국가핵심기술
클라우드 컴퓨팅 서비스 이용을 위한
보안관리 안내서

2025. 4

산업통상자원부

kaits 한국산업기술보호협회

안 내 사 항

- 본 안내서는 국가핵심기술을 보유·관리하고 있는 대상기관이 국가핵심기술을 클라우드 컴퓨팅 서비스를 이용하여 저장하는 경우 또는 클라우드 컴퓨팅 서비스를 통해 수출하는 경우에 지켜야 할 보안관리 사항으로, 「산업기술의 유출방지 및 보호에 관한 법률」(이하 '산업기술보호법') 제10조(국가핵심기술의 보호조치), 제11조(국가핵심기술의 수출 등) 및 「산업기술보호지침」 제17조(수출승인 신청 대상) 등 관계 법령과 지침, 「국가 클라우드 컴퓨팅 보안 가이드라인」(국가정보원), 「클라우드컴퓨팅서비스 보안인증제도 안내서」(과학기술정보통신부) 등을 토대로 작성되었습니다.

- 본 안내서의 보안관리 항목 등은 국가핵심기술을 보유·관리하고 있는 대상기관의 고유한 특성 및 실제 운영 환경에 맞게 적용하시면 됩니다.

- 또한, 본 안내서는 2025년 4월말 기준으로 제도적 사실 및 유효한 법규를 토대로 작성되었으므로, 이후 최신 개정 내용 및 구체적인 사실관계 등에 따라 달리 적용될 수 있음을 알려드립니다.

국가핵심기술
클라우드 컴퓨팅 서비스 이용을 위한
보안관리 안내서

Contents

안내서 개요

1장

1장 안내서 개요

목적 및 필요성

최근 모든 산업 분야에서 디지털 전환(Digital Transformation)이 가속화되면서 관련 시장이 매년 가파르게 성장하고 있음

이러한 흐름에 따라 클라우드 컴퓨팅 서비스 환경의 중요성이 더욱 커지고, 국가핵심기술을 보유·관리하고 있는 대상기관(이하 1장에서 '국가핵심기술 보유기관'이라 함)은 클라우딩 컴퓨팅 서비스 이용 준비를 거듭하고 있으며, 실제 국가핵심기술 보유기관의 일반영역에서 업무 수행 및 데이터 관리의 효율성 측면에서 클라우드 컴퓨팅 서비스 이용이 확산되는 추세임

* 국가핵심기술 보유기관의 클라우드 컴퓨팅 서비스 이용에 대한 수요가 확대되고 있으며, 클라우드 컴퓨팅 서비스를 통한 국가핵심기술 수출 유형도 발생

이에, 본 안내서는 국가핵심기술 보유기관이 클라우드 컴퓨팅 서비스 환경에서 국가핵심기술과 직·간접적으로 관련된 정보가 클라우드 컴퓨팅 서비스에 저장·처리되고, 외국기업 등에 접근권한의 부여·열람·사용 등을 허용하는 과정에서 준수해야 할 보안관리 사항을 안내하여, 국가핵심기술 보유기관이 클라우드 컴퓨팅 서비스를 안전하게 사용할 수 있도록 하는 것을 목적으로 함

따라서, 국가핵심기술 보유기관이 클라우드 컴퓨팅 서비스를 이용함에 있어, 보안관리 사항을 마련하고, 이행하기 위해 본 안내서를 활용할 것을 권고함

추진 경과

그간 클라우드 컴퓨팅 서비스 환경에서 적재(저장·처리)할 수 있는 국가핵심기술 관련 정보의 보안관리에 대한 고려사항을 검토하고 통제항목을 개발하기 위해,

산업부·국정원은 '국가핵심기술 클라우드 협의체*'를 구성('23.9월)하고, 다양한 전문가와 함께 클라우드 컴퓨팅 서비스 이용을 위한 조건 등을 검토하였으며, '범정부 기술유출 합동대응단'('24.11월)에서 추진 방향에 대해 논의한 바 있음

* 산업부, 국정원, 산업기술보호협회, 국가핵심기술 보유기관, 학계, 로펌 및 민간 전문가 등 20여명 구성

아울러, '제5차 산업기술의 유출방지 및 보호에 관한 종합계획'('24.12월)에 국가핵심기술 보유기관의 클라우드 컴퓨팅 서비스 이용에 따른 보호기준 마련 계획을 반영하였음

이후 국가핵심기술 클라우드 컴퓨팅 서비스 이용을 위한 구체적인 보안관리 안내서 초안을 마련하여, 국가핵심기술 보유기관과 클라우드 컴퓨팅 서비스 사업자를 대상으로 의견 수렴 및 간담회 등을 실시하였음(~'25.4월)

효 력

국가핵심기술 보유기관이 클라우드 컴퓨팅 서비스를 이용하고자 할 경우, 「산업기술보호법」, 「산업기술보호지침」 상 국가핵심기술의 보호조치를 준수하여야 함

이 안내서의 내용과 관련 법규가 서로 일치하지 않는 경우에는 「산업기술보호법」, 「산업기술보호지침」에 규정된 내용이 안내서보다 우선임

또한 국가핵심기술 보유기관 및 클라우드 컴퓨팅 서비스 사업자는 「산업기술보호법」, 「산업기술보호지침」, 본 안내서 외 클라우드 컴퓨팅 서비스 관련 법령을 준수하여야 함

구 성

본 안내서의 구성은 다음과 같음

제1장에서는 '국가핵심기술의 클라우드 컴퓨팅 서비스 이용을 위한 보안관리 안내서'의 전반적인 개요에 대해 설명함

제2장에서는 클라우드 컴퓨팅 서비스 환경 내 국가핵심기술 관련 정보를 저장·처리하는 경우, 국가핵심기술 보유기관과 클라우드 컴퓨팅 서비스 사업자가 준수해야 할 보안관리 항목을 제시함

제3장에서는 클라우드 컴퓨팅 서비스에 저장된 국가핵심기술 관련 정보에 외국기업 등에 접근권한 부여·열람·사용 등의 허용하는 경우, 국가핵심기술 보유기관과 클라우드 컴퓨팅 서비스 사업자가 준수해야 할 보안관리 항목을 제시함

별첨으로 국내·외 클라우드 컴퓨팅 서비스 관련 법·제도 현황에 대해 열거하고, 클라우드 컴퓨팅 서비스 환경에서의 국가핵심기술 보호 실태조사 체크리스트를 안내함

용어 정의

본 안내서에서 사용되는 용어정의는 아래 표와 같음

용 어	정 의
국가핵심기술의 보호조치	▸ 「산업기술보호법」 제10조, 동법 시행령 제14조, 「산업기술 보호지침」 제8조 내지 제16조에 따른 국가핵심기술의 보호 조치를 말함
산업기술보호지침	▸ 「산업기술보호법」 제8조 및 동법 시행령 제10조에 따라 국가 핵심기술 등 산업기술의 유출을 방지하고 보호하기 위해 필요한 사항을 규정한 지침을 말함
클라우드 컴퓨팅 서비스	▸ 인터넷을 통해 컴퓨팅 리소스를 사용할 수 있는 서비스로, 스토리지, 서버, 네트워킹, 소프트웨어 등을 말함
클라우드 컴퓨팅 서비스 이용자	▸ 「산업기술보호법」에 따라 국가핵심기술을 보유·관리하고 있는 대상기관을 말함
클라우드 컴퓨팅 서비스 사업자	▸ 클라우드 기반의 컴퓨팅 서비스를 제공하는 업체로 AWS (아마존), Azure(마이크로소프트), NAVER Cloud(네이버), kt cloud(케이티) 등이 있음
공급망	▸ 제품 생산을 위한 원재료(raw material)부터 완제품 (final product)이 최종소비자에게 전달되기까지의 재화, 서비스 및 정보의 흐름이 이뤄지는 연결망을 뜻함
서비스 연속성	▸ 조직이 중단 사태가 발생했을 때에도 클라우드 컴퓨팅 서비스를 제공할 수 있는 능력을 의미함
가상화 보안	▸ 가상화된 환경에서 시스템, 네트워크, 데이터 등을 보호하는 것을 의미함
하이퍼바이저	▸ 단일 물리적 머신에서 여러 가상 머신을 실행하는데 사용할 수 있는 소프트웨어를 의미함

설계 과정

[1단계] 국가핵심기술 보유기관 및 클라우드 컴퓨팅 서비스 사업자 개별 보안관리 항목 도출

이 용 자	▸「국가 클라우드 컴퓨팅 보안 가이드라인」(국정원) 참고
제 공 자	▸「클라우드컴퓨팅서비스 보안인증제도 안내서」(과기부) 참고

[2단계] 산업보안 체계로 도출 항목 재구성 및 항목별 이행주체 구분

①관리적 보안, ②물리적 보안, ③기술적 보안, ④보안사고 대응, ⑤수출 시 보안관리

[3단계] 국가핵심기술 보유기관이 클라우드 컴퓨팅 서비스 이용 시, 현재 또는 향후에 발생 가능한 보안 위험성 등을 고려, 국가핵심기술 보호조치 및 수출 시, 보안관리의 특화된 항목 개발

[4단계] 국가핵심기술 보유기관과 클라우드 컴퓨팅 서비스 사업자간 책임 공유 또는 협업 항목 추가

[1단계] 국가핵심기술 보유기관 및 클라우드 컴퓨팅 서비스 사업자 개별 보안관리 항목 도출

☞ 국가핵심기술 보유기관의 경우, 국가·공공기관의 클라우드 컴퓨팅 도입 시, 보안수준을 향상시킬 수 있는 보안성 확인 기준인 「국가 클라우드 컴퓨팅 보안 가이드라인」(국정원)을 참고하여 이용자 문항 도출

☞ 클라우드 컴퓨팅 서비스 사업자의 경우, 제공하는 서비스에 대해 「클라우드 컴퓨팅 발전 및 이용자 보호에 관한 법률」 제23조의2에 따라 정보보호 수준의 향상 및 보장을 위한 「클라우드컴퓨팅서비스 보안인증제도 안내서」(과기부)를 참고하여 제공자 문항 도출

이용자 예시

국가 클라우드 컴퓨팅 보안 가이드라인		도출 항목
▸이용기관은 민간 사업자가 클라우드 컴퓨팅 서비스망을 대상으로 자체적으로 수행한 운용관리에 대한 보안 취약성 개선 결과를 주기적으로 보고받아야 한다.		▸▲이용자는 제공자가 자체 또는 외부 전문기관으로부터 수행한 클라우드 컴퓨팅 서비스 운용관리 전반에 대한 보안 취약점 개선 결과를 확인하여야 하며, ▲제공자는 운용관리 전반에 대한 보안 취약점 점검을 정기적으로 이행하고, 점검 및 개선 결과를 이용자에게 제공하여야 한다.
▸이용기관은 민간 사업자가 클라우드 컴퓨팅 서비스망에 대하여 자체적으로 실시한 모의훈련 및 취약점 점검 결과를 주기적으로 확인하여야 한다.		
▸이용기관은 중요 업무자료에 대한 암호화 수준 등에 대한 보안 요구사항을 도출하여 계약 시 반영하여야 하며, 중요 업무자료에 대한 생성·보관·처리·수신하기 위한 정책적·기술적 방안을 민간 사업자로부터 제공받아야 한다.	⇨	▸국가핵심기술 관련 정보에 대한 ▲암호화 수준에 대한 보안 요구사항을 도출하여 계약 시 반영하여야 하며, ▲생성된 국가핵심기술 관련 정보에 대한 생성·보관·처리·수신하기 위한 기술적 방안 등을 제공자에게 제공받아야 한다.
▸이용기관은 침해사고 발생 시 민간 사업자로부터 발생내용, 원인, 조치현황 등을 신속하게 파악하고 「국가 정보보안 기본지침」에 명시된 사고 대응 절차를 수행하여야 한다.		▸클라우드 컴퓨팅 서비스와 관련하여 ▲침해사고 발생 시, 제공자로부터 발생내용, 원인, 조치현황 등을 신속하게 파악하고, ▲사고대응 절차를 수행하여야 한다.

