

---

# 재난안전통신망 장비 · 서비스 도입 · 개발 가이드라인

---

2024. 4.



행정안전부

# 목 차

## 1. 개요

1.1. 추진배경 .....	1
1.2. 작성 근거 및 목적 .....	1
1.3. 가이드라인의 주요 내용 .....	1
1.4. 가이드라인의 적용 범위 .....	1

## 2. 재난안전통신망 소개

2.1. 개요 .....	2
2.2. 재난안전통신망 구축 현황 .....	3
2.2.1. 재난안전통신망 시스템 .....	3
2.2.2. 재난안전통신망 주요 기능 .....	8
2.2.3. 재난안전통신망 제공 기술 .....	10
2.2.4. 재난안전통신망 기본서비스 .....	12

## 3. 재난안전통신망 기반 응용서비스 소개

3.1. 개요 .....	25
3.2. 응용서비스 아키텍처 .....	27

## 4. 단계별 주요 수행내용 및 절차

4.1. 개요 .....	28
4.2. 기획 단계 .....	30
4.2.1. 기획 단계 업무흐름도 .....	30
4.2.2. 서비스 기획 .....	30
4.2.3. 서비스 확정 .....	38
4.3. 개발 단계 .....	40
4.3.1. 개발 단계 업무흐름도 .....	40
4.3.2. 서비스 상세설계 .....	40
4.3.3. 서비스 개발 .....	42
4.4. 구축 단계 .....	50
4.4.1. 구축 단계 업무흐름도 .....	50
4.4.2. 시스템 구축 .....	51
4.4.3. 서비스 검증 .....	56
4.4.4. 서비스 개통 .....	60
4.5. 운영 단계 .....	62
4.5.1. 운영 단계 업무흐름도 .....	62
4.5.2. 계획수립 .....	62
4.5.3. 운영 및 점검 .....	62
【붙임 1】 재난안전통신망 관련 법·제도 .....	64
【붙임 2】 재난안전통신망 관련 표준 .....	68
【붙임 3】 사용기관의 응용서비스 적용을 위한 체크리스트 .....	70
【붙임 4】 개발조직의 응용서비스 적용을 위한 체크리스트 .....	71
【붙임 5】 재난안전통신망 연동 방안 .....	73
【붙임 6】 재난안전통신망 등록·연계 신청서 양식 .....	138

- 부 록 -

<b>[부록 A] 용어</b>	<b>139</b>
<b>[부록 B] 약어</b>	<b>150</b>
<b>[부록 C] 참고 문헌</b>	<b>152</b>
<b>[부록 D] 재난안전통신망 활용 장비 · 서비스 도입 사례</b>	<b>153</b>
D-1) 시스템 관리기	153
D-2) 재난안전통신망을 활용한 지하전력구 무선통신망시설	154
D-3) 소방 UHF 통신망과 재난안전통신망 통합운영시스템	155
D-4) 재난안전통신망 연계 녹취장비	156
D-5) 재난안전통신망 연동 서비스	157
D-6) 모바일오피스 서비스	158
D-7) 현장영상전송시스템 서비스	159
<b>[부록 E] 재난안전통신망법</b>	<b>160</b>
<b>[부록 F] 재난안전통신망 운영 및 사용에 관한 규정</b>	<b>170</b>
<b>[부록 G] 재난안전통신망 단말기 개통 절차</b>	<b>177</b>
G-1) 단말기 개통에 대한 담당 기관	177
G-2) 자원 관리 (참고)	178
G-3) SIM 등록 절차	178
G-4) 단말기 등록 절차	179
G-5) 단말기 개통/변경 업무 절차	179
<b>[부록 H] 재난안전통신망 앱스토어 사용자 매뉴얼</b>	<b>180</b>
H-1) 앱스토어 접속	180
H-2) 앱 등록	180
H-3) 앱 목록 조회	182
<b>[부록 I] 재난안전통신망 개발자 포털의 API</b>	<b>187</b>
I-1) APIs	187
I-2) API 문서	189
I-3) API 문서 내역 예시	194



<b>[부록 J] 재난안전통신망 IPv6 주소체계 및 도입현황 .....</b>	<b>198</b>
J-1) IPv6 개요 및 구조 .....	198
J-2) IPv6의 주소표기 및 통신방식 .....	201
J-3) ICMPv6 .....	203
J-4) IPv6 전환 기술 .....	207
J-5) IPv6 주소 체계화 .....	210
J-6) 사용기관 IPv6 주소할당 .....	215
<b>[부록 K] 재난안전통신망 포털 서비스 이용 .....</b>	<b>222</b>
K-1) 인터넷망에서 접속 시 신청서 작성 .....	222
K-2) 국가정보통신망 업무망에서 접속 시 신청서 작성 .....	224
<b>[부록 L] FirstNet의 응용서비스 목록 .....</b>	<b>225</b>
L-1) FirstNet API .....	225
L-2) FirstNet IoT .....	226
L-3) FirstNet 앱 .....	227

## 1. 개 요

### 1.1. 추진배경

- 정부는 국민이 안전한 삶을 누릴 수 있도록 재난안전관리에 경찰·소방·지자체 등 재난 관련 기관이 범부처적 협조체계가 가능하도록 PS-LTE 기술 방식의 전국 단일 재난안전통신망을 구축·운영
  - 이에 따라, 기관 간 협업을 위한 재난현장 서비스, 기관별 특화 서비스뿐만 아니라 대국민 재난안전관리 서비스 제공에 필요한 인프라 기반 마련

### 1.2. 작성 근거 및 목적

- 「재난안전통신망법」, 「재난 및 안전관리 기본법」, 「재난 및 안전관리 기본법 시행령」, 및 「재난안전통신망 운영 및 사용에 관한 규정」에 근거하여 재난안전통신망 장비·서비스 도입·개발 가이드라인 작성
  - ※ 상세 관련 근거는 【붙임1】 재난안전통신망 관련 법·제도를 참조하고, 재난안전통신망법과 재난안전통신망 운영 및 사용에 관한 규정 전문은 【부록 E】와 【부록 F】에 수록
- 본 가이드라인은 재난안전통신망 기반 장비의 도입과 공공안전 응용서비스의 개발·운영을 희망하는 사용기관, 관련 업체 등의 이해를 돕기 위하여 마련

### 1.3. 가이드라인의 주요 내용

- 재난안전통신망 구축 현황 및 응용서비스 소개
- 장비, 응용서비스 도입과 관련된 단계별 수행내용 및 절차
- 재난안전통신망 관련 법·제도 및 응용서비스 연동방안 등

### 1.4. 가이드라인의 적용 범위

- 본 가이드라인은 재난안전통신망의 기본 장비(지령장치, 단말기)와 기본서비스\* 이외의 장비와 응용서비스를 포함
  - \* 단말기나 지령장치 등에서 사용되는 통화 및 메시지 전송 기능 등 재난안전통신망에서 요구하는 37개 주요 기능 기반 서비스

## 2. 재난안전통신망 소개

### 2.1. 개요

- (배경) 경찰·소방·지자체 등 재난 관련기관이 공동으로 사용할 수 있는 PS-LTE\* 기술방식의 전국 단일 통신망을 구축

\* Public Safety – Long Term Evolution : 재난안전용 4세대 무선 통신 기술(국제표준)로서 한국뿐만 아니라 미국, 영국 및 EU 등에서도 구축·운영 중임

※ 재난안전통신망 관련 표준은 【붙임2】 참조

- (목적) 재난안전통신망 구축을 통한 통합적 재난관리체계 기반 마련 및 현장 즉시 대응 역량 강화
- (기능) 사용기관들이 재난 상황 시 동시·다중으로 상황전파, 실시간 동원자원 활용, 초동대응, 일제지령, 통합지휘, 자원의 탄력적 배치 등 입체적인 재난 대응에 필요한 상호통신을 효율적으로 지원하는 환경 제공

[그림 1] 재난안전통신망 개념도



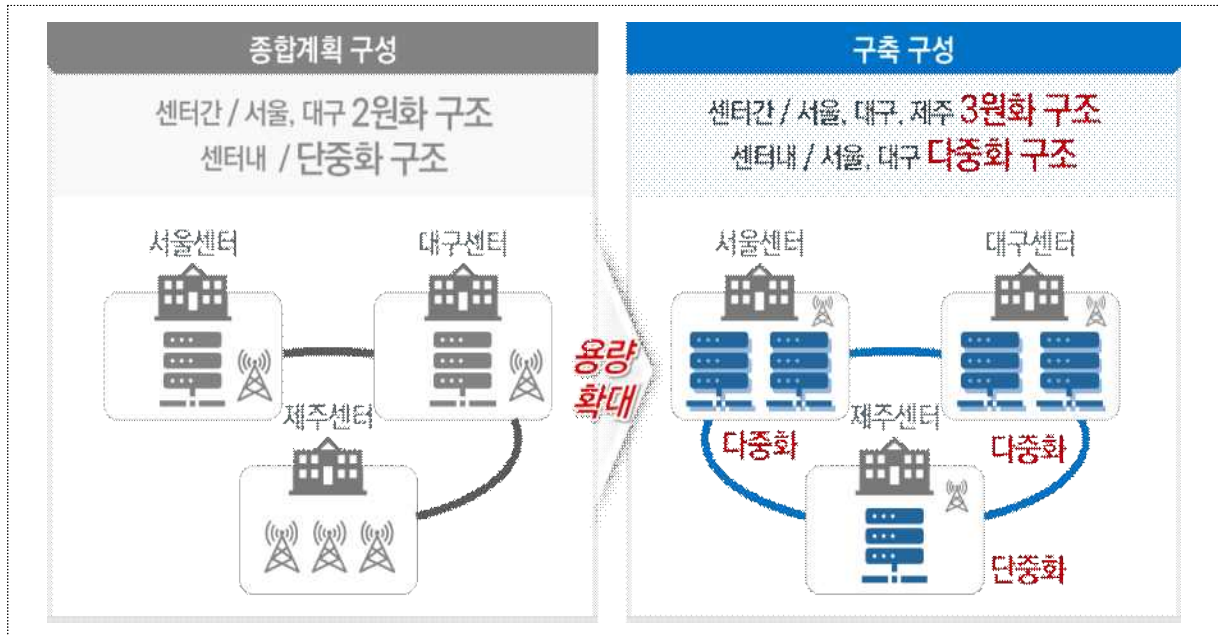
## 2.2. 재난안전통신망 구축 현황

### 2.2.1. 재난안전통신망 시스템

재난안전통신망 시스템은 일반 이동통신 시스템과 동일하게 △이동통신교환국(주제어시스템), △기지국, △이동국(단말장비)으로 구성

- (주제어 시스템) 재난안전통신망의 주제어 시스템은 서울, 대구, 제주센터에 구축되어 있으며 재난안전통신망의 안정성과 생존성을 높이기 위해 센터 간 다원화 및 다중화하여 구축

[그림 2] 재난안전통신망 시스템 구성 체계



- 주요 설비를 이중화로 구축하여 장애 시 서비스가 단절되지 않도록 상호 백업체계로 구성되어 있으며, 약 40만 대의 재난안전통신망 단말기 수용 가능
  - ※ 전송로의 주요 통신국사(집중노드) 이원화 및 전송망(전용회선) 이중화
  - ※ 주제어장비(EPC) 5식의 다중화(Active-Active) 및 EPC 내 이중화 (Active- Standby)

[표 2] 단말기 수용용량

분류	단말기 수용 라이선스		해당 단말기 종류
	사용 단말기 수	확장 가능 최대 용량	
PS-LTE	24만 대	40만 대	PS-LTE 단말기 PS-LTE 지령장치

## 1) 주제어 설비

- 주제어 설비는 재난안전통신망 필수기능인 통화서비스를 안정적으로 제공하기 위한 핵심 설비
- (코어망 설비) 3GPP Re.13 기반 eMBMS, MCPTT 기능의 원활한 제공을 위해 필요한 EPC, IMS 등의 장비로 구성
- (운영관리 설비) MDM, NMS 등 단말·망·보안을 관리하기 위한 장비로 구성
- (응용 설비) 앱스토어, 포털, 외부연계 게이트웨이 등 부가 서비스와 통합 플랫폼을 지원하기 위한 장비로 구성

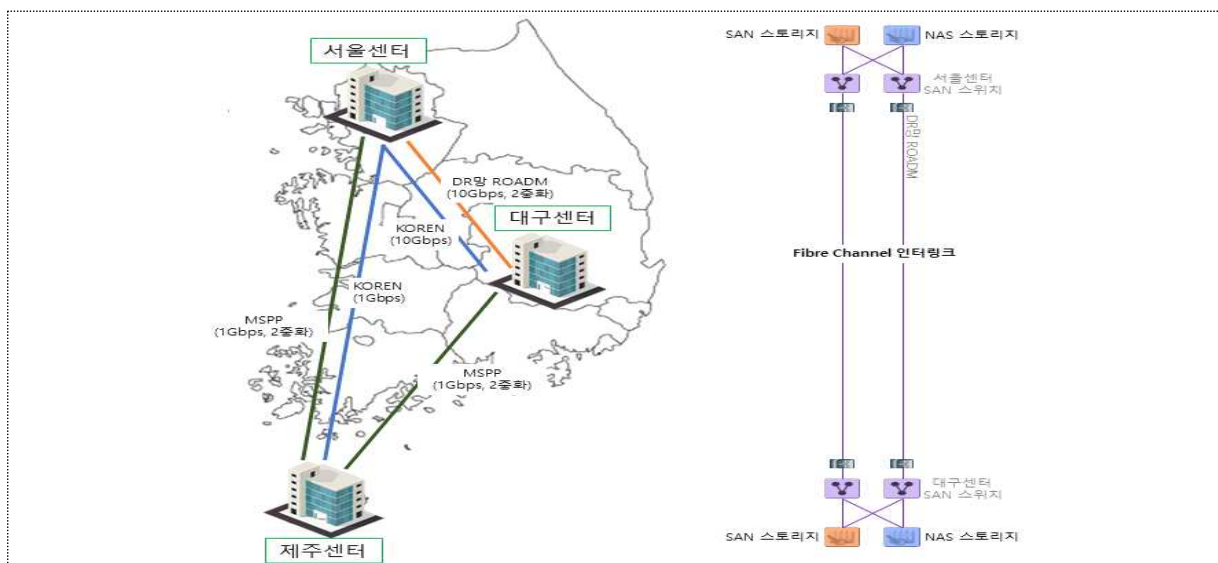
[그림 3] 재난안전통신망 주제어 설비의 기능적 구조(개략도)



## 2) 전송망

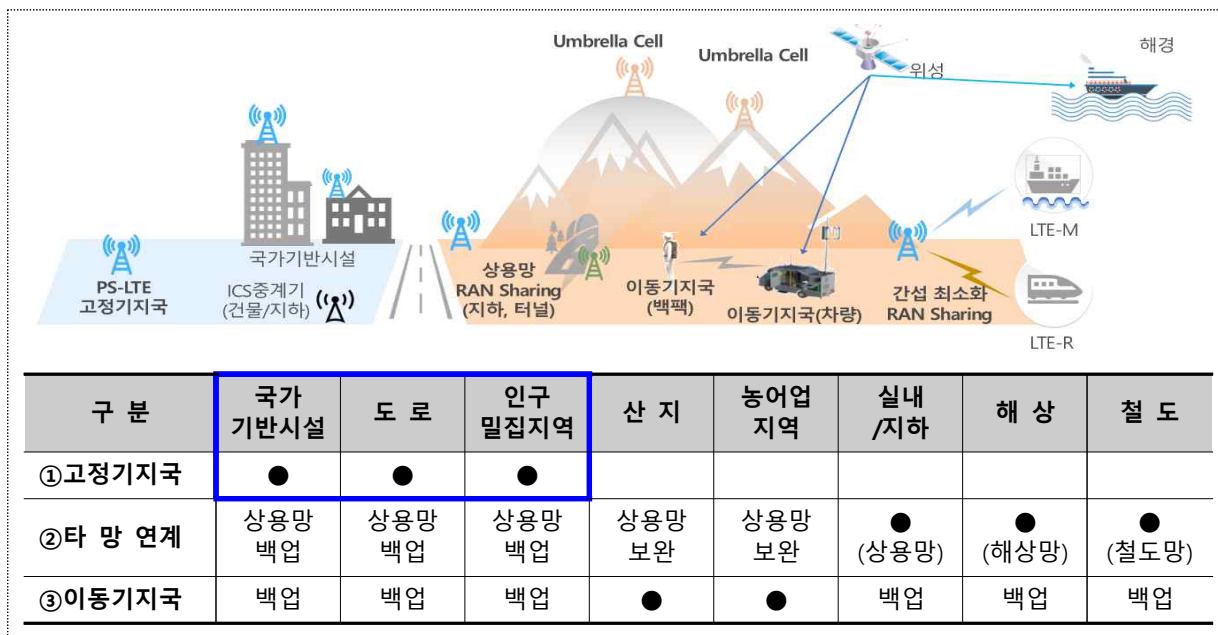
- 통신사업자의 전송망 시스템을 임차하되 재난안전통신망의 신뢰성 및 가용성 확보를 위해 충분한 전송 용량 확보

[그림 4] 운영센터 간 연결 전송망 구조



- (기지국 시스템) 재난안전통신망의 목적과 경제성을 고려하여 고정기지국, 타 통신망 연계, 이동기지국 등을 종합적으로 활용하여 전국적인 재난통신 서비스 제공
  - (고정기지국) 중부권 4,370개소('19.9), 남부권 8,147개소('20.9) 및 수도권 5,048개소('21.3) 등 총 17,565개소
  - (타 통신망 연계) 700MHz 대역의 동일 주파수를 사용하는 해상망(LTE-M), 철도망(LTE-R)과 연계하여 효율적인 망 구축 및 상용망 백업(KT, SKT) 체계 구축
  - ※ 전파 강도에 따라 재난안전통신망 > 해상망/철도망 > 상용망 순서로 기지국을 공유하며, 재난안전통신망 전파가 약한 해상은 해상망이, 공공망의 모든 전파가 약한 지역은 상용망이 신호 처리
  - (이동기지국) 통화용량 확장, 통신장애 등에 대비하여 이동기지국 배치·운영\*
    - ※ (차량형 20대) 전국 어디서나 3시간 이내 통신 서비스 제공을 위해 주요 지역에 분산 배치 (휴대형 42대) 119화학센터(7), 119특수구조대(4), 시도소방본부(19) 등 현장대응기관 배치

[그림 5] 재난안전통신망 기지국 구성



- (단말장비) 평시·재난시 경찰, 소방, 해경 등 재난관련 기관들이 재난안전통신망 서비스(그룹통화 등)를 이용하기 위한 상용 장비
  - (단말기) 재난안전통신망 서비스(개별통화, 그룹통화, 메시지 등)를 사용할 수 있는 장비로서 사용기관별 수요 및 사용 목적에 따라 다양한 유형\*의 단말기를 자체 구매하여 사용

\* <단말기 유형> 휴대형(스마트폰형, 무전기형, 복합형), 차량형, 고정형, 기타

※ 단말기 구매는 재난안전통신망 종합지원시스템(<https://www.safenet.go.kr>)의 단말기 구매 규격을 참조

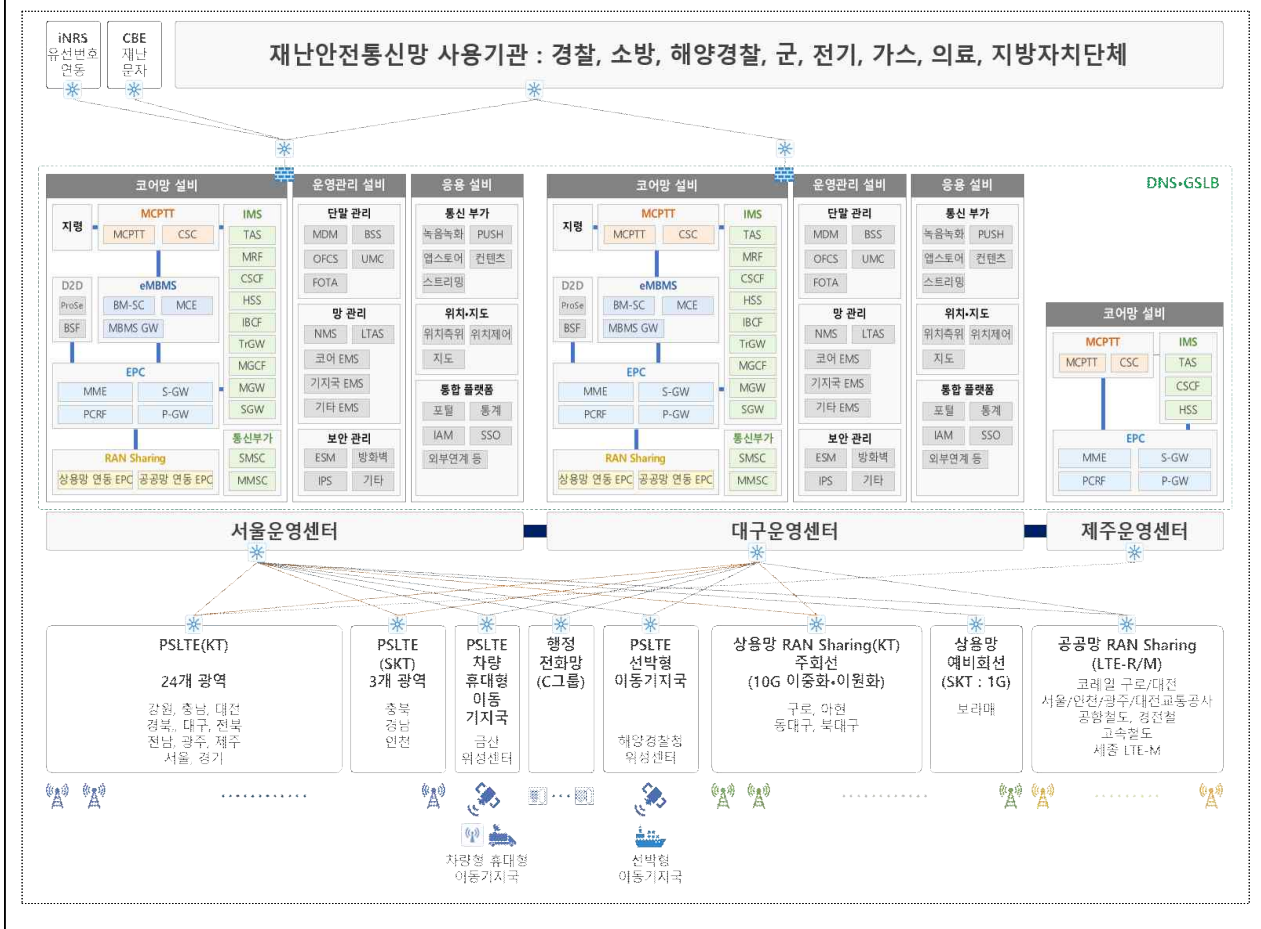
- (지령장치) 사용기관 상황실에서 주로 사용하는 장비로 재난안전통신망 단말의 통화그룹별 사용자를 관리하고, 음성·영상 그룹통화, 메시지 등을 통해 지령하는 용도로 사용기관의 수요 및 사용 목적에 따라 지령장치를 자체 구매하여 사용

