스템 운영 등)를 참고하여 정리할 수 있다. 해당 고시에 따르면, 진료기록 보관시스템에 포함되는 기록의 범위는 진료기록부·조산기록부·간호기록부를 비롯하여 진단서, 상해진단서, 사망진단서(시체검안서), 사산(사태) 증명서, 처방전, 진료비 계산서·영수증, 진료비 세부 산정 내역, 후유 장해 진단, 입·퇴원 및 통원 기록, 진료 이력, 수술 기록, 검사 결과, 방사선 판독 등 진료 행위 전반에 걸친 모든 기록을 포함한다. 전자의무기록은 이러한 진료기록부 등을 「전자서명법」에 따른 전자서명이 포함된 전자문서 형태로 작성·보존하는 것을 의미한다.

각 법률에서 정의하는 '침해사고'의 개념과 범위는 다음과 같다. 「개인정보 보호법」 제34조는 개인정보의 유출 사고를 침해사고로 규정하여, 개인정보가 분실·도난·유출된 경우를 포함한다. 「정보통신망법」 제2조 제1항 제7호는 '침해사고'를 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위로 인하여 발생한 사태로 정의하고 있으며 공격 방법도 각 목에서 규정하고 있다. 「정보통신기반 보호법」 제2조 제3호에서도 이와 유사하게 전자적 침해행위로 인하여 발생한 사태로 정의하고 있다.

한편 「의료법」 시행령 제10조의11에서는 '진료 정보 침해사고'의 유형을 별도로 규정하고 있으며, 그 범위는 진료 정보의 도난·유출·파기·손상·은닉·멸실, 그리고 전자의무기록 시스템의 교란·마비 등으로 명시되어 있다. 이는 의료기관에서 발생할 수 있는 정보 유출 사고뿐 아니라 시스템 장애나 데이터 손상 등 의료정보시스템 자체의 기능적 위협까지 포

함하는 의료환경에 특화된 형태로 일반 정보보안 법령보다 더 넓은 범위로 정의하고 있다.

1. 예방(Preparation) 단계

〈표 3-1〉의 내용을 바탕으로, 예방 단계는 다음의 다섯 가지 세부 영역으로 구분하여 비교하였다. 1) 보호(안전·안전성) 조치, 2) 정보보안 인증, 3) 사전 점검(위험 평가), 4) 보안 교육 및 훈련, 5) 정보보안 담당 인력 및 조직(CISO 등)의 구성이다.

1) 보호(안전·안전성) 조치

개인정보 보호법 제29조는 개인정보 처리자에게 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하기 위한 기술적·관리적·물리적 안전조치 의무를 부과하고 있으며, 동법 시행령 제30조에서는 접근통제, 암호화, 접속기록 보관, 악성프로그램 방지 등 구체적 기준을 제시하고 있다. 또한 시행령 제30조의2는 공공시스템 운영기관에 대한 추가 안전조치 사항을 별도로 명시하여, 공공의료기관을 포함한 공공부문 전반의 정보보안 수준을 제도적으로 강화하고 있다.

정보통신망법 제45조에서는 정보통신서비스 제공자 및 정보통신망 연계 기기 등의 제조·수입자에게 정보통신망의 안정성 확보 의무를 부과하고 있다. 한편, 정보통신기반 보호법 제10조와 제11조는 주요 정보통신기반시설의 보호지침 제정과 보호조치 명령 제도를 규정하여 국가 기반시설 차원의 정보보호 관리 체계를 마련하고 있다.

의료법에서는 제21조의2 '진료기록의 송부 등'과 제23조 '전자의무기록'을 통해 의료정보의 송·수신 및 전자의무기록 관리에 관한 안전조치를

규정하고 있다.또한 동법 시행규칙 제16조와 제30조의6은 전자의무기록 및 진료기록부 등의 관리·보존에 필요한 시설과 장비 기준을 세부적으로 규정하고 있으며, 「전자의무기록의 안전성·신뢰성 확보에 관한 고시」 제5조에서는 전자의무기록의 분실·도난·유출·위조·변조 또는 훼손 등 사고에 대비한 보호 대책과, 전자의무기록 시스템이 유·무선 네트워크에 연결될 때 요구되는 정보보호 조치를 명시하고 있다. 이와 더불어 개인정보 보호법 제29조 및 동법 시행령 제30조의 안전조치 의무는 의료기관의 개인정보(진료정보) 처리에도 준용되어 의료법상 진료 정보보호의 기본 원칙을 보완하는 기능을 수행하고 있다.

보호(안전·안전성) 조치 의무를 위반한 경우의 제재는 법률별로 다음과 같이 상이하다. 개인정보 보호법 제75조 제1항은 안전조치 의무를 위반한 개인정보 처리자에게 5천만 원 이하의 과태료를 부과하도록 하고 있으며, 정보통신망법 제76조 또한 안정성 확보 의무를 위반한 경우 3천만 원 이하의 과태료를 부과할 수 있도록 규정하고 있다. 정보통신기반 보호법 제30조 제1항 및 제2항은 주요 정보통신기반시설의 보호지침 미이행 또는 보호조치 명령 불이행 시 5천만 원 이하의 과태료를 부과할 수 있도록 규정하여, 국가 기반시설 차원에서 비교적 높은 수준의 제재를 두고 있다.

반면, 의료법 제92조에서는 의료기관이 진료기록의 관리·보존 또는 전자의무기록의 안전관리 의무를 위반한 경우 300만 원 이하의 과태료를 부과할 수 있도록 규정하고 있어, 일반 정보보호 법령에 비해 상대적으로 낮은 수준의 제재를 두고 있다.

또한, 의료법 제66조 '자격정지 등'에서는 의료인이 법령상 의무를 위반한 경우 1년의 범위에서 자격정지 처분을 할 수 있도록 규정하고 있으나, 그 근거는 제1항 제10호의 '그 밖에 이 법 또는 이 법에 따른 명령을

위반한 때'라는 포괄적 규정에 의존하고 있다. 이러한 구조는 의료정보 유출이나 진료기록 관리 부실 등 정보보호 위반 행위에 대해 명시적 근거 없이 일반 조항을 통해 제재하는 한계를 지닌다.

진료정보는 환자의 생명과 건강에 직접적인 영향을 미치는 고도의 민감정보임을 고려할 때, 의료기관과 의료인의 정보보호 의무 위반에 대해 단순한 소액의 과태료 수준의 제재를 넘어 별도의 행정처분 및 형사적 책임을 명확히 규정하는 법적 근거 마련이 필요하다.

2) 정보보안 인증

개인정보 보호법 제32조의2에서는 개인정보보호 인증제도를 규정하고 있으며, 개인정보처리자의 개인정보 보호조치 수준을 객관적으로 평가하여 인증을 부여할 수 있도록 하고 있다. 이를 통해 기업 및 기관의 개인정보 관리 체계의 신뢰성을 높이고, 개인정보 유출 사고 예방을 유도하는 제도적 기반을 마련하였다.

정보통신망법 제47조는 정보보호 관리체계 인증(ISMS) 제도를 규정하여 정보통신서비스 제공자 등에게 정보보호 관리체계의 수립·운영 여부를 인증받을 수 있도록 하고 있다. 또한 제48조의6에서는 정보통신망 연결기기 등에 대한 보안 인증제도를 별도로 규정하여, 단말기기·네트워크 장비 등 정보통신망에 직접 연결되는 기기의 보안성을 검증할 수 있도록 하고 있다. 이와 같은 인증제도는 정보통신서비스 제공자 및 관련 산업 전반의 보안 수준을 일정 기준 이상으로 유지하기 위한 핵심 제도적 장치로 기능하고 있다.

의료법에서는 제23조의2 '전자의무기록의 표준화 등'에서 전자의무기록의 상호운용성과 안전성을 확보하기 위한 표준화 및 인증제도를 규정하고 있으며, 제58조의6 '인증서와 인증마크'에서는 보건의료정보시스템

인증제도를 근거로 하여, 인증기관의 지정·운영 및 인증서 발급·표시 절차를 명문화하고 있다. 특히 전자의무기록 인증제는 의료기관 간 진료정보의 상호 교류 및 환자 안전 확보를 위한 기술적·관리적 표준을 마련함으로써, 의료정보시스템의 신뢰성 확보와 사이버 보안 수준 제고를 동시에 추구하는 제도로 평가된다.

다만 의료 분야의 인증제도는 정보통신망법상의 정보보호 관리체계 인증(ISMS)이나 개인정보보호법 상의 개인정보보호 인증 제도에 비해 적용 대상과 인증 기준이 상대적으로 협소하며, 인증 취득의 법적 구속력이 약하다는 한계를 지닌다. 따라서 의료정보시스템의 복잡성과 데이터 민감도를 고려할 때 의료기관 규모와 정보시스템 수준에 따라 차등화된 인증 기준 및 사후관리 체계 마련 등 제도적 보완이 필요하다.

전자의무기록 인증제는 의료기관에서 사용하는 전자의무기록 시스템의 기능성, 상호운용성, 보안성, 신뢰성 등을 국가가 평가하여 인증하는 제도로 의료정보의 품질 향상과 안전한 관리 체계 구축을 목표로 하고 있다. 이 제도는 의료법 제23조의2(전자의무기록의 표준화 등) 및 제58조의6(인증서와 인증마크)에 근거하여 운영되며, 보건복지부가 총괄하고 건강보험심사평가원이 인증 업무를 수행한다. 이를 통해 의료기관 간 진료정보의 표준화와 상호 연계성을 확보하고, 환자 안전 및 의료정보 보호 수준을 제고하는 것이 주요 목적이다.

그러나 현행 EMR 인증제는 법적 개념과 제도적 적용 범위 간의 괴리를 내포하고 있다. 의료법 제23조는 전자의무기록을 '진료기록부 등'을 전자서명법에 따른 전자서명이 포함된 전자문서 형태로 작성·보존한 것으로 정의하고 있으나 실제 인증 제도에서는 진료지원 시스템(OCS, LIS, PACS 등)이 인증 대상에서 제외되어 있다. 이는 의료정보의 생성·저장·전달 과정이 상호 연계된 통합 정보환경임에도 불구하고 법령상 '전자의

무기록'을 의료인이 직접 작성·관리하는 법정 진료기록 중심으로 한정하고 있기 때문이다.

그 결과, OCS·LIS·PACS 등 진료지원 시스템이 EMR과 데이터를 주고받으며 환자의 진료 정보를 생성·관리함에도 불구하고, 이들 시스템의 보안성·신뢰성·표준 준수 여부는 인증평가의 직접 대상이 되지 않는 한계가 존재한다. 이러한 구조는 실제 진료 현장에서 발생하는 사이버 보안 위험이 EMR 외부 시스템을 통해 확산될 수 있다는 점에서 의료정보 보호 체계의 실효성을 저하시키는 요인으로 지적된다.

따라서 EMR 인증제도가 의료기관의 정보보호 수준을 종합적으로 담보하기 위해서는 EMR-OCS-LIS-PACS 간 데이터 연동 구조를 평가 항목에 포함하거나 의료기관 내 진료정보시스템 전체를 포괄하는 통합 인증 체계로 발전시키는 등 인증 대상의 범위 확대와 제도적 보완이 필요하다.

3) 사전 점검(위험 평가)

위험평가 단계에서는 정보시스템의 취약점을 사전에 점검하고, 개인정보 처리나 정보통신망 운영 과정에서 발생할 수 있는 위험 요소를 사전에 식별·분석하여 피해를 예방하는 제도적 장치를 규정하고 있다.

개인정보 보호법 제33조에서는 공공기관 또는 개인정보처리자가 개인정보를 대규모로 처리하거나 새로운 기술·서비스를 도입할 경우, 그 처리로 인한 사생활 침해 위험을 미리 분석·평가하는 '개인정보 영향 평가' 제도를 규정한다. 또한 제63조의2에서는 개인정보 처리 실태를 사전에 점검할 수 있는 근거를 마련하여, 개인정보보호위원회가 고위험 기관에 대해 사전 실태 점검을 할 수 있도록 하고 있다. 이러한 제도는 개인정보 처리 전 단계에서 위험 식별-평가-개선 권고로 이어지는 예방 중심의 관리 체계를 형성한다.

정보통신망법 제45조의2에서는 정보통신서비스 제공자에게 정보보호 사전점검을 권고할 수 있도록 규정하고 있으며, 동법 시행령 제36조의3에서는 구체적인 점검 기준(시스템 구조, 접근통제, 로그 관리, 악성코드 방지 등)을 제시하고 있다. 이는 법적 의무보다는 권고적 성격의 예방조치에 해당하지만, 정보통신서비스 전반의 안정성 확보를 위한 행정적 유도 장치로 기능한다.

정보통신기반 보호법 제9조는 주요 정보통신기반시설의 관리기관에 주기적으로 취약점 분석·평가를 실시하도록 규정하고 있으며, 동법 시행령 제17조에서 그 시기와 방법을 명시한다. 이에 따라 국가기반시설 운영기관은 매년 또는 정기적으로 시스템 취약점을 점검하고 개선계획을 수립해야 하며, 미이행 시 동법 제30조 제3항에 따라 500만 원 이하의 과태료가 부과될 수 있다.

한편, 의료법 시행령 제10조의12 제1호에서는 진료정보 침해사고의 예방 및 대응을 위한 조치로서 '의료기관의 전자의무기록 시스템에 대한 취약점 점검'을 명시하고 있다. 또한 「전자의무기록의 안전성·신뢰성 확보에 관한 고시」 제3조에서는 정기적인 현황 조사를, 제4조에서는 조사 결과에 따른 개선 권고를 규정하고 있다. 그러나 이는 법적 강제성이 아닌 권고 수준에 그치며, 개선 미이행 시 별도의 행정처분이나 과태료 규정은 존재하지 않는다.

이와 달리 개인정보보호법 제75조 제2항은 영향평가를 이행하지 않거나 허위로 제출한 경우 3천만 원 이하의 과태료를, 정보통신기반 보호법은 취약점 분석·평가 미이행 시 500만 원 이하의 과태료를 부과할 수 있도록 명시하고 있다. 이에 비해 의료법 체계에서는 취약점 점검 미이행에 대한 명시적 제재 근거가 부재하여, 실질적인 위험평가 체계의 실효성이 낮은 것으로 평가된다.

따라서 의료기관의 전자의무기록 시스템에 대한 취약점 점검이 형식적 절차에 그치지 않고 실질적인 예방 기능을 수행하기 위해서는 법적 의무화, 점검 주기 명문화, 결과 보고 및 개선 이행 관리 체계 구축 등의 제도적 보완이 필요하다.

4) 보안 교육 및 훈련

보안 훈련 단계는 개인정보 및 진료정보의 보호를 위한 인적·조직적 관리 체계의 핵심 구성요소로, 개인정보 취급자나 정보시스템 운영자 등 관련 인력이 보안 의식을 유지하고 침해사고에 대응할 수 있도록 교육과 훈련을 하는 것을 목표로 한다.

개인정보 보호법 시행령 제28조에서는 개인정보 처리자에게 개인정보 취급자에 대한 정기적인 교육 의무를 부여하고 있으며, 교육 내용에는 개인정보 보호 원칙, 안전조치 의무, 침해사고 대응 절차 등이 포함된다. 이는 개인정보보호위원회가 수립한 '개인정보보호 교육 지침'을 통해 구체화되어, 공공기관과 민간 부문 모두가 교육 계획 수립·이행·기록 관리 등을 수행해야 한다.

정보통신망법 시행령 제36조의2에서는 정보통신서비스 제공자와 관련 종사자에게 정보보호 교육 및 훈련 의무를 명시하고 있으며, 이는 사이버 공격 대응, 시스템 보안 관리, 악성코드 감염 대응 등을 중심으로 한 실무형 훈련으로 운영된다. 동법 조항상의 '정보통신망의 안전성 확보를 위한 조치'의 일부로서, 사업자 규모와 서비스 특성에 따라 자율적이지만 상시적인 보안 훈련 체계 구축이 권장된다.

정보통신기반 보호법 시행령 제19조는 기반시설 관리기관의 보호대책 내용에 교육 및 훈련을 포함하도록 규정한다. 이에 따라 국가 주요 기반시설 담당자는 보안사고 대응 훈련, 취약점 점검 교육, 재난 대응 시나리

오 기반 모의훈련 등을 주기적으로 실시해야 하며, 그 결과는 보호 대책 보고서에 반영된다. 이는 정보보호 담당자 및 운영 인력의 현장 대응 역량 강화를 위한 제도적 장치라 할 수 있다.

의료법 시행령 제10조의12 제1호에서는 진료정보 침해사고의 예방 및 대응을 위한 조치로 '의료인 또는 의료기관 개설자에 대한 교육 및 훈련'을 규정하고 있다. 이 조항은 전자의무기록 시스템을 포함한 진료 정보보호를 위한 인적 관리 체계를 제도적으로 반영한 것이지만, 법적 의무 조항이 아닌 권고적 성격을 가지며, 세부적인 교육 주기·내용·이행평가 기준이 명문화되어 있지 않아 실효성이 제한적이다. 또한 보건복지부의 「의료기관 정보보호 가이드라인」(비법령성 문서)에서도 의료기관의 정보보호 책임자(CISO)와 개인정보 취급자를 대상으로 한 정기적 정보보호 교육을 권고하고 있으나 이는 행정지침 수준의 권고 사항에 불과하며 법률로서의 구속력이 없다.

현재 대부분의 의료기관은 이러한 가이드라인과 내부규정에 따라 자율적으로 교육을 하고 있으나 개인정보보호법상 의무교육과 달리 교육체계의 표준화나 사후관리 절차가 부재하다는 점에서 제도의 실효성이 낮다. 따라서 의료기관 종사자의 정보보호 역량을 체계적으로 강화하기 위해서는 법적 의무화, 교육 기준의 세분화, 인증제도 및 평가 체계와의 연계 강화 등 제도적 보완이 필요하다.

이와 같이, 일반 정보보안 법령(개인정보보호법, 정보통신망법, 정보통신기반 보호법)은 교육 의무, 주기, 내용 및 감독 체계가 명문화되어 있는 반면, 의료법상 교육조항은 권고적 성격에 머물러 있다. 따라서 의료기관 종사자의 보안 역량 강화를 위해서는 법적 의무화, 교육표준 마련, 인증제도와의 연계 강화 등 제도적 보완이 필요하다.

5) 정보보안 담당 인력 및 조직(CISO 등)

정보보호 체계의 효과적인 운영을 위해서는 기술적·관리적 보호조치 뿐 아니라 정보보호 전담 조직과 책임자의 지정이 필수적이다. 각 법률은 조직 내 정보보호 거버넌스 구축을 위한 책임자(CISO, 개인정보보호 책임자 등) 지정 의무를 규정하고 있으나 의료법에서는 이러한 인적·조직적 관리 체계에 관한 규정이 상대적으로 미비하다.

개인정보보호법 제32조의2에서는 개인정보 처리자에게 개인정보보호 책임자(Chief Privacy Officer, CPO)를 지정하도록 의무화하고 있으며, 책임자의 역할로 개인정보 보호 계획 수립·이행, 침해사고 대응, 내부 관리 감독 등을 규정하고 있다. 정보통신망법 제45조의3 또한 정보통신서비스 제공자에게 정보보호 최고책임자(Chief Information Security Officer, CISO)를 지정하도록 명시하며, 일정 규모 이상의 사업자는 독립적 지위를 갖는 전담 임원을 선임해야 한다. 정보통신기반 보호법 제5조에서는 주요 정보통신기반시설 관리기관이 정보보호 책임자 지정 및 보호 대책 수립을 의무화하고 있으며 국가 주요 기반시설의 관리 책임자는 보호지침 준수, 취약점 평가, 침해사고 대응 등의 임무를 수행한다.

반면, 의료법에서는 정보보호 전담 조직 또는 책임자(CISO 등) 지정에 관한 명시적 의무 조항이 존재하지 않는다. 의료법 제23조의4 '진료정보 침해사고의 예방 및 대응 등'에서는 보건복지부 장관을 주체로 하여 진료정보 침해사고의 예방 및 대응에 관한 기본 체계를 규정하고 있을 뿐 의료기관 내부의 정보보호 조직 구성이나 책임자 지정 의무는 포함하지 않는다. 특히 동조 제2호와 제5호는 각각 '진료정보 침해사고의 예보·경보', '그 밖에 진료정보 침해사고 예방 및 대응을 위하여 대통령령으로 정하는 사항'으로 위임 규정되어 있어 구체적인 조직 운영 기준은 시행령 또는 하위지침 수준에서만 다뤄지고 있다. 동법 시행규칙 제16조의4에서는 진료정보 침해사고의 예방 및 대응 업무를 한국사회보장정보원에 위

탁할 수 있도록 규정하고 있어, 실질적인 보안 관리의 중심이 의료기관 내부가 아닌 외부 공공기관에 위치하는 구조를 갖는다. 이는 의료기관 단위의 정보보호 관리 체계가 제도적으로 충분히 내재화되지 않았음을 보여준다.

이와 같이 일반 정보보호 법령은 조직 내 정보보호 책임자의 지정과 역할을 명확히 규정하여 거버넌스 체계를 확보하고 있는 반면, 의료법은 진료정보보호의 중요성에 비해 의료기관 내부의 정보보호 책임 체계에 대한 법적 근거가 부족하다. 따라서 향후 의료법 체계에서도 의료기관 규모 및 정보시스템 복잡도에 따라 정보보호 책임자 지정 의무화 및 내부 보안 조직 운영 기준을 명문화할 필요가 있다.

2. 탐지 및 분석(Detection & Analysis) 단계

탐지 및 분석 단계는 정보보안 침해사고 발생 시 그 사실을 인지하고, 관계기관에 통지·신고하며, 이후 사고 원인과 피해 범위를 분석하는 과정을 포함한다. 각 법률은 이 단계에서 통지 주체·대상·기한 및 미통지 시 제재, 그리고 사고 분석의 주체 및 절차를 구체적으로 규정하고 있다.

개인정보보호법 제34조에서는 개인정보의 유출을 침해사고로 정의하고, 개인정보 처리자에게 유출 사실을 인지한 즉시 개인정보보호위원회 및 정보주체에게 통지할 의무를 부과하고 있다. 동법 시행령 제39조와 제40조는 각각 통지와 신고의 구체적 절차를 명시하며, 유출 사실을 안 때부터 72시간 이내에 신고하도록 규정하고 있다. 미통지 시에는 동법 제75조 제1항에 따라 5천만 원 이하의 과태료가 부과된다. 또한 동법 제34조 제6항은 개인정보보호위원회가 유출 사고의 원인 분석과 재발 방지 조치를 명령할 수 있도록 규정함으로써 사후 분석 체계를 제도화하고 있다.

정보통신망법 제48조의3에서는 정보통신서비스 제공자에게 침해사고 발생 시 과학기술정보통신부 장관 또는 한국인터넷진흥원(KISA)에 신고할 의무를 부여하고 있으며, 이용자에게도 피해 사실을 통지하도록 하고 있다. 미신고 시에는 동법 제76조에 따라 3천만 원 이하의 과태료가 부과된다. 또한 동법 제48조의4에서는 침해사고의 원인 분석과 정보 공유 절차를 규정하여, 국가 차원의 사이버 보안 상황 인식 및 정보 분석 체계가 구축되어 있다.

정보통신기반 보호법 제13조에서는 주요 정보통신기반시설 관리기관이 침해사고 발생 시 관계 행정기관, 수사기관 또는 한국인터넷진흥원에 즉시 통보하도록 규정하고 있으며, 미통지 시에는 제30조에 따라 500만 원 이하의 과태료가 부과된다. 또한 동법 제16조는 정보 공유·분석센터(ISAC)의 설치·운영 근거를 마련하여, 침해사고 정보를 실시간으로 공유·분석하고 재발 방지 대책을 수립하도록 하고 있다.

반면 의료법에서는 진료 정보 침해사고의 예방 및 대응(제23조의 4)과 통지(제23조의 3)를 별도로 규정하고 있다. 제23조의3에 따르면, 의료인 또는 의료기관 개설자는 진료정보 침해사고가 발생한 경우 보건복지부 장관에게 통지해야 하며, 이후 보건복지부는 관계 행정기관에 이를 보고할 수 있다. 통지 방법은 동법 시행규칙 제16조의 2에 따라 정해지지만, 신고 기한이나 세부 절차, 미통지 시 제재 기준은 명확히 규정되어 있지 않다. 제23조의4에서는 보건복지부 장관을 주체로 하여 사고 정보의 수집·전파(제1호), 침해사고의 예보·경보(제2호), 긴급조치(제3호), 전자적 침해행위의 탐지·분석(제4호) 등을 수행하도록 규정하고 있으나, 이는 중앙정부 차원의 대응 체계에 한정되어 있으며 개별 의료기관의 자체 분석·보고 의무는 구체화되어 있지 않다.

또한 의료법 제92조는 진료정보 보호 의무 위반 시 300만 원 이하의

과태료를 규정하고 있어, 일반 정보보호 법률의 제재 수준(수천만 원 이하)에 비해 상대적으로 제재 강도가 현저히 낮다.

개인정보보호법, 정보통신망법 및 정보통신기반 보호법은 사고 인지-신고-분석의 절차와 책임 주체, 제재 기준을 구체적으로 규정하고 있는 반면, 의료법은 통지 의무와 대응 주체만 명시되어 있고, 세부 절차·기한·제재 및 분석체계의 내재화가 미흡하다.

이는 의료기관 차원의 침해사고 대응 및 분석 역량이 제도적으로 뒷받침되지 못하고 있음을 보여주며, 향후 의료기관 단위의 사고 인지·통보·분석 절차를 의무화하고, 보건복지부-의료기관-한국사회보장정보원 간의 역할 분담을 명확히 하는 체계 정비가 필요하다.

3. 대응 및 복구(Containment/Eradication/Recovery) 단계

대응 및 복구 단계는 침해사고 발생 직후 피해 확산을 차단하고, 손상된 시스템과 데이터를 복구하며, 향후 유사 사고 재발을 방지하기 위한 기술적·관리적 조치를 포함한다. 각 법률은 사고 대응의 주체, 복구 조치의 범위, 관련 기관 간 협력체계 등을 규정하고 있다.

개인정보보호법 제34조의2에서는 개인정보가 유출되거나 노출된 경우 해당 개인정보의 삭제·차단 등 필요한 조치를 신속히 취할 것을 규정하고 있으며, 제64조는 침해사고 발생 시 개인정보보호위원회가 시정조치·개선명령을 내릴 수 있는 법적 근거를 제공한다. 이를 통해 피해자의 추가 피해를 방지하고, 위반행위의 재발을 방지하는 사후관리 체계를 제도화하고 있다.

정보통신망법 제48조의 2 에서는 정보통신서비스 제공자에게 침해사고 발생 시 즉시 대응 및 복구 조치를 수행할 의무를 부여하고, 필요시 관

계기관의 지원을 받을 수 있도록 규정한다. 또한 제48조의5에서는 정보통신망 연결기기(예: IoT·서버 등) 관련 침해사고에 대해서도 대응·복구 의무를 명시하여, 네트워크 전체의 복원력(resilience)을 확보하도록 하고 있다.

정보통신기반 보호법 제14조에서는 주요 정보통신기반시설의 관리기관이 침해사고 발생 시 피해 복구 및 정상 운영 회복을 위한 조치를 취하도록 의무화하고 있으며, 제15조에서는 중앙행정기관의 장이 침해사고 대응을 위한 대책본부를 구성하여 기관 간 협조 체계를 운영하도록 규정하고 있다. 이는 국가 기반시설 차원의 복구 지휘 체계를 제도적으로 마련한 것이다.

반면 의료법 제23조의4 '진료정보 침해사고의 예방 및 대응 등'에서는 보건복지부 장관을 주체로 하여 진료정보 침해사고 발생 시 예보·경보(제2호), 긴급조치(제3호), 전자의무기록 침해행위의 탐지·분석(제4호) 등을 수행하도록 규정하고 있다. 동법 시행규칙 제16조의3에서 침해사고 발생 시 보건복지부 장관이 진료정보의 추가 유출 방지, 관련 시스템의 일시 차단, 복구 지원 등의 긴급조치를 할 수 있도록 정하고 있다. 또한 동법 시행규칙 제16조의4는 이러한 예방 및 대응 업무를 한국사회보장정보원에 위탁할 수 있도록 규정하여, 실제 복구 지원과 기술적 대응의 실무를 공공기관이 수행하도록 하고 있다.

의료법 체계에서는 개인정보보호법이나 정보통신망법과 달리 의료기관 자체의 복구 책임·복구계획 수립 의무가 명시되어 있지 않으며 복구 과정의 기술적 기준·절차·보고 체계 또한 구체화되어 있지 않다. 결과적으로 의료기관 단위의 신속한 복구·대응 역량 확보보다는 중앙행정기관(보건복지부 및 위탁기관)의 사후적 개입에 의존하는 구조를 가지고 있으며 이는 의료정보시스템의 분산 구조와 민감도에 비추어볼 때 제도적 공

백으로 평가된다.

따라서 의료법상 대응 및 복구 체계의 실효성을 확보하기 위해서는 의료기관별 침해사고 복구계획 수립 의무화, 복구 절차 및 기술 표준의 구체화, 공공기관과 의료기관 간 실시간 정보 공유·지원 체계 확립이 필요하다.

4. 사후 활동(Post-Event Activity) 단계

사후 조치 단계는 침해사고 발생 후 피해 확산을 방지하고, 사고의 원인 및 대응 결과를 평가하여 재발을 방지하기 위한 제도적 절차를 말한다. 이 단계는 단순한 복구 이후의 행정적 마무리가 아니라, 사고 대응 전 과정을 검토하고 제도·기술·관리적 개선을 도출하는 핵심 단계이다.

개인정보보호법에서는 제64조를 통해 침해사고 발생 이후 개인정보보호위원회가 위반행위에 대한 시정명령, 과징금 부과, 재발방지 계획 제출 요구를 명할 수 있도록 규정하고 있으며, 필요한 경우 위반기관을 대상으로 재점검 또는 재평가를 실시할 수 있다. 이는 사후관리의 행정적 강제수단을 명시한 사례로 평가된다.

정보통신망법 제48조의5에서는 정보통신망 연결기기(예: 서버, IoT, 단말기 등)와 관련된 침해사고의 대응뿐 아니라 사고 이후의 재발 방지 대책 수립과 개선 조치 이행을 포함하도록 규정하고 있다. 이 조항은 네트워크 기반 서비스의 복원력(resilience)을 확보하고, 침해사고 이후에도 시스템 취약점의 재점검 및 보안 기준 재설정을 의무화함으로써, 사후관리 단계의 제도적 기반을 마련한 대표적 규정이다.

정보통신기반 보호법은 제15조를 통해 중앙행정기관장이 침해사고 대응 및 복구 과정에서 구성된 대책본부를 중심으로 사후평가와 보고를 수

행하도록 규정하고 있다. 또한 사고 원인 및 대응 과정 분석 결과는 정보 공유·분석센터(ISAC)를 통해 다른 기반시설에 전파되어 유사 사고의 예방 및 국가 차원의 위기 대응 능력을 제고하는 데 활용된다.

반면, 의료법에서는 진료정보 침해사고의 사후평가 및 개선 조치 명령에 대한 규정이 비교적 제한적이다. 의료법 제23조의4 제4항에서는 보건복지부 장관은 진료정보 침해사고의 재발 방지에 필요한 개선 조치를 명할 수 있다고 규정하고 있으나, 구체적인 절차·평가 기준·이행점검 방식이 하위 법령에서 명문화되어 있지 않다. 사후평가의 주체 역시 보건복지부 또는 위탁기관(한국사회보장정보원)에 한정되어 있어, 의료기관 자체의 내부 점검이나 재발 방지 계획 수립 의무는 부재하다.

이와 같은 구조는 침해사고의 사후관리 책임이 의료기관 내부가 아닌 중앙행정기관 중심으로 운영되고 있음을 의미하며, 실제 의료기관 단위의 재발 방지 노력이나 자율 평가 체계로 연결되기 어렵다.

따라서 의료법 체계에서도 사후관리 단계의 실효성을 높이기 위해 의료기관의 사후평가 및 보고 의무 명문화, 재발 방지 계획 수립 및 이행점검 절차의 제도화, 보건복지부와 의료기관 간 사후관리 협력 체계 구축이 필요하다.

〈표 3-2〉 정보보안 및 보건의료 분야 주요 법률의 정보보안 침해사고 대응 생애주기별 비교

		정보보안 분야	보건·의료 분야
보호 대상		개인정보보호법 제2조 제1호: 개인정보 정보통신망법 제2조 제1호: 정보통신망 정보통신기반 보호법 제2조 제1호: 정보통신기반시설	**의료법** 제22조 (진료기록부 등): 진료기록부 등 **의료법** 제23조 (전자의무기록): 전자의무기록
침해 사고	정의	개인정보보호법 제34조: 유출 사고를 침해사고로 정의 정보통신망법 제2조 제1항 제7호: 침해사고 정보통신기반 보호법 제2조 제3항: 침해사고	**의료법 시행령** 제10조의 11 (진료정보 침해사고의 유형): 진료정보의 도난·유출·파기·손상·은닉·멸실. 전자의무기록시스템의 교란·마비
예방 (Preparation)	보호(안전, 안전성) 조치	개인정보보호법 제29조 (안전조치의무) 개인정보보호법 시행령 제30조 (개인정보 안전성 확보조치 기준) 개인정보보호법 시행령 제30조의 2 (공공시스템 운영기관 등의 개인정보 안전성 확보 조치 등) 정보통신망법 제45조 (정보통신망의 안정성 확보 등) 정보통신기반 보호법 제10조 (보호지침)	**의료법** 제21조의 2 (진료기록의 송부 등) **의료법** 제23조 (전자의무기록) **의료법 시행 규칙** 제16조 (전자의무기록의 관리·보존에 필요한 시설과 장비 등) **의료법 시행 규칙** 제30조의 6 (진료기록부등의 관리·보존에 필요한 시설 및 장비) **전자의무기록의 안전성·신뢰성 확보에 관한 고시** 제5조 (전자의무기록 보호 대책 공지) - 전자의무기록의 분실·도난·유출·위조·변조 또는 훼손 등 사고 대비에 필요한 사항 - 전자의무기록 시스템과 유무선 인터넷 연결 시 정보보호에 필요한 사항 개인정보보호법 제29조, 개인정보보호법 시행령 제30조의 의료정보 안전조치 의무 준용

		정보보안 분야	보건·의료 분야
예방 (Preparation)	보호(안전, 안전성) 조치	(미조치 시) 개인정보보호법 제64조 (시정조치 등) 개인정보보호법 제75조 제1항 (과태료) : 5천만원 이하 정보통신망법 제76조 (과태료): 3천만원 이하 정보통신기반 보호법 제11조 (보호조치 명령) 정보통신기반 보호법 제30조 제1항 및 제2항 (과태료): 5천만원 이하	(미조치 시) **의료법** 제92조 (과태료): 300만원 이하
	정보 보안 인증	개인정보보호법 제32조의 2 (개인정보보호 인증) 정보통신망법 제47조 (정보보호 관리체계의 인증) 정보통신망법 제48조의 6 (정보통신망연결기기등에 관한 인증)	**의료법** 제23조의 2 (전자의무기록의 표준화 등) **의료법** 제58조의 6 (인증서와 인증마크)
	사전 점검 (위험 평가)	개인정보보호법 제33조 (개인정보 영향평가) 개인정보보호법 제63조의2(사전 실태점검) 정보통신망법 제45조의 2 (정보보호 사전점검) : 권고할 수 있다. 정보통신망법 시행령 제36조의 3 (정보보호 사전점검기준) 정보통신기반 보호법 제9조 (취약점의 분석·평가) 정보통신기반 보호법 시행령 제17조 (취약점 분석·평가의 시기) (미조치 시) 개인정보보호법 제75조 제2항 (과태료): 3천만원 이하 정보통신기반 보호법 제30조 제3항 (과태료) : 5백만원 이하	**의료법 시행령** 제10조의 12 제1호 (진료정보 침해사고의 예방 및 대응을 위한 조치) 1. 의료기관의 전자의무기록시스템에 대한 취약점 점검 **전자의무기록의 안전성·신뢰성 확보에 관한 고시** 제3조 (현황조사) **전자의무기록의 안전성·신뢰성 확보에 관한 고시** 제4조 (개선권고) (미조치 시)

		정보보안 분야	보건·의료 분야
예방 (Preparation)	보안 교육 및 훈련	개인정보보호법 시행령 제28조 (개인정보취급자에 대한 교육) 정보통신망법 시행령 제36조의2 (정보보호 교육·훈련) 정보통신기반 보호법 시행령 제19조 (보호대책의 내용)	**의료법 시행령** 제10조의 12 제1호 (진료정보 침해사고의 예방 및 대응을 위한 조치) 2. 의료인 또는 의료기관 개설자에 대한 교육 및 훈련
	정보 보안 담당 인력 및 조직 (CISO 등)	개인정보보호법 제32조의 2 (개인정보보호책임자 지정 등) 정보통신망법 제45조의 3 (정보보호 최고책임자의 지정 등) 정보통신기반 보호법 제5조 (주요정보통신기반시설보호대책의 수립 등) : 정보보호책임자	**의료법** 제23조의 4 (진료정보 침해사고의 예방 및 대응 등): 주체는 보건복지부장관 2. 진료정보 침해사고의 예보·경보 5. 그 밖에 진료정보 침해사고 예방 및 대응을 위하여 대통령령으로 정하는 사항 **의료법 시행 규칙** 제16조의4 (진료정보 침해사고의 예방 및 대응을 위한 업무의 위탁): 한국사회보장정보원
탐지 및 분석 (Detection & Analysis)	사고 인지	개인정보보호법 제34조 (개인정보 유출 등의 통지·신고) 개인정보보호법 시행령 제39조 (개인정보 유출 등의 통지) 개인정보보호법 시행령 제40조 (개인정보 유출 등의 신고) 정보통신망법 제48조의 3 (침해사고의 신고 등) 정보통신기반 보호법 제13조 (침해사고의 통지)	**의료법** 제23조의 4 (진료정보 침해사고의 예방 및 대응 등) : 주체는 보건복지부장관 2. 진료정보 침해사고의 예보·경보 3. 진료정보 침해사고에 대한 긴급조치 4. 전자의무기록에 대한 전자적 침해행위의 탐지·분석

		정보보안 분야	보건·의료 분야
탐지 및 분석 (Detection & Analysis)	통지(신고) 주체	개인정보보호법 제34조 (개인정보 유출 등의 통지·신고): 개인정보처리자, 72시간 이내 신고 정보통신망법 제48조의 3 (침해사고의 신고 등) : 정보통신서비스 제공자 정보통신기반 보호법 제13조 (침해사고의 통지) : 주요정보통신기반시설 관리기관	**의료법** 제23조의 3 (진료정보 침해사고의 통지) : 의료인 또는 의료기관 개설자
	통지(신고) 대상	개인정보보호법 제34조 (개인정보 유출 등의 통지·신고): 해당 정보주체 정보통신망법 제48조의 3 (침해사고의 신고 등) : 과학기술정보통신부장관, 한국인터넷진흥원 정보통신기반 보호법 제13조 (침해사고의 통지) : 관계 행정기관, 수사기관 또는 인터넷진흥원	**의료법** 제23조의 3 (진료정보 침해사고의 통지) : 의료인 또는 의료기관 개설자 → 보건복지부장관 → 관계 행정기관 **의료법 시행규칙** 제16조의 2 (진료정보 침해사고의 통지 방법)
	미통지 (미신고) 시	개인정보보호법 제75조 제1항 (과태료): 5천만원 이하 정보통신망법 제76조 (과태료): 3천만원 이하	**의료법** 제92조 (과태료): 300만원 이하
	사고 분석	개인정보보호법 제34조 (개인정보 유출 등의 통지·신고) 정보통신망법 제48조의 4 (침해사고의 원인 분석 등) 정보통신기반 보호법 제16조 (정보공유·분석센터)	**의료법** 제23조의 4 (진료정보 침해사고의 예방 및 대응 등) : 주체는 보건복지부장관 1. 진료정보 침해사고에 관한 정보의 수집·전파 4. 전자의무기록에 대한 전자적 침해행위의 탐지·분석

		정보보안 분야	보건·의료 분야
대응 및 복구 (Containment/ Eradication/ Recovery)	대응 및 복구	개인정보보호법 제34조의 2 (노출된 개인정보의 삭제·차단) 개인정보보호법 제64조 (시정조치 등) 정보통신망법 제48조의 2 (침해사고의 대응 등) 정보통신망법 제48조의 5 (정보통신망연결기기등 관련 침해사고의 대응 등) 정보통신기반 보호법 제14조 (복구조치) 정보통신기반 보호법 제15조 (대책본부의 구성 등)	**의료법** 제23조의 4 (진료정보 침해사고의 예방 및 대응 등) : 주체는 보건복지부장관 2. 진료정보 침해사고의 예보·경보 3. 진료정보 침해사고에 대한 긴급조치 5. 그 밖에 진료정보 침해사고 예방 및 대응을 위하여 대통령령으로 정하는 사항 **의료법 시행 규칙** 제16조의3 (진료정보 침해사고에 대한 긴급조치) **의료법 시행 규칙** 제16조의4 (진료정보 침해사고의 예방 및 대응을 위한 업무의 위탁): 한국사회보장정보원
이후 활동 (Post-Event Activity)	사후 조치	개인정보보호법 제64조 (시정조치 등) 정보통신망법 제48조의 5 (정보통신망연결기기등 관련 침해사고의 대응 등) 정보통신기반 보호법 제15조 (대책본부의 구성 등) 정보통신기반 보호법 시행령 제23조 (대책본부의 운영)	

출처: 보건복지부, 의료법 및 의료법 시행령·시행규칙 (2025); 과학기술정보통신부, 정보통신망 이용촉진 및 정보보호 등에 관한 법률 (2025); 과학기술정보통신부, 정보통신기반 보호법 (2025); 개인정보보호위원회, 개인정보 보호법 및 시행령 (2025); 보건복지부, 전자의무기록의 안전성·신뢰성 확보에 관한 고시 (2023) 참고하여 저자 작성.

정보보안 분야의 일반 법령(개인정보 보호법, 정보통신망법, 정보통신기반 보호법)은 예방-탐지·분석-대응·복구-사후 활동의 전 주기에 걸쳐 명시적이고 집행력 있는 대응·관리 체계(의무 규정, 신고·통지 기한, 시정·개선 명령, 과징금·과태료 등)를 갖추고 있다. 반면, 보건의료 분야의 법령(의료법 및 하위 규정)은 예방과 탐지 단계에 규정이 집중되어 있고, 사후평가·재발 방지·이행점검으로 이어지는 폐쇄루프형(Closed-loop) 관리체계는 상대적으로 미흡하다. 이로 인해 침해사고 이후의 제도적 학습과 내부 통제 고도화가 체계적으로 축적되지 못하는 한계가 나타난다.

특히 의료기관의 내부 거버넌스(정보보호 책임자 지정, 전담 조직의 역할·권한, 정례 훈련 및 모의 대응) 의무 수준과 표준화 정도가 일반 법령 대비 낮으며, 통지·신고의 기한과 양식, 미통지 시 제재 근거도 구체화되어 있지 않아 현장 집행력이 약하다. 또한 사후평가-재발 방지 계획-이행점검-재평가로 이어지는 절차가 제도적으로 내재화되지 않아 사고 후 개선 활동이 기관별 자율·권고 수준에 머무르는 경향이 있다.

이에 따라, 다음 〈표 3-3〉에서는 정보보안 및 보건의료 분야의 주요 법률을 중심으로 각 법령이 규정하고 있는 핵심 제도 및 관리 체계 요소(인증제도, 점검·평가제도, 통보·보고 체계, 복구 지원 및 사후평가 등)를 비교·정리하였다. 이를 통해 정보보호 법제 전반의 완성도와 의료정보 보호 법제의 보완 필요 영역을 구체적으로 도출할 수 있다.

〈표 3-3〉 정보보안 및 보건의료 분야 주요 법률 및 주요 제도

구분	법률	주요 제도	핵심 목표
정보보안	- 개인정보 보호법, 시행령	- 개인정보 영향평가(PIA) - 개인정보보호 인증제(PIMS/PIPL) - 개인정보보호책임자(CPO) 지정 - 안전성 확보조치 의무 (기술적·관리적 보호조치) - 침해사고 통지·신고 제도	개인정보의 안전성 확보 및 침해사고 예방

구분	법률	주요 제도	핵심 목표
정보 보안	- 정보통신망 이용촉진 및 정보보호 등에 관한 법률, 시행령	- 정보보호 관리체계 인증(ISMS) - 정보통신망 연계기기 보안 인증(ISMS-P/ISMS-기기) - 정보보호 최고책임자(CISO) 지정 - 침해사고 신고 및 복구·대응 의무 - 이용자 통지 제도	정보통신망 및 관련 서비스의 안정성 확보
	- 정보통신기반 보호법, 시행령	- 주요 정보통신기반시설 지정·관리 제도 - 보호지침 수립 및 보호조치 명령 제도 - 취약점 분석·평가 제도 - 정보공유·분석센터(ISAC) 운영 - 복구 및 대책본부 운영	국가 기반시설 보호 및 정보통신 기반 안정성 확보
보건 ·의료	- 의료법, 시행령	- 전자의무기록(EMR) 인증제 - 보건의료정보시스템 인증제(HIE) - 진료정보 침해사고 통지·긴급조치 제도 - 진료정보 보호 및 안전관리 의무 - 의료정보보호센터(의료ISAC) 운영	진료정보의 안전 관리 및 의료정보 보호

출처: 보건복지부, 의료법 및 의료법 시행령·시행규칙 (2025); 과학기술정보통신부, 정보통신망 이용촉진 및 정보보호 등에 관한 법률 (2025); 과학기술정보통신부, 정보통신기반 보호법 (2025); 개인정보보호위원회, 개인정보 보호법 및 시행령 (2025); 보건복지부, 전자의무기록의 안전성·신뢰성 확보에 관한 고시 (2023) 참고하여 저자 작성.

제2절 국내외 정책 동향

1. 국내 의료기관 관련 정보보안 제도

가. 병원정보시스템 보안 가이드라인

국가정보원은 국민 생명과 직결된 병원 전산시스템과 의료정보 등을 사이버 공격으로부터 보호하기 위해 '병원정보시스템 보안 가이드라인(2025년 4월)'을 마련하였다.

'병원정보시스템 보안 가이드라인'의 목적은 모든 환자와 병원 구성원이 안심하고 신뢰할 수 있는 병원정보시스템을 구축하고 운영하기 위한 보안 대책을 제시하고 있으며, 이를 통해 위협으로부터 환자 데이터를 보호하고 병원 서비스의 연속성을 확보함으로써 사용자가 신뢰할 수 있는 환경을 조성하는 것이다(국가정보원, 2025. p.6).

'병원정보시스템 보안 가이드라인'은 진료 및 행정정보 시스템(OCS, EMR, PACS, LIS 등), 외부 연계시스템, 환자 포털, 모바일·원격진료 시스템, 의료기기 및 단말기, 내·외부 사용자 접근통제 등 6개 핵심 영역에 대한 보안 모델과 세부 보안 대책을 제시하고 있으며, 국립대병원 뿐만 아니라 민간 종합병원까지 정보보안 담당자가 실무에 쉽게 적용 가능하도록 설계되었다(국가정보원, 2025).

'병원정보시스템 보안 가이드라인'은 병원정보시스템 운영 시 발생할 수 있는 정보보안 사고를 방지하기 위하여 네트워크 보안 대책, 시스템 및 애플리케이션 보안 대책, 관리적 보안 대책과 그 하위 세부 보안 대책을 제시하고 있다.

〈표 3-4〉 병원정보시스템 보안 대책 구성

구분	보안대책	세부 보안대책
네트워크 보안대책	네트워크공통 보안대책	- 네트워크 분리 및 접근제어
	연계 구간별 네트워크 보안대책	- 시스템 내 연계 구간 - 시스템 간 연계 구간 - 인터넷 연계 구간 - 의료기기 및 단말기 연계구간
	상세 네트워크 보안대책	- DMZ 구간 구성 - 망연계 솔루션 - 네트워크 장비에 대한 안전성 설정
시스템 및 애플리케이션 보안대책	시스템 보안대책	- 권한관리 - 접근통제 - 계정관리 - 사용자 인증 - 불필요한 포트 및 서비스 제거 - 시스템 업데일 및 보안패치 - 악성코드 통제 - 정보 유출 통제 - 노트북 및 모바일 기기 관리 - 이동식 저장매체 보안
	애플리케이션 보안대책	- SDLC 및 SPDL 적용 - 웹·애플리케이션 취약점 점검 - 암호화 정책
	의료기기 및 의료정보 보안대책	- 의료기기 보안성 검토 - 의료기기 보안대책 - 의료기기 통신 보안 - 의료정보의 저장·연계 - 제3자 서비스 수준 계약
관리적 보안 대책	정보보안 정책 및 조직	- 정보보안 정책 수립 - 경영진의 책임 - 정보보안 조직의 역할 및 책임 - 인적 보안
	자산 관리	- 정보자산 관리 - 취약점 점검 및 위험평가 - 보안대책 수립
	운영 관리	- 원격 접속 통제 - 외부 유지보수 관리 - 외주 개발 관리 감독 - 로깅과 모니터링 - 백업·복구 및 연속성 관리

구분	보안대책	세부 보안대책
관리적 보안 대책	물리 보안	- 보호구역 지정 - 재난·재해 대비 물리적 보호대책 수립 - 출입 통제 - 작업통제
	환자의 개인정보보호	- 개인정보 개요 - 개인정보의 수집·이용 - 개인정보의 제3자 제공 - 개인정보 처리 업무위탁 - 영업의 양도 - 개인정보파일의 등록(공공의료기관) - 개인정보의 파기 - 개인정보 처리방침의 수립 및 공개 - 개인정보 보호 책임자 지정 - 정보주체의 권익보호 - 피해 구제 방법

출처: 국가정보원. (2025). 병원정보시스템 보안 가이드라인. pp.7-8.

본 가이드라인은 의료기관이 준수해야 하는 기본 보안 수칙을 명시하고 있어 의료기관의 실제적인 보안 업무에 많은 도움이 될 것으로 여겨진다. 다만 본 가이드라인은 법적 효력을 갖지 않은 권고 사항이라는 점에서 분명한 한계가 있다.

나. 의료기기 사이버 보안 허가·심사 가이드라인

'의료기기 사이버 보안 허가·심사 가이드라인'은 의료기기 허가·심사 시 사이버 보안이 요구되는 의료기기의 적용 대상을 명확히 하고 제품의 특성에 따라 적용할 수 있는 보안 요구사항과 허가·심사 시 제출해야 하는 자료의 범위를 정하여 통신이 가능한 의료기기의 안전관리를 확보하고자 마련되었다(식품의약품안전처, 2023). '의료기기 사이버 보안 허가·심사 가이드라인'은 국제 조화를 이루기 위해 국제 의료기기 규제당국자 포럼(International Medical Device Regulators Forum, IMDRF)의 '의료

기기 사이버 보안 원칙 및 지침'(Principles and Practices for Medical Device Cybersecurity, IMDRF, 2020)의 2.0 적용 범위, 3.0 정의, 5.0 시판 전 고려 사항을 차용하여 적용하였다(식품의약품안전처, 2023).

본 가이드라인은 의료기기의 사이버 보안 확보를 위한 것으로 소프트웨어를 포함하는 의료기기[펌웨어(Firmware) 및 프로그램 가능 논리 제어기(Programmable Logic Controller(PLC)를 포함하는 의료기기) 또는 소프트웨어로만 존재하는 의료기기(소프트웨어 의료기기(Software as a Medical Device, SaMD))]중 유·무선 통신(Wi-Fi, 블루투스, USB, RS-232, LAN 등)을 사용하거나 통신 경로가 존재하는 의료기기에 적용한다.

본 가이드라인에 따라 유·무선 통신 경로가 있는 의료기기는 정보의 위·변조, 오작동 또는 의료기기에 승인되지 않은 접근 등을 방지하기 위한 대책을 마련해야 한다. 제조자는 의료기기의 잠재적 결함으로 인해 사용자에게 발생할 수 있는 위해의 정도, 의료기기의 통신 방법 및 사용 환경을 종합적으로 고려하여 의료기기 사이버 보안 요구사항 적용 여부를 식별하고 식별된 요구 사항에 대해 사이버 보안 안전성을 확인할 수 있는 검증자료를 제출하여야 한다(식품의약품안전처, 2023).

의료기기 사이버 보안 요구사항은 식별 및 인증, 사용 통제, 시스템 무결성, 데이터 기밀성, 이벤트 적시 대응, 자원 가용성 등 6개 항목과 그에 따른 요구사항으로 구성되어 있으며, 각각의 요구사항은 구체적인 세부 요구사항, 시험 기준, 시험방법, 적용 예외 사항으로 구성되어 있다.

'의료기기 사이버 보안 허가·심사 가이드라인'은 의료기기 허가·심사 시 사용자의 건강에 직접적인 영향을 미칠 수 있는 사이버 보안 위협에 대하여 적용할 수 있는 최소한의 권고 사항을 제시한다. 다만, 의료기기 허가 후 관리나 사용자(의료기관 등)의 관리적 보안 또는 사용자의 건강

에 직접적으로 영향을 미치지 않는 개인정보 유출 등은 의료법 및 개인정보보호법 등 타 법령을 준수하도록 권장하고 있다.

〈표 3-5〉 의료기기 사이버 보안 요구사항

항목	요구사항 번호	요구사항
식별 및 인증 (IA)	IA-01	- 사용자 식별 및 인증
	IA-02	- 계정관리
	IA-03	- 식별정보 관리
	IA-04	- 인증정보 간리
	IA-05	- 비밀번호 강도 설정
	IA-06	- 인증정보에 대한 피드백
	IA-07	- 연속적인 로그인 시도 실패 시 로그인 제한
	IA-08	- 시스템 사용 알림 메시지
사용 통계 (UC)	UC-01	- 권한 부여
	UC-02	- 모바일 코드 사용 통제
	UC-03	- 세션 잠금
	UC-04	- 감사기록 생성
	UC-05	- 감사 처리 실패 대응
	UC-06	- 타임스탬프
	UC-07	- 부인방지
시스템 무결성(SI)	SI-01	- 통신에 대한 무결성 보장
	SI-02	- 악성코드로부터 보호
	SI-03	- 보안 기능 검증
	SI-04	- 소프트웨어 및 정보에 대한 무결성 점검
	SI-05	- 입력값 검증
	SI-06	- 오류 시 사전 결정된 상태로 출력
	SI-07	- 오류 처리
	SI-08	- 업데이트
	SI-09	- 업데이트에 대한 진본성 및 무결성 검증
	SI-10	- 물리적 변조 방지
	SI-11	- 부트 프로세스 무결성 검증
데이터 기밀성(DC)	DC-01	- 정보에 대한 기밀성 보장
	DC-02	- 보건의료정보 비식별화
	DC-03	- 안전한 암호화 사용
이벤트 적시 대응(TRE)	TRE-01	- 감사로그에 대한 비인가된 접근 제한
자원가용성(RA)	RA-01	- 서비스 거부(Denial of Service, DoS) 방지
	RA-02	- 의료기기 백업
	RA-03	- 의료기기 복구 및 재구성
	RA-04	- 네트워크 및 보안 구성 설정
	RA-05	- 불필요한 기능 비활성화

출처: 식품의약품안전처. (2023). 의료기기의 사이버 보안 허가심사 가이드라인. pp.10-11

다. 정보보호 및 개인정보보호 관리 체계(ISMS-P) 인증 제도

정보보호 및 개인정보보호 관리 체계(ISMS-P) 인증제도는 「정보통신망 이용 촉진 및 정보보호 등에 관한 법률」(이하 '정보통신망법'이라 한다) 제47조, 제47조의2 및 제47조의7, 동법 시행령 제47조부터 제54조까지의 규정과 동법 시행규칙 제3조에 따른 정보보호 관리 체계 인증, 그리고 「개인정보 보호법」 제32조의2와 동법 시행령 제34조의2부터 제34조의8까지의 규정에 따른 개인정보보호 관리 체계 인증을 법적 근거로 한다.

〈표 3-6〉 정보보호 및 개인정보보호 관리 체계 인증(ISMS-P)의 유형

구분	설명
정보보호 관리체계 인증 (ISMS)	- 정보보호 중심으로 인증하는 경우 * 기존의 정보보호 관리체계 인증(ISMS) 의무대상 기업·기관, 개인정보를 보유하지 않거나 개인정보 흐름의 보호가 불필요한 조직 등
정보보호 및 개인정보보호 관리체계 인증(ISMS-P)	- 개인정보의 흐름과 정보보호 영역을 모두 인증하는 경우 * 보호하고자 하는 정보서비스가 개인정보의 흐름을 가지고 있어 개인정보 처리 단계별 보안강화가 필요한 조직
정보보호 관리체계 예비인증	- 가상자산사업자가 실제 서비스 운영 전 임시적으로 시스템을 구축·운영한 경우 * 「특정금융정보법」에 따라 사업 영위를 위하여 신고를 해야 하지만, 2개월 이상의 운영 이력이 없어 정보보호 관리체계 인증(ISMS) 인증 심사를 진행할 수 없는 신규 가상자산사업자

출처: 한국인터넷진흥원. (2024c). 정보보호 및 개인정보보호 관리 체계(ISMS-P) 인증제도 안내서. p.4

정보보호 및 개인정보보호 관리 체계(ISMS-P) 인증제도는 정보보호 및 개인정보보호의 관리 체계 수립 및 운영 여부를 국가 지정 인증기관이 심사·인증하는 제도이며, 인증 유형은 정보보호 관리 체계 인증(ISMS), 정보보호 및 개인정보보호 관리 체계 인증(ISMS-P), 정보보호 관리 체계

예비인증 등 3가지로 구분할 수 있다. 조직의 정보보호를 위해 인증을 취득하고자 하는 경우에는 정보보호 관리 체계 인증(ISMS)을 취득할 수 있으며, 정보서비스에 개인정보 흐름이 포함되어 개인정보 처리 단계별 보안을 강화하고자 하는 경우에는 정보보호 관리 체계 인증(ISMS) 범위에 '개인정보 처리 단계별 요구사항' 분야를 포함하여 정보보호 및 개인정보보호 관리 체계 인증(ISMS-P)을 취득할 수 있다(한국인터넷진흥원, 2024). 한편 정보보호 관리 체계 예비인증은 「특정금융정보법」 제7조 제1항(신고)을 이행하고자 하나 2개월 이상의 운영 이력이 없어 본 인증 취득에 어려움을 겪는 신규 가상자산 사업자가 임시 시스템에 대하여 정보보호 관리 체계 예비인증을 취득할 수 있도록 마련된 제도이다.

정보보호 및 개인정보보호 관리 체계(ISMS-P) 인증 기준은 관리 체계 수립 및 운영(16개), 보호 대책 요구사항(64개), 개인정보 처리 단계별 요구사항(21개)으로 구성되어 있으며, 인증 유형에 따른 인증 기준은 〈표 3-7〉과 같다.

정보보호 및 개인정보보호 관리 체계 인증(ISMS-P) 의무 대상자는 정보통신망 서비스를 제공하는 자(ISP), 정보통신시설 사업자(IDC), 전년도 매출액 또는 세입 등이 1,500억 원 이상이거나 정보통신 서비스 부문의 전년도 매출액이 100억 원 이상 또는 전년도 일일 평균 이용자 수가 100만 명 이상으로서 대통령령으로 정하는 기준에 해당하는 자이다. 의료기관의 경우 「의료법」 제3조의4에 따른 상급종합병원이 정보보호 관리 체계(ISMS) 인증 의무 대상이며, 전년도 매출액 또는 세입이 1,500억 원 이상인 의료기관 중 대통령령으로 정하는 기준에 해당하는 경우에도 의무 대상이 된다.

한편 의료기관의 정보보호 및 개인정보보호 관리 체계 인증(ISMS-P) 또는 정보보호 관리 체계(ISMS) 인증은 의료기관이 자체적으로 정보보호

관리 체계를 수립하고 운영하도록 유도함으로써 단순한 기술적 보안을 넘어 조직 전체의 보안 역량을 강화하는 데 그 의미가 있다. 다만 의료기관의 정보보호 및 개인정보보호 관리 체계 인증(ISMS-P) 제도는 상급종합병원을 제외한 대부분의 의료기관이 인증 의무 대상이 아니기 때문에 의료기관 전반의 보안 역량을 강화하는 데에는 한계가 있다.

〈표 3-7〉 정보보호 및 개인정보보호 관리 체계 인증(ISMS-P)의 유형에 따른 인증 기준

인증 영역	인증기준	항목수	적용 여부	
			ISMS	ISMS-P
1. 관리체계 수립 및 운영(16개)	1.1. 관리체계 기반 마련	6	○	○
	1.2 위험 관리	4	○	○
	1.3 관리체계 운영	3	○	○
	1.4 관리체계 점검 및 개선	3	○	○
2. 보호대책 요구사항 (64개)	2.1 정책, 조직, 자산 관리	3	○	○
	2.2 인적 보안	6	○	○
	2.3 외부자 보안	4	○	○
	2.4 물리 보안	7	○	○
	2.5 인증 및 권한관리	6	○	○
	2.6 접근통제	7	○	○
	2.7 암호화 적용	2	○	○
	2.8 정보시스템 도입 및 개발 보안	6	○	○
	2.9 시스템 및 서비스 운영관리	7	○	○
	2.10 시스템 및 서비스 보안관리	9	○	○
	2.11 사고 예방 및 대응	5	○	○
	2.12 재해 복구	2	○	○
3. 개인정보 처리 단계별 요구사항 (21개)	3.1 개인정보 수집 시 보호조치	7	-	○
	3.2 개인정보 보유 및 이용 시 보호조치	5	-	○
	3.3 개인정보 제공 시 보호조치	4	-	○
	3.4 개인정보 파기 시 보호조치	2	-	○
	3.5 정보주체 권리보호	3	-	○

출처: 한국인터넷진흥원. (2024c). 정보보호 및 개인정보보호 관리 체계(ISMS-P) 인증제도 안내서. p.10.

라. 전자의무기록 시스템 인증 제도

전자의무기록 시스템 인증제는 환자 안전과 진료 연속성 지원을 목적으로 국내 전자의무기록 시스템에 대한 국가적 표준과 적합성 검증을 통해 업체의 표준 제품 개발을 유도하고, 시스템의 상호 호환성 확보 등 품질 향상을 통해 의료소비자에게 양질의 의료서비스가 제공될 수 있도록 하기 위한 제도이다. 이 제도는 「의료법」 제23조의2(전자의무기록의 표준화 등), 동법 시행령 제10조의7(전자의무기록의 표준화), 제10조의8(전자의무기록 시스템의 인증) 및 제10조의9(전자의무기록 시스템의 인증 표시), 그리고 「전자의무기록 시스템 인증제도 운영에 관한 고시」를 법적 근거로 한다.

〔그림 3-1〕 전자 의무 기록 시스템 인증 기준 구성도

출처: 보건복지부. (2025). 전자 의무 기록 시스템 인증 기준 해설서. p.14.

전자의무기록 시스템의 인증 기준은 기능성 27개, 상호운용성 20개, 보안성 12개 등 3개 영역, 57개 인증 기준으로 구성되어 있다.

전자의무기록 시스템 인증 기준 중 보안 관리 인증 기준은 「의료법」 제23조(전자의무기록), 동법 시행규칙 제16조(전자의무기록의 관리·보존에 필요한 시설과 장비 등) 및 「전자의무기록의 관리·보존에 필요한 시설과 장비에 관한 기준」에 따라 전자의무기록 시스템이 의료기관의 의료정보를 안전하게 보존·관리하도록 하는 기능을 요구하는 것이다(보건복지부, 2025).

보안 관리 인증 기준은 접근 관리, 암호화 및 정보보호 관리, 감사 및 접속 기록 관리, 백업 및 외부 보관 등 4개 중분류와 12개 인증 기준으로 구성되어 있으며, 의료기관의 종별 및 규모와 관계없이 모든 의료기관에서 필수적으로 해당 기준을 충족해야 한다.

〈표 3-8〉 전자 의무 기록 시스템 인증 기준 중 보안 관리 인증 기준

대분류	중분류	인증기준	유형1	유형2	유형3
보안 관리	접근관리	계정 및 비밀번호 관리	필수	필수	필수
		권한 및 이력관리	필수	필수	필수
		인증(로그인) 실패 관리	필수	필수	필수
		미사용 시 접속 차단	필수	필수	필수
	암호화 및 정보보호 관리	고유식별정보 암호화	필수	필수	필수
		고유식별정보 마스킹	필수	필수	필수
		비밀번호 암호화	필수	필수	필수
	감사 및 접속기록 관리	접속기록 생성	필수	필수	필수
		의무기록 추가기재·수정 이력 관리	필수	필수	필수
		전자서명	필수	필수	필수
	백업 및 외부 보관	백업	필수	필수	필수
		외부보관 및 클라우드 컴퓨팅 서비스 (의료기관 외부 집적정보통신시설 이용 서비스)	필수	필수	필수

출처: 보건복지부. (2025). 전자 의무 기록 시스템 인증 기준 해설서. p.201.

접근 관리는 개인정보에 대한 접근 권한을 제한하고 접근을 통제하기 위한 기능으로 계정 및 비밀번호 관리, 권한 및 이력 관리, 인증(로그인) 실패 관리, 미사용 시 접속 차단 등 4개 인증 기준으로 구성되어 있다.

암호화 및 정보보호 관리는 개인정보를 안전하게 저장·전송하기 위한 조치와 개인정보 출력 시(인쇄, 화면 표시, 파일 생성 등) 필요한 안전조치를 포함하는 기능으로 고유 식별 정보 암호화, 고유 식별 정보 마스킹, 비밀번호 암호화 등 3개 인증 기준으로 구성되어 있다.

감사 및 접속기록 관리는 전자의무기록의 추가 기재 및 수정 시 전·후 기록 보존 및 접속기록 별도 보관, 전자서명 기능, 전자서명 이후 전자의무기록의 변경 여부 확인 등 전자의무기록의 이력 관리와 개인정보 침해 사고 대응에 필요한 기능으로 접속기록 생성, 의무기록 추가 기재·수정 이력 관리, 전자서명 등 3개 인증 기준으로 구성되어 있다.

마지막으로 백업 및 외부 보관은 전자의무기록의 백업 저장 장비, 의료기관 외부 장소에 전자의무기록 저장 장비 또는 백업 저장 장비를 설치하는 경우의 시설과 장비 요건, 재해·재난 대비 안전조치에 필요한 기능으로 백업, 외부 보관 및 클라우드 컴퓨팅 서비스(의료기관 외부 집적 정보통신 시설 이용 서비스) 등 2개 인증 기준으로 구성되어 있다.

한편, 전자의무기록 시스템 인증제 보안성 인증 기준의 한계는 전자 의무 기록 시스템은 제품을 대상으로 인증서가 발급되며, 사용인증은 기능의 변경 없이 사용하는지 여부를 확인하고 있어서 운영 환경의 정확성을 보증할 수 없다는 것이며, 따라서 전자 의무 기록 시스템이 설치되고 운영되는 환경 및 운영 유지 절차 등에 관한 사항에 대해서는 절차 준수의 정확성을 보증할 수 없다(보건복지부, 2025).

2. 주요 외국의 의료기관 관련 정보보안 제도

가. ISO/IEC 27001

ISO/IEC 27001은 정보보호 관리 체계(ISMS)의 국제표준으로 사이버 위협 환경의 변화에 맞추어 지속적으로 개정되어 왔다. 영국 표준인 BS7799를 기반으로 2005년 ISO/IEC 27001:2005가 국제표준으로 공식 발표되었으며, 2013년에는 다른 경영시스템 국제표준과의 일관성과 통합이 용이하도록 상위 수준 구조(HLS, High-Level Structure)를 적용한 ISO/IEC 27001:2013으로 1차 개정되었고, 2022년에는 정보보호 관리 체계(ISMS) 본문 요구사항을 일부 간소화하고 명확화한 ISO/IEC 27001:2022로 2차 개정되었다.

ISO/IEC 27001의 핵심은 체계적이고 위험 기반(risk-based) 접근 방식이다. 조직이 보유한 정보 자산(데이터, 시스템, 인력 등)의 가치를 평가하고 해당 자산에 대한 잠재적 위험을 식별하며 이를 관리하기 위한 적절한 보호 대책을 수립한다. 이는 모든 위험에 동일한 수준의 자원을 투입하는 대신 가장 중요한 위험에 우선순위를 두어 효율적인 보안 투자를 가능하게 한다.

ISO/IEC 27001은 PDCA(Plan-Do-Check-Act) 사이클을 통해 ISMS의 지속적인 개선을 위한 구조를 제공한다. 계획(Plan) 단계에서는 정보보안 정책과 목표를 수립하고 위험을 평가하며, 실행(Do) 단계에서는 계획에 따라 보호 대책을 이행한다. 점검(Check) 단계에서는 시스템의 효과를 모니터링하고 내부 감사를 수행하며, 조치(Act) 단계에서는 점검 결과를 바탕으로 개선 활동을 수행하여 시스템이 최신 위협에 대응할 수 있도록 한다.

최신 버전인 ISO/IEC 27001:2022의 부속서 A(Annex A)에는 정보보안 위험을 처리하기 위해 고려해야 할 통제 항목으로 조직적 통제(37개), 인적 통제(8개), 물리적 통제(14개), 기술적 통제(37개) 등 4개 영역에 걸쳐 총 93개의 통제 항목이 제시되어 있다.

이 표준은 특정 산업에 국한되지 않고 모든 산업 분야와 규모의 조직에 적용될 수 있지만 의료기관이 사이버 보안 및 정보보호 관리 체계를 구축하고 운영하는 데에도 효과적인 프레임워크를 제공한다. 특히 민감한 개인정보인 환자 정보를 다루는 의료기관에서는 정보보안 및 정보보호에 대한 국제 기준을 충족함으로써 환자의 신뢰를 확보하고 관련 법규 준수를 체계적으로 관리할 수 있기 때문에 ISO/IEC 27001 인증을 활용하고 있다.

나. ISO/IEC 80001-1

ISO/IEC 80001-1은 의료기기가 IT 네트워크에 통합될 때 발생하는 위험을 관리하기 위한 국제표준이다. 이 표준은 의료기기가 단순히 네트워크에 연결되는 것을 넘어, 병원 내 전체 IT 시스템의 일부로서 기능할 때 환자의 안전, 기기의 유효성, 그리고 데이터 및 시스템 보안이 유지되도록 하는 것을 목표로 한다.

이 표준의 핵심 원칙은 책임 명확화와 위험 기반 접근이다. 의료기기 제조업체뿐 아니라 의료기관에도 네트워크에 연결된 의료기기의 안전한 사용에 대한 책임을 명확히 부여하고 있으며 이는 의료기기를 구매·설치·운영하는 과정에서 발생할 수 있는 잠재적 위험을 관리하기 위한 것이다. 또한 ISO/IEC 80001-1은 ISO 14971(의료기기 위험관리 표준)과 연계하여 네트워크에 연결된 의료기기로 인해 발생할 수 있는 위험을 식

별·평가·통제하는 체계적인 프로세스를 제시한다. 이 과정에는 잠재적 위해(harm)의 심각성, 발생 가능성, 그리고 환자 안전, 기기 유효성, 데이터 및 시스템 보안에 미치는 영향을 종합적으로 고려해야 한다.

이 표준에서는 의료기기 네트워크의 위험관리가 안전(safety), 유효성(effectiveness), 보안(security) 등 세 가지 핵심 속성을 유지해야 한다고 강조하고 있다. 첫째, 안전은 환자, 사용자, 제3자에게 신체적 상해나 건강상의 위해가 발생하지 않도록 하는 것이다. 둘째, 유효성은 의료기기가 의도된 임상적 목적에 맞게 올바르게 기능하도록 하는 것이다. 셋째, 보안은 정보 자산의 기밀성, 무결성, 가용성을 비인가된 활동으로부터 보호하는 것을 의미한다.

ISO 80001-1은 의료기기가 네트워크에 연결되기 전(사전 평가), 연결되는 동안(설치 및 통합), 그리고 사용 및 유지 보수되는 전체 기간에 걸쳐 위험관리가 이루어져야 한다고 요구하고 있으며, 변경 사항이 발생할 때마다 위험을 재평가하여 새로운 위협에 대응할 수 있도록 한다.

다. 미국 NIST Cybersecurity Framework(NIST, 2024a)

NIST Cybersecurity Framework(CSF)는 미국 국립표준기술원(National Institute of Standards and Technology, NIST)이 개발한 사이버 보안 관리 프레임워크로 특정 기술적 요구사항을 강제하기보다는 조직이 사이버 보안 위험을 관리하고 개선하는 데 활용할 수 있는 자발적 가이드라인을 제공한다. 이는 모든 규모와 산업 분야의 조직이 자체적인 위험관리 전략을 수립하고 실행할 수 있도록 지원한다.

NIST CSF(Cybersecurity Framework)는 2013년 미국의 주요 기반 시설 사이버 보안 강화를 위해 개발되었으며 2014년에는 5가지 핵심 기

능(식별, 보호, 탐지, 대응, 복구)을 중심으로 프레임워크 코어(Core), 프로파일(Profile), 구현 계층(Implementation Tier)의 세 가지 요소로 구성된 CSF 1.0이 발표되었다. 이후 사이버 보안 환경 변화와 다양한 조직의 활용 수요를 반영하여 최신 버전인 CSF 2.0이 2024년에 발표되었다.

NIST CSF의 핵심은 거버넌스(Govern), 식별(Identify), 보호(Protect), 탐지(Detect), 대응(Respond), 복구(Recover) 등 여섯 가지 핵심 기능으로 구성되며 이러한 기능은 사이버 보안 위협에 대한 조직의 방어 역량을 체계적으로 관리하기 위한 주요 활동 영역을 나타낸다.

[그림 3-2] NIST CSF 2.0 프레임워크

출처: National Institute of Standards and Technology. (2024a). The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29). U.S. Department of Commerce., p.6.

거버넌스 기능은 조직의 사이버 보안 위험관리 활동 전반에 대한 전략적 리더십과 방향을 제시한다(NIST, 2024a). 이 기능은 조직의 사이버 보안 위험관리 전략, 기대치, 그리고 정책이 명확하게 수립되고, 조직 전

체에 효과적으로 전달되며, 그 이행 여부가 지속적으로 모니터링되도록 보장한다(NIST, 2024a). 거버넌스 활동은 조직이 자신의 임무와 이해관계자의 기대라는 큰 틀 안에서 나머지 5가지 기능(식별, 보호, 탐지, 대응, 복구)의 결과를 어떻게 달성하고 우선순위를 정할지에 대한 정보를 제공하는 상위 수준의 방향을 제시한다(NIST, 2024a). 따라서 거버넌스는 사이버 보안을 단순한 기술적 문제가 아니라 조직의 보다 광범위한 전사적 위험관리(Enterprise Risk Management, ERM) 전략에 통합하는 데 결정적인 역할을 수행한다(NIST, 2024a). 구체적으로 거버넌스 기능이 다루는 핵심 영역은 조직의 상황에 대한 이해를 바탕으로 사이버 보안 전략과 사이버 보안 공급망 위험관리(Cybersecurity Supply Chain Risk Management, C-SCRM)를 수립하고 이에 따른 역할·책임·권한을 명확히 하며 관련 정책을 정의하고 수립된 사이버 보안 전략 전반에 대한 감독 체계를 갖추는 것을 포함한다(NIST, 2024a).

식별 기능은 조직의 현재 사이버 보안 위험을 이해하는 데 필수적이다. 이 기능은 조직의 자산(데이터, 하드웨어, 소프트웨어, 시스템, 시설, 서비스 및 인력 등), 공급업체 및 관련 사이버 보안 위험을 파악할 수 있도록 함으로써, 조직이 거버넌스 기능에서 정의된 위험관리 전략과 임무 요구사항에 부합하도록 노력의 우선순위를 정할 수 있다(NIST, 2024a). 더불어 이 기능은 조직의 정책, 계획, 프로세스, 절차 및 관행 중에서 사이버 위험 관리를 지원하는 부분에 대한 개선 기회를 식별하며, 이는 여섯 가지 기능 전체의 노력에 정보를 제공하는 기반이 된다(NIST, 2024a).

보호 기능은 조직의 사이버 보안 위험을 관리하기 위한 안전장치로 사용된다(NIST, 2024a). 자산과 위험이 식별되고 우선순위가 지정되면, 보호기능은 해당 자산을 보호하여 부정적인 사이버 보안 사건의 발생 가능성과 영향을 방지하거나 낮추고, 기회를 활용할 가능성과 영향을 높이는

능력을 지원한다(NIST, 2024a). 이 기능의 주요 결과에는 신원 관리, 인증 및 접근통제, 인식 제고 및 교육, 데이터 보안, 플랫폼 보안, 기술 인프라의 복원력 확보 등이 포함된다(NIST, 2024a).

탐지 기능은 잠재적인 사이버 공격과 침해를 찾아내고 분석하는 역할을 한다(NIST, 2024a). 이 기능은 사이버 공격 및 사건이 발생하고 있음을 나타낼 수 있는 비정상적인 상황, 침해 지표(Indicators of Compromise), 그리고 기타 잠재적으로 불리한 이벤트를 시기적절하게 발견하고 분석할 수 있도록 지원한다(NIST, 2024a). 탐지 활동은 성공적인 사건 대응 및 복구 활동을 수행하는 데 필수적인 선행 단계이다(NIST, 2024a).

대응 기능은 탐지된 사이버 보안 사건에 대해 실제적인 대응 조치를 수행하는 활동을 지원한다(NIST, 2024a). 이 기능은 사이버 보안 사건의 영향을 억제하는 능력을 지원하며, 사건으로 인한 피해 확산을 막는 데 초점을 맞추고 있다(NIST, 2024a). 이 기능의 결과에는 사건 관리, 분석, 완화 조치, 보고 및 소통이 포함된다(NIST, 2024a).

복구 기능은 사이버 보안 사건으로 인해 영향을 받은 자산 및 운영을 복구하는 데 필요한 활동을 포함한다(NIST, 2024a).

NIST CSF는 단순한 기술적 솔루션 목록이 아니라 조직의 경영진과 보안 담당 조직이 협력하여 사이버 보안 문제를 비즈니스 위험 관점에서 접근하도록 유도하는 프레임워크이다.이 프레임워크는 유연성이 높아 ISO/IEC 27001, HIPAA 등 다양한 산업 표준 및 규제와 함께 활용될 수 있으며 조직의 사이버 보안 성숙도를 평가하고 개선 방향을 제시하는 데 효과적인 도구로 활용된다.

NIST CSF는 의료기관 및 보건의료 분야에서 사이버 위험을 관리하고 미국의 HIPAA(Health Insurance Portability and Accountability Act) 규정을 준수하는 데 있어 가장 널리 활용되는 프레임워크 중 하나이

다. NIST CSF는 그 자체로 규제는 아니지만 미국 의료기관의 HIPAA Security Rule 준수를 위한 실질적인 가이드라인 역할을 하고 있다.

라. (유럽연합) NIS2 지침(European Union, 2022)

이 지침은 유럽연합(EU) 전역에서 보다 높은 공동 사이버 보안 수준을 달성하기 위한 조치를 규정한 것으로 총 18개 주요 분야(고위험 분야 11개, 기타 중요 분야 7개)에서 사이버 보안을 강화하기 위한 통합된 법적 체계를 구축하고 회원국들이 국가 사이버 보안 전략을 수립하며 국경 간 대응 및 집행을 위해 유럽연합과 협력할 것을 요구하고 있다(EU, 2025).

이 지침은 유럽연합 전체에서 높은 수준의 사이버 보안을 달성하기 위한 조치를 규정하고 있으며 이를 위해 회원국이 국가 사이버 보안 전략을 채택하고 법적 기관, 사이버 위기관리 기관, 사이버 보안에 대한 단일 연락 창구(Single Point of Contact) 및 컴퓨터 보안 사고 대응팀(CSIRT)을 지정하거나 설립하도록 요구한다. 또한 중요 기관으로 지정된 기관에 대한 사이버 보안 위험관리 조치와 사고 보고 의무, 그리고 회원국의 감독 및 집행 의무를 함께 규정하고 있다.

이 지침은 회원국이 사이버 보안 역량을 강화하도록 요구하는 동시에, 더 많은 분야의 기관에 위험관리 조치 및 보고 요건을 도입하고, 협력, 정보 공유, 감독 및 사이버 보안 조치 시행에 대한 규칙을 수립하도록 요구하고 있다. 또한 각 회원국이 공급망 보안, 취약성 관리, 사이버 보안 교육 및 인식 제고 정책을 포함하는 국가 사이버 보안 전략을 채택하도록 규정하고 있다. 이에 따라 회원국은 필수 서비스 운영자 목록을 작성하고 이를 정기적으로 업데이트하여 해당 기관들이 이 지침의 요구사항을 준수하도록 관리해야 한다.

이 지침에는 유럽연합 전역의 상호 신뢰와 사이버 보안 역량 강화를 위한 감독, 집행 및 자발적 동료 평가 조항도 포함되어 있으며 사이버 보안 위험관리 조치 미준수에 대한 최고 경영진의 책임을 규정함으로써 이사회 차원의 사이버 보안 관리 책임을 강조하고 있다.

한편 사이버 위협 정보 교환과 사고 대응을 위해 컴퓨터 보안 사고 대응팀(CSIRT) 네트워크가 구축되었으며 대규모 사이버 보안 사고나 위기 상황을 관리하기 위해 유럽 사이버 위기 연락망(EU-CyCLONe)이 운영되고 있다.

마. 일본: 의료정보시스템 안전관리 가이드라인(후생노동성, 2023)

일본 후생노동성의 '의료정보시스템 안전관리 가이드라인'은 2005년 3월 초판이 제정되었으며 정보통신 기술 및 법적 환경 변화에 맞추어 여러 차례 개정되었다. 2023년 5월에는 최신 기술 동향과 의료기관에 대한 사이버 공격의 다양화 및 고도화에 대응하기 위해 최신 버전인 제6.0판이 개정되었다.

이 가이드라인의 목적은 의료정보시스템의 안전관리를 통해 의료의 질을 향상시키고 의료정보 보호와 시스템의 안정적 운용을 확보하는 것이다. 또한 의료기관, 의료정보시스템, 의료정보를 처리하는 인력 등 가이드라인이 적용되는 주체와 범위를 정의하고 있으며 의료정보의 높은 중요성을 강조하고 시스템의 안정적 운용이 환자의 생명과 직결된다는 점을 명시하고 있다.

이 가이드라인은 의료기관 보안을 경영층(경영 관리), 기획자(기획 관리), 운영자(시스템 운용)로 구분하여 맞춤형 지침을 제공하고 있다. 경영 관리편은 의료정보 시스템의 안전관리에 대한 경영진의 책임과 의무를

명확히 제시하고 있다. 최고 경영진이 안전관리의 최종적인 책임을 진다는 점을 명시하고, 이를 위한 역할과 의무(정보보안 방침 수립, 위험관리, 인력 및 예산 확보 등)를 규정하고 있다. 또한 사이버 공격이나 자연재해 등으로 시스템이 중단될 경우에 대비하여 의료서비스를 지속적으로 제공하기 위한 사업연속성계획(BCP)을 수립하고 이를 정기적으로 검토하고 훈련할 것을 강조하고 있다. 그리고 시스템 사업자 관리에 있어서 외부 정보시스템 및 서비스 제공업체(클라우드 등)를 선정하고 관리하는 기준을 제시하고 있다. 사업자의 보안 체계를 검토하고, 계약서에 보안 관련 내용을 명확히 포함하도록 요구하고 있다.

기획 관리편은 의료정보 시스템의 안전관리를 실질적으로 기획하고 실행하는 담당자를 위한 지침이다. 가이드라인에 따른 안전관리 체제를 조직 내에 구축하고, 각 부서와 담당자 간의 역할 분담을 명확히 할 것을 요구하고 있다. 또한 ISO/IEC 27001과 같은 국제 표준을 참고하여 의료정보시스템의 안전관리를 체계적으로 실행하고 유지할 수 있는 정보보안 관리체계(ISMS)를 구축하는 방법을 제시하고 있다. 그리고 위험평가 방법, 위험평가에 따른 대책 수립, 그리고 이를 주기적으로 재검토하고 개선하는 절차를 상세하게 설명하고 있으며, 정보보안 규정을 제정하고 지속적으로 교육 및 훈련을 하도록 안내하고 있다.

시스템 운용편은 의료정보시스템의 일상적 운영과 기술적 보안 대책에 중점을 두고 있으며 시스템 개발 및 운영 시 준수해야 할 기술적·물리적 보안 규정을 제시하고 있다. 의료정보 시스템에 대한 접근 권한을 관리하고, 사용자 인증(패스워드, 다중 인증 등)을 강화하는 방법을 명시하고 있다. 또한 시스템을 외부 네트워크와 분리하거나 방화벽을 설정하는 등 네트워크 보안 대책과 데이터 백업, 암호화, 반출 및 폐기 절차에 대한 데이터 보안 기준을 제공하고 있다. 또한 최신 사이버 위협 정보를 지속적으로

파악하고 시스템 취약점을 관리하며 침입 탐지 및 방어 시스템을 운영하는 등 사이버 보안을 위한 구체적인 기술적 대응 방안을 제시하고 있다.

이 가이드라인은 일본 후생노동성이 의료기관이 의료정보시스템의 안전관리를 위해 참고하고 준수해야 할 지침을 제시한 것으로 「개인정보보호법」, 「의료법」 등 상위 법령의 내용을 의료 분야에 맞게 구체화하고 해석한 것이다. 따라서 이 가이드라인을 위반했다고 해서 직접적인 법적 처벌을 받지는 않지만 해당 지침을 준수하지 않아 사고가 발생할 경우 관련 법규 위반으로 이어질 수 있다.

제3절 소결

본 장에서는 정보보안(일반법)과 보건의료(특별법)를 2×4 분석틀(예방-탐지·분석-대응·복구-사후 활동 × 정보보안-보건의료)에 교차 적용하여 국내 의료기관 사이버 보안 법·제도 현황과 정책 동향을 점검하였다.

점검 결과 개인정보보호법·정보통신망법·정보통신기반보호법 등 일반 법령은 단계별 의무, 신고·통지 기한, 시정·개선 명령 및 제재 체계가 비교적 명확하게 규정되어 있어 사고 전 주기에 걸친 관리 사이클이 작동하는 반면, 의료법 체계는 예방과 탐지·분석 단계의 규정 비중이 높고 대응·복구 및 사후평가로 이어지는 폐쇄루프(Closed-loop)형 관리가 취약한 것으로 나타났다.

특히 의료기관 내부 거버넌스 측면에서 정보보호 최고책임자(CISO) 지정, 전담 조직의 권한과 역할, 정례 교육·훈련의 법정 의무화 수준이 일반 법령 대비 미흡하다. 침해사고 통지의 주체와 절차는 규정되어 있으나 신고 기한과 양식, 미통지 시 제재 기준이 구체화되어 있지 않아 현장 집행력이 떨어지고, 사후평가-재발 방지 계획-이행점검-재평가로 이어지는 절차도 제도적으로 내재화되지 못하고 있다. 그 결과 사고 이후의 학습과 내부 통제가 기관별 자율 수준에 머물 가능성이 높다.

제도 수단 측면에서는 EMR 인증제가 기능성·상호운용성·보안성을 포괄하나, 실제 환자 데이터 흐름에 긴밀히 연동되는 OCS·LIS·PACS 등 진료 지원 시스템이 인증평가의 직접 대상에서 벗어나 있는 구조적 한계가 확인된다.ISMS-P는 관리 체계 전반을 다루는 강점이 있으나 의료 부문에서 의무 적용 범위가 제한적이어서 산업 전반의 보안 역량의 하방 균형을 끌어올리는 데 제약이 있다.

반면 국가정보원의 '병원정보시스템 보안 가이드라인'과 식품의약품안

전처의 '의료기기 사이버 보안 허가·심사 가이드라인'은 현장의 실무 적용성을 높이는 상세 대책을 제공하지만 권고 성격이라는 한계로 인해 제도적 구속력과 지속 가능한 이행 점검 체계로 연결되기 어렵다.

국외 동향은 거버넌스의 선행 배치와 위험 기반 접근(Risk-based approach)을 공통적으로 강조한다.NIST CSF 2.0은 '거버넌스(Govern)' 기능을 핵심 축으로 격상하여 전사적 위험관리와 공급망 위험관리(C-SCRM)를 결합하고 ISO/IEC 27001은 PDCA 기반의 지속 개선 구조를 통해 관리 체계의 지속적 개선을 가능하게 한다. 일본 후생노동성 가이드라인은 경영층–기획자–운영자별 역할을 명확히 규정하여 조직 내 책임의 단절을 완화한다. 이러한 흐름은 국내 의료법 체계가 기술·조치 목록 중심을 넘어, 조직책임·감독·사후 개선까지 포함하는 관리 체계 법제를 보강해야 함을 시사한다.

정책적으로는 첫째, 의료기관의 규모와 정보시스템 복잡도에 비례한 정보보호 책임자(CISO) 지정 의무와 내부 보안 조직 운영 기준을 법률 및 시행령 수준에서 명문화하고, 정례 교육·모의훈련의 최소 주기, 범위 및 평가 기준을 표준화할 필요가 있다. 둘째, 진료 정보 침해사고의 신고 기한(예: 인지 후 72시간 이내), 통지 양식, 미이행 시 제재 기준을 구체화하여 탐지–통지–분석 절차의 신속성과 책임성을 높여야 한다. 셋째, EMR 중심 인증을 의료기관 내 데이터 연동 생태계 전반(EMR-OCS-LIS-PACS-의료기기)으로 확장하거나 상호 연계성과 보안성을 동시에 평가하는 공동 평가 모듈을 도입하여 실제 운영 환경의 위험을 반영할 필요가 있다. 넷째, ISMS-P와 EMR 인증 간 교차 인정 또는 연계 평가 체계를 설계하여 중복 부담을 줄이면서 핵심 통제의 실효성을 높이고, 상급종합병원 외 대형·중형 병원에 대한 단계적 의무화 및 인센티브 정책을 병행할 필요가 있다. 다섯째, 다섯째, 사후관리 공백을 해소하기 위해 사후평가–

재발 방지 계획 제출–이행점검–재평가로 이어지는 폐쇄루프(Closed-loop) 관리 절차를 정례화하고, ISAC과 연계한 위협 정보 및 사고 사례 공유 체계를 제도화하여 조직 간 학습을 촉진할 필요가 있다. 여섯째, 여섯째, 의료기기 사이버 보안 관리에서는 허가·심사 단계의 요구사항과 병원 운영 단계의 관리 통제를 연계하고, 공급망 보안, 취약점 관리, 패치 관리 거버넌스를 포함하는 계약 및 조달 기준을 정비할 필요가 있다.

종합하면, 종합하면 국내 의료기관 사이버 보안 체계는 다층의 가이드라인과 개별 제도가 축적되어 있음에도 불구하고 전사적 거버넌스, 신고 체계, 사후 개선 절차의 규범화를 통해 '침해사고 전 주기 관리 체계'가 하나의 관리 사이클로 작동하도록 하는 법제 개선이 핵심 과제로 도출된다.

제4장

의료기관 사이버 보안 침해 사례

제 4 장 의료기관 사이버 보안 침해 사례

제1절 국내 사례[2)]

국내 의료기관은 디지털 전환의 가속화에 따라 전자의무기록(EMR), 의료영상저장전송시스템(PACS), 처방·검사 오더링 시스템 등 정보화 수준이 높아지고 있으나, 이러한 시스템 의존성의 증가는 곧 사이버 위협 노출을 확대시키는 결과로 이어지고 있다. 특히 병원 운영의 핵심 데이터가 디지털 환경에 집중되어 있음에도 불구하고, 상당수 기관에서는 보안 인력과 전담 조직이 부족하여 위협 탐지와 사고 대응이 체계적으로 이루어지지 못하는 실정이다. 이러한 구조적 한계 속에서 2020년 이후 보고된 국내 의료기관 침해사고는 꾸준히 증가하고 있으며, 그 중에서도 랜섬웨어 공격이 절대적 비중을 차지하고 있다.

침해사고의 주요 진입 경로는 원격 데스크톱 프로토콜(RDP)과 데이터베이스 포트(1433) 등 외부 개방 서비스, VPN 장비의 알려진 취약점, 그리고 악성 이메일 등으로 확인된다. 초기 계정과 비밀번호를 변경하지 않거나 보안 업데이트를 지연하는 관리적 취약성 역시 공격자에게 빈번히 악용되는 요소이다. 공격 과정에서는 Mimikatz, Process Hacker, AnyDesk, NirSoft 계열 패스워드 추출 도구 등 상용화된 해킹 도구가 사용되어 계정 정보 탈취와 권한 상승, 내부 확산이 반복적으로 이루어졌다. 이는 공격자가 고도의 맞춤형 공격 기법보다는 이미 검증된 도구와 취약점 악용을 결합하여 상대적으로 낮은 비용으로 큰 피해를 유발했음

2) 한국사회보장정보원. (2025). 의료정보보호센터 내부 자료

을 시사한다.

피해는 의료기관의 핵심 운영 자산에 집중되었다. EMR과 PACS를 비롯하여 진단검사 서버, 회계 및 보험 청구 시스템, 가상화 서버 이미지까지 암호화 피해를 입은 사례가 다수 보고되었으며 백업용 NAS나 외장 저장장치까지 동시 감염된 경우도 적지 않았다. 이로 인해 일부 기관에서는 단순한 데이터 손실을 넘어 응급실 진료 지연, 수술 일정 차질, 영상검사 중단 등 환자 안전에 직결되는 의료서비스 차질이 발생하였다.

사건의 결과는 기관별 복구 역량에 따라 크게 달라졌다. 별도 네트워크에 보관된 백업 데이터를 통해 비교적 신속하게 정상화를 달성한 경우가 있는 반면 복구 수단이 없었던 기관들은 해커에게 금전이나 가상화폐를 직접 지불한 뒤 복구 키를 확보하는 방식으로 운영을 재개하였다. 또한 복구가 부분적으로만 이루어져 영상 데이터나 검사 기록이 장기간 손실된 채 불완전하게 운영을 지속한 사례도 존재하였다. 특히 소규모 의원과 중소병원에서는 전담 보안 인력의 부재와 제한된 예산으로 인해 이러한 불완전 복구나 금전 지불 의존 사례가 더 빈번하게 나타났다.

1. 의원 사례

가. 사례 1 (2024년) – Steloj 랜섬웨어 감염과 가상화폐 지불

2024년 한 의원급 의료기관은 데이터베이스(DB) 포트를 외부에 그대로 개방한 상태로 운영되고 있었다. 이러한 환경은 보안 패치 미적용, 포트포워딩 설정 등과 맞물려 외부 공격자에게 사실상 “열린 문”과 같은 상황을 제공하였다. 결국 Steloj 계열 랜섬웨어가 침투하여 EMR 서버 전체가 암호화되었고 환자 진료기록과 처방 데이터에 접근할 수 없는 상황이

발생하였다.

기관은 전담 IT 담당자가 부재하여 초기 대응이 늦었고 내부적으로는 환자 데이터를 확인할 방법이 전혀 없었다. 응급 진료와 외래 진료는 수기 방식으로 전환되었으나 환자 불편이 크게 증가했고 병원 신뢰도에도 악영향을 미쳤다. 복구 방안을 찾지 못한 기관은 공격자와 직접 협상에 나설 수밖에 없었으며 약 0.0142 BTC(당시 약 126만 원 상당)를 지불한 뒤 복구 키를 확보하였다. 복구는 단계적으로 진행되었으나 일부 파일은 손상되어 완전하게 복구되지 못하였다.

이 사례는 소규모 의료기관이 구조적으로 취약한 보안 환경에 놓여 있으며 결국 공격자와의 협상에 의존할 수밖에 없는 현실을 보여준다. 특히 소액의 가상화폐 지불이 실제 의료기관 운영 과정에서 발생했다는 점에서 국내 의료기관 사이버 보안 거버넌스의 취약성을 보여주는 사례로 평가될 수 있다.

나. 사례 2 (2024년) – PACS 20TB 영상 데이터 손실

2024년 또 다른 의원에서는 TRINITY LOCK 계열 랜섬웨어가 PACS 서버와 검진 서버를 공격하였다. 총 20TB에 달하는 대규모 영상 데이터가 암호화되었고 OS 부팅 영역까지 훼손되면서 서버 자체가 정상적으로 구동되지 않았다. EMR과 검진 서버는 백업 데이터를 통해 복구가 가능했으나 PACS에 저장된 영상 데이터는 일부만 복구되었고 상당량의 데이터는 영구적으로 손실되었다.

이 사건은 의료영상 데이터의 특수성과 대용량 특성을 감안할 때, 단순한 백업으로는 충분한 대비가 되지 않음을 보여준다. 영상 데이터는 주기적 백업이 어렵고 복구 시간도 길어, 공격 발생 시 환자 치료 일정이 장기

간 지연될 수 있다.

다. 사례 3 (2020년) – 백업 동시 암호화, 3,300만 원 지불

2020년 한 의원급 의료기관에서는 EMR 서버와 백업 서버, 외장 HDD까지 동시에 암호화되는 사건이 발생하였다. 공격자는 동일 네트워크 상에 있던 모든 저장 자산을 목표로 삼았고 결과적으로 환자 진료 기록 전체가 암호화되어 접근이 불가능한 상태가 되었다.

의료기관은 복구 수단이 전혀 없는 상태에서 약 3,300만 원 상당의 금액을 지불하고 복구 키를 확보하였다. 복구 이후에도 데이터 일부는 손상되었고 환자 진료는 며칠간 지연되었다. 이 사건은 백업 데이터가 네트워크로부터 물리적으로 분리되지 않을 경우 동일한 공격에 의해 동시에 암호화될 수 있다는 점을 보여주는 사례로 평가된다.

2. 병원 사례

가. 사례 1 (2023년) – BlackCat 랜섬웨어, VPN 취약점 악용

2023년 국내 한 병원은 국제적으로 활동하는 BlackCat 랜섬웨어 조직의 공격을 받았다. 병원은 환자 진료 시스템의 원격 접근 편의를 위해 VPN 장비를 운영하고 있었는데 이미 공개된 취약점이 장기간 패치되지 않은 상태였다. 공격자는 해당 취약점을 통해 내부망으로 침입하였고 초기 단계에서 관리자 권한을 확보한 뒤 주요 서버에 대한 암호화 작업을 수행하였다.

피해는 병원의 핵심 인프라 전반으로 확산되었다. EMR, OCS, PACS

등 총 9대의 주요 서버가 감염되었으며 환자의 진료 기록과 영상 자료, 검사 결과 조회가 전면 불가능해졌다. 응급 환자는 인근 병원으로 이송되어야 했고 예약된 수술 일정도 대거 연기되었다. 이 과정에서 의료진은 종이 차트와 수기 입력 방식으로 응급 대응을 이어갔지만 정상적인 진료 서비스의 질은 크게 저하되었다.

병원은 내부 IT 팀과 유지보수 업체의 협력을 통해 복구를 시도했으나 고도화된 랜섬웨어 암호화 방식으로 인해 자체 복구는 불가능하다는 결론에 도달하였다. 결국 병원은 공격자와 접촉하여 금전을 지불하고 복구키를 확보하였다. 복구 과정은 단계적으로 진행되어 약 1주일 후에야 정상 진료가 가능했으며 그 사이 환자 민원과 언론의 관심이 집중되었다.

이 사건은 글로벌 랜섬웨어 조직이 국내 병원을 직접적인 공격 대상으로 삼기 시작했다는 점에서 중요한 의미를 가진다. 해외 랜섬웨어 조직의 공격 패턴이 VPN 장비 취약점을 통해 국내 의료 환경에 그대로 적용된 사례로 일반적인 정보보안 취약점이 실제 의료서비스 중단으로 이어질 수 있음을 보여주는 사례로 평가된다.

나. 사례 2 (2022년) – Phobos 랜섬웨어, 비트코인 지불

2022년 한 중규모 병원에서는 Phobos 계열 랜섬웨어 공격이 발생하였다. 병원은 EMR 서버를 인터넷에 직접 연결한 상태로 운영하고 있었는데 보안 업데이트가 제때 이루어지지 않아 공격자에게 쉽게 침투 경로를 제공하였다.

공격자는 원격 접속을 통해 서버에 진입한 뒤 주요 데이터베이스 파일을 암호화하였다. 감염 직후 병원 전체의 진료 기록 접근이 차단되었고 의료진은 환자의 과거 진료 기록을 확인할 수 없는 상황에 놓였다. EMR

을 기반으로 한 처방 및 검사 연동도 불가능해지면서 의료기관은 사실상 진료 중단에 가까운 상황에 직면하였다. 환자 진료는 임시로 수기 방식으로 전환되었으나 환자 대기 시간이 크게 증가하였고 의료사고 가능성에 대한 우려도 제기되었다.

해당 병원은 별도의 오프라인 백업이나 이중화 체계를 마련하지 않은 상태였다. 내부적으로 복구를 시도했으나 모든 데이터가 암호화된 상태에서는 복구 방법을 찾지 못하였고 결국 공격자와 직접 협상을 통해 0.4 BTC(당시 약 1,100만 원 상당)를 지불하였다. 지불 이후 복구 키를 제공받아 데이터를 복구하였지만 일부 파일은 손상된 상태로 남아 완전한 복구는 이루어지지 못하였다.

이 사건은 국내 의료기관에서도 실제로 가상화폐 지불이 이루어졌음을 확인할 수 있는 사례라는 점에서 의미가 있다. 또한 중규모 병원이라 하더라도 별도의 DR(Disaster Recovery) 체계가 마련되어 있지 않으면 공격자와의 협상 외에는 대응 수단이 제한될 수 있음을 보여주는 사례로 평가된다.

다. 사례 3 (2021년) – Avaddon 랜섬웨어, 내부 확산과 권한 탈취

2021년 한 병원은 Avaddon 계열 랜섬웨어 공격으로 광범위한 피해를 입었다. 최초 침투 경로는 명확히 확인되지 않았으나 공격자는 네트워크 진입 직후 Mimikatz와 같은 권한 탈취 도구를 실행해 관리자 계정을 확보하였다. 이후 Process Hacker와 PCHunter와 같은 도구를 이용하여 보안 솔루션 프로세스를 무력화시킨 뒤 내부 서버 전반으로 랜섬웨어를 확산시켰다.

감염 범위는 웹 서버, OCS/EMR, 가상화 서버 6대, NAS 저장소, PC

2대에 이르렀다. 병원은 응급실 운영을 일시적으로 중단하였고 예약된 수술 일정도 연기해야 했다. 환자 기록과 검사 데이터가 암호화되면서 의료진은 환자의 과거 진료 이력을 확인할 수 없었으며 일부 환자는 타 의료기관으로 전원 조치가 이루어졌다.

병원은 외부 보안업체와 협력하여 복구를 시도하였으나 데이터 일부는 손상된 상태로 남아 완전한 복구가 이루어지지 않았다. 복구에는 수 주의 기간이 소요되었으며 그 기간 동안 병원은 정상적인 의료서비스 운영을 하지 못하였다. 이 사건은 공격자가 고급 해킹 기법이 아닌 범용 해킹 도구의 조합만으로도 병원 전체 시스템을 단기간에 무력화할 수 있음을 보여주는 사례이다.

3. 종합병원 사례

가. 사례 1 (2024년) – TRINITY LOCK, 대규모 영상 데이터 손실

2024년 한 종합병원에서는 TRINITY LOCK 계열 랜섬웨어 감염이 발생하였다. 공격자는 외부에 노출된 원격 접속 서비스의 보안 설정 미비를 이용해 내부망에 침투한 뒤 주요 서버들을 빠르게 암호화하였다. 피해는 EMR 서버, PACS 서버, 검진 서버 등 총 5대의 주요 서버에 걸쳐 발생했으며 특히 PACS 서버에는 약 20TB에 달하는 환자 영상 데이터가 저장되어 있었다.

영상 데이터는 수년간 축적된 검사 기록으로 암호화 직후 의료진은 환자의 과거 영상 비교와 진단을 즉시 수행할 수 없었다. 응급 상황에서는 일부 환자의 검사와 수술이 지연되었고 장기 치료 환자의 경우 기존 영상 자료가 없어 치료 계획 수립에도 차질이 발생하였다. 또한 서버 자체의

운영체제 부팅 영역까지 손상되어 단순한 데이터 복구를 넘어 장비 교체와 시스템 재구축이 필요한 상황이 발생하였다.

병원은 외부 보안업체와 협력하여 복구 작업을 진행했으나 영상 데이터의 용량이 방대하고 암호화 범위가 넓어 복원은 부분적으로만 가능하였다. 그 결과 환자의 영상 데이터 중 일부는 영구적으로 손실되었으며 이를 대체하기 위해 일부 환자에 대한 검사 재촬영이 진행되었다. 이 사건은 대규모 의료영상 데이터의 특성상 단일 사이버 공격만으로도 병원 전체 진료 기능이 장기간 마비될 수 있음을 보여주는 사례로 평가된다.

나. 사례 2 (2023년) – LOCKBIT, 치료계획 서버 마비

2023년 또 다른 종합병원에서는 LOCKBIT 계열 랜섬웨어 감염이 발생하였다. 공격자는 VPN 장비의 취약점을 통해 내부망에 진입하였으며 이후 권한을 확보해 치료계획 서버와 분석용 PC를 집중적으로 암호화하였다.

