SSiS 한국사회보장정보원	보 도 자 료		
보도시점 (엠바고)	2026. 06. 29.(월) 배포 후 즉시 사용	배 포 일	2026. 06. 29.(월)

융합보안 연구 성과 빛났다 …

한국사회보장정보원, ‘우수논문 기관상’ 수상

의료기관 사이버위협 분석과 PACS 보안 강화를 위한 현장 중심 해법 제시

학계·공공기관과 협력해 국민이 안심하는 디지털 복지·의료 환경 조성

한국사회보장정보원(원장 김현준)은 6월 26일(금) 대전 라마다호텔에서 열린 ‘2026 한국융합보안학회 하계학술대회’에서 융합보안 연구와 학술 교류에 기여한 공로로 ‘우수논문 기관상’을 수상했다.

융합보안은 사이버보안뿐만 아니라 사람·시설·제도까지 함께 살펴 복합적인 위험에 대응하는 보안 방식이다. 국민의 복지 관련 정보와 서비스가 디지털로 긴밀히 연결된 오늘날, 보안사고는 개인정보 유출을 넘어 복지 서비스의 중단으로까지 이어질 수 있어 국민의 일상과 직결된다.

한국사회보장정보원은 이번 학술대회에 ‘의료기관 침해사고 동향 및 의료영상저장전송시스템(PACS) 보안성 개선 연구’를 제출했다. 연구진은 랜섬웨어로 의료영상과 환자정보가 훼손되는 위험을 분석하고, 접근통제 강화와 통신 암호화, 네트워크 분리, 안전한 백업 등 실질적인 개선방안을 제시했다.

특히 국민이 이용하는 주요 사회보장 정보서비스를 운영하는 기관으로서, 현장의 보안 문제를 연구로 연결하고 학계·공공기관과 협력을 확대해 온 점을 높이 평가받았다.

김현준 한국사회보장정보원장은 “보안은 단순히 시스템을 지키는 일이 아니라 국민의 개인정보와 일상을 지키는 일”이라며 “앞으로도 학계와 적극 협력해 국민이 안심하고 이용할 수 있는 복지·의료 정보환경을 만들겠다”고 밝혔다.

사진

[사진 자료: 한국융합보안학회 하계학술대회 시상식에서 김현준 원장(오른쪽)이 우수논문 기관상을 수상 후 기념 촬영을 하고 있다. / 한국사회보장정보원]

담당본부	정보보호본부	책임자	김유석 본부장	02-6360-6570
담당부서	정보보안부	담당자	김종섭 부 장	02-6360-5501

붙임 1 논문 요약본

의료기관 침해사고 동향 및 의료영상저장전송시스템(PACS) 보안성 개선 연구

김유석[1]⋆, 김완중[2], 전연진[3]
한국사회보장정보원[1], 보건복지정보보호관리단[2]

A Study on Trends in Security Incidents at Healthcare Institutions and Improvements to the Security of Picture Archiving and Communication Systems (PACS)

Yuseok Kim[1]*, Wanjung Kim[2], Yeunjin Chun[3]

최근 의료기관은 랜섬웨어, 내부자 위협, 공급망 공격 등 다양한 사이버 위협에 지속적으로 노출되고 있다. 특히 PACS는 의료영상 데이터와 환자 개인정보를 저장·전송하는 핵심 시스템으로 보안 침해 시 의료서비스 중단 위험이 크다. 본 연구에서는 국내외 의료기관 침해사고 사례와 PACS 시스템의 구조적 취약점을 분석하였다. 또한 DICOM 통신 구조와 의료기관 네트워크 환경의 보안 취약점을 기반으로 주요 공격 시나리오를 도출하였다. 이를 해결하기 위해 Zero Trust 기반 접근통제, 망분리, DICOM 암호화, 백업·복구 강화 등 PACS 보안성 향상 방안을 제안하였다.

Key Words : PACS, Ransomware, DICOM, Zero Trust, Medical Security, Cyberattack

1. 서 론

디지털 헬스케어환경의 확산과 함께 의료기관의 정보화수준은 빠르게 발전하고 있다. 의료기관은 EMR, PACS, OCS, LIS 등 다양한 의료정보시스템을 통합적으로 운영하며 환자진료 효율성과 의료서비스 품질을 향상시키고 있다. 그러나 의료정보시스템의 확대는 동시에 사이버공격 표면 증가라는 새로운 위험을 초래하고 있다.

