과학기술정보통신부

I-KOREA 4.0
사람 중심의 4차산업혁명 실현

5G보안협의회 기술분과 보고서

# 5G 보안 기술개발 로드맵

2020. 12.

과학기술정보통신부

# 목 차

# Ⅰ 추진배경 및 현황 분석

## 1. 추진배경

□ **세계 최초 5G 상용화 및 단독모드(SA; Stand-alone) 5G 전환 임박**

○ ’19년 4월 3일, 국내 이동통신 3사의 **세계 최초 5G 상용화**

- 국내 5G 가입자의 수는 865만 8,222명으로서, ‘1,000만명’ 시대를 앞두고 있음 (’20.10.05. 기준)

○ ’21년부터 단독모드 5G 망으로의 전환이 예상됨에 따라, 네트워크 슬라이싱(Network Slicing) 기술을 활용한 **다양한 5G+ 융합서비스가 활성화**될 전망임

○ 5G 네트워크의 혁신과 초고속·초연결·초저지연의 5G+ 융합서비스를 통해 국가 경제성장을 뒷받침할 **4차 산업혁명과 디지털 뉴딜정책의 핵심 기반**이 될 것으로 예상됨

□ 성공적인 5G 생태계 활성화를 위한 **국가차원의 정교하고 체계화된 정보보안 전략 수립 시급**

○ 5G의 혁신*은 새롭게 폭증된 공격접점과 보다 진화된 보안위협을 수반할 것으로 예상되므로 보안성의 확보·보장없이는 5G 생태계의 성공적인 정착과 확산을 기대하기 어려움

* 20Gbps급의 초고속, 1km$^2$당 100만개 이상의 초연결, 1ms내의 초저지연 등을 보장

○ 5G 상용화 및 단독모드 전환 이후, 이동통신 기술 및 융합서비스의 점진적인 발전에 따른 고도화되는 보안위협에 효과적으로 대응할 수 있는 국가 차원의 체계화된 5G 보안 전략 수립이 필요함

○ 美·中 등 기술선진국과의 경쟁을 위해 우수기술을 보유한 벤처를 발굴·지원하고, 전문인력 양성 및 연구개발 활성화를 통한 **국내 5G 보안 기술·솔루션 고도화를 통한 글로벌 경쟁력 확보 필요**

## 2. 국내외 시장 및 기술 동향

□ 국내외 시장 동향

○ 5G 상용화 및 서비스 확산에 힘입어 5G 보안 시장은 지속적인 성장세를 보일 것으로 전망됨 (Mind Commerce, ’18.09)

- 전 세계 5G 보안 시장 규모는 2024년에 약 40억 달러, 2025년에 약 70억 달러로 연평균 50%의 성장률(CAGR)을 보일 것으로 전망함

※ 5G 보안 시장 중 약 95% 이상(’19년 기준 4억 27백만달러)이 보안솔루션 분야가 차지하고 있음

※ 보안서비스 분야는 상대적으로 높은 연평균 성장률(61.4%)로 인해 2025년에는 3억 77백만 달러를 차지할 것으로 전망

※ 5G 공격 탐지대응 분야는 2019년 1억 44백만달러로 연평균 53.7% 고성장할 것으로 전망하며, 전체 5G 보안시장 중 약 26% 비중을 차지

- 국내 5G 보안 시장은 2019년 143억원으로(세계시장의 약 2.27%)이며, 연평균 59% 고성장하여, 2025년에는 약 2,794억원 규모로 세계 시장의 약 3% 비중을 차지

○ 5G와 타 산업간 융합이 가속화됨에 따라 5G+ 5대 핵심서비스 분야에서 ‘26년 692조원의 글로벌 신규 시장이 창출될 것으로 전망됨 (KISDI, ’19.01)

- 에릭슨에 따르면, '20년부터 5G 기반 B2B 시장이 본격적으로 열리면서, '26년에는 전세계적으로 5G B2B 부문에서만 6,190억 달러 규모의 시장이 열릴 것으로 전망함 (서울경제신문, '20.02.)

□ 국내외 기술 동향

○ 3GPP의 5G 기술 표준화와 더불어 5G 보안에 대한 연구가 활발히 진행되고 있으나 아직 초기 단계임

- 국외에서는 5G 환경에서의 다양한 잠재적 보안위협 분석에 대한 연구가 진행되고 있으나, 대부분의 이동통신 보안 기술 연구는 아직 4G LTE의 보안 취약점 발견 및 검증 연구 비중이 높음

※ 유럽연합은 2019년 5G 네트워크의 고도화된 위협에 대응하고 회원국의 통일된 사이버 보안 방안을 마련하기 위해 ISO/IEC 27005(Information Security Risk Management) 위험관리 방법론에 기초하여 국가별 5G 네트워크 사이버보안 위험평가 보고서[1]를 발간한 바 있음

※ 미국 국토부 산하 사이버보안 및 기반시설 보안국(CISA)은 2019년 5G 도입에 따른 위험 검토 보고서[2]를 발간한 바 있으며, 공급망과 네트워크 등을 통한 보안 취약점 발생시의 보안 강화 방안을 제시함

※ A. Dutta[3]는 2017년 ETSI Security Day에서 5G 네트워크의 특징과 관련된 보안 이슈 분석 연구결과를 발표한 바 있음

※ S.R. Hussain, et.al.의 2018년 발표 논문[4]에 따르면, 4G LTE 환경에서 프로토콜 취약점을 이용한 13개의 기존 LTE 취약점을 재확인하고, 10개의 새로운 취약점을 도출하여 발표한 바 있음

※ T. Fei, et.al,의 2019년 발표 논문[5]에 따르면, 4G LTE 환경에서 브로드캐스팅 채널 등 암호화되지 않은 무선 채널을 이용한 주요 정보 탈취 등의 공격 실험 결과를 발표한 바 있음

※ 유럽네트워크정보보호원(ENISA)이 2018년 발간한 보고서[6]에 따르면, 4G

1) EU, Coordinated Risk Assessment of the Cyber-Security of 5G Networks, 2019.10.9.
2) CISA, Overview of Risks Introduced by 5G Adoption in the United States, 2019.07.31.
3) A. Dutta, "Security Challenges and Opportunities in SDN/NFV and 5G Network," ETSI Security Day, 2017
4) S.R. Hussain, et.al., "LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE," NDSS Symposium 2018, San Diego, CA, Feb. 2018
5) T. Fei and W. Wang, "LTE is Vulnerable: Implementing Identity Spoofing and Denial-of-Service Attacks in LTE Networks," IEEE GLOBECOM 2019, Waikoloa, HI, Dec. 2019
6) ENISA, "Signalling Security in Telecom SS7/Diameter/5G: EU level assessment of the current situation," Mar.

이동통신 환경에서 사업자의 망간 상호접속(interconnection) 프로토콜의 취약점을 이용한 보안 위협을 조사하여 발표한 바 있음

- 한국은 세계 최초 5G 상용화 이후, 5G 서비스가 확산되고 있으나, 5G 네트워크 보안 기술 개발은 초기 단계임

※ 세계 최초 5G 상용화('19.04.03.), 정부의『혁신성장을 위한 5G+ 전략』발표('19.04.08.), 5G 가입자 100만명 돌파('19.06.10.), 5G 이동통신 장비 점유율 1위 달성('19년 1사분기) 등

※ 정부는 2019년 8월, 『5G보안협의회』를 발족하고, 5G의 본격적인 도입과 확산에 따라 새롭게 대두되는 보안 이슈를 점검하고 주요 선진국의 5G 보안 정책, 5G 핵심 네트워크 보안위협 및 대응기술, 5G 보안 국제표준화 동향 등을 논의하고 있음

※ 한국정보보호학회 5G보안연구회는 5G 보안기술 이슈에 대한 워크샵 및 논문집 발간을 통해 국내 5G 보안 이슈의 공유 및 연구개발 협력을 노력하고 있음

※ 한국인터넷진흥원은 2019년부터 "지능형 5G 코어망 비정상 공격 탐지 및 대응 기술 개발" 과제를 수행하고 있음

※ 한국전자통신연구원은 2020년부터 "5G+ 서비스 안정성 보장을 위한 엣지 시큐리티 기술 개발" 과제를 수행하고 있음

2018. (available from https://www.enisa.europa.eu/publications/signalling-security-in-telecom-ss7-diameter -5g)

# Ⅱ 연구 추진 타당성

## 1. 기존 연구현황

□ 세계 최초 5G 상용화('19.04.03.) 및 5G+ 융합서비스 확산에 대응하는 **5G 인프라 보안 기술개발** 추진

○ DDoS, 구성 설정오류 및 프로토콜 취약점을 악용한 공격으로부터 **5G 코어망을 보호하기 위한 위협대응 기술개발**

* 지능형 5G 코어망 비정상 공격 탐지 및 대응 기술 개발(KISA, '19~'22)

- 5G 이동통신망(NSA/SA) 전용 트래픽 수집 기술 개발
- 기계학습 기반 지능형 5G망 비정상 트래픽 탐지·대응 기술 개발
- 5G 이동통신망(NSA/SA) 전용 보안 관제 및 모니터링 기술 개발
- 5G 이동통신망(NSA/SA) 보안 취약점 분석 연구 및 이동통신사 실증

○ 5G 네트워크 인프라가 가상화되고, 코어망 기능이 점차 엣지 영역에 분산 배치됨에 따른 **엣지 기반 위협대응 기술개발**

* 5G+ 서비스 안정성 보장을 위한 엣지 시큐리티 기술 개발(ETRI, '20~'23)

- 5G 엣지 네트워크 고성능 트래픽 분석 및 위협탐지 기술
- MEC 오케스트레이션 및 플랫폼 보안 기술
- 5G 엣지 기반 지능형 보안 위협 분석 및 보안 관제 기술
- 5G MEC 기반 B2B 핵심서비스 보안 실증