제공자 예시

클라우드컴퓨팅 서비스 보안인증제도 안내서		도출 항목
▸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.		▸▲이용자의 국가핵심기술 관련 정보 자산이 저장되는 시설을 보호하기 위한 물리적 보호구역을 지정하고, ▲각 보호구역에 대한 보안대책을 마련·이행하여야 한다.
▸클라우드 시스템, 백업 시스템 및 데이터와 이를 위한 관리·운영 인력의 물리적 위치는 국내로 한정하여야 한다.		▲클라우드 시스템, 백업시스템 및 데이터와 이를 위한 관리·운영 인력의 물리적 위치는 국내로 한정하여야 하며, ▲관련 보안기능을 제공하여야 한다.
▸클라우드컴퓨팅서비스 제공자의 관리 영역과 이용자의 서비스 영역, 이용자간 서비스 영역의 네트워크 접근은 물리적 또는 논리적으로 분리하여야 한다.	⇨	▸제공자의 관리 영역과 이용자의 서비스 영역, 이용자 간 서비스 영역의 네트워크 접근은 물리적 또는 논리적으로 분리하여야 한다.
▸입·출력, 전송 또는 데이터 교환 및 저장소의 데이터에 대해 항상 데이터 무결성을 확인하여야 한다.		▸이용자의 국가핵심기술 관련 정보의 입·출력, 전송 또는 교환 및 저장에 대한 제공자의 정보 무결성 확인 방안이 마련되어야 한다.
▸이용자에게 데이터를 추적하기 위한 방안을 제공하고, 이용자가 요구하는 경우 구체적인 제공정보(이용자의 정보가 저장되는 위치 정보 등)를 공개하여야 한다.		▸▲이용자에게 국가핵심기술 관련 정보를 추적하기 위한 방안을 제공하고, ▲이용자가 요구하는 경우, 구체적인 제공 정보(이용자의 정보가 저장되는 위치정보 등)를 공개하여야 한다.

[2단계] 산업보안 체계로 도출 항목 재구성 및 항목별 이행주체 구분

- 「국가 클라우드 컴퓨팅 보안 가이드라인」 보안기준의 경우, 1. 보안 기본원칙(가. 정책적 측면에서의 기본원칙, 나. 기술적 측면에서의 기본원칙), 2. 세부 보안기준(①정책, ②클라우드 인프라, ③가상환경 보안, ④데이터, ⑤인증 및 권한, ⑥사고 및 장애대응)으로 구성되어 있으며,
- 「클라우드컴퓨팅서비스 보안인증제도 안내서」의 경우, 1. 정보보호 정책 및 조직, 2. 인적보안 ~ 13. 시스템 개발 및 도입 보안 및 14. 국가기관 등의 보안요구사항으로 구성되어 있음

☞ 본 안내서의 경우, 산업보안 체계를 바탕으로 다음과 같이 구성하였음

구 분	분 류		이행주체
1	기본원칙		공 통 / 이용자 / 제공자
2	관리적 보안	①규 정	공 통
		②정 책	공 통 / 이용자
		③인 력	공 통 / 이용자 / 제공자
		④자 산	제공자
		⑤보안감사	제공자
3	물리적 보안	①보호구역	제공자
		②시설 및 장비 등 인프라	제공자
4	기술적 보안	①자료·데이터	공 통 / 이용자 / 제공자
		②인증 및 권한	공 통 / 이용자 / 제공자
		③네트워크	공 통 / 이용자 / 제공자
		④공급망	제공자
		⑤가상화	제공자
		⑥시스템 개발 및 도입 보안	제공자
5	보안사고 대응	①사 고	공 통 / 이용자 / 제공자
		②장 애	공 통 / 제공자
		③가용성	제공자
6	수출 시, 보안관리		공 통 / 이용자

[3단계] 국가핵심기술 보유기관이 클라우드 컴퓨팅 서비스 이용 시, 현재 또는 향후에 발생 가능한 보안 위험성 등을 고려, 국가핵심기술 보호조치 및 수출 시, 보안관리의 특화된 항목 개발

클라우드 컴퓨팅 서비스 이용 시 보안 위험성

① 국가핵심기술 보유기관 관리자의 실수로 인한 정보 노출 또는 악의적인 정보 유출

② 국가핵심기술 관련 정보가 어느 장소에 어떠한 형태로 저장되어 있는지 알 수 없음

③ 클라우드 컴퓨팅 서비스(가상화 환경) 자체에 대한 보안 취약점(해킹) 존재

④ 재해 및 재난 등에 의한 클라우드 컴퓨팅 서비스 운영 장애

⑤ 클라우드 컴퓨팅 서비스 사업자가 국가핵심기술 관련 정보에 임의 접근 가능(물리적 직접 접근 + 논리적 간접 접근)

⑥ 클라우드 컴퓨팅 서비스 사업자 본사(해외)에서 원격 접속하여, 클라우드 컴퓨팅 서비스에 대한 유지보수 작업 진행

⑦ 클라우드 컴퓨팅 서비스 사업자 대상으로 클라우드 데이터 센터에 대한 점검 비협조

⑧ 클라우드 컴퓨팅 서비스 사업자가 사업을 종료·철수·폐업하는 경우

⑨ 해외 정부기관(법원 등)에 의한 국가핵심기술 관련 정보의 노출 가능성 존재

⑩ 외국기업 등에 접근권한 허용 시, 접근권한 허용 대상 외 열람 가능, 국가핵심기술 관련 정보 임의 저장 등

국가핵심기술의 보호조치		클라우드 컴퓨팅 서비스 보안관리 항목
(시행령 제14조제1호) 국가핵심기술에 대한 보호 등급의 부여와 보안관리규정의 제정	⇨	▸이용자와 제공자는 보안관리 규정 내 클라우드 컴퓨팅 서비스 보안관리(관리적, 물리적, 기술적 보안관리, 보안사고 대응 등)의 내용을 마련하여야 한다.
(시행령 제14조제2호) 국가핵심기술 관리책임자와 보안 전담인력의 지정		▸이용자와 제공자는 클라우드 컴퓨팅 서비스 정보자산과 보안에 관련된 모든 임직원 및 외부 업무 관련자의 보안 역할과 책임을 명확하게 정의하여야 한다.
(시행령 제14조제3호) 국가핵심기술 보호구역의 통신시설과 통신수단에 대한 보안		▸제공자는 장비의 미승인 반출입을 통한 이용자의 국가핵심기술 관련 정보 자산 유출, 악성코드 감염 등의 침해사고 예방을 위하여, ▲보호구역 내 임직원 및 외부 업무 관련자에 의한 장비 반출입 절차를 수립하고, ▲기록 및 관리하여야 한다.
(시행령 제14조제4호) 국가핵심기술 관련 정보의 처리 과정과 결과에 관한 자료의 보호		▸▲이용자는 클라우드 컴퓨팅 서비스와 분리된 별도의 안전한 장소에서 저장·관리하고 있는 고유한 키를 활용하여 해당 데이터를 암호화하여 관리해야 하며, 제공자의 고유한 키를 활용하여 추가적인 암호화를 진행하여 해당 데이터를 저장하여야 한다. ▲제공자는 이용자가 별도로 보유한 키를 활용하여 암호화된 데이터에 대해 추가적인 암호화를 수행할 수 있도록 필요한 제반 환경을 제공하여야 한다.
(시행령 제14조제5호) 국가핵심기술을 취급하는 전문인력의 구분 및 관리		▸이용자와 제공자는 클라우드 컴퓨팅 서비스의 ▲시스템 운용, 개발 및 보안 등에 관련된 임직원의 경우, 주요 직무자로 지정하여 관리하고, ▲직무지정 범위는 최소화하여야 한다.
(시행령 제14조제6호) 국가핵심기술을 취급하는 전문인력에 대한 보안교육 실시		▸이용자와 제공자는 관련 법률, 국가핵심기술 보호조치 사항, 클라우드 보안사고 사례, 사고에 따른 법적 책임, 침해신고를 포함한 사고 대응 방법 등이 포함된 직무별, 담당 분야별 교육을 정기적으로 수행하여야 한다.
(시행령 제14조제7호) 국가핵심기술의 유출 사고에 대한 대응체제 구축		▸이용자는 클라우드 컴퓨팅 서비스와 관련하여 침해사고 발생 시, ▲제공자로부터 발생내용, 원인, 조치현황 등을 신속하게 파악하고, ▲사고대응 절차를 수행하여야 한다.

수출 시 보안관리 항목
▸외국기업 등의 접근권한 허용 대상에 ▲최소한의 권한을 부여하고, ▲필요한 국가핵심기술 관련 정보만 식별하여 ▲최소한으로 제공하여야 한다.
▸외국기업 등의 접근권한 허용 대상 전원에 대해 보안서약서 징구 및 보안교육을 정기적으로 시행하여야 한다.

[4단계] 국가핵심기술 보유기관과 클라우드 컴퓨팅 서비스 사업자간 책임 공유 또는 협업 항목 추가

구 분	보안관리 항목
기본원칙	▸이용자와 제공자는 클라우드 컴퓨팅 서비스 환경 內 또는 이용자가 외국기업 등의 접근 권한 허용하는 경우, 국가핵심기술 관련 정보 보호를 위해 보안 협업 대책을 지속적으로 마련하여야 한다.
관리적 보안관리 – 정책	▸▲이용자는 제공자가 자체 또는 외부 전문기관으로부터 수행한 클라우드 컴퓨팅 서비스 운용관리 전반에 대한 보안 취약점 개선 결과를 확인하여야 하며, ▲제공자는 운용관리 전반에 대한 보안 취약점 점검을 정기적으로 이행하고, 점검 및 개선 결과를 이용자에게 제공하여야 한다.
기술적 보안관리 – 자료·데이터	▸이용자는 제공자와 협의하여 클라우드 컴퓨팅 서비스에 저장 또는 전송 중인 국가핵심기술 관련 정보를 보호하기 위해 암호화 대상, 암호 강도(복잡도), 키관리, 암호 사용에 대한 정책을 마련·이행하여야 한다.
기술적 보안관리 – 네트워크	▸▲이용자는 국가핵심기술 관련 정보 보호를 위해 보안관제 체계를 구축하고, 실시간 모니터링을 수행하여야 한다. ▲제공자는 이용자의 보안관제 수행에 필요한 제반사항(로그기록 등)을 지원하여야 한다.
보안사고 대응 – 사고	▸▲이용자는 클라우드 컴퓨팅 서비스 이용 계약 시, 제공자의 사고조사에 대한 적극적인 협조 및 지원의무를 명시하여야 하며, ▲제공자는 산업통상자원부, 국가정보원 및 이용자의 조사 요청에 협조하여야 한다.

클라우드 컴퓨팅 서비스 환경 內 국가핵심기술 관련 정보를 저장·처리하는 경우

2장

2장 클라우드 컴퓨팅 서비스 환경 內 국가핵심기술 관련 정보를 저장·처리하는 경우

기본원칙

이용자

국가핵심기술을 보유·관리하고 있는 대상기관의 장(이하 '이용자'라 함)이 클라우드 컴퓨팅 서비스를 이용하고자 하는 경우, 「산업기술보호법」 제10조, 동법 시행령 제14조, 「산업기술보호지침」 제8조 내지 제16조의 ▲국가핵심기술의 보호조치 등에 관한 보안관리 수준을 클라우드 컴퓨팅 환경에서도 유지해야 하며, ▲아래와 같은 추가적인 관리적·물리적·기술적 보안관리 및 보안사고 대응절차 마련·이행을 하여야 한다.

클라우드 컴퓨팅 서비스 이용의 종료, 이전 등에 따른 국가핵심기술 관련 정보 폐기 조치 시, ▲제공자에게 관련된 모든 정보 폐기를 요청하여야 하며, 폐기된 정보를 복구할 수 없도록 삭제되었는지 제공자의 협조를 통해 ▲완전 삭제·폐기되었음을 확인하여야 한다.

제공자

클라우드 컴퓨팅 서비스 사업자*(이하 '제공자'라 함)는 이용자의 국가핵심기술 보호조치와 보안관리 사항에 적극 협조하여야 한다.

이용자의 국가핵심기술 관련 정보가 저장·처리 등을 위해 클라우드 컴퓨팅

서비스 이용 시, ▲클라우드 시스템, 백업시스템 및 데이터와 이를 위한 관리·운영 인력의 물리적 위치는 국내로 한정하여야 하며, ▲관련 보안기능을 제공하여야 한다.

이용자의 국가핵심기술 관련 정보가 저장·처리되는 공간에 대한 물리적 위치정보(시, 도 수준)를 이용자에게 제공하여야 한다.

▲이용자의 국가핵심기술 관련 정보에 대해 접근하지 않는다는 것을 보장해야 한다. 클라우드 컴퓨팅 서비스 운용을 위해 ▲부득이한 경우(사고 및 장애 대응, 유지보수 등), 이용자에 사전 승인을 받고 진행해야 하며, 이용자의 국가핵심기술 관련 정보에 접근하는 동안의 ▲모든 로그(log) 기록은 저장되어야 하며, ▲이용자에게 제공하여야 한다.

클라우드 컴퓨팅 서비스 종료 시, ▲이용자에게 최소 6개월 이전에 사전 통보를 하고, ▲이용자가 국가핵심기술 관련 정보를 안전하게 이전할 수 있도록 적극 협조하여야 한다.

클라우드 컴퓨팅 서비스 이용의 종료, 이전 등에 따른 국가핵심기술 관련 정보 폐기 조치 시, ▲이용자와 관련된 모든 정보를 폐기하여야 하며, ▲폐기된 데이터를 복구할 수 없도록 삭제 방안을 마련·이행하여야 하며, ▲이용자에게 완전 삭제·폐기되었음을 확인할 수 있는 자료 등을 제공하여야 한다.

