

의료기관 정보보안 강화를 위한 지원 서비스 소개

2023년 05월 23일

의료정보보호센터 이성훈

1. 의료기관 정보보안 환경

의료기관 대상 사이버공격 급증!!!

환자 정보 노리는 랜섬웨어 공격 급증...5년 사이 2배 증가
발행날짜: 2023-01-03 05:30:00

JAMA에 2016년부터 2021년까지 공격 특성 분석 연구 게재
평균 43건에서 91건으로 두배 이상 증가...병원 셋다온까지

[메디칼타임즈=이인복 기자] 환자 정보를 노리는 랜섬웨어 공격이 급증하고 있다.

이로 인해 수천만명의 환자 정보가 유출되고 있는 것으로 확인됐다.

상급종합병원 41곳 로그인 정보 다크웹서 유통
..."관리자 계정도 포함"

입력 2023.05.12 20:07 김혜경 기자(hkmind9000@inews24.com)

잇따르는 대형병원 의료기

北 해커들은 왜 '서울대병원'을 공격했나
검사결과 · 진단명 · 의학사진 등 민감 의료정보도 유출
"의료기관 정보보호 투자 미흡...전면 개선 필요"

입력 : 2022-08-11 18:36

서울대병원 지난해 발생한 사이버 공격 피해 사례 공유, 의료진과 실무자 정보

[아이뉴스24 김혜경 기자] 서울대병원 지난해 발생한 사이버 공격 피해 사례 공유, 의료진과 실무자 정보

해킹조직이 2년 전 발생한 서울대병원 개인정보 유출 사건 배후로 지목되면서 공격...
...탈취 등의 목적이 제기되는 가운데 의료기관의 취약한 정보보호...
...의 90%에 해당하는 곳에서 로그인 정보가 유출돼 다크웹에

해외 디지털헬스 해킹 피해 심각...
우리도 안전하지 않아

2023.03.13 12:04 김홍진 기자 khj2076@hitnews.co.kr
미국 정부, 환자기록 노출 12년간 3억8500건
디지털 서비스 도입, 원격 근무형태로 늘 많아져
IoT, CCTV, 클라우드 전문업체 협업도 고려해야

[보안뉴스 김영명 기자] 서울대학교병원, 서울대병원의 해킹 사례가 잇달아 드러나면서 국내 의료기관의 보안 문제로 한 국내 의료기관의 보안대책에 관심이 모아지고 있다.

병원 노리는 해커들...의료기관 보안 '비상'

서울대병원, 지난해 7월 이어 올해 의심 정황 발생...보안 강화에도 우려 지속
병원 디지털화 따른 보안 빈틈...의료ISAC, 지역협의회 구축 등 노력

기사승인 2022-07-15 06:00:14 박선혜 기자 betough@kukinews.com

2022년 1월 290곳 랜섬웨어에 노출
...데이터 노출 수준 '심각'

mbiz.com

랜섬웨어에 노출된 것으로 나타났다. 정부·교육·의료 등 대규모 조직이 랜섬웨어 공격을 받았다. 보안업계는 교육 발생 건수가 적더라도 막대한 피해로 이어질 수 있는

사이버 보안 투자는 1% 이하

2019-10-22 11면 정용철기자 jungyc@etnews.com

...정보가 저장된 병원이 전 세계 사이버 공격 대상이 되고 있는 가운데, 미국조차도 병원 IT 예산 중 사이버 보안 투자는 5%가 채 안 되는 것으로 나타났다. 국내는 IT 적당부서조차 없는 곳이 수두룩한데다 보안 예산은 물론 시스템 현황조차 파악이 안된다. ... 목적 환자 생명까지 위협하는 의료기기 해킹 위협까지 고조되면서 의료 ... 시급하다.

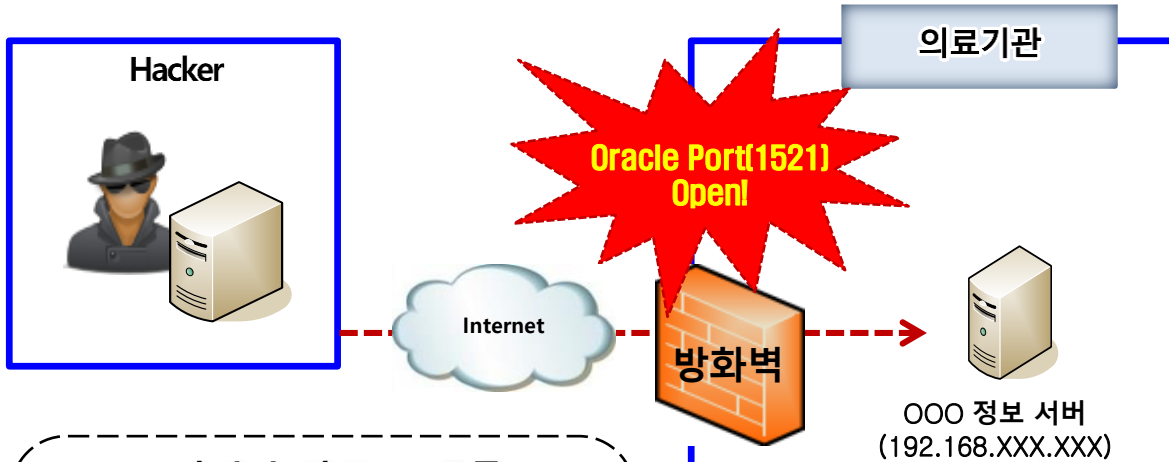
병원들 전산망 사이버공격 급증" 경계령

2023-01-29 16:05 yonglae@yna.co.kr

의료기관 네트워크 상대로 랜섬웨어 공격 급증

(서울=연합뉴스) 김용래 기자 = 신종 코로나바이러스 감염증(코로나19) 사태가 악화하는 미국에서 전국 병원과 의료·보건기관들을 상대로 사이버범죄가 급격히 늘고 있다고 미 연방수사국(FBI)이 경고했다.

