

5G+ 융합 생태계 변화에 따른 보안 대책 방안

2021.06.03

(주)원스
조학수 부사장

목차

- Part I: 5G+ 및 MEC 동향
- Part II: MEC의 보안 전략

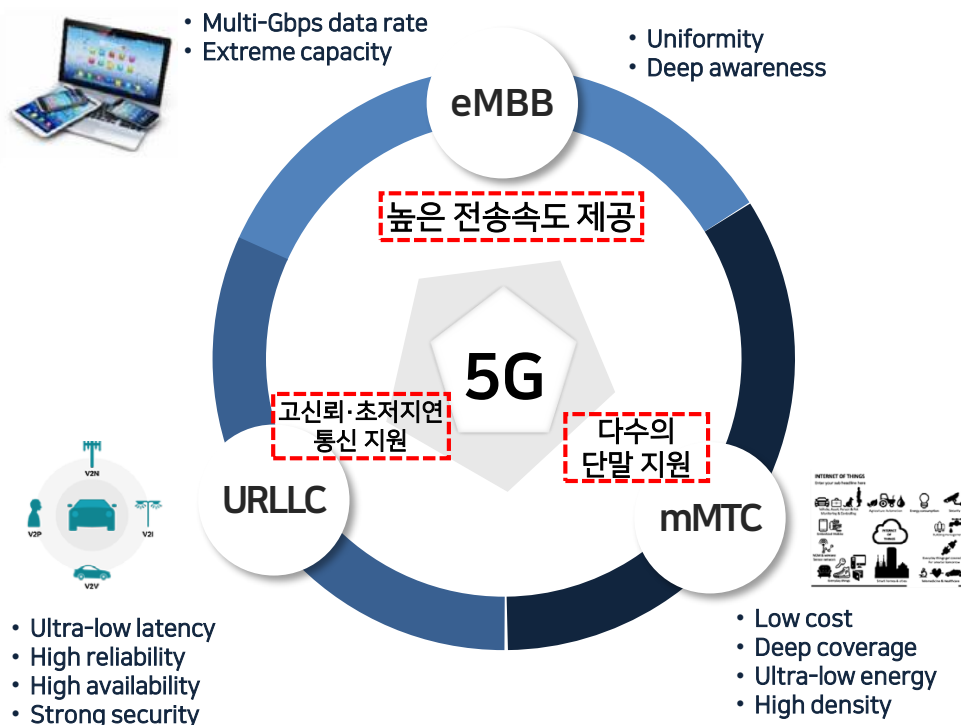
I

Part I: 5G+ 및 MEC 동향



5G는 기존 사람간 이동통신을 넘어 모든 사물을 연결하고 산업의 디지털 혁신을 촉발

• 4차 산업 혁명 핵심 서비스를 제공하기 위한 핵심 통신 인프라를 제공



핵심 성능		4G	5G	4G 대비
초고속	최대 전송속도	1Gbps	20Gbps	20배
초저지연	전송 지연	100분의1초	1,000분의1초	1/10
초연결	최대기기연결수	십만개/km ²	백만개/km ²	10배



[초고속] 실감미디어

360 입체 무선 홀로그램



[초저지연] 자율주행차

안전한 완전자율주행(level 4)



[초연결] 스마트공장

무선 기반 유연한 생산체계



초고속

초저지연

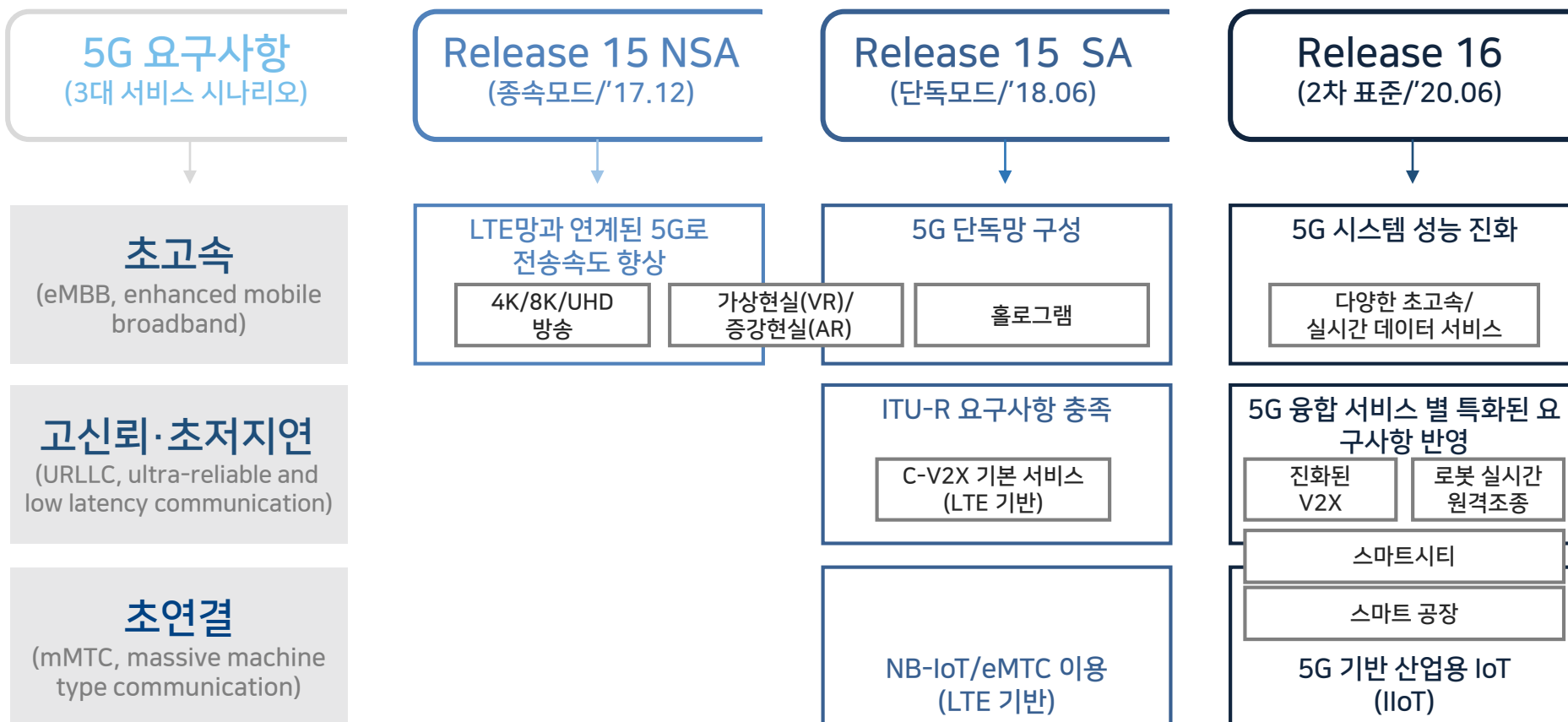
초연결성

출처: DNA플러스2019, 5G기반 디바이스 제조산업 실태조사 결과, NIA, 2019.12

출처: 혁신성장 실현을 위한 5G+ 전략, 대한민국 정부, 2019.04

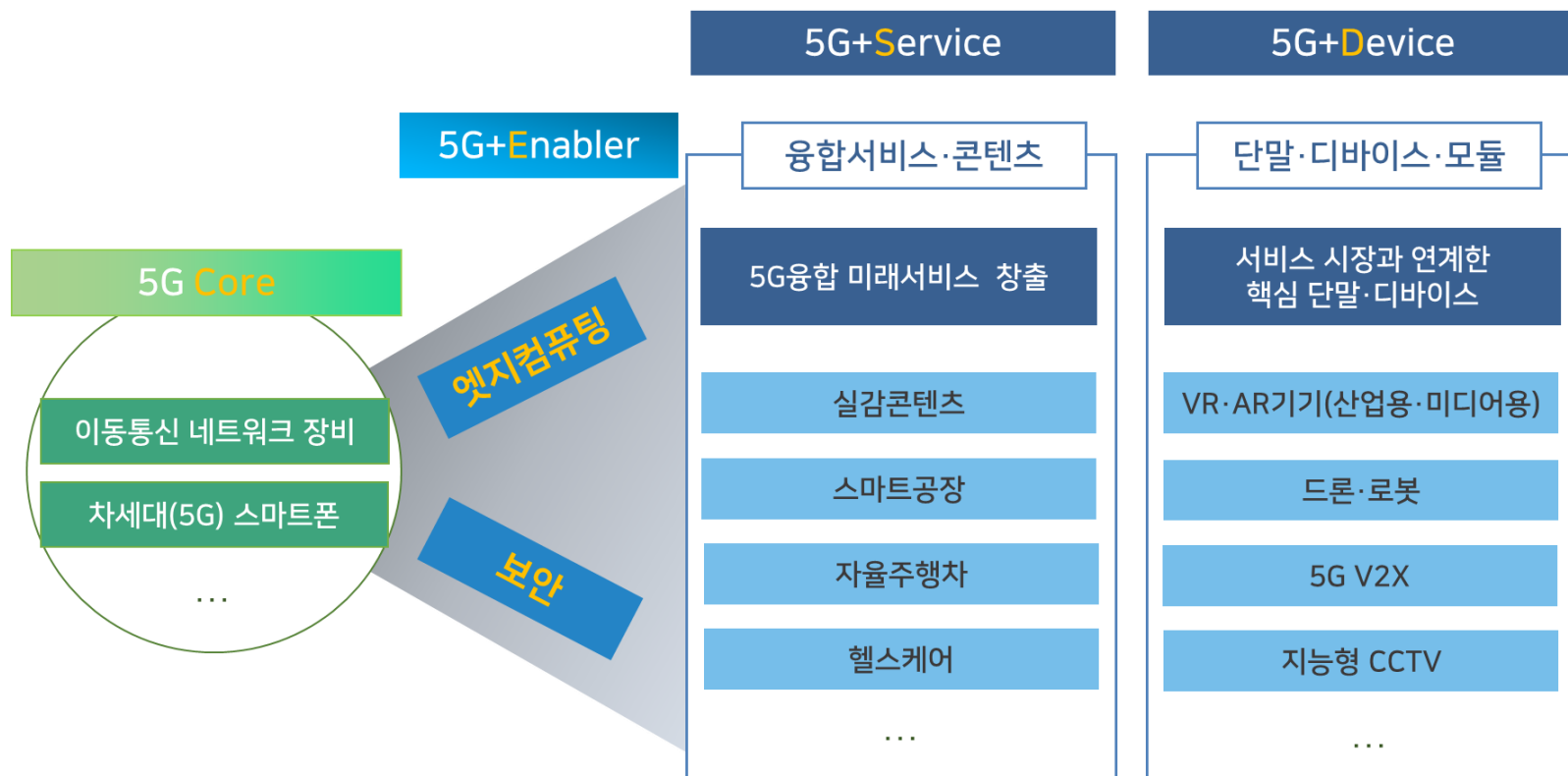
5G+는 경제·사회 전반에서 5G 기반의 디지털 전환과 지능화 혁신을 통한 산업·서비스 창출

