연구 1-04-2026-005-15

SSIS

이슈&트렌드

발행인 김현준 | **발행처** 한국사회보장정보원 | **발행일** 2026년 4월 17일

2026 Vol. 03

| 제도·전달체계 |

의료기관 진료정보보호를 위한 제언

고려대학교 의료원 의학지능정보본부장 | 박홍석 교수

SSiS 한국사회보장정보원

요 약

01 의료분야 사이버 위협 동향

- 국내 의료기관 침해사고 인지 2020년 18건 → 2024년 71건(약 3.9배 급증), 중소의료기관 취약성 심각

02 국내 의료기관 보안 역량 및 인프라 한계

- 상급종합병원 평균 보안예산 8.6억 원 대비 중소 병원급(2~5천만 원 수준)의 구조적 보안 취약성 심각

03 국내 법·제도 및 ISAC 운영 현황

- 의료법 개정안 계류 중(2025.2), 의료ISAC 법적 권한·예산 타 분야 대비 미흡

04 국내외 벤치마킹 및 시사점

- 독일 KHZG(지원+의무 결합형), 미국 H-ISAC(위협정보 공유 허브) 모델 적용 검토 필요

05 제언

- 의료법 내 '진료정보보호 지원제도' 신설, 의료ISAC 고도화를 통한 국가적 의료 연속성 보장 및 위험기반 차등 지원체계 구축 등 제언

Ⅰ 서론

- 2025년 대한민국은 전례 없는 사이버 보안 위기에 직면함. SK텔레콤 USIM 정보 2,300만 건 유출(2025.4), KT 서버 해킹(2025.11), 예스24 랜섬웨어 연속 피해(2025.6·8)까지 국가 기반시설 연쇄 침해 사고가 국민 신뢰를 심각하게 훼손함. 의료 분야 역시 예외가 아님.
- 2026년 2월 국내 상급종합병원의 전산망이 잇따라 랜섬웨어에 감염된 사건은 국내 의료기관 사이버 위협이 현실화되고 있음을 보여주는 상징적 사례임. 의료 정보는 다크웹에서 높은 가격에 거래되는 주요 표적을 넘어, 침해 발생 시 해당 지역의 응급의료 체계와 환자 진료망 전체를 마비시키는 사회적 재난의 뇌관임. 의료기관의 사이버 보안 붕괴는 단순한 기업의 재산상 손해나 개인정보 유출 사고가 아니며, 진료 지연 및 환자 사망으로 직결되는, 국민 생명과 직결된 국가 안보 위협으로 다루어져야 함.
- 독일 뒤셀도르프 대학병원 사례(2020)는 랜섬웨어 공격으로 응급 환자 사망에 직접적 영향을 미친 사건으로 기록되어 있으며, 미국 Change Healthcare 사건(2024.2)은 단일 기관 침해가 전국 의료 청구·결제 시스템을 수주간 마비시킨 공급망 위기의 교훈을 남김.
- 이에 본고에서는 의료기관 진료정보보호를 위한 환경 분석, 주요 이슈, 그리고 정책 제언을 제시하고자 함.

1.1 환경 및 현황 분석

◆ 1.1.1 의료분야 사이버 위협 동향

- 의료기관을 대상으로 한 사이버 공격은 단순 정보 유출에서 진료 서비스 마비로 진화하고 있음. 공격 유형 측면에서는 ▲랜섬웨어 ▲DDoS ▲계정 탈취·웹셸 ▲공급망 공격(제3자·협력업체 경유)이 복합적으로 활용되고 있으며, 공격 주체는 금전적 목적의 사이버 범죄 조직에서 국가 배후 조직으로 확대되고 있음.
- 국내 의료기관 침해사고는 최근 5개년 통계 기준 2020년 18건에서 2024년 71건으로 약 3.9배 증가하였음. 주요 국내 사례로는 ▲서울상급종합병원 웹셸 공격으로 약 83만 명 개인정보 탈취(2021, 북한 소행 추정) ▲지방상급종합병원 권역심뇌혈관질환센터 관리자 페이지 해킹 및 텔레그램 공개(2024.11) ▲대한결핵협회 백업 개발서버 해킹 15만여 명 정보 해외 유출(2024.9) 등을 들 수 있음.

