우리가 만들어가는 지속가능한 내일: 연결, 혁신, 번영

개인정보보호위원회

수신 ISMS-P 인증기업
(경유)
제목 ISMS-P 인증기업 특별 사후점검 실시 및 결과 회신 요청의 건

1. 귀 사 및 기관의 무궁한 발전을 기원합니다.

2. 최근 ISMS-P 인증을 취득한 기업의 해킹사고 등이 빈번하게 발생함에 따라 ISMS-P 인증 무용론까지 제기되며 국민 불안이 가중되는 상황에 있습니다.

3. 이에 개인정보보호위원회는 대국민 피해 확산 방지와 인증의 실효성 유지를 위해 개인정보보호법 제32조의2(개인정보 보호 인증)에 따라 ISMS-P 인증기업(기관)을 대상으로 특별 사후점검을 실시하고자 하오니 적극 협조하여 주시기 바랍니다.

가. 점검대상 : ISMS-P 인증 기업(기관) 전체
나. 점검기간 : ~'25.12.31.(수)
다. 점검내용 : 개인정보 처리 IT자산에 대해 "*1)**비밀번호 관리**, 2)**암호화 적용**, 3)**로그 및 접속기록**, 4)**패치 관리**, 5)**사고 대응 및 복구**" 실태 전수 조사
라. 점검방법 : 기업(기관) **자체 점검** 실시 후 **CEO 결과보고**
마. 이행점검 : 26년도 사후심사 시 이행여부 확인
* 단, 유출사고가 발생한 사실이 있는 인증기업의 경우 '26.1월 현장점검을 통해 이행여부 확인 예정
바. 결과제출 : **'26.1.11.(일)**까지 **붙임 파일**(양식1~7) 이메일(**help@isms-p.or.kr**) 제출
사. 문 의 처 : 한국인터넷진흥원 ISMS-P 인증 헬프데스크(T.1544-3770(ARS 1번))

붙임 점검결과 양식 1부. 끝.

가이드 범위 및 참고 시 주의사항 1/2

통합인증	분야(인증 기준 항목수)
1. 관리체계 수립 및 운영	1.1 관리체계 기반 마련(6) **1.2 위험관리(4)** 1.3 관리체계 운영(3) 1.4 관리체계 점검 및 개선(3)
2. 보호 대책 요구 사항	2.1 정책,조직,자산관리(3) 2.2 인적보안(6) 2.3 외부자 보안(4) 2.4 물리보안(7) **2.5 인증 및 권한 관리(6)** **2.6 접근 통제(7)** **2.7 암호화 적용(2)** **2.8 정보시스템 도입 및 개발 보안(6)** **2.9 시스템 및 서비스 보안관리(9)** **2.10 시스템 및 서비스 보안 관리(9)** **2.11 사고 예방 및 대응(5)** **2.12 재해복구(2)**

[ISMS-P 인증기준 중 가이드 범위]

ISMS-P 가이드-이론

서태호 강사

topasvga@naver.com

강사 소개

서태호 강사

topasvga@naver.com

NAVER

HANGAME

SK

TRAINER

NAVER Cloud

NAVER Cloud
Certified Expert AI

NAVER Cloud
Certified Professional AI

NAVER CLOUD PLATFORM
Certified Professional Security

NAVER Cloud
Certified Professional

aws certified Solutions Architect Professional

aws certified SysOps Administrator Associate

aws certified Solutions Architect Associate

Google Cloud Certified PROFESSIONAL CLOUD ARCHITECT

Microsoft CERTIFIED AZURE ADMINISTRATOR ASSOCIATE

목적

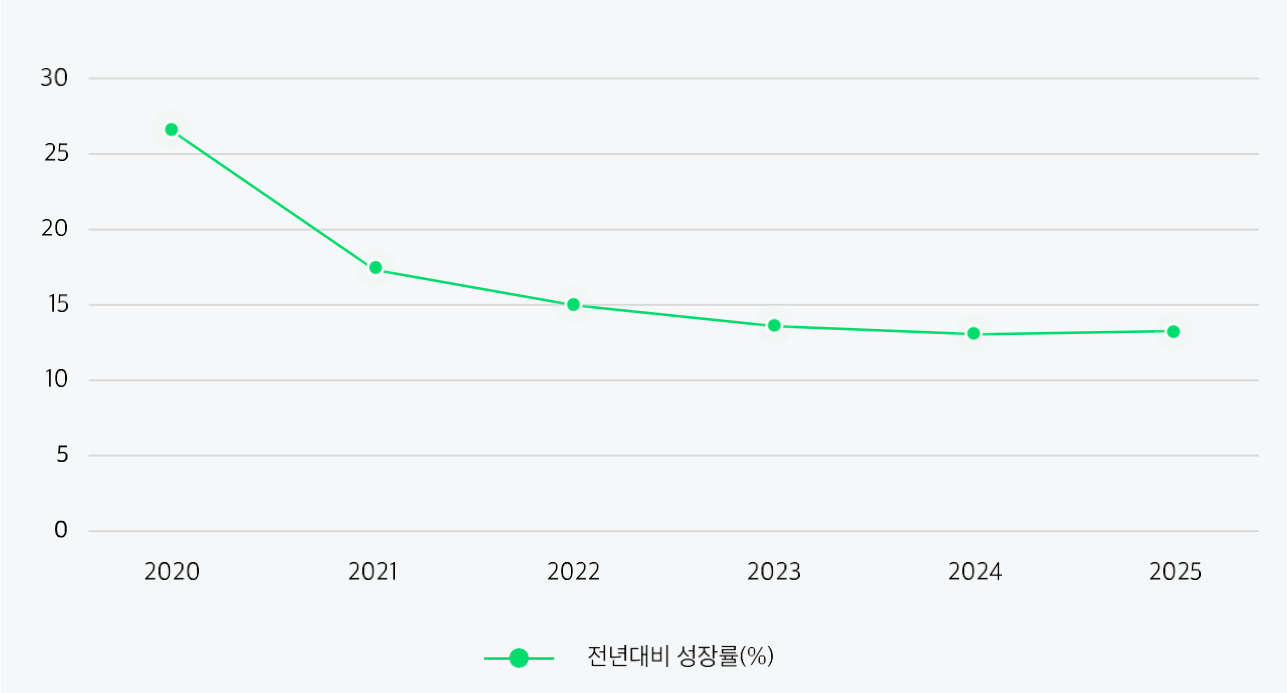
ISMS-P 인증 기준에 맞게 점검하기

목차

1. 소개

국내/외 DX Trend는 지속적으로 증가될 것으로 전망 됩니다.

