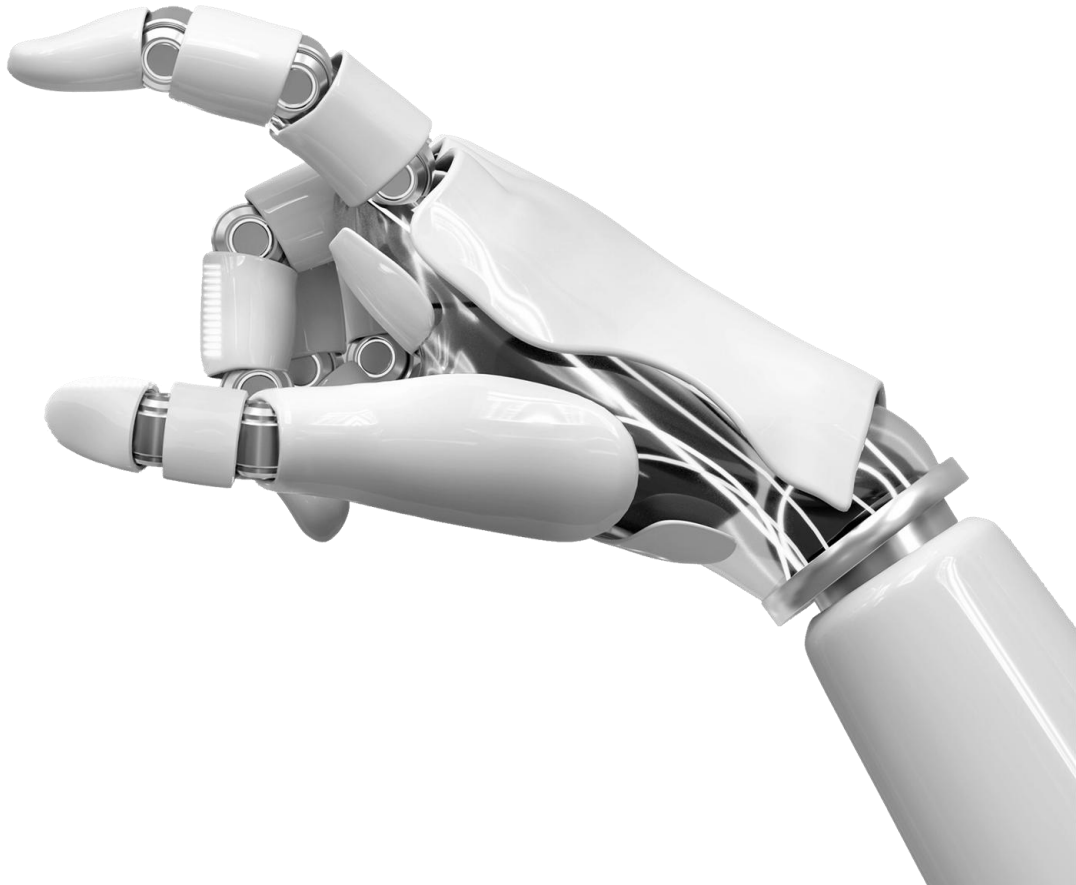
# AX 시대, 데이터 주권의 필수 인프라
# KT Secure Public Cloud

# Index

I.

# AX 시대의 클라우드 인프라

1. 하이퍼스케일 클라우드와 데이터 주권
2. KT-MS 하이퍼스케일 클라우드



# 01. 하이퍼스케일 클라우드와 데이터 주권

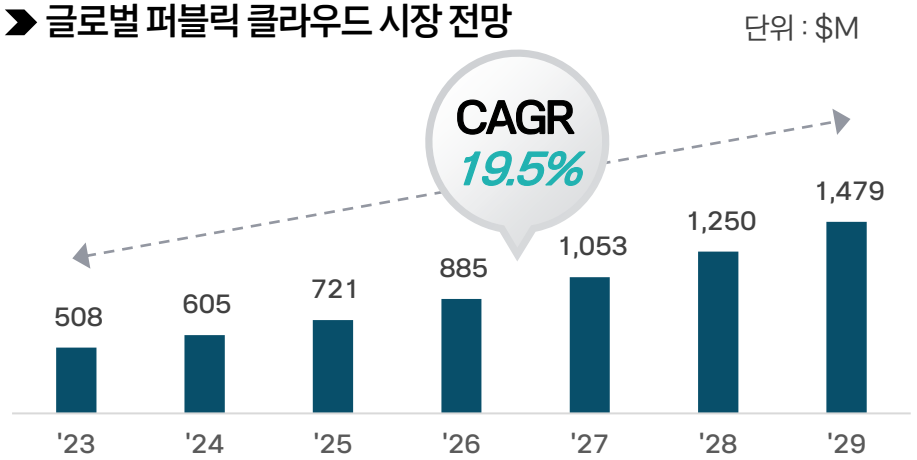
AX 시대가 도래하면서 기업 고객은 최신 AI 기술을 신속히 도입할 수 있는 하이퍼스케일 클라우드가 필수로 인식하고 있는 반면, 글로벌 단위 하이퍼스케일 수준 운영으로 인한 자국 데이터의 해외 상주 및 접근 등 보안 침해 우려에 대한 데이터 주권 이슈가 커지고 있음

