교육부	보 도 자 료	다시, 대한민국! 새로운 국민의 나라

보도 일시	(인터넷) 2022. 6. 3.(금) 06:00 (지 면) 2022. 6. 3.(금) 석간	배포 일시	2022. 6. 2.(목) 15:30
담당 부서	교육안전정보국 정보보호팀	책임자	팀장 김도영 (044-203-6515)
		담당자	사무관 장창헌 (044-203-6504)

국립대학병원 사이버 위협 예방을 위해 나선 교육부

- 국립대학병원 사이버위협에 예방적 대응체계 마련 -

주요 내용

□ 코로나19 확산 상황에서 **대학병원**을 **표적**으로 한 **사이버위협 증가**로 다양한 **피해 발생**

□ 이에 대응하기 위해 **선제적 예방-사고대응 지원-병원 대응역량 제고의 정보보호 강화방안**을 **마련**하여 국립대학병원의 정보보호 지원

□ 교육부는 국립대학병원에 대해 **사이버위협 탐지·분석·복구 등**을 **신속**하게 **대응**하여 **사고예방** 및 **피해**를 **최소화**하기 위한 **국립대학병원 정보보호 강화방안**을 국가정보원과 합동으로 **마련**하였다.

○ 이는 최근 대학병원 **해킹**을 통해 시스템에 **접근**하여 **데이터**를 **암호화**하고 이를 풀어주는 **대가**로 **금품**을 **요구**하는 **악성프로그램**(랜섬웨어) 등 **사이버공격 증가**에 대한 **사전 예방 및 대응**이 목적이다.

□ 이번에 마련한 방안의 주요 내용을 살펴보면 첫째, **사이버 위협**에 대한 **예방활동**을 **강화**하여 **사이버공격**을 **사전 방지**한다.

○ 국립대학병원 **기반시설**의 **보호대책***을 **집중 점검**하고, **병원의 중요시설이 주요정보통신기반시설**로 **추가 지정**될 수 있도록 **관련 기관과 협의**한다.

* **① 백업시스템 구축, ② 위기발생 시 복구방안, ③ 업무연속성 계획 등**

○ 교육부 정보보호 수준진단은 병원에 특화된 별도 지표를 마련하고, 모바일 앱 및 의료정보시스템 대상 **취약점**을 **진단**하여 **조치**한다.

○ 최근 병원 내 다수의 주요서비스에서 제공되는 **병원 모바일앱**이나 인터넷에 연결되어 위험에 노출된 **의료장비**의 **보안 취약점 진단**을 통해 취약점을 제거하여 **침해사고**를 **사전 예방**한다.

○ 또한, **교육부 정보보호 교육센터**를 통해 **대학병원 직원**에 대한 정보보안 및 개인정보보호 **교육을 지원**하고, 국립대학병원을 대상으로 **사이버공격 대응 훈련**(분산 서비스 거부 공격, 해킹메일 등)을 **확대**한다.

□ 둘째, **침해사고 대응체계**를 **구축**하여 **사이버공격**에 대해 **신속**하게 **대응**한다.

○ 국가 사이버위협 정보공유시스템(NCTI), 교육부 사이버위협 정보공유 시스템을 활용하여 **정보공유**를 **강화**하고, **국립대학병원 정보보안 협의체**를 **구성**하여 병원별 문제점을 협력하여 해결한다.

○ 알려지지 않은 사이버위협 탐지를 위해 **차세대 사이버위협 탐지체계**를 개발·배포하고 **인공지능(AI) 기반 통합 보안관제**를 실시하며, **국가정보원**과 **침해사고 대응 체계**를 **구축**하여 사이버공격 시 **합동 조사·분석**한다.

○ 침해사고 원인 조사, 복구 및 대응에 대한 컨설팅 등 신속한 정상화를 **지원**하고, **유관기관**(국가정보원 등)과 **협력**하여 **개발된 악성코드 대응 기술**을 국립대학병원에 **배포**한다.

