클라우드
역량강화 교육

2023. 11

행정안전부

NIA 한국지능정보사회진흥원

클라우드 역량 강화 교육

클라우드 역량강화 교육은 행정안전부와 한국지능정보사회진흥원이 ’22년 행정 · 공공 클라우드 전환 기관을 대상으로 권역별(서울, 충청, 영남, 호남/제주)로 진행한 교육입니다.

이용시 출처를 밝혀 주시기 바랍니다.

- 한국지능정보사회진흥원 [공공클라우드 전환팀]
  ※ 공공클라우드 지원센터(https://cpcp.or.kr) 홈페이지 / 자료실

목 차

PART Ⅰ

PART Ⅱ

PART

클라우드 역량 강화 교육

정부 정책 방향 및 성공 사례

1. 디지털플랫폼정부 클라우드 정책 방향
2. 정보시스템 클라우드 전환·통합사례 및 성과발표(서울권)
3. 정보시스템 클라우드 전환·통합사례 및 성과발표(충청권)
4. 정보시스템 클라우드 전환·통합사례 및 성과발표(영남권)
5. 정보시스템 클라우드 전환·통합사례 및 성과발표(호남권)

디지털플랫폼정부 클라우드 정책방향

NIA 공공 클라우드 전환팀
강현구 팀장

행정안전부 NIA 한국지능정보사회진흥원

디지털플랫폼정부 클라우드 정책방향

CONTENTS

Ⅰ 디지털플랫폼정부 추진방향

행정안전부
NIA 한국지능정보사회진흥원

NIA 한국지능정보사회진흥원

01 디지털플랫폼정부 추진 필요성

성과 디지털 기술을 적극 수용하여 세계 최고 수준의 전자정부 구현

컴퓨터·PC 시대 ('67~)
- 인구 통계업무에 IBM1401 도입('67.4)
- 1~2차 행정전산화 기본계획 ('78~)
- 5대 국가기간전산망 사업('87~)

인터넷 시대 ('00~)
- 전자정부법· 전자정부특별위원회('01)
- 전자정부지원사업('01~)
- 정부민원포털(민원24) 구축('02)

모바일 시대 ('10~)
- 모바일 전자정부 기본계획('10)
- 공공데이터법('13)
- 정부3.0 추진위원회 ('14)
- 정부 통합 포털 정부24 개통('17~)

UN 전자정부 발전지수 2위

한계 분업화 구조 하에서 기관별로 개별 시스템 고도화 ➔ 국민 관점의 통합적 서비스 제공에 걸림돌

칸막이에 막힌 부처

따로 노는 17,060개 정보시스템

창고에 갇힌 데이터

단위 시스템 안에 고립된 데이터

파편화된 서비스

데이터 단절 = 서비스 단절

02 디지털플랫폼정부 비전 및 목표

문제점 개선

1. 정부부처간 칸막이
2. 공공과 민간의 칸막이
3. 디지털 기술과 아날로그 제도간 정책

추진 과제

1. 국민께는 하나의 정부로서 개인화된 맞춤형 서비스
2. 기업에는 민관 협업 바탕의 새로운 도약과 성장의 공간 마련
3. 정부는 모든 부처가 함께 똑똑하게 일하는 정부로 혁신

인공지능·데이터로 만드는

"세계 최고의 디지털플랫폼정부"

비 전

Strategy 01 ▸▸▸ 하나의 정부

1. 디지털을 기본으로 행정체계 전반 혁신 (Digital by Design)
2. 데이터 칸막이의 근원적 해소
3. **디지털플랫폼정부 혁신인프라 구현**

Strategy 02 ▸▸▸ 똑똑한 나의 정부

1. 한곳에서, 한번의 신청으로 끝나는 통합서비스
2. 요구하지 않아도 알아서 챙겨주는 초개인화 서비스
3. 국민 누구나 혜택을 누리는 환경 조성
4. 인공지능·데이터 기반의 과학적 행정 일상화
5. 투명하고 공정한 디지털 민주주의 실현

Strategy 03 ▸▸▸ 민관이 함께 하는 성장 플랫폼

1. 민관이 함께 사회문제를 발굴·해결하는 협업플랫폼 구축

Strategy 04 ▸▸▸ 신뢰하고 안심할 수 있는 DPG 구현

1. 개인정보에 대한 정보주체, 국민의 권리 강화

03 디지털플랫폼정부 주요 목표전략

Strategy 1.3 디지털플랫폼정부 혁신인프라 구현

민간 기반의 클라우드 네이티브 전면 전환

클라우드 네이티브 및 SaaS 적용 의무화 ('24 ~)

고도화 계획이 없는 기존 주요 시스템* 대해서도 모듈화된 서비스 구조(MSA)를 반영한 클라우드 네이티브 전환 지원('23~)**

* ▲서비스 복잡도가 높은 시스템, ▲명확한 경계가 가능한 시스템, ▲더 이상 확장할 수 없는 한계지점에 도달한 시스템 등 시급성, 파급효과 등을 종합적으로 고려

** (Micro Service Architecture) 작고 가벼운 서비스 구조

클라우드 네이티브(Cloud Native) 란?

▸ 클라우드 특화 기술*을 사용하여 클라우드 컴퓨팅의 장점을 최대한 활용할 수 있는 서비스를 구축하고 운영하는 방식

*개발·운영의 통합 운영(DevOps), 자동통합·배포(CI/CD), 작고 가벼운 서비스 구조(MSA)

< 기존 방식 대비 클라우드 네이티브의 장점 >

기존방식(Monolithic)	클라우드 네이티브
• 크고 복잡한 통구조 • 확장, 구축 및 개선에 많은 시간·비용 소요 • 인공지능 등 첨단 기술 적시 도입 어려움	• 작고 빠른 서비스 개발·배포 • 탄력적·효율적 자원 활용 • 최신기술 도입 용이등 민간 혁신기술 활용성 및 서비스 유연성 강화

04 공공 클라우드 전환 로드맵 변화

공공 클라우드 전환 사업이 행정안전부 주도에서 부처별 추진으로 전환됨

RoadMap 공공 클라우드 네이티브 전환

추진 배경

- 정부 재정 투자방향 변화
- 보안인증제 개편
- 신기술 보편화 등

추진 환경

- 정부 정책 '민간 클라우드 우선 이용' ' 클라우드 네이티브 우선 적용 ' 으로 발전 등

추진 방향

범 정부 정보자원 등록·관리 시스템에 등록된 모든 시스템의 클라우드 네이티브 전환

추진 기간

2024년 부터 2030년 까지 7개년 추진

행정안전부 주도 ▶▶ **부처별 추진**

출처: 전자신문 2023-05-03

디지털플랫폼정부 클라우드 정책방향

II 클라우드 네이티브 기본 개념

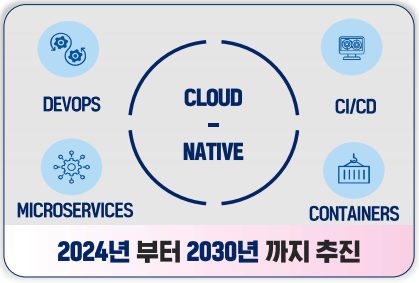
01 클라우드 네이티브 기본개념
02 클라우드 네이티브 구성요소

01 클라우드 네이티브 - 기본개념

핵심요소 클라우드를 클라우드 답게 사용하기 위함

전환 로드맵 변화

클라우드 네이티브 전환



Application 개발 측면

- MSA(API 중심)
- DevOps(CI/CD)

IT 인프라 운영측면

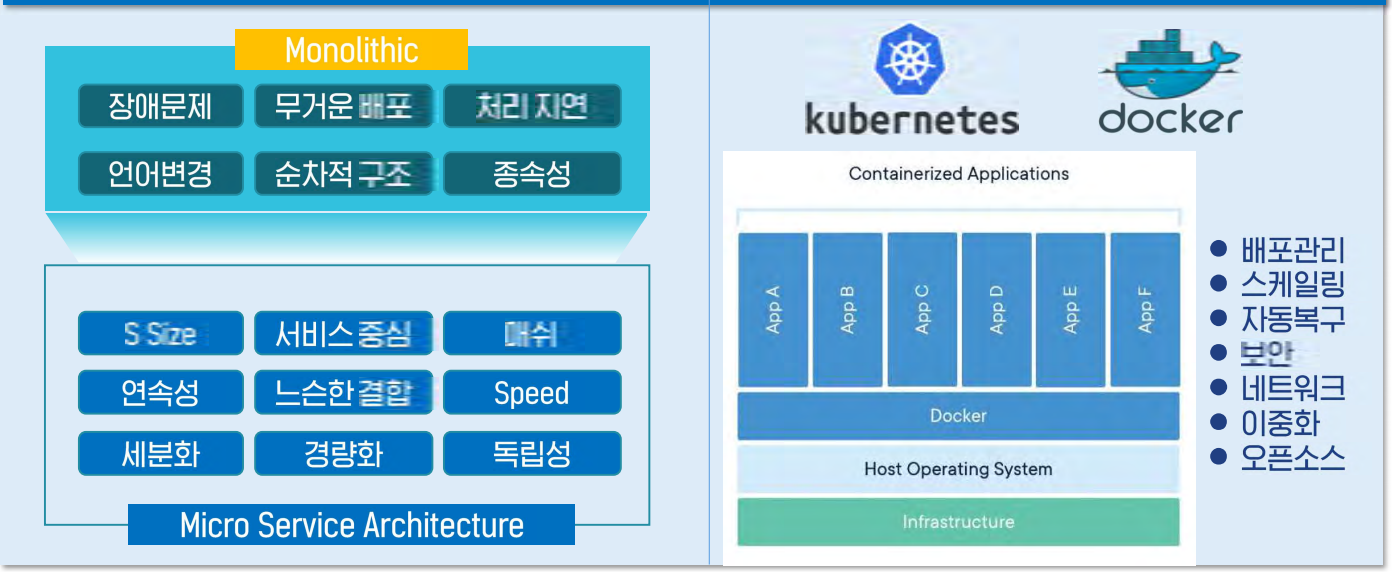
- 컨테이너(Container)
- 공개SW(Open Source)

- 민첩성 (빠른 배포 및 테스트)
- 이식성 (컨테이너 보급)
- 확장성 (빠른 개발/증설)
- 표준성 (소스, OS 등)
- 협력성 (조직 간 소통)
- 경제성 (자원활용율 증대)

02 클라우드 네이티브 - 구성요소(1/2)

MSA : 단일 AP가 다수의 느슨하게 결합되고 독립적으로 배치 가능한 더 작은 서비스로 구성된 클라우드

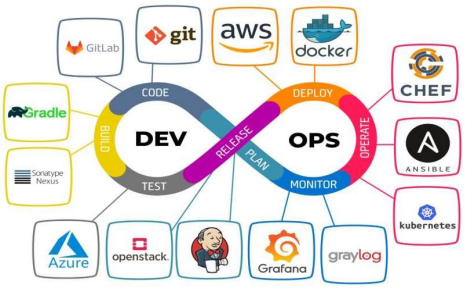
컨테이너 : 환경 종속적이지 않은 필요한 모든 요소를 포함하는 소프트웨어 패키지



02 클라우드 네이티브 - 구성요소(2/2)

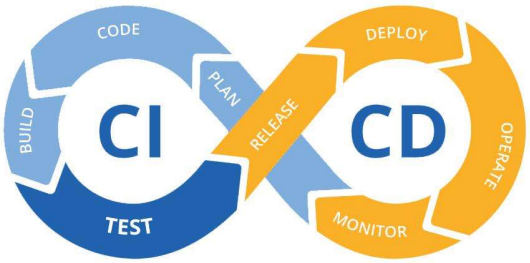
DevOps : 개발(Development) 과 운영(Operation)합성어 협업을 통한 지속적 향상 강조

- 빠른 작업 속도
- 신속한 제공
- 안정성 향상
- 높은 확장성
- 협업 강화
- 보안체계 유지



CI/CD : 어플리케이션 개발단계부터 배포까지 모든 단계들을 자동화 하여 효율적 배포 진행

- CI (Continuous Integration) : 버그 수정 또는 새로운 기능이 Main Repository에 주기적으로 빌드 / 테스트 되어 통합하는 것
- CD (Continuous Deployment) : 변경이 출시되자 마자 자동으로 사용자에게 배포되는 모든 과정을 자동화 하는 것



디지털플랫폼정부 클라우드 정책방향

III 클라우드컴퓨팅서비스 이용안내 가이드

01 클라우드컴퓨팅서비스 기본개념
02 도입시 고려요소
03 이용료 산정 및 서비스 계약 방안
04 자체 계약을 위한 계약 절차 및 프로세스

행정안전부
NIA 한국지능정보사회진흥원

NIA 한국지능정보사회진흥원

01 클라우드컴퓨팅서비스 기본개념 – 서비스 유형 등

클라우드컴퓨팅서비스 유형 따른 서비스 제공 범위

클라우드 서비스 제공 사업자(CSP)

구분	제공서비스
클라우드 제공 방식	• 공유, 프라이빗 클라우드 제공
네트워크	• 상용망, 전용망, VPN, VPC, CDN, NAT 등
보안체계	• 접근제어, 침입탐지/대응, 인증, 암호키, 로그인 및 모니터링, 취약점 관리, 모의 훈련제공 등
오토 스케일링	• 자원정책, 모니터링, 정책기반 자동(매뉴얼) 스케줄링 등
백업	• DBMS 백업, 파일 백업 등
장애, 재해	• 고가용성(HA), 재해복구(DR) 구성
SaaS 제품	• 기관 맞춤형 업무서비스, 업무자동화 솔루션, 블록체인, 화상회의, 빌링 서비스, 회계관리, 주소제공 등
기타	• IoT 관련, AI(음성/얼굴 등 인식, 번역, 지도, 빅데이터 등)

매니지먼트 제공 사업자(MSP)

구분	제공서비스
컨설팅	• 클라우드 환경 도입을 위한 방법론, 절차, 비용 등 전체 ISP수립 계획 지원 • 문제점 개선 및 고도화 방향 제시 등
마이그레이션	• 성능 및 비용 절감이 가능하도록 클라우드 환경으로 자원 이전 측면 기술지원 및 전환 제공 • 신기술에 기반한 운영 효율성, 편리성 강화 등 전용 AP 플랫폼 등으로의 이전/전환 제공
유지보수	• 클라우드 환경에서 최적의 상태를 유지하도록 테스트, 예방정비, 장애 처리 등의 운영/유지 관리 서비스 인력 제공
운영지원	• 업무지원, AP개발, 자원의 조정, 모니터링 등의 운영인력 제공
서비스 유통	• CSP 사업자의 클라우드 통합 환경 및 개별 IaaS, 이용기관 맞춤 플랫폼 등의 PaaS, SaaS 중재(대행)하여 제공 • MSP 사업자의 자체 개발 특화 SaaS 제품 제공

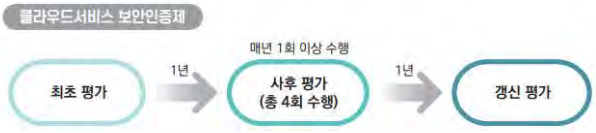
NIA 한국지능정보사회진흥원

01 클라우드컴퓨팅서비스 기본개념 - 클라우드 보안 인증제도 소개(CSAP)

보안인증 유형·등급 및 종류

• 클라우드서비스 보안인증제도의 인증 유형은 **IaaS, SaaS(표준등급, 간편등급), DaaS**이며, 인증 등급은 상·중·하로 구분됩니다. 또한, 평가 종류는 최초평가, 사후평가, 갱신평가가 있습니다.

※ 기존 인증제도는 상·중등급 변경 시행전까지 인증 신청가능



• 인증 유형 및 등급

- **(인증 유형)** IaaS, SaaS, DaaS 인증 유형으로 구분되며, 유효기간은 5년으로 운영

구 분	IaaS	SaaS		DaaS
		표준등급	간편등급	
인증항목	116개	79개	31개	110개
유효기간	5년			

- **(인증 등급)** 상·중·하 등급 인증 등급으로 구분되며, 유효기간은 5년으로 운영

구 분	하등급	하등급 SaaS	중등급	상등급
인증항목	64개	30개	추후 안내 예정	
유효기간	5년			

보안인증 체계

구 분	주관기관	주요역할
정책기관	과학기술정보통신부	• 보안인증 관련 법·제도 개선 및 정책 수립 • 인증/평가기관의 지정 및 감독
인증기관	한국인터넷진흥원	• 인증 신청접수 • 보안인증기준, 지침 개발 • 인증서 발급 • 인증된 클라우드서비스 관리 • 기타 인증업무 수행
평가기관	한국인터넷진흥원 및 과학기술정보통신부에서 지정한 기관	• 보안인증기준에 따라 인증평가 수행을 위한 평가팀 구성 • 보안인증기준에 따라 인증평가 수행
인증위원회	한국인터넷진흥원	• 평가결과를 통한 인증 심의·의결 • 인증취소의 타당성 심의 • 학계, 연구기관, 기술자문기관 등 클라우드 관련 전문가 15인 이내로 구성
기술 자문기관	국가보안기술연구소	• 국가·공공기관 민간 클라우드서비스 이용 보안기준 마련 • 국가·공공 클라우드 안전성 강화 대책 수립
인증신청인	클라우드서비스 제공자	• IaaS, SaaS, DaaS 등 클라우드서비스 제공 • 자체 보안활동 정기· 수시 수행

02 도입시 고려요소 – 민간 클라우드컴퓨팅서비스 우선 도입

클라우드컴퓨팅서비스 관련 법 제도

클라우드 컴퓨팅 법

제12조 (국가기관등의 클라우드 컴퓨팅 도입 촉진)
② 정부는 『국가정보화 기본법』에 따른 국가 정보화 정책이나 사업추진에 필요한 예산을 편성할 때에는
클라우드 컴퓨팅 도입을 우선적으로 고려하여야 한다.

예산안 편성 및 기금운영계획안 작성 세부지침

중앙관서는 정보시스템 구축·운영 예산 요구시 **클라우드 컴퓨팅 도입·전환 가능성을 우선적으로 고려하고**, 클라우드컴퓨팅 서비스 이용규모와 향후 변동 규모 등을 종합적으로 검토하여 적정 예산을 요구

디지털플랫폼 정부 실현계획 ('23년 4월)

1.3 디지털플랫폼정부 혁신인프라 구현
■ 민간 기반의 클라우드 네이티브 전면 전환
❍ 신규 시스템 구축 및 기존 시스템 고도화 시, **민간 클라우드 우선 적용 및 불가피한 사유가 없는 한 클라우드 네이티브 및 SaaS 적용 의무화 ('24 ~)**

클라우드 네이티브 전환 로드맵 수립 · 이행

1) 기관별 '24년~'30년 전환 로드맵 수립
2) 정보자원통합심의위원회 통해 심의·의결

로드맵 수립 → 심의·의결 → 네이티브 전환이행 → 로드맵 이행점검 → 수정계획 제출 → 로드맵 변경관리

3) 기관 자체적 클라우드 전환 추진
4) 행안부 매년 로드맵 이행점검
5) 점검 결과에 따라 수정 전환계획 제출
6) 정보자원통합심의위원회 통해 심의·의결

행정 · 공공기관 클라우드 네이티브 전환 로드맵 수립

민간 클라우드 "우선" 클라우드 컴퓨팅 도입

네이티브 및 SaaS "의무"

민간 기반 클라우드 네이티브 전면 전환

02 도입시 고려요소 – 이용기획 체크리스트 활용

1. 사업 대상 결정 → **2. 정보자원 파악** → **3. 상용 SaaS 우선 이용검토** → **4. 고려사항 종합검토** → **5. 클라우드컴퓨팅서비스 최종 이용여부 판단**

1. 사업 대상 결정	2. 정보자원 파악	3. 상용 SaaS 우선 이용검토	4. 고려사항 종합검토	5. 클라우드컴퓨팅서비스 최종 이용여부 판단
✓ 전환·재구축 사업, 신규 구축 사업 등 사업 유형 확인	✓ 디지털서비스 이용지원 시스템 활용	✓ 보안성, 안전성 등 종합 검토	✓ 도입 여부 결정	

이용기획 체크리스트(예시)

1.사업 대상 결정		
1.1. 클라우드컴퓨팅서비스 도입검토에 사업 추진방향 결정		
● 전환 재구축 사업 추진	□	→ 2.1번 문항으로
● 신규사업으로 추진 H/W	□	→ 2.2번 문항으로
2. 정보자원 파악		
2.1. 전환 재구축 추진		
● 현재 서비스 중인 정보시스템(서비스) 파악	□	
● 정보시스템과 연계된 네트워크 구조의 SW 환경및 HW 자원파악	□	
● 정보시스템 유지보수 및 운영 인력 관련 파악	□	
● 파악된 자료를 근거로 비용, 보안, 운영환경 등의 현황 종합 정리	□	
2.2. 신규 구축 추진		
● 신규 도입 정보시스템 목적 및 서비스 정의	□	
● 신규 정보시스템 구성에 필요한 자원 파악 (레거시 추진시/ 클라우드 추진시)	□	
3.상용 SaaS 우선 이용 검토		
3.1 디지털서비스 이용지원시스템의 상용 SaaS 이용가능 여부		→ 해당 없으면 3.2번으로 이동
● SaaS 이용료, 이용 제공 범위 등의 현 제공방식 대비 비교 자료 확보	□	
● 레거시 방식으로 신규 도입 시의 고려 항목 관련 비교 자료 확보	□	
3.2 디지털서비스 이용지원시스템의 IaaS 서비스 활용 계획		
● 시스템 구성에 필요한 IaaS 자원 및 개발항목 등 자료 확보	□	
● IaaS 자원별 이용료, 구축, 운영 범위 등의 고려 항목 비교 자료 확보	□	
4. 고려사항 종합검토		
4.1 SaaS 및 IaaS 클라우드컴퓨팅서비스도입을 위한 종합(비교) 검토		→ 아래 종합검토표 예시 참고
● (보안성) CSAP인증 서비스 여부 및 미인증 보안 국정원 사전검토	□	
● (안정성) 업무 무중단의 현 안정성 대비 검토	□	
● (확장성) 상면, 자원, 운영관리 측면의 검토	□	
● (비용효율성) 레거시 기준 기년 비용 비교 검토	□	
● (기타) 업무 효율성, 접근성 등의 검토	□	
5. 클라우드컴퓨팅서비스 최종 이용여부 판단		
5.1. 고려사항 종합 검토 결과		
● 상용 SaaS 도입	□	→ 구매 및 이용
● 복합 IaaS 활용 도입	□	→ ISP등 도입계획
● 미도입	□	→ 불가 사유 마련

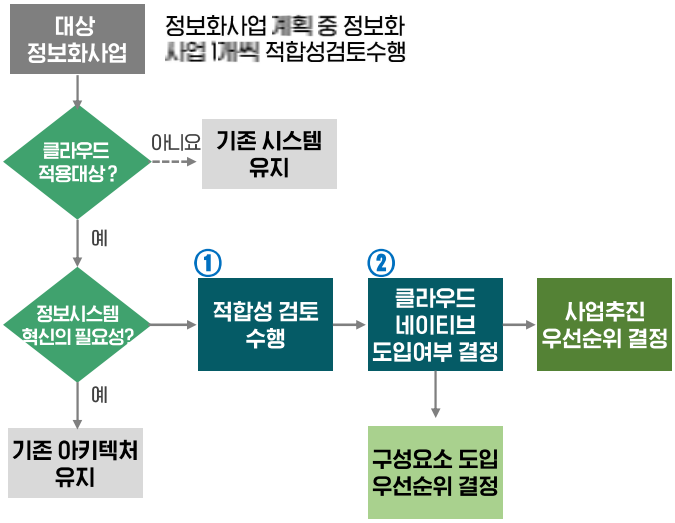
클라우드컴퓨팅서비스 도입 관련 검토항목(예시)

고려항목	검토 항목	체크
보안성	CSAP 보안인증 제품 여부 및 보안 미인증 서비스는 사전 협의 검토	□
	클라우드 연계경로 상의 보안취약점 여부	□
	현 보안 관리 항목 대비 클라우드 보안항목 비교	□
	보안 위협에 대한 빠른 인지 및 조치 가능 여부	□
안정성	현 시스템 구조 대비 클라우드 적용 구조 비교	□
	장애 발생 시 복구 및 영향 범위 비교	□
	이용자원 및 기술지원 범위 비교	□
	재난 발생 시 복구 시나리오	□
확장성	향후 이용 범위 증가 시 추가 확장 용이성	□
	특정 기술 업체에 대한 종속성 여부 비교	□
	상면 등의 인프라 확충 관련 비교	□
	정책 및 기술 동향을 고려한 중장기 보장성	□
비용 효율성	초기 투자비용 비교	□
	유지보수 비용 비교	□
	회선 접속 비용 비교	□
	향후 시스템 확장 시 추가비용 비교	□
기타	이용의 편의성	□
	업무의 이동성	□
	가용성에 따른 자원의 확대·축소	□
	기타 특화 내용	□

참고: 행정·공공기관 클라우드컴퓨팅서비스 이용안내서

02 도입시 고려요소 – 클라우드 네이티브 적합성 검토

클라우드 네이티브 적합성 수행 개요



참고: 클라우드 네이티브 정보시스템 구축을 위한 발주자 안내서

① 클라우드 네이티브 적합성 검토 체크리스트 활용

목표 구분	적합성 검토 항목	점검사항
정책 및 업무 변화 대응	정책 및 업무 변화에 대한 민첩한 대응	1-1. 한국판 뉴딜과 같은 새로운 정책, 기관별 업무계획 등 다양한 정보화 요구사항 변화에 대해 신속한 대응이 필요합니까?
	디지털 혁신 및 지능화 지원	1-2. 디지털 혁신 및 지능 정보화 관련 신기술(빅데이터, AI, 블록체인, IoT 등)의 도입이 필요하고, 연관된 애플리케이션의 개발 또는 개선이 요구됩니까?
안정적 서비스 운영	서비스 개선 요구사항 적시 대응	2-1. 서비스 이용자의 접은 CSR(Customer Service Request, 고객의 서비스 요구사항)에 대해 적시 대응이 필요합니까? 또는 초기 개발비의 약 15% 이상을 매년 추가개발 및 유지보수 비용으로 사용하고 있습니까?
	접속 지연, 서비스 장애 문제 신속한 해결	2-2. 다양한 원인에 의한 장애 발생 시 장애복구(예:시스템 증설, 업그레이드 등)를 위해 서비스를 중단한 적이 있습니까? 또는 이용자의 폭증에 의한 접속지연으로 이용자의 불만이 제기된 적이 있습니까?
	소규모 서비스 분리 및 독립적 운영	2-3. 소규모 서비스 단위로 기능과 DB가 명확하게 분리되고, 독립적으로 서비스를 실행할 수 있습니까? (공통 기능 및 데이터 사용 유무, 타 시스템과의 연계성, 서비스 의존 관계 등 확인)
	다양한 플랫폼 환경에서의 이식성 보장	2-4. 개발-테스트-운영 환경에서 안정적이고 지속적인 배포가 필요하거나 다양한 플랫폼 환경에 애플리케이션 배포가 요구됩니까?
개발 품질 향상	개발-운영 협업 조직체계 구현	3-1. 시스템 개발 및 운영 시 개발팀과 운영팀의 분리에 의한 의사소통의 문제, 개발 및 배포 지연 등의 문제가 존재합니까?
	전문인력 역량 강화	3-2. 개발-빌드-배포 과정의 품질 향상을 위해 전문 인력을 확보하거나 기존 인력에 대한 전문적인 교육이 필요합니까?
개발 생산성 향상	코딩-빌드-테스트-배포 파이프라인 자동화	4-1. 개발된 SW를 형상관리 시스템에 커밋한 후 개발/검증/운영 서버에서 각각 빌드, 테스트, 배포하는 과정 전체에 대해 자동화 도구를 도입하거나 추가할 필요가 있습니까?
	기술 변경 용이성 확보	4-2. 오픈소스 SW를 비롯한 다양한 기술의 도입, 업그레이드, 업데이트 등 작업 수행 시 연관된 서비스에 대한 변경 작업이 복잡하여 개발 상의 어려움을 겪은 적이 있습니까?

② 클라우드 네이티브 도입여부 결정 기준

"예"응답수	도입여부 결정 기준	비고
1개 ~ 3개	• 기존의 애플리케이션 아키텍처 유지	• 적합성 검토 항목의 답변을 기준으로 클라우드 네이티브 구성요소를 부분적으로 도입
4개	• 기존의 애플리케이션 아키텍처 유지 • 필요시 클라우드 네이티브 구성요소 일부 도입 가능	
5개	• 클라우드 네이티브 도입 가능	
6개 ~ 8개	• 적극적으로 클라우드 네이티브 도입	
9개 ~ 10개	• 매우 적극적으로 클라우드 네이티브 도입	• 우선적으로 정보화사업 추진

03 이용료 산정 및 서비스 계약 방안

클라우드컴퓨팅서비스 별 이용료 산정 방안

구분	자원	자원 이용료 부과
IaaS	서버	• vCore/Mem/Disk, OS
	스토리지	• HDD, SSD, NAS, Object, block
	네트워크	• 로드 밸런서, 트래픽, 공인IP, VPN
	백업	• Full Backup, 증분백업, 백업용량
	보안	• 웹방화벽, IPS/IDS, DDoS • DB접근제어, DB암호화 • 서버접근제어, 서버백신
	관제	• 기본관제(Computing 자원) • 추가관제(WEB, WAS, Session) • 운영지원, 보안관제
고려사항		• CSP 별 부과기준 다름 • 서비스 규모, 이용시간, 계약기간 에 따른 할인율 상이 • 기본 이용료 외 3rd Party 이용료 반드시 확인 필요

구분	서비스	개발에 필요한 플랫폼을 제공하는 서비스
PaaS	K-PaaS	• 컨테이너 서비스 인프라 제공, 컨테이너(CaaS), 플랫폼(PaaS) 비용 부과
	Container	• Kubernetes 등 컨테이너화된 AP의 배포, 확장 및 관리 자동화 서비스
	CI/CD	• 클러스터 내 개발, 이미지관리, 소스 빌드 등 CI/CD에 필요한 기능 비용
	DevOps	• 형상관리, 소스병합, 빌드, 배포, 연결, 릴리즈 등 결합상품

구분	서비스	완성형 상품 서비스 부과
SaaS	비즈니스 서비스	• 메일, 메신저, 오피스솔루션, 협업솔루션, 화상회의솔루션
	정보 조회 서비스	• 조회통계서비스, 법인조회서비스
	고객관리 서비스	• 상담관리 서비스
	시스템지원 서비스	• 문자단축URL, 문자서비스, 시스템 성능분석, API관리 서비스
	위치정보 서비스	• IP 기반위치정보 서비스, 지도 서비스
	데이터분석 서비스	• 유전체 분석 서비스, 빅 데이터분석 서비스

NIA 한국지능정보사회진흥원

03 이용료 산정 및 서비스 계약 방안

서비스 이용 단계 및 절차

이용기획단계	도입 단계	이용단계	이용종료단계
사업대상 결정	사업계획 수립	서비스 이용 계약	계약의 해지 및 해제
클라우드 컴퓨팅 서비스 이용여부 검토	정보화사업 사전협의	SLA 체결	이용정보 반환 및 폐기
SaaS 이용여부 우선 검토	국정원 보안성 검토	운영관리	이용 종료
클라우드컴퓨팅서비스 이용 ISP 수립	이용료 산정	서비스 수준 및 사용량 측정	
중기재정계획 수립	이용료 예산편성 및 확보	이용료 정산	

※ 중앙 공공기관은 서비스 이용계약을 체결하는 경우 표준계약서를 사용할 수 있으며, MSP 사업자와 추진할 때는 MSP 사업자와 CSP 사업자 간에 체결된 EA(기업협정, Enterprise Agreement), 이용약관 등이 계약서의 내용에 포함되어야 하며, 발주기관은 이를 확인하여야 한다.

NIA 한국지능정보사회진흥원

04 자체 계약을 위한 계약 절차 및 프로세스

계약 방안

조달청 일반용역

조달청요청 접수 → 규격검토 및 사전규격공개 → 입찰공개 → 낙찰자 선정 → 계약체결

수의계약

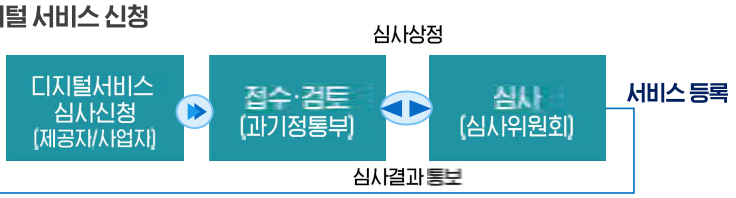
「국가를 당사자로 하는 계약에 관한 법률 시행령」 제26조 제1항 제5호 아목
아. 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 시행령」 제8조의2제1항에 따라 선정된 디지털 서비스에 관한 계약을 하는 경우

카탈로그 계약

「조달사업법시행령」 제16조제3항
③ 조달청장은 제2항에도 불구하고 「국가를 당사자로 하는 계약에 관한 법률 시행령」 제26조 제1항 제5호 아목에 따른 수요물자의 경우에는 심사를 통해 1인을 계약상대자로 결정할 수 있다.

계약 절차 및 프로세스

1) 디지털 서비스 신청



1-1)수의계약

1-2) 카탈로그 계약

정보시스템 클라우드전환·통합 사례 및 성과발표(서울권)

㈜클로잇
황인주 수석

행정안전부 NIA 한국지능정보사회진흥원

정보시스템 클라우드전환·통합 사례 및 성과발표

CONTENTS

정보시스템 클라우드 전환·통합 사례 및 성과발표

I 사업개요

행정안전부
NIA 한국지능정보사회진흥원

NIA 한국지능정보사회진흥원

01 사업 범위

본 사업은 수도권 27개 공공기관 , 133개 정보시스템을 클라우드로 전환 한 후, 1년간의 클라우드 운영 포함

01 행정·공공기관 설계 확정
- 기관별 규모 난이도 분석
- 전환 대상 기관 전환 계획 협의
- 난이도별 전환 일정 확정
- 선행 설계 대비 차이 시스템 대응

02 클라우드 서비스 환경 구성
- CSP 별 서버, NW, 스토리지 환경 구성
- 전환 서비스 이용 및 기술 지원
- 보안 관련 규정 준수 및 보안체계 확립
- 정보시스템 보안대책 마련

03 클라우드 전환 및 검증
- 전환 전 성능 측정
- 변경 SW별 전환 방안 수립
- SW 변경 대응 수정 및 데이터 이관
- 전환 후 기능 안정성 및 성능 점검

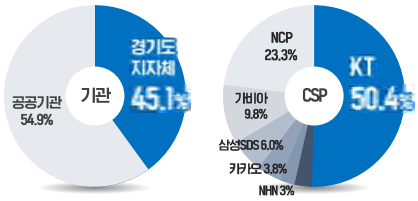
04 성과 관리
- 전환에 따른 정량·정성적 효과 분석
- 자원 활용 효과 분석
- 산업 활성화 / 탄소절감 기여 분석
- 클라우드 전환에 따른 비용 효과 분석

05 클라우드 운영
- 상시 모니터링
- 기관별 SLA관리
- 운영 SR 처리
- 서비스 이용 기술지원

02 사업 특징

01 특정 기관/CSP 비중이 높음

클라우드 전환 경험이 필요!

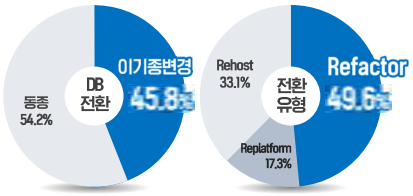


2차년도 연속사업 기관
가평군, 광명시, 도로교통공단, 한국환경산업기술원

클라우드 전환 사업 전문가 투입

02 이기종 DB 변경이 많음

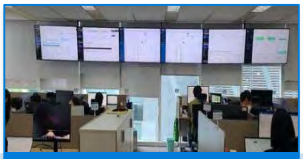
전환 난이도가 높음!



Refactor	Replatform	Rehost
소스코드 변경	플랫폼 변경	단순 전환

전문기술 협업 체계

03 1년간 운영 포함



통합관제센터 운영

1. 원-채널 장애지원 체계 수립
2. 24x365 모니터링/보안관제
3. 정보자원의 탄력적 운영

침해사고 대응 | 장애 대응

안정적 운영 체계

03 사업 일정(1/2)

일정 수립 고려사항

1 철저한 사전 분석에 의한 업무 분장

27개 전환기관 / 133개 전환 업무 / 6개 CSP + SaaS → 4개 전환 팀 구성

2 전환 난이도에 따른 전환 일정 수립

- A등급 : 충분한 시험운영 연계테스트 시행
- B/C 등급 : 우선 전환

3 대용량 데이터 사전이관 실시

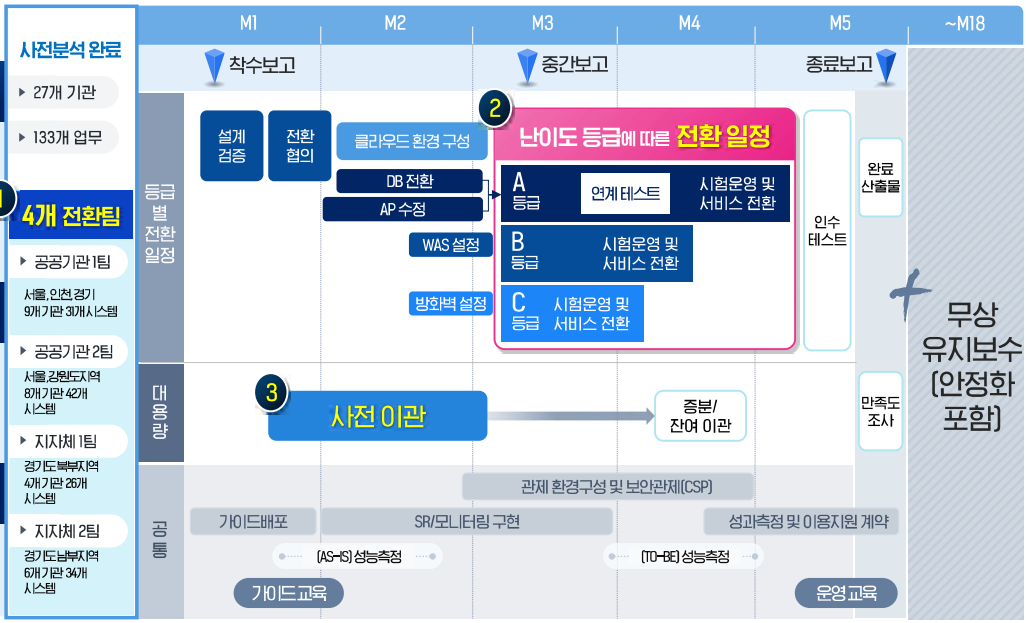
대용량데이터 이관시간 단축을 위한 **사전 이관 실시**

사전분석 완료

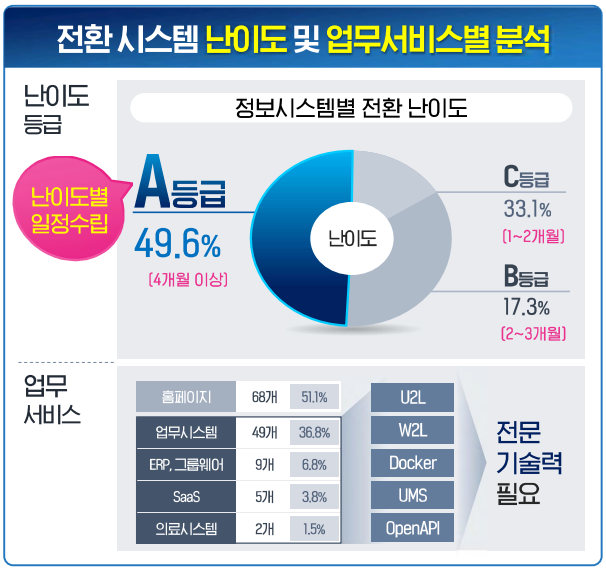
- 27개 기관
- 133개 업무

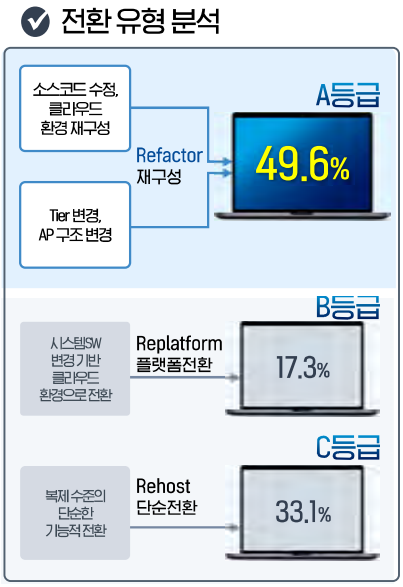
1 4개 전환팀

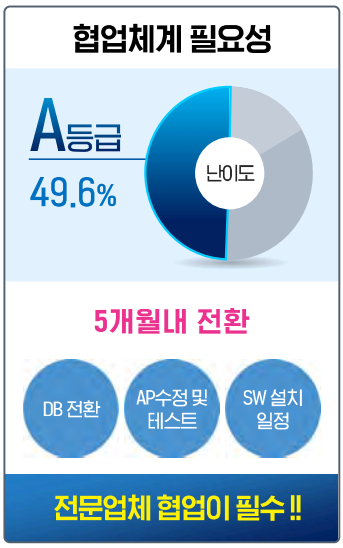
- 공공기관 1팀 — 서울, 인천, 경기 9개기관 31개 시스템
- 공공기관 2팀 — 서울, 강원도지역 8개기관 42개 시스템
- 지자체 1팀 — 경기도북부지역 4개기관 26개 시스템
- 지자체 2팀 — 경기도남부지역 6개기관 34개 시스템



03 사업 일정(2/2)







정보시스템 클라우드 전환·통합 사례 및 성과발표

II 클라우드 전환 성과

01 클라우드 전환배경
02 클라우드 전환성과
03 운영 체감 성과

01 클라우드 전환 배경(A기관)

목적 및 필요성

보안 강화
- 설계 및 시스템 성능 최적화를 통한 장애 및 보안 대비

서비스 연속성
- 성능 향상 및 서비스를 고려한 이중화 구성
- 자원 최적화로 서비스 집중 시기에 탄력적 자원 증설 대응

성능향상
- 시스템 및 SW구성 설정 최적화 안정성 향상
- 공개SW 도입을 통한 기술지원

전환이슈

장비 노후화
- 정보 자원의 50% 이상이 노후화로 시스템 운영의 효율성이 저하
- 안정적인 대국민 서비스 제공에 어려움 발생

인력부족
- 기관의 전담인력 부족으로 보안 취약 발생
- 하드웨어 장애 발생시 즉각적인 장애 대응 어려움

라이선스
- 주요 서비스의 고가의 상용 라이선스SW(오라클, MS, MS-SQL등) 추가 구매의 부담 발생
- 윈도우 서버 업데이트 종료로 보안 취약점 노출

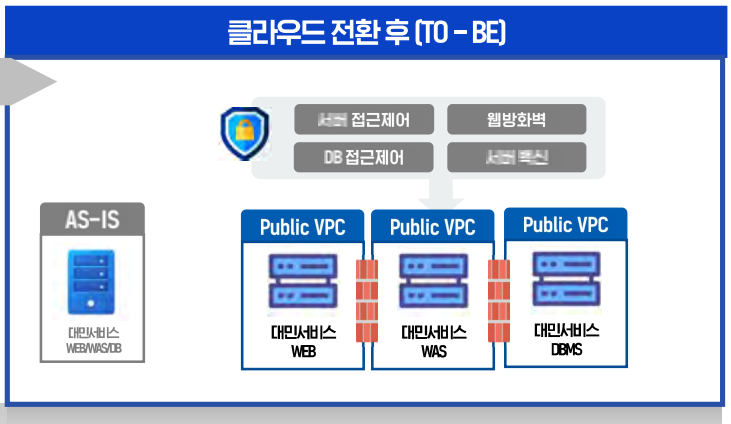
02 클라우드 전환 성과(1/10)

웹서비스 분리 구성 및 보안 서비스 일괄 적용으로 웹서비스 정보화 자원 표준화

클라우드 전환 전(AS-IS)

1. 물리 서버1대에 WEB, WAS, DB구성으로 보안 취약점 발생
2. 물리서버 하나에 여러 도메인 서버 구축 운영으로 장애시 장애 확산
3. 노후된 보안 장비 및 부족한 보안 SW 라이선스

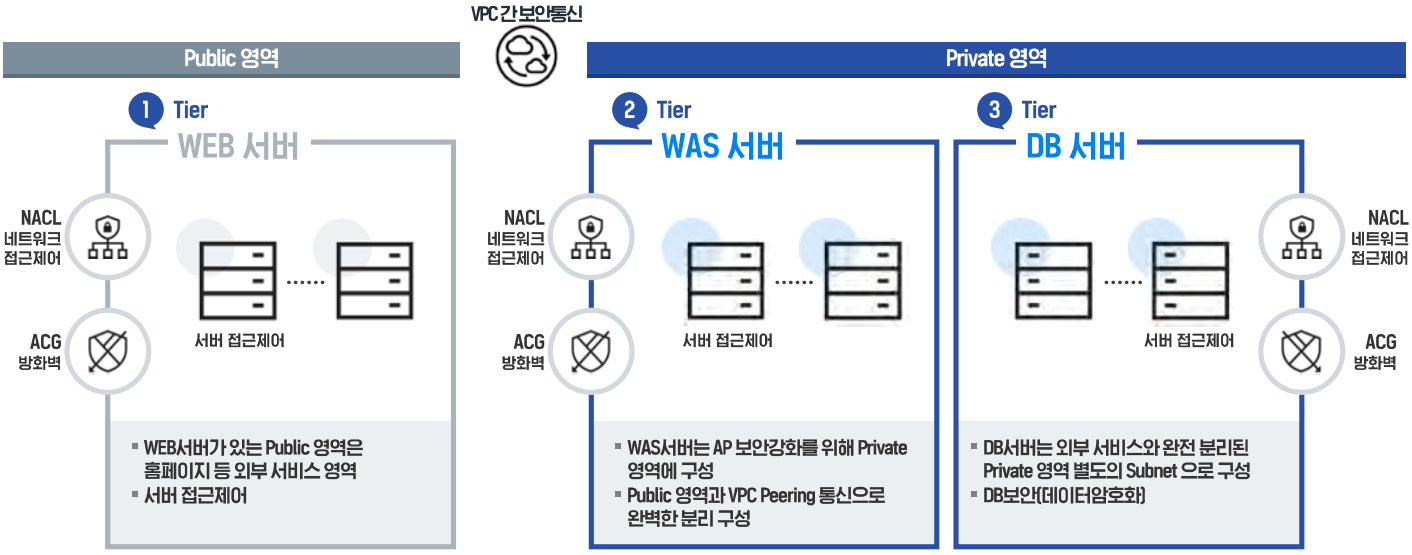
클라우드 전환 후 (TO - BE)



1. 보안 강화를 위한 3티어 WEB, WAS, DB서버 분리 구성 (보안 강화)
2. 물리서버에 구축된 여러 서비스를 분산 구축(안정성 Up)
3. 공통 보안서비스 필요 적용(보안성 UP)

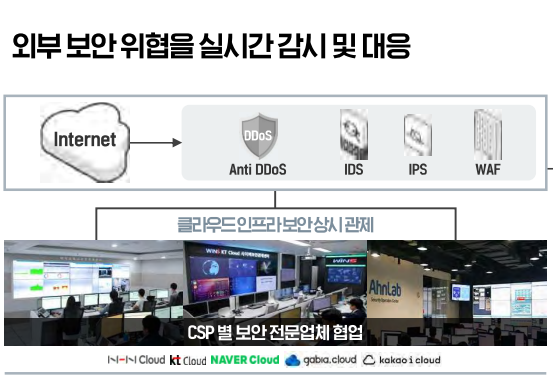
02 클라우드 전환 성과(2/10)

