(ISO 27001 정보보호 국제표준 인증)

ISAE 3402 TYPE 2 SOC 인증 (Service Organization Control)
(국제감사인증위원회 인증)

(클라우드서비스 우수 SLA 인증)

Cloud의 보안체계와 준비도

- 공공기관의 민간 Cloud 도입을 위한 방향성

kt 기업사업컨설팅본부

2015.11.30

01 Cloud의 필요성 대두

- 지난 5년 전 스마트폰의 등장과 함께 폭발적으로 쏟아져 나오는 미디어/금융/게임/소셜 등 수 많은 서비스의 수용을 위해 민간에서는 Cloud가 필수적 IT Infra로 자리 매김 하였음

- 공공기관의 IT 서비스도 다각화 되고 국민 친화적으로 발전하면서 효율적인 인프라의 필요성과 함께 Cloud의 활용이 부각 됨

국가 R&D | 국가 학술정보 | 공공기관 스마트 협업 | CCTV 영상 보안관리 | 국가 대형 이벤트

초중고 S/W 교육 | 지자체 대민서비스 | 선거 관리 | 헌법 기관 자료 백업

02 민간 Cloud, 활용할 수 있을까?

- 민간분야 만큼 공공분야에서도 Cloud를 도입 해야 할 필요성이 있지만, 공공 시스템의 중요한 보안성에 대한 우려 등 부정적인 의견이 존재 함

적극적 도입 필요

- 공공기관 IT에 민간 Cloud를 도입하여 **효율적 투자/운영**
- **우수한 외부 IT Resource** 활용
- 민간 **Cloud 생태계 활성화**로 산업 발전효과
- 글로벌 사업자 대비 **국내 Cloud 경쟁력** 확보

부정적 도입 의견

- 공공기관이 **불특정 유저와 같은 플랫폼**을 공유할 수 있는가?
- 민간 Cloud가 **기존의 보안 수준**을 만족 시켜줄 수 있는가?
- 우리 기관만의 **별도의 환경**을 만들어 줄 수 있는가?
- **막연한 불안감**

Cloud의 장점을 유지하면서 Legacy 기반의 보안 수준을 제공해야 공공기관 도입이 가능

중소 개발사를 포함한 국내 IT 산업 발전에 도움이 되는 방향의 Cloud 생태계 조성 필요

03 보안 제공 수준

- Cloud 환경에서도 기본적인 수준의 보안 기능부터 Legacy 보안 수준의 항목을 제공
- 일부 항목에 대해서는 AWS, MS 등 Global Cloud에서도 갖추고 있지 않은 국내 Compliance 수준을 만족 시키는 보안 기능을 Local 기업이 갖추고 있음

	Public Cloud 기본 보안	가상화 기반의 보안 기능	LEGACY 기반의 보안 기능	사용자 별 물리적 분리
제공 내용	- Software Firewall - 유저 별 Network 분리 - Cloud 콘솔 계정	- 웹방화벽, 가상 IPS 등 **가상화 기반 네트워크 보안** - DB 암호화, 접근제어 등 **서버 기반 보안 솔루션**	- **Appliance IPS, Firewall** - DMZ/Private Network 분리 - **Dedicated Private 회선** 연동	- 특정 **User 그룹(공공기관) 별 별도 분리** 된 Zone 제공 - 특정 **User 단위 별도 시스템** 제공
사례	- 대부분 Cloud 사업자 제공	- **AWS, MS**: Trend Micro(IPS), WAF 등 **Global 3rd Party Tool** - kt:, SKT, LGU+ 등 **국내 사업자 : Global 솔루션** 및 **국내 보안 솔루션 탑재**(펜타시큐리티 등)	- **AWS, MS: 해당 없음** - **kt: Firewall**(Secure Zone), **Firewall+IPS**(Enterprise Zone)	- **AWS, MS: Government 전용** Cloud Zone 제공 - **kt: Enterprise/Government 전용** Cloud Zone 제공 **특정 User 단독 시스템(VPC)** 제공

❖ VPC: Virtual Private Cloud

04 해외 Cloud 사업자 대비 우수한 보안성 제공 사례(1)