## 2. 연구 추진 필요성

### □ 5G 기술 현황

○ 초고속·초저지연·초연결의 국제전기통신연합 IMT-2020 비전 및 요구사항 충족을 위해 5G 네트워크의 **구조적 변화 불가피**

- 이동통신·무선랜(WiFi)·위성 등 다양한 접속기술을 통해 수많은 다양한 종류의 센서·기기가 연결되는 **접속 환경 다변화**
- SDN*/NFV**를 통한 본격적인 **네트워크 소프트웨어화**

* 소프트웨어 정의 네트워킹(Software-defined Networking; SDN): 네트워크 장비의 제어부분을 트래픽 전송부분과 분리하여 트래픽 전달을 개방형 인터페이스를 통해 제어하는 기술

** 네트워크 기능 가상화(Network Functions Virtualization; NFV): 전용 HW 기반 네트워크 장비의 HW와 SW를 분리하여 네트워크 기능을 범용의 HW 상에서 운용하는 기술

- MEC* 확산에 따른 **분산 네트워크 구조화**

* 멀티액세스 엣지 컴퓨팅(Multi-access Edge Computing): 데이터의 처리·저장 등의 컴퓨팅 서비스를 원격의 중앙 클라우드가 아닌 사용자와 물리적으로 가까운 네트워크 엣지에서 제공하는 기술

< 기존 이동통신(4G) 대비 5G 핵심성능 비교 : 국제전기통신연합(ITU) >

| 핵심성능 | | 4G | 5G | 4G 대비 |
|---|---|---|---|---|
| **초고속** | 최대 전송속도 | 1 Gbps | **20 Gpbs** | 20배 |
| **초저지연** | 전송지연 | 100분의 1초 | **1,000분의 1초** | 1/10 |
| **초연결** | 최대 기기 연결수 | 십만개/$km^2$ | **백만개/$km^2$** | 10배 |

○ 3GPP를 중심으로 5G 상용화를 위한 1차 표준화(Release 15)가 완료('19.3)되고, 5G 융합서비스를 지원하는 2차 표준화(Release 16) 의 완료(~'20.6) 이후, 3차 표준화(Release 17)에서도 지속적으로 진행될 전망임('~21.9)

○ 4G/5G 연계방식(NSA)의 5G 세계 최초 상용화('19.4) 이후, 5G 단독 방식(SA)의 네트워크 구축시('20~) **5G+ 융합서비스* 본격화** 기대

* 5G+ 융합서비스: 제조·미디어·자동차·의료 등 각 분야에서 5G 특성(초고속·초저지연·초연결 서비스별 특화 네트워크 제공 등)을 활용하여 새로운 가치를 구현하는 서비스로서, 실감콘텐츠·스마트공장·자율주행차·스마트시티·디지털 헬스케어 등이 있음

## □ 5G 보안 이슈

○ 4G의 보안위협* 뿐만 아니라, 5G의 **구조적 환경 변화**에 따른 새로운 잠재적 위협 존재

* 무선 재밍, 가입자 신원정보(IMSI) 탈취, 허위기지국을 이용한 중간자 공격, 상호접속 프로토콜(Diameter) 취약점을 활용한 공격, 은닉채널을 통한 정보유출 등

- **(코어망)** 네트워크 가상화에 따른 SDN/NFV 인프라 취약점 공격, 제어 평면의 서비스 기반 구조* 인터페이스 공격 등 새로운 위협 존재

* 서비스 기반 구조(Service-based Architecture): 5G 네트워크 기능을 작은 서비스 단위로 세분화하고 세분화된 네트워크 기능간에는 HTTP 인터페이스를 통해 연동함으로써 구조의 유연성과 확장성을 강화하기 위해 도입된 개념

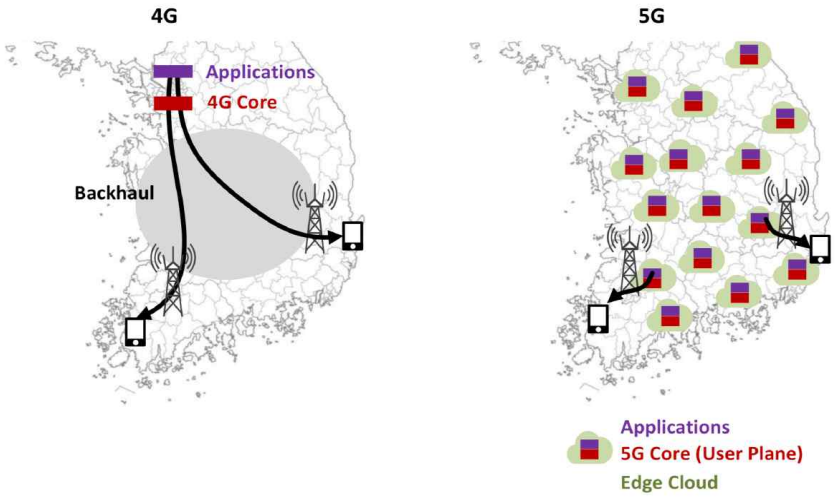
- **(액세스망 및 엣지)** 액세스망에서의 서비스거부 공격, MEC를 통한 감염·정보유출, 네트워크 슬라이싱* 침해공격 등 새로운 공격 발생 가능

* 네트워크 슬라이싱(Network Slicing): 하나의 물리적 네트워크를 가상화를 통해 **논리적으로 서로 독립된 종단간(end-to-end) 네트워크를 제공**하는 기술로서, 서로 다른 서비스 품질 특성을 요구하는 다양한 5G 융합서비스를 위한 핵심기술


- **(단말)** 다양한 종류의 대규모 센서·기기의 접속에 따라 디바이스 펌웨어나 SW가 악의적으로 변경되거나 보안 기능이 탑재되지 않는 등 단말의 취약점을 이용한 공격* 발생 가능성 증가

* 시만텍의 사이버 보안 전망(2019)에 따르면, 5G가 확산됨에 따라 IoT 디바이스 공격이 증가할 것으로 전망함

- **(네트워크 구조)** 5G 네트워크의 가상화·분산화에 따른 공격 접점의 증가로 인해 실시간 통합 보안관제 및 대응 한계 직면




○ **5G+ 융합서비스 활성화를 저해**하는 보안위협 우려 해소 필요

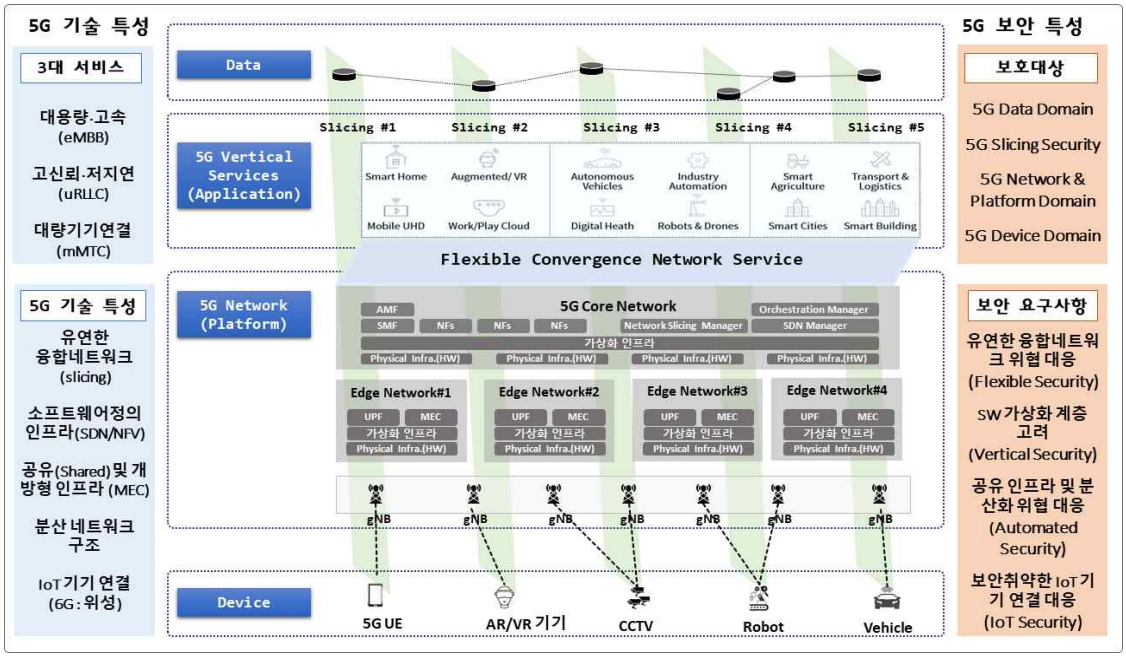
- **(서비스)** 5G+ 융합서비스별 ICT 적용수준, 보안 적용환경 및 기능 요구사항의 차이로 인해 5G+ 융합서비스에 대한 보안 기술* 적용 어려움

