의료분야 랜섬웨어 예방·대응 안내서

2020.7월

진료정보침해대응센터

보건복지부

한국사회보장정보원
KOREA SOCIAL SECURITY INFORMATION SERVICE

목 차

본 안내서는 국내·외 의료기관을 대상으로 한 랜섬웨어 공격에 대한 감염예방과 대응방법에 대한 정보를 제공합니다.

1. 개요

□ 목 적

○ 본 안내서는 의료기관이 랜섬웨어 공격을 사전에 예방하고, 사고 발생 시 신속한 대응과 복구를 할 수 있도록 그 방법을 상세히 안내하고자 함

○ 또한, 진료정보 침해사고 발생에 따른 신고방법과 의료기관이 24시간×365일 사이버공격을 예방·대응할 수 있는 의료ISAC[1] 보안서비스도 활용을 권고

□ 배 경

○ 최근 의료기관에 대한 **랜섬웨어(Ransomware)[2] 피해가 늘어**나고 있으나, **필요한 보안정책 수립**과 **보안설정**이 **미흡**하여 감염사례가 지속 발생하고 있음

○ 의료기관의 피해예방을 위한 **기본적인 보안설정**과 사고발생시 **피해를 최소화**하기 위한 **예방·대응 방법**을 **의료기관은 숙지할** 필요가 있음

○ 정부에서는 진료정보의 보호를 위하여 의료법 개정을 통해 의료기관에 대한 **진료정보 보호의무 조항을 신설**하고, 정부의 역할도 강화하고 있음

- (경과) 의료법 개정 공포('19.8.27) 및 의료법 및 동법 시행령 시행('20.2.28)

- (업무위탁) 한국사회보장정보원(진료정보침해대응센터) 운영('20.2.28)

- (통지의무) 의료기관은 진료정보 침해사고가 발생할 경우, 즉시 보건복지부 및 진료정보침해대응센터에 사고발생 신고(통지)*를 해야함

※ **의료법 제23조의3(진료정보 침해사고의 통지)** : 의료기관(의료인)은 "진료정보 침해사고"가 발생한 때에는 진료정보침해대응센터(보건복지부장관) 즉시 통지

---

1) 의료ISAC(Healthcare Information Sharing & Analysis Center) : 의료분야의 해킹이나 악성코드 등 사이버 위협에 효과적으로 대응하기 위한 공동 대응체계로, 국내에는 총 4개 ISAC(의료/금융/통신/지자체) 있다.
※ (운영기관) 한국사회보장정보원, (부서명칭) 의료기관공동보안관제센터, (근거) 정보통신기반 보호법 제16조(정보공유·분석센터), www.hisac.or.kr

2) 랜섬웨어(Ransomware)는 컴퓨터 데이터를 감염시켜 접근을 제한하고 일종의 몸값을 요구하는 악성 소프트웨어의 한 종류이다. 컴퓨터로의 접근이 제한되기 때문에 제한을 없애려면 해당 악성 프로그램을 개발한 자에게 지불을 강요받게 된다. 몸값을 뜻하는 Ransom과 Software(소프트웨어)가 더하여진 합성어이다. (출처: 위키백과, ko.wikipedia.org)

- (예방·대응) 보건복지부(한국사회보장정보원)는 진료정보 침해사고의 예방 및 대응 등 의료기관의 정보보호 수준제고를 위한 법조항* 신설

* **의료법 제23조의4(진료정보 침해사고의 예방 및 대응)** : 보건복지부장관은 진료정보 침해사고에 관한 정보의 ①수집·전파, ②예보·경보, ③긴급조치, ④전자적 침해행위의 탐지·분석, ⑤취약점 점검, ⑥교육 및 훈련 등 수행

□ 안내서 활용 범위

○ **(대상기관)** 약 7만여개 의료기관(상급·종합병원, 병·의원, 요양병원, 보건의료원 등)
※ `19년 건강보험심사평가원 건강보험통계 기준(전국 요양기관)

○ **(적용대상)** 의료기관이 보유·관리하고 있는 **진료정보**에 대한 전자적 침해행위(도난·유출·파괴·손상·은닉·멸실 등)가 발생할 수 있는 **정보시스템과 전자의무기록시스템** 등

○ **(활용)** 본 안내서는 일반적인 의료기관의 네트워크 환경을 고려하여 권고하고 있으며, 적용대상 시스템의 최신 환경에 맞추어 활용할 필요

○ **(주의)** 본 안내서를 활용하여 의료기관이 보안설정을 시행할 경우, 전자의무기록시스템 및 그와 관련된 정보시스템에 대한 의료기관 업무 영향도를 **정보보호 전문가와 사전검토 후 시행하는 것을 권고**

□ 용어 정의

○ **진료정보** : 개인의 질병·부상·출산·사망에 대한 예방·진단·치료·재활 등 진료과정에서 생산·수집되어 의학적 지식 또는 부호·숫자·문자·음성·음향·영상 등으로 표현된 모든 종류의 정보(개인정보보호법」 제2조제1호에 따른 개인정보를 포함)를 말함(출처: 보건복지부 고시 제2016-233호, 2017.01.01.)

○ **전자의무기록** : 의료인이나 의료기관 개설자가 진료기록부등을 전자서명법에 따른 전자서명이 기재된 전자문서를 말함(출처: 의료법 제23조)

○ **진료정보 침해사고**: 전자의무기록에 대한 전자적 침해행위로 진료정보가 유출되거나 의료기관의 업무가 교란·마비되는 등 대통령령으로 정하는 사고를 말함(출처: 의료법 제23조의3)

○ **병원정보시스템(HIS, Hospital information System)** : 병원의 전반적인 관리 업무를 전산 시스템으로 자동화한 시스템, 병원의 인사 관리 및 급여 관리, 환자의 외래와 입·퇴원관리, 의료 수가 관리, 급식 관리, 병원의 시설 및 의료 장비 관리등 그 속성상 병원의 종사자를 위한 시스템을 말함

○ **전자의무기록(EMR, Electronic Medical Record)** : 의료인이나 의료기관 개설자가 진료기록부 등을 전자서명법에 따른 전자서명이 기재된 전자문서를 말함(출처: 의료법 제23조)

○ **처방전달시스템(OCS, Ordering Communication System)** : 의료기관에서 컴퓨터망을 통해 의사의 처방을 각종 진료 지원부에 전달함으로써 진료 및 처방에 소요되는 시간을 대폭 줄이고, 처방 내역을 컴퓨터에 저장해 두고 환자 진단 시에 이를 손쉽게 조회할 수 있어 진료의 질을 높일 수 있는 의료정보시스템를 말함

○ **의료영상저장시스템(PACS, Picture Archiving and Communication System)** : 의학영상정보시스템으로서 의학용 영상정보의 저장, 판독 및 검색 기능 등의 수행을 통합적으로 처리하는 시스템을 말함. 즉, PACS는 X선, CT, MRI, PET, SPECT 등에 의해 촬영된 모든 방사선 검사 결과를 디지털 이미지로 변환, 촬영과 동시에 대용량 기억장치에 저장시켜 영상의학과 전문가가 모니터를 통해 판독할 수 있도록 해주는 시스템를 말함

2. 의료기관 랜섬웨어 공격동향

2-1. 국내·외 랜섬웨어 공격 현황

□ 全세계 랜섬웨어 피해는 115억 달러(12조 2,049억원) 전망('19년, 사이버크라임)

<출처 : 지란지교시큐리티>

○ 랜섬웨어 침해 건수는 줄어든 반면, 피해 규모나 공격 양상은 갈수록 커지고 고도화되고 있음

○ 사이버 범죄자는 데이터를 암호화하는 것뿐만 아니라, 데이터를 도용해 인터넷에 공개하는 등 새로운 유형의 위협으로 진화

※ `19년 12월, 메이즈(Maze)라는 해커그룹은 몸 값 지불을 거부할 경우, 랜섬웨어에 감염된 조직에서 도난당한 데이터를 공개하겠다고 위협

□ 랜섬웨어는 기업 대상의 다양한 산업으로 점차 확대(2020 보안위협전망, 안랩)

○ 불특정 개인PC 대상의 무차별 공격에서 공공기관 및 기업 대상 APT(Advanced Persistent Threat)[3]를 통한 타깃형으로 확대

3) APT(Advanced Persistent Threat) : "지능형 지속 공격"은 잠행적이고 지속적인 컴퓨터 해킹 프로세스들의 집합으로, 특정 실체를 목표로 하는 사람이나 사람들에 의해 종종 지휘된다. 보통 개인 단체, 국가, 또는 사업체나 정치 단체를 표적으로 삼는다. "고급(Advanced) 프로세스는 시스템 내의 취약점을 공격하기 위해 악성 소프트웨어를 이용한 복잡한 기법을 나타낸다. "지속(Persistent) 프로세스는 외부 C&C(커맨드 앤드 컨트롤) 시스템이 지속적으로 특정 대상의 데이터를 감시하고 추출한다. "위협(Threat) 프로세스는 공격을 지휘할 때 인간이 동반됨을 뜻한다. (출처: ko.wikipodia.org)

○ 지방자치단체, 병원, 학교 또는 경찰서와 같은 공공기관을 대상으로 랜섬웨어 공격 시, 업무중단, 정보유출 등 피해 강도는 더 커짐

- 미국은 랜섬웨어 공격이 '19년 12월 기준으로 113개 정부기관, 지방자치단체, 주정부에 영향을 미쳤으며, 764개의 의료 서비스 제공업체와 89개의 대학교 및 단과대학 등이 영향을 받을 가능성이 있다고 보고 (2019.12월, 보안 업체 엠시소프트(Emsisoft) 보고서)

