발 간 등 록 번 호
11-1741000-000180-01

정부사물인터넷 도입 가이드라인

2019. 7

행 정 안 전 부

NIA 한국정보화진흥원

목 차

일 러 두 기

□ 배경 및 목적

○ 모든 사람과 사물을 연결하는 초연결사회가 도래함에 따라 다양한 센서를 일상생활 속 사물에 탑재하여 데이터를 수집·공유할 수 있게 되어

○ 수집된 데이터를 실시간·지능적으로 처리하여 공공서비스에 활용하기 위해 사물인터넷 기술이 활발히 도입중이므로 이에 대한 기술기준이나 표준정립이 필요

□ 적용범위 : 사물인터넷을 도입하려는 행정기관

□ 가이드라인의 성격

○ 행정기관이 사물인터넷 기술을 활용하여 정부서비스를 구현·운영할 경우 고려해야 할 기준이나 참고 사항을 포괄적으로 정리한 안내서 역할

* 사물인터넷을 활용한 정부서비스 도입·운영시 고려해야 할 사항을 종합적으로 제공하여 행정기관간 상호호환성, 서비스 확장성·연속성·보안성 및 인프라의 효율적 구축·운영관리를 지원

○ 본 가이드라인은 법·제도 등 타 기관에서 제시하는 일반적인 권고내용을 포함하고 있으므로, 이행계획 수립 시 **반드시 관련 권고의 최신내용 확인을 권장**

□ 주요용어* 정의

* 가이드라인 활용 및 의사소통 시 혼돈을 줄 수 있는 용어를 "주요용어"로 정의하며, 기술용어와 같은 내용과 성격이 명확한 용어에 대한 정의나 설명은 각 주 등 본문에서 기술함

용어	정의
사물인터넷(IoT)	• Internet of Thing의 약칭, 인터넷을 기반으로 다양한 사물, 데이터, 프로세스 및 사람을 유기적으로 연결하고, 상황을 분석·예측·판단하여 지능화된 융합서비스를 자율적으로 제공하는 제반인프라(ETRI, 2017)
정부사물인터넷(G-IoT) = 정부사물인터넷 인프라	• Government-IoT의 약칭, 행정기관 등 정부가 국가·사회 현안 해결의 수단으로 활용하는 IoT 기술 및 관련 인프라를 통칭
디바이스 또는 단말	• 용도별 센서가 내장되어 센싱한 데이터를 게이트웨이로 전송
게이트웨이	• 센싱 데이터를 네트워크서버로 전송하고, 서비스 제어신호를 디바이스로 전송(소형·저전력 등 열악한 디바이스의 처리능력을 보충)
네트워크서버	• 디바이스·게이트웨이 간 전송 효율화 및 디바이스 배터리 수명연장
관리서버	• 디바이스 등록·인증 등 사물인터넷 서비스 전반을 관리
애플리케이션서버	• 서비스 제공 및 이용자와 서비스 간 소통창구(WEB 등) 역할
운영서버	• G-IoT 인프라에 대한 운영관리 및 관제를 위한 시스템
정부사물인터넷 네트워크 = 정부사물인터넷 망	• 디바이스·게이트웨이·플랫폼 간 연결을 담당하는 네트워크 - 디바이스네트워크(디바이스~게이트웨이 간), 백홀네트워크(게이트웨이~플랫폼 간), 백엔드네트워크(플랫폼~플랫폼 간) 등 기능별로 구분
정부사물인터넷 플랫폼	• 관리서버·애플리케이션서버·운영서버 등 G-IoT서비스 시스템
정부사물인터넷 서비스	• 약자보호, 안내, 시설관리 등 IoT기술로 구현된 정부서비스
정부사물인터넷 공통기반	• G-IoT서비스 간 시너지 창출을 위해 구축한 정부 공통활용 시설
행정망(행정정보통신망)	• 행정기관이 개별 구축한 업무용 정보통신망
자체망	• 행정기관이 자체적으로 구축한 G-IoT망(자가망·행정망 등)
정부공통망	• 국가정보통신망(K-Net), 국가융합망 등 행정기관 공통활용 망
상용망	• 통신사업자가 구축하여 상용으로 제공하는 망
상용 사물인터넷 망	• 사물인터넷 서비스 구현을 위해 제공하는 상용화 네트워크
상용 사물인터넷 서비스	• 네트워크·플랫폼 등 사물인터넷 서비스 전체를 상용화 제공

(요약)

정부사물인터넷 도입 가이드라인

제1절 사물인터넷 개요

1 사물인터넷

가 사물인터넷(IoT*) 정의 * IoT : Internet of Thing의 약어

○ 정보통신기술 기반으로 모든 사물**을 연결해 사람과 사물, 사물과 사물 간에 정보를 교류하고 상호 소통하는 지능형 인프라 및 서비스 기술

** 사물은 웨어러블 디바이스, 모바일 장치, 가전제품 등 다양한 임베디드 시스템을 의미하며, 상호간 통신을 위해 IP주소·OID(Object IDentifier) 등 식별할 수 있는 고유의 식별자를 가짐

나 주요 특징

○ 모든 사물을 인터넷으로 연결하여 사물 간 센싱, 네트워킹, 정보처리 등으로 사람의 개입 없이 지능적·자율화 서비스를 제공하는 방향으로 발전 중

다 구성 요소

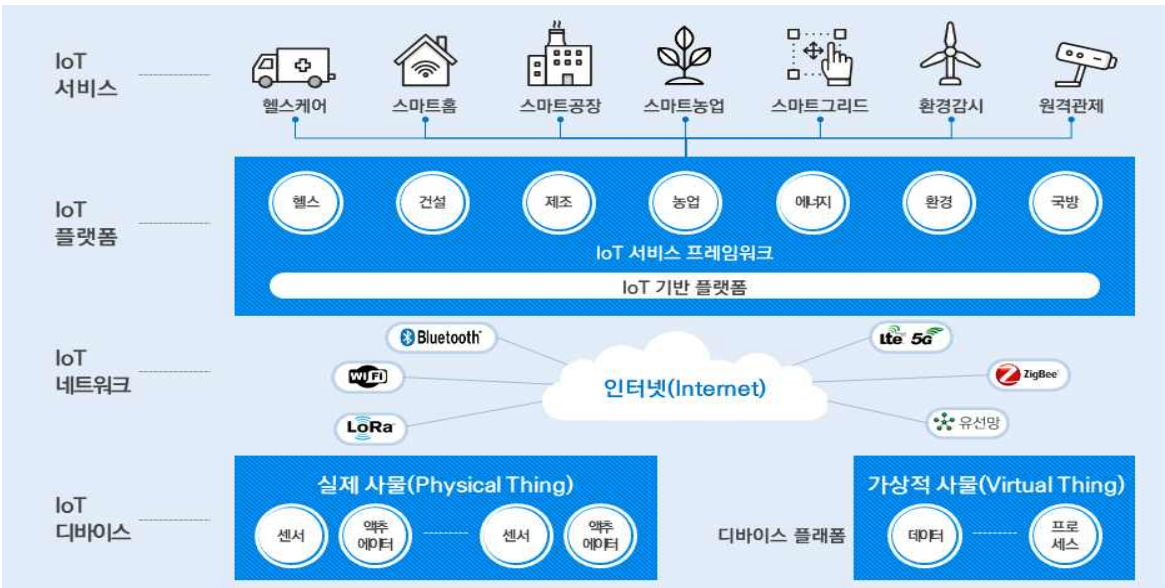
○ (디바이스) 데이터 수집용 센서, 제어용 액추에이터, 통신모듈 등으로 구성

○ (네트워크) 근거리·장거리(저전력) 무선통신, 유선통신 기술로 구성

○ (플랫폼) 빅데이터·인공지능 등 지능정보기술로 구현된 서비스 프레임워크

○ (서비스) 헬스케어·스마트홈·환경감시·원격관리 등 IoT로 구현한 서비스

≪그림1-1 : 사물인터넷 구성 개념도≫



라 사물통신

○ (RFID*) 사물에 소형 전자칩과 안테나로 구성된 전자태그(Tag)를 부착하고, 리더(Reader)가 무선주파수로 전자태그의 고유정보를 읽어 사물을 인식

* Radio-Frequency IDentification의 약칭. 유통 경로, 재고 관리, 교통카드, 지불 결제, 출입 통제, 도시 관리, 차량 · 선박 등의 위치 추적 등의 분야에서 활용 중

○ (RFID/USN**) IT839정책(정보통신부, 2004)의 일환으로 시작된 사물통신 인프라

** Ubiquitous Sensor Network의 약칭. 온도·습도·가스·열감지 등 다양한 목적의 센서와의 정보 전송 네트워크를 구성하여 언제, 어디서나, 다양한 서비스를 제공할 목적의 서비스 인프라

○ (M2M***) 지능화된 기기들이 사람을 대신해서 사물간 통신을 수행하는 기술

*** Machine To Machine의 약칭. M2M과 사물인터넷은 1)사물 간 통신을 한다는 점과 2)사물에 기본적인 지능을 구현한다는 공통점 때문에 서로 혼용되기도 함

○ M2M은 주로 사람이 접근하기 힘든 지역의 원격 제어나 위험물의 상시 검사 등의 영역에서 적용된 반면, RFID는 홈 네트워킹이나 물류, 유통 분야에 적용되다가 NFC로 진화해 모바일 결제 부문으로 영역을 확장

마 사물통신과 사물인터넷

○ (연관성) 사물인터넷은 사물통신(RFID/USN, M2M;사물지능통신)의 진화된 개념

○ (차이점) 사물통신은 상황에 대처하기 위해 사물과 통신하는 것에 중점하나, 사물인터넷은 인간을 둘러싼 환경에 중심을 두고 자율적 상황대처에 중점

≪표1-1 : 사물통신과 사물인터넷 비교≫

구분	사물통신 (RFID/USN, M2M)	사물인터넷 (IoT)
통신·네트워크	사물통신을 위한 목적망 (근거리망, 이동망 등)	자율화 서비스를 위한 초연결망 (근거리망, 이동망, 저전력·장거리망 등)
디바이스 구성형태	RFID·센서 중심	센서, 액추에이터 등 실제 사물과 데이터와 프로세스 등을 포함한 가상 사물
사물의 구동 수준	수동적 (단순 정보 수집)	자율적 (자율 판단하는 지능 보유)
서비스 플랫폼	모니터링 정보 처리	의미 기반 모니터링 및 자율 제어
사물 연결 규모	수천만 개의 사물	수백 억 이상의 사물
서비스 적응성	수직적 대응 서비스 제공	즉시적 맞춤식·지능화 서비스 제공

2 정부사물인터넷

가 정부사물인터넷(G-IoT*) 정의 * G-IoT : Government-IoT의 약어

○ 정부가 공공(대민서비스 혁신), 산업(생산성·효율성 및 부가가치 향상), 개인(안전, 편리 등 삶의 질 제고) 등 국가 사회 현안 해결의 수단으로 사물인터넷 기술을 활용하기 위해 도입·운영하는 서비스·플랫폼·네트워크·디바이스 등 사물인터넷 인프라를 정부사물인터넷이라고 정의

≪표1-2 : 지자체 정부사물인터넷 도입·운영 사례≫

구분	주요 서비스(예시)
시설관리	• 주차관리, 원격검침, 조명제어, 음식물종량제 관리 등
안내	• 관광 다국어안내, 보건정보서비스, 버스정보시스템
약자보호	• 안심 벨, 사회적약자 위치관리, 응급안전알림 등
재난안전	• 지진계측, 홍수감시, 이상음원인식, 응급지원 등

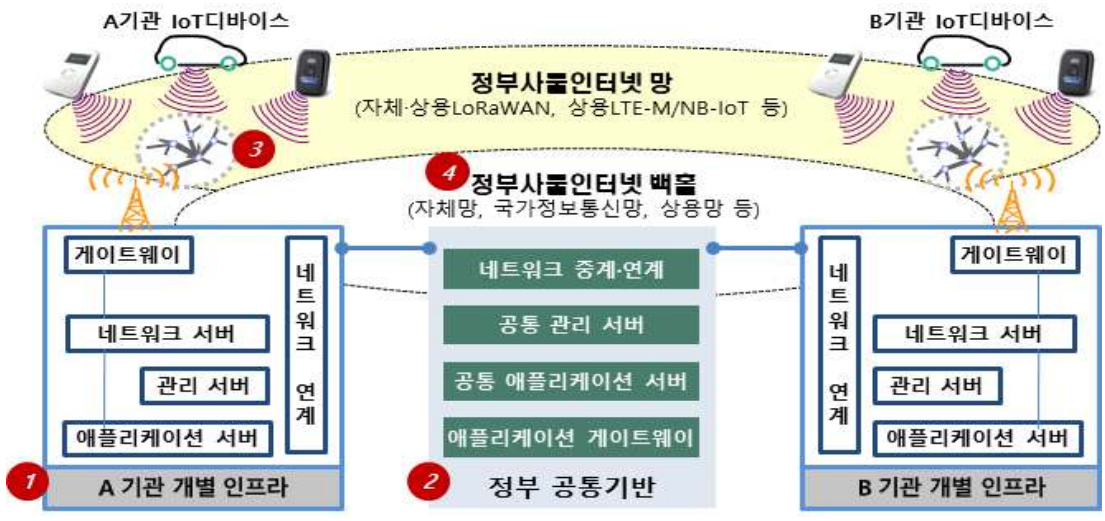
나 구성 요소

○ (행정기관 개별 인프라①) 각 행정기관이 개별 구축한 G-IoT 인프라

○ (정부 공통기반②) 기관간 연계 등 공동활용을 위해 구축한 시스템

○ (정부사물인터넷 망③·백홀④) 디바이스·게이트웨이 간 무선망과 플랫폼 연결망

≪그림1-2 : 정부사물인터넷 구성 개념도≫



다 사물인터넷과 정부사물인터넷

○ 사물인터넷은 사업자 이익을 위해 서비스를 개발하고 활용 및 제공하는 반면, 정부사물인터넷은 국민 편익과 보호를 위해 도입 및 서비스 제공

※ 사물인터넷과 정부사물인터넷은 동일한 사물인터넷 기술(디바이스·네트워크·플랫폼 등)을 활용한다는 점은 같으나, 도입 목적과 사용 주파수 대역, 법·제도 적용관점 등에서 차이가 있음

≪표1-3 : 사물인터넷과 정부사물인터넷 서비스 비교≫

구분	사물인터넷	정부사물인터넷
운영 주체	민간 사업자	정부(행정기관)
제공 목적	이익 창출	국민 편익제공 및 보호
주요 규제	이용자 보호, 개인정보 보호 등	개인정보 보호 등
주파수 대역	면허 및 비면허 대역 모두 활용	면허(임차)·비면허(자가/임차) 구분 활용
디바이스 네트워크 기술	LTE-M·NB-IoT, 5G, LoRa·Sigfox 등	

라 관련 법·제도

○ 사물인터넷은 특성상 정보통신, 교통, 환경, 의학, 안전, 건축 등 다양한 분야와 연관되고, 생활 전반에 걸쳐 활용되므로 여러 분야의 법률과 관련

≪표1-4 : 사물인터넷과 정부사물인터넷 적용되는 관련 법·제도≫

법·제도	주요 조항
개인정보 보호법	• 제3조 개인정보 보호 원칙 • 제17조 개인정보의 제3자 제공 • 제21,23조 민감정보 동의와 개인정보 파기
위치정보의 보호 및 이용 등에 관한 법률 (약칭 "위치정보법")	• 제2조 정의 • 제3장 위치정보의 보호
정보통신망 이용촉진 및 정보보호 등에 관한 법률 (약칭 "정보통신망법")	• 제4장 개인정보의 보호 • 제5장 정보통신망에서의 이용자 보호 등 • 제6장 정보통신망의 안정성 확보 등 • 제7장 통신과금서비스
전기통신사업법	• 제6조 기간통신사업의 등록 등
정보통신 진흥 및 융합 활성화 등에 관한 특별법 (약칭 "정보통신진흥특별법")	• 제3조 기본원칙 • 제28,29조 공공부문의 정보통신장비 구축사업 등 • 제36,37조 신규 정보통신융합등 기술·서비스의 신속처리 등
의료법	• 제27조 무면허 의료행위 등 금지 • 제33조 개설 등 • 제34조 원격진료
의료기기법	• 제6조 제조업의 허가 등
자동차관리법	• 제3장 자동차의 안전기준 및 자기인증
[보안지침] : 국가·공공기관 사물인터넷(IoT) 보안 가이드라인(국가정보원)	

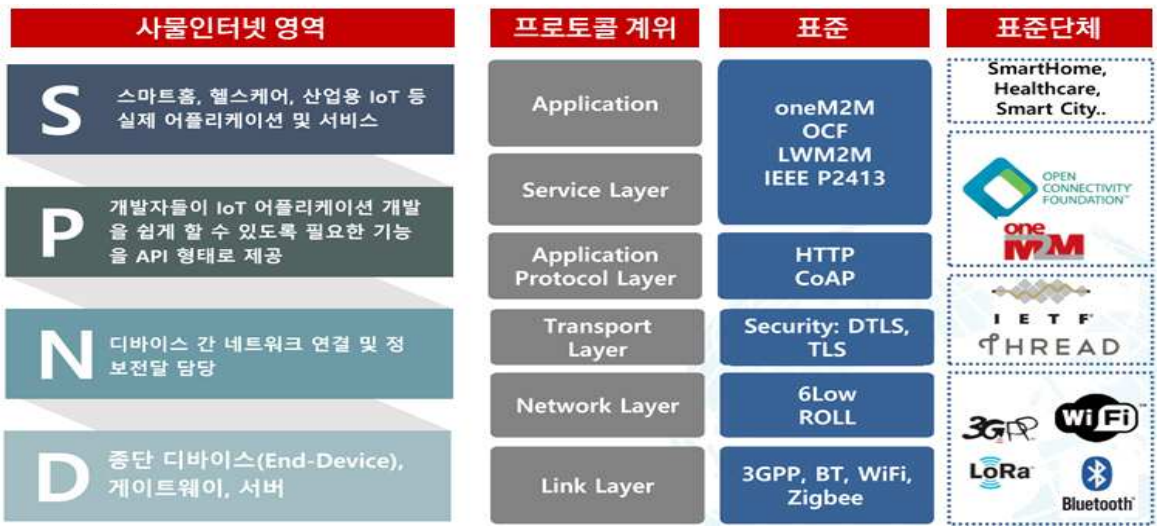
3 사물인터넷 관련 표준

가 사물인터넷 표준화 개선방향

○ 행정기관에서 자체적으로 사물인터넷을 도입할 경우 서비스 연속성 보장, 타 서비스 및 공통기반 등에 대한 연동 및 호환성·상호운용성, 향후 확장성 확보를 위해 관련 NB-IoT·LTE-M·5G 등 국제표준, oneM2M·OCF·LoRa 등 개방형 표준 아키텍처 채택 필요

나 사물인터넷 영역별 표준 및 표준화 단체

≪그림1-3 : 영역별 표준 및 표준화 단체 (자료출처: TTA)≫



다 행정기관 자체망 구축시 적용표준

○ (LoRa=네트워크) 저전력 장거리 전송을 저비용으로 구현하기 위한 표준으로 디바이스가 게이트웨이에 연결되어 데이터가 전송·분석·활용되는 구조

○ (oneM2M=플랫폼) TTA(한국)·TIS(미국)·ITU-T(국제) 등 각국 표준화 단체가 참여하여 만든 IoT플랫폼 규격이며, 현재 2단계(Release*2) 표준화 진행 중

* Rel.1: 공통서비스 기능정의 등, Rel.2: 플랫폼 및 네트워크 연동 등, Rel.3: 연동기술 확대 등

○ (OCF=장치간 상호연동) 삼성·인텔·퀄컴·시스코 등 H/W제조사가 참여하여 만든 IoT기기 상호연동성 보장 규격이며, 사물인터넷 유무선 연결기술들을 활용하여 다양한 사물인터넷 서비스(Profiles)를 개발할 수 있도록 구성

제2절 사물인터넷 인프라 구성

1 사물인터넷 인프라 개요

○ 디바이스·네트워크·플랫폼·서비스 등 일반 IT기반 서비스와 동일하나, 사물인터넷을 위한 디바이스(다량·저전력)와 게이트웨이(초연결)가 강조되는 구성

≪그림2-1 : 사물인터넷 인프라 구성도≫

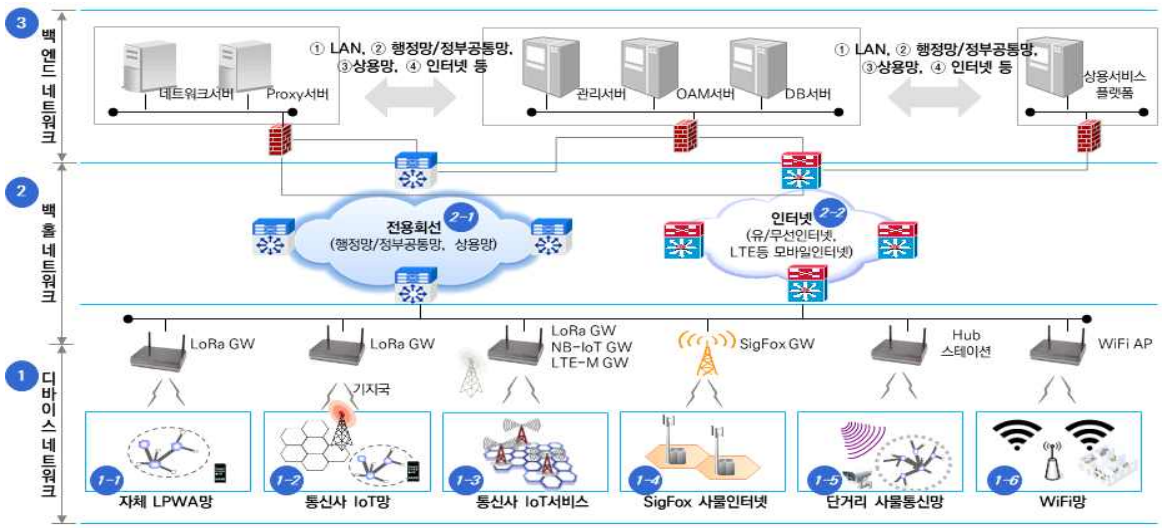
가 네트워크 구성

○ (디바이스 네트워크①) 디바이스와 게이트웨이 간 네트워크로 다양한 모델이 있으나, 주로 사물인터넷에 적합한 저전력·장거리(LPWA) 무선통신망으로 구성

○ (백홀 네트워크②) 게이트웨이 환경에 맞는 다양한 유·무선 전송망으로 구성

○ (백엔드 네트워크③) 트래픽 집중 구간이므로 초고속·고가용성 IP망으로 구성

≪그림2-2 : 사물인터넷 네트워크 구성도≫



나 디바이스

○ IoT디바이스는 주위 환경에서 온도·습도·가스·위치·동작 등의 데이터를 수집하는 장치로 용도별 해당 센서와 데이터 전송용 통신모듈을 포함하며,

- 센싱 및 데이터 전송에 배터리와 같은 전원이 필요하며, 수량이 대량인 점과 설치 위치로 인해 배터리 교체가 어려우므로 저전력화가 중요

≪그림2-3 : 사물인터넷 디바이스 구성 개념도≫

다 게이트웨이

○ IoT디바이스로부터 데이터를 수집하고, 데이터를 네트워크서버로 전달하며, 디바이스의 소형·저전력 특성으로 인한 낮은 성능과 메모리 한계를 보충

- 디바이스와는 유선*, 근거리**·장거리*** 무선 등 다양한 방식으로 통신

* Ethernet, FTTx 등 ** WiFi, Zigbee, Bluetooth, Z-Wave, RFID 등 *** LTE-M, NB-IoT, SigFox, LoRa 등

≪표2-1 : 사물인터넷 게이트웨이 주요 기능≫

기능	내용
사물간 연결 및 메시지 교환 지원 기능	• 다양한 사물 및 서버 플랫폼간의 통신을 위한 상호 연결지원 및 메시지 라우팅 기능
수집데이터 처리·전송 기능	• 응용에 따라 여러 사물로부터 수신한 정보를 합병(merge) 및 가공하여 외부로 전송하는 기능
다양한 네트워크 프로토콜 간 변환기능	• 지그비 등 저전력 센서 네트워크, CoAP, HTTP, 인터넷 등 다양한 프로토콜을 사용하는 사물간 통신을 위한 프로토콜 변환기능
사물 디바이스 관리 기능	• 사물 디바이스와의 연결을 위한 사물 연결 소프트웨어와 연동을 수행하고 연결된 사물 디바이스를 관리하는 기능
리소스 관리 기능	• 사물 디바이스의 프로파일 및 수집된 정보와 게이트웨이 내부의 정보를 관리하는 기능
서버플랫폼 연동 기능	• 사물인터넷 서버 플랫폼과 연동을 통해 정보수집 및 제어서비스를 제공하는 기능
보안 기능	• 사물인터넷 게이트웨이, 사물 디바이스, 사물네트워크에 대한 사이버 공격에 대응하기 위한 보안 기능

2 디바이스 네트워크

가 디바이스 네트워크 개요

○ 디바이스 네트워크는 디바이스와 게이트웨이 간 통신을 담당하며, 디바이스는 집안・안심존・교량 등 특정장소에 고정되어 있는 경우도 있지만, 이동하는 형태도 있으므로 상황에 맞게 통신기술 적용 필요

○ 사물인터넷 디바이스 네트워크는 주로 무선방식을 적용하며, 통신 거리에 따라 저전력 광역 무선망(LPWAN, Low Power Wide Area Network)과 근거리 무선통신으로 구분

나 저전력 광역 무선망(LPWAN)

○ 사용 주파수 대역에 따라 면허* ・비면허** 대역으로 구분하며, 비면허 대역은 LoRaWAN과 SigFox, 면허 대역은 LTE-M과 NB-IoT가 대표적 기술

≪표2-2 : 저전력 광역 무선망 주요 기술방식 비교≫

구분	비면허 대역 LPWA기술		면허 대역 LPWA기술	
	LoRaWAN	Sigfox	LTE-M	NB-IoT
커버리지	~5Km(도심) ~15Km(비도심)	~10Km(도심) ~30Km(비도심)	~11Km	~15Km
배터리 수명	~10년	~10년	~10년	~10년
통신모듈 가격	~5$	~5$	~20$	~10$
표준화	LoRa얼라이언스 (완료)	ETSI (완료)	Cat-1: 3GPP Rel.8(완료) PSM: 3GPP Rel.12(완료)	3GPP Rel.13(완료) 3GPP Rel.14(진행)
주파수대역	920MHz	920MHz	LTE	LTE
대역폭	500KHz	200KHz	20MHz	200KHz
통신속도	< 5Kbps	< 1Kbps	다운:10M, 업:5Mbps	~100Kbps

다 근거리 무선통신망

○ 커버리지가 매우 제한적인 단점이 있지만, 특화된 용도가 있고 각종 기기에 범용으로 적용된 기술도 있어서 장거리 유・무선 기술과 조합하면 효과적

≪표2-3 : 주요 근거리 무선통신 기술방식 비교≫

구분	블루투스	NFC	지그비	지웨이브	WiFi
주파수 대역	2.4GHz	13.56MHz	2.4GHz(글로벌)	868~929MHz	2.4G, 5GHz, 60GHz
전송거리	1~100m	10cm이내	100m이상	100m이상	약 100m
전송속도	~2M(BLE~1M)bps	424Kbps	250Kbps	40Kbps	ac~1.7G , ah100Kbps ax 9.6Gbps, ay 20Gbps
응용분야	주변기기 (헤드셋 마우스 등)	전자결재, 기기간 직접전송	홈 네트워킹, 빌딩 자동화	홈 네트워킹, 빌딩 자동화	인터넷 접속, 무선LAN 구성
소비전력	1~100mW	50mW	1~100mW(Low)	Low	평균 100mW
특징	저전력 가능, AP없이 접속가능, 커버리지에 제약	무 전원 동작, 전파간섭 없음	저전력·저비용 네트워크 구성 가능, 타 통신과 간섭 우려	전파 효율성 및 호환성 우수	전력소모 많고 소형화 어려움, 커버리지 확장 가능

3 백홀·백엔드 네트워크

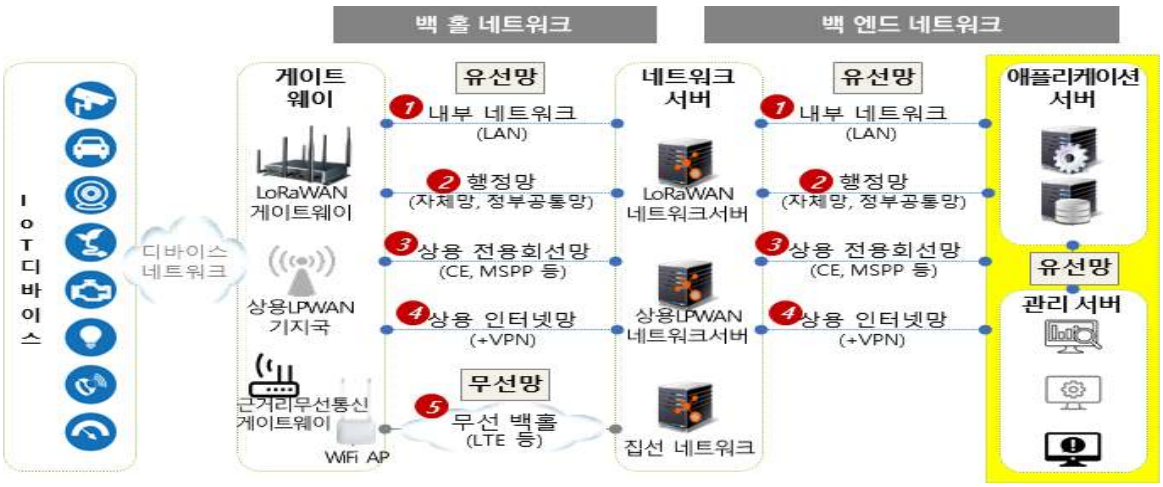
가 백홀·백엔드 네트워크 개요

○ (백홀) 수많은 센서로부터 게이트웨이에 전달된 수집 데이터를 네트워크서버 등 중앙서버로 전달하기 위해 사용되는 기술로 유선* · 무선** 방식으로 망을 구성

* LAN(Ethernet), 전용회선(행정망·상용망), 인터넷 등, ** 3G·LTE, WiFi, M/W(MicroWave), TVWS 등

○ (백엔드) 중앙서버 간 다량 · 대용량 데이터 전송을 담당하는 백본 네트워크이므로 초고속 · 고신뢰성 구성이 필요하여 주로 유선망으로 다중화 구성

≪그림2-4 : 백홀·백엔드 네트워크 구성모델≫



나 구성 유형

○ 중앙서버들은 동일센터에 설치되거나 원격으로 분산 설치될 수 있으며, 구성유형은 서버의 구축 위치와 서버 간 통신망 종류에 따라 구분

≪표2-4 : 중앙서버 설치위치에 백홀·백엔드 따른 네트워크 구성유형≫

구성 유형		네트워크 구간별 통신망 종류		서버 설치위치		
		GW↔NS(백홀)	NS↔AS(백엔드)	GW	NS	AS
동일 위치내 운영		LAN	LAN	동일 위치		
게이트웨이가 원격지에 위치		자체망	LAN	원격	동일 위치	
		상용인터넷망(VPN)	LAN	원격	동일 위치	
모든 서버가 서로 다른 위치	WAN 혼용	자체망	정부공통망	원격	원격	원격
		상용 인터넷망(VPN)	상용 전용회선망	원격	원격	원격
		자체망	상용 전용회선망	원격	원격	원격
	WAN 통일	상용 인터넷망(VPN)	상용 인터넷망(VPN)	원격	원격	원격
상용 플랫폼을 활용하는 경우		상용사물인터넷망	상용망(VPN)·정부공통망	원격	원격	원격
		상용 사물인터넷 서비스		원격	원격	원격

※ <범례> GW: 게이트웨이, NS: 네트워크서버, AS: 애플리케이션서버, VPN: 인터넷 보안 강화용

제3절 정부사물인터넷 인프라 도입기준

1 디바이스·게이트웨이 도입기준

가 공통 사항

○ IEEE 및 IETF, ETSI, 3GPP 등의 관련 표준을 준수하고, 개방형 표준을 준수*하여 개발된 제품 도입 * LoRa 디바이스 및 게이트웨이의 경우 LoRaWAN Specification 규격

○ 국내 전파 관련법을 준수한 제품*을 도입

* [과학기술정보통신부령 제1호, 2017.7.26. 고시]「전파법」제45조 및 「무선설비규칙」제19조에 따라 신고하지 아니하고 개설할 수 있는 무선국용 무선설비의 기술기준(제 8조)을 만족하여야 함

○ 옥외 설비의 경우 전기제품외함 보호규격(IEC-529 Standard) 조건에 따라 방수·방진 규격 IP-54 이상을 만족하는 제품을 도입* * 인증기관 시험성적서 제출

○ [전기방송통신설비의 기술기준에 관한 규정] 제22조의 규정에 따라 방송통신설비의 안전성 및 신뢰성 등에 관한 기준 충족 필수

나 디바이스 도입기준

○ (디바이스 역할) 정부사물인터넷 서비스에서 내장 센서를 통한 데이터 수집과 필요에 따라 제어장치를 통한 제어가 실제로 이루어지는 구성요소

※ 디바이스 형태는 ❶ 센서와 통신모듈 둘 다 내장한 형태와, ❷ 센서만 내장하고 데이터 전송을 위해 별도의 통신모듈을 외부에서 연결하는 형태, ❸ 좀 더 많은 서비스 기능을 부여하기 위해 "①·②"의 형태에서 GPS·Gyro센서와 근거리무선통신 모듈까지 포함하는 다기능 형태가 있음

○ (H/W 고려요소) 외부 인터페이스, 동작 및 보관 온·습도, 주파수 인증, 주파수 범위, 하향링크 및 재전송채널, 채널당 주파수 대역폭, 배터리 수명, 무선 출력, 송신전 신호감지, 운영채널 설정 기능, 최소 성능 요구사항, 안테나 이득, 소비전력, 배터리 잔량 체크 등

○ (S/W 지원요소) 저전력 동작, 디바이스 클래스(A·B·C), 재전송, 배터리 잔량 전송 등

다 게이트웨이 도입기준

○ (게이트웨이 기능) 디바이스와는 해당 사물인터넷 표준 무선통신방식으로 데이터를 송·수신하고, 네트워크서버와는 TCP/IP 방식으로 송·수신

○ (H/W 고려요소) 디바이스의 고려사항에 더하여 형상(함체 등), 냉각방식, 실시간 분석, 파라미터 설정, 마운트 형식, 접지, 방진·방수 규정, 진동기준, 염수 환경 기준, 송신출력, 유·무선 백홀 연동 및 이중화, IP주소할당, Reset 기능 등을 고려

○ (S/W 지원요소) 네트워크서버 연동, 접근제어, 장비상태·트래픽·구성 정보수집 등

2 네트워크 도입기준

가 디바이스 네트워크 구성모델

○ 디바이스와 게이트웨이간의 사물통신망은 자체망 또는 통신사의 망을 활용한 6가지 유형의 모델이 있으며 이중 유리한 방식으로 구축가능

≪표3-1 : 정부사물인터넷 디바이스 네트워크 구성모델≫

구성 모델		행정기관 구축운영 여부				비고
번호	모델명	Dev	GW	NS	AS	
모델1	자체 LPWA망 활용	O	O	O	O	자체 LoRa망 구축 및 운영
모델2	통신사 IoT서비스 활용	O	×	×	O	IoT망과 IoT플랫폼을 상용서비스 활용
모델3	통신사 IoT망 활용	O	×	O	O	LoRa, NB-IoT, LTE-M 등
모델4	Sigfox 사물인터넷망 활용	O	×	×	O	Sigfox 서비스 활용
모델5	근거리 사물인터넷망 활용	O	O	O	O	BLE, ZigBee/Z-Wave 방식
모델6	WiFi 통신방식 활용	O	O	O	O	무선 AP를 활용한 WiFi 방식

※ <범례> Dev: 디바이스, GW: 게이트웨이, NS: 네트워크서버, AS: 애플리케이션서버

나 디바이스 네트워크 자체망 구축기준

○ (구축요건) 행정기관의 자체망은 서비스 수요(예상수요 포함)가 많거나, 다른 서비스와 공동활용 등 경제성*·타당성**을 확보할 수 있을 경우 구축 고려

* 자체 인프라가 있거나, 관련 기반시설이 많을수록 경제성 확보에 유리

** 상용망이 없거나, 상용망 이용이 어려울 경우 자체망 구축 타당성이 증가

○ (설계 고려사항) △서비스 수요(확정된 수요와 향후 확대예정 수요), △서비스 형태(고정형·이동형), △전송 특성(데이터 특성, 전송 요구속도 등), △지역특성 등 구축환경, △보유 인프라 등 경제성, △적기공급 등 실현성 고려

다 게이트웨이 백홀 네트워크 구축기준

○ 백홀 회선은 게이트웨이(기지국) 설치 위치 및 환경에 맞추어 유선 또는 무선 방식으로 구성하고, 회선은 보안성* 및 가용성(이중화 등) 확보

* 통신사업자의 상용 유·무선 회선을 백홀로 이용하는 경우 해당 사업자로 하여금 서비스 제공 구간에 대한 보안성을 강구하도록 하고, 별도 보안성 검토 필요

○ 백홀 구성시 구축되는 스위치, 라우터 등 네트워크 장비는 적정용량*의 장비로 구성

* TTA『네트워크 구축을 위한 장비 규모산정 지침(TTAK.KO-01-0103)』참조하여 행정기관 환경에 맞도록 조정(customizing) 적용

3 서비스 플랫폼 도입기준

가 플랫폼의 주요역할

○ 사물(사람·물건·기기·데이터 등)간 통신 및 상호작용을 위해 아래의 역할을 수행하는 시스템으로 하드웨어와 소프트웨어, 네트워크를 포함

- (보안 및 인증) 사용자 인증 및 권한관리, 디바이스 및 시스템 보안관리(Key 등)
- (리소스 및 서비스 관리) 서비스 및 리소스 관리, 디바이스 장치 관리 등
- (연결 및 네트워크 관리) 디바이스 프로토콜 게이트웨이, 네트워크 연결관리 등
- (데이터 처리) 수집 데이터의 파싱·가공 및 저장·분석, 결과 처리 등

나 플랫폼 도입기준

○ (공통 사항) 디바이스 장애나 게이트웨이의 장애는 피해범위가 제한적이지만, 서버 장애는 서비스 전체에 문제가 되므로 고가용성 구성(장치·네트워크·전원 이중화 등)하고

- 서버들을 구성하는 시스템은 CPU·RAM 등 H/W 성능은 서비스가 원활하게 제공될 수 있도록 적정하게 확보하여야 하며(“제4장 5절 시스템 용량 산정기준” 참조)
- 서비스 제공을 위한 애플리케이션들의 S/W의 규격은 상호연동성·확장성을 위해 OneM2M·OCF 등 사물인터넷 개방형 표준 준수 필요

○ (네트워크서버) 여러 게이트웨이에서 전송되어 오는 △디바이스의 중복 메시지* 제거와 △메시지에 응답해야 할 게이트웨이 결정, △데이터 전송률 관리 등으로 네트워크 용량 최대화를 도모하며, △디바이스 배터리 수명을 연장하는 등 사물인터넷 네트워킹 전반을 관장하는 역할을 수행하므로

- 네트워크 및 트래픽 제어, 패킷 버퍼링, 디바이스 주소 할당 등이 주요 고려사항

* LoRa 디바이스는 연결가능한 모든 게이트웨이로 데이터를 전송하므로 네트워크서버에 중복 메시지 발생

○ (관리서버) 서비스에 문제가 없도록 IoT디바이스 및 관련 시스템을 관리하며,

- 관제 및 운영을 위한 연동, 로그 수집·검증·저장·분석을 통한 장애 및 성능 감시, 등록된 디바이스에 대한 상태와 실시간으로 추적하여 문제 발견 및 조치에 관한 기능들이 도입 시 고려해야 할 사항

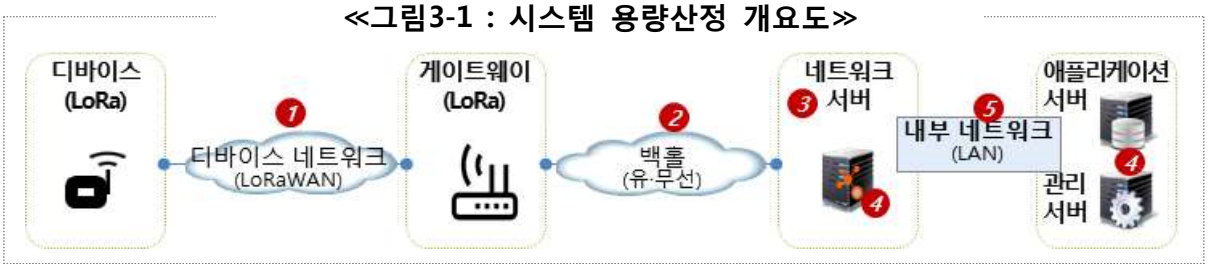
○ (애플리케이션서버) 정부사물인터넷 서비스의 목표 서비스 제공과 관련한 애플리케이션에 대한 개발·배포·업데이트 환경을 제공

4 시스템 용량 산정기준

가 시스템 용량산정 개요

○ 원활한 정부사물인터넷 서비스 제공을 위해 네트워크 및 서버 하드웨어 등 시스템을 구성하는 주요 요소에 대한 적정한 용량 확보 필요

≪그림3-1 : 시스템 용량산정 개요도≫



나 구성별 용량산정 주요요소

❶ (디바이스 네트워크) △디바이스의 단위 전송 데이터크기와 빈도수, △디바이스 수량 등 전송량으로 사물인터넷 디바이스 네트워크 용량 산출

❷ (백홀 통신회선) 백홀회선 대역폭[bps]은 △신설시 전송량[Byte]× 8[bit] ÷ 전송시간[sec], △기존 운영시 트래픽 이용량·이용률을 측정하여 산정

※ 각 게이트웨이에서 네트워크서버로 전송하는 백홀회선의 적정 대역폭이 확보되지 않으면 병목현상에 따른 전송지연·데이터유실 등으로 서비스 품질이 나빠지게 됨

❸ (네트워크서버) △서비스의 트래픽 특성, △서비스 관련 서버와의 연동구조, △디바이스 동시 연결 게이트웨이 수, △초당 전송 요청수 등의 조건을 고려