* 실감콘텐츠·스마트공장·자율주행차·스마트시티·디지털 헬스케어 등 5G+ 융합서비스별 보안모델 부재

# Ⅲ 주요 연구주제 내용

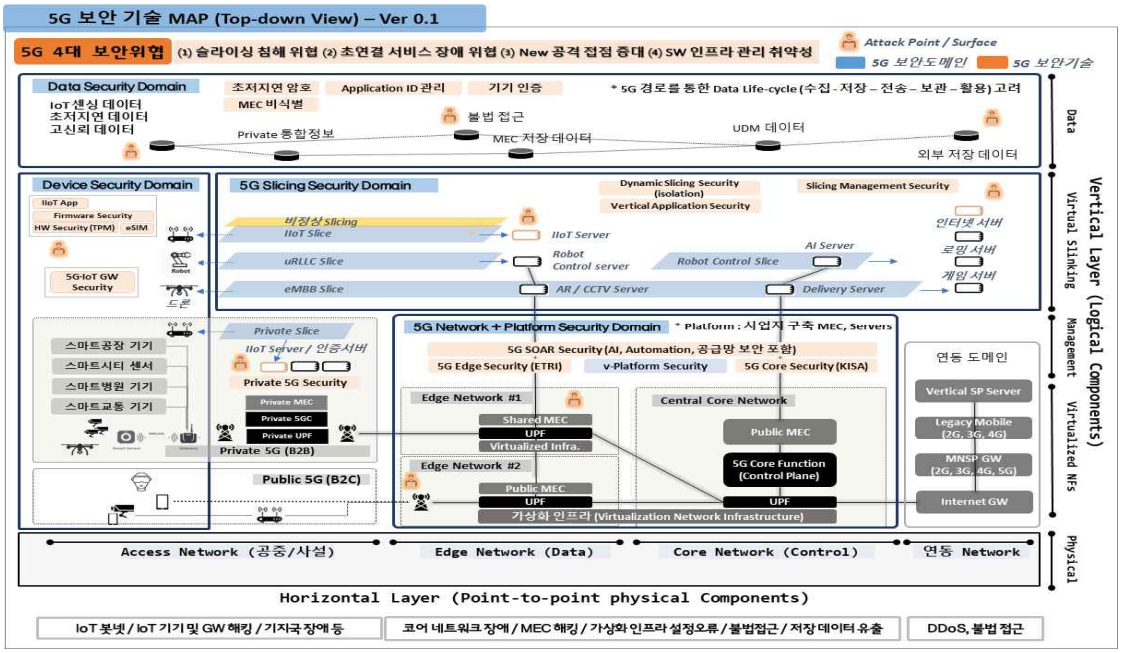
## 1. 주요 연구주제

○ 5G 성능목표와 기술특성에 따라, 보호대상 및 보안요구사항을 분석하여 4개 영역으로 분류(Device-Network(Platform)-Service-Data)




○ (기술 Map) 5G 구성요소, 보안위협(Attack Surface), 보안기술 구성

- 5G 특화 4대 보안위협에 대응하기 위해, 각 영역별 보안기술 도출



□ 5G 네트워크 슬라이싱 침해 위협 대응 기술

○ 5G 네트워크 슬라이싱을 통해 동일한 하드웨어 인프라에서 서비스별로 논리적으로 네트워크를 격리하면서, 인프라 자원고갈 공격, 비인가 슬라이스에 대한 데이터 도청/변조 등의 보안 위협 증대

- 네트워크 슬라이스 배포, 설정, 운영 등 네트워크 라이프사이클 라이프사이클 전주기에 대한 보안 침해 위협 대응 기술 개발

□ 5G 초연결 서비스 장애 위협 대응 기술

○ 이기종 망·기기·서비스가 상호 연결성이 강화됨에 따라, 단일지점의 해킹과 DDoS 확산 대비 **초연결 5G망 장애를 방지·억제기술 필요**

- 유연(Scalable), 자동화(Automated), 분산(Distributed) 개념의 5G 네트워크 및 서비스 장애위협 대응기술 개발

  * 단일 지점 공격 방어 기술에서 연결망 확산 방지, 격리 및 억제 중심 기술 개발로 전환

□ 공격접점 증대로 인한 위협 대응 기술

○ WiFi 및 대규모 IoT 연결 등 **접속환경의 다변화**, SDN/NFV 기술을 통한 **네트워크 소프트웨어화**, 가상화·MEC 확산에 따른 **분산 네트워크 구조화** 등에 따른 **공격 접점(Attack Surface)이 급증**

- 5G 단말 및 네트워크 보안 기술 개발을 통해 접속환경 다변화에 따른 보안 위협에 대응하고,

- 5G 네트워크 및 서비스 플랫폼 보안 기술 개발을 통해 네트워크 소프트웨어화 및 분산 네트워크 구조화에 따른 보안 위협에 대응 필요

□ 소프트웨어 인프라의 복잡성 대응을 위한 5G 자동 보안관리 및 관제기술

○ 네트워크 기반 기술의 소프트웨어화 및 가상화, 관리 대상/영역의 다변화, 네트워크 참여자 증가에 따른 **관리 복잡성 급증**

- SDN/NFV 등 SW 네트워크 기반 기술에 내재된 보안위협을 해소하고,
- 5G 네트워크의 관리 복잡도 증가 대응을 위한 보안 관리기술 및 관제 기술의 자동화 필요

## 2. 세부 연구내용

### (연구주제1) 5G 네트워크 슬라이싱 침해 위협 대응 기술

□ 필요성

○ 다양한 5G 서비스가 물리적 자원을 공유하는 논리적인 네트워크 환경에서 제공됨에 따라, 불완전한 네트워크 격리 취약성에 의한 데이터 유출/변조, 공유 인프라 자원 고갈 공격에 따른 서비스 지연 및 장애 등의 새로운 보안 위협이 발생함

- 네트워크 슬라이싱 기술은 5G 융합서비스 핵심 기술로, 서비스의 성능/보안 요구사항 만족을 위해서는 네트워크 슬라이싱 침해 위협 대응이 필수적.

**위협 시나리오**

○ 물리적 네트워크 자원을 공유하면서 사실상 서비스별 맞춤형 가상 전용망 제공이 가능한 5G 네트워크 슬라이싱 기술을 기반으로 스마트의료, 스마트교통, 스마트팩토리 등의 서로 다른 종류의 서비스를 제공하며 5G 망운용 효율을 높이고 있다.

○ 하지만 다수의 네트워크 슬라이스가 동일한 장비의 물리적 자원을 공유하고, 서로 공존하는 상황에서 네트워크 슬라이스와 물리적 자원 공유 관리 즉, 가상화의 보안취약점으로 인해 서로 엄격히 격리되고 보호되어야 하는 슬라이스 간 무단 접근 및 서비스 장애가 발생할 수 있다.

○ 특히 스마트홈서비스, 스마트의료, 스마트팩토리 등의 서비스가 공존하는 상황에서 각 서비스를 위한 슬라이스 간 접근제어 기능이 부재하거나 미비한 점을 이용하여 상대적으로 보안이 취약한 스마트홈 서비스를 통해 스마트의료나 스마트팩토리용 슬라이스를 접근하여 개인적인 의료정보의 무단 유출이나 스마트공장 도메인의 무단 침입을 통해 스마트공장을 불법제어하는 사고가 발생할 수 있다.

○ 또한 슬라이스를 위한 자원 관리 기능(가상화)을 해킹하여 슬라이스를 위한 자원 할당을 방해함으로써 슬라이스 기반 서비스 지연 혹은 서비스 불가능 상황을 초래할 수 있으며 공유된 자원에 접근하여 타 서비스 데이터의 불법유출, 위변조 등의 심각한 피해를 유발한다.

- 가상머신 해킹으로 허용된 네트워크 슬라이스 범위를 벗어난 네트워크 자원 접

**위협 시나리오**

근으로 네트워크 슬라이스용 자원 할당 장애 유발 및 비인가 네트워크 슬라이스 데이터 불법 접근 등의 위협 발생

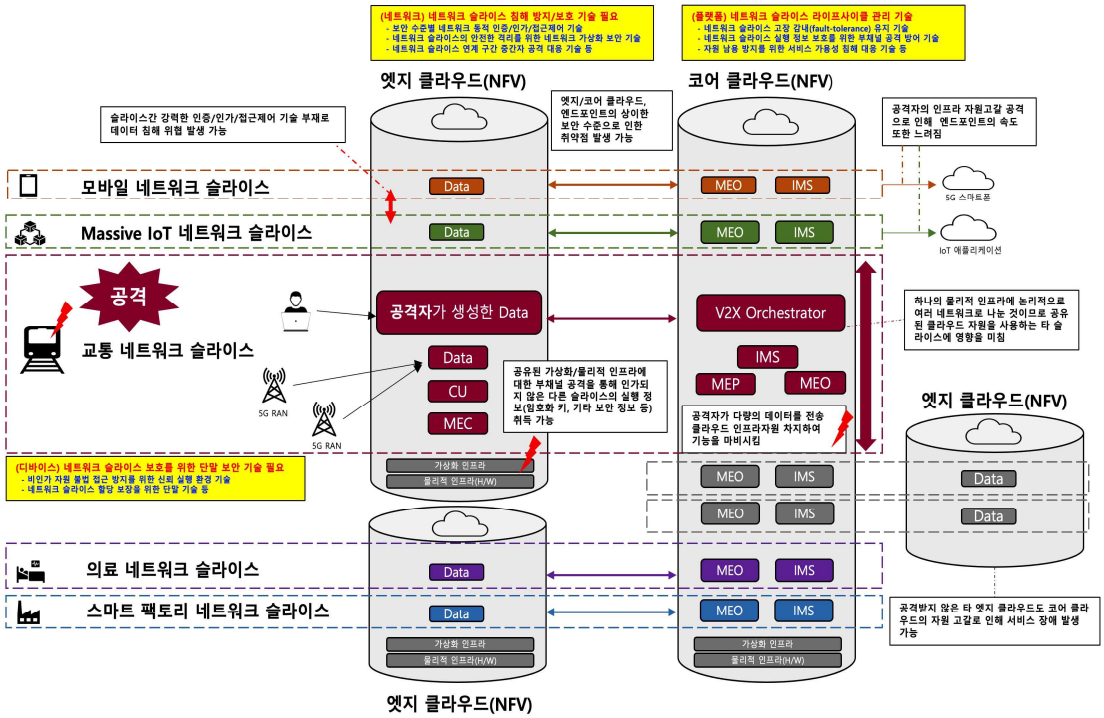
* 네트워크 슬라이싱 보안 위협이 가능한 가상머신 해킹 사례 발표 (Pwn2Own 2017)