- 5G+는 기술적으로 3GPP Release 16을 근간으로 다양한 융합 서비스 제공



5G+ 전략산업 후보군 도출 후 10대 핵심사업과 5대 핵심서비스 도출

- 정부는 '19. 4월 5G 기반의 새로운 산업과 서비스를 창출하기 위한 5G+ 전략 발표
 - ✓ 5G+ 제공을 위한 핵심 필요 기술(5G+Enabler)로 엣지컴퓨팅과 보안을 선정



'20년『한국판 뉴딜』종합계획의 10대 과제 중 지능형(AI) 정부 과제 선정

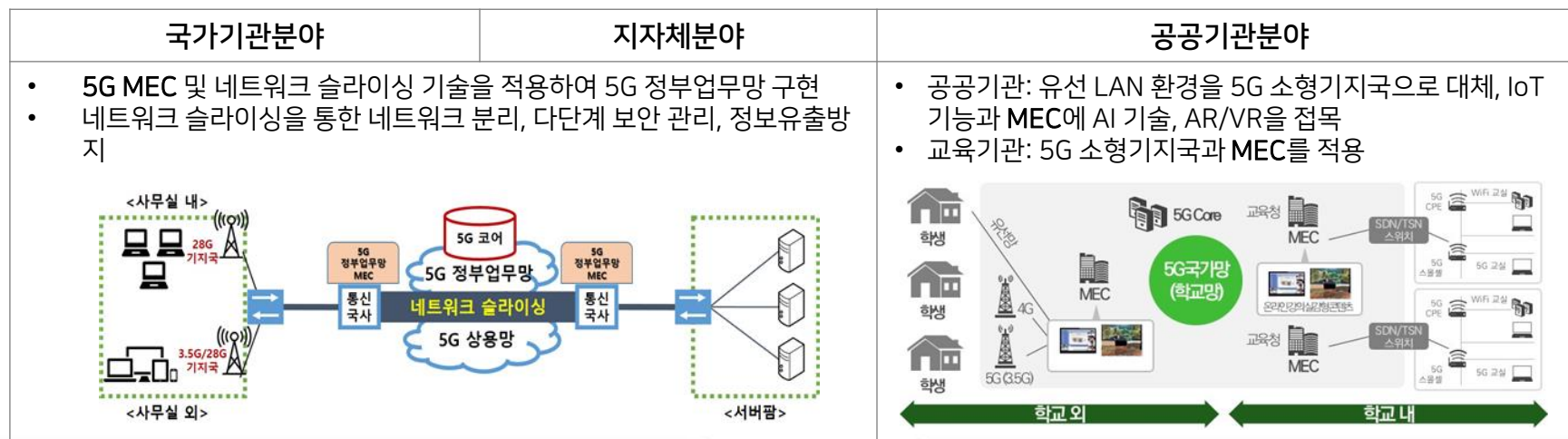
- 黨·政·民 협업을 통해 선정한 10대 대표 과제 중 지능형(AI) 정부 과제 채택 (총 9.7조 투입)

현재 상황	
"정부서비스에 신분증·종이 증명서 필요, 내·외부망 분리된 유선망 중심 업무환경"	
성과 지표	'20년
공공서비스 디지털전환	대면 업무 중심의 공공서비스
5G 국가망	유선망 중심 업무환경
행정·공공기관 클라우드 전환	17% (정보화 H/W 22.4만대 중 3.9만대)



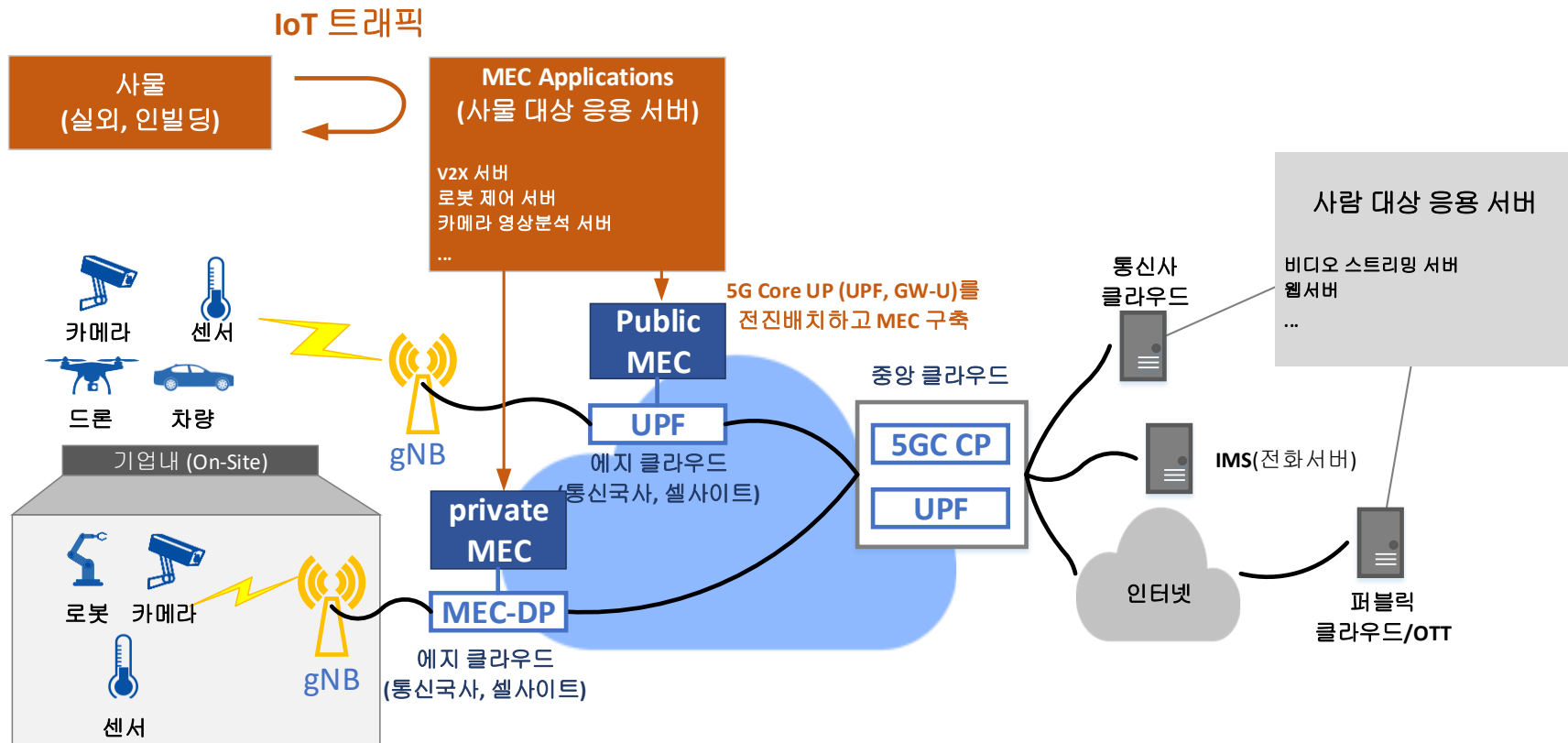
미래 모습	
"모바일 인증으로 Paperless 정부서비스, 언제·어디서든 Smart Office 구현"	
'22년	'25년
주요 공공서비스 중 50% 디지털 전환	80% 이상 디지털 전환
5G 기반 무선망 선도 도입	全 정부청사에 5G 기반 무선망 구축
50%	100%

