Headline

의료기관을 겨냥한 사이버 공격 증가와 보안 대응 전략

EQST 사업그룹 EQST Lab 팀 김세용 수석

■ 개요

디지털 기술의 발전은 의료 서비스의 질을 향상시키는 한편, 새로운 형태의 보안 위협도 함께 초래하고 있다. 병원은 방대한 양의 개인정보와 진료 데이터를 보유하고 있으며, 다양한 의료기기들이 네트워크로 연결된 복합적인 IT 환경에서 운영 중이다. 특히 24 시간 작동되는 시스템의 경우, 시스템 중단이 환자의 생명과 직결될 수 있어 점검이나 유지보수가 자유롭지 않다. 이와 같은 특수성은 공격자에게 표적이 되며, 이를 노린 해킹, 랜섬웨어, DDoS 와 같은 시스템 마비형 공격이 지속적으로 시도되고 있다.

구분	계	발생유형		
		DDoS 공격	악성코드 감염·유포 (랜섬웨어)	시스템해킹
2020 년	5	0	5(5)	0
2021 년	5	2	1(1)	2
2022 년	23	1	5(5)	17
2023 년	39	1	7(6)	31
2024 년	57	0	4(4)	53
계	129	4	22(21)	103

* 출처 : 보안뉴스(자료 : 한국인터넷진흥원, 단위 : 건)

표 1. 의료기관 침해사고

사고 증가 추세

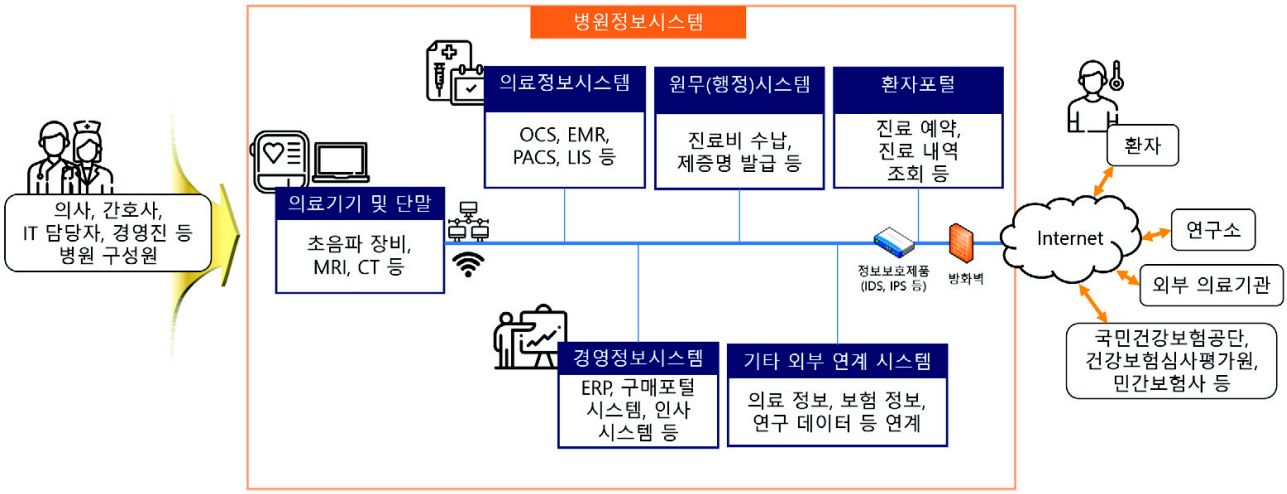
최근 몇 년간 병원을 대상으로 한 사이버 공격은 국내외에서 꾸준히 증가하고 있다. 해외에서는 대형 병원 네트워크가 랜섬웨어에 감염되어 수술 일정이 취소되거나 환자 기록 접근이 차단되는 사례가 있었으며, 국내에서는 환자 정보 유출 사고가 발생했다.

이러한 사건들은 의료기관의 보안 수준에 대한 우려를 키우고 있으며, 병원 내 정보자산과 시스템 보호에 대한 필요성을 더욱 부각시키고 있다.

시스템 복잡성

병원의 정보기술 인프라는 전자의무기록(EMR), 병원 내 네트워크, 의료장비 시스템 등으로 구성되어 있으며, 진료 편의성과 업무 효율성을 위해 지속적으로 디지털화되어 왔다.

하지만 그 이면에는 여러 보안 취약점이 존재한다. 예를 들어, 외부 협력업체 시스템과의 연계, 인터넷을 통한 장비 접근, 구 버전 소프트웨어의 지속적 사용 등이 해커의 주요 침투 경로로 악용될 수 있다.



