MPIS 2018

MEDICAL CENTER PRIVACY INFORMATION SECURITY CONFERENCE 2018

2018 의료기관 개인정보보호&정보보호 컨퍼런스

의료기관 정보보호 인증 준비

박 나 룡

브로콜리 CISO/CPO

보안전략연구소 소장

CONTENTS

CHAPTER 1

정보보호관리체계 (ISMS)

1. 정보보호관리체계
2. 필요성
3. 인증 제도
4. 인증 대상
5. 인증 범위

CHAPTER 2

정보보호 관리적 기준

1. 정보보호 관리 과정
2. 정보보호정책 수립 및 범위설정
3. 경영진 책임 및 조직의 구성
4. 위험관리
5. 정보보호대책 구현
6. 사후 관리

CHAPTER 3

정보보호대책

1. 정보보호 대책
2. 세부점검 항목 – 인적보안
3. 세부점검 항목 – 접근통제
4. 세부점검 항목 – 운영보안

CHAPTER 4

개인정보보호 위반 사례

CHAPTER 1

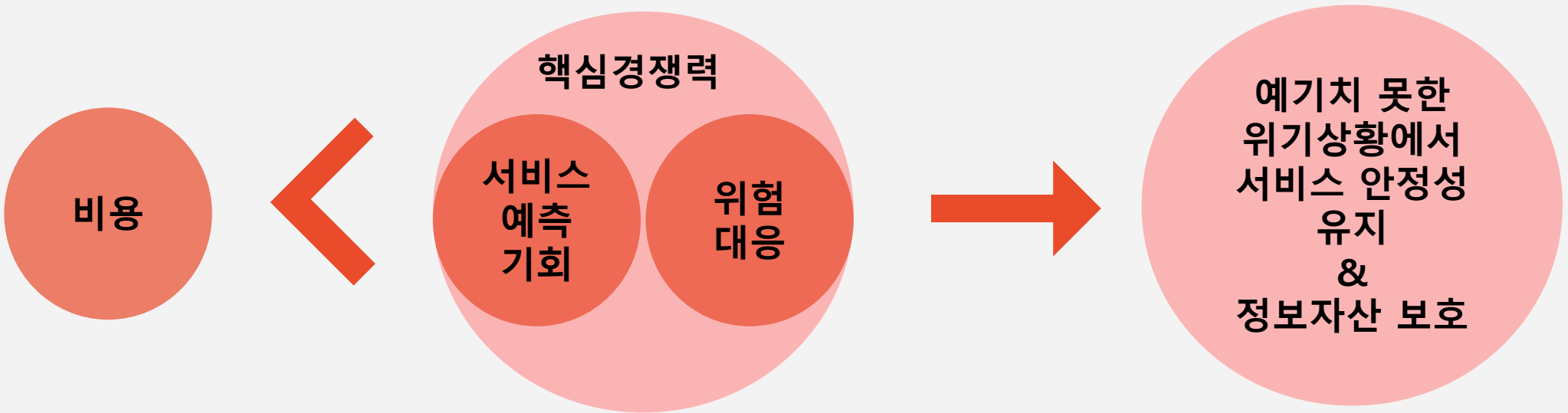
정보보호관리체계 (ISMS)

- 정보보호관리체계
- 필요성
- 인증 제도
- 인증 대상
- 인증 범위

정보보호관리체계 (ISMS)