- 한국정보화진흥원에서 '5G기반 정부업무망 레퍼런스 실증' 공모 (2년 195억원 투입)

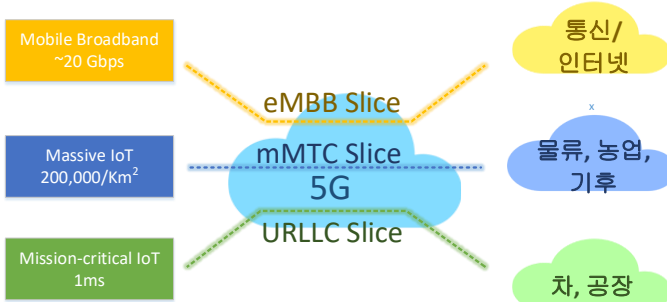
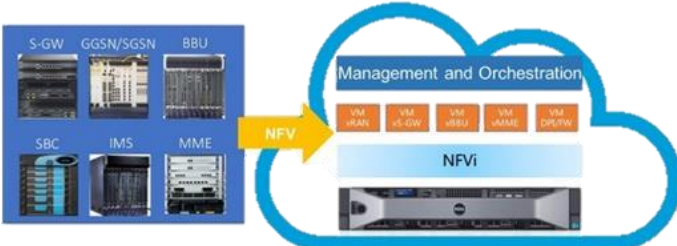


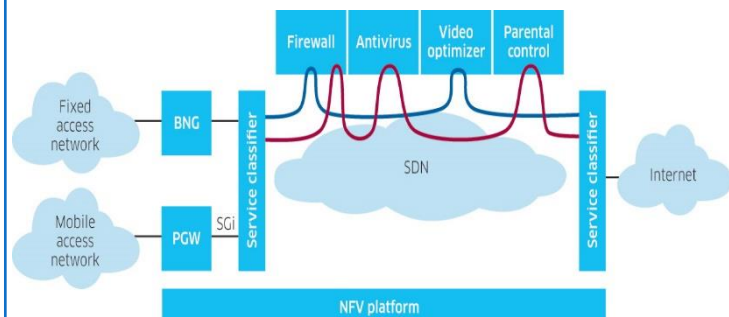
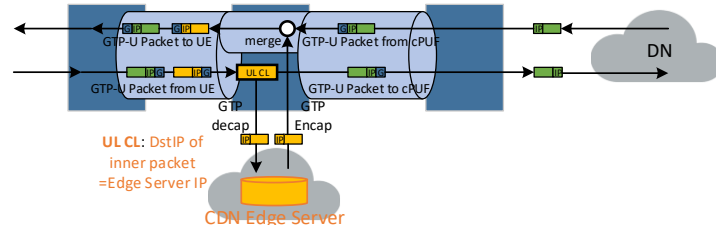
에지(서비스 응용/컴퓨팅 수행)를 단말 가까이에 배치하여 초저지연, 백홀망 트래픽 경감

- 네트워크 지연시간 단축 및 백홀 트래픽 부하 경감
- 특정 지역 또는 기업 맞춤형 특화 서비스 제공
- 용도에 따라 **Public MEC**와 **Private MEC**로 구분



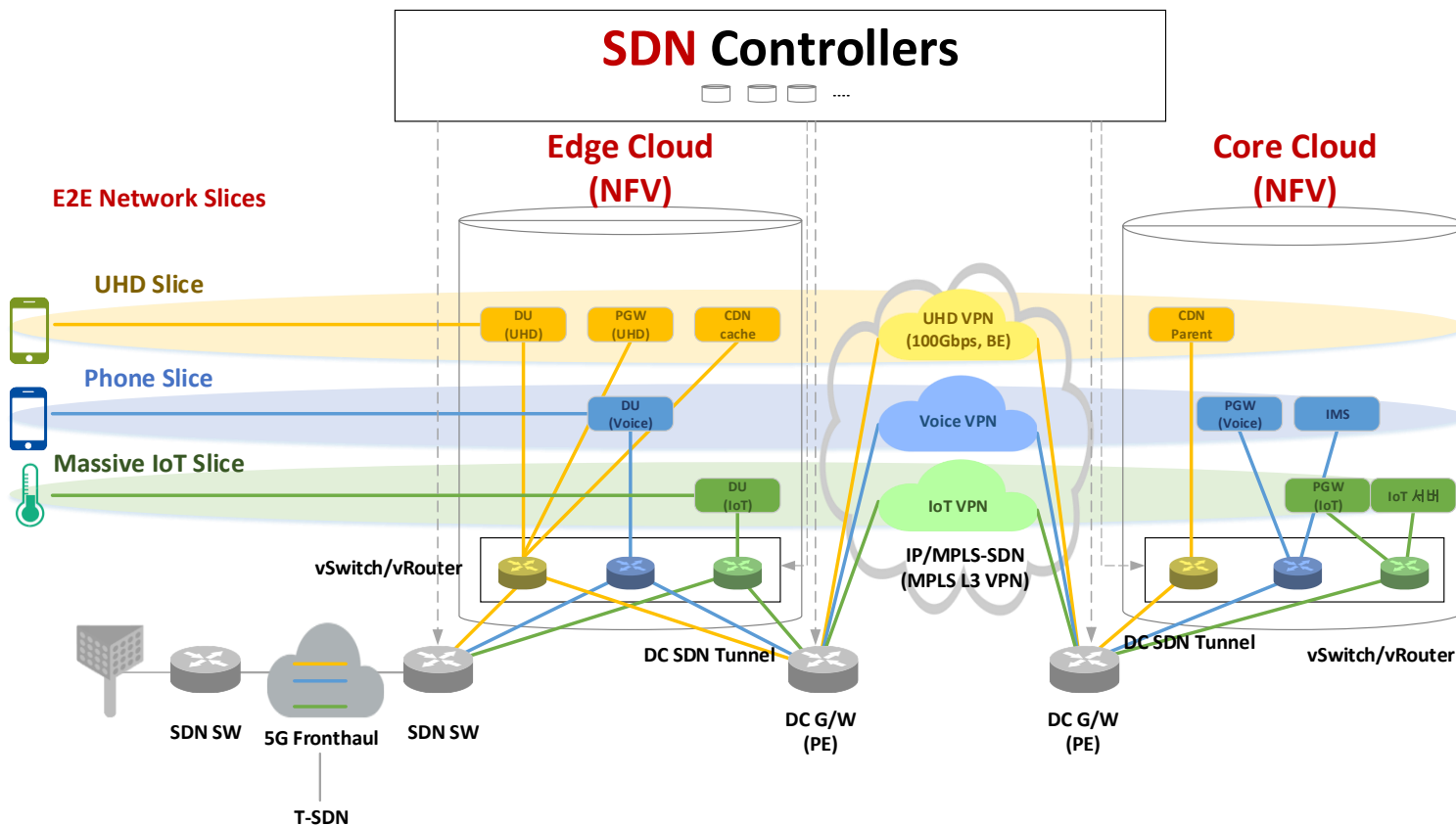
MEC를 제공하기 위해서는 Network Slicing, NFV, Service Chaining, Local Breakout 필요

구분	특징
Network Slicing	 <p>단일 네트워크를 다수의 가상 네트워크로 분할 (서비스 별 특성에 따른 자원을 할당)</p>
NFV	 <p>가상화된 네트워크 기능 S/W를 탑재 (서버 자원 효율성 향상으로 비용 감소)</p>

구분	특징
Service Chaining	 <p>트래픽이 경유할 VNF를 유연하게 조합함으로써, 네트워크 리소스 사용을 최적화</p>
Local Breakout	 <p>GTP 패킷 핸들링을 통해 패킷 전송 경로를 제어</p>