## | 하이퍼스케일 퍼블릭 클라우드

### 초고속 AX 시대의 필수 인프라, 하이퍼스케일 클라우드

➤ ChatGPT 출시 타임라인


➤ 글로벌 퍼블릭 클라우드 시장 전망



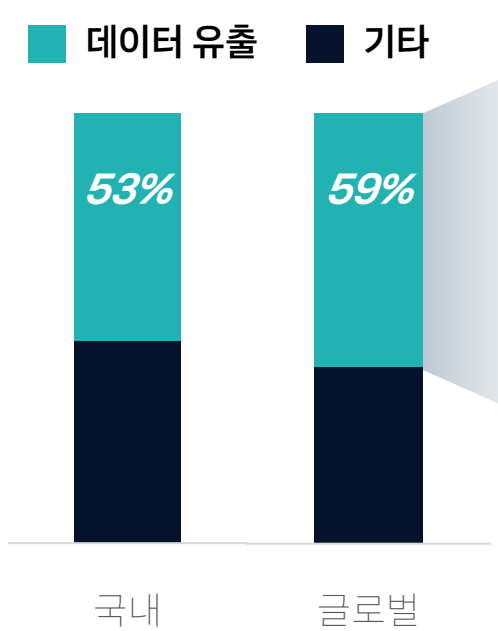

Source : Gartner (2025)

## | 데이터 주권

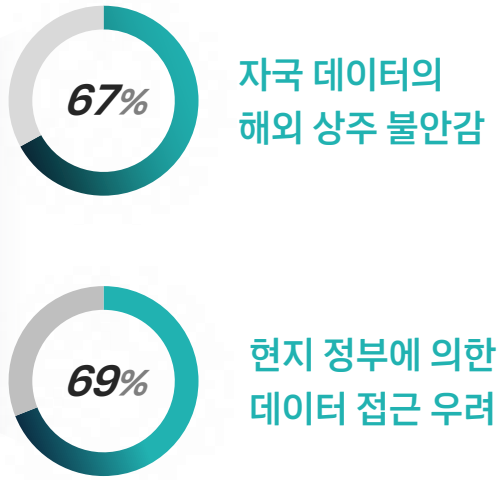
But,

### 데이터 유출로 인한 데이터 주권 이슈로 클라우드 도입 우려

➤ 클라우드 도입의 주요 장애 요인[1)]




➤ 우려하는 데이터 유출 형태[2)]




1) KDI, 클라우드에 대한 실태 및 인식조사 (2021), Fortinet, Cloud Security Report(2024); KT Analysis
2) Capgemini Research Institute, Cloud Sovereignty Survey(2021) ; KT Analysis

# 02. KT-MS 하이퍼스케일 클라우드

KT는 AI, 보안, 안정성 등에서 글로벌 최고 수준인 Azure를 기반으로 MS 본사와의 다이렉트 협력체계를 통해 데이터 주권은 지키면서 한국 기업 고객들의 성공적인 AX를 지원할 수 있는 최상의 하이퍼스케일 클라우드 서비스를 제공함

Microsoft Azure

kt

**KT-MS 클라우드**

## AI

### 다양한 최신 AI 모델 제공

- ChatGPT
- Copilot
- Phi
- Llama

✓ AI 챗봇 시장 81% 점유[1]

✓ CSP로는 독점 공급

## 보안

### 글로벌 최고 수준의 보안성 제공

제로 트러스트 Top 랭킹[2]

*CSP 3사 중 유일*

✓ 매년 10억불 이상 보안 투자

✓ 34,000명 보안 인력 상주

## 안정성

### 국내·외 최다 리전으로 가용성 및 안정성 보장

CSP 3사 국내 및 글로벌 리전 개수[3]

| | Azure | aws | Google Cloud |
|---|---|---|---|
| 국내 | 2개 | 1개 | 1개 |
| 글로벌 | 70개 | 31개 | 35개 |

## Global

### MS 글로벌 본사의 다이렉트 기술지원

고객 — kt — 본사

vs. 고객 — MSP — CSP 한국 — CSP 본사

## Expert

### KT-MS 협력 AX 전문가 서비스 제공

AXD 센터

AX 전담 전문가 조직(Cloud 포함)

kt 200명 + 100명

## 협력

### 클라우드 서비스 고도화 공동 개발

kt — 서비스 고도화 — Product Group

1) statcounter. AI Chatbot Market Share Worldwide(2025)
2) The Forrester Wave: Zero Trust Platforms(2025)
3) '25년 8월 기준, 각 사 공식 홈페이지

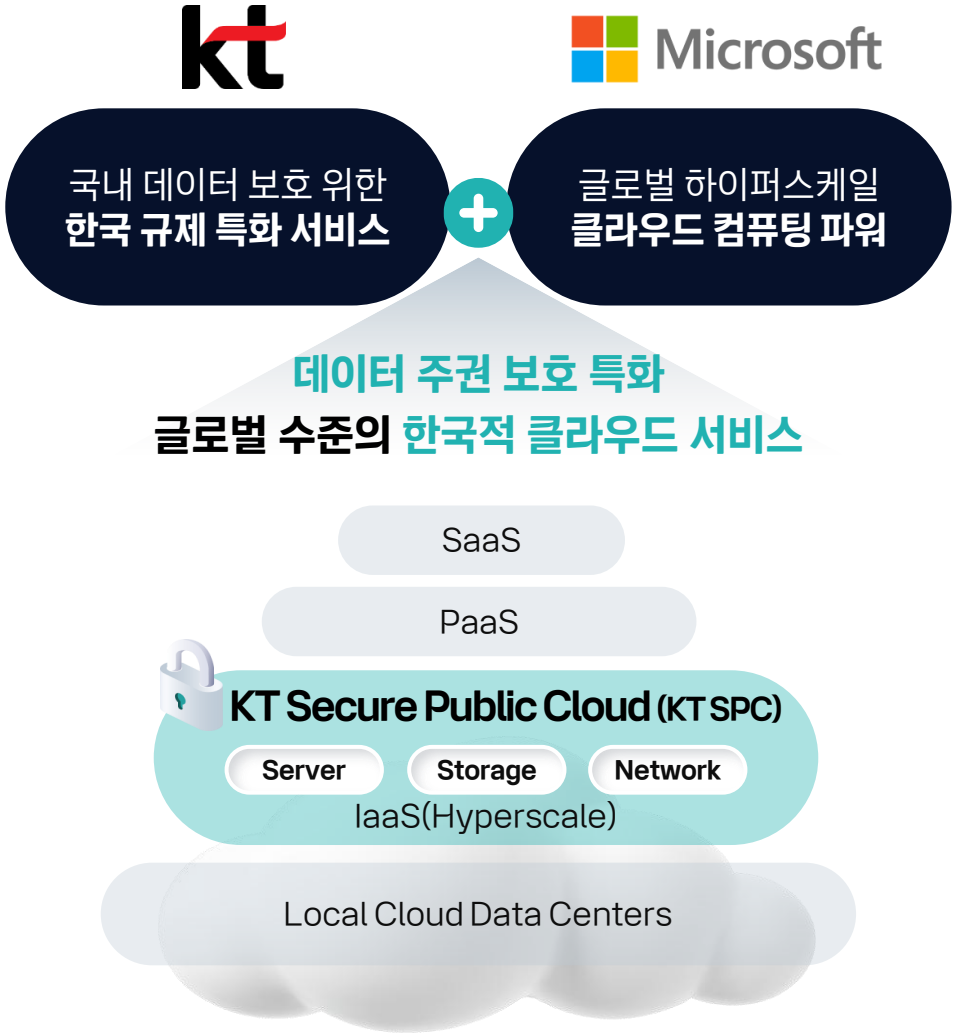
II.