* 출처 : 국가정보원 병원정보시스템 보안가이드라인(2025.4)

그림 1. 병원정보시스템

정책 대응 현황

사이버 위협이 현실화되면서 정부 차원의 대응도 강화되고 있다. 보건복지부, 국가정보원, 한국인터넷진흥원(KISA) 등 관계 기관은 의료기관의 보안 역량 강화를 위한 정책적 가이드라인을 마련하고 있으며, 그 중에서도 2025 년 4 월 발표된 '병원정보시스템 보안 가이드라인'은 현장의 실무자가 참고할 수 있는 구체적인 기준을 제시하고 있다. 이 가이드는 병원이 보안 체계를 점검하고, 보유 자산을 식별하며, 다양한 위협에 대응할 수 있도록 기반을 마련하는 데 목적이 있다.

■ 병원 보안의 구조적 취약성

운영 환경의 제약

의료기관은 생명과 직결된 진료를 수행하는 조직 특성상, 연속적인 시스템 운영이 절대적으로 요구된다. 그로 인해 병원은 일반 기업과 달리 시스템 점검, 네트워크 변경, 보안 패치 적용 등을 자유롭게 시행하기 어렵다. 또한, 각 진료과와 외부 협력 조직이 병원 시스템에 접근하는 구조는 보안 정책을 일관되게 적용하기 어렵게 하는 요인이 된다.

기술 인프라의 노후화

일부 병원에서 사용 중인 정보 시스템은 개발된 지 오래되어 운영체제가 구형이거나, 보안 패치가 더 이상 제공되지 않는 상태로 운용되고 있다. 전자의무기록(EMR), 처방전달시스템(OCS), 의료영상저장전송시스템(PACS) 등은 서로 독립적으로 구축되어 있어 통합 관리가 어렵고, 이들 간 연동을 위한 인터페이스는 새로운 보안 취약점의 발생 가능성을 높이고 있다.

의료기기의 보안 한계

병원 내 다양한 의료기기는 진단, 치료, 감시 목적으로 사용되며 네트워크로 연결되는 경우가 많다. 그러나 상당수 기기는 개발 당시부터 보안을 고려해 설계되지 않았고, 구형 운영체제 또는 변경되지 않은 기본 계정·비밀번호 상태로 운용되는 경우가 있다. 또한 펌웨어가 업데이트되지 않아 취약점이 장기간 방치되는 상황도 발생한다. 의료기기는 고가의 장비인 만큼 교체가 현실적으로 어려우며, 감염 시 내부망을 통해 병원 전체 시스템에 영향을 줄 수 있는 위험 요소가 된다.