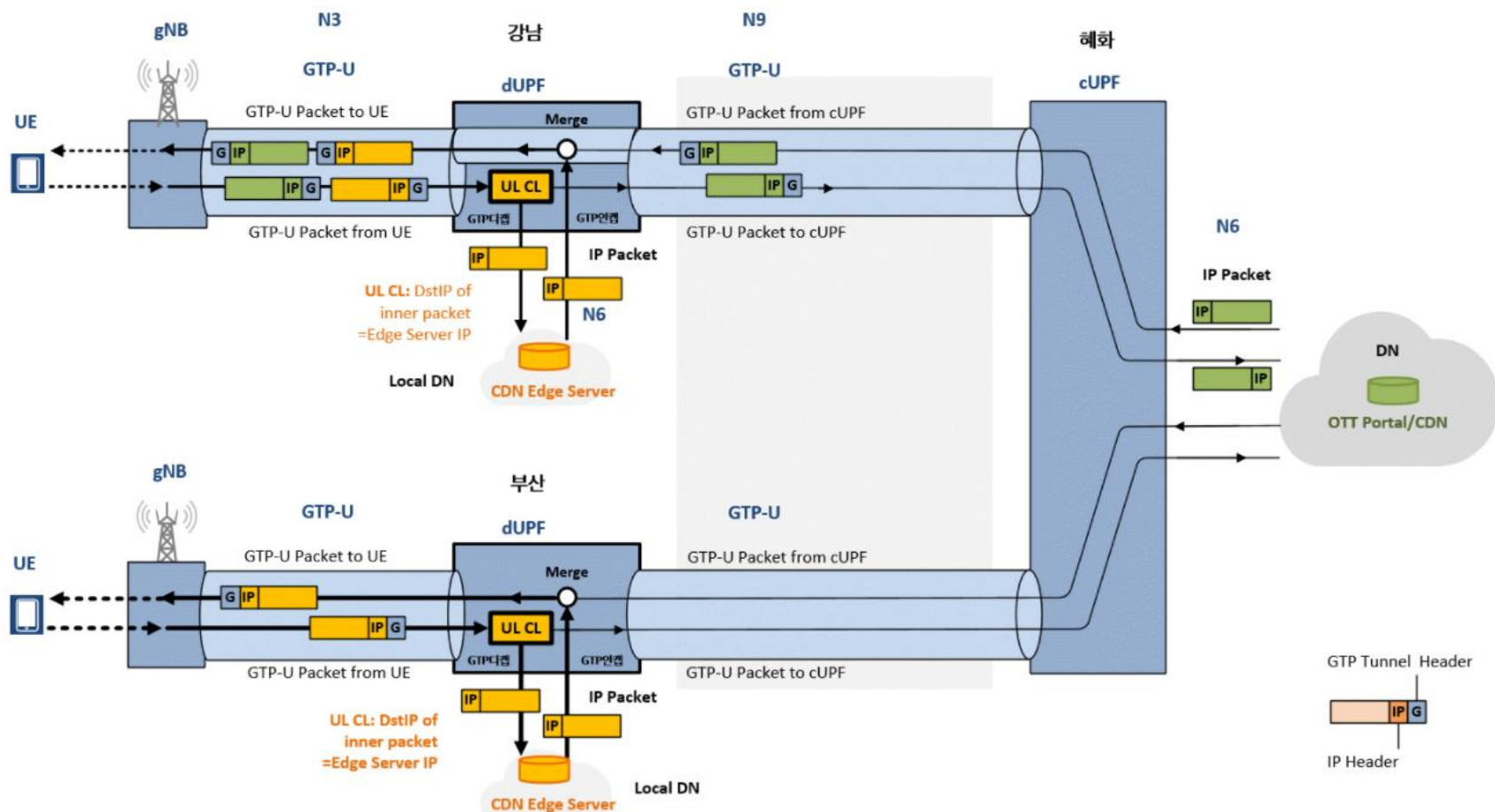
Network Slicing: NFV와 SDN 기술을 적용하여 서비스 별 요구 품질을 만족시키는 기술

- 품질 요구사항이 다른 서비스들을 단일망에서 융통성 있게 수용
- 서비스 별로 대역폭 할당, 경유 네트워크 기능을 할당할 수 있음



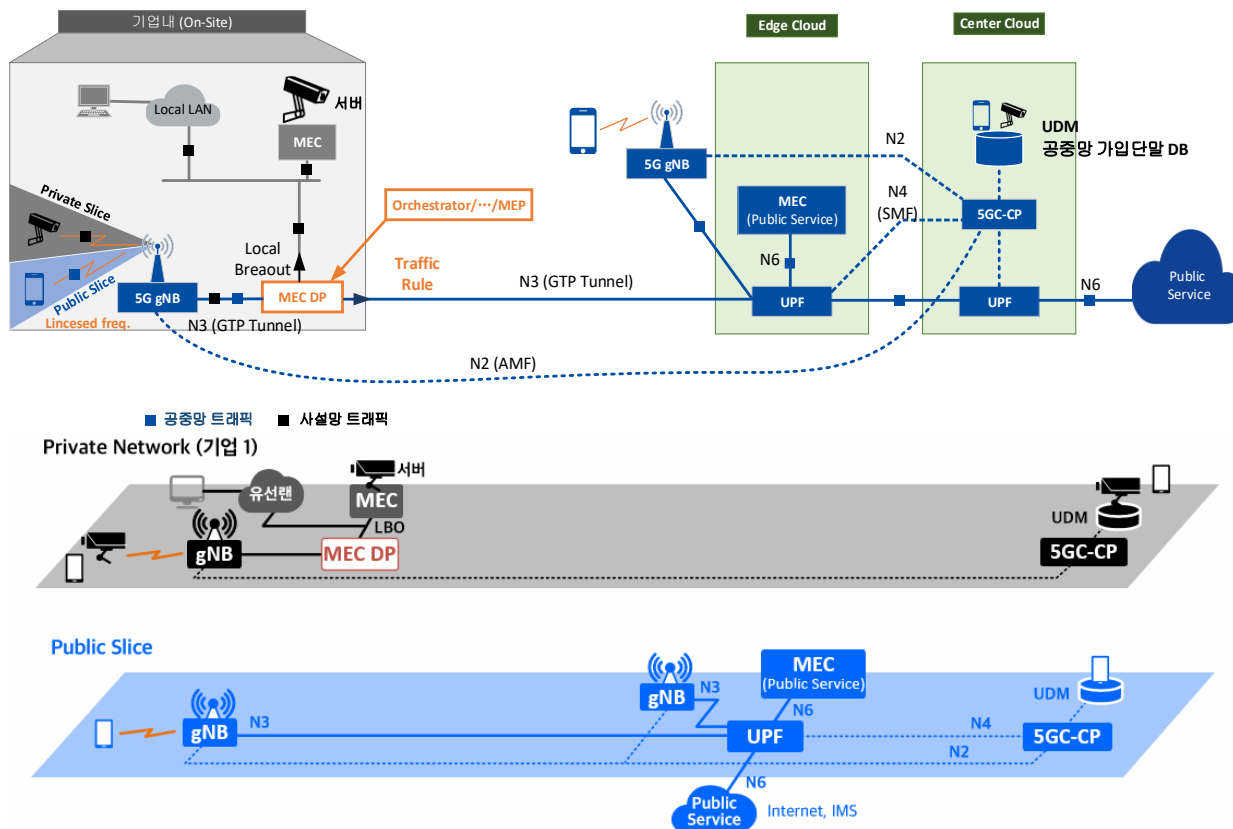
Local Breakout: 패킷 정보를 기반으로 패킷의 전송 경로를 제어

- UL CL(Uplink Classifier)을 이용하여 두 경로의 트래픽을 분리



네트워크 슬라이싱과 LBO를 활용한 MEC 방안

- 사설망 트래픽은 이통사망으로 전달되지 않음
- 비싼 UPF 대신 저가의 MEC-DP를 사용하여 구축 비용 절감



Public MEC는 클라우드 서비스 제공에 유리, Private MEC는 근거리 특화 서비스에 유리

특징	Public MEC	Private MEC
주요 응용 사례	스마트시티, 원격에서 클라우드 서비스 제공	스마트 공장, 원격의료
연결 가능한 단말	매우 많음 (불특정 다수의 사용자 수용)	비교적 적음 (자격이 있는 일부 사용자 수용)
성능	고속의 처리속도 필요	낮은 처리속도
장비 가격	높음	낮음
보안 이슈	Security for MEC (MEC 내의 보안 이슈가 중요)	MEC for Security (유통되는 트래픽에 대한 보안 기능 중요)
유사 형태	고가의 클라우드 서버	저가의 스위치 형태로 구성 가능