○ 랜섬웨어 감염 시 백업 파일까지 암호화 등 피해 범위가 확대되며, 점차 높은 금액의 복구비용을 요구하고 있음

□ 다양한 감염 경로, 강력한 암호화 알고리즘 등으로 지능화

○ 많은 기업이 네트워크 및 보안관리를 MSP*에 아웃소싱 함에 따라, 특정 액세스 권한을 가진 MSP 해킹도 랜섬웨어 감염 경로로 부상

* MSP(Managed Service Provider) : 네트워크를 통해 여러 기업들에게 네트워크, 어플리케이션, 시스템 등을 관리하는 사업자

○ 공격대상 직원이 관심을 가지거나 자주 방문하는 사이트 해킹(워터링 홀)을 통한 랜섬웨어 감염 경로도 부활하고 있음

※ Internet Explorer 취약점을 악용해 RIG Exploit Kit 공격으로 유포되는 Buran 랜섬웨어 발견('19.6월)

○ 대부분 랜섬웨어 해커조직은 데이터를 암호화 시 암호해독이 거의 불가능한 강력한 암호화 알고리즘인 AES256을 사용

○ 최근 이중 암호화 알고리즘을 사용한 새로운 랜섬웨어(PXJ*)도 등장

* '20년 2월에 바이러스토탈을 통해 발견된 랜섬웨어 PXJ는 AES로 먼저 데이터를 암호화한 후, 한 번 더 RSA로 암호화하는 등 이중으로 암호화 알고리즘을 사용

□ 국내 랜섬웨어 공격을 통한 피해액은 지속적으로 증가

○ ’19년 상반기, 러시아 조직 ’갠드크랩(Gandcrab)’이 배포한 랜섬웨어에 감염된 복호화 사례를 집계한 결과, 한국이 11%로 가장 높음

※ 한국(11%), 중국(7%), 인도(7%), 독일(7%), 미국(6%) 등(출처 : 한국랜섬웨어대응센터)

○ 한국 맞춤형 이메일을 보내 PC에 랜섬웨어를 감염시키는 사례도 꾸준히 증가하고 있음

※ ’16년 한국에서 활동하는 랜섬웨어 ’넴티(NEMTY)’는 입사지원서, 상담·문의 등을 가장하거나 공정거래위원회를 사칭한 이메일을 보내 피해를 야기

○ 윈도우7 지원종료 등 보안취약점을 악용한 변종 랜섬웨어 공격에 대한 피해 우려가 높아지고 있음

- 워너크라이는 ‘17년 5월 기술 지원이 종료됐던 윈도우XP 취약점을 노려 전 세계 150개국 30만대에 달하는 PC를 감염시켜 피해를 발생시킴

- 한국에서도 000영화관의 일부 상영관 광고서버가 랜섬웨어에 감염돼 영상 송출이 중단되는 사고 발생

2-2. 의료분야 랜섬웨어 공격 현황

□ 생명을 긴급하게 다루는 의료 분야는 거액의 몸값을 요구하는 랜섬웨어의 주요 공격 대상이 되고 있음

○ 병원의 인프라 및 전자의무기록 저장소가 랜섬웨어 공격을 받아 일부 수술이 중단되거나, 대규모 환자 의료기록에 접근하지 못하여 병원 업무가 마비되는 상황이 발생하고 있음

의료서비스 피해 사례
사례① 2017년 7월, 스코틀랜드 나부 래넉셔의 국민 건강 서비스(NHS) 시스템이 랜섬웨어에 감염되어, 65만 4,000명이 넘는 환자에 대한 예약이 미뤄지거나 취소되는 사태 발생 - 해당 랜섬웨어는 피싱 전자 메일로 전송된 멀웨어 형태로 시스템에 침투 - 해커는 해당 보건기관에 50비트코인 또는 21만 8,000달러(약 2억 4,500만원)을 요구
사례② 2019년 12월, 미국 뉴저지의 가장 큰 병원 운영 단체가 랜섬웨어에 당해 5일 동안 뉴저지 최대 병원 건강 네트워크(Hackensack Meridian Health)가 마비됨 - 약 100여개의 선택적 수술 일정이 조정, 종이로 사용하는 등 의료 업무에 불편함 초래 - 운영 정상화를 위해 공격자들에게 요구한 돈을 지불하고 시스템을 복구한 것으로 알려짐

□ 환자의 민감한 의료 기록을 보유하고 있으나, 이에 대한 보안은 미흡

○ 의료 분야는 상대적으로 사물인터넷 장비들이 많은 편이나, 중요한 디지털 자산들과 망분리 사례가 없어, 환자 데이터베이스 등 중요 자산에 큰 방해없이 도달할 수 있는 상황

의료기록 파괴 사례
사례① 2015년 12월부터 이란인 해커 2명이 미국 도시 애틀란타, 뉴어크, 샌디에고의 인프라 및 콜로라도주의 대중교통국, 의료 관련 기관 6곳의 시스템에 랜섬웨어 공격 - 200명 이상이 피해, 3000만달러(약 336억원) 손실, 해커는 600만달러(약67억원) 수익
사례② 2018년, 미국 미주리주 해리슨빌의 병원 내 인프라 및 전자건강 기록 저장소가 랜섬웨어 공격으로 즉각 일부 수술이 중단
사례③ 2019년 1월, 호주 멜버른의 심장병원 카브리니(Cabrini)가 랜섬웨어 공격을 받아 약 1만 5,000여명의 환자 의료기록에 접근하지 못하게 됨 - 감염 경로는 병원 소프트웨어를 사용하던 누군가가 실수로 피싱 메일의 링크를 열어 감염 - 암환자의 신상정보 등 민감한 의료 기록이 포함, 암호 화폐를 지불했으나 일부 파일은 미복구

□ 최근 ‘코로나19‘이슈 등을 악용한 랜섬웨어 공격이 급증하고 있으며, 이에 랜섬웨어 대응을 위한 기관 및 기업 간 공조·협력 움직임 활발

○ 기존 랜섬웨어 변경 형태로 등장하여, ‘코로나 바이러스’로 명칭을 변경하거나 랜섬노트 내 ‘코로나’ 키워드를 언급하는 사례가 다수 발견

○ 전 세계 법 집행기관*과 IT 보안업체들이 랜섬웨어 사이버범죄 비즈니스 모델을 붕괴하고자, **랜섬웨어 복구 프로젝트(No More Ransom)**[4] 운영

* 네덜란드 경찰청(National High Tech Crime Unit), 유로폴(European Cybercrime Centre)

- 2020년 6월 기준, REDRUM, JAVALOCKER, GOGOOGLE 등 12개 랜섬웨어에 대한 일부 데이터는 복구 가능

랜섬웨어 명	주요 내용
ChineseBAT 변종	- 'Wuahn China' 키워드가 포함된 엑셀파일로 위장하여 유포 - 사용자 파일을 암호화하지만, 다수 파일이 암호화되지 않고 삭제 처리됨
Deniz Kizi	- '19.12월 중순 최초 발견 후, 지속적인 버전 업그레이드를 통해 기능 개선 - 최근 발견된 샘플은 'MPRESS 패커'를 사용하여 보안 SW의 탐지 우회 시도
Hakbit 변종	- 코로나19 이슈를 노리고, 이름을 "Corona Ransomware'로 변경 - 사용자PC를 감염시킨 후 보여주는 랜섬노트에 디코더(decoder)명이 'Corona decryption'이라 명명되어 있으며, 랜섬노트 최하단에는 'Corona ransomware'라 명시되어 있음
MBRlock 변종	- 사용자 파일을 암호화 후 보여주는 랜섬노트에 'CORONAVIRUS is there'이라는 키워드가 포함됨 - 파일 암호화 이후에는 PC 재부팅을 시도하지만 부팅이 불가함
Netfilim	- 넴티 2.5와 코드상 매우 유사하나, 서비스형 랜섬웨어 구성요소가 제거됨 - 노출된 윈도우 원격 접속·관리 기능(RDP)을 노리고 유포되며, Tor 브라우저가 아닌 이메일통신을 통해 랜섬머니 결제를 유도함 - 랜섬머니를 지불하지 않는 피해자의 데이터는 공개한다고 협박
NetWalker 변종	- Mailto 랜섬웨어의 변종으로, 최근 코로나 이슈를 악용한 피싱 메일을 통해 유포 중임 - 복호화 페이지 내 캡챠(Captcha)를 사용

<출처 : `20년, 이글루시큐리티 >

4) 노모어랜섬(No more ransom) 프로젝트 : 전세계의 법집행기관 및 IT보안 업체들이 범죄자들에게 돈을 지불하지 않고 암호화된 데이터를 복원하는 것을 목표로 설립, **일부 알려진 랜섬웨어의 경우 복호화 방법**과 키(Key)를 제공(www.nomoreransom.org)한다.