\* <지령장치 유형> 고정형, 거치·분리형, 기타

### 재난안전통신망 시스템 아키텍처

- (운영 센터) 서울, 대구, 제주센터 간 전송망을 다중으로 구축하여 특정 센터에 장애가 발생하더라도 다른 센터에서 해당 센터까지 운영할 수 있도록 구성
- (주제어 설비) 코어망 설비, 운영관리 설비, 응용 설비로 구성되어 재난안전통신망 필수 기능을 제공
- (기지국 및 타 망 연계 설비) 고정기지국(국가기반시설(점), 주요도로(선), 인구밀집 지역(면))과 휴대형 이동기지국(산간·농어촌 지역)을 통해 통신을 지원하고, 음영 지역(건물 내부, 지하, 해안 등)에서는 상용망 및 타 통합공공망(해상망, 철도망)과의 통신망 연동기술(RAN-Sharing)을 활용하여 통신을 지원

[그림 6] 재난안전통신망 시스템 아키텍처 (전체)





재난안전통신망 시스템 아키텍처(계속)

약어	Full Name	설명
MCPTT	Mission Critical Push To Talk	안전망 음성/영상 그룹/개별 통화 서비스
CSC	Common Service Core	MCPTT 그룹, 가입자, 서비스 정보 관리 및 제공
ProSe	Proximity Service	Off Network 상황에서 단말 간 직접통신을 위한 정보 관리 및 제공
BSF	Bootstrapping Server Function	단말과 ProSe Function 서버 간 인증 기능 제공 및 암호화 키 교환 기능 제공
MBMS-GW	Multimedia Broadcast/Multicast Service Gateway	MBMS 베어러 컨텍스트 정보관리 및 PTT 미디어 전달 기능
BM-SC	Broadcast Multicast Service Center	MBMS Session 관리기능
MCE	Multi cell Coordination Entity	MBMS Session 관리 및 기지국 무선 자원 할당 기능
MME	Mobility Management Equipment	단말의 Mobility Management 및 Session 관리
S-GW	Serving Gateway	EPS 베어러, Packet 관리
P-GW	Packet Data Network Gateway	IP 라우팅, 패킷 필터링, IP 주소할당 기능
SAE GW	System Architecture Evolution Gateway	S-GW, P-GW 통합형 장비
PCRF	Policy and Charging & Enforcement Function	QoS 정책제어 기능
TAS	Telephony Application Server	음성/영상 호 부가서비스 제공
MRFC	Multimedia Resource Function Controller	멀티미디어 변환 및 Transcoding 서비스 제공
CSCF	Call Session Control Function	SIP 기반 멀티서비스를 위한 SIP 호처리 기능
HSS	Home Subscriber Server	LTE/IMS/MCPTT 가입자 정보(위치정보, 인증정보, 서비스 정보) 관리 및 제공
IBCF	Interconnection Border Control Function	IMS 망간 연동을 위한 보안 및 NAT Traversal 기능 제공
TrGW	Transition Gateway	IMS 코어망 간의 미디어 컨트롤, IPv4와 IPv6 주소변환 등의 기능을 수행하는 장비
MGCF	Media Gateway Control Function	MGW(Media Gateway)를 제어하는 장치
MGW	Media Gateway	회선 교환망과 패킷 교환망 사이에 매체의 처리 및 변환을 수행하는 장치
SMSC	Short Message Service Center	단말기로 문자, 숫자 메시지를 송수신하는 서비스를 위한 서버
MMSC	Multimedia Message Service Center	멀티미디어 메시지 송수신 기능 및 E-Mail 송수신 서비스를 위한 서버
MDM	Mobile Device Management	원격에서 단말기의 잠금, 데이터 삭제 등을 지원
BSS	Billing Support System	재난안전통신망 단말기별 이용통계 정보를 기반으로 이용료를 산정
OFCS	Offline Charging System	망을 이용한 후 자원 사용량을 기반으로 이용료를 산정하는 Offline 과금
UMC	USIM Management Center	USIM의 정보들을 관리하여, USIM의 인증, 관리 및 개통 기능을 제공
FOTA	Firmware Over The Air	단말기 하드웨어를 제어하는 펌웨어의 설치/실행에 대한 통제
NMS	Network Management System	주제어/기지국/네트워크/전원 시설 상태 및 장애 감시 서비스
LTAS	LTE Traffic Analysis System	LTE 트래픽 및 시그널 분석 기능을 제공
ESM	Enterprise Security Management	보안장비의 통합관제를 통한 효율적 관리 서비스
방화벽	-	미리 정의된 규칙에 기반하여 트래픽을 모니터링하고 제어하는 보안 시스템
IPS	Intrusion Prevention System	악성 트래픽을 식별하고 네트워크에 유입되는 것을 차단하는 보안 시스템
녹음녹화	-	음성, 영상, 문자 등의 데이터에 대한 녹취, 파일 다운로드 및 재생을 하는 시스템
PUSH	-	사용자 단말기로 메시지를 보내는 데 사용되는 서버
앱스토어	-	재난안전통신망에서 사용되는 앱을 등록, 배포, 관리
컨텐츠	-	MCPTT 단말 및 서버와 연동하여 MCPTT의 컨텐츠 파일 전송 기능을 제공
스트리밍	-	재난현장의 영상을 촬영하여 전송하고, 실시간으로 영상을 모니터링하는 서비스
위치추위	-	통합 위치제어 및 대용량 위치이력 정보를 관리할 수 있는 시스템
포털	-	업무지원 및 커뮤니케이션 수단으로 각 시스템을 유기적으로 연결하는 시스템
통계	-	응용시스템에서 생성된 집계 정보를 다차원 분석하는 통계보고서 서비스
IAM	Identity and Access Management	업무시스템 및 인프라 시스템의 계정 및 권한을 관리하는 시스템
SSO	Single Sign On	로그인 후 다른 시스템 접속 시 별도의 인증없이 자동 로그인 기능을 제공
외부연계	-	각 응용 시스템에서 개발/제공하는 API를 Open API Gateway를 통해 외부에 공개



## 2.2.2. 재난안전통신망 주요 기능

### 2.2.2.1. 재난안전통신망 주요 기능

- 재난안전통신망은 통신망의 생존·신뢰성, 재난 대응성, 보안성, 운영·효율성, 상호운용성 측면에서 37개의 주요 요구기능을 정의하고 있으며, 주제어시스템, 기지국 및 단말기에서 제공하는 기능은 아래 [표 3]과 같음

[표 3] 재난안전통신망 장비별 주요 기능

요구기능	주요 기능	주제어	기지국	단말기
직접통화/단말중계	ProSE, eProSE, UE to Network relay (추후 적용 예정)	○	○	○
단말 이동성	Tracking Area Update, Service Request, S1 Release, Paging, S1/X2 Handover, Event Report 등	○	○	○
호 폭주 대처	Threshold Crossing Alert, Inbound/Outbound Event Throttling, PDN GW Control of Overload, AC Barring 등	○	○	○
단독기지국 운용 모드	이동기지국	○	○	
통화품질	EMC, Radio Resource Management, CIR/EIR 기술 등 그룹통신을 위한 Mission Critical QCI	○	○	○
백업/복원	스토리지 미러링, 데이터 복제	○		
개별통화	3GPP IMS, TTAK.KO-06.0338/R2 등	○		○
그룹통화	3GPP IMS/GCSE, eMBMS 등	○	○	○
지역선택호출	GIS, GEO Fencing	○	○	
통화그룹편성	3GPP 릴리스 13 MCPTT	○		
가로채기	3GPP 릴리스 13 MCPTT	○		○
비상통화	3GPP 릴리스 13 MCPTT	○		○
단말기 위치확인	S-GPS, GLONASS, Location information	○	○	○
영상통화	3GPP IMS/GCSE	○		○
주변음 청취	TTAK.KO-06.0496 재난안전통신망 단말기 기술규격	○		○
복수통화 그룹수신	3GPP 릴리스 13 MCPTT	○		○
개방형/표준준수	3GPP, 인증기관 등 표준 연동 규격 적용	○	○	○
호 연결	MCPTT KPI1, KPI2, KPI3	○	○	○
망 연동	LTE Roaming, PSTN/PLMN Interworking, 전용회선	○		○
단말기 사용허가/금지	EIR Interworking/ HSS Provisioning, Identity Management	○		○
암호화	Platform Key Signing, AS Security, NAS Security, TLS, sRIP, SSL, WS-Security 등	○	○	○
인증	EPS-AKA, IMS AKA, SIP Digest, 2 Factor, DB 및 서비스 접근제어시스템 인증 등	○		○
보안규격	CC인증, 국정원 보안적합성 인증, 인증기관 보안인증 등	○	○	○
통합보안관제	ESM(통합보안관제시스템), SSH	○		○
상황전파 메시지	재난문자	○	○	○
가입자 용량 확보	Call Model	○		○
다자간 전이중통화	3-Way Conference	○		○
데이터통신	PDN Connection, PCC Rule Processing, Bearer Activation/ Deactivation/ Modification	○	○	○
통화내용 녹음녹화	녹음/녹화	○		○
발신번호 표시	MMTEL(OIP)	○		○
원격 망 관리	MDM, EIR Interworking, HSS Provisioning	○		○
망관리 시스템	NMS, EMS	○	○	
보고서 생성	NMS, EMS	○	○	

## 2.2.2.2. QCI (QoS Class Identifier)

- QCI란 서비스의 우선순위, 정보 전송 성능 등을 정의한 것으로 3GPP 23.203에서 정의한 표준 QCI를 재난안전통신망에서도 동일하게 적용

[표 4] 표준 QCI 특성 (출처: 3GPP 23.203)

QCI	리소스 형태	우선순위	패킷지연 규격	패킷 오류율	서비스 예
1	GBR	2	100ms	$10^{-2}$	대화 음성
2		4	150ms	$10^{-3}$	대화 영상 (라이브 스트리밍)
4		5	300ms	$10^{-6}$	비대화 영상 (버퍼 된 스트리밍)
65		0.7	75ms	$10^{-2}$	미션크리티컬 사용자 평면 PTT 음성 (즉, MCPTT)
66		2	100ms	$10^{-2}$	논 미션크리티컬 PTT 음성
67		1.5	100ms	$10^{-3}$	미션크리티컬 비디오 사용자 평면
5		1	100ms	$10^{-6}$	IMS 신호
6	Non-GBR	6	300ms	$10^{-6}$	영상 (버퍼 된 스트리밍) TCP 기반 (즉, www, e-mail, chat, ftp, p2p 파일 공유, 프로그레시브 영상, 등)
7		7	100ms	$10^{-3}$	음성, 영상 (라이브 스트리밍)
8		8	300ms	$10^{-6}$	영상 (버퍼 된 스트리밍) TCP 기반 (즉, www, e-mail, chat, ftp, p2p 파일 공유, 프로그레시브 영상, 등)
9		9			
69		0.5	60ms	$10^{-6}$	미션크리티컬 지연 민감 신호(시그널링) (즉, MCPTT 신호, MC Video 신호)
70		5.5	200ms	$10^{-6}$	미션크리티컬 데이터 (즉, QCI 6/8/9와 같은 예의 서비스들)

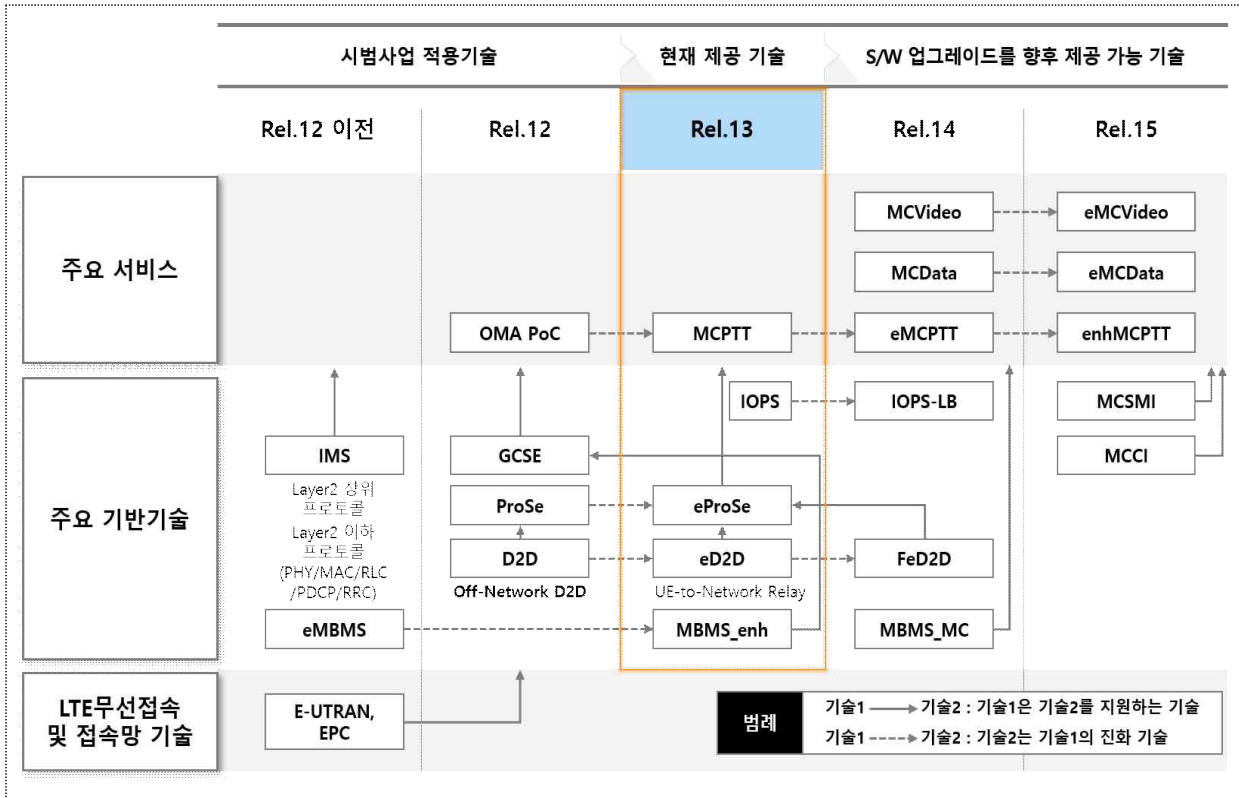
※ 주) MCVideo를 위한 QCI 67과 69는 3GPP 릴리스 15에서 추가된 기능

- 사용자 간 통화의 양과 데이터 전송량이 증가하여 재난안전통신망에서 모든 서비스를 처리하기 어려운 경우 우선순위가 높은 MCPTT 등 음성통화 서비스를 우선 처리

### 2.2.3. 재난안전통신망 제공 기술

- 재난안전통신망은 현재 3GPP Rel.13을 기반으로 구축되었으며, 향후 SW 업그레이드를 통해 MCS(Mission-Critical Service) 등 Rel.14, Rel.15의 주요 서비스 제공 예정

[그림 7] 재난안전통신망 제공 기술



#### 2.2.3.1. 현재 제공 가능 통신기술

- (R13 PS-LTE) 3GPP에서 제정한 재난안전 통신에 필요한 기능들을 표준화한 릴리스13 기반의 이동 통신기술
- (구성) 우리나라의 재난안전통신망은 면허 대역의 주파수(718~728/773~783MHz)를 사용하여 UL(Up Link), DL(Down Link) 각각 10MHz의 대역폭으로 구성

[그림 8] 국내 통합공공망 주파수 할당 현황



- (용량) 대역폭 10MHz에 의해 셀 용량\*이 결정되며, 각각의 단말이 사용하는 트래픽에 따라 기지국에서의 수용 용량을 결정
- \* 셀 용량이 75Mbps인 PS-LTE에서 이론상 SD급(1Mbps) 동영상을 동시에 75명이 사용 가능. 75명 초과 사용 때 무선 트래픽 양이 증가하여 서비스 품질 저하 발생
- ※ 일반적인 환경에서 PS-LTE는 약 300 devices/cell 수용 가능
- (커버리지) 개활지 지역은 35km 이내이며 도심지역은 0.5km~1km 이내
- (특징) ISM 밴드 (Industrial Scientific Medical Band) 대비 전파간섭의 영향이 적고, 파장이 길어 외부환경에 상대적으로 영향을 덜 받는 통신기술

### 2.2.3.2. 향후 제공 가능 통신기술

- (R14 PS-LTE) 3GPP 릴리스 14 이상으로 업그레이드하여 릴리스 13 대비 개선된 기능을 지원
  - 미션 크리티컬 서비스는 자동차 안전, 산업제어, 항공 관제, 드론 운행, 의료 서비스 등 고신뢰성, 초지연, 고가용성이 필요한 분야에서 활용되는 서비스로서 미션크리티컬 지원 데이터(MCData) 및 미션크리티컬 지원 비디오(MCVideo) 등이 릴리스 14에서 지원되는 대표적인 미션 크리티컬 서비스임
  - 공통의 그룹관리(Group Management), 형상관리(Configuration Management), 위치 관리(Location Management), 계정관리(Identity Management), 보안키 관리(Key Management) 지원
  - 범용 구현의 직접통화/단말중계 지원 (V2X와 통합하여 지원될 예정)

[표 5] 향후 제공 가능 통신기술

요구기능	주요 기능	비고
MCData	미션크리티컬 지원의 데이터	R14 이후 업그레이드 필요
MCVideo	미션크리티컬 지원의 비디오	R14 이후 업그레이드 필요
상황 전파 메시지	MCData Signaling Control	R14 이후 업그레이드 필요
공통 Management	공통 Group, Configuration, Identity, Key Management	R14 이후 업그레이드 필요
직접통화/단말중계	ProSE, eProSE, UE to Network relay	C-V2X와 함께 범용 구현 적용 필요
eMBB	Enhanced Mobile Broadband	5G 업그레이드와 NR 구축 필요
URLLC	Ultra-reliable Low Latency Communication	5G 업그레이드와 NR 구축 필요

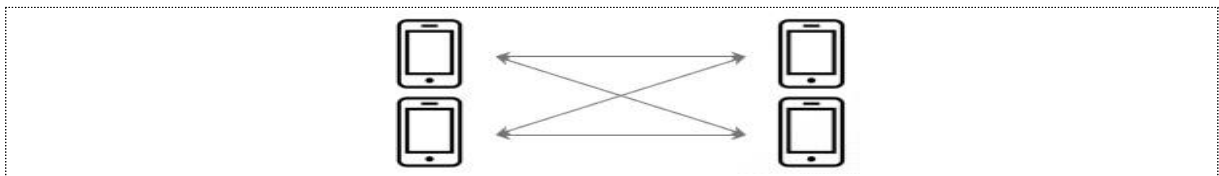
## 2.2.4. 재난안전통신망 기본서비스

- 단말기 및 지령장치 등에서 기본적으로 사용할 수 있는 음성·영상 개별 및 그룹 통화와 문자 메시지 전송 등 기본서비스로 아래와 같음

### 2.2.4.1. 그룹통화/통신 (MCPTT)

- 그룹통화/통신은 기지국 여부와 상관없이, 동일한 통화 그룹에 속해 있는 단말기 상호 간 1대 다수로 통화/통신하는 기능을 제공
- MCPTT(Mission Critical Push To Talk)\*에 의한 그룹(1:N) 간의 음성통화, 영상통화 및 데이터 서비스가 단말기를 통하여 기본적으로 제공
  - \* MCPTT는 재난안전통신을 위하여 특화된 무전기의 기본 통화방식의 푸시투토크(Push to Talk) 서비스로서, 3GPP 릴리스 13에서 표준화됨
- QCI 65/69에 의하여 호 폭주 상황에서도 높은 우선순위에 따라 신속한 호접속과 통화 품질 유지가 가능하며 지역 선택 호출, 통화그룹 편성, 가로채기, 비상통화, 주변음 청취, 발신번호(ID) 표시, 통화 중 데이터 통신 등을 지원

