클라우드서비스 보안인증제 안내서

2019. 3.

과학기술정보통신부
Ministry of Science and ICT

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

문서이력

개정일	버전	내역	비고
2016.05	1.0	클라우드컴퓨팅서비스 보안인증제도 안내서	최초제정 (IaaS용)
2017.07	1.1	기관 주소 및 연락처 변경 인증사업자 보안관리 활동 추가 부처명 변경(미래창조과학부→과학기술정보통신부)	부분개정
2018.06	2.0	클라우드서비스 보안인증제 확대시행(IaaS→IaaS·SaaS)에 따른 SaaS 보안인증 기준 추가 및 수정	개정(IaaS·SaaS 통합용)
2019.03	2.1	행안부 민간 클라우드 이용 가이드라인 개정 내용 반영 SaaS 구축 절차 및 안내사항 등 추가	부분개정

CONTENTS

클라우드서비스 보안인증제 안내서

I

클라우드컴퓨팅서비스 보안인증제도

1. 보안인증제 개요
2. 보안 평가·인증체계
3. 기대효과

Ⅰ 클라우드컴퓨팅서비스 보안인증제도

1. 보안인증제 개요

클라우드컴퓨팅서비스(이하 '클라우드서비스') 보안인증제도는 클라우드서비스 제공자가 제공하는 서비스에 대해 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제23조 제2항에 따라 정보보호 기준의 준수여부 확인을 인증기관에 요청하는 경우 인증기관이 이를 평가·인증하여 이용자들이 안심하고 클라우드서비스를 이용할 수 있도록 지원하는 제도입니다.

목적 및 필요성

⇨ 공공기관에게 안전성 및 신뢰성이 검증된 민간 클라우드서비스 공급

⇨ 객관적이고 공정한 클라우드서비스 보안인증제를 실시하여 이용자의 보안 우려를 해소하고, 클라우드서비스의 경쟁력 확보

추진 근거

⇨ 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제5조에 의한 「제1차 클라우드컴퓨팅 기본계획」('15.11.10, 국무회의)에 따른 클라우드 서비스 보안인증제 시행

- **(보안인증)** 공공기관이 안전하게 민간 클라우드를 이용할 수 있도록 클라우드 보안인증제도 마련(국정원 · 과학기술정보통신부 · 행정안전부, '15년)

  ※ 공공기관 **보안지침**(국정원), 민간 클라우드 **보안인증제도**(과학기술정보통신부), **평가**(KISA) 등 보안인증체계를 마련하고 인증실시('16년~)

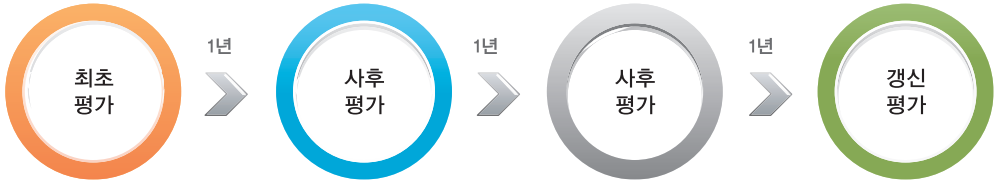
⇨ 「클라우드컴퓨팅서비스 정보보호에 관한 기준 고시」 제 7조에 따른 정보보호 기준의 준수여부 확인 (과학기술정보통신부 고시 제2017-7호)

《 클라우드컴퓨팅서비스 정보보호에 관한 기준 》

제7조(정보보호 기준의 준수여부 확인) 과학기술정보통신부장관은 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제5조에 따른 "기본계획"(2015년 12월 7일 확정, 정보통신전략위원회) 상의 "보안인증제" 시행을 위해 클라우드컴퓨팅서비스 제공자가 그 서비스가 이 기준을 준수하는지 확인을 요청한 경우에는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」제52조에 따른 "한국인터넷진흥원" 의 장이 그 서비스를 조사 또는 시험·평가하여 인증 할 수 있다.

평가·인증 종류

클라우드서비스 보안 평가·인증 종류는 최초평가, 사후평가, 갱신평가가 있습니다.



⇒ **최초평가**는 보안인증을 처음으로 취득할 때 진행하는 평가이며, 인증의 범위에 중요한 변경이 있어 다시 인증을 신청할 때에도 실시

※ 최초평가를 통해 인증을 취득하면, 3년의 유효기간을 부여

⇒ **사후평가**는 보안인증을 취득한 이후 지속적으로 클라우드서비스 보안 평가·인증 기준을 준수하고 있는지 확인하기 위한 평가이며, 인증 유효기간(3년) 안에 매년 1회 이상을 시행

⇒ **갱신평가**는 보안인증 유효기간(3년)이 만료되기 전에 클라우드서비스에 대한 인증의 연장을 원하는 경우에 실시하는 평가

※ 갱신평가를 통과하는 경우, 3년의 유효기간을 다시 부여

추진경과

⇒「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 시행('15.9.28)

⇒「클라우드컴퓨팅 정보보호 대책」 수립·발표('15.9.9, 경제관계장관회의)

⇒「제1차 클라우드컴퓨팅 기본계획」 수립·발표('15.11.10, 국무회의)

※ 공공부문 민간 클라우드 이용 촉진을 위한 제도 마련

⇒「클라우드컴퓨팅서비스에 대한 정보보호 기준 고시」 제정·시행('16.4.4)

※ 제7조(정보보호 기준의 준수여부 확인)에 따라 시험·평가 및 인증을 위한 근거 마련

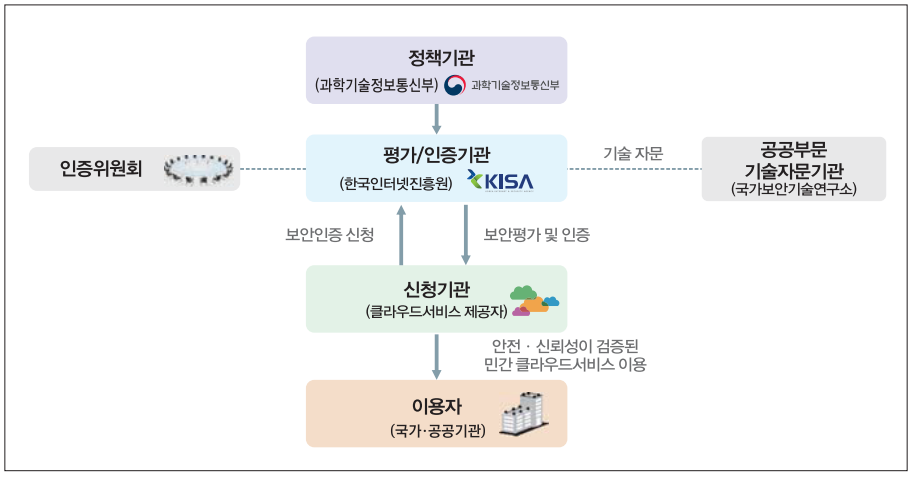
⇒ IaaS 대상 클라우드서비스 보안인증제도 시행('16.6.1)

⇒ 클라우드보안인증제 확대(IaaS → IaaS·SaaS) 시행('18.8.1)

2. 보안 평가·인증체계

클라우드서비스 보안 평가·인증체계는 역할과 책임에 따라 정책기관, 평가/인증기관, 인증위원회, 기술 자문기관, 신청기관, 이용자로 구분합니다.
정책기관은 과학기술정보통신부, 평가/인증기관은 한국인터넷진흥원, 공공부문 기술자문기관은 국가보안기술연구소에서 그 역할을 수행하고 있습니다.

조직 및 역할



구 분	주관기관	주요역할
정책기관	과학기술정보통신부	· 평가·인증 관련 법·제도 개선 및 정책 수립 · 평가/인증기관의 지정 및 감독
평가/인증기관	한국인터넷진흥원	· 평가·인증 신청접수 · 평가·인증기준, 지침 개발 · 평가를 통한 인증업무 수행 · 인증서 발급 및 인증된 클라우드서비스 관리
인증위원회	한국인터넷진흥원	· 평가결과를 통한 인증 심의·의결 · 인증취소의 타당성 심의 · 학계, 연구기관, 기술자문기관 등 클라우드 관련 전문가 5인 이상 10인 이내로 구성
기술자문기관	국가보안기술연구소	· 국가·공공기관 민간 클라우드서비스 이용 보안기준 마련 · 국가·공공 클라우드 안전성 강화 대책 수립
신청기관	클라우드사업자	· IaaS, SaaS 등 클라우드서비스 제공 · 자체 보안활동 정기·수시 수행

3. 기대효과

클라우드서비스 제공자(민간 사업자) 관점

⇨ 객관적이고 공정한 클라우드서비스 보안인증을 통해 **이용자 신뢰도 향상** 및 클라우드서비스 제공자의 **정보보호 수준 향상**

⇨ 클라우드서비스를 이용하는 **국가·공공기관의 정보화 사업에 입찰 참여 가능**

- 조달청 나라장터(종합쇼핑몰) 클라우드 카탈로그 상품 등록 가능

※ 국가·공공기관은 조달청 나라장터에 등록된 보안인증을 획득한 클라우드서비스 선택

클라우드서비스 이용자(국가·공공기관) 관점

⇨ 인증 받은 클라우드서비스를 이용함으로써, 클라우드 도입의 걸림돌인 **보안 우려를 해소하고, 안전한 클라우드서비스 구축 및 이용 활성화**

클라우드 보안인증 사업자 목록 확인

☞ 홈페이지(https://isms.kisa.or.kr) - 클라우드보안인증제 - 인증서 발급현황

인증의 홍보

⇨ 클라우드서비스 보안인증을 받은 자는 **인증 받은 내용을 문서·송장·광고 등에 표시**할 수 있으며, **클라우드서비스 보안인증 표시 사용** 가능

※ 보안인증을 표시할 경우, 평가·인증의 범위와 유효기간을 반드시 함께 표시하여야 함

클라우드서비스 보안인증의 의미

- 클라우드서비스 보안인증을 받은 사업자의 클라우드서비스가 100% 안전한 것은 아님
- 보안인증을 받았다는 것은 국가·공공기관이 클라우드서비스를 이용하기 위한 최소한의 정보보호 요건을 충족했음을 의미

Ⅱ

평가·인증대상 및 범위

1. 보안 평가·인증대상
2. 보안 평가·인증범위
3. 보안 평가·인증기준

Ⅱ 평가·인증대상 및 자산 범위

1. 보안 평가·인증 대상

평가·인증대상

⇨ 클라우드 보안인증 신청기관은「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률(이하 '클라우드컴퓨팅법'이라 한다)」제20조에 따라 공공기관의 업무를 위하여 클라우드서비스를 제공하려는 자(클라우드서비스 제공자)를 말한다.

《 클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 》

제20조(공공기관의 클라우드컴퓨팅서비스 이용 촉진) 정부는 공공기관이 업무를 위하여 클라우드컴퓨팅서비스 제공자의 클라우드컴퓨팅서비스를 이용할 수 있도록 노력하여야 한다.

⇨ 클라우드 보안인증 평가·인증대상은 동법 시행령 제3조에 따라, 클라우드컴퓨팅기술을 이용하여 정보시스템의 인프라, 응용프로그램, 개발환경 중 어느 하나 이상을 제공하는 클라우드서비스가 해당 된다.

※ 클라우드서비스 보안인증제는 클라우드컴퓨팅법 시행령 제3조제1호, 제3조제2호의 서비스를 대상으로 시행하며, 동 시행령 제3조제3호는 향후 확대 예정

《 클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 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

《 클라우드서비스 유형 및 평가대상 》

구 분	서비스 유형	평가여부
IaaS	컴퓨팅 자원(CPU), 스토리지 등 정보시스템의 인프라를 제공하는 서비스	평가
SaaS	인프라(IaaS) 외에 각종 응용프로그램(소프트웨어)을 제공하는 서비스	
PaaS	클라우드 관련 서비스를 개발하는 환경(플랫폼) 제공	미평가

※ PaaS는 현재 인증 수요가 적어 평가대상에서 제외되며, 향후 수요를 고려해 시행 검토

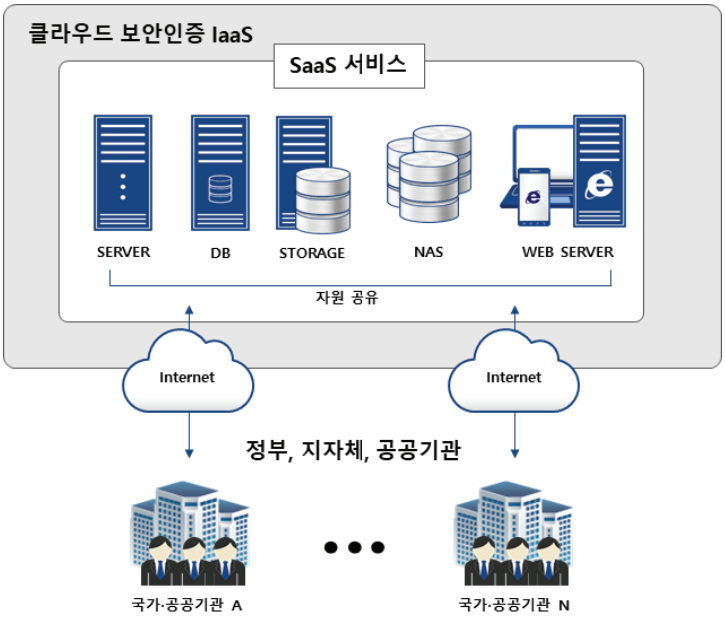
SaaS 평가·인증대상

⇒ SaaS 서비스는 기본적으로 클라우드서비스 보안인증을 받은 IaaS 서비스 환경에서 구축되어야 한다.