- 글로벌 클라우드 시장이 전년 대비 16% 성장한 4,740억 달러 규모로 성장할 것으로 전망하며, 새로운 디지털 워크로드의 95% 이상이 클라우드 네이티브 플랫폼에 배포 될 것으로 전망했습니다.



[Public Cloud 서비스 시장 연평균 성장률 전망 (source: Korea Cloud Opportunity Forecast by industry 2021-2025,IDC)]

네이버 클라우드 플랫폼을 통해 DX준비

- 과학 기술정보 통신부에서 발표한 디지털 뉴딜 실행계획에 따라 공공기관의 2,149개 정보시스템 중 97% 이상을 퍼블릭 클라우드 상에 구성될 계획이므로 클라우드에서 운영되는 공공기관 개인정보처리시스템의 비중은 앞으로도 지속해서 증가될 것으로 보입니다.

* DX = 디지털 전환(Digital Transformation)

2. 정보보호 및 개인정보보호 관리체계 인증(ISMS-P)제도의 개요

ISMS-P 개요

- 정보보호 및 개인정보보호 관리체계 인증제도는 ‘정보통신망 이용 촉진 및 정보보호’ 등에 관한 법률 제47조와 제47조의2,같은 법 시행령 제47조부터 제54조까지의 규정 및 같은 법 시행규칙 제3조에 따른 정보보호 관리체계 인증과 ‘개인정보 보호법’, 제32조의 3, 같은 법 시행령 제34조의 2부터 제 34조의 8가지의 규정에 따른 개인정보보호 관리체계 인증을 법적근거로 하고 있으며,기업 기관의 정보보호 및 개인정보보호를 위한 일련의 조치와 활동이 인증기준에 적합함을 한국인증진흥원 또는 인증기관이 증명하는 제도를 말합니다.

- ISMS-P인증은 ‘정보통신망 이용촉진 및 정보보호 등에 관한 법률’에 따라 인증을 의무적으로 취득해야 하는 ‘의무대상자’와 자별적으로 취득할 수 있는 ‘자율 신청자’로 구분 됩니다.

ISMS-P 개요

- 자율 신청자
- 의무대상자 기준에 해당하지는 않지만 자발적으로 정보보호 및 개인정보 보호 관리체계를 구축하고 운영하는 기업과 기관은 임의신청자로 분류되며,임의 신청자가 인증 취득을 희망할 경우 자율적으로 신청하여 인증심사를 받을 수 있습니다.

ISMS-P 개요

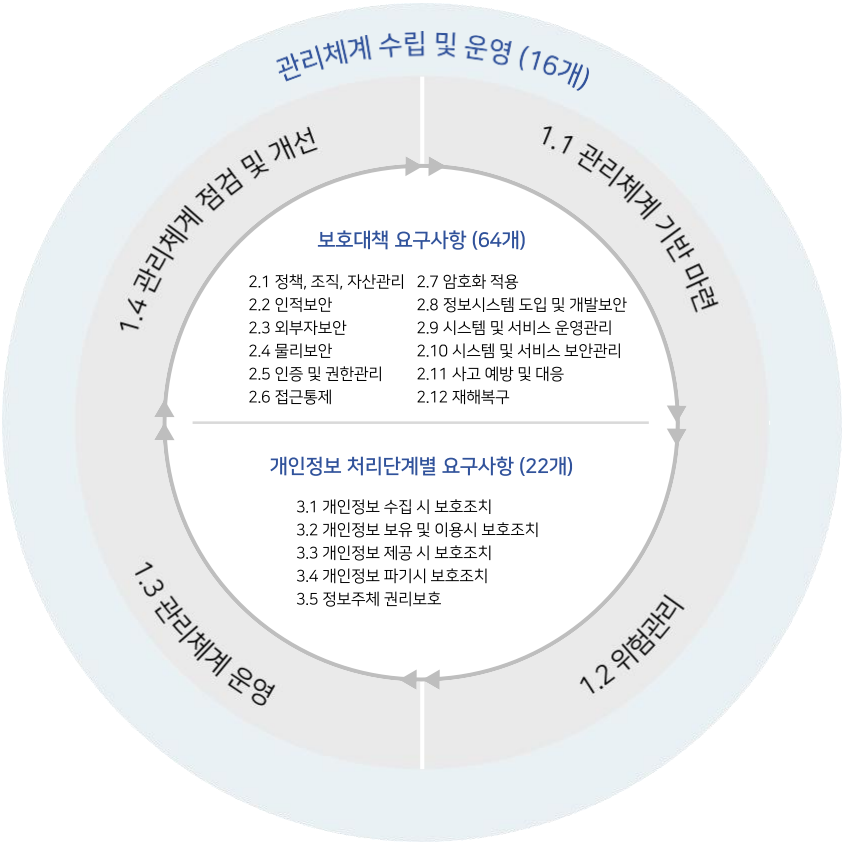
- 의무대상자
- 인증 의무 대상자는 '전기통신 사업법' 제 2조 제8호에 따른 전기통신 사업자의 전기통신 역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자로서 아래의 표에서 기술한 의무 대상자 기준에 하나에 해당되는 기업과 기관을 말합니다.

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

[정보보호 및 개인정보보호 관리체계 인증 의무 대상자 기준(Source:한국인터넷 진흥원)]

ISMS-P 인증기준

- ‘1. 관리체계 수립 및 운영(16개)’, ‘2. 보호대책 요구사항(64개)’, ‘3.개인 정보 처리단계별 요구사항(22개)’으로 구성되어 있으며, ISMS-P인증은 102개 인증 기준으로 구성되어 있다.



