의료기관공동보안관제센터 (의료ISAC) 소개

2020년 1월

보건복지부

사회보장정보원

목 차

1. 센터 일반 1

- 센터 개요 1
- 설립취지 및 법적근거
- 추진경과

2. 제공 서비스 2

- 서비스 종류
- 보안관제
- 정보공유
- 침해대응
- 교육 및 훈련
- 보안관제 맞춤형보고서

3. 회원 가입 및 비용 7

- 가입 대상
- 가입 절차 및 방법
- 연회비
- 병원 부담 비용

4. 기대 효과 9

[첨부] 병상수별 연회비 기준 10

1 센터 일반

◈ ISAC(Information Sharing & Analysis Center)
동종 또는 유사 업무 분야별로 **해킹이나 악성코드 등 사이버위협**에 효과적으로 대응하기 위한 **공동 대응체계**
※ 국내 업무 분야별 4개 ISAC 운영 중(의료/금융/통신/지자체)

❑ 센터 개요

○ **(명칭)** 의료기관공동보안관제센터(의료ISAC)

○ **(운영기관)** 사회보장정보원

○ **(운영예산)** 국고 및 가입기관 연회비

❑ 설립취지 및 법적근거

○ **(취지)** 의료분야 정보통신시설을 보호하고자 「정보통신기반 보호법」 제16조에 의거 의료기관공동보안관제센터(의료ISAC)를 설립·운영

○ **(근거)** 「정보통신기반 보호법」 제16조(정보공유 · 분석센터)

❑ 추진경과

○ ('15.04월) 미래부 「K-ICT 시큐리티 발전전략」에 '의료분야 ISAC 확대' 과제 포함

○ ('16.10월) 보건복지부 「보건산업 종합발전전략」에 '보건의료분야 사이버 안전체계 확대·강화' 과제 추가

○ ('18.05~09월) 병원장, 병원보안 실무자 대상 설명회 3회 실시

○ ('18.11월) 의료기관공동보안관제센터(의료ISAC) 개소

○ ('19.02월~) 민간의료기관, 진료정보교류 문서저장소 24x365 보안관제

'19.8월 의료법 개정으로 동법 제23조3에 의거 모든 의료기관은 진료정보 침해사고를 보건복지부로의 통지하여야 함

2 제공 서비스

❑ 서비스 종류

○ 기본서비스와 선택서비스로 구분하여 제공

- (기본서비스) 보안관제, 정보공유, 침해대응, 교육·훈련 … 연회비
- (선택서비스) 보안관제 맞춤형보고서 … 별도비용

※ 기본서비스 중 정보공유는 별도 신청기관에 대해 무상 제공

❑ 보안관제

○ 상시 보안관제

- 회원기관의 정보시스템에 대한 24시간 365일 사이버침해 대응 보안관제 서비스 제공

서비스 구성	주요 내용
보안로그 분석	▪ 보안장비(방화벽, IDS/IPS, 웹방화벽 등)로부터 실시간으로 보안위협 로그를 취합, 분석 및 대응
네트워크 트레픽 분석	▪ 네트워크 트래픽에 대해 실시간으로 위협 요소 및 이상 행위를 탐지하고 분석 및 대응
웹페이지 모니터링 (위변조/웹쉘/ 악성코드)	▪ 웹페이지에 대한 위변조 탐지, 웹쉘 삽입, 악성코드 유포 및 경유지 악용 여부를 실시간으로 모니터링하고 대응

○ 침해행위 탐지・분석

- 보안관제로 탐지된 이벤트 중 침해행위로 의심되는 건에 대해 분석을 통해 점검(또는 조치) 요청 또는 권고

○ 사이버 위협 분석

- 내・외부로부터 신규 취약점 또는 위협 정보를 수집하고 보안관제로 탐지된 이벤트와의 연관분석 수행

❑ 정보공유

○ 회원간 정보공유

- 회원간 침해사고 피해사례, 최신 보안위협 정보를 공유하여 공동 대응

○ 사이버위협 정보공유

- 보안관제 탐지현황, C-TAS, 정보보호 전문업체 정보를 활용한 보건・의료 분야 위협정보 분석 및 공유

  ※ C-TAS : 한국인터넷진흥원(KISA)에서 운영하는 사이버 위협정보 분석·공유 시스템(Cyber Threat Analysis & Sharing system)