# KT Secure Public Cloud (SPC)

1. KT Secure Public Cloud(SPC) 란
2. 주요 특징
3. KT SPC 보안성 검증
4. Demo
5. 도입사례

# 01. KT Secure Public Cloud (SPC) 란

KT는 우리나라 기업 고객의 AX 추진의 근간이 되는 데이터 보안 강화를 위해, 글로벌 하이퍼스케일 클라우드 컴퓨팅 파워 기반 데이터 주권 (Data Sovereignty) 특화 한국적 Secure Public Cloud 서비스를 MS와 공동 제공함




## I KT SPC 주요 특징

**1 국내 데이터 상주**

**국내에 물리적으로 위치한** 퍼블릭 클라우드 인프라 운영


**2 국내 보안 컴플라이언스 적용**

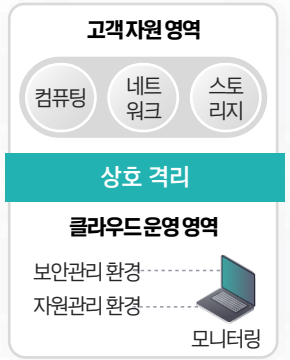
**국내 법제도 및 기업 보안** 맞춤형 서비스 적용


**3 데이터 全 생애주기 보안**

**데이터 보안 등급별 운영 全 단계 암호화 기술 제공**


**4 고객 자원 소유권 강화**

고객 자원의 **직접 관리 및 운영자와 격리된** 환경 제공



# 02. 주요 특징 | ① 국내 데이터 상주

KT SPC는 고객의 데이터 주권을 보호하기 위해 한국 내 데이터 상주 요건을 원칙으로 하며, 이를 위해 국내 서비스와 일부 아·태(Asia-Pacific) 서비스의 사용 범위를 국내 리전으로 자동화된 코드로 설정하여 강제화함

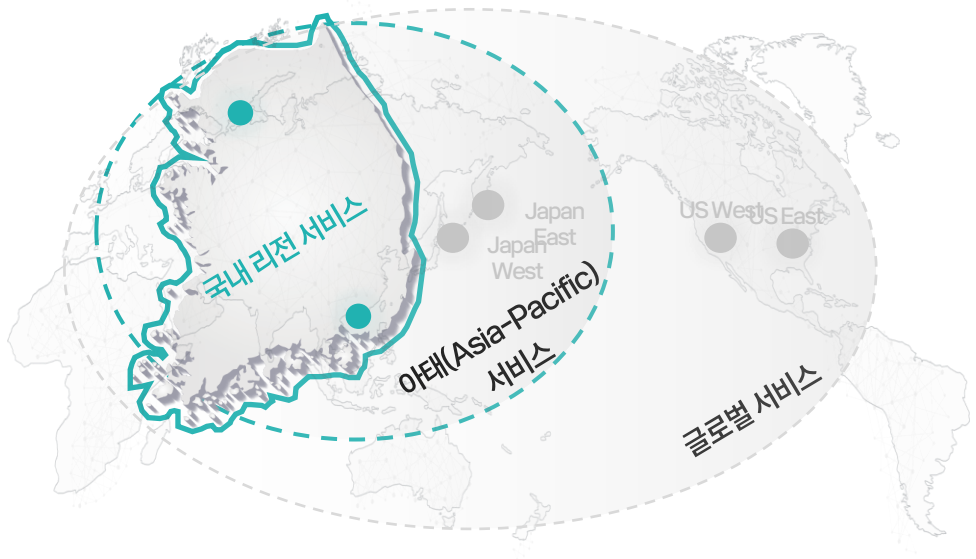
## 데이터 상주 (Data Residency) 의미

**데이터 상주란?**

자국민, 기관의 데이터를 타국이 통제하거나 감시할 수 없도록
데이터가 생성된 국가/지역에 저장되고 처리되어야 함을 의미

## 클라우드 서비스 위치 기반 데이터 상주 범위

**Azure의 200여개 서비스 중 국내 상주 요건 준수 114개 서비스 제공**
**: 국내 + 아태 서비스 일부**




## 자동화 기반 데이터 상주 정책 강제화

**국내 규정을 준수하는 자동화된 코드를 통해 데이터 위치 통제**

개인정보 보호법 제28조의8 (개인정보의 국외 이전) **준수**

① 개인정보처리자는 개인정보를 국외로 제공·처리·위탁·보관 하여서는 아니 된다

**데이터 상주 프로그래밍**

**PaC (Policy as Code)**

```
"listOfAllowedLocations": {
  "type": "Array",
  "metadata": {
    "description": "The list c
    "strongType": "location",
```