3. 의료기관 랜섬웨어 피해 예방 방법

3-1. 진료정보 백업조치

□ 백업의 필요성

○ **(의료정보시스템 노출)** 병·의원급 의료기관에서는 방화벽 등 보안장비를 운용하고 있지 않은 곳이 많아 랜섬웨어 감염에 취약할 수 있음

○ 특히, 영상판독(X-ray, CT, MRI 등)을 위해 외부 영상의학과 전문의에게 원격 판독을 의뢰하는 경우가 많아, 접속하는 원격 단말기가 악성코드에 감염 노출

○ 랜섬웨어 감염시 대가를 지불하지 않고, 원복할 수 있는 방법은 데이터 백업이 유일

□ 백업 정책

○ **(주기적인 백업정책 수립)** EMR, PACS 등 진료정보를 기록·보관·관리하는 정보시스템에 대한 일·주·월·년 단위 백업 정책수립이 필요

○ **(대상별 정책)** 백업 대상에 따라 시스템 백업, 데이터 백업, 변경 로그 백업 등으로 목적에 다양한 방식이 존재

- 다중 백업이라도 랜섬웨어로부터 진료정보를 안전하게 보호하기 위해서는 소산백업 이후 네트워크를 분리하여 보관 필요

<진료정보 보호를 위한 백업정책 적용 예시>

대상별 종류	백업대상	백업방식	백업주기
데이터베이스 (진료정보 포함)	DBMS / 구성파일	FULL	격주 / 주 1회
	DB Archive Log	FULL/INC[5]	
파일시스템 백업	Application실행 파일 및 소스	FULL/INC	
	진료정보 및 일반 DATA	FULL/INC	
	각종 Log 파일	FULL	
시스템 백업(OS)	OS 파일 시스템 백업 (Boot 영역)	FULL	월간 백업 변경작업 전

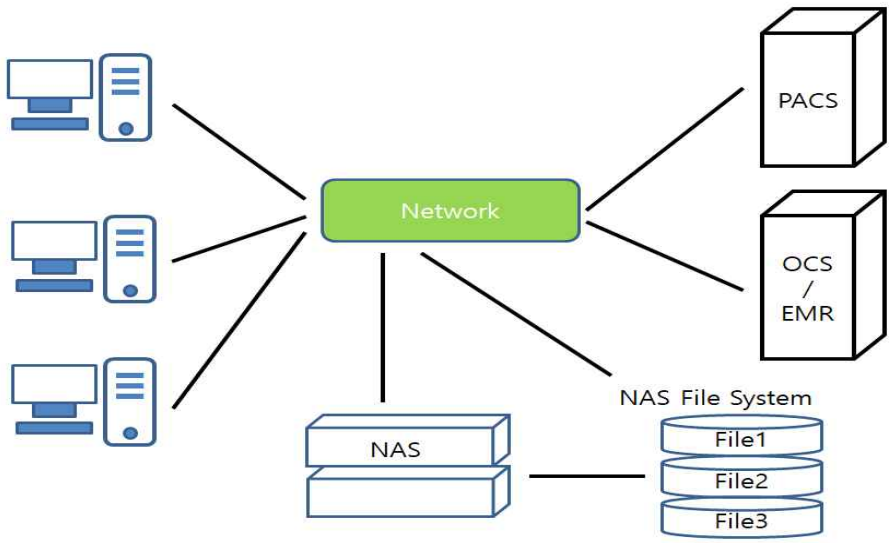
<출처: 중소기업정보시스템백업지침(TTAK.KO-12.0340 표준, 2018.12.19.>

5) FULL은 Full Backup을 말함, INC는 Incremental Backup을 말함

□ 규모별 백업방법

○ **(대형병원)** 상급종합, 종합병원 등 대형병원 내부에 1차적으로 자체백업시스템(NAS 또는 테이프 방식)구축하여 진료정보를 안전하게 보호할 필요 있음

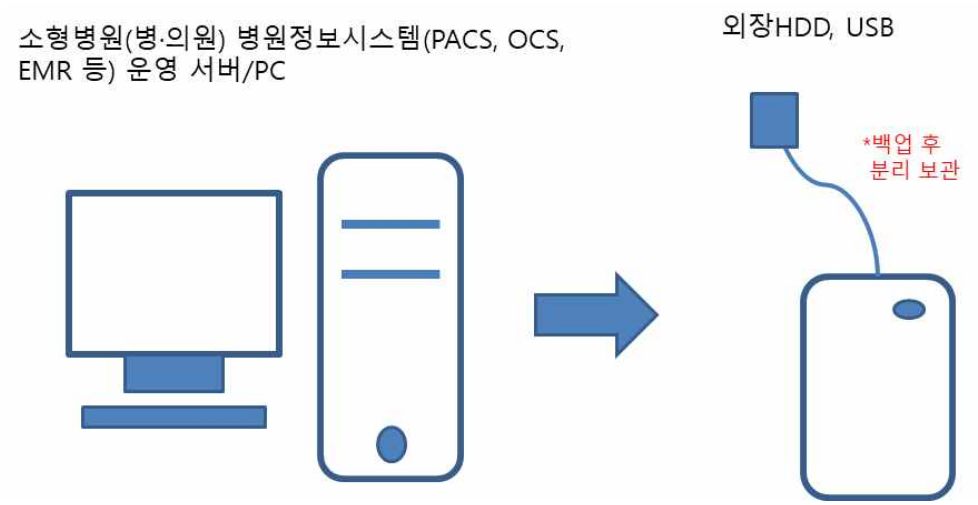
- NAS 백업은 다양한 백업기능을 제공하며, 동일장소 데이터 백업 시 온라인 백업 후 백업 매체(테이프) Off-Site 보관(네트워크 분리)도 가능
- 또한, 백업 전/후 시스템 관리시 접근통제 절차 마련하여 보안성을 강화할 필요(예: 허가된 사용자만 접근 가능하도록 별도 캐비넷에 보관)



<NAS 백업 구성 개요>

○ **(소형병원)** 병·의원, 한의원 등 소형병원의 경우 백업시스템 도입시 예산투자에 어려움을 고려하여, 1차적으로 외장HDD(USB도 가능)를 활용할 필요

- 외장HDD, USB 백업은 데이터 용량이 비교적 작은 경우 적합, 별도의 백업 소프트웨어 없어 사용자가 직접 백업 계획을 수립
- 매일·주단위 등 주기적으로 데이터 백업을 실시한 후 캐비넷 또는 문서고에 보관하는 등 통제 절차 필요, 외장HDD 또는 USB를 시스템에서 분리하여 별도 잠금장치가 있는 케비넷에 보관



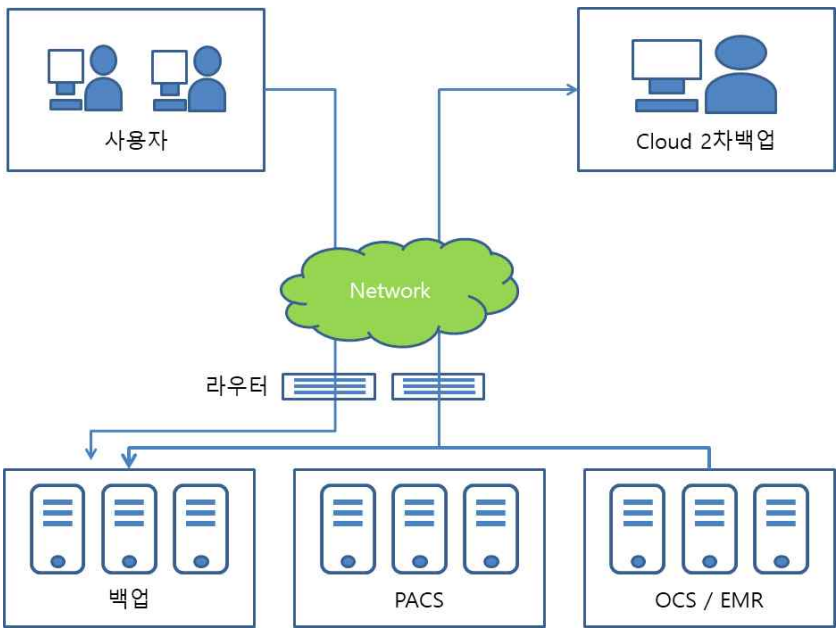
<외장HDD, USB 백업 예시>

<참고>

o **(Cloud 백업)** 최근 많은 공공클라우드 서비스 사업자가 백업서비스를 제공하고 있어, **모든 의료기관은 2차 백업에 클라우드 활용 가능**

- 외부 영역에 데이터를 백업하는 방식, 외부 소산 관리가 용이하며, 보안 서비스를 제공받을 수 있는 장점, 다양한 백업 기능을 사용할 수 있어 유리