※ SaaS 사업자는 행정안전부의 「행정·공공기관 민간 클라우드 이용 가이드라인('18.12)」을 참고하여 제공 가능한 서비스를 구축하여야 함(부록 A "행정·공공기관 민간 클라우드 이용 가이드라인(요약)" 참조)

⇒ SaaS 평가·인증대상은 다수의 기관을 대상으로 퍼블릭(Public) 형태로 소프트웨어를 제공하는 서비스를 말한다.

※ 인증 제외대상 : 설치형 S/W, 단일기관 만을 위한 제공되는 SaaS



⇒ 또한 보안서비스(SecaaS)의 경우, 주요 보안기능이 아래의 정보보호 제품 유형(24종)에 해당하는지 확인하고 도입인증 요건을 만족하는 버전의 보안기능으로 서비스를 구축하여야 한다.

구분	정보보호 제품 유형	도입인증 요건	비고
1	침입차단시스템(FW)	**국내·외 CC인증**	EAL 2 이상 또는 관리 PP 준수
2	침입방지시스템(IPS) (침입탐지 포함)		
3	통합보안관리제품		
4	웹 응용프로그램 침입차단 제품		
5	서버 접근통제 제품		
6	DB 접근통제 제품		
7	네트워크 접근통제 제품		
8	인터넷전화 보안 제품		
9	무선침입방지시스템		
10	무선랜 인증 제품		
11	가상화 제품		
12	네트워크 자료유출방지 제품		
13	디지털 복합기 (완전삭제 또는 데이터 암호화)		
14	스마트폰 보안관리 제품		
15	스마트 카드		EAL 4 이상
16	가상사설망 제품	**국내·외 CC인증 및 검증필 암호모듈**	EAL 2 이상 또는 관련 PP 준수 KCMVP 필히 적용
17	소프트웨어기반 보안USB		
18	호스트 자료유출방지 제품 (매체제어 제품 포함)		
19	스팸메일 차단시스템	**국내·외 CC인증 또는 국가용 보안요구사항 GS인증**	CC인증 : EAL 2 이상 또는 관련 PP 준수 GS인증 : ISO/IEC 25023 및 국가용 보안요구사항 준수
20	패치관리시스템		
21	망간자료전송 제품		
22	DDoS 대응장비	**국내·외 CC인증 또는 국가용 보안요구사항 준수 성능평가**	CC인증 : EAL 2 이상 또는 관련 PP 준수 성능평가 : 국가용 보안요구사항 준수
23	안티바이러스 제품		
24	소스코드 보안약점 분석도구		

2. 보안 평가·인증 범위

평가·인증 범위

⇒ 클라우드 보안인증 평가·인증범위는 클라우드서비스에 포함되거나 관련 있는 자산(시스템, 설비, 시설 등), 조직, 지원서비스 등이 모두 포함된다.

⇒ 클라우드서비스는 구축 형태, 서비스 유형 등에 따라 다양해지기 때문에, 「예비점검」 단계를 통해 최종 평가범위가 결정된다.

〈 클라우드서비스 자산분류(예) 〉

구 분	설 명
서버	· 각종 프로그램이 운영되는 서버(Windows, Unix, Linux) 등
네트워크	· 라우터, 스위치, 허브 등
정보보호시스템	· 침입차단시스템, 침입방지시스템, 웹방화벽, 가상사설망 제품 등
소프트웨어	· 패키지 소프트웨어, 시스템 소프트웨어, 오픈소스 SW 등
응용프로그램	· 관리, 모니터링, 빌링, 분석 프로그램 등
데이터베이스	· MS-SQL, MySQL, 오라클 등
홈페이지	· 서비스 정보 안내, 신청 및 관리 등을 위한 홈페이지 등
단말기	· PC, 노트북, 모바일 디바이스 등
매체	· USB, 외장형 메모리, 디스크, 테이프 등
문서	· 정보보호 정책 지침, 절차, 매뉴얼 등
설비	· 출입보안, 전기·공조·소방 설비, 부대설비 등
가상자원 운영 S/W	· 하이퍼바이저, 클라우드 플랫폼 등
가상자원	· 가상서버, 가상PC, 가상 스토리지, 가상 네트워크, 배포이미지 등
지원서비스	· Auto Scaling, Load Balancer, DNS, 모니터링, 로그 분석 등

3. 보안 평가·인증기준

⇒ IaaS는 관리적·물리적·기술적 및 공공기관용 추가 보호조치로 총 14개 분야 117개 통제항목으로 구성

⇒ SaaS는 관리적·기술적 및 공공기관용 추가 보호조치로 총 13개 분야 78개 통제항목으로 구성

※ SaaS는 IaaS 위에 구축되어 IaaS 보다 통제항목이 약 33%가 줄었으며, 서비스 특징 등을 고려하여 "예비점검" 단계에서 평가 범위 및 항목이 일부 조정될 수 있음

〈클라우드서비스 보안 평가·인증기준 항목 수〉

통제 분야	통제 항목	통제항목 수	
		IaaS	SaaS
1. 정보보호 정책 및 조직	1.1. 정보보호 정책	3	3
	1.2. 정보보호 조직	2	2
2. 인적보안	2.1. 내부인력 보안	6	4
	2.2. 외부인력 보안	3	-
	2.3. 정보보호 교육	3	1
3. 자산관리	3.1. 자산 식별 및 분류	3	1
	3.2. 자산 변경관리	3	1
	3.3. 위험관리	4	1
4. 서비스 공급망 관리	4.1. 공급망 관리정책	2	2
	4.2. 공급망 변경관리	2	1
5. 침해사고관리	5.1. 침해사고 절차 및 체계	3	3
	5.2. 침해사고 대응	2	2
	5.3. 사후관리	2	2
6. 서비스 연속성 관리	6.1. 장애대응	4	4
	6.2. 서비스 가용성	3	2

<클라우드서비스 보안 평가·인증기준 항목 수>

통제 분야	통제 항목	통제항목 수	
		IaaS	SaaS
7. 준거성	7.1. 법 및 정책 준수	2	1
	7.2. 보안 감사	2	2
8. 물리적 보안	8.1. 물리적 보호구역	6	-
	8.2. 정보처리 시설 및 장비보호	6	-
9. 가상화 보안	9.1. 가상화 인프라	6	2
	9.2. 가상 환경	4	4
10. 접근통제	10.1. 접근통제 정책	2	2
	10.2. 접근권한 관리	3	3
	10.3. 사용자 식별 및 인증	5	5
11. 네트워크 보안		6	5
12. 데이터 보호 및 암호화	12.1. 데이터 보호	6	6
	12.2. 매체 보안	2	-
	12.3. 암호화	2	2
13. 시스템 개발 및 도입 보안	13.1. 시스템 분석 및 설계	5	5
	13.2. 구현 및 시험	4	4
	13.3. 외주 개발 보안	1	1
	13.4. 시스템 도입 보안	2	-
14. 공공부문 추가 보안요구 사항		8	7
총 계		**117**	**78**

※ 세부 평가·인증기준은 부록 D의 '클라우드컴퓨팅서비스 정보보호에 관한 기준' 참조

클라우드서비스 보안인증제 안내서

III

평가·인증 절차

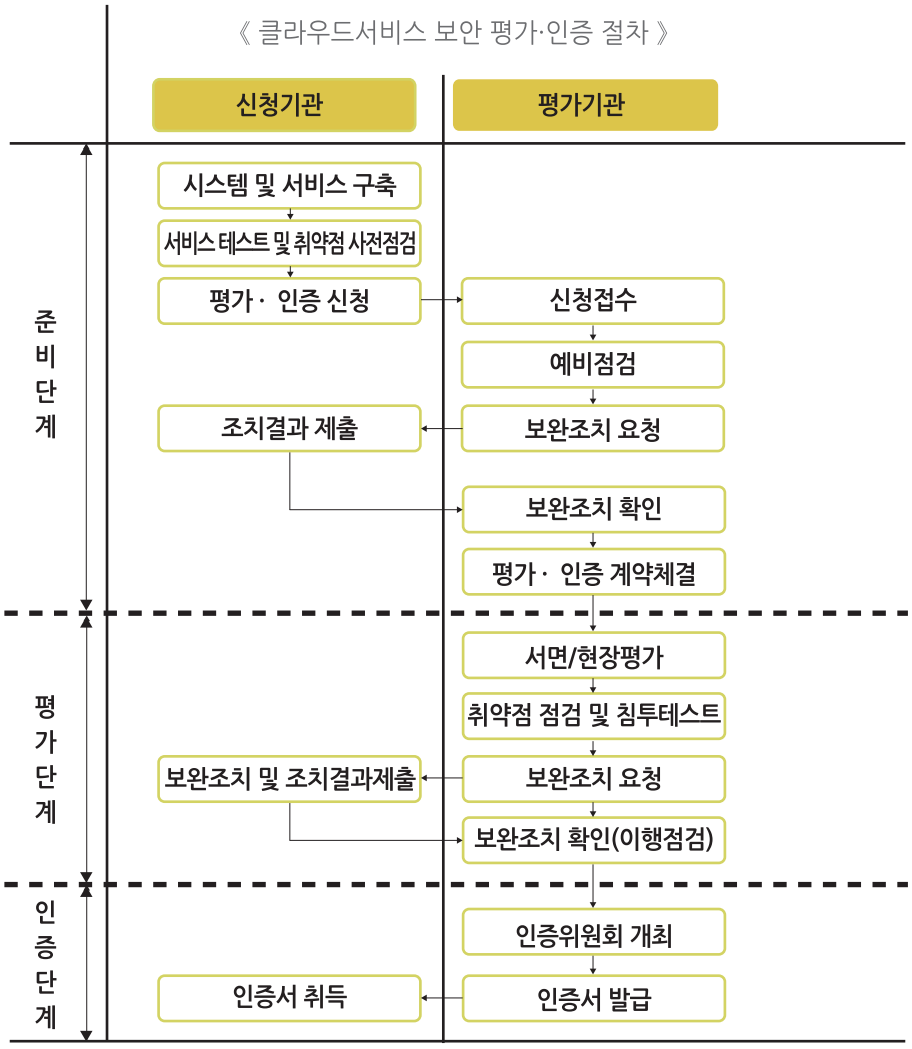
1. 평가·인증 절차
2. 사후 관리 절차

Ⅲ 평가 · 인증 절차

1. 평가 · 인증 절차

클라우드서비스 보안인증의 평가·인증 절차는 다음 그림과 같이 평가·인증 신청부터 인증서 발급까지는 총 3~6개월 정도가 소요됩니다.
신청기관은 당해년도 내에 클라우드서비스 보안인증서를 발급 받기를 원하는 경우, 미리 일정을 잘 계획하셔서 가능한 상반기에 평가·인증 신청을 해 주시기 바랍니다.

《 클라우드서비스 보안 평가·인증 절차 》



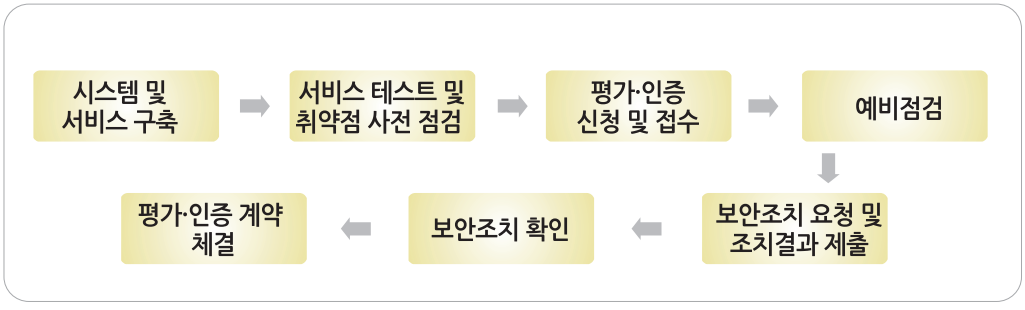
⇨ 상기 절차는 최초평가를 기준으로 하였으며, 1년 단위로 실시하는 사후평가(IaaS, SaaS 공통)에서는 준비단계 없이 평가단계로 넘어간다.

주요 평가단계별 소요일수

- ▸ IaaS : 예비점검 5일 - 서면/현장평가 7일 - 취약점점검 10일 - 모의침투테스트 10일
- ▸ SaaS : 예비점검 5일 - 서면/현장평가 · 취약점점검(동시) 7일 - 모의침투테스트 10일

※ 평가단계별 소요일수는 클라우드서비스 자산 규모에 따라 일부 변동 될 수 있음

1 준비단계



① 시스템 및 서비스 구축

⇨ 신청기관은 제공하는 서비스 유형(IaaS, SaaS 등)을 고려하여 클라우드 시스템을 구축한다.

- IaaS인 경우에는 주센터, 재해복구(DR)센터, 이용자·관리자 포털, 가상자원 관리시스템 등 인프라 제공과 관련된 클라우드 시스템을 구축
- SaaS인 경우에는 보안인증을 받은 IaaS 사업자가 제공하는 가상환경 위에 클라우드 시스템을 구축하며, 다음 아래 사항을 확인 후 진행

1) 「SaaS 구축 신청서」를 제출 후 인증 받은 IaaS 사업자와 계약하여 SaaS 서비스 구축

※ 「SaaS 구축 신청서」는 「홈페이지(https://isms.kisa.or.kr) - 클라우드보안인증제 - 자료실」 참조

※ SaaS 구축 신청 시 사전컨설팅을 신청하는 경우, 신청기관은 평가·인증기관(KISA)으로부터 주요 인증기준의 만족 여부 등을 사전에 확인 받을 수 있음

2) 클라우드 정보보호 기준(11.1.4 데이터 보호)에 의거 이용기관별 데이터를 논리적으로 분리하여 구축

구 분		보안요구사항
이용기관별 데이터 저장	DB	이용기관별로 DB테이블 분리하여 데이터를 저장 ※ 단 서비스 가입을 위한 기관 가입정보는 공통 DB테이블 사용 가능
	스토리지	이용기관별로 논리적으로 분리된 스토리지에 저장 ※ 하나의 스토리지 공간에 파일시스템(폴더) 단위 저장은 불가

3) 클라우드 서비스 연속성 보장을 위해 중요 데이터에 대한 소산 백업 환경 구축

② 서비스 테스트 및 취약점 사전 점검

⇨ 신청기관은 실 운영 환경에서 서비스 운영을 위한 기본적인 테스트 및 취약점 사전 점검을 완료 후 인증·평가 신청을 하여야 한다.