City
광역시·도
시·군·구

항만·군부대·병원
·학교·광장

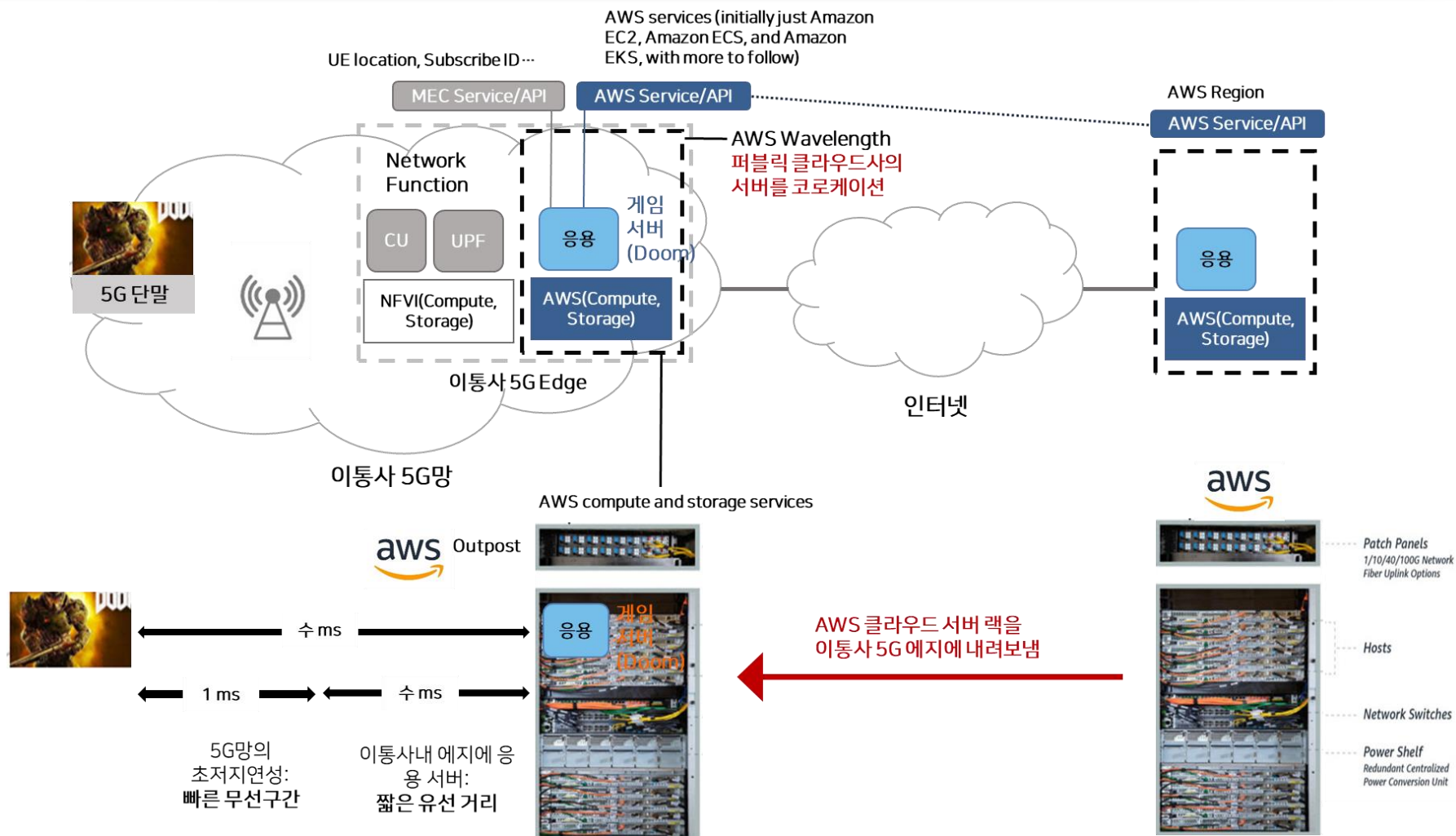
오피스·홈

**Public
MEC**

3.5GHz
기지국

**Private
MEC**

28GHz 기지국
/스몰셀

SKT-Amazon, SKT-MS, LGU⁺-Google 등 저지연 클라우드 서비스 제공

지능형 교통체계 및 V2I 형태의 자율 주행 서비스

- KT, 제주 C-ITS 광고



- KT, 현대모비스 5G 자율주행

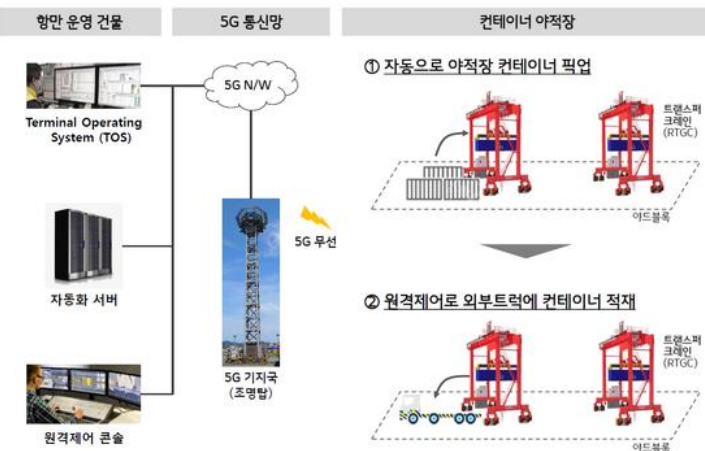


공장, 항만, 병원 등에서 5G MEC를 이용한 원격 제어

• LG U+, 부산항만공사



5G 항만 크레인 자동화 개념도



• SKT 스마트 팩토리



정부업무망에 대한 실증

- LG U+, 금오공대 정부 업무망 실증

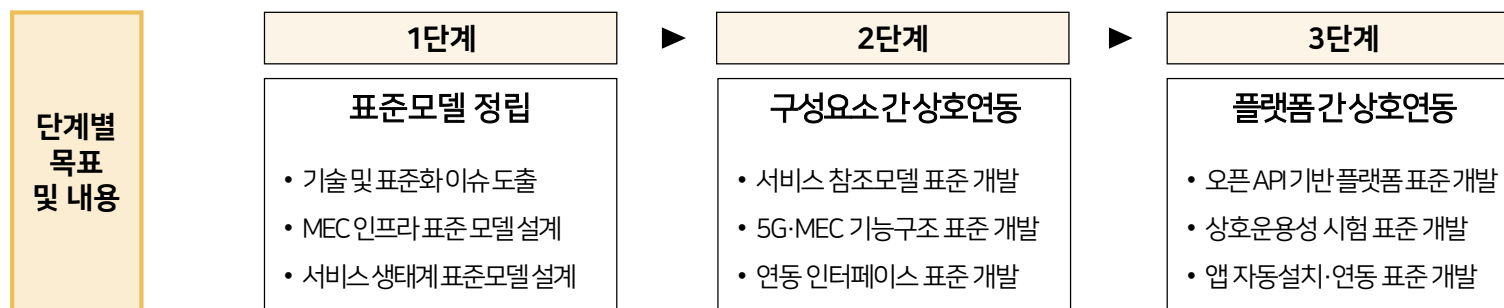


- 세종시 정부업무망 실증

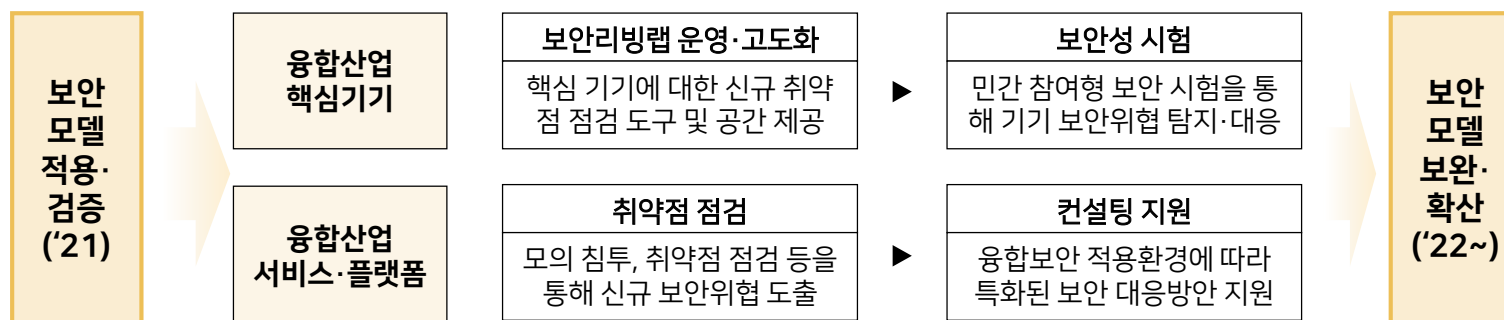


이통사 주도의 초기 시범적용·출현 단계

- 서비스 상호 연동을 위한 국제·국내 표준화 추진



- 오픈 API 기반 개방형 MEC 플랫폼 개발
- 주요 서비스 별 보안 위협 진단 및 참조 모델 개발



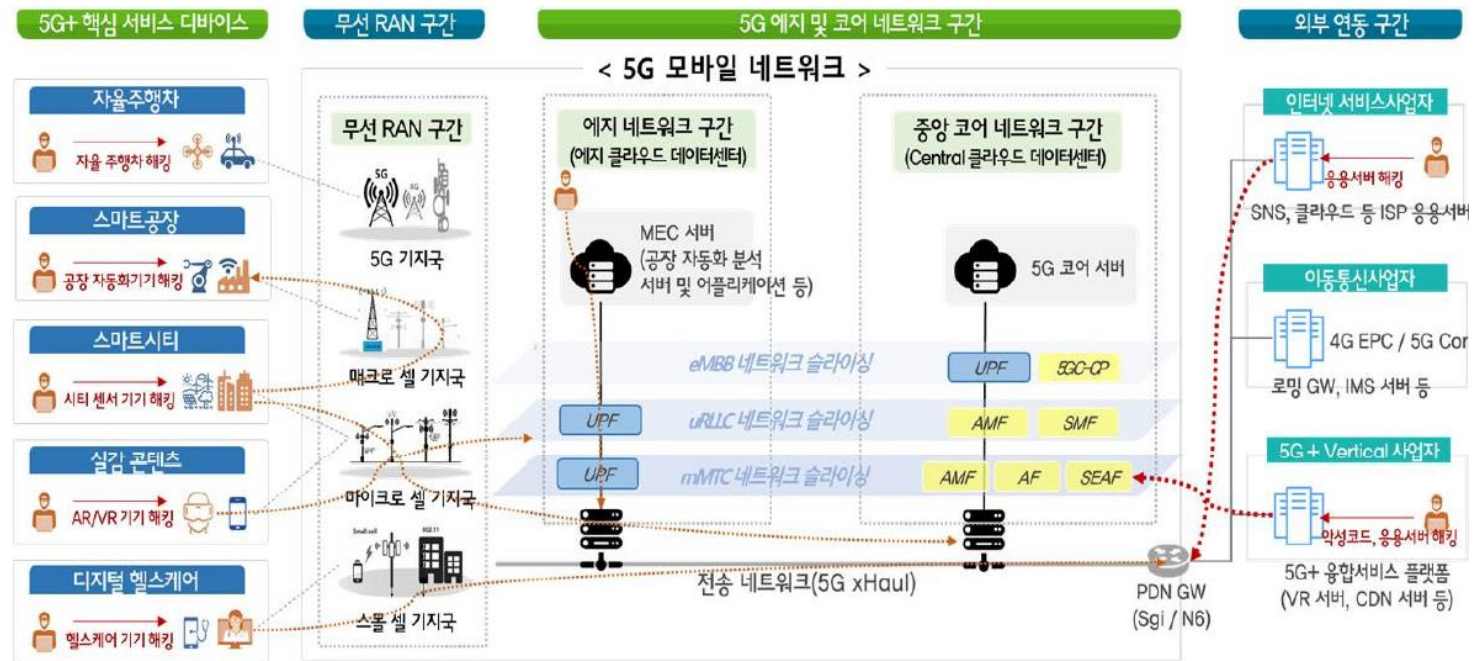
II

MEC 보안 전략



5G+에서 발생 가능한 보안 이슈

- 보안접점 증가 및 가상화/네트워크 슬라이싱으로 인한 5G 분산 코어망 보안 이슈 증가