- **AWS를 사용 중 보안에 대한 규제 이슈 및 높은 보안성 만족을 위해 kt ucloud biz 선택**

GS SHOP

- 기존 Legacy 인프라 및 AWS 환경에서 IT Infra 운영 중
- **정보통신망법 28조** 준수 및 **ISMS** 대응 가능한 보안기능 요구

구분	kt ucloud biz		참고(AWS)
	Public Cloud 기준	Enterprise Cloud 기준	
가상 네트워크 제공	계정 별 VLAN 단위 기본 제공	계정 별 VLAN 단위 분리 제공 DMZ/Private Zone 분리구조 제공	VPC 적용 시 별도 적용 가능
네트워크 보안	Software Firewall 제공	Appliance IPS+Firewall 제공	Software Firewall 제공
망분리(서비스/내부망)	미지원	Hardware Network 기반 제공	Virtual Network 기반 제공
로그 및 모니터링	ucloud watch(무상), Sycros(유상)		Cloudwatch
접근통제(콘솔)	OTP 및 멀티계정 권한제어		MFA 및 IAM 제공
외부 네트워크 연결	Site2Site VPN, 전용회선, MPLS-VPN 등 제공		Site2Site VPN
별도 시스템 Customizing	Baremetal 형태 제공		미지원

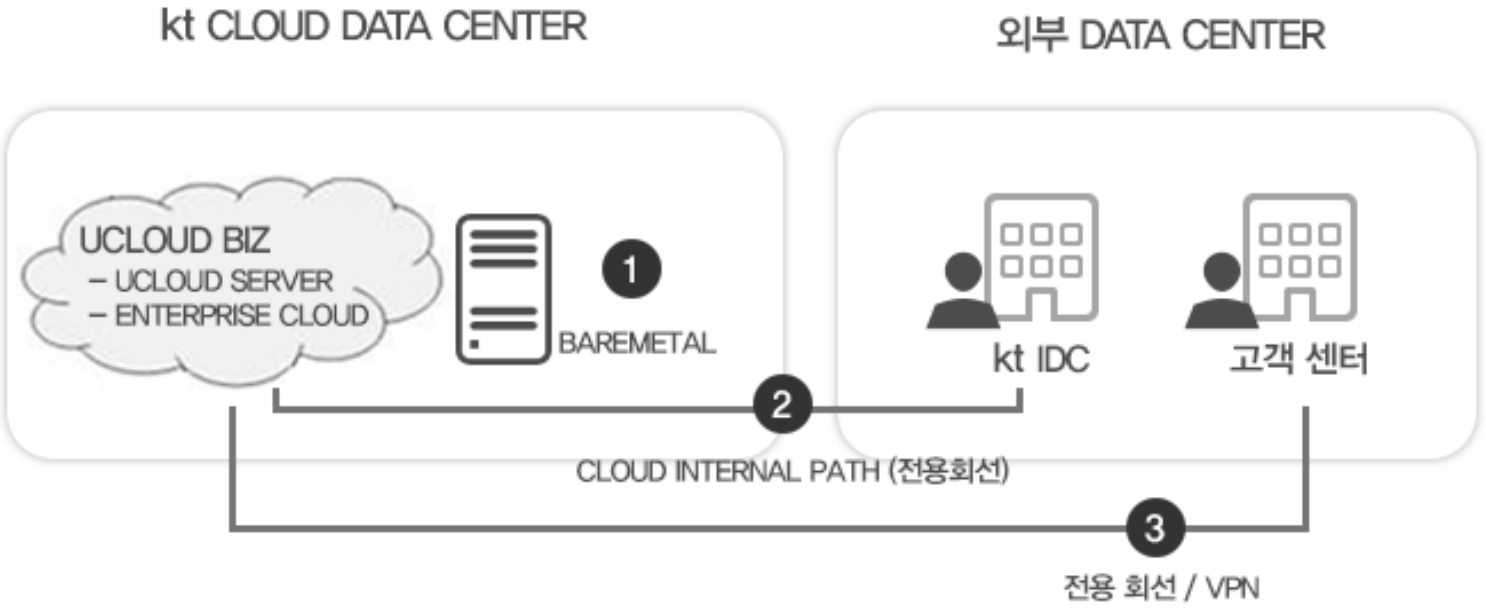
04 해외 Cloud 사업자 대비 우수한 보안성 제공 사례(2)