※ 단, 진료정보의 외부 보관은 안전을 담보해야 함, 법적규정을 준수할 필요



<Cloud 백업 예시>

3-2. 의료기관 네트워크 보안설정

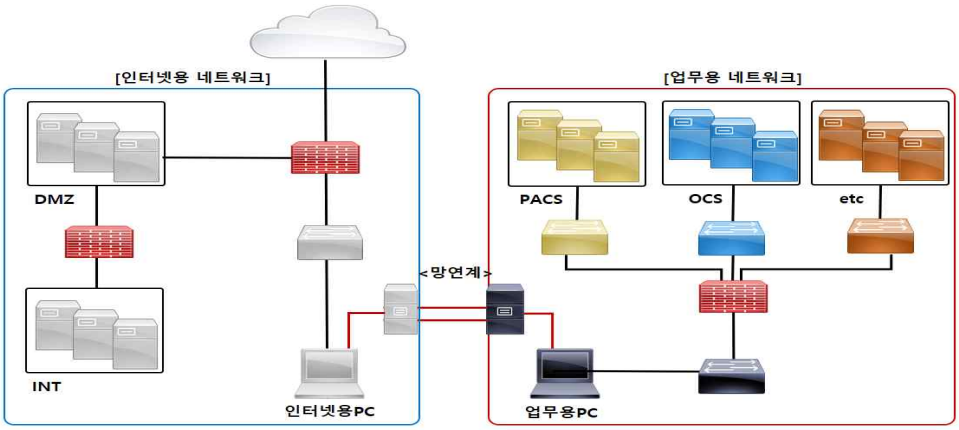
□ 네트워크 보안설정

○ 인터넷용과 업무용으로 구분하여 사용

- 의료기관 네트워크는 2회선 이상으로 분리·구성하여, **인터넷용(환자, 보호자 등)과 업무용**으로 분리운영

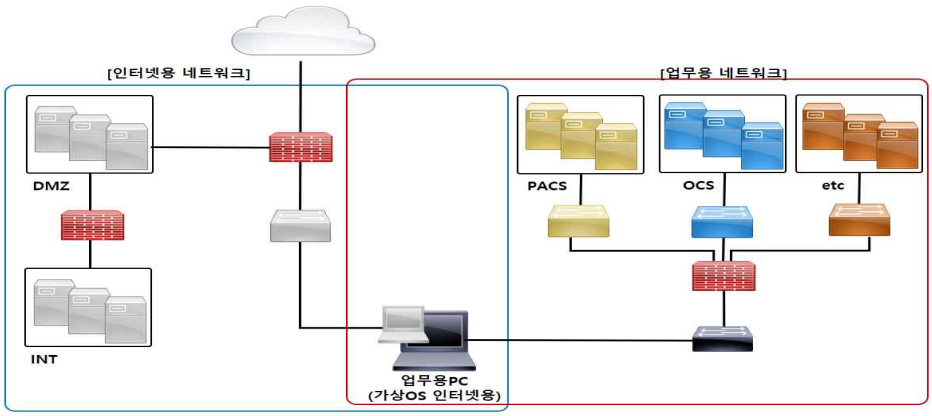
○ 업무용에 인터넷 접속은 별도의 설정

- 업무용 네트워크는 진료 및 접수 등 의료기관에서 수행되는 업무 외에는 차단하고 직원의 인터넷 접속은 외부 인터넷 접근이 필요한 업무(외부 메일 열람, 타기관 접근 등) 수행을 화이트리스트 방식 정책 적용



<물리적 네트워크 분리 예시>

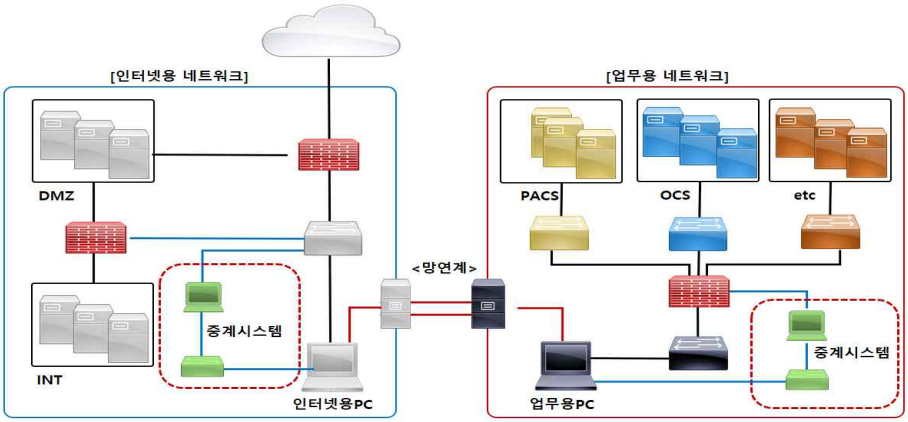
- 네트워크를 분리가 어려운 의료기관일 경우 논리적 네트워크 분리 후 가상PC를 이용하여 네트워크 분리



<논리적 네트워크 분리 예시>

○ DMZ구간, 서버구간 네트워크의 분리

- 서버가 위치한 네트워크는 내부망(업무망, 인터넷망)과 다른 네트워크로 구분 및 제공되는 서비스 외에 불필요한 통신은 방화벽 등으로 접근 차단
- 원격 접근 필요할 경우 비인가 접근 불가하도록 중계시스템 또는 접근통제시스템 이용하여 불필요한 접근 차단



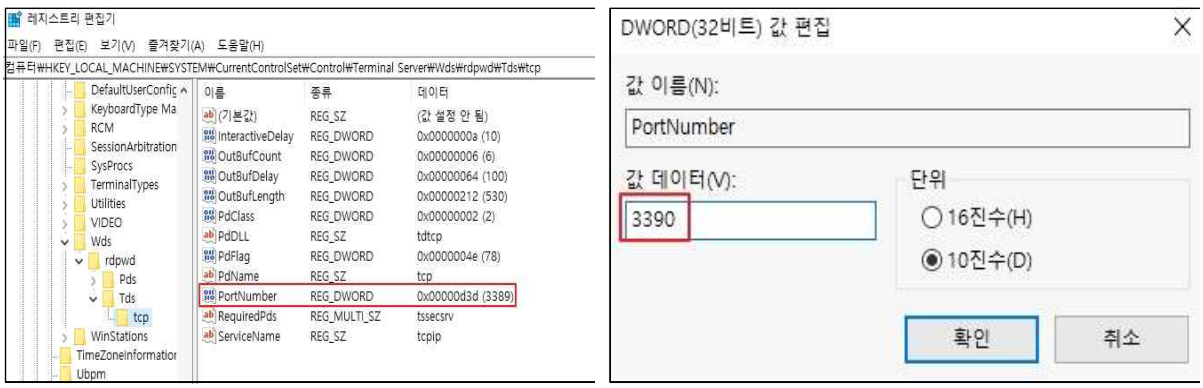
<서버구간 네트워크 분리 및 원격접근 예시)>

○ 원격 데스크톱(RDP) 보안설정

- 서버관리를 위한 원격접속용 원격데스크톱(RDP)은 외부 침입의 경로로 악용되는 경우가 많아 원칙적으로 사용을 중지해야 함

※ RDP 비활성화 : Windows 설정 → 시스템 → 원격 데스크톱 → 원격 데스크톱 활성화 끄기

- 불가피하게 사용이 필요할 경우 알려진 포트(3389)를 반드시 변경

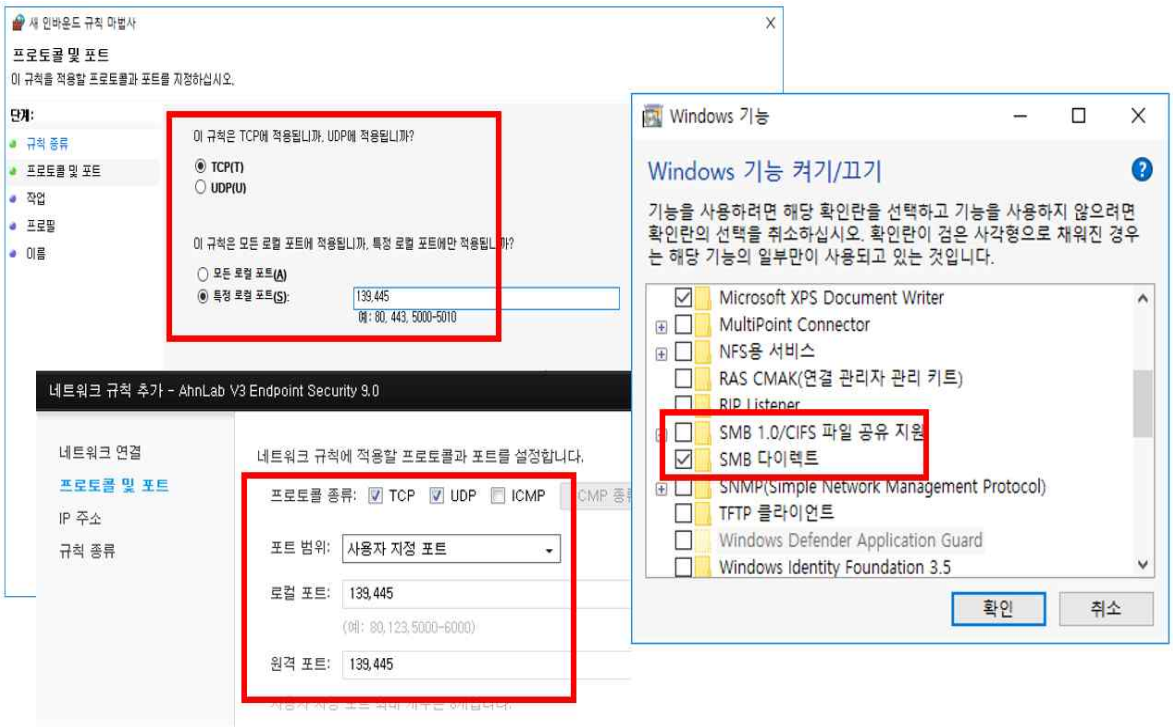


▶ [레지스트리 편집기]를 실행 후 [PortNumber]를 선택
▶ 10진수를 선택하여 원하는 임의의(예: 3390)포트 번호로 변경 후 사용

□ 업무용 PC 보안설정

○ SMB[6] 서비스 중지 및 통신 차단

- 윈도우 방화벽 또는 백신에서 제공하는 개인방화벽 기능을 이용하여 SMB통신 포트(TCP 139,445)를 차단정책을 활성화하고 SMB 파일 공유 지원 프로그램을 제거