※ 네트워크서버는 디바이스와의 전송 동작방식(Class A·B·C 3종)에 따른 전송제어, 디바이스에서 전송하는 데이터의 처리 등 LoRa 자체망 구축에서 성능에 대한 이슈가 가장 중요한 노드

❹ (서버 하드웨어) △CPU*, △메모리**, △디스크*** 등의 용량이 주요 성능요소

* 해당 서비스 처리를 위한 CPU규모 산정(tpmC단위) 후, 적정한 성능을 지닌 서버기종 선정

** 서버 구성방안에 의거하여, 서버별 시스템 S/W 및 응용 프로그램 등의 메모리 사용량으로 산정

*** CPU 규모산정에 따른 서버 구성방안에 의거하여, 서버별 OS, 시스템 S/W, DB의 데이터, DB의 아카이브(Archive) 및 백업 영역 등의 디스크 사용량을 산정

❺ (네트워크 장비) 서버 간 부하분산 및 연동 등을 위한 L2/L3/L4스위치*, 방화벽** 등 네트워크 구성장치도 병목점이 될 수 있으므로 처리성능에 대한 고려가 필요

* 포트 수량, 트래픽 처리량, 스위칭 용량 등 고려 ** TCP 처리량, 동시 세션수 등 고려

제4절 정부사물인터넷 네트워크 구축기준

1 구축 고려사항

가 서비스 도입 고려사항

○ 제공하고자 하는 서비스의 특성에 따라 적합한 디바이스·네트워크 등 인프라 요구가 달라지므로 서비스 특성에 따른 고려사항을 우선 분석

≪표4-1 : 제공 서비스 특성 및 고려사항 분석 예시≫

구분	데이터특성	서비스예시	접속기술	주요 고려사항
미션 크리티컬 서비스	• 반드시 무중단 서비스 • 많은 데이터양 • 높은 실시간성 • 모니터링 + 제어 • 높은 네트워크 안정성 • QoS 보장 • 높은 보안성	• 커넥티드 카 • 자율주행 차 • 커넥티드 CCTV	LTE·3G 등	<어떠한 경우에도 통신이 가능해야 함> • 망 안정성·신뢰성 확보 • 데이터의 실시간 전송 • 실시간 제어 가능 여부
대량형 서비스	• 전송 데이터양 많음 • 실시간 모니터링 • QoS 보장 • 빠른 데이터 전송 속도	• 공장 자동화 • 차량 공유 서비스 • 스마트 교통 시스템 • 재난 방송 • 전자결재	LTE-M Cat1	• 대역폭(전송속도) 보장 • 데이터의 준 실시간 전송 (낮은 전송지연)
소물형 서비스	• 전송 데이터양 적음 242 byte이하 • 비실시간성 • 변화적은 데이터 • 다량 데이터 수집	• 물자관리 • 보안등·가로등 제어 • 미아치매노인 위치관제 • 원격검침(수도·가스 등) • 지하시설물 관제	LoRa, NB-IoT 등	• 배터리 수명 (5~10년 보장) • 저전력·장거리 통신 • 전파방해 요소 해소 (음영지역 등)

나 네트워크 구축 고려사항

≪표4-2 : 네트워크 구축 고려사항≫

디바이스 네트워크	게이트웨이 백홀 및 백엔드 네트워크	공통 고려사항
• 서비스 특성 및 접속기술 (미션크리티컬·대용량·소물통신 등) • 주파수 면허·비면허 대역 여부 • 커버리지 영역 및 전파통신 환경 • 디바이스 저전력 요구(전원형태) 여부	• 투자비 재원확보 용이성 • 운영인력 확보 용이성 • 구성방법 및 보안 요구수준 • 연동 커버리지 요구 수준 • 수요 등 서비스 확장·확대 여부	• 서비스 보안 • 연동 및 호환성·상호운용성 규격 • 구축·운영 사업자 선정 • 무선주파수 구성

다 디바이스 식별 및 네트워크 연동 고려사항

○ (디바이스 식별) 객체 식별자(OID) 기반으로 정부사물인터넷 디바이스 식별

※ 식별체계 : 상위노드(인터넷진흥원 관리) + 제조사 식별노드(전자부품연구원 관리) + 제품모델 식별노드 (해당기관 관리, 지역번호·서비스번호) + 일련번호 식별노드(해당기관 관리, 시리얼번호)

○ (네트워크 연동) 국제표준·개방형표준, 통신사표준(상용망) 등으로 연동

※ 자체LoRa예시 : 디바이스↔네트워크서버 간 LoRaWAN1.1, 네트워크서버↔애플리케이션서버 간 OneM2M Rel.1 연동

2 네트워크 구축 절차

가 단계별 주요내용

≪표4-3 : 네트워크 구축 단계별 주요내용≫

분석 및 기본설계 ≫	설치현장 실사 ≫	상세설계 및 구축 ≫	검수 ≫	최적화
• 서비스 및 지역 특성 분석 • 디바이스 수량 및 데이터 특성 기반 설계 • 백홀 망 사용여부	• 출입 등 구축환경 확인 • 설치 가능여부 확인 • 전원·백홀 포설가능 확인 • 전파방해 요소 확인	• 기본설계 보완 상세설계 • 발주 및 계약 • 안전관리요원 배치 • 네트워크 구축 및 감리	• 지정상면에 설치여부 • 설계도 준수여부 • 정보통신공사 기준 및 설치가이드 준수여부 등	• 기지국 최적화 • 무선환경 최적화 • 시스템 최적화

나 무선망 기본설계

○ 서비스 및 데이터 특성*을 고려하여 데이터 전송특성 및 커버리지 분석

* △서비스 적용범위, △서비스 형태(고정형·이동형, 서비스타입 등), △데이터 량, △데이터 전송주기 등

○ 전송특성·커버리지 분석결과를 근거로 커버리지 맵(기본 셀 설계*)을 구성

* 셀 설계 고려사항 : △서비스 범위 내 기지국 존재여부, △중첩 셀 존재 여부, △중복 채널 존재 여부 등

다 현장실사 및 상세설계

○ 게이트웨이 설치 예정 기지국을 방문하여 현장 실사*

* 실사 고려사항 : △게이트웨이 상면확보 유무, △전원 공급 가능 여부, △백홀 연결 가능 여부, △무선 백홀 사용시 수신 감도, △빌딩, 기타 구조물, 산, 강, 바다, 호수 등에 의한 전파 방해요소 존재여부, △건물주 및 토지주와의 협의요건 (공간사용료, 접근 가능 시간대등) 및 설치허가 여부 등

○ 실사결과를 반영하여 각 노드(기지국 등)별 필요한 장비 및 부자재를 확정*

* 상세설계 고려사항 : △유선망 백홀 이용 시 백홀 케이블 길이, △전력선 포설 길이, △기타 필요 부자재 (커넥터, 브래킷, 백업용 전원장치), △태양광 발전설비 사용 필요시 설치 반영 등

라 무선망 구축 및 검수

○ 무선망 구축규모가 크거나, 불확실성이 내제된 경우는 시범구축 후 확대 구축 등 다단계로 구축을 추진할 경우 무선망 완성도를 더 높일 수 있음

○ 구축 전·중간·후 감리 및 검수*를 시행하여 무선망 구축 적합성을 검증

* 검수 고려사항 : △정보통신공사 설계기준의 준수여부, △명시된 설치 지정장소 등 설계서 준수여부, △시방서 등 설치 가이드라인 준수여부, △주물자, 부자재, 부가장비 등의 설치현황과 설치완료 보고서와의 정합성 등

마 무선망 최적화

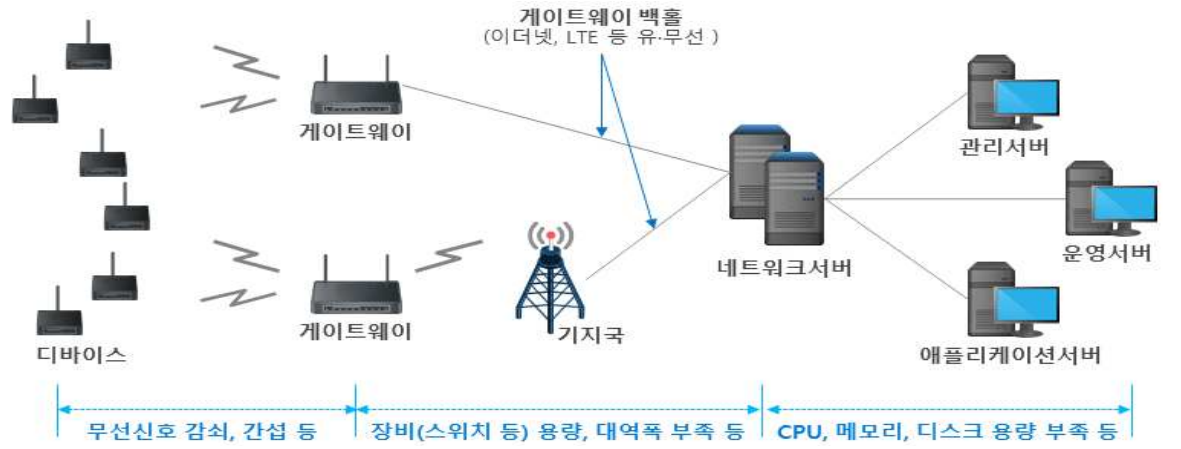
○ 설치완료 후 실제 무선망 설계에서 제시한 커버리지, 전파 수신감도 등을 측정하여 음영지역 파악·개선 등 무선망을 최적의 상태로 구성

3 품질 관리

가 서비스 품질저하 요소

○ 사물인터넷 서비스 품질저하는 무선신호 감쇠 및 간섭 등에 의한 무선통신 품질저하, 게이트웨이 백홀 대역폭 부족에 따른 병목현상, 플랫폼을 구성하는 서버 및 네트워크 용량부족 등으로 인하여 발생

≪그림4-1 : 사물인터넷 서비스 품질저하 요소≫



나 서비스 품질확보 방안

○ (무선통신 품질) 전파인증 제품을 사용하고, 무선환경 최적화* 주기적 시행

* 기지국별 출력 및 파라미터 확인 및 조정, 게이트웨이 안테나 조정 및 설치위치 변경, 인접 셀 간 커버리지 조정, 디바이스 밀집도 분석 및 데이터 전송 주기 조정 등

○ (백홀・백엔드 품질) 유・무선 통신회선 대역폭, 네트워크 장비 용량 및 성능 등의 주기적* 품질측정과 증설 등 품질저하 구간에 대한 개선 이행

* 연 1회 이상 또는 서비스 품질저하가 발생한 경우 유·무선 통신회선 트래픽 이용량 및 네트워크 구성장비의 포트·CPU·메모리 이용률 측정 및 분석을 통하여 문제구간 개선

- 트래픽 이용량은 업무시간 내 최근 3개월간의 최번시평균 이용량을 기준으로 대역폭 조정

○ (플랫폼 품질) 플랫폼을 구성하는 서버 및 네트워크 장비 성능측정* 및 개선

* 성능지표 : 시스템 응답시간(response time) 및 시간당 처리량(throughput), CPU·메모리·디스크 등 시스템자원 사용량(utilization), 효율성(efficiency = 시간당 처리량 ÷ 자원 사용량)

<참조지침> ※ **관련지침이나 가이드라인은 최신 버전을 확인한 후 참조**
(통신회선) "행정기관 통신회선 대역폭 관리 가이드라인, 행정안전부"
(서버·시스템) "정보시스템 성능관리 지침(TTAK.KO-10.0292), TTA"
(네트워크장비) "네트워크 구축을 위한 장비 규모산정 지침(TTAK.KO-01-0103), TTA"

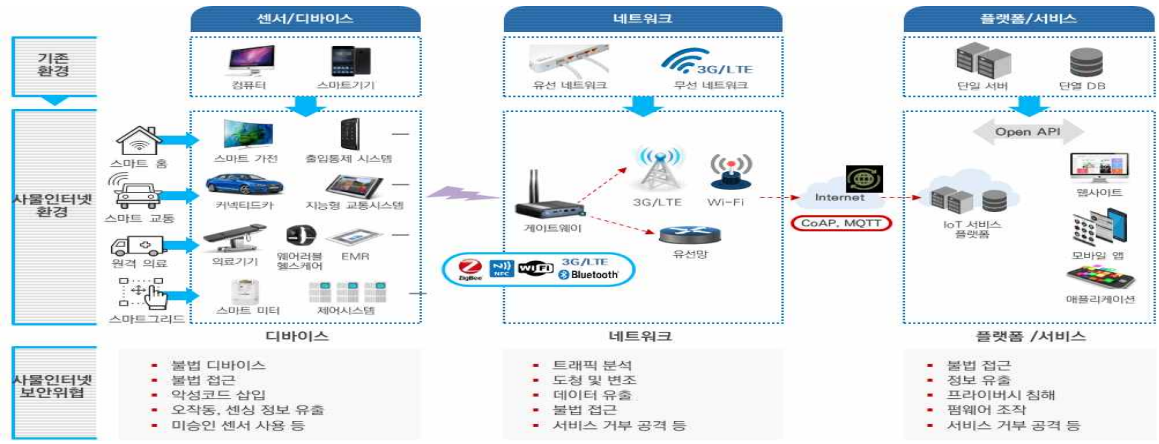
제5절 정부사물인터넷 보안

1 사물인터넷 보안

가 사물인터넷 보안위협

○ 차량, 홈·가전, 헬스케어 등 사물인터넷 서비스를 구성하고 있는 디바이스 및 관련 시스템의 오작동이나 불법조작이 발생하게 되면, 이용자의 신체나 생명, 재산에까지 피해가 발생할 수 있고, 피해범위도 사회 전반에 파급 가능

≪그림5-1 : 사물인터넷 환경에서의 보안위협≫



나 보안 요구사항

○ 사물인터넷은 이종 장치들과 유·무선 네트워크 기술, 그리고 지능화 플랫폼을 기반으로 제공되므로 구성요소 및 서비스는 설계부터 운영·폐기까지 모든 단계 별 보안 취약점 및 요구사항을 점검하여 보안대책 내재화 필요

※ 국가정보원의 "국가공공기관 사물인터넷(IoT) 보안 가이드라인" 준수

≪표5-1 : 사물인터넷 공통보안가이드라인 (자료출처: IoT보안얼라이언스)**≫**

단계	보안 원칙
설계	**(보안원칙1) 정보보호와 프라이버시 강화를 고려한 IoT 제품·서비스 설계** ① IoT 장치의 특성을 고려하여 보안 서비스의 경량화 구현, ② IoT 서비스 운영 환경에 적합한 접근권한 관리 및 인증, 종단간 통신 보안, 데이터 암호화 등의 방안 제공, ③ 소프트웨어 보안기술과 하드웨어 보안 기술의 적용 검토 및 안전성이 검증된 보안 기술 활용, ④ 민감 정보 보호를 위해 암호화, 비식별화, 접근 관리 등의 방안 제공, ⑤ 민감 정보 수집목적 및 이용방법 등에 대한 운영정책 가시화를 통해 투명성 보장
개발	**(보안원칙2) 안전한 소프트웨어 및 하드웨어 개발 기술 적용 및 검증** ⑥ 보안 취약점 사전 예방을 위해 시큐어 코딩 적용, ⑦ 다양한 S/W에 대해 보안 취약점 점검 수행 및 보안패치 방안 구현, ⑧ 다양한 하드웨어 보안 기법 적용
배포 설치 구성	**(보안원칙3) 안전한 초기 보안설정 방안 제공** ⑨ IoT 제품·서비스 설치 시 Secure by Default 원칙에 따라 파라미터 설정 **(보안원칙4) 안전한 설치를 위한 보안 프로토콜 준수 및 안전한 파라미터 설정** ⑩ 안전성을 보장하는 보안 프로토콜 적용 및 보안 서비스 제공 시 안전한 파라미터 설정
운영	**(보안원칙5) IoT 제품·서비스의 취약점 보안패치 및 업데이트 지속 이행** ⑪ IoT 제품·서비스의 보안취약점 분석 및 보안패치 이행, ⑫ IoT 제품·서비스 보안 취약점 및 조치사항에 대해 공지
관리	**(보안원칙6) 안전한 운영·관리를 위한 정보보호 및 프라이버시 관리체계 마련** ⑬ 개인정보보호정책 수립 및 기술적·관리적 보호조치 마련
폐기	**(보안원칙7) IoT 침해사고 대응체계 및 책임추적성 확보 방안 마련** ⑭ 보안 침해사고에 대비하여 침입탐지 및 모니터링 수행, ⑮ 침해사고 발생 원인분석 및 책임 추적성 확보를 위해 로그기록 저장·관리

2 디바이스 및 디바이스 보안

가 디바이스 관련 보안 위협

≪표5-2 : 사물인터넷 디바이스 관련 보안 위협≫

보안위협	보안취약점
간섭·Jamming·충돌	노이즈 발생, 동시 동일 주파수 접속(혼선), 주파수 위변조 등을 통해 실제 신호의 정상적인 송수신을 방해하는 공격
Sybil 공격	사물인터넷 디바이스 네트워크에서 다중식별이 허용되는 취약점을 이용한 공격으로, 각 디바이스나 센서에 Unique ID를 부여하지 않을 경우 발생
트래픽 분석	암호화되지 않은 패킷 또는 프레임의 페이로드를 분석하여 정보를 취하는 공격 (암호화 할 경우 상대적으로 안전하지만, System Performance에 영향이 갈 수 있음)
서비스 거부	주변 노드에 지속적인 광고 패킷을 송신, 프레임 반복 수정, CRC 반복 체크로 시스템에 무리를 주거나 주파수 Jamming 등으로 신호 송수신을 방해하는 공격
동기화 해제	Device Pool에 잘못된 시간 정보를 송신하여 디바이스가 계속적으로 시간을 교정하는데 자원을 소모하도록 하는 공격
Wormhole	상호통신이 허가되지 않은 두 디바이스의 무선통신 모듈을 공격해 상호간 통신을 가능하게 조작하여 통신경로 고의 변경 또는 악성코드 배포경로로 이용하는 공격
위변조(Tampering)	단말에 저장된 데이터 혹은 송수신 데이터를 임으로 위조 및 변조하는 공격
도청(Eavesdropping	암호화되지 않은 디바이스(센서)와 게이트웨이 구간 정보를 도청하는 공격
선택적 포워딩(Selective Forwarding) **공격**	선택적으로 특정 노드에 패킷을 포워딩하지 않게 하여 해당 노드를 블랙홀로 만들어 버리는 공격
Spoofing	네트워크에 공유된 Key를 취득하여 허가되지 않는 위조된 디바이스(센서)를 네트워크에 접속시켜 악의적인 행위를 하도록 하는 공격

나 보안 요구사항

≪표5-3 : 사물인터넷 디바이스 관련 보안 요구사항≫

요구사항	요구내용
기밀성 (Confidentiality)	• 디바이스 간 전송되는 메시지는 불법적인 sniffing 또는 도청 방지를 위해 암호화된 형태로 메시지 전송 • 디바이스에서는 정보유출 방지를 위해 개인정보 및 암호키와 같은 중요 데이터를 암호화하여 안전하게 처리 및 저장 관리 • 기기 복제 방지를 위해 디바이스의 고유 식별정보가 외부로 유출되거나 변경되지 않도록 안전하게 처리 및 관리
무결성 (Integrity)	• 데이터 위변조 방지를 위해 디바이스에 데이터 무결성 검증 기능을 제공
가용성 (Availability)	• 물리적 제거·파괴 및 비정상적인 설치시도 등의 위협예방을 위해 디바이스에서 주기적인 Keep Alive 메시지 전송 또는 기기 상태 정보 전송 기능을 제공 • 디바이스에서 안전한 소프트웨어 업데이트 및 보안 패치 기능을 제공 • 디바이스에서 소프트웨어 오류나 악성코드 감염에 의한 오동작 시에도 해당 모듈 분리 및 제거, 접근권한 제한 등의 기능을 통해 소프트웨어 안전성을 보장
인증/허가 (Authentication/ Authorization)	• 안전하고 자율적인 통신 환경 구축을 위해 디바이스에서 기기 간 상호인증 기능을 제공 • 정보유출 방지 및 프라이버시 보호를 위해 디바이스에서 Ownership 제어와 같은 권한제어 및 설정 기능을 제공 • 불법적인 사용자 및 기기의 접근을 차단하는 접근제어 기능을 디바이스에서 제공
선택사항	• 별도 UI가 제공(OS 기반)되는 사물인터넷 기기의 경우 비인가 된 사용자의 접근 차단을 위한 사용자 인증 및 불법적인 기기의 접근차단을 위한 기기 인증 기능을 제공하고, 안전하고 강력한 비밀번호 설정 및 주기적인 업데이트 기능 제공

3 게이트웨이·네트워크서버 보안

가 게이트웨이·네트워크서버 보안 위협

≪표5-4 : 게이트웨이·네트워크서버 보안 위협≫

보안위협	보안취약점
사물봇(ThingBot)	광범위한 사물로 구성된 사물봇에 의한 트래픽 폭증 공격
프로토콜 변환 취약점 공격	사물인터넷 기기는 자원의 제약(저전력·소형화, 낮은 연산능력 등)으로 경량 프로토콜을 사용하고, 이를 게이트웨이가 고기능성 프로토콜로 전환하는 과정에서 데이터 기밀성 훼손, 악의적인 위·변조, 보안정책 훼손, 임의의 메시지 주입 등의 보안 위협이 존재
서비스 마비	게이트웨이 프론트홀(디바이스 방향)은 주로 무선을 통해 이루어지므로, 무선 프로토콜의 취약점과 Jamming 등으로 게이트웨이의 통신을 방해하거나 동작을 정지시키는 등 서비스가 불가능하게 하는 위협
악성코드 감염	악성코드 감염으로 사물인터넷 게이트웨이가 좀비화 되어 DDoS 등 공격에 악용될 수 있으며, 감염된 게이트웨이를 통해 사용자 데이터의 유출이 가능하고, 또한 사물인터넷 게이트웨이에 연결된 디바이스를 감염시킴으로써 2차 피해를 유발할 수 있음
데이터 유출	도청, 중간자 공격, 메시지 위·변조 등을 통해 공격자가 개인정보 등 사용자의 민감한 정보를 습득할 수 있음
메시지 불법 동작 제어	재전송 공격, 메시지 위·변조 등을 통해 특정한 동작을 수행하는 메시지를 주입하여 공격자가 게이트웨이의 동작을 악의적으로 제어할 수 있음
웹 인터페이스 취약점	게이트웨이 접근을 위한 웹 인터페이스의 취약점을 활용한 공격(사이트 간 요청위조 등)으로 관리자권한 탈취 등의 피해를 입을 수 있음
물리적 탈취	물리적인 접근을 통해 악의적인 공격자는 게이트웨이의 펌웨어를 임의로 교체하거나 하드웨어 인터페이스 또는 플래쉬 메모리의 물리적인 탈취를 통해 데이터를 획득할 수 있음

나 보안 요구사항

≪표5-5 : 사물인터넷 디바이스 관련 보안 요구사항≫

요구구분	요구내용
필수사항	• 프로토콜 변환 과정에서 데이터 기밀성을 유지하고, 악의적인 위·변조를 방지 • Buffer Overflow 공격 등 임의의 메시지를 주입하여 발생할 수 있는 보안위협에 대응(Secure Coding 준수 등) • 송·수신 데이터는 불법적인 sniffing 또는 도청 방지를 위해 암호화된 형태로 전송 • 프로토콜 취약점을 이용한 공격을 감내(Fault tolerant)할 수 있어야 함 • 프로토콜 변환, 통신방식 변환 등의 과정에서 보안정책이 일관성 있게 적용될 수 있도록 하여야 함 • 방화벽, IDS·IPS와 같은 수단을 통해 네트워크 침입 탐지 및 차단 등 네트워크 트래픽을 제어할 수 있어야 함 • 사물인터넷 네트워크 및 디바이스에 대한 모니터링 기능을 지원하고, 오작동, 악의적인 조작, 트래픽 폭증과 같은 이상 징후를 탐지할 수 있어야 함 • 디바이스의 최초 등록 시, 게이트웨이와의 보안키(Secure Key) 합의, 보안정책 설정과 같은 초기 보안 설정을 지원할 수 있도록 인터페이스를 제공하여야 함 • 서비스 제공 지원을 위한 보안터널링(Secure Tunneling) 기능을 제공해야 함 • 네트워크서버에 등록되는 디바이스는 (초)경량·저전력 기기를 위한 비밀키 설정 등을 대행하는 기능을 제공할 수 있어야 함
선택사항	• 자신에게 연결된 사물인터넷 기기로 구성된 그룹의 생성, 관리 및 그룹 키 관리 기능을 제공할 수 있어야 함

4 서비스 보안

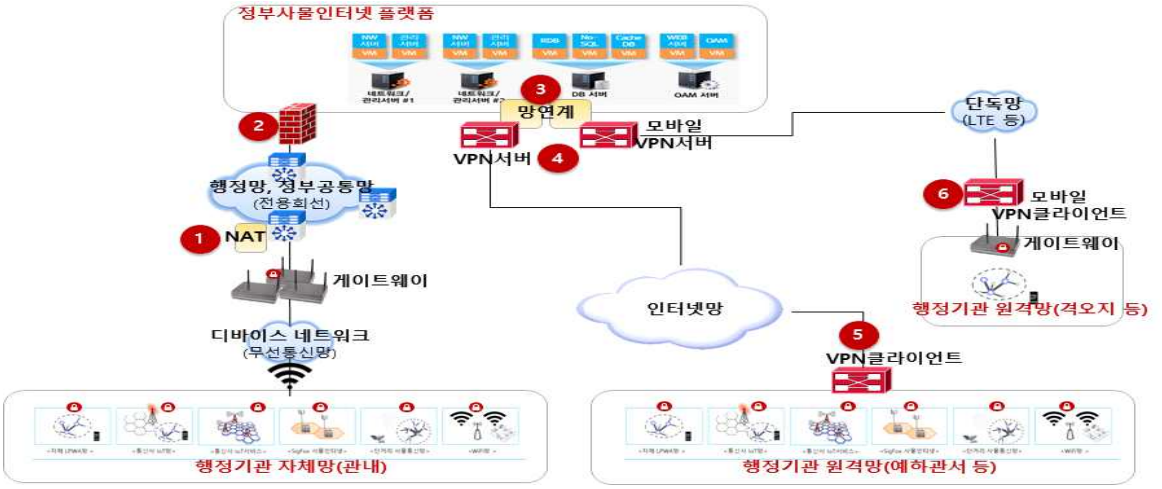
가 전송 데이터 암호화

≪그림5-2 : 정부사물인터넷 구성 구간별 보안적용 개요(LoRa 예시)≫

서비스 구성구간	프로토콜	암호화방식	인증방식	메시지
①디바이스↔네트워크서버	LoRa WAN	AES128·256	Basic(AppEUI, DevEUI, App Key)	-
②네트워크서버↔관리서버	oneM2M	TLS(인증서)·IPSec	OAuth 2.0	Json
③디바이스↔관리서버	oneM2M, OCF	TLS/DTLS(PSK)	OAuth 2.0 또는 Basic(DevID, Token)	Json, XML
	Private	TLS(PSK)·IPSec	-	-
④애플리케이션↔관리서버	Rest API	TLS(인증서)·IPSec	OAuth 2.0	Json, XML

나 서비스 연계·연동구간 보안

≪그림5-3 : 정부사물인터넷 서비스 연계·연동구간 보안구성 사례≫



①플랫폼 접속용 IP주소 변환을 위한 NAT 구성	②플랫폼 서버 및 네트워크 보호를 위한 보안장비 구성
③이기종간 연동을 위한 망연계시스템 구성	④보안이 취약한 인터넷망 연계를 위한 VPN 구성
⑤디바이스↔관리서버	⑥격오지 무선백홀 연계를 위한 모바일VPN 구성

다 개인정보 보호

○ 사물인터넷은 직·간접적으로 개인정보를 담고 있거나, 데이터 분석에 의한 사생활 침해소지가 크므로 관련 법·제도* 및 규정에 따라 개인정보 보호 구현

* 개인정보 보호법, 위치정보법, 정보통신망법, 전기통신사업법, 정보통신진흥특별법 등

제6절 정부사물인터넷망 공통기반

1 공통기반 개요

가 공통기반 구축 목적

○ 로밍 등을 통한 지역한계 극복 및 공통기반을 활용한 빠른 서비스 구현과 타기관·상용서비스 연계·협업을 통한 융·복합 서비스 가능한 기반 제공

나 구성 요소

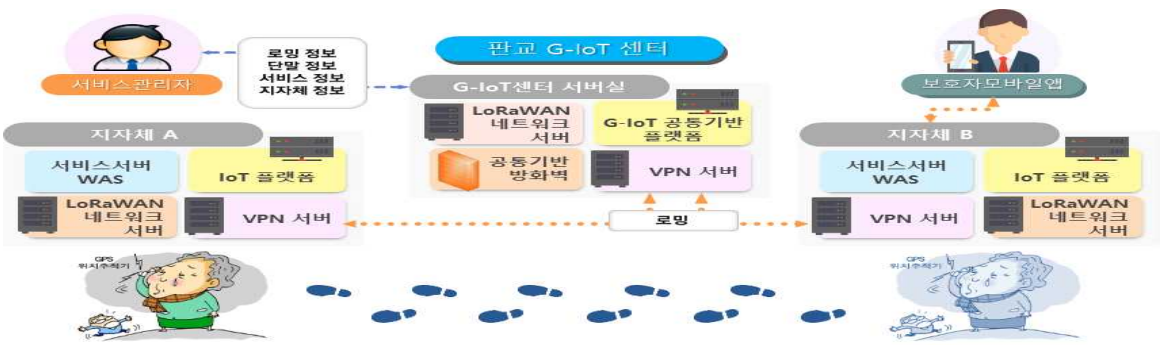
○ ①타기관과 연계 환경, ②연계 디바이스 및 서비스에 대한 운영·관리 환경, ③정부사물인터넷 시험환경, ④상용 망 및 서비스 연계환경 등으로 구성

≪그림6-1 : 정부사물인터넷 공통기반 구성 개념도≫

다 공통기반의 역할

○ 행정기관에서 구축한 다양한 통신표준(LoRaWAN, oneM2M, OCF)을 수용하여 행정기관이 구축한 정부사물인터넷 인프라간 통신중계 역할

≪그림6-2 : 정부사물인터넷 데이터 흐름(통신중계 기능 예시)≫



※ 행정기관에서 서비스하는 이동형 디바이스가 서비스지역을 벗어나서 타 기관으로 이동해도 공통기반의 통신중계 기능을 통해 타지역에서도 서비스를 끊김없이 이용 가능

2 구성요소별 기능

가 네트워크서버 기능

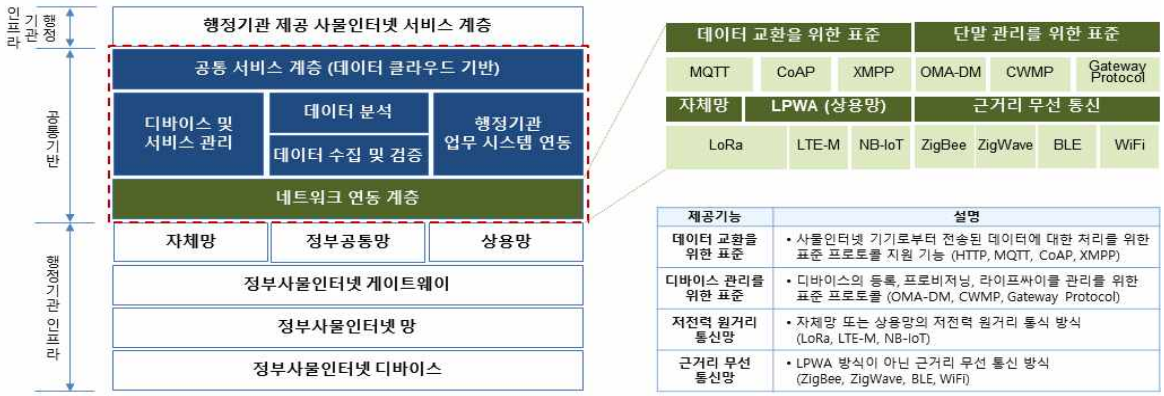
○ 네트워크서버 표준 기능에 행정기관 디바이스 로밍 지원기능을 추가*

* 추가된 기능은 디바이스가 타지역으로 이동하여 해당지역의 네트워크서버가 공통기반 측으로 디바이스 확인을 요청하는 경우, 관리기능에 등록된 디바이스 정보를 확인하여 인증하는 역할

○ 네트워크서버 등 공통기반의 네트워크 연동계층은 이종 디바이스와 연동을 지원*

* LPWA, MQTT, CoAP, HTTP 등의 전송계층 프로토콜에 대한 인터페이스 제공과 변환기능 수행

≪그림6-3 : 정부사물인터넷 공통기반 네트워크 연동계층≫

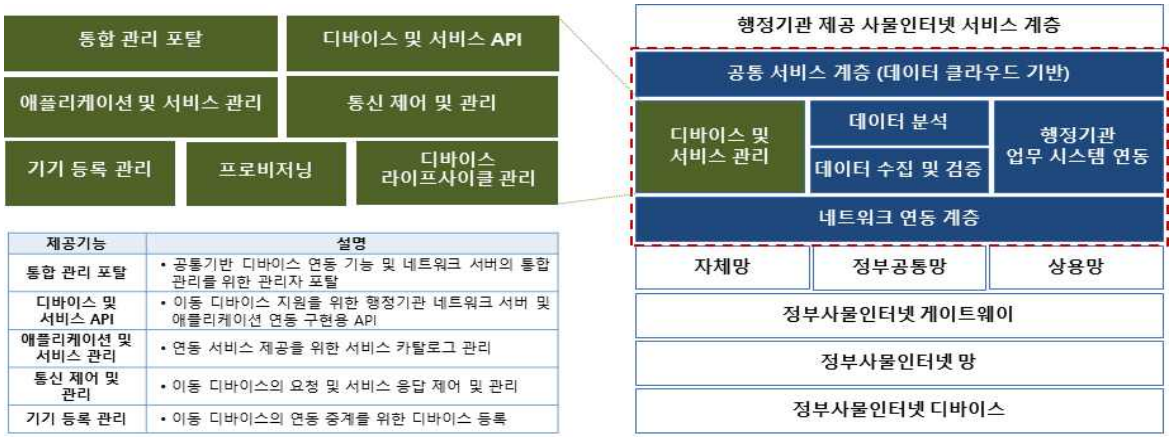


나 디바이스·서비스 관리기능

○ 행정기관 간 디바이스 연계를 지원하기 위하여 해당 디바이스 및 게이트웨이 등록 등 관련 서비스에 대한 정보를 공통기반 관리서버에서 통합 운영

○ 행정기관과 공통기반 간 연동방식에 따라 이동 디바이스의 소속지역 네트워크 서버에 전달하거나, 필요한 서비스 시스템에 전달하는 역할을 담당

≪그림6-4 : 정부사물인터넷 공통기반 디바이스 및 서비스 관리계층≫



3 공통기반 연계 운영관리

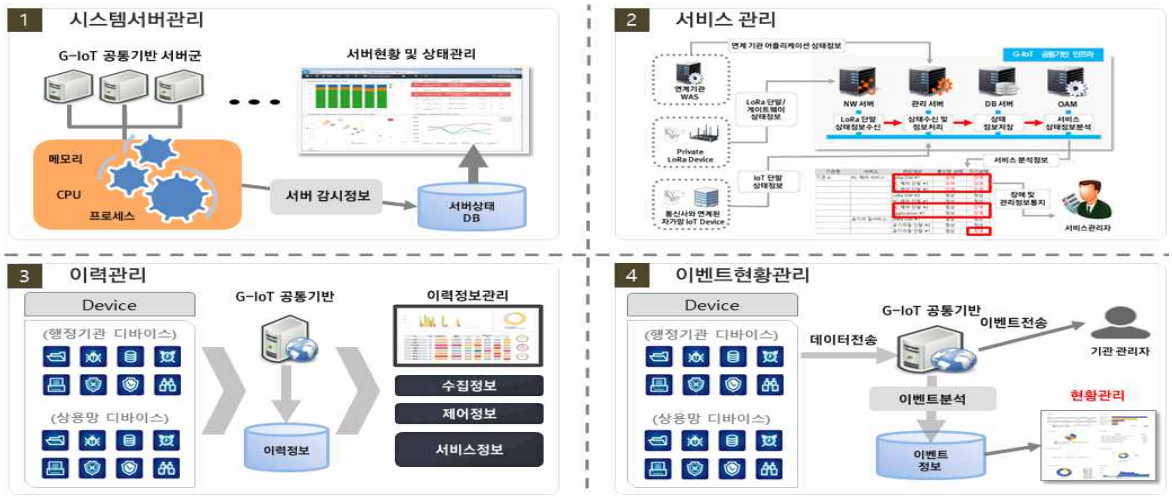
가 연계 운영관리 주요기능

○ 디바이스·시스템·서버 관리* 및 서비스 관리**, 패킷 이력관리, 각종 경고·장애 등 이벤트 발생현황 및 이력관리, 대시보드 및 이용통계 기능제공

* 공통기반과 연계된 서비스를 관리하기 위해 디바이스의 상태, 서버·시스템 상태, 행정기관 애플리케이션의 상태 등의 서비스 정보 모니터링 기능을 공통기반에서 구현

** 서비스 관리를 위해 행정기관 애플리케이션 시스템의 개방형API로 공통기반 관리서버와 연계

≪그림6-5 : 정부사물인터넷 공통기반 연계 운영관리 주요기능≫



나 연계 서비스 구성 및 관리

○ 공통기반의 관리서버·OAM서버 등 운영관리시스템*을 통해 연계 서비스를 구성하여 운영관리

* 로그인 후 권한에 따라 접근메뉴에 차이가 있으며, 다량의 디바이스에 대한 일괄등록 지원

≪그림6-6 : 정부사물인터넷 공통기반 연계 운영관리시스템 메뉴구성≫

제1장

정부사물인터넷 인프라 도입기준

제1절 사물인터넷 개요

1. 사물인터넷(IoT, Internet of Thing) 개념

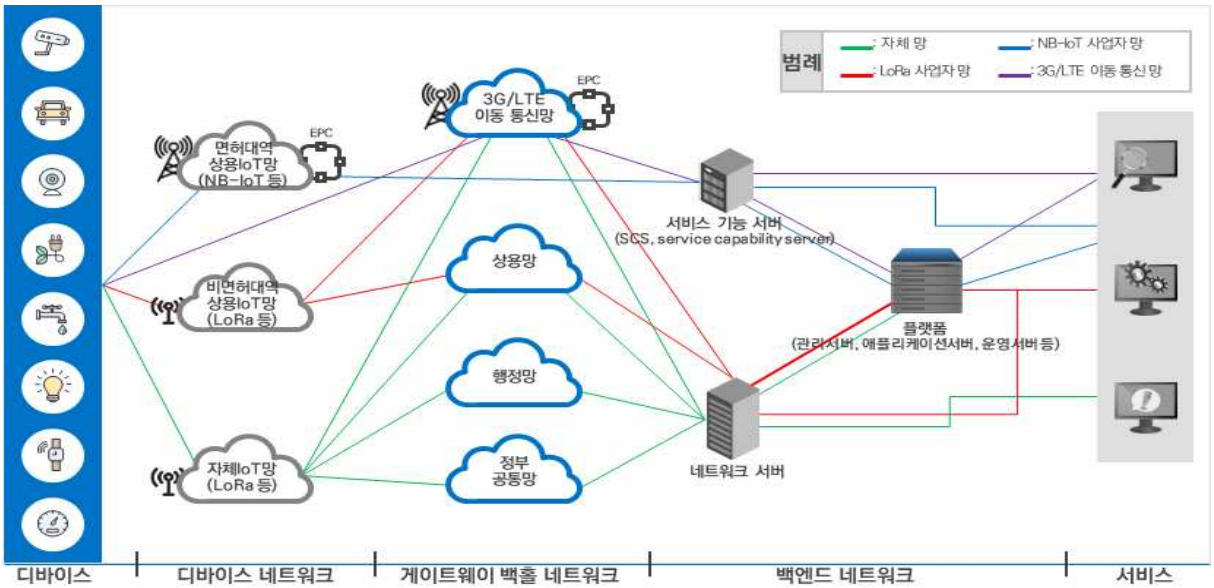
□ 정 의

사물인터넷은 **“정보통신기술 기반으로 모든 사물을 연결해 사람과 사물, 사물과 사물 간에 정보를 교류하고 상호 소통하는 지능형 인프라 및 서비스 기술”** 이다. 다양한 센서를 일상생활 속 사물에 탑재하여 데이터를 수집·공유할 수 있으며, 데이터를 실시간·지능적으로 처리하여 헬스케어, 스마트 에너지, 지능형 교통서비스, 건물·교량 등 사회 인프라 원격관리서비스 등 다양한 서비스를 구현할 수 있다.

□ 구 성

사물인터넷 서비스는 △각종 센서·액추에이터를 내장하여 사물과 지능화·자율적 상호작용을 제공하는 사물인터넷 디바이스, △모든 사물을 유·무선 통신망을 통해 연결하여 상호 소통하게 하는 사물인터넷 네트워크 △물리·가상의 사물과 연계·협업하여 지능형 서비스를 제공하는 사물인터넷 서비스 플랫폼, △이용자의 사생활 보호와 안전한 시스템 운영을 보장하는 사물인터넷 보안으로 구성된다.

< 사물인터넷 인프라 구성모델 >



2. 사물인터넷 구성요소

가. 디바이스

사물인터넷 디바이스는 설치된 주변 환경에서 온도·습도·가스 원격감지, 위치, 모션, 영상 등의 정보를 수집하는 장치로 센서모듈과 통신모듈을 모두 포함한다.

외부의 물리적·화학적 자극에 대해 전기적 신호로 바꾸어 주는 센서와 센서에서 나온 아날로그 신호를 디지털 신호로 바꾸어 주는 신호 프로세스부, 그리고 이들 부품에 전원을 공급해 주는 전원부, 신호 프로세스의 출력 신호를 외부 사용자에게 전달하고 통신을 할 수 있는 통신모듈로 구성되어 있다.

< 사물인터넷 센서 구성 개념도>

나. 게이트웨이

게이트웨이는 디바이스·센서로부터 데이터를 수집하고, 수집된 데이터를 플랫폼 서버로 전달하는 역할을 담당하는 장치이다.