- 기존 사용 중인 Legacy 환경에서 Private한 연동을 통한 Infra 확장 구성

NEXON

com2uS 컴투스

- AWS의 경우 Public Network를 통한 Hybrid 구성 제공
- 전용회선 및 내부 패치를 통한 높은 보안 및 품질의 Hybrid 제공



- Global Cloud 서비스의 경우 Public Internet을 통한 연동 방식으로 망 폭주 시 품질 및 보안에 대한 우려가 있음
- 전용회선을 통한 Hybrid 구성 시 공공기관과의 완벽한 Private한 연동 및 확장이 가능

05 공공기관 수용 시 시나리오

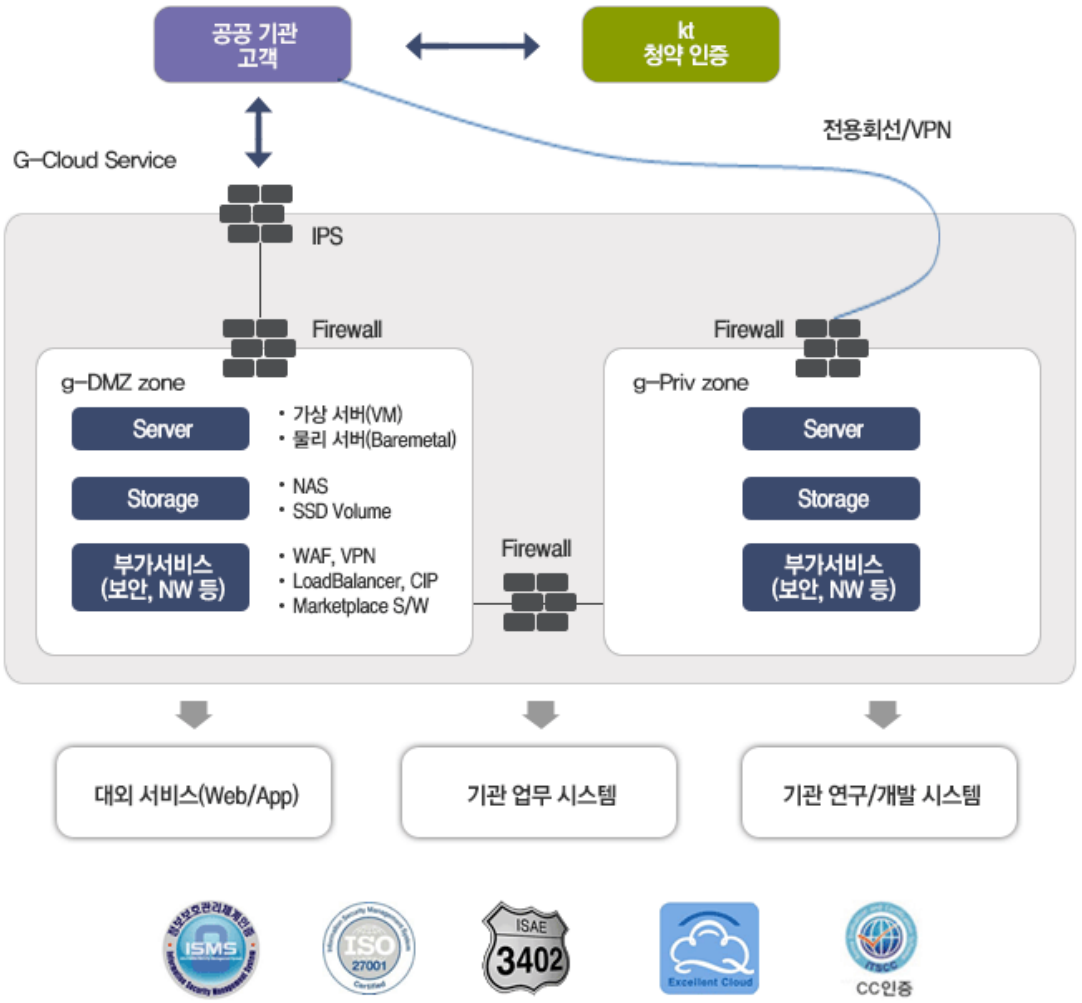
- 서비스 별 필요한 보안 수준에 만족 시킬 수 있는 Cloud 서비스를 채택하여 도입