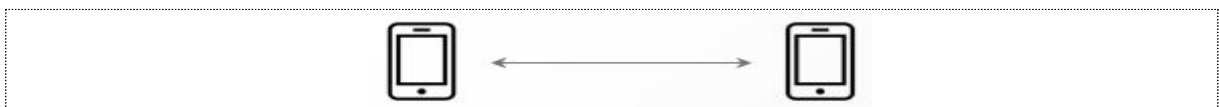
[그림 9] 그룹통화/통신 개념도



### 2.2.4.2. 개별통화/통신 (VoLTE)

- 단말기 또는 시스템 관리자가 임의의 단말 또는 시스템과 식별번호(ID 또는 전화번호)를 선택하여 개별통화/통신하는 기능을 제공
- VoLTE(Voice over LTE)에 의한 개별(1:1) 간의 음성통화, 영상통화 및 데이터 서비스가 단말기를 통하여 기본적으로 제공
- 다자간 전이중 음성통화, 다자간 전이중 영상통화 및 공중망과의 연계 통신이 가능

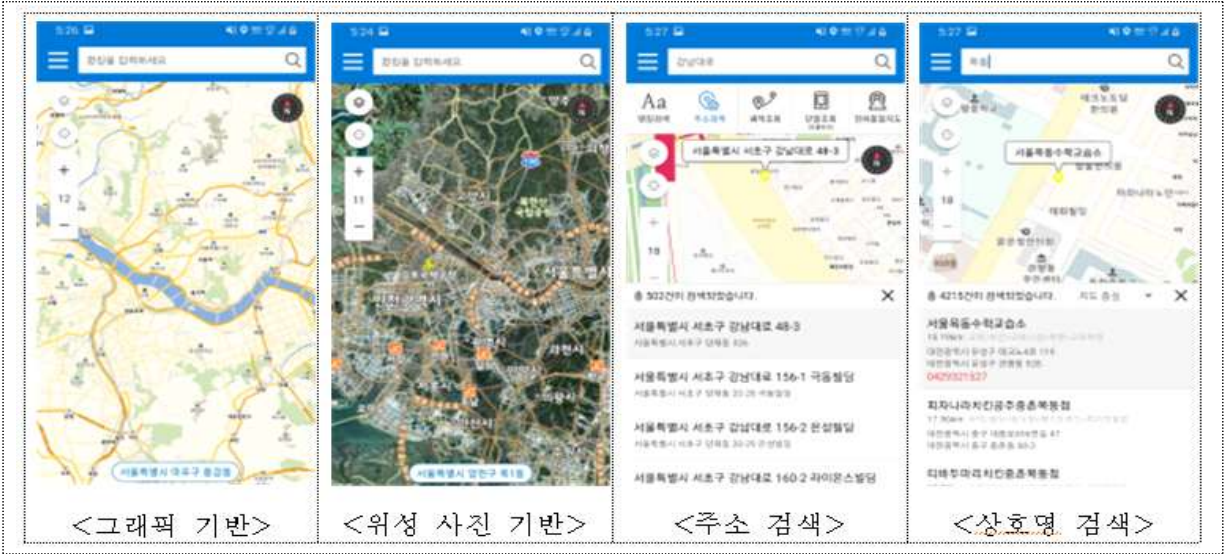
[그림 10] 개별통화/통신 개념도



2.2.4.3. 위치 검색 서비스

- 전자지도와 위성사진을 기반으로 도로명, 지번 및 상호를 이용하여 위치를 검색할 수 있는 기능
- 재난안전통신망에서 기본서비스로 제공할 수 있는 지도 검색 서비스에 대한 예시와 기능은 아래 [그림 11]과 [표 6] 참조

[그림 11] 지도 검색 서비스 예시



[표 6] 지도 검색 기능 및 사용장치

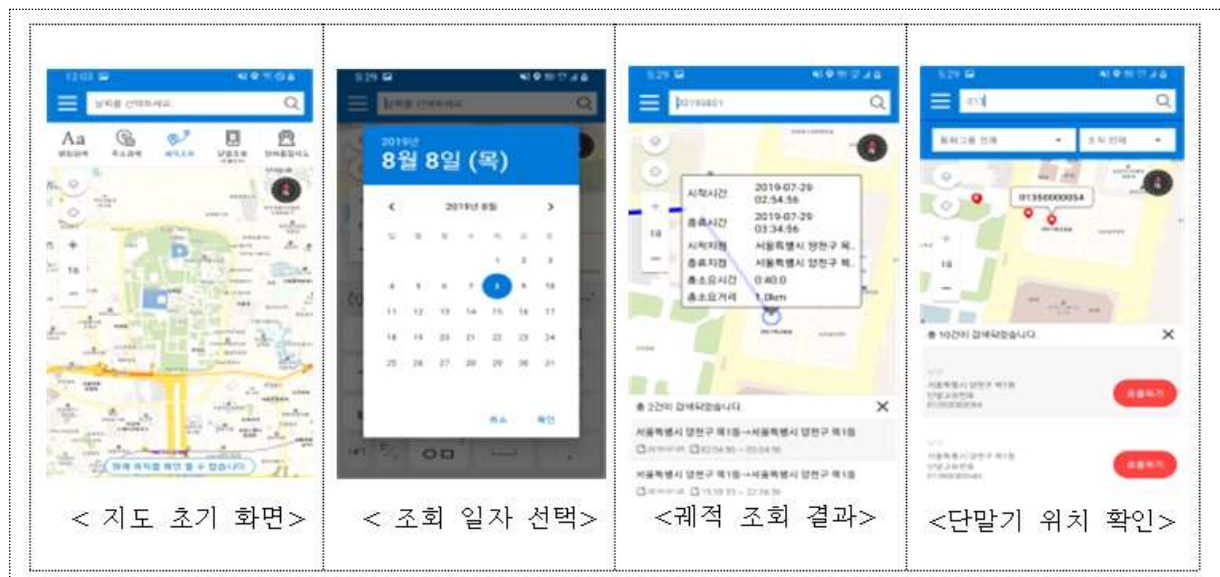
기능명	설명	사용장치
도로명 주소 검색	• 도로명 주소를 기반으로 지도 검색	단말기 지령장치
지번 주소 검색	• 지번 주소를 기반으로 지도 검색	
상호 검색	• 상호를 기반으로 지도 검색	



## 2.2.4.4. 궤적 조회

- 단말기나 지령장치의 GPS 기능을 활용하여 특정 장비가 어느 시점에 어떤 지점에 있었는지를 조회할 수 있는 기능을 제공
- 재난안전통신망에서 기본 서비스로 제공 가능한 궤적 조회 서비스에 대하여 예시와 기능은 아래 [그림 12]와 [표 7] 참조

[그림 12] 궤적 조회 서비스 예시



[표 7] 궤적 조회 기능 및 사용장치

기능명	설명	사용장치
최근 궤적	• 조회를 요청한 현재 일자를 기준으로 일주일 치의 궤적을 자동으로 조회	단말기 지령장치
특정 기간 궤적	• 특정 기간이나 일자를 기준으로 궤적을 조회	
단말기 위치 조회	• 조회하고자 하는 단말기의 전화번호(개별)를 입력하거나 조직을 선택하여 위치를 확인 • 검색된 단말기를 대상으로 개별통화 혹은 메시지 전송 가능	지령장치

## 2.2.4.5. 웹 포털

- 재난안전통신망에서 제공하는 웹 포털 서비스는 웹 기반의 서비스를 활용 및 다양한 검색 기능을 제공
  - (고객지원) 개통/자원신청, 부가서비스 신청, 서비스 요청, 통화앱 관리, 센터 방문예약 및 모바일 도움말 등록 등 업무에 필요한 서비스 제공
  - (소식, 안내) 공지사항, 안전일정, 사용량조회, 알림 발송 관리 등 전달되는 다양한 소식 및 안내 서비스 제공
  - (참여센터) 제안하기, 설문조사, 온라인 상담 등 다양한 참여 기능 제공
  - (정보조회) 자료실, 이용안내, 자주하는 질문, 긴급전화번호 안내 등 정보성 서비스 제공

[그림 13] 웹 포털 서비스 화면



[표 8] 웹 포털 기능 및 사용장치

기능명	설명	사용장치
웹 기반 서비스 접근	• 사용자의 웹 기반 서비스를 사용하기 위한 플랫폼	단말기 지령장치 PC
검색 기능	• 사용자가 웹 기반 서비스 및 콘텐츠를 검색	



## 2.2.4.6. 웹 기반 PUSH/MMS

- 재난안전통신망 단말기를 휴대하고 있는 현장의 사용자 등에게 PUSH\* 또는 MMS 메시지 형태로 일괄적으로 알림 사항을 전송할 수 있는 기능 제공

\* PUSH 기능은 단말기에 설치된 앱 간 이벤트를 전달하여 메시지를 팝업창으로 표시하는 기능을 제공

[그림 14] PUSH 서비스 구성도 및 웹 기반 PUSH/MMS 서비스 예



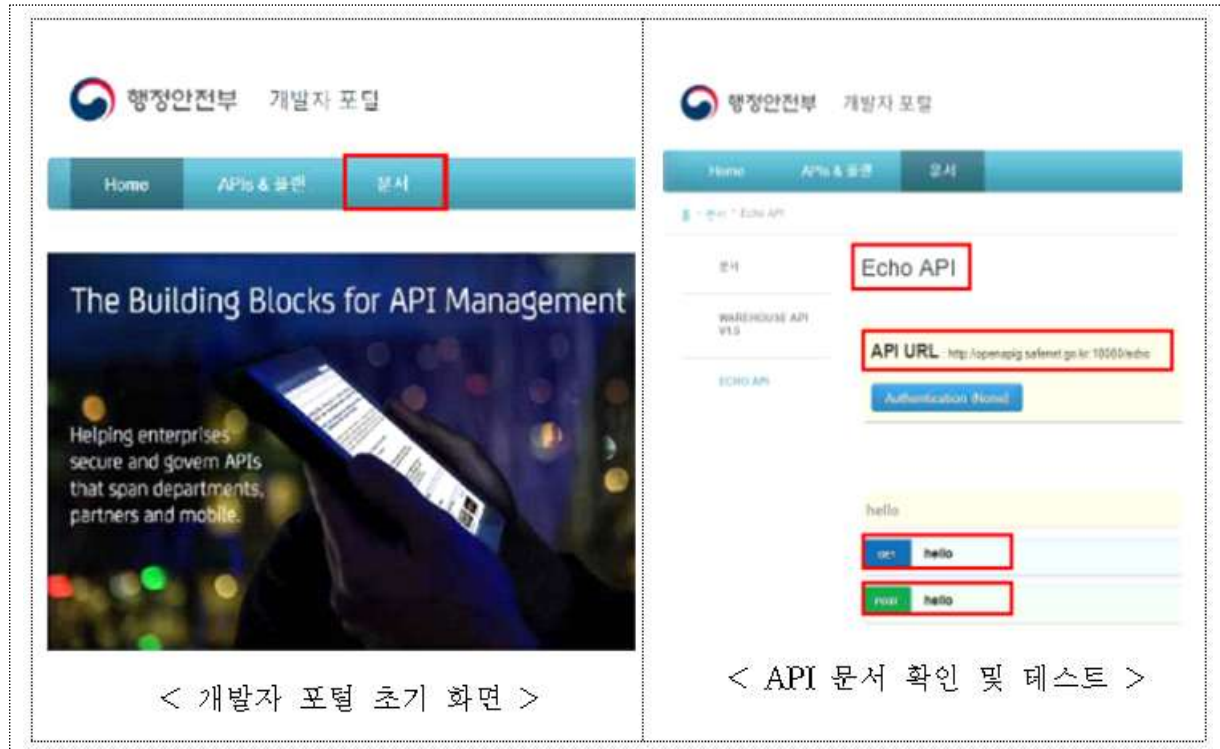
[표 9] 웹 기반 PUSH/MMS 기능 및 사용장치

기능명	설명	사용장치
웹 기반 PUSH	• 웹 기반 환경에서 공지 등 알림 사항을 PUSH 메시지 형태로 전송	지령장치 PC
웹 기반 MMS	• 웹 기반 환경에서 공지 등 알림 사항을 MMS 메시지 형태로 전송	

## 2.2.4.7. 개발자 포털(Open API)

- 재난안전통신망 개발자 포털은 재난안전통신망 서비스 개발에 필요한 API 문서와 API 호출 테스트 서비스를 제공

[그림 15] 개발자 포털 화면 예



[표 10] 개발자 포털 기능 및 사용장치

기능명	설명	사용장치
API 문서 확인	<ul style="list-style-type: none"> <li>재난안전통신망 서비스 개발 및 연계에 필요한 API 호출 정보, 명칭 또는 리소스명, 호출 방식, 호출 파라미터 등 확인</li> </ul>	단말기 PC
API 호출 테스트	<ul style="list-style-type: none"> <li>API 파라미터를 실제 입력하여 API 호출 테스트를 실행하고 응답 결과를 확인</li> </ul>	

- 재난안전통신망 개발자 포털에 등록되어 있는 API 리스트는 아래 [표 11] 참조  
 ※ 상세한 내용은 [부록 I]를 참고

[표 11] 재난안전통신망 개발자 포털의 API 목록

분류	API
BSS (단말기 개통)	단말기 사용량 조회, 통화그룹 목록 조회
CMD (지령)	통화그룹 단말 목록 조회, 통화그룹 생성, 통화그룹 사용자 추가, 재난발생 등록, 재난종결 설정, 재난변경 설정, 통화그룹 사용자 삭제, 통화그룹 정보 변경, 통화그룹 삭제
GIS (지도)	단말기 목록 및 위치정보, 기지국 목록 및 위치정보, 단말기 위치 표시(WMS), 단말기 위치 표시(WFS), 기지국 위치 표시(WMS), 기지국 위치 표시(WFS), 동적통화그룹 영역 표시 (WMS), 동적통화그룹 영역 표시 (WFS), 배경지도 서비스, POI 검색, 주소 검색
ISM (운영서비스관리)	나의 CSR 목록 수신, 나의 CSR 상세 수신
LPS (위치측위)	단말위치 조회, 위치반경 조회, 단말궤적 조회, 통화그룹 생성 개별승인 요청
POT (포털)	통화그룹 생성 개별승인 요청, 통화그룹 생성 일괄승인 요청, 승인상태 확인 요청
PSH (푸시전송)	휴대용 단말기에 Push 전송 요청
REC (녹음녹화)	음성 목록 조회, 영상 목록 조회, 문자 전송내역 조회

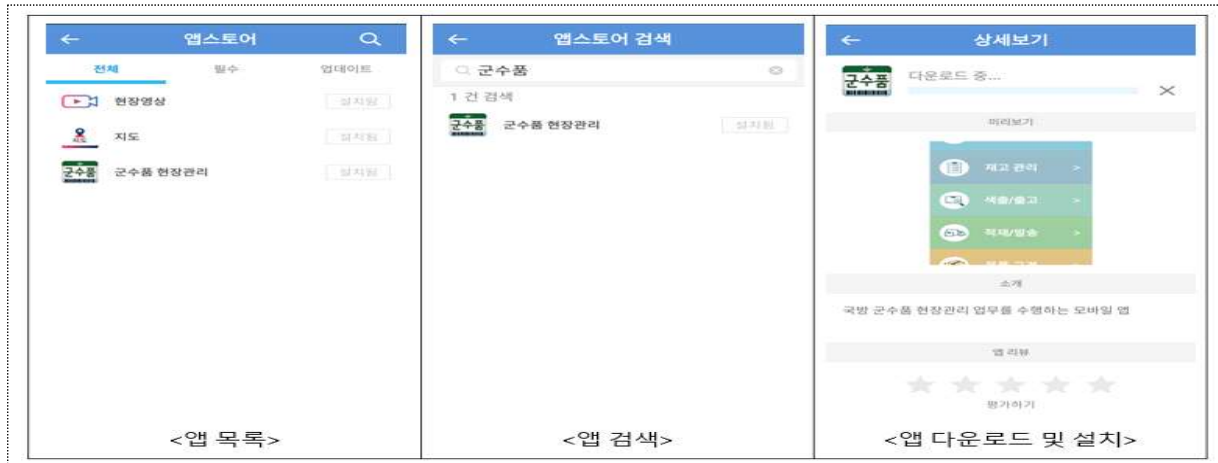
## 참고사항

- ◇ 개발자 포털 이용이 필요한 경우에는 행정안전부 재난안전통신망과와 사전협의 필요

## 2.2.4.8. 앱스토어

- (앱 검색 및 설치) 재난안전통신망 앱스토어에서 제공하는 앱 목록, 검색 및 다운로드/설치가 가능

[그림 16] 앱스토어 목록 화면 예

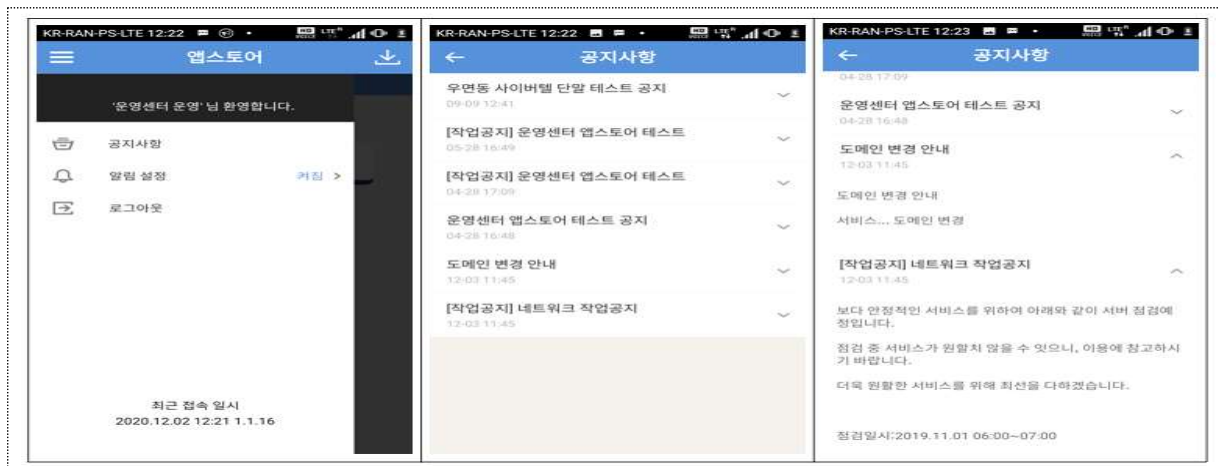


[표 12] 앱스토어 목록 기능 및 사용 장치

기능명	설명	사용장치
앱 목록	• 재난안전통신망에서 이용이 가능한 앱 목록을 확인	단말기
앱 검색	• 사용자가 원하는 앱을 검색	
앱 다운로드 및 설치	• 사용자가 하는 앱을 다운로드 받아 단말기에 설치	

- (앱 스토어 공지사항 및 알림 설정) 재난안전통신망의 앱스토어에서 제공하는 공지사항 및 알림 설정이 가능

[그림 17] 앱스토어 공지사항 설정 화면



[표 13] 앱스토어 공지사항 기능 및 사용장치

기능명	설명	사용장치
공지사항	• 앱 서비스 업데이트 및 장애 등 공지	단말기 지령장치 PC
알림 설정	• 공지사항에 대한 PUSH 알림 수신 여부 설정	

- (앱스토어 등록 및 관리) 재난안전통신망의 앱 스토어에서 제공하는 앱 등록, 다운로드 현황 및 버전 관리가 가능

[그림 18] 앱스토어 등록 화면 예시

The screenshot displays the '앱스토어 등록' (App Store Registration) interface. It includes a '다운로드현황' (Download Status) table with columns for '번호' (No.), '버전' (Version), '어플리케이션명' (Application Name), 'OS', '상태' (Status), and '건수' (Count). The table lists several apps, including '재난안전통신망 앱스토어' (Disaster Safety Communication Network App Store). Below the table, there are sections for '앱 등록' (App Registration) with fields for version info, app icon, package name, APK file, and screenshots. To the right, there is a '버전 관리' (Version Management) section for 'Android' showing a list of versions (1.5 to 3.2) and their status (사용안함 - Not Used).