공 통

▲이용자는 클라우드 컴퓨팅 서비스와 분리된 별도의 안전한 장소에서 저장·관리하고 있는 고유한 키를 활용하여 해당 데이터를 암호화하여 관리해야 하며, 제공자의 고유한 키를 활용하여 추가적인 암호화(이중 암호화)를 진행하여 해당 데이터를 저장하여야 한다. ▲제공자는 이용자가 별도로 보유한 키를 활용하여 암호화된 데이터에 대해 추가적인 암호화(이중 암호화)를 수행할 수 있도록 필요한 제반 환경을 제공하여야 한다.

이용자와 제공자는 클라우드 컴퓨팅 서비스 환경 內 국가핵심기술 관련 정보 보호를 위해 보안 협업 대책을 지속적으로 마련하여야 한다.

이용자와 제공자는「산업기술보호법」제17조 등에 따라 실시하는 클라우드 컴퓨팅 서비스 환경에서의 국가핵심기술의 보호 및 관리 현황에 대한 실태조사에 적극 협조하여야 한다.

관리적 보안

구 분	이행주체	보안관리
①규 정	공 통	•보안관리 규정 내 ▲클라우드 컴퓨팅 서비스 보안관리(관리적, 물리적, 기술적 보안관리, 보안사고 대응 등)의 내용을 마련하여야 하며, ▲규정에 영향을 받는 모든 임직원 및 외부 업무 관련자에게 제공하여야 한다. •클라우드 컴퓨팅 서비스 ▲보안관리 규정의 적합성, 적절성, 유효성 등에 대해 정기적으로 검토하고, ▲관련 법률 변경 및 내·외부 보안사고 발생 등의 중대한 사유가 발생한 경우에는 추가로 검토하고 변경하여야 한다. •클라우드 컴퓨팅 서비스 ▲보안관리 규정 및 규정 시행문서의 이력관리 절차를 수립·시행하며, ▲최신본으로 유지하여야 한다.
②정 책	공 통	•클라우드 컴퓨팅 서비스 정보자산과 보안에 관련된 모든 임직원 및 외부 업무 관련자의 보안 역할과 책임을 명확하게 정의하여야 한다. •▲이용자는 제공자가 자체 또는 외부 전문기관으로부터 수행한 클라우드 컴퓨팅 서비스 운용관리 전반에 대한 보안 취약점 개선 결과를 확인하여야 하며, ▲제공자는 운용관리 전반에 대한 보안 취약점 점검을 정기적으로 이행하고, 점검 및 개선 결과를 이용자에게 제공하여야 한다.
	이용자	•클라우드 컴퓨팅 서비스 이용을 위해 제공자와 계약 시, ▲관련 법률 및 지침, 가이드, 보안체계, 이용자 보안 사항 등을 고려한 보안 요구사항을 정의하고, ▲국가핵심기술과 관련한 보호조치 위반, 보안사고 발생에 관한 책임사항 등의 내용을 반영하여야 한다. •클라우드 컴퓨팅 서비스 도입·운용에 있어 사용자와 관리자를 지정·운용하여야 한다. •클라우드 컴퓨팅 서비스 환경으로 ▲이전(저장·처리)될 국가핵심기술 관련 정보 자산에 대한 관리정책을 마련하고, ▲정보자산 목록관리를 하여야 한다.
③인 력	공 통	•클라우드 컴퓨팅 서비스의 ▲시스템 운용, 개발 및 보안 등에

구 분	이행주체	보안관리
		관련된 임직원의 경우, 주요 직무자로 지정하여 관리하고, ▲직무지정 범위는 최소화하여야 한다. •외부 인력(외부 유지보수 직원, 외부 용역자 포함)에 의한 국가핵심기술 관련 정보 자산 접근 등과 관련된 보안 요구사항을 계약에 반영하여야 한다. •외부 인력에 대해 계약서에 명시한 ▲보안 요구사항 준수 여부를 정기적으로 점검하고, ▲위반사항이나 침해사고 발생 시 적절한 조치를 수행하여야 한다. •외부 인력과의 계약 만료 시, 자산 반납, 접근권한의 회수, 국가핵심기술 관련 정보 파기, 업무 수행 시 알게 된 정보의 대한 비밀유지서약 등을 확인·이행하여야 한다.
	이용자	•클라우드 컴퓨팅 서비스를 제공하는 ▲시스템에 접근 가능한 사용자와 관리자를 식별하고, ▲직무별 권한 부여, 폐기 등에 관한 절차를 마련하여야 한다. •관련 법률, 국가핵심기술 보호조치 사항, 클라우드 보안사고 사례, 사고에 따른 법적 책임, 침해신고를 포함한 사고 대응 방법 등이 포함된 직무별, 담당 분야별 교육을 정기적으로 수행하여야 한다.
	제공자	•관련 법률, 클라우드 보안사고 사례, 사고에 따른 법적 책임, 침해신고를 포함한 사고 대응 방법 등이 포함된 직무별, 담당 분야별 교육을 정기적으로 수행하여야 한다.
④자 산	제공자	•클라우드 컴퓨팅 서비스에 사용된 ▲정보자산(정보, 정보시스템, 정보보호시스템 등)에 대한 자산분류 기준을 수립하고, ▲식별된 자산의 목록을 작성하여 관리하여야 한다. •식별된 자산마다 책임자 및 관리자를 지정하여 책임소재를 명확히 하여야 한다. •기밀성, 무결성, 가용성, 법적요구사항 등을 고려하여 ▲자산의 보안 등급을 부여하고, ▲보안 등급별 취급 절차에 따라 관리

구 분	이행주체	보안관리
		하여야 한다. •클라우드 컴퓨팅 서비스에 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. •클라우드 컴퓨팅 서비스에 사용된 ▲자산(시설, 장비, 소프트웨어 등)의 변경을 지속적으로 모니터링하여 허가 받지 않은 변경을 탐지하고, ▲최신의 변경 이력을 유지하여야 한다. •클라우드 컴퓨팅 서비스에 사용된 자산(시설, 장비, 소프트웨어 등)의 변경 후에는 보안성 및 호환성 등에 대한 작업 검증을 수행하여야 한다. •관리적, 기술적, 물리적, 보안사고 대응 등 보안 전 영역에 대한 위험식별 및 평가가 가능하도록 위험관리 방법과 계획을 사전에 수립하여야 한다. •취약점 점검 정책에 따라 정기적으로 기술적 취약점(유·무선 네트워크, 운영체제 및 인프라, 응용 프로그램 등)을 점검하고 보완하여야 한다. •위험관리 방법 및 계획에 따라 ▲보안 전 영역에 대한 위험 식별 및 평가를 정기적으로 수행하고, ▲그 결과에 따라 수용 가능한 위험수준을 설정하여 관리하여야 한다. •법규 및 계약 관련 요구사항과 위험수용 수준을 고려하여 위험 평가 결과에 따라 통제할 수 있는 방법을 선택하여 처리하여야 한다.
⑤보안감사	제공자	•법적 요구사항 및 보안 정책 준수 여부를 보증하기 위해 ▲독립적 보안감사 계획을 수립하여 정기적으로 시행하고, ▲개선 조치를 취하여야 한다. •▲보안감사 증적(로그)은 식별할 수 있는 형태로 기록 및 모니터링 되어야 되고, ▲비인가된 접근 및 변조로부터 보호되어야 한다.

물리적 보안

구 분	이행주체	보안관리
①보호구역	제공자	•▲이용자의 국가핵심기술 관련 정보 자산이 저장되는 시설을 보호하기 위한 물리적 보호구역을 지정하고, ▲각 보호구역에 대한 보안대책을 마련·이행하여야 한다. •물리적 보호구역에 ▲인가된 자만이 접근할 수 있도록 출입을 통제하는 시설을 갖추어야 하고, ▲출입 및 접근 이력을 정기적으로 검토하여야 한다. •▲물리적 보호구역 내에서의 유지보수 등의 작업 절차를 수립하고, ▲작업에 대한 기록을 정기적으로 검토하여야 한다. •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. •각 보호구역의 중요도 및 특성에 따라 화재, 전력 이상 등 인재 및 자연재해 등에 대비하여 필요한 설비(화재 감지기, 소화 설비, 누수 감지기, 항온 항습기, 무정전 전원 장치(UPS), 이중 전원선 등)를 갖추어야 한다.
②시설 및 장비 등 인프라	제공자	•물리적 및 환경적 위험으로부터 잠재적 손상 및 비인가된 접근 가능성을 최소화하기 위하여, 정보처리시설 내 장비의 위치를 파악하고, 배치하여야 한다. •정보를 송수신하는 통신케이블이나 전력을 공급하는 전력 케이블은 손상이나 도청으로부터 보호하여야 한다. •정보처리시설은 가용성과 무결성을 지속적으로 보장할 수 있도록 유지보수하여야 한다. •장비의 미승인 반출입을 통한 이용자의 국가핵심기술 관련

구 분	이행주체	보안관리
		정보 자산 유출, 악성코드 감염 등의 침해사고 예방을 위하여, ▲보호구역 내 임직원 및 외부 업무 관련자에 의한 장비 반출입 절차를 수립하고, ▲기록 및 관리하여야 한다. • 정보처리시설 내의 저장 매체를 포함하여 ▲모든 장비를 파악하고, ▲이용자의 국가핵심기술 관련 정보가 저장된 장비를 폐기하는 경우, 복구 불가능하도록 하여야 한다. ▲재사용하는 경우에도 복구 불가능 상태에서 재사용하여야 한다.

기술적 보안

구 분	이행주체	보안관리
①자료·데이터	공 통	•▲제공자는 국가핵심기술 관련 정보에 대한 접근제어, 위·변조 방지 등 정보 처리에 대한 보호 기능을 이용자에게 제공하여야 하며, ▲이용자는 이를 확인하여야 한다. •제공자와 협의하여 클라우드 컴퓨팅 서비스에 저장 또는 전송 중인 국가핵심기술 관련 정보를 보호하기 위해 암호화 대상, 암호 강도(복잡도), 키관리, 암호 사용에 대한 정책을 마련·이행하여야 한다. •제공자와 협의하여 암호키 생성, 이용, 보관, 배포, 파기에 대한 내용을 담은 암호키 관리 절차를 수립하여야 하며, 이용자의 암호키는 이용자에 의해 통제가 가능한 별도의 물리적으로 분리된 서버에 보관·백업하고, 최소한의 접근권한을 부여하여야 한다.
	이용자	•▲국가핵심기술 관련 정보 유형, 법적 요구사항, 민감도 및 중요도에 따라 정보를 분류·관리하여야 한다. •제공자와 계약 단계에서 국가핵심기술 관련 정보의 소유권을 명확히 명시하여야 한다. •국가핵심기술 관련 정보에 대한 ▲암호화 수준에 대한 보안 요구사항을 도출하여 계약 시 반영하여야 하며, ▲생성된 국가핵심기술 관련 정보에 대한 보관처리·수신하기 위한 기술적 방안 등을 제공자에게 제공받아야 한다.
	제공자	•이용자의 국가핵심기술 관련 정보의 입·출력, 전송 또는 교환 및 저장에 대한 제공자의 정보 무결성 확인 방안이 마련되어야 한다. •▲이용자에게 국가핵심기술 관련 정보를 추적하기 위한 방안을 제공하고, ▲이용자가 요구하는 경우, 구체적인 제공 정보(이용자의 정보가 저장되는 위치정보 등)를 공개하여야 한다.
②인증 및 권한	공 통	•▲이용자는 클라우드 컴퓨팅 서비스와 분리된 별도의 개별 인증과 접근통제 방법을 적용하고, 정기적인 접속기록 및 최소권한 관리 검토 등 안전하게 관리하여야 하며, ▲제공자는 필요한 제반 환경을 제공하여야 한다.