기능	내용
사물간 연결 및 메시지 교환 지원 기능	• 다양한 사물 및 서버 플랫폼간의 통신을 위한 상호 연결지원 및 메시지 라우팅 기능
수집데이터 처리 및 전송 기능	• 응용에 따라 여러 사물로부터 수신한 정보를 합병(merge) 및 가공하여 외부로 전송하는 기능
다양한 네트워크 프로토콜 간 변환기능	• 지그비 등 저전력 센서 네트워크, CoAP, HTTP, 인터넷 등 다양한 프로토콜을 사용하는 사물간 통신을 위한 프로토콜 변환기능
사물 디바이스 관리 기능	• 사물 디바이스와의 연결을 위한 사물 연결 소프트웨어와 연동을 수행하고 연결된 사물 디바이스를 관리하는 기능
리소스 관리 기능	• 사물 디바이스의 프로파일 및 수집된 정보와 게이트웨이 내부의 정보를 관리하는 기능
서버플랫폼 연동 기능	• 사물인터넷 서버 플랫폼과 연동을 통해 정보수집 및 제어서비스를 제공하는 기능
보안 기능	• 사물인터넷 게이트웨이, 사물 디바이스, 사물네트워크에 대한 사이버 공격에 대응하기 위한 보안 기능

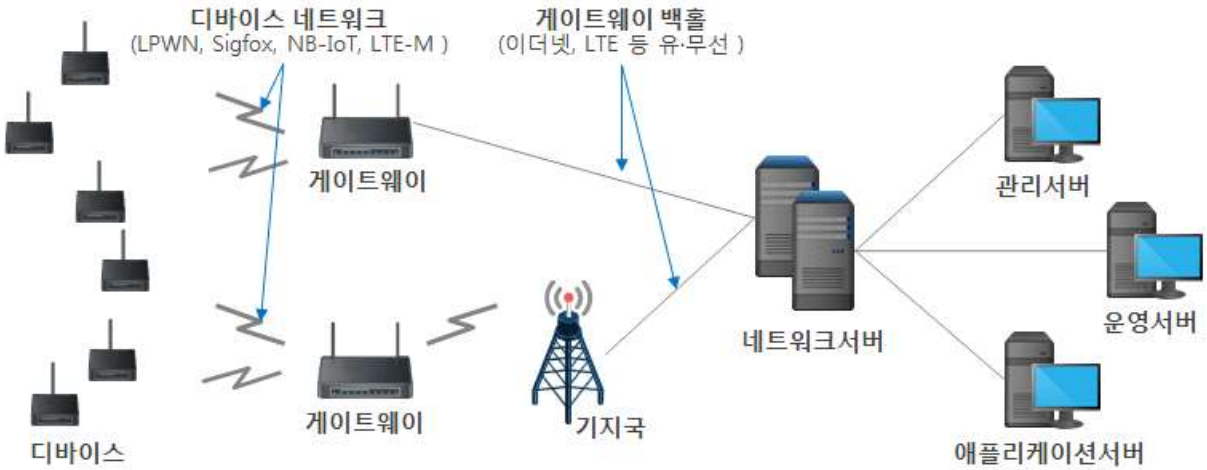
다. 네트워크

사물인터넷의 연결은 유선과 무선 모두 가능하다. 유선망은 주로 게이트웨이 계층 이후의 연결에 적용되고, 무선망은 사물인터넷 디바이스(센서)와 게이트웨이 간 연결을 담당한다.

사물인터넷 디바이스와 센서 및 게이트웨이간 통신망을 디바이스 네트워크라고 하고 통신거리에 따라 근거리 무선통신망과 저전력 광역무선망(LPWAN, low-power wide area network)으로 구분 한다.

게이트웨이와 네트워크서버간 통신망을 백홀 네트워크라고 하며 무선과 유선망으로 구성 된다

< 사물인터넷 네트워크>



라. 서비스 플랫폼

서비스 플랫폼이란 '사물(사람, 물건, 기기, 데이터 등)'을 인터넷을 통해 상호 연결하는 네트워크, 애플리케이션과 같은 소트프웨어, 서버 등 하드웨어 시스템을 포함하며, 사물간의 통신 및 상호작용, 보안·인증, 리소스 및 서비스 관리 등 사물인터넷 서비스 제공의 핵심 역할을 담당한다.

- **(보안 및 인증 기능)** : 사물인터넷 서비스 사용자 인증 및 권한관리, 디바이스 및 시스템 보안관리, Key 관리 등
- **(리소스 및 서비스 관리)** : 서비스 및 리소스 관리, 디바이스 장치 관리 등
- **(연결 및 네트워크 관리)** : 디바이스 프로토콜 게이트웨이, 네트워크 연결관리 기능 등
- **(데이터 분석)** : 수집 데이터 파싱, 가공, 데이터 처리·저장·분석, 연관 분석 등

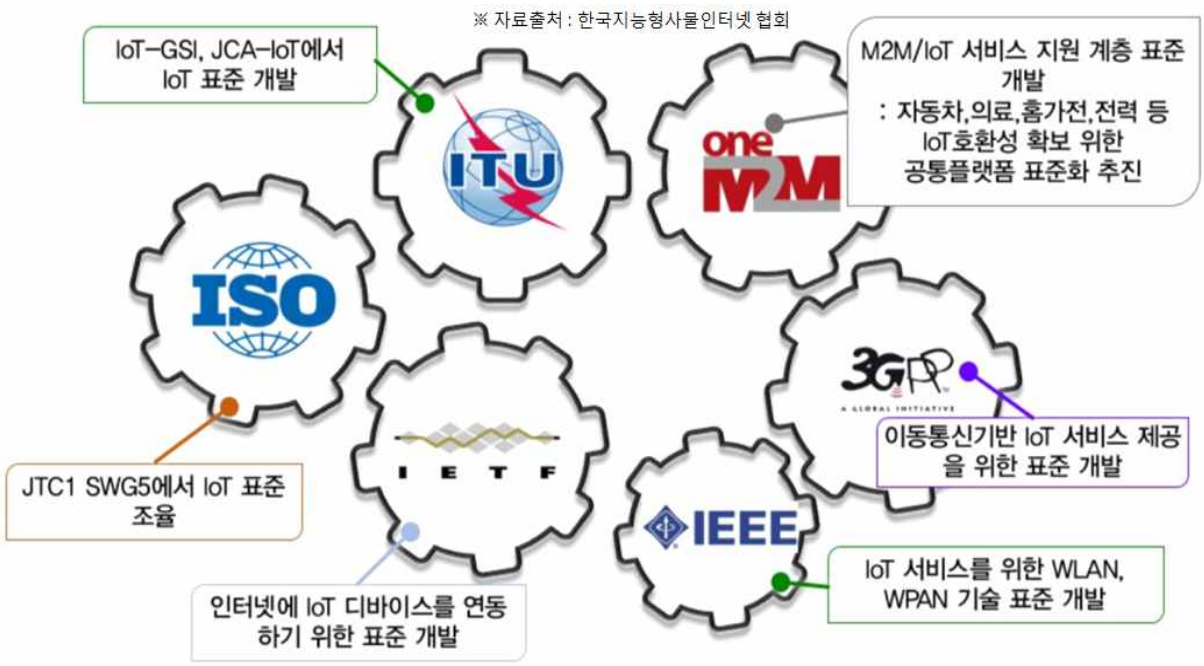
제2절 사물인터넷 표준화 동향

각종 사물을 인터넷에 연결하여 다양한 서비스에 활용할 수 있는 융합 기술인 사물인터넷에 대한 표준화는 서비스의 공통성, 호환성, 통일성을 갖추기 위해 필요하며, 기업·국가·학계 등의 다양한 참여를 통해 연구되고 있다. 사물인터넷 플랫폼 기술 동향을 국제 컨소시움, 국외 업체, 국내 업체에 따라 분류하고 각 플랫폼의 특징 및 동향을 살펴본다. 또한 국제 표준화 단체의 사물인터넷 관련 기술 표준화 동향을 소개한다.

1. 사물인터넷 관련 국제 표준단체 및 활동기준

W3C, ITU-T, oneM2M, IETF 등 다양한 국제 표준 기구는 사물인터넷 관련 기술의 표준을 개발하고 있다. ITU-T에서는 표준모델, ISO에서는 IOT 표준 조율, oneM2M에서는 서비스지원계층 표준 개발, 3GPP는 이동통신기반 IoT서비스 제공을 위한 표준개발, IETF는 인터넷에 IoT디바이스를 연동하기 위한 표준 개발, IEEE에서는 IoT서비스를 위한 WLAN 및 WAPAN기술 표준을 정의하고 있다.

< 표준화 단체 및 주요 활동내용 >



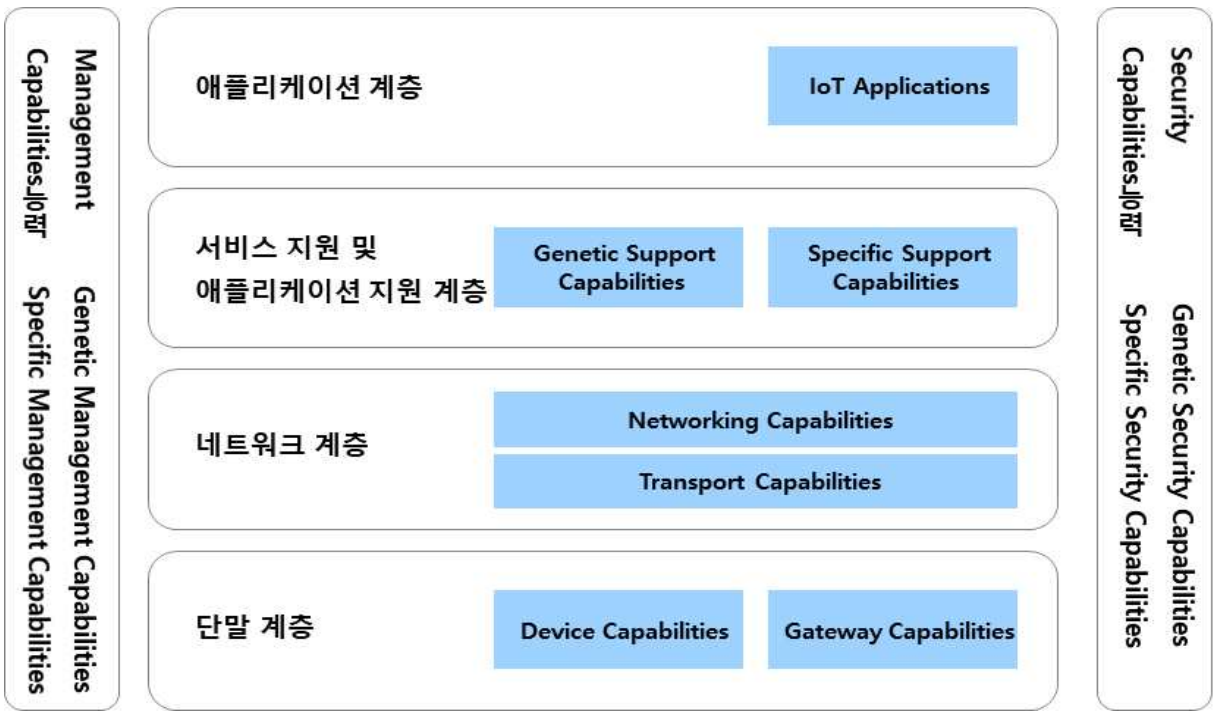
사물인터넷 기술은 다양한 표준 및 개발 기구들에서 표준화되고 연구되며, 유사하지만 서로 다르게 정의되고 있다.

< 국제 표준화 단체 활동기준 >

구분	기준
ITU-T	• 사물인터넷 정의 (ITU-T Content Application Protocol Y.2060)
	• 통신사업자 관점의 IoT 요구사항, 네트워크 기능, 서비스 표준 개발
	• 별도의 IoT-GSI, JCA-IoT 그룹 운영
oneM2M	• 다양한 M2M/IoT 서비스 지원공통서비스 지원 계층 표준 개발
	• Requirement/Architecture/Protocols/Security/Management 표준
3GPP	• MTC(Machie-Type Communication)서비스 지원, 기존의 이동통신 기술을 확장하는 표준 개발
	• 이동통신의 Radio/Network 표준 개발
IEEE	• IEEE 802.x 계열 무선기술을 M2M/IoT 에 적합한 수정 표준 개발
	• 스마트 미터링 등의 서비스에 적합한 IEEE 802.11ah 표준 개발
IETF	• 저전력 무선 기술을 사용 단말을 인터넷에 연동하는 표준 개발
	• 인터넷에 기반 IoT 서비스 지원, CoAP 프로코콜 개발 및 확장
ISO	• IoT 의 개념, 시장의 요구사항 분석 및 IoT 표준화 갭 분석 작업 시작
	• JTC1 SWG5 에서 ISO 내 사물인터넷 표준화 동향과 표준 조율

ITU-T에서 제시하고 있는 ITU 정의 사물인터넷 시스템 목표아키텍처 참조모델은 ITU-T Y.2060 Reference Model에 정의하고 있다.

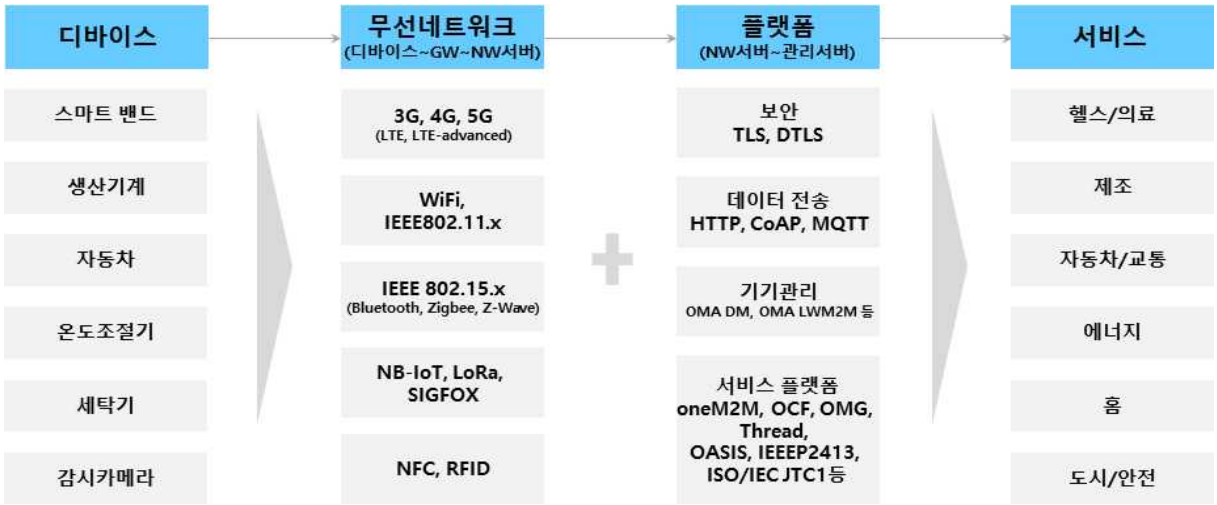
< ITU 정의 사물인터넷 시스템 목표아키텍처 참조모델 >



2. 국내 표준화 진행현황 (한국정보통신기술협회, 2018년 현재)

한국정보통신기술협회(TTA)에서는 사물인터넷 구간별 표준화를 진행하고 있으며, 디바이스, 무선네트워크, 플랫폼, 서비스 등 사물인터넷을 구성하는 각 구간에 대한 표준을 진행하고 있다.

< 사물인터넷 구간별 국내 표준화 진행기준 >



3. OSI 7 Layer별 표준화 동향 (인터페이스, 데이터 포맷, 보안)

네트워크 계위별 표준화 진행내용은 다음과 같다.

< 네트워크 계위별 표준화 진행내용 >

<table>
<tr><th rowspan="2">프로토콜 스택
(OSI 7 Layer)</th><th colspan="3">표준화 동향</th><th rowspan="2">표준 개발 단체</th></tr>
<tr><th>인터페이스</th><th>데이터 포멧</th><th>보안</th></tr>
<tr><td>어플리케이션 계층</td><td rowspan="2">oneM2M
OMA DM, LWM2M
IEEE P2413
OCF</td><td rowspan="2"></td><td rowspan="2"></td><td>oneM2M, OMA, IEEE</td></tr>
<tr><td>서비스 계층</td><td rowspan="3">IETF, OASIS</td></tr>
<tr><td>세션 계층</td><td rowspan="2"></td><td rowspan="2">HTTP, CoAP, MQTT</td><td rowspan="3">DTLS, TLS</td></tr>
<tr><td>전달 계층</td></tr>
<tr><td>네트워크 계층</td><td>6LowPAN</td><td></td></tr>
<tr><td>링크 계층</td><td rowspan="2">3GPP MTC
802.15.4</td><td rowspan="2"></td><td rowspan="2"></td><td rowspan="2">IEEE, 3GPP</td></tr>
<tr><td>물리 계층</td></tr>
</table>

4. 사물인터넷 관련 표준화 목록

< 행정기관 자체망 구축을 위한 표준 규격 목록 >

규격 제정 단체	규격 문서
ITU-T https://www.itu.int	Recommendation ITU-T Y.4500.1 : oneM2M - Functional architecture
	Recommendation ITU-T Y.4500.2 : oneM2M - Requirements
	Recommendation ITU-T Y.4500.4 : oneM2M - Service layer core protocol specification
	Recommendation ITU-T Y.4500.5 : oneM2M - management enablement (OMA)
	Recommendation ITU-T Y.4500.6 : oneM2M management enablement (BBF)
	Recommendation ITU-T Y.4500.8 : oneM2M - CoAP protocol binding
	Recommendation ITU-T Y.4500.9 : oneM2M - HTTP protocol binding
	Recommendation ITU-T Y.4500.10 : oneM2M - MQTT protocol binding
	Recommendation ITU-T Y.4500.11 : oneM2M - Common terminology
	Recommendation ITU-T Y.4500.12 : oneM2M base ontology
	Recommendation ITU-T Y.4500.13 : oneM2M - Interoperability testing
	Recommendation ITU-T Y.4500.14 : oneM2M - LwM2M interworking
	Recommendation ITU-T Y.4500.15 : oneM2M - Testing framework
	Recommendation ITU-T Y.4500.20 : oneM2M - WebSocket protocol binding
	Recommendation ITU-T Y.4500.22 : oneM2M - Field device configuration
	Recommendation ITU-T Y.4500.23 : oneM2M - Home appliances information model and mapping
	Recommendation ITU-T Y.4500.32 : oneM2M - MAF and MEF interface specification
LoRa Alliance https://www.lora-alliance.org	LoRaWAN™ Specification v1.1
	LoRaWAN™ Back-End Interfaces v1.0
	LoRaWAN™ Regional Parameters v1.1rB
OCF https://openconnectivity.org	OCF Bridging Specification v2.0.1
	OCF Cloud Specification v2.0.1
	OCF Core Specification v2.0.1
	OCF Device Specification v2.0.1
	OCF Resource to AllJoyn Interface Mapping v2.0.1
	OCF Resource Type Specification v2.0.1
	OCF Security Specification v2.0.1
	OCF Wi-Fi Easy Setup Specification v2.0.1

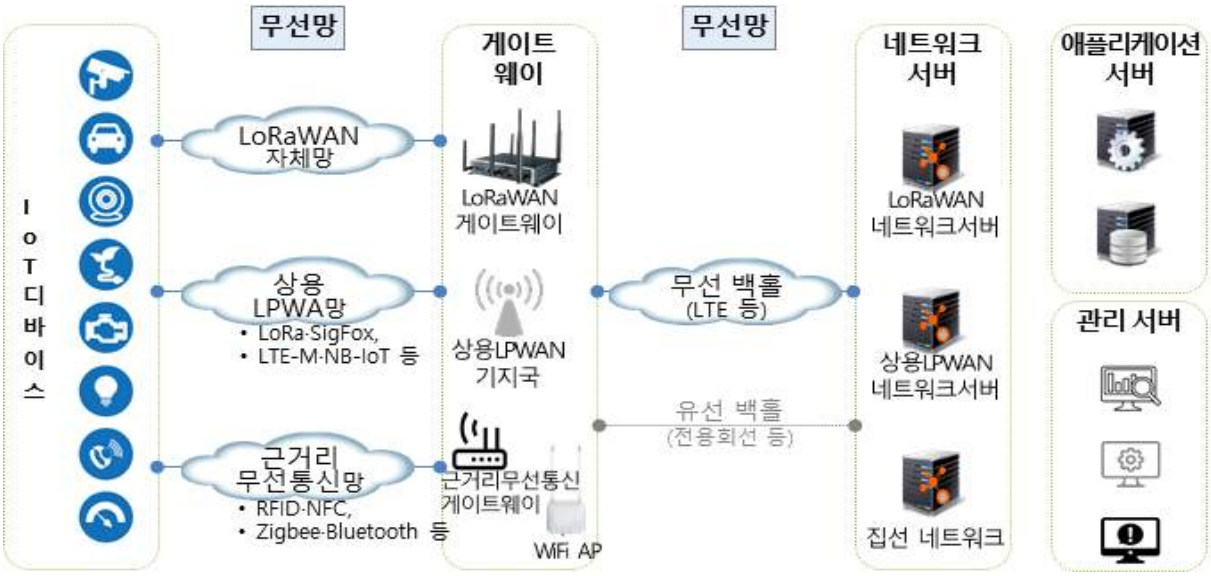
제3절 네트워크 구성기준

1. 무선망 구성

사물인터넷 무선망은 주로 디바이스·센서와 게이트웨이 간의 데이터 전송용으로 주로 구축된다. 게이트웨이와 네트워크 서버 구간에서도 유선망 구축이 어렵거나 유선망 보다 무선망을 구축하는 것이 유리할 경우에도 적용할 수 있다.

무선망은 사물인터넷 서비스 제공내용에 따라 RFID·NFC 기술을 적용한 근접형과 Zigbee·Bluetooth 기술을 적용한 근거리형, 넓은 통신거리를 가지는 LoRa·Sigfox·LTE-M·NB-IoT와 같은 저전력 광역통신망(LPWAN) 기술들을 적용한 광대역형 방식 중 1개 이상을 조합하여 구성한다.

< 사물인터넷 무선망 구성도 >



※ 게이트웨이와 네트워크 서버 간 백홀은 보안성·경제성·상호운용성·확장성 및 운영관리를 고려하여 유선, 무선, 유·무선 등으로 구성방식을 선택

비면허 주파수 대역을 사용하는 LPWAN은 LoRaWAN과 Sigfox가 대표적이며, 면허 대역 LPWAN은 LTE-M과 NB-IoT가 대표적이다. 면허 대역은 주파수 사용 허가를 받은 통신사업자가 구축하여 서비스를 제공한다. 비면허 대역은 통신사업자가 제공하는 서비스를 이용할 수도 있지만, 행정기관에서도 자체적으로 통신망을 구축하여 사물인터넷 서비스를 제공할 수 있다.

행정기관이 비면허대역을 활용하여 정부사물인터넷망을 자체 구축할 경우, 서비스 연속성, 연동 및 상호운용성, 향후 확장성 확보를 위해 OneM2M, OCF, LoRa 기반의 개방형 표준 아키텍처를 채택할 것을 권고한다.

※ **자체망은 서비스 수요가 많거나 다른 서비스와 공통활용 등으로 경제성·타당성을 확보할 수 있을 경우 구축**

- 자체 인프라가 있거나, 관련 기반시설이 많을수록 **경제성** 확보에 유리
- 상용망이 없거나, 상용망 이용이 어려울 경우 자체망 구축 **타당성**이 증가

가. 저전력 광대역 무선망(LPWAN) 기술

1) LoRaWAN

LoRa는 장거리통신을 의미하는 Long Range의 약자이며, LoRaWAN은 전력소모가 많은 3G・LTE 등 기존 이동통신망과 달리 저전력으로 장거리* 통신이 가능한 방식이다. 또한 3G나 LTE에 비해 낮은 인프라 구축비용과 높은 확장성을 갖고 있다. * 약 20mA의 전력 소모로 10km 이상 통신 가능

2) SigFox

디바이스(Object)가 센싱한 데이터를 ISM밴드(유럽 868, 미국 915MHz) 주파수를 사용하여 게이트웨이(기지국)로 전송하며, 게이트웨이는 수천 개의 디바이스로부터 수신된 데이터를 서버로 전송하는 방식으로 LoRa 무선통신방식과 마찬가지로 디바이스 신호를 가능한 여러 기지국이 수신하게 되며, 임의의 기지국에서 충돌이 발생하더라도, 다른 기지국에서도 같은 신호를 수신하기 때문에 기지국 수신 다이버시티의 효과를 가진다.

3) LTE-M

기존 LTE 면허대역을 이용한다는 점에서 초기 투자비용이 적고 다른 IoT 전용 네트워크와 비교했을 때 10Mbps/5Mbps(다운/업로드) 수준으로 빠른 속도가 장점이다. LPWAN 기술에 기반을 둔 LoRa 또는 SigFox와는 다르게 상시 전원이 확보 가능한 장치에 사용되며, 별도의 무선 통신망의 구축이 요구되지 않는 분야에서 활용이 가능하다.

4) NB-IOT (Narrow Band-IoT)

기존 LTE의 장점인 망 안정화, 로밍 등의 차별화를 활용하면서 가격 및 성능 등의 조건을 LoRa, SigFox와 같은 IoT전용망을 구현하기 위한 방향으로 발전 중이다. LTE-M과 달리 인접대역 주파수와 간섭을 막기 위한 가드밴드를 이용한다.

< LPWN 네트워크 기술방식 비교>

구분		비면허 대역		면허대역	
		SigFox	LoRa	LTE-M	NB-IoT
커버리지		~ 30km(지방) ~ 10km(도심)	~ 15km(지방) ~ 5km(도심)	~ 11km	~ 15km
주파수	대역	900MHz	900MHz	LTE 주파수	LTE 주파수
	대역폭	200KHz	~ 500KHz	20MHz	200KHz
표준화		ETSI	LoRa Alliance	3GPP Rel.8, Rel.12	3GPP Rel.13
통신속도		~ 1Kbps	~ 5Kbps	DL : ~10Mbps UL : ~5Mbps	~ 100Kbps
Device Stack		Non-IP	Non-IP	IP	Non-IP, IP
배터리 수명		~ 10년	~ 10년	~ 10년	~ 10년
주요 특징	장점	• 저전력 장거리 통신	• 저전력 장거리 통신 • LTE-M 모듈 ¼ 가격 • 저렴한 구축 비용	• 전국 서비스 가능 • 통신 품질의 안정성 • 기존 네트워크 활용	• 통신 품질의 안정성 • 실내커버리지 가능
	단점	• 비면허 대역으로 네트워크 불안정	• 비면허 대역으로 네트워크 불안정	• 고가의 통신모듈 가격	• LoRa에 비해 2배 비싼 통신 모듈 가격

나. 근거리 무선통신망 기술

근거리 무선통신 기술은 커버리지가 매우 제한적인 단점이 있지만, 특화된 용도가 있고 범용으로 각종 기기에 적용된 기술들도 있어서 여러 가지 근거리 무선통신 기술들을 혼용하거나, 장거리 유·무선통신 기술과 조합하여 사용할 수 있다.

1) 블루투스(bluetooth)

작고, 저렴한 가격(5달러), 적은 전력소모(100㎽)로 휴대폰, 노트북, PDA 등과 같은 휴대용 장치, 가정용 전자제품, PC 주변 장치들을 근거리(10~100m)에서

무선으로 연결하기 위한 무선 인터페이스 규격이다. WiFi가 이더넷 기반의 유선LAN을 대체한다면, 블루투스는 유선USB를 대체하는 기술로 ISM대역인 2.4GHz를 사용한다.

배터리 소모가 비교적 큰 편이기 때문에 사용시간이 생각보다 짧고, 널리 사용되는 통신규약인 Wi-Fi와 주파수 대역이 겹치기 때문에 Wi-Fi 신호가 강한 곳에서는 끊김 현상이 일어날 수 있다는 것이 단점이다.

※ **저전력 블루투스** (**BLE**, Bluetooth Low Energy)

- BLE기술은 사물인터넷을 지원하기 위한 블루투스 4.0표준에 포함된 규격 중의 하나이며, BLE는 단독으로 구현될 수 있고 기존의 블루투스 컨트롤러와 함께 구현될 수도 있음
- BLE는 전력 소모를 줄이기 위해 최대 전력 소모량을 15mA로 제한하고, 전송 속도는 1Mbps이기 때문에 음성이나 대용량 파일을 전송하는 데는 부적합 함

2) NFC(Near Field Communication)

전자태그(RFID) 기술 중 하나로 블루투스보다는 덜 익숙하지만, 최근 삼성페이, 티머니교통카드와 같은 전자결제 서비스가 등장하게 되면서 사용이 증가되고 있는 근거리 통신기술이다.

NFC는 기기 간의 통신을 위한 준비시간이 0.1초 이내로 매우 짧으며, 혼선을 일으키지 않고 안정적으로 연결을 처리하기 때문에 각종 전자결제에 적합한 반면, 통신거리가 최대 10cm에 불과해 매우 짧고, 전송속도 역시 블루투스에 비해 현격히 떨어지므로 블루투스와 NFC는 상호 보완적으로 활용된다.

※ **RFID** (Radio Frequency Identification)

- IC칩을 내장해 무선으로 관련 정보를 관리하는 태깅 기술
- 전자태그, 스마트태그, 전자 라벨, 무선식별 등으로 불리기도 하며, 식품·동물·사물 등 다양한 개체에 부착 또는 내장하여 정보관리 가능

3) 지그비(Zigbee)

사물인터넷 디바이스들 사이의 통신에 필요한 특수한 요구사항들을 고려하는 초기부터 꾸준히 발전되어 온 표준 기술이다. 지능형 홈 네트워크, 빌딩 등의 근거리 무선통신 시장과 산업용기기 자동화, 물류 환경 모니터링 등의 분야에서 활용이 가능하다.

데이터 전송 속도는 블루투스보다 느린 250kbps에 그치지만 전력 소모가 적으며, WiFi와 블루투스가 이동기기에 주로 탑재됐다면 지그비는 셋톱박스 등 고정된 액세스 포인트에 적합한 기술이다.

4) 지웨이브(Z-Wave)

홈오토메이션의 모니터링과 컨트롤을 위한 저전력 통신 기술로써, 지그비와 직접적으로 경쟁하는 근거리 통신 기술이다. 800~900MHz 주파수 대역을 사용하므로 2.4GHz를 사용하는 다른 표준과 비교해 통신 거리가 길고, 활용도가 높다. WiFi, Bluetooth, ZigBee 등 혼잡한 2.4GHz주파수 기반의 통신 기술에 비해 간섭에 자유로운 점이 장점이다.

5) 무선LAN(WiFi)

이더넷(Ethernet)이라 불리는 유선LAN을 무선화 했다는 의미에서 무선 LAN(WLAN, Wireless LAN)으로 통칭된다. 최근에 출시되는 개인용 휴대 장치들은 대부분 WiFi를 기본으로 지원하며, AP(Access Point)혹은 WiFi 핫스팟(Hot Spot)을 통해서 인터넷에 접속한다.

< 주요 근거리 무선통신 기술 비교 >

구분	블루투스	NFC	지그비	지웨이브	WiFi
주파수 대역	2.4GHz	13.56MHz	2.4GHz(글로벌)	868~929MHz	2.4G, 5GHz, 60GHz
전송거리	1~100m	10cm이내	100m이상	100m이상	약 100m
전송속도	~2M(BLE~1M)bps	424Kbps	250Kbps	40Kbps	ac~1.7G , ah100Kbps ax 9.6Gbps, ay 20Gbps
응용분야	주변기기 (헤드셋, 마우스 등)	전자결재, 기기간 직접전송	홈 네트워킹, 빌딩 자동화	홈 네트워킹, 빌딩 자동화	인터넷 접속, 무선LAN 구성
소비전력	1~100mW	50mW	1~100mW(Low)	Low	평균 100mW
특징	저전력 가능, AP없이 접속가능, 커버리지에 제약	무 전원 동작, 전파간섭 없음	저전력·저비용 네트워크 구성 가능, 타 통신과 간섭 우려	전파 효율성 및 호환성 우수	전력소모 많고 소형화 어려움, 커버리지 확장 가능

2. 유선망 구성

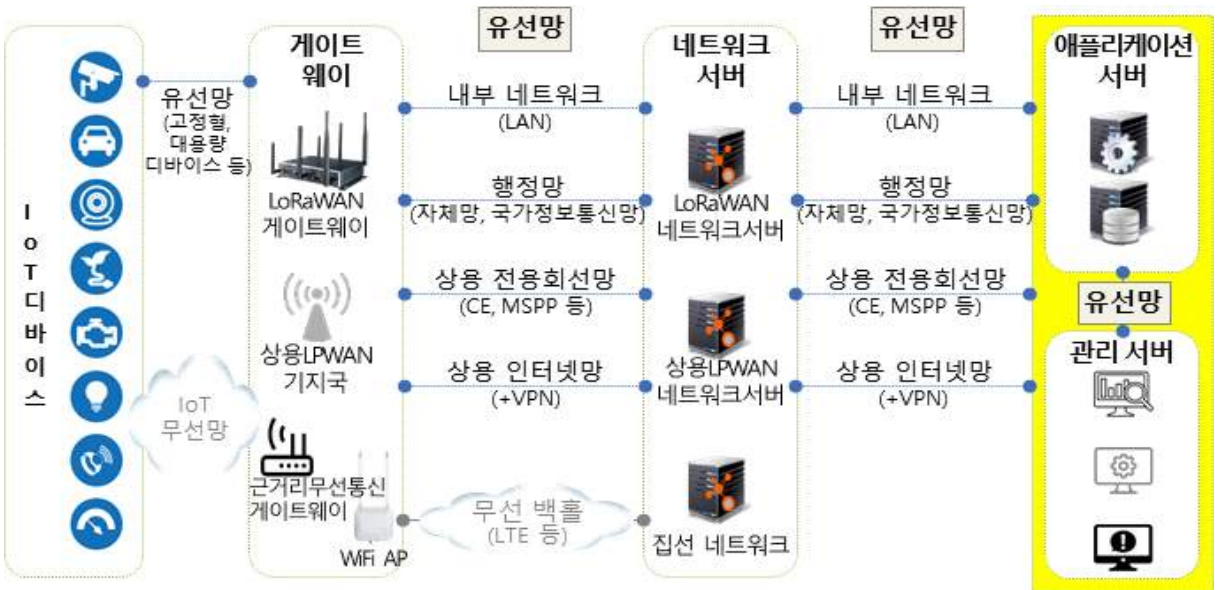
사물인터넷 유선망은 주로 게이트웨이와 네트워크서버 간, 네트워크서버와 애플리케이션서버 간, 각종 서버·시스템과 관리서버 간 네트워킹을 위해 구축된다.

디바이스(센서)와 게이트웨이 간 연결에도 실시간·대용량 트래픽을 발생시키는 디바이스(커넥티드CCTV 등)의 경우 유선망 연결을 통해 서비스 품질을 확보할 수 있다. 고정형 디바이스이면서 무선망보다 유선망 구축이 더 유리한 경우 유선망으로 구축한다.

네트워크서버, 애플리케이션서버 등 각종 정부사물인터넷 서비스 제공 관련 서버·시스템들이 동일한 장소에 구축되어 있을 경우에는 내부 네트워크(LAN)로 연결한다. 서버·시스템들이 동일 장소에 있지 않고 각각 원거리에 위치하여 외부 네트워크(WAN)로 상호간 연결해야 되는 경우도 있다.

WAN 유선망 구축은 필요에 따라 행정기관이 보유한 자체망, 상용망 및 인터넷망을 활용할 수 있다. 보안에 취약한 상용 인터넷회선을 사용할 경우 암호화 터널링(VPN) 기술 적용하는 등 보안성 강화를 위한 조치가 필요하다.

< 사물인터넷 유선망 구성도 >



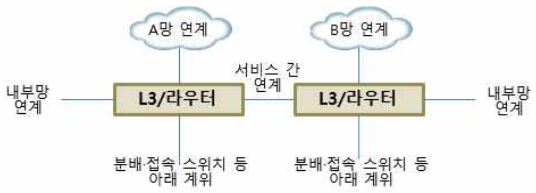
□ 내부 네트워크(LAN) 구성

LAN은 소규모 구성시 1개의 장비로 연결하는 1계위로 구성하기도 하지만, 규모가 커지거나 망이 복잡해지면 2계위·3계위 등 다계위로 구성해야 한다. 장비 구성형태에 따라 백본형과 분배·접속형으로 나눌 수 있으며, 백본형은 트래픽이 여러 방향으로 유통되며, 분배·접속형은 다수의 다운링크에서 1~2개의 업링크로 트래픽이 수직적으로 유통된다.

1) LAN 구성모델

구분	구성모델(예시)		
	1계위 (백본스위치 1대로 모두 수용)	**2계위** (백본-접속스위치로 2계위로 분할)	**3계위** (백본-분배-접속스위치 등 3계위 분할)
개념도			
설명	• 서비스 규모가 작아서 1개의 단위 LAN으로 구성이 가능한 경우	• 서비스의 규모가 커서 여러 대의 서버·시스템으로 구성해야 하는 경우	• 규모가 큰 다수의 서비스를 동일 LAN에서 구현하는 등 네트워크 규모가 큰 경우

2) LAN 구성형태

구분	백본형	분배·접속형
개념도		
설명	• 주로 백본 스위치의 구성형태로 트래픽 흐름이 복잡하고 처리량도 많은 구성 • 트래픽 처리 유형은 수직(업·다운로드) 트래픽, 중계 트래픽, 수평(내부) 트래픽 등 3가지 트래픽 유형 모두 존재할 수 있음	• 주로 분배·접속 스위치의 구성형태로 트래픽이 수직적으로 유통되는 형태 • 다운링크의 트래픽이 업링크로 집선되므로 업링크 이용률이 품질을 좌우할 수 있으므로 과부하가 걸리지 않도록 유의 필요

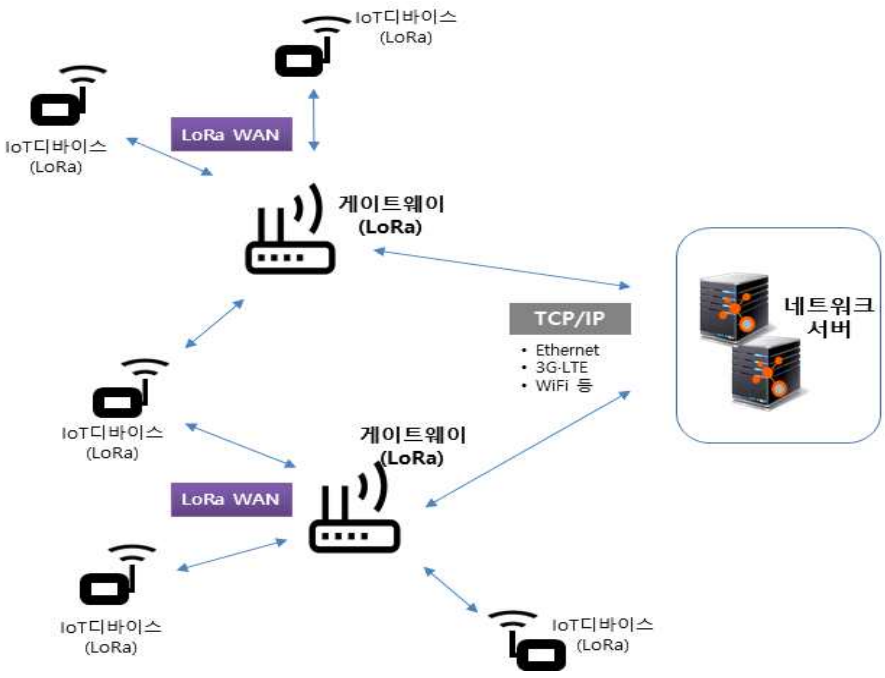
제4절 센서 · 게이트웨이 도입 기준

1. 센서 · 게이트웨이 개요

센서는 사물인터넷(IoT) 디바이스에 내장되어 빛, 온도, 압력, 소리, 화학성분 등의 여러 가지 물리량의 검출 또는 변화의 감지・구분・계측을 하는 소자이다. 게이트웨이는 센서가 검출한 물리량을 정부사물인터넷 서비스 플랫폼(애플리케이션 서버 등)이 수집・분석・처리할 수 있도록 전달한다.

게이트웨이는 센싱된 데이터를 단순히 전달만 하는 것이 아니라, 소형・저전력 특성에 기인하여 열악한 디바이스의 처리 능력과 메모리 한계를 보충하는 등 데이터를 종합한 후 네트워크 서버로 데이터를 전송한다.

< 디바이스(센서)·게이트웨이 데이터 전달 개념도(LoRa예시) >

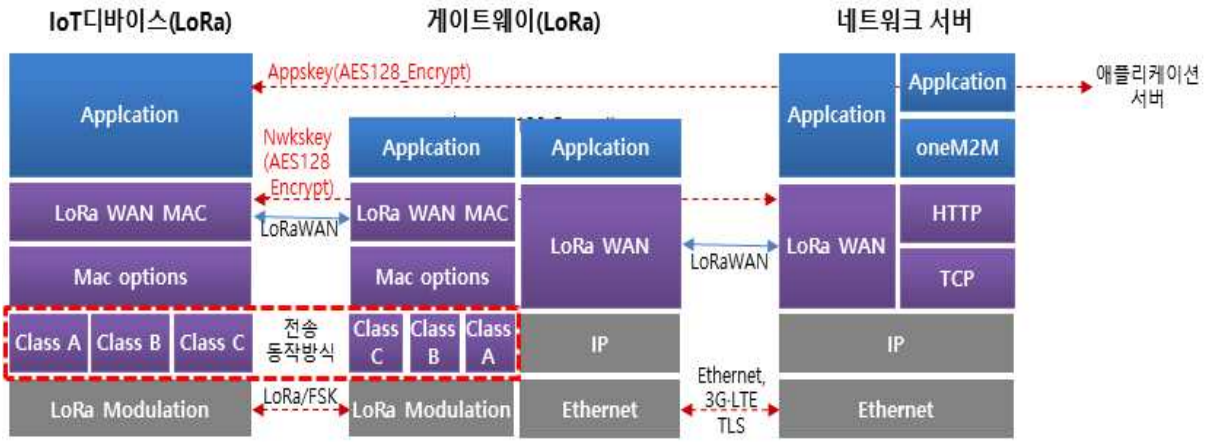


예를 들어, LoRa 네트워크에서 디바이스는 3가지 전송방식(Class)을 가진다. 첫 번째 방식 Class A에서는 평상시 송・수신 모두 꺼두었다가 디바이스가 데이터를 송신할 때, 송신 데이터를 전송한 이후에 정해진 시간동안 잠깐 수신 신호를 감지한다. 게이트웨이에서 센서 장치로 제어 명령 등의 Down Link 데이터가 있을 경우 RIT(receiver initiated transmission) 방식으로 처리한다.