서비스 수준에 따른 보안 민감도

서비스 유형	수용 방안	제공 보안 기능
단순 Web, App 등 보안 이슈가 없는 공공 서비스	Public Cloud	✓ Software 기반 Firewall, WAF, IPS 등 네트워크 보안 기능 ✓ DB 암호화, 백신 등 미들웨어 기반 보안 ✓ Cloud 콘솔 인증(OTP) 및 서버 권한제어
대국민 서비스 등 일반적인 수준의 공공 서비스	G-Cloud Zone	✓ IPS, Firewall, VPN 등 Appliance 기반의 네트워크 보안 기능 ✓ DMZ와 Private Zone의 물리적 분리 ✓ 물리적 전용회선을 통한 Private 연동
기관 내부 시스템의 Back-up/DR 및 주요 개인정보 수용 대외 서비스	G-Cloud Zone + VPC	✓ 물리적으로 분리된 전용 Cloud 시스템 제공 ✓ 별도의 네트워크/보안 장비 연동 등 Customizing
기관 내부 업무 및 보안에 민감한 수준의 Infra	On-Site VPC	✓ 기관 내부에 Cloud 시스템 구축 ✓ 원격 보안관제 및 시스템 운영 제공

06 공공기관 전용 특화 서비스 소개

- 인증된 공공기관에게만 제공이 되는 민간 사용자와는 분리 된 공공기관 특화 Cloud 존



1 공공기관 전용 Cloud Zone

- 물리적 분리(System, N/W, 보안)
- 인가된 공공기관 이용자만 계약
- 별도 G-Cloud 사용자 포탈

2 강력한 보안의 Cloud

- DMZ와 Private NW 분리로 Backend 시스템 격리
- CC인증 IPS 및 Firewall 보안 기본
- 사용 부처별 네트워크 분리
  - L2(VLAN)기반 보장
- 다양한 보안강화 부가서비스
  (웹방화벽, DB암호화, 웹쉘보호 등)

3 내부통제 신뢰성

- 완벽한 사설 네트워크(전용회선) 연동
- 클라우드데이타센터의 엄격한 출입 보안 통제
- ISO27001, ISMS 등 내부통제 인증

06 공공기관 전용 특화 서비스 소개

- G-Cloud는 국내 공공기관에 특화 된 보안 기능을 제공

CC 인증 보안 시스템 구성

CC인증 국산 보안 시스템으로 강력한 보안 구성

구분	장비 / 공급사	비고
IPS(침입탐지)	Sniper 10G IPS / 윈스테크	국내 보안전문 중소기업
방화벽	SECUI MF2/ 시큐아이	
웹방화벽	WAPPLESS/ 펜타시큐리티	국내(국정원) CC 인증

IPS, 방화벽 보안 관제 제공

전문 보안 관제 제공으로 운영 부담 해소

모니터링
이상트래픽 모니터링
(DDoS, Warm, 웹공격)

운영
(IPS/DDoS, FW, WAF
사용자 정책 적용

보안 매니지드 (IPS, FW, WAF)

대응, 사고분석
사용자 정의 정책 대응
침해사고 로그분석, 재발방지

보고서
장애처리, 월간 보고서

07 공공기관 전용 특화 서비스 소개

- 일반적인 Cloud 서비스에서 제공하는 논리적인 분리를 넘어서
  공공기관 별도의 물리적 H/W의 독립성이 보장된 Cloud 구성이 가능해야 함

KT VPC(Virtual Private Cloud)