[표 14] 앱스토어 등록 및 사용장치

기능명	설명	사용장치
앱 등록	• 앱스토어에 등록하기 위한 기능으로 신규 또는 업데이트 버전으로 구분하여 등록이 가능	지령장치 PC
앱 다운로드 현황	• 앱 종류별 사용자 다운로드 현황을 파악	
안드로이드 등 버전 관리	• 안드로이드 등 OS 버전 지원 사항을 관리	

※ 앱스토어의 사용 매뉴얼은 [부록 H]를 참고

## 2.2.4.9. MDM(Mobile Device Management)

○ 재난안전통신망에 사용되는 다양한 장치(단말기, 지령장치, 컴퓨터)에 대한 통신 기능 차단 및 원격 관리 등에 대한 기능을 제공

※ 단, MDM은 보안 정책에 따라 기관별 개별 구축·운영할 수 없으므로 기관별 적용 정책은 행정안전부 재난안전통신망과와 사전 협의하여 결정

[그림 19] MDM 제어화면



[표 15] MDM 기능 및 사용장치

기능명	설명	사용장치
통신 기능 차단	<ul style="list-style-type: none"> <li>다음 항목에 대한 기능 차단 여부를 설정                             <ul style="list-style-type: none"> <li>- 카메라, WiFi, GPS, USB, NFC, OTA 업그레이드, 스크린샷, 외장메모리, 마이크, PS-LTE 접속, 블루투스, 테더링, 공장 초기화, 시간 변경, 인터넷 브라우저 등</li> </ul> </li> </ul>	단말기 지령장치 PC
단말기 원격 잠금	<ul style="list-style-type: none"> <li>단말기 분실, 탈취 시 원격지에 있는 관리자가 단말기를 잠금 조치</li> </ul>	
단말기 초기화	<ul style="list-style-type: none"> <li>단말기 프로그램 오류 및 자료 유실 등이 우려되는 경우 관리자가 원격으로 공장 초기화 기능 실행</li> </ul>	
앱 차단	<ul style="list-style-type: none"> <li>재난안전통신망 운영 정책에 위배되는 앱은 자동으로 설치를 차단하거나 삭제 조치</li> </ul>	

## 2.2.4.10. 재난안전통신망 보안 환경

- 재난안전통신망은 관련 지침 준수를 통해 보안 환경을 조성하여 보안성을 확보하고 보안취약점이 발생하지 않도록 운영·관리

[표 16] 재난안전통신망 관련 지침

정보통신 기반	<ul style="list-style-type: none"> <li>• 정보통신기반 보호법</li> <li>• 국가 정보보안 기본지침</li> <li>• 보안업무규정</li> <li>• 정부사물인터넷 도입 가이드라인</li> </ul>
보안규격	<ul style="list-style-type: none"> <li>• CC 인증</li> <li>• 보안적합성 검증 (국정원)</li> <li>• PS-LTE 릴리스 13 표준 규격 (2016, 3GPP)</li> <li>• 재난안전통신망(PS-LTE) : 기능적 요구사항(2015, TTA)</li> <li>• 인증기관 보안규격 등</li> </ul>
개인정보 보안	<ul style="list-style-type: none"> <li>• 개인정보 보호법</li> </ul>
개발보안	<ul style="list-style-type: none"> <li>• 소프트웨어개발보안가이드 (KISA)</li> </ul>

## 2.2.4.11. 재난안전통신망(PS-LTE) 서비스 보안

○ 재난안전통신망 서비스의 보안성 확보를 위해 아래 [표 17]의 보안 기능준수

[표 17] 재난안전통신망 보안 요구 기능

보안요구기능	설명
① 단말기 사용허가 및 금지	시스템 관리기에서 단말기를 유효화 (사용등록·허가) 또는 무효화(사용금지·불용) 시킬 수 있는 기능
② 암호화	전송구간을 암호화하여 도.감청을 방지하는 기능
③ 인증	허가된 사용자에게만 유효화된 통신서비스를 제공하는 기능
④ 보안규격	보안장비 등의 탑재를 위한 표준인터페이스 제공
⑤ 통합보안관제	해킹 방어를 위한 방화벽, 침입탐지·예방 등 통합 보안 관제 기능

○ (주제어시스템 보안) 주제어시스템 보안은 아래 [표 18]의 보안 항목 준수

[표 18] 주제어 시스템 보안 항목

번호	주제어 시스템보안	세부 내용
1	주제어시스템 관리자 식별 및 인증	주 제어시스템 구성 장비에 접근하는 관리자에 대한 식별 및 인증 기능을 제공해야 함
2	가입자 및 단말기 식별 및 인증	재난안전통신망에 접근하는 가입자 및 단말기에 대한 식별 및 인증 기능을 제공해야 함 ※ 3GPP PS-LTE 표준 적용
3	저장데이터 보호	주 제어시스템 구성 장비에 저장되는 중요정보에 대한 기밀성 및 무결성을 보장해야 함
4	통합보안관제	주 제어시스템에 대한 외부로부터의 공격 및 내부 자료 유출 등 보안사고 예방/탐지/대응을 위해 정보 보호제 품(방화벽, IPS, 서버 보안, DB 암호화, 악성코드 탐지 등)을 설치하여 운영해야 함
5	보안 약점	주 제어시스템 구성 장비 및 정보보호제품에 탑재되는 소프트웨어는 Secure Coding을 적용하여 보안 약점이 존재하지 않아야 함



## ○ (통신망 보안) 통신망 보안은 아래 [표 19]의 보안 항목 준수

[표 19] 통신망 보안 항목

번호	통신망 보안	세부 내용
1	기지국 장비 관리자 식별 및 인증	기지국 장비(RU, DU 등)에 접근하는 관리자에 대한 식별 및 인증 기능을 제공해야 함 ※ HSM과 동일한 보안 수준의 기능 적용
2	전송데이터 보호	단말기/통신망/주제어 시스템 간 통신 데이터에 대한 기밀성 및 무결성을 보장해야 함
3	저장데이터 보호	기지국 장비(RU, DU 등)에 저장된 재난안전통신망 관련 중요정보 (망 설정 정보 등)의 기밀성 및 무결성을 보장해야 함
4	보안 약점 제거	기지국 장비(RU, DU 등)에 탑재되는 소프트웨어는 Secure Coding을 적용하여 보안 약점이 존재하지 않아야 함

## ○ (단말기 보안) 단말기 보안은 아래 [표 20]의 보안 항목 준수

[표 20] 단말기 보안 항목

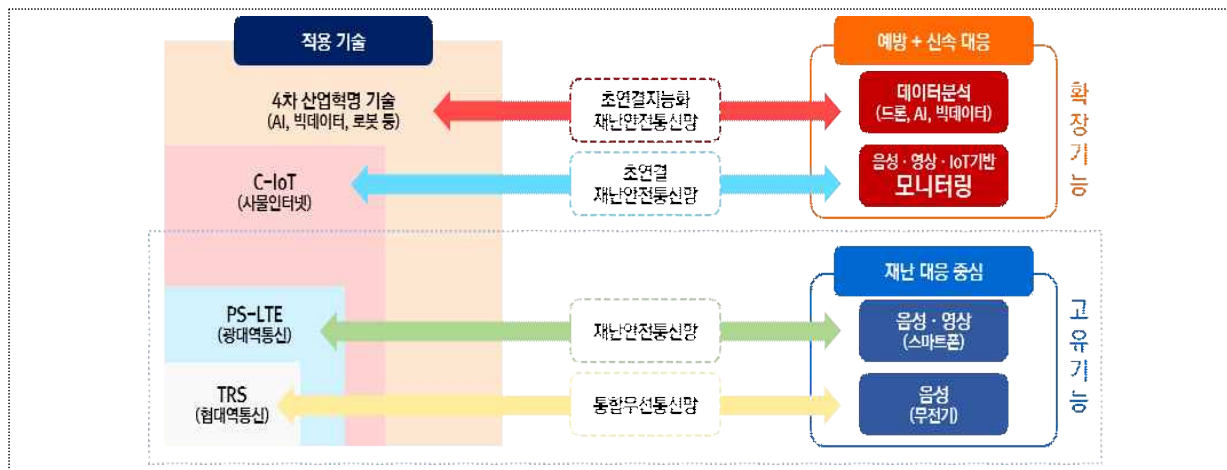
번호	단말기 보안	세부 내용
1	단말기 사용자 식별 및 인증	단말기 접근 사용자의 식별 및 인증 기능을 제공해야 함
2	가입자 및 단말기 식별 및 인증	재난안전통신망에 접근하는 가입자 및 단말기에 대한 식별 및 인증 기능을 제공해야 함
3	매체 제어 및 통신 경로 접근통제	단말기 내 중요 정보 유출방지를 위한 비인가 통신 경로 및 매체의 접근통제 기능을 제공해야 함
4	저장데이터 보호	단말기 또는 USIM 정보의 기밀성 등을 보장해야 함
5	USIM 복제 및 도용 방지	가입자 정보 복제 및 타 기관 USIM 도용 등 불법 접근을 방지해야 함
6	악성코드 탐지	악성코드 탐지 기능을 제공해야 함
7	인증서 보호 및 전자서명 검증	소프트웨어 업데이트 시 전자서명 검증 사용 및 인증서 보관, 유효성을 검증 기능을 제공해야 함
8	자체 시험	단말기의 정상 동작 여부, OS의 무결성 확인 등 자체 시험 기능 및 시험 실패 시 대응 기능을 제공해야 함
9	원격 잠금 및 원격 삭제	분실된 단말기에 대한 원격 잠금 및 원격삭제 또는 단말 초기화 기능을 제공해야 함
10	화면 잠금	단말기 일정 시간 이상 미사용 시 제공해야 함
11	시스템 서비스 접근통제	소프트웨어 및 사용자에게 의한 단말기 시스템 서비스(카메라, 마이크, GPS, 주소록 등)의 비인가 된 사용을 방지하는 기능을 제공해야 함
12	보안 약점 제거	단말기에 탑재되는 소프트웨어는 Secure Coding을 적용하여 보안 약점이 존재하지 않아야 함

### 3. 재난안전통신망 기반 응용서비스 소개

#### 3.1. 개요

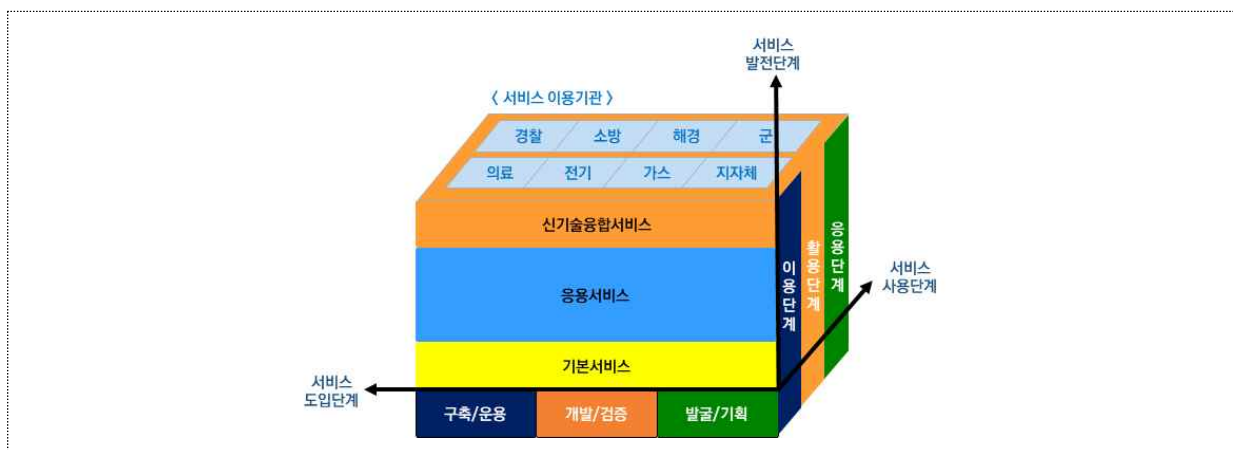
- (정의) 재난관리(예방·대비·대응·복구 활동) 측면과 안전관리(재난이나 각종 사고로부터 생명 및 재산의 안전을 확보하는 활동) 측면에서 재난 관련기관이 평시 또는 재난 시에 실제 업무에 활용할 수 있는 서비스
- (목적) 응용서비스는 현재 재난 대응 중심의 서비스에서 향후 시스템 업데이트 또는 추가 구축에 따라 재난의 예방과 신속 대응을 위한 확장기능으로 진화

[그림 20] 재난안전통신망 응용서비스의 진화 개념도



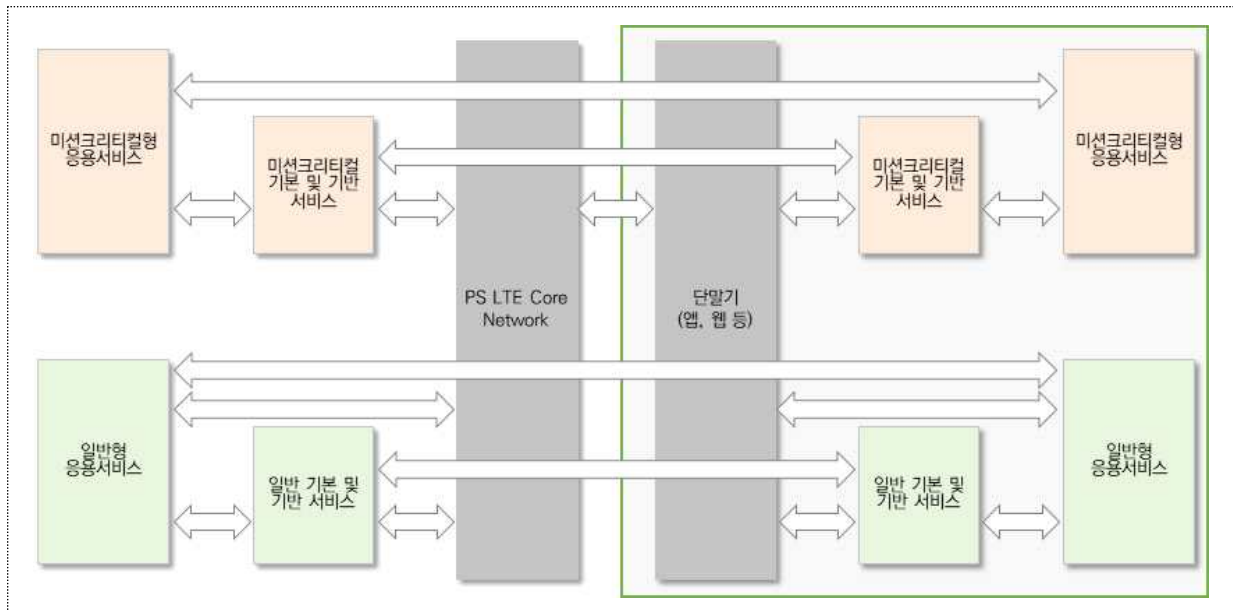
- (개념모델) 응용서비스는 기본서비스 기반 위에 구축되는 것으로 3GPP 후속 릴리스에 맞춰 기본서비스 및 응용서비스도 업그레이드

[그림 21] 공공안전서비스 프레임워크



- (범위) 재난관리와 안전관리를 위한 단말기 기반의 서비스
- (분류) 응용서비스는 미션크리티컬형 응용서비스와 일반형 응용서비스로 구분
  - (미션크리티컬형) 재난안전통신망 기본 서비스, 인터페이스 및 API를 기반으로 개발되는 시스템적 응용서비스로 시스템과 잘 통합된 서비스를 제공 가능
  - (일반형) 가용한 재난안전통신망 기본 서비스, 인터페이스 및 API가 미비하거나 이를 이용하기가 불가능한 경우에 별도로 개발하여 구축
- ※ 다른 무선통신망을 통하여 이용하고 있는 기존의 응용서비스들은 일반형 도입이 유리
- (구조) 응용서비스의 구조는 총 4가지로 미션크리티컬형, 진화된 미션크리티컬형, 일반형, 진화된 일반형으로 구분

[그림 22] 응용서비스의 간략한 구조도

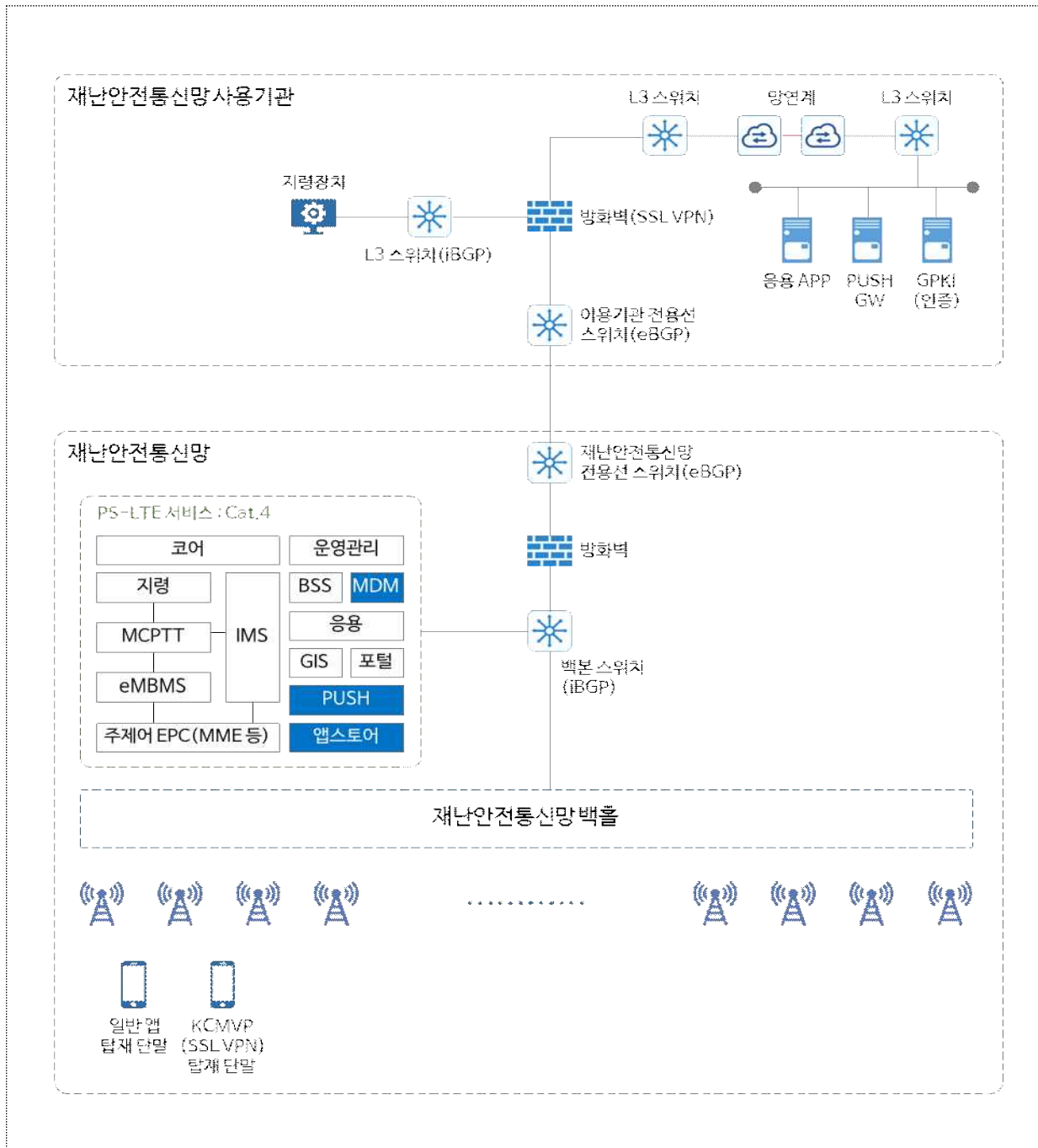


※ 이와 무관하게 단말기 간의 D2D 또는 DMR 통신을 이용하는 서비스는 행정안전부와 협의 후 구현 가능

### 3.2. 응용서비스 아키텍처

- 사용기관에서는 응용서비스 도입·개발 시 아래 [그림 23]의 아키텍처 예시와 같이 전용선을 통한 연계망을 구축하고, 필요에 따라 응용 APP, PUSH GW, GPKI 인증 서버 등을 추가로 도입하여야 함

[그림 23] 단말기 기반 앱 서비스 아키텍처 예시



- 사용 범위에 따라 기관 개별 응용서비스와 기관 공동 활용 서비스로 분류
- ※ 기관별 장비·서비스 도입사례는 부록 D 참조

## 4. 단계별 주요 수행내용 및 절차

### 4.1. 개요

장비·서비스 도입·개발 가이드라인은 총 4단계(기획, 개발, 구축, 운영단계)로 구성되어 있으며, 각 단계별로 사용기관(또는 사업체)과 지원기관의 주요 활동과 지원활동에 대하여 설명

#### □ 가이드라인 단계 및 구성

- 재난안전통신망 장비·서비스 도입·개발의 단계는 기획, 개발, 구축 및 운영 총 4단계로 구성

[표 21] 가이드라인 단계 및 주요내용

단계(Phase) 구분	주요 내용		
기획 단계	<ul style="list-style-type: none"> <li>행정안전부와 장비·서비스 도입·개발을 위한 조건 검토 등 사전협의를 통한 사업계획(안) 확정</li> </ul>		
	주요 산출물	<ul style="list-style-type: none"> <li>✓서비스 모델</li> <li>✓보안성 검토서</li> </ul>	<ul style="list-style-type: none"> <li>✓사전협의를서</li> <li>✓사업계획서</li> </ul>
개발 단계	<ul style="list-style-type: none"> <li>사용기관(제조사 포함) 주도로 기획 의도와 재난안전통신망 보안 및 요구기능에 부합되는 장비·서비스 개발</li> </ul>		
	주요 산출물	<ul style="list-style-type: none"> <li>✓상세설계서</li> </ul>	<ul style="list-style-type: none"> <li>✓보안인증서</li> </ul>
구축 단계	<ul style="list-style-type: none"> <li>개발된 장비·서비스는 재난안전통신망 기술기준에 따라 검증을 수행하고, 재난안전통신망 운영센터를 통해 반입/연동 승인 후 개통</li> </ul>		
	주요 산출물	<ul style="list-style-type: none"> <li>✓시험성적서</li> <li>✓검증서</li> <li>✓검수완료서</li> </ul>	
운영 단계	<ul style="list-style-type: none"> <li>실제 장비·서비스를 운영·관리하는 사용기관은 운영계획을 수립·이행하고 서비스 유사·중복성에 대한 점검 및 진단</li> </ul>		
	주요 산출물	<ul style="list-style-type: none"> <li>✓운영계획서</li> </ul>	

- 장비·서비스 도입·개발 가이드라인의 각 단계는 단계에 대한 주요내용 설명 및 업무흐름도, 그리고 업무별 주요 Activity로 구성
  - (단계요약) 가이드라인의 단계별 주요내용을 요약하여 설명
  - (업무흐름도) 가이드라인 단계별로 관계기관의 주요업무를 도식화하여 설명
  - (Activity) 업무흐름도에 따른 사용기관과 지원기관 등 관계기관의 주요 업무 및 지원내용을 설명