- 취약점 사전 점검은 평가·인증 대상의 자산에 대해서는 취약점 점검(CVE, CCE 등)을 실시하고 조치율이 80% 이상일 경우 완료

※ CCE 취약점 점검은 KISA에서 제공하는 점검 스크립트를 사용할 수 있으며, 점검 스크립트가 없는 시스템은 신청기관에서 자체 실시한 보안 점검 결과를 제출

③ 평가·인증 신청 및 접수

⇨ 평가·인증 신청은 다음의 서류를 준비하여 평가·인증기관에 제출한다.

클라우드서비스 보안인증 신청서류

- ○ 클라우드서비스 보안인증 신청 공문 1부
- ○ 클라우드서비스 보안인증 신청서 1부
- ○ 취약점 점검 및 침투테스트 동의서 1부 (SaaS는 IaaS 사업자의 동의 포함)
- ○ 클라우드서비스 보안인증 명세서 1부 (클라우드서비스 보안운영 명세서 포함)
- ○ 법인/개인 사업자 등록증 1부
- ○ 정보시스템 취약점 (CVE, CCE) 자체 점검 결과 1부
- ○ 보안기능변경 영향분석서 (CC인증 제품군 SecaaS만 해당)

※ 신청서 및 기타 양식은 평가·인증기관 "홈페이지(http://isms.kisa.or.kr) - 클라우드보안인증제 - 자료실"에서 다운로드가 가능

⇨ 신청기관은 보안인증 신청서류를 방문접수 또는 등기우편으로 제출

※ 신청서류가 누락되거나 신청서류 내용이 미비하여 평가·인증기관의 보완 요청이 있을 경우, 신청서류를 재구비 또는 보완한 후 다시 신청하여야 함

인증 신청 및 접수문의

○ 주소 : 전라남도 나주시 진흥길 9(빛가람동 301-2) 한국인터넷진흥원 6층 클라우드인증팀 클라우드서비스 보안인증담당자 앞

○ 연락처 : 061)820-1662, 1664, 1638, 1639 cloud@kisa.or.kr

④ 예비점검

⇨ 예비점검이란 평가·인증 계약체결 전에 공공기관용 클라우드서비스의 필수요건 준수여부, 클라우드 시스템의 규모, 위험 식별 및 평가 수행여부, 운영명세서 등 평가·인증에 필요한 기초자료 구비 유무, 평가·인증 준비상태 및 운영여부를 사전에 확인하는 것이다.

- 예비점검을 통해 인증범위 적정성, 평가·인증 전 구축 및 운영 현황 등을 확인하고 평가·인증 진행여부 및 평가일정을 결정

⇨ 또한 신청기관이 제출한 자산대장과 실제 가동 중인 자산을 비교 및 확인하고 적절한 점검 방법을 도출한다.

- 취약점 점검을 위해, VPN환경 제공여부, 원격 접속 시 방화벽 작업, 자동 점검도구 설치 가능 여부를 체크

⑤ 보완조치 요청 및 조치결과 제출

⇨ 평가팀은 신청기관 담당자에게 예비점검 결과를 설명하고, 예비점검 보고서를 통해 미흡사항에 대한 보완조치를 요청한다.

⇨ 신청기관은 보완조치를 완료하고, 평가/인증기관에 통보하여야 한다.

⑥ 보완조치 확인

⇨ 평가팀장은 보완조치의 적절성을 확인하고 평가·인증의 진행여부를 판단한다.

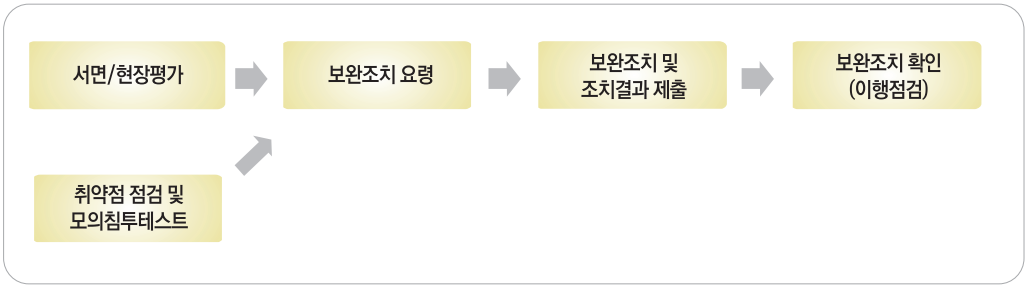
구 분	세부조치
보완조치 완료 시	평가·인증 계약을 체결하고 다음 평가 단계를 진행
보완조치 미흡 시	재보완 조치 또는 평가·인증 중단 여부를 판단하여 진행

⑦ 평가·인증 계약체결

⇨ 평가·인증 진행이 결정된 이후 인증범위, 평가·인증기간, 평가·인증 수수료 등을 협의하고 평가·인증 계약을 체결한다.

※ 민간 클라우드서비스 도입 활성화 및 안전하고 신뢰할 수 있는 클라우드서비스 제공을 위해 일정기간 동안 정부에서 클라우드서비스 보안인증제의 평가인증 수수료를 지원 中

2 평가단계



①-1) 서면/현장평가

⇨ 서면/현장평가는 클라우드서비스가 보안 평가·인증기준에 맞게 적절하게 구축·운영되고 있는지 확인한다.

※ 신청기관이 서비스 시연을 진행하거나 평가팀에게 테스트용 계정을 부여하여 확인 가능

⇨ 서면평가는 정보보호 정책, 지침, 매뉴얼(절차) 등 내부규정 존재 여부 및 해당 내부 규정이 평가·인증기준에 충족하는지 평가. 또한, 신청기관에서 제출한 증적자료 확인을 통해 운영의 적정성을 확인한다.

⇨ 현장평가는 서면평가의 결과와 관리적·물리적·기술적 보호대책 이행 여부를 확인하기 위하여 담당자 인터뷰, 관련 시스템 확인 등의 방법으로 평가한다.

※ 현장평가의 경우 서면평가 진행현황에 맞춰 일정을 조율하여 진행

⇨ 평가팀은 서면/현장평가를 통하여 도출된 문제점에 대해 부적합 보고서를 작성하고, 신청기관 담당자와의 회의를 통해 부적합 보고서의 적절성을 상호 협의하여 결정한다.

※ 신청기관은 평가팀이 작성한 부적합 보고서에 사실과 다른 내용이 있는지 검토

①-2) 취약점 점검 및 모의침투테스트

⇨ 평가팀은 클라우드서비스 보안 평가·인증기준 중 기술적 보호조치 항목 중 취약점 점검 및 침투테스트가 필요한 항목에 대해 점검도구(툴), 수동점검, 침투테스트 등을 통해 확인한다.

※ 취약점 점검 및 침투테스트는 한국인터넷진흥원에서 지정한 수행기관 또는 한국인터넷진흥원을 통해 진행함

취약점 점검 구분

○ CCE(Common Configuration Enumeration) : 취약한 설정에 대한 점검
- 비밀번호 길이/복잡성, 기본 계정 삭제 등 시스템 구성 및 설정에 관한 규정(또는 정책)을 준수하는지 점검

○ CVE(Common Vulnerabilities and Exposures) : OS, Application 고유의 취약점
- 벤더가 제공하는 패치와 관련된 취약점으로써, Mitre에서 CVE코드(예를 들면, CVE-2009-2521) 부여 관리

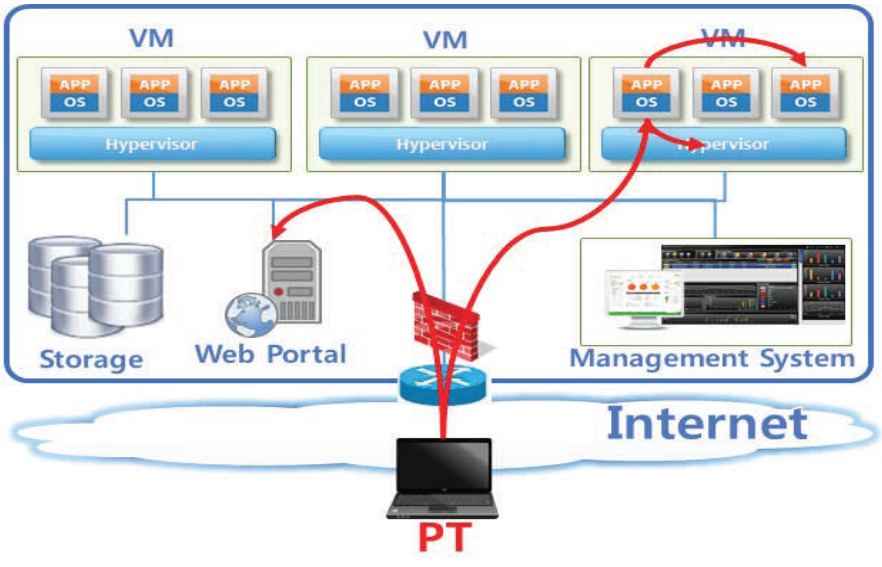
○ 소프트웨어 보안약점 진단(시큐어코딩) : IaaS 웹 포털, SaaS 웹 포털 및 기능 등

※ SaaS 서비스 특성에 따라 점검 범위 조정 가능

⇨ 평가팀은 클라우드서비스 모델, 구축 유형 등을 고려하여 신청기관과 협의한 후 모의침투 계획, 침투 시나리오 등을 통해 확인한다.

- IaaS는 포털, 가상환경(VM) 등 외부 경로를 통한 침투테스트 수행
  ① 외부 인터넷을 통한 클라우드서비스 포털로의 침투
  ② 이용자 VM을 통한 하이퍼바이저 또는 다른 VM으로의 침투
- SaaS는 예비점검, 서면평가 등을 통해 수립한 침투시나리오를 바탕으로 침투테스트를 수행

〈 클라우드서비스 외부 침투테스트 경로(예시) 〉



② 보완조치 요청

⇨ 평가팀은 종료회의를 통해 신청기관 담당자에게 서면/현장평가, 취약점 점검 및 침투테스트 결과를 설명하고, 보완조치요청서를 통해 부적합 사항 및 취약점에 대한 보완조치를 요청한다.

※ 향후 진행 사항 및 일정에 대한 사항 안내

③ 보완조치 및 조치결과 제출

⇨ 신청기관은 보완조치 요청을 받은 날로부터 30일 이내 보완조치를 완료하고 보완조치 내역서를 작성하여 평가·인증기관에 제출한다.

※ 필요시 공문을 통해 최대 60일 이내로 추가 연장 가능

④ 보완조치 확인(이행점검)

⇨ 평가팀장은 보완조치 내역서의 적절성을 판단하고 이행점검을 통해 실제 이행 여부를 현장에서 확인하여 보완조치 여부를 판단한다.

구 분	세부조치
보완조치 완료 시	보완조치 완료 확인서에 서명 후 인증 단계로 진행
보완조치 미흡 시	재보완조치 또는 평가중단 여부를 판단하여 진행

평가 시 유의사항

○ 평가 중 인증준비 미흡, 요청사항 대응 미흡, 중요 부적합 사항 미조치 등 평가 지속이 어렵다고 판단 될 경우 평가 중단 및 평가팀 철수가 이루어질 수 있음

3 인증 단계

인증위원회 개최 ➡ 인증서 발급 및 취득

① 인증위원회 개최

⇨ 평가가 완료된 신청기관에 대하여 평가·인증기관은 “평가 결과보고서”를 작성하여 인증위원회 안건으로 상정한다.

⇨ 인증위원회는 학계, 연구기관, 기술자문기관 등 클라우드 관련 전문가 5인 이상 10인 이내로 구성되며 각 상정된 안건에 대하여 다음의 사항을 심의·의결한다.

인증위원회 심의·의결 사항

- ○ 평가 결과가 평가·인증기준에 적합한지 여부
- ○ 사후평가 결과 인증취소사유를 발견한 경우에 그 결과의 적합성 여부
- ○ 그 밖에 클라우드서비스 보안인증과 관련하여 위원장이 필요하다고 인정하는 사항

⇨ 위원장은 각 위원들이 작성한 인증위원회 심의의견을 취합하여 클라우드서비스 보안 평가·인증 심의 결과서를 작성한다.

인증 심의·의결 원칙

- ○ 부적합 사항에 대해 모두 조치 완료된 경우에만 적합하다고 판단하는 것 원칙임
- ○ 단, 해당 부적합 사항이 경미하여 클라우드서비스 보안 관점에서 영향이 거의 없다고 판단되는 경우에는 조건부로 적합하다고 판단할 수 있음

⇨ 인증위원회에서는 심의 결과에 따라 추가 보완조치를 요구할 수 있으며, 이 경우 평가팀장을 통해 신청기관에게 해당사항과 더불어 보완조치 기한이 전달된다.

⇨ 신청기관은 해당사항을 보완 완료 후 평가팀장에게 수정된 “보완조치 내역서”를 제출하여야 한다.

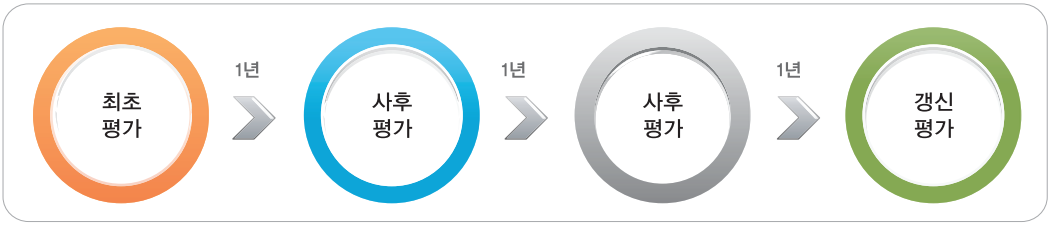
⇨ 보완조치 이행여부를 확인한 평가팀장은 해당사항에 대한 결과보고서를 차기 인증위원회에 상정하여 최종 인증 여부를 의결 받게 된다.

