국가 클라우드 컴퓨팅 보안 가이드라인

국가정보원 NATIONAL INTELLIGENCE SERVICE

NSR 국가보안기술연구소

문서이력

개정일	버전	내 역	비 고
2012. 12	1.0	초판 작성	
2016. 05	2.0	공공기관의 민간 클라우드 컴퓨팅 서비스 도입 관련 보안기준 추가	전면 개정
2018. 05	3.0	SaaS 환경 보안기준, 클라우드 업무환경 접속 단말 보안기준, 가이드라인 요약 추가	
2019. 03	3.5	행안부 『행정·공공기관 민간 클라우드 이용 가이드라인』 반영, 국정원 『국가 정보보안 기본지침』 개정 반영	부분 개정
2023. 01	4.0	시스템 중요도 분류 절차 및 클라우드 영역별 보안기준 추가, 국정원 『국가 정보보안 기본지침』 개정 반영, 가이드라인 명칭을 『국가 클라우드 컴퓨팅 보안 가이드라인』으로 개정	부분 개정

목 차

제3장
클라우드 컴퓨팅 도입 22

제4장
클라우드 컴퓨팅 보안기준 46

부록목차

부록

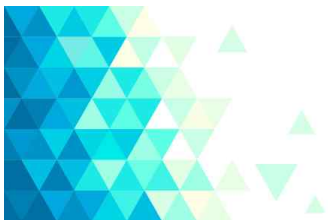
그림목차

그림 목차

그림목차

표 목차

표 목차



제1장
개요

제1절 목적 및 필요성

클라우드 컴퓨팅은 가상화 기술과 초고속 네트워크 기술을 이용하여 IT 자원의 효율성을 높이는 기술로서 국내·외 민간기업과 국가·공공기관에서의 이용이 확대되고 있다.

하지만 클라우드 컴퓨팅은 자원공유, 가상화 등 클라우드 컴퓨팅의 특성으로 인한 보안 위협을 내재하고 있으며 IT자원 및 사용자들의 정보가 집적되어 있기 때문에 해킹, DDoS 공격의 표적이 되기 쉽고, 사고 발생시 대규모 피해가 발생 할 수 있다.

따라서 클라우드 컴퓨팅을 도입하고자 하는 경우에는 클라우드 컴퓨팅의 특징과 개념, 시스템 및 데이터 보안성 등을 명확히 이해하여 도입 타당성을 신중하게 검토해야 한다. 또한 발생 가능한 보안위협을 최소화하기 위하여 보안 기준을 준수해야 하며 안전한 클라우드 컴퓨팅 서비스를 구축·도입해야 한다.

이에 국가정보원은 국가·공공기관의 클라우드 컴퓨팅 도입 시 보안수준을 향상시킬 수 있는 보안성 확인 기준으로서 「국가 클라우드 컴퓨팅 보안 가이드라인」을 만들게 되었다.

국가·공공기관은 본 가이드라인뿐만 아니라 「국가 정보보안 기본지침」, 「정보통신망 보안관리 실무요령」, 「국가·공공기관 업무전산망 분리 및 자료전송 보안 가이드라인」, 「안전한 정보통신 환경 구현을 위한 네트워크 구축 가이드라인」, 「국가·공공기관 용역업체 보안관리 가이드라인」등 관련 규정 및 가이드라인에 명시된 보안요구사항들을 종합적으로 검토하여 클라우드 컴퓨팅 사업계획을 수립하여야 한다. 사업계획 수립 시에는 행정안전부의 『행정·공공기관 클라우드컴퓨팅서비스 이용안내서』에 따라 사업타당성 검토를 수행하고 클라우드 이전 여부를 결정해야 한다. 수립된 사업계획은 국가정보원에 보안성검토를 의뢰하여 안전성 확인 절차를 거쳐야 하며, 검토 결과에 따라 클라우드 컴퓨팅 사업을 수행할 수 있다.

제2절 구성 및 용어

1. 가이드라인 구성

본 가이드라인의 구성은 다음과 같다. 제2장에서는 클라우드 컴퓨팅 개념 및 특징과 클라우드 컴퓨팅 환경에서 나타날 수 있는 보안 위협에 대하여 알아본다. 제3장에서는 국가·공공기관의 클라우드 컴퓨팅 도입 유형 및 절차에 대해 기술하고, 마지막으로 제4장에서는 국가·공공기관의 클라우드 컴퓨팅 보안 기준에 대하여 기술한다.

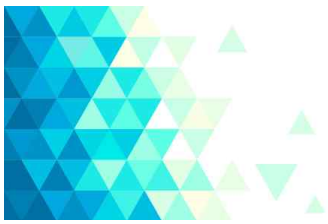
2. 주요 용어정의

본 가이드라인에서 사용되는 용어 정의는 [표 1]과 같다.

용 어		정 의
클라우드 컴퓨팅		집적·공유된 정보통신기기, 정보통신설비, 소프트웨어 등 정보통신자원을 이용자의 요구나 수요 변화에 따라 정보통신망을 통하여 신축적으로 이용할 수 있도록 하는 정보처리체계
클라우드 인프라		클라우드 컴퓨팅 제공을 목적으로 하는 설비, 하드웨어, 가상화 인프라
클라우드 컴퓨팅 서비스		클라우드 컴퓨팅을 활용하여 정보통신자원을 제공하는 서비스로 서버, 저장장치, 네트워크 등을 제공하는 서비스, 응용프로그램 등 소프트웨어를 제공하는 서비스, 응용프로그램 등 소프트웨어 개발·배포·운영·관리 등을 위한 환경을 제공하는 서비스 등을 포함
하이퍼바이저		단일 컴퓨팅시스템에서 서로 다른 다수의 운영체제를 동시에 실행하기 위한 플랫폼 또는 소프트웨어
가상머신 (VM:Virtual Machine)		가상화 기술에 의해 논리적 시스템 자원(CPU, 메모리, 디스크, 네트워크 등)을 이용, 독립적으로 OS 운영환경이 실행되는 시스템
가상 환경	**가상서버**	서버 가상화를 통해 독립적으로 제공되는 서버형태의 가상머신
	가상PC	데스크톱 가상화를 통해 독립적으로 제공되는 PC형태의 가상머신
	가상S/W	애플리케이션 가상화를 통해 독립적으로 제공되는 S/W

용 어	정 의
가상자원	가상 인프라를 통해 가상화된 가상 머신, 가상 스토리지, 가상 소프트웨어 등의 자원
가상 인프라	가상환경을 제공하기 위해 필요한 하이퍼바이저, 가상 머신, 가상자원 인터페이스 등으로 구성된 인프라
인프라 제공 서비스	서버, 스토리지, 네트워크 등 인프라 자원을 가상환경으로 만들어 필요에 따라 사용하도록 제공 하는 클라우드 컴퓨팅 서비스
플랫폼 제공 서비스	개발을 위한 플랫폼 자원을 별도 구축 없이, 가상환경으로 만들어 필요에 따라 사용하도록 제공하는 클라우드 컴퓨팅 서비스
소프트웨어 제공 서비스	응용 소프트웨어를 별도의 설치없이, 네트워크를 통해 사용하도록 제공하는 클라우드 컴퓨팅 서비스
CSP(Cloud Service Provider) 클라우드 관리자	민간 사업자의 시스템 및 전산 환경을 통제 및 관리할 수 있는 권한을 가진 관리자
시스템관리자	클라우드 컴퓨팅 구성요소에 접근하여 클라우드 환경을 통제할 수 있는 권한을 가진 관리자
인증서버	단말PC를 이용하여 클라우드 컴퓨팅 환경에 접근하는 관리자 및 사용자를 인증하기 위한 구성요소
자원관리서버	가상화서버의 하이퍼바이저, 가상머신 자원사용률을 모니터링하고, 사용자에게 가상머신 사용권한을 부여하거나 회수하기 위한 구성요소
가상화서버	하이퍼바이저 기술을 이용하여 다수의 가상머신을 독립적으로 실행하는 구성요소
가상PC 사용자	가상PC에 원격 접근하여 가상PC를 사용할 수 있는 권한을 가진 사용자
국가용 보안요구사항 준수 성능평가	국가용 보안요구사항을 준수하여 받은 성능평가
통합관리기관	행정기관등의 정보시스템을 통합적으로 구축·관리하기 위해 지정한 전담기관

[표 1] 용어 정의



제2장
클라우드 컴퓨팅 개념

제1절 클라우드 컴퓨팅 개념

1. 클라우드 컴퓨팅 정의

클라우드 컴퓨팅은 1965년 미국의 전산학자 존 매카시가 '앞으로의 컴퓨팅 환경은 공공시설을 쓰는 것과도 같을 것'이라는 개념을 제시한데서 유래한다. 최근에는 초고속 네트워크와 가상화 기술의 발전으로 원격의 사용자에게 논리적으로 분할된 컴퓨팅 자원을 끊김이 없이 제공하는 서비스가 가능해짐으로써 클라우드 컴퓨팅 개념이 대두되고 있다.

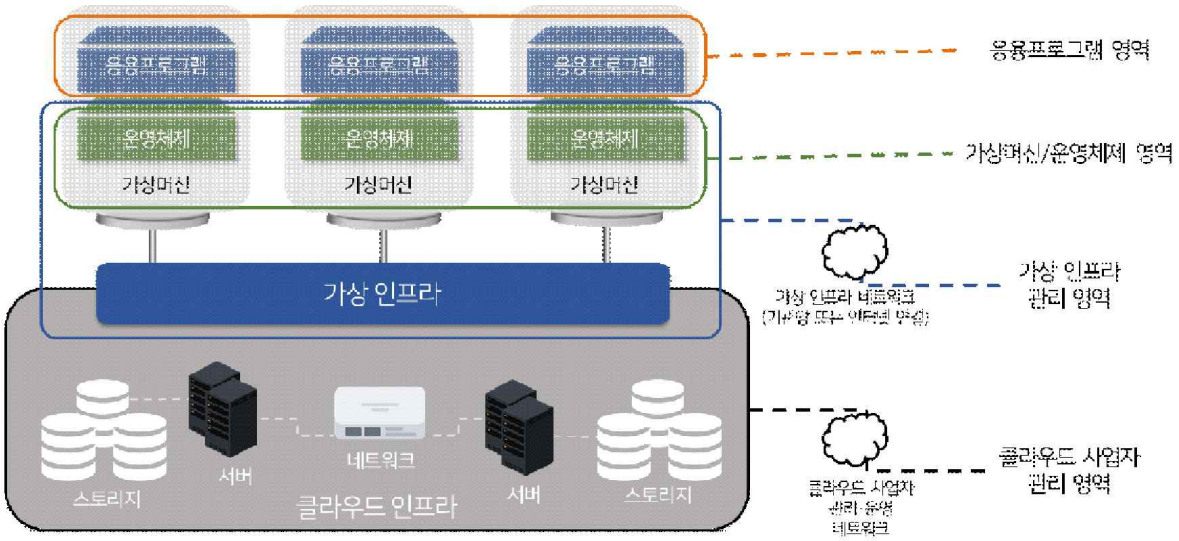
국제적으로 공신력 있는 기관 중 하나인 미국표준기술연구소(NIST)는 '이용자가 IT자원을 필요한 만큼 빌려서 사용하고, 서비스 부하에 따라서 실시간 확장성을 지원받으며, 사용한 만큼 비용을 지불하는 컴퓨팅'으로 정의하고 있다. 유명 리서치 기관인 가트너는 '인터넷 기술을 활용해 많은 고객들에게 수준 높은 확장성을 가진 자원들을 서비스로 제공하는 것'으로 정의하고 있으며, 국내의 경우 한국정보통신기술협회(TTA)에서는 '인터넷 기술을 활용하여 IT 자원을 서비스로 제공하는 컴퓨팅'으로 정의하고 있다.

이러한 정의에 포함된 공통된 요소는 클라우드 컴퓨팅을 이용하면 가상화 기술을 이용하여 가상의 컴퓨팅 자원(가상서버, 가상네트워크, 스토리지, 플랫폼, 소프트웨어 등)을 사용자에게 제공하는 것이 가능하다는 점이다. 본 가이드라인에서는 '클라우드 컴퓨팅 서비스'를 클라우드 컴퓨팅을 활용하여 정보통신자원을 제공하는 서비스로 서버, 저장장치, 네트워크 등을 제공하는 서비스, 응용프로그램 등 소프트웨어를 제공하는 서비스, 응용프로그램 등 소프트웨어 개발 · 배포 · 운영 · 관리 등을 위한 환경을 제공하는 서비스 등을 포함하는 것으로 정의한다.

2. 클라우드 컴퓨팅 구성

클라우드 컴퓨팅은 물리적으로 클라우드 컴퓨팅 환경을 제공하는 클라우드 인프라, 클라

우드 인프라를 기반으로 하이퍼바이저 등의 가상화 기술을 이용하여 만든 가상환경으로 구성된 가상 인프라, 가상 인프라에서 제공되는 가상머신, 가상머신에서 동작하는 운영체제와 응용프로그램으로 구성된다.



[그림 1] 클라우드 컴퓨팅 구성 개념도

클라우드 인프라는 가상 인프라를 만들기 위한 물리적 서버, 네트워크, 스토리지 장비들로 구성되며 클라우드 구축기관 또는 클라우드 인프라 사업자와 같은 클라우드 서비스 제공자가 관리한다. 클라우드 서비스 제공자는 클라우드 관리·운영시스템을 이용하여 VPC(Virtual Private Cloud)와 같은 가상 인프라를 구성하여 제공할 수 있다. VPC란 서버 가상화 및 네트워크 가상화 기술(하이퍼바이저, 네트워크 기능 가상화(NFV) 및 소프트웨어 정의 네트워크(SDN) 등)을 기반으로, 논리적으로 분리된 가상 네트워크상에 구성된 클라우드 자원을 말한다. 클라우드 인프라의 관리·운영 네트워크는 가상 인프라 네트워크과 분리되어야 하며 안전하게 관리해야 한다.

가상 인프라는 가상 서버, 가상 네트워크, 가상 스토리지 등의 가상환경으로 구성된다. 클라우드에는 여러 가상 인프라가 구성될 수 있으며, 각각의 가상 인프라들은 논리적으로 격리되도록 구성해야 한다. 논리적으로 격리된 가상 인프라는 가상머신 탈출 등의 제로데이 취약점, 관리자 부주의로 인한 설정 오류 등으로 가상 인프라간 격리 훼손이 발생 할 수 있다. 따라서 가상 인프라 영역의 시스템 및 데이터에 비인가 접근 할 수 있는 취약점을 방지/완화/제거하고, 비인가 접근에 대한 모니터링을 해야 한다. 또한, 가상 인프라는

인터넷 또는 기관 네트워크로 연결될 수 있으므로 방화벽, IDS, IPS 등 정보보호시스템을 이용한 보호가 필수적이다.

클라우드 컴퓨팅은 클라우드 구축 유형, 서비스 형태에 따라 클라우드 인프라, 가상 인프라, 가상머신, 용용프로그램 등 각 구성 요소에 서로 다른 관리 주체가 있을 수 있다. 따라서 전체 구성에 대한 이해와 여러 관리 주체 중에 기관과 사용자가 관리하는 관리 범위에 대한 이해가 필수적이며, 이를 바탕으로 안전한 클라우드 이용 계획을 마련해야 한다.

제2절 클라우드 컴퓨팅 분류

1. 목적별 분류

클라우드 컴퓨팅은 목적에 따라 국가기관 행정업무를 위해 구축·사용하는 '업무용 클라우드 컴퓨팅'과 외부에 공개하여 국민에게 대민서비스 등을 제공하기 위한 '공개용 클라우드 컴퓨팅'으로 분류할 수 있다.

가. 업무용 클라우드 컴퓨팅

업무용 클라우드 컴퓨팅은 기관에서 업무용으로 사용하는 IT 자원을 클라우드 컴퓨팅으로 구축한 형태이다. 기존 컴퓨팅 환경에서 외부와의 접근이 차단된 업무서버, 업무PC, 업무용 S/W가 업무용 클라우드로 전환 될 수 있다. 업무용 클라우드에는 중요한 업무 자료가 있을 수 있으므로 더욱 안전한 관리가 필수적이다.

나. 공개용 클라우드 컴퓨팅

공개용 클라우드 컴퓨팅은 기관에서 사용하는 IT 자원 중 인터넷 연결이 필수적인 자원을 클라우드 컴퓨팅으로 구축한 형태이다. 기존 컴퓨팅에서 DMZ영역과 같이 공개용 홈페이지, 메일 서버, DNS서버를 운용하는 대민서비스 영역이 공개용 클라우드로 전환될 수 있다. 공개용 클라우드는 DDoS 공격, 외부로부터의 해킹 등의 다양한 공격이 발생할 수 있어 방화벽, IDS, IPS, DDoS 차단시스템 등 정보보호시스템을 이용한 보호가 필요하다.

2. 서비스별 분류

클라우드 컴퓨팅은 제공하는 서비스의 형태에 따라 인프라 제공 서비스(IaaS), 플랫폼 제공 서비스(PaaS), 소프트웨어 제공 서비스(SaaS)와 인프라, 플랫폼, 소프트웨어를 둘 이상 복합하여 제공하는 복합서비스로 분류할 수 있다.

서비스별 분류	내용
인프라 제공 서비스 (Infrastructure as a Service)	o 서버, 스토리지, 네트워크등 인프라 자원을 가상환경으로 만들어 필요에 따라 사용하도록 제공 o 서버, 저장장치, 네트워크 등을 서비스 형태로 제공
플랫폼 제공 서비스 (Platform as a Service)	o 개발을 위한 플랫폼 자원을 별도 구축없이, 가상환경으로 만들어 필요에 따라 사용하도록 제공
소프트웨어 제공 서비스 (Software as a Service)	o 응용 소프트웨어를 별도의 설치없이, 네트워크를 통해 사용하도록 제공 o 애플리케이션를 서비스 형태로 제공
복합서비스	o 인프라, 플랫폼, 소프트웨어 제공 서비스를 둘 이상 복합하여 서비스로 제공 o 예) DaaS 등

[표 2] 서비스별 분류

가. 인프라 제공 서비스(IaaS)

IaaS는 사용자가 별도의 인프라를 구축하지 않고 인터넷을 통해 가상서버, 가상PC 등의 컴퓨팅 자원을 이용하는 서비스 유형이다.

사용자는 인터넷을 통해 윈도우, 리눅스 등의 가상서버 환경을 생성하고, 필요한 네트워크 환경을 구성함으로서 홈페이지 서버 등으로 활용할 수 있다. IaaS는 CPU, 메모리와 같은 가상자원의 성능 또는 네트워크 데이터 이용량에 따라 비용을 지불하는 것이 특징이다.

나. 플랫폼 제공 서비스(PaaS)

PaaS는 별도의 개발 플랫폼을 구축하지 않더라도 자바와 같은 웹 애플리케이션 개발환경이나 MySQL과 같은 DB환경을 제공함으로써, 사용자가 쉽게 애플리케이션을 개발하여 사용할 수 있는 기능을 제공하는 서비스 유형이다.

PaaS를 이용하여 소프트웨어를 개발·활용하고자 하는 사용자는 별도의 인프라 구축 및 개발 플랫폼 구축 없이 PaaS가 제공하는 개발 플랫폼을 활용할 수 있다. 이러한 PaaS는 IaaS를 이용하는 비용과 개발 플랫폼을 이용하는 비용을 서비스 요금으로 지불하고 이용하게 된다.

다. 소프트웨어 제공 서비스(SaaS)

SaaS는 소프트웨어를 별도로 구매하거나 설치하지 않고 소프트웨어가 설치되어 서비스하는 클라우드에 접속하여 해당 소프트웨어를 이용하는 유형이다.

사용자는 웹 표준 기반으로 동작하는 웹오피스, 화상회의, 협업솔루션 등 다양한 SaaS가 등장하고 있다. 이러한 SaaS는 서비스를 제공하는 클라우드와 네트워크로 연결된 곳에서는 언제 어디서든 소프트웨어를 활용 할 수 있는 것이 특징이다.

라. 복합서비스

복합서비스는 IaaS, PaaS, SaaS 형태의 둘 이상의 서비스를 복합하여 클라우드 서비스 제공하는 유형이다.

복합서비스의 대표적인 사례에는 DaaS(Desktop as a Service)가 있다. DaaS는 인프라 서비스로 제공되는 가상PC와 소프트웨어를 제공한다.

제3절 클라우드 컴퓨팅 특징

1. 기존 컴퓨팅 환경과의 차이

기존 컴퓨팅 환경의 서버, PC, 소프트웨어는 물리적으로 독립된 자원 단위로서 기관의 서버실 또는 사무실의 개인 자리에 위치한다. 새로운 자원이 필요한 경우, 물리적 자원에 대한 구매, 설치 등의 과정이 필요하며 운영의 주체에 따라 서로 다른 운영 및 보안관리가 이루어진다.

클라우드 환경의 가상의 컴퓨팅 자원(가상서버, 가상네트워크, 스토리지, 플랫폼, 소프트웨어 등)은 논리적으로 독립된 자원단위로서 데이터 센터 내부에 위치하며 경우에 따라 여러 곳의 데이터 센터에 분산되어 위치한다. 클라우드 환경에서 새로운 자원이 필요한 경우, 클라우드에서 필요한 가상자원을 신속하게 추가하여 이용하는 것이 가능하며 제공되는 가상자원들은 동일 수준의 운영 및 관리가 이루어진다. 클라우드 컴퓨팅과 기존 컴퓨팅 환경의 차이점을 표로 정리하면 [표 3]과 같다.

대상	기존 환경	클라우드 환경	특 징
서버	IT 자원 개별 구축·운용	IT 자원 통합 구축·운용	중앙집중화
	물리적 서버 단위 이용	논리적 서버 단위 이용	신속한 서버자원 추가
	서버별 운용 환경 상이	동일 서버 운용 환경 제공	서버 보안정책 반영 용이
소프트웨어	사무실의 PC 등 고정 장소	장소 이동 가능	중앙집중화
	물리적 PC에 설치 후 이용	서비스 단위 이용	신속한 자원 추가
	개인PC 운용 환경 상이	동일 서비스 환경 제공	정책반영 용이

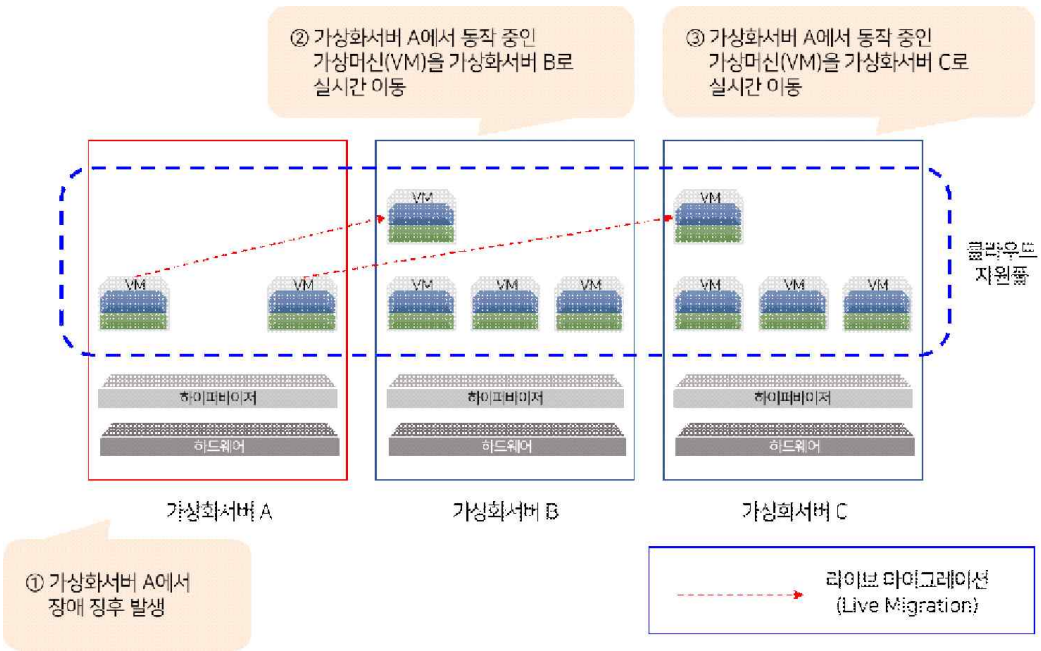
[표 3] 클라우드 컴퓨팅과 기존 컴퓨팅 환경과의 차이

가. 자원제공/회수

클라우드 사용자가 필요한 자원을 요청하면 클라우드 관리자는 필요한 만큼의 가상의 컴퓨팅 자원을 클라우드 사용자에게 제공한다. 클라우드 사용자가 가상자원 사용을 종료하면 종료된 자원을 회수하여 다른 클라우드 사용자가 사용 할 수 있도록 한다.

나. 장애처리

클라우드 컴퓨팅은 가상자원을 동적으로 관리 할 수 있어 장애처리에 용이하다. 예를 들어, 가상화서버에 장애징후가 발생하는 경우, 가상화서버에서 동작중인 가상머신을 다른 가상화서버로 이동시켜 장애 상황에서도 정상적인 서비스를 지원한다. 클라우드 컴퓨팅 장애처리 개념도는 [그림 2]와 같다.



[그림 2] 클라우드 컴퓨팅 장애처리 개념도

다. 부하분산

가상화서버들의 부하를 모니터링하고 새로운 자원 요청 시, 부하가 낮은 서버의 가상머신을 사용자에게 제공한다. 부하가 높은 가상화 서버의 가상머신들을, 부하가 낮은 가상화 서버의 가상머신으로 실시간 이동시킴으로써 부하를 분산시킬 수 있다.

라. 보안관리

하이퍼바이저의 보안업데이트 및 가상화 서버 재부팅이 필요한 경우, 가상화 서버에서 동작 중인 모든 가상머신을 다른 가상화 서버로 이동시킨 후, 업데이트 및 재부팅 등의 작업을 수행함으로써 가상머신 중단 없이 시스템 보안관리가 가능하다.

마. 효율성관리

가상서버 가동률이 낮은 저녁시간 때에는 가상서버를 전체 가상화 서버에서 일부 가상화 서버로 이동시킨 후, 사용하지 않는 가상화 서버의 전원을 종료할 경우, 클라우드 컴퓨팅에 소요되는 전력을 절약할 수 있다.

2. 클라우드 컴퓨팅 도입 시 장점

클라우드 컴퓨팅은 가상화 기술에 의해 논리적으로 분리된 자원을 이용하여 비용을 절감할 수 있고, 물리적 위치를 중앙으로 집중시킴으로써 관리가 용이하다. 또한 컴퓨팅 자원의 이용량에 따라 CPU, 메모리 등의 가상자원을 동적으로 할당·회수함으로써 가용성을 높일 수 있는 장점이 존재한다.

가. 가상화 기술을 이용한 비용 절감

(1) 다수의 가상머신 운용

물리적 자원을 논리적으로 분할하여 다수의 가상머신을 효율적으로 운용할 수 있으므로 서버, 스토리지, 네트워크 장비의 구입비용을 절감할 수 있다.

(2) 컴퓨팅 자원 재사용 용이

사용자가 반납한 컴퓨팅 자원을 회수하여 다른 사용자에게 재할당할 수 있으므로, 서버 등의 장비를 매번 구매할 필요가 없다.

(3) 운용 비용 절감

사용자별로 소프트웨어를 구매하여 설치할 필요 없이, 중앙서버에 접속하여 서비스형 소프트웨어를 다수의 사용자가 이용할 수 있으므로, 소프트웨어 구매 및 유지보수 비용을 절감할 수 있다.

나. 물리적 위치 중앙집중화에 의한 관리 편의성 제공

(1) 물리적 접근 통제 강화

가상머신의 하드디스크, 네트워크 카드, 메모리 등 자원에 물리적 접근이 불가하여 탈취·훼손 위험성이 줄어든다.

(2) 비인가 통신망 통제 강화

블루투스, 테더링 등 네트워크 임의설정이 불가하여 비인가 우회 통신망에 의한 자료 유출 등의 위험성이 줄어든다.

(3) 자원 사용현황 모니터링 강화

물리·가상 자원의 CPU, 메모리, 하드디스크 등 시스템 자원 사용현황에 대한 모니터링이 가능하다.

다. 신속한 서버자원 추가·회수를 통한 신축성 제공

(1) 가상머신 부하분산 가능

사용 중인 가상머신의 CPU·메모리 등 사용량이 증가할 경우, 클라우드 자원의 다른 가상머신을 추가 할당하여 부하분산이 가능하다.

(2) 유휴자원 활용도 향상

가용률이 낮은 서버에 할당된 자원을 가용율이 높은 서버에 할당하는 것이 가능하여 유휴자원의 활용도를 향상시킬 수 있다.

(3) 신속한 OS 복구 지원

가상머신이 해킹 또는 악성코드 감염에 의해 OS가 파괴된 경우 가상머신을 재할당하여 신속한 복구가 가능하다.

3. 클라우드 컴퓨팅 도입 시 단점

클라우드 컴퓨팅 환경에서는 데이터가 중앙에 집중하게 되므로 자료의 대량 유출이 야기될 수 있고, 장애 발생 시 클라우드 컴퓨팅을 이용하는 업무 전체가 중단될 수 있으며, 동일한 환경의 가상머신 모두가 취약점에 대한 보안위협을 공유하게 되는 잠재적 위험성이 있다. 또한 클라우드 컴퓨팅은 동일한 물리 서버를 다수의 사용자에게 할당함에 따라 다른 사용자가 자료를 무단 열람할 수도 있으므로 접근제어 등 관리에 만전을 기해야 한다.

가. 대량 자료유출 위험성 증대

(1) 악성코드 감염 가상머신에 의한 유출

가상머신이 악성코드에 감염될 경우 클라우드 자원 전체에 악성코드가 전파되어 서버에 저장된 자료 전체가 유출되는 등의 심각한 피해로 이어질 수 있다.

(2) 클라우드 관리자에 의한 유출

클라우드 관리자가 스토리지에 직접 접근하여 데이터를 열람할 수 있는 경우, 관리자 위협에 의해 스토리지에 존재하는 모든 데이터가 유출 될 수 있다.

나. 장애발생시 클라우드 컴퓨팅 마비

(1) 네트워크 장애

기존 IT 환경에서는 네트워크 장애 발생 시 로컬PC에서 일부업무를 수행할 수 있지만, 클라우드 환경에서는 모든 업무를 수행할 수 없다.

(2) 인증서버, 자원관리서버 장애

인증서버 장애 발생 시 가상자원으로 로그인을 할 수 없고, 자원관리서버 장애 발생 시 가상자원을 할당받을 수 없으므로 모든 업무를 수행할 수 없다.

(3) 가상화 서버 장애

가상화 서버 장애 발생 시 해당 가상화 서버상의 일부 가상머신을 이용하는 사용자들은 업무 수행이 어려울 수 있다.

(4) 스토리지 장애

스토리지 장애 발생 시 업무 수행이 어려울 수 있고, 스토리지에 저장된 데이터가 훼손될 위험이 있다.

다. 동일 보안위협 공유

(1) 가상머신 취약점 공유

운영체제 또는 응용프로그램상의 취약점이 존재하는 가상머신을 할당할 경우 모든 가상머신은 동일한 취약점에 대한 보안위협을 공유하게 된다.

(2) 네트워크 취약점 공유

공유폴더 비인가 접근 등 네트워크 취약점이 존재하는 가상머신을 할당할 경우 모든 가상머신은 동일한 네트워크 보안위협을 공유하게 된다.

라. 다중 임차 위협에 노출

(1) 비인가자에 의한 업무자료 무단 접근

클라우드 컴퓨팅은 가상화 기술을 이용하여 IT자원을 논리적으로 다수의 사용자에게 할당한다. 논리적 격리 기술이 발전과 동시에 지속적인 제로데이 취약점이 보고되고 있어 취약점 발현시 논리적 격리 훼손이 발생할 수 있다. 또한, 적절한 접근제어를 하지 않을 경우 비인가자가 다른 사용자의 가상자원에 무단 접근하여 자료의 유출·훼손·변조 등을 할 수 있다.

제4절 클라우드 컴퓨팅 보안 위협

제3절의 클라우드 컴퓨팅 특징에서 살펴보았듯이 클라우드 컴퓨팅은 자원 공유와 집중화 때문에 얻는 장점도 많지만 이로 인해 더욱 외부 공격에 취약할 수 있는 단점이 있다. 그러므로 클라우드 컴퓨팅 도입 과정에서 도입 전·후로 발생할 수 있는 보안 위협들을 식별하고 위협을 최소화하는 과정이 필요하다. 이를 위해, 본 절에서는 클라우드 컴퓨팅 환경의 구성요소(가상환경, 클라우드 인프라, 정책, 사고·장애 대응, 인증·권한, 데이터) 및 보안속성(인증, 기밀성, 무결성, 가용성, 감사, 권한)을 정의하고 이에 따른 보안 위협을 식별하였다.

1. 클라우드 컴퓨팅 환경 구성요소

[그림 3] 클라우드 컴퓨팅 환경 구성요소

가. 가상환경

기존의 PC, 서버 등의 정보시스템은 클라우드 인프라를 통해 가상화되어 사용자에게 서비스 형태로 제공된다. 대표적인 가상화 서비스로 인프라 제공 서비스(IaaS), 플랫폼 제공 서비스(PaaS), 소프트웨어 제공 서비스(SaaS)를 꼽을 수 있다. 클라우드 환경은 가상화를 기반으로 하는 자원공유 등과 같은 클라우드 환경만의 특징이 존재한다. 그러므로 클라우드 환경 특성에 맞는 보안 대책 마련이 필요하다.

나. 클라우드 인프라

사용자에게 가상환경을 제공하기 위한 클라우드 인프라는 설비, 하드웨어, 가상화 인프라로 구성되어 있다. 클라우드 인프라의 많은 부분들은 기존 정보시스템과 유사한 부분이 많기 때문에 신속한 보안업데이트, 주기적인 취약점 점검 등 기존 보안 대책이 적절하게 유지되어야 한다.

(1) 설비

클라우드 인프라 구성 요소에서 설비는 클라우드 컴퓨팅 환경 제공을 위한 물리적 장소 및 건물, 안전 장비, 방재 시설 등을 의미한다.

(2) 하드웨어

클라우드 인프라 구성 요소에서 하드웨어는 클라우드 컴퓨팅 환경 제공을 위한 서버, PC, 네트워크 장비, 저장소 등을 의미한다.

(3) 가상화 인프라

클라우드 인프라 구성 요소에서 가상 운영환경은 클라우드 컴퓨팅 환경 제공을 위한 호스트 운영체제, 하이퍼바이저, 데이터베이스 등을 의미한다.

다. 정책

클라우드 컴퓨팅 환경은 서비스 사용자와 서비스 제공자 간의 관계를 중심으로 이루어진다. 이 둘 간의 상호관계에 대한 신뢰성 유지를 위해서 법, 규정, 가이드라인, 계약 등과 같은 각종 준수사항을 만족시켜야 한다. 이를 위해서, 서비스 사용자는 자신이 준수해야 할 사항들을 식별해야 하며 이를 서비스 제공자에게 부과할 의무를 지닌다. 이러한 준수사항들은 정책적으로 명시화되어 사용자와 제공자 상호간에 공유되어야 하며, 준수 여부를 지속적으로 확인하여야 한다.

라. 사고 및 장애 대응

클라우드 컴퓨팅은 다수의 사용자들이 서비스 제공자의 컴퓨팅 자원을 공유하는 형태이다. 이는 사고 및 장애 발생 시 컴퓨팅 자원을 공유하고 있는 사용자들 모두에게 그 피해가 전파될 수 있다는 것을 의미한다. 그러므로 사고 신고 및 조사 체계 확립, 데이터 백업 등 복구 절차, 사고 및 장애 피해 격리 등과 같은 보안 강화 방안을 마련해야 한다.

마. 인증 및 권한

클라우드 컴퓨팅 환경은 다수의 사용자가 공유 자원에 접속하여 사용하는 특성을 지니고 있다. 또한, 외부 사용자들도 공유되는 자원에 접속할 수 있는 권한을 지닐 수 있다. 그러므로 서비스 제공자의 클라우드 컴퓨팅 환경 내에서 권한 부여 정책, 비인가자의 접근통제 정책 등과 같은 보안 강화 방안을 마련해야 한다.

바. 데이터

클라우드 컴퓨팅 환경은 구축 및 서비스 유형에 따라 사용자의 IT 자원에 대한 통제 수준이 달라지는 특징을 지니고 있다. 이는 기존 정보시스템 환경 수준으로 데이터 통제를 할 수 없다는 것을 의미한다. 그러므로 데이터에 대한 안전성을 확보하는 보안 강화 방안을 마련해야 한다.

2. 클라우드 컴퓨팅 환경 보안속성

클라우드 컴퓨팅의 모든 구성요소가 준수해야 하는 보안기준으로서의 보안속성을 [표 4]와 같이 분류한다.

보안속성	내 용
인증	클라우드 컴퓨팅에 접근하는 사용자를 식별하여 불법적인 사용자의 접근을 차단하는 보안속성
기밀성	클라우드 컴퓨팅에서 유통되거나 저장되는 데이터를 비인가자가 탈취하더라도 데이터의 정보를 얻지 못하도록 하는 보안속성
무결성	클라우드 컴퓨팅에서 유통되거나 저장되는 데이터를 비인가자가 위·변조 못하도록 하는 보안속성
가용성	클라우드 컴퓨팅에서 클라우드 컴퓨팅 구성요소에 대한 접근성을 항시 보장하는 보안속성
감사	클라우드 컴퓨팅에 접근한 사용자 기록을 항시 유지하여 해킹 등의 사고발생시 원인 규명을 위한 용도로 사용되는 보안속성
권한	클라우드 관리자, 가상서버 관리자, 사용자에 따른 접근 권한 및 접근 영역의 분리를 통해 클라우드 컴퓨팅의 접근통제에 사용하는 보안속성

[표 4] 클라우드 컴퓨팅 보안속성

3. 클라우드 컴퓨팅 환경 구성 요소에 따른 보안 위협

클라우드 컴퓨팅 환경에서는 악성코드 감염, DDoS와 같은 기존 정보시스템 환경에서 나타날 수 있는 보안 위협과 더불어 자원의 공유와 가상화를 통해 중앙 집중화된 환경으로 인한 보안 위협이 존재한다.

[표 5]에서는 각 클라우드 환경 구성요소 별 보안 위협 예시를 보여준다. 또한, 해당 보안 위협에 대응하기 위해 준수해야 할 대표적 보안속성을 제시하고 있다. 각 보안속성 준수를 위한 보안기준은 제4장에서 살펴본다.

클라우드 컴퓨팅 환경 구성 요소	보안 위협 예시		보안속성
가상환경	- 악성코드 감염 - SaaS 애플리케이션 취약점 - 인터페이스 및 API 취약점 - 가상자원 격리 위협 - 개발·운영 가상환경 비인가 접근 - App 데이터 변조		기밀성·무결성
클라우드 인프라	설비	- 물리적 위협 (화재, 정전 등)	기밀성·무결성
	하드웨어	- QoS - DDoS - Flood Attack - 네트워크 장비 설정 오류	
	가상화 인프라	- Multi-Tenancy (다중임차) - 공유 위협 - 솔루션 설정 오류	
정책	- 규정/법 미준수 - 인적 보안	- SLA 위반 - 용역 관리	감사
사고 및 장애 대응	- 동일 사고 재 발생 - 백업/복원 실패 - 사고 후 운영 실패		가용성
인증 및 권한	- 계정 탈취 - 내부자 위협	- 권한 상승/오용 - 단말 보안	인증·권한
데이터	- 데이터 유출 - 데이터 위치 (사법관할권) - 데이터 안전성 (백업 및 복원)	- 데이터 파괴	기밀성·무결성

[표 5] 보안 위협 예시

제3장
클라우드 컴퓨팅 도입

제1절 클라우드 컴퓨팅 도입 유형

국가·공공기관이 클라우드 컴퓨팅을 도입할 때에는 기관의 업무 특성, 보안성, 비용 등을 검토하여 클라우드 자원[1]을 다른 기관과 공유할 것인지, 기관 단독으로 사용할 것인지를 결정해야 한다. 또 클라우드 자원을 기관이 직접 물리적으로 통제할 것인지 아니면 다른 기관에게 물리적 통제권을 주고 위탁 관리할 것인지를 결정해야 한다.

클라우드는 자원공유 여부에 따라, 기관이 독자적으로 자원을 사용하는 기관용(Private)과 특정 커뮤니티에 속한 기관 간 클라우드 자원을 공유하는 커뮤니티용(Community), 민간 사업자에서 제공하는 서비스로 모든 사용자가 자원을 공유하는 공개용(Public)으로 분류할 수 있다.

또 클라우드 자원에 대한 물리적 통제권 여부에 따라, 기관이 직접 클라우드 자원에 대한 통제권을 갖는 직접 구축 클라우드(On-site)와 민간 사업자 등이 구축한 클라우드 시스템을 이용하여 기관의 자원을 위탁하는 외주 클라우드(Out-sourced)로 나눌 수 있다.

이에 따라 국가·공공기관이 클라우드 컴퓨팅을 도입하는 유형에는 클라우드 자원 공유 및 통제권 여부에 따라 ① 단일 기관이 도입하고 이용하는 유형(On-site Private) ② 커뮤니티에 속한 특정기관이 도입하고 커뮤니티에 속한 기관들이 자원을 공유하는 유형(On-site Community) ③ 민간 사업자에서 구축한 클라우드의 물리적 자원을 이용하는 유형(Out-sourced) ④ 민간 사업자 구축 클라우드 자원을 이용하면서 기존 내부 정보시스템과의 연계를 하는 유형(Hybrid) ⑤ 기관이 다수의 외주 클라우드를 연계하여 활용하는 유형(Multi) ⑥ 민간 사업자에서 제공하는 공개 클라우드를 이용하는 민간 클라우드(Public)로 [표 6]과 같이 분류할 수 있다.

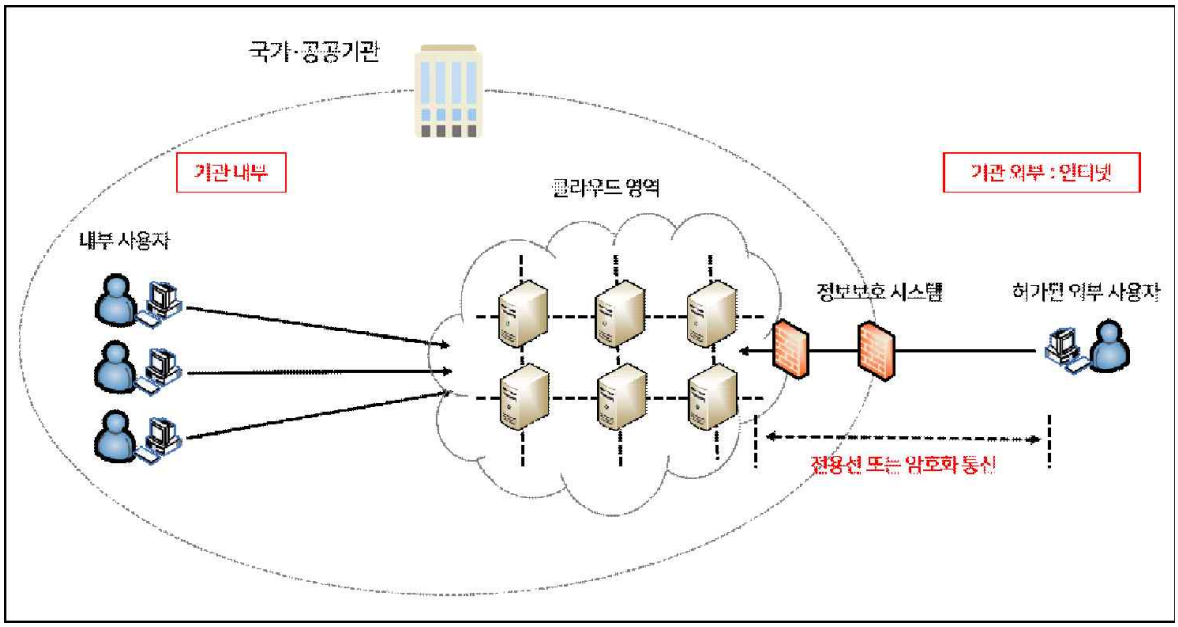
1) 클라우드 자원 : 클라우드 인프라 구축을 위한 물리적 설비, 서버, 장비 등

국가·공공기관은 민간 클라우드컴퓨팅서비스 국가정보원 국가사이버안보센터 홈페이지(www.ncsc.go.kr)에 게시된 도입요건 확인을 완료한 "민간 사업자 클라우드 컴퓨팅 서비스"를 이용한다. 도입요건 확인을 완료하지 않은 서비스를 도입하려는 경우에는 국가정보원의 보안기준(국가 정보보안 기본지침 및 동 가이드라인)에 부합하는 민간 사업자 클라우드 컴퓨팅 서비스 도입을 위하여, 운용 이전에 상위기관 또는 전문평가기관에 안전성 확인 및 국가정보원의 적합 여부 확인을 받아야 한다.

유형	내용	참조 기준
① 기관 구축·이용 (On-site Private)	o 기관이 자체 구축하고 직접 관리 o 기관이 클라우드 자원 통제권 보유 o 다른 기관과의 자원 공유 없음	제4장 제1절
② 기관 구축· 커뮤니티 이용 (On-site Community)	o 기관이 자체 구축하고 직접 관리 o 기관이 클라우드 자원 통제권 보유 o 커뮤니티에 속한 기관 간 클라우드 자원 공유 o 커뮤니티 외부 기관과의 자원 공유 없음	
③ 기관 이용 외주 (Out-sourced)	o 다수 기관이 공공 영역을 공동 임차 o 기관이 클라우드 자원 통제권 미보유 o 공용 영역 내 기관들과의 자원 공유	제4장 제2절
④ 하이브리드 (Hybrid)	o 기관 내부 정보시스템과 기관 외부의 외주 클라우드를 연계하여 활용 o 기관과 클라우드 제공자 간 클라우드 자원통제 공유 o 다른 기관과의 자원 공유 없음	
⑤ 멀티 클라우드 (Multi Cloud)	o 기관이 다수의 상용 클라우드를 연계하여 활용 o 기관이 클라우드 자원 통제권 미보유	
⑥ 공개 클라우드 (Public Cloud)	o 상용 클라우드 서비스를 활용 o 기관이 클라우드 자원 통제권 미보유 o 모든 기관 또는 사용자와 자원 공유	-

[표 6] 국가·공공기관 클라우드 컴퓨팅 구축 유형

1. 기관 구축·이용 클라우드



[그림 4] 기관 구축·이용 클라우드 구성도

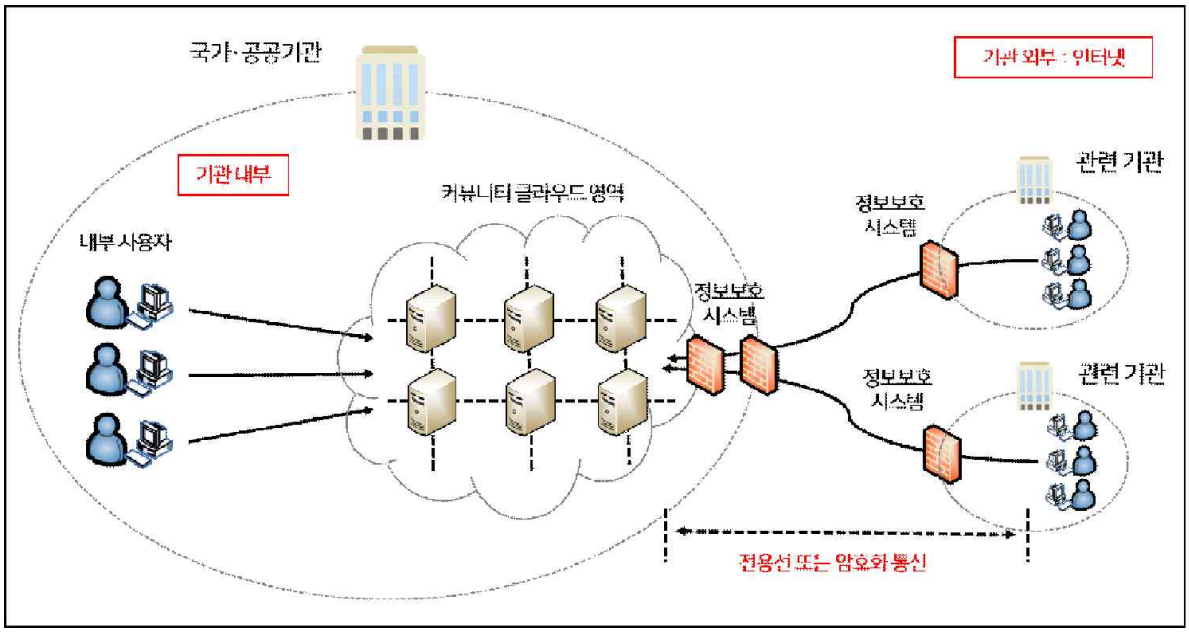
국가·공공기관 중 기관의 업무 특성으로 인해 독립적인 네트워크를 사용하거나 보안상 중요한 기관은 다른 기관과 자원을 공유하기 어렵다. 또 IT 자원에 대해 그 기관이 직접 통제권을 보유하여 장애나 사고 발생 시 즉시 대응해야 한다. 이에 따라 이러한 기관들이 클라우드 컴퓨팅을 도입할 때에는 기관이 직접 클라우드 컴퓨팅 환경을 구축하고 그 기관만이 클라우드 자원을 사용하는 기관 구축·이용 클라우드 유형이 적합하다. 이 유형의 클라우드 구성도는 [그림 4]와 같다.

○ 네트워크는 기관 내부에 위치하여 기관 시스템관리자가 직접 통제

○ 기관 외부에서 접근하는 경우 전용선 또는 암호화 통신(VPN 등)

○ 기관 내부망과 외부망 사이에 정보보호 시스템 구축

2. 기관 구축·커뮤니티 이용 클라우드



[그림 5] 기관 구축·커뮤니티 이용 클라우드 구성도

국가·공공기관 중 동일 네트워크를 사용하거나 업무 특성이 유사한 다른 기관과 IT 자원을 공유하는 데 문제가 없고, 클라우드 컴퓨팅 환경을 독자적으로 구축·관리하는 것이 곤란할 경우 선택할 수 있는 클라우드 유형이다. 커뮤니티에 속한 대표기관이 클라우드 컴퓨팅 환경을 구축하고 이를 커뮤니티에 속한 기관들과 클라우드 자원을 공유하여 공동으로 이용한다. 이 유형은 커뮤니티에 속한 기관간에는 클라우드 자원을 공유하나 커뮤니티에 속하지 않은 기관과의 자원공유는 없다. 이 유형의 클라우드 구성도는 [그림 5]와 같다.