최근 랜섬웨어 공격 조직은 의료기관을 주요 목표로 삼고 있다. 의료기관은 24시간 중단없는 서비스가 요구되며 환자생명과 직결되는 특성상 시스템복구를 위해 비용을 지불 할 가능성이 높기 때문이다.
특히 PACS는 의료영상 데이터의 저장과 전송을 담당하는 핵심인프라로 시스템 장애시 영상판독이 불가능해져 의료행위 전체에 영향을 줄 수 있다.

의료기관은 다양한 제조사의 의료기기와 운영체제가 혼재되어 있고 노후장비 비율도 높다. 일부 의료기기는 제조사 지원종료로 인해 보안패치 적용이 어려우며 원격 유지보수 포트가 상시 개방된 경우도 존재한다. 이러한 환경은 랜섬웨어 및 내부 확산형 공격에 매우 취약하다.

본 연구에서는 의료기관 침해사고 동향과 PACS 보안 위협을 분석하고 랜섬웨어 대응 중심의 PACS 보안성 개선 방안을 제안한다.

2. 본 론

2.1 의료기관 침해사고 동향 분석

최근 의료기관을 대상으로 하는 랜섬웨어 공격은 지속적으로 증가하고 있다. 공격자는 이메일 첨부파일, 원격접속 포트, 취약한 의료기기 등을 통해 내부망에 침투한 후 EMR 및 PACS 서버를 암호화하여 금전을 요구한다. 의료기관은 서비스 중단시 환자진료에 직접적인 영향을 미치기 때문에 일반기업보다 공격에 취약하다.

국내 의료기관사례에서는 Windows 10, Server 2012 등 지원종료 운영체제를 사용하는 사례가 다수 확인되었다. 또한 의료기기 특성상 보안패치 적용이 어려운 환경도 존재한다. 랜섬웨어 공격은 단순 데이터 암호화를 넘어 환자정보 유출 및 의료 영상 위변조 가능성까지 확대되고 있다.

(표 1) 국내 연도별 침해사고 신고현황

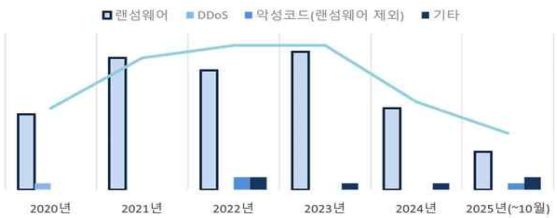
구분 \ 연도	2023년	2024년	2025년
DDoS	213(16.7%)	285(15.1%)	588(24.7%)
악성코드	300(23.5%)	229(12.1%)	354(14.9%)
서버해킹	583(45.6%)	1,057(56.0%)	1,053(44.2%)
기타	181(14.1%)	316(16.7%)	388(16.3%)
합 계	1,277	1,887	2,383

2.2 PACS 시스템 구조 및 보안 취약점

PACS는 영상획득장치, PACS 서버, 데이터베이스, PACS Viewer, 웹서버 등으로 구성된다. 의료영상은 DICOM 프로토콜을 이용하여 전송되며, 환자 메타데이터와 함께 저장된다. 그러나 DICOM은 기본적으로 암호화와 강력한 인증기능이 부족하여 중간자 공격이나 데이터 변조에 취약할 수 있다.

또한 PACS Viewer PC의 보안설정 미흡, 계정관리 부재, 공유폴더 설정 등도 주요 취약점으로 분석된다. 원격 유지보수를 위해 개방된 RDP 포트와 VPN 계정 탈취 역시 주요 침해 경로이다. 내부 사용자PC 감염 이후 내부 확산(Lateral Movement)을 통해 PACS 서버로 접근하는 공격도 빈번하다.

(표 1) 의료기관 연도별 침해사고 신고 현황



2.3 랜섬웨어 공격 시나리오 분석

랜섬웨어 공격은 일반적으로 초기침투, 내부확산, 권한상승, 데이터 암호화 단계로 진행된다.

첫 번째 단계에서는 이메일 피싱 또는 원격접속 취약점을 통해 악성코드가 유입된다.

두 번째 단계에서는 내부 PC를 스캔하며 공유폴더 관리자계정, PACS, 서버 위치를 탐색한다.

세 번째 단계에서는 관리자권한 탈취 후 PACS 서버 및 저장소에 접근한다.