② 인증서 발급 및 취득

⇨ 인증기관의 장은 인증위원회 심의·의결 결과를 신청기관에 통보하고, 평가·인증기준에 적합한 경우 인증서를 발급한다.

⇨ 신청기관은 인증서를 수령한 이후 보안인증 표시를 사용할 수 있다.

2. 사후 관리 절차



1 사후 평가 및 갱신 평가

① 사후 평가

⇨ 사후 평가는 인증취득기관이 지속적으로 클라우드서비스 보안 평가·인증기준의 준수 여부를 확인하기 위해 인증 유효기간 중 매년 1회 이상 시행하는 평가·인증을 말한다.

⇨ 인증 취득기관은 인증 발급일 기준으로 매 1년 이전에 평가를 받아야 하며, 인증 유효기간 내 평가를 받지 않는 경우 인증이 취소된다.

⇨ 인증이 취소된 경우, 인증을 재취득하기 위해서는 최초 평가부터 다시 평가를 받아야 한다.

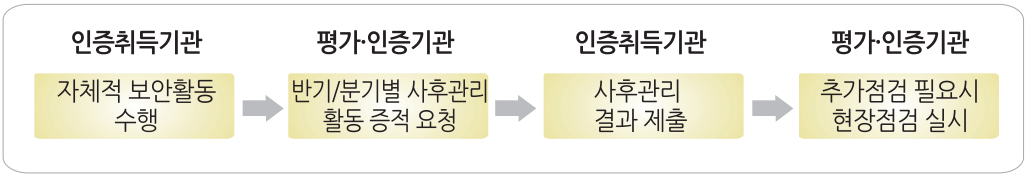
② 갱신평가

⇨ 클라우드서비스 보안인증의 유효기간은 3년이며, 갱신평가는 인증 유효기간이 만료될 때 유효기간 연장을 목적으로 시행하는 평가·인증을 말한다

⇨ 갱신평가는 유효기간(인증발급일 기준) 만료 전에 평가를 받아야 하며, 인증유효기간 내 평가를 받지 않을 경우 인증 효력을 상실한다.

⇨ 갱신평가를 통해 연장되는 인증 유효기간은 3년이며, 최초평가와 마찬가지로 인증위원회에서 인증 유효기간 연장에 대한 심의·의결을 받도록 하고 있다.

2 사후관리



⇨ 사후관리는 인증취득 이후 인증취득기관의 지속적 보안수준 유지를 위해 분기마다 인증취득기관의 자체적인 보안활동 결과를 제출하고 이를 평가·인증기관이 확인하는 활동을 말한다.

⇨ 인증취득기관은 분기별로 보안관리 활동을 수행하고, 수행한 결과를 평가·인증기관에 통보한다.

※ 평가·인증기관과 협의하여 제출시기를 조정할 수 있음

- (분기) 자산 및 기능 변경 내역(IaaS·SaaS), 지원서비스 목록(IaaS만 해당) 등

※ 클라우드 시스템의 대규모 변경(ex:센터 이전, 신규 서비스 구축을 위한 장비 도입, 서비스 기능 변경 등)이 발생한 경우는 분기별 제출과 상관없이 상시 통보

- (반기) 자체 취약점 점검 결과 및 보완조치 증적

사후관리 제출서류

○ 사후관리 회신 공문 1부

○ 사후관리 이행결과 요약서 1부

- 클라우드서비스 관련 자산 증설 및 변동된 **자산 현황**
- 신규 취약점 대비를 위한 **취약점(CVE) 점검 결과 및 조치 내역**
- 클라우드서비스 관련 정책, 지침 등 **기타 변동된 사항**
- 지원서비스 목록 **(IaaS인 경우만 해당)**
- 기능변경(인터페이스 변경, 버그수정, 패치 적용 등) 이력 **(SaaS인 경우만 해당)**

○ 사후관리 이행결과 증적

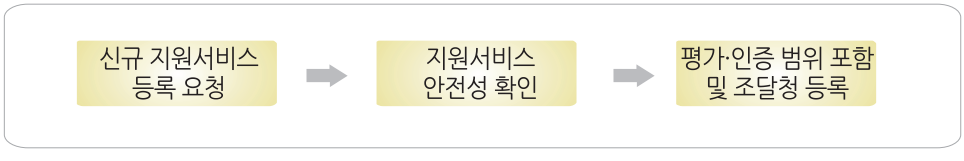
- 클라우드 시스템 증설 및 변동 자산 반영된 자산관리대장 1부
- CVE 취약점 점검 결과 및 보완조치 증적

※ CVE 취약점 점검 도구는 인증취득기관이 보유하고 있는 도구를 이용하여 점검

- 지원서비스 등록신청서 (서비스별 1부) **(IaaS만 해당)**

※ 사후관리 제출관련 서류는 평가·인증기관 "홈페이지(https://isms.kisa.or.kr) - 클라우드보안인증제 - 자료실"에서 다운로드가 가능

3 지원서비스 관리



⇨ 지원서비스는 IaaS에서 제공하는 IT인프라(서버, 네트워크, 스토리지 등)의 효율성, 편의성을 제공하는 부가적인 서비스로써, 반드시 평가·인증 범위에 있는 공공 영역에 구축되어야 한다.

※ 대표적인 지원서비스는 서버를 지원하는 Auto Scaling, 네트워크를 지원하는 Load Balancer, DNS, 그리고 스토리지를 지원하는 백업 등이 해당됨

⇨ 인증취득기관이 신규 지원서비스를 제공하기 위해서는 “지원서비스 등록신청서”를 작성한 후 평가·인증기관에 제출(상시)하여야 한다.

※ 지원서비스 등록신청서는 서비스 소개, 서비스 유형, 공공존 구축여부, 서비스 구조, 외부연동 여부, 개인정보 취급여부 등의 내용을 포함

⇨ 평가·인증기관은 인증취득기관이 제출한 신청서를 검토(필요 시 점검 가능) 후 지원서비스 등록 가능여부를 판단한다.

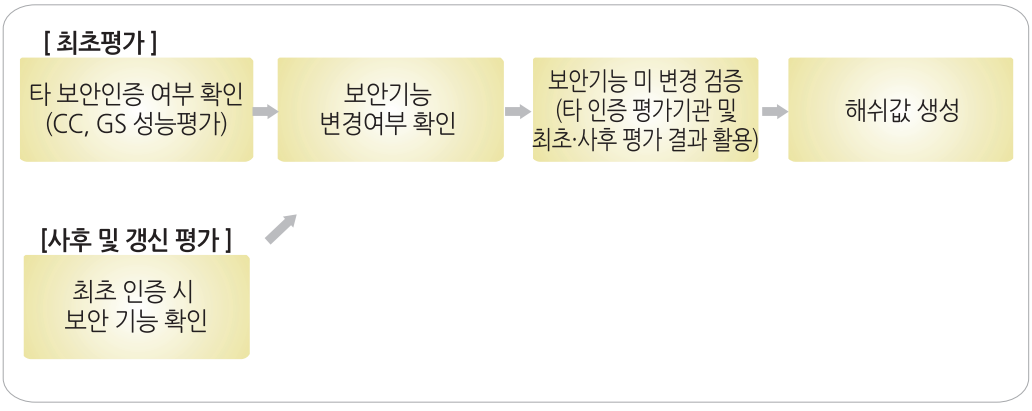
구 분	세부조치
지원서비스 등록 가능한 서비스	지원서비스 목록을 조달청으로 전달 ※ 조달청은 나라장터 종합쇼핑몰에 등록된 클라우드서비스의 카탈로그 목록을 갱신
지원서비스 등록 불가능한 서비스	SaaS 보안인증 신청 후 제공하도록 인증취득기관에 통보

⇨ 사후평가(연 1회) 시 평가·인증기관은 지원서비스에 대한 서면/현장평가를 진행(필요시 취약점 점검 수행)한 후 평가·인증 범위 내 지원서비스를 목록화하여 관리한다.

지원서비스 관리 시 유의사항

o 신규 지원서비스를 등록신청 없이 제공하는 경우 인증 취소 등의 조치가 취해질 수 있음

4 형상 관리 (CC인증 제품군 SecaaS만 해당)



⇨ 형상관리는 SecaaS 보안기능(예 : WAF의 유해 트래픽 차단 기능, 감사기록 생성 기능 등)의 형상변경 여부를 평가·인증기관이 확인하는 것을 말한다.

- 최초 평가인 경우, 타 보안인증(CC평가, GS인증 등) 취득 제품의 보안기능이 클라우드 환경에 적용되면서 형상의 변경 여부를 확인
- 사후 또는 갱신 평가인 경우, 보안인증 취득 이후에 발생하는 보안기능의 형상 변경 이력을 확인

시기별 형상관리 비교 대상

○ **(최초 평가)** 타 보안인증(CC평가, GS인증 등) 취득 제품의 보안기능과 클라우드 환경에 최초 구축된 SecaaS의 보안기능

○ **(사후·갱신평가)** 최초인증 취득 시점의 SecaaS 보안기능과 사후·갱신평가 시점의 SecaaS 보안기능

⇨ 인증취득기관은 보안기능 변경 영향분석서를 최초 및 사후평가(매년) 시 작성하여 제출하여야 한다.

※「보안기능 변경 영향분석서」는「홈페이지(https://isms.kisa.or.kr) - 클라우드보안인증제 - 자료실」참조

형상관리 시 유의사항

형상 변경 시 확인되지 않은 보안기능에 대한 변경이 있을 경우 인증 취소 등의 조치가 취해질 수 있음

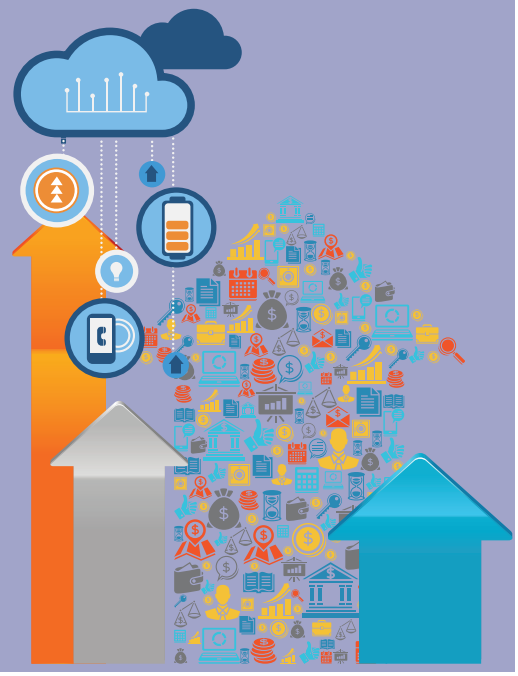
부록

A. 행정·공공기관 민간 클라우드 이용 가이드라인(요약)

B. 재해복구(DR)센터 구축 기준

C. 평가·인증 관련 각종 양식

D. 평가·인증 통제항목표(IaaS용, SaaS용)



(부록 A) 행정·공공기관 민간 클라우드 이용 가이드라인(요약)

□ 이용 대상기관

⇨「전자정부법」제2조에 따른 행정기관 및 공공기관

□ 이용 대상정보

구 분	중앙부처	지자체	공공기관
대국민서비스	민간 클라우드 이용 기능		
대국민서비스 (업무시스템 등)	전자정부클라우드 플랫폼 적용 (G-클라우드)	전용 클라우드(권고)	민간 클라우드 이용 가능

※ 안보, 수사 관련 정보, 민감정보 처리시스템과 개인정보영향평가 대상 시스템은 민간 클라우드 이용 제외

□ 행정·공공기관 클라우드 도입절차

구 분	인증여부	도입절차
자체 클라우드 구축 또는 솔루션 도입	불필요	정보화 사업 계획 수립 → 보안성 검토 → 정보화 사업 수행
민간 클라우드 서비스 이용	필요	

① 기관 자체 클라우드 구축 또는 민간 클라우드 이용 여부 검토

② 민간 클라우드 컴퓨팅서비스 이용 가능 여부 검토

※ 클라우드 보안인증(IaaS, SaaS)을 받은 서비스만 이용 가능

※ 인증현황 : 한국인터넷진흥원 인증제도 홈페이지(https://isms.kisa.or.kr/main/csap/issue/)

③ 정보보호에 관한 사항은 국가정보원에 보안성 검토 요청

※ 국정원의 국가 공공기관 클라우드컴퓨팅 보안 가이드라인 준수

④ 국가정보원의 보안성 검토 결과 등을 반영하여 민간 클라우드 이용

문의 및 지원

o 중앙행정기관 및 소속 공공기관은 **한국정보화진흥원** 문의
- 공공 클라우드 지원센터 : 1522-0089, http://cpcp.ceart.kr, cpcp@nia.or.kr

o 지방자치단체 및 지방공기업은 **지역정보개발원**에 문의
- 공공 클라우드 지원센터 : 02-2031-9281, cloud@klid.or.kr

(부록 B) 재해복구(DR)센터 구축 기준

1. 필수(요구) 조건

⇨ 단순 데이터의 원격지 백업센터가 아닌, 자체적으로 서비스 운영이 가능한 재해복구(DR)센터
- 공공 클라우드 전용 서버, 스토리지, 네트워크, 상면 등을 구비