□ 셋째, **안전한 네트워크 환경 및 의료 기반(인프라)**을 개선하여 **역량을 강화한다.**

○ 병원 시스템 특성에 맞게 내부망·인터넷망 등으로 **망(네트워크) 영역**을 **분리**하고, 병원 **정보보호시스템 운영**에 대한 **전문적 지원(컨설팅)**을 제공한다.

○ 병원에서 사물인터넷 기반 **의료기기 구매** 시 준수하여야 할 **의료기기 보안관리 지침(가이드)** 및 **의료기기 유형별 보안점검 목록**을 **마련**하고 이에 따른 자체 보안점검을 추진한다.

□ **이난영 교육부 교육안전정보국장**은 “초연결 초지능 사회에서 의료정보 시스템 및 의료기기 등에 대한 사이버공격이 증가하고 있으므로, 국립대학병원의 정보보호 체계 강화를 통해 국민께서 안전한 의료정보서비스를 받을 수 있도록 노력하겠다.”라고 밝혔다.

【붙임】 1. 국내외 병원 사이버공격 피해 사례
2. 과제별 추진 일정
3. 악성코드 특징
4. 국립대학병원 정보보호 강화 방안(요약)

붙임 1 국내외 병원 사이버공격 피해 사례

<독일 사례> 2020.9.18 독일 뒤셀도르프 대학병원 서버 30대가 랜섬웨어에 감염되면서 병원 서비스가 마비됐다. 이로 인해 지난 17일 수술받을 예정이었던 한 여성 환자는 32㎞ 떨어진 다른 병원으로 이송되다 결국 사망했다.

<미국 사례> 2021.8.17. 하이브(Hive)라는 랜섬웨어 운영자들이 비영리 단체인 메모리얼 헬스 시스템(Memorial Health System)을 공격하여 마비시켰다. 때문에 직원들은 종이와 펜으로 업무를 진행하고 있다고 한다. 메모리얼 헬스 시스템은 3개의 병원을 합친 작은 의료 그룹사로 미국 일부 지역에서 적잖은 환자들에게 의료 서비스를 제공하고 있다. 이번 랜섬웨어 공격으로 예약된 수술이 중단되고, 일부 환자들을 다른 병원으로 후송하기도 했다. 또한 최근 랜섬웨어 공격의 유행에 따라, 공격자들이 환자들의 의료 기록과 개인정보를 훔쳐갔을 가능성도 높게 점쳐지고 있다. 실제로 하이브는 정보 유출용 사이트를 공개하고 있기도 하다.

<국내사례> '랜섬웨어' 병원 노린다…사이버 공격 빨간불

2021.06.29 코로나19 이슈 악용 사례 급증…EMR 선진국도 환자 정보 위태

인터폴(국제형사경찰기구)로부터 국내 병원에 대한 랜섬웨어 공격에 주의를 당부하는 권고문이 접수되는 등 심각한 상황이다.

무엇보다 국내 의료기관들의 전자의무기록시스템(EMR) 운영 비율이 100%를 육박하고 있는 만큼 각종 해킹이나 악성 프로그램 공격 대상으로 지목되고 있다.

실제 일부 병원에서 랜섬웨어 공격을 받아 수술이 중단되거나 환자 의무기록에 접근하지 못해 병원업무가 마비되는 상황이 발생하기도 했다.

서울의 한 대학병원에서는 시스템을 잠그거나 데이터를 암호화해 사용할 수 없도록 하고 이를 인질로 금전을 요구하는 랜섬웨어 공격 징후가 포착돼 비상이 걸리기도 했다.

특히 의료 분야는 사물인터넷 장비들이 많지만 중요한 디지털 자산과의 망분리 사례가 없는 경우가 많아 상대적으로 랜섬웨어 공격에 취약하다는 지적이다.

실제 보건복지부에 따르면 국내 의료기관의 전자의무기록시스템(EMR) 도입율은 92.1%에 달한다. 종별로는 상급종합병원 100%, 종합병원 98.9%, 병원 95.8%, 의원 95.7% 순이다.