- 논리적인 독립성을 제공하는 Public Cloud 외에 VPC를 통한 **물리적으로 분리 된 Cloud 제공**
  → Private한 환경의 Cloud 서비스

- 시스템의 사양, Service Offering을 **사용자 니즈에 맞게 Customizing** 가능

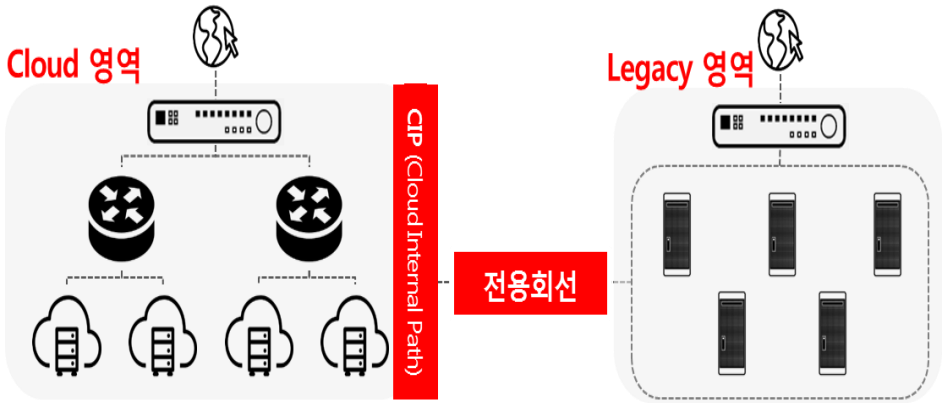
VPC의 민간 제공 사례: S전자

- 사용 목적: 자사 모바일 기기의 연동 서비스 운영 및 차세대 Fintech 서비스의 운영 인프라
- 자사의 보안 규정에 맞는 보안 장비 연동 등 Public Cloud에 제공하지 않는 Infra Customizing
- Cloud의 Maintenance와 별도로 자사의 스케쥴에 맞추어 Cloud 인프라 운영

08 공공기관 전용 특화 서비스 소개

- 공중 인터넷 망이 아닌 전용회선을 통한 Legacy 인프라와의 완벽한 보안 연동 필요

KT Hybrid Cloud 구성도



차별점

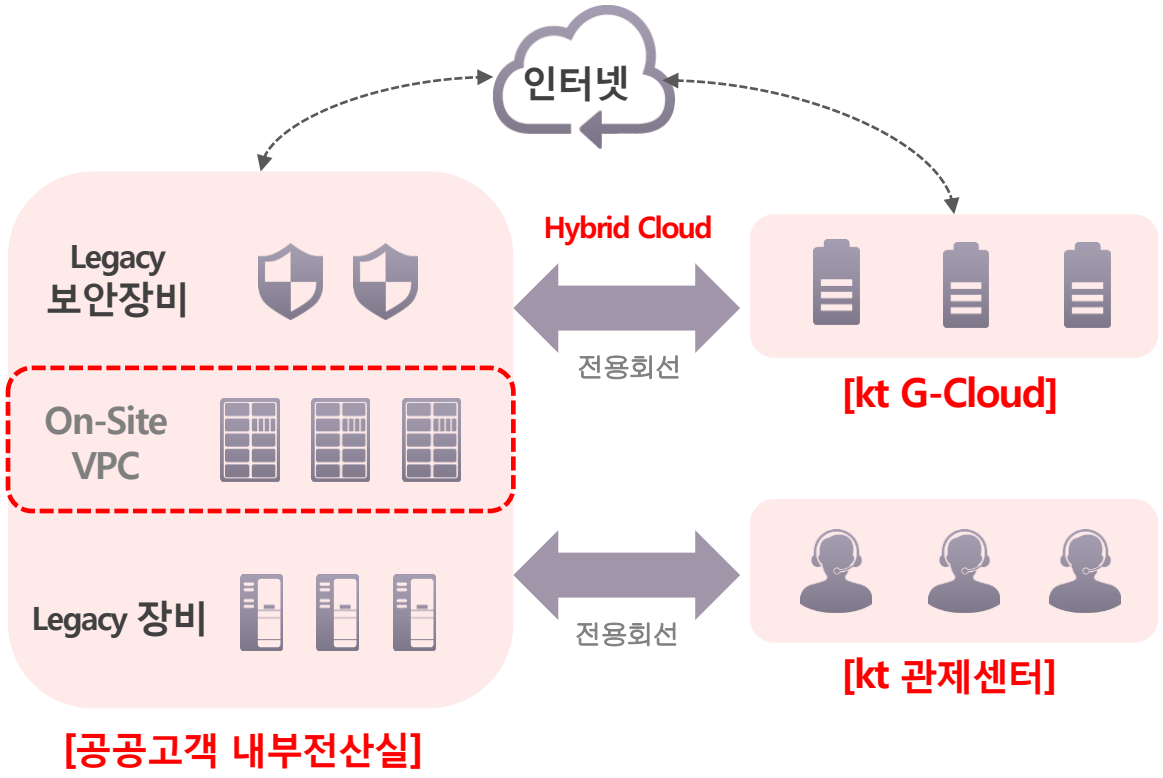
- Cloud의 서비스 네트워크 외에 **내부 연동을 위한 CIP(Cloud Internal Path) 제공**
- CIP에 폐쇄망인 전용회선을 연동하여 **원격 시설과의 네트워크와 Private한** 연동 구성