※ 단 네트워크는 공공 전용으로 별도 구축을 요구하지 않으며, 민간용으로 운영 가능

⇨ 재해복구센터 내 공공 클라우드 시스템의 물리적 분리(네트워크는 제외)와 접근통제는 필요

2. 자율사항

⇨ 상기 필수조건 외에 나머지 조건사항은 신청기관의 자율 기준에 따름

〈 자율 기준 허용 사항 〉

- 주센터, DR센터 간 지리적 거리(이격 거리)
- DR서비스 복구시간(실시간 내지는 수시간 소요)
- DR센터 내 이중화 구성 여부

3. 참고사항

⇨ 재해복구센터가 원거리에 위치하는 경우, 재해 · 재난 대응력은 높아지나, 관리가 어렵고 통신비용이 증가하므로, 신청기관은 종합적으로 고려하여 최적의 위치 선정 필요

구 분	한국시설안전공단	금융권	가트너
지리적 거리	30~80Km	일정거리 이상	~ 60마일(~ 96.5km)
복구시간	Hot site(4시간 이내) Warm site(수일~수주) Cold site(수주~수개월)	3시간 이내	-

※ 가트너의 경우, 네트워크 지연(latency)를 고려하여 96.5km 이내 권고

(부록 C) 평가·인증 관련 각종 양식

① 클라우드서비스 보안인증 신청양식

평가 · 인증 신청 제출서류

1. 클라우드서비스 보안인증 신청서

2. 취약점 점검 및 침투테스트 동의서

3. 클라우드서비스 보안인증 명세서
   - 클라우드서비스 보안인증의 범위
   - 정보시스템 및 네트워크 범위
   - 클라우드서비스 보안 운영 내역
   - 클라우드서비스 보안 관련 주요 문서 목록
   - 국내·외 품질경영체제 인증서 취득 명세
   - [별지] 클라우드서비스 보안운영 명세서

4. 사업자등록증 (또는 고유번호증)

5. 정보시스템 취약점(CVE, CCE) 자체 점검 결과

6. 보안기능 변경 영향분석서(CC인증 제품군 SecaaS 신청기관용)

② 기타 별지 양식

1. SaaS 구축 신청서(SaaS 신청기관용)

2. 사후관리 이행결과 요약서

3. 지원서비스 등록신청서

※ 신청서 및 기타 양식은 평가·인증기관 "홈페이지(https://isms.kisa.or.kr) – 클라우드보안인증제 - 자료실"에서 다운로드가 가능

(부록 D) 평가·인증 통제항목표(IaaS용, SaaS용)

① IaaS용 통제항목표 (117개 통제항목)

관리적 보호조치

구 분			세부조치사항
1. 정보보호 정책 및 조직	1.1. 정보보호 정책	1.1.1. 정보보호 정책 수립	정보보호 정책을 문서화하고, 정보보호 최고책임자의 승인 후 정책에 영향을 받 모든 임직원 및 외부 업무 관련자에게 제공하여야 한다
		1.1.2. 정보보호 정책 검토 및 변경	정보보호 정책의 타당성 및 효과를 연 1회 이상 검토하고, 관련 법규 변경 및 내·외 보안사고 발생 등의 중대한 사유가 발생할 경우에는 추가로 검토하고 변경하여 한다.
		1.1.3. 정보보호 정책문서 관리	정보보호 정책 및 정책 시행문서의 이력관리 절차를 수립하고 시행하며, 최신본으 유지하여야 한다.
	1.2. 정보보호 조직	1.2.1. 조직 구성	정보보호 활동을 계획, 실행, 검토하는 정보보호 전담조직을 구성하고 정보보호 최 책임자를 임명하여야 한다.
		1.2.2. 역할 및 책임 부여	정보자산과 보안에 관련된 모든 임직원 및 외부 업무 관련자의 정보보호 역할 책임을 명확하게 정의하여야 한다. 또한 서비스 이용자의 정보보호 역할과 책임 서비스 수준 협약 등을 통해 명확하게 정의하여야 한다.
2. 인적보안	2.1. 내부인력 보안	2.1.1. 고용계약	고용 계약서에 정보보호 정책 및 관련 법률을 준수하도록 하는 조항 또는 조건을 포 시키고, 새로 채용하거나 합류한 근무 인력이 클라우드컴퓨팅서비스의 설비, 자 자산에 첩근이 허용되기 이전에 서명을 받아야 한다.
		2.1.2. 주요 직무자 지정 및 감독	클라우드컴퓨팅서비스의 시스템 운영 및 개발, 정보보호 등에 관련된 임직원의 경 주요 직무자로 지정하여 관리하고, 직무 지정 범위는 최소화하여야 한다.
		2.1.3. 직무 분리	권한 오남용 등 내부 임직원의 고의적인 행위로 발생할 수 있는 잠재적인 위협을 줄이 위하여 직무 분리 기준을 수립하고 적용하여야 한다.
		2.1.4. 비밀유지 서약서	정보보호와 개인정보보호 등을 위해 필요한 사항을 비밀유지서약서에 정의하고 주기 으로 갱신하여야 한다.
		2.1.5. 상벌규정	정보보호 정책을 위반한 임직원에 대한 징계 규정을 수립하고, 위반 사항이 발생 규정에 명시된 대로 징계 조치를 취하여야 한다. 또한 정보보호 정책을 충실히 이행 임직원에 대한 보상 방안도 마련하여야 한다.
		2.1.6. 퇴직 및 직무변경	임직원의 퇴직 또는 직무 변경에 관한 책임을 명시적으로 정의하고 수행하여야 한 또한 이에 대한 접근권한도 제거하여야 한다.

구 분			세부조치사항
	2.2. 외부인력 보안	2.2.1. 외부인력 계약	외부인력(외부유지보수직원, 외부용역자 포함)에 의한 정보자산 접근 등과 관련된 보안요구사항을 계약에 반영하여야 한다.
		2.2.2. 외부인력 보안 이행 관리	계약서에 명시한 보안요구사항 준수 여부를 주기적으로 점검하고 위반사항이나 침해사고 발생 시 적절한 조치를 수행하여야 한다.
		2.2.3. 계약 만료 시 보안	외부인력과의 계약 만료 시 자산 반납, 접근권한의 회수, 중요정보 파기, 업무 수행 시 알게 된 정보의 대한 비밀 유지서약 등을 확인하여야 한다.
	2.3. 정보보호 교육	2.3.1. 교육 프로그램 수립	모든 임직원 및 외부 업무 관련자를 포함하여 연간 정보보호 교육 프로그램을 수립하여야 한다.
		2.3.2. 교육 시행	모든 임직원 및 외부 업무 관련자를 대상으로 연 1회 이상 정보보호 교육을 시행하고 정보보호 정책 및 절차의 중대한 변경, 내·외부 보안사고 발생, 관련 법규 변경 등의 사유가 발생하면 추가 교육을 실시하여야 한다.
		2.3.3. 평가 및 개선	정보보호 교육 시행에 대한 기록을 남기고 결과를 평가하여 개선하여야 한다.
3. 자산관리	3.1. 자산 식별 및 분류	3.1.1. 자산 식별	클라우드컴퓨팅서비스에 사용된 정보자산(정보시스템, 정보보호시스템, 정보 등)에 대한 자산분류기준 수립하고 식별된 자산의 목록을 작성하여 관리하여야 한다.
		3.1.2. 자산별 책임할당	식별된 자산마다 책임자 및 관리자를 지정하여 책임소재를 명확히 하여야 한다.
		3.1.3. 보안등급 및 취급	기밀성, 무결성, 가용성, 법적요구사항 등을 고려하여 자산의 보안 등급을 부여하고, 보안 등급별 취급 절차에 따라 관리하여야 한다.
	3.2. 자산 변경관리	3.2.1. 변경관리	클라우드컴퓨팅서비스에 사용된 자산(시설, 장비, 소프트웨어 등)의 변경이 필요한 경우 보안 영향 평가를 통해 변경 사항을 관리하여야 한다. 또한 이용자에게 큰 영향을 주는 변경에 대해서는 사전에 공지를 하여야 한다.
		3.2.2. 변경 탐지 및 모니터링	클라우드컴퓨팅서비스에 사용된 자산(시설, 장비, 소프트웨어 등)의 변경을 지속적으로 모니터링하여 허가 받지 않은 변경을 탐지하고 최신의 변경 이력을 유지하여야 한다.
		3.2.3. 변경 후 작업검증	클라우드컴퓨팅서비스에 사용된 자산(시설, 장비, 소프트웨어 등)의 변경 후에는 보안성 및 호환성 등에 대한 작업 검증을 수행하여야 한다.
	3.3. 위험관리	3.3.1. 위험관리 계획수립	관리적, 기술적, 물리적, 법적 분야 등 정보보호 전 영역에 대한 위험식별 및 평가가 가능하도록 위험관리 방법과 계획을 사전에 수립하여야 한다.

구 분			세부조치사항
	3.3. 위험관리	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.
		3.3.3. 위험분석 및 평가	위험관리 방법 및 계획에 따라 정보보호 전 영역에 대한 위험 식별 및 평가를 연 1회 이상 수행하고 그 결과에 따라 수용 가능한 위험수준을 설정하여 관리하여야 한다.
		3.3.4. 위험처리	법규 및 계약관련 요구사항과 위험수용 수준을 고려하여 위험평가 결과에 따라 통제할 수 있는 방법을 선택하여 처리하여야 한다.
4. 서비스 공급망 관리	4.1. 공급망 관리 정책	4.1.1. 공급망 관리 정책 수립	클라우드컴퓨팅서비스에 대한 접근과 서비스 연속성을 저해하는 위험을 식별하고 최소화하기 위해 공급망과 관련한 보안 요구사항을 정의하는 관리 정책을 수립하여야 한다.
		4.1.2. 공급망 계약	클라우드컴퓨팅서비스 범위 및 보안 요구사항을 포함하는 공급망 계약을 체결하고 다자간 협약 시 책임을 개별 계약서에 각각 명시해야하며, 해당 서비스에 관련된 모든 이해관계자에게 적용하여야 한다.
	4.2. 공급망 변경관리	4.2.1. 공급망 변경관리	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 제시하여야 한다.
		4.2.2. 공급망 모니터링 및 검토	클라우드컴퓨팅서비스 공급망 상에서 발생하는 기록 및 보고서는 정기적으로 모니터링 및 검토하여야 한다.
5. 침해 사고관리	5.1. 침해사고 대응 절차 및 체계	5.1.1. 침해사고 대응 절차 수립	침해사고에 대한 효율적이고 효과적인 대응을 위해 신고절차, 유출 금지 대상, 사고처리 절차 등을 담은 침해사고 대응절차를 마련하여야 한다. 침해사고 대응절차는 이용자와 제공자의 책임과 절차가 포함되어야 한다.
		5.1.2. 침해사고 대응 체계 구축	침해사고 정보를 수집·분석·대응할 수 있는 보안관제 시스템 및 조직을 구성 · 운영하고, 침해사고 유형 및 중요도에 따라 보고 및 협력체계를 구축하여야 한다.
		5.1.3. 침해사고 대응 훈련 및 점검	침해사고 대응과 관련된 역할 및 책임이 있는 담당자를 훈련시켜야 하고, 주기적으로 침해사고 대응 능력을 점검하여야 한다.
	5.2. 침해사고 대응	5.2.1. 침해사고 보고	침해사고 발생 시 침해사고 대응절차에 따라 법적 통지 및 신고 의무를 준수하여야 한다. 또한 클라우드컴퓨팅서비스 이용자에게 발생 내용, 원인, 조치 현황 등을 신속하게 알려야 한다.
		5.2.2. 침해사고 처리 및 복구	침해사고 발생 시 침해사고 대응절차에 따라 처리와 복구를 신속하게 수행하여야 한다.
	5.3. 사후관리	5.3.1. 침해사고 분석 및 공유	침해사고가 처리 및 종결된 후 발생 원인을 분석하고 그 결과를 이용자에게 알려야 한다. 또한 유사한 침해사고에 대한 신속한 처리를 위해 침해사고 관련 정보 및 발견된 취약점을 관련 조직 및 임직원과 공유하여야 한다

구 분			세부조치사항
	5.3. 사후관리	5.3.2. 재발방지	침해사고 관련 정보를 활용하여 유사한 침해사고가 반복되지 않도록 침해사고 재발방지 대책을 수립하고, 필요한 경우 침해사고 대응 체계도 변경하여야 한다.
6. 서비스 연속성 관리	6.1. 장애대응	6.1.1. 장애 대응절차 수립	관련 법률에서 규정한 클라우드컴퓨팅서비스의 중단으로부터 업무 연속성을 보장하기 위해 백업, 복구 등을 포함하는 장애 대응 절차를 마련하여야 한다.
		6.1.2. 장애 보고	클라우드컴퓨팅서비스 중단이나 피해가 발생 시 장애 대응절차에 따라 법적 통지 및 신고 의무를 준수하여야 한다. 또한 클라우드컴퓨팅서비스 이용자에게도 발생 내용, 원인, 조치 현황 등을 신속하게 알려야 한다.
		6.1.3. 장애 처리 및 복구	클라우드컴퓨팅서비스 중단이나 피해가 발생할 경우, 서비스 수준 협약(SLA)에 명시된 시간 내에 장애 대응절차에 따라 해당 서비스의 장애를 처리하고 복구시켜야 한다.
		6.1.4. 재발방지	장애 관련 정보를 활용하여 유사한 서비스 중단이 반복되지 않도록 장애 재발방지 대책을 수립하고, 필요한 경우 장애 대응 절차도 변경하여야 한다.
	6.2. 서비스 가용성	6.2.1. 성능 및 용량 관리	클라우드컴퓨팅서비스의 가용성을 보장하기 위해 성능 및 용량에 대한 요구사항을 정의하고, 지속적으로 관리할 수 있는 모니터링 방법 또는 절차를 수립하여야 한다.
		6.2.2. 이중화 및 백업	정보처리설비(예 : 클라우드컴퓨팅서비스를 제공하는 물리적인 서버, 스토리지, 네트워크 장비, 통신 케이블, 접속 회선 등)의 장애로 서비스가 중단되지 않도록 정보 처리설비를 이중화하고, 장애 발생 시 신속하게 복구를 수행하도록 백업 체계도 마련하여야 한다.
		6.2.3. 서비스 가용성 점검	서비스 가용성에 대한 영향 평가를 주기적으로 점검하여야 한다.
7. 준거성	7.1. 법 및 정책 준수	7.1.1. 법적요구사항 준수	정보보호 관련 법적 요구사항을 식별하고 준수하여야 한다.
		7.1.2. 정보보호 정책 준수	정보보호 정책 및 서비스 수준 협약에 포함된 보안 요구사항을 식별하고 준수하며 이용자가 요구하는 경우 관련 증거를 제공하여야 한다.
	7.2. 보안 감사	7.2.1. 독립적 보안감사	법적 요구사항 및 정보보호 정책 준수 여부를 보증하기 위해 독립적 보안감사 계획을 수립하여 시행하고 개선 조치를 취하여야 한다.
		7.2.2. 감사기록 및 모니터링	보안감사 증적(로그)은 식별할 수 있는 형태로 기록 및 모니터링 되어야 되고 비인가 된 접근 및 변조로부터 보호되어야 한다.