[ISMS-P 인증기준 (Source : 한국 인터넷진흥원(]

3. 네이버 클라우드 플랫폼의 보안

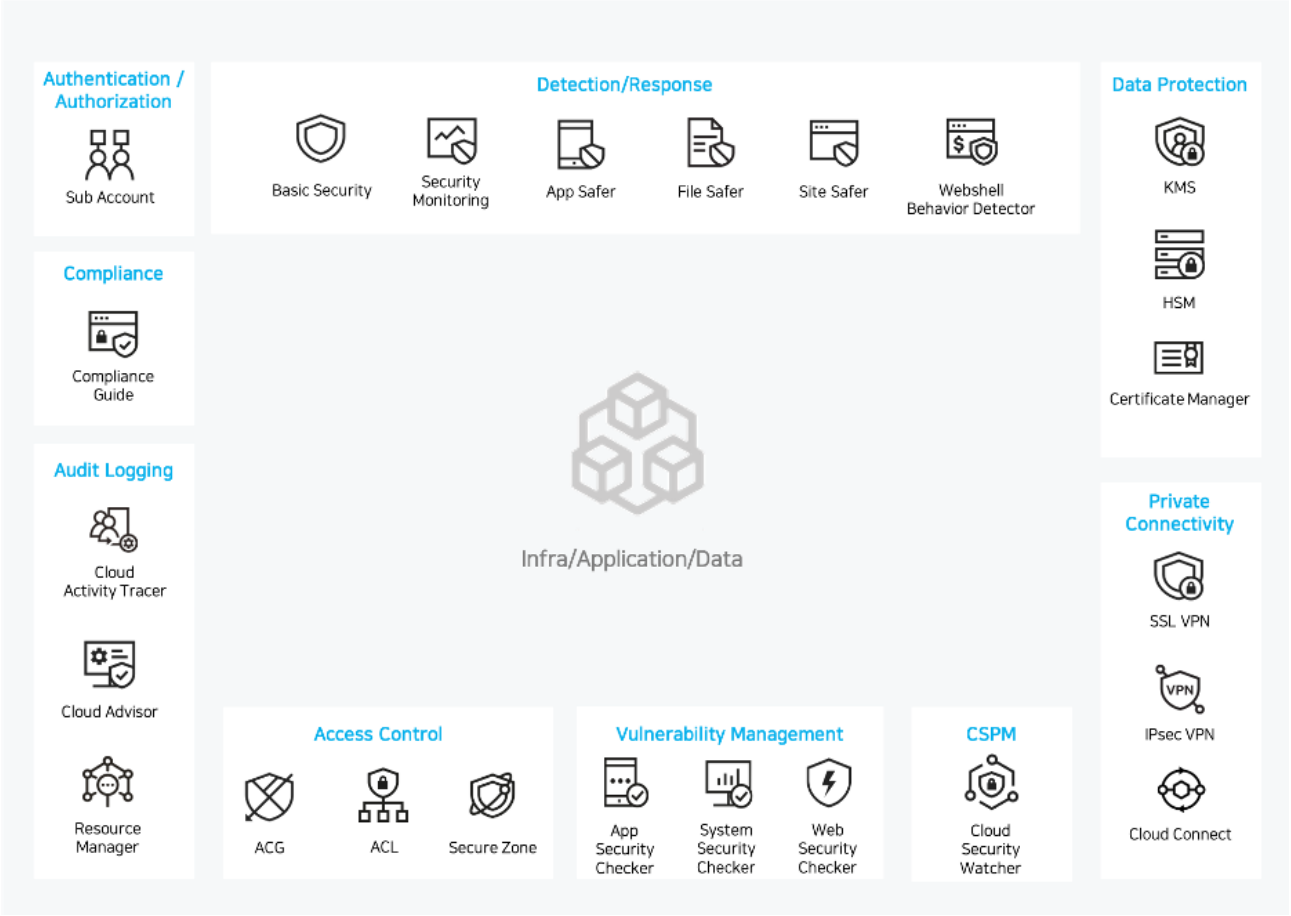
클라우드 공동 책임

- 클라우드에 구성한 고객의 클라우드 리소스를 안정적으로 보호할 수 있도록 클라우드 서비스 제공자와 고객이 각각의 역할을 나누어 함께 책임을 다하는 것을 말합니다.

구분	IAAS	PAAS	SAAS
Data	고객 책임	고객 책임	고객 책임
인터페이스 (APIs,GUIs)	고객 책임	고객 책임	고객 책임 CSP 책임
Application	고객 책임	고객 책임	CSP 책임
프로그래밍언어	고객 책임	고객 책임	CSP 책임
OS	고객 책임	CSP 책임	CSP 책임
가상머신	고객 책임	CSP 책임	CSP 책임
하이퍼바이저	CSP 책임	CSP 책임	CSP 책임
스토리지	CSP 책임	CSP 책임	CSP 책임
네트워크	CSP 책임	CSP 책임	CSP 책임
물리적 환경 데이터 센터	CSP 책임	CSP 책임	CSP 책임

네이버 클라우드 플랫폼의 보안 서비스

- 고객이 ISMS-P 인증기준 준수를 위해 필요로 하는 다양한 보안 서비스를 제공하고 있으며, 총 9개의 영역에 대한 보안 서비스를 제공하고 있습니다.