의료기관 침해사고 사례



비인가 접근 IP 목록

No.	IP	국가
1	211.138.77.66	China
2	113.105.136.152	China
3	121.15.14.17	China
4	222.235.72.84	Korea Republic Of
5	123.254.183.80	Korea Republic Of
6	220.249.93.30	China
7	222.170.218.103	China
8	120.194.252.136	China
9	222.133.51.131	China
10	218.28.0.151	China
11	218.204.14.93	China
12	50.22.175.28	USA - Florida
13	112.133.61.27	Korea Republic Of
14	183.129.160.229	China
15	60.191.38.78	China
16	60.164.249.187	China
17	221.203.30.40	China

의료기관

Oracle Port(1521)
Open

방화벽

OOO 정보 서버
(192.168.XXX.XXX)

1

14/07/04 09:17
Oracle Listener Port(1521)를 이용,
211.138.77.66로부터 최초 접근

2

16/01/03 08:10 ~ 17/07/25 00:14
악성코드 설치/시도 흔적 확인 및
smss.exe, oracle.exe 악성코드 탐지

3

17/11/07 23:49:54, 17/11/07 23:49:58
8555.exe, up.exe 생성

4

17/11/07 23:50:00(추정;Code로 확인)
cpu6432.exe 생성

5

17/11/07 23:50:22
java.exe 실행(가상화폐 채굴 프로그램)

6

17/11/28 08:08 ~ 17/11/28 17:25
Oracle.exe 및 java.exe 백신 탐지

C&C 목록

중요 악성코드

N	악성코드	C&C
1	smss.exe	ddos.sdo180.com (222.73.85.102)
2	Oracle.exe	zll855.no-ip.info / rat.pzchao.com (107.161.80.213)

주요 악성코드 행위

No.	악성코드	행위
1	8555.exe	oracle.exe 생성 후 실행
2	up.exe	win32shell.bat 생성 및 cpu6432.exe 다운로드 후 실행
3	cpu6432.exe	가상화폐 채굴 프로그램 압축해제 후 실행

분석 결과 및 권고 사항

분석 결과

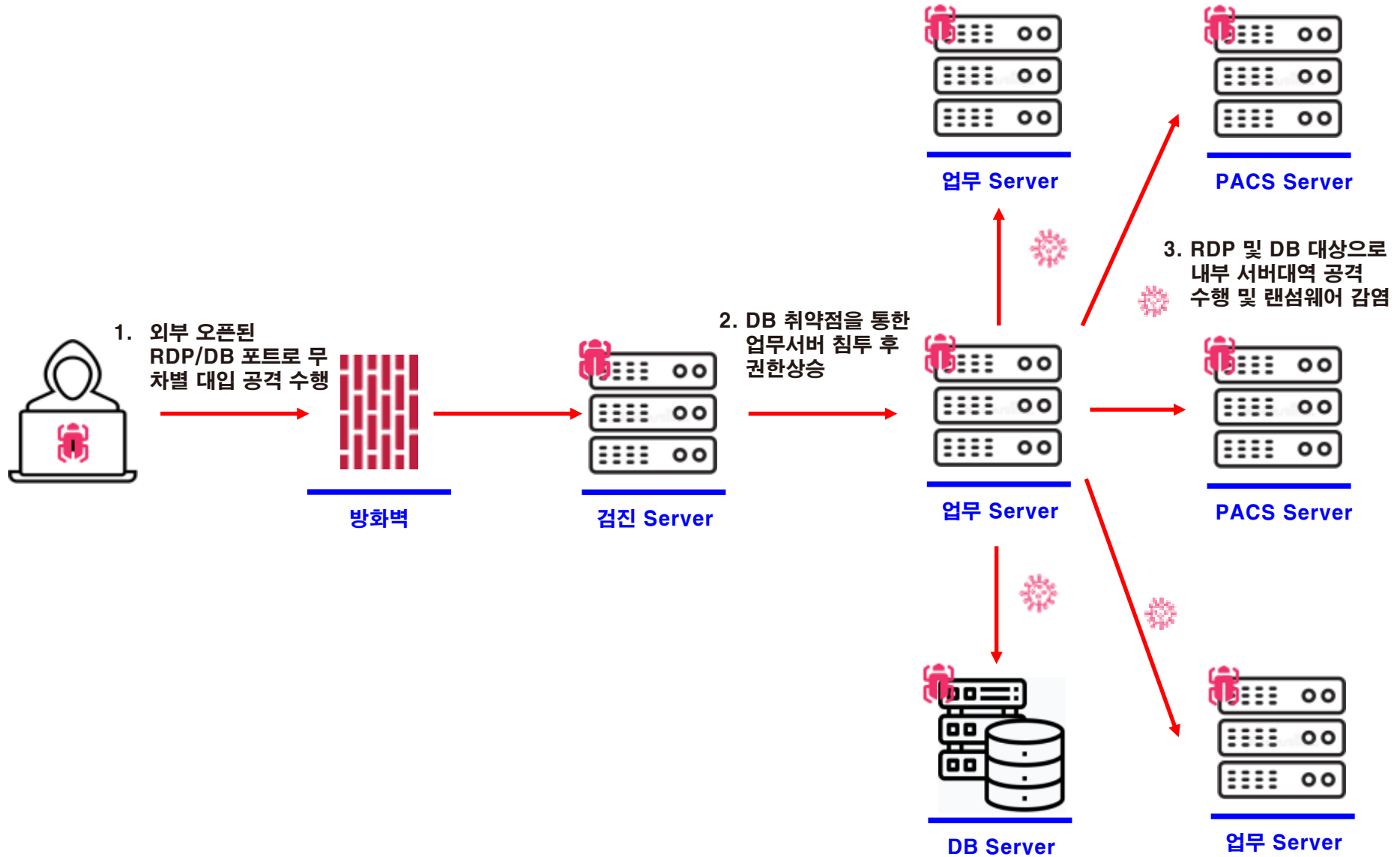
Oracle Listener Port(1521)의 외부 접근이 가능하도록
방화벽에서 OPEN 되어 있어 2014년부터 비인가 접근이 진행
된 것으로 판단됩니다.

공격자는 오라클 계정 정보의 획득(무차별 대입 또는
취약점 이용) 후 악성코드 다운로드와 실행을 수행하였습니다.