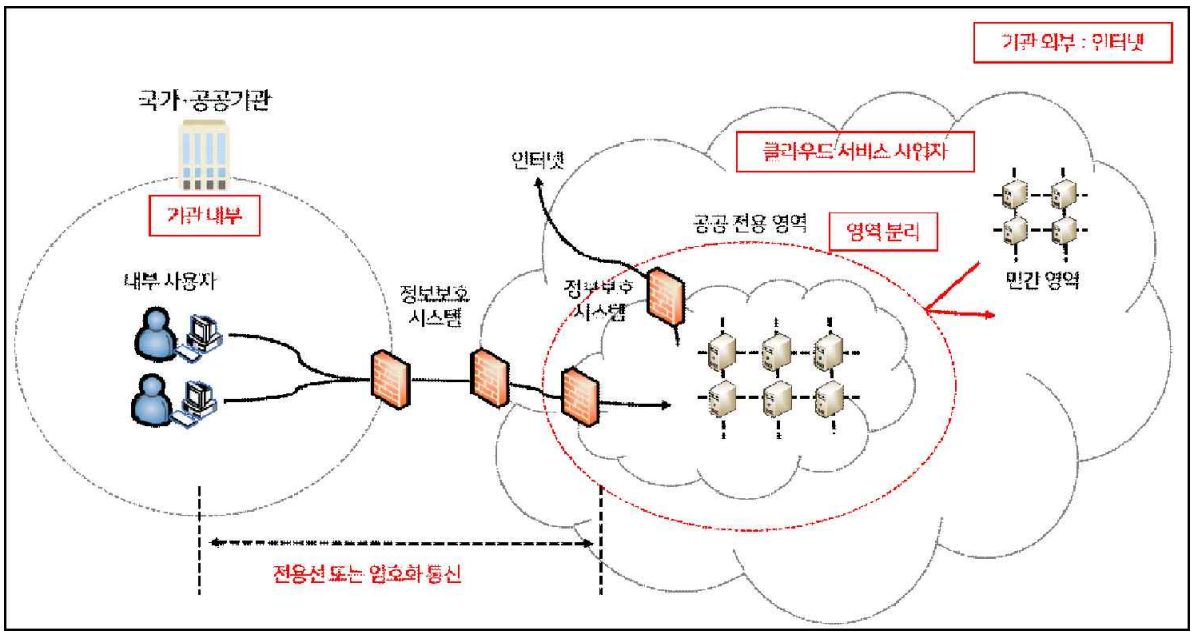
○ 네트워크는 대표기관 내부 또는 커뮤니티에 속한 특정기관 내부에 위치하여 커뮤니티 기관 시스템관리자가 직접 통제

○ 기관들 사이의 통신은 외부와는 분리된 네트워크를 이용하거나 전용선 또는 암호화 통신(VPN 등)

○ 커뮤니티 기관 자원 간 접근통제 적용

○ 기관 내부망과 커뮤니티 클라우드 망 사이에 정보보호 시스템 구축

3. 기관 이용 외주 클라우드



[그림 6] 기관 이용 외주 클라우드 구성도

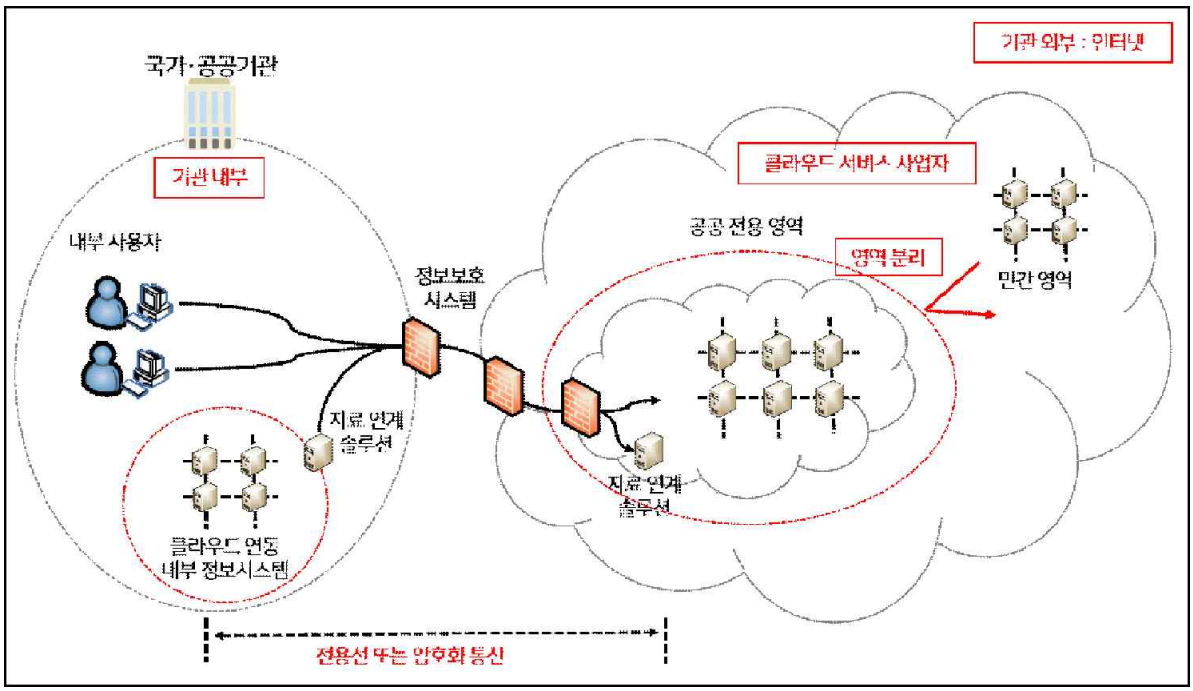
기관 중 규모가 작아 독자적인 클라우드 컴퓨팅 환경을 자체 구축하는 것이 비효율적이고 관리상 어려움이 있는 기관이 고려할 수 있는 유형이다. 이 유형은 기관의 IT 자원이 민간 사업자 네트워크 내부에 위치하며 민간 사업자가 통제함에 따라 기관의 직접 통제가 어렵다. 여기서 '외주(Out-sourced)'라 함은 민간 클라우드 컴퓨팅 사업자가 운영하는 것을 의미한다. 이 유형의 클라우드 구성도는 [그림 6]과 같다.

○ 공공영역은 민간영역과 분리된 형태로 구축(공공 전용 민간 클라우드)

○ 기관 내부와의 통신은 전용선 또는 암호화 통신(VPN 등)

○ 외부 인터넷 연결 구간 사이에 침입탐지시스템 등의 정보보호 시스템 마련

4. 하이브리드 클라우드



[그림 7] 하이브리드 클라우드 구성도

이 유형은 기관이 기존에 운영 중인 정보시스템을 유지하면서 클라우드 컴퓨팅의 장점을 활용하기 위한 유형이며 클라우드 구성도는 [그림 7]과 같다.

하이브리드 클라우드는 기관 망 내부에 위치해야 하는 보안 수준이 높은 데이터에 대하여 기관이 보안 통제권을 유지하면서도 클라우드 컴퓨팅 서비스를 활용하기 위하여 고안된 유형이다. 또한, 기관의 기존에 존재하는 IT 자원을 그대로 활용할 수 있으므로 비용 절감 측면에서도 효용성이 크다. 하지만 민간 사업자 네트워크 내부에 위치한 기관의 IT 자원에 대해서는 기관의 직접 통제가 어려운 문제가 있으며, 특히 이 유형을 내부 사용자들이 연계하여 사용하는 경우, 외부인에 의한 위험은 없으나 악의적 내부자 또는 민간 클라우드 내부로 부터의 위험은 존재한다. 또한, 정보시스템과의 연동 접점이 존재하기 때문에 클라우드 컴퓨팅 서비스에서 정보시스템으로 접근하는 지점에서의 높은 수준의 보안 통제 정책 적용이 필요하다.

기관 내부 사용자, 기존에 운영 중인 정보시스템과 클라우드 제공자 서비스 간의 통신은 전용선 또는 암호화 통신(VPN 등)을 이용해야 하며, 특히 기존 정보시스템과의 통신 시 보안 통제를 적용할 수 있는 보안 솔루션을 도입하여 정보시스템에 대해 보호를 해야 한다. 또한, 내부 중요 데이터가 이 접점을 통해 클라우드 컴퓨팅 서비스로 유출되는 것을 막기 위한 유출 방지 솔루션이 필요하다.

○ 공공영역은 민간영역과 분리된 형태로 구축

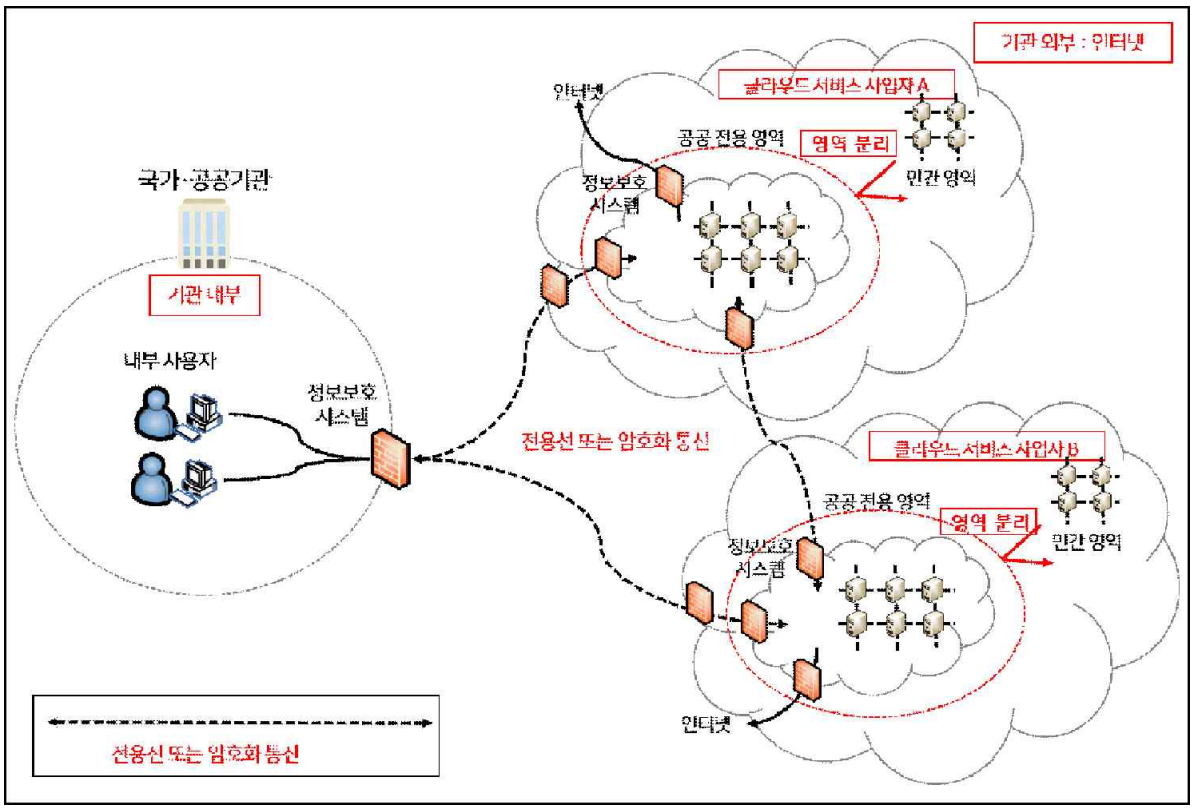
○ 기관 내부와의 통신은 전용선 또는 암호화 통신(VPN 등)

○ 기관 내부망과 민간 사업자 망 사이에 자료 교환을 위한 자료연계솔루션, 침입탐지 시스템 등 정보보호 시스템 구축

○ 기관 내부 정보시스템과 클라우드 컴퓨팅 서비스 간 자료 교환 등을 위한 자료연계 솔루션 구축

○ 하이브리드 클라우드 구축 기관은 기관 내부와 민간의 클라우드 영역에서 다른 기관과의 네트워크는 차단

5. 멀티 클라우드



[그림 8] 멀티 클라우드 구성도

이 유형은 기관이 다수의 외주 클라우드를 연계하여 활용하기 위한 유형이며 클라우드 구성도는 [그림 8]과 같다. 멀티 클라우드는 두 개 이상의 클라우드 서비스를 연계, 운용 및 관리하기 위한 기술로서, 다수의 클라우드 인프라(IaaS)를 연계한 멀티 클라우드 인프라에서 다수의 클라우드 서비스(PaaS, SaaS)들을 유연하게 운용할 수 있다. 멀티 클라우드를 구성하는 단위 클라우드 서비스의 사업자는 클라우드 간 연동을 위해 상호 운용성을 지원하는 API(Application Programming Interface) 등을 제공한다.

이 유형의 클라우드는 단일 클라우드 서비스를 활용하는 기관 이용 외주 클라우드와 비교하여 서비스 영역이 광범위한 특성이 있다. 멀티 클라우드를 구성하는 모든 단위 클라우드 서비스의 공공 영역은 민간 영역과 분리되어야 하며, 단위 클라우드 서비스 간 상호 연동 구간에 전용선 또는 암호화 통신을 적용하고 정보보호 시스템을 구축하는 등 보안대책을 수립해야 한다.

○ 공공영역은 민간영역과 분리된 형태로 구축

○ 기관 내부와의 통신은 전용선 또는 암호화 통신(VPN 등)

○ 외부 인터넷 연결 구간 사이에 침입탐지시스템 등의 정보보호 시스템 마련

○ 멀티 클라우드를 위한 외부 클라우드 서비스 간 통신은 전용선 또는 암호화 통신(VPN 등)

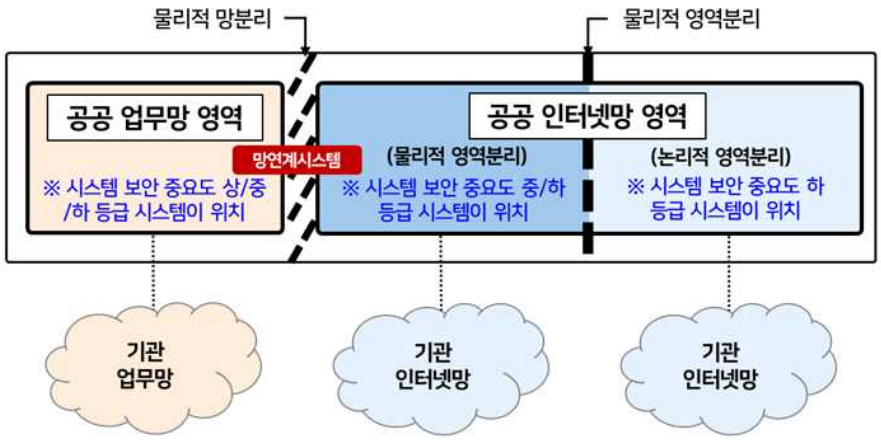
○ 멀티 클라우드를 위한 외부 클라우드 서비스 연결 구간에 침입탐지시스템 등의 정보보호 시스템 마련

제2절 클라우드 영역 분류

1. 클라우드 영역

국가・공공기관은 「국가 정보보안 기본지침」에 근거하여 중요자료의 외부 유출을 방지하기 위해 업무망(내부망)과 인터넷망(외부망)을 분리하여 운영하고 있다. 이는 인터넷을 통한 업무 관련 정보에 대한 접근을 차단하는 것으로서 안전한 업무환경 구축을 목적으로 한다. 각급기관의 업무망과 연동된 클라우드는 각급기관의 업무망으로 보며, 각급기관의 인터넷망과 연동된 클라우드는 각급기관의 인터넷망으로 보고 이에 따른 보안대책을 마련해야 한다 (「국가 정보보안 기본지침」 제41조 참조).

국가·공공기관이 업무망과 인터넷망에서 클라우드를 활용하기 위한 클라우드 영역은 다음과 같이 공공 업무망 영역, 공공 인터넷망 영역(물리적 영역 분리), 공공 인터넷망 영역(논리적 영역 분리)으로 분류한다. 국가·공공기관은 시스템 중요도 (상, 중, 하) 등급에 따라 클라우드 영역을 선택한다. 시스템 중요도 분류 절차는 본 가이드라인 제3장 제3절을 참조한다.



	공공 업무망 영역	공공 인터넷망 영역	
분리 방안	물리적 망분리	물리적 영역분리	논리적 영역분리
인터넷 연결	X	O	O
위치 가능한 시스템 보안 중요도 등급	上 / 中 / 下	中 / 下	下

[그림 9] 클라우드 영역 분류 개념

[그림 9]에서 물리적 망분리란 「국가 정보보안 기본지침」 제40조 및 「국가·공공기관 업무전산망 분리 및 자료전송 보안가이드라인」에 따른 물리적 망분리를 의미한다.

영역분리는 국가기관용 클라우드 컴퓨팅 서비스가 일반 이용자용 클라우드 컴퓨팅 서비스와 데이터 및 프로세스 등의 간섭없이 국가정보원 및 이용기관의 보안관제, 사고조사, 예방보안활동 유지를 위한 제반환경을 만족시킬 수 있는 보호조치를 말한다.

영역분리는 물리적 또는 논리적으로 수행할 수 있다. 시스템 중요도 상/중/하 등급에 적용되는 물리적 영역분리는 일반 이용자용 서비스 영역과 물리적으로 분리하여 구축한다. 논리적 영역분리는 하 등급만 허용되며 서버 가상화 및 네트워크 가상화 기술(하이퍼바이저, 네트워크 기능 가상화(NFV) 및 소프트웨어 정의 네트워크(SDN) 등)을 기반으로, 논리적으로 분리된 가상 네트워크상에 구성할 수 있다.

분류	특징
공공 업무망 영역	- 공공 업무망 영역은 다음과 같은 클라우드 센터에 위치 : 각급기관이 자체 구축·운영하는 클라우드 센터 : 통합관리기관이 운영하는 데이터센터 : 공공 업무망 전용 민간 사업자 클라우드 센터 - 각급 기관의 업무망과 연결하여 클라우드 서비스 제공하며 인터넷과의 접점 없음 - 민간 서비스 영역과 물리적 영역 분리가 되어 있으며 공공 인터넷망 영역과 물리적 망분리된 영역 - 단, 공공 인터넷망 영역과 자료 전송 체계 구축 운영 가능 - 영역 내부에서 기관 및 서비스별 분리 - 시스템 중요도 상/중/하 등급 위치 가능 - 국내 관리·운영

분류	특징
공공 인터넷망 영역 (물리적 영역분리)	- 물리적으로 영역분리된 공공 인터넷망 영역은 다음과 같은 클라우드 센터에 위치 : 각급기관이 자체 구축·운영하는 클라우드 센터 : 통합관리기관이 운영하는 데이터센터 : 공공 인터넷망 전용 민간 사업자 클라우드 센터 - 각급 기관의 인터넷망과 연결하여 클라우드 서비스 제공 - 민간 서비스 영역과 물리적 영역분리가 되어 있으며, 공공 업무망 영역과 물리적 망분리 된 영역 - 영역 내부에서 기관 및 서비스별 분리 - 시스템 중요도 중/하 등급 위치 가능 - 국내 관리·운영
공공 인터넷망 영역 (논리적 영역분리)	- 논리적으로 영역분리된 공공 인터넷망 영역은 다음과 같은 클라우드 센터에 위치 : 공공 인터넷망 전용 민간 사업자 클라우드 센터 - 각급 기관의 인터넷망과 연결하여 클라우드 서비스 제공 - 민간 서비스 영역과 논리적 영역분리 - 영역 내부에서 기관 및 서비스별 분리 - 시스템 중요도 하 등급 위치 가능 - 국내 관리·운영

[표 7] 클라우드 영역 분류

2. 클라우드 영역 기본원칙

가. 클라우드 영역의 공통 기본원칙

○ 클라우드 컴퓨팅 서비스를 운용하기 위한 모든 구성요소는 국내에 위치(데이터 서버, 관리·운영 서버, 인증서버, 로그 및 백업서버 등)

※ 대한민국의 배타적 법적관할하에 있는 시설에 위치해야 함

※ 해외에서의 공공용 민간 클라우드 영역에 대한 관리·운영 금지

○ 국내에 위치한 관리주체가 관리·운영을 수행

※ 클라우드 컴퓨팅 서비스 운영 및 관리 인력은 「국가 정보보안 기본지침」 제26조 2항에 따라 결격사유가 없는 인원

○ 클라우드 컴퓨팅 서비스 접속 및 데이터 암호화 시, 검증필 암호모듈(KCMVP) 활용

○ 클라우드 컴퓨팅 서비스 접속 시, 전용선 또는 암호화 통신(VPN 등)을 이용

○ 클라우드 컴퓨팅 서비스 접속/인증 시, 다중요소(Multi-factor) 인증방식을 적용

○ 클라우드 컴퓨팅 서비스 영역 내부에서 기관 및 서비스별 분리

○ 클라우드 컴퓨팅 서비스는 보안관제, 사고조사, 예방보안활동 등 국가정보원 및 이용기관의 사이버위협 대응활동 유지를 위한 제반환경을 만족

○ 백업·비상복구·변경관리·침해사고대응 등 클라우드 컴퓨팅 시스템 운영의 전반적인 절차에 관한 표준운영절차(SOP)를 수립

나. 클라우드 영역별 기본원칙

[공공 업무망 영역]

○ 각급기관이 자체 구축·운영하는 클라우드 센터, 통합관리기관이 구축·운영하는 데이터센터 또는 공공 업무망 전용 민간 사업자 클라우드 센터에 위치

○ 국가·공공기관용 클라우드 컴퓨팅 서비스의 물리자원(서버, 네트워크, 보안장비 등), 출입통제, 운영인력 등은 민간 이용자용 클라우드 컴퓨팅 서비스 영역과 분리 운영

○ 클라우드 컴퓨팅 서비스 운영 및 관리 인력은 국내에 거주하는 대한민국 국적을 가진 인원으로 구성

○ 공공 업무망 영역은 각급기관의 내부망과 연동된 내부망으로 간주하며 「국가정보보안 기본지침」 제40조(내부망·인터넷망 분리)를 준수

○ 공공 업무망 영역은 외부 인터넷과 연결 접점이 없으며, 내부 보안관제 정보는 기관 자체 보안관제체계와 연동하여 관리

○ 공공 업무망 영역과 공공 인터넷망 영역 간 자료전송이 필요한 경우, 망연계 및 일방향 전송 기능을 지원

○ 시스템 중요도 상/중/하 등급 위치 가능

[공공 인터넷망 영역 (물리적 영역분리)]

○ 각급기관이 자체 구축·운영하는 클라우드 센터, 통합관리기관이 구축·운영하는 데이터센터 또는 공공 인터넷망 전용 민간 사업자 클라우드 센터에 위치

○ 국가·공공기관용 클라우드 컴퓨팅 서비스의 물리자원(서버, 네트워크, 보안장비 등), 출입통제, 운영인력 등은 민간 이용자용 클라우드 컴퓨팅 서비스 영역과 분리 운영

○ 클라우드 컴퓨팅 서비스 운영 및 관리 인력은 국내에 거주하는 대한민국 국적을 가진 인원으로 구성

○ 기관의 보안관제 체계와 연동하도록 인터넷 접속 환경 구성 (공공 인터넷망 영역의 네트워크 트래픽이 기관의 보안관제 영역을 경유하거나, 공공 인터넷망 영역 보안관제 정보를 「사이버안보 업무규정」 제14조에 따른 정부보안관제체계와 연계하여 운영)

○ 시스템 중요도 중/하 등급 위치 가능

[공공 인터넷망 영역 (논리적 영역분리)]

○ 공공 인터넷망 전용 민간 사업자 클라우드센터에 위치

○ 국가·공공기관용 클라우드 컴퓨팅 서비스 영역과 민간 이용자용 클라우드 컴퓨팅 서비스 영역 간 논리적 영역분리를 수행

○ 클라우드 컴퓨팅 서비스 운영 및 관리 인력은 국내에 거주하는 인원으로 구성

○ 논리적으로 영역 분리를 하는 경우, 영역 분리를 훼손하여 데이터에 접근할 수 있는 취약점을 방지/완화/제거하고, 비인가 접근 모니터링 수행

○ 공공기관은 인터넷 연결시 기관의 기존 보안관제 체계와 연동하도록 구성 (공공영역 보안관제 정보를 「사이버안보 업무규정」 제14조에 따른 정부보안관제체계와 연계하여 운영)

○ 시스템 중요도 하 등급 위치 가능

제3절 시스템 중요도 분류 기준 및 절차

1. 시스템 중요도 분류 기준

국가·공공기관이 클라우드 컴퓨팅 서비스를 도입하고자 할 경우, 이용대상 시스템의 보안 중요도를 식별해야 한다. 시스템 중요도는 이용대상 시스템의 특성과 목적, 취급 정보의 중요도 및 파급영향, 기관의 특성 등을 고려하여 [표 8]과 같이 상, 중, 하 등급으로 분류한다. 각 분류 등급의 파급영향은 각 보안속성(기밀성, 무결성, 가용성)이 침해될 경우의 영향 수준을 종합적으로 고려해야 한다. 「보안업무규정」 제2조에 따른 비밀은 시스템 중요도 식별 대상에서 제외한다. 각 보안속성이 달성하고자 하는 보안 목표는 [표 9]와 같다.

분류 등급	세부사항		영역 분리
상	파급영향	- 해당 정보시스템에 대한 침해는 운영기관, 자산 및 개인에게 치명적 악영향을 미칠 수 있음	물리적 분리
	분류기준	- 국가 중대 이익(안보, 국가안전, 국방, 통일, 외교 등), 수사·재판 등 민감정보를 포함하거나 행정 내부 업무 등을 운영하는 시스템	
중	파급영향	- 해당 정보시스템에 대한 침해는 운영기관, 자산 및 개인에게 심각한 영향을 미칠 수 있음	물리적 분리
	분류기준	- 비공개 업무자료를 포함 또는 운영하는 시스템	
하	파급영향	- 해당 정보시스템에 대한 침해는 운영기관, 자산 및 개인에게 제한적인 영향을 미칠 수 있음	물리적 또는 논리적 분리
	분류기준	- 개인정보를 포함하지 않고 공개된 공공데이터를 포함 또는 운영하는 시스템	

* 행정 내부업무의 경우, 시스템 중요도를 고려하여 등급 조정 가능

[표 8] 시스템 중요도 분류 등급 및 세부사항

보안속성	보안 목표
기밀성	- 민감한 정보(국가 중대 이익과 관련된 정보 및 개인정보 등)를 보호하기 위해 해당 정보에 대한 비인가 접근과 유출을 차단
무결성	- 취급 정보에 대해 허가되지 않은 변경 또는 삭제를 방지
가용성	- 취급 정보에 대한 안정적인 접근과 원활한 사용을 보장

[표 9] 보안속성별 보안 목표

2. 시스템 중요도 및 영역 분류 절차

수행 절차	단계별 고려사항
① 이용 대상 시스템 식별	- 클라우드 컴퓨팅 서비스 이용대상 시스템을 식별 - 시스템 특성, 목적과 활용방식을 확인 (타 시스템 연계 여부 반드시 확인)
② 취급 정보유형 식별	- 이용 대상 시스템이 취급하는 정보유형을 식별 - 국가 중대 이익과 관련된 정보, 행정 내부업무 정보 등 민감한 정보를 취급하는지 반드시 확인
③ 시스템 중요도 등급 선정	- 시스템 목적, 기관 특성, 시스템이 침해되었을 경우의 파급 영향 등을 종합적으로 고려하여 시스템 중요도 등급을 선정 (기밀성, 무결성 및 가용성에 대한 영향과 위험도를 고려)
④ 클라우드 영역 선정	- 시스템 중요도 등급에 따라, 시스템을 운용할 클라우드 영역 선정 (공공업무망, 물리적 영역분리된 공공 인터넷망 및 논리적 영역분리된 공공 인터넷망 영역 중 선택)

[표 10] 시스템 중요도 및 영역 분류 절차

시스템 중요도 분류 절차는 ① 이용 대상 시스템 식별, ② 취급 정보유형 식별, ③ 시스템 중요도 등급 선정 및 ④ 클라우드 영역 선정의 단계를 갖는다. 각 단계별 고려사항은 [표 10]과 같다. 첫 번째 단계에서, 「국가 정보보안 기본지침」 제2조에 따른 도입기관의 정보보안담당관은 시스템의 특성, 목적 및 활용방식 등을 [표 11]의 시스템 중요도 분류 체크리스트에 기술한다. 또한 시스템이 기 구축된 내·외부 정보시스템 또는 민간 클라우드 컴퓨팅 서비스와 연계하여 동작하는 경우 해당 사항을 '시스템 설명' 란에 반드시 기록한다.

두 번째 단계에서, 정보보안담당관은 대상 시스템이 취급하는 정보유형을 식별하여 시스템 중요도 분류 체크리스트를 작성한다. 이 때, '취급 정보유형 확인'의 비고란을 참고하여 시스템 중요도 등급 선정에 반영한다.

세 번째 단계에서, 정보보안담당관은 대상 시스템 침해 시 보안 영향(기밀성, 무결성 및 가용성 훼손 시 영향)을 검토하고 상기 사항들을 종합적으로 고려하여 시스템 중요도 등급을 결정한다.

네 번째 단계에서, 정보보안담당관은 분류된 시스템 중요도 등급에 따라 대상 시스템을 운용할 클라우드 영역을 선정한다. (영역별 특성과 보안원칙은 제3장 제2절 참조) 이 때, '시스템 기본정보 확인'의 비고란을 참고하여 클라우드 영역 선정에 반영한다. 작성된 체크리스트는 보안성 검토 단계에서 확인한다. 보안성 검토를 포함한 전반적인 클라우드 컴퓨팅 서비스 도입 절차는 본 가이드라인 제3장 제5절을 참조한다.

시스템 중요도 분류 체크리스트

기관명	시스템 명칭

시스템 설명

*(*시스템의 특성, 목적 및 활용방식 등을 간략하게 기술, 타 시스템 연계 여부 및 연계 방식을 반드시 포함)*
- 국가 중대 이익(안보, 국가안전, 국방, 통일, 외교 등), 수사·재판 등 민감정보를 포함하거나 행정 내부 업무 등을 운영하는 시스템

취급 정보유형 확인		비고
- 국가 중대 이익에 관련된 정보 및 기관의 민감한 정보를 취급하는가?	☐	*해당 사항이 하나라도 체크된 경우 (상) 등급 *행정 내부업무의 경우, 시스템 중요도를 고려하여 등급 조정가능
- 국가·국민 안전과 관련된 정보를 취급하는가?	☐	
- 중앙행정기관 및 지자체의 행정 내부업무 정보를 취급하는가?	☐	
- 실시간 소통, 일정 공유, 전자메일 등 협업과 관련된 정보를 취급하는가?	☐	*해당 사항이 하나라도 체크된 경우 (중) 등급 이상
- 공공기관의 내부 업무 정보를 취급하는가?	☐	
- 개인정보를 취급하는가?	☐	
- 각급 기관의 교육과 관련된 정보를 취급하는가? (개인정보 및 비공개 자료를 포함하지 않는 경우)	☐	*해당 사항이 하나라도 체크된 경우 (하) 등급 이상
- 대민 서비스와 관련된 정보를 취급하는가? (개인정보 및 비공개 자료를 포함하지 않는 경우)	☐	

기타 취급 정보유형

*(*상기 유형 이외에 시스템이 취급하는 정보유형을 명시)*

침해 시 보안영향 수준		
- 국가, 기관 및 국민의 이익, 권리, 자산, 안전 또는 업무수행의 공정성 등에 치명적인 악영향을 미치는가?	☐	*해당 사항이 체크된 경우 (상) 등급 이상
- 국민 생활에 심각한 영향을 미치는가? (국민 생활 불편 초래 등)	☐	*해당 사항이 체크된 경우 (중) 등급 이상

기밀성 훼손 시 영향	무결성 훼손 시 영향	가용성 훼손 시 영향
상 / 중 / 하	상 / 중 / 하	상 / 중 / 하
*(*대상시스템의 기밀성이 훼손되었을 경우의 영향을 간략하게 기술)* *예 :* *(상) XXX 정보유출 시 치명적 악영향 발생* *(중) XXX 정보유출 시 심각한 영향 발생* *(하) XXX 정보유출 시 제한적 영향 발생*	*(*대상시스템의 무결성이 훼손되었을 경우의 영향을 간략하게 기술)* *예 :* *(상) XXX 정보훼손 시 치명적 악영향 발생* *(중) XXX 정보훼손 시 심각한 영향 발생* *(하) XXX 정보훼손 시 제한적 영향 발생*	*(*대상시스템의 가용성이 훼손되었을 경우의 영향을 간략하게 기술)* *예 :* *(상) 서비스 중단 시 치명적 악영향 발생* *(중) 서비스 중단 시 심각한 영향 발생* *(하) 서비스 중단 시 제한적 영향 발생*

시스템 중요도 등급 분류	☐ 상	☐ 중	☐ 하

('침해 시 보안영향 수준'의 기밀성/무결성/가용성 훼손 시 영향(상/중/하) 중에서 가장 높게 체크된 수준에 따라 시스템 중요도 등급을 선정, 단 기관 담당자의 판단에 따라 조정 가능하되, 이를 위한 보안대책과 조정 및 선정 사유를 기술)*

*********** 참고사항 ***********
- *공공 업무망 영역에서 시스템 중요도 (상), (중), (하) 등급 시스템 운용 가능*
- *공공 인터넷망 영역(물리적 영역분리)에서 시스템 중요도 (중), (하) 등급 시스템 운용 가능*
- *공공 인터넷망 영역(논리적 영역분리)에서 시스템 중요도 (하) 등급 시스템만 운용 가능*

시스템 기본정보 확인		비고
- 망 분리 기관의 업무망과 연동하는 시스템인가?	☐	*공공 업무망 영역에서 운용
- 인터넷 연결이 필요한 시스템인가?	☐	*공공 인터넷망 영역에서 운용

클라우드 영역 분류	☐ 공공 업무망 영역	☐ 공공 인터넷망 영역 (물리적 영역분리)	☐ 공공 인터넷망 영역 (논리적 영역분리)

*(*시스템 운용 영역 선정 사유를 기술, 영역 간 연계가 필요할 경우 망연계시스템 활용 등 보안대책을 기술)*

*********** 참고사항 ***********
- *공공 업무망 영역: 업무망과 인터넷망의 물리적 망분리 정책에 따라 구성 (인터넷 접점이 없는 망분리 영역)*
- *공공 인터넷망 영역(물리적 영역분리): 업무망과 인터넷망의 물리적 망분리 정책에 따라 구성, 일반 이용자 영역과 물리적 영역분리*
- *공공 인터넷망 영역(논리적 영역분리): 일반 이용자 영역과 논리적으로 영역분리된 클라우드*

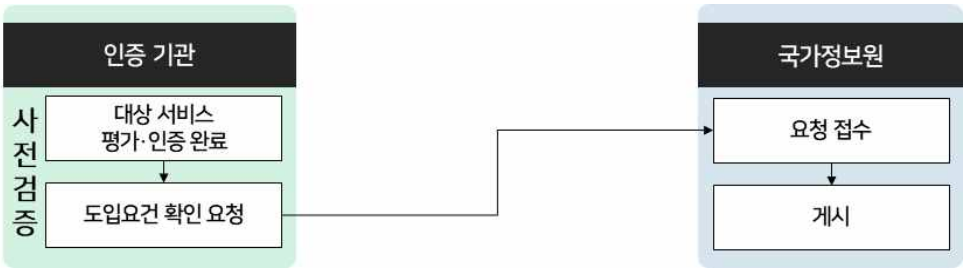
정보보안담당관	년 월 일	성명:	(서명)

[표 11] 시스템 중요도 분류 체크리스트

제4절 클라우드 컴퓨팅 서비스 도입요건

국가·공공기관이 시스템 중요도 및 영역 분류를 완료하면 클라우드 컴퓨팅 서비스 도입요건을 만족하는 클라우드를 도입할 수 있다. 클라우드 컴퓨팅 서비스 도입요건 확인은 국가·공공기관의 안전한 클라우드 컴퓨팅 활용을 위해 「국가 정보보안 기본지침」 및 「국가 클라우드 컴퓨팅 보안 가이드라인」에 따라, 각급기관이 도입하는 클라우드 컴퓨팅 서비스의 국가정보원 보안기준 만족 여부를 검토한다.

클라우드 컴퓨팅 서비스 도입요건 확인은 요청 주체에 따라 두 가지 분류를 갖는다. 첫 번째로, 관계법령에 따른 인증기관이 클라우드 컴퓨팅 서비스 인증·평가를 완료하고 국가정보원에 민간 클라우드 컴퓨팅 서비스 도입요건 확인을 요청 할 수 있다(사전검증 : 이용기관에 도입 · 구축되기전 서비스 자체에 대한 보안기준 적합여부를 확인). 인증기관이 도입요건 확인 요청시 국가정보원 보안기준을 만족하는 평가기준에 따라 인증을 수행했다는 증빙서류(인증서 등)를 제출하면 국가정보원은 추가 절차 없이 바로 국가정보원 국가사이버안보센터 홈페이지에 게시한다.

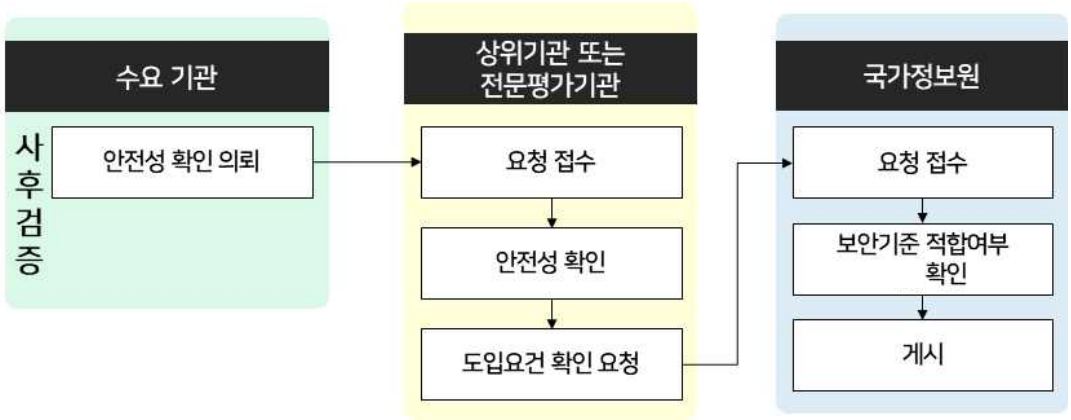


[그림 10] 사전검증을 통한 클라우드 컴퓨팅 서비스 도입요건 확인

구분	내용
사전검증	- 관계법령에 따른 인증기관(CSAP 인증기관 등)에 의해 인증 · 평가받은 클라우드 컴퓨팅 서비스 - 인증기관이 증빙서류(인증서 등)를 준비, 국가정보원에 도입요건 확인 요청 - 요청 접수 및 게시(국가정보원)
사후검증	- 국가정보원장과 사전협의 하에 수요기관이 안전성 확인을 완료한 클라우드 컴퓨팅 서비스 - 이 때, 안전성 확인은 상급기관 또는 전문평가기관에 요청 - 상급기관 또는 전문평가기관은 국가정보원 보안기준에 따라 안전성 확인 - 국가정보원에 적합여부 및 도입요건 확인 요청 - 요청 접수 및 검토(보안기준 적합여부 이행 확인) 후 게시(국가정보원)

[표 12] 사전검증와 사후검증

두 번째로, 수요기관이 대상 서비스의 안전성을 확인하고 국가정보원에 도입요건 확인을 요청 할 수 있다(사후검증 : 수요기관에 도입 · 구축 완료 후 운용전 보안기준 적합여부를 확인). 사후검증에서 수요기관은 상급기관 또는 전문평가기관에게 안전성 확인을 의뢰한다. 국가정보원의 보안기준에 따라 안전성 확인을 완료한 상급기관 또는 전문평가기관은 국가정보원에 대상 서비스의 도입요건 확인을 요청한다. 국가정보원은 보안기준 적합여부에 대한 확인 절차를 수행하며 적합여부 확인이 완료되면 국가정보원 국가사이버안보센터 홈페이지에 게시한다.



국가정보원의 보안기준 미 준수, 사고조사·예방보안활동 비협조 등 심각한 부적합 사유 발생 시 홈페이지 게시를 취소하거나 부적합 사유 개선 시까지 홈페이지 게시를 유보할 수 있다. 클라우드 컴퓨팅 서비스 도입요건 확인과 관련하여 상세한 내용은 국가정보원 국가사이버안보센터 홈페이지(ncsc.go.kr)를 참조한다.

【 도입 · 운영시 유의사항 】

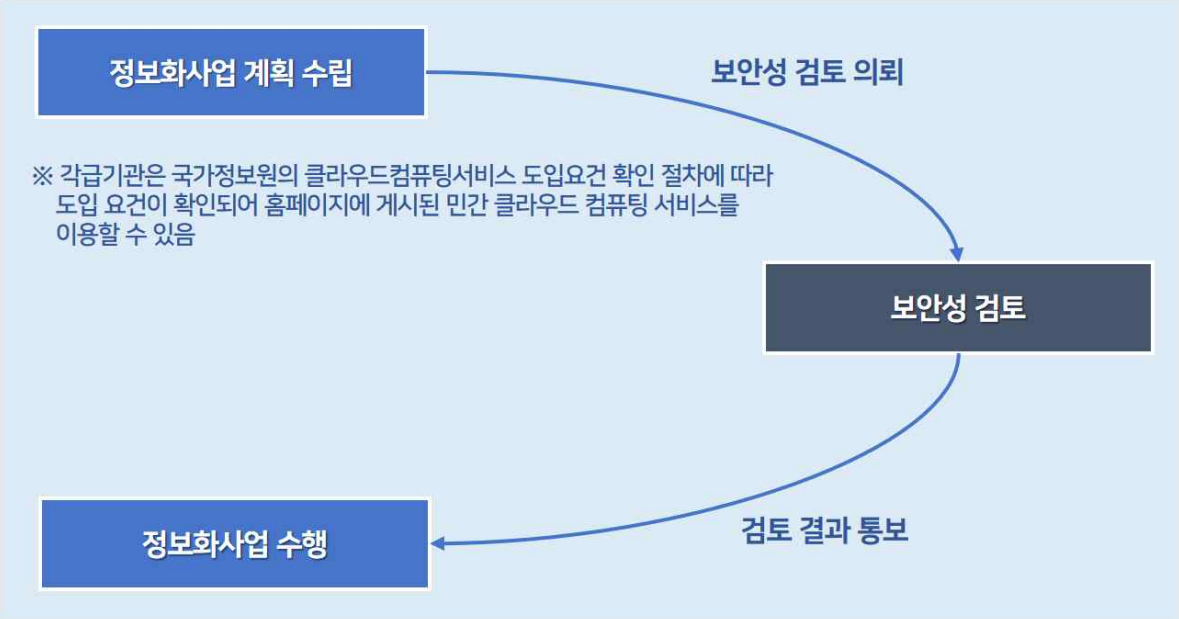
① 국가·공공기관은 '도입요건 확인'이 완료되어 국가정보원 홈페이지에 게시된 클라우드 컴퓨팅 서비스를 이용하는 것을 원칙으로 함

② 국가정보원 국가사이버안보센터 홈페이지에 미게시 클라우드 컴퓨팅 서비스를 이용해야 하는 특별한 사유가 발생한 경우에는 다음의 절차를 수행

- 클라우드 컴퓨팅 서비스 사업자에게 관계법령에 따른 인증기관에서 인증 · 평가를 받고 국가정보원 국가사이버안보센터 홈페이지에 게시되도록 요구하거나
- 수요기관이 직접 사후검증 절차를 통해 '도입요건 확인' 절차를 수행하고 국가정보원 국가사이버안보센터 홈페이지에 게시되도록 진행

③ 이용기관은 도입 완료 후에도 보안관제 · 사고조사 · 예방보안 등 사이버위협 대응 활동을 수행해야 하며 국가정보원의 보안기준 만족 여부가 유지되는지 등을 확인하고 적절한 조치를 취해야 함

제5절 클라우드 컴퓨팅 도입절차



[그림 12] 클라우드 컴퓨팅 도입 절차

국가·공공기관은 기관의 클라우드 사용목적 및 요구사항에 따라 국가·공공기관은 정보화 사업 계획을 수립하고, 국가정보원의 보안성 검토 과정을 거쳐 클라우드 컴퓨팅을 도입해야 한다. 또한, 각급기관이 민간 클라우드 컴퓨팅 서비스를 도입하고자 할 경우에는 본 가이드라인에 따른 이용 절차와 보안기준 등을 확인하고 본 가이드라인 제3장 제4절에 소개된 클라우드 컴퓨팅 서비스 도입요건 확인 절차에 따라 확인이 완료된 서비스를 도입할 수 있다 (보안성 검토 필수). 또한 민간 클라우드 컴퓨팅 서비스 사업자와 계약 시 해킹사고, 장애대응 및 재발방지 등에 필요한 조치를 위해 국가정보원 및 이용기관의 보안관제 및 사고조사, 예방보안활동 등에 적극 협조하도록 하는 내용을 명시하여야 한다.

1. 정보화사업 계획 수립

○ 투입이 예상되는 자료·장비 가운데, 보안관리가 필요한 사항에 대한 보안요구 사항을 마련하여 정보화사업 계획서(안)에 반영

- 도입하고자 하는 IT 자원의 사용 목적, 보안성, 성능, 비용 등 요구사항 및 기술을 분석
- 인터넷 연결 클라우드 환경을 통한 업무망 데이터 유출 방지 방안

- 업무망 환경과 인터넷 연결 클라우드 환경 간의 물리적/논리적 분리

- 외부에 위치한 민간 사업자 측 데이터센터를 이용하는 경우 국가·공공기관 클라우드 영역과 민간 클라우드 영역을 물리적/논리적으로 영역 분리하여 구축(공공전용 민간클라우드)

○ 정보화사업 계획 수립 단계에서 보안 요구사항을 도출하여 자체 보안대책을 수립하여야 하고 보안심사위원회의 심사를 거쳐야 함

○ 각급 기관의 장은 정보화사업 계획 수립 단계에서 「공공기록물 관리에 관한 법률」, 「개인정보 보호법」, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 등을 참고하여 클라우드 컴퓨팅 도입 유형을 결정하여야 함

○ 도입 대상 시스템에 대해 본 가이드라인 제3장 제3절의 시스템 중요도 분류를 수행하고, 제3장 제2절의 클라우드 영역별 기본원칙, 제4장 클라우드 컴퓨팅 보안기준 준수 방안을 수립하여 보안성 검토를 의뢰해야 함

※ 시스템 중요도에 따른 필수/권고 항목은 [부록 4] 클라우드 컴퓨팅 보안기준 체크리스트 참고

2. 보안성 검토

○ 클라우드 컴퓨팅 도입에 관한 정보화 사업 계획서(안)을 국가 정보보안 기본지침에 따라 보안대책의 적절성을 평가하는 보안성 검토를 받아야 함

※ 전자정부법 제56조 및 동법 시행령 제69조, 사이버안보 업무규정 제9조

※ 「국가 정보보안 기본지침」의 <정보화사업 단계별 보안조치 사항(요약)>을 참고하여 관련 절차 준수

○ 「국가 정보보안 기본지침」등에 명시되어 있는 보안 요구사항과 본 가이드라인에서 제시하고 있는 보안 기준을 정보화사업 계획에 반영, 보안성 검토 수행

※ 본 가이드라인에 따라 작성한 시스템 중요도 분류 체크리스트와 클라우드 영역별 보안 기본 원칙을 준수하기 위한 보안대책을 반드시 작성하여 제출 (세부사항은 본 가이드라인 '제3장 제2절 클라우드 영역 분류' 및 '제3장 제3절 시스템 중요도 분류 절차'의 내용 참조)

3. 정보화사업 수행

○ 정보화사업 수행 상 보안 관리는 「사이버안보 업무규정」, 「보안업무규정」, 「보안업무규정 시행규칙」, 「국가 정보보안 기본지침」, 「개인정보 보호법」, 각 행정기관의 「정보보안 기본지침」 등에 따라 시행

※ 국가정보원장은 클라우드 서비스의 도입·운영에 있어서 본 가이드라인의 보안 기준과 관련된 중대한 위반 사항을 발견할 경우, 각급기관의 장에게 해당 서비스의 운용 및 활용 중지를 요청할 수 있음 (민간 클라우드 컴퓨팅 서비스 포함)

※ 수행업체 대표자명의 확인서, 참여인력 서약서, 보안확약서(대표자용, 참여인력용), 정보보안 각서를 클라우드서비스 보안인증제를 통해 징구할 수 있음

○ 참여 인원 신원 확인, 보안서약서 징구, 보안교육 실시, 참여 인원 보안점검 실시를 통한 보안관리 수행

○ 사업 수행 장소는 CCTV, 시건장치 등 비인가자 출입통제 대책 마련된 공간을 사용하고 정기적인 보안점검을 수행

○ 사업 수행에 필요한 자료 및 장비에 대한 반입·출입 통제 수행

○ 사업 완료 시 제공된 사업과 관련된 제반자료에 대한 전량 회수 및 노트북·보조기억매체의 전자기록 자료 삭제 조치를 하고, 보안확약서 작성 및 제출을 받아야 함

제4장
클라우드 컴퓨팅 보안기준

국가·공공기관 클라우드 도입과 운영 상 보안 관리는 기존 국가·공공기관 정보시스템 보안관리 체계 위에서 이루어져야 한다. 그러므로 본 가이드라인은 기존 국가·공공기관 정보시스템 보안관리 체계와의 연속성 유지를 위하여 「전자정부법」 및 동법 시행령, 사이버안보 업무규정(대통령령), 「국가 정보보안 기본지침」, 「보안업무규정」(대통령령), 「정보 및 보안업무 기획·조정규정」(대통령령), 「국가사이버안전관리규정」(대통령훈령), 「정보통신기반보호법」과 동법 시행령, 「공공기록물 관리에 관한 법률 시행령」, 「국가·공공기관 용역업체 보안관리 가이드라인」, 「네트워크 구축 가이드라인」 등을 준용하는 국가·공공기관 클라우드 도입 보안체계 [그림 13]에 따라 국가 정보보안을 위하여 클라우드 컴퓨팅 도입 시 각급기관이 수행하여야 할 클라우드 컴퓨팅 보안기준을 제시한다.

[그림 13] 국가·공공기관 클라우드 컴퓨팅 도입 보안체계

클라우드 컴퓨팅 도입 보안기준은 기관 자체 클라우드 컴퓨팅 구축 보안기준, 민간 클라우드 컴퓨팅 서비스 이용 시 준수하여야 할 보안기준으로 구분하고 각각의 보안 기본원칙과 보안 기준으로 구성되어 있다. 보안 기본원칙은 기존 국가·공공기관 정보시스템 보안관리 체계와의 연속성 유지를 위해 마련되었으며, 국가·공공기관은 이러한 원칙 아래에서 클라우드 컴퓨팅 설계를 하여야 한다. 보안 기준은 보안 기본원칙에 대한 세부사항들을 담고 있으며, 클라우드 컴퓨팅 환경 구성요소(정책, 클라우드 인프라, 가상 환경, 데이터, 인증 및 권한, 사고 및 장애 대응) 별로 고려해야 할 보안기준을 포함하고 있다.

제1절 기관 자체 클라우드 컴퓨팅 구축 보안기준

1. 보안 기본원칙

기관 자체 클라우드 컴퓨팅 구축은 기관에서 자체적으로 클라우드 컴퓨팅 시스템을 구축하여 직접 클라우드 자원에 대한 통제권을 갖는 형태로 기존 정보시스템의 보안 통제 수준을 클라우드 컴퓨팅 환경에서도 그대로 유지할 수 있다. 하지만 클라우드 컴퓨팅 특성으로 인하여 발생할 수 있는 보안 위협이 존재하기 때문에 이에 대한 보안 관리 방안을 마련하여 구축을 하여야 한다. 특히, 가상화된 자원에 대한 사용자 간 공유로 발생할 수 있는 보안 위협을 식별하고, 대응 및 관리 방안을 고려해야 한다.

이에 본 가이드라인은 기존 국가·공공기관 정보시스템 보안관리 체계 연속성 유지 및 클라우드 컴퓨팅 특성에 따른 보안위협 대응 목적을 가지고, 기술적·정책적 측면 보안 기본원칙을 마련하였으며, 국가·공공기관은 보안 기본원칙에 기반을 두고 기관 구축 클라우드 컴퓨팅을 설계해야 한다. 보안 기본원칙은 모든 클라우드 컴퓨팅 서비스 유형에 공통적으로 적용해야 하는 원칙, IaaS 환경 및 SaaS 환경에 추가적으로 요구되는 원칙을 포함한다. 또한 PaaS 환경의 경우 SaaS 환경과 동일한 원칙을 준용한다.

가. 정책적 측면에서의 기본원칙

[공통 기본원칙]

① 클라우드 컴퓨팅 서비스를 이용하려는 국가·공공기관은 본 가이드라인에 따라 이용 대상에 대한 시스템 중요도 등급 분류 및 클라우드 영역 분류를 수행하고 관련 보안기준을 사전 확인하여야 함

- '제3장 제2절 국가·공공기관 활용 클라우드 영역 분류' 및 '제3장 제3절 시스템 중요도 분류 기준 및 절차'의 내용 참조

② (도입 정보보호시스템 안전성 확인) 클라우드 컴퓨팅 서비스 구축을 위해 도입되는 보안 기능을 가진 정보통신제품 중에서 전자정부법 제56조에 규정된 전자문서의 위조, 변조, 훼손 또는 유출을 방지하기 위한 목적으로 도입하는 제품은 국가정보원장이 안전성을 확인한 제품을 사용하여야 함

※ 기타 세부사항은 국가정보원의 보안적합성 검증제도에 따름

※ 클라우드 인프라에서 중대한 보안 취약점이 발견되어 긴급한 보안패치 등이 필요한 경우 유관기관 협의 하에 인증 요건을 유예할 수 있음

③ (인터넷 · 업무망 분리) 망 분리기관에서는 인터넷이 연결된 가상환경에서 업무 관련 데이터 처리를 하지 못하며, 망 미분리 기관은 인터넷과 업무 영역 간 자료 교환이 되지 않도록 기술적 통제대책을 구현하여 업무 관련 데이터 처리를 하여야 한다.