물리적 보호조치

구 분			세부조치사항
8. 물리적 보안	8.1. 물리적 보호구역	8.1.1. 물리적 보호구역 지정	중요 정보 및 정보처리시설을 보호하기 위한 물리적 보안 구역(예 : 주요 정보처리 설비 및 시스템 구역, 사무실, 외부인 접견실 등)을 지정하고, 각 보안 구역에 대한 보안 대책을 마련하여야 한다.
		8.1.2. 물리적 출입통제	물리적 보안 구역에 인가된 자만이 접근할 수 있도록 출입을 통제하는 시설(예 : 경비원, 출입 통제 시스템 등)을 갖추어야 하고, 출입 및 접근 이력을 주기적으로 검토하여야 한다.
		8.1.3. 물리적 보호구역 내 작업	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 공간 보호	사무실 및 설비 공간에 대한 물리적인 보호방안을 수립하고 적용하여야 한다.
		8.1.5. 공공장소 및 운송 · 하역 구역 보호	공공장소 및 운송 · 하역을 위한 구역은 내부 정보처리시설로부터 분리 및 통제하여야 한다.
		8.1.6. 모바일 기기 반출 · 입	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 · 관리하여야 한다.
	8.2. 정보처리 시설 및 장비보호	8.2.1. 정보처리 시설의 배치	물리적 및 환경적 위험으로부터 잠재적 손상을 최소화하고 비인가 된 접근 가능성을 최소화하기 위하여, 정보처리시설 내 장비의 위치를 파악하고 배치하여야 한다.
		8.2.2. 보호설비	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 갖추어야 한다.
		8.2.3. 케이블 보호	데이터를 송수신하는 통신케이블이나 전력을 공급하는 전력 케이블은 손상이나 도청으로 부터 보호하여야 한다.
		8.2.4. 시설 및 장비 유지보수	정보처리시설은 가용성과 무결성을 지속적으로 보장할 수 있도록 유지보수하여야 한다.
		8.2.5. 장비 반출 · 입	장비의 미승인 반출·입을 통한 중요 정보 유출, 악성코드 감염 등의 침해사고 예방을 위하여, 보안 구역 내 직원 및 외부 업무 관련자에 의한 장비 반출·입 절차를 수립하고, 기록 및 관리하여야 한다.
		8.2.6. 장비 폐기 및 재사용	정보처리시설 내의 저장 매체를 포함하여 모든 장비를 파악하고, 민감한 데이터가 저장된 장비를 폐기하는 경우 복구 불가능하도록 하여야 한다. 또한 재사용하는 경우에도 복구 불가능 상태에서 재사용하여야 한다.

기술적 보호조치

구 분			세부조치사항
9. 가상화 보안	9.1. 가상화 인프라	9.1.1. 가상자원 관리	가상자원(가상 머신, 가상 스토리지, 가상 소프트웨어 등)의 생성, 변경, 회수 등에 대한 관리 방안을 수립하여야 한다.
		9.1.2. 가상자원 회수	이용자와의 계약 종료 시 가상자원 회수 절차에 따라 백업을 포함한 모든 클라우드 시스템에서 삭제하여야 한다.
		9.1.3. 가상자원 모니터링	가상자원에 대한 무결성 보장하기 위한 보호조치 및 가상자원의 변경(수정, 이동, 삭제, 복사)에 대해 모니터링 하여야 한다. 또한, 가상자원에 손상이 발생한 경우 이를 이용자에게 알려주어야 한다.
		9.1.4. 하이퍼바이저 보안	가상자원을 관리하는 하이퍼바이저의 기능 및 인터페이스에 대한 접근 통제 방안을 마련하여야 한다. 또한 하이퍼바이저에 대한 소프트웨어 업데이트 및 보안패치를 최신으로 유지하여야 한다.
		9.1.5. 공개서버 보안	가상자원을 제공하기 위한 웹사이트와 가상소프트웨어(앱, 응용프로그램)를 배포하기 위한 공개서버에 대한 물리적, 기술적 보호대책을 수립하여야 한다.
		9.1.6. 상호 운용성 및 이식성	클라우드컴퓨팅서비스 제공자는 표준화된 가상화 포멧, 이식성이 높은 가상화 플랫폼, 공개 API 등을 이용하여 클라우드컴퓨팅서비스 간의 상호 운용성 및 이식성을 높여야 한다.
	9.2. 가상 환경	9.2.1. 악성코드 통제	바이러스, 웜, 트로이목마 등의 악성코드로부터 이용자의 가상 환경(가상PC, 가상 서버, 가상 소프트웨어 등)을 보호하기 위한 악성코드 탐지, 차단 등의 보안기술을 지원하여야 한다. 또한 이상 징후 발견 시 이용자 통지하고 사용 중지 및 격리 조치를 수행하여야 한다.
		9.2.2. 인터페이스 및 API 보안	가상 환경(가상PC, 가상 서버, 가상 소프트웨어 등) 접근을 위한 인터페이스 및 API에 대한 보안 취약점을 주기적으로 분석하고, 이에 대한 보호방안을 마련하여야 한다.
		9.2.3. 데이터 이전	이용자가 기존 정보시스템 환경에서 클라우드컴퓨팅서비스의 가상 환경으로 전환 시 안전하게 데이터를 이전하도록 암호화 등의 기술적인 조치방안을 제공하여야 한다.
		9.2.4. 가상 소프트웨어 보안	클라우드컴퓨팅서비스 제공자는 출처, 유통경로 및 제작자가 명확한 소프트웨어로 구성된 가상환경을 제공하여야 한다.
	10.1. 접근통제 정책	10.1.1. 접근통제 정책 수립	비인가자의 접근을 통제할 수 있도록 접근통제 영역 및 범위, 접근통제 규칙, 방법 등을 포함하여 접근통제 정책을 수립하여야 한다.
		10.1.2. 접근기록 관리	접근기록 대상을 정의하고 서비스 통제, 관리, 사고 발생 책임 추적성 등을 보장할 수 있는 형태로 기록되고 유지하여야 한다.

구 분			세부조치사항
10. 접근통제	10.2. 접근 권한 관리	10.2.1. 사용자 등록 및 권한부여	클라우드 시스템 및 중요정보에 대한 접근을 통제하기 위하여 공식적인 사용자 등록 및 해지 절차를 수립하고 업무 필요성에 따라 사용자 접근권한을 최소한으로 부여하여야 한다.
		10.2.2. 관리자 및 특수 권한관리	클라우드 시스템 및 중요정보 관리 및 특수 목적을 위해 부여한 계정 및 권한을 식별하고 별도 통제하여야 한다.
		10.2.3. 접근권한 검토	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. 사용자 식별	클라우드 시스템에서 사용자를 유일하게 구분할 수 있는 식별자를 할당하고 추측 가능한 식별자 사용을 제한하여야 한다. 동일한 식별자를 공유하여 사용하는 경우 그 사유와 타당성을 검토하고 책임자의 승인을 받아야 한다.
		10.3.2. 사용자 인증	클라우드 시스템에 대한 접근은 사용자 인증, 로그인 횟수 제한, 불법 로그인 시도 경고 등 안전한 사용자 인증 절차에 의해 통제하여야 한다.
		10.3.3. 강화된 인증 수단 제공	이용자가 클라우드컴퓨팅서비스에 대해 다중 요소 인증 등 강화된 인증 수단을 요청하는 경우 이를 제공하기 위한 방안을 마련하여야 한다.
		10.3.4. 사용자 패스워드 관리	법적 요구사항, 외부 위협요인 등을 고려하여 패스워드 복잡도 기준, 초기 패스워드 변경, 변경주기 등 사용자 패스워드 관리절차를 수립·이행하고 패스워드 관리 책임이 사용자에게 있음을 주지시켜야 한다. 특히 관리자 패스워드는 별도 보호대책을 수립하여 관리하여야 한다.
		10.3.5. 이용자 패스워드 관리	고객, 회원 등 외부 이용자가 접근하는 클라우드 시스템 또는 웹서비스의 안전한 이용을 위하여 계정 및 패스워드 등의 관리절차를 마련하고 관련 내용을 공지하여야 한다.
11. 네트워크 보안	11.1. 네트워크 보안	11.1.1. 네트워크 보안 정책 수립	클라우드컴퓨팅서비스와 관련된 내·외부 네트워크에 대해 보안 정책과 절차를 수립하여야 한다.
		11.1.2. 네트워크 모니터링 및 통제	DDoS, 비인가 접속 등으로 인한 서비스 중단 및 중요 정보 유출 등을 막기 위해 네트워크를 모니터링하고 통제하여야 한다.
		11.1.3. 네트워크 정보보호 시스템 운영	클라우드컴퓨팅서비스와 관련된 내·외부 네트워크를 보호하기 위하여 정보보호시스템(방화벽, IPS, IDS, VPN 등)을 운영하여야 한다.
		11.1.4. 네트워크 암호화	클라우드 시스템에서 중요 정보가 이동하는 구간에 대해서는 암호화된 통신채널을 사용하여야 한다.
		11.1.5. 네트워크 분리	클라우드컴퓨팅서비스 제공자의 관리 영역과 이용자의 서비스 영역, 이용자 간 서비스 영역의 네트워크 접근은 물리적 또는 논리적으로 분리하여야 한다.

구 분			세부조치사항
		11.1.6. 무선 접근통제	클라우드 시스템은 무선망과 분리하고, 무선접속에 대한 접근을 통제하여야 한다. 무선접속을 사용하는 경우 그 사유와 타당성을 검토하고 책임자의 승인을 받아야 한다.
12. 데이터 보호 및 암호화	12.1. 데이터 보호	12.1.1. 데이터 분류	데이터 유형, 법적 요구사항, 민감도 및 중요도에 따라 데이터를 분류하고 관리하여야 한다.
		12.1.2. 데이터 소유권	이용자와 서비스 수준 협약 단계에서 데이터의 소유권을 명확하게 확립하여야 한다.
		12.1.3. 데이터 무결성	입 · 출력, 전송 또는 데이터 교환 및 저장소의 데이터에 대해 항상 데이터 무결성을 확인하여야 한다.
		12.1.4. 데이터 보호	데이터에 대한 접근제어, 위 · 변조 방지 등 데이터 처리에 대한 보호 기능을 이용자에게 제공하여야 한다.
		12.1.5. 데이터 추적성	이용자에게 데이터를 추적하기 위한 방안을 제공하고, 이용자가 요구하는 경우 구체적인 제공정보(이용자의 정보가 저장되는 국가의 명칭 등)를 공개하여야 한다.
		12.1.6. 데이터 폐기	클라우드컴퓨팅서비스 종료, 이전 등에 따른 데이터 폐기 조치 시 이용자와 관련된 모든 데이터를 폐기하여야 하며, 폐기된 데이터를 복구할 수 없도록 삭제 방안을 마련하여야 한다.
	12.2. 매체 보안	12.2.1. 저장매체 관리	중요정보를 담고 있는 하드디스크, 스토리지 등의 저장매체 폐기 및 재사용 절차를 수립하고 매체에 기록된 중요정보는 복구 불가능하도록 완전히 삭제하여야 한다.
		12.2.2. 이동매체 관리	중요정보 유출을 예방하기 위해 외장하드, USB, CD 등 이동매체 취급, 보관, 폐기, 재사용에 대한 절차를 수립하여야 한다. 또한 매체를 통한 악성코드 감염 방지 대책을 마련하여야 한다.
	12.3. 암호화	12.3.1. 암호 정책 수립	클라우드컴퓨팅서비스에 저장 또는 전송 중인 데이터를 보호하기 위해 암호화 대상, 암호 강도(복잡도), 키관리, 암호 사용에 대한 정책을 마련하여야 한다. 또한 정책에는 개인정보 저장 및 전송 시 암호화 적용 등 암호화 관련 법적 요구사항을 반드시 반영하여야 한다.
		12.3.2. 암호키 관리	암호키 생성, 이용, 보관, 배포, 파기에 관한 안전한 절차를 수립하고, 암호키는 별도의 안전한 장소에 보관하여야 한다.
13. 시스템 개발 및 도입 보안	13.1. 시스템 분석 및 설계	13.1.1. 보안요구사항정의	신규 시스템 개발 및 기존 시스템 변경 시 정보보호 관련 법적 요구사항, 최신 보안 취약점, 정보보호 기본요소(기밀성, 무결성, 가용성) 등을 고려하여 보안요구사항을 명확히 정의하고 이를 적용하여야 한다.
		13.1.2. 인증 및 암호화 기능	클라우드 시스템 설계 시 사용자 인증에 관한 보안요구사항을 반드시 고려하여야 하며 중요정보의 입·출력 및 송수신 과정에서 무결성, 기밀성이 요구될 경우 법적 요구사항을 고려하여야 한다.