구 분	이행주체	보안관리
		•▲이용자는 클라우드 컴퓨팅 서비스에 대해 인증서(PKI) 기반, OTP, 지문 등 다중요소 인증을 통한 강화된 인증수단을 사용하여야 하며, ▲제공자는 이를 제공하기 위한 방안을 마련하여야 한다. •비인가자의 접근을 통제할 수 있도록 접근통제 영역 및 범위, 접근통제 규칙, 방법 등을 포함하여 접근통제 정책을 수립하여야 한다. •▲접근기록 대상을 정의하고, ▲서비스 통제, 관리, 사고 발생 책임 추적성 등을 보장할 수 있는 형태로 기록되고, ▲유지(1년 이상)하여야 한다. •▲법적 요구사항, 외부 위협요인 등을 고려하여 패스워드 복잡도 기준, 초기 패스워드 변경, 변경 주기 등 사용자 및 관리자 패스워드 관리 절차를 수립·이행하고 패스워드 관리 책임이 사용자 및 관리자에게 있음을 주지시켜야 한다. ▲특히 관리자 패스워드는 별도 보호대책을 수립하여 관리하고, 이용자 패스워드 관리절차는 공지하여야 한다.
	이용자	•클라우드 컴퓨팅 서비스에서 ▲사용자를 유일하게 구분할 수 있는 식별자를 할당하고, 추측 가능한 식별자 사용을 제한하여야 한다. ▲동일한 식별자를 공유하여 사용하는 경우, 그 사유와 타당성을 검토하여 보안책임자의 승인을 받아야 한다. •클라우드 컴퓨팅 서비스에 대한 접근을 사용자 인증, 접근 주체별 권한 부여, 로그인 횟수 제한, 불법 로그인 시도 경고 등 안전한 사용자 인증 절차에 의해 통제하여야 한다. •클라우드 컴퓨팅 서비스 및 국가핵심기술 관련 정보에 대한 접근을 통제하기 위하여 ▲공식적인 사용자 등록 및 해지 절차를 수립하고, ▲업무 필요성에 따라 사용자 접근권한을 최소한으로 부여하여야 한다. ▲접근권한에 대해 정기적으로 점검하여야 한다. •클라우드 컴퓨팅 서비스 및 국가핵심기술 관련 정보 관리 등 ▲특수 목적을 위해 부여한 계정 및 권한을 식별하고, ▲목록 관리 및 별도 통제하여야 한다. ▲접근권한에 대해 정기적으로 점검하여야 한다. •클라우드 컴퓨팅 서비스 및 국가핵심기술 관련 정보에 대한

구 분	이행주체	보안관리
		접근을 관리하기 위하여 접근권한 부여, 이용, 변경·해지(직무·부서 변경, 장기간 미사용, 휴직 및 퇴직 등)의 적정성 여부를 정기적으로 점검·반영하여야 한다.
	제공자	•클라우드 시스템 및 중요 정보에 대한 접근을 통제하기 위하여 ▲공식적인 사용자 등록 및 해지 절차를 수립하고, ▲업무 필요성에 따라 사용자 접근권한을 최소한으로 부여하여야 한다. ▲접근권한에 대해 정기적으로 점검하여야 한다. •클라우드 시스템 및 중요 정보 관리 등 ▲특수 목적을 위해 부여한 계정 및 권한을 식별하고, ▲목록관리 및 별도 통제하여야 한다. ▲접근권한에 대해 정기적으로 점검하여야 한다. •클라우드 시스템 및 중요 정보에 대한 접근을 관리하기 위하여 접근권한 부여, 이용, 변경·해지(직무·부서 변경, 장기간 미사용, 휴직 및 퇴직 등)의 적정성 여부를 정기적으로 점검·반영하여야 한다. •클라우드 시스템에서 ▲사용자를 유일하게 구분할 수 있는 식별자를 할당하고, 추측 가능한 식별자 사용을 제한하여야 한다. ▲동일한 식별자를 공유하여 사용하는 경우, 그 사유와 타당성을 검토하여 책임자의 승인을 받아야 한다. •클라우드 시스템에 대한 접근을 사용자 인증, 접근 주체별 권한 부여, 로그인 횟수 제한, 불법 로그인 시도 경고 등 안전한 사용자 인증 절차에 의해 통제하여야 한다.
③네트워크	공 통	•클라우드 컴퓨팅 서비스와 관련된 내·외부 네트워크에 대해 보안 정책과 절차를 수립하여야 한다. •제공자의 관리 영역과 이용자의 서비스 영역, 이용자 간 서비스 영역의 네트워크 접근은 물리적 또는 논리적으로 분리하여야 한다. •▲이용자는 국가핵심기술 관련 정보 보호를 위해 보안관제 체계를 구축하고, 실시간 모니터링을 수행하여야 한다. ▲제공자는 이용자의 보안관제 수행에 필요한 제반사항(로그기록 등)을 지원하여야 한다.
	이용자	•클라우드 컴퓨팅 서비스와 관련된 내·외부 네트워크를 보호하기

구 분	이행주체	보안관리
		위하여 정보보안시스템(VPN, 전용선 등)을 운영하여야 한다. •클라우드 컴퓨팅 서비스에서 국가핵심기술 관련 정보가 이동하는 구간에 대해서는 암호화된 통신채널을 사용하여야 한다. •클라우드 컴퓨팅 서비스의 무선접속을 사용하는 경우, 그 사유와 타당성을 검토하고 보안책임자의 승인을 받아야 한다.
	제공자	•외부공격(DDoS, 해킹, 비인가 접속 등)으로 인한 서비스 중단 및 국가핵심기술 관련 정보 유출 등을 막기 위해 ▲네트워크를 모니터링하고 통제하여야 한다. 또한 ▲이상징후 발견 시, 이용자에게 즉시 통지하고, 조치하여야 한다. •클라우드 컴퓨팅 서비스와 관련된 내·외부 네트워크를 보호하기 위하여 정보보안시스템(방화벽, IPS, IDS, VPN 등)을 운영하여야 한다. •클라우드 시스템에서 중요 정보가 이동하는 구간에 대해서는 암호화된 통신채널을 사용하여야 한다. •클라우드 시스템은 ▲무선망과 분리하고, 무선접속에 대한 접근을 통제하여야 한다. ▲무선접속을 사용하는 경우, 그 사유와 타당성을 검토하고 책임자의 승인을 받아야 한다.
④공급망	제공자	•클라우드 컴퓨팅 서비스에 대한 접근과 서비스 연속성을 저해하는 위험을 식별하고 최소화하기 위해 공급망과 관련한 보안 요구사항을 정의하는 관리 정책을 수립하여야 한다. •클라우드 컴퓨팅 서비스 ▲범위 및 보안 요구사항을 포함하는 공급망 계약을 체결하고, ▲다자간 협약 시 책임을 개별 계약서에 각각 명시해야 하며, 해당 서비스에 관련된 ▲모든 이해관계자에게 적용하여야 한다. •보안 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. •클라우드 컴퓨팅 서비스 공급망 상에서 발생하는 기록 및 보고서는 정기적으로 모니터링 및 검토하여야 한다.
⑤가상화	제공자	•▲가상자원(가상 머신, 가상 스토리지, 가상 소프트웨어 등)의 생성, 변경, 회수 등에 대한 관리 방안을 수립하고, ▲사용

구 분	이행주체	보안관리
		목록을 유지하여야 한다. • 이용자와의 계약 종료 시, 가상자원 회수 절차에 따라 가상자원 내 존재하는 ▲이용자의 국가핵심기술 관련 백업을 포함한 모든 정보는 복구할 수 없는 상태로 삭제하여야 하며, ▲삭제 이력을 이용자에게 제공하여야 한다. • ▲가상자원에 대한 무결성 보장하기 위한 보안조치 및 가상자원의 변경(수정, 이동, 삭제, 복사)에 대해 모니터링 하여야 한다. ▲또한, 가상자원에 손상이 발생한 경우, 이를 이용자에게 즉시 알려야 한다. • ▲가상자원을 관리하는 하이퍼바이저의 기능 및 인터페이스에 대한 접근 통제 방안을 마련·이행하여야 한다. ▲또한 하이퍼바이저에 대한 소프트웨어 업데이트 및 보안패치를 최신으로 유지하여야 한다. • 가상자원을 제공하기 위한 웹사이트와 가상 소프트웨어(앱, 응용프로그램)를 배포하기 위한 공개서버에 대한 물리적, 기술적 보안관리 대책을 수립하여야 한다. • 표준화된 가상화 포맷, 이식성이 높은 가상화 플랫폼, 공개 API 등을 이용하여 클라우드 컴퓨팅 서비스 간의 상호 운용성 및 이식성을 높여야 한다. • 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, 이용자에게 즉시 통지하고, 사용 중지 및 격리 조치를 수행하여야 한다. • 가상 환경(가상PC, 가상 서버, 가상 소프트웨어 등) 접근을 위한 ▲인터페이스 및 API에 대한 보안 취약점을 정기적으로 분석하고, ▲이에 대한 보호방안을 마련·이행하여야 한다. • 이용자가 기존 정보시스템 환경에서 클라우드 컴퓨팅 서비스의 가상 환경으로 전환 시, 안전하게 정보를 이전하도록 기술적인

구 분	이행주체	보안관리
		조치방안을 제공하여야 한다. •출처, 유통경로 및 제작자가 명확한 소프트웨어로 구성된 가상환경을 제공하여야 한다.
⑥시스템 개발 및 도입 보안	제공자	•신규 시스템 개발 및 기존 시스템 변경 시, ▲보안 관련 법적 요구사항, 최신 보안취약점, 보안의 기본요소(기밀성, 무결성, 가용성) 등을 고려하여 보안요구사항을 명확히 정의하고, ▲이를 적용하여야 한다. •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. •클라우드 시스템 설계 시, 사용자의 인증, 권한 변경, 중요정보 이용 및 유출 등에 대한 감사증적을 확보할 수 있도록 하여야 한다. •클라우드 시스템 설계 시, 업무의 목적 및 중요도에 따라 접근 권한을 부여할 수 있도록 하여야 한다. •▲로그기록의 정확성을 보장하고 법적인 자료로서 효력을 지니기 위해 클라우드 시스템 시각을 공식 표준시각으로 정확하게 동기화 하여야 한다. ▲또한 서비스 이용자에게 시각 정보 동기화 기능을 제공하여야 한다. •▲안전한 코딩방법에 따라 클라우드 시스템을 구현하고, ▲분석 및 설계 과정에서 도출한 보안요구사항이 정보시스템에 적용되었는지 확인하기 위하여 시험을 수행하여야 한다. •▲개발 및 시험 시스템은 운영시스템에 대한 비인가 접근 및 변경의 위험을 감소하기 위해 원칙적으로 분리하여야 한다. ▲분리하여 운영하기 어려운 경우, 그 사유와 타당성을 검토하고, 안전성 확보 방안을 마련하여야 한다. •시스템 시험 과정에서 운영데이터 유출을 예방하기 위해 시험 데이터 생성, 이용 및 관리, 파기, 기술적 보호조치에 관한

구 분	이행주체	보안관리
		절차를 수립하여 이행하여야 한다. • ▲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. • 클라우드 시스템 개발을 외주 위탁하는 경우, ▲분석 및 설계 단계에서 구현 및 이관까지의 준수해야 할 보안요구사항을 계약서에 명시하고, ▲이행여부를 관리·감독하여야 한다. • 클라우드 시스템의 ▲처리 속도와 용량에 대하여 정기적인 모니터링을 수행하고, ▲안정성의 확보에 필요한 시스템 도입 계획을 수립하여야 한다. • 새로 도입되는 시스템에 대한 ▲인수 기준이 수립되어야 하며, ▲인수 전에 테스트가 수행되어야 한다.

보안사고 대응

구 분	이행주체	보안관리
①사 고	공 통	•클라우드 컴퓨팅 서비스 및 클라우드 시스템 ▲침해사고에 대한 효율적이고, 효과적인 대응을 위해 신고 절차*, 유출 금지 대상, 사고 처리 절차 등을 담은 침해사고 대응절차를 마련하여야 한다. ▲침해사고 대응절차는 이용자와 제공자의 책임과 절차가 포함되어야 한다. * 「산업기술보호법」 제15조에 따라, 동법 제14조 각 호의 어느 하나에 해당하는 행위가 발생할 우려가 있거나, 발생한 때에는 즉시 산업통상자원부 및 국가정보원에 신고 절차 포함
	공 통	•침해사고 정보를 수집·분석·대응할 수 있는 ▲보안관제 체계 및 조직을 구성·운영하고, ▲침해사고 유형 및 중요도에 따라 보고 및 협력체계를 구축하여야 한다.
	공 통	•▲침해사고 대응과 관련된 역할 및 책임이 있는 담당자를 훈련시켜야 하고, ▲정기적으로 침해사고 대응 능력을 점검하여야 한다.
	공 통	•▲이용자는 클라우드 컴퓨팅 서비스 이용 계약 시, 제공자의 사고조사에 대한 적극적인 협조 및 지원의무를 명시하여야 하며, ▲제공자는 산업통상자원부, 국가정보원 및 이용자의 조사 요청에 협조하여야 한다.
	공 통	•클라우드 컴퓨팅 서비스 및 클라우드 시스템 침해사고 관련 정보를 활용하여 유사한 침해사고가 반복되지 않도록 ▲침해사고 재발방지 대책을 수립하고, ▲필요한 경우, 침해사고 대응 체계도 변경하여야 한다.
	이용자	•클라우드 컴퓨팅 서비스와 관련하여 ▲침해사고 발생 시, 제공자로부터 발생내용, 원인, 조치현황 등을 신속하게 파악하고, ▲사고대응 절차를 수행하여야 한다.
	제공자	•▲침해사고 발생 시, 침해사고 대응절차에 따라 법적 통지 및 신고 의무를 준수하여야 한다. ▲또한 이용자에게 발생 내용, 원인, 조치 현황 등을 신속하게 알려야 하며, ▲대응절차에 따라 처리와 복구를 신속하게 수행하여야 한다.