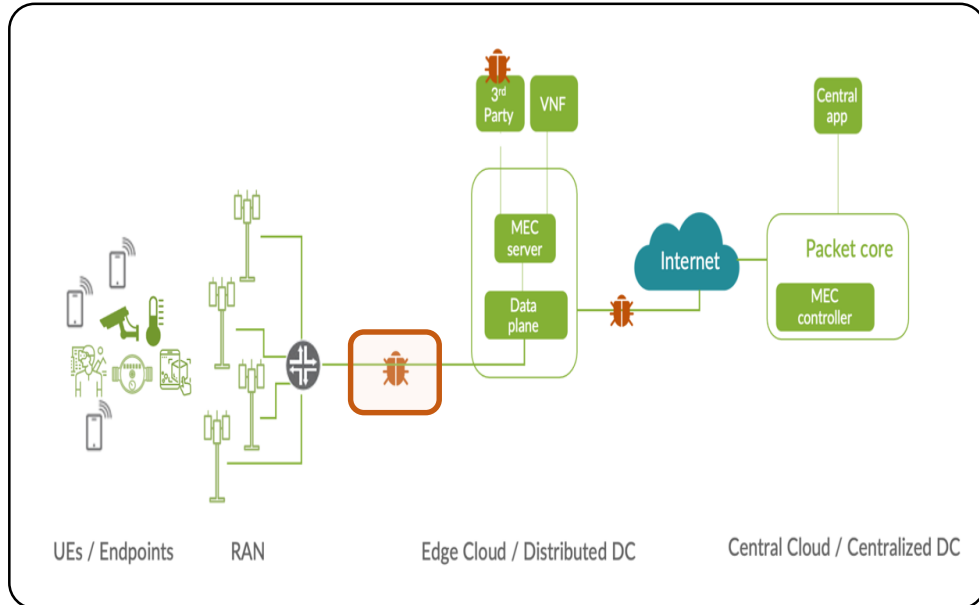
사용자 장치(UE)	무선 RAN 구간	5G 엣지 및 코어 네트워크 구간	외부 서비스 연동 구간
악성코드 감염 펌웨어 해킹 디바이스 탬퍼링 IoT 봇넷 감염	무선 자원 재밍 (Jamming) RAN DDoS 허위기지국(Rogue BS)	(플랫폼) SDN/NFV 플랫폼 취약점, MEC 서버 취약점 (API) 3rd Party 어플리케이션 API 및 부적절한 권한 접근 (서비스) DDoS 서비스 장애, 네트워크 슬라이싱 위협 (네트워크) 분산 네트워크 망 장애, 보안 관리·유지	응용서버 취약점 API 취약점 공격 로밍 취약점, 가입자 정보 가로채기

출처: 김한국, 최보민, 박성민, 심원태, "5G 네트워크 기술 진화에 따른 보안 이슈와 사이버대응 기술의 고려사항", 주간기술동향, 2019.10.09

5G 단말로부터 전달되는 보안 위협

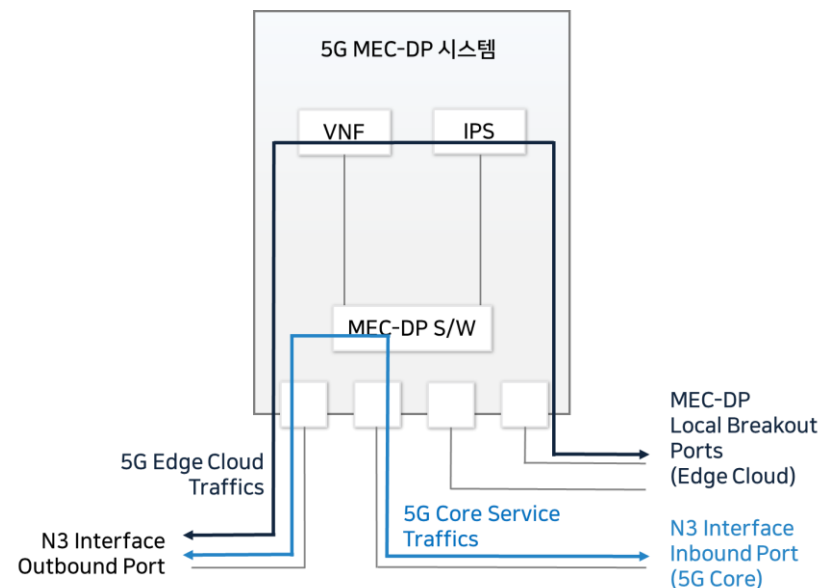
위협

- MEC 플랫폼 및 응용 서비스에 대한 대규모 접속 시 DDoS 유발
- 네트워크 슬라이싱 침해를 통한 무선 및 공유 자원 고갈
- MITM(Man In The Middle) 공격에 취약
 - 허위 기지국 발생 시 UE와 5G망 사이 중간자 공격 가능



대응

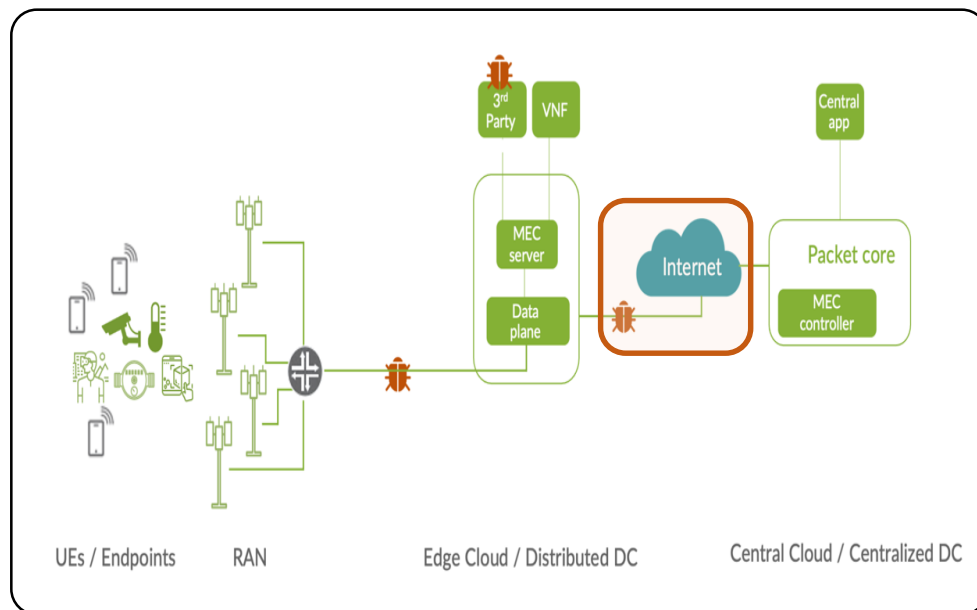
- 경량·저지연 네트워크 보안 장비를 통한 위협 탐지 및 차단
 - LBO, IPS 기능을 가진 80Gbps급 Secured MEC-DP