[네이버 클라우드 플랫폼 보안 서비스 MAP]

보안 서비스 별 설명 요약

구분	서비스
인증/인가	Sub Account
감지/응답	Basic Security , Security Monitoring , App Safer , File Safer Site Safer , Webshell Behavior Detector
Data 보호	KMS, HSM , Certificate Manager
사설 연결	SSL VPN , IPsec VPN , Cloud Connect
CSPM	Cloud Security Watcher
감염 관리	App Security Checker , System Security Checker , Web Security Watcher
접근제어	ACG , NACL , Secure zone
감사 로그	Cloud Activity Tracer , Cloud Advisor , Resource Manager
컴플라이언스	Compliance Guide

[네이버 클라우드 플랫폼 보안 상품의 내용 및 제공 대상

보안 서비스 별 설명 1/4

구분	서비스	주요 기능
인증/인가	Sub Account	역할 기반 접근 제어 기능을 통한 권한 관리
감지/응답	Basic Security	안전한 인터넷 비즈니스 지원을 위한 무료 보안 서비스
감지/응답	Security Monitoring	전문 인력을 통해 다양한 보안 위협으로부터 24시간 365일 안전하게 보호
감지/응답	App Safer	모바일 애플리케이션의 보안 위협을 빠르고 정확하게 탐지
감지/응답	File Safer	파일과 아웃링크의 악성 여부를 쉽게 간편하게 탐지
감지/응답	Site Safer	웹 사이트의 악성코드 배포 여부에 대해 신속한 탐지 및 알람
감지/응답	Webshell Behavior Detector	웹 서버스를 공격하는 다양한 웹쉘을 행위 기반 실시간 탐지

보안 서비스 별 설명 2/4

구분	서비스	주요 기능
Data 보호	KMS	중요 정보 암호화 키에 대한 엄격한 관리 및 안전한 보호
Data 보호	HSM	Hardware Security Module을 이용하여 암호화 키를 안전하게 보호
Data 보호	Certificate Manager	SSL 인증서의 손쉬운 등록 및 관리 서비스를 제공
Data 보호	Private CA	사설 CA를 운영하고 사설 인증서를 발급 및 관리(사설 CA(인증기관)는 조직내부에서만 사용)
사설 연결	SSL VPN	PC에 클라이언트 설치를 통해 VPC로 안전하게 접근 가능한 SSL 가상 사설망 제공
사설 연결	IPsec VPN	IPsec 장비간 네트워크와의 연결을 암호화하여 사설 통신이 가능하도록 연결
사설 연결	Cloud Connect	데이터 센터와 네이버 클라우드 플랫폼을 전용 사설 네트워크로 연결

보안 서비스 별 설명 3/4

구분	서비스	주요 기능
CSPM	Cloud Security Watcher	보안 준수 현황 점검,리소스 현황 식별,자산 변경 감시 등 클라우드 보안 형상 관리 서비스
감염 관리	App Security Checker	모바일 앱 서비스 보안의 위협 요소를 세밀하게 진단
감염 관리	System Security Checker	서버의 운영체제와 WAS의 보안 설정을 점검
감염 관리	Web Security Watcher	웹 서비스에 대한 주요 취약점 자동 진단
접근제어	ACG	IP주소/포트 기반 필터링 기능으로 리소스의 네트워크 접근 관리, 예) 웹(80) 포트 허용
접근제어	NACL	IP주소/포트 기반의 필터링 기능으로 서브넷에 적용하여 네트워크 접근 제어 관리
접근제어	Secure zone	개인정보 등 중요 정보 자원을 보다 안전하게 관리하는 네트워크

보안 서비스 별 설명 4/4

구분	서비스	주요 기능
감사 로그	Cloud Activity Tracer	콘솔과 API를 통해 수행되는 계정 활동을 모두 기록 , AWS CloudTrail과 동일
감사 로그	Cloud Advisor	모범사례에 따른 서비스 이용 권장 지침 점검 리포트를 제공, AWS 트러스트 어드바이저와 동일
감사 로그	Resource Manager	모든 리소스들을 통합적으로 관리할 수 있는 서비스
컴플라이언스	Compliance Guide	보안 인증 및 규제 대응에 필요한 사항들을 알기 쉽게 정리한 가이드 제공

4. 인증기준 별 보안 서비스 구성 방안

가이드 범위 및 참고 시 주의사항 1/2

통합인증	분야(인증 기준 항목수)
1. 관리체계 수립 및 운영	1.1 관리체계 기반 마련(6) **1.2 위험관리(4)** 1.3 관리체계 운영(3) 1.4 관리체계 점검 및 개선(3)
2. 보호 대책 요구 사항	2.1 정책,조직,자산관리(3) 2.2 인적보안(6) 2.3 외부자 보안(4) 2.4 물리보안(7) **2.5 인증 및 권한 관리(6)** **2.6 접근 통제(7)** **2.7 암호화 적용(2)** **2.8 정보시스템 도입 및 개발 보안(6)** **2.9 시스템 및 서비스 보안관리(9)** **2.10 시스템 및 서비스 보안 관리(9)** **2.11 사고 예방 및 대응(5)** **2.12 재해복구(2)**

[ISMS-P 인증기준 중 가이드 범위]

가이드 범위 및 참고 시 주의사항 2/2

통합인증	분야(인증 기준 항목수)
3. 개인정보 처리단계별 요구사항	3.1 개인정보 수집시 보호 조치(7) 3.2 개인정보 보유 및 이용 시 보호조치(5) 3.3 개인정보 제공시 보호조치(4) 3.4 개인정보 파기 시 보호조치(3) 3.5 정보주체 권리보호(3)

[ISMS-P 인증기준 중 가이드 범위]

ISMS-P 인증기준 1.2.1 (정보자산 식별)

- 조직의 업무특성에 따라 정보자산 분류기준을 수립하여 관리체계 범위 내 모든 정보자산을 식별 분류하고, 중요도를 산정한 후 그 목록을 최신으로 관리하여야 한다.