피해는 치료계획 서버 8대와 분석용 PC 9대에서 발생하였다. 이들 시스템에는 항암 치료, 장기 질환 관리 등 환자의 개별 치료 계획과 임상시험 관련 데이터가 저장되어 있었으며 병원 의료진은 이를 기반으로 치료 방향을 결정하고 있었다. 그러나 데이터가 암호화되면서 환자 치료 일정이 지연되었고 일부 환자는 타 의료기관으로 전원 조치가 이루어졌다. 특히 항암 치료와 같이 일정의 연속성이 중요한 환자에게는 치료 지연으로 인한 의료적 부담이 크게 증가하였다.

병원은 일부 데이터를 백업 자료를 통해 복구하였으나 최신 자료는 손실된 상태로 남았다. 복구 과정에는 수 주 이상의 기간이 소요되었으며 그 기간 동안 병원은 응급 환자 중심의 제한적인 진료 운영을 해야 했다. 이 사건은 종합병원에서 환자의 생명과 직접적으로 연결된 임상 데이터

역시 주요 공격 대상이 될 수 있음을 보여주며 환자 안전 차원에서 보다 엄격한 사이버 보안 관리 체계가 필요함을 시사한다.

다. 사례 3 (2021년) – Phobos, PACS 및 검사 서버 암호화

2021년 한 종합병원에서는 Phobos 계열 랜섬웨어 공격으로 PACS 서버 4대, 검진 서버 2대, MCC 서버 1대가 암호화되었다. PACS는 방사선 검사와 각종 진단 이미지를 저장하는 핵심 시스템으로 감염 직후 영상 판독과 진단 지원이 불가능해졌다.

응급실과 외래 진료는 수기로 전환되었으나 영상 자료가 없어 정확한 진단을 내리기 어려운 상황이 발생하였다. 수술 일정이 대거 연기되었고 일부 환자는 동일 검사를 타 의료기관에서 재검사 받아야 했다. 이로 인해 환자의 불편이 가중되었으며 의료비와 시간이 추가로 소요되었다.

병원은 외부 보안업체와 함께 복구를 시도하였으나 암호화 범위가 방대하여 전체 복구에는 수 주의 기간이 소요되었다. 복구 이후에도 일부 영상 파일은 손상된 상태로 남아 장기적인 환자 진료 기록 관리에 공백이 발생하였다. 이 사건은 대규모 데이터를 관리하는 종합병원조차 체계적인 사이버 보안 대비가 부족할 경우 환자 치료와 연구 활동에 심각한 차질이 발생할 수 있음을 보여주는 사례이다.

4. 상급종합병원 사례

가. 사례 1 (2025년) – 주차운영망을 통한 8base 랜섬웨어 감염

2025년 국내 한 병원에서는 외부에 개방된 부대사업 운영망을 통해 공격자가 침입하여 8base 계열 랜섬웨어를 실행하는 사건이 발생하였다. 조사에 따르면 피해 시스템은 총 50여 대였으며 이 중 15대(서버 7대, PC 8대)가 직접 채증 대상이 되었다. 일부 서버와 PC에서는 AnyDesk 원격 제어 프로그램 설치 흔적과 RDP 통신 기록, 악성 도구 실행 내역이 확인되었다.

공격자는 방화벽이나 접근 통제가 적용되지 않은 부대사업 운영망을 최초 진입 지점으로 삼았다. 부대사업 운영 DB 서버가 내부망과 부대사업망을 동시에 연결하는 구조로 구성되어 있었던 점이 주요 취약점이 되었으며 공격자는 해당 서버에 AnyDesk를 설치해 안정적인 원격 접속 기반을 확보하였다. 이후 원격 제어 기능을 이용해 랜섬웨어를 다운로드하고 실행하였으며 RDP 서비스가 활성화된 시스템을 대상으로 측면 이동(Lateral Movement)을 시도하여 내부 진료학과 A서버와 PC, 진료 학과 B PC, 부대사업 운영실 서버 등으로 감염을 확산시켰다.

랜섬웨어는 Phobos 계열인 8base로 감염된 파일의 확장자를 “.eightbase”로 변경하면서 접근을 차단하였다. 이로 인해 치료 계획 수립과 환자 데이터 관리가 지연되었고 부대사업 운영 시스템 또한 중단되었다. 복구 과정에서 외부 보안업체가 투입되었으나 암호화 범위가 넓어 상당한 복구 비용과 시간이 소요되었다. 병원은 수천만 원 규모의 재정적 피해를 입었으며 진료 일정 지연과 환자 불만 증가로 장기적인 신뢰도 저하가 우려되는 상황에 직면하였다.

이번 사건은 의료기관의 핵심 진료망이 아닌 부대사업 운영 시스템의 보안 취약성이 병원 전체 운영에 치명적인 영향을 줄 수 있음을 보여주는 대표적인 사례로 평가된다. 특히 부대사업 운영망과 내부 진료망을 동시에 연결한 서버 구조는 공격자에게 이상적인 침투 교두보로 작용하였으며 단순한 관리 소홀과 기초 보안 미비가 대규모 피해로 직결될 수 있음을 보여준다.

나. 사례 2 (2024년) – 웹서버 취약점 통한 진료정보 침해

2024년 국내 한 상급종합병원에서는 외부에 개방된 웹 서버 취약점이 악용되며 진료정보가 침해되는 사건이 발생하였다. 문제의 서버는 방화벽 설정 오류와 보안 패치 미적용 상태로 장기간 운영되고 있었으며 공격자는 이를 통해 내부망에 접근하였다. 초기에는 단순한 외부 침입으로 보였으나 이후 환자 진료정보 일부가 암호화되면서 진료 업무에 직접적인 타격이 발생하였다.

피해는 병원의 핵심 운영에 즉각적으로 반영되었다. 외래 진료에서는 환자의 과거 진료 기록과 검사 이력을 조회할 수 없어 의료진이 수기로 진료 기록을 작성해야 했으며 환자 예약 일정도 대거 연기되었다. 검사와 수술이 취소되거나 지연되면서 환자 불만이 급증하였고 의료진 역시 환자 안전을 충분히 확보하기 어려운 상황에 놓였다. 이는 단순한 IT 장애를 넘어 실제 환자 치료 과정에 직접적인 차질을 초래한 심각한 사건이었다.

재정적 손실 또한 상당하였다. 외래 진료 지연으로 인해 하루 수천만 원 규모의 수익 손실이 발생하였으며 예약 취소와 재예약 과정에서 추가 인력이 투입되면서 운영 비용도 증가하였다. 복구 과정에서는 외부 보안 업체가 긴급 투입되었고 서버 재설치 및 시스템 재구축에만 억 원 단위의

비용이 소요되었다. 단기적인 재정 손실뿐 아니라 언론 보도와 환자 민원으로 인한 평판 하락은 장기적인 환자 감소와 의료기관 신뢰 저하로 이어질 가능성이 크다.

이 사건은 대형 의료기관이라 하더라도 기본적인 보안 관리가 미흡할 경우 환자 안전, 병원 운영, 재정 전반에 심대한 영향을 미칠 수 있음을 보여주는 대표적인 사례라 할 수 있다.

다. 사례 3 (2022년) – 랜섬웨어 감염, 환자정보 유출 의혹

2022년 상급종합병원에서 발생한 사건은 랜섬웨어 감염과 더불어 환자 개인정보 유출 의혹까지 제기되면서 사회적 파장을 일으켰다. 공격자는 병원 내부 서버를 암호화했을 뿐 아니라 일부 데이터를 외부로 전송한 정황까지 확인되었다. 해당 서버에는 환자의 진료 기록, 검사 결과, 수납 내역이 포함되어 있어 단순한 데이터 마비를 넘어 환자 개인정보 침해 우려가 강하게 제기되었다.

직접적인 피해는 심각하였다. 외래 진료와 예약 진료가 전면 중단되었고 응급 환자 치료 역시 수기 방식으로 전환해야 했다. 의료진은 과거 진료 데이터를 확인할 수 없어 정확한 처방과 치료에 큰 제약을 받았으며 환자 안전을 충분히 확보하기 어려운 상황이 이어졌다. 수많은 환자가 불편을 호소하였고 일부 환자는 타 의료기관으로 전원 조치가 이루어졌다.

금전적 손실 규모도 상당하였다. 진료 중단으로 인한 하루 손실만 수억 원에 달했을 것으로 추정되며 외부 복구업체 투입과 디지털 포렌식 조사 의뢰 비용으로 수천만 원이 추가 지출되었다. 무엇보다 개인정보 유출 의혹이 사회적으로 확산되면서 다수의 환자가 병원을 상대로 민원을 제기하였고 언론에서도 사건이 대대적으로 보도되었다. 이는 병원의 신뢰도

와 브랜드 가치에 큰 타격을 주었으며 장기적으로 환자 감소로 이어질 가능성을 남겼다.

이 사건은 상급종합병원과 같은 대형 의료기관이라 하더라도 사이버 공격에 노출될 경우 단순한 IT 시스템 장애를 넘어 환자 안전, 병원 재정, 사회적 신뢰에 동시에 심각한 영향을 미칠 수 있음을 보여주는 중대한 사례이다.

라. 사례 4 (2020년) – 환자망 서비스 거부 공격

2020년 한 상급종합병원에서는 환자용 무선 네트워크를 대상으로 한 대규모 서비스 거부(DoS) 공격이 발생하였다. 공격자는 대량의 트래픽을 환자망에 유입시켜 네트워크를 마비시켰으며 수십 분 동안 환자와 보호자가 온라인 서비스를 이용할 수 없는 상태가 지속되었다.

직접적인 데이터 유출이나 시스템 암호화는 발생하지 않았지만 환자 서비스 이용 환경은 크게 악화되었다. 원무·수납 업무가 지연되면서 대기 시간이 길어졌고 온라인 예약 및 상담 서비스도 중단되었다. 일부 환자는 예약을 취소하거나 재예약해야 했으며 보호자들은 불편을 호소하며 민원을 제기하였다.

이 사건으로 병원은 긴급 인력을 투입해 수기 방식으로 접수를 진행해야 했으며 보안 장비 재설정과 네트워크 복구를 위해 수천만 원 규모의 비용이 투입되었다. 하루 동안 발생한 수익 손실 역시 수천만 원 수준에 달했을 것으로 추산된다. 직접적인 랜섬 지불은 없었지만 서비스 차질로 인한 운영 손실과 환자 민원 대응 비용이 상당한 수준으로 발생하였다.

이 사례는 데이터 암호화가 발생하지 않더라도 서비스 가용성만 차단되어도 병원 운영에 상당한 금전적 피해와 신뢰도 하락을 초래할 수 있음

을 보여주는 사례이다.

5. 피해 양상 종합 분석

국내 의료기관 침해사고는 기관 규모와 IT 성숙도에 따라 양상이 달라지지만 침투 경로의 반복성, 공격자 도구·기법의 전형성, 백업 및 망분리 실패로 인한 피해 확산, 임상 운영 차질과 금전 손실의 동시 발생이라는 공통적인 특징을 분명히 보여준다. 아래 분석은 수집된 사례 전반에서 공통적으로 확인되는 주요 패턴을 정리한 것이다.

가. 초기 침투 경로: 단순하지만 치명적인 “열린 문”

공격자들은 복잡한 제로데이 취약점보다 이미 알려진 취약점과 잘못된 시스템 설정을 지속적으로 악용하는 경향을 보인다. 반복적으로 관찰된 주요 침투 경로는 다음과 같이 정리할 수 있다.

- 원격접속 서비스 노출: RDP(주로 3389, 변조 포트 포함), SSH(22/2222) 등이 외부에 개방되거나 접근제어 없이 운영됨. 포트포워딩·UPnP 자동 개방이 방치된 사례 다수.
- DB 포트 외부 노출: MSSQL(1433), MySQL(3306), Oracle(1521) 등 데이터베이스 포트가 인터넷에 직접 노출되거나 약한 인증으로 운영되어 1차 침투 또는 2차 확산에 악용.
- VPN/방화벽 취약점: 알려진 취약점이 패치되지 않은 VPN·방화벽 장비가 관문으로 활용. 관리 페이지(예: 4433 등) 노출과 접근제어 미흡이 결합 될 때 내부망 접근이 용이.
- 웹서비스 취약점·메일 기반 유입: 의료기관 홈페이지·웹서버의 취약

점(웹셸 업로드 등) 및 악성첨부 메일을 통한 초기 실행이 확인됨.

- 초기 암호·기본 계정 사용, 패치 미적용: 기본 관리자 계정 유지, 장기간 누적된 보안 업데이트 미적용이 침입 난이도를 낮춤.

핵심은 '복잡해서 막기 어려운 공격'이 아니라 '너무 기본이라 간과된 구멍'에서 사건이 시작된다는 점이다.

나. 공격 도구·전술(TTPs): 범용 툴 조합으로 병원 전역 무력화

사례 전반에 등장하는 도구와 절차는 국제적으로 통용되는 범용 툴과 일치한다.

- 원격제어·지속성 확보: AnyDesk 등 합법 원격지원 도구의 악용.
- 권한탈취·자격증명 수집: mimikatz, NirSoft 계열(예: WebBrowser PassView, WirelessKeyView, NetPass 등), NLBrute 등으로 계정·암호를 수집하거나 무차별 대입.
- 방어우회·프로세스 종료: ProcessHacker, PCHunter, Defender 비활성화 도구(dControl/DD.exe), 시스템 잠금 파일 강제 해제(unlocker) 등으로 EDR/AV 무력화.
- 정찰·횡적이동: NS.exe, netscan, IPscan 등으로 네트워크·공유폴더를 탐색 후 SMB/RDP를 통해 내부 확산.
- 부가적 악성행위: 코인 마이너(xmrig) 설치, 로그 삭제 스크립트(LogDelete.bat)로 추적 회피.

특징은 고급 APT 전용 도구가 아니더라도 위와 같은 범용 도구의 단순한 조합만으로 EMR·OCS·PACS, 가상화 기반 서버, NAS까지 단기간에 광범위한 암호화를 발생시킬 수 있다는 점이다.

다. 피해 확산 메커니즘: 백업·가상화·공유 인프라의 역설

피해 규모를 키운 결정적 요인은 백업·가상화·공유 스토리지의 설계/운영 실패다.

- 온라인/동일망 백업의 동시 암호화: 동일 서버 또는 동일 스토리지/동일 권한 체계에 백업을 미러링해두다가 본 데이터와 함께 암호화되는 사례가 반복. 외장 HDD, NAS 등도 같은 영역에 존재해 '함께 잠김'.
- 가상화 환경의 단일 실패점: VM 관리 노드·이미지 저장소가 침해되며, 다수 임상·업무 VM이 연쇄 암호화. 단일 관리 평면에 의존할수록 충격은 기하급수적으로 확대.
- 광범위한 파일공유·공유폴더 스캔: 파일서버·이미지서버·사용자 공유폴더가 네트워크 전체에 개방되어 있거나 접근제어가 느슨해 확산 속도가 빠름.
- 대용량 의료영상의 구조적 취약성: PACS 수십 TB 규모 영상은 백업·복구에 장시간·대비용이 필요. 일부 병원은 실질적으로 부분 복구 외 대안이 없어 재촬영·재검사 비용과 진료 지연이 누적됨.

요약하면, 가용성 확보를 위해 설계된 요소들이 적절한 통제와 분리 없이 결합될 경우 오히려 시스템의 복원력을 약화시킬 수 있다.

라. 임상 운영 영향: 수기 진료 전환과 치료 연속성 붕괴

사건 발생 직후 EMR·OCS·PACS에 대한 접근이 불가능해지면서 임상 현장에 가장 큰 영향을 미친다.

- 외래·응급 진료 지연: 과거 이력·검사 결과 조회가 막혀 수기 기록으

로 전환. 대기시간 증가, 정확성 저하, 환자 불만 급증.
- 수술·검사 일정 대거 연기/취소: 영상 판독 불가, 치료계획 서버 암호화 등으로 전원(타 병원 이송)까지 발생.
- 영상·치료계획 데이터 손실의 장기 파장: 재촬영·재계획으로 환자 부담·임상 성과 저하, 연구·임상시험 지연.
- 의원급은 단일 서버(EMR) 의존으로 즉시 진료 중단 리스크가 높고, 병원/종합병원은 다계층 시스템 동시 타격,
- 상급종합병원은 대외 서비스/네트워크 장애가 전체 운영 신뢰에 미치는 2차 파장이 두드러짐.

마. 금전 손실 구조: 직접 지불보다 더 큰 "보이지 않는 비용"

금전 피해는 직접 지불(가상화폐), 복구·포렌식 비용, 운영상 손실, 평판·규제 비용으로 구성된다.

- 직접 지불: 의원·병원급에서 수백만~수천만 원 규모 지불 사례가 확인됨(재협상·추가요구로 비용 증가한 케이스 포함). 상급종합은 공개적으로 지불을 인정하는 경우가 드물지만, 외부 복구·포렌식 비용은 억 단위로 치솟는 경향.
- 운영상 손실: 외래·수술·검사 중단으로 하루 수천만~수억 원 수준의 매출 공백이 발생할 수 있음. 접수·민원 대응을 위한 인력 초과 투입도 누적 비용을 키움.
- 평판·규제 비용: 환자 이탈에 따른 장기 수익 감소, 보안 신고 지연에 따른 과태료 부과 사례 확인, 향후 법률 리스크(민원/소송) 가능성.
- 백업/인프라 재구축 투자: 피해 후 설비 교체·망분리·로그·모니터링 체계 보강에 추가 자본적 지출이 뒤따름.

결국 직접 지불액보다 운영·평판·재발 방지 투자 비용이 더 크다는 점이 국내 사례에서도 일관되게 관찰된다.

바. 거버넌스·프로세스의 공백: "알았지만 안 했거나, 몰라서 못 했다"

- 사고 인지·보고 체계 미비: 신고 의무를 인지하지 못해 지연 신고·과태료가 발생한 사례가 존재. 초기 통지·의사결정이 늦어 피해 확산.
- 외주·유지보수 계약의 회색지대: 벤더가 취약점을 인지하고도 통지·조치를 누락하거나, 복구 비용·책임 범위에 대한 계약 명확성이 부족해 분쟁이 발생.
- 교육·훈련 부족: 테이블탑/모의훈련이 없는 기관은 초기 격리·의사결정이 지연. 반대로 훈련 경험이 있는 곳은 재난의료 원칙 기반 대응본부 가동 등으로 피해를 상대적으로 축소.
- 사이버 보험의 한계: 개인정보 유출 중심 담보로 복구·운영 손실은 미보장되는 사례 다수. 보장 공백이 재정 리스크로 전이.

핵심은 기술적 문제 이전에 조직적 대응 역량과 계약 및 보장 체계의 공백이 피해를 확대시킨다는 점이다.

사. 규모별 특징: 무엇이 다치고, 어떻게 무너지는가

- 의원: EMR 단일 실패점(SPOF) 의존, DB 포트 노출·포트포워딩, 백업 동시 암호화. 직접 지불 비율 높음.
- 병원: VPN/RDP 취약점 기반 내부 확산, 권한 탈취 후 가상화·NAS 포함 다계층 암호화, 외부 복구 의존 증가.
- 종합병원: PACS 대용량·치료계획·임상결정 데이터가 직접 타격. 복

구 장기화·부분 복구가 현실적 한계.

- 상급종합병원: 외부 서비스·웹서버·환자망 공격이 사회적 신뢰·환자 경험에 즉시 타격. 직접 지불 보다는 운영상 손실·평판 비용이 지배.

아. 최근 흐름: 암호화와 데이터 유출의 결합, 가상화 및 관리 평면 공격, 방어 우회 기법의 상시화

최근 사례에서는 데이터 유출 정황과 이중 갈취(암호화와 데이터 공개 협박)가 결합된 공격 형태가 증가하는 경향이 나타난다. 동시에 VM, 관리 콘솔, 방화벽 관리자 포트 등 관리 평면을 대상으로 한 공격 시도가 늘어나고 있으며, EDR 및 Microsoft Defender와 같은 보안 솔루션을 우회하기 위한 도구의 사용도 점차 일반화되고 있다. 이러한 흐름은 단순한 기술적 방어만으로는 대응이 어려우며, 운영 관리, 권한 관리, 접근 통제 체계 등 조직적 보안 관리 역량이 핵심적인 대응 요소임을 시사한다.

자. 반사실적 관찰: 무엇이 있었다면 달라졌는가

분석적 관점에서 볼 때 다음과 같은 통제 장치가 존재했다면 피해 규모는 상당히 축소되었을 가능성이 높다.

- 외부와 분리된 독립 백업과 정기적인 복구 훈련: 본 서버와 같은 위치에 두는 온라인 백업이 아니라, 물리적으로 분리된 백업을 유지하고 정기적으로 복구 훈련을 진행했다면, 동시에 암호화되는 피해를 막고 실제 상황에서도 더 빠른 정상화를 이끌 수 있었을 것임.
- 원격 접속과 관리자 페이지에 대한 다중 인증과 접근 제한: 단순한 비밀번호가 아니라 휴대폰 인증 같은 추가 인증을 강제하고, 특정 사용자나 특정 네트워크만 접근할 수 있도록 제한했더라면, 원격 접속 포

트를 통한 침투와 관리자 권한 탈취 시도가 크게 줄었을 것임.

- 보안 프로그램 무력화 방지와 최소 권한 운영: 서버나 PC에서 불필요하게 높은 권한을 주지 않고, 보안 프로그램을 임의로 종료할 수 없도록 설정했더라면, 공격자가 보안 체계를 쉽게 무력화하지 못했을 것임.
- 모의훈련과 초기 격리 절차 숙련: 사고 초기에 어떤 시스템을 끊고 어떤 순서로 대응해야 하는지 미리 훈련했다면, 첫 24~72시간 동안의 확산을 효과적으로 차단하고 환자 전원이나 진료 지연을 줄일 수 있었을 것임.

6. 시사점

국내 의료기관 사이버 보안 침해사고의 양상을 종합적으로 살펴보면 몇 가지 중요한 시사점을 확인할 수 있다.

첫째, 기초 보안 관리의 미비가 주요 침투 경로로 작동한다는 점이다. 대부분의 사례에서 공격자는 복잡한 제로데이 취약점이나 맞춤형 악성코드를 활용하기보다 이미 알려진 VPN·RDP 취약점, 패치되지 않은 웹 서버, 외부에 노출된 데이터베이스 포트 등을 통해 시스템에 접근하였다. 즉 침해사고는 첨단 공격 기술보다는 기본적인 보안 수칙이 준수되지 않은 환경에서 주로 발생하는 것으로 나타났다. 이는 기초 보안 통제의 준수 여부가 실제 피해 규모를 좌우하는 중요한 요인임을 의미한다.

둘째, 의료기관의 규모와 정보화 수준에 따라 피해의 성격이 상이하게 나타난다는 점이다. 의원급 의료기관은 단일 EMR 서버에 의존하는 구조적 특성으로 인해 단일 실패점이 곧바로 진료 차질로 이어졌으며 이로 인해 공격자와의 직접 협상이나 금전 지불 사례가 상대적으로 많이 나타났

다. 반면 중규모 병원은 VPN과 RDP를 통한 내부망 침투 이후 다수의 서버, NAS, 가상화 환경이 동시에 암호화되는 피해가 발생하면서 복구 비용과 운영 차질이 크게 증가하였다. 종합병원은 PACS와 치료계획 서버 등 대규모 임상 데이터 자산이 타격을 받아 장기적인 진료 지연으로 이어졌고 상급종합병원은 네트워크 및 웹 서버 침해를 통해 대외적 신뢰와 환자 서비스 경험에 직접적인 타격을 입는 양상이 뚜렷하게 나타났다.

셋째, 백업 관리의 미흡이 피해 확산의 주요 요인으로 작용했다는 점이다. 많은 기관에서 백업 데이터를 동일 서버 또는 동일 네트워크 환경에 저장하는 운영 방식으로 인해 본 데이터와 백업 데이터가 동시에 암호화되는 사례가 반복적으로 발생하였다. 그 결과 백업이 존재함에도 불구하고 실제 복구 과정에서는 활용되지 못하였고, 고비용의 복구업체 의존이나 공격자와의 협상으로 이어지는 경우가 많았다. 이는 백업의 존재 여부보다 백업의 물리적 분리와 정기적인 복구 검증 체계가 더욱 중요함을 보여준다.

넷째, 금전적 손실은 단순한 랜섬 지불 비용을 넘어선다는 점이다. 의원 및 병원급 의료기관에서는 수백만 원에서 수천만 원 수준의 직접 지불 사례가 다수 확인되었으나, 실제로 더 큰 손실은 진료 중단으로 인한 수익 공백과 환자 이탈에서 발생하였다. 상급종합병원의 경우 직접적인 랜섬 지불은 상대적으로 드물지만 하루 수억 원 규모의 운영 손실과 억 원 단위의 복구 비용, 그리고 신뢰도 하락으로 인한 장기적인 재정적 타격이 두드러졌다. 따라서 피해 규모를 단순히 공격자에게 지불한 비용만으로 평가하는 것은 불완전하며 운영 손실, 복구 비용, 평판 손실을 포함한 총체적 비용 관점에서 접근할 필요가 있다.

다섯째, 조직적 대응 역량의 부족이 피해 확대의 중요한 요인으로 작용했다는 점이다. 다수의 의료기관이 사고 인지 및 보고 절차에 익숙하지

않아 초기 대응이 지연되었으며 일부 기관에서는 신고 지연으로 과태료가 부과되기도 하였다. 또한 유지보수 업체와의 계약 구조가 명확하지 않아 취약점을 인지하고도 적시에 통보하지 않거나 복구 비용 분담을 둘러싼 분쟁이 발생한 사례도 확인되었다. 반면 사전에 모의훈련을 수행한 일부 병원은 대응본부를 신속하게 가동하여 피해 규모를 상대적으로 축소할 수 있었다. 이는 단순한 기술적 보안 강화뿐 아니라 보고 체계, 계약 관리, 교육 및 훈련 체계와 같은 조직적 거버넌스 요소가 실제 복원력에 결정적인 영향을 미친다는 점을 보여준다.

결과적으로 국내 사례는 의료기관의 사이버 보안 위협이 단순한 IT 시스템 문제가 아니라 진료 연속성, 환자 안전, 병원 재정, 사회적 신뢰와 직결되는 문제임을 명확히 보여준다. 따라서 국내 의료기관의 보안 개선 논의에서는 첨단 보안 기술의 도입 여부에 앞서 기초 보안 통제 준수, 물리적으로 분리된 백업 관리, 운영 손실을 고려한 복구 전략, 조직적 대응 역량 강화가 핵심적인 정책 과제로 도출된다.

제2절 해외 사례: 미국

HIPAA Journal은 건강보험 양도 및 책임에 관한 법(Health Insurance Portability and Accountability Act, HIPAA)과 관련된 주요 정보 제공 매체로, 교육, 규제 동향, 집행 사례, 데이터 침해 현황, 컴플라이언스 모범 사례 등을 전문적으로 보도한다. 뉴스 보도 외에도 개인정보 보호·보안·침해 통보 규칙 준수를 지원하기 위한 자문 자료, 참고 자료, 교육 프로그램 등을 운영하고 있으며, 10년 이상 6,000편 이상의 기사를 발행해왔다. 모든 콘텐츠는 HIPAA 전문가가 제작 및 검토하며 최신 법령과 지침에 맞추어 지속적으로 업데이트되고, 규제 변화와 침해 사건에 대한 신속하고 심층적인 정보를 제공한다.

2009년 10월 미국 보건복지부(Department of Health and Human Services, HHS) 산하 민권사무국(Office for Civil Rights, OCR)이 자사 웹사이트에 보건의료 데이터 침해 사건 요약을 처음 게시하기 시작한 이후 HIPAA Journal은 관련 통계를 수집하여 보건의료 데이터 침해 통계(Healthcare Data Breach Statistics) 웹 페이지에 게시하고 있다. 해당 페이지는 민권사무국(OCR)의 자료를 기반으로 작성되며 2025년 6월 30일까지의 데이터를 포함하고 있으며 최소 월 단위로 업데이트된다. 최신 보건의료 데이터 침해 현황과 추세는 이 페이지를 통해 확인할 수 있으며 HIPAA에 따른 기관의 의무를 이해할 수 있도록 'HIPAA 준수 체크리스트(HIPAA Compliance Checklist)'도 무료로 제공되고 있다.

2009년 이후 보고된 보건의료 데이터 침해 사건 가운데 가장 큰 규모는 2015년 Anthem Inc.에서 발생한 사건으로 약 7,880만 명의 기록이 유출된 것으로 보고되었다. 당시에는 이와 같은 대규모 침해 사건이 다시 발생할 가능성이 낮을 것으로 여겨졌으나 2024년 Change Healthcare

에 대한 대규모 랜섬웨어 공격으로 해당 기록이 경신되었다. 이 사건에서는 약 1억 9천만 명의 환자의 개인정보가 유출된 것으로 보고되었으며 이는 현재까지 확인된 최대 규모의 보건의료 데이터 침해 사건으로 기록되고 있다.

한편, 미국의 의료정보관리업체인 PJ&A(Practice & Action)에서 발생한 대규모 개인정보 유출 사고의 경우 민권사무국(OCR)에 보고된 침해 피해 규모는 8,952,212명이었으나, 일부 계약 주체(covered entity)[3] 고객이 별도로 보고함에 따라 실제 영향을 받은 인원은 1,300만 명을 초과하는 것으로 추정된다. 이러한 통계는 보고 주체를 기준으로 산출되기 때문에 협력 업체(business associate)에서 침해가 발생한 경우 협력 업체가 직접 보고하거나 영향을 받은 각 HIPAA 적용 기관이 개별적으로 보고할 수 있다.

예를 들어 2022년 전자건강기록(EHR) 공급업체 Eye Care Leaders가 랜섬웨어 공격을 받은 이후 최소 39개 HIPAA 적용 기관이 피해 사실을 별도로 보고하였으며 이로 인해 309만 건 이상의 기록이 유출된 것으로 나타났다. 또한 2019년 American Medical Collection Agency (AMCA) 사건 역시 각 적용 기관이 개별적으로 피해 사실을 보고하면서 피해 규모가 총 2,500만 명 이상으로 집계되었다. 이처럼 협력 업체의 데이터 침해 사건은 일부 계약 주체가 별도로 보고하는 경우가 많기 때문에 실제 피해 규모가 공식 보고 수치보다 과소 집계될 가능성이 존재한다.

3) 미국 HIPAA 법에서 보호해야 하는 건강 정보를 다루는 의료 관련 주체로 모두 HIPAA의 프라이버시·보안 규정을 따라야 할 법적 의무가 있음. 병원, 클리닉, 약국 등 보건의료 제공자(Healthcare Provider), 건강 보험 기관(Health Plan), 의료데이터를 전산 처리하는 정보중개기관(Healthcare Clearinghouse)이 해당됨.

〈표 4-1〉 미국 역대 최대 규모 보건의료 데이터 침해 사건

순위	연도	기관명	주(State)	기관 유형	침해 받은 개인 정보 수	침해 유형
1	2024	Change Healthcare, Inc.	미네소타	협력업체	190,000,000	해킹/IT 사고
2	2015	Anthem Inc.	인디애나	건강보험 기관	78,800,000	해킹/IT 사고
3	2023	Welltok, Inc.	콜로라도	협력업체	14,782,887	해킹/IT 사고
4	2024	Kaiser Foundation Health Plan, Inc.	캘리포니아	건강보험 기관	13,400,000	무단접근/정보노출
5	2019	Optum360, LLC	미네소타	협력업체	11,500,000	해킹/IT 사고
6	2023	HCA Healthcare	테네시	협력업체	11,270,000	해킹/IT 사고
7	2015	Premera Blue Cross	워싱턴	건강보험 기관	11,000,000	해킹/IT 사고
8	2019	Laboratory Corporation of America Holdings (LabCorp)	노스캐롤라이나	보건의료 제공자	10,251,784	해킹/IT 사고
9	2015	Excellus Health Plan, Inc.	뉴욕	건강보험 기관	9,358,891	해킹/IT 사고
10	2023	Perry Johnson & Associates, Inc. (PJ&A)	네바다	협력업체	9,302,588	해킹/IT 사고
11	2023	Maximus, Inc.	버지니아	협력업체	9,179,390	해킹/IT 사고
12	2023	Managed Care of North America	조지아	협력업체	8,627,242	해킹/IT 사고
13	2014	Community Health Systems Professional Services Corporation	테네시	보건의료 제공자	6,121,158	해킹/IT 사고

순위	연도	기관명	주(State)	기관 유형	침해 받은 개인 정보 수	침해 유형
14	2023	PharMerica Corporation	켄터키	보건의료 제공자	5,815,591	해킹/IT 사고
15	2025	Yale New Haven Health System	코네티컷	보건의료 제공자	5,556,702	해킹/IT 사고
16	2024	Ascension Health	미주리	보건의료 제공자	5,466,931	해킹/IT 사고
17	2025	Episource, LLC	캘리 포니아	협력업체	5,418,866	해킹/IT 사고
18	2011	Science Applications International Corporation	버지니아	협력업체	4,900,000	분실
19	2025	Blue Shield of California	캘리 포니아	협력업체	4,700,000	해킹/IT 사고
20	2023	HealthEC LLC	뉴저지	협력업체	4,656,293	해킹/IT 사고
21	2011	University of California, Los Angeles Health	캘리 포니아	보건의료 제공자	4,500,000	해킹/IT 사고
22	2014	Community Health Systems Professional Services Corporation	테네시	협력업체	4,500,000	도난
23	2024	Health Equity, Inc.	유타	협력업체	4,300,000	해킹/IT 사고
24	2023	Reventics, LLC	플로리다	협력업체	4,212,823	해킹/IT 사고
25	2021	20/20 Eye Care Network, Inc	플로리다	협력업체	4,142,440	해킹/IT 사고
26	2022	OneTouch Point, Inc.	위스콘신	협력업체	4,112,892	해킹/IT 사고

순위	연도	기관명	주(State)	기관 유형	침해 받은 개인 정보 수	침해 유형
27	2023	Colorado Department of Health Care Policy & Financing	콜로라도	건강보험 기관	4,091,794	해킹/IT 사고
28	2013	Advocate Health and Hospitals Corporation, (Advocate Medical Group)	일리노이	보건의료 제공자	4,029,530	도난
29	2024	Concentra Health Services, Inc.	텍사스	보건의료 제공자	3,998,163	해킹/IT 사고
30	2016	Banner Health	애리조나	보건의료 제공자	3,620,000	해킹/IT 사고
31	2021	Florida Healthy Kids Corporation	플로리다	건강보험 기관	3,500,000	해킹/IT 사고
32	2015	Medical Informatics Engineering	인디애나	협력업체	3,500,000	해킹/IT 사고
33	2016	Newkirk Products, Inc.	뉴욕	협력업체	3,466,120	해킹/IT 사고
34	2023	Regal Medical Group, Lakeside Medical Organization, ADOC Acquisition, & Greater Covina Medical Group	CA	보건의료 제공자	3,388,856	해킹/IT 사고
35	2020	Trinity Health	미시간	협력업체	3,320,726	해킹/IT 사고
36	2023	CareSource	오하이오	협력업체	3,180,537	무단접근/공개
37	2023	Cerebral, Inc.	델라웨어	협력업체	3,179,835	무단접근/공개
38	2024	Centers for Medicare & Medicaid Services	메릴랜드	건강보험 기관	3,112,815	해킹/IT 사고

순위	연도	기관명	주(State)	기관 유형	침해 받은 개인 정보 수	침해 유형
39	2023	Nations Benefits Holdings, LLC	플로리다	협력업체	3,099,502	해킹/IT 사고
40	2022	Advocate Aurora Health	위스콘신	보건의료 제공자	3,000,000	무단접근/공개
41	2019	Dominion Dental Services, Inc., Dominion National Insurance Company, and Dominion Dental Services USA, Inc.	버지니아	건강보험 기관	2,964,778	해킹/IT 사고
42	2021	Lincare Holdings Inc.	플로리다	보건의료 제공자	2,918,444	해킹/IT 사고
43	2024	Acadian Ambulance Service, Inc.	루이지애나	보건의료 제공자	2,896,985	해킹/IT 사고
44	2022	Connexin Software, Inc.	필라델피아	협력업체	2,846,039	해킹/IT 사고
45	2023	Navvis & Company, LLC	미주리	협력업체	2,824,726	해킹/IT 사고
46	2024	A&A Services (Sav-Rx)	네브라스카	협력업체	2,812,336	해킹/IT 사고
47	2023	ESO Solutions, Inc.	텍사스	협력업체	2,700,000	해킹/IT 사고
48	2023	Harvard Pilgrim Health Care	메사추세츠	건강보험 기관	2,662,337	해킹/IT 사고
49	2018	AccuDoc Solutions, Inc.	노스캐롤라이나	협력업체	2,652,537	해킹/IT 사고

순위	연도	기관명	주(State)	기관 유형	침해 받은 개인 정보 수	침해 유형
50	2021	NEC Networks, LLC (CaptureRx)	텍사스	협력업체	2,600,000	해킹/IT 사고
51	2021	Smile Brands, Inc.	캘리포니아	협력업체	2,592,494	해킹/IT 사고
52	2024	WebTPA Employer Services, LLC (WebTPA)	텍사스	협력업체	2,518,533	해킹/IT 사고
53	2023	Norton Healthcare Inc.	켄터키	보건의료 제공자	2,500,000	해킹/IT 사고
54	2023	Enzo Clinical Labs, Inc.	뉴욕	보건의료 제공자	2,470,000	해킹/IT 사고
55	2023	Florida Health Sciences Center, Inc. (Tampa General Hospital)	플로리다	보건의료 제공자	2,430,920	해킹/IT 사고
56	2021	Forefront Dermatology, S.C.	위스콘신	보건의료 제공자	2,413,553	해킹/IT 사고
57	2024	INTEGRIS Health	오클라호마	보건의료 제공자	2,385,646	해킹/IT 사고
58	2022	Shields Health Care Group, Inc.	메사추세츠	협력업체	2,380,483	해킹/IT 사고
59	2023	Postmeds, Inc.	캘리포니아	보건의료 제공자	2,364,359	해킹/IT 사고
60	2023	Centers for Medicare & Medicaid Services	메릴랜드	건강보험 기관	2,342,357	해킹/IT 사고
61	2024	Medical Management Resource Group, L.L.C.	애리조나	협력업체	2,264,157	해킹/IT 사고

순위	연도	기관명	주(State)	기관 유형	침해 받은 개인 정보 수	침해 유형
62	2016	21st Century Oncology	플로리다	보건의료 제공자	2,213,597	해킹/IT 사고
63	2023	McLaren Health Care	미시간	보건의료 제공자	2,103,881	해킹/IT 사고
64	2023	Berry, Dunn, McNeil & Parker, LLC	메인	협력업체	2,068,426	해킹/IT 사고
65	2014	Xerox State Healthcare, LLC	텍사스	협력업체	2,000,000	무단접근/공개
66	2023	Arietis Health, LLC	플로리다	협력업체	1,975,066	해킹/IT 사고
67	2023	Great Expressions Dental Centers	미시간	보건의료 제공자	1,925,397	해킹/IT 사고
68	2022	Professional Finance Company, Inc.	콜로라도	협력업체	1,918,941	해킹/IT 사고
69	2011	IBM	뉴욕	협력업체	1,900,000	알 수 없음
70	2022	Apria Healthcare LLC	인디애나	보건의료 제공자	1,868,831	해킹/IT 사고
71	2023	Pension Benefit Information, LLC	미네소타	협력업체	1,866,694	해킹/IT 사고
72	2023	Fred Hutchinson Cancer Center	워싱턴	보건의료 제공자	1,840,927	해킹/IT 사고
73	2024	Summit Pathology and Summit Pathology Laboratories, Inc.	콜로라도	보건의료 제공자	1,813,538	해킹/IT 사고
74	2023	Performance Health Technology	오레건	협력업체	1,752,076	해킹/IT 사고

순위	연도	기관명	주(State)	기관 유형	침해 받은 개인 정보 수	침해 유형
75	2023	NASCO	조지아	협력업체	1,744,655	해킹/IT 사고
76	2024	OnePoint Patient Care	애리조나	보건의료 제공자	1,741,152	해킹/IT 사고
77	2019	Clinical Pathology Laboratories, Inc.	텍사스	보건의료 제공자	1,733,836	해킹/IT 사고
78	2020	Dental Care Alliance, LLC	플로리다	협력업체	1,723,375	해킹/IT 사고
79	2011	GRM Information Management Services	뉴저지	협력업체	1,700,000	도난
80	2022	Baptist Medical Center	텍사스	보건의료 제공자	1,608,549	해킹/IT 사고
81	2019	Inmediata Health Group	푸에르토 리코	정보 중개기관	1,565,338	무단접근/공개
82	2021	Eskenazi Health	인디애나	보건의료 제공자	1,515,918	해킹/IT 사고
83	2022	Community Health Network, Inc. as an Affiliated Covered Entity	인디애나	보건의료 제공자	1,500,000	무단접근/공개

출처: https://www.hipaajournal.com/healthcare-data-breach-statistics/ 2025. 7.29. 인출

제3절 해외 사례: 일본

1. 사카구치 카즈키 외(2023). 의료기관에 대한 사이버 공격 사례 연구: 민간 병원 및 의원의 피해 사례로부터 배우다

가. 연구 배경

최근 사이버 공격이 전 세계적으로 증가하면서 그 수법이 점점 더 정교하고 과격해지고 있으며, 일본 역시 이러한 위협에서 예외가 아니다. 특히 2022년 9월부터 11월까지 일본은 사이버 공격의 주요 표적 국가 중 하나로 나타났으며 공격 대상 수 기준으로 세계 2위를 기록하였다. 또한 일본 내에서는 랜섬웨어 감염 피해가 급증하고 있으며 이로 인해 기업 활동의 중단이나 지연 등 사회·경제적 피해가 확대되고 있다.

의료계 역시 이러한 사이버 위협에 직접적으로 노출되어 있다. 일본 경찰청의 보고에 따르면 2022년 의료·복지 분야에서만 20건의 랜섬웨어 피해 신고가 접수되었으며 같은 해 10월 발생한 오사카 급성기·종합의료센터의 랜섬웨어 사건은 일본 사회에서 큰 주목을 받았다. 또한 사이버 공격의 대상이 대형 병원뿐 아니라 의원급 의료기관까지 확대되고 있는 것으로 확인되었다. 특히 2021년 11월 도쿠시마현 쓰루기초 한다병원에서 발생한 랜섬웨어 공격 사건을 계기로 사이버 공격이 단순한 운영 비용 손실을 넘어 환자 건강 피해, 개인정보 유출, 병원의 신뢰도 하락 및 명성 훼손 등 심각한 사회적 문제로 이어질 수 있다는 인식이 확산되었다. 더 나아가 개별 의료기관이 사이버 공격으로 공공의료 기능을 수행하지 못할 경우 이는 개별 기관의 문제를 넘어 지역 의료 체계 전체에 중대한 영향을 미칠 가능성이 있다.

이러한 문제를 해결하는 것은 일본 정부가 추진하고 있는 온라인 자격 확인 시스템과 마이넘버 카드 기반 건강보험증 활용 등 의료 디지털 전환(Digital Transformation, DX)의 도입을 안정적으로 추진하기 위한 중요한 전제 조건이다. 따라서 의료기관이 직면한 사이버 보안 문제를 명확히 규명하고 이에 대한 대응 방안을 마련하는 것이 중요한 정책 과제로 부상하고 있다.

이에 따라 일본의사회종합정책연구기구(日本医師会総合政策研究機構)는 기존 실태 조사를 통해 의료기관의 조직 구조와 리스크 관리 측면에서 나타나는 문제점을 분석해 왔다. 그러나 본 연구에서는 기존 조사에 더해 사이버 공격 피해를 실제로 경험한 의료기관을 대상으로 심층 인터뷰를 실시하여 보다 구체적이고 실증적인 정보를 수집하였다. 특히 사이버 공격 피해와 관련된 공개 자료가 매우 제한적이라는 점을 고려하여 연구진이 독자적으로 데이터를 수집하고 분석을 수행하였다.

나. 연구 요약

사카구치 카즈키 외(2023)는 사례 연구를 통해 2021년 하반기부터 2022년 상반기까지 사이버 공격 피해를 경험한 일본 내 의료기관을 분석하였다. 본 연구는 민간 병원 및 의원을 대상으로 한 세 가지 사례를 심층적으로 검토하여, 의료기관의 사이버 보안 대응 과정에서 나타나는 현행 문제점을 규명하고 향후 개선 과제를 도출하는 것을 목적으로 수행되었다. 연구의 구성은 다음과 같다.

- 제1장: 배경과 목적
- 제2장: 대상과 방법
- 제3장: 사례 개요

- 제4장: 현재의 문제점과 향후 개선 방향
- 제5장: 고찰 및 정책 제언

사카구치 카즈키 외(2023)는 일본 의료기관의 사이버 공격 대응 과정에서 나타난 5가지 주요 문제점을 다음과 같이 제시하였다.

첫째, 사이버 공격 피해 복구에는 막대한 비용과 인적·물적 자원이 소요되며, 이는 수천만 엔 규모의 재정적 부담을 초래한다.

둘째, 의료기관의 정보시스템 관리 인력이 부족하여, 사이버 보안 위협 대응 역량이 미흡하다.

셋째, 행정 당국이 사전에 경고한 기존 보안 취약점이 사이버 공격의 주요 침입 경로로 악용되는 사례가 확인되었다.

넷째, 정보시스템 및 네트워크 장비의 판매·유지보수 업체와 사이버 공격 발생 시 복구 작업 및 비용 부담과 관련된 명확한 계약 체계가 마련되지 않은 실정이다.

다섯째, 사이버 공격 피해를 입은 의료기관에 대한 행정 기관의 지원 및 협력 체계가 미흡하여, 효과적인 대응이 어려운 상황이다.

이와 함께 연구에서는 향후 개선을 위한 3가지 주요 대응 방안을 제안하였다.

첫째, 사이버 공격 발생에 대비한 업무 연속성 계획(Business Continuity Plan, BCP) 수립이 필수적이며, 위기 상황에서 효과적으로 활용될 수 있도록 사전 대비가 필요하다.

둘째, 지역의료 연계 시스템에 업로드된 진료 정보를 사이버 공격 발생 시 백업 데이터로 활용할 수 있도록 관리 체계를 구축해야 한다.

셋째, 사이버 공격은 모든 의료기관이 표적이 될 수 있는 잠재적 위험 요소임을 인식하고, 경영진 및 의료 종사자의 보안 의식을 제고하는 것이

중요하다.

또한, 연구진은 인터뷰를 통해 수집한 정보를 바탕으로, 정부 및 공공기관, 관련 단체가 의료기관을 대상으로 제공해야 할 지원 및 정보 제공 방안을 구체적으로 정리하였다. 이를 토대로, 연구에서는 다음과 같은 4가지 정책적 제언을 제시하였다.

첫째, 행정 기관 간 협력을 강화하고, 사이버 공격 피해 의료기관에 대한 지원을 위해 전문 기관과의 연계 체계를 구축할 필요가 있다.

둘째, 행정 기관이 발표하는 시스템 보안 취약점 관련 정보를 의료 현장에 신속하고 효과적으로 전달할 수 있도록 정보 공유 체계를 재검토할 필요가 있다.

셋째, 업무 연속성 계획(BCP) 수립, 테이블탑 훈련(Tabletop Exercis), 보안 점검 체크리스트 정비 등 의료기관의 사이버 보안 대응 역량을 강화할 수 있도록 지원해야 한다.

넷째, 의료기관이 사이버 보안 대책을 강화할 수 있도록, 보안 인력 확충 및 예산 확보를 위한 재정적·행정적 지원이 필요하다.

따라서 본 연구는 사이버 위협이 증가하는 의료 환경에서 의료기관의 실질적인 대응 역량을 강화하고 행정적 지원 체계를 개선하기 위한 중요한 정책적 시사점을 제공한다.

다. 사례 조사 대상 및 조사 방법

본 연구의 조사 대상은 사이버 공격 피해를 경험한 일본의 의료기관 3개소(병원 2개소, 의원 1개소)이다. 연구 대상 기관은 사전 문헌 조사를 수행한 후 일본의사회종합정책연구기구의 네트워크를 통해 선정하고 협조를 요청하였다. 조사 내용의 민감성과 기밀성을 고려하여 인터뷰 과정

에서 수집된 정보는 정책 제언 및 학술 연구 목적에 한하여 활용하기로 하였다. 또한 보고서 작성 및 공개 과정에서는 개인 및 기관이 특정되지 않도록 익명성을 보장하는 조건을 설정하였다.

본 연구에서는 반구조화 인터뷰(semi-structured interview) 기법을 적용하였다. 조사 대상자에게 사전에 연구 목적과 인터뷰 가이드를 제공하였으며 핵심 항목을 제시한 개요형 가이드와 구어체 질의응답 형식의 가이드를 병행하여 상황에 따라 활용하였다. 인터뷰의 주요 조사 항목은 다음과 같다. 조사의 주요 항목은 다음과 같다.

- 사이버 공격을 받은 후 복구에 이르기까지의 과정
- 공격 대응 및 시스템 복구를 담당한 인력 체계
- 외부 업체, 공공기관, 전문가 등으로부터 받은 조언 및 지원
- 의료정보 시스템 및 기타 물리적 피해 상황
- 사이버 공격의 시스템 침입 경로 및 그 특정 과정
- 시스템 복구에 소요된 비용과 시간
- 공격을 대비한 사전 준비 상태
  (관리 체계, 보험, 교육·훈련, BCP)
- 정부 및 공공기관, 관련 단체에서 제공해야 할 지원 및
  정보 제공 방안

조사 기간은 2022년 9월부터 2022년 12월까지이다. 신종 코로나바이러스 감염증 확산 상황과 인터뷰 내용의 민감성 및 기밀성을 고려하여 인터뷰 장소는 대상자의 요청에 따라 결정하였다. 그 결과 1건은 온라인 방식으로, 2건은 현장 인터뷰 방식으로 진행되었다.

청취한 내용의 정확성과 객관성을 보장하기 위해, 모든 인터뷰는 2명

또는 3명의 인터뷰어가 참여하는 체제로 진행되었다. 또한, 인터뷰 후에는 매번 기록 메모를 작성한 후, 인터뷰에 참여한 여러 명이 이를 검토하여 내용의 신뢰성을 확인하였다. 아울러, 대상자의 요청이 있을 경우, 확인을 위해 사후에 기록 메모를 제공하였다.

라. A(병원) 사례

A 사례는 2022년 상반기에 발생하였으며 공격을 받은 기관은 지방 중핵 도시(지방 경제와 행정을 담당하는 중심 도시)에 위치한 의료법인 소속의 중소 규모 병원(99병상 미만)이다. 공격 유형은 랜섬웨어(Cring)로, 전자차트시스템(EMR) 서버 내 데이터가 동일 서버에 보관된 백업 데이터와 함께 암호화되었다. 디지털 포렌식 조사 결과, VPN 장비(기업이나 기관에서 외부 사용자가 내부 네트워크에 안전하게 접속할 수 있도록 암호화된 연결을 제공하는 보안 장치)의 보안 취약점이 악용되어 공격이 이루어진 것으로 추정되었다. 특히, 해당 취약점은 정부에서 이미 사전 경고한 기존의 보안 취약점이었다.

A 사례에서 직접 대응한 인력은 시스템 책임자 1인에 불과하였다. 내부적으로는 IT 지식이 있는 방사선사 1인이 업무를 지원하였으며, 외부에서는 전자차트 및 네트워크 장비 벤더에서 여러 명이 지원을 위해 파견되었다. 또한, 개인정보 유출 대응을 위해 변호사를 신규 고용하였으며, 보험사에서 추천한 업체를 통해 디지털 포렌식 조사를 외주로 진행하였다. 추가적으로, 후생노동성 의정국에 연락하고, IPA(정보처리추진기구, 경제산업성 산하 IT 보안 및 기술 진흥 기관)에 자문을 요청하였으며, 도·도·부·현 경찰청 사이버 범죄 창구에 신고하였다.

본 사건에서는 공격 발생 2주 전, 다른 시스템 업데이트 과정에서 외부

백업 파일이 생성되었으며, 이를 활용하여 데이터를 복구할 수 있었다. 또한, 병원에서 일부 종이 차트를 병행하여(약 처방 및 검사 오더 기록) 운영하고 있었던 점이 복구 과정에서 유용하게 작용하였다. 그러나, 이러한 우연한 요소들이 작용했음에도 불구하고, 시스템 복구에는 막대한 비용과 노동력이 소요되었으며, 보험 보상으로는 복구 비용을 전액 충당할 수 없었다.

〈표 4-2〉 A(병원)의 피해 사례 개요

피해 발생 시기	2022년 상반기	발생 시간대	이른 아침
설립 주체	☐ 국공립·공공 ☐ 사회보험 관계 단체 ☐ 기타 법인 ☑ 의료법인 ☐ 개인		
병상 규모	☐ 병원 500병상 이상 ☐ 병원 200~499병상 ☐ 병원 100~199병상 ☑ 병원 99병상 미만 ☐ 병상이 있는 의원 ☐ 병상이 없는 의원		
소재지	지방 중핵 도시	공격 유형	랜섬웨어 (Cring)
침입 경로	VPN 장비 (Fortinet사의 FortiGate)		
피해 시스템	전자차트(EMR) 시스템 (서버): 데이터 백업은 진행했지만, 동일한 서버에 미러링 작업을 수행한 탓에 백업 데이터까지 암호화됨.		
간접 피해 시스템	피해 시스템과 연결된 모든 단말기뿐만 아니라, 동일한 서버에 있던 의료정보 시스템과 공유 스토리지(각 부서의 업무 파일 보관 공간)도 동시에 암호화됨		
복구 소요 시간	진료 가능 상태까지 1일, 시스템 재구축 및 데이터 복구까지 2주 소요		
복구 비용	약 5,000만 엔 ① 데이터 복구 및 신규 시스템 구입 비용: 2500만엔 ② 외주 업체 비용 및 병원 내부 인건비: 400~500만엔 ③ 개인정보 유출 대책 비용: 2,000만엔 (사과문 발송 및 콜센터, 변호사 비용)		
대응 인력 (내부)	시스템 책임자 1인(시스템에 익숙한 방사선사 1인 지원)		
대응 인력 (외부)	전자차트(EMR) 시스템 벤더: 3인 VPN 장비 벤더: 1인		
기타 외부 지원자	고문 변호사가 소개한 변호사: 개인정보 유출 대책을 지원 디지털 포렌식 업체: 보험사 추천으로 외주 진행 민간 보험회사: 개인정보 유출 보험 및 포렌식 업체 소개		
행정기관 연락 상담	후생노동성 의정국 신고 IPA(정보처리진흥기구)에 상담 요청 도·도·부·현 경찰청 사이버 범죄 창구신고 및 상담		

사이버 보험 가입 여부	가입됨. 단, 개인정보 유출 피해만 보상하는 보험이었음 개인정보 유출 대응 비용(2,000만 엔)은 보상받았으나, 나머지 3,000만 엔은 병원 자체 부담
임직원 대상 교육훈련	없음. 지진 등 자연재해로 인한 ICT 시스템 마비 대비 교육훈련의 필요성이 논의되었으나, 실제로 시행되지 않음
비상 시 행동 계획(BCP) 보유 여부	있음. 단, 자연재해를 중심으로 한 BCP로 작성되었으며, 향후 사이버 공격 대응 절차를 포함할 예정
기타 특이 사항	공격 2주 전, 병원의 다른 시스템 업데이트 과정에서 전자차트(EMR) 회사가 외부 백업을 생성한 것이 남아 있어 데이터 복구에 활용됨. 일부 종이 차트(약 처방·검사 오더 기록)를 병행 운영한 점도 복구 과정에 큰 도움이 되었음.

출처: 사카구치 카즈키, 츠츠미 노부유키, 하라 유이치. (2023. 4. 11.). 의료 기관에 대한 사이버 공격 사례 연구: 민간 병원·의원의 피해 사례에서 배우다. 일본의사회종합정책연구기구 리서치 리포트 No.136. p.7

마. B(병원) 사례

B 사례는 2022년 상반기에 발생하였다. 공격을 받은 기관은 대도시권 근교에 위치한 의료법인 소속의 중소 규모 병원(100~199병상)이었다. 공격 유형은 랜섬웨어(LockBit 2.0)로, 전자차트(EMR) 시스템 서버 내 데이터가 암호화되었다. 또한, 전자차트(EMR)와 연동된 오더링 시스템 및 의료 회계 시스템도 사용할 수 없게 되었으며, 복구까지 약 2개월 동안 종이 차트와 대체용 레세콘(의료 회계 시스템)으로 운영할 수밖에 없었다. 도·도·부·현 경찰청(이하 경찰)의 조사 결과, 침입 경로는 VPN 장비의 보안 취약점일 가능성이 높다는 결론이 나왔다. 이 취약점 역시 정부에서 이미 사전 경고한 기존의 보안 취약점이었다.

피해 병원에는 전담 IT 담당자가 없었으며, 대응은 사무장이 주도하여 구성한 대응 본부가 수행하였다. 외부에서는 전자차트(EMR) 벤더에서 파견된 지원 인력이 복구를 지원하였으며, 경찰에 피해 신고를 하고 개인정보 유출 대응을 위해 변호사와 상담을 진행하였다. 경찰로부터는 적극

적인 협력을 받을 수 있었으나, 후생노동성 및 IPA에서는 구체적인 조언이나 지원을 받지 못하였다.

본 사례에서 주목할 점은, 전담 시스템 담당자가 없었음에도 불구하고 시스템 장애를 대비한 모의 훈련(테이블탑 훈련)을 사전에 수행하였으며, 재난 의료 원칙에 따라 대응본부를 즉시 가동하고 체계적으로 복구 작업을 진행했다는 점이다. 또한, 시간과 비용 문제로 포렌식 조사는 진행하지 않기로 결정하였지만, 경찰의 협조를 받아 침입 경로를 특정하고, 다크웹 조사를 통해 개인정보 유출이 없음을 확인하였다.

복구 과정에서는 지역 의료 연계 시스템의 클라우드 데이터를 적극적으로 활용하며, 수기 기록과 대체 레세콘(의료 회계 시스템, 의료청구 프로그램)을 병행하여 2개월간 운영했다. 그러나, 이러한 대응에도 불구하고 데이터 복구 비용만 약 5,000만 엔이 소요되었으며, 기타 비용을 포함하면 총 7,000만 엔 이상의 비용과 노동력이 필요하였다. 시간적 제약으로 인해 데이터 복구 비용의 세부 내역을 충분히 검토할 수 없었으며, 비용의 투명성이 다소 부족한 문제가 남아 있었다.

〈표 4-3〉 B(병원)의 피해 사례 개요

피해 발생 시기	2022년 상반기	발생 시간대	심야 ~ 이른 아침
설립 주체	☐ 국공립·공공 ☐ 사회보험 관계 단체 ☐ 기타 법인 ☑ 의료법인 ☐ 개인		
병상 규모	☐ 병원 500병상 이상 ☐ 병원 200~499병상 ☑ 병원 100~199병상 ☐ 병원 99병상 미만 ☐ 병상이 있는 의원 ☐ 병상이 없는 의원		
소재지	대도시권 근교	공격 유형	랜섬웨어 (LockBit 2.0)
침입 경로	VPN 장비 (Fortinet사의 FortiGate)		
피해 시스템	전자차트(EMR) 시스템 (서버) 서버의 관리 화면에 LockBit 2.0이 표시되어 즉시 사이버 공격임을 인지		
간접 피해 시스템	피해 시스템과 연결된 모든 단말기 및 의료 정보 시스템 오더링 시스템(검사 및 처방) 및 레세콘도 사용 불가 종이 차트 운영 및 대체 레세콘 활용하여 대응		

복구 소요 시간	당일 새벽, 진료 가능하다고 판단하여 진료는 중단하지 않음. 시스템 재구축 및 데이터 복구까지 2개월 소요 복구 전까지 종이 차트로 운영
복구 비용	약 7,000만 엔 이상 ① 다크웹 조사 비용: 수백만 엔 ② 서버 데이터 복구 비용: 약 5,000만 엔 (기본 요금 3,800만 엔 + 성공 보수 1,000만 엔) ③ 초과 근무 수당 및 기타 비용: 약 2,000만 엔
대응 인력 (내부)	사무장 및 대책본부 구성원(이사장, 병원장, 각 부서장)
대응 인력 (외부)	전자차트(EMR) 벤더에서 지원 인력 파견
기타 외부 지원자	경찰의 전면적 협력 및 지원이 있었음. 후생노동성은 보고를 요청했으나 실질적 조언이나 지원은 없었음. IPA에서도 구체적인 조언 없었음. 개인정보 유출 및 피해 신고 관련 변호사 상담 진행
행정기관 연락 상담	후생노동성 의정국에 연락하여 IPA에 상담 도·도·부·현 경찰의 사이버 범죄 창구에 피해 신고를 제출하여 상담
사이버 보험 가입 여부	가입되어 있었으나 보상 한도가 1,000만 엔으로 제한되어 나머지는 자체 부담
임직원 대상 교육훈련	있음. 시스템 장애를 대비한 대응 매뉴얼을 정비하고, 평소 모의 훈련을 실시하였고 사건 발생 2개월 전에 해당 훈련을 진행한 바 있음.
비상 시 행동 계획(BCP) 보유 여부	있음. 재난 의료의 기본 원칙 CSCATTT(스캐트)를 기반으로 한 대응 매뉴얼 보유함. 대응본부 구성원도 사전에 지정되어 있었음.
기타 특이 사항	지역 의료 연계를 위해 각종 진료 데이터를 클라우드에 업로드하고 있었으며, 복구 전까지 해당 데이터를 활용하였음. 포렌식 조사는 시간과 비용 문제로 진행하지 않았음. 원칙적으로 모든 단말기를 감염된 것으로 간주하고 데이터 복구에 전념 전담 시스템 담당자가 없는 병원이었으나, 사무장을 중심으로 대책 본부가 경찰 및 외부 업체의 지원을 활용하여 대응한 사례임.

출처: 사카구치 카즈키, 츠츠미 노부유키, 하라 유이치. (2023. 4. 11.). 의료 기관에 대한 사이버 공격 사례 연구: 민간 병원·의원의 피해 사례에서 배우다. 일본의사회종합정책연구기구 리서치 리포트 No.136. p.9

바. C(의원) 사례

C 사례는 2021년 하반기에 발생하였다. 공격을 받은 기관은 대도시권에 위치한 개인운영하는 병산이 없는 의원이었다. 공격 유형은 랜섬웨어

(Cring)로 전자차트(EMR) 시스템 서버 내의 진료 데이터가 암호화되었다. 또한, 전자차트(EMR)와 연결된 각종 의료 정보 시스템이 사용 불가능해졌으며, 동일 서버에 저장되어 있던 인사·회계 등의 핵심 업무 시스템 데이터도 접근 불가한 상태가 되었다.

포렌식 조사 결과, 침입 경로는 VPN 장비의 취약점으로 추정되었다. A와 B 사례와 동일하게, 해당 취약점은 정부에서 사전 경고한 보안 취약점이었다. 그러나, 시스템 유지보수 업체는 해당 취약점을 인지하고 있었음에도 대응하지 않았을 뿐만 아니라, 고객(의원 측)에게도 이를 알리지 않았다는 점이 사후적으로 문제가 되었다. 또한, 복구 비용 부담 문제로 유지보수 업체와 의원 간 갈등이 발생하였다.

본 사례에서 직접 대응은 총무 시스템 담당자 1명이 하였으며 외부에서는 의원 내 시스템의 보수 관리 위탁 업체가 지원했다. 후생노동성 의정국에 연락하고 경찰에도 신고했지만 특별한 조언이나 지원은 얻을 수 없었다. 1인 체제의 복구 작업으로 바쁜 가운데 후생노동성에서는 잦은 보고만을 요구하며 스트레스가 많은 상황이 있었다고 한다. 암호화된 데이터는 보수 위탁업체의 기술자에 의해 90% 정도 복원할 수 있었다. 완전한 복구라고 할 수 없으며, 공격을 당한 지 1년 반이 지난 지금도 과거 데이터를 조회하기 위해 별도의 시스템을 운영하고 있어, 이중으로 시간과 비용이 소요되는 상황이다.

본 사건에서는 사전 경고가 있었던 VPN 장비의 취약성에 대해 유지보수 위탁 업체가 알고 있었음에도 불구하고 대응하지 않았을 뿐만 아니라, 고객에게도 알리지 않아 사후적으로 문제가 되었다. 게다가, 후생노동성의 대응도 문제가 있었다. 행정 당국은 보고를 요구하여 정보를 얻는 데에만 집중했을 뿐 현장에는 큰 부담이 가중되었다. 피해 현장을 고려하여 조언이나 지원을 제공하거나, 복구를 지원할 전문 기관을 안내하는 등의 대응은 이루어지지 않았다.

〈표 4-4〉 C(의원)의 피해 사례 개요

피해 발생 시기	2021년 하반기	발생 시간대	심야
설립 주체	☐ 국공립·공공 ☐ 사회보험 관계 단체 ☐ 기타 법인 ☐ 의료법인 ☑ 개인		
병상 규모	☐ 병원 500병상 이상 ☐ 병원 200~499병상 ☐ 병원 100~199병상 ☐ 병원 99병상 미만 ☐ 병상이 있는 의원 ☑ 병상이 없는 의원		
소재지	대도시권	공격 유형	랜섬웨어(Cring)
침입 경로	VPN 장비 (Fortinet사의 FortiGate)		
피해 시스템	전자차트(EMR) 시스템 (서버) 시스템 유지보수 업체로부터 전자차트 시스템이 사용 불가능하다는 연락을 받고 공격 사실을 인지		
간접 피해 시스템	피해 시스템과 연결된 모든 단말기 및 의료 정보 시스템 레세콘, 오더링 시스템(검사 및 처방), 온라인 시스템, 의료영상관리시스템, 진료 예약 시스템, 동일 서버 내 인사·회계 핵심 업무 시스템도 사용 불가		
복구 소요 시간	진료는 중단하지 않았음. 전날까지의 데이터를 조회할 수 없어 불완전한 상태에서 진료를 지속함. 데이터 복구는 여전히 진행 중임.(과거 데이터 조회를 위해 별도 시스템을 유지 중이며, 이로 인해 이중 작업 및 추가 비용 발생)		
복구 비용	수천만 엔 규모 (구체적 금액 확인 불가) ① 포렌식 조사 비용 ② 시스템 재구축 비용 (서버, 단말기, 네트워크 장비 및 소프트웨어 재설정) ③ 암호화된 데이터 복구 비용(유지보수 업체 기술자가 복구 진행) ④ 전자차트 시스템과 연동된 모든 시스템의 전체 스캔 및 재설정을 위한 비용. 그 외 직원들의 초과 근무 비용 및 정신적 부담은 측정 불가		
대응 인력 (내부)	총무·시스템 담당자 1인이 단독으로 복구 작업 수행		
대응 인력 (외부)	의원의 시스템 유지보수 업체에서 복구 지원		
기타 외부 지원자	변호사와 상담: 유지보수 업체와의 복구 비용 부담 문제 논의 후생노동성: 구체적 조언이나 지원 없이 보고만 요구 경찰: 범인이 특정되지 않는 한 대응할 수 없다는 입장		
행정기관 연락 상담	후생노동성 의료정책국에 연락 경찰 사이버 범죄 창구에 신고		
사이버 보험 가입 여부	미가입. 앞으로도 가입할 계획 없음.		

임직원 대상 교육훈련	없음. 현재는 유지보수 업체와 협력하여 표적형 이메일 훈련 및 e-러닝 교육 진행 중임.
비상 시 행동 계획(BCP) 보유 여부	있음. 그러나 지진 대비 BCP였으며, 사이버 공격 대응에는 도움이 되지 않았음,
기타 특이 사항	유지보수 업체가 VPN 장비의 취약점을 사전에 인지하고 있었음에도 조치를 취하지 않았으며, 고객(의원)에게도 알리지 않았음. 결국 해당 취약점을 악용한 공격이 발생하였음. 복구 비용 부담 문제로 유지보수 업체와 갈등 발생 후생노동성과 경찰 모두 실질적 지원 없이 보고만 요구하여 행정적 부담으로 인해 피해 기관에 추가적인 스트레스와 부담 가중되었음.

출처: 사카구치 카즈키, 츠츠미 노부유키, 하라 유이치. (2023. 4. 11.). 의료 기관에 대한 사이버 공격 사례 연구: 민간 병원·의원의 피해 사례에서 배우다. 일본의사회종합정책연구기구 리서치 리포트 No.136. p.11

본 연구에서는 분석한 세 가지 피해 사례를 정리하고, 각 사례의 개요를 표로 정리한 후, 피해 발생부터 복구에 이르는 과정, 사이버 공격의 침입 경로, 기타 사례별 특징을 상세히 설명하였다. 사례 분석을 통해 도출된 현재 의료 현장에서의 주요 문제점과 향후 개선을 위한 시사점을 핵심 논점별로 정리하였으며 이를 바탕으로 정부 및 행정기관을 위한 정책적 시사점을 제언하였다.

사. 인터뷰 질문[4)]

1. 사이버 공격을 받고 복구에 이르기까지의 경위에 대해 가급적 자세하게 말씀해 주세요.
2. 사이버 공격에 대한 대응, 시스템의 복구에 해당한 인원 체제에 대해 말씀해 주세요.

4) 사카구치 카즈키, 츠츠미 노부유키, 하라 유이치. (2023. 4. 11.). 의료 기관에 대한 사이버 공격 사례 연구: 민간 병원·의원의 피해 사례에서 배우다. 일본의사회종합정책연구기구 리서치리포트 No.136. pp. 28-30

3. 사이버 공격에 대응, 시스템의 복구에 있어서, 어떤 외부의 업자나 공적기관, 전문가등에 상담했습니까? 각각 어떤 조언이나 지원이 있었습니까?
4. 사이버 공격의 피해를 입은 귀원의 정보 시스템에 대해 말씀해 주세요.
5. 사이버 공격의 시스템에 대한 침입 경로, 특정 침입 경로에 이른 경위에 대해 말씀해 주세요.
6. 원내의 정보 시스템이나 단말, USB 메모리 등의 외부 매체의 관리 지침의 정비 상황에 대해 말씀해 주세요.
7. 시스템 복구에 필요한 직접적, 간접적 비용과 시간에 대해 구체적으로 말씀해 주세요.
8. 사이버 공격으로 인한 피해를 보상하는 보험에 가입했습니까? 가입한 경우 보험에 따라 실제 피해·손실의 어느 정도를 충당할 수 있었습니까?
9. 사이버 공격을 가정한 임직원을 위한 교육·훈련의 실시 상황에 대해 말씀해 주세요. 그 교육·훈련은 실제 상황에서 어떻게 도움이 되었습니까?
10. 사이버공격을 가정한 대응 절차나 비상 시의 행동 계획 등의 보유 상황에 대해 말씀해주세요.
11. 의료기관의 사이버 보안 확보에 있어서 다음과 같은 관공청, 공적기관·단체로부터 의료현장에 대해 어떠한 지원이나 지원, 정보제공이 있어야 한다고생각하십니까?

(1) 후생 노동성

(2) 경찰

(3) 총무성, 경제산업성, 디지털청 등, ICT 및 디지털 기술에 관한 부처

(4) 의료 정보 시스템 및 의료 기기의 업계 단체
(5) 의사회나 병원 단체
(6) 기타

제4절 해외 사례: 유럽

2022년 11월 공식 출범한 EuRepoC(European Repository of Cyber Incidents)는 유럽연합(EU)과 전 세계에서 발생하는 사이버 공격 사건을 체계적으로 수집·분류·분석하는 독립 연구 컨소시엄이다. 이 저장소는 정치·법률·기술의 3가지 관점에서 사건을 다층적으로 정리하며, 연구자와 정책결정자, 시민사회, 언론인 등 다양한 이해관계자가 신뢰성 있는 최신 데이터를 열람하고 다운로드할 수 있도록 공개 데이터베이스 형태로 운영되고 있다.

EuRepoC는 60개 이상의 분류 체계를 기반으로 사건을 정치적·기술적·법적 기준에 따라 코드화한다. 매일 전 세계 220개 이상의 출처와 600여 개의 트위터 계정에서 수집한 정보를 데이터베이스에 반영하고 있으며, 이를 통해 유럽 내 사이버 위협 동향 분석과 관련 정책 연구의 핵심 자료를 제공한다. 이 데이터는 교육, 학술 연구, 정책 토론 등 다양한 분야에서 폭넓게 활용되고 있다.

특히 EuRepoC 데이터베이스에는 의료 분야를 포함한 다양한 보건의료 사이버 보안 사건이 다수 기록되어 있다. 본 절에서는 EuRepoC 데이터베이스를 비롯하여 보도자료와 뉴스 기사 등을 참고해 유럽 일부 국가에서 보고된 주요 사이버 보안 사고 사례를 정리하였다.

1. 영국: 시노비스(Synnovis) 랜섬웨어 침해 사건 (NHS England, 2025)

2024년 6월 3일 남동부 런던 지역의 여러 NHS(National Health Service) 기관을 대신하여 혈액 검사 서비스를 제공하는 병리학 실험실

Synnovis가 사이버 공격을 받았다. 이후 6월 20일 사이버 범죄 조직 Qilin은 공격 중단의 대가로 약 5천만 달러의 몸값을 요구하였으며 Synnovis 소유라고 주장하는 약 400GB 규모의 데이터를 다크웹에 게시하였다. 이 사건을 통해 민감 정보가 외부로 유출된 사실이 확인되었다.

사건 발생 직후 영국 NHS는 '중대 사고(Critical Incident)'를 선포하고 인근 병원과 검사실로 검체를 우회 처리하는 비상 조치를 시행하였다. Synnovis의 초기 분석 결과 공격자가 공개한 데이터 일부는 자사 시스템에서 유출된 것으로 확인되었으며 일부 파일에는 환자의 이름, NHS 번호, 검사 코드 등 개인 식별이 가능한 정보가 포함되었을 가능성이 있는 것으로 나타났다. 검사 코드는 환자에게 요청된 검사 종류를 식별하는 데 활용될 수 있다. 다만 현재까지 환자의 검사 요청 및 결과가 저장된 실험실 정보관리 시스템(Laboratory Information Management System, LIMS)의 전체 데이터베이스가 유출되었다는 증거는 확인되지 않았으며 조사는 계속 진행 중이다.

이 사건은 네트워크 기반 운영에 의존하는 의료 시스템이 사이버 공격으로 인해 심각한 장애를 겪을 수 있음을 보여주는 사례이다. 해당 공격으로 인해 NHS는 혈액 검사 수행에 필수적인 핵심 시스템을 사용할 수 없게 되었으며, 그 결과 3,000건이 넘는 진료가 연기되거나 취소되었다. 여기에는 1,000건 이상의 선택적 시술과 2,000건 이상의 외래 진료가 포함되었다. 이러한 대규모 일정 변경은 병원 운영 전반에 상당한 혼란을 초래하였으며 일부 환자의 경우 생명에 위협이 될 수 있는 상황이 발생하였다.

국가범죄수사국(National Crime Agency, NCA)과 국가사이버보안센터(National Cyber Security Centre, NCSC)는 유출된 데이터의 진위와 범위를 확인하기 위해 Synnovis와 협력하여 조사를 진행하고 있다.

현재 대부분의 임상 서비스는 복구되어 정상적으로 운영되고 있으며 일부 행정 업무만 제한적으로 남아 있어 환자 진료에 미치는 영향은 크지 않은 것으로 보고되고 있다.

NHS England와 Synnovis는 랜섬웨어 공격에 대응하기 위해 공동으로 대응 조치를 수행하고 있으며 공개된 데이터의 규모와 성격, 그리고 영향을 받은 환자를 식별하기 위한 추가 분석을 진행하고 있다. 이러한 분석 과정은 복잡하고 시간이 오래 소요될 수 있어 최종적으로 피해자를 확정하기까지 수개월이 걸릴 가능성이 있다.

해당 사건은 이미 사법당국과 영국 정보위원회(Information Commissioner's Office, ICO)에 보고되었으며 국가사이버보안센터(NCSC)와의 협력도 진행되고 있다. Synnovis는 추가 조사 결과가 확인되는 대로 공식 업데이트를 제공할 예정이며 NHS 또한 조사 진행 상황에 따라 관련 정보를 지속적으로 공개하고 있다. 아울러 영향을 받은 환자를 지원하기 위해 전용 헬프라인을 운영하고 있다.

2. 프랑스: Viamedis·Almerys 개인정보 유출 사건 (IT Governance EU, 2024)

IT Governance Europe의 주간 보고에 따르면 2024년 2월 5일부터 11일 사이 유럽 보건의료 부문에서 여러 건의 중대한 사이버 침해 사건이 발생하였으며 그중 가장 큰 피해는 프랑스에서 보고되었다. 2024년 1월 말 프랑스의 건강보험 청구 처리 대행업체인 Viamedis와 Almerys가 피싱 기반 사이버 공격을 받았으며 조사 결과 두 업체의 시스템에서 보험 청구 처리에 필요한 일부 개인정보가 유출된 정황이 확인되었다. 노출된 정보에는 성명, 생년월일, 사회보장번호, 건강보험 관련 기본 정보가 포

함되었으며 의료 기록이나 금융 정보는 유출 범위에 포함되지 않은 것으로 파악되었다. 이번 사건은 약 3,300만 명의 보험 가입자와 그 가족에게 영향을 미친 대규모 개인정보 침해 사례로 평가된다.

유출된 정보는 계약자 및 그 가족의 성명, 생년월일, 사회보장번호, 건강보험사명, 계약 보장 내역 등 건강보험 청구 처리에 필요한 기본 인적 사항이 중심이었으며 금융정보, 구체적인 의료 기록, 환급 내역, 주소·전화번호·이메일 등 연락처 정보는 포함되지 않은 것으로 파악되었다.

프랑스 개인정보보호위원회(Commission Nationale de l'Informatique et des Libertés, CNIL)는 이번 대규모 개인정보 유출 사건에 대한 조사를 진행하고 있으며 각 건강보험사와 위탁계약을 체결한 두 대행업체를 통해 모든 피해자에게 개별 통지를 시행하도록 지시하였다. 또한 개인정보 악용 가능성을 경고하며 피해자들에게 건강보험 환급과 관련한 의심스러운 연락에 주의하고 계좌 활동을 정기적으로 확인할 것을 권고하였다. CNIL은 피해 규모가 매우 큰 점을 고려하여 사건 당시 적용된 보안 조치가 유럽 일반개인정보보호법(General Data Protection Regulation, GDPR) 요건에 부합했는지 여부를 조사하고 있다. 현재 조사와 함께 피해 최소화 조치와 책임 규명 절차가 진행되고 있으며 피해자 보호를 위한 후속 권고도 지속적으로 제공되고 있다.

3. 독일: AMEOS 병원 네트워크 사이버 공격 사건 (ComplianceHub Wiki, 2024)

독일의 대형 의료기관 네트워크인 AMEOS 병원 네트워크가 고도화된 사이버 공격을 받았다. 이번 공격은 지능형 지속 위협(Advanced Persistent Threat, APT) 기법[5]이 사용된 것으로 알려졌으며, 제로데이

취약점[6]과 네트워크 내 횡적 이동(lateral movement)[7], 다양한 보안 우회 기술[8]이 동원되었다. 이로 인해 환자 정보, 직원 기록, 협력사 데이터 등 민감한 정보가 유출됐을 가능성이 제기되고 있다.

AMEOS 측은 침해 사실을 확인한 즉시 네트워크를 격리하고 핵심 시스템을 차단했으며, 외부 디지털 포렌식 전문가를 긴급 투입했다. 또한 GDPR에 따라 독일 연방정보보안청 AMEOS 측은 침해 사실을 확인한 즉시 네트워크를 격리하고 핵심 시스템을 차단하였으며 외부 디지털 포렌식 전문가를 긴급 투입하였다. 또한 GDPR에 따라 독일 연방정보보안청(Bundesamt für Sicherheit in der Informationstechnik, BSI)에 사건을 신속히 보고하였다. 이후 취약점 패치 수행, 엔드포인트 탐지 및 대응(Endpoint Detection and Response, EDR) 시스템 도입, 제로트러스트 아키텍처 강화, 그리고 전 직원 대상 보안 교육 확대 등 보안 체계를 전면적으로 강화하였다.

이번 사건은 2020년 뒤셀도르프 대학병원 랜섬웨어 공격과 함께 독일 의료 분야 전반이 직면한 사이버 보안 위기를 다시 한 번 보여주는 사례로 평가된다. 의료 데이터는 다크웹에서 높은 가치를 가지며 장기적으로 악용될 가능성이 크다. 그러나 의료기관은 레거시 시스템((Legacy System)의 광범위한 사용, 복잡한 규제 준수 요구, 제한된 보안 예산, 그리고 환자 진료의 연속성 유지라는 특성으로 인해 보안 패치와 인프라 개선이 쉽

5) 특정 목표를 노리고 장기간 은밀하게 침투·잠복하며 데이터를 탈취하는 고도화된 표적형 사이버 공격
6) 보안 전문가나 소프트웨어 제작사도 아직 발견하지 못했거나 공개하지 않은 보안상의 결함
7) 공격자가 한 시스템이나 장비를 침투한 뒤, 그 내부 네트워크 내 다른 시스템들로 옮겨 다니면서 권한을 확장하거나 더 많은 정보를 훔치는 과정으로 네트워크 속에서 가로로 이동하며 공격 범위를 넓히는 행위
8) 공격자가 네트워크나 시스템의 보안 장치(방화벽, 안티바이러스, 접근 통제 등)를 뚫거나 무력화하기 위한 여러 방법들을 뜻함. 대표적으로 암호화된 악성코드, 권한 상승, 백도어 설치, 감지 회피 등이 있음.

지 않은 구조적 한계를 가지고 있다.

독일에서는 IT Security Act를 통해 대형 병원을 중요 기반시설로 지정하고 의무적인 사고 보고와 보안 표준 준수를 요구하고 있으며, Patient Data Protection Act를 통해 의료기관의 보안 요건을 강화하고 있다. 또한 일반 개인정보 보호 규정(General Data Protection Regulation, GDPR) 위반 시 최대 2천만 유로 또는 전 세계 매출의 4%에 해당하는 벌금이 부과될 수 있으며, 유럽 의료기기 규정(Medical Device Regulation) 위반 시 국가별 형사 처벌이 이루어질 가능성도 있다.

4. 터키 이스탄불 Bağc ı lar 교육·연구병원 사이버 공격 사건 (Duvar English, 2024)

2024년 4월 12일 터키 이스탄불의 Bağc ı lar 교육·연구병원(İstanbul Eğitim ve Araşt ı rma Hastanesi)이 해외 해커 조직의 사이버 공격을 받았다. 공격자는 병원의 보안 취약점을 이용해 병원 정보 시스템에 침투하여 2007년부터 최근까지 촬영된 CT, MRI, PET-CT, X-ray 영상과 각종 검사 결과, 그리고 환자 및 직원의 개인정보를 대규모로 탈취한 것으로 알려졌다.

이 과정에서 병원의 영상 저장·전송 시스템(Simplex)이 심각하게 손상되었으며 해당 시스템에는 별도의 백업 체계가 없어 영상 데이터가 완전히 소실된 것으로 나타났다. 병원 내 또 다른 시스템인 Bilbest는 일부 백업 데이터를 통해 복구 작업이 진행 중이나 마지막 백업 이후 약 12일간의 환자 데이터는 복원할 수 없는 것으로 확인되었다. 또한 E-nabiz(전자 건강 기록) 시스템에 저장된 자료와 의료진 성과 정보 일부에서도 데이터 손실이 발생한 것으로 보고되었다.

해커들은 병원 측에 약 20만 달러의 금전을 요구한 것으로 알려졌으며 일부 병원 직원들은 관리진의 책임 부족과 미흡한 대응이 피해를 확대시켰다고 비판하였다. 해당 병원은 약 438병상 규모로 100여 개 진료과목을 운영하며 하루 평균 약 5,000건, 연간 약 200만 건의 진료를 수행하는 대형 의료기관이다. 현재 다수의 IT 전문가가 시스템 복구 작업에 투입된 상태이다. 이번 사건은 대규모 의료 데이터와 환자 개인정보 유출, 그리고 병원 정보 시스템 마비를 동시에 초래한 사례로 평가되며 특히 백업 체계의 부재와 보안 관리 미흡이 피해 확산의 주요 원인으로 지적되고 있다.

제5절 소결

국내 의료기관에서 발생한 사이버 보안 침해사고는 의료정보시스템의 고도화와 디지털 의존도가 높아질수록 더욱 빈번하고 심각해지는 경향을 보이고 있다. 전자의무기록(EMR), 의료영상저장전송시스템(PACS), 처방전달시스템(OCS) 등은 병원 운영의 핵심 인프라이지만, 이들 시스템에 대한 보안 관리가 충분히 이루어지지 않아 공격자의 주요 표적이 되고 있다. 대부분의 침해사고는 복잡한 제로데이 취약점이나 고도의 해킹 기술에 의해 발생한 것이 아니라, 이미 알려진 보안 취약점과 잘못된 설정, 그리고 관리적 부주의에서 비롯된 것으로 나타났다. 즉, 패치 미적용, 초기 계정 비밀번호 미변경, 외부 포트 노출, VPN 장비 취약점 방치 등이 주요 침입 경로로 작용하였다. 이는 첨단 보안 기술의 도입 여부보다 기본적인 보안 수칙의 준수 여부가 피해의 심각도를 결정하는 핵심 요인임을 보여준다.

기관 규모에 따라 피해 양상에는 뚜렷한 차이가 나타난다. 의원급 의료기관의 경우 단일 전자의무기록(EMR) 서버에 진료 정보가 집중되어 있어 단일 장애가 곧바로 진료 중단으로 이어지는 구조적 취약성을 보였다. 이로 인해 공격자와의 협상이나 금전적 지불이 실제로 이루어지는 사례가 비교적 많이 나타났다. 중규모 병원에서는 가상사설망(VPN)이나 원격 데스크톱 프로토콜(Remote Desktop Protocol, RDP)을 통해 내부망이 침입된 이후 다수의 서버와 가상화 환경이 동시에 암호화되는 피해가 발생하였다. 종합병원에서는 의료정보시스템 서버 등 대규모 데이터 자산이 공격을 받아 복구가 장기간 지연되는 사례가 확인되었으며, 상급종합병원에서는 부대사업망이나 웹서버 취약점을 통한 외부 침입으로 병원 운영 전반이 교란되는 사례가 보고되었다. 이처럼 의료기관 규모와 IT 인

프라 수준에 따라 피해의 범위와 결과는 다르게 나타났지만, 공통적으로 환자 진료 지연, 수술 일정 차질, 영상 데이터 손실 등 환자 안전에 직접적인 영향을 미쳤다는 점에서 심각성이 크다.

피해를 확대시킨 주요 요인은 백업 관리의 실패였다. 많은 기관이 백업 데이터를 본 서버와 동일한 네트워크 또는 동일 스토리지에 저장하고 있어 본 데이터와 함께 백업 데이터까지 동시에 암호화되는 사례가 반복되었다. 이러한 구조는 '백업이 존재하지만 실제 복구는 불가능한' 상황을 초래하였으며, 결국 외부 복구업체의 지원이나 공격자와의 협상에 의존할 수밖에 없는 결과로 이어졌다. 또한 백업의 물리적 분리와 정기적인 복구 검증이 이루어지지 않아 복구 계획이 실질적인 대응 수단이 아니라 형식적인 절차에 머무른 기관이 대부분이었다.

금전적 손실은 단순히 공격자에게 지급한 몸값에 그치지 않는다. 의원과 중소병원의 경우 수백만 원에서 수천만 원 규모의 직접 지불 사례가 확인되었으며, 대형병원에서는 복구, 디지털 포렌식, 시스템 재구축 등에 수억 원 규모의 비용이 발생하였다. 그러나 더 큰 손실은 진료 중단으로 인한 수익 공백과 환자 이탈, 그리고 언론 보도에 따른 평판 하락에서 나타났다. 특히 상급종합병원의 경우 단 하루의 진료 지연만으로도 수억 원 규모의 재정 손실이 발생하며 환자 신뢰의 하락은 장기적인 브랜드 가치 저하로 이어질 수 있다. 따라서 의료기관의 피해 비용을 단순한 '랜섬 지불액'으로만 산정하는 것은 현실을 충분히 반영하지 못하며, 운영 손실, 복구 비용, 평판 손실 등을 모두 포함한 총체적 관점에서 평가할 필요가 있다.

또한 조직적 대응 역량의 부족 역시 피해 확산의 주요 요인으로 지적된다. 일부 기관에서는 사고 인지와 보고 절차가 정립되어 있지 않아 신고가 지연되거나 법정 통지 의무를 위반하여 과태료가 부과된 사례도 확인

되었다. 유지보수 업체와의 계약 구조가 불명확하여 책임 소재가 분명하지 않거나 복구 비용 분담을 둘러싼 분쟁이 발생한 경우도 있었다. 반면 사전에 모의훈련과 테이블탑 훈련을 실시한 병원은 대응본부를 신속히 가동하여 피해를 상대적으로 최소화할 수 있었다. 이러한 사례는 단순한 기술적 방어 역량뿐 아니라 보고 체계, 의사결정 구조, 훈련 체계, 계약 구조 등 조직적 거버넌스가 실제 복원력의 핵심 요소임을 보여준다.

결과적으로 국내 의료기관의 사이버 보안 문제는 단순한 정보기술적 취약성의 문제가 아니라 진료 연속성, 환자 안전, 병원 재정, 사회적 신뢰를 동시에 위협하는 복합적인 문제로 나타났다. 따라서 향후 의료기관 보안 정책은 첨단 보안 기술의 도입 여부보다 기본적인 보안 수칙의 준수, 분리된 백업 관리, 운영 손실을 고려한 복구 전략, 그리고 조직적 대응 역량 강화에 초점을 맞출 필요가 있다.

또한 현행 의료법 제23조의3이 '진료정보 침해사고 발생 시 통지' 의무만을 규정하고 있다는 점을 고려할 때, 사전 예방과 보안 관리체계 구축을 포함하는 포괄적인 사이버 보안 조항으로의 제도 개선이 필요하다. 이를 위해 보건복지부 주도의 의료 보안 관리체계(Healthcare ISMS) 도입, 정보보호 최고책임자(CISO) 지정, 독립적인 백업 및 복구 훈련 의무화, 사이버 위협 정보 공유 체계 구축 등이 제도적으로 뒷받침될 필요가 있다. 나아가 국제 표준(ISO/IEC 27799, NIST CSF, ENISA 프레임워크)과의 정합성을 확보함으로써 국내 의료 보안 수준을 글로벌 기준에 부합하도록 개선할 필요가 있다.

종합하면 국내외 의료기관 사례는 '보안은 기술이 아니라 관리이며 예방이 곧 치료'라는 점을 공통적으로 보여준다. 앞으로의 의료법과 정책 설계는 단순한 사고 통지 체계를 넘어 환자 안전을 중심으로 한 예방적 사이버 보안 관리체계 구축 방향으로 전환될 필요가 있다.

제5장

의료기관 사이버 보안 실태조사

제 5 장 의료기관 사이버 보안 실태조사

제1절 조사 개요 및 내용

1. 조사 개요

전 세계적으로 디지털 전환이 급격히 진행됨에 따라 의료기관을 겨냥한 사이버 위협이 지속적으로 증가하고 있다. 세계보건기구(WHO)의 2024년 보고서에 따르면 코로나19 팬데믹 기간 동안 의료기관을 대상으로 한 사이버 공격이 전 세계적으로 급증한 것으로 나타났다. 이러한 사이버 위협은 단순한 개인정보 탈취를 넘어 수술 지연과 진료 마비 등 환자의 생명과 건강에 중대한 영향을 미칠 수 있으며, 의료기관에도 직접적·간접적인 경제적 피해를 초래하고 있다.

그러나 우리나라 의료기관은 사이버 보안의 중요성에 대한 인식이 여전히 부족한 것으로 평가되며 관련 연구 역시 제한적인 수준에 머무르고 있다. 2024년 의료정보보호센터(ISAC)의 실태조사에 따르면 국내 상급종합병원의 40.0%, 종합병원의 92.9%가 보안관제서비스에 가입하지 않은 상태로 사실상 사이버 위협에 무방비로 노출되어 있는 것으로 나타났다. 주요 해외 국가에서는 의료기관을 대상으로 한 사이버 위협의 실태를 분석하고 대응 방안을 마련하기 위한 연구가 활발히 수행되고 있는 반면 국내에서는 관련 연구가 거의 부재하다.

이에 본 조사는 우리나라 의료기관의 사이버 보안 실태를 점검하고 문제점을 개선하기 위한 실증적 자료를 확보하는 것을 목적으로 한다. 구체적으로는 의료기관이 직면하고 있는 사이버 위협과 보안 현황을 종합적

으로 파악하고 침해사고 경험, 보안관제서비스 이용 현황, 대응 역량 등을 분석할 계획이다. 또한 보안관제서비스 미가입 사유, 현행 서비스의 문제점과 개선 필요 사항, 사이버 보안 강화를 위한 정책적 지원 요구 등을 조사하여 이를 바탕으로 의료기관 사이버 보안 역량 강화를 위한 정책 개선 방안을 도출하고자 한다.

가. 조사 대상

조사의 목표 모집단은 전국의 상급종합병원과 종합병원이며, 실제 조사에 활용된 모집단은 건강보험심사평가원이 제공한 '전국 병의원 및 약국 현황' 자료(2025년 3월 기준)에 등재된 상급종합병원 및 종합병원이다. 조사의 기본 단위는 의료기관으로 설정하여, 각 기관을 대상으로 사이버 보안 실태를 파악하였다.

나. 조사 지역 및 규모

조사는 전국 17개 시도를 대상으로 실시하였으며, 조사 대상은 상급종합병원 47개소와 종합병원 330개소로 구성하였다. 본 조사는 해당 의료기관 전체를 포함하는 전수조사 방식으로 진행되었다.

다. 조사 방법 및 조사 기간

조사 방법은 온라인 설문조사를 기본으로 하였으며, 조사업무는 (사)대한병원협회에 위탁하여 수행하였다. 조사 기간은 2025년 7월 28일부터 8월 22일까지 총 26일간 진행되었다.

2. 조사 내용

조사 내용은 표 5-1과 같으며 조사 참여 동의서, 개인정보 수집 동의서 및 조사표는 각각 부록 1~3에 수록하였다.

설문문항 개발을 위해 '2020년 보건의료정보화 실태조사' 설문조사, '2024년 정보보호 실태조사(기업)', '의료기관 정보보안 강화 지원전략 수립 인터뷰 질의서', '의료기관에 대한 사이버 공격 사례 연구 조사표' 등 4개의 정보보안 및 보건의료정보 관련 설문조사의 문항을 참고하였으며, 설문 문항의 선정 및 보완은 전문가 자문 및 연구진 검토를 통해 결정하였다.

〈표 5-1〉 의료기관 사이버 보안 실태조사 조사 내용 및 참고문헌

영역	문항		참고문헌 등				
			1	2	3	4	5
Ⅰ. 기본정보	1	기관명, 요양기관기호	기본문항				
	2	(대표)응답자 성명, 연락처	기본문항				
	3	(1-2문항) 응답자 소속 및 직무	기본문항				
Ⅱ. 의료기관 보안관제 등	4	보안관제 실시 여부	○				
	5	보안관제 유형	○				
	6	획득한 보안인증체계	○				
	7	(4-6문항) 응답자 소속 및 직무	기본문항				
Ⅲ. 의료기관 정보화/ 개인정보보호/ 정보보안 예산 현황	8	운영 및 투자 예산 규모		○			
	8-1	예산 규모 적절성에 대한 의견		○			
	9	(8문항) 응답자 소속 및 직무	기본문항				
Ⅳ. 전자 의무기록 시스템 인증제도	10	전자의무기록시스템 인증제도 인지 여부	○				
	11	인증된 전자의무기록시스템 도입 여부	○				
	11-1	인증된 전자의무기록시스템 도입 의향	○				
	12	(10-11문항) 응답자 소속 및 직무	기본문항				

영역	문항		참고문헌 등				
			1	2	3	4	5
Ⅴ. 의료정보 시스템 구축' 및 유지보수 현황	13	의료정보시스템 도입 여부 및 형태, 상용제품 여부, 유지보수 형태	○				
	14	의료정보시스템 연계 여부	○				
	15	클라우드 서비스 도입 현황	○				
	16	(13-15문항) 응답자 소속 및 직무	기본문항				
Ⅵ. 의료정보 시스템 정보화 담당조직 및 인력	17	정보화 업무 전담 부서 여부	○	○			
	18	정보화 업무 담당 인력 현황	○	○	○		
	19	정보보안 담당인력 충분성에 대한 의견			○		
	19-1	정보보안 담당인력 부족 문제 해결에 필요한 지원			○		
	20	(17-19문항) 응답자 소속 및 직무	기본문항				
Ⅶ. 정보보안 (교육)	21	정보보안 교육 시행 여부 몇 주기		○			
	21-1	정보보안 교육 참석 수준		○			
	21-2	주로 실시한 정보보안 교육 방법		○			
	21-3	임직원 대상 정보보안 교육의 효과		○			
	21-4	임직원 대상 정보보안 교육의 만족도		○			
	22	정보보호 및 정보보안 교육 미시행 이유		○			
	23	(21-22문항) 응답자 소속 및 직무	기본문항				
Ⅷ. 정보보호 및 정보보안 (정책)	24	정보보호 및 정보보안 관련 가이드라인 등 규정 필요성 여부		○			
	25	정보보호 및 정보보안 관련 자체 규정 여부		○			
	26	정보보호 및 정보보안 관련 자체 규정 포함 내용		○			
	27	(24-26문항) 응답자 소속 및 직무	기본문항				
Ⅸ. 정보보안 업무 관련 애로사항	28	정보보안 업무 관련 가장 큰 애로사항			○		
	29	어려움을 해결하기 위해 가장 필요한 지원			○		
	30	(28-39문항) 응답자 소속 및 직무	기본문항				
Ⅹ. 보안사고 (침해사고) 등	31	보안사고(침해사고) 발생 가능성에 대한 의견		○			
	32	최근 3년 간 보안사고(침해사고) 발생 여부		○			
	32-1	최근 3년 간 보안사고(침해사고) 발생 유형		○			
	32-2	보안사고(침해사고) 발생 시 평균 인지 시간		○		○	

영역	문항		참고문헌 등				
			1	2	3	4	5
	32-3	보안사고(침해사고) 발생 시 평균 대응 시간		○		○	
	32-4	보안사고(침해사고) 발생 시 복구 비용				○	
	32-5	보안사고(침해사고) 발생 시 파악 및 대응 수준		○		○	
	32-6	보안사고(침해사고) 발생 시 주요 원인				○	
	33	보안사고(침해사고) 대응 시 가장 큰 어려움	○			○	
	34	보안사고(침해사고) 발생 시 신고를 주저하는 이유		○	○		
	35	보안사고(침해사고) 신고율 향상을 위한 필요한 지원			○		
	36	주요 정보시스템에 정보보안 사항 적용 여부	○			○	
	37	(31-36문항) 응답자 소속 및 직무	기본문항				
Ⅺ. 정부지원 및 정책 개선 요구사항	38	정보보안 업무 강화를 위한 정부 지원 사항			○		
	38-1	법적/제도적 개선이 필요한 정보보안 관련 사항			○		
	39	(38문항) 응답자 소속 및 직무	기본문항				
Ⅻ. 보안관제 체계 도입 관련	40	보안관제 체계 도입 필요성 여부					○
	40-1	보안관제 체계 도입 필요성의 이유					○
	40-2	보안관제 체계 도입 시 기대 효과					○
	41	보안관제 체계 도입 저해 요인			○		
	42	보안관제 체계 도입 촉진을 위한 필요한 지원			○		
	43	보안관제 도입 효과를 높이기 위해 필요한 요소			○		
	44	보안 사고 예방을 위한 보안관제 체계의 효과			○		
	44-1	보안 사고 예방에 효과가 없다고 생각하는 이유			○		
	45	의료법 상 실시간 보안관제 의무화 포함 필요 여부			○		
	45-1	실시간 보안관제가 불필요하다고 생각하는 이유			○		
	46	중소 의료기관을 위한 클라우드 기반 보안관제 서비스 도입에 대한 의견					○
	46-1	중소 의료기관을 위한 클라우드 기반 보안관제 서비스를 부정적으로 생각하는 이유					○
	47	의료정보보호 관제서비스 이용 시 장점			○		
	48	정보보안이 가장 취약하다고 생각되는 부분			○		
	49	(40-48문항) 응답자 소속 및 직무	기본문항				

영역	문항		참고문헌 등				
			1	2	3	4	5
Ⅻ. 의료정보 보호센터 및 보안관제 가입 활성화 등	50	의료정보보호센터 보안관제서비스(ISAC) 가입여부					○
	50-1	의료정보보호센터와의 협력체계 구축 정도			○		
	50-2	의료정보보호센터와의 협력을 위한 개선점			○		
	51	보안관제 서비스 가입 활성화를 위해 필요한 지원			○		
	52	보안관제 가입 의무화 정책 필요성			○		
	52-1	보안관제 가입 의무화가 필요하다고 생각하는 이유			○		
	53	(50-52문항) 응답자 소속 및 직무	기본문항				
ⅩⅣ. 기타: LLM(대형언어모델) 기반 AI 서비스 등	54	LLM서비스 도입 여부					○
	55	LLM서비스의 주요 활용분야					○
	56	LLM서비스 도입에 따른 보안이슈 우려사항					○
	57	LLM서비스 도입 후 정보보안 사고					○
	58	LLM서비스에 특화된 보안툴 도입여부					○
	58-1	도입된 LLM서비스 보안툴의 종류					○
	58-2	도입된 LLM서비스의 보안툴의 만족도					○
	58-2	(54-58문항) 응답자 소속 및 직무	기본문항				

주: 1. 한국보건의료정보원. (2021). 2020년 보건의료정보화 실태조사 결과보고서. pp.387-441.
2. 한국정보보호산업협회. (2025). 2024년 정보보호 실태조사. pp.184-203.
3. 한국사회보장정보원. (2024). 의료기관 정보보안 강화 지원전략 수립 인터뷰 질의서(내부자료).
4. 사카구치 카즈키, 츠츠미 노부유키, 하라 유이치. (2023. 4. 11.). 의료 기관에 대한 사이버 공격 사례 연구: 민간 병원·의원의 피해 사례에서 배우다. 일본의사회종합정책연구기구 리서치 리포트 No.136
5. 연구진 회의 및 전문가 자문 결과

출처: 주 1~5를 참고하여 저자 작성

제2절 조사 결과

본 조사에서는 종합병원 330개소와 상급종합병원 47개소 등 총 377개 기관을 모집단으로 설정하였다. 이 중 종합병원 222개소와 상급종합병원 41개소가 응답하여 전체 응답률은 69.8%로 집계되었다. 응답기관의 구성비는 종합병원 84.4%, 상급종합병원 15.6%로 나타났으며, 이는 모집단의 구성비(종합병원 87.5%, 상급종합병원 12.5%)와 비교할 때 큰 차이를 보이지 않는 수준이었다.

〈표 5-2〉 의료기관 종별 응답현황(모집단 vs. 응답기관)

구분	모집단		표본집단(응답기관)	
	빈도(개소)	비율(%)	빈도(개소)	비율(%)
상급종합병원	47	12.5	41	15.6
종합병원	330	87.5	222	84.4
합계	377	100	263	100

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

$$\text{표본 비율 } (p) = \frac{222}{263} = 0.844$$
$$SE = \sqrt{\frac{p(1-p)}{n}} = \sqrt{\frac{0.844 \times 0.156}{263}} = 0.0224$$
$$1.96 \times SE = 1.96 \times 0.0224 = 0.0439$$

종합병원 응답비율의 표준오차는 약 0.022(±2.2%p)로 계산되었으며, 95% 신뢰수준에서의 오차범위는 ±4.4%p로 산정되었다. 모집단의 종합병원 비율(87.5%)은 해당 신뢰구간([80.0%, 88.8%]) 내에 포함되어 있어 표본이 통계적으로 모집단을 충분히 반영하고 있는 것으로 판단된다.

따라서 본 연구에서는 추가적인 가중치(weight) 보정을 실시하지 않고, 원시자료(raw data)를 그대로 활용하여 분석을 수행하였다. 이는 표

본의 대표성이 확보되어 있으며, 가중치 적용에 따른 분석 왜곡 가능성이 낮다고 판단되었기 때문이다.

다만, 종합병원(222개소)과 상급종합병원(41개소) 간 표본 규모의 불균형이 존재하여 기관유형 간 통계적 차이를 검정하기에는 한계가 있다. 특히 상급종합병원의 표본수가 상대적으로 적어, 집단 간 평균 또는 비율의 차이에 대한 통계적 검정(t-검정, $\chi 2$ 검정 등)을 수행할 경우 검정력이 충분히 확보되기 어렵다. 이에 따라 본 연구에서는 기관유형 간 단순 비교 결과를 해석함에 있어 통계적 유의성보다는 경향성 중심으로 참고하는 것을 권고한다.

지역 구분은 기관의 소재지를 기준으로 하되 시·도 및 시·군·구 단위로 세분화할 경우 특히 상급종합병원의 경우 기관이 식별될 가능성이 있어 이를 방지하기 위해 지역 유형을 도시(동)와 비도시(읍·면)로 단순화하여 구분하였다.

〈표 5-3〉 의료기관 종별 지역별 응답현황

구분	계	상급종합병원	종합병원
도시(동)	248개소(94.3%)	39개소(95.1%)	209개소(94.1%)
비도시(읍·면)	15개소(5.7%)	2개소(4.9%)	13개소(5.9%)
합계	263개소(100%)	41개소(100%)	222개소(100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

그러나 응답기관의 대부분이 도시지역(248개소, 94.3%)에 분포하고 비도시지역은 15개소(5.7%)에 불과하여 지역 유형 간 표본 불균형이 뚜렷하게 나타났다. 이에 따라 도시·비도시 간 차이를 통계적으로 검정하거나 지역별 결과를 비교·해석하는 데에는 한계가 있다. 따라서 본 연구에서는 지역 유형별 분석보다는 전체 표본(263개소)을 기준으로 한 종합적인 결과 해석을 중심으로 분석을 수행하였다.