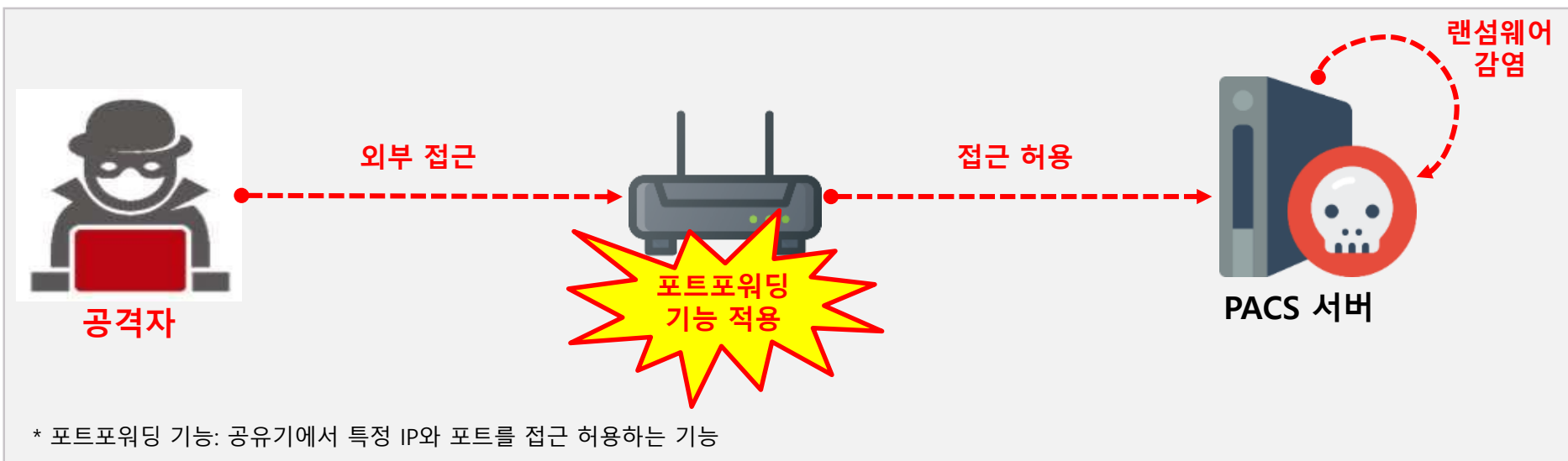
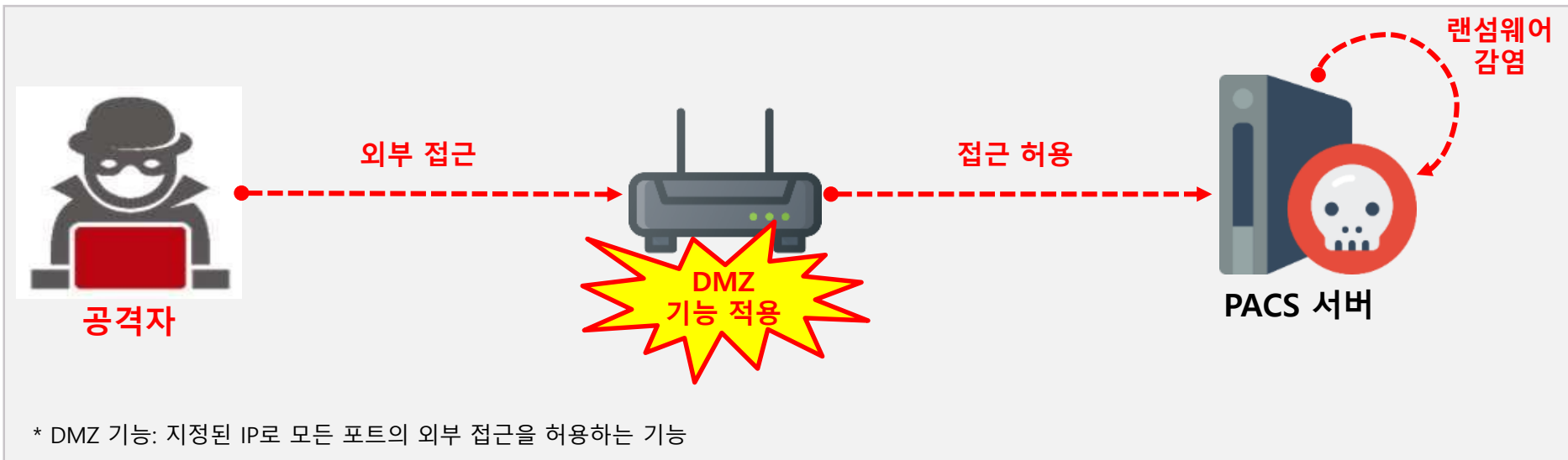
권고 사항

- 방화벽 접근 통제
- Oracle Port 변경
- Oracle Patch / Update
- 백신 로그 주기적 확인
- 악성코드 발견 시 정보보안 부서로 전달
- 서버 포맷 및 재설치
- 서버 정보(계정, IP) 등 변경