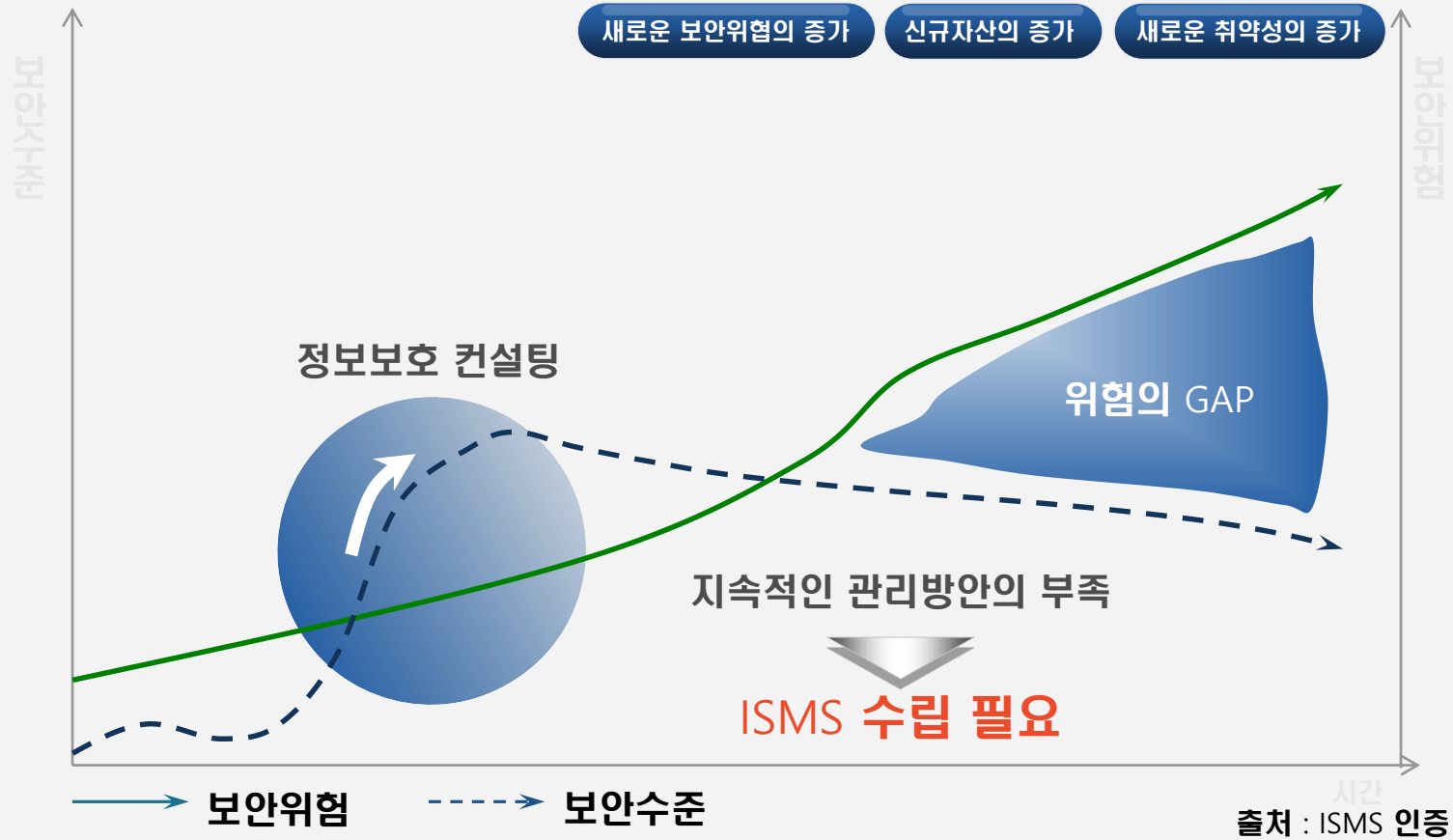
Information Security Management System

기업·기관이 각종 위협으로부터 주요 정보자산을 보호하기 위해 수립·관리·운영하는 종합적인 체계



정보보호관리체계의 필요성

지속적인 정보보호관리 없이는 위험의 GAP이 점점 커짐



출처 : ISMS 인증 최초심사 착수회의 자료집

정보보호관리체계 인증제도

정의

인증 대상기관이 수립·운영하고 있는 정보보호관리체계(ISMS)의 기술적, 물리적,관리적 정보보호대책이 인증심사기준(방통위 고시)에 지정된 심사기관이 객관적으로 평가하여 인증하는 제도

법적근거

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제 47조 및 동법 시행령

심사내용

5개 분야 정보보호 관리과정 12개의 인증 통제사항에 대한 적합성 평가
정보보호 대책 13개 분야, 92개 인증 통제사항에 대한 적합성 평가

정보보호관리체계 인증 대상

의무대상자

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제 47조 2항 및 시행령 제49조

구분	의무대상자 기준
ISP	「전기통신사업법」 제6조제1항에 따른 허가를 받은 자로서 서울특별시 및 모든 광역시에서 정보통신망서비스를 제공하는 자
IDC	정보통신망법 제46조에 따른 집적정보통신시설 사업자
다음의 조건 중 하나라도 해당하는 자	연간 매출액 또는 세입이 1,500억원 이상인 자 중에서 다음에 해당되는 경우 - 「의료법」 제3조의4에 따른 상급종합병원 - 직전연도 12월 31일 기준으로 재학생 수가 1만명 이상인 「고등교육법」 제2조에 따른 학교
	정보통신서비스 부문 전년도(법인인 경우에는 전 사업연도를 말한다) 매출액이 100억원 이상인 자
	전년도 직전 3개월간 정보통신서비스 일일평균 이용자 수가 100만명 이상인 자

❖ 2016년 개정된 시행령에서 상급 종합병원 및 대학교이 의무대상 범위에 포함

출처 : IISMS 인증제도 안내서_KISA

정보보호관리체계 인증 대상

의무 인증대상자 유의사항

✓ 인

✓ 인

✓ 인

인증 절차 내용	① 준비			② 심사					③ 인증	
	ISMS 운영	인증 신청	인증 신청	심사 준비	인증 심사	보완 조치	조치 확인	심사 결과보고서 작성	인증위원회 심의 준비	인증위원회 심의 및 인증서 교부
소요 시간	2개월 (최소)	5일	5일	30일	5일	30일	5일	5일	30일	2일

※ 위 소요기간은 평균적인 수치이며, 인증범위 및 규모, 정보보호 환경 등 내·외부 요인에 따라 변동 될 수 있음

✓ ISMS 인증제도 안내서 구축 및 운영에 필요한 소요기간을 확인하여 인증심사에 차질이 없도록 준비해야 한다.

정보보호관리체계 인증 범위

의료분야 정보보호 관리체계 인증범위 예시

구분	설명	
의료정보 시스템	EMR	전자의무기록(Electronic Medical Record). 진료, 진료지원, 원무 등 병원 업무 전반을 포괄하는 시스템
	OCS	처방전달시스템(Order Communication System). EMR과 별도의 OCS 운영할 경우 포함
원격의료 시스템	u-헬스케어 등	컴퓨터, 화상통신 등 정보통신 기술을 활용하여 먼곳에 있는 의료인에게 의료지식이나 기술을 지원하는 의료 활동
홈페이지	정보 제공	의료 기관 소개, 이용안내, 건강 정보 제공 등
	진료 예약/조회	온라인 진료 예약, 현황 조회 등
	진단검사결과 조회	혈압, 혈당, 맥박, 키, 체중 등 건강진단 검사 결과 조회
	증명서 발급/출력	진단서, 소견서, 입원사실증명서, 의료비 납입 증명서 등
	기타	온라인 상담, 민원 처리 등