## 단계별 가이드라인 구성 방식

### 4.X. XX 단계

#### 각 단계의 구성에 대한 안내

#### 4.X.1. XX 단계 업무 흐름

[표 xx] XX 단계 업무 흐름

XX 단계 업무 흐름 삽입

#### 4.X.2. 업무 흐름에 따른 Activity 기술

□ Activity 정의, 고려사항, 도입 지침, 지원요청 등 서술

##### ① 상세내용 기술



00을 위한 00 (Activity 명칭 및 지원내용 등)

▶ 00

• 00

※ 가이드라인의 주요 서류에 대해서는 작성 방법 및 예시 제시

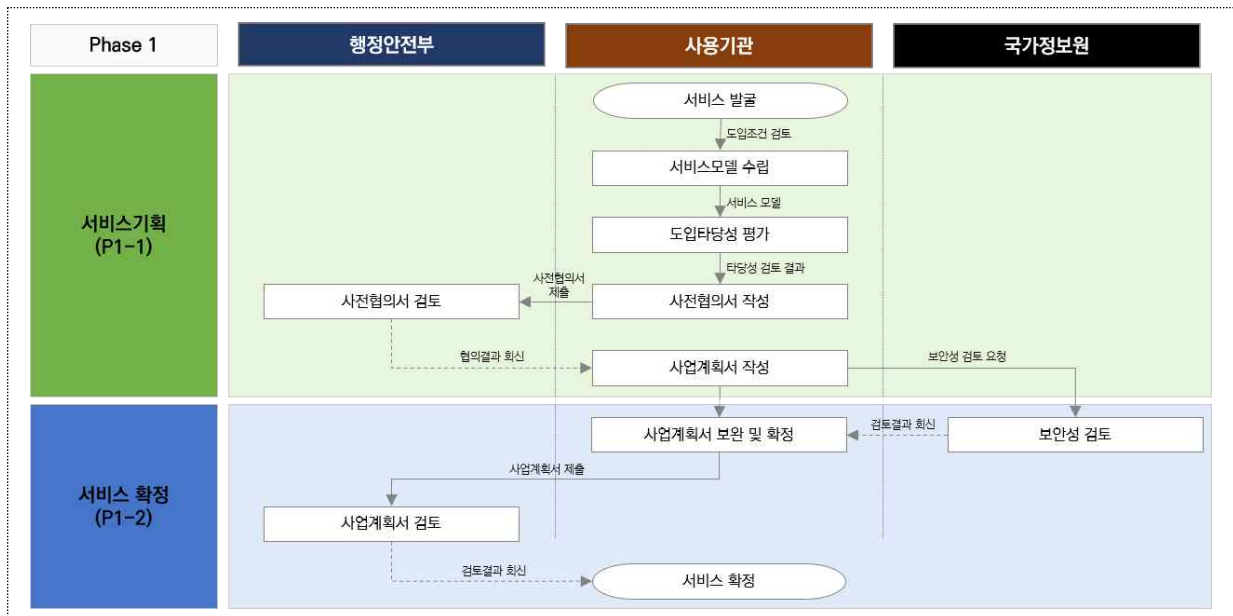
## 4.2. 기획 단계

사용기관에서 도입·개발하는 장비·서비스에 대해 재난안전통신망 수용조건 검토와 보안성 검토 결과를 바탕으로 사전협의를 통해 응용서비스를 확정하는 단계

### 4.2.1. (Phase 1) 기획 단계 업무흐름도

- 응용서비스 기획 단계는 서비스 기획과 서비스 확정, 총 2단계로 구성
  - (P1-1 서비스 기획) 사용기관에서 장비·서비스 개발 및 서비스 제공 방안을 수립하여 행정안전부와 사전협의를 거쳐 사업계획서를 작성
  - (P1-2 서비스 확정) 보안성 검토 결과를 반영한 사업계획서를 가지고 행정안전부의 검토를 통해 서비스 제공 계획 확정

[그림 24] 응용서비스 기획 단계 업무흐름도



### 4.2.2. (P1-1) 서비스 기획

#### 4.2.2.1. 장비·서비스 개발 및 응용서비스 제공 방안 마련

- (필수 요구사항) 사용기관은 도입하고자 하는 응용서비스가 재난안전통신망에서 요구하는 규격사항을 만족하는지를 확인
  - ※ 사전에 확인이 불가능한 사항은 사후에 확인하는 조건으로 추진

[표 22] 재난안전통신망 요구 규격

번호	요구사항	비고
1	재난안전통신망에 부하가 걸리지 않는 범위 내에서의 응용서비스 추가	재난안전통신망 운영센터에서 판정
2	해당 응용서비스를 위해 재난안전통신망 S/W 또는 라이선스가 추가로 필요할 경우, 이들이 포함되어야 함	
3	동시 이용자들이 안정적으로 서비스를 받을 수 있도록 운영 가능하여야 함	
4	유니코드(UTF-8) 지원하여야 함	텍스트의 입출력이 사용되는 경우
5	IPv6의 수용이 가능하여야 함	
6	OS 호환성이 보장되어야 함	데스크톱형을 위한 윈도우, 스마트폰형 단말기를 위한 안드로이드 등
7	재난안전통신망 도입 단말기와의 호환성이 있어야 함	단말기가 사용될 경우, 해당 단말기에 적용
8	원격에서 소프트웨어 버전을 업데이트 및 제어 관련 구성 변경이 가능하여야 함	단말기가 사용될 경우, 해당 단말기에 적용
9	재난안전통신망에서 지원이 가능한 기술이어야 함	

○ (도입조건) 재난안전통신망 기반의 응용서비스 도입을 위해 아래의 3가지 도입 조건에 부합되는지를 검토

① 목적성 부합

가) 재난안전통신망법 「제4장 제16조」에 해당되는 경우에 한하여 재난안전통신망의 사용이 가능

나) 기관 개별 서비스 주목적이 「재난 및 안전관리 기본법 제3조 제11호」에 해당되는 경우\*에 한하여 수용 가능

\* 재난관리책임기관 · 긴급구조기관 및 긴급구조지원기관이 재난안전통신망을 재난관리업무에 이용하거나 재난현장에서의 통합지휘에 활용하는 경우



다) 재난안전통신망 운영 및 사용에 관한 규정「제3장 제22조 사용 신청」에 따라 서비스 이용 목적에 부합하는지 점검

※ 재난안전통신망 목적에 부합, 수용 통신량 및 기술적 방법, 중복성 문제 등

라) 위 기준에 부합하지 않는 경우에는「전기통신사업법 제65조」에 따라 재난 안전통신망의 목적 外 사용으로 법 위배 사항에 해당

## ② 중복성 최소화

가) 특별한 사유가 없는 한 재난안전통신망 기본서비스를 사용하는 것을 우선 검토

나) 기본 서비스와 기능적인 중복성이 있으나 보안 침해 우려, 트래픽 용량 부족 등 필요 사유가 명백한 경우에는 일부 중복 허용

## ③ 타당성 확보

가) 재난안전통신망과 연계/이전하기 위해 관련 법령, 기술적, 경제적, 정책적 타당성 여부를 사전에 자체 검토한 후 행정안전부와 협의 추진

○ (수용조건) 재난안전통신망 기반을 활용한 응용서비스 도입을 위하여 아래의 5가지 수용조건에 부합되는지를 검토

### ① 재난안전통신망 사용에 대한 검토

가) 다음에 해당하는 경우에는 재난안전통신망 사용의 일부를 제한할 수 있음

- 재난안전통신망의 안정적인 품질을 유지하기 어려운 서비스인 경우
- 일시적인 통신량 폭주로 장비의 정상적인 동작이 불가능한 경우
- 보안에 피해가 있거나 우려되는 경우
- 상용망 이용요금 등을 장기간 납부하지 않은 경우
- 재난안전 업무에 무관한 인터넷 사이트 등을 접속하는 경우

※ 재난안전통신망 운영 및 사용에 관한 규정「제3장 제24조 사용 제한」을 참조

### ② 비용 부담

가) 다음에 해당하는 경우에는 사용기관이 재난안전통신망 비용을 부담하여야 함

- 사용기관 개별 서비스를 기간통신사업자의 이동통신망 기지국을 경유하여 재난 안전통신망에 연결하는 경우에 발생하는 이동통신요금

- 사용기관 개별 장비를 재난안전통신망과 연결하기 위하여 필요한 기간통신사업자의 전용회선 요금
- 기타 행정안전부장관이 필요하다고 인정하는 사항인 경우

나) 행정안전부장관은 기간통신사업자와 재난안전통신망 사용기관의 비용 절감 등 효율적인 관리를 위한 협약을 체결할 수 있음

※ 재난안전통신망 운영 및 사용에 관한 규정「제3장 제26조 비용 부담」을 참조

### ③ 무선 커버리지 확장

가) 재난안전통신망 고정기지국의 무선 커버리지 外 지역(실내, 지하, 산악 등)에서 기관 개별 서비스를 제공하는 경우에는 해당 사용기관의 부담으로 고정기지국 등 추가 설치 고려

나) 위의 사유로 기관 자체 고정기지국을 설치할 필요성이 있다고 판단되는 경우에는 반드시 행정안전부와 사전 협의 후 추진

※ 재난안전통신망 운영 및 사용에 관한 규정「제3장 제9조 주파수 관리」을 참조

### ④ IP 주소 체계

가) 재난안전통신망과 연계하고자 하는 서비스는 IPv6 주소 체계를 따라야 하며 불가피한 사유가 있는 경우에는 NAT 장비를 이용하여 IPv4를 사용할 수 있음

※ IPv6 주소체계는 [부록 J] 재난안전통신망 IPv6 주소체계 참조

### ⑤ 타 기관 정보 연계

가) 재난안전통신망 내 타 기관의 정보와 연계한 서비스를 개발·이용하고자 하는 경우에는 타 기관의 동의를 얻은 후 재난안전통신망 운영센터와 사전 협의

- 재난안전 서비스에 활용 가능한 활용데이터의 종류, 연계성, 범용성 여부 등
- 타 사용기관 또는 공공기관과의 상호연계 또는 공동이용 방안 및 중복여부 등

나) 타 기관과 연계되는 활용데이터는 지속적 또는 실시간 생산되어 타 데이터와 연계 융합 등 범용성이 높은 데이터인지 검토하여야 함

※ 재난안전통신망의 이용 가능 여부에 대한 사용기관 차원의 사전검토는 【붙임 3】 사용기관의 응용서비스 적용을 위한 체크리스트를 참조

○ (서비스 발굴) 재난안전을 위한 응용서비스가 상기의 필수요구사항, 도입조건, 수용조건을 모두 만족하는 경우 응용서비스를 선정하여 타당성 평가를 수행

## 4.2.2.2. 응용서비스 도입 타당성 평가

- 사용기관은 필수 요구사항 및 조건을 검토하여 만족하는 경우 타당성 점검지표로 타당성 평가를 자체적으로 수행하여 적정 여부를 판단

※ 아래 [표 23]의 타당성 평가 지표는 예시이며, 실제 운영에 따라 수정이 가능

[표 23] 타당성 점검지표 예시

지표 유형	세부 평가지표	지표 정의	평가방안
업무 부합성	목표의 명확성	사업목표가 구체적이고, 다양한 관점에서의 목표가 설정되었는지 여부	명확성 높음 - 4점 명확성 보통 - 3점 명확성 낮음 - 2점
	서비스 적정성	재난안전통신망을 통해 장애 없는 재난안전 서비스 구현이 가능한지 여부	적정성 높음 - 4점 적정성 보통 - 3점 적정성 낮음 - 2점
	서비스 완결성	신규 서비스를 도입하였을 때, 서비스의 목적을 충분히 달성할 수 있는지 여부	완결성 높음 - 4점 완결성 보통 - 3점 완결성 낮음 - 2점
	정보제공 수집유형	해당 서비스가 정보를 제공하거나 수집하는 유형	양방향형 - 4점 일부 양방향형 - 3점 정보제공/수집형 - 2점
파급 효과	활용 빈도	해당 서비스가 재난안전통신망에서 구현 시 예상되는 활용도 수준	활용 빈도 높음 - 4점 활용 빈도 보통 - 3점 활용 빈도 낮음 - 2점
	시급성	신규 서비스 구축 시점상 즉시 의사결정이 필요한지 여부	즉시 구축 필요 - 4점 구축 시급성 보통 - 3점 구축 시급성 낮음 - 2점
	수요의 범위	신규 서비스의 수요 범위가 특정 사용기관 또는 계층인지 여부	사용기관 공동 사용 - 4점 일부 사용기관 사용 - 3점 특정 사용기관 사용 - 2점
실현 용이성	단말 범용성	OS(운영체계) 범용성을 확보하고 단말 종속성이 낮은지 여부 검토	범용성 높음 - 4점 범용성 보통 - 3점 범용성 미확보 - 2점
	사업의 연속성	이미 구축된 시스템의 재난안전 서비스 여부(전환 여부)	전환 서비스 - 4점 신규 구축 서비스 - 4점
	법적근거 확보여부	사업의 법적 근거를 확보했고 근거로 제시할 수 있는지 여부	법적 근거 확보 - 4점 법적 근거 미확보 - 2점

타당성 평가 결과 (예)

유형	내용	결과
적정 의견	타당성 평가 결과 모든 평가지표 유형이 적정기준 점수인 75점 이상인 경우	사업추진
한정 의견	타당성 평가 결과 3개의 평가지표 유형 중 2개 유형이 적정기준점수인 75점 이상인 경우	기획안 수정/폐기 고려
부적정 의견	타당성 평가 결과 적정기준점수인 75점 이상의 평가지표 유형이 없거나 1개인 경우	기획안 폐기 고려

## 참고사항

- ◇ 타당성 평가지표 100점 기준 환산 방법(예시)
- 업무 부합성 : 업무 부합성 평가 점수 합계 x 100 ÷ 16
  - 파급효과 : 파급효과 평가 점수 합계 x 100 ÷ 12
  - 실현 용이성 : 실현 용이성 평가 점수 합계 x 100 ÷ 12

## 4.2.2.3. 사전협의를 작성

## □ 사전협의를 작성 및 협의

- 타당성 검토 결과를 바탕으로 사전협의를 작성하여 행정안전부 재난안전통신망과와 응용서비스 도입 사전협의를 수행
- 사전협의를 작성항목은 아래 [표 24]을 참조하여 작성하되 필요한 경우 항목 추가 등 조정 가능

[표 24] 사전협의를 작성 항목

항목	주요내용
1. 개요	<ul style="list-style-type: none"> <li>○ 추진배경 및 필요성</li> <li>○ 응용서비스 내용</li> <li>○ 소요 예산 내용</li> <li>○ 기대효과 등</li> </ul>
2. 현황 및 문제점	<ul style="list-style-type: none"> <li>○ 응용서비스 도입 전 업무 및 정보화 현황</li> <li>○ 문제점 및 개선 방향 등</li> </ul>
3. 추진 내용	<ul style="list-style-type: none"> <li>○ 응용서비스 기능 및 필요 데이터량</li> <li>○ 목표 시스템 구성 (S/W, H/W)</li> <li>○ 재난안전통신망 연동</li> </ul>
4. 추진 체계	<ul style="list-style-type: none"> <li>○ 대상 사업과 관련하여 참여주체별 역할과 기능을 명시</li> </ul>
5. 추진 일정	<ul style="list-style-type: none"> <li>○ 사업 추진 일정을 월별로 제시</li> </ul>
6. 중점 협의 사항	<ul style="list-style-type: none"> <li>○ 다양한 현안 중 행정안전부와 중점적으로 협의할 사항을 작성 ※ APP 연계 방안 등</li> </ul>

※ (필요시 추가 제출 자료) 사업계획서(안), 제안요청서, 과업지시서, 관련 용역보고서 등 상세 사업내용 및 상용망에서 재난안전통신망으로 전환 시 소요예산 비교 검토 자료 등

- 사용기관은 행정안전부 재난안전통신망과와 사전 협의된 결과가 반영된 최종 사업계획서를 작성하여 국정원 보안성 검토를 수행

## 참고사항

◇ 서비스 사용 시 필요 데이터량 산정 예시 (현장 동원 인원 : 200명 기준)

재난 시 평균의 셀 처리 용량을 초과하는 데이터 트래픽이 발생할 가능성이 크므로, 응용 서비스의 MCPTT 적용 등급과 특정 상황에서의 서비스 차단 기준을 고려하여 산정

서비스에 따른 생성 데이터의 크기(예)

서비스	Codec/Packet		비고
	적용규격	비트율 [Kbps]	
음성통화	EVS(NB, WB, SWB)	9.6	Default
		13.2	
		16.4	
		24.4	
영상통화	VoLTE : H.265(VGA)	536.4	VGA(15fps)
	MCPTT : H.264(QVGA)	256	QVGA(15fps)
메시지	SMS	7.88	
	MMS	1001.1	사진(0.5MB) 기준
영상데이터	H.264	VGA(15fps)	512
	H.265	VGA(15fps)	512
	H.265	720P(24fps)	1,000
센서데이터	-	13	

※ 음성통화와 영상 데이터에 대하여 TTAK.KO-06.0496 재난안전통신망 단말기 기술 규격을 참고

서비스 사용주기 기준 소요용량 산정

통신서비스	사용인원 [명]	사용데이터 속도 [Kbps]	사용데이터 길이 [초]	사용주기 [초]	시간당 사용데이터량 [Mbps]
PTT 음성	200	9.6	10	20	3,456.0
영상통화	200	536.4	30	600	38,620.8
영상 데이터	50	1,000.0	10	300	18,000.0
MMS 메시지	10	1,001.1	10	10	36,039.6
합계 [Mbps]					96,116.4
셀 데이터 처리 용량(Throughput) [Mbps]					26.699

(산출 내역)

- PTT 음성) 200[명] x 9.6[Kbps] x 10[s] x 3,600 / 20[s] = 3,456.0[Mbps]
- 영상통화) 200[명] x 536.4[Kbps] x 30[s] x 3,600 / 600[s] = 38,620.8[Mbps]
- 영상 데이터) 50[명] x 1000.0[Kbps] x 10[s] x 3,600 / 300[s] = 18,000[Mbps]
- MMS 메시지) 10[명] x 1,001.1[Kbps] x 10[s] x 3,600 / 10[s] = 36,039.6[Mbps]
- 합계 = 97,412.4[Mbit/h]
- 셀 데이터처리 용량(Throughput) = 96,116.4[Mbps] / 3,600 = 26.699[Mbps]

서비스 사용빈도 기준 소요용량 산정

통신서비스	사용인원 [명]	사용빈도 [%]	사용데이터 [Kbps]	셀 용량 [Mbps]
PTT 음성	200	50%	9.6	0.960
영상통화	200	10%	536.4	10.728
영상 데이터	50	10%	1,000.0	5.000
MMS 메시지	10	100%	1,001.1	10.011
셀 데이터 처리 용량(Throughput)				26.699

(산출 내역)

- PTT 음성) 200[명] x 0.5 x 9.6[Kbps] = 0.960[Mbps]
- 영상통화) 200[명] x 0.1 x 536.4[Kbps] = 10.728[Mbps]
- 영상 데이터) 50[명] x 0.1 x 1000.0[Kbps] = 5.000[Mbps]
- MMS 메시지) 10[명] x 0.1 x 1,001.1[Kbps] = 10.011[Mbps]
- 셀 데이터 처리 용량(Throughput) (= 합계) = 26.699[Mbps]



## 사전협의서 주요 검토 지원 내용

### ▶ 법제도

- ✓ 「재난안전통신망법」, 「재난 및 안전관리 기본법」 및 「동법의 시행령」에서 규정한 재난안전통신망의 이용범위 및 대상기관 부합 여부 평가
  - ※ 이용범위 : 재난현장 긴급통신 수단 또는 재난안전 관련 분야
  - ※ 대상기관 : 재난안전통신망 8대 분야 사용기관 및 재난 관련기관

### ▶ 목적의 명확성

- ✓ 해당 서비스가 재난안전통신망의 목적에 맞는 재난안전 관련 분야 또는 공공성·시급성 등의 목적 여부 평가
  - ※ 이용분야 : [부록 D] 기관 장비/서비스 도입 사례 참조

### ▶ 유사성 및 중복성

- ✓ 해당 서비스가 타 기관 및 민간영역에서 이미 개발되어 운영 중인지 (민간영역 침해 여부 등) 등 유사·중복 여부 식별
  - ※ 타 기관 및 민간영역과의 유사, 중복 여부에 대한 조사, 평가 결과 제시 필요

### ▶ 재난안전통신망 특성

- ✓ 해당 서비스 적용 시 재난안전통신망의 필수 제공기능(MCPTT 등)의 성능에 미치는 영향도 분석을 통한 망 내 서비스 우선순위 적용 등
  - ※ 재난 등 비상상황 시 재난안전통신망을 우선적으로 서비스함에 따른 서비스 제약 (중단, 품질 저하 등)을 고려

### ▶ 기술

- ✓ 해당 서비스가 현재의 재난안전통신망에서 제공하는 규격·기술로 수용 및 연계 가능 여부 평가 등

### 4.2.3. (P1-2) 서비스 확정

#### 4.2.3.1. 보안성 검토

- 사용기관은 사용기관 자체 정보통신망 또는 정보시스템을 재난안전통신망과 연계하고자 하는 경우에는 국가정보원에 보안성 검토를 의뢰
  - ※ 재난안전통신망 운영 및 사용에 관한 규정「제3장 제27조 연계 사용」을 검토
  - ※ 기초자치단체가 해당 상위기관에서 검토 받는 것으로 국가정보원 검토를 대체하지 않음에 유의
- 사용기관은 작성된 사업계획서를 가지고 자체적으로 보안성 검토 고려사항을 확인 후 국가정보원에 보안성 검토를 요청