④ (공급망 관리) 공급망 위험식별, 변경관리 및 모니터링을 포함하는 공급망 관리 정책 및 체계가 마련되어야 함

[SaaS 환경 추가 기본원칙]

⑤ 국가·공공기관에서 사용되는 SaaS 구축 시 필요한 애플리케이션은 「행정기관 및 공공기관 정보시스템 구축·운영 지침」 및 「소프트웨어 개발보안 가이드」에 따라, 소프트웨어 개발단계부터 보안 취약점의 원인인 보안 약점을 배제하여 개발되어야 함

⑥ SaaS 클라우드 인프라, 개발·운영 환경의 물리적 위치는 국내로 한정되어야 하며, SaaS에서 처리되는 데이터에 대한 물리적 위치도 국내로 한정됨

※ 민간 클라우드 인프라에 자체 구축 시 이용 기관용 SaaS 관리 데이터(소스코드, 설정 파일, 로그, 사용자 계정 정보 등), 운영인력 등은 민간 사용자 영역과 분리되어 국내에 위치하여야 함

⑦ SaaS를 제공하기 위한 SaaS 개발·운영 환경, 클라우드 인프라 환경에 대한 보안성을 확인하여야 함

⑧ SaaS 개발·운영 환경은 SaaS 서비스 가용성을 보장할 수 있어야 하며, 사고 및 장애에 대응할 수 있는 체계가 마련되어야 함

⑨ SaaS는 허가받은 외부 연동 서비스(스토리지, 데이터베이스, 빅데이터 처리 등)와 연계되어야 함

나. 기술적 측면에서의 기본원칙

[공통 기본원칙]

⑩ (내부 업무용 영역과 외부 공개용 클라우드 컴퓨팅 서비스 사용영역의 분리) 업무포털, 그룹웨어 등 비공개 업무 용도로 쓰이는 클라우드 영역과 대민서비스, 인터넷 홈페이지 등 외부 공개용 클라우드 컴퓨팅 서비스를 사용 및 관리하기 위한 영역은 분리되어 운영되어야 한다.

⑪ 중요장비 이중화 및 백업체계를 구축, 표준운영절차를 수립하여야 한다.

- 클라우드 컴퓨팅은 중요 시스템들이 중앙집중식으로 구성되어 장애발생시 모든 업무가 마비될 수 있으므로 네트워크 스위치, 스토리지, 가상머신 등 중요자산을 이중화하고 클라우드 컴퓨팅 서비스의 가용성을 보장하기 위해 백업체계를 구축
- 백업·비상복구·변경관리·침해사고대응 등 클라우드 컴퓨팅 서비스 운영의 전반적인 절차에 관한 표준운영절차(SOP[2]) 등을 수립

⑫ 관리자 및 이용자에 대한 접근통제 및 격리 수단을 확보하여야 한다.

- 관리자가 이용자에 할당된 자원(메모리·HDD 등)에 임의 접근하지 못하도록 접근제어 및 격리 등을 통한 기술적 통제 수단을 마련
- 이용자가 본인에게 할당된 자원 이외의 자원에 접근하지 못하도록 기술적 통제 수단 마련(비정상 통신경로 발생 차단 등)

⑬ 클라우드에 저장 및 송수신되는 중요 업무자료를 암호화하여야 한다.

- 해킹 및 비인가자에 의해 스토리지에 저장된 중요 업무자료 절취 시, 열람·실행이 불가토록 데이터를 암호화
- 해킹 및 비인가자에 의해 중요 업무자료 송수신 과정에서 스니핑 등의 공격으로 탈취 시, 열람·실행이 불가토록 송수신 자료의 암호화
- 저장 및 송수신되는 중요 업무자료를 암호화하기 위해 가상사설망·호스트 자료유출 방지 제품 등 정보보호 제품을 도입할 경우는 검증필 암호모듈 탑재제품 이용(「국가 정보보안 기본지침」 검증필 암호모듈 목록 및 운용관리 참조)

2) SOP : Standard Operating Procedure

⑭ 클라우드 컴퓨팅 서비스에 대한 보안관제를 수행하여야 한다.

- 클라우드 컴퓨팅 서비스의 해킹 탐지를 위한 보안관제 및 대응 체계를 마련해야 함
- 자체 구축한 클라우드에 탑재된 정보시스템에 대하여 해킹탐지 및 대응체계 마련을 위해 클라우드 환경에 적합한 보안관제 시스템 구축하고 이에 대한 직접 보안관제를 수행하여야 함
- 다른 기관이 운영하는 보안관제시스템을 활용하는 것이 더 효율적인 경우에는 「국가사이버안전관리규정」 제10조의2에 따라 다른 기관의 보안관제센터에 위탁 가능
- 책임있는 보안관제 업무 수행 및 관리 등을 위해 보안관제에 필요한 전담 직원을 상시 배치해야 하며, 필요시 「국가사이버안전관리규정」 제10조의2 제4항에 따라 보안관제전문업체의 인원을 파견받아 보안관제 업무 수행
- 클라우드에 구축된 보안관제 시스템은 정부보안관제체계와 연계되어야 하며, 세부사항은 국가정보원의 클라우드 보안관제 관련 별도 가이드라인(2023년 상반기 발간 예정)준용

[SaaS 환경 추가 기본원칙]

⑮ 외부 공개용 SaaS 영역은 내부 업무용 SaaS 영역과 분리되어야 한다.

- 외부 공개용 SaaS 가상머신은 DMZ 영역 내에 위치
- 외부 공개용 SaaS 영역과 내부 업무용 SaaS 영역 간에 접근통제 수단을 마련

⑯ SaaS 애플리케이션 보안성 강화 방안을 마련하여야 한다.

- SaaS 애플리케이션을 공유하는 다수의 사용자 간 자원 격리 방안 마련
- SaaS 애플리케이션 개발 및 운영 시 인터페이스 및 API의 취약점에 대한 주기적인 검증 수행
- SaaS 애플리케이션 설계 및 개발 단계에서 취약점을 제거하고 SaaS 운영 중에도 주기적으로 취약점 제거를 수행하여야 함
- SaaS 애플리케이션 접근을 위한 네트워크 프로토콜 보호 방안 마련
- SaaS 애플리케이션 관련 데이터(소스코드, 설정파일, 로그 정보 등)에 대한 보호 방안 마련

2. 세부 보안기준

기관이 자체적으로 클라우드 컴퓨팅 서비스를 안전하게 도입하기 위한 세부 보안기준은 [표 13]과 같다. 정책, 클라우드 인프라, 가상환경 보안, 데이터, 인증 및 권한, 사고 및 장애 대응 영역에 대한 총 16개의 세부 보안기준이 있으며, 모든 유형의 클라우드 컴퓨팅 서비스에 적용해야 하는 공통 보안기준, IaaS 및 SaaS 환경에서 요구되는 추가 보안 기준을 포함한다. 또한 PaaS 환경의 경우 SaaS 환경과 동일한 기준을 준용한다.

분류	세부 보안기준	적용범위		
		공통 보안기준	IaaS 추가 보안기준	SaaS 추가 보안기준
정책 (3)	시스템 보호	√	√	-
	인적 관리	√	-	-
	보안 감사	-	√	-
클라우드 인프라 (1)	가상화 인프라	√	√	-
가상환경 보안 (6)	보안 관리	√	√	-
	보안 관리 - SaaS 어플리케이션 개발	-	-	√
	보안 관리 - 개발·운영 환경	-	-	√
	악성코드 방지	√	-	-
	접근 통제	√	-	-
데이터 (2)	관리	√	-	√
	암호화	√	-	-
인증 및 권한 (2)	인증	√	-	-
	권한	√	-	-
사고 및 장애대응 (2)	사고	√	-	-
	장애	√	-	-

[표 13] 기관 구축 클라우드 컴퓨팅 보안기준 분류

가. 정책

(1) 시스템 보호

[공통 보안기준]

① (보안 요구사항 정의) 클라우드 컴퓨팅 서비스 도입 시 관련 법률 및 지침, 보안 체계, 도입 기관 보안 사항 등을 참고하여 다음과 같은 내용이 포함되도록 보안 요구사항을 정의하여야 한다.

- 도입 및 운영 관련 관리 담당자 및 책임자
- 도입 관련 참여 인원 정보
- 도입 및 운영에 투입할 인력 및 조직
- 정보보호 기능요구사항 및 기능명세
- 정보보호와 관련된 문서화 요구사항
- 정보보호 지침관련 요구사항 해결 방안
- 안전성 확인을 위한 보안성 검증 계획
- 정보보호시스템 제품 유형별 도입 인증 요건 확인 및 검증필 암호모듈 탑재 대상 식별

② (보안책임 식별) 클라우드 컴퓨팅 서비스 도입·운용에 있어서 사용자와 관리자를 지정 운용하여야 한다.

- 사용자는 가상 PC, 가상 서버, 클라우드 기반 소프트웨어 등 클라우드 컴퓨팅 자원을 이용하거나 본인 계정으로 클라우드 컴퓨팅 환경 접속 관련한 보안 책임을 지님
- 관리자는 가상 자원에 대한 계정 할당, 가상환경 유지 등과 같은 클라우드 컴퓨팅 관리에 관련한 보안책임을 지님
- 관리자는 주기적으로 클라우드 컴퓨팅 서비스와 관련된 보안관리 현황을 확인하고 정보보안담당관에게 관련 내용을 통보(보고)하여야 함

- 정보보안담당관은 클라우드 컴퓨팅 서비스 운용과 관련한 보안 취약점을 발견하거나 보안대책 강구가 필요하다고 판단할 경우, 사용자 또는 관리자에게 시정을 요구할 수 있음

③ (보안위협 식별) 클라우드 컴퓨팅 서비스를 구축하여 다루고자 하는 업무 또는 데이터와 연관된 법령, 수행 요구사항, 정책, 규정, 표준, 가이드라인 등을 참고하여 보안 위협 대상을 식별하여야 한다.

- 클라우드 컴퓨팅과 관련된 물리적 설비, 하드웨어 장비, 가상 인프라, 가상머신 내 소프트웨어 등에 대한 보안위협 식별

④ (이전 정보자산 관리) 클라우드 컴퓨팅 서비스환경으로 이전 될 정보자산에 대한 관리 정책을 마련하고 정보자산 목록 관리를 하여야 한다.

- 기밀성, 무결성, 가용성, 법적 요구사항 등을 고려하여 이전 여부를 결정하여야 함
- 정보자산 이전 과정에서의 보안 위협 식별 및 보안 대책 마련

[IaaS 환경 추가 보안기준]

⑤ (형상 변경관리) 형상 변경에 영향을 받는 물리적·논리적 요소를 식별하고 형상 변경사항을 지속적으로 확인 및 검토를 하여야 한다.

- 시스템 구성 하드웨어 자산목록, 가상 머신 내 운영체제 및 소프트웨어, 보안 정책 등의 기준 형상을 마련하고 이에 대한 변경 여부를 지속적으로 확인
- 형상 변경 시 영향을 받는 물리적·논리적 요소 정보, 변경 수행을 위해 시스템 및 서비스에 접근하는 접근 기록, 변경 사항 등의 기록을 생성
- 기준 형상 변경 시 기관 정보보안담당관에게 형상 변경에 따른 보안 영향 분석 결과를 보고

⑥ (클라우드 시스템 모니터링) 클라우드 컴퓨팅 환경 내 모니터링 수집 대상 및 위치를 정의하고 시스템 운영 상황, 장애 발생 대응 도구 동작 여부 등을 모니터링 하여야 한다.

- 다음을 포함한 모니터링 수집 대상 정의
  - 클라우드 컴퓨팅 접속 사용자 현황
  - 클라우드 컴퓨팅 접속 단말 IP 혹은 MAC 주소
  - 보안 정책 이벤트
  - 가상머신에 할당된 자원 사용 현황
  - 클라우드 컴퓨팅 자원 운영 현황
  - 비정상 행위
- 다음을 포함한 모니터링 수집 위치 정의
  - 클라우드 내부 네트워크(가상)와 외부 네트워크(실제) 간 경계
  - 클라우드 컴퓨팅 서비스 간 네트워크

(2) 인적 관리

[공통 보안기준]

⑦ (인적 접근관리) 클라우드 컴퓨팅 서비스에 접근 가능한 사용자 및 관리자를 식별하고 직무별 권한 부여, 폐기 등에 관한 절차를 마련하여야 한다.

- 인적 보안 정책에 따라 클라우드 시스템 접근 권한을 부여하고 주기적으로 권한에 대한 재심사 수행
- 퇴직 및 직무 변경 등의 상황이 발생한 경우 인적 보안 정책 및 절차에 따라 자산 반납, 접근 권한 폐기, 조정 등의 절차 수행

⑧ (정보보안 교육) 안전한 클라우드 컴퓨팅 서비스 사용을 위한 정보보호 및 정보보호 관리 체계, 클라우드 보안 사고 사례, 사고에 따른 법적 책임, 사고 대응 방법 등이 포함된 직무별, 담당 분야 별 교육을 주기적으로 수행하여야 한다.

- 클라우드 컴퓨팅 관련사항을 포함하여 정보보안 교육계획을 수립하고 연 1회 이상 모든 소속 공무원 등을 대상으로 교육(온라인 교육을 포함)을 실시하여야 한다.
- 정기 정보보안 교육 미 참석자는 보충 교육을 통해 필수로 교육을 이수하여야 함
- 클라우드 관련 정보보안 교육 및 기술 세미나 참석을 장려하는 등 정보보안 담당관의 업무 전문성을 제고하기 위하여 노력하여야 함

(3) 사후 추적을 위한 감사자료 관리

[IaaS 환경 추가 보안기준]

⑨ (사후 추적을 위한 모니터링 및 로그관리) 보안 요구사항, 가용성 요구사항, 감사 요구사항, 법적 요구사항 등과 같은 요구사항들에 대한 준수 여부를 판별하기 위하여 다음과 같은 대상들에 대한 모니터링 및 로그 관리를 수행하여야 한다.

- 사용자 계정 로그인 성공/실패 이벤트
- 계정관리 이벤트
- 데이터 접근
- 정책 변경
- 관리자 권한으로 실행하는 기능
- 시스템 이벤트
- 가상머신 내 응용 소프트웨어

⑩ (로그자료 보호) 로그자료는 사후 추적대상을 식별할 수 있는 형태로 기록되고 1년 이상 보호되어야 한다.

- 사후 추적대상에 대한 사건유형, 발생일시, 발생장소, 사건발생 출처, 결과, 사건 관련 주체/이용자 식별정보 등을 알 수 있는 형태로 정보 기록
- 클라우드 시스템 접근 (단말PC, IP, 사용자ID, 시간, 작업내용 등) 관련 로그 기록을 1년 이상 유지 및 관리
- 비인가자에 대한 감사 저장소 접근을 방지
- 인가되지 않은 생성, 접근, 변경, 삭제 등으로부터 로그기록 보호

나. 클라우드 인프라

(1) 가상화 인프라

[공통 보안기준]

① (가상자원 관리) 다음과 같은 가상자원에 대한 사용 목록을 유지하여야 한다.

- 가상 머신
- 가상 스토리지
- 가상 애플리케이션 등

② (가상자원 회수) 가상자원 회수 시 가상자원 내에 존재하는 사용자 관련 데이터를 복구할 수 없는 형태로 삭제하여야 한다.

- 가상자원 회수 시 가상자원 내에 존재하는 사용자 개인정보, 업무 관련 자료, 설정 파일 등과 같은 사용자 관련 데이터를 복구할 수 없도록 데이터를 삭제하여야 함

③ (가상자원 모니터링) 가상자원에 대한 모니터링을 주기적으로 수행하여야 한다.

- 가상 자원에 대한 변경 발생 시 이를 로깅하고 이에 대한 이벤트 발생
- 가상자원에서 발생한 네트워크 트래픽이 임의로 수집되지 않도록 가상 스위치 보안 정책 설정

④ (자산 이전 보안) 기존 정보시스템 환경에서 클라우드 가상환경으로 이전 시 자산보호를 위한 암호화 등 안전한 이전 수단을 이용하여야 한다.

[IaaS 환경 추가 보안기준]

⑤ (하이퍼바이저 보안관리) 2단계 인증, IP기반 필터링 등 하이퍼바이저 관리 기능 및 관리자에 대한 접근 통제 방안을 마련하고, 하이퍼바이저에 대한 업데이트 및 보안 패치를 최신으로 유지하여야 한다.

[SaaS 환경 추가 보안기준]

⑥ (가상화 인프라 보안성 확인) SaaS 개발·운영을 위한 가상환경은 『국가 클라우드 컴퓨팅 보안 가이드라인』의 보안기준을 준수하는 클라우드 컴퓨팅 인프라 상에서 구축·운영되어야 한다.

다. 가상환경 보안

(1) 보안 관리

[공통 보안기준]

① (개발 보안관리) 가상환경에서 시스템, 애플리케이션, SaaS 등을 자체 또는 외주로 도입 및 개발하고자 하는 경우 다음과 같은 보안대책을 수립하여야 한다.

- 개발 및 테스트를 위한 가상 개발환경은 운영 중인 클라우드 서비스 환경과 분리
- 가상 개발 환경에 대한 비인가 접근 통제
- 개발에 사용되는 소스코드 및 소프트웨어 보안관리
- 외부 용역업체와 계약하여 개발을 하고자 하는 경우 다음의 사항을 추가적으로 준수
  - · 외부인력 대상 신원확인, 보안서약서 징구, 보안교육 및 점검
  - · 외부인력의 보안준수 사항 확인 및 위반 시 배상책임의 계약서 명시
  - · 외부인력의 접근권한 및 제공자료 보안대책
  - · 외부인력에 의한 자료 무단반출 여부 확인

  ※ 용역업체의 보안관리에 관련한 그 밖의 사항에 대해서는 『국가 정보보안 기본지침』의 용역업체 보안, 발주기관내 작업장소 보안, 원격지 개발보안, 원격지에서의 온라인 개발, 소프트웨어 산출물 제공 및 누출금지정보 유출시 조치에 대한 조항과 『국가·공공기관 용역업체 보안관리 가이드라인』의 내용을 준수
- SaaS를 도입 및 개발하고자 하는 경우 [부록 3] “SaaS 구축 유형”을 참고하여 구축

② (유지보수) 가상환경을 구성하는 시스템, 애플리케이션, SaaS 등을 유지 보수하고자 하는 경우 다음과 같은 보안대책을 수립하여야 한다.

- 유지보수 인원에 대한 보안서약서 집행, 보안교육 등을 포함한 유지보수 인가 절차를 마련하고 인가된 인원만 유지보수에 참여
- 관리자는 직접 또는 용역업체를 활용하여 정보시스템을 유지보수할 경우 콘솔 또는 지정된 단말기로부터의 접속만을 허용하여야 한다.
- 유지보수 일시, 담당자 인적사항, 출입통제 조치사항 및 작업수행 내용 등의 기록을 유지
- 클라우드 가상환경 유지보수에 관련한 그 밖의 사항에 대해서는 「국가 정보보안 기본지침」의 정보시스템 유지보수를 준용

③ (온라인 유지보수) 지정된 단말기를 통해 유지보수를 함에 있어, 각급 기관은 필요한 경우 다음과 같은 보안대책에 서면으로 동의하는 경우에 한하여 인터넷을 통한 온라인 유지보수를 허용할 수 있다. (보안·네트워크 장비는 제외, 예: IaaS 구성요소인 가상화 관리시스템은 정보보호제품에 해당하므로 온라인 유지보수 대상에서 제외됨)

- 지정된 장소에 설치된 지정된 단말기에서만 접속 및 해당 단말기에 대한 접근 인원 통제
- 지정 단말기는 용역업체의 온라인 접속을 통제하기 위한 온라인 용역 통제 시스템을 경유하여 유지보수 대상에 접속하는 등 소통구간 보호·통제
- 접속사실이 기록된 로그기록을 1년 이상 보관
- 지정 단말기는 온라인 용역 통제시스템에 대한 접속 전용으로 운용하고 다른 목적의 인터넷 접속은 차단
- 유지보수 계약 시행일로부터 종료 후 30일이 경과하는 날까지의 기간 중에 발주기관, 발주기관의 상급기관 및 국가정보원장의 정기 또는 수시 보안점검(불시 점검 포함) 수검

- 온라인 용역 통제시스템이 구축되지 않았으나 온라인 유지보수를 즉각 실시하지 않고서는 기관 업무수행에 현저한 저해가 있다고 예상되는 경우에는 기관의 인터넷망과 연계된 가상환경의 시스템, 애플리케이션 및 SaaS에 한하여 직접 접속하는 온라인 유지보수를 일시적으로 허용
- 온라인 유지보수에 관련한 그 밖의 사항에 대해서는 「국가 정보보안 기본지침」의 지정 단말기를 통한 온라인 유지보수를 준용

[IaaS 보안기준]

④ (인터넷 연결 가상PC 보안관리) 비인가자가 인터넷에 연결된 가상PC를 무단으로 조작하여 전산 자료를 절취, 위·변조 및 훼손시키지 못하도록 다음과 같은 보안대책을 마련하여 사용자의 인터넷 연결 가상PC에 적용하여야 한다.

- 최신 백신 소프트웨어 설치
- 메신저·P2P·웹하드 등 업무에 무관하거나 보안에 취약한 프로그램과 비인가 프로그램·장치 설치 금지
- 특별한 사유가 없는 한 문서프로그램은 읽기 전용으로 운용
- 음란·도박·증권 등 업무와 무관한 사이트 접근 차단 조치
- 무단으로 업무자료의 작성·저장 및 소통을 금지하고 최신 백신을 활용하여 바이러스 감염 여부 등을 주기적으로 점검
- 그 밖에 보안관리와 관련한 사항은 「국가 정보보안 기본지침」의 단말기 보안을 준용

⑤ (가상PC 보안관리) 가상PC 사용자는 PC 등 단말기 보안관리에 준하여 일체의 보안관리 책임을 지니며, 기관은 다음과 같은 보안 대책을 마련하여 사용자의 가상PC에 적용하여야 한다.

- 가상PC 접속용 장비·자료(문서자료 암호화 비밀번호)·사용자(로그온 비밀번호)별 비밀번호를 주기적으로 변경 사용하고 지문인식·OTP 등 생체인식 기술과 2단계 인증 적용 권고
- 가상 PC 작업을 일정 시간 중단시 비밀번호 등을 적용한 화면보호 조치

- 최신 백신 운용·점검, 침입차단·탐지시스템 등을 운용하고 가상 운영체제(OS) 및 각종 응용프로그램의 최신 보안 패치 유지
- 업무상 불필요한 응용프로그램 설치 금지 및 공유 폴더의 삭제
- 그 밖에 보안관리와 관련한 사항은 「국가 정보보안 기본지침」의 단말기 보안을 준용

⑥ (가상서버 보안관리) 서버 관리자는 가상머신을 할당받아 가상서버를 운용할 경우, 해킹을 통한 자료 절취, 위·변조 등에 대비한 보안대책을 수립·시행하여야 하며 세부사항은 「국가 정보보안 기본지침」의 서버 보안을 준용

⑦ (웹서버 등 공개용 가상서버 보안관리) 비인가자의 가상서버 내 저장자료 절취 및 위·변조, 분산서비스거부(DDoS) 공격 등에 대비하기 위하여 국가정보원장이 안전성을 검증한 침입차단·탐지시스템 및 DDoS 대응시스템을 설치하는 등 보안대책을 강구하여야 한다.

- 비인가자의 공개서버 내 비공개 정보에 대한 무단 접근을 방지하기 위하여 사용자를 제한하고 불필요한 계정 삭제
- 공개서비스에 필요한 프로그램을 개발하고 시험하기 위하여 사용된 도구(컴파일러 등)에 대한 개발 완료 후 삭제를 원칙으로 함
- 공개가상서버의 보안관리에 관련한 그 밖의 사항에 대해서는 「국가 정보보안 기본지침」의 공개서버 보안을 준용

⑧ (가상머신 내 소프트웨어 보안관리) 가상머신 내에 보안 상 취약한 소프트웨어 설치 방지, 보안 업데이트 등의 보안 관리 방안을 마련하여야 한다.

- 가상머신 내에 출처, 유통경로 및 제작자가 명확하지 않은 소프트웨어 설치 방지 및 탐지
- 주기적으로 소프트웨어에 대한 보안 패치 및 업데이트 실시

(2) 보안 관리 - SaaS 애플리케이션 개발

[SaaS 환경 보안기준]

⑨ (SaaS 애플리케이션 인증 및 권한) SaaS 애플리케이션 설계 및 개발 단계에서 SaaS 애플리케이션 접근을 위한 안전한 인증 방안이 마련되어야 하고, 접근 권한 정책을 수립하여 사용 및 관리 권한을 부여하여야 한다.

- SaaS 애플리케이션 설계 및 개발 시 기관의 인증 체계를 고려하여 안전한 인증 방안 적용하여야 함
- SaaS 애플리케이션 사용을 위한 권한 정책을 수립하고 그에 따른 사용 및 관리 권한을 부여하여야 함
- API 등을 통해 연동 서비스 호출 시 안전한 인증 방안 적용
- 인증 시 사용되는 인증키에 대한 보호 방안을 마련
- SaaS 사용자 데이터에 대한 접근 권한 정책을 수립하고 그에 따른 사용 및 관리 권한을 부여하여야 함

⑩ (SaaS 애플리케이션 기밀성) SaaS 애플리케이션의 데이터 처리(송·수신, 저장, 연산 등) 과정에서 데이터를 보호하기 위한 수단을 마련하여야 한다.

- SaaS 애플리케이션의 중요 데이터를 송·수신할 때에는 TLS 등의 암호화 프로토콜을 적용하여야 함
- SaaS 애플리케이션을 통해 생성된 사용자 데이터는 암호화 수단을 사용하여 안전하게 보호되어야 함
- SaaS 애플리케이션에서 사용되는 암호화키에 대한 보호 방안 마련

⑪ (연동서비스 호출 기밀성) SaaS 애플리케이션 설계 및 개발단계에서 연동서비스 호출 시 송·수신되는 인증정보, 메시지 등을 보호하기 위한 수단을 마련하여야 한다.

- 연동서비스 호출을 통한 데이터 송·수신 시에 TLS 등의 암호화 프로토콜을 적용하여야 함
- 연동서비스 인증에 사용되는 인증정보에 대한 보호방안 마련

⑫ (SaaS 애플리케이션 무결성) SaaS 애플리케이션 설계 및 개발 단계에서 사용자 데이터에 대한 무결성 검증 방안을 마련하여야 한다.

- SaaS 애플리케이션에서 처리되는 사용자 데이터의 위·변조 탐지를 위한 무결성 검증
- 연동 서비스 호출 시 송·수신되는 데이터에 대한 무결성 검증
- SaaS는 허가받은 연동 서비스와 연동되어야 함
- SaaS 사용자의 가상 자원 및 데이터가 사용자 별로 분리되어 안전하게 관리가 되어야 함
- SaaS 애플리케이션 개발 시 신뢰할 수 있는 소프트웨어만을 사용하고, 무결성 검증을 수행하여야 함

⑬ (SaaS 애플리케이션 가용성) SaaS 애플리케이션은 사용자 업무 연속성을 보장할 수 있는 형태로 설계 및 개발되어야 한다.

- 가용성에 대한 사용자 요구사항을 충족시킬 수 있는 형태로 SaaS 애플리케이션을 설계 및 개발하여야 함
- 가용성에 대한 사용자 요구사항을 충족시킬 수 있는 개발·운영 가상환경 및 클라우드 인프라 환경을 선정하여야 함

⑭ (SaaS 감사기록 관리) 보안 요구사항, 가용성 요구사항, 감사 요구사항, 법적 요구사항 등에 대한 준수 여부를 판별하기 위하여 SaaS에 대한 모니터링 및 로그 관리를 수행하여야 한다.

- 사용자 계정 로그인 성공/실패 이벤트
- 계정관리 이벤트
- 데이터 접근
- 정책 변경
- 관리자 권한으로 실행하는 기능
- 웹 기반으로 발생하는 이상행위

⑮ (SaaS 감사기록 보호) SaaS에서 생성된 로그 자료는 사후 추적대상을 식별할 수 있는 형태로 기록되고 1년 이상 보호되어야 한다.

- 사후 추적대상에 대한 사건유형, 발생일시, 발생장소, 사건발생 출처, 결과, 사건 관련 주체/이용자 식별정보 등을 알 수 있는 형태로 정보 기록
- 접근 (단말PC, IP, 사용자ID, 시간, 작업내용 등) 관련 로그 기록을 1년 이상 유지·관리
- 비인가자에 대한 감사 저장소 접근을 방지
- 인가되지 않은 생성, 접근, 변경, 삭제 등으로부터 로그 기록 보호

⑯ (SaaS 애플리케이션 보안관리) SaaS 애플리케이션 보안을 위해 주기적 취약점 점검, 보안업데이트 등의 보안 관리 방안을 마련하여야 한다.

- SaaS 애플리케이션을 대상으로 주기적인 취약점 점검, 최신 보안 패치, 업데이트, 침투테스트 등을 실시
- SaaS 구축에 사용되는 인터페이스 및 API에 대한 주기적인 보안점검 수행

⑰ (SaaS 애플리케이션 개발) 자체 또는 외주로 SaaS 애플리케이션 개발을 하고자 하는 경우 다음과 같은 보안대책을 수립하여야 한다.

- SaaS 보안취약점의 원인인 보안약점을 배제하도록 개발 단계 별 보안활동을 수행하여 개발하여야 함
- 출처, 유통경로 및 제작자가 명확하지 않은 소스코드 및 소프트웨어는 개발에 사용될 수 없음
- 개발에 사용되는 소스코드 및 소프트웨어 보안관리
- 외부용역 업체와 계약하여 개발하고자 하는 경우 다음 사항을 추가로 준수
  - 외부인력 대상 신원확인, 보안서약서 징구, 보안교육 및 점검
  - 외부 인력의 보안준수 사항 확인 및 위반 시 배상책임의 계약서 명시
  - 외부 인력의 접근권한 및 제공자료 보안대책
  - 외부 인력에 의한 자료 무단반출 여부 확인

(3) 보안 관리 - 개발·운영 환경

[SaaS 환경 보안기준]

⑱ (개발·운영 환경 인증 및 권한) 개발·운영 환경 접속을 위한 안전한 인증 방안을 마련해야 하고, 접근 권한 정책을 수립하여 사용 및 관리 권한을 부여하여야 한다.

- 인증에 사용되는 인증정보 보호 방안을 마련하여야 함
- SaaS 개발 및 운영에 필요한 데이터(SaaS 애플리케이션 소스파일, 설정 파일, 관리 로그, 사용자 인증 정보 등)에 대한 접근 통제 정책을 마련하고, 그에 따른 이용 및 관리 권한을 부여하여야 함
- SaaS 개발 및 운영에 필요한 서비스 포트 외에 불필요한 서비스 포트를 제거하고, 관리용 서비스와 사용자용 서비스를 분리하여 운영하여야 함
- SaaS 가상 서버 및 가상 스토리지에 대한 접근 권한 정책 수립

⑲ (개발·운영 환경 기밀성) 개발·운영 환경 관리에 필요한 데이터 보호 방안을 마련하여야 한다.

- SaaS 애플리케이션 관련 데이터(소스파일, 설정 파일 등)를 개발·운영 환경으로 송·수신할 때에는 TLS 등의 암호화 프로토콜을 적용하여야 함
- 개발·운영 환경 관리에 필요한 데이터를 암호화하여 안전하게 저장 및 처리하여야 함
- 개발·운영 환경 내에서 사용되는 암호화키에 대한 보호 방안을 마련해야 함

⑳ (개발·운영 환경 무결성) 개발·운영 환경 내 저장된 SaaS 관련 데이터에 대한 무결성 검증을 수행하여야 한다.

- 개발·운영 환경에 저장된 SaaS 애플리케이션 관련 데이터(소스파일, 설정 파일 등)에 대한 무결성 검증
- 개발·운영 환경은 허가받은 연동 서비스와 연동되어야 함
- 개발·운영 환경 관리에 필요한 데이터는 사용자별로 분리되어 관리되어야 함
- 개발·운영 환경 구축 시 신뢰할 수 있는 소프트웨어만을 사용하여 구축하고, 무결성 검증을 수행하여야 함
- SaaS를 개발하고 테스트 중인 개발 환경은 SaaS 운영 환경과 분리 구축되어 SaaS 운영 환경 내 저장된 데이터, 설정 값 등에 영향을 미치지 않도록 하여야 함

㉑ (개발·운영 환경 가용성) 개발·운영 환경은 SaaS 운영 연속성을 보장할 수 있는 형태로 구축되어야 한다.

- 가용성에 대한 사용자 요구사항을 충족시킬 수 있는 형태로 개발·운영 가상 환경을 구축하여야 함
- 가용성에 대한 사용자 요구사항을 충족시킬 수 있는 클라우드 인프라 환경을 선정하여야 함

㉒ (개발·운영 환경 감사기록 관리) 보안 요구사항, 가용성 요구사항, 감사 요구사항, 법적 요구사항 등에 대한 준수 여부를 판별하기 위하여 개발·운영 환경에 대한 모니터링 및 로그 관리를 수행하여야 한다.

- 사용자 계정 로그인 성공/실패 이벤트
- 계정관리 이벤트
- 데이터(사용자 소스파일, 설정 정보, 로그기록 등) 접근
- 정책 변경
- 관리자 권한으로 실행하는 기능
- SaaS 가상머신 및 스토리지에 대한 이상행위

㉓ (개발·운영 환경 감사기록 보호) 개발·운영 환경 운영 중 생성된 로그 자료는 사후 추적대상을 식별할 수 있는 형태로 기록되고 1년 이상 보호되어야 한다.

- 사후 추적대상에 대한 사건유형, 발생일시, 발생장소, 사건발생 출처, 결과, 사건 관련 주체/이용자 식별정보 등을 알 수 있는 형태로 정보 기록
- 접근 (단말PC, IP, 사용자ID, 시간, 작업내용 등) 관련 로그 기록을 1년 이상 유지·관리
- 비인가자에 대한 감사 저장소 접근을 방지
- 인가되지 않은 생성, 접근, 변경, 삭제 등으로부터 로그기록 보호

㉔ (개발·운영 환경 보안관리) 개발·운영 환경 보안을 위해 주기적 취약점 점검, 보안 업데이트 등의 보안관리 방안을 마련하여야 한다.

- 개발·운영 환경 구축에 필요한 소프트웨어를 대상으로 주기적인 취약점 점검, 최신 보안 패치, 업데이트, 침투테스트 등을 실시
- 개발·운영 환경 구축에 사용되는 인터페이스 및 API에 대한 주기적인 보안 점검 수행

㉕ (개발·운영 가상서버 보안관리) 개발·운영 환경 구축을 위해 가상서버를 운용할 경우, 해킹을 통한 자료 절취, 위·변조 등에 대비한 보안대책을 수립·시행하여야 하며 관련 세부사항은 「국가 정보보안 기본지침」의 서버 보안을 준용하여야 한다.

㉖ (웹서버 등 공개용 개발·운영 가상서버 보안관리) 개발·운영 환경 구축을 위해 공개용으로 운영되는 가상서버를 운용할 경우, 비인가자의 가상서버 내 저장자료 절취 및 위·변조, 분산서비스거부(DDoS) 공격 등에 대비하기 위하여 국가정보원장이 안전성을 검증한 침입차단·탐지시스템 및 DDoS 대응시스템을 설치하는 등 보안대책을 강구하여야 한다.

- 비인가자의 공개서버 내 비공개 정보에 대한 무단 접근을 방지하기 위하여 사용자를 제한하고 불필요한 계정 삭제
- 공개서비스에 필요한 프로그램을 개발하고 시험하기 위하여 사용된 도구(컴파일러 등)에 대한 개발 완료 후 삭제를 원칙으로 함
- 공개가상서버의 보안 관리에 관련한 그 밖의 사항에 대해서는 「국가 정보보안 기본지침」의 서버 보안을 준용

(4) 악성코드 감염방지

[공통 보안기준]

㉗ (악성코드 감염방지) 웜·바이러스, 해킹프로그램, 스파이웨어 등 악성코드에 의한 위협을 제거하기 위해 악성코드 방지 대책을 수립·시행하여야 한다.

- 가상머신 내 운영체제, 소프트웨어 등에 대한 주기적인 보안패치 실시
- 백신은 최신상태로 업데이트·상시 감시상태로 설정하고 주기적인 점검 실시
- 보안에 취약하고 업무상 불필요하거나 출처, 유통경로 및 제작자가 명확하지 않은 소프트웨어를 사용할 수 없으며 클라우드 컴퓨팅 외부에 위치한 망으로 자료 입수 시 최신 백신으로 진단 후 사용
- 사용 금지 대상 소프트웨어에 대한 설치 금지, 설치 탐지 등과 같은 보안 통제 방안을 마련하여 보안 관리 수행
- 외부 악성코드 위협 접근통제를 위한 침입차단시스템 등의 보안대책 마련

㉘ (악성코드 탐지 조치) 가상머신에 악성코드가 설치되거나 감염된 사실을 발견하였을 경우에 다음과 같은 조치를 하여야 한다.

- 악성코드 감염원인 규명 등을 위하여 감염된 가상머신 사용을 중지하고 격리 조치 수행
- 심각할 경우 감염 환경을 보존하고 원인 파악 이후 초기 상태로 복구
- 악성코드의 감염확산 방지를 위하여 정보보안담당관에게 관련 사실을 즉시 통보하여야 함
- 각급 기관은 악성코드가 신종이거나 감염피해가 심각하다고 판단할 경우에는 관련 사항을 국가정보원장에게 신속히 통보하여야 함
- 각급기관은 국가정보원장이 해당 기관에 악성코드 감염사실을 확인하여 조치를 권고할 경우, 즉시 이행하여야 함
- 악성코드 감염의 확산과 재발을 방지하기 위해 원인을 분석하고 예방조치 수행

(5) 접근 통제

[공통 보안기준]

㉙ (접근 제한 방안) 이동식 저장매체 사용 통제, 다중요소(Multi-factor) 인증, 자동 로그아웃 등을 포함하여 다음과 같은 접근 제한 방안을 마련하여야 한다.

- 클라우드 시스템에 대한 USB등의 이동식 저장매체 사용 통제
- 식별 번호가 등록된 이동매체만 사용
- 인증서(PKI)기반, OTP, MAC, 지문 등 다중요소(Multi-factor) 인증 제공
- 일정 시간 이상 업무 작업 중단 시 비밀번호 등이 적용된 화면보호 조치
- 일정 시간 이상 업무 작업 중단 시 자동 로그아웃 등이 적용된 보호 조치
- 중요 기능에 대한 동일 사용자의 동시 세션 제한

㉚ (식별정보 관리) 사용자 또는 장치를 유일하게 식별할 수 있는 식별 방법을 마련하고 식별정보를 관리하여야 한다.

- 사용자를 유일하게 구분할 수 있는 식별자(아이디)를 할당하여 모든 사용자에 대한 책임 추적성 보장
- 관리자 및 특수권한 계정의 경우 추측 가능한 식별자(root, admin, administrator 등)의 사용 제한
- 시스템 설치 및 유지 이후 임시로 할당된 식별자 제거
- 계정 및 비밀번호의 유효 기간을 두고 만료 시 재발급 절차를 거쳐야함

㉛ (사용자계정 생성) 계정 유형 식별, 계정 그룹 설정 등을 담은 다음과 같은 계정 권한 생성 절차를 마련하여야 한다.

- 계정 유형 식별(즉, 개인 이용자, 그룹, 시스템, 응용프로그램, 게스트, anonymous, 임시 등)

- 계정 그룹 설정
- 클라우드 시스템 및 서비스 접근이 허용된 자에 대한 식별 및 접근권한 명세
- 계정 생성과 권한 설정 요청 기능 지원
- 게스트 또는 임시 계정에 대한 승인 및 모니터링
- 외부인에 대한 계정 부여 정책
- 사용자 및 관리자 업무 환경 변화에 따른 대응
- 계정 삭제 대상 식별
- 계정 삭제 대상 관리 정책

㉜ (사용자계정 관리) 다음과 같은 내용을 포함한 사용자계정 보안관리 방안을 마련하여 사용자계정(ID) 부여 및 보안관리를 수행하여야 한다.

- 사용자별 또는 그룹별로 접근권한 부여
- 업무상 불가피하게 외부인에게 계정을 부여해야 하는 경우 공공기관 책임하에 필요 업무에 한하여 특정 기간만 접속할 수 있게 하는 등의 보안 조치 강구 후 허용
- 사용자 식별 수단이 없는 사용자 계정 사용 금지
- 사용자가 5회 이상에 걸쳐 로그인 실패 시 접속을 중단시키고 비인가자의 침입 여부를 확인 점검
- 직원의 퇴직 또는 보직변경 발생 시 사용하지 않는 사용자 계정을 신속히 삭제
- 특별한 사안이 없는 한 유지보수 등을 위한 외부업체 직원에게 관리자 계정 제공을 금지
- 사용자 계정의 부여 및 관리 적합성 여부를 연2회 이상 점검

㉝ (비밀번호 관리) 다음과 같은 비밀번호 관리 방안을 마련하여야 한다.

- 숫자·문자·특수문자 등을 혼합하여 안전하게 설정하고 정기적으로 변경·사용하여야 한다.

- 사용자(ID)와 동일하지 않아야 하며, 개인 신상 및 부서명칭 등과 관계가 없도록 설정
- 사전에 등록된 단어는 사용을 피하며, 동일 단어 또는 숫자 반복 사용 금지
- 사용된 비밀번호 재사용 금지
- 여러 사람이 동일한 비밀번호로 접근하는 것을 금지하도록 권고
- 응용프로그램 등을 이용한 자동 비밀번호 입력기능 사용 금지

㉞ (접근 기록 관리) 접근 기록은 서비스 통제, 관리, 사고 발생 책임 추적성 등을 보장할 수 있는 형태로 기록되고 1년 이상 보관, 유지하여야 한다.

- 다음과 같은 접근 기록 대상을 포함
  - · 접속자, 클라우드 시스템 및 서비스, 가상 머신 내 소프트웨어, 가상 머신 등 접속 대상
  - · 로그 온·오프, 파일 열람·출력 등 작업 종류, 작업 시간
  - · 접속 성공·실패 등 작업 결과
  - · 클라우드 컴퓨팅 망 외부로의 데이터 전송 정보 등
- 비인가자의 접속 시도, 정보 위변조 및 무단 삭제 등의 의심스러운 활동이나 위반 혐의가 발생한 사실을 발견한 경우 정보보안담당관에게 즉시 보고
- 접근 기록은 정보보안 사고 발생 시 확인 등을 위하여 최소 1년 이상 보관하여야 하며 접근 기록 위·변조 및 외부 유출 방지 대책을 강구해야 함

㉟ (첨단 정보통신기기 보안관리) 스마트폰·IoT기기·전자제어장비 등 첨단 정보통신기기를 활용하여 클라우드 컴퓨팅 관리 및 접속하기 위해서는 자체 보안대책을 수립 및 시행하여야 한다.

㊱ (인터페이스 및 API 보안) 가상환경 접근을 위한 인터페이스 및 API에 대한 보안 방안을 마련하여야 한다.

라. 데이터

(1) 데이터 관리

[공통 보안기준]

① (비밀 데이터 처리규격) 클라우드 시스템에서 기관의 비밀을 전자적으로 안전하게 처리하기 위해 다음 사항을 포함한 국가정보원장이 별도로 규정한 보안 규격을 준수하여야 한다.

- 비밀의 생산, 등록, 보관, 사용, 유통 및 재분류, 이관, 파기 등 전 처리과정에서 요구되는 보안기능
- 비밀의 관리를 위한 기능
- 비밀을 표시하기 위한 양식 및 외형 정의
- 비밀을 전자적으로 처리하면서 발생하는 각종 이벤트 기록·관리 기능
- 비밀을 관리하기 위한 각종 대장 및 카드 정의
- 사용자 및 시스템 관리 기능
- 그 밖에 비밀을 전자적으로 처리하는데 필요한 보안·관리 기능

② (데이터 송·수신 관리) 기관 내부에 위치한 클라우드 접속 단말과 클라우드 컴퓨팅 환경 간 비인가 데이터 송·수신을 차단하여야 한다.

③ (데이터 폐기) 클라우드 시스템 폐기, 이전 등에 따른 데이터 폐기 조치 시 폐기된 데이터는 복구할 수 없는 형태로 삭제되어야 한다.

- 데이터 폐기처리는 기관의 정보보안담당관 승인을 필요로 하며, 처리 절차 및 처리 결과를 정보보안담당관에게 보고

[SaaS 환경 추가 보안기준]

④ (데이터 격리성) 사용자별 데이터 보안 요구 사항 수준에 따라 물리적 또는 논리적으로 데이터를 사용자별로 분리할 수 있는 방안을 마련하여 SaaS 애플리케이션 및 개발·운영 환경을 구축하여야 한다.

⑤ (데이터 기밀성) 데이터 송수신, 연산, 저장 시 데이터 암호화 등의 수단을 적용하여 SaaS 애플리케이션 취약점 등을 이용한 보안 위협으로부터 데이터 노출 시 기밀성을 유지할 수 있어야 한다.

⑥ (데이터 무결성) SaaS 애플리케이션 및 개발·운영 환경에서 처리되는 중요 데이터에 대한 무결성 검증을 수행하여야 한다.

⑦ (데이터 추적성) SaaS 애플리케이션 및 개발·운영 환경에서 생성되는 중요 데이터에 대한 추적성을 보장하여야 한다.

- 사용자의 SaaS 애플리케이션 데이터 폐기 시 사용될 수 있도록 추적성을 보장할 수 있는 식별자를 제공하여야 함
- 사용자의 법적, 보안 요구사항 등에 따라 데이터 저장 위치 설정, 물리적 위치 추적성 보장 등을 제공하여야 함

⑧ (데이터 폐기) SaaS 사용 종료 등의 이유로 인한 데이터 폐기 시 SaaS 환경 내에 존재하는 사용자 관련 데이터는 복구할 수 없는 형태로 삭제되어야 한다.

- 사용자의 SaaS 애플리케이션 사용 종료, 이전 등에 따른 데이터 폐기 조치 시 폐기된 데이터를 복구할 수 없도록 데이터를 삭제하여야 함

(2) 암호화

[공통 보안기준]

⑨ (데이터 처리) 클라우드 시스템을 도입할 경우, 중요 업무자료에 대한 암호화 수준 등에 대한 보안요구사항을 도출하여 반영하여야 하며, 중요 업무자료에 대한 생성·보관·처리·수신하기 위한 정책적·기술적 방안 강구해야 한다.

⑩ (암호 정책 수립) 클라우드 가상자원에 저장 또는 전송 중인 중요 업무자료를 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 (암호키 관리) 암호키 생성, 이용, 보관, 배포, 파기에 대한 내용을 담은 암호키 관리 절차를 수립하여야 하며 안전한 암호키 관리 여부를 확인하여야 한다.

- 암호키는 별도의 물리적으로 분리된 서버에 백업하고 최소 접근 권한을 부여하여야 함

마. 인증 및 권한

(1) 인증

[공통 보안기준]

① (인증 정책 수립) 서비스 관리환경, 가상머신, 가상 응용프로그램, SaaS 등의 접근 대상 및 주체를 식별하여 인증 정책을 수립하여야 한다.

② (기관 인증 체계 연동) 기관 필요에 따라 클라우드 접근 대상 별로 기관의 인증 체계와 연동할 수 있는 인증 시스템을 설계 및 구축하여야 한다.

(2) 권한

[공통 보안기준]

③ (접근 권한 관리) 접근 대상, 권한 부여 절차 등을 담은 사용자, 관리자의 접근 권한 관리절차를 수립하여야 한다.

- 접근 대상, 권한부여절차, 권한 수준, 권한 부여조건 등의 내용을 사용자, 관리자의 접근 권한 관리절차에 포함
- 사용자 및 관리자 별 관리 절차 마련
- 권한 부여 조건을 정의하고 조건에 따라 사용자에게 적합한 접근 수준을 지닌 권한 부여

④ (권한 부여 정책) 클라우드 접근 대상에 따라 접근 주체별로 이용·관리 권한을 부여하여야 한다.

바. 사고 및 장애 대응

(1) 사고

[공통 보안기준]

① (사고 대응절차) 신고 절차, 유출 금지 대상, 사고 처리 절차 등을 담은 보안사고 발생 대응 절차를 마련하여야 한다.

- 다음과 같은 내용을 보안사고 발생 대응 절차에 포함
  - 보안사고 발생 시 해당 처리부서와 국가 사이버 안전센터로 신고 절차
  - 보안 담당자 검토 및 승인 절차
  - 보안사고 대응조직 체계 및 조직 구축
  - 신고 대상 보안사고 정의, 유출 금지 대상
  - 사고 처리 절차, 사고 발생 보고서
  - 보안 사고 대응 계획
  - 사고 조사 범위 지정
- 시스템관리자는 사이버 공격과 관련한 정보를 확인한 경우에는 전화·팩스·이메일 등 통신수단을 활용하여 지체 없이 그 사실을 정보보안담당관에게 통보하여야 함
  - 대규모 사이버공격 발생시
  - 사이버공격으로 인하여 피해가 발생하거나 피해 발생이 예상되는 경우
  - 사이버공격이 확산될 우려가 있는 경우
  - 그 밖에 사이버공격 계획 등 사이버안전에 위협을 초래할 수 있는 정보를 입수한 경우
- 사고 대응을 위하여 대내외 관련 기관 및 전문가와 협조체계 구축
- 전시·사변 또는 이에 준하는 국가비상사태 발생 시에 대비하여 비상사태 단계별 공공기관 클라우드 시스템의 소산·이동·파기 절차·방법 등 조치방안 일체를 포함하는 대응책 강구

② (사고 조사) 정보보안 사고가 발생한 때에는 즉시 피해확산 방지를 위한 조치를 취하고 사고 발생일시, 사고내용 등을 포함하는 보고서를 작성하여 국가 정보보안 기본 지침 제140조에 따른 조사기관의 장에게 통보하여야 한다.

- 다음과 같은 내용을 사고 발생 보고서에 포함
  - · 사고 발생일시
  - · 보고자와 보고일시
  - · 사고내용 (원인, 발견사항, 피해내용 등)
  - · 사고대응 경과 내용
  - · 사고대응까지의 소요시간
  - · 사고자 및 관계자의 인적 사항
  - · 조치 내용 등

2) 장애

[공통 보안기준]

③ (장애 대응절차) 장애 대응 요구사항, 담당자 정의 및 연락처 등을 담은 장애 대응 절차를 마련하여야 한다.

- 다음과 같은 내용을 장애 대응 절차에 포함
  - · 장애 대응 계획서
  - · 도입 기관의 장애 대응 요구사항
  - · 장애 대응 관련 담당자 정의 및 연락처
  - · 클라우드 컴퓨팅 시스템 파기, 훼손 및 장애 시 정상적인 업무 유지에 필요한 핵심 기능
  - · 클라우드 컴퓨팅 시스템 복원 시 보안성에 영향을 미치는 요소
  - · 업무연속성 관련 인력 및 조직

- 지정한 복구시간 이내에 클라우드 컴퓨팅을 재개할 수 있도록 대체 프로세스를 마련
- 재난방지대책을 정기적으로 시험하고 검토해야 하며 업무 연속성에 대한 영향 평가를 실시하여야 함
- 클라우드 컴퓨팅을 위한 백업시설은 클라우드 시스템 구축 장소와 물리적으로 일정거리 이상 떨어진 안전한 장소에 설치하여야 하며 전력공급원 이원화 분리 등 클라우드 시스템의 가용성을 최대화 할 수 있도록 하여야 함

④ (백업 및 복구 관리) 백업 시기 및 방법, 백업본 유지 기간 등을 담은 데이터에 대한 백업과 복구절차를 마련하여야 한다.