**예시**

국내 리전 강제화 및 해외 자원 생성 제한

# 02. 주요 특징 | ② 국내 보안 컴플라이언스 적용

KT SPC는 국내 법제도의 기술적 보안 요건을 반영한 보안 정책을 기반으로, 기업 고객이 포함된 산업 및 내부 요구 규제 사항도 적용 할 수 있는 확장성 있고 유연한 보안 컴플라이언스 체계를 제공함

## 국내 법제도의 기술적 보안 요건 반영

- 공공데이터 이용법
- 데이터기반 행정 활성화법
- 데이터산업 진흥법 …

데이터 규제


디지털 보안 규제

- 개인정보보보법
- 위치정보보호법
- 전자서명법 …

산업별 규제

- 전자금융거래법
- 산업기술보호법
- 국가공간정보법 …

| 기술적 보안 요건 |
|---|
| 1 자산 인벤토리 구축 |
| 2 패치 관리 |
| 3 가용성 확보 |
| … 백업 및 복구 관리 |
| 8 암호키 관리 |
| 9 네트워크 암호화 |
| … 악성코드 탐지 및 방어 |
| 16 권한 위임 및 최소 권한 원칙 |
| 17 사용자 인증 |
| … 로그 수집 관리 |
| 26 이상 행동 탐지 |
| 27 인터넷 접속 통제 |
| 28 전용 단말 사용 |
| 29 취약점 스캔 및 관리 |
| … |

기술적 보안 요건 반영

## KT SPC 보안 정책 적용

### KT SPC 보안 정책

일반 정책 + 산업 규제 대응 정책

일반 정보시스템 운영관리 및 정보보호를 위한 정책

산업별 규제 충족을 위한 보안 정책

■ **KT 사례 : 총 873개 정책 적용(일반 814개, 산업 규제 59개)**

| 보안 영역 | 세부 | 정책 반영 사항 |
|---|---|---|
| ID 관리 | 사용자 권한 관리 | Azure Resource에 접근하는 계정에 최소한의 권한을 부여 |
| | 사용자 식별 | Azure Resource에 접근하는 계정은 고유한 계정명을 부여 |
| 네트워크 보안 | 정보시스템 접근 | Azure Resource에 접근 시, MFA 등 강화된 인증을 사용 |
| | 인터넷 접속 통제 | 개인정보 저장 DB는 공개 네트워크에 위치하지 않도록 제한 |
| | … | |
| 데이터 보호 | 데이터 접근 정책 | Azure Resource의 물리적 위치는 대한민국 국내로 제한 |
| | 데이터 암호화 | 중요 정보 저장 시 고객 관리형 키를 사용하여 자원 구성 |
| | … | |
| 백업 및 복구 | 백업 및 복구 관리 | 중요 정보는 저장장소로부터 물리적으로 거리가 있는 곳에 소산 보관 |
| | 이중화 및 백업 | 접속 네트워크 회선과 장애발생에 대비가 필요한 자원은 이중화 |
| | … | |

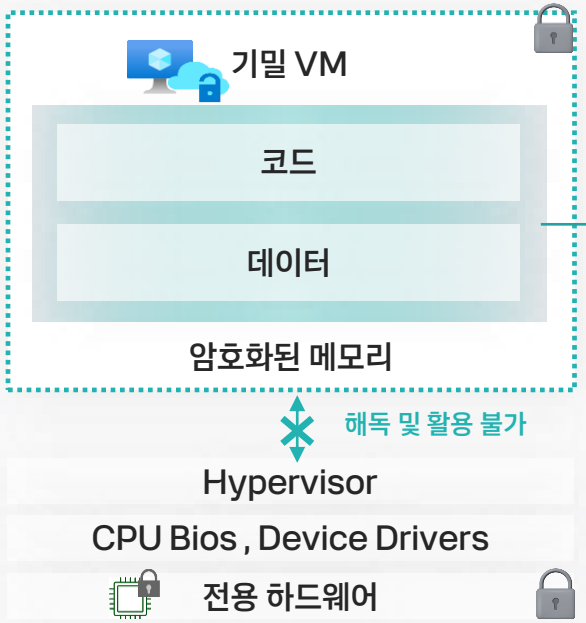
…

# 02. 주요 특징 | ③ 데이터 全 생애주기 보호

KT SPC는 기밀 컴퓨팅을 사용하여 메모리에서 사용되는 데이터를 암호화하고, 고객키를 안전하게 보관하는 관리형 HSM 서비스를 활용하여 저장 중인 데이터를 암호화하며 TLS 기반 전송 암호화를 적용해  데이터 전 생애 주기에 걸쳐 보안성 강화함