의료기관 침해사고 사례



의료기관 침해사고 사례



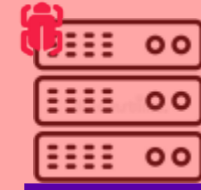
의료기관 침해사고 사례

1차 공격



1. 외부 노출된 포트 및 취약점을 통하여 내부 업무 서버 점거

2. 영상 데이터 약 41만건(163GB) 암호화



PACS Server



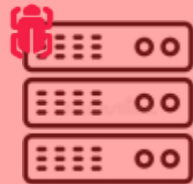
3. 1차 사고 이후 센터에서 권고한 재발방지 대책 미이행

2차 공격



4. 외부 노출된 포트 및 취약점을 통하여 내부 업무 서버 점거

1차 공격지

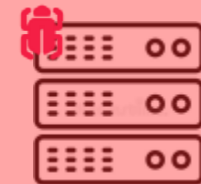


업무 Server

5. RDP 서비스가 활성화된 시스템을 탐색하고 무차별 공격 수행 및 측면이동

6. 영상데이터 약 15만건(2,334GB) 암호화

2차 공격지



PACS Server

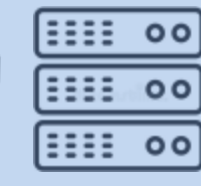


7. 2차 사고 이후 센터에서 권고한 재발 방지 대책 즉각 이행

사고 발생 없음



8. 재발방지 대책 이행 이후 현재까지 사고발생 이력 없음



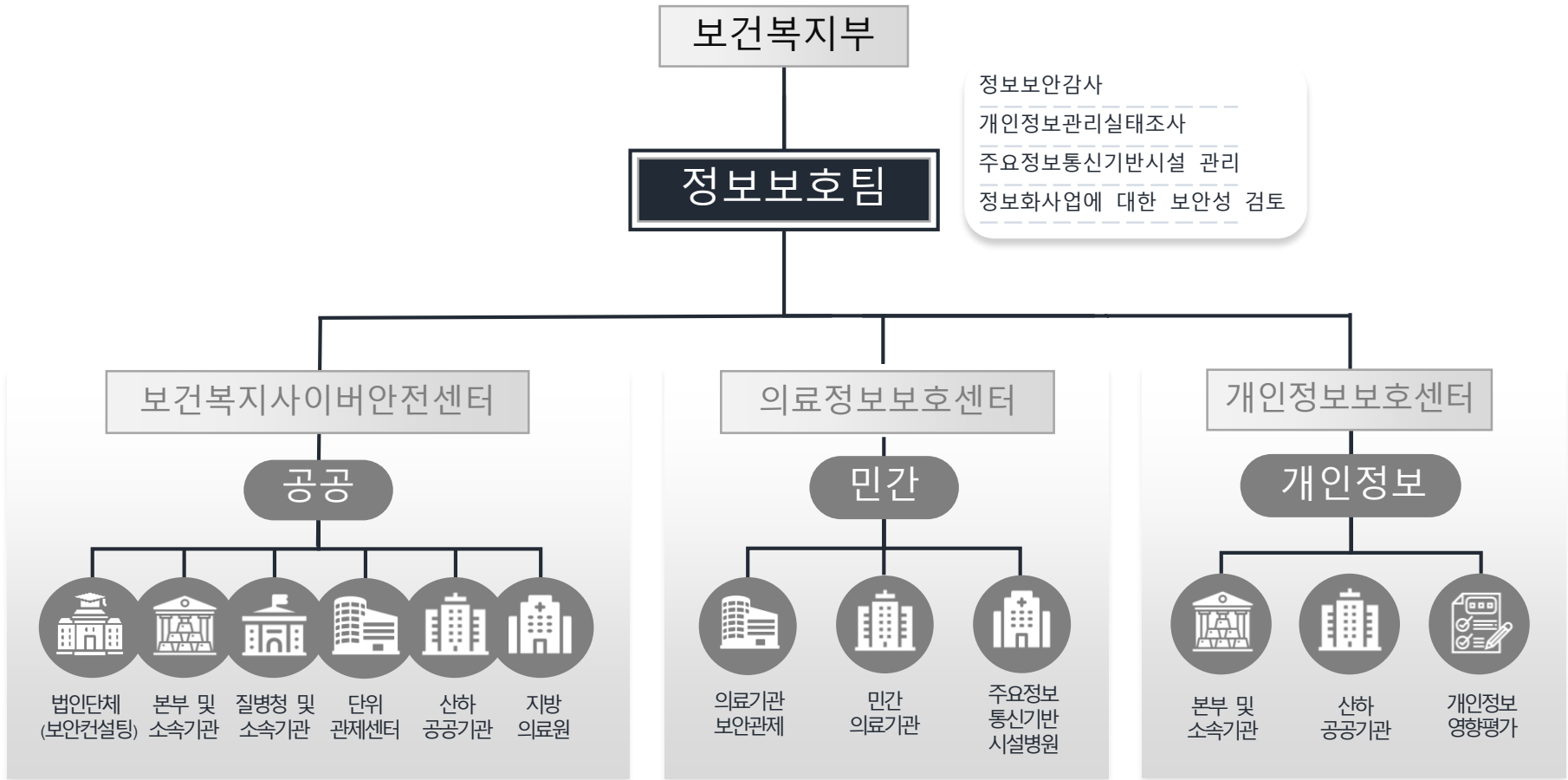
PACS Server

의료기관 업무의 특성

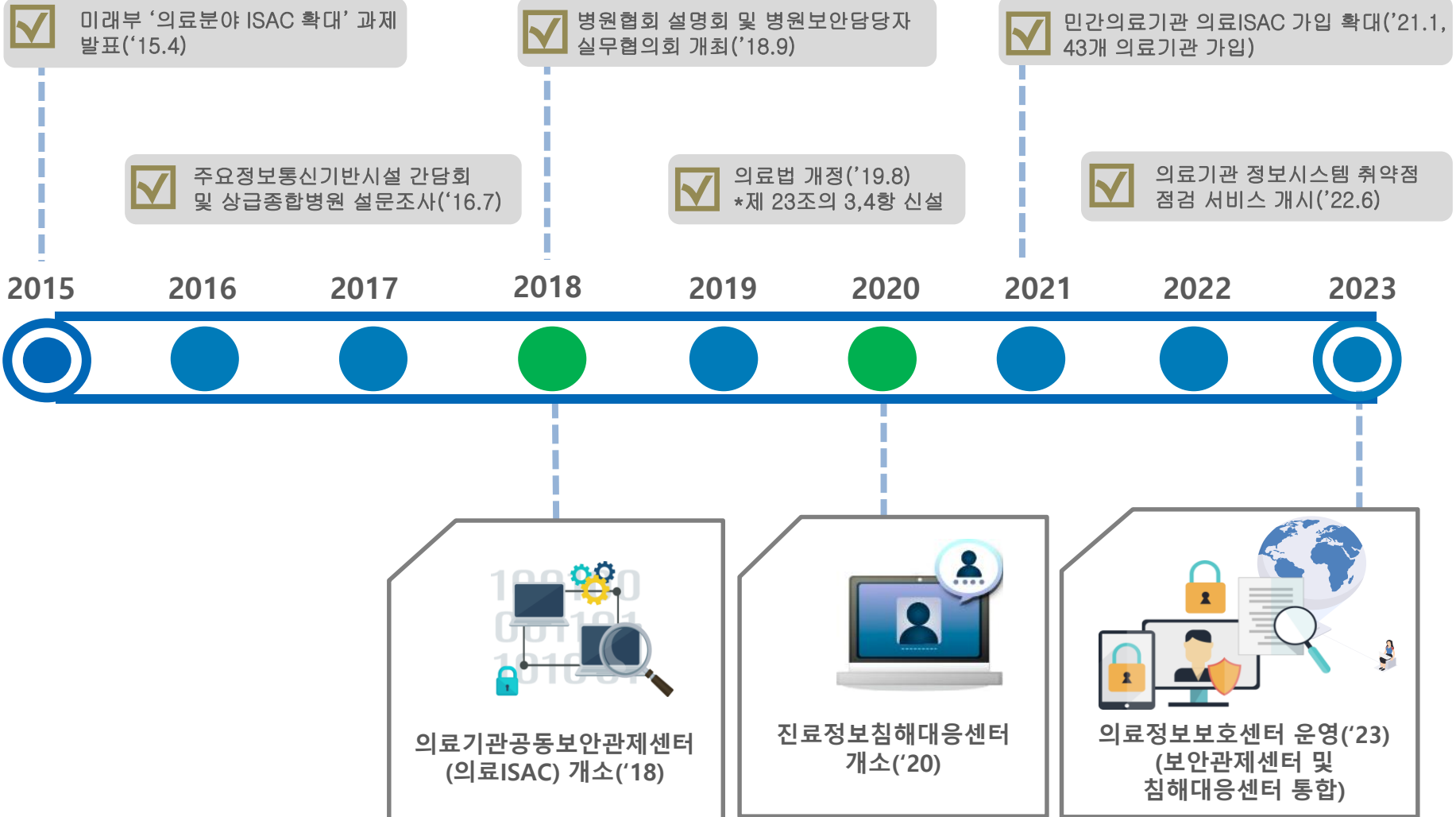
	주요 내용	고려 사항
생명 우선	환자생명 vs 정보보안	• 보안으로 진료 지연 時 생명 위험
다양한 업무	진료 + 교육 + 연구	• 진료 外 교육과 연구 보안 필요
무정지	365일, 24시간 근무	• 24시간 운영체계 확립 필요
개인정보	췁직원 개인정보 취급	• 개인정보 취급자 별도관리 불가
공용 PC	업무 목적 공동 사용	• 공용 PC에 대한 보안 관리 필요
Server, PC	서버, PC, 시스템 수량 ?	• 과제비, 연구비로 자체 구축
의료기기	의료기기는 전산시스템 ?	• 보안패치 한계, 대용량 데이터