구 분	이행주체	보안관리
②장 애	공 통	•▲제공자는 관련 법률에서 규정한 클라우드 컴퓨팅 서비스의 중단으로부터 업무 연속성을 보장하기 위해 백업, 복구 등을 포함하는 장애 대응절차를 마련하여야 하며, ▲이용자는 장애 대응 요구사항, 담당자 정의 및 연락처 등을 포함한 장애 대응절차를 마련하여야 한다. •▲이용자는 업무영향도 평가 등을 통해 제공자와 협의·산정한 복구시간을 계약 내 반영하여야 하며, ▲제공자는 계약에 명시된 시간 내에 대응절차에 따라 해당 서비스의 장애를 처리하고 복구시켜야 한다. •이용자와 제공자가 협의하여 장애 관련 정보를 활용, ▲유사한 서비스 중단이 반복되지 않도록 장애 재발방지 대책을 수립하고, ▲필요한 경우, 장애 대응 절차도 수정·보완하여야 한다.
	제공자	•클라우드 컴퓨팅 서비스 ▲중단이나 피해가 발생 시, 장애 대응절차에 따라 법적 통지 및 신고 의무를 준수하여야 한다. ▲이용자에게도 발생 내용, 원인, 조치 현황 등을 신속하게 알려야 한다.
③가용성	제공자	•클라우드 컴퓨팅 서비스의 가용성을 보장하기 위해 ▲성능 및 용량에 대한 요구사항을 정의하고, ▲지속적으로 관리할 수 있는 모니터링 방법 또는 절차를 수립하여야 한다. •정보처리설비(클라우드 컴퓨팅 서비스를 제공하는 물리적인 서버, 스토리지, 네트워크 장비, 통신 케이블, 접속 회선 등)의 장애로 서비스가 중단되지 않도록 ▲정보처리설비를 이중화하고, ▲장애 발생 시, 신속하게 복구를 수행하도록 백업 체계도 마련·이행하여야 한다. •서비스 가용성에 대한 영향 평가를 정기적으로 점검하여야 한다.

클라우드 컴퓨팅 서비스에 저장된 국가핵심기술 관련 정보에 대한 외국기업 등의 접근권한 부여·열람·사용 등을 허용하는 경우

1. 기본원칙
2. 보안관리

3장

3장 클라우드 컴퓨팅 서비스에 저장된 국가핵심기술 관련 정보에 대한 외국기업 등의 접근권한 부여·열람·사용 등을 허용하는 경우

기본원칙

이용자

클라우드 컴퓨팅 서비스에 저장된 국가핵심기술 관련 정보에 대한 외국기업 등의 접근권한 부여·열람·사용 등의 허용(이하 '접근권한 허용'라 함)하는 경우, 「산업기술보호법」, 동법 시행령, 「산업기술보호지침」 등에 근거, 국가연구개발비 지원 여부에 따라 국가핵심기술 수출승인 신청 또는 수출신고를 하여야 한다.

공 통

이용자와 제공자는 '제2장 – 클라우드 컴퓨팅 서비스 환경 內 국가핵심기술 관련 정보를 저장·처리하는 경우'에 명시된 ▲관리적·물리적·기술적 보안관리 및 보안사고 대응절차 마련·이행을 하여야 하며, ▲아래와 같은 추가적인 보안관리를 하여야 한다.

이용자가 외국기업 등의 접근권한 허용하는 경우, 이용자와 제공자는 국가핵심기술 관련 정보 보호를 위해 보안 협업 대책을 지속적으로 마련하여야 한다.

▲이용자는 외국기업 등의 접근권한을 허용한 국가핵심기술 관련 정보에 대해 완전 삭제 방안을 마련하고, 허용기간 종료 이후 즉시 삭제·폐기하여야 하며, 삭제·폐기 이력을 유지(1년 이상)하여야 한다. ▲제공자는 이에 적극 협조하여야 한다.

보안관리

구 분	이행주체	보안관리
인 력	이용자	•외국기업 등의 접근권한 허용 대상 전원에 대해 보안서약서 징구 및 보안교육을 정기적으로 시행하여야 한다.
자료·데이터	이용자	•▲외국기업 등의 접근권한 허용 대상이 접속한 단말기에 국가핵심기술 관련 정보를 직접 저장할 수 없도록 제한하여야 한다. ▲국가핵심기술 관련 정보를 접속한 단말기에 직접 저장하여야 할 경우에는, 클라우드 컴퓨팅 서비스와 분리된 이용자에 의해 통제가 가능한 별도의 안전한 장소에서 저장·관리하고 있는 고유한 키를 활용하여 암호화한 형태로 저장하여야 한다.
인증 및 권한	공 통	•▲이용자는 외국기업 등의 접근권한 허용 대상 다중요소 인증을 통한 강화된 인증수단을 사용하여야 한다. ▲제공자는 이에 필요한 제반환경을 제공해야 한다.
	이용자	•외국기업 등의 접근권한 허용 대상에 ▲최소한의 권한을 부여하고, ▲필요한 국가핵심기술 관련 정보만 식별하여 ▲최소한으로 제공하여야 한다.
네트워크	이용자	•▲격리된 환경을 통한 간접 접속 방식을 적용하여 외국기업 등의 접근권한 허용 대상이 ▲사전 식별·지정된 단말기를 통해서만 이용할 수 있도록 해야 한다. •외국기업 등의 접근권한 허용기간 동안 ▲계정, 접근, 로그(부여·열람·사용 등) 등의 이상행위에 대한 실시간 모니터링을 수행하여야 하며, ▲이상징후 발견 시, 조치하여야 한다.
로 그	이용자	•외국기업 등의 접근권한 허용기간 동안 로그 및 이용 기록 등을 유지(1년 이상)·관리하여야 하며, 정기적으로 확인하여야 한다.
사 고	공 통	•외국기업 등의 접근권한 허용 시, ▲침해사고에 대한 효율적이고, 효과적인 대응을 위해 신고 절차*, 유출 금지 대상, 사고처리 절차 등을 담은 침해사고 대응절차를 마련하여야 한다. ▲침해사고 대응절차는 이용자와 제공자, 외국기업 등의 접근권한 허용 대상의 책임과 절차가 포함되어야 한다.

구 분	이행주체	보안관리
		* 「산업기술보호법」 제15조에 따라, 동법 제14조 각 호의 어느 하나에 해당하는 행위가 발생할 우려가 있거나, 발생한 때에는 즉시 산업통상자원부 및 국가정보원에 신고 절차 포함
		• 외국기업 등의 접근권한 허용과 관련하여 ▲침해사고 발생 시, 발생내용, 원인, 조치현황 등을 신속하게 파악하고, ▲사고대응 절차를 수행하여야 한다.
		• 외국기업 등의 접근권한 허용 시, 침해사고 관련 정보를 활용하여 유사한 침해사고가 반복되지 않도록 ▲침해사고 재발방지 대책을 수립하고, ▲필요한 경우, 침해사고 대응 체계도 변경하여야 한다.
	이용자	• ▲외국기업 등의 접근권한 허용과 관련 계약 시, 외국기업 등의 접근권한 허용 대상의 사고조사에 대한 적극적인 협조 및 지원의무를 명시하여야 하며, ▲외국기업 등의 접근권한 허용 대상이 산업통상자원부, 국가정보원 및 이용자의 조사 요청에 협조하도록 한다.

별 첨

1. 국내·외 클라우드 컴퓨팅 서비스 관련 법·제도 현황
2. 클라우드 컴퓨팅 서비스 환경에서의
   국가핵심기술 보호 실태조사 체크리스트

별첨1 국내·외 클라우드 컴퓨팅 서비스 관련 법·제도 현황

〈 해외 클라우드 서비스 사업자 주요 규정[1] 〉

국 가	규 정	주 요 내 용
 (미국)	FedRAMP 인증	▸ 美 연방 정부기관이 민간 클라우드 이용시 FedRAMP 인증은 필수 ▸ 국방부 외 모든 연방 정부 기관이 사용하는 클라우드 서비스 및 제품에 대해, 데이터의 민감도 및 중요도를 기준으로 High, Moderate, Low 3단계 등급으로 나누고, 해당 등급별 보안요구 항목을 차등하여 인증제도를 운영 ※ NIST에서 발행한 SP 800-53을 근간으로 하여 영향 수준에 따른 통제 항목 제시
 (EU)	EUCS 인증 체계	▸ EU 사이버보안법(EU Cybersecurity Act)에 근거하여 클라우드 서비스의 신뢰와 보안을 강화하기 위한 EU전역의 사이버보안 인증 체계 ▸ CSP가 EU의 사이버 보안 요구 사항을 준수하는지 평가하고 인증하는 프레임워크를 제공하며 EU데이터 주권과 데이터 현지화 요구사항에 중점 ※ 여러 보안 수준(Basic, Substantial, High)으로 위험수준에 따른 인증을 제공
 (프랑스)	SecNum Cloud 인증	▸ CSP의 신뢰성 확보를 위한 목적의 클라우드 보안인증 제도로 CSP가 주요 정부기관 등의 '매우 민감한 데이터'를 다루기 위해서는 인증 취득 필요
 (일본)	ISMAP 인증	▸ 정부에 조달하고자 하는 클라우드 서비스는 보안 요구 사항 충족 여부를 평가 ※ JIS Q 27001, 27002, 27017과 NIST SP 800-53을 인증 기준으로 채택
 (싱가포르)	MTCS 인증	▸ 민간 클라우드 서비스 안전성 확보를 위해 MTCS 인증을 도입하고, 공공 클라우드 입찰 시 필수적으로 요건 운영 ▸ 클라우드 보안 국가표준(MTCS SS584)에 따라 데이터 민감도·중요성 기반 3단계(Tier 1~3)로 분류·인증
 (캐나다)	ISO 27001 인증	▸ 통신보안국(CSE) 산하 사이버안전센터(CCCS)의 국제표준 인증(ISO 27001)을 받은 제품만 이용 가능하며, 필요시 추가 보안조치 요구 ▸ 민감정보를 일반(A급), 심각(B급), 매우심각(C급)으로 분류하고, 민감정보 C급부터 기밀정보를 민간 클라우드 제한
 (호주)	국가 공인 인증제도	▸ 디지털전환국(DTA)의 '국가 공인 인증제도'를 받은 제품만 사용 가능 ▸ 인증등급은 상위(Strategic), 하위(Assured) 레벨로 구분

1) 클라우드 컴퓨팅 서비스 보안인증에 관한 고시 규제영향분석서('24.2), 국내외 클라우드 서비스 보안 인증제 동향 및 국내 CSAP 인증 개선방안('21.12), 해외사업자만 득보는 공공클라우드 규제완화('22), ANSSI 등 자료 취합 등 업데이트

〈 국내 클라우드 컴퓨팅 서비스 사업자 주요 규정[2] 〉

대 상	규 정	주 요 내 용
CSP (클라우드 컴퓨팅 서비스 사업자)	클라우드 컴퓨팅법	▸ 클라우드 컴퓨팅의 발전 및 이용을 촉진하고 클라우드 컴퓨팅 서비스를 안전하게 이용할 수 있는 기반 조성을 위한 법률 ※ 클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률
	CSAP 인증	▸ 클라우드서비스 제공자가 제공하는 서비스에 대해 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」에 따라 정보보호 수준의 향상 및 보장을 위하여 보안인증기준에 적합한 클라우드 컴퓨팅 서비스에 대한 보안인증 수행 제도 ※ 국가·공공기관을 대상 필수 인증

〈 국내 클라우드 컴퓨팅 서비스 이용자별 주요 규제 및 가이드라인 〉

분 야	규 정	주 요 내 용
행정 및 공공기관	행정·공공기관 클라우드 컴퓨팅 서비스 이용안내서 (행안부)	▸ 행정기관 및 공공기관이 안전하고 효율적으로 클라우드 컴퓨팅 서비스를 도입·이용하기 위한 절차와 방법 안내 목적 ※ 행정기관 등의 장이 정보통신자원(정보통신기기, 정보통신설비, 소프트웨어 등)을 클라우드 컴퓨팅 서비스로 전환하거나 신규 도입할 때 활용할 수 있는 안내서
	국가 클라우드 컴퓨팅 보안 가이드라인 (국정원)	▸ 국가·공공기관의 클라우드 컴퓨팅 도입 시 보안수준을 향상 시킬 수 있는 보안성 확인 기준으로 ▲클라우드 컴퓨팅 개념, ▲보안 위협, ▲유형별 절차, ▲보안 기준 제시 ※ 클라우드 컴퓨팅 사업계획은 국가정보원에 보안성검토를 의뢰하여 안전성 확인 절차를 거쳐야하며, 결과에 따라 클라우드 컴퓨팅 사업 수행
금 융	전자금융감독 규정 (금융위원회)	▸ 금융회사가 전자금융거래의 안전성과 신뢰성을 확보하고, 금융소비자를 보호하기 위해 준수해야할 규정 ※ 클라우드 컴퓨팅 서비스 이용 시 연속성 계획 및 안전성 확보조치 등 수립·시행
	금융분야 클라우드 컴퓨팅 서비스 이용가이드 (금융보안원)	▸ 금융회사가 클라우드 컴퓨팅 서비스를 이용하고자 할 경우, 요구되는 세부절차와 금융시스템 안정성 및 금융소비자 보호를 위해 필요한 사항의 안내 목적 ※ 클라우드 서비스를 이용함에 있어 보안 대책을 수립·운영하기 위해 가이드 활용을 권고
방위산업	방위산업기술 보호지침 (방사청)	▸ 방위산업 관련 업체의 방위산업기술보호에 필요한 방법과 절차를 제공하고, 실태조사 등에 필요한 사항에 대한 지침 ※ 방위산업 기술보호를 위해 정보통신망 분리 및 제한된 클라우드 서비스 사용
국가 핵심기술	산업기술보호 지침 (산업부)	▸ 국가핵심기술 등 산업기술의 유출을 방지하고 보호하기 위해 활용할 수 있는 방법/절차 등을 규정한 지침 ※ 국가핵심기술 보유기관 대상 클라우드 서비스 이용 시, 경우에 따라 수출승인 또는 신고 필요