5G 코어망에 대한 보안 위협

위협

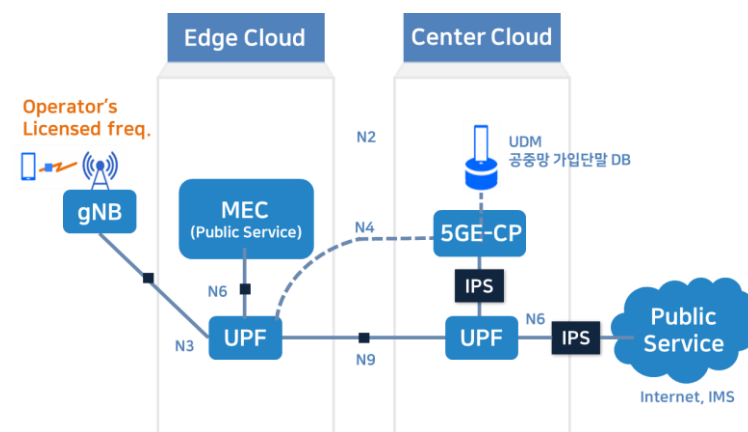
- 네트워크 가상화 및 서비스 기반 구조(SBA)에 따른 보안 위협
 - SDN/NFV 인프라 취약점 공격
 - 5GC 제어 기능에 대한 조작이나 감염
 - 공개 소프트웨어 취약점을 악용한 공격



출처: Juniper networks

대응

- 5G 코어망을 위한 고속 위협방지시스템 개발
 - 250Gbps 급 패킷 수집 및 위협 분석

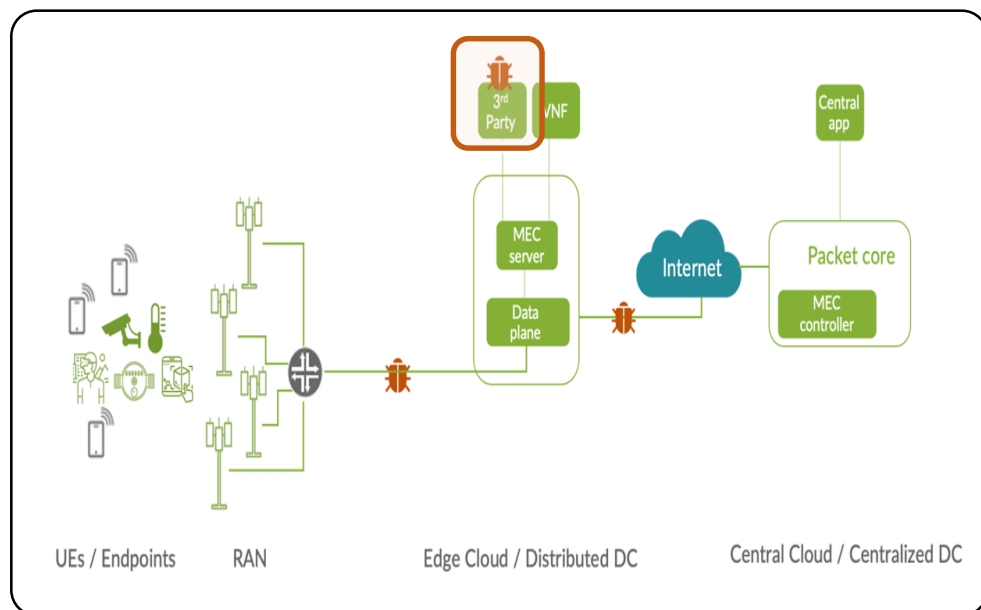


출처: netmanias

MEC 플랫폼 및 App 보안 위협

위협

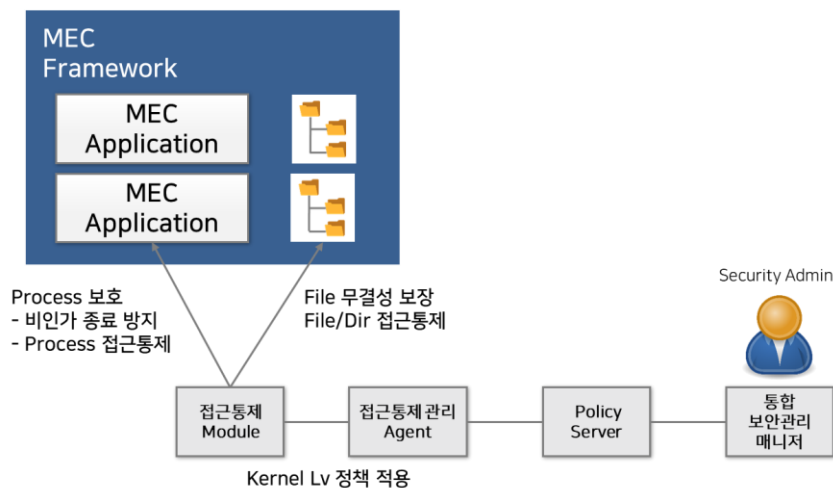
- 3rd Party App의 악성코드 감염 및 조작으로 인한 서비스 장애
 - MEC의 리소스를 비정상적으로 사용
 - 비정상적 내부 정보 접근



출처: Juniper networks

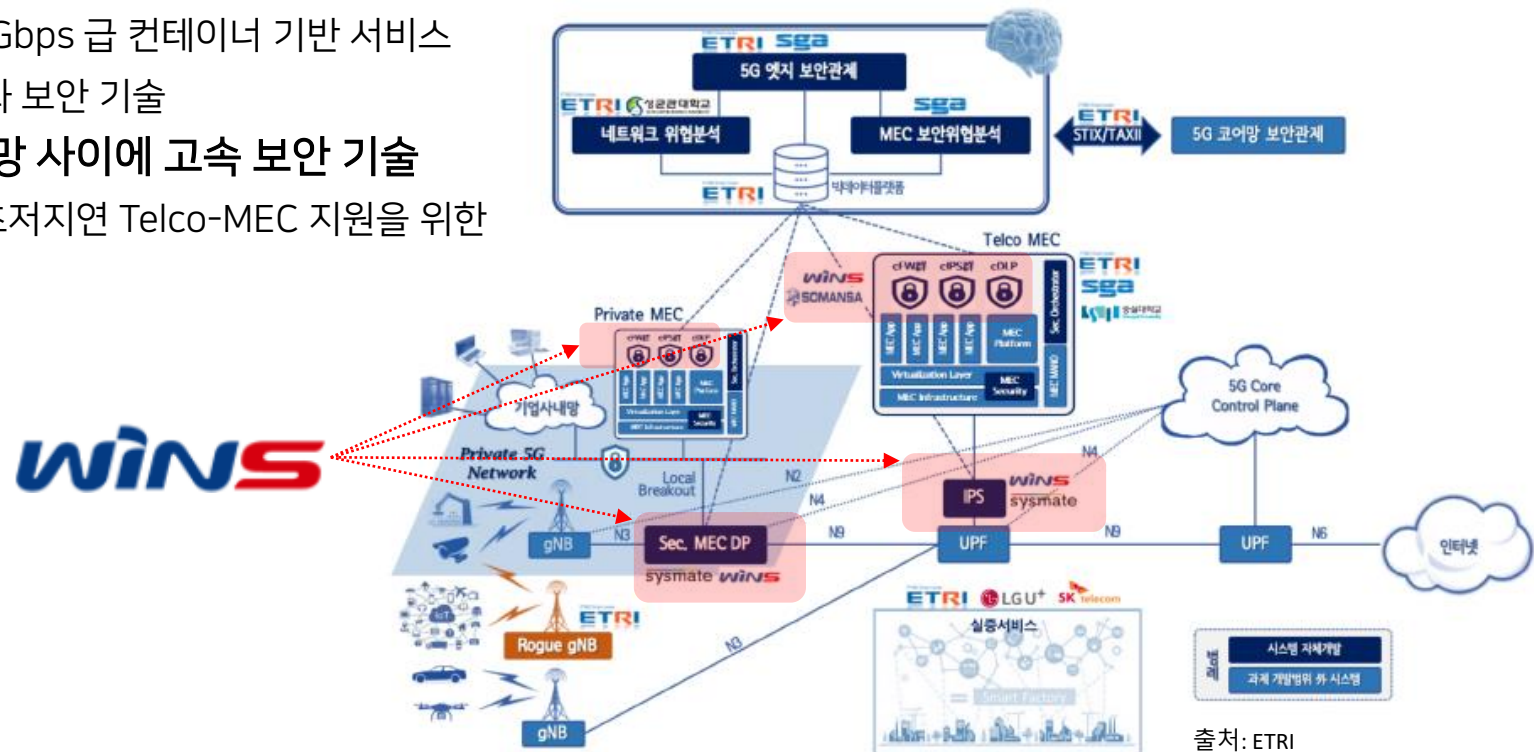
대응

- 가상화 플랫폼 보안위협 탐지 기술 개발
 - ETSI 표준 기반 MEC 플랫폼 구조 설계 및 구축
 - MEC 컨테이너 보호를 위한 하드웨어 샌드박싱 제어
 - MEC 플랫폼 비인가 접근 및 제어, 변조, 권한 조작 방지
 - 비인가 MEC 호스트 접근 탐지 및 통제



5G+ 서비스 안정성 보장을 위한 엣지 시큐리티 기술 개발

- MEC 구간의 가상화된 보안기술
 - MEC-DP 용 보안 엔진
 - Local Breakout을 지원하는 80GBps 급 가상 보안 기술
 - MEC 용 보안 엔진
 - 20Gbps 급 컨테이너 기반 서비스 특화 보안 기술
- MEC와 Edge망 사이에 고속 보안 기술
 - 초고속/ 초저지연 Telco-MEC 지원을 위한 보안 기술



