

배포용

의료기관 외부보관 EMR 인증심사 안내서 [Ver.2]

2022. 3.

목 차

I. 개요	1
II. 인증신청 방법	4
III. 인증심사 절차	6
양식1. 인증기준 면제 신청서	14
양식2A. EMR 점검표 (ISMS-P 또는 ISMS 제출)	15
양식2B. EMR 점검표 (ISMS-P 또는 ISMS 미제출)	17
양식2-1. 이중화된 네트워크의 구성 증빙자료 제출 양식	22
양식2-2. 인증 정보보호제품 도입 점검표	23
양식2-3. 정보보호제품 인증서 증빙자료 제출 양식	24
양식2-4. 물리적 위치의 한정 증빙자료 제출 양식	25
양식2-5. 클라우드컴퓨팅 사용 서비스 규격 확인서	26
양식3. 클라우드컴퓨팅 서비스 정보보호 기준 고시 항목별 점검표 ..	27
양식4. IaaS 및 인프라 취약점 점검 및 모의침투 테스트 수행 확인서	43
양식5. SaaS 및 SW 취약점 점검 및 모의침투 테스트 수행 확인서	44
양식6. 집적정보통신시설 사업자 제출자료 적합성 확인서	45

목 차

참고1 일부 인증기준 항목에 대한 심사 면제	47
참고2 국가 공공기관의 정의	48
참고3 상용(商用) 클라우드컴퓨팅 서비스	49
참고4 취약점 점검 및 모의침투 테스트 도입 취지	52
참고5 정보보호 전문 서비스 기업	53
참고6 클라우드 보안서비스 도입기준 변경 공지	54

I. 개요

◇ 본 안내서는 「전자의무기록시스템 인증제」 보안성 인증기준 S014 (외부보관 및 클라우드 컴퓨팅 서비스) 개정('21.6월)에 따라, 인증기준 해설 및 인증심사 절차를 설명하기 위한 안내서입니다.

□ 목적

- 의료기관 등이 전자의무기록을 의료기관 외부에 안전하게 관리·보존하는지 여부를 심사 및 인증하는 절차와 기준을 정함

□ 적용대상

- 의료기관 외부의 집적정보통신시설을 이용하는 전자의무기록시스템
- 의료기관 내부에 의료기관이 자체적으로 정보통신설비(사설 클라우드 환경 등)를 구축하여, 상용(商用)으로 제공하는 전자의무기록시스템

<(참고) 집적정보통신시설과 상용 클라우드컴퓨팅서비스 관련 해설>

- ▶ 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제46조 및 「**집적정보 통신시설 보호지침**」 고시
 - 제2조(정의) 1. "**집적정보통신시설**"이라 함은 법 제2조제2호에 따른 정보통신서비스를 제공하는 **고객의 위탁을 받아** 컴퓨터장치 등 전자정부법 제2조제13호에 따른 **정보시스템을 구성하는 장비**(이하 "정보시스템 장비"라 한다)를 **일정한 공간**(이하 "전산실"이라 한다)에 **집중하여 관리하는 시설**을 말한다.
- ▶ **클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률**
 - 제2조(정의) 1. "**클라우드컴퓨팅(Cloud Computing)**"이란 **집적·공유된** 정보통신기기, 정보통신설비, 소프트웨어 등 정보통신자원(이하 "정보통신자원"이라 한다)을 이용자의 요구나 수요 변화에 따라 정보통신망을 통하여 신속적으로 이용할 수 있도록 하는 정보처리체계를 말한다.
 - 3. "**클라우드컴퓨팅서비스**"란 클라우드컴퓨팅을 활용하여 **상용(商用)**으로 타인에게 정보통신자원을 제공하는 서비스로서 대통령령으로 정하는 것을 말한다.
 - 제16조(클라우드컴퓨팅기술 기반 집적정보통신시설의 구축 지원)

○ (적용 제외대상)

- 의료기관이 자체적으로 정보통신설비를 구축하여 **해당 의료기관 내부적으로 활용하는 비상용(非商用) 전자의무기록시스템**

- 예) ① 의료원 체제의 모(母) 의료기관이 소속 의료기관에 전자의무기록시스템 서비스를 하는 경우
- ② 국가·공공기관이 소속 의료기관에 전자의무기록시스템 서비스를 하는 경우

□ 근거

○ 「의료법」 제23조(전자의무기록) 제2항

② 의료인이나 의료기관 개설자는 보건복지부령으로 정하는 바에 따라 전자의무기록을 안전하게 관리·보존하는 데에 필요한 시설과 장비를 갖추어야 한다.

○ 「의료법 시행규칙」 제16조(전자의무기록의 관리·보존에 필요한 시설과 장비) 제1항

① 의료인이나 의료기관의 개설자는 법 제23조제2항에 따라 전자의무기록(電子醫務記錄)을 안전하게 관리·보존하기 위하여 다음 각 호의 시설과 장비를 갖추어야 한다.

○ 「전자의무기록의 관리 보존에 필요한 시설과 장비에 관한 기준 고시」 제7조(의료기관 외의 장소 관리·보존시 추가적인 조치)

제7조(의료기관 외의 장소 관리·보존시 추가적인 조치) 전자의무기록 관리자가 의료기관 외의 장소에서 전자의무기록을 관리·보존하는 경우에는 규칙 제16조제1항제3호부터 제7호까지에 따른 시설과 장비에 대하여 별표에 따른 추가적인 조치를 하여야 한다.

○ 「개인정보보호법」 제29조(안전조치의무)

제29조(안전조치의무) 개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.

○ 「개인정보 보호법 시행령」 제30조(개인정보의 안전성 확보 조치) 제1항

- ① 개인정보처리자는 법 제29조에 따라 다음 각 호의 안전성 확보 조치를 하여야 한다.
1. 개인정보의 안전한 처리를 위한 내부 관리계획의 수립·시행
 2. 개인정보에 대한 접근 통제 및 접근 권한의 제한 조치
 3. 개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치
 4. 개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치
 5. 개인정보에 대한 보안프로그램의 설치 및 갱신
 6. 개인정보의 안전한 보관을 위한 보관시설의 마련 또는 잠금장치의 설치 등 물리적 조치

○ 「클라우드컴퓨팅법」 제23조(신뢰성 향상) 제2항

② 과학기술정보통신부장관은 클라우드컴퓨팅서비스의 품질·성능에 관한 기준 및 정보보호에 관한 기준(관리적·물리적·기술적 보호조치를 포함한다)을 정하여 고시하고, 클라우드컴퓨팅서비스 제공자에게 그 기준을 지킬 것을 권고할 수 있다.

□ 외부보관 EMR 인증기준

- (인증기준 번호) S014
- (인증기준 명칭) 외부보관 및 클라우드 컴퓨팅 서비스 (의료기관 외부 집적정보통신시설 이용 서비스)
- (인증기준 내용)

<인증기준 S014>

1. 「의료법」 제23조(전자의무기록) 제2항에 따른 보건복지부 고시 「전자의무기록의 관리 보존에 필요한 시설과 장비에 관한 기준」과 동 기준 [별표]「의료기관 외의 장소에 전자의무기록 보관시 필요한 추가적인 조치」를 준수하는 서비스를 이용하여야 한다.
2. 「클라우드 컴퓨팅 발전 및 이용자 보호에 관한 법률」 제23조(신뢰성 향상) 제2항에 따른 과기부 고시 「클라우드컴퓨팅 서비스 정보보호에 관한 기준」 제3조(관리적 보호조치), 제4조(물리적 보호조치), 제5조(기술적 보호조치) 기준을 만족하는 서비스를 이용하여야 한다.
 - 단, 국가·공공 의료기관은 한국인터넷진흥원의 CSAP 인증을 받은 서비스를 이용하여야 한다.
3. (시범) 의료데이터 이외의 데이터와 혼재되지 않도록 별도의 분리된 의료 데이터 전용의 독립 네트워크를 구성할 수 있다.

[해당 기관] 의료기관 외부의 집적정보통신시설을 이용하는 전자의무기록시스템 개발 기관
[용어 설명] '국가·공공 기관'은 전자정부법 제2조 제2항 '행정기관', 제3항 '공공기관'의 정의를 따름

[관련 법령] 의료법 제23조제2항, 같은 조 제4항 및 같은 법 시행규칙 제16조, 보건복지부 고시 「전자의무기록의 관리 보존에 필요한 시설과 장비에 관한 기준」, 클라우드 컴퓨팅법 제23조제2항, 과기부 고시 「클라우드컴퓨팅서비스 정보보호에 관한 기준」

- (제1호) 보건복지부 고시 '전자의무기록의 관리 보존에 필요한 시설과 장비에 관한 기준'(이하 EMR시설장비기준 고시) 준수 여부 심사
- (제2호) 과학기술정보통신부 고시 '클라우드컴퓨팅 서비스 정보보호에 관한 기준 제3조~제5조 관리적, 물리적, 기술적 보호조치 준수 여부 심사
- (제3호) 시범기준으로 의료 데이터 전용 독립 네트워크를 구성하여 서비스하도록 권고함

※ S014 인증기준 변경('21.6월) 이전에 인증을 받은 전자의무기록시스템이 S014 인증기준 대상인 경우는 해당 인증 유효기간 만료 후 인증갱신 시 심사함

II. 인증신청 방법

□ 개요

- EMR 외부보관 방식을 클라우드컴퓨팅 서비스 여부에 따라 **단순 외부보관(그룹 I)**과 **클라우드 기반 외부보관(그룹 II)**으로 구분
 - (그룹 I) 클라우드 방식이 아닌 경우 S014 인증기준 제1호만 적용
 - (그룹 II) 클라우드 방식인 경우 S014 인증기준 제1호와 제2호를 모두 적용
- 관련 보안인증(ISMS-P, ISO 27017, ISO 27018) 보유 여부에 따라 심사 방식을 구분하여 적용

◆ 관련 보안인증 : ISMS-P*, ISO 27017, ISO 27018

▶ ISMS-P* : 정보보호 및 개인정보보호 관리체계, 한국인터넷진흥원(KISA)

- 정보보호 및 개인정보보호를 위한 일련의 조치와 활동이 인증기준에 적합함을 증명하는 제도
- * 기존의 ISMS와 PIMS가 ISMS-P 인증제도로 통합·운영 중이며, 한시적으로 ISMS도 인정

▶ ISO 27017 : 클라우드서비스정보보안 인증, ISO/IEC

- 클라우드 서비스 제공자(Cloud Service Provider)의 클라우드 보안에 필요한 보안통제와 구현지침

▶ ISO 27018 : 클라우드서비스개인정보보호 인증, ISO/IEC

- 공용(public) 클라우드 환경에서 개인식별정보(PII, Personally Identifiable Information) 보호를 위한 실행지침

<EMR 인증심사 유형별 적용사항>

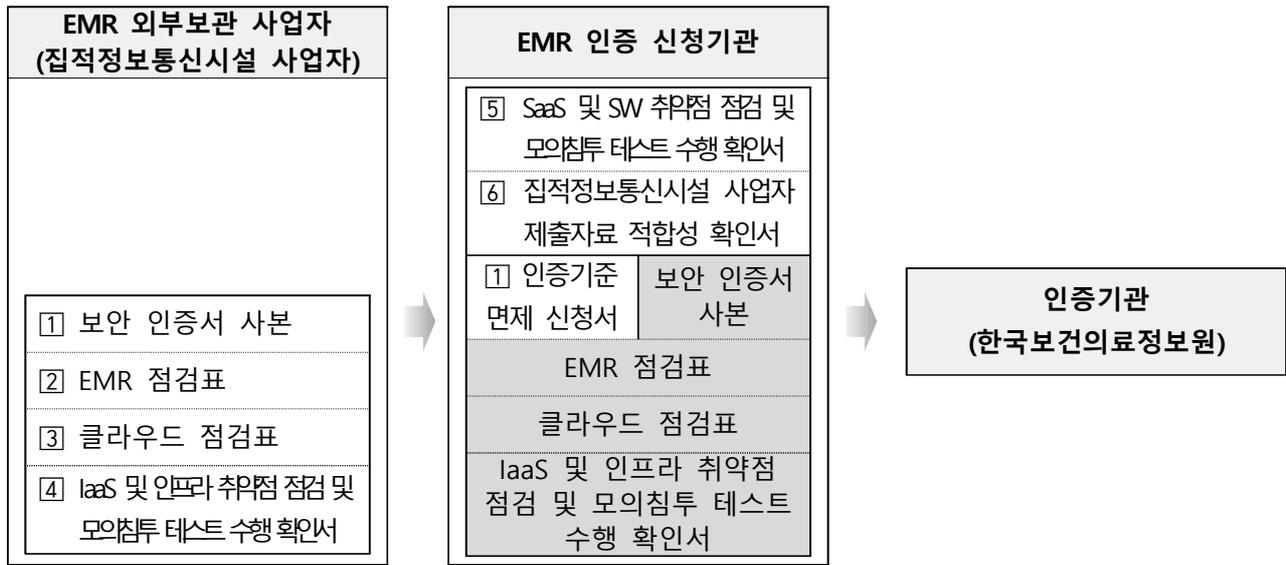
구 분	외부보관 인증기준(S014) 적용사항	제출자료 (공통제출 양식2-1~5,4,5,6)		
		제1호 (EMR 시설장비기준)	제2호 (클라우드정보보호기준)	
단순 외부보관 (그룹 I)	(I-1) ISMS-P 보안인증 보유	일부 적용*	-	양식1,2A
	(I-2) ISMS-P 보안인증 미보유	전부 적용	-	양식2B
클라우드 기반 외부보관 (그룹 II)	(II-1) ISMS-P, ISO 27017, ISO 27018 보안인증 전부 보유 또는 CSAP 인증* 보유 * 국가공공의료기관에 서비스 제공시	일부 적용*	면제	양식1,2A
	(II-2) ISMS-P 보안인증 보유	일부 적용*	일부 적용**	양식1,2A,3
	(II-3) ISMS-P, ISO 27017, ISO 27018 보안인증 미보유	전부 적용	전부 적용	양식2B,3

* 보안인증 통제항목과 중복되지 않는 부분을 심사(이중화된 네트워크의 구성, 인증된 정보보호제품 사용, 물리적 위치 국내 한정 등)

** ISMS-P와 중복되지 않는 부분을 심사

□ **제출 자료** ... 제출 양식 참조

<S014 인증신청 시 제출자료 및 취합 절차(예시)>



- **(보안인증서 사본)** 인증기준 면제신청서 및 보유하고 있는 인증서 사본(양식①)
- **(EMR 점검표)** EMR 시설장비기준 고시의 별표 전체 또는 일부* 항목별 점검표 및 증빙자료(양식②)
 - * 보안인증(ISMS-P, ISO 27017, 27018)의 통제항목과 중복되는 사항을 제외한 항목으로, 물리적 위치 국내 한정, 인증제품 사용, 이중화된 네트워크의 구성 등
- **(클라우드 점검표)** 클라우드컴퓨팅 서비스 정보보호 기준 고시의 관리적, 물리적, 기술적 조치 항목별 점검표 및 증빙자료(양식③)
 - 미적용 : 그룹 I (단순 외부보관)은 클라우드 점검표 미적용
 - 제출면제 : 그룹II(클라우드 기반 외부보관)는 ISMS-P(또는 ISMS), ISO 27017, ISO 27018 인증서 3종을 모두 보유한 경우 '클라우드 점검표' 제출 면제
- **(취약점 점검 및 모의침투 테스트 수행 확인서)**
 - EMR 외부보관 사업자 : IaaS / 인프라 취약점 점검 및 모의침투 테스트 확인서(양식④)
 - EMR 인증 신청기관 : SaaS / SW 취약점 점검 및 모의침투 테스트 확인서(양식⑤)
- **(EMR 외부보관 사업자 제출자료 적합성 확인서)** EMR 인증 신청기관은 EMR 외부보관 사업자 제출자료에 대한 적합성을 점검하고 확인서 제출(양식⑥)
- EMR 외부보관 사업자가 준비한 자료는 **EMR 인증 신청기관**을 경유하여 인증기관에 제출

Ⅲ. 인증심사 절차

□ 개요

- 보안인증*이 있는 경우 해당 보안인증의 통제항목과 중복되지 않는 부분 위주로 심사하고, 취약점 점검 등은 자체 또는 위탁 수행여부를 확인
 - * 단순 외부보관(그룹 I)은 ISMS-P(또는 ISMS) 인증서 1종,
클라우드 기반 외부보관(그룹 II)은 ISMS-P(또는 ISMS), ISO 27017, ISO 27018 인증서 3종 보유해야 함
- 보안인증이 없는 경우(일부만 있는 경우 포함) 항목별 점검표 및 증빙을 통해 직접심사하고 취약점 점검 등은 자체 또는 위탁 수행여부를 확인

□ 인증기관 역할

- EMR 인증신청 기관이 제출한 자료의 확인 및 심사
- 심사 내역 중의 미조치, 미흡 사항 등에 대해 인증 신청기관에 시정 요구하거나 평가 중단할 수 있음
- 또한, 인증 취득 후 제출한 서류가 거짓으로 판명될 경우 인증을 취소할 수 있음

□ 그룹별 제출 자료 세부 안내

① 단순 외부보관(그룹 I)

- (그룹 I -1) ISMS-P 보안인증 보유

1. 인증기준 면제신청서 및 ISMS-P 인증서 사본 1부...[양식1]

2. EMR 시설장비기준 고시에 따른 EMR 점검표 및 해당 증빙자료* ...[양식2A]

* EMR 점검표 및 증빙자료는 아래 4개 항목을 제출(필요 시 추가 항목 요구 가능)

- ① 항목 2.1. 정보시스템 네트워크의 물리적 또는 논리적 회선 분리 구성에 대한 증빙자료
· 둘 이상의 경로를 제공하는 내부망 및 라우터의 이중화를 구성하는 증빙자료
· 장애 대응 관련 증빙자료...[양식2-1]
- ② 항목 2.2. 집적정보통신시설의 네트워크 보안을 위한 인증된 정보보호시스템 도입 여부 증빙 자료...
[양식2-2, 2-3]
- ③ 항목 3.1. EMR시스템 보안을 위한 인증된 정보보호시스템 도입 여부 증빙 자료...[양식2-2, 2-3]
- ④ 항목 4.3. 집적정보통신시설 내에서 인증대상 EMR시스템의 물리적 위치가 국내 한정됨을 증빙하는 자료 등[양식2-4, 2-5]

3. IaaS 및 인프라 취약점 점검 및 모의침투 테스트 수행 확인서* ...[양식4]

* 최근 1년 이내 수행

4. 집적정보통신시설 사업자 제출자료 적합성 확인서 ...[양식6]

5. SaaS 및 SW 취약점 점검 및 모의침투 테스트 수행 확인서* ...[양식5]

* 최근 1년 이내 수행

○ (그룹 I -2) ISMS-P 보안인증 미보유

1. EMR 시설장비기준 고시에 따른 EMR 점검표 및 해당 증빙자료* ...[양식2B]

* EMR 점검표 모든 항목에 대해 점검 체크하고, 모든 항목에 대한 증빙자료 제출

2. IaaS 및 인프라 취약점 점검 및 모의침투 테스트 수행 확인서* ...[양식4]

* 최근 1년 이내 수행

3. 집적정보통신시설 사업자 제출자료 적합성 확인서 ...[양식6]

4. SaaS 및 SW 취약점 점검 및 모의침투 테스트 수행 확인서* ...[양식5]

* 최근 1년 이내 수행

② 클라우드 기반 외부보관(그룹Ⅱ)

○ (그룹Ⅱ-1) 보안인증 3종 전부 보유 또는 CSAP 보유

1. 인증기준 면제신청서 및 ISMS-P, ISO 27017, ISO 27018 인증서 사본 각 1부
또는 인증 신청기관이 국가·공공의료기관인 경우 CSAP 인증서 사본 1부...[양식1]

2. EMR 시설장비기준 고시에 따른 EMR 점검표 및 해당 증빙자료* ...[양식2A]

* EMR 점검표 및 증빙자료는 아래 4개 항목을 제출(필요 시 추가 항목 요구 가능)