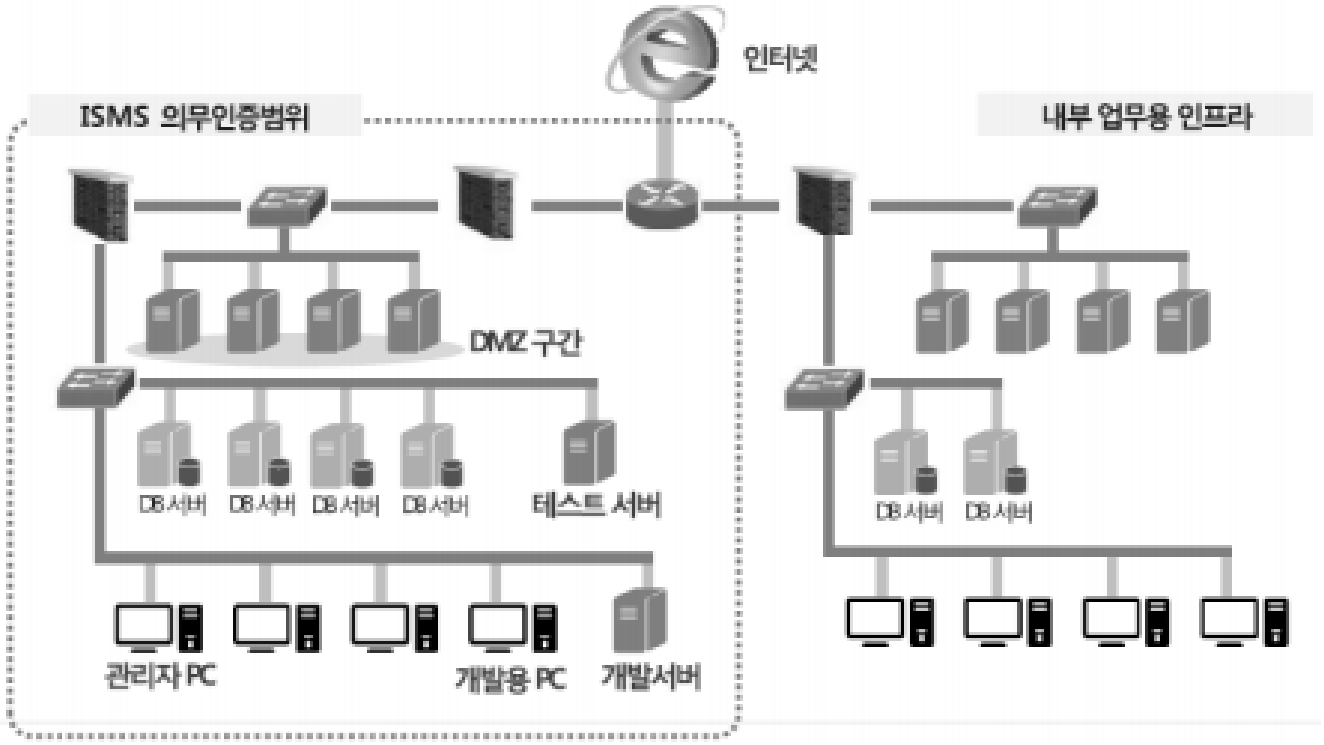
※ 홈페이지 부문은 병원별로 인터넷에서 접근 가능한 모든 대고객 서비스 포함

❖ 인증범위 예시는 반드시 인증 의무 범위에 포함되어야 하는 범위를 나타낸 것이며, 본 사례에 포함되지 않았다고 해서 인증 의무 범위에서 제외된다는 의미는 아님

출처 : IISMS 인증제도 안내서_KISA

정보보호관리체계 인증 범위

의무 인증대상자인 경우,
인증범위는 신청기관의 인증 의무대상 요건에 해당하는 정보통신 서비스를 포함



ISMS 의무 인증범위 설정 예시

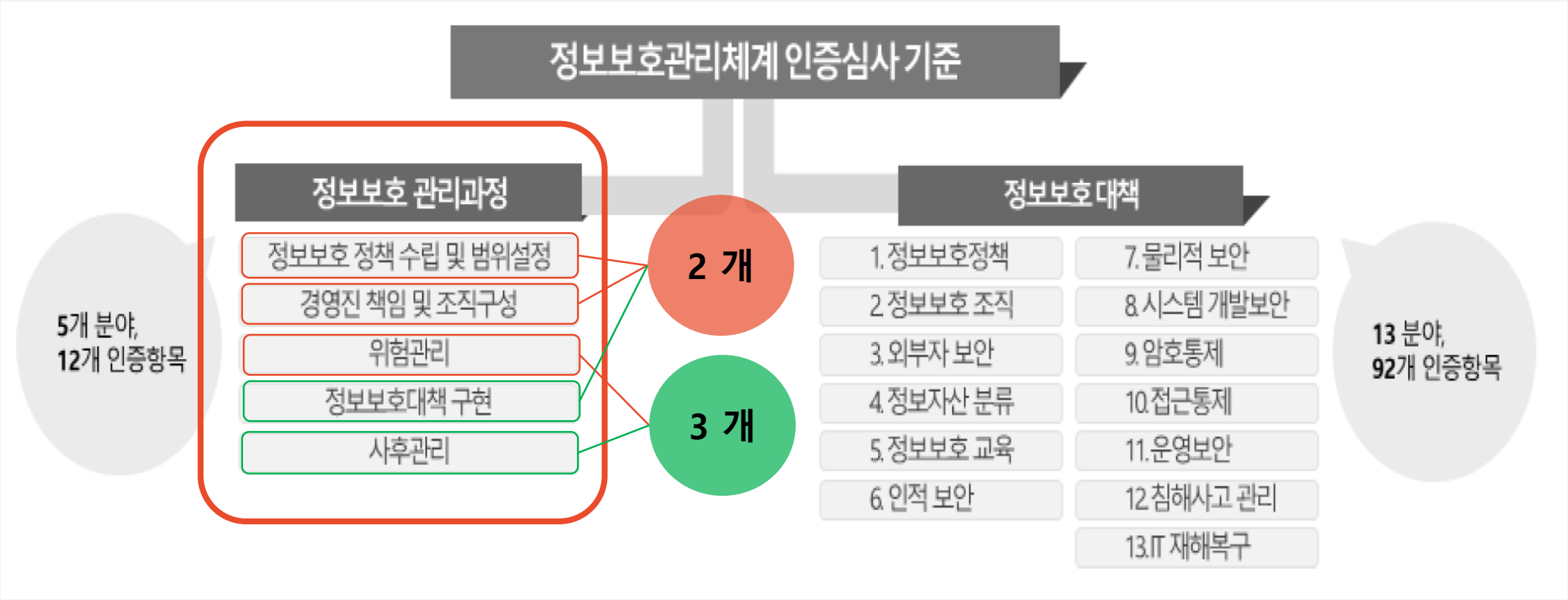
- 해당 서비스의 직접적인 운영 및 관리를 위한 백오피스 시스템은 인증범위에 포함되며, 해당 서비스와 관련이 없더라도 그 서비스의 핵심정보자산에 접근가능 하다면 포함
  ISMS 의무인증범위 내에 있는 서비스, 자산, 조직(인력)을 보호하기 위한 보안시스템은 포함
- 정보통신서비스와 직접적인 관련성이 낮은 전사적자원관리시스템(ERP), 분석용데이터 베이스(DW), 그룹웨어 등 기업 내부 시스템, 영업/마케팅 조직은 일반적으로 인증범위 에서 제외

CHAPTER 2

정보보호 관리적 기준

- 정보보호 관리 과정
- 정보보호정책 수립 및 범위설정
- 경영진 책임 및 조직의 구성
- 위험관리
- 정보보호대책 구현
- 사후 관리

정보보호관리체계 인증 기준 – 정보보호 관리과정



출처 : IISMS **인증제도 안내서**_KISA

정보보호 관리과정

1. 정보보호정책 수립 및 범위설정

1.1 정보보호정책의 수립

조직이 수행하는 모든 정보보호 활동의 근거를 포함할 수 있도록 정보보호 정책을 수립
해당 정책은 국가나 관련 산업에서 정하는 정보보호 관련 법, 규제를 만족