- 네트워크 슬라이스 간 불완전한 격리로 타 네트워크 슬라이스 기반 서비스 데이터 불법 접근 및 인가되지 않은 서비스 도메인으로의 불법 침입 등의 위협 발생

## □ 기술 정의 및 연구 목표

### ○ 5G 네트워크 슬라이싱 라이프사이클 전주기 보안 위협 대응 기술

- (목표) 5G 융합서비스별 성능/보안 요구사항 충족 및 서비스 슬라이스별 차등화된 보안 정책, 보안 기술 적용을 위한 네트워크 슬라이싱 전주기(배포, 설치, 운영, 폐기 등) 보안 기술 및 침입 탐지/대응 기술 개발




* MEO(Mobile Edge Orchestrator) 모바일 엣지의 데이터를 통합하는 기능
* IMS : IP 기반의 멀티미디어 서비스를 위한 유무선 통신 플랫폼 환경
* MEC(Mobile Edge Computing) : 기존의 중앙집중식 클라우드 접근이 아닌 주변기기들을 이용해 데이터 서비스를 주고받을 수 있는 기능
* MEP(Mobile Edge Platform) : MEC를 관리, 사용할 수 있는 플랫폼
* V2X Orchestrator : V2X 서비스를 제공하기 위한 데이터를 통합하는 기능

□ 주요 핵심기술

o (디바이스) 네트워크 슬라이스 보호를 위한 단말 보안 기술
- (운영환경 보안) 비인가 자원 불법 접근 방지를 위한 신뢰 실행 환경 기술
  * 하나의 단말 내에서 네트워크 슬라이스 기반 복수의 서비스 운용 시 슬라이스 격리, 서비스 간 비인가 접근 차단, 보안정책 수립 등
- (보안 HW 모듈) 단말 신뢰 실행 환경 보장을 위한 보안 하드웨어 기술
- (슬라이스 가용성 보장) 네트워크 슬라이스 가용성 보장을 위한 고의적 단말 자원 고갈 방지 기술

o (네트워크) 네트워크 슬라이스 침해 방지 및 보호 기술
- (수준별 동적보안) 보안 수준별 네트워크 슬라이스 동적 인증/인가/접근제어 기술
  * 서비스 보안 수준 및 운영 영역에 따라 단계별(primary & secondary) 인증 고려
  * 네트워크 슬라이스 구성요소(슬라이스, 슬라이스 매니저, 하드웨어 등) 간 인증(키관리 포함), 접근제어 기술 적용을 통한 위장(impersonation) 공격 방지
  * 낮은 지연시간이 요구되는 서비스의 경우 경량 인증/고속 암호 적용, 높은 보안성을 제공해야 하는 서비스의 경우 빠른 액세스 인증과 강력한 암호 적용 등 서비스 성능/보안 요구사항에 따른 맞춤형 보안 기술 적용
- (가상화 보안) 네트워크 슬라이스 안전한 격리를 위한 네트워크 가상화 보안 기술
- (중간자 공격 대응) 네트워크 슬라이스 연계 구간 중간자 공격 대응 기술
  * 에지 수준에서 네트워크 슬라이스를 위해 동적 트래픽 제어 과정에서 코어망과 RAN 사이에 중간자 공격 가능성 차단

o (플랫폼) 네트워크 슬라이스 라이프사이클 관리 기술
- (고장감내) 무지연 서비스 보장을 위한 네트워크 슬라이스 고장 감내(fault-tolerance) 유지 기술

* 네트워크 슬라이스에 할당된 자원 장애 등에 따른 서비스 지연을 방지하기 위해 신속한 가용 자원 대체 등을 통해 끊김 없는 네트워크 슬라이스 기반 서비스 제공

- (부채널 공격 대응) 네트워크 슬라이스 실행 정보(예, 암호키, 기타 보안정보 등) 노출 방지를 위한 부채널 공격 방어 기술
- (자원 남용 방지) 악의적인 네트워크 슬라이스 인스턴스의 하드웨어 자원 남용을 통한 서비스 가용성 침해 대응 기술
- (슬라이스 취약성 점검) 네트워크 슬라이스 보안 취약성 분석 및 점검 기술

* 서비스 도메인 특화 AI 기반 지능형 비정상 행위 탐지 기술

□ 기대효과

○ 5G 네트워크 슬라이싱 보안 기술 개발을 통해 네트워크 가상화/격리 및 보안, End-to-End 보안 및 융합서비스 데이터 보안 기술력 선점

○ 5G 핵심기술인 네트워크 슬라이싱 관련 보안 기술 개발을 통해 5G 융합서비스 보안성 및 QoE(Quality of Experience) 향상

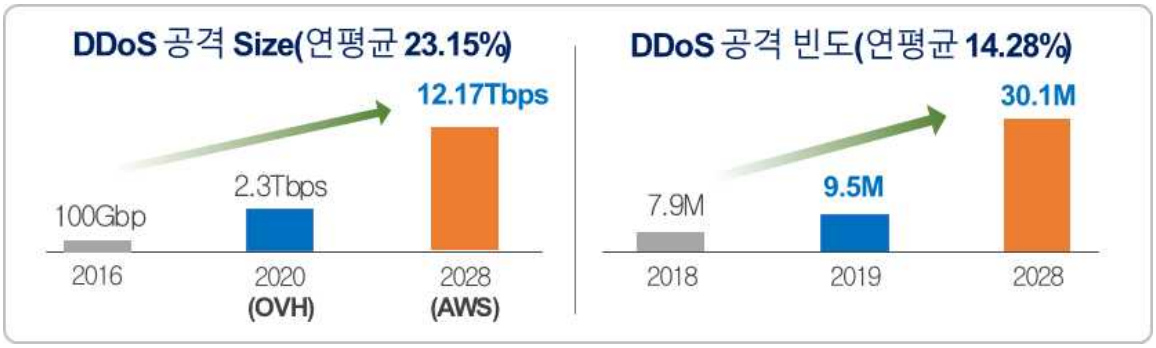
## (연구주제2) 5G 초연결 서비스 장애 위협 대응 기술

### □ 필요성

○ 이기종 망·기기·서비스의 상호 연결이 강화됨에 따라, 단일지점의 해킹과 DDoS 공격에 인한 **초연결 5G 통신 장애 방지·억제기술 필요**

- 데이터 트래픽 증가 대비 DDoS 공격* 강도 비례 증가 예측

* 공격사이즈 연평균 증가율 23.15%('16년 1테라 → '28년 12.17테라), 공격빈도 연평균 증가율 14.28%('18년 7.9백만건 → '28년 30백만건)




**위협 시나리오**

o 악성코드 감염된 Massive IoT 기기가 봇넷 무기화되어 5G 인프라(기지국, 네트워크, MEC 등) 대상으로 DDoS* 공격 시 **통신 블랙 아웃**

- 5G 통신 장애는 결제, 쇼핑, 통신 등 인터넷 서비스 연쇄적 피해 확산

* 예) '18년 KT 아현지사(화재장애), '20년 미국 T-모바일 네트워크 장애(버라이즌 등 연쇄적 장애)

- 4G 대비 10배 많은 1km$^2$ 당 100만개 IoT 기기 연결, '16년 미라이 DDoS 공격 규모 기준 11Tbps 급의 IoT 봇넷 DDoS 공격 발생 가능

* 16년 미라이 악성코드(14만대, 최대 1.5Tbps) 공격 발생

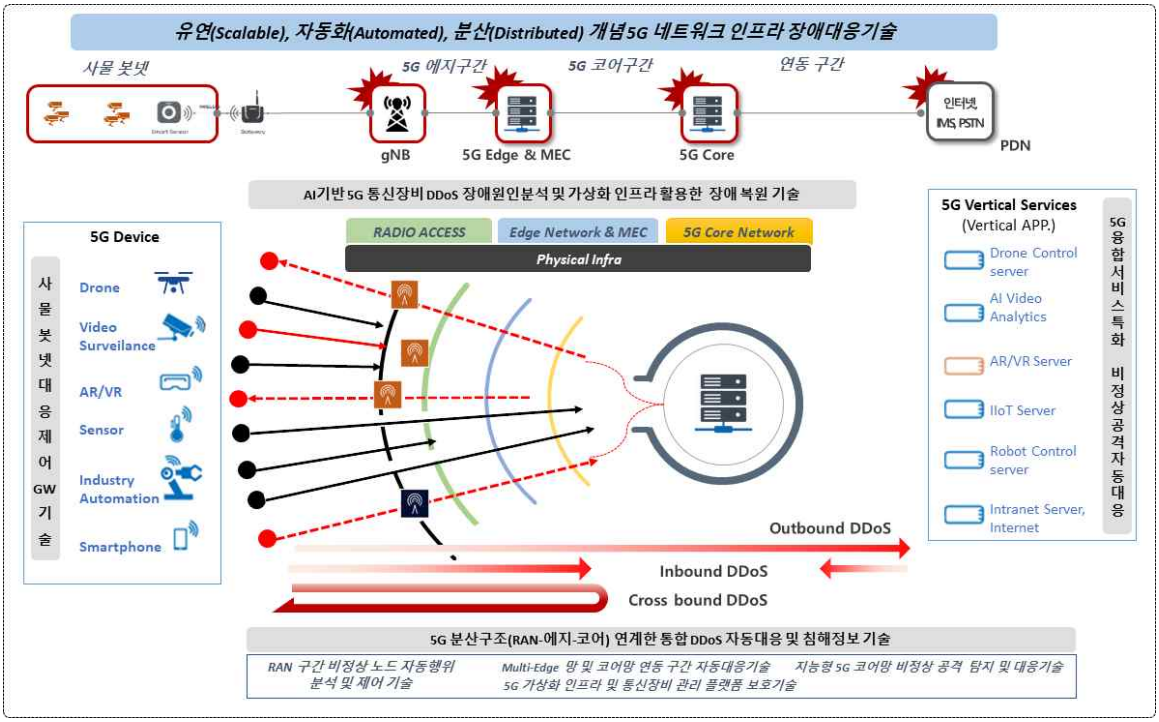
### □ 기술 정의 및 연구 목표

○ **유연(Scalable), 자동화(Automated), 분산(Distributed) 개념의 5G 네트워크 인프라 DDoS 공격 대응기술**

- (목표) 5G 성능목표에 유연하게 대응하고 고속·정교·대량 DDoS 공격의 실시간 대응·억제를 위해 현 보안기술 성능(고속, 실시간, 정교) 개선