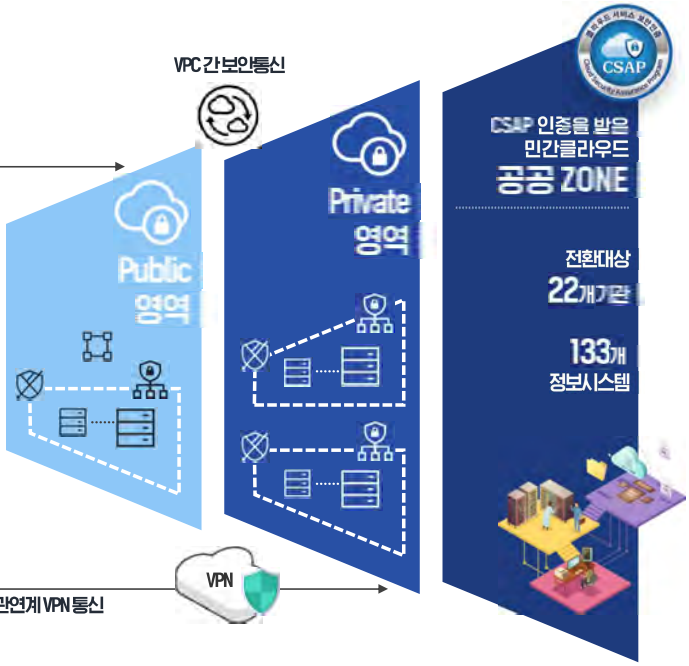
기본 3Tier 로 DB서버 분리 및 업무 영역별 접근제어, 방화벽으로 강력한 보안 환경 구성



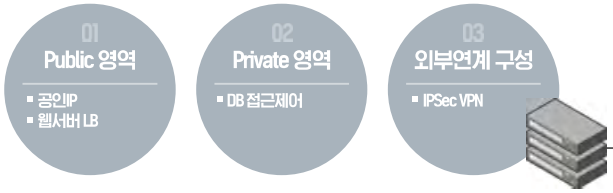
02 클라우드 전환 성과(3/10)

1 외부 보안 위협을 실시간 감시 및 대응





2 VPC의 강력한 보안 환경 구성



* LB(Load Balancer) : 웹 부하분산 / VPN(Virtual Private Network) : 가상 사설 네트워크

02 클라우드 전환 성과(4/10)

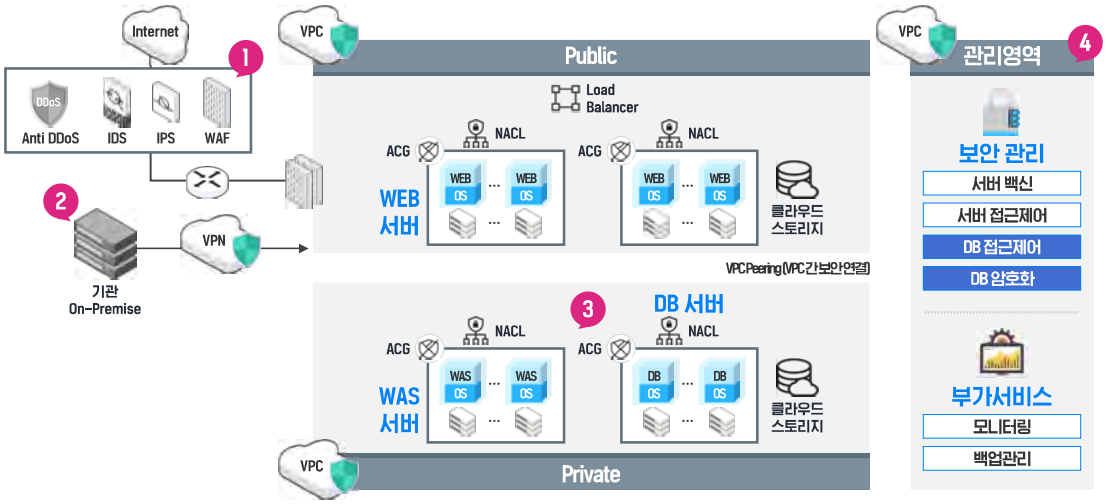
CSAP 인증된 클라우드 보안 ZONE 및 서비스, 관리 영역 완전 분리

1 보안강화
필수 보안서비스 적용

2 기관 운영현황과 동일한 서비스 구성
네트워크(LB, 공인IP), 연계(IPSec VPN 통신 연결)

3 3Tier 분리
WEB/WAS/DB서버 영역분리

4 서버백신, 접근제어, 암호화 적용
서버, DB 접근제어 및 암호화등 보안관리 구성

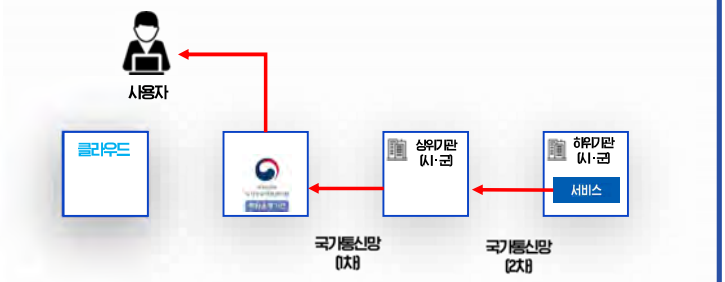


24시간x365일 모니터링 | 장애대응 및 관리 자동화 | 클라우드 전문인력 서비스 지원 | 직통전화 연결

02 클라우드 전환 성과(5/10)

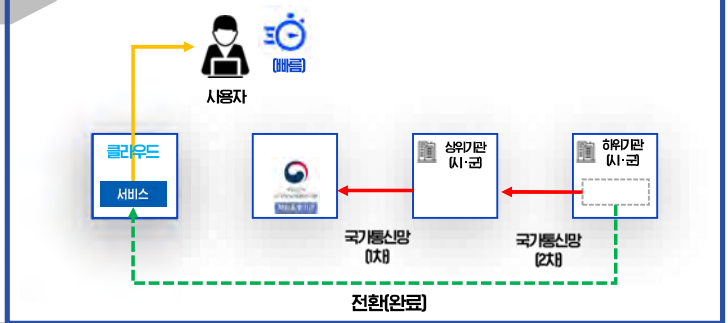
웹서비스 경로 단순화로 서비스 안정성 및 접근 속도 개선

클라우드 전환 전(AS-IS)



1. 전환대상 기관(상위 및 하위기관 포함)의 인터넷 서비스 이용 경로는 하위기관 -> 상위 기관-> 국가정보자원관리원 회선 이용
2. 웹서버의 경로는 기관 및 국가정보자원관리원을 거치면서 다수의 장애 발생 요인 보유(장애 리스크)
3. 다수 기관 경로로 서비스 지연(Latency)발생(지연)

클라우드 전환 후 (TO - BE)



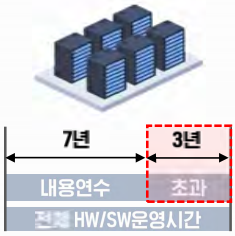
1. 전환 이후 인터넷 서비스 이용경로는 클라우드센터에서 사용자에게 바로 전달됨
2. 웹서비스 경로 단순화로 장애 발생요인 제거 (안정화)
3. 경로에 의한 서비스 지연(Latency)없음(매출)

02 클라우드 전환 성과(6/10)

국산 및 공개 SW 우선 전환 라이선스 비용 절감 및 정보자원 선진화

클라우드 전환 전(AS-IS)

정보시스템 노후화



외산 / 사용 소프트웨어

1. 내용연수가 지난 HW 및 SW는 신규 구매를 통해 정기적인 예산 집행 발생
2. 외산 및 상용SW 구매를 통한 고비용의 라이선스 비용 발생 및 높은 유지보수 요율에 따라 관리 비용 상승
   (오라클의경우 공급가의 22%를 매년 유지보수비 발생)

클라우드 전환 후 (TO - BE)

정보시스템 선진화

국산 / 공개 소프트웨어

1. 내용연수 제한없이 사용한 만큼의 리소스 이용료를 지불하며, 필요시 자원 리소스 사용/반환 쉬움 (비용 효율화)
2. 기존 고비용의 외산 및 상용SW를 국산 및 공개 SW로 전환 라이선스 및 유지보수 비용 절감 (비용 절감)

02 클라우드 전환 성과(7/10)

주요 개선 효과 비교

AS-IS (레거시 환경)

- 시스템 노후화로 인한 장애 요소 발생
- WEB/WAS 단일구성으로 보안 취약점 발생
- 상용 SW(오라클,Unix) 높은 유지보수 비용 지불
- 구버전SW 사용, 백신 미적용으로 취약점 발생
- 사용자 접근통제/감사 체계 개선 필요
- 인프라 운영 시스템 모니터링 알람 및 백업 체계 부재로 장애 시 초동조치 및 시스템 복구 체계 어려움

TO-BE (클라우드 환경)

- 클라우드 기술 적용으로 탄력적 자원 활용 및 SW 구매 비용 절감 가능
- 클라우드 전환 후 서버 분할 구성을 통한 보안 안정성 증대
- 최신SW 업그레이드, 보안패치를 통한 취약점 제거, 서버백신 적용, 사용자 접근통제 체계 적용으로 보안성 강화
- 전문 클라우드 MSP의 24×365 관제/운영관리로 장애예방 체계 강화 및 백업체계 구축으로 서비스 연속성 확보

NIA 한국지능정보사회진흥원

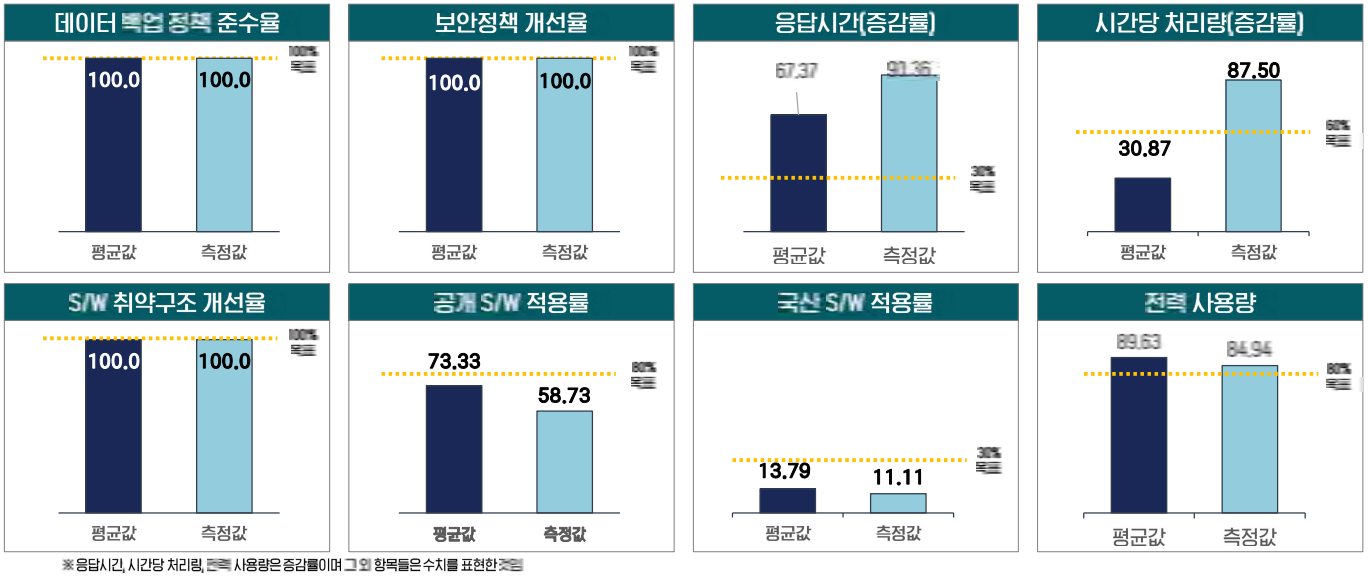
02 클라우드 전환 성과(8/10)

서버 백신, 접근제어, DB암호화, 백업, 모니터링 SW를 관리서버로 분리 구성

NIA 한국지능정보사회진흥원

02 클라우드 전환 성과(9/10)

A기관 세부 분석결과, 응답시간, 시간당 처리량은 전체 평균값보다 비교적 높게 측정되었으며, 특히 시간당 처리량은 평균(약 30%)보다 상당히 높은 결과(약 88%)를 나타냄



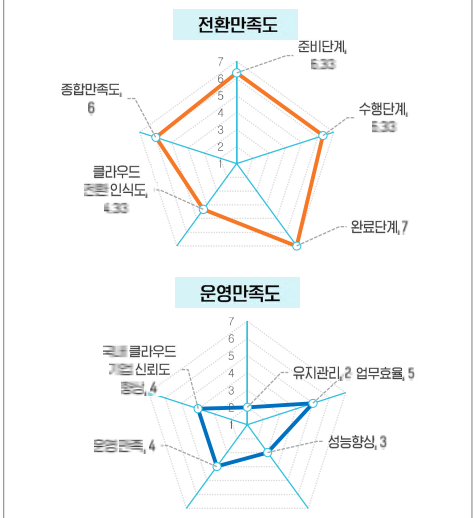
※응답시간, 시간당 처리량, 전력 사용량은 증감률이며 그외 항목들은 수치를 표현한것임

NIA 한국지능정보사회진흥원

02 클라우드 전환 성과(10/10)

A 기관 데이터 백업 정책 준수율, 보안정책 개선율, S/W 취약구조 개선율, 전력 사용량에서 성과목표 달성

만족도 조사 결과



전환 전/후 성과 비교

측정지표	응답	전환 전	전환 후	분석 결과	목표	달성
전환만족도	0	-	-		5점	
운영만족도	0	-	-		5점	
데이터 백업 정책 준수율	0	17.87점	100.00점	▲459.67% (▲82.13점)	100점	0
보안정책 개선율	0	25.63점	100.00점	▲290.24% (▲74.38점)	100점	0
응답시간	0				▼30% 이상	
시간당 처리량	0				▲50% 이상	
S/W 취약구조 개선율	0	67.57%	100.00%	▲32.43%	100%	0
공개 S/W 적용률	0	54.05%	58.73%	▲8.65%	▲80% 이상	X
국산 S/W 적용률	0	10.81%	11.11%	▲2.78%	▲30% 이상	X
전력 사용량	0	59,568kW	8,970kW	▼84.94%	▼80% 이상	0

▲ : 증가, ▼ : 절감

NIA 한국지능정보사회진흥원

03 운영 체감 성과

A 기관

대표 홈페이지 **긴급 자원 수요**에 대해 **단기간 내 자원 확장** 등 유연한 대응이 가능 했습니다.

정보시스템 **신규 또는 재구축 시 도입 절차 간소화로** 구축 기간 단축이 가능 했습니다.

유연성 | 기간 단축

B 기관

자체 진행중인 프로젝트에 있어 신규 서버 **자원 부족에 대한** 걱정이 없어서 좋습니다

온프레미스 대비 클라우드 전환 후 MSP에서 제공하는 **모니터링 및 통계 품질에 대해** 만족합니다.

확장성 | 운영품질

C 기관

MSP 점검을 통해 대표 홈페이지 하위 서비스 **선제적 문제 확인** 및 **사전 조치로** 장애를 예방 하였습니다.

검증된 안정화 버전 적용으로 기관 내부 운영 대비 보안이 강화되어 안심이 됩니다.

장애예방 | 보안강화

D 기관

기존 대비 여러 정보시스템을 **하나로 통합관리** 할 수 있어 편리 합니다.

최신화 장비와 **자원 활용도 증대**로 효율적인 운영이 가능합니다.

편의성 | 효율성

E 기관

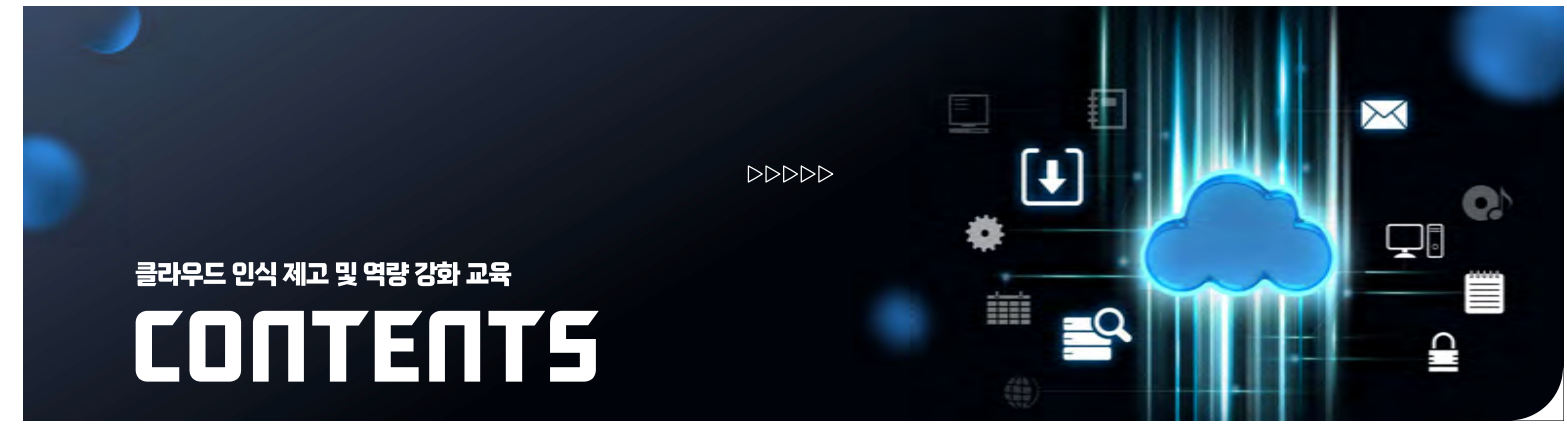
전환 후 시간이 경과함에 따른 **서버 노후화 및 교체 관련 쟁점이 없어져서** 좋습니다.

클라우드 **보안정책이 최신화 유지** 되어 안심이 됩니다.

용이성 | 보안강화

정보시스템 클라우드전환·통합 사례 및 성과발표(충청권)

㈜네이버클라우드
김성배 이사



클라우드 인식 제고 및 역량 강화 교육

CONTENTS

클라우드 인식 제고 및 역량 강화 교육

I 사업개요

01 사업 범위
02 사업 추진 일정

01 사업 범위

사업명	2022년 클라우드컴퓨팅서비스 활용모델 적용을 위한 지자체 시범 사업
사업기간	2022년 9월30일 ~ 2023년 2월 28일
사업목적	• 탄력적·안정적 서비스 제공을 위한 정보시스템 클라우드 전환 • 정보자원의 활용효율 극대화를 제공하는 클라우드 서비스
사업 범위	· A기관 및 2개 기관 총 123개 정보시스템

기관명	전환 시스템
정보통합센터	33
00시설공단	13
00도시교통공사	7
도시통합정보센터	70
합계	123

사업자	NAVER Cloud

NIA 한국지능정보사회진흥원

사업 추진 경과

클라우드 인식 제고 및 역량 강화 교육

II 전환결과

01 전환 결과
02 구축 및 전환 결과
03 시스템 구성도

01 전환 결과

AI 스마트시티로의 S기관 미래 목표 구현

창의적 도전을 통한 지역 발전

B 행복한 주민의 삶

E 공감과 참여의 공동체형성

S 최첨단 ICT 기반 구축

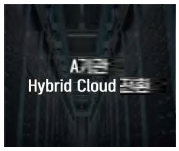
T 빛나는 미래도시 구현

주민의 행복하고 아름다운 삶 실현

스마트시티로의 S시 발전을 위한 첫걸음으로의 클라우드 전환

클라우드 기반 조성 → **인공지능 클라우드 기반 조성** → **스마트시티 OO**

혼합민간주도형 + Hybrid Cloud 구성



- 혼합민간주도형 및 Hybrid Cloud 구성으로 OO특별자치시만의 인공지능 스마트시티 서비스 기반 환경 업그레이드 및 확산을 위한 기반 인프라 구축 및 확보

시민의 삶의 질 향상을 위한 AI

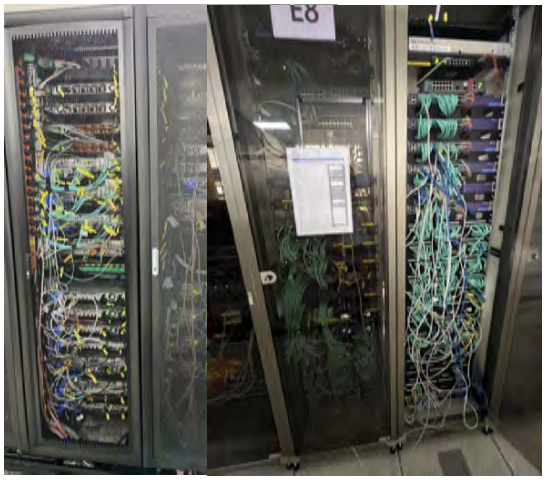
- 네이버 AI 교육지원 프로그램인 '소프트웨어야 놀자'에서 인공지능과 데이터 교육 실시하여 AI를 통한 OO시민 삶의 질 향상

스마트시티 OO의 완성

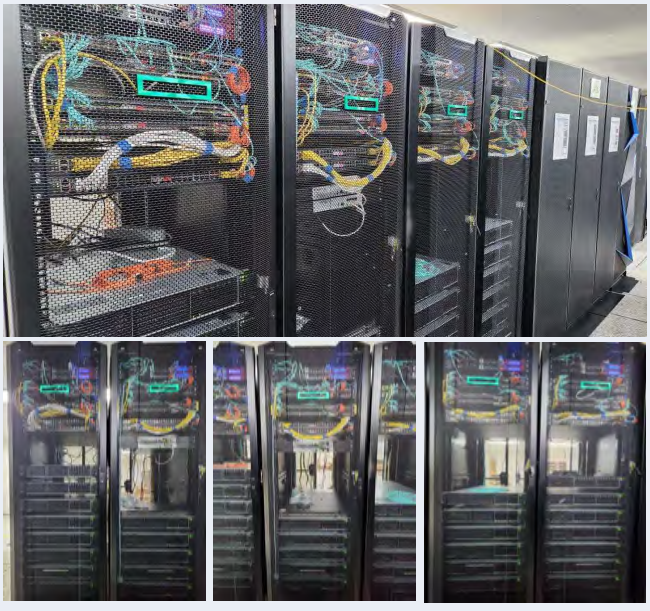
- 시민의 삶의 질 향상을 위한 인적 · 물적 기반 환 제공
- IT 신기술에 대한 학교부터 유니콘 기업까지의 교육 및 육성을 통한 지역 경제 활성
- 농지가 많은 OO시의 특성을 고려한 스마트팜 지원 및 구축

02 구축 및 전환 결과

클라우드 전환 전(AS-IS)

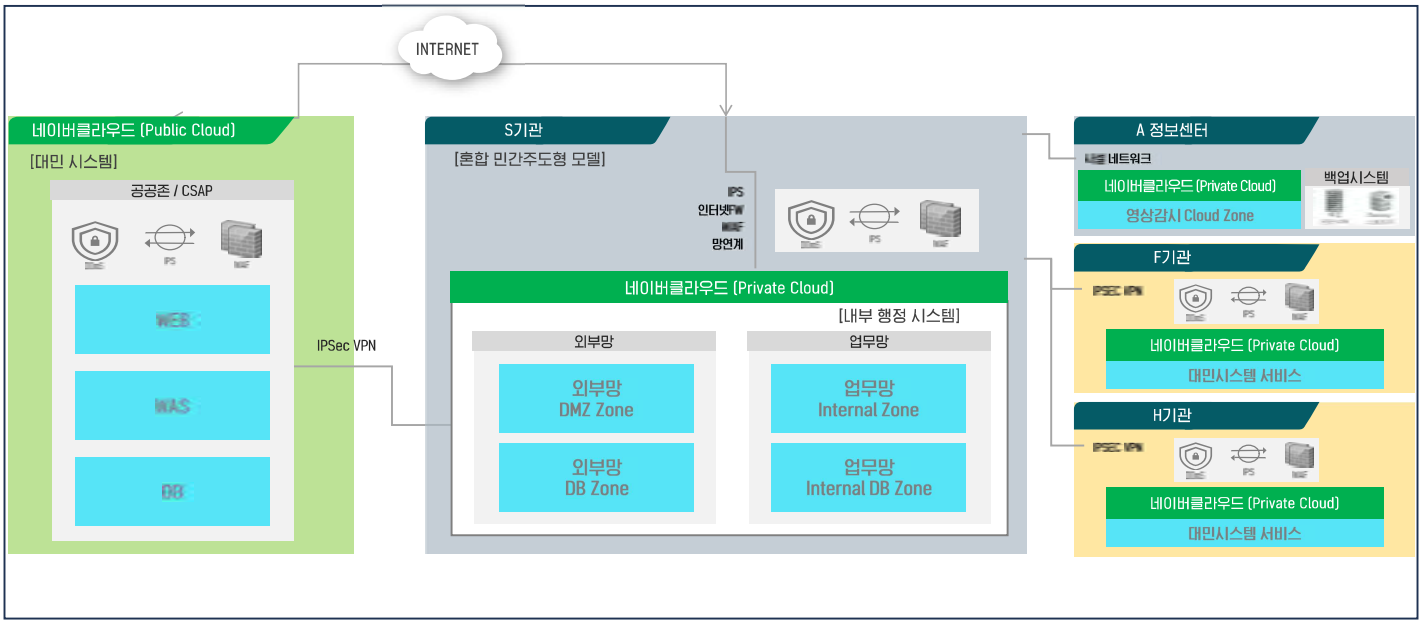


클라우드 전환 후(TO-BE)



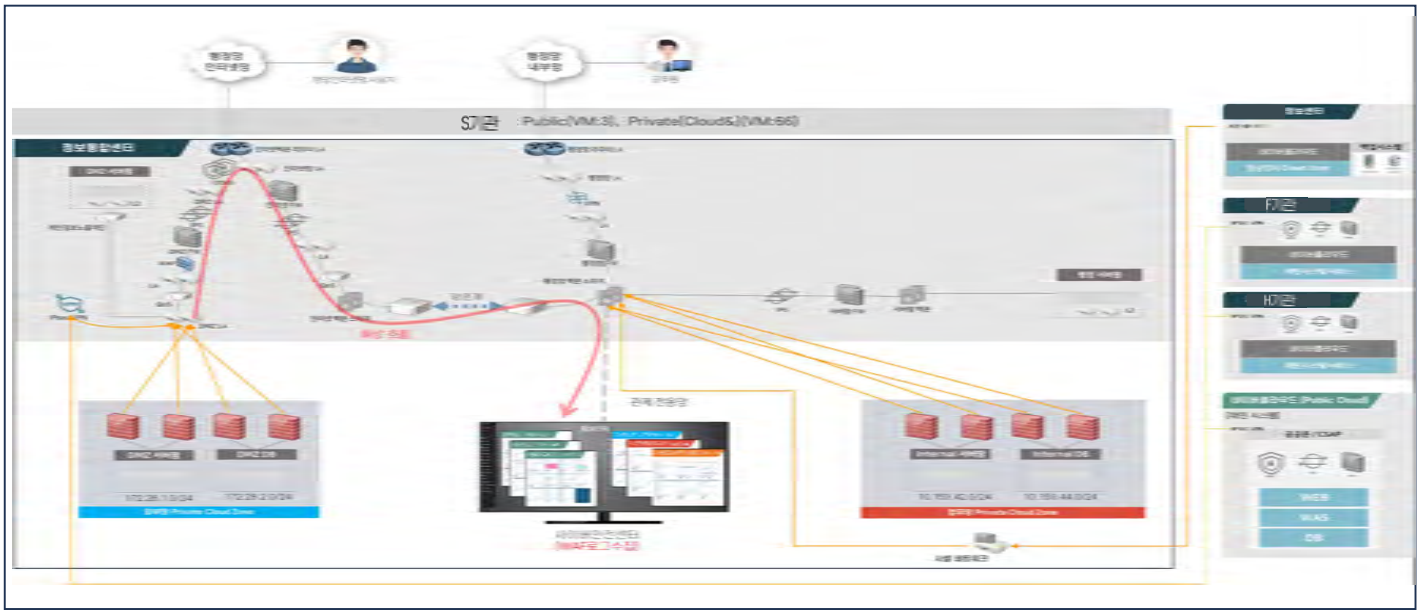
03 시스템 구성도(1/3)

전체 시스템 개념도



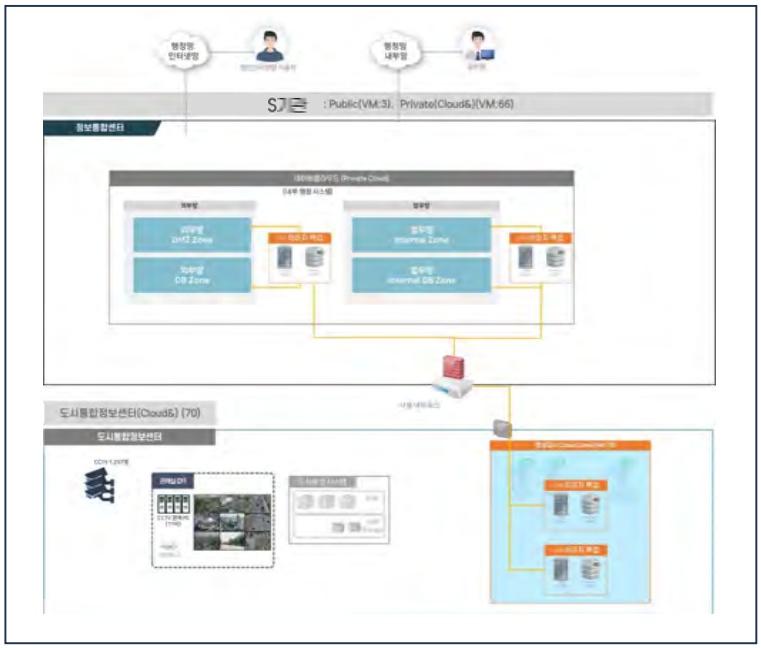
03 시스템 구성도(2/3)

관제 구성도



03 시스템 구성도(3/3)

DR 구성도



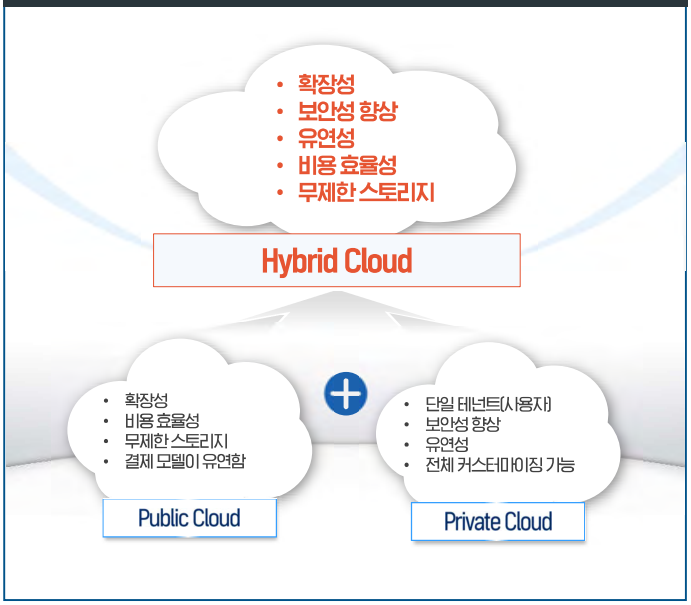
클라우드 인식 제고 및 역량 강화 교육

III 사업 성과

01 사업성과
02 성과 측정 통합 분석 결과
03 기타 추가 성과
04 전환 우수 사례

01 사업 성과

혼합민간주도형 + Hybrid Cloud



하이브리드 클라우드 장점

워크로드 마이그레이션	• 새로운 클라우드 환경에서 클라우드 네이티브 서비스에 액세스하면서 익숙한 툴과 프로세스를 사용하여 재편 없이 신속하게 워크로드를 마이그레이션함
애플리케이션 최적화촉진	• 하이브리드 클라우드를 통해 동일한 클라우드 플랫폼에서 가상 머신 기반 워크로드를 계속 운영하면서 마이크로 서비스 및 컨테이너 기반 애플리케이션을 생성 및 배포할 수 있음
확장성향상	• 익숙한 툴과 프로세스를 사용하면서 퍼블릭 클라우드 공급업체의 즉각적인 대응력과 확장성을 거의 실시간으로 활용할 수 있음
보안정책및 규정준수 강화	• 하이브리드 클라우드에서는 보안 정책이 각 애플리케이션에 연결되어 워크로드의 배포 및 관리 위치와 상관없이 일관된 적용이 가능함
보안성강화	• 하이브리드 클라우드는 중요한 데이터와 어플리케이션을 프라이빗 클라우드에 배치하여 보안성을 높일 수 있음.
유연성향상	• 다양한 애플리케이션 요구 사항과 디지털 비즈니스 이니셔티브가 있는 조직을 위해 하이브리드 클라우드는 워크로드와 데이터가 배포되는 위치와 시기에 대한 옵션을 제공하여 변화하는 요구에 대한 IT 반응을 가속화할 수 있게 함
복잡도감소	• 환경 전반에서 단일 운영 모델을 사용함으로써 IT는 운영을 간소화하여 자본 및 운영 비용의 조합을 최적화하고, 운영 및 보안 리스크를 줄이며, 사일로 및 기술 격차를 방지하면서 운영 효율성을 높일 수 있음
비용절감	• 하이브리드 클라우드는 비즈니스에 필요한 리소스를 선택적으로 구성할 수 있어 비용을 절감할 수 있음.

02 성과 측정 통합분석 결과

기관/ 항목(전환결과)	A 정보센터			F 기관			H 기관			B 통합센터		
	전환 전	전환 후	증감	전환 전	전환 후	증감	전환 전	전환 후	증감	전환 전	전환 후	증감
데이터 백업 정책 준수율	40.00점	100.00점	▲150% (▲60점)	0.00점	100.00점	▲100.00% (▲100점)	60.00점	100.00점	▲66.7% (▲40점)	40.00점	100.00점	▲150% (▲60점)
보안정책 개선율	90.00점	100.00점	▲11.1% (▲10.00점)	67.14점	100.00점	▲48.9% (▲32.86점)	77.69점	100.00점	▲28.7% (▲22.31점)	58.07점	100.00점	▲69.3% (▲41.93점)
응답시간	-	-	-	2.41초	2.07초	▲14.1% (▲0.34초)	0.86초	0.65초	▲24.7% (▲0.21초)	0.20초	0.15초	▲25.0% (▲0.05초)
시간당 처리량	-	-	-	18.69tps	19.61tps	▲4.9% (▲0.92tps)	12.63tps	12.54tps	▼0.67% (▼0.09tps)	403.30tps	429.84tps	▲6.6% (▲26.54tps)
S/W 취약구조 개선율	65.57%	0%	▲34.43%	35.42%	0.00%	▲64.58%	55.17%	0.0%	▲44.83%	58.3%	0.00%	▲42.08%
공개 S/W 적용률	-	-	-	89.58%	93.62%	▲4.5%	79.31%	86.96%	▲8.8%	65.00%	69.12%	▲6.3%
국산 S/W 적용률	-	-	-	2.08%	4.26%	▲104.3%	0.0%	2.17%	-	4.00%	17.65%	▲341.2%
전력 사용량	213,744	19,622	90.8%▼	84,096kW	6,728kW	▼92.0%	42,048kW	6,447kW	▼84.7%	140,160kW	19,622kW	▼86.0%
결과(100점)		70.0			85.0			77.5			85.0	

범 례	
	▲ 우수 : 목표치를 보유하였거나 전환 이후 개선되어 목표치를 달성함 ▲ 보통 : 전환 이후 개선되었으나 목표치는 달성하지 못함 ▶ 보존 : 전환 이전과 비교하여 전환 이후에 아무런 변화가 없을 때 ▼ 저하 : 전환 이전과 비교하여 성과가 저하됨

03 기타 추가 성과 – DR 구축(1/4)

추진배경 및 목적

카카오 데이터 센터 화재, Log4j 보안 취약점 사태, 랜섬웨어 등
정보 보안 및 서비스 연속성 관련 사회적 이슈 대두

정보보안 이슈 대두
2021.12.11

"컴퓨터 역사상 최악 취약점 돌연" 전세계 보안업계 화들짝 (연합뉴스)

판교 데이터센터 화재
2022.10.15

데이터센터 화재로 카카오·네이버 서비스 무더기 장애…복구 중 (연합뉴스)

고객정보 유출
2023.01.10

LG유플러스 해킹 공격으로 18만 명 고객 정보 유출 (MBC)

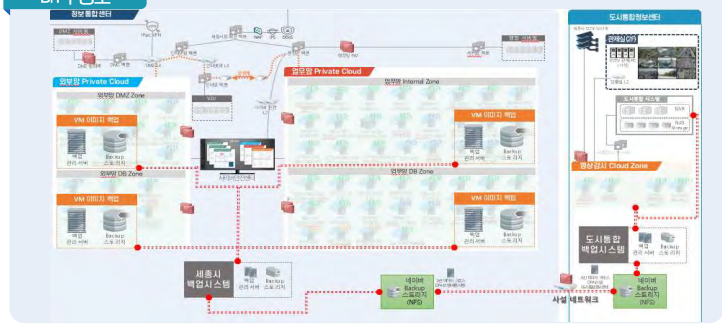
선제적 대응체계 마련 및 대처역량 강화 필요

DR구축 목표

S기관
전용 DR(Disaster Recovery) 체계 구축

- S기관 B 통합센터와 A 정보센터는 자기망(10G)으로 구성되어 있으며, 지리적으로도 구분되어 있음
- S기관 인프라 환경구성을 활용한 B통합센터와 A정보센터 간 소산 Cross DR 시스템 구축

DR 구성도



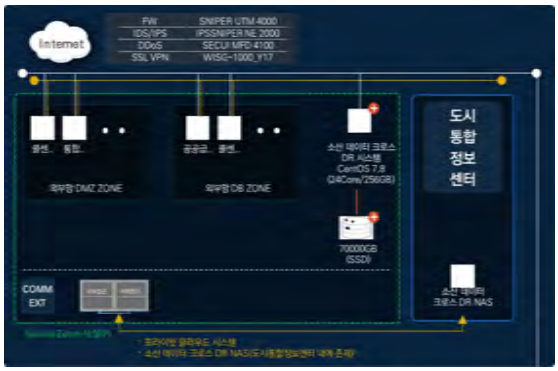
03 기타 추가 성과 – DR 구축(2/4)

기타 추가 성과 – DR 상세 구성도

A정보센터 → B통합센터

- A 정보센터 Private Cloud 시스템의 CCTV 마스터 데이터, 영상 데이터 등을 대상으로 백업 수행
- 백업 대상 데이터를 제외한 구성은 정보통합센터와 동일

B통합센터 → A정보센터



- B 통합센터 Private Cloud 시스템의 OS이미지, File 데이터, DBMS 데이터를 대상으로 백업 수행
- Private Cloud 시스템의 백업 데이터를 NFS, SAMBA를 통하여 데이터 저장
- 저장된 데이터는 도시통합정보센터 내의 자기망을 통하여 NAS에 저장
- 서비스 네트워크 망이 아닌 별도의 백업 망 구성으로 서비스 간섭 배제

03 기타 추가 성과 – DR 구축(3/4)

기타 추가 성과 – DR 기대효과

S기관 자가망을 활용한 기관 간 소산 데이터 Cross DR 시스템 구축을 통한

비용 절감 및 데이터 보안 & 업무 연속성 확보

1 데이터 보안 확보 및 업무 연속성 확보

- 데이터 손실, 다운타임 또는 사이버 공격에 신속 복구 가능
- 소산 백업을 통해 최근 발생한 화재 등의 물리적 위협에 대응
- 인터넷을 통한 자가망을 데이터 전송으로 외부 침입에 대한 위협이 감소
- 인터넷 연결이 끊어지더라도 데이터 백업을 수행 할 수 있기 때문에 데이터 손실을 예방
- 자가망은 인터넷 대역폭 제한에 영향을 받지 않으므로 백업 및 복원 작업이 더 빠르게 수행

2 보안성 만족하는 시스템 안정성 보장

- 보안성 검토 결과에 따른 대응방안 수립 및 조치를 통한 클라우드 전환 시스템에 대한 안전성 보장
- 보안 요구사항을 충족하는 클라우드 서비스 구성으로 관리적 보안, 물리적 보안 측면에서 보안 강화
- FW, IPS(IDS), DDoS, 서버백신, 접근제어 등 필수 보안서비스 적용 및 국정원 CC인증 제품 활용으로 보안성 강화

3 S기관 자가망 활용을 통한 비용 절감

- 자가망 활용을 통한 데이터 전송은 별도의 트래픽을 발생 시키지 않기 때문에 인터넷 대역폭 사용량과 네트워크 대역폭 비용을 줄일 수 있음
- 클라우드 전환 이후 유휴장비가 된 기존 인프라 구성 장비를 활용하여, 유휴자원 활용을 통한 비용 절감

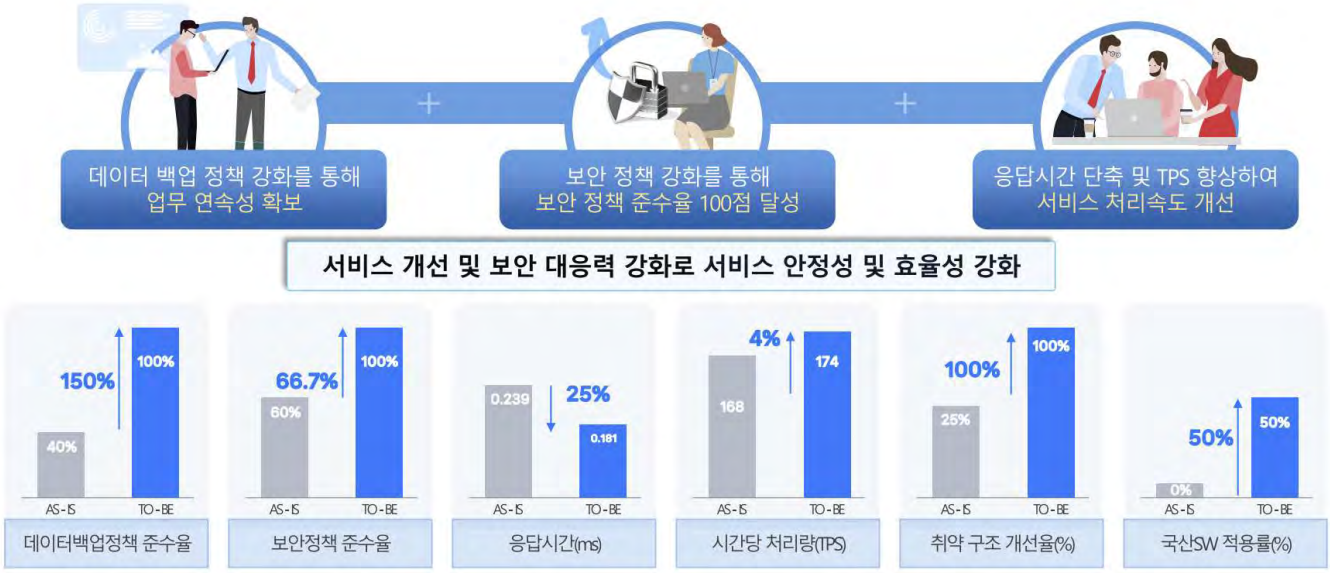
4 시스템S/W 취약구조 개선을 통한 보안 거버넌스 강화

- 해커 등 외부 공격에 대한 취약점을 줄이고, 시스템 보안을 강화, S/W 안정성·신뢰도 확보
- 개발생산성 향상 및 사용자 만족도 제고

03 기타 추가 성과 – Cloud 도입 효과(4/4)

04 전환 우수 사례(1/2)

전환 우수사례 – A시스템



04 전환 우수 사례(2/2)

부서 · 산하기관 담당자 인터뷰

기관 담당자 만족도 향상

서비스 안정성 향상

S기관 환경연구과

클라우드 전환을 통해 서비스 안정성이 향상되어 황사 · 미세먼지가 매우 심한 날에도 대응 가능하여 만족도가 높아졌습니다.

S기관 세원관리과

번호판영치 시스템을 전환하였고, 24시간 대응체계를 통해 이슈없이 서비스를 운영하고 있어 서비스 안정성이 올라가 만족합니다.

시스템부하감소

F기관 경영지원팀

클라우드 전환 후 시스템 부하가 감소된 것을 확인했습니다. 또한 서비스 알림을 통해 리스크를 사전 예방할 수 있어 만족합니다.

S기관 자원재난과

총 4개의 시스템을 클라우드로 전환하였고, 안정적인 운영 덕분에 시스템 부하가 많이 감소했습니다.

클라우드 전환을 통한 보안 강화

기관요구사항을 충족하는 보안표준 모델 제시

S기관 행정정보담당

클라우드 모델(하이브리드 클라우드)을 통해 기관의 보안요구사항이 충족되었고, 본 사업의 보안체계가 타 지자체에 표준 모델이 될 정도로 시스템 보안이 강화되었습니다.
하이브리드 클라우드 서비스 구성으로 관리적 보안, 물리적 보안 측면에서 보안이 강화되었다고 생각합니다.

DR을 통한 데이터 보안 확보

S기관 도시통합정보센터

기관 간 소산 데이터 Cross DR 시스템 구축을 통해 도시통합정보센터와 정보통합센터 간 백업을 수행하여 데이터 손실, 다운타임 또는 화재와 같은 물리적 재난에도 신속한 복구를 기대하고 있습니다. 인터넷 연결이 끊어지더라도 데이터 백업을 수행 할 수 있기 때문에 데이터 손실 예방이 될 거라 생각되어 만족합니다.