- ① 항목 2.1. ·정보시스템 네트워크의 물리적 또는 논리적 회선 분리 구성에 대한 증빙자료
·둘 이상의 경로를 제공하는 내부망 및 라우터의 이중화를 구성하는 증빙자료
·장애 대응 관련 증빙자료...[양식2-1]
- ② 항목 2.2. 집적정보통신시설의 네트워크 보안을 위한 인증된 정보보호시스템 도입 여부 증빙 자료...
[양식2-2, 2-3]
- ③ 항목 3.1. EMR시스템 보안을 위한 인증된 정보보호시스템 도입 여부 증빙 자료...[양식2-2, 2-3]
- ④ 항목 4.3. 집적정보통신시설 내에서 인증대상 EMR시스템의 물리적 위치가 국내 한정됨을 증빙하는
자료 등[양식2-4, 2-5]

3. IaaS 및 인프라 취약점 점검 및 모의침투 테스트 수행 확인서* ...[양식4]

* 최근 1년 이내 수행

4. 집적정보통신시설 사업자 제출자료 적합성 확인서 ...[양식6]

5. SaaS 및 SW 취약점 점검 및 모의침투 테스트 수행 확인서* ...[양식5]

* 최근 1년 이내 수행

○ (그룹Ⅱ-2) ISMS-P 보유(ISO 27017, ISO 27018 미보유)

1. 인증기준 면제신청서 및 ISMS-P 보안인증서 사본 1부 ...[양식1]

2. EMR 시설장비기준 고시에 따른 EMR 점검표 및 해당 증빙자료* ...[양식2A]

* EMR 점검표 및 증빙자료는 아래 4개 항목을 제출(필요 시 추가 항목 요구 가능)

- ① 항목 2.1. ·정보시스템 네트워크의 물리적 또는 논리적 회선 분리 구성에 대한 증빙자료
·둘 이상의 경로를 제공하는 내부망 및 라우터의 이중화를 구성하는 증빙자료
·장애 대응 관련 증빙자료...[양식2-1]
- ② 항목 2.2. 집적정보통신시설의 네트워크 보안을 위한 인증된 정보보호시스템 도입 여부 증빙 자료...
[양식2-2, 2-3]
- ③ 항목 3.1. EMR시스템 보안을 위한 인증된 정보보호시스템 도입 여부 증빙 자료...[양식2-2, 2-3]
- ④ 항목 4.3. 집적정보통신시설 내에서 인증대상 EMR시스템의 물리적 위치가 국내 한정됨을 증빙하는
자료 등[양식2-4, 2-5]

3. 클라우드 점검표 및 해당 증빙자료* ...[양식3]

* S014 제2호에 따른 심사를 위해 일부 보유한 보안인증서의 통제항목에 포함되지 않는 부분을 심사하며, 클라우드 점검표를 작성할 대상 항목은 인증기관이 별도 고지(고지받은 후 점검표 및 증빙자료 작성 제출)

4. IaaS 및 인프라 취약점 점검 및 모의침투 테스트 수행 확인서* ...[양식4]

* 최근 1년 이내 수행

5. 집적정보통신시설 사업자 제출자료 적합성 확인서 ...[양식6]

6. SaaS 및 SW 취약점 점검 및 모의침투 테스트 수행 확인서* ...[양식5]

* 최근 1년 이내 수행

○ (그룹 II-3) 보안인증 전체 미보유

1. EMR 시설장비기준 고시에 따른 EMR 점검표 및 해당 증빙자료* ...[양식2B]

* EMR 점검표 모든 항목에 대해 점검 체크하고, 모든 항목에 대한 증빙자료 제출

2. 클라우드 점검표 및 해당 증빙자료 ...[양식3]

3. IaaS 및 인프라 취약점 점검 및 모의침투 테스트 수행 확인서* ...[양식4]

* 최근 1년 이내 수행

4. 집적정보통신시설 사업자 제출자료 적합성 확인서 ...[양식6]

5. SaaS 및 SW 취약점 점검 및 모의침투 테스트 수행 확인서* ...[양식5]

* 최근 1년 이내 수행

◆ 보안인증 미보유(일부 보유)시 직접심사 방안

- (개요) 실비 상당 수수료 징수하고, 전문기관 위탁, 또는 ISMS 인증 심사원 등 외부전문가로 별도 심사팀 구성하여 수행
- (직접심사 대상) 보안인증 일부 보유 또는 미보유
- (기관별 제출자료)

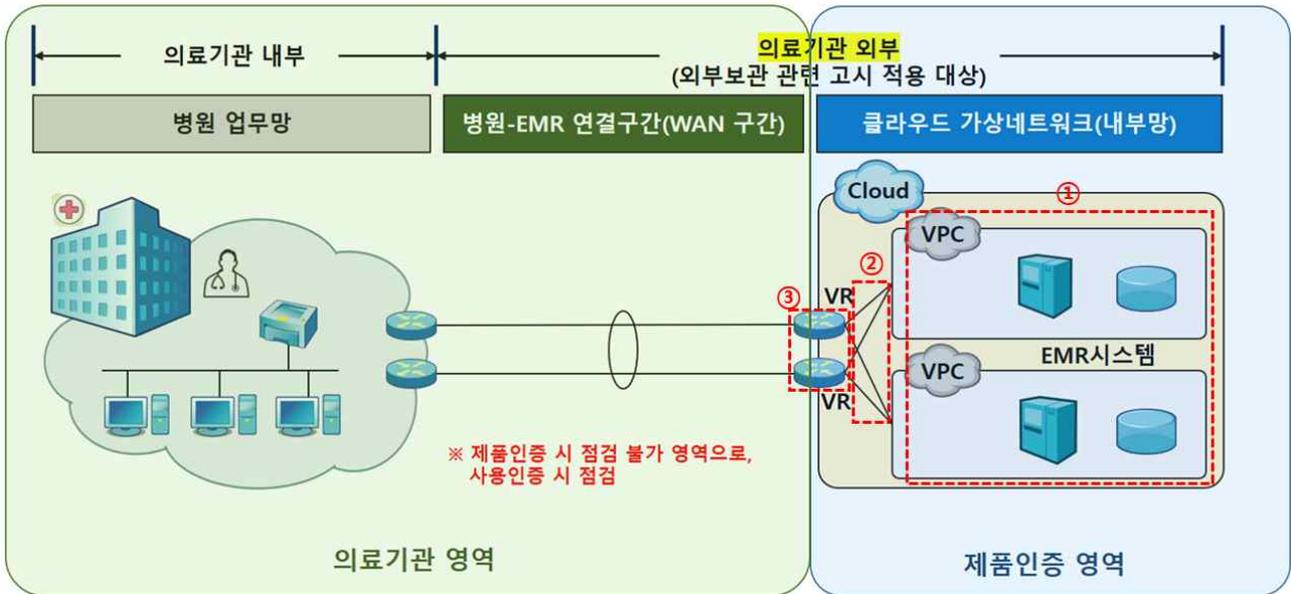
구분	EMR 외부보관 사업자			EMR 인증 신청기관	
제출자료	EMR 점검표	클라우드 점검표	IaaS(인프라) 취약점 점검 및 모의침투 테스트 수행 확인서	EMR 외부보관 사업자 제출자료 적합성 확인서	SaaS(SW) 취약점 점검 및 모의침투 테스트 수행 확인서

- (심사내용) 전자의무기록 시설장비 기준고시 준수 여부 확인, 클라우드컴퓨팅 서비스 정보보호 기준고시 제3조(관리적 보호조치), 제4조(물리적 보호조치), 제5조(기술적 보호조치) 준수 여부 확인, IaaS 및 SaaS 취약점 점검 및 모의 침투 테스트 등

□ 인증기준 S014 제1호 일부심사 점검 항목 안내

① 이중화된 네트워크의 구성

- 중단없이 서비스가 가능하도록 네트워크 각 구간별(회선, 내부망 구성 경로, 라우터, 장애발생 대책 등 4개항목) 이중화 여부를 심사 ... [양식2-1]



고시규정		점검내용
이중화된 네트워크의 구성	둘 이상 회선분리 (물리적, 논리적 포함)	①가상사설클라우드(VPC) 등고가용성(HA) 구성을 위한 네트워크 구간 이중화 구성 ※ 병원-EMR 연결구간(WAN 구간)은 사용인증 시 점검
	둘 이상 경로 제공 내부망	②클라우드 내부 네트워크 경로 이중화 구성
	라우터 이중화	③물리적 라우터 또는 가상라우터(VR) 이중화 구성
	장애 발생 시 대책	HA 설정 및 장애대응 절차 등

② 인증된 정보보호·보안 제품의 사용

- 정보보호·보안기능에 해당하는 제품 도입 시 CC인증 등 국정원 요건 적합 여부 등 심사 ... [양식2-2,3]

고시규정			점검내용	
			정보보호 제품	비고
네트워크 보안* 에 관한 시설과 장비	네트워크 보호시스템 운영	침입차단시스템, 침입탐지시스템 등 인증된 정보보호시스템을 운영 하여 내.외부 네트워크를 보호하여야 한다.	침입차단시스템	CC인증 또는 보안기능 확인서 등
			침입탐지(방지)시스템	
			가상사설망(VPN) ※ 전용선 또는 안전한 접속 수단으로 대체 가능	
전자의무 기록시스템 보안** 에 관한 시설과 장비	인증된 정보보호·보안제품의 사용	국가정보원장 이 인증 필요성을 인정하는 정보보호시스템의 경우 CC 인증 제품 등 도입요건 을 만족한 제품을 사용하여야 한다.	DB암호화제품 (CC인증 또는 보안기능 확인서 + 검증필 암호모듈 탑재)	국가정보원 보안적합성 검증 사전인증 요건
			DB접근통제제품 (CC인증 또는 보안기능 확인서)	
			안티바이러스제품 (CC인증·성능평가·보안기능 확인서 중 어느 하나)	

* (네트워크 보안) 전자의무기록의 관리보존에 필요한 시설과 장비에 관한 기준 제6조의 개인정보보호법 안전성 확보조치 여부 + 점검내용의 인증된 네트워크 보호시스템 운영 여부

** (전자의무기록시스템 보안) 전자의무기록의 관리보존에 필요한 시설과 장비에 관한 기준 제6조의 개인정보보호법 안전성 확보조치 여부 + 관련제품 도입 시 국가정보원 도입요건 만족 여부

③ 물리적 위치 한정

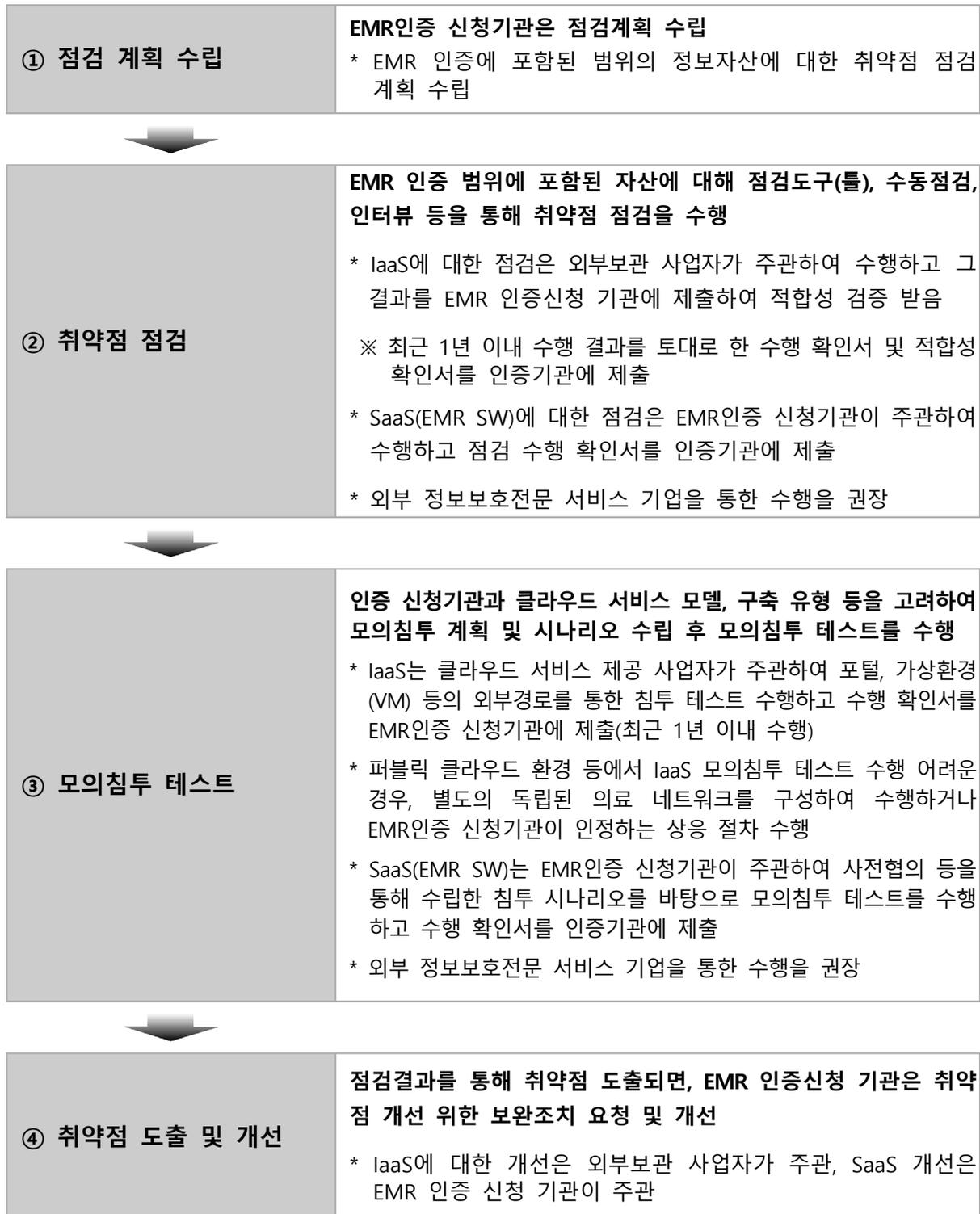
- 클라우드 서비스 계약서(SLA) 및 관리콘솔에 명기된 위치(리전) 확인하고, 계약된 서비스별 리전의 국내 한정 확인 양식을 추가로 제출 ... [양식2-4,5]

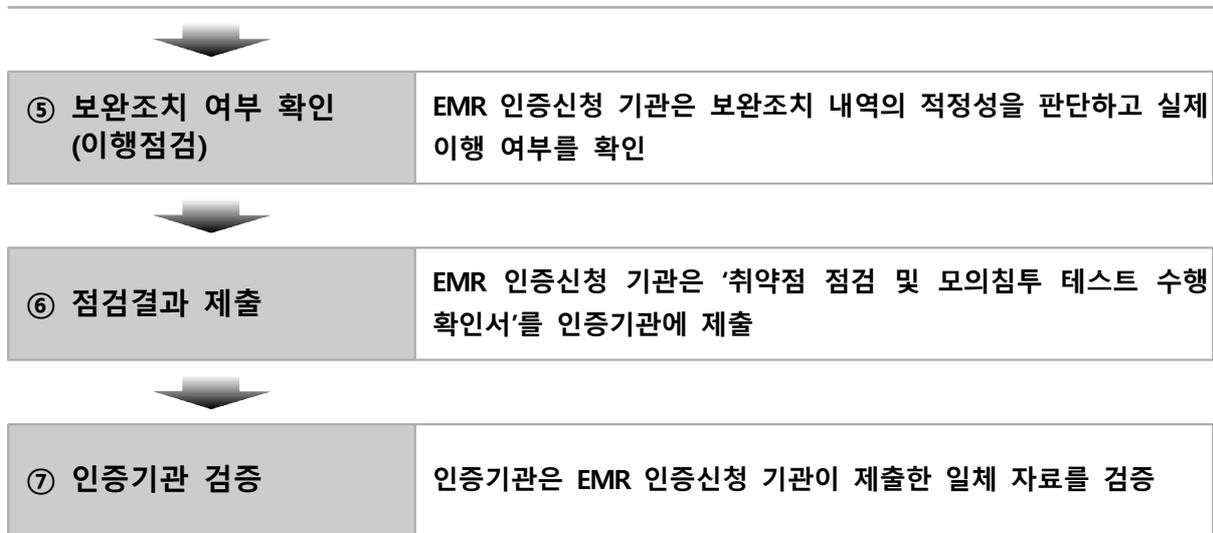
고시 규정			점검내용
전자의무기록 보존 장소에 대한 물리적 접근방지 시설과 장비	물리적 위치의 한정	- 전자의무기록 시스템 및 그 백업장비의 물리적 위치는 국내로 한정 한다.	- 서비스 계약서 및 관리 콘솔 리전 등 - 계약된 서비스별 리전 국내 한정 확인 양식

□ 보안취약점 점검 및 모의침투 테스트 점검

- EMR 인증 신청기관이 자체 점검계획을 수립하여 집적정보통신 시설 및 클라우드 EMR 서비스에 대한 보안취약점 등 점검 수행 확인서를 인증기관에 제출

<취약점 점검 및 모의침투 테스트 진행 절차>





◆ **취약점 점검 및 모의침투 테스트 도입 취지**

▶ (취약점 점검) 클라우드 서비스 제공 사업자 등은 관련 법령*에 따라 주기적으로 취약점을 점검 및 보완하여야 함

* 클라우드컴퓨팅서비스 정보보호에 관한 기준 고시 [별표1] 관리적 보호조치 3.3.2(취약점 점검)
취약점 점검 정책에 따라 주기적으로 기술적 취약점(예: 유·무선 네트워크, 운영체제 및 인프라, 응용 프로그램 취약점 등)을 점검하고 보완하여야 한다.

▶ (모의침투 테스트) 전자의무기록 외부보관 서비스는 의료기관 외부에 민감한 의료정보를 관리하며 클라우드 서비스는 자원의 가상화 및 공유를 기반으로 하여 정보보안에 더욱 취약함

- 따라서, EMR 인증 심사 시 보안사고에 실질적 대응이 가능하고 가장 효율적인 보안성 평가 방법인 모의침투 테스트 수행 여부를 확인하고자 함

* 한국인터넷진흥원의 CSAP 인증에서도 활용

인증기준 면제 신청서

신청기관				
신청종류	[]최초심사	[]갱신심사	[]변경심사	
신청구분	[]제품인증	[]사용인증	[]제품, 사용인증	
인증유형	[]유형1			
	[]유형2			
	[]유형3			
면제기준 (해당항목에 √ 표시)	[]기능성			
	[]상호운용성	진료정보교류사업 요구기능 충족 면제기준 : I001~I010(총 10개)		
	[]보안성 (S001~S013)	[]	정보보호관리체계 인증(ISMS) 면제기준 : S001~S008, S010~S011, S013(총 11개)	
		[]	정보보호 및 개인정보보호 관리체계 인증(ISMS-P) 면제기준 : S001~S011, S013(총 12개)	
		[]	청구소프트웨어 보안기능 검사인증 면제기준 : S001~S007, S010~S011(총 9개) ※ 청구소프트웨어 보안기능 검사 인증서만 제출한 기관의 경우, 보안성 영역 인증기준(S001~S013)에 대해 현장심사를 실시할 수 있습니다.	
	[]보안성 (S014)	[]	[]ISMS-P(또는 ISMS) []ISO 클라우드 보안인증(ISO 27017) []ISO 클라우드 개인정보보호 인증(ISO 27018) 면제기준 : S014(총 1개) ※ 인증기준 S014 관련 자료는 집적정보통신시설 사업자가 준비하고 EMR 인증 신청기관을 경유하여 제출	
[]		클라우드 보안인증(CSAP) - IaaS 면제기준 : S014(총 1개) ※ 인증기준 S014 관련 자료는 집적정보통신시설 사업자가 준비하고 EMR 인증 신청기관을 경유하여 제출		
관련문서 또는 시스템	※ 관련 문서* 또는 시스템이 있는 경우 작성 * (예시) ISMS 인증서 사본 등			

위와 같이 인증심사 일부 면제를 위한 신청서를 제출합니다.