- (범위) (D)사물봇넷 대응 제어 GW, 엑세스(AN)-에지(EN)-코어망(CN) 연동구간, 수직계층 상호 연계 구간에 대한 비정상 트래픽 억제기술

  * 단일 지점 방어에서 연결망 확산 방지, 격리 및 억제 중심 기술개발로 전환




## □ 주요 핵심기술

○ (디바이스) Massive 5G 사물 봇 탐지·제어 게이트웨이 기술

- 저사양 사물기기 5G 연동 시 보안 게이트웨이 기술

○ (네트워크) 5G 분산구조 (코어-에지) 연계한 통합 DDoS 자동 대응(탐지·차단·억제·복원) 및 침해정보공유 기술

- (코어) 지능형 5G 코어망 비정상 공격 탐지 및 대응 기술

  * (KISA) 5G NSA·SA 비정상 공격 수집, 탐지 및 모니터링 기술 등

- (Access) Deception기반 Massive 비정상 노드 자동 행위 분석·제어 기술

  * 비정상 노드(IoT 봇, GW 등) 탐지, RAN Slicing 장애 대응 등

- (에지) Multi-Edge 망 및 코어망 연동 구간 자동 대응기술

  * (ETRI) 5G 에지보안과제 일부 또는 연계

○ (플랫폼) AI기반 5G 통신장비 DDoS 장애 원인 분석 및 가상화 인프라 활용한 복원 기술

- AI기술을 적용하여 5G 통신장비의 DDoS 장애 원인을 신속하게 탐지하고 분석하는 기술
- SDN/NFV, 슬라이싱 등 5G 가상화 인프라 기술을 활용하여 DDoS 발생 시 신속 우회 경로 확보 및 장애 복원 자동화 기술

* 공격 접점 증대 위협대응기술로 이관

○ (사설 5G 망·서비스) 사설 5G 망 기반 융합서비스 (스마트시티, 스마트공장 등) 비정상 공격 대응 및 억제 기술

- 슬라이싱 기술을 이용한 초연결 네트워크 DDoS 장애 대응 기술
- 사설 5G 기반 융합 서비스별 특화된 DDoS 대응기술

* Private 5G 구축 모델 : 스마트시티, 스마트공장 등

□ 기대효과

○ 초연결 5G 네트워크 및 서비스 보안기술 확보로 5G 네트워크 인프라 보호 및 5G 연결된 융합 서비스 장애 확산 방지

○ 글로벌 5G 기술 경쟁 각축 속 국내 5G 보안 원천기술 확보와 Post 5G(6G) 보안 기술력 선점

## (연구주제3) 공격접점 증대로 인한 위협 대응 기술

□ 필요성

○ WiFi 및 대규모 IoT 연결 등 **접속환경의 다변화**, SDN/NFV 기술을 통한 **네트워크 소프트웨어화**, 가상화·MEC 확산에 따른 **분산 네트워크 구조화** 등에 따른 **공격 접점(Attack Surface)이 급증**

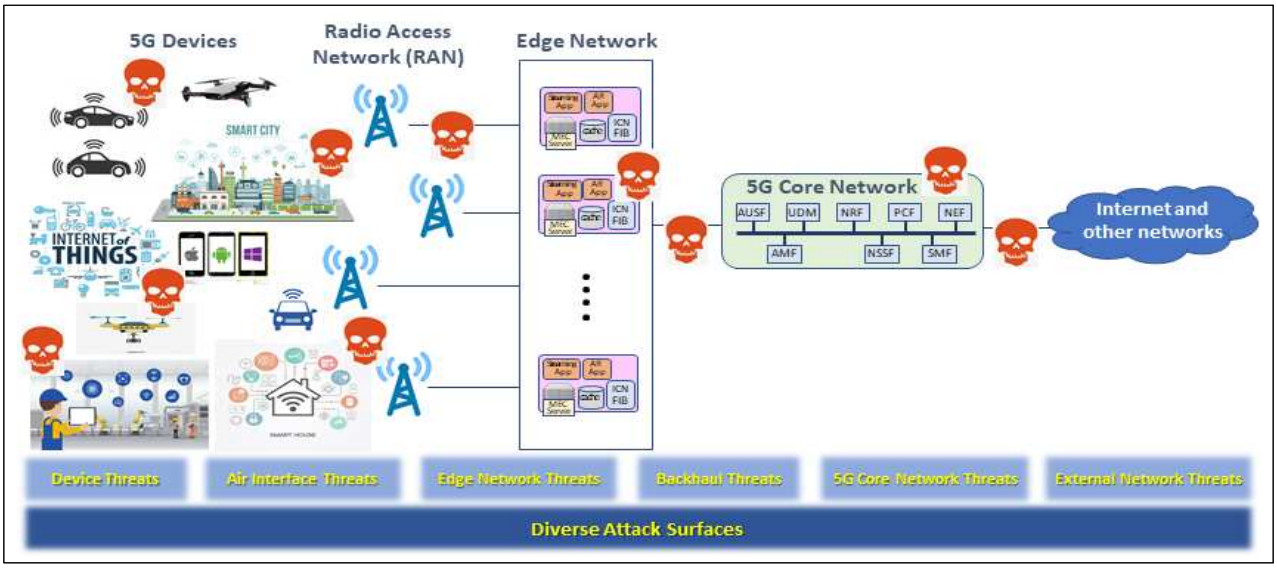
○ 5G 환경에서 새롭게 부각된 공격 접점별 위협 대응 기술 개발을 통한 **5G 네트워크 인프라 및 5G+ 융합서비스 가용성 보장** 필요

**위협 시나리오**

○ 초기 설정된 계정/패스워드를 그대로 사용하는 CCTV, NAS 같은 취약한 IoT 디바이스들을 좀비화하는 IoT 봇넷에 의해 무선 자원에 과도한 접속을 요청하는 RAN DDoS 공격으로 인하여 액세스망의 통신장비가 다운되어 네트워크 장애가 발생하고, 동시에 다발적으로 스마트 공장 內 MEC에서 실행 중인 공정제어(PLC) 소프트웨어와 로봇제어 소프트웨어 등이 악성코드에 감염되어 부품 조립 및 무빙 공정이 셧다운되거나 중요 기업 정보를 외부로 유출하는 공격 발생 가능

□ 기술 정의 및 연구 목표

○ 5G 단말, 네트워크, MEC 플랫폼에서의 지능형 침해위협 분석·탐지 및 자동화 기술



□ 주요 핵심기술

○ (디바이스) 엣지 컴퓨팅 기반 원격 디바이스 보안 기술

- (대규모 자율 인증) Massive IoT 기기 식별 및 자율 인증 기술
- (저사양 단말 보호) 자원 제약적 기기 보호를 위한 공격 대응 및 방어 기술

○ (네트워크) 5G 엣지 환경에서의 액세스 보호 기술

- (허위 기지국 탐지) 비정상(허위) 기지국 탐지 기술
- (무선 채널 보호) 무선 브로드캐스팅 채널 보호 기술

○ (플랫폼) 5G MEC 플랫폼 및 클라우드 네이티브 보호 기술

- (MEC 플랫폼 보안) MEC 플랫폼 비인가 접근 제어 및 취약성 검증 기술
- (MEC 응용 보안) MEC 응용 무결성 검증 및 이상행위 탐지 기술
- (MEC 데이터 보안) MEC 민감 정보 위변조 및 유출 방지 기술
- (컨테이너 보안) 컨테이너 런타임 이상행위 탐지 기술

○ (데이터) 탈중앙화된 분산 환경에서의 다중 도메인 인증 기술

- (MEC 데이터 비식별화) 5G MEC 저장 데이터 비식별화 기술
- (TTP-Free 인증) 다중 도메인 인증 및 분산 ID 관리 기술

□ 기대효과

○ 5G 단말·네트워크·MEC에 대한 공격접점 취약성 대응을 통한 5G 인프라 보안성 강화

○ 자동화된 실시간 5G 통합 분석 및 탐지를 통한 5G+ 융합서비스 활성화에 기여

## (연구주제4) 소프트웨어 인프라의 복잡성 대응을 위한 5G 자동 보안관리 및 관제기술

□ 필요성

- ㅇ SDN/NFV, 클라우드, 네트워크 슬라이싱 등 네트워크 소프트웨어화 및 가상화, 멀티도메인/레이어/서비스 등 관리 대상 및 영역의 다변화, massive IoT 디바이스 등 네트워크 참여자 증가에 따른 **관리 복잡성 급증**
- ㅇ 소프트웨어 기반기술에 내재된 **SW 보안위협을 해소**하고 **신뢰성을 보장**하며, SW 기반 네트워크의 확장성과 가용성 보장을 위한 **위협 탐지 및 대응 기술의 자동화** 필요

**위협 시나리오**

o 스마트 팩토리는 공장 내 설비와 기계에 센서가 설치되어 데이터를 실시간으로 수집, 분석하고 공정을 제어하여 생산과정 전 단계가 자동화된 공장을 의미하며 수많은 장비, 센서와 서버의 연결을 위해 5G 무선환경이 필수

o 다양한 이기종 IT 장비의 보안설정 취약점은 공격 진입점이 될 수 있으며, 악성코드 주입, 제어시스템 설정 변경 등을 통해 생산 중단, 매출 손실, 작업장 인명 피해 등 사고 유발 가능