○ 최신 보안동향 정보공유

- 보건・의료 분야와 관련된 정보보호 이슈(기사, 동향, 현황 등)

❑ 침해대응

○ 침해사고 경보

- 대내・외 위협 상황 발생 시 위기 단계별 경보 발령 및 대처 요령 전파(※ 위기단계 : 관심→주의→경계→심각)

○ 침해사고 긴급조치 지원

- 의료기관 정보시스템 대상 사이버 침해사고 발생 시 신고접수
- 초기대응 지원 및 필요 시 현장조사로 사고 원인 분석・조치 지원

○ 침해사고 복구 지원

- 의료기관의 데이터 및 시스템 복구를 위한 계획 수립 지원
- 침해사고의 확산 또는 재발방지를 위한 대책수립 지원

❑ 교육 및 훈련

○ 정보보호책임자(CISO) 정보보안 교육

- 정보보호책임자가 알아야 할 의료분야 포함 다양한 산업분야 최신 정보보호

동향 및 신규 위협 정보 교육

○ **정보보호담당자 전문 교육**

- 의료기관 정보보호담당자 대상 침해사고 대응능력 향상을 위한 정보보호 전문기술 교육

○ **사이버위기 대응 모의훈련**

- 사이버위기 발생 시 대응역량 강화를 위한 모의침투 등 위기대응 모의훈련 실시

❑ 보안관제 맞춤형보고서

○ 보안위협 심층분석 및 조치가이드

- 신청기관에서 매월 발생·탐지된 보안위협을 심층분석하고, 유효한 보안위협에 대해 기관이 실질적으로 조치할 수 있도록 대응가이드 제공

○ 사전예방 가이드

- 신청기관에 실제 공격이 발생하지 않았지만 국내·외 보안위협 동향 및 의료 센터 전체에서 탐지된 보안위협에 대해 신청기관의 영향도 분석 및 사전예방을 위한 대응가이드 제공

3 회원 가입 및 비용

❑ 가입 대상

○ 「의료법」에 명시된 의료기관 또는 의료기관 단체

❑ 가입 절차 및 방법

절차	주요내용	소요기간
모집공고 (센터)	▪ 의료ISAC 홈페이지 모집 공고	수시
참가신청 (신청기관)	▪ 신청공문 발송	
가입승인 (센터)	▪ 가입승인 통보(공문발송)	-
현장조사 및 시스템 구축 일정 논의 (센터, 신청기관)	▪ 네트워크, 보안장비 등 보안관제 서비스를 위한 환경조사 ▪ 보안관제를 위한 시스템 구축 일정 및 네트워크 구성 협의	2~5일
장비구축 및 연계·연동 (신청기관)	▪ 가입기관에 보안관제용 장비 구축 ▪ 가입기관과 의료ISAC 센터 간 보안관제 장비 연계·연동	2~3개월
서비스 실시	▪ 보안관제 서비스 실시	

❑ 연회비

❍ 연회비는 기본운영비와 분담운영비의 합으로 부과

- (기본운영비) 병원규모와 무관하게 공통으로 소요되는 운영경비(교육, 행사, 자료비 등)
- (분담운영비) 병상수를 규모별로 상, 중, 하로 차등 부과되는 운영경비(인건비, 구축비 등)

❍ 2년차부터 연회비 부과(가입 1년차 면제)