년 월 일

전자의무기록 인증신청 기관장(대표자)

(서명 또는 인)

재단법인 한국보건 의료정보원 귀중

※ 인증심사 일부 면제 대상임을 확인할 수 있는 증빙자료를 반드시 제출

□ EMR 점검표

전자의무기록의 관리 보존에 필요한 시설과 장비에 관한 기준 내 [별표] '의료기관 외의 장소에 전자의무기록 보관시 필요한 추가적인 조치' 사항 중 4개 항목에 대한 증빙자료 제출 (필요 시 그 외 항목에 대한 증빙 요구 가능)

의료기관 외의 장소에 전자의무기록 보관시 필요한 추가적인 조치(일부)

* 점검 항목표 (Y: 만족함, P: 부분적으로 만족함, N: 만족하지 않음, N/A: 해당 없음)

분류	항목	점검내용	Y	P	N	N/A
2.네트워크 보안에 관한 시설과 장비	2.1. 이중화된 네트워크의 구성	물리적 또는 그에 준하는(논리적 포함) 둘 이상의 회선으로 분리되어 있는가?				
		둘 이상의 경로를 제공하는 내부망을 구성하고 있는가?				
		라우터의 이중화 구성하고 있는가?				
		장애발생 시에도 지속적인 서비스 제공을 위한 대책을 수립하고 있는가?				
	2.2. 네트워크 보호시스템 운영	인증된 정보보호시스템을 운영하여 내.외부 네트워크를 보호하고 있는가?				
3.전자의무기록 시스템 보안에 관한 시설과 장비	3.1. 인증된 정보보호·보안제품의 사용	정보보호시스템에 대한 CC 인증 제품 등 도입 요건을 만족한 제품을 사용하고 있는가?				
4.전자의무기록 보존 장소에 대한 물리적 접근방지 시설과 장비	4.3. 물리적 위치의 한정	전자의무기록 시스템 및 그 백업장비의 물리적 위치는 국내인가?				

□ EMR 관리 · 보존 시설장비 기준 고시 증적자료 목록 (예시)

분류	항목	점검내용	증적 자료(예시)
2. 네트워크 보안에 관한 시설과 장비	2.1	물리적 또는 그에 준하는(논리적 포함) 둘 이상의 회선으로 분리되어 있는가?	<ul style="list-style-type: none"> 서비스 계약서(SLA) 정보시스템 및 네트워크 구성도 성능 및 네트워크 모니터링 절차 장애대응 절차
		둘 이상의 경로를 제공하는 내부망을 구성하고 있는가?	<ul style="list-style-type: none"> 정보시스템 및 네트워크 구성도 성능 및 네트워크 모니터링 절차 장애대응 절차
		라우터의 이중화 구성하고 있는가?	<ul style="list-style-type: none"> 정보시스템 및 네트워크 구성도 성능 및 네트워크 모니터링 절차 장애대응 절차
		장애발생 시에도 지속적인 서비스 제공을 위한 대책을 수립하고 있는가?	<ul style="list-style-type: none"> 서비스 계약서(SLA) 정보시스템 및 네트워크 구성도 성능 및 네트워크 모니터링 절차 장애대응 절차 장애조치보고서
	2.2	인증된 정보보호시스템을 운영하여 내.외부 네트워크를 보호하고 있는가?	<ul style="list-style-type: none"> 정보시스템 인수 기준 및 절차 정보시스템 및 네트워크 구성도 정보시스템 운영 절차 보안시스템 구성 보안시스템 운영 절차 방화벽 정책
3. 전자의무기록 시스템 보안에 관한 시설과 장비	3.1	CC 인증 제품 등 도입요건을 만족한 제품을 사용하고 있는가?	<ul style="list-style-type: none"> 인증 받은 제품의 인증서 등 증적 서류 정보시스템 인수 기준 및 절차 정보시스템 및 네트워크 구성도 정보시스템 운영 절차 보안시스템 구성 보안시스템 운영 절차 방화벽 정책
4. 전자의무기록 보존장소에 대한 물리적 접근방지 시설과 장비	4.3	전자의무기록 시스템 및 그 백업장비의 물리적 위치는 국내인가?	<ul style="list-style-type: none"> 서비스 계약서(SLA) 국내설비 목록 리스트 국내 물리적 위치 확인서 사용자 데이터 보호 정책 문서 데이터 해외 이전불가 기술적 보증 증빙 자료

□ **EMR 점검표**

전자의무기록의 관리 보존에 필요한 시설과 장비에 관한 기준 내 [별표] '의료기관 외의 장소에 전자의무기록 보관시 필요한 추가적인 조치' 사항 중 전체 항목에 대한 증빙자료 제출

※ 3-1. CC 인증제품 등 도입요건 만족의 경우” P(partial)도 가능하나, 다른 항목은 모두 Y 또는 N/A이어야 함

* 점검 항목표 (Y: 만족함, P: 부분적으로 만족함, N: 만족하지 않음, N/A: 해당 없음)

분류	항목	점검내용	Y	P	N	N/A
1.전자의무기록의 백업저장 장비	1.1	전자의무기록 등의 정보를 백업할 경우, 전자의무기록 시스템을 중단하지 않고 백업하는가?				
	1.2	백업된 데이터를 신속하게 복구할 수 있는 시스템이 존재하는 가?				
		백업된 데이터를 복구하는 관리 절차가 존재하는가?				
	1.3	백업된 데이터의 위.변조 및 비정상적으로 삭제되지 않도록 전자인증 처리 등 보호조치가 이루어지는가?				
1.4	백업 설비와 전자의무기록 시스템 설비가 물리적으로 분리되어 있는가?					
2. 네트워크 보안에 관한 시설과 장비	2.1	물리적 또는 그에 준하는(논리적 포함) 둘 이상의 회선으로 분리되어 있는가?				
		둘 이상의 경로를 제공하는 내부망을 구성하고 있는가?				
		라우터의 이중화 구성하고 있는가?				
	2.2	장애발생 시에도 지속적인 서비스 제공을 위한 대책을 수립하고 있는가?				
2.2	인증된 정보보호시스템을 운영하여 내.외부 네트워크를 보호하고 있는가?					
3.전자의무기록 시스템 보안에 관한 시설과 장비	3.1	정보보호시스템에 대한 CC 인증 제품 등 도입요건을 만족한 제품을 사용하고 있는가?				
	3.2	데이터 및 소프트웨어의 무결성 보장을 위한 보호조치가 이루어지는가?				
		중요정보에 대해 암호화하고 있는가?				
	3.3	전자의무기록시스템의 기술적 보호조치를 위한 시스템을 구성하고 있는가?				
3.4	데이터 무결성을 보장하기 위한 관리 방안을 수립하고 있는가?					
	데이터 훼손.유출 시 즉시 의료기관에 보고할 수 있는 프로세스가 수립되어 있는가?					
4.전자의무기록 보존장소에 대한 물리	4.1	전자의무기록 시스템이 위치한 공간에 출입통제를 하고 있는가?				
		보호구역내에서의 작업 절차를 수립하고 작업에 대한 기록을 주기적으로 검토하는가?				

적 접근방지 시설과 장비	4.2	출입통제 및 이력관리 시스템이 갖추어져 있는가?				
		출입통제시스템에 대한 접근통제 및 암호화 기능이 갖추어져 있는가?				
	4.3	전자의무기록 시스템 및 그 백업장비의 물리적 위치는 국내인가?				
5.전자의무기록 시스템을 실시간으로 점검할 수 있는 시설과 장비	5.1	전자의무기록시스템의 동작여부와 상태를 점검할 수 있는 장비가 존재하는가?				
		전자의무기록시스템에 이상 발생 시 이를 기록하고 관리자에게 보고하는가?				
	5.2	네트워크 장비에서 발생하는 트래픽을 기록하고 네트워크의 상태를 점검하는가?				
6.예비장비	6.1	전자의무기록 시스템의 장애를 대비하여 보조시스템을 운영하는가?				
7. 폐쇄 회로 텔레비전 등의 감시장비	7.1	전자의무기록 관리시설은 사각지대 없이 24시간 CCTV 실시간 촬영을 하고 있는가?				
		CCTV 시스템에 대한 접근통제 정책이 존재하는가?				
	7.2	전자의무기록 시스템과 관련된 구역에서 침입감지시스템을 운영하고 있는가?				
		침입감지시 관리자에게 신속히 알리는 기능이 존재하는가?				
	7.3	출입통제장치로부터 출입현황정보를 확인할 수 있는 장비가 존재하는가?				
		출입현황정보는 자동으로 저장하고 지정된 관리자만 기록에 접근할 수 있는가?				
8. 재해예방 시설	8.1	화재경보장치가 존재하며, 정상작동하는가?				
	8.2	소화장치가 존재하는가?				
		소화장치를 주기적으로 관리하는가? 소화기 점검표 등 확인				
	8.3	수재 예방설비가 존재하는가?				
		전자의무기록을 위한 시스템 및 네트워크 설비에 전원을 공급하는 콘센트와 해당 장비는 바닥으로부터 이격하고 있는가?				
	8.4	정전발생시 지속적인 업무의 수행이 가능하도록 추가연료 보충 없이 2시간 이상 발전할 수 있는 자가발전설비가 존재하는가?				
		30분이상 전원을 공급해 줄 수 있는 무정전 전원공급장치(UPS) 설비가 존재하는가?				
	8.5	전산실은 항상 항온항습기를 통하여 일정한 온도와 습도를 유지하는가? - 온도: 16°C 이상 28°C 이하 - 습도: 40% 이상 70% 이하				
		항온항습기를 주기적으로 점검하는가? - 온습도 기록계 확인				

□ EMR 관리 · 보존 시설장비 기준 고시 증적자료 목록 (예시)

분류	항목	점검내용	증적 자료(예시)
1. 전자의무기록의 백업 저장 장비	1.1	전자의무기록 등의 정보를 백업할 경우, 전자의무기록 시스템을 중단하지 않고 백업하는가?	<ul style="list-style-type: none"> ·정보시스템 구성도 ·백업 관리 절차 ·백업 테스트 결과
	1.2	백업된 데이터를 신속하게 복구할 수 있는 시스템이 존재하는 가?	<ul style="list-style-type: none"> ·정보시스템 구성도 ·복구 관리 절차 ·복구 테스트 결과
		백업된 데이터를 복구하는 관리 절차가 존재하는 가?	<ul style="list-style-type: none"> ·정보시스템 및 네트워크 구성도 ·복구 관리 절차 ·복구 테스트 결과
	1.3	백업된 데이터의 위.변조 및 비정상적으로 삭제되지 않도록 전자인증 처리 등 보호조치가 이루어지는 가?	<ul style="list-style-type: none"> ·정보시스템 및 네트워크 구성도 ·백업 및 복구 관리 절차 ·백업 및 복구 테스트 결과 ·본인인증 및 부인방지방안 절차
	1.4	백업 설비와 전자의무기록 시스템 설비가 물리적으로 분리되어 있는가?	<ul style="list-style-type: none"> ·정보시스템 및 네트워크 구성도 ·백업 및 복구 절차 ·백업 및 복구 테스트 결과 ·소산백업 현황
2. 네트워크 보안에 관한 시설과 장비	2.1	물리적 또는 그에 준하는(논리적 포함) 둘 이상의 회선으로 분리되어 있는가?	<ul style="list-style-type: none"> ·서비스 계약서(SLA) ·정보시스템 및 네트워크 구성도 ·성능 및 네트워크 모니터링 절차 ·장애대응 절차
		둘 이상의 경로를 제공하는 내부망을 구성하고 있는가?	<ul style="list-style-type: none"> ·정보시스템 및 네트워크 구성도 ·성능 및 네트워크 모니터링 절차 ·장애대응 절차
	2.1	라우터의 이중화 구성하고 있는가?	<ul style="list-style-type: none"> ·정보시스템 및 네트워크 구성도 ·성능 및 네트워크 모니터링 절차 ·장애대응 절차
		장애발생 시에도 지속적인 서비스 제공을 위한 대책을 수립하고 있는가?	<ul style="list-style-type: none"> ·서비스 계약서(SLA) ·정보시스템 및 네트워크 구성도 ·성능 및 네트워크 모니터링 절차 ·장애대응 절차 ·장애조치보고서
	2.2	인증된 정보보호시스템을 운영하여 내.외부 네트워크를 보호하고 있는가?	<ul style="list-style-type: none"> ·정보시스템 인수 기준 및 절차 ·정보시스템 및 네트워크 구성도 ·정보시스템 운영 절차 ·보안시스템 구성 ·보안시스템 운영 절차 ·방화벽 정책
3. 전자의무기록 시스템 보안에 관한 시설과 장비	3.1	CC 인증 제품 등 도입요건을 만족한 제품을 사용하고 있는가?	<ul style="list-style-type: none"> ·인증 받은 제품의 인증서 등 증적 서류 ·정보시스템 인수 기준 및 절차 ·정보시스템 및 네트워크 구성도 ·정보시스템 운영 절차 ·보안시스템 구성 ·보안시스템 운영 절차 ·방화벽 정책
	3.2	데이터 및 소프트웨어의 무결성 보장을 위한 보호조치가 이루어지는가?	<ul style="list-style-type: none"> ·데이터 무결성 조치 방안 ·정보시스템 자산목록 ·응용프로그램 접근권한 분류 체계 ·DB 접근제어 정책

		중요정보에 대해 암호화하고 있는가?	<ul style="list-style-type: none"> •로그관리 절차 •암호통제 정책 •암호화 적용현황(저장 및 전송 시) •암호화 솔루션 관리 화면
	3.3	전자의무기록시스템의 기술적 보호조치를 위한 시스템을 구성하고 있는가?	<ul style="list-style-type: none"> •외부자 및 수탁자 보안점검 결과 •외부자 및 수탁자 교육 내역 •개인정보 위탁 계약서 •정보시스템 및 네트워크 구성도 •서버 보안 설정 •정보시스템 자산 목록 •응용프로그램 접근권한 분류 체계 •DB 접근 제어 정책 •VPN 접근제어 정책 •주요 시스템 시간 동기화 증적
	3.4	데이터 무결성을 보장하기 위한 관리 방안을 수립하고 있는가?	<ul style="list-style-type: none"> •데이터 무결성 조치 방안 •정보시스템 자산목록 •응용프로그램 접근권한 분류 체계 •정보시스템 및 네트워크 구성도 •DB 접근제어 정책 •로그관리 절차
		데이터 훼손·유출 시 즉시 의료기관에 보고할 수 있는 프로세스가 수립되어 있는가?	<ul style="list-style-type: none"> •침해사고 대응 지침·절차·매뉴얼 •침해사고 대응 조직도 및 비상연락망
4. 전자의무기록 보존장소에 대한 물리적 접근방지 시설과 장비	4.1	전자의무기록 시스템이 위치한 공간에 출입통제를 하고 있는가?	<ul style="list-style-type: none"> •물리적 보안 지침(보호구역 지정 기준) •보호구역 지정 현황 •보호구역 표시 •보호구역 별 보호대책 현황
		보호구역내에서의 작업 절차를 수립하고 작업에 대한 기록을 주기적으로 검토하는가?	<ul style="list-style-type: none"> •물리적 보안 지침(보호구역 지정 기준) •보호구역 지정 현황 •보호구역 별 보호대책 현황
	4.2	출입통제 및 이력관리 시스템이 갖추어져 있는가?	<ul style="list-style-type: none"> •출입 관리대장 및 출입로그 •출입 등록 신청서 및 승인내역 •출입기록 검토서 •출입통제시스템 관리화면
		출입통제시스템에 대한 접근통제 및 암호화 기능이 갖추어져 있는가?	<ul style="list-style-type: none"> •출입 관리대장 및 출입로그 •출입 등록 신청서 및 승인 내역 •출입기록 검토서 •출입통제시스템 관리화면
	4.3	전자의무기록 시스템 및 그 백업장비의 물리적 위치는 국내인가?	<ul style="list-style-type: none"> •서비스 계약서(SLA) •국내설비 목록 리스트 •국내 물리적 위치 확인서 •사용자 데이터 보호 정책 문서 •데이터 해외 이전불가 기술적 보증 증빙 자료
5. 전자의무기록시스템을 실시간으로 점검할 수 있는 시설과 장비	5.1	전자의무기록시스템의 동작여부와 상태를 점검할 수 있는 장비가 존재하는가?	<ul style="list-style-type: none"> •성능 및 용량 모니터링 절차 •성능 및 용량 모니터링 증적 (내부 보고 결과 등) •장애대응 절차 •장애조치보고서
		전자의무기록시스템에 이상 발생 시 이를 기록하고 관리자에게 보고하는가?	<ul style="list-style-type: none"> •성능 및 용량 모니터링 절차 •성능 및 용량 모니터링 증적(내부 보고 결과 등)

			<ul style="list-style-type: none"> •장애대응 절차 •장애조치보고서
	5.2	네트워크 장비에서 발생하는 트래픽을 기록하고 네트워크의 상태를 점검하는가?	<ul style="list-style-type: none"> •이상행위 분석 및 모니터링 현황 •이상행위 발견 시 대응 증적
6.예비장비	6.1	전자의무기록 시스템의 장애를 대비하여 보조시스템을 운영하는가?	<ul style="list-style-type: none"> •IT 재해 복구, 지침 •IT 재해 복구, 계획 •비상연락망
7.폐쇄회로 텔레비전 등의 감시장비	7.1	전자의무기록 관리시설은 사각지대 없이 24시간 CCTV 실시간 촬영을 하고 있는가?	<ul style="list-style-type: none"> •영상정보처리기기 운영 현황 •영상정보처리기기 안내판 •영상정보처리기기 운영, 관리방침 •영상정보처리기기 관리화면(계정/권한 내역, 영상정보 보존기간 등)
		CCTV 시스템에 대한 접근통제 정책이 존재하는가?	<ul style="list-style-type: none"> •영상정보처리기기 운영 현황 •영상정보처리기기 운영, 관리방침 •영상정보처리기기 관리화면(계정/권한 내역, 영상정보 보존기간 등)
	7.2	전자의무기록 시스템과 관련된 구역에서 침입감지시스템을 운영하고 있는가?	<ul style="list-style-type: none"> •물리적 보안 지침(보호구역 지정 기준) •보호구역 지정 현황 •보호구역 표시 •보호구역 별 보호대책 현황
		침입감지시 관리자에게 신속히 알리는 기능이 존재하는가?	<ul style="list-style-type: none"> •출입 관리대장 및 출입 로그 •출입 등록 신청서 및 승인 내역 •출입기록 검토서 •출입통제시스템 관리화면(출입자 등록 현황 등)
	7.3	출입통제장치로부터 출입현황정보를 확인할 수 있는 장비가 존재하는가?	<ul style="list-style-type: none"> •출입 관리대장 및 출입 로그 •출입통제시스템 관리화면(출입자 등록 현황 등)
		출입현황정보는 자동으로 저장하고 지정된 관리자만 기록에 접근할 수 있는가?	<ul style="list-style-type: none"> •출입 관리대장 및 출입 로그 •출입 등록 신청서 및 승인 내역 •출입기록 검토서 •출입통제시스템 관리화면(출입자 등록 현황 등)
8. 재해예방 시설	8.1	화재경보장치가 존재하며, 정상작동하는가?	<ul style="list-style-type: none"> •물리적 보안 지침(보호설비 관련) •전산실 설비 현황 및 점검표 •IDC 위탁운영 계약서, SLA 등
		소화장치가 존재하는가?	
	8.2	소화장치를 주기적으로 관리하는가? 소화기 점검표 등 확인	
	8.3	수재 예방설비가 존재하는가?	
		전자의무기록을 위한 시스템 및 네트워크 설비에 전원을 공급하는 콘센트와 해당 장비는 바닥으로부터 이격하고 있는가?	
	8.4	정전발생시 지속적인 업무의 수행이 가능하도록 추가연료 보충 없이 2시간 이상 발전할 수 있는 자가발전설비가 존재하는가?	
30분이상 전원을 공급해 줄 수 있는 무정전 전원공급장치(UPS) 설비가 존재하는가?			
8.5	전산실은 항상 항온항습기를 통하여 일정한 온도와 습도를 유지하는가? - 온도: 16°C 이상 28°C 이하 - 습도: 40% 이상 70% 이하		
	항온항습기를 주기적으로 점검하는가? - 온습도 기록계 확인		

양식2-1

이중화된 네트워크의 구성 증빙자료 제출 양식

(1) 증빙자료 제출 양식 : 2.1 항목

항목	분류	증빙자료	
2.1	이중화된 네트워크의 구성	<input type="checkbox"/> 점검항목 물리적 또는 그에 준하는(논리적 포함) 둘 이상의 회선으로 분리되어 있는가? 둘 이상의 경로를 제공하는 내부망 및 라우터의 이중화를 구성하고 있으며, 장애 발생 시 지속적인 서비스 제공을 위한 대책을 수립하고 있는가?	
		<input type="checkbox"/> 점검 세부내용 의료데이터 전송을 위한 이중화된 네트워크를 구성하여야 하며 아래 조건을 충족하여야 한다. · 물리적 또는 그에 준하는 (논리적 포함) 둘 이상의 회선 분리 · 둘 이상의 경로를 제공하는 내부망 구성 여부 · 라우터의 이중화 구성 여부 · 장애 발생 시 지속적인 서비스 제공을 위한 대책 여부	
		<input type="checkbox"/> 증빙자료 설명 · 정보시스템 네트워크의 물리적 또는 논리적 회선 분리 구성에 대한 증빙자료 · 둘 이상의 경로를 제공하는 내부망 및 라우터의 이중화를 구성하는 증빙자료 · 장애 대응 관련 증빙자료	<input type="checkbox"/> 증빙자료 예시 ● 서비스 계약서 (SLA) ● 정보시스템 및 네트워크 구성도 ● 성능 및 네트워크 모니터링 절차 ● 장애대응 절차 ● 병원 연결구간 이중화 구성 방안(계획)
		<input type="checkbox"/> 증빙자료 1. 물리적 또는 그에 준하는 (논리적 포함) 둘 이상의 회선 분리 2. 둘 이상의 경로를 제공하는 내부망 구성 여부 3. 라우터의 이중화 구성 여부 4. 장애 발생 시 지속적인 서비스 제공을 위한 대책 여부 <p style="text-align: center;">1~4 각 증빙자료 붙임</p>	

양식2-2

인증 정보보호제품 도입 점검표

(2) 증빙자료 제출 양식 : 2.2 및 3.1 항목

인증 정보보호제품 도입 점검표

집적정보통신시설	사업자명		
	구분	[]	집적정보통신시설
		[]	클라우드컴퓨팅기술 기반 집적정보통신시설

아래 표에 도입 정보보호제품 및 인증 여부를 점검하여 표시

- ① 도입 정보보호제품 목록은 국가정보원 보안적합성 검증의 제품 유형 목록 참고
- ② 네트워크 보안(의료법 시행규칙 제16조제1항제4호) 관련 인증은 국내외 CC인증, 성능평가 확인서, 보안기능 확인서 등을 포함
- ③ 전자의무기록시스템 보안(의료법 시행규칙 제16조제1항제5호) 관련 인증은 국가정보원 보안적합성 검증의 도입 요건 참고

	도입 정보보호제품	인증 여부		기타
		예	아니오	
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				

상기와 같이 인증 정보보호제품 도입 점검표를 제출합니다.