- 다음과 같은 내용을 백업과 복구 관련 계약 사항에 포함
  - · 백업 시기 및 방법
  - · 백업본 유지 기간
  - · 백업 대상 데이터
  - · 복구 방법 및 기간
  - · 복구 요청 승인 조건
  - · 백업 및 복구를 위한 가용 자원

제2절 민간 클라우드 컴퓨팅 서비스 이용 보안기준

1. 보안 기본원칙

민간 클라우드 컴퓨팅 서비스 이용은 민간 사업자가 제공하는 클라우드 컴퓨팅 서비스를 기관이 이용하는 형태이다. 이 때, 민간 클라우드 컴퓨팅 서비스를 도입하려는 기관은 기존 내부 정보시스템에 대한 기관 보안 통제 수준을 클라우드 컴퓨팅 환경 하에서도 유지해야 하며, 서비스 제공자는 공공 전용 민간클라우드 영역에 대해 정부기관에 준하는 보안관리를 수행해야 한다. 따라서 서비스 제공자는 사고 또는 장애 발생 시 국가기관의 장애사고 절차에 따라 협조체계를 구성·대응하여야 하며, 피해확산, 재발방지, 복구 등에 필요한 조치를 위해 국가정보원 및 이용기관의 보안관제 및 사고조사 등 예방보안 활동에 적극 협조하여야 한다. 이를 위해 이용 기관은 서비스 제공자와 계약 시 해당 사항을 반드시 명시해야 한다.

이에 본 가이드라인에서는 기존 기관 정보시스템 보안관리 체계와의 연속성 유지 및 클라우드 컴퓨팅 환경의 특성에 따른 보안위협 대응, 민간 사업자 신뢰성 확인의 목적을 가지고, 기술적·정책적 측면에서의 보안 기본원칙을 마련하였다. 이용 기관은 본 가이드라인에서 제시하는 보안 기본원칙과 공통 보안기준을 바탕으로 보안관리 체계와의 연속성을 유지하기 위한 보안 요구사항을 정의해야 한다. 또한 보안요구사항을 민간 사업자가 이행할 수 있는지 여부를 면밀히 검토하여야 한다. 보안 기본원칙은 모든 클라우드 컴퓨팅 서비스 유형에 공통적으로 적용해야 하는 원칙, IaaS 환경 및 SaaS 환경에 추가적으로 요구되는 원칙으로 구분된다. 또한 PaaS 환경의 경우 SaaS 환경과 동일한 원칙을 준용한다.

가. 정책적 측면에서의 기본원칙

[공통 기본원칙]

① 민간 클라우드 컴퓨팅 서비스를 이용하려는 국가·공공기관은 본 가이드라인에 따라 이용 대상에 대한 시스템 중요도 등급 분류 및 클라우드 영역 분류를 수행하고 관련 보안기준을 사전 확인하여야 한다.

- '제3장 제2절 국가·공공기관 활용 클라우드 영역 분류' 및 '제3장 제3절 시스템 중요도 분류 기준 및 절차'의 내용 참조

※ 시스템 중요도에 따른 필수/권고 항목은 [부록 4] 클라우드 컴퓨팅 보안기준 체크리스트 참고

② 클라우드 시스템 및 데이터의 물리적 위치는 국내로 한정하고, 국가·공공기관용 클라우드 컴퓨팅 서비스의 자원(서버, 네트워크, 보안장비 등), 출입통제, 운영인력 등은 민간 이용자용 클라우드 컴퓨팅 서비스 영역과 분리 운영하여야 하며 기관 담당자는 이를 확인하여야 한다.

- 클라우드 컴퓨팅 서비스 자원(서버, 네트워크, 보안장비 등)은 민간 이용자용 클라우드 컴퓨팅 서비스 영역과 물리적/논리적으로 분리 운영할 수 있음, 영역 분리 형태와 보안 고려사항은 본 가이드라인 '제3장 제2절 클라우드 영역 분류' 및 '제3장 제3절 시스템 중요도 분류 기준 및 절차'의 내용 참조
- 클라우드 컴퓨팅 서비스 운영 및 관리 인력은 국가정보보안 기본지침 제26조 2항에 결격사유가 없는 인원으로 구성

③ 국가정보원이 도입요건 확인을 완료한 민간 클라우드 컴퓨팅 서비스를 이용하여야 한다.

- 이용 기관은 민간 클라우드 컴퓨팅 서비스 이용시 국가정보원이 도입요건 확인을 완료한 민간 클라우드 컴퓨팅 서비스 목록을 수시로 확인 (국가정보원 보안기준 만족 여부 확인)

※ 서비스 이용 계약 시 이용기관은 국가정보원 및 해당 기관의 보안관제 및 사고조사, 예방보안활동 등에 적극 협조하도록 하는 내용을 명시해야 함

※ 서비스 이용 계약 이후 사업자의 기준 준수여부는 이용 기관이 수시 확인 필요

④ 도입 정보보호시스템 안전성을 확인하여야 한다.

- 민간 클라우드 컴퓨팅 서비스 구축을 위해 도입되는 보안 기능을 가진 정보통신제품 중에서 전자정부법 제56조에 규정된 전자문서의 위조, 변조, 훼손 또는 유출을 방지하기 위한 목적으로 도입하는 제품은 국가정보원장이 안전성을 확인한 제품을 사용하여야 함

※ 기타 세부사항은 국가정보원의 보안적합성 검증제도에 따름

※ 클라우드 인프라에서 중대한 보안 취약점이 발견되어 긴급한 보안패치 등이 필요한 경우 유관기관 협의 하에 인증 요건을 유예할 수 있음

⑤ 각급기관의 내부망과 연동된 공공 전용 민간클라우드는 각급기관의 내부망으로 간주하며, 각급기관의 인터넷망과 연동된 공공 전용 민간클라우드는 각급기관의 인터넷망으로 간주하여 「국가 정보보안 기본지침」에 따라 보안관리를 하여야 한다.

⑥ 이용기관은 클라우드 운영·이용에 대한 보안 관리 책임이 있으며, 클라우드 서비스 제공자와 기관의 보안 관리 체계를 반영하는 보안 서비스수준협약(SLA)을 맺어야 한다.

※ 이용기관은 내부 정보시스템에 대한 보안 관리 체계를 클라우드 환경하에서도 최대한 유지하기 위해, 민간 사업자와 계약 시 국가정보원 및 이용기관의 예방 보안활동에 적극 협조하도록 하는 내용을 명시해야 함

⑦ 이용기관은 공급망 관리 정책을 수립하고 관련 보안 요구사항을 계약 상 반영토록 하여야한다.

※ 공급망 관리 정책은 공급망의 위험 식별, 변경관리 및 모니터링 등의 내용을 포함해야 함

[SaaS 환경 추가 기본원칙]

⑧ 망 미분리 기관은 SaaS를 사용하는 단말에서 인터넷과 업무 영역 간 자료 교환이 되지 않도록 기술적 통제대책을 구현하여 SaaS를 사용하여야 한다.

⑨ SaaS 클라우드 인프라, 개발·운영 환경의 물리적 위치는 국내로 한정되어야 하며, SaaS에서 처리되는 데이터에 대한 물리적 위치도 국내로 한정한다.

※ 민간 클라우드 인프라 이용 시 이용기관용 SaaS 관리 데이터(소스코드, 설정 파일, 로그, 사용자 계정 정보 등), 운영인력 등은 민간 사용자 영역과 분리되어 국내에 위치하여야 함

※ SaaS 관리 데이터는 민간 이용자용 클라우드 컴퓨팅 서비스 영역과 물리적/논리적으로 분리 운영할 수 있음, 영역 분리 형태와 보안 고려사항 등은 본 가이드라인 제3장 제2절에 따른 클라우드 영역별 기본원칙을 참조

⑩ SaaS를 제공하기 위한 SaaS 개발·운영 환경, 클라우드 인프라 환경에 대한 보안성을 확인하여야 한다.

⑪ SaaS 개발·운영 환경은 SaaS 서비스 가용성을 보장할 수 있어야 하며, 사고 및 장애에 대응할 수 있는 체계가 마련되어야 한다.

⑫ SaaS는 허가받은 외부 연동 서비스(스토리지, 데이터베이스, 빅데이터 처리 등)와 연계되어야 한다.

나. 기술적 측면에서의 기본원칙

[공통 기본원칙]

⑬ 내부 업무와 인터넷 서비스 업무의 클라우드 컴퓨팅 혼용을 금지한다.

- 업무망·인터넷 분리 원칙에 따라 기관의 내부 업무시스템은 인터넷 서비스를 제공하는 클라우드 컴퓨팅 시스템에서 운영되어서는 안 됨

⑭ 중요장비 이중화 및 백업체계 구축하고 표준운영절차를 수립하여야 한다.

- 클라우드 컴퓨팅은 중요 시스템들이 중앙집중식으로 구성되어 장애 발생 시 업무가 마비될 수 있으므로 네트워크 스위치, 스토리지 등 중요장비 및 가상자산을 이중화하여야 하며 가용성을 보장하기 위해 백업체계를 구축
- 백업·비상복구·변경관리·침해사고대응 등 클라우드 컴퓨팅 시스템 운영의 전반적인 절차에 관한 표준운영절차(SOP) 등을 수립

⑮ 관리자 및 이용자에 대한 접근통제 및 격리 수단을 확보하여야 한다.

- 관리자가 이용자에 할당된 자원(메모리·HDD 등), 데이터에 임의 접근하지 못하도록 접근제어 및 격리 등을 통한 기술적 접근통제 수단을 마련
- 이용자가 본인에게 할당된 자원 이외의 자원에 접근하지 못하도록 기술적 통제 수단 마련(비정상 통신경로 발생 차단 등)

⑯ 클라우드에 저장 및 송수신되는 중요 업무자료를 암호화 한다.

- 해킹 및 비인가자에 의해 스토리지에 저장된 중요 업무자료 절취 시, 열람·실행이 불가토록 데이터를 암호화
- 해킹 및 비인가자에 의해 중요 업무자료 송수신 과정에서 스니핑 등의 공격으로 탈취 시, 열람·실행이 불가토록 송수신 자료의 암호화

- 저장 및 송수신되는 중요 업무자료를 암호화하기 위해 가상사설망·호스트 자료유출 방지 제품 등 정보보호 제품을 도입할 경우는 검증필 암호모듈 탑재제품을 이용(「국가 정보보안 기본지침」 참조)

⑰ 민간 클라우드 컴퓨팅 서비스에 대한 보안관제를 수행하여야 한다.

- 민간 사업자는 국가기관 등의 클라우드 컴퓨팅 서비스 보안관제 수행 및 정부보안관제체계와 연계하기 위해 필요한 제반환경을 지원하여야 함
- 이용 기관은 클라우드에 존재하는 기관 자원에 대한 사이버공격 정보를 수집, 분석, 대응하기 위해 클라우드에 적합한 보안관제 시스템을 구축하고 이에 대한 직접 보안관제를 수행하여야 함
- 다른 기관이 운영하는 보안관제시스템을 활용하는 것이 더 효율적인 경우에는 「국가사이버안전관리규정」 제10조의2에 따라 다른 기관의 보안관제센터에 위탁 가능
- 책임있는 보안관제 업무 수행 및 관리 등을 위해 보안관제에 필요한 전담 직원을 상시 배치해야 하며, 필요시 「국가사이버안전관리규정」 제10조의2 제4항에 따라 보안관제전문업체의 인원을 파견받아 보안관제 업무 수행
- 클라우드 내에 존재하는 자원에 대한 기술적·정책적 보안관제 방안 마련
- 클라우드에 구축된 보안관제 시스템은 정부보안관제체계와 연계되어야 하며, 세부사항은 국가정보원의 클라우드 보안관제 관련 별도 가이드라인(2023년 상반기 발간 예정)준용

⑱ 클라우드 가상화 보안 모니터링 및 관리를 강화하여야 한다.

- 민간 클라우드 컴퓨팅 서비스 내 가상 자원에 대한 모니터링 및 관리 수단 마련
- 가상화 환경 보안 강화 수단 마련

⑲ 클라우드 상호운용성을 지원할 수 있는 형태로 구축하여야 한다.

- 데이터와 클라우드 컴퓨팅 서비스가 특정 사업자나 회사로부터 종속되는 문제를 방지하기 위하여 표준화된 가상 이미지 포맷, 인터페이스, API를 지원할 수 있는 형태로 구축하여야 함

[SaaS 환경 추가 기본원칙]

⑳ SaaS 애플리케이션 보안성 강화 방안을 마련하여야 한다.

- SaaS 애플리케이션을 공유하는 다수의 사용자 간 자원 격리 방안 마련
- SaaS 애플리케이션 개발 및 운영 시 인터페이스 및 API의 취약점에 대한 주기적인 검증 수행
- SaaS 애플리케이션 설계 및 개발 단계에서 취약점을 제거하고 SaaS 운영 중에도 주기적으로 취약점 제거를 수행하여야 함
- SaaS 애플리케이션 접근을 위한 네트워크 프로토콜 보호 방안 마련
- SaaS 애플리케이션 관련 데이터(소스코드, 설정파일, 로그 정보 등)에 대한 보호 방안 마련

2. 세부 보안기준

기관이 민간 클라우드 컴퓨팅 서비스를 안전하게 이용하기 위한 세부 보안기준은 [표 14]와 같다. 정책, 클라우드 인프라, 가상환경 보안, 데이터, 인증 및 권한, 사고 및 장애 대응 영역에 대한 총 17개의 세부 보안기준이 있으며, 모든 민간 클라우드 컴퓨팅 서비스 유형에 적용해야 하는 공통 보안기준, IaaS 및 SaaS 환경에서 요구되는 추가 보안기준을 포함한다. 또한 PaaS 환경의 경우 SaaS 환경과 동일한 기준을 준용한다.

분류	세부 보안기준	적용범위		
		공통 보안기준	IaaS 추가 보안기준	SaaS 추가 보안기준
정책 (3)	시스템 보호	√	√	-
	인적 관리	√	-	-
	보안 감사	-	√	-
클라우드 인프라 (3)	설비	-	√	-
	하드웨어	-	√	
	가상화 인프라	√	√	√
가상환경 보안 (5)	보안 관리	√	√	-
	보안 관리 - SaaS 어플리케이션 개발	-	-	√
	보안 관리 - 개발·운영 환경	-	-	√
	악성코드 방지	√	-	-
	접근 통제	√	-	√
데이터 (2)	관리	√	-	√
	암호화	√	-	-
인증 및 권한 (2)	인증	√	-	-
	권한	√	-	-
사고 및 장애대응 (2)	사고	√	-	-
	장애	√	-	-

[표 14] 민간 클라우드 컴퓨팅 서비스 보안기준 분류

가. 정책

(1) 시스템 보호

[공통 보안기준]

① (보안요구사항 정의) 민간 클라우드 컴퓨팅 서비스 도입 시 관련 법률 및 지침, 보안 체계, 도입 기관 보안 사항 등을 고려한 보안 요구 사항을 정의하고 보안 SLA(Service Level Agreement)에 반영하여야 한다.

- 민간 클라우드 컴퓨팅 서비스를 운영하는 민간 사업자는 기관의 보안요구사항을 반영하여 보안대책을 수립하여야 함
- 다음과 같은 내용이 포함되도록 보안 요구 사항 정의
  - · 도입 및 운영 관련 관리 담당자 및 책임자 (공공기관 정보보안담당자, 시스템관리자, 민간 사업자 측 담당자 및 책임자 등)
  - · 도입 관련 참여 인력 정보
  - · 도입 및 운영에 투입할 인력 및 조직
  - · 정보보호 기능요구사항 및 기능명세
  - · 정보보호와 관련된 문서화 요구사항
  - · 정보보호 지침관련 요구사항 해결 방안
  - · 민간 클라우드 컴퓨팅 서비스를 운영하는 데이터센터의 물리적 위치
  - · 데이터가 저장되는 물리적 위치
  - · 안전성 확인을 위한 보안성 검증 계획
  - · 정보보호시스템 제품 유형별 도입 인증 요건 확인 및 검증필 암호모듈 탑재 대상 식별

② (보안책임 식별) 민간 클라우드 컴퓨팅 서비스 도입·운용에 있어서 해당 서비스 이용자와 관리자를 지정 운용하여야 한다.

- 서비스 이용자는 가상 PC, 가상 서버, 클라우드 기반 소프트웨어 등 클라우드 컴퓨팅 서비스를 이용하거나 본인 계정으로 클라우드 컴퓨팅 서비스에 접속함에 따른 보안책임을 가지며 이는 기관 내부의 정보시스템 자원을 이용할 때 준수하여야 할 보안책임과 동일한 책임이 유지되어야 함
- 이용기관의 관리자는 이용 기관 클라우드 컴퓨팅 서비스에 대한 계정 할당, 가상환경 유지, 보안 위협 관리 등과 같은 서비스 관리에 관련한 보안책임을 지님
- 민간 사업자는 이용 기관 클라우드 컴퓨팅 서비스 제공을 위한 클라우드 시스템 관리 책임을 지니며, 설비 유지, 시스템 운용에 대한 관리 대장 작성, 변경 최종 현황 유지 등과 같은 보안책임을 지님
- 민간 사업자는 이용 기관의 정보보안담당자에게 주기적으로 보안 관리 현황을 담은 보고서를 제출
- 이용기관의 정보보안담당관은 민간 클라우드 컴퓨팅 서비스 이용과 관련한 보안 취약점을 발견하거나 보안대책 강구가 필요하다고 판단할 경우, 사용자·관리자·민간 사업자에게 시정을 요구할 수 있음

③ (보안위협 식별) 민간 클라우드 컴퓨팅 서비스를 이용하여 다루고자 하는 업무 또는 데이터와 연관된 법령, 수행 요구사항, 정책, 규정, 표준, 가이드라인 등을 참고하여 보안 위협 대상을 식별하여야 한다.

- 클라우드 컴퓨팅과 관련된 물리적 설비, 하드웨어 장비, 가상 인프라, 가상머신 내 소프트웨어 등에 대한 보안위협 식별

④ (이전 정보자산 관리) 클라우드 컴퓨팅 환경으로 이전될 정보자산에 대한 관리정책을 마련하고 정보자산 목록 관리를 하여야 한다.

- 기밀성, 무결성, 가용성, 법적 요구사항 등을 고려하여 이전 여부를 결정하여야 함

  ※ 본 가이드라인 및 행정안전부의 『행정·공공기관 클라우드컴퓨팅서비스 이용 안내서』 참고

- 정보자산 이전 과정에서의 보안 위협 식별 및 보안 대책 마련

⑤ (형상 변경관리) 형상 변경에 영향을 받는 물리적·논리적 요소를 식별하고 형상 변경 사항을 지속적으로 확인 및 검토를 하여야 한다.

- 시스템 구성 하드웨어 자산목록, 가상 머신 내 운영체제 및 소프트웨어, 보안 정책 등의 기준 형상을 마련하고 이에 대한 변경 여부를 지속적으로 확인
- 형상 변경 시 영향을 받는 물리적·논리적 요소 정보, 변경 수행을 위해 시스템 및 서비스에 접근하는 접근 기록, 변경 사항 등의 기록을 생성
- 기준 형상 변경 시 기관 정보보안담당관에게 형상 변경에 따른 보안 영향 분석 결과를 보고

⑥ (클라우드 시스템 모니터링) 클라우드 컴퓨팅 환경 내 모니터링 수집 대상 및 위치를 정의하고 시스템 운영 상황, 장애 발생 대응 도구 동작 여부 등을 모니터링 하여야 한다.

- 다음을 포함한 모니터링 수집 대상 정의
  - · 사용자 접속
  - · 접속 단말 IP 혹은 MAC 값
  - · 보안 정책 이벤트
  - · 할당된 자원 사용 현황
  - · 운영 현황
  - · 비정상 행위

- 다음을 포함한 모니터링 수집 위치 정의
  · 클라우드 내부 네트워크와 외부 인터넷 망 간 경계
  · 클라우드 컴퓨팅 서비스 간 네트워크

⑦ (보안관제센터 설치·운영) 공공기관은 사이버공격 정보를 수집·분석·대응할 수 있는 자체 보안관제 체계를 구축하여야 하며, 불가피한 사유 시 위탁할 수 있다.

- 민간 사업자는 이용기관에 클라우드 컴퓨팅 서비스 보안관제 수행에 필요한 제반 환경을 지원하여야 함

⑧ (클라우드 운영환경 보안관리) 이용기관은 민간 사업자가 클라우드 컴퓨팅 서비스망을 대상으로 자체적으로 수행한 운용관리에 대한 보안 취약성 개선 결과를 주기적으로 보고받아야 한다.

⑨ (모의훈련 및 취약점 점검) 이용기관은 민간 사업자가 클라우드 컴퓨팅 서비스망에 대하여 자체적으로 실시한 모의훈련 및 취약점 점검 결과를 주기적으로 확인하여야 한다.

- 이용기관에 임차된 민간 클라우드 컴퓨팅 서비스망 및 자원에 직접적으로 영향을 미칠 수 있는 침투 테스트와 같은 모의훈련 수행 시 관련 정보를 이용기관과 민간 사업자 간에 공유하여야 함

(2) 인적 관리

[공통 보안기준]

⑩ (인적 접근관리) 이용기관은 민간 클라우드 컴퓨팅 서비스를 제공하는 시스템에 접근 가능한 사용자와 관리자를 식별하고 직무별 권한 부여, 폐기 등에 관한 절차를 마련하여야 한다.

- 인적 보안 정책에 따라 클라우드 시스템 접근 권한을 부여하고 주기적으로 권한에 대한 재심사 수행
- 퇴직 및 직무 변경 등의 상황이 발생한 경우 인적 보안 정책 및 절차에 따라 자산 반납, 접근 권한 폐기, 조정 등의 절차 수행

⑪ (정보보안 교육) 안전한 민간 클라우드 컴퓨팅 서비스 활용을 위한 정보보호 및 정보보호 관리 체계, 클라우드 보안 사고 사례, 사고에 따른 법적 책임, 사고 대응 방법 등이 포함된 직무별, 담당 분야별 교육을 주기적으로 수행하여야 한다.

- 민간 사업자는 자체 클라우드 관련 보안 교육을 주기적으로 실시하여야 하며, 시행 결과를 이용기관에 통보하여야 함
- 정기 정보보안 교육 미참석자는 보충 교육을 통해 필수로 교육을 이수하여야 함
- 클라우드 관련 정보보안 교육 및 기술 세미나 참석을 장려하는 등 정보보안 담당관의 업무 전문성을 제고하기 위하여 노력하여야 함

(3) 사후 추적을 위한 감사자료 관리

[IaaS 환경 보안기준]

⑫ (정보보안 감사) 이용기관은 정보보안 감사에 필요한 관련 자료에 대한 종류를 정의하고, 필요시에 민간 사업자에게 해당 감사 로그를 요청하고 열람하여야 한다.

⑬ (사후 추적을 위한 모니터링 및 로그관리) 보안 요구사항, 가용성 요구사항, 감사 요구사항, 법적 요구사항 등과 같은 요구사항들에 대한 준수 여부를 판별하기 위하여 다음과 같은 대상들에 대한 모니터링 및 로그관리를 수행하여야 한다.

- 사용자 계정 로그인 성공/실패 이벤트
- 계정관리 이벤트
- 데이터 접근
- 정책 변경
- 관리자 권한으로 실행하는 기능
- 시스템 이벤트

⑭ (로그 자료 보호) 로그 자료는 사후 추적대상을 식별할 수 있는 형태로 기록되고 1년 이상 보호되어야 한다.

- 사후 추적대상에 대한 사건유형, 발생일시, 발생장소, 사건발생 출처, 결과, 사건 관련 주체/이용자 식별정보 등을 알 수 있는 형태로 정보 기록
- 클라우드 시스템 접근 (단말PC, IP, 사용자ID, 시간, 작업내용 등) 관련 로그 기록을 1년 이상 유지 및 관리
- 비인가자에 대한 감사 저장소 접근을 방지
- 인가되지 않은 생성, 접근, 변경, 삭제 등으로부터 로그기록 보호

나. 클라우드 인프라

(1) 설비

[IaaS 환경 보안기준]

① (출입통제) 민간 사업자의 데이터센터 시설 내 이용 기관 클라우드 컴퓨팅 서비스 제공을 위한 시스템의 물리적 위치를 파악하고 접근이 가능한 모든 물리적 장소에 대한 출입 통제를 하여야 한다.

- 다음과 같은 물리적 보호 구역을 정의하고 관리
  - · 이용 기관 클라우드 컴퓨팅 서비스 운용 설비 및 시스템 구역
  - · 외부인 접견 구역
  - · 기타 사무실 구역
- 다음과 같은 물리적 보호 구역에 대한 보안대책을 포함
  - · 방재대책 및 외부로부터의 위해(危害) 방지대책
  - · 상시 이용하는 출입문은 한 곳으로 정하고 이중 잠금장치 설치
  - · 출입자 인증·식별 등을 위한 출입문 보안장비 설치 및 주야간 감시대책
  - · 휴대용 저장매체를 보관할 수 있는 용기 비치
  - · 정보시스템 안전지출 및 긴급파기 계획 수립
  - · 관리책임자 및 자료·장비별 취급자 지정 운용
  - · 정전에 대비한 비상전원 공급, 시스템의 안정적 중단 등 전력관리 대책
  - · 비상조명 장치 등 비상탈출 대책
  - · 카메라 장착 휴대폰 등을 이용한 불법 촬영 방지 대책 등

② (방재설비 구축) 화재, 전력 이상 등 인재 및 자연재해 등에 대비하여 필요한 설비를 갖추고 있어야 한다.

- 다음과 같은 설비를 방재 및 위해 방지 대응에 포함
  · 화재감지 및 소화설비
  · 누수감지기
  · CCTV, 외부침입감지 및 경보, 출입통제시스템
  · 파손 방지
  · UPS, 비상발전기, 전압유지기
  · 전력선 이중화

(2) 하드웨어

[IaaS 환경 보안기준]

③ (물리자산 관리) 민간 클라우드 컴퓨팅 서비스 운용에 필요한 물리 자산 목록을 유지하고 회수, 폐기 등의 자산 변화 상황을 반영하여야 한다.

- 서버, 네트워크 스위치 등의 물리 자산에 대하여 자산번호, 바코드, 시리얼 번호 등과 같은 물리 자산 식별자를 정의하여 자산 변화 관리

④ (전자정보 저장매체 불용처리) 민간 클라우드 컴퓨팅 서비스 운용에 따른 전자정보 저장매체 불용처리 규정은 민간 사업자의 내부 지침을 따르되, 기관 필요에 따라 전자정보 저장매체 불용처리 관련 보안 요구사항을 계약 상 반영토록 하여야한다.

⑤ (하드웨어자원 미혼용) 이용 기관의 민간 클라우드 컴퓨팅 서비스 운용에 사용된 하드웨어 자원은 국가·공공기관 클라우드 컴퓨팅 서비스 제공을 위한 시스템에서만 사용되어야 한다.

- 국가·공공기관 클라우드 컴퓨팅 서비스 제공을 위한 전용 물리적 영역을 마련(본 가이드라인 제3장 제2절의 클라우드 영역 분류 참조)
- 회수된 국가·공공기관 클라우드 하드웨어 자원은 국가·공공기관 클라우드 컴퓨팅 서비스 제공을 위한 시스템에서만 사용

⑥ (네트워크 장비 보안 관리) 민간 클라우드 컴퓨팅 서비스 운용에 따른 네트워크 장비 보안 관리는 민간 사업자의 내부 관리 규정에 따르되, 기관 필요에 따라 네트워크 장비 보안 관리 관련 보안 요구사항을 계약상 반영토록 하여야 한다.

⑦ (유지보수) 민간 클라우드 컴퓨팅 서비스 운용에 따른 유지보수 보안관리 지침은 민간 사업자의 내부 관리 규정에 따르되, 기관 필요에 따라 유지보수 관련 보안 요구사항을 계약상 반영토록 하여야 한다.

- 유지보수 도중에 발생할 수 있는 비인가된 기존 형상 변경, 보안 위협 발견 등과 같은 예외적 상황에 대한 해당 정보를 제공받고 검토 방안을 마련하여야 함

⑧ (네트워크 보안) 민간 클라우드 컴퓨팅 서비스 외부로부터 발생하는 DDoS, 비인가 접속 등의 위협을 막기 위한 보안 대비책을 마련해야 하며 다음과 같은 내용을 포함한 네트워크 모니터링 및 통제를 수행하여야 한다.

- 보안·네트워크 장비는 콘솔에서 관리함을 원칙으로 하되, 장비 관리자의 접속 및 발주기관내 용역업체 작업장소에서의 접속의 경우, 기관 내 지정 단말기로부터의 접속·관리를 허용
- 비인가 네트워크(테더링 등) 사용 보안 대책 수립
- 불필요한 서비스 포트 제거
- 서비스 거부 공격에 대한 대비한 DDoS 대응 장비 등 도입
- 방화벽, IPS/IDS, 가상사설망(VPN) 등 정보보호시스템 도입
- 네트워크 장비 등 신규 전산장비 도입 시 기본(default) 계정을 삭제 또는 변경하고 시스템 운영을 위한 관리자 계정 별도 생성
- 펌웨어 무결성 및 소프트웨어·서버 운영체제 취약점과 최신 업데이트 여부를 주기적으로 확인하여 항상 최신 버전으로 유지
- 클라우드 시스템 내부와 외부 사이 간 네트워크 모니터링

※ 그 밖의 보안·네트워크 장비 설치·운용 시의 보안 고려사항은 「국가 정보보안 기본지침」의 보안·네트워크장비 보안 내용 참조

(3) 가상화 인프라

[공통 보안기준]

⑨ (가상자원 관리) 다음과 같은 가상자원에 대한 사용 목록을 유지하여야 한다.

- 가상 머신
- 가상 스토리지
- 가상 애플리케이션 등

⑩ (가상자원 회수) 가상자원 회수 시 가상자원 내에 존재하는 사용자 관련 데이터는 복구할 수 없는 형태로 삭제되어야 한다.

- 가상자원 회수 시 가상자원 내에 존재하는 사용자 개인정보, 업무 관련 자료, 설정 파일 등과 같은 사용자 관련 데이터를 복구할 수 없도록 데이터를 삭제하여야 함

⑪ (가상자원 모니터링) 가상자원에 대한 모니터링을 주기적으로 수행하여야 한다.

- 가상자원에 대한 변경 발생 시 이를 로깅하고 이에 대한 이벤트 발생
- 가상자원에서 발생한 네트워크 트래픽이 임의로 수집되지 않도록 가상 스위치 보안 정책 설정

⑫ (자산 이전 보안) 기존 정보시스템 환경에서 클라우드 가상환경으로 이전 시 자산 보호를 위한 암호화 등 안전한 이전 수단을 이용하여야 한다.

[IaaS 환경 추가 보안기준]

⑬ (하이퍼바이저 보안관리) 2단계 인증, IP기반 필터링 등 하이퍼바이저 관리 기능 및 관리자에 대한 접근 통제 방안을 마련하고 하이퍼바이저에 대한 업데이트 및 보안 패치를 최신으로 유지하여야 한다.

[SaaS 환경 추가 보안기준]

⑭ (가상화 인프라 보안성 확인) 『국가 클라우드 컴퓨팅 보안 가이드라인』의 보안기준을 준수하는 클라우드 컴퓨팅 인프라 상에서 SaaS환경을 구축·개발·운영하여야 한다.

- 『국가 클라우드 컴퓨팅 보안 가이드라인』의 보안기준을 준수하는 클라우드 컴퓨팅 인프라를 이용
- 국가정보원이 도입요건 확인을 완료한 민간 클라우드 인프라를 이용

다. 가상환경 보안

(1) 보안관리

[공통 보안기준]

① (개발 보안관리) 가상환경에서 시스템, 애플리케이션, SaaS 등을 자체 또는 외주로 도입 및 개발하고자 하는 경우 다음과 같은 보안대책을 수립하여야 한다.

- 개발 및 테스트를 위한 가상 개발환경은 운영 중인 클라우드 서비스 환경과 분리
- 가상 개발 환경에 대한 비인가 접근 통제
- 개발에 사용되는 소스코드 및 소프트웨어 보안관리
- 외부용역 업체와 계약하여 개발하고자 하는 경우 다음 사항을 추가적으로 준수
  - 외부인력 대상 신원확인, 보안서약서 징구, 보안교육 및 점검
  - 외부인력의 보안준수 사항 확인 및 위반 시 배상책임의 계약서 명시
  - 외부인력의 접근권한 및 제공자료 보안대책
  - 외부인력에 의한 자료 무단반출 여부 확인
- SaaS를 도입 및 개발하고자 하는 경우 [부록 3] “SaaS 구축 유형”을 참고하여 구축

[IaaS 환경 추가 보안기준]

② (인터넷 연결 가상PC 보안관리) 비인가자가 인터넷에 연결된 가상환경을 무단으로 조작하여 전산 자료를 절취, 위·변조 및 훼손시키지 못하도록 다음과 같은 보안 대책을 마련하여 사용자의 인터넷 연결 가상PC에 적용하여야 한다.

- 메신저·P2P·웹하드 등 업무에 무관하거나 보안에 취약한 프로그램과 비인가 프로그램·장치 설치 금지
- 특별한 사유가 없는 한 문서프로그램은 읽기 전용으로 운용
- 음란·도박·증권 등 업무와 무관한 사이트 접근 차단 조치
- 무단으로 업무자료의 작성·저장 및 소통을 금지하고 최신 백신을 활용하여 바이러스 감염 여부 등을 주기적으로 점검
- 그 밖에 보안관리와 관련한 사항은 「국가 정보보안 기본지침」의 단말기 보안을 준용

③ (가상PC 보안관리) 가상PC 사용자는 PC 등 단말기 보안 관리에 준하여 일체의 보안 관리 책임을 지니며, 기관은 다음과 같은 보안 대책을 마련하여 사용자의 가상PC에 적용하여야 한다.

- 가상PC 접속용 장비·자료(문서자료 암호화 비밀번호)·사용자(로그온 비밀번호)별 비밀번호를 주기적으로 변경 사용하고 지문인식·OTP 등 생체인식 기술과 2단계 인증 적용 권고
- 가상PC 작업을 일정 시간 중단시 비밀번호 등을 적용한 화면보호 조치
- 최신 백신 운용·점검, 침입차단·탐지시스템 등을 운용하고 가상 운영체제(OS) 및 각종 응용프로그램의 최신 보안 패치 유지
- 업무상 불필요한 응용프로그램 설치 금지 및 공유 폴더의 삭제
- 그 밖에 보안관리와 관련한 사항은 「국가 정보보안 기본지침」의 단말기 보안을 준용

④ (가상서버 보안관리) 서버 관리자는 가상머신을 할당받아 가상서버를 운용할 경우, 해킹을 통한 자료 절취, 위·변조 등에 대비한 보안대책을 수립·시행하여야 하며 세부사항은 「국가 정보보안 기본지침」의 서버 보안을 준용

⑤ (웹서버 등 공개용 가상서버 보안관리) 이용 기관 담당자는 비인가자의 가상서버 내 저장자료 절취 및 위·변조, 분산서비스거부(DDoS) 공격 등에 대비하기 위하여 국가정보원장이 안전성을 검증한 침입차단·탐지시스템 및 DDoS 대응시스템을 설치하는 등 보안대책을 마련하여야 한다.

- 비인가자의 공개서버 내 비공개 정보에 대한 무단 접근을 방지하기 위하여 사용자를 제한하고 불필요한 계정 삭제
- 공개서비스에 필요한 프로그램을 개발하고 시험하기 위하여 사용된 도구(컴파일러 등)에 대한 개발 완료 후 삭제를 원칙으로 함
- 공개가상서버의 보안관리에 관련한 그 밖의 사항에 대해서는 「국가 정보보안 기본지침」의 공개서버 보안을 준용

⑥ (가상머신 내 소프트웨어 보안관리) 가상머신 내에 보안 상 취약한 소프트웨어 설치 방지, 보안업데이트 등의 보안 관리 방안을 마련하여야 한다.

- 가상머신 내에 출처, 유통경로 및 제작자가 명확하지 않은 소프트웨어 설치 방지 및 탐지
- 주기적으로 소프트웨어에 대한 보안 패치 및 업데이트 실시

(2) 보안관리 - SaaS 애플리케이션 개발

[SaaS 환경 보안기준]

⑦ (SaaS 애플리케이션 인증 및 권한) SaaS 애플리케이션 설계 및 개발 단계에서 정책을 수립하여 사용 SaaS 애플리케이션 접근을 위한 안전한 인증 방안이 마련되어야 하고, 접근 권한및 관리 권한을 부여하여야 한다.

- SaaS 애플리케이션 설계 및 개발 시 기관의 인증 체계를 고려하여 안전한 인증 방안 적용하여야 함
- SaaS 애플리케이션 사용을 위한 권한 정책을 수립하고 그에 따른 사용 및 관리 권한을 부여하여야 함
- API 등을 통해 연동 서비스 호출 시 안전한 인증 방안 적용
- 인증 시 사용되는 인증키에 대한 보호 방안을 마련
- SaaS 사용자 데이터에 대한 접근 권한 정책을 수립하고 그에 따른 사용 및 관리 권한을 부여하여야 함

⑧ (SaaS 애플리케이션 기밀성) SaaS 애플리케이션의 데이터 처리(송·수신, 저장, 연산 등) 과정에서 데이터를 보호하기 위한 수단을 마련하여야 한다.

- SaaS 애플리케이션의 중요 데이터를 송·수신할 때에는 TLS 등의 암호화 프로토콜을 적용하여야 함
- SaaS 애플리케이션을 통해 생성된 사용자 데이터는 암호화 수단을 사용하여 안전하게 보호되어야 함
- SaaS 애플리케이션에서 사용되는 암호화키에 대한 보호 방안 마련

⑨ (연동서비스 호출 기밀성) SaaS 애플리케이션 설계 및 개발 단계에서 연동 서비스 호출 시 송·수신되는 인증 정보, 메시지 등을 보호하기 위한 수단을 마련하여야 한다.

- 연동 서비스 호출을 통한 데이터 송·수신시에 TLS 등의 암호화 프로토콜을 적용하여야 함
- 연동 서비스 인증에 사용되는 인증 정보에 대한 보호 방안 마련

⑩ (SaaS 애플리케이션 무결성) SaaS 애플리케이션 설계 및 개발 단계에서 사용자 데이터에 대한 무결성 검증 방안을 마련하여야 한다.

- SaaS 애플리케이션에서 처리되는 사용자 데이터의 위·변조 탐지를 위한 무결성 검증
- 연동 서비스 호출 시 송·수신되는 데이터에 대한 무결성 검증
- SaaS는 허가받은 연동 서비스와 연동되어야 함
- SaaS 사용자의 가상 자원 및 데이터가 사용자 별로 분리되어 안전하게 관리가 되어야 함
- SaaS 애플리케이션 개발 시 신뢰할 수 있는 소프트웨어만을 사용하고, 무결성 검증을 수행하여야 함

⑪ (SaaS 애플리케이션 가용성) SaaS 애플리케이션은 사용자 업무 연속성을 보장할 수 있는 형태로 설계 및 개발되어야 한다.

- 가용성에 대한 사용자 요구사항을 충족시킬 수 있는 형태로 SaaS 애플리케이션을 설계 및 개발하여야 함
- 가용성에 대한 사용자 요구사항을 충족시킬 수 있는 개발·운영 가상환경 및 클라우드 인프라 환경을 선정하여야 함

⑫ (SaaS 감사기록 관리) 보안 요구사항, 가용성 요구사항, 감사 요구사항, 법적 요구사항 등에 대한 준수 여부를 판별하기 위하여 SaaS에 대한 모니터링 및 로그 관리를 수행하여야 한다.

- 사용자 계정 로그인 성공/실패 이벤트
- 계정관리 이벤트
- 데이터 접근
- 정책 변경
- 관리자 권한으로 실행하는 기능
- 웹 기반으로 발생하는 이상행위

⑬ (SaaS 감사기록 보호) SaaS에서 생성된 로그 자료는 사후 추적대상을 식별할 수 있는 형태로 기록되고 1년 이상 보호되어야 한다.

- 사후 추적대상에 대한 사건유형, 발생일시, 발생장소, 사건발생 출처, 결과, 사건 관련 주체/이용자 식별정보 등을 알 수 있는 형태로 정보 기록
- 접근 (단말PC, IP, 사용자ID, 시간, 작업내용 등) 관련 로그 기록을 1년 이상 유지·관리
- 비인가자에 대한 감사 저장소 접근을 방지
- 인가되지 않은 생성, 접근, 변경, 삭제 등으로부터 로그기록 보호

⑭ (SaaS 애플리케이션 보안관리) SaaS 애플리케이션 보안을 위해 주기적 취약점 점검, 보안 업데이트 등의 보안 관리 방안을 마련하여야 한다.

- SaaS 애플리케이션을 대상으로 주기적인 취약점 점검, 최신 보안 패치, 업데이트, 침투테스트 등을 실시
- SaaS 구축에 사용되는 인터페이스 및 API에 대한 주기적인 보안점검 수행

⑮ (SaaS 애플리케이션 개발) 자체 또는 외주로 SaaS 애플리케이션 개발을 하고자 하는 경우 다음과 같은 보안대책을 수립하여야 한다.

- SaaS 보안취약점의 원인인 보안약점을 배제하도록 개발 단계 별 보안활동을 수행하여 개발하여야 함
- 출처, 유통경로 및 제작자가 명확하지 않은 소스코드 및 소프트웨어는 개발에 사용될 수 없음
- 개발에 사용되는 소스코드 및 소프트웨어 보안관리
- 외부용역 업체와 계약하여 개발하는 경우 다음의 사항을 추가적으로 준수
  - · 외부인력 대상 신원확인, 보안서약서 징구, 보안교육 및 점검
  - · 외부 인력의 보안준수 사항 확인 및 위반 시 배상책임의 계약서 명시
  - · 외부 인력의 접근권한 및 제공자료 보안대책
  - · 외부 인력에 의한 자료 무단반출 여부 확인

(3) 보안관리 - 개발·운영 환경

[SaaS 환경 보안기준]

⑯ (개발·운영 환경 인증 및 권한) 개발·운영 환경 접속을 위한 안전한 인증 방안이 마련되어야 하고, 접근 권한 정책을 수립하여 사용 및 관리 권한을 부여하여야 한다.

- 인증에 사용되는 인증정보 보호 방안을 마련하여야 함
- SaaS 개발 및 운영에 필요한 데이터(SaaS 애플리케이션 소스파일, 설정 파일, 관리 로그, 사용자 인증 정보 등)에 대한 접근 통제 정책을 마련하고, 그에 따른 이용·관리 권한을 부여하여야 함
- SaaS 개발 및 운영에 필요한 서비스 포트 외에 불필요한 서비스 포트를 제거하고, 관리용 서비스와 사용자용 서비스를 분리하여 운영하여야 함
- SaaS 가상 서버 및 가상 스토리지에 대한 접근 권한 정책 수립

⑰ (개발·운영 환경 기밀성) 개발·운영 환경 관리에 필요한 데이터 보호 방안을 마련하여야 한다.

- SaaS 애플리케이션 관련 데이터(소스파일, 설정 파일 등)를 개발·운영 환경으로 송·수신할 때에는 TLS 등의 암호화 프로토콜을 적용하여야 함
- 개발·운영 환경 관리에 필요한 데이터를 암호화하여 안전하게 저장 및 처리하여야 함
- 개발·운영 환경 내에서 사용되는 암호화키에 대한 보호 방안을 마련해야 함

⑱ (개발·운영 환경 무결성) 개발·운영 환경 내 저장된 SaaS 관련 데이터에 대한 무결성 검증을 수행하여야 한다.

- 개발·운영 환경에 저장된 SaaS 애플리케이션 관련 데이터(소스파일, 설정 파일 등)에 대한 무결성 검증
- 개발·운영 환경은 허가받은 연동 서비스와 연동되어야 함
- 개발·운영 환경 관리에 필요한 데이터는 사용자 별로 분리되어 관리되어야 함
- 개발·운영 환경 구축 시 신뢰할 수 있는 소프트웨어만을 사용하여 구축하고, 무결성 검증을 수행하여야 함
- SaaS를 개발하고 테스트 중인 개발 환경은 SaaS 운영 환경과 분리 구축되어 SaaS 운영환경 내 저장된 데이터, 설정값 등에 영향을 미치지 않도록 하여야 함

⑲ (개발·운영 환경 가용성) 개발·운영 환경은 SaaS 운영 연속성을 보장할 수 있는 형태로 구축되어야 한다.

- 가용성에 대한 사용자 요구사항을 충족시킬 수 있는 형태로 개발·운영 가상 환경을 구축하여야 함
- 가용성에 대한 사용자 요구사항을 충족시킬 수 있는 클라우드 인프라 환경을 선정하여야 함

⑳ (개발·운영 환경 감사기록 관리) 보안 요구사항, 가용성 요구사항, 감사 요구사항, 법적 요구사항 등에 대한 준수 여부를 판별하기 위하여 개발·운영 환경에 대한 모니터링 및 로그관리를 수행하여야 한다.

- 사용자 계정 로그인 성공/실패 이벤트
- 계정관리 이벤트
- 데이터(사용자 소스파일, 설정 정보, 로그기록 등) 접근
- 정책 변경
- 관리자 권한으로 실행하는 기능
- SaaS 가상머신 및 스토리지에 대한 이상행위

㉑ (개발·운영 환경 감사기록 보호) 개발·운영 환경 운영 중 생성된 로그 자료는 사후 추적대상을 식별할 수 있는 형태로 기록되고 1년 이상 보호되어야 한다.

- 사후 추적대상에 대한 사건유형, 발생일시, 발생장소, 사건발생 출처, 결과, 사건 관련 주체/이용자 식별정보 등을 알 수 있는 형태로 정보 기록
- 접근 (단말PC, IP, 사용자ID, 시간, 작업내용 등) 관련 로그 기록을 1년 이상 유지·관리
- 비인가자에 대한 감사 저장소 접근을 방지
- 인가되지 않은 생성, 접근, 변경, 삭제 등으로부터 로그기록 보호

㉒ (개발·운영 환경 보안관리) 개발·운영 환경 보안을 위해 주기적 취약점 점검, 보안 업데이트 등의 보안관리 방안을 마련하여야 한다.

- 개발·운영 환경 구축에 필요한 소프트웨어를 대상으로 주기적인 취약점 점검, 최신 보안 패치, 업데이트, 침투 테스트 등을 실시
- 개발·운영 환경 구축에 사용되는 인터페이스 및 API에 대한 주기적인 보안 점검 수행

㉓ (개발·운영 가상서버 보안관리) 개발·운영 환경 구축을 위해 가상서버를 운용할 경우, 해킹을 통한 자료 절취, 위·변조 등에 대비한 보안대책을 수립·시행하여야 하며 관련 세부 사항은 「국가 정보보안 기본지침」의 서버 보안을 준용하여야 한다.

㉔ (웹서버 등 공개용 개발·운영 가상서버 보안관리) 개발·운영 환경 구축을 위해 공개용으로 운영되는 가상서버를 운용할 경우, 비인가자의 가상서버 내 저장자료 절취 및 위·변조, 분산서비스거부(DDoS) 공격 등에 대비하기 위하여 국가정보원장이 안전성을 검증한 침입차단·탐지시스템 및 DDoS 대응시스템을 설치하는 등 보안대책을 마련하여야 한다.

- 비인가자의 공개서버 내 비공개 정보에 대한 무단 접근을 방지하기 위하여 사용자를 제한하고 불필요한 계정 삭제
- 공개서비스에 필요한 프로그램을 개발하고 시험하기 위하여 사용된 도구(컴파일러 등)에 대한 개발 완료 후 삭제를 원칙으로 함
- 공개 가상서버의 보안 관리에 관련한 그 밖의 사항에 대해서는 「국가 정보보안 기본지침」의 서버 보안을 준용

(4) 악성코드 감염방지

[공통 보안기준]

㉕ (악성코드 감염방지) 웜·바이러스, 해킹프로그램, 스파이웨어 등 악성코드에 의한 위협을 제거하기 위해 악성코드 방지 대책을 수립·시행하여야 한다.

- 가상머신 내 운영체제, 소프트웨어 등에 대한 주기적인 보안패치 실시
- 백신은 최신상태로 업데이트·상시 감시상태로 설정하고 주기적인 점검 실시
- 보안에 취약하고 업무상 불필요하거나 출처, 유통경로 및 제작자가 명확하지 않은 소프트웨어를 사용할 수 없으며 클라우드 컴퓨팅 외부에 있는 망으로 자료 입수 시 최신 백신으로 진단 후 사용
- 관리자는 사용 금지 대상 소프트웨어에 대한 설치 금지, 설치 탐지 등과 같은 보안 통제 방안을 마련하여 보안 관리하여야 함
- 외부 악성코드 위협 접근 통제를 위한 침입차단시스템 등의 보안 대책 마련

㉖ (악성코드 탐지 조치) 가상머신에 악성코드가 설치되거나 감염된 사실을 발견하였을 경우에 다음과 같은 조치를 하여야 한다.

- 악성코드 감염원인 규명 등을 위하여 감염된 가상머신 사용을 중지하고 격리 조치 수행
- 심각할 경우 감염 환경을 보존하고 원인 파악 이후 초기 상태로 복구
- 악성코드의 감염확산 방지를 위하여 정보보안담당관에게 관련 사실을 즉시 통보하여야 함
- 각급기관은 악성코드가 신종이거나 감염피해가 심각하다고 판단할 경우에는 관련 사항을 국가정보원장에게 신속히 통보하여야 함
- 각급기관은 국가정보원장이 해당 기관에 악성코드 감염사실을 확인하여 조치를 권고할 경우, 즉시 이행하여야 함
- 악성코드 감염의 확산 및 재발을 방지하기 위하여 원인을 분석하고 예방조치를 수행

(5) 접근 통제

[공통 보안기준]

㉗ (접근 제한 방안) 이동식 저장매체 사용 통제, 다중요소(Multi-factor) 인증, 자동 로그아웃 등을 포함하여 다음과 같은 접근 제한 방안을 마련하여야 한다.

- 클라우드 시스템에 대한 USB등의 이동식 저장매체 사용 통제
- 식별 번호가 등록된 이동매체만 사용
- 인증서(PKI)기반, OTP, MAC, 지문 등 다중요소(Multi-factor) 인증 제공
- 일정 시간 이상 업무 작업 중단 시 비밀번호 등이 적용된 화면보호 조치
- 일정 시간 이상 업무 작업 중단 시 자동 로그아웃 등이 적용된 보호 조치
- 주요 중요 기능에 대한 동일 사용자의 동시 세션 제한

㉘ (식별정보 관리) 사용자 및 장치를 유일하게 식별할 수 있는 식별 방법을 마련하고 식별 정보를 관리하여야 한다.

- 사용자를 유일하게 구분할 수 있는 식별자(아이디)를 할당하여 모든 사용자에 대한 책임 추적성 보장
- 관리자 및 특수권한 계정의 경우 추측 가능한 식별자(root, admin, administrator 등)의 사용 제한
- 시스템 설치 및 유지 이후 임시로 할당된 식별자 제거
- 계정 및 비밀번호의 유효 기간을 두고 만료 시 재발급 절차를 거쳐야함

㉙ (사용자계정 생성) 계정 유형 식별, 계정 그룹 설정 등을 담은 다음과 같은 계정 권한 생성 절차를 마련하여야 한다.

- 계정 유형 식별(즉, 개인 이용자, 그룹, 시스템, 응용프로그램, 게스트, anonymous, 임시 등)
- 계정 그룹 설정
- 클라우드 시스템 및 서비스 접근이 허용된 자에 대한 식별 및 접근권한 명세
- 계정 생성과 권한 설정 요청 기능 지원
- 게스트 또는 임시 계정에 대한 승인 및 모니터링
- 외부인에 대한 계정 부여 정책
- 사용자 및 관리자 업무 환경 변화에 따른 대응
- 계정 삭제 대상 식별
- 계정 삭제 대상 관리 정책

㉚ (사용자계정 관리) 다음과 같은 내용을 포함한 사용자계정 보안관리 방안을 마련하여 사용자계정(ID) 부여 및 보안 관리를 수행하여야 한다.