※ 병원별 연회비 예상액은 [첨부] “병상수별 연회비 기준” 참조

❑ 병원 부담 비용

○ 의료ISAC의 보안관제 서비스를 위해 관제대상 기관은 보안관제용 하드웨어 및 소프트웨어 설치 필요

○ 보안관제 연계를 위해 내부에 구축되어 장비 구축 비용은 **자체 부담(최소 1천만원 이상 소요)**

※ 병원 네트워크, 정보시스템 구성, 보안관제 신청 범위에 따라 구매 내역 상이

<table>
<tr><th rowspan="2">관제 방식</th><th colspan="3">관제 연동</th><th rowspan="2">관제 수준</th><th rowspan="2">설명</th></tr>
<tr><th>대상</th><th>방식</th><th>선택/필수</th></tr>
<tr><td>네트워크 분석</td><td>위협관리 센서 (TMS센서)</td><td>센터와 장비연계</td><td>선택</td><td rowspan="7">상</td><td>의료ISAC 관제분석을 통해 제작 된 탐지 정책을 활용한 고도화된 관제</td></tr>
<tr><td rowspan="6">로그 분석</td><td rowspan="2">웹서버</td><td>웹쉘탐지 Agent</td><td>선택</td><td>WEB/WAS에 업로드 된 웹쉘 관제</td></tr>
<tr><td>ESM Agent</td><td>선택</td><td>WEB/WAS 엑세스 로그 수집 관제</td></tr>
<tr><td>IDS/IPS/UTM</td><td>ESM Agent</td><td>선택</td><td rowspan="3">중</td><td rowspan="3">웹취약점(SQL인젝션, XSS 등) 공격 및 자동화 툴을 이용한 공격 등을 관제</td></tr>
<tr><td>웹방화벽</td><td>ESM Agent</td><td>선택</td></tr>
<tr><td>방화벽</td><td>ESM Agent</td><td>필수</td></tr>
<tr><td>전송 암호화</td><td>VPN</td><td>구간암호화</td><td>필수</td><td>하</td><td>비인가접근 탐지 및 악의적인 IP 접근 탐지 등 방화벽 로그 분석을 통한 관제
의료ISAC과 의료기관 간 암호화 통신</td></tr>
</table>

※ Agent는 연동할 대상 장비 당 1개 필요(예, 5개 대상 연동 시 Agent 5개 필요)

4 기대 효과

❑ 공동 보안관제를 통한 비용절감

○ 병원별 24시간 365일 보안관제 시 연간 약 2.3억원 비용 소요 (보안관제 교대근무 4명 기준)

○ 정보보호 관리체계 개선으로 병원당 연간 약 1.64억원 보안사고 피해비용 절감

※ (출처) ISMS인증의 경제적 효과 분석 (KISA, '10.2월)

❑ 법적 의무사항 준수

○ 의료법 정보보호 관련 조항 준수

- 보안에 관한 시설 장비 보안조치, 진료기록전송지원시스템의 보안체계 마련 이행

○ 개인정보보호법 및 개인정보의 안전성 확보조치 기준에 포함된 내부관리 계획 수립 시 활용

○ ISMS 인증기준 준수(일부항목)

- 사고 예방 및 대응, 시스템 및 서비스 보안관리, 인식제고 및 교육훈련

❑ 침해사고 피해 최소화

○ 최신 해킹정보, 위협정보의 신속한 회원기관 간 공유를 통해 사이버 침해사고 사전 예방

○ 사이버침해로 피해가 발생할 경우, 즉각적인 사고전파 및 조기 대응으로 동일사고 피해 확산 방지

○ 의료기관 보안위협에 대한 전문적·효율적 대응체계 구축으로 의료기관에 특화된 보안관제 서비스 제공 가능

[첨부] 병상수별 연회비 기준

가. 상급종합병원

(단위: 만원)

병상수		기본운영비	분담운영비	연회비(총계)
상	1,500 이상	300	1,500	1,800
중	800 이상부터 1,500 미만	300	1,200	1,500
하	800 미만	300	900	1,200

나. 종합병원

(단위: 만원)

병상수		기본운영비	분담운영비	연회비(총계)
상	500 이상	300	600	900
중	200 이상부터~ 500 미만	300	400	700
하	200 미만	300	200	500

다. 의료원의 인터넷망이 통합된 경우

- 기본운영비는 개별병원별로 부과하고, 분담운영비는 의료원이 속한 개별 병원의 병상수의 합으로 부과
- 상급종합병원과 종합병원으로 구성된 의료원의 경우 상급종합병원의 부과기준 적용

※ “의료기관 단체”의 연회비는 별도 부과기준을 적용