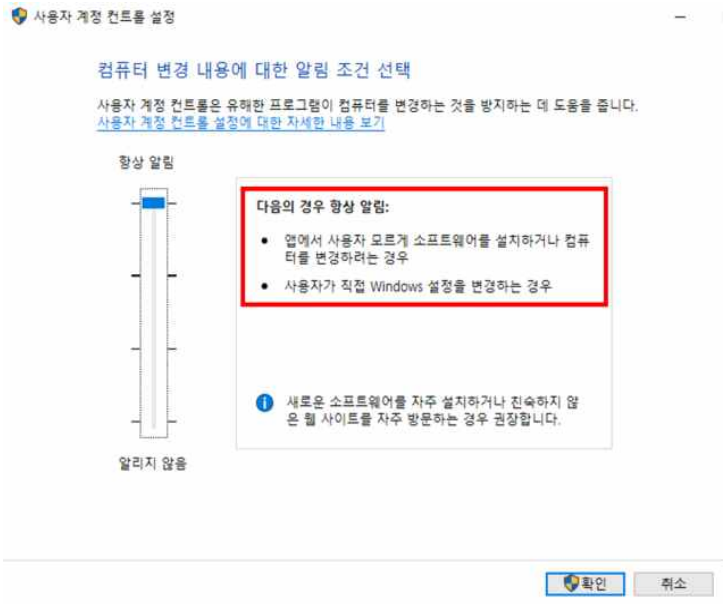


<윈도우 방화벽 설정 및 SMB 파일공유 지원 제거>

○ 사용자 계정 컨트롤(UAC) 활성화

- 관리자 수준의 권한으로 실행이 필요한 경우 사용자에게 알림으로써 랜섬웨어 및 악성코드 등이 사용자 모르게 설치 및 실행되는 것을 방지

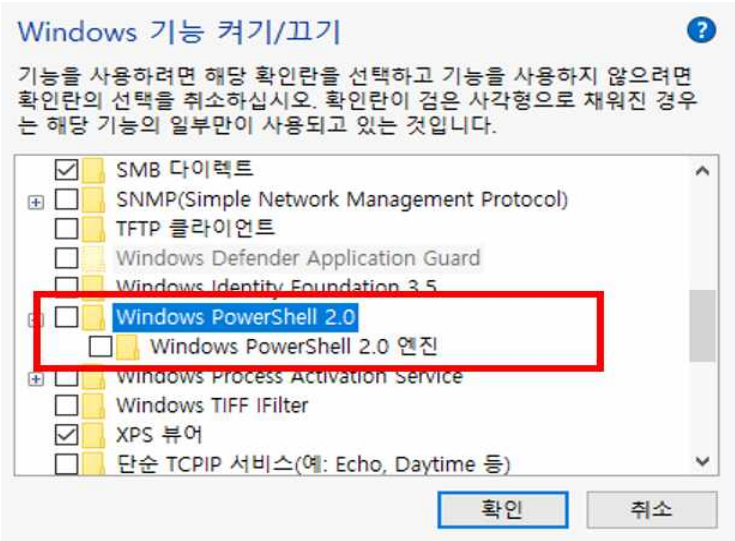
6) SMB(Server Message Block)란 마이크로소프트사와 인텔이 윈도우 시스템이 다른 시스템의 디스크나 프린터와 같은 자원을 공유할 수 있도록 하기 위해 개발되었다. SMB는 OS/2, NT, WIN9x를 사용하는 컴퓨터끼리 파일 공유등의 서비스를 구현하는데 사용되는 프로토콜이다. TCP/IP 기반하의 NETBIOS 프로토콜은 NFS, NIS, lpd와 같은 유닉스의 분산인증구조와 유사하다.



<사용자 계정 컨트롤(UAC) 설정>

○ 윈도우 파워쉘 기능 비활성화

- 파워쉘은 리눅스에 쉘스크립트과 같이 윈도우에서 제공하는 스크립트로 사용하지 않을 경우 해당 기능 중지하여 파워쉘을 이용한 랜섬웨어 감염을 방지



<윈도우 파워쉘 기능 중지>

3-3. 의료기관 랜섬웨어 예방수칙

□ 백신 소프트웨어 설치 및 최신 업데이트

○ 업무용 PC·서버에는 백신 소프트웨어 설치하고, PC·서버가 최신 공격탐지 패턴을 적용할 수 있도록 주기적인 업데이트(예: 컴퓨터 시작시, 매일 10시 등)

□ 외부에서 내부 서버·PC로 원격접근 금지

○ 원격데스크톱, 텔넷(Telnet) 등의 **원격접속 프로그램은 필요시에만** 서비스를 연결하여 사용하고, **그 외의 시간에는 서비스 이용을 중단**

□ EMR, PACS, OCS 등 모든 진료정보 매일매일 백업

○ 의료정보시스템(EMR, PACS 등) 및 의료기관 관리하는 모든 진료정보는 **백업시스템(외장HDD, USB 등 포함)**을 활용하여 **주기적으로 백업**

□ 출처가 불분명한 이메일, URL링크 열람금지

○ 의료기관의 **자체메일**이나 **외부메일서비스**를 이용하는 경우, 악성코드(랜섬웨어, 애드웨어 등)를 다운로드하게 하는 **불분명한 악성메일 열람금지**

- 메일서버 보안시스템(스팸필터 등)을 운용중인 의료기관이라도 APT 공격을 위한 피싱 메일에 노출될 수가 있으니 주의가 요구

□ Windows 10 등 모든 소프트웨어 최신 업데이트

○ Windows 10 등 의료기관이 운용하는 **PC·서버**에 대해서는 주기적으로 **최신 업데이트**를 적용할 수 있도록 **점검(매일·매주·월간 등)**

※ Windows XP·7 등 서비스 종료된 소프트웨어는 각별한 주의가 요구되며, 필요시 최신 버전으로 업그레이드

□ 내부 파일공유(SMB) 금지 및 외부 공유사이트 접근 주의

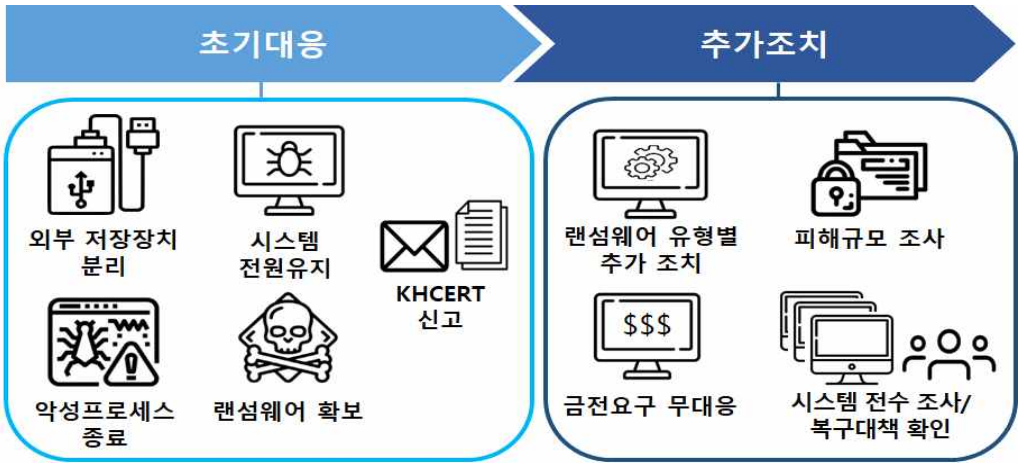
○ 진료정보를 공유하기 위한 공유 디렉토리 사용은 랜섬웨어외에도 진료정보 유출 사고가 발생될 수 있어, **공유 디렉토리 사용은 금지**

- **토렌트 등 불법 다운로드 링크**를 통한 파일 다운로드는 **원천차단**

4. 의료기관 랜섬웨어 침해사고 대응방법

4-1. 의료기관 초동조치 및 복구요령

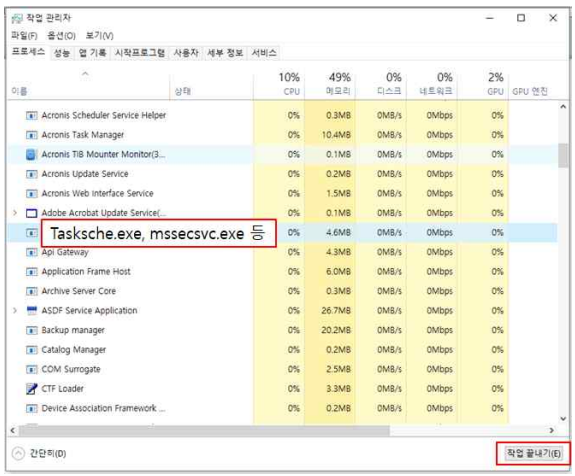
□ 전자의무기록시스템(PACS, EMR, OCS 등) 랜섬웨어 감염 조치방법



<전자의무기록시스템 초기대응 및 추가조치>

○ **(초기대응)** 담당자는 의심 증상 발견시 초기대응 수행

- 피해시스템에 USB 등 직접 연결된 외부 저장장치가 있을 경우 분리
- 부팅영역까지 암호화로 인한 부팅 불가를 고려하여 시스템의 전원유지
- 실행중인 프로세스를 확인(실행파일 경로 확인)하여 비정상 또는 의심되는 프로세스를 확인하여 종료 처리* 및 악성파일 원본 확보
- KHCERT로 사고내용 신고(통지) 및 기술지원 요청(부록 B 참조)



① Ctrl + Alt + Delete
② "작업관리자" 선택
③ 좌측 화면에서 악성(비정상) 프로세스 (Tasksche.exe, mssecsvc.exe) 확인
※ 좌측 프로세스는 워너크라이 랜섬웨어의 악성 프로세스 예시이며, 악성코드 유형에 따라 프로세스 명은 상이할 수 있음
④ 해당 프로세스 클릭 후 우측하단 "작업 끝내기" 선택

<*악성(비정상) 프로세스 종료 방법 - WannaCry 랜섬웨어 예시>

○ **(추가조치)** 초기대응 수행 후 KHCERT의 안내사항 이행 및 자체 추가조치
- 암호화된 파일의 확장자, 랜섬노트, 감염 메시지 등을 확인하여 랜섬웨어 유형 확인 및 랜섬웨어 특성에 따른 추가 대응방안 적용
- 파일 복구를 위한 금전 지불에도 복구를 보장받지 못하는 경우를 고려하여 해커의 금전요구에 대응하지 말 것
- 추가적인 피해시스템 확인을 위한 정보시스템 전수조사, 암호화된 데이터 확인을 통한 피해규모 파악
- 암호화된 데이터에 대한 백업 여부 및 복구대책 확인