[표 25] 보안성 검토 관련 고려사항

항목	상세내용
공통사항	<ul style="list-style-type: none"> <li>○ 재난안전통신망의 모든 주소체계는 IPv6임</li> <li>○ 신규도입 장비는 취약점이 제거된 최신 버전으로 운영하고 운용과정에서도 각 제품별 업체가 제공하는 최신 보안패치 적용</li> <li>○ 국가 · 공공기관이 도입하는 정보보호시스템과 네트워크 장비는 유형에 따라 CC 인증 또는 보안기능 확인서 등 사전 인증을 획득</li> </ul>
외부망 연계	<ul style="list-style-type: none"> <li>○ 재난안전통신망은 외부 인터넷(네이버, 구글 등)과 단절된 자가통신망임</li> <li>○ WiFi 무선라우터 등 비인가 정보통신 장치를 활용한 인터넷 무단 접속을 금지</li> <li>○ 네트워크 장비와 단말기에서 사용하는 IP 대역을 제외한 인터넷 IP대역은 네트워크 장비에서 차단(화이트리스트 정책 적용)</li> <li>○ 상용망과 외부망 연동구간에 보안시스템과 NAT를 활용하여 인터넷 직접 연결을 차단하고 재난안전통신망과 상용망 연동 구간은 보안시스템, VPN 등을 활용하여 취약점을 최소화</li> </ul>
트래픽 우선 순위	<ul style="list-style-type: none"> <li>○ 재난상황으로 데이터 대량 발생시 응용서비스의 데이터보다 기본서비스의 음성정보를 우선적으로 처리</li> </ul>
단말기 관련	<ul style="list-style-type: none"> <li>○ 단말기는 국정원 '모바일 활용 업무에 대한 보안 가이드라인'에서 명시된 모바일 현장 행정업무용 단말기 운용방침 준용</li> <li>○ 긴급 상황 시 양손이 자유로운 상태에서 통신망을 사용할 수 있도록 단말기에 음성 전송을 위한 블루투스 이어폰에 한하여 연결 허용</li> <li>○ 단말기 미사용시 기본적으로 일정시간(8시간) 이후 '자동잠금' 기능을 활성화 시키되 필요 시 해당 기능 비활성화 등은 탄력적으로 운용 가능</li> <li>○ 운영체제에서 기본 제공하는 구글 플레이어 · 웹브라우저 등 불필요한 통신 기능과 응용프로그램은 삭제하거나 비활성화</li> <li>○ 단말기에 문서 등 저장 불가(직접 촬영한 동영상과 사진 제외)</li> <li>○ OS와 백신은 최신 업데이트 버전으로 운영토록 내부 별도 업데이트 서버 운영</li> </ul> <hr/> <ul style="list-style-type: none"> <li>○ 시큐어 코딩 적용 여부 확인</li> <li>○ (물리적 보안) 디바이스 보드 내에 디버그 포트(UART, JTAG)나 물리적 접촉에 의한 데이터 추출 가능 여부를 확인(물리적 접촉에 의한 해킹 공격의 가능 여부)</li> <li>○ (데이터 보안) 보호해야할 데이터를 암호화 등을 통해 보호할 수 있는지 확인하고, 데이터 보안 제공 방안을 확인</li> </ul>

#### 4.2.3.2. 사업계획서 및 서비스 확정

- 사용기관은 국가정보원의 응용서비스에 대한 보안성 검토 결과가 반영된 최종 사업계획서를 행정안전부 재난안전통신망과에 제출 및 검토를 받은 후 응용서비스를 최종적으로 확정



#### 응용서비스 도입·개발 지원체계 및 역할

##### ▶ 지원체계



##### ▶ 기관별 역할

구분		주요 업무
총괄기관	행정안전부	<ul style="list-style-type: none"> <li>재난안전통신망 이용 및 응용 총괄</li> <li>재난안전통신망 이용 및 응용 정책협의 및 관계부처 협의</li> <li>재난안전통신망 통신자원 망 할당</li> </ul>
지원기관	한국지능정보 사회진흥원	<ul style="list-style-type: none"> <li>재난안전통신망 이용 및 응용신청 접수·관리·지원</li> <li>심의위원회 구성·운영</li> <li>재난안전통신망 이용 및 응용 수요조사 및 발굴</li> <li>재난안전통신망 이용 및 응용 가이드라인 제작·보완·배포 등을 통한 이용활성화</li> </ul>
신청기관	8대 사용기관	<ul style="list-style-type: none"> <li>재난안전통신망을 통한 이용 및 응용서비스에 대한 요구사항 마련 및 신청</li> <li>확정된 재난안전통신망 이용 및 응용서비스의 예산확보 및 개발</li> </ul>



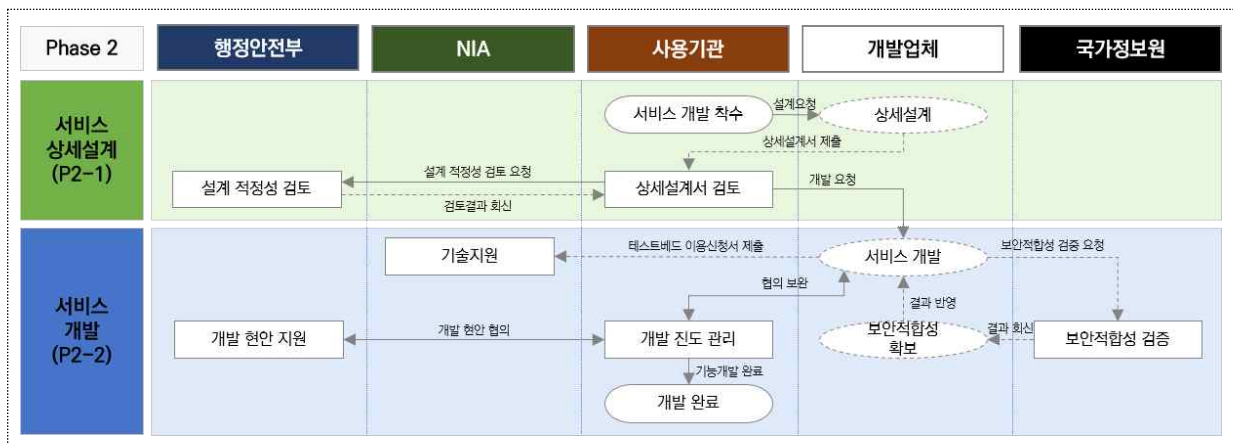
### 4.3. 개발 단계

사용기관이 개발업체와 응용서비스 개발을 위한 상세설계를 실시하고 이를 기반으로 서비스를 개발하여 보안적합성 검증 단계를 거쳐 서비스 개발을 완료하는 단계

#### 4.3.1. (Phase 2) 개발 단계 업무흐름도

- 응용서비스 개발 단계는 서비스 상세설계 단계와 서비스 개발 단계, 총 2단계로 구성
  - (P2-1 상세설계) 사용기관이 개발업체를 통해 서비스에 대한 상세설계를 실시하고 행정안전부 재난안전통신망과와 협의를 통해 상세설계를 확정
  - (P2-2 서비스 개발) 상세설계를 기반으로 개발에 착수하여 개발된 제품 및 서비스에 대한 지원기관의 지원 및 보안적합성 검증을 통해 개발 완료

[그림 25] 응용서비스 개발 단계 업무흐름도



#### 4.3.2. (P2-1) 서비스 상세설계

##### 4.3.2.1. 상세설계 시 고려사항 검토

- 효율적인 응용서비스 개발을 위한 개발언어, 개발방식 및 필요기술 검토
- 서비스의 이용과 제공을 고려하여 Front-end와 Back-end를 종합적으로 검토
  - Front-end : 응용서비스 중 사용자에게 직접적으로 보이는 부분(예: UI/UX, Client 등)
  - Back-end : 응용서비스 중 사용자에게 보이지는 않지만, 서비스 제공에 중요한 역할을 담당하는 부분 (예: Server, Data base 등)

- 재난안전통신망의 폐쇄성을 고려
  - 인터넷 접속이 불가능한 재난안전통신망의 폐쇄성을 고려하여 기능을 구현
- 재난안전통신망의 제한된 네트워크 자원을 고려
  - 재난안전통신망의 제한된 네트워크 대역폭 고려하여 서비스를 제공할 수 있도록 설계 및 기능을 구현

[표 26] 응용서비스 앱 개발 고려사항

구분	옵션	세부내용
Front-end	1. OS 네이티브 앱 개발방식	<ul style="list-style-type: none"> <li>· iOS, Android와 같은 특정 OS용으로 개발하는 방식</li> <li>· 장점: 하드웨어 및 기능을 구현하는데 제약조건이 없으므로 다양한 기능과 시나리오 개발에 유익</li> <li>· 단점: 개발언어는 해당 OS에서만 지원하므로 각각의 개발자들이 필요</li> </ul>
	2. 크로스 플랫폼 솔루션 개발방식	<ul style="list-style-type: none"> <li>· 자바스크립트(JS) 기반으로 개발한 하나의 앱으로 특정 OS 플랫폼에서 호환되어 작동할 수 있는 개발방식</li> <li>예) Xamarin, React Native 및 Native Script와 같은 Cross 플랫폼 개발방식</li> <li>· 장점: 네이티브 앱을 JS 방식으로 개발함으로써 외부 DK의 도움으로 빠른 개발과 예산의 효율성이 높음</li> <li>· 단점: 외부 솔루션이 지원하는 범위 내에서 기능구현이 가능하므로 기능구현의 확장성이 떨어짐</li> </ul>
	3. 하이브리드 앱	<ul style="list-style-type: none"> <li>· 가장 많은 개발팀이 사용하는 방식으로써 모든 장치와 OS에 호환할 수 있는 웹과 네이티브의 호환 방식으로 개발하는 방식</li> <li>· 장점: 각각의 플랫폼마다 모두 다른 코딩을 할 필요가 없음. 비용 효율성이 높고 참여 가능한 개발자가 많음</li> <li>· 단점: 일반적인 네이티브 앱보다 성능 측면에서 부족할 수 있음</li> </ul>
Back-end	1. 개발언어 선택	<ul style="list-style-type: none"> <li>· Front end 개발언어 중 선택(Object C, Swift, JAVA, .NET, PHP, Python, JS 등) 하거나 다른 언어를 선택 가능</li> <li>· 외부 연동시스템이나 향후 확장성 개발도 고려하여 선택 필요</li> </ul>
	2. 데이터베이스 및 데이터 구조	<ul style="list-style-type: none"> <li>· 예산, 요구 성능, 용량을 고려하여 선택</li> <li>예) MySQL, MongoDB, PostgreSQL, Oracle</li> </ul>
	3. 호스팅	<ul style="list-style-type: none"> <li>· 소요 예산, 호스팅 비용, 예상 성능, 안정성 고려</li> <li>· 사용자 증가에 따른 확장 방안 계획수립 필요</li> </ul>

※ 현재 재난안전통신망 단말기는 안드로이드 OS 기반

- 개발업체에서 상세설계가 완료되면 사용기관은 행정안전부 재난안전통신망과에 설계의 적정성에 대한 검토를 요청
- 행정안전부 재난안전통신망과의 설계 적정성 검토 결과가 반영된 최종 상세설계서를 바탕으로 서비스 개발에 착수

## 참고사항

- ◇ 【붙임 4】 개발조직의 응용서비스 적용을 위한 체크리스트를 통한 사전확인



## 응용서비스 개발 방향 설정 지원내역

- ▶ 사용기관은 응용서비스 개발을 위한 방향 설정에 있어서 행정안전부는 아래의 항목에 대하여 지원
  - ✓ 재난안전통신망 인프라 연동방안\*
    - \* 인프라 연동방안 상세 내용은 【붙임 5】 참조
  - ✓ 재난안전통신망 이용 관련 요구사항
    - ※ 재난안전통신망 인프라 연계 방안은 재난안전통신망 구성 환경, 요구 규격 및 요구사항 준수를 원칙으로 함

### 4.3.3. (P2-2) 서비스 개발

#### 4.3.3.1. 단말기 기반 서비스 개발 지침 검토

- 응용서비스 개발 시에는 아래 [표 27]의 사항들을 고려하여 개발

[표 27] 응용서비스 개발 시 고려사항

항목	설명
1. 사용자 인증	허용된 사용자의 식별 수단 제공 필요
2. 사용 편의성을 우선한 UI 설계	사용 편의성을 고려한 직관적인 UI
3. 접근권한	과도한 접근권한 허용 금지
4. 정보보호	중요정보나 개인정보 유출방지
5. 국정원 보안적합성 인증	공공기관에 도입하는 IT 제품의 안정성을 검증하는 제도
6. 보안 소프트웨어 연동	백신, MDM 연동
7. 운영체제 변조 대응	운영체제 변조 상황에 대한 대응
8. 분실상황 대응	단말기 분실상황에 대한 대응
9. 리소스 사용	과도한 리소스 사용 방지
10. 업데이트	추가 기능 개발 및 OS 호환성을 유지하기 위함

#### ① 사용자 인증

- 인가된 사용자만 사용할 수 있도록 사용자를 확인하는 기능 제공 필요
- 기본적으로 ID/PW 방식을 사용, 필요에 따라 추가 인증 수단 제공 필요
  - 예) IMEI, UDID와 같은 기기 고유정보, SMS, OTP, 공인인증서, 생체정보 등
- 단순한 비밀번호 사용금지
  - 예) 연속된 숫자, 문자, 혹은 쉽게 유추가 가능한 단순한 비밀번호
- SSO(Single Sign-On) 사용 중인 사용기관의 경우 SSO 인증 방식을 우선 고려

## ② 사용 편의성을 우선한 UI 설계

- 사용 편의성과 기능 동작을 우선하고 서비스 목적에 부합하는 UI/UX 설계 필요
- 사용기관의 특성(긴급 상황 대응, 현장 출동 빈도, 근무지 환경)에 따라 '평시 모드', '재난 시 모드'로 구분하여 화면 구성 가능

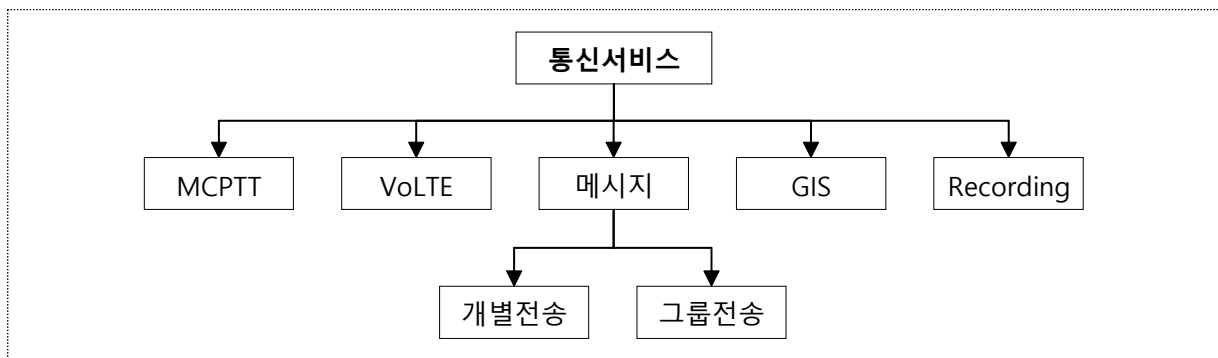
예) 재난 시 모드: 인증 절차 간소화, 필수기능 위주로 메뉴, 아이콘 구성

→ 긴급 상황에서 앱의 사용성과 상황 대응력의 향상 가능

- 사용 환경이 모바일 단말 환경일 경우 화려하거나 많은 리소스를 사용하는 화면구성은 지양

→ 제한된 화면크기, 제한된 입력 수단을 고려하여 사용자 입력을 최소화하고, 자동완성 기능을 제공하는 등의 쉬운 사용 방법 제공

[그림 26] UI 메뉴 구조 예시



- 기능접근이 쉽도록 화면 구성이 직관적이어야 하며 메뉴 구조의 구성은 3단 이상을 지양
- 모바일 기기의 화면 해상도에 따라 호환성을 고려하여 사용자 인터페이스 설계
- 화면을 구성하는 데 색상, 글자체, 용어 사용 등에 있어서 일관성을 유지
- 모바일 웹의 경우 특정 브라우저에서만 동작하는 설계 방식은 지양
- 저작권이 확보된 이미지만 사용

## ③ 접근 권한

- 방송통신위원회의 '스마트폰 앱 접근 권한 개인정보보호 안내서' 지침 준수
- 불필요한 과도한 권한 요청은 금지하며 사용되는 권한과 목적에 대해서 사용자가 인지할 수 있는 수단 제공

예) 설치 시 팝업 형태로 안내, 사용자가 선택하여 확인 가능한 메뉴

## ④ 정보보호

- 기능 동작에 필수적인 정보가 아닌 것은 요청하거나 저장 금지
- 인증정보와 같은 중요한 정보를 저장할 때는 암호화하여 저장

- 하드코딩 된 암호화키나 Base 64와 같은 단순 인코딩은 사용금지
  - 중요한 정보를 전송할 때는 해당 정보를 암호화하여 전송하거나 암호 통신 프로토콜을 이용한 신뢰된 채널을 이용하여 전송
- ⑤ 국정원 보안적합성 인증
- 개발단계에서부터 국가·공공기관의 도입을 위한 국정원 보안적합성 인증을 고려하여 개발
- ⑥ 보안 소프트웨어 연동
- 악의적인 외부의 공격이나, 사용자의 실수로 정보가 유출되는 것을 방지하기 위하여 보안 소프트웨어(백신, MDM 등) 연동
  - 앱 최초 실행 시, 앱 사용 중 주기적으로 보안 소프트웨어 동작 여부 확인
  - 보안 소프트웨어의 비정상 동작이 감지되면 즉시 앱 사용 중지 기능 제공
  - 보안 소프트웨어의 최신 버전으로 유지할 수 있는 방법 제공
- 예) 보안 소프트웨어가 최신 버전이 아닐 경우 사용기능의 제약을 발생
- MDM은 일괄적으로 모든 사용기관의 사용자에게 동일 정책 적용 지양
  - 사용기관의 특성, 요구되는 보안 수준의 차이에 따라 차등적으로 MDM 정책 적용 권장
- ⑦ 운영체제 변조 대응
- 보안취약점이 발생할 수 있는 운영체제 변조 탐지기능
  - 운영체제 변조 발생 시 정보보호 수단 제공
- 감사기록 생성 및 운영 서버 통보, 내부 저장데이터 삭제 및 초기화
- ⑧ 분실상황 대응
- 단말기의 분실, 도난 등의 사고 발생 시 대응할 수 있는 원격 통제 수단 제공
- 로그아웃 또는 앱 초기화, 앱 잠금, 저장자료 삭제 등
- ⑨ 리소스 사용
- 단말기의 과도한 전력 소모하게 하거나 불필요한 네트워크 접속 및 데이터 전송 금지
  - 상황에 따라 전송 데이터(영상, 음성)의 품질(크기)을 자동/수동으로 조절할 수 있다면 제한된 네트워크 자원을 더 효율적으로 이용 가능
- ⑩ 업데이트
- 앱을 수정하거나 추가 요구기능 개발에 대한 업데이트
  - 단말기 펌웨어나 OS 업데이트 이후 호환성을 위한 적극적인 지원
  - 업데이트 개발 완료 후 앱스토어 등록 전 검증

- 재난안전통신망과 연동하여 서비스를 제공하는 응용서비스는 서비스의 안전성 및 신뢰성을 확보하기 위하여 아래 [표 28~33]을 기준으로 소스코드를 점검

[표 28] 입력데이터

번호	보안약점	설명
1	SQL삽입	검증되지 않은 외부 입력값이 SQL 쿼리문 생성에 사용되어 악의적인 쿼리가 실행될 수 있는 보안약점
2	크로스사이트 스크립트	검증되지 않은 외부 입력값에 의해 사용자 브라우저에서 악의적인 스크립트가 실행될 수 있는 보안약점
3	운영체제 명령어 삽입	검증되지 않은 외부 입력값이 운영체제 명령어 생성에 사용되어 악의적인 명령어가 실행될 수 있는 보안 약점
4	오버플로우 (정수형, 메모리 버퍼)	정수값 및 메모리 버퍼의 경계값이 범위를 넘어서는 경우, 프로그램이 예기치 않게 동작될 수 있는 보안약점
5	입력값 유효성	지정된 길이 초과, 악성코드 포함 등 검증

[표 29] 에러처리

번호	보안약점	설명
1	오류 메시지 및 시스템 데이터 정보노출	사용자가 볼 수 있는 오류 메시지나 스택 정보에 시스템 내부 데이터나 디버깅 관련 정보가 공개되는 보안약점
2	오류 상황 대응 부재	시스템에서 발생하는 오류상황을 처리하지 않아 프로그램 실행정지 등 의도하지 않은 상황이 발생할 수 있는 보안약점
3	부적절한 예외 처리	예외에 대한 부적절한 처리로 인해 의도하지 않은 상황이 발생될 수 있는 보안약점

[표 30] 코드오류

번호	보안약점	설명
1	Null Pointer 역참조	Null로 설정된 변수의 주소값을 참조했을 때 발생하는 보안 약점
2	부적절한 자원 해제	사용된 자원을 적절히 해제 하지 않으면 자원 누수 등이 발생하고, 자원이 부족하여 새로운 입력을 처리할 수 없게 되는 보안 약점