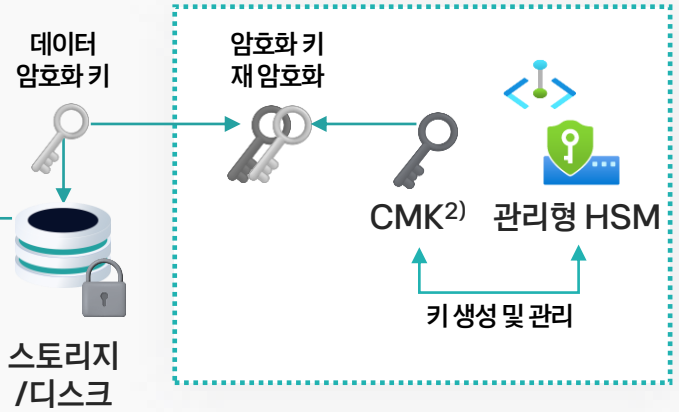
## 사용 중(in Use) 데이터 보호

기밀 컴퓨팅의 하드웨어가 생성한 TEE[1] 내
메모리에서 사용 중 데이터 실시간 암호화



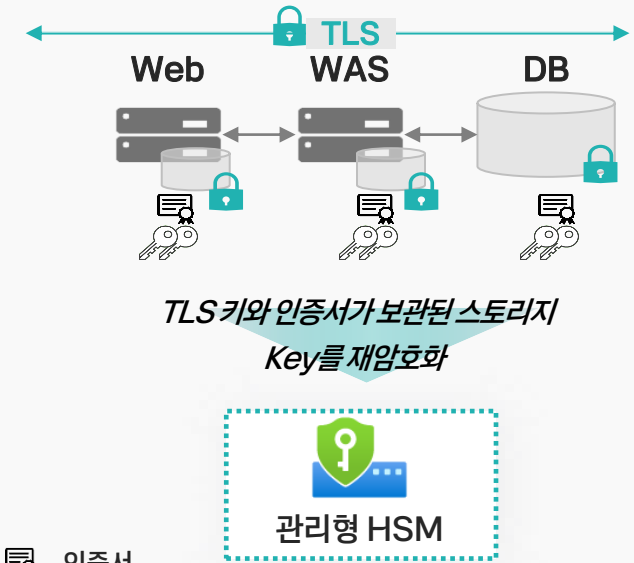

## 저장 중(at Rest) 데이터 보호

하드웨어 모듈인 mHSM고객전용에서 생성된 키로
스토리지/디스크 데이터 암호화 키 재암호화




## 전송 중(in Transit) 데이터 보호

TLS(통신암호화 프로토콜) Key와 인증서가
보관된 스토리지 Key를 mHSM으로 재암호화




1) TEE(Trusted Execution Environment): 외부 시스템으로부터 격리된 안전한 환경에서 코드와 데이터를 보호하면서 실행 할 수 있도록 만든 하드웨어 기반 보호 환경
2) CMK(Customer-managed key): 고객 관리형 키로 관리형 HSM에서 생성 되었으며, 데이터 암호화 Key를 재암호화는 KEK(Key Encryption Key) 역할 수행

# 암호키 유출 걱정 없는 mHSM

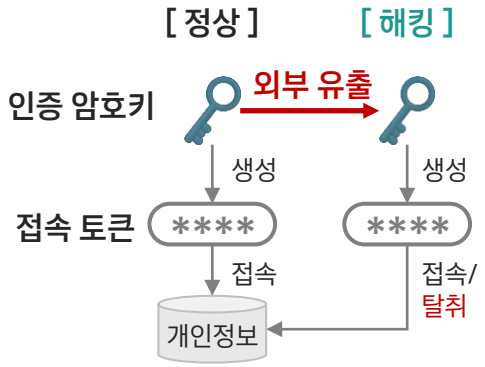
## C사 해킹 사례

**개요**

'25년 3,370만명 개인정보 유출

**원인**

### ① 인증 암호키 외부 유출




- 개발자가 퇴사하면서 인증키 유출

### ② 동일 암호키 장기간 유지

- '24.12 퇴사 이전 인증키 최근까지 유효

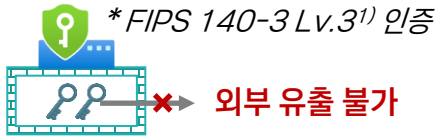
### ③ 이상 행동 감시 X

- 암호키 유출, 접속 토큰 생성 감지 못함

## KT SPC mHSM을 통한 암호키 완벽 보안

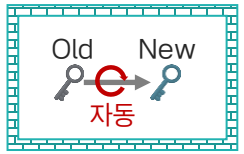
**암호키 유출 불가, 자동화 및 체계적인 암호키 관리**

### ① mHSM 외부로 암호키 유출 불가



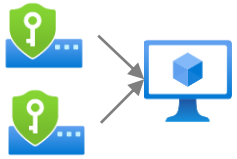

- 암호키는 mHSM 내부에만 존재
- 클라우드 운영자도 접근 불가

### ② 암호키 주기적 자동 갱신




- 주기적인 갱신으로 기존 키 재활용 불가

### ③ 이상 행동 감시 및 경고 자동화



- 암호키 관련 이상 행동 자동 모니터링
- 이상 발생 시 자동 상황 전파

### ④ KT SPC 운영 노하우 추가 지원

**암호키 생애주기 거버넌스 체계 수립**

[ 키관리 프로세스]
- 키 정책 수립
- 키 생성/저장/사용
- 키 교체/폐기
- 모니터링/감사

[ 키관리 조직 ]
보안팀
운영팀
개발팀
감사팀

**역할별 권한 제어로 내부자 상시 통제**

| 작업 | 키소유자 | 키이용자 | 감사자 | … |
|---|---|---|---|---|
| 키 생성 | ○ | | | |
| 사인 요청 | | ○ | | |
| 감사 | ○ | | ○ | |
| … | … | | | |