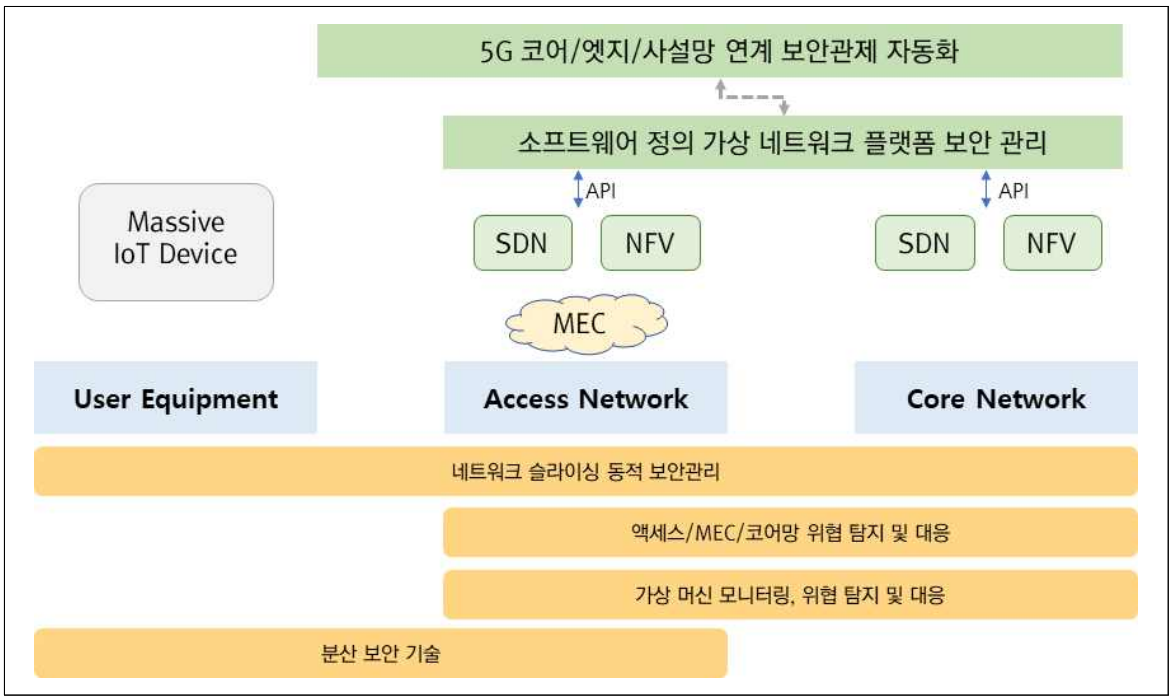
* 텔넷 포트 활성화, 관리자 계정 설정 오류 등 보안에 취약한 기본 설정 사용 시 위협에 노출
* Microsoft, 보안 설정 오류로 인해 2억 5천만명 고객 정보 유출(2019. 12.)

o 보안관리 대상의 증가로 보안가시성이 떨어져 오류, 침해의 탐지, 대응이 어려우며 장시간 피해 발생 가능

* AWS S3 Bucket(가상 스토리지 컨테이너) 설정 오류로, 1억 9000만명의 미국 유권자 개인정보(중요 파일, 패스워드, 집주소 등) 2주간 노출(2017. 6)

□ 기술 정의 및 연구 목표

○ 네트워크 소프트웨어화, 가상화에 따른 취약성 분석, 대응 기술 및 관리 복잡도 해소를 위한 자동 보안관리 및 관제 기술 개발




□ 주요 핵심기술

○ **(네트워크) 5G 코어/엣지/사설망 연계 보안관제 자동화 기술**

- (보안 자동 관제) 5G 네트워크 보안 자동 관제(SOAR)
  * SOAR(Security Orchestration Automatic Response): 다양한 보안 위협에 대한 대응 프로세스를 자동으로 분석하여 사이버 공격을 효과적으로 대응할 수 있도록 제공하는 플랫폼
- (지능형 위협 탐지/대응) 지능형 액세스/MEC/코어망 위협 탐지 및 대응 기술
  * 비정상 단말 엑세스 탐지/차단, MEC 유해 트래픽 탐지/차단, AI 기반 위협 탐지, 보안 수준 저하 없이 암호화 트래픽에 대한 보안 가시성을 확보할 수 있는 기술
- (분산 보안 관리) 중앙집중형을 탈피한 분산 인증 및 분산 보안 관리/제어 기술

* 분산 보안 관리/제어 기술: 전체 망이 아닌, 필요한 부분에 적절한 보안 기능을 배포하여 위협에 대응

o **(플랫폼) E2E 네트워크 슬라이싱 동적 보안관리 기술**

- (보안속성 연계 및 관리) 5G 망구성요소 간(UE-gNB-AMF 간)의 네트워크 슬라이스 보안 수준 유지를 위한 구성 요소 간 보안속성 연계 및 동적 관리 기술

  * UE(User Equipment)
  * gNodeB: 5G NR(New Radio) 기지국 명칭
  * AMF(Access and Mobility Function): 5G 코어망에서 단말의 이동성을 관리하는 네트워크 기능
  * Context(서비스, 데이터, 액세스, 슬라이스 등)에 따른 네트워크 보안 설정(security configuration) 개발 및 동적 적용 기술

- (전주기 관리) 네트워크 슬라이스 전주기(배포, 설치, 운영, 폐기 등) 관리 및 운영 상황 시각화 기술

o **(네트워크&플랫폼) 소프트웨어 정의 가상 네트워크 플랫폼 보안 관리 기술**

- (가상 머신 보안) MEC/NFV API 보호 기술
- (HW 기반 보안성 강화) HW 보안 Anchor(TEE, TPM 등) 기반 보안성 강화 기술

□ 기대효과

o 소프트웨어화 된 네트워크의 보안 관리 자동화 기술 개발을 통한 관리 복잡도 해소, 보안성 강화 및 확장성/가용성 확보에 기여

o 소프트웨어 기반 네트워크 보안 핵심기술 개발을 통해 SECaaS (Security as a service) 등의 신산업 창출에 기여

# Ⅳ 연차별 기술개발 로드맵

| 연구주제 | 현재 | 1단계 | | | 2단계 | | |
|---|---|---|---|---|---|---|---|
| | '20 | '21 | '22 | '23 | '24 | '25 | '26 |
| 5G 네트워크 슬라이싱 침해 위협 대응 기술 | | | 비인가 불법 접근 방지용 단말 신뢰 실행환경 기술 | | | 슬라이스 가용성 보장용 단말 자원 고갈 방지 기술 | |
| | | | 자원제약적 단말용 경량 보안 HW 기술 | | | | |
| | | | 보안 수준별 네트워크 슬라이스 동적 인증/인가 접근제어 기술 | | | 네트워크 슬라이스 중간자 공격 대응 기술 | |
| | | | 네트워크 가상화 보안 기술 | | | 네트워크 슬라이스 서비스 가용성 침해 대응 기술 | |
| | | | 네트워크 슬라이스 고장 감내 유지 기술 | | | | |
| | | | | 네트워크 슬라이스 부채널 공격 방어 기술 | | | |
| | | | 네트워크 슬라이스 보안 취약성 분석 및 점검 기술 | | | | |
| 5G 초연결 서비스 장애 위협 대응 기술 | | Deception기반 사물봇 자동 행위분석·제어 기술 | | | | | |
| | | 5G 코어망 비정상 공격 탐지 기술 | | | | | |
| | | Multi-Edge 망·코어망 연동 구간 자동 대응기술 | | | | | |
| | | | AI기반 5G 통신장비 DDoS 장애 원인분석 기술 | | | 가상화 인프라 활용한 장애 복원기술 | |
| | | | | 슬라이싱 기술을 이용한 사설 5G 환경 DDoS 장애 대응 기술 | | | |
| | | | 사설 5G 망 기반 융합 서비스별 비정상 공격 대응기술 | | | | |
| 공격접점 증대로 인한 위협 대응 기술 | | | | 대규모 기기 자율 인증 기술 | | | |
| | | | 저사양 단말 보호 기술 | | | | |
| | | 허위 기지국 탐지 기술 | | | | | |
| | | | 무선 채널 보호 기술 | | | | |
| | | MEC 플랫폼 보안 기술 | | | | | |
| | | MEC 응용 보안 기술 | | | | | |
| | | MEC 데이터 보안 기술 | | | | | |
| | | 컨테이너 보안 기술 | | | | | |
| | | | MEC 데이터 비식별화 기술 | | | | |
| | | | | TTP-Free 인증 기술 | | | |
| 소프트웨어 인프라의 복잡성 대응을 위한 5G 자동 보안관리 및 관제기술 | | 액세스/MEC/코어망 지능형 위협 탐지, 대응 기술 | | | | | |
| | | | | 5G 네트워크 자동 보안관제 기술 | | | |
| | | | 분산 보안 관리 기술 | | | | |
| | | 네트워크 보안속성 연계 및 동적 관리 기술 | | | | | |
| | | | 네트워크 슬라이스 전주기 관리 기술 | | | | |
| | | MEC/NFV API 보호 기술 | | | | | |
| | | | | HW 보안 Anchor를 이용한 SW 네트워크 보안성 강화 기술 | | | |

# Ⅴ 기대성과 및 파급효과

□ 5G 보안 선도기술 확보를 위한 기반 마련

○ **(5G 전역적 안정성 확보)** 5G 단말, 네트워크, 플랫폼, 데이터 등 5G 전역적인 보안취약점 분석 및 대응기술 확보를 위한 전략 수립 가능