- 보호대책 관련 서비스
  - Resource Manager

ISMS-P 인증기준 1.2.1 (정보자산 식별)

정보자산 유형	서비스 유형	서비스 명	클라우드 리소스 식별 값
서버	Cpmpute	Server(SSD,GPI,Bare Metal 등)	서버 이름
	Container	Container Registory	이미지 이름
		Kubernetes Service	Cluster이름, Worker node이름, Pod이름
	Storage	Object Storage(Archive Storage등)	버킷 이름
		NAS	NAS 볼륨 이름
데이터	Database	Cloud DB (Postgre SQL, MySQL,Mongo DB 등)	DB Server 이름
보안 시스템	Security	전체 상품	네이버 클라우드 플랫폼 서비스 명
네트워크	Networking	VPC	VPC이름,Subnet이름,Route Table이름
		Load Balancer	로드 밸런서 이름
	Content Delivery	전체 서비스	네이버 클라우드 플랫폼 서비스 명
	Developer Tools	전체 서비스	네이버 클라우드 플랫폼 서비스 명
정보 시스템	Mgmt & Governacne	전체 서비스	네이버 클라우드 플랫폼 서비스 명
	Console	네이버 클라우드 플랫폼 콘솔	네이버 클라우드 플랫폼 콘솔

ISMS-P 인증기준 2.5.1 (사용자 계정 관리)

- 정보시스템과 개인정보 및 중요정보에 대한 비인가 접근을 통제하고 업무 목적에 따른 접근권한을 최소한으로 부여할 수 있도록 사용자 등록 해지 및 접근권한 부여,변경,말소 절치를 수립,이행하고, 사용자 등록 및 권한부여시 사용자에게 보안책임이 있음을 규정화하고 인식시켜야 한다.

- 보호대책 관련 서비스
  - Sub Account
  - Cloud DB
  - System Security Checker

ISMS-P 인증기준 2.5.2 (사용자 식별)

- 사용자 계정은 사용자별로 유일하게 구분할 수 있도록 식별자를 할당하고 추측 가능한 식별자 사용을 제한하여야 하며, 동일한 식별자를 공유하여 사용하는 경우 그 사유와 타당성을 검토하여 책임자의 승인 및 책임추적성 확보 등 보완대책을 수립 이행 하여야 한다.

- 보호대책 관련 서비스
  - Sub Account
  - System Security Checker

ISMS-P 인증기준 2.5.3 (사용자 인증)

- 정보시스템과 개인정보 및 중요정보에 사용자의 접근은 안전한 인증절차와 필요에 따라 강화된 인증방식을 적용하여야 한다. 또한 로그인 횟수 제한,불법 로그인 시도 경고 등 비인가자 접근 통제방안을 수립 이행하여야 한다.

- 보호대책 관련 서비스
  - Sub Account
  - Cloud Activity Tracer
  - SSL VPN

ISMS-P 인증기준 2.5.4 (비밀번호 관리)

- 법적 요구사항,외부 위협요소 등을 고려하여 정보시스템 사용자 및 고객,회원등 정보주체(이용자)가 사용하는 비밀번호 관리절차를 수립,이행하여야 한다.

- 보호대책 관련 서비스
  - Sub Account
  - Cloud DB
  - System Security Checker

ISMS-P 인증기준 2.5.5 (특수 계정 및 권한 관리)

- 정보시스템 관리,개인정보 및 중요정보 관리 등 특수 목적을 위하여 사용하는 계정 및 권한은 최소한으로 부여하고 별도로 식별하여 통제하여야 한다.

- 보호대책 관련 서비스
  - Sub Account
  - Cloud DB
  - System Security Checker
  - Cloud Activity Tracer

ISMS-P 인증기준 2.5.6 (접근권한 검토)

- 정보시스템과 개인정보 및 중요정보에 접근하는 사용자 계정의 등록,이용, 삭제 및 접근 권한 부여,변경,삭제 이력을 남기고 주도적으로 검토하여 적정성 여부를 점검하여야 한다.

- 보호대책 관련 서비스
  - Cloud Activity Tracer
  - Object Storage
  - Cloud DB
  - System Security Checker

ISMS-P 인증기준 2.6.1 (네트워크 접근)

- 네트워크에 대한 비인가 접근을 통제하기 위하여 IP관리,단말 인증 등 관리 절차를 수립,이행하고, 업무목적 및 중요도에 따라 네트워크 분리(DMZ,서버팜,DB존,개발존 등)와 접근 통제를 적용하여야 한다.

- 보호대책 관련 서비스
  - VPC
  - Network ACL/ ACG
  - NAT Gateway
  - IPsec VPN
  - Cloud Connect
  - Object Storage

ISMS-P 인증기준 2.6.2 (정보시스템 접근)

- 서버,네트워크 시스템 등 정보시스템에 접근을 허용하는 사용자,접근제한 방식,안전한 접근수단 등을 정의하여 통제하여야 한다.

- 보호대책 관련 서비스
  - Network ACL/ ACG
  - Sub Account
  - Server
  - Kubernetes Service
  - Cloud DB
  - System Security Checker

ISMS-P 인증기준 2.6.4 (데이터베이스 접근)

- 테이블 목록 등 데이터베이스 내에서 저장 관리되고 있는 정보를 식별하고, 정보의 중요도와 응용프로그램 및 사용자 유형 등에 따라 접근통제 정책을 수립,이행하여야 한다.

- 보호대책 관련 서비스
  - Cloud DB
  - VPC
  - Network ACL/ ACG

ISMS-P 인증기준 2.6.6 (원격접근 통제)

- 보호구역 이외 장소에서의 정보시스템 관리 및 개인정보 처리는 원칙적으로 금지하고, 재택근무, 장애 대응,원격협업 등 불가피한 사유로 원격접근을 허용하는 경우 책임자 승인,접근 단말 지정,접근 허용범위 및 기간설정, 강화된 인증,구간 암호화,접속단말 보안(백신,패치 등)등 수립,이행하여야 한다.

- 보호대책 관련 서비스
  - Sub Account
  - Network ACL/ ACG
  - SSL VPN
  - IPsec VPN
  - Cloud Connect

ISMS-P 인증기준 2.6.7 (인터넷 접속 통제)

- 인터넷을 통한 정보유출,악성코드 감염,내부망 침투 등을 예방하기 위하여 주요 정보시스템,주요 직무 수행 및 개인정보 취급 단말기 등에 대한 인터넷 접속 또는 서비스(P2P,웹하드,메신저 등)를 제한하는 등 인터넷 접속 통제 정책을 수립,이행하여야 한다.

- 보호대책 관련 서비스
  - Network ACL/ ACG

ISMS-P 인증기준 2.7.1 (암호정책 적용)

- 개인정보 및 주요정보 보호를 위하여 법적 요구사항을 반영한 암호화 대상, 암호 강도,암호 사용 정책을 수립하고 개인정보 및 주요정보의 저장,전송, 전달시 암호화하여야 한다.