- 사용자별 또는 그룹별로 접근권한 부여
- 업무상 불가피하게 외부인에게 계정을 부여해야 하는 경우 이용기관 책임하에 필요 업무에 한하여 특정기간 동안만 접속할 수 있게 하는 등의 보안조치 강구 후 허용
- 사용자 식별 수단이 없는 사용자계정 사용 금지
- 사용자가 5회 이상에 걸쳐 로그인 실패 시 접속을 중단시키도록 설정하고 비인가자의 침입 여부를 확인 점검
- 직원의 퇴직 또는 보직변경 발생 시 사용하지 않는 사용자계정을 신속히 삭제
- 특별한 사안이 없는 한 유지보수 등을 위한 외부업체 직원에게 관리자계정 제공을 금지
- 사용자계정의 부여 및 관리 적합성 여부를 연2회 이상 점검

㉛ (비밀번호 관리) 다음과 같은 비밀번호 관리 방안을 마련하여야 한다.

- 숫자·문자·특수문자 등을 혼합하여 안전하게 설정하고 정기적으로 변경·사용하여야 한다.
- 사용자(ID)와 동일하지 않아야 하며, 개인 신상 및 부서명칭 등과 관계가 없도록 설정
- 사전에 등록된 단어는 사용을 피하며, 동일 단어 또는 숫자 반복 사용 금지
- 사용된 비밀번호 재사용 금지
- 여러 사람이 동일한 비밀번호로 접근하는 것을 금지하도록 권고
- 응용프로그램 등을 이용한 자동 비밀번호 입력기능 사용 금지

㉜ (접근 기록 관리) 접근 기록은 서비스 통제, 관리, 사고 발생 책임 추적성 등을 보장할 수 있는 형태로 기록되고 1년 이상 보관, 유지되어야 한다.

- 다음과 같은 접근 기록 대상을 포함
  - · 접속자, 클라우드 시스템 및 서비스, 가상 머신 내 소프트웨어, 가상 머신 등 접속 대상
  - · 로그 온·오프, 파일 열람·출력 등 작업 종류, 작업 시간
  - · 접속 성공·실패 등 작업 결과
  - · 클라우드 컴퓨팅 망 외부로의 데이터 전송 정보 등
- 비인가자의 접속 시도, 정보 위변조 및 무단 삭제 등의 의심스러운 활동이나 위반 혐의가 발생한 사실을 발견한 경우 즉시 신고
- 접근 기록은 정보보안 사고 발생 시 확인 등을 위하여 최소 1년 이상 보관하여야 하며 접근기록 위·변조 및 외부유출 방지 대책을 강구해야 함

[SaaS 환경 추가 보안기준]

㉝ (첨단 정보통신기기 보안관리) SaaS를 관리 또는 접속하기 위해 스마트폰·IoT기기·전자제어장비 등 첨단 정보통신기기를 활용하고자 하는 경우 자체 보안대책을 수립하여 시행하여야 한다.

라. 데이터

(1) 데이터 관리

[공통 보안기준]

① (데이터 분류) 이용 기관은 민간 클라우드 컴퓨팅 서비스 이용시 데이터 유형, 법적 요구사항, 민감도 및 중요도에 따라 데이터를 분류하고 관리하여야 하며, 민간 사업자에게도 동일한 분류 및 관리를 요청하여야 한다.

② (데이터 소유권) 이용 기관은 민간 클라우드 컴퓨팅 서비스를 이용하고자 할 때, 사업자와 서비스 수준 협약 단계에서 데이터의 소유권을 명확히 명시하여야 한다.

③ (데이터 무결성) 이용 기관 중요 데이터의 입·출력, 전송 또는 교환 및 저장에 대한 민간 사업자의 데이터 무결성 확인 방안이 마련되어야 한다.

④ (데이터 보호) 민간 사업자는 데이터에 대한 접근제어, 위·변조 방지 등 데이터 처리에 대한 보호 기능을 이용자에게 제공하여야 하며 이용 기관은 이를 확인하여야 한다.

⑤ (데이터 추적성) 이용 기관은 민간 클라이드 컴퓨팅 서비스 이용 시 이용 기관 데이터(백업자료 포함)의 물리적 위치를 확인하여야 하며 민간 사업자는 데이터를 추적하기 위한 방안을 제공하여야 한다.

⑥ (데이터 폐기) 민간 클라우드 컴퓨팅 서비스 이용의 종료, 이전 등에 따른 데이터 폐기 조치 시 이용 기관은 민간 사업자에게 관련된 모든 데이터 폐기를 요청하여야 하며 폐기된 데이터를 복구할 수 없도록 삭제되었는지 확인하여야 한다.

[SaaS 환경 추가 보안기준]

⑦ (데이터 격리성) 사용자별 데이터 보안 요구 사항 수준에 따라 물리적 또는 논리적으로 데이터를 사용자별로 분리할 수 있는 방안을 마련하여 SaaS 애플리케이션 및 개발·운영 환경을 구축하여야 한다.

⑧ (데이터 기밀성) 데이터 송수신, 연산, 저장 시 데이터 암호화 등의 수단을 적용하여 SaaS 애플리케이션 취약점 등을 이용한 보안 위협으로부터 데이터 노출 시 기밀성을 유지할 수 있어야 한다.

⑨ (데이터 무결성) SaaS 애플리케이션 및 개발·운영 환경에서 처리되는 중요 데이터에 대한 무결성 검증을 수행하여야 한다.

⑩ (데이터 추적성) SaaS 애플리케이션 및 개발·운영 환경에서 생성되는 중요 데이터에 대한 추적성을 보장하여야 한다.

- 사용자의 SaaS 애플리케이션 데이터 폐기 시 사용될 수 있도록 추적성을 보장할 수 있는 식별자를 제공하여야 함
- 사용자의 법적, 보안 요구사항 등에 따라 데이터 저장 위치 설정, 물리적 위치 추적성 보장 등을 제공하여야 함
- 제3자의 클라우드 서비스를 제공받아서 SaaS 환경을 구축하는 경우에도 제3자로부터 데이터 추적성을 보장받을 수 있어야 함

⑪ (데이터 폐기) SaaS 사용 종료 등의 이유로 인한 데이터 폐기 시 SaaS 환경 내에 존재하는 사용자 관련 데이터는 복구할 수 없는 형태로 삭제되어야 한다.

- 사용자의 SaaS 애플리케이션 사용 종료, 이전 등에 따른 데이터 폐기 조치 시 폐기된 데이터를 복구할 수 없도록 데이터를 삭제하여야 함
- 제3자의 클라우드 서비스를 제공받아서 SaaS 환경을 구축하는 경우에도 제3자의 클라우드 서비스로부터 사용자 데이터가 폐기되었음을 확인하여야 함

(2) 암호화

[공통 보안기준]

⑫ (데이터 처리) 이용 기관은 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.

⑬ (암호 정책 수립) 이용 기관은 민간 사업자와 협의하여 민간 클라우드 컴퓨팅 서비스에 저장 또는 전송 중인 중요 업무자료를 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.

⑭ (암호키 관리) 이용 기관은 민간 사업자와 협의하여 암호키 생성, 이용, 보관, 배포, 파기에 대한 내용을 담은 암호키 관리 절차를 수립하여야 하며 안전한 암호키 관리 여부를 확인하여야 한다.

- 암호키는 별도의 물리적으로 분리된 서버에 백업하고 최소 접근권한을 부여하여야 함

마. 인증 및 권한

(1) 인증

[공통 보안기준]

① (사용자 식별) 민간 클라우드 컴퓨팅 서비스에서 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.

② (사용자 인증) 민간 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.

③ (강화된 인증수단 이용) 이용 기관은 민간 클라우드 컴퓨팅 서비스를 이용할 때 인증서(PKI)기반, OTP, 지문 등 다중요소(Multi-factor) 인증을 통한 강화된 인증수단 사용을 권고

④ (기관 인증 체계 연동) 기관 필요에 따라 클라우드 접근 대상 별로 기관의 인증 체계와 연동할 수 있는 인증 시스템을 설계 및 구축하여야 한다.

(2) 권한

[공통 보안기준]

⑤ (사용자 등록 및 접근 권한 관리) 민간 클라우드 컴퓨팅 서비스 및 중요정보에 대한 접근을 통제하기 위하여 공식적인 사용자 등록 및 해지 절차를 수립하고 업무 필요성에 따라 사용자 접근 권한을 최소한으로 부여하여야 한다.

- 접근 대상, 권한부여절차, 권한 수준, 권한 부여조건 등의 내용을 사용자, 관리자의 접근 권한 관리절차에 포함
- 사용자 및 관리자 별 관리 절차 마련
- 권한 부여 조건을 정의하고 조건에 따라 사용자에 적합한 접근 수준을 지닌 권한 부여

⑥ (관리자 및 특수 권한 관리) 민간 클라우드 컴퓨팅 서비스 및 중요정보 관리 및 특수 목적을 위해 부여한 계정 및 권한을 식별하고 별도 통제하여야 한다.

⑦ (접근권한 검토) 민간 클라우드 컴퓨팅 서비스 및 중요정보에 대한 접근을 관리하기 위하여 접근권한 부여, 이용(장기간 미사용), 변경(퇴직 및 휴직, 직무변경, 부서변경)의 적정성 여부를 정기적으로 점검하여야 한다.

바. 사고 및 장애 대응

(1) 사고

[공통 보안기준]

① (사고 대응절차) 이용 기관은 침해사고 발생 시 민간 사업자로부터 발생내용, 원인, 조치현황 등을 신속하게 파악하고 「국가 정보보안 기본지침」 등에 명시된 사고 대응 절차를 수행하여야 한다.

- 민간 사업자는 침해사고 발생 시 침해사고 대응절차에 따라 법적 통지 및 신고 의무를 준수하여야 하며 이용자에게 발생내용, 원인, 조치사항 등을 신속하여 알려야 할 의무를 가짐
- 민간 클라우드 컴퓨팅 서비스 이용 시 침해사고 발생 시 신고의무와 신고의무 미이행 시 과징금 부과 등 제재사항을 계약서에 반영

② (침해사고 조사 및 대응) 이용 기관은 민간 클라우드 컴퓨팅 서비스 이용 계약시 민간 사업자의 사고조사에 대한 적극적인 협조 및 지원의무를 명시하여야 하며, 민간 사업자는 필요시 국가정보원 및 이용기관의 조사 요청에 협조하여야 함

- 클라우드 컴퓨팅 서비스를 제공하는 민간 사업자는 사고 또는 장애 발생 시 이용 기관의 사고·장애 대응 절차에 따라 해당 이용 기관, 대내·외 관련 기관 및 전문가와 협조체계를 구성하여 대응하여야 하며, 국가정보원 및 이용 기관의 사고·장애 대응에 적극 협조하여야 함

(2) 장애

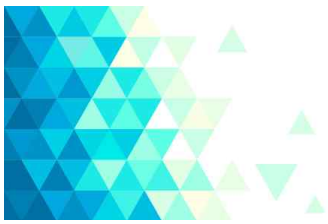
[공통 보안기준]

③ (장애 대응절차 수립) 민간 사업자는 관련 법률에서 규정한 클라우드 컴퓨팅 서비스의 중단으로부터 업무 연속성을 보장하기 위해 백업, 복구 등을 포함하는 장애 대응절차를 마련하여야 하며 이용기관은 장애 대응 요구사항, 담당자 정의 및 연락처 등을 담은 장애 대응절차를 마련하여야 한다.

- 다음과 같은 내용을 장애 대응 절차에 포함
  - · 장애 대응 계획서
  - · 도입 기관의 장애 대응 요구사항
  - · 장애 대응 관련 담당자 정의 및 연락처
  - · 이용 기관의 민간 클라우드 컴퓨팅 서비스를 운영하는 시스템 파기, 훼손 및 장애 시 정상적인 업무 유지에 필요한 핵심 기능
  - · 이용 기관의 민간 클라우드 컴퓨팅 서비스를 운영하는 시스템 복원 시 보안성에 영향을 미치는 요소
  - · 업무연속성 관련 인력 및 조직

④ (장애 처리 및 복구) 이용 기관은 서비스 수준 협약에 업무영향도 평가 등을 통해 산정한 복구시간을 서비스 수준 협약(SLA)에 반영하여야 하며 민간 사업자는 서비스 수준 협약(SLA)에 명시된 시간 내에 장애 대응절차에 따라 해당 서비스의 장애를 처리하고 복구시켜야 한다.

⑤ (재발방지) 이용 기관은 민간 사업자와 협의하여 장애 관련 정보를 활용하여 유사한 서비스 중단이 반복되지 않도록 장애 재발방지 대책을 수립하고, 필요한 경우 장애 대응 절차도 변경하여야 한다.



부 록

[부록 1] 민간 클라우드 도입 정보화사업 보안 특약 (예시)

1. 클라우드 컴퓨팅 서비스 사업자는 OOO의 보안정책을 위반하였을 경우 OOO의 사업자 보안위규 처리 기준에 따라 위규자 및 관리자를 행정조치 하고 OOO의 보안 위약금 부과 기준에 따라 보안 위약금을 OOO에게 납부한다.

2. 클라우드 사업자는 사업 수행에 사용되는 문서, 인원, 장비 등에 대하여 물리적, 관리적, 기술적 보안대책 및 OOO의 누출금지 대상정보에 대한 보안관리계획을 사업제안서에 기재해야 하며, 해당 정보 누출시 OOO은 국가계약법 시행령 제76조에 따라 사업자를 부정당업체로 등록한다.

3. 민간 클라우드 도입 정보화사업 수행과정에서 취득한 자료와 정보에 관하여 사업수행 중은 물론 사업 완료 후에도 이를 외부에 유출해서는 안 되며, 사업완료시 정보보안 담당자의 입회하에 완전 폐기 또는 반납해야 한다.

4. 클라우드 사업자는 사업 최종 산출물에 대해 정보보안전문가 또는 전문보안 점검도구를 활용하여 보안 취약점을 점검, 도출된 취약점에 대한 개선을 완료하고 그 결과를 제출해야 한다.

5. 클라우드 사업자는 OOO의 클라우드 도입 및 운영 보안 요구사항 충족시켜야 하며, 보안 요구사항에 근거가 되는 법, 가이드라인, 절차 등은 다음과 같다.

   가. 「국가정보원법」 및 「사이버안보 업무규정」

   나. 「전자정부법」과 동법 시행령

   다. 「정보통신기반보호법」과 동법 시행령

   라. 「국가 정보보안 기본지침 (국가정보원)」

   마. 「국가 클라우드 컴퓨팅 보안 가이드라인 (국가정보원)」

바. 「국가·공공기관 업무 전산망 분리 및 자료전송 보안 가이드라인 (국가정보원)」

사. 「안전한 정보통신 환경 구현을 위한 네트워크 구축 가이드라인 (국가정보원)」

아. 「국가·공공기관 용역업체 보안관리 가이드라인 (국가정보원)」

6. 클라우드 사업자는 OOO이 보안 요구사항 준수 모니터링, 외부 위협 대응, 국가·공공기관 데이터 보호 등의 목적으로 클라우드 사업자의 시설, 모니터링 로그, 문서, 데이터베이스 등에 접근하는 것을 허용하여야 하며, OOO은 OOO 이외의 他 클라우드 컴퓨팅 서비스 임차인 자원에 침범하지 않는 한에서 접근 및 관련 정보를 수집할 수 있다.

7. 클라우드 사업자는 OOO의 클라우드 보안관제 수행 및 정부보안관제체계와 연계하기 위한 제반환경 지원에 적극적으로 협조해야 한다.

8. 클라우드 사업자는 국가정보원 및 OOO이 클라우드 컴퓨팅 서비스 망 운용 관리에 따른 보안 취약점 개선·발굴, 사이버공격 위협에 대한 예방, 대응, 실태평가, 안전성 및 보안대책의 적합성과 이행여부 확인 등의 목적으로 클라우드 사업자 시설에 대한 현장실사 방문, 안전성 보안 측정 실시, 보안진단·점검 등 수행 요청 시 이에 성실히 응해야한다.

9. 클라우드 사업자는 국가정보원 및 OOO이 8항의 현장실사, 안전성 보안측정 실시, 보안점검 등 수행 목적으로 기술적 지원을 요청할 시에 모니터링 도구, 로그 수집 기술 등의 제반 환경을 제공하여야 하며, OOO의 기본 형상 변경에 대한 실시간 모니터링 수행 및 형상 변경 결과 보고를 OOO에게 하여야 한다.

10. 클라우드 사업자는 사고 또는 장애 발생 시 OOO의 사고·장애 대응 절차에 따라 OOO의 정보보안담당자, 대내외 관련 기관 및 전문가와 협조체계 구성하여 대응하여야 하며, 국가정보원 및 OOO의 사고·장애 대응 및 예방보안 활동 등에 적극적으로 협조해야 한다.

11. 클라우드 사업자는 OOO의 데이터 보안 규격에 따라 OOO의 데이터를 검증필 국가표준암호화 암호모듈을 사용하여 전자적으로 안전하게 처리하여야 하며, OOO의 데이터가 OOO의 서비스 및 시스템 영역 외에서 사용되는 것을 방지하여야 한다.

[부록 2] SaaS 구축 유형

1. SaaS 구축 유형

<table>
<tr><th colspan="2">구분</th><th colspan="4">SaaS 환경 구축 유형 및 특징</th></tr>
<tr><td rowspan="3">SaaS 환경 구축 유형</td><td rowspan="2">구축 형태</td><td colspan="2">국가·공공기관 구축 클라우드 컴퓨팅 인프라</td><td colspan="2" rowspan="2">민간 클라우드 컴퓨팅 인프라(3)</td></tr>
<tr><td>내부구축(1)</td><td>커뮤니티 구축(2)</td></tr>
<tr><td>개발 주체</td><td colspan="2">기관</td><td>기관</td><td>민간</td></tr>
<tr><td rowspan="5">보안 관리</td><td>클라우드 인프라</td><td>기관</td><td>커뮤니티 구축기관</td><td>민간</td><td>민간</td></tr>
<tr><td>개발·운영 환경</td><td>기관</td><td>커뮤니티 구축기관</td><td>민간</td><td>민간</td></tr>
<tr><td>SaaS 개발·운영</td><td>기관</td><td>커뮤니티 구축기관/기관</td><td>기관</td><td>민간</td></tr>
<tr><td>SaaS 이용</td><td>기관</td><td>기관</td><td>기관</td><td>기관</td></tr>
<tr><td colspan="2">이용기관 보안통제수준</td><td>상</td><td>중</td><td>하</td><td>하</td></tr>
</table>

[표 15] SaaS 환경 구축 유형

(1) 국가·공공기관 구축 클라우드 컴퓨팅 인프라 : 내부 구축

(2) 국가·공공기관 구축 클라우드 컴퓨팅 인프라 : 커뮤니티 구축

(3) 민간 클라우드 컴퓨팅 인프라 이용

○ 『국가·공공기관 구축 클라우드 컴퓨팅 인프라-내부 구축』은 SaaS 도입 기관이 내부에 구축된 클라우드 컴퓨팅 인프라 상에 SaaS를 도입하여 이용하는 경우로 기관 보안 통제 수준이 높고, 대부분의 보안관리 책임이 기관에 있음

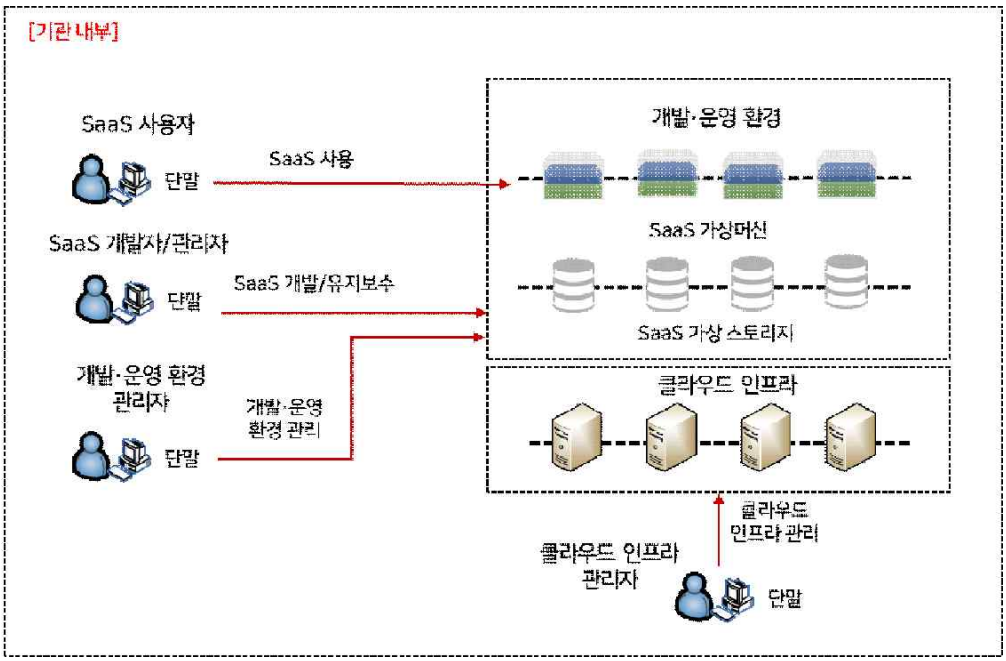
○ 『국가·공공기관 구축 클라우드 컴퓨팅 인프라-커뮤니티 구축』은 정부통합전산센터와 같이 여러 기관이 공유하는 커뮤니티 클라우드 컴퓨팅 인프라에 구축된 SaaS를 도입 기관이 이용하는 형태이고, 도입 기관 내부에 구축하는 것보다 보안 통제 수준이 낮으며, 커뮤니티 클라우드 컴퓨팅 인프라 구축기관과 도입 기관이 보안관리 책임을 공유함

○ 『민간 클라우드 컴퓨팅 인프라』 중 기관 SaaS 개발은 민간 클라우드 컴퓨팅 인프라에 도입 기관이 직접 SaaS를 개발하고 이용하는 경우로 취약점 제거, 보안패치 개발 등 기관이 개발과 관련된 보안 활동 통제

○ 『민간 클라우드 컴퓨팅 인프라』 중 민간 SaaS 개발은 민간 사업자에 의해 개발되어 민간 클라우드 컴퓨팅 인프라에서 운영 중인 SaaS를 도입 기관이 이용하는 경우로 개발과 관련된 보안 활동을 민간 사업자에게 위탁 운영

2. SaaS 구축 유형별 보안관리 범위

가. 국가·공공기관 구축 클라우드 컴퓨팅 인프라 이용 : 내부 구축



[그림 14] 국가·공공기관 구축 클라우드 컴퓨팅 인프라 이용 : 내부 구축

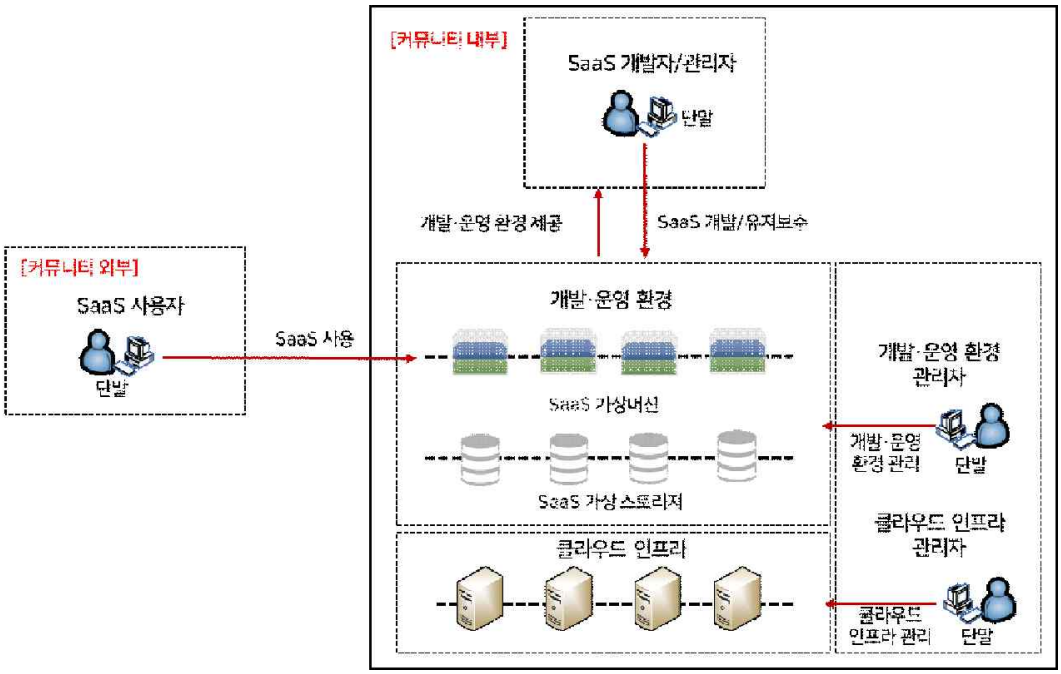
『국가·공공기관 구축 클라우드 컴퓨팅 인프라-내부 구축』 유형은 도입 기관이 자체적으로 클라우드 컴퓨팅 인프라를 포함한 모든 SaaS 환경의 각 구성요소를 구축·개발·운영하는 형태이다. [그림 14]와 같이 도입 기관 내부에서 개발·운영 환경 구축, SaaS 개발, 클라우드 인프라 구축이 이루어지기 때문에 기관 보안 통제 수준이 높고 모든 보안 관리의 책임이 도입 기관에게 있다.

본 구축 유형으로 SaaS 환경을 구축하는 도입 기관은 [표 16]의 각 주체 별 보안관리 범위를 식별하고, 이에 대한 보안책임 사항을 주지하여야 한다.

주체	보안관리 범위
도입 기관 (SaaS 사용자/ SaaS 개발·관리자/ 개발·운영 환경 관리자/ 클라우드 인프라 관리자)	• SaaS 사용 관련 보안 • SaaS 애플리케이션 개발 및 유지보수 • SaaS 애플리케이션 취약점 점검 • 개발·운영 가상환경 구축 및 운영 • SaaS 가상머신 및 가상 스토리지 관리 • 클라우드 인프라/개발·운영 환경 보안관리 • 클라우드 인프라/개발·운영 환경 사고·장애 대응

[표 16] (보안관리 범위) 국가·공공기관 구축 클라우드 컴퓨팅 인프라 이용 : 내부 구축

나. 국가·공공기관 구축 클라우드 컴퓨팅 인프라 이용 : 커뮤니티 구축



[그림 15] 국가·공공기관 구축 클라우드 컴퓨팅 인프라 이용 : 커뮤니티 구축

『국가·공공기관 구축 클라우드 컴퓨팅 인프라-커뮤니티 구축』 유형은 커뮤니티 클라우드 컴퓨팅 인프라에서 개발되어 운영 중인 SaaS를 도입 기관이 이용하는 형태이다. [그림 15]와 같이 커뮤니티 클라우드 컴퓨팅 인프라 내에 클라우드 인프라, 개발·운영 환경, SaaS 가상머신 및 가상 스토리지 등이 존재하고, 이에 대한 보안관리 책임을 커뮤니티 클라우드 컴퓨팅 인프라 구축기관과 도입 기관이 공유하게 된다.

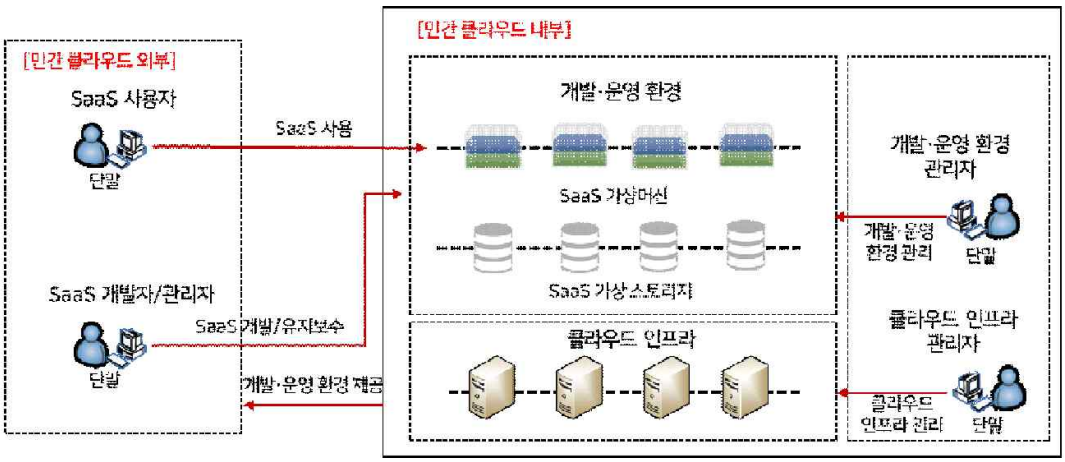
본 구축 유형으로 SaaS 환경을 구축하는 도입 기관은 [표 17]의 각 주체 별 보안관리 범위를 식별하고, 이에 대한 보안책임 사항을 주지하여야 한다.

주체	보안관리 범위
도입 기관 (SaaS 사용자)	• SaaS 사용 관련 보안
커뮤니티 구축 기관 (SaaS 개발·관리자 개발·운영 환경 관리자/ 클라우드 인프라 관리자)	• SaaS 애플리케이션 개발 및 유지보수 • SaaS 애플리케이션 취약점 점검 • 개발·운영 환경 구축 및 운영 • SaaS 가상머신 및 가상 스토리지 관리 • 클라우드 인프라/개발·운영 환경 보안관리 • 클라우드 인프라/개발·운영 환경 사고·장애 대응

[표 17] (보안관리 범위) 국가·공공기관 구축 클라우드 컴퓨팅 인프라 이용 : 커뮤니티 구축

다. 민간 클라우드 컴퓨팅 인프라 이용

1) 도입 기관에서 SaaS를 자체 개발하고 이용



[그림 16] 민간 클라우드 컴퓨팅 인프라 이용 : 기관 SaaS 개발

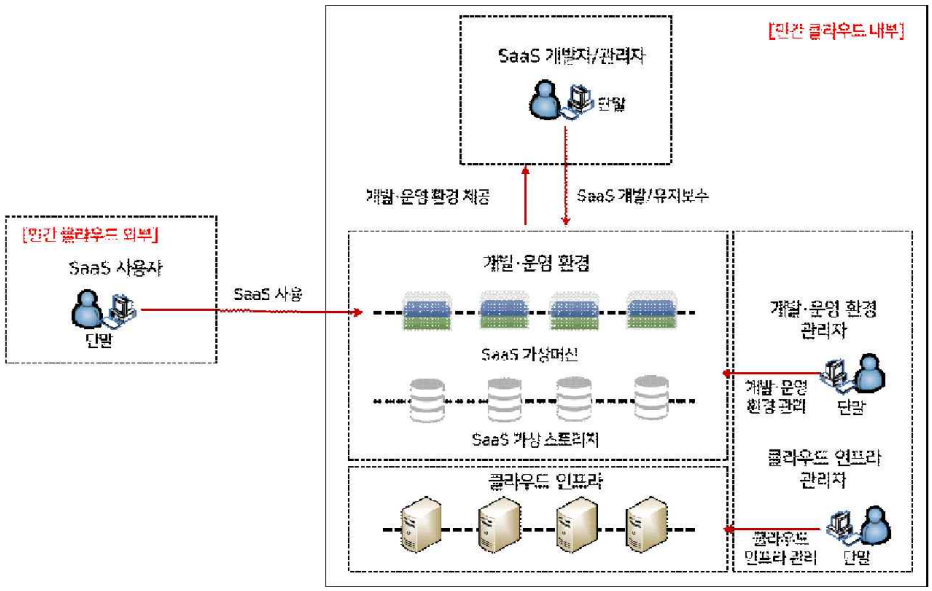
『민간 클라우드 컴퓨팅 인프라 - 기관 개발』 유형은 민간 클라우드 컴퓨팅 인프라 내에서 도입 기관이 자체적으로 SaaS를 개발하고 이용하는 형태이다. [그림 16]과 같이 도입 기관에서 SaaS 개발을 수행하기 때문에 보안 취약점 제거, 보안 패치 등과 같은 보안 활동을 직접 수행하게 된다. 하지만 민간 사업자 내부의 개발·운영 환경을 이용하고 대부분의 SaaS 관련 데이터들이 도입 기관 외부에 저장되기 때문에 도입 기관의 데이터 보안 통제 수준이 낮다.

본 구축 유형에서 도입 기관은 [표 18]과 같은 보안관리 책임을 식별하고 이에 대한 책임 의무를 민간 사업자와 공유하여야 한다. 그리고 이에 대한 보안책임 사항을 민간 사업자와의 계약사항에 명확히 반영하여야 한다.

주체	보안관리 범위
도입 기관 (SaaS 사용자/ SaaS 개발·관리자)	• SaaS 사용 관련 보안 • SaaS 애플리케이션 개발 및 유지보수 • SaaS 애플리케이션 취약점 점검 • 민간 사업자 제공 서비스 보안성 확인
민간 사업자 (개발·운영 환경 관리자/ 클라우드 인프라 관리자)	• 개발·운영 환경 구축 및 운영 • SaaS 가상머신 및 가상 스토리지 관리 • 클라우드 인프라/개발·운영 환경 보안관리 • 클라우드 인프라/개발·운영 환경 사고·장애 대응

[표 18] (보안관리 범위) 민간 클라우드 컴퓨팅 인프라 이용 : 기관 SaaS 개발

2) 민간 사업자에 의해 개발된 SaaS를 도입 기관이 이용



[그림 17] 민간 클라우드 컴퓨팅 인프라 이용 : 민간 SaaS 개발

『민간 클라우드 컴퓨팅 인프라 - 민간 개발』 유형은 민간 사업자에 의해 개발되어 민간 클라우드 컴퓨팅 인프라에서 운영 중인 SaaS를 도입 기관에서 이용하는 형태이다. 본 유형에서는 도입 기관이 사용하는 SaaS에 관련된 대부분의 데이터들이 민간 사업자 내부 환경에 저장된다. 또한 SaaS 보안 취약점 제거, 보안 패치 등과 같은 SaaS 개발과 관련된 보안 활동을 민간 사업자에게 의존하게 되기 때문에 도입 기관의 보안 통제 수준이 낮다.

본 구축 유형에서 도입 기관은 [표 19]과 같은 보안관리 책임을 식별하고 이에 대한 책임 의무를 민간 사업자와 공유하여야 한다. 그리고 이에 대한 보안책임 사항을 민간 사업자와의 계약사항에 명확히 반영하여야 한다.

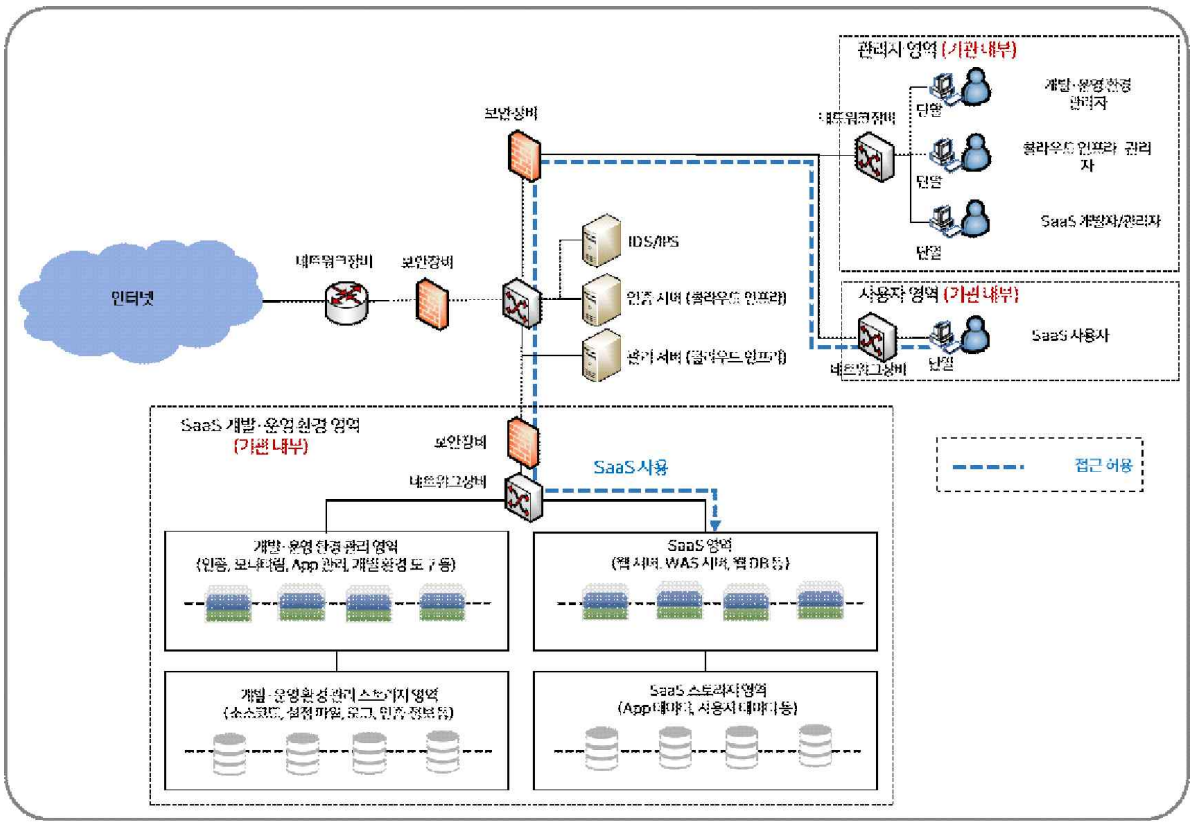
주체	보안관리 범위
도입 기관 (SaaS 사용자)	• SaaS 사용 관련 보안 • 민간 사업자 제공 서비스 보안성 확인
민간 사업자 (SaaS 개발·관리자 개발·운영 환경 관리자/ 클라우드 인프라 관리자)	• SaaS 애플리케이션 개발 및 유지보수 • SaaS 애플리케이션 취약점 점검 • 개발·운영 가상환경 구축 및 운영 • SaaS 가상머신 및 가상 스토리지 관리 • 클라우드 인프라/개발·운영 환경 보안관리 • 클라우드 인프라/개발·운영 환경 사고·장애 대응

[표 19] (보안관리 범위) 민간 클라우드 컴퓨팅 인프라 이용 : 민간 SaaS 개발

3. SaaS 구축 유형별 보안기준

가. 국가·공공기관 구축 클라우드 컴퓨팅 인프라 : 내부 구축

1) 기관 내부 SaaS 사용자에 의한 기관 내부 SaaS 접근



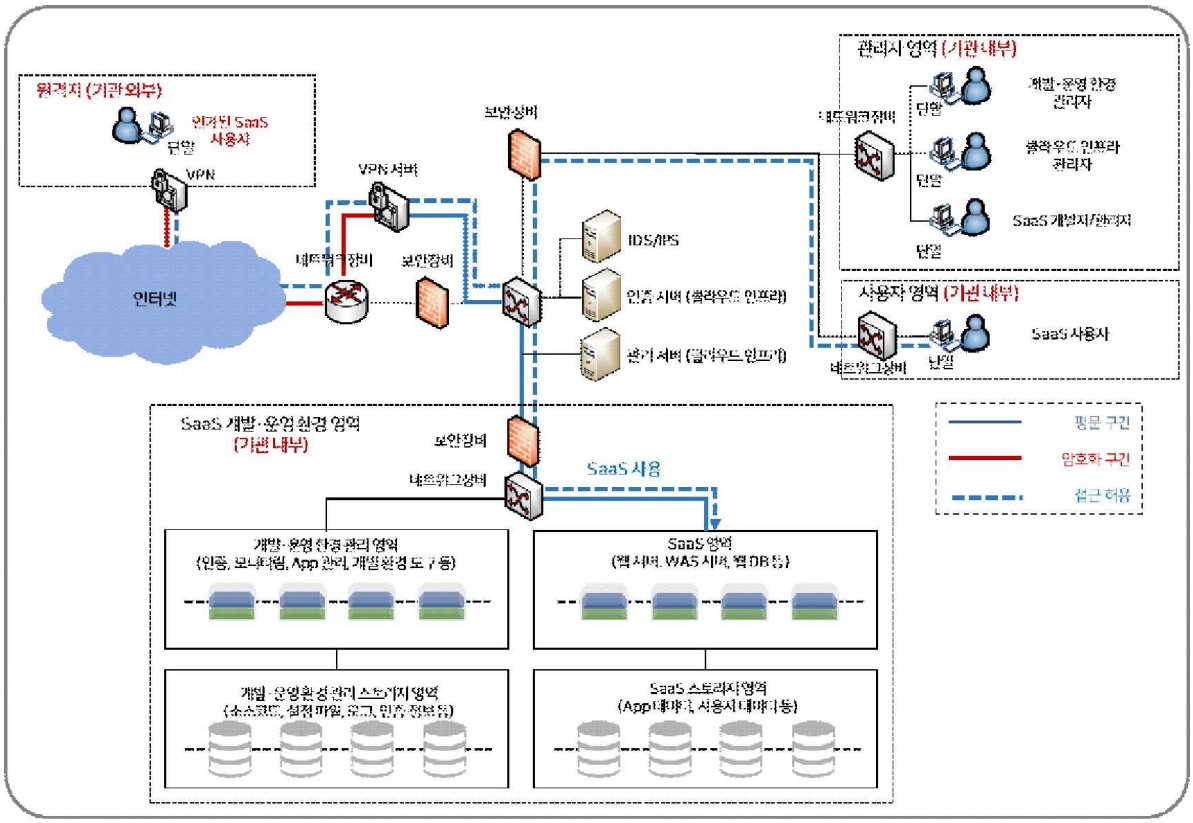
[그림 18] 기관 내부 SaaS 사용자에 의한 기관 내부 SaaS 접근

○ 기관 내부 SaaS 사용자는 기관 내부의 사용자 영역에 위치한 지정 단말을 통해 SaaS 접근이 가능함

○ 기관 내부 SaaS 사용자가 인터넷이 연결된 SaaS 사용 시 내부 업무 영역과 분리된 환경에서 접근이 가능함

○ 사용자 영역과 관리자 영역은 분리 운영되어야 하며, SaaS 환경 관리를 위한 단말을 지정하여 관리해야 함

2) 원격지에 위치한 인가된 SaaS 사용자에 의한 기관 내부 업무용 SaaS 접근



[그림 19] 원격지에 위치한 기관 내부 사용자에 의한 기관 내부 업무용 SaaS 접근

○ 원격지에 위치한 인가된 SaaS 사용자를 위한 VPN 서버를 두고, 원격근무 단말 내 설치된 VPN 클라이언트를 통해 VPN 서버 가상터널을 형성하여 암호화 통신을 하여야 함

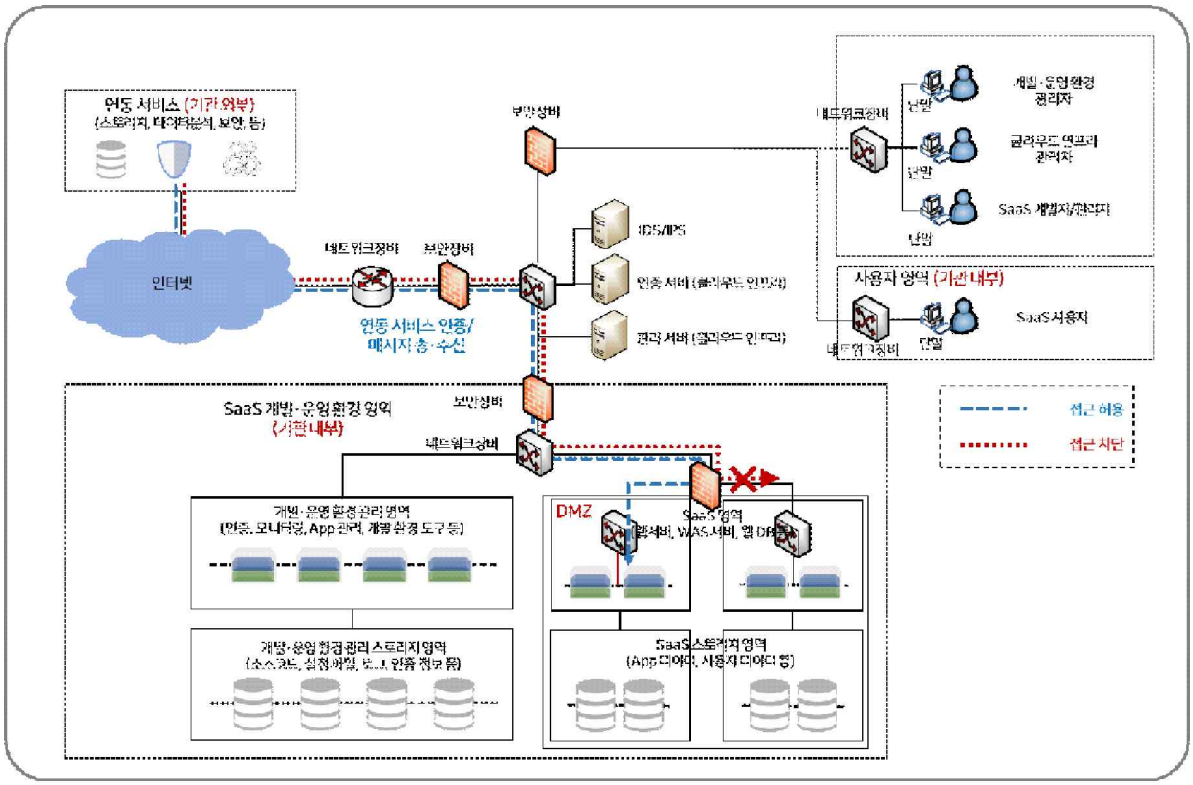
- 공인인증서, 휴대폰 인증 등을 수행하여 사용자 인증을 강화하여야 함

○ 원격지에 위치한 인가된 SaaS 사용자가 접근 가능한 SaaS 기능 및 영역을 제한하고 내부 침입차단시스템을 구축을 통해 접근 통제 수행

- 업무자료의 다운로드 및 저장을 차단하기 위한 자료유출방지시스템 구축

○ IDS, IPS 등의 보안 장비를 통하여 VPN 서버를 통해 내부로 유입되는 악성트래픽을 탐지 및 차단하여야 함

3) 기관 내부에 위치한 SaaS와 외부에 위치한 연동 서비스 간 연계



[그림 20] 기관 내부에 위치한 SaaS와 외부에 위치한 연동 서비스 간 연계

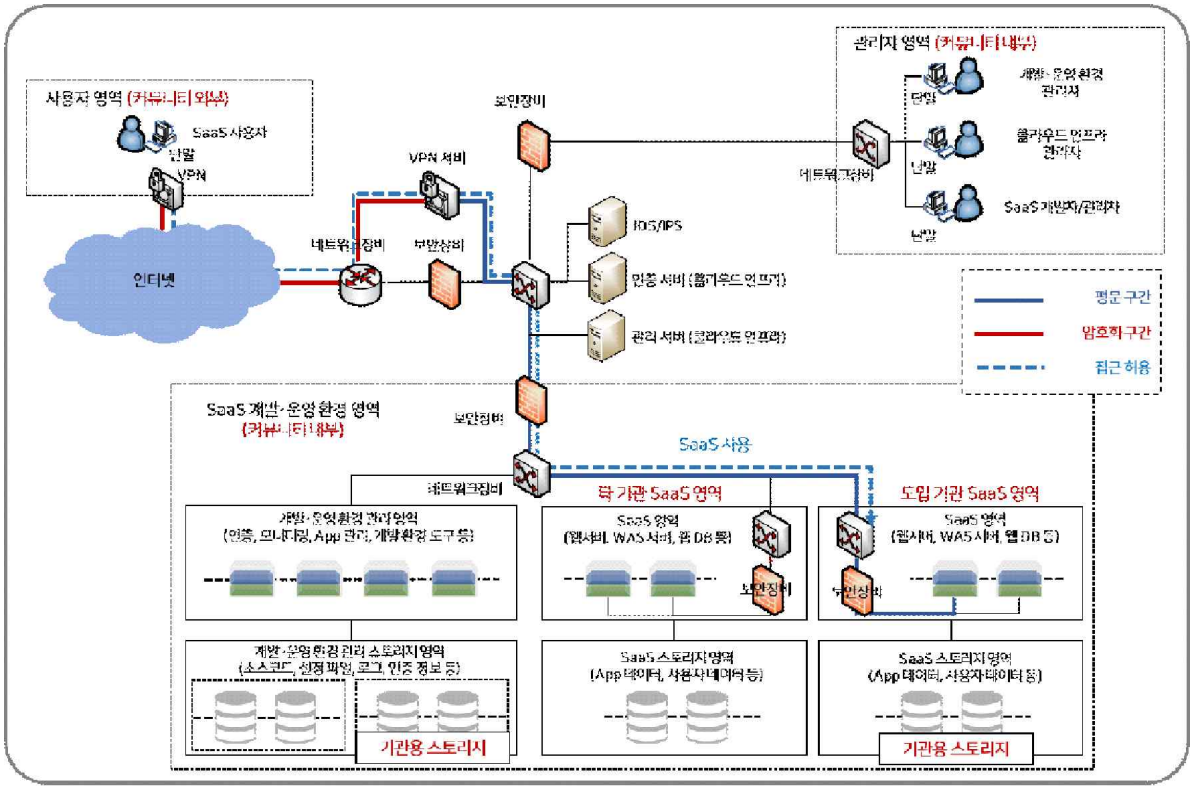
○ 외부 연동 서비스와 연계가 필요한 경우, SaaS 운영에 필요한 가상 머신, 스토리지 등을 DMZ 영역에 위치시키고, 연동 서비스와의 인증 및 중요 메시지 송·수신 시 암호화 등의 수단을 적용하여 보안 위협으로 노출된 데이터에 대한 기밀성을 유지하여야 함

○ 연동 서비스는 DMZ 영역 내부에 위치한 가상 머신과만 통신이 가능하며, 침입차단시스템을 이용하여 연동 서비스가 DMZ 영역이외의 SaaS 영역으로 접근하는 것을 차단하여야 함

○ DMZ 영역과 다른 SaaS 영역 간의 연계는 연계서버를 통해서만 이루어져야 하며, 그 외의 접근은 침입차단시스템을 이용하여 차단되어야 함

나. 국가·공공기관 구축 클라우드 컴퓨팅 인프라 : 커뮤니티 구축

1) 커뮤니티 클라우드 컴퓨팅 인프라에 위치한 업무용 SaaS에 기관 내부 SaaS 사용자 접근



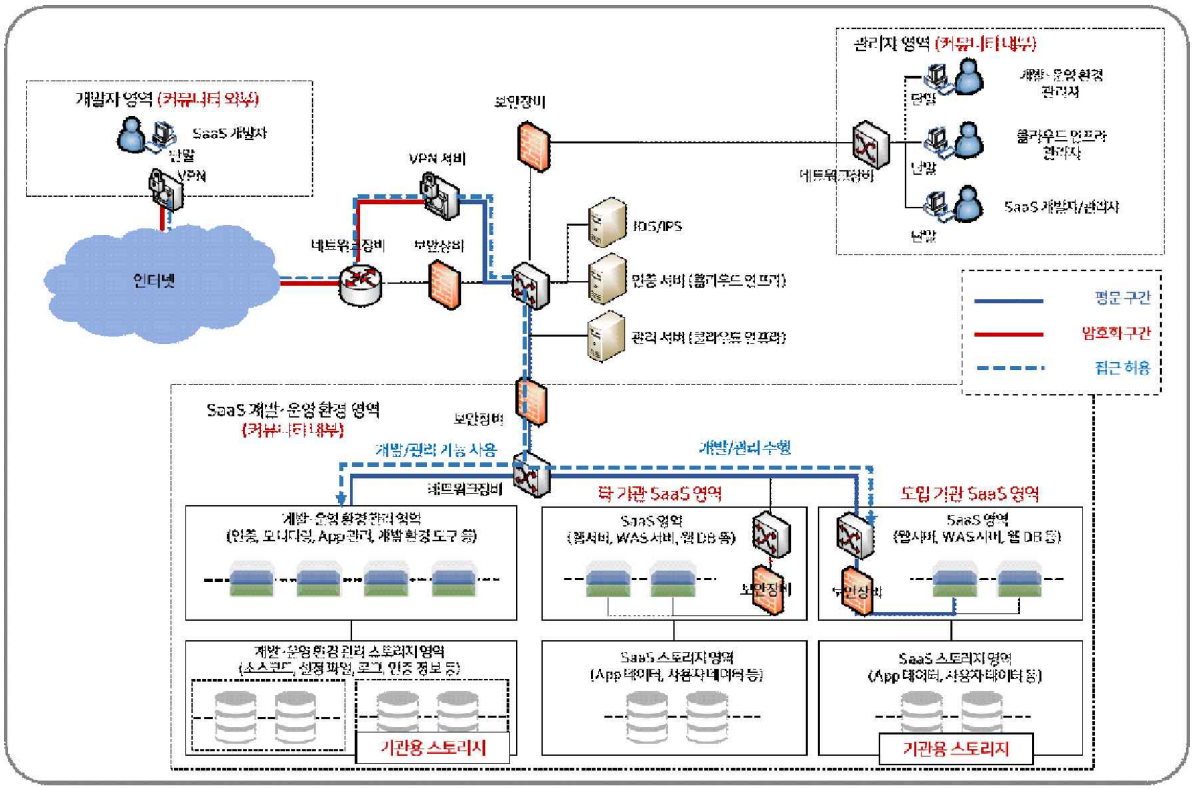
[그림 21] 커뮤니티 클라우드 컴퓨팅 인프라에 위치한 업무용 SaaS에 기관 내부 SaaS 사용자 접근