Class A가 송신 위주의 전송방식이라면, 두 번째 방식 Class B는 수신 위주의 서비스에 적합한 전송방식이다. Class B에서는 일정 시간 간격마다 주기적으로 신호를 수신할 수 있는 상태가 되고, 해당 시간에 게이트웨이로부터 데이터를 수신할 수 있다.

세 번째 방식 Class C의 경우, 항상 수신이 가능 상태를 유지하는 방식이다. 때문에 타 Class에 비해 최소 지연시간을 갖지만, 가장 많은 전력을 소비한다. Class C를 사용하기 위해서는 충분한 전력이 공급되는 상황에서 고려해야 한다. Class C는 원격제어 등 실시간 서비스 구현에 적합한 전송방식이다.

< 프로토콜 스택(LoRa예시) >



2. 디바이스(센서) 도입 기준

디바이스는 정부사물인터넷 서비스에서 내장 센서를 통한 데이터 수집과 필요에 따라 제어장치를 통한 제어가 실제로 이루어지는 구성요소이다.

디바이스는 ❶ 센서와 통신모듈 둘 다 내장한 형태와, ❷ 센서만 내장하고 데이터 전송을 위해 별도의 통신모듈을 외부에서 연결하는 형태, ❸ 좀 더 많은 서비스 기능을 부여하기 위해 "❶·❷"의 형태에서 Gyro센서와 디바이스 온도를 측정하는 온도 센서 모듈까지 포함하는 다기능 형태가 있다. "❷"의 형태에서는 센서·제어장치와 LoRa 통신모듈 간 연결은 내부 유선 시리얼 통신(UART등) 으로 연결이 가능해야 한다.

본 디바이스 도입 기준은 행정기관이 자체 구축하는 LoRaWAN을 기준으로 하였다. 디바이스는 LoRa 표준이 규정하고 있는 Class별 전송방식과 패킷 암호·복호화 기능 등을 수행한다.

각 서비스에서 요구하는 서비스 의존적인 요구사항을 제외하고, 네트워크 연결 등 일반적인 사물인터넷 관련 도입 기준에 대해서 다룬다. 상용 IoT망과 IoT서비스를 사용하는 경우의 도입 기준도 해당 사업자의 요구사항을 따라야 하므로 제외하였다.

가. 디바이스 H/W 측면의 도입 기준

디바이스는 다양한 센서와 연동을 위한 인터페이스를 제공해야 한다. 제공하고자 하는 정부사물인터넷 서비스의 특성에 따라 특정 센서와 연동하는 경우 그에 필요한 해당 인터페이스만 제공할 수도 있다.

디바이스의 기본구조는 마이크로컨트롤러(MCU, Micro Controller Unit)와 연동 인터페이스, 그리고 통신모듈 등으로 구성된다.

< LoRa 디바이스 구조 >

■ **UART(범용 비동기화 송수신기: Universal asynchronous receiver/transmitter)**

- 병렬 데이터의 형태를 직렬 방식으로 전환하여 데이터를 전송하는 컴퓨터 하드웨어의 일종

■ **SPI 버스(직렬 주변기기 인터페이스 버스: Serial Peripheral Interface Bus)**

- 전이중 통신 모드로 동작하는 동기화 직렬 데이터 연결 표준
  - 장치들은 마스터-슬레이브 모드로 통신하며, 여기서 마스터 장치는 데이터 프레임을 초기화 한다.

■ **I²C(아이스퀘어드시: Inter-Integrated Circuit)**

• 마더보드, 임베디드 시스템, 휴대전화 등에 저속의 주변 기기를 연결하기 위해 사용

- SPI 통신은 노드 수에 따라 필요한 통신핀이 많아지는 단점이 있으나, I2C는 이런 단점들을 보완할 수 있는 동기식(synchronous) 시리얼 통신 방법

■ **ADC(A/D변환기 또는 A/D컨버터: Analog-to-Digital Converter)**

• 일종의 디지털 컴퓨터인 MCU가 신호를 처리할 수 있도록 아날로그 신호를 디지털 신호로 변환시켜주는 역할

■ **GPIO(다용도 입출력 포트: General Purpose Input/Output)**

• MCU가 주변장치와 통신하기 위해 범용으로 사용되는 입·출력 포트

- 특화된 입출력 레지스터를 통해 주변장치와 통신하며, 주로 병렬버스방식 사용

< 디바이스 H/W측면의 도입 기준(LoRa예시) >

항목	기준	설명
외부 인터페이스	• UART, I2C, SPI, GPIO, ADC	• 다양한 센서 및 기기 연동을 위해 다양한 인터페이스를 제공해야한다. • 근거리 무선 통신 기술은 위 유선 인터페이스를 통해서 해당 기술의 통신 모듈과 연동한다. (BLE, Zigbee, Z-wave 등)
동작 온/습도	• -20 ~ 50℃, 10 ~ 90%	• 일반적인 환경에서 동작시 문제가 없어야한다.
보관 온/습도	• -40 ~ 70℃, 10 ~ 90%	• 기준 보관 온도에서 보관후 동작시 문제가 없어야한다.
주파수 인증	• 주파수 대역에 대한 기술 기준에 따른 적합 인증을 받아야한다.	• 주파수 대역의 국내 기술 기준 및 무선설비 규칙 준수해야하며, 해당 기관의 인증을 받아야한다.
주파수 범위	• 917 ~ 923.5MHz	• 대한미국 무선설비규칙에서 할당한 LoRa 주파수 대역을 지원해야 한다. • LoRa가 사용하는 채널은 ch20 ~ ch32 이다.
하향링크 채널	• 최근 상향 링크 채널 주파수 사용	• 최근 상향 링크 채널 주파수를 하향링크 채널 주파수 위치가 되도록 동작해야한다.
RX2 채널 설정	• RX2 채널 설정 기능	• RX2의 채널 주파수 위치 및 SF, DR는 고정 설정이 가능해야 한다.
채널당 주파수 대역폭	• 125KHz	• 채널당 주파수 대역폭은 설정으로 변경이 가능해야한다.
배터리 수명	• 최대 8년 이하	• 사용자 전송 데이터의 주기에 따라 배터리 수명이 변경될 수 있다. • 디바이스의 크기 및 배터리의 최대 용량등을 산정하여 계산하여야 한다. • 수도 AMI의 경우 수도 미터기의 연한이 7년임을 고려할 때 이보다 더 많은 배터리

항목	기준	설명
		수명을 가져야 한다. • 2차 전지를 사용할 경우 에너지 하베스팅을 고려한 수명이 결정되어야 한다.
무선 출력	• 10 ~ 25mW (10 ~ 14dBm) • 1dBm 단위로 설정이 가능해야한다.	• 신고하지 아니하고 개설할 수 있는 무선국용 무선설비의 기술기준 제 8조 4항 참고 • 단, 최대 출력 사용시 배터리 수명이 단축된다.
송신전 신호감지	• 국내 기술기준에 부합하는 송신전 신호감지 규정을 설정할 수 있어야한다.	• 신고하지 아니하고 개설할 수 있는 무선국용 무선설비의 기술기준 제 8조 7항 참고
운영 채널 설정 기능	• 운영 채널 변경 설정	• 네트워크서버는 다채널 중 혼잡한 채널을 피해 유휴 채널로 디바이스와 통신 할 수 있도록 디바이스에 설정한다.
최소 성능 요구사항	• Data Rate에 따른 설정 값과 전송 속도를 보장해야한다.	• LoRaWAN Regional Parameters V1.0 2.8.3 KR920-923 Data Rate and End-device Output Power encoding에 근거 • 아래 "Tx Date Rate"표 참조
안테나 이득	• Average Gain –2dBi이상 (웨어러블 디바이스의 경우 –4dBi)	• 안테나 성능 기준을 충족하지 못할 경우, 송·수신 열화로 서비스 장애가 발생할 수 있다.
소비전력	• 하드웨어 Clock을 제외한 모든 하드웨어 컴포넌트를 Power Off 또는 Deep Sleep Mode를 설정하여 소모전력 최소화	• 설정 시간 이후 깨어나 동작하도록 하여 배터리 수명 최대화를 위한 기능
배터리 잔량 체크	• 배터리 잔량을 체크할 수 있는 하드웨어 구성	• 배터리 잔량 확인을 통한 디바이스 상태 체크를 위한 기능 • 잔량 부족 디바이스에 대한 처리지원을 위한 기능

< 디바이스 Tx Date Rate(LoRa예시) >

Data Rate	설정	**전송속도**(단위 : bps)
0	SF12 / 125KHz	250
1	SF11 / 125KHz	440
2	SF10 / 125KHz	980
3	SF10 / 125KHz	1760
4	SF10 / 125KHz	3125
5	SF10 / 125KHz	5470
6~15	RFU	

나. 디바이스 S/W 측면의 도입 기준

< 디바이스 S/W측면의 도입 기준(LoRa예시) >

항목	기준	설명
저전력 동작 지원	• 저전력 동작 지원	• 하드웨어 컴포넌트들에 대한 Deep Sleep 또는 Power off 처리 등 저전력 동작 지원으로 배터리 수명을 확보해야한다.
디바이스 클래스 지원	• 설정을 통해 디바이스 Class (A·B·C)를 변경 가능해야한다.	• 소프트웨어로 디바이스 클래스를 설정할 수 있고, 설정된 Class로 동작해야한다.
재전송 지원	• ADR(Adaptive Data Rate)기반 재전송 지원	• Confirmed UP 재전송이 연송 2회 실패시 Data Rate를 낮추어서 재전송한다. 서비스에 따라서 재전송 횟수를 설정할수 있어야한다.
배터리 잔량 전송	• H/W적으로 구성된 배터리 잔량 측정 값의 전달	• 디바이스의 배터리 잔량 확인을 위한 기능

3. 게이트웨이 도입 기준

게이트웨이는 사물인터넷 표준을 준수하는 장치로 디바이스와는 해당 표준 무선통신방식으로 데이터를 송・수신하고, 네트워크 서버와는 TCP/IP 방식으로 송・수신한다.

LoRa 디바이스의 경우 통신이 가능한 여러 게이트웨이와 데이터를 주고받는 등 비교적 가용성이 높다. 하지만, 게이트웨이가 많은 디바이스들을 수용하고 있거나, 장애에 민감한 서비스를 제공할 경우, 인근에 다른 게이트웨이가 없는 경우, 백홀회선의 빈번한 장애 또는 장애복구에 장시간이 소요되는 환경에 설치된 경우에는 최소한 게이트웨이의 백홀 이중화를 고려할 필요가 있다.

게이트웨이와 네트워크서버 간 TCP/IP 연결은 Ethernet 전용회선과 같은 유선망으로 연결하거나, 3G・LTE 또는 WiFi와 같은 무선 무선망으로 연결하기도 한다. 또한, 게이트웨이는 실내와 같은 양호한 환경에 설치되기도 하지만, 눈・비에 노출되거나 온・습도가 관리되지 않는 열악한 환경에 설치되기도 한다.

게이트웨이 도입 기준은 개방형 표준 LoRa를 기준으로 하드웨어 형상 및 주파수 특성을 정의하는 H/W적 측면과 게이트웨이의 기능적 특성을 정의하는 S/W 기능적인 측면으로 분리하여 제시 한다.

가. 게이트웨이 H/W 측면의 도입 기준

< 게이트웨이 H/W측면의 도입 기준(LoRa예시) >

항목	기준	설명
형상	• 옥외 일체형 장비	• 함체내에 제어부, 채널부, RF부 및 전원 공급부를 모두 포함한다.
외부 인터페이스	• 안테나, 백홀, 전원이 연결 가능해야한다	• 안테나 : 커넥터로 옴니 또는 섹터 안테나와 연결 가능해야한다. • 백홀 연결 : RJ-45를 기본으로 한다. PoE를 지원 할 수 있고, 3G·LTE 모뎀과 연결이 가능한 이더넷 WAN 포트 또는 USB포트가 지원되어야한다. • 전원 : 단상 220V (60Hz) AC 또는 PoE(48V Class 0)로 연결이 가능해야하며, 상전 연결이 어려운 경우, 태양광 발전으로 동작이 가능해야한다.
냉각방식	• 자연냉각	• 별도의 FAN없이 냉각이 가능해야한다.
실시간 분석	• 디버깅 포트를 통한 실시간 로그 모니터링	• 오류 발생시 노트북을 연결하여 장비의 동작 로그를 확인하고 원인 분석이 가능해야한다.
파라미터 설정	• 디버깅 포트를 통한 설정 관리	• 게이트웨이 동작에 관련된 파라미터 설정이 가능해야한다.
마운트 형식	• Wall 마운트 Pole마운트 지원	• 디바이스는 설치 환경에 특성에 따라서 Wall 마운트 형식 또는 Pole 마운트 형식으로 설치가 가능해야한다.
접지	• 접지용 단자 부착	• 어레스터(arrester)는 커넥터 일체형으로 장비에 포함한다.
동작 온·습도	• -20 ℃ ~ 50 ℃ • 10 % ~ 90%	• -20 ℃에서 cold start를 지원해야한다.
보관 온·습도	• -40 ℃ ~ 70 ℃ • 10 ~ 90%	• 장시간 보관후 전원 ON시 정상 동작해야한다.
방진/방수 규정	• IEC-529규격 중 IP65 이상 만족	• 먼지의 침입을 완전히 방지하여 보호가 되어야 하고, 외함의 모든 방향에서 분사되는 물에 대하여 영향을 받지 않아야 함. • 전기제품 외함 보호규격(IEC-529 표준) 참조
진동기준	• 주파수 범위 : 5 ~ 100Hz • 중력가속도(g=m/s^2): 0.1g • 진동축 : 3축 • Sweep rate : 0.1 oct/min • Duration of Sweep : 90min	• GR-63 core 표준 참조
염수 환경 기준	• 염수환경기준 - PH : 6.5 ~ 7.2	• IEC 68-2-11 Ka 표준 참조

항목	기준	설명
	• 온도 : 35℃± 2℃ • 습도 : 85% RH이상 • 시간 : 168 Hour	
주파수 범위	• 917 ~ 923.5MHz	• 대한미국 무선설비규칙에서 할당한 LoRa 주파수 대역을 지원해야 한다. • LoRa가 사용하는 채널은 CH20 ~ CH32 이다.
하향링크 채널	• 최근 상향 링크 채널 주파수 사용	• 최근 상향 링크 채널 주파수를 하향링크 채널 주파수 위치가 되도록 동작해야한다.
RX2 채널 설정	• RX2(재전송) 채널 설정 기능	• RX2의 채널 주파수 위치 및 SF(Spreading Factor), Data Rate는 고정 설정이 가능해야 한다.
채널당 주파수 대역폭	• 125KHz	• 채널당 주파수 대역폭은 설정으로 변경이 가능해야한다.
송신전 신호감지	• 국내 기술기준에 부합하는 송신전 신호감지 규정을 설정할 수 있어야한다.	• 신고하지 아니하고 개설할 수 있는 무선국용 무선설비의 기술기준 제 8조 7항 참고
송신출력	• 채널별로 0 ~ 200mW 범위 내	• 신고하지 아니하고 개설할 수 있는 무선국용 무선설비의 기술기준 제 8조 4항 참고 • 0.1 mW단위로 설정 가능해야한다.
유선 백홀 연동	• 백홀은 RJ45로 연결되어야 하고 100Mbps, 1Gbps를 자동인식하고 지원해야한다.	• 네트워크 서버와 연결을 위한 백홀 연동 IPv4, IPv6를 모두 지원해야한다.
무선백홀 연동	• 장비내 3G·LTE 모뎀을 장착하여 무선 백홀 설정이 가능해야한다.	• 유선 백홀을 구성할 수 없는 경우, 무선 백홀을 연결할 수 있어야한다. • 3G·LTE모뎀연동을 위한 USB 인터페이스가 있어야한다.
IP주소할당	• 백홀 인터페이스에는 IP주소를 Static 또는 Dynamic 방식으로 설정이 가능해야한다.	• 주소할당은 아래 중 한 가지 방식으로 설정이 가능해야한다. - Static, DHCP, Stateless Address Auto-configuration(IPv6)
백홀 이중화	• 유선 백홀이 기본 Active 인터페이스이고, 무선 백홀은 Standby 인터페이스로 동작한다.	• 백홀 네트워크의 이중화를 통해 서비스의 안정성을 높인다.
Reset 기능	• 하드웨어 리셋 스위치 장착	• 장비에 문제 발생시 하드웨어 리셋 스위치로 장비를 재기동할 수 있어야 한다.

나. 게이트웨이 S/W 도입 기준

< 게이트웨이 S/W측면의 도입 기준(LoRa예시) >

항목	기준	설명
NS연동 기능	• GWMP(Gateway Message Protcol) 및 JSON지원	• Network Server 와의 연동을 위한 규격을 준수해야한다. - Software Solution Gateway to Server Definition 규격 참고
접근제한	• 관리자만 접근이 가능해야한다.	• 비인가된 접속을 통한 데이터 수집을 막기 위해 디버깅 포트를 통한 직접 접근 및 원격 접근 제어가 필요하다
장비 상태 수집 전달	• 장비의 내부온도, 채널별 신호 상태, 메시지 수신 성공 여부, 안테나 상태 수집 전달	• 운영서버에서 기지국의 상태를 확인할 수 있어야한다.
트래픽 정보	• 장비를 통한 상·하향 메시지 량 및 전송속도에 대한 통계 데이터 전달	• 장비의 성능 및 트래픽 엔지니어링을 위한 트래픽 통계 전달 필요
구성정보 관리	• 장비의 S/W, F/W 버전, serial 및 구성 파라미터 등의 정보를 관리하고 인가된 사용자에 대해 원격 변경을 지원해야 한다.	• 해당 정보들을 관리하고 필요시 운영서버로 전달할 수 있어야한다.

4. 센서 · 게이트웨이 상호운용성 기준

< 센서·게이트웨이 상호운용성 >

구분	관련 국제표준	관련단체/기술내용	관련 TTA 표준
2G·3G·4G 등 이동통신망	3GPP TS 36, 101 3GPP TS 23.003 등 (2,990 여개)	• 3GPP 이동통신 국제 표준화 단체 - GSM, GPRS, CDMA, WCDMA, HSDPA, HSUPA, HSPA+, LTE, LTE-Advanced 등	TTAT.3G-36.101 AE.IR-M.2083 (IMT-2020 비전)
LoRa	LoRaWAN R1.0 등	• LoRA Alliance - 저전력 광대역, 비면허 Sub-GHz 대역, CSS(Chip Spread Spectrum) 방식	
NB-IoT (협대역 IoT)	3GPP Realease 13 등	• 3GPP - stand-alone, guard band, in-band 운용모드 지원	TTAR-06.0170 (3GPP Rel.13 분석)
와이파이 (WiFi)	IEEE 802.11 a/b/g/n/ac IEEE 802.11ah 등	• WiFi-Alliance - 저전력 장거리 전송, 고효율	TTAK-KO-04.0215 (스마트 전원)

구분	관련 국제표준	관련단체/기술내용	관련 TTA 표준
블루투스 (Bluetooth)	Bluetooth spec. IEEE 802.15.1 IETF RFC 7668 등	• Bluetooth SIG - IPv6, 6LowPAN 기반, A2DP, AVRCP, DI, HFP, HID, HOGP, HSP, MAP, OPP, PAN, PBAP - 블루투스 5.0 400m 까지 지원	TTAE.IF-RFC7668. TTAE-OT-12.0018 (저전력 블루투스)
지그비 (ZigBee)	ZigBee PRO Specification 등	• ZigBee Alliance - IEEE 802.15.4 PHY&MAC 기반 저전력, 저비용	TTAK-KO-04-0216 (홈에너지 관리)
지웨이브 (Z-Wave)	Z-Wave Specification	• Z-Wave Alliance - ITU-T G.9959 기반, Sub 1GHz, 저전력 양방향, 무선메시, GFSK(가우시안 주파수 편이 방식) 사용	TTAE-IF-RFC7428 (IPv6 패킷 전송)
근거리 무선통신 (NFC)	NFC Forum Tech Spec. ISO/IEC 18092 등	• NFC(Near Field Communication) Forum - NFC 기반 사물 인터넷	TTAK,KO-10.0968 (NFC 기기간 연속성)

제5절 서버 도입 기준 (네트워크 · 애플리케이션 · 관리 서버 등)

1. 서버 도입 개요

정부사물인터넷 제공에서 서버들은 거점노드 또는 센터노드에 구축되어 각종 디바이스에서 보내는 데이터들을 수집・분석・처리하며, 처리결과 피드백이 필요하거나 원격제어 등 디바이스에 명령을 전달해야 할 경우 디바이스로 관련 데이터들을 송신한다.

디바이스 장애나 게이트웨이의 장애는 피해범위가 제한적이지만, 각 서버에서 장애가 발생하면 전체 서비스에 영향을 주게 되므로 가용성 구성이 중요하다. 가용성 구성은 서버 H/W와 네트워크 연결 등 주요 구성 요소들을 이중화・이원화 구성하거나, 서버 과부하에 대처하기 위한 부하분산 구성이 있다. 서버에 대한 전원 공급도 상전・UPS 등으로 다원화한다.

네트워크 서버는 여러 LoRa 게이트웨이에서 전송되어 오는 디바이스의 중복 메시지를 제거하고, 메시지에 응답해야 할 게이트웨이 결정한다. 또한, 데이터 전송률 관리 등으로 네트워크 용량 최대화와 디바이스 배터리 수명을 연장하는 등 LoRaWAN 네트워킹을 관장하므로 네트워크 및 트래픽 제어, 패킷 버퍼링, 디바이스 주소 할당 등 도입시 주요 고려사항들이 있다.

관리서버는 서비스에 문제가 없도록 디바이스 및 관련 시스템을 관리하며, 관제 및 운영를 위한 연동, 로그 수집・검증・저장・분석을 통한 장애 및 성능 감시, 등록된 디바이스에 대한 상태와 실시간으로 추적하여 문제발견 및 조치에 관한 기능들이 도입시 고려해야 할 사항이다.

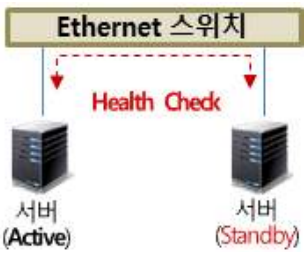
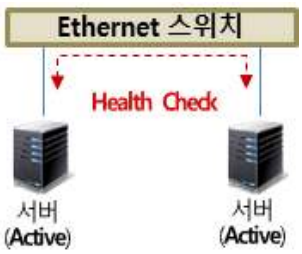
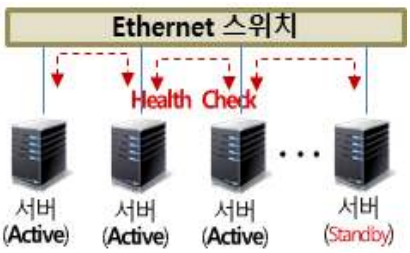
애플리케이션 서버는 정부사물인터넷 서비스의 목표 서비스 제공과 관련 애플리케이션에 대한 개발・배포・업데이트 환경을 제공한다.

각종 서버들을 구성하는 시스템은 CPU・RAM 등 H/W 성능은 서비스가 원활하게 제공될 수 있도록 적정하게 확보하여야 하며(“제5절 시스템 용량” 참조), 서비스 제공을 위한 애플케이션 S/W의 규격은 OneM2M・OCF 등 사물인터넷 개방형 표준을 준수하여야 한다.

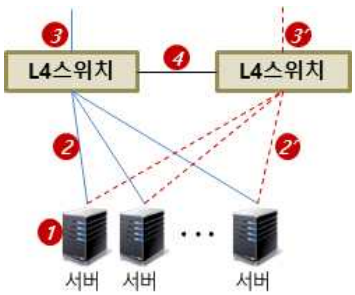
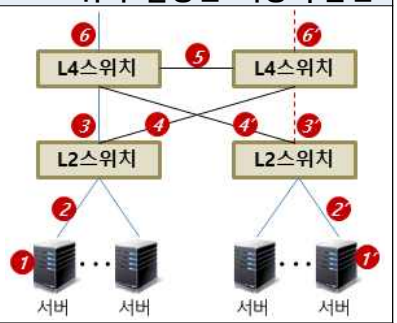
2. 서버 도입 기준

가. 서버 이중화 구성방안

< 서버 이중화 구조(동작방식) >

구분	(1) Active-Standby 방식	(2) Active-Active 방식	(3) N+1 방식
개념도			
설명	• 동일 용량의 서버 2대로 구성 • 서버는 상호간에 상태를 체크하여, Active 장애시 설정정보 등을 Standby로 전달하여 서비스 유지	• 동일한 2개 서버가 동시에 서비스를 제공하여 평시는 "1"방식보다 2배 처리용량 • 1대 장애시 정상 서버가 모든 서비스를 처리	• 여러 대의 동작서버에 1대의 대기서버를 두는 방식 • 분산처리, 확장성 등을 고려할 때 가장 효율적인 동작방식
특징	• 데이터의 실시간 동기화와 2개 서버 단위로 증설 필요	• 데이터의 실시간 동기화와 부하분산용 L4스위치 필요	• 서버간 부하분산용 L4스위치와 여러 서버 장애시 서버 과부하 대책 필요

< 서버 부하분산 및 이중화 구성방안 >

구분	부하분산 방식	이중화 및 부하분산 방식	
		서버 네트워크카드(NIC) 이중화분산	L2스위치 활용한 이중화·분산
개념도			
설명	• 동일기능 서버 2대 이상으로 부하분산 구성	• 네트워크 장애에서도 서비스가 가능하도록 서버NIC 이중화	• 서비스별 또는 동일 서비스 서버들을 그룹화하여 네트워크·서버 이중화 및 부하분산
특징	• 최소 1대 이상의 서버가 가용상태일 경우 서비스 가능하나 • 네트워크(③의 장비 및 연결) 장애시 서비스 중단	• 가용성이 높은 구성이지만, • 서버에서도 이중화 네트워크에 대한 경로제어 S/W의 설정이 필요한 등 구성 복잡	• 서버 네트워크의 이중화 구성에서 많이 사용되는 방식 • 동일한 서비스의 경우 서버가 많은 대규모 서비스의 경우 가능

※ 서버는 각각 IP주소를 가지므로 동일한 기능을 가진 여러 대의 서버로 부하를 분산할 경우 L4계층 이상의 스위치 필요

나. 네트워크서버 도입 고려사항

< LoRa 네트워크서버 도입 기준 >

항목	기준	설명
표준지원	• LoRa Alliance의 1.0.2 이상 준수 • Software Solution Gateway to Server Definition	• LoRa Alliance의 1.0.2 표준을 준수해야 한다. • Network Server와의 연동 규격은 Software Solution Gateway to Server Definition 규격 준수
연결성	• IPv4, IPv6 지원	• 각 entity는 IPv4나 IPv6를 통해 연동 가능해야한다.
Activation	• OTAA지원	• LoRa Alliance에서 규정한 Over-The-Air Activation을 지원해야 한다.
처리 지연	• packet 처리 지연 속도 기준 - Signaling Processing Delay : 5ms 이내 - Traffic Processing Delay : 1ms 이내	• Packet 처리에 대한 높은 신뢰성을 보장하여야 하며, 처리 성공률 보장해야한다.
트래픽 제어	• interface별/NE별 트래픽 제어	• 초당 메시지 송출 및 수신 량을 제어할 수 있어야한다.
DDoS 탐지	• 비정상 트래픽 유발 정보 추출 및 차단	• 임계치 이상의 이상 트래픽을 발생시키는 디바이스에 대한 차단 및 목록 추출 기능 제공
위치 측위 기능	• 기지국 기반 위치 측위 기능 지원	• GPS정보가 없더라도 기지국 수신 시간 정보를 기반으로 위치 측위가 가능해야한다. 도난, 경로 추적 등에 활용 가능
네트워크 제어 기능	• MAC 명령어 지원	• LoRaWAN에서 정의한 네트워크 제어 기능을 제공해야한다.
패킷 버퍼링	• 패킷버퍼 지원	• 디바이스가 데이터 수신이 불가능한 경우 패킷 버퍼링 기능 제공. 퍼버 사이즈는 설정이 가능해야하고, 납품 업체는 최적의 버퍼사이즈를 제시해야한다.
주소 할당	• 디바이스 주소 할당	• Join 처리 절차에서 특정 Device EUI 와 Application EUI를 기반으로 고정된 디바이스 주소를 할당 할 수 있어야 한다.
적응적 대역폭 할당	• 채널별 ADR(Adaptive Data Rate) 기능 지원	• 각 채널별 디바이스의 채널 세기에 따라 SF 및 data rate를 적응적으로 할당할 수 있어야 한다.

다. 관리서버 도입 고려사항

< LoRa 관리서버 도입 기준 >

항목	기준	설명
연동 관리	• 시스템들 간 연결 관리	• 연동 시스템들 간의 연동 상태 관리
로깅	• 이벤트 메시지 로그 처리	• 시스템 이벤트 메시지들에 대한 로깅 기능이 제공되어야한다. • 로그는 파일 형태로 저장할수 있어야 하고, 발생 타입이나 ID별로 출력이 가능해야한다. • 로그저장 기간은 운영자가 설정이 가능해야 한다.
백업/복원	• 구성정보 및 DB정보에 대한 백업 및 복원	• 설정된 주기 또는 운영자 요구에 따라서 구성 정보 및 DB정보를 백업/복원 기능을 제공해야한다. • 백업/복원 작업으로 인한 서비스 중단이 발생하지 않아야 한다.
구성관리	• H/W, S/W에 대한 형상 관리	• 모든 NE, 서버, S/W에 대한 형상 정보를 관리할 수 있어야한다.
상태 관리	• H/W, S/W에 대한 상태 관리	• 모든 NE, 서버, S/W에 대한 상태 정보를 관리하고 장애 시 해당 내용을 운영자가 인지할 수 있도록 해야 한다.
고장 관리	• 서비스 오류나 장비 오류 관리	• H/W오류, 사용률, 패킷처리 오류에 대한 심각도에 따라 등급을 정의하고, 가청 경보를 통해 운영자가 인지할 수 있도록 해야 한다. • 설정된 운영자에게는 SMS등을 통해서 알림을 주어 빠른 조치가 가능하도록 해야 한다.
성능 감시	• 성능이나 시스템의 사용률 감시	• 모든 구성 요소들에 대한 성능과 시스템 사용률을 감시하여 해당 정보를 운영자가 파악할 수 있도록 해주어야 한다. 운영자를 성능 데이터를 기반으로 증설에 대한 결정을 할 수 있다.
통계 관리	• 성능, 고장 등에 대한 통계 관리	• 수집된 성능, 고장 데이터들을 기반으로 주기적인 통계의 산출 및 관리가 가능해야 한다. • 통계 주기는 5분, 10분, 15분 1시간, 24시간을 기본으로 하며, 월별 통계도 추출이 가능해야한다.
계정관리	• 관리자 정보 관리	• 관리자의 등록/수정/삭제/조회 등이 가능해야하며, 아이디 암호 관리를 통해 인증된 사용자만 접근이 가능하도록 해야 한다. • 암호의 aging기능을 제공해한다.
기지국 관리 기능	• 기지국 정보 관리 기능	• 기지국 구성정보, 연결상태, 성능 정보 등을 관리해야 한다.

항목	기준	설명
		• 기지국 관리 서비는 별도로 제공 될 수도 있다. 이 경우, 필요하다면 네트워크 서버 운영자 서버와 연동을 제공해야 한다.
Trace	• 실시간 Trace 지원	• 특정 Device ID나 메시에 대해서 실시간 Trace가 가능해야 한다. 실시간 Trace를 통해 문제점을 발견하고 해결할 수 있다.
Device관리	• 등록 디바이스 상태 관리	• 등록된 디바이의 상태 정보를 수집하고, 디바이스 장애 여부를 판단할 수 있어야 한다. - 예) 배터리 잔량 부족 시 해당 장비에 배터리 교체 • 디바이스 관리 기능은 서비스 서버에서 제공을 기본으로 한다. 단, 서비스 서버에서 제공하지 않을 경우에 운영자 서버에서 관리가 가능해야한다.

3. 관리서버 상호운용성

< 관리서버 상호운용성 >

구분	관련 국제표준	관련단체/기술내용	관련 TTA 표준
OCF	OIC Core Spec 등	• OCF(Open Connectivity Foundation) - 개방형 IoT 플랫폼 표준화, OIC 핵심구조, 인터페이스, 프로토콜, 서비스 등 정의	-
OMG	OMG Data Distribution Service Spec 등	• OMG(Object Management Group) - 데이터 통신, 보안, IFML(상호작용 흐름 모델링 언어) 등 정의	-
oneM2M	oneM2M Technical Spec. (0001, 0003, 0004, 0008, 0009, 0010 등)	• oneM2M - 프레임워크, 보안, 메시지 프로토콜 (CoAP, HTTP, MQTT) 등 정의	TTAT.MM-TS 0001, 0003, 0004, 0008, 0009, 0010 등
OASIS	MQTT ver 3.1.1 등	• OASIS MQTT 기술위원회 - 클라이언트/서버 게시/구독형 경량 프로토콜	-
Thread	Thread Specification	• Thread Group - 6LoWPANrlqks 네트워크 프로토콜, QES(고급암호표준) 적용	-
IEEE P2413	IEEE P2413 Standard	• IEEE P2413 워킹그룹 - IoT 아키텍처 프레임워크, 참조모델 등 정의	-

제6절 시스템 용량 기준

< 시스템 용량산정 개요도(예시) >

원활한 정부사물인터넷 서비스 제공을 위해 시스템을 구성하는 주요 요소에 대한 적정한 용량을 확보하여야 한다. 주요 요소의 용량산정 고려사항에 대해 개략 살펴보면 아래와 같다.

❶ 디바이스의 단위 송출 데이터크기와 빈도수, 디바이스 수량으로 LoRaWAN 용량(센서·게이트웨이 등)을 산출할 수 있다. ❷ 각 게이트웨이에서 네트워크 서버로 전송하는 백홀회선의 적정 대역폭이 확보되지 않으면 병목현상에 따른 전송지연·데이터유실 등으로 서비스 품질이 나빠진다. ❸ 네트워크 서버는 디바이스와의 전송 동작방식에 따른 전송제어와 디바이스에서 전송하는 데이터의 처리를 원활하게 해야 하므로 적정 용량의 확보가 필요하다. ❹ 각 서버의 CPU·메모리·디스크 등 처리 성능도 서비스 품질에 영향이 크다. ❺ 서버 간 부하분산 및 연동 등을 위한 L2/L3/L4스위치, 방화벽 등 네트워크 구성장치도 병목점이 될 수 있으므로 처리성능에 대한 고려가 필요하다.

1. 데이터 전송량 예측

각 디바이스는 내·외장 센서의 종류와 수량, 전송 빈도수에 따라 단위 전송량이 달라진다. 게이트웨이는 각 디바이스로부터 송·수신되는 데이터 양을 기준하여 처리용량과 백홀 전송량을 산정해야 하며, 백홀의 종류(과금방식)에 따라 회선대역폭을 산정하거나, 소요 데이터 용량을 산정해야 한다.

전용회선 등 유선망은 대부분 거리·속도 병산 요금제이며, 매달 일정 금액의 요금만 지불하면 데이터 전송량에 무관하게 사용할 수 있기 때문에 적정 회선속도(대역폭) 산정 및 이용률 등 트래픽 관리가 중요하다.

(1) 디바이스별 전송량[Byte/시간]
= 전송데이터 크기(Byte) × 3600초 ÷ 전송주기(초)

(2) 게이트웨이 유선(정액제) 백홀 소요 대역폭[bps]
= Σ {디바이스별 전송량(Byte/시간) × 8(bit) ÷ 3600초} × 공유율*

* 공유율 : 모든 디바이스가 동시에 전송을 하는 것이 아니므로 적용하는 보정 값("1" 이하 값)
- 모든 디바이스가 동일한 전송량을 가질 경우 "**단위전송량×동시전송수×8÷3600**"로 산정 가능

(3) 게이트웨이 무선(종량제) 백홀 소요 데이터 용량[Byte/월]
= Σ {디바이스별 전송량(Byte/시간) × 24시간 × 28~31일}

2. 네트워크 서버 성능

행정기관의 자체망 구축에서 성능에 대한 이슈가 가장 중요한 노드는 LoRa 네트워크 서버이다. 네트워크 서버의 성능을 산정하기 위해서는 서비스의 트래픽 특성, 서비스 관련 서버와의 연동구조, 디바이스에 동시에 연결되는 게이트웨이 수 등의 조건을 고려해야한다

네트워크 서버 성능산정을 위한 트랜잭션(TR) 수
= 초당 전송요청 수
× {연결 게이트웨이 수 × (상향링크 TR수 + 하향링크 TR수)
+ 서비스 서버 TR수*}

* 서비스 서버 TR수 : 네트워크 서버와 연결된 서비스 관련 서버들과의 초당 TR수

※ JOIN 처리, MAC 명령어 처리, 서비스 데이터 처리 등으로 유형을 정의하고 각 유형별로 분포 비율을 산정하여 최종 예상 TR수를 산정

가. 디바이스와의 전송 동작방식

■ **전송동작 Class**

- A : 디바이스 송신 중심, 디바이스가 송신동작을 한 후 잠시동안 수신하는 방식

- B : 디바이스 수신 중심, 일정한 시간 간격마다 주기적으로 수신하는 방식
- C : 디바이스가 항상 수신할 수 있는 방식, 실시간 서비스 구현에 적합한 방식

→ 상·하향 링크 TR수와 관련된다.

나. 경유 기지국 수

■ **LoRa 디바이스는 데이터 전달이 가능한 여러 게이트웨이로 전송한다.**

- 디바이스에서는 상향링크로 데이터를 전송하고 이를 수신한 모든 게이트웨이는 네트워크 서버로 전달하고, 네트워크 서버에서는 동일한 메시지를 수집하고, 이들 중 최적의 경로를 찾아 하향 링크로 데이터를 전달하는 구조이다.
- 따라서 불특정하게 다수의 동일한 메시지를 수신하는 특성이 있으며, 이 특성은 기지국 수가 많을수록 심화된다.

→ 연결 게이트웨이 수와 관련된다.

다. 데이터 전송 주기

■ **전송 주기**

- 전송주기가 짧을수록 전송량이 많아짐

→ 초당 전송요청 수의 근거가 된다.

라. 송 · 수신 트랜잭션(TR) 수

→ 상·하향 링크 TR수와 관련된다.

■ **Confirmed/Unconfirmed 데이터**

- **Confirmed** : 게이트웨이에 응답을 요청하는 데이터이며, 응답을 받지 못했을 때 8회까지 재전송을 진행한다.

- Confirmed Uplink 데이터를 보냈을 때, 열악한 무선환경 등의 이유로 모듈 재전송이 8회 동안 이루어진다면, 이는 최대 1분 이상의 시간이 소요될 수 있다.

- **Unconfirmed** : 응답을 요청하지 않은 채 1회 전송하며, 재전송 회수를 따로 설정할 수 있다.

■ **송·수신 트랜잭션수(TR, transaction)**

- 1개의 디바이스가 1개의 게이트웨이와 연결되는 조건으로 상향링크에 대한 **Confirmed 데이터의 TR수는 2개**, **Unconfirmed는 1개의 TR**이 발생한다.

[참고 : 네트워크 서버 성능기준(LoRa예시)]

수용 디바이스 개수, TPS 및 이중화 구성에 따른 LoRaWAN 네트워크서버의 적정 대수는 아래와 같다

< 디바이스 개수, TPS 및 이중화 구성을 고려한 네트워크 서버 적정수량 예시 >

수용 디바이스 수량	TPS (Transaction per sec)	LoRaWAN 네트워크 서버 H/W 대수	LoRaWAN 네트워크 서버 S/W 운영수
2k ~ 5k	1000TPS	2	1
5k ~ 10k	1000TPS	2	1
10k ~ 20k	1000TPS	2	1
20k ~ 50k	1000TPS	2	1
50k ~ 1,000k	2000TPS	4	2
1,000k ~ 1,500k	3000TPS	6	3
1,500k ~ 2000k	4000TPS	8	4
2,000k ~ 5,000k	5000TPS	10	5

3. 서버 H/W 용량 (참조 : "정보시스템 하드웨어 규모산정 지침", 2018, TTA)

서버의 하드웨어(H/W) 구성 분야는 시스템 가격 및 성능 측면에서 가장 중요한 CPU, 메모리, 디스크, 그리고 스토리지 등 4가지 분야로 나눌 수 있다. CPU는 해당 업무를 처리하는데 필요한 적정 용량을 산정하며, 나머지 분야는 CPU 용량에 따른 서버 구성방안에 의하여 산정된다.

- CPU : 해당 업무를 처리하기 위한 CPU 규모를 계산한 후, 적정한 성능을 지닌 서버 기종을 선정한다.
- 메모리 : CPU 규모산정에 따른 서버 구성방안에 의거하여, 서버별 시스템 S/W, 응용 프로그램 등의 메모리 사용량을 산정한다.
- 디스크 : CPU 규모산정에 따른 서버 구성방안에 의거하여, 서버별 OS, 시스템 S/W, DB의 데이터, DB의 아카이브(Archive) 및 백업 영역 등의 디스크 사용량을 산정한다.
- 스토리지 : CPU를 기준으로 산정된 서버 규모에 따라 필요한 스토리지의 규모를 산정한다.

가. CPU (데이터베이스 서버 기준)

CPU는 산정대상 시스템이 WEB이나 WAS서버로 쓰이는 경우 WEB/WAS 산정기준을 적용하고, DB서버로 쓰이는 경우에는 OLTP 또는 OLTP & Batch 애플리케이션 산정기준을 적용한다.

일반적으로 OLTP 또는 OLTP & Batch 애플리케이션을 위한 서버의 규모 산정을 위한 tpmC 추정방법은 시스템 아키텍처, 서비스 제공형태 등에 따라 다르다. 따라서, 해당 서비스 시스템에 대한 업무 내용을 상세하게 분석해야만 적정 성능을 보장할 수 있는 규모를 산정할 수 있다.