구 분			세부조치사항
13. 시스템 개발 및 도입 보안	13.1. 시스템 분석 및 설계	13.1.3. 보안로그 기능	클라우드 시스템 설계 시 사용자의 인증, 권한 변경, 중요정보 이용 및 유출 등에 대한 감사증적을 확보할 수 있도록 하여야 한다.
		13.1.4. 접근권한 기능	클라우드 시스템 설계 시 업무의 목적 및 중요도에 따라 접근권한을 부여할 수 있도록 하여야 한다.
		13.1.5. 시각 동기화	로그기록의 정확성을 보장하고 법적인 자료로서 효력을 지니기 위해 클라우드 시스템 시각을 공식 표준시각으로 정확하게 동기화 하여야 한다. 또한 서비스 이용자에게 시각 정보 동기화 기능을 제공하여 한다.
	13.2. 구현 및 시험	13.2.1. 구현 및 시험	안전한 코딩방법에 따라 클라우드 시스템을 구현 하고, 분석 및 설계 과정에서 도출한 보안요구사항이 정보시스템에 적용되었는지 확인하기 위하여 시험을 수행하여야 한다.
		13.2.2. 개발과 운영환경 분리	개발 및 시험 시스템은 운영시스템에 대한 비인가 접근 및 변경의 위험을 감소하기 위해 원칙적으로 분리하여야 한다. 단 분리하여 운영하기 어려운 경우 그 사유와 타당성을 검토하고 안전성 확보 방안을 마련하여야 한다.
		13.2.3. 시험 데이터 보안	시스템 시험 과정에서 운영데이터 유출을 예방하기 위해 시험데이터 생성, 이용 및 관리, 파기, 기술적 보호조치에 관한 절차를 수립하여 이행하여야 한다.
		13.2.4. 소스 프로그램 보안	소스 프로그램에 대한 변경관리를 수행하고 인가된 사용자만이 소스 프로그램에 접근할 수 있도록 통제절차를 수립하여 이행하여야 한다. 또한 소스 프로그램은 운영환경에 보관하지 않는 것을 원칙으로 한다.
	13.3. 외주 개발 보안	13.3.1. 외주 개발 보안	클라우드 시스템 개발을 외주 위탁하는 경우 분석 및 설계단계에서 구현 및 이관까지의 준수해야 할 보안요구사항을 계약서에 명시하고 이행여부를 관리 · 감독하여야 한다.
	13.4. 시스템 도입 보안	13.4.1. 시스템 도입 계획	클라우드 시스템의 처리 속도와 용량에 대하여 주기적인 모니터링을 수행하고 안정성의 확보에 필요한 시스템 도입 계획을 수립하여야 한다.
		13.4.2. 시스템 인수	새로 도입되는 시스템에 대한 인수 기준이 수립되어야 하며, 인수 전에 테스트가 수행되어야 한다.

공공기관용 클라우드컴퓨팅서비스 추가 보호조치

구 분			세부조치사항
14. 공공기관 보안요구사항	14.1. 관리적 보호조치	14.1.1. 보안서비스 수준 협약	공공기관의 보안 요구사항이 반영된 보안서비스 수준 협약을 체결하고, 클라우드컴퓨팅서비스 관련 정보보호 정보를 공공기관에 제공하여야 한다.
		14.1.2. 도입 전산장비 안전성	클라우드컴퓨팅서비스 구축을 위해 도입되는 서버·PC 가상화 솔루션 및 정보보호 제품 중에 CC인증이 필수적인 제품군은 국내·외 CC인증을 받은 제품을 사용하여야 한다.
		14.1.3. 보안관리 수준	클라우드컴퓨팅서비스 운영 장소 및 망은 공공기관 내부 정보 시스템 운영 보안 수준에 준하여 보안 관리하여야 한다.
		14.1.4. 사고 및 장애 대응	클라우드컴퓨팅서비스를 제공하는 민간 사업자는 사고 또는 장애 발생 시 공공기관의 사고 · 장애 대응 절차에 따라 해당 공공기관, 대내 · 외 관련 기관 및 전문가와 협조체계를 구성하여 대응하여야 하며, 공공기관의 사고·장애 대응에 적극 협조하여야 한다.
	14.2. 물리적 보호조치	14.2.1. 물리적 위치 및 분리	클라우드 시스템 및 데이터의 물리적 위치는 국내로 한정하고, 공공기관용 클라우드컴퓨팅서비스의 물리자원(서버, 네트워크, 보안장비 등), 출입통제, 운영인력 등은 일반 이용자용 클라우드컴퓨팅서비스 영역과 분리하여 운영하여야 한다.
		14.2.2. 중요장비 이중화 및 백업체계 구축	클라우드컴퓨팅서비스를 제공하는 사업자는 네트워크 스위치, 스토리지 등 중요장비를 이중화하고 서비스의 가용성을 보장하기 위해 백업체계를 구축하여야 한다.
	14.3. 기술적 보호조치	14.3.1. 검증필 암호화 기술 제공	클라우드컴퓨팅서비스를 통해 생성된 중요자료를 암호화하는 수단을 제공하는 경우에는 검증필 국가표준암호화 기술을 제공하여야 한다.
		14.3.2. 보안관제 제반환경 지원	공공기관에 클라우드컴퓨팅서비스 보안관제 수행에 필요한 제반환경을 지원하여야 한다.

① SaaS용 통제항목표 (78개 통제항목)

관리적 보호조치

구 분			세부조치사항
1. 정보보호 정책 및 조직	1.1. 정보보호 정책	1.1.1. 정보보호 정책 수립	정보보호 정책을 문서화하고, 정보보호 최고책임자의 승인 후 정책에 영향을 받는 모든 임직원 및 외부 업무 관련자에게 제공하여야 한다
		1.1.2. 정보보호 정책 검토 및 변경	정보보호 정책의 타당성 및 효과를 연 1회 이상 검토하고, 관련 법규 변경 및 내·외부 보안사고 발생 등의 중대한 사유가 발생할 경우에는 추가로 검토하고 변경하여야 한다.
		1.1.3. 정보보호 정책문서 관리	정보보호 정책 및 정책 시행문서의 이력관리 절차를 수립하고 시행하며, 최신본으로 유지하여야 한다.
	1.2. 정보보호 조직	1.2.1. 조직 구성	정보보호 활동을 계획, 실행, 검토하는 정보보호 전담조직을 구성하고 정보보호 최고책임자를 임명하여야 한다.
		1.2.2. 역할 및 책임 부여	정보자산과 보안에 관련된 모든 임직원 및 외부 업무 관련자의 정보보호 역할과 책임을 명확하게 정의하여야 한다. 또한 서비스 이용자의 정보보호 역할과 책임도 서비스 수준 협약 등을 통해 명확하게 정의하여야 한다.
2. 인적보안	2.1. 내부인력 보안	2.1.1. 고용계약	고용 계약서에 정보보호 정책 및 관련 법률을 준수하도록 하는 조항 또는 조건을 포함시키고, 새로 채용하거나 합류한 근무 인력이 클라우드컴퓨팅서비스의 설비, 자원, 자산에 첩근이 허용되기 이전에 서명을 받아야 한다.
		2.1.2. 주요 직무자 지정 및 감독	클라우드컴퓨팅서비스의 시스템 운영 및 개발, 정보보호 등에 관련된 임직원의 경우 주요 직무자로 지정하여 관리하고, 직무 지정 범위는 최소화하여야 한다.
		2.1.3. 직무 분리	권한 오남용 등 내부 임직원의 고의적인 행위로 발생할 수 있는 잠재적인 위협을 줄이기 위하여 직무 분리 기준을 수립하고 적용하여야 한다.
		2.1.4. 비밀유지 서약서	정보보호와 개인정보보호 등을 위해 필요한 사항을 비밀유지서약서에 정의하고 주기적으로 갱신하여야 한다.
	2.2. 정보보호 교육	2.2.1. 교육 시행	모든 임직원 및 외부 업무 관련자를 대상으로 연 1회 이상 정보보호 교육을 시행하고 정보보호 정책 및 절차의 중대한 변경, 내·외부 보안사고 발생, 관련 법규 변경 등의 사유가 발생하면 추가 교육을 실시하여야 한다.
3. 자산관리	3.1. 자산 식별 및 분류	3.1.1. 자산 식별	클라우드컴퓨팅서비스에 사용된 정보자산(정보시스템, 정보보호시스템, 정보 등)에 대한 자산분류기준 수립하고 식별된 자산의 목록을 작성하여 관리하여야 한다.

구 분			세부조치사항
3. 자산관리	3.2. 자산 변경관리	3.2.1. 변경관리	클라우드컴퓨팅서비스에 사용된 자산(시설, 장비, 소프트웨어 등)의 변경이 필요한 경우 보안 영향 평가를 통해 변경 사항을 관리하여야 한다. 또한 이용자에게 큰 영향을 주는 변경에 대해서는 사전에 공지를 하여야 한다.
	3.3. 위험관리	3.3.1. 취약점 점검	취약점 점검 정책에 따라 주기적으로 기술적 취약점(예 : 유·무선 네트워크, 운영체제 및 인프라, 응용 프로그램 취약점 등)을 점검하고 보완하여야 한다.
4. 서비스 공급망 관리	4.1. 공급망 관리 정책	4.1.1. 공급망 관리 정책 수립	클라우드컴퓨팅서비스에 대한 접근과 서비스 연속성을 저해하는 위험을 식별하고 최소화하기 위해 공급망과 관련한 보안 요구사항을 정의하는 관리 정책을 수립하여야 한다.
		4.1.2. 공급망 계약	클라우드컴퓨팅서비스 범위 및 보안 요구사항을 포함하는 공급망 계약을 체결하고 다자간 협약 시 책임을 개별 계약서에 각각 명시해야하며, 해당 서비스에 관련된 모든 이해관계자에게 적용하여야 한다.
	4.2. 공급망 변경관리	4.2.1. 공급망 변경관리	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 제시하여야 한다.
5. 침해 사고관리	5.1. 침해사고 대응 절차 및 체계	5.1.1. 침해사고 대응 절차 수립	침해사고에 대한 효율적이고 효과적인 대응을 위해 신고절차, 유출 금지 대상, 사고처리 절차 등을 담은 침해사고 대응절차를 마련하여야 한다. 침해사고 대응절차는 이용자와 제공자의 책임과 절차가 포함되어야 한다.
		5.1.2. 침해사고 대응 체계 구축	침해사고 정보를 수집·분석·대응할 수 있는 보안관제 시스템 및 조직을 구성 · 운영하고, 침해사고 유형 및 중요도에 따라 보고 및 협력체계를 구축하여야 한다.
		5.1.3. 침해사고 대응 훈련 및 점검	침해사고 대응과 관련된 역할 및 책임이 있는 담당자를 훈련시켜야 하고, 주기적으로 침해사고 대응 능력을 점검하여야 한다.
	5.2. 침해사고 대응	5.2.1. 침해사고 보고	침해사고 발생 시 침해사고 대응절차에 따라 법적 통지 및 신고 의무를 준수하여야 한다. 또한 클라우드컴퓨팅서비스 이용자에게 발생 내용, 원인, 조치 현황 등을 신속하게 알려야 한다.
		5.2.2. 침해사고 처리 및 복구	침해사고 발생 시 침해사고 대응절차에 따라 처리와 복구를 신속하게 수행하여야 한다.
	5.3. 사후관리	5.3.1. 침해사고 분석 및 공유	침해사고가 처리 및 종결된 후 발생 원인을 분석하고 그 결과를 이용자에게 알려야 한다. 또한 유사한 침해사고에 대한 신속한 처리를 위해 침해사고 관련 정보 및 발견된 취약점을 관련 조직 및 임직원과 공유하여야 한다
		5.3.2. 재발방지	침해사고 관련 정보를 활용하여 유사한 침해사고가 반복되지 않도록 침해사고 재발방지 대책을 수립하고, 필요한 경우 침해사고 대응 체계도 변경하여야 한다.
6. 서비스 연속성 관리	6.1. 장애대응	6.1.1. 장애 대응절차 수립	관련 법률에서 규정한 클라우드컴퓨팅서비스의 중단으로부터 업무 연속성을 보장하기 위해 백업, 복구 등을 포함하는 장애 대응 절차를 마련하여야 한다.

구 분			세부조치사항
6. 서비스 연속성 관리	6.1. 장애대응	6.1.2. 장애 보고	클라우드컴퓨팅서비스 중단이나 피해가 발생 시 장애 대응절차에 따라 법적 통지 및 신고 의무를 준수하여야 한다. 또한 클라우드컴퓨팅서비스 이용자에게도 발생 내용, 원인, 조치 현황 등을 신속하게 알려야 한다.
		6.1.3. 장애 처리 및 복구	클라우드컴퓨팅서비스 중단이나 피해가 발생할 경우, 서비스 수준 협약(SLA)에 명시된 시간 내에 장애 대응절차에 따라 해당 서비스의 장애를 처리하고 복구시켜야 한다.
		6.1.4. 재발방지	장애 관련 정보를 활용하여 유사한 서비스 중단이 반복되지 않도록 장애 재발방지 대책을 수립하고, 필요한 경우 장애 대응 절차도 변경하여야 한다.
	6.2. 서비스 가용성	6.2.1. 성능 및 용량 관리	클라우드컴퓨팅서비스의 가용성을 보장하기 위해 성능 및 용량에 대한 요구사항을 정의하고, 지속적으로 관리할 수 있는 모니터링 방법 또는 절차를 수립하여야 한다.
		6.2.2. 이중화 및 백업	정보처리설비(예 : 클라우드컴퓨팅서비스를 제공하는 물리적인 서버, 스토리지, 네트워크 장비, 통신 케이블, 접속 회선 등)의 장애로 서비스가 중단되지 않도록 정보 처리설비를 이중화하고, 장애 발생 시 신속하게 복구를 수행하도록 백업 체계도 마련하여야 한다.
7. 준거성	7.1. 법 및 정책 준수	7.1.1. 법적요구사항 준수	정보보호 관련 법적 요구사항을 식별하고 준수하여야 한다
	7.2. 보안 감사	7.2.1. 독립적 보안감사	법적 요구사항 및 정보보호 정책 준수 여부를 보증하기 위해 독립적 보안감사 계획을 수립하여 시행하고 개선 조치를 취하여야 한다.
		7.2.2. 감사기록 및 모니터링	보안감사 증적(로그)은 식별할 수 있는 형태로 기록 및 모니터링 되어야 되고 비인가 된 접근 및 변조로부터 보호되어야 한다.