1. 의료기관 보안관제 등

가. 보안관제 실시 여부

보안관제는 네트워크 장비와 보안 시스템 등을 원격 시스템(또는 장소)에서 관리하고, 인가받지 않은 외부 침입을 실시간으로 탐지하여 관제센터로 경보를 전송함으로써 외부 침입에 대한 즉각적인 대응과 역추적, 그리고 이기종 시스템 간 보안 관리를 수행할 수 있도록 하는 통합 보안 관리 체계를 의미한다.

〈표 5-4〉는 보안관제 실시 여부를 조사한 결과를 나타낸 것이다. 전체 응답기관(263개소) 중 '실시하고 있음'이 57.0%(150개소), '실시하지 않음'이 43.0%(113개소)로 나타났다.

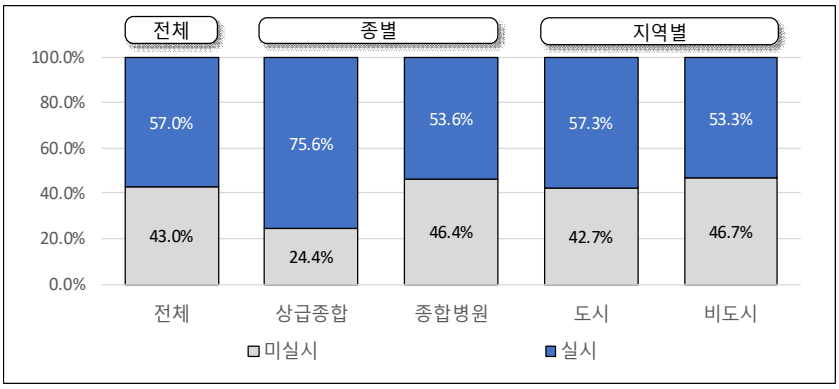
〈표 5-4〉 보안관제 실시 여부

구분		실시 n(%)	미실시 n(%)	합계 n(%)
전체	전체	150 (57.0)	113 (43.0)	263 (100.0)
종별	상급종합병원	31 (75.6)	10 (24.4)	41 (100.0)
	종합병원	119 (53.6)	103 (46.4)	222 (100.0)
지역별	도시(동)	142 (57.3)	106 (42.7)	248 (100.0)
	비도시(읍·면)	8 (53.3)	7 (46.7)	15 (100.0)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

의료기관 종별로 살펴보면 상급종합병원(41개소)의 75.6%(31개소), 종합병원(222개소)의 53.6%(119개소)가 보안관제를 실시하고 있는 것으로 나타났다. 지역별로 살펴보면 도시지역 의료기관(248개소)의 57.3%(142개소), 비도시지역 의료기관(15개소)의 53.3%(8개소)가 보안관제를 실시하고 있는 것으로 나타났다.

[그림 5-1] 보안관제 실시 여부



출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

종합하면 의료기관의 보안관제 도입률은 절반 수준에 머물러 있으며, 특히 종합병원과 일부 지역에서는 도입이 제한적인 것으로 나타났다. 이에 따라 보안관제 도입 확대를 위한 정책적 지원과 제도적 기반 강화가 필요한 것으로 나타났다.

나. 보안관제 유형

〈표 5-5〉는 보안관제 유형을 조사한 결과를 나타낸 것이다. 보안관제를 '실시하고 있음'으로 응답한 의료기관 150개소를 대상으로 해당 의료기관에서 운영 중인 보안관제 유형을 복수 응답 방식으로 조사한 결과 총 189건의 응답이 확인되었으며, 이는 의료기관당 평균 1.26개의 보안관제 유형을 운영하고 있는 것으로 나타났다.

총 응답수(189건)를 기준으로 보안관제 유형별 응답 비율을 살펴보면 '자체 보안관제'가 32.8%(62건)로 가장 높은 비율을 차지하였으며, '사이버안전센터(복지부, 교육부 등)' 22.2%(42건), '위탁(원격) 보안관제' 20.6%

(39건), '의료기관공동보안관제센터(의료ISAC)' 18.5%(35건), '위탁(파견) 보안관제' 3.2%(6건), '기타' 2.6%(5건), 순으로 나타났다. 기타 응답에는 정기점검 위탁, 민간 통합보안센터, 지자체 기반 사이버안전센터, 방화벽 관제 위탁, 의료원·계열사 통합관제 시스템 이용 등이 포함되었다.

〈표 5-5〉 보안관제 유형(복수 응답)

(단위: 개소, %)

항목	응답수	응답 비율
자체 보안관제	62	32.8%
위탁(파견) 보안관제	6	3.2%
위탁(원격) 보안관제	39	20.6%
사이버안전센터(복지부, 교육부 등)	42	22.2%
의료기관공동보안관제센터(ISAC)	35	18.5%
기타	5	2.6%
합계	189	100%

주: 응답수: 최대 6개까지 복수응답을 허용함
출처: 한국보건사회연구원. (2025). 의료기관 사이버보안 실태조사 원자료를 활용하여 저자 작성

〈표 5-6〉은 보안관제 유형 개수를 조사한 결과를 나타낸 것이다. 1개 유형만 운영하는 기관이 78.7%(118개소)로 대부분을 차지하였으며, 2개 유형 16.7%(25개소), 3개 유형 4.7%(7개소)로 나타났다.

종별로 보면 상급종합병원은 1개 유형 58.1%, 2개 유형 35.5%, 3개 유형 6.5%로 다층적 운영 비중이 상대적으로 높았으나, 종합병원은 1개 유형 84.0%로 단일 체계 의존도가 높은 것으로 나타났다.

종합하면 의료기관의 보안관제 운영은 단일 유형 중심 구조가 지배적이며, 다층적 관제 체계 구축은 제한적인 것으로 나타났다. 이에 따라 다양한 관제 유형을 결합한 다층적 보안관제 체계 구축 지원이 필요한 것으로 나타났다.

〈표 5-6〉 보안관제 유형 개수

(단위: 개소, %)

구분		1개	2개	3개	합계
전체	전체	118 (78.7)	25 (16.7)	7 (4.7)	150 (100.0)
종별	상급종합병원	18 (58.1)	11 (35.5)	2 (6.5)	31 (100.0)
	종합병원	100 (84.0)	14 (11.8)	5 (4.2)	119 (100.0)
지역별	도시(동)	111 (78.2)	24 (16.9)	7 (4.9)	142 (100.0)
	비도시(읍·면)	7 (87.5)	1 (12.5)	0 (0.0)	8 (100.0)

주: 괄호 안은 비율을 의미함.
출처: 한국보건사회연구원. (2025). 의료기관 사이버보안 실태조사 원자료를 활용하여 저자 작성

다. 보안인증체계

1) 보안관제 인증 여부

〈표 5-7〉은 보안관제 인증 여부를 조사한 결과를 나타낸 것이다. 보안관제를 실시하고 있는 의료기관(150개소) 중 인증을 획득한 기관은 32.6%(49개소), 미획득 기관은 67.3%(101개소)로 나타났다.

종합하면 보안관제 분야에서 인증제도 활용 수준은 전반적으로 낮은 것으로 나타났다. 이에 따라 보안관제 인증 활성화를 위한 제도적 지원이 필요한 것으로 나타났다.

〈표 5-7〉 보안관제 인증 여부

(단위: 개소, %)

항목	응답수	응답 비율
있음	49	32.6%
없음	101	67.3%
합계	150	100.0%

출처: 한국보건사회연구원. (2025). 의료기관 사이버보안 실태조사 원자료를 활용하여 저자 작성

2) 보안인증체계 유형

〈표 5-8〉은 획득한 보안인증체계를 조사한 결과를 나타낸 것이다. 복수응답 결과 ISMS가 60.0%(39개소)로 가장 높은 비중을 차지하였다.

기타 응답(25.9%)에는 전자의무기록시스템 인증, ISO 27799, ISO 27701, 개인정보영향평가(PIA), 주요정보통신기반시설 관리체계, 방화벽 인증, 청구소프트웨어 인증, 계열병원 통합 ISMS 등 다양한 인증이 포함되었다.

이는 의료기관이 일반 정보보호 인증뿐 아니라 의료 및 개인정보 특화 인증을 병행하여 적용하고 있음을 보여준다.

종합하면 의료기관은 다양한 인증체계를 병행 적용하고 있으나 표준화 수준은 제한적인 것으로 나타났다. 이에 따라 의료 특화 보안인증체계의 표준화 및 통합 관리가 필요한 것으로 나타났다.

〈표 5-8〉 획득한 보안인증체계(복수 응답)

(단위: 개소, %)

항목	응답수	응답 비율
ISMS	39	60.0%
ISMS-P	3	3.5%
ISO27001	8	10.6%
기타	16	25.9%
합계	66	100.0%

주: 최대 4개까지 복수응답을 허용함
출처: 한국보건사회연구원. (2025). 의료기관 사이버보안 실태조사 원자료를 활용하여 저자 작성

3) 보안인증체계 보유 개수

〈표 5-9〉는 획득한 보안인증체계 개수를 조사한 결과를 나타낸 것이〈표 5-9〉는 보안인증 보유 개수를 조사한 결과를 나타낸 것이다. 인증을 보유하지 않은 기관이 67.3%(101개소)로 가장 많았으며, 1개 24.0%, 2개 6.7%, 3개 이상은 극히 소수로 나타났다.

종별로 보면 상급종합병원은 인증 보유 비율이 높고 다중 인증을 운영하는 경향이 나타났으나, 종합병원은 84.9%가 인증을 보유하지 않아 격차가 크게 나타났다.

종합하면 의료기관 간 보안인증 도입 수준의 격차가 크게 나타났으며, 특히 종합병원의 인증 도입이 매우 제한적인 것으로 나타났다. 이에 따라 종합병원을 중심으로 보안인증 도입 지원 및 제도화가 필요한 것으로 나타났다.

〈표 5-9〉 획득한 보안관제 인증체계 개수

(단위: 개소, %)

구분		0개	1개	2개	3개	4개	합계
전체	전체	101 (67.3%)	36 (24.0%)	10 (6.7%)	2 (1.3%)	1 (0.7%)	150 (100%)
종별	상급 종합병원	0 (0.0%)	22 (71.0%)	6 (19.4%)	2 (6.5%)	1 (3.2%)	31 (100%)
	종합병원	101 (84.9%)	14 (11.8%)	4 (3.4%)	0 (0.0%)	0 (0.0%)	119 (100%)
지역별	도시(동)	94 (66.2)	36 (25.4%)	9 (6.3%)	2 (1.4%)	1 (0.7%)	142 (100.0)
	비도시 (읍·면)	7 (87.5%)	0 (0.0%)	1 (12.5)	0 (0.0%)	0 (0.0%)	8 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버보안 실태조사 원자료를 활용하여 저자 작성

2. 의료기관 정보화/개인정보보호/정보보안 예산[9] 현황

가. 의료기관 정보화/개인정보보호/정보보안 예산 규모

ISMS-P 인증 기준 중 '관리 체계 수립 및 운영 영역'의 '자원 할당 항목(1.1.6)'에서는 "최고경영자는 정보보호와 개인정보보호 분야별 전문성을 갖춘 인력을 확보하고, 관리체계의 효과적 구현과 지속적 운영을 위한 예산 및 자원을 할당하여야 한다"고 규정하고 있다.

〈표 5-10〉은 의료기관의 2024년과 2025년 정보화, 개인정보보호 및 정보보안 분야의 운영 및 투자 예산 규모를 조사한 결과를 나타낸 것이다.

2024년 기준 응답기관의 정보화·개인정보보호·정보보안 분야 운영 및 투자 예산 총액의 평균은 2,275.1백만 원으로 나타났다. 세부 항목별로는 정보화 예산이 평균 2,009.8백만 원으로 가장 높았으며, 정보보안 예산 216.1백만 원, 개인정보보호 예산 49.2백만 원 순으로 나타났다.

중간값 기준으로도 정보화 예산이 150백만 원으로 가장 높았으며, 정보보안 예산 20백만 원, 개인정보보호 예산 11백만 원 순으로 나타났다. 최대값은 정보화 예산 46,475백만 원, 정보보안 예산 4,863백만 원, 개인정보보호 예산 1,270백만 원으로 기관 간 편차가 매우 크게 나타났으며, 표준편차 또한 정보화 5,356.3백만 원, 정보보안 636.5백만 원, 개인정보보호 141.3백만 원으로 확인되었다.

---

9) 정보화 예산: 정보시스템 운영, 유지보수, 개발, 네트워크 운영 등 단순 정보시스템 운영 등에 소요되는 예산
개인정보보호 예산: 개인정보를 보호하기 위한 활동(시스템 구축, 컨설팅, 교육, 홍보, 인증 등) 등에 소요되는 예산
정보보안 예산: 정보시스템에 대한 기밀성, 무결성, 가용성을 유지 보호하기 위해 취하는 활동(시스템 구축) 등에 소요되는 예산

〈표 5-10〉 정보화/개인정보보호/정보보안 운영 및 투자예산 규모

(단위: 백만원)

구분	2024년 예산액			
	정보화	개인정보보호	정보보안	총액
n	263	263	263	263
평균	2,009.8	49.2	216.1	2,275.1
표준편차	5,356.3	141.3	636.5	5,814.6
최소값	0	0	0	0
Q1.25%	50	2	4	76
중간값.50%	150	11	20	190
Q3.75%	1,345	30	99	1,414
최대값	46,475	1,270	4,863	49,888
최빈값	0	0	0	0
상위10평균	13,934.9	327.4	1,575.7	15,315.8
하위10평균	0.6	0	0	2.4
구분	2025년 예산액			
	정보화	개인정보보호	정보보안	총액
n	263	263	263	263
평균	1,835.4	48.8	177.8	2,062.1
표준편차	4,916.1	137.1	455.5	5,313.8
최소값	0	0	0	0
Q1.25%	50	2	5	77.5
중간값.50%	140	12	21	180
Q3.75%	1,320.5	34	100	1,516
최대값	51,629	1,300	4,129	55,441
최빈값	0	0	0	0
상위10평균	12,562.7	320.4	1,169.1	13,665.8
하위10평균	0.6	0	0	2.1

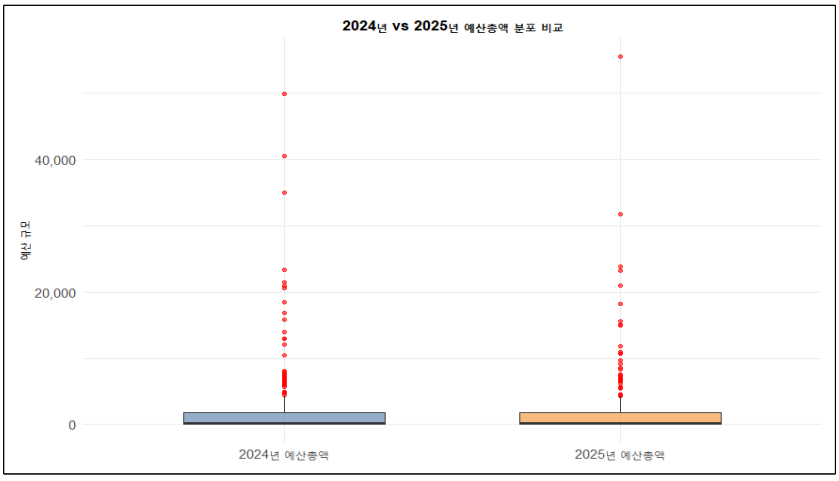
주: 총액=정보화 예산+개인정보보호 예산+정보보안
출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

2025년 기준 응답기관의 정보화·개인정보보호·정보보안 분야 운영 및 투자 예산 총액의 평균은 2,062.1백만 원으로 나타났다. 세부 항목별로는 정보화 예산이 평균 1,835.4백만 원으로 가장 높았으며, 정보보안 예

산 177.8백만 원, 개인정보보호 예산 48.8백만 원으로 나타났다.

중간값 기준으로도 정보화 예산이 140백만 원으로 가장 높았으며, 정보보안 예산 21백만 원, 개인정보보호 예산 12백만 원 순으로 나타났다. 최대값은 정보화 예산 51,629백만 원, 정보보안 예산 4,129백만 원, 개인정보보호 예산 1,300백만 원으로 나타나 기관 간 편차가 매우 크게 나타났으며, 표준편차는 정보화 4,916.1백만 원, 정보보안 455.5백만 원, 개인정보보호 137.1백만 원으로 확인되었다.

[그림 5-2] 정보화/개인정보보호/정보보안 운영 및 투자 예산 총액 비교
: 2024 vs. 2025



출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

2024년 대비 2025년에는 전체 정보화 관련 예산이 전반적으로 감소한 것으로 나타났다. 정보화 부문의 예산 비중이 여전히 가장 크지만, 개인정보보호 및 정보보안 부문은 상대적으로 감소 폭이 크지 않아 보안 및 개인정보 관리 요구가 일정 부분 반영된 것으로 나타났다. 또한 일부 기관은 높은 수준의 정보화 예산을 확보하고 있는 반면, 다수 기관은 상대

적으로 낮은 수준에 머물러 있어 예산 분포의 불균형이 크게 나타났다.

〈표 5-11〉은 정보화, 개인정보보호 및 정보보안 관련 예산액이 0원인 응답기관을 조사한 결과를 나타낸 것이다. 2024년에는 전체 응답기관 중 2024년 기준 전체 응답기관 중 정보화 예산이 0원인 기관은 21개소(8.0%), 개인정보보호 예산이 0원인 기관은 49개소(18.6%), 정보보안 예산이 0원인 기관은 45개소(17.1%)로 나타났다. 이를 종합하면 전체의 약 5.7%에 해당하는 의료기관이 세 항목 모두에서 예산을 편성하지 않은 것으로 나타났다. 즉, 다수의 의료기관이 개별 항목에 일정 수준의 예산을 확보하고 있으나, 일부 의료기관에서는 정보화·개인정보보호·정보보안 전반에 대한 예산이 부재한 것으로 나타났다.

2025년에는 정보화 예산이 0원인 기관이 22개소(8.4%), 개인정보보호 예산이 0원인 기관이 49개소(18.6%), 정보보안 예산이 0원인 기관이 44개소(16.7%)로 나타났다. 또한 세 항목 모두에서 예산이 없는 기관은 16개소(6.1%)로 집계되어 전년 대비 소폭 증가한 것으로 나타났다.

〈표 5-11〉 정보화/개인정보보호/정보보안 관련 예산액이 0원인 경우

(단위: 개소, %)

구분		예산액이 0원인 기관 수	전체 응답기관 중 비율(%)
2024년	정보화 예산	21	8.0
	개인정보보호 예산	49	18.6
	정보보안 예산	45	17.1
	총액	15	5.7
2025년	정보화 예산	22	8.4
	개인정보보호 예산	49	18.6
	정보보안 예산	44	16.7
	총액	16	6.1

주: 총액=정보화 예산+개인정보보호 예산+정보보안
출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

종합하면 일부 의료기관에서는 여전히 정보보안 및 개인정보보호 관련 예산이 편성되지 않은 상태가 지속되고 있으며, 항목별 예산 편성 격차 또한 크게 나타났다. 특히 개인정보보호와 정보보안 부문은 예산 미편성 기관 비율이 약 20% 수준에 이르는 것으로 나타났다. 이에 따라 정보보안 및 개인정보보호 예산의 최소 편성 기준 마련과 함께 예산 미편성 기관에 대한 관리 및 지원 강화가 필요한 것으로 나타났다.

〈표 5-12〉는 의료기관의 종별 및 지역별 정보화 운영 및 투자 예산 규모를 조사한 결과를 나타낸 것이다.

2024년 기준 상급종합병원의 평균 정보화 예산은 9,274.7백만 원으로, 종합병원 668.1백만 원에 비해 약 13.9배 높은 수준으로 나타났다. 중간값 또한 상급종합병원 6,194백만 원, 종합병원 100백만 원으로 큰 격차를 보여, 병원 규모에 따라 정보화 예산 규모의 차이가 뚜렷하게 나타났다.

2025년에도 이러한 경향은 유지되어, 상급종합병원의 평균 예산은 8,226.5백만 원, 종합병원은 587.7백만 원으로 나타났으며, 전년 대비 각각 약 11% 내외 감소한 것으로 나타났다.

〈표 5-12〉 종별 지역별 정보화 운영 및 투자 예산 규모

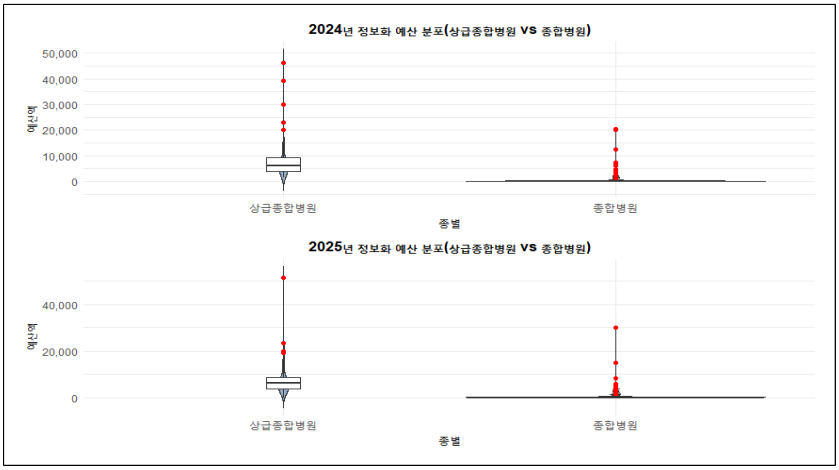
(단위: 백만원)

구분			n	평균	표준편차	중간값	최소값	최대값
2024년	종별	상급종합병원	41	9274.7	9743.5	6194	1449	46475
		종합병원	222	668.1	2286.8	100	0	20474
	지역별	도시(동)	248	2075.9	5484.3	150	0	46475
		비도시(읍·면)	15	916.6	2210.3	70	0	7570
2025년	종별	상급종합병원	41	822.6	851.9	502	0	4129
		종합병원	222	58.7	152.5	15	0	1406
	지역별	도시(동)	248	182.1	462.4	21	0	4129
		비도시(읍·면)	15	106.1	323.6	20	0	1271

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

종합하면 정보화 예산은 상급종합병원을 중심으로 집중되는 구조가 지속되고 있으며, 병원 규모에 따른 예산 격차가 크게 나타났다. 이에 따라 종합병원 등 중소 규모 의료기관의 정보화 투자 역량 강화를 위한 재정 지원 확대가 필요한 것으로 나타났다.

[그림 5-3] 종별 정보화 운영 및 투자 예산 비교: 2024 vs. 2025



출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

〈표 5-13〉는 의료기관의 종별 및 지역별 개인정보보호 운영 및 투자 예산 규모를 조사한 결과를 나타낸 것이다.

2024년 기준 상급종합병원의 평균 개인정보보호 예산은 158.4백만 원으로, 종합병원 29.1백만 원에 비해 약 5배 높은 수준으로 나타났으며, 중간값 또한 상급종합병원 20백만 원, 종합병원 11백만 원으로 나타나 병원 규모에 따른 예산 격차가 뚜렷하게 확인되었다.

2025년에도 이러한 경향은 유지되어, 상급종합병원의 평균 예산은 139.2백만 원, 종합병원은 29.8백만 원으로 나타났으며, 전년 대비 소폭 감소한 것으로 나타났다.

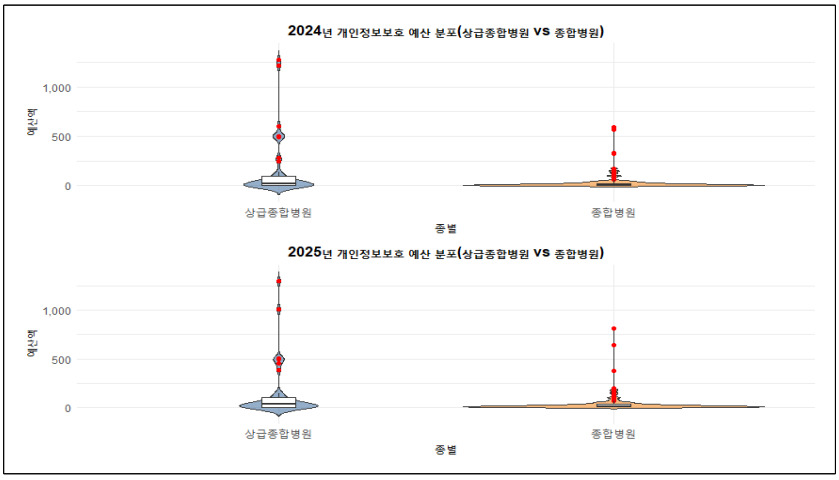
〈표 5-13〉 종별 지역별 개인정보보호 운영 및 투자 예산 규모

(단위: 백만원)

구분			n	평균	표준편차	중간값	최소값	최대값
2024년	종별	상급종합병원	41	158.4	301.1	20	0	1270
		종합병원	222	29.1	68	10	0	589
	지역별	도시(동)	248	51.2	145.2	11	0	1270
		비도시(읍·면)	15	17.4	22	10	0	90
2025년	종별	상급종합병원	41	139.2	278.7	31	0	1300
		종합병원	222	32.2	80.1	11	0	816
	지역별	도시(동)	248	50.6	140.8	12	0	1300
		비도시(읍·면)	15	19.1	23.8	14	0	90

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

[그림 5-4] 종별 개인정보보호 운영 및 투자 예산 비교: 2024 vs. 2025



출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

종합하면 개인정보보호 예산은 상급종합병원을 중심으로 집중되는 구조가 지속되고 있으며, 중소 규모 의료기관의 예산 수준은 상대적으로 낮게 나타났다. 이에 따라 의료기관 간 개인정보보호 투자 격차 완화를 위한 재정 지원 및 제도적 보완이 필요한 것으로 나타났다.

〈표 5-14〉는 의료기관의 종별 및 지역별 정보보안 운영 및 투자 예산 규모를 조사한 결과를 나타낸 것이다.

〈표 5-14〉 종별 지역별 정보보안 운영 및 투자 예산 규모

(단위: 백만원)

구분			n	평균	표준편차	중간값	최소값	최대값
2024년	종별	상급종합병원	41	1023.2	1157.9	540	82	4863
		종합병원	222	67	307.4	14	0	4271
	지역별	도시(동)	248	221.5	651	20	0	4863
		비도시(읍·면)	15	126.8	310.5	20	0	1185
2025년	종별	상급종합병원	41	822.6	851.9	502	0	4129
		종합병원	222	58.7	152.5	15	0	1406
	지역별	도시(동)	248	182.1	462.4	21	0	4129
		비도시(읍·면)	15	106.1	323.6	20	0	1271

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

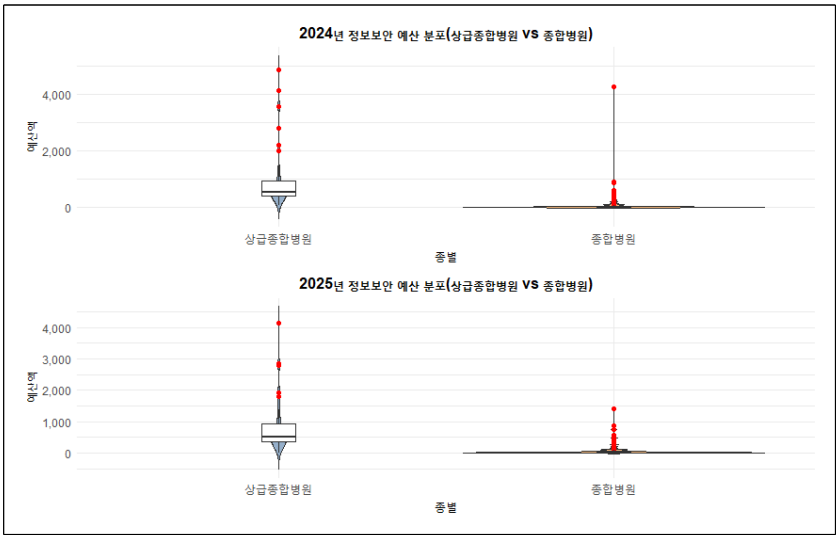
2024년 기준 상급종합병원의 평균 정보보안 예산은 1,023.2백만 원으로, 종합병원 67.0백만 원에 비해 약 15배 높은 수준으로 나타났다. 중간값 또한 상급종합병원 540백만 원, 종합병원 14백만 원으로 나타나 병원 규모에 따른 예산 격차가 매우 크게 나타났다.

2025년에도 유사한 경향이 나타났으며, 상급종합병원의 평균 예산은 822.6백만 원, 종합병원은 58.7백만 원으로 나타났고, 전년 대비 각각 약 19.6%와 12.4% 감소한 것으로 나타났다.

종합하면 2024년 기준 평균 정보화 예산(2,009.8백만 원) 대비 개인정보보호 예산은 2.4%(49.2백만 원), 정보보안 예산은 10.8%(216.1백만 원)으로 나타났다. 또한 2025년 기준 평균 정보화 예산(1,835.4백만 원) 대비 개인정보보호 예산은 2.7%(48.8백만 원), 정보보안 예산은 9.7%(177.8백만 원)으로 나타나, 개인정보보호 예산 비율은 여전히 3% 미만 수준에 머무르고 있는 것으로 나타났다.

이에 따라 의료기관의 정보보안 및 개인정보보호 투자 수준은 정보화 투자 대비 상대적으로 낮은 구조가 지속되고 있으며, 특히 중소 규모 의료기관을 중심으로 예산 격차가 크게 나타나고 있다. 따라서 정보보안 및 개인정보보호 예산의 적정 수준 확보와 병원 규모 간 투자 격차 완화를 위한 재정적·제도적 지원이 필요한 것으로 나타났다.

[그림 5-5] 종별 정보보안 운영 및 투자 예산 비교: 2024 vs. 2025



출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

나. 의료기관 정보화/개인정보보호/정보보안 예산 적절성

1) 정보화 예산 적절성

전체 의료기관(263개소)을 대상으로 조사한 결과, '매우 적절하다' 1.9%(5개소), '적절하다' 20.2%(53개소), '보통이다' 60.8%(161개소), '적절하지 않다' 14.1%(37개소), '매우 적절하지 않다' 3.0%(8개소)로 나타났다. 이를 긍정적 의견(매우 적절하다+적절하다)과 부정적 의견(적절하지 않다+매우 적절하지 않다)으로 구분하면, 긍정적 의견은 22.1%, 부정적 의견은 17.1%로 나타났다.

〈표 5-15〉 정보화 예산 규모 적절성에 대한 의견

(단위: 개소, %)

구분		매우 적절하다	적절하다	보통이다	적절하지 않다	매우 적절하지 않다	합계
전체	전체	5 (1.9%)	53 (20.2%)	160 (60.8%)	37 (14.1%)	8 (3%)	263 (100%)
종별	상급종합병원	1 (2.4%)	12 (29.3%)	23 (56.1%)	3 (7.3%)	2 (4.9%)	41 (100%)
	종합병원	4 (1.8%)	41 (18.5%)	137 (61.7%)	34 (15.3%)	6 (2.7%)	222 (100%)
지역별	도시(동)	4 (1.6%)	52 (21%)	151 (60.9%)	33 (13.3%)	8 (3.2%)	248 (100%)
	비도시(읍·면)	1 (6.7%)	1 (6.7%)	9 (60%)	4 (26.7%)	0 (0.0%)	15 (100%)

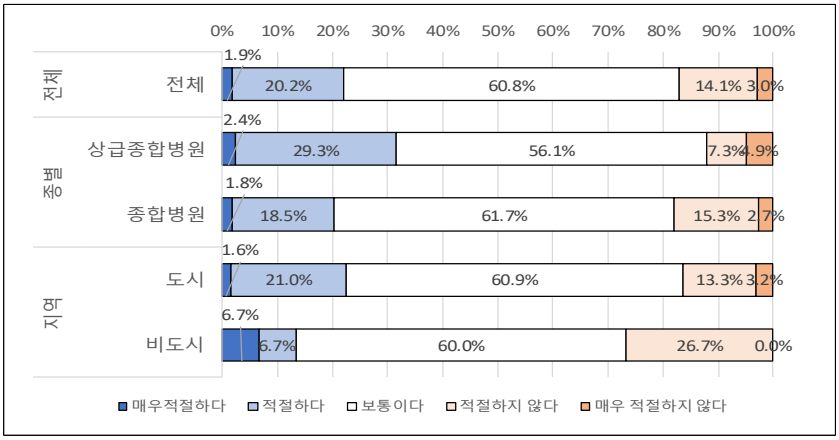
출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

의료기관 종별로 살펴보면, 상급종합병원(41개소)은 긍정적 의견 31.7%, 부정적 의견 12.2%로 나타났으며, 종합병원(222개소)은 긍정적 의견 20.3%, 부정적 의견 18.0%로 나타났다.

종합하면 정보화 예산 적절성에 대해서는 긍정적 의견이 부정적 의견

보다 높은 것으로 나타났으며, 상급종합병원이 종합병원보다 긍정적 인식이 높은 것으로 나타났다. 다만 일부 종합병원을 중심으로 예산 적절성에 대한 부정적 인식이 확인되어, 의료기관 간 정보화 투자 격차 완화를 위한 재정적 지원 확대가 필요한 것으로 나타났다.

[그림 5-6] 정보화 예산 규모 적절성에 대한 의견



출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

2) 개인정보보호 예산 적절성

〈표 5-16〉은 개인정보보호 예산 규모 적절성 의견을 조사한 결과를 나타낸 것이다.

전체 의료기관(263개소)을 대상으로 조사한 결과, '매우 적절하다' 1.1%(3개소), '적절하다' 5.3%(14개소), '보통이다' 48.3%(127개소), '적절하지 않다' 35.4%(93개소), '매우 적절하지 않다' 9.9%(26개소)로 나타났다. 이를 긍정적 의견과 부정적 의견으로 구분하면, 긍정적 의견은 6.4%, 부정적 의견은 45.3%로 나타났다.

〈표 5-16〉 개인정보보호 예산 규모 적절성에 대한 의견

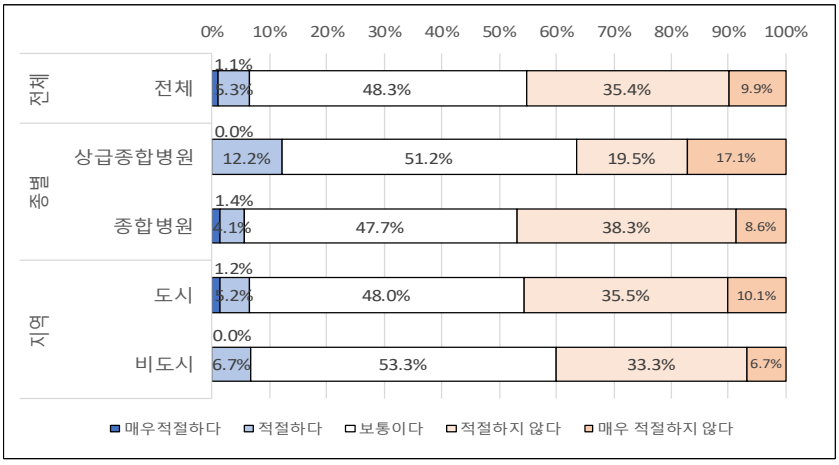
(단위: 개소, %)

구분		매우 적절하다	적절하다	보통이다	적절하지 않다	매우 적절하지 않다	합계
전체	전체	3 (1.1%)	14 (5.3%)	127 (48.3%)	93 (35.4%)	26 (9.9%)	263 (100.0%)
종별	상급종합병원	0 (0.0%)	5 (12.2%)	21 (51.2%)	8 (19.5%)	7 (17.1%)	41 (100.0%)
	종합병원	3 (1.4%)	9 (4.1%)	106 (47.7%)	85 (38.3%)	19 (8.6%)	222 (100.0%)
지역별	도시(동)	3 (1.2%)	13 (5.2%)	119 (48.0%)	88 (35.5%)	25 (10.1%)	248 (100%)
	비도시(읍·면)	0 (0.0%)	1 (6.7%)	8 (53.3%)	5 (33.3%)	1 (6.7%)	15 (100.0%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

의료기관 종별로 보면, 상급종합병원은 긍정적 의견 12.2%, 부정적 의견 36.6%로 나타났으며, 종합병원은 긍정적 의견 5.5%, 부정적 의견 45.6%로 나타났다.

[그림 5-7] 개인정보보호 예산 규모 적절성에 대한 의견



출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

종합하면 개인정보보호 예산 적절성에 대해 부정적 의견이 크게 나타났으며, 특히 종합병원에서 부정적 인식 비율이 높은 것으로 나타났다. 이에 따라 개인정보보호 예산의 절대 규모 확대와 함께 중소 의료기관 중심의 재정 지원 강화가 필요한 것으로 나타났다.

3) 정보보안 예산 적절성

전체 의료기관(263개소)을 대상으로 조사한 결과, '매우 적절하다' 1.1%(3개소), '적절하다' 6.5%(17개소), '보통이다' 48.7%(128개소), '적절하지 않다' 35.4%(93개소), '매우 적절하지 않다' 8.4%(22개소)로 나타났다. 이를 긍정적 의견과 부정적 의견으로 구분하면, 긍정적 의견은 7.6%, 부정적 의견은 43.8%로 나타났다.

〈표 5-17〉 정보보안 예산 규모 적절성에 대한 의견

(단위: 개소, %)

구분		매우 적절하다	적절하다	보통이다	적절하지 않다	매우 적절하지 않다	합계
전체	전체	3 (1.1%)	17 (6.5%)	128 (48.7%)	93 (35.4%)	22 (8.4%)	263 (100%)
종별	상급종합병원	0 (0.0%)	6 (14.6%)	21 (51.2%)	11 (26.8%)	3 (7.3%)	41 (100%)
	종합병원	3 (1.4%)	11 (5%)	107 (48.2%)	82 (36.9%)	19 (8.6%)	222 (100%)
지역별	도시(동)	2 (0.8%)	16 (6.5%)	123 (49.6%)	86 (34.7%)	21 (8.5%)	248 (100%)
	비도시(읍·면)	1 (6.7%)	1 (6.7%)	5 (33.3%)	7 (46.7%)	1 (6.7%)	15 (100%)

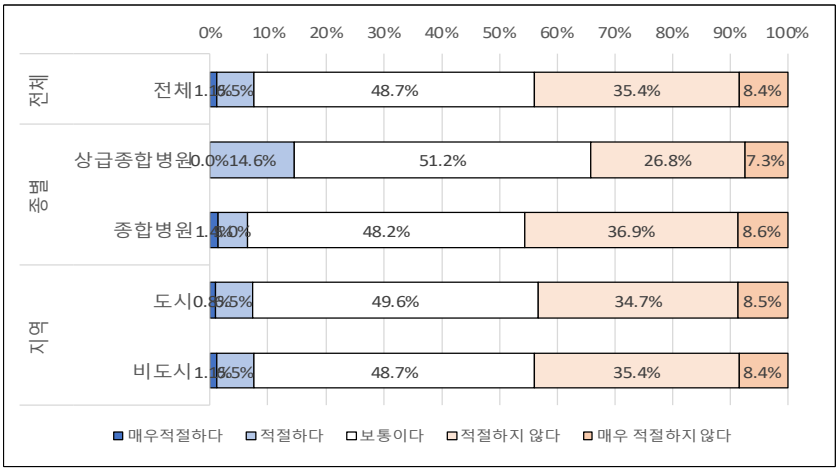
출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

의료기관 종별로 보면, 상급종합병원은 긍정적 의견 14.6%, 부정적 의견 34.1%로 나타났으며, 종합병원은 긍정적 의견 6.4%, 부정적 의견

45.5%로 나타났다.

종합하면 정보보안 예산 적절성에 대해 부정적 의견이 높게 나타났으며, 종합병원을 중심으로 예산 부족에 대한 인식이 크게 나타났다. 이에 따라 정보보안 예산의 안정적 확보와 함께 의료기관 간 투자 격차 완화를 위한 정책적 지원 강화가 필요한 것으로 나타났다.

[그림 5-8] 정보보안 예산 규모 적절성에 대한 의견



출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

3. 전자의무기록시스템 인증제도

전자의무기록시스템 인증제도란 「의료법」 제23조의2에 따라 환자 안전과 진료 연속성 지원을 목적으로, 국내 전자의무기록시스템에 대한 국가 표준과 적합성 검증을 통해 표준 제품 개발을 유도하고 시스템 간 상호운용성을 확보함으로써 품질 향상을 도모하는 제도이다. 또한 전자의무기록시스템 인증은 정보보안 관점에서 접근통제, 암호화, 인증관리, 백업관리, 로그 감시, 시스템 무결성 등 다양한 보안 요건을 포함하고 있다.

가. 전자의무기록시스템 인증제도 인지 여부

〈표 5-18〉은 전자의무기록시스템 인증제도 인지 여부를 조사한 결과를 나타낸 것이다.

전체 응답기관(263개소)을 대상으로 조사한 결과, '들어본 적이 있고 자세한 내용을 알고 있다'는 응답이 73.4%(193개소), '들어본 적은 있으나 자세한 내용은 모른다'는 응답이 26.6%(70개소)로 나타났으며, 제도를 전혀 인지하지 못한 기관은 없는 것으로 나타났다.

〈표 5-18〉 전자의무기록시스템 인증제도 인지 여부

(단위: 개소, %)

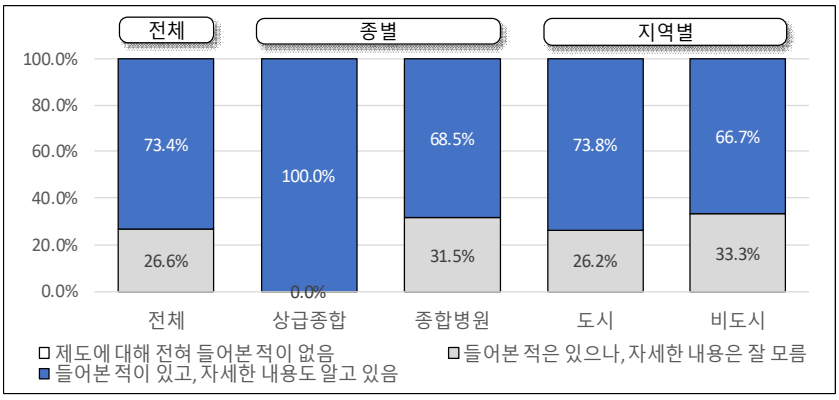
구분		들어본 적이 있고, 자세한 내용도 알고 있음	들어본 적은 있으나, 자세한 내용은 잘 모름	제도에 대해 전혀 들어본 적이 없음	합계
전체	전체	193 (73.4%)	70 (26.6%)	0 (0.0%)	263 (100%)
종별	상급종합병원	41 (100%)	0 (0.0%)	0 (0.0%)	41 (100%)
	종합병원	152 (68.5%)	70 (31.5%)	0 (0.0%)	222 (100%)
지역별	도시(동)	183 (73.8%)	65 (26.2%)	0 (0.0%)	248 (100%)
	비도시(읍·면)	10 (66.7%)	5 (33.3%)	0 (0.0%)	15 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

의료기관 종별로 살펴보면 상급종합병원(41개소)은 100.0%(41개소)가 제도를 인지하고 있는 것으로 나타났으며, 종합병원(222개소)은 '자세히 알고 있다' 68.5%(152개소), '들어본 적은 있으나 자세한 내용은 모른다' 31.5%(70개소)로 나타났다.

종합하면 전자의무기록시스템 인증제도에 대한 전반적인 인지도는 높은 수준으로 나타났으나, 종합병원을 중심으로 제도에 대한 이해 수준의 차이가 존재하는 것으로 나타났다. 이에 따라 제도에 대한 이해도 제고를 위한 교육 및 홍보 강화가 필요한 것으로 나타났다.

[그림 5-9] 전자의무기록시스템 인증제도 인지 여부



출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

나. 인증된 전자의무기록시스템 도입 여부 및 도입 의향

〈표 5-19〉은 인증된 전자의무기록시스템 도입 여부를 조사한 결과를 나타낸 것이다.

전체 응답기관(263개소) 중 72.2%(190개소)가 인증된 전자의무기록시스템을 도입하였으며, 27.8%(73개소)는 도입하지 않은 것으로 나타났다.

의료기관 종별로 보면 상급종합병원(41개소)은 100.0%(41개소)가 도입한 반면, 종합병원(222개소)은 67.1%(149개소)가 도입, 32.9%(73개소)는 미도입 상태로 나타났다.

종합하면 상급종합병원은 인증제도 도입이 완료된 반면, 종합병원에서는 도입 수준이 상대적으로 낮은 것으로 나타났다. 이에 따라 중소 규모 의료기관을 중심으로 인증제도 도입 확산을 위한 정책적 지원이 필요한 것으로 나타났다.

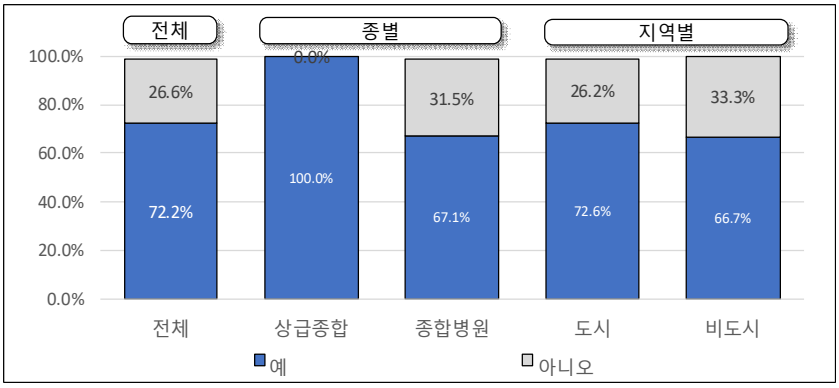
〈표 5-19〉 인증된 전자의무기록시스템 도입 여부

(단위: 개소, %)

구분		예	아니오	합계
전체	전체	190 (72.2%)	73 (27.8)	263 (100%)
종별	상급종합병원	41 (100%)	0 (0.0%)	41 (100%)
	종합병원	149 (67.1%)	73 (32.9%)	222 (100%)
지역별	도시(동)	180 (72.6%)	68 (27.4%)	248 (100%)
	비도시(읍·면)	10 (66.7%)	5 (33.3%)	15 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

[그림 5-10] 인증된 전자의무기록시스템 도입 여부



출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

〈표 5-20〉은 인증된 전자의무기록시스템 미도입 의료기관을 대상으로 인증된 전자의무기록시스템 도입 의향을 조사한 결과를 나타낸 것이다.

인증된 전자의무기록시스템을 도입하지 않은 의료기관(73개소) 중 '도입 의향이 있다'는 응답은 32.9%(24개소), '도입 의향이 없다'는 응답은 67.1%(49개소)로 나타났다.

의료기관 종별로 보면 상급종합병원은 전 기관이 이미 도입한 상태이며, 종합병원에서는 도입 의향이 있는 기관이 32.9%(24개소)에 그친 것으로 나타났다.

〈표 5-20〉 인증된 전자의무기록시스템 도입 의향

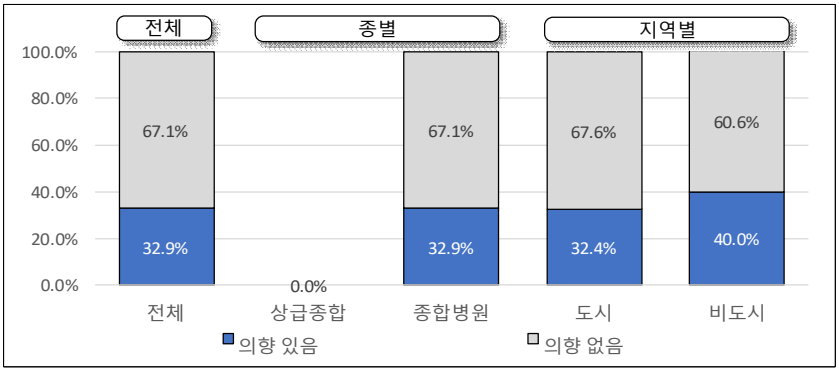
(단위: 개소, %)

구분		의향 있음	의향 없음	합계
전체	전체	24 (32.9%)	49 (67.1%)	73 (100%)
종별	상급종합병원	0 (0.0%)	0 (0.0%)	0 (100%)
	종합병원	24 (32.9%)	49 (67.1%)	73 (100%)
지역별	도시(동)	22 (32.4%)	46 (67.6%)	68 (100%)
	비도시(읍·면)	2 (40.0%)	3 (60.0%)	5 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

종합하면 인증제도 미도입 기관의 도입 의향은 전반적으로 낮은 수준으로 나타났으며, 특히 종합병원에서 도입 의지가 제한적인 것으로 나타났다. 이에 따라 인증제도 도입을 유도하기 위한 재정 지원, 인센티브 제공 및 제도적 유인 강화가 필요한 것으로 나타났다.

[그림 5-11] 인증된 전자의무기록시스템 도입 의향



출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

4. 의료정보 시스템 구축 및 유지보수 현황

가. 의료정보 시스템 구축 및 유지보수 현황

전체 응답기관(263개소)을 기준으로 보면, '전자의무기록시스템'은 모든 기관(100%)에서 도입되어 의료기관의 전산화 기반이 전반적으로 정착된 것으로 나타났다. '처방전달시스템'(98.9%)과 '의료영상저장전송시스템'(99.6%) 역시 대부분의 기관에서 구축되어 핵심 진료정보시스템은 높은 도입 수준을 보였다.

반면 '임상검사정보시스템'(67.3%), '약국관리시스템'(71.9%), '진료과 및 회송시스템'(63.9%), '진료정보교류시스템'(69.6%) 등 진료지원성 시스템은 상대적으로 낮은 도입률을 보였으며, '모바일 전자의무기록시스템'은 29.7%, '원격의료시스템'은 11.0%에 그쳐 모바일·원격 진료 기반 시스템은 제한적으로 운영되고 있는 것으로 나타났다.

의료기관 종별로 보면 상급종합병원은 대부분의 항목에서 높은 도입률을 보였다. '전자의무기록시스템'과 '의료영상저장전송시스템'은 전 기관에서 구축되어 있었으며, '처방전달시스템', '진료과 및 회송시스템', '진료정보교류시스템', '건강검진정보시스템'도 90% 이상의 높은 도입률을 보였다. 또한 '임상검사정보시스템'과 '약국관리시스템' 역시 각각 87.8%, 85.4%로 비교적 높은 수준을 유지하고 있었다. '모바일 전자의무기록시스템'은 61.0%로 나타났으나, '원격의료시스템'은 17.1%로 낮은 수준에 머물러 있었다.

종합병원의 경우 '전자의무기록시스템'은 전 기관에서 구축되어 있었으며, '처방전달시스템', '의료영상저장전송시스템', '건강검진정보시스템'도 95% 이상으로 높은 도입률을 보였다.

〈표 5-21〉 의료정보시스템 도입 여부(진료정보)

(단위: 개소, %)

구분	전자의무기록시스템(EMR)			모바일 전자의무기록시스템(EMR)		
	예	아니오	합계	예	아니오	합계
전체	263 (100%)	0 (0.0%)	263 (100%)	78 (29.7%)	185 (70.3%)	263 (100%)
상급 종합병원	41 (100%)	0 (0.0%)	41 (100%)	25 (61%)	16 (39%)	41 (100%)
종합병원	222 (100%)	0 (0.0%)	222 (100%)	53 (23.9%)	169 (76.1%)	222 (100%)
도시(동)	248 (100%)	0 (0.0%)	248 (100%)	74 (29.8%)	174 (70.2%)	248 (100%)
비도시 (읍·면)	15 (100%)	0 (0.0%)	15 (100%)	4 (26.7%)	11 (73.3%)	15 (100%)
구분	처방전달시스템(OCS)			의료영상저장전송시스템(PACS)		
	예	아니오	합계	예	아니오	합계
전체	260 (98.9%)	3 (1.1%)	263 (100%)	262 (99.6%)	1 (0.4%)	263 (100%)
상급 종합병원	40 (97.6%)	1 (2.4%)	41 (100%)	41 (100%)	0 (0.0%)	41 (100%)
종합병원	220 (99.1%)	2 (0.9%)	222 (100%)	221 (99.5%)	1 (0.5%)	222 (100%)
도시(동)	245 (98.8%)	3 (1.2%)	248 (100%)	247 (99.6%)	1 (0.4%)	248 (100%)
비도시 (읍·면)	15 (100%)	0 (0.0%)	15 (100%)	15 (100%)	0 (0.0%)	15 (100%)
구분	임상검사정보시스템(LIS)			약국관리시스템		
	예	아니오	합계	예	아니오	합계
전체	177 (67.3%)	86 (32.7%)	263 (100%)	189 (71.9%)	74 (28.1%)	263 (100%)
상급 종합병원	36 (87.8%)	5 (12.2%)	41 (100%)	35 (85.4%)	6 (14.6%)	41 (100%)
종합병원	141 (63.5%)	81 (36.5%)	222 (100%)	154 (69.4%)	68 (30.6%)	222 (100%)
도시(동)	168 (67.7%)	80 (32.3%)	248 (100%)	179 (72.2%)	69 (27.8%)	248 (100%)
비도시 (읍·면)	9 (60.0%)	6 (40.0%)	15 (100%)	10 (66.7%)	5 (33.3%)	15 (100%)

구분	진료과 및 회송 시스템(상/하/원)			진료정보교류시스템(복지부)		
	예	아니오	합계	예	아니오	합계
전체	168 (63.9%)	95 (36.1%)	263 (100%)	183 (69.6%)	80 (30.4%)	263 (100%)
상급 종합병원	40 (97.6%)	1 (2.4%)	41 (100%)	39 (95.1%)	2 (4.9%)	41 (100%)
종합병원	128 (57.7%)	94 (42.3%)	222 (100%)	144 (64.9%)	78 (35.1%)	222 (100%)
도시(동)	159 (64.1%)	89 (35.9%)	248 (100%)	174 (70.2%)	74 (29.8%)	248 (100%)
비도시 (읍·면)	9 (60.0%)	6 (40.0%)	15 (100%)	9 (60.0%)	6 (40.0%)	15 (100%)
구분	원격의료시스템			건강검진정보시스템		
	예	아니오	합계	예	아니오	합계
전체	29 (11.0%)	234 (89.0%)	263 (100%)	249 (94.7%)	14 (5.3%)	263 (100%)
상급 종합병원	7 (17.1%)	34 (82.9%)	41 (100%)	37 (90.2%)	4 (9.8%)	41 (100%)
종합병원	22 (9.9%)	200 (90.1%)	222 (100%)	212 (95.5%)	10 (4.5%)	222 (100%)
도시(동)	28 (11.3%)	220 (88.7%)	248 (100%)	235 (94.8%)	13 (5.2%)	248 (100%)
비도시 (읍·면)	1 (6.7%)	14 (93.3%)	15 (100%)	14 (93.3%)	1 (6.7%)	15 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

반면 '임상검사정보시스템', '약국관리시스템', '진료과 및 회송시스템', '진료정보교류시스템'은 57~69% 수준으로 나타났으며, '모바일 전자의무기록시스템'(23.9%)과 '원격의료시스템'(9.9%)은 매우 낮은 도입률을 보였다.

종합하면 의료기관의 전자의무기록시스템, 처방전달시스템, 의료영상저장전송시스템 등 핵심 진료정보시스템은 전반적으로 구축되어 전산화 기반이 안정적으로 형성된 것으로 나타났다. 반면 모바일 전자의무기록시스템, 원격의료시스템 및 진료지원성 정보시스템은 도입 수준이 상대적으로 낮아 의료정보의 연계성과 디지털 진료환경 확장에는 한계가 존

재하는 것으로 나타났다. 또한 상급종합병원과 종합병원 간 시스템 도입 수준의 격차가 확인됨에 따라, 모바일·원격 진료 기반 확대와 진료지원 시스템 고도화를 위한 정책적 지원 및 의료기관 간 격차 완화 노력이 필요한 것으로 나타났다.

〈표 5-22〉는 환자 서비스 관련 의료정보시스템 도입 여부를 조사한 결과를 나타낸 것이다.

전체 응답기관(263개소) 중 '의료기관 포털(대표 홈페이지)'을 운영하는 기관은 255개소(97.0%)로 나타나 대부분의 의료기관이 자체 홈페이지를 통한 환자 정보 제공 체계를 구축하고 있는 것으로 확인된다. '의료기관 포털(웹) 기반 개인건강기록'을 운영하는 기관은 40개소(15.2%)로 나타나 아직 도입률이 낮은 수준이었다. 한편 '모바일 개인건강기록' 시스템을 도입한 기관은 67개소(25.5%)로 나타났다.

의료기관 종별로 살펴보면 상급종합병원은 모든 항목에서 종합병원보다 높은 수준의 환자용 정보서비스를 제공하고 있는 것으로 나타났다. 상급종합병원의 경우 '의료기관 포털(대표 홈페이지)'은 97.6%(40개소), '의료기관 포털(웹) 기반 개인건강기록'은 46.3%(19개소), '모바일 개인건강기록'은 58.5%(24개소)로 나타났다. 반면 종합병원은 '의료기관 포털(대표 홈페이지)' 96.8%(215개소), '의료기관 포털(웹) 기반 개인건강기록' 9.5%(21개소), '모바일 개인건강기록' 15.3%(34개소)로 나타나 전반적으로 낮은 수준이었다.

종합하면 의료기관은 대부분 기본적인 홈페이지 수준의 정보 제공 체계는 구축되어 있으나, 웹·모바일 기반 개인건강기록 등 환자 참여형 서비스는 전반적으로 초기 단계에 머물러 있는 것으로 나타났다. 상급종합병원은 환자 맞춤형 진료정보 제공과 모바일 접근성 강화를 위한 디지털 헬스케어 서비스를 비교적 적극적으로 도입하고 있는 반면, 종합병원은 단순 정보 제공 중심의 기본형 서비스에 머무르고 있는 것으로 분석된다.

〈표 5-22〉 의료정보시스템 도입 여부(환자 서비스)

(단위: 개소, %)

구분	의료기관 포털(대표 홈페이지)			의료기관 포털(웹) 기반 개인건강기록(PHR)		
	예	아니오	합계	예	아니오	합계
전체	255 (97.0%)	8 (3.0%)	263 (100%)	40 (15.2%)	223 (84.8%)	263 (100%)
상급 종합병원	40 (97.6%)	1 (2.4%)	41 (100%)	19 (46.3%)	22 (53.7%)	41 (100%)
종합병원	215 (96.8%)	7 (3.2%)	222 (100%)	21 (9.5%)	201 (90.5%)	222 (100%)
도시(동)	240 (96.8%)	8 (3.2%)	248 (100%)	39 (15.7%)	209 (84.3%)	248 (100%)
비도시 (읍·면)	15 (100%)	0 (0.0%)	15 (100%)	1 (6.7%)	14 (93.3%)	15 (100%)
구분	모바일 개인건강기록(PHR)			여백		
	예	아니오	합계			
전체	67 (25.5%)	196 (74.5%)	263 (100%)			
상급 종합병원	33 (80.5%)	8 (19.5%)	41 (100%)			
종합병원	34 (15.3%)	188 (84.7%)	222 (100%)			
도시(동)	66 (26.6%)	182 (73.4%)	248 (100%)			
비도시 (읍·면)	1 (6.7%)	14 (93.3%)	15 (100%)			

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

〈표 5-23〉은 진료 지원 및 경영 정보 관련 의료정보시스템 도입 여부를 조사한 결과를 나타낸 것이다. 전체 응답기관(263개소) 중 '원무관리·보험청구시스템'을 운영하는 기관은 254개소(96.6%)로 나타나 대부분의 기관이 진료비 청구 및 행정업무의 전산화를 완료한 것으로 나타났다. '전자적 자원관리시스템'은 183개소(69.6%)에서 도입되어 비교적 높은 수준을 보였으며, '내부직원지원시스템'은 81개소(30.8%), '전사적 데이터웨어하

우스'는 61개소(23.2%)로 나타나 도입률이 상대적으로 낮은 수준이었다.

〈표 5-23〉 의료정보시스템 도입 여부(진료 지원 및 경영 정보)

(단위: 개소, %)

구분	원무관리, 보험청구시스템			전자적 자원관리시스템(ERP)		
	예	아니오	합계	예	아니오	합계
전체	254 (99.6%)	9 (3.4%)	263 (100%)	183 (69.6%)	80 (30.4%)	263 (100%)
상급 종합병원	38 (92.7%)	3 (7.3%)	41 (100%)	25 (61%)	16 (39%)	41 (100%)
종합병원	216 (97.3%)	6 (2.7%)	222 (100%)	158 (71.2%)	64 (28.8%)	222 (100%)
도시(동)	239 (96.4%)	9 (3.6%)	248 (100%)	172 (69.4%)	76 (30.6%)	248 (100%)
비도시 (읍·면)	15 (100%)	0 (0.0%)	15 (100%)	11 (73.3%)	4 (26.7%)	15 (100%)
구분	내부직원지원시스템(ESS)			전사적데이터웨어하우스(EDW)		
	예	아니오	합계	예	아니오	합계
전체	81 (30.8%)	182 (69.2%)	263 (100%)	61 (23.2%)	202 (76.8%)	263 (100%)
상급 종합병원	24 (58.5%)	17 (41.5%)	41 (100%)	26 (63.4%)	15 (36.6%)	41 (100%)
종합병원	57 (25.7%)	165 (74.3%)	222 (100%)	35 (15.8%)	187 (84.2%)	222 (100%)
도시(동)	77 (31.0%)	171 (69.0%)	248 (100%)	58 (23.4%)	190 (76.6%)	248 (100%)
비도시 (읍·면)	4 (26.7%)	11 (73.3%)	15 (100%)	3 (20.0%)	12 (80.0%)	15 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

종별로 살펴보면, 상급종합병원과 종합병원 모두 기본적인 행정·경영 정보시스템을 폭넓게 도입하고 있는 것으로 나타났다. '원무관리·보험청구시스템'은 상급종합병원 38개소(92.7%), 종합병원 216개소(97.3%)에서 구축되어 거의 모든 기관이 운영 중이었다. '전자적 자원관리시스템'은 상급종합병원 25개소(61.0%), 종합병원 158개소(71.2%)로, 두 유형

간 큰 차이는 없었다. 반면 '내부직원지원시스템'은 상급종합병원이 24개소(58.5%)로 종합병원(25.7%, 57개소)에 비해 두 배 이상 높았고, '전사적 데이터웨어하우스' 역시 상급종합병원 26개소(63.4%)로 종합병원(15.8%, 35개소)에 비해 도입률이 현저히 높았다.

종합하면 의료기관의 행정·경영지원 정보시스템은 원무관리·보험청구 시스템을 중심으로 기본적인 구축은 이루어졌으나, 전자적 자원관리시스템, 내부직원지원시스템, 전사적 데이터웨어하우스 등 경영정보 및 내부 의사결정 지원을 위한 고도화된 시스템은 전반적으로 확산 초기 단계에 머물러 있는 것으로 나타났다.

〈표 5-24〉는 교육 및 연구 관련 의료정보시스템 도입 여부를 조사한 결과를 나타낸 것이다.

전체 응답기관(263개소) 중 '보수교육 전산시스템'을 운영 중인 기관은 21.3%(56개소), '조사연구 전산시스템'은 15.2%(40개소)로 나타나, 의료기관 내 교육 및 연구 지원을 위한 정보화 수준은 전반적으로 낮은 것으로 나타났다.

의료기관 종별로 살펴보면 상급종합병원은 '보수교육 전산시스템' 51.2%, '조사연구 전산시스템' 46.3%로 나타나, 종합병원(각각 15.8%, 9.5%)보다 도입률이 현저히 높은 것으로 나타났다. 이는 상급종합병원이 교육·연구 기능 강화를 위해 정보시스템을 적극적으로 활용하고 있는 반면, 종합병원은 상대적으로 도입 수준이 낮음을 보여준다.

종합하면 의료기관의 교육·연구 및 연구데이터 관리·분석 지원을 위한 정보화 수준은 전반적으로 미흡하여 진료 및 행정 중심의 정보화에 비해 디지털 전환이 상대적으로 지연된 것으로 나타났다. 특히 병원 규모에 따라 교육·연구 정보화 수준의 격차가 확인되었다.

〈표 5-24〉 의료정보시스템 도입 여부(교육 및 연구)

(단위: 개소, %)

구분	보수교육 전산시스템			조사연구 전산시스템		
	예	아니오	합계	예	아니오	합계
전체	56 (21.3%)	207 (78.7%)	263 (100%)	40 (15.2%)	223 (84.8%)	263 (100%)
상급 종합병원	21 (51.2%)	20 (48.8%)	41 (100%)	19 (46.3%)	22 (53.7%)	41 (100%)
종합병원	35 (15.8%)	187 (84.2%)	222 (100%)	21 (9.5%)	201 (90.5%)	222 (100%)
도시(동)	54 (21.8%)	194 (78.2%)	248 (100%)	39 (15.7%)	209 (84.3%)	248 (100%)
비도시 (읍·면)	2 (13.3%)	13 (86.7%)	15 (100%)	1 (6.7%)	14 (93.3%)	15 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

〈표 5-25〉는 기타 부대사업 관련 의료정보시스템 도입 여부를 조사한 결과를 나타낸 것이다.

〈표 5-25〉는 기타 부대사업 관련 의료정보시스템 도입 여부를 조사한 결과를 나타낸 것이다. 전체 응답기관(263개소) 중 '부설 노인복지시설 전산시스템'은 2.3%(6개소)에 불과해 도입 수준이 매우 낮은 것으로 나타났으며, '부설 장례식장 전산시스템'은 44.5%(117개소), '부설 주차시스템'은 59.3%(156개소)로 나타났다. 기타 시스템은 0.4%(1개소)로 매우 제한적인 수준이었다.

의료기관 종별로 살펴보면 상급종합병원은 '부설 노인복지시설 전산시스템' 2.4%, '부설 장례식장 전산시스템' 51.2%, '부설 주차시스템' 78.0%로 나타났으며, 종합병원은 각각 2.3%, 43.2%, 55.9%로 나타나 전반적으로 상급종합병원이 높은 도입 수준을 보였다.

종합하면 의료기관의 비진료 부문 및 기타 부대사업 관련 정보화는 일부 영역에 한정되어 있으며 전반적으로 낮은 수준에 머물러 있는 것으로 나타났다.

〈표 5-25〉 의료정보시스템 도입 여부(기타 부대사업)

(단위: 개소, %)

구분	부설 노인복지시설 전산시스템			부설 장례식장 전산시스템		
	예	아니오	합계	예	아니오	합계
전체	6 (2.3%)	257 (97.7%)	263 (100%)	117 (44.5%)	146 (55.5%)	263 (100%)
상급 종합병원	1 (2.4%)	40 (97.6%)	41 (100%)	21 (51.2%)	20 (48.8%)	41 (100%)
종합병원	5 (2.3%)	217 (97.7%)	222 (100%)	96 (43.2%)	126 (56.8%)	222 (100%)
도시(동)	5 (2.0%)	243 (98%)	248 (100%)	110 (44.4%)	138 (55.6%)	248 (100%)
비도시 (읍·면)	1 (6.7%)	14 (93.3%)	15 (100%)	7 (46.7%)	8 (53.3%)	15 (100%)
구분	부설 주차장 전산시스템			기타		
	예	아니오	합계	예	아니오	합계
전체	156 (59.3%)	107 (40.7%)	263 (100%)	1 (0.4%)	262 (99.6%)	263 (100%)
상급 종합병원	32 (78.0%)	9 (22.0%)	41 (100%)	-	-	-
종합병원	124 (55.9%)	98 (44.1%)	222 (100%)	1 (0.5%)	221 (99.5%)	222 (100%)
도시(동)	146 (58.9%)	102 (41.1%)	248 (100%)	1 (0.4%)	247 (99.6%)	248 (100%)
비도시 (읍·면)	10 (66.7%)	5 (33.3%)	15 (100%)	-	-	-

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

〈표 5-26〉은 진료정보 관련 의료정보시스템의 도입형태를 SI개발과 상용제품으로 구분하여 조사한 결과를 나타낸 것이다.

전체적으로 '전자의무기록시스템'은 상용제품 57.8%, SI개발 42.2%로 나타나 절반 이상의 기관이 외부 상용 솔루션을 도입하여 운영하고 있는 것으로 나타났다. '처방전달시스템' 역시 상용제품 57.3%, SI개발 42.7%로 유사한 구조를 보였으며, '의료영상저장전송시스템'은 상용제품 89.7%로 외부 전문 솔루션 의존도가 매우 높은 것으로 나타났다. 반

면 ‘진료과 및 회송시스템’과 ‘모바일 전자의무기록시스템’은 SI개발과 상용제품이 유사한 비중으로 나타나 시스템 특성에 따라 구축 방식이 혼재된 양상을 보였다.

의료기관 종별로 살펴보면 상급종합병원은 주요 진료정보시스템을 자체 개발(SI) 방식으로 구축하는 비중이 높은 것으로 나타났다. 전자의무기록시스템, 처방전달시스템, 임상검사정보시스템, 약국관리시스템 등 핵심 시스템에서 SI개발 비율이 70% 이상으로 나타나, 기관 특성에 맞춘 맞춤형 시스템 운영이 이루어지고 있는 것으로 나타났다. 반면 의료영상저장전송시스템은 대부분 상용제품을 도입하고 있어, 표준화 및 외부 연계성이 중요한 영역에서는 상용 솔루션을 활용하는 경향이 확인되었다.

종합병원의 경우 주요 진료정보시스템은 전반적으로 상용제품 중심으로 구축되어 있는 것으로 나타났다. 전자의무기록시스템, 처방전달시스템, 의료영상저장전송시스템 등 대부분의 시스템에서 상용제품 도입 비율이 높게 나타나, 표준화된 솔루션을 활용하는 경향이 뚜렷하게 확인되었다. 다만 일부 시스템에서는 SI개발이 병행되고 있어 기관별 운영 환경에 따라 혼합형 구조가 나타나고 있었다.

종합하면 의료기관의 진료정보시스템은 전반적으로 상용제품 중심으로 구축되어 있으며, 특히 영상·검사 등 외부 연계성과 표준화가 중요한 영역일수록 상용제품 의존도가 높은 것으로 나타났다.

〈표 5-26〉 의료정보시스템 도입 형태(진료정보)

(단위: 개소, %)

구분	전자의무기록시스템(EMR)			모바일 전자의무기록시스템(EMR)		
	SI개발	상용제품	합계	SI개발	상용제품	합계
전체	111 (42.2%)	152 (57.8%)	263 (100%)	39 (50.0%)	39 (50.0%)	78 (100%)
상급 종합병원	32 (78.0%)	9 (22.0%)	41 (100%)	11 (44.0%)	14 (56.0%)	25 (100%)
종합병원	79 (35.6%)	143 (64.4%)	222 (100%)	28 (52.8%)	25 (47.2%)	53 (100%)
도시(동)	104 (41.9%)	144 (58.1%)	248 (100%)	38 (51.4%)	36 (48.6%)	74 (100%)
비도시 (읍·면)	7 (46.7%)	8 (53.3%)	15 (100%)	1 (25.0%)	3 (75.0%)	4 (100%)
구분	처방전달시스템(OCS)			의료영상저장전송시스템(PACS)		
	SI개발	상용제품	합계	SI개발	상용제품	합계
전체	111 (42.7%)	149 (57.3%)	260 (100%)	27 (10.3%)	235 (89.7%)	262 (100%)
상급 종합병원	32 (80.0%)	8 (20.0%)	40 (100%)	4 (9.8%)	37 (90.2%)	41 (100%)
종합병원	79 (35.9%)	141 (64.1%)	220 (100%)	23 (10.4%)	198 (89.6%)	221 (100%)
도시(동)	104 (42.4%)	141 (57.6%)	245 (100%)	25 (10.1%)	222 (89.9%)	247 (100%)
비도시 (읍·면)	7 (46.7%)	8 (53.3%)	15 (100%)	2 (13.3%)	13 (86.7%)	15 (100%)
구분	임상검사정보시스템(LIS)			약국관리시스템		
	SI개발	상용제품	합계	SI개발	상용제품	합계
전체	81 (45.8%)	96 (54.2%)	177 (100%)	89 (47.1%)	100 (52.9%)	189 (100%)
상급 종합병원	27 (75.0%)	9 (25.0%)	36 (100%)	27 (77.1%)	8 (22.9%)	35 (100%)
종합병원	54 (38.3%)	87 (61.7%)	141 (100%)	62 (40.3%)	92 (59.7%)	154 (100%)
도시(동)	76 (45.2%)	92 (54.8%)	168 (100%)	84 (46.9%)	95 (53.1%)	179 (100%)
비도시 (읍·면)	5 (55.6%)	4 (44.4%)	9 (100%)	5 (50.0%)	5 (50.0%)	10 (100%)

구분	진료과 및 회송 시스템(상/하/원)			진료정보교류시스템(복지부)		
	SI개발	상용제품	합계	SI개발	상용제품	합계
전체	88 (52.4%)	80 (47.6%)	168 (100%)	78 (42.6%)	105 (57.4%)	183 (100%)
상급 종합병원	31 (77.5%)	9 (22.5%)	40 (100%)	27 (69.2%)	12 (30.8%)	39 (100%)
종합병원	57 (44.5%)	71 (55.5%)	128 (100%)	51 (35.4%)	93 (64.6%)	144 (100%)
도시(동)	84 (52.8%)	75 (47.2%)	159 (100%)	74 (42.5%)	100 (57.5%)	174 (100%)
비도시 (읍·면)	4 (44.4%)	5 (55.6%)	9 (100%)	4 (44.4%)	5 (55.6%)	9 (100%)
구분	원격의료시스템			건강검진정보시스템		
	SI개발	상용제품	합계	SI개발	상용제품	합계
전체	16 (55.2%)	13 (44.8%)	29 (100%)	58 (23.3%)	191 (76.7%)	249 (100%)
상급 종합병원	6 (85.7%)	1 (14.3%)	7 (100%)	21 (56.8%)	16 (43.2%)	37 (100%)
종합병원	10 (45.5%)	12 (54.5%)	22 (100%)	37 (17.5%)	175 (82.5%)	212 (100%)
도시(동)	16 (57.1%)	12 (42.9%)	28 (100%)	55 (23.4%)	180 (76.6%)	235 (100%)
비도시 (읍·면)	0 (0.0%)	1 (100%)	1 (100%)	3 (21.4%)	11 (78.6%)	14 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

반면 상급종합병원은 자체 개발 중심의 맞춤형 시스템을 운영하는 경향이 강한 반면, 종합병원은 상용제품 중심의 표준화된 시스템을 도입하는 경향이 뚜렷하게 나타났다.

〈표 5-27〉은 환자 서비스 관련 의료정보시스템의 도입형태를 SI개발과 상용제품으로 구분하여 조사한 결과를 나타낸 것이다.

'의료기관 포털(대표 홈페이지)'은 총 응답기관(255개소) 중 SI개발 160개소(62.7%), 상용제품 95개소(37.3%)로 나타나 자체 구축 비중이 상대적으로 높게 나타났다. 반면 '의료기관 포털(웹) 기반 개인건강기록'은 총 응답기관(40개소) 중 SI개발 20개소(50.0%), 상용제품 20개소

(50.0%)로 나타나 두 방식이 동일한 수준을 보였으며, '모바일 개인건강기록'은 총 응답기관(67개소) 중SI개발 25개소(37.3%), 상용제품 42개소(62.7%)로 나타나 상용제품 중심의 도입 경향이 나타났다.

〈표 5-27〉 의료정보시스템 도입 형태(환자 서비스)

(단위: 개소, %)

구분	의료기관 포털(대표 홈페이지)			의료기관 포털(웹) 기반 개인건강기록(PHR)		
	SI개발	상용제품	합계	SI개발	상용제품	합계
전체	160 (62.7%)	95 (37.3%)	255 (100%)	20 (50.0%)	20 (50.0%)	40 (100%)
상급 종합병원	32 (80.0%)	8 (20.0%)	40 (100%)	12 (63.2%)	7 (36.8%)	19 (100%)
종합병원	128 (59.5%)	87 (40.5%)	215 (100%)	8 (38.1%)	13 (61.9%)	21 (100%)
도시(동)	148 (61.7%)	92 (38.3%)	240 (100%)	20 (51.3%)	19 (48.7%)	39 (100%)
비도시 (읍·면)	12 (80.0%)	3 (20.0%)	15 (100%)	0 (0.0%)	1 (100%)	1 (100%)
구분	모바일 개인건강기록(PHR)			여백		
	SI개발	상용제품	합계			
전체	25 (37.3%)	42 (62.7%)	67 (100%)			
상급 종합병원	14 (42.4%)	19 (57.6%)	33 (100%)			
종합병원	11 (32.4%)	23 (67.6%)	34 (100%)			
도시(동)	25 (37.9%)	41 (62.1%)	66 (100%)			
비도시 (읍·면)	0 (0.0%)	1 (100%)	1 (100%)			

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

의료기관 종별로 살펴보면 상급종합병원은 환자 서비스 관련 시스템 전반에서 SI개발 비중이 높은 것으로 나타났다. '의료기관 포털(대표 홈

페이지)'과 '웹 기반 개인건강기록' 모두 자체 개발 중심으로 구축되어 있었으며, '모바일 개인건강기록' 역시 SI개발 비중이 일정 수준 유지되면서도 상용제품 활용이 병행되는 양상이 나타났다. 반면 종합병원은 전반적으로 상용제품 중심의 도입 경향을 보였으며, 특히 개인건강기록 및 모바일 서비스 영역에서 상용제품 의존도가 높은 것으로 나타났다.

종합하면 의료기관의 환자 서비스 관련 정보시스템은 기관 고유의 웹 기반 서비스 영역에서는 자체 개발 중심으로 구축되는 경향이 나타나는 반면, 모바일 및 개인건강기록 등 확장형 서비스 영역에서는 상용제품 활용이 확대되는 이중적 구조가 나타났다. 특히 병원 규모에 따라 구축 방식의 차이가 확인되었다.

〈표 5-28〉은 진료 지원 및 경영 정보 관련 의료정보시스템의 도입형태를 SI개발과 상용제품으로 구분하여 조사한 결과를 나타낸 것이다.

'원무관리·보험청구시스템'은 총 응답기관(254개소) 중 SI개발 102개소(40.2%), 상용제품 152개소(59.8%)로 나타나 상용제품 도입 비중이 높은 것으로 나타났다. '진료지원 자원관리시스템'은 총 응답기관(183개소) 중 SI개발 61개소(33.3%), 상용제품 122개소(66.7%)로 나타나 상용제품 중심의 구축 경향이 나타났다. 반면 '내부지원시스템'은 총 응답기관(81개소) 중 SI개발 51개소(63.0%), 상용제품 30개소(37.0%)로 나타나 자체 구축형 시스템의 비중이 높았으며 '전사적 데이터웨어하우스' 또한 총 응답기관(61개소) 중 SI개발 38개소(62.3%), 상용제품 23개소(37.7%)로 나타나 SI개발 중심의 경향을 보였다.

의료기관 종별로 살펴보면 상급종합병원은 전반적으로 SI개발 비중이 높은 것으로 나타났다. 주요 시스템 대부분에서 자체 구축 형태를 통해 병원 운영 특성에 맞는 맞춤형 시스템을 운영하고 있는 것으로 나타났다. 반면 종합병원은 '원무관리·보험청구시스템'과 '자원관리시스템' 등에서

상용제품 비중이 높게 나타났으며, 일부 내부 시스템에서는 SI개발과 상용제품을 병행하는 형태를 보였다.

〈표 5-28〉 의료정보시스템 도입 형태(진료 지원 및 경영 정보)

(단위: 개소, %)

구분	원무관리, 보험청구시스템			전자적 자원관리시스템(ERP)		
	SI개발	상용제품	합계	SI개발	상용제품	합계
전체	102 (40.2%)	152 (59.8%)	254 (100%)	61 (33.3%)	122 (66.7%)	183 (100%)
상급 종합병원	29 (76.3%)	9 (23.7%)	38 (100%)	17 (68.0%)	8 (32.0%)	25 (100%)
종합병원	73 (33.8%)	143 (66.2%)	216 (100%)	44 (27.8%)	114 (72.2%)	158 (100%)
도시(동)	97 (40.6%)	142 (59.4%)	239 (100%)	57 (33.1%)	115 (66.9%)	172 (100%)
비도시 (읍·면)	5 (33.3%)	10 (66.7%)	15 (100%)	4 (36.4%)	7 (63.6%)	11 (100%)
구분	내부직원지원시스템(ESS)			전사적데이터웨어하우스(EDW)		
	SI개발	상용제품	합계	SI개발	상용제품	합계
전체	51 (63.0%)	30 (37.0%)	81 (100%)	38 (62.3%)	23 (37.7%)	61 (100%)
상급 종합병원	19 (79.2%)	5 (20.8%)	24 (100%)	17 (65.4%)	9 (34.6%)	26 (100%)
종합병원	32 (56.1%)	25 (43.9%)	57 (100%)	21 (60.0%)	14 (40.0%)	35 (100%)
도시(동)	49 (63.6%)	28 (36.4%)	77 (100%)	37 (63.8%)	21 (36.2%)	58 (100%)
비도시 (읍·면)	2 (50.0%)	2 (50.0%)	4 (100%)	1 (33.3%)	2 (66.7%)	3 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

종합하면 의료기관의 진료 지원 및 경영 정보시스템은 행정·청구 등 표준화가 용이한 영역에서는 상용제품 중심으로 구축되는 반면, 내부 자원관리 및 데이터 통합 등 핵심 운영 영역에서는 자체 개발을 통해 기능적 통합성과 운영 효율성을 확보하려는 경향이 나타났다. 또한 병원 규모에

따라 구축 방식의 차이가 확인되어 상급종합병원은 자체 개발 중심, 종합병원은 상용제품 중심의 구조가 형성되어 있는 것으로 나타났다.

〈표 5-29〉는 교육 및 연구 관련 의료정보시스템의 도입형태를 SI개발과 상용제품으로 구분하여 조사한 결과를 나타낸 것이다.

'보수교육 전산시스템'은 총 응답기관(56개소) 중 SI개발 24개소(42.9%), 상용제품 32개소(57.1%)로 상용제품 도입 비중이 다소 높게 나타났다. '조사연구 전산시스템'은 총 연구기관(40개소) 중 SI개발 24개소(60.0%), 상용제품 16개소(40.0%)로 자체 구축 중심의 경향이 나타났다.

의료기관 종별로 살펴보면 상급종합병원은 '보수교육 전산시스템'에서 SI개발과 상용제품이 유사한 수준으로 나타났으며, '조사연구 전산시스템'에서는 SI개발 비중이 높은 것으로 나타나 연구 기능 중심의 자체 구축 경향이 뚜렷하게 나타났다. 반면 종합병원은 '보수교육 전산시스템'에서 상용제품 활용 비중이 높게 나타났으며, '조사연구 전산시스템'은 SI개발과 상용제품이 유사한 수준으로 나타나 기관 여건에 따라 혼합형 구조를 보였다.

종합하면 의료기관의 교육 및 연구 관련 정보시스템은 업무 성격에 따라 도입 형태가 구분되는 것으로 나타났다. 교육 영역은 운영 효율성과 표준화 측면에서 상용제품 활용이 상대적으로 높은 반면, 연구 영역은 맞춤형 기능과 데이터 관리 필요성으로 인해 자체 개발 비중이 높은 것으로 나타났다. 특히 상급종합병원은 연구 기능 강화를 위해 자체 개발 중심의 시스템을 운영하는 반면, 종합병원은 교육 영역에서는 상용제품을 활용하고 연구 영역에서는 제한적으로 자체 구축을 병행하는 구조를 보이고 있어, 기관 규모에 따른 정보화 전략 차이가 존재하는 것으로 나타났다.

〈표 5-29〉 의료정보시스템 도입 형태(교육 및 연구)

(단위: 개소, %)

구분	보수교육 전산시스템			조사연구 전산시스템		
	SI개발	상용제품	합계	SI개발	상용제품	합계
전체	24 (42.9%)	32 (57.1%)	56 (100%)	24 (60.0%)	16 (40.0%)	40 (100%)
상급 종합병원	10 (47.6%)	11 (52.4%)	21 (100%)	13 (68.4%)	6 (31.6%)	19 (100%)
종합병원	14 (40.0%)	21 (60.0%)	35 (100%)	11 (52.4%)	10 (47.6%)	21 (100%)
도시(동)	23 (42.6%)	31 (57.4%)	54 (100%)	23 (59.0%)	16 (41.0%)	39 (100%)
비도시 (읍·면)	1 (50.0%)	1 (50.0%)	2 (100%)	1 (100%)	0 (0.0%)	1 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

〈표 5-30〉은 기타 부대사업 관련 의료정보시스템의 도입형태를 SI개발과 상용제품으로 구분하여 조사한 결과를 나타낸 것이다.

'부설 노인복지시설 전산시스템'을 도입한 6개소 중 SI개발 1개소(16.7%), 상용제품 5개소(83.3%)로 상용제품 중심으로 운영되고 있는 것으로 나타났다. '부설 장례식장 전산시스템'을 도입한 117개소 중 SI개발 37개소(31.6%), 상용제품 80개소(68.4%)로 상용제품 비중이 높은 것으로 나타났다. '부설 주차장 전산시스템'을 도입한 156개소 중 SI개발 12개소(7.7%), 상용제품 144개소(92.3%)로 대부분이 상용제품을 도입한 것으로 나타났다. '기타 시스템'은 전체 1개소로 1개소(100.0%) 모두 상용제품을 도입한 것으로 나타났다.

의료기관 종별로 살펴보면 상급종합병원은 일부 시스템에서 SI개발과 상용제품을 병행하는 경향을 보였으며, 특히 장례식장 전산시스템은 두 방식이 유사한 수준으로 나타났다. 반면 종합병원은 대부분의 부대사업 시스템에서 상용제품 중심의 구축 구조가 뚜렷하게 나타났다.

종합하면 의료기관의 부대사업 관련 정보시스템은 외부 서비스와의 연계 및 운영 표준화가 요구되는 특성으로 인해 상용제품 의존도가 높은 것으로 나타났다. 또한 병원 규모에 따라 구축 방식의 차이가 일부 존재하나, 전반적으로는 상용제품 중심의 구조가 형성되어 있는 것으로 확인되었다.

〈표 5-30〉 의료정보시스템 도입 형태(기타 부대사업)

(단위: 개소, %)

구분	부설 노인복지시설 전산시스템			부설 장례식장 전산시스템		
	SI개발	상용제품	합계	SI개발	상용제품	합계
전체	1 (16.7%)	5 (83.3%)	6 (100%)	37 (31.6%)	80 (68.4%)	117 (100%)
상급 종합병원	0 (0.0%)	1 (100%)	1 (100%)	10 (47.6%)	11 (52.4%)	21 (100%)
종합병원	1 (20.0%)	4 (80.0%)	5 (100%)	27 (28.1%)	69 (71.9%)	96 (100%)
도시(동)	1 (20.0%)	4 (80.0%)	5 (100%)	34 (30.9%)	76 (69.1%)	110 (100%)
비도시 (읍·면)	0 (0.0%)	1 (100%)	1 (100%)	3 (42.9%)	4 (57.1%)	7 (100%)
구분	부설 주차장 전산시스템			기타		
	SI개발	상용제품	합계	SI개발	상용제품	합계
전체	12 (7.7%)	144 (92.3%)	156 (100%)	0 (0.0%)	1 (100%)	1 (100%)
상급 종합병원	6 (18.8%)	26 (81.2%)	32 (100%)	-	-	-
종합병원	6 (4.8%)	118 (95.2%)	124 (100%)	0 (0.0%)	1 (100%)	1 (100%)
도시(동)	12 (8.2%)	134 (91.8%)	146 (100%)	0 (0.0%)	1 (100%)	1 (100%)
비도시 (읍·면)	0 (0.0%)	10 (100%)	10 (100%)	-	-	-

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

〈표 5-31〉은 진료정보 관련 의료정보시스템의 유지보수 형태를 자체, 위탁, 자체+위탁으로 구분하여 조사한 결과를 나타낸 것이다.

전체적으로 볼 때, 의료정보시스템의 유지보수 형태는 위탁 중심으로 운영되고 있는 것으로 나타났다.

'전자의무기록시스템'은 총 응답기관(263개소) 중 자체 50개소(19.0%), 위탁 148개소(56.3%), 자체+위탁 65개소(24.7%)로 나타났으며, '모바일 전자의무기록시스템'은 총 응답기관(78개소) 중 자체 12개소(15.4%), 위탁 44개소(56.4%), 자체+위탁 22개소(28.2%)로 나타났고, '처방전달시스템'은 총 응답기관(260개소) 중 자체 54개소(20.8%), 위탁 143개소(55.0%), 자체+위탁 63개소(24.2%)로 나타나 절반 이상의 의료기관이 위탁 형태 운영하고 있었다.

'의료영상시스템'은 총 응답기관(262개소) 중 자체 7개소(2.7%), 위탁 202개소(77.1%), 자체+위탁 63개소(20.2%)로 위탁 형태 운영하는 것으로 나타나 의료기관의 위탁 형태 운영 비중이 매우 높았다. '임상검사정보시스템'은 총 응답기관(177개소) 중 자체 38개소(21.5%), 위탁 92개소(52.0%), 자체+위탁 47개소(26.6%)로 나타났으며, '약국관리시스템'은 총 응답기관(189개소) 중 자체 44개소(23.34%), 위탁 100개소(52.9%), 자체+위탁 45개소(23.8%)로 나타나 절반 이상의 의료기관이 위탁 형태 운영하고 있었다.

'진료과 회송 시스템'은 총 응답기관(168개소) 중 자체 44개소(26.2%), 위탁 81개소(48.2%), 자체+위탁 43개소(25.6%)로 나타나 절반에 가까운 의료기관이 위탁 형태로 운영하고 있었으나 타 정보시스템에 비해 위탁운영 비중은 다소 낮은 것으로 나타났다.

'진료정교류시스템'은 총 응답기관(183개소) 중 자체 36개소(19.7%), 위탁 108개소(59.0%), 자체+위탁 39개소(21.3%)로 나타났으며, '원격

의료시스템'은 총 응답기관(29개소) 중 자체 7개소(24.1%), 위탁 15개소(51.7%), 자체+위탁 7개소(24.1%)로 절반 이상의 의료기관이 위탁 형태 운영하고 있었고, '건강점진정보시스템'은 총 응답기관(249개소) 중 자체 26개소(10.4%), 위탁 183개소(73.5%), 자체+위탁 40개소(16.1%)로 나타나 의료기관의 위탁 형태 운영 비중이 매우 높게 나타났다.

상급종합병원은 종합병원에 비해 진료정보 관련 의료정보시스템의 유지보수 형태 중 자체 비중이 좀더 높은 경향을 보이고 있으나 대부분의 의료정보시스템에서 위탁이 절반을 상회하는 수준으로 나타났다. 구체적으로 상급종합병원의 경우 대부분의 진료정보 관련 의료정보시스템의 유지보수 형태에서 위탁 비중이 가장 높게 나타났으나. '전자의무기록시스템', '처방전달시스템' 등 일부 의료정보시스템의 유지 보수 형태에서는 자체 비중이 가장 높게 나타났다. 반면 종합병원의 경우, 전반적으로 의료정보시스템의 유지보수 형태에서 위탁 비중이 가장 높게 나타났다.

종합하면 의료기관의 진료정보 관련 정보시스템 유지보수는 전반적으로 위탁 중심 구조가 형성되어 있으며, 자체 운영 역량보다는 외부 전문업체에 대한 의존도가 높은 것으로 나타났다. 특히 병원 규모에 따라 유지보수 방식의 차이가 일부 존재하나, 전체적으로 위탁 중심 운영이 일반화되어 있어 내부 보안관리 역량 강화와 외부 위탁 관리체계의 체계화가 필요한 것으로 나타났다.

〈표 5-31〉 의료정보시스템 유지보수 형태(진료정보)

(단위: 개소, %)

구분	전자의무기록시스템(EMR)				모바일 전자의무기록시스템(EMR)			
	자체	위탁	자체+위탁	합계	자체	위탁	자체+위탁	합계
전체	50 (19.0%)	148 (56.3%)	65 (24.7%)	263 (100%)	12 (15.4%)	44 (56.4%)	22 (28.2%)	78 (100%)
상급 종합병원	17 (41.5%)	10 (24.4%)	14 (34.1%)	41 (100%)	5 (20.0%)	13 (52.0%)	7 (28.0%)	25 (100%)
종합병원	33 (14.9%)	138 (62.2%)	51 (23%)	222 (100%)	7 (13.2%)	31 (58.5%)	15 (28.3%)	53 (100%)
도시 (동)	48 (19.4%)	140 (56.5%)	60 (24.2%)	248 (100%)	12 (16.2%)	41 (55.4%)	21 (28.4%)	74 (100%)
비도시 (읍·면)	2 (13.3%)	8 (53.3%)	5 (33.3%)	15 (100%)	0 (0.0%)	3 (75.0%)	1 (25.0%)	4 (100%)
구분	처방전달시스템(OCS)				의료영상저장전송시스템(PACS)			
	자체	위탁	자체+위탁	합계	자체	위탁	자체+위탁	합계
전체	54 (20.8%)	143 (55.0%)	63 (24.2%)	260 (100%)	7 (2.7%)	202 (77.1%)	53 (20.2%)	262 (100%)
상급 종합병원	18 (45%)	10 (25%)	12 (30%)	40 (100%)	3 (7.3%)	27 (65.9%)	11 (26.8%)	41 (100%)
종합병원	36 (16.4%)	133 (60.5%)	51 (23.2%)	220 (100%)	4 (1.8%)	175 (79.2%)	42 (19.0%)	221 (100%)
도시 (동)	52 (21.2%)	135 (55.1%)	58 (23.7%)	245 (100%)	6 (2.4%)	192 (77.7%)	49 (19.8%)	247 (100%)
비도시 (읍·면)	2 (13.3%)	8 (53.3%)	5 (33.3%)	15 (100%)	1 (6.7%)	10 (66.7%)	4 (26.7%)	15 (100%)
구분	임상검사정보시스템(LIS)				약국관리시스템			
	자체	위탁	자체+위탁	합계	자체	위탁	자체+위탁	합계
전체	38 (21.5%)	92 (52.0%)	47 (26.6%)	177 (100%)	44 (23.3%)	100 (52.9%)	45 (23.8%)	189 (100%)
상급 종합병원	12 (33.3%)	12 (33.3%)	12 (33.3%)	36 (100%)	13 (37.1%)	11 (31.4%)	11 (31.4%)	35 (100%)
종합병원	26 (18.4%)	80 (56.7%)	35 (24.8%)	141 (100%)	31 (20.1%)	89 (57.8%)	34 (22.1%)	154 (100%)
도시 (동)	36 (21.4%)	87 (51.8%)	45 (26.8%)	168 (100%)	42 (23.5%)	95 (53.1%)	42 (23.5%)	179 (100%)
비도시 (읍·면)	2 (22.2%)	5 (55.6%)	2 (22.2%)	9 (100%)	2 (20%)	5 (50%)	3 (30%)	10 (100%)

구분	진료과 및 회송 시스템(상/하/원)				진료정보교류시스템(복지부)			
	자체	위탁	자체+위탁	합계	자체	위탁	자체+위탁	합계
전체	44 (26.2%)	81 (48.2%)	43 (25.6%)	168 (100%)	36 (19.7%)	108 (59.0%)	39 (21.3%)	183 (100%)
상급 종합병원	17 (42.5%)	12 (30.0%)	11 (27.5%)	40 (100%)	18 (46.2%)	13 (33.3%)	8 (20.5%)	39 (100%)
종합병원	27 (21.1%)	69 (53.9%)	32 (25.0%)	128 (100%)	18 (12.5%)	95 (66%)	31 (21.5%)	144 (100%)
도시 (동)	43 (27.0%)	74 (46.5%)	42 (26.4%)	159 (100%)	34 (19.5%)	101 (58%)	39 (22.4%)	174 (100%)
비도시 (읍·면)	1 (11.1%)	7 (77.8%)	1 (11.1%)	9 (100%)	2 (22.2%)	7 (77.8%)	0 (0.0%)	9 (100%)
구분	원격의료시스템				건강검진정보시스템			
	자체	위탁	자체+위탁	합계	자체	위탁	자체+위탁	합계
전체	7 (24.1%)	15 (51.7%)	7 (24.1%)	29 (100%)	26 (10.4%)	183 (73.5%)	40 (16.1%)	249 (100%)
상급 종합병원	2 (28.6%)	4 (57.1%)	1 (14.3%)	7 (100%)	12 (32.4%)	15 (40.5%)	10 (27.0%)	37 (100%)
종합병원	5 (22.7%)	11 (50.0%)	6 (27.3%)	22 (100%)	14 (6.6%)	168 (79.2%)	30 (14.2%)	212 (100%)
도시 (동)	7 (25.0%)	14 (50.0%)	7 (25.0%)	28 (100%)	24 (10.2%)	172 (73.2%)	39 (16.6%)	235 (100%)
비도시 (읍·면)	0 (0.0%)	1 (100%)	0 (0.0%)	1 (100%)	2 (14.3%)	11 (78.6%)	1 (7.1%)	14 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

〈표 5-32〉는 환자 서비스 관련 의료정보시스템의 유지보수 형태를 자체, 위탁, 자체+위탁으로 구분하여 조사한 결과를 나타낸 것이다.

전체적으로 환자 서비스 관련 시스템 역시 위탁 중심으로 운영되고 있는 것으로 나타났다. '의료기관 포털'은 총 응답기관(255개소) 중 자체 25개소(9.8%), 위탁 180개소(70.6%), 자체+위탁 50개소(19.6%)로 나타났으며, '모바일 개인건강기록'은 총 응답기관(67개소) 중 자체 7개소(10.4%), 위탁 41개소(61.2%), 자체+위탁 19개소(28.4%)로 나타나 의료기관의 위탁 형태 운영 비중이 상당히 높은 것으로 나타났다.

‘의료기관 포털(웹) 기반 개인건강기록’은 총 응답기관(40개소) 중 자체 5개소(12.5%), 위탁 20개소(50.0%), 자체+위탁 15개소(37.5%)로 나타나 의료기관의 위탁 형태 운영 비중이 절반 수준으로 나타났다.

〈표 5-32〉 의료정보시스템 유지보수 형태(환자 서비스)

(단위: 개소, %)

구분	의료기관 포털(대표 홈페이지)				의료기관 포털(웹) 기반 개인건강기록(PHR)			
	자체	위탁	자체+위탁	합계	자체	위탁	자체+위탁	합계
전체	25 (9.8%)	180 (70.6%)	50 (19.6%)	255 (100%)	5 (12.5%)	20 (50.0%)	15 (37.5%)	40 (100%)
상급 종합병원	3 (7.5%)	24 (60%)	13 (32.5%)	40 (100%)	1 (5.3%)	10 (52.6%)	8 (42.1%)	19 (100%)
종합병원	22 (10.2%)	156 (72.6%)	37 (17.2%)	215 (100%)	4 (19.0%)	10 (47.6%)	7 (33.3%)	21 (100%)
도시(동)	24 (10%)	170 (70.8%)	46 (19.2%)	240 (100%)	5 (12.8%)	19 (48.7%)	15 (38.5%)	39 (100%)
비도시 (읍·면)	1 (6.7%)	10 (66.7%)	4 26.7%)	15 (100%)	0 (0%)	1 (100%)	0 (0%)	1 (100%)
구분	모바일 개인건강기록(PHR)				여백			
	자체	위탁	자체+위탁	합계				
전체	7 (10.4%)	41 (61.2%)	19 (28.4%)	67 (100%)				
상급 종합병원	3 (9.1%)	20 (60.6%)	10 (30.3%)	33 (100%)				
종합병원	4 (11.8%)	21 (61.8%)	9 (26.5%)	34 (100%)				
도시(동)	7 (10.6%)	40 (60.6%)	19 (28.8%)	66 (100%)				
비도시 (읍·면)	0 (0.0%)	1 (100%)	0 (0%)	1 (100%)				

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

종합하면 의료기관의 환자 서비스 관련 정보시스템 유지보수 역시 위탁 중심으로 운영되고 있으며, 일부 시스템에서 자체 또는 혼합형 운영이 이루어지고 있으나 전반적으로 외부 위탁 의존도가 높은 구조가 형성되어

있는 것으로 나타났다. 이에 따라 유지보수 과정에서의 보안관리 강화와 외부 위탁업체에 대한 관리·통제 체계 마련이 필요한 것으로 나타났다.

〈표 5-33〉은 진료 지원 및 경영 정보시스템의 유지보수 형태를 자체, 위탁, 자체+위탁으로 구분하여 조사한 결과를 나타낸 것이다.

'원무관리·보험청구시스템'은 총 응답기관(254개소) 중 자체 52개소(20.5%), 위탁 152개소(59.8%), 자체+위탁 50개소(19.7%)로 나타났으며, '전자적 자원관리시스템'은 총 응답기관(183개소) 중 자체 33개소(18.0%), 위탁 119개소(65.0%), 자체+위탁 31개소(16.9%)로 나타나 유지보수 형태가 절반 이상 위탁으로 운영되고 있는 것으로 나타났다.

반면 '내부직원지원시스템'은 총 응답기관(81개소) 중 자체 27개소(33.3%), 위탁 33개소(40.7%), 자체+위탁 21개소(25.9%)로 나타나 위탁 비중이 다소 높은 수준으로 나타났으며, '전사적 데이터웨어하우스'는 총 응답기관(61개소) 중 자체 15개소(24.6%), 위탁 20개소(32.8%), 자체+위탁 26개소(42.6%)로 나타나 자체+위탁 형태의 유지보수가 가장 높은 비중을 보였다.

의료기관 종별로 살펴보면 상급종합병원의 경우 '원무관리·보험청구시스템'은 자체 15개소(39.5%), 위탁 13개소(34.2%), 자체+위탁 10개소(26.3%)로 자체 비중이 다소 높게 나타났으며, '전자적 자원관리시스템'은 자체 8개소(32.0%), 위탁 6개소(24.0%), 자체+위탁 11개소(44.0%)로 자체+위탁 형태가 다소 높은 것으로 나타났다. '내부직원지원시스템'은 자체 8개소(33.3%), 위탁 7개소(29.2%), 자체+위탁 9개소(37.5%)로 나타났으며, '전사적 데이터웨어하우스'는 자체 6개소(23.1%), 위탁 7개소(26.9%), 자체+위탁 13개소(50.0%)로 자체+위탁 중심으로 운영되고 있었다.

한편 종합병원의 경우 '원무관리·보험청구시스템' 139개소(64.4%),

‘전자적 자원관리시스템’ 113개소(71.5%), ‘내부직원지원시스템’ 26개소(45.6%), ‘전사적 데이터웨어하우스’ 13개소(37.1%)의 유지보수 형태가 위탁으로 나타나 전반적으로 위탁 중심으로 운영되고 있었다.

〈표 5-33〉 의료정보시스템 유지보수 형태(진료 지원 및 경영 정보)

(단위: 개소, %)

구분	원무관리, 보험청구시스템				전자적 자원관리시스템(ERP)			
	자체	위탁	자체+위탁	합계	자체	위탁	자체+위탁	합계
전체	52 (20.5%)	152 (59.8%)	50 (19.7%)	254 (100%)	33 (18.0%)	119 (65.0%)	31 (16.9%)	183 (100%)
상급 종합병원	15 (39.5%)	13 (34.2%)	10 (26.3%)	38 (100%)	8 (32.0%)	6 (24.0%)	11 (44.0%)	25 (100%)
종합병원	37 (17.1%)	139 (64.4%)	40 (18.5%)	216 (100%)	25 (15.8%)	113 (71.5%)	20 (12.7%)	158 (100%)
도시(동)	49 (20.5%)	143 (59.8%)	47 (19.7%)	239 (100%)	30 (17.4%)	111 (64.5%)	31 (18%)	172 (100%)
비도시 (읍·면)	3 (20.0%)	9 (60.0%)	3 (20.0%)	15 (100%)	3 (27.3%)	8 (72.7%)	0 (0.0%)	11 (100%)
구분	내부직원지원시스템(ESS)				전사적데이터웨어하우스(EDW)			
	자체	위탁	자체+위탁	합계	자체	위탁	자체+위탁	합계
전체	27 (33.3%)	33 (40.7%)	21 (25.9%)	81 (100%)	15 (24.6%)	20 (32.8%)	26 (42.6%)	61 (100%)
상급 종합병원	8 (33.3%)	7 (29.2%)	9 (37.5%)	24 (100%)	6 (23.1%)	7 (26.9%)	13 (50.0%)	26 (100%)
종합병원	19 (33.3%)	26 (45.6%)	12 (21.1%)	57 (100%)	9 (25.7%)	13 (37.1%)	13 (37.1%)	35 (100%)
도시(동)	25 (32.5%)	32 (41.6%)	20 (26.0%)	77 (100%)	14 (24.1%)	19 (32.8%)	25 (43.1%)	58 (100%)
비도시 (읍·면)	2 (50.0%)	1 (25.0%)	1 (25.0%)	4 (100%)	1 (33.3%)	1 (33.3%)	1 (33.3%)	3 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

종합하면 진료 지원 및 경영 정보시스템의 유지보수는 업무 특성과 시스템 중요도에 따라 위탁과 자체 운영이 혼합된 구조를 보이고 있으나, 전반적으로는 위탁 중심의 운영이 우세한 것으로 나타났다. 특히 상급종

합병원은 자체 운영 역량을 일부 보유하고 있는 반면, 종합병원은 외부 위탁 의존도가 높은 구조를 보이고 있어 기관 간 유지보수 역량의 차이가 존재하는 것으로 나타났다. 이에 따라 내부 운영 역량 강화와 함께 외부 위탁 관리체계의 체계적 운영이 필요한 것으로 나타났다.