CPU(tpmC단위)

= (분당 트랜잭션 수
× 기본tpmC 보정 × 피크타임 부하 보정 × DB크기 보정
× 애플리케이션 구조 보정 × 애플리케이션 부하 보정 × 클러스터 보정
× 시스템 여유율)
÷ 시스템 목표 활용률

< 서버 CPU 용량산정 요소 >

구분	산정항목	내용	적용범위	일반값
O1	**분당 트랜잭션 수**	• 산정 대상 서버에서의 분당 트랜잭션 발생 추정치의 합	-	업무수 : 2 업무당 트랜잭션수 : 4~6개
O2	**기본tpmC 보정**	• 실험환경에서 측정한 tpmC 수치를 복잡한 실제 환경에 맞게 적용하기 위한 보정	-	5
O3	**피크타임 부하 보정**	• 업무가 과중한 시간대에 시스템이 원활하게 운영될 수 있도록 피크타임을 고려한 보정	1.2 ~ 1.5	1.3
O4	**데이터베이스 크기 보정**	• 데이터베이스 테이블의 레코드 건수와 전체 데이터베이스 볼륨을 고려한 보정	1.5 ~ 2.0	1.7
O5	**애플리케이션 구조 보정**	• 애플리케이션의 구조와 요구되는 응답 시간에 따른 성능 차이를 감안한 보정	1.1 ~ 1.5	1.2
O6	**애플리케이션 부하 보정**	• 온라인 작업을 수행하는 피크타임에 일괄 작업 등이 동시에 이루어지는 경우를 감안한 보정	1.3 ~ 2.2	1.7
O7	**클러스터 보정**	• 클러스터 환경에서 장애를 대비한 보정	2-NODE : 1.4~1.5 3-NODE : 1.3	-
O8	**시스템 여유율**	• 예기치 못한 업무의 증가 등을 위한 여유율	-	1.3
O9	**시스템목표 활용율**	• 시스템의 안정적인 운영을 전제로 한 CPU 활용율	-	0.7

[참고 : CPU 용량산정 사례]

< LoRa IoT 서비스 행정기관 DB서버 CPU 용량산정 사례 >

구분		항목	산정값	산정식	산정 근거
일 발생 건수		(A)	216,000	750×12×24	사이트단말수 × 시간당 단말전송건수 × 하루시간
일 트랜잭션 처리 수		(B)	1,296,000	(A)×6	건당 트랜잭션(조회 5건, 저장 1건)
연계업무 가중 부하 보정		(C)	7,776,000	(B)×6	트랜잭션 당 연계업무 처리 건수
분당 트랜잭션 수		(D)	5,400	(C)/24/60	24시간 기준 (일일 Txn/24시간/60분)
보정계수	Peak 시 보정	(E)	10,800	(D)×2	Peak Time을 대비한 2배 보정율
	네트워크 보정	(F)	14,040	(E)×1.3	원격지 사용에 따른 시간 손실의 보정
	애플리케이션 복잡도	(G)	18,252	(F)×1.3	애플리케이션 복잡도에 의한 보정율
	DB 크기 보정	(H)	23,727	(G)×1.3	DB크기에 따른 영향 보정
	클러스터링 예비율	(I)	35,590	(H)×1.5	클러스터링을 대비한 보정 계수
	확장 예비율	(J)	53,385	(I)×1.3	시스템 확장을 고려한 보정 계수
	작업부하 보정	(K)	67,062	(J)×1.2	최대 작업 부하를 가장한 보정 계수
	기타작업 보정	(L)	113,334	(K)×1.3	On-line과 Batch 작업 동시 수행시 부하
	시스템 여유율	(M)	147,335	(L)×1.3	30% 시스템 여유율
계(tpmC)			**191,535**		서버당 tpmC(DB서버 1대 기준)

※ tpmC 참조 사이트 : http://www.tpc.org/tpcc/results/tpcc_results.asp?print=false&orderby=tpm&sortby=desc

※ tpmC = 일 발생 건수 × 일 트랜잭션처리 수 × 연계업무 가중 부하 보정 × 네트워크 보정(30%) × 피크타임 보정(50%) × I/O 부하(20%) × 년간 업무증가 및 여유율(연 20%)

이 CPU 용량산정은 Enterprise Model의 tpmC 값 191,535을 기준으로 한 행정기관 LoRa IoT 서비스 행정기관 데이터베이스 서버의 트랜잭션 량을 분석한 결과이다.

용량산정시 고려되었던 핵심 기준은 한 행정기관 당 750개의 단말이 동시에 Access 할때의 Job Load량의 Inflation이었다. 기준이 되는 일 발생 트랜잭션 처리 수(1,296,000)는 DB 엔진을 대상으로 분석한 결과 값이며, DB 크기와 트랜잭션 분석(조회 5: 저장 1건)의 비율이 적용됐다. CPU당 처리할 수 있는 분당 트랜잭션 양을 비교한 결과 750개의 단말의 대상으로 할 경우, 현재 트랜잭션의 가중한 결과 현재 CPU 사용률(Idle Time 90% 이상)을 고려해 4~8 core x86 표준 서버에서 충분이 동작할 수 있음을 알 수 있다.

물론 이런 구성이 완벽한 CPU 용량산정이라고 볼 수는 없지만, 애플리케이션 개발업체의 검증된 보정율과 하드웨어 공급사의 시스템 사양을 기준으로 최대한 객관적인 수준의 사이징을 유도했다.

나. 메모리

시스템에서 구동되는 프로세스의 수와 그 프로세스가 사용하는 메모리 크기가 메모리 산정에 큰 영향을 미친다. 따라서 프로그래밍 언어나 스레드 사용, 특정 시스템에 대한 메모리 구성 특성 등이 메모리 용량산정 변수가 될 수 있으나, 시스템의 용도와 구조를 바탕으로 단순화하여 메모리 용량을 산정하도록 한다.

메모리(MB단위)

= {시스템 영역 + (사용자당 필요메모리 × 사용자수) + 미들웨어 버퍼캐시 메모리} × 버퍼캐시 보정 × 시스템여유율

< 서버 메모리 용량산정 >

구분	산정항목	내용	적용범위	일반값
M1	**시스템 영역**	• OS, DBMS 엔진, 미들웨어 엔진, 기타 유틸리티 등의 소요 공간	-	구동 SW크기의 합으로 산정
M2	**사용자당 필요메모리**	• 애플리케이션, 미들웨어, DBMS 의 사용에 필요한 사용자당 메모리	1MB ~ 3MB	2MB
M3	**동시사용자 수**	• 소프트웨어나 시스템을 네트워크상에서 동시에 사용하는 사용자	-	CPU의 동시 사용자수와 동일
M4	**OS 버퍼캐시 보정**	• 처리 속도를 향상시키기 위해 일정량의 데이터를 임시로 모아 놓은 기억장소를 위한 보정	1.1 ~ 1.3	1.15
M5	**미들웨어 버퍼캐시 메모리**	• DBMS 의 공유메모리, WAS 의 heap size 등 미들웨어에서 사용하는 캐시영역	-	각 미들웨어의 요구에 의해 결정
M6	**시스템 여유율**	• 시스템의 안정된 운영을 위한 보정	-	1.3

※ In-memory는 위 산정기준을 적용하지 않고 실제 데이터 용량을 기준으로 적절히 산정해야 함

다. 디스크

백업 정책에 의해 디스크 요구량은 큰 차이를 가지기 때문에 데이터 백업 방안은 디스크 용량산정의 주요 고려 요소이다. 적정 디스크 용량산정을 위해 데이터의 중요도를 고려하여 상황에 적절한 백업 정책을 수립할 필요가 있다.

데이터 백업을 수행하기 위한 방법과 도구는 여러 가지가 존재하는데, 여기에서는 디스크 용량에 포함되는 백업요소로 DBMS에서 제공되는 Archive 백업과 하드웨어적인 RAID 디스크 사용에 의한 백업만을 포함한 규모산정 방안을 제시한다.

시스템디스크

= (시스템OS 영역 + 응용프로그램 영역 + SWAP 영역)
× 파일시스템 오버헤드 × 시스템디스크 여유율 × RAID 여유율

데이터디스크

= (데이터 영역 + 백업 영역)
× 파일시스템 오버헤드 × 데이터디스크 여유율 × RAID 여유율

< 서버 디스크 용량산정 >

구분	산정항목	내용	적용범위	일반값
D1	**시스템OS 영역**	• 운영체제 및 시스템 소프트웨어 등을 위한 영역	-	설치 OS크기 + 시스템SW크기 등
D2	**응용프로그램 영역**	• 미들웨어 및 응용소프트웨어 영역, 데이터베이스 설치 영역, 기타 유틸리티 설치 영역 등 응용프로그램을 대상으로 함	-	모든 설치 프로그램 크기의 합
D3	**SWAP 영역**	• 시스템 장애 시의 Dump 역할 수행과 메모리 대용의 효율적인 wapping 을 수행하기 위한 작업 공간	-	산정식*
D4	**파일시스템 오버헤드**	• 일반 사용자 관리영역을 위한 수퍼유저의 관리 공간 및 I-node Overhead, 수퍼블럭, 실린더그룹 등 파일관리 공간	-	1.1
D5	**시스템/데이터 디스크 여유율**	• 시스템의 안정된 운영을 위한 보정으로 업무의 중요도나 긴급도를 감안하여 적용	1.2 ~ 1.5	1.3
D6	**데이터 영역**	• 실제 필요한 데이터량	-	실제 필요한 데이터량 + α
D7	**백업 영역**	• 데이터와 데이터의 변경내역 정보 등의 백업을 위한 공간	-	백업정책에 의해 산정
D8	**RAID 여유율**	• RAID 디스크가 도입될 경우 데이터 보호를 위한 패러티 영역으로 사용되는 공간을 위한 보정	-	• RAID1, RAID0+1, RAID1+0 : 2.0 • RAID5 : 1.3 • RAID6 : 1.4

※ SWAP 영역 : 512M + (메모리 크기 – 256M) × 1.25

- DB암호화하는 기관은 DB암호화에 따라 추가되는 데이터 크기를 반영한 용량을 추가할 수 있음

라. 스토리지

스토리지 크기는 서버성능에 의존적이므로 서버 성능당 스토리지 성능 비율 즉, tpmC당 IOPS 비율로 설정한다. OLTP&Batch 서버는 산정된 tpmC 성능치의 2%를 IOPS로 산정하며, WEB/WAS 서버의 경우 OLTP&Batch 서버에 비해 I/O가 작으므로 tpmC 성능치 크기의 0.5%를 IOPS로 산정한다.

4. 네트워크 장비 용량 (참조 : "네트워크 구축을 위한 장비 규모산정 지침", 2017, TTA)

가. 장비군별 성능 기준

■ **접속형 L2/L3 스위치(라우터 포함)**

- L2/L3 스위치의 규모산정을 위한 성능기준은 downlink 포트수량, 업링크 포트수량, 처리량(Throughput), 패브릭 스위칭 용량(Fabric switching capacity)이 있다.

  - **처리량(Throughput)** : 장비가 패킷 손실없이 전달 가능한 최대 패킷 전송률을 말하며, 일반적으로 pps (packet per second)의 단위로 표현된다.

  - **스위칭 용량(Switching Capacity)** : 장비의 임의 포트로 입력된 패킷을 목적지 포트까지 스위칭하여 전달하는 능력을 말하며, 일반적으로 bps(bit per second) 단위로 표현된다.

■ **분배형·백본형 L3 스위치**

- 분배형/백본형 L3 스위치의 규모산정을 위한 성능기준은 처리량과 스위칭 용량이 있으며, 상기 접속형 L2/L3 스위치의 정의와 각각 동일하다.

■ **L4/L7 장비(보안장비 포함)**

- L4/L7 장비의 규모산정을 위한 성능기준은 TCP 처리량과 동시세션수(CS, Concurrent sessions)가 있다.

  - **TCP Throughput(처리량)** : TCP 프로토콜을 통해 전송 가능한 최대 데이터양을 의미하며, 일반적으로 bps 단위로 표현된다.

  - **동시세션수** : 장비가 동시에 유지할 수 있는 최대 TCP 세션의 수를 말한다.

나. 보정 계수 및 보정 값

다양한 유형의 트래픽을 처리하는 네트워크 장비에서 일률적으로 적용할 수 있는 보정 값을 산정하기가 어려우므로 각 유형별 특성을 반영한 보정 수치를 “보정 계수”라 명칭하고, 모든 접속포트의 보정 계수를 산정·합산하여 평균한 값을 “보정 값”으로 정하였다. 행정기관에서 서비스별 이용량의 조사·분석 결과를 기반으로 보정 값을 산정하도록 권장하지만, 이용량 산정이 어려울 경우에 사용할 수 있도록 아래 표를 참조할 수 있다.

< 주요 서비스별 소요 대역폭 및 보정계수 >

주요서비스 종류 (A)	단위 (B)	크기 [대표크기] (C)	희망 응답시간 (D)	요구 대역폭 (E)	보정계수	
					FE (F)	GbE (G)
일반업무(WEB기반) **인터넷검색 포함**	건	수백KB~수MB [10MB]	3초	27Mbps	0.3	0.03
문서전송을 포함한 범용서비스 메일/문서시스템 등	건	수백KB~수십MB [100MB]	10초	80Mbps	0.8	0.08
전화(인터넷전화)	통화	64Kbps [100Kbps]	실시간	100Kbps	0.001	0.0001
보안 업데이트	건	수백KB~수MB [10MB]	3초	27Mbps	0.3	0.03
FullHD영상 (HEVC/H.265~MPEG4/H.264) **영상회의/CCTV 등**	채널	4.5M~9Mbps [10Mbps]	실시간	10Mbps	0.1	0.01
3D지도검색 지역/각도 대한 크기차이	건	10MB~60MB [60MB]	10초	48Mbps	0.5	0.05
무선LAN(Wi-Fi) **AP장치 접속용**	대	802.11n [15M~150Mbps] 802.11ac [88M~867Mbps]	실시간	150Mbps 867bps	- -	0.15 0.87

다. L2/L3 스위치(라우터 포함) 용량 산정

일반적으로 접속형 L2/L3 스위치의 규모는 접속되는 단말 수에 의한 다운링크의 포트수와 각 단말에 제공할 Bandwidth와 업링크의 용량 및 이중화 제공(Link Aggregation, VRRP, 회선 이중화 등)을 위한 소요포트 여부에 따라 결정된다. 또한, 접속형 L2/L3 스위치의 다운링크에는 단말기뿐만 아니라, 무선 AP와 같은 분배스위치 역시 접속될 수 있다.

< L2/L3 스위치 용량산정 >

구분	항목	내용	입력값 범위	일반값
1	다운링크 포트용량	필요 포트의 이론적 최고 용량	1 ~ XXX	1 Gbps
2	소요 다운링크 포트 수	다운링크에 활용되는 포트 수의 총합	1 ~ XXX	
3	다운링크 확장계수	다운링크의 향후 사용이 예상되는 포트 수	100% ~ 200%	120%
4	다운링크 안정성 계수	예기치 못한 네트워크 증가 및 시스템의 안정된 운영을 위한 여유률	100% ~ 150%	120%
5	다운링크별 보정계수	"표_ 주요 서비스별 소요대역폭 및 보정계수" 참고	0 ~ 1	**0.1**
6	업링크 포트 이중화	이중화 구현 기술에 따른 소요 포트 비율	100% ~ 200%	200%
7	이론적패킷처리상수	1GE 에서 이론적인 최대 패킷 처리 상수		1,488,095
8	양방향 상수	Tx/Rx를 고려한 양방향 상수		2
산정식		• 다운링크 포트 전체 수량 = 다운링크 소요 포트 수 × 다운링크 확장계수 × 다운링크 안정성 계수 • 업링크용량 = 다운링크 포트용량 × 다운링크 포트 전체 수량 × 다운링크별 보정계수 {업링크 단위용량, 업링크 포트수량} = F(업링크 용량) 업링크 포트 전체 용량 = 업링크 포트수량 × 업링크 포트별 단위용량 • 스위칭 용량 = {∑(i의 이론적 최대 용량 × i의 포트 수량)} × 양방향 상수 단, i ∈ 다운링크 & 업링크 I/O 인터페이스 종류 = {10/100 Base Tx, 100/1000 Base Tx, 1000 Base Fx 등} • Throughput = {∑다운링크 & 업링크인터페이스 타입별 용량(i)} × 이론적 패킷 처리상수		

※ (단, {A, B} = F(x)는 x를 처리할 수 있는 최소 Interface의 단위 용량과 포트 수를 나타내며, 최소 Interface의 단위 용량은 ISP나 특정 요구에 따라 Upgrade 될 수 있음)

라. 분배형 · 백본형 L3 스위치 용량 산정

분배형・백본형 L3 스위치의 트래픽 특성은 Burst하기 보다는 지속적인 양을 유지하는 형태다. 많은 곳의 트래픽이 모이는 특성상 장비의 이중화, 인터페이스의 이중화, 이중화 지원방식(N+1 or 1 : 1 등) 및 안정성 등이 특히 중요하므로 이중화 지원 및 시스템 확장을 위한 여유율 등을 고려하여야 한다.

< 분배형·백본형 L3 스위치 용량산정 >

구분	항목	내용	입력값 범위	일반값
1	Interface 종류별 최대 포트용량	필요 포트의 이론적 최고 용량	1 ~ XXX	Interface의 종류에 따라 다름
2	Interface 종류별 포트 수	해당 인터페이스 종류에 활용되는 포트 수의 총합(이중화 소요 포트 수 포함)	1 ~ XXX	
3	시스템 확장계수	향후 확장이 예상되는 인터페이스의 비율	100% ~ 200%	120%
4	시스템 안정성계수	예기치 못한 네트워크 증가 및 시스템의 안정된 운정을 위한 여유률	100% ~ 150%	120%

구분	항목	내용	입력값 범위	일반값
5	이론적패킷처리상수	1GE 에서 이론적인 최대 패킷 처리 상수		1,488,095
6	양방향 상수	Tx/Rx를 고려한 양방향 상수		2
산정식		• 스위칭 용량 = {∑(인터페이스 종류별 최대 용량 × 인터페이스 종류별 포트 수)} × 시스템 확장계수 × 시스템 안정성계수 × 양방향 상수 • Throughput = {∑(인터페이스 종류별 최대 최대용량 × 인터페이스 종류별 포트 수)} × 시스템 확장계수 × 시스템 안정성계수 × 이론적 패킷 처리상수		

※ (단, 시스템 확장계수는 과거 3년간 시스템 증가율이 있는 경우, 이를 대체할 수 있음)

마. L4/L7장비(보안장비 포함) 용량 산정

공통적으로 적용할 수 있는 여러 L4 성능 지표 중에서 가장 일반적으로 사용되는 TCP Throughput, CPS(Connection Per Second), TPS(Transaction Per Second), CS(Concurrent Session) 등을 활용할 수 있지만, CPS와 TPS는 In-Line 모드로 적용되는 장비의 경우 업체의 구현현황에 따라 다르게 적용될 수 있으므로 해당 지표를 제외하고, TCP Throughput과 CS를 활용하여 해당 장비군의 규모를 산정 한다.

TCP Throughput은 L2 헤더 정보까지를 포함하기로 하며, 양방향을 합산한 결과 값으로 정의한다. 해당 장비군을 운영한 통계치가 존재하는 경우, 과거 Peak치에 대한 통계치를 활용하고, 신규 도입인 경우에는 시스템 관리자나 기획자가 목표하는 서비스를 기준으로 성능 규모를 산정한다.

< L4/L7장비 용량 산정 >

구분	항목	내용	입력값 범위	일반값
1	최근 1년간 최대 동시세션수	최대 동시 TCP 세션 수	0 ~ xxx	통계치
2	과거3 개년 동시세션수의 평균증가율	과거 3개년 동시세션 수 평균 증가율	0 ~ xxx	통계치
3	세션별 평균데이터량	세션별로 전송되는 데이터의 평균값	1 ~ xxx	통계치
4	시스템 확장 고려상수	향후 확장이 예상되는 비율	100 ~ xxx	120
산정식		• 목표 동시세션수 = 최근 1년간 최대 동시세션수 × 과거3개년 동시세션수 평균 증가율(1+α) • TCP Throughput = 목표 동시세션수 × {세션별 평균데이터량/세션별 평균유지시간(sec)} × 시스템확장 상수(1.2)		

제2장

정부사물인터넷 네트워크 구축기준

제1절 네트워크 구성 모델

정부사물인터넷은 ❶디바이스↔게이트웨이, ❷게이트웨이↔네트워크서버, ❸네트워크서버↔애플리케이션서버 등 3개의 주요 네트워킹 구간을 가지며, 네트워킹에 적용된 통신방식과 망 구성방식으로 도입 모델을 분류할 수 있다.

정부사물인터넷의 도입 모델은 IoT디바이스와 이와 접속하는 게이트웨이 장비 간의 통신방식*을 기준으로 6가지로 분류하고, 게이트웨이 이후 네트워크 서버와 애플리케이션 서버 간의 TCP/IP망 구성방식**에 따라 9 가지로 분류한다.

* 디바이스와 게이트웨이 간 통신방식은 디바이스-게이트웨이 간 전송거리와 사물인터넷 서비스 커버리지에 따라 장거리·근거리 등의 통신기술 및 자체망·상용망 등의 망 구성방식을 가지며,

** 네트워크서버는 여러 게이트웨이 트래픽을 집선하고, 애플리케이션서버는 여러 사물인터넷 서비스를 담당할 수 있으므로 구성방식에 따라 각기 구축하는 위치에 차이가 있다.

< 정부사물인터넷 도입모델 현황 >

구분	네트워킹 구간 구분	
	디바이스❶↔게이트웨이	게이트웨이❷↔네트워크❸↔애플리케이션
통신기술 및 구성방식	• **저전력 광대역 통신방식** : LPWA - LoRa, NB-IoT, LTE-M, Sigfox • **근거리 무선 통신방식** - BLE, ZigBee/Z-Wave, WiFi	• **유·무선 TCP/IP 통신방식** - 자체망, 정부공통망, 상용망

제공하고자 하는 사물인터넷 서비스 모델 및 환경, 보유 자원 및 재원, 추진 로드맵 등을 고려하여 도입 모델을 선택할 수 있다. 도입 모델은 추진 단계와 장기 비전에 따라 다양하게 적용될 수 있고, 발전적으로 변화할 수 있는 등 유기적으로 진화가 가능하다.

1. 디바이스 네트워크 구성 모델(6종류)

: 디바이스와 게이트웨이 간 네트워킹 모델

디바이스는 댁내・안심존・교량 등 특정장소에 고정(고정형)되어 있는 경우도

있지만, 장소에 상관없이 이동(이동형)할 수 있으며, 일례로 치매환자용 웨어러블 디바이스의 경우 댁내에 있을 수도 있고 거리를 배회할 수도 있다.

디바이스와 게이트웨이 간 네트워킹은 서비스 형태에 따라 고정형·이동형·혼합형을 고려해야 하며, 이동형 서비스의 경우 지역한계를 벗어나는 경우에도 서비스가 가능하도록 지역 간 연계도 고려해야 한다. 정부사물인터넷 망 구성 모델은 아래와 같이 6 종으로 분류된다.

< 디바이스 네트워크 구성 모델 >

구성 모델		행정기관 구축·운영 여부				비고
번호	모델명	Dev	GW	NS	AS	
모델1	**자체 LPWA망 활용**	O	O	O	O	자체 LoRa 망 운영
모델2	**통신사 IoT서비스 활용**	O	×	×	O	IoT망과 IoT플랫폼을 상용서비스 활용
모델3	**통신사 IoT망 활용**	O	×	O	O	LoRa, NB-IoT, LTE-M 등
모델4	**Sigfox 사물인터넷망 활용**	O	×	×	O	Sigfox 서비스 활용
모델5	**근거리 사물인터넷망 활용**	O	O	O	O	BLE, ZigBee/Z-Wave 방식
모델6	**WiFi 통신방식 활용**	O	O	O	O	무선 AP를 활용한 WiFi 방식

※ Dev : IoT디바이스, GW : 게이트웨이, NS : 네트워크 서버, AS : 애플리케이션 서버

고정형 서비스의 정부사물인터넷 망 구성 모델은 “5·6” 번, 이동형 서비스는 “1 ~ 4” 번이 적합하다. 해당 모델 중에서 서비스와 환경에 맞게 선택 도입하지만, 여러 모델을 혼합 도입해야 할 경우도 있다. 예를 들어 치매환자 돌봄과 같은 혼합형 서비스의 경우 댁내에는 “6” 번 또는 “5·6” 번을 동시 적용, 거리배회 감시는 “1” 번, 타 지역 이동에 따른 서비스 연속성을 위해서는 “3” 번 모델까지 혼용 구성해야 한다.

<모델1> 자체 LPWA망 활용

- **(개요)** 비면허 대역 LoRa기반의 LoRaWAN 구현으로 행정기관이 구현한 대표적인 사례이며, 향후 정부사물인터넷 망의 공통기반에서 채택할 대표 표준 모델
- **(데이터 흐름)** LoRa IoT디바이스(자가) → LoRa GW(자가) → NW서버(자가) → AS 서버(자가) → 사물인터넷서비스 순으로 데이터 전달

< 자체 LPWA망(LoRa 기반) 활용모델 운영 개요 >

구분	구간	적용 기술
연계표준	디바이스 ↔ 네트워크 서버	LoRaWAN 1.1
	네트워크 서버 ↔ 애플리케이션 서버	oneM2M ReleAES 1
보안	디바이스 ↔ 네트워크 서버	AES-128·256 보안
	네트워크 서버 ↔ 애플리케이션 서버	TLS 1.2, IPSec 보안
인증	LoRa GW ↔ 네트워크 서버	VPN 인증
	네트워크 서버 ↔ 애플리케이션 서버	OAuth 2.0 인증
운영 개념도		

<모델2> 통신사 IoT서비스 활용

- **(개요)** 통신 사업자가 제공하는 면허대역 전역 무선망 및 통신사 플랫폼을 이용하는 IoT 정보를 수신하고 통신사 플랫폼이 전용망을 통해 행정기관의 애플리케이션 정보를 전달하여 서비스 제공
  - 통신사의 IoT 망을 활용하므로 전국 로밍 지원은 기본이지만, 행정기관은 통신사의 IoT 플랫폼 서비스 가입이 필요
  - 면허대역 LPWA 통신 방식 : LTE-M, NB-IoT
- **(데이터 흐름)** LoRa IoT디바이스(자가, 통신사 등록) → 기지국(통신사) → 상용플랫폼(통신사) → AS서버(자가) → 사물인터넷서비스 순으로 데이터 전달

< 통신사 IoT서비스 활용 모델 운영 개요 >

구분	구간	적용 기술
연계표준	디바이스 ↔ 통신사플랫폼	LoRaWAN, NB-IoT, LTE-M
	통신사플랫폼 ↔ 애플리케이션 서버	oneM2M, OCF, 통신사 표준
보안	디바이스 ↔ 통신사플랫폼	통신사 보안
	통신사플랫폼 ↔ 애플리케이션 서버	TLS 1.2, IPSec 보안
인증	디바이스 ↔ 통신사플랫폼	통신사 단말 인증
	통신사플랫폼 ↔ 애플리케이션 서버	통신사 플랫폼 인증
운영 개념도		

<모델3> 통신사 IoT망 활용

- **(개요)** 정부사물인터넷망을 LoRaWAN 자체망 대신 통신사업자가 제공하는 면허대역 IoT망으로 구성하는 모델로써, 모델1과 유사하게 구현가능(통신사 협의필요)
  - 통신사의 전국망을 활용하므로, 지역 간 단말 이동에 대한 로밍이 기본 제공
- **(데이터 흐름)** IoT디바이스(자가, 통신사 등록) → 통신사 IoT망 → NW서버(자가) → AS서버(자가) → 사물인터넷서비스 순으로 데이터 전달

< 통신사 IoT망 활용모델 운영 개요 >

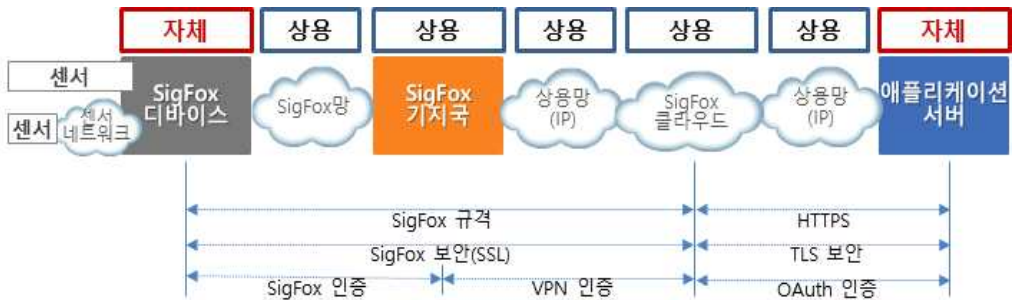
구분	구간	적용 기술
연계표준	디바이스 ↔ 통신사 IoT망	LoRaWAN 1.1
	네트워크 서버 ↔ 애플리케이션 서버	oneM2M, ReleAES
보안	디바이스 ↔ 네트워크 서버	AES-128·256 보안
	네트워크 서버 ↔ 애플리케이션 서버	TLS 1.2, IPSec 보안
인증	디바이스 ↔ 네트워크 서버	통신사 인증
	네트워크 서버 ↔ 애플리케이션 서버	OAuth 2.0 인증
운영 개념도		

<모델4> Sigfox 사물인터넷망 활용

- **(개요)** 개념적으로는 LoRaWAN과 유사한 구조를 가지고 있으나, Sigfox는 통신사 서비스 방식으로만 운영 가능
- **(데이터 흐름)** Sigfox디바이스(자가) → Sigfox기지국(서비스사업자) → Sigfox클라우드(서비스사업자) → AS서버(자가) → 사물인터넷서비스 순으로 데이터 전달

< Sigfox 사물인터넷망 활용모델 운영 개요 >

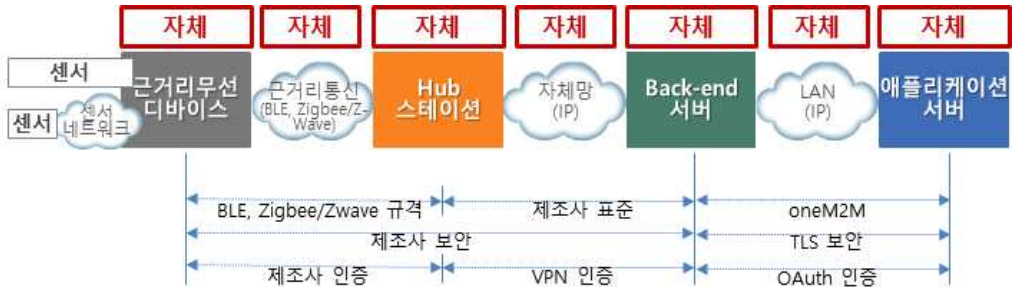
구분	구간	적용 기술
연계표준	Sigfox디바이스 ↔ Sigfox Back-end 서버	Sigfox 표준
	Back-end 서버 ↔ 애플리케이션 서버	HTTPS
보안	Sigfox디바이스 ↔ Back-end 서버	Sigfox 보안 (SSL)
	Back-end 서버 ↔ 애플리케이션 서버	TLS 1.2, IPSec 보안
인증	Sigfox디바이스 ↔ Sigfox 기지국	Sigfox 인증
	Sigfox 기지국 ↔ Sigfox 클라우드	VPN 인증
	Sigfox 클라우드 ↔ 애플리케이션 서버	OAuth 2.0 인증

구분	구간	적용 기술
운영 개념도		

<모델5> 근거리 사물인터넷망 활용

- **(개요)** BLE, ZigBee/Z-Wave 등의 근거리 무선 통신기술을 활용하여 구현된 모델
  - WiFi도 근거리 무선 통신기술의 일종이지만, WiFi는 기본적으로 IP기반이라는 점을 고려하여 별도의 모델(모델6)로 분리하였음
  - 모델1의 LoRa 통신을 근거리 무선 통신기술로 대치하는 것으로 Hub Station이 LoRa 게이트웨이 역할을 수행하게 됨
- **(데이터 흐름)** 근거리 무선디바이스(자가) → Hub Station(자가) → Back-end서버 → AS서버(자가) → 사물인터넷서비스 순으로 데이터 전달

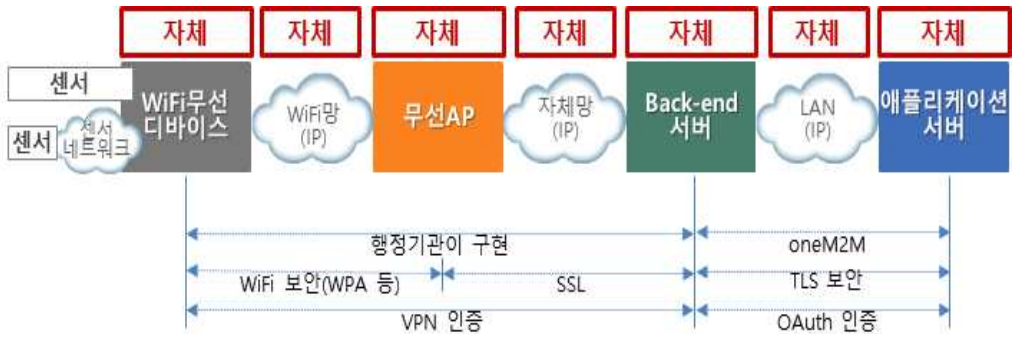
< 표 별첨2-5 : 근거리 사물인터넷망 활용모델 운영 개요 >

구분	구간	적용 기술
연계표준	근거리무선 디바이스 ↔ Hub 스테이션	BLE, Zigbee/ZWave 표준
	Hub 스테이션 ↔ Back-end 서버	제조사 표준
	Back-end 서버 ↔ 애플리케이션 서버	oneM2M ReleAES 1
보안	근거리무선 디바이스 ↔ Back-end 서버	제조사 보안
	Hub 스테이션 ↔ Back-end 서버	VPN 보안
인증	근거리무선 디바이스 ↔ Hub 스테이션	제조사 인증
	Hub 스테이션 ↔ Back-end 서버	VPN 인증
	Back-end 서버 ↔ 애플리케이션 서버	OAuth 2.0 인증
운영 개념도		

<모델6> WiFi 통신방식 활용

- **(개요)** 사물인터넷망을 WiFi 기반으로 구성하는 모델
  - 게이트웨이가 컴퓨팅 능력을 가진 장비가 아닌 네트워크 장비(무선AP)로 구현 가능한 장점이 있으나, 향후 종단 컴퓨팅 환경(Edge Computing 또는 Fog Computing)으로 진화에 제약이 될 수 있음
- **(데이터 흐름)** WiFi무선 디바이스(자가) → 무선AP(자가) → Back-end서버 → AS서버(자가) → 사물인터넷서비스 순으로 데이터 전달

< WiFi 통신방식 활용모델 운영 개요 >

구분	구간	적용 기술
연계표준	WiFi무선 디바이스 ↔ Back-end 서버	행정기관이 구현
	Back-end 서버 ↔ 애플리케이션 서버	oneM2M ReleAES 1
보안	WiFi무선 디바이스 ↔ 무선 AP	WiFi 보안 (WPA 등)
	AP ↔ Back-end 서버	SSL
	Back-end 서버 ↔ 애플리케이션 서버	TLS 1.2, IPSec 보안
인증	WiFi무선 디바이스 ↔ Back-end 서버	VPN 인증
	Back-end 서버 ↔ 애플리케이션 서버	OAuth 2.0 인증
운영 개념도		

2. 백홀 네트워크 구성 유형(9종류)

: (백홀)게이트웨이와 네트워크서버, (백엔드)네트워크서버와 애플리케이션서버 간 네트워킹 모델

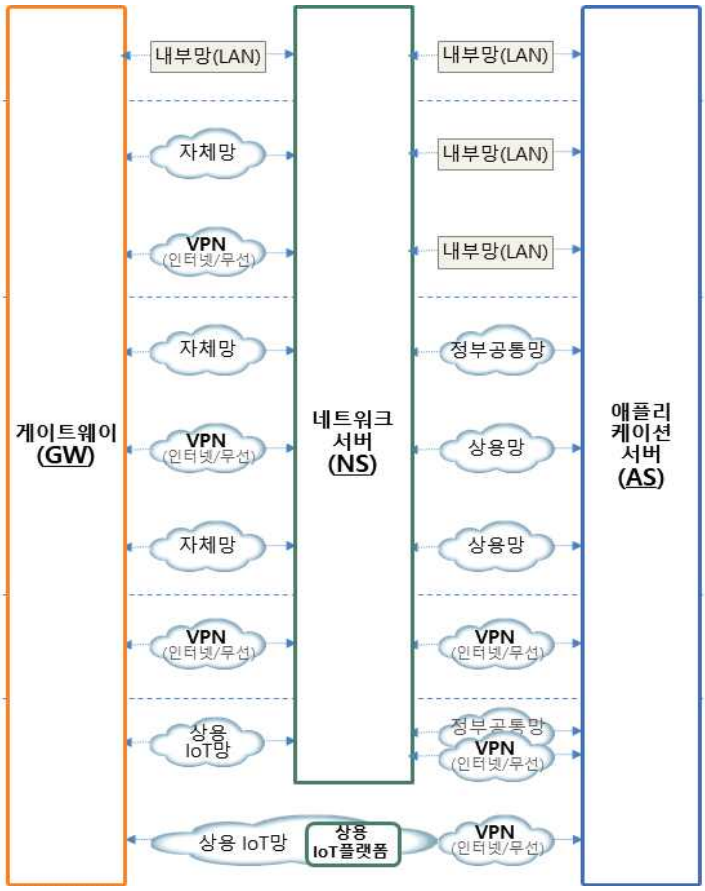
정부사물인터넷 망과는 달리 서비스플랫폼 구성은 TCP/IP 통신방식(IP망)을 통하여 상호 접속되는 단순한 구조이다. 하지만 플랫폼은 서비스 트래픽이 모이는 센터 역할을 하므로 구성방식에 따라 중앙집중 또는 분산집중 형태로 구축된다. 따라서 구성 모델은 서버의 구축 위치와 서버간 네트워킹을 위한 통신망의 종류에 따라 9종의 도입 모델로 분류할 수 있다.

< 백홀 네트워크 구성 유형 >

구성 유형		유형 번호	망 종류		설치 위치		
			GW↔NS	NS↔AS	GW	NS	AS
동일 위치내 운영		유형1	LAN	LAN	동일 위치		
게이트웨이가 원격지에 위치		유형2-A	자체망	LAN	원격	동일 위치	
		유형2-B	상용망(VPN)	LAN	원격	동일 위치	
모든 서버가 서로 다른 위치	WAN 혼용	유형3-A	자체망	정부공통망	원격	원격	원격
		유형3-B	상용망(VPN)	상용망	원격	원격	원격
		유형3-C	자체망	상용망	원격	원격	원격
	WAN 통일	유형4	상용망(VPN)	상용망(VPN)	원격	원격	원격
상용 플랫폼을 활용하는 경우		유형5-A	상용사물인터넷망	상용망(VPN)·정부공통망	원격	원격	원격
		유형5-B	상용 사물인터넷 서비스		원격	원격	원격

※ LAN=내부 로컬망, WAN=외부망 : 자체망·정부공통망·상용망=전용회선·상용망(VPN)=인터넷or무선
※ GW : 게이트웨이, NS : 네트워크 서버, AS : 애플리케이션 서버

< 정부사물인터넷 백홀 네트워크 구성유형 개요 >

유형 번호	구성도	비고
유형1		• GW·NS·AS가 모두 동일위치에 설치되어 LAN으로 연결
유형2-A 유형2-B		• NS·AS는 동일위치, GW는 원격지(디바이스 인근위치 등)에 설치된 경우이며, • GW와 NS는 WAN, NS와 AS는 LAN으로 연결
유형3-A 유형3-B 유형3-C		• GW·NS·AS가 모두 다른 위치에 설치되어 WAN으로 연결하며, • WAN은 연결환경에 따라 자체망·정부공통망·상용망 등 혼용하여 구성
유형4		• "유형3"과 같으나 WAN을 VPN으로 통일한 경우
유형5-A 유형5-B		• 통신사 제공, 상용IoT망을 이용하거나, 상용IoT서비스(플랫폼)로 운영되는 유형 • "2. 정부사물인터넷 망 구성" 모델3=A형, 모델2·4=B형에 해당

제2절 네트워크 구축 고려사항

1. 서비스 특성 고려사항

정부사물인터넷을 위한 네트워크를 구축하기 전에 우선적으로 서비스 종류, 이동성 등 서비스 특성에 따라 네트워크 인프라 구축 기술, 비용 등일 달라지므로 어떤 서비스를 제공할 것인지를 먼저 결정해야 한다.

가. 서비스 특성 분류

정부사물인터넷 서비스는 사용량을 측정하는 미터링(Metering or Telemetering), 위치를 추적하는 트래킹(Tracking), 상황에 대한 모니터링 & 제어, 헬스케어 등으로 구분할 수 있다. 각 서비스의 특성 및 서비스 예를 정리하면 아래와 같다.

< IoT 서비스 분류 예시 >

구분	설명	이동성	서비스 예시
미터링	사람이 수작업으로 진행하던 검침을 자동화하여 수작업으로 인한 오류를 최소화하고 인건비 절감 효과 발생	낮음	• 가스 검침 • 수도 검침 • 전력 검침
트래킹	웨어러블 형태의 소형 통신 모듈을 사람 또는 사물(애완동물, 고가상품, 자동차 등)에 부착하여 정확한 위치를 파악하는 디바이스로 아동, 여성, 치매노인의 경우 사고 예방 및 긴급 상황에서 빠른 대응이 가능	높음	• 물류 관제 • 약자 보호 • 위치기반 정보 안내
모티터링 & 제어	원거리 시설물이나 지하시설물과 같이 상태를 모니터링하거나 원격제어가 힘든 시설물들에 적용, 지속적인 상태 모니터링 및 원격제어가 가능	낮음	• 온/습도 측정 • 스마트 조명 • 독성 가스 측정 • 지하시설물 관제 • 축산물 관리
헬스케어	주기적으로 각종 건강정보 수집하고 수집한 데이터를 기반으로 건강상태를 체크할 수 있으며, 주로 근거리 접속 기술을 사용	중간	• 혈압계 • 혈당계 • 심박 측정기

서비스의 분류에 따라서 이동성 및 데이터의 보안성 등에 차이가 있을 수 있다. 또한, 동일한 분류의 서비스들도 데이터의 특성이나 전송주기에 따라서 필요로 하는 접속 기술이나 고려사항 등이 달라질 수 있다.

나. 데이터 특성 분류

사물인터넷 네트워크는 송·수신되는 데이터의 특성에 따라 사용되는 무선 기술, 백홀의 용량 등이 달라질 수 있으므로 제공하는 서비스가 어떤 데이터 특성을 가지는지를 결정해야 한다.