병·의원급 의료기관의 경우 영상판독을 위해 외부 영상의학과 전문의에게 원격 판독을 의뢰하는 경우가 많아 접속하는 원격 단말기가 악성코드 감염에 노출될 위험이 크다.

때문에 의료기관은 피해 예방을 위한 기본적인 보안설정과 사고발생시 피해를 최소화하기 위한 예방.대응 방법을 숙지할 필요가 있다

붙임 2 **과제별 추진일정**

추진 과제	추진일정	소관기관
전략1. 사이버 위협에 대한 선제적 예방		
1 안전한 기반시설 관리 체계 구축		
① 주요정보통신기반시설 예방 체계 강화	'22~	교육부, 국정원, 국립대학병원
2 국립대학병원 예방활동 강화		
① 정보보호 수준진단 지표 개선	'23~	교육부, KERIS
② 보안취약점 사전 대응을 통한 예방활동 강화	'22~	교육부, KERIS, 국립대학병원
3 국립대학병원 직원 보안인식 제고		
① 사이버공격 대응훈련 및 전문교육 확대	'22~	교육부, KERIS, 국립대학병원
전략2. 정보공유 – 탐지·분석 – 복구 등 사고대응 지원		
1 기관간 협력을 통한 정보공유 강화		
① 기관간 정보공유·협력 채널 활성화	'22~	교육부, KERIS, 국립대학병원
2 사이버공격 탐지·분석 및 신속한 복구 지원		
① 사이버공격 탐지·분석	'22~	교육부, 국정원, KERIS
② 신속한 피해복구 지원	'22~	교육부, 국정원, KERIS, 국립대학병원
전략3. 진화하는 사이버위협에 대한 핵심 대응 역량 제고		
1 국립대학병원 현장맞춤형 보안 강화		
① 의료분야별 보안대책 강화	'23~	교육부, KERIS, 국립대학병원
② 환자정보(개인정보) 보안대책 강화	'22~	교육부, KERIS, 국립대학병원
2 국립대학병원 정보보호 기반 마련		
① 사이버보안 지침 및 매뉴얼 등 개정	'22~	교육부, KERIS
② 정보보호 조직 및 인력 강화	'22~	교육부, 국립대학병원

붙임 3 악성코드 특징

□ (**감염 원인**) 악성코드가 삽입된 **홈페이지 방문** 또는 **이메일 열람**, 서버-네트워크 등 **시스템 취약점 해킹** 등 다양한 방식으로 감염

< 감염경로 >

구분	홈페이지 방문	이메일·SNS 유포	타깃형(APT) 공격
감염 경로	악성코드가 유포 중인 홈페이지 방문	첨부파일 다운로드·링크 실행 시 설치	해커가 서버 침투 및 악성코드 설치
원인	운영체제 등 **SW 취약점 존재**	**이용자 부주의 등 보안인식 부족**	**기관의 보안관리 수준 취약**

□ (**피해 형태**) **해킹조직**이 이메일·SNS 등을 통해 **악성코드**를 **대량**으로 **살포**하는 등 **무차별적**으로 **공격**

o **서비스형 랜섬웨어***를 통해 해킹에 대한 **전문지식 없이도 악성코드 등 공격이 가능**하게 됨에 따라 범죄의 문턱도 낮아짐

* 별도의 프로그래밍 지식 없이도 비용을 지급하면 서비스 형태로 제공되는 랜섬웨어

o 대학병원 의료진 외 정보시스템 운영 담당자, 시설 담당자 등 의료시스템 취약 분야에 대한 **다양한 분야가 공격 대상**

□ (**피해 복구**) 사전에 백업된 파일을 활용하거나 공개된 일부 복구도구*를 사용하는 것을 제외하고 **암호화된 파일**의 **복구가 어려움**

* 국제 랜섬웨어 대응 프로젝트 그룹(No More Ransome) 150종 보유

o 피해자가 금전을 지불해도 파일이 복구되지 않거나, 개인정보가 공개되는 등 **2차 피해 가능성 상존**

□ (**대응 방안**) 해킹조직이 **다국적 기업화**되고, **가상자산**과 **다크웹**(Dark Web)*을 사용하여 **해킹 추적**에 **기술적, 절차적 어려움 발생**