〈표 5-34〉는 교육 및 연구 관련 의료정보시스템의 유지보수 형태를 자체, 위탁, 자체+위탁으로 구분하여 조사한 결과를 나타낸 것이다.

'보수교육 전산시스템'은 총 응답기관(56개소) 중 자체 13개소(23.2%), 위탁 35개소(62.5%), 자체+위탁 8개소(14.3%)로 나타났으며, '조사연구 전산시스템'은 총 응답기관 (40개소) 중 자체 9개소(22.5%), 위탁 24개소(60.0%), 자체+위탁 7개소(17.5%)로 나타나 유지보수 형태는 절반 이상 위탁으로 운영되고 있는 것으로 나타났다.

의료기관 종별로 살펴보면 상급종합병원의 경우 '보수교육 전산시스템'은 자체 4개소(19.0%), 위탁 15개소(71.4%), 자체+위탁 2개소(9.5%)로 나타났으며, '조사연구 전산시스템'은 자체 4개소(21.1%), 위탁 12개소(63.2%), 자체+위탁 3개소(15.8%)로 나타났다.

한편 종합병원의 경우 '보수교육 전산시스템'은 자체 9개소(25.7%), 위탁 20개소(57.1%), 자체+위탁 6개소(17.1%)로 나타났으며, '조사연구 전산시스템'은 자체 5개소(23.8%), 위탁 12개소(57.1%), 자체+위탁 4개소(19.0%)로 나타났다. 유지보수 형태는 절반 이상 위탁으로 운영되고 있는 것으로 나타났다.

종합하면 교육 및 연구 관련 정보시스템의 유지보수는 기관 유형에 관계없이 위탁 중심으로 운영되고 있으며, 자체 운영보다는 외부 전문업체에 대한 의존도가 높은 구조가 형성되어 있는 것으로 나타났다. 이에 따라 교육·연구 시스템의 안정적 운영을 위해 외부 위탁 관리체계 강화와 함께 내부 관리 역량 보완이 필요한 것으로 나타났다.

〈표 5-34〉 의료정보시스템 유지보수 형태(교육 및 연구)

(단위: 개소, %)

구분	보수교육 전산시스템				조사연구 전산시스템			
	자체	위탁	자체+위탁	합계	자체	위탁	자체+위탁	합계
전체	13 (23.2%)	35 (62.5%)	8 (14.3%)	56 (100%)	9 (22.5%)	24 (60.0%)	7 (17.5%)	40 (100%)
상급 종합병원	4 (19%)	15 (71.4%)	2 (9.5%)	21 (100%)	4 (21.1%)	12 (63.2%)	3 (15.8%)	19 (100%)
종합병원	9 (25.7%)	20 (57.1%)	6 (17.1%)	35 (100%)	5 (23.8%)	12 (57.1%)	4 (19.0%)	21 (100%)
도시(동)	12 (22.2%)	34 (63.0%)	8 (14.8%)	54 (100%)	8 (20.5%)	24 (61.5%)	7 (17.9%)	39 (100%)
비도시 (읍·면)	1 (50.0%)	1 (50.0%)	0 (0.0%)	2 (100%)	1 (100%)	0 (0.0%)	0 (0.0%)	1 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

〈표 5-35〉는 기타 부대사업 관련 의료정보시스템의 유지보수 형태를 자체, 위탁, 자체+위탁으로 구분하여 조사한 결과를 나타낸 것이다.

'부설 노인복지시설 전산시스템'은 총 응답기관(6개소) 중 자체 1개소(16.7%), 위탁 5개소(83.3%)로 나타났다. '부설 장례식장 전산시스템'은 총 응답기관(117개소) 중 자체 15개소(12.8%), 위탁 88개소(75.2%), 자체+위탁 14개소(12.0%)로 나타나 유지보수 형태는 대부분 위탁으로 운영되고 있는 것으로 나타났다. 또한 '부설 주차장 전산시스템'은 총 응답기관(156개소) 중 자체 5개소(3.2%), 위탁 136개소(87.2%), 자체+위탁 15개소(9.6%)로 나타나 대부분의 경우 위탁으로 운영되고 있는 것으로 나타났다.

의료기관 종별로 살펴보면, 상급종합병원 뿐만 아니라 종합병원도 '부설 노인보기시설 전산시스템', '부설 장례장식장 전산시스템', '부설 주차장 시스템' 유지보수 형태가 대부분 위탁으로 운영하고 있는 것으로 나타났다.나타났다.

〈표 5-35〉 의료정보시스템 유지보수 형태(기타 부대사업)

(단위: 개소, %)

구분	부설 노인복지시설 전산시스템				부설 장례식장 전산시스템			
	자체	위탁	자체+위탁	합계	자체	위탁	자체+위탁	합계
전체	0 (0.0%)	5 (83.3%)	1 (16.7)	6 (100%)	15 (12.8%)	88 (75.2%)	14 (12.0%)	117 (100%)
상급 종합병원	0 (0.0%)	1 (100%)	0 (0.0%)	1 (100%)	5 (23.8%)	13 (61.9%)	3 (14.3%)	21 (100%)
종합병원	0 (0.0%)	4 (80.0%)	1 (20.0%)	5 (100%)	10 (10.4%)	75 (78.1%)	11 (11.5%)	96 (100%)
도시(동)	0 (0.0%)	4 (80.0%)	1 (20.0%)	5 (100%)	14 (12.7%)	82 (74.5%)	14 (12.7%)	110 (100%)
비도시 (읍·면)	0 (0.0%)	1 (100%)	0 (0.0%)	1 (100%)	1 (14.3%)	6 (85.7%)	0 (0.0%)	7 (100%)
구분	부설 주차장 전산시스템				기타			
	자체	위탁	자체+위탁	합계	자체	위탁	자체+위탁	합계
전체	5 (3.2%)	136 (87.2%)	15 (9.6%)	156 (100%)	0 (0.0%)	1 (100%)	0 (0.0%)	1 (100%)
상급 종합병원	2 (6.2%)	26 (81.2%)	4 (12.5%)	32 (100%)	-	-	-	-
종합병원	3 (2.4%)	110 (88.7%)	11 (8.9%)	124 (100%)	0 (0.0%)	1 (100%)	0 (0.0%)	1 (100%)
도시(동)	5 (3.4%)	127 (87%)	14 (9.6%)	146 (100%)	0 (0.0%)	1 (100%)	0 (0.0%)	1 (100%)
비도시 (읍·면)	0 (0.0%)	9 (90.0%)	1 (10.0%)	10 (100%)	-	-	-	-

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

종합하면 기타 부대사업 관련 의료정보시스템의 유지보수는 대부분 외부 위탁에 의존하고 있으며, 이는 다른 의료정보시스템에 비해 위탁 비중이 더욱 높은 특징을 보인다. 이러한 결과는 부대사업 영역의 경우 표준화된 상용 솔루션 활용과 외부 전문업체 의존도가 높은 구조가 형성되어 있었다.

〈표 5-36〉은 진료정보 관련 의료정보시스템 솔루션 유지보수 여부를 조사한 결과를 나타낸 것이다.

‘전자의무기록시스템(EMR)’은 총 응답기관(263개소) 중 244개소(92.8%)에서 유지보수를 실시하고 있어 대부분의 기관이 핵심 진료정보시스템에 대한 지속적인 관리 체계를 갖추고 있는 것으로 나타났다. ‘모바일 전자의무기록시스템’은 총 응답기관(78개소) 중 71개소(91.0%)에서 유지보수가 이루어지고 있어 높은 수준을 보였다.

‘처방전달시스템(OCS)’은 총 응답기관(260개소) 중 237개소(91.2%), ‘의료영상저장전송시스템(PACS)’은 총 응답기관(262개소) 중 258개소(98.5%)에서 유지보수가 이루어지고 있어 핵심 진료지원 시스템에 대한 관리 수준은 전반적으로 매우 높은 것으로 나타났다. ‘임상검사정보시스템(LIS)’응 총 응답기관(177개소) 중 159개소(89.8%), ‘약국관리시스템’은 총 응답기관(189개소) 중 170개소(89.9%)로 나타나 대부분의 기관에서 유지보수를 수행하고 있는 것으로 나타났다.

또한 ‘진료과 및 회송시스템’은 총 응답기관(168개소) 중139개소(82.7%), ‘진료정보교류시스템’은 총 응답기관(183개소) 중 152개소(83.1%)에서 유지보수가 이루어지고 있었으며 ‘건강검진정보시스템’은 총 응답기관(249개소) 중 235개소(94.4%)로 높은 수준을 보였다. 반면 ‘원격의료시스템’은 총 응답기관(29개소) 중 21개소(72.4%)로 상대적으로 낮은 유지보수 수준을 나타냈다.

의료기관 종별로 살펴보면 상급종합병원은 일부 시스템을 제외하고 전반적으로 높은 유지보수 수준을 보였다. ‘전자의무기록시스템’은 80.5%(33개소), ‘처방전달시스템’은 75.0%(30개소), ‘의료영상저장전송시스템’은 95.1%(39개소)로 나타났으며 ‘임상검사정보시스템’과 ‘약국관리시스템’은 각각 80.6%(29개소), 74.3%(26개소)로 나타났다. 또한 ‘진료과 및 회송시스템’은 77.5%(31개소), ‘진료정보교류시스템’은 69.2%(27개소)로 나타났다. ‘건강검진정보시스템’은 83.8%(31개소)로 비교적 높은 수준이었으나 ‘원격의료시스템’은 71.4%(5개소)로 낮은 수준을 보였다.

〈표 5-36〉 의료정보시스템 솔루션 유지보수 여부(진료정보)

(단위: 개소, %)

구분	전자의무기록시스템(EMR)			모바일 전자의무기록시스템(EMR)		
	예	아니오	합계	예	아니오	합계
전체	244 (92.8%)	19 (7.2%)	263 (100%)	71 (91.0%)	7 (9.0%)	78 (100%)
상급 종합병원	33 (80.5%)	8 (19.5%)	41 (100%)	21 (84.0%)	4 (16.0%)	25 (100%)
종합병원	211 (95.0%)	11 (5.0%)	222 (100%)	50 (94.3%)	3 (5.7%)	53 (100%)
도시(동)	230 (92.7%)	18 (7.3%)	248 (100%)	67 (90.5%)	7 (9.5%)	74 (100%)
비도시 (읍·면)	14 (93.3%)	1 (6.7%)	15 (100%)	4 (100%)	0 (0.0%)	4 (100%)
구분	처방전달시스템(OCS)			의료영상저장전송시스템(PACS)		
	예	아니오	합계	예	아니오	합계
전체	237 (91.2%)	23 (8.8%)	260 (100%)	258 (98.5%)	4 (1.5%)	262 (100%)
상급 종합병원	30 (75%)	10 (25.0%)	40 (100%)	39 (95.1%)	2 (4.9%)	41 (100%)
종합병원	207 (94.1%)	13 (5.9%)	220 (100%)	219 (99.1%)	2 (0.9%)	221 (100%)
도시(동)	223 (91%)	22 (9.0%)	245 (100%)	243 (98.4%)	4 (1.6%)	247 (100%)
비도시 (읍·면)	14 (93.3%)	1 (6.7%)	15 (100%)	15 (100%)	0 (0.0%)	15 (100%)
구분	임상검사정보시스템(LIS)			약국관리시스템		
	예	아니오	합계	예	아니오	합계
전체	159 (89.8%)	18 (10.2%)	177 (100%)	170 (89.9%)	19 (10.1%)	189 (100%)
상급 종합병원	29 (80.6%)	7 (19.4%)	36 (100%)	26 (74.3%)	9 (25.7%)	35 (100%)
종합병원	130 (92.2%)	11 (7.8%)	141 (100%)	144 (93.5%)	10 (6.5%)	154 (100%)
도시(동)	151 (89.9%)	17 (10.1%)	168 (100%)	160 (89.4%)	19 (10.6%)	179 (100%)
비도시 (읍·면)	8 (88.9%)	1 (11.1%)	9 (100%)	10 (100%)	0 (0.0%)	10 (100%)

구분	진료과 및 회송 시스템(상/하/원)			진료정보교류시스템(복지부)		
	예	아니오	합계	예	아니오	합계
전체	139 (82.7%)	29 (17.3%)	168 (100%)	152 (83.1%)	31 (16.9%)	183 (100%)
상급 종합병원	31 (77.5%)	9 (22.5%)	40 (100%)	27 (69.2%)	12 (30.8%)	39 (100%)
종합병원	108 (84.4%)	20 (15.6%)	128 (100%)	125 (86.8%)	19 (13.2%)	144 (100%)
도시(동)	130 (81.8%)	29 (18.2%)	159 (100%)	143 (82.2%)	31 (17.8%)	174 (100%)
비도시 (읍·면)	9 (100%)	0 (0.0%)	9 (100%)	9 (100%)	0 (0.0%)	9 (100%)
구분	원격의료시스템			건강검진정보시스템		
	예	아니오	합계	예	아니오	합계
전체	21 (72.4%)	8 (27.6%)	29 (100%)	235 (94.4%)	14 (5.6%)	249 (100%)
상급 종합병원	5 (71.4%)	2 (28.6%)	7 (100%)	31 (83.8%)	6 (16.2%)	37 (100%)
종합병원	16 (72.7%)	6 (27.3%)	22 (100%)	204 (96.2%)	8 (3.8%)	212 (100%)
도시(동)	20 (71.4%)	8 (28.6%)	28 (100%)	221 (94.0%)	14 (6.0%)	235 (100%)
비도시 (읍·면)	1 (100%)	0 (0.0%)	1 (100%)	14 (100%)	0 (0.0%)	14 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

반면 종합병원의 경우 '전자의무기록시스템'은 95.0%(211개소), '처방전달시스템'은 94.1%(207개소), '의료영상저장전송시스템'은 99.1%(219개소)로 대부분의 기관에서 유지보수가 이루어지고 있었다. '임상검사정보시스템'과 '약국관리시스템'은 각각 92.2%(130개소), 93.5%(144개소)로 나타났으며 '진료과 및 회송시스템'과 '진료정보교류시스템'도 각각 84.4%(108개소), 86.8%(125개소)로 비교적 높은 수준을 보였다. '건강검진정보시스템'은 96.2%(204개소)로 높은 수준을 유지하고 있었으며 '원격의료시스템'은 72.7%(16개소)로 상대적으로 낮은 수준이었다.

종합하면 전자의무기록시스템, 처방전달시스템, 의료영상저장전송시스템 등 핵심 진료정보시스템은 대부분의 의료기관에서 유지보수가 이루어지고 있어 안정적인 운영 기반이 전반적으로 확보된 것으로 나타났다. 또한 임상검사, 약국관리, 건강검진 등 주요 진료지원 시스템 역시 높은 유지보수 수준을 보이고 있어 의료서비스 제공의 안정성이 유지되고 있는 것으로 나타났다. 반면 진료과 및 회송시스템, 진료정보교류시스템, 원격의료시스템 등 일부 연계·확장형 시스템은 상대적으로 유지보수 수준이 낮아 기능 고도화 및 지속적인 품질 관리 측면에서 보완이 필요한 것으로 나타났다.

한편 상급종합병원은 전반적으로 유지보수 체계를 갖추고 있으나 일부 시스템에서는 종합병원보다 낮은 수준을 보이고 있으며, 종합병원은 핵심 시스템을 중심으로 전반적으로 높은 유지보수 수준을 유지하고 있는 것으로 나타났다. 이는 시스템 규모, 운영 방식, 외부 솔루션 의존도 등의 차이에 기인한 것으로 해석된다.

〈표 5-37〉은 환자 서비스 관련 의료정보시스템 솔루션 유지보수 여부를 조사한 결과를 나타낸 것이다.

'의료기관 포털(대표 홈페이지)'은 총 응답기관(255개소) 중 237개소

(92.9%)에서 유지보수를 실시하고 있어 대부분의 기관이 기본적인 환자 정보 제공 시스템에 대한 관리 체계를 갖추고 있는 것으로 나타났다. '의료기관 포털(웹 기반 개인건강기록, PHR)'은 총 응답기관(40개소) 중 34개소(85.0%)에서 유지보수가 이루어지고 있었으며, '모바일 개인건강기록(PHR)'은 총 응답기관(67개소) 중 56개소(83.6%)로 나타나 환자 참여형 서비스 역시 전반적으로 높은 유지보수 수준을 보였다.

의료기관 종별로 살펴보면 상급종합병원은 전반적으로 높은 유지보수 수준을 보였다. '의료기관 포털(대표 홈페이지)'은 95.0%(38개소), '웹 기반 개인건강기록(PHR)'은 89.5%(17개소), '모바일 개인건강기록(PHR)'은 84.8%(28개소)로 대부분의 기관에서 유지보수가 이루어지고 있었다. 반면 종합병원의 경우 '의료기관 포털(대표 홈페이지)'은 92.6%(199개소)로 높은 수준을 유지하고 있었으며, '웹 기반 개인건강기록(PHR)'과 '모바일 개인건강기록(PHR)'은 각각 81.0%(17개소), 82.4%(28개소)로 나타나 상급종합병원에 비해 다소 낮은 수준을 보였다.

종합하면 의료기관의 환자 서비스 정보시스템은 전반적으로 높은 유지보수 수준을 보이고 있어 기본적인 시스템 운영과 서비스 제공의 안정성은 확보된 것으로 나타났다. 특히 의료기관 포털(대표 홈페이지)은 대부분의 기관에서 유지보수가 이루어지고 있어 환자 대상 정보 제공 기능은 안정적으로 운영되고 있는 것으로 나타났다. 반면 개인건강기록(PHR) 기반 서비스는 상대적으로 유지보수 수준이 다소 낮아 기능 고도화와 지속적인 서비스 품질 관리 측면에서 일부 보완이 필요한 것으로 나타났다.

상급종합병원은 환자용 디지털 서비스 전반에서 안정적인 유지보수 체계를 갖추고 있는 반면, 종합병원은 일부 서비스에서 유지보수 수준이 상대적으로 낮아 환자 참여형 서비스의 지속적 운영과 품질 관리 측면에서 차이가 나타나는 것으로 분석된다.

〈표 5-37〉 의료정보시스템 솔루션 유지보수 여부(환자 서비스)

(단위: 개소, %)

구분	의료기관 포털(대표 홈페이지)			의료기관 포털(웹) 기반 개인건강기록(PHR)		
	예	아니오	합계	예	아니오	합계
전체	237 (92.9%)	18 (7.1%)	255 (100%)	34 (85.0%)	6 (15.0%)	40 (100%)
상급 종합병원	38 (95.0%)	2 (5.0%)	40 (100%)	17 (89.5%)	2 (10.5%)	19 (100%)
종합병원	199 (92.6%)	16 (7.4%)	215 (100%)	17 (81.0%)	4 (19.0%)	21 (100%)
도시(동)	225 (93.8%)	15 (6.2%)	240 (100%)	33 (84.6%)	6 (15.4%)	39 (100%)
비도시 (읍·면)	12 (80.0%)	3 (20.0%)	15 (100%)	1 (100%)	0 (0.0%)	1 (100%)
구분	모바일 개인건강기록(PHR)			여백		
	예	아니오	합계			
전체	56 (83.6%)	11 (16.4%)	67 (100%)			
상급 종합병원	28 (84.8%)	5 (15.2%)	33 (100%)			
종합병원	28 (82.4%)	6 (17.6%)	34 (100%)			
도시(동)	55 (83.3%)	11 (16.7%)	66 (100%)			
비도시 (읍·면)	1 (100%)	0 (0.0%)	1 (100%)			

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

〈표 5-38〉은 진료 지원 및 경영 정보 관련 의료정보시스템 솔루션 유지보수 여부를 조사한 결과를 나타낸 것이다.

'원무관리·보험청구시스템'은 총 응답기관(254개소) 중 231개소(90.9%)에서 유지보수를 실시하고 있어 대부분의 기관이 행정·청구 시스템에 대한 안정적인 운영 관리 체계를 갖추고 있는 것으로 나타났다.

'전자적 자원관리시스템(ERP)'은 총 응답기관(183개소) 중 168개소(91.8%)에서 유지보수가 이루어지고 있어 도입된 기관을 중심으로 높은

수준의 관리가 이루어지고 있는 것으로 나타났다. '내부직원지원시스템(ESS)'은 총 응답기관(81개소) 중 65개소(80.2%)에서 유지보수가 이루어지고 있었으며 '전사적 데이터웨어하우스(EDW)'는 총 응답기관(61개소) 중 53개소(86.9%)로 나타나 경영 및 데이터 기반 시스템 역시 전반적으로 안정적인 운영 관리가 이루어지고 있는 것으로 나타났다.

의료기관 종별로 살펴보면 상급종합병원은 일부 시스템에서 종합병원보다 낮은 유지보수 수준을 보였다. '원무관리·보험청구시스템'은 76.3%(29개소), '전자적 자원관리시스템(ERP)'은 80.0%(20개소)로 나타났으며 '내부직원지원시스템(ESS)'과 '전사적 데이터웨어하우스(EDW)'도 각각 75.0%(18개소), 80.8%(21개소)로 나타났다.

반면 종합병원의 경우 '원무관리·보험청구시스템'은 93.5%(202개소), '전자적 자원관리시스템(ERP)'은 93.7%(148개소)로 높은 수준을 보였으며 '내부직원지원시스템(ESS)'과 '전사적 데이터웨어하우스(EDW)'도 각각 82.5%(47개소), 91.4%(32개소)로 나타나 전반적으로 상급종합병원보다 높은 유지보수 수준을 보였다.

종합하면 원무관리·보험청구시스템을 중심으로 한 행정·경영 정보시스템은 대부분의 의료기관에서 유지보수가 이루어지고 있어 기본적인 운영 안정성은 전반적으로 확보된 것으로 나타났다. 또한 전자적 자원관리시스템과 전사적 데이터웨어하우스 등 경영 및 데이터 기반 시스템도 도입된 기관을 중심으로 높은 유지보수 수준을 보이고 있어 데이터 기반 경영 환경이 점진적으로 안정화되고 있는 것으로 나타났다.

다만 내부직원지원시스템은 상대적으로 유지보수 수준이 다소 낮아 인사·조직 관리 등 내부 운영 지원 기능의 지속적인 고도화에는 일부 한계가 존재하는 것으로 나타났다. 또한 상급종합병원은 다양한 시스템을 운영하고 있음에도 일부 영역에서 유지보수 수준이 상대적으로 낮게 나타난 반면, 종합병원은 주요 행정 및 경영 시스템 전반에서 높은 유지보수

수준을 유지하고 있어 운영 관리 체계 측면에서 차이가 나타나는 것으로 분석된다.

한편 상급종합병원은 다양한 시스템을 운영하고 있음에도 불구하고 일부 영역에서 유지보수 수준이 상대적으로 낮게 나타난 반면, 종합병원은 주요 행정 및 경영 시스템 전반에서 높은 유지보수 수준을 유지하고 있어 운영 관리 체계 측면에서 차이가 나타나는 것으로 나타났다.

〈표 5-38〉 의료정보시스템 솔루션 유지보수 여부(진료 지원 및 경영 정보)

(단위: 개소, %)

구분	원무관리, 보험청구시스템			전자적 자원관리시스템(ERP)		
	예	아니오	합계	예	아니오	합계
전체	231 (90.9%)	23 (9.1%)	254 (100%)	168 (91.8%)	15 (8.2%)	183 (100%)
상급 종합병원	29 (76.3%)	9 (23.7%)	38 (100%)	20 (80.0%)	5 (20.0%)	25 (100%)
종합병원	202 (93.5%)	14 (6.5%)	216 (100%)	148 (93.7%)	10 (6.3%)	158 (100%)
도시(동)	217 (90.8%)	22 (9.2%)	239 (100%)	157 (91.3%)	15 (8.7%)	172 (100%)
비도시 (읍·면)	14 (93.3%)	1 (6.7%)	15 (100%)	11 (100%)	0 (0.0%)	11 (100%)
구분	내부직원지원시스템(ESS)			전사적데이터웨어하우스(EDW)		
	예	아니오	합계	예	아니오	합계
전체	65 (80.2%)	16 (19.8%)	81 (100%)	53 (86.9%)	8 (13.1%)	61 (100%)
상급 종합병원	18 (75.0%)	6 (25.0%)	24 (100%)	21 (80.8%)	5 (19.2%)	26 (100%)
종합병원	47 (82.5%)	10 (17.5%)	57 (100%)	32 (91.4%)	3 (8.6%)	35 (100%)
도시(동)	61 (79.2%)	16 (20.8%)	77 (100%)	50 (86.2%)	8 (13.8%)	58 (100%)
비도시 (읍·면)	4 (100%)	0 (0.0%)	4 (100%)	3 (100%)	0 (0.0%)	3 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

〈표 5-39〉는 교육 및 연구 관련 의료정보시스템 솔루션 유지보수 여부를 조사한 결과를 나타낸 것이다.

'보수교육 전산시스템'은 총 응답기관(56개소) 중 49개소(87.5%)에서 유지보수를 실시하고 있어 도입된 기관을 중심으로 비교적 높은 수준의 관리가 이루어지고 있는 것으로 나타났다. '조사연구 전산시스템'은 총 응답기관(40개소) 중 38개소(95.0%)에서 유지보수가 이루어지고 있어 보수교육 전산시스템보다 더 높은 유지보수 수준을 보였다.

의료기관 종별로 살펴보면 상급종합병원은 '보수교육 전산시스템' 95.2%(20개소), '조사연구 전산시스템' 94.7%(18개소)로 대부분의 기관에서 유지보수가 이루어지고 있는 것으로 나타났다. 반면 종합병원의 경우 '보수교육 전산시스템'은 82.9%(29개소), '조사연구 전산시스템'은 95.2%(20개소)로 나타나 조사연구 전산시스템은 상급종합병원과 유사한 수준을 보였으나 보수교육 전산시스템은 상대적으로 낮은 유지보수 수준을 보였다.

〈표 5-39〉 의료정보시스템 솔루션 유지보수 여부(교육 및 연구)

(단위: 개소, %)

구분	보수교육 전산시스템			조사연구 전산시스템		
	예	아니오	합계	예	아니오	합계
전체	49 (87.5%)	7 (12.5%)	56 (100%)	38 (95.0%)	2 (5.0%)	40 (100%)
상급 종합병원	20 (95.2%)	1 (4.8%)	21 (100%)	18 (94.7%)	1 (5.3%)	19 (100%)
종합병원	29 (82.9%)	6 (17.1%)	35 (100%)	20 (95.2%)	1 (4.8%)	21 (100%)
도시(동)	47 (87.0%)	7 (13.0%)	54 (100%)	37 (94.9%)	2 (5.1%)	39 (100%)
비도시 (읍·면)	2 (100%)	0 (0.0%)	2 (100%)	1 (100%)	0 (0.0%)	1 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

종합하면 의료기관의 교육 및 연구 관련 정보시스템은 도입된 기관을 중심으로 전반적으로 높은 유지보수 수준을 보이고 있어 기본적인 운영 안정성은 확보된 것으로 나타났다. 특히 조사연구 전산시스템은 매우 높은 유지보수율을 보이며 연구데이터 관리 및 분석 지원 체계의 안정성이 확보된 것으로 나타났다. 반면 보수교육 전산시스템은 상대적으로 유지보수 수준이 다소 낮아 교육 관리 기능의 지속적인 운영 및 고도화 측면에서 일부 보완이 필요한 것으로 나타났다.

한편 상급종합병원은 교육·연구 시스템 전반에서 안정적인 유지보수 체계를 갖추고 있는 반면 종합병원은 일부 교육 시스템에서 유지보수 수준이 상대적으로 낮아 교육 기능의 체계적 운영 측면에서 차이가 나타나는 것으로 나타났다.

〈표 5-40〉은 기타 부대사업 관련 의료정보시스템 솔루션 유지보수 여부를 조사한 결과를 나타낸 것이다.

'부설 노인복지시설 전산시스템'은 총 응답기관(6개소) 중 5개소(83.3%)에서 유지보수가 이루어지고 있어 도입된 기관을 중심으로 비교적 높은 수준의 관리가 이루어지고 있는 것으로 나타났다. '부설 장례식장 전산시스템'은 총 응답기관(117개소) 중 104개소(88.9%)에서 유지보수가 이루어지고 있었으며 '부설 주차장 전산시스템'은 총 응답기관(156개소) 중 135개소(86.5%)로 나타나 부대사업 관련 시스템 전반에서 비교적 높은 유지보수 수준을 보였다. '기타 시스템'은 1개소(100.0%)에서 유지보수가 이루어졌으나 사례 수가 매우 적어 일반화에는 한계가 있는 것으로 나타났다.

의료기관 종별로 살펴보면 상급종합병원은 '부설 노인복지시설 전산시스템'과 '부설 주차장 전산시스템'에서 각각 100.0%(1개소), 87.5%(28개소)의 유지보수율을 보였으며 '부설 장례식장 전산시스템'은 81.0%(17

개소)로 나타났다. 반면 종합병원의 경우 '부설 노인복지시설 전산시스템'은 80.0%(4개소), '부설 장례식장 전산시스템'은 90.6%(87개소), '부설 주차장 전산시스템'은 86.3%(107개소)로 나타나 전반적으로 안정적인 유지보수 수준을 보였다.

〈표 5-40〉 의료정보시스템 솔루션 유지보수 여부(기타 부대사업)

(단위: 개소, %)

구분	부설 노인복지시설 전산시스템			부설 장례식장 전산시스템		
	예	아니오	합계	예	아니오	합계
전체	5 (83.3%)	1 (16.7%)	6 (100%)	104 (88.9%)	13 (11.1%)	117 (100%)
상급 종합병원	1 (100%)	0 (0.0%)	1 (100%)	17 (81.0%)	4 (19.0%)	21 `(100%)
종합병원	4 (80.0%)	1 (20.0%)	5 (100%)	87 (90.6%)	9 (9.4%)	96 (100%)
도시(동)	4 (80.0%)	1 (20.0%)	5 (100%)	97 (88.2%)	13 (11.8%)	110 (100%)
비도시 (읍·면)	1 (100%)	0 (0.0%)	1 (100%)	7 (100%)	0 (0.0%)	7 (100%)
구분	부설 주차장 전산시스템			기타		
	예	아니오	합계	예	아니오	합계
전체	135 (86.5%)	21 (13.5%)	156 (100%)	1 (100%)	0 (0.0%)	1 (100%)
상급 종합병원	28 (87.5%)	4 (12.5%)	32 (100%)	-	-	-
종합병원	107 (86.3%)	17 (13.7%)	124 (100%)	1 (100%)	0 (0.0%)	1 (100%)
도시(동)	125 (85.6%)	21 (14.4%)	146 (100%)	1 (100%)	0 (0.0%)	1 (100%)
비도시 (읍·면)	10 (100%)	0 (0.0%)	10 (100%)	-	-	-

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

종합하면 의료기관의 부대사업 관련 정보시스템은 도입된 기관을 중심으로 전반적으로 높은 유지보수 수준을 보이고 있어 기본적인 운영 안정

성은 확보된 것으로 나타났다. 특히 장례식장 및 주차장 시스템은 비교적 높은 유지보수율을 보이며 운영 관리 체계가 안정적으로 유지되고 있는 것으로 나타났다. 반면 노인복지시설 시스템은 유지보수율 자체는 높으나 도입 기관 수가 매우 적어 전반적인 확산 및 관리 체계 수준을 일반화하기에는 한계가 있는 것으로 나타났다.

한편 상급종합병원과 종합병원 모두 부대사업 시스템에서 전반적으로 유사한 수준의 유지보수를 보이고 있으며, 이는 해당 영역이 진료·행정 시스템에 비해 상대적으로 표준화된 운영 구조를 갖고 있기 때문으로 나타났다.

나. 인터넷 연결 여부

〈표 5-41〉은 진료정보 관련 의료정보시스템의 인터넷 연결 여부를 조사한 결과를 나타낸 것이다.

진료정보 관련 의료정보시스템의 인터넷 연결 여부에 대해 '전자의무기록시스템(EMR)'은 총 응답기관(263개소) 중 133개소(50.6%)에서 인터넷과 연결되어 운영되고 있어 절반 수준에 머물러 있는 것으로 나타났다. '모바일 전자의무기록시스템'은 총 응답기관(78개소) 중 41개소(52.6%)로 유사한 수준을 보였다. '처방전달시스템(OCS)'은 총 응답기관(260개소) 중 135개소(51.9%), '의료영상저장전송시스템(PACS)'은 총 응답기관(262개소) 중 128개소(48.9%)에서 인터넷과 연결되어 있었으며, '임상검사정보시스템(LIS)'은 총 응답기관(177개소) 중 82개소(46.3%), 과 '약국관리시스템'은 총 응답기관(189개소) 중 100개소(52.9%)로 나타나 주요 진료지원 시스템의 인터넷 연결 여부는 기관별로 혼재된 양상을 보였다. 또한 '진료과 및 회송 시스템'은 총 응답기관(168

개소) 중 107개소(63.7%), '진료정보교류시스템'은 총 응답기관(183개소) 중 140개소(76.5%)로 나타나 진료 연계 및 정보교류 시스템은 상대적으로 높은 인터넷 연결 수준을 보였다. '원격의료시스템'은 총 응답기관(29개소) 중 23개소(79.3%)로 높은 수준을 보인 반면 '건강검진정보시스템'은 총 응답기관(249개소) 중 144개소(57.8%)로 절반 수준이었다.

의료기관 종별로 살펴보면 상급종합병원은 전반적으로 인터넷 연결 수준이 낮은 경향을 보였다. '전자의무기록시스템'은 17.1%(7개소), '처방전달시스템'은 20.0%(8개소), '의료영상저장전송시스템'은 22.0%(9개소)로 나타났으며 '임상검사정보시스템'과 '약국관리시스템'도 각각 22.2%(8개소), 25.7%(9개소)로 대부분의 핵심 시스템에서 인터넷 연결이 제한적으로 이루어지고 있었다. 반면 '진료과 및 회송 시스템'은 45.0%(18개소), '진료정보교류시스템'은 69.2%(27개소)로 나타나 일부 연계 시스템에서는 비교적 높은 연결 수준을 보였으며 '원격의료시스템'은 100.0%(7개소)로 모든 기관에서 인터넷 연결이 이루어지고 있었다. 그러나 '건강검진정보시스템'은 29.7%(11개소)로 낮은 수준을 보였다.

종합병원의 경우 '전자의무기록시스템'은 56.8%(126개소), '처방전달시스템'은 57.7%(127개소), '의료영상저장전송시스템'은 53.8%(119개소)로 나타나 상급종합병원에 비해 상대적으로 높은 인터넷 연결 수준을 보였다. '임상검사정보시스템'과 '약국관리시스템'도 각각 52.5%(74개소), 59.1%(91개소)로 절반 이상의 기관에서 인터넷과 연결되어 있었다. 또한 '진료과 및 회송 시스템'은 69.5%(89개소), '진료정보교류시스템'은 78.5%(113개소)로 높은 수준을 보였으며 '원격의료시스템'은 72.7%(16개소), '건강검진정보시스템'은 62.7%(133개소)로 전반적으로 상급종합병원보다 높은 인터넷 연결 수준을 유지하고 있는 것으로 나타났다.

〈표 5-41〉 의료정보시스템과 인터넷 연결 여부(진료정보)

(단위: 개소, %)

구분	전자의무기록시스템(EMR)			모바일 전자의무기록시스템(EMR)		
	예	아니오	합계	예	아니오	합계
전체	133 (50.6%)	130 (49.4%)	263 (100%)	41 (52.6%)	37 (47.4%)	78 (100%)
상급 종합병원	7 (17.1%)	34 (82.9%)	41 (100%)	11 (44.0%)	14 (56.0%)	25 (100%)
종합병원	126 (56.8%)	96 (43.2%)	222 (100%)	30 (56.6%)	23 (43.4%)	53 (100%)
도시(동)	124 (50.0%)	124 (50.0%)	248 (100%)	39 (52.7%)	35 (47.3%)	74 (100%)
비도시 (읍·면)	9 (60.0%)	6 (40.0%)	15 (100%)	2 (50.0%)	2 (50.0%)	4 (100%)
구분	처방전달시스템(OCS)			의료영상저장전송시스템(PACS)		
	예	아니오	합계	예	아니오	합계
전체	135 (51.9%)	125 (48.1%)	260 (100%)	128 (48.9%)	134 (51.1%)	262 (100%)
상급 종합병원	8 (20.0%)	32 (80.0%)	40 (100%)	9 (22.0%)	32 (78.0%)	41 (100%)
종합병원	127 (57.7%)	93 (42.3%)	220 (100%)	119 (53.8%)	102 (46.2%)	221 (100%)
도시(동)	126 (51.4%)	119 (48.6%)	245 (100%)	119 (48.2%)	128 (51.8%)	247 (100%)
비도시 (읍·면)	9 (60.0%)	6 (40.0%)	15 (100%)	9 (60.0%)	6 (40.0%)	15 (100%)
구분	임상검사정보시스템(LIS)			약국관리시스템		
	예	아니오	합계	예	아니오	합계
전체	82 (46.3%)	95 (53.7%)	177 (100%)	100 (52.9%)	89 (47.1%)	189 (100%)
상급 종합병원	8 (22.2%)	28 (77.8%)	36 (100%)	9 (25.7%)	26 (74.3%)	35 (100%)
종합병원	74 (52.5%)	67 (47.5%)	141 (100%)	91 (59.1%)	63 (40.9%)	154 (100%)
도시(동)	76 (45.2%)	92 (54.8%)	168 (100%)	95 (53.1%)	84 (46.9%)	179 (100%)
비도시 (읍·면)	6 (66.7%)	3 (33.3%)	9 100%)	5 (50.0%)	5 (50.0%)	10 (100%)

구분	진료과 및 회송 시스템(상/하/원)			진료정보교류시스템(복지부)		
	예	아니오	합계	예	아니오	합계
전체	107 (63.7%)	61 (36.3%)	168 (100%)	140 (76.5%)	43 (23.5%)	183 (100%)
상급 종합병원	18 (45.0%)	22 (55.0%)	40 (100%)	27 (69.2%)	12 (30.8%)	39 (100%)
종합병원	89 (69.5%)	39 (30.5%)	128 (100%)	113 (78.5%)	31 (21.5%)	144 (100%)
도시(동)	102 (64.2%)	57 (35.8%)	159 (100%)	132 (75.9%)	42 (24.1%)	174 (100%)
비도시 (읍·면)	5 (55.6%)	4 (44.4%)	9 (100%)	8 (88.9%)	1 (11.1%)	9 (100%)
구분	원격의료시스템			건강검진정보시스템		
	예	아니오	합계	예	아니오	합계
전체	23 (79.3%)	6 (20.7%)	29 (100%)	144 (57.8%)	105 (42.2%)	249 (100%)
상급 종합병원	7 (100%)	0 (0.0%)	7 (100%)	11 (29.7%)	26 (70.3%)	37 (100%)
종합병원	16 (72.7%)	6 (27.3%)	22 (100%)	133 (62.7%)	79 (37.3%)	212 (100%)
도시(동)	22 (78.6%)	6 (21.4%)	28 (100%)	136 (57.9%)	99 (42.1%)	235 (100%)
비도시 (읍·면)	1 (100%)	0 (0.0%)	1 (100%)	8 (57.1%)	6 (42.9%)	14 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

종합하면 진료정보시스템의 인터넷 연결 여부는 전체적으로 절반 내외 수준에 머물러 있어 의료기관별 보안 정책 및 운영 전략에 따라 상이한 네트워크 구조가 적용되고 있는 것으로 나타났다. 특히 전자의무기록시스템과 처방전달시스템 등 핵심 시스템은 인터넷과 분리된 내부망 중심으로 운영되는 경향이 여전히 강한 반면 진료정보교류시스템과 원격의료시스템 등 외부 연계가 필수적인 시스템은 상대적으로 높은 인터넷 연결 수준을 보이고 있는 것으로 나타났다.

한편 상급종합병원은 보안 및 개인정보 보호 강화를 위해 인터넷 분리

정책을 보다 엄격하게 적용하고 있는 반면 종합병원은 외부 연계 및 접근성을 고려하여 상대적으로 인터넷 연결을 허용하는 비율이 높은 것으로 나타났다. 이는 의료정보의 민감성과 서비스 확장성 간 균형을 고려한 운영 전략의 차이에 기인한 것으로 나타났다.

〈표 5-42〉는 환자 서비스 관련 의료정보시스템의 인터넷 연결 여부를 조사한 결과를 나타낸 것이다.

환자 서비스 관련 의료정보시스템의 인터넷 연결 여부에 대해 '의료기관 포털(대표 홈페이지)'은 총 응답기관(255개소) 중 240개소(94.1%)에서 인터넷과 연결되어 운영되고 있어 대부분의 기관이 외부 접근이 가능한 형태로 운영하고 있는 것으로 나타났다. '의료기관 포털(웹 기반 개인건강기록, PHR)'은 총 응답기관(40개소) 중 36개소(90.0%)에서 인터넷과 연결되어 해당 시스템을 도입한 기관에서는 대부분 외부 접근성을 확보하고 있는 것으로 나타났다. '모바일 개인건강기록(PHR)'은 총 응답기관(67개소) 중 55개소(82.1%)에서 인터넷과 연결되어 환자 참여형 모바일 서비스는 전반적으로 인터넷 기반으로 운영되고 있는 것으로 나타났다.

의료기관 종별로 살펴보면 상급종합병원은 모든 항목에서 높은 인터넷 연결 수준을 보였다. '의료기관 포털(대표 홈페이지)'은 92.5%(37개소), '웹 기반 개인건강기록'은 89.5%(17개소), '모바일 개인건강기록'은 78.8%(26개소)로 대부분의 기관에서 인터넷과 연결되어 운영되고 있는 것으로 나타났다. 반면 종합병원의 경우 '의료기관 포털(대표 홈페이지)'은 94.4%(203개소)로 높은 수준을 유지하고 있었으며 '웹 기반 개인건강기록'과 '모바일 개인건강기록'은 각각 90.5%(19개소), 85.3%(29개소)로 나타나 상급종합병원과 유사하거나 다소 높은 수준을 보였다.

종합하면 환자 서비스 정보시스템은 대부분 인터넷과 연결된 형태로 운영되고 있어 환자의 접근성과 이용 편의성을 중심으로 시스템이 구축·

운영되고 있는 것으로 나타났다. 특히 의료기관 포털과 개인건강기록(PHR) 서비스는 높은 인터넷 연결 수준을 보이며 환자 대상 정보 제공 및 참여형 서비스가 외부 접근 기반으로 설계되어 있는 것으로 나타났다.

〈표 5-42〉 의료정보시스템과 인터넷 연결 여부(환자 서비스)

(단위: 개소, %)

구분	의료기관 포털(대표 홈페이지)			의료기관 포털(웹) 기반 개인건강기록(PHR)		
	예	아니오	합계	예	아니오	합계
전체	240 (94.1%)	15 (5.9%)	255 (100%)	36 (90.0%)	4 (10.0%)	40 (100%)
상급 종합병원	37 (92.5%)	3 (7.5%)	40 (100%)	17 (89.5%)	2 (10.5%)	19 (100%)
종합병원	203 (94.4%)	12 (5.6%)	215 (100%)	19 (90.5%)	2 (9.5%)	21 (100%)
도시(동)	225 (93.8%)	15 (6.2%)	240 (100%)	35 (89.7%)	4 (10.3%)	39 (100%)
비도시 (읍·면)	15 (100%)	0 (0.0%)	15 (100%)	1 (100%)	0 (0.0%)	1 (100%)
구분	모바일 개인건강기록(PHR)			여백		
	예	아니오	합계			
전체	55 (82.1%)	12 (17.9%)	67 (100%)			
상급 종합병원	26 (78.8%)	7 (21.2%)	33 (100%)			
종합병원	29 (85.3%)	5 (14.7%)	34 (100%)			
도시(동)	54 (81.8%)	12 (18.2%)	66 (100%)			
비도시 (읍·면)	1 (100%)	0 (0.0%)	1 (100%)			

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

〈표 5-43〉은 진료 지원 및 경영 정보 관련 의료정보시스템의 인터넷 연결 여부를 조사한 결과를 나타낸 것이다.

‘원무관리·보험청구시스템’은 총 응답기관(254개소) 중 144개소(56.7%)에서 인터넷과 연결되어 운영되고 있어 절반을 다소 상회하는 수준으로 나타났다. 반면 ‘전자적 자원관리시스템(ERP)’은 총 응답기관(183개소) 중 86개소(47.0%)로 절반에 미치지 못하는 수준을 보였다. ‘내부직원지원시스템(ESS)’은 총 응답기관(81개소) 중 35개소(43.2%)에서 인터넷과 연결되어 있었으며 ‘전사적 데이터웨어하우스(EDW)’는 총 응답기관(61개소) 중 15개소(24.6%)로 나타나 경영 및 데이터 기반 시스템일수록 인터넷 연결 비율이 낮은 경향을 보였다.

의료기관 종별로 살펴보면 상급종합병원은 전반적으로 인터넷 연결 수준이 낮은 것으로 나타났다. ‘원무관리·보험청구시스템’은 18.4%(7개소), ‘전자적 자원관리시스템’은 12.0%(3개소)로 낮은 수준을 보였으며 ‘내부직원지원시스템’과 ‘전사적 데이터웨어하우스’도 각각 25.0%(6개소), 15.4%(4개소)로 대부분의 시스템에서 인터넷 연결이 제한적으로 이루어지고 있는 것으로 나타났다. 반면 종합병원의 경우 ‘원무관리·보험청구시스템’은 63.4%(137개소), ‘전자적 자원관리시스템’은 52.5%(83개소)로 나타나 상급종합병원보다 높은 인터넷 연결 수준을 보였다. ‘내부직원지원시스템’은 50.9%(29개소)로 절반 수준이었으며 ‘전사적 데이터웨어하우스’는 31.4%(11개소)로 나타나 여전히 낮은 수준을 유지하고 있는 것으로 나타났다.

종합하면 진료 지원 및 경영 정보시스템의 인터넷 연결 수준은 시스템 유형에 따라 차이를 보이는 것으로 나타났다. 원무·보험청구 등 외부 연계가 필요한 시스템은 비교적 높은 연결 비율을 보이는 반면 전사적 데이터웨어하우스와 같은 내부 데이터 관리 시스템은 인터넷과 분리된 형태로 운영되는 경향이 뚜렷하게 나타났다. 또한 상급종합병원은 보안 및 내부 데이터 보호를 위해 인터넷 연결을 제한하는 경향이 강한 반면 종합병원은 업무 효율성과 외부 연계를 고려하여 상대적으로 인터넷 연결을 허

용하는 비율이 높은 것으로 나타났다.

이는 경영 및 행정 데이터의 민감성과 활용 목적에 따라 네트워크 운영 전략이 차별적으로 적용되고 있음을 보여주는 결과로 나타났다. 또한 향후 데이터 활용 확대와 보안 요구 간 균형 확보가 중요한 과제로 나타났다.

〈표 5-43〉 의료정보시스템과 인터넷 연결 여부(진료 지원 및 경영 정보)

(단위: 개소, %)

구분	원무관리, 보험청구시스템			전자적 자원관리시스템(ERP)		
	예	아니오	합계	예	아니오	합계
전체	144 (56.7%)	110 (43.3%)	254 (100%)	86 (47.0%)	97 (53.0%)	183 (100%)
상급 종합병원	7 (18.4%)	31 (81.6%)	38 (100%)	3 (12.0%)	22 (88.0%)	25 (100%)
종합병원	137 (63.4%)	79 (36.6%)	216 (100%)	83 (52.5%)	75 (47.5%)	158 (100%)
도시(동)	134 (56.1%)	105 (43.9%)	239 (100%)	78 (45.3%)	94 (54.7%)	172 (100%)
비도시 (읍·면)	10 (66.7%)	5 (33.3%)	15 (100%)	8 (72.7%)	3 (27.3%)	11 (100%)
구분	내부직원지원시스템(ESS)			전사적데이터웨어하우스(EDW)		
	예	아니오	합계	예	아니오	합계
전체	35 (43.2%)	46 (56.8%)	81 (100%)	15 (24.6%)	46 (75.4%)	61 (100%)
상급 종합병원	6 (25.0%)	18 (75.0%)	24 (100%)	4 (15.4%)	22 (84.6%)	26 (100%)
종합병원	29 (50.9%)	28 (49.1%)	57 (100%)	11 (31.4%)	24 (68.6%)	35 (100%)
도시(동)	31 (40.3%)	46 (59.7%)	77 (100%)	14 (24.1%)	44 (75.9%)	58 (100%)
비도시 (읍·면)	4 (100%)	0 (0.0%)	4 (100%)	1 (33.3%)	2 (66.7%)	3 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

〈표 5-44〉는 교육 및 연구 관련 의료정보시스템의 인터넷 연결 여부를 조사한 결과를 나타낸 것이다. '보수교육 전산시스템'은 총 응답기관(56

개소) 중 39개소(69.6%)에서 인터넷과 연결되어 운영되고 있어 비교적 높은 수준을 보였다. 반면 '조사연구 전산시스템'은 총 응답기관(40개소) 중 21개소(52.5%)로 절반 수준에 머물러 있는 것으로 나타났다.

의료기관 종별로 살펴보면 상급종합병원은 '보수교육 전산시스템' 66.7%(14개소), '조사연구 전산시스템' 52.6%(10개소)로 나타나 전반적으로 절반 이상에서 인터넷 연결이 이루어지고 있는 것으로 나타났다. 반면 종합병원의 경우 '보수교육 전산시스템'은 71.4%(25개소)로 상급종합병원보다 다소 높은 수준을 보였으며 '조사연구 전산시스템'은 52.4%(11개소)로 유사한 수준을 나타냈다.

〈표 5-44〉 의료정보시스템과 인터넷 연결 여부(교육 및 연구)

(단위: 개소, %)

구분	보수교육 전산시스템			조사연구 전산시스템		
	예	아니오	합계	예	아니오	합계
전체	39 (69.6%)	17 (30.4%)	56 (100%)	21 (52.5%)	19 (47.5%)	40 (100%)
상급 종합병원	14 (66.7%)	7 (33.3%)	21 (100%)	10 (52.6%)	9 (47.4%)	19 (100%)
종합병원	25 (71.4%)	10 (28.6%)	35 (100%)	11 (52.4%)	10 (47.6%)	21 (100%)
도시(동)	37 (68.5%)	17 (31.5%)	54 (100%)	20 (51.3%)	19 (48.7%)	39 (100%)
비도시 (읍·면)	2 (100%)	0 (0.0%)	2 (100%)	1 (100%)	0 (0.0%)	1 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

종합하면 교육 및 연구 정보시스템의 인터넷 연결 수준은 전반적으로 절반 이상에서 이루어지고 있어 진료정보 및 경영정보 시스템에 비해 상대적으로 개방적인 네트워크 운영이 이루어지고 있는 것으로 나타났다. 특히 보수교육 전산시스템은 비교적 높은 인터넷 연결 수준을 보이며 외

부 교육 콘텐츠 및 플랫폼과의 연계를 고려한 운영이 이루어지고 있는 것으로 나타났다. 반면 조사연구 전산시스템은 절반 수준에 머물러 있어 연구데이터의 보안 및 내부 관리 필요성에 따라 인터넷 연결이 제한적으로 운영되고 있는 것으로 나타났다.

한편 상급종합병원과 종합병원 간 큰 차이는 나타나지 않아 교육 및 연구 영역에서는 전반적으로 유사한 수준의 인터넷 기반 활용이 이루어지고 있는 것으로 나타났다.

〈표 5-45〉는 기타 부대사업 관련 의료정보시스템의 인터넷 연결 여부를 조사한 결과를 나타낸 것이다.

'부설 노인복지시설 전산시스템'은 총 응답기관(6개소) 중 4개소(66.7%)에서 인터넷과 연결되어 운영되고 있어 도입된 기관을 기준으로 비교적 높은 수준을 보였다. '부설 장례식장 전산시스템'은 총 응답기관(117개소) 중 57개소(48.7%)로 절반에 미치지 못하는 수준이었으며 '부설 주차장 전산시스템'은 총 응답기관(156개소) 중 83개소(53.2%)로 절반 수준의 인터넷 연결 비율을 나타냈다. '기타 시스템'은 인터넷 연결 사례가 없거나(0.0%) 매우 제한적으로 나타났다.

의료기관 종별로 살펴보면 상급종합병원은 '부설 노인복지시설 전산시스템'이 100.0%(1개소)로 나타났으나 사례 수가 매우 적은 것으로 나타났다. '부설 장례식장 전산시스템'은 42.9%(9개소)로 낮은 수준을 보였으며 '부설 주차장 전산시스템'은 34.4%(11개소)로 나타나 전반적으로 인터넷 연결 수준이 낮은 경향을 보였다.

반면 종합병원의 경우 '부설 노인복지시설 전산시스템'은 60.0%(3개소), '부설 장례식장 전산시스템'은 50.0%(48개소), '부설 주차장 전산시스템'은 58.1%(72개소)로 나타나 상급종합병원보다 전반적으로 높은 인터넷 연결 수준을 보였다.

〈표 5-45〉 의료정보시스템과 인터넷 연결 여부(기타 부대사업)

(단위: 개소, %)

구분	부설 노인복지시설 전산시스템			부설 장례식장 전산시스템		
	예	아니오	합계	예	아니오	합계
전체	4 (66.7%)	2 (33.3%)	6 (100%)	57 (48.7%)	60 (51.3%)	117 (100%)
상급 종합병원	1 (100%)	0 (0.0%)	1 (100%)	9 (42.9%)	12 (57.1%)	21 (100%)
종합병원	3 (60.0%)	2 (40.0%)	5 (100%)	48 (50.0%)	48 (50.0%)	96 (100%)
도시(동)	3 (60.0%)	2 (40.0%)	5 (100%)	54 (49.1%)	56 (50.9%)	110 (100%)
비도시 (읍·면)	1 (100%)	0 (0.0%)	1 (100%)	3 (42.9%)	4 (57.1%)	7 (100%)
구분	부설 주차장 전산시스템			기타		
	예	아니오	합계	예	아니오	합계
전체	83 (53.2%)	73 (46.8%)	156 (100%)	0 (0.0%)	1 (100%)	1 (100%)
상급 종합병원	11 (34.4%)	21 (65.6%)	32 (100%)			
종합병원	72 (58.1%)	52 (41.9%)	124 (100%)	0 (0.0%)	1 (100%)	1 (100%)
도시(동)	76 (52.1%)	70 (47.9%)	146 (100%)	0 (0.0%)	1 (100%)	1 (100%)
비도시 (읍·면)	7 (70.0%)	3 (30.0%)	10 (100%)			

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

종합하면 의료기관의 부대사업 관련 정보시스템은 인터넷 연결 수준이 전반적으로 절반 내외에 머물러 있어 진료 및 환자 서비스 시스템에 비해 상대적으로 제한적인 네트워크 운영이 이루어지고 있는 것으로 나타났다. 특히 장례식장 및 주차장 시스템은 일부 외부 서비스와의 연계를 위해 인터넷 연결이 이루어지고 있으나 보안 및 운영 특성에 따라 완전한 개방형 구조로 운영되지는 않고 있는 것으로 나타났다.

한편 상급종합병원은 전반적으로 인터넷 연결을 제한하는 경향이 강한

반면 종합병원은 운영 효율성과 외부 서비스 연계를 고려하여 상대적으로 인터넷 연결을 허용하는 비율이 높은 것으로 나타났다.

다. 병원 내 정보시스템 연결

〈표 5-46〉은 진료정보 관련 의료정보시스템과 병원 내 정보시스템 연결 여부를 조사한 결과를 나타낸 것이다.

‘전자의무기록시스템(EMR)’은 총 응답기관(263개소) 중 247개소(93.9%)에서 병원 내 다른 정보시스템과 연계되어 운영되고 있어 핵심 진료정보시스템 간 연계 기반이 전반적으로 높은 수준으로 구축된 것으로 나타났다. ‘모바일 전자의무기록시스템’은 총 응답기관(78개소) 중 72개소(92.3%)에서 연계되어 모바일 기반 환경에서도 내부 시스템 간 연계가 상당 부분 이루어지고 있는 것으로 나타났다.

‘처방전달시스템(OCS)’은 총 응답기관(260개소) 중 247개소(95.0%), ‘의료영상저장전송시스템(PACS)’은 총 응답기관(262개소) 중 244개소(93.1%)에서 타 시스템과 연계되어 운영되고 있어 진료 과정 전반에 걸친 시스템 간 연동이 높은 수준으로 이루어지고 있는 것으로 나타났다. ‘임상검사정보시스템(LIS)’은 총 응답기관(177개소) 중 160개소(90.4%), ‘약국관리시스템’은 총 응답기관(189개소) 중 172개소(91.0%)로 나타나 주요 진료지원 시스템도 대부분 연계 체계를 갖추고 있는 것으로 나타났다.

또한 ‘진료과 및 회송 시스템(상/하/원)’은 총 응답기관(168개소) 중 156개소(92.9%), ‘진료정보교류시스템(복지부)’은 총 응답기관(183개소) 중 169개소(92.3%)에서 연계되어 운영되고 있어 진료 연속성 확보를 위한 시스템 간 연계도 비교적 높은 수준으로 나타났다. 한편 ‘건강검진정보시스템’은총 응답기관(249개소) 중 234개소(94.0%)로 높은 연계율

을 보였으나 '원격의료시스템'은 총 응답기관(29개소) 중 22개소(75.9%)로 상대적으로 낮은 수준에 머물러 있는 것으로 나타났다.

의료기관 종별로 살펴보면 상급종합병원은 대부분의 시스템에서 종합병원보다 높은 연계 수준을 보였다. '전자의무기록시스템'은 97.6%(40개소), '처방전달시스템'과 '의료영상저장전송시스템'은 각각 95.0%(38개소), 95.0%(38개소)로 나타났으며 '임상검사정보시스템'과 '약국관리시스템'도 각각 97.2%(35개소), 97.1%(34개소)로 높은 수준을 보였다. 또한 '진료과 및 회송 시스템(상/하/원)'은 100.0%(40개소), '진료정보교류시스템'은 97.4%(38개소)로 대부분의 기관에서 연계가 이루어지고 있는 것으로 나타났다. 다만 '원격의료시스템'은 71.4%(5개소)로 상대적으로 낮은 수준을 보였다.

반면 종합병원의 경우 '전자의무기록시스템'은 93.2%(207개소), '처방전달시스템'은 95.0%(209개소), '의료영상저장전송시스템'은 93.2%(206개소)로 핵심 시스템 간 연계는 전반적으로 양호한 수준을 보였다. '임상검사정보시스템'과 '약국관리시스템'은 각각 88.7%(125개소), 89.6%(138개소)로 나타났으며 '진료과 및 회송 시스템(상/하/원)'과 '진료정보교류시스템'은 각각 90.6%(116개소), 91.0%(131개소)로 비교적 높은 수준을 보였다. 다만 '원격의료시스템'은 77.3%(17개소)로 여전히 낮은 수준에 머물러 있는 것으로 나타났다.

종합하면 전자의무기록시스템을 중심으로 처방전달시스템, 의료영상저장전송시스템 등 핵심 진료정보시스템 간 연계는 대부분의 의료기관에서 높은 수준으로 구축되어 병원 내 정보 흐름의 통합 기반은 상당 부분 확보된 것으로 나타났다. 또한 임상검사, 약국관리 등 진료지원 시스템 역시 전반적으로 연계가 이루어지고 있어 진료 전 과정의 정보 활용 기반이 강화된 것으로 나타났다.

반면 원격의료시스템은 상대적으로 연계 수준이 낮아 비대면 진료 및 외부 연계 확장 측면에서는 여전히 제한적인 수준에 머물러 있는 것으로 나타났다. 상급종합병원은 전반적으로 시스템 간 연계 수준이 높고 진료·정보교류 기능까지 통합적으로 운영되고 있는 반면 종합병원은 핵심 진료시스템 중심의 연계에 머무르고 있어 일부 고도화된 연계 체계는 제한적인 것으로 나타났다.

〈표 5-46〉 의료정보시스템과 병원 내 정보시스템 연결 여부(진료정보)

(단위: 개소, %)

구분	전자의무기록시스템(EMR)			모바일 전자의무기록시스템(EMR)		
	예	아니오	합계	예	아니오	합계
전체	247 (93.9%)	16 (6.1%)	263 (100%)	72 (92.3%)	6 (7.7%)	78 (100%)
상급 종합병원	40 (97.6%)	1 (2.4%)	41 (100%)	24 (96.0%)	1 (4.0%)	25 (100%)
종합병원	207 (93.2%)	15 (6.8%)	222 (100%)	48 (90.6%)	5 (9.4%)	53 (100%)
도시(동)	234 (94.4%)	14 (5.6%)	248 (100%)	69 (93.2%)	5 (6.8%)	74 (100%)
비도시 (읍·면)	13 (86.7%)	2 (13.3%)	15 (100%)	3 (75.0%)	1 (25.0%)	4 (100%)
구분	처방전달시스템(OCS)			의료영상저장전송시스템(PACS)		
	예	아니오	합계	예	아니오	합계
전체	247 (95.0%)	13 (5.0%)	260 (100%)	244 (93.1%)	18 (6.9%)	262 (100%)
상급 종합병원	38 (95.0%)	2 (5.0%)	40 (100%)	38 (92.7%)	3 (7.3%)	41 (100%)
종합병원	209 (95.0%)	11 (5.0%)	220 (100%)	206 (93.2%)	15 (6.8%)	221 (100%)
도시(동)	232 (94.7%)	13 (5.3%)	245 (100%)	229 (92.7%)	18 (7.3%)	247 (100%)
비도시 (읍·면)	15 (100%)	0 (0.0%)	15 (100%)	15 (100%)	0 (0.0%)	15 (100%)

구분	임상검사정보시스템(LIS)			약국관리시스템		
	예	아니오	합계	예	아니오	합계
전체	160 (90.4%)	17 (9.6%)	177 (100%)	172 (91.0%)	17 (9.0%)	189 (100%)
상급 종합병원	35 (97.2%)	1 (2.8%)	36 (100%)	34 (97.1%)	1 (2.9%)	35 (100%)
종합병원	125 (88.7%)	16 (11.3%)	141 (100%)	138 (89.6%)	16 (10.4%)	154 (100%)
도시(동)	153 (91.1%)	15 (8.9%)	168 (100%)	165 (92.2%)	14 (7.8%)	179 (100%)
비도시 (읍·면)	7 (77.8%)	2 (22.2%)	9 (100%)	7 (70.0%)	3 (30.0%)	10 (100%)
구분	진료과 및 회송 시스템(상/하/원)			진료정보교류시스템(복지부)		
	예	아니오	합계	예	아니오	합계
전체	156 (92.9%)	12 (7.1%)	168 (100%)	169 (92.3%)	14 (7.7%)	183 (100%)
상급 종합병원	40 (100%)	0 (0.0%)	40 (100%)	38 (97.4%)	1 (2.6%)	39 (100%)
종합병원	116 (90.6%)	12 (9.4%)	128 (100%)	131 (91.0%)	13 (9.0%)	144 (100%)
도시(동)	150 (94.3%)	9 (5.7%)	159 (100%)	162 (93.1%)	12 (6.9%)	174 (100%)
비도시 (읍·면)	6 (66.7%)	3 (33.3%)	9 (100%)	7 (77.8%)	2 (22.2%)	9 (100%)
구분	원격의료시스템			건강검진정보시스템		
	예	아니오	합계	예	아니오	합계
전체	22 (75.9%)	7 (24.1%)	29 (100%)	234 (94.0%)	15 (6.0%)	249 (100%)
상급 종합병원	5 (71.4%)	2 (28.6%)	7 (100%)	36 (97.3%)	1 (2.7%)	37 (100%)
종합병원	17 (77.3%)	5 (22.7%)	22 (100%)	198 (93.4%)	14 (6.6%)	212 (100%)
도시(동)	21 (75.0%)	7 (25.0%)	28 (100%)	222 (94.5%)	13 (5.5%)	235 (100%)
비도시 (읍·면)	1 (100%)	0 (0.0%)	1 (100%)	12 (85.7%)	2 (14.3%)	14 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

〈표 5-47〉은 환자 서비스 관련 의료정보시스템과 병원 내 정보시스템 연결 여부를 조사한 결과를 나타낸 것이다.

‘의료기관 포털(대표 홈페이지)’은 총 응답기관(255개소) 중 132개소(51.8%)에서 병원 내 다른 정보시스템과 연계되어 운영되고 있어 절반 수준에서 내부 시스템과의 연계가 이루어지고 있는 것으로 나타났다. 반면 ‘의료기관 포털(웹 기반 개인건강기록, PHR)’은 총 응답기관(40개소) 중 37개소(92.5%)에서 연계되어 해당 시스템을 도입한 기관에서는 대부분 내부 시스템과의 연계가 함께 이루어지고 있는 것으로 나타났다. ‘모바일 개인건강기록(PHR)’은 총 응답기관(67개소) 중 611개소(91.0%)에서 연계되어 모바일 기반 환자 서비스에서도 높은 연계 수준을 보였다.

의료기관 종별로 살펴보면 상급종합병원은 모든 항목에서 종합병원보다 높은 연계 수준을 보였다. ‘의료기관 포털(대표 홈페이지)’은 92.5%(37개소)가 타 시스템과 연계되어 운영되고 있는 것으로 나타났으며 ‘웹 기반 개인건강기록’과 ‘모바일 개인건강기록’도 각각 94.7%(18개소), 93.9%(31개소)로 대부분의 기관에서 연계가 이루어지고 있는 것으로 나타났다.

반면 종합병원의 경우 ‘의료기관 포털(대표 홈페이지)’은 44.2%(95개소)만이 연계되어 있어 상급종합병원에 비해 낮은 수준을 보였다. ‘웹 기반 개인건강기록’과 ‘모바일 개인건강기록’은 각각 90.5%(19개소), 88.2%(30개소)로 나타나 도입된 경우에는 비교적 높은 연계 수준을 보였으나 전체적인 확산 수준은 제한적인 것으로 나타났다.

종합하면 환자용 정보시스템 가운데 개인건강기록(PHR) 기반 서비스는 도입된 기관을 중심으로 병원 내부 시스템과의 연계가 비교적 잘 이루어지고 있는 것으로 나타났다. 반면 의료기관 포털(대표 홈페이지)은 절반 수준에서만 내부 시스템과 연계되어 운영되고 있어 단순 정보 제공 기능에 머무르는 경우가 상당한 것으로 나타났다. 상급종합병원은 환자용 디지털 서비스 전반에서 시스템 간 연계를 적극적으로 추진하고 있는 것으로

나타난 반면 종합병원은 일부 시스템에 한정된 연계에 머무르고 있어 환자 참여형 서비스의 통합적 운영 수준은 상대적으로 낮은 것으로 나타났다.

〈표 5-47〉 의료정보시스템과 병원 내 정보시스템 연결 여부(환자 서비스)

(단위: 개소, %)

구분	의료기관 포털(대표 홈페이지)			의료기관 포털(웹) 기반 개인건강기록(PHR)		
	예	아니오	합계	예	아니오	합계
전체	132 (51.8%)	123 (48.2%)	255 (100%)	37 (92.5%)	3 (7.5%)	40 (100%)
상급 종합병원	37 (92.5%)	3 (7.5%)	40 (100%)	18 (94.7%)	1 (5.3%)	19 (100%)
종합병원	95 (44.2%)	120 (55.8%)	215 (100%)	19 (90.5%)	2 (9.5%)	21 (100%)
도시(동)	129 (53.8%)	111 (46.2%)	240 (100%)	36 (92.3%)	3 (7.7%)	39 (100%)
비도시 (읍·면)	3 (20.0%)	12 (80.0%)	15 (100%)	1 (100%)	0 (0.0%)	1 (100%)
구분	모바일 개인건강기록(PHR)			여백		
	예	아니오	합계			
전체	61 (91.0%)	6 (9.0%)	67 (100%)			
상급 종합병원	31 (93.9%)	2 (6.1%)	33 (100%)			
종합병원	30 (88.2%)	4 (11.8%)	34 (100%)			
도시(동)	60 (90.9%)	6 (9.1%)	66 (100%)			
비도시 (읍·면)	1 (100%)	0 (0.0%)	1 (100%)			

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

〈표 5-48〉은 진료 지원 및 경영 정보 관련 의료정보시스템과 병원 내 정보시스템 연결 여부를 조사한 결과를 나타낸 것이다.

'원무관리·보험청구시스템'은 총 응답기관(254개소) 중 233개소(91.7%)

에서 병원 내 다른 정보시스템과 연계되어 운영되고 있어 행정·청구 기능과 진료정보 간 연계는 대부분의 기관에서 구축된 것으로 나타났다. 반면 '전자적 자원관리시스템(ERP)'은 총 응답기관(183개소) 중 103개소(56.3%)에서 연계되어 절반 수준에 머물러 있는 것으로 나타났다. '내부직원지원시스템(ESS)'은 총 응답기관(81개소) 중 61개소(75.3%)로 비교적 높은 수준의 연계를 보였으며 '전사적 데이터웨어하우스(EDW)'는 총 응답기관(61개소) 중 52개소(85.2%)에서 연계되어 해당 시스템을 도입한 기관에서는 대부분 내부 시스템과의 연계가 함께 이루어지고 있는 것으로 나타났다.

의료기관 종별로 살펴보면 상급종합병원은 전반적으로 높은 연계 수준을 보였다. '원무관리·보험청구시스템'은 100.0%(38개소)가 연계되어 운영되고 있는 것으로 나타났으며 '전자적 자원관리시스템'은 96.0%(24개소)로 매우 높은 수준을 보였다. 또한 '내부직원지원시스템'과 '전사적 데이터웨어하우스'도 각각 91.7%(22개소), 88.5%(23개소)로 대부분의 기관에서 연계가 이루어지고 있는 것으로 나타났다.

반면 종합병원의 경우 '원무관리·보험청구시스템'은 90.3%(195개소)로 높은 수준을 유지하고 있었으나 '전자적 자원관리시스템'은 50.0%(79개소)로 절반 수준에 머물러 있는 것으로 나타났다. '내부직원지원시스템'은 68.4%(39개소)로 나타났으며 '전사적 데이터웨어하우스'는 82.9%(29개소)로 도입된 기관 내에서는 비교적 높은 연계 수준을 보였다.

종합하면 원무관리·보험청구시스템을 중심으로 한 행정·진료 연계는 대부분의 의료기관에서 안정적으로 구축되어 있는 것으로 나타났다. 반면 전자적 자원관리시스템(ERP) 등 경영자원 통합 시스템의 연계 수준은 상대적으로 낮아 병원 운영 전반의 통합적 관리 체계는 아직 충분히 확산되지 않은 것으로 나타났다. 또한 내부직원지원시스템과 전사적 데이터

웨어하우스는 도입된 기관을 중심으로 비교적 높은 연계 수준을 보이고 있는 것으로 나타났다. 그러나 전체적인 확산 수준이 제한적이어서 데이터 기반 의사결정 체계는 일부 기관에 국한되어 있는 것으로 나타났다.

〈표 5-48〉 의료정보시스템과 병원 내 정보시스템 연결 여부(진료 지원 및 경영 정보)

(단위: 개소, %)

구분	원무관리, 보험청구시스템			전자적 자원관리시스템(ERP)		
	예	아니오	합계	예	아니오	합계
전체	233 (91.7%)	21 (8.3%)	254 (100%)	103 (56.3%)	80 (43.7%)	183 (100%)
상급 종합병원	38 (100%)	0 (0.0%)	38 (100%)	24 (96.0%)	1 (4.0%)	25 (100%)
종합병원	195 (90.3%)	21 (9.7%)	216 (100%)	79 (50.0%)	79 (50.0%)	158 (100%)
도시(동)	223 (93.3%)	16 (6.7%)	239 (100%)	98 (57.0%)	74 (43.0%)	172 (100%)
비도시 (읍·면)	10 (66.7%)	5 (33.3%)	15 (100%)	5 (45.5%)	6 (54.5%)	11 (100%)
구분	내부직원지원시스템(ESS)			전사적데이터웨어하우스(EDW)		
	예	아니오	합계	예	아니오	합계
전체	61 (75.3%)	20 (24.7%)	81 (100%)	52 (85.2%)	9 (14.8%)	61 (100%)
상급 종합병원	22 (91.7%)	2 (8.3%)	24 (100%)	23 (88.5%)	3 (11.5%)	26 (100%)
종합병원	39 (68.4%)	18 (31.6%)	57 (100%)	29 (82.9%)	6 (17.1%)	35 (100%)
도시(동)	59 (76.6%)	18 (23.4%)	77 (100%)	50 (86.2%)	8 (13.8%)	58 (100%)
비도시 (읍·면)	2 (50%)	2 (50%)	4 (100%)	2 (66.7%)	1 (33.3%)	3 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

상급종합병원은 경영·인사·데이터 관리 영역까지 포함한 통합적 시스템 연계를 적극적으로 구축하고 있는 것으로 나타난 반면 종합병원은 원무·청구 등 기본 행정 기능 중심의 연계에 머무르고 있어 경영정보 고도

화 수준에서 차이가 나타나는 것으로 나타났다.

〈표 5-49〉는 교육 및 연구 관련 의료정보시스템과 병원 내 정보시스템 연결 여부를 조사한 결과를 나타낸 것이다.

'보수교육 전산시스템'은 총 응답기관(56개소) 중 25개소(44.6%)에서 병원 내 다른 정보시스템과 연계되어 운영되고 있어 절반에 미치지 못하는 수준으로 나타났다. '조사연구 전산시스템'은 총 응답기관(40개소) 중 27개소(67.5%)에서 연계되어 보수교육 전산시스템에 비해 상대적으로 높은 연계 수준을 보였으나 여전히 제한적인 수준에 머물러 있는 것으로 나타났다.

의료기관 종별로 살펴보면 상급종합병원은 종합병원보다 전반적으로 높은 연계 수준을 보였다. '보수교육 전산시스템'은 52.4%(11개소), '조사연구 전산시스템'은 73.7%(14개소)에서 연계되어 운영되고 있어 교육 및 연구 기능과 타 시스템 간 연계가 비교적 활발한 것으로 나타났다.

반면 종합병원의 경우 '보수교육 전산시스템'은 40.0%(14개소), '조사연구 전산시스템'은 61.9%(13개소)로 나타나 상급종합병원에 비해 전반적인 연계 수준이 낮은 것으로 나타났다.

종합하면 의료기관의 교육 및 연구 관련 정보시스템은 병원 내 다른 정보시스템과의 연계 수준이 전반적으로 낮아 진료 및 행정 영역에 비해 정보 활용과 데이터 연계 기반이 충분히 구축되지 않은 것으로 나타났다. 특히 보수교육 전산시스템은 연계율이 낮아 인력 역량 관리 및 교육 이력의 통합적 활용이 제한적인 것으로 나타났으며 조사연구 전산시스템 역시 일부 기관에 한정된 연계가 이루어지고 있어 연구데이터의 체계적 관리 및 활용 기반은 아직 초기 단계에 머물러 있는 것으로 나타났다.

상급종합병원은 교육·연구 기능과 관련된 시스템 연계를 비교적 적극적으로 추진하고 있는 것으로 나타난 반면 종합병원은 진료 및 행정 중심

의 정보시스템에 집중되어 있어 교육·연구 분야의 시스템 연계 수준은 상대적으로 미흡한 것으로 나타났다.

〈표 5-49〉 의료정보시스템과 병원 내 정보시스템 연결 여부(교육 및 연구)

(단위: 개소, %)

구분	보수교육 전산시스템			조사연구 전산시스템		
	예	아니오	합계	예	아니오	합계
전체	25 (44.6%)	31 (55.4%)	56 (100%)	27 (67.5%)	13 (32.5%)	40 (100%)
상급 종합병원	11 (52.4%)	10 (47.6%)	21 (100%)	14 (73.7%)	5 (26.3%)	19 (100%)
종합병원	14 (40.0%)	21 (60.0%)	35 (100%)	13 (61.9%)	8 (38.1%)	21 (100%)
도시(동)	24 (44.4%)	30 (55.6%)	54 (100%)	26 (66.7%)	13 (33.3%)	39 (100%)
비도시 (읍·면)	1 (50.0%)	1 (50.0%)	2 (100%)	1 (100%)	0 (0.0%)	1 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

〈표 5-50〉은 기타 부대사업 관련 의료정보시스템과 병원 내 정보시스템 연결 여부를 조사한 결과를 나타낸 것이다.

'부설 노인복지시설 전산시스템'은 총 응답기관(6개소) 중 1개소(16.7%)에서만 병원 내 다른 정보시스템과 연계되어 운영되고 있어 연계 수준이 매우 제한적인 것으로 나타났다. '부설 장례식장 전산시스템'은 총 응답기관(117개소) 중 47개소(40.2%)에서 연계되어 절반에 미치지 못하는 수준을 보였으며, '부설 주차장 전산시스템'은 총 응답기관(156개소) 중 90개소(57.7%)로 상대적으로 높은 연계율을 보이는 것으로 나타났다. '기타 시스템'은 1개소(100%)에서 연계되어 있었으나 사례 수가 매우 적어 일반화에는 한계가 있는 것으로 나타났다.

의료기관 종별로 살펴보면 상급종합병원은 '부설 노인복지시설 전산시

스템'의 경우 연계 사례가 없는 것으로 나타났으며(0.0%, 0개소), '부설 장례식장 전산시스템'은 47.6%(10개소), '부설 주차장 전산시스템'은 71.9%(23개소)에서 연계가 이루어지고 있어 일부 부대사업 영역에서는 비교적 높은 연계 수준을 보이는 것으로 나타났다.

〈표 5-50〉 의료정보시스템과 병원 내 정보시스템 연결 여부(기타 부대사업)

(단위: 개소, %)

구분	부설 노인복지시설 전산시스템			부설 장례식장 전산시스템		
	예	아니오	합계	예	아니오	합계
전체	1 (16.7%)	5 (83.3%)	6 (100%)	47 (40.2%)	70 (59.8%)	117 (100%)
상급 종합병원	0 (0.0%)	1 (100%)	1 (100%)	10 (47.6%)	11 (52.4%)	21 (100%)
종합병원	1 (20.0%)	4 (80.0%)	5 (100%)	37 (38.5%)	59 (61.5%)	96 (100%)
도시(동)	1 (20.0%)	4 (80.0%)	5 (100%)	44 (40.0%)	66 (60.0%)	110 (100%)
비도시 (읍·면)	0 (0.0%)	1 (100%)	1 (100%)	3 (42.9%)	4 (57.1%)	7 (100%)
구분	부설 주차장 전산시스템			기타		
	예	아니오	합계	예	아니오	합계
전체	90 (57.7%)	66 (42.3%)	156 (100%)	1 (100%)	0 (0.0%)	1 (100%)
상급 종합병원	23 (71.9%)	9 (28.1%)	32 (100%)	-	-	-
종합병원	67 (54.0%)	57 (46.0%)	124 (100%)	1 (100%)	0 (0.0%)	1 (100%)
도시(동)	88 (60.3%)	58 (39.7%)	146 (100%)	1 (100%)	0 (0.0%)	1 (100%)
비도시 (읍·면)	2 (20.0%)	8 (80.0%)	10 (100%)	-	-	-

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

반면 종합병원의 경우 '부설 노인복지시설 전산시스템'은 20.0%(1개소)로 매우 낮은 수준을 보였으며 '부설 장례식장 전산시스템'은 38.5%(37개소)로 나타났다. 또한 '부설 주차장 전산시스템'은 54.5%(67개소)로 절반 수준의 연계율을 보이는 것으로 나타났다.

종합하면 의료기관의 부대사업 관련 정보시스템은 전반적으로 병원 내 다른 정보시스템과의 연계 수준이 낮아 진료 및 행정 영역에 비해 정보 통합 및 운영 효율화 수준이 제한적인 것으로 나타났다. 특히 노인복지시설 및 장례식장 관련 시스템은 연계율이 낮아 병원 내 핵심 시스템과의 데이터 연동 및 통합 관리가 충분히 이루어지지 않고 있는 것으로 나타났다. 반면 주차장 전산시스템은 상대적으로 연계 수준이 높은 편이나 여전히 절반 수준에 머물러 있어 전반적인 부대사업 영역의 디지털 통합 수준은 아직 초기 단계에 있는 것으로 나타났다.

상급종합병원은 일부 부대사업 영역에서 비교적 높은 연계 수준을 보이고 있는 것으로 나타났으나 전체적으로는 제한적인 수준이며, 종합병원은 전반적으로 낮은 연계 수준을 보여 부대사업 영역의 정보화 및 통합 관리 체계는 아직 충분히 구축되지 않은 것으로 나타났다.

라. 외부 연계시스템 연결

〈표 5-51〉은 진료정보 관련 정보시스템과 외부 연계시스템 연결 여부를 조사한 결과를 나타낸 것이다.

'전자의무기록시스템(EMR)'은 총 응답기관(263개소) 중 247개소(93.9%)에서 외부 연계시스템과 연결되어 운영되고 있어 핵심 진료정보시스템의 대외 연계 기반이 전반적으로 높은 수준으로 구축된 것으로 나타났다. '모바일 전자의무기록시스템'은 총 응답기관(78개소) 중 72개소(92.3%)

에서 외부 연계가 이루어지고 있어 모바일 기반 환경에서도 외부 시스템과의 연동이 상당 수준 확보된 것으로 나타났다.

'처방전달시스템(OCS)'과 총 응답기관(260개소) 중 247개소(95.0%), '의료영상저장전송시스템(PACS)은 총 응답기관(262개소) 중 244개소(93.1%)에서 외부 연계가 이루어지고 있었으며 '임상검사정보시스템(LIS)'은 총 응답기관(177개소) 160개소(90.4%), '약국관리시스템'은 총 응답기관(189개소) 172개소(91.0%)로 나타나 주요 진료지원 시스템 역시 대부분 외부 연계 체계를 갖추고 있는 것으로 나타났다.

또한 '진료과 및 회송 시스템'은 총 응답기관(189개소) 중 156개소(92.9%), '진료정보교류시스템'은 총 응답기관(183개소) 중 169개소(92.3%)에서 외부 연계가 이루어지고 있어 의료기관 간 진료 연속성과 정보 공유를 위한 연계 기반도 높은 수준으로 구축된 것으로 나타났다. '건강검진정보시스템'은 총 응답기관(249개소) 중 234개소(94.0%)로 높은 외부 연계율을 보였다. 반면 '원격의료시스템'은 총 응답기관(29개소) 중 22개소(75.9%)로 다른 시스템에 비해 상대적으로 낮은 수준에 머물러 있는 것으로 나타났다.

의료기관 종별로 살펴보면 상급종합병원은 대부분의 시스템에서 종합병원보다 높은 외부 연계 수준을 보였다. '전자의무기록시스템'은 97.6%(40개소), '처방전달시스템'과 '의료영상저장전송시스템'은 각각 95.0%(38개소), 92.7%(38개소)로 나타났으며 '임상검사정보시스템'과 '약국관리시스템'도 각각 97.2%(35개소), 97.1%(34개소)로 대부분의 기관에서 외부 시스템과 연결되어 있는 것으로 나타났다. 또한 '진료과 및 회송 시스템'은 100.0%(40개소), '진료정보교류시스템'은 97.4%(38개소)로 매우 높은 수준을 보였으며 '건강검진정보시스템' 역시 97.3%(36개소)로 나타났다. 다만 '원격의료시스템'은 71.4%(5개소)로 상대적으로 낮은 수

준을 보이는 것으로 나타났다.

반면 종합병원의 경우 '전자의무기록시스템'은 93.2%(207개소), '처방전달시스템'은 95.0%(209개소), '의료영상저장전송시스템'은 93.2%(206개소)로 핵심 시스템은 높은 외부 연계 수준을 유지하고 있는 것으로 나타났다. '임상검사정보시스템'과 '약국관리시스템'은 각각 88.7%(125개소), 89.6%(138개소)로 나타났으며 '진료과 및 회송 시스템'과 '진료정보교류시스템'은 각각 90.6%(116개소), 91.0%(131개소)로 비교적 높은 수준을 보이는 것으로 나타났다. '건강검진정보시스템'은 93.4%(198개소)로 높은 수준을 유지하고 있었으며 '원격의료시스템'은 77.3%(17개소)로 여전히 낮은 수준에 머물러 있는 것으로 나타났다.

종합하면 전자의무기록시스템을 중심으로 처방전달시스템, 의료영상저장전송시스템 등 핵심 진료정보시스템은 대부분의 의료기관에서 외부 연계시스템과 연결되어 있어 의료기관 간 정보 공유 및 진료 연속성 확보를 위한 대외 연계 기반은 전반적으로 높은 수준에서 구축된 것으로 나타났다. 또한 진료과 및 회송 시스템, 진료정보교류시스템, 건강검진정보시스템 등도 높은 연계율을 보이며 의료데이터의 교환 및 활용 기반이 상당 부분 마련된 것으로 나타났다. 반면 원격의료시스템은 외부 연계 수준이 상대적으로 낮아 비대면 진료 및 원격의료 서비스 확산을 위한 인프라는 아직 충분히 확보되지 않은 것으로 나타났다.

상급종합병원은 전반적으로 외부 연계 수준이 높고 다양한 진료 및 정보교류 시스템 간 연동이 이루어지고 있는 것으로 나타난 반면 종합병원은 핵심 시스템 중심의 연계에 머무르고 있어 일부 진료지원 및 원격의료 영역에서는 연계 수준의 격차가 존재하는 것으로 나타났다.

〈표 5-51〉 의료정보시스템과 외부 연계시스템 연결 여부(진료정보)

(단위: 개소, %)

구분	전자의무기록시스템(EMR)			모바일 전자의무기록시스템(EMR)		
	예	아니오	합계	예	아니오	합계
전체	247 (93.9%)	16 (6.1%)	263 (100%)	72 (92.3%)	6 (7.7%)	78 (100%)
상급 종합병원	40 (97.6%)	1 (2.4%)	41 (100%)	24 (96.0%)	1 (4.0%)	25 (100%)
종합병원	207 (93.2%)	15 (6.8%)	222 (100%)	48 (90.6%)	5 (9.4%)	53 (100%)
도시(동)	234 (94.4%)	14 (5.6%)	248 (100%)	69 (93.2%)	5 (6.8%)	74 (100%)
비도시 (읍·면)	13 (86.7%)	2 (13.3%)	15 (100%)	3 (75.0%)	1 (25.0%)	4 (100%)
구분	처방전달시스템(OCS)			의료영상저장전송시스템(PACS)		
	예	아니오	합계	예	아니오	합계
전체	247 (95.0%)	13 (5.0%)	260 (100%)	244 (93.1%)	18 (6.9%)	262 (100%)
상급 종합병원	38 (95.0%)	2 (5.0%)	40 (100%)	38 (92.7%)	3 (7.3%)	41 (100%)
종합병원	209 (95.0%)	11 (5.0%)	220 (100%)	206 (93.2%)	15 (6.8%)	221 (100%)
도시(동)	232 (94.7%)	13 (5.3%)	245 (100%)	229 (92.7%)	18 (7.3%)	247 (100%)
비도시 (읍·면)	15 (100%)	0 (0.0%)	15 (100%)	15 (100%)	0 (0.0%)	15 (100%)
구분	임상검사정보시스템(LIS)			약국관리시스템		
	예	아니오	합계	예	아니오	합계
전체	160 (90.4%)	17 (9.6%)	177 (100%)	172 (91.0%)	17 (9.0%)	189 (100%)
상급 종합병원	35 (97.2%)	1 (2.8%)	36 (100%)	34 (97.1%)	1 (2.9%)	35 (100%)
종합병원	125 (88.7%)	16 (11.3%)	141 (100%)	138 (89.6%)	16 (10.4%)	154 (100%)
도시(동)	153 (91.1%)	15 (8.9%)	168 (100%)	165 (92.2%)	14 (7.8%)	179 (100%)
비도시 (읍·면)	7 (77.8%)	2 (22.2%)	9 (100%)	7 (70.0%)	3 (30.0%)	10 (100%)

구분	진료과 및 회송 시스템(상/하/원)			진료정보교류시스템(복지부)		
	예	아니오	합계	예	아니오	합계
전체	156 (92.9%)	12 (7.1%)	168 (100%)	169 (92.3%)	14 (7.7%)	183 (100%)
상급 종합병원	40 (100%)	0 (0.0%)	40 (100%)	38 (97.4%)	1 (2.6%)	39 (100%)
종합병원	116 (90.6%)	12 (9.4%)	128 (100%)	131 (91.0%)	13 (9.0%)	144 (100%)
도시(동)	150 (94.3%)	9 (5.7%)	159 (100%)	162 (93.1%)	12 (6.9%)	174 (100%)
비도시 (읍·면)	6 (66.7%)	3 (33.3%)	9 (100%)	7 (77.8%)	2 (22.2%)	9 (100%)
구분	원격의료시스템			건강검진정보시스템		
	예	아니오	합계	예	아니오	합계
전체	22 (75.9%)	7 (24.1%)	29 (100%)	234 (94.0%)	15 (6.0%)	249 (100%)
상급 종합병원	5 (71.4%)	2 (28.6%)	7 (100%)	36 (97.3%)	1 (2.7%)	37 (100%)
종합병원	17 (77.3%)	5 (22.7%)	22 (100%)	198 (93.4%)	14 (6.6%)	212 (100%)
도시(동)	21 (75.0%)	7 (25.0%)	28 (100%)	222 (94.5%)	13 (5.5%)	235 (100%)
비도시 (읍·면)	1 (100%)	0 (0.0%)	1 (100%)	12 (85.7%)	2 (14.3%)	14 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

〈표 5-52〉는 환자 서비스 관련 정보시스템과 외부 연계시스템 연결 여부를 조사한 결과를 나타낸 것이다.

'의료기관 포털(대표 홈페이지)'은 총 응답기관(255개소) 중 132개소(51.8%)에서 외부 연계시스템과 연결되어 운영되고 있어 절반 수준에서만 대외 연계가 이루어지고 있는 것으로 나타났다. 반면 '의료기관 포털(웹 기반 개인건강기록, PHR)'은 총 응답기관(40개소) 중 37개소(92.5%)에서 외부 연계가 이루어지고 있어 해당 시스템을 도입한 기관에서는 대부분 외부 시스템과의 연계가 함께 구축된 것으로 나타났다. '모

바일 개인건강기록(PHR)'은 총 응답기관(67개소) 중 61개소(91.0%)에서 외부 연계가 이루어지고 있어 높은 수준을 보이는 것으로 나타났다.

〈표 5-52〉 의료정보시스템과 외부 연계시스템 연결 여부(환자 서비스)

(단위: 개소, %)

구분	의료기관 포털(대표 홈페이지)			의료기관 포털(웹) 기반 개인건강기록(PHR)		
	예	아니오	합계	예	아니오	합계
전체	132 (51.8%)	123 (48.2%)	255 (100%)	37 (92.5%)	3 (7.5%)	40 (100%)
상급 종합병원	37 (92.5%)	3 (7.5%)	40 (100%)	18 (94.7%)	1 (5.3%)	19 (100%)
종합병원	95 (44.2%)	120 (55.8%)	215 (100%)	19 (90.5%)	2 (9.5%)	21 (100%)
도시(동)	129 (53.8%)	111 (46.2%)	240 (100%)	36 (92.3%)	3 (7.7%)	39 (100%)
비도시 (읍·면)	3 (20.0%)	12 (80.0%)	15 (100%)	1 (100%)	0 (0.0%)	1 (100%)
구분	모바일 개인건강기록(PHR)			여백		
	예	아니오	합계			
전체	61 (91.0%)	6 (9.0%)	67 (100%)			
상급 종합병원	31 (93.9%)	2 (6.1%)	33 (100%)			
종합병원	30 (88.2%)	4 (11.8%)	34 (100%)			
도시(동)	60 (90.9%)	6 (9.1%)	66 (100%)			
비도시 (읍·면)	1 (100%)	0 (0.0%)	1 (100%)			

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

의료기관 종별로 살펴보면 상급종합병원은 모든 항목에서 종합병원보다 높은 외부 연계 수준을 보였다. '의료기관 포털(대표 홈페이지)'은 92.5%(37개소)가 외부 시스템과 연계되어 있었으며 '웹 기반 개인건강기

록'과 '모바일 개인건강기록'도 각각 94.7%(18개소), 93.9%(31개소)로 대부분의 기관에서 외부 연계가 이루어지고 있는 것으로 나타났다.

반면 종합병원의 경우 '의료기관 포털(대표 홈페이지)'은 44.2%(95개소)로 상급종합병원에 비해 낮은 수준을 보였다. '웹 기반 개인건강기록'과 '모바일 개인건강기록'은 각각 90.5%(19개소), 88.2%(30개소)로 나타나 도입된 기관에서는 비교적 높은 외부 연계 수준을 보였으나 전체적으로는 제한적인 수준에 머물러 있는 것으로 나타났다.

종합하면 환자용 정보시스템 중 개인건강기록(PHR) 기반 서비스는 도입된 기관을 중심으로 외부 시스템과의 연계가 비교적 잘 이루어지고 있는 반면 의료기관 포털(대표 홈페이지)은 절반 수준에서만 외부 연계가 이루어지고 있어 단순 정보 제공 기능 중심으로 운영되는 경우가 상당한 것으로 나타났다.

상급종합병원은 환자용 디지털 서비스 전반에서 외부 연계를 적극적으로 구축하고 있는 것으로 나타난 반면 종합병원은 일부 시스템에 한정된 연계에 머무르고 있어 환자 참여형 서비스의 대외 확장성과 활용 수준은 상대적으로 낮은 것으로 나타났다.

〈표 5-53〉은 진료 지원 및 경영 정보 관련 정보시스템과 외부 연계시스템 연결 여부를 조사한 결과를 나타낸 것이다.

'원무관리·보험청구 청구시스템'은 총 응답기관(254개소) 중 233개소(91.7%)에서 외부 연계시스템과 연결되어 운영되고 있어 행정·청구 기능과 외부 시스템 간 연계는 대부분의 기관에서 구축된 것으로 나타났다. 반면 '전자적 자원관리시스템(ERP)'은 총 응답기관(183개소) 중 103개소(56.3%)에서 외부 연계가 이루어져 절반 수준에 머물러 있었으며 경영자원 통합 시스템의 대외 연계는 상대적으로 미흡한 것으로 나타났다. '내부직원지원시스템(ESS)'은 총 응답기관(81개소) 중 61개소(75.3%)에

서 외부 연계가 이루어지고 있었으며 '전사적 데이터웨어하우스(EDW)'는 총 응답기관(61개소) 중 52개소(85.2%)에서 외부 시스템과 연결되어 운영되고 있어 해당 시스템을 도입한 기관에서는 대외 연계가 비교적 활발하게 이루어지고 있는 것으로 나타났다.

의료기관 종별로 살펴보면 상급종합병원은 전반적으로 높은 외부 연계 수준을 보였다. '원무관리·보험청구 청구시스템'은 100.0%(38개소)가 외부 시스템과 연계되어 있었으며 '전자적 자원관리시스템'은 96.0%(24개소)로 매우 높은 수준을 나타냈다. 또한 '내부직원지원시스템'과 '전사적 데이터웨어하우스'도 각각 91.7%(22개소), 88.5%(23개소)로 대부분의 기관에서 외부 연계가 이루어지고 있는 것으로 나타났다.

반면 종합병원의 경우 '원무관리·보험청구 청구시스템'은 90.3%(195개소)로 높은 수준을 유지하고 있었으나 '전자적 자원관리시스템'은 50.0%(79개소)로 절반 수준에 머물러 있는 것으로 나타났다. '내부직원지원시스템'은 68.4%(39개소)로 나타났으며 '전사적 데이터웨어하우스'는 82.9%(29개소)로 도입된 기관 내에서는 비교적 높은 외부 연계 수준을 보이는 것으로 나타났다.

종합하면 원무관리·보험청구 시스템을 중심으로 한 행정·재정 정보의 외부 연계는 대부분의 의료기관에서 안정적으로 구축되어 있는 반면 전자적 자원관리시스템(ERP) 등 경영자원 통합 시스템의 외부 연계 수준은 상대적으로 낮아 병원 운영 전반의 대외 연계 기반은 아직 충분히 확산되지 않은 것으로 나타났다. 또한 내부직원지원시스템과 전사적 데이터웨어하우스는 도입된 기관을 중심으로는 높은 외부 연계 수준을 보이고 있으나 전체적인 확산 수준이 제한적이어서 데이터 기반 경영 및 외부 데이터 활용 체계는 일부 기관에 국한되어 있는 것으로 나타났다.

한편 상급종합병원은 경영·인사·데이터 관리 영역까지 포함한 대외 연

계를 적극적으로 구축하고 있는 것으로 나타난 반면 종합병원은 원무·청구 등 기본 행정 기능 중심의 연계에 머무르고 있어 경영정보 고도화 및 외부 연계 활용 수준에서 차이가 나타나는 것으로 나타났다.

〈표 5-53〉 의료정보시스템과 외부 연계시스템 연결 여부(진료 지원 및 경영 정보)

(단위: 개소, %)

구분	원무관리, 보험청구시스템			전자적 자원관리시스템(ERP)		
	예	아니오	합계	예	아니오	합계
전체	233 (91.7%)	21 (8.3%)	254 (100%)	103 (56.3%)	80 (43.7%)	183 (100%)
상급 종합병원	38 (100%)	0 (0.0%)	38 (100%)	24 (96.0%)	1 (4.0%)	25 (100%)
종합병원	195 (90.3%)	21 (9.7%)	216 (100%)	79 (50.0%)	79 (50.0%)	158 (100%)
도시(동)	223 (93.3%)	16 (6.7%)	239 (100%)	98 (57.0%)	74 (43.0%)	172 (100%)
비도시 (읍·면)	10 (66.7%)	5 (33.3%)	15 (100%)	5 (45.5%)	6 (54.5%)	11 (100%)
구분	내부직원지원시스템(ESS)			전사적데이터웨어하우스(EDW)		
	예	아니오	합계	예	아니오	합계
전체	61 (75.3%)	20 (24.7%)	81 (100%)	52 (85.2%)	9 (14.8%)	61 (100%)
상급 종합병원	22 (91.7%)	2 (8.3%)	24 (100%)	23 (88.5%)	3 (11.5%)	26 (100%)
종합병원	39 (68.4%)	18 (31.6%)	57 (100%)	29 (82.9%)	6 (17.1%)	35 (100%)
도시(동)	59 (76.6%)	18 (23.4%)	77 (100%)	50 (86.2%)	8 (13.8%)	58 (100%)
비도시 (읍·면)	2 (50.0%)	2 (50.0%)	4 (100%)	2 (66.7%)	1 (33.3%)	3 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

〈표 5-54〉은 교육 및 연구 관련 정보시스템과 외부 연계시스템 연결 여부를 조사한 결과를 나타낸 것이다.

'보수교육 전산시스템'은 총 응답기관(56개소) 중 25개소(44.6%)에서

외부 연계시스템과 연결되어 운영되고 있어 절반에 미치지 못하는 수준으로 나타났다. '조사연구 전산시스템'은 총 응답기관(40개소) 중 27개소(67.5%)에서 외부 연계가 이루어지고 있어 보수교육 전산시스템에 비해 상대적으로 높은 수준을 보였으나 여전히 제한적인 수준에 머물러 있는 것으로 나타났다.

〈표 5-54〉 의료정보시스템과 외부 연계시스템 연결 여부(교육 및 연구)

(단위: 개소, %)

구분	보수교육 전산시스템			조사연구 전산시스템		
	예	아니오	합계	예	아니오	합계
전체	25 (44.6%)	31 (55.4%)	56 (100%)	27 (67.5%)	13 (32.5%)	40 (100%)
상급 종합병원	11 (52.4%)	10 (47.6%)	21 (100%)	14 (73.7%)	5 (26.3%)	19 (100%)
종합병원	14 (40.0%)	21 (60.0%)	35 (100%)	13 (61.9%)	8 (38.1%)	21 (100%)
도시(동)	24 (44.4%)	30 (55.6%)	54 (100%)	26 (66.7%)	13 (33.3%)	39 (100%)
비도시 (읍·면)	1 (50.0%)	1 (50.0%)	2 (100%)	1 (100%)	0 (0.0%)	1 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

의료기관 종별로 살펴보면 상급종합병원은 종합병원보다 높은 외부 연계 수준을 보였다. '보수교육 전산시스템'은 52.4%(11개소), '조사연구 전산시스템'은 73.7%(14개소)에서 외부 연계가 이루어지고 있어 교육 및 연구 기능과 외부 시스템 간 연계가 비교적 활발하게 이루어지고 있는 것으로 나타났다. 반면 종합병원의 경우 '보수교육 전산시스템'은 40.0%(14개소), '조사연구 전산시스템'은 61.9%(13개소)로 나타나 상급종합병원에 비해 전반적인 외부 연계 수준이 낮은 것으로 나타났다.

종합하면 의료기관의 교육 및 연구 관련 정보시스템은 외부 연계 수준

이 전반적으로 낮아 진료 및 행정 영역에 비해 대외 데이터 활용 및 협력 기반이 충분히 구축되지 않은 것으로 나타났다. 특히 보수교육 전산시스템은 외부 연계율이 낮아 교육 이력 관리 및 외부 교육체계와의 연동이 제한적인 것으로 나타났으며, 조사연구 전산시스템 역시 일부 기관에 한정된 연계가 이루어지고 있어 연구데이터의 공유 및 협력 기반은 아직 초기 단계에 머물러 있는 것으로 나타났다.

한편 상급종합병원은 교육·연구 분야에서 외부 연계를 비교적 적극적으로 구축하고 있는 것으로 나타난 반면 종합병원은 진료 및 행정 중심의 정보시스템에 집중되어 있어 교육·연구 영역의 외부 연계 수준은 상대적으로 미흡한 것으로 나타났다.

〈표 5-55〉는 기타 부대사업 관련 정보시스템과 외부 연계시스템 연결 여부를 조사한 결과를 나타낸 것이다.

부설 노인복지시설 전산시스템'은 총 응답기관(6개소) 중 1개소(16.7%)에서 외부 연계시스템과 연결되어 운영되고 있어 외부 연계 수준이 매우 제한적인 것으로 나타났다. '부설 장례식장 전산시스템'은 총 응답기관(117개소) 중 47개소(40.2%)에서 외부 연계가 이루어지고 있어 절반에 미치지 못하는 수준을 보였으며, '부설 주차장 전산시스템'은 총 응답기관(156개소) 중 90개소(57.7%)로 상대적으로 높은 외부 연계율을 보이는 것으로 나타났다. '기타 시스템'은 1개소(100%)에서 외부 연계가 이루어졌으나 사례 수가 매우 적어 일반화에는 한계가 있었다.

종합하면 의료기관의 부대사업 관련 정보시스템은 전반적으로 외부 연계 수준이 낮아 진료 및 행정 영역에 비해 대외 연계 및 데이터 활용 기반이 제한적인 것으로 나타났다. 특히 노인복지시설 및 장례식장 관련 시스템은 외부 연계율이 낮아 관련 서비스 간 정보 공유 및 통합 운영이 충분히 이루어지지 않고 있는 것으로 나타났다. 반면 주차장 전산시스템은 상

대적으로 높은 외부 연계 수준을 보였으나 절반 수준에 머물러 있어 부대사업 전반의 디지털 연계 수준은 초기 단계에 있는 것으로 나타났다.

〈표 5-55〉 의료정보시스템과 외부 연계시스템 연결 여부(기타 부대사업)

(단위: 개소, %)

구분	부설 노인복지시설 전산시스템			부설 장례식장 전산시스템		
	예	아니오	합계	예	아니오	합계
전체	1 (16.7%)	5 (83.3%)	6 (100%)	47 (40.2%)	70 (59.8%)	117 (100%)
상급 종합병원	0 (0.0%)	1 (100%)	1 (100%)	10 (47.6%)	11 (52.4%)	21 (100%)
종합병원	1 (20.0%)	4 (80.0%)	5 (100%)	37 (38.5%)	59 (61.5%)	96 (100%)
도시(동)	1 (20.0%)	4 (80.0%)	5 (100%)	44 (40.0%)	66 (60.0%)	110 (100%)
비도시 (읍·면)	0 (0.0%)	1 (100%)	1 (100%)	3 (42.9%)	4 (57.1%)	7 (100%)
구분	부설 주차장 전산시스템			기타		
	예	아니오	합계	예	아니오	합계
전체	90 (57.7%)	66 (42.3%)	156 (100%)	1 (100%)	0 (0.0%)	1 (100%)
상급 종합병원	23 (71.9%)	9 (28.1%)	32 (100%)	-	-	-
종합병원	67 (54.0%)	57 (46.0%)	124 (100%)	1 (100%)	0 (0.0%)	1 (100%)
도시(동)	88 (60.3%)	58 (39.7%)	146 (100%)	1 (100%)	0 (0.0%)	1 (100%)
비도시 (읍·면)	2 (20.0%)	8 (80.0%)	10 (100%)	-	-	-

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

한편 상급종합병원은 일부 부대사업 영역에서 비교적 높은 외부 연계 수준을 보이고 있는 것으로 나타났으나 전체적으로는 제한적인 수준이며, 종합병원은 전반적으로 낮은 연계 수준을 보여 부대사업 영역의 대외 연계 및 통합 운영 체계는 아직 충분히 구축되지 않은 것으로 나타났다.