년 월 일

집적정보통신시설 사업자(대표자)

(서명 또는 인)

재단법인 한국보건 의료정보원 귀중

※ 인증받은 정보보호제품의 인증서는 별도 제출
 ※ 도입된 정보보호제품 목록이 사실과 다를 경우 EMR인증의 취소 사유가 될 수 있음

양식2-3

정보보호제품 인증서 증빙자료 제출 양식

의료기관 외의 장소에 전자의무기록 보관 시, 전자의무기록시설장비기준 고시에 따라 국정원장이 인증을 요구하는 정보보호제품은 CC 인증 등 인증서*를 제출해야 함
 * 국내 CC인증, 국제 CC인증, GS인증, 성능평가확인서, 보안기능확인서, 검증필 암호모듈

※ ‘인증 정보보호제품 도입 점검표’ 내 제품유형 항목에 대해 아래 표 양식을 참조하여 인증서 증빙자료 붙임

번호	정보보호시스템 제품 유형	증빙자료 세부사항
1	[정보보호시스템 제품유형] 예) 침입차단시스템	<input type="checkbox"/> 국내 CC 인증 <input type="checkbox"/> 국외 CC 인증 <input type="checkbox"/> GS인증 <input type="checkbox"/> 성능평가확인서 <input type="checkbox"/> 보안기능확인서 <input type="checkbox"/> 인증 없음
		<input type="checkbox"/> 검증필 암호모듈 탑재 <input type="checkbox"/> 검증필 암호모듈 미탑재 ※ 국정원 보안적합성 검증 사전인증 해당 제품에 한함
		[증빙자료(인증서 사본) 붙임]

※ (참고) 국가정보원 ‘보안적합성 검증 제도’ 관련 사이트 https://www.nis.go.kr:4016/AF/1_7_2_1.do 참조하여 작성

양식2-4

물리적 위치의 한정 증빙자료 제출 양식

(3) 증빙자료 제출 참고자료 : 4.3 항목

4.3	물리적 위치의 한정	<input type="checkbox"/> 점검항목 전자의무기록시스템 및 그 백업장비의 물리적 위치는 국내인가?		
		<input type="checkbox"/> 점검 세부내용 전자의무기록 시스템 및 그 백업장비의 물리적 위치는 국내로 한정한다.		
		<table border="1" style="width: 100%;"> <tr> <td style="width: 50%;"> <input type="checkbox"/> 증빙자료 설명 시스템 및 백업시스템의 국내 물리적 위치와 사용자 데이터 보호 정책 및 데이터 해외 이전불가 기술적 보증을 대한 증빙자료 </td> <td style="width: 50%;"> <input type="checkbox"/> 증빙자료 예시 <ul style="list-style-type: none"> • 서비스 계약서 (SLA) • 국내설비 목록 리스트 • 국내 물리적 위치 확인서 • 사용자 데이터 보호 정책 문서 • 데이터 해외 이전불가 기술적 보증 증빙 자료 </td> </tr> </table>	<input type="checkbox"/> 증빙자료 설명 시스템 및 백업시스템의 국내 물리적 위치와 사용자 데이터 보호 정책 및 데이터 해외 이전불가 기술적 보증을 대한 증빙자료	<input type="checkbox"/> 증빙자료 예시 <ul style="list-style-type: none"> • 서비스 계약서 (SLA) • 국내설비 목록 리스트 • 국내 물리적 위치 확인서 • 사용자 데이터 보호 정책 문서 • 데이터 해외 이전불가 기술적 보증 증빙 자료
<input type="checkbox"/> 증빙자료 설명 시스템 및 백업시스템의 국내 물리적 위치와 사용자 데이터 보호 정책 및 데이터 해외 이전불가 기술적 보증을 대한 증빙자료	<input type="checkbox"/> 증빙자료 예시 <ul style="list-style-type: none"> • 서비스 계약서 (SLA) • 국내설비 목록 리스트 • 국내 물리적 위치 확인서 • 사용자 데이터 보호 정책 문서 • 데이터 해외 이전불가 기술적 보증 증빙 자료 			
		<input type="checkbox"/> 증빙자료 <div style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <p>1. 계약문서 점검 확인</p> <ul style="list-style-type: none"> - ‘서비스 계약서(SLA)’ 및 ‘국내설비 목록 리스트’ 등을 통하여 명시된 EMR SW의 운영장비 및 백업장비(데이터 포함)의 지리적 위치가 국내인지 여부를 점검* - IaaS(인프라) 서비스 제공자의 사용자 데이터 보호 정책 및 데이터 해외 이전 불가에 대한 사항을 기술적으로 보증할 수 있는 자료 확인 <p>* 클라우드컴퓨팅 서비스인 경우 IaaS 클라우드컴퓨팅서비스 인프라 관리시스템을 통하여 SaaS서비스 가입자(EMR업체)가 계약 시 환경 설정상의 지정된 리전을 확인한다.</p> <p>* 또한, EMR시스템 구성을 위해 클라우드 환경에서 사용한 제품/서비스를 모두 식별하고, 국내 리전 범위를 벗어나는 제품/서비스 존재 여부를 확인한다.</p> <p>※ 문서로 제출한 증빙 자료에 대하여 심사하며, 추가 확인이 필요한 경우 추가 증빙자료 확인을 위한 현장심사 가능</p> </div> <p style="text-align: center; margin-top: 20px;"><i>증빙자료 붙임</i></p>		

클라우드컴퓨팅 사용 서비스 규격 확인서

집적정보통신시설 사업자명	
---------------	--

아래 표에 사용중인 서비스 및 규격을 확인하여 리전 한정 서비스 여부를 표기
서비스 목록은 계약서(SLA)와 일치하여야 함

사용중인 서비스 목록	리전 위치		리전 한정	
	국내 여부		서비스 여부	
	예	아니오	예	아니오
1 예) Amazon EC2, S-g2 등				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				

상기와 같이 사용중인 서비스의 목록 및 규격 확인서를 제출합니다.

년 월 일

집적정보통신시설 사업자(대표자)

(서명 또는 인)

재단법인 한국보건 의료정보원 귀중

※ 서비스 수준 계약서(SLA) 별도 제출
 ※ 서비스 규격이 사실과 다를 경우 EMR인증의 취소 사유가 될 수 있음

양식3

클라우드컴퓨팅 서비스 정보보호 기준 고시 항목별 점검표

□ 클라우드컴퓨팅 서비스 정보보호 기준 고시 통제항목 점검표

○ 관리적 보호조치

* 점검 항목표 (Y: 만족함, P: 부분적으로 만족함, N: 만족하지 않음, N/A: 해당 없음)

분류	항목	점검내용	Y	P	N	N/A
1. 정보 보호 정책 및 조직	1.1. 정보 보호 정책	1.1.1. 정보보호 정책을 문서화하고, CIO 승인 후 모든 임직원 및 외부 업무 관련자에게 제공 하는가?				
		1.1.2. 정보보호 정책의 타당성 및 효과를 연 1회 이상 검토하는가? 관련 법규 변경 및 내·외부 보안사고 발생 등의 중대한 사유가 발생할 경우에는 정보보호 정책의 타당성 및 효과를 추가로 검토하고 변경하는가?				
		1.1.3. 정보보호 정책 및 정책 시행문서의 이력관리 절차를 수립하고 시행하며, 최신본으로 유지하는가?.				
	1.2. 정보 보호 조직	1.2.1. 정보보호 활동을 계획, 실행, 검토하는 정보보호 전담조직을 구성하고 정보보호 최고책임자를 임명하는가?				
		1.2.2. 정보자산과 보안에 관련된 모든 임직원 및 외부 업무 관련자의 정보보호 역할과 책임을 명확하게 정의하는가? 서비스 이용자의 정보보호 역할과 책임도 서비스 수준 협약 등을 통해 명확하게 정의하는가?				
2. 인적 보안	2.1. 내부 인력 보안	2.1.1. 고용 계약서에 정보보호 정책 및 관련 법률을 준수하도록 하는 조항 또는 조건을 포함 하는가? 새로 채용하거나 합류한 근무 인력이 클라우드컴퓨팅서비스의 설비, 자원, 자산에 접근이 허용되기 이전에 서명을 받는가?				
			2.1.2. 클라우드컴퓨팅서비스의 시스템 운영 및 개발, 정보보호 등에 관련된 임직원의 경우 주요 직무자로 지정하여 관리하고, 직무 지정 범위는 최소화하는가?			
		2.1.3. 권한 오남용 등 내부 임직원의 고의적인 행위로 발생할 수 있는 잠재적인 위협을 줄이기 위하여 직무 분리 기준을 수립하고 적용하는가?				
		2.1.4. 정보보호와 개인정보보호 등을 위해 필요한 사항을 비밀유지서약서에 정의하고 주기적으로 갱신하는가?				
		2.1.5. 정보보호 정책을 위반한 임직원에 대한 징계 규정을 수립하고, 위반 사항이 발생 시 규정에 명시된 대로 징계 조치를 취하는가? 정보보호 정책을 충실히 이행한 임직원에 대한 보상 방안도 마련하는가?				
			2.1.6. 임직원의 퇴직 또는 직무 변경에 관한 책임을 명시적으로 정의하고 수행하는가?. 또한 이에 대한 접근권한도 제거하고 있는가?			
	2.2. 외부 인력 보안	2.2.1. 외부인력(외부유지보수직원, 외부용역자 포함)에 의한 정보자산 접근 등과 관련된 보안 요구사항을 계약에 반영하였는가?				
		2.2.2. 계약서에 명시한 보안요구사항 준수 여부를 주기적으로 점검하는가? 위반사항이나 침해사고 발생 시 적절한 조치를 수행하는가?				
			2.2.3. 외부인력과의 계약 만료 시 자산 반납, 접근권한의 회수, 중요정보 파기, 업무 수행 시 알게 된 정보의 대한 비밀 유지서약 등을 확인하는가?			
	2.3.	2.3.1. 모든 임직원 및 외부 업무 관련자를 포함하여 연간 정보보호 교육 프로그램을 수립하는가?				

	정보 보호 교육	2.3.2.	모든 임직원 및 외부 업무 관련자를 대상으로 연 1회 이상 정보보호 교육을 시행하는가?				
		2.3.3.	정보보호 정책 및 절차의 중대한 변경, 내·외부 보안사고 발생, 관련 법규 변경 등의 사유가 발생하면 추가 교육을 실시하는가?				
		2.3.3.	정보보호 교육 시행에 대한 기록을 남기고 결과를 평가하여 개선하는가?				
3. 자산 관리	3.1. 자산 식별 및 분류	3.1.1.	클라우드컴퓨팅서비스에 사용된 정보자산(정보시스템, 정보보호시스템, 정보 등)에 대한 자산분류기준 수립하고 식별된 자산의 목록을 작성하여 관리하는가?				
		3.1.2.	식별된 자산마다 책임자 및 관리자를 지정하여 책임소재를 명확히 하는가?				
		3.1.3.	기밀성, 무결성, 가용성, 법적요구사항 등을 고려하여 자산의 보안 등급을 부여하고, 보안 등급별 취급 절차에 따라 관리하는가?				
	3.2. 자산 변경 관리	3.2.1.	클라우드컴퓨팅서비스에 사용된 자산(시설, 장비, 소프트웨어 등)의 변경이 필요한 경우 보안 영향 평가를 통해 변경 사항을 관리하는가?				
			이용자에게 큰 영향을 주는 변경에 대해서는 사전에 공지하는가?				
		3.2.2.	클라우드컴퓨팅서비스에 사용된 자산(시설, 장비, 소프트웨어 등)의 변경을 지속적으로 모니터링하여 허가 받지 않은 변경을 탐지하고 최신의 변경 이력을 유지하는가?				
		3.2.3.	클라우드컴퓨팅서비스에 사용된 자산(시설, 장비, 소프트웨어 등)의 변경 후에는 보안성 및 호환성 등에 대한 작업 검증을 수행하는가?				
	3.3. 위험 관리	3.3.1.	관리적, 기술적, 물리적, 법적 분야 등 정보보호 전 영역에 대한 위험식별 및 평가가 가능하도록 위험관리 방법과 계획을 사전에 수립하는가?				
		3.3.2.	취약점 점검 정책에 따라 주기적으로 기술적 취약점(예 : 유·무선 네트워크, 운영체제 및 인프라, 응용 프로그램 취약점 등)을 점검하고 보완하는가?				
		3.3.3.	위험관리 방법 및 계획에 따라 정보보호 전 영역에 대한 위험 식별 및 평가를 연 1회 이상 수행하는가?				
			위험 식별 및 평가 결과에 따라 수용 가능한 위험수준을 설정하여 관리하는가?				
		3.3.4.	법규 및 계약관련 요구사항과 위험수용 수준을 고려하여 위험평가 결과에 따라 통제할 수 있는 방법을 선택하여 처리하는가?				
4. 서비스 공급망 관리	4.1. 공급망관리 정책	4.1.1.	클라우드컴퓨팅서비스에 대한 접근과 서비스 연속성을 저해하는 위험을 식별하고 최소화하기 위해 공급망과 관련한 보안 요구사항을 정의하는 관리 정책을 수립하는가?				
		4.1.2.	클라우드컴퓨팅서비스 범위 및 보안 요구사항을 포함하는 공급망 계약을 체결하고 다자간 협약시 책임을 개별 계약서에 각각 명시하는가? 또한 해당 서비스에 관련된 모든 이해관계자에게 적용하는가?.				
	4.2. 공급망 변경 관리	4.2.1.	정보보호 정책, 절차 및 통제에 대한 수정 및 개선이 필요하다고 판단될 경우 서비스 공급망 상에 발생할 수 있는 위험에 대한 검토를 통해 안전성을 확보 후 계약서 내용 변경 방안을 제시하는가?				
		4.2.2.	클라우드컴퓨팅서비스 공급망 상에서 발생하는 기록 및 보고서는 정기적으로 모니터링 및 검토하는가?				
5. 침해 사고 관리	5.1. 침해 사고 대응 절차 및 체계	5.1.1.	침해사고에 대한 효율적이고 효과적인 대응을 위해 신고절차, 유출 금지 대상, 사고 처리 절차 등을 담은 침해사고 대응절차를 마련하는가? 또한 침해사고 대응절차는 이용자와 제공자의 책임과 절차를 포함하는가?				
		5.1.2.	침해사고 정보를 수집·분석·대응할 수 있는 보안관제 시스템 및 조직을 구성·운영하는가? 침해사고 유형 및 중요도에 따라 보고 및 협력체계를 구축하는가?.				
	5.1.3.	침해사고 대응과 관련된 역할 및 책임이 있는 담당자를 훈련하고, 주기적으로 침해사고 대응 능력을 점검하는가?					

5.2. 침해 사고 대응	5.2.1.	침해사고 발생 시 침해사고 대응절차에 따라 법적 통지 및 신고 의무를 준수하는가?					
		클라우드컴퓨팅서비스 이용자에게 발생 내용, 원인, 조치 현황 등을 신속하게 알리는가?					
	5.2.2.	침해사고 발생 시 침해사고 대응절차에 따라 처리와 복구를 신속하게 수행하는가?					
	5.3. 사후 관리	5.3.1.	침해사고가 처리 및 종결된 후 발생 원인을 분석하고 그 결과를 이용자에게 알리는가?				
		5.3.2.	유사한 침해사고에 대한 신속한 처리를 위해 침해사고 관련 정보 및 발견된 취약점을 관련 조직 및 임직원과 공유하는가?				
	5.3.2.	침해사고 관련 정보를 활용하여 유사한 침해사고가 반복되지 않도록 침해사고 재발방지 대책을 수립하고, 필요한 경우 침해사고 대응 체계도 변경하는가?					
6. 서비스 연속성 관리	6.1. 장애 대응	6.1.1.	관련 법률에서 규정한 클라우드컴퓨팅서비스의 중단으로부터 업무 연속성을 보장하기 위해 백업, 복구 등을 포함하는 장애 대응 절차를 마련하는가?				
		6.1.2.	클라우드컴퓨팅서비스 중단이나 피해가 발생 시 장애 대응절차에 따라 법적 통지 및 신고 의무를 준수하는가?				
			클라우드컴퓨팅서비스 이용자에게도 발생 내용, 원인, 조치 현황 등을 신속하게 알리는가?				
		6.1.3.	클라우드컴퓨팅서비스 중단이나 피해가 발생할 경우, 서비스 수준 협약(SLA)에 명시된 시간 내에 장애 대응절차에 따라 해당 서비스의 장애를 처리하고 복구시키는가?				
	6.1.4.	장애 관련 정보를 활용하여 유사한 서비스 중단이 반복되지 않도록 장애 재발방지 대책을 수립하고, 필요한 경우 장애 대응 절차도 변경하는가?					
	6.2. 서비스 가용성	6.2.1.	클라우드컴퓨팅서비스의 가용성을 보장하기 위해 성능 및 용량에 대한 요구사항을 정의하고, 지속적으로 관리할 수 있는 모니터링 방법 또는 절차를 수립하는가?				
		6.2.2.	정보처리설비(예 : 클라우드컴퓨팅서비스를 제공하는 물리적인 서버, 스토리지, 네트워크 장비, 통신 케이블, 접속 회선 등)의 장애로 서비스가 중단되지 않도록 정보 처리설비를 이중화하는가?				
			장애 발생 시 신속하게 복구를 수행하도록 백업 체계도 마련하는가?				
		6.2.3.	서비스 가용성에 대한 영향 평가를 주기적으로 점검하는가?				
	7. 준거성	7.1. 법 및 정책 준수	7.1.1.	정보보호 관련 법적 요구사항을 식별하고 준수하는가?			
7.1.2.			정보보호 정책 및 서비스 수준 협약에 포함된 보안 요구사항을 식별하고 준수하며 이용자가 요구하는 경우 관련 증거를 제공하는가?				
7.2. 보안 감사		7.2.1.	법적 요구사항 및 정보보호 정책 준수 여부를 보증하기 위해 독립적 보안감사 계획을 수립하여 시행하고 개선 조치를 취하는가?				
		7.2.2.	보안감사 증거(로그)은 식별할 수 있는 형태로 기록 및 모니터링 되어야 되고 비인가된 접근 및 변조로부터 보호되는가?				