**백업/복구 체계로 안정성 강화**


- mHSM 클러스터 구성
- 주기적 백업

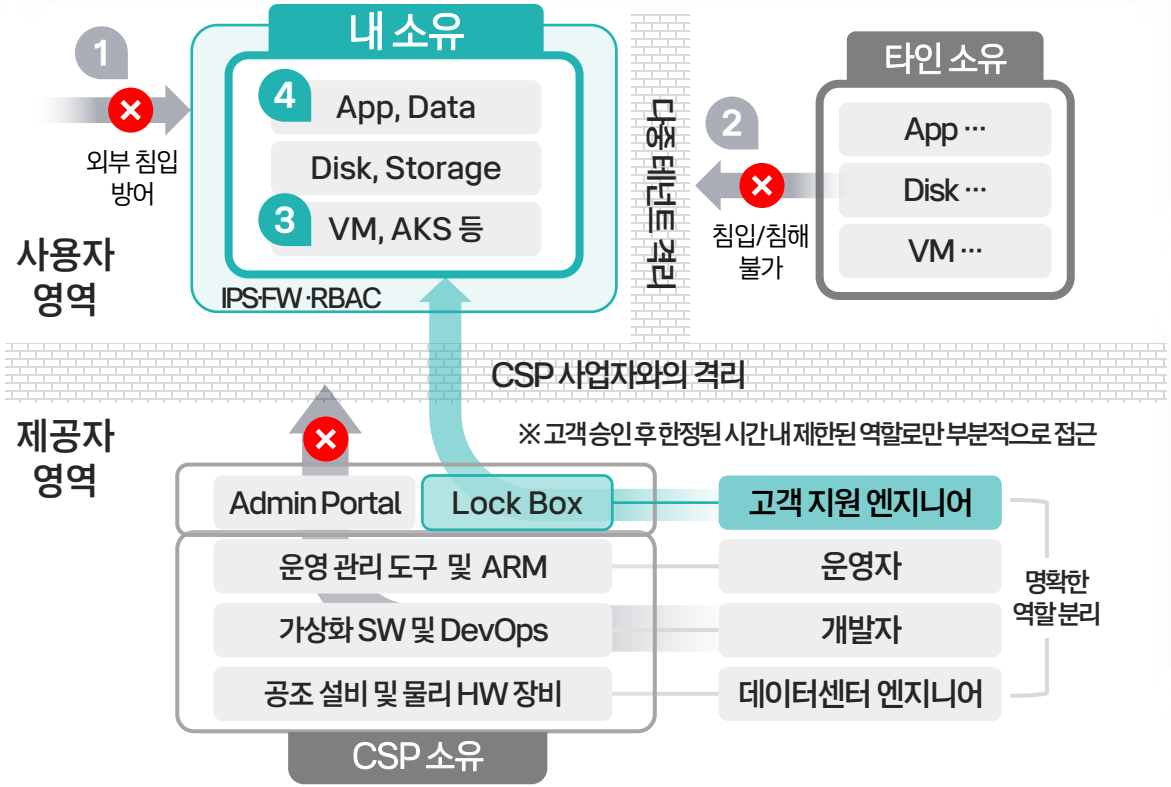
1) Federal Information Processing Standard, 미국 연방 정보 처리 표준, 사실상의 글로벌 보안 벤치마크

# 02. 주요 특징 | ④ 고객 자원 소유권 강화

KT SPC는 고객이 직접 생성한 자원에 대해 고객 소유권을 보장하며, 강력한 격리 기능을 통해 타사는 물론 CSP 사업자로부터 고객 소유 자원을 격리시키고, CSP 엔지니어 지원이 불가피한 경우 고객 승인 후 제한된 역할로 접근을 통제함

## 자원 소유권의 정의와 범위

자신의 계정으로 생성한 가상화 자원과 데이터를 자유롭게 이용/삭제할 수 있는 권리이며
VM, AKS, Disk, Database, Files 등의 서비스를 대상으로 함




## 자원 소유권의 위협 요인 및 대응 방안

| | | | |
|---|---|---|---|
| 외부의 위협 | 1 | 외부에서의 익명 사용자의 침입 | IPS·FW·Entra ID·RBAC·ZTA 기반 침입 및 수평 이동 차단 |
| | 2 | 타인의 과도한 자원 사용으로 내 서비스의 성능 저하 | 서비스별 QoS 자동 설정 통해 시끄러운 이웃 방지 및 성능 유지 |
| 자원내부 위협 | 3 | 특정 자원에서 문제 발생 (VM Hang, Resource Deadlock) | 운영투명성 제공 고객 승인 절차 또는 사후 보고 체계 하에서 표준 관리도구 통해 JIT[1] 접근 |
| | 4 | 악의적 프로그램이 중요 정보 탈취 | 운영투명성 제공 사용·저장 데이터 이중 암호화 및 고객 증명 서비스로 투명성/안전성 제공 |

1) JIT (Just In Time) 시스템에서 정의한 표준 접근 시간을 의미하며 통상 개별 작업에 필요한 최소의 시간

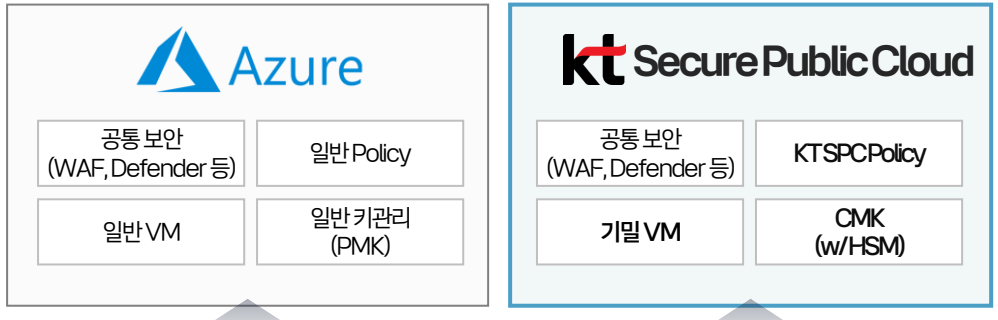
# 03. KT SPC 보안성 검증

제3자를 통한 객관적인 보안성 검증 결과, KT SPC는 일반 Azure 보다 고수준의 보안성을 보유한 것으로 나타났고, CSAP 기준도 대부분 충족하는 것으로 나타남