마. 클라우드 서비스 도입

〈표 5-56〉은 클라우드 서비스 도입 현황과 관련하여 진료정보 관련 정보시스템과 환자 서비스 관련 정보시스템을 구분하여 조사한 결과를 나타낸 것이다.

클라우드 서비스 도입 현황에 응답한 263개 응답기관을 기준으로 볼 때 '진료정보(EMR, OCS, PACS) 클라우드 서비스'는 22개소(8.4%)에서 도입되어 대부분의 기관이 여전히 온프레미스 기반으로 운영하고 있는 것으로 나타났다. 반면 '환자 서비스(포털, 웹) 클라우드 서비스'는 46개소(17.5%)에서 도입되어 진료정보 시스템에 비해 상대적으로 높은 수준을 보였으나 전반적으로는 낮은 도입률에 머물러 있는 것으로 나타났다.

의료기관 종별로 살펴보면 상급종합병원은 '진료정보 클라우드 서비스' 17.1%(7개소), '환자 서비스 클라우드 서비스' 36.6%(15개소)로 나타나 종합병원보다 높은 도입 수준을 보였다. 특히 환자 서비스 영역에서는 비교적 적극적인 클라우드 활용이 이루어지고 있는 것으로 나타났다.

〈표 5-56〉 클라우드 서비스 도입 현황

(단위: 개소, %)

구분	진료정보(EMR, OCS, PACS)			환자 서비스(포털, 웹)		
	도입	미도입	합계	도입	미도입	합계
전체	22 (8.4%)	241 (91.6%)	263 (100%)	46 (17.5%)	217 (82.5%)	263 (100%)
상급 종합병원	7 (17.1%)	34 (82.9%)	41 (100%)	15 (36.6%)	26 (63.4%)	41 (100%)
종합병원	15 (6.8%)	207 (93.2%)	222 (100%)	31 (14.0%)	191 (86.0%)	222 (100%)
도시(동)	22 (8.9%)	226 (91.1%)	248 (100%)	45 (18.1%)	203 (81.9%)	248 (100%)
비도시 (읍·면)	0 (0.0%)	15 (100%)	15 (100%)	1 (6.7%)	14 (93.3%)	15 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

반면, 종합병원의 경우 '진료정보 클라우드 서비스'는 6.8%(15개소), '환자 서비스 클라우드 서비스'는 14.0%(31개소)로 나타나 상급종합병원에 비해 전반적인 도입 수준이 낮은 것으로 확인되었다.

종합하면 의료기관의 클라우드 서비스 도입은 전반적으로 낮은 수준에 머물러 있는 것으로 나타났다. 상급종합병원은 디지털 전환 및 서비스 고도화를 위해 클라우드 도입을 점진적으로 확대하고 있는 반면, 종합병원은 기존 시스템 유지 중심의 운영으로 인해 클라우드 전환이 제한적인 수준에 머물러 있는 것으로 평가된다.

5. 의료정보시스템 정보화 담당조직 및 인력

가. 정보화 엄무 전담 부서

정보보안 관점에서 정보시스템의 정보화·정보보안·개인정보보호 담당 조직과 인력은 조직의 핵심 자산과 비즈니스 연속성을 보호하고 관련 법규를 준수하며 잠재적인 위험을 사전에 예방하고 신속하게 대응하는 데 있어 핵심적인 역할을 수행하는 주체이다.

〈표 5-57〉은 정보화 업무 전담 부서 여부를 조사한 결과를 나타낸 것이다.

의료정보시스템 구축 및 운영 등 정보화 업무를 담당하는 전담부서 유무에 대해 전체 응답기관(263개 의료기관)을 대상으로 조사한 결과, 89.4%(235개소)가 전담부서가 있다고 응답하였으며 10.6%(28개소)는 전담부서가 없다고 응답한 것으로 나타났다. 의료기관 종별로 살펴보면 상급종합병원(41개소)의 경우 100.0%(41개소)가 전담부서를 운영하고 있는 것으로 나타난 반면, 종합병원(222개소)의 경우 87.4%(194개소)만

이 전담부서를 운영하고 있는 것으로 나타났다.

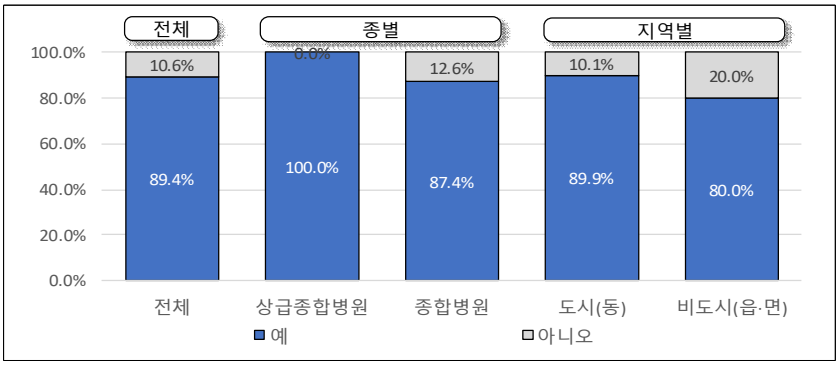
〈표 5-57〉 정보화 업무 전담 부서 여부

(단위: 개소, %)

구분		예	아니오	합계
전체	전체	235 (89.4%)	28 (10.6%)	263 (100%)
종별	상급종합병원	41 (100%)	0 (0.0%)	41 (100%)
	종합병원	194 (87.4%)	28 (12.6%)	222 (100%)
지역별	도시(동)	223 (89.9%)	25 (10.1%)	248 (100%)
	비도시(읍·면)	12 (80.0%)	3 (20.0%)	15 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

〔그림 5-12〕 정보화 업무 전담 부서 여부



출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

나. 정보화 업무 담당 인력

〈표 5-58〉은 정보화 담당 인력 현황을 조사한 결과를 나타낸 것이다.

전체 응답기관(263개소)의 정보화 업무 담당 인력 현황을 살펴보면 평균 인력 규모는 '개발자'(8.3명)가 가장 많았으며, 다음으로 '정보시스템 담당자'(2.2명), '관리자'(1.4명), '네트워크 담당자'(1.0명), '정보보안 담

당자'(0.9명), '정보보호 담당자'(0.9명) 순으로 나타났다.

종합하면 의료기관의 정보화 인력 구조는 개발 및 시스템 운영 인력 중심으로 구성되어 있으며 정보보안 및 개인정보보호 인력은 상대적으로 부족한 것으로 나타났다. 일부 기관에서는 보안 전담 인력 없이 운영되는 사례도 확인되어 의료기관의 사이버 보안 대응 역량은 기관 규모에 따라 차이가 나타날 가능성이 있는 것으로 보인다. 특히 중소 규모 의료기관을 중심으로 보안 전문 인력 확충과 정책적 지원이 필요한 것으로 나타났다.

〈표 5-58〉 정보화 업무 담당 인력 현황

(단위: 명)

구분	관리자	정보보안 담당자	정보보호 담당자	네트워크 담당자	개발자	정보시스템 담당자
평균	1.4	0.9	0.9	1	8.3	2.2
표준편차	2.2	1.3	1.1	1.3	15.9	3.7
최소값	0	0	0	0	0	0
Q1.25%	0.5	0.3	0.4	0.3	0.5	0.5
중간값.50%	1	0.5	0.5	0.5	1.1	1
Q3.75%	1	1	1	1.1	10.6	2
최대값	22	16	11	16	126	40
상위10평균	5.9	2.9	2.9	2.8	42.1	10.5
하위10평균	0.2	0	0	0	0	0.2

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

〈표 5-59〉은 종별, 지역별 정보화 담당 인력 현황을 조사한 결과를 나타낸 것이다.

정보화 업무 담당 인력을 의료기관 종별로 살펴보면 전반적으로 상급종합병원이 종합병원에 비해 모든 직군에서 평균 인력 규모가 높은 것으로 나타났다. '관리자'는 상급종합병원(평균 3명)이 종합병원(1.1명)보다

약 3배 많은 것으로 나타났으며, '정보보안 담당자' 역시 상급종합병원 1.9명, 종합병원 0.7명으로 상급종합병원이 더 많은 인력을 보유하고 있는 것으로 나타났다. '정보보호 담당자' 또한 상급종합병원 1.9명, 종합병원 0.7명으로 유사한 격차가 나타났다. '네트워크 담당자'는 상급종합병원 1.8명, 종합병원 0.8명으로 나타났으며, '개발자'의 경우 상급종합병원 24.3명, 종합병원 5.4명으로 약 4.5배 이상의 큰 차이를 보이는 것으로 나타났다. '정보시스템 담당자' 역시 상급종합병원 5.4명, 종합병원 2.3명으로 나타나 전반적으로 상급종합병원이 인력 규모 측면에서 우위에 있는 것으로 나타났다.

〈표 5-59〉 종별 지역별 정보화 업무 담당 인력 현황

(단위: 명)

구분			평균	표준편차	최소값	중앙값	최대값
관리자	종별	상급종합병원	3	4.4	0	2	22
		종합병원	1.1	1.2	0	1	9
	지역별	도시(동)	1.4	2.2	0	1	22
		비도시(읍·면)	1.2	1.2	0.1	0.5	5
정보 보안 담당자	종별	상급종합병원	1.9	2.6	0.5	1	16
		종합병원	0.7	0.7	0	0.5	4
	지역별	도시(동)	0.9	1.3	0	0.5	16
		비도시(읍·면)	0.9	0.9	0.1	0.5	3
정보 보호 담당자	종별	상급종합병원	1.9	2.1	0	1	11
		종합병원	0.7	0.7	0	0.5	4
	지역별	도시(동)	0.9	1.1	0	0.5	11
		비도시(읍·면)	0.9	0.8	0.1	0.5	3
네트 워크 담당자	종별	상급종합병원	1.8	1	0	2	5
		종합병원	0.8	1.3	0	0.5	16
	지역별	도시(동)	1	1.3	0	0.5	16
		비도시(읍·면)	0.9	0.8	0.1	0.5	3

구분			평균	표준편차	최소값	중앙값	최대값
개발자	종별	상급종합병원	24.3	23.1	0	18	126
		종합병원	5.4	12.1	0	1	100
	지역별	도시(동)	8.6	16.2	0	1.1	126
		비도시(읍·면)	3.5	6.1	0	1	21
정보 시스템 담당자	종별	상급종합병원	5.4	6.7	0	4	40
		종합병원	1.6	2.5	0	1	20
	지역별	도시(동)	2.3	3.8	0	1	40
		비도시(읍·면)	1.4	1.3	0.1	1	5

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

종합하면 정보화 업무 담당 인력은 상급종합병원에 집중되어 있으며 특히 개발 및 시스템 운영 인력에서 이러한 격차가 두드러지게 나타나는 것으로 나타났다. 반면 정보보안 및 개인정보보호 인력은 전반적으로 평균 규모가 1명 미만 수준에 머물러 있는 것으로 나타났으며 종별 구분과 관계없이 최소 인력 또는 겸직 형태로 운영되는 경우가 많은 것으로 나타났다. 이는 의료기관의 정보보안 대응 역량이 기관 규모에 따라 불균형하게 나타날 가능성이 있음을 보여준다. 특히 종합병원을 중심으로 보안 전문 인력 확충과 제도적 지원이 필요함을 시사한다.

〈표 5-60〉은 정보화 담당 인력 중 내부 인력 비중을 조사한 결과를 나타낸 것이다.

전체 응답기관의 정보화 및 정보보안 관련 담당 인력 중 내부 인력 비중을 살펴보면 평균적으로 '관리자' 92.6%, '정보보안 담당자' 86.5%, '정보보호 담당자' 90.8%, '정보시스템 담당자' 79.4%로 대부분 직군에서 내부 인력 중심으로 운영되고 있는 것으로 나타났다. 반면 '네트워크 담당자'는 74.0%, '개발자'는 66.9%로 상대적으로 내부 인력 비중이 낮은 것으로 나타나 일부 기능에서는 외부 인력에 대한 의존이 존재하는 것으로 나타났다.

종합하면 의료기관의 정보화 업무는 전반적으로 내부 인력 중심으로 운영되고 있는 것으로 나타났으나 네트워크 및 개발 분야를 중심으로 외부 인력 의존도가 상대적으로 높게 나타나는 것으로 나타났다. 일부 기관에서는 특정 기능을 외부 인력에 위탁하여 운영하는 사례도 확인되었다. 이러한 구조는 핵심 보안 영역에 대한 내부 통제 역량 확보 측면에서 한계로 작용할 가능성이 있으며, 보안 및 시스템 운영의 안정성을 확보하기 위해 내부 전문 인력 확충과 외주 관리 체계 강화가 필요한 것으로 나타났다.

〈표 5-60〉 정보화 업무 담당 내부 인력 비중

(단위: 명, %)

구분	관리자	정보보안 담당자	정보보호 담당자	네트워크 담당자	개발자	정보시스템 담당자
n	259	244	245	241	222	257
평균	92.6	86.5	90.8	74	66.9	79.4
표준편차	20.4	26.6	22.5	36	40.8	32
최소값	0	0	0	0	0	0
Q1.25%	100	100	100	50	26.4	50
중간값.50%	100	100	100	100	100	100
Q3.75%	100	100	100	100	100	100
최대값	100	100	100	100	100	100
상위10평균	100	100	100	100	100	100
하위10평균	37.3	35.3	36	0	0	11

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

〈표 5-61〉은 정보화 담당 인력 중 내부 인력 비중을 종별, 지역별로 조사한 결과를 나타낸 것이다. 정보화 업무 담당 인력의 내부 인력 비중을 의료기관 종별로 살펴보면, 전반적으로 종합병원이 상급종합병원에 비해 대부분 직군에서 내부 인력 비중이 높은 것으로 나타났다. '관리자'는 종합병원 93.8%, 상급종합병원 86.1%로 7.0%p의 차이를 보였으며, '정보보안

담당자'는 종합병원 86.9%, 상급종합병원 84.2%로 나타났다. '정보보호 담당자'는 상급종합병원 95.9%로 가장 높았으며 종합병원은 89.8%로 나타났다. '네트워크 담당자'는 종합병원 76.9%, 상급종합병원 59.1%로 17.0%p의 큰 차이를 보였으며, '개발자'는 종합병원 68.0%, 상급종합병원 61.3%로 나타났다. 또한 '정보시스템 담당자' 역시 종합병원 81.9%, 상급종합병원 65.7%로 종합병원이 상대적으로 높은 내부 인력 비중을 보였다.

상급종합병원은 '관리자', '네트워크 담당자', '개발자', '정보시스템 담당자' 등에서 내부 인력 비중이 전체 평균보다 낮은 경향을 보여 일부 기능을 외부 인력에 의존하는 비율이 상대적으로 높은 것으로 나타났다. 반면 종합병원은 대부분 직군에서 전체 평균과 유사하거나 높은 수준을 보여 내부 인력 중심의 운영 경향이 보다 뚜렷한 것으로 나타났다.

〈표 5-61〉 종별 지역별 정보화 업무 담당 내부 인력 비중 평균

(단위: %)

구분	관리자	정보보안 담당자	정보보호 담당자	네트워크 담당자	개발자	정보시스템 담당자
전체	92.6	86.5	90.8	74	66.9	79.4
상급종합병원	86.1	84.2	95.9	59.1	61.3	65.7
종합병원	93.8	86.9	89.8	76.9	68.0	81.9
도시(동)	92.9	86.6	91.1	73.4	66.5	79.3
비도시(읍·면)	88.2	83.9	85.6	82.5	72.0	80.5

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

특히 네트워크 및 개발 분야에서 외부 인력 활용 수준의 차이가 두드러지게 나타났으며, 이는 기관 규모에 따라 정보화 인력 운영 방식에 차이가 존재함을 보여주는 결과로 나타났다. 또한 외부 인력 의존도가 높은 영역에 대해서는 내부 역량 강화와 함께 외주 관리 체계의 정교화가 필요함을 시사한다.

다. 정보화 담당인력의 충분성에 대한 의견

〈표 5-62〉는 정보보안 담당인력의 충분성에 대해 조사한 결과를 나타낸 것이다.

전체 응답기관(263개소)을 대상으로 정보보안 담당 인력의 충분성에 대해 조사한 결과, '매우 충분하다' 0.4%(1개소), '충분하다' 0.4%(1개소), '보통이다' 20.2%(53개소), '부족하다' 51.0%(134개소), '매우 부족하다' 28.1%(74개소)로 나타났다. 이를 종합하면 긍정적인 의견('매우 충분하다'+'충분하다')은 0.8%(2개소)에 불과한 반면, 부정적인 의견('부족하다'+'매우 부족하다')은 79.1%(208개소)로 나타나 대부분의 의료기관이 정보보안 담당 인력이 부족하다고 인식하고 있는 것으로 나타났다.

의료기관 종별로 살펴보면 상급종합병원(41개소)은 '매우 충분하다' 및 '충분하다' 응답이 없는 것으로 나타났으며, '보통이다' 19.5%(8개소), '부족하다' 51.2%(21개소), '매우 부족하다' 29.3%(12개소)로 나타나 부정적인 의견이 80.5%에 달하는 것으로 나타났다. 종합병원(222개소)의 경우 '매우 충분하다' 0.5%(1개소), '충분하다' 0.5%(1개소), '보통이다' 20.3%(45개소), '부족하다' 50.9%(113개소), '매우 부족하다' 27.9%(62개소)로 나타나 부정적인 의견이 78.8%로 나타났다.

종합하면 정보보안 담당 인력의 충분성에 대해 대부분의 의료기관이 부족하다고 인식하고 있는 것으로 나타났다. 이는 의료기관 전반에서 정보보안 인력 수급 문제가 구조적으로 존재함을 보여주는 결과로 나타나며, 정보보안 인력 확충을 위한 정책적 지원이 필요한 것으로 나타났다.

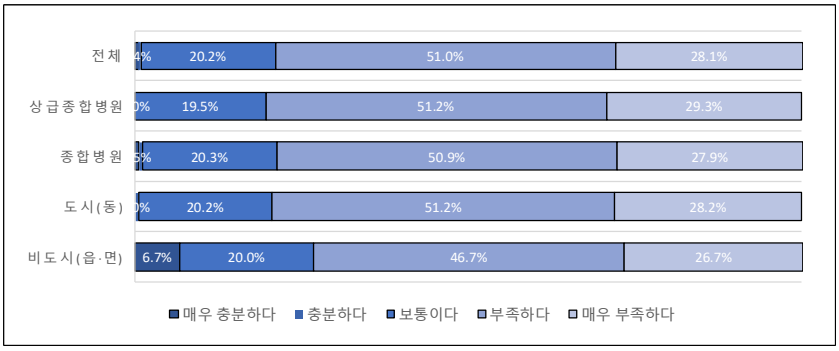
〈표 5-62〉 정보보안 담당인력 충분성에 대한 의견

(단위: 개소, %)

구분		매우 충분하다	충분하다	보통이다	부족하다	매우 부족하다	합계
전체	전체	1 (0.4%)	1 (0.4%)	53 (20.2%)	134 (51.0%)	74 (28.1%)	263 (100%)
종별	상급종합병원	0 (0.0%)	0 (0.0%)	8 (19.5%)	21 (51.2%)	12 (29.3%)	41 (100%)
	종합병원	1 (0.5%)	1 (0.5%)	45 (20.3%)	113 (50.9%)	62 (27.9%)	222 (100%)
지역별	도시(동)	0 (0.0%)	1 (0.4%)	50 (20.2%)	127 (51.2%)	70 (28.2%)	248 (100%)
	비도시(읍·면)	1 (6.7%)	0 (0.0%)	3 (20.0%)	7 (46.7%)	4 (26.7%)	15 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

[그림 5-13] 정보보안 담당인력 충분성에 대한 의견



출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

라. 정보화 담당인력 부족 문제 해결에 필요한 지원

〈표 5-63〉은 정보보안 담당인력 부족 문제 해결하기 위해 필요한 지원에 대해 조사한 결과를 나타낸 것이다.

정보보안 담당 인력이 '부족하다' 또는 '매우 부족하다'고 응답한 208

개 의료기관을 대상으로 정보보안 담당 인력 부족 문제를 해결하기 위해 필요한 지원에 대해 우선순위를 고려하여 3개를 선택하도록 한 결과, 1순위에서는 '예산 확대를 통한 인력 고용'이 75.5%로 가장 높게 나타났다. 2순위에서는 '정부의 인력 지원 및 파견'이 33.7%로 가장 높은 비율을 보였으며, 3순위에서는 '외부 전문 인력 활용 지원'이 33.7%로 가장 높게 나타났다.

〈표 5-63〉 정보보안 담당인력 부족 문제 해결에 필요한 지원(순위별 빈도)

(단위: 개소, %)

항목	1순위	2순위	3순위
정보의 인력 지원 및 파견	34 (16.3%)	70 (33.7%)	52 (25.0%)
정보보호 교육 및 훈련 프로그램 강화	5 (2.4%)	58 (27.9%)	69 (33.2%)
예산 확대를 통한 인력 고용	157 (75.5%)	35 (16.8%)	14 (6.7%)
외부 전문 인력 활용 지원	10 (4.8%)	44 (21.2%)	70 (33.7%)
기타(직접 입력)	2 (1.0%)	1 (0.5%)	3 (1.4%)
합계	208 (100%)	208 (100%)	208 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

〈표 5-64〉는 정보보안 담당인력 부족 문제 해결하기 위해 필요한 지원에 대해 우선순위에 따른 가중치(1순위 3점, 2순위 2점, 3순위 1점)를 부여하여 중요도를 산출한 결과이다.

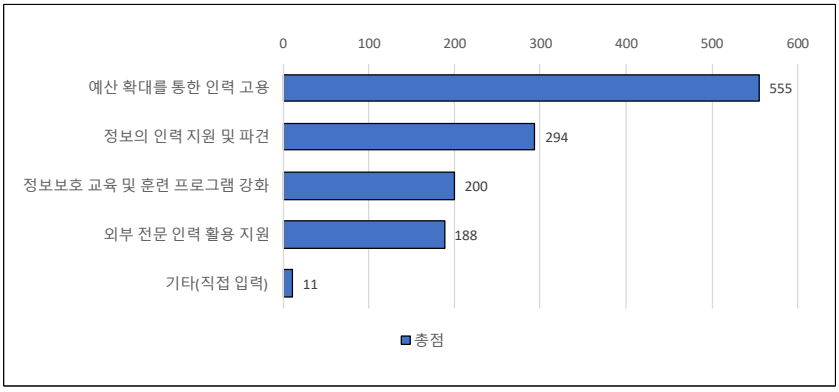
〈표 5-64〉 정보보안 담당인력 부족 문제 해결에 필요한 지원(중요도 순위)

항목	응답 수	점수	평균 점수	중요도 순위
정보의 인력 지원 및 파견	156	294	1.88	2
정보보호 교육 및 훈련 프로그램 강화	132	200	1.52	3
예산 확대를 통한 인력 고용	206	555	2.69	1
외부 전문 인력 활용 지원	124	188	1.52	4
기타	6	11	1.83	5

주: 1순위는 3점, 2순위는 2점, 1순위에는 1점의 점수를 부여하여 가중 평균 점수 산출하였음.
출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

의료기관의 정보보안 담당 인력 부족 문제를 해결하기 위해 필요한 지원은 '예산 확대를 통한 인력 고용'이 가장 높은 것으로 나타났다. 다음으로 '정부의 인력 지원 및 파견', '정보보호 교육 및 훈련 프로그램 강화', '외부 전문 인력 활용 지원', '기타' 순으로 나타났다.

〔그림 5-14〕 정보보안 담당인력 부족 문제 해결에 필요한 지원(중요도 순위)



출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

6. 정보보안(교육)

정보보안 교육은 조직의 보안 수준을 강화하고 사이버 침해사고를 예방하는 데 있어 중요한 요소 중 하나이다. 정보보안 교육은 일회성에 그치지 않고 지속적이고 실용적인 프로그램으로 운영될 필요가 있으며, 교육 대상의 역할과 책임에 따라 차별화된 방식으로 운영되는 것이 중요하다.

본 조사에서는 교육 대상을 최고정보책임자(CIO) 및 최고정보보호책임자(CISO), 전산부서원, 정보보안 담당자, 의료진, 의료진 외 전 직원 등 5개 그룹으로 구분하여 정보보안 교육의 시행 여부와 시행 주기, 참여 수준, 교육 방법 등을 조사하였다. 또한 임직원의 교육 효과와 교육 만족도,

교육 미시행 이유 등에 대해서도 함께 조사하였다.

가. 대상자별 정보보안 교육 여부 및 주기, 참석 수준, 교육 방법

1) 최고정보책임자(CIO), 정보보호 최고책임자(CISO)

의료기관의 최고정보책임자(CIO)와 최고정보보호책임자(CISO)는 기관의 정보보호 정책을 수립하고 보안관리 체계를 총괄하는 핵심 의사결정자로서, 정기적인 보안 교육을 통해 최신 보안 위협에 대응하고 전략적 관리 역량을 강화하는 것이 중요하다. 이들의 교육 시행 여부와 주기, 교육 방식은 기관의 보안관리 수준과 정책 이행의 성숙도를 평가하는 주요 지표로 활용될 수 있다.

〈표 5-65〉는 최고정보책임자(CIO)와 최고정보보호책임자(CISO)를 대상으로 한 정보보안 교육 시행 여부에 대해 조사한 결과를 나타낸 것이다.

전체 응답기관(263개소) 중 85.6%(225개소)가 의료기관 내 최고정보책임자(CIO) 또는 정보보호 최고책임자(CISO)를 대상으로 정보보안 교육을 시행하고 있는 것으로 나타났으며, 14.4%(38개소)는 교육을 시행하지 않는 것으로 나타났다.

의료기관 종별로 살펴보면 상급종합병원의 경우 95.1%(39개소)가 교육을 시행하고 있는 것으로 나타났으며, 종합병원은 83.8%(186개소)로 나타났다. 이는 상급종합병원이 종합병원에 비해 정보보안 교육 시행 수준이 높은 것으로 나타나, 기관 규모가 클수록 보안관리 체계가 제도적으로 보다 정착되어 있음을 보여주는 결과로 나타났다.

종합하면 전체적으로 10개 기관 중 8개 이상이 정보보안 책임자를 대상으로 정기적인 보안 교육을 시행하고 있는 것으로 나타나 제도적 기반

은 비교적 안정적으로 구축된 것으로 나타났다. 다만 종합병원의 경우 인력과 예산의 제약으로 인해 교육을 시행하지 못하는 사례가 일부 존재하는 것으로 나타나, 정부 또는 지자체 차원의 지원 프로그램을 통해 교육 참여를 확대할 필요가 있는 것으로 나타났다.

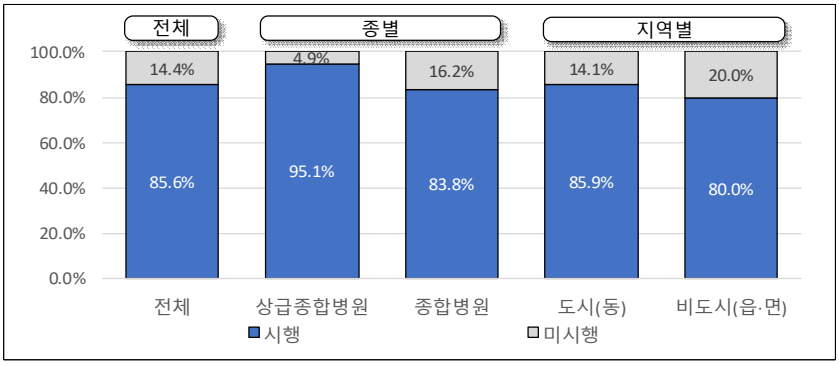
〈표 5-65〉 정보보안 교육 시행 여부(CIO, CISO)

(단위: 개소, %)

구분		시행	미시행	합계
전체	전체	225 (85.6%)	38 (14.4%)	263 (100%)
종별	상급종합병원	39 (95.1%)	2 (4.9%)	41 (100%)
	종합병원	186 (83.8%)	36 (16.2%)	222 (100%)
지역별	도시(동)	213 (85.9%)	35 (14.1%)	248 (100%)
	비도시(읍·면)	12 (80.0%)	3 (20.0%)	15 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

[그림 5-15] 정보보안 교육 시행 여부(CIO, CISO)



출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

〈표 5-66〉은 최고정보책임자(CIO) 및 최고정보보호책임자(CISO)를 대상으로 실시한 정보보안 교육 시행 주기에 대해 조사한 결과를 나타낸 것이다.

의료기관의 최고정보책임자(CIO) 및 최고정보보호책임자(CISO)를 대상으로 정보보안 교육을 실시한다고 응답한 의료기관(225개소)을 기준으로 교육 시행 주기를 살펴보면, 85.3%(192개소)가 연 1회 주기로 교육을 시행하고 있는 것으로 나타났다. 다음으로 반기 8.9%(20개소), 비정기 3.1%(7개소), 분기 2.7%(6개소) 순으로 나타나 대부분의 기관이 최소 연 1회 이상 정기적인 정보보안 교육을 운영하고 있는 것으로 나타났다.

의료기관 종별로 살펴보면 상급종합병원(39개소)은 87.2%(34개소)가 연 1회 주기로 교육을 시행하고 있었으며, 반기 5.1%(2개소), 비정기 7.7%(3개소)로 나타났다. 종합병원(186개소)은 연 1회 84.9%(158개소), 반기 9.7%(18개소), 분기 3.2%(6개소), 비정기 2.2%(4개소)로 나타나 상급종합병원과 유사한 분포를 보이는 것으로 나타났다.

〈표 5-66〉 정보보안 교육 시행 주기(CIO, CISO)

(단위: 개소, %)

구분		분기	반기	년1회	비정기	합계
전체	전체	6 (2.7%)	20 (8.9%)	192(85.3%)	7 (3.1%)	225 (100%)
종별	상급종합병원	0 (0.0%)	2 (5.1%)	34 (87.2%)	3 (7.7%)	39 (100%)
	종합병원	6 (3.2%)	18 (9.7%)	158 (84.9%)	4 (2.2%)	186 (100%)
지역별	도시(동)	5 (2.3%)	19 (8.9%)	182 (85.4%)	7 (3.3%)	213 (100%)
	비도시(읍·면)	1 (8.3%)	1 (8.3%)	10 (83.3%)	0 (0.0%)	12 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

종합하면 전체 의료기관의 85% 이상이 최고정보책임자(CIO) 및 최고정보보호책임자(CISO)를 대상으로 연 1회 정기적인 정보보안 교육을 실시하고 있는 것으로 나타났으며, 일부 기관에서는 반기 또는 분기 단위의 교육도 운영되고 있는 것으로 나타났다. 또한 상급종합병원과 종합병원 간 교육 주기와 비율이 전반적으로 유사하게 나타나, 기관 규모와 관계없이 보안관리 책임자를 대상으로 한 정기적 교육이 비교적 안정적으로 운

영되고 있는 것으로 나타났다.

〈표 5-67〉은 최고정보책임자(CIO) 및 최고정보보호책임자(CISO)를 대상으로 실시한 정보보안 교육 참석 수준에 대해 조사한 결과를 나타낸 것이다.

의료기관의 최고정보책임자(CIO) 및 최고 정보보호 책임자(CISO)를 대상으로 정보보안 교육을 한다고 응답한 의료기관(225개소) 중 67.6%(152개소)가 '반드시 참여함(80~100%)'으로 응답하였으며, 20.0%(45개소)이 '대체로 참여함(60~79%)', 10.2%(23개소)가 '보통(40~59%)', 1.3%(3개소)가 '거의 참여하지 않음(20~39%)', 0.9%(2개소)가 '전혀 참여하지 않음(0~19%)'으로 나타났다. 전체적으로 87.6%(197개소)의 의료기관에서 보안관리 책임자가 적극적인 참여(반드시 참여함+대체로 참여함)를 보이는 것으로 확인된다.

의료기관 종별로 살펴보면 상급종합병원(39개소)은 '반드시 참여함'이 69.2%(27개소), '대체로 참여함'이 25.6%(10개소), '보통'이 5.1%(2개소)로 나타나 모든 기관이 일정 수준 이상 교육에 참여하고 있는 것으로 나타났다. 종합병원(186개소)은 '반드시 참여함'이 67.2%(125개소), '대체로 참여함'이 18.8%(35개소), '보통'이 11.3%(21개소), '거의 참여하지 않음'이 1.6%(3개소), '전혀 참여하지 않음'이 1.1%(2개소)로 나타나 상급종합병원에 비해 참여 수준이 다소 낮은 것으로 나타났다.

종합하면 전체 의료기관의 약 90%에 가까운 기관에서 최고정보책임자(CIO) 및 최고정보보호책임자(CISO)가 정보보안 교육에 적극적으로 참여하고 있는 것으로 나타났다. 이는 의료기관의 보안관리 책임자들이 교육의 중요성을 인식하고 적극적으로 참여하고 있음을 보여주는 결과로 나타났다. 다만 일부 종합병원에서 참여 수준이 상대적으로 낮게 나타난 점은 향후 개선이 필요한 부분으로 나타났다.

〈표 5-67〉 정보보안 교육 참석 수준(CIO, CISO)

(단위: 개소, %)

구분		반드시 참여함 (80~100%)	대체로 참여함 (60~79%)	보통 (40~59%)	거의 참여하지 않음 (20~39%)	전혀 참여하지 않음 (0~19%)	합계
전체	전체	152 (67.6%)	45 (20%)	23 (10.2%)	3 (1.3%)	2 (0.9%)	225 (100%)
종별	상급 종합병원	27 (69.2%)	10 (25.6%)	2 (5.1%)	0 (0.0%)	0 (0.0%)	39 (100%)
	종합병원	125 (67.2%)	35 (18.8%)	21 (11.3%)	3 (1.6%)	2 (1.1%)	186 (100%)
지역별	도시(동)	144 (67.6%)	42 (19.7%)	22 (10.3%)	3 (1.4%)	2 (0.9%)	213 (100%)
	비도시 (읍·면)	8 (66.7%)	3 (25%)	1 (8.3%)	0 (0.0%)	0 (0.0%)	12 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

〈표 5-68〉은 최고정보책임자(CIO) 및 최고정보보호책임자(CISO)를 대상으로 주로 실시한 정보보안 교육 방법 대해 조사한 결과를 나타낸 것이다.

전체 응답기관(225개소)을 기준으로 최고정보책임자(CIO) 및 최고정보보호책임자(CISO)를 대상으로 한 교육 방법을 살펴보면 '정부·지자체·공공기관 주관 교육'이 43.1%(97개소)로 가장 높게 나타났으며, '민간전문기관 위탁교육'이 36.0%(81개소), '자체교육(내부강사)' 15.6%(36개소), '자체교육(외부강사)' 5.3%(12개소) 순으로 나타났다. 즉 공공기관 주관 교육과 민간전문기관 위탁교육이 전체의 약 80%를 차지하는 것으로 나타났으며, 자체 교육의 비중은 상대적으로 낮은 것으로 나타났다.

의료기관 종별로 살펴보면 상급종합병원(39개소)은 '정부·지자체·공공기관 주관 교육' 25.6%(10개소), '민간전문기관 위탁교육' 10.3%(4개소), '자체교육(외부강사)' 15.4%(6개소), '자체교육(내부강사)' 48.7%(19개소)로 나타나 내부 강사를 활용한 자체교육 중심으로 운영되는 경향

이 나타났다. 반면 종합병원(186개소)은 '정부·지자체·공공기관 주관 교육' 46.8%(87개소), '민간전문기관 위탁교육' 41.4%(77개소)로 나타나 외부기관 중심의 교육 형태가 주를 이루는 것으로 나타났다.

종합하면 최고정보책임자(CIO) 및 최고정보보호책임자(CISO)를 대상으로 한 정보보안 교육은 정부·공공기관 주관 교육과 민간 전문기관 위탁 교육이 중심적으로 운영되고 있는 것으로 나타났다. 다만 상급종합병원은 내부 강사를 활용한 자체 교육 체계를 비교적 적극적으로 운영하고 있는 반면, 종합병원은 외부기관 중심의 교육 의존도가 높은 것으로 나타났다. 이는 기관 규모가 클수록 내부 교육 역량을 구축하는 경향이 나타나고 있음을 보여주는 결과로 나타났다.

〈표 5-68〉 주로 실시한 정보보안 교육 방법(CIO, CISO)

(단위: 개소, %)

구분		정부/지자체/공공기관 교육 참여	민간전문기관위탁	자체교육(외부강사)	자체교육(내부강사)	합계
전체	전체	97 (43.1%)	81 (36%)	12 (5.3%)	35 (15.6%)	225 (100%)
종별	상급종합병원	10 (25.6%)	4 (10.3%)	6 (15.4%)	19 (48.7%)	39 (100%)
	종합병원	87 (46.8%)	77 (41.4%)	6 (3.2%)	16 (8.6%)	186 (100%)
지역별	도시(동)	92 (43.2%)	76 (35.7%)	12 (5.6%)	33 (15.5%)	213 (100%)
	비도시(읍·면)	5 (41.7%)	5 (41.7%)	0 (0.0%)	2 (16.7%)	12 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

〈표 5-69〉는 최고정보책임자(CIO) 및 최고정보보호책임자(CISO)를 대상으로 실시한 정보보안 교육 방식에 대해 조사한 결과를 나타낸 것이다. 전체 응답기관(225개소) 중 81.3%(183개소)가 의료기관의 최고정보책임자(CIO) 및 최고정보보호책임자(CISO)를 포함한 임직원을 대상으로 '온라인' 형태의 정보보안 교육을 실시하고 있었으며, 18.7%(42개소)

는 '오프라인' 방식으로 운영하고 있는 것으로 나타났다. 대부분의 기관이 온라인 교육을 중심으로 운영하고 있어 시간과 장소의 제약 없이 참여할 수 있는 비대면 교육 체계가 보편화된 것으로 나타났다.

의료기관 종별로 살펴보면 상급종합병원(39개소)은 74.4%(29개소)가 온라인 교육을, 25.6%(10개소)가 오프라인 교육을 실시하고 있는 것으로 나타났으며, 종합병원(186개소)은 82.8%(154개소)가 온라인 교육, 17.2%(32개소)가 오프라인 교육을 운영하고 있는 것으로 나타났다. 즉, 상급종합병원은 종합병원에 비해 오프라인 교육 비중이 다소 높은 반면, 종합병원은 온라인 중심의 교육 체계가 보다 확산된 것으로 나타났다.

〈표 5-69〉 임직원 대상 정보보안 교육 방식(CIO, CISO)

(단위: 개소, %)

구분		온라인	오프라인	합계
전체	전체	183 (81.3%)	42 (18.7%)	225 (100%)
종별	상급종합병원	29 (74.4%)	10 (25.6%)	39 (100%)
	종합병원	154 (82.8%)	32 (17.2%)	186 (100%)
지역별	도시(동)	172 (80.8%)	41 (19.2%)	213 (100%)
	비도시(읍·면)	11 (91.7%)	1 (8.3%)	12 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

종합하면 의료기관의 최고정보책임자(CIO) 및 최고정보보호책임자(CISO)를 포함한 임직원을 대상으로 한 정보보안 교육은 전반적으로 온라인 중심으로 운영되고 있는 것으로 나타났으며, 상급종합병원에서는 오프라인 교육을 병행하는 비율이 상대적으로 높은 것으로 나타났다. 이는 대형 의료기관의 경우 현장 중심의 실습형 교육이나 사례 기반 교육을 병행하는 반면, 종합병원은 교육 접근성과 운영 효율성을 고려하여 온라인 교육 중심으로 운영하고 있는 것으로 해석된다.

2) 전산부서원

전산부서는 의료정보시스템의 구축, 운영, 유지보수, 네트워크 및 접근 통제 관리 등 병원 내 핵심 정보보호 업무를 수행하는 실무 부서로서, 정기적인 교육은 사이버 위협 대응 역량과 내부 보안정책 준수를 유지하기 위해 중요한 요소이다. 또한 교육 참여 수준과 교육 방식은 기관의 기술적 보안 역량 강화 정도를 가늠할 수 있는 주요 지표로 활용될 수 있다.

〈표 5-70〉은 전산부서원을 대상으로 한 정보보안 교육 시행 여부에 대해 조사한 결과를 나타낸 것이다.

전체 의료기관(263개소) 중 95.8%(252개소)가 전산부서원을 대상으로 정보보안 교육을 시행하고 있는 것으로 나타났으며, 4.2%(11개소)는 교육을 시행하지 않는 것으로 나타났다.

〈표 5-70〉 정보보안 교육 시행 여부(전산 부서원)

(단위: 개소, %)

구분		시행	미시행	합계
전체	전체	252 (95.8%)	11 (4.2%)	263 (100%)
종별	상급종합병원	41 (100%)	0 (0.0%)	41 (100%)
	종합병원	211 (95.0%)	11 (5.0%)	222 (100%)
지역별	도시(동)	237 (95.6%)	11 (4.4%)	248 (100%)
	비도시(읍·면)	15 (100%)	0 (0.0%)	15 (100%)

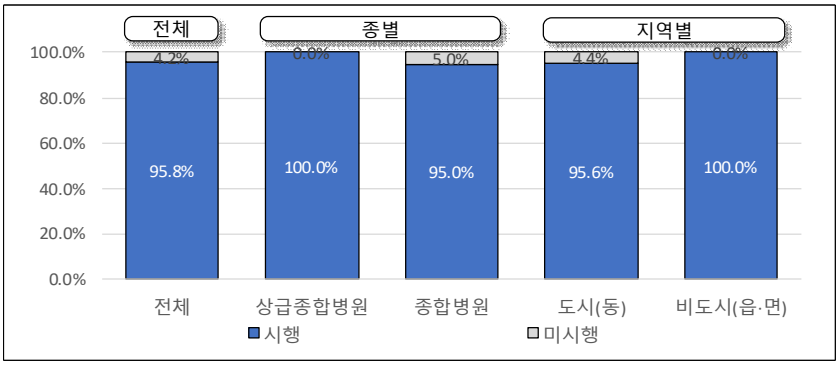
출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

의료기관 종별로 살펴보면 상급종합병원(41개소)은 100.0%(41개소)가 교육을 시행하고 있는 것으로 나타났으며, 종합병원(222개소)은 95.0%(211개소)가 교육을 시행하고 있고 5.0%(11개소)는 교육을 시행하지 않는 것으로 나타났다. 상급종합병원은 모든 기관에서 교육을 시행하고 있는 것으로 나타나 정보보안 교육에 대한 인식 수준과 제도적 정착 수준이

매우 높은 것으로 나타났다.

종합하면 전산부서원을 대상으로 한 정보보안 교육은 전체 의료기관의 약 96%에서 시행되고 있는 것으로 나타나 제도적 정착 수준이 매우 높은 것으로 나타났다. 이는 의료기관 전산 인력의 보안 역량 강화를 위한 교육이 전국적으로 보편화되어 있음을 보여주는 결과로 나타났다.

[그림 5-16] 정보보안 교육 시행 여부(전산 부서원)



출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

〈표 5-71〉은 전산부서원을 대상으로 실시한 정보보안 교육 시행 주기에 대해 조사한 결과를 나타낸 것이다.

의료기관의 전산부서원을 대상으로 정보보안 교육을 실시한다고 응답한 의료기관(252개소)을 기준으로 교육 시행 주기를 살펴보면, 75.4%(190개소)가 연 1회 주기로 교육을 시행하고 있는 것으로 나타났다. 다음으로 반기 13.9%(35개소), 분기 7.1%(18개소), 비정기 3.6%(9개소) 순으로 나타나 대부분의 의료기관이 연 1회 이상 정기적인 교육을 시행하고 있는 것으로 나타났다.

의료기관 종별로 살펴보면 상급종합병원(41개소)은 80.5%(33개소)가 연 1회 주기로 교육을 시행하고 있었으며, 반기 12.2%(5개소), 비정기

7.3%(3개소) 순으로 나타났다. 종합병원(211개소)은 연 1회 74.4%(157개소), 반기 14.2%(30개소), 분기 8.5%(18개소), 비정기 2.8%(6개소)로 나타나 상급종합병원과 유사한 분포를 보이는 것으로 나타났다.

종합하면 전체 의료기관의 약 4분의 3(75%)이 연 1회 주기로 전산부서원을 대상으로 정보보안 교육을 실시하고 있는 것으로 나타났으며, 반기 또는 분기 단위로 보다 자주 교육을 시행하는 기관도 약 20% 수준으로 나타났다. 이는 대부분의 의료기관이 정기적인 교육 체계를 운영하고 있음을 보여주는 결과로 나타났으나, 일부 기관에서는 여전히 비정기적 운영에 머무르고 있어 교육의 체계성과 지속성을 강화할 필요가 있는 것으로 나타났다.

〈표 5-71〉 정보보안 교육 시행 주기(전산 부서원)

(단위: 개소, %)

구분	분기	반기	년1회	비정기	합계
전체	18 (7.1%)	35 (13.9%)	190 (75.4%)	9 (3.6%)	252 (100%)
상급종합병원	0 (0.0%)	5 (12.2%)	33 (80.5%)	3 (7.3%)	41 (100%)
종합병원	18 (8.5%)	30 (14.2%)	157 (74.4%)	6 (2.8%)	211 (100%)
도시(동)	16 (6.8%)	33 (13.9%)	179 (75.5%)	9 (3.8%)	237 (100%)
비도시(읍·면)	2 (13.3%)	2 (13.3%)	11 (73.3%)	0 (0.0%)	15 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

〈표 5-72〉는 전산부서원을 대상으로 실시한 정보보안 교육 참석 수준에 대해 조사한 결과를 나타낸 것이다.

의료기관의 전산부서원을 대상으로 정보보안 교육을 실시한다고 응답한 의료기관(252개소)을 기준으로 교육 참여 수준을 살펴보면, 77.0%(194개소)가 '반드시 참여함(80~100%)'으로 응답한 것으로 나타났다. 다음으로 '대체로 참여함(60~79%)'이 16.7%(42개소), '보통(40~59%)'이 6.0%(15개소)로 나타났으며, '거의 참여하지 않음(20~39%)' 및 '전혀

참여하지 않음(0~19%)'으로 응답한 기관은 없는 것으로 나타났다. 이는 전산부서원의 정보보안 교육 참여율이 매우 높은 수준임을 보여주는 결과로 나타났다.

의료기관 종별로 살펴보면 상급종합병원(41개소)은 '반드시 참여함'이 65.9%(27개소), '대체로 참여함'이 26.8%(11개소), '보통'이 7.3%(3개소)로 나타났으며, 종합병원(211개소)은 '반드시 참여함'이 79.1%(167개소), '대체로 참여함'이 14.7%(31개소), '보통'이 5.7%(12개소)로 나타났다. 이는 종합병원이 상급종합병원에 비해 교육 참여 수준이 다소 높은 것으로 나타났다.

〈표 5-72〉 정보보안 교육 참석 수준(전산 부서원)

(단위: 개소, %)

구분		반드시 참여함 (80~100%)	대체로 참여함 (60~79%)	보통 (40~59%)	거의 참여 하지 않음 (20~39%)	전혀 참여 하지 않음 (0~19%)	합계
전체	전체	194 (77.0%)	42 (16.7%)	15 (6.0%)	1 (0.4%)	0 (0.0%)	252 (100%)
종별	상급 종합병원	27 (65.9%)	11 (26.8%)	3 (7.3%)	0 (0.0%)	0 (0.0%)	41 (100%)
	종합병원	167 (79.1%)	31 (14.7%)	12 (5.7%)	1 (0.5%)	0 (0.0%)	211 (100%)
지역별	도시(동)	182 (76.8%)	41 (17.3%)	13 (5.5%)	1 (0.4%)	0 (0.0%)	237 (100%)
	비도시 (읍·면)	12 (80.0%)	1 (6.7%)	2 (13.3%)	0 (0.0%)	0 (0.0%)	15 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

종합하면 전체 의료기관의 약 94%가 전산부서원의 정보보안 교육 참여를 적극적으로 유도하고 있는 것으로 나타났으며, 특히 '반드시 참여함' 응답이 77.0%로 나타나 교육 참여도가 매우 높은 수준임을 보여주는 결과로 나타났다. 이는 전산부서가 의료기관 내 정보보호의 핵심 역할을

수행하는 조직으로서 높은 책임 의식을 가지고 교육에 참여하고 있음을 보여주며, 의료기관의 보안관리 체계가 비교적 안정적으로 운영되고 있음을 시사하는 결과로 나타났다.

〈표 5-73〉은 전산부서원을 대상으로 실시한 정보보안 교육 방법에 대해 조사한 결과를 나타낸 것이다.

의료기관의 전산부서원을 대상으로 정보보안 교육을 실시한다고 응답한 전체 응답기관(252개소)을 기준으로 교육 운영 방식을 살펴보면, 46.8%(118개소)가 '정부·지자체·공공기관 주관 교육'에 참여하고 있는 것으로 나타났다. 다음으로 '민간전문기관 위탁교육' 28.2%(71개소), '자체교육(내부강사)' 18.7%(47개소), '자체교육(외부강사)' 6.3%(16개소) 순으로 나타났다. 즉 절반에 가까운 의료기관이 공공부문 주관 교육을 중심으로 교육에 참여하고 있는 것으로 나타났으며, 내부 강사를 활용한 자체교육도 일정 비중을 차지하고 있는 것으로 나타났다.

의료기관 종별로 살펴보면 상급종합병원(41개소)은 '정부·지자체·공공기관 주관 교육' 7.3%(3개소), '민간전문기관 위탁교육' 22.0%(9개소), '자체교육(외부강사)' 22.0%(9개소), '자체교육(내부강사)' 48.8%(20개소)로 나타나 내부 강사를 활용한 자체교육 비중이 가장 높은 것으로 나타났다. 반면 종합병원(211개소)은 '정부·지자체·공공기관 주관 교육' 54.5%(115개소), '민간전문기관 위탁교육' 29.4%(62개소), '자체교육(외부강사)' 3.3%(7개소), '자체교육(내부강사)' 12.8%(27개소)로 나타나 공공부문 주관 교육에 대한 의존도가 높은 것으로 나타났다.

전체적으로 의료기관 전산부서의 정보보안 교육은 공공기관 주관 교육 또는 민간기관 위탁교육 형태가 중심적으로 운영되고 있는 것으로 나타났다. 다만 상급종합병원에서는 내부 강사를 활용한 자체교육 비중이 상대적으로 높게 나타났다. 이는 병원 규모가 클수록 내부 보안 전문 인력

을 기반으로 한 자율적인 교육 체계가 구축되어 있음을 보여주는 결과로 나타났으며, 중소 규모 병원에서는 여전히 외부 기관에 대한 의존도가 높은 구조가 유지되고 있음을 시사한다.

〈표 5-73〉 주로 실시한 정보보안 교육 방법(전산 부서원)

(단위: 개소, %)

구분		정부/지자체/공공기관 교육 참여	민간전문기관위탁	자체교육(외부강사)	자체교육(내부강사)	합계
전체	전체	118 (46.8%)	71 (28.2%)	16 (6.3%)	47 (18.7%)	252 (100%)
종별	상급종합병원	3 (7.3%)	9 (22%)	9 (22%)	20 (48.8%)	41 (100%)
	종합병원	115 (54.5%)	62 (29.4%)	7 (3.3%)	27 (12.8%)	211 (100%)
지역별	도시(동)	110 (46.4%)	65 (27.4%)	16 (6.8%)	46 (19.4%)	237 (100%)
	비도시(읍·면)	8 (53.3%)	6 (40%)	0 (0.0%)	1 (6.7%)	15 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

〈표 5-74〉는 전산부서원을 대상으로 실시한 정보보안 교육 방식에 대해 조사한 결과를 나타낸 것이다.

의료기관 전산부서원을 대상으로 정보보안 교육을 실시한다고 응답한 전체 응답기관(252개소)을 기준으로 교육 방식(온라인·오프라인)을 살펴보면, 64.7%(163개소)가 '온라인' 교육을 실시하고 있었으며, 35.3%(89개소)는 '오프라인' 교육을 운영하고 있는 것으로 나타났다. 이는 전산부서의 정보보안 교육이 온라인 중심으로 운영되고 있으나, 일정 비율의 의료기관에서는 오프라인 교육을 병행하고 있음을 보여주는 결과로 나타났다.

의료기관 종별로 살펴보면 상급종합병원(41개소)은 65.9%(27개소)가 온라인 교육, 34.1%(14개소)가 오프라인 교육을 실시하고 있는 것으로 나타났으며, 종합병원(211개소)은 64.5%(136개소)가 온라인 교육, 35.5%(75개소)가 오프라인 교육을 실시하고 있는 것으로 나타났다. 두 집단 모

두 유사한 분포를 보여 전산부서원을 대상으로 한 정보보안 교육은 병원 규모와 관계없이 유사한 방식으로 운영되고 있는 것으로 나타났다. 전체적으로 전산 부서원 대상 정보보안 교육은 온라인 중심으로 운영되고 있으나, 오프라인 교육도 병행하는 기관이 적지 않다.

〈표 5-74〉 임직원 대상 정보보안 교육 방식(전산 부서원)

(단위: 개소, %)

구분		온라인	오프라인	합계
전체	전체	163 (64.7%)	89 (35.3%)	252 (100%)
종별	상급종합병원	27 (65.9%)	14 (34.1%)	41 (100%)
	종합병원	136 (64.5%)	75 (35.5%)	211 (100%)
지역별	도시(동)	154 (65.0%)	83 (35.0%)	237 (100%)
	비도시(읍·면)	9 (60.0%)	6 (40.0%)	15 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

3) 정보보안 담당자

정보보안 담당자는 병원의 보안 정책 수립과 점검, 침해사고 대응을 직접 수행하는 핵심 실무 인력으로, 주기적인 교육은 기술적·관리적 보안 역량을 유지하고 강화하는 데 중요한 요소이다. 또한 교육 참여 수준과 교육 방식은 의료기관의 보안관리 체계 성숙도를 보여주는 주요 지표로 활용될 수 있다.

의료진은 환자정보를 직접 처리하는 주요 인력으로서, 정보보안 교육은 환자정보 보호, 진료정보 접근통제, 비인가 정보 유출 방지 등 임상 현장에서 발생할 수 있는 다양한 보안 위협에 대응하기 위한 필수적인 활동이다. 따라서 의료진의 교육 참여 수준과 교육 방식은 의료기관의 개인정보 보호 수준과 조직 내 보안 인식이 실제 업무에 어떻게 적용되고 있는지를 평가할 수 있는 중요한 지표로 볼 수 있다.

〈표 5-75〉는 정보보안 담당자를 대상으로 한 정보보안 교육 시행 여부에 대해 조사한 결과를 나타낸 것이다.

전체 의료기관(263개소) 중 95.8%(252개소)가 의료기관 내 정보보안 담당자를 대상으로 정보보안 교육을 시행하고 있는 것으로 나타났으며, 4.2%(11개소)는 교육을 시행하지 않는 것으로 나타났다.

〈표 5-75〉 정보보안 교육 시행 여부(정보보안 담당자)

(단위: 개소, %)

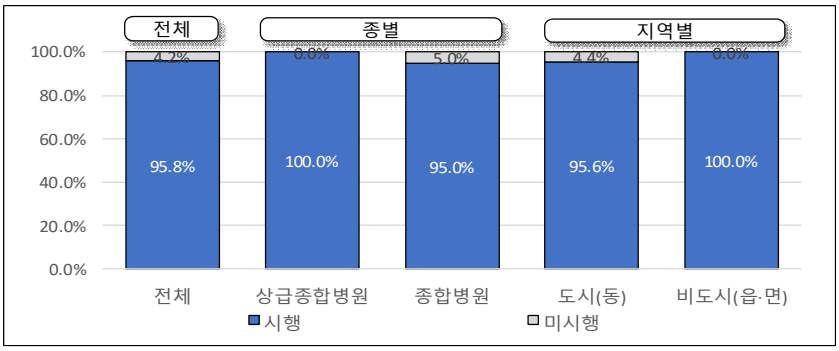
구분		시행	미시행	합계
전체	전체	252 (95.8%)	11 (4.2%)	263 (100%)
종별	상급종합병원	41 (100%)	0 (0.0%)	41 (100%)
	종합병원	211 (95.0%)	11 (5.0%)	222 (100%)
지역별	도시(동)	237 (95.6%)	11 (4.4%)	248 (100%)
	비도시(읍·면)	15 (100%)	0 (0.0%)	15 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

의료기관 종별로 살펴보면 상급종합병원(41개소)은 모든 기관이 교육을 시행하고 있는 것으로 나타났으며, 종합병원(222개소)은 95.0%(211개소)가 교육을 시행하고 있고 5.0%(11개소)는 교육을 시행하지 않는 것으로 나타났다. 상급종합병원은 모든 기관에서 교육이 이루어지고 있는 것으로 나타나 제도적 정착 수준이 매우 높은 것으로 나타났으며, 종합병원에서도 대부분의 기관에서 교육이 시행되고 있는 것으로 나타났다.

종합하면 전체 의료기관의 약 96%가 정보보안 교육을 시행하고 있는 것으로 나타나 의료기관 내 정보보안 교육이 전반적으로 높은 수준에서 정착되어 있는 것으로 나타났다.

[그림 5-17] 정보보안 교육 시행 여부(정보보안 담당자)



출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

〈표 5-76〉은 정보보안 담당자를 대상으로 실시한 정보보안 교육 시행 주기에 대해 조사한 결과를 나타낸 것이다.

의료기관 내 정보보안 담당자를 대상으로 정보보안 교육을 실시하고 있다고 응답한 의료기관(252개소)을 기준으로 교육 시행 주기를 살펴보면, 69.0%(174개소)가 연 1회 주기로 교육을 시행하고 있는 것으로 나타났다. 다음으로 반기 16.3%(41개소), 분기 9.1%(23개소), 비정기 5.6%(14개소) 순으로 나타나 대부분의 의료기관이 연 1회 이상 정기적인 교육을 시행하고 있는 것으로 나타났다.

의료기관 종별로 살펴보면 상급종합병원(41개소)은 56.1%(23개소)가 연 1회 주기로 교육을 시행하고 있었으며, 반기 17.1%(7개소), 분기 7.3%(3개소), 비정기 19.5%(8개소) 순으로 나타났다. 종합병원(211개소)은 연 1회 71.6%(151개소), 반기 16.1%(34개소), 분기 9.5%(20개소), 비정기 2.8%(6개소)로 나타나 상급종합병원에 비해 교육 주기가 보다 정례화되어 있는 것으로 나타났다.

종합하면 정보보안 담당자를 대상으로 보안교육을 실시하고 있는 의료기관의 약 70%가 연 1회 주기로 교육을 시행하고 있으며, 반기 또는 분기

단위로 보다 자주 교육을 시행하는 기관도 약 25% 수준으로 나타났다. 상급종합병원은 일부 기관에서 비정기적 교육 운영 비율이 상대적으로 높게 나타났으나, 종합병원은 정례화된 교육 체계를 운영하는 비율이 높은 것으로 나타났다. 전반적으로 대부분의 의료기관이 정보보안 담당자를 대상으로 정기적인 교육 체계를 운영하고 있는 것으로 나타났다.

〈표 5-76〉 정보보안 교육 시행 주기(정보보안 담당자)

(단위: 개소, %)

구분		분기	반기	년1회	비정기	합계
전체	전체	23 (9.1%)	41 (16.3%)	174 (69.0%)	14 (5.6%)	252 (100%)
종별	상급종합병원	3 (7.3%)	7 (17.1%)	23 (56.1%)	8 (19.5%)	41 (100%)
	종합병원	20 (9.5%)	34 (16.1%)	151 (71.6%)	6 (2.8%)	211 (100%)
지역별	도시(동)	21 (8.9%)	39 (16.5%)	163 (68.8%)	14 (5.9%)	237 (100%)
	비도시(읍·면)	2 (13.3%)	2 (13.3%)	11 (73.3%)	0 (0.0%)	15 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

〈표 5-77〉은 정보보안 담당자를 대상으로 실시한 정보보안 교육 참석 수준 에 대해 조사한 결과를 나타낸 것이다.

의료기관의 정보보안 담당자를 대상으로 정보보안 교육을 실시하고 있다고 응답한 의료기관(252개소)을 기준으로 교육 참여 수준을 살펴보면, 79.8%(201개소)가 '반드시 참여함(80~100%)'으로 응답한 것으로 나타났다. 다음으로 '대체로 참여함(60~79%)' 13.5%(34개소), '보통(40~59%)' 6.7%(17개소) 순으로 나타났으며, '거의 참여하지 않음(20~39%)' 또는 '전혀 참여하지 않음(0~19%)'으로 응답한 기관은 없는 것으로 나타났다. 이는 전반적으로 모든 의료기관에서 정보보안 담당자의 교육 참여율이 매우 높은 수준임을 보여주는 결과로 나타났다.

의료기관 종별로 살펴보면 상급종합병원(41개소)은 '반드시 참여함'이 75.6%(31개소), '대체로 참여함'이 19.5%(8개소), '보통'이 4.9%(2개소)

로 나타났으며, 종합병원(211개소)은 '반드시 참여함'이 80.6%(170개소), '대체로 참여함'이 12.3%(26개소), '보통'이 7.1%(15개소)로 나타나 종합병원이 상급종합병원보다 참여 수준이 다소 높은 것으로 나타났다.

종합하면 정보보안 담당자를 대상으로 보안교육을 실시하고 있는 의료기관의 약 80%가 정보보안 담당자가 반드시 교육에 참여한다고 응답한 것으로 나타났으며, 나머지 기관에서도 대부분 정기적으로 교육에 참여하고 있는 것으로 나타났다. 또한 상급종합병원과 종합병원 모두 정보보안 담당자의 교육 참여율이 전반적으로 높은 것으로 나타나, 정보보안 담당자가 의료기관 내 보안체계 강화의 핵심 역할을 수행하고 있으며 교육을 통한 보안 역량 강화가 실질적으로 이루어지고 있음을 보여주는 결과로 나타났다.

〈표 5-77〉 정보보안 교육 참석 수준(정보보안 담당자)

(단위: 개소, %)

구분		반드시 참여함 (80~100%)	대체로 참여함 (60~79%)	보통 (40~59%)	거의참여 하지 않음 (20~39%)	전혀 참여 하지 않음 (0~19%)	합계
전체	전체	201 (79.8%)	34 (13.5%)	17 (6.7%)	0 (0.0%)	0 (0.0%)	252 (100%)
종별	상급종합병원	31 (75.6%)	8 (19.5%)	2 (4.9%)	0 (0.0%)	0 (0.0%)	41 (100%)
	종합병원	170 (80.6%)	26 (12.3%)	15 (7.1%)	0 (0.0%)	0 (0.0%)	211 (100%)
지역별	도시(동)	188 (79.3%)	33 (13.9%)	16 (6.8%)	0 (0.0%)	0 (0.0%)	237 (100%)
	비도시(읍·면)	13 (86.7%)	1 (6.7%)	1 (6.7%)	0 (0.0%)	0 (0.0%)	15 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

〈표 5-78〉은 정보보안 담당자를 대상으로 주로 실시한 정보보안 교육 방법 대해 조사한 결과를 나타낸 것이다.

의료기관의 정보보안 담당자를 대상으로 정보보안 교육을 실시하고 있다고 응답한 의료기관(252개소)을 기준으로 교육 운영 방식을 살펴보면, 60.7%(153개소)가 '정부·지자체·공공기관 주관 교육'에 참여하고 있는

것으로 나타났다. 다음으로 '민간전문기관 위탁교육' 24.2%(61개소), '자체교육(내부강사)' 11.9%(30개소), '자체교육(외부강사)' 3.2%(8개소) 순으로 나타났다. 전체적으로 공공기관 주관 교육의 비중이 가장 높은 것으로 나타났으며, 자체교육은 약 15% 수준으로 제한적으로 운영되고 있는 것으로 나타났다.

의료기관 종별로 살펴보면 상급종합병원(41개소)은 '정부·지자체·공공기관 주관 교육' 36.6%(15개소), '민간전문기관 위탁교육' 14.6%(6개소), '자체교육(외부강사)' 12.2%(5개소), '자체교육(내부강사)' 36.6% (15개소)로 나타나 외부기관 교육과 함께 내부 강사를 활용한 자체교육을 병행하는 경향이 나타났다. 반면 종합병원(211개소)은 '정부·지자체·공공기관 주관 교육' 65.4%(138개소), '민간전문기관 위탁교육' 26.1%(55개소), '자체교육(외부강사)' 1.4%(3개소), '자체교육(내부강사)' 7.1%(15개소)로 나타나 공공기관 주관 교육에 대한 의존도가 높은 것으로 나타났다.

〈표 5-78〉 주로 실시한 정보보안 교육 방법(정보보안 담당자)

(단위: 개소, %)

구분		정부/지자체/공공기관 교육 참여	민간전문 기관위탁	자체교육 (외부강사)	자체교육 (내부강사)	합계
전체	전체	153 (60.7%)	61 (24.2%)	8 (3.2%)	30 (11.9%)	252 (100%)
종별	상급종합병원	15 (36.6%)	6 (14.6%)	5 (12.2%)	15 (36.6%)	41 (100%)
	종합병원	138 (65.4%)	55 (26.1%)	3 (1.4%)	15 (7.1%)	211 (100%)
지역별	도시(동)	144 (60.8%)	56 (23.6%)	8 (3.4%)	29 (12.2%)	237 (100%)
	비도시(읍·면)	9 (60.0%)	5 (33.3%)	0 (0.0%)	1 (6.7%)	15 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

종합하면 정보보안 담당자를 대상으로 한 정보보안 교육은 약 60%의 의료기관이 정부 또는 공공기관이 주관하는 프로그램을 통해 운영하고

있는 것으로 나타났다. 또한 상급종합병원은 내부 강사를 활용한 자체교육 비중이 상대적으로 높은 반면, 종합병원은 공공기관 주관 또는 민간 위탁 중심으로 교육을 운영하고 있는 것으로 나타났다. 이는 병원 규모가 클수록 내부 보안 전문 인력을 활용한 자율적 교육 체계가 정착되고 있는 반면, 중소 규모 의료기관에서는 외부기관 의존도가 여전히 높은 구조가 유지되고 있음을 보여주는 결과로 나타났다.

〈표 5-79〉는 정보보안 담당자를 대상으로 실시한 정보보안 교육 방식에 대해 조사한 결과를 나타낸 것이다.

의료기관에서 정보보안 담당자를 대상으로 정보보안 교육을 실시하고 있다고 응답한 의료기관(252개소)을 기준으로 교육 방식을 살펴보면, 53.6%(135개소)가 '온라인' 교육을 실시하고 있었으며, 46.4%(117개소)는 '오프라인' 교육을 운영하고 있는 것으로 나타났다. 전체적으로 온라인 교육이 다소 높은 비중을 차지하고 있으나, 오프라인 교육도 절반에 가까운 수준으로 운영되고 있어 대면 중심의 전문 교육 역시 중요한 역할을 수행하고 있는 것으로 나타났다.

의료기관 종별로 살펴보면 상급종합병원(41개소)은 46.3%(19개소)가 온라인 교육을 실시하고 있었으며, 53.7%(22개소)는 오프라인 교육을 운영하고 있는 것으로 나타나 오프라인 교육 비중이 다소 높은 것으로 나타났다. 반면 종합병원(211개소)은 55.0%(116개소)가 온라인 교육, 45.0%(95개소)가 오프라인 교육을 운영하고 있는 것으로 나타나 온라인 교육 비중이 상대적으로 높은 것으로 나타났다.

종합하면 정보보안 담당자를 대상으로 한 교육은 온라인과 오프라인을 병행하는 형태로 운영되고 있는 것으로 나타났다. 특히 상급종합병원은 대면 교육을 통한 실습 중심 학습 비중이 상대적으로 높은 반면, 종합병원은 교육 접근성과 운영 효율성을 고려한 온라인 중심 교육 체계가 비교

적 확대되어 있는 것으로 나타났다. 이러한 결과는 의료기관의 규모와 교육 운영 여건에 따라 교육 방식이 차이를 보이고 있음을 보여주는 결과로 나타났다.

〈표 5-79〉 임직원 대상 정보보안 교육 방식(정보보안 담당자)

(단위: 개소, %)

구분	온라인	오프라인	합계
전체	135 (53.6%)	117 (46.4%)	252 (100%)
상급종합병원	19 (46.3%)	22 (53.7%)	41 (100%)
종합병원	116 (55%)	95 (45%)	211 (100%)
도시(동)	125 (52.7%)	112 (47.3%)	237 (100%)
비도시(읍·면)	10 (66.7%)	5 (33.3%)	15 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

4) 의료진

의료기관의 의료진은 다양한 업무 과정에서 환자정보를 직접 처리하기 때문에, 정보보안 교육은 조직 전체의 보안 인식 제고와 보안 사고 예방을 위해 중요한 요소이다. 교육 시행 여부와 주기, 참여 수준, 그리고 온라인·오프라인 등 교육 방식은 의료진의 보안 정책 이해도와 실무 적용 수준을 보여주는 주요 지표로 활용될 수 있으며, 의료기관의 전반적인 보안관리 수준을 평가하는 기준이 된다.

〈표 5-80〉은 의료진을 대상으로 한 정보보안 교육 시행 여부에 대해 조사한 결과를 나타낸 것이다.

전체 의료기관(263개소) 중 90.1%(237개소)가 의료진을 대상으로 정보보안 교육을 시행하고 있는 것으로 나타났으며, 9.9%(26개소)는 교육을 시행하지 않는 것으로 나타났다.

〈표 5-80〉 정보보안 교육 시행 여부(의료진)

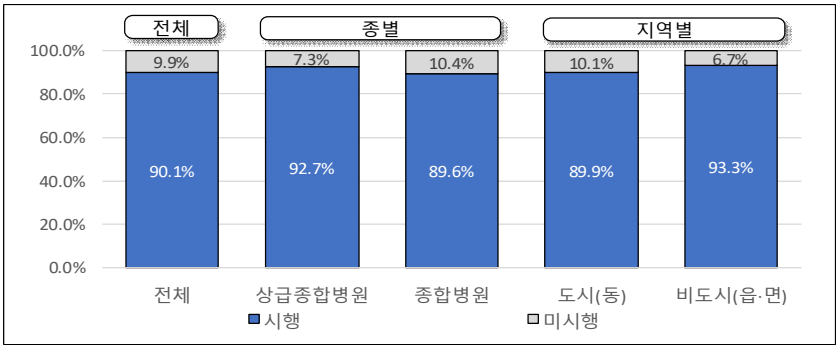
(단위: 개소, %)

구분		시행	미시행	합계
전체	전체	237 (90.1%)	26 (9.9%)	263 (100%)
종별	상급종합병원	38 (92.7%)	3 (7.3%)	41 (100%)
	종합병원	199 (89.6%)	23 (10.4%)	222 (100%)
지역별	도시(동)	223 (89.9%)	25 (10.1%)	248 (100%)
	비도시(읍·면)	14 (93.3%)	1 (6.7%)	15 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

의료기관 종별로 살펴보면 상급종합병원(41개소)은 92.7%(38개소)가 교육을 시행하고 있었으며, 7.3%(3개소)는 교육을 시행하지 않는 것으로 나타났다. 종합병원(222개소)은 89.6%(199개소)가 교육을 시행하고 있었고 10.4%(23개소)는 교육을 시행하지 않는 것으로 나타나 상급종합병원에 비해 다소 낮은 시행률을 보이는 것으로 나타났다.

[그림 5-18] 정보보안 교육 시행 여부(의료진)



출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

종합하면 의료진을 대상으로 한 정보보안 교육은 전체 의료기관의 90% 이상에서 시행되고 있는 것으로 나타나 전반적으로 높은 수준에서 정착되어 있는 것으로 나타났다. 다만 일부 종합병원에서 교육 미시행 사

례가 확인되어, 의료진을 포함한 전 구성원을 대상으로 한 정보보안 교육을 보다 강화할 필요가 있는 것으로 나타났다.

〈표 5-81〉은 의료진을 대상으로 실시한 정보보안 교육 시행 주기에 대해 조사한 결과를 나타낸 것이다.

의료기관 내 의료진을 대상으로 정보보안 교육을 실시하고 있다고 응답한 의료기관(237개소)을 기준으로 교육 시행 주기를 살펴보면, 85.7%(203개소)가 연 1회 주기로 교육을 시행하고 있는 것으로 나타났다. 다음으로 반기 9.3%(22개소), 분기 3.0%(7개소), 비정기 2.1%(5개소) 순으로 나타나 대부분의 의료기관이 연 1회 이상 정기적인 교육을 운영하고 있는 것으로 나타났다.

의료기관 종별로 살펴보면 상급종합병원(38개소)은 94.7%(36개소)가 연 1회 주기로 교육을 시행하고 있었으며, 비정기 교육이 5.3%(2개소)로 나타났다. 종합병원(199개소)은 연 1회 83.9%(167개소), 반기 11.1%(22개소), 분기 3.5%(7개소), 비정기 1.5%(3개소) 순으로 나타나 상급종합병원에 비해 교육 주기가 다소 덜 정례화된 것으로 나타났다.

〈표 5-81〉 정보보안 교육 시행 주기(의료진)

(단위: 개소, %)

구분		분기	반기	년1회	비정기	합계
전체	전체	7 (3.0%)	22 (9.3%)	203 (85.7%)	5 (2.1%)	237 (100%)
종별	상급종합병원	0 (0.0%)	0 (0.0%)	36 (94.7%)	2 (5.3%)	38 (100%)
	종합병원	7 (3.5%)	22 (11.1%)	167 (83.9%)	3 (1.5%)	199 (100%)
지역별	도시(동)	6 (2.7%)	21 (9.4%)	191 (85.7%)	5 (2.2%)	223 (100%)
	비도시(읍·면)	1 (7.1%)	1 (7.1%)	12 (85.7%)	0 (0.0%)	14 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

종합하면 의료진을 대상으로 정보보안 교육을 실시하고 있는 의료기관의 85% 이상이 연 1회 주기로 정기적인 교육을 시행하고 있는 것으로 나

타났으며, 일부 기관에서는 반기 또는 분기 단위의 추가 교육도 운영하고 있는 것으로 나타났다. 또한 상급종합병원은 전반적으로 교육 주기가 보다 정례화되어 있는 것으로 나타났다.

〈표 5-82〉는 의료진을 대상으로 실시한 정보보안 교육 참여 수준에 대해 조사한 결과를 나타낸 것이다.

의료기관 내 의료진을 대상으로 정보보안 교육을 실시하고 있다고 응답한 의료기관(237개소)을 기준으로 교육 참여 수준을 살펴보면, 48.1%(114개소)가 '반드시 참여함(80~100%)', 27.0%(64개소)가 '대체로 참여함(60~79%)', 21.1%(50개소)가 '보통(40~59%)', 3.4%(8개소)가 '거의 참여하지 않음(20~39%)', 0.4%(1개소)가 '전혀 참여하지 않음(0~19%)'으로 나타났다. '반드시 참여함'과 '대체로 참여함'을 합한 적극적인 참여 비율은 75.1%로 나타나, 기관 내 다른 직군에 비해 상대적으로 낮은 수준을 보이는 것으로 나타났다.

의료기관 종별로 살펴보면 상급종합병원(38개소)은 '반드시 참여함' 47.4%(18개소), '대체로 참여함' 28.9%(11개소), '보통' 15.8%(6개소), '거의 참여하지 않음' 7.9%(3개소)로 나타났다. 종합병원(199개소)은 '반드시 참여함' 48.2%(96개소), '대체로 참여함' 26.6%(53개소), '보통' 22.1%(44개소), '거의 참여하지 않음' 2.5%(5개소), '전혀 참여하지 않음' 0.5%(1개소)로 나타나 상급종합병원과 유사한 분포를 보이는 것으로 나타났다.

종합하면 의료진의 정보보안 교육 참여 수준은 전반적으로 양호한 것으로 나타났으나, '반드시 참여함' 응답 비율이 절반에 미치지 못해 다른 직군에 비해 참여 수준이 다소 낮은 것으로 나타났다. 이는 의료진이 진료 중심의 업무 일정으로 인해 보안 교육 참여가 상대적으로 제한될 수 있는 현실을 반영하는 결과로 나타났으며, 향후 의료진의 교육 참여를 제도적으로 강화할 필요가 있음을 보여주는 결과로 나타났다.

〈표 5-82〉 정보보안 교육 참석 수준(의료진)

(단위: 개소, %)

구분		반드시 참여함 (80~100%)	대체로 참여함 (60~79%)	보통 (40~59%)	거의 참여 하지 않음 (20~39%)	전혀 참여 하지 않음 (0~19%)	합계
전체	전체	114 (48.1%)	64 (27%)	50 (21.1%)	8 (3.4%)	1 (0.4%)	237 (100%)
종별	상급종합병원	18 (47.4%)	11 (28.9%)	6 (15.8%)	3 (7.9%)	0 (0.0%)	38 (100%)
	종합병원	96 (48.2%)	53 (26.6%)	44 (22.1%)	5 (2.5%)	1 (0.5%)	199 (100%)
지역별	도시(동)	106 (47.5%)	61 (27.4%)	49 (22%)	6 (2.7%)	1 (0.4%)	223 (100%)
	비도시(읍·면)	8 (57.1%)	3 (21.4%)	1 (7.1%)	2 (14.3%)	0 (0.0%)	14 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

〈표 5-83〉은 의료진을 대상으로 주로 실시한 정보보안 교육 방법에 대해 조사한 결과를 나타낸 것이다.

의료진을 대상으로 정보보안 교육을 실시하고 있다고 응답한 의료기관(237개소)을 기준으로 교육 운영 방식을 살펴보면, 57.8%(137개소)가 '민간전문기관 위탁교육'을 통해 교육을 실시하고 있는 것으로 나타났다. 다음으로 '자체교육(내부강사)' 26.6%(63개소), '자체교육(외부강사)' 10.1%(24개소), '정부·지자체·공공기관 주관 교육' 5.5%(13개소) 순으로 나타났다. 전체적으로 민간전문기관 위탁 형태의 교육이 절반 이상을 차지하여 가장 보편적인 방식으로 운영되고 있는 것으로 나타났다.

의료기관 종별로 살펴보면 상급종합병원(38개소)은 '정부·지자체·공공기관 주관 교육' 0.0%(0개소), '민간전문기관 위탁교육' 18.4%(7개소), '자체교육(외부강사)' 21.1%(8개소), '자체교육(내부강사)' 60.5%(23개소)로 나타나 내부 강사를 활용한 자체교육 중심으로 운영되는 경향이 나타났다. 반면 종합병원(199개소)은 '정부·지자체·공공기관 주관 교육' 6.5%(13개소), '민간전문기관 위탁교육' 65.3%(130개소), '자체교육(외부강사)' 8.0%(16개소), '자체교육(내부강사)' 20.1%(40개소)로 나타나 외부기관 중심의 교육 운영 비중이 높은 것으로 나타났다.

종합하면 의료진을 대상으로 한 정보보안 교육은 민간전문기관에 위탁하여 운영되는 비중이 가장 높은 것으로 나타났다. 또한 상급종합병원은 내부 강사를 활용한 자체교육 중심의 교육 체계를 운영하고 있는 반면, 종합병원은 외부기관에 의존하는 교육 방식이 상대적으로 높은 것으로 나타났다.

〈표 5-83〉 주로 실시한 정보보안 교육 방법(의료진)

(단위: 개소, %)

구분		정부/지자체/공공기관 교육 참여	민간전문기관위탁	자체교육(외부강사)	자체교육(내부강사)	합계
전체	전체	13 (5.5%)	137 (57.8%)	24 (10.1%)	63 (26.6%)	237 (100%)
종별	상급종합병원	0 (0.0%)	7 (18.4%)	8 (21.1%)	23 (60.5%)	38 (100%)
	종합병원	13 (6.5%)	130 (65.3%)	16 (8.0%)	40 (20.1%)	199 (100%)
지역별	도시(동)	13 (5.8%)	125 (56.1%)	24 (10.8%)	61 (27.4%)	223 (100%)
	비도시(읍·면)	0 (0.0%)	12 (85.7%)	0 (0.0%)	2 (14.3%)	14 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

〈표 5-84〉는 의료진을 대상으로 실시한 정보보안 교육 방식 대해 조사한 결과를 나타낸 것이다.

의료진을 대상으로 정보보안 교육을 실시하고 있다고 응답한 의료기관(237개소)을 기준으로 교육 방식을 살펴보면, 88.6%(210개소)가 '온라인' 교육을 실시하고 있었으며, 11.4%(27개소)는 '오프라인' 교육을 운영하고 있는 것으로 나타났다. 전체적으로 온라인 교육이 압도적으로 높은 비중을 차지하고 있는 것으로 나타나 의료진의 업무 특성과 시간 제약을 고려한 비대면 교육 중심의 운영이 일반화되어 있는 것으로 나타났다.

의료기관 종별로 살펴보면 상급종합병원(38개소)은 86.8%(33개소)가 온라인 교육을 실시하고 있었으며, 13.2%(5개소)는 오프라인 교육을 운

영하고 있는 것으로 나타났다. 종합병원(199개소)은 88.9%(177개소)가 온라인 교육, 11.1%(22개소)가 오프라인 교육을 운영하고 있는 것으로 나타나 두 집단 모두 온라인 중심의 교육 형태를 보이는 것으로 나타났다.

종합하면 의료진을 대상으로 한 정보보안 교육은 대부분 온라인 방식으로 운영되고 있는 것으로 나타났다. 이는 시간 효율성과 접근성을 중시하는 의료 환경의 특성을 반영한 결과로 나타났으며, 상급종합병원에서는 일부 대면 교육을 병행하고 있는 반면 종합병원은 온라인 중심의 교육 체계가 비교적 안정적으로 운영되고 있는 것으로 나타났다.

〈표 5-84〉 임직원 대상 정보보안 교육 방식(의료진)

(단위: 개소, %)

구분		온라인	오프라인	합계
전체	전체	210 (88.6%)	27 (11.4%)	237 (100%)
종별	상급종합병원	33 (86.8%)	5 (13.2%)	38 (100%)
	종합병원	177 (88.9%)	22 (11.1%)	199 (100%)
지역별	도시(동)	197 (88.3%)	26 (11.7%)	223 (100%)
	비도시(읍·면)	13 (92.9%)	1 (7.1%)	14 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

5) 의료진 외 전 직원

의료기관의 의료진 외 전 직원(행정, 전산, 시설, 지원 등 비의료직)은 다양한 업무 과정에서 환자 정보와 행정 데이터를 처리하기 때문에, 정보보안 교육은 조직 전체의 보안 인식 제고와 보안 사고 예방을 위해 중요한 요소이다. 교육 시행 여부와 주기, 참여 수준, 그리고 온라인·오프라인 등 교육 방식은 비의료직 종사자의 보안 정책 이해도와 실무 적용 수준을 보여주는 주요 지표로 활용될 수 있으며, 기관의 전반적인 보안 관리 수준을 평가하는 기준이 된다.

〈표 5-85〉는 의료진 외 전 직원을 대상으로 한 정보보안 교육 시행 여부에 대해 조사한 결과를 나타낸 것이다.

전체 의료기관(263개소) 중 91.6%(241개소)가 의료기관 내 의료진 외 전 직원을 대상으로 정보보안 교육을 시행하고 있는 것으로 나타났으며, 8.4%(22개소)는 교육을 시행하지 않는 것으로 나타났다.

의료기관 종별로 살펴보면 상급종합병원(41개소)은 97.6%(40개소)가 교육을 시행하고 있었으며, 2.4%(1개소)는 교육을 시행하지 않는 것으로 나타났다. 종합병원(222개소)은 90.5%(201개소)가 교육을 시행하고 있었고 9.5%(21개소)는 교육을 시행하지 않는 것으로 나타났다.

〈표 5-85〉 정보보안 교육 시행 여부(의료진 외 전 직원)

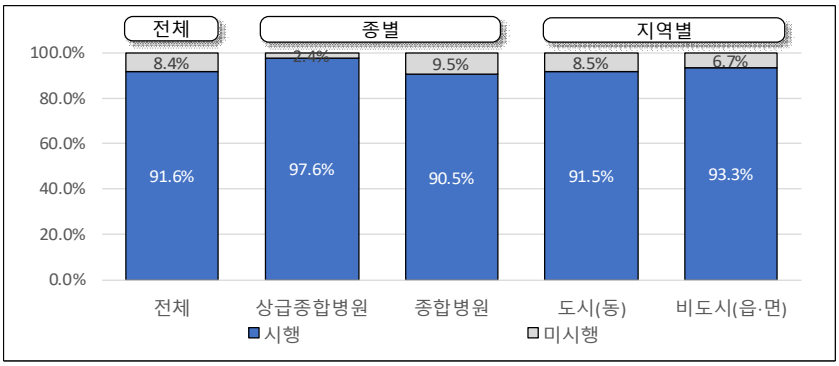
(단위: 개소, %)

구분		시행	미시행	합계
전체	전체	241 (91.6%)	22 (8.4%)	263 (100%)
종별	상급종합병원	40 (97.6%)	1 (2.4%)	41 (100%)
	종합병원	201 (90.5%)	21 (9.5%)	222 (100%)
지역별	도시(동)	227 (91.5%)	21 (8.5%)	248 (100%)
	비도시(읍·면)	14 (93.3%)	1 (6.7%)	15 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

종합하면 의료진 외 전 직원을 대상으로 한 정보보안 교육은 전체 의료기관의 90% 이상에서 시행되고 있는 것으로 나타나 전반적으로 높은 수준에서 정착되어 있는 것으로 나타났다. 특히 상급종합병원은 대부분의 기관에서 교육이 시행되고 있는 것으로 나타났으나, 일부 종합병원에서는 여전히 교육 미시행 사례가 존재하는 것으로 나타나 전 직원을 대상으로 한 정보보안 인식 제고 교육을 지속적으로 강화할 필요가 있는 것으로 나타났다.

[그림 5-19] 정보보안 교육 시행 여부(의료진 외 전 직원)



출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

〈표 5-86〉은 의료진 외 전 직원을 대상으로 실시한 정보보안 교육 시행 주기에 대해 조사한 결과를 나타낸 것이다.

의료기관 내 의료진 외 전 직원을 대상으로 정보보안 교육을 실시하고 있다고 응답한 의료기관(241개소)을 기준으로 교육 시행 주기를 살펴보면, 87.1%(210개소)가 연 1회 주기로 교육을 시행하고 있는 것으로 나타났다. 다음으로 반기 8.7%(21개소), 분기 2.9%(7개소), 비정기 1.2%(3개소) 순으로 나타나 대부분의 의료기관이 연 1회 이상 정기적인 교육을 운영하고 있는 것으로 나타났다.

의료기관 종별로 살펴보면 상급종합병원(40개소)은 97.5%(39개소)가 연 1회 주기로 교육을 시행하고 있는 것으로 나타났으며, 종합병원(201개소)은 연 1회 85.1%(171개소), 반기 10.4%(21개소), 분기 3.5%(7개소), 비정기 0.5%(1개소)로 나타났다. 이는 상급종합병원은 거의 모든 기관에서 연 1회 정기교육을 시행하고 있는 반면, 종합병원에서는 일부 기관이 반기 또는 분기 단위로 교육을 실시하고 있는 것으로 나타났다.

〈표 5-86〉 정보보안 교육 시행 주기(의료진 외 전 직원)

(단위: 개소, %)

구분		분기	반기	년1회	비정기	합계
전체	전체	7 (2.9%)	21 (8.7%)	210 (87.1%)	3 (1.2%)	241 (100%)
종별	상급종합병원	0 (0.0%)	0 (0.0%)	39 (97.5%)	1 (2.5%)	40 (100%)
	종합병원	7 (3.5%)	21 (10.4%)	171 (85.1%)	2 (1%)	201 (100%)
지역별	도시(동)	6 (2.6%)	20 (8.8%)	198 (87.2%)	3 (1.3%)	227 (100%)
	비도시(읍·면)	1 (7.1%)	1 (7.1%)	12 (85.7%)	0 (0.0%)	14 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

종합하면 의료진 외 전 직원을 대상으로 정보보안 교육을 실시하고 있는 의료기관의 약 87%가 연 1회 주기의 정기 교육을 시행하고 있는 것으로 나타났다. 특히 상급종합병원은 대부분의 기관에서 정례화된 교육 체계를 운영하고 있는 것으로 나타났으며, 종합병원 역시 높은 시행률을 보이고 있는 것으로 나타났다. 다만 일부 기관에서는 여전히 교육 주기가 불규칙한 사례가 확인되어 전 직원 대상 보안 교육의 체계적 운영과 지속적인 이행 점검이 필요할 것으로 나타났다.

〈표 5-87〉은 의료진 외 전 직원을 대상으로 실시한 정보보안 교육 참여 수준에 대해 조사한 결과를 나타낸 것이다.

의료기관 내 의료진 외 전 직원을 대상으로 정보보안 교육을 실시하고 있다고 응답한 의료기관(241개소)을 기준으로 교육 참여 수준을 살펴보면, '반드시 참여함(80~100%)'이 53.9%(130개소)로 가장 높게 나타났다. 다음으로 '대체로 참여함(60~79%)' 27.0%(65개소), '보통(40~59%)' 18.3%(44개소), '거의 참여하지 않음(20~39%)' 0.4%(1개소), '전혀 참여하지 않음(0~19%)' 0.4%(1개소) 순으로 나타났다. '반드시 참여함'과 '대체로 참여함'을 합한 적극적 참여 비율은 80.9%로 나타나, 대부분의 의료기관에서 비의료직 직원들이 정보보안 교육에 비교적 적극적으로 참여하고 있는 것으로 확인되었다.

의료기관 종별로 살펴보면 상급종합병원(40개소)은 '반드시 참여함' 62.5%(25개소), '대체로 참여함' 30.0%(12개소), '보통' 7.5%(3개소)로 나타나 모든 기관에서 일정 수준 이상의 참여가 이루어지고 있었다. 반면 종합병원(201개소)은 '반드시 참여함' 52.2%(105개소), '대체로 참여함' 26.4%(53개소), '보통' 20.4%(41개소), '거의 참여하지 않음'과 '전혀 참여하지 않음'이 각각 0.5%(1개소)로 나타나 상급종합병원에 비해 참여 강도가 다소 낮은 것으로 나타났다.

〈표 5-87〉 정보보안 교육 참석 수준(의료진 외 전 직원)

(단위: 개소, %)

구분		반드시 참여함 (80~100%)	대체로 참여함 (60~79%)	보통 (40~59%)	거의 참여 하지 않음 (20~39%)	전혀 참여 하지 않음 (0~19%)	합계
전체	전체	130 (53.9%)	65 (27.0%)	44 (18.3%)	1 (0.4%)	1 (0.4%)	241 (100%)
종별	상급종합병원	25 (62.5%)	12 (30.0%)	3 (7.5%)	0 (0.0%)	0 (0.0%)	40 (100%)
	종합병원	105 (52.2%)	53 (26.4%)	41 (20.4%)	1 (0.5%)	1 (0.5%)	201 (100%)
지역별	도시(동)	121 (53.3%)	62 (27.3%)	42 (18.5%)	1 (0.4%)	1 (0.4%)	227 (100%)
	비도시(읍·면)	9 (64.3%)	3 (21.4%)	2 (14.3%)	0 (0.0%)	0 (0.0%)	14 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

의료기관 내 의료진 외 전 직원을 대상으로 정보보안 교육을 실시하고 있다고 응답한 의료기관의 약 81%에서 비의료직 직원이 정보보안 교육에 적극적으로 참여하고 있는 것으로 나타났으며, 상급종합병원에서 종합병원보다 참여율이 더 높은 것으로 확인되었다. 이는 비의료직 직원들이 병원 내 정보보호 업무를 수행하는 실무 인력으로서 보안 교육의 중요성을 인식하고 있음을 보여주며, 기관 전반에 걸쳐 정보보안 문화가 점차 정착되고 있음을 시사한다.

〈표 5-88〉은 의료진 외 전 직원을 대상으로 주로 실시한 정보보안 교육 방법에 대해 조사한 결과를 나타낸 것이다.

의료기관 내 의료진 외 전 직원을 대상으로 정보보안 교육을 실시하고 있다고 응답한 의료기관(241개소)의 교육 운영 방식을 살펴보면, 58.1%(140개소)가 '민간전문기관 위탁교육'을 통해 교육을 실시하고 있는 것으로 나타나 가장 높은 비중을 차지하였다. 다음으로 '자체교육(내부강사)' 25.3%(61개소), '자체교육(외부강사)' 11.2%(27개소), '정부·지자체·공공기관 주관 교육' 5.4%(13개소) 순으로 나타났다. 전반적으로 민간전문기관 위탁 형태의 교육이 가장 일반적인 방식으로 운영되고 있으며, 내부 강사를 활용한 자체교육도 일정 수준에서 이루어지고 있는 것으로 확인되었다.

의료기관 종별로 살펴보면, 상급종합병원(40개소)은 '민간전문기관 위탁교육' 22.5%(9개소), '자체교육(외부강사)' 20.0%(8개소), '자체교육(내부강사)' 57.5%(23개소)로 나타나 내부강사를 활용한 자체교육 비중이 매우 높은 것으로 확인되었다. 반면 종합병원(201개소)은 '정부·지자체·공공기관 주관 교육' 6.5%(13개소), '민간전문기관 위탁교육' 65.2%(131개소), '자체교육(외부강사)' 9.5%(19개소), '자체교육(내부강사)' 18.9%(38개소)로 나타나 외부기관 중심의 교육 운영이 주를 이루고 있었다.

종합하면 의료진 외 전 직원 대상 정보보안 교육은 전반적으로 민간전문기관 위탁 형태가 중심으로 운영되고 있으며, 상급종합병원은 내부강사를 활용한 자체교육 중심의 자율적 교육 체계를 갖추고 있는 것으로 나타났다. 반면 종합병원은 외부기관 의존도가 높은 구조를 보이고 있어, 향후 내부 보안 전문 인력 확충과 자체 교육 운영 체계의 강화가 필요함을 시사한다.

〈표 5-88〉 주로 실시한 정보보안 교육 방법(의료진 외 전 직원)

(단위: 개소, %)

구분		정부/지자체/공공기관 교육 참여	민간전문 기관위탁	자체교육 (외부강사)	자체교육 (내부강사)	합계
전체	전체	13 (5.4%)	140 (58.1%)	27 (11.2%)	61 (25.3%)	241 (100%)
종별	상급종합병원	0 (0.0%)	9 (22.5%)	8 (20%)	23 (57.5%)	40 (100%)
	종합병원	13 (6.5%)	131 (65.2%)	19 (9.5%)	38 (18.9%)	201 (100%)
지역별	도시(동)	13 (5.7%)	128 (56.4%)	27 (11.9%)	59 (26%)	227 (100%)
	비도시(읍·면)	0 (0.0%)	12 (85.7%)	0 (0.0%)	2 (14.3%)	14 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

〈표 5-89〉는 의료진 외 전 직원을 대상으로 실시한 정보보안 교육 방식에 대해 조사한 결과를 나타낸 것이다.

의료기관 내 의료진 외 전 직원을 대상으로 정보보안 교육을 실시하고 있다고 응답한 의료기관(241개소)의 교육 방식(온라인·오프라인)을 살펴보면, 88.8%(214개소)가 '온라인' 교육을 실시하고 있었으며 11.2%(27개소)가 '오프라인' 교육을 운영하고 있었다. 대부분의 기관이 온라인 방식으로 교육을 운영하고 있어, 비의료직 직원의 근무 일정과 업무 환경을 고려한 효율적인 교육 방식이 정착된 것으로 나타났다.

의료기관 종별로 보면 상급종합병원(40개소)은 85.0%(34개소)가 온라인 교육을, 15.0%(6개소)가 오프라인 교육을 실시하고 있었다. 종합병원(201개소)은 89.6%(180개소)가 온라인, 10.4%(21개소)가 오프라인 교육을 운영하고 있어 종합병원에서 온라인 교육 비중이 다소 높은 것으로 확인되었다. 이는 상급종합병원이 일부 실습형 대면교육을 병행하는 반면, 종합병원은 온라인 중심의 비대면 교육 체계를 보다 적극적으로 활용하고 있음을 보여준다.

의료진 외 전 직원 대상 정보보안 교육은 대부분 온라인 방식으로 운영

되고 있으며, 이는 기관 규모와 관계없이 공통적으로 나타나는 경향이다. 상급종합병원은 일부 오프라인 교육을 병행하여 현장 실습형 교육을 강화하고 있으나, 전반적으로는 시간 효율성과 접근성을 고려한 온라인 중심의 교육 체계가 정착된 것으로 확인된다.

〈표 5-89〉 임직원 대상 정보보안 교육 방식(의료진 외 전 직원)

(단위: 개소, %)

구분		온라인	오프라인	합계
전체	전체	214 (88.8%)	27 (11.2%)	241 (100%)
종별	상급종합병원	34 (85.0%)	6 (15.0%)	40 (100%)
	종합병원	180 (89.6%)	21 (10.4%)	201 (100%)
지역별	도시(동)	201 (88.5%)	26 (11.5%)	227 (100%)
	비도시(읍·면)	13 (92.9%)	1 (7.1%)	14 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

나. 임직원 대상 정보보안 교육의 효과, 만족도

1) 임직원 대상 정보보안 교육의 효과

〈표 5-90〉은 임직원 대상 정보보안 교육의 효과에 대해 조사한 결과를 나타낸 것이다. 임직원 대상 정보보안 교육의 효과에 대해 응답한 의료기관(257개소) 중 '매우 효과적이다' 2.3%(6개소), '효과적이다' 23.7%(61개소), '보통이다' 67.7%(174개소)로 나타나 전체의 93.7%가 '보통 이상'으로 평가하였다. 반면 '효과가 없는 편이다'는 5.8%(15개소), '전혀 효과가 없다'는 0.4%(1개소)로 나타나 전반적으로 교육 효과에 대해 긍정적으로 인식하는 경향이 확인되었다.

의료기관 종별로 살펴보면 상급종합병원(41개소)은 '매우 효과적이다' 2.4%(1개소), '효과적이다' 34.1%(14개소), '보통이다' 61.0%(25개소),

‘효과가 없는 편이다’ 2.4%(1개소)로 나타나 대부분의 기관에서 교육 효과를 긍정적으로 평가하였다. 반면 종합병원(216개소)은 ‘매우 효과적이다’ 2.3%(5개소), ‘효과적이다’ 21.8%(47개소), ‘보통이다’ 69.0%(149개소), ‘효과가 없는 편이다’ 6.5%(14개소), ‘전혀 효과가 없다’ 0.5%(1개소)로 나타나 긍정적 평가 비율이 상급종합병원보다 다소 낮은 수준이었다.

〈표 5-90〉 임직원 대상 정보보안 교육의 효과

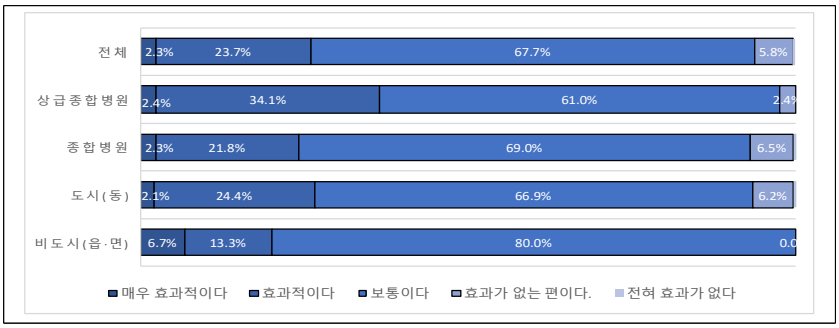
(단위: 개소, %)

구분		매우 효과적이다	효과적이다	보통이다	효과가 없는 편이다	전혀 효과가 없다	합계
전체	전체	6 (2.3%)	61 (23.7%)	174 (67.7%)	15 (5.8%)	1 (0.4%)	257 (100%)
종별	상급 종합병원	1 (2.4%)	14 (34.1%)	25 (61%)	1 (2.4%)	0 (0.0%)	41 (100%)
	종합병원	5 (2.3%)	47 (21.8%)	149 (69%)	14 (6.5%)	1 (0.5%)	216 (100%)
지역별	도시(동)	5 (2.1%)	59 (24.4%)	162 (66.9%)	15 (6.2%)	1 (0.4%)	242 (100%)
	비도시 (읍·면)	1 (6.7%)	2 (13.3%)	12 (80.0%)	0 (0.0%)	0 (0.0%)	15 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

종합하면 의료기관의 임직원 대상 정보보안 교육은 전반적으로 긍정적인 평가를 받고 있으며, ‘보통 이상’의 효과를 체감한 기관이 90% 이상으로 나타났다. 다만 일부 기관에서는 교육 효과에 대한 체감도가 낮은 응답도 확인되어 교육 내용의 실무 적용성 강화와 사례·실습 중심 교육 확대 등 교육 효과성 제고를 위한 개선이 필요한 것으로 나타났다.

[그림 5-20] 임직원 대상 정보보안 교육의 효과



출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

2) 임직원 대상 정보보안 교육의 만족도

〈표 5-91〉은 임직원 대상 정보보안 교육의 만족도에 대해 조사한 결과를 나타낸 것이다. 임직원 대상 정보보안 교육의 만족도 조사에 응답한 의료기관(257개소) 중 '매우 높다' 1.6%(4개소), '높은 편이다' 19.1%(49개소), '보통이다' 73.5%(189개소)로 나타나 전체의 94.2%가 '보통 이상'의 만족도를 보였다. 반면 '낮은 편이다'는 5.1%(13개소), '매우 낮다'는 0.8%(2개소)로 나타나 부정적 평가는 상대적으로 낮은 수준이었다.

의료기관 종별로 살펴보면 상급종합병원(41개소)은 '매우 높다' 2.4%(1개소), '높은 편이다' 24.4%(10개소), '보통이다' 70.7%(29개소), '낮은 편이다' 2.4%(1개소)로 나타나 전반적으로 긍정적 응답 비율이 높은 편이었다. 반면 종합병원(216개소)은 '매우 높다' 1.4%(3개소), '높은 편이다' 18.1%(39개소), '보통이다' 74.1%(160개소), '낮은 편이다' 5.6%(12개소), '매우 낮다' 0.9%(2개소)로 나타나 '보통' 수준의 응답 비율이 상대적으로 높은 것으로 나타났다.

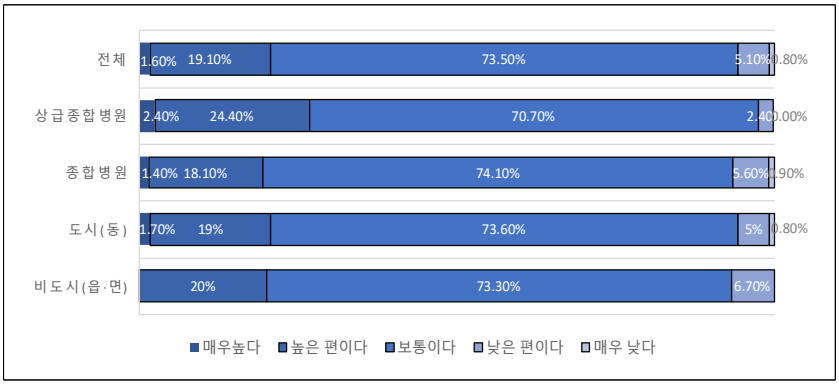
〈표 5-91〉 임직원 대상 정보보안 교육의 만족도

(단위: 개소, %)

구분		매우 높다	높은 편이다	보통이다	낮은 편이다	매우 낮다	합계
전체	전체	4 (1.6%)	49 (19.1%)	189 (73.5%)	13 (5.1%)	2 (0.8%)	257 (100%)
종별	상급 종합병원	1 (2.4%)	10 (24.4%)	29 (70.7%)	1 (2.4%)	0 (0.0%)	41 (100%)
	종합병원	3 (1.4%)	39 (18.1%)	160 (74.1%)	12 (5.6%)	2 (0.9%)	216 (100%)
지역별	도시(동)	4 (1.7%)	46 (19.0%)	178 (73.6%)	12 (5.0%)	2 (0.8%)	242 (100%)
	비도시 (읍·면)	0 (0.0%)	3 (20.0%)	11 (73.3%)	1 (6.7%)	0 (0.0%)	15 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

〔그림 5-21〕 임직원 대상 정보보안 교육의 만족도



출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

종합하면 의료기관의 임직원 대상 정보보안 교육에 대한 만족도는 전반적으로 '보통 이상' 수준이 높은 것으로 나타났으며, 대부분의 기관에서 교육 운영에 대해 일정 수준의 만족도를 보이고 있는 것으로 확인되었다. 다만 일부 기관에서는 낮은 만족도 응답도 확인되어 교육 내용의 실

무 적용성과 교육 방식 개선을 통한 교육 만족도 제고가 필요한 것으로 나타났다.

의료기관의 임직원들은 정보보안 교육에 대해 전반적으로 긍정적인 만족도를 보이고 있으며, 특히 '보통 이상' 응답이 전체의 90% 이상으로 나타났다. 이는 교육 내용이 현장 요구에 일정 수준 부합하고 있음을 보여준다. 다만 상급종합병원과 일부 기관에서는 상대적으로 낮은 만족도 응답도 확인되어 교육 내용의 실무 적용성과 교육 참여 흥미도 제고를 위한 교육 콘텐츠 개선이 필요한 것으로 나타났다.

7. 정보보호 및 정보보안(정책)

의료기관의 정보보호 관련 규정·지침 인식은 향후 기관 내 보안관리 제도의 정비 및 표준화 방향을 가늠하는 핵심 지표이다. 내부적으로 정보보호 및 보안 관련 규정을 제정·운영하고 있는지 여부는 각 기관의 보안관리 체계 구축 수준과 실질적인 거버넌스 운영 여부를 보여준다. 또한 규정에 포함된 기술적, 관리적, 물리적 보안 항목은 의료기관이 기술적 통제, 인적·조직적 관리, 물리적 접근통제 등 각 측면에서 얼마나 체계적으로 보안을 제도화하고 있는지를 평가하는 기준이 된다.