○ 물리적 보호조치

분류	항목	점검내용	Y	P	N	N/A	
8. 물리적 보안	8.1. 물리적 보호 구역	8.1.1.	중요 정보 및 정보처리시설을 보호하기 위한 물리적 보안 구역(예 : 주요 정보처리 설비 및 시스템 구역, 사무실, 외부인 접근실 등)을 지정하였는가?				
		지정된 각 보안 구역에 대한 보안 대책을 마련하는가?					
	8.1.2.	물리적 보안 구역에 인가된 자만이 접근할 수 있도록 출입을 통제하는 시설(예 : 경비원, 출입 통제 시스템 등)을 갖추었는가?					

			통제된 시설에 대한 출입 및 접근 이력을 주기적으로 검토하는가?				
	8.1.3.		유지보수 등 주요 정보처리 설비 및 시스템이 위치한 보호구역 내에서의 작업 절차를 수립하고 작업에 대한 기록을 주기적으로 검토하여야 한다.				
	8.1.4.		사무실 및 설비 공간에 대한 물리적인 보호방안을 수립하고 적용하는가?				
	8.1.5.		공공장소 및 운송·하역을 위한 구역은 내부 정보처리시설로부터 분리 및 통제하는가?				
	8.1.6.		노트북 등 모바일 기기 미승인 반출입을 통한 중요정보 유출, 내부망 악성코드 감염 등의 보안사고 예방을 위하여 보호구역 내 임직원 및 외부인력 모바일 기기 반출입 통제 절차를 수립하고 기록·관리하는가?				
8.2. 정보 처리 시설 및 장비 보호	8.2.1.		물리적 및 환경적 위험으로부터 잠재적 손상을 최소화하고 비인가 된 접근 가능성을 최소화하기 위하여, 정보처리시설 내 장비의 위치를 파악하고 배치하는가?				
	8.2.2.		각 보안 구역의 중요도 및 특성에 따라 화재, 누수, 전력 이상 등 자연재해나 인재에 대비하여 화재 감지기, 소화 설비, 누수 감지기, 항온 항습기, 무정전 전원 장치(UPS), 이중 전원선 등의 설비를 갖추고 있는가?				
	8.2.3.		데이터를 송수신하는 통신케이블이나 전력을 공급하는 전력 케이블은 손상이나 도청으로부터 보호하는가?				
	8.2.4.		정보처리시설은 가용성과 무결성을 지속적으로 보장할 수 있도록 유지보수 하는가?				
	8.2.5.		장비의 미승인 반출·입을 통한 중요정보 유출, 악성코드 감염 등의 침해사고 예방을 위하여, 보안 구역 내 직원 및 외부 업무 관련자에 의한 장비 반출·입 절차를 수립하고, 기록 및 관리하는가?				
	8.2.6.		정보처리시설 내의 저장 매체를 포함하여 모든 장비를 파악하고, 민감한 데이터가 저장된 장비를 폐기하는 경우 복구 불가능하도록 하는가? 재사용하는 경우에도 복구 불가능 상태에서 재사용하는가?				

○ 기술적 보호조치

분류	항목	점검내용	Y	P	N	N/A	
9. 가상 화 보안	9.1. 가상화 인프라	9.1.1.	가상자원(가상 머신, 가상 스토리지, 가상 소프트웨어 등)의 생성, 변경, 회수 등에 대한 관리 방안을 수립하는가?				
		9.1.2.	이용자와의 계약 종료 시 가상자원 회수 절차에 따라 백업을 포함한 모든 클라우드 시스템에서 삭제하는가?				
		9.1.3.	가상자원에 대한 무결성 보장하기 위한 보호조치 및 가상자원의 변경(수정, 이동, 삭제, 복사)에 대해 모니터링하는가?				
			가상자원에 손상이 발생한 경우 이를 이용자에게 알려주는가?				
		9.1.4.	가상자원을 관리하는 하이퍼바이저의 기능 및 인터페이스에 대한 접근 통제 방안을 마련하는가?				
			하이퍼바이저에 대한 소프트웨어 업데이트 및 보안패치를 최신으로 유지하는가?				
		9.1.5.	가상자원을 제공하기 위한 웹사이트와 가상소프트웨어(앱, 응용프로그램)를 배포하기 위한 공개서버에 대한 물리적, 기술적 보호대책을 수립하는가?				
		9.1.6.	클라우드컴퓨팅서비스 제공자는 표준화된 가상화 포맷, 이식성이 높은 가상화 플랫폼, 공개 API 등을 이용하여 클라우드컴퓨팅서비스 간의 상호 운용성 및 이식성을 높이는가?				
	클라우드컴퓨팅서비스 제공자는 클라우드컴퓨팅서비스 간의 상호 운용성 및 이식성을 높이기 위해 표준화된 가상화 포맷, 이식성이 높은 가상화 플랫폼, 공개 API 등을 이용하는가?						
	9.2. 가상	9.2.1.	바이러스, 웜, 트로이목마 등의 악성코드로부터 이용자의 가상 환경(가상PC, 가상 서버, 가상 소프트웨어 등)을 보호하기 위한 악성코드 탐지, 차단 등의 보안기술을 지원하는				

			가?					
			이상 징후 발견 시 이용자 통지하고 사용 중지 및 격리 조치를 수행하는가?					
	환경	9.2.2.	가상 환경(가상PC, 가상 서버, 가상 소프트웨어 등) 접근을 위한 인터페이스 및 API에 대한 보안 취약점을 주기적으로 분석하고, 이에 대한 보호방안을 마련하는가?					
		9.2.3.	이용자가 기존 정보시스템 환경에서 클라우드컴퓨팅서비스의 가상 환경으로 전환 시 안전하게 데이터를 이전하도록 암호화 등의 기술적인 조치방안을 제공하는가?					
		9.2.4.	클라우드컴퓨팅서비스 제공자는 출처, 유통경로 및 제작자가 명확한 소프트웨어로 구성된 가상환경을 제공하는가?					
10. 접근 통제	접근 통제 정책	10.1.1.	비인가자의 접근을 통제할 수 있도록 접근통제 영역 및 범위, 접근통제 규칙, 방법 등을 포함하여 접근통제 정책을 수립하는가?					
		10.1.2.	접근기록 대상을 정의하고 서비스 통제, 관리, 사고 발생 책임 추적성 등을 보장할 수 있는 형태로 기록되고 유지하는가?					
	10.2. 접근 권한 관리	10.2.2.	클라우드 시스템 및 중요정보에 대한 접근을 통제하기 위하여 공식적인 사용자 등록 및 해지 절차를 수립하는가?					
			업무 필요성에 따라 사용자 접근권한을 최소한으로 부여하는가?					
		10.2.3.	클라우드 시스템 및 중요정보 관리 및 특수 목적을 위해 부여한 계정 및 권한을 식별하고 별도 통제하여야 한다.					
		10.2.4.	클라우드 시스템 및 중요정보에 대한 접근을 관리하기 위하여 접근권한 부여, 이용(장기간 미사용), 변경(퇴직 및 휴직, 직무변경, 부서변경)의 적정성 여부를 정기적으로 점검하여야 한다.					
	10.3. 사용자 식별 및 인증	10.3.1.	클라우드 시스템에서 사용자를 유일하게 구분할 수 있는 식별자를 할당하고 추측 가능한 식별자 사용을 제한하는가?					
			동일한 식별자를 공유하여 사용하는 경우 그 사유와 타당성을 검토하고 책임자의 승인을 받는가?					
		10.3.2.	클라우드 시스템에 대한 접근은 사용자 인증, 로그인 횟수 제한, 불법 로그인 시도 경고 등 안전한 사용자 인증 절차에 의해 통제하는가?					
		10.3.3.	이용자가 클라우드컴퓨팅서비스에 대해 다중 요소 인증 등 강화된 인증 수단을 요청하는 경우 이를 제공하기 위한 방안을 마련하는가?					
		10.3.4.	법적 요구사항, 외부 위협요인 등을 고려하여 패스워드 복잡도 기준, 초기 패스워드 변경, 변경주기 등 사용자 패스워드 관리절차를 수립·이행하고 패스워드 관리 책임이 사용자에게 있음을 주지시키는가?					
			관리자 패스워드는 별도 보호대책을 수립하여 관리하는가?					
	10.3.5.	고객, 회원 등 외부 이용자가 접근하는 클라우드 시스템 또는 웹서비스의 안전한 이용을 위하여 계정 및 패스워드 등의 관리절차를 마련하고 관련 내용을 공지하는가?						
	11. 네트워크 보안	11.1. 네트워크 보안	11.1.1.	클라우드컴퓨팅서비스와 관련된 내·외부 네트워크에 대해 보안 정책과 절차를 수립하는가?				
			11.1.2.	DDoS, 비인가 접속 등으로 인한 서비스 중단 및 중요 정보 유출 등을 막기 위해 네트워크를 모니터링하고 통제하는가?				
11.1.3.			클라우드컴퓨팅서비스와 관련된 내·외부 네트워크를 보호하기 위하여 정보보호시스템(방화벽, IPS, IDS, VPN 등)을 운영하는가?					
11.1.4.			클라우드 시스템에서 중요 정보가 이동하는 구간에 대해서는 암호화된 통신채널을 사용하는가?					
11.1.5.			클라우드컴퓨팅서비스 제공자의 관리 영역과 이용자의 서비스 영역, 이용자 간 서비스 영역의 네트워크 접근은 물리적 또는 논리적으로 분리하는가?					
11.1.6.			클라우드 시스템은 무선망과 분리하고, 무선접속에 대한 접근을 통제하는가?					

		6.	무선접속을 사용하는 경우 그 사유와 타당성을 검토하고 책임자의 승인을 받는가?					
12. 데이터 보호 및 암호화	12.1. 데이터 보호	12.1. 1.	데이터 유형, 법적 요구사항, 민감도 및 중요도에 따라 데이터를 분류하고 관리하는가?					
		12.1. 2.	이용자와 서비스 수준 협약 단계에서 데이터의 소유권을 명확하게 확립하는가?					
		12.1. 3.	입·출력, 전송 또는 데이터 교환 및 저장소의 데이터에 대해 항상 데이터 무결성을 확인하는가?					
		12.1. 4.	데이터에 대한 접근제어, 위·변조 방지 등 데이터 처리에 대한 보호 기능을 이용자에게 제공하는가?					
		12.1. 5.	이용자에게 데이터를 추적하기 위한 방안을 제공하고, 이용자가 요구하는 경우 구체적인 제공정보(이용자의 정보가 저장되는 국가의 명칭 등)를 공개하는가?					
		12.1. 6.	클라우드컴퓨팅서비스 종료, 이전 등에 따른 데이터 폐기 조치 시 이용자와 관련된 모든 데이터를 폐기하며, 폐기된 데이터를 복구할 수 없도록 삭제 방안을 마련하는가?					
	12.2. 매체 보안	12.2. 1.	중요정보를 담고 있는 하드디스크, 스토리지 등의 저장매체 폐기 및 재사용 절차를 수립하고 매체에 기록된 중요정보는 복구 불가능하도록 완전히 삭제하는가?					
		12.2. 2.	중요정보 유출을 예방하기 위해 외장하드, USB, CD 등 이동매체 취급, 보관, 폐기, 재사용에 대한 절차를 수립하는가? 매체를 통한 악성코드 감염 방지 대책을 마련하는가?					
	12.3. 암호화	12.3. 1.	클라우드컴퓨팅서비스에 저장 또는 전송 중인 데이터를 보호하기 위해 암호화 대상, 암호 강도(복잡도), 키관리, 암호 사용에 대한 정책을 마련하는가? 정책에는 개인정보 저장 및 전송 시 암호화 적용 등 암호화 관련 법적 요구사항을 반드시 반영하는가?					
		12.3. 2.	암호키 생성, 이용, 보관, 배포, 파기에 관한 안전한 절차를 수립하고, 암호키는 별도의 안전한 장소에 보관하는가?					
	13. 시스템 개발 및 도입 보안	13.1. 시스템 분석 및 설계	13.1. 1.	신규 시스템 개발 및 기존 시스템 변경 시 정보보호 관련 법적 요구사항, 최신 보안취약점, 정보보호 기본요소(기밀성, 무결성, 가용성) 등을 고려하여 보안요구사항을 명확히 정의하고 이를 적용하는가?				
			13.1. 2.	클라우드 시스템 설계 시 사용자 인증에 관한 보안요구사항을 반드시 고려하는가?				
중요정보의 입·출력 및 송수신 과정에서 무결성, 기밀성이 요구될 경우 법적 요구사항을 고려하는가?								
13.1. 3.			클라우드 시스템 설계 시 사용자의 인증, 권한 변경, 중요정보 이용 및 유출 등에 대한 감사증적을 확보할 수 있도록 하는가?					
13.1. 4.			클라우드 시스템 설계 시 업무의 목적 및 중요도에 따라 접근권한을 부여할 수 있도록 하는가?					
13.1. 5.		로그기록의 정확성을 보장하고 법적인 자료로서 효력을 지니기 위해 클라우드 시스템 시각을 공식 표준시각으로 정확하게 동기화 하는가? 또한 서비스 이용자에게 시각 정보 동기화 기능을 제공하는가?						
13.2. 구현 및 시험		13.2. 1.	안전한 코딩방법에 따라 클라우드 시스템을 구현하고, 분석 및 설계 과정에서 도출한 보안요구사항이 정보시스템에 적용되었는지 확인하기 위하여 시험을 수행하는가?					
		13.2. 2.	개발 및 시험 시스템은 운영시스템에 대한 비인가 접근 및 변경의 위험을 감소하기 위해 원칙적으로 분리하는가? 단 분리하여 운영하기 어려운 경우 그 사유와 타당성을 검토하고 안전성 확보 방안을 마련하는가?					
		13.2. 3.	시스템 시험 과정에서 운영데이터 유출을 예방하기 위해 시험데이터 생성, 이용 및 관리, 파기, 기술적 보호조치에 관한 절차를 수립하여 이행하는가?					
		13.2. 4.	소스 프로그램에 대한 변경관리를 수행하고 인가된 사용자만이 소스 프로그램에 접근할 수 있도록 통제절차를 수립하여 이행하는가?					

			소스 프로그램은 운영환경에 보관하지 않는 것을 원칙으로 하는가?				
13.3. 외주 개발 보안	13.3. 1.		클라우드 시스템 개발을 외주 위탁하는 경우 분석 및 설계단계에서 구현 및 이관까지의 준수해야 할 보안요구사항을 계약서에 명시하고 이행여부를 관리·감독하는가?				
13.4. 시스템 도입 보안	13.4. 1.		클라우드 시스템의 처리 속도와 용량에 대하여 주기적인 모니터링을 수행하고 안정성의 확보에 필요한 시스템 도입 계획을 수립하는가?				
	13.4. 2.		새로 도입되는 시스템에 대한 인수 기준이 수립되며, 인수 전에 테스트가 수행되는가?				

□ 클라우드컴퓨팅 서비스 정보보호 기준 고시 증적자료 목록 (예시)

○ 기술적 보호조치

분류	항목	점검내용	증적자료
1. 정보 보호 정책 및 조직	1.1. 정보 보호 정책	1.1.1. 정보보호 정책을 문서화하고, CIO 승인 후 모든 임직원 및 외부 업무 관련자에게 제공하는가?	<ul style="list-style-type: none"> 정보보호 정책서 정보보호시행문서 정보보호최고책임자의승인을확인할수있는내부결재문또는서명본 정책및지침의배포증적(공지사항게시판이용등)
		1.1.2. 정보보호 정책의 타당성 및 효과를 연 1회 이상 검토하는가? 관련 법규 변경 및 내·외부 보안사고 발생 등의 중대한 사유가 발생할 경우에는 정보보호 정책의 타당성 및 효과를 추가로 검토하고 변경하는가?	<ul style="list-style-type: none"> 정보보호정책 검토회의록 정보보호정책/지침검토 및개정이력 주요변경사항공유예시
		1.1.3. 정보보호 정책 및 정책 시행문서의 이력관리 절차를 수립하고 시행하며, 최신본으로 유지하는가?	<ul style="list-style-type: none"> 정보보호 정책서 및 시행문서의 이력 관리 내역 정보보호정책서및시행문서최신본배포증적
	1.2. 정보 보호 조직	1.2.1. 정보보호 활동을 계획, 실행, 검토하는 정보보호 전담조직을 구성하고 정보보호 최고책임자를 임명하는가?	<ul style="list-style-type: none"> 정보보호 조직 구성도 정보보호최고책임자임명장또는승인문서 직무기술서
		1.2.2. 정보자산과 보안에 관련된 모든 임직원 및 외부 업무 관련자의 정보보호 역할과 책임을 명확하게 정의하는가? 서비스 이용자의 정보보호 역할과 책임도 서비스 수준 협약 등을 통해 명확하게 정의하는가?	<ul style="list-style-type: none"> 직무기술서 정보보호활동평가지표 SLA또는이용자와의계약서
	2. 인적 보안	2.1. 내부 인력 보안	2.1.1. 고용 계약서에 정보보호 정책 및 관련 법률을 준수하도록 하는 조항 또는 조건을 포함하는가? 새로 채용하거나 합류한 근무 인력이 클라우드컴퓨팅서비스의 설비, 자원, 자산에 접근이 허용되기 이전에 서명을 받는가?
2.1.2. 클라우드컴퓨팅서비스의 시스템 운영 및 개발, 정보보호 등에 관련된 임직원의 경우 주요 직무자로 지정하여 관리하고, 직무 지정 범위는 최소화하는가?			<ul style="list-style-type: none"> 주요 직무자 현황 직무기술서 주요가상정보시스템계정 및 권한관리대장
2.1.3. 권한 오남용 등 내부 임직원의 고의적인 행위로 발생할 수 있는 잠재적인 위협을 줄이기 위하여 직무 분리 기준을 수립하고 적용하는가?			<ul style="list-style-type: none"> 직무 분리 기준 직무기술서 주요직무자현황 직무 미분리시 보완 통제 현황
2.1.4. 정보보호와 개인정보보호 등을 위해 필요한 사항을 비밀유지서약서에 정의하고 주기적으로 갱신하는가?			<ul style="list-style-type: none"> 정보보호서약서 및 비밀유지 서약서 (임직원 및 외부인력) 외주용역계약서 서약서등중요문서보관
2.1.5. 정보보호 정책을 위반한 임직원에 대한 징계 규정을 수립하고, 위반 사항이 발생 시 규정에 명시된 대로 징계 조치를 취하는가? 정보보호 정책을 충실히 이행한 임직원에 대한 보상 방안도 마련하는가?			<ul style="list-style-type: none"> 상벌 관련 규정 정보보호 지침위반자 징계내역
2.1.6. 임직원의 퇴직 또는 직무 변경에 관한 책임을 명시적으로 정의하고 수행하는가?. 또한 이에 대한 접근권한도 제거하고 있는가?			<ul style="list-style-type: none"> 퇴직 및 직무변경 절차서 퇴직자 보안점검 체크리스트 및 점검내역 퇴직시자산반납관리대장 보안서약서
2.2. 외부 인력		2.2.1. 외부인력(외부유지보수직원, 외부용역자 포함)에 의한 정보자산 접근 등과 관련된 보안요구사항을 계약에 반영하였는가?	<ul style="list-style-type: none"> 위탁 계약서 정보보호협약서 RFP,외주용역평가표