Hybrid Cloud 제공 사례

- 위메프: 자사 서비스 개발용 VDI에 전용회선을 연동으로 개발Source 유출의 원천 차단
- 넥슨코리아: 피파온라인 등 대형 PC온라인 게임을 IDC와 Private한 환경의 Cloud와 연동

09 공공기관 전용 특화 서비스 소개

• 공공기관 전산실 내 물리적으로 독립된 Private Cloud 구성하고, G-Cloud와 연동을 통해 DR 및 확장성 제공



1 공공기관 내부 VPC 구축

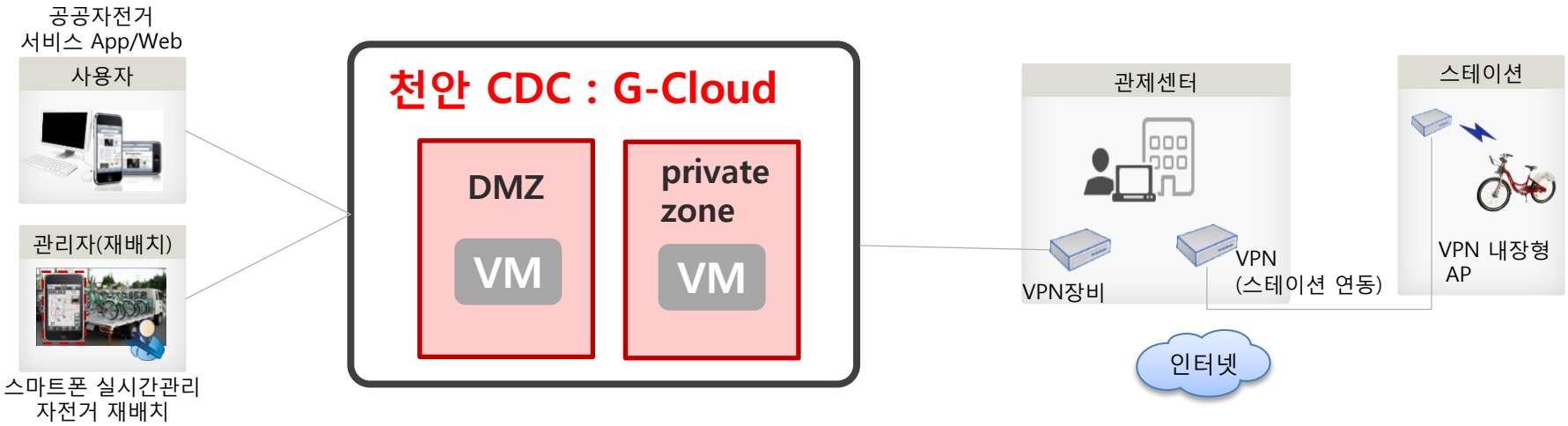
- 공공기관 내부 전산실에 VPC 구축을 통해 고객 니즈 충족
- kt 관제센터에서 24시간*365일 원격 모니터링을 통해 안정성 증대
- 추가 시스템 구축 등 인프라 커스터마이징 구축 가능