□ 의료기관 네트워크 및 보안장비 랜섬웨어 감염 조치방법

<의료기관 네트워크 및 보안장비 초기대응 및 추가조치>

○ **(초기대응)** 의료기관 담당자는 랜섬웨어의 피해확산을 차단하기 위해 의료기관 네트워크 및 보안장비를 통한 초기대응 수행
- 피해시스템에 네트워크로 연결된 외부 저장장치의 연결 해제
- 랜섬웨어 확산 방지를 위해 피해시스템에 대한 네트워크 격리(랜선 분리)
- RDP, TeamViewer 등 내·외부 원격접속 및 SMB 포트 차단

○ **(추가조치)** 의료기관 담당자는 전자의무기록시스템 등 중요서버 영역으로 랜섬웨어 확산을 차단하기 위해 추가조치 수행
- EMR, PACS 등 전자의무기록시스템에 대한 피해 확산이 예상되는 경우, 인터넷 또는 피해 시스템이 포함된 영역에 대한 네트워크 차단
- 침입탐지시스템(IDS), 방화벽, 백신 SW 등 보안장비 이벤트 및 로그 확인을 통한 감염 경로·원인 파악

□ (공통) 백업 자료를 활용한 복구방법

<백업자료를 활용한 복구방법>

○ 의료기관 담당자는 피해범위에 따라 자체 복구 대책 또는 진료정보침해대응센터(KHCERT) 가이드를 참고하여 복구절차 수립 및 복구 수행

- (1단계) 데이터, 소프트웨어, 시스템, 하드웨어 등 피해복구 범위결정
- (2단계) 다수의 시스템을 복구하는 경우 업무 중요도 및 특성에 따라 피해복구 우선순위 결정
- (3단계) 백업 데이터를 통한 데이터 복구, 시스템 재설치 등 피해복구

○ Windows OS에서 제공하는 백업 복구 기능을 활용하여 특정 복원시점으로 데이터 및 시스템 복구

- Windows 복구 옵션(복구, 초기화, 복원)*을 선택하여 시스템 재설치

  *복구(OS재설치, 개인 파일 및 설정 유지), 초기화(OS재설치, 사용자 파일 및 설정 삭제), 복원(최근 시스템 변경 사항에 대한 실행 취소)

- Windows 파일 히스토리를 사용하여 데이터 복원*

  * Windows 검색→“파일복원” 입력→“파일 히스토리로 파일 복원” 선택→복원이 필요한 파일의 이름을 검색 상자에 입력→복원 대상 파일 선택→“복원” 버튼 선택

  ※ 단, Windows OS에서 제공하는 복구 기능이 활성화되어 있고, 복구를 위한 볼륨 쉐도우 복사본이 정상일 경우 적용 가능

○ 백업 솔루션을 통한 암호화된 데이터 복구

- 백업 파일 존재 여부를 파악, 원본 및 백업 파일의 감염, 손상 여부 확인 등 복구 대상 선정
- 백업 데이터를 복구하기 위한 솔루션에 따라 백업 목록에서 복구 대상 파일・폴더・디스크 등을 선택하여 복구 수행

4-2. 재발 방지대책 적용방법

□ 전자의무기록시스템(PACS, EMR, OCS 등) 재발 방지대책

<전자의무기록시스템 재발 방지대책>

○ 전자의무기록시스템의 원격데스크탑(RDP) 사용 자제, 불가피하게 사용할 경우 기본 포트 변경* 및 접근가능 계정 설정**

*레지스트리 편집기를 통한 RDP 포트 변경, 윈도우 방화벽에서 해당 포트 허용 설정,인터넷 공유기에서 외부 RDP 접속에 대한 포트 포워딩 설정

**제어판→시스템→원격데스크톱→사용자계정에서 접속 가능한 계정 설정

○ 운영체제의 기본 계정 삭제*, 원격접속을 위한 계정 별도부여 및 권한 최소화, 로그인 암호 복잡도(영문, 숫자, 특수문자 조합 및 10자리 이상) 설정

*윈도우 설정→계정→가족 및 다른 사용자 선택 후 GUEST 계정 선택 후 제거

○ 전자의무기록시스템의 운영 서버와 물리적으로 분리된 백업체계* 운영 및 점검

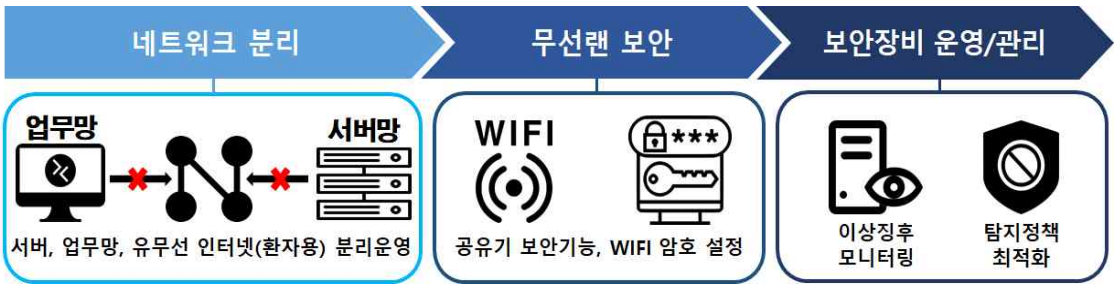
*사이버 공격 대응을 위한 중소기업 정보시스템 백업 지침(TTA.KO-12.0340, 2018.12.19) 참고

○ 업무용 PC(서버, 워크스테이션 포함)의 백신 SW 설치, 운영 및 정기적 업데이트 실시

○ 전자의무기록시스템에 설치된 운영체제 및 응용프로그램에 대한 최신 업데이트 및 보안패치 설치・유지

○ 의료기기에 포함된 PC・워크스테이션에 불필요한 서비스 제거 및 백신SW 설치 운영

□ 의료기관 네트워크 및 보안장비 재발 방지대책



<의료기관 네트워크 및 보안장비 재발 방지대책>

○ 서버(PACS, EMR), 업무망, 유무선 인터넷망 분리 운영*

*물리적(2PC, 1PC, 폐쇄망) 또는 논리적(PC·서버 가상화 등) 망분리(참고: 개인정보의 기술적·관리적 보호조치 기준 해설서(방통위, KISA))

○ 공유기 보안기능(VPN, IP/MAC 접근제어) 활성화 및 WIFI 암호 설정*

*관리자 페이지 및 WIFI 비밀번호 설정, 공유기 원격관리 기능 해제, 공유기 펌웨어 최신버전 유지 등 보안 설정(참고: 유·뮤선 공유기 보안 설정 권고, www.krcert.or.kr, 보안공지)

○ 보안장비 탐지정책 최적화 유지관리, 탐지 이벤트・이상징후* 모니터링

*원격접속시도 증가, SMB 포트(139, 445)를 통한 트래픽 증가, 킬스위치(랜섬웨어 확산 여부를 결정하는 역할) 관련 URL 접속 시도 탐지 등

4-3. 진료정보 침해사고 신고 및 기술지원

□ 진료정보 침해사고 신고(통지)기관 안내

○ 명칭 : 진료정보침해대응센터(KHCERT)

※ KHCERT : Korea Healthcare Computer Emergency Response Team

○ 전담기관 : 한국사회보장정보원

※ (관련근거) 의료법 시행규칙 제16조의4(진료정보 침해사고의 예방 및 대응을 위한 업무의 위탁)에 따라 전문기관(한국사회보장정보원)에 위탁

○ 역할 : 진료정보 침해사고의 신고(통지) 접수, 침해사고 예방・대응 등

□ 진료정보 침해사고 통지(신고) 방법

○ (사고신고) 포털*에서 양식 다운로드 후 사고통지(신고)서 작성・신고

*진료정보침해대응센터(KHCERT) 홈페이지: www.khcert.or.kr

○ (사고접수) 365일 24시간 신고접수 처리

○ (계획수립) 피해범위, 조사대상에 따른 현장/원격 조사 등 대응계획 수립

○ (사고조사) 피해시스템, 보안장비 등 사고 데이터 수집 및 사고경위 파악/사고조사 지원

○ (사고분석/기술지원) 사고유형, 침투경로, 취약사항 등 원인 분석/서비스 정상화를 위한 복구 기술지원

※ 세부내용 [부록-B] 진료정보 침해사고 신고 안내서 참고

□ 진료정보침해대응센터 기술지원 내용

○ 침해사고 원인분석 및 침투경로 등 침해사고 원인분석 지원

- 사고 원인 및 공격에 이용된 취약점, 세부 공격 경로 및 기법
- 공격 방어/차단 방안, 피해/유출 세부 내역
- 수집된 법적 증거자료, 공격자 식별 정보
- 침해대응 담당은 의료기관 담당자의 요청에 따라 원인제거 및 사고대응을 지원

○ 의료기관 업무 정상화를 위한 전자의무기록시스템 복구 지원

1단계		
피해복구 범위결정	데이터 복구	○ 정보시스템 내 데이터만 손상된 경우
	S/W 복구	○ 피해 사고가 발생한 시스템의 프로그램 및 운영체제에 단순 오류가 발생한 경우
	시스템 재설치	○ 피해 사고가 발생한 시스템의 운영체제에 복구 불가능한 심각한 오류가 발생한 경우
	하드웨어 교체	○ 피해 사고가 발생한 시스템의 하드웨어적 손상이 발생한 경우

⇩

2단계	
피해복구 우선순위 결정	○ 피해복구 대상 시스템이 두 개 이상인 경우, 기관의 업무 중요도 및 특성에 따라 복구 우선순위 결정 기준 마련 ○ 즉시 조치해야 할 복구 내용과 중장기적인 계획에 의해서 수행해야 할 복구 내용 결정