3. 자산 관리	보안	2.2.2.	계약서에 명시한 보안요구사항 준수 여부를 주기적으로 점검하는가?	<ul style="list-style-type: none"> •업무 위탁 계약서 •보안점검체크리스트등 점검결과 •보안조치및교육내역(결과,명단,교재등)
			위반사항이나 침해사고 발생 시 적절한 조치를 수행하는가?	
		2.2.3.	외부인력과의 계약 만료 시 자산 반납, 접근권한의 회수, 중요정보 파기, 업무 수행 시 알게 된 정보의 대한 비밀 유지서약 등을 확인하는가?	<ul style="list-style-type: none"> •보안점검 체크리스트 등 점검 결과 * (정보및개인정보파기 확인) •비밀유지확인서
	2.3. 정보 보호 교육	2.3.1	모든 임직원 및 외부 업무 관련자를 포함하여 연간 정보보호 교육 프로그램을 수립하는가?	•연간 교육계획서
		2.3.2.	모든 임직원 및 외부 업무 관련자를 대상으로 연 1회 이상 정보보호 교육을 시행하는가?	<ul style="list-style-type: none"> •연간 교육계획서 •교육참석자목록 •교육이수증 •교육수행관련자료
			정보보호 정책 및 절차의 중대한 변경, 내·외부 보안사고 발생, 관련 법규 변경 등의 사유가 발생하면 추가 교육을 실시하는가?	
		2.3.3.	정보보호 교육 시행에 대한 기록을 남기고 결과를 평가하여 개선하는가?	<ul style="list-style-type: none"> •연간 교육계획서 •교육참석자목록 •교육이수증 •교육결과보고서 •교육자료
	3.1. 자산 식별 및 분류	3.1.1.	클라우드컴퓨팅서비스에 사용된 정보자산(정보시스템, 정보보호시스템, 정보 등)에 대한 자산분류기준 수립하고 식별된 자산의 목록을 작성하여 관리하는가?	<ul style="list-style-type: none"> •정보자산 분류기준 •정보자산목록
		3.1.2.	식별된 자산마다 책임자 및 관리자를 지정하여 책임소재를 명확히 하는가?	<ul style="list-style-type: none"> •정보자산 분류기준 •정보자산목록(책임자/관리자지정현황포함)
3.1.3.		기밀성, 무결성, 가용성, 법적요구사항 등을 고려하여 자산의 보안 등급을 부여하고, 보안 등급별 취급 절차에 따라 관리하는가?	<ul style="list-style-type: none"> •정보자산 분류기준 •정보자산목록 •정보자산보안등급부여현황 •보안등급별취급절차및보안통제현황 	
3.2. 자산 변경 관리		3.2.1.	클라우드컴퓨팅서비스에 사용된 자산(시설, 장비, 소프트웨어 등)의 변경이 필요한 경우 보안 영향 평가를 통해 변경 사항을 관리하는가?	<ul style="list-style-type: none"> •자산 변경 절차 •변경요청/승인이력 •보안영향평가결과 •이용자 고지 이력
			이용자에게 큰 영향을 주는 변경에 대해서는 사전에 공지하는가?	
		3.2.2.	클라우드컴퓨팅서비스에 사용된 자산(시설, 장비, 소프트웨어 등)의 변경을 지속적으로 모니터링하여 허가 받지 않은 변경을 탐지하고 최신의 변경 이력을 유지하는가?	<ul style="list-style-type: none"> •변경이력 내역서 •변경관리대장 •미승인변경탐지방안(Checksum)
3.2.3.		클라우드컴퓨팅서비스에 사용된 자산(시설, 장비, 소프트웨어 등)의 변경 후에는 보안성 및 호환성 등에 대한 작업 검증을 수행하는가?	<ul style="list-style-type: none"> •보안영향평가 결과 •작업 내역서 •사전 영향평가서 	
3.3. 위험 관리		3.3.1.	관리적, 기술적, 물리적, 법적 분야 등 정보보호 전 영역에 대한 위험식별 및 평가가 가능하도록 위험관리 방법과 계획을 사전에 수립하는가?	<ul style="list-style-type: none"> •위험 평가 방법론 •위험 평가 계획서
		3.3.2.	취약점 점검 정책에 따라 주기적으로 기술적 취약점(예 : 유·무선 네트워크, 운영체제 및 인프라, 응용 프로그램 취약점 등)을 점검하고 보완하는가?	<ul style="list-style-type: none"> •취약점 점검 계획서 •침투테스트 계획 및 결과 •취약점 점검 결과 보고서 •취약점 보완 보고서
		3.3.3.	위험관리 방법 및 계획에 따라 정보보호 전 영역에 대한 위험 식별 및 평가를 연 1회 이상 수행하는가?	<ul style="list-style-type: none"> •위험 평가 방법론 •위험분류표 •위험분석 및 평가계획서 •위험분석 및 평가결과서
			위험 식별 및 평가 결과에 따라 수용 가능한 위험수준을 설정하여 관리하는가?	
3.3.4.		법규 및 계약관련 요구사항과 위험수용 수준을 고려하여 위험평가 결과에 따라 통제할 수 있는 방법을 선택하여 처리하는가?	•정보보호책임자 승인결과	

				<ul style="list-style-type: none"> ·위험분석 및 평가계획서 ·위험분석 및 평가결과서
4. 서비스 공급망 관리	4.1. 공급망관리 정책	4.1.1.1.	클라우드컴퓨팅서비스에 대한 접근과 서비스 연속성을 저해하는 위험을 식별하고 최소화하기 위해 공급망과 관련한 보안 요구사항을 정의하는 관리 정책을 수립하는가?	<ul style="list-style-type: none"> ·공급망 현황 ·공급망 계약서 ·공급망의 연속성 저해가 등 위험
		4.1.1.2.	클라우드컴퓨팅서비스 범위 및 보안 요구사항을 포함하는 공급망 계약을 체결하고 다자간 협약시 책임을 개별 계약서에 각각 명시하는가? 또한 해당 서비스에 관련된 모든 이해관계자에게 적용하는가?.	<ul style="list-style-type: none"> ·공급망 계약서, 협약서, 부속서 등 (역할 및 책임 명시)
	4.2. 공급망 변경 관리	4.2.1.1.	정보보호 정책, 절차 및 통제에 대한 수정 및 개선이 필요하다고 판단될 경우 서비스 공급망 상에 발생할 수 있는 위험에 대한 검토를 통해 안전성을 확보 후 계약서 내용 변경 방안을 제시하는가?	<ul style="list-style-type: none"> ·공급망 계약서 ·계약변경 관리 절차 ·공급망위험 검토 결과
		4.2.1.2.	클라우드컴퓨팅서비스 공급망 상에서 발생하는 기록 및 보고서는 정기적으로 모니터링 및 검토하는가?	<ul style="list-style-type: none"> ·공급망 계약서 ·공급망보안요구사항 ·공급망위험검토결과 ·공급망운영보고서
5. 침해사고 관리	5.1. 침해사고 대응 절차 및 체계	5.1.1.	침해사고에 대한 효율적이고 효과적인 대응을 위해 신고절차, 유출 금지 대상, 사고 처리 절차 등을 담은 침해사고 대응절차를 마련하는가?	<ul style="list-style-type: none"> ·침해사고 관리지침 ·침해사고대응절차 ·침해사고대응조직
			또한 침해사고 대응절차는 이용자와 제공자의 책임과 절차를 포함하는가?	
		5.1.2.	침해사고 정보를 수집·분석·대응할 수 있는 보안관제 시스템 및 조직을 구성·운영하는가?	<ul style="list-style-type: none"> ·침해사고 관리지침 ·외부관제용역계약서 ·침해사고대응조직 ·비상연락망(외부기관포함) ·침해사고유형 및 중요도 분류 ·침해사고 모니터링 및 대응조직,방법,절차 ·관제보고서
	침해사고 유형 및 중요도에 따라 보고 및 협력체계를 구축하는가?.			
	5.1.3.	침해사고 대응과 관련된 역할 및 책임이 있는 담당자를 훈련하고, 주기적으로 침해사고 대응 능력을 점검하는가?	<ul style="list-style-type: none"> ·모의훈련 계획서 ·모의훈련결과보고서 ·침해사고대응절차 	
	5.2. 침해사고 대응	5.2.1.	침해사고 발생 시 침해사고 대응절차에 따라 법적 통지 및 신고 의무를 준수하는가?	<ul style="list-style-type: none"> ·침해사고 보고서 ·침해사고관리대장 ·비상연락망 ·침해사고보고및통지절차 ·침해사고발생시신고,통지 내용(항목/서식)
			클라우드컴퓨팅서비스 이용자에게 발생 내용, 원인, 조치 현황 등을 신속하게 알리는가?	
	5.2.2.	침해사고 발생 시 침해사고 대응절차에 따라 처리와 복구를 신속하게 수행하는가?	<ul style="list-style-type: none"> ·침해사고 대응 결과보고서 ·침해사고관리대장 ·침해사고대응절차(이용자 요청지원포함) 	
5.3. 사후 관리	5.3.1.	침해사고가 처리 및 종결된 후 발생 원인을 분석하고 그 결과를 이용자에게 알리는가?	<ul style="list-style-type: none"> ·침해사고 관련 이용자 고지 내역 (항목/서식) ·침해사고 대응 결과보고서 ·침해사고 대응 절차(공유) 	
		유사한 침해사고에 대한 신속한 처리를 위해 침해사고 관련 정보 및 발견된 취약점을 관련 조직 및 임직원과 공유하는가?		
5.3.2.	침해사고 관련 정보를 활용하여 유사한 침해사고가 반복되지 않도록 침해사고 재발방지 대책을 수립하고, 필요한 경우 침해사고 대응 체계도 변경하는가?	<ul style="list-style-type: none"> ·침해사고 재발방지 대책 ·임직원 인식개선 교육등 활동 		
6. 서비스연속성 관리	6.1. 장애 대응	6.1.1.	관련 법률에서 규정한 클라우드컴퓨팅서비스의 중단으로부터 업무 연속성을 보장하기 위해 백업, 복구 등을 포함하는 장애 대응 절차를 마련하는가?	<ul style="list-style-type: none"> ·장애대응 매뉴얼 및 절차 ·비상연락망
		6.1.2.	클라우드컴퓨팅서비스 중단이나 피해가 발생 시 장애 대응절차에 따라 법적 통지 및 신고 의무를 준수하는가?	<ul style="list-style-type: none"> ·장애대응 매뉴얼 및 절차 ·신고및통보내역(서식/항목) ·장애관리현황(대장)
			클라우드컴퓨팅서비스 이용자에게도 발생 내용, 원인, 조치 현황 등을 신	

			속하게 알리는가?	
	6.1.3.		클라우드컴퓨팅서비스 중단이나 피해가 발생할 경우, 서비스 수준 협약 (SLA)에 명시된 시간 내에 장애 대응절차에 따라 해당 서비스의 장애를 처리하고 복구시키는가?	<ul style="list-style-type: none"> ·장애대응 매뉴얼 및 절차 ·장애조치 보고서 ·서비스 수준 협약(SLA)
	6.1.4.		장애 관련 정보를 활용하여 유사한 서비스 중단이 반복되지 않도록 장애 재발방지 대책을 수립하고, 필요한 경우 장애 대응 절차도 변경하는가?	<ul style="list-style-type: none"> ·장애조치 보고서 ·재발방지 대책 ·장애대응 절차
	6.2. 서비스 가용성	6.2.1.	클라우드컴퓨팅서비스의 가용성을 보장하기 위해 성능 및 용량에 대한 요구사항을 정의하고, 지속적으로 관리할 수 있는 모니터링 방법 또는 절차를 수립하는가?	<ul style="list-style-type: none"> ·성능·용량 분석 보고서 ·모니터링 절차서 ·모니터링 대상 및 임계치 현황 ·임계치 초과 시 조치계획
6.2.2.		정보처리설비(예 : 클라우드컴퓨팅서비스를 제공하는 물리적인 서버, 스토리지, 네트워크 장비, 통신 케이블, 접속 회선 등)의 장애로 서비스가 중단되지 않도록 정보 처리설비를 이중화하는가?	<ul style="list-style-type: none"> ·DR 서비스 계약서 ·시스템구성도(이중화) ·서비스 복구 조직 및 절차 	
		장애 발생 시 신속하게 복구를 수행하도록 백업 체계도 마련하는가?	<ul style="list-style-type: none"> ·백업 관리대상 ·백업 절차서 	
6.2.3.		서비스 가용성에 대한 영향 평가를 주기적으로 점검하는가?	<ul style="list-style-type: none"> ·DR 서비스 계약서 ·서비스 연속성 계획 ·비즈니스 영향 평가 ·자산 목록 ·네트워크/시스템 구성도 ·DR 소개 자료 및 이용자 매뉴얼 	
7. 준거성	7.1. 법 및 정책 준수	7.1.1.	정보보호 관련 법적 요구사항을 식별하고 준수하는가?	<ul style="list-style-type: none"> ·식별된 법적 요구사항 및 검토 결과
		7.1.2.	정보보호 정책 및 서비스 수준 협약에 포함된 보안 요구사항을 식별하고 준수하며 이용자가 요구하는 경우 관련 증거를 제공하는가?	<ul style="list-style-type: none"> ·정보보호 정책서 ·계약서, 서비스 준수 협약서 ·식별된 보안요구사항 준수 여부 검토 결과
	7.2. 보안 감사	7.2.1.	법적 요구사항 및 정보보호 정책 준수 여부를 보증하기 위해 독립적 보안감사 계획을 수립하여 시행하고 개선 조치를 취하는가?	<ul style="list-style-type: none"> ·보안감사 계획서 ·보안감사결과보고서 ·보안감사이행조치결과서
		7.2.2.	보안감사 증거(로그)은 식별할 수 있는 형태로 기록 및 모니터링 되어야 되고 비인가된 접근 및 변조로부터 보호되는가?	<ul style="list-style-type: none"> ·보안감사 로그 유형, 보존기간 등 현황 ·로그 백업 대장 ·로그기록 백업매체 관리 증거 ·로그기록 검토/보고 증거

○ 물리적 보호조치

분류	항목	점검내용	증적자료	
8. 물리적 보안	8.1. 물리적 보호 구역	8.1.1.	중요 정보 및 정보처리시설을 보호하기 위한 물리적 보안 구역(예 : 주요 정보처리 설비 및 시스템 구역, 사무실, 외부인 접근실 등)을 지정하였는가?	<ul style="list-style-type: none"> ·보호구역 지정 현황 ·보호구역 물리적 보안대책 ·시스템 구성도(물리적 구성 확인 가능)
			지정된 각 보안 구역에 대한 보안 대책을 마련하는가?	
	8.1.2.	물리적 보안 구역에 인가된 자만이 접근할 수 있도록 출입을 통제하는 시설(예 : 경비원, 출입 통제 시스템 등)을 갖추었는가?	<ul style="list-style-type: none"> ·보호구역 지정 현황 ·보호구역 물리적 보안대책 ·보호구역 인가자 목록 ·출입관리대장 ·출입카드 발급현황 ·출입자 이력 검토 증거 	
		통제된 시설에 대한 출입 및 접근 이력을 주기적으로 검토하는가?		
8.1.3.	유지보수 등 주요 정보처리 설비 및 시스템이 위치한 보호구역 내에서의 작업 절차를 수립하고 작업에 대한 기록을 주기적으로 검토하여야 한다.	<ul style="list-style-type: none"> ·보호구역 내 작업 절차 ·작업 신청서 ·출입관리대장(출입카드발 		

			<ul style="list-style-type: none"> 급현황 등) ·작업 기록서 ·통제구역 CCTV 배치도 ·모바일기기 반출입관리 대장(백신 등)
	8.1.4.	사무실 및 설비 공간에 대한 물리적인 보호방안을 수립하고 적용하는가?	<ul style="list-style-type: none"> ·공공 사무기기 현황 및 보호대책 ·공용 업무환경 보안 관리자 지정 ·공용업무환경 점검 내역
	8.1.5.	공공장소 및 운송·하역을 위한 구역은 내부 정보처리시설로부터 분리 및 통제하는가?	<ul style="list-style-type: none"> ·공공장소(접견구역, 회의실 등) 및 운송 하역 구역 현황 ·출입통제 대책
	8.1.6.	노트북 등 모바일 기기 미승인 반출입을 통한 중요정보 유출, 내부망 악성코드 감염 등의 보안사고 예방을 위하여 보호구역 내 임직원 및 외부인력 모바일 기기 반출입 통제절차를 수립하고 기록·관리하는가?	<ul style="list-style-type: none"> ·모바일기기 반출입 통제 절차 (백신 설치, 카메라 보안 실패 등 포함) ·모바일기기 반출입 신청서 및 승인 문서 ·모바일기기 반출입 이력 검토 내역
8.2. 정보처리시설 및 장비 보호	8.2.1.	물리적 및 환경적 위험으로부터 잠재적 손상을 최소화하고 비인가 된 접근 가능성을 최소화하기 위하여, 정보처리시설 내 장비의 위치를 파악하고 배치하는가?	<ul style="list-style-type: none"> ·정보자산 배치도 ·정보자산 목록
	8.2.2.	각 보안 구역의 중요도 및 특성에 따라 화재, 누수, 전력 이상 등 자연재해나 인재에 대비하여 화재 감지기, 소화 설비, 누수 감지기, 항온 항습기, 무정전 전원 장치(UPS), 이중 전원선 등의 설비를 갖추고 있는가?	<ul style="list-style-type: none"> ·보호설비 운영 절차 및 기준 ·보호구역 내 설비 현황 ·정보자산 목록 ·위탁운영업체의 물리적 보호설비에 대한 정기운영점검결과 ·물리적 보호설비 주기적 검토 내역
	8.2.3.	데이터를 송수신하는 통신케이블이나 전력을 공급하는 전력 케이블은 손상이나 도청으로부터 보호하는가?	·전력 및 통신케이블 보호 대책
	8.2.4.	정보처리시설은 가용성과 무결성을 지속적으로 보장할 수 있도록 유지보수 하는가?	·보호구역 내 시설 및 장비 정기점검 내역
	8.2.5.	장비의 미승인 반출·입을 통한 중요정보 유출, 악성코드 감염 등의 침해 사고 예방을 위하여, 보안 구역 내 직원 및 외부 업무 관련자에 의한 장비 반출·입 절차를 수립하고, 기록 및 관리하는가?	<ul style="list-style-type: none"> ·보호구역 내 장비 등 반출입 절차 ·반출입 신청서 ·반출입 관리 대장
	8.2.6.	정보처리시설 내의 저장 매체를 포함하여 모든 장비를 파악하고, 민감한 데이터가 저장된 장비를 폐기하는 경우 복구 불가능하도록 하는가?	<ul style="list-style-type: none"> ·저장매체 폐기 절차 ·저장매체 데이터 삭제 관련 증적
		재사용하는 경우에도 복구 불가능 상태에서 재사용하는가?	<ul style="list-style-type: none"> ·공공용 저장매체 재사용 시 보관 관련 증적 ·저장매체 폐기 관리대장 ·폐기 확인 증적

○ 기술적 보호조치

분류	항목	점검내용	증적자료
9. 가상화 보안	9.1. 가상화 인프라	9.1.1. 가상자원(가상 머신, 가상 스토리지, 가상 소프트웨어 등)의 생성, 변경, 회수 등에 대한 관리 방안을 수립하는가?	<ul style="list-style-type: none"> ·가상자원 관리 절차 및 방법 ·가상자원점검내역 ·이용자가상자원완전삭제 관련증적
	9.1.2.	이용자와의 계약 종료 시 가상자원 회수 절차에 따라 백업을 포함한 모든 클라우드 시스템에서 삭제하는가?	<ul style="list-style-type: none"> ·계약서 및 SLA ·이용자가상자원회수절차 ·이용자가상자원완전삭제