정보시스템 클라우드전환·통합 사례 및 성과발표(영남권)

kt cloud
한기수 이사

행정안전부 NIA 한국지능정보사회진흥원

정보시스템 클라우드전환·통합 사례 및 성과발표

CONTENTS

I kt cloud 소개

01 kt cloud's Strengths

NIA 한국지능정보사회진흥원

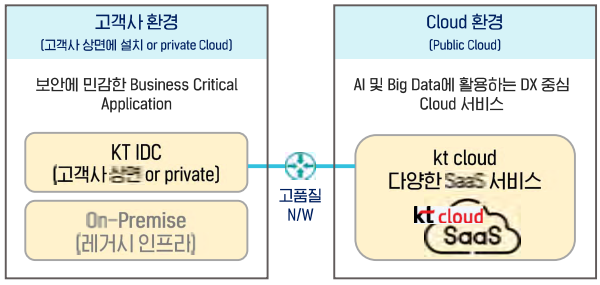
01 kt cloud's Strengths(1/4)

국내 유일 '클라우드-IDC-네트워크' 통합 보유

통합 보유의 강점을 활용하여 kt cloud IDC간의 연결성 및 타 CSP와의 편리한 확장성을 제공합니다

안정적인 Hybrid Cloud 환경 제공

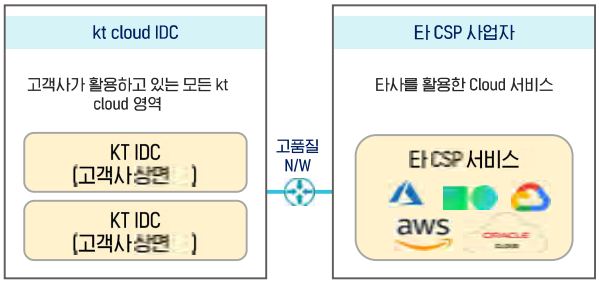
kt cloud가 보유한 네트워크 및 IDC를 활용한
Hybrid Cloud 최적화



➢ 고품질의 네트워크 + 국내 최초/최대 규모의 IDC를 활용하여 Network Latency가 최소화된 Hybrid Cloud 환경 지원

한 번의 연결로 Multi Connectivity 지원

kt cloud의 IDC 외에도
단 한번의 연결로 타 CSP로의 자유로운 확장성



➢ 하나의 상품을 이용하여 타사 Cloud로의 자유로운 확장 지원 ex> Connect Hub, HCX, 전용회선/VPN

01 kt cloud's Strengths(2/4)

고객 맞춤 서비스

One & Only · 고객 맞춤 · Trust · 최초 인증

기존 상품 기반으로 반영 가능한 고객 요구사항을 수용하여 고객 맞춤형 서비스를 제공합니다

고객 맞춤형 상품 지원

고객사 비즈니스 환경에 맞추어
재구성한 상품 제공 가능

서비스형 및 구축형 모두 제공

SaaS 형태의 서비스형 외에도
고객사 상면에 설치되는 구축형 상품 제공

01 kt cloud's Strengths(3/4)

핵심적인 공공 레퍼런스 보유

One & Only · 고객 맞춤 · Trust · 최초 인증

안정성 및 보안성 모두 중요시하는 국가 주요 서비스는 kt cloud를 사용하고 있습니다

국가 주요 서비스와 함께하는 kt cloud

전국적으로 활용하는 국가 주요 서비스를
kt cloud 기반으로 운영 중

제주특별자치도 — Cloud 활용모델기반한 Cloud 전환 사업
제주도청외 6개 기관 대상 114개 시스템 Cloud전환 행안부 사업

소상공인시장진흥공단 — 손실보상시스템
전국 소상 공인 대상으로 안정적인 18만명의 동시접속자 수용

행안부 — 주관 공공전환사업
특허청 산하 7개 기관 Legacy to Cloud 공공전환 사업으로 KT 대규모 유치

우정사업본부 — VPC 서비스형 VDI 제공
전국 대상 31,000여명의 사용자 기반 VDI 서비스 제공

질병관리청 COOV — 코로나19 검사의뢰서
코로나 시기 전국민 활용 시 갑작스러운 데이터 급증에 대비할 수 있는 클라우드 제공

정보통신산업진흥원 nipa — 인공지능 고성능 컴퓨팅 자원 임차 사업
400개 이상의 기업 지원, 누적 120PFLOPS/1년 고성능 연산자원 제공

국내 다수 공공 레퍼런스

핵심 공공 시스템 및 다양한 서비스에 도입한
다양한 Reference 보유

제주특별자치도 · 서울특별시 · 국회도서관 · 국방전산정보원 · 소상공인시장진흥공단 · 질병관리청 · 우정사업본부 · 경기도일자리재단 · nipa · NIA 한국지능정보사회진흥원 · TS 한국교통안전공단 · Kdata 한국데이터산업진흥원 · 경상북도 GYEONGSANGBUK-DO · iPET · 청도군 CHEONGDO-GUN · 청송군 · 경주시 GYEONG JU

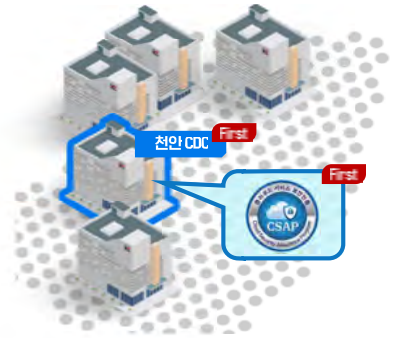
01 kt cloud's Strengths(4/4)

기준에 최적화된 보안 수준

다양한 인증을 통해 높은 안정성과 신뢰성을 보장합니다

One & Only 고객 맞춤 Trust 최초 인증

국내 최초 공공 CSAP 인증 획득



- 국내 최초 2015년 공공기관 전용 클라우드 구축 이후 국내 최초 2016년 CSAP 인증 획득

금융 클라우드 보안 요건 만족

- 기본보호조치 109개 항목 All 충족
- 금융부문 추가보호조치 32개 항목 All 충족

국내외 다양한 보안 인증 취득

정보시스템 클라우드전환·통합 사례 및 성과발표

II 공공 클라우드 전환 성공 사례

01 사업 개요
02 사업 경과
03 사업 특징
04 사업 성과 요약
05 향후 방안

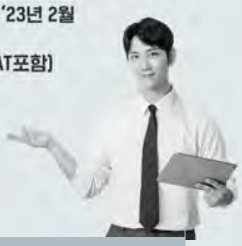
01 사업 개요

'22년도 클라우드컴퓨팅서비스 활용모델 적용을 위한 지자체 시범사업 **114개의 정보시스템의 클라우드 전환/설계/운영 및 성과관리를 완료**하였습니다

사업 개요

J기관에 최적화된 클라우드 활용모델 시범 사업

사업명	2022년 클라우드 컴퓨팅서비스 활용모델 적용을 위한 지자체 시범사업
사업기간	'22년 9월 ~ '23년 2월
사업비	86.4억원 (VAT포함)
주관사	kt cloud



사업착수 ('22.09) — 사업준공 ('23.02)

전환설계 기간 (6개월) | 운영 기간 (12개월)

사업 범위

J기관 포함 7개 기관, 114개 정보시스템 Cloud 전환

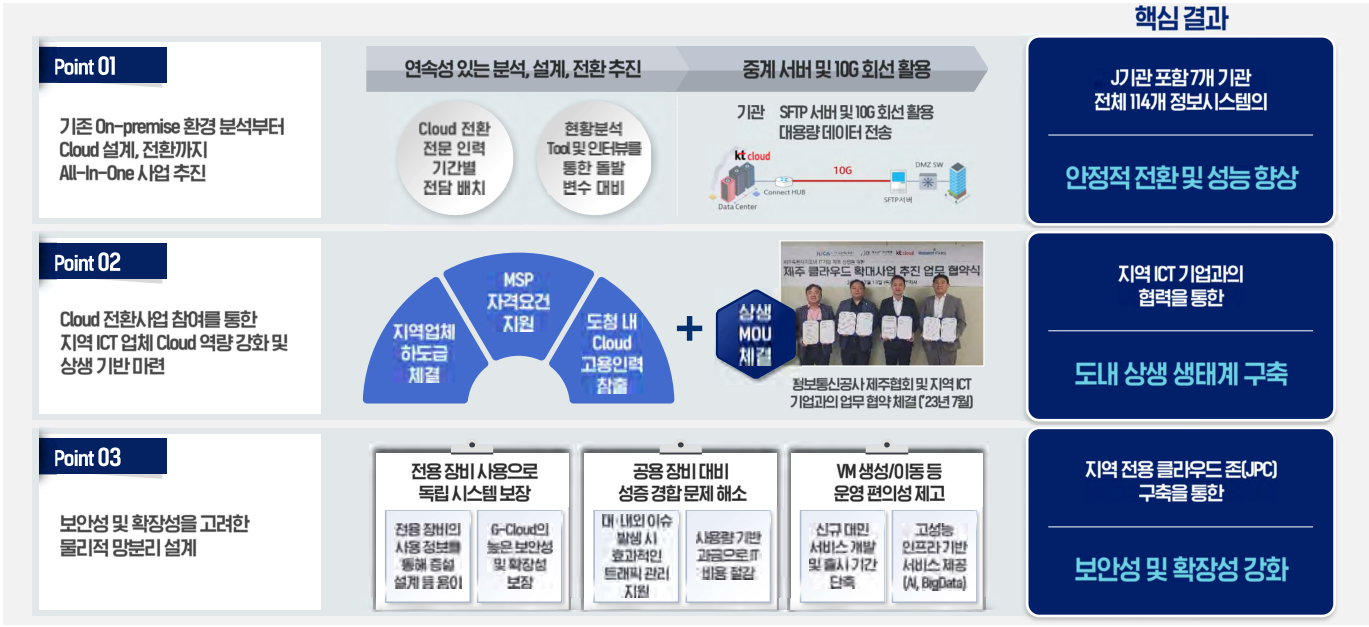
1	설계	J기관 최적의 인프라 설계	• 기관 전용 클라우드 존(JPC) 구축 • 전용 컴퓨팅 자원 할당, 국정원 보안관제 연동
2	전환	In-time 전환 수행	• 7개 기관, 114개 시스템 적기 전환 완료
3	운영	전문 인력을 통한 고품질 운영 서비스 제공	• 이용지원 및 SLA 계약 체결 • 24 X 365 매니지드 서비스 제공 • J기관 내 클라우드 전문 상주인력 지원
4	성과관리	Cloud 전환 성과 분석	• Cloud 전환에 대한 정량/정성적 효과 분석 • 이용자 만족도 조사, 우수사례 발굴 등 포함

02 사업 경과

본 사업은 설계/전환 통합 발주 사업으로, 매월 정기 간담회 등 적극적인 소통을 기반으로 **현황분석 > 설계 > 전환 > 최적화/안정화 단계를 적기 수행** 하였습니다.

03 사업 특징

지역 내 취약한 IT인프라 환경을 획기적으로 개선할 뿐만 아니라 도내 **상생 생태계 구축**까지 고려하였습니다.



03 사업 특징 – Cloud 전환 최종 구성도

kt cloud는 CSAP 인증 공공 클라우드 존 내에 물리적으로 완전히 분리된 제주 전용 클라우드 존을 구성하여 클라우드의 장점과 지역만을 위한 **안정성까지 완벽히 보장** 하였습니다.

NIA 한국지능정보사회진흥원

04 사업 성과 요약

7개 기관 114개 시스템의 전환으로 데이터 백업 정책 준수율, 보안정책 개선율, S/W 취약구조 개선율 등 **대부분의 항목이 큰 폭으로 개선**되었습니다.

전환 전/후 성과 비교

측정지표		응답	전환 전	전환 후	개선결과	
전환만족도		0			5.3점	
데이터 백업 정책 준수율		0	60.4%	100.0%	▲65.7% (▲39.6%p)	향상
보안정책 개선율		0	47.9%	100.0%	▲65.7% (▲39.6%p)	향상
응답시간		0	0.87초	0.28초	▼67.7% (▼0.59초)	단축
시간당 처리량		0	56.6tps	100.6tps	▲77.7% (▲44.0tps)	향상
S/W 취약구조 개선율		0	60.3%	0.0%	▼100.0%	개선
공개 S/W 적용률		0	65.0%	78.8%	▲21.1%	향상
국산 S/W 적용률		0	19.9%	15.8%	▼20.5%	감소
전력 사용량		0	693,372kW	91,945kW	▼86.7%	절감
운영 비용 절감		0	15,194,417천원	10,196,067천원	▼32.9%	절감
정보자원 절감률	CPU	0	8.09코어	5.85코어	▼27.7%	절감
	메모리	0	28.06GB	17.02GB	▼39.3%	절감

NIA 한국지능정보사회진흥원

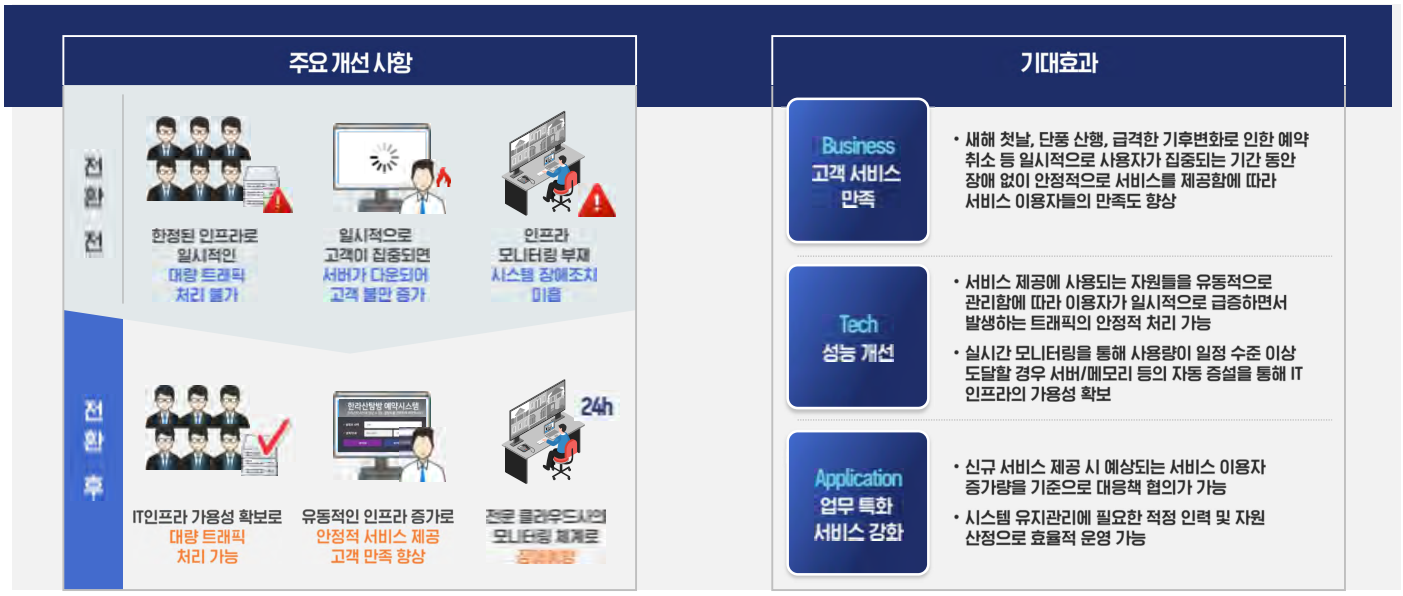
04 사업 성과 요약 - 관리 & 안정성 개선

J기관 내 여러 시스템의 서비스 가용성과 동시접속 가능량을 대폭 향상 시켜, 장애 제로화를 달성했습니다.

※기관 클라우드 전환 전/후 1년간 운영 데이터 참고

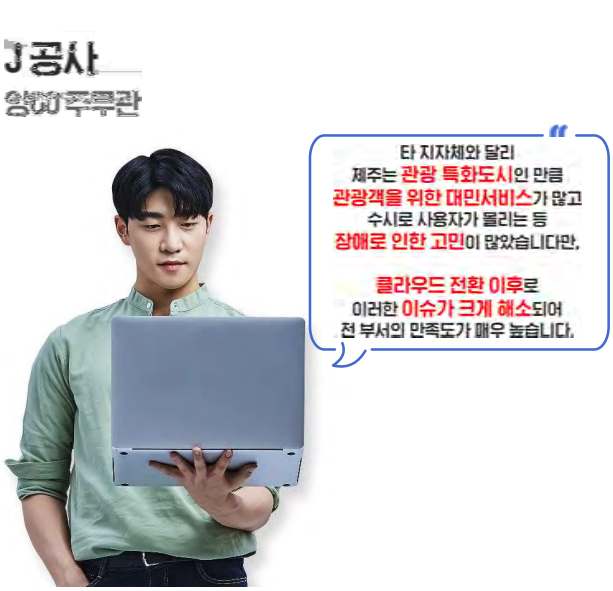
04 사업 성과 요약 - 만족도 향상 (1)

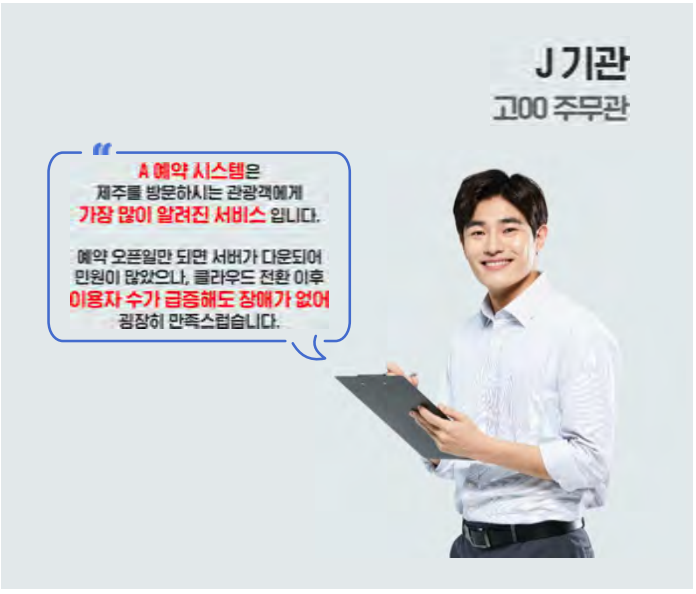
한정된 인프라로 기존 이용 고객의 불만이 많았으나 클라우드 전환을 통해 고객에게 안정적으로 예약서비스를 제공하고 있습니다.



04 사업 성과 요약 - 만족도 향상 (2)

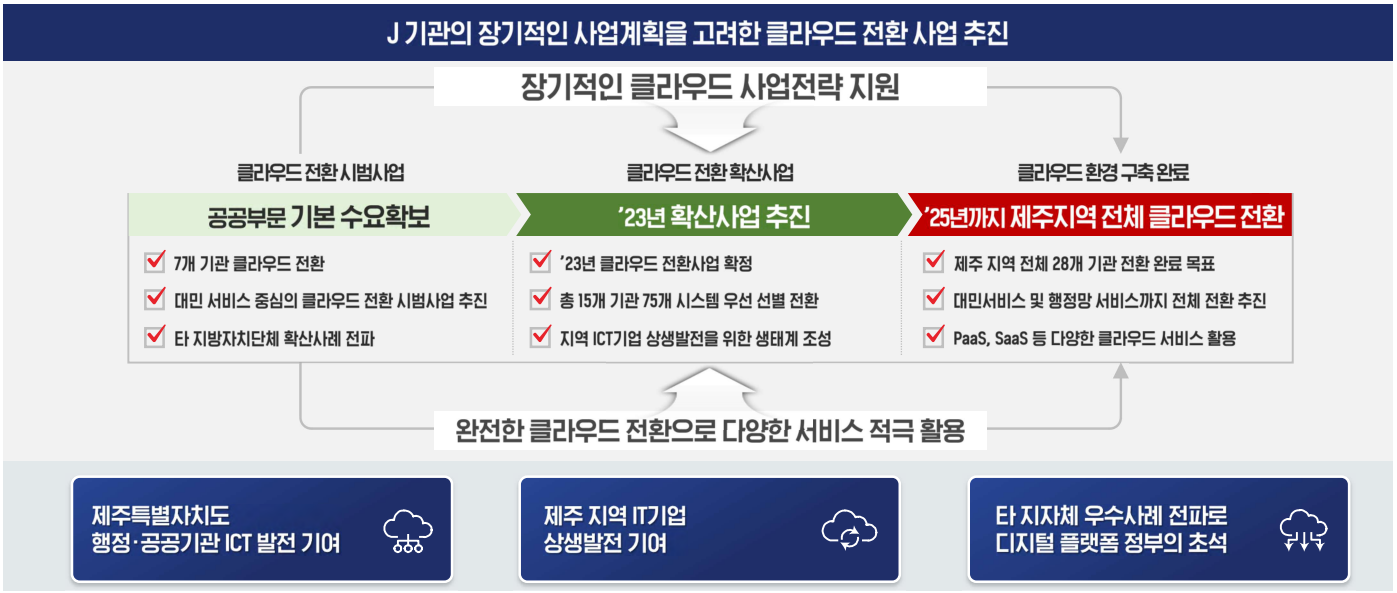
실 전환 대상 기관 실무 인터뷰를 실시하여 높은 서비스 만족도를 확인할 수 있었습니다.





05 향후 방안

성공적인 제주사업을 초석으로 지자체 자체발주사업인 2차 사업을 확정함으로써, 대한민국 공공분야 ICT발전에 기여하였습니다.



정보시스템 클라우드전환·통합 사례 및 성과발표

III 공공 클라우드 Trend

01 Cloud Native 란?
02 Cloud기반 SAP 소개
03 JP Jone이란?
04 kt cloud 온라인 교육 (Basic)

01 Cloud Native

kt cloud K2P 상품을 통해 보다 가볍고, 신속한 개발/배포가 가능하며 효과적인 장애 대응이 특징

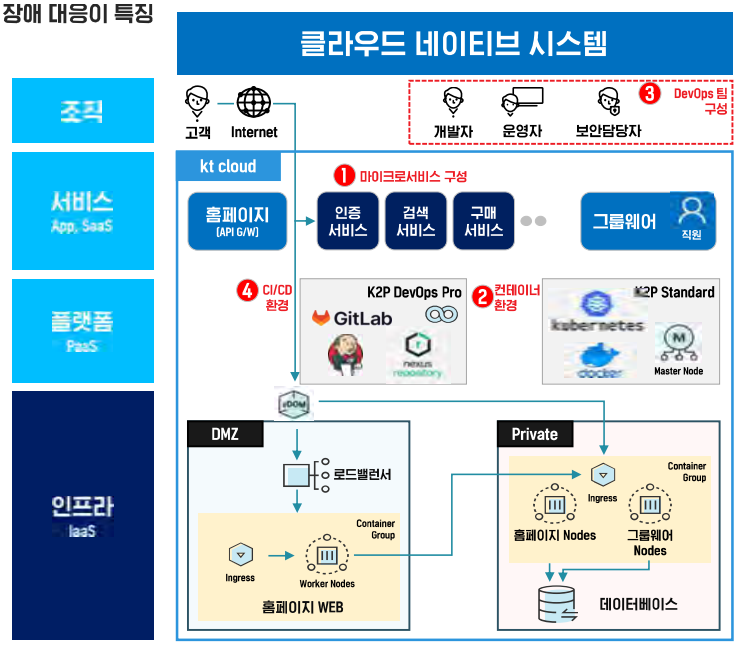
Cloud Native 적용을 위한 4가지 구성 요소로 구성하여 조직, 서비스, 플랫폼 관점에서의 변화 주도

1 마이크로서비스 (MSA)
대규모 애플리케이션을 각각 담당 영역을 가진 소규모의 독립적인 구성요소로 분리하여 아키텍처 구성

2 컨테이너 (Docker)
애플리케이션 실행에 필요한 모든 요소를 패키징하고, 공유된 운영체제(OS)에서 실행하여 VM에 비해 가볍게 구동

3 데브옵스 (DevOps)
애플리케이션을 보다 빠르게 개발 및 배포하는 것을 목표로 개발팀과 운영팀 간 단일한 협업 프로세스를 구성하는 방법론

4 CI/CD (Continuous Integration Continuous Delivery)
지속적인 통합, 지속적인 서비스 제공, 지속적인 배포를 통해 애플리케이션 개발 단계를 자동화 하여 더욱 빠르게 빌드/배포



향후 사업 추진

* '23 행안부 - NIA 활용모델 사업 모델
- 네이티브 1단계 (컨테이너 + SaaS)
- 네이티브 2단계 (MSA +컨테이너 +SaaS)

"23년도
- 행안부 - NIA 클라우드 컴퓨팅 활용모델 사업 2,3번 모델 추진 중

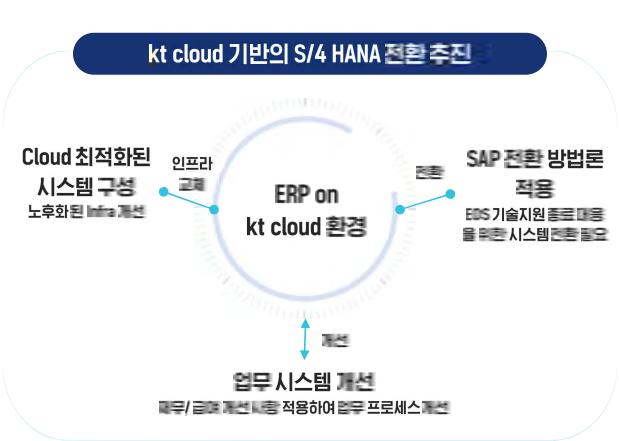
"24년도
- '24 ~ 30년 행안부 - NIA 네이티브 전환 사업 추진 예정

※ 23년 이후 공공 클라우드 전환 사업 필수 키워드 'Cloud Native'

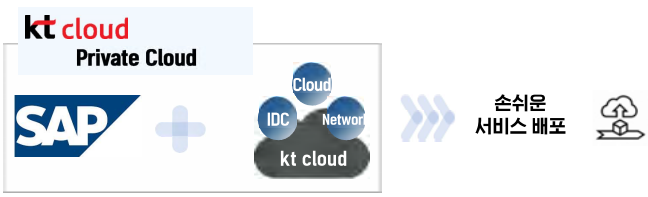
02 kt cloud SAP ERP

kt cloud on VM 구축부터 SAP Korea와 협업을 통한 kt cloud만의 SAP ERP 상품 개시

kt cloud Vmware 존을 활용 및 구축하여 고객사 ERP 시스템을 마이그레이션을 성공적으로 수행



SAP KOREA과 협업을 통한, kt cloud Private Cloud 형태의 상품 개시 확정



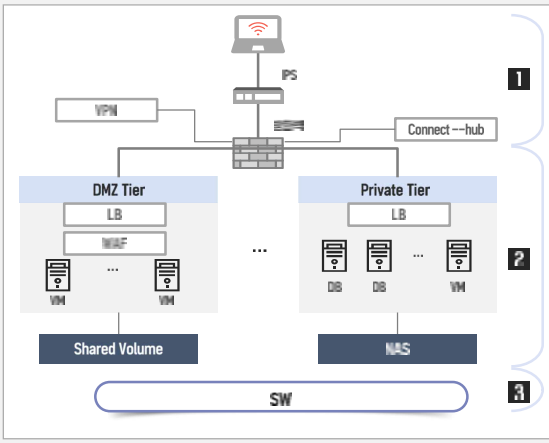
향후 ERP 추진 계획

"23년도
- 강원랜드 (추진 중)
- 한국농어촌공사 (추진 중)

"24년도
- JDC (제주 국제 자유 도시 개발 센터)

03 G-Cloud 구조 및 특징 (D1 Zone)

G-Cloud D1



- IPS, 방화벽 등의 네트워크 보안 장치 및 서비스 제공 (CC인증 받은 보안장비 적용)
- 방화벽을 중심으로 여러 Tier 네트워크 구성을 통해 다양한 Architecture 수용
- 2021년 11월 기존 G-Cloud에서 G-Cloud D1 상품으로 업그레이드 완료

공공 규제에 맞추어 구성한 공공 전용 Zone으로,
대민/대고객 서비스 및 공공기관 내부업무 시스템에 적용

특장점

1 확장성 있는 클라우드 인프라 구조
[기존적으로 DMZ Tier 및 Private Tier 제공]
[고객 니즈에 따라 여러 Tier 네트워크를 추가 가능]
[방화벽을 통해 Tier 네트워크 간 라우팅 및 ACL 적용]

2 고성능 컴퓨팅 제공
[최대 스펙 : 64vcore/256GB VM]
[NVIDIA Tesla A100 기반의 GPU 서버 제공]

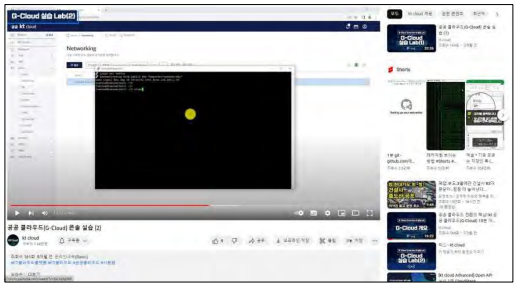
3 제공 OS
[CentOS 7.6,/7.8/7.9, Ubuntu 18.04, Windows 2019]
[MS-SQL 2016/2019] [RHEL8 가능 (BYOL)]

보안 매니지드 서비스 제공

보안 모니터링	보안 장치 운영
보안 대응, 사고분석	월간 보안 보고서

04 kt cloud 온라인 교육

난이도	No.	강좌명(패키지명)	학습시간	강의명	URL
Basic	1	Cloud 이해	50분	1. Cloud 중요성	https://youtu.be/2SxzY6q0eIQ
				2. Cloud 제공방식	https://youtu.be/aK2PubXhE5o
				3. Cloud 사용이유	https://youtu.be/VoYbZ0x24zo
	2	kt cloud Overview	48분	1. kt cloud 선택의 이유(Why&Whc)	https://youtu.be/N2AQSv6Rfy0
				2. kt cloud 개요(What)	https://youtu.be/7lv0mxfJnh0
	3	kt cloud 서비스 실습 Lab	80분	1. kt cloud 고객 시스템환경	https://youtu.be/kcnFet9NIvY
				2. kt cloud Server 생성 기초 실습	https://youtu.be/PJ3xkpuJOqw
				3. Load Balancer 서동 실습	https://youtu.be/c6adm_daeRM
				4. kt cloud Management 상품 실습	https://youtu.be/nVBE6ZDfk5k
	4	kt cloud Container Essential	40분	1. Docker 기본 개념의 이해	https://youtu.be/ekoj7EGIV1E
				2. Kubernetes 기본 개념의 이해	https://youtu.be/AaPcTszeF1Y
				3. EPC Container 상품 소개	https://youtu.be/TarwYDtvggw
				4. EPC DevOps Suite 상품 소개	https://youtu.be/R5d82OYj5fg
	5	Cloud 보안의 이해	34분	1. Cloud 서비스 보호-NW 보안	https://youtu.be/QZIyMAES-hE
				2. Cloud 서비스 보호-서버 보안	https://youtu.be/Yix9fgQ3S5k
				3. Cloud 서비스 접근 보안-접속 제어	https://youtu.be/KcfA6iT19lM
	6	Cloud Network의 이해	52분	1. Network 개념 및 장비 역할	https://youtu.be/sijwmDmxBH4
				2. kt cloud Zone Architecture	https://youtu.be/mMXzbvZGm8w
				3. kt cloud Network 구조 소개	https://youtu.be/QjhGmYzrd9g
	7	kt cloud Container Essential	42분	1. Container 기본 개념의 이해	https://youtu.be/hpFzsZTEPos
				2. Kubernetes 기본 개념의 이해	https://youtu.be/OhwZuDpGPWU
				3. Container 상품 소개	https://youtu.be/uvUxAUUXSmc
	8	G-Cloud Overview & 실습 Lab	62분	1. G-Cloud 개요	https://youtu.be/wtK5B1i8nYI
				2. G-Cloud 실습 Lab(1)	https://youtu.be/N8aY4rYCeRU
				3. G-Cloud 실습 Lab(2)	https://youtu.be/4VlRVaXHKI0



정보시스템 클라우드전환·통합 사례 및 성과발표(호남권)

삼성SDS

권조훈 프로

행정안전부 NIA 한국지능정보사회진흥원

정보시스템 클라우드전환·통합 사례 및 성과발표

CONTENTS

정보시스템 클라우드전환·통합 사례 및 성과발표

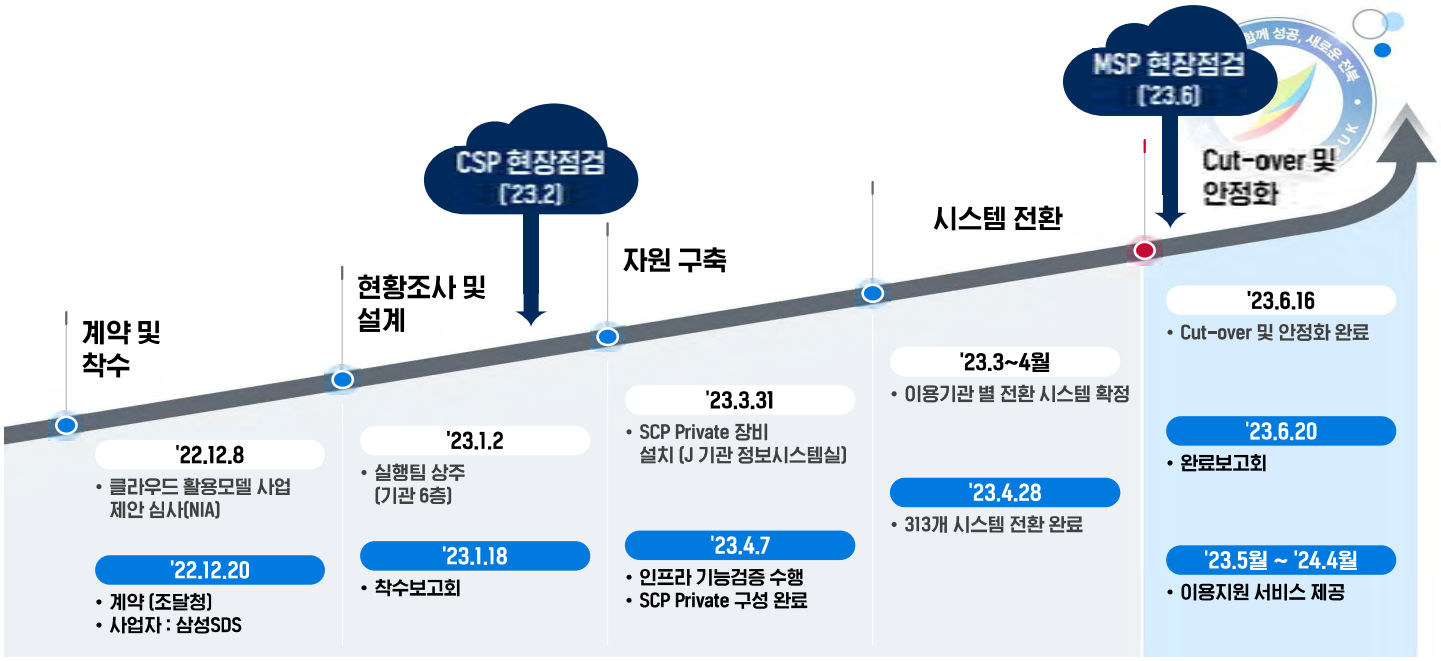
I 사업 개요

01 사업 개요
02 추진 경과
03 활용 모델

01 사업 개요

사업 개요	
사업 명	'22년 지자체 클라우드컴퓨팅서비스 활용모델 시범사업
사업 예산	약 151억원 (VAT 포함)
사업 기간	2022. 12. 20 ~ 2023. 04. 28 (약 4개월)
사업 추진 조직	• 주관기관: 한국지능정보사회진흥원 • 사 업 자: 삼성SDS
사업 내용	• 정보시스템 현황 분석 및 클라우드 전환 계획 수립 • 클라우드 자원 구성 및 전환 • 클라우드 매니지드 서비스 제공 • 기술 및 운영 지원, 성과관리 등
전환 대상	• J 기관 및 14개 시군 (259개 정보시스템)

02 추진 경과



03 활용 모델

J 기관
"지역맞춤 민간협력형" 모델 개발 및 적용

행정안전부
클라우드컴퓨팅서비스 활용모델

"민간 주도형" 기반
+
기존 전산실과 설비 재활용
사업기간 단축 및 예산 절감된
"민간 위탁형" 적용
+
강력한 보안 및 유연한 확장성 갖춘
"민간 이용형(CSAP)" 활용

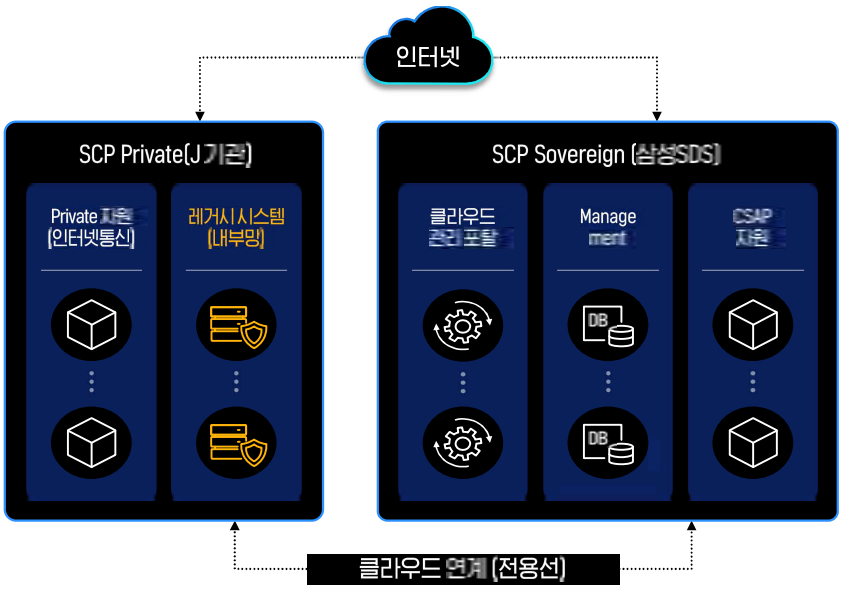
활용 모델	토지/건물	설비/인프라	서비스 운영	서비스 이용
민간 위탁형	공공 (민간인프라 도입)		민간	단일
다수 민간 위탁형				다수
혼합 민간 위탁형				혼합
민간 주도형	공공	민간 (신규)		단일
다수 민간 주도형				다수
혼합 민간 주도형				혼합
민간 구축형	민간 (신규, 이용)			단일
다수 민간 구축형				다수
혼합 민간 구축형				혼합
민관 공유형 (Hybrid)		민간 (이용)		혼합
민간 이용형 (CSAP)				단일
다수 민간 이용형 (Multi)				다수

II 사례와 특징

행정안전부
NIA 한국지능정보사회진흥원

NIA 한국지능정보사회진흥원

01 J기관 클라우드 플랫폼 | SCP Private + Sovereign(CSAP)



Key Point

- 클라우드 자원을 고객 현장에 배치하는 SCP Private과 민간센터 자원을 활용하는 SCP Sovereign
- 기관 On-Site 자원 재활용 환경 제공
- 업무 범위와 목적에 따른 전환
  - Private: 내부연계·민감정보 보유 업무
  - Sovereign: 비용효율성 중심 대민서비스

02 Samsung Cloud Platform(SCP) 구축

SCP Private 장비 이전·설치

✔ 장비 구성·테스트, 이전 준비 (삼성 데이터센터)

✔ 랙 운송 및 기관내 정보시스템실 반입·설치

J 기관 SCP 구축

J 기관

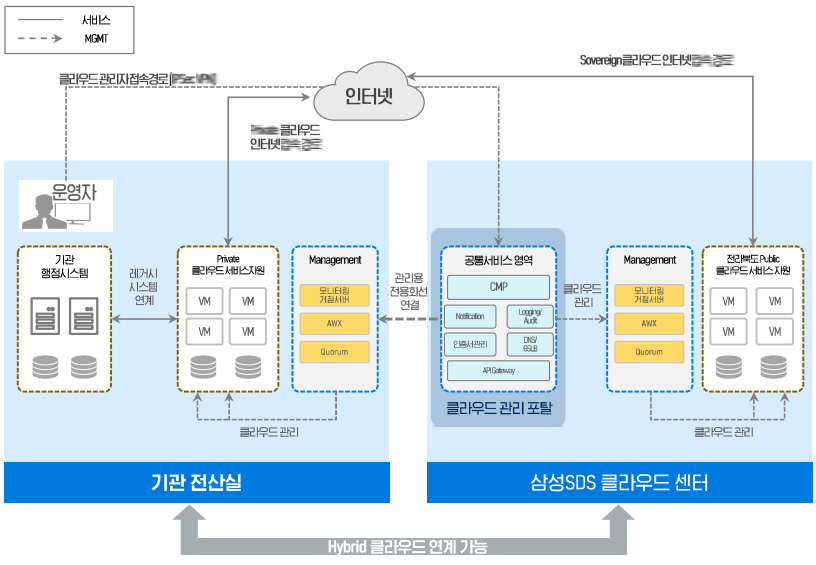
SCP Private 클라우드

삼성데이터센터

SCP Sovereign 클라우드

03 J 기관 클라우드 구성

클라우드 구성도



주요 구성 내역

❶ 클라우드 자원 구성	• 기관 전산실의 기존 설비를 재활용하여 SCP Private 구축 • 삼성SDS 클라우드 센터 SCP Sovereign(CSAP) 자원 활용
❷ 클라우드 보안 구성	• 최신 보안기술이 적용된 IPSec 기반 VPN 운영관리 경로 제공 • 운영자는 클라우드 내부의 접근제어 영역을 통해서만 서비스 영역에 접근이 가능함 • 필수 보안SW 적용 등 국가 클라우드컴퓨팅 보안 가이드 준수
❸ 보안관제 및 망 분리	• J 기관 관문보안 정책 및 망연계 아키텍처 업그레이드 • J 기관 전용IPS 및 사이버침해대응센터 연계
❹ 대국민 서비스	• J 기관 보안관문과 SCP Sovereign 보안 관문을 통한 인터넷 사용자 서비스 제공

NIA 한국지능정보사회진흥원

04 활용 모델 특징 | ① 비용 효율성 + 강화된 보안

현장 데이터 처리 속도 및 민감 데이터 보안성 향상, 데이터 주권 확보 등의 프라이빗 클라우드 도입 효과 외에
SCP Sovereign 추가 구성을 통한 **클라우드 전환의 유연성과 가용성/확장성/안정성 확보**

SCP Private Cloud (기관 정보시스템실, 6층)	SCP Sovereign Cloud (공공클라우드, 상암센터)
J 기관을 중심으로 내부/외부연계 및 민감정보 보유 유무를 고려하여 대상 선정	시군을 중심으로 편리성, 운영성, 비용효율성을 고려하여 대상 선정

재난안전대책본부	도립국악원	실시간대기정보시스템
		
• 내부 연계 • 연계 데이터 다수 (기상,강수,강설 등)	• 내부연계(예약) • 민감정보(수강신청)	• 연계 다수 (43개 측정소) • 개인정보(SMS)

주요 구성 및 특징

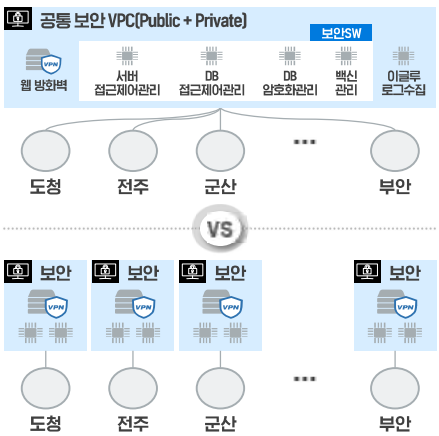
SCP Private Cloud	✔ 기관 6층 전산실에 전용랙 3대로 구성 ✔ 기관 보안환경 재활용으로 비용 효율성 ✔ 내부/외부 연계 시스템에 대한 현장 데이터 처리속도 향상 ✔ 개인정보 등 민감데이터에 대한 보안 향상 ✔ 기관 전산실 증축 또는 J 통합데이터 센터 건립 시 신속한 전환/확장 가능
+ (SCP Sovereign Cloud)	✔ 삼성SDS 상암데이터센터 자원구성 (춘천데이터센터와 DR 구성 가능) ✔ 신속한 클라우드 전환 및 고수준의 가용성/안정성 제공 ✔ 보안 솔루션 등 구독형 솔루션 도입 용이 ✔ 기관 Private Cloud와 Hybrid 구성 가능

NIA 한국지능정보사회진흥원

04 활용 모델 특징 | ② 이용요금 최적화 설계

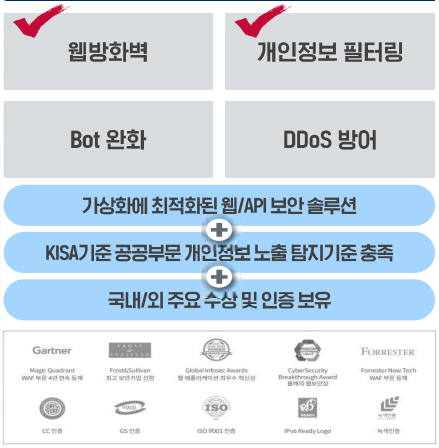
이용기관에서 공통적으로 이용하는 자원을 통합하고 최적의 인프라 설계기준을 적용하여 **이용요금 부담 최소화**

보안SW 통합



공통 보안인프라 통합으로 비용 절감

개인정보 필터링 기능 통합



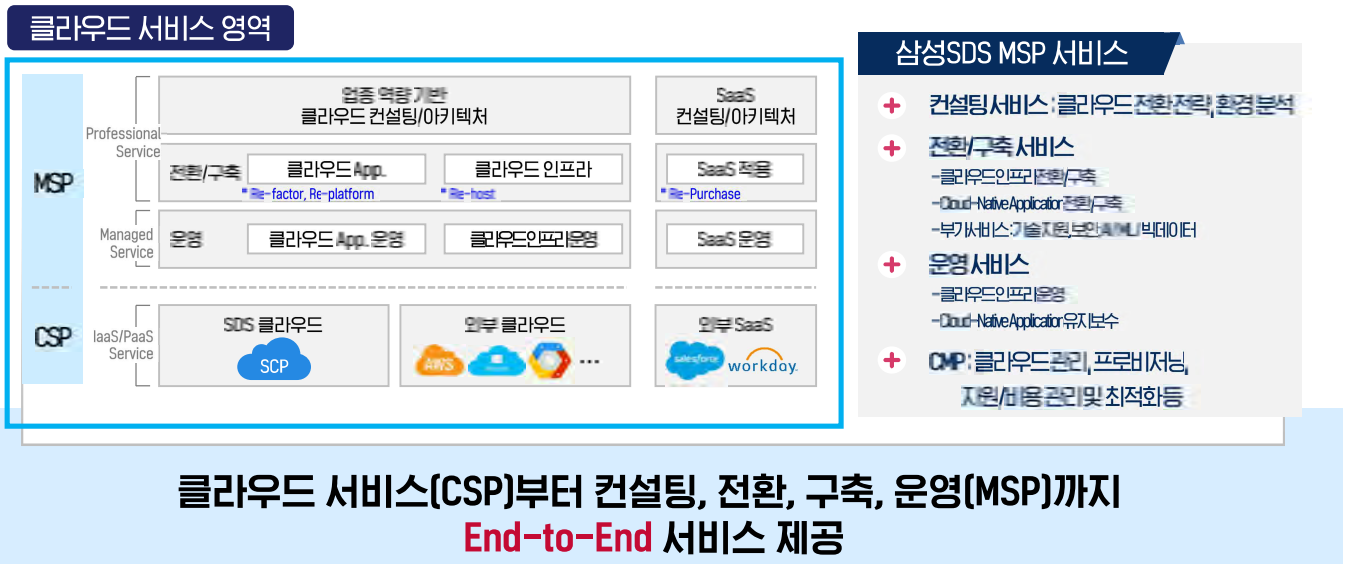
기능 통합으로 비용 절감

인프라 설계기준 최적화

최적 VM 타입 적용으로 요금 절감

04 활용 모델 특징 | ③ CSP + MSP 통합 추진체계

삼성SDS는 클라우드 서비스 뿐 아니라 전환 & 운영까지 일괄 책임지고 수행이 가능한 통합 추진체계를 갖추고 있으며,
공공/금융/제조 및 서비스 등 다양한 비즈니스 영역에서 쌓은 경험과 역량을 활용하여 클라우드 전환을 성공적으로 리딩



클라우드 서비스(CSP)부터 컨설팅, 전환, 구축, 운영(MSP)까지
End-to-End 서비스 제공

III 성과 평가

01 클라우드 전환 성과 지표
02 클라우드 전환 우수 사례
03 이용기관 평가 (인터뷰)