- ✓ [최고경영자 등 경영진의 정보보호에 대한 의지 및 방향] ,[조직의 정보보호 목적, 범위, 책임], [조직이 수행하는 관리적, 기술적, 물리적 정보보호 활동의 근거] 가 포함된 최상위 수준의 정보보호 정책 수립
- ✓ 정보보호 상위 정책을 시행하기 위한 세부적인 수행주체, 방법, 절차 등은 정보보호 지침, 절차, 매뉴얼 등의 형식으로 수립

1.2 범위설정

조직에 미치는 영향을 고려하여 중요한 업무, 서비스, 조직, 자산 등을 포함할 수 있도록 정보보호 관리체계의 범위를 설정하고 범위 내 모든 자산을 식별하여 문서화 하여야 함

- ✓ 정보보호정책에 조직이 준수하여야 하는 법령 및 관련조항을 명시하여야 함

정보보호 관리과정

2. 경영진 책임 및 조직의 구성

2.1 경영진 참여

정보보호 조직이 수행하는 정보보호 활동 전반에 경영진의 참여가 이뤄지도록 보고 및 의사결정 체계수립

- ✓ 정보보호정책의 제 · 개정 승인 및 공표, 위험관리, 내부감사 등과 같은 중요한 사안에 대해 경영진이 참여하여야 하고 경영진의 책임과 역할을 정보보호정책에 명시해야 함

2.2 정보보호 조직 구성 및 자원 할당

최고경영자는 조직의 규모, 업무 중요도 분석을 통해 정보보호 관리체계의 지속적 운영이 가능하도록 정보보호 최고책임자, 실무조직 등 정보보호 조직을 구성하고 정보보호 관리체계 운영 활동을 수행하는데 필요한 자원(예산 및 인력)을 확보해야 함

가장 중요한.... 하지만,..

정보보호 관리과정

3. 위험관리

3.1 위험관리 방법 및 계획 수립

정보보호 조직이 수행하는 정보보호 활동 전반에 경영진의 참여가 이뤄지도록 보고 및 의사결정체계 수립

- ✓ 정보보호정책의 제 · 개정 승인 및 공표, 위험관리, 내부감사 등과 같은 중요한 사안에 대해 경영진이 참여하여야 하고 경영진의 책임과 역할을 정보보호정책에 명시해야 함

3.2 위험 식별 및 평가

위험관리 방법 및 계획에 따라 정보보호 전 영역에 대한 위험 식별 및 평가를 연 1회 이상 수행
해당 결과에 따라 조직에서 수용 가능한 위험수준을 설정하여 관리해야 함

- ✓ 수용 가능한 목표 위험수준을 정하고 이를 초과하는 위험을 식별해야 함(해당 수준은 최고책임자 등 경영진의 의사결정에 의해 설정된다)
- ✓ 위험처리의 시급성, 예산 할당, 구현에 요구되는 기간에 따라 이행 우선순위를 정해야 함

정보보호 관리과정

3. 위험관리

3.3 정보보호대책 선정 및 이행계획 수립

위험을 수용 가능한 수준으로 감소시키기 위한 정보보호대책을 선정
그 대책의 구현 우선순위, 일정, 담당부서 및 담당자 지정, 예산 등을 포함한 이행계획을 수립
최종 최고 경영진의 승인

- ✓ 식별된 위험의 처리 전략(위험감소, 위험회피, 위험전가, 위험수용 등)을 수립
- ✓ 위험 식별 및 평가 결과에 근거하여 정보보호 대책을 선정하고 정보보호 관리체계 인증 기준에서 제시하는 정보보호 대책 통제항목(92개)과의 연계성도 함께 고려