2) 한국인터넷진흥원, 법령정보센터 등

별첨2 클라우드 컴퓨팅 서비스 환경에서의 국가핵심기술 보호 실태조사 체크리스트

1 클라우드 컴퓨팅 서비스 내 국가핵심기술 관련 정보 저장·처리 - 이용자(42개)

점검 항목	비 고
1. 클라우드 컴퓨팅 서비스에 대한 보안관리 규정 또는 정책을 보유하고 있습니까? ① 보유하고 있다. (☞ **2번**으로) ② 보유하고 있지 않다. (☞ **6번**으로)	
2. 클라우드 보안관리 규정 또는 정책 내 관리적, 물리적, 기술적 보안관리, 보안사고 대응 등의 내용을 모두 포함하고 있습니까? ① 모든 영역을 포함하고 있다. ② 일부 영역만 포함하고 있다. ③ 어느 영역도 포함하지 않는다.	
3. 클라우드 보안관리 규정 또는 정책의 적합성, 적절성, 유효성 등에 대해 정기적으로 검토를 하고 있습니까? ① 정기적으로 검토하고 있다. ② 필요 시, 검토하고 있다. ③ 제정 이후 검토한 적이 없다.	
4. 클라우드 보안관리 규정 또는 정책의 제·개정 시 경영진에게 승인을 받고 있습니까? ① 경영진에게 항상 서면으로 승인받고 있다. ② 경영진에게 일부 중요한 내용만 구두로 보고하고 있다. ③ 경영진에게 보고하지 않는다.	
5. 클라우드 보안관리 규정 또는 정책의 제·개정 시, 규정·정책에 영향을 받는 모든 임직원 및 외부 업무 관련자에게 그 내용을 알 수 있도록 공지하고 있습니까? ① 공지하고 있다. ② 주요 직무자에게만 공지하고 있다. ③ 공지하지 않는다.	
6. CSP*(이하 "제공자")와 체결한 계약서 내 보안(관련 법률 및 지침, 가이드, 보안체계, 이용자 보안 사항 등)관련 요구사항이 반영되어 있습니까? <CSP(Cloud Service Provider> ▸ 클라우드 서비스를 제공하는 기업으로, IT인프라 및 플랫폼을 구축·운영하며 서비스를 제공하는 사업자 ① 계약서 등에 보안 관련 요구사항이 명확히 반영되어 있다. (☞ **7번**으로) ② 계약서 등에 보안 관련 요구사항이 일부만 반영되어 있다. (☞ **7번**으로) ③ 보안 관련 요구조항이 반영되어 있지 않다. (☞ **8번**으로)	
7. 계약서 내 국가핵심기술과 관련한 보호조치 위반, 보안사고 발생에 대한 책임 사항 등이 명시되어 있습니까? ① 모든 책임사항 등이 명시되어 있다. ② 일부 책임사항 등에 대해서만 명시되어 있다. ③ 반영되어 있지 않다.	

점검 항목	비 고
8. 제공자와 계약 단계에서 국가핵심기술 관련 정보의 소유권을 명시하여 반영하고 있습니까? ① 명시하여 반영되어 있다. ② 일부만 반영되어 있다. ③ 반영되어 있지 않다.	
9. 제공자와 국가핵심기술 관련 정보 보호를 위해 보안 협업 대책을 마련하고 있습니까? ① 정기적으로 협의 및 보안 협업 대책을 마련하고 있다. ② 필요 시, 협의 및 보안 협업 대책을 마련하고 있다. ③ 마련하고 있지 않다.	
10. 클라우드 컴퓨팅 서비스 정보자산과 보안에 관련된 모든 인원(임직원 및 외부 관련자 등)에 대하여 보안 역할과 책임을 정의하고 있습니까? ① 모든 인원에 대하여 보안 역할과 책임을 명확하게 정의하고 있다. ② 일부 인원에 대해서만 보안 역할과 책임을 정의하고 있다. ③ 보안 역할과 책임을 정의하고 있지 않다.	
11. 클라우드 컴퓨팅 서비스를 운영 및 관리하는 전담인력이 지정되어 있습니까? ① 전담인력이 지정되어 있다. ② 전담인력은 아니나, 겸직인력이 지정되어 있다. ③ 전담인력 또는 겸직인력이 지정되어 있지 않다.	
12. 제공자가 자체 또는 외부 전문기관으로부터 수행한 클라우드 컴퓨팅 서비스 운용 관리 전반에 대한 보안 취약점 개선 결과를 확인하고 있습니까? ① 정기적으로 확인하고 있다. ② 필요 시, 확인하고 있다. ③ 확인하고 있지 않거나, 제공받고 있지 않다.	
13. 클라우드 컴퓨팅 서비스 환경으로 이전(저장·처리) 될 국가핵심기술 관련 정보 자산에 대한 관리정책을 마련하고 있습니까? ① 관리정책을 마련하고 있다. ② 별도 관리정책이 없다.	
14. 클라우드 컴퓨팅 서비스 환경으로 이전(저장·처리) 될 국가핵심기술 관련 정보자산에 대해 목록관리를 실시하고 있습니까? ① 모든 정보자산에 대해 목록관리를 실시하고 있다. (☞ **15번**으로) ② 일부 정보자산에 대해서만 목록관리를 실시하고 있다. (☞ **15번**으로) ③ 실시하고 있지 않다. (☞ **16번**으로)	
15. 국가핵심기술 관련 정보 유형, 법적 요구사항, 민감도 및 중요도에 따라 정보를 분류·관리하고 있습니까? ① 모든 정보를 분류·관리하고 있다. ② 일부 정보에 대해서만 분류·관리하고 있다. ③ 분류·관리하고 있지 않다.	
16. 클라우드 컴퓨팅 서비스에 접근 가능한 사용자와 관리자를 식별하고 있습니까? ① 식별하고 있다. (☞ **17번**으로) ② 식별하고 있지 않다. (☞ **19번**으로)	

점검 항목	비 고
17. 식별된 사용자와 관리자의 직무별 권한부여, 폐기 등에 관한 관리 절차가 마련되어 있습니까? ① 관리 절차가 마련되어 있다. ② 관리 절차가 마련되어 있으나, 실제 이행은 미흡하다. ③ 별도의 관리 절차가 마련되어 있지 않다.	
18. 사용자와 관리자의 접근권한의 적절성에 대해 정기적으로 점검하고 있습니까? ① 정기적으로 점검하고 있다. ② 필요 시, 점검하고 있다. ③ 점검하고 있지 않다.	
19. 외부 인력(외부 유지보수 직원, 외부 용역자 포함)에 의한 국가핵심기술 관련 정보자산 접근 등과 관련된 보안 요구사항을 계약에 반영하고 있습니까? ① 계약에 반영하고 있다. (☞ **20번**으로) ② 반영하고 있지 않다. (☞ **21번**으로)	
20. 외부 인력에 대해 계약서에 명시한 보안 요구사항 준수 여부를 정기적으로 점검하고 있습니까? ① 정기적으로 점검하고 있다. ② 필요 시, 점검하고 있다. ③ 점검하고 있지 않다.	
21. 클라우드 컴퓨팅 서비스에 접근 가능한 사용자와 관리자 대상 다음과 같은 보안교육을 실시하고 있습니까? **(☞ 해당내용 직접 체크(√))** ☐ 직무별, 담당 분야별 교육 정기적으로 보안교육 실시 ☐ 신규 사용자 및 관리자나 보안사고 발생 등 필요하다고 판단되는 경우, 추가 보안교육 실시 ☐ 보안교육 과정에 산업기술보호 관련 법률, 국가핵심기술 보호조치, 사고에 따른 법적 책임, 침해신고를 포함한 사고 대응 방법, 클라우드 보안사고 사례 등의 내용 반영 등	
22. 클라우드 컴퓨팅 서비스 이용 시, 운용과 관련한 구성요소*는 국내에 위치하고 있습니까? * 클라우드 시스템, 백업시스템 및 데이터와 이를 위한 관리·운영 인력 등 ① 국내에 위치하고 있다. (☞ **23번**으로) ② 해외에 위치하고 있다. (☞ **23번**으로) ③ 제공자로부터 위치 정보를 제공받고 있지 않다. (☞ **24번**으로)	
23. 국가핵심기술 관련 정보가 저장·처리되어 있는 공간의 위치 정보*를 제공받고 있습니까? * 위치 정보란 시/군/구를 포함한 행정구역을 의미 ① 정확한 위치 정보를 제공받고 있다. ② 대략적인 위치 정보만 제공받고 있다.	

점검 항목	비 고
24. 클라우드 컴퓨팅 서비스 내 국가핵심기술 관련 정보 저장·처리 시 이중 암호화*를 적용하고 있습니까? <이중 암호화> ▸ 이용자는 클라우드 컴퓨팅 서비스와 분리된 별도의 안전한 장소에서 저장·관리하고 있는 고유한 키를 활용하여 해당 데이터를 암호화 하며, 제공자의 고유한 키를 활용하여 추가적인 암호화를 진행하여 해당 데이터를 저장하는 것을 말함 ① 이중 암호화를 적용하고 있다. ② 한 가지의 암호키를 활용하여 적용하고 있다. ③ 암호화를 적용하고 있지 않다.	
25. 클라우드 컴퓨팅 서비스에 저장 또는 전송 중인 국가핵심기술 관련 정보를 보호하기 위한 암호화 정책이 마련되어 있습니까? ① 암호화 정책이 마련되어 있다. ② 별도의 암호화 정책이 마련되어 있지 않다.	
26. 암호키 생성, 이용, 보관, 배포, 파기에 대한 내용을 담은 암호키 관리 절차를 수립하고 있습니까? ① 암호키 관리 절차를 수립하고 있다. ② 별도의 암호키 관리 절차를 수립하고 있지 않다.	
27. 암호키에 대해 다음과 같은 보안관리를 하고 있습니까? (☞ **해당내용 직접 체크(√)**) ☐ (생성) 암호화 대상, 암호 강도·복잡도, 암호키 생성 등 ☐ (배포) 최소 권한 원칙에 따른 권한 부여 등 ☐ (보관) 물리적으로 분리된 별도 공간에 보관 및 백업 등 ☐ (관리) 키 회전 주기 설정, 손실 등에 따른 복구 절차, 모니터링 등 ☐ (파기) 사용하지 않는 키 폐기 절차 등	
28. 클라우드 컴퓨팅 서비스 접근을 통제하기 위하여 사용자 인증 절차*를 마련하고 있습니까? <사용자 인증 절차> ▸ 접근 주체별 권한 부여, 로그인 횟수 제한, 불법 로그인 시도에 대한 경고 등 ① 사용자 인증 절차를 마련하여 실시하고 있다. ② 사용자 인증 절차를 마련하고 있으나, 실시는 미흡하다. ③ 별도의 사용자 인증 절차를 마련하고 있지 않다.	
29. 클라우드 컴퓨팅 서비스 인증과 관련하여 다음과 보안관리를 하고 있습니까? (☞ **해당내용 직접 체크(√)**) ☐ 클라우드 컴퓨팅 서비스와 분리된 별도의 개별 인증과 접근통제 방법 적용 ☐ 정기적인 접속기록 및 최소권한 관리 검토 ☐ 필요한 제반 환경 제공자로부터 협조	
30. 클라우드 컴퓨팅 서비스 및 국가핵심기술 관련 정보 관리 등 특수 목적을 위해 부여한 계정 및 권한을 식별하고 있습니까? ① 식별하고 있다. (☞ **31번**으로) ② 식별하고 있지 않다. (☞ **33번**으로)	