* 일반적인 방법으로 접속자·서버를 확인할 수 없어 사이버범죄에 많이 활용되는 웹

붙임 4 국립대학병원 정보보호 강화 방안(요약)

1 추진 목적

□ 의료시설분야 사이버공격의 피해 확대방지를 위해 **체계적 예방·대응·복구** 등에 대한 **국립대학병원 정보보안 강화 대책**을 **신속하게 수립 및 추진** 필요

2 주요 추진과제

□ **(예방 활동)** 사이버위협에 대한 **예방활동을 강화**하여 사이버공격을 **사전 차단**

o **안전한 기반시설 관리체계 구축**

- 국립대학병원 **기반시설 지정 확대** 및 기반시설 **보호대책*** 집중 검토 등 **주요정보통신기반시설 예방 체계 강화**('22년~)

* ①백업시스템 구축, ②위기발생 시 복구 방안, ③업무연속성계획 등

o **국립대학병원 예방활동 강화**

- **병원 환경**(의료정보시스템 및 응급실 관리, 자체 시스템 개발체계 등)에 맞는 **정보보호 수준진단 지표 개발 추진**('23년~)

- 국립대학병원의 **모바일앱** 및 **의료정보시스템** 대상 **보안취약점 진단**을 통해 취약점을 제거하여 **침해사고 사전 예방**('22년~)

o **국립대학병원 직원 보안인식 제고**

- **교육부 정보보호 교육센터**를 통한 국립대학병원 직원 정보보호 **교육 지원** 및 **교육부 사이버공격 대응훈련*** **확대** 실시('22년~)

* 병원 모의 해킹 및 분산 서비스 거부 공격(DDoS), 해킹메일 대응 훈련 등

□ **(사고대응 지원)** 침해사고 **대응체계를 구축**하여 사이버공격에 대해 **신속하게 대응 지원**

o **기관간 협력을 통한 정보 공유 강화**

- 정보공유시스템*을 활용해 **정보공유**를 **강화**하고 **국립대학병원 정보보안 협의체**를 **구성**하여 **병원별 문제점 및 개선 방안 도출**('22년~)

* 국가사이버위협 정보공유시스템(NCTI), 교육사이버위협 정보공유시스템

o **사이버공격 탐지·분석 및 신속한 복구 지원**

- 교육부와 국가정보원은 **침해사고 대응체계**를 **구축**하여 사이버공격 시 **합동 조사·분석** 등 대응하며, **차세대 사이버위협 탐지체계 배포** 추진('22년~)
- 침해사고 발생 시 **사고 원인 조사**를 **적극 지원**하고, **복구 및 대응에 대한 컨설팅** 등 **침해사고 복구 지원 강화**('22년~)
- 악성코드 관련 **유관기관**(국정원 등)과 **협력**하여 **복구 기술**을 병원에 **신속 배포**('24년~)

□ **(역량 제고)** 안전한 **네트워크 환경 및 의료인프라를 개선**하여 역량을 강화

o **국립대학병원 현장맞춤형 보안 강화**

- 병원 시스템 특성에 맞게 내부망·인터넷망 등으로 **네트워크 영역**을 **분리**하고, 병원 정보시스템 운영에 대한 **컨설팅**을 **추진**한다.('23년~)
- 환자정보(개인정보)를 취급하는 담당자에 대한 **개인정보 교육 강화** 및 웹·모바일로 확대되는 **의료정보서비스에 대한 보안 강화** 지원('22년~)

o **국립대학병원 정보보호 기반 마련**

- **국립대학병원 현장에 맞게** 「교육부 정보보안 기본지침」 및 「교육부 사이버분야 위기대응 실무 매뉴얼」 등 **개정 추진**('22년~)
- **환자 생명이 좌우**되는 **의료기기**를 운영하는 **병원 특성**에 따라 사이버위협에 즉각 대응할 수 있도록 **자체 조직 구성**('22년~)