정보보호 관리과정

4. 정보보호대책 구현

4.1 정보보호대책의 효과적 구현

정보보호대책 이행 계획에 따라 보호대책 구현
경영진은 이행 결과의 정확성 및 효과성 여부를 확인

✓ 식별된 위험에 대하여 위험 수준이 감소되었음을 보장하기 위하여 정보보호 최고책임자 등은 경영진에게 이행 여부를 검토 및 확인 받아야 함

4.2 내부 공유 및 교육

구현된 정보보호대책을 실제 운영/ 시행할 부서 및 담당자 배정
실제 교육 시행

✓ 정책(지침 및 절차 포함) 신규 제정 및 개정 / 정보시스템 신규 도입 및 개선 시, 해당 내용을 공유하고 교육하여야 함

정보보호 관리과정

5. 사후 관리

5.1 법적요구사항 준수검토

조직이 준수해야 할 정보보호 관련 법적요구사항을 지속적으로 파악하여 최신성 유지

- ✓ 조직이 준수해야하는 법적 요구사항의 준수여부를 주기적 (최소 연 1회 이상) 검토

5.2 정보보호 관리체계 운영현황 관리

정보보호 활동의 수행 주기를 손쉽게 확인할 수 있도록 문서화하고 최신성 여부를 주기적으로 검토

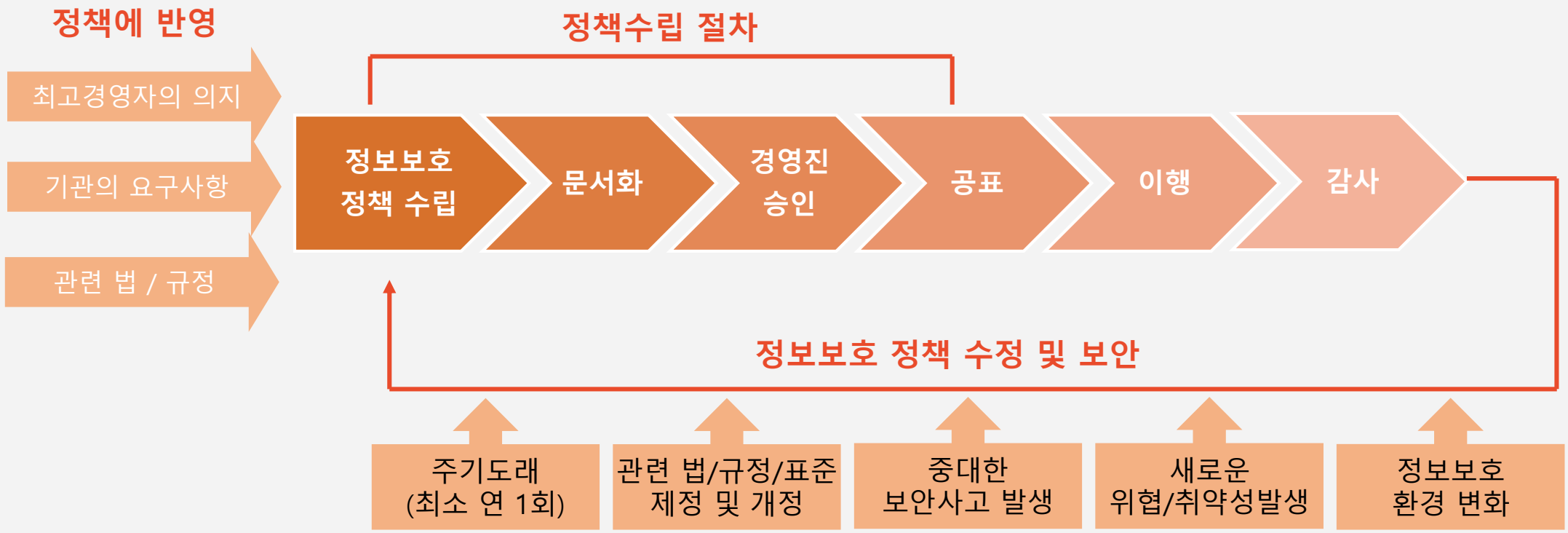
- ✓ 그 운영현황을 확인할 수 있도록 수행 주기, 수행 주체(담당부서, 담당자)를 정의한 문서(운영현황표)를 주기적 (최소 연 1회 이상) 관리