[표 31] API 오용

번호	보안약점	설명
1	취약한 API 사용	취약하다고 알려진 함수를 사용함으로써 예기치 않은 보안 위협에 노출될 수 있는 보안약점

[표 32] 모바일 환경 특화

번호	보안약점	설명
1	안드로이드 등 애플리케이션 컴포넌트의 부적절한 접근 허용	안드로이드 등 애플리케이션 컴포넌트 설정으로 부적절한 접근이 허용되어 외부의 애플리케이션에 의해 의도치 않게 실행될 수 있는 보안약점
2	민감한 정보 전송을 위한 암시적 intent사용	암시적 intent를 사용하여 민감한 정보가 전송시 도청, 악성 코드 및 이상 행위를 위한 접근이 가능한 보안약점
3	접근제어 없이 내·외부 저장소 사용	내·외부저장소(SD카드 등)에 중요한 정보를 암호화하여 저장하지 않아 정보가 노출되거나 수정이 가능한 보안약점
4	안드로이드 등의 권한 검사 우회	권한이 전혀 없는 호출 프로그램이 응용 프로그램의 권한을 사용하게 되어 권한 검사를 우회할 수 있는 보안약점
5	클래스 로딩 하이재킹	프로그램의 클래스 로드 시 검색되는 디렉토리의 이름이 변경되어 클래스 경로를 공격자가 명시적으로 제어할 수 있는 보안약점
6	소스코드 난독화 미적용	역공학 기술에 의한 소스코드 유출 및 보안메커니즘 우회 등이 발생할 수 있는 보안약점

[표 33] 기능 보안취약점 기준

번호	항목	세부점검내용
1	임의기능	명세되지 않은 기능 존재 여부
		악성행위 기능 존재 여부 (불법 녹음, 임의 데이터 전송, 임의로 위치정보 수집·전송 등)
2	최소권한	동일한 개인키로 서명된 다른 앱과 UID 공유 여부(Android)
		기능사용 요청 권한과 기능사용 여부 적절성 여부(Android)
3	중요정보 관리	사용자 인증 방법의 적절성 유무
		비밀번호 조합규칙(영문·숫자·특수문자 등 조합)
4	플랫폼 보안모델	루팅, 탈옥 등과 같은 플랫폼 변조 기능 존재 여부
		플랫폼에서 제공하는 보안기능 사용의 적절성 여부
5	상용/공개용 모듈	상용 또는 공개모듈 사용 목적 및 기능의 적절성 여부
		해당 모듈에 대한 개발업체의 안전성 확인 방법 및 결과의 적절성 여부
6	공개영역 취약점	모바일 플랫폼(예, 안드로이드, iOS, 윈도우모바일 등) 등에 대해 알려진(및 신규) 취약점 존재 여부

[표 34] 보안기능

번호	보안약점	설명
1	취약한 암호화 알고리즘 사용	중요정보(금융정보, 개인정보, 인증정보 등)의 기밀성을 보장할 수 없는 취약한 암호화 알고리즘을 사용하여 정보가 노출될 수 있는 보안 약점
2	중요정보 평문저장	중요정보(비밀번호, 개인정보 등)를 암호화하여 저장하지 않아 정보가 노출될 수 있는 보안 약점
3	중요정보 평문전송	중요정보(비밀번호, 개인정보 등) 전송시 암호화하지 않거나 안전한 통신채널을 이용하지 않아 정보가 노출될 수 있는 보안 약점
4	하드코드된 비밀번호	소스코드내에 비밀번호가 하드코딩되어 소스코드 유출시 노출 우려 및 주기적 변경 등 수정(관리자 변경 등)이 용이하지 않는 보안 약점
5	충분하지 않은 키 길이 사용	데이터의 기밀성, 무결성 보장을 위해 사용되는 키의 길이가 충분하지 않아 기밀정보 누출, 무결성이 깨지는 보안 약점
6	적절하지 않은 난수 값 사용	예측 가능한 난수사용으로 공격자로 하여금 다음 숫자 등을 예상하여 시스템 공격이 가능한 보안 약점
7	하드코드된 암호화 키	소스코드내에 암호화키가 하드코딩되어 소스코드 유출시 노출 우려 및 키 변경이 용이하지 않는 보안 약점
8	주석문 안에 포함된 시스템 주요정보	소스코드 내의 주석문에 인증정보 등 시스템 주요정보가 포함되어 소스코드 유출 시 노출될 수 있는 보안 약점



#### 4.3.3.3. 보안적합성 검증

- 국가정보원의 보안적합성 검증을 통한 응용서비스의 안전성을 검증
  - 개발업체는 개발중인 응용서비스를 사용기관에 도입하기 위하여 국가정보원의 보안적합성 검증\*을 수행하여 안전성을 사전에 확보
  - 국정원의 보안 사전인증이 필요한 제품은 CC인증 및 보안기능확인서를 확보

[그림 27] 보안적합성 검증 절차



\* 보안적합성 검증은 국가정보원 홈페이지의 보안적합성 검증([https://www.nis.go.kr:4016/AF/1\\_7\\_2\\_1.do](https://www.nis.go.kr:4016/AF/1_7_2_1.do))을 참조하여 수행

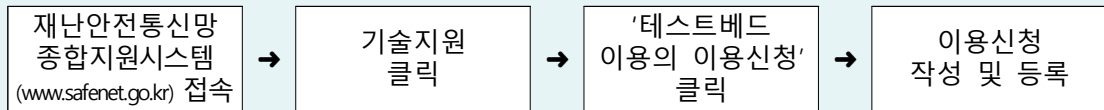
#### 4.3.3.4. 기술지원(테스트베드 사용) 요청

- 시험환경, 장비, 계측기 및 차폐실이 마련된 재난안전통신망 테스트베드는 서울, 대구, 대전 총 3개소로 운영
- 사용기관/개발업체는 서비스 개발 시 테스트베드 활용이 필요한 경우에 재난안전통신망 종합지원시스템([www.safenet.go.kr](http://www.safenet.go.kr))을 통해 사용을 신청하여 무료로 이용 가능
  - ※ 신청기관 및 개발업체에서 처음으로 기술지원 및 시험검증 신청을 하기 위해서는 기관별로 담당자를 지정하여 회원가입을 진행
- 사용기관/개발업체가 테스트베드를 활용하여 서비스를 개발할 때 한국지능정보사회진흥원에 기술지원 요청이 가능



## 테스트베드 이용신청 및 기술지원 내용

### ▶ 테스트베드 이용신청 절차



### ▶ 테스트베드 이용신청 작성 방법

**이용신청**

**기본사항**

*신청기관명 (신청서 표기 대상)	테스트 test		
*주소	06934	유리변호장기	테스트
*이름(담당자)	테스트	직위	
*연락처	010	1234	1234
*이메일	test	@naver.com	
*과제명(연구내용)			

**신청구분**

\*신청구분 ☐ 기존 ☐ 신규

☐ 테스트베드 이용 ☐ 기술지원(기술/서비스시험) ☐ 기술검증 ☐ 기타

**세부 신청내용**

\*이용장소 ☐ 서울 ☐ 대구 ☐ 대전

\*이용일시 0000-00-00 ~ 0000-00-00

\*이용자

\*목적

\*내용

\*검토사항

☐ 재난안전통신망 활용 서비스 개발 및 이용 등을 위한 테스트베드 이용신청서를 제출하여, 관련 자료 제출 및 보안 관리에 착각적으로 협조하겠습니다.

**Annotations:**

- 로그인 정보로 신청 시 자동 선택
- 관련 과제명 또는 연구내용을 기술
- 기존 또는 신규 클릭
  - 기존 : 사용 경험 有
  - 신규 : 사용 경험 無
- 4개의 항목 중 하나를 클릭
  - 테스트베드 이용 : 단순 테스트 베드 이용 시
  - 기술지원 : 연구개발을 위한 테스트베드 이용 시
  - 기술검증 : 시험검증을 위한 테스트베드 이용 시
  - 기타 : 그 외의 경우
- 이용하고자 하는 테스트베드 위치 클릭
- 테스트베드 이용일자 선택
- 테스트베드 실제 이용 인력 성명 입력
- 테스트베드를 이용하는 목적 입력
- 상세 테스트베드 이용내용 입력
- 테스트베드 이용과 관련 요청사항 입력
- 테스트베드 이용 관련 협조 체크

### ▶ 테스트베드 검증 기술지원 항목

- ✓ 소스코드 취약점 점검
- ✓ 서비스 검증항목 적정성 검토
- ✓ 서비스 검증방안 적정성 검토 등

※ 테스트베드 이용 관련 사항은 [www.safenet.go.kr](http://www.safenet.go.kr) 참고

#### 4.3.3.5. 개발 진도관리

- 사용기관은 서비스 개발 시 행정안전부 재난안전통신망과와 수시로 개발 관련 현안에 대하여 협의하여 최종적으로 서비스 개발을 완료

## 4.4. 구축 단계

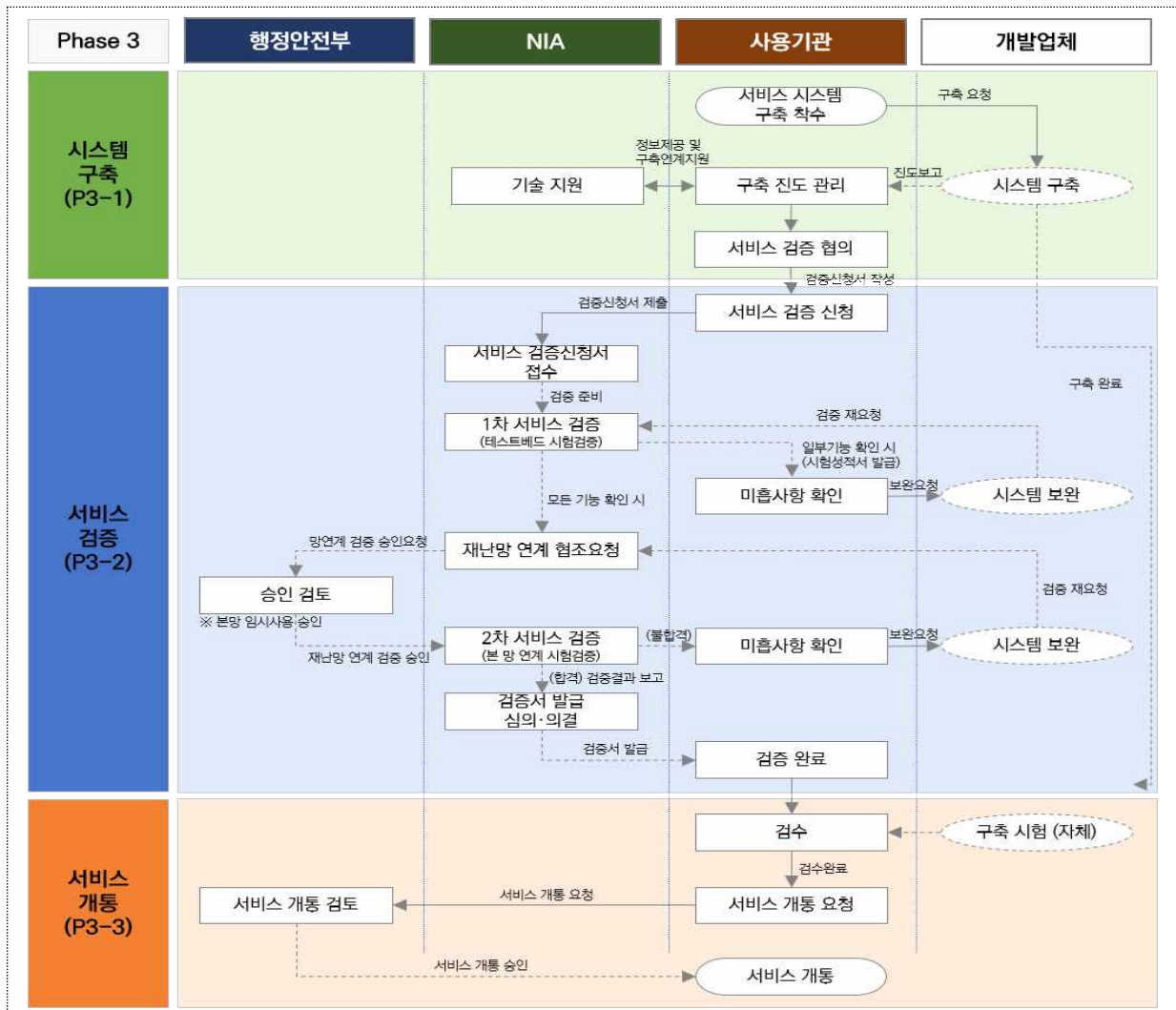
응용서비스 시스템을 구축하고 1~2차 시험·검증을 통해 검증 완료 후 행정안전부의 승인을 통해 서비스를 개통하는 단계

### 4.4.1. (Phase 3) 구축 단계 업무흐름도

○ 응용서비스의 개발 단계는 시스템 구축, 서비스 검증 및 서비스 개통, 총 3단계로 구성

- (P3-1 시스템 구축) 사용기관이 개발업체를 통해 응용서비스 시스템을 구축
- (P3-2 서비스 검증) 사용기관이 구축된 응용서비스에 대하여 한국지능정보사회진흥원을 통해 1~2차 시험·검증을 받는 단계
- (P3-3 서비스 개통) 검수 완료 후 행정안전부에 공문으로 서비스 개통을 요청

[그림 28] 응용서비스 구축 단계 업무흐름도



## 4.4.2. (P3-1) 시스템 구축

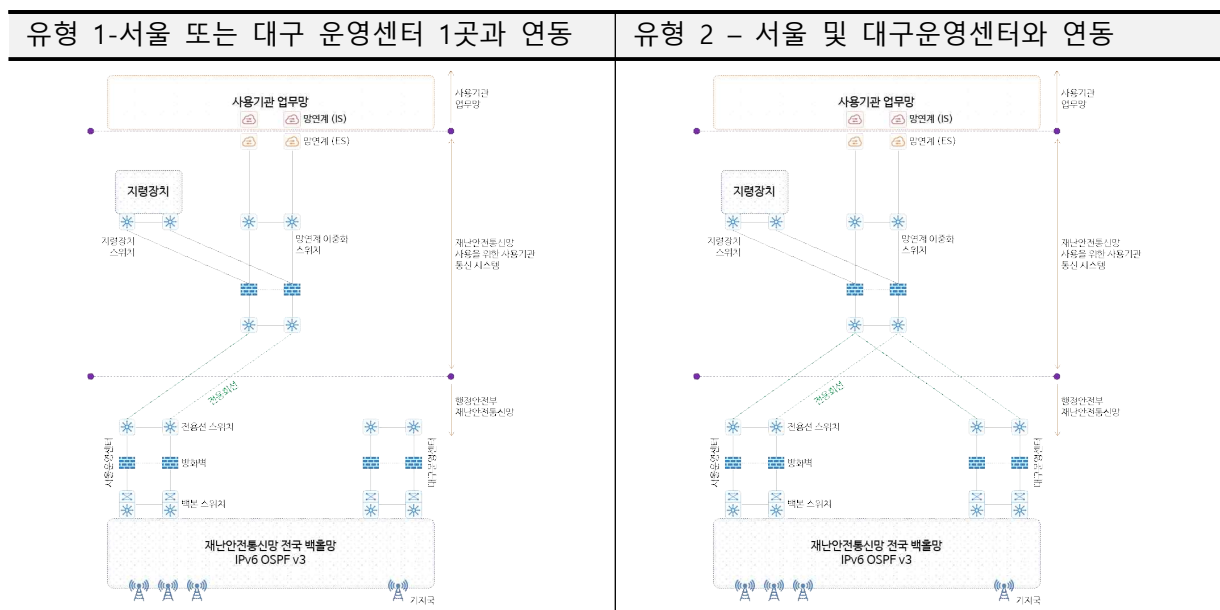
### 4.4.2.1. 시스템 구축

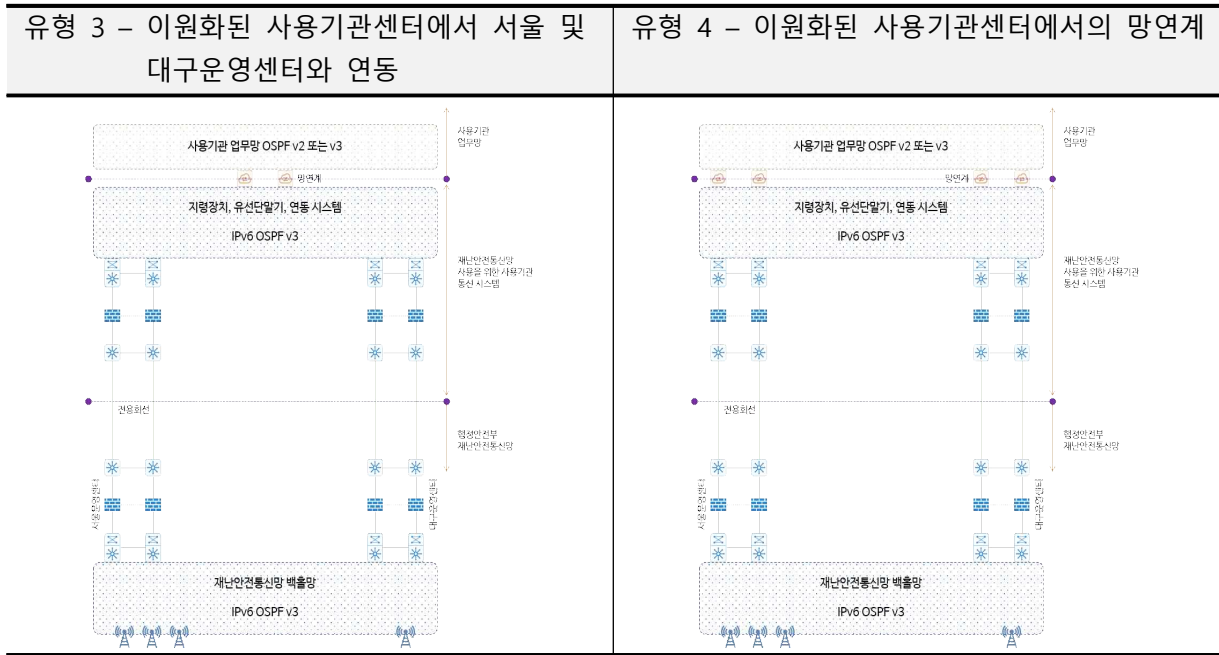
- 사용기관은 개발된 응용서비스 이용을 위하여 개발업체를 활용하여 응용서비스를 위한 시스템 구축을 진행
- 사용기관과 개발업체는 재난안전통신망 기반의 서비스 활용을 위하여 시스템 구축 시 재난안전통신망과의 연동을 위한 고려사항을 반영하여 구축

### 4.4.2.2. 재난안전통신망 연동 시 고려사항

- 사용기관은 기술 및 장비를 검토하고 재난안전통신망 연동에 적합한 장비를 구비하여 구축
  - ※ 연동부분은 행정안전부 재난안전통신망과와 사전협의 된 사항에 대해서만 연동이 가능
- 재난안전통신망과의 상세한 연동 방안에 대해서는 한국지능정보사회진흥원에 지원을 요청
  - ※ 상세 연동 방안은 【붙임 5】 재난안전통신망 연동 방안 참조
- (전용회선 연동) 사용기관이 재난안전통신망과의 전용회선 연동 방식은 사용기관의 연동유형에 따라 총 4개의 방식으로 연동이 가능

[그림 29] 사용기관 유형별 회선연동 방식

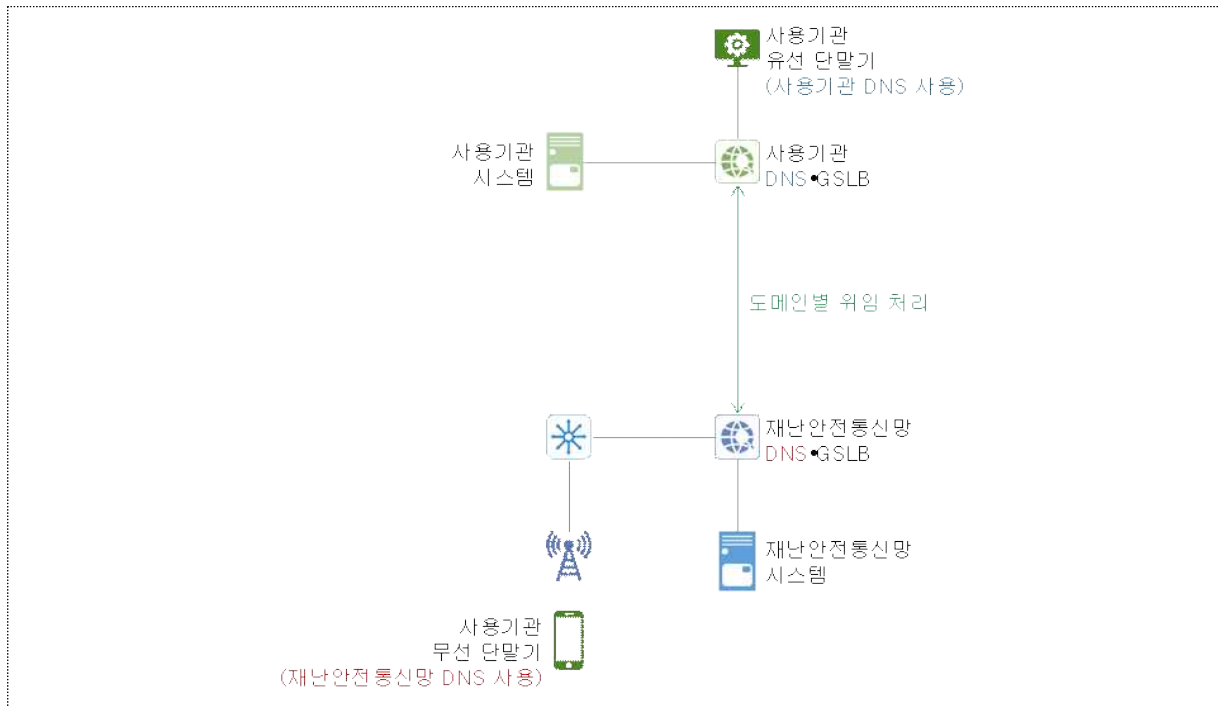




- ※ 실 서비스 운영/제공 시 전용선 구축/임차 관련 GNS 참고하여 비용확인 후 활용
- ※ 서비스 테스트를 위한 테스트베드와 연계는 KOREN 회선 활용 가능