○ 도입 기관 내부 SaaS 사용자는 전용선 또는 암호화 통신(VPN 등)을 통하여 커뮤니티 클라우드 컴퓨팅 인프라에 구축된 도입 기관의 업무용 SaaS에 접근이 가능

○ 커뮤니티 클라우드 컴퓨팅 인프라에 구축된 도입 기관 SaaS 영역은 타 기관 SaaS 영역과 분리(물리적/논리적) 운영되어야 함

○ 도입 기관 SaaS를 위한 애플리케이션 및 개발·운영 가상환경 관리 관련 스토리지는 타 기관의 스토리지와 분리(물리적/논리적)되어 운영되어야 함

2) 커뮤니티 클라우드 인프라 내에 도입 기관 SaaS 자체 개발



[그림 22] 커뮤니티 클라우드 인프라 내에 도입 기관 SaaS 자체 개발

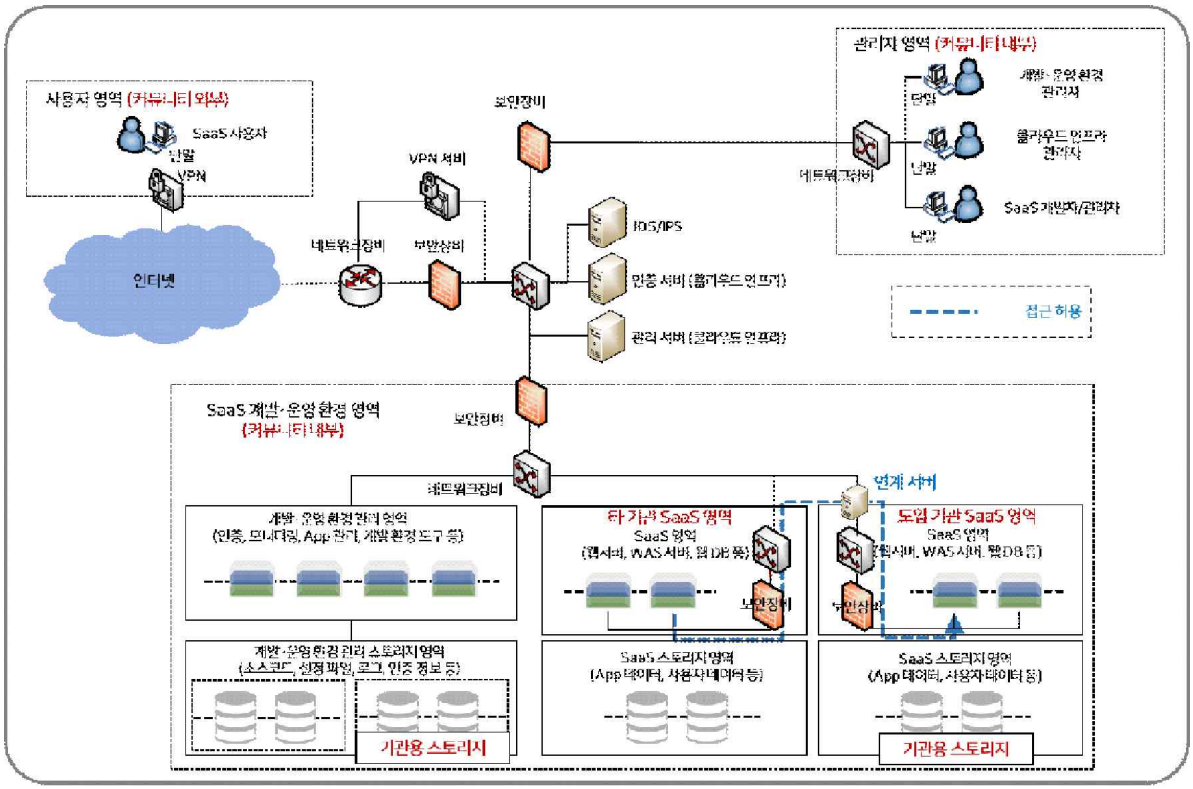
○ 커뮤니티 클라우드 컴퓨팅 인프라 내에서 도입 기관이 자체적으로 SaaS를 개발하는 경우 기관 내에 사용자 영역과 개발자 영역을 분리하여 개발을 수행하여야 함

○ 도입 기관 내부 SaaS 개발자는 기관 내부 개발자 영역에 위치한 지정 단말을 통해서 SaaS 개발을 수행하여야 함

○ 기관 내부 SaaS 개발자는 전용선 또는 암호화 통신(VPN 등)을 통하여 커뮤니티 클라우드 인프라에 구축된 개발·관리 기능에 접근 가능

- 개발/관리 기능을 이용하지 않고 기관에 할당된 SaaS 가상머신에 직접 개발·운영 환경을 구축하여 SaaS를 개발하는 경우도 전용선 또는 암호화 통신(VPN 등)을 이용한 통신을 하여야 함

3) 커뮤니티 클라우드 인프라 내 도입 기관 SaaS와 타 기관 SaaS 상호 연계



[그림 23] 커뮤니티 클라우드 인프라 내 도입 기관 SaaS와 타 기관 SaaS 상호 연계

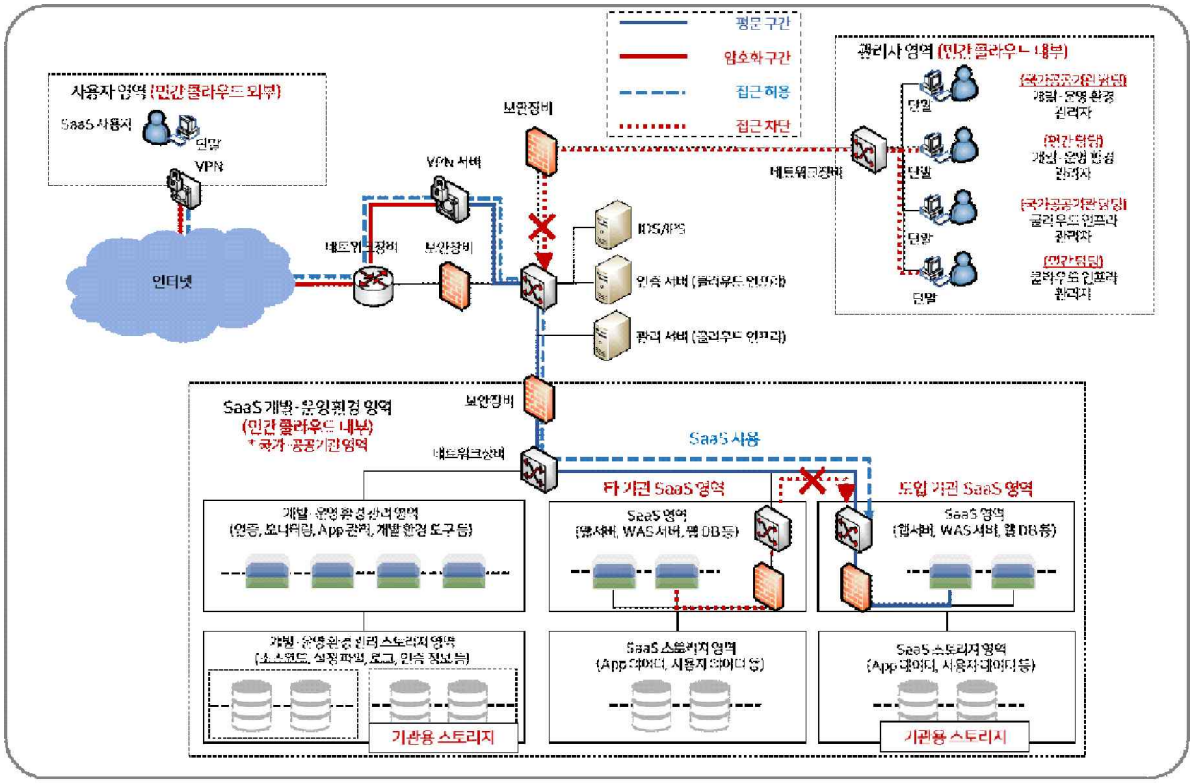
○ 커뮤니티 클라우드 컴퓨팅 인프라 상에 구축된 타 기관 SaaS와 도입 기관 SaaS 간의 통신은 연계 서버를 통해서만 가능하며 정보공유, 자료전송 등으로 제한

○ 도입 기관은 연계 서버 관리에 대한 보안관리 정책을 수립하고 이행

- 도입 기관의 보안정책 및 사용기준에 따라 접근 가능한 SaaS와 제한 SaaS를 정하고 접근 제어
- 타 기관에 제공될 수 있는 도입 기관의 접근 자료를 중요도에 따라 나누고, 자료 접근에 대한 인증 강화 방안 마련
- 타 기관 접근 인증 이후 SaaS 사용 이력에 대한 로그데이터 유지

다. 민간 클라우드 컴퓨팅 인프라 이용

1) 민간 클라우드 컴퓨팅 인프라에 구축된 도입 기관 업무용 SaaS에 기관 내부 SaaS 사용자 접근 - 『공통』



[그림 24] 민간 클라우드 컴퓨팅 인프라에 구축된 도입 기관 SaaS에 기관 내부 SaaS 사용자 접근

○ 기관 내부 SaaS 사용자는 전용선 또는 암호화 통신(VPN 등)을 통하여 민간 클라우드 컴퓨팅 인프라에 구축된 도입 기관의 업무용 SaaS에 접근이 가능

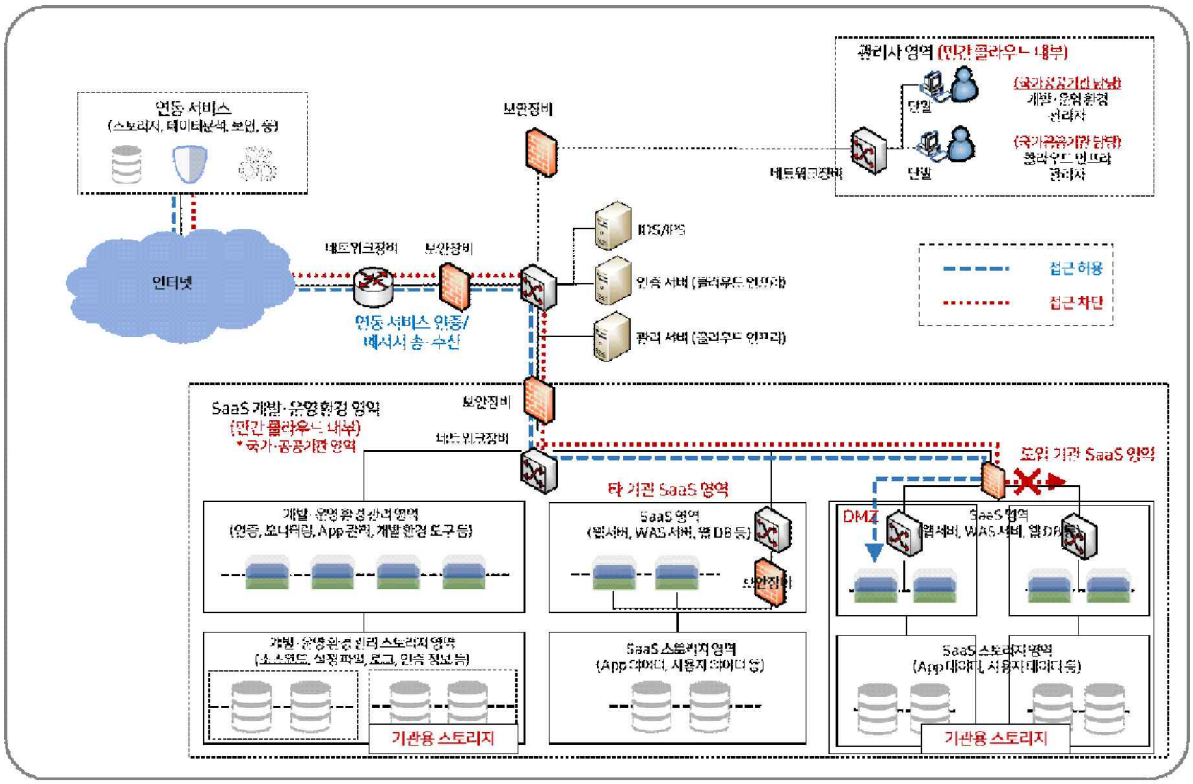
○ 민간 사업자는 민간 클라우드 서비스 영역과 공공기관 클라우드 서비스 영역을 물리적/논리적으로 분리하여 운영·관리를 수행 하여야 함

- 민간 서비스 영역을 담당하는 관리자에 대한 공공 영역 접근을 차단하여야 함

○ 도입 기관 SaaS 영역은 공공기관 영역 내에 존재하는 타 기관 SaaS 영역과 분리되어야 함

- 도입 기관 SaaS를 위한 애플리케이션 스토리지 및 개발·운영 가상환경 관리 관련 스토리지는 타 기관의 스토리지와 분리(물리적/논리적)

2) 기관 SaaS 영역 내 위치한 SaaS와 외부에 위치한 연동 서비스 간 연계 - 『공통』



[그림 25] 기관 SaaS 영역 내 위치한 SaaS와 외부에 위치한 연동 서비스 간 연계

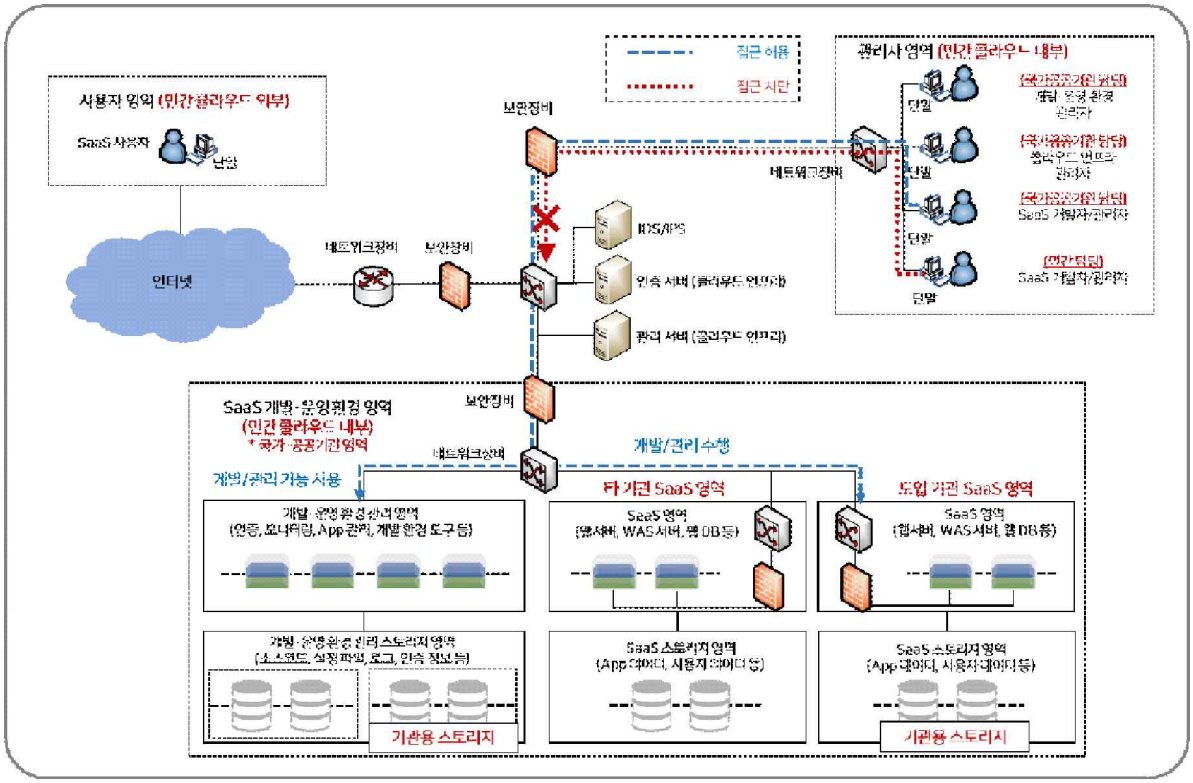
○ 외부 연동 서비스와 연계가 필요한 경우, SaaS 운영에 필요한 가상 머신, 스토리지 등을 DMZ 영역에 위치시키고, 연동 서비스와의 인증 및 메시지 송·수신 시 암호화 등의 수단을 적용하여 보안 위협으로 노출된 데이터에 대한 기밀성을 유지하여야 함

○ 연동 서비스는 DMZ 영역 내부에 위치한 가상 머신과만 통신이 가능하며, 침입차단시스템을 이용하여 연동 서비스가 DMZ 영역이외의 SaaS 영역으로 접근하는 것을 차단하여야 함

○ DMZ 영역과 다른 SaaS 영역 간의 연계는 연계서버를 통해서만 이루어져야 하며, 그 외의 접근은 침입차단시스템을 이용하여 차단되어야 함

3) 민간 클라우드 컴퓨팅 인프라 내 도입 기관 SaaS 자체 개발

- 『기관에서 SaaS 개발』 유형



[그림 26] 민간 클라우드 컴퓨팅 인프라 내 도입 기관 SaaS 자체 개발

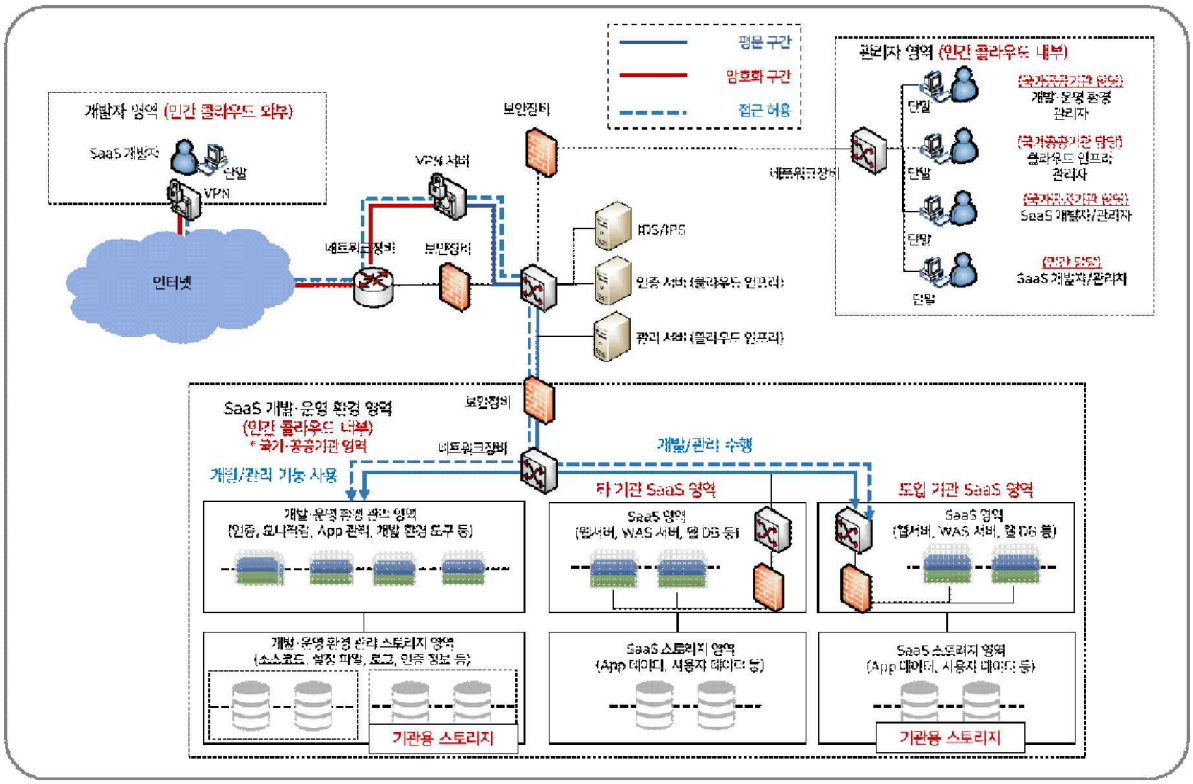
○ 도입 기관에서 자체적으로 민간 클라우드 컴퓨팅 인프라 내에 SaaS를 개발하는 경우 사용자 영역과 분리된 개발자 영역에서 개발이 수행되어야 함

○ 도입 기관 내부 SaaS 개발자는 기관 내부에 위치한 개발자 영역의 지정 단말을 통해서 SaaS 개발을 수행하여야 함

○ 도입 기관 내부 SaaS 개발자는 전용선 또는 암호화 통신(VPN 등)을 통하여 민간 클라우드 인프라에 구축된 개발·관리 기능에 접근 가능

- 개발·관리 기능을 이용하지 않고 도입 기관에 할당된 가상머신에 직접 개발·운영 환경을 구축하여 SaaS를 개발하는 경우도 전용선 또는 암호화 통신(VPN 등)을 이용한 통신을 하여야 함

4) 국가·공공기관용 SaaS 민간 개발 - 『민간에서 SaaS 개발』 유형



[그림 27] 민간에서 국가·공공기관용 SaaS 개발

○ 도입 기관의 SaaS를 개발하는 민간 사업자에 대한 보안 관리는 기관의 용역업체 보안관리 규정에 따라 수행

※ 국가·공공기관 영역에 기 구축된 SaaS를 이용하는 경우 민간 클라우드 컴퓨팅 서비스 보안인증을 통해 보안 관리 수행 여부 확인 가능

○ SaaS 구축을 위한 애플리케이션 개발은 「행정기관 및 공공기관 정보시스템 구축·운영 지침」 및 「소프트웨어 개발보안 가이드」(행정안전부)에 따라 개발되어야 함

○ 민간 사업자가 기관의 SaaS를 민간 클라우드 컴퓨팅 인프라 상에서 개발하는 경우 국가·공공기관을 담당하는 SaaS 개발자와 관리자를 지정하여 운영하여야 함

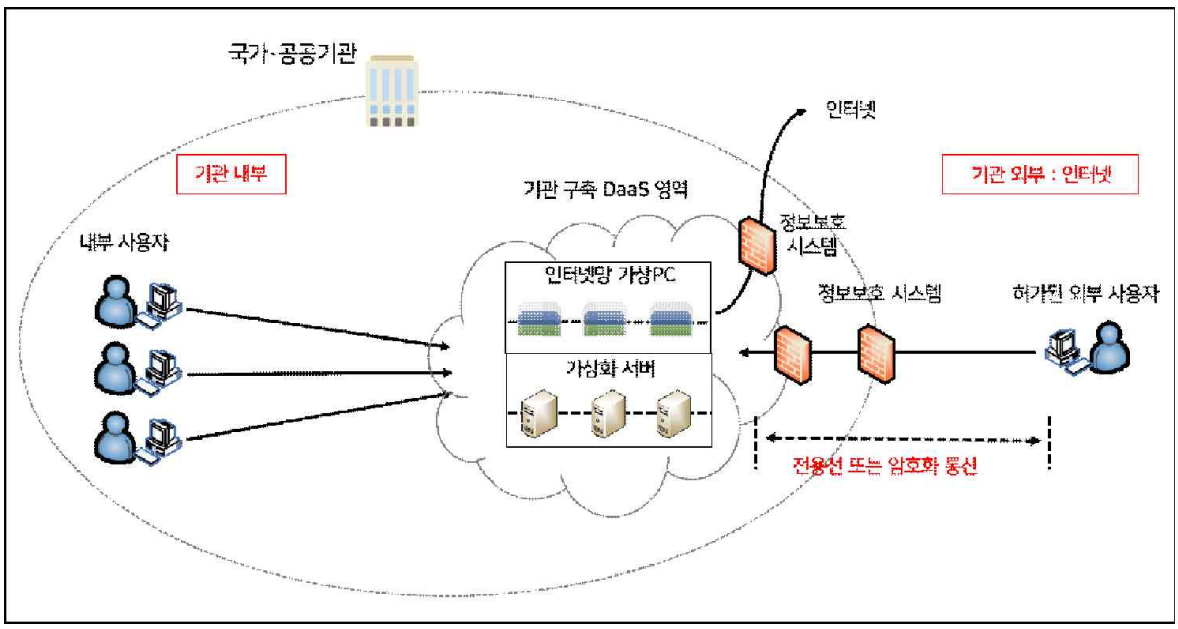
- SaaS 개발자와 관리자가 민간 클라우드 컴퓨팅 인프라 외부에 위치한 경우 전용선 또는 암호화 통신(VPN 등)을 통하여 민간 클라우드 컴퓨팅 인프라에 구축된 개발·관리 기능에 접근 가능

[부록 3] 인터넷망 DaaS 구축 보안대책

본 부록은 기관이 인터넷망 DaaS를 도입할 경우의 보안 기준을 제시한다. 인터넷망 DaaS 구축 형태는 기관 내부의 사용자 PC에서, 자체 구축한 DaaS 서비스를 이용하거나 민간 클라우드 서비스 사업자의 공공 영역에 있는 인터넷망 가상 PC를 이용하는 형태를 말한다. 구축 시 업무망과 인터넷망 분리 및 분리망간 자료전송 시 준수해야할 보안 고려사항은 「국가·공공기관 업무전산망 분리 및 안전한 자료전송 보안 가이드라인」을 참조한다.

1. 자체구축형 DaaS

자체구축형 DaaS 구성은 [그림 28]과 같으며, DaaS 도입 시 제4장 제1절의 보안 기본원칙과 세부 보안기준을 준수해야 한다 (공통 기본원칙 및 공통 보안기준). 또한 도입 기관은 자체구축형 DaaS의 도입, 운용 및 폐기에 대해 다음과 같은 보안기준을 준수해야 한다.



[그림 28] 자체구축형 인터넷망 DaaS 구성 예시

가. 도입 단계 보안기준

○ 보안성 유지 계획 수립

- 인터넷망 가상 PC의 보안 업데이트 및 보안 설정 관리 등을 포함한 사용자 단말의 보안성 유지 및 관리 대책을 수립

○ 보안대책 수립

- [접속단말 접근제어] 인터넷망 가상 PC에 비인가 단말의 접근을 방지하기 위한 대책 수립 (예: 접속단말에 대한 IP/MAC 기반 접근제어 등)

  * 가상화관리솔루션의 접속단말 IP/MAC 제어 기능 등을 활용

- [매체제어] 사용자 PC에서 인터넷망 가상 PC 접속 시, 화면 렌더링, 입력장치 및 프린터 리디렉션 이외의 자료교환 통제 대책 수립 (예: 가상화관리솔루션의 단말 정책관리 기능 활용 등)

  * 인터넷망 가상 PC의 USB, 클립보드, 공유폴더 리디렉션 및 화면 캡처 등을 차단

  * 접속단말-인터넷망 가상 PC간 자료교환은 기관 내부망-인터넷망 가상 PC간 별도로 구축한 망연계 솔루션 등을 활용

- [안전한 망간 자료교환] 망 분리 환경에서, 기관 내부망과 인터넷망 가상 PC 간 안전한 자료전송을 위한 대책 수립 (예: 망연계 솔루션 운용 등)

- [악성코드 대응] 악성코드로부터 인터넷망 가상 PC를 보호하기 위한 보안대책 수립 (예: 백신 솔루션 운용 등)

  * 클라우드용 백신 운용체계 구축, 안티바이러스 스톰방지 방안 마련 등의 보안대책 수립

- [유해사이트 차단] 인터넷망 가상 PC에서 업무와 무관한 인터넷 사용을 통제하기 위한 대책 수립 (예: 유해사이트 차단 솔루션 운용 등)

- [업무자료 유출방지] 인터넷망 가상 PC에서, 비공개 업무자료 유출 방지 대책 및 업무자료의 생산·자료저장 방지 대책 수립 (예: 가상머신 클린 이미지 제공, 가상머신 내 홈폴더 초기화 기술 적용 등)

- [보안수준 관리] 인터넷망 가상 PC에 대한 보안관리 대책 수립 (예: 최신 패치가 적용된 가상 PC 이미지 활용 등)

  * 인터넷망 가상 PC 생성에 이용되는 가상머신 원본 이미지는 최신 보안패치가 적용되어야 함

- [접속단말 보호] 실행파일 검증 등 비인가 프로그램 및 위·변조 프로그램 실행 차단 대책 수립

- [디스크 암호화] 인터넷망 가상 PC에 대한 침해사고 및 자료유출에 대비한 저장자료 보호 대책 수립 (예: 전체 디스크 암호화 또는 홈폴더 암호화 적용 등)

나. 운영 단계 보안기준

○ 인터넷망 가상PC 보안관리

(정보보안담당관 고려사항)

- 도입 단계 보안기준에 제시된 보안대책을 준수하기 위한 정보보호 솔루션 및 보안기능을 운용·관리 (각 항목의 예시 참조)

- 인터넷망 가상 PC 운영체제에 적절한 보안정책이 적용되어 있는지 주기적으로 점검 (가상 PC를 Pooled 방식으로 운용할 경우, 해당 가상PC의 마스터 이미지에 대한 보안 업데이트를 정기적으로 수행하여야 함)

(사용자 고려사항)

- 정기적인 보안 업데이트를 통해서 인터넷망 가상 PC의 운영체제와 설치 프로그램의 최신 상태를 유지

- 인터넷망 가상 PC의 접속 패스워드를 설정하여 사용하고 주기적으로 변경

  * 국가 정보보안 기본지침 제 76조(비밀번호 관리)의 각 항을 참조하여 수행

- 파일이 첨부된 이메일 열람 주의

  * 국가 정보보안 기본지침 제 77조(전자우편 보안)의 각 항을 참조하여 수행

- 악성코드 탐지 및 방지 프로그램 사용

- 업무무관 또는 보안에 취약한 비인가 프로그램 설치 금지·차단

- 출처, 유통경로 및 제작자가 불분명한 응용프로그램의 사용 금지

- 인터넷망 가상 PC에서 특별한 사유가 없는 한 문서 프로그램을 읽기 전용으로 운용

○ 보안감사 및 사고 대응

- 정보보안감사를 실시할 경우, 도입기관은 보안 요구사항, 감사 요구사항 및 법적 요구사항 등에 대한 준수 여부를 판별하기 위해, 인터넷망 가상 PC의 보안 관리와 관련한 세부 사항을 점검

  * 국가 정보보안 기본지침의 정보보안점검 체크리스트 등을 참조

- 사이버 공격으로 인한 사고 발생 시, 피해 기관은 피해 최소화 및 확산 방지를 위해 DaaS 가상PC의 시스템 및 로그를 기록을 보전 (예: 보안정책 변경 사항 및 운영체제·소프트웨어 패치 내역 등)

  * 국가 정보보안 기본지침 제 135조(초동 조치) 참조

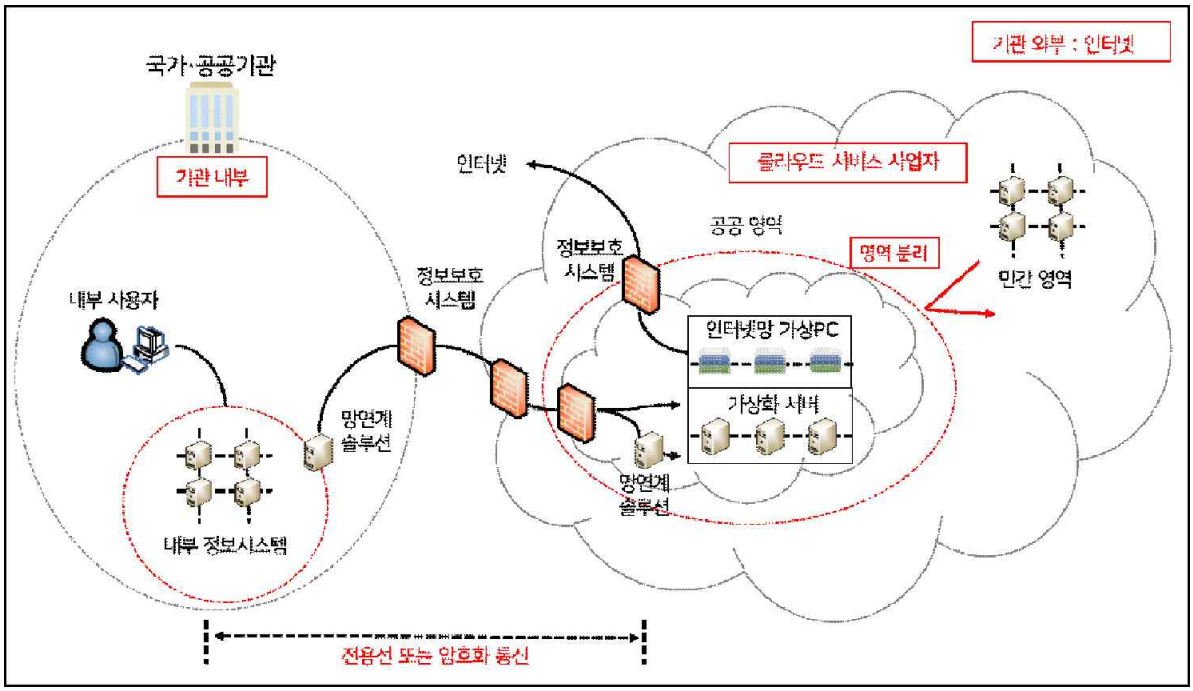
다. 폐기 단계 보안기준

○ (데이터 폐기) DaaS 사용 종료 등의 이유로 인한 데이터 폐기 시 DaaS 환경 내에 존재하는 사용자 관련 데이터는 복구할 수 없는 형태로 삭제되어야 함

- 사용자의 DaaS 애플리케이션 사용 종료, 이전 등에 따른 데이터 폐기 조치 시 폐기된 데이터를 복구할 수 없도록 데이터를 삭제하여야 함

2. 민간 서비스형 DaaS

민간 서비스형 DaaS 구성은 [그림 29]과 같으며, DaaS 도입 시 제4장 제2절의 보안 기본원칙과 세부 보안기준을 준수해야 한다 (공통 기본원칙 및 공통 보안기준). 또한 도입 기관의 사용자 및 정보보안담당관은 민간 서비스형 DaaS의 보안성을 확보하기 위해 도입-운영-폐기의 단계 별로 다음과 같은 보안 기준을 고려한다.



[그림 29] 민간 서비스형 인터넷망 DaaS 구성 예시

가. 도입 단계 보안기준

○ 민간 클라우드 컴퓨팅 서비스 이용 시 보안대책

- 민간 클라우드 컴퓨팅 서비스 이용 시 보안기준 확인
  - o 본 가이드라인 제3장 제3절의 보안 중요도 등급 분류를 수행하고 제3장 제2절의 클라우드 영역 기본원칙을 준수
- DaaS 구성 애플리케이션 보안취약점 제거
  - o 「행정기관 및 공공기관 정보시스템 구축·운영 지침」 및 「소프트웨어 개발 보안 가이드」에 따라, 소프트웨어 개발단계부터 보안취약점의 원인인 보안약점을 배제하여 개발

- 국가정보원이 도입요건 확인을 완료한 민간 클라우드 인프라를 이용

- 클라우드 컴퓨팅 서비스 물리적 위치 및 영역 분리

  o 클라우드 시스템 및 데이터(소스코드, 설정 파일, 로그, 사용자 계정 정보 등)의 물리적 위치는 국내로 한정

  o 국가·공공기관용 클라우드 컴퓨팅 서비스의 자원(서버, 네트워크, 보안장비 등), 출입통제, 운영인력 등은 민간 이용자용 클라우드 컴퓨팅 서비스 영역과 분리 운영

  * 클라우드 컴퓨팅 서비스 자원은 민간 이용자용 클라우드 컴퓨팅 서비스 영역과 물리적/논리적으로 분리 운영할 수 있음, 물리적/논리적 분리 형태와 보안 고려사항 등은 본 가이드라인 제3장 제2절 및 제3절의 관련 보안기준 참조

- 도입 정보보호시스템 안전성 확인

  o DaaS 환경 구성에 필요한 가상화 제품, 가상화 관리제품 등과 같은 정보보호시스템 도입 시 보안적합성 검증 절차를 준수

  o 민간 클라우드 컴퓨팅 서비스 구축을 위해 도입되는 보안 기능을 가진 정보통신제품 중에서 전자정부법 제56조에 규정된 전자문서의 위조, 변조, 훼손 또는 유출을 방지하기 위한 목적으로 도입하는 제품은 국가정보원장이 안전성을 확인한 제품을 사용하여야 함

  * 기타 세부사항은 보안적합성 검증제도에 따름

○ 보안성 유지 계획 수립

- 인터넷망 가상 PC의 보안 업데이트 및 보안 설정 관리 등을 포함한 사용자 단말의 보안성 유지 및 관리 대책을 수립

○ 보안대책 수립

- [접속단말 접근제어] 인터넷망 가상 PC에 비인가 단말의 접근을 방지하기 위한 대책 수립 (예: 접속단말에 대한 IP/MAC 기반 접근제어 등)

  * 가상화관리솔루션의 접속단말 IP/MAC 제어 기능 등을 활용

- [매체제어] 사용자 PC에서 인터넷망 가상 PC 접속 시, 화면 렌더링, 입력장치 및 프린터 리디렉션 이외의 자료교환 통제 대책 수립 (예: 가상화관리솔루션의 단말 정책관리 기능 활용 등)

  * 인터넷망 가상 PC의 USB, 클립보드, 공유폴더 리디렉션 및 화면 캡처 등을 차단

  * 접속단말-인터넷망 가상 PC간 자료교환은 기관 내부망-인터넷망 가상 PC간 별도로 구축한 망연계 솔루션 등을 활용

- [안전한 망간 자료교환] 망 분리 환경에서, 기관 내부망과 인터넷망 가상 PC간 안전한 자료전송을 위한 대책 수립 (예: 망연계 솔루션 운용 등)

- [악성코드 대응] 악성코드로부터 인터넷망 가상 PC를 보호하기 위한 보안대책 수립 (예: 백신 솔루션 운용 등)

  * 클라우드용 백신 운용체계 구축, 안티바이러스 스톰 방지 방안 마련 등의 보안대책 수립

- [유해사이트 차단] 인터넷망 가상 PC에서 업무와 무관한 인터넷 사용을 통제하기 위한 대책 수립 (예: 유해사이트 차단 솔루션 운용 등)

- [업무자료 유출방지] 인터넷망 가상 PC에서, 비공개 업무자료 유출 방지 대책 및 업무자료의 생산·자료저장 방지 대책 수립 (예: 가상머신 클린 이미지 제공, 가상머신 내 홈폴더 초기화 기술 적용 등)

- [보안수준 관리] 인터넷망 가상 PC에 대한 보안관리 대책 수립 (예: 최신 패치가 적용된 가상 PC 이미지 활용 등)

  * 인터넷망 가상 PC 생성에 이용되는 가상머신 원본 이미지는 최신 보안패치가 적용되어야 함

- [실행파일 검증] 비인가 프로그램 및 위·변조 프로그램 실행 차단 대책 수립

- [디스크 암호화] 인터넷망 가상 PC에 대한 침해사고 및 자료유출에 대비한

저장자료 보호 대책 수립 (예: 전체 디스크 암호화 또는 홈폴더 암호화 적용 등)

나. 운영 단계 보안기준

○ 인터넷망 가상PC 보안관리

(정보보안담당관 고려사항)

- 도입 단계 보안기준에 제시된 보안대책을 준수하기 위한 정보보호 솔루션 및 보안기능을 운용·관리 (각 항목의 예시 참조)

- 인터넷망 가상 PC 운영체제에 적절한 보안정책이 적용되어 있는지 주기적으로 점검

(사용자 고려사항)

- 정기적인 보안 업데이트를 통해서 인터넷망 가상 PC의 운영체제와 설치 프로그램의 최신 상태를 유지

- 인터넷망 가상 PC의 접속 패스워드를 설정하여 사용하고 주기적으로 변경

  * 국가 정보보안 기본지침 제 76조(비밀번호 관리)의 각 항을 참조하여 수행

- 파일이 첨부된 이메일 열람 주의

  * 국가 정보보안 기본지침 제 77조(전자우편 보안)의 각 항을 참조하여 수행

- 악성코드 탐지 및 방지 프로그램 사용

- 업무무관 또는 보안에 취약한 비인가 프로그램 설치 금지·차단

- 출처, 유통경로 및 제작자가 불분명한 응용프로그램의 사용 금지

- 인터넷망 가상 PC에서 특별한 사유가 없는 한 문서 프로그램을 읽기 전용으로 운용

○ 보안감사 및 사고 대응

- 정보보안감사를 실시할 경우, 도입기관은 보안 요구사항, 감사 요구사항 및 법적 요구사항 등에 대한 준수 여부를 판별하기 위해, 인터넷망 가상 PC의 보안 관리와 관련한 세부 사항을 점검

  * 국가 정보보안 기본지침의 정보보안점검 체크리스트 등을 참조

- 사이버 공격으로 인한 사고 발생 시, 피해 기관은 피해 최소화 및 확산 방지를 위해 DaaS 가상PC의 시스템 및 로그를 기록을 보전 (예: 보안정책 변경 사항 및 운영체제·소프트웨어 패치 내역 등)

  * 국가 정보보안 기본지침 제 135조(초동 조치) 참조

다. 폐기 단계 보안기준

○ (데이터 폐기) DaaS 사용 종료 등의 이유로 인한 데이터 폐기 시 DaaS 환경 내에 존재하는 사용자 관련 데이터는 복구할 수 없는 형태로 삭제되어야 함

- 사용자의 DaaS 애플리케이션 사용 종료, 이전 등에 따른 데이터 폐기 조치 시 폐기된 데이터를 복구할 수 없도록 데이터를 삭제하여야 함
- 제3자의 클라우드 서비스를 제공받아서 DaaS 환경을 구축하는 경우에도 제3자의 클라우드 서비스로부터 사용자 데이터가 폐기되었음을 확인하여야 함

[부록 4] 클라우드 컴퓨팅 보안기준 체크리스트

1. 기관 구축 클라우드 컴퓨팅 보안기준 체크리스트

○ 기본원칙

번호	점검항목	적용 범위	점검 결과	비고
정책적 측면				
①	이용 대상에 대한 시스템 중요도 등급 분류 및 클라우드 영역 분류를 수행하고 관련 보안기준을 확인하였는가? (시스템 중요도 및 클라우드 영역 관련 보안 기본원칙 등)	공통		
②	정보보호시스템 도입 시 보안적합성 검증 절차를 준수하고, 정보보호시스템 제품 유형별 도입 인증 요건을 확인하였는가?			
③	인터넷과 업무망이 분리된 기관에서 인터넷이 연결된 가상환경 사용 시, - 업무 관련 데이터를 처리하지 않도록 보안 대책을 마련하고 있는가? - 인터넷과 업무 영역 간 자료교환이 되지 않도록 기술적 통제대책을 구현하여 적용하고 있는가?			
④	공급망 관리 정책을 수립하고 공급망 관련 보안 위험식별, 변경관리 및 모니터링을 수행하고 있는가?			
⑤	SaaS 구축 시 필요한 애플리케이션이 「행정기관 및 공공기관 정보시스템 구축·운영 지침」 및 「소프트웨어 개발보안 가이드」(행정안전부)에 따라, 소프트웨어 개발단계부터 보안취약점의 원인인 보안약점을 배제하여 개발되었는가?	SaaS		
⑥	SaaS 클라우드 인프라, 개발·운영 환경과 SaaS에서 처리되는 데이터의 물리적 위치가 국내인가?			
⑦	SaaS를 제공하기 위한 SaaS 개발·운영 환경, 클라우드 인프라 환경에 대한 보안성을 확인하고 있는가?			
⑧	SaaS 개발·운영 환경이 SaaS 서비스 가용성을 보장할 수 있으며, 사고 및 장애에 대응할 수 있는 체계를 마련하고 있는가?			
⑨	SaaS는 허가받은 외부 연동 서비스(스토리지, 데이터베이스, 빅데이터 처리 등)와 연계되어 있는가?			
기술적 측면				
⑩	업무포털, 그룹웨어 등 비공개 업무 용도로 쓰이는 클라우드 영역과 외부 공개용 클라우드 컴퓨팅 서비스를 사용 및 관리하기 위한 영역을 분리하여 운영하고 있는가?	공통		
⑪	중요장비를 이중화하고 백업체계를 구축하고 있는가? - 네트워크 스위치, 스토리지 등 중요장비를 이중화하고 클라우드 컴퓨팅 서비스의 가용성을 보장하기 위해 백업체계를 구축 - 백업·비상복구·변경관리·침해사고대응 등 클라우드 컴퓨팅 시스템 운영의 전반적인 절차에 관한 표준운영절차(SOP) 등을 수립			

번호	점검항목	적용 범위	점검 결과	비고
⑫	관리자가 또는 다른 이용자가 특정 이용자에 할당된 자원(메모리·HDD 등) 및 데이터에 임의 접근하지 못하도록 접근제어 및 격리 등을 통한 기술적 통제 수단을 마련하고 있는가?	공통		
⑬	클라우드에 저장 및 송수신되는 중요 업무자료를 암호화하고 있는가? - 스토리지 저장 데이터 및 송수신 자료의 암호화 - 암호화를 위해 정보보호 제품을 도입할 경우 검증필 암호모듈 탑재			
⑭	클라우드 컴퓨팅 서비스에 대한 보안관제를 수행하고 있는가?			
⑮	외부 공개용 SaaS 영역이 내부 업무용 SaaS 영역과 분리되어 있는가?	SaaS		
⑯	SaaS 애플리케이션 보안성 강화 방안이 마련되어 있는가? (사용자 간 자원 격리, 취약점 점검 계획, 데이터 보호 등)			

○ 정책

번호	점검항목	적용 범위	점검 결과	비고
시스템 보호				
①	클라우드 컴퓨팅 서비스 도입 시 관련 법률 및 지침, 보안 체계, 정책, 규정, 표준, 가이드라인 및 도입 기관 보안 사항 등을 참고하여 보안 요구 사항을 마련하였는가?	공통		
②	사용자와 관리자를 지정하여 클라우드 컴퓨팅 시스템을 도입·운용하고 있는가?			
③	클라우드 컴퓨팅 서비스를 구축하여 다루고자 하는 업무 또는 데이터와 연관된 법령, 수행 요구사항, 정책, 규정, 표준, 가이드라인 등을 참고하여 클라우드 컴퓨팅과 관련된 물리적 설비, 하드웨어 장비, 가상 인프라, 가상머신 내 소프트웨어 등에 대한 보안위협을 식별하였는가?			
④	클라우드 컴퓨팅 환경으로 이전될 정보자산에 대한 관리정책을 마련하고 정보자산 목록을 관리하고 있는가?			
⑤	형상 변경에 영향을 받는 물리적·논리적 요소를 식별하고 현상 변경 사항을 지속적으로 확인 및 검토하고 있는가?	IaaS		
⑥	클라우드 컴퓨팅 환경 내 모니터링 수집 대상 및 위치를 정의하고 모니터링 수단을 통해 시스템 운영 상황, 장애 발생 대응 도구 동작 여부 등을 모니터링하고 있는가?			

번호	점검항목	적용 범위	점검 결과	비고
인적 관리				
⑦	클라우드 컴퓨팅 서비스에 접근 가능한 사용자 및 관리자를 식별하고 직무별 권한 부여, 폐기 등에 관한 절차를 마련하고 있는가?	공통		
⑧	정보보호 및 정보보호 관리 체계, 클라우드 보안 사고 사례, 사고에 따른 법적 책임, 사고 대응 방법 등이 포함된 직무별, 담당 분야 별 교육을 주기적으로 수행하고 있는가?			
사후 추적을 위한 감사자료 관리				
⑨	보안 요구사항, 가용성 요구사항 ,감사 요구사항, 법적 요구사항 등과 같은 요구사항들에 대한 준수 여부를 판별하기 위한 모니터링 및 로그관리를 수행하고 있는가?	IaaS		
⑩	감사 정보를 감사 대상을 식별할 수 있는 형태로 1년 이상 기록 및 보호하고 있는가?			

○ 클라우드 인프라

번호	점검항목	적용 범위	점검 결과	비고
가상화 인프라				
①	가상 머신, 가상 스토리지, 가상 애플리케이션 등의 가상자원 사용 목록을 유지하고 있는가?	공통		
②	가상자원 내에 존재하는 사용자 관련 데이터를 복구할 수 없는 형태로 삭제 후 가상자원을 회수하고 있는가?			
③	가상자원에 대한 모니터링을 주기적으로 수행하고 있는가?			
④	기존 정보시스템 환경에서 클라우드 가상환경으로 이전 시 안전한 이전 수단을 이용하고 있는가?			
⑤	하이퍼바이저 관리 기능 및 관리자에 대한 접근 통제 방안을 마련하고, 하이퍼바이저에 대한 업데이트 및 보안패치를 최신으로 유지하고 있는가?	IaaS		
⑥	SaaS 개발·운영을 위한 가상환경이 『국가 클라우드 컴퓨팅 보안 가이드라인』의 보안기준을 준수하는 클라우드 컴퓨팅 인프라 상에서 구축 및 운영 되고 있는가?	SaaS		

○ 가상환경 보안

번호	점검항목	적용 범위	점검 결과	비고
보안 관리				
①	가상환경에서 시스템, 애플리케이션, SaaS 등을 자체 또는 외주로 도입 및 개발하고자 하는 경우 보안대책을 수립하고 있는가? (운영중인 클라우드 서비스 환경과 분리, 비인가 접근 통제 등)	공통		
②	가상환경을 구성하는 시스템, 애플리케이션, SaaS 등을 유지보수하고자 하는 경우 보안대책을 수립하고 있는가? (유지보수 인원관리, 지정된 단말기만 접속, 유지보수 기록 유지 등)			
③	지정된 단말기를 통한 온라인 유지보수 시 보안·네트워크 장비 제외, 소통구간 보호·통제, 인터넷 접속 차단 등의 보안대책을 마련하고 있는가?			
④	비인가자가 인터넷에 연결된 가상PC를 무단으로 조작하여 전산 자료를 절취, 위·변조 및 훼손시키지 못하도록 보안대책을 마련하여 사용자의 인터넷 연결 가상PC에 적용하였는가?	IaaS		
⑤	PC 등 단말기 보안관리에 준하는 보안대책을 마련하여 사용자의 가상PC에 적용하였는가? ※ 가상 PC 접속용 장비·자료(문서자료 암호화 비밀번호)·사용자(접속 비밀번호)별 비밀번호 주기적 변경, 가상 PC 작업 일정 시간 이상 중단시 비밀번호 등을 적용한 화면보호, 최신 백신 운용·점검, 가상 운영체제(OS) 및 응용프로그램의 최신 보안패치 유지 등			
⑥	서버 관리자는 가상머신을 할당받아 가상서버를 운용할 경우, 해킹을 통한 자료 절취, 위·변조 등에 대비한 보안대책을 수립·시행하고 있는가? ※ 국가 정보보안 기본지침의 서버 보안을 준용			
⑦	비인가자의 가상서버 내 저장자료 절취 및 위·변조, 분산서비스거부(DDoS) 공격 등에 대비하기 위하여 보안대책을 강구하였는가?			
⑧	가상머신 내에 보안 상 취약한 소프트웨어 설치 방지, 보안 업데이트 등의 보안 관리 방안을 마련하였는가?			
보안 관리 - SaaS 애플리케이션 개발				
⑨	SaaS 애플리케이션 설계 및 개발 단계에서 SaaS 애플리케이션 접근을 위한 안전한 인증 방안이 마련되고, 접근 권한 정책을 수립하여 사용 및 관리 권한을 부여하였는가?	SaaS		
⑩	SaaS 애플리케이션의 데이터 처리(송·수신, 저장, 연산 등) 과정에서 데이터를 보호하기 위한 수단을 마련하였는가?			
⑪	SaaS 애플리케이션 설계 및 개발단계에서 연동서비스 호출 시 송·수신되는 인증정보, 메시지 등을 보호하기 위한 수단을 마련하였는가?			