II . 지원 서비스 소개

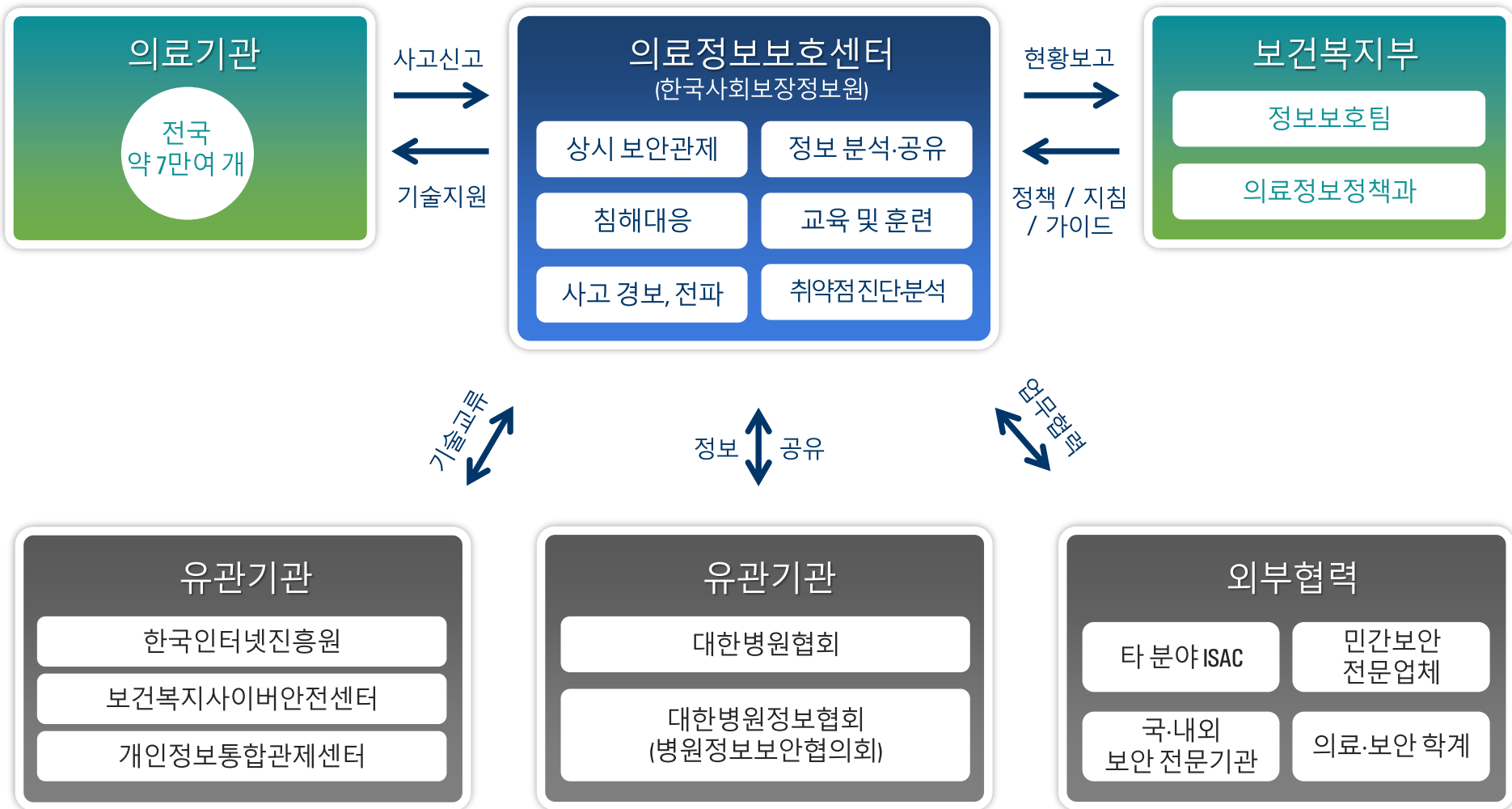
의료기관 정보보안 거버넌스



의료기관 정보보안 지원 조직

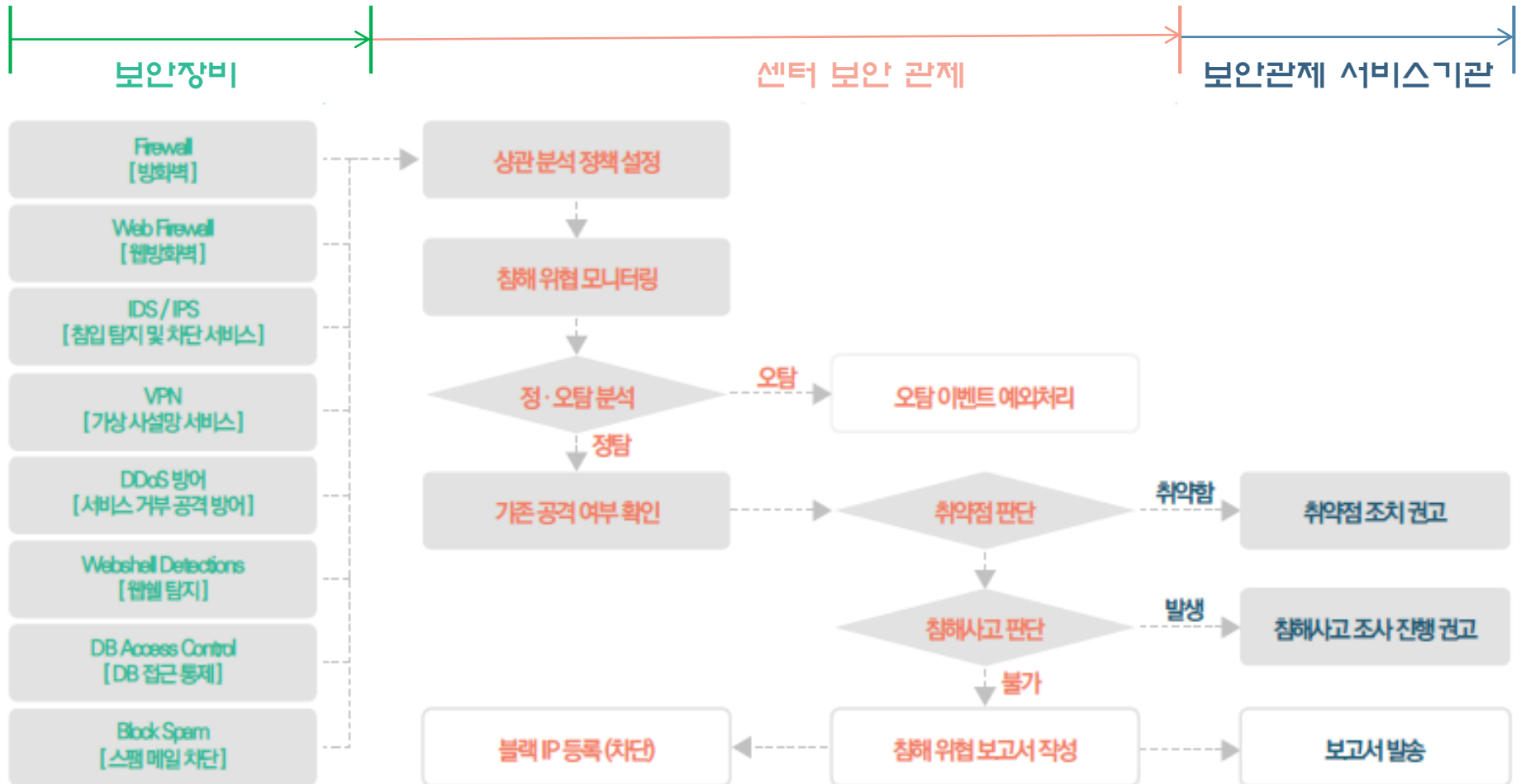


의료정보보호센터 운영체계



지원 서비스 - 보안관제

24시간 365일 실시간 모니터링을 통한 침해행위 사전 탐지 및 침해사고 신고 접수



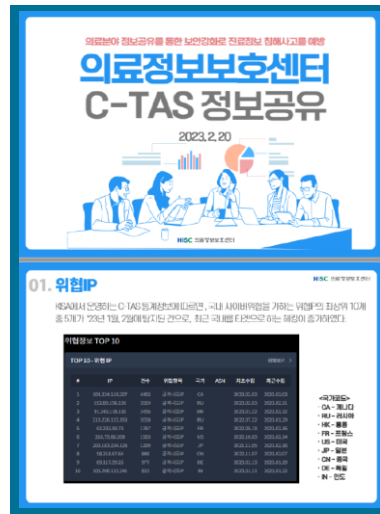
지원 서비스 - 정보공유



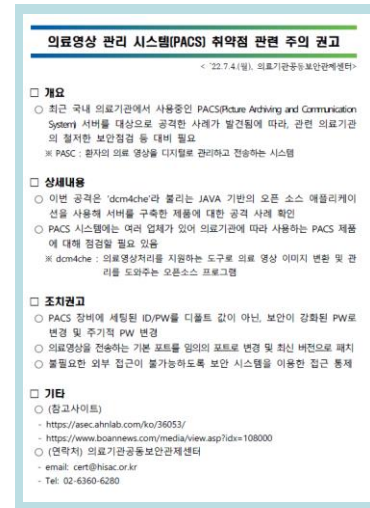
보안관제 심층분석보고서



보안관제 결과보고서



유관기관 공유 정보

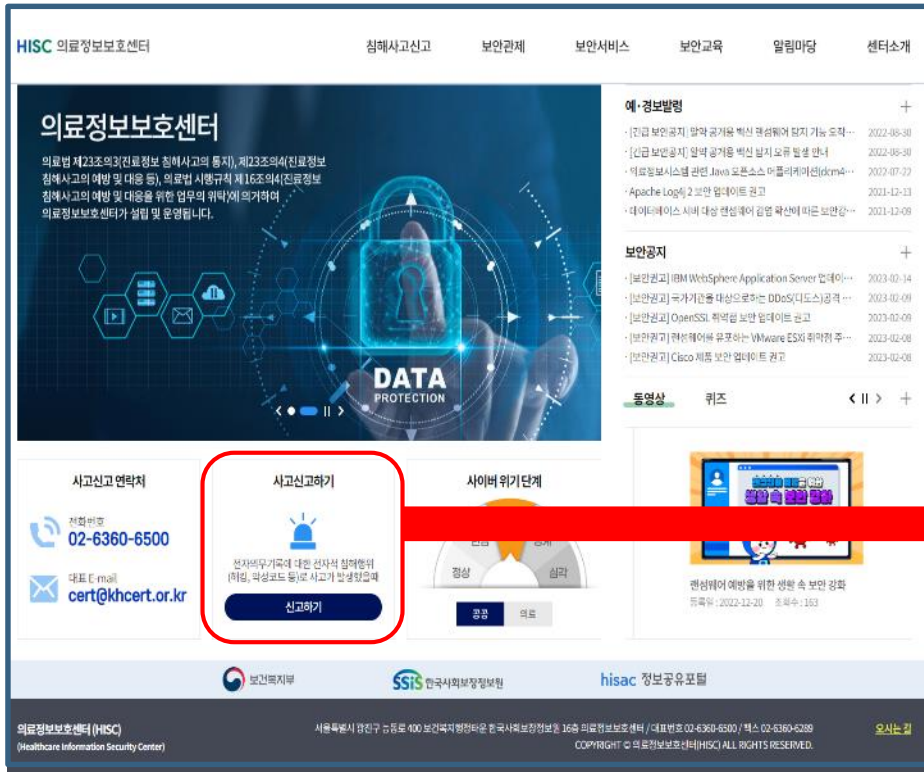


보안이슈 및 보안권고

구분	내용	구분	내용
언론보도	의료 및 보안 분야 관련 뉴스 기사 등	센터 보안관제 실적	기관별 맞춤 보고서
보안 권고	전일 보안관제에서 탐지된 위협정보	보안전문업체 동향지	전문보안업체 동향지 공유
	KISA, 국가정보원 등 보안 권고 사항	국내·외 보안 이슈	랜섬웨어 확산 등 이슈 공유