출처: ETRI

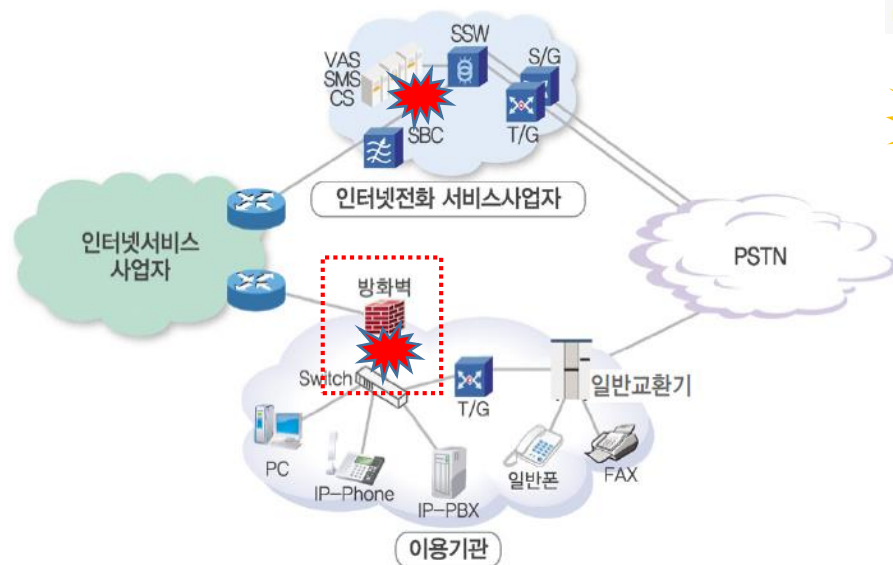
행정기관망 VoIP 도입

- 2008년 행정기관 인터넷전화 전면 도입 계획 발표

- 국민 통신비 20% 절감 목표
- vs. 해킹으로 인한 도청 우려

[Why] 모든 관공서에 인터넷전화... 260억 아끼려다 몽땅 도청 당할라

행정기관·지자체 일부 도입 - "민간용 회선과 별도로 운영... 보안 수준도 문제 없다"
 연말까지 100% 전환 계획
 해킹·도청 등 각종 사고 우려 - 기술적으로 안전하다 해도 인증서 분실·복사할 가능성
 정전되면 아예 사용 못 해
 일부 통신업계서도 반대 의견 - "인터넷, 언제든 '뚫릴' 위험"
 미리 전환한 일부 기관에선 팩스 폭주로 혼선 빚기도



도·감청 위협

인터넷망 위협

SIP/RTP 취약점

안전에 대한
신뢰도

VoIP망 전용 보안 솔루션

도입운영 가이드라인

기기 인증 기능

암호화 기능

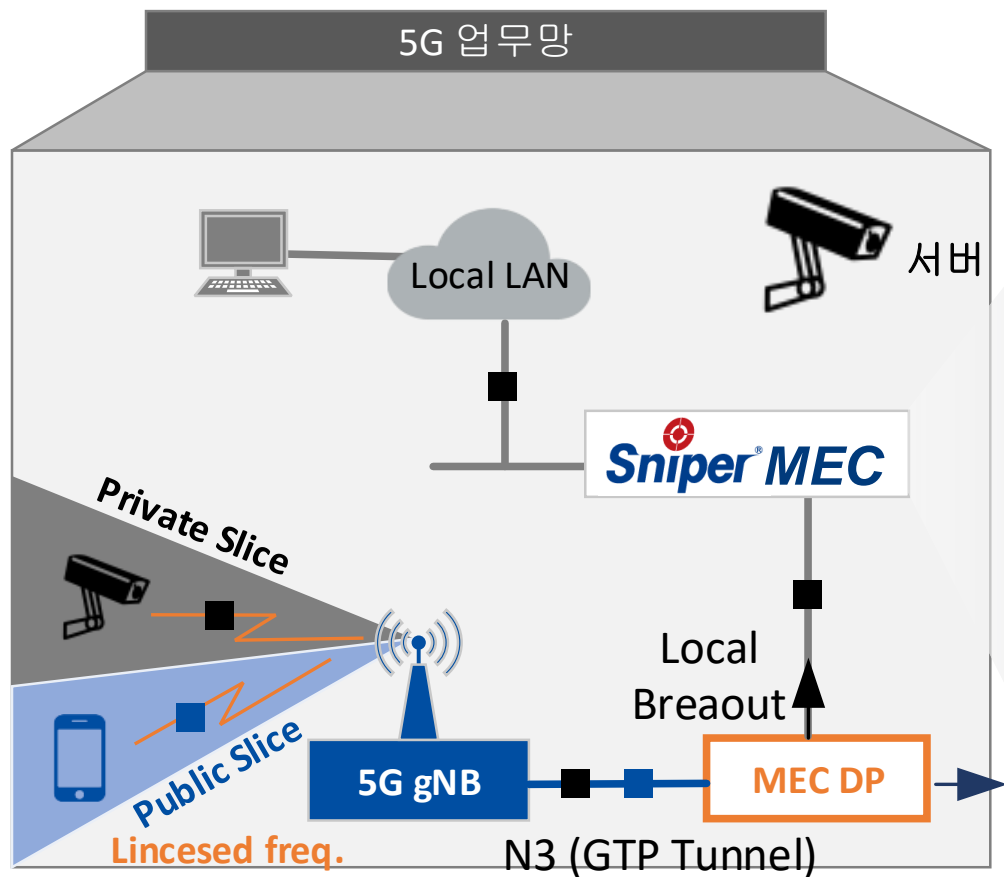
방화벽 기능

CC인증

경량화

출처: 행정기관 인터넷전화 도입운영 가이드라인, NIA

5G 업무망 보호를 위한 Sniper-MEC



DDoS
방어 기능침입차단
기능방화벽
기능사용자·서비스
권한 관리 기능기기/사용자
관리 기능

단말 인증 기능

망분리/망연계
기능

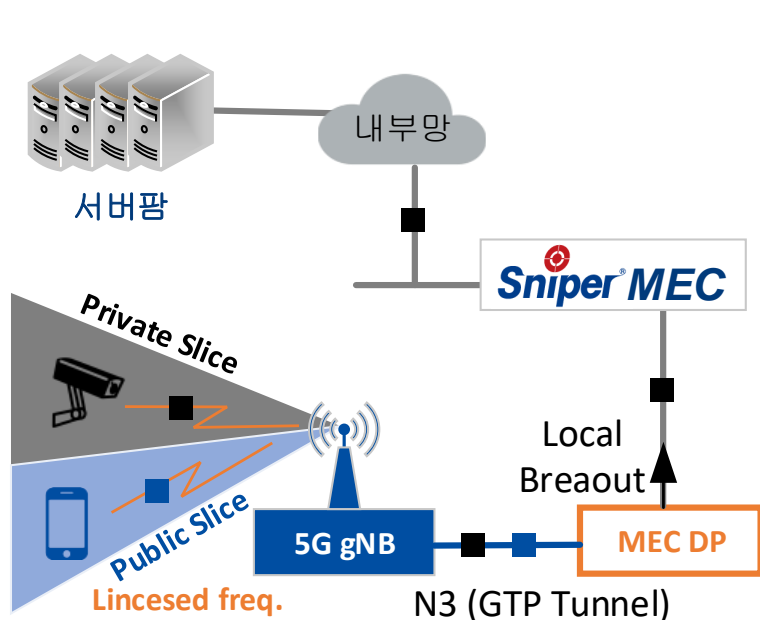
망접근 제어 기능

암호화(VPN) 기능

5G Private MEC를 위한 통합 보안 솔루션 개발

- 지능형(AI)정부를 위한 정부업무망
 - 유선 LAN 환경을 5G 소형 기지국으로 대체
 - 5G MEC 및 네트워크 슬라이싱 기술을 적용
 - 네트워크 슬라이싱을 통한 망분리, 정보유출 방지

[미래 뉴스] '원스 Sniper-MEC' MEC 보안 분야 최초 CC 인증 획득!



Private MEC 전용 보안 솔루션

도입운영 가이드라인

MEC 보안 기능

암호화 기능

사용자/기기 권한 관리

망접근제어

단일 벤더 장비/응용

CC인증

경량화

MEC 국제 표준 준수

- 5G+는 B2C를 넘어 B2B로 확장하기 위해 필수적인 인프라임
 - 정부는 5G+를 제공하기 위한 필수 기술(5G+ Enabler)은 MEC와 Security로 정의하고 있음
- 5G MEC에서 보안은 선택이 아닌 필수 요소임
 - Public MEC는 AWS와 같은 3rd party 장비 또는 망기능이 탑재되며, 외부망 연동 발생이 예상됨
 - Private MEC는 기존에 구축된 Enterprise 망과 이동통신망이 직접 연결됨
- 윈스는 5G MEC를 위한 통합 보안 솔루션을 개발 진행하고 있음
 - 윈스는 MEC 용 통합 보안 솔루션을 개발하기 위한 모든 솔루션을 보유하고 있음
 - Private MEC를 위한 One Box 형태의 통합 보안 기술 솔루션 개발



.....
감사합니다



Q & A