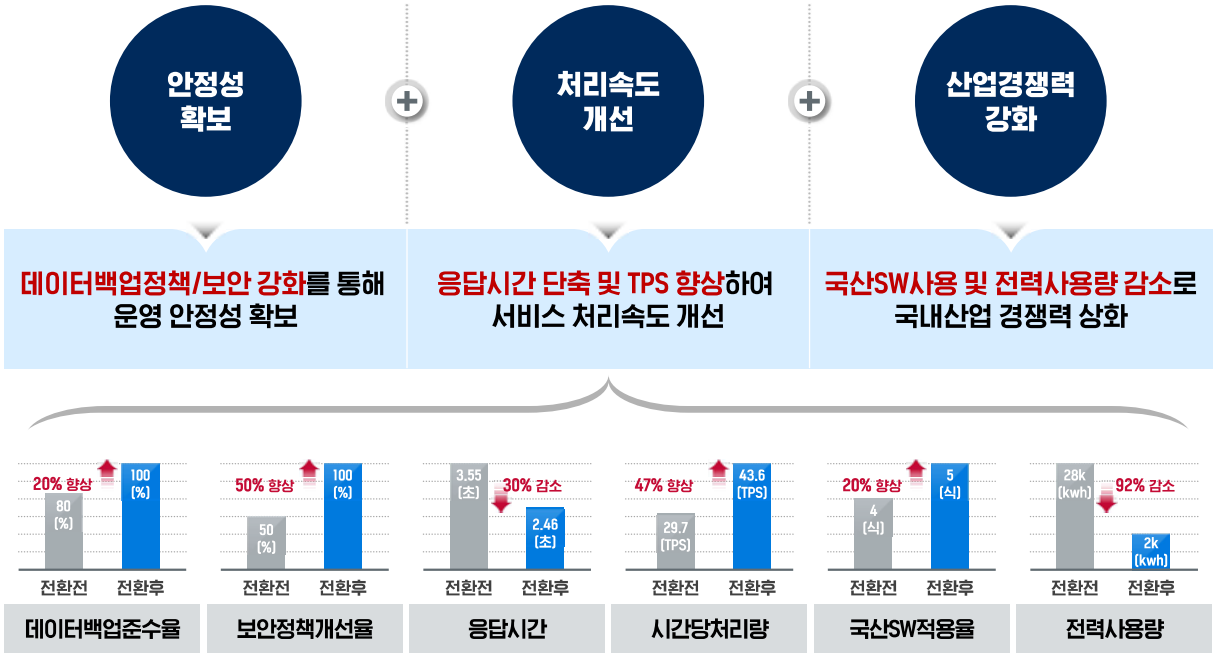
행정안전부
NIA 한국지능정보사회진흥원

01 클라우드 전환 성과 지표 | 종합

공통 성과 지표 : 7개 영역 11개 지표

구분		종합 분석 결과 (전체 평균)			
		전환 전	전환 후	증감	성능 향상률
❶ 이용자 만족	전환만족도	-	5.6 점	-	-
	운영만족도	-	5.4 점	-	-
❷ 보안/장애대응 강화	데이터 백업 정책 준수율	40.82 점	100 점	▲ 58.18 점	145.0% 향상
❸ 구성 관리	보안정책 준수율	50.82 점	100 점	▲ 49.18 점	96.8% 향상
❹ 성능향상	응답시간	6.53 초	2.90 초	▼ 3.63 초	55.6% 절감
	시간당 처리량	109.37 TPS	183.24 TPS	▲ 73.86 TPS	67.5% 향상
	SW 취약구조 개선률	56.4 %	0 %	▼ 56.4 %	100.0% 절감
❺ 비용절감	공개 SW 적용률	255 206 식 (80.8%)	273 228 식 (83.5%)	▲ 22 식 (2.7%)	10.7% 향상
❻ 국내 산업 경쟁력 강화	국산 SW 적용률	255 33 식 (12.9%)	273 45 식 (16.5%)	▲ 12 식 (3.6%)	4.7% 향상
❼ 에너지절감/탄소 중립	전력 사용량	567,648 kwh	75,126 kwh	▼ 492,522 kwh	86.8% 절감
	탄소 배출량	271.4 톤	35.9 톤	▼ 235.5 톤	
	식재 효과	65,712 그루	8,697 그루	▼ 57,015 그루	

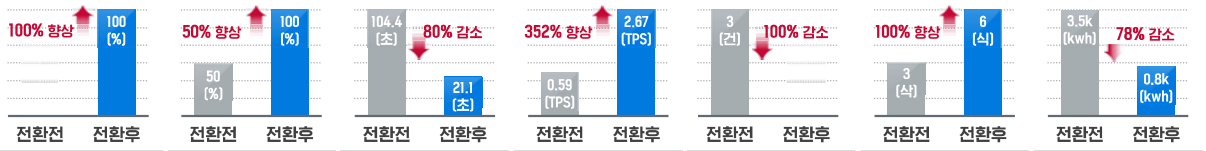
02 클라우드 전환 우수 사례 | 1 J 기관 대표홈페이지



03 클라우드 전환 우수 사례 | ② J 기관 소방본부홈페이지

업무연속성 확보 + **운영안정성 개선** + **처리속도 개선**

업무연속성 확보	운영안정성 개선	처리속도 개선
데이터 백업 정책 강화를 통해 업무 연속성 확보	보안정책강화/취약구조개선으로 운영안정성 개선	응답시간 단축 및 TPS 향상하여 서비스 처리속도 개선



03 클라우드 전환 우수 사례 | 인터뷰

J 기관 정보화정책과 박00 팀장

성과 내용 요약

- **노후 정보시스템에 의한 장애발생 예방**
  - 정보자원 60~70% 이상이 노후장비*로 빈번한 장애 발생
    * 서버,스토리지,백업장비,네트워크,보안장비 등
  - 정보시스템 클라우드 전환에 따라 개별 서버 등의 장애 발생에 따른 운영중단 예방
- **최신 OS 및 S/W 사용으로 보안 강화**
  - 최초 시스템 도입 시 설치된 OS 및 S/W를 계속 사용하고 있었으나, EOS 된 S/W를 최신버전으로 교체하여 보안 강화 (MySQL 5.6, 5.7 에서 8.0로 변경 등)
- **향후 클라우드 이용료 인하 필요**
  - 행정·공공기관의 신속한 클라우드 전환을 유도하기 위해 이용료 인하가 필수적임 (VM 통합, 공통인프라 보안 통합 등)

A기관 정보화정책과 홍00 주무관

성과 내용 요약

- **유연한 대응 가능**
  - 홈페이지 사용량 급증 시 코어 수를 바로 늘릴 수 있어 수요 대응 가능
- **통합 모니터링 기능**
  - CPU, 메모리, 스토리지 사용량을 통합 모니터링 시스템을 통해 간편하게 확인할 수 있어 관리편의성 증대
- **백업 강화**
  - 최근 2주간의 일일백업을 제공하여 문제 발생 전 시점으로 쉽게 전환 가능
- **Oracle 탈피**
  - 금번 전환시 Oracle 을 Tibero로 전환하여 향후 유지보수 비용 절감

J 기관 클라우드 활용모델 시범사업 성공 요소

신뢰할 수 있고 안전성 입증된 클라우드 서비스(SCP)

- **클라우드 보안 인증(CSAP)** 획득한 클라우드 서비스(SCP)
- 국정원『**국가 클라우드컴퓨팅 보안 가이드라인**』준수
- 운영관리자 **접근 보안 강화 및 공공기관 망분리** 기준 적용

기관 특성에 최적화된 클라우드 서비스 환경 및 비용 효율화 제공

- 전라북도 중장기 클라우드 발전계획을 실현하기 위한 아키텍처
- 합리적인 이용요금 정책을 위한 **클라우드 공통자원 통합** 설계
- 전라북도 **데이터 주권을 유지**하기 위한 클라우드 서비스 환경

신속한 의사결정 체계(TF) 및 통합(CSP+MSP) 사업자

- 도·시군, 지방공사, 공단 참여하는 **전북클라우드전환T/F를 통한 신속한 의사결정**
- 클라우드 서비스(CSP)와 **전환·운영 매니지드 서비스(MSP) 동시 제공**
- **분명한 책임소재, Grey영역이 없는 R&R 기반 사업 수행**

PART

II

클라우드 역량 강화 교육

클라우드 기술 교육

1. 컨테이너에 대한 이해와 적용 사례
2. 왜 클라우드 네이티브를 도입해야 하나요
3. 클라우드 환경에서의 정보보호 관리체계 수립
4. 클라우드 최적화를 통한 비용 절감 방법

컨테이너에 대한 이해와 적용 사례

윤 지 현 강사

행정안전부 NIA 한국지능정보사회진흥원

컨테이너에 대한 이해와 적용 사례

CONTENTS

I 컨테이너란 무엇인가?

행정안전부
NIA 한국지능정보사회진흥원

01 클라우드 컴퓨팅

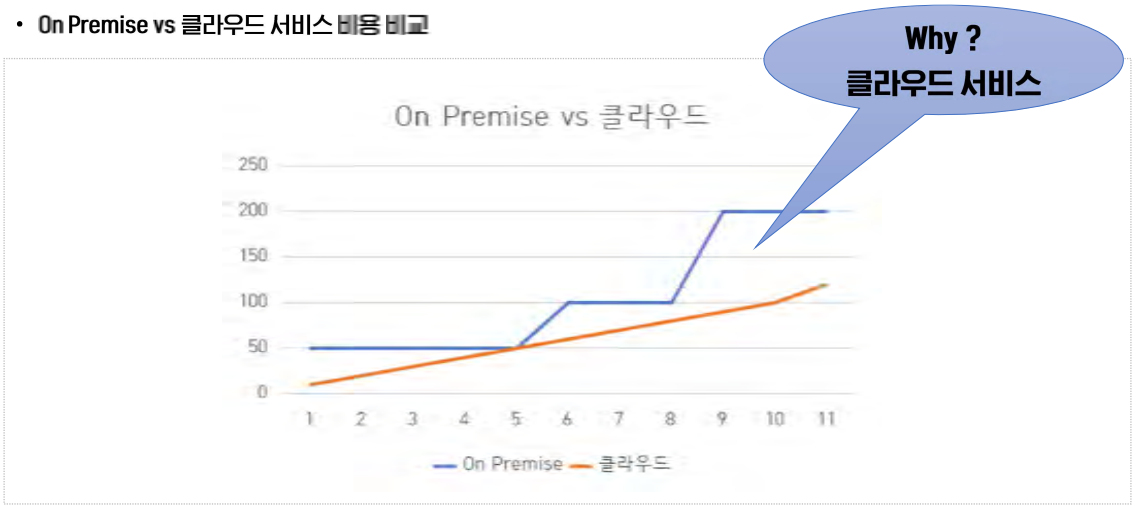
클라우드 컴퓨팅이란?

• 출처 : https://www.Wikimedia.org

01 클라우드 컴퓨팅

클라우드 컴퓨팅 장점

- On Premise vs 클라우드 서비스 비용 비교



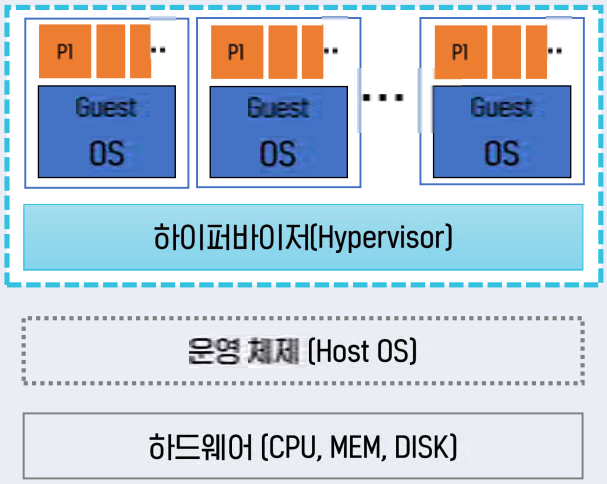
01 클라우드 컴퓨팅

클라우드 컴퓨팅의 핵심

02 가상화 기술

전통적인 컴퓨터 구조 및 운영 체제

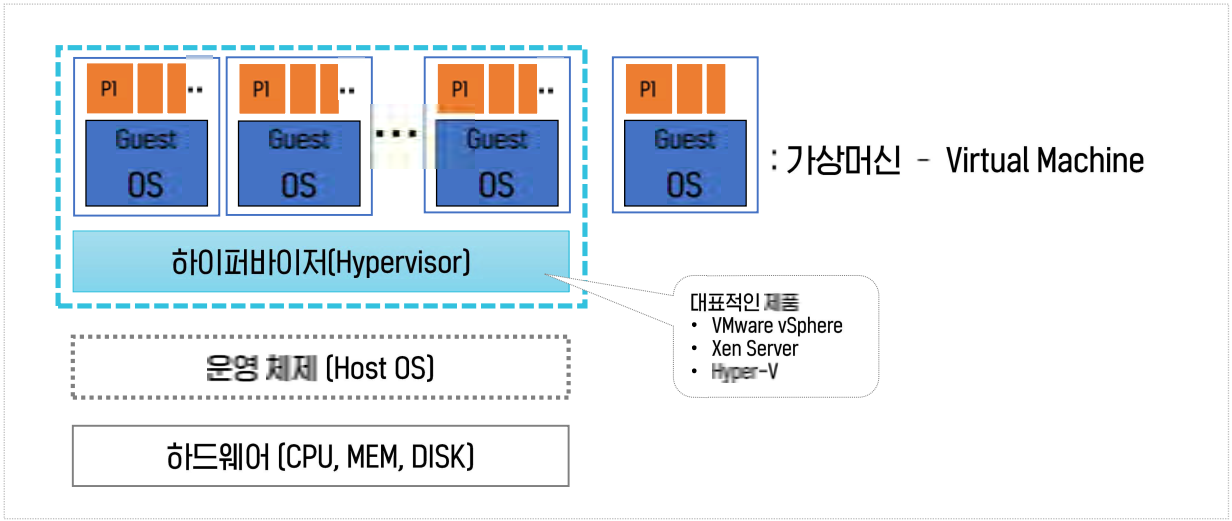
가상화 기술



02 가상화 기술

가상 머신(Virtual Machine)

가상 머신은 가상화 기술의 대표적인 형태로 다양한 운영 체제(OS) 및 하이퍼바이저를 사용
물리적 서버 내 여러 개의 확장 가능한 격리된 서버를 수행

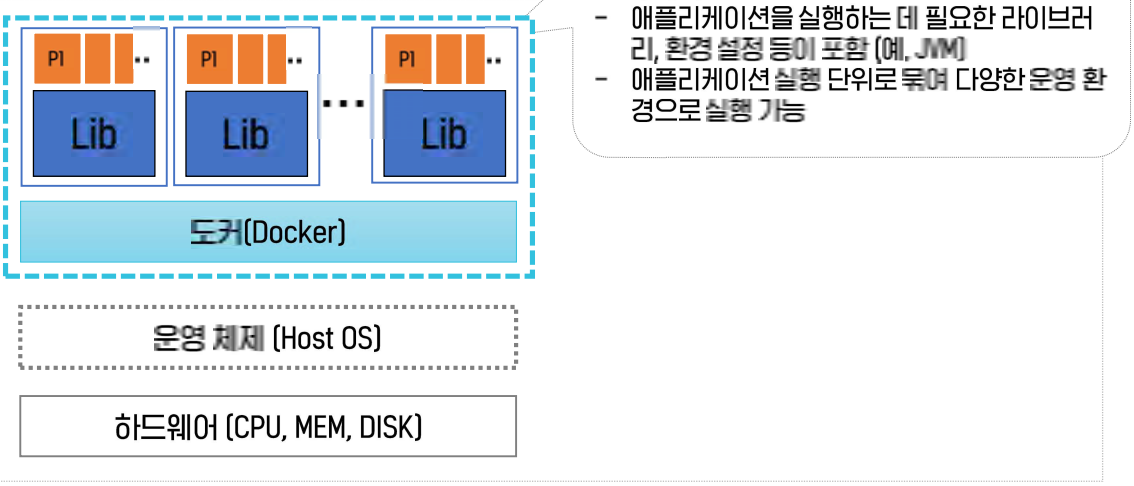


03 컨테이너의 정의

컨테이너란?

호스트 운영체제의 커널을 공유하면서 격리된 컴퓨팅 자원을 제공하는 가상화 기술

• 컨테이너 실행 모습



컨테이너에 대한 이해와 적용 사례

II 가상 머신과 컨테이너

01 가상 머신 vs 컨테이너
02 가상 머신 대비 컨테이너의 장점
03 컨테이너 관리 기술

행정안전부
NIA 한국지능정보사회진흥원

01 가상 머신 vs 컨테이너

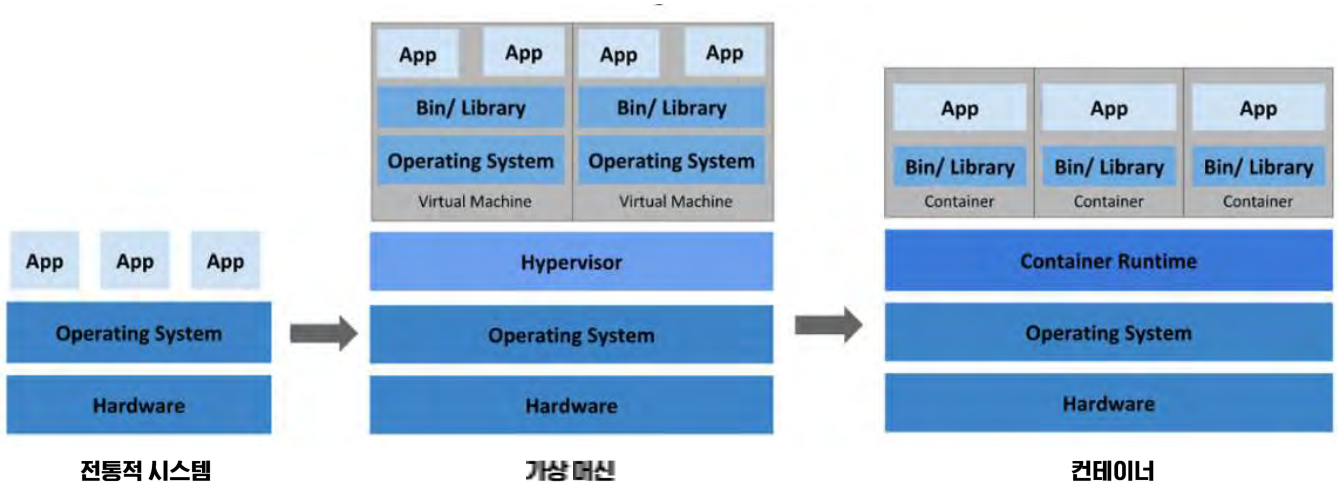
가상 머신, 컨테이너 비교 설명

가상화 기술	설명
가상 머신 (Virtual Machines, VMs)	하나의 물리적 서버에서 여러 개의 가상 서버를 동시에 실행하는 기술
컨테이너 가상화 (Containerization)	운영체제를 공유하면서 애플리케이션을 독립적인 환경에서 실행하는 기술

01 가상 머신 vs 컨테이너

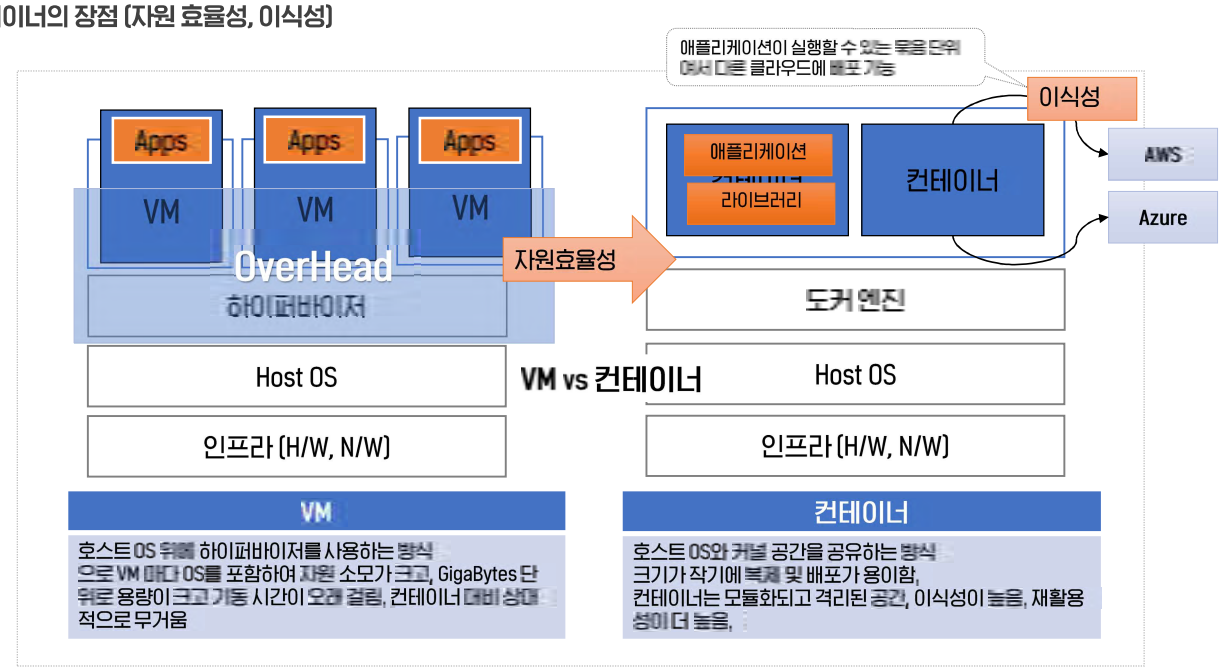
전통적 시스템, 가상 머신, 컨테이너 시스템 구성 차이

가상 머신은 전통적 시스템 대비 Hypervisor가 추가되어 여러 개의 VM 수행
컨테이너는 VM 대비 Guest OS, Hypervisor 부분 제외되어 이미지 용량 축소, 이기종 OS에서의 이식성 증가



02 가상 머신 대비 컨테이너 장점

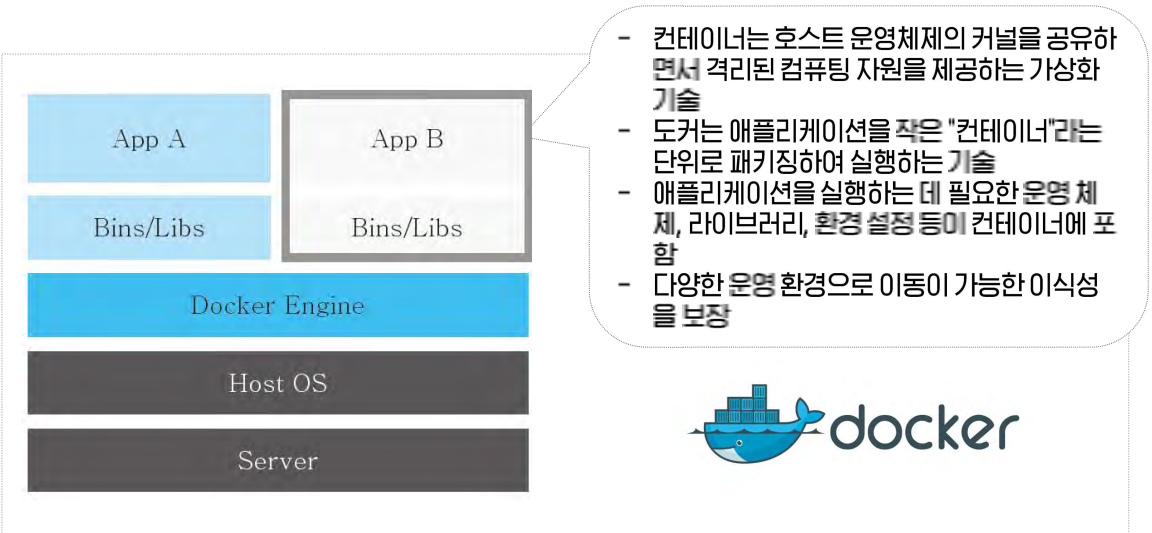
컨테이너의 장점 (자원 효율성, 이식성)



03 컨테이너 관리 기술

도커 (Docker)의 컨테이너 관리 기술

도커(Docker)는 컨테이너화 기술을 사용하여 애플리케이션을 실행하고 배포하는 오픈 소스 플랫폼
애플리케이션(컨테이너 이미지)를 배포 및 구동할 수 있는 컨테이너 엔진의 종류



II 가상 머신과 컨테이너

03 컨테이너 관리 기술

도커 (Docker) 허브 및 명령어

https://hub.docker.com/ 를 이용하여 미리 구성된 도커 이미지를 검색, Pull, Push 수행
도커 이미지는 계층적 구조로 반복 생성되며 공유 가능

- 도커 허브를 이용한 도커 이미지 활용

✓ 이미지 목록 보기
$ docker images

✓ 이미지 검색
$ docker search <이미지 이름>

✓ 이미지 받기
$ docker pull \
<이미지 이름>:<버전>
※ lastest를 지정하면 최신 버전

✓ 이미지 삭제
$ docker rmi <이미지 id>

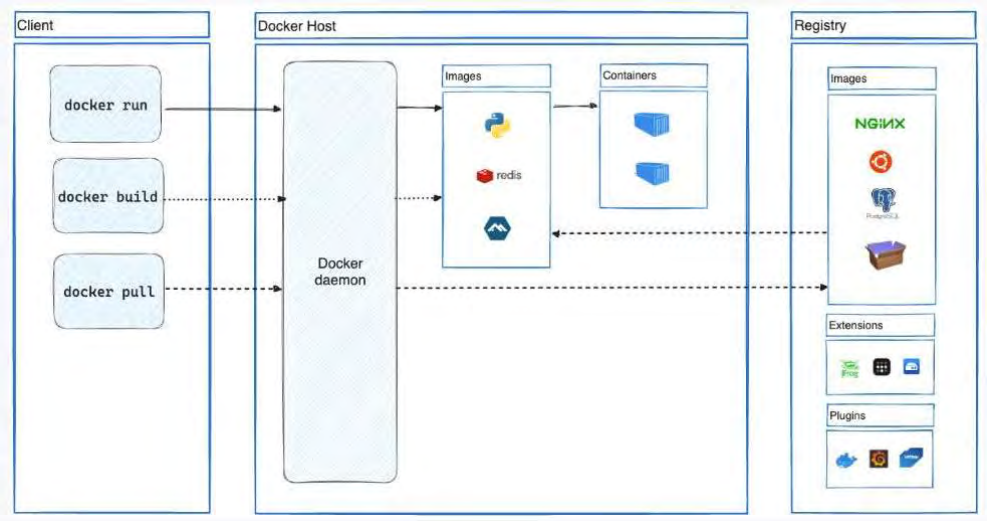
https://docs.docker.com/engine/reference/commandline/docker 에서 자세한 명령을 확인할 수 있다.

II 가상 머신과 컨테이너

03 컨테이너 관리 기술

도커(Docker)의 실행 과정

Docker 명령들(run, build, pull)을 통해서 이미지를 생성하거나 조회해서 가져오는 실행

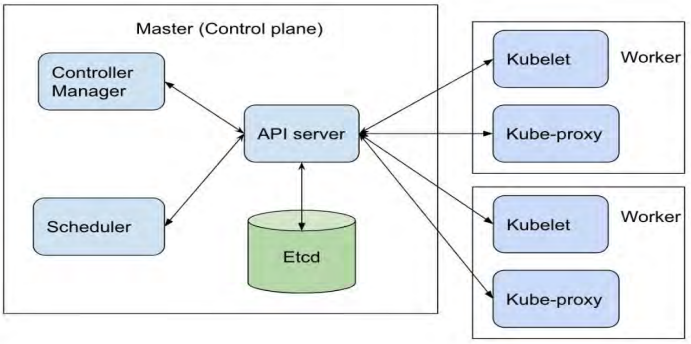


도커 컨테이너 실행 과정 (출처: 도커 공식 사이트)

03 컨테이너 관리 기술

쿠버네티스

- 구성 요소: 컨트롤 플레인(마스터), 클러스터 상태 저장 Etcd, 클러스터 노드(kubelet)



Control Plane 컨트롤 플레인

- 3개 주요 컴포넌트가 실행
- kube-apiserver, kube-controller-manager, kube-scheduler
- 쿠버네티스 서비스의 상태 저장 스토리지 서비스 - Etcd
- Etcd - 분산 시스템 데이터를 저장하는 key-value 방식 저장

Worker 워커 노드

- 컨트롤 플레인으로부터 부여 받은 컨테이너가 실행되는 노드
- Kubelet은 Docker, Containerd 같은 컨테이너런타임을 이용해 컨테이너를 수행하는 역할
- Kube-proxy는 노드에서 실행되는 네트워크 프록시로, 노드의 네트워크 규칙을 유지/관리 내부 컨테이너간의 통신, 외부와의 통신 가능

컨테이너에 대한 이해와 적용 사례

II 컨테이너 사용 사례

01 컨테이너 사용 증가 이유
02 마이크로 서비스
03 하이브리드 / 멀티클라우드

행정안전부
NIA 한국지능정보사회진흥원

01 컨테이너 사용 증가 이유

현대 IT의 시스템적 요구사항

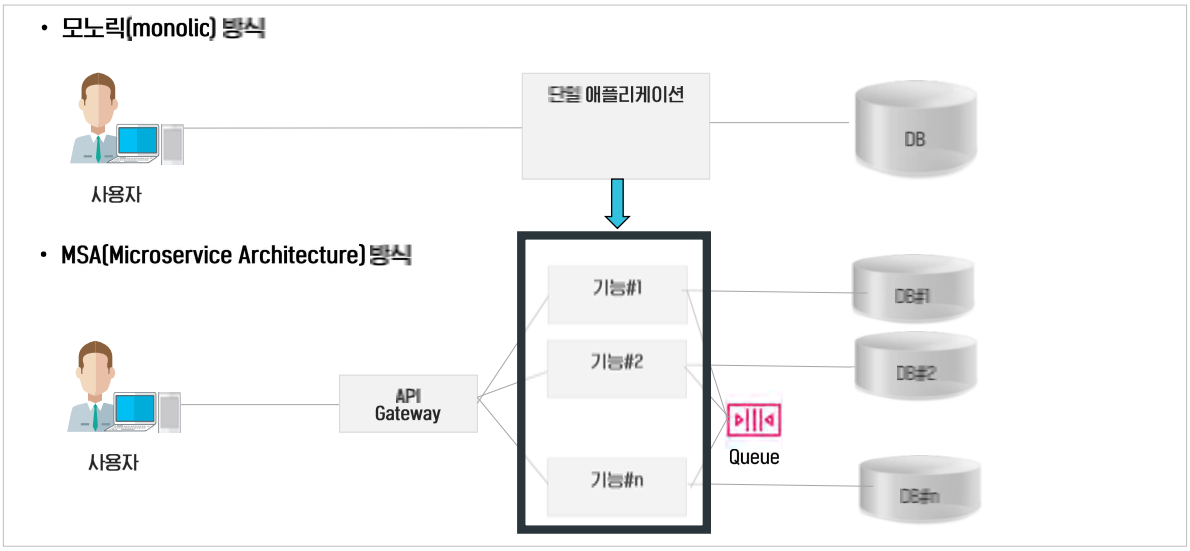
인프라 자원의 효율성에 대한 요구, MSA 아키텍쳐 구조에 대한 니즈, 멀티 클라우드 도입 검토 등 컨테이너 사용 증가

요구사항	설명
애플리케이션 배포 주기	사용자 대상 프론트앤드 애플리케이션의 빠른 배포 주기에 대한 니즈가 있음. MSA로 구조화 하여 반영 주기를 단축할 수 있음.
자원 효율에 대한 니즈	클라우드 인프라 사용량 증가에 따른 자원 효율화에 대한 니즈가 있음. PaaS 형태로 구축 시 자원의 오버헤드 효율화 가능
멀티 클라우드 니즈 증가에 따른 이식성	CSP Lock에 대해서 기피하여 멀티 클라우드 사용 확대, 타 클라우드로의 이전 가능한 형태 요구. 컨테이너화 하여 빠른 이전 가능

02 마이크로서비스

모노릭(monolic) 방식 vs MSA

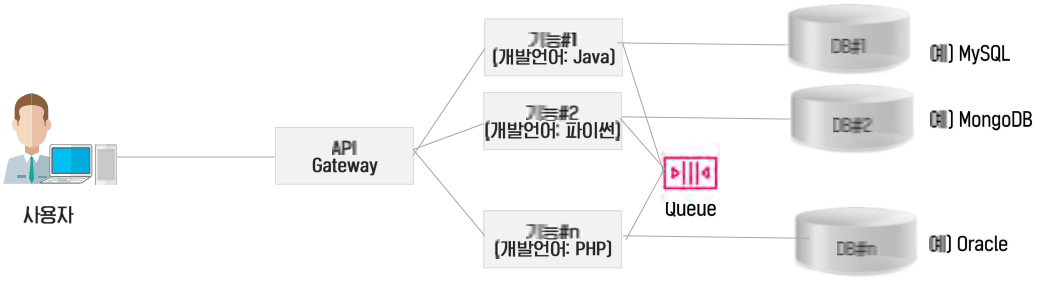
MSA는 애플리케이션을 작은, 독립적인 기능 단위인 마이크로서비스로 분할하는 소프트웨어 아키텍처
독립적으로 배포 실행될 수 있는 작은 애플리케이션으로 구성



03 마이크로서비스

MSA 특징

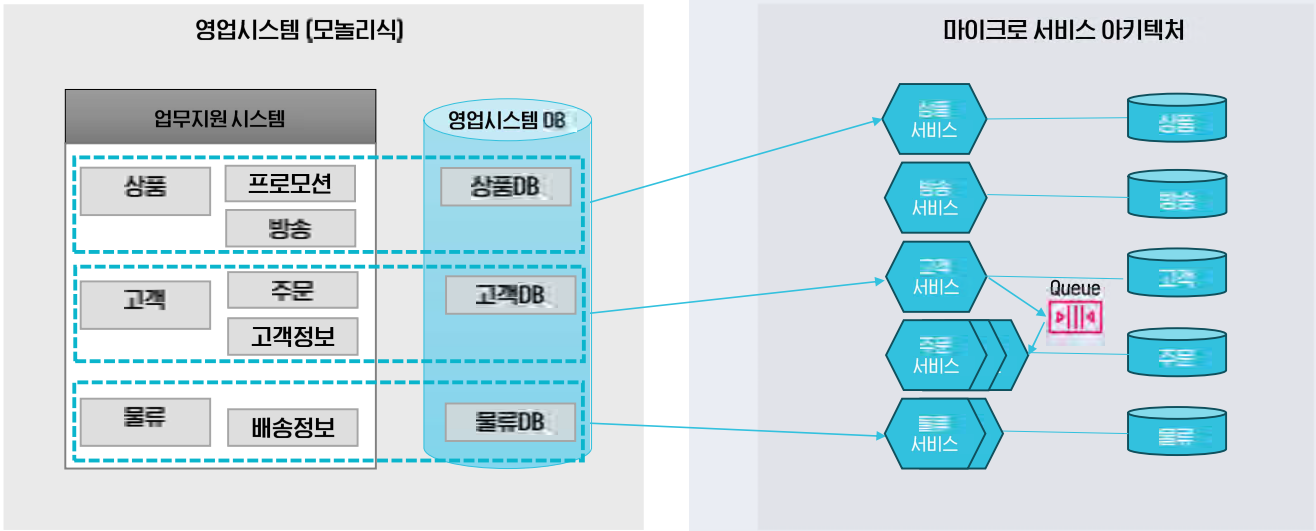
- MSA(Microservice Architecture) 특징: 폴리글랏 (다양한 구성)



개발	기능별 개발언어와 DB의 종류, 배포 주기를 달리 할 수 있다.
운영	하나의 기능이 장애가 나더라도 전체 시스템에 영향을 적게 미칠 수 있다.
조직	기능단위로 개발 조직을 운영할 수 있다. 독립적인 스케쥴로 개발 및 운영할 수 있다.

02 마이크로서비스

MSA 도메인 식별



03 하이브리드 / 멀티 클라우드

클라우드 유형

클라우드 서비스 유형에는 형태에 따라서 퍼블릭 클라우드, 프라이빗 클라우드, 하이브리드 클라우드 멀티 클라우드 종류가 있음

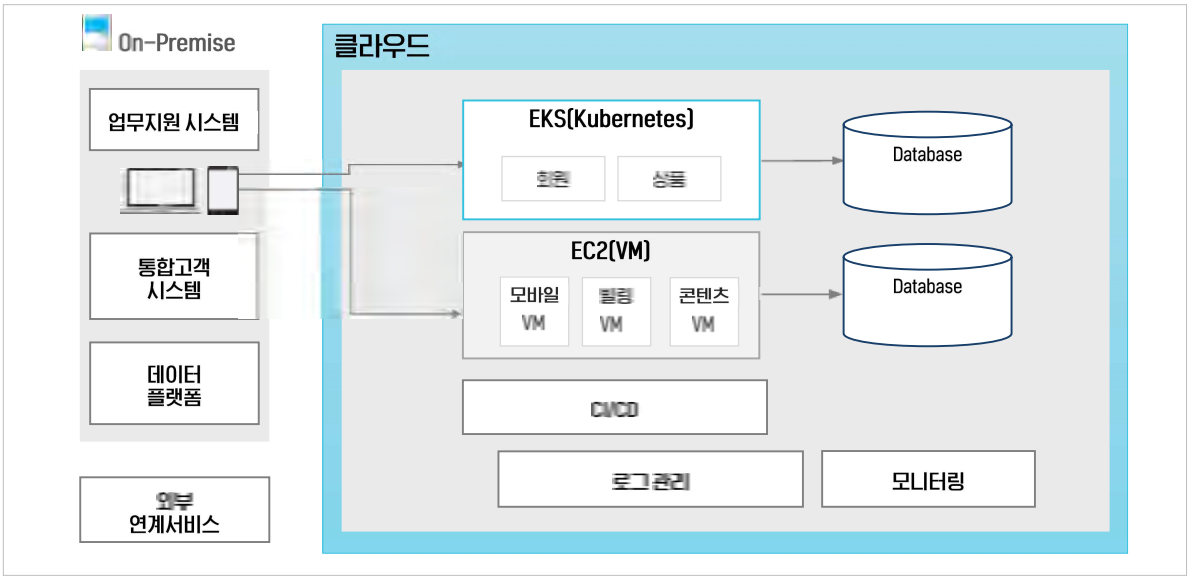
Public 클라우드	AWS, Azure, GCP 등의 공용 클라우드 서비스
Private 클라우드	기업의 데이터 센터 내 클라우드 환경 구성
하이브리드 클라우드	On Premise 서버와 클라우드를 조합하여 사용하는 방식
멀티 클라우드	여러 CSP(Public 클라우드)를 조합해서 사용하는 방식

- CSP : Cloud Service Provider (AWS, Azure, GCP 등)
- MSP : Managed Service Provider (SDS, CNS, C&C, 메가존, 베스핀 등)

03 하이브리드 / 멀티 클라우드

하이브리드 방식

하이브리드 클라우드는 기존 On-Premise 시스템과 클라우드 서비스를 혼합하여 사용하는 방식



03 하이브리드 / 멀티 클라우드

멀티클라우드 방식

멀티 클라우드는 CSP 사들의 클라우드 서비스를 혼합하여 시스템을 구성하는 방식의 클라우드 유형

왜 클라우드 네이티브를 도입해야 하나요?

윤지현 강사

행정안전부 NIA 한국지능정보사회진흥원

왜 클라우드 네이티브를 도입해야 하나요?

CONTENTS

왜 클라우드 네이티브를 도입해야 하나요?

I 클라우드 네이티브 개념

01 클라우드 네이티브 정의
02 클라우드 네이티브 개념
03 클라우드 서비스 유형

행정안전부
NIA 한국지능정보사회진흥원

NIA 한국지능정보사회진흥원

01 클라우드 네이티브 정의

클라우드 네이티브란?

애플리케이션과 서비스를 클라우드 환경에 맞게 개발, 운영, 확장하는 방식

CNCF (Cloud Native Computing Foundation) v1.0
클라우드 네이티브 전환할 수 있는 기술 정의 및 오픈 소스를 관리하는 단체

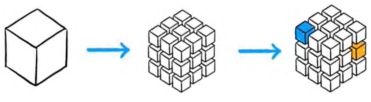
- 퍼블릭, 프라이빗, 하이브리드 클라우드 환경에서 확장성 있는 애플리케이션
- 컨테이너, 서비스 메시(Mesh), 마이크로서비스(Micro Service) 인프라 구조, 선언적 API로 접근
- 자동화, 회복성, 편리성, 가시성을 갖는 느슨하게 결합된 시스템 (개발 및 실행 환경)
- 엔지니어는 최소한의 수고로, 영향력이 크고, 예측 가능한 변경을 할 수 있는 기술 정의

클라우드 네이티브
(형용사/명사)

클라우드 컴퓨팅의 장점을 최대한 활용할 수 있는
(효율적인 자원이용, 탄력적 수요 대응 등)
정보시스템 분석·설계·구현 및 실행하는 환경

클라우드 네이티브
애플리케이션

클라우드 환경에서 최적화되어 실행되는 애플리케이션



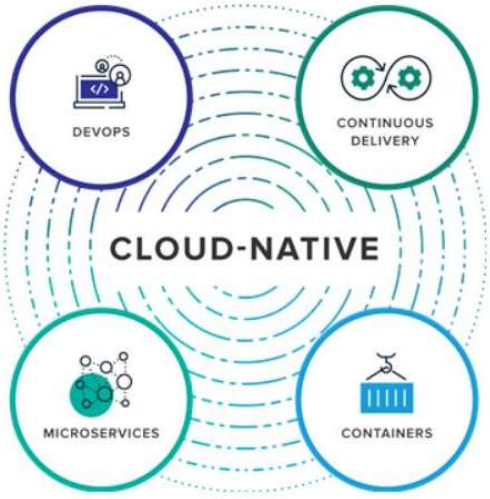
01 클라우드 네이티브 정의

클라우드 네이티브란?

애플리케이션과 서비스를 클라우드 환경에 맞게 개발, 운영, 확장하는 방식

CNCF (Cloud Native Computing Foundation)

- 가벼운 컨테이너로 포장(패키징)되 배포함으로써 물리적 인프라스트럭처를 효율적으로 사용
- 각각의 컨테이너는 그 자체로 독립적이며 완결성을 갖기 때문에 호환성 혹은 특정 기술에 종속될 필요 없이 컨테이너가 제공하는 기능에 최적화된 기술 활용
- 컨테이너로 포장된 각 기능들은 API 호출을 이용, 서로 연계됨으로써 더 큰 서비스로 발전 가능
- 고성능의 하드웨어가 필요한 경우, 이를 별도의 서비스로 분리하여 배포함으로써 성능 최적화
- 애자일(Agile), 데브옵스(DevOps) 프로세스에 기반한 자동 통합/배포(CI/CD: Continuous Integration / Continuous Delivery) 사용
- 다수 서비스들을 컨테이너 기반으로 동적 배포를 하기 위해서는 고도의 자동화 도구가 필수적임

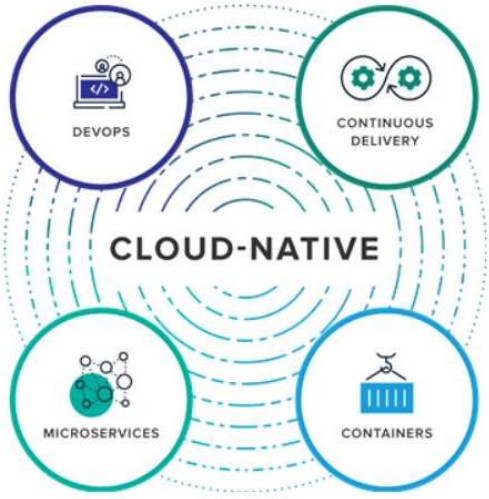


클라우드 네이티브 핵심 요소 (출처: Pivotal)

01 클라우드 네이티브 정의

클라우드 네이티브란?

클라우드 환경에 맞게 개발, 운영, 확장하는 방식에 따른 기술적 측면



아키텍처 측면	마이크로서비스 아키텍처(MSA)
개발 측면	선언적 API 서비스 메시
인프라 측면	컨테이너화 (Containerization)
운영측면	자동화 (DevOps-CI/CD)

NIA 한국지능정보사회진흥원

02 클라우드 네이티브 개념

클라우드 네이티브란?

클라우드 네이티브의 아키텍처, 개발, 인프라, 운영 측면의 기술 요소

아키텍처 측면	마이크로서비스 아키텍처(MSA)	애플리케이션을 작은 독립적인 서비스로 분해하여 개발, 배포, 확장, 유지보수가 용이하도록 하는 아키텍처 패턴
개발 측면	선언적 API 서비스 메시	의도를 명시적으로 선언하는 API를 통해 시스템의 상태를 관리하고 제어하는 방식,
인프라 측면	컨테이너화 (Containerization)	애플리케이션과 모든 종속성을 독립된 단위로 패키징하여 이식성과 확장성을 향상시키는 기술,
운영측면	자동화 (DevOps-CI/CD)	지속적 통합, 지속적 배포, 스케일링, 운영 등의 작업을 자동화하여 빠른 개발과 안정적인 운영을 지원,

NIA 한국지능정보사회진흥원

02 클라우드 도입 단계

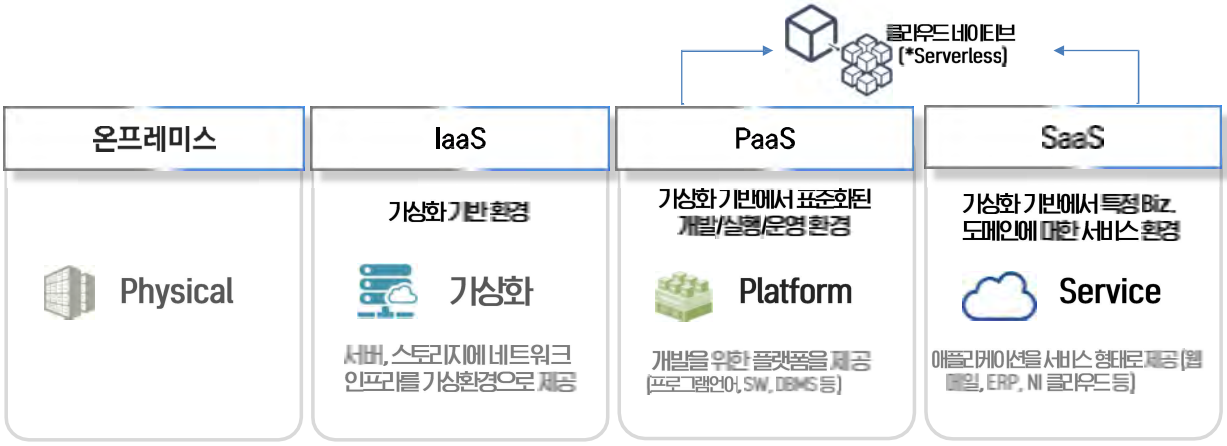
클라우드 유형 변화 단계

가상화된 컴퓨팅 자원을 효율적으로 사용하려는 측면의 단계를 거쳐 클라우드 네이티브 형태로 발전함

03 클라우드 유형

클라우드 서비스 유형

클라우드 사용하는 방식에 따른 유형으로 IaaS, PaaS, SaaS 일반적으로 제공되는 형태임



* Severless : 서버리스 컴퓨팅은 서버가 존재하지만, 사용자의 운영 개입 없이 클라우드 플랫폼에서 자동으로 관리되는 서비스로, 애플리케이션 함수 실행 서비스 및 백엔드 서비스를 포괄

03 클라우드 유형

클라우드 서비스 모델 발전

컨테이너와 서버리스 등의 최신 기술이 발달되면서 CaaS, FaaS 등 다양한 클라우드 서비스 모델로 세분화되고 있음

왜 클라우드 네이티브를 도입해야 하나요?