보안동향 및 기술정보	분기별 정보보호 심층분석 보고서 공유(센터)	침해사고 사례 및 대응 절차	실제 침해사고 사례를 유형별로 분류 공유
사이버 위기 예·경보	침해사고 사이버 위기 예·경보		

지원 서비스 - 침해사고 대응

의료정보보호센터 홈페이지(www.hisc.or.kr)



의료분야 사이버 보안, 당신의 소중한 신고로부터 시작됩니다.



의료기관이 랜섬웨어 또는 해킹 피해를 보았다면?

▶ 의료법 제23조의3(의료정보 침해사고의 통지)에 근거하여 의무적으로 의료정보보호센터로 신고해야 합니다.

의료법 제23조의3(의료정보 침해사고의 통지)

① 의료인 또는 의료기관 개설자는 전자와무기록에 대한 전자적 침해행위로 진료정보가 유출되거나 의료기관의 업무가 교란·마비되는 등 대통령령으로 정하는 사고(이하 "의료정보 침해사고"라 한다)가 발생한 때에는 보건복지부장관에게 즉시 그 사실을 통지하여야 한다.

의료법 시행규칙 제18조의4(의료정보 침해사고의 통지 방법)

① 의료인 또는 의료기관 개설자는 법 제23조의3제4항에 따른 의료정보 침해사고(이하 "의료정보 침해사고"라 한다)가 발생한 경우 다음 각 호의 사항을 서면, 전화, 팩스, 전자우편 또는 이와 유사한 방법으로 보건복지부장관에게 통지해야 한다.