5.3 내부감사

정보보호 관리체계가 정해진 정책 및 법적 요구사항에 따라 효과적으로 운영되고 있는지 점검

- ✓ 내부감사 기준, 범위, 수행주기, 감사인력(객관성 확보를 위해 제3자가 감사를 수행하는 것이 원칙) 을 수립

정보보호 관리과정



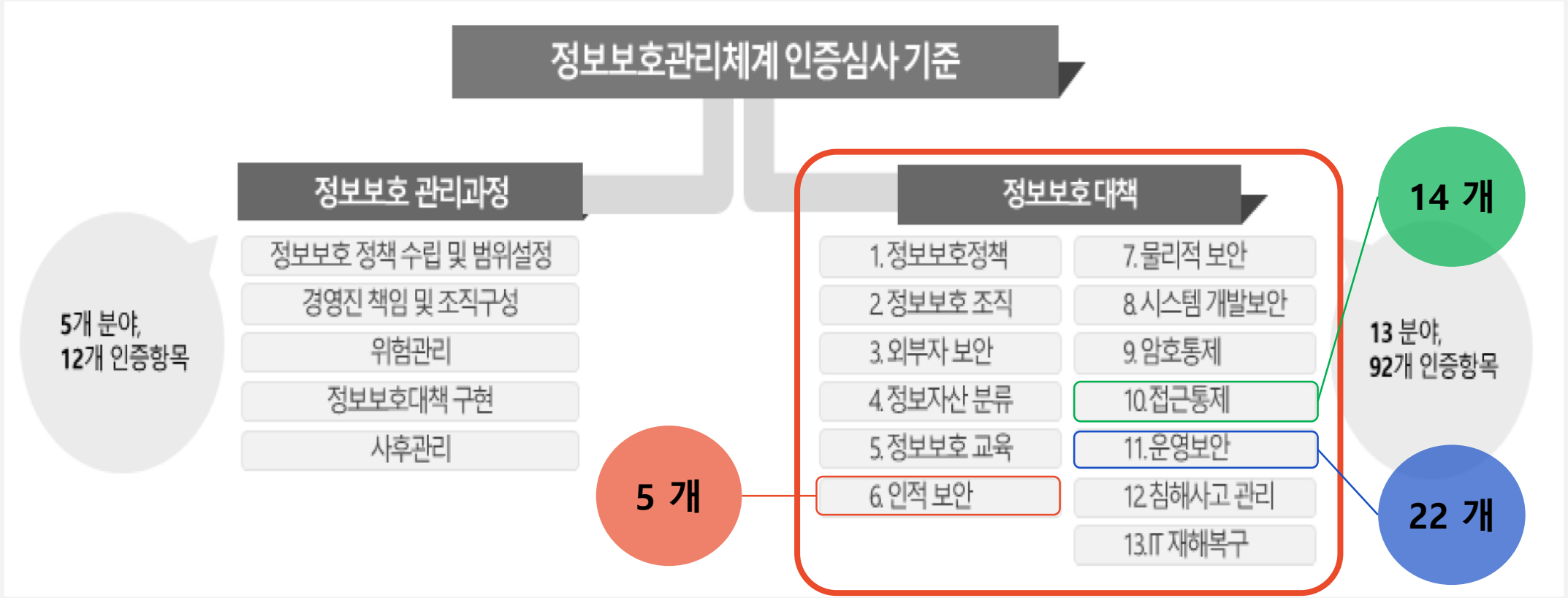
출처 : 의료기관을 위한 정보보호 안내서 _보건복지부

CHAPTER 3

정보보호 대책

- 정보보호 대책
- 세부점검 항목 – 인적보안
- 세부점검 항목 – 접근통제
- 세부점검 항목 – 운영보안

정보보호관리체계 인증 기준-정보보호 대책



출처 : IISMS 인증제도 안내서_KISA

정보보호 대책

세부정검 항목 6. 인적보안

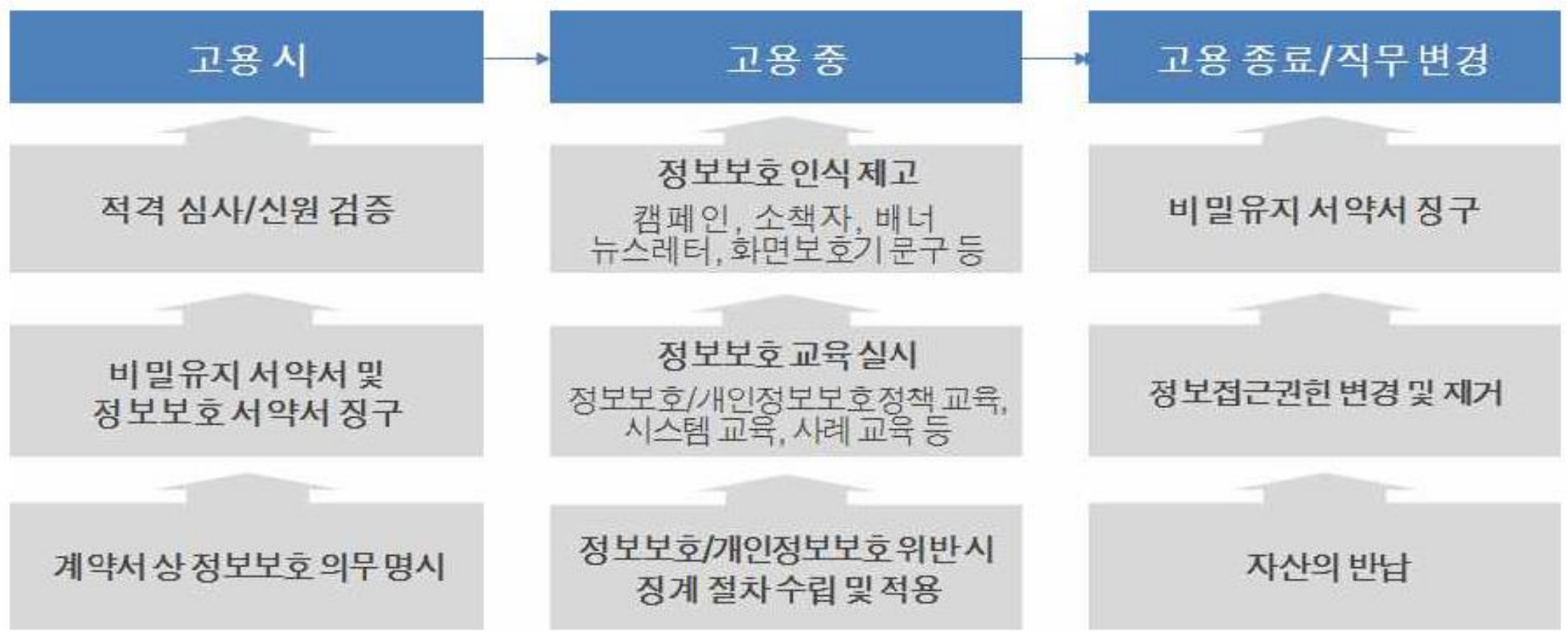
목적

병원에서 근무하는 인력에 대한 정보보호 방안을 마련하여 정보보호 사고의 가능성을 최소화

- 고용 시 해당 인력의 적격성을 평가,비밀유지 서약서 및 정보보호 서약서 징구,근로계약서 상 정보보안 책임과 의무 명시를 수행한다.
- 고용 중 의료진 및 임직원을 대상으로 정보보안 교육 및 훈련을 제공하고,정보보호의무 위반 시 징계절차를 마련한다.
- 고용 종료나 직무 변경 시 퇴직자 및 전근자에 대한 정보보호 절차가 마련되어야 하고, 비밀유지 서약서를 징구한다.

정보보호 대책

1. 인적보안



출처 : 의료기관을 위한 정보보호 안내서 _보건복지부

정보보호 대책

세부정검 항목 10. 접근통제

목적

정당한 권한이 있고 확인된 자만이
병원의 정보 및 EMR과 같은 진료정보시스템, 처방전달시스템(OCS), 진단검사 장비, 임상방사선 장비 등의 의료기기 및 정보처리 시설에 접근할 수 있게 함으로써 정보보호 사고에 대한 가능성을 최소화

접근권한 정의

직무분류와 사용자의 역할 등 특성에 따른 접근권한 정의

- 고용형태 : 정규직원, 계약직원, 임시직원, 외부협력사 직원 등
- 직무특성 : 경영자, 의사, 간호사, 원무과직원, 연구자 등
- 근무영역 : 응급실, 입원병동, 외래병동 등

정보보호 대책

세부정검 항목 10. 접근통제

목적

정당한 권한이 있고 확인된 자만이
병원의 정보 및 EMR과 같은 진료정보시스템, 처방전달시스템(OCS), 진단검사 장비, 임상방사선 장비 등의 의료기기 및 정보처리 시설에 접근할 수 있게 함으로써 정보보호 사고에 대한 가능성을 최소화

접근 권한 설정 및 인증 절차

사용자 등록 및 해지 절차 수립

- 유일한 사용자 계정 사용 (1인 1계정/ 개별 권한 부여)
- 퇴직자 계정 “즉시 " 비활성화 혹은 제거
- 주기적 계정 유효성 및 중복성 점검

정보보호 대책

세부정검 항목 10. 접근통제

접근 권한 설정 및 인증 절차

사용자 접근권한 설정 절차 수립

- 담당업무별 최소권한 부여 원칙
- 전출입, 퇴직 등 권한 변동사유 발생 즉시 권한 조정
- 주기적 접근 권한 점검
- 관리자(admin, super user)접근은 엄격하게 적용하고 승인절차와 기록 유지

사용자 인증/인가 절차 수립

- 안전한 로그인 절차 수립
- 영문 · 숫자 · 특수문자 포함 추측하기 어려운 비밀번호 설정
- 시스템/기기 도입 시 초기설정 비밀번호 변경
- 싱글 사인온(Single Sign-On)을 사용할 경우 주요 정보시스템 접근 시 재인증이나 다중(Multi-factor) 인증 등 별도의 보안대책 마련

정보보호 대책

세부정검 항목 10. 접근통제

접근 권한 설정 및 인증 절차

비인가 접근 차단 대책 수립

- **해킹**이나 **비인가자의 접근**을 **차단**할 수 있는 대책 마련
- 업무용 시스템의 물리적 또는 논리적 **인터넷 차단**
- 비인가자의 접근 차단을 위한 **침입차단 및 탐지 시스템 설치**
- **백신** 및 **패치관리**, 매체사용 통제, 불법 소프트웨어 통제, **P2P/메신저 사용 관리**
- 보안구역의 경계구역 **출입통제 강화**(상 · 하차구간, 우편함 등)