외부 연계 시스템의 위험

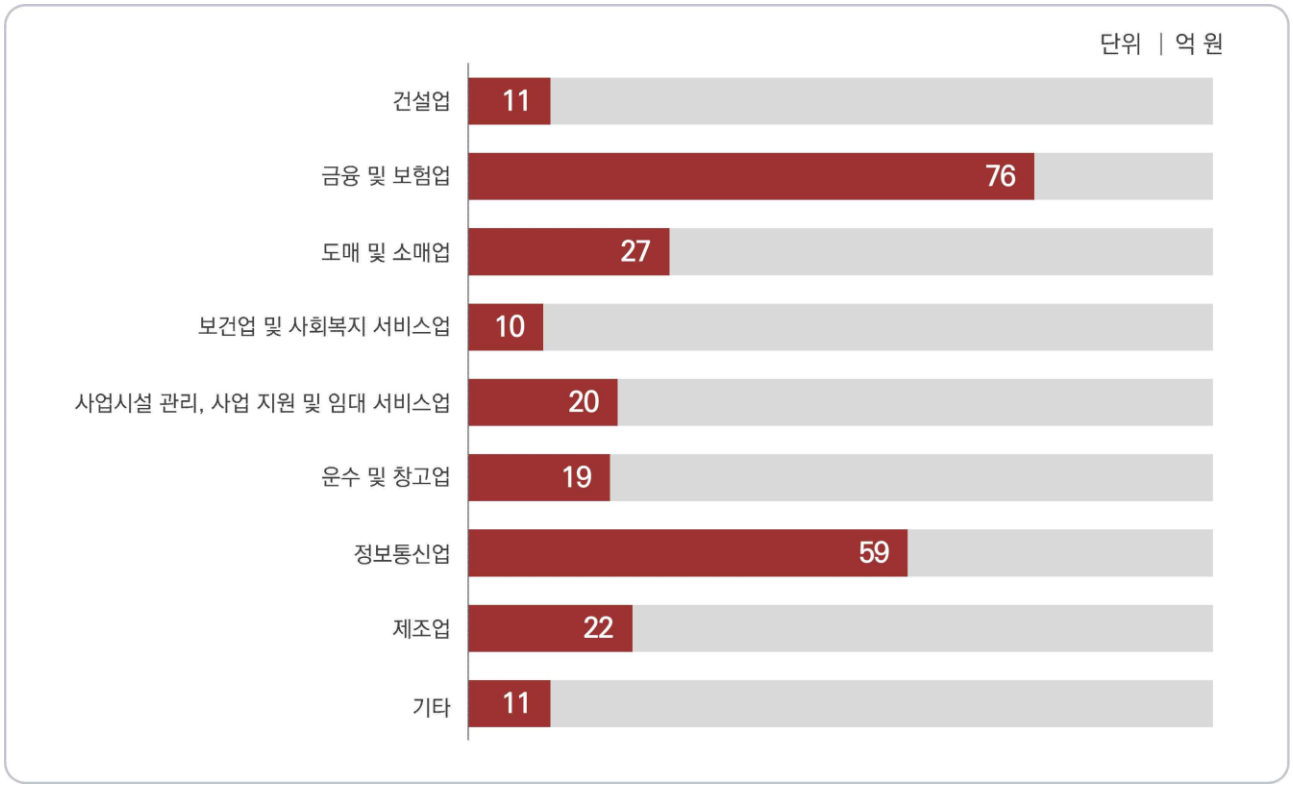
원격진료, 클라우드 기반 플랫폼, 원내외 협력 시스템 등은 병원 네트워크의 경계를 점점 확장 시키고 있으며, 이 과정에서 새로운 공격 지점이 형성된다. 외부에서 사용하는 VPN, API 연동 포인트, 진료정보 교류시스템 등은 인증 부족, 암호화 미적용, 접근통제 부재와 같은 문제로 인해 해킹에 취약한 환경이 될 수 있다.

보안 책임 체계의 부재

병원 내 정보보안에 대한 인식은 상대적으로 낮은 편이다. 또한, 전문적이고 독립적인 보안 조직이 부재하고 전담 예산이 확보되지 않는 경우가 많다. 특히 중소형 병원의 경우, 위기 상황이 발생해도 신속하게 대응하기 어려우며, 사고 분석이나 재발 방지를 위한 체계적인 대응도 쉽지 않다. 이러한 조직적 한계는 기술적 취약점보다도 더 본질적인 보안 위협이 될 수 있다.

보안 투자와 인식의 한계

정보보호의 중요성이 점차 부각되고 있음에도 불구하고, 실제 의료기관의 보안 투자는 여전히 낮은 수준에 머물러 있다. 한국인터넷진흥원(KISA)이 2024 년에 12 월에 발표한 조사에 따르면, 의료 업종의 정보보호 투자액은 8 개 주요 산업군 중 가장 낮은 수준으로 나타났다. 대한병원협회도 중소병원을 중심으로 보안 예산 편성과 전문 인력 확보가 어려운 현실을 지적하고 있다. 외부 감사나 보안 인증 획득을 위한 목적으로 일시적으로 투자를 진행하지만, 일상적 운영에서 보안을 전략적으로 관리하는 조직 문화는 부재하다고 평한다. 보안을 선택 가능한 항목이 아닌 필수 인프라로 바라보는 시각의 전환이 필요하다.



* 출처: 2024 정보보호 공시 현황 분석 보고서

그림 2. 업종별 평균 정보보호 투자액

■ 법적 책임과 보상 구조

병원 보안에 대한 투자와 관리 체계가 충분히 자리 잡지 못한 또 다른 원인 중 하나는, 정보 유출 사고에 따른 법적·도의적 책임이 미약하다는 점이다. 의료정보는 가장 민감한 개인정보 중 하나임에도 불구하고, 사고 발생 시 피해자에 대한 실질적인 보상이 이뤄지지 않거나, 기관이 감수해야 할 책임 범위가 상대적으로 낮은 편이다.

국내 사례

국내에서는 사고 발생 시 과태료 부과나 재발 방지 권고에 그치는 경우가 많다. 2018 년부터 2020 년까지 17 개 종합병원에서 환자 정보 유출 사고가 발생했지만, 개인정보보호위원회는 이 중 16 개 병원에 과태료를 부과하고 시정 권고를 내렸을 뿐, 피해자에 대한 직접적인 보상은 이루어지지 않았다.