1. 의료기관의 명칭
2. 의료정보 침해사고의 발생일시
3. 진료정보의 유출 범위 등 피해내역
4. 의료정보 침해사고의 대응을 위한 기술지원 요청사항

※ 신고하지 않을 경우 의료법 위반으로 3백만원 이하의 과태료 부과

침해사고 신고를 해야 하는 이유

신속한 원인 파악	위험 요소 제거	추가 피해 확산 방지
취약점 진단	취약점 조치	재발 및 복구비용 방지

침해사고 신고 후 받을 수 있는 지원

(사고조사) 침해사고 원인분석

- 사고유형 및 침투경로 등 파악
- 침해사고 재발방지대책 마련
- 시스템 및 보안장비 점검 지원

(사고예방) 보안서비스 지원

- 취약점 진단 서비스 제공
- 홈페이지 악성코드 탐지서비스 제공
- 해킹메일 오의혹권 지원
- 정보보안 교육 지원

침해사고 신고 방법


	의료정보보호센터(www.hisc.or.kr) 침해사고신고 메뉴
	전화 문의 02-6360-6500
	이메일 문의 cert@hisc.or.kr

지원 서비스 - 취약점 점검

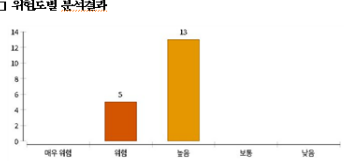
의료정보보호센터 Healthcare Information Security Center

1차 웹 취약점 점검결과 및 수정가이드

2023. 1. 2.

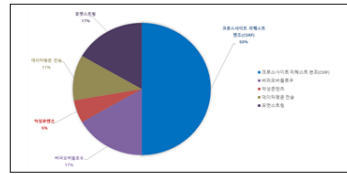


□ 위험도별 분석결과



위험도	매우위험	위험	높음	보통	낮음	총계
개수	0	5	13	0	0	18

□ 점검항목별 분석결과



항목	검출 취약점
LDAP 연계성	0
SQL 연계성	0

영역별 취약점 결과

영역	소계	24	10	10	4	417
웹	1. 설정	15	6	7	2	487
	2. 솔루션 취약점	5	1	2	2	400
	3. 접근 제어	3	3	0	0	0
	4. 패치 관리	1	0	1	0	100
네트워크	소계	570	248	318	4	558
	1. 계정 관리	62	15	47	0	759
	2. 기능 관리	322	162	160	0	497
	3. 로그 관리	82	35	45	2	549
	4. 접근 관리	86	35	49	2	570
5. 패치 관리	18	1	17	0	950	
보안 장비	소계	427	333	69	25	162
	1. 계정 관리	90	75	17	0	189
	2. 기능 관리	139	97	17	25	123
	3. 로그 관리	126	104	22	0	175
	4. 접근 관리	54	45	9	0	167
5. 패치 관리	18	14	4	0	223	

점검영역	취약성명	세부내용
계정 관리	계정 및 패스워드 보안 정책 설정 미흡	· 기본관리자 계정 사용 중요취약 취약
		· 패스워드 이식 및 취약한 패스워드 사용 중요취약 취약
서비스 관리	불필요한 서비스 허용	· 사용하지 않는 서비스 활성화 중요취약
		· 공유 폴더 사용 중요취약 취약
모양 관리	서버 보안 설정 미흡	· OS 업데이트 기능 비활성화 중요취약
		· 화면보호기 미설정 중요취약
로그 관리	로그 저장 및 관리 미흡	· 로그의 접근 권한 설정 미흡 중요취약
		· 이종식 미디어(USB 등) 보안대책 미수립 중요취약 취약
패치 관리	OS·응용 프로그램 보안 패치 및 업데이트 관리 미흡	· 시스템 관리 설정 미흡 중요취약 취약
		· 노후화 시스템 사용 중요취약 취약
접근 관리	시스템 접근 관리 및 설정 미흡	· 사용자 정렬이별 권한 수권 설정 미흡 중요취약
		· VTY 접근(ACT) 미설정 취약
패널 및 디렉토리 관리	파일 및 디렉토리 권한 설정 미흡	· 권한 IP 및 포트 제한 미설정 중요취약
		· 웹서버 IP 및 포트 제한 미설정 취약