II 클라우드 네이티브 기반 기술

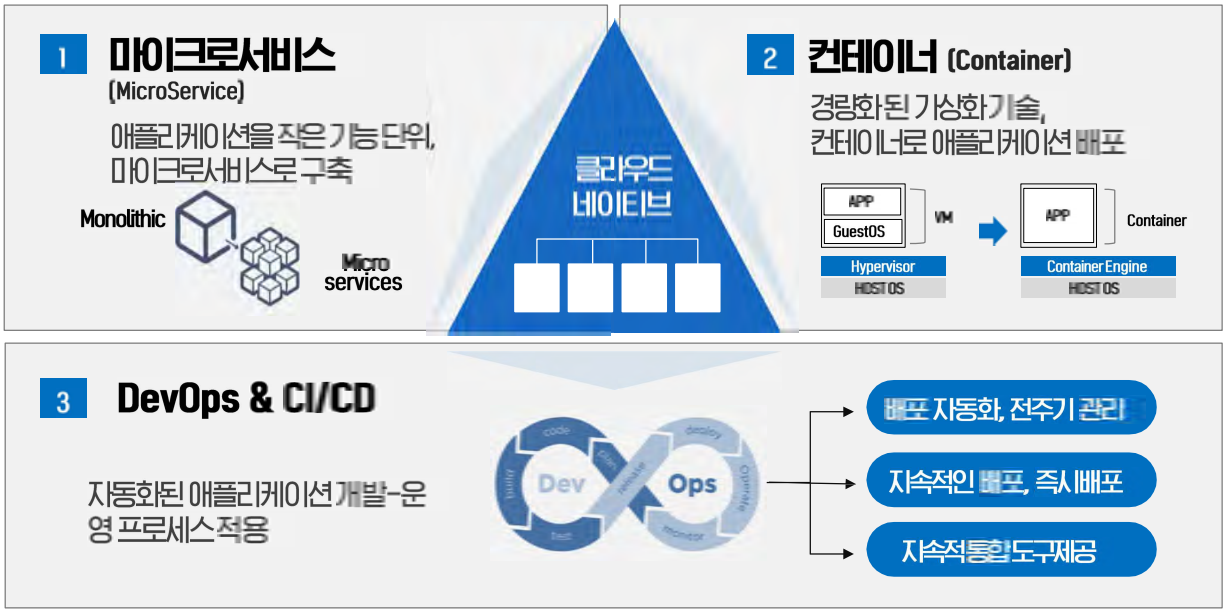
행정안전부
NIA 한국지능정보사회진흥원

NIA 한국지능정보사회진흥원

01 클라우드 네이티브 구성 요소

클라우드 네이티브 기술

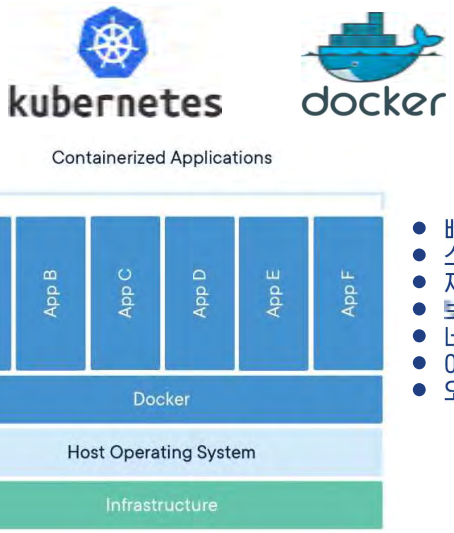
클라우드를 더 클라우드 답게 사용하기 위한 네이티브 기술 - 마이크로서비스, 컨테이너, DevOps, CI/CD



01 클라우드 네이티브 구성요소(1/2)

MSA : 단일 AP가 다수의 느슨하게 결합되고 독립적으로 배치 가능한 더 작은 서비스로 구성된 클라우드

컨테이너 : 환경 종속적이지 않은 필요한 모든 요소를 포함하는 소프트웨어 패키지

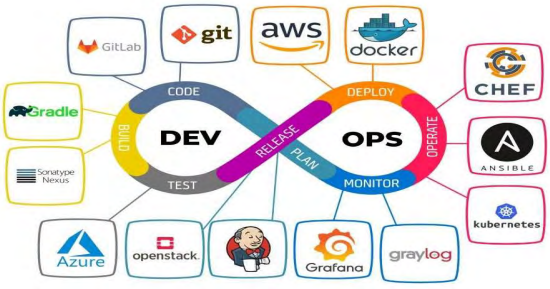


- 배포관리
- 스케일링
- 자동복구
- 보안
- 네트워크
- 이중화
- 오픈소스

01 클라우드 네이티브 구성요소(2/2)

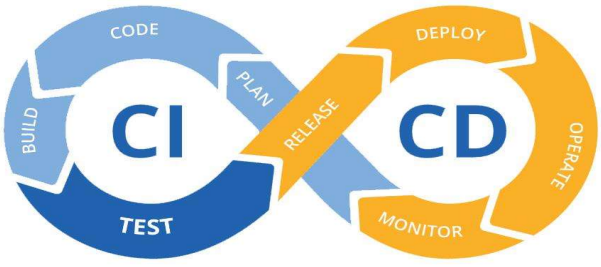
DevOps : 개발(Development)과 운영(Operation)합성어 협업을 통한 지속적 향상 강조

- 빠른 작업 속도
- 신속한 제공
- 안정성 향상
- 높은 확장성
- 협업 강화
- 보안체계 유지



CI/CD : 어플리케이션 개발단계부터 배포까지 모든 단계들을 자동화 하여 효율적 배포 진행

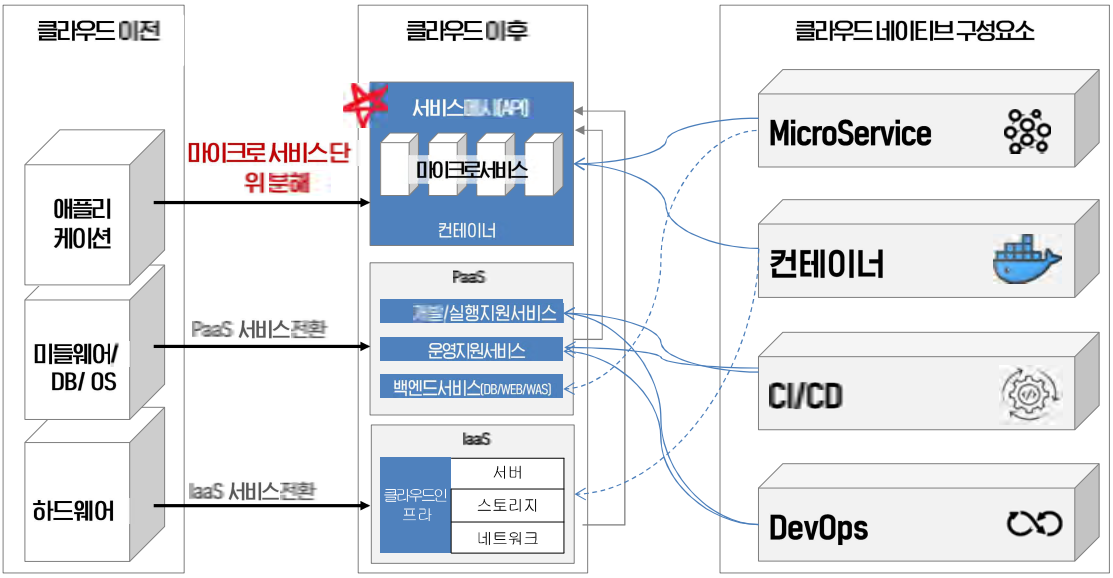
- CI (Continuous Integration) : 버그 수정 또는 새로운 기능이 Main Repository에 주기적으로 빌드 / 테스트 되어 통합하는 것
- CD (Continuous Deployment) : 변경이 출시되자 마자 자동으로 사용자에게 배포되는 모든 과정을 자동화 하는 것



01 클라우드 네이티브 구성요소

클라우드 네이티브 개발 및 인프라 환경

클라우드 환경에 적합한 애플리케이션의 단위 및 배포 환경



02 마이크로서비스

마이크로서비스 정의

가트너에서 제시한
마이크로서비스 기능 모델

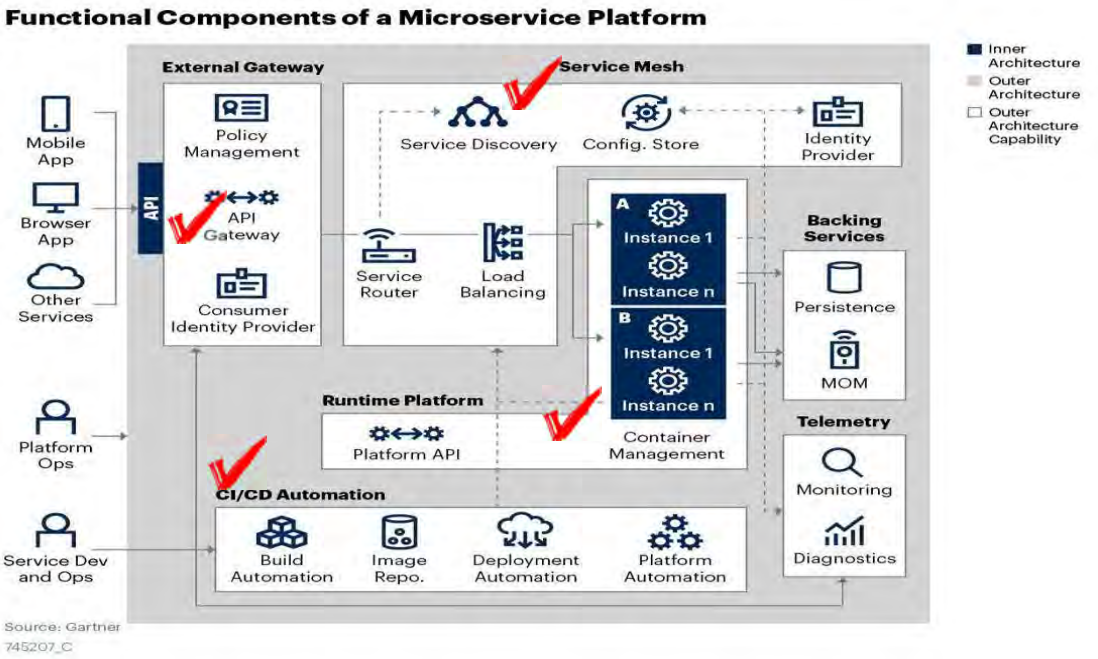
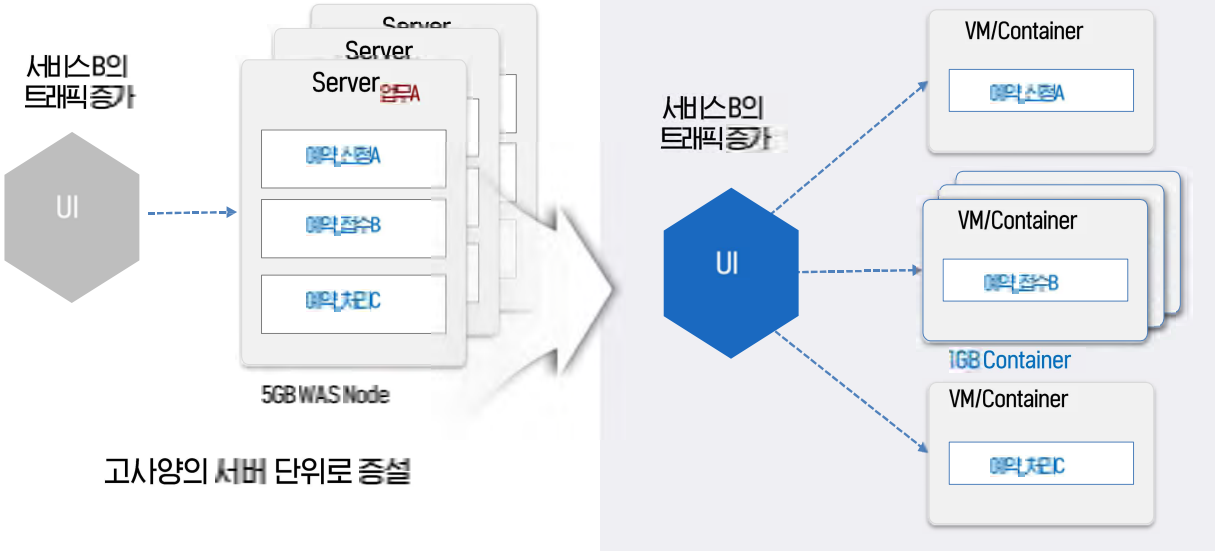


그림. 1 Functional Components of Micro Service Platform (출처: Gartner)

02 마이크로서비스

마이크로서비스 특징 – 유연한 확장성

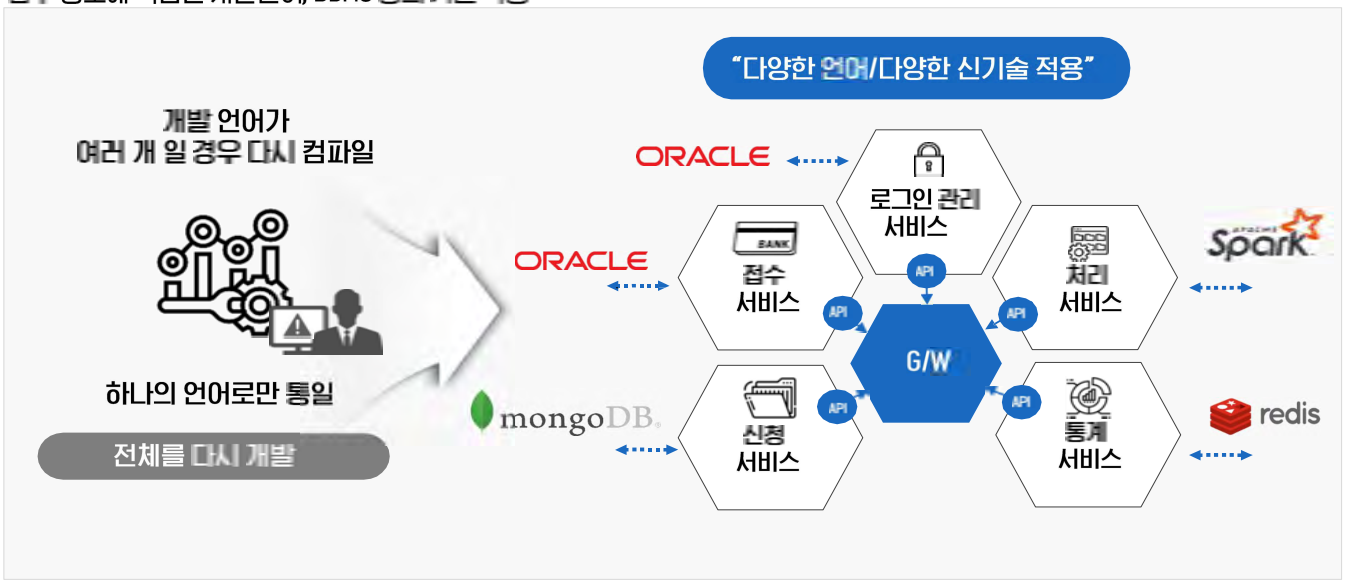
탄력적, 선택적인 서비스 확장 제공하는 방식으로 단위 업무 부하에 따라서 선택적으로 자원을 증가하여 대응



02 마이크로서비스

마이크로서비스 특징 – 폴리그랏

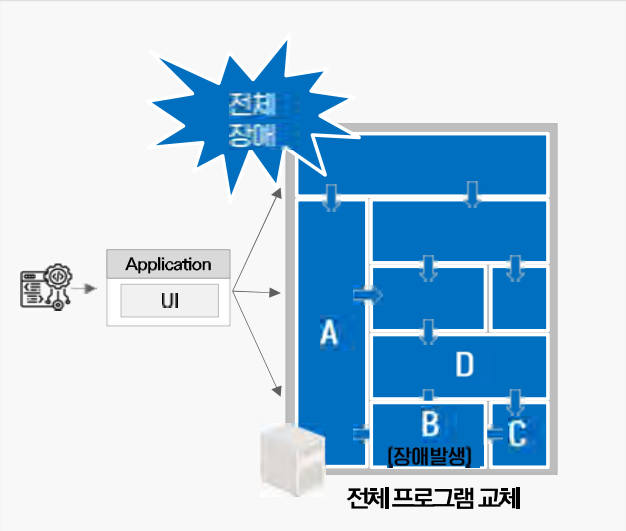
기존에는 요구사항이나 전체를 다시 개발 빠른 요구에 대응 부합하는 선택적 개발
업무 용도에 적합한 개발언어, DBMS 등의 기술 적용

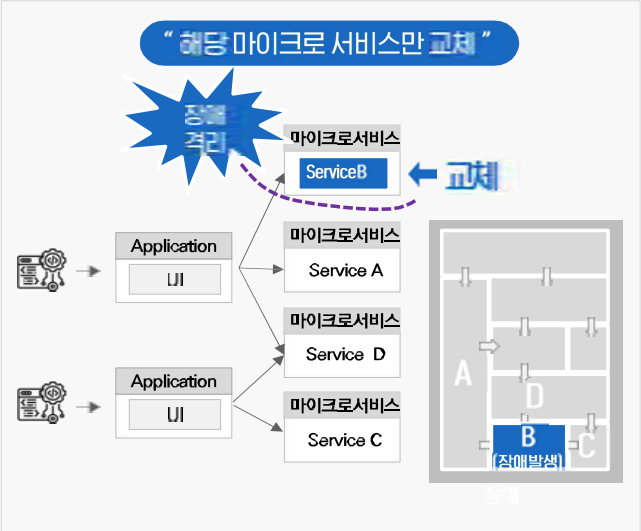


02 마이크로서비스

마이크로서비스 특징 – 장애 격리

탄력적, 선택적인 서비스 확장을 제공 작은 서비스 단위로 업데이트, 변경 및 교체를 제공하며
마이크로서비스별 격리를 통하여 전체 장애 전파를 최소화

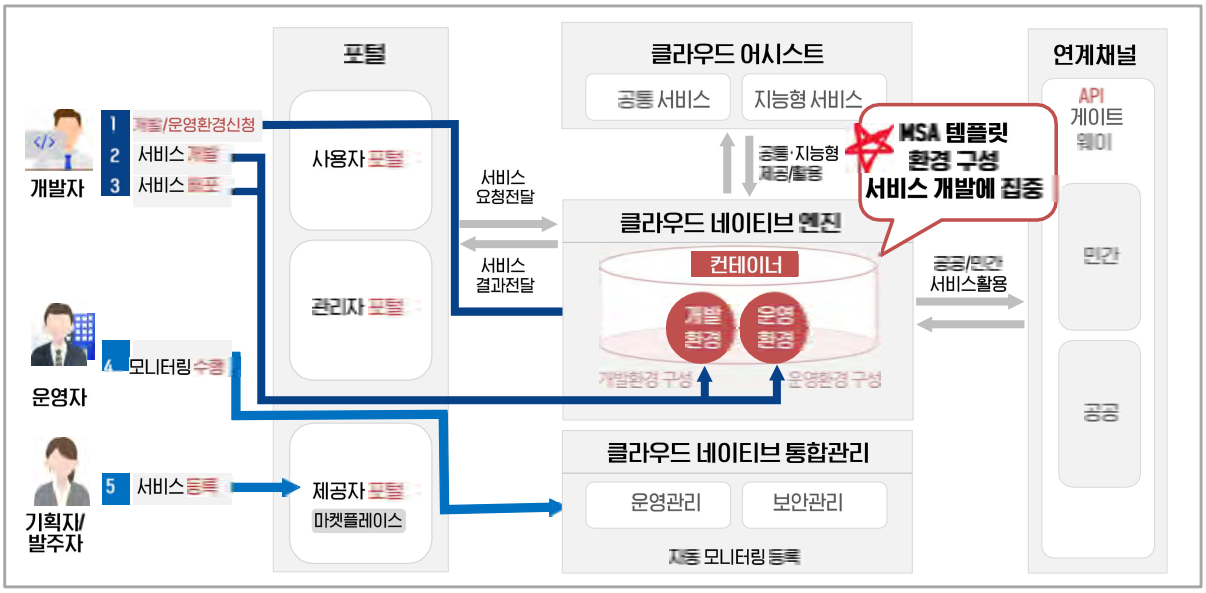




03 클라우드 네이티브 애플리케이션 구현

클라우드 네이티브 애플리케이션 – 전자정부 클라우드 플랫폼 기반

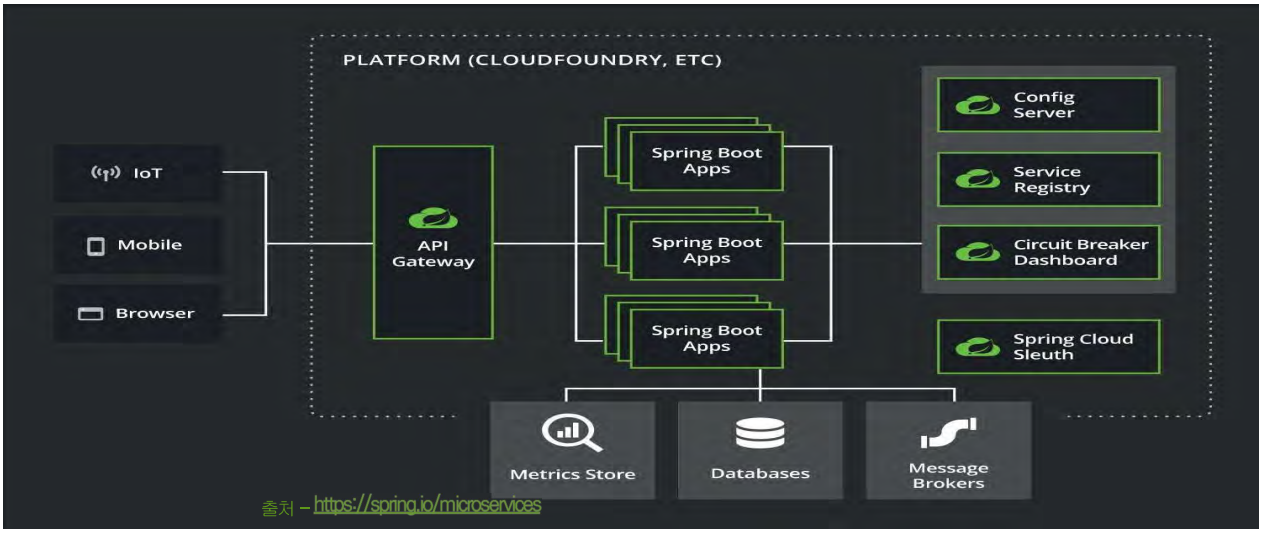
개발 초기 단계부터 제공되는 템플릿을 배포해보면 빠르게 환경 구성하여 서비스 개발에 집중



03 클라우드 네이티브 애플리케이션 구현

Spring Cloud 기반의 Service Mesh 구현

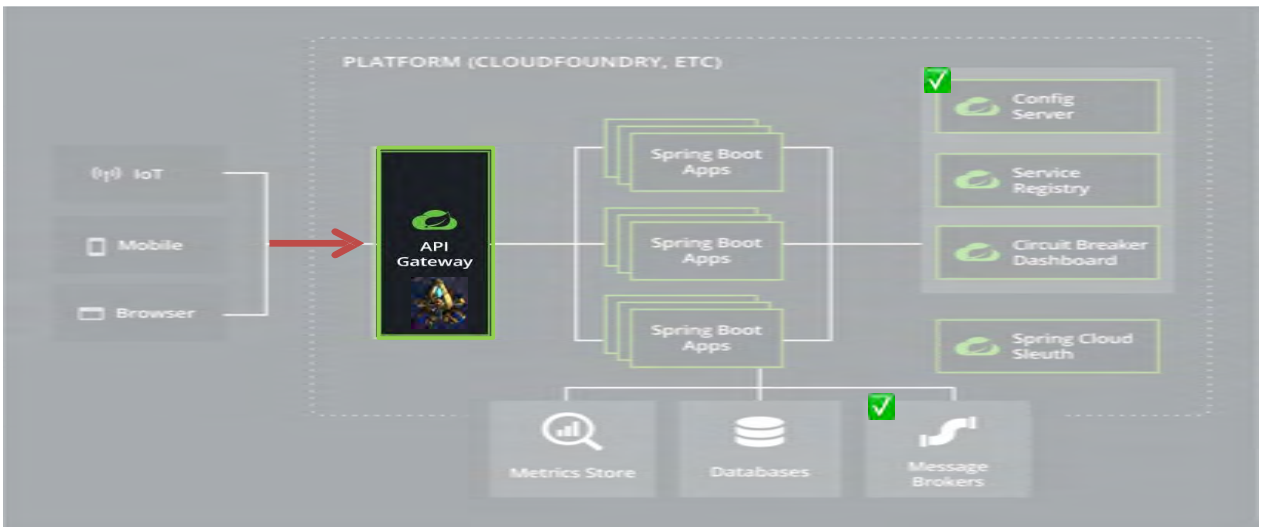
하나의 시스템을 여러 시스템으로 나누었지만 서로 데이터를 공유하고 통신할 수 있도록 구성.



03 클라우드 네이티브 애플리케이션 구현

Spring Cloud 기반의 Service Mesh 구현 – API G/W

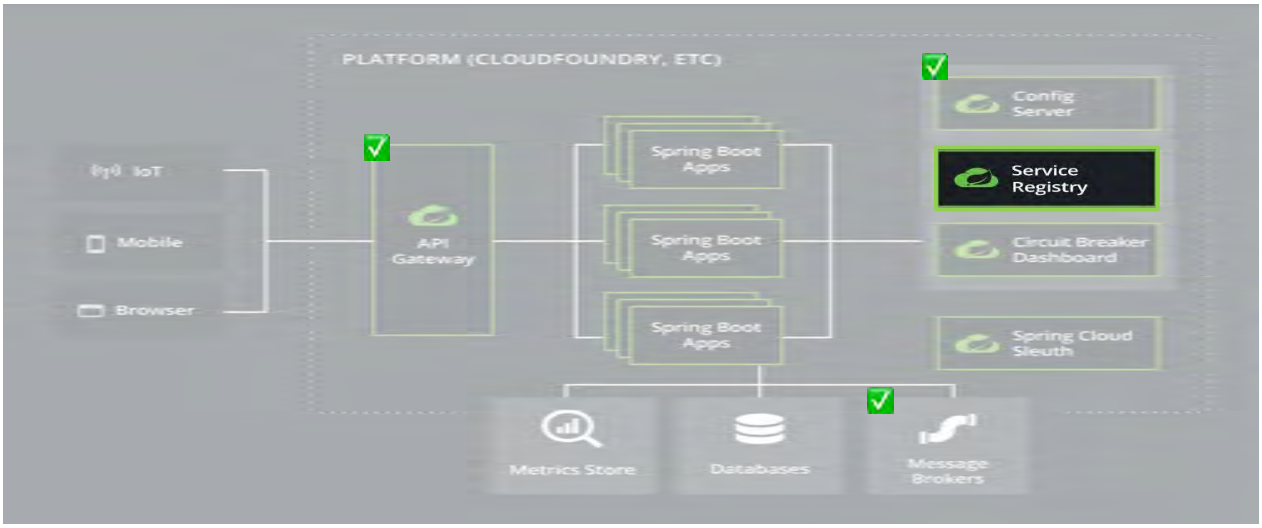
외부의 모든 요청을 처리하는 단일 진입점, 인증/인가/로깅 등 처리 후 대상 서비스로 라우팅



03 클라우드 네이티브 애플리케이션 구현

Spring Cloud 기반의 Service Mesh 구현 – Service Registry/Discovery (Eureka Server)

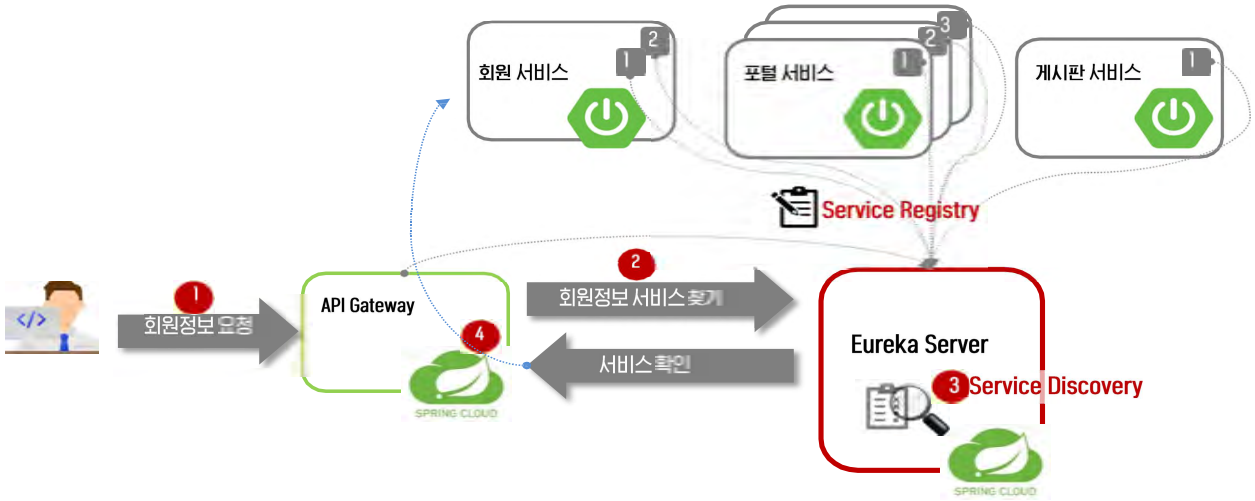
여러 마이크로서비스들을 등록하여 관리하고 API 요청 시 해당 서비스를 찾아 호출



03 클라우드 네이티브 애플리케이션 구현

Spring Cloud 기반의 Service Mesh 구현 – Service Registry/Discovery (Eureka Server)

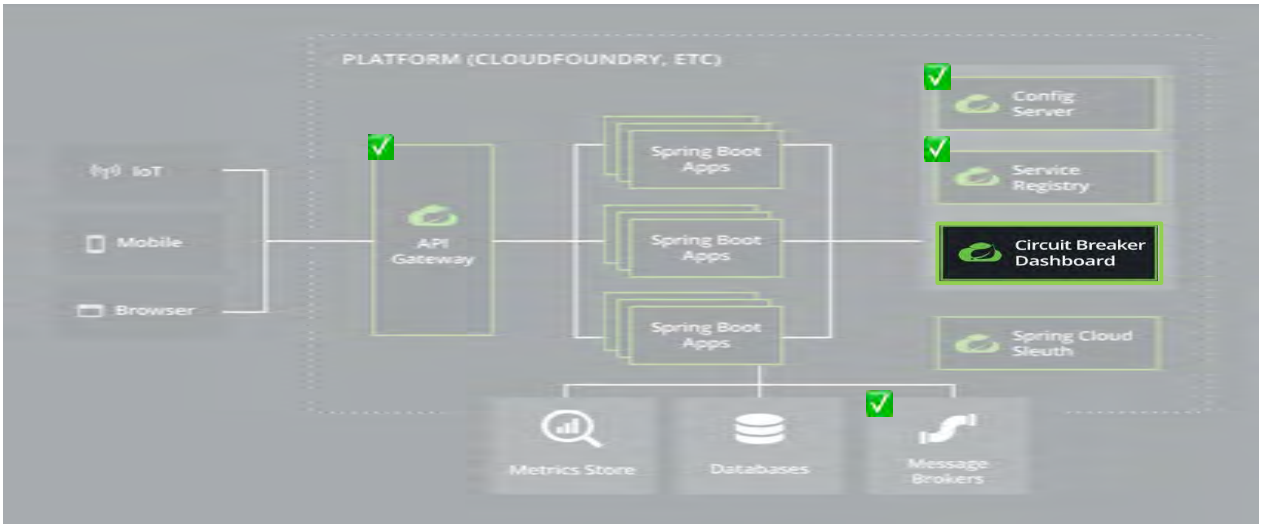
마이크로서비스 인스턴스들이 Eureka Server에 자신을 등록하면 API 요청 시 해당 서비스를 찾아 연결



03 클라우드 네이티브 애플리케이션 구현

서비스 매쉬에 대한 이해 – Circuit Breaker

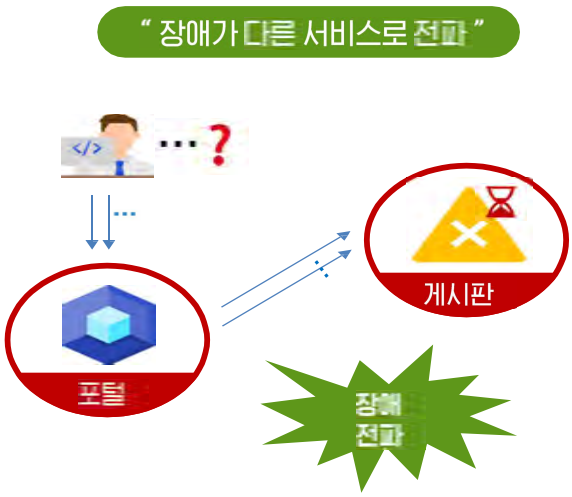
서비스의 장애가 다른 서비스에 전파되지 못하도록 막음

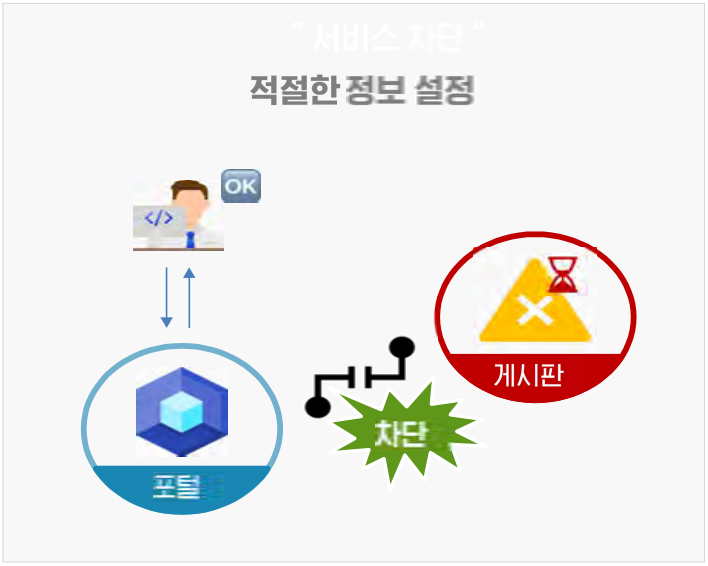


03 클라우드 네이티브 애플리케이션 구현

서비스 매쉬에 대한 이해 – Circuit Breaker

서비스 간 통신 시 응답 지연 등의 장애 발생 시 요청 차단

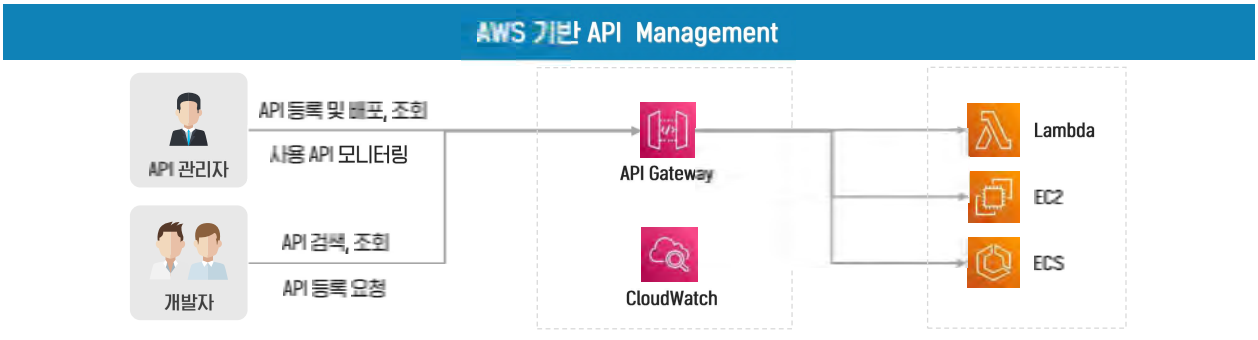




03 클라우드 네이티브 애플리케이션 구현

API Gateway에서의 API 관리

Amazon API Gateway 기반으로 개발자가 API를 손쉽게 생성, 게시, 유지 관리, 모니터링 및 보안 유지할 수 있도록 하는 환경을 제공하고 RESTful API 및 WebSocket API를 지원

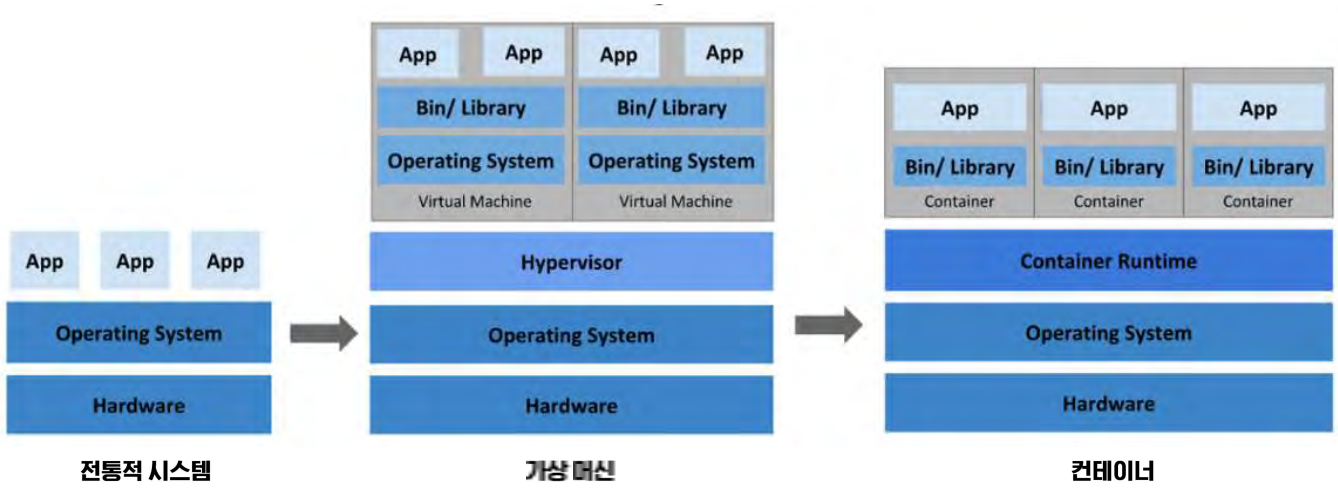


손쉬운 API 생성 및 배포	API 인증 및 권한 부여	API 버전 관리	API 작업 모니터링
•API Gateway 콘솔을 통하여 REST API 및 관련 리소스와 메서드 정의 •API 수명 주기 관리, 클라이언트 SDK 생성, API 지표 조회 기능 지원	•API Gateway는 API 요청의 인증을 위한 REST API 및 WebSocket API용 서명 •서명 버전 4는 IAM주) 및 액세스 정책을 통해 API 및 다른 모든 AWS 리소스에 대한 액세스 권한 부여	•여러 버전의 API 실행 가능 (최신 버전 게시된 후에도 어플리케이션에서 이전 API 버전을 계속 호출 가능) •API 버전별로 여러 릴리스 단계 관리 가능	•API Gateway 대시보드를 통해 서비스에 요청된 호출을 모니터링 가능

04 컨테이너

가상 머신, 컨테이너 시스템 구성 차이

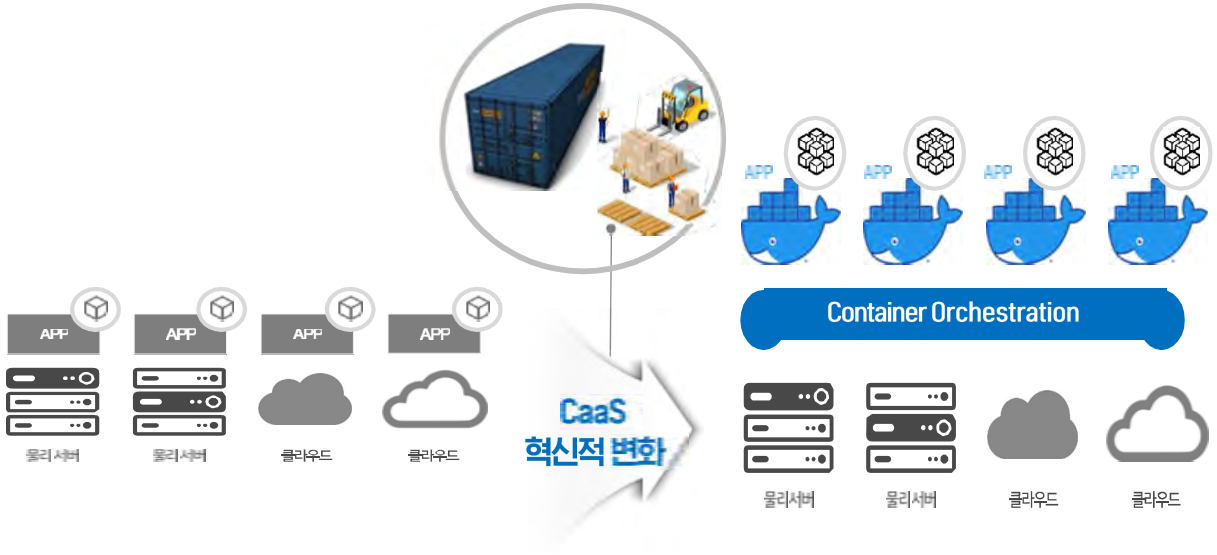
가상 머신은 전통적 시스템 대비 Hypervisor가 추가되어 여러 개의 VM 수행
컨테이너는 VM 대비 Guest OS, Hypervisor 부분 제외되어 이미지 용량 축소, 이기종 OS에서의 이식성 증가



04 컨테이너

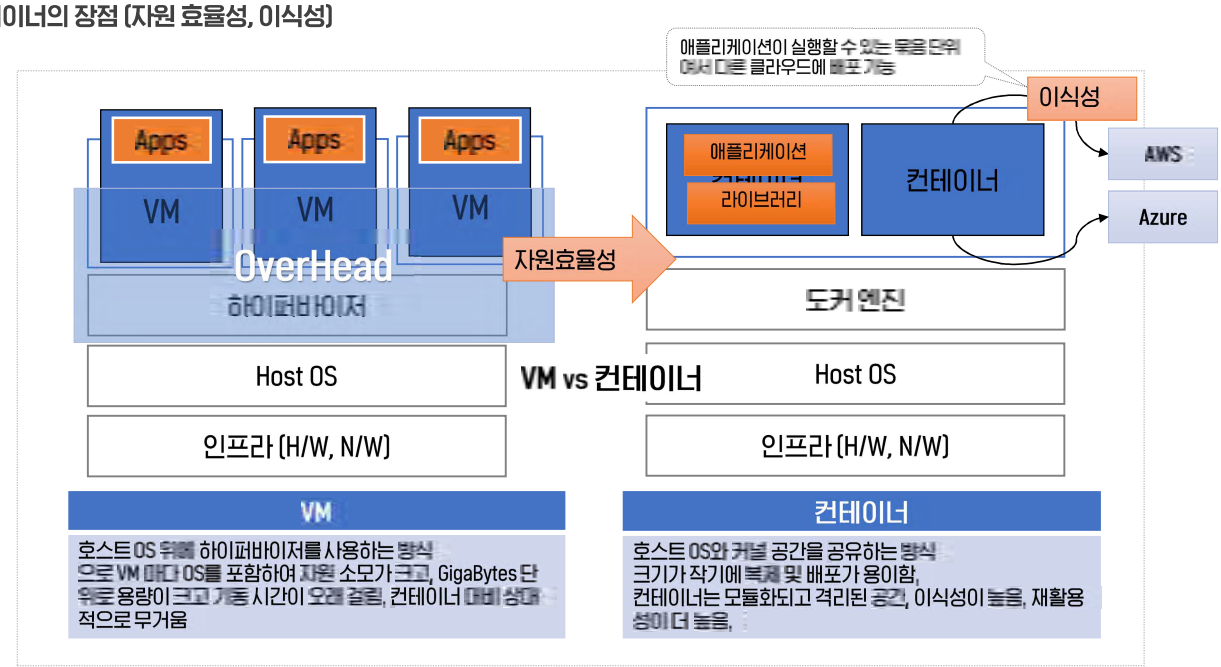
컨테이너 기술

컨테이너 기술을 기반으로 이식성을 제공, CaaS(Containers-as-a-Service)를 통한 서비스 개발 및 운영의 현대화



04 컨테이너

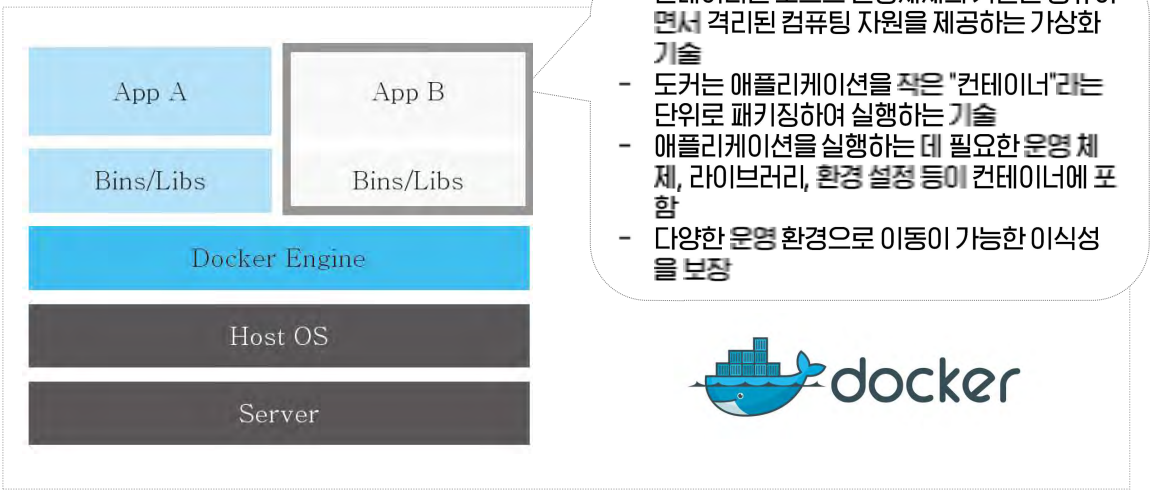
컨테이너의 장점 (자원 효율성, 이식성)



04 컨테이너

컨테이너 관리 기술 – 도커

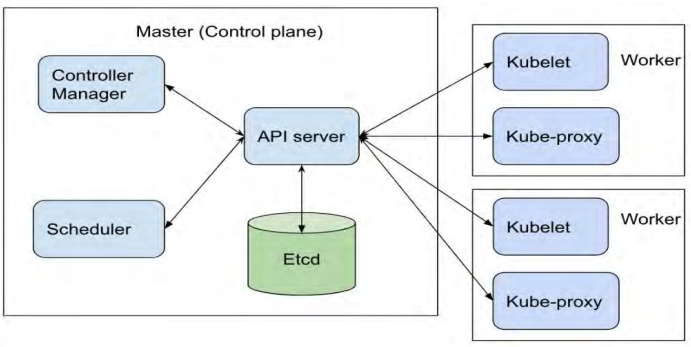
도커(Docker)는 컨테이너화 기술을 사용하여 애플리케이션을 실행하고 배포하는 오픈 소스 플랫폼
애플리케이션(컨테이너 이미지)를 배포 및 구동할 수 있는 컨테이너 엔진의 종류



04 컨테이너

컨테이너 관리 기술 – 쿠버네티스

쿠버네티스(Kubernetes)는 구성 요소: 컨트롤 플레인(마스터), 클러스터 상태 저장 Etcd, 클러스터 노드(kubelet)



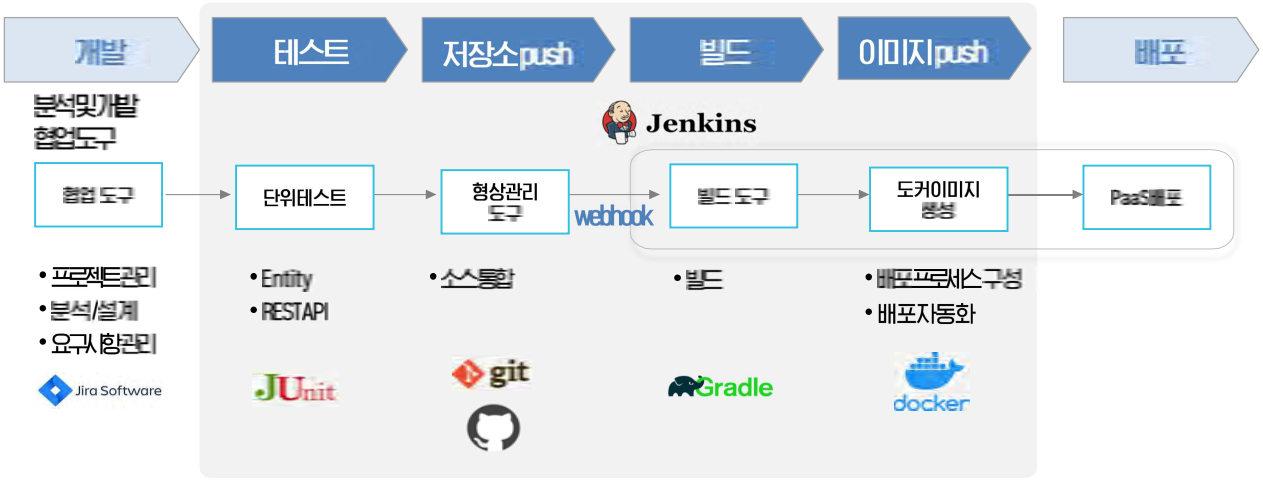
Control Plane 컨트롤 플레인
- 3개 주요 컴포넌트가 실행
- Kube-apiserver, kube-controller-manager, kube-scheduler
- 쿠버네티스 서비스의 상태 저장 스토리지 서비스 – Etcd
- Etcd – 분산 시스템 데이터를 저장하는 key-value 방식 저장

Worker 워커 노드
- 컨트롤 플레인으로부터 부여 받은 컨테이너가 실행되는 노드
- Kubelet은 Docker, Containerd 같은 컨테이너런타임을 이용해 컨테이너를 수행하는 역할
- Kube-proxy는 노드에서 실행되는 네트워크 프록시로, 노드의 네트워크 규칙을 생성/관리 내부 컨테이너간의 통신, 외부와의 통신 가능

05 CI / CD

빌드 및 배포 자동 파이프라인

개발된 소스가 저장소에 올라가면 자동으로 빌드되고, 도커 이미지가 생성되어 도커 레지스트리에 업로드 후 서비스가 배포됨



왜 클라우드 네이티브를 도입해야 하나요?