해외 사례

반면 해외에서는 환자 개인정보 유출에 대해 손해 배상이 실제로 이루어지고 있다. 미국의 A 병원은 2023 년 해킹 사고로 환자 정보가 유출된 사건에서 약 65 만 달러(약 9 억 원)를 피해자 집단에 지급하기로 합의하고, 추가로 2 년간 무료 신용 모니터링 서비스를 제공했다.

또 다른 사례로, 미국 보건의료 기업 B 사는 같은 해 개인정보 유출 사고에 대해 각 피해자에게 최대 10,000 달러(약 1,400 만 원)의 보상을 포함한 합의 절차를 진행 중이다.

■ 보안 사고 분석

의료기관을 대상으로 한 사이버 공격은 시스템 마비, 진료 중단, 환자정보 유출 등 다양한 형태로 나타나고 있으며, 피해는 단순한 금전적 손실을 넘어 환자의 생명과 직결되는 상황으로 이어질 수 있다. 국내외 병원에서 발생한 대표적인 사례들은 의료기관이 직면한 보안 문제를 보여준다. 특히 최근에는 북한 해킹 조직이 병원을 표적으로 삼고 있다는 정황이 지속적으로 포착되고 있으며, 국가정보원은 북한이 보건의료기관을 주요 타깃으로 삼아 다양한 침투 시도를 하고 있다고 발표했다.

국내 사례

2021 년 C 병원은 북한 해킹 조직의 공격을 받아 내부망이 침해되는 대규모 보안 사고를 겪었다. 경찰청에 따르면, 공격자는 약 두 달간 병원 네트워크에 잠입해 환자 약 81 만 명과 전·현직 직원 1 만 7 천여 명의 개인정보를 유출했다. 공격은 국내외 외부 서버를 경유하고 병원 시스템 취약점을 이용하여 이루어졌으며, 경찰청은 공격 근원지의 IP 주소, IP 주소 세탁 기법, 시스템 침입·관리 수법, 북한 어휘 사용 등을 근거로 북한 해킹 조직의 소행으로 판단하였다.

2023 년 7 월에는 17 개 종합병원에서 총 18 만 5 천여 건의 환자 개인정보가 유출된 사건이 발생했다. 경찰 수사에 따르면, 병원 또는 제약사 직원이 특정 처방 정보를 확인하고 이를 이메일이나 USB 등을 통해 외부로 유출한 것으로 확인되었으며, 이는 의약품 판매질서 위반 관련 수사 과정에서 드러났다.

해외 사례

2020 년 9 월, 독일 D 병원은 외부 해킹 공격으로 전산망이 마비되었고, 이로 인해 응급 진료와 예약 시스템이 중단되었다. 응급환자 한 명이 다른 병원으로 이송 도중 사망하는 안타까운 사례까지 발생했으며, 원인은 Citrix VPN 장비의 취약점을 통한 침입으로 밝혀졌다.