2 Hybrid Cloud 구성

- 서비스 확장/폭주 및 DR 상황에 따라 탄력적으로 인프라 확장
- 전용회선 기반의 Private한 Hybrid 구성으로 보안 및 품질 보장

[공공] 서울시 공공자전거 서비스

• 서울시 공공 자전거 서비스 제공을 위한 서버 환경을 G-Cloud 기반으로 제공



사업 개요

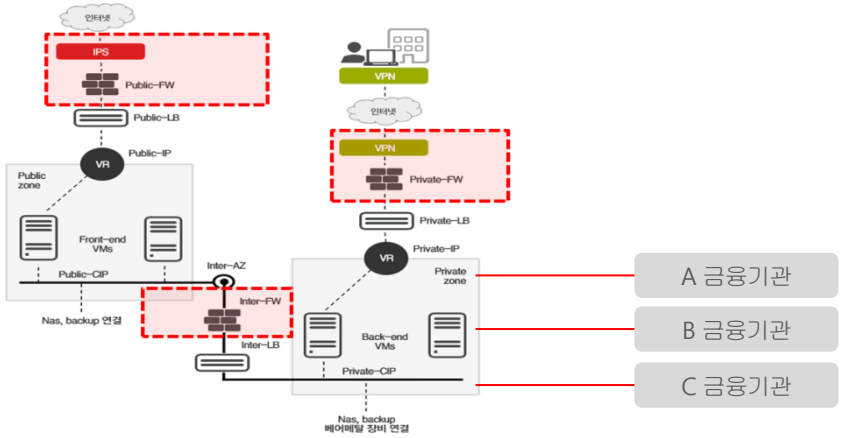
- ✓ **스마트폰을 통하여 공공자전거 대여**
- ✓ **사업 규모 및 일정**
  - 스테이션 150개소, 자전거 2,000대
  - 설치장소 : 5대 거점(4대 문안, 여의도, 상암, 신촌, 성수)
  - 서비스 제공시기 : 2015년 9월
  - 2020년까지 2만대로 확대 추진 예정

인프라 구성 특징

- ✓ **G-Cloud에 서버 인프라 수용**
  - 공공기관을 위한 전용 Cloud zone
  - CC인증을 받은 보안장치로 보안 기능을 강화
- ✓ **VPN을 통해 Hybrid cloud 구성**
  - VPN으로 관제센터와 연계
  - 자전거 Station을 VPN을 통해 제어

[금융] Samsung Pay / UDID

Samsung Pay



- ✓ **삼성전자의 금융 서비스(Fintech)**
  - **스마트폰 기반**으로 제공되는 **간편 결제** 서비스
- ✓ **Enterprise Zone 활용**
  - 보안 강화를 위해 **물리적인 IPS/방화벽 제공**
- ✓ **전용회선을 통한 Hybrid 구성**
  - 외부의 결제 관련 서비스 연동을 위해 **전용회선으로 보안이 확보된 Private 네트워크 구성**
- ✓ **VPC(Virtual Private Cloud)** 기반의 Cloud 시스템 구성
  - Enterprise Zone 내 **타 고객사 시스템과 물리적 분리**

UDID

- ✓ **Fintech 서비스 분야의 스타트업 기업**
  - **PG, 통신과금, 간편결제** 분야 서비스 준비 중
  - **높은 보안 기능이 필요**한 금융 분야의 신규 사업 추진 중 **자체 구축에 대한 높은 비용 부담을 Cloud로 해소**
- ✓ **금융 서비스의 Compliance 이슈**
  - 금융감독원의 보안성 심의 및 인가 대상에 해당
  - 각종 보안 심의 기준 협의 후 **최종 인가 예정**

Thank you