○ **(미래 핵심기술 확보)** 5G 및 5G$^{+}$ 융합서비스 확산에 대비한 정보보안 경쟁력 강화 및 6G 시대를 대비한 핵심 원천기술 확보

□ 5G$^{+}$ 융합서비스 확산 및 정보보안 산업 육성 기여

○ **(5G$^{+}$ 융합서비스 확산 기여)** 정보보안 우려 해소를 통해 융합서비스 확산 및 신산업 창출 등 4차 산업혁명 중심의 혁신성장 기여

○ **(정보보안 산업 경쟁력 강화)** 정보보안 기술 선진국과의 기술격차 해소를 통한 산업 경쟁력 강화 기여

# 붙임 1 5G 보안 기술개발 로드맵 보호대상 및 문제정의

## □ 보호대상 정의

○ 5G+ 서비스 환경 변화에 따른 보호대상 : **4개 대분류와 11개 중분류**로 구성

| 분류 | 보호대상 유형 | 5G+ 시대의 환경 변화 | |
|---|---|---|---|
| | | As-Is (2019) | To-be (2021 ~ 2027) |
| 데이터 (3) | **실감 미디어 데이터** | 데이터 + 동영상 | 데이터 + 입체영상 + 홀로그램 |
| | | 자막, 이미지, 단방향 중심 | 8K UHD, 디지털 홀로그램 데이터, 메타정보(센싱정보 포함), 양방향 등 |
| | **실시간 제어 및 센싱 데이터** (5G 망을 통해 전송되는 초저지연성 데이터) | 사물기기의 인터넷 연결 | Mission Critical 데이터 급증 |
| | | IoT 센싱 정보(시공간 정보)의 단순 전송 수준 | 초저지연성이 요구되는 5G 서비스에서 실시간 제어 및 센싱 데이터 급증 |
| | **개인 · 민감 정보** (개인정보, 금융정보, 인증정보, 생체정보 등) | 개인정보보호 중심 | 데이터 보호와 활용 중심 |
| | | 개인 식별정보(주민등록번호 등)와 신용카드번호 등 일부 금융정보 활용이 제한적 활용 | 보호대상 데이터(개인생활패턴, 원격의료정보, 생체인증정보 등)가 다양화되고, 가명 처리, 동형 암호화 등 프라이버시 보호기술을 접목한 데이터 활용 증가 |
| 디바이스 (3) | **차세대 스마트 기기** (eMBB: 대용량, 초고속, 고성능 특성) | LTE 스마트폰 | 차세대 스마트폰 및 AR 기기 |
| | | 음성/영상 통화, 인터넷, 실시간 동영상 (최대 1Gbps 속도) | - Enhanced Broadband 지원 및 이동형 기기<br>- 4K/8K 실감영상, 홀로그램 등 전송속도 10~20 Gbps 급 |
| | **Massive IoT 기기** (mMTC: 저사양·저전력·고정형 및 대규모 이종 기기 연동 특성) | 근거리 및 유선 통신연동, 단일 프로토콜 연동 | 5G망 및 이종•대규모 IoT 통합•연동형 기기 |
| | | Wifi, Zigbee, 블루투스 탑재, 무선 AP 통해 유선 인터넷망 연결(10만개 연결) | - 대규모 IoT 기기에서의 이종 프로토콜 보안 연동 및 보안관리<br>- LTE-M, NB-IoT 모뎀 탑재, 5G 기지국을 통해 연결 (1km$^2$ 당 100만개 이상) |
| | **Mission Critical 기기** (uRLLC: 고신뢰·초저지연 서비스 및 이동형 특성) | 폐쇄망/전용망 구성 | 고신뢰•초저지연 위한 Edge 및 5G망 통합•연동형 기기 |
| | | 유선 인터넷에 연결 중앙 클라우드에 접근 방식 | - 이종 기기 • 네트워크 환경에서의 응답속도 10ms 이하 초저지연 및 고신뢰성(보안, QoS 관점) 제공<br>- 자율주행자동차, 로봇, 드론, 원격 수술 기기, 실시간 제어기 등 |

| 분류 | 보호대상 유형 | 5G+ 시대의 환경 변화 | |
|---|---|---|---|
| | | As-Is (2019) | To-be (2021 ~ 2027) |
| 네트워크 (3) | **5G 코어망** (RAN - 중앙 코어망) | 중앙집중형 코어망 구조 | 분산형 코어망 구조(SA 구조) |
| | | 기기/기지국(5G) + 코어망(4G LTE) 사용하는 구조 | 코어 장비의 클라우드화, 코어망 기능의 분리(CU-DU), SDN/NFV기반 네트워크 슬라이싱 등 |
| | **5G 엣지망** (RAN - MEC) | 단일 엑세스망(RAN) 구조 | 멀티 엑세스망 + 에지클라우드(MEC) |
| | | 광대역 서비스를 제공하는 단일 엑세스망(2G, 3G, 4G) | 유무선 통합 다중 엑세스망 (5G, wifi 등) + MEC |
| | **5G 사설망** (기기 - 기지국) | 독립형 이동통신 단독망 | 5G 공중망 공유하는 전용 사설 이통망 |
| | | 국내 일부 PS-LTE 전용 로컬망 | 스마트공장, 스마트시티 등 (기지국, UPF 통신장비, MEC) |
| 플랫폼 (2) | **서비스 플랫폼** (사설 MEC, 이통사 MEC, 중앙클라우드 등) | 이동통신망 외부/독립적 | 이동통신망 내부/종속적 |
| | | 이동통신망과 독립적인 외부의 중앙집중형 클라우드 서비스 플랫폼 | 이동통신망과 상호연동되는 망 내의 분산/멀티 클라우드 서비스 플랫폼 |
| | **융합서비스** (스마트공장, 스마트시티 등) | 유무선 복합 통신기반 융합서비스 | 5G 단일 통신기반 융합서비스 |
| | | 유선(위치), 4G(지연), WiFi(QoS) 등에 따른 제한된 융합서비스 환경 | 초연결·초저지연·초고속 서비스에 따른 QoS 보장 융합서비스 환경 |

## □ 보호대상별 보안기술 분류 및 정의

| 구분 | 보호 대상 | 세분류 | 보안기술 정의 | 관련된 세부 기술 예시 |
|---|---|---|---|---|
| 데이터 보안 | 실감 미디어 데이터 | **저작권 보호/ 권한 관리** | 실감 미디어 데이터에 대한 불법 변조 및 유통 방지 등 저작권을 보호하고 데이터에 대한 소유권 등 권한 관리를 강화하기 위한 기술 | - 홀로그램 등 실감 미디어별 DRM<br>- 컨텐츠 사용 이력 추적 기술<br>- 사용자별 및 행위별 권한 관리 기술<br>- 스트리밍 컨텐츠 무결성 검증 기술<br>- 컨텐츠 특화 암호화 기술 등 |
| | 실시간 제어 및 센싱 데이터 | **초저지연 암호기술** | 실시간 센싱 데이터를 안전하게 전송하기 위한 초저지연 암호 기술, 대용량 데이터를 실시간으로 안전하게 전송하기 위한 초고속 암호 기술 | - 초고속, 초저지연 특성 환경을 위한 암호, 인증 기술<br>- 암호프로토콜, SW/HW 초저지연 구현기술<br>- 부채널 공격 대응 기술 등 |
| | 개인·민감 정보 | **사용자 인증** | 사용자 인지 없이 사용자 신원을 확인할 수 있는 무접촉·무매체 인증 기술 또는 TTP (제3자 공인 신뢰기관) 없이 신원을 확인 할 수 있는 인증 기술 | - 제로 로그인 기술 (seamless & effortless authentication)<br>- TTP-free 인증(multi-domain 인증, 분산 ID)<br>- 화상회의/원격의료/온라인 강의 및 시험 보안 기술 등 |
| | | **개인정보 보호** | 서비스별로 데이터 활용성을 보장하면서 개인/민감 정보를 보호할 수 있는 기술 | - 정형·비정형 데이터의 개인정보 비식별화 기술<br>- 안전한 가명처리 기술<br>- 이종 도메인 데이터 공동 활용을 위한 동형암호 및 차분 프라이버시 등 |
| | | **데이터 신뢰성 강화** | 데이터 신뢰성 보장을 위한 기술, 미래 보안위협 대응 기술 | - 데이터 전주기 신뢰성 보장 기술<br>- AI 데이터 오염 공격 방지 기술<br>- 5G 적합 키관리 기술<br>- 양자내성 암호기술 등 |
| 디바이스 보안 | 차세대 스마트 기기 | **악성코드 등 비정상 공격 탐지** | 차세대 스마트폰 및 AR 기기에서의 실감 스트리밍 컨텐츠 (동영상, 홀로그램 등), AI 기술에 포함된 악성코드, 악의적 공격 행위 실시간으로 탐지 및 대응 | - 실감 스트리밍 컨텐츠 악성코드 탐지 기술<br>- 차세대 스마트기기용 AI 기술 취약성, 프라이버시 침해 대응 기술 |
| | Massive IoT 기기 | **이종 기기 인증 및 보안 관리** | 저사양·이종 IoT 기기의 안전성 강화를 위해, HW 단계에서부터 시작하여, Firmware, OS, SW, 서비스 단계까지 일체형으로 통합·연동하는 보안 기술 및 보안 취약성 대응·관리 기술 | - 저가 IoT 기기용 Vertical 보안 통합 연동 기술 (TPM, 보안 MCU 등 HW 보안에서 TrustZone, SW, 프로토콜 보안 연동)<br>- IoT 기기용 Trust Anchor 기술<br>- 다양한 인증·인가 기술 연동형 기기 보안 기술<br>- 저가 IoT 기기용 취약성 자동 탐지·대응 기술 |