< 데이터 특성에 따른 분류 예시 >

구분	데이터 특성	서비스 예시	접속 기술
미션 크리티컬 데이터 전송서비스	• 무중단 서비스 • 많은 데이터양 • 높은 실시간성 • 모니터링 + 제어 • 높은 네트워크 안정성 • QoS보장 • 높은 보안성	• 커넥티드 카 • 자율주행 차 • 커넥티드 CCTV	이동 통신망 서비스 (LTE, 3G 등)
대용량 데이터 전송서비스 (대량형)	• 전송 데이터양 많음 • 실시간 모니터링 • QoS 보장 • 빠른 데이터 전송 속도	• 공장 자동화 • 차량 공유 서비스 • 스마트 교통 시스템 • 재난 방송 • 전자결재	LTE-M Cat1
소용량 데이터 전송서비스 (소물형)	• 전송 데이터양 적음 242 byte이하 • 비실시간성 • 변화적은 데이터 • 데이터 수집	• 스마트 홈 • 물자관리 • 보안등/가로등 제어 • 미아/치매노인 위치 관제 • 원격검침 • 지하시설물 관제	LoRa, NB-IoT 등

□ 미션 크리티컬 데이터 전송서비스

데이터양이 많고, 실시간으로 모니터링 및 제어가 되어야 하는 서비스로, 서비스의 중단 발생시 심각한 인명 또는 재산피해가 발생될 수 있으므로 서비스의 안정성 및 신뢰성을 최우선적으로 고려해야 서비스에 해당된다.

[주요 고려사항]

- **망의 안정성·신뢰성 확보 여부**
  - 어떠한 경우에도 통신이 가능해야 한다.
- **데이터의 실시간 전송 여부**
  - 수집된 데이터는 실시간으로 전송되어 판단 및 조치가 가능해야 한다.

- **실시간 제어 가능 여부**
  - 수집 데이터를 기반으로 실시간 제어나 안내가 가능해야 한다.

□ 대용량 데이터 전송서비스

대용량 전송이 가능한 무선기술을 적용해야 하는 대량형 서비스로 데이터 전송 주기가 짧고, 전송 데이터의 크기가 50KB 이상인 서비스이며, 데이터 유실에 민감한 특성이 있는 서비스가 해당된다.

[주요 고려사항]

- **대역폭 보장 여부**
  - 데이터 유실이 발생하지 않아야 한다.
- **데이터의 준 실시간 전송 여부**
  - 데이터의 전송 지연이 적어야 한다.

□ 소용량 데이터 전송서비스

소용량 전송이 가능한 무선기술을 사용해야 하는 소물형 서비스로 데이터 전송 주기가 길고, 전송 데이터의 크기가 242Byte 이하이며, 데이터 유실에도 크게 영향이 없는 서비스가 해당된다.

[주요 고려사항]

- **배터리 수명**
  - 배터리 수명이 5 ~ 10년을 보장해야 한다.

다. 이동성에 따른 분류

특정한 장소에 디바이스가 설치되어 이동이 없이 사용되는 고정형 서비스와 디바이스가 상황에 따라 수시로 이동하여 사용되는 이동형 서비스로 분류할 수 있다. 이러한 서비스의 이동성에 따라 전원공급 방식, IoT 네트워크 구축 수량 등이 달라질 수 있다

< 이동성에 따른 분류 예시 >

구분	설명	서비스 예시	접속 기술
고정형	o 특정한 장소에 디바이스가 설치되어 이동이 없는 서비스를 의미하며 통상적으로 상전을 사용하고, 배터리는 정전 발생시 백업 전원으로 사용	검침	가스검침, 수도검침, 전력검침 등
		보안	CCTV 관제, 출입문 관제, 출입자 관리 등
		공장 자동화	생산라인 관리, 공조시스템관리 등
	o 상전 사용이 불가하거나 서비스 유형상 전원을 배터리로 공급하여야 하는 경우, 배터리는 교체 및 충전이 가능하여야 하며, 배터리의 수명은 최대 5~10년 이상이어야 함	에너지 관리	빌딩에너지관리, 조도관리, 공조시스템관리 등
		시설물 관리	지하시설물관리, 가로등 관리 등
이동형	o 이동성이 높은 사물에 디바이스를 설치하여 사물의 정보를 관제하는 서비스로 배터리를 사용하여 전력이 공급되는 경우가 많음 o 배터리는 장기간 사용이 되어야 하므로 교체 및 충전이 가능하거나 최대 5~10년의 배터리 사용이 가능하여야 함	트랙킹	세이프와치, 애완동물 관리, 물류관리, 차량관제 등
		헬스케어	심장박동계, 혈당계, 체중계 등

□ 고정형 서비스의 고려사항

- **상시전원(이하"상전"이라한다) 공급 여부**
  - 고정형 서비스의 경우에는 일반적으로 상시 전원을 공급한다.
  - 위치 특성상 상시전원의 공급이 어려운 경우, 배터리를 사용하며, 배터리 수명은 최대 5 ~ 10년을 보장해야 한다.
- **무선망 안전성 확보**
  - 지하, 건물 중심부, 승강기 내부 등과 같이 약전계 영역에 디바이스를 설치할 경우 디바이스의 무선 출력을 전파법 규정 내에서 상향 조정한다.
  - 전파 출력의 상향 조정으로도 망의 신뢰성 확보가 어려운 경우에는 Pico G/W등의 추가를 통해 망의 안정성을 확보해야 한다.

□ 이동형 서비스의 고려사항

- **배터리 수명**
  - 이동형 서비스의 경우, 상전의 공급이 어려움으로 배터리 수명에 대한 이슈가 크다.

- 원활한 서비스를 위해서는 약 5 ~ 10년의 배터리 수명을 보장해야 한다.

• **전국망 서비스 여부**

- 이동형 서비스의 경우, 동일한 Network Server를 사용하는 네트워크상에서는 서비스의 제공이 가능하나, 전국을 대상으로 한 이동형 서비스 제공이 필요한 경우에는 Network Server 간의 이동성 제공을 위한 처리가 필요하다.
- 전국망 서비스가 필요한 경우에는 사업자가 구축한 IoT망을 임대하여 사용하는 것을 권장한다.

2. 지역적 특성 고려사항

국가기관이 IoT 네트워크를 구축하기 위해서는 지역적 특성을 우선 고려하여야 한다. 지역적인 특성은 도심과 농·어촌 지역으로 구분할 수 있다.

< 지역적 특성 비교 >

항목	도심지역	농어촌 지역
지역적 특성	인구 10만 이상의 도시	인구 10만 미만의 읍면동
	인구밀집 지역 또는 5층 이상의 건물이 다량 분포되어 있는 지역	논밭 등으로 구성된 개활지 및 바다, 호수 등이 있으며 5층 이하 건물들이 다량 분포된 지역
전파 방해 요소	높음	낮음
	• 고층건물에 의한 전파방해 • 지하시설물에 디바이스 설치 시 전파 전송 불가 • 같은 주파수 대역 사용 생활기기 (무선 마이크, 무선 전화기 등)	• 산에 의한 전파 방해 • 호수 및 바다 등 물에 의한 전파 방해
커버리지	좁음	넓음
	고층건물 등의 전파 방해로 커버리지 좁음	개활지 등으로 인해 커버리지 넓음
백 홀 망 연동	용이	어려움
	통신사 상용인터넷, 통신사 무선망, 자체망	
전력 공급	용이	어려움
	도심지역 건물 내 설치 시 전력 공급 용이	야대지 또는 개활지에 설치 시 전력선 포설 등 전력공급 어려움

가. 공통 고려사항

도시지역과 농어촌 지역에 구분 없이 공통으로 확인해야 할 고려사항은 아래와 같다.

< 지역적 특성 공통 고려사항 >

항목	고려사항
전원	• 220V 전원공급 가능 여부 • 전력선 포설 용이성 • 일정한 전압공급 유무 • 백업 전원공급 장치 (발전기, UPS 등) 유무
백홀	• 유선 백홀 사용 시 백홀 용 케이블 포설 용이성 • 무선 백홀 사용 시 3G/LTE 수신감도
접근성	• 설치 및 유지보수를 위한 출입용이성 • 장소의 보안장비 (경비원, 출입문 잠금장치, CCTV 등) 유무

나. 도심 지역에서의 고려사항

도심지역에서는 고층건물 및 옥외 광고물들에 의한 전파 방해요소와 건물 지하 및 승강기내부 등 다양한 전파 방해 요소에 대한 고려가 우선 이루어져야 한다.

< 도심 지역 고려사항 >

항목	고려사항
전파방해 요소	• 고층건물에 의한 전파 방해 • 옥외 광고물에 의한 전파 방해 • 지역 내 900MHz 생활기기 (무선 마이크, 무인주차 차단기, 무선전화기 등)의 밀집도 • 지하실 또는 승강기 내 수신감도

다. 농어촌 지역에서의 고려사항

농어촌 지역의 경우 백홀 연결과 전원공급에 대한 사항이 중요 고려사항으로 백홀망 연결이나 전원공급이 어려운 경우에 대한 대응방안이 전제되어야 한다.

또한, 전파 방해요소의 경우 농어촌 지역은 도심과 다르게 산이나 호수, 강, 바다 등 자연적인 지형에 의한 방해요소들에 대한 고려가 선행되어야 하고, 설치 위치가 산이나 논밭 등 접근이 용이하지 않을 수 있다.

< 농·어촌 지역 고려사항 >

항목	고려사항
전파방해 요소	• 산에 의한 전파 방해 • 호수, 강, 바다에 의한 전파 반사 및 흡수
전원	• 공통 고려사항을 포함 • 신규 설치장소에 220V 전원공급 불가 시 발전기, 태양열전원 공급 가능 여부 • 태양열 발전 사용시 관련 기기에 대한 상태 감시 및 1일 이상의 사용이 가능한 축전지 용량
백홀	• 무선 백홀 사용 시 3G/LTE 수신감도 • 3G/LTE 연동이 어려울 경우, Wi-Fi 백홀를 사용한 연동 고려
접근성	• 기지국이 산이나 논/밭 등에 설치될 수 있으므로 접근 용이성 체크 필수

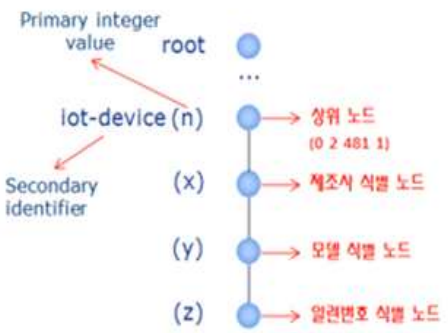
3. 디바이스 식별 고려사항

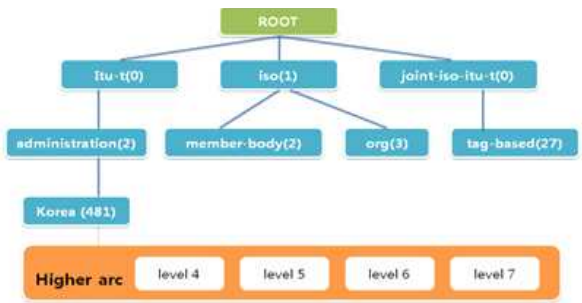
가. 디바이스 식별 표준

□ oneM2M 디바이스는 객체식별자(OID) 표준체계 적용

- **사물인터넷 디바이스 식별을 위한 객체식별자(OID) 기반 식별체계**

< OID 식별 구조 >





① 제조사 식별 노드

- 사물인터넷 디바이스 제조 및 생산하는 회사 또는 개인을 식별하기 위한 목적의 노드입니다.
- 해당 노드는 사물인터넷 디바이스용 객체식별자 {0 2 481 1 } 객체식별자 관리기관인 전자부품연구원에서 할당 및 관리합니다.

② 모델 식별 노드

- 사물인터넷 디바이스 제품의 모델을 식별하기 위한 목적의 노드입니다.
- 해당 노드는 제조사 식별 노드를 할당받은 기관에서 할당 및 관리합니다.

③ 일련번호 식별 노드

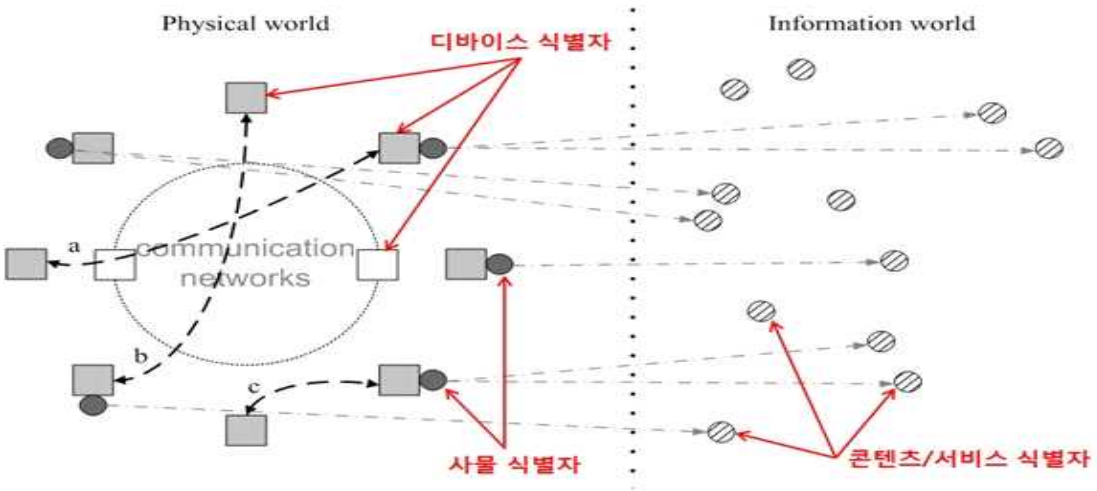
- 사물인터넷 디바이스 제품의 시리얼번호를 식별하기 위한 목적의 노드입니다.
- 해당 노드는 제조사 식별 노드를 할당받은 기관에서 할당 및 관리합니다.

나. 객체 식별자(OID) 식별 규정

□ 객체식별자(OID) 발급 및 관리

- 객체식별자 {0 2 481 }의 할당관리기관
  - 객체식별자 {02 481 }의 할당관리기관은 한국인터넷진흥원(KISA)이 담당
- 사물인터넷 디바이스 식별을 위한 객체식별자 할당
  - 사물인터넷 디바이스 식별을 위한 객체식별자 {0 2 481 1 }의 하위노드는 "객체식별자 기반 사물인터넷 디바이스 식별 체계" (TTAK.KO-06.0365R1, 2015)[4]에 따라 할당한다.
- 객체식별자 {0 2 481 1 }의 할당관리기관
  - 객체식별자 {02 481 1 }의 할당관리기관은 전자부품연구원(KETI)이 담당한다.

< 사물인터넷 객체식별 위치 개념도 >



□ 객체식별자 {0 2 481 } 하부노드 할당 규칙

< 객체별 하부노드 할당 규칙 >

1 차 정수 값 (Primary Integer Value)	**2 차 식별자** (Secondary Identifier)	**용도**
0	N/A	reserved
1	iot-device	사물인터넷 디바이스 식별
2 ~	N/A	reserved

□ 레벨 기준의 객체식별자 {0 2 481 } 하부노드*의 할당

* 하부노드 : 서비스, 디바이스, 게이트웨이 등 객체

oneM2M 규격에 따라 디바이스 아이디는 ITU-T X.660 ¦ ISO/IEC 9834-1 문서에 따라 OID 생성을 권장한다. 디바이스 아이디 발급 형식은 아래와 같다.

- 서비스 OID : 0.2.481.1.<서비스하는 지자체 지역번호>.<서비스아이디>.0
- 단말 OID : 0.2.481.1.<서비스하는 지자체 지역번호>.<서비스아이디>.SN
- G/W OID : 0.2.481.1.<서비스하는 지자체 지역번호>.<서비스아이디>.SN

※ SN : "0"값을 제외한 자동 일련번호 또는 단말 시리얼 번호(고유 식별 번호)

< 객체별 하부노드 할당 규칙 >

레벨	**Number**	**예시 설명**	**비고**
1	0	identifies the managing organization ITU-T	
2	2	identifies "Administration"	
3	481	identifies the data country code for Korea	
4	1	Higher arc, identifies an M2M device	디바이스 관련 ID 값
5	N	identifies the device Manufacturer	
6	N	identifies the device Model	
7	N	identifies the device Serial number	

※ ex) OID : 0.2.481.1.100.1003.12345

제3절 네트워크 구축방안

1. 구축 절차

사물인터넷 네트워크 구축은 아래 그림과 같이 지역적/지형적 특성의 분석을 통해 전체적인 망구조를 설계하고, 설계된 위치를 기반으로 게이트웨이(기지국) 설치 위치를 방문하여 실사를 통해 설치를 진행하게 된다. 이후 음영지역 여부를 확인하고, 확인된 음영 지역 해소를 위한 처리를 수행한다.

< 네트워크 구축 절차 >

분석 및 기본설계 ≫	설치현장 실사 ≫	상세설계 및 구축 ≫	검수 ≫	최적화
• 서비스 및 지역 특성 분석 • 디바이스 수량 및 데이터 특성 기반 설계 • 백홀 망 사용여부	• 출입 등 구축환경 확인 • 설치 가능여부 확인 • 전원·백홀 포설가능 확인 • 전파방해 요소 확인	• 기본설계 보완 상세설계 • 발주 및 계약 • 안전관리요원 배치 • 네트워크 구축 및 감리	• 지정상면에 설치여부 • 설계도 준수여부 • 정보통신공사 기준 및 설치가이드 준수여부 등	• 기지국 최적화 • 무선환경 최적화 • 시스템 최적화

1) 망 설계 및 분석, 설치 사이트 검증

망 설계 및 분석은 서비스 및 지역의 특성을 고려하여 아래 그림과 같은 단계로 진행된다. 망 설계 및 분석 단계는 전체 구축 절차 중 “망 설계 및 분석”과 “설치 사이트 검증”까지를 포함한다.

< 무선망 설계 절차 >

□ Traffic 및 Coverage 분석시 고려사항

- 서비스 적용 범위
- 서비스 특성 : 이동형 또는 고정형 서비스 유형 및 종류
- 데이터 량(Mbps)
- 데이터 전송 주기(초·분·시간)

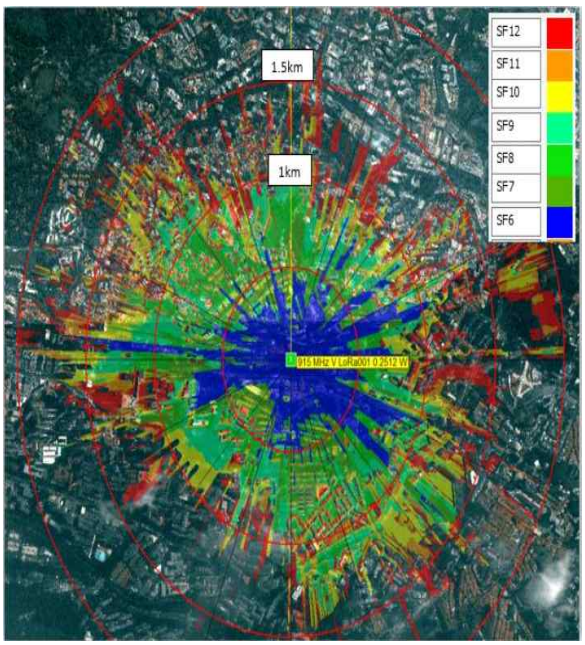
□ 기본 커버리지 설계(Nominal Cell Planning)시 고려사항

Traffic 및 Coverage 분석의 결과를 적용하여 네트워크 커버리지 맵을 구성하는 것을 의미하며, 전문 무선망 셀 플래닝 도구(Tool)를 사용하여 수행한다.

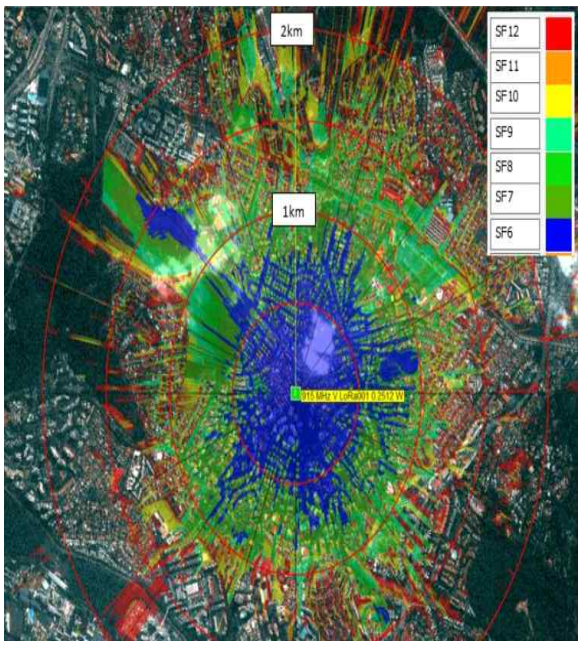
- 서비스 범위(Coverage) 내 신호세기 측정
- 중첩 셀/채널 존재 여부
- 신호간섭 분석 및 최적 주파수 할당
- 게이트웨이(기지국) 장비 설치 위치 최적화

< 게이트웨이(기지국) 커버리지 시뮬레이션 예시 >

[셀 반경 2Km 커버리지 신호세기 예시]



[셀 반경 2Km 커버리지 신호세기 예시]



□ **실사(Survey)시 고려사항**

네트워크 커버리지 맵을 바탕으로 Gateway 설치 예정인 위치를 방문하여 현장 확인을 하여야 한다.

- LoRa 게이트웨이 상면 확보 유무
- 전원공급 가능 여부
- 백홀 연결 가능 여부
- 무선 백홀 사용시 수신 감도
- 빌딩, 기타 구조물, 산, 강, 바다, 호수 등에 의한 전파방해요소 존재 여부
- 건물주 및 토지주와의 협의요건(공간사용료, 접근 가능 시간대 등) 및 설치허가 여부

□ **사물인터넷 네트워크 디자인시 고려사항**

실사 결과물을 이용하여 각 사이트별로 필요한 부가장비 및 부자재를 확정하는 단계를 의미한다.

- 유선망 백홀 이용 시 백홀 케이블 길이
- 전력선 포설 길이
- 기타 필요 부자재(커넥터, 브래킷, 백업용 전원장치 등) 파악
- 태양발전 사용시 설치 가능 여부

2) 설치 및 구축

사물인터넷 네트워크 디자인이 완료되면, Cell 사이트 확정하고 실제 구축을 위한 발주단계로 이행하게 된다. 네트워크 시스템을 현장에 배송하고, 설치인력이 설치를 진행하는 것을 의미한다. 현장 설치시 아래 표에 명시된 사항을 준수하여 시공한다.

< IoT 네트워크 시공시 준수사항 >

항목	고려사항
안전	• 시공 시 안전요원이 항시 상주하여 안전장구 착용 및 안전사항을 준수하는지 관리 감독한다.
물자수급	• 물자수급 시 발주처의 물량발송과 시공처의 물량입고 수량이 명시된 영수증을 관리한다.
시공 장소 비치 문서	• Site Survey 리포트 • 설치 가이드
설치 완료	• 설치완료 후 아래 항목이 포함된 설치완료 리포트를 작성하여 제출한다. - 시공자 및 시공사 - 설치완료 사진(Gateway, 부가장비, 케이블 포설 등)

□ 자체망 구축

자체망 구축방식의 경우는 통신비 절감, 높은 데이터 보안이 가능하나, 추가 구축비용이 발생할 수 있고, 전담운영조직 구성 등 운영비 증가 또는 통신사 대비 상대적으로 안정성이 낮은 단점이 있다.

- 장점 : 통신비 절감이 되고 높은 데이터 보안이 가능
- 단점 : 전담 운영 조직 구성 등 운영비 증가, 망의 안정성 및 QoS 확보 어렵고 통신사 망 대비 상대적으로 낮은 안정성 확보가 가능

※ 인프라 구축비(투자비), 운영인력 확보 및 커버리지 등을 고려하여야 함

□ 상용망 이용

통신사의 유선망/무선망 이용하는 경우는 망 안정성, 유지보수 비용 절감이 유리하나, 지속적인 통신비용이 발생할 수 있다.

- 장점 : 정기적인 유지보수에 따른 망 안정성, QoS 보장(Quality of Service) 및 유지보수 비용 절감
- 단점 : 지속적인 통신비 발생, 신규 설치에 따른 포설비용 발생

※ 통신 서비스 비용 지불, 통신단말 유형정의, 국가기관 이용 수준에 맞는 보안성 확보 및 향후 서비스 확장성을 고려하여야 함

3) 검수

설치완료 후 감리를 진행하는 것으로 Gateway 및 기타 부자재와 부가장비들의 설치가 Site Survey 리포트 및 설치 가이드라인에 준하는지 감리하는 것을 의미한다.

- 정보통신공사 설계기준의 준수 여부 확인
- Site Survey 리포트에 명시된 설치 지정장소 준수 여부 확인
- 설치 가이드라인 준수 여부 확인
- 주물자, 부자재, 부가장비 등의 설치 현황과 설치완료 리포트와의 정합성 체크

4) 망 최적화

설치완료 후 실제 망 설계에서 제시한 커버리지, 전파 수신감도 등을 측정하여 음영지역 파악하고 개선하여 무선망을 최적의 상태로 구성하는 것을 의미한다. 망 최적화 시 무선 환경 측정방법은 아래와 같다.

- 측정 장비(Frequency Analyzer) 및 야기 안테나를 이용하여 도로에서 측정
- 측정 인력이 전문 DM(Diagnostic Monitor) 도구(Tool)를 이용하여 측정(지하 및 건물 내)
- 망 최적화시 아래 표에 명시된 방법으로 무선망 최적화를 진행한다.

< IoT 네트워크 최적화시 고려사항 >

항목	고려사항
기지국 최적화	• 기지국별 출력 확인 및 조정 • 기지국별 파라미터 확인 및 조정
무선환경 최적화	• 기지국 호 시험 • 기지국 게이트웨이 안테나 조정 및 설치위치 변경 • 인접 셀간 커버리지 조정 • 디바이스 밀집도 분석 및 데이터 전송 주기 조정
시스템 최적화	• 네트워크 서버의 오버로드 파악 및 조치 • 조인 및 기타 프로세스의 최적화

□ 음영지역 해소

음영지역이란 게이트웨이에서 송신하는 전파가 미치지 못하거나, 신호가 미약하여 디바이스와 게이트웨이 간 데이터 송수신이 원활하지 못한 것을 말한다. 아래와 같이 2가지의 방법으로 음영지역을 최소화할 수 있다.

< 음영지역 최소화 방안 >

항목	설명	특징
Small Cell 구성	• 음영지역에 Pico 또는 Small Cell 장비 설치	• 낮은 구축 비용 • 셀 중첩 최소화 • 별도의 관리 필요 • 통신비 증가(백홀망으로 3G/LTE 이용)
추가 Gateway 설치	• 음영지역에 Gateway 추가 설치를 통한 음영지역 해소	• 관리의 일관성 유지 • 기존 안정화된 무선망에 영향도 가중

2. 소요예산

시스템 구축 및 인프라 구축 및 운영비용이 고려되어야 한다.

시스템 구축비에는 IoT응용 소프트웨어 개발비용과 소프트웨어 라이선스 비용이 포함되며, 인프라 구축비는 센서노드 구매, 네트워크 인프라 등이 비용과 운영인력·통신비·유지보수 비용 등 운영 예산이 수립되어야 한다. 특히, 백홀을 위한 망구축비용과 연간 운영비가 필요하다.

<사물인터넷 인프라 구축을 위한 소요예산 항목>

구분	항목	자체망 구축 고려사항	비고
시스템 구축	소프트웨어 개발	• IoT 응용시스템 개발 비용	
	소프트웨어 라이선스	• 상용 소프트웨어 라이선스 비용(OS, DBMS 등)	
인프라 구축	컴퓨팅 서버	• 데이터를 수집하고 분석하는 작업의 서버와 서비스를 제공하기 위해 필요한 서버	
	네트워크 인프라	• 망 구축 비용	백홀
	센서노드 구매	• 센서 노드 구매 비용	
	센서노드 설치비	• 센서 노드 설치 및 통합 작업	
운영	운영인력	• 서비스 Open 후 운영인력에 대한 년간 비용	
	통신비	• 전용망 및 상용망 사용료 : 년간 비용	백홀
	유지보수 비용	• 응용시스템 및 상용소프트웨어, 장비 유지보수 비용 등	

3. 상호호환성 확보

장비 간 연동 호환성을 위한 제공버전 및 권장버전은 다음과 같으며, 통상적으로 관련표준을 준수하는 시스템 도입이 필수적이며 및 최신 버전사용이 필요하다.

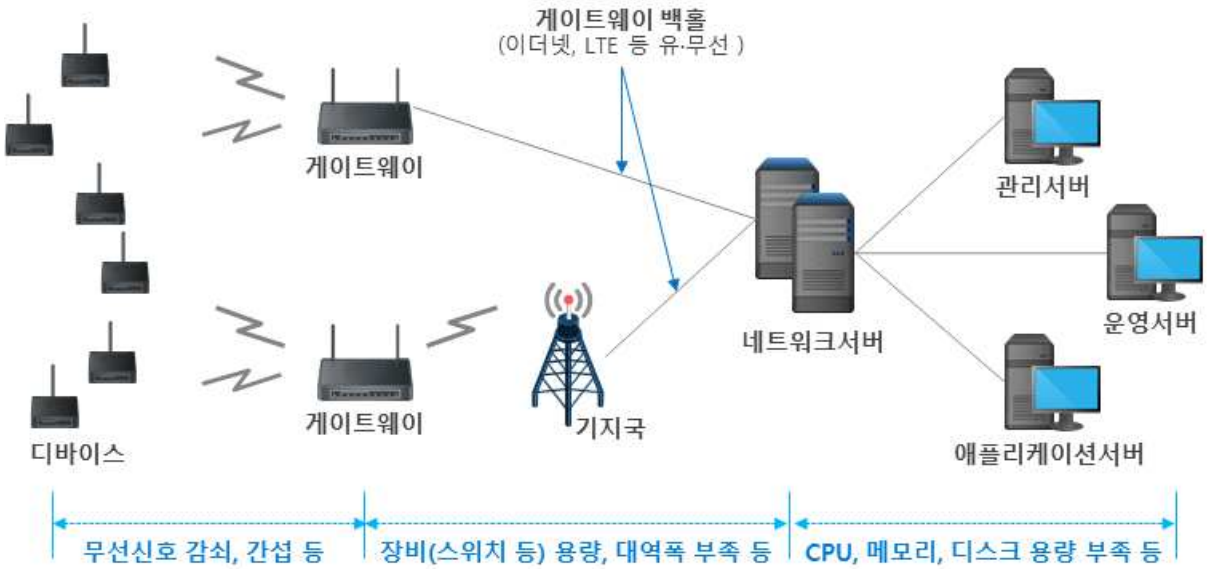
구분	이미지	표준	버전		비고
			제공버전	권장버전	
LoRa		LoRa Alliance	LoRaWAN 1.1, 1.2	BLE 1.1	최신 버전 권장
NB-IoT		NB-IOT Alliance	LTE Cat.1, Cat.0, Cat.M1 LTE-M, NB-LTE	LTE-M	
LTE-M		LTE-M Alliance	LTE Cat.1, Cat.0, Cat.M1 LTE-M, NB-LTE	LTE-M	
SigFox	sigfox	UNB	UNB		
Zigbee	Z-WAVE	Zigbee Alliance	Zigbee 3.0	Zigbee 3.0	
Z-Wave	ZigBee	Z-Wave Alliance	Z-Wave		
블루투스		Bluetooth Alliance	BLE 4.1, 4.2, 5.0	BLE 5.0	
WiFi	Wi Fi	WiFi alliance	802.11.ax, 802.11.ah	802.11.ax, 802.11.ah	

제4절 네트워크 품질관리 방안

1. 품질 영향요소

사물인터넷 인프라의 품질(성능)에 영향을 미치는 요소는 무선신호 감쇠·간섭 등에 의한 무선통신 품질저하, 게이트웨이와 서버 간 데이터 전송을 위한 유·무선 백홀 대역폭 부족, 플랫폼·서비스 서버 성능 저하 3가지로 분류될 수 있다.

< IoT 인프라 품질저하 요소 >



2. 품질 확보방안

□ 디바이스와 게이트웨이 구간

일반적으로 사물인터넷 디바이스는 무선 통신을 담당하는 통신 모듈을 탑재하고 있다. 통신 모듈 자체의 품질이 보장됐다 하더라도, 통신 모듈과 부품이 디바이스에 탑재되는 방식과 디바이스가 처한 환경에 따라서 통신 모듈의 성능이 제대로 나오지 않고 무선 통신 품질이 악화될 수 있다.

예를 들어, 디바이스 뿐 아니라 게이트웨이 등 중계 장치는 물론 서버와

애플리케이션 등 모든 것이 정상적으로 동작하고 있는데도 갑자기 연결이 끊기거나 애플리케이션이 멈추는 경우가 있다. 이렇게 무선 통신 품질을 악화시키는 요인으로 다음과 같은 것들이 있다.

① 전파 감쇠(Radio-Wave Attenuation)
② 전파 간섭(Radio-Wave Interference)
③ 디바이스 내부에서의 전파 반사(Internal Radio-Wave Reflections)
④ 디바이스 내부 간섭(Internal Interference)

① 전파 감쇠(Radio-Wave Attenuation)

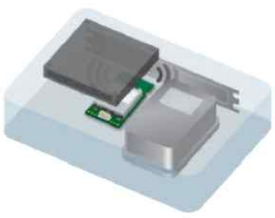
- 전파는 장애물의 영향을 받기 쉽다. 벽, 천장, 기둥 등 건물의 구조물을 통과하며 전파가 감쇠하고 이로 인해 통신 품질이 저하된다.
- 디바이스를 개발할 때에는 디바이스가 어떤 환경에서 사용되고 어디에 설치되는지 고려해야 한다.

② 전파 간섭(Radio-Wave Interference)

- 전파는 통신 외 용도로도 사용된다. 예를 들어 전자레인지는 음식을 가열하기 위해 2.4 GHz 대역을 이용한다.
- WiFi나 블루투스 또한 2.4 GHz 대역을 이용하므로, WiFi를 이용하는 디바이스 근처에서 전자레인지를 사용하면 전자레인지에서 새어 나오는 전파와 디바이스의 전파가 간섭을 일으켜 디바이스의 연결이 끊길 수 있다.

③ 디바이스 내부에서의 전파 반사(Internal Radio-Wave Reflections)

- 디바이스에 탑재된 통신 모듈의 주변에 있는 부품으로 인해 디바이스 안에서 전파 반사가 일어나면 전파가 산란하면서 통신을 방해할 수 있다.
- 디바이스 케이스 안에 포함된 금속 부분에서 전파 반사가 일어나는 경우에도 마찬가지이다.



④ 디바이스 내부 간섭(Internal Interference)

- 디바이스 안에 탑재된 다양한 부품에서 발생하는 전파는 통신 모듈과 간섭을 일으킬 수 있다.
- 이런 부품으로, 예를 들어, IC 칩과 전원 회로를 들 수 있다. 특히 소형의 고성능 IoT 디바이스에서는 통신 모듈 주변에 부품이 밀집해 있어 디바이스 내부 간섭이 일어나기 쉽다는 점을 주의해야 한다.

□ 게이트웨이와 플랫폼・서비스 구간

게이트웨이와 플랫폼・서비스 구간에서 성능저하 원인은 설치되어 있는 L2/L3 스위치, F/W, IPS 등 네트워크 장비의 용량 및 성능 저하로 인한 품질저하와 LTE, 전용회선 등 유・무선 백홀 대역폭 부족으로 인한 품질저하 크게 2가지 문제로 분류될 수 있다.

① 네트워크 장비 성능 확보

- TTA『네트워크 구축을 위한 장비 규모산정 지침(TTAK.KO-01-0103)』을 참조하여 구축되어 있는 네트워크 장비의 규모를 산정하고, 적정용량 장비로 교체하여 성능을 확보하여야 한다.

② 유·무선 백홀 대역폭 확보

- GNS 회선 및 통신사업자 3G/LTE망을 백홀로 사용하는 경우 대역폭 증설은 비용증가가 수반되므로 실시간 트래픽(사용량) 모니터링을 실시하여 증·감속 기준을 적용한 후「회선 구성방식」등의 환경을 반영하여 최종적으로 조정한다.

※ 자가망 회선을 구성한 경우는 회선 증속에 비용이 발생되지 않으므로 처음부터 충분한 대역폭을 확보

- 트래픽 량은 업무시간 내 최근 3개월의 평균 최대 트래픽 량을 기준으로 하고, 필요시 6개월의 트래픽 량 추이를 참고하여 조정한다.

※ 통신회선 대역폭 사용량은 통신망관리시스템(NMS)를 통하여 측정하거나, 필요시 통신사업자에 사용량 정보 요청

□ 플랫폼・서비스 서버 품질 확보

목표 응답시간 내에 업무가 처리되지 않거나 사용이 불가능하게 되면 해당 정보시스템을 이용하는 사용자에게 엄청난 불편을 주는 것은 물론이고 대외적인 이미지 손상 및 막대한 경제적 손실을 끼치는 경우를 흔치 않게 볼 수 있다.

따라서, 정보시스템이 서비스를 제공하도록 정의된 시간 동안 목표 응답시간 내에 모든(정의된 부하량 내) 사용자의 요청을 성공적으로 처리할 수 있도록 유지, 관리 및 개선하는 활동이 더욱 중요하다.

정보시스템의 서비스 품질(QoS)을 결정하는 속성들 중의 하나인 성능을 나타내는 일반적인 지표에는 다음과 같은 것들이 있다.

< 시스템 성능을 나타내는 일반적인 지표 예시 >

성능 지표	정의	단위(예시)	목표
응답 시간 (response time)	작업 처리를 요청한 시간으로부터 이를 시스템이 처리하여 결과를 보여줄 때까지 소요된 시간	초	낮춤
시간당 처리량 (throughput)	시스템이 성공적으로 처리한 단위 시간당 요청(트랜잭션) 처리 건수	TPS* OPS**	높임
자원 사용량 (utilization)	자원(CPU, 메모리, 디스크 등)들의 용량 중 실제 사용하고 있는 값의 비율	%	높임
효율성 (efficiency)	시간당 처리량을 자원 사용량 또는 비용으로 나눈 값	%, tpmC***	높임

* TPS (Transactions per Second; 초당 트랜잭션 처리건수)

** OPS (Operations per Second; 초당 요청 처리건수)

*** tpmC (Transactions per Minute per Cost; 단위 비용당 분당 처리건수)

플랫폼・서비스 시스템 성능관리를 위해 필요한 업무 절차 및 산출물, 구체적인 문서양식 등은 업무를 수행하는 기관의 규모, 업무 분야, 시스템의 종류 및 유형에 따라 많은 차이가 있을 수 있으므로, 하나의 정보시스템 성능관리 지침을 모든 기관에 동일하게 적용하는 것은 현실적으로 불가능하다.

TTA 『정보시스템 하드웨어 규모산정 지침, TTAK-KO-10-0292』을 참조하여 기관의 환경에 맞도록 지침을 적절하게 조정(customizing)하여 기관별 성능관리 지침서 및 절차서를 작성하고 이를 업무에 활용하여야 한다.

제3장

정부사물인터넷 보안 준수사항

사물인터넷을 도입하는 기관은 본 가이드라인의 보안준수사항 외에 국가정보원의 “국가·공공기관 사물인터넷 보안가이드라인“을 반드시 만족하여야 한다.

제1절 사물인터넷 보안 요구사항

1. 사물인터넷 보안 위협

사물인터넷 환경에서의 보안 위협은 기존의 보안위협과 달리 차량, 홈·가전, 헬스케어 등 기기 및 시스템 본래의 기능에 대해 오작동이나 불법조작을 발생시켜 이용자의 신체나 생명, 재산 등에까지 피해가 확대될 수 있다.

또한, 사물인터넷을 구성하는 수많은 기기와 시스템들이 서로 네트워크로 연결되어 작동하는 특성으로 인하여 다른 기기 및 서비스에도 영향을 미치는 등 사물인터넷의 광범위한 연결은 예상하지 못했던 문제도 야기시킨다.

< IoT 환경에서의 보안위협 >

2. 사물인터넷 구성요소별 보안 요구사항

가. 디바이스 보안

□ 디바이스의 통신에 대한 보안위협

디바이스·센서와 게이트웨이 간 통신 주파수에 노이즈를 발생시키거나, 동시에 동일한 주파수에 접속 또는 신호의 위·변조로 실제 정상 신호를 방해하는 방법 등으로 보안을 위협할 수 있다.

이러한 보안위협은 전파 간섭(Interference) 및 방해(Jamming), 충돌(Collision) 등 무선링크에 대한 공격에서부터 네트워크에 공유된 Key를 취득하여 허가되지 않은(Fake) 디바이스를 네트워크에 접속시켜 악의적인 행위를 하도록 조종하는 공격까지 수없이 많이 존재한다.

< IoT 디바이스 관련 보안 위협 >

보안위협	위협내용
Interference/ Jamming/Collision	• 노이즈 발생, 동시 동일 주파수 접속, 주파수 위변조 등을 통해 실제 신호의 정상적인 송수신을 방해하는 공격
Sybil	• 기존의 Wireless Ad-hoc이나 센서 네트워크에서 Multi-Identity가 허용되는 취약점을 이용한 공격으로 각 디바이스나 센서에 Unique ID를 부여하지 않을 경우 발생
Traffic Analysis	• 암호화되지 않은 NPDU(패킷), DLPDU(프레임) 페이로드를 분석하여 정보를 취하는 공격(단, 암호화 할 경우 상대적으로 안전하지만, System Performance에 영향이 갈 수 있음)
DoS	• 주변 노드에 지속적인 광고 패킷을 송신, DLPDU 반복 수정, CRC 반복 체크로 시스템에 무리를 주거나 주파수 Jamming 등을 통해 신호 송수신을 방해하는 공격
De-synchronization	• Device Pool에 잘못된 시간 정보를 송신하여 디바이스가 계속적으로 시간을 교정하는데 자원을 소모하도록 하는 공격
Wormhole	• 상호 통신이 허가되지 않은 두 디바이스의 무선 통신 모듈을 공격해 상호간 통신을 가능하게 만들고, 통신 라우팅을 고의로 변경하거나 악성코드 배포 경로로 이용하는 공격
Tampering	• 단말에 저장된 데이터 혹은 송수신 데이터를 임으로 위변조하는 공격
Eavesdropping	• 암호화되지 않은 디바이스(센서)와 게이트웨이 구간 정보를 도청하는 공격
Selective Forwarding Attack	• 선택적으로 특정 노드에 패킷을 포워딩하지 않게 하여 해당 노드를 블랙홀로 만들어 버리는 공격
Spoofing	• 네트워크에 공유된 Network-Key를 취득하여 허가되지 않는 Fake 디바이스(센서)를 네트워크에 접속시켜 악의적인 행위를 하도록 하는 공격

□ 디바이스 보안 요구사항

■ 기밀성(Confidentiality) 관련 보안 요구사항

- 사물인터넷 기기 간 전송되는 메시지는 불법적인 스니핑(sniffing) 또는 도청 방지를 위해 메시지 암호화된 형태로 전송되어야 한다.
- 사물인터넷 기기는 정보유출 방지를 위해 개인정보 및 암호키와 같은 중요 데이터를 암호화하여 안전하게 처리 및 저장 관리하여야 한다.
- 사물인터넷 기기는 기기 복제 방지를 위해 기기 고유 식별정보가 외부로 유출되거나 변경되지 않도록 안전하게 처리 및 관리해야 한다.