점검 항목	비 고
31. 특수 목적을 위해 부여한 계정에 대해 목록관리를 실시하고 있습니까? ① 모든 계정에 대해 목록관리를 실시하고 있다. ② 일부 계정에 대해서만 목록관리를 실시하고 있다. ③ 실시하고 있지 않다.	
32. 특수 목적을 위해 부여한 접근권한의 적절성에 대해 정기적으로 점검하고 있습니까? ① 정기적으로 점검하고 있다. ② 필요 시, 점검하고 있다. ③ 점검하고 있지 않다.	
33. 클라우드 컴퓨팅 서비스와 관련된 내·외부 네트워크에 대해 보안 정책과 절차를 수립하고 있습니까? ① 네트워크에 대해 보안 정책과 절차를 수립하고 있다. ② 네트워크에 대해 보안 정책과 절차를 수립하고 있지 않다.	
34. 네트워크별* 접근은 물리적 또는 논리적으로 분리하여 운영하고 있습니까? * 제공자 관리영역, 이용자 서비스 영역, 이용자 간 서비스 영역 등 ① 전체 네트워크에 대해 물리적 또는 논리적으로 분리하여 운영하고 있다. ② 일부 네트워크에 대해서만 물리적 또는 논리적으로 분리하여 운영하고 있다. ③ 분리하여 운영하고 있지 않다.	
35. 클라우드 컴퓨팅 서비스와 관련된 내·외부 네트워크를 보호하기 위하여 정보보안시스템(VPN, 전용선 등)을 구축·운영하고 있습니까? ① 대다수의 정보보안시스템을 구축·운영하고 있다. ② 일부의 정보보안시스템을 구축·운영하고 있다. ③ 구축·운영하고 있지 않다.	
36. 클라우드 컴퓨팅 서비스에서 국가핵심기술 관련 자료가 이동하는 구간에 대해 암호화된 통신채널을 사용하고 있습니까? ① 항상 암호화된 통신채널을 사용하고 있다. ② 일부 상황에서만 암호화된 통신채널을 사용하고 있다. ③ 암호화된 통신채널을 사용하고 있지 않다.	
37. 국가핵심기술 관련 정보 보호를 위한 보안관제 체계를 구축하고, 모니터링을 실시하고 있습니까? ① 실시간 모니터링을 하고 있다. ② 모니터링을 하고 있으나, 실시간 모니터링은 미흡하다. ③ 모니터링을 하고 있지 않다.	
38. 클라우드 컴퓨팅 서비스 이용 시 침해사고를 예방하기 위한 대응절차를 마련하고 있습니까? ① 침해사고 대응절차를 마련하고 있다. (☞ **39번**으로) ② 침해사고 대응절차를 마련하고 있지 않다. (☞ **41번**으로)	

점검 항목	비 고
39. 침해사고를 예방하기 위한 대응절차에 다음과 같은 내용을 반영하고 있습니까? **(☞ 해당내용 직접 체크(√))** ☐ 보안사고 식별 및 보고 - ① 보안사고 식별 및 보고, ② 관련 법에 따른 법적 신고 , ③ 보안사고 자체 조사 및 응급조치 등 ☐ 증거확보 및 대응 검토 - ① 보안사고 대응 증거 확보, ② 법적 조치 사전 검토, ③ 당사자 간의 합의 검토 등 ☐ 상황 분석 및 대응 조치 - ① 사고대응팀 구성, ② 보안사고 공동 대응 조치 및 복구 등 ☐ 재발 방지 조치 - ① 보안사고 분석 및 대응조치 문서화, ② 법적 대응 및 조치 검토 등	
40. 침해사고 대응절차에 이용자와 제공자의 역할과 책임을 반영하고 있습니까? ① 반영하고 있다. ② 반영하고 있지 않다.	
41. 클라우드 컴퓨팅 서비스 이용 시 장애사고를 예방하기 위한 대응절차를 마련하고 있습니까? * 장애 대응 요구사항, 담당자 정의 및 연락처 등 ① 장애대응 절차를 마련하고 있으며, 절차에 따라 이행하고 있다. ② 장애대응 절차를 마련하고 있으나, 절차에 따른 실제 대응은 미흡하다. ③ 별도 대응 절차가 없다.	
42. 클라우드 컴퓨팅 서비스의 이용 종료 또는 이전 시 사후조치 절차를 다음과 같이 마련하고 있습니까? **(☞ 해당내용 직접 체크(√))** ☐ 제공자에게 관련된 모든 정보 폐기 요청 절차 ☐ 제공자 협조를 통해 완전 삭제·폐기 내역 확인 절차 ☐ 제공자의 비밀유지 의무 및 분쟁 해결 절차 등	

2 클라우드 컴퓨팅 서비스 내 국가핵심기술 관련 정보 저장·처리 - 제공자(45개)

점검 항목	비 고
1. 클라우드 컴퓨팅 서비스에 대한 보안관리 규정 또는 정책을 보유하고 있습니까? ① 보유하고 있다. (☞ **2번**으로) ② 보유하고 있지 않다. (☞ **6번**으로)	
2. 클라우드 보안관리 규정 또는 정책 내 관리적, 물리적, 기술적 보안관리, 보안사고 대응 등의 내용을 모두 포함하고 있습니까? ① 모든 영역을 포함하고 있다. ② 일부 영역만 포함하고 있다. ③ 어느 영역도 포함하지 않는다.	
3. 클라우드 보안관리 규정 또는 정책의 적합성, 적절성, 유효성 등에 대해 정기적으로 검토를 하고 있습니까? ① 정기적으로 검토하고 있다. ② 필요 시, 검토하고 있다. ③ 제정 이후 검토한 적이 없다.	
4. 클라우드 보안관리 규정 또는 정책의 제·개정 시 경영진에게 승인을 받고 있습니까? ① 경영진에게 항상 서면으로 승인받고 있다. ② 경영진에게 일부 중요한 내용만 구두로 보고하고 있다. ③ 경영진에게 보고하지 않는다.	
5. 클라우드 보안관리 규정 또는 정책의 제·개정 시, 규정·정책에 영향을 받는 모든 임직원 및 외부 업무 관련자에게 그 내용을 알 수 있도록 공지하고 있습니까? ① 공지하고 있다. ② 주요 직무자에게만 공지하고 있다. ③ 공지하지 않는다.	
6. 이용자와 국가핵심기술 관련 정보 보호를 위해 보안 협업 대책을 마련하고 있습니까? ① 정기적으로 협의 및 보안 협업 대책을 마련하고 있다. ② 필요 시, 협의 및 보안 협업 대책을 마련하고 있다. ③ 마련하고 있지 않다.	
7. 클라우드 컴퓨팅 서비스 운용관리 전반에 대한 보안 취약점 점검을 실시하고 있습니까? ① 자체 또는 외부 전문기관으로부터 정기적으로 실시하고 있다. (☞ **8번**으로) ② 필요 시, 실시하고 있다. (☞ **8번**으로) ③ 실시하고 있지 않다. (☞ **10번**으로)	
8. 보안 취약점 점검 결과 미흡한 부분을 개선하고 있습니까? ① 개선조치를 시행하고 있다. ② 개선조치를 유도하고 있으나, 실제 개선은 미흡하다. ③ 별다른 개선조치를 시행하고 있지 않다.	
9. 보안 취약점 점검 및 개선결과를 이용자에게 제공하고 있습니까? ① 정기적으로 제공하고 있다. ② 필요 시, 제공하고 있다. ③ 제공하고 있지 않다.	

점검 항목	비 고
10. 클라우드 컴퓨팅 서비스 운용을 위해 부득이한 경우*, 이용자의 국가핵심기술 관련 정보에 접근 시, 다음과 같은 절차를 마련하고 있습니까? * 사고 및 장애대응, 유지 등 □ 이용자 사전 협조 및 승인 □ 접근하는 동안의 모든 로그(log)기록 저장 및 제공 □ 조치 사항에 대한 검토 결과 공유 등	
11. 클라우드 컴퓨팅 서비스 정보자산과 보안에 관련된 모든 인원(임직원 및 외부 관련자 등)에 대하여 보안 역할과 책임을 정의하고 있습니까? ① 모든 인원에 대하여 보안 역할과 책임을 명확하게 정의하고 있다. ② 일부 인원에 대해서만 보안 역할과 책임을 정의하고 있다. ③ 보안 역할과 책임을 정의하고 있지 않다.	
12. 외부 인력(외부 유지보수 직원, 외부 용역자 포함)에 의한 국가핵심기술 관련 정보자산 접근 등과 관련된 보안 요구사항을 계약에 반영하고 있습니까? ① 계약에 반영하고 있다. (☞ **13번**으로) ② 반영하고 있지 않다. (☞ **14번**으로)	
13. 외부 인력에 대해 계약서에 명시한 보안 요구사항 준수 여부를 정기적으로 점검하고 있습니까? ① 정기적으로 점검하고 있다. ② 필요 시, 점검하고 있다. ③ 점검하고 있지 않다.	
14. 클라우드 컴퓨팅 서비스 및 클라우드 시스템에 접근 가능한 사용자와 관리자 대상 다음과 같은 보안교육을 실시하고 있습니까? **(☞ 해당내용 직접 체크(√))** □ 직무별, 담당 분야별 교육 정기적으로 보안교육 실시 □ 신규 사용자 및 관리자나 보안사고 발생 등 필요하다고 판단되는 경우, 추가 보안교육 실시 □ 보안교육 과정에 산업기술보호 관련 법률, 사고에 따른 법적 책임, 침해신고를 포함한 사고 대응 방법, 클라우드 보안사고 사례 등의 내용 반영 등	
15. 클라우드 컴퓨팅 서비스 이용 시, 운용과 관련한 구성요소*는 국내에 위치하고 있습니까? * 클라우드 시스템, 백업시스템 및 데이터와 이를 위한 관리·운영 인력 등 ① 국내에 위치하고 있다. ② 해외에 위치하고 있다.	
16. 국가핵심기술 관련 정보가 저장·처리되어 있는 공간의 위치 정보*를 이용자에게 제공하고 있습니까? * 위치 정보란 시/군/구를 포함한 행정구역을 의미 ① 정확한 위치 정보를 제공하고 있다. ② 대략적인 위치 정보만 제공하고 있다.	

점검 항목	비 고
17. 국가핵심기술 관련 정보 자산이 저장되는 시설을 보호구역으로 설정하고 있습니까? ① 보호구역으로 설정하고 있다. (☞ **18번**으로) ② 일부 중요 시설만 보호구역으로 설정하고 있다. (☞ **18번**으로) ③ 설정하고 있지 않다. (☞ **19번**으로)	
18. 각 보호구역에 대한 보안대책을 다음과 같이 마련하여 운영하고 있습니까? **(☞ 해당내용 직접 체크(√))** ☐ 보호구역 내 출입허가 절차 ☐ 보호구역 내 출입 및 접근 이력의 정기적 점검 ☐ 보호구역 내 유지보수 등의 작업 절차 ☐ 보호구역 내 유지보수 등의 작업 이력의 정기적 점검 등	
19. 이용자의 국가핵심기술 관련 정보에 대한 접근제어, 위·변조 방지 등 정보 처리에 대한 보호 기능을 이용자에게 제공하고 있습니까? ① 정보 처리에 대한 보호 기능을 제공하고 있다. ② 정보 처리에 대한 보호 기능 일부만을 제공하고 있다. ③ 제공하고 있지 않다.	
20. 이용자의 국가핵심기술 관련 정보 처리*에 대한 무결성 확인 방안이 마련되어 있습니까? <국가핵심기술 관련 정보 처리> ▸ 국가핵심기술 관련 정보의 입·출력, 전송 또는 교환 및 저장 등 ① 무결성 확인 방안이 마련되어 있다. ② 일부 무결성 확인 방안이 마련되어 있다. ③ 무결성 확인 방안이 마련되어 있지 않다.	
21. 이용자에게 국가핵심기술 관련 정보에 대한 추적하기 위한 방안을 제공하고 있습니까? ① 추적 방안을 제공하고 있다. ② 제공하고 있지 않다.	
22. 이용자가 요구하는 경우, 국가핵심기술 관련 정보에 대한 구체적인 정보(저장되는 위치정보 등)를 공개하고 있습니까? ① 공개하고 있다. ② 일부 공개하고 있다. ③ 공개하고 있지 않다.	
23. 클라우드 시스템 접근을 통제하기 위하여 사용자 인증 절차*를 마련하고 있습니까? <사용자 인증 절차> ▸ 접근 주체별 권한 부여, 로그인 횟수 제한, 불법 로그인 시도에 대한 경고 등 ① 사용자 인증 절차를 마련하여 실시하고 있다. ② 사용자 인증 절차를 마련하고 있으나, 실시는 미흡하다. ③ 별도의 사용자 인증 절차를 마련하고 있지 않다.	
24. 이용자가 클라우드 컴퓨팅 서비스에 대해 다중 요소 인증 등 강화된 인증 수단을 요청하는 경우, 이를 제공하기 위한 방안을 마련하고 있습니까? ① 마련하고 있다. ② 일부 마련하고 있다. ③ 마련하고 있지 않다.	