- 보호대책 관련 서비스
  - Server
  - Cloud DB
  - Object Storage
  - KMS
  - Certificate Manager

ISMS-P 인증기준 2.7.2 (암호키 관리)

- 암호키의 안전한 생성,이용,보관,파기를 위한 관리 절차를 수립,이행하고,필요 시 복구방안을 마련하여야 한다.

- 보호대책 관련 서비스
  - KMS
  - Sub Account

ISMS-P 인증기준 2.8.5 (소스 프로그램 관리)

- 소스 프로그램은 인가된 사용자만이 접근할 수 있도록 관리하고,운영환경에 보관하지 않는 것을 원칙으로 하여야 한다.

- 보호대책 관련 서비스
  - Sub Account
  - SourceCommit
  - File Safer

ISMS-P 인증기준 2.8.6 (운영환경 이관)

- 신규 도입,개발 또는 변경된 시스템을 운영환경으로 이관할 때는 통제된 절차를 따라야 하고,실행코드는 시험 및 사용자 인수 절차에 따라 실행 되어야 한다.

- 보호대책 관련 서비스
  - SourceDeploy
  - SourceCommit
  - SourceBuild
  - Object Storage
  - SourcePipeline
  - Sub Account

ISMS-P 인증기준 2.9.2 (성능 및 장애관리)

- 정보시스템의 가용성 보장을 위하여 성능 및 용량 요구사항을 정의하고 현황을 지속적으로 모니터링하여야 하며,장애 발생시 효과적으로 대응하기 위한 탐지,기록,분석,복구,보고등의 절차를 수립,관리하여야 한다.

- 보호대책 관련 서비스
  - Cloud insight
  - Web service Monitoring System
  - Network Traffice Monitoring

ISMS-P 인증기준 2.9.3 (백업 및 복구 관리)

- 정보시스템의 가용성과 데이터 무결성을 유지하기 위하여 백업 대상,주기, 방법,보관장소,보관기간,소산 등의 절차를 수립,이행하여야 한다. 아울러 사고 발생시 적시에 복구할 수 있도록 관리하여야 한다.

- 보호대책 관련 서비스
  - Backup
  - Server
  - Cloud DB
  - Object Storage

ISMS-P 인증기준 2.9.4 (로그 및 접속기록 관리)

- 정보시스템의 가용성과 데이터 무결성을 유지하기 위하여 백업 대상,주기, 방법,보관장소,보관기간,소산 등의 절차를 수립,이행하여야 한다. 아울러 사고 발생시 적시에 복구할 수 있도록 관리하여야 한다.

- 보호대책 관련 서비스
  - Cloud Activity Tracer
  - Cloud Log Analytics
  - Object Storage
  - Server
  - Kubernetes Service
  - Cloud DB
  - Sub Account

ISMS-P 인증기준 2.9.5 (로그 및 접속기록 점검)

- 정보시스템의 정상적인 사용을 보장하고 사용자 오남용(비인가접속,과다조회 등)을 방지하기 위하여 접근 및 사용에 대한 로그 검토기준을 수립하여 주기적으로 점검하며, 문제 발생시 사후 조치를 적시에 수행하여야 한다.

- 보호대책 관련 서비스
  - Cloud Log Analytics
  - Resource Manager Observer
  - Cloud Activity Tracer
  - Object Storage
  - Search Engine Service

ISMS-P 인증기준 2.10.1 (보안시스템 운영)

- 보안시스템 유형별로 관리자 지정,최신 정책 업데이트,룰셋변경,이벤트 모니터링 등의 운영 절차를 수립,이행하고 보안시스템별 정책적용 현황을 관리하여야 한다.

- 보호대책 관련 서비스
  - Sub Account
  - Network ACL/ ACG
  - Security Monitoring
  - Object Storage
  - KMS
  - SSL VPN
  - Certificate Manager
  - Marketplace

ISMS-P 인증기준 2.10.2 (클라우드 보안)

- 클라우드 서비스 이용 시 서비스 유형(SaaS,PaaS,IaaS 등)에 따른 비인가 접근,설정오류 등에 따라 중요정보와 개인정보가 유,노출되지 않도록 관리자 접근 및 보안 설정에 대한 보호대책을 수립,이행하여야 한다.

- 보호대책 관련 서비스
  - SLA
  - Sub Account
  - Cloud Activity Tracer
  - Resource Manager
  - Cloud Security Watcher

ISMS-P 인증기준 2.10.3 (공개서버 보안)

- 외부 네트워크에 공개되어 있는 서버의 경우 내부 네트워크와 분리하고 취약점 점검,접근통제,인증,정보 수집,저장,공개 절차 등 강화된 보호대책을 수립,이행하여야 한다.

- 보호대책 관련 서비스
  - Certificate Manager
  - Security Monitoring
  - Web Security Checker
  - System Security Checker
  - Network ACL/ ACG
  - VPC
  - Server

ISMS-P 인증기준 2.10.4 (전자거래 및 핀테크 보안)

- 전자거래 및 핀테크 서비스 제공시 정보유출이나 데이터 조작,사기 등의 침해사고 예방을 위해 인증,암호화 등의 보호대책을 수립하고,결제 시스템 등 외부 시스템과 연계할 경우 안정성을 점검하여야 한다.

- 보호대책 관련 서비스
  - NAT Gateway
  - Network ACL/ ACG

ISMS-P 인증기준 2.10.9 (악성코드 통제)

- 바이러스,웜,트로이목마,랜섬웨어등의 악성코드로부터 개인정보 및 중요정도,정보시스템 및 업무용 단말기 등을 보호하기 위하여 악성코드 예장,탐지,대응 등의 보호대책을 수립,이행하여야 한다.