III 클라우드 네이티브 도입 및 전환

01 클라우드 네이티브 동향
02 클라우드 네이티브 도입 사례
03 클라우드 네이티브 적합성 검토

01 클라우드 네이티브 동향

클라우드 네이티브 국내 동향

현재 국내외 클라우드 시장은 IaaS에서 PaaS 중심으로 이동

개발자를 위한 플랫폼 서비스, PaaS

경쟁력 있는 PaaS가
SaaS 및 IaaS 점유율 확대의 원천

운영체제 | 실행 환경 | 개발 환경
분석환경 | 데이터 베이스 | 웹 서버

클라우드 서비스의 차별성 PaaS가 결정

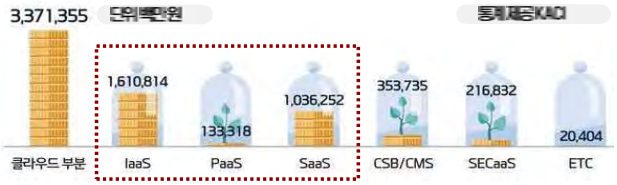
글로벌 PaaS 시장 규모 2026년까지 연평균
19.6%로 성장 예상

2020년 약67조 원 → 2026년 약196조 원

출처: '2026년까지 서비스로의 플랫폼 시장' 보고서

국내 PaaS 시장의 무한한 가능성에 주목해야 할 시점

2019년 국내 클라우드 서비스 부문별 매출 현황



IaaS와 SaaS 성장세는 이미 정점

클라우드 시장 확대와 함께 국내 PaaS 시장 성장 필수

PaaS 시장의 성장 가속 시점 도래

02 클라우드 네이티브 도입사례

클라우드 네이티브 국내외 도입 사례

선진 사례

AWS

빠른 배포 구현

수 천개 팀(자율적 DevOps팀) X 마이크로서비스 아키텍처
X 지속적 배포(CD) X 다양한 개발 환경

넷플릭스

가입자 대상서비스 확대

Netflix Open Source Software Center

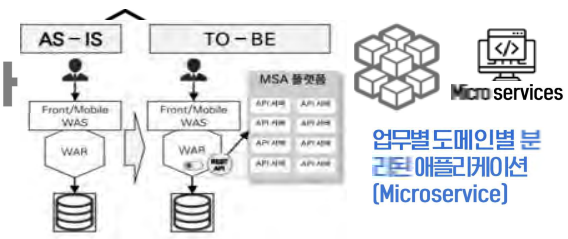
카카오

계열사 신규서비스 확대 및 빠른 출시사례

카카오의 애자일 문화, 일하는 방식 관리를
위한 전담팀 및 개발플랫폼 운영

11번가

서비스 분리를 통한 점진적 MSA 전환

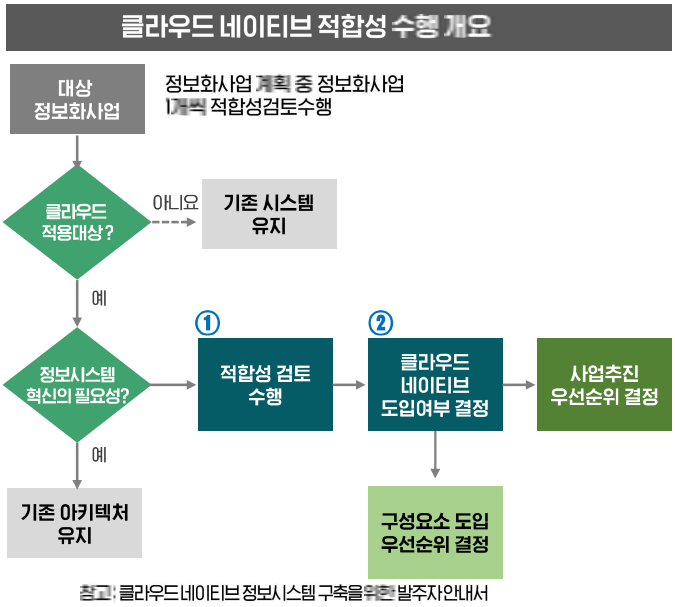


업무별 도메인별 분리된 애플리케이션 (Microservice)

03 클라우드 네이티브 적합성 검토

클라우드 네이티브 적합성 수행

클라우드 적용 및 아키텍처 상 클라우드 네이티브 도입 여부 확인하여 수행



참고: 클라우드네이티브 정보시스템 구축을위한 발주자안내서

III 클라우드 네이티브 도입 및 전환

03 클라우드 네이티브 적합성 검토

NIA 한국지능정보사회진흥원

클라우드 네이티브 적합성 수행

클라우드 네이티브 적합성 검토 체크리스트 및 도입 여부 결정 기준

① 클라우드 네이티브 적합성 검토 체크리스트 활용

목표 구분	적합성 검토 항목	질의사항
정책 및 업무 변화 대응	정책 및 업무 변화에 대한 민첩한 대응	1-1. 한국판 뉴딜과 같은 새로운 정책, 기관별 업무계획 등 다양한 정보화 요구사항 변화에 대해 신속한 대응이 필요합니까?
	디지털 혁신 및 지능화 지원	1-2. 디지털 혁신 및 지능 정보화 관련 신기술(빅데이터, AI, 블록체인, IoT 등)의 도입이 필요하고, 연관된 애플리케이션의 개발 또는 개선이 요구됩니까?
안정적 서비스 운영	서비스 개선 요구사항 적시 대응	2-1. 서비스 이용자의 잦은 CSR(Customer Service Request, 고객의 서비스 요구사항)에 대해 적시 대응이 필요합니까? 또는 초기 개발비의 약 15% 이상을 매년 추가개발 및 유지보수 비용으로 사용하고 있습니까?
	접속 지연, 서비스 장애 문제 신속한 해결	2-2. 다양한 원인에 의한 장애 발생 시 장애복구(예.시스템 증설, 업그레이드 등)를 위해 서비스를 중단한 적이 있습니까? 또는 이용자의 폭증에 의한 접속지연으로 이용자의 불만이 제기된 적이 있습니까?
	소규모 서비스 분리 및 독립적 운영	2-3. 소규모 서비스 단위로 기능과 DB가 명확하게 분리되고, 독립적으로 서비스를 실행할 수 있습니까? (공통 기능 및 데이터 사용 유무, 타 시스템과의 연계성, 서비스 의존 관계 등 확인)
	다양한 플랫폼 환경에서의 이식성 보장	2-4. 개발-테스트-운영 환경에서 안정적이고 지속적인 배포가 필요하거나 다양한 플랫폼 환경에 애플리케이션 배포가 요구됩니까?
개발 품질 향상	개발·운영 협업 조직체계 구현	3-1. 시스템 개발 및 운영 시 개발팀과 운영팀의 분리에 의한 의사소통의 문제, 개발 및 배포 지연 등의 문제가 존재합니까?
	전문인력 역량 강화	3-2. 개발-빌드-배포 과정의 품질 향상을 위해 전문 인력을 확보하거나 기존 인력에 대한 전문적인 교육이 필요합니까?
개발 생산성 향상	코딩-빌드-테스트-배포 파이프라인 자동화	4-1. 개발된 SW를 형상관리 시스템에 커밋한 후 개발/검증/운영 서버에서 각각 빌드, 테스트, 배포하는 과정 전체에 대해 자동화 도구를 도입하거나 추가할 필요가 있습니까?
	기술 반영 용이성 확보	4-2. 오픈소스 SW를 비롯한 다양한 기술의 도입, 업그레이드, 업데이트 등 작업 수행 시 연관된 서비스에 대한 변경 작업이 복잡하여 개발 상의 어려움을 겪은 적이 있습니까?

② 클라우드 네이티브 도입여부 결정 기준

"예"응답수	도입여부 결정 기준	비고
1개 ~ 3개	• 기존의 애플리케이션 아키텍처 유지	• 적합성 검토 항목의 답변을 기준으로 클라우드 네이티브 구성요소를 부분적으로 도입
4개	• 기존의 애플리케이션 아키텍처 유지 • 필요시 클라우드 네이티브 구성요소 일부 도입 가능	
5개	• 클라우드 네이티브 도입 가능	
6개 ~ 8개	• 적극적으로 클라우드 네이티브 도입	
9개 ~ 10개	• 적극적으로 클라우드 네이티브 도입	• 우선적으로 정보화사업 추진

클라우드 환경에서의 정보보호 관리체계 수립

NHN Cloud
박관규 이사

행정안전부 NIA 한국지능정보사회진흥원

CONTENTS

클라우드 환경에서의 정보보호 관리체계 수립

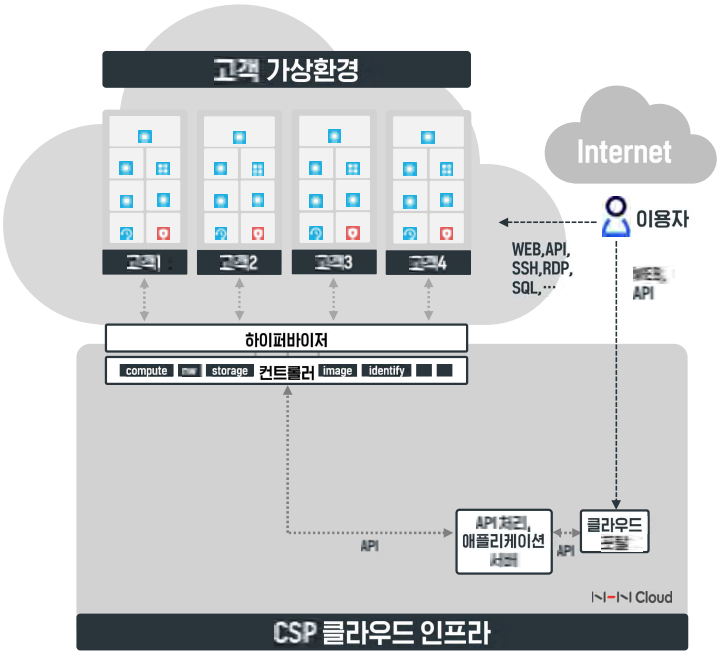
I 클라우드 보안 개요

행정안전부
NIA 한국지능정보사회진흥원

NIA 한국지능정보사회진흥원

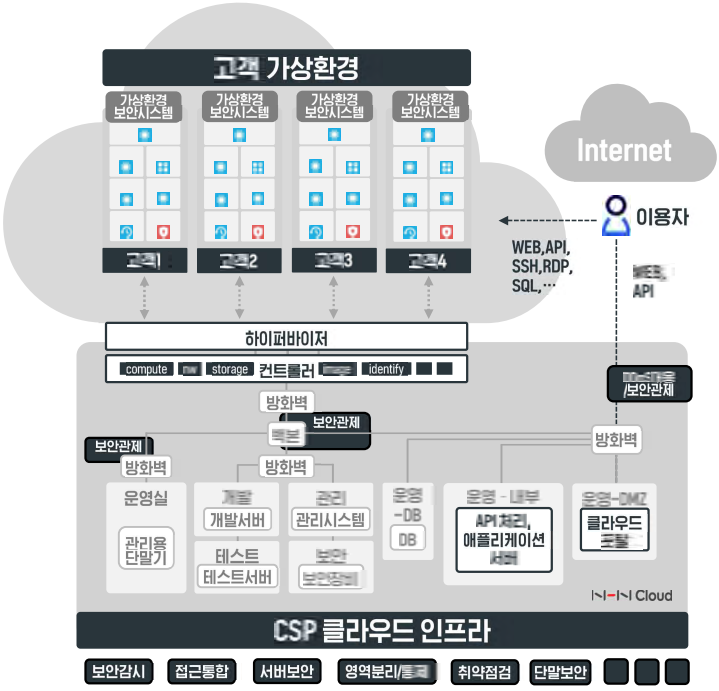
01 클라우드 기본 구조와 보안

상용 클라우드 기본 구조



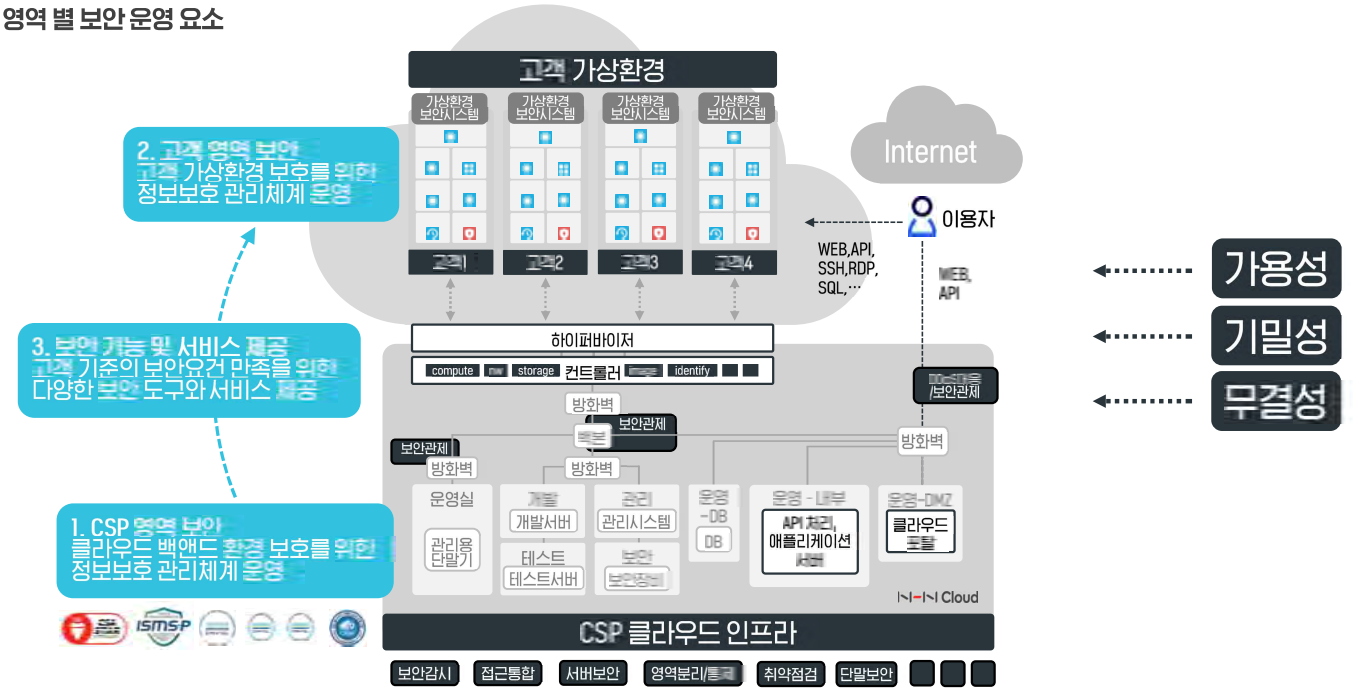
01 클라우드 기본 구조와 보안

상용 클라우드 기본 구조



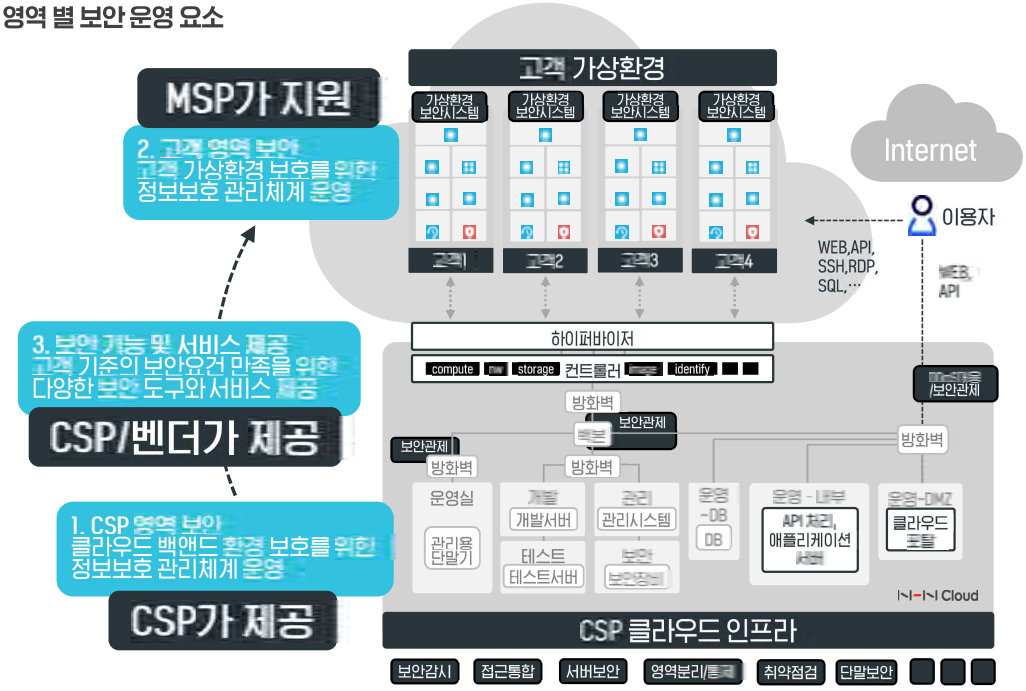
01 클라우드 기본 구조와 보안

영역 별 보안 운영 요소



01 클라우드 기본 구조와 보안

영역 별 보안 운영 요소



- 가용성
- 기밀성
- 무결성

02 클라우드 보안 책임 모델

이용 유형 별 관리/보안 주체를 인식하고 운영 필요

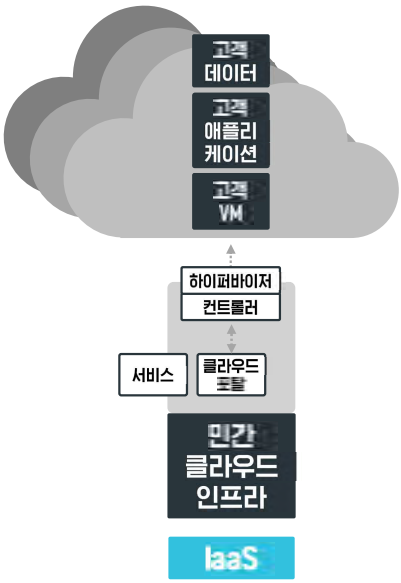
클라우드 책임 모델 예시

고객 | Cloud

보호 대상	보안 주체			
	레거시	IaaS	PaaS	SaaS
클라우드 포탈 고객 영역				
데이터				
어플리케이션				
가상 네트워크				
운영체제				
클라우드 소프트웨어				
하이퍼바이저				
물리 시스템 (시스템/스토리지/DB/네트워크)				
물리 시설				

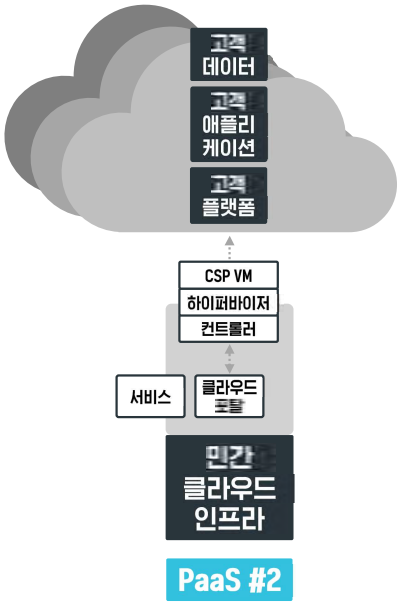
03 클라우드 이용 유형 분류

IaaS 및 SaaS 제공 구조



03 클라우드 이용 유형 분류

PaaS 제공 구조



클라우드 환경에서의 정보보호 관리체계 수립

II 주요 위협과 대비책

01 클라우드 주요 보안 위협
02 제로트러스트 개념
03 클라우드 보안 서비스 구조
04 주로 챙겨야 할 것들

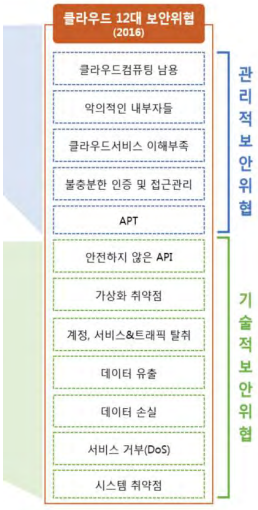
행정안전부
NIA 한국지능정보사회진흥원

NIA 한국지능정보사회진흥원

01 클라우드 주요 보안 위협

레거시와 유사하되 가상화 및 API 이슈가 강조됨

"CSA 클라우드 서비스의 보안위협 현황"
- 클라우드 정보보호 안내서 - KISA



"클라우드 서비스 관련 보안위협"
- 금융분야 클라우드컴퓨팅서비스 이용 가이드 - 금융보안원

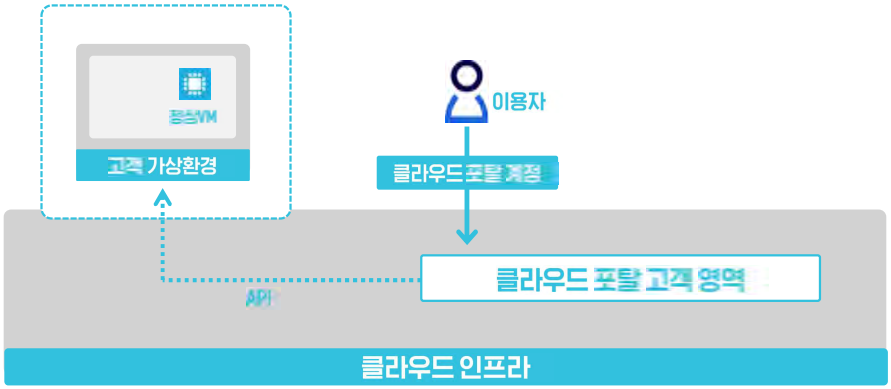
"클라우드 컴퓨팅 환경 구성 요소에 따른 보안 위협"
- 국가 공공기관 클라우드 컴퓨팅 보안 가이드라인 - 국가정보원

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	검사
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

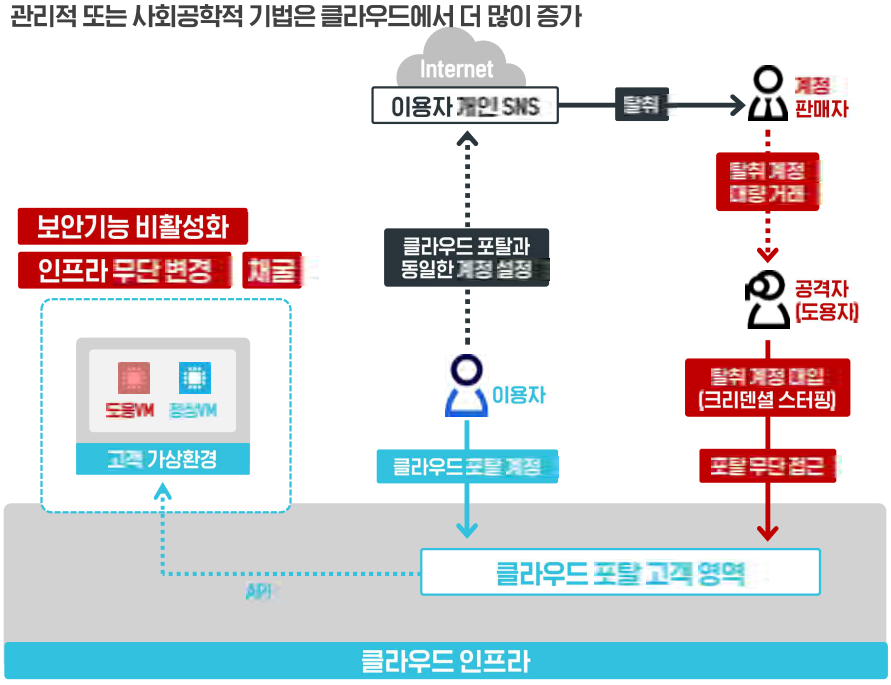
01 클라우드 주요 보안 위협

관리적 또는 사회공학적 기법은 클라우드에서 더 많이 증가



01 클라우드 주요 보안 위협

관리적 또는 사회공학적 기법은 클라우드에서 더 많이 증가

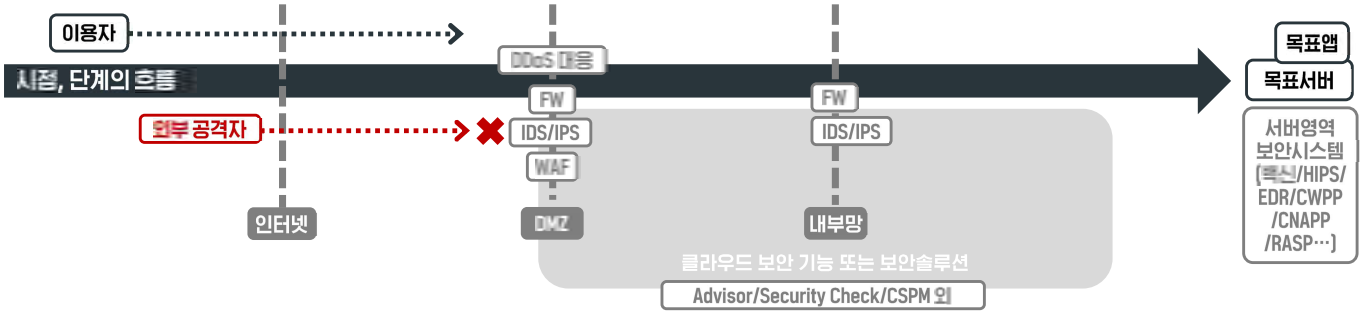


근절하거나 검증하기 어려운 영역

※자매품
- 개인 레파지토리에 회사 개발코드 저장
- 개인 PC로 회사 업무망 접속

02 제로트러스트 개념

지능적인 위협 요소들

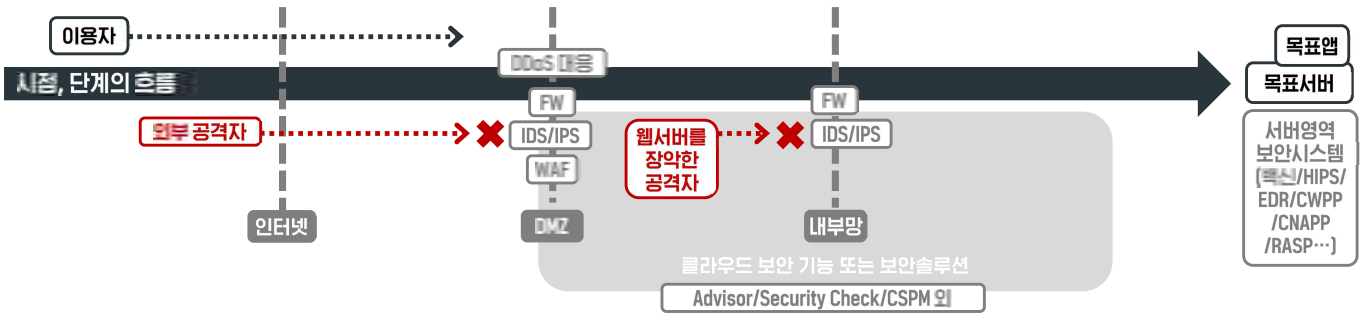


II 주요 위협과 대비책

02 제로트러스트 개념

NIA 한국지능정보사회진흥원

지능적인 위협 요소들

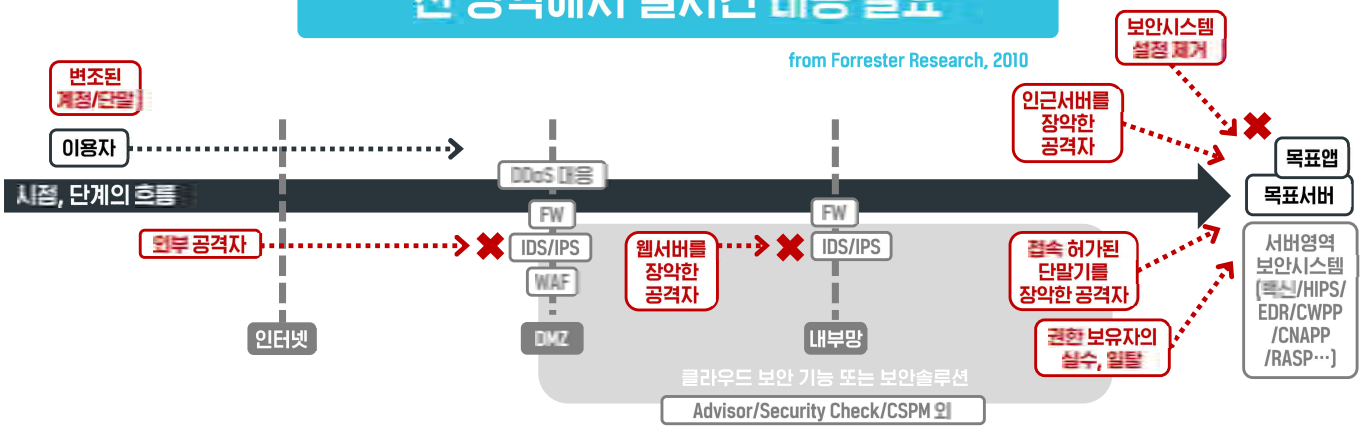


02 제로트러스트 개념

기본 개념

모든 신원/자산의 위협을 상시 식별하고, 전 영역에서 실시간 대응 필요

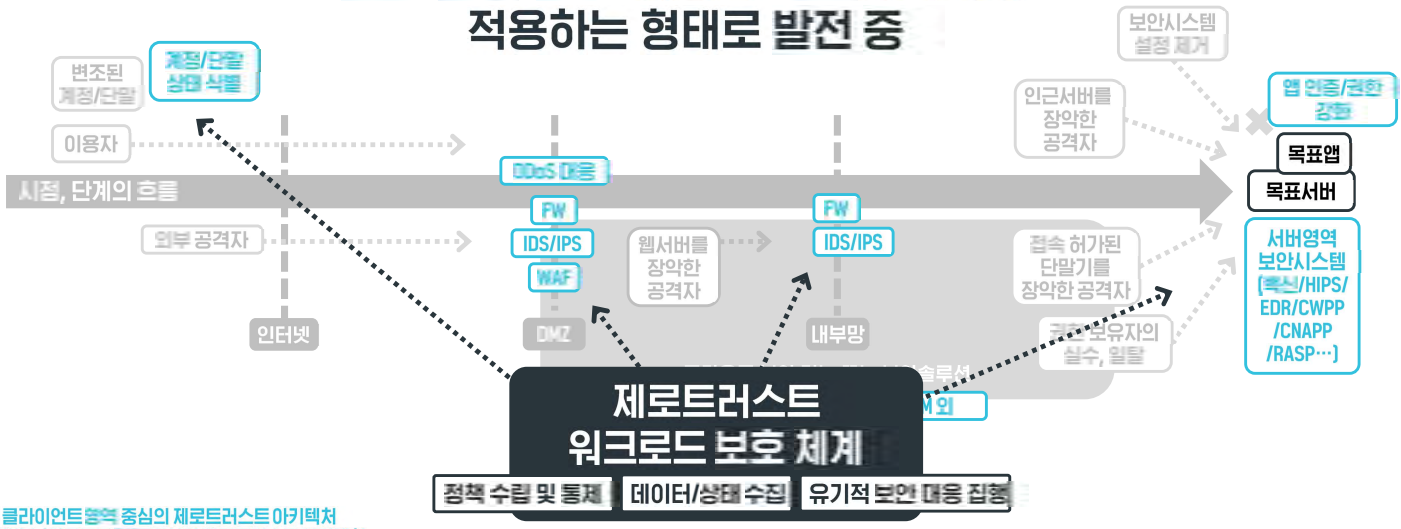
from Forrester Research, 2010



02 제로트러스트 개념

다각도 검토와 적용 필요

인증/통제/감시/대응을 모든 레이어에 적용하는 형태로 발전 중



※ ZTNA: 클라이언트 영역 중심의 제로트러스트 아키텍처
※ ZTA: 서비스/워크로드 영역 중심의 제로트러스트 아키텍처

02 제로트러스트 개념

업계 및 정책 추세

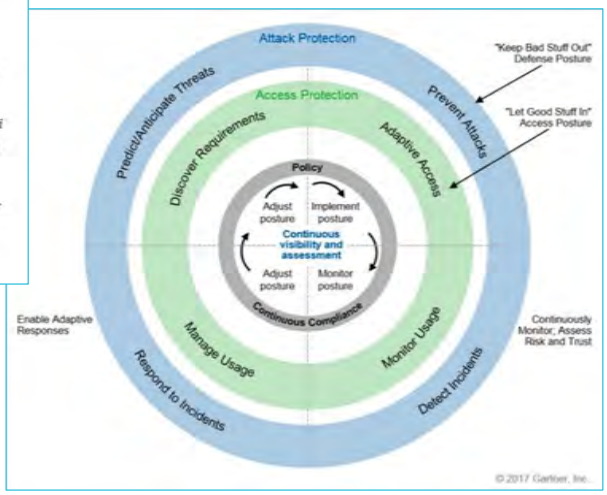
Gartner: "By 2023, 60% Of Enterprises Will Use the Zero Trust Security Model"

Alex Khomich · Follow
Published in InfoSec Write-ups · 5 min read · Jun 24, 2022

The research company Gartner, in its status report *Zero Trust Architecture and Solutions*, predicted the future of ZTA. By 2023, 60% of organizations will use a Zero Trust security model instead of virtual private networks. This is because the network infrastructure of enterprises is becoming more complex, and many employees work remotely. There are more loopholes for hackers to break into a corporate network and steal data. The Zero Trust approach to cybersecurity is designed to protect businesses from today's threats. Let's take a closer look at how it works.

✓ 관련 사상 강조 및 확산 중이며, 차세대 전략으로써 관심 집중

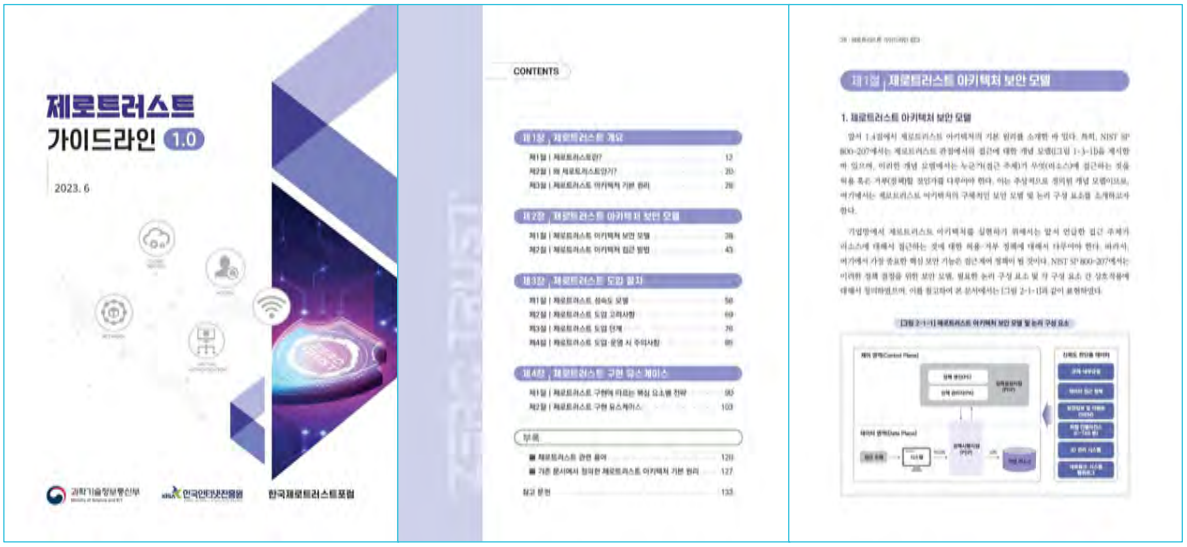
✓ 보안실효성 측면에서 반드시 필요하나, 개념 특성 상 장기적 노력과 투자 필요



02 제로트러스트 개념

업계 및 정책 추세

KISA 제로트러스트 모델링 가이드라인 배포 (23.6)
→ 전반적인 구성 요소와 모델링 방향을 명시



02 제로트러스트 개념

업계 및 정책 추세

금융 클라우드 이용가이드 (2023)

- 클라우드시스템을 통해 송수신되는 모든 정보에 대해서는 가능한 범위에서 기존의 금융회사 데이터 관리 및 통제 원칙을 적용
  - 특히, 클라우드 시스템 간의 접속 및 정보 송수신에 대해서도 외부시스템과 동일하게 통제를 적용하는 등 제로트러스트 모델(Zero Trust Model)*을 지향하여 설계
    * 내·외부 자원 모두 잠재적으로 악성 요인이 있음을 간주하고, 각 시스템이 모든 접근을 검증하도록 하는 모델
  - 필요 시, 클라우드 환경에서의 데이터 보안 및 관리 가시성 확보, 위협 탐지 및 접근 통제 등을 보조하는 솔루션 도입 등을 검토

국정원 계획 기사

2026년부터 정부 全기관에 K-제로 트러스트 적용된다

발행일 : 2023-07-19 12:29 지면 : 2023-07-20 18면

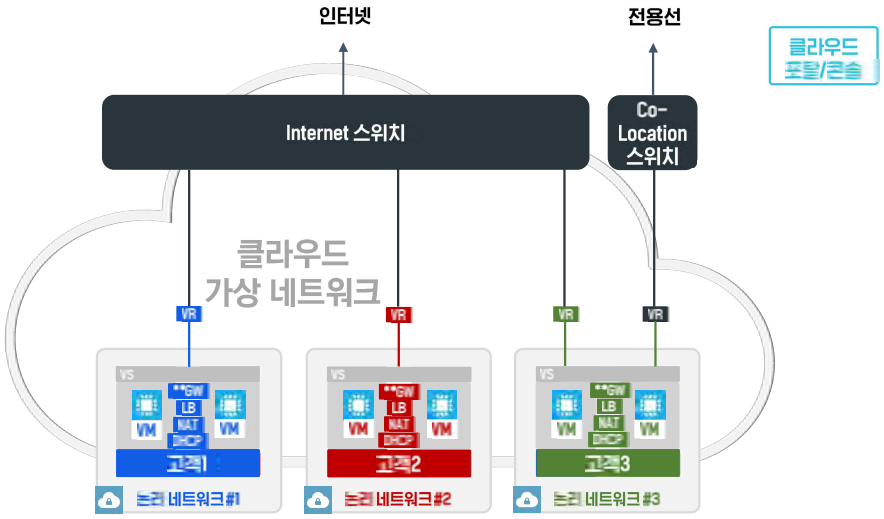
"2026년부터 전 국가·공공기관을 대상으로 한국형(K) 제로 트러스트를 적용하겠습니다."

백종욱 국가정보원 3차장은 19일 경기도 성남시 국가사이버안보협력센터에서 열린 기자간담회에서 "K-제로 트러스트 보안정책을 2024년부터 부처별로 시범 적용하겠다"면서 이 같이 밝혔다.

제로 트러스트는 '결코 신뢰하지 말고, 항상 검증하라'(Never trust, Always verify)는 핵심 철학을 바탕으로 기존 경계형 보안 체계를 보완하는 개념이다. 국정원은 지난해 8월부터 K-제로 트러스트 구축을 국정과제로 채택, K-제로 트러스트 아키텍처와 가이드라인 개발에 착수했다. 2024년까지 K-제로 트러스트 개발을 마치면 1년여간 시범 적용을 거친 후 범정부로 확대할 계획이다.