취약점 점검결과 보고서

보고서 상세내용

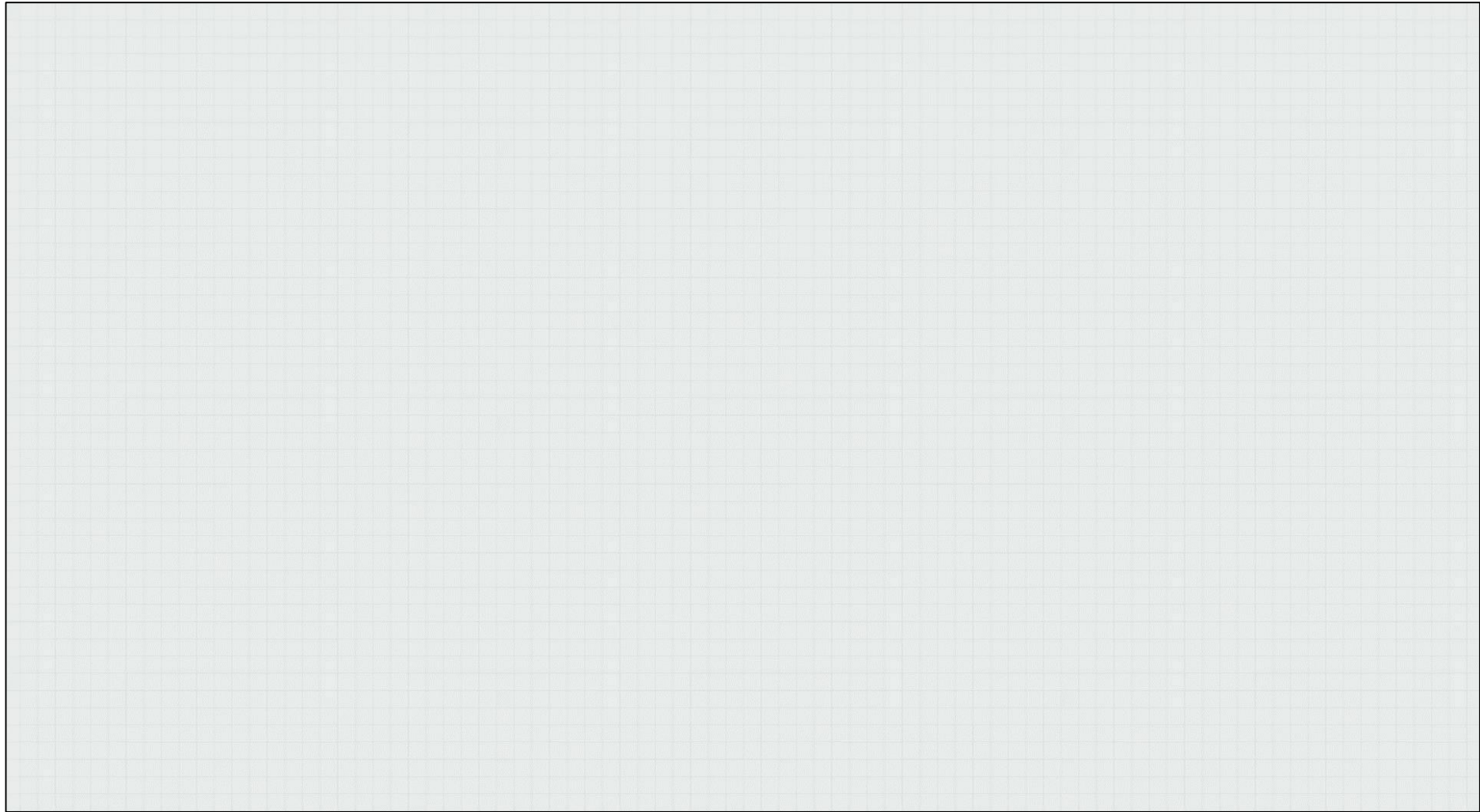
영역별 취약점 결과

주요 취약 항목 정리

<취약점 점검 신청 절차>



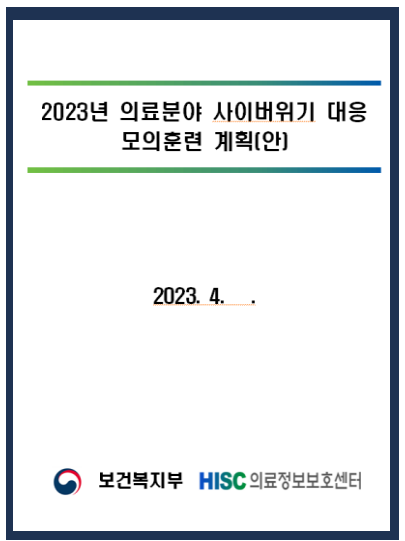
지원 서비스 - 모의해킹 진단



지원 서비스 - 교육 / 훈련



2022년 교육 및 간담회



사이버위기 대응 훈련



위기대응 절차



해킹 메일 모의훈련

구분	주요 내용
집합교육	교육수요에 바탕 한 참가기관 정보보안담당자 등 교육
출장교육	참가기관이 요구하는 교육내용 등에 대해 의료정보보호센터에서 직접 참가기관을 방문하여 교육
워크샵	정보보호 이슈사항 토의 및 참가기관 및 유관기관과의 공조체계 강화
사이버위기 대응 모의훈련	사이버위기 발생 시 대응역량 강화를 위한 모의침투, 해킹메일 발송 등 위기대응 모의훈련 실시
해킹 메일 모의훈련	해킹 메일 훈련을 실시하여 임직원들의 보안의식 제고

지원 서비스 - 의료정보보호센터

HISC 의료정보보호센터
침해사고신고
보안관제
보안서비스
보안교육
알림마당
센터소개

신고안내 사고신고 처리절차	보안관제 대상 및 절차 권리 및 의무 정보공유	악성코드탐지서비스 정보시스템 취약점 점검서비스 웹 취약점 점검 서비스 해킹메일 훈련서비스 정보보안 영상 제공 서비스	동영상 퀴즈	예·경보발령 자료실 보안공지 보안뉴스	개소 및 이력 주요업무 공지사항 FAQ 오시는 길
----------------------	------------------------------------	---	-----------	-------------------------------	---



- [보안권고] WordPress 제품 보안 업데이트 권고 2023-05-17
- [보안권고] 의료기관 계정정보 다크웹 유통 정황에 따른 보... 2023-05-16
- [보안권고] 나모 웹에디터 제품군 보안패치 적용 및 웹페이... 2023-05-16
- [보안권고] 리눅스 권한 상승 취약점 보안 업데이트 권고 2023-05-12
- [보안권고] Hikvision 제품 보안 업데이트 권고 2023-05-04

동영상
퀴즈
< || > +



의료기관 랜섬웨어, 백업으로 대비해요!
등록일 : 2022-12-20 조회수 : 1666

사고신고 연락처

전화번호
02-6360-6500

대표 E-mail
cert@khcert.or.kr

사고신고하기



전자의무기록에 대한 전자적 침해행위
(해킹, 악성코드 등)로 사고가 발생했을때

신고하기

사이버 위기단계



공공
의료

의료정보보호센터 (HISC)
(Healthcare Information Security Center)

서울특별시 광진구 능동로 400 보건복지행정타운 한국사회보장정보원 16층 의료정보보호센터 / 대표번호 02-6360-6500 / 팩스 02-6360-6289

COPYRIGHT © 의료정보보호센터(HISC) ALL RIGHTS RESERVED.

오시는 길

III. 향후 계획

사이버안전 체계 확대

공공분야 대응체계

- ✓ 정부가 주체가 되는 대응 체계
- ✓ 분야별 중앙행정기관 소속·산하 공공기관
- ✓ 의무 가입 및 정부 부담 비용으로 운영

보건복지 공공 분야

관련법 (훈령)국가사이버안전관리규정

운영기관 분야별 부문보안관제센터

가입기관 소속 공공 의료기관, 지방의료원

민간의료 대응체계

- ✓ 정부가 아닌 민간 자율 대응 체계
- ✓ 분야별 정보통신기반시설 주도
- ✓ 희망 가입 및 회원비로 운영

민간의료 분야

관련법 (법)정보통신기반보호법

운영기관 정보공유·분석센터

가입기관 상급 종합병원, 종합병원 등

공공과 민간의 상호조화를 통한 사이버보안 대응 체계 발전 노력

의료기관 정보보안 강화 지원 전략

Strategy 1

의료기관 지원 법·제도 기반 마련

- 정보보안 지원을 위한 의료법 개정
- 전자의무기록 안전성 확보를 위한 고시 제정

Strategy 2

의료기관 참여 확대를 위한 지원 강화

- 초기 보안관제 장비 투자를 위한 예산 지원
- 정보보안 관리 수준 향상 기관 회원비 감면 등 인센티브 제공

Strategy 3

의료기관 자체 역량 강화

- 의료기관 자체 정보보안 기준 마련
- 전담조직 및 전문인력 양성

Strategy 4

전문성을 강화한 조직체계 정비

- 취약점 점검 및 관리 수준 진단
- 전담인력 증원
- 보안관제 자체 운영



감사합니다.