◆ 1.1.2 국내 사이버 위협 동향

- 한국인터넷진흥원(KISA)의 침해사고 통계에 따르면 2023년 전체 침해사고는 전년 대비 12% 증가한 1,277건, 2024년 상반기에는 전년 동기(664건) 대비 35% 급증한 899건으로 집계되었음. 웹셸(56%) 및 DDoS(17%) 공격이 주를 이루고 있으며, 공급망 공격 경로가 빠르게 증가하는 추세임.
- 의료 분야에서는 2024년 보안관제 탐지 기준 상급종합병원에 대한 침해 시도가 57,623건(전체 76%)으로

집중되어 있으나, 실제 침해사고 발생은 의원급(49.5%)에서 가장 높게 나타남. 이는 보안관제에 가입하지 않은 중소 의료기관이 탐지 자체를 하지 못하고 있는 구조적 사각지대를 시사함.

II 주요 이슈

2.1 국내 의료기관 보안 역량 및 인프라 한계

- 의료기관 간 보안 역량 격차는 구조적·만성적 문제로 고착화되어 있음. 상급종합병원은 평균 보안예산 8.6억 원, 전담 인력 2.1명 수준에서 ISMS 기반 거버넌스를 유지하는 반면, 중소 병원급 기관은 2~5천만 원 예산에 겸직 인력 0.6명에 불과함.

의료기관 유형	보안 역량 현황
상급종합병원	보안예산 평균 약 8.6억원, 전담인력 2.1명, ISMS 인증 기반 거버넌스 운영
종합병원	보안예산 평균 약 3.9억원 수준, 외부 보안관제 서비스 활용
병원급	보안예산 2~5천만원, 주요 통제(MFA·백업·망분리) 도입률 저조
의원급	보안예산 수백만원 이하(추정), 기본 보안도구조차 미비

- 실태조사(표본 135개 기관, 2024) 결과 예산 부족(53.5%)과 전문인력 부족이 보안체계 도입·운영의 주된 장애요인으로 확인되었음. 개별 기관에 의존하는 자율적 보안 구축 방식은 국가 전체 의료망의 방어 수준을 가장 취약한 중소기관 수준으로 하향 평준화시키는 구조적 한계를 지니고 있음. 이는 단순한 예산 및 인력 부족의 문제를 넘어, 지역 주민의 1차 진료를 담당하는 중소 의료기관이 사이버 보안 위협에 구조적으로 노출되어 있음을 시사함.

2.2 국내 법·제도 및 ISAC 운영 현황

- 현행 의료법·개인정보보호법·정보통신망법 체계에는 의료기관에 대한 재정·행정 지원의 범위·대상·절차와 의무·평가·환류 연계가 불명확함. 2025년 2월 발의된 의료법 개정안(전진숙 의원안)은 ▲전산시스템 보호를 위한 기술적 조치 의무 신설 ▲행정·재정적 지원 근거 신설 등을 주요 골자로 하나, 현재 국회에 계류 중임.
- 의료정보보호센터(의료ISAC)는 진료정보 침해사고 신고·대응 지원, 취약점 점검, 교육·홍보 등 ISAC 기능을 수행하고 있으나, 타 분야(금융·정보통신) ISAC과 비교 시 법적 강제성, 예산(1개 기관당 투입 예산), 인력 측면에서 현저히 열악함. 특히 보안관제 회원기관 가입률이 낮아 탐지·대응 사각지대가 광범위하게 존재함.

2.3 국내외 벤치마킹 및 시사점

- 해외 주요국의 의료기관 정보보호 지원 사례를 비교하면 다음과 같음.

국가	주요 지원 모델
독일 (KHZG)	연방·주정부 약 43억 유로 디지털화 기금 조성, 지원금의 최소 15% 이상 정보보안 의무 투자. '지원-의무-제재'의 폐쇄루프 구현
일본	의료법·개인정보보호법 기반 보안체계 구축 의무 부과, 중소병원 대상 보안설비 보조·현물형 실행지원 패키지(전수점검·백업·관제·훈련) 표준화
미국 (H-ISAC)	HIPAA/HITECH 규범 준수 의무화, 부문 허브형 정보공유체계(H-ISAC)와 연방 CISA 연계, 위협정보 공유·경보·컨설팅 기능 중심

- 국내 시사점으로는 ▲지원과 의무를 동시에 설계(보조금 집행조건에 필수 보안통제 이행 명시) ▲현물형 실행지원 패키지 표준모듈화 ▲의료ISAC의 법적 근거 명문화 및 위협정보 공유 허브 기능 강화가 필요함.