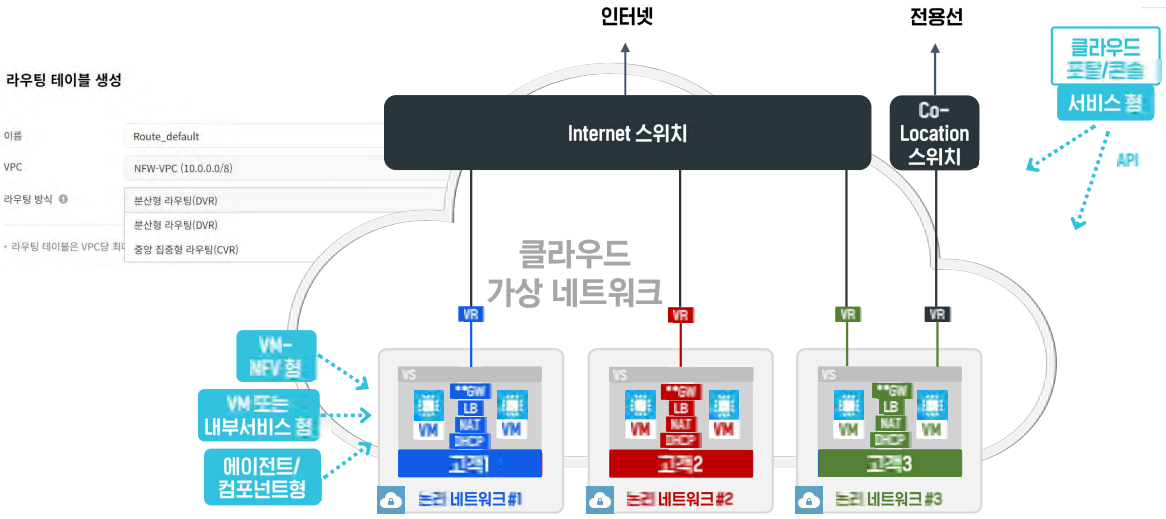
03 클라우드 보안 서비스 구조

동적 구현된 가상 네트워크에 보안 시스템을 조합



03 클라우드 보안 서비스 구조

동적 구현된 가상 네트워크에 보안 시스템을 조합



대규모 네트워크 생성/분리를 위한 동적 네트워크 기술로(예:SDN)
논리 네트워크 구현하고 그 위에 보안 기능 제공

NHN Cloud 소개 서비스

Security

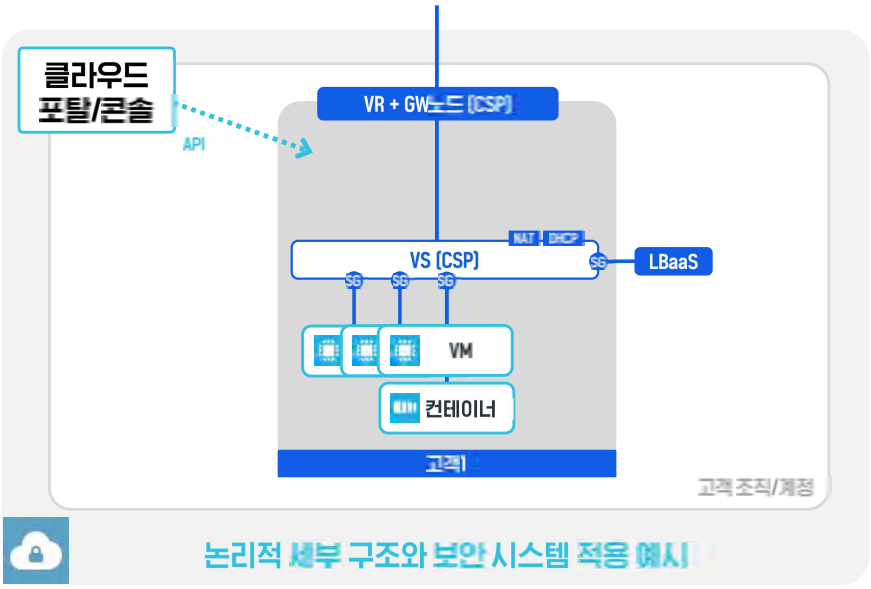
- NHN AppGuard
- App Security Check
- Server Security Check
- Webshell Threat Detector
- Security Monitoring
- Basic Security
- CAPTCHA
- OTP
- WEB Firewall
- Vaccine
- Secure Key Manager
- Security Compliance
- DDoS Guard
- SIEM
- Security Advisor
- Network Firewall NEW

주요 위협과 대비책

03 클라우드 보안 서비스 구조

NIA 한국지능정보사회진흥원

동적 구현된 클라우드 네트워크에 보안 시스템을 조합

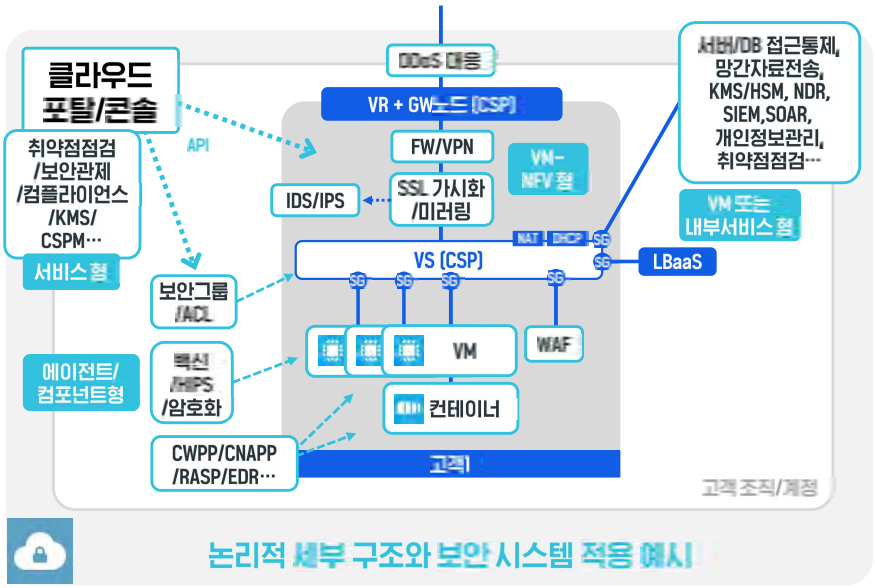


논리적 세부 구조와 보안 시스템 적용 예시

SDN/NFV를 활용한 보안 도구는
기 활용되고 있으며,
차세대 보안도구를 접목·배포하는
것은 CSP와 벤더들의 숙제

03 클라우드 보안 서비스 구조

동적 구현된 클라우드 네트워크에 보안 시스템을 조합



논리적 세부 구조와 보안 시스템 적용 예시

SDN/NFV를 활용한 보안 도구는
기 활용되고 있으며,
차세대 보안도구를 접목·배포하는
것은 CSP와 벤더들의 숙제

04 주로 챙겨야 할 것들

영역 별 주로 챙겨야 할 것들

1 계정 관리
- 콘솔/가상자원 계정 보안 (2차 인증, 접속지 제한 외)
- 조직/개인 별 권한 최소화, 직무분리 반영 등

2 접근통제
- 모든 접근자/목적지/경로/업무 식별 후 최소권한 부여
- 신규 유형 서비스, 오픈소스 등의 통제방안 사전 검토

3 네트워크 분리, 단말 연계
- 클라우드 접속 단말에 대한 보안 대책 적용
- 통제/감시나 분리 기준에 최적화된 네트워크 구성

4 암호화, 개인정보 보호
- 개인정보보호 가이드를 활용한 기술/관리적 체계 적용
- 클라우드 환경에서의 보안 시스템 특성 고려

5 로깅, 감사
- 가상자원 별 로그 요건 식별하여 로깅 적용
- 클라우드 콘솔, 신규 유형 서비스에 대한 로깅도 검토

6 보안 모니터링, 취약점 점검
- 접점/호스트 영역 상시 감시 및 대응체계 적용
- 클라우드 콘솔, 컨테이너 이미지 등도 점검 수행

7 가상서버영역 보안 강화
- 서버 관리방안 수립 및 적용 (생성/변경/회수 등)
- 기술 보안대책 적용 (악성코드/패치/무결성/암호화 외)

8 관리/운영 보안 적용
- 클라우드 운영 업무에 대한 조직/체계/절차 재정비
- 정보보호 체크리스트를 클라우드 기준으로 재점검

인프라 안전성 파워 게이지

Ⅲ 전환 간 주요 이슈

행정안전부
NIA 한국지능정보사회진흥원

01 물리 망분리

IT에서 말하는 분리

※ 퀴즈탐험 분리의 세계

1. 대역 분리 = 서브넷 이상으로 나눈다

2. 영역/환경 분리 = 서브넷 이상으로 나누고
   서로 간 통신을 제한하되 그 안의 시스템과
   관리계정 체계를 나눈다

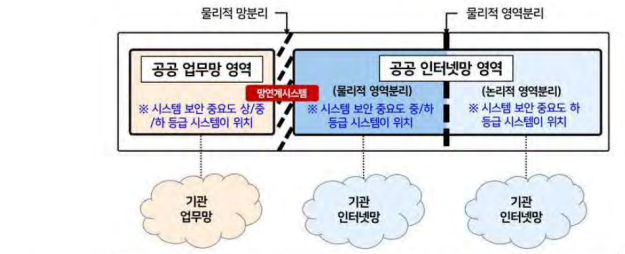
3. 망분리 = 서로 통신이 도달하지 않도록
   회선, 백본장비, 시스템과 관리계정 체계를 나눈다

01 물리 망분리

국정원 클라우드 망분리 기준과 주체 별 고민

공공 인터넷망 영역은
등급에 따라 완화 되었으나,

업무망 영역은
물리 망분리 요건 명확화



	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

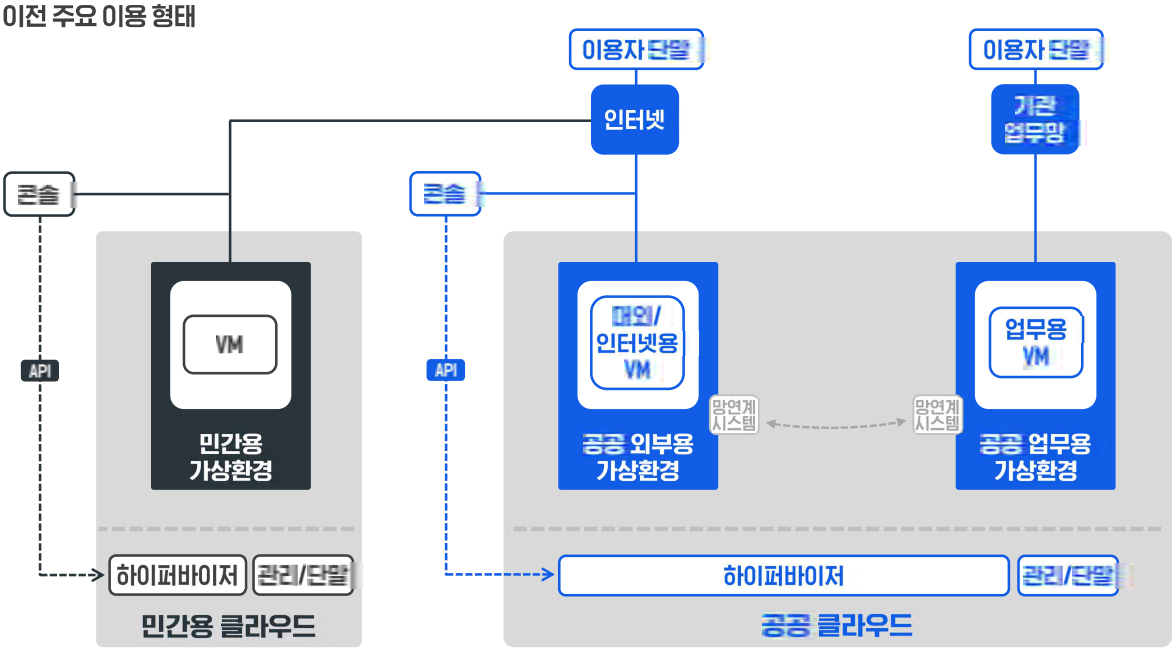
공공 업무망 영역

- 민간 서비스 영역과 물리적 영역 분리가 되어 있으며 공공 인터넷망 영역과 물리적 망분리된 영역
- 단, 공공 인터넷망 영역과 자료 전송 체계 구축 운영 가능

[국가 클라우드 컴퓨팅 보안 가이드라인(2023.01) – 제3장 제2절 클라우드 영역 분류]

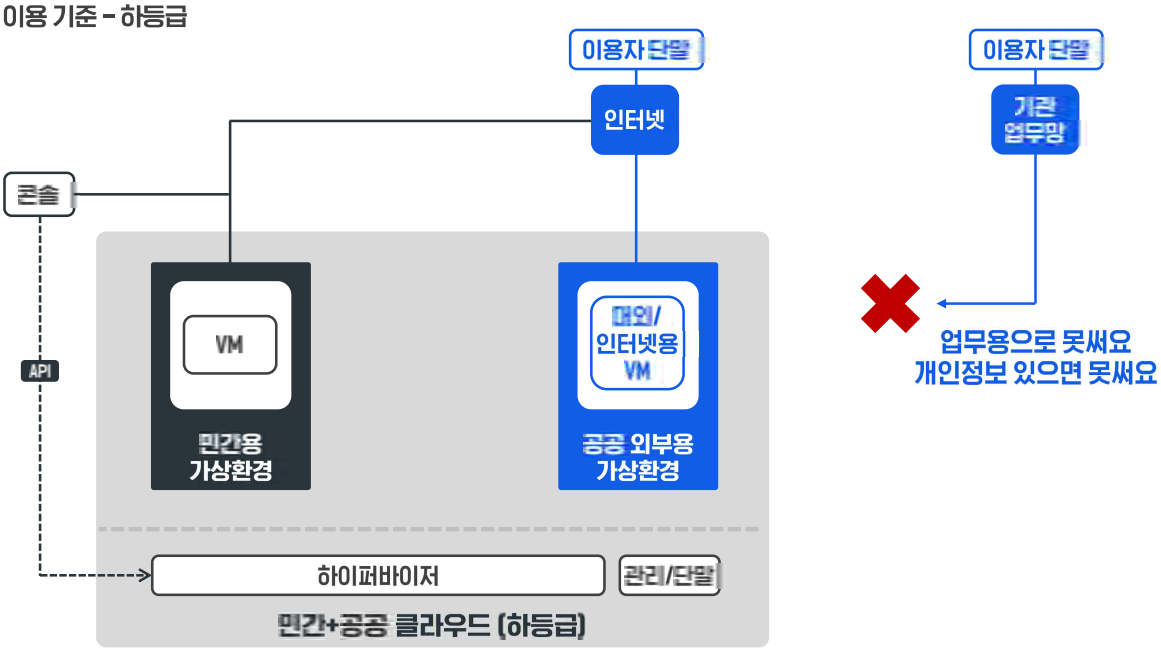
01 물리 망분리

2022 이전 주요 이용 형태



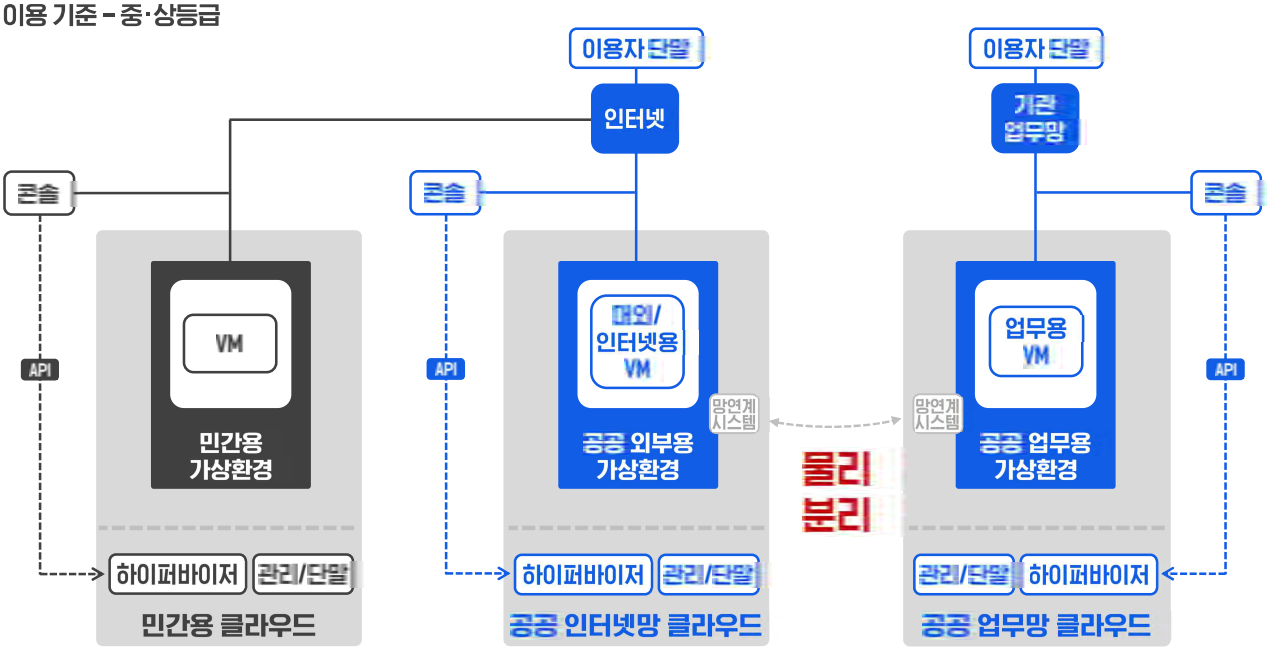
01 물리 망분리

2023 이용 기준 – 하등급



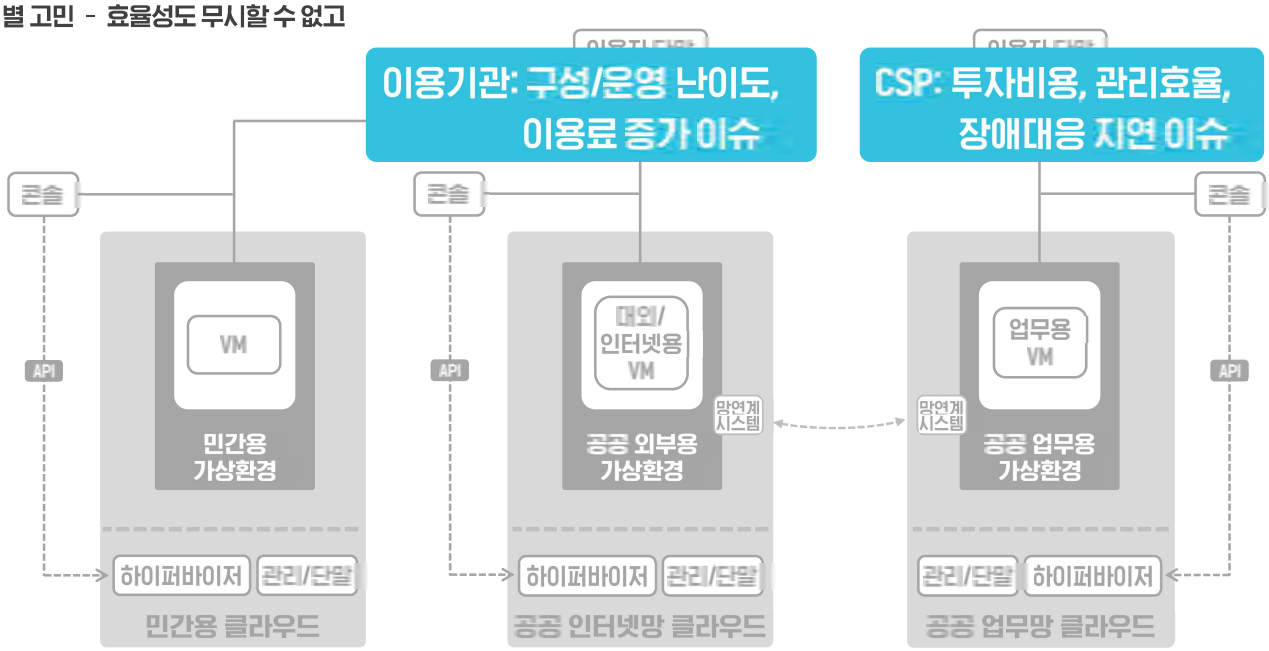
01 물리 망분리

2023 이용 기준 – 중·상등급



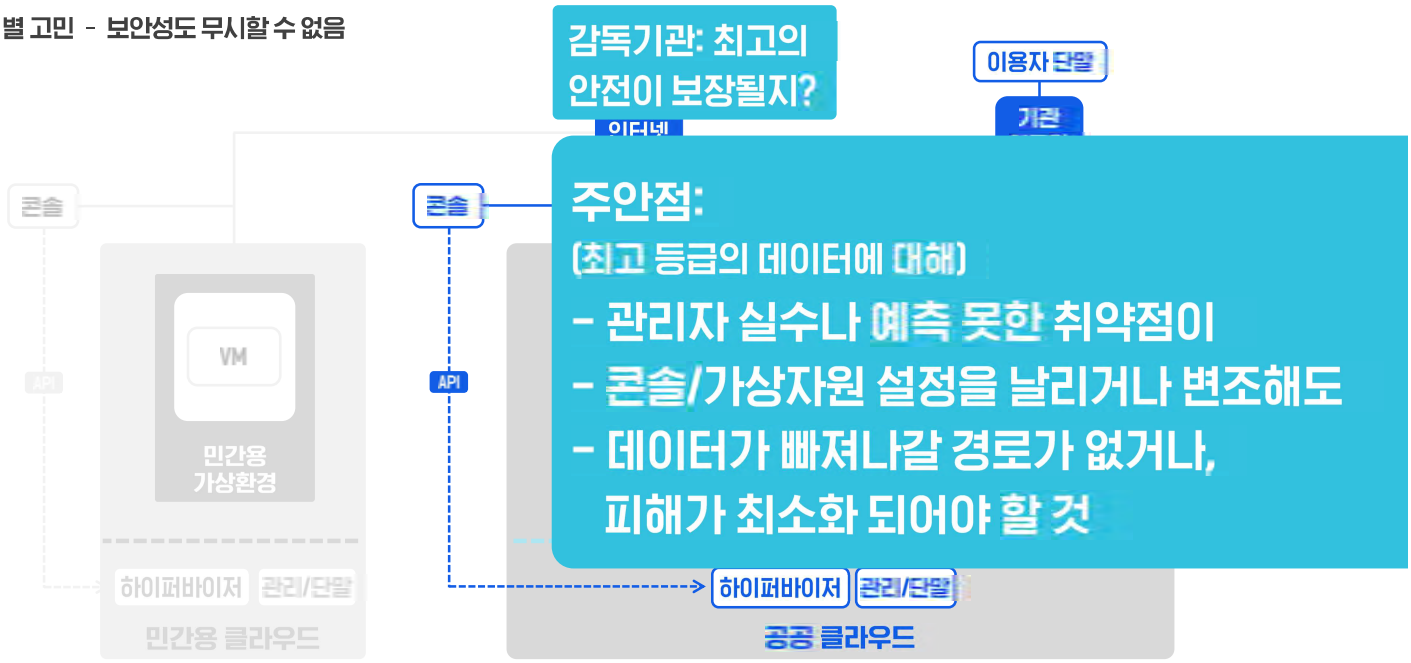
01 물리 망분리

주체 별 고민 - 효율성도 무시할 수 없고



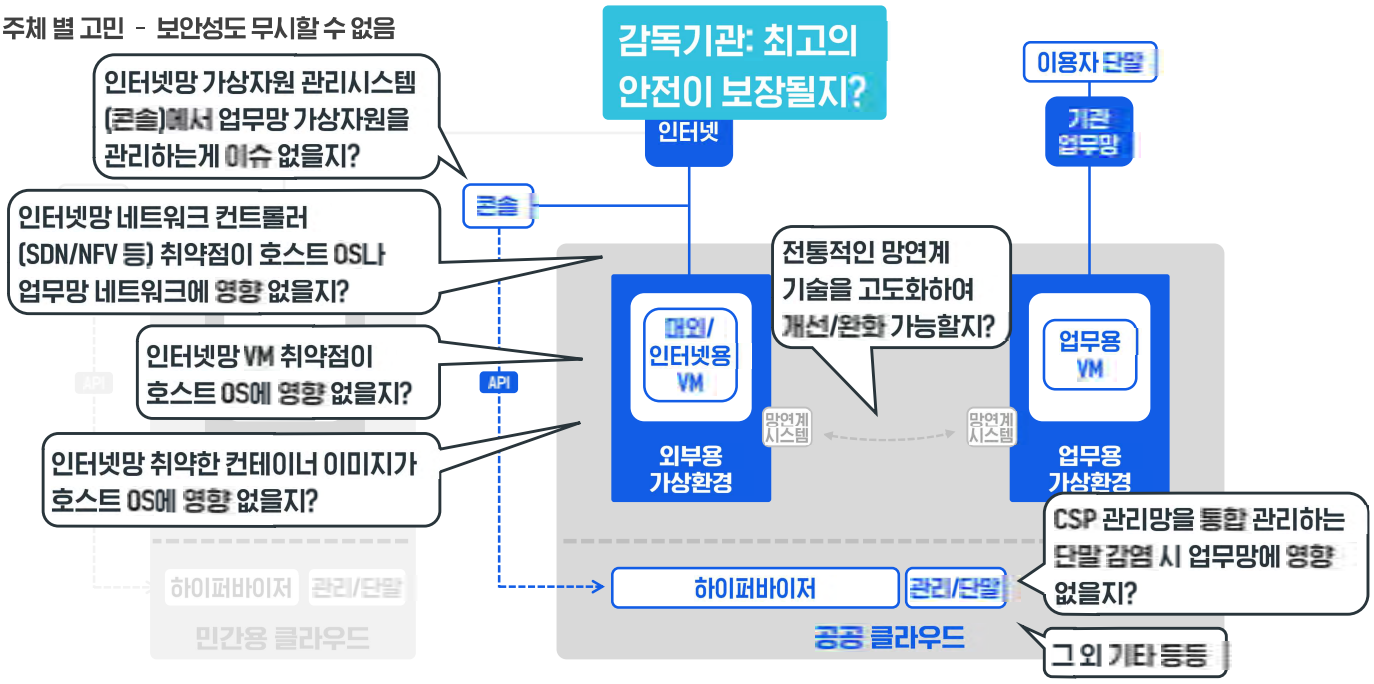
01 물리 망분리

주체 별 고민 - 보안성도 무시할 수 없음



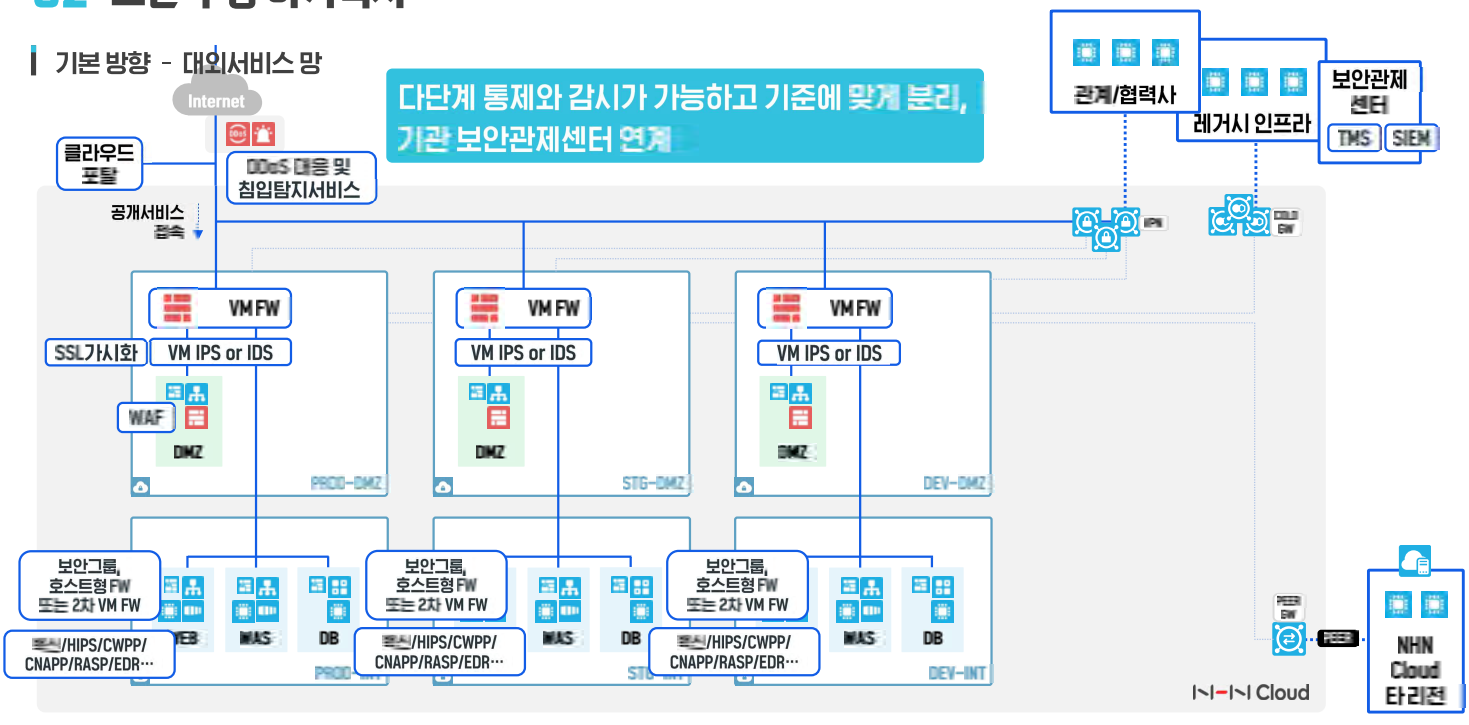
01 물리 망분리

주체 별 고민 - 보안성도 무시할 수 없음



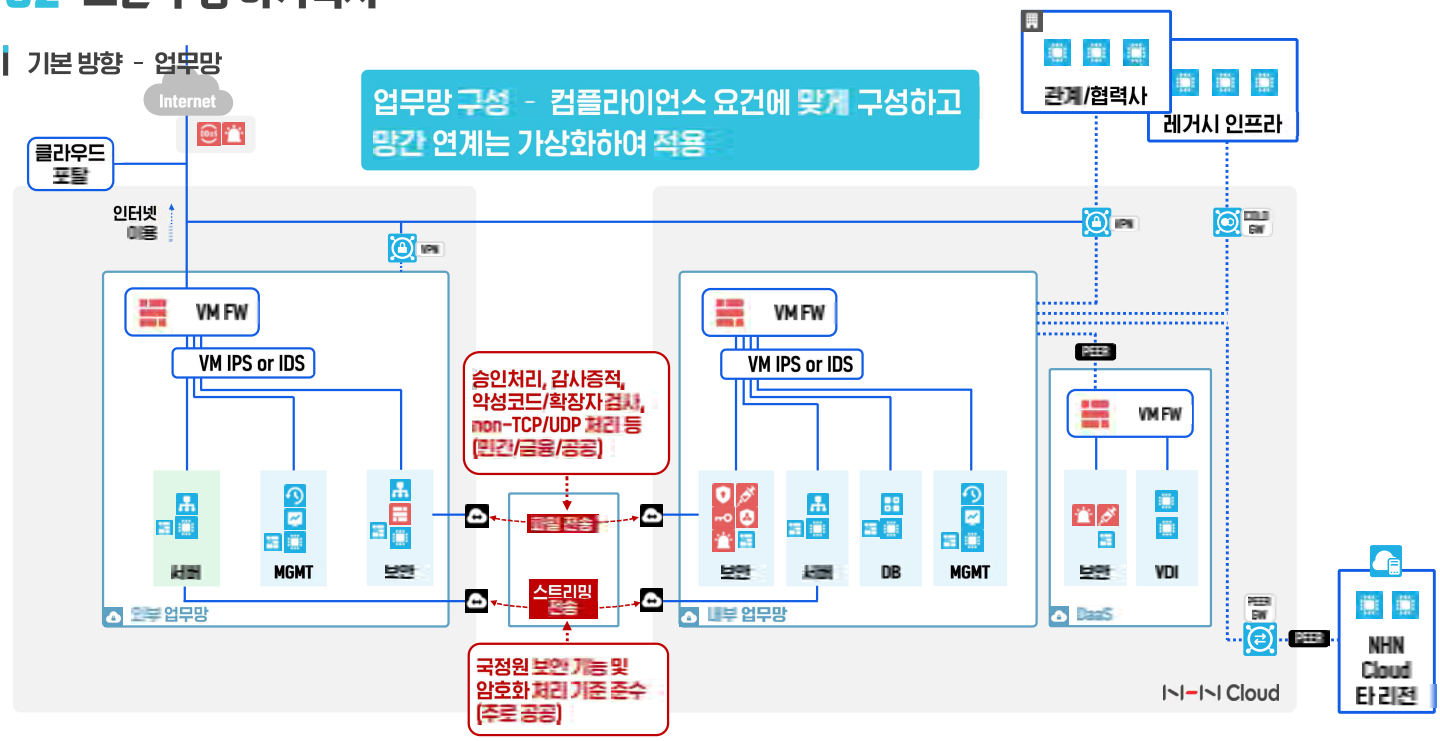
02 보안 구성 아키텍처

기본 방향 - 대외서비스 망



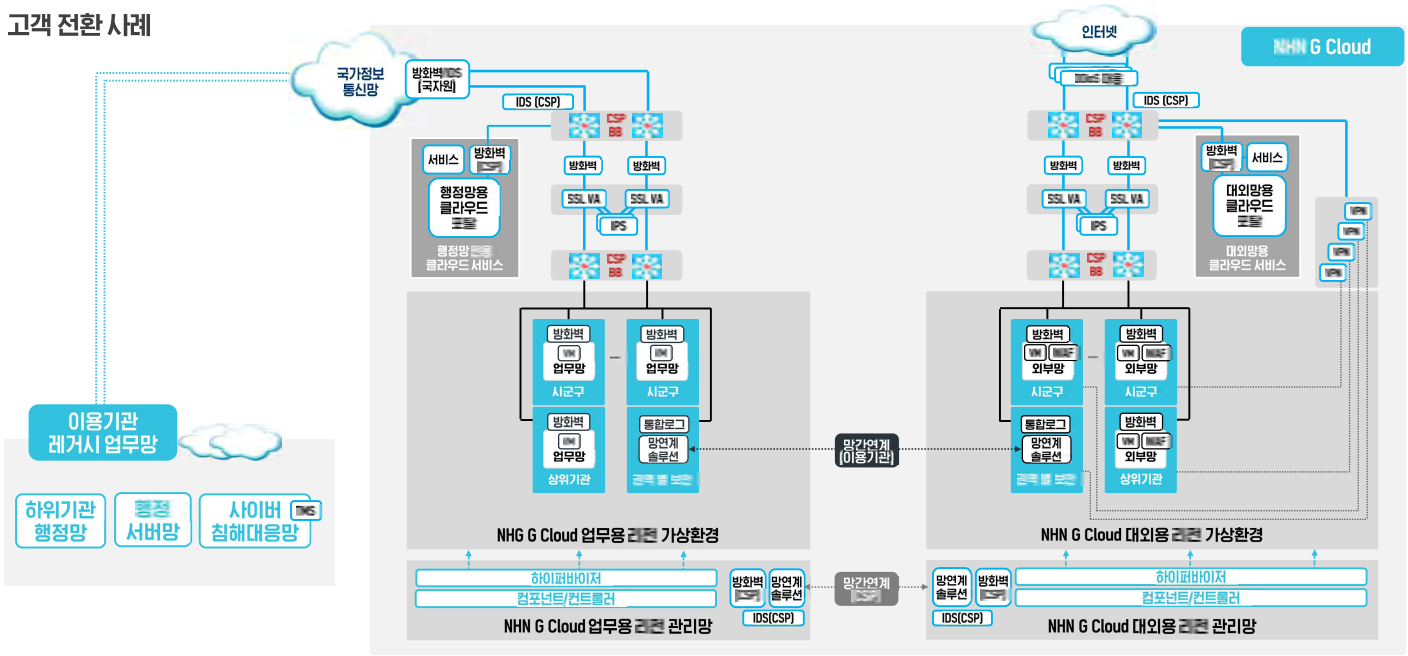
02 보안 구성 아키텍처

기본 방향 - 업무망



02 보안 구성 아키텍처

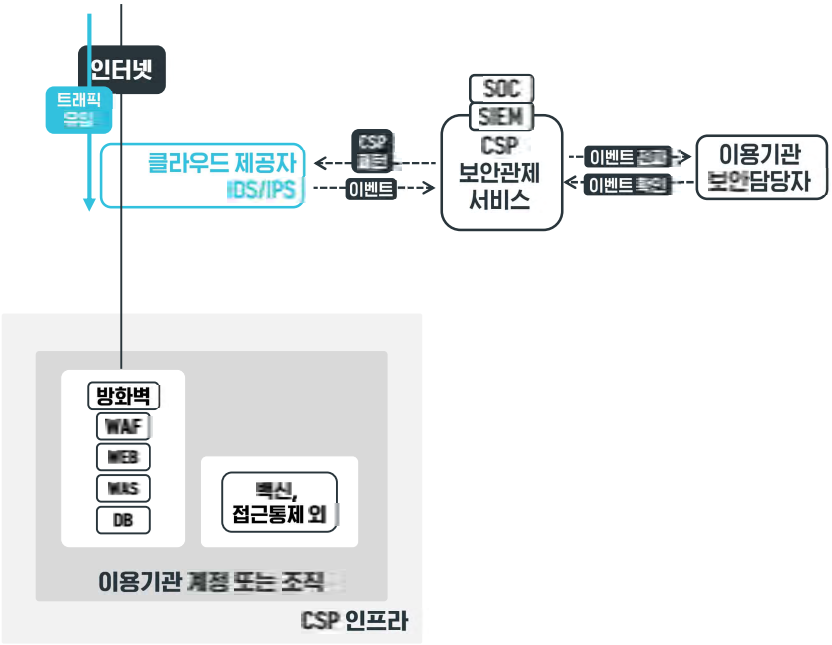
고객 전환 사례



03 보안관제 요건 대응

이전에 많이 제공되던 CSP 보안관제 형태

CSP의 통합 보안관제 서비스 이용

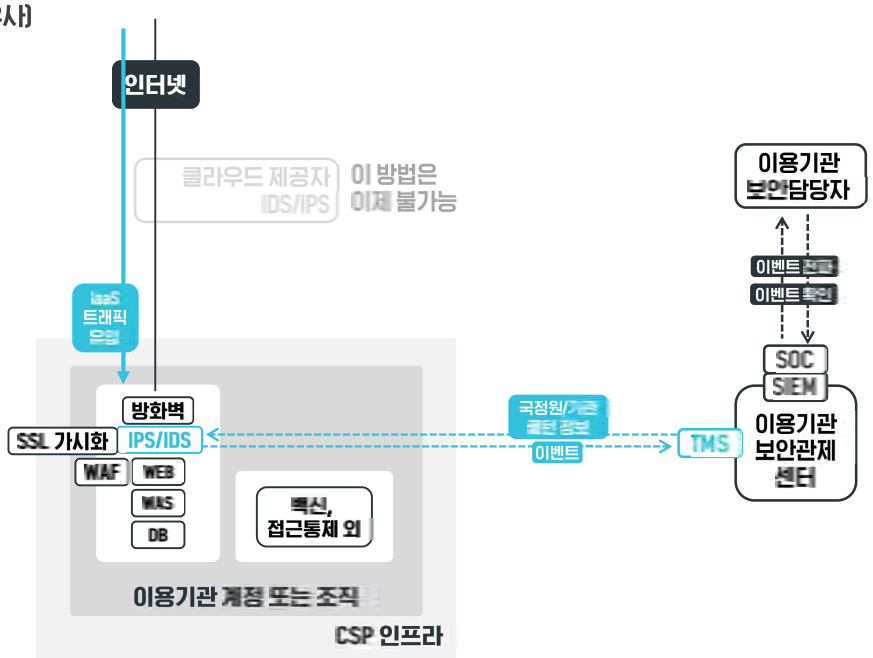


03 보안관제 요건 대응

2023.4 국정원 IaaS 보안관제 기준 (PaaS도 유사)

핵심 내용

1. 기관에 의한 직접 보안관제
2. 기관 별 임차 영역에 IDS/IPS 배치
3. 레거시 보안관제센터의 TMS와 연동
4. SSL 가시화 적용

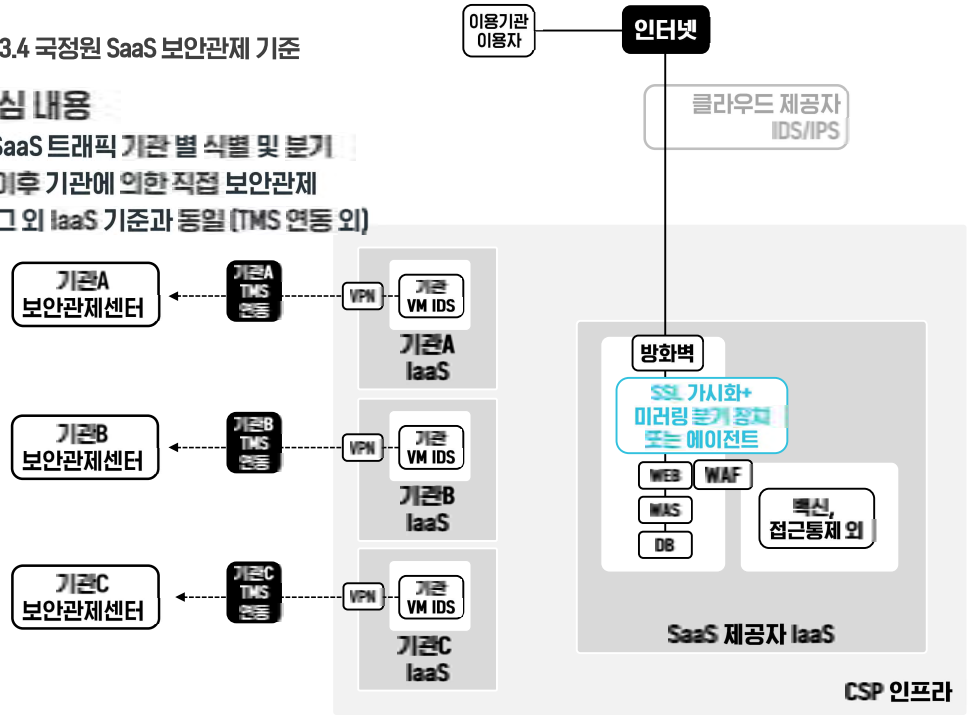


03 보안관제 요건 대응

2023.4 국정원 SaaS 보안관제 기준

핵심 내용

1. SaaS 트래픽 기관 별 식별 및 분기
2. 이후 기관에 의한 직접 보안관제
3. 그 외 IaaS 기준과 동일 (TMS 연동 외)

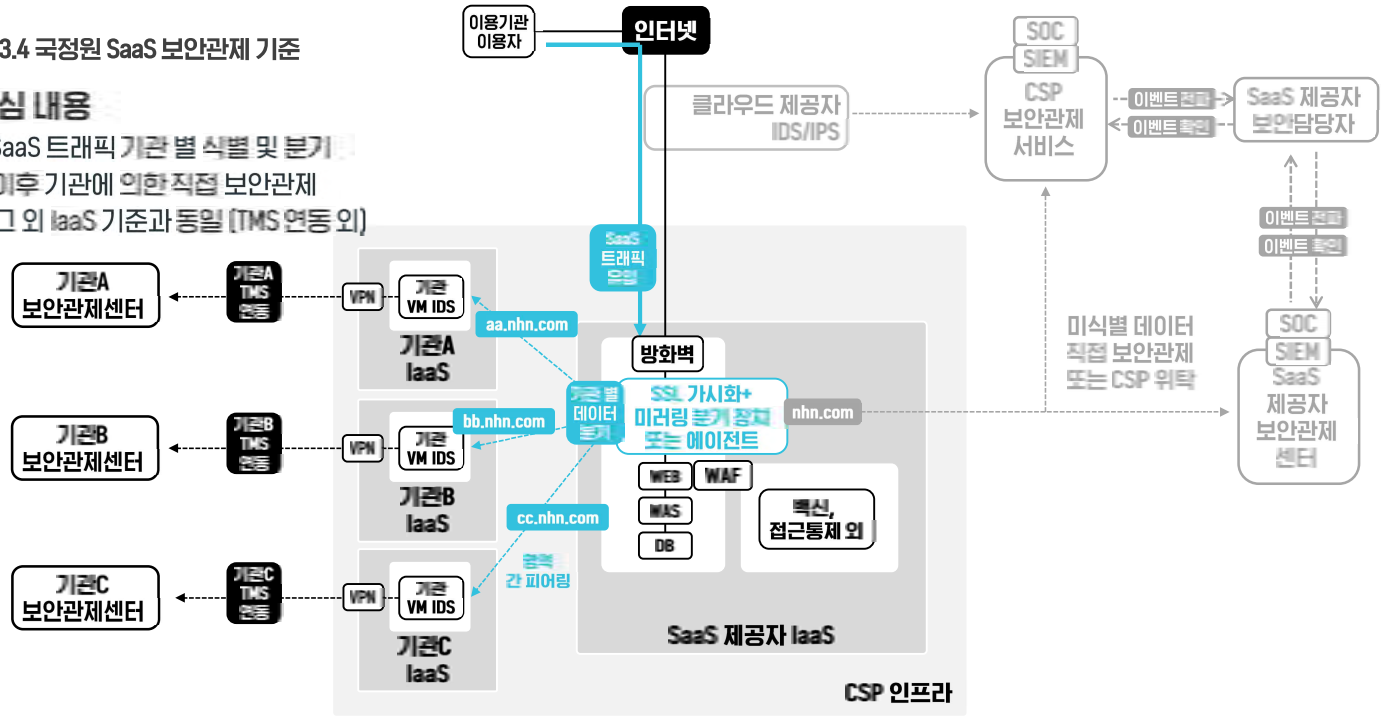


03 보안관제 요건 대응

2023.4 국정원 SaaS 보안관제 기준

핵심 내용

1. SaaS 트래픽 기관 별 식별 및 분기
2. 이후 기관에 의한 직접 보안관제
3. 그 외 IaaS 기준과 동일 (TMS 연동 외)



03 보안관제 요건 대응

주요 상위 규정 참고

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 **기관 직접 관제**
- 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 **전문업체는 파견만**
- 클라우드에 구축된 보안관제 시스템은 정부보안관제체계와 연계되어야 하며, 세부사항은 국가정보원의 클라우드 보안관제 관련 별도 가이드라인(2023년 상반기 발간 예정)준용

**[국가 클라우드 컴퓨팅 보안 가이드라인 (2023.01) -
제4장 제2절 민간 클라우드 컴퓨팅 서비스 이용 보안기준
- 중 가.정책적 측면에서의 기본원칙 부분]**

⑤ 보안관제센터를 운영하는 기관의 장은 제1항에 따른 탐지규칙정보를 「공공기관의 정보공개에 관한 법률」 제9조제1항에 따른 비공개 대상 정보 및 「국가정보자료관리규정」 제2조제1호에 따른 국가정보자료로서 취급·관리하여야 한다. <개정 2020.7.1.>

민간 장비에 패턴 전송 금지

**[국가 정보보안 기본 지침 -
제133조(탐지규칙정보 개발 및 배포) 부분]**

② 보안관제센터를 운영하는 기관의 장과 국가정보원장은 제1항의 업무를 수행하기 위하여 보안관제 대상기관의 장과 협의하여 사이버공격에 관한 정보를 실시간 탐지하는 장비[암호화된 사이버공격 패킷을 가시화(可視化)하는 장비를 포함한다]를 보안관제 대상기관의 정보통신망에 설치·운용하거나 탐지규칙정보를 제공하여 관련 정보를 실시간 처리할 수 있다.

SSL 가시화 적용

**[국가 정보보안 기본 지침 -
제134조(공격정보 탐지·처리) 부분]**

03 보안관제 요건 대응

사실은 4월 개정 이전에도 준수했어야 함

하기 문서에 세부 명시되지 않았다면

상위 규정의 내용을 따랐어야 함

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.

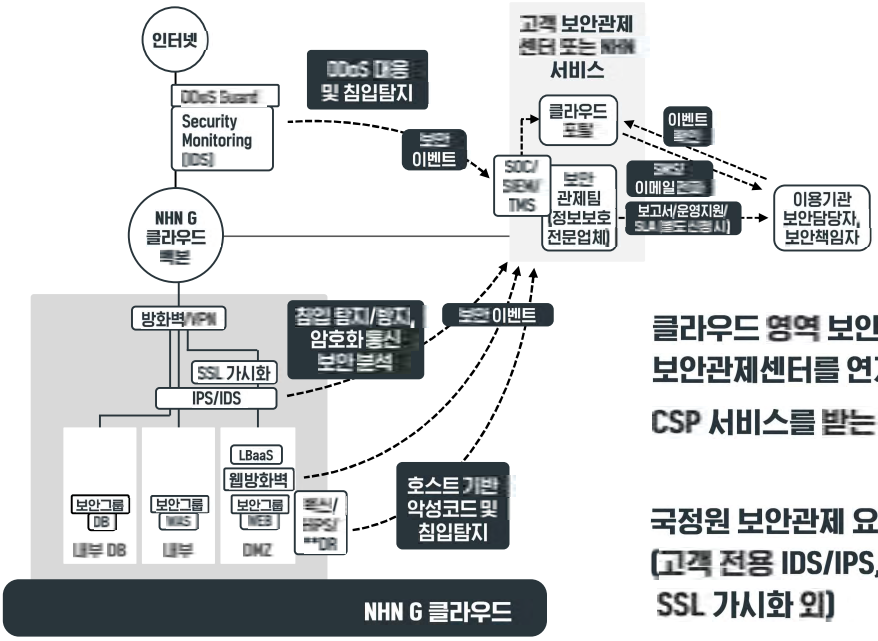
제7장 사이버위협 탐지 및 대응

제1절 보안관제

제131조(보안관제센터 설치·운영) ① 「사이버안보 업무규정」 제14조제2항에 따라 부문보안관제센터 또는 단위보안관제센터를 설치·운영하여야 하는 기관의 장은 해당 보안관제센터를 국가보안관제체계와 연계 운영하여야 한다. 이 경우 연계 방법은 국가보안관제체계를 운영하는 국가정보원장과 사전 협의하여 정한다.