| 구분 | 보호 대상 | 세분류 | 보안기술 정의 | 관련된 세부 기술 예시 |
|---|---|---|---|---|
| 5G 네트워크 보안 | | **대규모 기기 보안 관리** | 대규모 IoT 기기와 이종 프로토콜 연동, 코어망과 엣지망 연동 상황에서의 대규모 기기 보안 관리 기술 | - 대규모 IoT 기기(1km$^2$ 당 100만개 이상)의 보안 키 관리, 취약성 관리, 보안 관제 기술<br>- 엣지 기반 원격 기기 보안관리 기술<br>- Zero-Trust 기반 Massive 기기 자율 보안 기술 |
| | Mission Critical 기기 | **실시간 신뢰 보안 관리 및 운영** | 실시간성과 신뢰성, 보안성이 동시 요구되는 Mission Critical 기기의 내외부로부터의 악의적 행위 탐지•대응•방지 기술 및 보안 관리 기술 | - 실시간 고신뢰 서비스에서 가용성 및 보안성 동시 제공형 보안 기술<br>- 이종 고신뢰 기기용 10msec 이하의 지연시간을 갖는 end-to-end 보안 기술<br>- 이동체의 고신뢰 보안 관리 기술(키 관리, 공격 탐지·대응, 프라이버시 보호, 보안 관제 등)<br>- AI 기반 기기에 대한 악의적 공격 탐지 및 대응 기술 |
| | 5G 코어망 (ISP) | **네트워크 및 장비 보안** | Control Plane 및 User Plane 통신장비 대상으로 하는 DDoS, 공격, 프로토콜 취약점 공격,SDN/NFV 취약점, 정보유출 등을 보호하기 위한 기술 | - 5GC SDN/NFV 보안기술<br>- 코어망 비정상 탐지 모니터링 기술<br>- 5GC 공급망 SW 검증 및 진단 기술<br>- Service Based Architecture API Security (HTTP/2 및 Rest API |
| | | **5G 통합 SOAR** | 5G 네트워크 자동보안관제기술 (코어 - 에지 - 사설망 분산연계) | - Vertical Security (SDN/NFV 통합 보안 모니터링)<br>- 통합 Network Slicing 격리 및 관제기술<br>- 5G 코어/에지/사설망 통합 보안 자동관제 기술 |
| | 5G 에지망 (ISP) | **RAN 보안** | 무선 액세스 취약점을 이용한 공격, 악성코드 감염 단말, 허위 기지국을 이용한 RAN 자원 고갈 및 DDoS 방지하기 위한 기술 | - 지능형 비정상 단말 탐지 기술<br>- 액세스 공유자원 보호 기술<br>- 비정상(허위) 기지국 탐지 기술<br>- 무선 브로드캐스팅 채널 보호 기술 등 |
| | | **MEC 보안** | MEC 탑재 NFs 및 응용 SW 해킹 (악성코드 감염) 방지하고, 엣지 네트워크에서의 보안위협이 코어망으로 확대되는 것을 방지하기 위한 기술 | - 지능형 엣지 네트워크 보안 기술<br>- MEC 유해트래픽 탐지 및 차단 기술<br>- MEC 처리 데이터 보호기술 등 |
| | 5G 사설망 (사설망 | **Private 슬라이싱 보안** | 기업용 5G Private 전용망 장비 보호와 전용 네트워크 슬라이싱 보호 기술 | - 동적 네트워크 슬라이싱 보안제어 및 모니터링기술<br>- RAN Slicing 보호기술<br>- PNF/VNF 연동 보안 기술 |

| 구분 | 보호 대상 | 세분류 | 보안기술 정의 | 관련된 세부 기술 예시 |
|---|---|---|---|---|
| | 구축 기업) | **Private 통신장비 및 기기 접근통제** | 기업용 5G Private 전용망에 연결되는 도메인 특화된 IoT 기기 접근제어 및 1차/2차 인증 기술 | - 5G Private 연결 Industrial IoT Secondary 인증 기술<br>- 네트워크 슬라이싱 간 인증 기술<br>- Zero-Trust 기반 Private 통신장비(UPF, MEC) 접근통제 기술 |
| 플랫폼 보안 | 서비스 플랫폼 | **분산/ 멀티 클라우드 보안** | 기지국 또는 지역/광역국사의 MEC 및 중앙 클라우드 등 이동통신망 내의 분산 구조·멀티 클라우드 환경에서의 서비스 안정성 보장 기술 | - 클라우드의 비인가 접근 및 제어, 변조, 권한 조작 방지 기술<br>- 클라우드 데이터 위변조 및 유출 방지 기술<br>- 클라우드 응용의 악성코드 감염 및 이상행위 탐지 기술<br>- Zero-Trust 기반 클라우드간 서비스 이동성 및 연동관리 기술<br>- 클라우드 취약점 점검 기술 등 |
| | | **사설 MEC 보안** | 기업 및 기관의 사설 5G망(Non-Public Network) 내에 구축되는 MEC에 대한 내외부 단말의 접근 통제 및 데이터 보호 기술 | - 내외부 단말의 사설MEC 접근제어 기술<br>- 사설 유선망-5G망 네트워크 접근제어 기술<br>- MEC 데이터 및 시스템자원 정밀 접근제어 기술 등 |
| | | **클라우드 네이티브 환경 보안** | 클라우드 네이티브(Cloud-Native) 환경의 도입 및 확산에 따른 마이크로서비스 구조 기반 컨테이너 보호 기술 | - 컨테이너 런타임 이상징후 탐지 기술<br>- 컨테이너 이미지 무결성 및 취약성 검증 기술<br>- 컨테이너 제어 권한 탈취 방지 기술<br>- 개방형 API 취약성 검증 기술 등 |
| | | **서비스 트래픽 보안** | UDP 세션 공격이나 비정상 암호화 트래픽 등 유해 트래픽으로부터 서비스 플랫폼을 보호하기 위한 기술 | - UDP/QUIC 프로토콜 비정상 행위 탐지 기술<br>- AI 기반 암호화 트래픽 이상징후 탐지 기술 등 |
| | 융합 서비스 | **스마트 공장 보안** | 스마트공장에서 사용되는 다양한 기기의 보안성 및 신뢰성 확보를 위한 기기별 인증, 상호 보안 인증과 비인가 접근 차단 등 분석을 통한 5G 보안취약성 자동 진단 기술 | - 5G 기반 제조인프라 통합보안 및 자동 대응 기술<br>- 제어시스템 무선통신 보안 기술<br>- 스마트공장 5G 보안취약성 자동 진단기술 등 |
| | | **스마트 시티 보안** | 5G 환경의 스마트시티 운영 시스템을 대상으로 발생하는 외부(DDoS, 사이버표적공격 등) 및 내부(내부자 데이터 유출 등)의 사이버 보안 위협을 탐지하는 보안관리 기술 | - 스마트시티 이종기기 상호 인증 기술, 스마트시티 통합운영 플랫폼 보안 위협 탐지·대응 기술<br>- 5G기반 스마트시티 통합보안 관제 및 자동대응 기술 |

# 붙임 2 5G보안협의회 기술분과 및 기술로드맵 작업반 위원 명단

## □ 기술분과

| 구분 | 이름 | 소속 및 직위 | 전자우편 |
|---|---|---|---|
| 분과장 | 유일선 | 순천향대학교 교수 | ilsunu@gmail.com |
| 전문기관 | 정현철 | IITP 차세대보안 PM | hcjeong@iitp.kr |
| | 김익균 | ETRI 정보보호연구본부장 | ikkim21@etri.re.kr |
| | 이석래 | KISA 정보보호산업본부장 | slleeks@kisa.or.kr |
| | 권대성 | NSR 암호연구센터장 | ds_kwon@nsr.re.kr |
| 학계 | 김호원 | 부산대학교 교수 | howonkim@pusan.ac.kr |
| | 안효범 | 공주대학교 교수 | hbahn@kongju.ac.kr |
| | 박기웅 | 세종대학교 교수 | woongbak@sejong.ac.kr |
| | 최형기 | 성균관대학교 교수 | meosery@g.skku.edu |
| | 이옥연 | 국민대학교 교수 | oyyi@kookmin.ac.kr |
| | 김환국 | 상명대학교 교수 | rinyfeel@smu.ac.kr |
| 이통사 | 이종식 | KT 상무 | jong-sik.lee@kt.com |
| | 박종관 | SKT 랩스장 | jongkwan.park@sk.com |
| | 이상헌 | LGU+ 상무 | sanghlee@lguplus.co.kr |
| 보안기업 | 조학수 | ㈜윈스 부사장 | marius71@wins21.co.kr |
| | 심상규 | 펜타시큐리티시스템 CTO | sgsim@pentasecurity.com |
| | 이동범 | 지니언스(주) 대표 | dblee@genians.com |
| 간사 | 김종현 | ETRI 책임연구원 | jhk@etri.re.kr |
| | 박종근 | ETRI 책임연구원 | queue@etri.re.kr |

# □ 기술로드맵 작업반

* 2020.11.06. 기준

| 소분과 | 이름 | 소속 및 직위 | 전자우편 |
|---|---|---|---|
| 데이터 | 권대성 | NSR 센터장 | ds_kwon@nsr.re.kr |
| | 김우환 | NSR 실장 | whkim5@nsr.re.kr |
| 디바이스 | 김호원 | 부산대학교 교수 | howonkim@pusan.ac.kr |
| | 임재덕 | ETRI 책임연구원 | jdscol92@etri.re.kr |
| 네트워크 | 김환국 | 상명대학교 교수 | rinyfeel@smu.ac.kr |
| | 유일선 | 순천향대학교 교수 | ilsunu@gmail.com |
| 플랫폼 | 박종근 | ETRI 책임연구원 | queue@etri.re.kr |
| | 김영수 | ETRI 책임연구원 | blitzkrieg@etri.re.kr |