가. 정보보호 및 정보보안 관련 가이드라인 등 규정 필요성

〈표 5-92〉는 정보보호 및 정보보안 관련 가이드라인 등 규정 필요성에 대한 인식을 조사한 결과를 나타낸 것이다.

전체 응답기관(263개소) 중 97.0%(255개소)가 정보보호 관련 규정·지침의 필요성에 대해 '예'라고 응답하였으며, 3.0%(8개소)만이 '아니오'라

고 응답하였다. 이는 대부분의 의료기관이 정보보호 및 보안 관련 가이드라인이나 규정의 필요성을 인식하고 있는 것으로 나타났다.

〈표 5-92〉 정보보호 및 정보보안 관련 가이드라인 등 규정 필요성

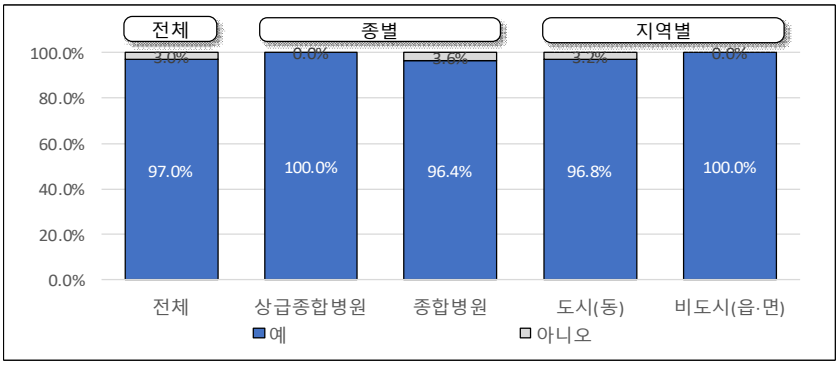
(단위: 개소, %)

구분		예	아니오	합계
전체	전체	255 (97.0%)	8 (3.0%)	263 (100%)
종별	상급종합병원	41 (100%)	0 (0.0%)	41 (100%)
	종합병원	214 (96.4%)	8 (3.6%)	222 (100%)
지역별	도시(동)	240 (96.8%)	8 (3.2%)	248 (100%)
	비도시(읍·면)	15 (100%)	0 (0.0%)	15 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

의료기관 종별로 살펴보면 상급종합병원(41개소)은 모든 기관(41개소, 100%)이 '예'라고 응답하여 보안 관련 규정의 필요성에 대해 전 기관이 공감하고 있는 것으로 나타났다. 종합병원(222개소) 역시 96.4%(214개소)가 '예', 3.6%(8개소)가 '아니오'라고 응답하여 대부분의 기관이 규정 제정의 필요성을 인식하고 있는 것으로 나타났다.

[그림 5-22] 정보보호 및 정보보안 관련 가이드라인 등 규정 필요성



출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

종합하면 의료기관 대부분이 정보보호 및 보안 관련 가이드라인·규정의 필요성을 인식하고 있으며, 이는 최근 증가하는 사이버 위협과 개인정보 침해 사고에 대응하기 위한 제도적 기반 마련의 중요성이 의료 현장에서도 폭넓게 인식되고 있음을 보여준다. 다만 일부 기관에서는 규정 필요성에 대한 인식이 낮은 응답도 확인되어 의료기관 전반의 정보보호 규정 정비와 보안 관리 체계의 제도화를 위한 정책적 지원이 필요한 것으로 나타났다.

나. 정보보호 및 정보보안 관련 자체 규정 여부

〈표 5-93〉은 정보보호 및 정보보안 관련 자체 규정 여부에 대해 조사한 결과를 나타낸 것이다.

전체 응답기관(263개소) 중 94.7%(249개소)가 내부적으로 정보보호 및 보안 관련 규정을 제정·운영하고 있는지에 대한 질문에 '예'라고 응답하였으며, 5.3%(14개소)는 '아니오'라고 응답하였다. 이는 대부분의 의료기관이 자체적인 정보보호 규정을 마련하고 있는 것으로 나타나 제도적 기반이 비교적 폭넓게 구축되어 있음을 보여준다.

의료기관 종별로 살펴보면 상급종합병원(41개소)은 모든 기관(41개소, 100%)이 자체 규정을 보유하고 있는 것으로 나타났다. 반면 종합병원(222개소)은 93.7%(208개소)가 '예', 6.3%(14개소)가 '아니오'라고 응답하여 일부 기관에서는 내부 보안규정이 마련되지 않은 것으로 나타났다.

종합하면 전체 의료기관의 약 95%가 정보보호 관련 자체 규정을 운영하고 있는 것으로 나타났으며, 이는 최근 강화된 법적·행정적 요구에 대응하기 위한 제도적 정비가 의료기관 전반에 확산되고 있음을 보여준다. 다만 일부 종합병원에서는 내부 규정이 마련되지 않았거나 체계적으로

운영되지 않는 사례도 확인되어 정보보호 규정의 제정 및 운영 체계 강화를 위한 제도적 보완이 필요한 것으로 나타났다.

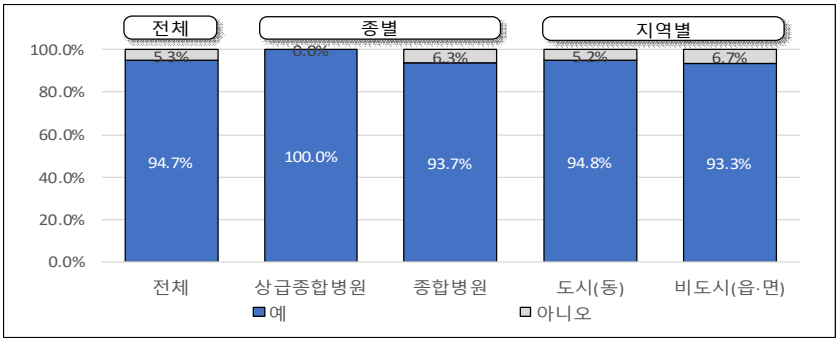
〈표 5-93〉 정보보호 및 정보보안 관련 자체 규정 여부

(단위: 개소, %)

구분		예	아니오	합계
전체	전체	249 (94.7%)	14 (5.3%)	263 (100%)
종별	상급종합병원	41 (100%)	0 (0.0%)	41 (100%)
	종합병원	208 (93.7%)	14 (6.3%)	222 (100%)
지역별	도시(동)	235 (94.8%)	13 (5.2%)	248 (100%)
	비도시(읍·면)	14 (93.3%)	1 (6.7%)	15 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

[그림 5-23] 정보보호 및 정보보안 관련 자체 규정 여부



출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

다. 정보보호 및 정보보안 관련 자체 규정 포함 내용

1) 정보보호 및 정보보안 관련 자체 규정 포함 내용: 기술적 보안

〈표 5-94〉는 정보보호 및 정보보안 관련 자체 규정에 포함된 내용 중 기술적 보안분야에 대해 조사한 결과를 나타낸 것이다.

전체 의료기관(263개소) 중 기술적 보안 항목의 내부 보안 규정 반영 현황을 살펴보면, '용역사업 보안'이 22.1%(58개소)로 가장 높은 비중을 차지하였다. 다음으로 '자료보안' 16.7%(44개소), '서버 보안' 11.4%(30개소) 순으로 나타났다. 반면 '정보통신시스템·네트워크 장비 보안' 3.4%(9개소), '인터넷 전화 보안' 4.2%(11개소), '클라우드 보안관리' 2.3%(6개소) 등은 상대적으로 낮은 비중을 보였다. 이는 의료기관의 내부 보안 규정이 데이터 보호 및 시스템 운영 안정성 확보와 관련된 항목 중심으로 구성되어 있는 것으로 나타났다.

의료기관 종별로 살펴보면 상급종합병원(41개소)은 '전자우편 보안' 36.6%, '업무시스템 보안' 24.4%, '비인가 IT 기기 관리' 19.5%, '원격근무시스템 보안' 14.6% 항목에서 비교적 높은 반영률을 보였다. 반면 '클라우드 보안관리', '정보보호시스템·네트워크 장비 보안', '인터넷 전화 보안', '서버 보안', '용역사업 보안' 항목은 규정에 반영되지 않은 것으로 나타났다.

종합병원(222개소)은 '용역사업 보안' 26.1%와 '자료보안' 19.4% 항목이 중심적으로 반영되어 있었으며, '서버 보안' 13.5%도 일정 수준 포함되어 있었다. 반면 'PC 등 단말기 보안' 9.0%(20개소), '업무시스템 보안' 8.1%(18개소), '전자우편 보안' 6.8%(15개소), '비인가 IT 기기 관리' 3.2%(7개소), '원격근무시스템 보안' 2.3%(5개소) 등은 상대적으로 낮은 수준으로 나타났다.

종합하면 의료기관의 기술적 보안 관련 규정은 주로 서버·운영시스템·자료보안 등 전통적인 보안관리 항목 중심으로 구성되어 있는 것으로 나타났다. 반면 클라우드, 원격근무, 비인가 IT 기기 관리 등 새로운 기술 환경과 관련된 보안 항목의 반영률은 상대적으로 낮게 나타나 의료기관 정보보호 규정이 변화하는 기술 환경에 대응할 수 있도록 기술적 보안 항목의 확대와 체계적 정비가 필요한 것으로 나타났다.

〈표 5-94〉 정보보호 및 정보보안 관련 자체 규정 포함 내용(기술적 보안분야)

(단위: 개소, %)

구분	클라우드 보안관리 (기술적)	정보보호시스템, 네트워크 장비 보안	인터넷 전화 보안
전체	6 (2.3%)	9 (3.4%)	11 (4.2%)
상급종합병원	0 (0.0%)	0 (0.0%)	0 (0.0%)
종합병원	6 (2.7%)	9 (4.1%)	11 (5.0%)
도시(동)	6 (2.4%)	9 (3.6%)	11 (4.4%)
비도시(읍·면)	0 (0.0%)	0 (0.0%)	0 (0.0%)
구분	서버 보안	용역사업 보안(기술적)	자료 보안
전체	30 (11.4%)	58 (22.1%)	44 (16.7%)
상급종합병원	0 (0.0%)	0 (0.0%)	1 (2.4%)
종합병원	30 (13.5%)	58 (26.1%)	43 (19.4%)
도시(동)	28 (11.3%)	55 (22.2%)	39 (15.7%)
비도시(읍·면)	2 (13.3%)	3 (20%)	5 (33.3%)
구분	PC 등 단말기 보안	업무시스템 보안	전자우편 보안
전체	21 (8.0%)	28 (10.6%)	30 (11.4%)
상급종합병원	1 (2.4%)	10 (24.4%)	15 (36.6%)
종합병원	20 (9.0%)	18 (8.1%)	15 (6.8%)
도시(동)	19 (7.7%)	27 (10.9%)	28 (11.3%)
비도시(읍·면)	2 (13.3%)	1 (6.7%)	2 (13.3%)
구분	비인가 IT 기기 관리	원격근무시스템 보안	합계
전체	15 (5.7%)	11 (4.2%)	263 (100%)
상급종합병원	8 (19.5%)	6 (14.6%)	41 (100%)
종합병원	7 (3.2%)	5 (2.3%)	222 (100%)
도시(동)	15 (6%)	11 (4.4%)	248 (100%)
비도시(읍·면)	0 (0.0%)	0 (0.0%)	15 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

2) 정보보호 및 정보보안 관련 자체 규정 포함 내용: 관리적 보안

〈표 5-95〉는 정보보호 및 정보보안 관련 자체 규정에 포함된 내용 중 관리적 보안분야에 대해 조사한 결과를 나타낸 것이다.

전체 응답기관(263개소) 중 의료기관이 내부 규정에 반영하고 있는 관리적 보안 항목을 살펴보면, '정보보안 감사'가 14.4%(38개소)로 가장 높은 비율을 보였다. 다음으로 '예산' 12.2%(32개소), '정보보안 교육' 9.9%(26개소) 순으로 나타났다. 반면 '정보보안에 대한 기관장의 관심' 2.7%(7개소)와 '클라우드 정책' 3.0%(8개소)는 상대적으로 낮은 비중을 보였다. 이는 의료기관의 관리적 보안 규정이 감사, 예산, 교육 등 전통적인 관리 항목 중심으로 구성되어 있는 것으로 나타났다.

의료기관 종별로 살펴보면 상급종합병원(41개소)은 '평가 결과에 따른 미비점 개선' 24.4%(10개소), '보안위규 조치 및 예방대책 마련' 22.0%(9개소) 항목에서 비교적 높은 반영률을 보였다. 반면 '책무', '인력', '조직', '인센티브', '예산', '정보보안 감사' 항목은 규정에 반영되지 않은 것으로 나타났다. 종합병원(222개소)은 '정보보안 감사' 17.1%(38개소)와 '예산' 14.4%(32개소)이 중심적으로 반영되어 있었으며, '정보보안 교육' 11.3%(25개소)도 일정 수준 포함되어 있었다.

〈표 5-95〉 정보보호 및 정보보안 관련 자체 규정 포함 내용(관리적 보안분야)

(단위: 개소, %)

구분	책무	인력	조직
전체	18 (6.8%)	12 (4.6%)	14 (5.3%)
상급종합병원	0 (0.0%)	0 (0.0%)	0 (0.0%)
종합병원	18 (8.1%)	12 (5.4%)	14 (6.3%)
도시(동)	18 (7.3%)	10 (4%)	14 (5.6%)
비도시(읍·면)	0 (0.0%)	2 (13.3%)	0 (0.0%)

구분	인센티브	예산	정보보안 감사[1]
전체	14 (5.3%)	32 (12.2%)	38 (14.4%)
상급종합병원	0 (0.0%)	0 (0.0%)	0 (0.0%)
종합병원	14 (6.3%)	32 (14.4%)	38 (17.1%)
도시(동)	14 (5.6%)	29 (11.7%)	35 (14.1%)
비도시(읍·면)	0 (0.0%)	3 (20%)	3 (20%)
구분	정보보안 교육	보안성 검토[2]	용역사업 보안[3]
전체	26 (9.9%)	11 (4.2%)	17 (6.5%)
상급종합병원	1 (2.4%)	1 (2.4%)	2 (4.9%)
종합병원	25 (11.3%)	10 (4.5%)	15 (6.8%)
도시(동)	23 (9.3%)	10 (4%)	17 (6.9%)
비도시(읍·면)	3 (20%)	1 (6.7%)	0 (0.0%)
구분	소프트웨어 개발보안	망분리 정책	정보자산 관리
전체	17 (6.5%)	11 (4.2%)	9 (3.4%)
상급종합병원	3 (7.3%)	2 (4.9%)	4 (9.8%)
종합병원	14 (6.3%)	9 (4.1%)	5 (2.3%)
도시(동)	16 (6.5%)	10 (4%)	9 (3.6%)
비도시(읍·면)	1 (6.7%)	1 (6.7%)	0 (0.0%)
구분	보안위규 조치 및 예방대책 마련	평가 결과에 따른 미비점 개선	정보보안에 대한 기관장의 관심
전체	12 (4.6%)	14 (5.3%)	7 (2.7%)
상급종합병원	9 (22%)	10 (24.4%)	5 (12.2%)
종합병원	3 (1.4%)	4 (1.8%)	2 (0.9%)
도시(동)	11 (4.4%)	14 (5.6%)	7 (2.8%)
비도시(읍·면)	1 (6.7%)	0 (0.0%)	0 (0.0%)
구분	클라우드 정책	기반시설 보호대책	합계
전체	8 (3%)	3 (1.1%)	263 (100%)
상급종합병원	3 (7.3%)	1 (2.4%)	41 (100%)
종합병원	5 (2.3%)	2 (0.9%)	222 (100%)
도시(동)	8 (3.2%)	3 (1.2%)	248 (100%)
비도시(읍·면)	0 (0.0%)	0 (0.0%)	15 (100%)

주: 1. 정보보안 감사는 상위기관 점검 또는 인증 심사 등 외부 점검을 의미함.
2. 보안성 검토는 제품 구매 시 네트워크 또는 장비 기능 등보안성 검토 수행 후 구입을 의미함.
3. 용역사업 보안은 관리적 측면, 계약서 상의 보안관련 내용 여부를 의미함.
출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

종합하면 의료기관의 관리적 보안 규정은 정보보안 감사, 예산, 교육 등 전통적 관리 항목 중심으로 운영되고 있는 것으로 나타났다. 반면 기관장의 보안 리더십, 클라우드 정책 등 변화하는 보안 환경을 반영한 관리 항목의 반영률은 상대적으로 낮게 나타났다. 또한 상급종합병원은 평가 결과 개선과 위규 예방대책 등 제도적 관리 항목 중심으로, 종합병원은 감사와 예산 중심의 운영 관리에 집중하는 경향이 확인되었다. 이에 따라 의료기관의 관리적 보안 체계를 조직 리더십 강화와 신기술 환경 대응을 포함한 전략적 관리 체계로 확대·정비하는 개선이 필요한 것으로 나타났다.

3) 정보보호 및 정보보안 관련 자체 규정 포함 내용: 물리적 보안

〈표 5-96〉은 정보보호 및 정보보안 관련 자체 규정에 포함된 내용 중 물리적 보안분야에 대해 조사한 결과를 나타낸 것이다.

전체 응답기관(263개소) 중 내부 규정에 포함된 물리적 보안 항목을 살펴보면, '영상감시장치(CCTV) 운영 및 출입자 통제'가 226개 기관(85.9%)으로 가장 높은 비중을 차지하였다. 이는 대부분의 의료기관이 물리적 보안을 위한 기본적인 통제 체계를 갖추고 있는 것으로 나타났다. 이어 '전산실·출입자 관련 설정 및 기록보안'이 17개 기관(6.5%), '출입통제시스템 운영'이 5개 기관(1.9%) 순으로 나타났다. 반면 '전산실 통제구역 지정'은 1개 기관(0.4%)에 불과해 전산실 접근 구역을 공식적으로 지정·관리하는 제도적 반영 수준은 매우 낮은 것으로 나타났다.

의료기관 종별로 살펴보면 상급종합병원(41개소)은 '영상감시장치(CCTV) 설치 및 운영' 92.7%(38개소)로 가장 높은 비중을 보였으며, '출입통제시스템 운영' 2.4%(1개소), '전산실 출입자 권한 설정 및 기록 관

리’ 2.4%(1개소), ‘외부인(방문자) 출입 절차 및 통제’ 2.4%(1개소) 순으로 나타났다. 반면 ‘전산실 통제구역 지정’ 항목은 규정에 반영된 사례가 없는 것으로 나타났다. 종합병원(222개소)은 ‘영상감시장치(CCTV) 설치 및 운영’ 84.7%(188개소), ‘전산실·출입자 기록보안’ 7.2%(16개소), ‘외부인(방문자) 출입 절차 및 통제’ 5.9%(13개소) 순으로 나타나 상급종합병원과 유사한 구조를 보였다.

〈표 5-96〉 정보보호 및 정보보안 관련 자체 규정 포함 내용(물리적 보안 분야)

구분	전산실 통제구역 지정	출입통제시스템 운영	전산실 출입자 권한 설정 및 기록 관리
전체	1 (0.4%)	5 (1.9%)	17 (6.5%)
상급종합병원	0 (0.0%)	1 (2.4%)	1 (2.4%)
종합병원	1 (0.5%)	4 (1.8%)	16 (7.2%)
도시(동)	1 (0.4%)	5 (2.0%)	16 (6.5%)
비도시(읍·면)	0 (0.0%)	0 (0.0%)	1 (6.7%)
구분	외부인(방문자) 출입 절차 및 통제	영상감시(CCTV) 설치 및 운영	합계
전체	14 (5.3%)	226 (85.9%)	263 (100%)
상급종합병원	1 (2.4%)	38 (92.7%)	41 (100%)
종합병원	13 (5.9%)	188 (84.7%)	222 (100%)
도시(동)	13 (5.2%)	213 (85.9%)	248 (100%)
비도시(읍·면)	1 (6.7%)	13 (86.7%)	15 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

종합하면 의료기관의 물리적 보안 규정은 ‘영상감시장치(CCTV) 운영 및 출입자 통제’ 중심으로 구성되어 있어 기본적인 물리적 통제 체계는 비교적 널리 구축된 것으로 나타났다. 반면 전산실 통제구역 지정, 출입 기록 관리, 출입 통제 시스템 운영 등 주요 정보 자산 보호와 관련된 세부 관리 항목의 반영률은 상대적으로 낮은 수준으로 나타났다. 이에 따라 의료기관의 물리적 보안 관리 체계를 주요 정보 자산 보호 중심으로 정교화

하고 접근통제 및 통제구역 관리 체계를 강화하는 개선이 필요한 것으로 나타났다.

8. 정보보안 업무 관련 애로사항

가. 정보보안 업무 관련 가장 큰 애로사항

〈표 5-97〉은 의료기관이 정보보안 업무를 수행하는 과정에서 직면하고 있는 주요 애로사항을 1·2·3순위로 조사한 결과를 나타낸 것이다.

전체 응답기관(263개소)을 기준으로 1순위 응답 항목을 살펴보면, '보안 인력 부족'을 선택한 기관이 69.6%(183개소)로 가장 높은 비중을 차지하였다. 다음으로 '보안 예산 부족'이 18.6%(49개소)로 나타났으며, '시스템 노후화 및 기술 지원 부족' 4.9%(13개소), '보안 기술적 지식 부족' 4.6%(12개소), '(자체) 보안 관련 정책 및 규정의 미비' 1.9%(5개소) 순으로 나타났다. 기타 응답은 1개소(0.4%)로 나타났다.

2순위 응답에서는 '보안 예산 부족'이 58.9%(155개소)로 가장 높은 비중을 차지하였으며, '보안 인력 부족' 16.0%(42개소), '보안 기술적 지식 부족' 13.7%(36개소) 순으로 나타났다. 이어 '시스템 노후화 및 기술 지원 부족' 8.4%(22개소), '(자체) 보안 관련 정책 및 규정의 미비' 2.7%(7개소) 순으로 나타났으며, 기타 응답은 0.4%(1개소)로 확인되었다.

3순위 응답에서는 '보안 기술적 지식 부족'이 39.9%(105개소)로 가장 높은 비중을 보였으며, '시스템 노후화 및 기술 지원 부족' 29.3%(77개소), '보안 예산 부족' 18.6%(49개소) 등이 뒤를 이었다.

〈표 5-98〉과 같이 의료기관이 정보보안 업무 관련 애로사항에 대해 우선순위별 가중치(1순위 3점, 2순위 2점, 3순위 1점)를 부여하여 중요도

를 산출한 결과이다.

'보안 인력 부족', 가장 중요한 문제로 인식되고 있는 것으로 나타났다. 다음으로 '보안 예산 부족', '보안 기술적 지식 부족', '시스템 노후화 및 기술 지원 부족', '(자체) 보안 관련 정책 및 규정의 미비', '기타' 순으로 나타났다.

기타 응답으로는 인력과 예산 문제 외에도 '경영진 또는 전 직원의 정보보안 인식 부족', '다양한 보안 솔루션 관리의 어려움' 등이 언급되었다.

〈표 5-97〉 정보보안 업무 관련 가장 큰 애로사항(순위별 빈도)

(단위: 개소, %)

항목	1순위	2순위	3순위
보안 인력 부족	183 (69.6%)	42 (16%)	17 (6.5%)
보안 예산 부족	49 (18.6%)	155 (58.9%)	35 (13.3%)
보안 기술적 지식 부족	12 (4.6%)	36 (13.7%)	105 (39.9%)
시스템 노후화 및 기술 지원 부족	13 (4.9%)	22 (8.4%)	77 (29.3%)
(자체) 보안 관련 정책 및 규정의 미비	5 (1.9%)	7 (2.7%)	25 (9.5%)
기타	1 (0.4%)	1 (0.4%)	4 (1.5%)
합계	263 (100%)	263 (100%)	263 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

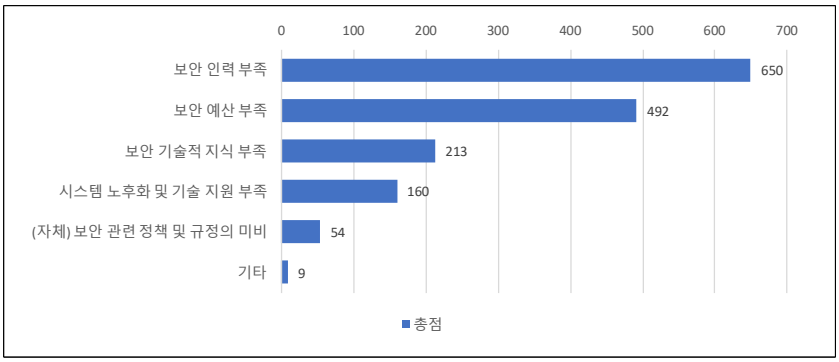
〈표 5-98〉 정보보안 업무 관련 가장 큰 애로사항(중요도 순위)

(단위: 개소, %)

항목	응답수	총점	중요도 순위
보안 인력 부족	242	650	1
보안 예산 부족	239	492	2
보안 기술적 지식 부족	153	213	3
시스템 노후화 및 기술 지원 부족	112	160	4
(자체) 보안 관련 정책 및 규정의 미비	37	54	5
기타	6	9	6

주: 1순위는 3점, 2순위는 2점, 1순위에는 1점의 점수를 부여하여 가중 평균 점수 산출하였음.
출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

[그림 5-24] 정보보안 업무 관련 가장 큰 애로사항(중요도 순위)



출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

종합하면 순위별 응답 빈도와 중요도 분석 결과 모두에서 보안 인력과 예산 부족이 의료기관 정보보안 운영의 핵심 애로 요인으로 나타났다. 이는 기술적 지원이나 제도 정비의 문제보다 정보보안 인력 확보와 예산 확보 등 기본적인 자원의 부족이 의료기관 보안 관리의 구조적 한계로 작용하고 있음을 보여준다. 이에 따라 의료기관의 정보보안 역량 강화를 위해 전문 인력 확보 지원과 안정적인 보안 예산 확보를 위한 정책적 지원 체계 마련이 필요한 것으로 나타났다.

나. 어려움을 해결하기 위해 가장 필요한 지원

〈표 5-99〉는 앞서 제시된 정보보안 관련 애로사항을 해소하기 위해 필요한 지원 요소를 1·2·3순위별로 조사한 결과를 나타낸 것이다.

전체 응답기관(263개소)을 기준으로 1순위 응답 항목을 살펴보면, '정부의 재정적 지원'이 66.9%(176개소)로 가장 높은 비중을 차지하였다. 다음으로 '전문 인력 지원'이 22.8%(60개소)로 나타났으며, '정보보안 관련 교육 및 훈련'은 6.1%(16개소), '기술적 컨설팅'은 3.0%(8개소)로 상

대적으로 낮은 수준을 보였다.

2순위 응답 항목에서는 '전문 인력 지원'이 55.1%(145개소)로 가장 높은 비중을 보였으며, 이어 '정보보안 관련 교육 및 훈련' 19.8%(52개소), '정부의 재정적 지원' 16.7%(44개소), '기술적 컨설팅' 8.4%(22개소) 순으로 나타났다.

3순위 응답 항목에서는 '정보보안 관련 교육 및 훈련'이 51.3%(135개소)로 가장 높은 비중을 보였으며, '기술적 컨설팅' 29.3%(77개소), '전문 인력 지원' 11.0%(29개소), '정부의 재정적 지원' 7.2%(19개소) 순으로 나타났다.

종합하면 의료기관은 정보보안 운영 과정에서 발생하는 애로사항을 해소하기 위해 재정 지원과 전문 인력 지원을 가장 중요한 정책적 지원 요소로 인식하고 있는 것으로 나타났다. 또한 교육·훈련 및 기술적 컨설팅 등 역량 강화 지원에 대한 요구도 일정 수준 확인되었다. 이에 따라 의료기관의 정보보안 역량 강화를 위해 재정 지원 확대와 전문 인력 지원을 중심으로 교육·훈련 및 기술 지원을 연계한 종합적인 지원 체계 구축이 필요한 것으로 나타났다.

〈표 5-99〉 어려움을 해결하기 위해 가장 필요한 지원(순위별 빈도)

(단위: 개소, %)

항목	1순위	2순위	3순위
정부의 재정적 지원	176 (66.9%)	44 (16.7%)	19 (7.2%)
전문인력 지원	60 (22.8%)	145 (55.1%)	29 (11%)
정보보안 관련 교육 및 훈련	16 (6.1%)	52 (19.8%)	135 (51.3%)
기술적 컨설팅	8 (3%)	22 (8.4%)	77 (29.3%)
기타	3 (1.1%)	0 (0.0%)	3 (1.1%)
합계	263 (100%)	263 (100%)	263 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

〈표 5-100〉은 정보보안 업무 수행 과정에서 겪는 어려움을 해소하기 위해 어떤 형태의 지원을 중요하게 인식하고 있는지에 대해 우선순위별 가중치(1순위 3점, 2순위 2점, 3순위 1점)를 부여하여 중요도를 산출한 결과이다.

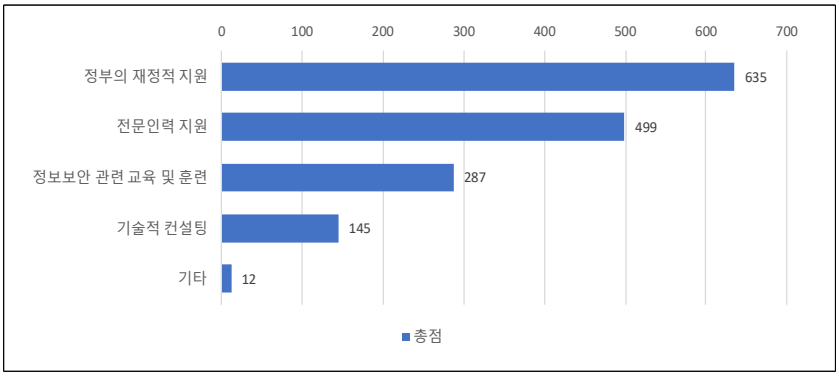
'정부의 재정적 지원', '전문 인력 지원', '정보보안 관련 교육 및 훈련', '기술적 컨설팅', '기타' 순으로 나타났다. 기타 응답에서는 인력 및 예산 문제 외에도 '기관장의 정보보안에 대한 적극적 관심'과 '보안 관련 제도의 법적 강제성 강화' 등이 언급되었다.

〈표 5-100〉 어려움을 해결하기 위해 가장 필요한 지원(중요도 순위)

항목	응답수	총점	중요도 순위
정부의 재정적 지원	239	635	1
전문인력 지원	234	499	2
정보보안 관련 교육 및 훈련	203	287	3
기술적 컨설팅	107	145	4
기타	6	12	5

주: 1순위는 3점, 2순위는 2점, 1순위에는 1점의 점수를 부여하여 가중 평균 점수 산출하였음.
출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

[그림 5-25] 어려움을 해결하기 위해 가장 필요한 지원(중요도 순위)



출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

순위별 응답 빈도와 중요도 분석 결과를 종합하면 의료기관의 정보보안 정책 실행 과정에서 가장 큰 제약 요인은 재정과 인력 부족으로 나타났다. 이는 의료기관 내부의 노력만으로 해결하기 어려운 구조적 한계가 존재함을 보여준다. 또한 의료기관들은 기술적 컨설팅이나 교육 지원보다 예산 확보와 전문 인력 지원을 보다 중요한 정책 지원 요소로 인식하고 있는 것으로 나타났다. 이에 따라 의료기관의 정보보안 역량 강화를 위해 안정적인 보안 예산 지원과 전문 인력 양성·배치 체계를 포함한 정책적 지원 체계 구축이 필요한 것으로 나타났다.

9. 보안사고(침해사고) 등

보안사고(침해사고) 등' 영역은 의료기관의 보안사고 대응 역량과 정보보호 관리 수준을 종합적으로 평가하기 위해 구성된 항목이다. 본 영역에서는 보안사고 발생 가능성에 대한 인식, 실제 사고 경험 여부, 사고 신고 체계, 주요 정보시스템의 보안 적용 수준 등을 중심으로 조사가 이루어졌다. 이를 통해 의료기관이 사이버 위협을 어느 수준으로 인식하고 있으며, 사고 발생 시 어떤 절차로 대응·신고하고 주요 시스템에서 어떠한 수준의 보안 통제를 적용하고 있는지를 파악할 수 있다. 또한 인증·접속 관리, 단말기·네트워크·DB·서버·애플리케이션 보안, 통합보안관리, 모바일 보안 등 세부 기술 영역별 보안 적용 현황을 분석하여 병원 규모(상급종합병원·종합병원) 및 지역(도시·비도시)별 보안 인프라 수준의 차이를 진단할 수 있도록 구성되었다.

가. 보안사고(침해사고) 발생 가능성

〈표 5-101〉은 소속 의료기관의 보안사고(침해사고) 발생 가능성에 대한 인식에 대해 조사한 결과를 나타낸 것이다.

전체 응답기관(263개소)을 기준으로 소속 의료기관의 보안사고(침해사고) 발생 가능성에 대한 인식을 살펴보면, '보통이다'가 57.8%(152개소)로 가장 높은 비중을 차지하였다. 다음으로 '그렇지 않다' 22.1%(58개소), '그렇다' 17.5%(46개소) 순으로 나타났다. '매우 그렇다'는 0.8%(2개소), '매우 그렇지 않다'는 1.9%(5개소)로 나타나 극단적인 응답은 상대적으로 적은 수준이었다. 이는 대부분의 의료기관이 보안사고 발생 가능성을 중간 수준으로 인식하고 있는 것으로 나타났다.

〈표 5-101〉 소속 의료기관의 보안사고(침해사고) 발생 가능성이 높은지에 대한 의견

(단위: 개소, %)

구분		매우 그렇다	그렇다	보통이다	그렇지 않다	매우 그렇지 않다	합계
전체	전체	2 (0.8%)	46 (17.5%)	152 (57.8%)	58 (22.1%)	5 (1.9%)	263 (100%)
종별	상급종합병원	2 (4.9%)	15 (36.6%)	14 (34.1%)	10 (24.4%)	0 (0.0%)	41 (100%)
	종합병원	0 (0.0%)	31 (14%)	138 (62.2%)	48 (21.6%)	5 (2.3%)	222 (100%)
지역별	도시(동)	2 (0.8%)	42 (16.9%)	145 (58.5%)	55 (22.2%)	4 (1.6%)	248 (100%)
	비도시(읍·면)	0 (0.0%)	4 (26.7%)	7 (46.7%)	3 (20%)	1 (6.7%)	15 (100%)

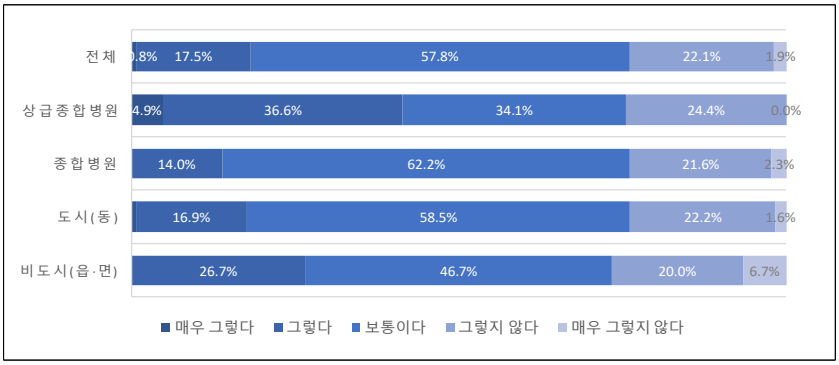
출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

의료기관 종별로 살펴보면 상급종합병원(41개소)은 '그렇다' 36.6%(15개소), '보통이다' 34.1%(14개소), '그렇지 않다' 24.4%(10개소) 순

으로 나타나 비교적 다양한 인식 분포를 보였다. 또한 '매우 그렇다' 응답이 4.9%(2개소)로 나타나 일부 기관에서는 보안사고 발생 가능성을 높게 인식하고 있는 것으로 나타났다. 반면 '매우 그렇지 않다' 응답은 없었다.

종합병원(222개소)은 '보통이다' 62.2%(138개소)로 응답이 가장 높은 비중을 차지하였으며, '그렇지 않다' 21.6%(48개소), '그렇다' 14.0%(31개소), '매우 그렇지 않다' 2.3%(5개소) 순으로 나타났다. '매우 그렇다' 응답은 없는 것으로 나타났다.

[그림 5-26] 소속 의료기관의 보안사고(침해사고) 발생 가능성이 높은지에 대한 의견



출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

종합하면 대부분의 의료기관이 보안사고 발생 가능성을 '보통' 수준으로 인식하고 있는 것으로 나타났으며, 상급종합병원은 종합병원에 비해 보안 위험에 대한 인식 수준이 상대적으로 높은 것으로 나타났다. 반면 종합병원에서는 보안사고 발생 가능성에 대한 인식이 비교적 낮거나 중간 수준에 집중되는 경향이 확인되었다. 이에 따라 의료기관의 보안 위협 인식 수준을 높이고 사고 대응 역량을 강화하기 위한 교육 및 보안 인식 제고 프로그램 확대 등 제도적 보완이 필요한 것으로 나타났다.

나. 보안사고(침해사고) 발생 경험

〈표 5-102〉는 최근 3년간 의료기관의 보안사고(침해사고) 발생 여부에 대해 조사한 결과를 나타낸 것이다.

최근 3년간 의료기관의 보안사고 발생 여부에 대한 응답을 살펴보면, 전체 응답기관(263개소) 중 '보안 사고가 발생했다'고 응답한 기관은 6.5%(17개소)로 나타났으며, '발생하지 않았다'고 응답한 기관은 93.5%(246개소)로 대다수를 차지하였다. 이는 전체 의료기관 기준 약 15곳 중 1곳 정도가 최근 3년 이내 실제 보안사고를 경험한 것으로 나타난 결과이다.

의료기관 종별로 살펴보면 상급종합병원(41개소)은 12.2%(5개소)에서 보안사고가 발생한 것으로 나타났으며, 87.8%(36개소)는 사고가 발생하지 않았다고 응답하였다. 반면 종합병원(222개소)은 5.4%(12개소)에서 보안사고가 발생하였고, 94.6%(210개소)는 사고가 없었다고 응답하였다.

〈표 5-102〉 최근 3년 간 보안사고(침해사고) 발생 여부

(단위: 개소, %)

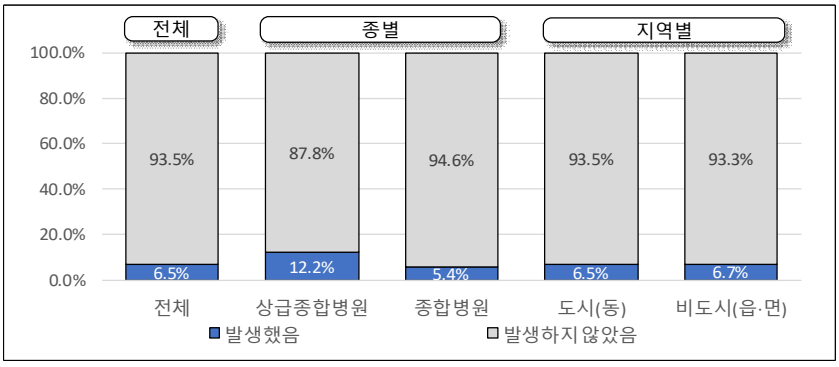
구분		발생했음	발생하지 않았음	합계
전체	전체	17 (6.5%)	246 (93.5%)	263 (100%)
종별	상급종합병원	5 (12.2%)	36 (87.8%)	41 (100%)
	종합병원	12 (5.4%)	210 (94.6%)	222 (100%)
지역별	도시(동)	16 (6.5%)	232 (93.5%)	248 (100%)
	비도시(읍·면)	1 (6.7%)	14 (93.3%)	15 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

종합하면 전체 의료기관의 보안사고 발생률은 6.5% 수준으로 나타났으나, 상급종합병원에서 종합병원보다 상대적으로 높은 발생률을 보였다. 이는 대형 병원이 공격 대상이 될 가능성이 높거나, 보안사고 탐지 및

보고 체계가 보다 체계적으로 운영되고 있기 때문일 가능성을 함께 시사한다. 한편 종합병원의 경우 보안사고 발생률이 상대적으로 낮게 나타났으나, 실제 사고 발생 여부와 별개로 사고 탐지 또는 보고가 충분히 이루어지지 않았을 가능성도 고려될 필요가 있다. 이에 따라 의료기관 전반에서 보안사고 탐지 및 보고 체계를 강화하고 침해사고 대응 절차의 표준화와 이행 점검을 확대하는 등 제도적 개선이 필요한 것으로 나타났다.

[그림 5-27] 최근 3년 간 보안사고(침해사고) 발생 여부



출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

〈표 5-103〉은 최근 3년간 의료기관에서 발생한 보안사고(침해사고)의 유형에 대해 조사한 결과를 나타낸 것이다.

전체 28건의 보안사고(침해사고) 중 '악성코드'가 8건(28.6%)으로 가장 높은 비중을 차지하였으며, 이어 '해킹메일' 7건(25.0%), '웹해킹', '네트워크 침입', '유해IP'가 각각 3건(10.7%), '정보 수집' 2건(7.1%), '홈페이지 위변조'와 '기타'가 각각 1건(3.6%) 순으로 나타났다. 기타 응답은 내부 침해 사례로 확인되었으며 '서비스 거부(DoS)' 사례는 보고되지 않았다. 이러한 결과는 의료기관에서 발생한 보안사고(침해사고)가 주로 악성메일, 악성코드 감염, 네트워크 침입 등 외부 공격형 위협에 의해 발생

하는 비중이 높음을 보여준다.

의료기관 종별로 살펴보면 상급종합병원에서는 총 13건의 보안사고(침해사고)가 보고되었으며, 그 중 '해킹메일'이 4건(30.8%)으로 가장 높은 비중을 차지하였다. 이어 '악성코드' 3건(23.1%), '네트워크 침입'과 '유해IP'가 각각 2건(15.4%), '웹해킹'과 '정보 수집'이 각각 1건(7.7%) 순으로 나타났다.

〈표 5-103〉 최근 3년 간 보안사고(침해사고) 발생 유형(복수 선택)

(단위: 개소, %)

구분	웹해킹	홈페이지 위변조	해킹메일	서비스거부	네트워크침입
전체	3 (10.7%)	1 (3.6%)	7 (25.0%)	0 (0.0%)	3 (10.7%)
상급종합병원	1 (7.7%)	0 (0.0%)	4 (30.8%)	0 (0.0%)	2 (15.4%)
종합병원	2 (13.3%)	1 (6.7%)	3 (20.0%)	0 (0.0%)	1 (6.7%)
도시(동)	3 (11.1%)	1 (3.7%)	7 (25.9%)	0 (0.0%)	3 (11.1%)
비도시(읍·면)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
구분	정보수집	악성코드	유해IP	기타	합계
전체	2 (7.1%)	8 (28.6%)	3 (10.7%)	1 (3.6%)	28 (100%)
상급종합병원	1 (7.7%)	3 (23.1%)	2 (15.4%)	0 (0.0%)	13 (100%)
종합병원	1 (6.7%)	5 (33.3%)	1 (6.7%)	1 (6.7%)	15 (100%)
도시(동)	2 (7.4%)	7 (25.9%)	3 (11.1%)	1 (3.7%)	27 (100%)
비도시(읍·면)	0 (0.0%)	1 (100%)	0 (0.0%)	0 (0.0%)	1 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

반면 종합병원에서는 총 15건의 사고가 보고되었으며, '악성코드'가 5건(33.3%)으로 가장 높은 비중을 차지하였고, '해킹메일' 4건(30.8%), '웹해킹' 2건(13.3%), '홈페이지 위변조', '네트워크 침입', '정보 수집', '유해IP', '기타'가 각각 1건(6.7%)으로 나타나 상대적으로 다양한 유형의 사고가 분포하는 특징을 보였다.

종합하면 최근 3년간 의료기관에서 발생한 보안사고는 이메일을 매개

로 한 침투형 공격과 악성코드 감염 등 외부 기인형 위협이 주요 유형으로 나타났다. 또한 상급종합병원은 외부 이메일 및 네트워크 기반 공격의 비중이 높은 반면, 종합병원은 다양한 유형의 공격에 노출되는 경향이 확인되었다. 이에 따라 의료기관의 보안사고 예방을 위해 이메일 보안 강화, 악성코드 탐지 및 차단 체계 구축, 네트워크 침입 대응 체계 강화 등 기술적 보안 통제 수준을 전반적으로 강화할 필요가 있는 것으로 나타났다.

〈표 5-104〉는 보안사고(침해사고) 발생 시 평균 인지 시간에 대해 조사한 결과를 나타낸 것이다.

최근 3년간 의료기관에서 보안사고(침해사고)가 발생했을 때 이를 인지하기까지 소요된 시간을 살펴보면, 전체 17건의 보안사고 사례 중 '4시간~12시간 미만'이 8건(47.1%)으로 가장 높은 비중을 차지하였다. 이어 '1~4시간 미만'이 6건(35.3%), '1시간 미만'이 2건(11.8%) 순으로 나타났다. '12시간 이상'이 소요된 사례는 1건(5.9%)으로 나타났으며, 기타 응답은 없었다. 전체적으로 보안사고의 약 82%가 12시간 이내에 인지된 것으로 나타나 대부분의 사고가 비교적 단시간 내에 탐지된 것으로 확인되었다.

의료기관 종별로 살펴보면 상급종합병원에서 발생한 5건의 사고 중 '1~4시간 미만'이 2건(40.0%), '4~12시간 미만'이 3건(60.0%)으로 나타나 모든 사고가 12시간 이내에 인지된 것으로 조사되었다. 반면 종합병원에서는 총 12건의 사고 중 '1시간 미만' 2건(16.7%), '1~4시간 미만' 4건(33.3%), '4~12시간 미만' 5건(41.7%), '12시간 이상' 1건(8.3%)으로 나타나 일부 사고의 경우 인지까지 상대적으로 더 많은 시간이 소요된 사례도 확인되었다.

이러한 결과를 종합하면 의료기관의 보안사고 인지 시간은 대체로 12시간 이내에 이루어지는 경우가 많은 것으로 나타났다. 상급종합병원은

상시 모니터링 체계와 전담 인력을 기반으로 비교적 안정적인 탐지 체계를 운영하는 것으로 나타난 반면, 종합병원은 병원별 보안관리 여건에 따라 사고 인지 시간이 1시간 미만부터 12시간 이상까지 다양한 분포를 보였다. 이는 일부 종합병원에서는 신속한 탐지가 이루어지고 있으나, 상당수 기관에서는 보안관제 인프라나 상시 감시 체계의 수준에 따라 사고 인지 시간이 지연될 가능성이 있음을 보여준다. 이러한 결과는 기관 간 보안 탐지 역량의 편차가 존재함을 시사한다.

〈표 5-104〉 보안사고(침해사고) 발생 시 평균 인지 시간

(단위: 개소, %)

구분		1시간 미만	1~4시간 미만	4시간~12시간 미만	12시간 이상	기타	합계
전체	전체	2 (11.8%)	6 (35.3%)	8 (47.1%)	1 (5.9%)	0 (0.0%)	17 (100%)
종별	상급종합병원	0 (0.0%)	2 (40.0%)	3 (60.0%)	0 (0.0%)	0 (0.0%)	5 (100%)
	종합병원	2 (16.7%)	4 (33.3%)	5 (41.7%)	1 (8.3%)	0 (0.0%)	12 (100%)
지역별	도시(동)	1 (6.2%)	6 (37.5%)	8 (50.0%)	1 (6.2%)	0 (0.0%)	16 (100%)
	비도시(읍·면)	1 (100%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	1 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

〈표 5-105〉는 보안사고(침해사고) 발생 시 평균 대응 시간에 대해 조사한 결과를 나타낸 것이다.

보안사고(침해사고)가 발생했을 때 의료기관이 실제 대응을 시작하기까지 소요된 시간을 살펴보면, 전체 17건의 보안사고 사례 중 '1~4시간 미만'이 6건(35.3%)으로 가장 높은 비중을 차지하였다. 이어 '4~12시간 미만'과 '12시간 이상'이 각각 4건(23.5%), '1시간 미만'이 3건(17.6%)으로 나타났다. 전체적으로 약 76%의 사례에서 사고 발생 후 12시간 이내에 대응이 이루어진 것으로 나타났다. 다만 일부 기관에서는 대응에 12시간 이상이 소요된 사례(48시간, 120시간)가 확인되었으며, 대응 시간

을 명확히 제시하지 못한 사례도 존재하였다.

의료기관 종별로 살펴보면 상급종합병원은 총 5건의 사고 중 '1~4시간 미만' 2건(40.0%), '4~12시간 미만' 2건(40.0%), '12시간 이상' 1건(20.0%)으로 나타났다. 반면 종합병원은 총 12건의 사고 중 '1시간 미만' 3건(25.0%), '1~4시간 미만' 4건(33.3%), '4~12시간 미만' 2건(16.7%), '12시간 이상' 3건(25.0%)으로 나타나 대응 시간이 비교적 넓은 범위로 분포하는 것으로 확인되었다.

〈표 5-105〉 보안사고(침해사고) 발생 시 평균 대응 시간

(단위: 개소, %)

구분		1시간 미만	1~4시간 미만	4시간~12시간 미만	12시간 이상	기타	합계
전체	전체	3 (17.6%)	6 (35.3%)	4 (23.5%)	4 (23.5%)	0 (0.0%)	17 (100%)
종별	상급종합병원	0 (0.0%)	2 (40.0%)	2 (40.0%)	1 (20.0%)	0 (0.0%)	5 (100%)
	종합병원	3 (25.0%)	4 (33.3%)	2 (16.7%)	3 (25.0%)	0 (0.0%)	12 (100%)
지역별	도시(동)	2 (12.5%)	6 (37.5%)	4 (25.0%)	4 (25.0%)	0 (0.0%)	16 (100%)
	비도시(읍·면)	1 (100%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	1 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

종합하면 대부분의 의료기관이 보안사고 발생 이후 12시간 이내에 초기 대응을 수행하는 것으로 나타났으나, 병원 규모, 보안 인력 구성, 보안 관제 체계 운영 여부 등에 따라 대응 시간의 편차가 존재하는 것으로 확인되었다. 이에 따라 의료기관 간 보안사고 대응 역량의 편차를 완화하고 신속한 대응 체계를 확보하기 위해 표준화된 침해사고 대응 프로토콜 마련과 보안관제 체계 강화 등 제도적 개선이 필요한 것으로 나타났다.

〈표 5-106〉은 보안사고(침해사고) 발생 시 복구 비용에 대해 조사한 결과를 나타낸 것이다.

의료기관에서 발생한 보안사고의 복구 비용을 금액 단위(원)로 분석한

결과, 전체 17건의 사례에서 평균 복구 비용은 약 7,361만 원으로 나타났다. 이는 보안사고가 단순한 시스템 장애 수준을 넘어 의료기관에 상당한 경제적 부담을 초래할 수 있음을 보여준다. 사례별로 살펴보면 복구 비용이 발생하지 않았다고 응답한 기관이 11개소(64.7%)로 가장 많았으나, 일부 기관에서는 최대 4억 원의 복구 비용이 보고되어 피해 규모의 편차가 큰 것으로 확인되었다.

의료기관 종별로 살펴보면 상급종합병원에서는 총 5건의 사고 중 4건(80.0%)이 복구 비용이 발생하지 않은 것으로 나타났으며, 1건(20.0%)에서는 약 2억 5천만 원의 복구 비용이 보고되었다. 반면 종합병원에서는 총 12건의 사고 중 7건(58.3%)이 복구 비용이 발생하지 않았으며, 5건(41.7%)에서는 0원에서 최대 4억 원까지 다양한 수준의 복구 비용이 발생한 것으로 나타났다.

전체적으로 의료기관의 보안사고 복구 비용은 기관 규모에 따라 일정한 차이를 보였다. 상급종합병원의 경우 대부분 복구 비용이 발생하지 않은 것으로 응답되었으나, 비용이 발생한 사례에서는 비교적 높은 금액이 보고되었다. 반면 종합병원은 복구 비용이 발생한 사례의 비중이 상대적으로 높고 금액의 분포 범위도 넓어 기관 간 편차가 큰 것으로 나타났다. 이러한 결과는 보안사고 발생 시 피해 규모와 복구 비용이 사고 유형, 대응 속도, 내부 기술 인력의 확보 여부 등에 따라 크게 달라질 수 있음을 보여준다.

한편 일부 기관에서 보안사고 발생에도 불구하고 복구 비용이 0원으로 응답된 사례가 다수 확인되었다. 이는 내부 인력을 활용한 자체 복구로 별도의 비용 집행이 이루어지지 않았을 가능성도 있으나, 사고 피해 규모가 실제보다 축소 보고되었을 가능성도 함께 고려될 필요가 있다. 해외 연구에서도 의료기관은 평판 문제나 법적 책임 등을 이유로 보안사고 피

해 규모를 축소 보고하는 경향이 존재하는 것으로 보고되고 있다. 이에 따라 보안사고 발생 시 피해 규모와 복구 비용을 보다 객관적으로 산정할 수 있는 기준과 조사 체계 마련이 필요한 것으로 나타났다.

〈표 5-106〉 보안사고(침해사고) 발생 시 복구 비용

(단위: 원)

구분	금액	종별	지역
1	400,000,000	종합병원	도시
2	300,000,000	종합병원	도시
3	250,000,000	종합병원	도시
4	250,000,000	상급종합병원	도시
5	50,000,000	종합병원	도시
6	1,500,000	종합병원	도시
7	0	종합병원	도시
8	0	상급종합병원	도시
9	0	종합병원	도시
10	0	종합병원	도시
11	0	종합병원	비도시
12	0	종합병원	도시
13	0	상급종합병원	도시
14	0	상급종합병원	도시
15	0	종합병원	도시
16	0	상급종합병원	도시
17	0	종합병원	도시
평균	73,617,647		

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

〈표 5-107〉은 보안사고(침해사고) 발생 시 파악 및 대응 수준에 대해 조사한 결과를 나타낸 것이다.

의료기관이 보안사고 발생 이후 사고 인지, 원인 분석 및 사후 대응을 얼마나 체계적으로 수행했는지를 살펴보면, 전체 17건의 사고 중 '사고 원인 분석과 향후 대응 방안까지 정리할 수 있었다'고 응답한 기관이 13개

소(76.5%)로 가장 높은 비중을 차지하였다. 이어 '사고 발생 사실만 정리할 수 있었다'는 3개소(17.6%), '사고 원인 분석까지만 수행하였다'는 1개소(5.9%)로 나타났다. 전반적으로 대부분의 의료기관이 사고 발생 이후 단순 사실 확인에 그치지 않고 원인 분석과 재발 방지 방안 마련까지 수행한 것으로 나타났다.

〈표 5-107〉 보안사고(침해사고) 발생 시 파악 및 대응 수준

(단위: 개소, %)

구분		사고 발생 사실만 정리할 수 있었다.	사고 원인 분석까지 할 수 있었다.	사고 원인 분석과 향후 대응방안까지 정리할 수 있었다.	합계
전체	전체	3 (17.6%)	1 (5.9%)	13 (76.5%)	17 (100%)
종별	상급종합병원	1 (20.0%)	1 (20.0%)	3 (60.0%)	5 (100%)
	종합병원	2 (16.7%)	0 (0.0%)	10 (83.3%)	12 (100%)
지역별	도시(동)	3 (18.8%)	1 (6.2%)	12 (75.0%)	16 (100%)
	비도시(읍·면)	0 (0.0%)	0 (0.0%)	1 (100%)	1 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

의료기관 종별로 살펴보면 상급종합병원은 사고 대응 수준이 '사고 발생 사실 정리'부터 '원인 분석 및 대응방안 마련'까지 비교적 다양한 수준으로 분포하는 것으로 나타나 기관 간 대응 역량에 일정한 차이가 존재하는 것으로 확인되었다. 반면 종합병원은 대부분의 기관이 '사고 원인 분석과 대응방안까지 정리할 수 있었다'고 응답하여 전반적으로 높은 대응 수준을 보였으나, 일부 기관에서는 사고 사실 확인 단계에 머무르는 사례도 확인되었다.

종합하면 대부분의 의료기관이 보안사고 발생 이후 원인 분석과 대응방안 마련까지 수행하고 있는 것으로 나타났으나, 일부 기관에서는 사고 대응 수준이 사실 확인 단계에 머무르는 사례도 확인되었다. 이에 따라

의료기관 간 사고 대응 역량의 편차를 줄이고 체계적인 사고 대응이 이루어질 수 있도록 표준화된 침해사고 대응 절차와 사후 분석 체계의 강화가 필요한 것으로 나타났다.

〈표 5-108〉은 보안사고(침해사고) 발생 시 주요 원인에 대해 조사한 결과를 나타낸 것이다.

전체 41건의 사례 중 '외부 사이버공격'이 16건(39.0%)으로 가장 높은 비중을 차지하였다. 다음으로 '기술적 취약점'이 13건(31.7%), '관리적 취약점'이 10건(24.4%), '네트워크 설정 미흡'이 2건(4.9%) 순으로 나타났다. 이러한 결과는 의료기관의 보안사고가 랜섬웨어, 피싱 등 외부 공격에 의해 촉발되는 경우가 많지만, 내부 시스템의 기술적 취약성과 관리적 통제 미흡 또한 사고 발생의 주요 요인으로 작용하고 있음을 보여준다.

의료기관 종별로 살펴보면 상급종합병원에서는 '외부 사이버공격'이 5건(41.7%)으로 가장 높은 비중을 차지하였으며, '기술적 취약점' 4건(33.3%), '관리적 취약점' 3건(25.0%) 순으로 나타났다. 종합병원에서는 '외부 사이버공격' 11건(37.9%), '기술적 취약점' 9건(31.0%), '관리적 취약점' 7건(24.1%), '네트워크 설정 미흡' 2건(6.9%)으로 나타나 다양한 요인이 복합적으로 작용하는 경향을 보였다.

종합하면 의료기관의 보안사고는 외부 사이버공격에 의해 발생하는 비중이 가장 높지만, 기술적 취약점과 관리적 미비 또한 유사한 수준으로 사고 발생에 영향을 미치는 것으로 나타났다. 이는 의료기관의 보안사고가 단일 원인보다는 외부 공격과 내부 관리·기술 체계의 취약성이 결합된 결과로 나타나는 특성을 보여준다. 이에 따라 외부 공격 대응을 위한 보안 인프라 강화와 함께 내부 시스템의 기술적 취약점 관리 및 보안 관리 체계 개선 등 종합적인 보안관리 체계 강화가 필요한 것으로 나타났다.

〈표 5-108〉 보안사고(침해사고) 발생 시 주요 원인(복수 선택)

(단위: 개소, %)

구분		기술적 취약점[1]	관리적 취약점[2]	외부 사이버 공격[3]	네트워크 설정 미흡	기타	합계
전체	전체	13 (31.7%)	10 (24.4%)	16 (39.0%)	2 (4.9%)	0 (0.0%)	41 (100%)
종별	상급종합병원	4 (33.3%)	3 (25.0%)	5 (41.7%)	0 (0.0%)	0 (0.0%)	12 (100%)
	종합병원	9 (31.0%)	7 (24.1%)	11 (37.9%)	2 (6.9%)	0 (0.0%)	29 (100%)
지역별	도시(동)	12 (31.6%)	9 (23.7%)	15 (39.5%)	2 (5.3%)	0 (0.0%)	38 (100%)
	비도시(읍·면)	1 (33.3%)	1 (33.3%)	1 (33.3%)	0 (0.0%)	0 (0.0%)	3 (100%)

주: 1. 기술적 취약점은 패치 미적용, 시스템 노후 등을 의미함.
2. 관리적 취약점은 체계, 행위 및 인식 제고 등을 의미함.
3. 외부 사이버 공격은 랜섬웨어, 피싱 등을 의미함.
출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

〈표 5-109〉는 보안사고(침해사고) 발생 시 주요 원인 개수에 대해 조사한 결과를 나타낸 것이다.

의료기관에서 발생한 보안사고(침해사고)가 단일 요인에 의해 발생했는지, 또는 복수의 요인이 복합적으로 작용했는지를 나타낸 것이다. 전체 17건의 사례 중 '2개 요인'과 '3개 요인'이 각각 6건(35.3%)으로 가장 높은 비중을 차지하였으며, '1개 요인'은 3건(17.6%), '4개 요인'은 2건(11.8%)으로 나타났다. 전체 사례의 70% 이상이 두 개 이상의 원인이 결합된 형태로 보고되어, 의료기관의 보안사고는 단일 요인보다는 외부 공격, 기술적 취약성, 관리적 미비 등 다양한 요인이 복합적으로 작용하여 발생하는 경우가 많은 것으로 나타났다.

이러한 결과는 앞서 분석한 보안사고 발생 원인 및 사고 대응 수준의 결과와도 일정 부분 일관되는 경향을 보인다. 즉 의료기관의 보안사고는 특정 단일 원인으로 설명되기보다는 외부 공격 요인과 내부 기술·관리 체계의 취약성이 상호 결합하여 발생하는 구조적 특성을 보이는 것으로 확인되었다.

종합하면 의료기관의 보안사고는 다양한 요인이 복합적으로 작용하는 경향을 보이고 있어, 사고 예방 정책 또한 단일 영역 중심의 대응만으로는 한계가 있을 수 있다. 이에 따라 기술적 보안 강화뿐만 아니라 관리적 통제, 인적 보안 관리 등을 포함한 통합적인 정보보호 관리체계 구축이 필요한 것으로 나타났다.

〈표 5-109〉 보안사고(침해사고) 발생 시 주요 원인 개수

구분	1개	2개	3개	4개	합계
기관 수	3개소 (17.6%)	6개소 (35.3%)	6개소 (35.3%)	2개소 (11.8%)	17개소 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

〈표 5-110〉은 보안사고(침해사고) 대응 시 가장 큰 어려움에 대해 조사한 결과를 나타낸 것이다.

전체 응답기관(263개소)을 대상으로 의료기관이 보안사고(침해사고) 발생 시 대응 과정에서 경험한 주요 어려움을 살펴보면, '보안 전문인력 부족'이 57.0%(150개소)로 가장 높은 비중을 차지하였다. 다음으로 '운영 비용 부담' 21.3%(56개소), '시스템의 기술적 한계' 14.8%(39개소), '매뉴얼 등 사고 대응 프로세스 부재' 2.7%(7개소) 순으로 나타났다. 반면 '사고 대응 조직 부재'는 1.5%(4개소), '경찰 또는 복지부의 무관심 혹은 괴롭힘'은 0.8%(2개소)로 상대적으로 낮은 비중을 보였다. '기타' 응답은 1.9%(5개소)로 확인되었으며, 주요 내용으로는 '직원 부주의', '보안 전담 인력 부재', '보안사고 미발생' 등이 제시되었다.

의료기관 종별로 살펴보면 상급종합병원(41개소)은 '보안 전문인력 부족'이 73.2%(30개소)로 가장 높은 비중을 차지하였으며, 이어 '운영 비용 부담' 14.6%(6개소), '시스템의 기술적 한계' 9.8%(4개소) 순으로 나타났다. 반면 '매뉴얼 등 사고 대응 프로세스 부재', '사고 대응 조직 부재',

‘경찰 또는 복지부의 무관심 혹은 괴롭힘’ 항목에 응답한 기관은 없는 것으로 나타났다.

종합병원(222개소)은 ‘보안 전문인력 부족’이 54.1%(120개소)로 가장 높은 비중을 차지하였으며, ‘운영 비용 부담’ 22.5%(50개소), ‘시스템의 기술적 한계’ 15.8%(35개소) 순으로 나타났다. 또한 ‘매뉴얼 등 사고 대응 프로세스 부재’ 3.2%(7개소), ‘경찰 또는 복지부의 무관심 혹은 괴롭힘’ 0.9%(2개소) 등 일부 응답도 확인되었다.

종합하면 의료기관의 보안사고 대응 과정에서 가장 큰 어려움은 보안 전문인력 부족으로 나타났으며, 그 다음으로 운영 비용 부담과 기술적 인프라 한계가 주요 요인으로 확인되었다. 특히 상급종합병원은 인력 부족 문제를 상대적으로 크게 인식하고 있는 반면, 종합병원은 인력뿐 아니라 운영 비용과 기술적 환경 등 다양한 요인에서 어려움을 경험하는 것으로 나타났다. 이에 따라 의료기관의 보안사고 대응 역량 강화를 위해 보안 전문인력 확보와 안정적인 예산 지원, 기술적 인프라 개선 등을 포함한 종합적인 정책 지원이 필요한 것으로 나타났다.

전체적으로 볼 때, 의료기관은 보안 사고 발생 시 전문 인력의 부재로 어려움에 직면하는 경우가 많았다. 또한 일부 기관은 기술적 대응 역량이 충분하지 않았고, 재정적 부담 역시 대응체계 구축의 주요 제약 요인으로 나타났다. 이러한 결과는 제도적 한계보다는 인력과 예산의 부족이 의료기관의 보안사고 대응 역량을 저해하는 핵심 요인으로 작용하고 있음을 보여준다.

〈표 5-110〉 보안사고(침해사고) 대응 시 가장 큰 어려움

(단위: 개소, %)

구분	보안 전문인력 부족	시스템의 기술적 한계	운영 비용 부담	매뉴얼 등 사고 대응 프로세스 부재
전체	150 (57.0%)	39 (14.8%)	56 (21.3%)	7 (2.7%)
상급종합병원	30 (73.2%)	4 (9.8%)	6 (14.6%)	0 (0.0%)
종합병원	120 (54.1%)	35 (15.8%)	50 (22.5%)	7 (3.2%)
도시(동)	143 (57.7%)	37 (14.9%)	51 (20.6%)	7 (2.8%)
비도시(읍·면)	7 (46.7%)	2 (13.3%)	5 (33.3%)	0 (0.0%)
구분	사고 대응 조직 부재	경찰 또는 복지부의 무관심 혹은 괴롭힘	기타	합계
전체	4 (1.5%)	2 (0.8%)	5 (1.9%)	263 (100%)
상급종합병원	0 (0.0%)	0 (0.0%)	1 (2.4%)	41 (100%)
종합병원	4 (1.8%)	2 (0.9%)	4 (1.8%)	222 (100%)
도시(동)	4 (1.6%)	1 (0.4%)	5 (2.0%)	248 (100%)
비도시(읍·면)	0 (0.0%)	1 (6.7%)	0 (0.0%)	15 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

다. 보안사고(침해사고) 신고

〈표 5-111〉은 보안사고(침해사고) 발생 시 신고를 주저하는 이유 개수에 대해 조사한 결과를 나타낸 것이다.

전체 응답기관(263개소)을 대상으로 보안사고(침해사고) 발생 시 신고를 주저하는 이유를 조사한 결과, 2개 이상 복수의 이유를 제시한 기관이 68.8%(181개소)로 나타났다. 세부적으로는 2개 이유를 제시한 기관이 55.1%(145개소)로 가장 많았으며, 3개 이유 12.9%(34개소), 4개 이유 0.8%(2개소)로 나타났다. 이는 다수의 의료기관이 보안사고 신고를 주저하는 원인을 단일 요인이 아니라 여러 요인이 복합적으로 작용하는 문제로 인식하고 있음을 보여준다.

〈표 5-111〉 보안사고(침해사고) 발생 시 신고를 주저하는 이유 개수

구분	1개	2개	3개	4개	합계
기관 수	82개소 (31.2%)	145개소 (55.1%)	34개소 (12.9%)	2개소 (0.8%)	263개소 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

〈표 5-112〉는 보안사고(침해사고) 발생 시 신고를 주저하는 이유에 대해 복수응답 방식으로 조사한 결과를 나타낸 것이다.

전체 응답(482건)을 기준으로 보안사고 발생 시 관계 기관에 신고하지 않거나 신고를 주저한 주요 이유를 살펴보면, '신고에 따른 법적 부담 우려'가 43.4%(209건)로 가장 높은 비중을 차지하였다. 다음으로 '의료기관 이미지(평판) 손상 우려' 40.2%(194건), '신고절차의 복잡성' 10.2%(49건), '내부 자체 처리 가능' 5.2%(25건) 순으로 나타났다. '기타' 응답은 1.0%(5건)으로, 신고 범위 판단 지연, 담당자 및 부서 문책 등 인사상 불이익 우려, 신고 예정 등의 이유가 포함되었다.

의료기관 종별로 살펴보면 상급종합병원 응답(76건)은 '신고에 따른 법적 부담 우려'와 '의료기관 이미지(평판) 손상 우려'가 각각 40.8%(31건)으로 가장 높은 비중을 차지하였다. 이어 '내부 자체 처리 가능' 7.9%(6건), '신고절차의 복잡성' 5.3%(4건) 순으로 나타났다. 종합병원 응답(406건)은 '신고에 따른 법적 부담 우려' 43.8%(178건), '의료기관 이미지(평판) 손상 우려' 40.1%(163건), '신고절차의 복잡성' 11.1%(45건), '내부 자체 처리 가능' 4.7%(19건) 순으로 나타나 상급종합병원과 유사한 경향을 보였다.

종합하면 의료기관은 법적 책임 부담과 기관 이미지 훼손에 대한 우려로 인해 보안사고 신고에 대해 신중한 태도를 보이는 경향이 확인되었다. 이는 보안사고 신고 지연 또는 누락이 제도적 요인뿐 아니라 조직 내부의 문화적·심리적 요인과도 관련될 수 있음을 보여준다. 이에 따라 보안사고

신고 활성화를 위해 법적 책임 부담을 다소 완화하고 신고 과정의 제도적 안정성을 확보하는 방향의 제도 개선이 필요한 것으로 나타났다.

〈표 5-112〉 보안사고(침해사고) 발생 시 신고를 주저하는 이유(복수 선택)

(단위: 개소, %)

구분	신고절차가 복잡하기 때문에	신고에 따른 법적 부담이 우려되기 때문에	의료기관 이미지(평판) 손상이 우려되기 때문에
전체	49 (10.2%)	209 (43.4%)	194 (40.2%)
상급종합병원	4 (5.3%)	31 (40.8%)	31 (40.8%)
종합병원	45 (11.1%)	178 (43.8%)	163 (40.1%)
도시(동)	47 (10.3%)	196 (43.1%)	183 (40.2%)
비도시(읍·면)	2 (7.4%)	13 (43.1%)	11 (40.7%)
구분	내부에서 자체적으로 처리 가능하기 때문에	기타	합계
전체	25 (5.2%)	5 (1.0%)	482 (100%)
상급종합병원	6 (7.9%)	4 (5.3%)	76 (100%)
종합병원	19 (4.7%)	1 (0.2%)	406 (100%)
도시(동)	24 (5.3%)	5 (1.1%)	455 (100%)
비도시(읍·면)	1 (3.7%)	0 (0.0%)	27 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

〈표 5-113〉는 보안사고(침해사고) 신고율 향상을 위한 필요한 지원항목 개수를 조사한 결과를 나타낸 것이다.

보안사고(침해사고) 신고율 향상을 위해 필요하다고 응답한 지원 항목이 2개 이상인 의료기관이 81.4%(214개소)로 대다수를 차지하였다. 세부적으로는 2개 항목을 선택한 기관이 43.3%(114개소)로 가장 많았고, 3개 18.3%(48개소), 4개 19.8%(52개소) 순으로 나타났다. 반면 1개 항목만 선택한 기관은 18.6%(49개소)에 불과하였다. 즉, 응답기관의 대다수는 단일 항목보다 2개 이상 복수의 지원방안을 동시에 필요로 하는 것

으로 확인되었다.

이러한 결과는 의료기관들이 단순히 특정 제도 개선보다는 다차원적 지원체계의 동시적 구축을 요구하고 있음을 보여준다. 특히 4개 항목 모두를 선택한 기관 비율이 19.8%(52개소)에 달한다는 점은, 현행 보안사고 신고제도의 제도적·운영상 한계가 다방면에서 존재함을 시사한다.

〈표 5-113〉 보안사고(침해사고) 신고율 향상을 위한 필요한 지원 개수

구분	1개	2개	3개	4개	합계
기관 수	49개소 (18.6%)	114개소 (43.3%)	48개소 (18.3%)	52개소 (19.8%)	263개소 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

〈표 5-114〉는 보안사고(침해사고) 신고율 향상을 위한 필요한 지원을 복수 응답 방식으로 조사한 결과를 나타낸 것이다.

전체 응답(484건) 중 보안사고(침해사고) 신고율을 높이기 위해 필요한 지원 방안으로 가장 많이 선택된 항목은 '법적 보호 제공'으로, 51.0%(247건)이었으며, 이는 보안사고 신고 시 기관이나 담당자에게 불이익이 발생하지 않도록 하는 법적 보호장치가 절실히 필요함을 반영한다. 그 다음으로 '신고 절차 간소화' 27.3%(132건), '정보보안 교육 및 홍보 강화' 21.7%(105건) 순으로 나타났다. 반면 '신고 인센티브 제공'을 선택한 응답은 없었으며(0건), 이는 현행 제도하에서 금전적 보상보다 절차적·법적 안정성이 우선순위로 인식되고 있음을 시사한다.

의료기관 종별로 살펴보면, 상급종합병원 응답(73건)은 '법적 보호 제공' 56.2%(41건), '신고 절차 간소화' 27.4%(20건), '정보보안 교육 및 홍보 강화' 16.4%(12건) 순으로 응답하였다. 종합병원 응답(411건)은 '법적 보호 제공' 50.1%(206건), '신고 절차 간소화' 27.3%(112건), '정보보안

교육 및 홍보 강화' 22.6%(93건) 으로, 상급종합병원과 유사한 경향을 보였다. 즉, 의료기관 규모와 관계없이 신고율 향상을 위해서는 무엇보다 법적 보호 제도 강화가 핵심적 과제로 인식되고 있음을 알 수 있다.

〈표 5-114〉 보안사고(침해사고) 신고율 향상을 위한 필요한 지원(복수 선택)

(단위: 개소, %)

구분	신고 절차 간소화	법적 보호 제공	신고 인센티브 제공
전체	132 (27.3%)	247 (51.0%)	0 (0.0%)
상급종합병원	20 (27.4%)	41 (56.2%)	0 (0.0%)
종합병원	112 (27.3%)	206 (50.1%)	0 (0.0%)
도시(동)	125 (27.4%)	233 (51.1%)	0 (0.0%)
비도시(읍·면)	7 (25.0%)	14 (50.0%)	0 (0.0%)
구분	정보보안 교육 및 홍보 강화	기타	합계
전체	105 (21.7%)	0 (0.0%)	484 (100%)
상급종합병원	12 (16.4%)	0 (0.0%)	73 (100%)
종합병원	93 (22.6%)	0 (0.0%)	411 (100%)
도시(동)	98 (21.5%)	0 (0.0%)	456 (100%)
비도시(읍·면)	7 (25.0%)	0 (0.0%)	28 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

이상의 결과를 종합하면 의료기관은 보안사고 신고 활성화를 위해 법적 보호 강화와 신고 절차의 단순화를 가장 중요한 과제로 인식하고 있으며, 금전적 인센티브 보다는 법적·절차적 안정성 확보와 교육·홍보 강화와 같은 실질적 지원을 요구하고 있다. 따라서 향후 정책 설계 시에는 의료기관의 규모와 특성에 따른 법적 보호 중심의 다층적 지원체계 구축이 필요하다.

라. 주요 정보시스템에 정보보안 사항 적용 여부

1) 인증

〈표 5-115〉는 의료기관이 주요 정보시스템에 적용하고 있는 인증 체계를 조사한 결과를 나타낸 것이다. 전체 응답기관(263개소) 중 '아이디/비밀번호(ID/PW)' 방식을 사용하고 있다고 응답한 기관은 99.6%(262개소)로 나타나, 대부분의 의료기관이 기본적인 인증 체계를 활용하고 있는 것으로 확인되었다. 또한 '공인인증서' 방식은 93.2%(245개소)가 도입하고 있는 것으로 나타났다.

반면 '다중요소 인증'은 20.5%(54개소), '본인확인 인증'은 21.3%(56개소), 'FIDO 인증'은 7.2%(19개소)로 나타나, 고도화된 인증 방식의 도입은 상대적으로 제한적인 수준에 머물러 있었다.

의료기관 종별로 살펴보면 상급종합병원(41개소)은 'ID/PW' 100%(41개소), '공인인증서' 87.8%(36개소), '다중요소 인증' 43.9% (18개소), '본인확인 인증' 53.7%(22개소), 'FIDO 인증' 12.2%(5개소)로 나타나 다양한 인증 방식을 비교적 폭넓게 적용하고 있는 것으로 나타났다.

반면 종합병원(222개소)은 'ID/PW' 99.5%(221개소), '공인인증서' 94.1%(209개소)로 기본 인증 체계는 높은 수준을 보였으나, '다중요소 인증' 16.2%(36개소), '본인확인 인증' 15.3%(34개소), 'FIDO 인증' 6.3%(14개소)로 고도 인증 방식의 도입률은 상급종합병원에 비해 낮은 수준으로 나타났다.

〈표 5-115〉 주요 정보시스템에 정보보안 사항 적용 여부(인증)

(단위: 개소, %)

구분	아이디/비밀번호			공인인증서		
	예	아니오	합계	예	아니오	합계
전체	262 (99.6%)	1 (0.4%)	263 (100%)	245 (93.2%)	18 (6.8%)	263 (100%)
상급 종합병원	41 (100%)	0 (0.0%)	41 (100%)	36 (87.8%)	5 (12.2%)	41 (100%)
종합병원	221 (99.5%)	1 (0.5%)	222 (100%)	209 (94.1%)	13 (5.9%)	222 (100%)
도시(동)	247 (99.6%)	1 (0.4%)	248 (100%)	230 (92.7%)	18 (7.3%)	248 (100%)
비도시 (읍·면)	15 (100%)	0 (0.0%)	15 (100%)	15 (100%)	0 (0.0%)	15 (100%)
구분	다중요소인증 (OTP, 2채널, 토큰, 보안카드, IC카드)			본인확인인증(SMS, I-PIN, 신용카드)		
	예	아니오	합계	예	아니오	합계
전체	54 (20.5%)	209 (79.5%)	263 (100%)	56 (21.3%)	207 (78.7%)	263 (100%)
상급 종합병원	18 (43.9%)	23 (56.1%)	41 (100%)	22 (53.7%)	19 (46.3%)	41 (100%)
종합병원	36 (16.2%)	186 (83.8%)	222 (100%)	34 (15.3%)	188 (84.7%)	222 (100%)
도시(동)	54 (21.8%)	194 (78.2%)	248 (100%)	56 (22.6%)	192 (77.4%)	248 (100%)
비도시 (읍·면)	0 (0.0%)	15 (100%)	15 (100%)	0 (0.0%)	15 (100%)	15 (100%)
	FIDO 인증(지문·안면 등 생체기반)			여백		
	예	아니오	합계			
전체	19 (7.2%)	244 (92.8%)	263 (100%)			
상급 종합병원	5 (12.2%)	36 (87.8%)	41 (100%)			
종합병원	14 (6.3%)	208 (93.7%)	222 (100%)			
도시(동)	19 (7.7%)	229 (92.3%)	248 (100%)			
비도시 (읍·면)	0 (0.0%)	15 (100%)	15 (100%)			

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

종합하면 의료기관의 정보시스템 인증 체계는 여전히 ID/PW 및 공인 인증서 기반의 전통적 인증 방식에 중심을 두고 있으며, 다중요소 인증이나 생체인식 기반 인증 등 고도화된 인증 체계의 도입은 일부 기관에 제한적으로 이루어지고 있는 것으로 나타났다. 또한 상급종합병원과 종합병원 간 인증 수준의 격차가 나타났다. 이에 따라 의료기관 전반의 계정 보안 강화를 위해 다중요소 인증 및 생체인증 등 고도 인증 체계 도입 확대와 함께, 기관 규모에 따른 기술·재정 지원을 통한 인증 수준 격차 해소가 필요한 것으로 나타났다.

2) PC 및 단말기 보안

〈표 5-116〉은 의료기관이 주요 정보시스템에서 PC 및 단말기 보안을 위해 적용하고 있는 정보보안 사항을 조사한 결과를 나타낸 것이다.

전체 응답기관(263개소) 중 'PC 방화벽'을 적용하고 있다고 응답한 기관은 91.6%(241개소)로 높은 수준을 보였으며, '백신 프로그램'은 99.2%(261개소)가 도입하고 있어 대부분의 기관에서 운영되고 있는 것으로 나타났다.

반면 'PC 키보드 보안'은 19.4%(51개소), '정보 유출 방지 솔루션'은 55.9%(147개소)로 항목 간 도입 수준의 편차가 나타났다. '패치 관리 시스템'은 26.2%(69개소), '보조기억장치 제어 솔루션'은 71.5%(188개소), '프린터 출력물 보안'은 56.3%(148개소), '개인정보 검색 솔루션'은 55.5%(146개소), '문서 암호화'는 46.4%(122개소)로 나타났다. 이는 대부분의 의료기관이 백신 및 방화벽 등 기본적인 보안 체계는 구축하고 있으나, 내부 정보 유출 방지나 문서 암호화 등 고도화된 보안 통제 기술의 도입은 상대적으로 제한적인 수준에 머물러 있음을 보여준다.

의료기관 종별로 살펴보면 상급종합병원은 전반적으로 종합병원보다 PC 및 단말기 보안 적용 수준이 높은 것으로 나타났다. 상급종합병원(41개소)에서는 '백신 프로그램' 100%(41개소), '정보 유출 방지 솔루션' 70.7%(29개소), '패치 관리 시스템' 87.8%(36개소), '보조기억장치 제어 솔루션' 87.8%(36개소), '프린터 출력물 보안' 73.2%(30개소), '개인정보 검색 솔루션' 78.0%(32개소), '문서 암호화' 70.7%(29개소)로 나타나 비교적 높은 도입 수준을 보였다.

〈표 5-116〉 주요 정보시스템에 정보보안 사항 적용 여부(PC/단말기 보안)

(단위: 개소, %)

구분	PC방화벽			백신		
	예	아니오	합계	예	아니오	합계
전체	241 (91.6%)	22 (8.4%)	263 (100%)	261 (99.2%)	2 (0.8%)	263 (100%)
상급 종합병원	32 (78.0%)	9 (22.0%)	41 (100%)	41 (100%)	0 (0.0%)	41 (100%)
종합병원	209 (94.1%)	13 (5.9%)	222 (100%)	220 (99.1%)	2 (0.9%)	222 (100%)
도시(동)	226 (91.1%)	22 (8.9%)	248 (100%)	246 (99.2%)	2 (0.8%)	248 (100%)
비도시 (읍·면)	15 (100%)	0 (0.0%)	15 (100%)	15 (100%)	0 (0.0%)	15 (100%)
구분	PC키보드보안(Anti-keylogger)			정보유출방지솔루션(DLP)		
	예	아니오	합계	예	아니오	합계
전체	51 (19.4%)	212 (80.6%)	263 (100%)	147 (55.9%)	116 (44.1%)	263 (100%)
상급 종합병원	4 (9.8%)	37 (90.2%)	41 (100%)	29 (70.7%)	12 (29.3%)	41 (100%)
종합병원	47 (21.2%)	175 (78.8%)	222 (100%)	118 (53.2%)	104 (46.8%)	222 (100%)
도시(동)	48 (19.4%)	200 (80.6%)	248 (100%)	135 (54.4%)	113 (45.6%)	248 (100%)
비도시 (읍·면)	3 (20.0%)	12 (80.0%)	15 (100%)	12 (80.0%)	3 (20.0%)	15 (100%)

구분	패치관리 시스템(PMS)			보조기억장치 제어솔루션		
	예	아니오	합계	예	아니오	합계
전체	69 (26.2%)	194 (73.8%)	263 (100%)	188 (71.5%)	75 (28.5%)	263 (100%)
상급 종합병원	36 (87.8%)	5 (12.2%)	41 (100%)	36 (87.8%)	5 (12.2%)	41 (100%)
종합병원	33 (14.9%)	189 (85.1%)	222 (100%)	152 (68.5%)	70 (31.5%)	222 (100%)
도시(동)	66 (26.6%)	182 (73.4%)	248 (100%)	176 (71.0%)	72 (29.0%)	248 (100%)
비도시 (읍·면)	3 (20.0%)	12 (80.0%)	15 (100%)	12 (80.0%)	3 (20.0%)	15 (100%)
구분	프린터 출력물 보안			개인정보 검색솔루션		
	예	아니오	합계	예	아니오	합계
전체	148 (56.3%)	115 (43.7%)	263 (100%)	146 (55.5%)	117 (44.5%)	263 (100%)
상급 종합병원	30 (73.2%)	11 (26.8%)	41 (100%)	32 (78.0%)	9 (22.0%)	41 (100%)
종합병원	118 (53.2%)	104 (46.8%)	222 (100%)	114 (51.4%)	108 (48.6%)	222 (100%)
도시(동)	139 (56%)	109 (44%)	248 (100%)	137 (55.2%)	111 (44.8%)	248 (100%)
비도시 (읍·면)	9 (60.0%)	6 (40.0%)	15 (100%)	9 (60.0%)	6 (40.0%)	15 (100%)
구분	문서암호화(DRM)			여백		
	예	아니오	합계			
전체	122 (46.4%)	141 (53.6%)	263 (100%)			
상급 종합병원	29 (70.7%)	12 (29.3%)	41 (100%)			
종합병원	93 (41.9%)	129 (58.1%)	222 (100%)			
도시(동)	113 (45.6%)	135 (54.4%)	248 (100%)			
비도시 (읍·면)	9 (60.0%)	6 (40.0%)	15 (100%)			

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

반면 'PC 방화벽'은 78.0%(32개소), 'PC 키보드 보안'은 9.8%(4개소)로 일부 기본 보안 항목의 도입률은 상대적으로 낮게 나타났다.

종합병원(222개소)은 'PC 방화벽' 94.1%(209개소), 'PC 키보드 보안' 21.2%(47개소)로 일부 기본 보안 항목에서 상급종합병원보다 높은 수준을 보였다. 그러나 '정보 유출 방지 솔루션' 53.2%(118개소), '패치 관리 시스템' 14.9%(33개소), '보조기억장치 제어 솔루션' 68.5%(152개소), '프린터 출력물 보안' 53.2%(118개소), '개인정보 검색 솔루션' 51.4%(114개소), '문서 암호화' 41.9%(93개소) 등 고도 보안 항목에서는 상대적으로 낮은 도입률을 보였다.

종합하면 의료기관의 PC 및 단말기 보안은 백신 및 방화벽 중심의 기본 보안 체계는 전반적으로 구축되어 있으나, 정보 유출 방지, 패치 관리, 문서 암호화 등 고도화된 보안 통제 체계는 기관별로 도입 수준의 편차가 나타났다. 또한 상급종합병원과 종합병원 간 보안 적용 수준의 차이도 확인되었다. 이에 따라 의료기관의 내부 정보 보호 강화를 위해 고도 보안 솔루션 도입 확대와 함께, 기관 규모에 따른 기술·재정 지원을 통한 보안 수준 격차 해소가 필요한 것으로 나타났다.

3) 네트워크 보안

〈표 5-117〉은 의료기관이 주요 정보시스템의 네트워크 보안을 위해 적용하고 있는 보안 사항을 항목별로 조사한 결과를 나타낸 것이다.

전체 응답기관(263개소) 중 '방화벽'은 전 의료기관(100%)에서 운영되고 있어, 기본적인 네트워크 접근 통제 체계는 모든 의료기관에 구축되어 있는 것으로 나타났다. '침입방지시스템'은 77.6%(204개소), '가상사설망'은 78.7%(207개소)로 비교적 높은 수준을 보였다.

〈표 5-117〉 주요 정보시스템에 정보보안 사항 적용 여부(네트워크 보안)

(단위: 개소, %)

구분	방화벽(FireWall)			침입방지시스템(IPS)		
	예	아니오	합계	예	아니오	합계
전체	263 (100%)	0 (0.0%)	263 (100%)	204 (77.6%)	59 (22.4%)	263 (100%)
상급 종합병원	41 (100%)	0 (0.0%)	41 (100%)	38 (92.7%)	3 (7.3%)	41 (100%)
종합병원	222 (100%)	0 (0.0%)	222 (100%)	166 (74.8%)	56 (25.2%)	222 (100%)
도시(동)	248 (100%)	0 (0.0%)	248 (100%)	192 (77.4%)	56 (22.6%)	248 (100%)
비도시 (읍·면)	15 (100%)	0 (0.0%)	15 (100%)	12 (80.0%)	3 (20.0%)	15 (100%)
구분	무선 침입방지시스템(W-IPS)			침입탐지시스템(IDS)		
	예	아니오	합계	예	아니오	합계
전체	64 (24.3%)	199 (75.7%)	263 (100%)	98 (37.3%)	165 (62.7%)	263 (100%)
상급 종합병원	23 (56.1%)	18 (43.9%)	41 (100%)	28 (68.3%)	13 (31.7%)	41 (100%)
종합병원	41 (18.5%)	181 (81.5%)	222 (100%)	70 (31.5%)	152 (68.5%)	222 (100%)
도시(동)	62 (25.0%)	186 (75%)	248 (100%)	93 (37.5%)	155 (62.5%)	248 (100%)
비도시 (읍·면)	2 (13.3%)	13 (86.7%)	15 (100%)	5 (33.3%)	10 (66.7%)	15 (100%)
구분	네트워크 접근통제(NAC)			통합위협관리(UTM)		
	예	아니오	합계	예	아니오	합계
전체	134 (51.0%)	129 (49.0%)	263 (100%)	92 (35.0%)	171 (65.0%)	263 (100%)
상급 종합병원	41 (100%)	0 (0.0%)	41 (100%)	22 (53.7%)	19 (46.3%)	41 (100%)
종합병원	93 (41.9%)	129 (58.1%)	222 (100%)	70 (31.5%)	152 (68.5%)	222 (100%)
도시(동)	128 (51.6%)	120 (48.4%)	248 (100%)	85 (34.3%)	163 (65.7%)	248 (100%)
비도시 (읍·면)	6 (40.0%)	9 (60.0%)	15 (100%)	7 (46.7%)	8 (53.3%)	15 (100%)

구분	전송구간 암호화(DMZ, 외부망 포함)			가상사설망(VPN)		
	예	아니오	합계	예	아니오	합계
전체	154 (58.6%)	109 (41.4%)	263 (100%)	207 (78.7%)	56 (21.3%)	263 (100%)
상급 종합병원	35 (85.4%)	6 (14.6%)	41 (100%)	39 (95.1%)	2 (4.9%)	41 (100%)
종합병원	119 (53.6%)	103 (46.4%)	222 (100%)	168 (75.7%)	54 (24.3%)	222 (100%)
도시(동)	145 (58.5%)	103 (41.5%)	248 (100%)	195 (78.6%)	53 (21.4%)	248 (100%)
비도시 (읍·면)	9 (60.0%)	6 (40.0%)	15 (100%)	12 (80.0%)	3 (20.0%)	15 (100%)
구분	DDoS 방지시스템			망분리(물리적, 논리적)		
	예	아니오	합계	예	아니오	합계
전체	82 (31.2%)	181 (68.8%)	263 (100%)	80 (30.4%)	183 (69.6%)	263 (100%)
상급 종합병원	23 (56.1%)	18 (43.9%)	41 (100%)	29 (70.7%)	12 (29.3%)	41 (100%)
종합병원	59 (26.6%)	163 (73.4%)	222 (100%)	51 (23.0%)	171 (77.0%)	222 (100%)
도시(동)	76 (30.6%)	172 (69.4%)	248 (100%)	77 (31.0%)	171 (69.0%)	248 (100%)
비도시 (읍·면)	6 (40.0%)	9 (60.0%)	15 (100%)	3 (20.0%)	12 (80.0%)	15 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

반면 '네트워크 접근통제시스템'은 51.0%(134개소), '전송 구간 암호화'는 58.6%(154개소)로 절반 수준의 도입률을 보였다. 또한 '무선 침입 방지 시스템' 24.3%(64개소), '통합위협관리' 35.0%(92개소), 'DDoS 방지시스템' 31.2%(82개소), '망분리(물리적·논리적)' 30.4%(80개소) 등은 상대적으로 낮은 수준에 머물러 있어 네트워크 보안 인프라의 고도화 수준에는 차이가 나타났다.

의료기관 종별로 살펴보면 상급종합병원은 종합병원에 비해 전반적으로 네트워크 보안 솔루션 도입률이 높은 것으로 나타났다. 상급종합병원

(41개소)은 '방화벽' 100%(41개소), '침입방지시스템' 92.7% (38개소), '무선 침입 방지 시스템' 56.1%(23개소), '침입탐지시스템' 68.3%(28개소), '네트워크 접근통제시스템' 100%(41개소), '통합위협관리' 53.7% (22개소), '전송 구간 암호화' 85.4%(35개소), '가상사설망' 95.1%(39개소), 'DDoS 방지시스템' 56.1%(23개소), '망분리' 70.7%(29개소)로 나타났다.

반면 종합병원(222개소)은 '방화벽' 100%(222개소)로 동일하게 나타났으나, '침입방지시스템' 74.8%(166개소), '무선 침입 방지 시스템' 18.5%(41개소), '침입탐지시스템' 31.5%(70개소), '네트워크 접근통제시스템' 41.9%(93개소), '통합위협관리' 31.5%(70개소), '전송 구간 암호화' 53.6%(119개소), '가상사설망' 75.7%(168개소), 'DDoS 방지시스템' 26.6%(59개소), '망분리' 23.0%(51개소)로 상급종합병원에 비해 낮은 수준을 보였다.

종합하면 의료기관은 방화벽, 침입탐지시스템, 침입방지시스템 등 기본적인 네트워크 보안 장비는 대부분 구축하고 있으나, 통합위협관리, 네트워크 접근통제, 무선 보안, DDoS 대응 등 고도화된 네트워크 보안 체계의 도입은 상대적으로 제한적인 수준에 머물러 있는 것으로 나타났다. 또한 상급종합병원과 종합병원 간 보안 인프라 수준의 차이도 확인되었다. 이에 따라 의료기관의 네트워크 보안 수준 향상을 위해 고도 보안 솔루션 도입 확대와 함께, 기관 규모에 따른 기술·재정 지원을 통한 보안 인프라 격차 해소가 필요한 것으로 나타났다.

4) 데이터베이스(DB) 보안

〈표 5-118〉은 의료기관이 주요 정보시스템의 데이터베이스(DB) 보안을 위해 적용하고 있는 정보보안 사항을 조사한 결과를 나타낸 것이다.

〈표 5-118〉 주요 정보시스템에 정보보안 사항 적용 여부(DB보안)

(단위: 개소, %)

구분	DB 접근제어			DB 암호화		
	예	아니오	합계	예	아니오	합계
전체	243 (92.4%)	20 (7.6%)	263 (100%)	250 (95.1%)	13 (4.9%)	263 (100%)
상급 종합병원	41 (100%)	0 (0.0%)	41 (100%)	41 (100%)	0 (0.0%)	41 (100%)
종합병원	202 (91.0%)	20 (9.0%)	222 (100%)	209 (94.1%)	13 (5.9%)	222 (100%)
도시(동)	230 (92.7%)	18 (7.3%)	248 (100%)	236 (95.2%)	12 (4.8%)	248 (100%)
비도시 (읍·면)	13 (86.7%)	2 (13.3%)	15 (100%)	14 (93.3%)	1 (6.7%)	15 (100%)
구분	DB 사용자 비밀번호 암호화			환자 고유식별정보 암호화		
	예	아니오	합계	예	아니오	합계
전체	252 (95.8%)	11 (4.2%)	263 (100%)	254 (96.6%)	9 (3.4%)	263 (100%)
상급 종합병원	39 (95.1%)	2 (4.9%)	41 (100%)	39 (95.1%)	2 (4.9%)	41 (100%)
종합병원	213 (95.9%)	9 (4.1%)	222 (100%)	215 (96.8%)	7 (3.2%)	222 (100%)
도시(동)	237 (95.6%)	11 (4.4%)	248 (100%)	239 (96.4%)	9 (3.6%)	248 (100%)
비도시 (읍·면)	15 (100%)	0 (0.0%)	15 (100%)	15 (100%)	0 (0.0%)	15 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

전체 응답기관(263개소) 중 'DB 접근제어'를 실시하고 있는 의료기관은 92.4%(243개소)로 나타나, 대부분의 의료기관이 기본적인 접근 통제 체계를 구축하고 있는 것으로 나타났다. 또한 'DB 암호화' 95.1%(250개소), 'DB 사용자 비밀번호 암호화' 95.8%(252개소), '환자 고유식별정보 암호화' 96.6%(254개소)로 나타나 전반적으로 높은 도입 수준을 보였다. 이는 대부분의 의료기관이 데이터베이스 접근통제와 주요 정보 암호화

체계를 폭넓게 적용하고 있음을 보여준다.

의료기관 종별로 살펴보면 상급종합병원과 종합병원 모두 전반적으로 높은 수준의 DB 보안 체계를 갖추고 있는 것으로 나타났다. 상급종합병원(41개소)은 'DB 접근제어'와 'DB 암호화'가 각각 100%(41개소)로 나타났으며, 'DB 사용자 비밀번호 암호화'와 '환자 고유식별정보 암호화'도 각각 95.1%(39개소)로 대부분의 기관에서 적용하고 있었다.

종합병원(222개소) 역시 'DB 접근제어' 91.0%(202개소), 'DB 암호화' 94.1%(208개소), 'DB 사용자 비밀번호 암호화' 95.9%(213개소), '환자 고유식별정보 암호화' 96.8%(215개소)로 전반적으로 높은 수준을 유지하고 있는 것으로 나타났다.

종합하면 의료기관의 데이터베이스 보안은 접근통제와 암호화 중심의 기본 보안 체계가 전반적으로 구축되어 있으며, 사용자 비밀번호 및 환자 고유식별정보에 대한 암호화도 폭넓게 적용되고 있는 것으로 나타났다. 다만 일부 기관에서는 DB 접근제어 등 핵심 통제 항목이 미적용된 사례도 확인되어, 데이터베이스 보안 정책의 전면 적용과 지속적인 점검·관리 체계 강화가 필요한 것으로 나타났다.

5) 서버 보안

〈표 5-119〉는 의료기관이 주요 정보시스템의 서버 보안을 위해 적용하고 있는 기술적 보안 조치를 조사한 결과를 나타낸 것이다.

전체 응답기관(263개소) 중 '서버 백신'을 적용하고 있는 기관은 90.1%(237개소)로 나타나, 대부분의 의료기관이 기본적인 서버 단위의 악성코드 방어 체계를 구축하고 있는 것으로 나타났다. 또한 '서버 접근제어'를 적용하고 있는 기관은 62.7%(165개소)로 나타나, 약 3분의 2 수준에서

접근권한 관리 체계를 운영하고 있는 것으로 나타났다. 이는 의료기관 전반에서 서버 기반의 기초 보안 수준은 확보되어 있으나, 접근제어 등 고도화된 보안 통제는 일부 기관에 한정되어 적용되고 있음을 보여준다.

의료기관 종별로 살펴보면 상급종합병원(41개소)은 '서버 백신' 97.6%(40개소), '서버 접근제어' 92.7%(38개소)로 나타나 대부분의 기관에서 서버 보안 체계를 구축하고 있는 것으로 나타났다. 반면 종합병원(222개소)은 '서버 백신' 88.7%(197개소), '서버 접근제어' 57.2%(127개소)로 나타나 상급종합병원에 비해 접근통제 수준이 낮은 것으로 나타났다.

〈표 5-119〉 주요 정보시스템에 정보보안 사항 적용 여부(서버보안)

(단위: 개소, %)

구분	서버백신(Linux, Windows Server)			서버 접근제어(Secure OS, 접근권한, 계정 및 로그관리 등)		
	예	아니오	합계	예	아니오	합계
전체	237 (90.1%)	26 (9.9%)	263 (100%)	165 (62.7%)	98 (37.3%)	263 (100%)
상급 종합병원	40 (97.6%)	1 (2.4%)	41 (100%)	38 (92.7%)	3 (7.3%)	41 (100%)
종합병원	197 (88.7%)	25 (11.3%)	222 (100%)	127 (57.2%)	95 (42.8%)	222 (100%)
도시(동)	225 (90.7%)	23 (9.3%)	248 (100%)	158 (63.7%)	90 (36.3%)	248 (100%)
비도시 (읍·면)	12 (80.0%)	3 (20.0%)	15 (100%)	7 (46.7%)	8 (53.3%)	15 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

종합하면 의료기관의 서버 보안은 백신 중심의 기본적인 방어 체계는 전반적으로 구축되어 있으나, 접근권한 관리 등 논리적 보안 통제 수준은 기관별로 차이가 나타났다. 또한 상급종합병원과 종합병원 간 보안 적용 수준의 격차도 확인되었다. 따라서 서버 보안 강화를 위해 접근제

어, 로그 관리, 권한 통제 등 고도화된 보안 통제 체계의 확대와 함께, 기관 규모에 따른 보안 역량 격차 해소를 위한 지원이 필요한 것으로 나타났다.

6) 애플리케이션 보안

〈표 5-120〉은 의료기관이 주요 정보시스템의 애플리케이션 보안을 위해 적용하고 있는 정보보안 사항을 조사한 결과를 나타낸 것이다.

전체 응답기관(263개소) 중 '웹 방화벽'을 도입한 기관은 43.0%(113개소), '유해사이트 차단 시스템'을 적용한 기관은 46.0%(121개소)로 나타나 절반 수준에 미치지 못하는 것으로 나타났다. 또한 '소스코드 점검 툴' 14.4%(38개소), '웹 스캐너' 11.0%(29개소), '웹서버 악성코드 탐지' 17.9%(47개소)로 나타나, 사전 예방 중심의 고도화된 보안 기술은 제한적으로 적용되고 있는 것으로 나타났다.

〈표 5-120〉 주요 정보시스템에 정보보안 사항 적용 여부(어플리케이션 보안)

(단위: 개소, %)

구분	웹방화벽(WAF)			유해사이트 차단시스템		
	예	아니오	합계	예	아니오	합계
전체	113 (43.0%)	150 (57.0%)	263 (100%)	121 (46.0%)	142 (54%)	263 (100%)
상급 종합병원	41 (100%)	0 (0.0%)	41 (100%)	37 (90.2%)	4 (9.8%)	41 (100%)
종합병원	72 (32.4%)	150 (67.6%)	222 (100%)	84 (37.8%)	138 (62.2%)	222 (100%)
도시(동)	108 (43.5%)	140 (56.5%)	248 (100%)	114 (46.0%)	134 (54%)	248 (100%)
비도시 (읍·면)	5 (33.3%)	10 (66.7%)	15 (100%)	7 (46.7%)	8 (53.3%)	15 (100%)

구분	소스코드 점검 툴			웹 스캐너		
	예	아니오	합계	예	아니오	합계
전체	38 (14.4%)	225 (85.6%)	263 (100%)	29 (11.0%)	234 (89.0%)	263 (100%)
상급 종합병원	18 (43.9%)	23 (56.1%)	41 (100%)	8 (19.5%)	33 (80.5%)	41 (100%)
종합병원	20 (9.0%)	202 (91.0%)	222 (100%)	21 (9.5%)	201 (90.5%)	222 (100%)
도시(동)	38 (15.3%)	210 (84.7%)	248 (100%)	27 (10.9%)	221 (89.1%)	248 (100%)
비도시 (읍·면)	0 (0.0%)	15 (100%)	15 (100%)	2 (13.3%)	13 (86.7%)	15 (100%)
구분	웹서버 악성코드 탐지			여백		
	예	아니오	합계			
전체	47 (17.9%)	216 (82.1%)	263 (100%)			
상급 종합병원	17 (41.5%)	24 (58.5%)	41 (100%)			
종합병원	30 (13.5%)	192 (86.5%)	222 (100%)			
도시(동)	45 (18.1%)	203 (81.9%)	248 (100%)			
비도시 (읍·면)	2 (13.3%)	13 (86.7%)	15 (100%)			

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

이는 의료기관의 애플리케이션 보안 체계가 기본적인 보호 장비 중심으로 구성되어 있으며, 능동적 예방 중심의 보안 통제는 상대적으로 부족한 수준임을 보여준다.

의료기관 종별로 살펴보면 상급종합병원은 종합병원에 비해 전반적으로 높은 수준의 보안 조치를 적용하고 있는 것으로 나타났다. 상급종합병원(41개소)은 '웹 방화벽' 100%(41개소), '유해사이트 차단 시스템' 90.2%(37개소), '소스코드 점검 툴' 43.9%(18개소), '웹 스캐너' 19.5% (8개소), '웹서버 악성코드 탐지' 41.5%(17개소)로 나타나 비교적 다양한 보

안 도구를 적용하고 있는 것으로 나타났다.

반면 종합병원(222개소)은 '웹 방화벽' 32.4%(72개소), '유해사이트 차단 시스템' 37.8%(84개소), '소스코드 점검 툴' 9.0%(20개소), '웹 스캐너' 9.5%(21개소), '웹서버 악성코드 탐지' 13.5%(30개소)로 나타나 전반적으로 낮은 도입 수준을 보였다.

종합하면 의료기관의 애플리케이션 보안은 웹 방화벽 등 기본적인 보안 장비 중심으로 운영되고 있으며, 소스코드 점검, 웹 취약점 진단, 악성코드 탐지 등 사전 예방 중심의 보안 관리 체계는 상대적으로 미흡한 수준으로 나타났다. 또한 상급종합병원과 종합병원 간 보안 적용 수준의 격차도 확인되었다. 이에 따라 애플리케이션 보안 강화를 위해 취약점 점검 및 소스코드 검증 등 사전 예방 중심의 보안 체계 도입 확대와 함께, 기관 규모에 따른 기술적 지원을 통한 보안 수준 격차 해소가 필요한 것으로 나타났다.