정보보호 대책

세부정검 항목 10. 접근통제

관리자 권한 및 특수 권한 관리 목적

병원의 시스템 관리자 권한이나 특수 권한이 공격자에 의해 탈취되었을 경우
일반 사용자 계정 도용에 비해 심각한 위험 초래

관리자 권한 및 특수 권한 관리

- 필요한 최소 인원에게 관리자 권한 및 특수 권한 부여
- 권한 부여 시 책임자의 승인을 포함한 인가 절차 수립
- 관리자 권한 식별, 관리자 계정 목록 관리
- 특수 권한은 반드시 필요한 경우에만 할당
- 특수 권한 계정 목록 관리
- 특수 권한 계정에 정보보호 시스템(침입차단 시스템 등) 관리자 및 응용 프로그램 관리자 계정 포함
- 유지보수 등을 위한 협력사 직원에게 부여하는 특수 권한 계정은 필요 시에만 생성하고 작업 완료 후 즉시 삭제 또는 정지하는 절차 적용

정보보호 대책

세부정검 항목 11. 운영 보안

목적

병원의 진료정보 시스템, 처방전달시스템(OCS), 진단검사 장비, 임상방사선 장비 등의 의료기기 및 정보처리시설 운영 시 필요한 정보보호 규정을 마련하여 안전하게 정보시스템과 통신시설을 운영

안티 바이러스와 패치

- 모든 서버와 컴퓨터에는 안티바이러스 소프트웨어를 설치하고 최소한 일 1회 자동 업데이트되며 전체 시스템 스캔을 주기적으로 실행하도록 설정
- 바이러스가 자동으로 제거되지 않을 때를 대비하여 감염된 기기 격리, 바이러스 수동제거, 재설치, 재설정 등과 같은 절차를 마련
- 중앙에서 통제되는 것과 동일한 수준의 환경설정 및 규정을 적용

정보보호 대책

세부정검 항목 11. 운영 보안

안전한 정보시스템 운영을 위한 정보보호

- 정보시스템 구성도 및 운영절차 문서화
- 기술적 취약성에 대한 대책 마련 및 소프트웨어 설치 제한
- 악성코드 방지 소프트웨어 설치 및 사용자 교육
- 변경관리절차 수립
- 자원 사용 용량 모니터링 및 예측 · 분석
- 백업 시 정보 암호화 및 원격지 소산, 주기적 백업, 백업 복구 테스트
- 사용자/운영자/관리자의 이벤트 로그를 모니터링 · 분석
- 정확한 로그 확보를 위하여 시간 동기화 및 로그기록 보호
- 감사 활동을 통한 정보보호 침해 방지, 감사기록 보호

정보보호 대책

세부정검 항목 11. 운영 보안

변경 관리

- 정보시스템의 구성요소를 변경할 경우

  변경으로 인하여 다른 시스템에 영향을 주거나 의도하지 않은 새로운 위험이 발생하거나

  전체적인 서비스 품질이 저하될 수 있음

- 변경관리의 목적

  병원 각 단위에서 정보시스템을 변경할 경우 변경 수행의 순차적인 절차를 규정함으로써

  신규 위험이나 취약점을 예방하고 데이터와 시스템의 무결성(integrity)을 유지하는 것

- 내부 변경관리절차 수립, 담당자의 역할 정립, 변경관리 툴 (tool) 활용 – 세 가지 요소가 적절히 결합
- 병원은 일반적인 변경과 민감한 정보처리를 위한 시스템의 긴급한 변경을 관리하는

  공식적 절차를 수립하고 문서화

- 변경을 요청 / 승인 / 적용하는 담당자는 각각 분리되어야 함

정보보호 대책

세부정검 항목 11. 운영 보안

백업과 복구

- 백업장치는 재해 · 재난이 발생했을 때 영향을 받지 않을 수 있도록 본 시스템과 별도 분리된 안전한 장소에 보관
- 백업 실패 보고는 즉시 검토하고 중요한 문제점은 바로 해결
- 백업과 복구가 적절하게 이루어지는지 확인하는 테스트는 최소 연 2회 실시

분리와 최소화

- 민감한 데이터와 시스템은 별개의 도메인이나 환경으로 구획화 하여 관리
- 보안의 관점에서 다른 역할을 수행하거나 다른 구역에 있는 서비스, 시스템, 데이터 및 사용자는 서로 분리
- 시스템에 불필요한 소프트웨어, 서비스, 프로토콜 및 기타 기능은 비활성화하거나 제거하여 문제가 발생할 가능성을 최소화

정보보호 대책

세부정검 항목 11. 운영 보안

로깅과 모니터링

- 로깅과 모니터링을 수행함으로써 규정 준수 여부를 평가하거나 침해 여부를 발견하고 대응 프로그램에 효과적으로 지원
- 시스템과 데이터베이스의 사용자 활동을 모니터링하는 활동 모니터링(activity monitoring)은 정보 접근 및 인증 이벤트 기록, 설정 변경, 데이터 전송 트래픽에 대한 상세한 기록을 제공
- 정보보호 침해를 일으킬 수 있는 비정상적인 행위가 발생하면 담당자에게 자동으로 알람을 발송하도록 설정
- 비인가 접근, 변조, 삭제로부터 로그파일을 보호하기 위하여 즉시 백업, 다중 인증, 업무상 필요할 경우만 접근하는 등의 보호조치가 필요

정보보호 대책

세부정검 항목 11. 운영 보안

노트북 관리

- **노트북 관리의 목적**

  진료정보, 개인식별정보 등 민감한 정보가 저장된 노트북의 분실 · 도난 및 손상은 가장 자주 발생하는 정보보호사고이기 때문에 노트북 관리에 주의가 필요함

  - 병원 내 의료진과 임직원의 노트북 등록
  - 전체 디스크 암호화 : 어떤 파일을 암호화할지 여부를 개인의 판단에 의존 하지 않고 시스템적으로 적용
  - 원격 추적 및 원격 데이터 리셋 기능 적용
  - 승인된 경우 외의 시스템 변경 불가, 소프트웨어 설치 불가
  - 노트북에 대한 정보보호 인식제고, 교육 및 훈련 제공