2.4 국내외 진료정보 침해사례 분석과 손실 추정

- 진료정보 침해사고로 인한 손실은 직접 손실(33.8%)보다 간접 손실(66.2%)이 약 2배 높음. 진료 중단으로 인한 기회비용이 가장 큰 비중을 차지하며, 500병상 규모 의료기관의 경우 하루 완전 중단 시 약 8.8억 원의 손실이 발생하고, 평균 복구 기간 40일 기준 누적 손실은 약 120억 원에 달함.

주요 해외 침해사고 손실 사례

- 독일 뒤셀도르프 대학병원(2020): 랜섬웨어로 응급 환자 사망 발생 → 의료 사이버 공격이 생명위협으로 직결됨을 입증
- 미국 Change Healthcare(2024.2): 약 1억 명 민감 의료정보 유출, 전국 의료 청구·결제 시스템 수주간 마비
- 영국 Synnovis(NHS, 2024.6): 약 3억 건 환자 정보 도난, 수천 건 진료·수술 중단, 약 602억원 손실 추산
- 국내 침해사고 급증: 2020년 18건 → 2024년 71건, 향후 5년간 누적 손실액 약 1조 5,324억원 전망

Ⅲ 제언

3.1 한국형 의료보안 정책 목표·방향

- 헌법 제36조 제3항은 국민 보건에 관한 국가 보호 의무를 명시하고 있음. 디지털 전환 환경에서 '진료연속성 보호'와 '진료정보의 안전한 처리·보관'은 실질적인 건강권 보장의 핵심 요소임. 진료정보는 개별 환자의 사적 정보이면서 동시에 감염병 대응·보건정책·건강보험 운영·의학 연구 등 공공 기능에 활용되는 공공재적 성격을 가짐.

- 본 연구는 한국형 의료보안 정책을 다음 세 축으로 설계할 것을 제안함.
  - 의료보안에 대한 국가책무성 확립: 헌법상 건강권에 기초한 국가–의료기관 공동책임 모델
  - 위험·연속성 기반 지원체계 구축: 병원 규모·위험도별 차등 기준 설정 및 예방–대응–복구 전 생명주기 대응
  - 의료ISAC 중심 민관 협력·통합 관제체계: 의료정보보호센터를 법적 근거 기반 위협정보 공유 허브로 격상

3.2 법·제도 정비

- 의료법 내 「진료정보보호 지원제도(가칭)」 신설 조항을 통해 지원–의무–평가–환류가 결합된 정합적 법제 패키지를 마련해야 함.
  - 기술적 보호조치 의무 신설: 전자의무기록·전산시스템 보호를 위한 기술적 조치 법정 의무화 (의료법 제23조 개정)
  - 재정·행정 지원 근거 명문화: 예방·대응 역량 제고를 위한 정부의 재정·행정 지원 법정화
  - 최소보안필수기준(Baseline Security) 제정: 병원 유형·위험등급별 필수 보안 통제 항목 고시화
  - 기본권 영향평가 도입 검토: 공공기관이 의료 AI·자동화 시스템 도입 시 사전 영향평가 제도화
  - 타 부처 협의체 구성: 보건복지부·과기정통부·질병관리청·KISA·의료정보보호센터 역할 분담 명확화
- 특히, 독일 KHZG 모델처럼 지원금 집행 조건에 필수 보안통제 이행을 명시하고, 미준수 시 환수·제재 조항을 하위법령에 구체화하는 '지원–의무–제재'의 폐쇄루프를 설계하는 것이 핵심임.