마지막으로 의료영상 데이터와 데이터베이스를 암호화하여 의료서비스를 마비시킨다.

특히 PACS 데이터 손실시 의료영상 판독이 불가능해져 진료 중단 및 환자 안전사고로 이어질 수 있다.

2.4 PACS 보안성 개선 방안

첫째, 의료정보망과 업무망을 분리하여 랜섬웨어 확산을 차단해야 한다.

둘째, Zero Trust 기반 접근통제를 적용하여 사용자 및 장비를 지속적으로 검증해야 한다.

셋째, DICOM 통신에 TLS 기반 암호화를 적용하고 장비간 인증체계를 강화해야 한다.

넷째, PACS 서버와 Viewer PC에 대한 계정관리 및 최소권한 정책을 적용해야 한다.

다섯째, 백업 데이터는 오프라인 또는 Immutable Storage 방식으로 보호해야 한다.

마지막으로 의료기관 종사자 대상 보안인식 교육과 모의훈련이 필요하다.

2.5 Zero Trust 기반 PACS 보안 모델

본 연구에서는 Zero Trust 기반 PACS 보안 모델을 제안한다. 제안 모델은 사용자 인증, 장비 무결성 검증, 네트워크 접근제어, 실시간 모니터링으로 구성된다. 사용자는 MFA 기반 인증을 수행하며, 접속 장비는 보안정책 준수 여부를 확인받아야 한다. 네트워크 구간에서는 NAC 및 마이크로 세그멘테이션을 적용하여 불필요한 접근을 차단한다. 또한 SIEM 및 EDR 연계를 통해 이상행위를 탐지하고 랜섬웨어 확산을 조기에 차단할 수 있다. 해당 모델은 기존 경계형 보안보다 내부 확산 공격에 효과적으로 대응할 수 있다.

2.6 기대효과

제안된 보안모델을 적용할 경우 랜섬웨어 감염 확산을 최소화할 수 있다. 또한 의료영상 데이터의 기밀성, 무결성, 가용성을 향상시킬 수 있다. Zero Trust 기반 접근제어를 통해 내부 사용자 위협 대응도 가능하다. 의료기관은 침해사고 발생시 신속한 복구체계를 확보할 수 있으며, 개인정보 유출 가능성을 감소시킬 수 있다. 결과적으로 환자 안전과 의료서비스 연속성을 보장하는 데 기여할 수 있다.

3. 결론

2025년은 통신, 유통, 금융 등 국민생활 밀접분야에서 전례 없이 잦은 침해사고와 함께 개인정보 유출 사고가 발생했다. 이로 인해 많은 국민들이 개인정보 유출에 따른 2차 피해가 발생할 수 있다는 걱정 등 불안감을 겪었으며, 직접적인 금전 피해를 입기도 했다. 이와 같이 올해 국내에서 발생한 침해사고는 국민 일상 및 국가 경제에도 큰 영향을 미쳤다고 볼 수 있다. 국민의 일상생활까지 침해사고에 영향을 받고 있는 상황에서 올 한 해 주요 사이버 침해사고 건들을 되돌아보며 사이버 보안 태세를 정비하고자 한다.

본 논문에서는 의료기관 침해사고 동향과 PACS 보안 취약점을 분석하고, 랜섬웨어 대응 중심의 보안성 개선방안을 제안하였다. 의료기관은 다양한 의료기기와 정보시스템이 연계되어 있어 일반 정보시스템보다 높은 보안위험에 노출되어 있다. 특히 PACS는 의료영상 데이터의 핵심 시스템으로 랜섬웨어 공격시 의료서비스 중단과 환자 안전 문제로 직결된다. 따라서 Zero Trust 기반 접근통제, DICOM 보안강화, 네트워크 분리, 백업체계 강화등 종합적인 보안대책이 필요하다.
향후 연구에서는 AI 기반 이상행위 탐지와 의료기기 보안 통합관제 분야에 대한 추가 연구가 필요하다.

참고문헌

[1] 한국사회보장정보원, 의료정보시스템 보안 위협 및 취약점분석, 2022.

[2] KISA, 스마트의료사이버보안 가이드, 2021.

[3] NIST SP 800-207, Zero Trust Architecture, 2020.

[4] 한국인터넷진흥원,랜섬웨어대응가이드, 2023.

[5] ISO/IEC 27001 Information Security Management Systems.

붙임2 한국융합보안학회 하계학술대회 및 워크숍 포스터