7) 통합보안관리

〈표 5-121〉은 의료기관이 주요 정보시스템에서 통합 보안 관리 기능을 어느 수준으로 운영하고 있는지를 조사한 결과를 나타낸 것이다.

전체 응답기관(263개소) 중 '표준인증 프로토콜(OAuth, SAML, OIDC)'을 적용한 의료기관은 10.6%(28개소)로 나타나, 대부분의 의료기관이 여전히 개별 시스템 단위의 인증 체계를 운영하고 있는 것으로 나타났다. '통합계정권한관리(SSO)'는 15.2%(40개소), '전사적 보안관리(ESM)'는 12.2%(32개소), '위협관리시스템(TMS)'은 17.1%(45개소)로 나타나 전반적으로 도입 수준이 낮은 것으로 나타났다.

의료기관 종별로 살펴보면 상급종합병원은 종합병원에 비해 모든 항목

에서 높은 도입률을 보였다. 상급종합병원(41개소)은 '표준인증 프로토콜' 24.4%(10개소), '통합계정권한관리(SSO)' 39.0%(16개소), '전사적 보안관리(ESM)' 26.8%(11개소), '위협관리시스템(TMS)' 46.3%(19개소)로 나타났다.

〈표 5-121〉 주요 정보시스템에 정보보안 사항 적용 여부(통합 보안 관리)

(단위: 개소, %)

구분	표준인증 프로토콜 (OAuth, SAML, OIDC)			통합계정권한관리(SSO)		
	예	아니오	합계	예	아니오	합계
전체	28 (10.6%)	235 (89.4%)	263 (100%)	40 (15.2%)	223 (84.8%)	263 (100%)
상급 종합병원	10 (24.4%)	31 (75.6%)	41 (100%)	16 (39%)	25 (61.0%)	41 (100%)
종합병원	18 (8.1%)	204 (91.9%)	222 (100%)	24 (10.8%)	198 (89.2%)	222 (100%)
도시(동)	27 (10.9%)	221 (89.1%)	248 (100%)	40 (16.1%)	208 (83.9%)	248 (100%)
비도시 (읍·면)	1 (6.7%)	14 (93.3%)	15 (100%)	0 (0.0%)	15 (100%)	15 (100%)
구분	전사적보안관리(ESM)			위협관리시스템(TMS)		
	예	아니오	합계	예	아니오	합계
전체	32 (12.2%)	231 (87.8%)	263 (100%)	45 (17.1%)	218 (82.9%)	263 (100%)
상급 종합병원	11 (26.8%)	30 (73.2%)	41 (100%)	19 (46.3%)	22 (53.7%)	41 (100%)
종합병원	21 (9.5%)	201 (90.5%)	222 (100%)	26 (11.7%)	196 (88.3%)	222 (100%)
도시(동)	32 (12.9%)	216 (87.1%)	248 (100%)	45 (18.1%)	203 (81.9%)	248 (100%)
비도시 (읍·면)	0 (0.0%)	15 (100%)	15 (100%)	0 (0.0%)	15 (100%)	15 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

반면 종합병원(222개소)은 각각 8.1%(18개소), 10.8%(24개소), 9.5%(21개소), 11.7%(26개소)로 나타나 전반적으로 낮은 수준을 보였다. 이는 상급종합병원이 인증·접속관리·위협탐지 등 다양한 보안 기능을 통합적으로 운영하는 반면, 종합병원은 일부 기능 중심의 단편적인 관리에 머물러 있는 경향이 나타났음을 보여준다.

종합하면 의료기관의 통합 보안 관리 수준은 전반적으로 제한적인 수준에 머물러 있으며, 표준 인증 기반의 통합 계정관리와 위협 탐지·대응 체계의 도입은 아직 초기 단계에 있는 것으로 나타났다. 또한 상급종합병원과 종합병원 간 통합 보안 수준의 격차도 확인되었다. 이에 따라 통합 보안 관리 체계 강화를 위해 표준 인증 기반의 계정관리 통합, 보안 이벤트 통합관리 및 위협 대응 자동화 체계 구축과 함께, 기관 규모에 따른 기술적 지원을 통한 보안 수준 격차 해소가 필요한 것으로 나타났다.

8) 모바일 앱 보안

〈표 5-122〉는 의료기관이 주요 정보시스템의 모바일·앱 환경에서 적용하고 있는 정보보안 조치를 조사한 결과를 나타낸 것이다.

전체 응답기관(263개소) 중 '앱 위변조 방지' 기능을 운영하는 의료기관은 18.3%(48개소)로 나타나, 모바일 환경에서의 보안 대응 체계를 구축한 기관은 제한적인 수준에 머물러 있는 것으로 나타났다. '데이터 암호화'는 27.4%(72개소)로 약 4분의 1 수준에 그쳤으며, '보안 키패드' 8.7%(23개소), '인증서 중계' 9.5%(25개소), '모바일 SSO' 9.5%(25개소)로 나타나 전반적으로 낮은 도입 수준을 보였다. 이는 의료기관의 모바일 보안 체계가 아직 초기 단계에 머물러 있음을 보여준다.

의료기관 종별로 살펴보면 상급종합병원은 종합병원에 비해 전반적으로 높은 수준의 모바일 보안 체계를 운영하고 있는 것으로 나타났다.

〈표 5-122〉 주요 정보시스템에 정보보안 사항 적용 여부(모바일 앱 보안)

구분	앱 위변조 방지			데이터 암호화		
	예	아니오	합계	예	아니오	합계
전체	48 (18.3%)	215 (81.7%)	263 (100%)	72 (27.4%)	191 (72.6%)	263 (100%)
상급 종합병원	24 (58.5%)	17 (41.5%)	41 (100%)	29 (70.7%)	12 (29.3%)	41 (100%)
종합병원	24 (10.8%)	198 (89.2%)	222 (100%)	43 (19.4%)	179 (80.6%)	222 (100%)
도시(동)	47 (19.0%)	201 (81.0%)	248 (100%)	71 (28.6%)	177 (71.4%)	248 (100%)
비도시 (읍·면)	1 (6.7%)	14 (93.3%)	15 (100%)	1 (6.7%)	14 (93.3%)	15 (100%)
구분	보안 키패드			인증서 중계		
	예	아니오	합계	예	아니오	합계
전체	23 (8.7%)	240 (91.3%)	263 (100%)	25 (9.5%)	238 (90.5%)	263 (100%)
상급 종합병원	9 (22.0%)	32 (78.0%)	41 (100%)	8 (19.5%)	33 (80.5%)	41 (100%)
종합병원	14 (6.3%)	208 (93.7%)	222 (100%)	17 (7.7%)	205 (92.3%)	222 (100%)
도시(동)	23 (9.3%)	225 (90.7%)	248 (100%)	25 (10.1%)	223 (89.9%)	248 (100%)
비도시 (읍·면)	0 (0.0%)	15 (100%)	15 (100%)	0 (0.0%)	15 (100%)	15 (100%)
구분	모바일 SSO			여백		
	예	아니오	합계			
전체	25 (9.5%)	238 (90.5%)	263 (100%)			
상급 종합병원	11 (26.8%)	30 (73.2%)	41 (100%)			
종합병원	14 (6.3%)	208 (93.7%)	222 (100%)			
도시(동)	25 (10.1%)	223 (89.9%)	248 (100%)			
비도시 (읍·면)	0 (0.0%)	15 (100%)	15 (100%)			

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

상급종합병원(41개소)은 '앱 위변조 방지' 58.5%(24개소), '데이터 암호화' 70.7%(29개소), '보안 키패드' 22.0%(9개소), '인증서 중계' 19.5%(8개소), '모바일 SSO' 26.8%(11개소)로 나타났다.

반면 종합병원(222개소)은 각각 10.8%(24개소), 19.4%(43개소), 6.3%(14개소), 7.7%(17개소), 6.3%(14개소)로 나타나 전반적으로 낮은 수준을 보였다. 이는 상급종합병원이 모바일 기반 의료서비스(예: 모바일 전자의무기록 등)를 운영함에 따라 보안 요구 수준이 상대적으로 높은 반면, 종합병원은 모바일 서비스 활용 수준이 제한적인 데 따른 차이로 나타났다.

종합하면 의료기관의 모바일 보안 수준은 전반적으로 초기 단계에 머물러 있으며, 모바일 환경에서의 인증, 데이터 보호, 애플리케이션 위변조 방지 등 핵심 보안 통제의 도입이 제한적인 수준으로 나타났다. 또한 상급종합병원과 종합병원 간 모바일 보안 수준의 격차도 확인되었다. 이에 따라 모바일 보안 강화를 위해 데이터 암호화, 앱 위변조 방지, 모바일 인증체계 등 핵심 보안 기술 도입 확대와 함께, 기관 규모에 따른 기술적 지원을 통한 보안 수준 격차 해소가 필요한 것으로 나타났다.

10. 정부 지원 및 정책 개선 요구사항

본 영역에서는 의료기관이 정보보안 업무 강화를 위해 필요로 하는 정부 지원 사항과 법적·제도적 개선 과제를 순위별로 조사한 결과를 제시하였다. 이를 통해 의료기관이 현장에서 요구하는 지원 방향과 제도적 기반을 구체적으로 파악하고자 하였다.

〈표 5-123〉은 의료기관의 정보보안 업무 강화를 위해 정부 지원이 필요한 사항을 1·2·3순위로 조사한 결과를 나타낸 것이다.

1순위 응답에서는 '보안장비 도입 지원'이 40.7%(107개소)로 가장 높게 나타났으며, '보안 예산 확대' 33.1%(87개소), '법제·제도적 개선' 21.3%(56개소), '정보보안 관련 전문교육 제공' 4.2%(11개소), '기타' 0.8%(2개소) 순으로 나타났다.

2순위 응답에서는 '보안 예산 확대' 44.1%(116개소)와 '보안장비 도입 지원' 36.9%(97개소)가 주요 항목으로 나타났으며, '법제·제도적 개선' 12.9%(34개소), '정보보안 관련 전문교육 제공' 4.9%(13개소), '기타' 1.1%(3개소) 순으로 나타났다.

3순위 응답에서는 '법적·제도적 개선'이 39.9%(105개소)로 가장 높게 나타났고, '정보보안 관련 전문교육 제공' 27.8%(73개소), '보안장비 도입 지원' 18.3%(48개소), '보안 예산 확대' 13.3%(35개소), '기타' 0.8%(2개소) 순으로 나타났다.

〈표 5-123〉 정보보안 업무 강화를 위한 정부 지원 사항(순위별 빈도)

(단위: 개소, %)

항목	1순위	2순위	3순위
보안장비 도입 지원	107 (40.7%)	97 (36.9%)	48 (18.3%)
보안 예산 확대	87 (33.1%)	116 (44.1%)	35 (13.3%)
법적/제도적 개선	56 (21.3%)	34 (12.9%)	105 (39.9%)
정보보안 관련 전문 교육 제공	11 (4.2%)	13 (4.9%)	73 (27.8%)
기타	2 (0.8%)	3 (1.1%)	2 (0.8%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

종합하면 의료기관은 정보보안 강화를 위해 보안장비 도입과 예산 확대를 우선적으로 필요로 하고 있으며, 중장기적으로는 법제·제도 개선과 전문교육 지원에 대한 수요도 함께 나타났다. 이는 의료기관의 보안 역량 강화가 단순한 기술 도입을 넘어 재정적 지원과 제도적 기반, 인적 역량 강화가 병행되어야 함을 보여준다. 이에 따라 보안 인프라 구축을 위한

재정 지원 확대와 함께, 법제·제도 정비 및 전문인력 양성을 포함한 종합적인 지원체계 마련이 필요한 것으로 나타났다.

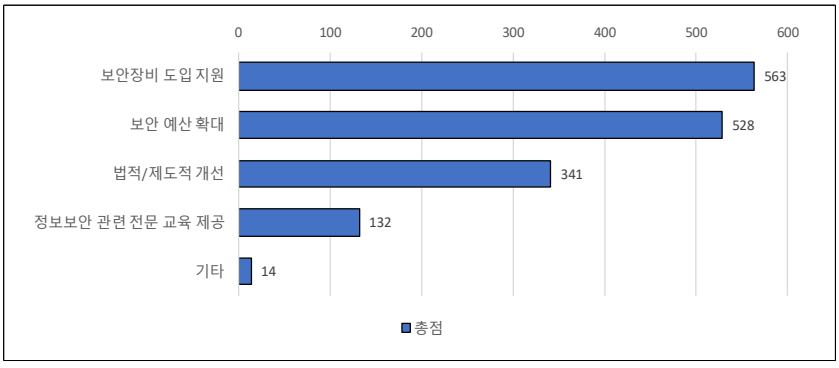
〈표 5-124〉는 의료기관의 정보보안 업무 강화를 위해 필요한 정부 지원 사항에 대해 우선순위별 가중치(1순위 3점, 2순위 2점, 3순위 1점)를 부여하여 중요도를 산출한 결과를 나타낸 것이다.

〈표 5-124〉 정보보안 업무 강화를 위한 정부 지원 사항(중요도 순위)

항목	응답수	총점	중요도 순위
보안장비 도입 지원	252	563	1
보안 예산 확대	238	528	2
법적/제도적 개선	195	341	3
정보보안 관련 전문 교육 제공	97	132	4
기타	7	14	5

주: 1순위는 3점, 2순위는 2점, 1순위에는 1점의 점수를 부여하여 가중 평균 점수 산출하였음.
출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

[그림 5-28] 정보보안 업무 강화를 위한 정부 지원 사항(중요도 순위)



출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

분석 결과 '보안장비 도입 지원'이 가장 높은 중요도를 보였으며, 이어 '보안 예산 확대', '법제·제도적 개선', '정보보안 관련 전문교육 제공',

‘기타’ 순으로 나타났다.

‘기타’ 응답으로는 ‘인력 증원’, ‘보안 전담 인력 제도화’, ‘정보보호 및 보안 인력에 대한 제도적 개선’ 등이 포함되어, 인력 기반 강화에 대한 요구도 함께 나타났다.

종합하면 의료기관은 보안 인프라 구축을 위한 장비 지원과 예산 확대를 가장 중요한 정부 지원 과제로 인식하고 있으며, 동시에 인력 확보와 제도적 기반 강화에 대한 수요도 함께 나타났다. 이에 따라 재정·장비 지원과 더불어 보안 인력 제도화 및 인력 기반 확충을 포함한 종합적 지원 체계 마련이 필요한 것으로 나타났다.

〈표 5-125〉는 법적·제도적 개선이 필요한 정보보안 관련 사항을 1·2·3순위로 조사한 결과를 나타낸 것이다.

1순위 응답에서는 ‘중소병원 대상 보안 지원 확대’가 52.8%(103개소)로 가장 높게 나타났으며, ‘보안관제 의무화 및 지원 법제화’ 37.4%(73개소), ‘개인정보보호법 강화’ 4.6%(9개소), ‘침해사고 신고 절차 간소화’ 2.6%(5개소), ‘기타’ 2.6%(5개소) 순으로 나타났다.

2순위 응답에서는 ‘보안관제 의무화 및 지원 법제화’ 37.4%(73개소), ‘개인정보보호법 강화’ 27.7%(55개소), ‘침해사고 신고 절차 간소화’ 21.0%(41개소), ‘중소병원 대상 보안 지원 확대’ 17.4%(34개소) 순으로 나타났다.

3순위 응답에서는 ‘개인정보보호법 강화’ 24.6%(48개소), ‘보안관제 의무화 및 지원 법제화’ 22.6%(44개소), ‘중소병원 대상 보안 지원 확대’ 11.8%(23개소), ‘침해사고 신고 절차 간소화’ 2.6%(5개소), ‘기타’ 1.5%(3개소) 순으로 나타났다.

종합하면 의료기관은 법적·제도적 개선 과제로 중소병원 대상 보안 지원 확대와 보안관제 의무화 및 지원 법제화를 가장 우선적인 과제로 인식

하고 있는 것으로 나타났다. 또한 개인정보보호법 강화와 침해사고 신고 절차 간소화에 대한 요구도 함께 나타났다. 이는 중소병원의 인력·예산 등 구조적 한계와 함께, 현행 제도의 지원 기능이 충분하지 않은 측면이 반영된 결과로 나타났다. 이에 따라 중소병원 중심의 보안 지원 확대와 보안관제 체계의 제도화, 신고 절차 개선 등을 포함한 법적·제도적 기반 강화가 필요한 것으로 나타났다.

〈표 5-125〉 법적/제도적 개선이 필요한 정보보안 관련 사항(순위별 빈도)

(단위: 개소, %)

항목	1순위	2순위	3순위
보안관제 의무화 및 지원 법제화	73 (37.4%)	66 (33.8%)	44 (22.6%)
개인정보보호법 강화	9 (4.6%)	54 (27.7%)	48 (24.6%)
중소병원 대상 보안 지원 확대	103 (52.8%)	34 (17.4%)	23 (11.8%)
침해사고 신고 절차 간소화	5 (2.6%)	41 (21.0%)	77 (39.5%)
기타	5 (2.6%)	0 (0.0%)	3 (1.5%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

〈표 5-126〉은 의료기관이 법적·제도적 개선이 필요하다고 인식한 정보보안 관련 사항에 대해 우선순위별 가중치(1순위 3점, 2순위 2점, 3순위 1점)를 부여하여 중요도를 산출한 결과를 나타낸 것이다.

분석 결과 '보안관제 의무화 및 지원 법제화'가 가장 높은 중요도를 보였으며, 이어 '개인정보보호법 강화', '중소병원 대상 보안 지원 확대', '침해사고 신고 절차 간소화', '기타' 순으로 나타났다.

'기타' 응답으로는 '보안 인력 비율 의무화(예: IT 인력의 10% 수준)', '인증 대상 확대', '보안 투자 비율 의무화', '정보보호 및 보안 인력(조직) 확충', 'ISMS 컨설팅 지원' 등이 포함되어, 인력·투자·제도 전반에 걸친 개선 요구가 함께 나타났다.

종합하면 의료기관은 법적·제도적 개선 과제로 보안관제 체계의 의무

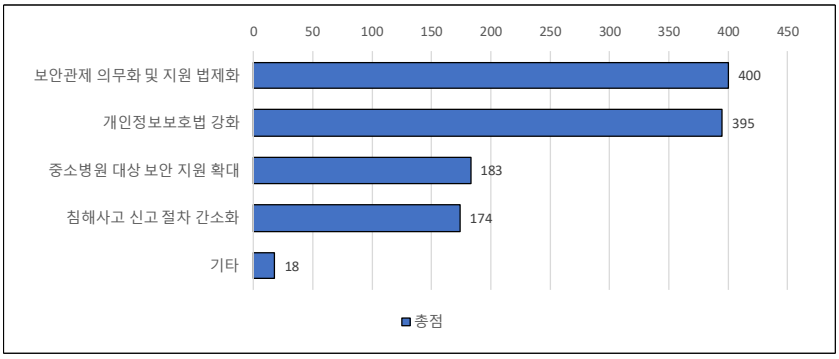
화와 제도적 지원을 가장 중요하게 인식하고 있으며, 동시에 개인정보 보호 강화와 중소병원 중심의 지원 확대에 대한 수요도 높은 것으로 나타났다. 이는 의료기관의 보안 역량 강화를 위해서는 단순한 권고 수준을 넘어 실질적 의무화와 지원을 병행하는 정책 접근이 필요함을 보여준다. 이에 따라 보안관제 의무화 및 지원 법제화를 중심으로, 중소병원 지원 확대와 보안 인력·투자 기준 마련 등 종합적인 제도 개선이 필요한 것으로 나타났다.

〈표 5-126〉 법적/제도적 개선이 필요한 정보보안 관련 사항(중요도 순위)

항목	응답수	총점	중요도 순위
보안관제 의무화 및 지원 법제화	160	400	1
개인정보보호법 강화	183	395	2
중소병원 대상 보안 지원 확대	111	183	3
침해사고 신고 절차 간소화	123	174	4
기타	8	18	5

주: 1순위는 3점, 2순위는 2점, 1순위에는 1점의 점수를 부여하여 가중 평균 점수 산출하였음.
출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

[그림 5-29] 법적/제도적 개선이 필요한 정보보안 관련 사항(중요도 순위)



출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

11. 보안관제 체계 도입 관련

본 영역에서는 보안관제 체계 도입 필요성, 도입 이유 및 기대효과, 저해 요인, 정책적 지원 수요, 제도 개선 필요성 등과 관련한 의료기관의 인식을 종합적으로 파악하고자 하였다. 이를 통해 의료기관이 보안관제 체계를 어떻게 인식하고 있으며, 향후 어떤 정책적 지원과 제도적 기반을 요구하는지를 분석하였다.

가. 보안관제 체계 도입 필요성 및 이유

〈표 5-127〉은 보안관제 체계 도입 필요성 여부를 조사한 결과를 나타낸 것이다.

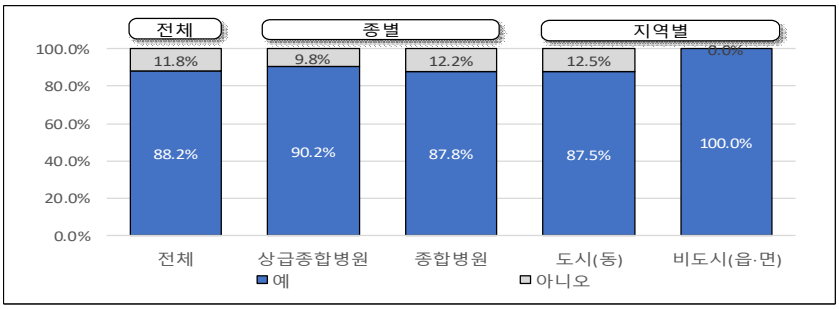
〈표 5-127〉 보안관제 체계 도입 필요성 여부

구분		예	아니오	합계
전체	전체	232 (88.2%)	31 (11.8%)	263 (100%)
종별	상급종합병원	37 (90.2%)	4 (9.8%)	41 (100%)
	종합병원	195 (87.8%)	27 (12.2%)	222 (100%)
지역별	도시(동)	217 (87.5%)	31 (12.5%)	248 (100%)
	비도시(읍·면)	15 (100%)	0 (0.0%)	15 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

전체 응답기관(263개소) 중 보안관제 체계 도입이 필요하다고 응답한 비율은 88.2%(232개소)로 나타났다. 의료기관 종별로는 상급종합병원 90.2%(37개소), 종합병원 87.8%(195개소)로 나타나, 대부분의 의료기관이 보안관제 체계 도입의 필요성을 인식하고 있는 것으로 나타났다.

[그림 5-30] 보안관제 체계 도입 필요성 여부



출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

〈표 5-128〉은 보안관제 체계 도입이 필요한 이유를 우선순위별로 조사한 결과를 나타낸 것이다.

1순위에서는 '실시간 위협 탐지 및 차단'이 67.2%(156개소)로 가장 높게 나타났으며, '보안사고 사전 예방' 25.4%(59개소), '법적 요구사항 준수' 6.0%(14개소), '데이터 무결성 및 신뢰성 확보' 1.3%(3개소) 순으로 나타났다.

2순위에서는 '보안사고 사전 예방' 63.8%(148개소), '실시간 위협 탐지 및 차단' 24.6%(57개소), '법적 요구사항 준수' 9.1%(21개소), '데이터 무결성 및 신뢰성 확보' 2.6%(6개소) 순으로 나타났다.

3순위에서는 '법적 요구사항 준수' 66.8%(155개소), '데이터 무결성 및 신뢰성 확보' 17.2%(40개소), '보안사고 사전 예방' 9.1%(21개소), '실시간 위협 탐지 및 차단' 6.9%(16개소) 순으로 나타났다.

종합하면 의료기관은 보안관제 체계 도입의 주요 이유로 실시간 위협 대응과 보안사고 사전 예방을 가장 중요하게 인식하고 있으며, 동시에 법적 요구사항 준수와 데이터 무결성 확보 역시 중요한 고려 요소로 작용하고 있는 것으로 나타났다.

〈표 5-128〉 보안관제 체계 도입 필요성의 이유(순위별 빈도)

(단위: 개소, %)

항목	1순위	2순위	3순위
실시간 위협 탐지 및 차단	156 (67.2%)	57 (24.6%)	16 (6.9%)
보안사고 사전 예방	59 (25.4%)	148 (63.8%)	21 (9.1%)
법적 요구사항 준수(개인정보보호법, 의료법 등)	14 (6.0%)	21 (9.1%)	155 (66.8%)
데이터 무결성 및 신뢰성 확보	3 (1.3%)	6 (2.6%)	40 (17.2%)
기타	0 (0.0%)	0 (0.0%)	0 (0.0%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

〈표 5-129〉는 보안관제 체계 도입이 필요한 이유에 대해 우선순위별 가중치(1순위 3점, 2순위 2점, 3순위 1점)를 부여하여 중요도를 산출한 결과이다.

'실시간 위협 탐지 및 차단'이 가장 중요한 것으로 나타났으며, 다음으로 '보안사고 사전 예방', '법적 요구사항 준수', '데이터 무결성 및 신뢰성 확보' 순으로 나타났다.

〈표 5-129〉 보안관제 체계 도입 필요성의 이유항(중요도 순위)

(단위: 개소, %)

항목	응답수	총점	중요도 순위
실시간 위협 탐지 및 차단	229	598	1
보안 사고 사전 예방	228	494	2
법적 요구사항 준수(개인정보보호법, 의료법 등)	190	239	3
데이터 무결성 및 신뢰성 확보	49	61	4
기타	0	0	5

주: 1순위는 3점, 2순위는 2점, 1순위에는 1점의 점수를 부여하여 가중 평균 점수 산출하였음.
출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

종합하면 의료기관은 보안관제 체계를 통해 실시간 대응 역량을 확보하는 것을 최우선 과제로 인식하고 있으며, 동시에 사고 예방 기능과 법적 요구사항 준수, 데이터 신뢰성 확보를 종합적으로 고려하고 있는 것으로 나타났다.

나. 보안관제 체계 도입 시 기대효과

〈표 5-130〉은 보안관제 체계 도입 시 기대효과에 대해 우선순위를 고려해 3개를 선택하게 한 결과이다.

1순위에서는 '실시간 위협 탐지 차단' 67.2%(156개소), '보안사고 사전 예방' 25.4%(59개소), '법적 요구사항 준수' 6.0%(14개소), '데이터 무결성 및 신뢰성 확보' 11.3%(3개소) 순으로 나타났다.

2순위에서는 '보안사고 사전 예방' 63.8%(148개소)와 '실시간 위협 탐지 및 차단' 24.6%(57개소), '법적 요구사항 준수' 9.1%(21개소), '데이터 무결성 및 신뢰성 확보' 2.6%(6개소) 순으로 나타났으며, 3순위에서는 '법적 요구사항 준수' 66.8%(155개소), '데이터 무결성 및 신뢰성 확보' 17.2%(40개소), '보안 사고 사전 예방' 9.1%(21개소), '실시간 위협 탐지 및 차단' 6.9%(16개소) 순으로 나타났다.

〈표 5-130〉 보안관제 체계 도입 시 기대 효과(순위별 빈도)

(단위: 개소, %)

항목	1순위	2순위	3순위
침해 사고에 대한 신속한 대응	175 (75.4%)	31 (13.4%)	20 (8.6%)
인력 효율화 및 비용 절감	19 (8.2%)	95 (40.9%)	34 (14.7%)
일관성 있는 보안 정책 적용	16 (6.9%)	57 (24.6%)	115 (49.6%)
보안 시스템 통합 관리	21 (9.1%)	48 (20.7%)	63 (27.2%)
기타	1 (0.4%)	1 (0.4%)	0 (0.0%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

종합하면 의료기관은 보안관제 체계 도입을 통해 실시간 위협 대응과 보안사고 예방 효과를 가장 크게 기대하고 있으며, 동시에 법적 요구사항 준수와 데이터 무결성 확보 역시 중요한 기대효과로 인식하고 있는 것으

로 나타났다.

〈표 5-131〉과 같이 보안관제 체계 도입 시 기대효과에 대해 우선순위별 가중치(1순위 3점, 2순위 2점, 3순위 1점)를 부여하여 중요도를 산출한 결과이다.

'침해 사고에 대한 신속한 대응', '인력 효율화 및 비용 절감', '보안 시스템 통합 관리', '일관성 있는 보안정책 적용' 순으로 나타났다.

종합하면 의료기관은 보안관제 체계를 통해 침해사고 대응 속도를 향상시키는 것을 가장 중요한 효과로 인식하고 있으며, 동시에 인력 운영의 효율화와 비용 절감, 보안 시스템의 통합적 관리, 그리고 보안정책의 일관성 확보 등 운영 효율성과 관리 체계 고도화 측면에서도 긍정적 효과를 기대하고 있는 것으로 나타났다.

〈표 5-131〉 보안관제 체계 도입 시 기대 효과(중요도 순위)

항목	응답수	총점	중요도 순위
침해 사고에 대한 신속한 대응	226	607	1
인력 효율화 및 비용 절감	148	281	2
일관성 있는 보안 정책 적용	188	277	3
보안 시스템 통합 관리	132	222	4
기타	2	5	5

주: 1순위는 3점, 2순위는 2점, 1순위에는 1점의 점수를 부여하여 가중 평균 점수 산출하였음.
출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

다. 보안관제 체계 도입 저해 요인

〈표 5-132〉는 보안관제 체계 도입 저해 요인에 대해 우선순위를 고려해 3개를 선택하게 한 결과이다.

1순위에서는 '초기 구축 비용 부담' 66.5%(175개소), '(내부)기술적 지

식 부족' 17.9%(47개소), '(내부)전문 인력 부족' 14.1%(37개소), '보안 관제 필요성에 대한 경영진의 인식 부족' 1.1%(3개소), '기타' 0.4%(1개소) 순으로 나타났고, 2순위에서는 '(내부)전문 인력 부족' 47.9%(126개소)와 '(내부)기술적 지식 부족' 22.1%(58개소), '초기 구축 비용 부담' 19.0%(50개소), '보안관제 필요성에 대한 경영진의 인식 부족' 11.0%(29개소) 순으로 나타났으며, 3순위에서는 '(내부)기술적 지식 부족' 31.9%(84개소), '보안관제 필요성에 대한 경영진의 인식 부족' 31.2%(82개소), '(내부)전문 인력 부족' 30.8%(81개소), '초기 구축 비용 부담' 5.7%(15개소), '기타' 0.4%(1개소) 순으로 나타났다.

종합하면 의료기관의 보안관제 체계 도입을 저해하는 주요 요인은 초기 구축 비용 부담을 중심으로, 전문 인력 부족과 기술적 역량 부족이 복합적으로 작용하고 있는 것으로 나타났다. 또한 일부 기관에서는 경영진의 보안관제 필요성에 대한 인식 부족도 도입 저해 요인으로 작용하고 있는 것으로 나타났다. 이는 보안관제 체계 확산을 위해 단순한 재정 지원뿐만 아니라 전문 인력 양성, 기술 지원, 그리고 조직 차원의 인식 제고를 포함한 종합적인 정책적 접근이 필요함을 시사한다.

〈표 5-132〉 보안관제 체계 도입 저해 요인(순위별 빈도)

(단위: 개소, %)

항목	1순위	2순위	3순위
초기 구축 비용 부담	175 (66.5%)	50 (19.0%)	15 (5.7%)
(내부)전문 인력 부족	37 (14.1%)	126 (47.9%)	81 (30.8%)
보안관제 필요성에 대한 경영진의 인식 부족	3 (1.1%)	29 (11.0%)	82 (31.2%)
(내부)기술적 지식 부족	47 (17.9%)	58 (22.1%)	84 (31.9%)
기타	1 (0.4%)	0 (0.0%)	1 (0.4%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

〈표 5-133〉과 같이 보안관제 체계 도입 저해 요인에 대해 우선순위별 가중치(1순위 3점, 2순위 2점, 3순위 1점)를 부여하여 중요도를 산출한 결과이다. '침해 사고에 대한 신속한 대응', '(내부)전문 인력 부족', '보안관제 필요성에 대한 경영진의 인식 부족', '(내부)기술적 지식 부족', '기타' 순으로 나타났다.

종합하면 의료기관의 보안관제 체계 도입을 저해하는 요인은 비용 부담을 중심으로 인력 부족과 기술적 역량 부족, 그리고 조직 차원의 인식 부족이 복합적으로 작용하고 있는 것으로 나타났다. 이는 보안관제 체계 확산을 위해 재정적 지원뿐만 아니라 전문 인력 양성, 기술 지원, 경영진 인식 제고 등 다각적인 정책적 접근이 필요함을 시사한다.

〈표 5-133〉 보안관제 체계 도입 저해 요인(중요도 순위)

항목	응답수	총점	중요도 순위
초기 구축 비용 부담	240	640	1
(내부)전문 인력 부족	244	444	2
보안관제 필요성에 대한 경영진의 인식 부족	189	341	3
(내부)기술적 지식 부족	114	149	4
기타	2	4	5

주: 1순위는 3점, 2순위는 2점, 1순위에는 1점의 점수를 부여하여 가중 평균 점수 산출하였음.
출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

라. 보안관제 체계 도입 촉진을 위한 필요한 지원

〈표 5-134〉는 보안관제 체계 도입 촉진을 위한 필요한 지원에 대해 우선순위를 고려해 3개를 선택하게 한 결과이다.

1순위에서는 '정부의 재정 지원' 81.0%(213개소), '보안 수준 점검 시스템' 10.3%(27개소), '전문 기술지원 및 교육' 4.6%(12개소), '보안관제 체계 구축 시 상담 창구' 2.3%(6개소), '법적 요건 강화' 0.8%(2개소), '기

타' 0.8%(2개소), '클라우드 서비스 제공' 0.4%(1개소) 순으로 나타났다.

2순위에서는 '전문 기술 지원 및 교육' 44.9%(118개소), '보안 수준 점검 시스템' 17.1%(45개소), '보안관제 체계 구축 시 상담 창구' 15.6%(41개소), '10.6' 81.0%(28개소), '클라우드 서비스 제공' 7.6% (20개소), '법적 요건 강화' 4.2%(11개소) 순으로 나타났다.

3순위에서는 '전문 기술 지원 및 교육' 29.3%(77개소), '보안관제 체계 구축 시 상담 창구' 24.0%(63개소), '클라우드 서비스 제공' 20.9%(55개소), '보안 수준 점검 시스템' 16.0%(42개소), '법적 요건 강화' 5.7%(15개소), '정부의 재정 지원' 4.2%(11개소) 순으로 나타났다.

종합하면 보안관제 체계 도입 촉진을 위해서는 무엇보다 정부의 재정 지원이 핵심적인 요소로 인식되고 있으며, 동시에 전문 기술지원 및 교육, 보안 수준 점검 체계 구축, 상담 지원 체계 마련 등 기술적·운영적 지원이 함께 요구되고 있는 것으로 나타났다. 또한 클라우드 서비스 제공과 법적 요건 강화에 대한 수요도 일부 확인되어, 다층적인 지원 정책이 필요함을 시사한다.

〈표 5-134〉 보안관제 체계 도입 촉진을 위한 필요한 지원(순위별 빈도)

(단위: 개소, %)

항목	1순위	2순위	3순위
정부의 재정 지원	213 (81.0%)	28 (10.6%)	11 (4.2%)
전문 기술지원 및 교육	12 (4.6%)	118 (44.9%)	77 (29.3%)
법적 요건 강화	2 (0.8%)	11 (4.2%)	15 (5.7%)
보안 수준 점검 시스템	27 (10.3%)	45 (17.1%)	42 (16.0%)
보안관제 체계 구축 시 상담 창구	6 (2.3%)	41 (15.6%)	63 (24.0%)
클라우드 서비스 제공	1 (0.4%)	20 (7.6%)	55 (20.9%)
기타	2 (0.8%)	0 (0.0%)	0 (0.0%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

〈표 5-135〉는 보안관제 체계 도입 촉진을 위해 필요한 지원에 대해 우선순위별 가중치(1순위 3점, 2순위 2점, 3순위 1점)를 부여하여 중요도를 산출한 결과이다.

'정부의 재정 지원', '전문 기술 지원 및 교육', '법적 요건 강화', '보안 수준 점검 시스템', '보안관제 체계 구축 시 상담 창구', '클라우드 서비스 제공', '기타' 순으로 나타났다.

종합하면 의료기관은 보안관제 체계 도입 촉진을 위해 재정적 지원을 최우선 과제로 인식하고 있으며, 동시에 전문 인력 양성과 기술 역량 강화를 위한 교육·지원, 제도적 기반 마련, 운영 지원 체계 구축 등을 함께 요구하고 있는 것으로 나타났다. 이는 보안관제 확산을 위해 재정·기술·제도적 지원이 결합된 종합적인 정책 접근이 필요함을 시사한다.

〈표 5-135〉 보안관제 체계 도입 촉진을 위한 필요한 지원(중요도 순위)

항목	응답수	총점	중요도 순위
정부의 재정 지원	252	706	1
전문 기술지원 및 교육	207	349	2
법적 요건 강화	114	213	3
보안 수준 점검 시스템	110	163	4
보안관제 체계 구축 시 상담 창구	76	98	5
클라우드 서비스 제공	28	43	6
기타	2	6	7

주: 1순위는 3점, 2순위는 2점, 1순위에는 1점의 점수를 부여하여 가중 평균 점수 산출하였음.
출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

마. 보안관제 체계 도입 효과를 높이기 위한 필요한 요소

〈표 5-136〉은 보안관제 도입 효과를 높이기 위해 필요한 요소에 대해 우선순위를 고려해 3개를 선택하게 한 결과이다.

1순위에서는 '실시간 위협 탐지 기술' 47.1%(124개소), '보안 인력 확충' 35.7%(94개소), '비용 효율적인 솔루션' 15.6%(41개소), '전 직원 보안 교육 강화' 1.5%(4개소) 순으로 나타났고, 2순위에서는 '보안 인력 확충' 41.1%(108개소)와 '실시간 위협 탐지 기술' 27.4%(72개소), '비용 효율적인 솔루션' 26.6%(70개소), '전 직원 보안 교육 강화' 4.9%(13개소) 순으로 나타났으며, 3순위에서는 '비용 효율적인 솔루션' 45.2%(119개소), '전 직원 보안 교육 강화' 21.3%(56개소), '실시간 위협 탐지 기술' 18.3%(48개소), '보안 인력 확충' 15.2%(40개소) 순으로 나타났다.

종합하면 보안관제 도입 효과를 극대화하기 위해서는 실시간 위협 탐지 기술 확보와 보안 인력 확충이 핵심 요소로 인식되고 있으며, 동시에 비용 효율적인 솔루션 도입과 전 직원 대상 보안 교육 강화도 중요한 보완 요소로 작용하고 있는 것으로 나타났다.

〈표 5-136〉 보안관제 도입 효과를 높이기 위해 필요한 요소(순위별 빈도)

(단위: 개소, %)

항목	1순위	2순위	3순위
실시간 위협 탐지 기술	124 (47.1%)	72 (27.4%)	48 (18.3%)
보안 인력 확충	94 (35.7%)	108 (41.1%)	40 (15.2%)
비용 효율적인 솔루션	41 (15.6%)	70 (26.6%)	119 (45.2%)
전 직원 보안 교육 강화	4 (1.5%)	13 (4.9%)	56 (21.3%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

〈표 5-137〉과 같이 보안관제 도입 효과를 높이기 위해 필요한 요소에 대해 우선순위별 가중치(1순위 3점, 2순위 2점, 3순위 1점)를 부여하여 중요도를 산출한 결과이다.

'실시간 위협 탐지 기술', '보안 인력 확충', '비용 효율적인 솔루션', '전 직원 보안 교육 강화' 순으로 나타났다.

종합하면 보안관제 도입 효과를 극대화하기 위해서는 실시간 위협 탐

지 기술 확보가 핵심적인 요소로 인식되고 있으며, 이를 뒷받침하는 보안 인력 확충과 비용 효율적인 솔루션 도입, 조직 전반의 보안 인식 강화를 위한 교육이 함께 이루어져야 하는 것으로 나타났다. 이는 기술·인력·비용·조직문화 요소가 균형 있게 작용할 때 보안관제 체계의 실효성이 높아질 수 있음을 시사한다.

〈표 5-137〉 보안관제 도입 효과를 높이기 위해 필요한 요소(중요도 순위)

항목	응답수	총점	중요도 순위
실시간 위협 탐지 기술	244	564	1
보안 인력 확충	242	538	2
비용 효율적인 솔루션	230	382	3
전 직원 보안 교육 강화	73	94	4

주: 1순위는 3점, 2순위는 2점, 1순위에는 1점의 점수를 부여하여 가중 평균 점수 산출하였음.
출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

바. 보안사고 예방을 위한 보안관제 체계의 효과 및 그 이유

〈표 5-138〉은 보안사고 예방을 위한 보안관제 체계의 효과에 대해 조사한 결과를 나타낸 것이다.

전체 의료기관(263개소)을 대상으로 보안관제 체계의 효과에 대해 조사한 결과 '매우 효과적이다' 27.0%(71개소), '효과적이다' 41.5%(17개소), '보통이다' 27.0%(71개소), '효과적이지 않다' 0.8%(2개소), '전혀 효과적이지 않다' 0.4%(1개소)로 응답하여, 긍정적인 의견(매우 효과적이다+효과적이다)이 71.9%이었으며, 부정적인 의견(효과적이지 않다+전혀 효과적이지 않다)이 1.2%로 나타났다.

의료기관 종별로 살펴보면 상급종합병원(41개소)은 '매우 효과적이다' 41.5%(17개소), '효과적이다' 53.7%(22개소), '보통이다' 4.9%(2개소)로 나타나 긍정적 의견이 95.2%로 매우 높게 나타났으며, 부정적 의견은

없는 것으로 나타났다. 반면 종합병원(222개소)은 '매우 효과적이다' 24.3%(54개소), '효과적이다' 43.2%(96개소), '보통이다' 31.1%(69개소), '효과적이지 않다' 0.9%(2개소), '전혀 효과적이지 않다' 0.5%(1개소)로 나타나 긍정적 의견은 67.5%, 부정적 의견은 1.4%로 나타났다.

〈표 5-138〉 보안 사고 예방을 위한 보안관제 체계의 효과에 대한 의견

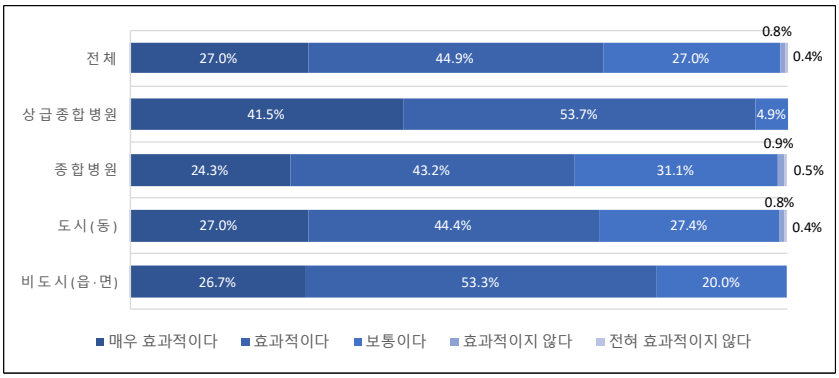
(단위: 개소, %)

구분		매우 효과적이다	효과적이다	보통이다	효과적이지 않다	전혀 효과적이지 않다	합계
전체	전체	71 (27.0%)	118 (44.9%)	71 (27%)	2 (0.8%)	1 (0.4%)	263 (100%)
종별	상급종합병원	17 (41.5%)	22 (53.7%)	2 (4.9%)	0 (0.0%)	0 (0.0%)	41 (100%)
	종합병원	54 (24.3%)	96 (43.2%)	69 (31.1%)	2 (0.9%)	1 (0.5%)	222 (100%)
지역별	도시(동)	67 (27%)	110 (44.4%)	68 (27.4%)	2 (0.8%)	1 (0.4%)	248 (100%)
	비도시(읍·면)	4 (26.7%)	8 (53.3%)	3 (20.0%)	0 (0.0%)	0 (0.0%)	15 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

종합하면 의료기관은 보안관제 체계가 보안사고 예방에 있어 효과적인 수단으로 인식하고 있는 것으로 나타났다. 특히 상급종합병원은 보안관제 효과에 대해 매우 높은 신뢰를 보이고 있는 반면, 종합병원은 긍정적 인식이 상대적으로 낮고 '보통' 응답 비중이 높아 체감 효과에 다소 차이가 존재하는 것으로 나타났다. 이는 보안관제 운영 수준, 인력 및 기술 역량, 투자 규모 등의 차이에 기인한 것으로 여겨진다.

[그림 5-31] 보안사고 예방을 위한 보안관제 체계의 효과에 대한 의견



출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

사. 의료법 상 실시간 보안관제 의무화 포함 필요

〈표 5-139〉는 의료법상 실시간 보안관제 의무화 포함 필요 여부에 대해 조사한 결과를 나타낸 것이다.

전체 의료기관(263개소)을 대상으로 의료법 상 실시간 보안관제 의무화 포함 필요 여부에 대해 조사한 결과 '매우 필요하다' 10.6%(28개소), '필요하다' 38.0%(100개소), '보통이다' 47.1%(124개소), '필요하지 않다' 4.2%(11개소)로 응답하여, 긍정적인 의견(매우 필요하다+필요하다)이 48.6%이었으며, 부정적인 의견(필요하지 않다+전혀 필요하지 않다)이 4.2%로 나타났다.

의료기관 종별로 살펴보면 상급종합병원(41개소)은 '매우 필요하다' 24.4%(10개소), '필요하다' 43.9%(18개소), '보통이다' 29.3%(12개소), '필요하지 않다' 2.4%(1개소)로 나타나 긍정적 의견이 68.3%로 비교적 높게 나타났으며, 부정적 의견은 2.4%로 낮게 나타났다. 반면 종합병원(222개소)은 '매우 필요하다' 8.1%(18개소), '필요하다' 36.9%(82개소),

‘보통이다’ 50.5%(112개소), ‘필요하지 않다’ 4.5%(10개소)로 나타나 긍정적 의견은 45.0%, 부정적 의견은 4.5%로 나타났다.

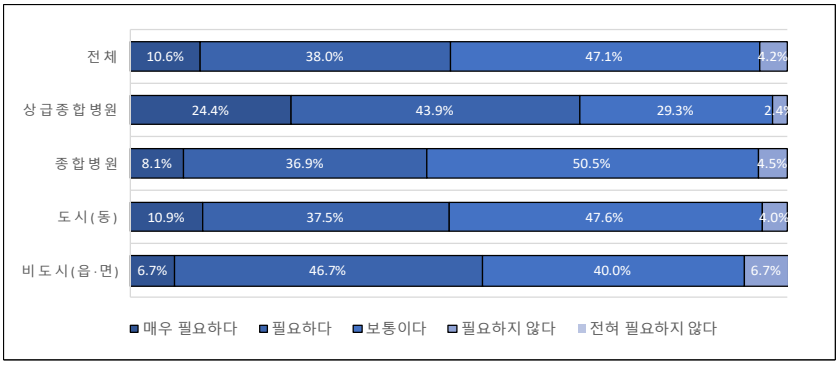
〈표 5-139〉 의료법상 실시간 보안관제 의무화 포함 필요 여부에 대한 의견

(단위: 개소, %)

구분		매우 필요하다	필요하다	보통이다	필요하지 않다	전혀 필요하지 않다	합계
전체	전체	28 (10.6%)	100 (38.0%)	124 (47.1%)	11 (4.2%)	0 (0.0%)	263 (100%)
종별	상급종합병원	10 (24.4%)	18 (43.9%)	12 (29.3%)	1 (2.4%)	0 (0.0%)	41 (100%)
	종합병원	18 (8.1%)	82 (36.9%)	112 (50.5%)	10 (4.5%)	0 (0.0%)	222 (100%)
지역별	도시(동)	27 (10.9%)	93 (37.5%)	118 (47.6%)	10 (4.0%)	0 (0.0%)	248 (100%)
	비도시(읍·면)	1 (6.7%)	7 (46.7%)	6 (40.0%)	1 (6.7%)	0 (0.0%)	15 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

[그림 5-32] 의료법상 실시간 보안관제 의무화 포함 필요 여부에 대한 의견



출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

종합하면 의료기관은 실시간 보안관제 의무화에 대해 전반적으로 필요성을 인식하고 있으나, ‘보통’ 응답 비중이 높아 제도 도입에 대해 신중한

태도를 보이고 있는 것으로 나타났다. 특히 상급종합병원은 의무화 필요성에 대한 인식이 상대적으로 높은 반면, 종합병원은 비용 부담, 인력 부족, 운영 여건 등의 현실적 제약으로 인해 상대적으로 낮은 수준의 수용도를 보이는 것으로 해석된다. 이는 향후 제도 도입 시 의료기관 규모와 여건을 고려한 단계적 적용과 지원 정책이 병행될 필요가 있음을 시사한다.

아. 중소 의료기관을 위한 클라우드 기반 보안관제서비스

〈표 5-140〉은 중소 의료기관을 위한 클라우드 기반 보안관제 서비스 도입에 대해 조사한 결과를 나타낸 것이다.

전체 의료기관(263개소)을 대상으로 조사한 결과 '매우 긍정적이다' 8.0%(21개소), '긍정적이다' 41.8%(110개소), '보통이다' 44.9%(118개소), '부정적이다' 4.2%(11개소), '매우 부정적이다' 1.1%(3개소)로 나타났다. 이를 긍정적 의견('매우 긍정적이다'+'긍정적이다')과 부정적 의견('부정적이다'+'매우 부정적이다')으로 구분하면, 긍정적 의견은 49.8%, 부정적 의견은 5.3%로 나타났다.

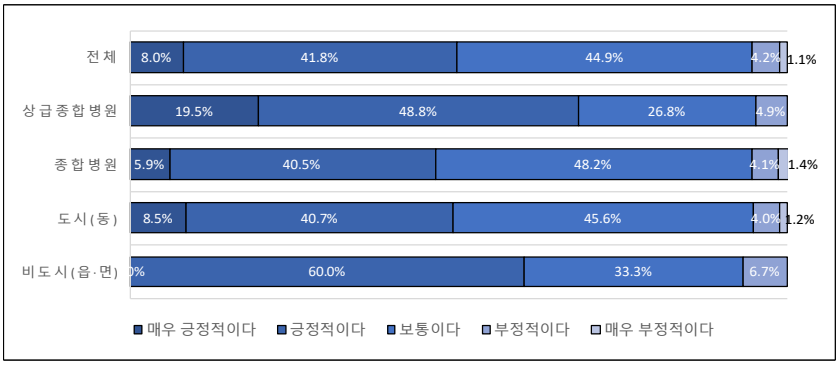
의료기관 종별로 살펴보면 상급종합병원(41개소)은 '매우 긍정적이다' 19.5%(8개소), '긍정적이다' 48.8%(20개소), '보통이다' 26.8%(11개소), '부정적이다' 4.9%(2개소)로 나타나 긍정적 의견이 68.3%로 비교적 높게 나타났으며, 부정적 의견은 4.9%로 낮은 수준을 보였다. 반면 종합병원(222개소)은 '매우 긍정적이다' 5.9%(13개소), '긍정적이다' 40.5%(90개소), '보통이다' 48.2%(107개소), '부정적이다' 4.1%(9개소), '매우 부정적이다' 1.4%(3개소)로 나타나 긍정적 의견은 46.4%, 부정적 의견은 5.5%로 나타났다.

〈표 5-140〉 중소 의료기관을 위한 클라우드 기반 보안관제 서비스 도입에 대한 의견

구분		매우 긍정적이다	긍정적이다	보통이다	부정적이다	매우 부정적이다	합계
전체	전체	21 (8.0%)	110 (41.8%)	118 (44.9%)	11 (4.2%)	3 (1.1%)	263 (100%)
종별	상급종합병원	8 (19.5%)	20 (48.8%)	11 (26.8%)	2 (4.9%)	0 (0.0%)	41 (100%)
	종합병원	13 (5.9%)	90 (40.5%)	107 (48.2%)	9 (4.1%)	3 (1.4%)	222 (100%)
지역별	도시(동)	21 (8.5%)	101 (40.7%)	113 (45.6%)	10 (4.0%)	3 (1.2%)	248 (100%)
	비도시(읍·면)	0 (0.0%)	9 (60.0%)	5 (33.3%)	1 (6.7%)	0 (0.0%)	15 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

[그림 5-33] 중소 의료기관을 위한 클라우드 기반 보안관제 서비스 도입에 대한 의견



출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

종합하면 의료기관은 중소 의료기관을 위한 클라우드 기반 보안관제 서비스 도입에 대해 전반적으로 긍정적인 인식을 보이고 있으나, '보통' 응답 비중이 높아 제도 도입에 대해 신중한 태도를 유지하고 있는 것으로 나타났다. 특히 상급종합병원은 클라우드 기반 보안관제 도입에 대해 높은 수용도를 보인 반면, 종합병원은 상대적으로 낮은 긍정 비율과 높은

‘보통’ 응답 비중을 보여 비용 부담, 보안 신뢰성, 운영 안정성 등에 대한 우려가 일부 존재하는 것으로 해석된다. 이는 향후 클라우드 기반 보안관제 서비스 확산을 위해 기술적 신뢰성 확보와 함께 비용 지원, 표준 가이드라인 마련, 단계적 도입 전략 등이 병행될 필요가 있음을 시사한다.

〈표 5-141〉은 의료정보보호 관제서비스 이용 시 장점에 대해 우선순위를 고려해 3개를 선택하게 한 결과이다.

1순위 응답에서는 ‘24*365 실시간 감시로 업무 중단 최소화’가 43.0%(113개소)로 가장 높게 나타났으며, 이어 ‘침해 사고 등에 대한 신속한 대응’ 19.8%(52개소), ‘조직·인력 효율화로 인건비 절감’ 17.1%(45개소) 순으로 나타났다.

2순위에서는 ‘24*365 실시간 감시로 업무 중단 최소화’가 27.0%(71개소)로 가장 높은 비중을 보였으며, 다음으로 ‘보안관제를 위한 설비 및 투자 비용 절감’ 17.1%(45개소), ‘침해 사고 등에 대한 신속한 대응’ 16.3%(43개소) 순으로 나타났다.

3순위에서는 ‘보안 전문가 활용에 따른 보안 전문성 강화’가 24.7%(65개소)로 가장 높게 나타났으며, 이어 ‘보안관제를 위한 설비 및 투자 비용 절감’과 ‘침해 사고 등에 대한 신속한 대응’이 각각 20.2%(53개소)로 나타났다.

종합하면 의료기관은 의료정보보호 관제서비스의 주요 장점으로 ‘24시간 상시 감시를 통한 서비스 중단 최소화’를 가장 중요하게 인식하고 있으며, 동시에 침해사고 대응의 신속성, 비용 절감, 전문성 확보 등 다양한 측면에서 긍정적인 효과를 기대하고 있는 것으로 나타났다. 특히 1·2순위에서 실시간 감시 기능이 지속적으로 가장 높은 비중을 차지한 점은 의료기관이 보안관제의 핵심 가치를 ‘지속적 모니터링과 즉각 대응 체계’에 두고 있음을 보여준다. 한편 3순위에서 보안 전문성 강화가 가장 높은

비중을 차지한 것은 내부 인력과 역량의 한계를 보완하기 위한 외부 전문 서비스 활용 수요가 존재함을 시사한다.

〈표 5-141〉 의료정보보호 관제서비스 이용 시 장점(순위별 빈도)

(단위: 개소, %)

항목	1순위	2순위	3순위
조직·인력 효율화로 인건비 절감	45 (17.1%)	20 (7.6%)	23 (8.7%)
24*365 실시간 감시로 업무 중단 최소화	113 (43.0%)	71 (27.0%)	18 (6.8%)
보안관제를 위한 설비 및 투자비용 절감	20 (7.6%)	45 (17.1%)	53 (20.2%)
보안전문가 활용에 따른 보안전문성 강화	12 (4.6%)	37 (14.1%)	65 (24.7%)
보안시스템 통합관리	17 (6.5%)	28 (10.6%)	28 (10.6%)
일관성 있는 보안정책 적용	4 (1.5%)	19 (7.2%)	23 (8.7%)
침해사고 등에 대한 신속한 대응	52 (19.8%)	43 (16.3%)	53 (20.2%)
기타	0 (0.0%)	0 (0.0%)	0 (0.0%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

〈표 5-142〉는 의료정보보호 관제 서비스 이용 시 장점에 대해 우선순위별 가중치(1순위 3점, 2순위 2점, 3순위 1점)를 부여하여 중요도를 산출한 결과이다.

〈표 5-142〉 의료정보보호 관제서비스 이용 시 장점(중요도 순위)

항목	응답수	총점	중요도 순위
조직·인력 효율화로 인건비 절감	88	198	4
24*365 실시간 감시로 업무 중단 최소화	202	499	1
보안관제를 위한 설비 및 투자비용 절감	118	203	3
보안전문가 활용에 따른 보안전문성 강화	114	175	5
보안시스템 통합관리	73	135	6
일관성 있는 보안정책 적용	46	73	7
침해사고 등에 대한 신속한 대응	148	295	2
기타	0	0	8

주: 1순위는 3점, 2순위는 2점, 1순위에는 1점의 점수를 부여하여 가중 평균 점수 산출하였음.
출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

‘24*365 실시간 감시로 업무 중단 최소화’, ‘침해사고 등에 대한 신속한 대응’, ‘보안관제를 위한 설비 및 투자 비용 절감’, ‘조직·인력 효율화로 인건비 절감’, ‘보안전문가 활용에 따른 보안전문성 강화’, ‘보안시스템 통합관리’, ‘일관성 있는 보안정책 적용’, ‘기타’ 순으로 나타났다.

종합하면 의료기관은 보안관제 서비스의 핵심 가치로 ‘실시간 감시 기반의 서비스 연속성 확보’를 가장 중요하게 인식하고 있으며, 동시에 침해사고 대응 역량 강화와 비용 효율성 확보를 주요 기대효과로 인식하고 있는 것으로 나타났다.

12. 의료정보보호센터 및 보안관제 가입 활성화 등

본 영역에서는 의료정보보호센터 보안관제서비스(ISAC) 가입 여부, 의료정보보호센터와의 협력체계 구축 정도, 의료정보보호센터와의 협력을 위한 개선점, 보안관제 서비스 가입 활성화를 위해 필요한 지원, 보안관제 가입 의무화 정책 필요성에 대한 의견을 구체적으로 파악하기 위한 목적으로 구성되었다.

〈표 5-143〉은 의료정보보호센터 보안관제서비스(ISAC) 가입 여부에 대해 조사한 결과를 나타낸 것이다.

전체 의료기관(263개소) 중 의료정보보호센터 보안관제서비스(ISAC)에 가입하였다고 응답한 의료기관은 16.2%(43개소), 가입하지 않았다고 응답한 의료기관은 83.7%(220개소)로 나타났다

의료기관 종별로 살펴보면 상급종합병원이 43.9%(18개소), 종합병원이 11.3%(25개소)가 의료정보보호센터 보안관제서비스(ISAC)에 가입했다고 응답했으며, 지역별로는 도시지역이 17.3(43개소)가 의료정보보호센터 보안관제서비스(ISAC)에 가입했다고 응답했으나, 비도시지역은 가

입한 의료기관이 없다고 응답했다.

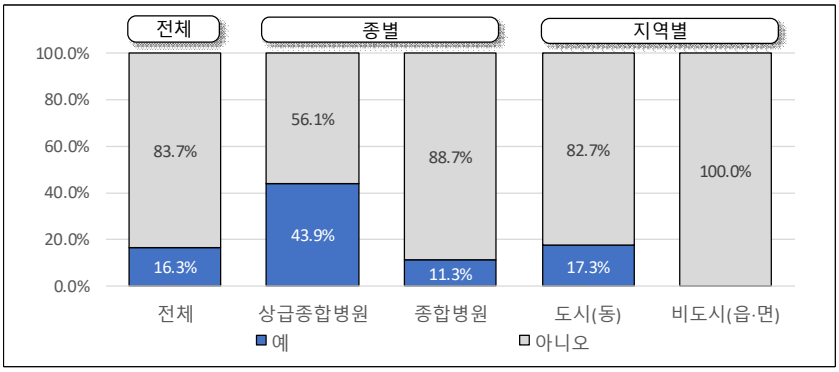
〈표 5-143〉 의료정보보호센터 보안관제서비스(ISAC) 가입 여부

(단위: 개소, %)

구분		예	아니오	합계
전체	전체	43 (16.3%)	220 (83.7%)	263 (100%)
종별	상급종합병원	18 (43.9%)	23 (56.1%)	41 (100%)
	종합병원	25 (11.3%)	197 (88.7%)	222 (100%)
지역별	도시(동)	43 (17.3%)	205 (82.7%)	248 (100%)
	비도시(읍·면)	0 (0.0%)	15 (100%)	15 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

[그림 5-34] 의료정보보호센터 보안관제서비스(ISAC) 가입 여부



출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

〈표 5-144〉는 의료정보보호센터와의 협력 체계 구축 정도를 조사한 결과를 나타낸 것이다.

의료정보보호센터 보안관제서비스(ISAC) 가입했다고 응답한 의료기관(43개소)을 대상으로 의료정보보호센터와의 협력체계 구축 정도를 조사한 결과, '매우 잘 구축되어 있다' 25.6%(11개소), '잘 구축되어 있다' 60.5%(26개소), '보통이다' 11.6%(5개소). '전혀 잘 구축되어 있지 않다'

2.3%(1개소)로 응답하여 긍정적인 의견(매우 잘 구축되어 있다+잘 구축되어 있다)이 86.1%, 부정적인 의견(잘 구축되어 있지 않다+전혀 구축되어 있지 않다)이 2.3%로 나타났다.

〈표 5-144〉 의료정보보호센터와의 협력 체계 구축 정도

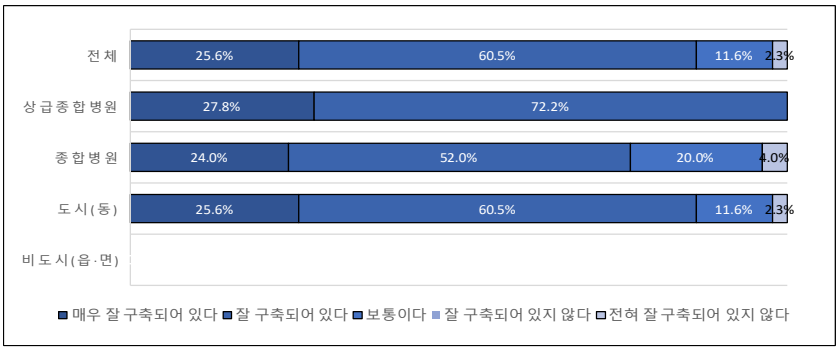
(단위: 개소, %)

구분		매우 잘 구축되어 있다	잘 구축되어 있다	보통이다	잘 구축되어 있지 않다	전혀 구축되어 있지 않다	합계
전체	전체	11 (25.6%)	26 (60.5%)	5 (11.6%)	0 (0.0%)	1 (2.3%)	43 (100%)
종별	상급종합병원	5 (27.8%)	13 (72.2%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	18 (100%)
	종합병원	6 (24.0%)	13 (52.0%)	5 (20.0%)	0 (0.0%)	1 (4.0%)	25 (100%)
지역별	도시(동)	11 (25.6%)	26 (60.5%)	5 (11.6%)	0 (0.0%)	1 (2.3%)	43 (100%)
	비도시(읍·면)	-	-	-	-	-	-

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

의료기관 종별로 상급종합병원(18개소)은 '매우 잘 구축되어 있다' 27.8%(5개소), '잘 구축되어 있다' 72.2%(13개소)로 응답하여 긍정적인 의견(매우 잘 구축되어 있다+잘 구축되어 있다)이 100.0%로 나타났고, 종합병원은 '매우 잘 구축되어 있다' 24.0%(6개소), '잘 구축되어 있다' 52.0%(13개소), '보통이다' 20.0%(5개소). '전혀 잘 구축되어 있지 않다' 4.0%(1개소)로 응답하여 긍정적인 의견(매우 잘 구축되어 있다+잘 구축되어 있다)이 76.0%, 부정적인 의견(잘 구축되어 있지 않다+전혀 구축되어 있지 않다)이 4.0%로 나타났다.

[그림 5-35] 의료정보보호센터와의 협력 체계 구축 정도



출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

〈표 5-145〉는 의료정보보호센터 보안관제서비스(ISAC) 가입했다고 응답한 의료기관(43개소)을 대상으로 의료정보보호센터와의 협력을 위한 개선점을 조사한 결과를 나타낸 것이다.

'추가적인 지원시스템 도입'이 44.2%(19개소)로 가장 높았고, 다음으로 '공유 기술 교육 및 훈련' 32.6%(14개소), '협력체계 정례화' 14.0%(6개소), '정보 공유 시스템 다변화' 7.0%(3개소), '기타' 23.3%(1개소) 순으로 나타났다.

의료기관 종별로 살펴보면 상급종합병원(18개소)은 '추가적인 지원시스템 도입'이 50.0%(9개소)로 가장 높았고, 다음으로 '공유 기술 교육 및 훈련' 27.8%(5개소), '정보 공유 시스템 다변화' 11.1%(2개소) 순으로 나타났고, 종합병원(25개소)은 '추가적인 지원시스템 도입'이 40.0%(10개소)로 가장 높았고, 다음으로 '공유 기술 교육 및 훈련' 36.0%(9개소), '공유 기술 교육 및 훈련' 20.0%(5개소) 순으로 나타났다.

종합하면 의료기관은 의료정보보호센터와의 협력 강화를 위해 기술적 지원 확대와 교육·훈련 제공을 핵심 개선 과제로 인식하고 있으며, 특히 추가적인 지원 시스템 도입에 대한 요구가 가장 높은 것으로 나타났다.

이는 기존 보안관제 서비스만으로는 의료기관의 다양한 보안 요구를 충분히 충족하기 어렵다는 인식이 반영된 결과로 해석된다. 또한 종합병원에서는 협력체계의 정례화 요구가 상대적으로 높게 나타나, 지속적이고 체계적인 협력 운영 기반 마련에 대한 필요성도 함께 제기되고 있다.

〈표 5-145〉 의료정보보호센터와의 협력을 위한 개선점

(단위: 개소, %)

구분		정보 공유 시스템 다변화	공유 기술 교육 및 훈련	협력체계 정례화	추가적인 지원시스템 도입	기타	합계
전체	전체	3 (7.0%)	14 (32.6%)	6 (14.0%)	19 (44.2%)	1 (2.3%)	43 (100%)
종별	상급종합병원	2 (11.1%)	5 (27.8%)	1 (5.6%)	9 (50.0%)	1 (5.6%)	18 (100%)
	종합병원	1 (4.0%)	9 (36.0%)	5 (20.0%)	10 (40.0%)	0 (0.0%)	25 (100%)
지역별	도시(동)	3 (7.0%)	14 (32.6%)	6 (14.0%)	19 (44.2%)	1 (2.3%)	43 (100%)
	비도시(읍·면)	-	-	-	-	-	-

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

〈표 5-146〉은 보안관제서비스 가입 활성화를 위해 필요한 지원에 대해 조사한 결과를 나타낸 것이다.

전체 의료기관(263개소)을 대상으로 보안관제 서비스 가입 활성화를 위해 필요한 지원을 조사한 결과, '비용 지원'이 67.7%(178개소)로 가장 높았고, 다음으로 '장비 도입 지원' 17.5%(46개소), '법적 지원 강화' 6.8%(18개소), '기술적 컨설팅' 6.1%(16개소), '기타' 1.9%(5개소) 순으로 나타났다.

의료기관 종별로 살펴보면 상급종합병원(41개소)은 '비용 지원'이 58.5%(24개소)로 가장 높았고, 다음으로 '장비 도입 지원' 24.4%(10개소), '기술적 컨설팅' 7.3%(3개소), '법적 지원 강화'와 '기타'가 각각 4.9%(2개소) 순으로 나타났으며, 종합병원(222개소)은 '비용 지원'이 69.4%(154개소)로 가장 높았고, 다음으로 '장비 도입 지원' 16.2%(36개소), '법적 지

원 강화' 7.2%(16개소), '기술적 컨설팅' 5.9%(13개소), '기타' 1.4%(3개소) 순으로 나타났다.

종합하면 의료기관은 보안관제서비스 가입 활성화를 위해 무엇보다 재정적 지원을 가장 시급한 과제로 인식하고 있으며, 특히 종합병원에서 그 요구가 더욱 크게 나타났다. 이는 중소 규모 의료기관일수록 보안 투자 여력이 제한적이라는 구조적 한계를 반영한 것으로 여겨진다. 또한 장비 도입 지원과 기술적 컨설팅에 대한 요구도 일정 수준 존재하여, 단순한 비용 지원을 넘어 초기 구축부터 운영까지를 포괄하는 통합적 지원 정책이 필요한 것으로 여겨진다.

〈표 5-146〉 보안관제서비스 가입 활성화를 위해 필요한 지원

(단위: 개소, %)

구분		비용 지원	장비 도입 지원	기술적 컨설팅	법적 지원 강화	기타	합계
전체	전체	178 (67.7%)	46 (17.5%)	16 (6.1%)	18 (6.8%)	5 (1.9%)	263 (100%)
종별	상급종합병원	24 (58.5%)	10 (24.4%)	3 (7.3%)	2 (4.9%)	2 (4.9%)	41 (100%)
	종합병원	154 (69.4%)	36 (16.2%)	13 (5.9%)	16 (7.2%)	3 (1.4%)	222 (100%)
지역별	도시(동)	166 (66.9%)	45 (18.1%)	16 (6.5%)	16 (6.5%)	5 (2.0%)	248 (100%)
	비도시(읍·면)	12 (80.0%)	1 (6.7%)	0 (0.0%)	2 (13.3%)	0 (0.0%)	15 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

〈표 5-147〉은 보안관제 가입 의무화 정책 필요성에 대해 조사한 결과를 나타낸 것이다.

전체 의료기관(263개소)을 대상으로 보안관제 가입 의무화 정책 필요성을 조사한 결과, '매우 필요하다' 11.0%(29개소), '필요하다' 25.5%(67개소), '보통이다' 58.2%(153개소). '필요하지 않다' 4.2%(11개소),

‘전혀 필요하지 않다’ 1.1%(3개소)로 응답하여 긍정적인 의견(매우 필요하다+필요하다)이 36.5%, 부정적인 의견(필요하지 않다+전혀 필요하지 않다)이 5.3%로 나타났다.

의료기관 종별로 살펴보면 상급종합병원(41개소)은 ‘매우 필요하다’ 26.8%(11개소), ‘필요하다’ 41.5%(17개소), ‘보통이다’ 26.8%(11개소). ‘필요하지 않다’ 4.9%(2개소)로 응답하여 긍정적인 의견(매우 필요하다+필요하다)이 68.3%, 부정적인 의견(필요하지 않다+전혀 필요하지 않다)이 4.9%로 나타났고, 종합병원(222개소)은 ‘매우 필요하다’ 8.1%(18개소), ‘필요하다’ 22.5%(50개소), ‘보통이다’ 64.0%(142개소). ‘필요하지 않다’ 4.1%(9개소), ‘전혀 필요하지 않다’ 1.4%(3개소)로 응답하여 긍정적인 의견(매우 필요하다+필요하다)이 30.6%, 부정적인 의견(필요하지 않다+전혀 필요하지 않다)이 5.5%로 나타났다.

〈표 5-147〉 보안관제 가입 의무화 정책 필요성에 대한 의견

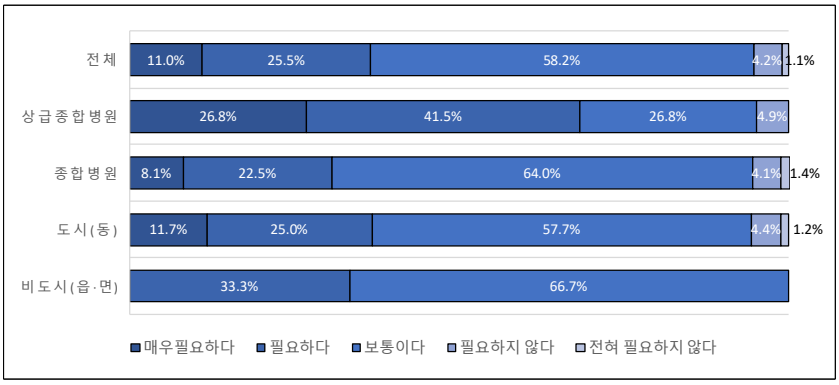
(단위: 개소, %)

구분		매우 필요하다	필요하다	보통이다	필요하지 않다	전혀 필요하지 않다	합계
전체	전체	29 (11.0%)	67 (25.5%)	153 (58.2%)	11 (4.2%)	3 (1.1%)	263 (100%)
종별	상급종합병원	11 (26.8%)	17 (41.5%)	11 (26.8%)	2 (4.9%)	0 (0.0%)	41 (100%)
	종합병원	18 (8.1%)	50 (22.5%)	142 (64.0%)	9 (4.1%)	3 (1.4%)	222 (100%)
지역별	도시(동)	29 (11.7%)	62 (25.0%)	143 (57.7%)	11 (4.4%)	3 (1.2%)	248 (100%)
	비도시(읍·면)	0 (0.0%)	5 (33.3%)	10 (66.7%)	0 (0.0%)	0 (0.0%)	15 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

종합하면 보안관제 가입 의무화 정책에 대해 의료기관은 전반적으로 필요성을 일정 수준 인식하고 있으나, 적극적인 찬성보다는 신중한 입장을 보이는 경향이 나타났다. 특히 상급종합병원은 정책 필요성에 대한 공감도가 높은 반면, 종합병원은 '보통' 응답 비중이 높아 의무화에 따른 비용 부담, 운영 여건, 인력 및 기술적 준비 수준 등에 대한 현실적 고려가 반영된 것으로 여겨진다.

[그림 5-36] 보안관제 가입 의무화 정책 필요성에 대한 의견



출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

13. 기타: LLM(대형언어모델) 기반 AI 서비스 등

본 영역에서는 최근 주목받고 있는 인공지능(AI) 기술인 LLM(대형 언어 모델)에 관련하여 의료기관의 LLM서비스 도입 여부, LLM서비스의 주요 활용 분야, LLM서비스 도입에 따른 보안 이슈 우려 사항, LLM서비스에 특화된 보안 툴 도입 여부, 도입된 LLM서비스 보안 툴의 종류, 도입된 LLM서비스의 보안 툴의 만족도 등에 대한 의견을 구체적으로 파악하기 위한 목적으로 구성되었다.

〈표 5-148〉은 의료기관의 LLM서비스 도입 여부를 조사한 결과를 나타낸 것이다.

전체 의료기관(263개소)을 대상으로 LLM서비스 도입 여부는 '이미 도입함' 7.2%(19개소), '시험 도입 중' 5.7%(15개소), '도입 예정' 8.7%(23개소), '도입계획 없음' 61.6%(162개소), '모르겠음' 16.7%(44개소)로 나타났다.

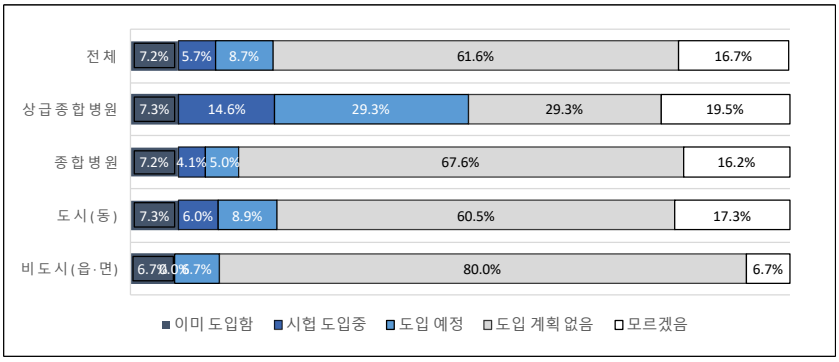
〈표 5-148〉 LLM서비스 도입 여부

(단위: 개소, %)

구분		이미 도입함	시험 도입 중	도입 예정	도입 계획 없음	모르겠음	합계
전체	전체	19 (7.2%)	15 (5.7%)	23 (8.7%)	162 (61.6%)	44 (16.7%)	263 (100%)
종별	상급종합병원	3 (7.3%)	6 (14.6%)	12 (29.3%)	12 (29.3%)	8 (19.5%)	41 (100%)
	종합병원	16 (7.2%)	9 (4.1%)	11 (5.0%)	150 (67.6%)	36 (16.2%)	222 (100%)
지역별	도시(동)	18 (7.3%)	15 (6.0%)	22 (8.9%)	150 (60.5%)	43 (17.3%)	248 (100%)
	비도시(읍·면)	1 (6.7%)	0 (0.0%)	1 (6.7%)	12 (80%)	1 (6.7%)	15 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

[그림 5-37] LLM서비스 도입 여부



출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

의료기관 종별로 살펴보면, 상급종합병원(41개소)은 '이미 도입함' 7.3%(3개소), '시험 도입 중' 14.6%(6개소), '도입 예정' 29.3%(12개소)인 것으로 나타났으며, 종합병원(222개소)은 '이미 도입함' 7.2%(16개소), '시험 도입 중' 4.1%(9개소), '도입 예정' 5.0%(11개소)인 것으로 나타났다.

종합하면 의료기관의 LLM 서비스 도입은 아직 초기 단계에 머물러 있으며, 특히 종합병원에서는 도입 계획이 없는 비율이 높아 기술 도입에 대한 신중한 태도가 나타나고 있다. 반면 상급종합병원은 시험 도입 및 도입 예정 비율이 상대적으로 높아, 연구·진료 지원 및 업무 효율화를 위한 신기술 도입이 점진적으로 확대되고 있는 것으로 나타났다.

〈표 5-149〉는 LLM서비스의 주요 활용분야에 대해 조사한 결과를 나타낸 것이다.

전체 의료기관(263개소)을 대상으로 LLM서비스 도입 여부에서 '이미 도입함', '시험 도입 중', '도입 예정'이라고 응답한 57개 의료기관을 대상으로 LLM서비스의 주요 활용 분야를 복수 응답으로 조사한 결과 총 응답 수 97개 중 '임상 지원' 44.3(43개)이 가장 많았으며, 다음으로 '행정 업무 자동화' 19.6%(19개), '환자 상담 챗봇' 18.6%(18개), '연구 및 데이터 분석' 14.4%(14개), '기타' 3.1%(3개) 순으로 나타났다.

의료기관 종별로 살펴보면, 상급종합병원 응답 수 47개 중 '임상 지원' 38.3%(18개), '환자 상담 챗봇' 21.3%(10개), '행정 업무 자동화'와 '연구 및 데이터 분석'이 각각 19.1%(9개), '기타' 2.1%(1개) 순으로 나타났으며, 종합병원 응답 수 50개 중 '임상 지원' 50.0%(25개), '행정 업무 자동화' 20.0%(10개), '환자 상담 챗봇' 16.0%(8개), '연구 및 데이터 분석' 10.0%(5개), '기타' 4.0%(2개) 순으로 나타났다.

종합하면 의료기관의 LLM서비스 활용은 전반적으로 '임상 지원' 분야

에 집중되어 있으며, 행정 업무 자동화와 환자 상담 등 보조적 영역으로 점진적으로 확산되고 있는 것으로 나타났다. 특히 상급종합병원은 환자 상담 및 연구 활용 비중이 상대적으로 높은 반면, 종합병원은 임상 지원과 행정 효율화 중심의 활용 경향이 두드러지는 것으로 나타났다.

〈표 5-149〉 LLM서비스의 주요 활용분야

(단위: 개소, %)

구분		임상 지원	행정 업무 자동화	환자 상담 챗봇	연구 및 데이터 분석	기타	합계
전체	전체	43 (44.3%)	19 (19.6%)	18 (18.6%)	14 (14.4%)	3 (3.1%)	97 (100%)
종별	상급종합병원	18 (38.3%)	9 (19.1%)	10 (21.3%)	9 (19.1%)	1 (2.1%)	47 (100%)
	종합병원	25 (50.0%)	10 (20.0%)	8 (16.0%)	5 (10.0%)	2 (4.0%)	50 (100%)
지역별	도시(동)	41 (44.6%)	18 (19.6%)	17 (18.5%)	13 (14.1%)	3 (3.3%)	92 (100%)
	비도시(읍·면)	2 (40.0%)	1 (20.0%)	1 (20.0%)	1 (20.0%)	0 (0.0%)	5 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

〈표 5-150〉 LLM서비스 도입에 따른 보안이슈 우려사항에 대해 조사한 결과를 나타낸 것이다.

LLM서비스 도입 여부에서 '이미 도입함', '시험 도입 중', '도입 예정'이라고 응답한 57개 의료기관을 대상으로 LLM서비스 도입에 따른 보안 이슈 우려 사항을 복수 응답으로 조사한 결과 총 응답 수 161개 중 '민감정보 유출' 30.4%(49개), '규정 미준수' 15.5%(25개), '데이터 익명화·암호화 부족' 14.3%(23개), '데이터 주권 문제' 11.2%(18개), 'AI 모델 조작 및 악성 입력' 9.9%(16개), '외부 해킹 시도' 9.9%(16개), '허가받지 않은 내부 직원의 무단 접근' 8.1%(13개), '기타' 0.6%(1개) 순으로 나타났다.

의료기관 종별로 살펴보면 상급종합병원 응답 수 64개 중 '민감정보 유출' 31.2%(20개), '규정 미준수' 18.8%(12개), '데이터 익명화·암호화

부족' 17.2%(11개)가 높게 나타났으며, 종합병원 응답 수 97개 중 '민감정보 유출' 29.9%(29개), '데이터 주권 문제' 15.5%(15개), '규정 미준수' 13.4%(13개)가 높게 나타났다.

종합하면 의료기관은 LLM 서비스 도입 시 가장 큰 보안 리스크로 민감정보 유출을 인식하고 있으며, 이와 함께 규정 준수, 데이터 보호, 모델 보안 등 다양한 위험요인에 대한 복합적인 우려를 가지고 있는 것으로 나타났다. 특히 상급종합병원은 개인정보 보호 및 규제 준수 측면에, 종합병원은 데이터 주권 및 관리 통제 측면에 상대적으로 높은 관심을 보이고 있어 의료기관 유형별로 보안 우려의 초점이 다소 상이한 것으로 나타났다.

〈표 5-150〉 LLM서비스 도입에 따른 보안이슈 우려사항

구분	민감정보 (환자 개인정보 등) 유출	데이터 주권 문제	AI 모델 조작 및 악성 입력	허가 받지 않은 내부 직원의 무단 접근	외부 해킹 시도
전체	49 (30.4%)	18 (11.2%)	16 (9.9%)	13 (8.1%)	16 (9.9%)
상급종합병원	20 (31.2%)	3 (4.7%)	6 (9.4%)	5 (7.8%)	6 (9.4%)
종합병원	29 (29.9%)	15 (15.5%)	10 (10.3%)	8 (8.2%)	10 (10.3%)
도시(동)	47 (30.5%)	18 (11.7%)	14 (9.1%)	12 (7.8%)	15 (9.7%)
비도시(읍·면)	2 (28.6%)	0 (0.0%)	2 (28.6%)	1 (14.3%)	1 (14.3%)
구분	데이터 익명화·암호화 부족	규정 미준수 (예: 개인정보 보호법, HIPAA 등)	기타	합계	여백
전체	23 (14.3%)	25 (15.5%)	1 (0.6%)	161 (100%)	
상급종합병원	11 (17.2%)	12 (18.8%)	1 (1.6%)	64 (100%)	
종합병원	12 (12.4%)	13 (13.4%)	0 (0.0%)	97 (100%)	
도시(동)	22 (14.3%)	25 (16.2%)	1 (0.6%)	154 (100%)	
비도시(읍·면)	1 (14.3%)	0 (0.0%)	0 (0.0%)	7 (100%)	

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

〈표 5-151〉은 LLM서비스에 특화된 보안툴 도입여부에 대해 조사한 결과를 나타낸 것이다.

LLM서비스 도입 여부에서 '이미 도입함', '시험 도입 중', '도입 예정'이라고 응답한 57개 의료기관을 대상으로 LLM서비스에 특화된 보안 툴 도입 여부를 조사한 결과 '이미 도입함' 3.5%(2개소), '시험 도입 중' 5.3%(3개소), '도입계획 없음' 50.9%(29개소), '모르겠음' 40.4%(23개소)로 나타났다.

의료기관 종별로 살펴보면 상급종합병원(21개소) 중 '이미 도입함' 또는 '시험 도입 중'이라는 응답이 전혀 없는 것으로 나타났으며, 종합병원(36개소) 중 '이미 도입함' 5.6%(2개소), '시험 도입 중' 8.3%(3개소)로 나타났다.

〈표 5-151〉 LLM서비스에 특화된 보안툴 도입여부

(단위: 개소, %)

구분		이미 도입함	시험 도입 중	도입 계획 없음	모르겠음	합계
전체	전체	2 (3.5%)	3 (5.3%)	29 (50.9%)	23 (40.4%)	57 (100%)
종별	상급종합병원	0 (0.0%)	0 (0.0%)	16 (76.2%)	5 (23.8%)	21 (100%)
	종합병원	2 (5.6%)	3 (8.3%)	13 (36.1%)	18 (50.0%)	36 (100%)
지역별	도시(동)	2 (3.6%)	3 (5.5%)	28 (50.9%)	22 (40.0%)	55 (100%)
	비도시(읍·면)	0 (0.0%)	0 (0.0%)	1 (50.0%)	1 (50.0%)	2 (100%)

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

종합하면 의료기관은 LLM기술 도입에 비해 보안 대응 체계 구축은 다소 미흡한 것으로 나타났다. 특히 절반 이상의 기관이 보안툴 도입 계획이 없다고 응답하고, 상당수 기관이 도입 여부를 명확히 인지하지 못하고 있는 점은 LLM관련 보안 인식과 대응 역량이 아직 충분히 정립되지 않았음을 시사한다. 이는 향후 LLM 기반 의료서비스 확산에 따라 개인정보

보호, 데이터 유출 방지, AI 모델 보안 등을 위한 특화된 보안 솔루션 도입과 함께 관련 가이드라인 및 정책적 지원이 병행될 필요가 있다.

〈표 5-152〉는 도입된 LLM서비스 보안툴의 종류에 대해 조사한 결과를 나타낸 것이다.

LLM서비스에 특화된 보안 툴을 '이미 도입함' 또는 '시험 도입 중'이라고 응답한 의료기관(5개소)을 대상으로 도입된 LLM서비스 보안 툴의 종류에 대해 복수 응답으로 조사한 결과 '입력/출력 데이터 필터링 솔루션'과 'AI 시스템 취약점 점검 및 위협 탐지 솔루션'이 각각 27.3%(3개소), '모델 접근제어 및 인증 솔루션'과 '모델 및 데이터 암호화 툴'이 각각 18.2%(2개소), 'AI 트래픽 모니터링 툴' 9.1%(1개소) 순으로 나타났다.

〈표 5-152〉 도입된 LLM서비스 보안툴의 종류

(단위: 개소, %)

구분		AI 트래픽 모니터링 툴	입력/출력 데이터 필터링 솔루션	모델 접근제어 및 인증 솔루션	모델 및 데이터 암호화 툴	AI 시스템 취약점 점검 및 위협 탐지 솔루션	기타
전체	전체	1 (9.1%)	3 (27.3%)	2 (18.2%)	2 (18.2%)	3 (27.3%)	0 (0.0%)
종별	상급종합병원	-	-	-	-	-	-
	종합병원	1 (9.1%)	3 (27.3%)	2 (18.2%)	2 (18.2%)	3 (27.3%)	0 (0.0%)
지역별	도시(동)	1 (9.1%)	3 (27.3%)	2 (18.2%)	2 (18.2%)	3 (27.3%)	0 (0.0%)
	비도시(읍·면)	-	-	-	-	-	-

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

종합하면 LLM 보안툴을 도입한 의료기관은 주로 데이터 입력·출력 단계에서의 통제와 AI 시스템의 취약점 점검 및 위협 탐지 기능을 중심으로 보안체계를 구축하고 있는 것으로 나타났다. 이는 LLM 서비스에서 발생할 수 있는 프롬프트 기반 공격, 민감정보 유출 등의 위험에 대응하기 위한 기본적인 방어 조치가 우선적으로 고려되고 있음을 보여준다. 반면 모

델 접근제어, 데이터 암호화, 트래픽 모니터링 등 보다 고도화된 보안 기능은 상대적으로 일부 기관에 한정되어 있어, LLM 보안체계가 아직 초기 단계에 머물러 있음을 보여준다.

특히 전체적으로 도입 기관 수가 매우 제한적이라는 점을 고려할 때, 의료기관의 LLM 보안 대응은 전반적으로 초기 탐색 단계에 있으며 향후 AI 보안 위협에 대응하기 위한 통합적이고 체계적인 보안 프레임워크 구축이 필요할 것으로 여겨진다.

〈표 5-153〉 도입된 LLM서비스의 보안툴의 만족도에 대해 조사한 결과를 나타낸 것이다.

LLM서비스에 특화된 보안 툴을 '이미 도입함' 또는 '시험 도입 중'이라고 응답한 의료기관(5개소)을 대상으로 도입된 LLM서비스의 보안 툴의 만족도를 조사한 결과 '높은 편이다'

〈표 5-153〉 도입된 LLM서비스의 보안툴의 만족도

(단위: 개소, %)

구분		매우 높다	높은 편이다	보통이다	낮은 편이다	매우 낮다
전체	전체	0 (0.0%)	2 (40.0%)	3 (60.0%)	0 (0.0%)	0 (0.0%)
종별	상급종합병원	-	-	-	-	-
	종합병원	0 (0.0%)	2 (40.0%)	3 (60.0%)	0 (0.0%)	0 (0.0%)
지역별	도시(동)	0 (0.0%)	2 (40.0%)	3 (60.0%)	0 (0.0%)	0 (0.0%)
	비도시(읍·면)	-	-	-	-	-

출처: 한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료를 활용하여 저자 작성

제3절 소결

본 장에서는 전국 상급종합병원과 종합병원을 대상으로 의료기관의 사이버 보안 실태를 조사하여 보안관제 운영 현황, 정보시스템 구축 환경, 조직 및 인력 운영, 보안 교육, 보안 정책 체계, 침해사고 대응 역량, 정책 지원 수요 등을 종합적으로 분석하였다.

주요 조사 결과를 요약하면 다음과 같다.

첫째, 보안관제 운영 현황을 보면 전체 의료기관 중 약 57%만이 보안관제를 운영하고 있으며, 약 43%의 의료기관은 보안관제를 실시하지 않는 것으로 나타났다. 특히 종합병원의 보안관제 도입률이 상급종합병원에 비해 낮게 나타나 의료기관 규모에 따른 보안 대응 역량 격차가 존재하는 것으로 확인되었다. 또한 보안관제를 운영하는 의료기관의 경우에도 대부분 단일 유형의 관제 체계를 운영하고 있어 다층적 보안관제 체계 구축은 제한적인 수준에 머물러 있는 것으로 나타났다.

둘째, 보안 인증체계 도입 수준은 전반적으로 낮은 것으로 나타났다. 보안관제를 실시하는 의료기관 중에서도 인증을 보유한 의료기관은 일부에 불과한 것으로 나타나 의료기관 전반의 보안 인증 도입 수준은 여전히 제한적인 것으로 확인되었다.

셋째, 정보화·개인정보보호·정보보안 예산 구조를 보면 정보화 예산에 비해 개인정보보호 및 정보보안 예산 비중이 매우 낮은 것으로 나타났다. 정보화 예산 대비 개인정보보호 예산은 평균 약 3% 미만 수준이며 정보보안 예산 역시 상대적으로 낮은 수준에 머물러 있는 것으로 확인되었다. 또한 일부 의료기관에서는 개인정보보호 또는 정보보안 관련 예산이 전혀 편성되지 않은 사례도 확인되어 보안 투자 기반이 충분히 확보되지 못한 의료기관도 존재하는 것으로 나타났다.

넷째, 정보화 및 보안 예산의 적절성 인식을 보면 정보화 예산에 대해서는 비교적 적절하다는 응답이 많은 반면, 개인정보보호 및 정보보안 예산에 대해서는 '적절하지 않다'는 응답이 40% 이상으로 나타났다. 이는 다수 의료기관이 현재의 보안 투자 수준이 충분하지 않다고 인식하고 있음을 시사한다.

다섯째, 전자의무기록시스템(EMR) 인증제도 인지도 및 도입 현황을 보면 제도에 대한 인지도는 전반적으로 높은 수준으로 나타났으며 인증된 전자의무기록시스템을 도입한 의료기관도 상당한 수준으로 확인되었다. 특히 상급종합병원은 대부분 인증 시스템을 도입한 반면 종합병원은 일부 의료기관에서 아직 도입하지 않은 것으로 나타나 의료기관 규모에 따른 도입 격차가 존재하는 것으로 확인되었다.

여섯째, 의료정보시스템 구축 및 운영 현황을 보면 대부분의 의료기관이 전자의무기록시스템, 검사정보시스템(LIS), 약국관리시스템 등 주요 의료정보시스템을 구축하고 있으며, 의료기관 홈페이지 등 환자 대상 정보서비스도 높은 수준으로 운영되고 있는 것으로 나타났다. 다만 개인건강기록(PHR) 시스템이나 모바일 기반 서비스의 도입률은 아직 낮은 수준으로 확인되었다.

일곱째, 의료정보시스템 유지보수 및 운영 방식을 보면 자체 운영보다는 외부 전문기업에 위탁하는 방식의 비중이 높은 것으로 나타났다. 이는 의료기관이 자체 정보기술(IT) 전문 인력을 충분히 확보하지 못하고 외부 서비스에 의존하는 구조임을 보여준다.

여덟째, 정보화 및 정보보안 조직과 인력 운영 현황을 보면 대부분의 의료기관이 정보화 담당 조직을 운영하고 있으나 정보보안 전문 인력은 충분하지 않은 것으로 나타났다. 일부 직무에서는 외부 인력 의존도가 높은 것으로 확인되어 의료기관의 내부 보안 역량 강화 필요성이 제기되었

다. 또한 의료기관 규모에 따라 내부 인력 중심 운영과 외주 활용 구조에 차이가 존재하는 것으로 나타났다.

아홉째, 정보보안 교육 실시 현황을 보면 다수 의료기관에서 일정 수준의 보안 교육을 실시하고 있으나 교육 방식, 참여 수준 및 교육 효과 측면에서는 기관별 차이가 존재하였다. 일부 의료기관에서는 교육이 형식적으로 운영되거나 교육 효과가 충분하지 않다는 의견도 확인되어 체계적인 보안 교육 프로그램의 필요성이 제기되었다.

열째, 정보보호 및 정보보안 정책 체계를 보면 상당수 의료기관이 자체 보안 규정이나 가이드라인을 보유하고 있었으나 규정의 범위와 구체성은 의료기관별로 차이가 존재하였다. 일부 의료기관에서는 보안 정책 체계가 충분히 정비되지 않은 사례도 확인되었다.

열한째, 정보보안 업무 수행 시 애로사항으로는 전문 인력 부족, 예산 부족, 보안 전문성 부족 등이 주요 문제로 나타났다. 특히 중소 규모 의료기관에서는 보안 인력 확보와 예산 확보가 가장 큰 어려움으로 나타났다.

열두째, 보안사고 및 침해사고 대응 역량을 보면 대부분의 의료기관이 사이버 공격 발생 가능성을 높게 인식하고 있었으나 실제 대응 경험이나 대응 역량에는 의료기관 간 차이가 존재하였다. 특히 침해사고 발생 시 대응 과정에서 전문 인력 부족과 대응 경험 부족이 주요 어려움으로 나타났다.

열셋째, 정부 지원 및 정책 개선 요구사항을 보면 보안관제 체계 구축을 위한 재정 지원, 전문 기술 지원 및 교육, 보안 수준 점검 체계, 법적 제도 강화 등이 주요 정책 지원 수요로 제시되었다. 특히 보안관제 체계 구축을 위한 정부의 재정 지원과 기술 지원이 가장 높은 우선순위로 나타났다.

열넷째, 보안관제 체계 도입 및 의료정보보호센터(ISAC) 협력 체계와 관련하여 다수 의료기관이 보안관제 체계 도입의 필요성을 인식하고 있

었으며 의료정보보호센터와의 협력 확대 필요성도 제기되었다. 특히 중소 의료기관의 경우 자체 보안관제 구축이 어려운 만큼 공동 보안관제 또는 클라우드 기반 보안관제 서비스 활용 필요성이 제기되었다.

열다섯째, LLM 기반 인공지능(AI) 서비스 도입과 보안 이슈와 관련하여 일부 의료기관에서 LLM 기반 서비스를 도입하거나 검토하고 있었으며, 이에 따른 개인정보 유출 위험, 데이터 오남용, 보안 취약점 등 새로운 유형의 보안 위험에 대한 우려가 제기되었다. 이는 향후 의료기관의 인공지능(AI) 활용 확대에 대응한 새로운 보안 관리체계 마련의 필요성이 제기되었다.

종합하면 국내 의료기관의 사이버 보안 수준은 일부 대형 의료기관을 중심으로 일정 수준의 관리체계가 구축되어 있으나 다수 의료기관에서는 보안관제 체계, 보안 인증 도입, 보안 예산 확보, 전문 인력 확보 등 핵심 보안 요소가 충분히 확보되지 않은 것으로 나타났다. 특히 의료기관 규모에 따른 보안 투자 격차와 전문 인력 부족 문제는 의료기관 사이버 보안 역량을 제한하는 주요 요인으로 확인되었다. 이에 따라 향후 정책적으로는 의료기관 최소 보안 역량 기준 마련, 보안관제 체계 확대, 중소 의료기관 보안 인프라 지원, 보안 인력 양성 및 교육 강화, 보안 인증제도 활성화, 인공지능(AI) 기반 의료서비스 보안 가이드라인 마련 등 종합적인 정책적 지원이 필요한 것으로 여겨진다.

제6장

결론 및 정책 개선 방안

제6장 결론 및 정책 개선 방안

제1절 결론

의료기관의 디지털 전환은 의료서비스의 질 향상, 환자 중심 진료체계 구축, 데이터 기반 정밀의료 구현 등 긍정적 변화의 촉매 역할을 하고 있다. EMR, PACS, OCS, 원격의료, 디지털 진단보조 인공지능 등은 진료 효율성 향상과 업무 자동화를 통해 의료기관 운영의 패러다임을 근본적으로 변화시키고 있으며, 의료데이터는 이제 임상연구·보험수가·헬스케어 산업 전반의 기반 인프라로 기능한다. 그러나 이러한 혁신은 동시에 새로운 리스크를 불러왔다. 의료기관은 환자 개인정보와 같은 고가치 데이터를 보유하고 있으며, 다크웹에서 금융정보 대비 10~20배 높은 가치를 갖는다는 보고가 있을 만큼 공격자에게 매력적인 표적이 되고 있다. 실제로 국내외 사례는 침해사고가 단순 정보유출을 넘어 생명안전, 진료 연속성, 대국민 신뢰에 영향을 미친다는 점을 보여주었다.

사이버 위협은 단순한 기술 문제가 아니라 의료생태계 전반을 압박하는 구조적 위험으로 진화하고 있다. 랜섬웨어는 의료기관 정보시스템을 암호화하여 진료중단을 초래하고, 사회공학 기반 침입은 내부직원의 판단을 교란하여 광범위한 네트워크 침해의 발판을 제공한다. 무결성 공격은 진단정보를 포함한 환자정보 변조를 야기할 수 있어 의료 현장의 임상적 오류를 유발할 수 있으며, IoT·의료기기 침해는 환자 모니터링·치료기기의 오작동을 유발해 물리적 안전에도 영향을 준다. 또한 최근 글로벌 사이버 범죄 생태계는 '이중·삼중 갈취' 전략을 활용하며, 데이터 유출 후 재협박하거나, 다크웹 재유통을 통해 피해를 확산시키는 경향을 보인다.

이러한 위협은 국가적 차원의 대응체계를 요구하며 기존 보안 수준을 넘어선 전략적 접근이 불가피하다.

정부 역시 의료법 개정을 통해 진료정보 침해사고 통지, 예보·경보, 긴급조치 등을 포함한 행정적 지원근거를 마련해 왔다. 그러나 여전히 많은 부분에서 제도적 공백이 존재한다. 첫째, 예방 중심적 의무가 명확하게 규정되어 있지 않아 반응적(reactive) 보안이 주류를 이루며, 이는 대규모 침해사고 발생 시 비용이 기하급수적으로 증가하는 구조적 한계를 야기한다. 둘째, 침해사고의 범위는 다소 협소하게 정의되어 있으며 데이터 무결성 손상, 시스템 마비, 의료서비스 중단 등은 보다 명확한 법적 근거를 필요로 한다. 셋째, 재발 방지를 위한 행정조치 권한, 과징금 부과 근거 등이 부족하여 사고 반복 가능성을 높인다. 넷째, 사고 보고체계 역시 디지털 전환 수준에 비해 자동화가 부족하며, 실시간 분석·연계 기능이 미흡하다.

본 연구에서 수행한 실태조사는 의료기관의 보안 수준을 다양한 관점에서 검토할 수 있는 실증자료를 제공하였다. 상급종합병원과 종합병원을 대상으로 한 설문은 의료기관 보안정책의 현황, 인력 구성, 침해사고 대응체계, 교육훈련 경험, 공급망 관리 수준 등 다차원적 요소를 포함했다. 응답률이 완전 대표성을 확보하기에는 일부 한계가 있었지만, 의료기관이 일상적으로 겪는 운영적 어려움과 인식 수준을 보여주는 유의미한 데이터를 제공하였다. 설문 결과를 종합하면 다수 기관이 보안예산 확보에 어려움을 겪고 있으며, 전문 인력 채용난, ISAC 참여 저조, 공급망 검증체계 미흡, 교육훈련 부재 등의 문제가 드러났다. 또한 경제적 피해 산정체계가 정형화되지 않아 피해보고의 정확성이 떨어지고 정책 설계의 근거자료 확보에 제약이 발생한다는 점이 확인되었다.

해외 사례 비교는 국내 정책의 미흡점을 더욱 선명하게 보여준다. 미

국, EU, 일본 등은 이미 분야별 정보공유·분석센터(ISAC) 체계를 구축하고, 랜섬웨어를 포함한 보건의료 분야 특화 보안 프레임워크를 운영하고 있으며, 침해사고 데이터를 공유하여 공격 패턴을 국가 단위에서 분석한다. 반면 국내 의료기관은 경험적 대응 수준에 머무르거나 공급망 보안, 의료기기 패치 관리 등 구조적 취약 요소를 체계적으로 관리하지 못하고 있다. 더불어 국제기구(ISO/IEC, ENISA, WHO 등)는 사이버 보안을 정보기밀 뿐 아니라 사회경제적 피해 관리까지 포함하는 확장 개념으로 정의하고 있으며, 이는 의료분야에서 특히 강조되어야 한다.

의료기관의 사이버 보안 역량은 기술적 요소만으로 구축될 수 없다. 정보보안은 조직문화, 예산 우선순위, 전문인력역량, 데이터 거버넌스, 협력 네트워크 등 복합적 요소가 교차하는 분야이다. 의료기관은 진료업무 중심 운영구조로 인해 보안에 대한 투자우선순위가 낮게 형성되는 경향이 있으며, 이러한 구조적 편향은 침해사고 발생 후 소모되는 복구 비용을 고려할 때 비효율적이다. 공격자는 의료기관의 '인적 오류'를 악용하는 사회공학 공격을 선호하며, 이는 기술적 장벽을 우회하는 효과적인 전략이기 때문이다. 따라서 체계적인 교육·훈련의 정례화는 필수적이며, 이를 정책적으로 의무화할 필요가 있다.

의료데이터의 경제적 가치 상승은 의료기관을 대상으로 한 사이버 공격 동기를 강화하고 있다. 또한 의료기기·IoT 장비는 사이버 위협을 확장시키는 중요한 요소다. 장비 수명주기 내 패치정책이 명확하지 않거나 제조사 업데이트가 불규칙한 경우, 의료기관은 심각한 취약성을 상시적으로 내재하게 된다. 따라서 기기에 내재된 소프트웨어의 업데이트 관리 기준, 인증제도, 취약점 모니터링을 하나의 생태계로 구축해야 한다. 공급망 보안 역시 중용성이 더욱 확대되고 있으며, 클라우드 서비스, 외주개발, 원격유지보수 등 다양한 제3자 개입 과정에서 데이터가 확산·조작될

가능성이 존재한다. 계약 기반 보안요구사항 표준화, 협력사 보안평가 및 제재 구조는 필수적이다.

거버넌스 측면에서도 개선이 필요하다. 의료기관 간 정보공유는 위협탐지의 1차적 방어선으로 작동한다. 의료ISAC은 이를 지원하기 위한 조직이지만 가입률은 저조하고 활용도도 낮다. 가입비 경감, 인센티브 도입, 참여등급제 등을 통해 적극적인 참여를 유도할 필요가 있다. 익명화 기반 사고정보 공유는 의료기관의 평판리스크 우려를 완화할 수 있으며, 장기적으로 사이버 보안문화 정착에 기여한다.

인공지능(AI) 기반 위협탐지 기술은 의료현장의 데이터 패턴 특성을 활용해 비정상행위를 조기에 탐지할 수 있으며, 인력부족 문제를 완화하는 기술적 보완장치가 될 수 있다. 다만 인공지능(AI) 적용에는 개인정보 보호 및 모델 학습 데이터 품질이라는 과제가 동반된다. 적대적 공격은 의료 AI 모델의 추론 과정 자체를 교란할 수 있어 장기적으로 임상 안전성에 영향을 줄 수 있다. 따라서 기술적 안전장치뿐 아니라 설명가능성 기반 거버넌스 역시 필요하다.