■ 무결성(Integrity) 관련 보안 요구사항

- 사물인터넷 기기는 데이터 위변조 방지를 위해 데이터 무결성 검증 기능을 제공해야 한다.

■ 가용성(Availability) 관련 보안 요구사항

- 사물인터넷 기기는 물리적 제거·파괴 및 비정상적인 설치 시도 방지를 위해 주기적인 Keep Alive 메시지 전송 또는 기기 상태 정보 전송 기능을 제공해야 한다.
- 사물인터넷 기기는 안전한 소프트웨어 업데이트 및 보안 패치 기능을 제공해야 한다.
- 사물인터넷 기기는 소프트웨어 오류나 악성코드 감염에 의한 오동작 시에도 해당 모듈 분리 및 제거, 접근 권한 제한 등의 기능을 통해 소프트웨어 안전성을 보장해야 한다.

■ 인증/허가(Authentication/Authorization) 관련 보안 요구사항

- 사물인터넷 기기는 안전하고 자율적인 통신 환경 구축을 위해 기기 간 상호인증 기능을 제공해야 한다.
- 사물인터넷 기기는 정보유출 방지 및 프라이버시 보호를 위해 Ownership 제어와 같은 권한 제어 및 설정 기능을 제공해야 한다.
- 사물인터넷 기기는 불법적인 사용자 및 기기의 접근을 차단하는 접근 제어 기능을 제공해야 한다.
- (선택) 별도 UI가 제공(OS 기반)되는 사물인터넷 기기의 경우
  - 비인가 된 사용자의 접근을 차단하기 위해 사용자 인증 기능을 제공할 수 있어야 한다.
  - 불법적인 기기의 접근을 차단하기 위해 기기 인증 기능을 제공할 수 있어야 한다.
  - 안전하고 강력한 비밀번호를 설정하고, 주기적인 업데이트 기능을 제공할 수 있어야 한다.

나. 게이트웨이 보안

□ 게이트웨이 보안위협

사물인터넷 게이트웨이는 수많은 사물인터넷 기기와 외부 환경(WAN)과의 연결점으로써 사물인터넷 기기로부터 방대한 센싱 데이터가 송·수신되고, 사물인터넷 기기의 제어(액츄에이션) 및 관리가 이루어진다. 이에 따라 악의적인 공격자의 공격 대상이 될 요인이 충분하다.

게이트웨이에 대한 보안위협은 게이트웨이 자체를 대상으로 한 위협과 게이트웨이와 기기 간, 게이트웨이 간, 게이트웨이와 연계하는 외부환경 간 네트워크를 대상으로 한 보안 위협, 그리고 게이트웨이의 서비스를 대상으로 하는 보안 위협으로 나눌 수 있다.

< 게이트웨이 관련 보안 위협 >

보안위협	위협내용
사물봇 (ThingBot)	• 광범위한 사물로 구성된 사물봇에 의한 트래픽 폭증 공격
프로토콜 변환 취약점 공격	• 사물인터넷 기기는 자원 제약(전력, 연산성능, 통신범위)으로 인하여 일반적으로 경량 프로토콜, 근거리 통신을 사용함. • 사물인터넷 게이트웨이가 이를 고기능성 프로토콜 또는 장거리 통신(Ethernet 등)으로 전환하는 과정에서 데이터 기밀성 훼손, 악의적인 위·변조, 보안정책 훼손, 임의의 메시지 주입으로 인한 보안 위협(예: Buffer overflow 공격)이 존재
서비스 마비	• 사물인터넷 게이트웨이와 사물인터넷 기기 사이의 통신은 주로 무선을 통해 이루어진다. • 이러한 무선 프로토콜의 특성(취약점) 또는 Jamming을 통해 사물인터넷 게이트웨이와 사물인터넷 기기 사이의 통신을 불가능하게 하거나, 사물인터넷 게이트웨이의 취약점을 통해 게이트웨이의 동작을 정지시키거나 서비스를 불가능하게 하는 위협
악성코드 감염	• 악성코드 감염으로 사물인터넷 게이트웨이가 좀비화 되어 DDoS 등 공격에 악용될 수 있고, 감염된 게이트웨이를 통해 사용자의 데이터가 유출될 수 있다. • 또한 사물인터넷 게이트웨이에 연결된 기기를 감염시킴으로써 2차 피해를 유발할 수 있음
데이터 유출	• 도청, 중간자 공격, 메시지 위·변조를 통해 공격자가 사용자의 민감한 정보(개인정보 등)를 습득할 수 있음
메시지 불법 동작 제어	• 재전송 공격, 메시지 위·변조를 통해 특정한 동작을 수행하는 메시지를 주입하여 악의적인 공격자가 사물인터넷 게이트웨이의 동작을 제어할 수 있음
웹 인터페이스 취약점	• 사물인터넷 게이트웨이 접근을 위한 웹 인터페이스의 취약점을 활용한 공격(CSRF 등)으로, 관리자 권한 탈취 등의 피해를 입을 수 있음
물리적 탈취	• 물리적인 접근을 통해 악의적인 공격자는, 사물인터넷 게이트웨이의 펌웨어를 임의로 교체하거나 하드웨어 인터페이스(예: JTAG) 또는 플래쉬 메모리의 물리적인 탈취를 통해 데이터를 획득할 수 있음

□ 게이트웨이 보안 요구사항

- 프로토콜 변환 과정에서 데이터 기밀성을 유지하고, 악의적인 위·변조를 방지할 수 있어야 한다.
- 임의의 메시지를 주입하여 발생할 수 있는 보안 위협(예: Buffer Overflow 공격)에 대응할 수 있어야 한다. (예: Secure Coding 준수)
- 송·수신 데이터는 불법적인 스니핑(sniffing) 또는 도청 방지를 위해 암호화된 형태로 전송되어야 한다.
- 프로토콜 취약점을 이용한 공격을 감내(Fault tolerant)할 수 있어야 한다.
- 프로토콜 변환, 통신 방식 변환 과정에서 보안 정책이 일관성을 갖고 적용될 수 있도록 하여야 한다.
- 방화벽, IPS와 같은 수단을 통해 네트워크 침입 탐지 및 네트워크 트래픽 제어를 할 수 있어야 한다.
- 사물인터넷 네트워크 및 기기에 대한 모니터링 기능을 지원하고, 오작동·악의적인 조작·트래픽 폭증과 같은 이상 징후를 탐지할 수 있어야 한다.
- 사물인터넷 기기의 최초 등록 시, 게이트웨이와의 보안키(Secure Key) 합의, 보안정책 설정과 같은 초기 보안 설정을 지원할 수 있도록 인터페이스를 제공하여야 한다.
- 사물인터넷 서비스 제공 지원을 위한 보안터널링(Secure Tunneling) 기능을 제공해야 한다.
- 네트워크서버에 등록되는 기기는 (초)경량, 저전력 기기를 위한 비밀키 설정 등을 대행하는 기능을 제공할 수 있어야 한다.
- (선택) 자신에게 연결된 사물인터넷 기기로 구성된 그룹의 생성, 관리 및 그룹 키 관리 기능을 제공할 수 있어야 한다.

다. 사물인터넷 서비스 보안

□ 서비스 보안위협

사물인터넷 서비스 플랫폼은 제공 서비스 및 사용자, 기기 등을 관리하고, 센터 시스템과 각 기기 간의 연결기능을 제공한다. 사물인터넷 환경의 특성상 각 장치들은 사용자의 민감 정보를 수집할 가능성이 높으므로 이러한 데이터는 처리 과정에서의 보안이 필수적이다.

< IoT 서비스 관련 보안 위협 >

보안위협	위협내용
Worm 및 Virus	• 시스템을 파괴하거나 작업을 지연 또는 방해할 수 있음
비인가된 접근	• 비인가자가 불법적으로 시스템에 로그인(Login)하여 디스크 자료 불법 열람, 삭제 및 변조 등 시스템에 물리적인 피해를 유발할 수 있음
패치되지 않은 시스템 OS 보안 취약성	• 운영체제, 데이터베이스, 응용 프로그램, 시스템 프로그램 등 모든 정보 자산에 존재하는 허점(버그)에 의해 주로 발생되며, 사용자의 민감정보 유출, 바이러스, 악성코드에 의한 시스템의 비정상적인 동작 발생할 수 있음
설정 오류 및 실수	• 패드워드 공유, 데이터 백업의 부재 등 운영자의 부주의와 태만으로 시스템의 불법접근 및 데이터 손실 등의 문제 발생 가능
기밀성/무결성 공격	• 네트워크 도·감청을 통해 데이터 위·변조, 악성코드 삽입, 암호키 유출 등을 통한 보안 위협 발생 가능
개인정보 유출 및 프라이버시 침해	• 다양한 디바이스로부터 수집된 단편적인 정보의 조합으로 새로운 개인식별 정보 생성

□ 서비스 보안 요구사항

- 플랫폼, 서비스-단말기, 플랫폼/서비스-게이트웨이 간 송·수신하는 메시지에 대해 메시지 인증 코드(MAC) 등을 이용하여 메시지에 대한 무결성을 검증하여야 한다.
- 서비스 플랫폼에서는 서비스 기능에 부합하는 데이터만 전송하고, 개인을 식별할 수 있거나 유추할 수 있는 데이터 또는, 다른 데이터와 연관하여 주요 정보가 될 수 있는 데이터 등은 전송하지 않아야 한다.
- 수집되는 데이터에 대해서는 임계 범위 설정 등을 통해 유효 값인지 검증하여야 한다.
- 서비스 플랫폼에서 사용하는 서버, 소프트웨어, 미들웨어 등에 기본적으로 설정되어 있는 패스워드(디폴트 패스워드)는 반드시 변경 후 사용하여야 한다.
- 서버 등의 장비에 대한 계정관리, 패스워드 설정, 잠금 설정, 화면보호기 설정 등 관련 지침을 준수하여 적절한 보안 수준을 유지하여야 한다.
- 플랫폼은 기존 인터넷망 및 업무망과 물리적 또는 논리적으로 분리하여야 하며, 인터넷망 또는 업무망과 연계가 필요한 경우 연계구간을 지정하여 운영하여야 한다.
- 디바이스 설정 및 관리에 있어서는 운영체제, 펌웨어, 소프트웨어에 대해서 주기적으로 무결성 검증을 수행하고 최신 업데이트 및 보안 패치를 적용하여야 한다.
- 단말기 도난, 탈취, 분실, 파괴 등을 식별하기 위해 관리 단말목록, 동작 상태, 업데이트 정보 등을 관리하여야 한다.
- 로그 유지 및 감시 경우 데이터에 대한 접근기록과 단말기, 게이트웨이, 서버 등의 장비에 대한 접근기록을 유지하고 비정상적인 접근을 주기적으로 감시하여야 한다.
- 디바이스, 게이트웨이, 서버에 대한 트래픽을 모니터링하여 악성코드 감염, 해킹 등의 비인가 접근, 오작동, 불능 등의 비정상 행위를 식별하고 차단할 수 있어야 한다.
- 개인정보 등 민감 정보를 수집할 경우, 해당 정보를 통해 가공되는 정보가 최소한의 개인정보를 포함하도록 정책을 수립하여야 한다.

제2절 정부사물인터넷 보안방안

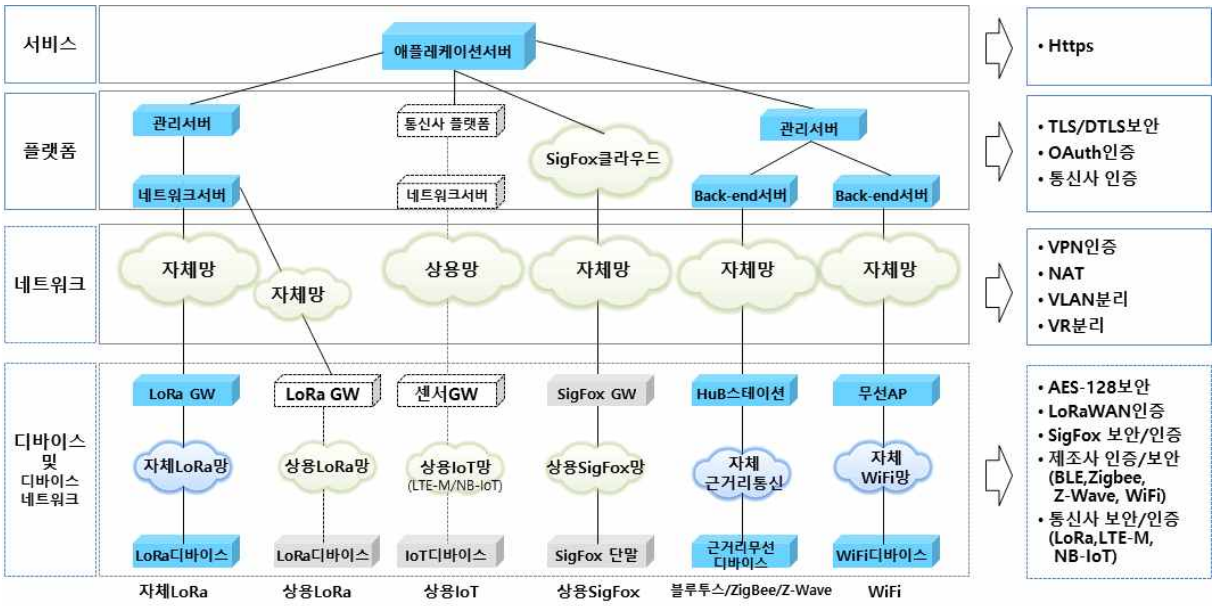
1. 정부사물인터넷 보안 참조모델

사물인터넷 보안 위협 및 요구사항에 대응하여 정부사물인터넷 인프라를 구성하는 각 계층의 특성에 맞게 보안방안을 적용한다.

서비스 계층에서는 보안이 강화된 HTTPS 프로토콜을 적용하여 서비스 데이터를 암호화 한다. 플랫폼 계층에서는 인증(자체구축의 경우 OAuth, 상용망의 경우 통신사 인증)과 암호화(TLS/DTLS 보안)를 적용한다. 네트워크의 경우 구성환경에 따라 VPN 암호화 터널링, NAT 기술로 IP주소 은닉, VR·VLAN 등 네트워크 가상화 기술로 트래픽을 분리하는 등 보안을 강화한다.

디바이스 및 디바이스 네트워크 계층에서는 다양한 정부사물인터넷 구축 환경에 따라 아래 참조모델과 같이 적절한 방식으로 보안을 강화한다.

< 정부사물통신망 보안 참조모델 >



- ① 자체 LWPA망 활용(LoRa)시 VPN/OAuth2.0 인증 및 TLS 1.2 보안 구현
- ② 통신사 IoT망 활용시 OAuth 2.0 인증 및 TLS 1.2 보안 구현
- ③ 통신사 IoT서비스 활용시 통신사 인증 및 TLS 1.2 보안 구현
- ④ SigFox 사물인터넷망 활용시 VPN/OAuth2.0 인증 및 TLS 1.2 보안 구현
- ⑤ 근거리 사물인터넷망 활용시 VPN/OAuth2.0 인증 및 TLS 1.2 보안 구현
- ⑥ WiFi통신방식 활용시 SSL 및 TLS 1.2 보안 구현

2. 암호화 보안터널 구성

사물인터넷 데이터를 보호하기 위해 각 전송구간 또는 전체 전송경로에 대한 암호화 기술을 적용하여 보안터널을 구성한다.

가. 보안터널 구성요소

□ 네트워크 Level 터널 구성

- 사업자 통신망(공중망) 활용시, VPN 터널 구성
- 인터넷 접속 구간 통신망 VPN 터널 구성
- 내부 네트워크 분리를 위한 VLAN 터널을 구성

□ 디바이스 Level 터널 구성

- 네트워크 서버 구간까지 VPN 터널 구성
- 게이트웨이 구간까지 VPN 터널 구성
- 애플리케이션 구간까지 VPN 터널 구성

□ 서비스 Level 터널 구성

- 네트워크 서버와 애플리케이션 서버 TLS보안 터널 구성

< 정부사물통신망 보안터널 구성내역 >

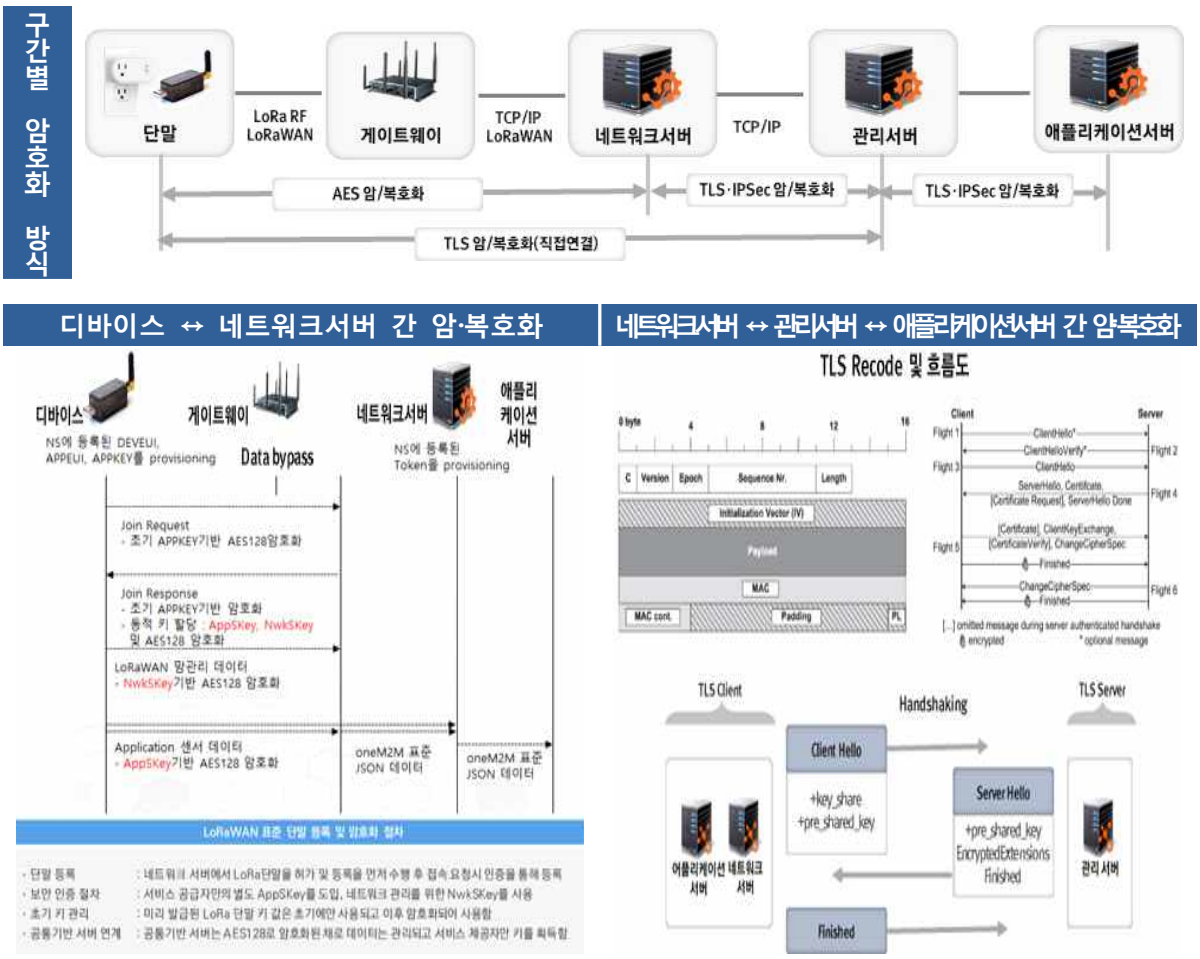
구분	게이트웨이 하단 구간				게이트웨이 상단 구간	
	디바이스 ↔ 센서GW/ 기지국/AP	**디바이스 ↔ 네트워크 서버**	**디바이스 ↔ 통신사플랫폼 /Back-end서버**	**디바이스 ↔ 애플리케이션 서버**	**GW**(HuB스테이션/기지국) ↔ **네트워크서버** (IoT플랫폼/ BackEnd서버/ SigFox클라우드)	**네트워크 서버 ↔ 애플리케이션 서버**
① 자체 LWPA망 활용(LoRa)		AES-128·256 보안				TLS 1.2, IPSec 보안
② 통신사 IoT망 활용		AES-128·256 보안				
③ 통신사 IoT 서비스 활용			통신사 보안			
④ SigFox 사물인터넷망 활용			SigFox 보안(SSL)			
⑤ 근거리 사물인터넷망 활용		제조사 보안				
⑥ WiFi 통신방식 활용	WiFi 보안 (WPA등)				SSL	

나. LoRa 구간별 암호화 터널 구성 (OneM2M LoRa)

□ 구간별 암·복호화 구현 예시(LoRa 기준)

- (디바이스-네트워크서버 간) 망관리 데이터는 NwkSKey기반 AES암호화, 애플리케이션 데이터는 AppsKey기반 AES암호화를 수행한다.
- (네트워크서버-관리서버 간) TLS기반 암·복호화를 수행한다.

< LoRa망 암호화 터널 구현(예시) - 암·복호화 >



□ 구간별 암호화 프로토콜 목록 (OneM2M 등)

- 사물인터넷에 대한 암호화 프로토콜 목록은 아래와 같으며, LoRa 하단은 LoRaWAN규격에 따른 AES-128, 상단 구간은 CoAP/MQTT에 따른 AES-128 암호화 프로토콜 사용

<표3-15 : 암호화 프로토콜 목록 >

통신 프로토콜	지원 암호	비고
Zigbee(IEEE 802.15.4)	AES-128	
Bluetooth(IEEE 802.15.1)	SAFER-SK128, AES-128	
6LoWPAN(IEEE 802.15.4, RFC 4919)	AES-128 / RSA-1024, ECC-160	
Z-Wave(IEEE 802.11)	TDES, AES-128	
LoRa(LoRaWAN Specification V1.0)	**AES-128**	**LoRa**
CoAP(RFC 7252)	**AES-128 / SHA-1 / ECC-160**	**LoRa**
MQTT (ver 3.1.1.)	**AES-128, AES-256, TDES / SHA-1, SHA-256, SHA-384**	**LoRa**
DDS (DDS Security V1.0)	AES-128, AES-256 / SHA-1, SHA-256 / RSA-2048	

※ 출처 : IoT환경에서의 암호인증기술 이용 안내서(17년, KISA)

3. 인증 방안

가. 사물인터넷 인증 구성요소

□ 디바이스 인증

- IoT센서 디바이스 인증 (해당 표준별 인증, 제조사 인증)
- IoT식별자를 기반으로 디바이스 인증 (TTA에서는 OID를 IoT식별표준으로 제정)
  - 예) SigFox인증, LoRaWAN인증, 통신사 인증 등

□ 네트워크 인증

- 인터넷망 또는 내부 사설망 사용시 VPN 인증
- 통신사업자 구간 플랫폼구간 인증후 내부 플랫폼 구간 인증
  - 예) VPN 인증, 모바일서비스 VPN 인증

□ 서비스 인증

- 사용자별 서비스 인증 (ID/PWD 로그인인증과 연계)
- 해당 부서 또는 조직이 사용할 수 있는 서비스를 구분하여 관리
  - 예) 애플리케이션 서버 사용을 위한 ID/PW 인증

□ 사용자 인증

- IoT디바이스를 사용하고 있는 사용자가 적법한 사용자 인지를 인증
- 센서 디바이스 생체 인증 또는 기기에 인증서를 탑재하여 추가적인 보안 실시
  - 예) 생체인증, PKI인증, OAuth인증

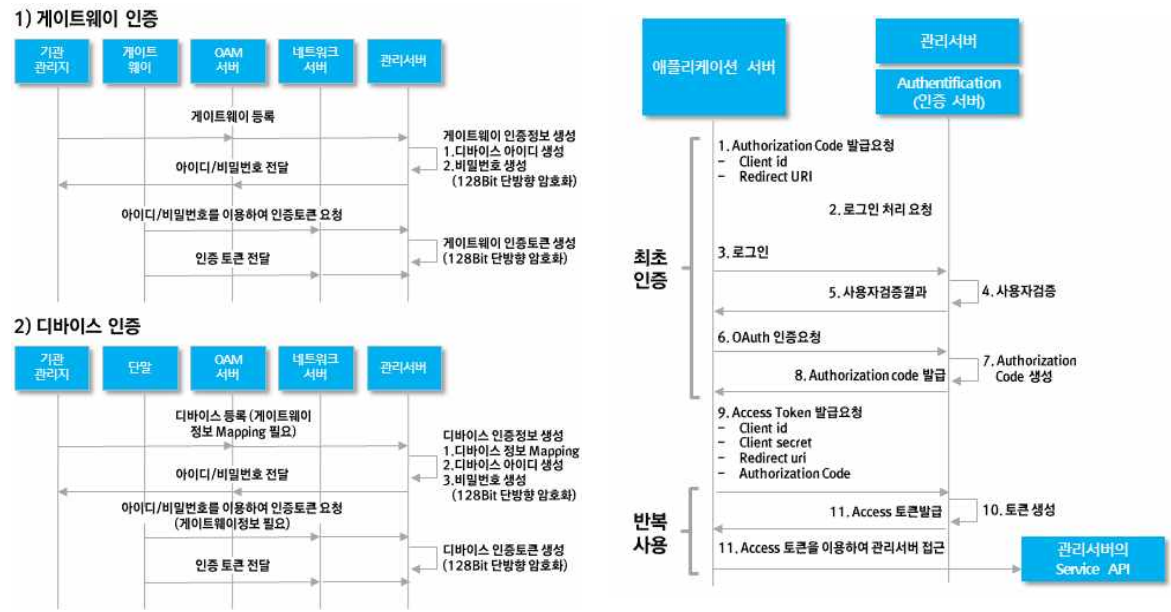
< 정부사물인터넷망 구간별 인증 적용내역 >

구분	게이트웨이 하단 구간				게이트웨이 상단 구간	
	디바이스 ↔ 센서GW/ 기지국/AP	디바이스 ↔ 네트워크 서버	디바이스 ↔ 통신사플랫폼 /Back-end서버	디바이스 ↔ 애플리케이션 서버	GW(HuB스테이션/기지국) ↔ 네트워크서버 (IoT플랫폼/ BackEnd서버/ SigFox클라우드)	네트워크 서버 ↔ 애플리케이션 서버
① 자체 LWPA망 활용(LoRa)		LoRaWAN 인증			VPN 인증	OAuth 2.0 인증
② 통신사 IoT망 활용		LoRaWAN 인증				OAuth 2.0 인증
③ 통신사 IoT 서비스 활용			통신사 인증			통신사 인증
④ SigFox 사물인터넷망 활용	SigFox 인증				VPN 인증	OAuth 2.0 인증
⑤ 근거리 사물인터넷망 활용	제조사 인증				VPN 인증	OAuth 2.0 인증
⑥ WiFi 통신방식 활용			VPN 인증			OAuth 2.0 인증

나. LoRa방식에서의 인증 구현예시

< LoRa망 인증 구현(예시) >

디바이스 ↔ 관리서버 간 (oneM2M)	관리서버 ↔ 애플리케이션서버 간 (OAuth)



- (게이트웨이 인증) 단말과 관리서버간 인증은 게이트웨이 인증정보를 생성하고, 생성된 ID/PWD를 이용하여 인증토큰을 전달한다.
- (디바이스 인증) 단말과 관리서버간 인증은 센서 인증정보를 생성하고 ID/PWD를 이용하여 디바이스의 인증토큰을 전달한다.
- (관리서버 인증) 관리서버와 애플리케이션 서버간 인증은 최초인증 사용자 검증하는 OAuth인증을 통하여 인증된 Code를 발급받고, Access토큰 발급을 통하여 애플리케이션에 접근한다.

4. 정부사물인터넷 연동 및 연계

서비스 확장성을 위해 외부 영역과 연동 및 연계가 필요한 경우가 있다. 외부 영역은 행정기관 자기 영역과는 서비스 환경, 인프라 구성방법 등의 차이로 보안수준에 차이가 있기 때문에 외부 영역과의 연결 시 적절한 보안방안이 필요하며, 방화벽・DDoS장비 등 보안시스템의 도입, NAT 및 VPN 기술 적용 등으로 내・외부 영역 간 연동・연계 영역을 구축하여 해결한다.

□ 네트워크(망)간 연동보안 대책

- (공중망·독립망 이용시 VPN연결 구성) 인터넷과 같은 공중망(public network)을 마치 전용선으로 사설망(private network)을 구축한 것처럼 사용할 수 있는 방식을 가상사설망을 구성한다. ※ 관련 장치는 CC인증 제품 사용
- (NAT장비 도입) 인터넷 보안제품에서 사용되는 네트워크 기술. 외부 네트워크에서 알려진 공인 주소와 다른 IP주소를 사용하는 내부 네트워크에서 IP주소를 변환하는 것. 한정된 하나의 공인IP를 여러 개의 내부 사설 IP로 변환하여 공인 IP를 절약하고, 외부 침입에 대한 보안성을 높이기 위한 기술을 적용한다.
- (DDoS 시스템 도입) 다수의 악의적인 사용자가 특정 사이트에 동시에 접속하여 과도한 트래픽을 일으켜 정상적인 서비스를 방해하는 크래킹(cracking), DoS (Distributed Denial of Service. 분산서비스거부공격)을 방어하는 시스템을 구축한다.
- (모바일서비스 게이트웨이 시스템 도입) 통신사업자 상용망과 정부망 연동시는 통신망 구간 및 모바일 플랫폼간 보안강화를 위하여 게이트웨이를 도입한다.

□ 외부서버와 연동보안 대책

- (망간 자료전송 시스템 구축) 인터넷PC와 업무PC간의 자료 전송 또는 공개서버와

업무서버 간 실시간 업무연계 시 망간 자료전송 운영

- 업무망과 인터넷망간 자료를 송·수신 할 경우, 해당 자료에 대한 로그기록 유지
- 업무망 PC에 저장된 주요 자료를 외부로 반출할 경우, 보안담당관 승인 및 반출목적 등을 기재한 서약서 징구

※ 망연계 시스템 구축관련 세부사항은 "국가·공공기관 업무망 인터넷 간 안정한 자료전송 보안가이드라인(2010.8)"을 참고하면 된다.

□ 센서 단말 인터페이스별 연동보안 대책

- 하드웨어적으로 발생 가능한 위험 요소는 외부인터페이스 위험, 물리적 접촉에 의한 위험 등이 있을 수 있다.
- 외부 인터페이스에 의한 보안 위험은 단말에서 정보 전송 및 전달을 위해 외부로 노출된 인터페이스 (이더넷, USB 등), 유지보수를 위하여 노출된 인터페이스(USB, UART 등)와 디버깅을 위해 만들어 놓은 인터페이스 (JTAG)를 통해 이루어진다.
- 외부 인터페이스 보안 위협에 대한 각 유형별 대응 방안은 아래 표와 같으며, 해당 내용을 확인해야 한다.

< 디바이스 인터페이스별 보안 대책 >

외부인터페이스 유형	인터페이스 종류	대책
일반 인터페이스	이더넷, USB	• 사용자 인증, 로깅 등을 통한 접근제어 • 네트워크 구간 암호화를 통한 스니핑 방지
유지보수용 인터페이스	USB, UART	• 커넥터에 대한 물리적 시건 장치 사용, 사용자 인증을 통한 접근제어 확인
개발용 인터페이스	JTAG	• 개발 종료 후 커넥터 제거

제3절 도입 단계별 보안 고려사항

1. 도입 전 고려사항

□ 시큐어 코딩 적용 여부 확인

- 시큐어 코딩이 적용되지 않은 경우, 해당 취약점을 통한 해커의 공격이 가능하다.
- 시큐어 코딩을 증명할 수 있는 인증서를 통해서 디바이스 및 납품 시스템의 소프트웨어 안정성을 확인한다.
- 오픈 소스를 사용하는 경우에는 사용한 오픈소스의 리스트와 적용 버전 및 보안 패치 적용 여부 등을 확인한다.

□ 물리적 보안 확인

- 디바이스 보드 내에 디버그 포트(UART, JTAG)나 물리적 접촉에 의한 데이터 추출 가능 여부를 확인하여 물리적 접촉에 의한 해킹 공격의 가능 여부를 확인한다.

□ 데이터 보안

- 서비스 관점에서 보호해야할 데이터를 암호화 등을 통해 보호할 수 있는지 확인 한다.
- 기기 및 시스템 공급자는 보호 대상인 데이터에 대해서 보안 제공 방안을 제시해야한다.
- 서비스 관점에서 보호해야할 데이터에는 아래 표와 같은 항목들이 있다.

< 보호 대상 데이터 예시 >

구분	보호 대상 데이터
콘텐츠	• 단말에서 생성된 데이터, 음성, 사진, 동영상 등
사용자 정보	• 사용자 개인 정보, 인증정보, 위치 정보 및 사용이력
기기 정보	• 기기 자체 정보(기종, ID, 시리어 번호 등) • 기기 인증정보
소프트웨어 상태 정보	• 소프트웨어 동작 상태, 네트워크 이용 상태 등
설정 정보	• 동작관련 설정 정보 • 네트워크 설정 정보 • 권한 설정 정보 • 버전
소프트웨어	• 펌웨어, OS, 미들웨어, 어플리케이션 정보 등
설계 정보	• 시스템을 구성하는 모든 기기 및 소프트웨어에 대한 사양 및 설계 정보

2. 구축 시 고려사항

□ 네트워크 보안

- IoT 네트워크에서 디바이스와 게이트웨이 사이 통신이 암호화 되지 않은 상태로 이루어질 경우, 공격자는 스니핑을 통해 수집한 데이터의 분석을 통해 명령체계를 확인할 수 있고, 이를 통해 해당 디바이스를 공격할 수 있다.
- 이를 방지하기 위해서는 데이터 전송시 암호화를 진행해야하고, 비정상적인 데이터의 차단할 수 있어야한다.
- 공급자는 네트워크 구간별로 보안 제공 방안을 제시하고, 제시된 구조로 구축해야한다.
- 또한 제어 명령 사용시 사용자에 알림 메시지를 전송하여 사용자에게 제어의 처리 결과를 알려주어야 한다.
- 사업자 IoT망을 사용하는 경우, 사업자가 제공하는 IoT 플랫폼과 각 행정기관 내 서비스 사이의 네트워크 보안 방안을 협의 하여야한다.

3. 운영 시 고려사항

□ 인증/접근제어

- 인증에는 ABP(Activation by Personalization)방식과 OTAA(Over The Air Activation) 방식이 존재한다.
- 정보유출이 가능한 ABP보다는 OTAA 방식의 사용을 권장하고, 구매시 OTAA의 지원 가능 여부를 확인해야한다.
- 초기설정 ID/PWD를 변경하지 않은 채 사용하거나 유지보수용 계정 및 하드코딩 된 계정이 삭제되지 않은 채 출시되어 해커가 손쉽게 IoT기기 관리자 권한을 획득하여 악성코드를 감염시킬 수 있다.
- 초기설정 ID/PW를 변경하거나 구입 제품에 유지보수용 계정을 삭제하였는지 확인해야한다.

□ 소프트웨어 보안

- IoT 서비스를 구성하는 각 장치에서는 소프웨어적인 보안 취약점이 발생할 수 있다.
- 소프트웨어에 문제가 발생할 경우, 보안 취약점에 대한 업데이트를 진행할 수 있어야한다.
- 납품 업체는 소프트웨어 업데이트 절차를 제시해야하고, 불법적인 소프트웨어 업데이트가 변조가 발생한 경우, 이를 인지하고 방지할수 있는 방안을 제시해야한다.

□ 보안키 관리

- IoT 시스템에서 사용되는 보안 관련 모든 키는 생성, 저장, 분배, 접근통제 및 파기를 위한 각 각의 처리 절차가 있어야한다.
- 납품 업체는 보안 관련키의 관리 방안을 제시해야한다.