## 제3자 보안성 검증

검증 기관 **theori**

세계 최대 해킹대회 'DEF CON CTF' 최다 우승(8회) 기록보유




**총 208개의 공격 시나리오로 비교 검증**

| 단계 | 공격행위 | 주요 목적 | 시나리오 |
|---|---|---|---|
| 1단계 | Web Application 침해 | 초기 진입 | 14개 |
| 2단계 | N/W인프라 노출/공격 | 내부망 이동 | 36개 |
| 3단계 | 공급망 보안 | 우회 침입 | 8개 |
| 4단계 | Azure 권한 탈취 | 클라우드 리소스 장악 | 76개 |
| 5단계 | Host 서버 권한 탈취 | 시스템 장악 | 74개 |

## 보안성 검증 결과

### 사이버 공격 방어율

일반 Azure **56%** 116건 < KT SPC **85%** 177건(+61)

### 공격 체인

정찰 → 무기화 → 전달 → 실행 → 설치 → **제어** → **목표달성**

**KT SPC** 추가 방어(61건) 중 **74%(45건)**가 **[제어]** 및 **[목표달성]** 단계 방어

### CSAP

CSAP '중' 등급 기술항목 43개 중

**KT SPC 98% (42건) 충족**

* 불가항목(1개) : CSP(Azure)의 관리 영역

# 04. Demo

KT SPC의 핵심기능인 데이터 상주, 보안 컴플라이언스 준수, 데이터 全생애주기 보호와 관련 기술을 시연

## Demo Case

| | |
|---|---|
| 1 데이터 상주 | 국내 리전으로 제한 |
| | 해외 리전에 자원 생성 불가 |
| 2 보안 컴플라이언스 준수 | 보안 정책 적용 |
| | 정책 준수 감사 |
| 3 기밀 컴퓨팅 활용 사용중 데이터 보호 | 신뢰성이 검증된 기밀 컴퓨팅 환경 구성(Attestation) |
| | 기밀 VM의 메모리 암호화를 통한 사용중 데이터 보호 |
| 4 mHSM 활용 저장(At-Rest) 데이터 보호 | 암호화 키 접근통제, 보안 및 감사 |
| | mHSM 활용 기밀 VM 디스크 보호 |

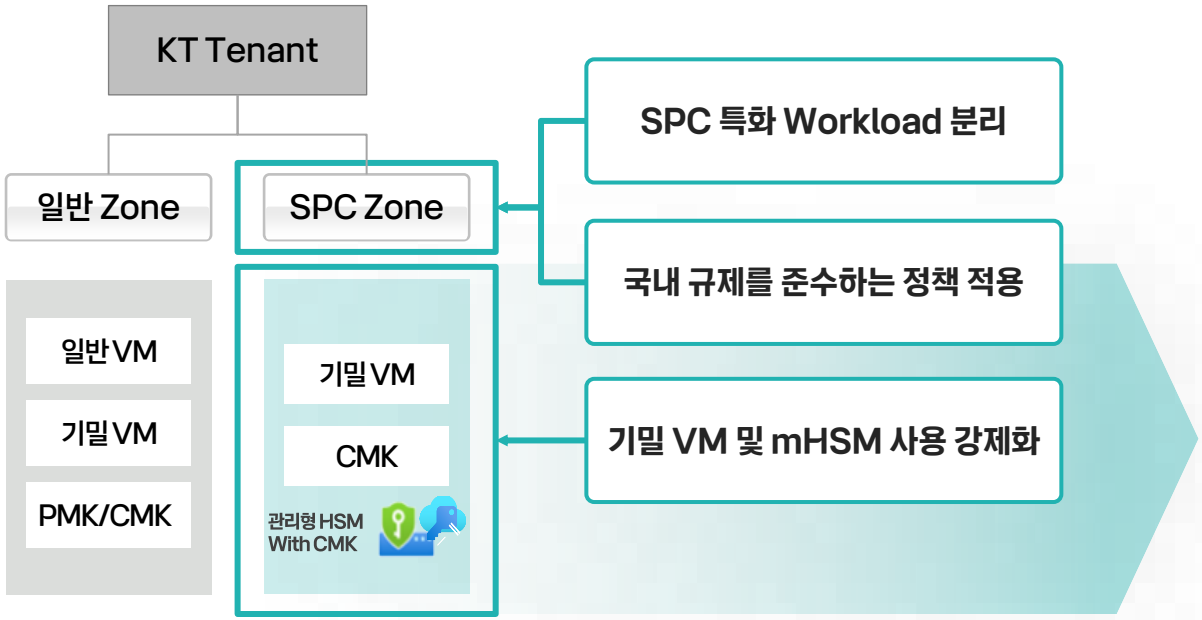
# 05. 도입 사례 | KT 사례

KT SPC 특화 정책을 적용할 수 있도록 랜딩존을 분리 구성하고, 고객 민감 데이터를 활용하는 시스템을 SPC Zone으로 이전하여 데이터 분석 활용성 증대, 보안 수준 강화 등의 효과를 제공함

## KT SPC 기반 랜딩존 구성

**랜딩존 이란?**

기업의 비즈니스 목표와 Align된 클라우드 서비스를 제공할 수 있도록 **체계적**으로 구성한 **클라우드 기반 환경**




## KT SPC 적용 시스템

**적용 현황**

- KT SPC 전환 대상 시스템 **61개** 선정
  : **개인정보보유여부(PII), 데이터 중요도** 등 고려
- 이중 37개 전환 완료, 나머지는 '26년 3월까지 전환 완료 예정