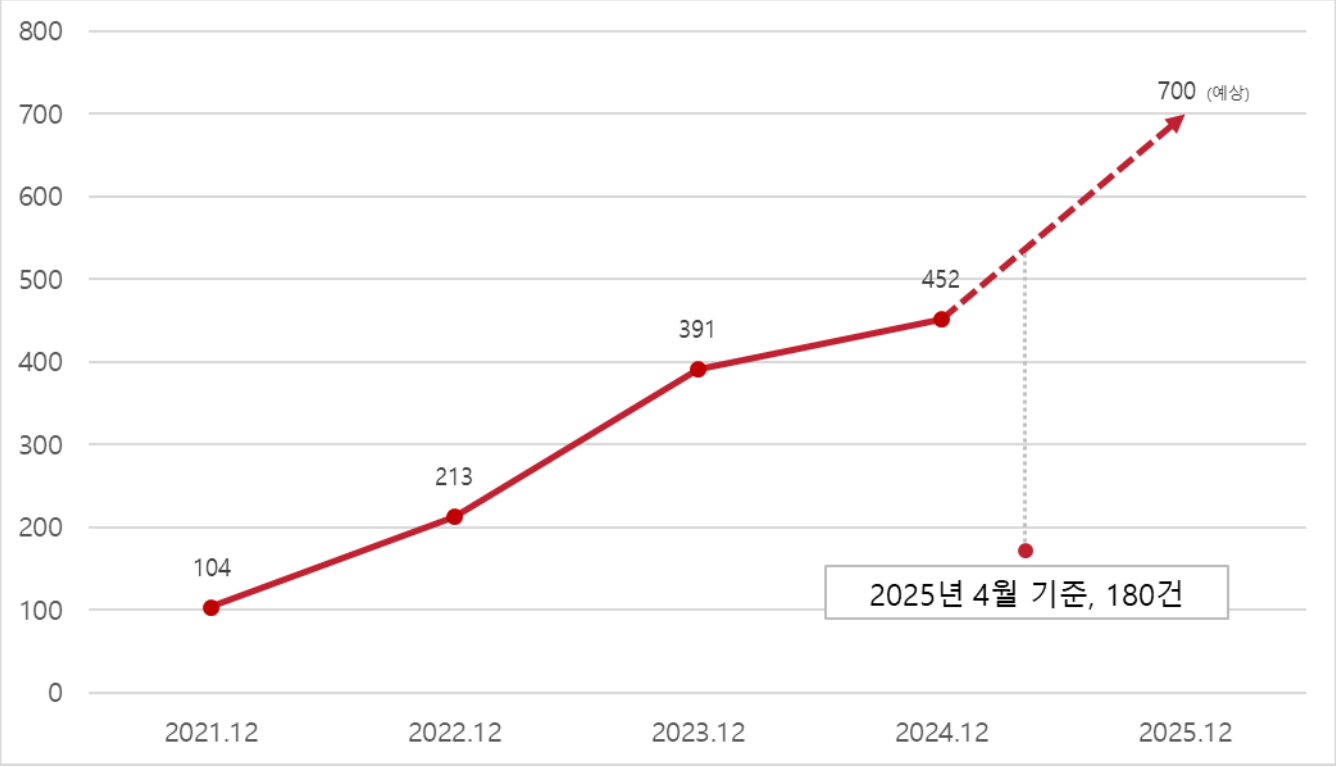
또한 2022 년 10 월, 미국의 비영리 의료조직인 E 사는 랜섬웨어 공격을 받아 21 개 주의 164 개 병원 및 진료소의 시스템이 동시에 마비되었고, 약 62 만 명의 환자 정보가 유출되었다. 공격은 외부 협력업체와의 시스템 연계 경로를 통해 이루어진 것으로 추정되고 있다.

■ 환자 개인정보 유출의 영향

병원이 다루는 정보는 단순한 이름이나 연락처 수준을 넘어, 환자의 진단명, 병력, 정신건강기록, 수술 이력, 감염병 내역 등 고도로 민감한 의료 기록을 포함한다. 이러한 정보가 유출될 경우, 그 피해는 단기간에 그치지 않으며, 취업·보험·사회적 낙인 등 다양한 측면에서 환자의 삶에 장기적인 영향을 미칠 수 있다.

최근 다크웹에서는 민감한 의료정보가 지속적으로 유통되고 있으며, 이들 데이터는 금융 범죄나 사회공학적 공격의 재료로 활용될 가능성이 높다. 유출된 의료정보는 한 번 퍼지면 사실상 삭제나 회수가 불가능하고, 어디까지 퍼졌는지 추적하기도 어렵다. 그 결과 피해자는 오랜 기간 2 차 피해에 노출되며, 이 피해는 시간이 지날수록 누적되고 심화되는 양상을 보인다.

실제로 다크웹에 게시된 의료 데이터 건 수는 2021 년 104 건에서 2024 년 452 건으로 약 4 배 증가했으며, 2025 년 4 월 현재까지 180 건이 확인되었다. 이 같은 증가 추세가 이어질 경우, 2025 년 연말까지 의료정보 게시 건 수는 700 건을 넘어설 것으로 예상된다.



* 출처 : SK 쉴더스

그림 3. 의료 데이터 다크웹 게시 건 수

■ 병원 정보보안 및 개인정보보호 컴플라이언스 의무사항

의료법에 따른 환자 정보보호 의무

의료법은 의료기관이 환자의 진료기록과 개인정보를 철저히 보호할 책임이 있음을 법적으로 명시하고 있다. 의료법 제19조에서는 의료인이 진료나 조제 과정 등 업무 중 알게 된 환자의 비밀을 누설하거나 발표해서는 안 된다고 규정하며, 이를 위반할 경우 형사처벌의 대상이 된다. 또한 제21조는 환자 본인이나 정당한 법적 권한을 가진 자에 한해 진료기록 열람을 허용하고 있으며, 제22조는 진료기록의 보존과 전자의무기록(EMR)의 안전한 관리 조치를 의무화하고 있다. 이러한 조항들은 환자 정보를 보호하기 위한 기본적인 법적 기반을 제공하며, 위반 시 과태료 또는 행정처분 등의 법적 제재가 따르게 된다.