정보보호 대책

세부정검 항목 11. 운영 보안

휴대용 저장장치

- **휴대용 저장장치에 대한 정보보호 중요성 증대**

  내 · 외부인 소유의 USB 저장장치를 통한 환자 및 직원의 개인정보 유출 증가

  바이러스에 감염된 USB 저장장치로 인한 전체 시스템 마비 및 파괴 위험

  진료정보교류를 위한 CD 사용 증가

  - 휴대용 저장장치 파악 및 등록 및 저장 데이터 암호화
  - USB 보안소프트웨어 설치 등 등록된 장치만 사용할 수 있도록 조치
  - 장치에 저장된 정보등급에 따라 보안 설정 및 규정 준수
  - 휴대용 장치의 분실 · 도난 및 손상에 대한 정보보호 인식제고, 교육 · 훈련 제공
  - 휴대용 장치 사용의 오 · 남용 모니터링
  - 저장장치 폐기나 재사용 시 복구할 수 없는 상태로 정보 삭제 및 매체 파기

정보보호 대책

세부정검 항목 11. 운영 보안

모바일 기기

- 모바일 기기 도난 · 분실이나 해킹을 통한 환자의 개인정보 유출 사고가 매년 증가하는 추세
  이에 따른 운영 대책 필요

  - 모바일기기 파악 및 등록 & 등록된 기기만 사용 가능 설정
  - 비밀번호 설정 및 정보 암호화
  - 망 분리, 진료정보 접속 제한, 유해사이트 차단
  - 도난 · 분실에 대비하여 원격 비활성화, 삭제 및 잠금 기능 적용
  - 기기 분실 · 도난 및 손상에 대한 정보보호 인식제고, 교육 · 훈련 제공
  - 기기 폐기 및 등록 해제 시 기기 아이디 비활성화
  - 기기 폐기 시 저장 정보를 복구할 수 없는 상태로 삭제했는지 확인

CHAPTER 4

개인정보보호 위반 사례

개인정보 보호 위반 사례

의료분야에서 발생하는 주요 개인정보보호 위반사례

진료목적 외 개인정보 수집	• 개인정보보호법 제 15조 개인정보 수집 시 고지사항 위반
환자 개인정보의 처리 위탁	• 수탁기관 및 위탁업무 내용 공개 위반 • 개인정보보호법 제 26조 처리위탁 업무에 따른 조치사항
환자 개인정보처리시스템의 접근권한	• 시스템 사용자 이력관리 미흡 • 개인정보 보호법 제 29조 개인정보 안정성 확보조치 위반
환자 개인정보 접속기록	• 접속기록 2년 보관 • 개인정보 보호법 제 29조 개인정보 안정성 확보 조치 위반
개인정보 암호화	• 병원 홈페이지 회원 가입 시 수집되는 개인정보 암호화 미흡 • 일방향 암호화

출처 :보안뉴스_의료분야 개인정보보호 주요 위반사례

개인정보 보호 위반 사례

사례 2. 진료목적 외 개인정보 수집 위반

A 병원은 홈페이지를 운영하고 있으나 회원가입은 받지 않고 있다.
다만, 상담 및 문의 게시판을 이용할 경우, 문의자의 이름, 전화번호를 기재하도록 의무화 하고 있다.

A병원에게 개인정보보호법 (제 15조 2항) 개인정보 수집 시 고지사항 위반으로 과태료 600만원이 부과된다.

회원가입 없이 게시판을 이용한 상담, 문의 시에도 이름, 전화번호 등 개인정보를 수집할 경우 정보주체에게 필수항목 ①수집·이용목적 ②수집항목 ③보유 및 이용기간 ④동의를 거부할 권리가 있다는 사실 및 불이익 내용 등 4가지를 고지하고 동의를 받아야 한다.

출처 :보안뉴스_의료분야 개인정보보호 주요 위반사례

개인정보 보호 위반 사례

사례 2. 개인정보 처리 위탁에 따른 조치사항 위반

C 병원은 혈액검사, 시스템 유지보수, 홈페이지 등 수탁업체가 다수 존재하지만, 홈페이지에 혈액검사 기관만을 공개하고 있다.

C병원에게 개인정보 처리 위탁에 따른 조치사항 위반(제26조제2항)으로 과태료 200만원이 부과된다.

홈페이지 기관만 공개하는 게 아니라 모든 수탁기관을 공개해야 하고, 수탁기관명과 위탁업무내용까지 모두 공개해야 한다.

출처 :보안뉴스_의료분야 개인정보보호 주요 위반사례

개인정보 보호 위반 사례

사례 3. 접근권한 위반

B병원의 개인정보처리 시스템의 경우 각 ID별 권한을 부여할 수 있는 기능만 존재하고 그 이력 관리에 대해서는 별도로 기능을 추가하지 않았다.

B병원에게 개인정보 안전성 확보조치 위반(제29조)으로 접근통제 및 접근권한 관리 미흡에 해당되며, 과태료 600만원이 부과된다.

접근권한을 부여할 수 있는 권한 외에 접근권한 이력관리도 동시에 해야 한다. 이를 위해서는 개인정보처리 시스템의 기능을 개선해 접근권한 이력관리가 이루어지도록 해야 한다.

출처 :보안뉴스_의료분야 개인정보보호 주요 위반사례

개인정보 보호 위반 사례

사례 4. 개인정보 접속기록 위반

D병원은 개인정보처리 시스템의 접속자 ID, 접속자 IP주소, 시간을 2년간 보관하도록 하고 있다.

D병원에게 개인정보 안전성 확보조치를 위한 접속기록 관리 위반(제29조)으로 과태료 600만원이 부과된다.

접속자가 개인정보처리 시스템을 통해 어떤 업무를 수행했는지 파악할 수 있는 정보(수행업무)를 접속기록에 추가해야 한다..

출처 :보안뉴스_의료분야 개인정보보호 주요 위반사례

개인정보 보호 위반 사례

사례 5. 개인정보 암호화 조치 위반

E병원은 홈페이지를 통해 회원 가입을 받고 있다. 회원 가입시 개인정보(비밀번호)를 수집하고 있지만, 개인정보를 암호화하지는 않은 상태다.

E병원에게 개인정보 안전성 확보조치를 위한 암호화 조치 위반으로 과태료 600만원이 부과된다.

홈페이지에서 비밀번호를 수집하는 기관의 경우 비밀번호가 유출, 변조되지 않도록 통신 암호화(SSL, TLS 등) 조치를 하고, DB를 저장할 때는 일방향 암호화를 적용해야 한다.

출처 :보안뉴스_의료분야 개인정보보호 주요 위반사례

Q&A

Thank you for your attention