점검 항목	비 고
25. 클라우드 시스템의 접근기록을 다음과 같이 관리하고 있습니까? **(☞ 해당내용 직접 체크(√))** ☐ 접근기록 대상 정의 ☐ 서비스 통제, 관리, 사고 발생 책임 추적성 등을 보장할 수 있는 형태로 기록 ☐ 접근기록 유지(1년 이상) 등	
26. 클라우드 시스템 및 중요 정보에 대한 접근을 통제하기 위하여 공식적인 사용자 등록 및 해지 절차를 수립하고 있습니까? ① 절차를 수립하고 있으며, 업무 필요성에 따라 사용자 접근권한을 최소한으로 부여하고 있다. ② 절차를 수립하고 있으나, 절차에 따른 이행은 미흡하다. ③ 절차를 수립하고 있지 않다.	
27. 클라우드 시스템 및 중요 정보 관리 등 특수 목적을 위해 부여한 계정 및 권한을 식별하고 있습니까? ① 식별하고 있다. (☞ **28번**으로) ② 식별하고 있지 않다. (☞ **30번**으로)	
28. 특수 목적을 위해 부여한 계정에 대해 목록관리를 실시하고 있습니까? ① 모든 계정에 대해 목록관리를 실시하고 있다. ② 일부 계정에 대해서만 목록관리를 실시하고 있다. ③ 실시하고 있지 않다.	
29. 특수 목적을 위해 부여한 접근권한의 적절성에 대해 정기적으로 점검하고 있습니까? ① 정기적으로 점검하고 있다. ② 필요 시, 점검하고 있다. ③ 점검하고 있지 않다.	
30. 클라우드 컴퓨팅 서비스와 관련된 내·외부 네트워크에 대해 보안 정책과 절차를 수립하고 있습니까? ① 네트워크에 대해 보안 정책과 절차를 수립하고 있다. ② 네트워크에 대해 보안 정책과 절차를 수립하고 있지 않다.	
31. 네트워크별* 접근은 물리적 또는 논리적으로 분리하여 운영하고 있습니까? * 제공자 관리영역, 이용자 서비스 영역, 이용자 간 서비스 영역 등 ① 전체 네트워크에 대해 물리적 또는 논리적으로 분리하여 운영하고 있다. ② 일부 네트워크에 대해서만 물리적 또는 논리적으로 분리하여 운영하고 있다. ③ 분리하여 운영하고 있지 않다.	
32. 클라우드 컴퓨팅 서비스와 관련된 내·외부 네트워크를 보호하기 위하여 정보보안 시스템(방화벽, IPS, IDS, VPN 등)을 구축·운영하고 있습니까? ① 대다수의 정보보안시스템을 구축·운영하고 있다. ② 일부의 정보보안시스템을 구축·운영하고 있다. ③ 구축·운영하고 있지 않다.	

점검 항목	비 고
33. 클라우드 시스템에서 중요 정보가 이동하는 구간에 대해 암호화된 통신채널을 사용하고 있습니까? ① 항상 암호화된 통신채널을 사용하고 있다. ② 일부 상황에서만 암호화된 통신채널을 사용하고 있다. ③ 암호화된 통신채널을 사용하고 있지 않다.	
34. 이용자의 보안관제 수행에 필요한 제반사항(로그기록 등)을 지원하고 있습니까? ① 보안관제에 필요한 제반사항을 상시 지원하고 있다. ② 필요 시, 지원하고 있다. ③ 지원하고 있지 않다.	
35. 외부공격(DDoS, 해킹, 비인가 접속 등)에 대해 대응하고 있습니까? ① 실시간 모니터링을 하고 있다. (☞ **36번**으로) ② 필요 시, 모니터링을 하고 있다. (☞ **36번**으로) ③ 모니터링을 하고 있지 않다. (☞ **37번**으로)	
36. 외부공격으로 인한 이상징후 발생 시, 이용자에게 통지하고, 조치하고 있습니까? ① 이용자에게 즉각 통지 및 조치하고 있다. ② 이용자에게 즉각 통지는 하고 있으나, 조치는 미흡하다. ③ 즉각 통지 및 조치는 하고 있지 않다.	
37. 클라우드 컴퓨팅 서비스 및 클라우드 시스템 이용 시 침해사고를 예방하기 위한 대응절차를 마련하고 있습니까? ① 침해사고 대응절차를 마련하고 있다. (☞ **38번**으로) ② 침해사고 대응절차를 마련하고 있지 않다. (☞ **42번**으로)	
38. 침해사고 대응절차에 침해사고 발생 시, 법적 통지 및 신고 의무에 대한 내용을 포함하고 있습니까? ① 법적 통지 및 신고 의무에 대한 내용을 포함하고 있다. ② 일부 법적 통지 및 신고 의무에 대한 내용을 포함하고 있다. ③ 포함하고 있지 않다.	
39. 침해사고 대응절차에 이용자와 제공자의 역할과 책임을 반영하고 있습니까? ① 반영하고 있다. ② 반영하고 있지 않다.	
40. 침해사고 발생 시, 이용자에게 통지하고, 조치하고 있습니까? ① 이용자에게 발생 내용, 원인, 조치 현황 등을 신속하게 알리고, 조치하고 있다. ② 이용자에게 신속하게 알리고 있으나, 조치는 미흡하다. ③ 즉각 통지 및 조치는 하고 있지 않다.	

점검 항목	비 고
41. 침해사고를 예방하기 위한 대응절차에 다음과 같은 내용을 반영하고 있습니까? **(☞ 해당내용 직접 체크(√))** □ 보안사고 식별 및 보고 - ① 보안사고 식별 및 보고(이용자), ② 관련 법에 따른 법적 신고, ③ 보안사고 자체조사 및 응급조치 등 □ 증거확보 및 대응 검토 - ① 보안사고 대응 증거 확보, ② 법적 조치 사전 검토, ③ 당사자 간의 합의 검토 등 □ 상황 분석 및 대응 조치 - ① 사고대응팀 구성, ② 보안사고 공동 대응 조치 및 복구 등 □ 재발 방지 조치 - ① 보안사고 분석 및 개선조치 보고서 제공(이용자), ② 법적 대응 및 조치 검토 등	
42. 클라우드 컴퓨팅 서비스의 업무 연속성을 보장하기 위한 백업 및 복구 등의 장애 대응 절차를 마련하고 있습니까? ① 장애대응 절차를 마련하고 있으며, 절차에 따라 이행하고 있다. (☞ **43번**으로) ② 장애대응 절차를 마련하고 있으나, 절차에 따른 실제 대응은 미흡하다. (☞ **43번**으로) ③ 별도 대응 절차가 없다. (☞ **45번**으로)	
43. 장애대응 절차에 장애 발생 시, 법적 통지 및 신고 의무에 대한 내용을 포함하고 있습니까? ① 법적 통지 및 신고 의무에 대한 내용을 포함하고 있다. ② 일부 법적 통지 및 신고 의무에 대한 내용을 포함하고 있다. ③ 포함하고 있지 않다.	
44. 장애 발생 시, 이용자에게 통지하고, 조치하고 있습니까? ① 이용자에게 발생 내용, 원인, 조치 현황 등을 신속하게 알리고, 조치하고 있다. ② 이용자에게 신속하게 알리고 있으나, 조치는 미흡하다. ③ 즉각 통지 및 조치는 하고 있지 않다.	
45. 클라우드 컴퓨팅 서비스의 제공 종료 또는 국가핵심기술 관련 정보의 이전 필요 시, 종료·이전 절차를 다음과 같이 마련하고 있습니까? **(☞ 해당내용 직접 체크(√))** □ 종료 또는 이전 실시 최소 6개월 전 사전 통보 □ 이용자 모든 정보의 이전 지원 □ 이용자 모든 정보의 완전 삭제·폐기 내역 제공 등에 대한 협조 □ 비밀유지 의무 및 분쟁 해결 지원 등	

③ 클라우드 컴퓨팅 서비스를 이용한 국가핵심기술 수출 - 이용자(14개)

점검 항목	비 고
1. 외국기업 등의 접근권한 허용 대상 보안서약서를 작성하고 있습니까? ① 모든 대상에 대해 보안서약서를 작성하고, 정기적으로 갱신하고 있다. ② 보안서약서를 작성하고 있으나, 계약 시점 또는 종료 시점에만 작성하고 있다. ③ 보안서약서를 별도로 작성하고 있지 않다.	
2. 외국기업 등의 접근권한 허용 대상 보안교육을 정기적으로 시행하고 있습니까? ① 정기적으로 실시하고 있다. ② 필요시, 실시하고 있다. ③ 실시하지 않고 있다.	
3. 외국기업 등의 접근권한 허용 대상에 제공되는 국가핵심기술 관련 정보를 식별하여 제공하고 있습니까? ① 식별하여 최소한으로 제공하고 있다. ② 일부만 식별하여 제공하고 있다. ③ 별도 식별하여 제공하고 있지 않다.	
4. 외국기업 등의 접근권한 허용 대상에 국가핵심기술 관련 정보 접근권한을 구분하여 부여하고 있습니까? ① 접근권한 인원을 구분하여 최소한으로 부여하고 있다. ② 접근권한을 구분하고 있으나, 실제 이행은 미흡하다. ③ 별도 구분하여 부여하고 있지 않다.	
5. 외국기업 등의 접근권한 허용 대상의 접근권한 적절성에 대해 정기적 점검하고 있습니까? ① 정기적으로 점검하고 있다. ② 필요 시, 점검하고 있다. ③ 점검하고 있지 않다.	
6. 외국기업 등의 접근권한 허용 대상에 다중 인증(MFA)* 방식을 운영하고 있습니까? <다중 인증> ▸ 다중 인증(Multi-Factor Authentication, MFA)은 두 개 이상의 서로 다른 인증을 요구하는 보안 방식 ① 계정 접근 시, 제한된 환경에서 2가지 이상의 인증을 요구하고 있다. ② 계정 접근 시, 1가지 인증 방식만 요구하고 있다. ③ 계정 접근 시, 별도 인증 방식은 요구하고 있지 않다.	
7. 외국기업 등의 접근권한 허용 대상의 비인가 단말기에 국가핵심기술 관련 정보의 저장을 제한하고 있습니까? ① 저장을 제한하고 있다. ② 저장을 제한하고 있으나, 일부 환경에서는 제한하지 않는다. ③ 별도 제한하지 않는다.	
8. 외국기업 등의 접근권한 허용 대상이 단말기에 국가핵심기술 관련 정보의 저장이 필요 시, 이용자가 통제 가능한 환경에서 암호화 하여 저장하고 있습니까? ① 통제 가능한 환경에서 암호화 하여 저장하고 있다. ② 통제 가능한 환경은 아니나, 암호화 하여 저장하고 있다. ③ 별도 암호화 하고 있지 않다.	

점검 항목	비 고
9. 외국기업 등의 접근권한 허용 대상이 국가핵심기술 관련 정보 이용 시, 다음과 같이 보안통제를 실시하고 있습니까? (☞ **해당내용 직접 체크(√)**) ☐ 물리적 또는 논리적으로 격리된 환경 ☐ 간접 접속 방식 적용 ☐ 사전 식별·지정된 단말기에서만 사용 ☐ 국가핵심기술 관련 정보의 열람, 회수, 폐기에 대해 정기적으로 점검 ☐ 로그·이용기록 유지(1년 이상) 및 정기적으로 점검	
10. 외국기업 등의 접근권한 허용 대상의 국가핵심기술 관련 정보 접근 허용기간 동안 이상행위에 대한 모니터링을 실시하고 있습니까? ① 실시간 모니터링을 하고 있다. ② 모니터링을 하고 있으나, 실시간 모니터링은 미흡하다. ③ 모니터링을 하고 있지 않다.	
11. 외국기업 등의 접근권한 허용 시 침해사고를 예방하기 위한 대응절차를 마련하고 있습니까? ① 침해사고 대응절차를 마련하고 있다. (☞ **12번**으로) ② 침해사고 대응절차를 마련하고 있지 않다. (☞ **14번**으로)	
12. 침해사고를 예방하기 위한 대응절차에 다음과 같은 내용을 반영하고 있습니까? (☞ **해당내용 직접 체크(√)**) ☐ 유출금지 대상 ☐ 사고처리 방안 ☐ 재발방지 조치 ☐ 침해신고 절차(관련 법에 따른 법적 신고 의무) 등	
13. 침해사고 대응절차에 외국기업 등의 접근권한 허용 대상의 역할과 책임을 반영하고 있습니까? ① 반영하고 있다. ② 반영하고 있지 않다.	
14. 외국기업 등의 접근권한 허용기간 종료 시, 다음과 같이 보안통제를 실시하고 있습니까? (☞ **해당내용 직접 체크(√)**) ☐ 국가핵심기술 관련 정보 완전 삭제·폐기 방안 마련 ☐ 완전 삭제·폐기에 대한 확인 ☐ 삭제·폐기에 대한 이력 유지(1년 이상)	

국가핵심기술
클라우드 컴퓨팅 서비스 이용을 위한
보안관리 안내서

국가핵심기술 클라우드 컴퓨팅 서비스 이용을 위한 보안관리 안내서

- 발행일 | 2025. 4.
- 발행처 | 산업통상자원부, 한국산업기술보호협회
- 주 소 | 서울 서초구 서운로1길 34 한국산업기술보호협회
- 전 화 | 02-3489-7000