- 보호대책 관련 서비스
  - Security Monitoring

ISMS-P 인증기준 2.11.1 (사고 예방 및 대응 체계 구축)

- 침해사고 및 개인정보 유출 등을 예방하고 사고 발생시 신속하고 효과적으로 대응할 수 있도록 내,외부 침해시도의 탐지,대응,분석 및 공유를 위한 체계와 절차를 수립하고,관련 외부기관의 및 전문가들과 협조체계를 구축하여야 한다.

- 보호대책 관련 서비스
  - SLA
  - Security Monitoring
  - Cloud Advisor

ISMS-P 인증기준 2.11.2 (취약점 점검 및 조치)

- 정보시스템의 취약점이 노출되어 있는지를 확인하기 위하여 정기적으로 취약점 점검을 수행하고 발견된 취약점에 대해서는 신속하게 조치하여야 한다. 또한 최신 보안 취약점의 발생 여부를 지속적으로 파악하고 정보시스템에 미치는 영향을 분석하여 조치하여야 한다.

- 보호대책 관련 서비스
  - Web Security Checker
  - System Security Checker
  - App Security Chercker
  - Container Registory
  - Cloud Advisor

ISMS-P 인증기준 2.11.3 (이상행위 분석 및 모니터링)

- 내/외부에 의한 침해시도,개인정보유출 시도,부정행위 등에 신속하게 탐지, 대응할 수 있도록 네트워크 및 데이터 흐름 등을 수집하여 분석하며,모니터링 및 점검 결과에 따른 사후조치는 적시에 이루어져야 한다.

- 보호대책 관련 서비스
  - Cloud Insight
  - Cloud Log Analytics
  - Cloud Activity Tracer
  - Search Engine Serice
  - Security Monitoring
  - Network Traffice Monitoring
  - Webshell Behaviror Detector

ISMS-P 인증기준 2.12.1 (재해,재난 대비 안전조치)

- 자연재해,통신,전력 장애,해킹 등 조직의 핵심 서비스 및 시스템의 운영 연속성을 위협할 수 있는 재해 유형을 식별하고 유형별 예상 피해규모 및 영향을 분석하여야 한다. 또한 복구 목표시간,복구 목표시점을 정의하고 복구 전략 및 대책,비상시 복구 조직,비상연락체계,복구 절차 등 재해 복구체계를 구축하여야 한다.

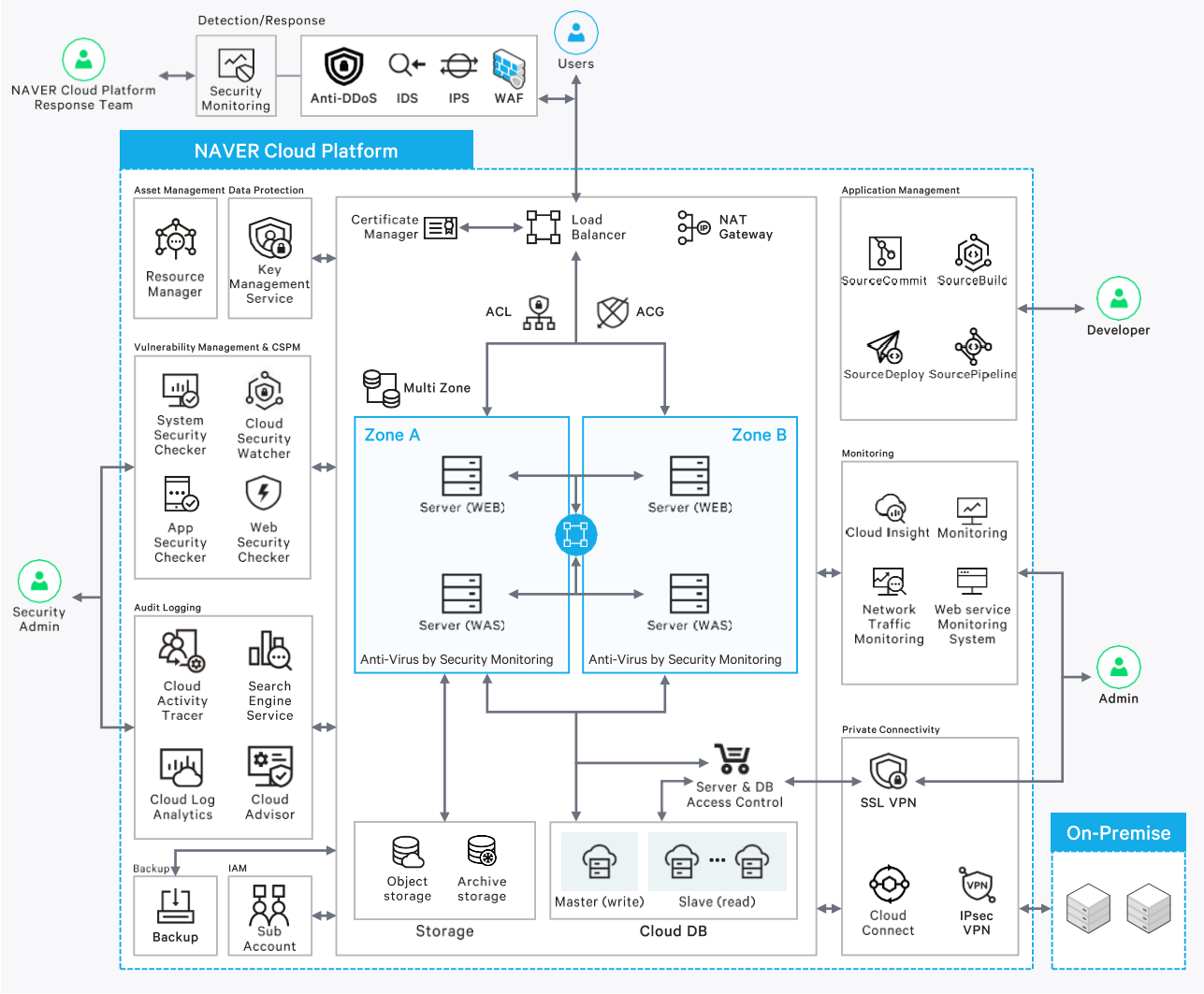
- 보호대책 관련 서비스
  - Backup
  - Server
  - Object Storage
  - VPC
  - Cloud DB