			기법설명증적	
	9.1.3.	가상자원에 대한 무결성 보장하기 위한 보호조치 및 가상자원의 변경(수정, 이동, 삭제, 복사)에 대해 모니터링하는가? 가상자원에 손상이 발생한 경우 이를 이용자에게 알려주는가?	<ul style="list-style-type: none"> 가상자원 무결성 보장 방안 (보호조치 및 모니터링) 가상자원 모니터링결과 손상발견시이용자통지절차 	
	9.1.4.	가상자원을 관리하는 하이퍼바이저의 기능 및 인터페이스에 대한 접근 통제 방안을 마련하는가? 하이퍼바이저에 대한 소프트웨어 업데이트 및 보안패치를 최신으로 유지하는가?	<ul style="list-style-type: none"> 하이퍼바이저 접근통제 및 보호대책 방안 하이퍼바이저접근기록검토증적 	
	9.1.5.	가상자원을 제공하기 위한 웹사이트와 가상소프트웨어(앱, 응용프로그램)를 배포하기 위한 공개서버에 대한 물리적, 기술적 보호대책을 수립하는가?	<ul style="list-style-type: none"> 네트워크 및 시스템 구성도 보안시스템운영현황 취약점점검및조치현황 	
	9.1.6.	클라우드컴퓨팅서비스 제공자는 표준화된 가상화 포맷, 이식성이 높은 가상화 플랫폼, 공개 API 등을 이용하여 클라우드컴퓨팅서비스 간의 상호 운용성 및 이식성을 높이는가? 클라우드컴퓨팅서비스 제공자는 클라우드컴퓨팅서비스 간의 상호 운용성 및 이식성을 높이기 위해 표준화된 가상화 포맷, 이식성이 높은 가상화 플랫폼, 공개 API 등을 이용하는가?	<ul style="list-style-type: none"> 가상화보안관리지침 클라우드상호운영/이식성제공방안(가상화포맷, 플랫폼,API등) 	
	9.2.1.	바이러스, 웜, 트로이목마 등의 악성코드로부터 이용자의 가상 환경(가상PC, 가상 서버, 가상 소프트웨어 등)을 보호하기 위한 악성코드 탐지, 차단 등의 보안기술을 지원하는가? 이상 징후 발견 시 이용자 통지하고 사용 중지 및 격리 조치를 수행하는가?	<ul style="list-style-type: none"> 정보자산 목록 (백신, 웹헬탐지, 웹방화벽 등 설치된 악성코드 통제 보안시스템 목록) 이상징후발견시통지및조치절차 	
	9.2.2.	가상 환경(가상PC, 가상 서버, 가상 소프트웨어 등) 접근을 위한 인터페이스 및 API에 대한 보안 취약점을 주기적으로 분석하고, 이에 대한 보호방안을 마련하는가?	<ul style="list-style-type: none"> 가상 환경 인터페이스(API) 취약점 점검 및 조치 현황 	
	9.2.3.	이용자가 기존 정보시스템 환경에서 클라우드컴퓨팅서비스의 가상 환경으로 전환 시 안전하게 데이터를 이전하도록 암호화 등의 기술적인 조치방안을 제공하는가?	<ul style="list-style-type: none"> 전송구간 암호화 솔루션 운영 현황(예: VPN 등) 데이터 이전 시 보안대책 	
	9.2.4.	클라우드컴퓨팅서비스 제공자는 출처, 유통경로 및 제작자가 명확한 소프트웨어로 구성된 가상환경을 제공하는가?	<ul style="list-style-type: none"> 정보자산목록 (가상 환경 관련 소프트웨어) 소프트웨어패치관리대장 공공기관 제공 필수SW현황 	
10. 접근 통제	10.1. 접근 통제 정책	10.1.1	비인가자의 접근을 통제할 수 있도록 접근통제 영역 및 범위, 접근통제 규칙, 방법 등을 포함하여 접근통제 정책을 수립하는가?	<ul style="list-style-type: none"> 접근통제 정책 및 방안 관리자단말기현황
		10.1.2	접근기록 대상을 정의하고 서비스 통제, 관리, 사고 발생 책임 추적성 등을 보장할 수 있는 형태로 기록되고 유지하는가?	<ul style="list-style-type: none"> 접근기록 생성 대상 목록 접근기록검토내역(보안로그)
	10.2. 접근 권한 관리	10.2.2	클라우드 시스템 및 중요정보에 대한 접근을 통제하기 위하여 공식적인 사용자 등록 및 해지 절차를 수립하는가? 업무 필요성에 따라 사용자 접근권한을 최소한으로 부여하는가?	<ul style="list-style-type: none"> 사용자 계정 등록, 변경, 삭제 승인 절차 및 승인 내역 접근권한분류체계 접근권한부여기록
		10.2.3	클라우드 시스템 및 중요정보 관리 및 특수 목적을 위해 부여한 계정 및 권한을 식별하고 별도 통제하여야 한다.	<ul style="list-style-type: none"> 사용자 계정 등록, 변경, 삭제 승인 내역 접근권한부여기록 특수권한자목록 외부자에게부여된계정목록
		10.2.4	클라우드 시스템 및 중요정보에 대한 접근을 관리하기 위하여 접근권한 부여, 이용(장기간 미사용), 변경(퇴직 및 휴직, 직무변경, 부서변경)의 적정성 여부를 정기적으로 점검하여야 한다.	<ul style="list-style-type: none"> 접근권한 검토 이력 (접근권한 점검대장) 이상징후 발견 시 조치절차
		10.3. 사용자	10.3.1	클라우드 시스템에서 사용자를 유일하게 구분할 수 있는 식별자를 할당하고 추측 가능한 식별자 사용을 제한하는가?

	식별 및 인증		동일한 식별자를 공유하여 사용하는 경우 그 사유와 타당성을 검토하고 책임자의 승인을 받는가?	·공용계정 발급 승인내역
		10.3.2	클라우드 시스템에 대한 접근은 사용자 인증, 로그인 횟수 제한, 불법 로그인 시도 경고 등 안전한 사용자 인증 절차에 의해 통제하는가?	·사용자 인증 화면 ·로그인 횟수 제한 설정 또는 제한된 화면 ·불법 로그인 시도 경고화면 ·강화된 인증 수단 제공화면
		10.3.3	이용자가 클라우드컴퓨팅서비스에 대해 다중 요소 인증 등 강화된 인증 수단을 요청하는 경우 이를 제공하기 위한 방안을 마련하는가?	·추가 인증수단 적용 화면 (OTP,전자우편인증등)
		10.3.4	법적 요구사항, 외부 위협요인 등을 고려하여 패스워드 복잡도 기준, 초기 패스워드 변경, 변경주기 등 사용자 패스워드 관리절차를 수립·이행하고 패스워드 관리 책임이 사용자에게 있음을 주지시키는가?	·패스워드 관리 절차 ·패스워드복잡도설정,변경 주기등설정화면
			관리자 패스워드는 별도 보호대책을 수립하여 관리하는가?	·시스템관리자패스워드관리대장
10.3.5	고객, 회원 등 외부 이용자가 접근하는 클라우드 시스템 또는 웹서비스의 안전한 이용을 위하여 계정 및 패스워드 등의 관리절차를 마련하고 관련 내용을 공지하는가?	·패스워드 관리 절차 ·패스워드복잡도설정,변경 주기등설정화면 ·이용자계정및패스워드관리방법및절차공지		
11. 네트워크 보안	11.1. 네트워크 보안	11.1.1	클라우드컴퓨팅서비스와 관련된 내·외부 네트워크에 대해 보안 정책과 절차를 수립하는가?	·정보자산목록 (IP정보 포함) ·네트워크구성도(IP정보포함) ·단말기접근통제방안 ·클라우드접속단말기지정현황 ·시스템원격접속현황및방법
		11.1.2	DDoS, 비인가 접속 등으로 인한 서비스 중단 및 중요 정보 유출 등을 막기 위해 네트워크를 모니터링하고 통제하는가?	·정보자산목록 (IP정보 포함) ·네트워크구성도 ·네트워크 모니터링 시스템 ·네트워크모니터링위탁시 계약서,SLA등
		11.1.3	클라우드컴퓨팅서비스와 관련된 내·외부 네트워크를 보호하기 위하여 정보보호시스템(방화벽, IPS, IDS, VPN 등)을 운영하는가?	·정보자산목록 (정보보호시스템) ·네트워크구성도 ·정보보호시스템관리자및 관리자PC현황 ·정보보호시스템로그 ·정보보호시스템정책관리절차 ·정보보호 시스템 정책타당성 검토 현황
		11.1.4	클라우드 시스템에서 중요 정보가 이동하는 구간에 대해서는 암호화된 통신채널을 사용하는가?	·클라우드 서비스 내에 암호화 통신 채널 사용 현황 (대상, 방법, 알고리즘 등)
		11.1.5	클라우드컴퓨팅서비스 제공자의 관리 영역과 이용자의 서비스 영역, 이용자 간 서비스 영역의 네트워크 접근은 물리적 또는 논리적으로 분리하는가?	·네트워크 구성도 (네트워크 분리 및 연계 방법)
		11.1.6	클라우드 시스템은 무선망과 분리하고, 무선접속에 대한 접근을 통제하는가?	·네트워크 구성도 ·무선네트워크 현황 ·무선네트워크 보호대책 ·무선네트워크 사용절차 ·주요단말기 지정현황(IP 정보포함)
			무선접속을 사용하는 경우 그 사유와 타당성을 검토하고 책임자의 승인을 받는가?	
12. 데이터 보호 및 암호화	12.1. 데이터 보호	12.1.1	데이터 유형, 법적 요구사항, 민감도 및 중요도에 따라 데이터를 분류하고 관리하는가?	·데이터 분류표 ·데이터 중요도 평가기준 ·데이터 흐름도/흐름표 ·데이터 현황/목록
		12.1.2	이용자와 서비스 수준 협약 단계에서 데이터의 소유권을 명확하게 확립하는가?	·클라우드서비스 제공 계약서, 약관, SLA 등
		12.1.3	입·출력, 전송 또는 데이터 교환 및 저장소의 데이터에 대해 항상 데이터	·데이터 무결성 조치 기술

			무결성을 확인하는가?	<ul style="list-style-type: none"> *시스템설계서등 •데이터흐름도/흐름표상의 무결성 보장 방안
		12.1.4	데이터에 대한 접근제어, 위·변조 방지 등 데이터 처리에 대한 보호 기능을 이용자에게 제공하는가?	<ul style="list-style-type: none"> •데이터 분류표 •데이터 중요도 평가기준 •데이터 현황 •데이터 보호 조치 기술 •시스템 설계서
		12.1.5	이용자에게 데이터를 추적하기 위한 방안을 제공하고, 이용자가 요구하는 경우 구체적인 제공정보(이용자의 정보가 저장되는 국가의 명칭 등)를 공개하는가?	<ul style="list-style-type: none"> •클라우드서비스 제공 계약서, SLA 등 •클라우드서비스 이용 홈페이지 화면(시스템으로 메커니즘구현시)
		12.1.6	클라우드컴퓨팅서비스 종료, 이전 등에 따른 데이터 폐기 조치 시 이용자와 관련된 모든 데이터를 폐기하며, 폐기된 데이터를 복구할 수 없도록 삭제 방안을 마련하는가?	<ul style="list-style-type: none"> •클라우드서비스 제공 계약서, 약관, SLA 등 •데이터 폐기 관련 기법/기술 * 시스템설계서등
	12.2 매체 보안	12.2.1	중요정보를 담고 있는 하드디스크, 스토리지 등의 저장매체 폐기 및 재사용 절차를 수립하고 매체에 기록된 중요정보는 복구 불가능하도록 완전히 삭제하는가?	<ul style="list-style-type: none"> •저장매체 처리 절차 및 방법 •저장매체 폐기 관리대장 •저장매체 용역계약서 및 확인서 •저장매체 폐기 확인증적
12.2.2		중요정보 유출을 예방하기 위해 외장하드, USB, CD 등 이동매체 취급, 보관, 폐기, 재사용에 대한 절차를 수립하는가?	<ul style="list-style-type: none"> •이동저장매체 관리절차서 •이동저장매체 관리대장 •이동저장매체 사용신청서 •이동저장매체 실태점검이력 	
		매체를 통한 악성코드 감염 방지 대책을 마련하는가?		
	12.3. 암호화	12.3.1	클라우드컴퓨팅서비스에 저장 또는 전송 중인 데이터를 보호하기 위해 암호화 대상, 암호 강도(복잡도), 키관리, 암호 사용에 대한 정책을 마련하는가?	<ul style="list-style-type: none"> •암호화 정책 •암호화 대상 및 방법
		정책에는 개인정보 저장 및 전송 시 암호화 적용 등 암호화 관련 법적 요구사항을 반드시 반영하는가?	<ul style="list-style-type: none"> •시스템 설계서 •시스템 변경 내역서 •보안요구사항 정의/반영 절차 	
12.3.2		암호키 생성, 이용, 보관, 배포, 파기에 관한 안전한 절차를 수립하고, 암호키는 별도의 안전한 장소에 보관하는가?	<ul style="list-style-type: none"> •암호화키 관리 절차 •암호화키 관리대장 •암호화키 소산 백업 	
13. 시스 템 개 발 및 도 입 보 안	13.1. 시스 템 분 석 및 설 계	13.1.1	신규 시스템 개발 및 기존 시스템 변경 시 정보보호 관련 법적 요구사항, 최신 보안취약점, 정보보호 기본요소(기밀성, 무결성, 가용성) 등을 고려하여 보안요구사항을 명확히 정의하고 이를 적용하는가?	<ul style="list-style-type: none"> •시스템 설계서 •시스템 변경 내역서 •보안요구사항 정의/반영 절차 •사용자 인증 기능 •중요데이터 전송 및 보관 시 적용기술/기법
		13.1.2	클라우드 시스템 설계 시 사용자 인증에 관한 보안요구사항을 반드시 고려하는가?	<ul style="list-style-type: none"> •시스템 설계서 •시스템 변경 내역서 •보안요구사항정의/반영절차 •사용자 인증 기능 •중요데이터 전송 및 보관 시 적용기술/기법
			중요정보의 입·출력 및 송수신 과정에서 무결성, 기밀성이 요구될 경우 법적 요구사항을 고려하는가?	
		13.1.3	클라우드 시스템 설계 시 사용자의 인증, 권한 변경, 중요정보 이용 및 유출 등에 대한 감사증적을 확보할 수 있도록 하는가?	<ul style="list-style-type: none"> •시스템 설계서 •시스템변경내역서 •보안요구사항정의/반영절차 •시스템감사증적생성및보호기능
		13.1.4	클라우드 시스템 설계 시 업무의 목적 및 중요도에 따라 접근권한을 부여할 수 있도록 하는가?	<ul style="list-style-type: none"> •시스템 설계서 •시스템변경내역서 •보안요구사항정의/반영절차 •시스템접근권한부여기능
		13.1.5	로그기록의 정확성을 보장하고 법적인 자료로서 효력을 지니기 위해 클라우드 시스템 시각을 공식 표준시각으로 정확하게 동기화 하는가? 또한 서비스 이용자에게 시각 정보 동기화 기능을 제공하는가?	<ul style="list-style-type: none"> •시스템 설계서 •시스템변경내역서 •보안요구사항정의/반영절차

				·시스템표준시각동기화설정
13.2. 구현 및 시험	13.2.1	·	안전한 코딩방법에 따라 클라우드 시스템을 구현하고, 분석 및 설계 과정에서 도출한 보안요구사항이 정보시스템에 적용되었는지 확인하기 위하여 시험을 수행하는가?	·시큐어 코딩 기준 ·보안요구사항충족시험증적
	13.2.2	·	개발 및 시험 시스템은 운영시스템에 대한 비인가 접근 및 변경의 위험을 감소하기 위해 원칙적으로 분리하는가? 단 분리하여 운영하기 어려운 경우 그 사유와 타당성을 검토하고 안전성 확보 방안을 마련하는가?	·개발/시험 및 운영 네트워크 구성도 ·운영환경이관절차
	13.2.3	·	시스템 시험 과정에서 운영데이터 유출을 예방하기 위해 시험데이터 생성, 이용 및 관리, 파기, 기술적 보호조치에 관한 절차를 수립하여 이행하는가?	·시험데이터 관리 절차 ·운영데이터의시험환경사용여부 ·운영전시험데이터및시험계정삭제여부
	13.2.4	·	소스 프로그램에 대한 변경관리를 수행하고 인가된 사용자만이 소스 프로그램에 접근할 수 있도록 통제절차를 수립하여 이행하는가? 소스 프로그램은 운영환경에 보관하지 않는 것을 원칙으로 하는가?	·소스코드 관리 절차 ·소스코드 관리 방법 *소스코드권한관리및접근통제
13.3. 외주 개발 보안	13.3.1	·	클라우드 시스템 개발을 외주 위탁하는 경우 분석 및 설계단계에서 구현 및 이관까지의 준수해야 할 보안요구사항을 계약서에 명시하고 이행여부를 관리·감독하는가?	·외주 개발 제안요청서/계약서 ·보안요구사항점검증적 ·검수(인수)확인서
13.4. 시스템 도입 보안	13.4.1	·	클라우드 시스템의 처리 속도와 용량에 대하여 주기적인 모니터링을 수행하고 안정성의 확보에 필요한 시스템 도입 계획을 수립하는가?	·시스템 도입 계획서
	13.4.2	·	새로 도입되는 시스템에 대한 인수 기준이 수립되며, 인수 전에 테스트가 수행되는가?	·시스템 인수 기준 ·검수(인수)확인서

양식4

laaS 및 인프라 취약점 점검 및 모의침투 테스트 수행 확인서

laaS 및 인프라 취약점 점검 및 모의침투 테스트 수행 확인서

집적정보통신시설	사업자명		
	구분	<input type="checkbox"/>	단순 외부보관
		<input type="checkbox"/>	클라우드 기반 외부보관
구분	취약점 점검	모의침투 테스트	
수행기관			
수행대상			
수행기간			
수행결과	<input type="checkbox"/> 점검결과 발견된 취약점 조치 완료 <input type="checkbox"/> 점검결과 발견된 취약점 조치 미완료 (미완료 시 사유 :)		

상기와 같이 취약점 점검 및 모의침투 테스트를 수행하였으며, 발견된 취약점에 대해 적절히 조치하였음을 확인합니다.

년 월 일

집적정보통신시설 사업자(대표자)

(서명 또는 인)

재단법인 한국보건의료정보원 귀중

※ 집적정보통신시설의 취약점 점검 및 모의침투 테스트 수행 결과는 1년 이내 수행한 내역에 한해 유효

양식5**SaaS 및 SW 취약점 점검 및 모의침투 테스트 수행 확인서****SaaS 및 SW 취약점 점검 및 모의침투 테스트 수행 확인서**

전자의무기록시스템	사업자명		
	제품명		
구분	취약점 점검	모의침투 테스트	
수행기관			
수행대상			
수행기간			
수행결과	<input type="checkbox"/> 점검결과 발견된 취약점 조치 완료 <input type="checkbox"/> 점검결과 발견된 취약점 조치 미완료 (미완료 시 사유 :)		

상기와 같이 취약점 점검 및 모의침투 테스트를 수행하였으며, 발견된 취약점에 대해 적절히 조치하였음을 확인합니다.

년 월 일

전자의무기록시스템 인증신청 기관장(대표자)

(서명 또는 인)

재단법인 한국보건 의료정보원 귀중

※ 집적정보통신시설의 취약점 점검 및 모의침투 테스트 수행 결과는 1년 이내 수행한 내역에 한해 유효

양식6

집적정보통신시설 사업자 제출자료 적합성 확인서

집적정보통신시설 사업자 제출자료 적합성 확인서

신청기관		
신청기관 형태	<input type="checkbox"/> 민간 의료기관	<input type="checkbox"/> 공공 의료기관
집적정보통신시설 사업자		
외부보관 방식	<input type="checkbox"/> 단순 외부보관	<input type="checkbox"/> 클라우드 기반 외부보관
	※ 「전자의료기록의 관리보존에 필요한 시설과 장비에 관한 기준」 제7조 참고 ※ 클라우드 형태의 경우 아래 클라우드 서비스 현황 확인	
적합성 항목 (해당항목에 √ 표시)	서비스 제공 구분	<input type="checkbox"/> 집적정보통신시설
		<input type="checkbox"/> 클라우드컴퓨팅기술 기반 집적정보통신시설
	보안인증	<input type="checkbox"/> ISMS-P(또는 ISMS) 정보보호 및 개인정보보호 관리체계, 한국인터넷진흥원(KISA)
		<input type="checkbox"/> ISO 27017 클라우드서비스 정보보안 인증, ISO/IEC
		<input type="checkbox"/> ISO 27018 클라우드서비스 개인정보보호 인증, ISO/IEC
		<input type="checkbox"/> CSAP - IaaS 클라우드 보안인증, 한국인터넷진흥원(KISA)
	EMR 점검표	<input type="checkbox"/> EMR 점검표 EMR 시설장비 기준 고시의 전체 또는 일부 항목별 점검표 및 증빙자료
	클라우드 점검표	<input type="checkbox"/> 클라우드 점검표 클라우드컴퓨팅 서비스 정보보호 기준 고시의 관리적, 물리적, 기술적 조치 항목별 점검표 및 증빙자료
수행 확인서	<input type="checkbox"/> 취약점 점검 수행 확인서 IaaS(또는 인프라) 취약점 점검 수행 확인서	
	<input type="checkbox"/> 모의침투 테스트 수행 확인서 IaaS(또는 인프라) 모의침투 테스트 수행 확인서	

참고1

일부 인증기준 항목에 대한 심사 면제

□ 관련근거

- 전자의무기록시스템 인증 제도 운영에 관한 고시(보건복지부 고시 제2021-2호) 제10조(인증기준)

제10조(인증기준) ① 인증기관의 장은 전자의무기록시스템 인증기준을 인증위원회의 심의 및 보건복지부장관의 승인을 거쳐 홈페이지 등에 공개하여야 한다.