3.3 의료ISAC 고도화·거버넌스

- 현 의료정보보호센터를 법적 근거를 갖춘 「의료ISAC」으로 격상하고, 타 분야 ISAC 및 국제 Health-ISAC과의 연계를 통해 국가 차원의 통합 관제·정보공유 허브로 육성해야 함.
  - 법적 근거 명문화: 의료법 또는 진료정보보호 지원법(가칭)에 의료ISAC의 위협정보 수집·공유·관제 지원 기능 명시
  - 예산·인력 확충: 타 분야 ISAC 수준으로 1개 기관당 투입 예산 현실화, 전문 분석 인력 증원
  - 위협정보 수집·분석·공유 표준화: IOC·TTP 기반 위협 인텔리전스 배포, '진료중단 방지 체크리스트' 등 현장 친화형 경보 포맷 개발
  - AI 기반 자동화 도입: 이상 탐지·분석 자동화로 소수 인력으로도 광범위한 관제 기능 수행
  - 다기관 공동 대응체계: 복지부·KISA·경찰청 등 관계기관과 합동 대응 체계 상시화
  - 인센티브 기반 참여 유도: ISAC 가입·정보공유 기관에 대한 보안비용 지원, 인증 평가 가점, 건강보험 수가 인센티브 제공

3.4 사회적 합의·커뮤니케이션 전략

- 진료정보보호 강화를 위한 법·제도 정비는 의료기관의 수용성과 국민의 사회적 합의를 전제로 해야 함. 의무 강화에 비해 지원 근거·범위의 불명확성으로 인한 의료계 단체(의협·치협 등)의 우려를 해소하기 위한 소통 전략이 필수적임.
  - 공청회·포럼을 통한 이해관계자 합의 도출: 의료단체·정부·시민사회·보안 전문가가 참여하는 정기적 공론화 과정 운영
  - '진료정보보호 = 국민건강권 보호' 프레임 확산: 보안 투자가 규제 부담이 아닌 환자 안전과 의료기관 지속가능성을 위한 투자임을 대국민 홍보
  - 가이드라인·교육 콘텐츠 제작·배포: 병원 규모·유형별 맞춤형 진료정보보호 가이드라인 및 온라인 교육 콘텐츠 개발·보급
  - 언론·정책 홍보 전략 수립: 침해사고 피해 현황, 제도 효과성 데이터를 활용한 정책 근거 기반 홍보 체계 구축

Ⅲ 맺음말

- 의료기관 진료정보 침해사고는 단순한 데이터 유출을 넘어 환자의 생명과 국민 건강권을 위협하는 국가적 과제로 부상하였음. 국내 상급종합병원 랜섬웨어 사건을 포함한 국내 의료기관 침해사고의 급증은 더 이상 개별 기관의 문제가 아니라 국가 보건 안보의 문제임을 명확히 보여줌.
- 본 연구의 핵심 제언을 요약하면, ▲의료법 내 「진료정보보호 지원제도」 신설을 통한 법적 근거 확보 ▲위험기반 차등 지원으로 중소 의료기관 보안 사각지대 해소 ▲의료ISAC 고도화로 통합 관제·위협정보 공유 체계 확립 ▲독일형 지원-의무-제재 결합 모델 도입으로 지속가능한 진료정보보호 생태계 구축임.
- 진료정보보호는 더 이상 미룰 수 없는 최우선 국가 보건 안보 과제로서, 중단 없는 환자 치료 환경을 보장하기 위한 조속한 입법과 파격적인 제도화를 강력히 촉구함.

참고문헌

고려대학교 박홍석 (2025. 12.).「진료정보보호 강화를 위한 제도적 지원방안 연구」

한국인터넷진흥원(KISA). (2024).「2024년 상반기 사이버 위협 동향 보고서」.

한국사회보장정보원. (2024. 12.).「2024년 의료기관 정보보안 강화 지원전략 수립 보고서」.

보건복지부. (2025. 2. 11.). 의료법 일부개정법률안(전진숙 의원 대표발의).

IBM Security. (2024). Cost of a Data Breach Report 2024.

OECD. (2024. 6.). Using AI to Manage Minimum Income Benefits and Unemployment Assistance. OECD Artificial Intelligence Papers No. 21.

Ransomware claims first fatality as healthcare under renewed assault. Computer Fraud & Security. 2020;2020(10):1-3.

IBacademy. (2020. 12. 15.). KHZG: The role of IT security in the digitalized hospital.

Health-ISAC. www.health-isac.org

SSIS 한국사회보장정보원 KOREA SOCIAL SECURITY INFORMATION SERVICE

04554 서울특별시 광진구 능동로 400 보건복지행정타운
대표전화 02-6360-6114 팩스 02-6360-6360 www.ssis.or.kr

집필자 박홍석 교수 고려대학교 의료원 의학지능정보본부장
문의 02-6360-6114