5. 인증기준 준수를 위한 참조 보안 Architecture

보안 서비스를 통해 ISMS-P보안 Architecture를 구성

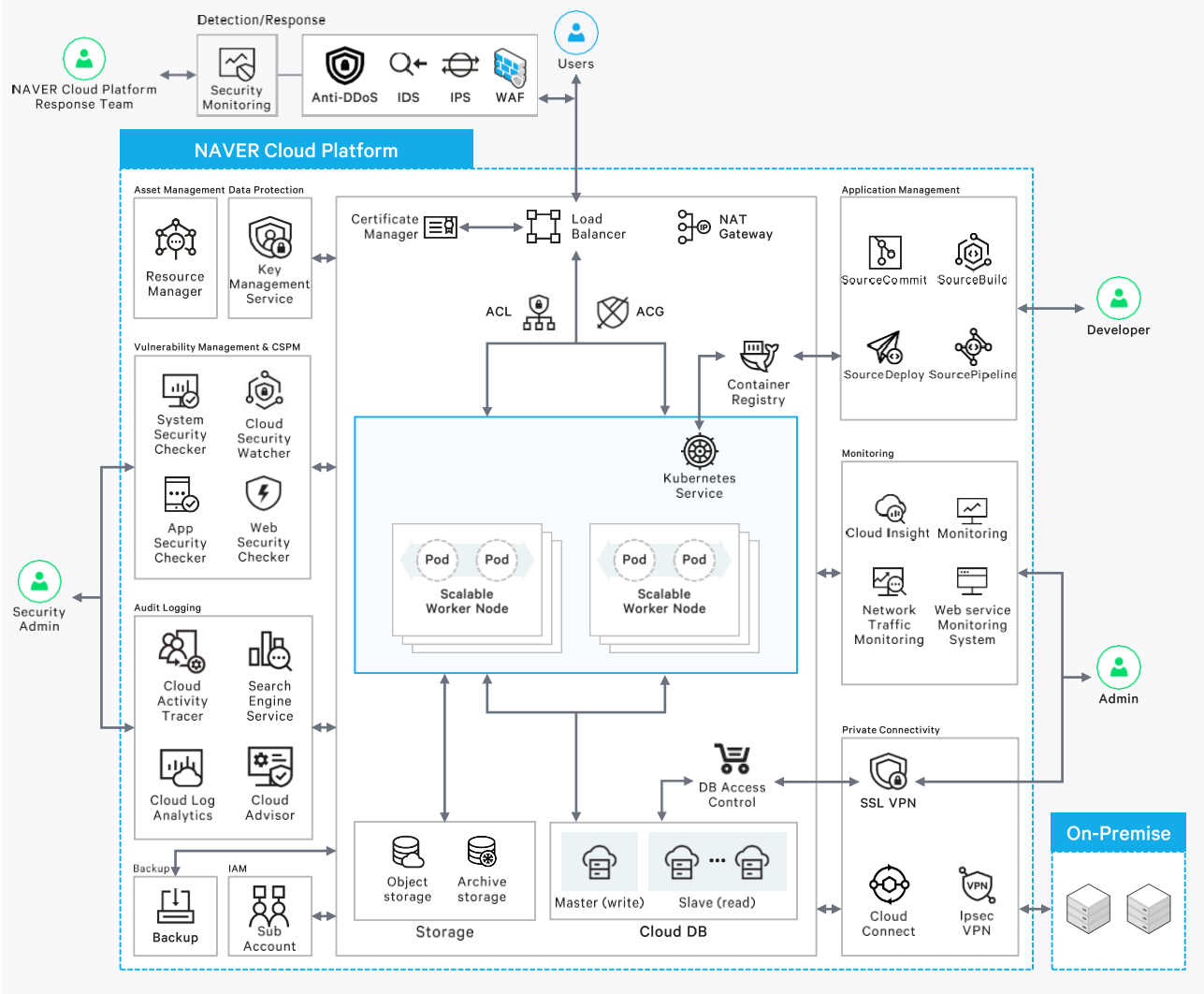
- 네이버 클라우드 플랫폼 고객이 서비스 구성을 위해 일반적으로 많이 사용되어지는 3-tier구조의 IaaS Architecture와 Kubernetes Service Architecturer 구성방안을 적용한 보안 Architecture 입니다.

IaaS 보안 Architecture (VPC)



[ISMS-P 인증을 위한 IaaS 보안 Architecture 구성 예시]

K8s보안 Architecture (VPC)



[ISMS-P 인증을 위한 k8s 보안 Architecture 구성 예시]

6. 끝맺음

서비스 기획 단계에서부터 ISMS-P인증기준 아키텍처를 고려

- 고객의 비즈니스가 성장함에 따라서 ISMS-P 구축의 필요성은 지속적으로 요구되어 질 것입니다. 서비스의 성장으로 인하여 '정보통신망 이용촉진 및 정보보호 등에 관한 법규 ' 에서 규정한 인증 취득 의무대상자에 해당 되는 경우,Compliance준수를 위하여 ISMS-P인증 취득이 필요합니다.

- 네이버 클라우드와 고객 간의 책임 영역을 정확히 이해하고,정보보호 관리체계 구성을 위해 필요한 네이버 클라우드 플랫폼의 서비스들은 무엇이 존재하는지,해당 서비스들의 기능은 무엇인지,해당 서비스들의 기능은 무엇인지, 서비스의 구성을 위해 고객이 고려해야 할 사항이 무엇인지 등을 명확히 이해하는 것이 중요합니다. 이를 고려하지 않고 구축된 고객의 서비스와 Architecture는 수정을 위해 시간과 노력,비용 등 많은 리소스의 투입이 필요해 질 수 밖에 없습니다.

- 따라서, 고객의 서비스 기획 단계에서부터 본 가이드를 참고하면 네이버 클라우드 플랫폼 환경에서 고객의 서비스에 안전한 정보보호 및 개인정보보호 관리체계의 Architecture를 구성하는데 도움이 될 수 있습니다.

감사합니다.