번호	점검항목	적용 범위	점검 결과	비고
⑫	SaaS 애플리케이션 설계 및 개발 단계에서 사용자 데이터에 대한 무결성 검증 방안을 마련하였는가?	SaaS		
⑬	SaaS 애플리케이션은 사용자 업무 연속성을 보장할 수 있는 형태로 설계 및 개발되었는가?			
⑭	보안 요구사항, 가용성 요구사항, 감사 요구사항, 법적 요구사항 등에 대한 준수 여부를 판별하기 위하여 SaaS에 대한 모니터링 및 로그 관리를 수행하는가?			
⑮	SaaS에서 생성된 로그 자료를 사후 추적대상을 식별할 수 있는 형태로 기록하고 1년 이상 보호하고 있는가?			
⑯	SaaS 애플리케이션 보안을 위해 주기적 취약점 점검, 보안업데이트 등의 보안 관리 방안을 마련하였는가?			
⑰	자체 또는 외주로 SaaS 애플리케이션 개발을 하고자 하는 경우 보안대책을 수립하였는가? ※ 출처가 불명확한 소스코드 및 소프트웨어 사용 금지, 소스코드 및 소프트웨어 보안관리, 외부 인력 관리 등			
보안 관리 - 개발·운영 환경				
⑱	개발·운영 환경 접속을 위한 안전한 인증 방안을 마련하고, 접근 권한 정책을 수립하여 사용 및 관리 권한을 부여하였는가?	SaaS		
⑲	개발·운영 환경 관리에 필요한 데이터 보호 방안을 마련하였는가?			
⑳	개발·운영 환경 내 저장된 SaaS 관련 데이터에 대한 무결성 검증을 수행하는가?			
㉑	개발·운영 환경은 SaaS 운영 연속성을 보장할 수 있는 형태로 구축되었는가?			
㉒	보안 요구사항, 가용성 요구사항, 감사 요구사항, 법적 요구사항 등에 대한 준수 여부를 판별하기 위하여 개발·운영 환경에 대한 모니터링 및 로그 관리를 수행하는가?			
㉓	개발·운영 환경 운영 중 생성된 로그 자료를 사후 추적대상을 식별할 수 있는 형태로 기록하고 1년 이상 보호하고 있는가?			
㉔	개발·운영 환경 보안을 위해 주기적 취약점 점검, 보안 업데이트 등의 보안관리 방안을 마련하였는가?			
㉕	개발·운영 환경 구축을 위해 가상서버를 운용할 경우, 해킹을 통한 자료 절취, 위·변조 등에 대비한 보안대책을 수립·시행하고 있는가?			
㉖	개발·운영 환경 구축을 위해 공개용으로 운영되는 가상서버를 운용할 경우, 비인가자의 가상서버 내 저장자료 절취 및 위·변조, 분산서비스 거부(DDoS) 공격 등에 대비하기 위한 보안대책을 강구하였는가? ※ 국가정보원장이 안전성을 검증한 침입차단·탐지시스템 및 DDoS 대응시스템 설치, 불필요 계정 삭제, 프로그램 개발·시험을 위해 사용된 도구(컴파일러 등)를 개발 완료 후 삭제 등			

번호	점검항목	적용 범위	점검 결과	비고
악성코드 방지				
㉗	웜·바이러스, 해킹프로그램, 스파이웨어 등 악성코드에 의한 위협을 제거하기 위해 악성코드 방지 대책을 수립·시행하고 있는가? ※ 운영체제, 소프트웨어 등에 대한 주기적인 보안패치, 백신 최신상태 업데이트 및 주기적인 점검, 사용 금지 대상 소프트웨어 설치 금지, 악성코드 위협 접근통제를 위한 침입차단시스템 등	공통		
㉘	가상머신에 악성코드가 설치되거나 감염된 사실을 발견하였을 경우 조치를 하고 있는가? ※ 감염된 가상머신 사용중지 및 격리, 감염확산 방지를 위해 정보보안 담당관에게 관련 사실 통보, 재발장비를 위한 원인분석 및 예방 등			
접근 통제				
㉙	이동식 저장매체 사용 통제, 다중요소(Multi-factor) 인증, 자동 로그아웃 등 접근 제한 방안을 마련하였는가? ※ 클라우드 시스템에 대한 이동식 저장매체 사용 통제, 식별 번호가 등록된 이동매체만 사용, 중요 기능에 대한 동일 사용자의 동시 세션 제한 등	공통		
㉚	사용자 또는 장치를 유일하게 식별할 수 있는 식별 방법을 마련하고 식별 정보를 관리하는가?			
㉛	계정 권한 생성 절차를 마련하였는가? ※ 계정 유형 식별, 계정 그룹 설정, 클라우드 시스템 및 서비스 접근 허용자 식별, 게스트 또는 임시 계정에 대한 승인 및 모니터링 등			
㉜	사용자계정 보안관리 방안을 마련하여 사용자계정(ID) 부여 및 보안관리를 수행하는가? ※ 사용자·그룹별 접근권한 부여, 사용자 식별 수단이 없는 계정 사용 금지, 5회 이상 로그인 실패 시 접속 중단 등			
㉝	비밀번호 관리 방안을 마련하였는가? ※ 숫자·문자·특수문자 등 혼합 설정 및 정기적 변경, 사용된 비밀번호 재사용 금지, 응용프로그램 등을 이용한 자동 입력 금지 등			
㉞	접근 기록을 서비스 통제, 관리, 사고 발생 책임 추적성 등을 보장할 수 있는 형태로 기록하고 1년 이상 보관, 유지하고 있는가?			
㉟	스마트폰·IoT기기·전자제어장비 등 첨단 정보통신기기를 활용하여 클라우드 컴퓨팅 관리 및 접속하기 위한 자체 보안대책을 수립 및 시행하고 있는가?			
㊱	가상환경 접근을 위한 인터페이스 및 API에 대한 보안 방안을 마련하였는가?			

○ 데이터

번호	점검항목	적용 범위	점검 결과	비고
데이터 관리				
①	클라우드 시스템에서 기관의 비밀을 전자적으로 처리할 시에 국가정보원장이 별도로 규정한 보안 규격을 준수하여 안전하게 처리하고 있는가?	공통		
②	기관 내부에 위치한 클라우드 접속 단말과 클라우드 컴퓨팅 환경 간 비인가된 데이터 송·수신을 차단하고 있는가?			
③	클라우드 시스템 폐기, 이전 등에 따른 데이터 폐기 조치 시 폐기된 데이터를 복구할 수 없는 형태로 삭제하고 있는가?			
④	사용자별 데이터 보안 요구사항 수준에 따라 물리적 또는 논리적으로 데이터를 사용자별로 분리할 수 있는 방안을 마련하여 SaaS 애플리케이션 및 개발·운영 환경을 구축하였는가?	SaaS		
⑤	데이터 송수신, 연산, 저장 시 데이터 암호화 등의 수단을 적용하여 SaaS 애플리케이션 취약점 등을 이용한 보안 위협으로부터 데이터 노출 시에 따른 기밀성을 유지하고 있는가?			
⑥	SaaS 애플리케이션 및 개발·운영 환경에서 처리되는 중요 데이터에 대한 무결성 검증을 수행하고 있는가?			
⑦	SaaS 애플리케이션 및 개발·운영 환경에서 생성되는 중요 데이터에 대한 추적성을 보장하고 있는가?			
⑧	SaaS 사용 종료 등의 이유로 인한 데이터 폐기 시 SaaS 환경 내에 존재하는 사용자 관련 데이터를 복구할 수 없는 형태로 삭제하고 있는가?			
암호화				
⑨	클라우드 시스템 도입 시 중요 업무자료에 대한 암호화 수준 등에 대한 보안요구사항을 도출하여 반영하였고, 중요 업무자료에 대한 생산·보관·처리·수신하기 위한 정책적·기술적 방안을 강구하고 있는가?	공통		
⑩	클라우드 시스템에 저장 또는 전송 중인 중요 업무자료를 보호하기 위한 암호 정책이 수립되었는가?			
⑪	암호키 관리 절차를 수립하고 암호키를 별도의 물리적으로 분리된 서버에 백업하고 최소 접근권한을 부여하여 관리하고 있는가?			

○ 인증 및 권한

번호	점검항목	적용 범위	점검 결과	비고
인증				
①	서비스 관리환경, 가상머신, 가상 응용프로그램, SaaS 등의 접근 대상 및 주체를 식별하였고 이에 따른 인증 정책을 수립하였는가?	공통		
②	기관 필요에 따라 클라우드 접근 대상 별로 기관의 인증 체계와 연동할 수 있는 인증 시스템을 설계 및 구축하였는가?			
권한				
③	접근 대상, 권한 부여 절차 등을 담은 사용자, 관리자의 접근 권한 관리절차를 수립하였는가?	공통		
④	클라우드 접근 대상에 따른 접근 주체별 이용 및 관리 권한을 부여하고 있는가?			

○ 사고 및 장애 대응

번호	점검항목	적용 범위	점검 결과	비고
사고				
①	신고 절차, 유출 금지 대상, 사고 처리 절차 등을 담은 보안사고 발생 대응 절차를 마련하고 있는가?	공통		
②	정보보안 사고가 발생한 때에는 즉시 피해확산 방지를 위한 조치를 취하고 사고 발생일시, 사고내용 등을 포함하는 보고서를 작성하여 조사기관의 장에게 통보하였는가?			
장애				
③	장애 대응 요구사항, 담당자 정의 및 연락처 등을 담은 장애 대응 절차를 마련하고 있는가?	공통		
④	백업 시기 및 방법, 백업본 유지 기간 등을 담은 데이터에 대한 백업과 복구 절차를 마련하였는가?			

2. 민간 클라우드 컴퓨팅 서비스 이용 보안기준 체크리스트

※ (민간 클라우드 컴퓨팅 서비스 이용) 비고의 '√' 항목은 자체 점검을 필수적으로 수행하여야 함

※ 자체 점검 : 민간 클라우드 컴퓨팅 서비스 이용기관이 반드시 자체 점검 해야 하는 항목

※ 권고 항목 : 시스템 중요도 하등급 - ㉮ 에 따른 권고 항목 표시, 권고 항목이 아닌 경우, 상/중/하 등급 모두 필수

○ 기본원칙

번호	점검항목	적용 범위	자체 점검	권고 항목	점검 결과
정책적 측면					
①	이용 대상에 대한 시스템 중요도 등급 분류 및 클라우드 영역 분류를 수행하고 관련 보안기준을 확인하였는가? (시스템 중요도 및 클라우드 영역 관련 보안 기본원칙 등)	공통	√	-	
②	클라우드 시스템 및 데이터의 물리적 위치는 국내로 한정하고, 국가·공공기관용 클라우드 컴퓨팅 서비스의 자원, 출입통제, 운영인력 등은 민간 이용자용 클라우드 컴퓨팅 서비스 영역과 분리 운영하고 있는가?		√	-	
③	국가정보원이 도입요건 확인을 완료한 민간 클라우드 컴퓨팅 서비스를 이용하고 있는가?		√	-	
④	정보보호시스템 도입 시 보안적합성 검증 절차를 준수하고 도입 정보보호시스템 안전성을 확인하였는가?		√	-	
⑤	내부망과 연동된 공공 전용 민간클라우드는 기관의 내부망으로 간주하고, 인터넷망과 연동된 공공 전용 민간클라우드는 기관의 인터넷망으로 간주하여 보안관리를 하고 있는가?		√	-	
⑥	클라우드 서비스 제공자와 기관의 보안 관리 체계를 반영하는 보안 서비스수준협약(SLA)을 맺고 있는가?		√	-	
⑦	공급망 관리 정책을 수립하고 관련 보안 요구사항을 계약 상에 반영하였는가?		√	-	
⑧	망 미분리 기관은 SaaS 사용 단말에서 인터넷과 업무 영역 간 자료교환이 되지 않도록 기술적 통제대책을 구현하여 SaaS를 사용하고 있는가?	SaaS		-	
⑨	SaaS 클라우드 인프라, 개발·운영 환경과 SaaS에서 처리되는 데이터의 물리적 위치가 국내인가?			-	
⑩	SaaS를 제공하기 위한 SaaS 개발·운영 환경, 클라우드 인프라 환경에 대한 보안성을 확인하고 있는가?			-	
⑪	SaaS 개발·운영 환경이 SaaS 서비스 가용성을 보장할 수 있으며, 사고 및 장애에 대응할 수 있는 체계를 마련하고 있는가?			-	
⑫	SaaS는 허가받은 외부 연동 서비스(스토리지, 데이터베이스, 빅데이터 처리 등)와 연계되어 있는가?			-	

번호	점검항목	적용 범위	자체 점검	권고 항목	점검 결과
기술적 측면					
⑬	업무포털, 그룹웨어 등 내부 업무 용도로 쓰이는 영역과 인터넷 서비스를 제공하는 영역을 분리하여 운영하고 있는가?	공통	√	-	
⑭	중요장비를 이중화하고 백업체계를 구축하고 있는가? - 네트워크 스위치, 스토리지 등 중요장비를 이중화하고 클라우드 컴퓨팅 서비스의 가용성을 보장하기 위해 백업체계를 구축 - 백업·비상복구·변경관리·침해사고대응 등 클라우드 컴퓨팅 시스템 운영의 전반적인 절차에 관한 표준운영절차(SOP) 등을 수립		√	-	
⑮	관리자가 또는 다른 이용자가 특정 이용자에 할당된 자원(메모리·HDD 등) 및 데이터에 임의 접근하지 못하도록 접근제어 및 격리 등을 통한 기술적 통제 수단을 마련하고 있는가?		√	-	
⑯	클라우드에 저장 및 송수신되는 중요 업무자료를 암호화하고 있는가? - 스토리지 저장 데이터 및 송수신 자료의 암호화 - 암호화를 위해 정보보호 제품을 도입할 경우 검증필 암호모듈 탑재		√	-	
⑰	클라우드 내에 존재하는 자원에 대한 기술적·정책적 보안관제 방안을 마련하고 민간 사업자로부터 보안관제센터 설치 및 운영에 필요한 제반 환경 구축 지원을 제공받았는가?		√	-	
⑱	민간 클라우드 컴퓨팅 서비스 내 가상 자원에 대한 모니터링 및 관리 수단을 마련하고 있는가?			-	
⑲	상호운용성 보장을 위해 표준화된 가상 이미지 포맷, 인터페이스, API를 지원할 수 있는 형태로 구축하고 있는가?			-	
⑳	SaaS 애플리케이션 보안성 강화 방안이 마련되어 있는가? (사용자 간 자원 격리, 취약점 점검 계획, 데이터 보호 등)	SaaS		-	

○ 정책

번호	점검항목	적용 범위	자체 점검	권고 항목	점검 결과
시스템 보호					
①	민간 클라우드 컴퓨팅 서비스 도입 시 관련 법률 및 지침, 보안체계, 도입 기관 보안 사항 등을 고려한 보안 요구 사항을 정의하고 이를 보안 SLA에 반영하고 있는가?	공통	√	-	
②	민간 클라우드 컴퓨팅 서비스 도입·운용에 있어서 사용자와 해당 관리자를 지정 운용하고 있는가?		√	-	
③	민간 클라우드 컴퓨팅 서비스를 이용하여 다루고자 하는 업무 또는 데이터와 연관된 법령, 수행 요구사항, 정책, 규정, 표준, 가이드라인 등을 참고하여 보안 위협 대상을 식별하고 있는가?		√	-	

번호	점검항목	적용 범위	자체 점검	권고 항목	점검 결과
④	클라우드 컴퓨팅 환경으로 이전 될 정보자산에 대한 관리 정책을 마련하고 정보자산 목록을 관리하고 있는가?	공통	√	-	
⑤	형상 변경에 영향을 받는 물리적·논리적 요소를 식별하고 형상 변경 사항을 지속적으로 확인 및 검토를 수행하는가?			㈐	
⑥	클라우드 컴퓨팅 환경 내 모니터링 수집 대상 및 위치를 정의하고 모니터링 수단을 통해 시스템 운영 상황, 장애 발생 대응 도구 동작 여부 등을 모니터링하고 있는가?			㈐	
⑦	민간 사업자로부터 필요한 제반 환경을 지원받아 사이버공격 정보를 수집·분석·대응할 수 있는 보안관제를 수행하는가?		√	-	
⑧	민간 사업자가 클라우드 컴퓨팅 서비스망을 대상으로 자체적으로 수행한 운용 관리에 대한 보안취약성 개선 결과를 주기적으로 보고 받는가?			㈐	
⑨	민간 사업자가 클라우드 컴퓨팅 서비스 망에 대하여 자체적으로 실시한 모의훈련 및 취약점 점검에 대한 결과를 주기적으로 보고 받는가?			㈐	
인적 관리					
⑩	클라우드 컴퓨팅 시스템에 접근 가능한 사용자 및 관리자를 식별하고 직무별 권한 부여, 폐기 등에 관한 절차를 마련하고 있는가?	공통		-	
⑪	정보보호 및 정보보호 관리 체계, 클라우드 보안 사고 사례, 사고에 따른 법적 책임, 사고 대응 방법 등이 포함된 직무별, 담당 분야 별 교육을 주기적으로 수행하고 있는가?			㈐	
사후 추적을 위한 감사자료 관리					
⑫	정보보안 감사에 필요한 관련 자료에 대한 종류를 정의하고, 필요시에 민간 사업자에게 해당 감사 로그를 요청하여 열람할 수 있는가?	IaaS	√	-	
⑬	보안 요구사항, 가용성 요구사항, 감사 요구사항, 법적 요구사항 등과 같은 요구사항들에 대한 준수 여부를 판별하기 위하여 모니터링 및 로그관리를 수행하고 있는가?			-	
⑭	감사 정보를 감사 대상을 식별할 수 있는 형태로 1년 이상 기록 및 보호하고 있는가?			-	

○ 클라우드 인프라

번호	점검항목	적용 범위	자체 점검	권고 항목	점검 결과
설비					
①	민간 사업자의 데이터센터 시설 내 국가·공공기관 클라우드 컴퓨팅 서비스 제공을 위한 시스템의 물리적 위치를 파악하고 물리적 보호 구역에 대한 보안대책을 마련하고 있는가?	IaaS		-	
②	민간 사업자의 데이터센터 시설 내 화재, 전력 이상 등 인재 및 자연재해 등에 대비하여 필요한 설비 구축 실태를 파악하고 있는가?			-	
하드웨어					
③	민간 클라우드 컴퓨팅 서비스 운용에 필요한 물리 자산 목록을 유지하고 회수, 폐기 등의 자산 변화 상황을 반영하는가?	IaaS		㈜	
④	기관에 필요한 전자정보 저장매체 불용처리 관련 보안 요구사항을 민간 사업자와의 계약 상에 반영하였는가?		√	-	
⑤	국가·공공기관 클라우드 컴퓨팅 서비스 제공을 위해 물리적으로 독립된 형태의 하드웨어 자원을 제공 받았는가? (본 가이드라인 제3장 제2절의 클라우드 영역 분류 참조)			㈜	
⑥	기관에 필요한 네트워크장비 보안관리 관련 보안요구사항을 민간 사업자와의 계약 상에 반영하였는가?		√	-	
⑦	기관에 필요한 유지보수 관련 보안 요구사항을 민간 사업자와의 계약 상에 반영하였는가?		√	-	
⑧	민간 클라우드 컴퓨팅 서비스 외부로부터 발생하는 DDoS, 비인가 접속 등의 위협을 막기 위한 보안 대비책을 마련하고, 네트워크 모니터링 및 통제를 수행하고 있는가?			-	
가상화 인프라					
⑨	가상 머신, 가상 스토리지, 가상 애플리케이션 등의 가상 자원 사용 목록을 유지하고 있는가?	공통		-	
⑩	가상 자원 내에 존재하는 사용자 관련 데이터를 복구할 수 없는 형태로 삭제 후 가상자원을 회수하고 있는가?			-	
⑪	가상 자원에 대한 모니터링을 주기적으로 수행하고 있는가?			㈜	
⑫	기존 정보시스템 환경에서 클라우드 가상환경으로 이전 시 안전한 이전 수단을 이용하고 있는가?		√	-	
⑬	하이퍼바이저 관리 기능 및 관리자에 대한 접근 통제 방안을 마련하고, 하이퍼바이저에 대한 업데이트 및 보안패치를 최신으로 유지하고 있는가?	IaaS		-	
⑭	『국가 클라우드 컴퓨팅 보안 가이드라인』의 보안기준을 준수하는 클라우드 컴퓨팅 인프라 상에서 SaaS환경을 구축·개발·운영하고 있는가?	SaaS		-	

○ 가상환경 보안

번호	점검항목	적용 범위	자체 점검	권고 항목	점검 결과
보안 관리					
①	가상환경에서 시스템, 애플리케이션, SaaS 등을 자체 또는 외주로 도입 및 개발하고자 하는 경우 보안대책을 수립하였는가? ※ 운영 중인 클라우드 서비스 환경과 분리, 비인가 접근 통제 등	공통	√	-	
②	비인가자가 인터넷에 연결된 가상환경을 무단으로 조작하여 전산자료를 절취, 위·변조 및 훼손시키지 못하도록 보안대책을 마련하여 사용자의 인터넷 연결 가상PC에 적용하였는가? ※ 최신 백신 설치, 보안 취약 및 비인가 프로그램·장치 설치 금지, 문서 프로그램 읽기 전용 운영, 업무자료 저장 금지 등	IaaS	√	-	
③	PC 등 단말기 보안 관리에 준하는 보안 대책을 마련하고 사용자의 가상PC에 적용하였는가? ※ 가상 PC 접속용 장비·자료(문서자료 암호화 비밀번호)·사용자(접속 비밀번호)별 비밀번호 주기적 변경, 가상 PC 작업 일정 시간 이상 중단시 비밀번호 등을 적용한 화면보호, 최신 백신 운용·점검, 가상 운영체제(OS) 및 응용프로그램의 최신 보안패치 유지 등		√	-	
④	서버 관리자는 가상머신을 할당받아 가상서버를 운용할 경우, 해킹을 통한 자료 절취, 위·변조 등에 대비한 보안대책을 수립·시행하고 있는가? ※ 국가 정보보안 기본지침의 서버 보안을 준용		√	-	
⑤	비인가자의 가상서버 내 저장자료 절취 및 위·변조, 분산서비스거부(DDoS) 공격 등에 대비하기 위한 보안대책을 마련하였는가? ※ 국가정보원장이 안전성을 검증한 침입차단·탐지시스템 및 DDoS 대응시스템 설치, 불필요 계정 삭제, 프로그램 개발·시험을 위해 사용된 도구(컴파일러 등)를 개발 완료 후 삭제 등		√	-	
⑥	가상머신 내에 보안 상 취약한 소프트웨어 설치 방지, 보안업데이트 등의 보안 관리 방안을 마련하였는가?		√	-	
보안 관리 - SaaS 애플리케이션 개발					
⑦	SaaS 애플리케이션 설계 및 개발 단계에서 정책을 수립하여 사용 SaaS 애플리케이션 접근을 위한 안전한 인증 방안을 마련하고, 접근 권한 및 관리 권한을 부여하였는가?	SaaS	√	-	
⑧	SaaS 애플리케이션의 데이터 처리(송·수신, 저장, 연산 등) 과정에서 데이터를 보호하기 위한 수단을 마련하였는가?			㉮	
⑨	SaaS 애플리케이션 설계 및 개발 단계에서 연동 서비스 호출 시 송·수신되는 인증 정보, 메시지 등을 보호하기 위한 수단을 마련하였는가?			㉮	
⑩	SaaS 애플리케이션 설계 및 개발 단계에서 사용자 데이터에 대한 무결성 검증 방안을 마련하였는가?			㉮	

번호	점검항목	적용 범위	자체 점검	권고 항목	점검 결과
⑪	SaaS 애플리케이션은 사용자 업무 연속성을 보장할 수 있는 형태로 설계 및 개발되었는가?	SaaS		㉮	
⑫	보안 요구사항, 가용성 요구사항, 감사 요구사항, 법적 요구사항 등에 대한 준수 여부를 판별하기 위하여 SaaS에 대한 모니터링 및 로그 관리를 수행하는가?				
⑬	SaaS에서 생성된 로그 자료는 사후 추적대상을 식별할 수 있는 형태로 기록하고 1년 이상 보호하고 있는가?				
⑭	SaaS 애플리케이션 보안을 위해 주기적 취약점 점검, 보안 업데이트 등의 보안 관리 방안을 마련하였는가?			㉮	
⑮	자체 또는 외주로 SaaS 애플리케이션 개발을 하고자 하는 경우 보안대책을 수립하였는가? ※ 출처가 불명확한 소스코드 및 소프트웨어 사용 금지, 소스코드 및 소프트웨어 보안관리, 외부 인력 관리 등			-	
보안 관리 - 개발·운영 환경					
⑯	개발·운영 환경 접속을 위한 안전한 인증 방안을 마련하고, 접근 권한 정책을 수립하여 사용 및 관리 권한을 부여하였는가?	SaaS	√	-	
⑰	개발·운영 환경 관리에 필요한 데이터 보호 방안을 마련하였는가?			㉮	
⑱	개발·운영 환경 내 저장된 SaaS 관련 데이터에 대한 무결성 검증을 수행하는가?			㉮	
⑲	개발·운영 환경은 SaaS 운영 연속성을 보장할 수 있는 형태로 구축되었는가?			㉮	
⑳	보안 요구사항, 가용성 요구사항, 감사 요구사항, 법적 요구사항 등에 대한 준수 여부를 판별하기 위하여 개발·운영 환경에 대한 모니터링 및 로그관리를 수행하는가?				
㉑	개발·운영 환경 운영 중 생성된 로그 자료는 사후 추적대상을 식별할 수 있는 형태로 기록하고 1년 이상 보호하는가?				
㉒	개발·운영 환경 보안을 위해 주기적 취약점 점검, 보안 업데이트 등의 보안관리 방안을 마련하였는가?			㉮	
㉓	개발·운영 환경 구축을 위해 가상서버를 운용할 경우, 해킹을 통한 자료 절취, 위·변조 등에 대비한 보안대책을 수립·시행하였는가?			-	
㉔	개발·운영 환경 구축을 위해 공개용으로 운영되는 가상서버를 운용할 경우, 비인가자의 가상서버 내 저장자료 절취 및 위·변조, 분산서비스거부(DDoS) 공격 등에 대비하기 위한 보안 대책을 마련하였는가? ※ 국가정보원장이 안전성을 검증한 침입차단·탐지시스템 및 DDoS 대응시스템 설치, 불필요 계정 삭제, 프로그램 개발·시험을 위해 사용된 도구(컴파일러 등)를 개발 완료 후 삭제 등			-	

번호	점검항목	적용 범위	자체 점검	권고 항목	점검 결과
악성코드 방지					
㉕	웜·바이러스, 해킹프로그램, 스파이웨어 등 악성코드에 의한 위협을 제거하기 위해 악성코드 방지 대책을 수립·시행하는가?	공통	√	-	
㉖	가상머신에 악성코드가 설치되거나 감염된 사실을 발견하였을 경우에 조치를 하고 있는가? ※ 감염된 가상머신 사용중지 및 격리, 감염확산 방지를 위해 정보보안담당관에게 관련 사실 통보, 재발장비를 위한 원인분석 및 예방 등		√	-	
접근 통제					
㉗	이동식 저장매체 사용 통제, 다중요소(Multi-factor) 인증, 자동 로그아웃 등 접근 제한 방안을 마련하였는가?	공통	√	-	
㉘	사용자 및 장치를 유일하게 식별할 수 있는 식별 방법을 마련하고 식별 정보를 관리하는가?			-	
㉙	계정 권한 생성 절차를 마련하였는가? ※ 계정 유형 식별, 계정 그룹 설정, 클라우드 시스템 및 서비스 접근 허용자 식별, 게스트 또는 임시 계정에 대한 승인 및 모니터링 등		√	-	
㉚	사용자계정 보안관리 방안을 마련하여 사용자계정(ID) 부여 및 보안관리를 수행하는가? ※ 사용자·그룹별 접근권한 부여, 사용자 식별 수단이 없는 계정 사용 금지, 5회 이상 로그인 실패 시 접속 중단 등			-	
㉛	비밀번호 관리 방안을 마련하였는가? ※ 숫자·문자·특수문자 등 혼합 설정 및 정기적 변경, 사용된 비밀번호 재사용 금지, 응용프로그램 등을 이용한 자동 입력 금지 등		√	-	
㉜	접근 기록을 서비스 통제, 관리, 사고 발생 책임 추적성 등을 보장할 수 있는 형태로 기록하고 1년 이상 보관, 유지하고 있는가?			㉮	
㉝	SaaS를 관리 또는 접속하기 위해 스마트폰·IoT기기·전자제어장비 등 첨단 정보통신기기를 활용하고자 하는 경우 자체 보안대책을 수립하여 시행하고 있는가?	SaaS		㉮	

○ 데이터

번호	점검항목	적용 범위	자체 점검	권고 항목	점검 결과
데이터 관리					
①	민간 클라우드 컴퓨팅 서비스 이용시 데이터 유형, 법적 요구사항, 민감도 및 중요도에 따라 데이터를 분류하고 관리하고 있으며, 민간 사업자에게도 동일한 분류 및 관리를 요청하고 있는가?	공통	√	-	
②	민간 클라우드 컴퓨팅 서비스를 이용하고자 할 때, 사업자와 서비스 수준 협약 단계에서 데이터의 소유권을 명확히 명시하였는가?		√	-	
③	기관의 중요 데이터에 대한 입·출력, 전송 또는 교환 및 저장에 대한 민간 사업자의 데이터 무결성 확인 방안이 마련되었는가?			㊎	
④	민간 사업자는 데이터에 대한 접근제어, 위·변조 방지 등 데이터 처리에 대한 보호 기능을 이용자에게 제공하고 있음을 확인하고 있는가?			㊎	
⑤	기관의 데이터(백업자료 포함)의 물리적 위치를 확인하고 있으며, 민간 사업자는 데이터를 추적하기 위한 방안을 제공하고 있는가?			㊎	
⑥	민간 클라우드 컴퓨팅 서비스 이용의 종료, 이전 등에 따른 데이터 폐기 조치 시에 관련된 모든 데이터 폐기를 요청하고 폐기된 데이터를 복구할 수 없도록 삭제되었는지 확인하였는가?			-	
⑦	사용자별 데이터 보안 요구 사항 수준에 따라 물리적 또는 논리적으로 데이터를 사용자별로 분리할 수 있는 방안을 마련하여 SaaS 애플리케이션 및 개발·운영 환경을 구축하였는가?	SaaS		㊎	
⑧	데이터 송수신, 연산, 저장 시 데이터 암호화 등의 수단을 적용하여 SaaS 애플리케이션 취약점 등을 이용한 보안 위협으로부터 데이터 노출 시에 따른 기밀성을 유지하고 있는가?			㊎	
⑨	SaaS 애플리케이션 및 개발·운영 환경에서 처리되는 중요 데이터에 대한 무결성 검증을 수행하고 있는가?			㊎	
⑩	SaaS 애플리케이션 및 개발·운영 환경에서 생성되는 중요 데이터에 대한 추적성을 보장하고 있는가?			㊎	
⑪	SaaS 사용 종료 등의 이유로 인한 데이터 폐기 시 SaaS 환경 내에 존재하는 사용자 관련 데이터를 복구할 수 없는 형태로 삭제하고 있는가?			-	
암호화					
⑫	중요 업무자료에 대한 암호화 수준 등에 대한 보안요구사항을 도출하여 계약 시 반영하고, 중요 업무자료에 대한 생성·보관·처리·수신하기 위한 정책적·기술적 방안을 민간 사업자로부터 제공받았는가?	공통	√	-	
⑬	클라우드 시스템에 저장 또는 전송 중인 중요 업무자료를 보호하기 위한 암호 정책이 수립되었는가?			-	
⑭	암호키 관리 절차를 수립하고 암호키를 별도의 물리적으로 분리된 서버에 백업하고 최소 접근권한을 부여하여 관리하고 있는가?			-	

번호	점검항목	적용 범위	자체 점검	권고 항목	점검 결과

○ 인증 및 권한

번호	점검항목	적용 범위	자체 점검	권고 항목	점검 결과
인증					
①	민간 클라우드 컴퓨팅 서비스에서 사용자를 유일하게 구분할 수 있는 식별자를 할당하고 추측 가능한 식별자 사용을 제한하고 있는가?	공통	√	-	
②	민간 클라우드 컴퓨팅 서비스에 대한 접근을 사용자 인증, 접근 주체별 권한 부여, 로그인 횟수 제한, 불법 로그인 시도 경고 등 안전한 사용자 인증 절차에 의해 통제하고 있는가?		√	-	
③	민간 클라우드 컴퓨팅 서비스를 이용할 때 인증서(PKI)기반, OTP, 지문 등 다중요소(Multi-factor) 인증을 통한 강화된 인증 수단을 사용하고 있는가?		√	-	
④	기관 필요에 따라 클라우드 접근 대상 별로 기관의 인증 체계와 연동할 수 있는 인증 시스템을 설계 및 구축하였는가?		√	㉮	
권한					
⑤	민간 클라우드 컴퓨팅 서비스 및 중요정보에 대한 접근을 통제하기 위하여 공식적인 사용자 등록 및 해지 절차를 수립하고 업무 필요성에 따라 사용자 접근 권한을 최소한으로 부여하고 있는가?	공통	√	-	
⑥	민간 클라우드 컴퓨팅 서비스 및 중요정보 관리와 같은 특수 목적을 위해 부여한 계정 및 권한을 식별하고 별도로 통제하고 있는가?		√	-	
⑦	민간 클라우드 컴퓨팅 서비스 및 중요정보에 대한 접근을 관리하기 위하여 접근권한 부여, 이용(장기간 미사용), 변경(퇴직 및 휴직, 직무변경, 부서변경)의 적정성 여부를 정기적으로 점검하고 있는가?		√	㉮	

○ 사고 및 장애 대응

번호	점검항목	적용 범위	자체 점검	권고 항목	점검 결과
사고					
①	침해사고 발생 시 민간 사업자로부터 발생내용, 원인, 조치현황 등을 신속하게 파악하고 「국가 정보보안 기본지침」 등에 명시된 사고 대응절차를 수행하고 있는가?	공통	√	-	
②	민간 클라우드 컴퓨팅 서비스 이용 계약시 민간 사업자의 사고조사에 대한 적극적인 협조 및 지원의무를 명시하여야 하며, 필요시 국가정보원 및 이용기관의 조사 요청에 협조하고 있는가?		√	-	
장애					
③	민간 사업자는 관련 법률에서 규정한 클라우드 컴퓨팅 서비스의 중단으로부터 업무 연속성을 보장하기 위해 백업, 복구 등을 포함하는 장애 대응절차를 마련하였으며, 이용기관은 장애 대응 요구사항, 담당자 정의 및 연락처 등을 담은 장애 대응절차를 마련하고 있는가?	공통	√	-	
④	이용 기관은 서비스 수준 협약에 업무영향도 평가 등을 통해 산정한 복구시간을 서비스 수준 협약(SLA)에 반영하여야 하며, 민간 사업자는 서비스 수준 협약(SLA)에 명시된 시간 내에 장애 대응절차에 따라 해당 서비스의 장애를 처리하고 복구시키고 있는가?		√	-	
⑤	민간 사업자와 협의하여 장애 관련 정보를 활용하여 유사한 서비스 중단이 반복되지 않도록 장애 재발방지 대책을 수립하고, 필요한 경우 장애 대응 절차도 변경하고 있는가?		√	-	

3. SaaS 구축 유형별 보안기준 체크리스트

○ 국가·공공기관 구축 컴퓨팅 인프라 이용 : 내부 구축

번호	점검항목	점검결과	비고
	기관 내부 SaaS 사용자에 의한 기관 내부 SaaS 접근		
1	기관 내부 SaaS 사용자가 기관 내부의 사용자 영역에 위치한 지정 단말을 통해 SaaS 접근하고 있는가?		
2	기관 내부 SaaS 사용자가 인터넷이 연결된 SaaS 사용 시 내부 업무 영역과 분리된 환경에서 접근하고 있는가?		
3	사용자 영역과 관리자 영역이 분리 운영되고, SaaS 환경 관리를 위한 단말을 지정하여 관리하고 있는가?		
	원격지에 위치한 인가된 SaaS 사용자에 의한 기관 내부 업무용 SaaS 접근		
4	원격지에 위치한 인가된 SaaS 사용자가 기관 내부에 구축된 SaaS에 접근 시 전용선 또는 암호화 통신(VPN 등)을 사용하고 있는가?		
5	내부 침입차단시스템을 이용하여 원격지에 위치한 인가된 SaaS 사용자가 접근 가능한 SaaS 기능 및 영역을 제한하고 있는가?		
6	IDS, IPS 등의 보안 장비를 통하여 VPN 서버를 통해 내부로 유입되는 악성트래픽을 탐지 및 차단하고 있는가?		
	기관 내부에 위치한 SaaS와 외부에 위치한 연동 서비스 간 연계		
7	외부 연동 서비스와 연계가 필요한 SaaS가 DMZ 영역에 위치하고 있는가?		
8	연동 서비스와의 인증 및 메시지 송·수신 시 암호화 등의 수단을 적용하여 보안 위협으로 노출된 데이터에 대한 기밀성을 유지하고 있는가?		
9	연동 서비스가 DMZ 영역에 위치한 SaaS와만 통신이 가능하고, 침입차단시스템을 이용하여 연동 서비스의 DMZ 영역이외의 SaaS 영역으로의 접근을 차단하고 있는가?		
10	DMZ 영역에 위치한 SaaS와 기관 내부 SaaS 영역 간의 연계가 연계서버를 통해서만 이루어지고, 그 외의 접근은 침입차단시스템을 이용하여 차단되고 있는가?		

○ 국가·공공기관 구축 컴퓨팅 인프라 이용 : 커뮤니티 구축

번호	점검항목	점검결과	비고
	커뮤니티 클라우드 컴퓨팅 인프라에 위치한 업무용 SaaS에 기관 내부 SaaS 사용자 접근		
11	도입 기관 내부 SaaS 사용자가 전용선 또는 암호화 통신(VPN 등)을 통하여 커뮤니티 클라우드 컴퓨팅 인프라에 구축된 도입 기관의 업무용 SaaS에 접근하고 있는가?		

12	커뮤니티 클라우드 컴퓨팅 인프라에 구축된 도입 기관 SaaS가 타 기관 SaaS 영역과 분리되어 운영되고 있는가?		
13	도입 기관 SaaS를 위한 애플리케이션 스토리지 및 개발·운영 가상환경 관리 관련 스토리지가 타 기관의 스토리지와 분리되어 운영되고 있는가?		
커뮤니티 클라우드 컴퓨팅 인프라 내에 도입 기관 SaaS 자체 개발			
14	커뮤니티 클라우드 컴퓨팅 인프라 내에서 도입 기관이 자체적으로 SaaS를 개발하는 경우 기관 내에 사용자 영역과 개발자 영역을 분리하여 개발을 수행하고 있는가?		
15	도입 기관 내부 SaaS 개발자가 기관 내부 개발자 영역에 위치한 지정 단말을 통해서 SaaS 개발을 수행하고 있는가?		
16	도입 기관 내부 SaaS 개발자가 전용선 또는 암호화 통신(VPN 등)을 통하여 커뮤니티 클라우드 인프라에 구축된 개발·관리 기능에 접근하고 있는가?		
커뮤니티 클라우드 인프라 내 도입 기관 SaaS와 타 기관 SaaS 상호 연계			
17	커뮤니티 클라우드 컴퓨팅 인프라 상에 구축된 타 기관 SaaS와 도입 기관 SaaS 간의 통신이 연계 서버를 통해서만 이루어지고 있는가?		
18	타 기관 SaaS와의 연계를 위한 연계 서버 운용 시 도입 기관은 연계 서버 관리에 대한 접근 제한 정책, 인증 강화, 로그데이터 수집 등과 같은 보안관리 정책을 수립하고 있는가?		

○ 민간 클라우드 컴퓨팅 인프라 이용

번호	점검항목	점검결과	비고
민간 클라우드 컴퓨팅 인프라에 구축된 도입 기관 업무용 SaaS에 기관 내부 SaaS 사용자 접근 - 『공통』			
1	기관 내부 SaaS 사용자가 전용선 또는 암호화 통신(VPN 등)을 통하여 민간 클라우드 컴퓨팅 인프라에 구축된 기관의 업무용 SaaS에 접근하고 있는가?		
2	민간 클라우드 서비스 영역과 국가·공공기관 클라우드 서비스 영역은 물리적/논리적으로 분리되어 구축 및 운영되고 있는가?		
3	도입 기관 SaaS 영역이 국가·공공기관 영역 내에 존재하는 타 기관 SaaS 영역과 분리되어 있는가?		
기관 SaaS 영역 내 위치한 SaaS와 외부에 위치한 연동 서비스 간 연계 - 『공통』			
4	외부 연동 서비스와 연계가 필요한 SaaS가 DMZ 영역에 위치하고 있는가?		
5	연동 서비스와의 인증 및 메시지 송·수신 시 암호화 등의 수단을 적용하여 보안 위협으로 노출된 데이터에 대한 기밀성을 유지하고 있는가?		
6	연동 서비스가 DMZ 영역에 위치한 SaaS와만 통신이 가능하고, 침입차단시스템을 이용하여 연동 서비스의 DMZ 영역이외의 기관 SaaS 영역으로의 접근을 차단하고 있는가?		

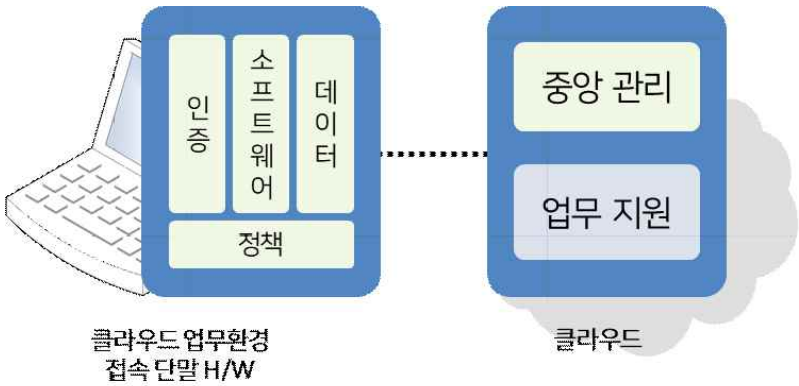
7	DMZ 영역에 위치한 SaaS와 기관 내부 SaaS 영역 간의 연계가 연계서버를 통해서만 이루어지고, 그 외의 접근은 침입차단시스템을 이용하여 차단되고 있는가?		
민간 클라우드 컴퓨팅 인프라 내 도입 기관 SaaS 자체 개발 - 『기관에서 SaaS 개발』 유형			
8	민간 클라우드 컴퓨팅 인프라 내에 도입 기관이 자체적으로 SaaS를 개발하는 경우 사용자 영역과 분리된 개발자 영역에서 SaaS 개발이 수행되고 있는가?		
9	도입 기관 내부 SaaS 개발자가 기관 내부 개발자 영역에 위치한 지정 단말을 통해서 SaaS 개발을 수행하고 있는가?		
10	도입 기관 내부 SaaS 개발자가 전용선 또는 암호화 통신(VPN 등)을 이용한 암호화 통신을 통하여 민간 클라우드 인프라에 구축된 개발·관리 기능에 접근하고 있는가?		
국가·공공기관용 SaaS 민간 개발 **- 『민간에서 SaaS 개발』 유형**			
11	국가·공공기관 SaaS를 개발하는 민간 사업자에 대한 보안 관리를 기관의 용역업체 보안관리 규정에 따라 수행하고 있는가?		
12	SaaS를 위한 SaaS 애플리케이션은 「행정기관 및 공공기관 정보시스템 구축·운영 지침」 및 「소프트웨어 개발보안 가이드」(행정안전부)에 따라 개발되었는가?		
13	민간 사업자가 국가·공공기관용 SaaS를 민간 클라우드 컴퓨팅 인프라 상에서 개발하는 경우 국가·공공기관 담당 SaaS 개발 및 관리자를 지정하여 운영하고 있는가?		

[부록 5] 클라우드 업무환경 접속단말 보안기준

클라우드 업무환경 접속단말(이하, 접속단말)을 대상으로 하는 사이버 위협은 클라우드로 전이하여 대규모 피해를 야기할 수 있다. 본 가이드는 이러한 피해를 사전에 예방하고, 클라우드 최외곽을 담당하는 접속단말의 보안성 제고를 위하여, 단말 운용 시 참고할 수 있는 보안기준을 제시한다. 이를 위해 접속단말 구성요소를 정의하고 보안 위협을 식별하며, 국가·공공기관 정보시스템 보안관리 체계 및 클라우드 기반 업무환경의 특성을 고려하여, 보안 원칙 및 기준을 제시한다.

1. 클라우드 업무환경 접속단말 구성요소

클라우드 업무환경 접속단말의 구성요소 및 클라우드 서비스와의 상호 관계를 [그림 30]과 같이 도식화할 수 있다.



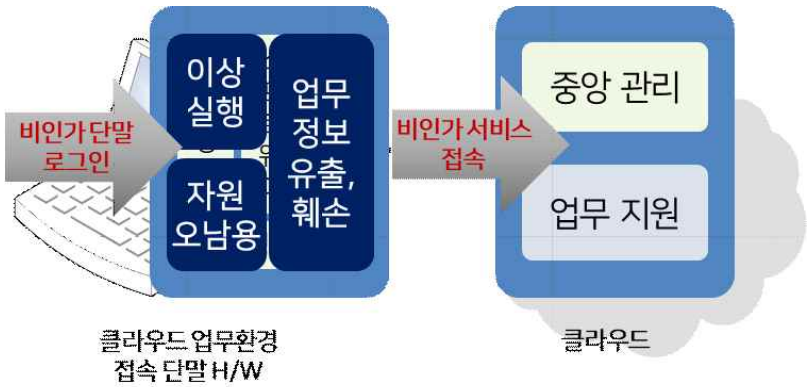
[그림 30] 클라우드 업무환경 접속단말 및 서비스 연동 구조

- 인증: 안전한 클라우드 서비스 이용을 위한 단말·사용자 식별·인증
- 소프트웨어: 접속단말 하드웨어를 운용하기 위한 소프트웨어 집합으로서 다음과 같이 구성
  - o 응용프로그램: 웹브라우저, 바탕화면 조정 등 클라우드 서비스 접속에 필요한 소프트웨어 및 사용자 인터페이스 등
  - o OS: 펌웨어, 부트로더, 커널, 시스템 라이브러리, 장치 드라이버, 시스템 서비스 등 응용프로그램 실행 지원을 위한 소프트웨어
- 데이터: 사용자 업무 수행을 위해 클라우드와 교환하는 정보

- 중앙 관리: 보안정책 배포, 감사 증적 등 중앙집중적 단말 보안 관리를 위한 서비스
- 업무 지원: 오피스, 저장소 등 사용자 업무 지원 서비스로서 기존 설치형 응용 프로그램의 기능을 대체

2. 클라우드 업무환경 접속단말 보안 위협 및 대응방안

클라우드 업무환경 접속단말과 관련하여 발생 가능한 보안위협을 [그림 31], [표 20]과 같이 정리할 수 있다.



[그림 31] 클라우드 업무환경 접속단말 보안 위협

구성요소	위협분류	사례
인증	비인가 단말 로그인	- 미등록 단말 사용 - 사용자 인증정보 도용, 위·변조
	비인가 서비스 접속	- 서비스 접속용 인증 정보 도용 및 위·변조
소프트웨어	이상 실행	- 펌웨어·부트로더 변조를 통한 시스템 탈취 - 루트킷 등 OS 변조를 통한 악성 코드 실행 - 응용프로그램 위·변조, 외부에서 악성코드 다운로드
데이터	업무 정보 유출·훼손	- 단말 내 업무·관리 정보 유출, 위·변조 - 비인가 연결을 통한 임의 정보 유출
정책 중앙 관리	자원 오남용	- 시스템디렉토리 등 비인가 논리자원 접근 - USB 메모리스틱, Wi-Fi 동글 등 비인가 주변장치 연결

[표 20] 클라우드 업무환경 접속단말 보안 위협의 분류와 사례

클라우드 업무환경 접속단말 구성요소별 보안 위협 대응을 위해 요구되는 보안속성 및 대응 방안을 정리하면 [표 21] 및 [표 22]와 같다.

보안속성	내 용
인증·권한	클라우드 서비스 및 접속단말 사용 시, 등록된 단말을 통해 인증을 완료한 사용자에 한하여, 인가된 범위 내에서 사용
기밀성	접속단말 내에서 데이터를 처리하는 동안 비인가자가 데이터의 내용을 알 수 없도록 보장
무결성	접속단말 내에서 데이터를 처리하는 동안 비인가자가 데이터를 위·변조할 수 없도록 보장
가용성	인가된 사용자가 항상 접속단말을 사용할 수 있도록 전산 자원 (중앙처리장치, 저장장치, 네트워킹 등)의 고갈 방지
감사·관리	관리자가 클라우드를 통해 접속단말의 보안 관련 기능을 원격 제어하고, 접속단말의 보안 관련 상태를 안전하게 기록·조회할 수 있도록 보장

[표 21] 클라우드 접속단말 보안 요구 속성

구성요소	위협분류	대응방안	요구속성
인증	비인가 단말 로그인 비인가 서비스 접속	- 클라우드가 제공하는 인증 서비스를 통해 사용자 인증 - 미식별 단말은 클라우드 서비스 접속 거부	인증·관리성
소프트웨어	이상 실행	- 부트 절차 및 프로그램 위·변조 방지 - 커널 및 시스템 주요 실행파일 위·변조 방지 - 응용 프로그램 위·변조 방지	권한·무결성
데이터	업무 정보 유출·훼손	- 업무 정보는 클라우드에 저장 - 임시 저장 정보의 복제·변조·유출 방지	권한·기밀성
정책 중앙 관리	자원 오남용	- 사용자·프로세스의 자원 접근 권한 차등화 - 개인 USB 메모리 스틱 등 비인가 장치 통제 - IrDA, Wi-Fi 동글 등 무선 데이터 교환 장치 통제	권한·가용성·감사·관리

[표 22] 접속단말 요소 별 위협 대응 방안

3. 보안 기본원칙

클라우드 접속단말을 위한 보안 원칙은 기존 국가·공공기관 정보시스템 보안관리 체계의 연속성 유지를 목적으로 하되 클라우드 컴퓨팅의 기술적·관리적 특성을 고려하여 정의한다.