03 보안관제 요건 대응

관련 CSP 제공 체계

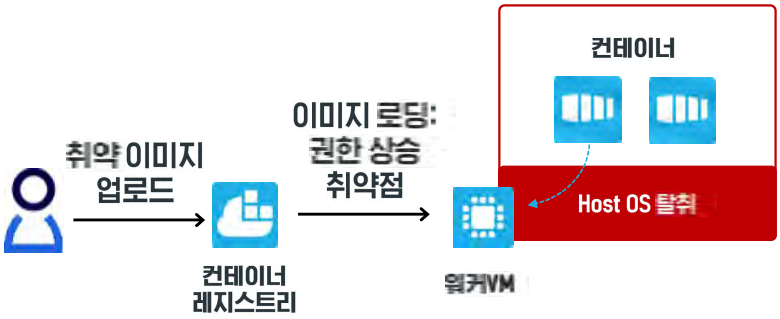


클라우드 영역 보안장비와 레거시망 보안관제센터를 연계하여 직접 수행하거나, CSP 서비스를 받는 형태로 선택 가능

국정원 보안관제 요건을 위한 도구 제공 (고객 전용 IDS/IPS, TMS 연동, 상위기관 연계, SSL 가시화 외)

04 컨테이너 보안

추가 위협 존재하나 아직은 생소한 경우가 많음



컨테이너 이미지 취약점을 악용한 권한 상승, Escape 등의 추가 위협 존재

→ 컨테이너 점검, 감사, 모니터링용 도구 추가 검토 필요

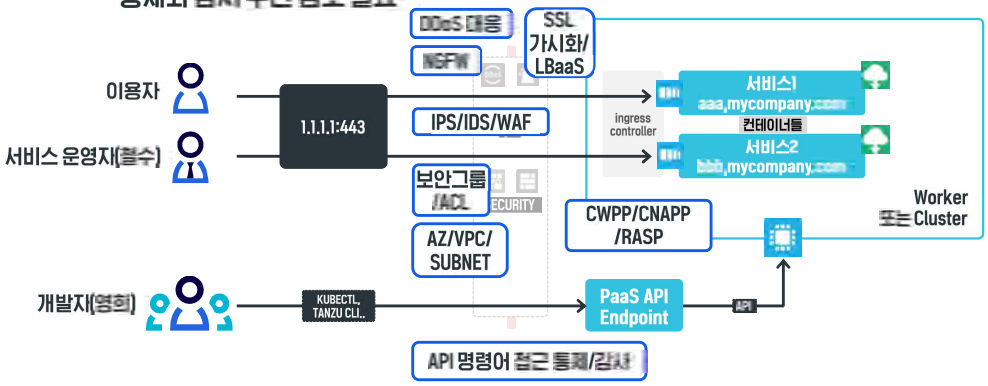
04 컨테이너 보안

더 많은 관심이 필요

이용자는 aaa로 웹 접속 허용한다
bbb웹는 철수만 들어가게 해야 겠다
보안사고 분석을 위해 aaa만 잠깐 막아놔야 겠다
원격 CLI 명령은 아무데서나 하면 안되겠다
원격 CLI 작업한 거 추적할 수 있어야 겠다

보안담당자

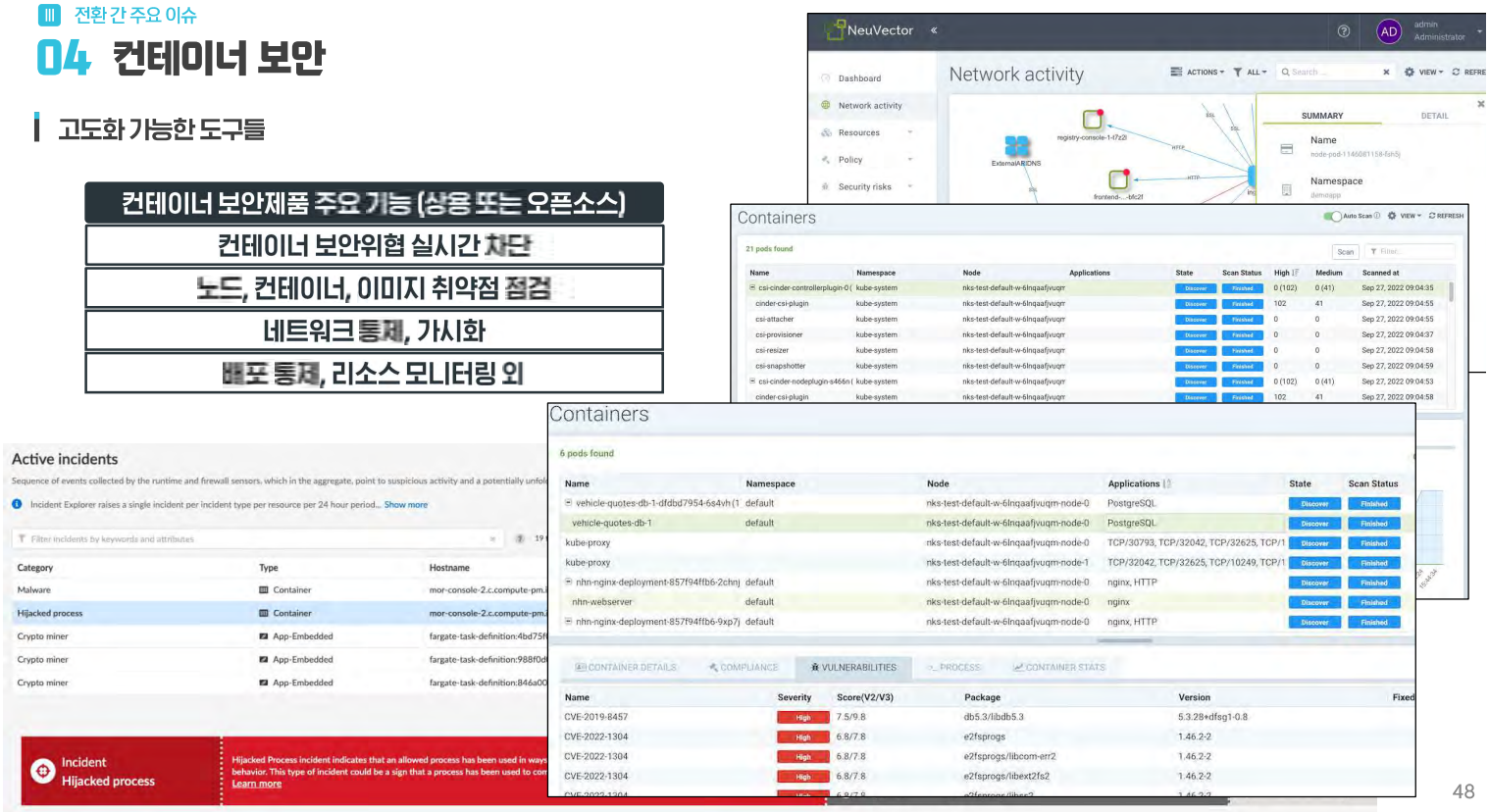
새로운 유형의 서비스에 대한
통제와 감시 수단 검토 필요



04 컨테이너 보안

고도화 가능한 도구들

컨테이너 보안제품 주요 기능 (상용 또는 오픈소스)
컨테이너 보안위협 실시간 차단
노드, 컨테이너, 이미지 취약점 점검
네트워크 통제, 가시화
배포 통제, 리소스 모니터링 외

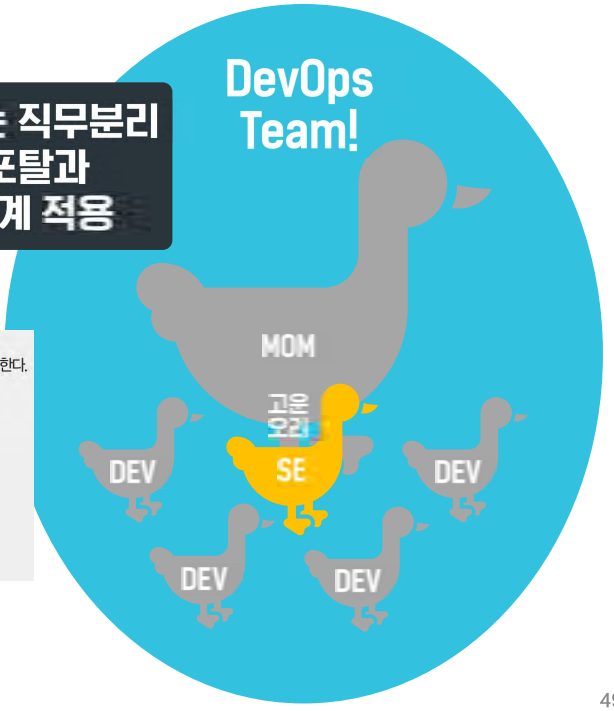


05 직무 분리

마이크로서비스에 특화된 유연한 조직 구성을 추구합니다. 그런데... 엥?

- 권한 오·남용 등으로 인한 잠재적인 피해 예방을 위하여 다음과 같이 직무 분리 기준을 수립하여 적용하여야 한다.
  - 개발과 운영 직무 분리
  - 정보보호담당자, 개인정보취급자와 정보보호 및 개인정보 모니터링 직무 분리
  - 정보시스템 및 개인정보처리시스템(서버, 데이터베이스, 네트워크 등) 간 운영직무 분리
  - 정보보호 및 개인정보보호 관리와 정보보호 및 개인정보보호 감사 업무 분리
  - 개인정보보호 관리와 개인정보처리시스템 운영직무 분리
  - 개인정보보호 관리와 개인정보처리시스템 개발직무 분리 등
  - 외부 위탁업체 직원에게 사용자 계정 등록·삭제(비활성화) 및 접근권한 등록·변경·삭제 설정 권한 부여 금지(다만 불가피한 경우 보완통제 적용)

우리 조직에 맞는 직무분리 기준 반영하여 포탈과 가상자원 권한체계 적용



〈 감독규정 〉
제26조(직무의 분리) 금융회사 또는 전자금융업자는 다음 각 호의 업무에 대하여 직무를 분리·운영하여야 한다.
1. 프로그래머와 오퍼레이터
2. 응용프로그래머와 시스템프로그래머
3. 시스템보안관리자와 시스템프로그래머
4. 전산자료관리자(librarian)와 그 밖의 업무 담당자
5. 업무운영자와 내부감사자
6. 내부인력과 전자금융보조업자 및 유지보수업자 등을 포함한 외부인력
7. 정보기술부문인력과 정보보호인력
8. 그 밖에 내부통제와 관련하여 직무의 분리가 요구되는 경우

- 조직 규모가 작거나 인적 자원 부족 등의 사유로 인하여 불가피하게 직무 분리가 어려운 경우 직무자 간의 상호 검토, 직무자의 책임추적성 확보 등의 보완통제를 마련하여야 한다.
  - 직무자 간 상호 검토, 상위관리자 승인 등으로 오·남용이 발생하지 않도록 관리
  - 개인별 계정 사용, 로그기록 및 감사·모니터링을 통한 책임추적성 확보 등

06 관리 운영

관리적인 운영 방안 수립은 필수

- 담당 조직 구성 및 역할 검토
- 자산 식별 및 관리
- 시스템 신청/승인/처리/증적
- 기록 감사와 모니터링
- 위협 식별 및 조치
- 교육 계획 및 수행
- 퇴사/전배자 변경 관리
- 지침과 가이드라인
- 외부 인력 보안 관리
- 기타 등등등 모든 관리사항

06 관리 운영

관리적인 운영 방안 수립은 필수

기술의 변화는 관리적 변화를 수반

06 관리 운영

계획해 보는 활동 자체가 큰 의미

정보보호관리체계 체크리스트 또는 운영문서 업데이트

		상세내용
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.
2.5.6	접근권한 검토	정보시스템과 개인정보 및 중요정보에 접근하는 사용자 계정의 등록·이용·삭제 및 접근권한의 부여·변경·삭제 이력을 남기고 주기적으로 검토하여 적정성 여부를 점검하여야 한다.
2.6.1	네트워크 접근	네트워크에 대한 비인가 접근을 통제하기 위하여 IP관리, 단말인증 등 관리절차를 수립·이행하고, 업무목적 및 중요도에 따라 네트워크 분리(DMZ, 서버팜, DB존, 개발존 등)와 접근통제를 적용하여야 한다.

06 관리 운영

계획해 보는 활동 자체가 큰 의미

정보보호관리체계 체크리스트 또는 운영문서 업데이트

		상세내용	클라우드 변동 유무	클라우드 적용 방안	주 검토 조직	추가 이슈	비고
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.	O	- 클라우드포탈, VM 등을 대상으로 한 특수 계정/권한 식별 및 관리 적용 - 클라우드포탈 내 멤버관리를 통해 인증 및 권한 부여 - 기존 레거시망 내 통합접근제어 시스템을 연동하여 VM 접근 계정 및 권한 적용 (VPN 연결)	보안정책팀 보안기술팀	- 클라우드에 추가된 새로운 유형의 시스템이 있을지 기술조직 인터뷰 필요	
2.5.6	접근권한 검토	정보시스템과 개인정보 및 중요정보에 접근하는 사용자 계정의 등록·이용·삭제 및 접근권한의 부여·변경·삭제 이력을 남기고 주기적으로 검토하여 적정성 여부를 점검하여야 한다.	O	- 클라우드포탈, VM 등의 사용자 계정 및 권한에 대해 이력 적용 방안 검토 - 클라우드포탈 계정에 대한 감사기록 도구 적용 (CloudTrail) - 기존 레거시망 내 통합접근제어 시스템을 연동하여 VM 접근 계정에 대한 감사기록 도구 적용	보안정책팀 IT시스템팀		
2.6.1	네트워크 접근	네트워크에 대한 비인가 접근을 통제하기 위하여 IP관리, 단말인증 등 관리절차를 수립·이행하고, 업무목적 및 중요도에 따라 네트워크 분리(DMZ, 서버팜, DB존, 개발존 등)와 접근통제를 적용하여야 한다.	O	- 클라우드 내 논리적 네트워크 구성을 파악하고 적절한 통제방안 적용 (보안그룹, ACL, VM방화벽 등)	보안기술팀 네트워크팀	- 세부 기능 비교 필요	

추가

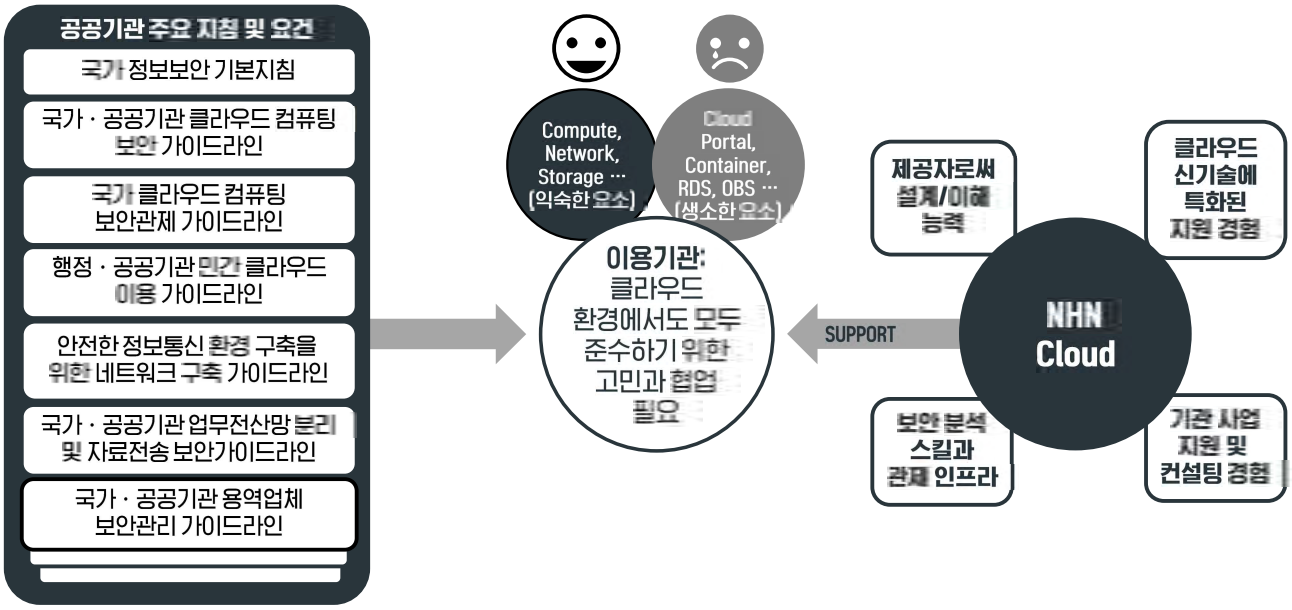
06 관리 운영

관련 서비스 활용

CSP가 제공하는 도구를 활용하는 것도 유용

07 전환에 대한 두려움?

관련 서비스 활용



클라우드 최적화를 통한 비용 절감 방법

㈜클로잇
허규연 수석

행정안전부 NIA 한국지능정보사회진흥원

클라우드 최적화를 통한 비용 절감 방법

CONTENTS

I 클라우드 최적화 개념

행정안전부
NIA 한국지능정보사회진흥원

NIA 한국지능정보사회진흥원

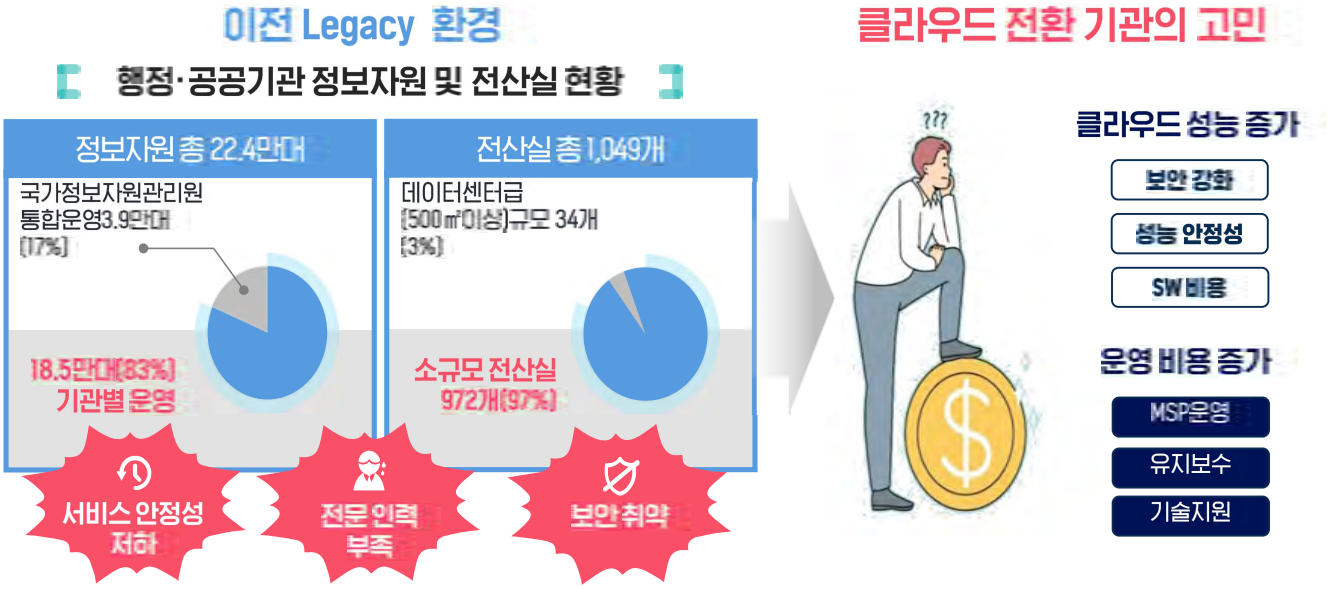
01 클라우드 최적화란 ?

성능을 향상시키는 동시에 클라우드 비용을 최적화하고 낭비를 제거하기 위해 워크로드와 리소스를 선택하고 할당하는 프로세스

NIA 한국지능정보사회진흥원

02 최적화의 필요성

기술적 고민(성능)보다는 비용적 고민으로 비용 최적화 니즈 증가



NIA 한국지능정보사회진흥원

03 비용 최적화 정의

비용 '가시성(Visibility)' 를 올바르게 확보하면서, 지속적인 자원 추적 및 관리를 끊임없이 진행해가는 과정

지표 / 프로세스 / 조직 확보가 필요

NIA 한국지능정보사회진흥원

04 비용 최적화 고려 요소
공공 클라우드 특성을 고려한 지속적 비용절감 요소 발굴이 필요

1 자원 최적화	✓ 상품 선택 – 성능 및 요구사항을 충족하며 사용 가능한 가장 저렴한 인스턴스를 선택 ✓ 미사용 자원 – 유휴 자원 및 리소스 등을 추적하여 절감
2 성능 최적화	✓ 사용량 추적 – CPU, MEM 등의 리소스 평균치를 확인하여 필요치 않는 리소스 반납 ✓ 스케일링 – 성능 요구사항에 맞게 리소스를 할당 및 할당 취소하여 비용을 절감
3 보안 최적화	✓ 중복비용 절감 – 통합 가능한 클라우드 운영 환경을 구성하여 중복 보안 시스템 비용 절감
4 모니터링 최적화	✓ 낭비자원 추적 – 가용한 모니터링 자원, APM 등을 통한 성능 분석을 통해 낭비되는 리소스 등을 추적하여 절감 ✓ 상품 출시 – 보다 저렴한 상품 출시 현황을 모니터링하여 가장 저렴한 상품 선택
5 빌링 최적화	✓ 약정할인 – 장기적인 할인 및 프로모션을 통하여 CSP 이용 비용 절감 ✓ 비용 분석 – 청구 내역 정밀 분석을 통해 이용 비용 절감 계획 수립

NIA 한국지능정보사회진흥원

05 비용 최적화 추진 절차
단회성 컨설팅이 아닌 지속적인 개선 활동이 필요

계획 수립 (Plan)	리소스 추적 (Track)	최적화 (Optimize)	지속적 개선 (Improve)
이용 현황 분석	가시성 확보	비용 최적화	지속적인 개선
✓ 자료 수집 ✓ 계약검토 ✓ 추진 조직 구성 ✓ 목표 설정	✓ 자원 분석 ✓ 비용 분석 ✓ 사용률 분석 ✓ 모니터링 툴 활용	✓ 유휴 리소스 제거 ✓ 중복 리소스 제거 ✓ 낭비 리소스 제거 ✓ 지속적 개선 방안 수립	✓ 신규 가격 정책 확인 ✓ 클라우드 환경에 맞는 조직 체계 구성 ✓ 지속적 교육을 통한 신기술 습득

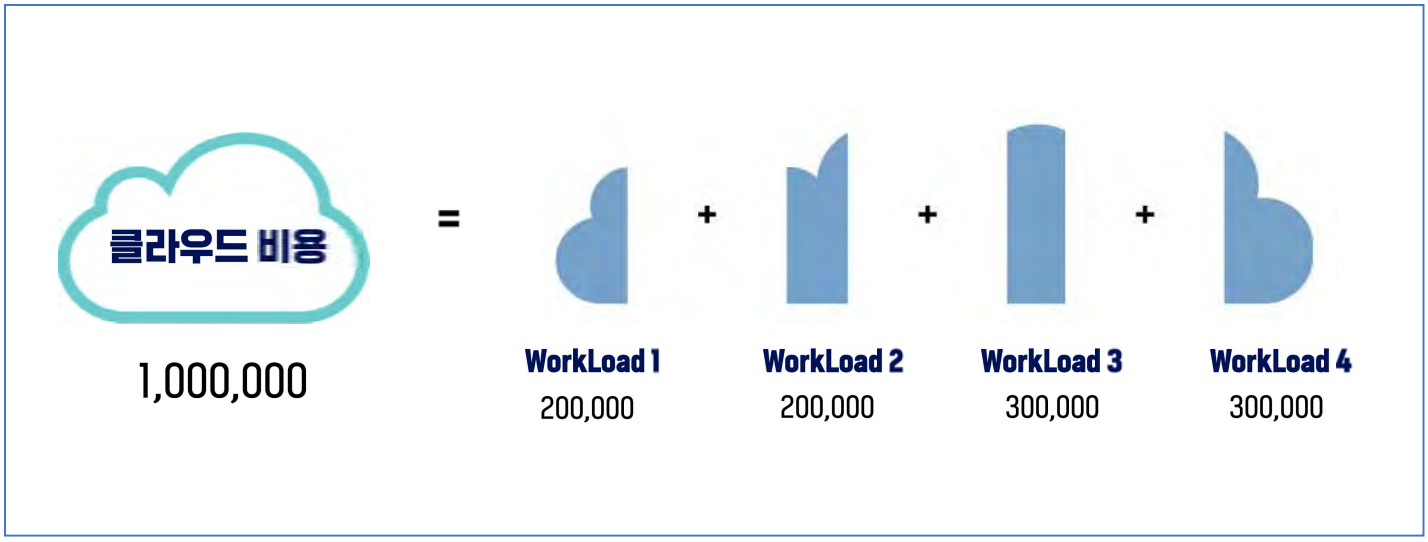
II 클라우드 최적화 추진방법

01 계획 수립
02 리소스 추적
03 최적화
04 지속적 개선

행정안전부
NIA 한국지능정보사회진흥원

01 계획 수립

자원유형 , 시스템별 자원/비용 사용 현황 파악이 필요



02 리소스 추적

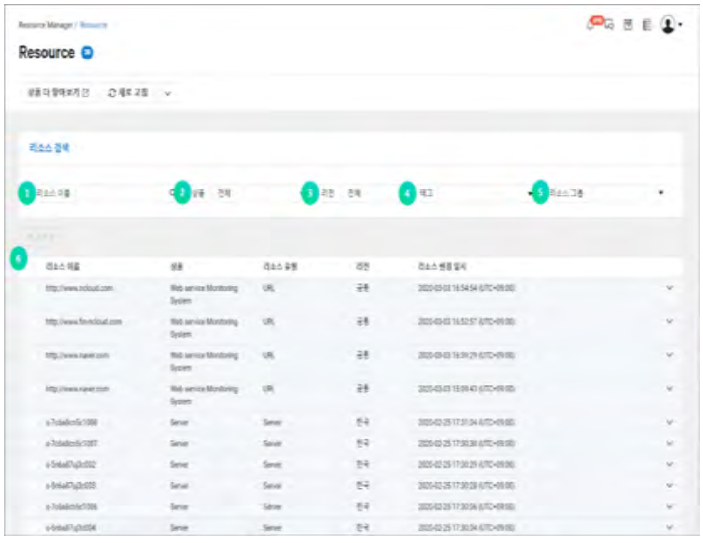
다양한 방법으로 리소스를 추적하여 최적화 요소를 찾을 수 있음

1 자원 사용량 정보로 확인	2 구성 추적으로 확인	3 정책 추적으로 확인
미사용 미연결 자원	ACG 미설정 자원	과도한 백업 자원
Stop 상태의 연결 자원	Stop 상태의 연결 자원	과도한 보안 자원
Auto Scaling으로 생성되어 서비스 되지 않는 자원		

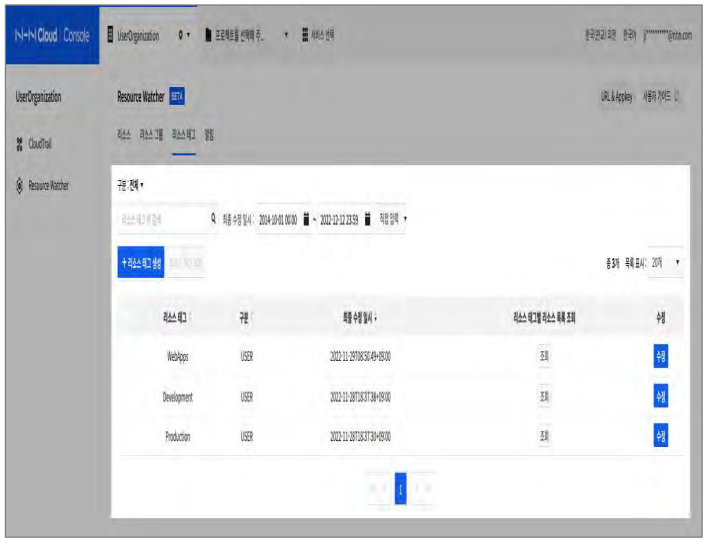
02 리소스 추적

CSP 에서 제공하는 콘솔을 활용하는 방법(1/2)

1) Resource Manager 를 활용한 리소스 찾기 (네이버 클라우드)



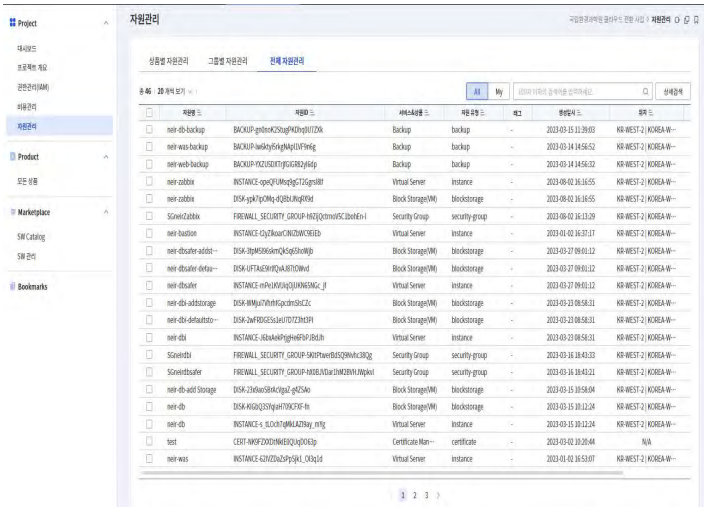
2) Resource Watcher 를 활용한 리소스 찾기 (NHN 클라우드)



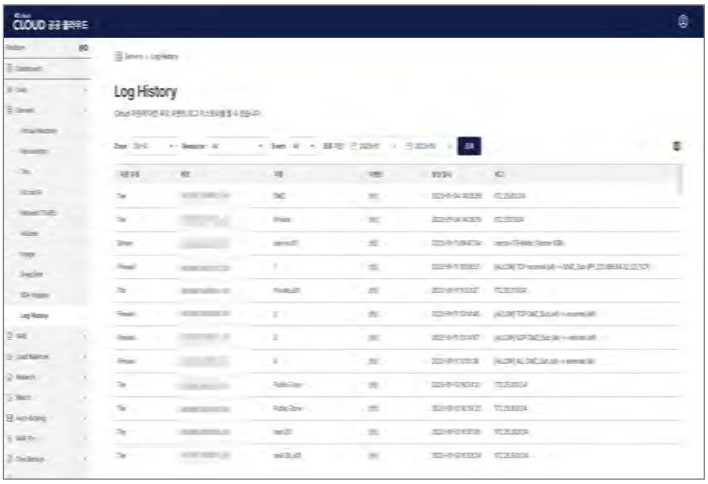
02 리소스 추적

CSP 에서 제공하는 콘솔을 활용하는 방법(2/2)

3) 자원관리 메뉴 를 활용한 리소스 찾기 (삼성 SDS)



4) Log History를 활용한 리소스 찾기 (KT 클라우드)



02 리소스 추적

MSP/CSP 에서 제공하는 보고서 및 대쉬보드를 활용하여 자원 사용률 추적

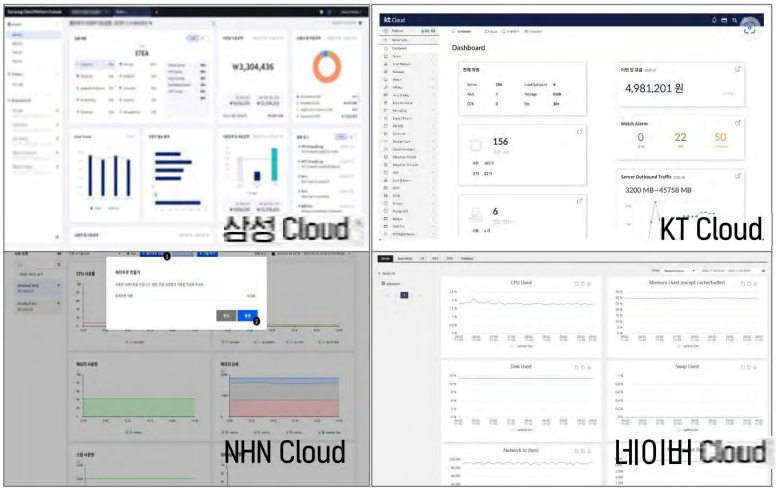
MSP 월간 운영 보고서 활용

가. 정보시스템별 자원 사용현황

○ CPU, Memory, Disk 등 자원 실제 사용현황

정보시스템	연결서버명	CPU 사용량 (%)		Memory 사용량 (%)	
		평균	최고	평균	최고
		0.50	50.60	17.23	17.60
		1.11	100	37.47	46.77
		0.23	28.40	16.11	16.70
		1.00	99.09	17.51	18.63
		0.29	45.14	14.93	15.32
		0.27	26.41	14.32	28.93
		0.29	82.70	10.96	41.02
		0.64	53.72	21.13	22.00
		0.53	64.75	9.86	10.39
		0.33	47.41	14.65	14.85

CSP 제공 리소스 모니터링 대쉬보드 활용



03 최적화
현재 시스템에 적합한 Type, Size 변경

1) 사용량 패턴 분석을 통해 현재 시스템에 적합한 Type, Size 변경

Downsize

사용한 만큼 과금

vCPU: 8 Memory : 16GB	vCPU: 4 Memory : 8GB
300,000 원	150,000 원

Modernize

신규 요금 정책 적용

vCPU: 8 Memory : 14GB	vCPU: 8 Memory : 16GB
300,000 원	220,000 원

03 최적화
꾸준히 사용되는 인스턴스는 장기계약을 하여 할인율 적용

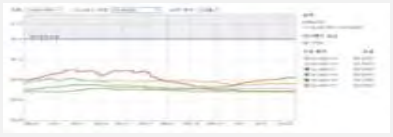
2) 지불옵션 선택 – 꾸준히 사용되는 Instance를 Reserved Instance로 구매

03 최적화
사용량 변동에 따라 다양한 클라우드 기술을 적용하여 최적화

3) 그 밖에 적용가능한 방법

Scheduling

항상 켜져 있는 Instance를 사용하는 시간에만 켜기



짧은 시간 많은 컴퓨팅 자원이 필요한 경우 (빅데이터 분석 등)

Spot Instance

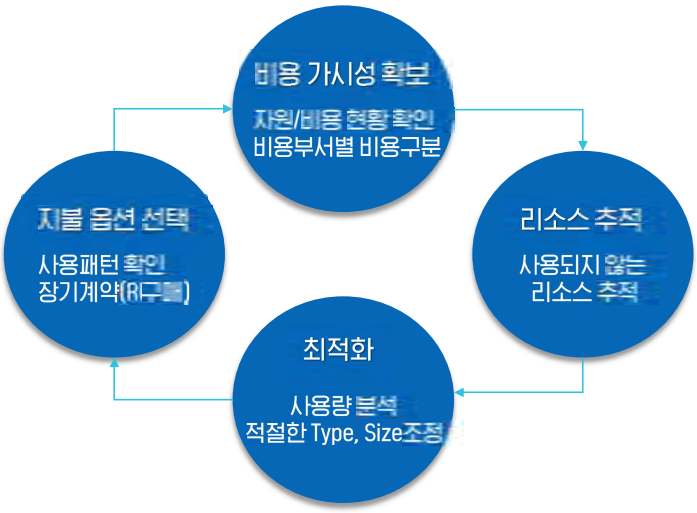
Auto Scaling

서비스의 Demand 와 Usage에 기반해 Scale Up / Down

목적에 따라 가장 비용 효율적인 Product 선택

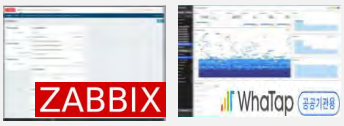
적절한 Product 사용

04 지속적 개선
반복 작업을 해야 함으로 이에 필요한 기술 및 프로세스 확립이 필요



비용 분석 및 예산 할당

전문가 투입을 통한 프로세스 확립



공개/상용 모니터링 툴 적용

기술 및 자동화 활용

Ⅲ 클라우드 최적화 성공전략

01 비용 최적화 성공을 위한 6Tips
02 최적화를 통한 비용 절감 사례
03 개선방안 제언

행정안전부
NIA 한국지능정보사회진흥원

NIA 한국지능정보사회진흥원

01 비용 최적화 성공을 위한 6 Tips

Plan

1 클라우드 비용이 어떤 식으로, 어떤 분야에 지출되는지 파악하라
- 정기적으로 발생하는 비용
- 제공업체 및 상품별 비용 구조
- 요금 과금 방식 (할인율, CSP 특성)

2 서비스 특성에 따라 클라우드 비용을 환산하라
- 개발환경 - 사용하지 않는 리소스
- 서비스 주기 특성 - 과도한 리소스 유지
- 자료보관방식 - 불필요한 전송비용, 보관주기

Track

3 클라우드 인프라의 설정을 확인하라
- 작은 설정 오류 하나 놓쳐서 큰 비용 손실 발생
- 확장성이 용이한 기술을 적용

4 투명성과 자동화가 핵심 중 핵심이다
- 자동화 기술을 도입하지 않으면 불가능
- 비용 절감을 위한 국내 CSP 의 노력도 필요

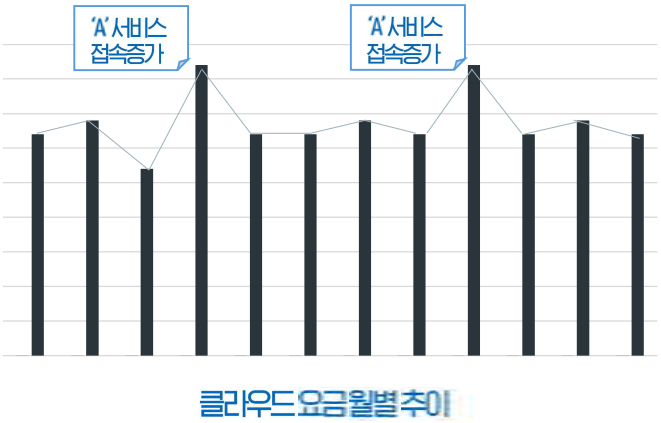
Optimize

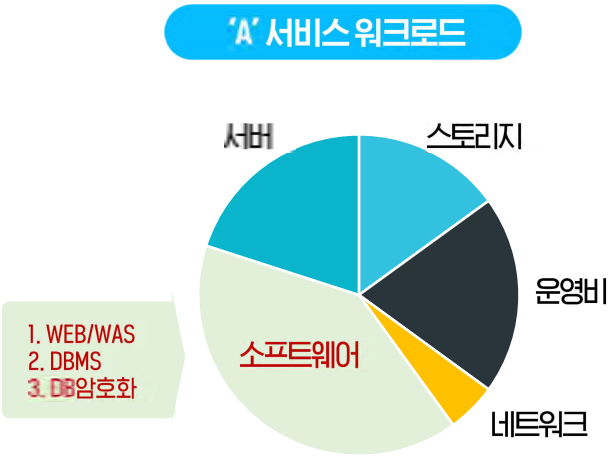
5 클라우드 관련 예산 관리 정책이 필요하다
- CSP 들의 획일화된 가격 정책
- 지속적인 서비스 발굴 및 가격 변경
- 고객에게 다양한 구매 정책 제공

6 애플리케이션의 구조 조정과 할인 규정 적용하기
- 단순 IaaS 중심에서 PaaS, SaaS 로 변경
- 애플리케이션의 구조에 대한 확장성도 고려

01 비용 최적화 성공을 위한 6 Tips

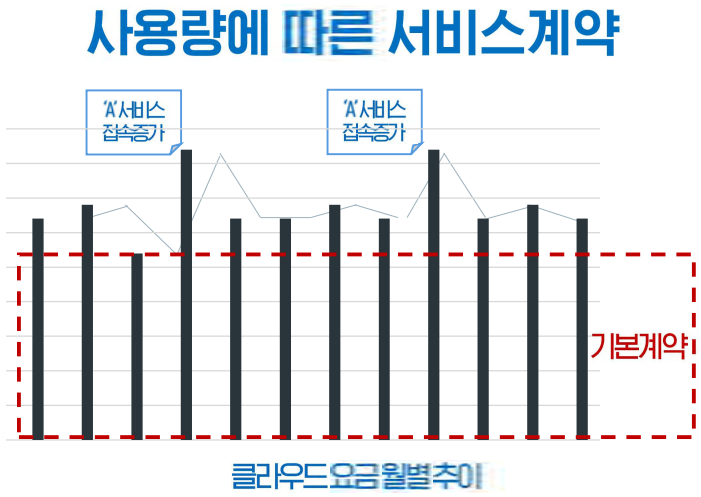
1. 클라우드 비용이 어떤 식으로, 어떤 분야에 지출되는지 파악하라





01 비용 최적화 성공을 위한 6 Tips

2. 서비스 특성에 따라 클라우드 비용을 환산하라

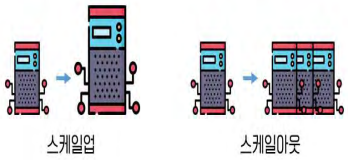


01 비용 최적화 성공을 위한 6 Tips
3. 클라우드 인프라의 설정을 확인하라

Auto Scaling

기본 개념

•현재 클라우드에서는 스케일아웃만 가능



•스케일업 - 서버의 용량을 증가
•스케일아웃 - 서버의 댓수를 증가

장점

•사용자가 더 많은 CPU와 메모리, 스토리지를 필요로 하는지 감지해 자동으로 할당

단점

복잡성과 운영	•과소할당, 과대할당이 발생
비용	•리소스를 효율적 관리 못하면 추가 비용 발생 •장기할인보다 못한 요금 인하 발생
성능저하	•스케일링 작업하는 동안 속도저하로 장애 발생 가능성이 존재
애플리케이션	•고정된 설정으로 동작하는 애플리케이션에서는 제대로 작동되지 않음 (설정값 복제 불가)

Auto Scaling 보다는 스케일업 활용이 유리

01 비용 최적화 성공을 위한 6 Tips
4. 투명성과 자동화가 핵심 중 핵심이다

클라우드 비용 투명성

4vCore/16GB 서버 구성 ▶ CSP 별 큰 차이 없음

구분	월요금	보안관제	합계
KT Cloud	197,700	40,240	237,940
Naver Cloud	203,120	WAF 관제별도	203,120+@
NHN Cloud	190,980	관제별도	190,980 + @

다양한 요금 모델 필요 aws

온디맨드	•기본 방식, 사용한 리소스/기간/용량에 따라 가격 산정
예약 인스턴스	•일정 기간동안 리소스를 예약하여 할인된 가격 산정
스팟 인스턴스	•남는 컴퓨팅 자원을 저렴하게 활용하는 방식
무료 계층	•초기 사용자들을 위해 일부 서비스를 무료로 제공

자동화 서비스와 도구 제공

AWS는 비용 및 사용량 가시성을 위한 서비스,도구 제공

01 비용 최적화 성공을 위한 6 Tips

5. 클라우드 관련 예산 관리 정책이 필요하다

1. 범위를 조사해 초과분을 파악
   - ✓ 요금 명세서 상세 내역
   - ✓ 큰 비용을 차지하는 요소를 파악
2. 리소스 사용 패턴을 분석하여 비효율적인 부분을 파악
   - ✓ 과도한 상품 / 낭비 자원 고려
   - ✓ CSP/MSP 계약 방식
3. 우선 순위를 지정해서 지출을 조정
   - ✓ 우선 순위가 낮은 서비스 지출 조정
   - ✓ 다른 계약 방식 변경 검토
4. 클라우드 서비스업체와 소통해 상황논의 비용 절감 대안모색
   - ✓ 클라우드 서비스 업체에 요금 할인을 요청
   - ✓ 저렴한 상품/ 계약 방식 변경

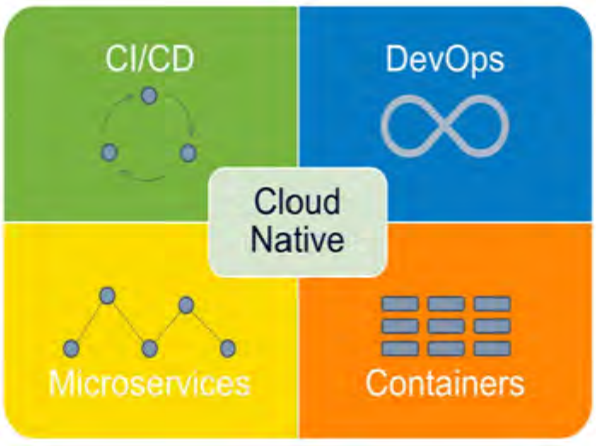
→ 워크로드별 요금정산
→ 자동화 기술/툴 제공
→ 다양한 서비스 발굴
→ 다양한 요금모델 제공

클라우드 서비스업체 (CSP,MSP)

01 비용 최적화 성공을 위한 6 Tips

6. 애플리케이션의 구조 조정과 할인 규정 적용하기

클라우드 네이티브 전환



1. 효율성 증가
   - ✓ 개발자는 자동화된 도구, 클라우드 서비스 및 설계를 활용하여 확장 가능한 애플리케이션 구축
2. 비용 절감
   - ✓ 물리적 인프라를 구축하고 유지할 필요가 없어 해당하는 운영 비용을 절감
3. 가용성 보장
   - ✓ 복원력이 뛰어나고 서비스 중단 없이 가용성이 높은 애플리케이션 구축이 가능

02 최적화를 통한 비용 절감 사례

K 기관 CLOIT 클라우드 최적화 컨설팅 사례

1. 자원 사용량 분석을 통한 자원 조정

서버명	CPU 최대사용률(%) < 80%이하		Memory 최대사용률(%) < 90%이하	
	최대	평균	최대	평균
	7.92	1.1	28.78	25.41
	1.99	1.07	19.41	27.18
	14.4	5.46	46.78	37.53
	31.82	5.24	47.94	31.16
	6.06	2.22	88.81	56.95
	3.44	0.65	44.73	35.07
	6.79	1.19	54.73	41.13
	3.45	0.82	27.94	24.91
	17.28	0.75	26.49	19.05
	20.83	3.51	20.2	16.47

서버명	AS-IS			TO-BE		
	CPU (vCore)	MEM (GB)	요금 (월, VAT별도)	CPU (vCore)	MEM (GB)	요금 (월, VAT별도)
	2	4	80,880	2	4	80,880
	2	4	80,880	2	4	80,880
	4	16	216,580	2	16	165,780 (-50,800)
	4	16	216,580	2	16	165,780 (-50,800)
	4	16	225,220	2	16	174,420 (-50,800)
	2	4	80,880	2	4	80,880
	2	4	80,880	2	4	80,880
	2	4	86,640	2	4	86,640
	4	8	188,800	2	8	134,300 (-54,500)
	4	16	242,340	2	16	194,420 (-47,920)

- ✓ 12개월 자원사용량 분석 : CPU, MEM등
- ✓ MSP 월간 보고서 및 CSP 제공 대쉬보드 활용

- ✓ 5대 VM CPU 하향 조정 : 4Core -> 2Core
- ✓ 비용 절감 : 년 약 300만원(월 25만원)

02 최적화를 통한 비용 절감 사례

H 기관 CLOIT 클라우드 최적화 컨설팅 사례

2. 백업 정책 및 솔루션 변경

백업 현황 (NCP Backup)			
Host명	백업 디렉토리명	백업 수행주기	보관 본수
		2주 1회	2

권고안 (Object Storage)		
백업매체	백업 수행주기	보관 본수
Object Storage	crond 설정 가능 한도에서 자유롭게 선택 가능	제한없음

- ✓ NCP Backup 서비스 이용한 데이터 백업
- ✓ 백업설정 변경 및 복구 작업 시 별도 신청서 작성하여 네이버클라우드 고객센터 접수
- ✓ 월 이용료 : 약 42만원(1.5 TB)

NCP Backup : 백업 솔루션을 이용하여 높은 안정성과 가용성 보장

- ✓ Object 스토리지 이용한 데이터 백업 (NCP 백업해지)
- ✓ 언제든 백업설정 변경 및 데이터 복구 (파일 다운로드) 가능
- ✓ 월 이용료 : 약 4만원(1.5 TB)

Object 스토리지: HTTPS를 지원하여 데이터가 암호화되어 안전하게 저장 및 다운로드 될 수 있게 제공하며, 저장된 데이터는 여러 단계의 보안 장비로 안전하게 보호

03 개선방안 제언 - 진정한 국내 클라우드 비용 최적화를 위해서는 …

1. 다양한 가격 정책

✓ 할인율

해지시 위약금 발생

✓ 사용한 만큼

할인율이 적용되지 않음

2. 클라우드 SW가격 정책

✓ 라이선스

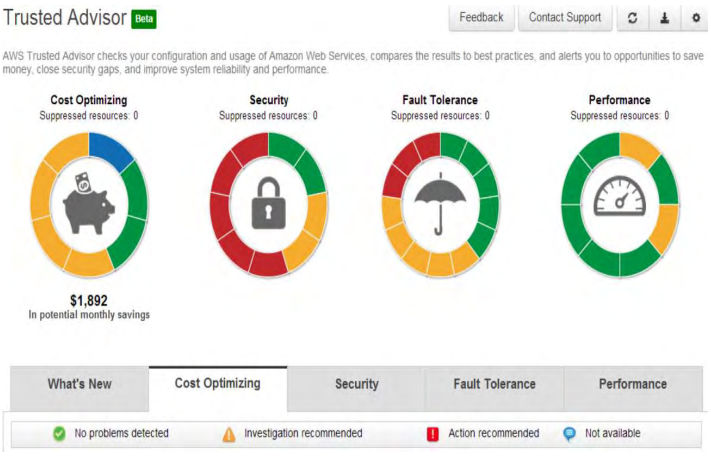
클라우드 라이선스 정책 정립

✓ 월정료

유지보수 정책 정립

03 개선방안 제언 - 진정한 국내 클라우드 비용 최적화를 위해서는 …

3. 비용 최적화 도구 제공..

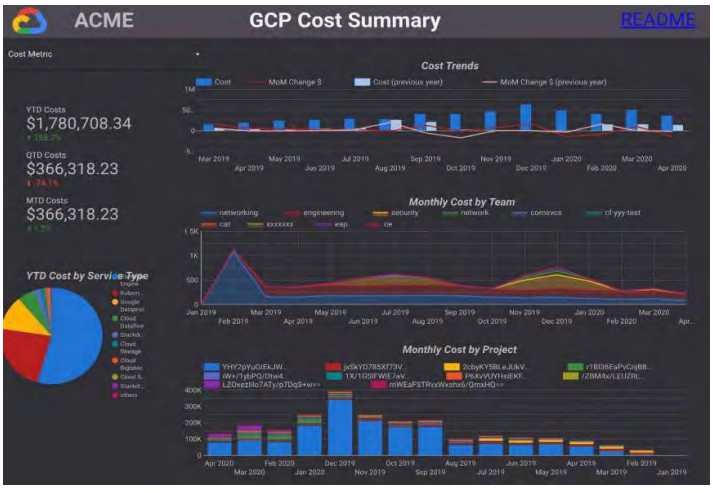


AWS Trusted Advisor

AWS Instance Scheduler

AWS Compute Optimizer

다양한 비용 최적화 도구



Google 데이터 스튜디오