기술적 보호조치

구 분			세부조치사항
8. 가상화 보안	8.1. 가상화 인프라	8.1.1. 가상자원 관리	가상자원(가상 머신, 가상 스토리지, 가상 소프트웨어 등)의 생성, 변경, 회수 등에 대한 관리 방안을 수립하여야 한다.
		8.1.2. 공개서버 보안	가상자원을 제공하기 위한 웹사이트와 가상소프트웨어(앱, 응용프로그램)를 배포하기 위한 공개서버에 대한 물리적, 기술적 보호대책을 수립하여야 한다.
	8.2. 가상 환경	8.2.1. 악성코드 통제	바이러스, 웜, 트로이목마 등의 악성코드로부터 이용자의 가상 환경(가상PC, 가상 서버, 가상 소프트웨어 등)을 보호하기 위한 악성코드 탐지, 차단 등의 보안기술을 지원하여야 한다. 또한 이상 징후 발견 시 이용자 통지하고 사용 중지 및 격리 조치를 수행하여야 한다.
		8.2.2. 인터페이스 및 API 보안	가상 환경(가상PC, 가상 서버, 가상 소프트웨어 등) 접근을 위한 인터페이스 및 API에 대한 보안 취약점을 주기적으로 분석하고, 이에 대한 보호방안을 마련하여야 한다.
		8.2.3. 데이터 이전	이용자가 기존 정보시스템 환경에서 클라우드컴퓨팅서비스의 가상 환경으로 전환 시 안전하게 데이터를 이전하도록 암호화 등의 기술적인 조치방안을 제공하여야 한다.
		8.2.4. 가상 소프트웨어 보안	클라우드컴퓨팅서비스 제공자는 출처, 유통경로 및 제작자가 명확한 소프트웨어로 구성된 가상환경을 제공하여야 한다.
9. 접근통제	9.1. 접근통제 정책	9.1.1. 접근통제 정책 수립	비인가자의 접근을 통제할 수 있도록 접근통제 영역 및 범위, 접근통제 규칙, 방법 등을 포함하여 접근통제 정책을 수립하여야 한다.
		9.1.2. 접근기록 관리	접근기록 대상을 정의하고 서비스 통제, 관리, 사고 발생 책임 추적성 등을 보장할 수 있는 형태로 기록되고 유지하여야 한다.
	9.2. 접근 권한 관리	9.2.1. 사용자 등록 및 권한부여	클라우드 시스템 및 중요정보에 대한 접근을 통제하기 위하여 공식적인 사용자 등록 및 해지 절차를 수립하고 업무 필요성에 따라 사용자 접근권한을 최소한으로 부여하여야 한다.
		9.2.2. 관리자 및 특수 권한관리	클라우드 시스템 및 중요정보 관리 및 특수 목적을 위해 부여한 계정 및 권한을 식별하고 별도 통제하여야 한다.
		9.2.3. 접근권한 검토	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.
	9.3. 사용자 식별 및 인증	9.3.1. 사용자 식별	클라우드 시스템에서 사용자를 유일하게 구분할 수 있는 식별자를 할당하고 추측 가능한 식별자 사용을 제한하여야 한다. 동일한 식별자를 공유하여 사용하는 경우 그 사유와 타당성을 검토하고 책임자의 승인을 받아야 한다.

구 분			세부조치사항
9. 접근통제	9.3. 사용자 식별 및 인증	9.3.2. 사용자 인증	클라우드 시스템에 대한 접근은 사용자 인증, 로그인 횟수 제한, 불법 로그인 시도 경고 등 안전한 사용자 인증 절차에 의해 통제하여야 한다.
		9.3.3. 강화된 인증 수단 제공	이용자가 클라우드컴퓨팅서비스에 대해 다중 요소 인증 등 강화된 인증 수단을 요청하는 경우 이를 제공하기 위한 방안을 마련하여야 한다.
		9.3.4. 사용자 패스워드 관리	법적 요구사항, 외부 위협요인 등을 고려하여 패스워드 복잡도 기준, 초기 패스워드 변경, 변경주기 등 사용자 패스워드 관리절차를 수립·이행하고 패스워드 관리 책임이 사용자에게 있음을 주지시켜야 한다. 특히 관리자 패스워드는 별도 보호대책을 수립하여 관리하여야 한다.
		9.3.5. 이용자 패스워드 관리	고객, 회원 등 외부 이용자가 접근하는 클라우드 시스템 또는 웹서비스의 안전한 이용을 위하여 계정 및 패스워드 등의 관리절차를 마련하고 관련 내용을 공지하여야 한다.
10. 네트워크 보안	10.1. 네트워크 보안	10.1.1. 네트워크 보안 정책 수립	클라우드컴퓨팅서비스와 관련된 내·외부 네트워크에 대해 보안 정책과 절차를 수립하여야 한다.
		10.1.2. 네트워크 모니터링 및 통제	DDoS, 비인가 접속 등으로 인한 서비스 중단 및 중요 정보 유출 등을 막기 위해 네트워크를 모니터링하고 통제하여야 한다.
		10.1.3. 네트워크 정보보호 시스템 운영	클라우드컴퓨팅서비스와 관련된 내·외부 네트워크를 보호하기 위하여 정보보호시스템(방화벽, IPS, IDS, VPN 등)을 운영하여야 한다.
		10.1.4. 네트워크 암호화	클라우드 시스템에서 중요 정보가 이동하는 구간에 대해서는 암호화된 통신채널을 사용하여야 한다.
		10.1.5. 네트워크 분리	클라우드컴퓨팅서비스 제공자의 관리 영역과 이용자의 서비스 영역, 이용자 간 서비스 영역의 네트워크 접근은 물리적 또는 논리적으로 분리하여야 한다.
11. 데이터 보호 및 암호화	11.1. 데이터 보호	11.1.1. 데이터 분류	데이터 유형, 법적 요구사항, 민감도 및 중요도에 따라 데이터를 분류하고 관리하여야 한다.
		11.1.2. 데이터 소유권	이용자와 서비스 수준 협약 단계에서 데이터의 소유권을 명확하게 확립하여야 한다.
		11.1.3. 데이터 무결성	입 · 출력, 전송 또는 데이터 교환 및 저장소의 데이터에 대해 항상 데이터 무결성을 확인하여야 한다.
		11.1.4. 데이터 보호	데이터에 대한 접근제어, 위 · 변조 방지 등 데이터 처리에 대한 보호 기능을 이용자에게 제공하여야 한다.

구 분			세부조치사항
11. 데이터 보호 및 암호화	11.1. 데이터 보호	11.1.5. 데이터 추적성	이용자에게 데이터를 추적하기 위한 방안을 제공하고, 이용자가 요구하는 경우 구체적인 제공정보(이용자의 정보가 저장되는 국가의 명칭 등)를 공개하여야 한다.
		11.1.6. 데이터 폐기	클라우드컴퓨팅서비스 종료, 이전 등에 따른 데이터 폐기 조치 시 이용자와 관련된 모든 데이터를 폐기하여야 하며, 폐기된 데이터를 복구할 수 없도록 삭제 방안을 마련하여야 한다.
	11.2. 암호화	11.2.1. 암호 정책 수립	클라우드컴퓨팅서비스에 저장 또는 전송 중인 데이터를 보호하기 위해 암호화 대상, 암호 강도(복잡도), 키관리, 암호 사용에 대한 정책을 마련하여야 한다. 또한 정책에는 개인정보 저장 및 전송 시 암호화 적용 등 암호화 관련 법적 요구사항을 반드시 반영하여야 한다.
		11.2.2. 암호키 관리	암호키 생성, 이용, 보관, 배포, 파기에 관한 안전한 절차를 수립하고, 암호키는 별도의 안전한 장소에 보관하여야 한다.
12. 시스템 개발 및 도입 보안	12.1. 시스템 분석 및 설계	12.1.1. 보안요구사항정의	신규 시스템 개발 및 기존 시스템 변경 시 정보보호 관련 법적 요구사항, 최신 보안 취약점, 정보보호 기본요소(기밀성, 무결성, 가용성) 등을 고려하여 보안요구사항을 명확히 정의하고 이를 적용하여야 한다.
		12.1.2. 인증 및 암호화 기능	클라우드 시스템 설계 시 사용자 인증에 관한 보안요구사항을 반드시 고려하여야 하며 중요정보의 입·출력 및 송수신 과정에서 무결성, 기밀성이 요구될 경우 법적 요구사항을 고려하여야 한다.
		12.1.3. 보안로그 기능	클라우드 시스템 설계 시 사용자의 인증, 권한 변경, 중요정보 이용 및 유출 등에 대한 감사증적을 확보할 수 있도록 하여야 한다.
		12.1.4. 접근권한 기능	클라우드 시스템 설계 시 업무의 목적 및 중요도에 따라 접근권한을 부여할 수 있도록 하여야 한다.
		12.1.5. 시각 동기화	로그기록의 정확성을 보장하고 법적인 자료로서 효력을 지니기 위해 클라우드 시스템 시각을 공식 표준시각으로 정확하게 동기화 하여야 한다. 또한 서비스 이용자에게 시각 정보 동기화 기능을 제공하여 한다.
	12.2. 구현 및 시험	12.2.1. 구현 및 시험	안전한 코딩방법에 따라 클라우드 시스템을 구현 하고, 분석 및 설계 과정에서 도출한 보안요구사항이 정보시스템에 적용되었는지 확인하기 위하여 시험을 수행하여야 한다.
		12.2.2. 개발과 운영환경 분리	개발 및 시험 시스템은 운영시스템에 대한 비인가 접근 및 변경의 위험을 감소하기 위해 원칙적으로 분리하여야 한다. 단 분리하여 운영하기 어려운 경우 그 사유와 타당성을 검토하고 안전성 확보 방안을 마련하여야 한다.
		12.2.3. 시험 데이터 보안	시스템 시험 과정에서 운영데이터 유출을 예방하기 위해 시험데이터 생성, 이용 및 관리, 파기, 기술적 보호조치에 관한 절차를 수립하여 이행하여야 한다.
		12.2.4. 소스 프로그램 보안	소스 프로그램에 대한 변경관리를 수행하고 인가된 사용자만이 소스 프로그램에 접근할 수 있도록 통제절차를 수립하여 이행하여야 한다. 또한 소스 프로그램은 운영환경에 보관하지 않는 것을 원칙으로 한다.

구 분			세부조치사항
12. 시스템 개발 및 도입 보안	12.3. 외주 개발 보안	12.3.1. 외주 개발 보안	클라우드 시스템 개발을 외주 위탁하는 경우 분석 및 설계단계에서 구현 및 이관까지의 준수해야 할 보안요구사항을 계약서에 명시하고 이행여부를 관리·감독하여야 한다.

공공기관용 클라우드컴퓨팅서비스 추가 보호조치

구 분			세부조치사항
13. 공공기관 보안 요구사항	13.1. 관리적 보호조치	13.1.1. 보안서비스 수준 협약	공공기관의 보안 요구사항이 반영된 보안서비스 수준 협약을 체결하고, 클라우드컴퓨팅서비스 관련 정보보호 정보를 공공기관에 제공하여야 한다.
		13.1.2. 도입 전산장비 안전성	클라우드컴퓨팅서비스 구축을 위해 도입되는 서버·PC 가상화 솔루션 및 정보보호 제품 중에 CC인증이 필수적인 제품군은 국내·외 CC인증을 받은 제품을 사용하여야 한다.
		13.1.3. 보안관리 수준	클라우드컴퓨팅서비스 운영 장소 및 망은 공공기관 내부 정보 시스템 운영 보안 수준에 준하여 보안 관리하여야 한다.
		13.1.4. 사고 및 장애 대응	클라우드컴퓨팅서비스를 제공하는 민간 사업자는 사고 또는 장애 발생 시 공공기관의 사고·장애 대응 절차에 따라 해당 공공기관, 대내·외 관련 기관 및 전문가와 협조체계를 구성하여 대응하여야 하며, 공공기관의 사고·장애 대응에 적극 협조하여야 한다.
	13.2. 물리적 보호조치	13.2.1. 물리적 위치 및 분리	클라우드 시스템 및 데이터의 물리적 위치는 국내로 한정하고, 공공기관용 클라우드컴퓨팅서비스의 물리자원(서버, 네트워크, 보안장비 등), 출입통제, 운영인력 등은 일반 이용자용 클라우드컴퓨팅서비스 영역과 분리하여 운영하여야 한다.
		13.2.2. 중요장비 이중화 및 백업체계 구축	클라우드컴퓨팅서비스를 제공하는 사업자는 네트워크 스위치, 스토리지 등 중요장비를 이중화하고 서비스의 가용성을 보장하기 위해 백업체계를 구축하여야 한다.
	13.3. 기술적 보호조치	13.3.1. 검증필 암호화 기술 제공	클라우드컴퓨팅서비스를 통해 생성된 중요자료를 암호화하는 수단을 제공하는 경우에는 검증필 국가표준암호화 기술을 제공하여야 한다.

클라우드서비스 보안인증제 안내서

2019년 3월 인쇄
2019년 3월 발행

발행인 한국인터넷진흥원장
발행처 한국인터넷진흥원(KISA, Korea Internet & Security Agency)
전라남도 나주시 진흥길 9(빛가람동 301-2)
Tel : 1544-5118

인쇄처 (사)한국장애인유권자연맹인쇄사업부
Tel: 02-325-1585

〈비매품〉