개인정보 보호법의 병원 적용

병원은 개인정보보호법상 '개인정보처리자'로 분류되며, 이에 따라 환자의 개인정보를 수집, 저장, 활용, 파기하는 전 과정에서 법적 책임을 진다. 개인정보보호법 제29조 및 시행령 제30조 등에 따라 의료기관은 개인정보를 안전하게 보호하기 위한 관리적·기술적·물리적 보호조치를 반드시 마련해야 하며, 제34조에 따라 개인정보 유출이 발생하면 즉시 관계기관에 신고하고 피해 확산을 방지해야 한다. 위반 시 과징금, 과태료 부과 및 형사처벌까지 가능하므로 병원의 정보보안 체계는 이 법의 요구사항을 충족해야 한다.

ISMS, ISMS-P 인증 의무화

ISMS(정보보호 관리체계) 인증, ISMS-P(정보보호 및 개인정보보호 관리체계) 인증은 과학기술정보통신부와 개인정보보호위원회가 공동으로 시행하는 국가 인증제도다. 정보통신망법 제47조 2항에 따라 전년도 기준으로 총 매출액 또는 세입이 1,500억 원 이상이며 의료법 제3조의4에 따른 상급 종합병원이거나, 정보통신서비스 매출이 100억 원 이상인 경우, 혹은 하루 평균 100만 명 이상의 이용자를 보유한 의료기관은 인증을 의무적으로 받아야 한다. 인증 기준에는 관리체계 수립 및 운영, 보호대책 요구사항, 개인정보 처리단계별 요구사항 등 3개 부문의 등 정보보호 전 영역이 포함된다.

전자서명법에 따른 전자의무기록(EMR) 보안 요건

전자의무기록(EMR)은 환자의 진료 정보가 집약된 민감한 데이터로서, 정보보안의 핵심 대상 중 하나다. 의료기관이 전자의무기록(EMR) 시스템을 운영할 경우, 해당 정보의 법적 효력 보장을 위해 전자서명 기술의 적용이 필수적이다. 의료법 제23조는 의료인이 진료기록부 등을 전자문서로 작성하는 경우, 전자서명법에 따른 전자서명을 포함해야 함을 명시하고 있으며, 의료법 시행규칙 제16조는 전자의무기록의 생성·저장, 전자서명의 검증이 가능한 장비를 갖출 것을 요구한다. 이러한 법적 요건은 전자의무기록(EMR) 시스템이 정보보안 측면에서 위·변조 방지, 무결성 등을 충족해야 함을 의미하며, 병원은 이를 위해 전자서명 기술을 포함한 보안 체계를 반드시 구축해야 한다.

■ 기술적 대응 전략

애플리케이션 보안 점검과 취약점 진단

병원에서 운영하는 외부 연계 시스템은 공격자에게 침투 지점이 될 수 있다. 이러한 위협에 대비하려면 정기적인 보안 점검과 취약점 진단이 필요하며, 점검 이력은 체계적으로 기록·관리되어야 한다. 특히 외부 보안 전문가를 활용한 시나리오 기반 진단은 내부 보안 점검 체계를 보완하는 데 효과적이다. 이러한 활동은 단발성으로 끝나는 것이 아니라, 시스템 변경이나 서비스 확장 시마다 반복적으로 수행되어야 할 보안 검증 루틴으로 정착되어야 한다.

네트워크 구조 보안

병원은 진료망, 행정망, 의료기기망, 외부망 등 다양한 네트워크가 혼재된 복합 환경을 운영한다. 이러한 구조는 보안 위협이 확산되기 쉬운 특성을 가지므로, 병원 내 네트워크는 논리적 또는 물리적으로 분리되어야 하며, 필요 시 VLAN 및 전용망을 통해 업무별 통신 영역을 분리해야 한다.

또한 외부 접속 시에는 VPN 기반의 보안 통신을 기본으로 하고, 장비 인증, 접속 시간·위치 제한 등 조건 기반 접근 정책이 병행되어야 한다. 이는 무분별한 원격 접속을 차단하고, 시스템의 불필요한 노출을 최소화하기 위한 핵심 방어 수단이다.

시스템 보안 및 패치 관리

병원의 정보시스템은 운영체제(OS), 데이터베이스(DB), 전자의무기록(EMR), 의료영상저장전송시스템(PACS), 웹 서버 등으로 구성되어 있으며, 각 구성요소마다 독립적 보안 설정과 정기적인 패치 적용이 필요하다. 패치가 어려운 시스템은 네트워크 접근 차단, 애플리케이션 제어, 화이트리스트 기반 실행 제한 등 대체 기술을 활용해야 한다.