② 인증기관의 장은 인증 심사에 있어 일부 인증기준 항목에 대해서는 심사를 면제할 수 있다. 다만, 면제와 관련한 사항은 보건복지부장관의 승인을 받아 홈페이지 등에 공개하여야 한다.

□ 면제사항

- (승인근거) 의료정보정책과-1539(2020.7.14., 「전자의무기록(EMR)시스템 인증제」 심사 면제 인증기준 항목 승인)
- (면제사항)

주관기관	타 인증제·사업		EMR 인증제(제품인증)	
	인증 프로그램·사업	대상	면제대상	면제 인증기준
한국보건 의료정보원	진료정보교류사업	의료기관	개발업체, 자체개발 의료기관*	I001-I010 상호운용성 인증기준 전체
한국 인터넷 진흥원	정보보호관리체계(ISMS)	의료기관	자체개발 의료기관	S009, S012, S014를 제외한 보안성 인증기준 전체
	정보보호및개인정보보호 관리체계(ISMS-P)	의료기관	자체개발 의료기관	S012, S014를 제외한 보안성 인증기준 전체
	ISMS-P(또는 ISMS), 클라우드서비스 보안인증(CSAP)	집적정보통신 시설 사업자, 클라우드서비스 제공 업체	개발업체	S014 제1호 일부, 제2호 전부
ISO 인증기관	ISO 클라우드 보안인증(ISO 27017), ISO 클라우드 개인정보보호 인증(ISO 27018)			
건강보험 심사 평가원	청구소프트웨어 보안기능 검사인증	개발업체, 자체개발 의료기관	개발업체, 자체개발 의료기관	S008, S009, S012,S014를 제외한 보안성 인증기준 전체

* 진료정보교류사업에 참여하는 의료기관에 진료정보교류 시스템을 제공하는 EMR 개발업체·자체개발 의료기관

** 상세내용은 「의료기관 외부보관 EMR 인증심사 안내」 참조

- 국가·공공의료기관은 전자정부법 제2조의 제2항 ‘행정기관’, 제3항 ‘공공기관’의 정의를 따름

※ 전자정부법 제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.

1. “전자정부”란 정보기술을 활용하여 행정기관 및 공공기관(이하 “행정기관등”이라 한다)의 업무를 전자화하여 행정기관등의 상호 간의 행정업무 및 국민에 대한 행정업무를 효율적으로 수행하는 정부를 말한다.
2. “행정기관”이란 국회·법원·헌법재판소·중앙선거관리위원회의 행정사무를 처리하는 기관, 중앙행정기관(대통령 소속 기관과 국무총리 소속 기관을 포함한다. 이하 같다) 및 그 소속 기관, 지방자치단체를 말한다.
3. “공공기관”이란 다음 각 목의 기관을 말한다.
 - 가. 「공공기관의 운영에 관한 법률」 제4조에 따른 법인·단체 또는 기관
 - 나. 「지방공기업법」에 따른 지방공사 및 지방공단
 - 다. 특별법에 따라 설립된 특수법인
 - 라. 「초·중등교육법」, 「고등교육법」 및 그 밖의 다른 법률에 따라 설치된 각급 학교
 - 마. 그 밖에 대통령령으로 정하는 법인·단체 또는 기관

참고3

상용(商用) 클라우드컴퓨팅 서비스

- 클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 제2조(정의)의 제3항 “클라우드컴퓨팅서비스”란 클라우드컴퓨팅을 활용하여 상용(商用)으로 타인에게 정보통신 자원을 제공하는 서비스로서 대통령령으로 정하는 것을 말함
- 클라우드컴퓨팅법 제21조에서 다른 법령에서 규정하고 있는 전산시설 등의 구비 요건을 대체할 수 있는 클라우드컴퓨팅서비스는 상용(商用)으로 제공되는 서비스 이어야 함
- 상용으로 타인에게 제공하는 클라우드컴퓨팅서비스여야 하므로 타인이 아닌 자기 스스로 이용을 위하여 구축한 전산시설등은 비록 클라우드컴퓨팅기술을 도입한 것이라도 이법의 클라우드 컴퓨팅서비스에 해당하지 않음
- 여기서 “상용”이란 무상·유상에 구애받지 않고 상업용으로 제공되는 것을 의미하므로 무상으로 제공되는 클라우드컴퓨팅서비스라도 상용으로 제공되고 있다면 포함될 수 있음. 무상으로 클라우드컴퓨팅서비스를 제공하더라도 광고를 통해서 수익을 올리고 있다면 상용에 해당함
- 반면 전산시설등의 사용 수수료를 내더라도 상용(商用)으로 제공되는 클라우드컴퓨팅서비스가 아니라면 이 법에서 말하는 클라우드컴퓨팅서비스에 해당하지 않음
예컨대 협회, 단체 등이 전용으로 구축한 클라우드컴퓨팅서비스는 포함되지 않음

※ 클라우드컴퓨팅 주요법령 해설서(2017.11) 중 일부

② 클라우드컴퓨팅서비스의 범위

○ 클라우드컴퓨팅서비스의 개념

- 법 제21조에서 다른 법령에서 규정하고 있는 전산시설등의 구비 요건을 대체할 수 있는 클라우드컴퓨팅서비스는 상용(商用)으로 제공되는 서비스여야 됩니다.
- 법 제2조 제3호가 클라우드컴퓨팅서비스를 ‘클라우드컴퓨팅을 활용하여 상용으로 타인에게 정보통신자원을 제공하는 서비스’로 정의하고 있기 때문입니다.
- 상용으로 타인에게 제공하는 클라우드컴퓨팅서비스여야 하므로 타인이 아닌 자기 스스로 이용을 위하여 구축한 전산시설등은 비록 클라우드컴퓨팅기술을 도입한 것이라도 이법의 클라우드 컴퓨팅서비스에 해당하지 않습니다.
- 여기서 “상용”이란 무상·유상에 구애받지 않고 상업용으로 제공되는 것을 의미하므로 무상으로 제공되는 클라우드컴퓨팅서비스라도 상용으로 제공되고 있다면 포함될 수 있습니다. 무상으로 클라우드컴퓨팅서비스를 제공하더라도 광고를 통해서 수익을 올리고 있다면 상용에 해당합니다.
- 반면 전산시설등의 사용 수수료를 내더라도 상용(商用)으로 제공되는 클라우드컴퓨팅서비스가 아니라면 이 법에서 말하는 클라우드컴퓨팅서비스에 해당하지 않습니다. 예컨대 협회, 단체 등이 전용으로 구축한 클라우드컴퓨팅서비스는 포함되지 않습니다.

○ 클라우드컴퓨팅서비스의 유형

- 클라우드컴퓨팅서비스는 서비스의 운영 방식 배치 모델에 따라 일반적으로 1) 프라이빗 클라우드컴퓨팅서비스, 2)퍼블릭 클라우드컴퓨팅서비스, 3) 커뮤니티 클라우드컴퓨팅서비스, 4) 하이브리드 클라우드컴퓨팅서비스 등으로 나뉩니다.
- 이 중에서 상용으로 제공되는 클라우드컴퓨팅서비스는 주로 퍼블릭 클라우드컴퓨팅서비스입니다. 직접 개발·구축·운영·관리하는 경우에는 원칙적으로 이 법에서 규정하고 있는 클라우드컴퓨팅서비스에 해당하지 않습니다.
- 커뮤니티 클라우드컴퓨팅서비스나 하이브리드 클라우드컴퓨팅서비스도 서비스의 배치 및 운영 방식만 다를 뿐 상용으로 제공이 가능하므로 상용으로 제공·이용되고 있는 한, 이 법에서 규정하고 있는 클라우드컴퓨팅서비스에 포함될 수 있습니다.
- 커뮤니티, 하이브리드 등의 방식으로 구축된 클라우드시스템이라도 서비스의 전부 또는 일부를 클라우드컴퓨팅서비스 제공자가 유상으로 제공하고 있다면 그 범위 내에서 제21조에서 규정하고 있는 클라우드컴퓨팅서비스로 볼 수 있습니다.

※ 금융분야 클라우드컴퓨팅서비스 이용가이드 발췌

FINANCIAL SECURITY INSTITUTE

제1장 평가 대상

☞ 「전자금융감독규칙」 개정안은 「클라우드컴퓨팅법」에서 정한 클라우드서비스 제공자를 평가대상으로 규정하고 있는 바,

- 금융회사가 제3자로부터 상용(商用)으로 제공받는 모든 유형^{*}의 클라우드 서비스 제공자가 평가대상에 해당

* IaaS, PaaS, SaaS

☞ 「클라우드컴퓨팅법」의 클라우드서비스 정의

[법 제2조(정의)] 이 법에서 사용하는 용어의 뜻은 다음과 같다.

3. "클라우드컴퓨팅서비스"란 클라우드컴퓨팅을 활용하여 상용(商用)으로 타인에게 정보통신자원을 제공하는 서비스로서 대통령령으로 정하는 것을 말한다.

[시행령 제3조(클라우드컴퓨팅서비스) 법 제2조 제3호에서 "대통령령으로 정하는 것"이란 다음 각 호의 어느 하나에 해당하는 서비스를 말한다.

1. 서버, 저장장치, 네트워크 등을 제공하는 서비스
2. 응용프로그램 등 소프트웨어를 제공하는 서비스
3. 응용프로그램 등 소프트웨어의 개발·배포·운영·관리 등을 위한 환경을 제공하는 서비스
4. 그 밖에 제1호부터 제3호까지의 서비스를 둘 이상 복합하는 서비스

☞ 이에, 금융회사가 자체 구축·운영(非상용 Private)하거나 상용이 아닌 클라우드서비스 제공자는 본 클라우드 규제 적용대상에 미 해당

- "상용" 여부의 판단은 과기정통부에서 제공하는 「클라우드컴퓨팅법 해설서」의 '상용' 기준 내용 등을 참고
- 다만, 이 경우 망분리 등 클라우드서비스 활용에 필요한 일부 규제의 예외를 인정받지 못할 수 있어 추진 시 고려 필요

☞ 과기정통부 「클라우드컴퓨팅법 해설서」의 '상용' 기준 내용(발췌)

'상용'이란 무상·유상에 구애받지 않고 상업용으로 제공되는 것을 의미하므로 무상으로 제공되는 클라우드컴퓨팅서비스라도 상용으로 제공되고 있다면 포함될 수 있습니다. 무상으로 클라우드컴퓨팅서비스를 제공하더라도 광고를 통해서 수익을 올리고 있다면 상용에 해당합니다.

반면, 전산시설등의 사용 수수료를 내더라도 상용(商用)으로 제공되는 클라우드컴퓨팅서비스가 아니라면 이 법에서 말하는 클라우드컴퓨팅서비스에 해당하지 아니합니다. 예컨대 협회, 단체 등이 전용으로 구축한 클라우드컴퓨팅서비스는 포함되지 않습니다.

94 금융보안원

④ 첨부4 클라우드서비스 이용 가이드 관련 FAQ

1. 고유식별정보 또는 개인신용정보를 처리하는 경우, 해당 정보를 처리하는 모든 시스템을 국내에 설치하도록 하고 있는데, 클라우드서비스 제공자의 관리시스템도 포함되나요?

⇒ 관련 시스템의 국내 설치 의무 여부는 “해당 정보의 처리 여부”에 따라 구분됩니다. 클라우드서비스 제공자의 관리시스템에서 고유식별정보 또는 개인신용정보가 일시적으로라도 처리된다면, 국내에 설치하여야 합니다. (감독규정 제14조의2제8항)

* “처리”는 개인정보의 수집, 생성, 연계, 이동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말합니다. (개인정보보호법 제2조제2호)

2. 개발망이나 SaaS 구축의 경우 내부망 시스템 및 단말기와 연결은 어떻게 구성되나요?

⇒ 개발망이나 SaaS 구축의 경우에도 본 가이드의 원칙이 동일하게 적용되며, 기존 내부망에 구축하던 업무용 시스템은 클라우드서비스 제공자 구간 내에서 인터넷과 논리적으로 분리된 내부망에 위치해야하며, 기존 개발망에 구축하던 개발용 시스템은 클라우드서비스 제공자 구간 내에서 논리적으로 구분된 개발망에 위치해야합니다.

3. 지주사 클라우드 이용 시에도 적용되나요?

⇒ 지주사가 비상용 프라이빗 클라우드를 구축하여 그 계열사가 이용하는 경우에는(감독규정 제11조제11호 및 제12호, 제15조제1항제5호 준수) 감독규정 제14조의2에서 부여하고 있는 의무 적용 대상이 아닙니다.

4. SaaS 사업자가 인증받은 IaaS를 기반으로 하고 있을 때, 별도 인증 또는 평가가 필요한가요?

⇒ SaaS가 해당 IaaS와 동일 수준의 보안 조치를 했다고 보기 어려우므로 별도 인증 또는 평가가 필요합니다.

참고4

취약점 점검 및 모의침투 테스트 도입 취지

- 전자의무기록 클라우드 (외부보관) 서비스 제공 사업자는 **관련 법령***에 따라 주기적으로 취약점을 점검 및 보완하여야 함

* (전자의무기록 외부보관 서비스)

- 전자의무기록 시설 장비 기준 고시 제6조(네트워크 및 전자의무기록 시스템 보안에 관한 시설과 장비 등) 전자의무기록 관리자는 불법적인 접근 및 침해사고를 방지하기 위하여 「의료법 시행규칙」(이하 "규칙"이라 한다) 제16조제1항제4호부터 제6호까지의 시설과 장비에 대하여 「개인정보보호법」 제29조에 따른 안전성 확보 조치를 하여야 한다.
- 개인정보 안전성 확보조치 기준고시 제6조(접근통제) ④ 고유식별정보를 처리하는 개인정보처리자는 인터넷 홈페이지를 통해 고유식별정보가 유출·변조·훼손되지 않도록 연 1회 이상 취약점을 점검하고 필요한 보안 조치를 하여야 한다.

* (전자의무기록 클라우드 서비스)

- 클라우드컴퓨팅서비스 정보보호에 관한 기준 고시 [별표1] 관리적 보호조치 3.3.2 (취약점 점검) 취약점 점검 정책에 따라 주기적으로 기술적 취약점(예: 유·무선 네트워크, 운영체제 및 인프라, 응용 프로그램 취약점 등)을 점검하고 보완하여야 한다.

- 이에 따라, EMR 인증 시 취약점 점검 수행 여부를 확인하고자 함

- (모의침투 테스트 시행 취지) 전자의무기록 시설 장비 기준 고시 제6조(네트워크 및 전자의무기록 시스템 보안에 관한 시설과 장비 등)와 클라우드컴퓨팅서비스 정보보호에 관한 기준 고시 [별표1] 관리적 보호조치 3.3.2(취약점 점검) 등은 클라우드컴퓨팅 서비스 제공 사업자 등이 준수해야 하는 기준이며, EMR 인증 시 취약점 점검 및 모의침투 테스트는 이를 근거로 진행되는 것이 아님

- 전자의무기록 외부 보관 서비스는 의료기관 외부에 민감한 의료정보를 관리하며 클라우드 서비스는 자원의 가상화 및 공유를 기반으로 하여 정보보안에 더욱 취약한 실정임
- 따라서 EMR 인증 심사 시, 보안사고에 실질적으로 대응할 수 있고 보안평가 방법론 측면에서 가장 적극적인 보안성 평가 방법인 모의침투 테스트를 취약점 점검과 함께 시행함

- * 한국인터넷진흥원의 클라우드 보안 인증(CSAP)에서도 취약점 점검 및 모의침투 테스트가 인증 심사의 대부분을 차지함

클라우드 상에서의 의료정보 유출 등 정보보안 문제 발생하면 기업의 존폐나 퇴출 뿐 아니라 의료 정보 활용 활성화의 근간이 흔들릴 수 있음

따라서, 민간 의료기관에 대해 외부보관 및 클라우드 보관을 허용하는 한편 의료정보의 안전성 확보를 위해 EMR 인증 시에 IaaS와 SaaS 등에 대한 자체 취약점 진단 및 모의 침투 테스트 절차를 수행할 필요 있음

- * 정보 보안에 소요되는 예산은 비용이 아니라 투자라는 측면에서 접근 필요

EMR 인증에서 클라우드 등에 대한 보안 심사를 강화함으로써 외부 및 클라우드 보관에 대한 신뢰성 제고와 클라우드 활용 활성화의 궁극적 효과를 기대할 수 있음

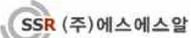
참고5

정보보호 전문 서비스 기업

※ EMR 인증 위한 취약점 점검 및 모의해킹 테스트 시 '정보보호 전문 서비스 기업'을 통해 수행하는 것을 권장

- 개요 : 주요 정보통신 기반시설의 취약점 분석·평가 업무 및 보호대책 수립 업무를 지원할 수 있는 전문서비스 기업을 지정하는 제도
- 법적 근거
 - 정보보호산업의 진흥에 관한 법률 제23조
 - 정보보호산업의 진흥에 관한 법률 시행규칙 제8조~제15조
 - 정보보호 전문서비스 기업 지정 등에 관한 고시(과학기술정보통신부 고시 제2017-24호)
- 정보보호 전문서비스 기업 지정 현황(28개 업체, 2022년 03월 기준)

(참고) <https://www.ksecurity.or.kr/kisis/subIndex/469.do>

참고6

클라우드 보안서비스 도입기준 변경 공지

□ 개요

- (주요 변경 내용) KISA 클라우드 보안인증을 획득한 클라우드 보안서비스 (SECaaS)는 CC인증 또는 보안기능 확인서가 없어도 각급기관에서 도입가능
 - ※ KISA 클라우드 보안인증서의 유효기간 확인 필수

구분	주요내용	
대상	- 웹방화벽 서비스, 스팸메일차단서비스 등 사전인증(CC인증 또는 보안기능확인서)이 필요한 정보보호제품을 포함하고 있는 클라우드 보안서비스	
시행기간	- 2021.6.14. ~ 2024. 12. 31	
주요내용	기존	변경내용
	- 사전인증 제품에 대해서 사전인증이 있어야만 신청가능	- 사전인증 제품에 대해서 사전인증이 없어도 신청가능

※ KISA 클라우드 보안인증 획득시 국가·공공기관 대상 보안적합성검증 생략 가능

□ 클라우드 보안서비스 도입기준 변경공지 원문 - 국가정보원

1. 각급기관의 원활한 클라우드 서비스 도입을 위해 클라우드 보안서비스 도입기준을 아래와 같이 한 시적으로 변경할 계획이오니 참고하시기 바랍니다.
 - * 클라우드 보안서비스(SECaaS, Security as a Service) : SaaS의 한 종류로 클라우드 환경에서 정보보호제품의 보안기능을 제공하는 서비스
- 가. 변경대상 : 웹방화벽서비스, 스팸메일차단서비스 등 사전인증(CC인증 또는 보안기능 확인서)이 필요한 정보보호제품을 포함하고 있는 클라우드 보안서비스
- 나. 시행기간 : 2021.6.14 ~ 2024.12.31.
- 다. 변경내용 : KISA 클라우드 보안인증이 유효한 민간 클라우드 보안서비스는 CC인증 또는 보안기능확인서가 없어도 각급기관에서 도입 가능
 - * 각급기관 자체 구축 클라우드는 해당되지 않음

※ 출처

https://www.nis.go.kr:4016/AF/1_7_2_3/view.do?seq=83¤tPage=1&selectBox=&searchKeyword=&fromDate=&toDate=