⇩

3단계		
피해복구	데이터 복구	○ 피해사고 발생 전에 백업하였던 데이터로 복원
	S/W 복구	○ 백신 프로그램을 이용한 악성코드 탐지 및 치료 ○ 소프트웨어 패치를 적용해 공격에 이용한 취약점 제거 ○ 응용프로그램 재설치 및 환경설정
	시스템 재설치	○ 운영체제 CD를 이용한 운영체제 재설치 ○ 필요한 응용프로그램 설치 ○ 백업한 자료를 이용한 데이터 복원 ○ 재설치 완료 후 정상상태 복귀 확인
	H/W 교체	○ 파손된 하드웨어 부품 교체 ○ 정보시스템 및 통신장비 등 교체
	비상통신망 가동	○ 통신망 장애 시 예비 통신회선으로 전환 ○ ISP업체 등과 유기적 협력

⇩

4단계	
사후관리	○ 복구조치 결과에 대한 검토회의 개최 ○ 기관 내 복구계획·절차 개선 및 변경

※ 세부내용 KHCERT 진료정보 침해사고 통지(신고) 대응 매뉴얼 참고

[부록-A] 랜섬웨어 정의 및 피해유형

□ 랜섬웨어(Ransom+ware) 정의

○ 랜섬웨어는 납치된 사람의 몸값을 의미하는 'Ransom'과 소프트웨어를 의미하는 'ware'의 합성어로 시스템을 악성코드에 감염시킨 후 컴퓨터 데이터를 암호화 후 복구 명목으로 돈을 요구하는 악성코드

○ 랜섬웨어는 이용자의 데이터, 시스템파일, 문서, 이미지, 동영상 등을 암호화하고 복구를 위한 금전을 요구하는 악성코드

< 정 의 >

랜섬웨어(Ransomware)란?

Ransom(몸값) + Software(소프트웨어) 의 합성어

시스템을 잠그거나 데이터를 암호화해 사용할 수 없도록 한 뒤, 이를 인질로 삼아 금전을 요구하는 악성 프로그램

구분	일반 악성코드	랜섬웨어
유포	웹사이트, 이메일, 네트워크 취약점 등 유포방식 동일	
감염	SW 취약점 또는 피해자의 실행으로 악성코드 감염 동일	
동작	정보 및 파일 유출, DDoS 공격 등	문서, 사진, MBR 등 데이터 암호화
대응	악성코드유포지 및 명령조정지(C&C)*서버 주소 차단 ※ C&C : 해커가 악성코드에 감염된 PC에 원격으로 접속하기 위한 서버PC로 악성코드 감염 시 C&C에 연결되어 해커의 명령을 수행	악성코드유포지 및 명령조정지(C&C)서버 주소 차단 ※ 복호화 키가 저장된 서버(도메인/IP)와의 통신 경로는 미차단
치료	백신 등을 통해 악성코드 치료	백신 등을 통해 악성코드 치료 → 암호화된 파일은 복구 어려움
피해	개인, 금융 정보 유출 및 이를 이용한 2차 공격으로 피해 발생	암호화된 파일에 대한 복호화를 빌미로 가상통화(비트코인 등)로 금전을 요구

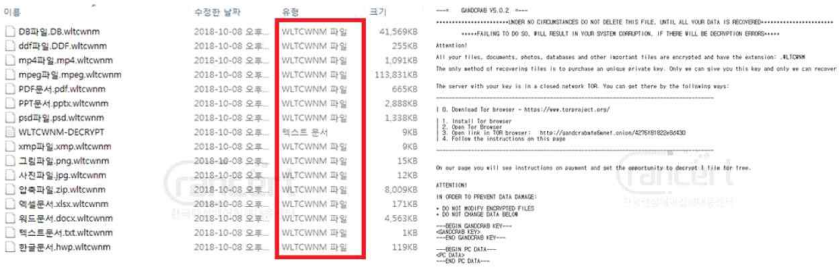
< 일반 악성코드와 랜섬웨어의 차이점 >

(출처: 랜섬웨어 대응가이드라인, 2018, 한국인터넷진흥원)

□ **랜섬웨어 감염 증상**(*아래 유형으로 감염 증상이 나타남)

○ **(웹서버 암호화)** PACS 등 웹서버 저장된 파일들을 암호화

○ **(파일암호화)** 개인의 파일(문서, 사진, 동영상 등)을 암호화, 비용 지불에 대한 설명이 있는 텍스트 파일(랜섬노트) 있음



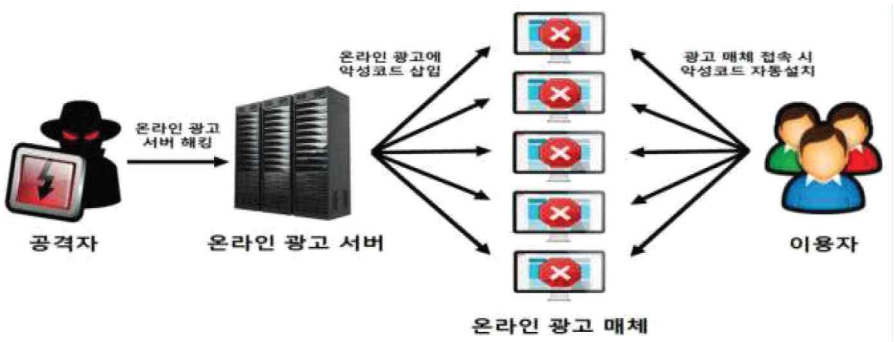
○ **(화면잠금)** 컴퓨터의 화면을 잠그고 비용을 요구, 이미지를 띄워서 모든 윈도우 창들을 사용하지 못하게 함

○ **(마스트 부트 레코드(MBR) 감염)** 컴퓨터의 MBR을 변경시켜 부팅이 되지 않도록 만들고 대신, 금전을 요구하는 화면을 띄움

□ 랜섬웨어 감염경로

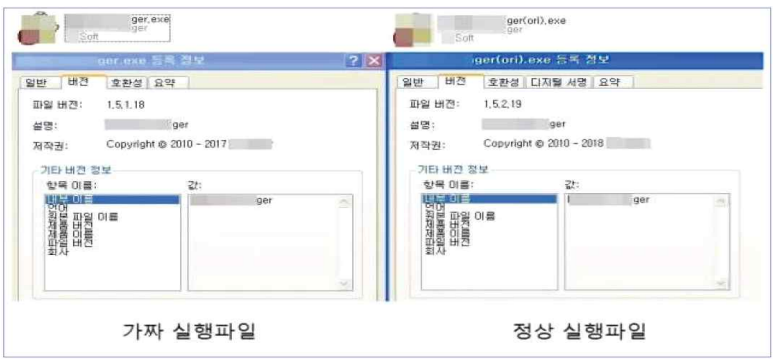
○ **(이메일)** 랜섬웨어를 유포하는 파일이 첨부되어 있거나 다운로드할 수 있는 URL 링크를 포함

○ **(취약점 악용)** 보안이 취약한 웹사이트나 커뮤니티에 접속할 경우 PC 내의 운영체제 및 응용프로그램의 취약점을 이용해 랜섬웨어를 다운로드하고 실행

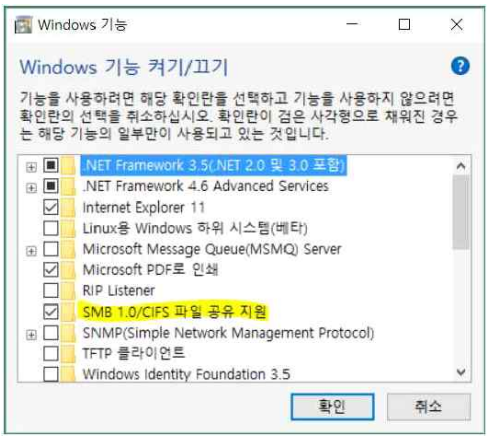


<멀버타이징(Malvertising) 공격개요>

○ **(파일 공유 사이트)** 영화, 사진, 프로그램 파일들 중 랜섬웨어가 담겨있는 위장파일이 있음



○ **(네트워크 전파)** 유·무선 네트워크의 설정 미흡**(특히, SMB 포트 이용)**으로 인해 랜섬웨어가 감염되고 확산(WannaCry 랜섬웨어)



<윈도우 파일 공유 기능>

[부록-B] 진료정보 침해사고 신고 안내서

▣ **진료정보 침해사고란?**

o **정의** : 전자의무기록에 대한 전자적 침해행위(해킹, 악성코드 등)로 진료정보가 유출, 시스템 교란·마비 등이 발생한 사태(**의료법 제23조의3**)

o **범위** : ①진료정보의 도난·유출, ②진료정보의 파기·손상·은닉·멸실, ③전자의무기록 시스템의 교란·마비(**의료법 시행규칙 제16조의3**)