의료기기 보안

의료기기는 주로 폐쇄형 운영체제(OS) 또는 펌웨어 기반으로 운영되며, 제조사 또는 유지보수 업체를 통해서만 변경이 가능한 구조가 많다. 이로 인해 보안 패치나 점검이 원활하지 않고, 구형 시스템이 장기간 방치되는 경우가 많다. 보안 대책으로는 전용 네트워크 분리, 보안 게이트웨이 설치, 접근 제어, 로그 기록, 권한 분리 등이 있으며, 특히 무선 연결 또는 원격 진단 기능이 있는 장비는 반드시 암호화 통신 및 인증 체계가 적용되어야 한다.

계정 관리 및 접근 통제

병원 전산 시스템은 다양한 직군이 사용하는 환경이며, 교대근무나 공용 계정 사용으로 인해 사용자별 활동 추적이 어렵다. 이를 해결하기 위해 역할 기반 접근 통제(RBAC)를 적용하고, 관리자 계정에는 이중 인증(MFA)을 반드시 설정해야 한다.

또한 외부 협력사나 파견 인력에게 부여하는 권한은 시간, 경로, 명령어 등 조건에 따라 제한하고, 모든 접근 기록은 감사 로그로 남겨 정기적으로 점검되어야 한다.

로그 분석 및 이상행위 탐지

보안 로그는 단순히 보관하는 데 그치지 않고, 이상행위를 조기에 감지하는 데 활용되어야 한다. 시스템 로그와 사용자 행위 데이터를 기반으로 이상 접근을 실시간 탐지할 수 있는 모니터링 체계를 갖춰야 하며, 접속 이력, 계정 사용 내역, 시스템 변경 사항 등을 주기적으로 분석하는 체계를 마련해야 한다. 이러한 체계는 내부자 위협, 랜섬웨어 감염 등 보안 위협을 조기에 차단하는 효과적인 수단이 된다.

■ 관리적 대응 전략

보안 인력과 내부 역량

병원 정보보안의 핵심은 전담 인력의 안정적인 확보에 있다. 2024년 기준, 병원급 의료기관 중 다수는 5명 미만의 보안 인력으로 운영되고 있으며, 전체 보건의료기관의 평균 정보보호 전담 인력 수는 2.8명에 불과하다. 특히 중소 병원의 경우, 상근 보안 인력을 두지 못해 보안 업무 전반을 외부 IT유지보수 업체에 위탁하는 경우가 일반적이다. 이러한 구조에서는 침해 사고 발생 시 즉각적인 대응이 어려울 뿐 아니라, 보안 운영의 지속 가능성도 낮아질 수 있다. 일정 규모 이상의 병원은 자체 보안 전담 인력을 확보하고, 네트워크·시스템·보안관제 등 분야를 분리해 기능별 역할을 수행할 수 있는 내부 구조를 갖추는 것이 바람직하다.

보안 교육과 인식 제고

병원은 다양한 직종이 공존하는 복합 조직이다. 단순한 교육 자료 배포만으로는 보안 인식이 충분히 전파되기 어려우며, 각 직무에 특화된 맞춤형 교육이 요구된다. 예를 들어, 의료진에게는 피싱 메일 탐지 훈련, 행정직에는 계정 관리 위험 교육, 장비 담당자에게는 의료기기 보안 절차 안내 등 업무 기반의 분리 교육이 필요하다. 이러한 교육은 연 1회 이상의 정기 교육과 모의 훈련을 병행하는 방식으로 구성되며, 지속적인 실천을 통해 병원 전반에 보안 문화를 정착시켜야 한다.

외주 및 공급망 보안

병원은 다양한 외부 업체와 연결된 구조를 갖고 있다. 협력사는 병원 시스템에 일정 수준 이상의 접근 권한을 보유하기 때문에, 해킹의 우회 경로로 악용될 수 있는 보안 취약점이 되기도 한다. 따라서 외주 계약 시에는 정보보호 관련 조항을 명시하고, 정기적인 보안 점검 및 준수 평가를 병행해야 한다. 또한 외부 접속은 시간, 권한, 세션 기록 등을 기반으로 통제하고, 이를 통해 외부 인력의 활동을 투명하게 관리할 수 있는 구조를 마련해야 한다.