제4절 도입 단계별 보안 진단항목

<보안등급 범례> 필수 ○, 권고 △, 해당사항 없음 ×

구분	지침	세부지침	내용	검증방법	보안 등급	
					Ⅰ형	Ⅱ형
설계·개발	정보보호와 프라이버시 강화를 고려한 G-IoT 서비스 시스템	G-IoT 서비스 시스템 분석을 통한 위험요소 인식	G-IoT 서비스 제공 관점에서 보호되어야 하는 기능이나 정보 등을 특정한다	-전송되는 중요정보 목록 확인 -정보 암호화 알고리즘 확인 -기기에서 처리되는 정보 종류 확인 -비식별화 방법의 적절성 확인	○	○
		G-IoT 서비스 시스템의 특성을 고려한 보안 서비스 구현	경량화된 보안 서비스를 구현해야 한다.	-KS X ISO/IEC 19790의 검증대상 알고리즘 사용 여부 확인 -KISA 및 NIST에서 제시한 테스트 벡터값을 적용하여 구현 정확성 검증	△	△
			인증정보를 안전하게 저장해야 한다.	-소스코드를 통해 하드코딩 되거나 평문으로 저장되는지 확인 -사용자 계정 및 중요 설정정보를 파일 형태로 추출 하는 기능이 있는 경우, 추출된 파일이 평문으로 되어 있는지 확인	△	△
	보안성이 확보된 소프트웨어 및 하드웨어 개발	하드웨어 공격을 상정한 하드웨어 설계	불필요한 외부 인터페이스를 비활성화해야한다.	-외부에 노출된 인터페이스는 제품 사용 설명서 또는 제조사가 제공하는 문서로 확인 -필요한 외부 인터페이스라도 비인가된 접속을 방지하기 위한 접근통제 기능이 적용되었는지 확인 -불필요한 외부 인터페이스가 존재할 경우 제거하거나 비활성화 가능여부를 확인	○	△
			비인가자의 내부 포트 접근에 대한 대처를 해야한다.	-제조사에서 제출한 제품 사용 설명서를 기반으로 내부 인터페이스 유무를 확인 -제거가 불가능한 인터페이스는 비활성화 여부를 확인하고, 사후 관리 및 디버깅에 필요한 인터페이스는 접근통제 기능이 적용되어 있는지 확인	○	△
			비인가자의 무단조작에 대한 대처를 해야한다.	-무단 조작 접근 방지기능과 접근 검출 방법이 구현되어 있는지 확인	○	△

구분	지침	세부지침	내용	검증방법	보안 등급	
					Ⅰ형	Ⅱ형
			유지보수 시의 위험 요소, 유지보수 도구에 의한 위험요소를 고려해야한다.	-JTAG와 같은 디버그 접근 차단 기능을 제공하는지 확인	○	△
			소프트웨어 및 하드웨어는 관련 기술의 최신 표준을 준용해야한다.	-제품 버전관리 문서를 기반으로 최신기술 준용 확인	○	○
		보안 취약점 사전 예방을 위한 소프트웨어 개발	개발 시 시큐어 코딩을 적용해야한다.	-소스코드 보안 분석 도구를 이용하여 소프트웨어에 대한 보안약점을 점검하고, 보안약점이 존재하는지 확인 -상용 또는 신뢰할 수 있는 공개용 보안취약점 점검도구를 사용하여 개발 기기의 보안 취약점 점검 및 제거 여부를 확인	○	△
			오픈소스 라이브러리를 사용 시에는 보안성 검토를 수행해야한다.	-보안취약점 공개영역(예, KrCERT, CVE, NVD, Security Focus, 논문 등) 을 통해 기기에 해당하는 보안취약점 존재 여부를 확인	○	△
			설계부터 양산 단계에 이르기까지 소프트웨어에 대한 보안성 검증 및 평가를 실시한다.	-소프트웨어 개발 방법론을 적용 여부 확인	△	△
배포.설치.구성	안전한 초기 보안설정	초기 구축시 네트워크 연결 방법 고려	연결구간 별로 보안을 적용해야한다.	-망 구축자가 제출한 망구축 설계서 확인	○	○
		초기 구축시 설정에 유의	보안에 유의하여 초기 설정(관리자 암호, 권한 설정 등)을 수행해야한다.	-'패스워드 안전성 검증 소프트웨어'를 사용하여 비밀번호를 검증 -기기에서 제공하는 서비스(포트) 및 목적, 용도 등을 확인함 -포트 스캔 등을 통해 불필요한 서비스가 존재하는지 확인함 -외부 접속 포트 사용 시, 해당 포트 접근을 위한 추가적인 보안 조치를 확인함	○	○

구분	지침	세부지침	내용	검증방법	보안 등급	
					Ⅰ형	Ⅱ형
				-인가된 사용자에 의해 서비스 활성화 가능 여부를 확인함		
	안전한 G-IoT 서비스 제공을 위한 안전한 파라미터 설정	보안 강화를 위한 안전한 파라미터 설정	G-IoT 단말의 보안 위협 및 고장에 대한 대책을 마련해야한다.	-고장 주입을 통한 기능 시험으로 네트워크 연결 해제 확인	○	○
			G-IoT 서비스의 유형이나 제공하는 기능에 따라 파라미터 변조를 통해 발생할 수 있는 위협에 대한 대책을 마련해야 한다.	-제조사의 보안 파라미터 설정을 확인	○	○
운영.관리.폐기	G-IoT 제품.서비스의 취약점 보안패치 및 업데이트	시스템 보안 취약점 대응 및 사후조치	G-IoT 서비스 제공자는 G-IoT 단말 보안 업데이트 등을 필요한 시기에 적절하게 실시하는 방법을 검토하고 적용해야한다.	-업데이트 수행 전 사용자 인증 기능을 제공하는지 확인 -기능 시험을 통해 업데이트 실패 시 롤백 기능의 존재 여부를 확인 -기능 시험을 통해 롤백 후, 기기가 정상 동작하는지 확인	○	△
			G-IoT 단말 제조사는 단말의 기본 기능에 보안 취약점이 존재하지 않도록 관리해야한다.	-제조사의 보안 관리 프로세스가 정의된 문서 확인	○	△
		네트워크 보안 취약점 대응 및 사후조치	폐쇄적인 네트워크로 운영되는 G-IoT 서비스 시스템에도 일반적 네트워크에서 전제되는 위험 요소를 고려해야 한다.	-보안 지침서 확인 -정기적 보안 교육 확인	○	○
			G-IoT 네트워크의 모든 통신구간에서 보안을 위한 기밀성, 무결성, 가용성 및 인증 측면에서 정보 보호를 고려해야 한다	-네트워크 트래픽 허용 및 차단 목록을 확인함 -허가된 프로토콜 목록 및 등록사유를 확인함	○	○
	안전한 운영 및 관리를 위한 정보보호 및 프라이버시 관리체계	소프트웨어/하드웨어 보안 취약점 상호 인지	G-IoT 서비스 관리자는 G-IoT 서비스 이용시 발생할 수 있는 보안 취약점을 분석하여, G-IoT 서비스 제공자 및 G-IoT 서비스 이용자와 공유해야한다.	-보안 지침서 확인	○	○
			보안 취약점 발생시 G-IoT 서비스 이용자로부터 보고 받아 즉	-보안 지침서 확인 -정기적 보안 교육 확인	○	△

구분	지침	세부지침	내용	검증방법	보안 등급	
					Ⅰ형	Ⅱ형
			각 조치를 취할 수 있는 신고 체계를 마련해야 한다			
		시설에 대한 물리적인 접근 방지	G-IoT 서비스 제공 시설은 인가된 보안 및 유지보수 인력만 허용하는 출입통제를 해야한다.	-보안 지침서 확인 -정기적 보안 교육 확인	○	△
			사용자 필요에 의해 기기에 저장된 중요한 정보를 삭제한 경우, 복원이 어렵도록 해야 한다	-삭제되는 중요한 정보 목록을 확인함 -중요한 정보를 삭제하는 방법을 확인함	○	△
	G-IoT 단말의 안전한 폐기를 위한 관리체계	도난 및 분실 G-IoT 단말의 관리체계	도난 되거나 분실된 G-IoT 단말의 조작 및 물리적인 공격에 대한 위험에 대비해야한다.	-보안관련 이벤트를 수행한 후 모니터링 확인	○	△
		G-IoT 단말의 폐기를 위한 관리체계	사용연한이 만료된 G-IoT 단말에서 정보를 수집하거나, 소프트웨어를 갱신하여 재판매되는 등의 위험에 대비해야한다.	-보안관련 이벤트를 수행한 후 모니터링 확인	○	△
	G-IoT 서비스 침해사고 대응체계 및 책임추적	보안 침해사고에 대비하여 침입탐지 및 모니터링 수행	G-IoT 단말의 보안 취약 상태를 G-IoT 네트워크 서버에서 확인하여, 취약점을 가진 G-IoT 단말을 선별하고, 이를 G-IoT 서비스 이용자에게 이를 통보해야 한다.	-보안관련 이벤트를 수행한 후 모니터링 확인	○	△
		침해사고 발생 원인분석 및 책임 추적 확보를 위한 로그기록 저장 및 관리	G-IoT 단말의 상태나 통신 상황을 파악하고 기록해야하며, G-IoT 서비스 이용 기록이 무단으로 삭제 또는 변조되지 않도록 해야 한다.	-보안관련 이벤트를 수행한 후 감사기록 로그를 확인함 -외부 서버로 감시기록(로그)을 전송하는 경우 정상적으로 전송 및 저장되는지 확인함	○	○

※ 보안등급 Ⅰ형 : 개인정보와 관련이 있고, 정보의 민감성이 높은 서비스에 활용되는 서비스

※ 보안등급 Ⅱ형 : 개인정보와 관련이 없거나 정보의 민감성이 낮은 서비스에 활용되는 서비스

제4장

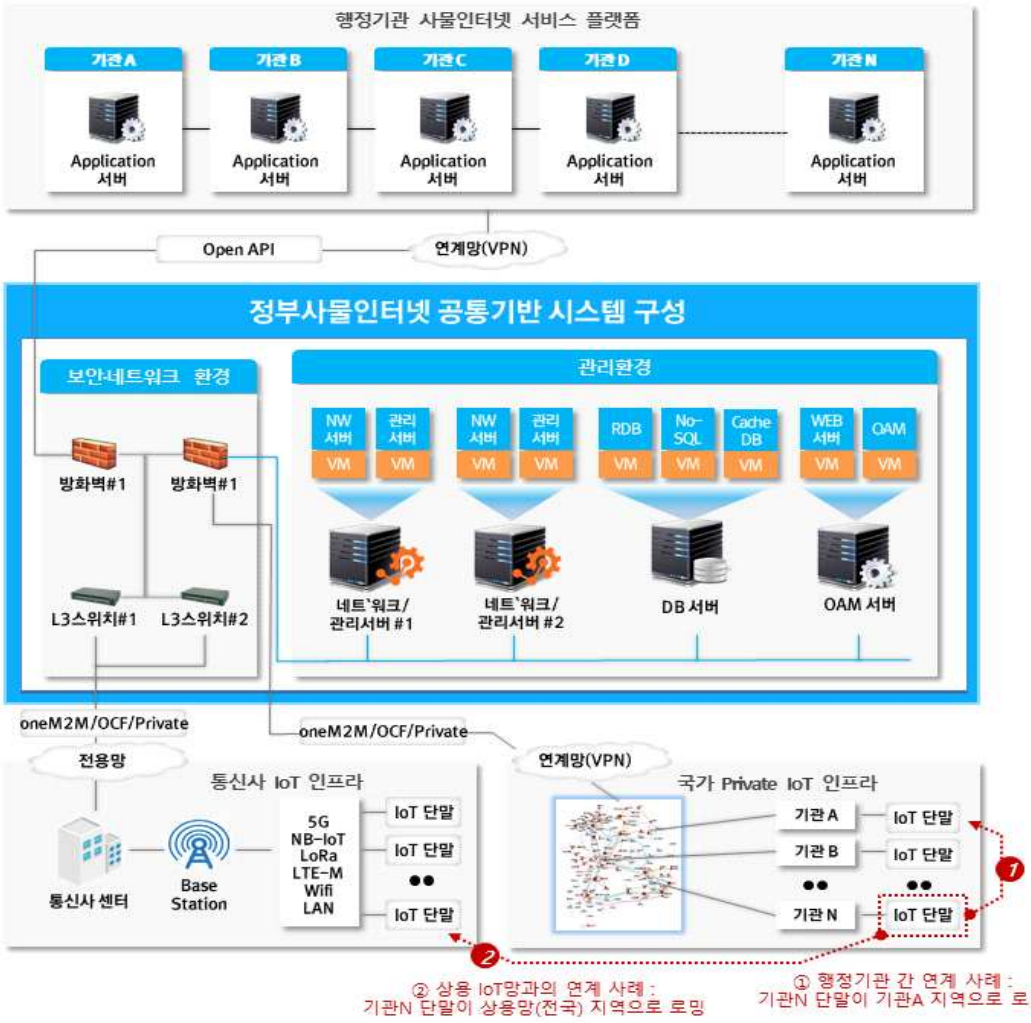
정부사물인터넷 공통기반

제1절 공통기반 소개

□ 공통기반 구성 및 역할

정부사물인터넷 공통기반은 서비스 로밍기능을 제공하여 행정기관이 서비스 지역에 대한 제약을 해소할 수 있도록 구축되었으며, 각 행정기관의 사물인터넷 디바이스 및 사물인터넷 데이터 처리, 연계 네트워크 관리 등을 위한 관리환경으로 구성된다.

< 정부사물인터넷 공통기반 시스템 구성도 >



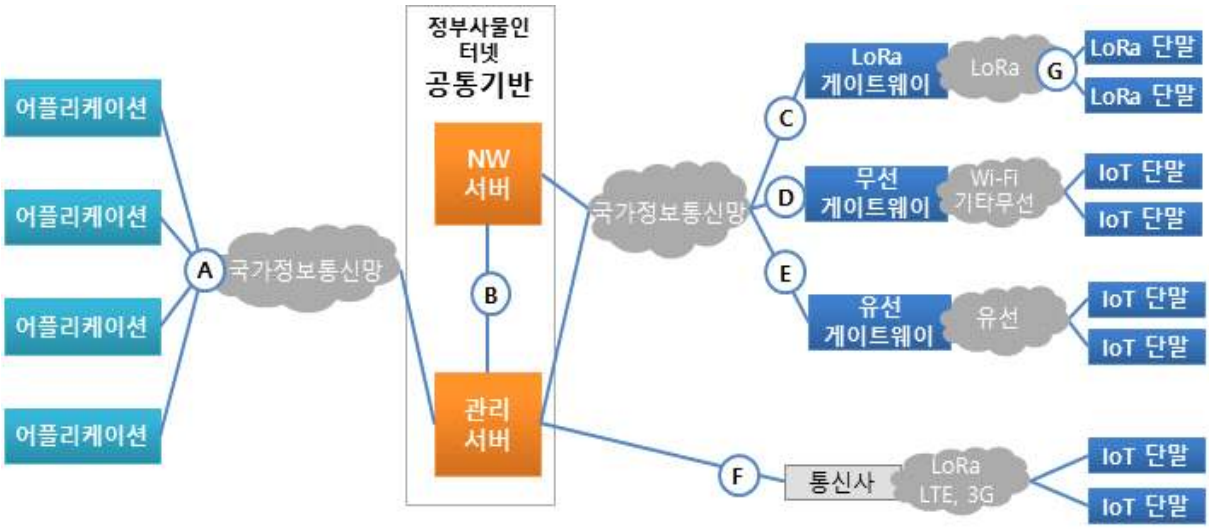
행정기관에 구축한 사물인터넷 디바이스가 해당 지역을 벗어나 타 지역으로 이동한 경우, 단말에서 생성된 데이터가 공통기반을 통해서 사물인터넷이 속한 행정기관으로 전달된다.

□ 공통기반 프로토콜

정부사물인터넷 공통기반과 행정기관의 사물인터넷 서비스 인프라와의 연계는 상호운용성 및 확장성을 위해 표준 프로토콜에 따른다.

주요 연동 인터페이스 구간 및 프로토콜은 아래와 같다.

< 정부사물인터넷 주요 연동 인터페이스 구간 >



< 정부사물인터넷 주요 연동 인터페이스 구간별 적용표준 >

인터페이스 구간		프로토콜	보안방식	인증방식	메시지포멧
Ⓐ	**애플리케이션 ⇔ 관리서버**	Rest API	TLS	OAuth 2.0	Json, XML
Ⓑ	**관리서버 ⇔ 네트워크서버**	oneM2M	TLS	OAuth 2.0	Json
Ⓒ·Ⓖ	**네트워크서버 ⇔ LoRa단말**	LoRaWAN	AES128	Basic (AppEUI, DevEUI, App Key)	-
Ⓓ·Ⓔ	**관리서버 ⇔ IoT단말**	oneM2M OCF	TLS DTLS	OAuth 2.0 또는 Basic (DevID, Token)	Json, XML
		Private	TLS	-	-
Ⓕ	**관리서버 ⇔ IoT단말**	oneM2M OCF	TLS DTLS	OAuth 2.0 또는 Basic (DevID, Token)	Json, XML
		Private	TLS	-	-

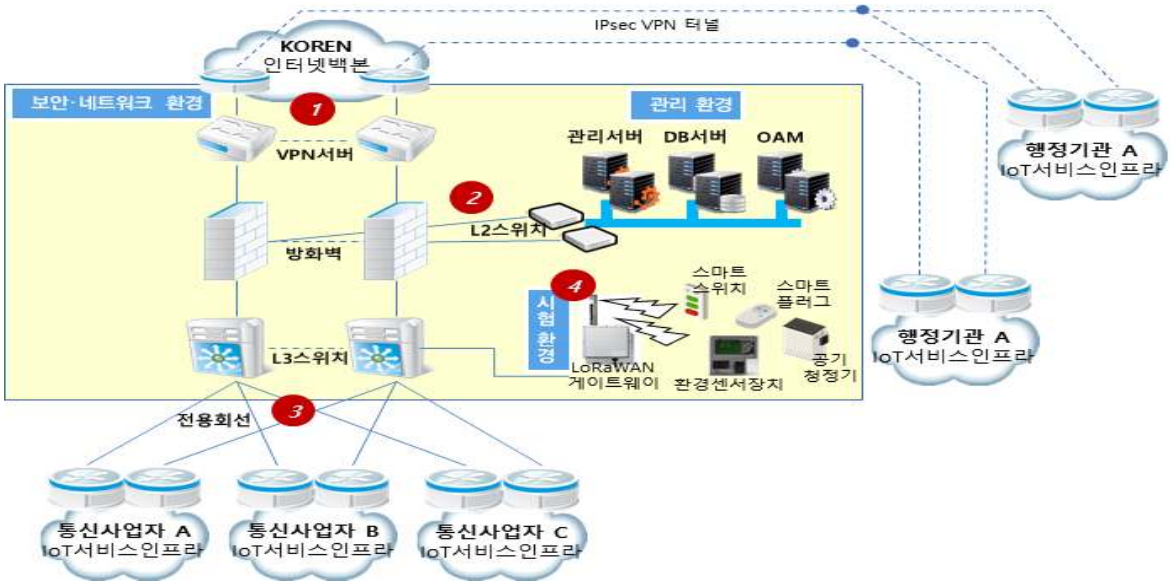
제2절 보안 및 네트워크 환경

1. 네트워크 환경

정부사물인터넷 공통기반의 보안·네트워크 환경은 크게 4개 부분으로 구성된다.

그림의 “❶”의 부분은 행정기관에서 공통기반을 활용할 수 있도록 연계하는 네트워크 이며, “❷”는 연계 행정기관에 대한 디바이스 등록·변경 등 서비스를 구성하고 운영관리하는 관리 환경과의 연계 네트워크, “❸”은 상용 IoT 망 또는 서비스를 이용하는 행정기관에 대해 공통기반을 활용할 수 있도록 통신사업자와 연계하는 네트워크, 마지막으로 “❹”는 IoT디바이스, 무선국 등 정부사물인터넷 관련 구성요소에 대한 보안성, 안정성을 시험·검증할 수 있도록 구축된 시험 환경과의 연계 네트워크이다.

< 공통기반의 보안·네트워크 환경 구성도 >



□ 행정기관 연계 네트워크

행정기관이 쉽게 공통기반과 연계망을 구성할 수 있도록 VPN서버가 구축되어 있다. 행정기관은 인터넷(전용회선 인터넷, 모바일 인터넷 등)을 통해 IPsec 암호화 VPN(보안성 강화)으로 연결한다.

이때 전송지연 등 서비스에 지장을 주는 요인이 발생하지 않도록 회선 대역폭을 충분하게 확보하는 등 회선품질에 유의해야 한다. 향후 서비스 품질 보장을 위해 정부사물인터넷을 위한 전용망을 확보하여 연계망 전환을 추진할 계획이다.

□ 관리환경 연계 네트워크

관리환경은 행정기관 간 연계와 관련 통신사업자 사물인터넷 망 및 서비스 플랫폼을 연계하여, 서비스 확장 및 다양한 융·복합 서비스 구현하는 중요한 시스템이므로 방화벽 등 보안시스템을 통하여 연계한다.

보안구간은 크게 세 가지로 구분된다. 첫 번째는 행정 기관 연계 구간, 두 번째는 상용 통신사업자 연계 구간, 세 번째는 시험 환경 연계 구간이다. 각 구간별 보안 취약점 특성을 반영하여 보안정책에 차별을 두어 적용한다.

2. 보안 환경

□ 물리적보안

- 출입·통제 시스템이 구축된 시설물에 공통기반을 설치하고 허가된 관리 요원만 접근이 가능
  - 비인가자 내부 인터페이스 (USB Locker, LAN Locker 등) 접근 방지, 시건장치를 통해 시스템 접근 통제
  - 허가된 요원도 인터페이스에 접근 시, 정해진 절차(접근 신청, USB 검사 등)를 통해 시스템에 접근

□ 네트워크보안

- 허가된 행정기관만 통신이 가능하도록 네트워크를 구성
  - CC 인증된 VPN 통신 장치를 통해 허가된 행정기관만 통신이 가능
- 도입된 방화벽을 통해 보안 및 인증(DDoS, 허가된 IP만 연계, G-SSL 등)
  - 지자체와 연계를 위해 보안성이 강화된 IoT 전용 VPN망을 사용하고 도입된 방화벽을 통해 보안 및 인증(DDOS, 허가된 IP만 연계, SSL 등)

□ 시스템보안

- 공통기반 시스템의 OS 및 소프트웨어의 보안
  - 원격관리 제한 및 방화벽 프로그램을 통한 시스템 접근 통제(IP Table)
  - 운영관리 시스템의 보안관리(반복된 인증 시도 제한, 비밀번호의 화면 노출 금지, 인증실패 정보 제공 금지, 세션관리, 감사기록 생성)
- 개발된 소프트웨어에 대한 시큐어 코딩 검증(KISA)

□ 운영보안

- 허가된 요원만 시스템이 접근이 가능하고 주기적으로 보안기능을 피치하고 Update 수행
- 관리 대상 인프라를 정해진 절차에 따라 보안 취약점을 점검
  - 시스템을 보안패치 및 Update를 수행하고 보안기능 설정 점검 및 운영

제3절 공통기반 구성요소별 기능

□ 공통기반 네트워크 서버 기능

공통기반 네트워크 서버는 LoRaWAN에서 정의한 네트워크 서버의 기본 기능에다가 연계된 행정기관 디바이스에 대한 로밍을 지원하기 위한 기능이 추가되어 있다. 추가된 기능은 디바이스가 타 지역으로 이동하여 방문한 지역의 네트워크 서버가 공통기반 측으로 미등록 단말 확인을 요청하는 경우, 디바이스 관리기능에 등록된 통합 단말 정보를 확인하여 이동 단말임을 인증해 준다.

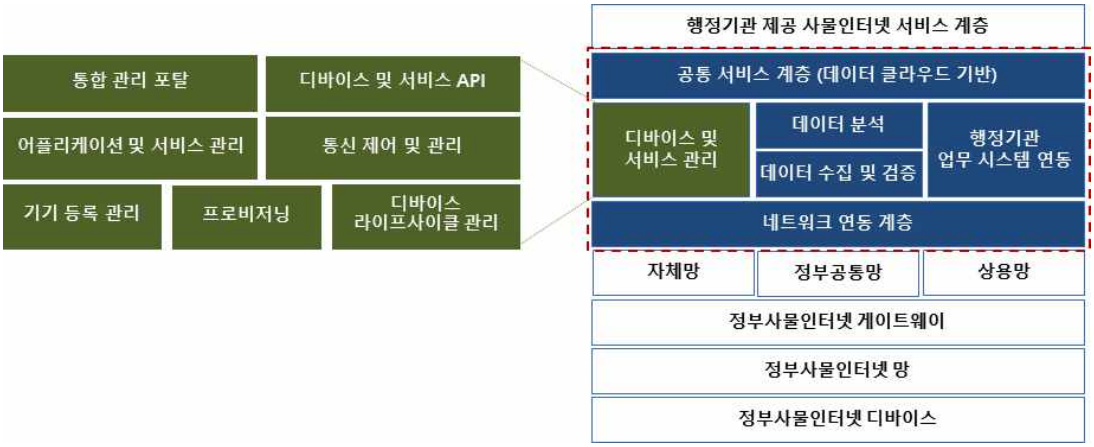
또한, 네트워크 서버 등 공통기반의 네트워크 연동 계층은 상이한 디바이스 통신 프로토콜의 연동을 지원하기 위하여 다양한 IoT 프로토콜(LoRa, MQTT, CoAP, HTTP 등)의 Transport Layer 프로토콜에 대한 인터페이스 제공과 변환 기능을 수행한다.

< 공통기반 네트워크 연동 계층 >

□ 공통기반 센서(디바이스)·서비스 관리 기능

행정기관 간 디바이스 연계를 지원하기 위하여 해당 디바이스(센서) 및 게이트웨이 등록 등 관련 서비스에 대한 정보를 공통기반 관리 서버에 통합 운영해야 한다. 공통기반의 디바이스·서비스 관리 기능은 연동 방식(상기 "제3절 2항" 참조)에 따라 이동 디바이스의 소속지역 네트워크 서버에 전달하거나, 필요한 서비스 시스템에 전달하는 역할을 담당한다.

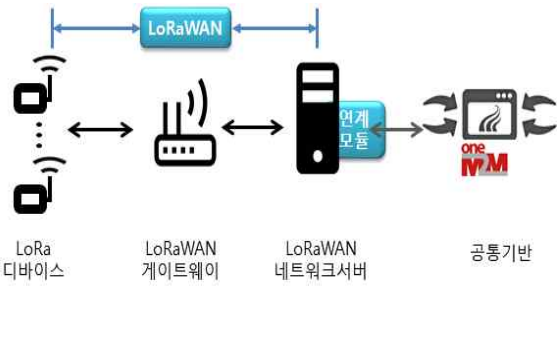
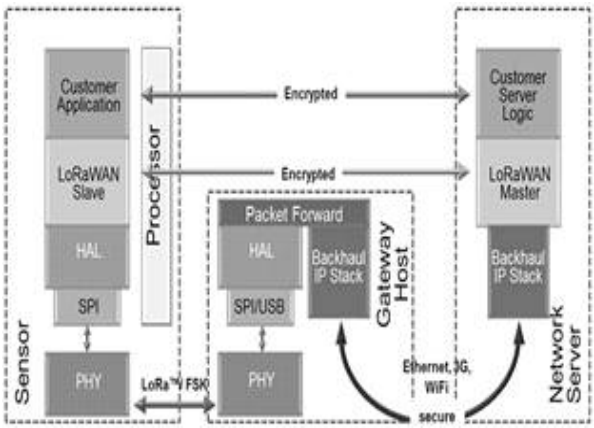
< 공통기반 디바이스·서비스 관리 계층 >



□ 센서・게이트웨이 연계

LoRaWAN을 이용하여 구축한 행정기관의 정부사물인터넷 게이트웨이 및 디바이스가 공통기반을 통해 모니터링・제어가 가능하도록 LoRaWAN 표준 프로토콜을 제공하고 공통기반과 연계가 가능하도록 LoRaWAN과 oneM2M 연동 프로토콜 바인딩을 제공한다.

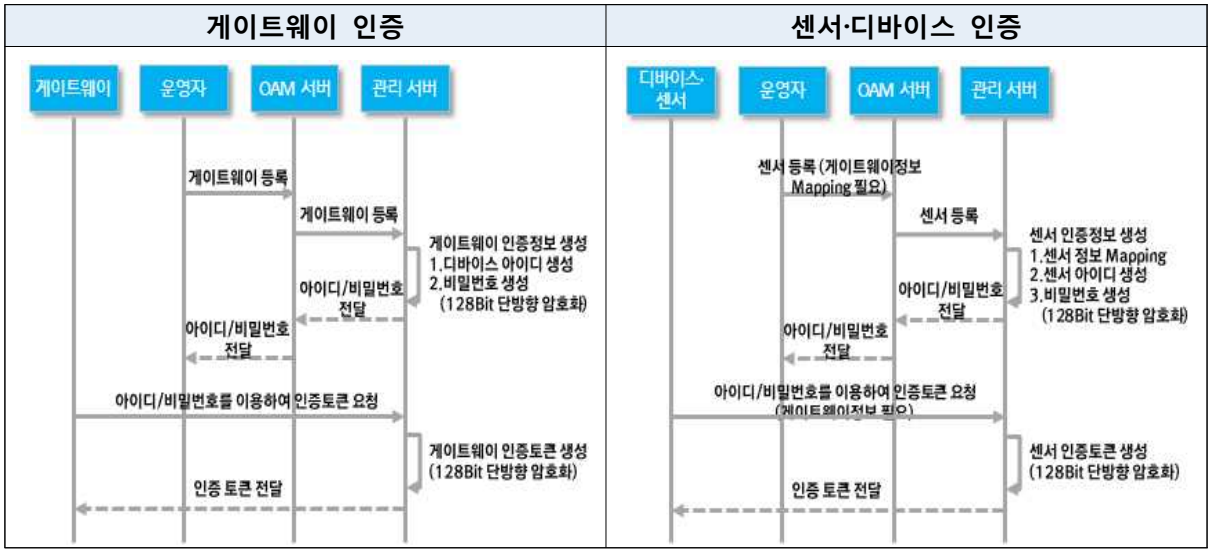
< 센서·게이트웨이 연계(LoRa예시) >

LoRa·oneM2M 적용하여 공통기반 연계	LoRaWAN 표준을 준수하여 통신
	
• LoRa Alliance의 LoRaWAN 표준 프로토콜 준수 • KC인증 LoRa 통신모듈 적용 • oneM2M 프로토콜 바인딩 규칙을 연계 모듈을 통해 제공	• LoRaWAN 표준 프로토콜을 이용한 통신 • LoRa단말 등록 절차 및 DRS 기능 지원 • AES128 보안, AppSKey/NwtSKey 키관리 • 단말, 게이트웨이 접속 실시간 관리

□ 센서(디바이스)·게이트웨이 인증

연계 서비스 제공은 사전에 등록된 디바이스(센서) 및 게이트웨이의 인증에서부터 시작한다. 공통 기반 관리 서버와 센서·게이트웨이 간 인증은 oneM2M 표준기술에 따르며, 인증받지 못한 센서·게이트웨이는 서비스에서 제외된다.

< 센서·게이트웨이 인증절차 >



□ 공통기반 관리서버 기능

공통기반의 관리서버는 통신 프로토콜을 처리하는 기능과, 정부사물인터넷 연결 및 공통기반의 제반 상황을 처리하는 운영관리 기능으로 구성된다.

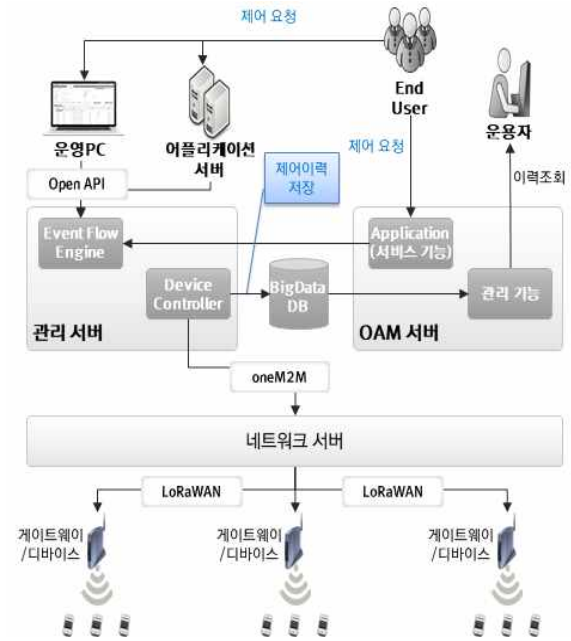
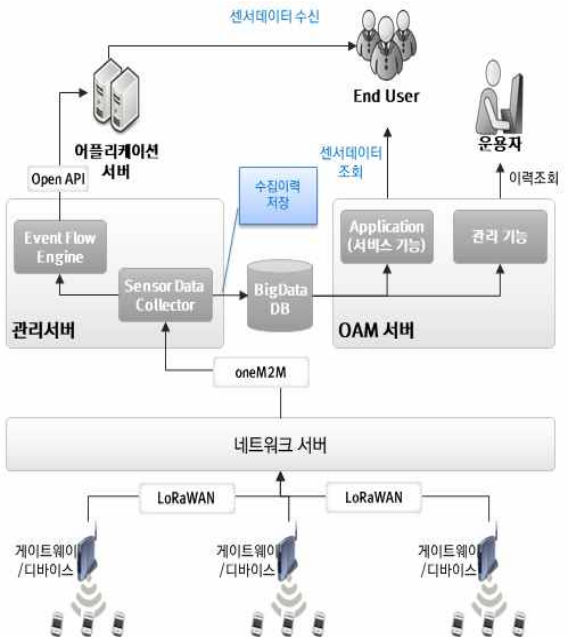
< 공통기반 관리서버의 처리 및 운영관리 계층 >

□ 관리서버의 실시간 제어 및 수집 데이터 흐름

제어 기능은 운영자가 OAM 통해 디바이스에 제어명령을 전달하면, 관리서버는 oneM2M 규격으로 네트워크 서버에게 전달하고, 네트워크 서버는 디바이스 및 서비스 정보를 확인하여 디바이스를 제어한다.

수집 기능은 디바이스가 LoRaWAN 규격으로 네트워크 서버에 센싱 데이터 등 각종 정보를 전달하면, 네트워크 서버는 oneM2M 규격으로 변환해서 관리서버에게 전달하게 된다.

< 관리서버의 실시간 제어 및 수집 데이터 흐름 >

제어 데이터 흐름도	수집 데이터 흐름도
	

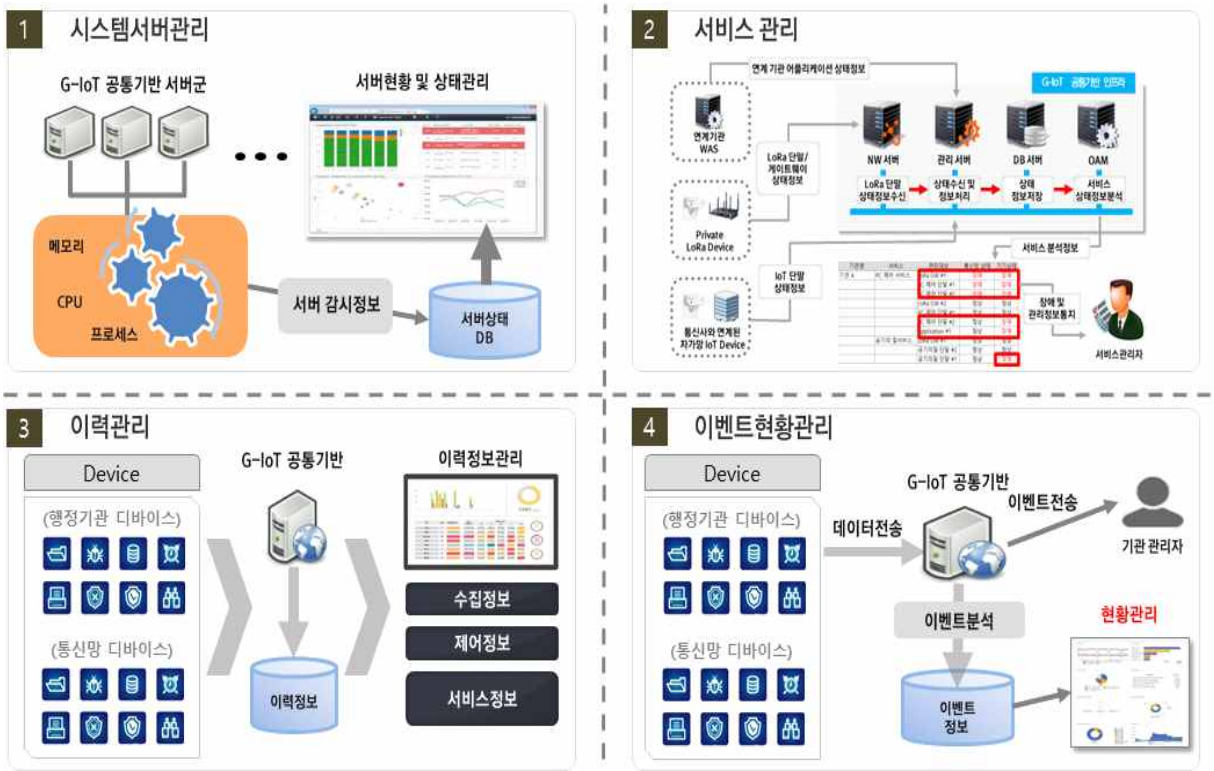
제4절 공통기반 연계 운영관리

□ 이용기관 연계 운영관리

공통기반과 연계된 서비스를 관리하기 위해 디바이스의 상태, 서버·시스템 상태, 행정기관 애플리케이션의 상태 등의 서비스 정보 모니터링 기능을 공통기반의 관리서버에서 구현하였다.

관리서버의 주요역할은 디바이스·시스템·서버 관리 및 서비스 관리, 패킷 이력관리, 각종 경고·장애 등 이벤트 발생현황 및 이력관리, 대시보드 및 이용통계 기능을 제공한다.

< 정부사물인터넷 공통기반 연계운영관리 주요기능 >



□ 연계 서비스 구성 및 관리

연계기관은 공통기반의 관리서버 및 OAM서버를 통해 연계 서비스를 구성하고 운영관리를 하게 된다. 운영관리 기능은 디바이스 관리, M2M 관

리, 서비스 관리, 운영담당자 관리, 통계 관리 그리고 종합 대시보드로 구성된다. 메뉴 구성은 아래와 같다.

운영관리시스템은 로그인 후 권한에 따라 접근할 수 있는 메뉴가 따로 있다. 이용기관의 운영담당자는 연계된 해당 서비스를 관리할 수 있고, 공통기반 운영담당자는 전체 메뉴에 접근하여 운영관리할 수 있다.

< 공통기반 운영관리(서비스 등록 등) 메뉴 구성 >

제5절 공통기반 연계절차

행정기관이 사물인터넷망 공통기반과 연계를 위해서는 연계관련 사전협의를 통해 연계 가능여부를 검토한 후 아래 절차에 의거 진행한다.

□ 절차

연계절차	단계별 수행 내용
연계관련 사전협의 (연계기관→ 행안부)	• 공통기반 이용 및 연계 관련 협의 - 연계 대상, 이용 목적, 용도 서비스, 이용 기간 - 연결 노드, 접속 방식, 연계 속도 등 • 공통기반 연동규격 검토 및 조정 - 필요시 기술교육, 세부절차 및 고려사항 협의·조정
↓	↓
연계신청 (연계기관→ 행안부)	• 이용기관은 전자문서를 통해 행정안전부로 이용 신청 (신청서 서식 "붙임") - 공문수신처 : 행정안전부 정보자원정책과
↓	↓
검토 및 승인 (행안부→ 연계기관)	• 이용자격 여부 및 접속환경 등 검토 후 공문으로 신청기관에 결과 회신 - 서비스 설정방안, 실무자 연락처 등 관련 안내사항 포함
↓	↓
준비	• 신청기관과 공통기반 연계 준비 - (이용기관) 기관 측 통신장비 준비, 개통일 협의 - (통신사업자 : 필요시) 물리적 통신회선 연계 등 - (행 안 부) 작업계획 수립, 전환 일정 및 계획 확정
↓	↓
연계	• 공통기반 설정 완료 및 이용 - (이용기관) 기관 측 관련 시스템 설정(개발*포함) 등 작업지원, 서비스 확인 * 행정기관에서 자체 개발할 경우, 개발 완료 후 국가정보원 보안검증 및 공통기반과의 연계 테스트 결과서를 운영기관에 제출 - (행안부) 공통기반 측 관련 시스템 설정 등 작업지원**, 서비스 확인 ** 운영기관의 작업지원 사항 - 로밍기능을 포함한 공통기반 연동 규격서 배포 및 기술 교육 - 공통기반과의 통신연계 확인, 단말등록 및 서비스 정상 동작 확인 - 공통기반 활용을 위한 행정기관 연계 단말 및 서비스 개발 지원 - 기타 단대단 통합 테스트 지원 등

- 붙임 -

1. 정부사물인터넷 사업자선정 체크리스트

2. 정부사물인터넷 보안 체크리스트

3. 정부사물인터넷 공통기반 연계신청서

붙임1. 정부사물인터넷 사업자선정 체크리스트

1. 주요 확인사항(공통)

구분	확인 사항	평가
표준 준수 (호환성상호운용성 확보 관련)	1) 관련 표준을 준수하여야 함 - 부문별 관련 표준목록 및 해당내용 제시 - 항목별 해당 표준 준수에 대한 세부내용 제시	
	2) 국제표준 준수가 어려울 경우 타당한 사유와 대응방안을 제시하여야 함 - 미준수 항목별 타당한 사유와 근거를 제시 - 해당 항목별 대응방안 및 이행 확약서 제출 (확약내용, 확약기간, 유·무상* 구분 등 * 유상의 경우 합당한 사유 및 산출근거 제시)	
	※ 표준 미준수, 호환성·상호운용성 확보 미확약 등에 따른 문제 발생시 상호 책임한계 구분 및 사후조치에 대한 협약 고려필요	
보안 내재화	1) 사물인터넷 서비스의 설계 및 개발, 설치, 운영 및 관리, 폐기까지 전주기에 걸쳐 발생할 수 있는 보안위협을 정의하여 제시하여야 함	
	2) "1)"의 위협에 대응할 수 있도록 취약점 및 보안 요구사항을 정의하고 이에 대한 보안 내재화 방안 제시 및 이행하여야 함	
개인정보 보호	1) 사물인터넷은 직·간접적으로 개인정보를 담고 있거나, 데이터 분석에 의한 사생활 침해소지가 크므로 관련 법·제도* 및 규정에 따라 개인정보 보호를 구현하여야 함 * 개인정보보호법, 위치정보법, 정보통신망법, 전기통신사업법, 정보통신진흥특별법 등	
서비스품질 확보	1) 서비스 품질이 확보될 수 있도록 무선통신 품질을 강화*하고, 각 구간 통신대역폭 및 장비용량, 플랫폼을 구성하는 서버 및 시스템 용량이 충분하게 확보·유지될 수 있도록 구성하고 운영**하여야 함 * 설치완료 후 실제 무선망 설계에서 제시한 커버리지, 전파 수신감도 등을 측정하여 음영지역 파악·개선 등 무선망을 최적의 상태로 구성하고 주기적으로 점검·정비 ** 운영결과는 주기적으로 발주기관에 보고 - 보고 항목은 별도 협약(GNS의 경우 이용지침서 SLA 참조)	
공통기반 연계 (서비스 확장성 확보 관련)	1) 발주기관이 정부사물인터넷 공통기반을 활용할 수 있도록 관련 네트워크 및 시스템에 대한 연계 방안을 제시하여야 함	
	2) 제공사(납품·구축 포함)는 발주기관 및 공통기반 운영기관 요청* 시 관련 연계 및 이용에 대한 지원을 하여야 함 * 해당 연계가 사업기간 이후에 발생되는 경우 등 사후 연계 요청에 대한 연계구성 및 기술지원 확약(협약시 명시 필요)	
기술지원	1) 발주기관에 제공된 사물인터넷 디바이스·센서 등 서비스 관련 기기들에 대한 업그레이드 등 지속적인 기술지원 서비스를 이행하여야 함	

2. 상용 IoT 사업자 선정시 고려사항

구분	고려 사항	비고
커버리지	1) 서비스 도입 지역 내 음영지역 유무	
	2) 음영 지역 발생 시 해당 이동통신사의 음영지역 해소 방법 및 기간	
디바이스 적합성	1) 해당 이동통신사에서 요구하는 디바이스 인증 요건	
	2) 해당 이동통신사의 자체기구 또는 지정 인증기관의 인증서 취득 시 복잡도 및 기간	
디바이스 등록용이성	1) IoT 서비스 도입 시 해당 이동통신사의 디바이스 등록 프로세스의 복잡도	
	2) 등록요청 후 처리기간	
서비스 등록용이성	1) 신규서비스 등록에 필요한 복잡도 및 기간	
	2) 해당 이동통신사의 지원 범위 (개발 및 테스트 환경 등)	
시스템 환경	1) 해당 이동통신사가 제공하는 시스템의 범위 (게이트웨이, 백홀, 네트워크서버, 서비스 플랫폼 등)	
	2) 국가기관 시스템과 연동 필요 시 연동 용이성	
데이터보안	1) 해당 이동통신사의 보안수준	
	2) 이용 이동통신사를 포함한 외부기관에 데이터 유출 불가시 자체망 구축 권고	
망 사용료 및 기타비용	1) 해당 이동통신사의 망 사용료, 서비스 등록비용, 디바이스 등록비용 그리고 기타 서비스 적용에 필요한 비용	
	2) 해당 이동통신사 지불 비용과 자체망 구축비용을 비교분석하여 선정	

붙임2. 정부사물인터넷 보안 체크리스트

[출처 : "국가·공공기관 사물인터넷(IoT) 보안 가이드라인" 부록1, 국가정보원]

보안단계	영역	항목	비고
도입 시	공통	인터페이스 보호	
		비인가자의 내부 포트 접근 방지	
		시큐어코딩 적용	
		모바일 앱의 보안성 고려	
		불필요한 서비스 제거	
		원격관리 제한	
		중요정보의 저장 및 처리	
		침입탐지·모니터링 제공	
		악성코드 탐지·제거	
	단말기 (디바이스)	초기 인증정보 변경	
		사용자 신원 검증 선행	
		반복된 인증 시도 제한	
		인증정보의 관리	
		비밀번호의 화면 노출 금지	
		인증 실패 정보 제공 금지	
		세션 관리	
		업데이트 관리	
		감사기록 생성	
		단말기 관리 및 파기	
	네트워크	ICT 정보보호시스템 적용	
		네트워크 분리 및 보호	
		전송정보 보호	
	플랫폼·서비스	접근 객체 인증	
		최신 업데이트 및 보안패치 적용	
		불필요한 서비스 제한 및 보안 설정	
		가용성 보장	
운영 중		보안 취약점 점검 및 모의침투 수행	
		체계적인 보안패치 방법론 확보·운영	
		보안기능 설정 점검·운영	
		침입탐지 및 모니터링 수행	
		로그 기록 저장·관리	
		인터페이스(USB 등) 관리	

붙임3. 정부사물인터넷 공통기반 연계신청서

1. 신청기관 및 연락처

기관명		부서명	
담당자*		연락처**	

* 신청내용에 대한 확인 및 협의를 담당하는 실무자

** 사무실 전화번호(자료전송 필요시 메일 주소 기재)

2. 신청 내용

구분		내 용		
신청 구분		□신규	□변경	□해지
이용 구분		□네트워크 연계	□서비스 연계	□공통기반 플랫폼 (가상화) 활용
세부 신청내용*				
연계 방식	접속장소			
	접속방식	□인터넷, ( )Mbps	□전용회선, ( )Mbps	
	기타사항**			
개통희망일				
이용 기간				
비 고				

* 이용 목적, 서비스 내용 및 주요 대상, 연계 규격 등 연계 구성 및 방식 검토를 위한 구체적인 정보(필요시 네트워크 간략 구성도 등 첨부)

** 인터넷 접속시 VPN 구성을 위한 정보, 전용회선의 경우 네트워크 구성경로 정보 등