종합적으로 본 연구는 국내 의료기관 보안 체계의 취약점을 다면적으로 규명하였으며, 침해사고 실태조사, 국내외 사례 검토, 법·제도 분석을 통해 정책적 개선 방향을 도출하였다.

첫째, 의료기관 사이버 보안은 국민 생명·건강에 영향을 미치는 국가적 과제이며, 더 이상 기술적 문제만으로 해석할 수 없다. 둘째, 예방 중심의 법·제도 개편이 무엇보다 중요하며, 사고 발생 후 대응 중심의 현행 구조는 한계가 명확하다. 셋째, 정보공유체계와 전문가 역량 양성은 장기적 보안 생태계 형성의 핵심이다. 넷째, 경제적 피해 산정 모델 구축은 국가 보안투자 효율성 판단의 기준을 마련할 수 있다. 다섯째, 공급망·IoT·AI 등 새로운 공격 벡터에 대응하기 위해 전문성을 갖춘 규제·인증체계가 필

요하다.

향후 정책 추진으로 다음과 같은 전략적 방향을 제시하고자 한다. 우선 단기적으로는 의료ISAC 참여 확대, 보안관제 가입 인센티브 설계, 랜섬웨어 대응 프로토콜 제정과 같은 실무효과가 높은 과제가 우선되어야 한다. 중기적으로는 의료기기·공급망 보안 인증제 구축, 침해사고 자동신고 플랫폼 연계, 보안전문인력 양성 프로그램 제도화가 필요하다. 장기적으로는 법적 예방조치 의무화, 무결성 공격 대응 거버넌스, AI 기반 조기 탐지 시스템 고도화 등 국가단위 보안 생태계 혁신을 추구해야 한다.

궁극적으로 의료분야 사이버 보안은 국민 신뢰, 디지털 헬스케어 산업, 인공지능 기반 의료혁신의 지속가능성을 보장하는 필수요건이다. 선제적이고 균형 있는 정책 개입을 통해 의료기관은 안전한 디지털 전환을 실현할 수 있으며, 사이버 위협이 의료혁신을 제약하는 장애물이 아니라 관리 가능한 위험으로 전환될 때, 국민이 체감하는 의료의 질적 향상은 더욱 뚜렷하게 구현될 것이다.

본 연구의 한계는 다음과 같다. 첫째, 본 연구에서 수행된 의료기관 사이버 보안 실태조사는 대한병원협회의 협조하에 상급종합병원과 종합병원을 대상으로 이루어졌으나, 상급종합병원은 전체 47개소 중 41개소(87.2%), 종합병원은 전체 330개소 중 222개소(67.3%)가 응답하였다. 비록 비교적 높은 응답 비율을 확보하였으나 전체 모집단을 통계적으로 충분히 대표하기에는 한계가 존재한다. 이에 따라 조사 결과를 일반화하는 과정에서 응답편의 및 표본대표성에 관한 유의한 해석적 주의가 요구된다.

둘째, 본 연구는 지역별(17개 시·도), 병상 규모별, 운영 특성별 등 다차원적 세분화를 통한 심층 분석이 가능하였으나, 분석 단위가 세분될 경우 개별 의료기관이 간접적으로 식별될 잠재적 위험이 식별되었다. 이는

연구윤리 측면에서 기관의 비식별성 유지 원칙과 개인정보 보호 요구를 저해할 소지가 있다. 이에 본 연구는 상급종합병원·종합병원 및 도시·비도시 권역 수준에서 결과를 제시하였으며, 이로 인해 미시적 수준의 변인을 반영한 비교분석 범위가 제한되는 연구적 제약이 발생하였다.

셋째, 사이버 보안사고를 경험한 의료기관의 경제적 피해규모를 조사하는 과정에서, 국내 의료환경에는 여전히 표준화된 비용 산정 기준 또는 공식적 평가 프레임워크가 부재한 것으로 확인되었다. 이로 인해 각 의료기관은 피해 규모를 내부 판단 또는 경험적 추정치에 근거하여 응답하는 경향을 보였으며, 이러한 임의적 산정 방식은 피해 금액의 신뢰도, 타당성, 기관 간 비교가능성을 저해하는 요인으로 작용하였다. 나아가 이러한 제약은 사이버 보안사고의 사회·경제적 영향 평가, 정책적 대응 우선순위 설정, 보험·보상체계 설계 등 후속 연구 및 제도적 논의를 제한할 수 있다. 따라서 의료기관 사이버 보안사고의 경제적 피해를 객관적·정량적으로 평가할 수 있는 체계적 산정방법론 개발과 후속 연구가 시급히 요구된다.

제2절 정책 개선 방안

1. 법·제도 기반 정비 및 규제 개선

가. 진료정보 침해사고 사전 예방 의무 명문화

「의료법」 제23조의3에서는 진료정보 침해사고 발생 시 의료기관의 즉각적인 통지 의무를 규정하고 있으나, 침해사고 발생 이전 단계에서의 예방조치에 대해서는 명확한 규정이 마련되어 있지 않다. 이러한 제도 구조는 의료기관의 정보보안 관리가 사전 예방보다는 침해사고 발생 이후 대응 중심으로 운영되는 경향을 강화할 가능성이 있으며, 결과적으로 정보보안 투자와 관리의 효율성을 저해하는 요인으로 작용할 수 있다.

이에 의료기관이 준수해야 할 최소한의 정보보안 관리 기준을 법령 또는 하위 지침을 통해 구체화하는 방안을 검토할 필요가 있다. 예를 들어 취약점 점검, 접근통제 강화, 데이터 암호화, 보안 로그 관리, 계정 관리, 백업 관리, 보안관제 운영 등 기본적인 관리적·기술적 보호조치를 의료기관 정보보안 관리 기준에 포함하는 방안을 고려할 수 있다. 이러한 기준은 의료기관의 규모와 정보보안 역량을 고려하여 단계적으로 적용하는 방식이 현실적인 정책 대안으로 여겨진다.

정책 추진 과정에서는 환자 안전 확보, 의료서비스 연속성 유지, 국가보건안보 강화 등 공익적 목적과 정책 추진의 필요성을 함께 제시할 필요가 있다. 이를 통해 정보보안 관리 기준이 단순한 규제가 아니라 의료서비스 안정성과 공공성을 유지하기 위한 제도적 장치라는 점을 명확히 할 수 있을 것으로 기대된다.

제도의 실효성을 높이기 위해 위반 시 개선명령, 행정지도, 시정조치

등 관리 수단을 포함한 제도적 관리체계를 함께 마련하는 방안도 검토될 수 있다. 이러한 사전 예방 중심의 정보보안 관리 기준이 관련 법령에 반영될 경우 침해사고 발생 가능성과 피해 규모를 감소시키는 효과가 기대되며, 향후 의료기관 내 정보보안 관리체계와 보안 문화 정착을 촉진하는 기반으로 활용될 수 있을 것으로 여겨진다.

나. 진료정보 침해사고 범위 확대

「의료법 시행령」 제10조의11에서는 진료정보 침해사고를 진료정보의 도난·유출·파기·손상·은닉·멸실과 전자의무기록시스템의 교란·마비 등으로 규정하고 있다. 그러나 이러한 정의는 주로 정보 유출이나 시스템 장애 중심으로 구성되어 있어 데이터 무결성 손상, 시스템 가용성 저하, 의료서비스 중단 등과 같은 다양한 사이버 위협 유형은 상대적으로 제한적으로 해석될 가능성이 있다.

실제 의료현장에서는 데이터 변조와 같은 무결성 공격이 임상적 판단 오류를 유발할 수 있으며, 시스템 가용성 공격은 진료 지연, 수술 일정 변경, 환자 전원 조치 등 의료서비스 운영에 직접적인 영향을 미칠 수 있다. 특히 랜섬웨어 공격 등은 정보 암호화와 시스템 마비를 동시에 유발하여 의료서비스의 연속성을 위협하는 사례로 보고되고 있다. 이러한 특성을 고려할 때 의료분야 사이버 위협은 단순한 정보 유출을 넘어 의료서비스 안정성과 환자 안전에도 영향을 미칠 수 있는 요소로 인식될 필요가 있다.

이에 따라 진료정보 침해사고의 정의를 데이터 삭제·변조·암호화, 시스템 가용성 저하, 의료서비스 중단, 의료기기 오작동 등 다양한 사이버 위협 유형을 포함하는 방향으로 확대하는 방안을 검토할 필요가 있다. 이러한 정의 확대는 개인정보보호법 및 정보통신망법 등 관련 법령에서 규

정하고 있는 침해사고 개념과의 정합성을 고려하여 추진될 필요가 있다.

침해사고 범위를 보다 명확하게 규정할 경우 사고 유형에 대한 정책 대응 기준을 구체화하고 의료기관의 보안 관리 범위를 명확히 하는 데 도움이 될 것으로 기대된다. 또한 사이버 침해사고에 대한 통계 관리와 정책 대응 체계를 보다 체계적으로 구축하는 기반으로 활용될 수 있을 것으로 여겨진다.

다. 재발방지 명령 및 과징금 근거 마련

침해사고가 반복적으로 발생하는 경우 이는 기관 내 구조적 보안 취약점이 지속되거나 정보보안 관리체계가 충분히 작동하지 못하고 있음을 보여주는 신호로 볼 수 있다. 이러한 상황에서는 침해사고의 재발을 방지하기 위한 제도적 관리 장치를 강화할 필요가 있다.

이에 침해사고 재발 방지를 위한 명령과 과징금 부과의 법적 근거를 마련하고, 사고 원인 분석 및 재발방지 개선계획 제출을 의무화하는 방안을 검토할 필요가 있다. 이러한 제도는 의료기관이 침해사고 이후 단순한 복구에 그치지 않고 보안 취약점 개선과 관리체계 정비를 체계적으로 수행하도록 유도하는 장치로 활용될 수 있을 것으로 기대된다.

최근 통신·플랫폼 분야의 대규모 침해사고를 계기로 사고 미신고, 조사 협조 미흡, 정보 은폐 논란 등이 사회적 문제로 제기되면서 사고조사 협조 의무와 제재 강화 필요성도 확대되고 있다. 이러한 입법 흐름을 고려하여 의료법에서도 침해사고 발생 시 자료 제출, 현장조사 협조, 재발방지 계획 수립 등 조사 협조 의무를 명확히 규정하는 방안을 검토할 필요가 있다.

다만 중소 규모 의료기관의 부담을 고려하여 제도의 단계적 적용, 과징

금 차등 부과 기준 마련, 행정적 지원 프로그램 연계 등을 병행하는 정책 접근이 필요할 것으로 여겨진다. 피해자 보호 측면에서는 개인정보보호법상 징벌적 손해배상 제도와의 정합성도 함께 검토될 필요가 있다.

이러한 제도적 장치는 의료기관의 침해사고 예방 및 대응 역량을 강화하고 보건의료 분야 전반의 사이버 위험 수준을 체계적으로 낮추는 데 기여할 것으로 기대된다. 또한 의료기관의 정보보안 관리체계 개선을 유도하고 사이버 침해사고 대응 거버넌스를 강화하는 기반으로 활용될 수 있을 것으로 여겨진다.

라. 정기적인 의료기관 사이버 실태조사 실시

의료기관을 대상으로 한 사이버 보안 실태조사는 의료기관의 보안 역량 수준, 위협 환경의 변화, 정책적 지원 수요 등을 체계적으로 파악하기 위한 중요한 기초자료로 활용될 수 있다. 현재 개인정보보호 실태점검, 정보보호 관리체계(ISMS) 인증 심사, 의료기관 인증평가 등 일부 관련 점검 제도가 운영되고 있으나, 의료분야 사이버 보안 수준을 종합적으로 파악할 수 있는 전국 단위의 정례적 조사체계는 제한적인 상황이다. 이러한 한계로 인해 의료기관 보안 수준의 전반적 현황을 파악하거나 정책적 지원 필요성을 체계적으로 분석하는 데 일정한 제약이 존재한다.

이에 의료기관 규모, 병상 수, 의료기기 도입 및 운용 환경, 외주 정보시스템 의존도 등 다양한 특성을 고려한 의료분야 특화 사이버 보안 실태조사 체계를 구축하는 방안을 검토할 필요가 있다. 이러한 조사는 기존 점검·인증 제도와 연계하여 운영할 경우 조사 부담을 최소화하면서도 정책 활용도를 높일 수 있을 것으로 여겨진다.

정기적인 실태조사는 의료기관의 보안 조직 및 전문 인력 확보 수준,

침해사고 대응 역량, 위험관리 및 통제 체계, 교육·훈련 수행 여부, 공급망 보안 관리 수준, AI 및 IoT 기반 기술 도입 현황 등 주요 요소를 지속적으로 점검·분석하는 기능을 수행할 수 있다. 이를 통해 의료기관 간 보안 역량 격차를 객관적으로 파악하고 국가 차원의 지원 정책 우선순위 설정, 규제 정책 운영 전략 수립, 정보보안 정책 로드맵 마련을 위한 계량적 근거를 제공할 수 있을 것으로 기대된다. 또한 반복 조사에 따른 시계열 데이터 축적은 정책 효과를 점검하고 개선 방향을 도출하기 위한 모니터링 및 피드백 체계 구축에도 활용될 수 있다.

실태조사 주기는 의료기술 확산 속도와 사이버 공격 기법 변화 등을 고려하여 1~2년 주기로 운영하는 방안을 검토할 수 있다. 조사 결과는 보건의료 정책 수립, 예산 편성, 위험 평가 등 다양한 정책 영역에서 활용될 수 있으며, 조사 결과를 기반으로 한 보안 수준 지표화는 의료기관의 자발적인 정보보안 역량 강화 노력에도 긍정적인 영향을 줄 것으로 기대된다. 또한 이러한 지표를 정보보호 인증제도나 재정 지원 정책과 연계할 경우 정책 추진의 실효성을 높이는 데 도움이 될 수 있을 것으로 여겨진다.

정기적인 실태조사 체계 구축은 의료분야 사이버 보안 거버넌스를 강화하고 위협 대응을 위한 공공자원의 효율적 배분 기반을 마련하는 데 기여할 수 있다. 또한 정책 개입 시점의 적시성을 높이고 국가 보건안보 차원의 보안 데이터 기반을 구축하는 데에도 중요한 역할을 수행할 수 있을 것으로 기대된다. 나아가 이러한 조사 체계는 단순한 현황 파악을 넘어 의료기관의 회복탄력성과 사이버 보안 종합 역량을 지속적으로 강화하기 위한 지표 기반 정책 관리체계 구축의 기반으로 활용될 수 있을 것으로 여겨진다.

마. 병원 규모별 맞춤형 보안 가이드 마련

중소규모 의료기관은 인력과 예산 측면에서 구조적 제약이 존재하여 대형 의료기관과 동일한 수준의 정보보안 기준을 일률적으로 적용하는 데에는 현실적인 한계가 있다. 특히 병원급 의료기관의 경우 정보보안 전담 인력을 별도로 확보하지 못한 사례가 많아 보안 관리체계 구축과 운영에 어려움이 나타나는 경우가 있다. 이러한 특성을 고려할 때 의료기관의 규모와 보안 역량을 반영한 위험 기반 접근(risk-based approach)을 적용하여 규모별 정보보안 관리 가이드를 마련할 필요가 있다.

우선 의료기관이 반드시 보호해야 할 핵심 정보자산을 중심으로 필수적인 보호요건을 정의하고, 이를 의료기관이 쉽게 적용할 수 있도록 체크리스트 기반의 보안 관리 가이드를 제공하는 방안을 검토할 수 있다. 이러한 가이드는 상급종합병원, 종합병원, 병원급 의료기관 등 규모별 운영 환경을 고려하여 차등화된 형태로 제시될 경우 현장 적용성이 높아질 것으로 기대된다.

또한 정부 차원의 표준 관리 템플릿을 제공할 경우 의료기관의 행정 문서 작성 부담을 완화하고 보안 관리체계 운영 현황을 보다 체계적으로 점검할 수 있는 기반을 마련할 수 있다. 아울러 의료기관 인증평가, 개인정보 보호 점검 등 기존 제도와의 연계를 통해 가이드 활용도를 높이는 방안도 함께 검토될 필요가 있다.

제도의 단계적 적용은 의료기관의 정책 수용성을 높이고 자발적인 참여를 유도하는 데 도움이 될 수 있다. 동시에 간이 보안 진단 도구를 개발·보급할 경우 의료기관이 자체적으로 취약점을 점검하고 관리할 수 있는 기반을 제공할 수 있을 것으로 기대된다.

이와 같은 차별화된 정책 접근은 중소규모 의료기관의 정보보안 관리

역량을 강화하는 동시에 국가 의료체계 전반의 사이버 보안 수준을 균형 있게 향상시키는 데 기여할 수 있을 것으로 여겨진다.

2. 기술·인프라 기반 보안역량 강화

가. 보안관제서비스 가입 인센티브 부여

보안관제서비스 가입률은 상급종합병원 약 60%, 종합병원 약 7.1% 수준으로 나타나(한국사회보장정보원, 2025) 의료기관 간 보안관제 활용 격차가 크게 존재하는 것으로 확인된다. 이러한 결과는 종합병원을 중심으로 사이버 위협에 대한 탐지 및 대응 역량이 충분히 확보되지 못하고 있을 가능성을 보여준다. 이에 따라 보안관제서비스 참여 확대를 위해 의료기관 평가 가점 부여, 국가 인증제도와의 연계 등 인센티브 기반 정책을 검토할 필요가 있다. 또한 병원급 의료기관을 대상으로 한 보안관제 참여 확대 방안은 향후 단계적으로 검토될 수 있을 것으로 여겨진다.

예를 들어 현행 의료기관 평가인증제도에서는 개인정보 보호 및 환자정보 관리 관련 항목이 일부 포함되어 있으나, 보안관제 운영, 정기적인 취약점 점검, 침해사고 대응체계 구축 등 사이버보안 운영 수준을 평가하는 지표는 제한적으로 반영되어 있는 상황이다. 이에 따라 의료기관 평가인증 지표에 정보보안 관리체계 구축 여부, 보안관제 운영 여부, 취약점 점검 수행 여부 등을 단계적으로 반영하고 이를 평가 가점과 연계하는 방안을 검토할 필요가 있다. 이러한 제도 개선은 의료기관의 자발적인 정보보안 투자와 보안관리 수준 향상을 유도하는 정책적 인센티브로 기능할 수 있을 것으로 기대된다.

또한 보안관제센터에서 축적되는 관제 데이터는 국가 차원의 위협 인

텔리전스 분석 역량을 강화하는 기반으로 활용될 수 있으며, 공격 패턴 및 관제 이벤트 정보를 활용한 정책 설계에도 활용 가능성이 있다. 인센티브 중심의 정책 접근은 의료기관의 제도 수용성을 높이면서도 규제 부담을 최소화할 수 있는 정책 수단으로 활용될 수 있을 것으로 여겨진다. 나아가 이러한 정책은 의료정보공유·분석센터(Medical ISAC)를 중심으로 한 위협정보 공유 체계와 연계될 경우 데이터 기반 사이버 위협 대응 역량을 강화하는 기반으로 활용될 수 있을 것으로 기대된다.

나. 의료기기·IoT 보안 인증체계 강화

초연결사회의 도래로 의료기기 및 IoT 기반 장비는 의료현장에서 진료 및 환자 모니터링 등 핵심 인프라로 활용되고 있으며, 보안 취약점 발생 시 환자 안전과 임상 업무에 직접적인 영향을 미칠 수 있다. 최근 의료기기의 네트워크 연결과 원격 관리 기능이 확대되면서 의료기기 보안은 의료기관 사이버 보안 관리의 중요한 요소로 부각되고 있다. 현재 국내에서는 식품의약품안전처가 「의료기기 사이버보안 가이드라인」을 통해 보안 설계 및 취약점 관리 등을 권고하고 있으나, 의료기기 보안 관리체계는 여전히 권고 중심으로 운영되고 있어 보다 체계적인 관리 기준 마련이 요구된다.

이에 의료기기 제조 및 운영 단계에서 보안 요구사항을 강화하고, 의료기기 수명주기를 고려한 보안 관리체계를 마련할 필요가 있다. 특히 패치 관리 정책, 소프트웨어 업데이트 관리, 취약점 보고 체계 등 기본적인 보안 관리 기준을 제도적으로 명확히 하고, 필요 시 기존 IoT 보안 인증제도와의 연계를 검토할 필요가 있다.

또한 의료기관이 의료기기 및 IoT 장비를 도입하는 과정에서 보안 인

증 여부 또는 보안 관리 수준을 구매 평가에 반영할 경우 제조사의 보안 투자 확대와 시장 경쟁을 통한 보안 수준 향상을 유도할 수 있다. 이러한 접근은 규제 중심 정책보다는 시장 메커니즘을 활용하여 보안 수준을 높이는 정책 수단으로 활용될 수 있다.

의료기기 보안 인증체계를 도입할 경우 산업계 부담을 고려하여 단계적 적용 방식을 검토할 필요가 있으며, 인증 심사와 기술 검증을 수행할 수 있는 전문 인력 확보도 제도 운영의 중요한 요소로 작용한다.

장기적으로는 의료기기 소프트웨어 구성요소 관리, 취약점 정보 공유, 보안 업데이트 체계 등을 포함한 의료기기 사이버보안 관리체계를 강화함으로써 의료기기 및 IoT 장비로 인한 사이버 공격 표면을 구조적으로 감소시키는 정책 기반을 마련할 수 있을 것으로 기대된다.

다. 의료기관 공급망 보안 관리체계 강화

초연결 사회의 확산과 함께 의료기기 및 IoT 기반 장비는 진료 지원, 환자 모니터링, 의료정보 수집 등 의료현장의 핵심 인프라로 활용되고 있다. 이러한 장비에서 보안 취약점이 발생할 경우 환자 안전과 임상 업무에 직접적인 영향을 미칠 수 있어 의료기기 보안은 의료기관 사이버보안 관리의 중요한 요소로 인식되고 있다. 최근 의료기기의 네트워크 연결과 원격 관리 기능이 확대되면서 의료기기 및 IoT 장비를 통한 사이버 공격 가능성도 점차 증가하고 있는 상황이다.

현재 국내에서는 식품의약품안전처가 「의료기기 사이버보안 가이드라인」을 통해 보안 설계, 취약점 관리, 소프트웨어 업데이트 관리 등 의료기기 보안 관리 방향을 제시하고 있다. 다만 이러한 제도는 권고 중심으로 운영되고 있어 의료기기 보안 관리 기준을 보다 체계적으로 운영하기 위

한 정책적 보완 필요성이 제기되고 있다.

이에 의료기기 제조 단계와 의료기관 운영 단계를 모두 고려한 의료기기 사이버보안 관리체계 강화 방안을 검토할 필요가 있다. 특히 패치 관리 정책, 소프트웨어 업데이트 관리, 취약점 보고 체계 등 기본적인 보안 관리 기준을 보다 명확히 하고, 필요 시 기존 IoT 보안 인증제도와의 연계 가능성도 함께 검토할 수 있을 것으로 여겨진다.

또한 의료기관이 의료기기 및 IoT 장비를 도입하는 과정에서 보안 인증 여부 또는 보안 관리 수준을 구매 평가 기준에 반영할 경우 제조사의 보안 투자 확대와 시장 경쟁을 통한 보안 수준 향상을 유도할 수 있을 것으로 기대된다. 이러한 접근은 규제 중심 정책보다는 시장 메커니즘을 활용하여 의료기기 보안 수준을 향상시키는 정책 수단으로 활용될 수 있을 것으로 여겨진다.

라. AI 기반 위협탐지·침해대응 적용 가이드 마련

최근 사이버 공격이 지능화·자동화되는 추세에 따라 AI 기반 위협탐지 기술을 활용한 보안 대응 체계의 필요성이 확대되고 있다. 특히 의료기관은 방대한 의료데이터와 복잡한 정보시스템 환경을 운영하고 있어 이상행위 탐지, 위협 패턴 분석, 보안 이벤트 자동 분석 등 AI 기반 보안 기술을 활용할 경우 침해사고 탐지 및 대응 역량을 강화하는 데 도움이 될 수 있다. 또한 보안 전문 인력 부족 문제를 보완하는 수단으로 활용될 가능성도 제기되고 있다.

다만 AI 기반 탐지 시스템은 알고리즘 오탐(false positive) 및 과소탐지(false negative) 가능성이 존재하므로 의료 환경에서의 안정적 활용을 위해 오탐 관리 기준과 모델 신뢰도 평가 체계를 마련할 필요가 있다.

특히 AI 탐지 결과가 진료정보시스템 운영이나 의료서비스 환경에 영향을 미칠 수 있다는 점을 고려하여 AI 탐지 결과에 대한 보안 담당자의 검증 절차 등 운영 기준을 함께 마련할 필요가 있다.

또한 AI 모델 학습에 활용되는 데이터의 품질 관리 기준과 개인정보 보호를 위한 비식별화 또는 가명정보 처리 기준을 명확히 제시할 필요가 있다. 의료정보공유·분석센터(의료ISAC) 등 위협정보 공유 체계를 통해 축적된 침해사고 사례 및 위협정보를 활용할 경우 AI 기반 탐지 모델의 실효성을 높이는 데 활용될 수 있을 것으로 기대된다.

마. 랜섬웨어 대응 표준 프로토콜 개발

랜섬웨어는 최근 의료기관을 대상으로 한 사이버 공격 가운데 가장 큰 피해를 유발하는 유형으로, 정보시스템 마비로 인한 진료 지연, 환자 전원 조치, 의료서비스 중단 등 환자 안전과 의료기관 운영에 직접적인 영향을 미칠 수 있다. 특히 의료기관은 전자의무기록(EMR), 영상정보시스템(PACS) 등 핵심 진료시스템에 대한 의존도가 높아 랜섬웨어 공격 발생 시 피해 규모가 확대될 가능성이 있다.

이에 따라 의료기관이 랜섬웨어 공격에 신속하게 대응할 수 있도록 암호화 차단, 네트워크 격리, 시스템 복구 및 백업 복원 절차 등 단계별 대응 절차를 포함한 표준 대응 프로토콜을 마련할 필요가 있다. 또한 의료정보시스템과 일반 업무망 간 네트워크 분리, 중요 시스템 접근 통제 강화, 백업 데이터의 분리 보관 및 무결성 관리 등 기본적인 보안 관리 기준을 함께 포함하는 것이 중요하다.

침해사고 발생 시 신속한 대응을 위해 침해사고 신고 절차 및 경보 전달 체계를 표준화하고 의료기관 간 위협정보 공유 체계를 강화하는 방안

도 함께 고려될 필요가 있다. 특히 의료정보공유·분석센터(Medical ISAC) 등 관련 기관과의 협력 체계를 통해 랜섬웨어 공격 징후를 조기에 인지하고 피해 확산을 방지할 수 있는 대응 기반을 마련할 필요가 있다.

또한 의료기관의 실제 대응 역량 강화를 위해 랜섬웨어 대응 시나리오 기반 모의훈련 및 대응 훈련 프로그램을 병행 운영하는 방안도 고려해 볼 수 있다. 이러한 대응 체계는 의료기관 구성원의 대응 능력을 향상시키고 침해사고 발생 시 초기 대응 시간을 단축하는 데 도움이 될 것으로 기대된다.

향후 국가 차원의 의료기관 랜섬웨어 대응 표준 프로토콜을 마련할 경우 의료기관 간 대응 수준의 편차를 완화하고 보건의료 분야 전반의 사이버 위협 대응 역량을 체계적으로 강화하는 기반으로 활용될 수 있을 것으로 여겨진다.

3. 거버넌스·정보공유 및 사고대응 체계 강화

가. 의료ISAC 참여 확대 전략 수립

의료ISAC는 의료기관 간 위협정보 공유를 통해 사이버 공격에 대한 탐지 및 대응 속도를 높이는 핵심 협력 체계로 기능한다. 그러나 현재 의료기관의 참여 수준은 제한적인 상황이며 참여기관 간 정보 공유 활성화에도 일정한 제약이 존재하여 국가 차원의 위협 대응 역량 확보에 한계가 나타나고 있다.

이에 따라 의료ISAC 참여 확대를 위한 정책적 지원 방안을 마련할 필요가 있다. 참여기관 확대를 위해 참여 인센티브 제공, 기관 규모를 고려한 참여 모델 마련, 정보 공유 부담을 완화할 수 있는 제도적 장치 도입 등

이 검토될 수 있다. 침해사고 정보를 익명화하여 공유하는 체계를 구축할 경우 의료기관의 참여 부담을 완화하고 위협정보 공유 활성화에도 도움이 될 것으로 여겨진다.

위협정보의 신뢰성과 활용도를 높이기 위해 공격 유형, 취약점 정보, 대응 사례 등에 대한 표준화된 정보 수집 및 공유 체계를 구축하는 방안도 필요하다. 이러한 체계는 의료기관 보안관제센터 또는 침해사고 대응 조직과 연계될 경우 위협정보 활용도를 높이는 데 기여할 수 있을 것으로 기대된다.

국제 ISAC 네트워크와의 협력 확대를 통해 글로벌 사이버 위협 정보를 신속하게 확보하고 이를 국내 의료기관과 공유하는 체계를 강화하는 방안도 고려될 수 있다. 의료기관 보안 담당자 간 전문 포럼 및 실무 협의체 운영은 위협 대응 경험 공유와 보안 역량 강화에 기여할 것으로 여겨진다.

향후 의료ISAC은 의료분야 위협 인텔리전스 체계의 핵심 인프라로 기능하며 의료기관 간 정보 공유와 공동 대응 역량을 강화하는 기반으로 활용될 수 있을 것으로 기대된다.

나. 침해사고 신고체계 자동화 플랫폼 구축

현재 의료기관의 침해사고 신고 절차는 기관별로 분산되어 있고 수작업 중심으로 처리되는 경우가 많아 신고 지연이나 정보 공유의 한계가 발생할 가능성이 존재한다. 침해사고 발생 시 관계기관 보고, 대응 절차 안내, 위협정보 공유 등이 동시에 이루어져야 하지만 이를 체계적으로 관리할 수 있는 통합 시스템은 충분히 구축되어 있지 않은 상황이다.

이러한 한계를 개선하기 위해 의료기관 침해사고 신고와 대응 과정을 통합적으로 관리할 수 있는 통합 신고·대응 플랫폼 구축을 검토할 필요가

있다. 해당 플랫폼은 침해사고 신고 접수, 사고 유형 분류, 대응 절차 안내, 관계기관 전파 등 주요 기능을 통합적으로 지원하여 신고 및 대응 절차의 신속성을 높이는 데 기여할 수 있을 것으로 기대된다.

플랫폼 내에 상황판(dashboard)을 구축할 경우 침해사고 발생 현황, 공격 유형, 위협 집중도 등을 실시간으로 파악할 수 있어 국가 차원의 사이버 위협 대응 상황을 보다 효과적으로 관리할 수 있을 것으로 여겨진다. 이러한 정보는 보건의료 분야 사이버 위협 동향 분석과 정책 수립을 위한 기초자료로 활용될 수 있다.

침해사고 정보를 비식별화하여 공유하는 체계와 보고서 자동 생성 기능을 도입할 경우 의료기관의 행정 부담을 완화하고 신고 절차의 효율성을 높이는 효과도 기대된다. 해당 플랫폼이 보안관제센터 및 의료ISAC과 연계되어 운영될 경우 의료기관 간 정보 공유와 공동 대응 역량을 강화하는 기반으로 활용될 수 있을 것으로 여겨진다.

다. 의료분야 보안전문인력 양성 프로그램 운영

의료기관은 전자의무기록(EMR), 의료영상저장전송시스템(PACS), 의료기기 네트워크 등 의료 분야에 특화된 정보시스템을 운영하고 있어 일반 정보보안 인력뿐 아니라 의료 환경에 대한 이해를 갖춘 전문 인력 확보가 중요하다. 그러나 현재 의료기관에서는 보안 전문 인력 수급이 제한적이며 특히 중소 규모 의료기관에서는 보안 전담 인력을 확보하는 데 어려움이 있는 상황이다.

이에 따라 의료환경 특성을 반영한 의료분야 사이버보안 전문인력 양성 프로그램 운영이 필요할 것으로 여겨진다. 국가 차원의 교육과정 개발을 통해 의료정보시스템 보안, 의료기기 및 IoT 보안, 개인정보 보호, 침

해사고 대응 등 의료 특화 보안 역량을 강화할 수 있는 교육 체계를 마련하는 방안이 고려될 수 있다.

기존 정보보안 교육기관 등과 연계하여 의료분야 보안 전문교육 과정을 확대하고 의료기관 보안 담당자 간 협력 네트워크와 교육 프로그램을 운영할 경우 보안 대응 경험과 실무 지식 공유에도 도움이 될 것으로 기대된다.

한편 AI 및 IoT 기반 기술 확산에 대응하여 의료기기 보안, 디지털 헬스 기술 보안 등 미래 위협 대응 역량을 강화하는 교육 과정도 단계적으로 확대될 필요가 있다. 이러한 전문 인력 양성 정책은 의료기관의 보안 대응 역량을 강화하고 보건의료 분야 전반의 사이버 보안 수준 향상에 기여할 것으로 기대된다.

라. 보안 교육 및 훈련 정례화

사회공학 공격은 이메일 피싱, 계정 탈취 등 인적 요인의 취약성을 악용하는 대표적인 사이버 공격 유형으로 의료기관의 정보보안 사고에서도 주요 원인으로 지적되고 있다. 이에 따라 의료기관 구성원의 보안 인식 제고와 대응 역량 강화를 위해 정기적인 정보보안 교육 및 훈련 체계를 운영할 필요가 있다.

현재 일부 의료기관에서는 개인정보 보호 및 정보보안 교육이 실시되고 있으나 교육 내용과 방식, 참여 수준에는 기관 간 차이가 존재한다. 기존 교육 체계를 기반으로 시나리오 기반 교육과 실제 침해사고 사례 및 공격 로그를 활용한 교육 콘텐츠를 확대할 경우 교육의 실효성이 높아질 것으로 여겨진다.

전 직원 대상 기본 교육과 함께 정보보안 담당자 및 관리자 대상 심화

교육 과정을 운영할 경우 침해사고 대응 및 보안 관리 역량 강화에도 도움이 될 것으로 기대된다. 온라인 교육 플랫폼을 활용할 경우 교육 접근성을 높이고 교육 운영 비용을 절감하는 효과도 기대된다.

교육 이수 현황과 학습 데이터를 체계적으로 관리할 경우 정책 수립과 교육 프로그램 개선을 위한 기초자료로 활용될 수 있다. 이러한 정기적인 보안 교육 및 훈련 체계는 조직 내 보안 문화 정착과 의료기관 사이버 대응 역량 강화에 기여할 것으로 여겨진다.

마. 의료기관 사이버 침해사고 경제적 피해 산정모델 개발

의료기관의 사이버 침해사고는 환자의 민감한 개인정보 보호에 위협이 될 뿐 아니라 시스템 복구 비용, 의료서비스 중단, 환자 전원 조치, 평판 하락 등 다양한 형태의 직·간접적 경제적 피해를 발생시킬 수 있다. 이러한 피해 규모는 의료기관의 정보보호 및 정보보안 투자 의사결정에 중요한 영향을 미치는 요소이다.

그러나 현재 의료기관의 침해사고 피해 규모는 기관별 임의 판단에 의해 보고되는 경우가 많아 객관성, 비교 가능성, 정책 활용성이 낮은 한계가 있다. 특히 의료기관은 침해사고 발생 시 의료서비스 정상화를 우선적으로 추진해야 하는 특성으로 인해 사고 이후 피해 규모를 체계적으로 산정하는 과정이 충분히 이루어지지 않는 경우가 많다. 또한 평판 하락이나 법적 책임 문제 등을 고려하여 피해 규모가 축소되거나 정확하게 보고되지 않는 사례도 발생할 수 있다.

이에 따라 의료기관 사이버 침해사고로 인한 경제적 피해를 체계적으로 산정할 수 있는 표준화된 피해 산정모델 개발을 검토할 필요가 있다. 해당 모델은 시스템 복구 비용, 서비스 중단에 따른 운영 손실, 개인정보

유출 대응 비용, 평판 손실 등 다양한 피해 요소를 포함하여 의료기관 특성을 반영한 피해 산정 기준을 마련하는 방향으로 설계할 수 있다.

이와 같은 피해 산정모델은 의료기관의 사이버 위험 수준을 보다 명확하게 인식할 수 있도록 하고, 정보보안 투자 의사결정 및 정책 지원 필요성을 판단하는 기초자료로 활용될 수 있다. 또한 국가 차원에서 의료분야 사이버 침해사고 피해 규모를 분석하고 보안 정책의 우선순위를 설정하는 데에도 활용될 수 있다.

참고문헌

[1장]

국정기획위원회. (2025). 이재명정부 국정운영 4개년 계획(안).

김병규. (2023.9.14.). 3년반 동안 의료기관서 해킹 등 사이버 침해사고 74건 발생. 연합뉴스. https://www.yna.co.kr/view/AKR20230914067000530

박은주. (2023.5.10.). 2021년 서울대병원 해킹·개인정보 유출사건, 북한 소행으로 드러났다. 보안뉴스. https://m.boannews.com/html/detail.html?idx=117945

의료법, 법률 제18289호 (2025).

의료법 시행령, 대통령령 제33629호 (2025).

의료법 시행규칙, 보건복지부령 제970호 (2025).

한국사회보장정보원. (2025). 의료정보보호센터 내부 자료

Abed, S. F., Allain-Ioos, 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

California Department of Public Health. (2021). Scripps Health Ransomware Incident Report. Sacramento, CA: CDPH.

ENISA. (2023). ENISA Threat LANDSCAPE: HEALTH SECTOR. European Union Agency for Cybersecurity.

National Audit Office. (2018). Investigation: WannaCry Cyber Attack and the NHS. London: NAO.

Ponemon Institute. (2023). Cost of a Data Breach Report 2023: Healthcare Industry Findings. IBM Security, pp.7–9.

Sutherland, E., Keelara, R., Eiszele, S., & Haugrud, J. (2023). FAST-TRACK ON DIGITAL SECURITY IN HEALTH. OECD Health Working Papers(164).

[2장]

과학기술정보통신부. (2025.7.4. 보도자료). SK텔레콤 침해사고 최종 조사결과 발표

금융보안원 홈페이지(https://www.fsec.or.kr/bbs/101)

뉴시스 조현아 기자(2025.07.09.). "계정 해킹됐어요" 그 문자가 '스미싱'…카카오뱅크, AI로 잡아낸다.
https://www.newsis.com/view/NISX20250709_0003244926

미국 정보공유·분석센터(ISAC) 국가협의회 홈페이지.
https://www.nationalisacs.org/members

의료법 시행규칙, 보건복지부령 제970호 (2025).

의료법, 법률 제18289호 (2025)

의료정보보호센터. (2025). 의료정보보호센터 홈페이지.
https://www.hisc.or.kr/main/main.do

이승덕. (2024, 10월 3일). 의료기관 해킹 등 사이버 침해사고 200건 넘어. 의학신문.

정보통신기반 보호법. (법률 제20068호. 2024. 1. 23., 일부개정)

한국사회보장정보원. (2025). 한국사회보장정보원 홈페이지. 2025.11.2. 인출.
https://www.ssis.or.kr/lay1/S1T748C1588/contents.do

한국인터넷진흥원. (2025a). 2025년 상반기 사이버 위협 동향 보고서.

한국인터넷진흥원. (2025b). 피싱 KISA에 신고하세요.
https://www.boho.or.kr/kr/bbs/view.do?searchCnd=1&bbsId=B0000127&searchWrd=&menu No=205021& pageIndex=1&categoryCode=&nttId=71822

한국인터넷진흥원. (2025c). 중소기업 침해사고 피해지원 서비스 동향 보고서

(2025년 상반기)-기업 타깃형 스피어 피싱 사례 및 대응방안.

Alodaynan, A. M., & Alanazi, A. A. (2021). A survey of cybersecurity vulnerabilities in healthcare systems. International Journal of Advanced and Applied Sciences, 8(12), 48-55.

Appari, A., & Johnson, M. E. (2010). Information security and privacy in healthcare: current state of research. International journal of Internet and enterprise management, 6(4), 279-314.

Bada, M., & Nurse, J. R. (2019). Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (SMEs). Information & Computer Security, 27(3), 393-410.

Borky, J. M., & Bradley, T. H. (2018). Protecting information with cybersecurity. In Effective model-based systems engineering (pp. 345-404). Cham: Springer International Publishing.

Cheswick, William; Bellovin, Steven M. (1994). Firewalls and Internet Security: Repelling The Wily Hacker. Addison Wesley. ISBN 978-0-201-63357-3.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. Technology innovation management review, 4(10).

ENISA. (2022a). ENISA threat landscape for the health sector 2022. European Union Agency for Cybersecurity.

ENISA. (2022b). ENISA Threat Landscape for Ransomware Attacks. European Union Agency for Cybersecurity.

ENISA. (2023). ENISA Threat LANDSCAPE: HEALTH SECTOR.

ENISA. (2024). ENISA threat landscape 2024. European Union Agency for Cybersecurity.

ENISA. (2025). 공식 홈페이지. https://www.enisa.europa.eu

European Commission. (2025, January 15). Bolstering the cybersecurity

of the healthcare sector. Retrieved from https://commission.europa.eu/news-and-media/news/bolstering-cybersecurity-healthcare-sector-2025-01-15_en

European Union. (2019). Regulation (EU) 2019/881 (Cybersecurity Act).

Ewoh, P., & Vartiainen, T. (2024). Vulnerability to cyberattacks and sociotechnical solutions for health care systems: systematic review. Journal of medical internet research, 26, e46904.

HCSN. (2025). Collective Defence for Health Critical Infrastructure. https://ci-isac.org.au/wp-content/uploads/2025/02/HCSN-Information-Pack.pdf

Health ISAC Japan (2025). Health ISAC Japan 정관. https://health-isac-japan.jp/wp-content/uploads/2025/08/aoi_HIJ202507.pdf

Health-ISAC. (2025a). https://health-isac.org

Health-ISAC. (2025b). Health-ISAC. 2024 Annual Report. p.5

HUSAIN, R., TYAGI, R., KHAN, R., & KOMAKULA, M. K. (2023). ENHANCING CYBER SECURITY IN HEALTH CARE INDUSTRY BY USING ISO 27001 ACCREDITATION. i-Manager's Journal on Digital Forensics & Cyber Security (JDF), 1(2).

International Organization for Standardization/International Electrotechnical Commission. (2012). ISO/IEC 27032:2012—Guidelines for cybersecurity. ISO.

International Organization for Standardization/International Electrotechnical Commission. (2016). ISO/IEC 27799:2016—Health informatics—Information security management in health using ISO/IEC 27002. ISO.

International Telecommunication Union. (2008). ITU-T X.1205: Overview of cybersecurity. ITU.

Jalali, M. S., & Kaiser, J. P. (2018). Cybersecurity in hospitals: a systematic, organizational perspective. Journal of medical Internet research, 20(5), e10059.

Kumari, S., Pattanaik, P., & Khan, M. Z. (2024). Impact of Cybersecurity Measures in the Healthcare Sector: A Comprehensive Review of Contemporary Approaches and EmergingTrends.

McLeod, A., & Dolezel, D. (2018). Cyber-analytics: Modeling factors associated with healthcare data breaches. Decision Support Systems, 108, 57-68.

National Council of ISACs. (2025). https://www.nationalisacs.org/about-isacs

National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity (Version 1.1). U.S. Department of Commerce.

National Institute of Standards and Technology. (2025). Glossary: Cyber Threat.

Organisation for Economic Co-operation and Development. (2019). OECD digital security risk management for economic and social prosperity: OECD recommendation and companion document. OECD Publishing.

Sangari, S., Dallal, E., & Whitman, M. (2022). Modeling under-reporting in cyber incidents. Risks, 10(11), 200.

Sardi, A., Rizzi, A., Sorano, E., & Guerrieri, A. (2020). Cyber risk in health facilities: A systematic literature review. Sustainability, 12(17), 7002.

Schiliro, F. (2023). Towards a contemporary definition of cybersecurity. arXiv preprint arXiv:2302.02274.

Shackelford, S. J. (2012). Toward cyberpeace: Managing cyberattacks

through polycentric governance. Am. UL Rev., 62, 1273.
The HIPAA Journal. (2024). 2024 healthcare data breach report.
United Nations General Assembly. (2010). Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Report of the Secretary-General (A/65/201). United Nations.
Vilakazi, K., & Adebesin, F. (2023). A systematic literature review on cybersecurity threats to healthcare data and mitigation strategies.
Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. computers & security, 38, 97-102.
Wasserman, L., & Wasserman, Y. (2022). Hospital cybersecurity risks and gaps: Review (for the non-cyber professional). Frontiers in digital health, 4, 862221.
World Health Organization. (2021). Global strategy on digital health 2020-2025. WHO.

[3장]
개인정보 보호법 시행령, 대통령령 제33107호 (2025).
개인정보 보호법, 법률 제19302호 (2025).
국가정보원. (2025). 병원정보시스템 보안 가이드라인. 국가정보원.
보건복지부·한국사회보장정보원. (2020). 의료기관 랜섬웨어 예방·대응 안내서 및 퀵매뉴얼. 보건복지부·한국사회보장정보원
보건복지부. (2025). 전자의무기록시스템 인증기준 해설서. 보건복지부.
식품의약품안전처. (2023). 의료기기의 사이버 보안 허가심사 가이드라인. 식품의약품안전처.
식품의약품안전처. (2025). 의료기기 사이버 보안 가이드라인(3종: N60, N70, N73). 식품의약품안전처.
의료법 시행규칙, 보건복지부령 제970호 (2025).

의료법 시행령, 대통령령 제33629호 (2025).
의료법, 법률 제18289호 (2025).
전자의무기록의 안전성·신뢰성 확보에 관한 고시, 보건복지부 고시 제2023-113호 (2023).
정보통신기반 보호법, 법률 제18220호 (2025).
정보통신망 이용촉진 및 정보보호 등에 관한 법률, 법률 제19289호 (2025).
한국인터넷진흥원. (2024a). KISA Insight 2024 Vol. 05: 침해사고 등 사이버 공격 대응 관점에서의 사이버 복원력 정책 이슈 분석 및 시사점. 한국인터넷진흥원.
한국인터넷진흥원. (2024b). KISA Insight 2024 Vol. 06: 미국 NIST 사이버 보안 프레임워크 2.0 주요 내용과 시사점. 한국인터넷진흥원.
한국인터넷진흥원. (2024c). 정보보호 및 개인정보보호 관리체계(ISMS-P) 인증 제도 안내서.
한국인터넷진흥원. (2025). 정보통신분야 침해사고 대응 안내서(개정본). 한국인터넷진흥원.
후생노동성(厚生労働省). (2023). 의료정보시스템의 안전관리 가이드라인 제6.0판(医療情報システムの安全管理に関するガイドライン 第6.0版). 후생노동성(厚生労働省).

European Union. (2022). Directive on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). Official Journal of the European Union. https://digital-strategy.ec.europa.eu/en/policies/nis2-directive)
National Institute of Standards and Technology (NIST). (2010). Contingency Planning Guide for Federal Information Systems (SP 800-34 Rev. 1). https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication

800-34r1.pdf

National Institute of Standards and Technology (NIST). (2024a). Cybersecurity Framework (CSF) 2.0. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

National Institute of Standards and Technology (NIST). (2024b). Computer Security Incident Handling Guide (SP 800-61 Rev. 3) (Draft). https://csrc.nist.gov/pubs/sp/800/61/r3/ipd

Nelson, A., Rekhi, S., Souppaya, M., & Scarfone, K. (2024). Incident response recommendations and considerations for cybersecurity risk management: a CSF 2.0 community profile (No. NIST Special Publication (SP) 800-61 Rev. 3 (Draft)). National Institute of Standards and Technology.

U.S. Department of Health and Human Services (HHS). (2023). Health Industry Cybersecurity Practices (HICP). https://405d.hhs.gov/cornerstone/hicp

U.S. Department of Health and Human Services (HHS). (2024). Operational Continuity-Cyber Incident (OCCI) Checklist. https://405d.hhs.gov/Documents/405d-occi-checklist-2024.pdf

[4장]

사카구치 카즈키, 츠츠미 노부유키, 하라 유이치. (2023. 4. 11.). 의료 기관에 대한 사이버 공격 사례 연구: 민간 병원·의원의 피해 사례에서 배우다. 일본의사회종합정책연구기구 리서치리포트 No.136. 2025. 3. 11. 인출. https://www.jmari.med.or.jp/wp-content/uploads/2023/04/RR136.pdf

한국사회보장정보원. (2025). 의료정보보호센터 내부 자료

ComplianceHub Wiki. (2024). 2025년 8월 12일 인출,

https://www.compliancehub.wiki/ameos-hospital-network-cyberattack-germanys-latest-healthcare-cybersecurity-crisis/

Duvar English. (2024). 2025년 8월 12일 인출, https://www.duvarenglish.com/medical-records-of-millions-stolen-in-turkish-state-hospital-data-leak-news-64215

IT Governance EU. (2024, February 11). 2025년 8월 12일 인출, https://www.itgovernance.eu/blog/en/the-week-in-cyber-security-and-data-privacy-in-europe-5-11-february-2024

NHS England. (2025). Synnovis cyber incident update. 2025년 8월 12일 인출, https://www.england.nhs.uk/synnovis-cyber-incident/

The HIPAA Journal. (2025, July 15). Healthcare data breach statistics. HIPAA Journal. Retrieved from https://www.hipaajournal.com/healthcare-data-breach-statistics/

[5장]

사카구치 카즈키, 츠츠미 노부유키, 하라 유이치. (2023. 4. 11.). 의료 기관에 대한 사이버 공격 사례 연구: 민간 병원·의원의 피해 사례에서 배우다. 일본의사회종합정책연구기구 리서치리포트 No.136. 2025. 3. 11. 인출. https://www.jmari.med.or.jp/wp-content/uploads/2023/04/RR136.pdf

한국보건사회연구원. (2025). 의료기관 사이버 보안 실태조사 원자료. 한국보건사회연구원.

한국보건의료정보원. (2021). 2020년 보건의료정보화 실태조사 결과보고서. pp.387-441

한국사회보장정보원. (2024). 의료기관 정보보안 강화 지원전략 수립 인터뷰 질의서(내부자료).

한국정보보호산업협회. (2025). 2024년 정보보호 실태조사. pp.184-203.3.

[6장]
한국사회보장정보원. (2025). 의료정보보호센터 내부 자료

[부록 1] 의료기관 사이버 보안 실태조사 조사 참여 동의서

○ 한국보건사회연구원은 국무총리실 산하 국가정책연구기관으로, 보건복지 분야 정책 현안을 분석하고 이에 근거한 정책 방안을 마련하고 있습니다.

○ 본 연구는 우리나라 의료기관 사이버 보안 강화를 위한 정책 대응 방안 마련을 위해 한국보건사회연구원에서 수행하는 연구입니다. 조사 결과는 의료기관의 사이버 위협 현황 및 사이버 보안 실태 파악하여 정책 개선 방안을 도출하기 위한 기초 자료로 활용되오니 귀하의 적극적인 협조와 정확한 작성을 부탁드립니다.

○ 본 조사는 약 30분간 소요될 예정입니다. 조사가 진행되는 도중에 응답하기 불편한 내용은 답변하지 않으셔도 됩니다. 언제라도 조사 참여 동의를 자발적으로 철회하고 연구 참여를 중단하여도 되며, 조사 참여의 철회나 중단에 따른 어떠한 불이익이나 차별도 없을 것입니다. 또한, 개인을 식별할 수 있는 지역, 개인식별정보 등을 공개하지 않기 때문에 조사 참여에 따라 예상되는 위험 및 손실, 이득은 없습니다.

○ 응답해주신 내용은 한국보건사회연구원에서 제공하는 개인정보 보안 프로그램이 설치되어 있는 컴퓨터에 입력 후 익명처리(성명과 연락처, 주소 등 개인식별정보를 모두 삭제 또는 비식별화 처리)된 파일의 형태로 보관하며, 연구의 최종결과물(연구보고서, 마이크로데이터 등) 작성 시에도 개인 혹은 기관 식별이 가능하지 않도록 자료를 처리합니다.

○ 연구의 최종결과물(연구보고서, 마이크로데이터 등)은 개인정보 비식별화 절차를 거친 이후 공공데이터의 제공 및 이용 활성화에 관한 법률 제26조(공공데이터의 제공)에 의해 공개될 수 있습니다. 또한, 연구의 최종결과물 작성 시에도 개인식별이 가능하지 않도록 자료를 처리합니다.

○ 연구참여자는 개인정보에 대한 비밀보장을 침해하지 않고 관련 규정이 정하는 범위 안에서 본 연구의 실시 절차와 자료의 신뢰성을 검증하기 위해 연구 결과를 직접 열람할 수 있습니다.

○ 현재 의료기관의 사이버 위협 현황 및 사이버 보안 실태와 문제점을 파악하고 대응 및 지원 방안 모색의 기초자료로 삼고자 하오니, 귀 기관의 적극적인 참여와 정확하고 솔직한 응답을 부탁드립니다. 감사합니다.

- 조사문의

· 한국보건사회연구원 ○○○ 연구원(044-287-####, ○○○@kihasa.re.kr)

· 대한병원협회 총무국 전산정보팀

○ 본인은 위 사항에 따라 조사 사실을 충분히 설명받고 숙지하였으며, 조사 참여를 거부할 권리가 있다는 사실을 인지하였으며, 위의 사항에 따라 조사 참여에 스스로 동의하였음을 확인합니다.

2025년 월 일

동의자 서명: _____(인)

[부록 2] 의료기관 사이버 보안 실태조사 조사 참여 동의서

개인정보 수집 이용 동의서

1. 개인정보 수집 및 이용 목적
   ① 국내 의료기관의 서비스 수준 및 국민의 의료제도 인식에 관한 사항을 파악
   ② 응답 내용에 대한 추가 질문 등 확인할 사항이 있는 경우 사용
2. 개인정보 수집 및 이용 항목
   ① 직접 수집 개인정보: 이름, 휴대폰번호
3. 개인정보 보유 및 이용 기간 : 연구 종료일('25.12.31.) 이후 즉시 폐기
4. 개인정보 동의 거부 고지 : 개인정보 수집 및 이용 동의를 거부할 수 있으며, 거부하는 경우 조사에 참여하실 수 없습니다.

개인정보 수집 및 이용 동의	개인정보 수집 및 이용에 동의합니다.	□ 동의함 □ 동의하지 않음

[부록 3] 의료기관 사이버 보안 실태조사 조사표

의료기관 사이버 보안 실태조사 조사표

Ⅰ 기본정보

1. 기관명, 요양기관기호

기관명: _____, 요양기관기호: _____

2. (대표)응답자 성명 및 연락처

응답자 성명: _____, 연락처(전화번호): _____

※ (대표)응답자 성명 및 연락처는 본 조사와 관련하여, 미응답 항목 추가적인 조사 및 질의 등을 위해 수집하는 것이오니 본 조사와 관련하여 응답 가능한 담당자 성명 및 연락처를 기재하여 주실 것을 요청함.

3. (1-2문항) 응답자 본인의 소속 및 직무

소속: _____, 직무: _____

※ 소속: 내부와 외부(아웃소싱) 구분하고 작성 부서명 기재
(예시) 내부(정보운영팀), 내부(정보보안팀), 내부(총무팀), 내부(의무기록실), 외부(외주업체) 등
※ 직무: 관리자(팀장급 이상) 및 담당자 구분하고 담당업무를 기재
(예시) 관리자, 정보보안 담당자, 정보보호 담당자, 네트워크 담당자, 개발자, 정보시스템운영 담당자 등

Ⅱ 의료기관 보안관제 등

4. 귀 기관은 사이버 공격에 대응하기 위한 보안관제를 실시하고 있습니까?

① 실시하고 있음
② 실시하지 않음

(보안관제)
네트워크 장비, 보안시스템 등을 원격시스템(또는 장소)에서 관리하며, 인가받지 않은 외부침입을 실시간으로 탐지하여 원격관제실에 경보를 보냄으로써 외부 침입에 즉각적인 대응 및 역추적, 이기종간에 보안 관리를 할 수 있는 통합보안을 말함.

5. 귀 기관의 보안관제 유형을 응답해 주십시오.(복수 선택 가능)

① 자체 보안관제
② 위탁(파견) 보안관제
③ 위탁(원격) 보안관제
④ 사이버안전센터(복지부, 교육부 등)
⑤ 의료기관공동보안관제센터(의료 ISAC)
⑥ 기타 (직접 입력: _____)

① 자체 보안관제: 의료기관에서 자체적으로 보안관제
② 위탁(파견) 보안관제: 위탁 보안관제업체가 의료기관에 상주하면서 보안관제
③ 위탁(원격) 보안관제: 위탁 보안관제업체가 외부에서 원격으로 보안관제
④ 사이버안전센터: 보건복지부, 교육부 등 정부부처 사이버안전센터에서 보안관제
⑤ 의료기관공동보안관제센터(의료 ISAC): 의료정보보호센터(HISC)에서 보안관제

6. 귀 기관에서 획득한 보안인증체계를 모두 선택해 주세요.(복수 선택 가능)

① ISMS
② ISMS-P
③ ISO 27001
④ 기타 (직접 입력: _____)
⑤ 없음

7. (4-6문항) 응답자 본인의 소속 및 직무

소속: _____, 직무: _____

※ 소속: 내부와 외부(아웃소싱) 구분하고 작성 부서명 기재
(예시) 내부(정보운영팀), 내부(정보보안팀), 내부(총무팀), 내부(의무기록실), 외부(외주업체) 등
※ 직무: 관리자(팀장급 이상) 및 담당자 구분하고 담당업무를 기재
(예시) 관리자, 정보보안 담당자, 정보보호 담당자, 네트워크 담당자, 개발자, 정보시스템운영 담당자 등

III 의료기관 정보화/개인정보보호/정보보안 예산 현황

8. 귀 기관의 운영 및 투자 예산 규모를 응답해 주십시오.

구분	정보화	개인정보보호	정보보안
2024년	백만원	백만원	백만원
2025년	백만원	백만원	백만원

정보화 예산: 정보시스템 운영, 유지보수, 개발, 네트워크 운영 등 단순 정보시스템 운영 등에 소요되는 예산
개인정보보호 예산: 개인정보를 보호하기 위한 활동(시스템 구축, 컨설팅, 교육, 홍보, 인증 등) 등에 소요되는 예산
정보보안 예산: 정보시스템에 대한 기밀성, 무결성, 가용성을 유지 보호하기 위해 취하는 활동(시스템 구축,) 등에 소요되는 예산

8-1. 귀 기관의 정보화/개인정보보호/정보보안 예산 규모는 적절하다고 생각하십니까?

구분	매우 적절하다	적절하다	보통이다	적절하지 않다	매우 적절하지 않다
정보화 예산 규모	①	②	③	④	⑤
개인정보보호 예산 규모	①	②	③	④	⑤
정보보안 예산 규모	①	②	③	④	⑤

9. (8문항) 응답자 본인의 소속 및 직무

소속: _____, 직무: _____

※ 소속: 내부와 외부(아웃소싱) 구분하고 작성 부서명 기재
(예시) 내부(정보운영팀), 내부(정보보안팀), 내부(총무팀), 내부(의무기록실), 외부(외주업체) 등
※ 직무: 관리자(팀장급 이상) 및 담당자 구분하고 담당업무를 기재
(예시) 관리자, 정보보안 담당자, 정보보호 담당자, 네트워크 담당자, 개발자, 정보시스템운영 담당자 등

Ⅳ 전자의무기록시스템 인증제도

10. 전자의무기록시스템 인증제도가 시행되고 있습니다. 귀 기관에서는 이 사실을 알고 있습니까?

① 들어본 적이 있고, 자세한 내용도 알고 있음
② 들어본 적은 있으나, 자세한 내용은 잘 모름
③ 제도에 대해 전혀 들어본 적이 없음

(전자의무기록시스템 인증제도)
환자 안전과 진료연속성 지원을 목적으로 국내 전자의무기록시스템에 대한 국가적 표준과 적합성 검증을 통해 업체의 표준제품 개발을 유도하여 시스템의 상호호환성 확보 등 품질 향상으로 의료소비자에게 양질의 의료 서비스를 제공될 수 있도록 하기 위한 제도를 말함.

11. 귀 기관에서는 전자의무기록시스템에 대해 인증을 받거나 또는 인증받은 전자의무기록시스템을 도입하였습니까?

① 예 ☞13번 문항으로 이동
② 아니요 ☞11-1번 문항으로 이동

11-1. (11문항 ② 응답자만)향후 귀 기관에서는 전자의무기록시스템에 대해 인증을 받거나 또는 인증받은 전자의무기록시스템을 도입할 의향이 있습니까?

① 의향 있음
② 의향 없음

12. (10~11 문항) 응답자 본인의 소속 및 직무

소속: _____, 직무: _____

※ 소속: 내부와 외부(아웃소싱) 구분하고 작성 부서명 기재
(예시) 내부(정보운영팀), 내부(정보보안팀), 내부(총무팀), 내부(의무기록실), 외부(외주업체) 등
※ 직무: 관리자(팀장급 이상) 및 담당자 구분하고 담당업무를 기재
(예시) 관리자, 정보보안 담당자, 정보보호 담당자, 네트워크 담당자, 개발자, 정보시스템운영 담당자 등

V 의료정보시스템 구축 및 유지보수 현황

13. 귀 기관에서는 다음의 의료정보시스템을 현재 구축하여 운영하고 있습니까? 운영하는 의료정보시스템의 상용제품 여부와 유지보수 형태를 응답해 주십시오. (필요시 외부 아웃소싱 업체에서 응답 가능)

	의료정보시스템 종류	도입여부		도입형태		유지보수 형태			솔루션 유지보수 여부	
		예	아니오	SI개발	상용제품	자체	위탁	자체+위탁 병행	예	아니오
진료정보	1) 전자의무기록시스템(EMR)	①	②	①	②	①	②	③	①	②
	2) 모바일 전자의무기록시스템(EMR)	①	②	①	②	①	②	③	①	②
	3) 처방전달시스템(OCS)	①	②	①	②	①	②	③	①	②
	4) 의료영상저장전송시스템(PACS)	①	②	①	②	①	②	③	①	②
	5) 임상검사정보시스템(LIS)	①	②	①	②	①	②	③	①	②
	6) 약국관리시스템	①	②	①	②	①	②	③	①	②
	7) 진료과 및 회송 시스템(상/하/원)	①	②	①	②	①	②	③	①	②
	8) 진료정보교류시스템(복지부)	①	②	①	②	①	②	③	①	②
	9) 원격의료시스템	①	②	①	②	①	②	③	①	②
	10) 건강검진정보시스템	①	②	①	②	①	②	③	①	②
환자서비스	11) 의료기관 포털(대표 홈페이지)	①	②	①	②	①	②	③	①	②
	12) 의료기관 포털(웹) 기반 개인건강기록(PHR)	①	②	①	②	①	②	③	①	②
	13) 모바일 개인건강기록(PHR)	①	②	①	②	①	②	③	①	②
진료지원 및 경영정보	14) 원무관리, 보험청구 창구시스템	①	②	①	②	①	②	③	①	②
	15) 전자적 자원관리시스템(ERP)	①	②	①	②	①	②	③	①	②
	16) 내부직원지원시스템(ESS)	①	②	①	②	①	②	③	①	②
	17) 전사적데이터웨어하우스(EDW)	①	②	①	②	①	②	③	①	②
교육 및 연구	18) 보수교육 전산시스템	①	②	①	②	①	②	③	①	②
	19) 조사연구 전산시스템	①	②	①	②	①	②	③	①	②
기타 부대사업	20) 부설 노인복지시설 전산시스템	①	②	①	②	①	②	③	①	②
	21) 부설 장례식장 전산시스템	①	②	①	②	①	②	③	①	②
	22) 부설 주차장 전산시스템	①	②	①	②	①	②	③	①	②
	23) 기타(_____)	①	②	①	②	①	②	③	①	②

(도입유형-SI개발): 해당 의료기관에서 개발(자체 또는 외부)한 의료정보시스템을 사용하는 경우
(도입유형-상용제품): 기존에 개발된 의료정보시스템을 구입 또는 임대하여 사용하는 경우
(솔루션 유지보수 여부): 의료정보시스템 운영을 위한 각종 상업용 솔루션의 유지보수가 신속히 이루어지고 있는지 여부

※ 기타 부대사업: 외부위탁 또는 외주업체에서 운영하는 경우 도입여부(예)로 기재하고 도입형태, 유지보수형태, 솔루션 유지보수 여부는 해당 기관에 문의하여 작성

14. 귀 기관의 의료정보시스템 관련 연계여부를 응답해 주십시오.
(필요시 외부 아웃소싱 업체에서 응답 가능)

	정보시스템 종류	인터넷 연결 여부		병원 내 정보시스템 연결 여부		외부 연계시스템 연계 여부	
		예	아니오	예	아니오	예	아니오
진료 정보	1) 전자의무기록시스템(EMR)	①	②	③	④	⑤	⑥
	2) 모바일 전자의무기록시스템(EMR)	①	②	③	④	⑤	⑥
	3) 처방전달시스템(OCS)	①	②	③	④	⑤	⑥
	4) 의료영상저장전송시스템(PACS)	①	②	③	④	⑤	⑥
	5) 임상검사정보시스템(LIS)	①	②	③	④	⑤	⑥
	6) 약국관리시스템	①	②	③	④	⑤	⑥
	7) 진료과 및 회송 시스템(상/하/원)	①	②	③	④	⑤	⑥
	8) 진료정보교류시스템(복지부)	①	②	③	④	⑤	⑥
	9) 원격의료시스템	①	②	③	④	⑤	⑥
	10) 건강검진정보시스템	①	②	③	④	⑤	⑥
환자 서비스	11) 의료기관 포털(대표 홈페이지)	①	②	③	④	⑤	⑥
	12) 의료기관 포털(웹) 기반 개인건강기록(PHR)	①	②	③	④	⑤	⑥
	13) 모바일 개인건강기록(PHR)	①	②	③	④	⑤	⑥
진료 지원 및 경영 정보	14) 원무관리, 보험청구 창구시스템	①	②	③	④	⑤	⑥
	15) 전자적 자원관리시스템(ERP)	①	②	③	④	⑤	⑥
	16) 내부직원지원시스템(ESS)	①	②	③	④	⑤	⑥
	17) 전사적데이터웨어하우스(EDW)	①	②	③	④	⑤	⑥
교육 및 연구	18) 보수교육 전산시스템	①	②	③	④	⑤	⑥
	19) 조사연구 전산시스템	①	②	③	④	⑤	⑥
기타 부대 사업	20) 부설 노인복지시설 전산시스템	①	②	③	④	⑤	⑥
	21) 부설 장례식장 전산시스템	①	②	③	④	⑤	⑥
	22) 부설 주차장 전산시스템	①	②	③	④	⑤	⑥
	23) 기타(_____)	①	②	③	④	⑤	⑥

인터넷 연결 여부: 해당 정보시스템이 인터넷에 연결되어 있는지 여부
병원 내 정보시스템 연결 여부: 해당 정보시스템이 병원 내 다른 정보시스템과 연결되어 있는지 여부
외부 연계시스템 연계: 해당 정보시스템이 외부 연계시스템과 연결되어 있는지 여부
* 외부 연계시스템 '아니오(미연계)'는 의료기관의 시스템과 연계 없이, 외부 정보시스템 웹페이지에 직접 접속하여 로그인 및 환자검색 후 필요한 정보를 모두 입력 및 조회하는 경우를 말함.
(외부 연계시스템 목록)
1) 감염병자동신고지원프로그램, 2) 예방접종등록관리시스템, 3) 연명의료정보처리시스템, 4) 개인정보통합관리시스템, 5) 진료정보교류시스템, 6) 의약품안전사용서비스(DUR), 7) E-평가자원시스템, 8) 보건의료자원통합신고포털, 9) 진료의뢰 회송 중계포털, 10) 국가응급환자정보공유(NEDIS), 11) 통합응급의료정보 인트라넷, 12) 의료기기 추적관리시스템, 13) 마약류통합관리시스템(NIMS), 14) 의약품이상사례보고시스템(KAERS)

15. 귀 기관의 클라우드 서비스 도입 현황에 대해 응답해 주십시오.
(필요시 외부 아웃소싱 업체에서 응답 가능)

	도입	미도입
1) 진료정보(EMR, OCS, PACS)	①	②
2) 환자서비스(포털, 웹)	①	②

(클라우드 서비스)
인터넷을 통해 서버, 스토리지, 데이터베이스, 네트워크, 소프트웨어 등 IT 자원을 필요에 따라 빌려 쓰는 형태의 서비스

16. (13-15문항) 응답자 본인의 소속 및 직무

소속: _____, 직무: _____

※ 소속: 내부와 외부(아웃소싱) 구분하고 작성 부서명 기재
(예시) 내부(정보운영팀), 내부(정보보안팀), 내부(총무팀), 내부(의무기록실), 외부(외주업체) 등
※ 직무: 관리자(팀장급 이상) 및 담당자 구분하고 담당업무를 기재
(예시) 관리자, 정보보안 담당자, 정보보호 담당자, 네트워크 담당자, 개발자, 정보시스템운영 담당자 등

VI 의료정보시스템 정보화 담당조직 및 인력

17. 현재 귀 기관에는 의료정보시스템 구축·운영·관리 등 **정보화 업무를 담당하는 전담부서**가 있습니까?

① 예
② 아니오

18. 현재 귀 기관에는 의료정보시스템 구축·운영·관리 등 정보화 업무를 담당하는 인력 현황에 대해 응답해 주십시오.

구분	설명	전담/겸직인력	
		내부인력	외부 또는 파견인력
관리자	전반적인 정보화 정책 및 계획 수립/시행/개선, 정보보안 및 정보보호 관리체계 구축 및 운영, 데이터 거버넌스 구축 및 운영 등	명	명
정보보안 담당자	방화벽, 침입탐지시스템 등 보안시스템 운영, 해킹.침입 등 외부 위협 발생시 신속 탐지 및 대응 등	명	명
정보보호 담당자	개인정보의 기술적, 관리적, 물리적 보호조치 등	명	명
네트워크 담당자	네트워크 시스템 설계, 운영 및 유지보수 등	명	명
개발자	정보자산 개발·유지관리, 기능 요구사항 개발(EMR화면 등)	명	명
정보시스템 담당자	서버 등 전산시스템 장비운영, 유지보수, 상용 소프트웨어 관리 등	명	명

(담당인력 계산방법)
* 1명이 2개 업무를 담당하는 경우, 각 업무의 총 합을 1로 하고, 업무비중을 고려하여 산정함.
  (예시) A직원이 개발업무, 정보시스템 담당업무, 정보보안 업무를 모두 담당하며, 각각의 업무 비중이 50%, 40%, 10%라면 개발자 0.5명, 정보시스템 담당자 0.4명, 정보보안 담당자 0.1명이며, 총 합은 1.0명으로 산정
  (예시) B직원이 정보보호 업무와 정보보안 업무를 모두 담당하며, 각각의 업무 비중이 60%, 40% 라면 정보보호 담당자 0.6명, 정보보안 담당자 0.4명, 총 합은 1.0명 임.
* 외주 또는 파견인력이 정기적/비정기적으로 업무를 수행하는 경우, 해당 인력의 업무시간을 고려하여 업무비중을 산정함.
  (예시: 정기적) 외주업체 직원이 정기적 또는 비정기적으로 4일/월 (1일/주) 방문하여 업무를 수행하는 경우 0.2명 임.

19. 귀 기관의 정보보안 담당인력은 충분하다고 생각하십니까?

① 매우 충분하다 (☞ 20문항으로 이동)
② 충분하다 (☞ 20문항으로 이동)
③ 보통이다 (☞ 20문항으로 이동)
④ 부족하다 (☞ 19-1문항으로 이동)
⑤ 매우 부족하다 (☞ 19-1문항으로 이동)

19-1. (19문항 ④, ⑤ 응답자만) 정보보안 담당인력 부족 문제를 해결하기 위해 필요한 지원은 무엇이라고 생각하십니까?
(1순위부터 3순위까지 선택하여 주십시오.)

1순위		2순위		3순위	

① 정보의 인력 지원 및 파견
② 정보보호 교육 및 훈련 프로그램 강화
③ 예산 확대를 통한 인력 고용
④ 외부 전문 인력 활용 지원
⑤ 기타(직접 입력: _____)

20. (17-19문항) 응답자 본인의 소속 및 직무

소속: _____, 직무: _____

※ 소속: 내부와 외부(아웃소싱) 구분하고 작성 부서명 기재
(예시) 내부(정보운영팀), 내부(정보보안팀), 내부(총무팀), 내부(의무기록실), 외부(외주업체) 등
※ 직무: 관리자(팀장급 이상) 및 담당자 구분하고 담당업무를 기재
(예시) 관리자, 정보보안 담당자, 정보보호 담당자, 네트워크 담당자, 개발자, 정보시스템운영 담당자 등

VII 정보보안(교육)

21. 귀 기관의 대상자별 **원내외 정보보안 교육 시행 여부 및 시행 주기**에 대해 응답해 주십시오.

구분	시행 여부		시행 주기			
	시행	미시행	분기별	반기별	년1회	비정기적(기타)
CIO, CISO	①	②	①	②	③	④ (직접 입력:)
전산 부서원	①	②	①	②	③	④ (직접 입력:)
정보보안 담당자	①	②	①	②	③	④ (직접 입력:)
의료진	①	②	①	②	③	④ (직접 입력:)
의료진 외 전 직원	①	②	①	②	③	④ (직접 입력:)

21-1. (21문항 시행여부 ①(시행) 응답자만) 귀 기관의 대상자별 **원내외 정보보안 교육 참석 수준**에 대해 응답해 주십시오.

구분	반드시 참여함 (80~100%)	대체로 참여함 (60~79%)	보통 (40~59%)	거의 참여하지 않음 (20~39%)	전혀 참여하지 않음 (0~19%)
CIO, CISO	①	②	③	④	⑤
전산 부서원	①	②	③	④	⑤
정보보안 담당자	①	②	③	④	⑤
의료진	①	②	③	④	⑤
의료진 외 전 직원	①	②	③	④	⑤

21-2. (21문항 시행여부 ①(시행) 응답자만) 귀 기관의 대상자별 **주로 실시한 정보보안 교육 방법은 무엇입니까?**

구분	정보보안 교육 방법				교육방식	
	정부/지자체/공공기관 교육 참여	민간 전문기관 위탁	자체 교육 (외부 강사)	자체교육 (내부 강사)	온라인 교육	오프라인 교육
CIO, CISO	①	②	③	④	①	②
전산 부서원	①	②	③	④	①	②
정보보안 담당자	①	②	③	④	①	②
의료진	①	②	③	④	①	②
의료진 외 전 직원	①	②	③	④	①	②

21-3. (21문항 시행여부 ①(시행) 응답자만) 귀 기관에서 실시한 **임직원 대상 정보보안 교육의 효과**는 어떠합니까?

① 매우 효과적이다
② 효과적이다
③ 보통이다
④ 효과가 없는 편이다
⑤ 전혀 효과가 없다

21-4. (21문항 시행여부 ①(시행) 응답자만) 귀 기관에서 실시한 **임직원 대상 정보보안 교육의 만족도**는 어떠합니까?

① 매우 높다
② 높은 편이다
③ 보통이다
④ 낮은 편이다
⑤ 매우 낮다

22. (21문항 시행여부 ②(미시행) 응답자만) 귀 기관의 대상자별 **원내외 정보보호 및 정보보안 미시행 이유**에 대해 간략하게 기술해 주십시오.

구분	미시행 이유
CIO, CISO	(직접 입력:_____)
전산 부서원	(직접 입력:_____)
정보보안 담당자	(직접 입력:_____)
의료진	(직접 입력:_____)
의료진 외 전 직원	(직접 입력:_____)

23. (21-22문항) 응답자 본인의 소속 및 직무

소속: _____, 직무: _____

※ 소속: 내부와 외부(아웃소싱) 구분하고 작성 부서명 기재
(예시) 내부(정보운영팀), 내부(정보보안팀), 내부(총무팀), 내부(의무기록실), 외부(외주업체) 등
※ 직무: 관리자(팀장급 이상) 및 담당자 구분하고 담당업무를 기재
(예시) 관리자, 정보보안 담당자, 정보보호 담당자, 네트워크 담당자, 개발자, 정보시스템운영 담당자 등

Ⅷ 정보보호 및 정보보안(정책)

24. 의료기관을 대상으로 한 **정보보호 및 정보보안 관련 별도의 지침이나 가이드라인 등의 규정**이 필요하다고 생각하십니까?

① 예
② 아니요

25. 현재 귀 기관에는 정보보호 및 보안 관련 지침이나 가이드라인 등 **별도의 자체 규정**이 있습니까?

① 예
② 아니요

26. **귀 기관의 규정에서 포함하고 있는 내용**을 모두 선택하여 주십시오.
(별도의 정보보호 및 정보보안 관련 자체 규정이 없더라도 다른 규정에 포함되어 있는 경우도 포함).

1. 기술적 보안분야
□1-① 클라우드 보안관리(기술적)
□1-② 정보보호시스템, 네트워크 장비 보안
□1-③ 인터넷 전화 보안
□1-④ 서버 보안
□1-⑤ 용역사업 보안(기술적)
□1-⑥ 자료 보안
□1-⑦ PC 등 단말기 보안
□1-⑧ 업무시스템 보안
□1-⑨ 전자우편 보안
□1-⑩ 비인가 IT 기기 관리
□1-⑪ 원격근무시스템 보안

3. 물리적 보안 분야
□ 3-① 전산실 통제구역 지정
□ 3-② 출입통제시스템 운영
□ 3-③ 전산실 출입자 권한 설정 및 기록 관리
□ 3-④ 외부인(방문자) 출입 절차 및 통제
□ 3-⑤ 영상감시(CCTV) 설치 및 운영

2. 관리적 보안 분야
□2-① 책무 □2-② 인력 □2-③ 조직
□2-④ 인센티브 □2-⑤ 예산
□2-⑥ 정보보안 감사
(상위기관 점검 또는 인증 심사 등 외부 점검)
□2-⑦ 정보보안 교육
□2-⑧ 보안성 검토
(제품 구매 시 네트워크 또는 장비 기능 등 보안성 검토 수행 후 구입)
□2-⑨ 용역사업 보안
(관리적 측면, 계약서 상의 보안관련 내용 여부)
□2-⑩ 소프트웨어 개발보안
□2-⑪ 망분리 정책
□2-⑫ 정보자산 관리
□2-⑬ 보안위규 조치 및 예방대책 마련
□2-⑭ 평가 결과에 따른 미비점 개선
□2-⑮ 정보보안에 대한 기관장의 관심
□2-⑯ 클라우드 정책
□2-⑰ 기반시설 보호대책

27. (24-26문항) 응답자 본인의 소속 및 직무

소속: _____, 직무: _____

※ 소속: 내부와 외부(아웃소싱) 구분하고 작성 부서명 기재
(예시) 내부(정보운영팀), 내부(정보보안팀), 내부(총무팀), 내부(의무기록실), 외부(외주업체) 등
※ 직무: 관리자(팀장급 이상) 및 담당자 구분하고 담당업무를 기재
(예시) 관리자, 정보보안 담당자, 정보보호 담당자, 네트워크 담당자, 개발자, 정보시스템운영 담당자 등

IX 정보보안 업무 관련 애로사항

28. 귀 기관의 정보보안 업무 수행에서 가장 큰 애로사항은 무엇입니까?(1순위부터 3순위까지 선택하여 주십시오.)

1순위		2순위		3순위	

① 보안 인력 부족
② 보안 예산 부족
③ 보안 기술적 지식 부족
④ 시스템 노후화 및 기술 지원 부족
⑤ (자체) 보안 관련 정책 및 규정의 미비
⑥ 기타(직접 입력:)

29. 정보보안 업무의 어려움을 해결하기 위해 가장 필요한 지원은 무엇이라고 생각하십니까?(1순위부터 3순위까지 선택하여 주십시오.)

1순위		2순위		3순위	

① 정부의 재정적 지원
② 전문인력 지원
③ 정보보안 관련 교육 및 훈련
④ 기술적 컨설팅
⑤ 기타(직접 입력:)

30. (28-29문항) 응답자 본인의 소속 및 직무

소속: _____, 직무: _____

※ 소속: 내부와 외부(아웃소싱) 구분하고 작성 부서명 기재
(예시) 내부(정보운영팀), 내부(정보보안팀), 내부(총무팀), 내부(의무기록실), 외부(외주업체) 등
※ 직무: 관리자(팀장급 이상) 및 담당자 구분하고 담당업무를 기재
(예시) 관리자, 정보보안 담당자, 정보보호 담당자, 네트워크 담당자, 개발자, 정보시스템운영 담당자 등

X 보안사고(침해사고) 등

31. 귀 기관에서는 보안사고(침해사고)가 발생할 가능성이 높다 생각하십니까?

① 매우 그렇다
② 그렇다
③ 보통이다
④ 그렇지 않다
⑤ 매우 그렇지 않다

32. 최근 3년간(2022년 이후) 귀 기관에서는 보안사고(침해사고)가 발생한 적이 있습니까?

① 발생 했음 ☞33-1번 문항으로 이동
② 발생하지 않았음 ☞34번 문항으로 이동

32-1. (32문항 ① 응답자만) 최근 3년간(2022년 이후) 귀 기관에서 경험한 보안사고(침해사고) 유형은 무엇입니까?(복수 선택 가능)

① 웹해킹
② 홈페이지 위변조
③ 해킹메일
④ 서비스거부
⑤ 네트워크침입
⑥ 정보수집
⑦ 악성코드
⑧ 유해IP
⑨ 기타(직접 입력:_____)

① 웹해킹: 인젝션, 세션탈취 등 웹페이지를 통한 사이버 공격 유형
② 홈페이지위변조: 홈페이지에 대한 이상 유무 모니터링 결과
③ 해킹메일: 이메일을 통한 악성코드 유포, 피싱 등의 사이버 공격 유형
④ 서비스거부: 정상적인 서비스 제공을 어렵게 만드는 가용성을 침해하는 사이버 공격 유형
⑤ 네트워크침입: 네트워크 통하거나 네트워크 프로토콜을 악용하여 수행하는 사이버 공격 유형
⑥ 정보수집: 공격대상의 OS, App 종류/버전, 에러정보 등 정보 수집 단계의 사이버 공격 유형
⑦ 악성코드: 시스템 파괴, 정보 유출 등의 악의적인 활동을 수행하는 소프트웨어 유형
⑧ 유해IP: 해킹시도, 스팸메일 등 사이버 공격에 악용되었다고 알려진 IP 유형

32-2. (32문항 ① 응답자만) 보안사고(침해사고) 발생 시 평균 인지 시간은 어느 정도입니까?

① 1시간 미만
② 1~4시간 미만
③ 4시간~12시간 미만
④ 12시간 이상
⑤ 기타(직접 입력: _____시간)

* 보안사고(침해사고) 인지 시간: 보안사고(침해사고) 발생시점부터 사실을 인지하기까지 소요된 시간
* 1일=24시간으로 환산
(예시) 1일 6시간 = 30시간

32-3. (32문항 ① 응답자만) 보안사고(침해사고) 발생 시 **평균 대응 시간**은 어느 정도입니까?

① 1시간 미만
② 1~4시간 미만
③ 4시간~12시간 미만
④ 12시간~24시간 미만
⑤ 기타(직접 입력: _____시간)

* 보안사고(침해사고) 대응 시간: 보안사고(침해사고) 발생 사실 인지 시점부터 원인을 파악하고, 문제해결 및 서비스를 복원하기까지 소요된 시간
* 1일=24시간으로 환산
(예시) 1일 6시간 = 30시간

32-4. (33문항 ① 응답자만) 보안사고(침해사고) 발생 시 복구 비용은 어느 정도 입니까?

_____원

(예시) 약 5억원 = 2억 5천만원(데이터 복구 및 신규 시스템 구입 비용) + 5천만원(외주 업체 비용 및 원내 인력 인건비) + 2억원(개인정보 유출 대책 비용, 사과문 발송 및 콜센터 운영, 변호사 비용)

32-5. (33문항 ① 응답자만) 보안사고(침해사고) 발생 시 사고 정보를 어느 수준까지 파악하고 대응할 수 있었는지에 대해 응답해주십시오.

① 사고 발생 사실만 정리할 수 있었다.
② 사고 원인 분석까지 할 수 있었다.
③ 사고 원인 분석과 향후 대응방안까지 정리할 수 있었다.

32-6. (33문항 ① 응답자만) 보안사고(침해사고)의 주요 원인으로 무엇을 꼽을 수 있습니까?(복수 선택 가능)

① 기술적 취약점 (패치 미적용, 시스템 노후 등)
② 관리적 취약점 (체계, 행위 및 인식 제고 등)
③ 외부 사이버 공격 (랜섬웨어, 피싱 등)
④ 네트워크 설정 미흡
⑤ 기타: (직접 입력: _____)

33. 귀 기관의 보안사고(침해사고) 대응에 가장 큰 어려움은 무엇입니까?

① 보안 전문인력 부족
② 시스템의 기술적 한계
③ 운영 비용 부담
④ 매뉴얼 등 사고 대응 프로세스 부재
⑤ 사고 대응 조직 부재
⑥ 경찰 또는 복지부의 무관심 혹은 괴롭힘
⑦ 기타: (직접 입력: _____)

34. 귀 기관에서 보안사고(침해사고) 발생하게 된다면, 보안사고 신고를 주저하게 하는 주요 이유는 무엇이라고 생각하십니까?(복수 선택 가능)

① 신고절차가 복잡하기 때문에
② 신고에 따른 법적 부담이 우려되기 때문에
③ 의료기관 이미지(평판) 손상이 우려되기 때문에
④ 내부에서 자체적으로 처리 가능하기 때문에
⑤ 기타: (직접 입력: _____)

35. 보안사고 신고율을 높이기 위해 필요한 지원은 무엇이라고 생각하십니까? (복수 선택 가능)

① 신고 절차 간소화
② 법적 보호 제공
③ 신고 인센티브 제공
④ 정보보안 교육 및 홍보 강화
⑦ 기타: (직접 입력: _____)

36. 귀 기관에서 운영하는 주요 정보시스템(진료정보 및 환자 서비스 등)에 다음의 각 정보보안 사항 적용 여부에 대해 응답해 주십시오.
(필요시 외부 아웃소싱 업체에서 응답 가능)

구분		도입(적용) 여부	
		예	아니오
인증	1) 아이디/비밀번호		
	2) 공인인증서		
	3) 다중요소인증(OTP, 2채널, 토큰, 보안카드, IC카드)		
	4) 본인확인인증(SMS, I-PIN, 신용카드)		
	5) FIDO 인증(지문·안면 등 생체기반)		
PC/단말기 보안	6) PC방화벽		
	7) 백신		
	8) PC키보드보안(Anti-keylogger)		
	9) 정보유출방지솔루션(DLP)		
	10) 패치관리 시스템(PMS)		
	11) 보조기억장치 제어솔루션(USB,이동식디스크등)		
	12) 프린터 출력물 보안		
	13) 개인정보 검색솔루션		
	14) 문서암호화(DRM)		

구분		도입(적용) 여부	
		예	아니오
네트워크 보안	15) 방화벽(FireWall)		
	16) 침입방지시스템(IPS)		
	17) 무선 침입방지시스템(W-IPS)		
	18) 침입탐지시스템(IDS)		
	19) 네트워크 접근통제(NAC)		
	20) 통합위협관리(UTM)		
	21) 전송구간 암호화(DMZ, 외부망 포함)		
	22) 가상사설망(VPN)		
	23) DDos 방지시스템		
	24) 망분리(물리적, 논리적)		
DB보안	25) DB 접근제어		
	26) DB 암호화(API, Plug-in, Hybrid,Token, TDE, File)		
	27) DB 사용자 비밀번호 암호화		
	28) 환자 고유식별정보 암호화		
서버보안	29) 서버백신(Linux, Windows Server)		
	30) 서버 접근제어(Secure OS, 접근권한, 계정 및 로그관 리 등을 위한 서버솔루션)		
어플리케이션 보안	31) 웹방화벽(WAF)		
	32) 유해사이트 차단시스템		
	33) 소스코드 점검 툴		
	34) 웹 스캐너		
	35) 웹서버 악성코드 탐지		
통합 보안 관리	36) 표준인증 프로토콜(OAuth, SAML, OIDC)		
	37) 통합계정권한관리(SSO)		
	38) 전사적보안관리(ESM)		
	39) 위협관리시스템(TMS)		
모바일 앱 보안	40) 앱 위변조 방지		
	41) 데이터 암호화		
	42) 보안 키패드		
	43) 인증서 중계		
	44) 모바일 SSO		

37. (31-36문항) 응답자 본인의 소속 및 직무

소속: _____, 직무: _____

※ 소속: 내부와 외부(아웃소싱) 구분하고 작성 부서명 기재
(예시) 내부(정보운영팀), 내부(정보보안팀), 내부(총무팀), 내부(의무기록실), 외부(외주업체) 등
※ 직무: 관리자(팀장급 이상) 및 담당자 구분하고 담당업무를 기재
(예시) 관리자, 정보보안 담당자, 정보보호 담당자, 네트워크 담당자, 개발자, 정보시스템운영 담당자 등

XI 정부 지원 및 정책 개선 요구사항

38. 정부나 공공기관이 의료기관 정보보안 업무 강화를 위해 가장 중점적으로 지원해야 할 사항은 무엇입니까?(1순위부터 3순위까지 선택하여 주십시오.)

1순위		2순위		3순위	

① 보안장비 도입 지원 (☞ 39문항으로 이동)
② 보안 예산 확대 (☞ 39문항으로 이동)
③ 법적/제도적 개선 (☞ 38-1문항으로 이동)
④ 정보보안 관련 전문 교육 제공 (☞ 39문항으로 이동)
⑤ 기타: (직접 입력_____) (☞ 39문항으로 이동)

38-1. (38문항 ③ 응답자만) 법적/제도적 개선이 필요한 정보보안 관련 사항은 무엇입니까?(1순위부터 3순위까지 선택하여 주십시오.)

① 보안관제 의무화 및 지원 법제화
② 개인정보보호법 강화
③ 중소병원 대상 보안 지원 확대
④ 침해사고 신고 절차 간소화
⑤ 기타 (직접 입력:_____)

1순위:_____, 2순위:_____, 3순위:_____

39. (38문항) 응답자 본인의 소속 및 직무

소속: _____, 직무: _____

※ 소속: 내부와 외부(아웃소싱) 구분하고 작성 부서명 기재
(예시) 내부(정보운영팀), 내부(정보보안팀), 내부(총무팀), 내부(의무기록실), 외부(외주업체) 등
※ 직무: 관리자(팀장급 이상) 및 담당자 구분하고 담당업무를 기재
(예시) 관리자, 정보보안 담당자, 정보보호 담당자, 네트워크 담당자, 개발자, 정보시스템운영 담당자 등

XII 보안관제 체계 도입 관련

40. 귀 기관에서는 보안관제 체계 도입이 필요하다고 생각하십니까?

① 예 (☞ 40-1문항으로 이동)

② 아니오 (☞ 41문항으로 이동)

40-1.(41문항 ① 응답자만) 귀 기관에서 보안관제 체계 도입의 필요성을 느끼는 주요 이유는 무엇이라고 생각하십니까?(1순위부터 3순위까지 선택하여 주십시오.)

1순위		2순위		3순위	

① 실시간 위협 탐지 및 차단

② 보안 사고 사전 예방

③ 법적 요구사항 준수 (개인정보보호법, 의료법 등)

④ 데이터 무결성 및 신뢰성 확보

⑤ 기타 (직접 입력:_____)

40-2.(40문항 ① 응답자만) 귀 기관에서 의료기관 보안관제 체계 도입시 기대하는 주요 효과는 무엇입니까? (1순위부터 3순위까지 선택하여 주십시오.)

1순위		2순위		3순위	

① 침해 사고에 대한 신속한 대응

② 인력 효율화 및 비용 절감

③ 일관성 있는 보안 정책 적용

④ 보안 시스템 통합 관리

⑤ 기타 (직접 입력:_____)

41. 보안관제 체계를 도입을 저해하는 요인은 무엇이라고 생각하십니까?
(1순위부터 3순위까지 선택하여 주십시오.)

1순위		2순위		3순위	

① 초기 구축 비용 부담
② (내부)전문 인력 부족
③ (내부)기술적 지식 부족
④ 보안관제 필요성에 대한 경영진의 인식 부족
⑤ 기타 (직접 입력:_____)

42. 보안관제 체계 도입을 촉진하기 위한 가장 필요한 지원은 무엇이라고 생각하십니까?(1순위부터 3순위까지 선택하여 주십시오)

1순위		2순위		3순위	

① 정부의 재정 지원
② 전문 기술지원 및 교육
③ 클라우드 서비스 제공
④ 법적 요건 강화
⑤ 보안 수준 점검 시스템
⑥ 보안관제 체계 구축 시 상담 창구
⑦ (직접 입력:_____)

43. 보안관제 도입 효과를 높이기 위해 가장 필요한 요소는 무엇이라고 생각하십니까?(1순위부터 3순위까지 선택하여 주십시오)

1순위		2순위		3순위	

① 실시간 위협 탐지 기술
② 보안 인력 확충
③ 비용 효율적인 솔루션
④ 전 직원 보안 교육 강화
⑤ 기타 (직접 입력:_____)

44. 실시간 보안관제 체계가 보안 사고를 예방하는데 얼마나 효과적일 것이라 생각하십니까?

① 매우 효과적이다	☞ 45문항으로 이동
② 효과적이다	☞ 45문항으로 이동
③ 보통이다	☞ 45문항으로 이동
④ 효과적이지 않다	☞ 44-1문항으로 이동
⑤ 전혀 효과적이지 않다	☞ 44-1문항으로 이동

44-1. (44문항 ④, ⑤ 응답자만) 효과적이지 않다고 생각하신 이유를 자유롭게 기술해주십시오.

(직접 입력)

45. 의료법 및 인증체계(ISMS-P, EMR 인증)에 실시간 보안관제 의무화를 포함해야 한다고 생각하십니까?

① 매우 필요하다	☞ 46문항으로 이동
② 필요하다	☞ 46문항으로 이동
③ 보통이다	☞ 46문항으로 이동
④ 필요하지 않다	☞ 45-1문항으로 이동
⑤ 전혀 필요하지 않다	☞ 45-1문항으로 이동

45-1.(45문항 ④, ⑤ 응답자만) 실시간 보안관제가 필요하지 않다고 생각하신 이유를 자유롭게 기술해주십시오.

(직접 입력)

46. 중소 의료기관을 위한 클라우드 기반 보안관제 서비스 도입에 대해 어떻게 생각하십니까?

① 매우 긍정적이다 ☞ 47문항으로 이동
② 긍정적이다 ☞ 47문항으로 이동
③ 보통이다 ☞ 47문항으로 이동
④ 부정적이다 ☞ 46-1문항으로 이동
⑤ 매우 부정적이다 ☞ 46-1문항으로 이동

46-1.(46문항 ④, ⑤ 응답자만) 클라우드 기반 보안관제 서비스를 부정적으로 생각하신 이유를 자유롭게 기술해주십시오.

(직접 입력)

47. 의료정보보호 관제서비스를 이용하는 장점은 무엇이라고 생각합니까?
(1순위부터 3순위까지 선택하여 주십시오.)

1순위		2순위		3순위	

① 조직 및 인력 효율화로 인건비 절감
② 24*365 실시간 감시를 통한 업무 중단 최소화
③ 보안관제를 위한 설비 및 투자비용 절감
④ 보안전문가 활용에 따른 보안전문성 강화

⑤ 보안시스템 통합관리
⑥ 일관성 있는 보안정책 적용
⑦ 침해사고 등에 대한 신속한 대응
⑧ 기타 (직접 입력:_____)

48. 귀 기관에서 정보보안이 가장 취약하다고 생각하는 부분은?
예: 사용자 인증 취약, 단말 취약, 네트워크 구성 현황 취약, 정보시스템 취약 서비스 사용, 시큐어 코딩 미준수 등

(직접 입력)

49. (40-48문항) 응답자 본인의 소속 및 직무

소속: _____, 직무: _____

※ 소속: 내부와 외부(아웃소싱) 구분하고 작성 부서명 기재
(예시) 내부(정보운영팀), 내부(정보보안팀), 내부(총무팀), 내부(의무기록실), 외부(외주업체) 등
※ 직무: 관리자(팀장급 이상) 및 담당자 구분하고 담당업무를 기재
(예시) 관리자, 정보보안 담당자, 정보보호 담당자, 네트워크 담당자, 개발자, 정보시스템운영 담당자 등

Ⅻ 의료정보보호센터 및 보안관제 가입 활성화 등

50. 귀 기관은 의료정보보호센터 보안관제서비스(ISAC)에 가입하였습니까?

① 예 ☞ 50-1문항으로 이동
② 아니오 ☞ 51문항으로 이동

50-1. 의료정보보호센터와의 협력체계가 얼마나 잘 구축되어 있다고 생각하십니까?

① 매우 잘 구축되어 있다
② 잘 구축되어 있다
③ 보통이다
④ 잘 구축되어 있지 않다
⑤ 전혀 구축되어 있지 않다

50-2. 의료정보보호센터와 협력하여 더 개선해야 할 부분은 무엇이라고 생각하십니까?

① 정보 공유 시스템 다변화
② 공유 기술 교육 및 훈련
③ 협력체계 정례화
④ 추가적인 지원 시스템 도입
⑤ 기타 (직접 입력:_____)

51. 보안관제 서비스 가입 활성화를 위해 필요한 지원은 무엇이라고 생각하십니까?

① 비용 지원
② 장비 도입 지원
③ 기술적 컨설팅
④ 법적 지원 강화
⑤ 기타 (직접 입력:_____)

52. 보안관제 가입을 의무화하는 정책에 대해 어떻게 생각하십니까?

① 매우 필요하다
② 필요하다
③ 보통이다
④ 필요하지 않다
⑤ 전혀 필요하지 않다.

52-1. (52문항 ①, ② 응답자만) 필요하다고 생각한 이유를 간략히 기술해 주십시오.

(직접 입력)

53. (50-52문항) 응답자 본인의 소속 및 직무

소속: _____, 직무: _____

※ 소속: 내부와 외부(아웃소싱) 구분하고 작성 부서명 기재
(예시) 내부(정보운영팀), 내부(정보보안팀), 내부(총무팀), 내부(의무기록실), 외부(외주업체) 등
※ 직무: 관리자(팀장급 이상) 및 담당자 구분하고 담당업무를 기재
(예시) 관리자, 정보보안 담당자, 정보보호 담당자, 네트워크 담당자, 개발자, 정보시스템운영 담당자 등

XIV 기타: LLM(대형언어모델) 기반 AI 서비스 등

54. 귀 기관에서는 LLM(대형언어모델) 기반 인공지능(AI) 서비스를 도입하고 있습니까?

① 이미 도입함 ☞ 55문항으로 이동
② 시험 도입 중 ☞ 55문항으로 이동
③ 도입 예정 ☞ 55문항으로 이동
④ 도입 계획 없음 ☞ 59문항으로 이동
⑤ 모르겠음 ☞ 59문항으로 이동

55. 도입된(또는 도입 예정인) LLM서비스의 주요 활용 분야는 무엇입니까? (복수 응답 가능)

① 임상 지원(진단, 판독 등)
② 행정 업무 자동화(문서 요약, 차트 정리 등)
③ 환자 상담 챗봇
④ 연구 및 데이터 분석
⑤ 기타(직접 입력: _____)

56. LLM서비스 도입(또는 도입 예정인) 이후, 새로운 정보보안 이슈나 우려 사항은 무엇입니까? (복수 응답 가능)

① 민감정보(환자 개인정보 등) 유출
② 데이터 주권 문제
③ AI 모델 조작 및 악성 입력
④ 허가 받지 않은 내부 직원의 무단 접근
⑤ 외부 해킹 시도
⑥ 데이터 익명화·암호화 부족
⑦ 규정 미준수(예: 개인정보보호법, HIPAA 등)
⑧ 기타(직접 입력: _____)

57. LLM서비스 도입 후 실제로 경험한 정보보안 사고 사례가 있다면 간단히 설명해 주십시오.
(직접 입력: _____)

58. 귀 기관에서는 LLM 서비스에 특화된 보안툴을 도입하고 있습니까?

① 이미 도입함 ☞ 58-1문항으로 이동
② 시험 도입 중 ☞ 58-1문항으로 이동
③ 도입 계획 없음 ☞ 59문항으로 이동
④ 모르겠음 ☞ 59문항으로 이동

58-1. 도입된(또는 도입 예정인) LLM 서비스 보안툴의 종류는 무엇입니까?
(복수 응답 가능)

① AI 트래픽 모니터링 툴
② 입력/출력 데이터 필터링 솔루션
③ 모델 접근제어 및 인증 솔루션
④ 모델 및 데이터 암호화 툴
⑤ AI 시스템 취약점 점검 및 위협 탐지 솔루션
⑥ 기타(직접 입력: _____)

58-2. 도입된 LLM 서비스 보안툴에 대한 만족도는 어떠십니까?

① 매우 높다
② 높은 편이다
③ 보통이다
④ 낮은 편이다
⑤ 매우 낮다

59. (54-58문항) 응답자 본인의 소속 및 직무

소속: _____, 직무: _____

※ 소속: 내부와 외부(아웃소싱) 구분하고 작성 부서명 기재
(예시) 내부(정보운영팀), 내부(정보보안팀), 내부(총무팀), 내부(의무기록실), 외부(외주업체) 등
※ 직무: 관리자(팀장급 이상) 및 담당자 구분하고 담당업무를 기재
(예시) 관리자, 정보보안 담당자, 정보보호 담당자, 네트워크 담당자, 개발자, 정보시스템운영 담당자 등

Abstract

Policy Strategies for Enhancing Cybersecurity in Healthcare Institutions

Project Head: Lee, Ki-ho

Advances in artificial intelligence (AI) and digital technology are enabling various innovations in the healthcare sector—such as improved diagnostic and treatment efficiency and the expansion of personalized medical services—while accelerating the adoption of digital approaches in healthcare environments. As the generation and utilization of medical data expand, driven by medical information systems such as electronic medical records (EMR), picture archiving and communication systems (PACS), and online prescription systems (OCS), reliance on digital technology in healthcare services continues to grow. However, the proliferation of this data-driven healthcare environment simultaneously heightens the importance of personal data protection and cybersecurity. Due to the sensitive nature of the personal and medical data they hold, healthcare institutions have become prime targets for cyberattacks. Indeed, the importance of cybersecurity has been increasingly emphasized as incidents such as ransomware attacks, data breaches, and disruptions to medical services continue to occur both domestically and internationally.

This study aimed to comprehensively analyze the cyber

Co-Researchers: An, Suin · Lee, Hyejung

threats to and current security status of healthcare institutions and, based on this analysis, to derive policy measures to strengthen their cybersecurity. To this end, the study reviewed prior domestic and international research, conducted comparative analyses of policies and systems, examined cyber incident cases, and conducted a cybersecurity survey targeting tertiary general hospitals and general hospitals.

The findings reveal that cybersecurity threats to healthcare institutions are continuously increasing alongside digital transformation, and that security vulnerabilities are expanding, particularly in complex environments where various technologies—such as medical information systems, medical devices, cloud services, and telemedicine platforms—are interconnected. The primary causes of security incidents are often linked to deficiencies in basic security management—such as failure to apply patches, inadequate management of default accounts, and neglect of VPN vulnerabilities—rather than sophisticated hacking techniques. These incidents are found to directly impact patient safety and the continuity of medical services, leading to delays in treatment, disruptions to surgical schedules, and data loss. Furthermore, healthcare institutions face structural challenges, including insufficient security budgets, a shortage of specialized personnel, inadequate training, and poor management of supply chain security. Additionally, the lack of robust systems for quantifying economic damages limits the avail-

ability of foundational data necessary for effective policy design.

Analysis of policies and regulations reveals that while general information security laws, such as the Personal Information Protection Act, provide relatively clear management frameworks covering the entire incident lifecycle, the Medical Services Act framework is skewed toward prevention and detection, resulting in weaker systems for response, recovery, and post-incident evaluation. Furthermore, existing security certification systems, such as EMR certification and ISMS-P, also have limitations in comprehensively managing the overall security levels of healthcare institutions.

In summary, cybersecurity in healthcare institutions emerges as a complex management challenge involving multiple factors—including organizational culture, budget priorities, personnel capabilities, data governance, and collaborative networks—that are more than just technical issues. Accordingly, key policy priorities include strengthening security governance in healthcare institutions, improving incident reporting and response systems, establishing comprehensive certification systems, institutionalizing regular security education and training, enhancing security management for medical devices and supply chains, and promoting threat intelligence sharing.

In terms of future policy directions, short-term measures include expanding participation in the Healthcare Information

Security Analysis and Coordination Center (ISAC), promoting security monitoring services, and establishing ransomware response protocols. In the medium term, efforts should focus on introducing security certification systems for medical devices and supply chains, developing automated incident reporting platforms, and institutionalizing cybersecurity workforce training. In the long term, it is essential to establish a national healthcare cybersecurity ecosystem by establishing a prevention-oriented legal and institutional framework and advancing AI-based threat detection technologies.

Cybersecurity in the healthcare sector serves as a critical foundation not only for protecting the lives and health of citizens but also for the sustainable development of the digital healthcare industry. Therefore, sustained policy attention and increased investment at the national level are required.

Key words: Cybersecurity, Cyber threats, Cyber attacks, Cyber incident