가. 정책적 측면에서의 기본원칙

○ 도입 전산장비 안전성 확인

- 클라우드 업무환경 구축 시, 클라우드 접속단말은 클라우드 인프라·플랫폼·서비스와 독립적인 요소가 아닌 통합요소로 간주하며, 보안성을 확인한 후 클라우드 기반 업무에 활용

○ 인터넷 · 업무망 분리

- 접속단말을 통해 인터넷과 업무 영역 간 데이터 교환이 발생하지 않도록 통제 대책을 마련

나. 기술적 측면에서의 기본원칙

○ 인증된 단말 및 사용자에 한하여 클라우드 접속 허용

- 클라우드에 접속 가능한 단말을 식별·구분할 수 있도록 대책을 마련하여, 임의의 단말을 클라우드에 연결하지 않도록 제한
- 접속이 인가된 단말에 한하여 기관망과의 안전한 네트워크 수립 후 접속단말 로그인 사용자 인증 수행
- 접속단말 로그인 사용자의 식별·인증 정보는 클라우드를 통해 등록·관리하며, 사용자 로그인 시 클라우드와 연계하여 인증 처리

  * 클라우드 접속을 위한 사용자 인증시 다중요소(Multi-factor) 인증 적용

○ 접속단말 소프트웨어 통제

- 단말관리자는 신뢰할 수 있는 소프트웨어를 사용하여 접속단말을 구성·운용하

며, 사용자가 임의의 소프트웨어를 설치·실행할 수 없도록 통제

- 접속단말의 OS 및 주요 시스템 소프트웨어(라이브러리, 서비스 데몬 등)를 위·변조할 수 없도록 통제
- 단말관리자는 접속단말을 신뢰할 수 있는 소프트웨어로만 구성·운용할 수 없을 경우, 백신 등 정보보호 보조 프로그램을 이용하여 응용 프로그램의 안전성을 확인

○ 단말에 업무 데이터 장기 보관 금지

- 사용자가 작성한 업무데이터는 클라우드 저장소에 저장한다.
- 안정적인 원격작업을 위해 단말에 임시 저장하는 파일은 작업 종료 후 또는 사용자 로그아웃 시 삭제
- 단말관리자의 인가 없이, 업무 정보를 클라우드를 통하지 않고 접속단말에서 직접 임의 반출·입하거나, 외부 장치로 임의 전송하지 않도록 보호조치

○ 클라우드를 통해 중앙 집중적 관리·통제 시행

- 단말관리자는 보안정책, 즉 접속단말의 보안성 유지에 필요한 제반 규칙·설정 집합을 정의하여 접속단말에 배포

  * 보안정책은 접속단말에 적용할 접근권한 규칙, 네트워크 통제 규칙, 주변장치 연결 규칙, 각종 서비스 설정 등을 포함

- 접속단말은 단말관리자가 배포하는 보안정책을 적용하고, 단말관리자의 요청에 따라 적용 결과를 반환
- 일반 사용자는 단말관리자가 정의한 보안정책을 임의로 수정 불가

  * 사용자는 보안정책에 명시된 바를 벗어나 접속단말의 자원을 사용하거나, 단말을 외부 장치 또는 네트워크와 연동할 수 없음

- 관리자는 클라우드를 통해 단말의 보안 상태 점검을 요청하고, 단말은 요청에 따라 보안 상태를 점검하여 관리자에게 전달
- 단말의 사용 및 보안 위협 발생과 관련하여 단말에서 수집한 주요 감사 이벤트는 클라우드에 전송, 저장
- 클라우드는 단말의 소프트웨어 업데이트·패치 상태, 보안 기능 실행 여부 등 보안 상태를 점검하여 안전하게 운용되고 있다고 판단되는 경우에만 접속을 허용

4. 세부 보안기준

가. 정책

○ (접속단말 시스템 보안책임) 클라우드 업무환경 구축 시, 해당 기관의 장은 접속단말의 사용자 및 단말관리자, 관리책임자를 지정 운용한다.

- 사용자는 접속단말 등 소관 정보시스템을 사용하거나 본인 계정으로 클라우드 업무환경에 접속하는 것과 관련한 보안책임을 가짐
- 단말관리자는 부서에서 사용하는 접속단말 하드웨어 및 소프트웨어 설치·설정 및 접속단말 운용에 필요한 서버·네트워크 장비 등 공동 사용 정보시스템의 운용과 관련한 보안책임을 가짐
- 클라우드 업무환경 접속단말 시스템을 운용하는 부서의 장은 해당 시스템의 관리책임자가 되며 주기적으로 클라우드 업무환경 운용과 관련된 정보보안담당관에게 관련내용을 통보
- 정보보안담당관은 클라우드 업무환경 접속단말의 운용과 관련하여 보안대책이 필요하거나 보안취약점을 발견할 경우, 사용자 및 단말관리자에게 시정을 요구할 수 있다.

○ (접속단말 관리) 단말관리자는 비인가자가 접속단말을 무단으로 조작하여 전산자료를 절취, 위·변조 및 훼손하지 못하도록 관리한다.

- 단말관리자는 다음과 같은 보안대책을 제공
  ① 단말 부팅 비밀번호를 설정하여 사용하고 주기적으로 변경·사용
  ② 단말 펌웨어 메뉴 진입 비밀번호를 설정하여, 사용자가 부팅 방법, 부팅 미디어, 부팅 순서 등을 임의변경하지 못하도록 보호
  ③ 커널 및 데몬 위·변조 방지 등 OS 보호

④ 실행파일 보호, 악성코드 탐지 등 응용 소프트웨어 보호

⑤ 10분 이상 사용자 입력 중단 시 화면보호기를 표시하고, 화면보호 해제 비밀번호 사용

⑥ OS·응용프로그램의 최신 업데이트 및 보안패치 적용

⑦ 그 밖에 국가정보원장이 안전성을 확인하여 배포한 프로그램의 운용 및 보안권고문 시행

- 정보보안담당관은 사용자가 접속단말의 교체·반납·폐기를 요청하거나, 고장으로 외부에 수리를 의뢰할 때, 하드디스크에 수록된 자료나 사용자 인증정보가 유출되지 않도록 조치
- 단말관리자는 사용자가 접속단말 등을 기관 외부로 반출하거나 내부로 반입할 경우 소프트웨어 위·변조, 악성코드 감염 등 접속단말의 보안상태를 점검

○ (사용자의 접속단말 보안관리) 정보보안담당관은 접속단말 보호를 위해 다음과 같은 보안대책을 접속단말 사용자에게 지원하며, 사용자는 이를 준수한다.

- 사용자(로그온 비밀번호)·자료(문서자료 암호화 비밀번호)·서비스(클라우드 서비스 접속 비밀번호) 별 비밀번호를 주기적으로 변경·사용
- 업무상 불필요한 프로그램의 설치·실행 금지
- USB 메모리 스틱CD/DVD 등 이동식 저장매체, 프린터스캐너 등 입출력 장치는 관리자의 인가를 득한 후에만 연결·사용
- 기관이 직접 관리하지 않거나, 운영을 위탁한 바 없는 네트워크 장비(사설 또는 공공장소의 Wi-Fi AP, 상용 3G/4G 장비 등)를 통한 상용 인터넷 접속 금지
- 상기 단말관리자의 접속단말 보안관리 행위 방해 금지
- 개인 소유의 PC 등 비인가 단말을 사용하여서는 아니되며, 부득이한 경우에는 정보보안담당관의 승인을 받아 사용

나. 인증 및 권한 관리

○ (기관 클라우드 인증 체계 연동) 기관은 클라우드 기반 업무환경 구축 시 클라우드 서비스 접속을 위한 통합 인증 체계를 구축하고, 해당 체계를 이용하여 접속단말 및 사용자 식별·인증을 처리할 수 있도록 시스템 연동 방안을 마련한다.

- 인가된 접속단말이 기관 인증 시스템과의 안전한 네트워크 수립 후 접속단말 사용자 인증을 수행할 수 있도록 인증 체계 구축(VPN선행인증 등)

○ (권한 관리) 단말관리자는 사용자에게 허용된 또는 금지된 행위를 구분하여 접근 정책을 정의한다.

다. 소프트웨어 보호

○ (부팅 보호) 단말관리자가 지정한 방법 외의 절차나 소프트웨어를 사용하여 접속단말을 부팅하지 않도록 한다.

○ (OS 및 응용 프로그램 보호) 악성코드·해킹 등 사이버위협에 대응하기 위하여 다음과 같이 보호한다.

- 신뢰할 수 있는 제작자가 개발한 소프트웨어 설치
- 설치한 소프트웨어는 보안정책에 따라 실행 및 설정
- 소프트웨어 실행파일의 위·변조 방지

○ (소프트웨어 제한) 클라우드 접속 이외의 기능을 제공하거나 업무 정보를 유출할 가능성이 있는 소프트웨어의 사용을 제한한다.

- 인증서버, 네임서버, 메일서버, 웹서버, 파일서버, 프린터서버 등 비인가 서비스의 설치·실행 금지
- 명령행 인터페이스를 통한 임의 명령 실행 금지
- 업무 정보를 외부에 평문 형태로 전송하는 소프트웨어 사용 금지

라. 데이터

○ (클라우드 저장소를 통한 정보 교환) 사용자가 작성·처리하는 업무 정보는 단말이 아닌 클라우드에 저장하는 것을 원칙으로 한다.

- 업무 연속성 및 효율성 제공을 위해 로그인 한 사용자가 읽거나 수정 가능한 업무 정보를 단말 내에 임시 저장
- 단말 내에 임시 저장한 정보는 사용자 로그아웃 시 모두 삭제

○ (용도별 저장영역 관리) 단말 내 데이터를 용도에 따라 분류하고, 별도의 영역에 저장하여, 한 영역에서 발생한 논리적 오류나 공간 소모로 인한 타 영역 영향을 최소화한다.

- 시스템 데이터: OS 및 서비스의 실행 파일, 설정 파일 등
- 공용 데이터: 시스템과 사용자가 공유하는 데이터
- 사용자 데이터: 사용자가 업무 수행을 위해 클라우드 서비스를 사용하여 생산·처리하는 데이터
- 감사 데이터: 감사를 목적으로 생성하는 데이터

○ (임의 정보 교환 금지) 근거리 통신(IrDA, 블루투스 등)을 이용하여, 단말과 외부장치 간 데이터를 임의 교환하지 않도록 한다.

○ (통신데이터 암호화) 접속단말과 클라우드 업무환경간 통신데이터는 암호화하여 송수신한다.

마. 중앙 관리

○ (단말의 배포) 단말관리자는 단말에 필요한 소프트웨어를 설치하고 초기 구동, 사용자 인증 및 클라우드 서비스 접속에 필요한 설정을 완료하여 사용자에게 전달한다.

○ (보안 정책 배포) 단말관리자는 접속단말 내에서 허용·금지된 사용자 권한, 네트워크 접속 규칙, 주변장치 연결 등의 단말 설정을 포함한 보안정책을 수립하여 단말에 배포한다.

○ (모니터링) 단말의 신뢰부팅 상태, 보안관리 상태 등을 중앙에서 단말관리자가 원격 모니터링할 수 있도록 한다.

○ (업데이트·패치) 단말에 설치한 소프트웨어의 최신 업데이트·보안 패치를 중앙에서 단말관리자가 강제 적용할 수 있도록 한다.

○ (감사 로그 관리) 접속단말은 다음과 같은 대상들을 감사정보로 기록하고, 클라우드로 전송한다.

- 사용자 및 단말관리자 계정 로그인 성공/실패 이벤트
- 계정관리 이벤트
- 데이터 접근 이력
- 보안정책 변경 이력 및 시스템 업데이트·패치
- 응용 소프트웨어 설치·실행
- 보안정책 위반 여부
- 비정상 네트워크 접근 기록

○ (감사 정보 보호) 감사를 목적으로 생성한 정보는 인가된 사용자만 열람할 수 있도록 접근을 통제하고, 유실되지 않도록 보호한다.

[부록 6] 클라우드 가상화 기술 보안기준

1. 목적 및 필요성

클라우드 컴퓨팅은 5G, AI 및 IoT를 비롯한 신규 정보통신기술(ICT)의 기반 인프라로 지목되고 있으며, 코로나19로 인한 디지털 업무 수요에 따라 국가·공공기관 업무 환경의 클라우드 컴퓨팅 전환이 본격화되고 있다. 이러한 흐름은 정부가 「제3차 클라우드 컴퓨팅 발전 기본계획」(`21.09.)에 따른 국가 클라우드 전면 전환을 추진하면서 더욱 가속화될 전망이다.

클라우드 컴퓨팅의 확산과 함께 항상 거론되는 것은 보안 문제이다. 클라우드 컴퓨팅은 기존 레거시 컴퓨팅 환경의 보안 위협을 상속하면서, 가상화 기술의 구조적 취약성을 모두 포함한다. 예를 들어, 기존 컴퓨팅 환경이 포함하는 서버·네트워크 구성요소의 보안 취약성과 함께 가상머신 또는 컨테이너와 같은 가상 인스턴스에 대한 탈출 문제, 그리고 가상 인스턴스를 관리하는 가상화 관리 제품 및 오케스트레이터 보안 취약성 등을 함께 고려해야 한다.

클라우드 컴퓨팅의 기반이 되는 하이퍼바이저 가상화 기술 및 컨테이너 가상화 기술에 대한 이해를 바탕으로 안전한 국가·공공기관 클라우드 컴퓨팅 활용을 유도하기 위한 보안기준을 제시한다. 각 점검항목은 중요도와 보안성에 따라 필수, 권고 및 선택으로 제시하였다. 또한 중요도가 높은 사항이라도, 가용성에 영향을 미칠 수 있거나 보편적인 배포 환경이 보안기준을 수용하기 어렵다고 판단되는 경우에 권고 또는 선택으로 제시하였다.

또한, 클라우드 컴퓨팅 기반의 정보화 사업 수행 시 참고할 수 있는 보안기준 및 점검항목을 제시하여 국가·공공기관 담당자들의 가상화 기술에 대한 이해와 보안 의식을 제고하고 정부 업무 서비스의 핵심 인프라인 클라우드 컴퓨팅에 대한 신뢰성과 보안성 향상에 기여할 수 있기를 기대한다.

2. 하이퍼바이저 가상화 기술 구성요소 및 보안기준

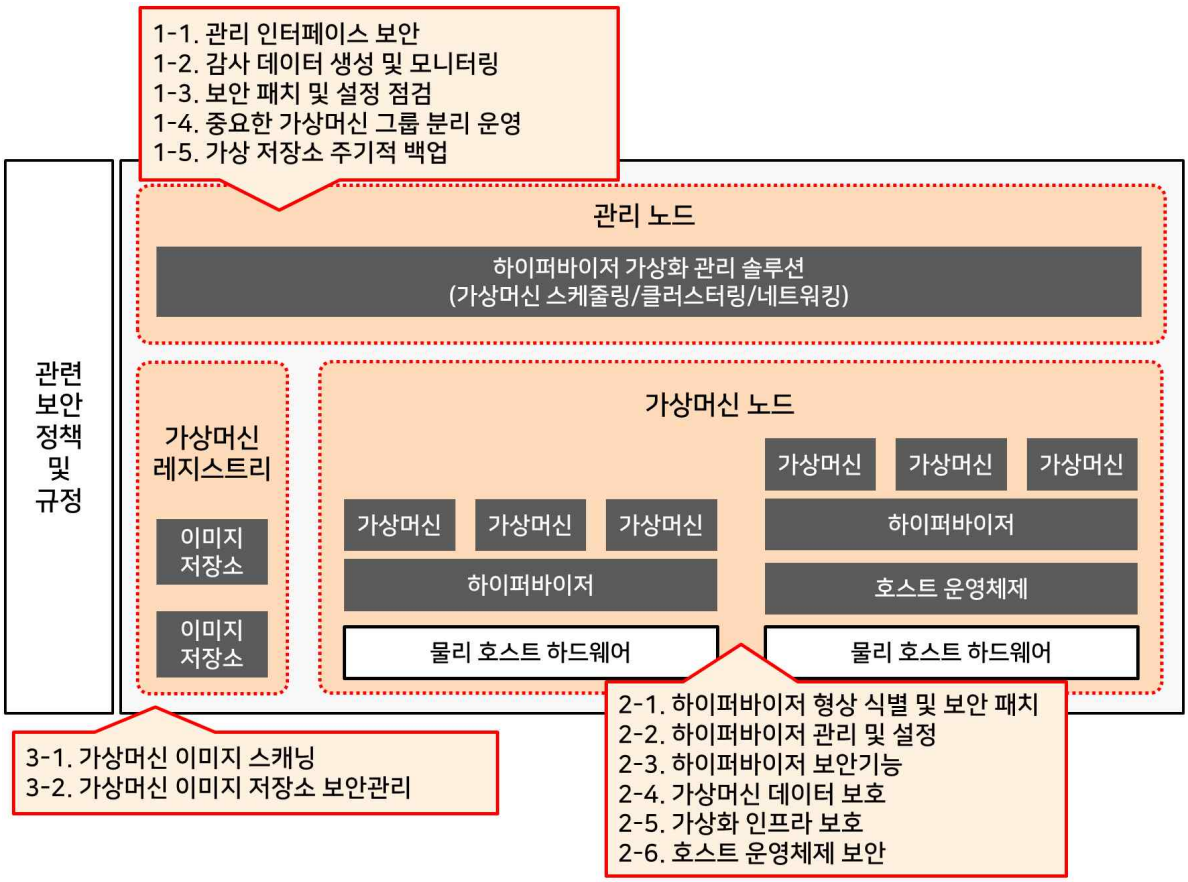
하이퍼바이저 가상화 기술을 활용할 경우 컴퓨팅 자원을 효율적으로 사용할 수 있고 서로 다른 운영체제 및 애플리케이션을 동시에 사용할 수도 있다. 클라우드 환경에서 새로운 자원이 필요한 경우, 신속하게 가상머신을 추가하여 이용하는 것이 가능하며 제공되는 가상서버와 가상PC를 일정한 수준으로 운영 및 관리 할 수 있다.

일반적인 가상화 제품 및 가상화 관리 제품의 구성을 참고하여 하이퍼바이저 가상화 기술 스택의 구성요소와 기능 및 역할을 다음과 같이 살펴볼 수 있다.

구성요소	기능 및 역할
[관리 노드]	하이퍼바이저 가상화 관리 솔루션이 실행되는 호스트 시스템
하이퍼바이저 가상화 관리 솔루션	관리자가 가상머신 노드와 하이퍼바이저를 제어하고 가상머신의 게스트 운영체제를 시작종료하고 새로운 가상머신 이미지를 생성하는 등 가상머신 스케줄링, 클러스터링 및 네트워킹 등 관리 (vSphere 등)
[가상머신 노드]	하이퍼바이저 가상화 환경이 운영되는 호스트 시스템
가상머신	자체 프로세서, 메모리, 네트워크 인터페이스, 스토리지를 가지고 하이퍼바이저 중계로 자원을 사용하는 가상 컴퓨터 시스템 환경 · 하이퍼바이저의 접근제어에 의해 각 가상머신이 사용 가능한 하드웨어 자원은 다른 가상머신과 격리되거나 공유 · 해당 자원을 활용하는 게스트 운영체제와 어플리케이션으로 구성
하이퍼바이저	하드웨어와 가상머신 사이에 존재하며 컴퓨팅 자원을 중계하여 가상화 계층을 구현하는 소프트웨어 · Type-1 하이퍼바이저 환경에서는 하이퍼바이저가 하드웨어를 제어하는 호스트 운영체제 역할을 수행 (Xen, ESXi 등) · Type-2 하이퍼바이저 환경에서는 호스트 운영체제 위에 별도 하이퍼바이저 모듈이 설치되어 동작 (VirtualBox 등)
호스트 운영체제	Type-2 하이퍼바이저 환경에서 하이퍼바이저와 하드웨어를 중계
[가상머신 레지스트리]	가상머신 이미지가 저장되는 저장소
이미지 저장소	가상머신 이미지와 스냅샷 이미지를 관리하는 이미지 저장소를 다양한 방법으로 구성하여 운영
[관련 보안정책 및 규정]	· 「국가 정보보안 기본지침」, 국가정보원 · 「국가 클라우드 컴퓨팅 보안 가이드라인」, 국가정보원 · 하이퍼바이저는 가상환경을 구현해주는 '가상화 제품'에 해당, CC인증 대상이지만 도입 요건을 필수가 아닌 권고로 제시 (2021.4.14부터 적용, 국가정보원 홈페이지 참조)

[표 23] 하이퍼바이저 가상화 기술 구성요소와 기능 및 역할

하이퍼바이저 가상화 기술 스택을 기반으로, 가상머신 기반 정부 업무 인프라의 안전성과 신뢰성을 제고하기 위한 보안기준의 전체 구성은 다음 예시와 같다.



[그림 32] 하이퍼바이저 가상화 기술 스택에 대한 보안기준

보안기준은 하이퍼바이저 가상화 기술 스택 구성요소인 관리 노드, 가상머신 노드 및 가상머신 레지스트리로 분류되어 있으며, 총 13개 보안기준과 39개의 세부 점검 항목을 제시한다. 각급 기관은 가상머신 기반의 업무 서비스 도입 및 운영 시 해당 보안 가이드의 내용을 준수해야 하며, 불가피하게 보안기능 및 설정을 해제할 경우 한시적으로 허용하며 별도의 보안대책을 마련하고 국가정보원 담당자와 협의해야 한다.

3. 컨테이너 가상화 기술 구성요소 및 보안기준

컨테이너 가상화 기술을 활용할 경우 자원의 신속한 확장이 가능하고 개발 환경에서 빌드한 컨테이너 이미지의 복사본을 운영 환경에서 그대로 실행할 수 있다. 해당 기술은 클라우드에 최적화된 서비스 구조인 마이크로서비스를 구축하고 운영하기에 적합한 특성을 갖고 있다.

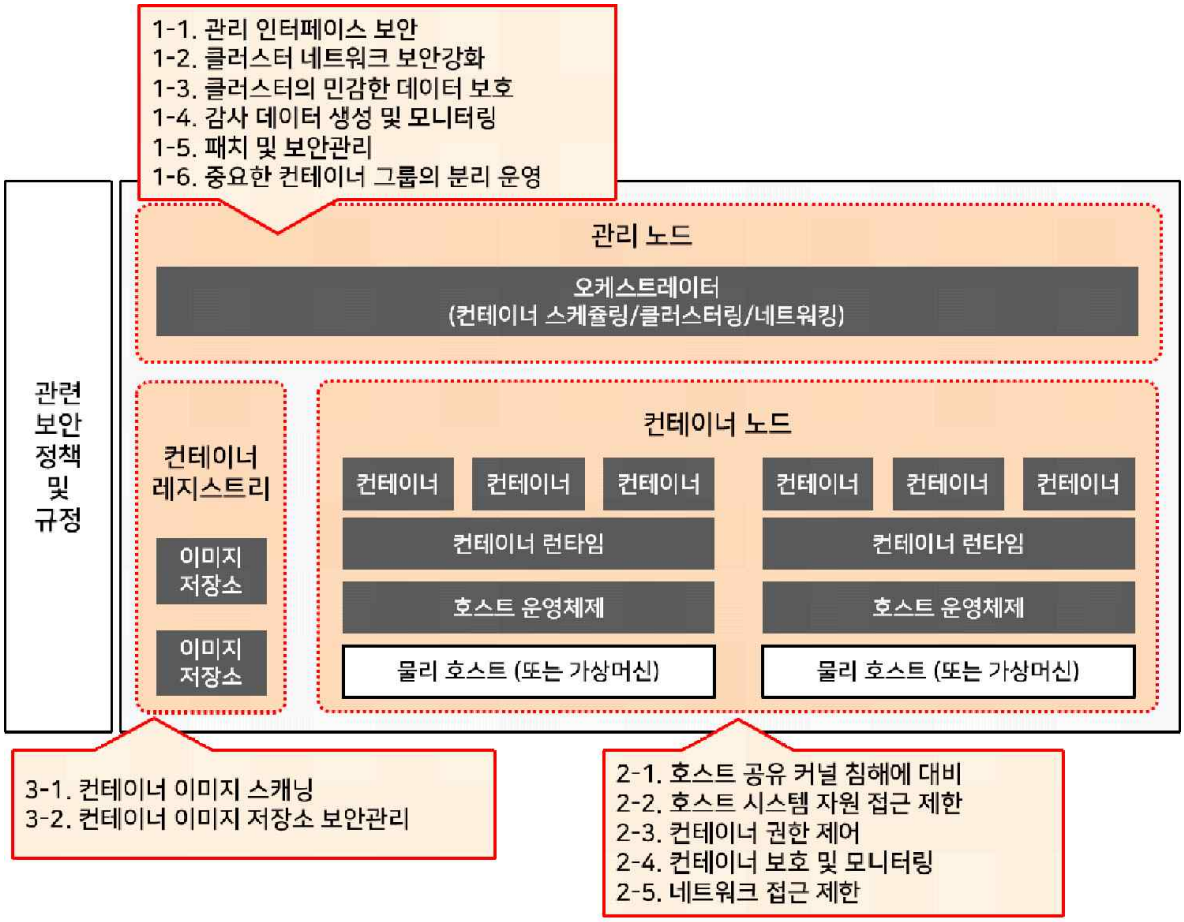
컨테이너의 런타임(runtime), 이미지(image) 및 배포(distribution)의 표준 규격을 제공하는 리눅스 재단 프로젝트인 OCI(Open Container Initiative)의 표준 규격[3]을 참고하여 컨테이너 가상화 기술 스택의 구성요소와 기능 및 역할을 다음과 같이 살펴볼 수 있다.

구성요소	기능 및 역할
[관리 노드]	오케스트레이터 등 가상화 관리 솔루션이 실행되는 호스트 시스템
오케스트레이터 (Orchestrator)	컨테이너 런타임으로 컨테이너를 지정된 컨테이너 노드에 배치하거나 문제가 발생한 컨테이너를 교체하거나 컨테이너 환경정보를 설정하는 등 스케줄링, 클러스터링 및 네트워킹을 관리하는 오케스트레이션 수행 (쿠버네티스 등)
[컨테이너 노드]	컨테이너 가상화 환경이 운영되는 호스트 시스템
컨테이너	애플리케이션과 환경정보가 포함된 독립적인 격리실행 가상 환경 · 컨테이너 이미지는 메타데이터, 어플리케이션 바이너리 및 공유 라이브러리를 패키징 하고 있는 tar 형식 파일
컨테이너 런타임	컨테이너를 쉽게 가져오거나 공유하고 구동할 수 있도록 지원하는 도구 (도커 등)
호스트 운영체제	컨테이너를 실행하는 기반 시스템 · 운영체제 네임스페이스(namespace), 컨트롤 그룹(cgroups) 기능으로 컨테이너 런타임은 컨테이너 격리(isolation)를 수행
[가상머신 레지스트리]	컨테이너 이미지가 저장되는 저장소
이미지 저장소	컨테이너 이미지를 관리하고 공유하기 위한 애플리케이션 · OCI는 이미지 저장소(레지스트리)에 대한 규격을 제시
[관련 보안정책 및 규정]	· 「국가 정보보안 기본지침」, 국가정보원 · 「국가 클라우드 컴퓨팅 보안 가이드라인」, 국가정보원 · 컨테이너 런타임은 가상환경을 구현해주는 '가상화 제품'에 해당, CC인증 대상이지만 도입 요건을 필수가 아닌 권고로 제시 (2021.4.14부터 적용, 국가정보원 홈페이지 참조)

[표 24] 컨테이너 가상화 기술 구성요소와 기능 및 역할

3) "Open Container Initiative", https://opencontainers.org/

컨테이너 가상화 기술 스택을 기반으로, 컨테이너 기반 정부 업무 인프라의 안전성과 신뢰성을 제고하기 위한 보안기준의 전체 구성은 다음 예시와 같다.



[그림 33] 컨테이너 가상화 기술 스택에 대한 보안기준

보안기준은 컨테이너 가상화 기술 스택 구성요소인 관리 노드, 컨테이너 노드 및 컨테이너 레지스트리로 분류되어 있으며, 총 13개 보안기준과 30개의 세부 점검항목을 제시한다. 각급 기관은 컨테이너 기반의 업무 서비스 도입 및 운영 시 해당 보안기준의 내용을 준수해야 하며, 불가피하게 보안기능 및 설정을 해제할 경우 한시적으로 허용하며 별도의 보안대책을 마련하고 국가정보원 담당자와 협의해야 한다.

4. 하이퍼바이저 가상화 기술 보안기준 및 점검항목

○ 관리노드

점검항목	중요도	점검결과
1-1. 관리 인터페이스에 대한 인증과 접근 제어를 강화해야 한다.		
(1) 관리자 계정 접근에 대해 다중요소(Multi-factor) 인증을 사용하고 있는가?	필수	
(2) 네트워크를 통한 관리 인터페이스 접속 시에는 암호화 프로토콜을 사용하고 있는가?	필수	
(3) 역할 기반 접근 제어(RBAC, Role Based Access Control) 정책을 적용하고 있는가?	필수	
1-2. 감사 데이터를 생성하고 모니터링 해야 한다.		
(1) 가상머신 운영 환경의 감사 데이터를 생성하고 모니터링하고 있는가?	필수	
(2) 감사 데이터 양에 대한 임계치를 설정하고 모니터링하고 있는가?	필수	
1-3. 관리 솔루션에 대한 보안 패치와 설정 점검을 주기적으로 수행해야 한다.		
(1) 관리 솔루션의 취약점에 대한 보안 패치를 수행하고 있는가?	필수	
(2) 주기적으로 취약한 설정을 점검하고 관리하고 있는가?	필수	
(3) 인가된 시간 서버와 관리 솔루션의 시간을 동기화하고 있는가?	필수	
1-4. 중요한 가상머신 그룹을 식별하고, 분리하여 운영해야 한다.		
(1) 중요도 높은 가상머신을 식별하고, 분리된 가상화 인프라 자원을 할당하고 있는가?	필수	
1-5. 가상 드라이브를 주기적으로 백업해야 한다.		
(1) 기관의 백업 정책을 준수하여 가상 드라이브를 주기적으로 백업하고 있는가?	필수	

○ 가상머신 노드

점검항목	중요도	점검결과
2-1. 하이퍼바이저 형상을 식별, 최신 보안패치와 설정 점검을 수행해야 한다.		
(1) 하이퍼바이저 기능으로 형상정보를 식별하고 기록 및 관리하고 있는가?	필수	
(2) 취약점이 발견된 경우, 취약점 제거 및 보안패치를 적용하고 있는가?	필수	
(3) 주기적으로 취약한 설정을 점검하고 관리하고 있는가?	필수	
(4) 인가된 시간 서버와 하이퍼바이저의 시간을 동기화하고 있는가?	필수	
2-2. 하이퍼바이저 관리 및 설정 기능 보안을 강화해야 한다.		
(1) 외부 네트워크를 통한 관리용 원격 접근을 금지하고 있는가?	필수	
(2) 관리 전용 물리 NIC을 할당하거나 가상 네트워크를 할당하고 있는가?	필수	
(3) 필요시에만 SSH 접속 등 쉘(shell)을 사용하고 있는가?	필수	
(4) 기관의 인가된 관리자만 보안관리 기능을 수행 가능하도록 설정하고 있는가?	필수	
(5) 네트워크로 보안관리 접속 시에는 암호화 프로토콜을 사용하고 있는가?	필수	
2-3. 하이퍼바이저 보안기능을 설정하여 운영해야 한다.		
(1) 관리 솔루션의 기능으로 정당한 사용자임을 식별 및 인증을 확인하고 있는가?	필수	
(2) 사용자 등록 시 기본(default) 비밀번호를 사용 금지 하고 있는가?	필수	
(3) 사용자 인증에 설정된 횟수만큼 연속적으로 실패하면, 식별 및 인증 기능이 비활성화되도록 설정하고 있는가?	필수	
(4) 비밀번호 등록 및 변경 시 비밀번호 보안성 기준을 준수 하고 있는가?	필수	
(5) 관리자·사용자가 관리 솔루션과 컴퓨터 시스템, 가상머신 이미지 저장소 간 데이터를 전송하는 경우에 암호통신 채널을 사용하여 전송하고 있는가?	필수	
(6) 관리 솔루션에 대한 관리 접속 시 전송 데이터를 보호하기 위해 암호통신 채널을 사용하여 전송하고 있는가?	필수	
2-4. 가상머신의 데이터를 보호해야 한다.		
(1) 가상머신간 자원이 상호 공유 및 침해되지 않도록 격리하고 있는가?	필수	
(2) 가상머신간 네트워크가 상호 연동 및 침해되지 않도록 분리하고 있는가?	필수	
(3) 가상스위치를 안전하게 설정하여 트래픽 유출 및 네트워크 기반 공격을 방지하고 있는가?	필수	

점검항목	중요도	점검결과
2-5. 가상머신에 할당된 가상화 인프라를 보호해야 한다.		
(1) 할당된 장치(device)에만 접근이 가능하도록 가상머신의 접근 제어 목록을 설정하고 있는가?	필수	
(2) 자원이 고갈되지 않도록 가상머신에 대한 자원 할당량을 적절히 제한하고 있는가?	필수	
(3) DoS(Denial of Service) 예방을 위해서 가상머신별 대역폭을 적절히 제한하고 있는가?	필수	
(4) 가상머신 보호 및 모니터링을 위한 보안대책을 적용하고 있는가?	필수	
(5) 가상머신의 설정 변경이 탐지된 경우, 감사 데이터를 생성하고 관리자에게 알림이 가도록 설정하고 있는가?	필수	
2-6. 호스트 운영체제의 침해에 대비해야 한다.		
(1) 가상머신 탈출 등 취약점을 식별하고 보안패치를 수행하고 있는가?	필수	
(2) 인가된 시간 서버와 호스트 운영체제의 시간을 동기화하고 있는가?	필수	
(3) 호스트 운영체제와 하이퍼바이저를 서로 다른 권한으로 운영하고 있는가?	선택	

○ 가상머신 레지스트리

점검항목	중요도	점검결과
3-1. 가상머신 이미지에 대한 주기적인 보안점검을 수행해야 한다.		
(1) 이미지 저장소에 취약하거나 오래된 버전의 이미지가 포함되지 않도록 관리·운영하고 있는가?	필수	
3-2. 가상머신 이미지 저장소를 안전하게 관리해야 한다.		
(1) 안전한 이미지 저장소로부터 전자서명된 신뢰할 수 있는 이미지 전송이 가능하도록 설정하고 있는가?	필수	

5. 컨테이너 가상화 기술 보안기준 및 점검항목

○ 관리 노드

점검항목	중요도	점검결과
1-1. 관리 인터페이스에 대한 인증과 접근 제어를 강화해야 한다.		
(1) 관리자 계정 접근에 대해 다중요소(Multi-factor) 인증을 사용하는가?	필수	
(2) 네트워크를 통한 관리 인터페이스 접속 시에는 암호화 프로토콜을 사용하고 있는가?	필수	
(3) RBAC(역할 기반 접근 제어, Role Based Access Control) 정책을 적용하고 있는가?	권고	
1-2. 클러스터의 네트워크 보안을 강화해야 한다.		
(1) 클러스터 관리 구성요소에 대한 불필요한 네트워크 접근을 차단하고 있는가?	필수	
(2) 클러스터 네트워크의 통신 채널을 암호화하고 있는가?	필수	
1-3. 클러스터의 민감한 데이터를 보호해야 한다.		
(1) 클러스터의 민감한 정보를 안전한 위치에 보관하고 인가되지 않은 사용자가 접근하지 못하도록 설정하고 있는가?	필수	
(2) 민감한 정보를 암호화하여 저장하고 있는가?	필수	
1-4. 감사 데이터를 생성하고 모니터링 해야 한다.		
(1) 컨테이너 운영 환경의 감사 데이터를 생성하고 모니터링하고 있는가?	필수	
(2) 감사 데이터의 임계치를 설정하고 모니터링 하고 있는가?	권고	
1-5. 주기적으로 보안 패치와 설정 점검을 수행해야 한다.		
(1) 오케스트레이터 취약점에 대한 보안 패치를 수행하고 있는가?	필수	
(2) 주기적으로 취약한 설정을 점검하고 관리하고 있는가?	필수	
1-6. 중요한 컨테이너 그룹을 식별하고, 분리하여 운영해야 한다.		
(1) 중요도가 높은 서비스를 식별하고, 분리된 컨테이너 자원을 할당하고 있는가?	필수	

○ 컨테이너 노드

점검항목	중요도	점검결과
2-1. 호스트 운영체제 커널의 침해에 대비해야 한다.		
(1) 가상머신 위에 호스트 운영체제와 컨테이너 런타임을 설치하고 컨테이너를 운영하고 있는가?	필수	
(2) 컨테이너 탈출 등에 영향을 줄 수 있는 취약점을 식별하고 보안 패치를 수행하고 있는가?	필수	
2-2. 호스트 시스템 자원에 대한 접근을 제한해야 한다.		
(1) 컴퓨팅 자원이 고갈되지 않도록 컨테이너에 대한 자원 할당량을 제한하고 있는가?	필수	
(2) I/O 장치 자원이 고갈되지 않도록 컨테이너별 대역폭을 제한하고 있는가?	필수	
(3) 호스트 운영체제에 대한 컨테이너의 접근을 제한하고 있는가?	필수	
(4) 컨테이너의 호스트 네트워크 자원 사용을 제한하고 있는가?	필수	
2-3. 컨테이너를 최소 권한으로 실행해야 한다.		
(1) 특권(Privileged) 모드 컨테이너의 실행을 금지하고 있는가?	필수	
(2) 호스트와 네임스페이스를 공유하는 것을 금지하고 있는가?	필수	
(3) 오케스트레이터의 컨테이너 권한 제어 기능을 활용하고 있는가?	필수	
2-4. 관리 인터페이스에 대한 인증과 접근 제어를 강화해야 한다.		
(1) SELinux, AppArmor와 같은 강제 접근제어 기술과 Seccomp와 같은 시스템 기능 제한 메커니즘을 활용하고 있는가?	필수	
(2) 컨테이너의 비정상적인 활동을 탐지할 수 있는 보안 솔루션을 활용하고 있는가?	필수	
(3) 컨테이너의 상태에 대한 모니터링을 수행해야 하고 있는가?	필수	
2-5. 컨테이너 및 컨테이너 런타임에 대한 네트워크 접근을 제한해야 한다.		
(1) 컨테이너 런타임의 관리 인터페이스 원격 접근을 금지하고 있는가?	필수	
(2) 컨테이너 런타임의 관리 인터페이스 접근을 위한 전용 물리 NIC을 할당하거나 불가능한 경우 전용 가상 네트워크를 할당 하고 있는가?	필수	
(3) 네트워크를 통한 컨테이너 런타임의 관리 인터페이스 접속 시에는 암호화 프로토콜을 사용하고 있는가?	필수	
(4) 컨테이너 내부 접속을 위한 SSH 서버를 제거했는가?	필수	

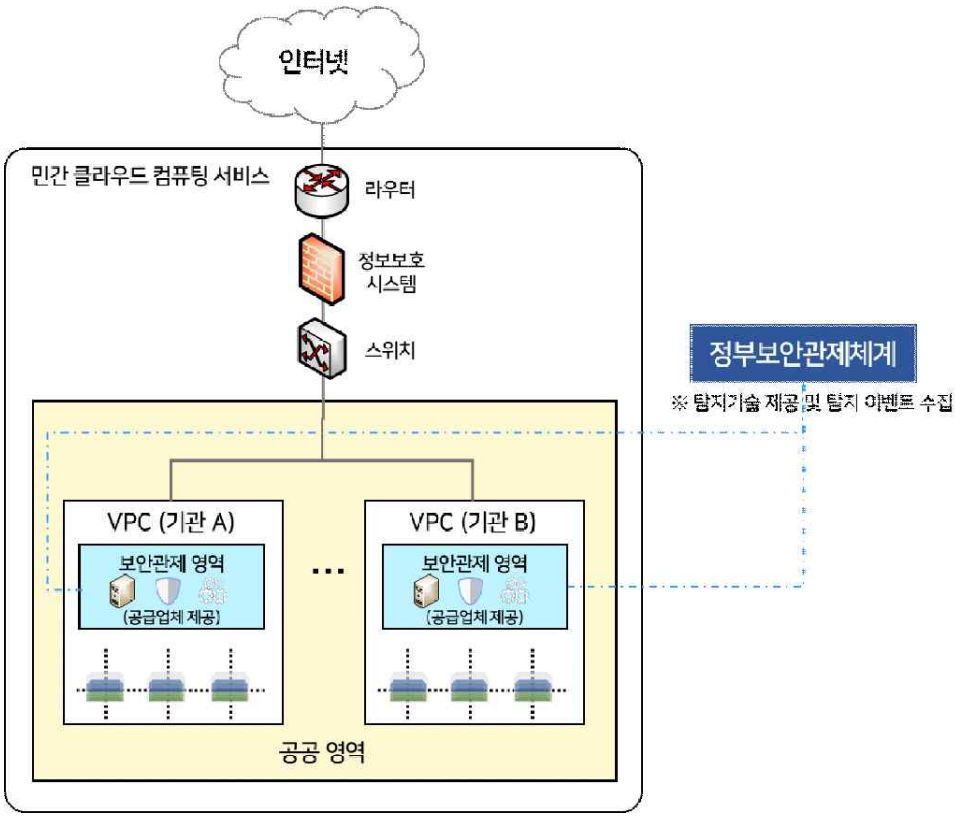
○ 컨테이너 레지스트리

점검항목	중요도	점검결과
3-1. 컨테이너 이미지에 대한 주기적인 보안점검을 수행해야 한다.		
(1) 이미지 저장소에 취약하거나 오래된 버전의 이미지가 포함되지 않도록 관리·운영하고 있는가?	필수	
3-2. 컨테이너 이미지 저장소를 안전하게 관리해야 한다.		
(1) 안전한 이미지 저장소로부터 전자 서명된 신뢰할 수 있는 이미지 전송이 가능하도록 설정하고 있는가?	필수	

[부록 7] 민간 클라우드 컴퓨팅 서비스 보안관제

[부록 7]은 국가·공공기관이 활용하는 민간 클라우드 영역에 대한 보안관제의 수행 개념과 특징을 소개한다.

이용기관은 기관이 이용하는 민간 클라우드 공공 영역에 대한 보호를 위해 「사이버안보 업무규정」 제14조에 따른 정부보안관제체계와 연계하여 보안관제를 수행해야 한다. 이를 위하여 서비스 공급업체는 기관의 보안관제 영역과 **정부보안관제체계를 연계할 수 있는 기반**을 제공해야 한다.



○ 서비스 공급업체는 기관 VPC 영역에서 보안관제를 수행할 수 있는 기반 제공 (침입탐지 및 암호화 트래픽 가시화 기능 등)

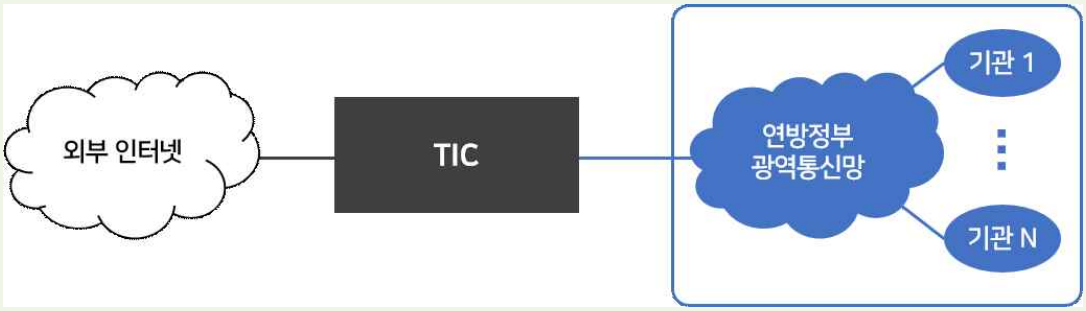
○ 서비스 공급업체는 기관의 보안관제 영역과 정부보안관제체계를 연계할 수 있는 기반 제공

○ 이용기관은 보안관제 영역에서 탐지기술을 적용하여 보안관제를 수행하며, 탐지정보를 정부보안관제체계와 연계

<관련 사례 1 - 美 연방정부의 TIC를 통한 연방 네트워크 보안>

TIC(Trusted Internet Connection)는 미국 연방정부가 예산관리국의 "Memorandum M-08-05"에 따라 연방 네트워크 보안을 위해 마련한 안전한 인터넷 접속 체계이다. 국토안보부 산하의 CISA는 TIC를 운영하여 연방정부 기관의 인터넷 접속에서 발생하는 보안 위험을 중앙집중식으로 모니터링하고 관리한다. 연방정부 기관은 외부 인터넷 접속을 위해 TIC 접속지점(TICAP)에 연결해야 하며 TIC는 보안 이벤트의 탐지, 분석 및 대응 체계를 제공한다. 이는 국가·공공기관을 대상으로 수행하는 보안관제와 유사한 면이 있다.

한편, 연방정부의 민간 클라우드 활용이 증가함에 따라, 각급기관은 FedRAMP 인증을 획득한 민간 클라우드 서비스를 이용할 때 TIC 규정을 준수한다. TIC 체계에 따라 기관이 접속하는 모든 외부 인터넷 트래픽은 TICAP에 연결되기 때문에 연방정부의 데이터를 포함하는 클라우드 트래픽은 TIC를 경유할 수 있다.



<TIC(Trusted Internet Connection) 개념>

<관련 사례 2 - 美 CISA의 CLAW(Cloud Log Aggregation Warehouse)>

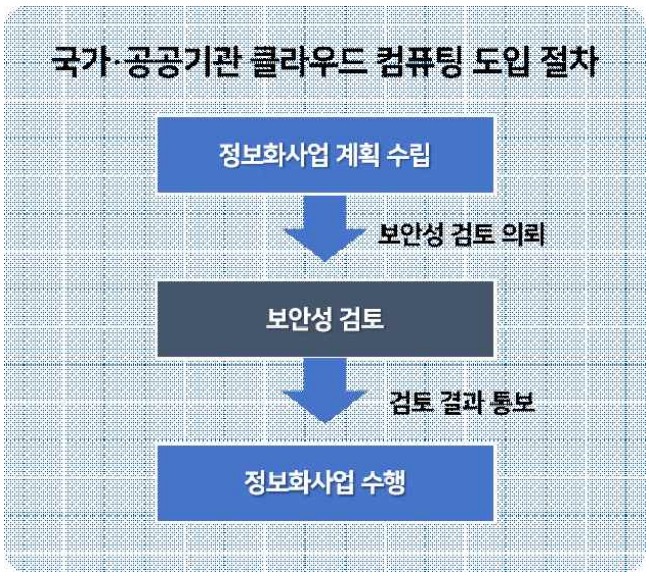
美 연방기관이 IT 인프라 자체를 클라우드로 이전하는 사례가 증가하면서, 연방정부의 일부 클라우드 트래픽이 TIC가 보호하는 경계를 벗어나게 되었다. CISA는 해당 트래픽에 대해 TIC 체계와 유사한 보안 기능을 제공하기 위한 사이버보안 프로그램인 CLAW를 시범적으로 운영하기 시작하였다[4].

CLAW는 서비스 제공자가 보안 이벤트 탐지 및 수집 기능을 제공하고, 이용기관이 해당 기능을 활용하여 보안 이벤트를 수집하고, CISA가 해당 이벤트를 기반으로 보안 모니터링을 수행함으로써 운영된다. 보안 이벤트의 종류는 서비스 제공자에 따라 다를 수 있으며, 접속 기록, 침입탐지/침입방지시스템 기록, API, DNS, VPN 및 방화벽 로그 등을 포함한다. 수집된 이벤트 로그는 별도의 클라우드 저장소에 저장되며 CISA는 해당 로그를 기반으로 보안 이벤트 탐지, 분석 및 대응을 수행한다.

4) "Modernizing Cybersecurity Programs", Department of Homeland Security, Nov.16.2020

[부록 8] 가이드라인 요약

1. 국가·공공기관 클라우드 컴퓨팅 도입 절차



○ 국가·공공기관은 정보화 사업과 예산편성 시 클라우드 컴퓨팅 도입을 우선 고려

○ 국가·공공기관은 민간 클라우드 컴퓨팅 서비스 이용 여부를 자체적으로 검토

- **국가정보원이 도입요건 확인을 완료한 민간 클라우드 컴퓨팅 서비스**를 보안규정을 준수하여 이용할 수 있음

※ [참고] 『국가 클라우드 컴퓨팅 보안 가이드라인』

- 제3장 4절 - 클라우드 컴퓨팅 서비스 도입요건

○ 정보보호에 관한 사항은 『국가 정보보안 기본지침』과 『국가 클라우드 컴퓨팅 보안 가이드라인』을 준수

: 국가·공공기관 클라우드 컴퓨팅 도입과 보안 관리는 **기존 국가·공공기관 정보시스템 보안관리 체계와의 연속성 상에서 수행**되어야 함

: 도입 기관의 업무 특성과 도입 대상 시스템의 보안성에 따라 클라우드 컴퓨팅 도입 유형 결정

※ [참고] 『국가 클라우드 컴퓨팅 보안 가이드라인』

- 제3장 1절 - 클라우드 컴퓨팅 도입 유형

- 제3장 2절 - 클라우드 영역 분류
- 제3장 3절 - 시스템 중요도 분류 기준 및 절차
- [부록 2] - SaaS 구축 유형
- [부록 3] - 인터넷망 DaaS 구축 보안대책
- [부록 5] - 클라우드 업무환경 접속단말 보안기준
- [부록 6] - 클라우드 가상화 기술 보안기준
- [부록 7] - 민간 클라우드 컴퓨팅 서비스 보안관제

: 클라우드 컴퓨팅 보안 기본원칙과 클라우드 컴퓨팅 환경 구성요소(정책, 클라우드 인프라, 가상 환경, 데이터, 인증·권한, 사고·장애 대응)별 세부 보안기준을 준수

※ [참고] 『국가 클라우드 컴퓨팅 보안 가이드라인』

- 제3장 2절 - 클라우드 영역 분류
- 제4장 1절 - 기관 자체 클라우드 컴퓨팅 구축 보안기준
- 제4장 2절 - 민간 클라우드 컴퓨팅 서비스 이용 보안기준

2. 클라우드 컴퓨팅 주요 보안 기본원칙

○ 기관 자체 클라우드 컴퓨팅 구축 보안 기본원칙

정책적 측면 보안 기본원칙	기술적 측면 보안 기본원칙
• 도입 정보보호시스템 안전성 확인 : 보안적합성 검증 절차 준수 및 제품유형별 도입 인증 요건 확인	• 내부 업무와 외부 공개용 클라우드 컴퓨팅 서비스 사용영역 분리 • 중요장비 이중화 및 백업체계 구축 • 관리자/이용자 접근통제 확보 • 클라우드 저장/송수신 중요 업무자료 암호화 : 검증필 암호모듈 탑재 대상 확인

○ 민간 클라우드 컴퓨팅 서비스 이용 보안 기본원칙

정책적 측면 보안 기본원칙	기술적 측면 보안 기본원칙
• 국가정보원이 도입요건 확인을 완료한 민간 클라우드 컴퓨팅 서비스 이용 • 민간 클라우드 컴퓨팅 서비스 이용 대상 시스템의 보안 중요도 등급 분류와 클라우드 영역 분류를 수행 (영역별 보안기준은 클라우드 영역 기본원칙을 확인) • 물리적 위치 및 공공 영역 분리 : 클라우드 시스템/데이터 국내 위치 : 국내에 위치한 관리주체가 관리·운영 : 민간 이용자 영역과 별도로 공공 영역 분리 • 보안관제, 사고조사, 예방보안활동 등 국가정보원 및 이용 기관의 사이버위협 대응 활동 유지를 위한 내용을 계약 상 반영 • 국가·공공기관 보안관리 체계에 준하여 민간 클라우드 컴퓨팅 시설/네트워크 보안관리 • 도입 정보보호시스템 안전성 확인 : 보안적합성 검증 절차 준수 및 제품유형별 도입 인증 요건 확인 • 이용대상 서비스의 범위를 벗어나는 외부 서비스 연동 시 안전성 확인 • 민간 사업자 보안기준 준수 여부 확인 • 보안취약점 배제 개발 : 「행정기관 및 공공기관 정보시스템 구축·운영 지침」 준수	• 기관의 내부 업무용 영역과 외부 클라우드 컴퓨팅 서비스를 사용·관리하기 위한 영역은 분리하여 운영 • 관리자/이용자 접근통제 확보 • 클라우드 저장/송수신 중요 업무자료 암호화 : 검증필 암호모듈 탑재 대상 확인 • 보안관제, 사고조사, 예방보안활동 등 국가정보원 및 이용 기관의 사이버위협 대응 활동 유지를 위한 제반환경 지원 여부 확인 • SaaS 애플리케이션 보안성 강화 방안 마련

이 가이드라인에는 네이버에서 제공한 나눔글꼴이 적용되어 있습니다.

이 저작물은 공공누리 출처표시-상업적이용금지-변경금지 조건에 따라 이용할 수 있습니다.

국가 클라우드 컴퓨팅 보안 가이드라인

발행일 2023년 1월

발행처 국가정보원

국가보안기술연구소