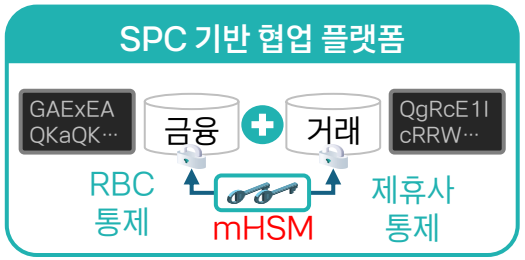
**적용 시스템**

| | |
|---|---|
| **빅데이터 타겟 시스템** | 마케팅을 위한 고객 민감 데이터 분석<br>Data \| 결제이력, 연령/성별/단말, 컨텐츠 사용이력 등<br>➔ 고객 민감 **데이터 분석 활용성 증대** |
| **제3자 제공 공동관리 플랫폼** | KT와 그룹사간 제3자 정보 동의 수집 및 관리<br>Data \| 동의 정보 조회 처리 이력(개인정보), 마케팅 정보 등<br>➔ 고객/그룹사 **정보 이용 신뢰성 강화** |
| **KT MVNO 통합 채널** | KT 알뜰폰 사업자 상품 가입 고객 관리<br>Data \| 성명, 생년월일, 주민등록번호 등 고객 개인정보<br>➔ 개인 정보 보호 및 **보안 수준 강화** |

...

# 05. 도입 사례 | 글로벌 사례

KT SPC는 헬스케어, 금융, 제조업 등에 적용하여 민감정보의 안전한 처리, 신뢰 기반 협력, AI 성능 개선 등의 효과를 제공함

| 산업 | 헬스케어 | 금융 | 제조 |
|---|---|---|---|
| 기관명 | UAE 정부 | RBC<br>(캐나다 1위 은행) | BOSCH<br>(세계 최대 車부품사) |
| 내용 | **1백만명 유전자 정보 분석**<br>  <br>• 백만명 유전자 정보의 안전한 처리 목적<br>• **UAE 리전으로 제한,** 국외 반출 방지<br>• mHSM 활용 **UAE만이 데이터 통제**<br>• 기밀 컴퓨팅 **신뢰 환경으로 안전한 글로벌 연구** 협업 | **제휴사 정보 결합 초개인화 서비스**<br>  <br>• 제휴사 정보와 결합한 안전한 초개인화 서비스 **목적**<br>• mHSM으로 **양사 데이터 통제권 유지**<br>• 기밀 컴퓨팅에서 **결합 정보를 암호화**하여 유출 방지 | **주행보조시스템 AI 성능 개선**<br>  <br>• 개인정보 비식별화로 AI 성능 저하 문제 **극복 목적**<br>• 기밀 컴퓨팅 **환경에서 개인정보 포함 원본 학습**<br>• AI 성능 개선 및 주행보조시스템 정교화 개발 지원 |
| Biz Value | **대규모 민감정보의**<br>**안전한 처리** 및 글로벌 협력 | **데이터 통제권을 유지**하면서<br>업체간 **신뢰 기반 협력** 지원 | 개인정보는 보호하면서<br>**원본 활용 AI 성능 개선** |

III.

# KT의 차별화된 클라우드 서비스

1. KT 클라우드 통합 서비스 오퍼링
2. KT SPC 체험 워크샵 제언

# 01. KT 클라우드 통합 서비스 오퍼링

KT는 고객의 SPC 전환 여정이 데이터 주권이 보장되는 안전한 클라우드 인프라를 통해 진행될 수 있도록 KT-MS 전략적 협력 기반의 전문인력을 통해 컨설팅 → 랜딩존 설계/구축 및 마이그레이션 → 운영의 전 IT 서비스 생명 주기에 걸친 통합 서비스를 제공함

## kt Secure Public Cloud 서비스

### Consulting

Sovereignty based
**클라우드 전환 전략 수립 컨설팅**

- 법규제 및 보안 컴플라이언스를 고려한 **보안등급 수립**
- 보안등급에 따른 **SPC 전환 대상** 및 일반 전환 대상 식별
- SPC 대상 포함 클라우드 전환 계획 수립

### Migration

**KT SPC 랜딩존 설계/구축 서비스**

- 고객사 **서비스 유형별** 랜딩존 설계/구축(SPC 포함)
- **SPC 특화 정책 적용**을 위한 랜딩존 설계/구축

**KT SPC 마이그레이션 서비스**

- 서비스 유형별 최적 환경 구축 및 클라우드 전환 수행
- **SPC 관련 워크로드 이전 및 보안성 검증**

### Operation

**KT 클라우드 매니지드 서비스**

- SPC 인프라 통합 운영
- 플랫폼 기반 통합 운영 체계
- 클라우드 운영 자동화 및 자원 · 비용 최적화 수행

kt Cloud 전문조직(컨설팅/구축/운영) 약 200명 + kt Microsoft KT-MS AX전담조직(Cloud포함) 약 300명 + Microsoft Azure Cloud 기술지원

# 02. KT SPC 체험 워크샵 제언

KT SPC 도입 과정과 보안 통제에 관한 실습 중심의 2 Days 워크샵을 통해 KT SPC의 가치를 체험해볼 것을 제언

## 워크샵 목적

1. KT SPC 도입 과정 이해
2. KT SPC를 활용한 규제 대응 보안 통제 체험
3. 기밀컴퓨팅, mHSM을 활용한 데이터 전생애 보호 체험

## 워크샵 프로그램(案)

*2 Days*

### Chapter 1. KT SPC 전환 전략 수립

- KT SPC 도입 여정
- 데이터 보안 등급에 따른 SPC 전환 대상 선정

### Chapter 3. 규제 대응 보안 통제

- 규제 분석을 통한 보안 정책 도출
- 보안 정책 적용 및 감사

### Chapter 2. KT SPC 환경(랜딩존) 구성

- 클라우드 랜딩존의 이해
- KT SPC 랜딩존 구성

### Chapter 4. 데이터 전생애 보호

- 기밀컴퓨팅 활용 사용중 데이터 보호
- 관리형 HSM 활용 저장중/전송중 데이터 보호

# 감사합니다.

전략·사업 컨설팅 부문 | Cloud Lead