대응 훈련과 사고 대응 체계 운영

2024년 기준, 전체 의료기관의 82.1%가 랜섬웨어나 해킹에 대비한 대응 훈련을 수행하고 있으며, 보건업의 대응 훈련 이행률은 96.2%로 가장 높은 수준을 기록했다. 이는 정기적 훈련이 보안 역량 강화에 실질적인 효과를 발휘함을 시사한다. 병원은 단순한 해킹 이메일 탐지 시나리오를 넘어서, 의료기기 오작동, 전자의무기록(EMR) 차단, 백업 시스템 이탈 등 복합 상황을 포함한 시나리오형 통합 훈련을 기획해야 한다. 이러한 훈련 결과는 보안 인식 향상은 물론, 전사적인 위기 대응 체계 구축의 출발점이 될 수 있다.

■ 병원정보시스템 보안가이드라인

2025 년 4 월, 국가정보원은 보건복지부, 한국인터넷진흥원(KISA)과 협력해 전국 의료기관을 대상으로 새로운 병원정보시스템 보안 가이드를 발표했다. 이는 최근 고도화된 병원 대상으로 지속되고 있는 사이버 공격, 특히 의료기기와 외부연계 시스템 등 새로운 형태의 IT 환경이 병원 내로 확산되면서, 기존 보안 체계만으로는 대응에 한계가 있다는 인식에서 비롯되었다.

병원 시스템이 마비될 경우, 단순한 서비스 중단을 넘어 환자의 생명에 영향을 줄 수 있다. 때문에, 다양한 위협 환경에 대응하기 위해 병원이 자율적으로 구축해야 할 보안 기준과 실무 지침이 마련되어야 있다.

가이드 구성

이번 가이드는 네트워크, 시스템 및 애플리케이션, 관리적 보안대책의 세 영역으로 구성되어 있다. 기술적 조치와 관리적 조치가 병원 환경에 맞게 조화를 이루도록 설계되었으며, 병원 규모에 따라 탄력적으로 적용할 수 있는 유연한 구조를 갖추고 있다.

항목	내용
네트워크 보안대책	병원 내부의 다양한 네트워크(진료망, 의료기기망, 외주망 등)를 구간별로 논리·물리적으로 분리하고, 외부 접속은 DMZ 구성을 통해 내부망을 보호하며, VPN·API 등 연계 통신은 암호화와 인증을 필수화 하는 등 병원 전반의 네트워크 환경에 대한 보호 체계를 명확히 규정함.
시스템 및 애플리케이션 보안대책	병원정보시스템을 구성하는 OS, DB, EMR, PACS, 웹 서버 등의 구성요소에 대해 보안 설정과 주기적 패치 관리를 요구하고, 의료기기 보안 항목을 별도로 마련하여 인터넷 차단, 접근 통제, 패치 확인을 강조하며, 원격진료 시스템과 클라우드 환경에서 발생할 수 있는 취약점 대응 방안도 포함함.
관리적 보안대책	병원 내 정보보호 책임자 지정, 조직 내 역할과 책임 분장, 계정·권한 관리 기준 수립, 외주 협력업체의 접근 통제, 보안 교육 시행, 보안 로그 보관 및 주기적 점검 절차 등 관리적인 통제를 통해 병원 전반의 보안 수준을 유지·운영할 수 있도록 요구함.

표2. 병원정보시스템 보안가이드 라인 개요

■ 맺음말

병원을 겨냥한 사이버 위협은 단순한 기술적 문제가 아니다. 이는 환자의 안전, 진료의 연속성, 그리고 공공의 신뢰와 직결되는 중대한 사안이다.

최근 국내외에서 발생한 병원 보안 사고들은 의료기관의 구조적 취약성과 운영상 허점을 정확히 파고들며, 단 한 번의 침입이 전체 시스템 마비로 이어지고, 때로는 환자의 생명에까지 영향을 미치는 상황을 초래하고 있다.

의료기관은 진료가 최우선인 환경 특성상, 시스템 점검이나 보안 강화 조치에 제약이 많은 것이 현실이다. 이 같은 제약은 공격자에게 '공격 성공률이 높은 표적'이라는 인식을 심어주며, 실제로 병원은 다른 산업에 비해 사고 대응이 늦고 피해 범위도 넓은 편이다.

의료 서비스는 앞으로 점점 더 디지털화되고, 환자정보의 흐름은 병원 내부를 넘어 연계 시스템으로 계속 확장될 것이다. 이런 환경에서 병원의 운영 안정성과 사회적 신뢰를 지키기 위해, 보안은 선택이 아닌 필수적 조건으로 인식되어야 한다.