❑ 진료정보침해대응센터 소개

❍ 명칭 : **진료정보침해대응센터(KHCERT)**

※ KHCERT : Korea Healthcare Computer Emergency Response Team

❍ 위탁기관 : 한국사회보장정보원

※ 의료법 시행규칙 제16조의4(진료정보 침해사고의 예방 및 대응을 위한 업무의 위탁)에 따라 전문기관(한국사회보장정보원)에 위탁

❍ 역할 : 진료정보 침해사고의 신고(통지) 접수, 침해사고 예방·대응 등

❍ 설립 법적근거

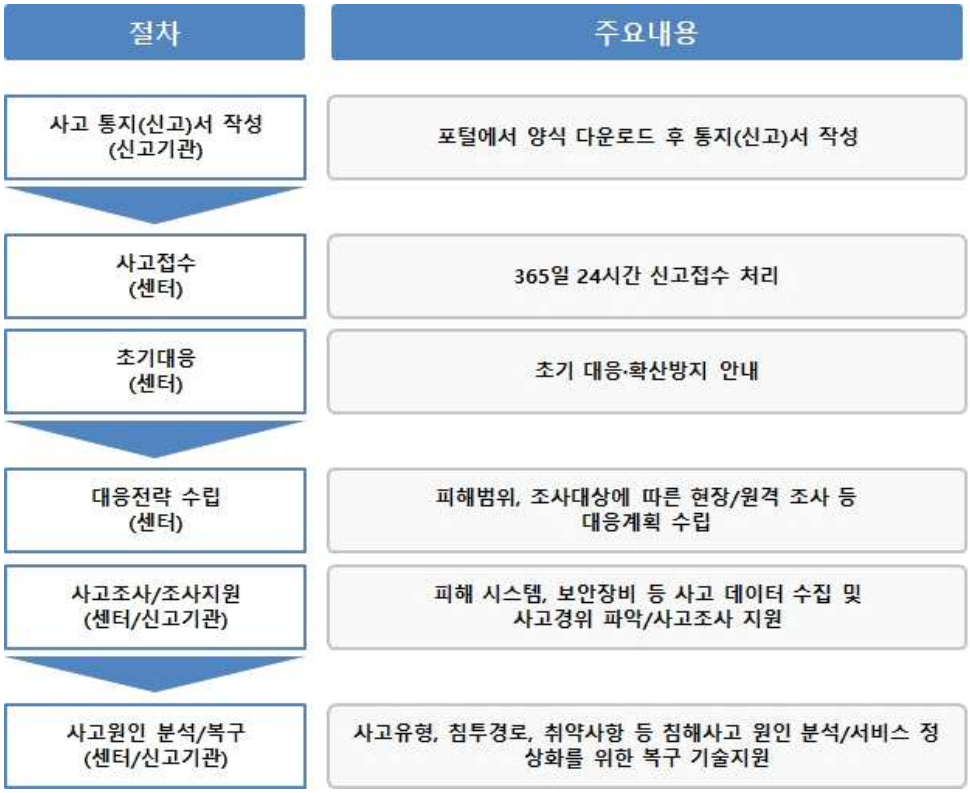
- 「의료법시행규칙」 제16조의4(진료정보 침해사고의 예방 및 대응을 위한 업무의 위탁)에 따라, 진료정보 침해사고 신고(통지) 접수, 사고 예방 및 대응 업무를 수행할 전문 조직 설립

❑ 센터 주요 업무

❍ **진료정보 침해사고 신고(통지) 접수**

- 365일 24시간 상황관제 등을 통한 즉각적 신고(통지) 접수
- 침해사고 피해범위, 사고종류에 따른 초기대응 방법 등 안내

<의료기관 진료정보 침해사고 신고(통지) 절차>



○ 피해 의료기관에 대한 사고조사・분석

※ 침해사고 증거데이터 수집 및 사고경위·종류, 침투경로, 취약사항 등 원인 분석

○ 국내 의료분야 사이버위기대응 경보발령 및 정보공유

○ 진료정보 침해사고에 대한 종합상황분석 체계 구축・운영

※ 의료기관 대상 종합 보안관제, 침해사고 신고 기반 현장조사, 악성코드 분석 등

○ 의료기관 대상 기술적・물리적・관리적 취약점 점검 등 기술지원

○ 진료정보 침해사고 예방・대응 관련 교육 및 훈련 등의 실시

❑ 침해사고 신고(통지) 안내

○ 신고 대상 : **의료기관 전체**(상급・종합병원, 병·의원, 요양병원, 보건의료원)

○ 문의 및 신고 : **진료정보침해대응센터(KHCERT)**

- **문의** : (TEL) 02-6360-6500
- **신고** : (E-mail) cert@khcert.or.kr

○ 온라인(홈페이지) 안내 : www.khcert.or.kr

진료정보 침해사고 통지서

기본정보		
의료기관 명칭		
담당자 성명		
연락처	이메일	
	전화 번호	유선전화: 핸드폰:
사고내용		
침해사고 발생일시		년 월 일 시 분(24시간 표기)
진료정보 유출현황		*예시) 환자 진료내역 등, 50,000건* *※ 유출된 의료정보의 유형, 유출 건수 등*
피해시스템 범위*		*예시) 111.222.333.444, DB서버, 윈도우서버2012, 웹해킹(추정), DB서버(10대) 등* *※ 피해 IP주소, 피해시스템 용도, 운영체제, 공격방법(추정), 피해범위(OO대) 등* * 피해시스템 범위 작성시 첨부된 시스템 분류 목록 및 공격방법 목록을 참고
기타		*※ 상기 내용 외, 기관 자체 조치·확인 사항(공격자 정보, 긴급조치 실시사항, 관련 보안제품 운영현황 등) 등 기술*
요청사항		
기술지원 요청사항		*예시) 피해현황 조사 지원, 원인분석 지원, 복구대책 수립 지원 등*

※ (관련근거) 의료법 제23조의3(진료정보 침해사고의 통지), 동법 시행규칙 제16조의2(진료정보 침해사고의 통지 방법)

<신고연락처: 진료정보침해대응센터(KHCERT)>

- [전화] 02-6360-6500
- [메일] cert@khcert.or.kr

진료정보 침해사고 통지를 위한 개인정보 수집·이용 동의서

「진료정보침해대응센터(KHCERT)」는 진료정보 침해사고 대응을 위하여 아래와 같이 개인정보를 수집·이용하고자 합니다.

▶ 개인정보 수집·이용 동의처리에 관련한 법적근거
- 개인정보 보호법 제15조

▶ 개인정보 수집·이용 동의

수집·이용 항목	수집·이용 목적	보유기간
의료기관명, 통지(신고)자 성명, 연락처(이메일, 전화번호)	진료정보 침해사고 통지 확인 및 침해대응 관련 업무처리	1년
개인정보를 수집·이용하는 데 동의를 거부할 권리가 있습니다. 동의를 거부할 경우, 관련 업무처리가 불가능합니다.		

개인정보를 수집·이용하는데 동의하십니까? [□ 동의함 □ 동의하지 않음]

년 월 일

소속
성명 (서명 또는 인)

진료정보침해대응센터장 귀하

<시스템 분류 목록>

기호	시스템 분류	설 명
가	웹서버	기관의 홈페이지 운영 및 웹서비스를 제공하는 서버
나	전자우편 서버	전자우편 송수신을 위해 운영하는 서버
다	DB/업무서버	홈페이지 및 업무지원을 위한 데이터베이스 서버
라	개발/임시서버	개발 및 운영 테스트를 위하여 사용하는 임시 서버
마	통신전송장비	라우터, 스위치 등 통신전송장비 일체
바	보안장비	방화벽, IDS, VPN 및 백신서버 등 정보보호제품 일체
사	개인/업무PC	기관내 사용자의 PC
아	교육/임시PC	교육장 또는 공용 작업을 위해 여러 명이 사용하는 PC
차	기타	위의 시스템 용도에 없는 경우 서술식으로 기술

<공격 유형 목록>

기호	공격 유형	설 명
A	웹해킹	인젝션, 세션탈취 등 웹페이지를 통한 사이버 공격 유형
B	홈페이지위변조	홈페이지 지연 및 단절, 오류 등 의도하지 않은 이상징후가 발견되거나 위변조가 발생하는 사이버 공격 유형
C	해킹메일	이메일을 통한 악성코드 유포, 피싱 등의 사이버 공격 유형
D	서비스거부	정상적인 서비스 제공을 어렵게 만드는 가용성을 침해하는 사이버 공격 유형
E	네트워크침입	네트워크 통하거나 네트워크 프로토콜을 악용하여 수행하는 사이버 공격 유형
F	정보수집	공격대상의 OS, App 종류/버전, 에러정보 등 단순 정보 수집 단계의 사이버 공격 유형
G	악성코드	시스템 파괴, 정보 유출 등의 악의적인 활동을 수행하는 소프트웨어를 통한 사이버 공격 유형
H	유해IP	해킹시도, 스팸메일 등 사이버 공격에 악용되었다고 알려진 IP를 통한 사이버 공격 유형
I	기타	위의 사이버 공격 유형에 포함되지 않을 경우 서술식으로 기술

※ 진료정보침해대응센터 공격유형 분류기준

[부록-C] 의료기관 랜섬웨어 예방·대응 퀵매뉴얼

의료분야 랜섬웨어 예방·대응 퀵매뉴얼

■ 랜섬웨어(Ransom + Software)

컴퓨터 데이터를 암호화하고 복원 조건으로
돈을 요구하는 악성 프로그램

■ 예방수칙

1. 백신 소프트웨어 설치 및 최신 업데이트
2. 외부에서 내부 서버·PC로 원격접근 금지
3. EMR, PACS, OCS 등 모든 진료정보 매일매일 백업
4. 출처가 불분명한 이메일, URL링크 열람금지
5. Windows 10 등 모든 소프트웨어 최신 업데이트
6. 내부 파일공유(SMB) 금지 및 외부 공유사이트 접근 주의

■ 감염 시 조치방법

초기조치	상태유지	신고
1 네트워크 차단	3 악성프로세스 종료	5 진료정보침해대응센터 신고
2 외장 HDD 분리	4 시스템 전원유지	02-6360-6500
		cert@khcert.or.kr

× [안내] 감염 시 조치 상세사항은 "의료분야 랜섬웨어 예방대응 안내서"를 참고하여 주십시요.

보건복지부 SSIS 한국사회보장정보원