- (DNS·GSLB 연동) DNS(Domain Name System) 및 부하분산과 단위 장애 시 가용성 보장을 위한 GSLB(Global Server Load Balancing)<sup>1)</sup>의 연동 구성도는 아래 [그림 30]과 같으며 재난망 DNS서버 이용 또는 사용기관 DNS서버 연동이 가능

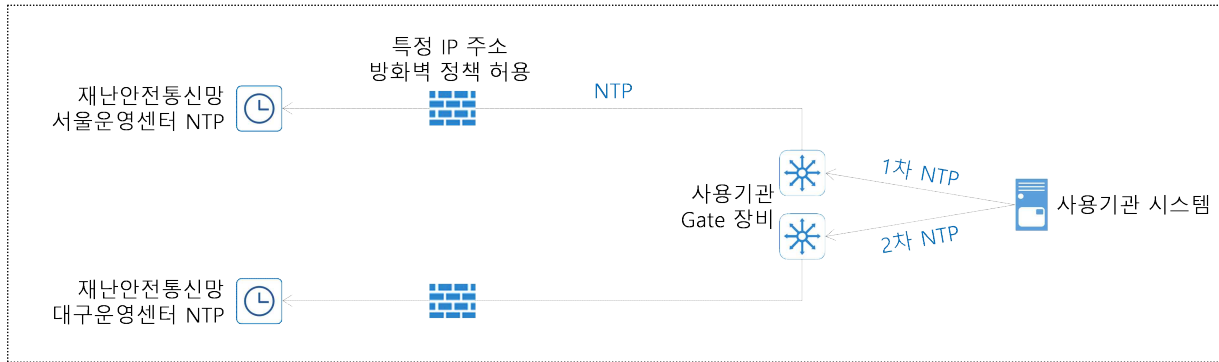
[그림 30] DNS·GSLB 연동 구성도



1) GSLB : 지능적 DNS 서비스로 DNS와 같이 동작하며, health check와 active/backup을 지정 가능하게 하여 재해복구(DR), 지역적 부하분산, 응답시간 중심의 서비스 제공이 가능

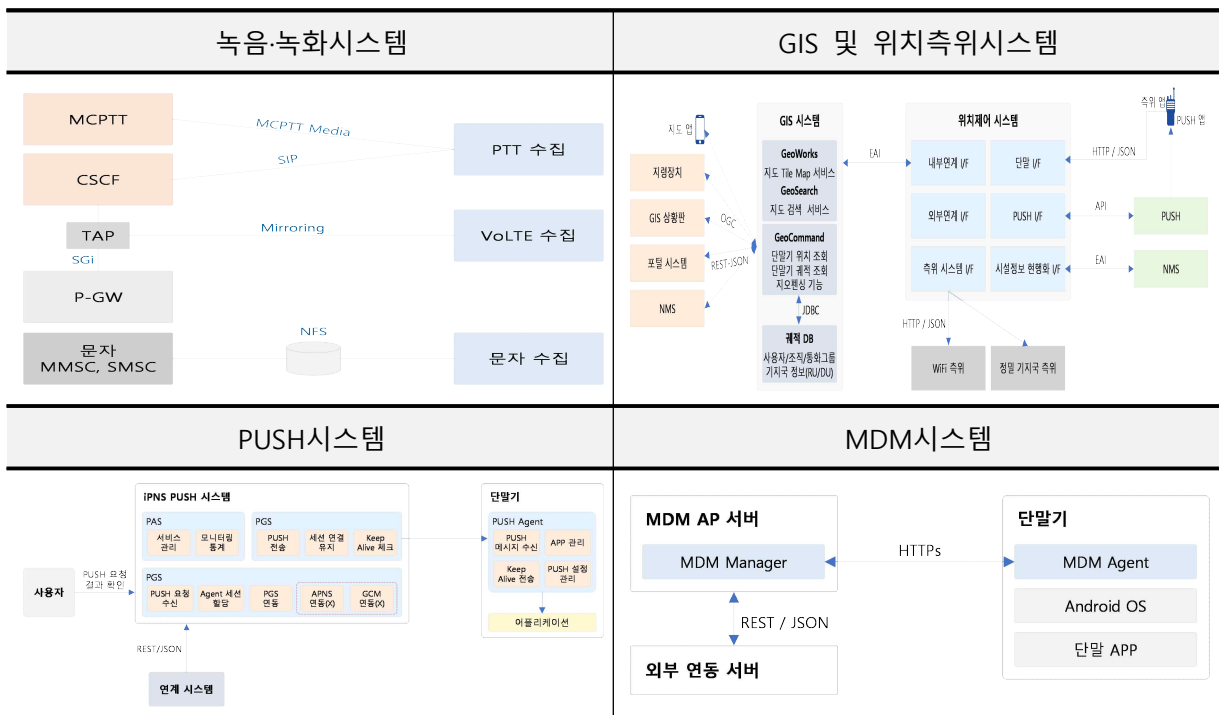
- (NTP·PTP 연동) 사용기관 시스템과 재난안전통신망 운영센터의 시간 동기화를 위해 NTP(Network Time Protocol)와 클럭 동기화 프로토콜인 PTP(Precision Time Protocol) 연동이 가능하며, NTP 연동 구성도는 아래 [그림 31]과 같으며, 재난망 NTP서버 또는 사용기관 NTP서버의 이용이 가능

[그림 31] NTP 연동 구성도



- (어플리케이션 연동) 단말기 기반 앱 서비스인 녹음·녹화 시스템, GIS 및 위치측위 시스템, PUSH 시스템 그리고 MDM 시스템 어플리케이션 연동은 아래 [그림 32]와 같이 인터페이스 구조로 연동이 가능

[그림 32] 시스템별 인터페이스 구조



- 재난안전통신망 앱 개발 포털을 통하여 재난안전통신망에서 제공되는 인터페이스와 실제로 제공되는 API 목록 및 연동방식은 아래 [표 35]와 같음

[표 35] API와 인터페이스 방식

구분	API 명칭	인터페이스 방식	설명
MDM	분실단말 잠금 등록/해제 요청	REST API	- Request : 시스템 아이디, 인증키, 단말 아이디 유형, 단말 아이디, 액션 코드, 예약 전송 일시, 잠금 메시지, 추가 필드 - Response : 요청 일련번호, 결과 코드, 결과 메시지
	분실단말 잠금 등록/해제 요청결과 조회	REST API	- Request : 시스템 아이디, 인증키, 요청 일련번호 - Response : 결과 코드, 결과 메시지, 요청 상태 정보, 처리 일시, 추가 필드
	단말 잠금 상태 조회	REST API	- Request : 시스템 아이디, 인증키, 단말 아이디 유형, 단말 아이디 - Response : 결과 코드, 결과 메시지, 단말 상태 코드, 추가 필드
BSS	단말 상태 통계	DBtoDB (Batch)	- Request : GUID, 집계일시, 조직 ID, 제조사 코드, 단말기 유형코드, 단말기 모델명, 상태코드, 단말기 수 - Response : GUID, 집계일시, 조직 ID, 제조사코드, 단말기유형코드, 단말기모델명, 상태코드, 단말기수
	사용자 개통 정보 연동	DBtoDB (Batch)	- Request : GUID, 집계일자, 조직 ID, 서비스 유형, 서비스그룹 코드, 서비스 ID, 단위 코드, 사용량, 금액 - Response : GUID, 집계 일자, 조직 ID, 서비스 유형, 서비스그룹 코드, 서비스 ID, 단위 코드, 사용량, 금액
IAM	조직정보 연동	DBtoDB	재난안전통신망 조직정보
	계정정보, 계정- 역할정보 연동	DBtoDB	계정 정보, 계정별 역할 정보
CSC	인증정보	XCAP	Authentication 데이터 정의 Token 데이터 정의
	그룹정보	XCAP	Access token, MCPTT ID, 콘텐츠 변경 여부를 판별하는 다이제스트 값, Group 정보
	서비스설정정보	XCAP	Access token, MCPTT ID, 콘텐츠 변경 여부를 판별하는 다이제스트 값, Service 정보
	Key정보	XCAP	Access token, MCPTT ID, Uri, key 정보
HSS	사용자 Profile 정보	SOAP	사용자 Profile 정보
GIS	지도맵 정보	REST/JSON	지도맵 이미지
	위치검색정보	REST/JSON	검색된 위치데이터
	위치 및 경로 정보	REST/JSON	단말기 위치 데이터, 기지국 위치 데이터, 단말기 위치 경로 데이터
	지오펜스 정보	REST/JSON	행정구역별 지오펜스 데이터
녹취서버	녹취서버 웹화면 접속 요청	REST/JSON	녹취서버 웹화면

구분	API 명칭	인터페이스 방식	설명
FOTA	단말 버전 정보 연동	REST/JSON	- Request : imei, msisdh, fwVer - Response : imei, msisdh, fwVer
NMS	CORE 시스템 알람 정보 연동	REST/JSON	- Request : systemid, alarmtime, alarmstatus, alarmcode, perceivedseverity, alarmname, networkelement, location, eventtype, probablecause, specificproblem, additionaltext, notificationid - Response : systemid, alarmtime, alarmstatus, alarmcode, perceivedseverity, alarmname, networkelement, location, eventtype, probablecause, specificproblem, additionaltext, notificationid

[표 36] 연동대상과 연동방식

연동대상	연동방식	프로토콜	연동 인터페이스
MDM	REST/JSON	HTTP	분실 단말 잠금 등록/해제 요청 분실 단말 잠금 등록/해제 요청결과 조회 단말 잠금 상태 조회
BSS	DBtoDB	HTTP	단말 상태 통계 사용자 개통정보 연동
IAM	DBtoDB	TCP/IP	조직정보 연동 계정정보, 계정-역할정보 연동
CSC	XCAP	HTTP	인증정보 그룹정보 서비스 설정정보 Key정보
HSS	SOAP	HTTP	사용자 Profile 정보 연동
GIS	REST/JSON	HTTP	지도맵 정보 위치검색정보 위치 및 경로 정보 지오펜스 정보
녹취 서버	REST/JSON	HTTP	녹취서버 웹화면 접속 요청
FOTA	REST/JSON	sFTP	단말 버전 정보 연동
NMS	REST/JSON	HTTP	CORE 시스템 알람 정보 연동

## 참고사항

- ◇ 본 가이드라인에 제시된 방법 외 다른 연동이 필요한 경우에는 사용기관에서 개발이 필요
- ◇ 재난안전통신망 개발자 포털의 API는 [부록 I] 참조

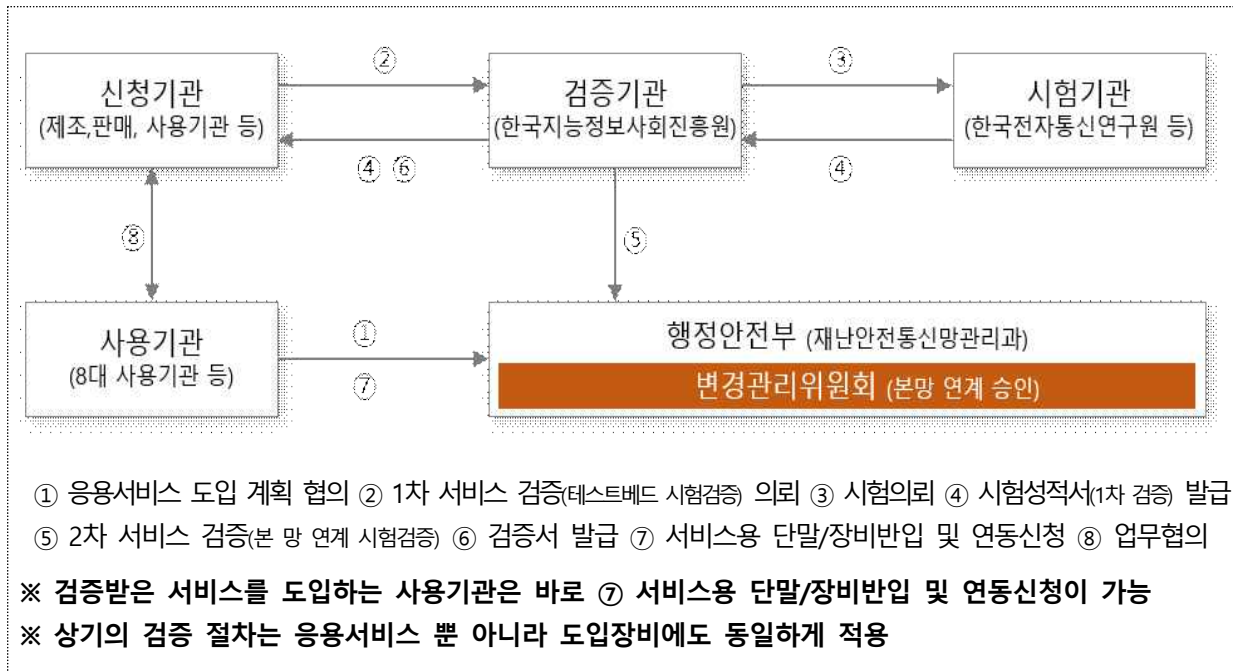


### 4.4.3. (P3-2) 서비스 검증

#### 4.4.3.1. 서비스 검증 신청

- 사용기관의 응용서비스 및 관련 장비 도입을 위해서는 신청기관이 검증기관인 한국지능정보사회진흥원에 서비스 검증을 의뢰하여 검증서를 발급

[그림 33] 응용서비스 검증 절차



※ 검증 비용은 사용기관 부담이 원칙이나 행정안전부장관이 필요하다고 인정하는 경우에는 예산 범위 내에서 지원 또는 부담 (재난안전통신망 운영 및 사용에 관한 규정「제3장 제28조 사용 장비 등 도입」 참조)

- 서비스 검증은 총 2단계로 기능 위주의 검증인 1차 시험(시험망)과 재난안전통신망 연계를 통한 검증인 2차 검증(본 망)으로 구성

- 1차 시험(시험망) 신청은 신청기관이 재난안전통신망 종합지원시스템([www.safenet.go.kr](http://www.safenet.go.kr))에 접속하여 시험검증신청서를 작성하여 접수

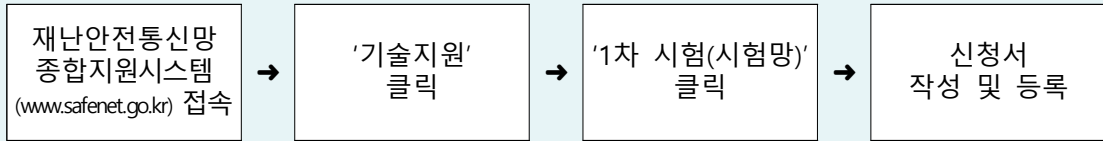
※ 처음으로 신청기관에서 시험검증 신청을 하기 위해서는 기관별로 담당자를 지정하여 회원가입을 진행

- 신청기관은 검증을 위한 검증범위 및 내용, 방법, 일정 등에 대한 검증계획을 수립하고, 검증환경 구성 방안 수립 및 검증환경을 시험기관과 함께 구성



## 서비스 시험검증(1차) 신청 및 결과확인 방법

### ▶ 서비스 시험검증 신청 절차



### ▶ 서비스 시험검증 신청 작성 방법

**시험검증신청**

**기본사항**

*신청기관명 (공영서 표기 대상)	테스트	test
*주소	06934	우편번호 서울특별시 동작구 동자동4길 58
*이름(담당자)	테스트	직위
*연락처	010	1234
*이메일	test	@naver.com

로그인 정보로 신청 시 자동 생성

**신청내용**

품목(기기/장비/서비스)	제조사	규격/모델명	세부사항(ow, Wer, 등)

시험검증 신청 품목 / 제조사 / 규격 / 모델명 / 사양 등 입력

**기술검증 신청**

기기/장비 기술검증

☐ 단말 ☐ 지령장치 ☐ IoT 단말

☐ 기타 기기/장비

☐ 증명서 신규 발행 ☐ 증명서 재발행

☐ 검증 마크(스티커)

\* 검증 마크 제작비(선택)는 신청기관 부담

서비스 기술검증

☐ 단말 기반 APP ☐ 재난안전통신망 기반 응용서비스

☐ 기타 서비스

기기/장비 기술검증과 서비스 기술검증 중 서비스 기술검증 부분을 체크

검증하고자 하는 항목 체크

**증명서/시험성적서 수령**

\*발행 희망일

0000-00-00

\*수령방법

☐ 직접수령 ☐ 택배 ☐ 우편 ☐ 기타

증명서/시험성적서 수령방법 체크

취소 등록

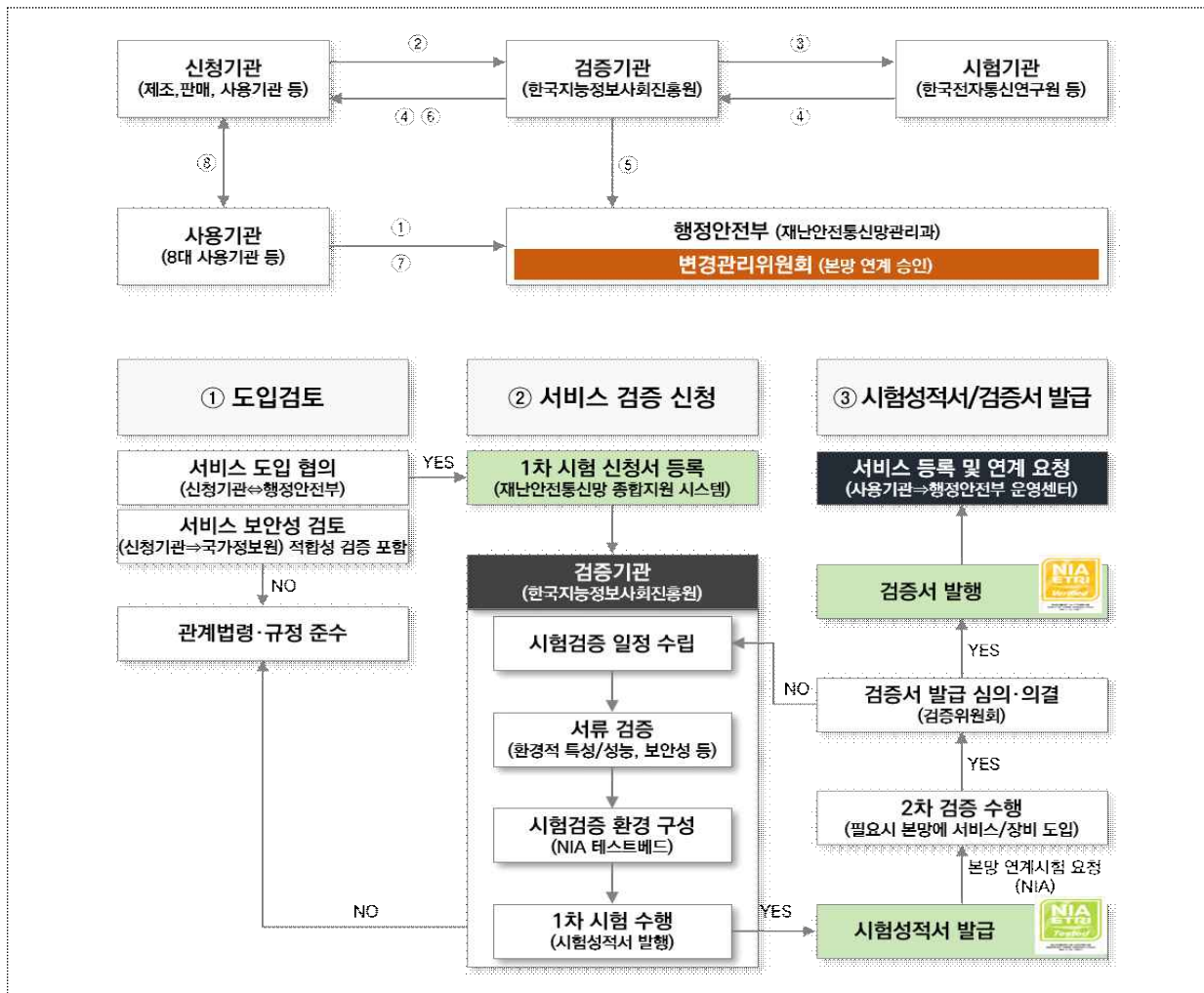
### ▶ 시험성적서/검증서 확인 방법



※ 시험항목 중 재난안전통신망 이용을 위해 필수적으로 요구되는 기능은 반드시 적합해야 하며, 부적합한 항목에 대해서는 조치 후 재시험 시행

- 2차 검증(본 망)은 검증기관인 한국지능정보사회진흥원에서 행정안전부에 본 망 연계 협조를 요청하여 변경관리위원회의 승인을 득한 후 검증을 수행
  - 2차 검증(본 망)을 위한 검증방법에 대해서는 사전에 검증기관 및 시험기관과 협의가 필요
  - ※ 2차 검증을 위해서는 1차 시험에서 모든 항목 적합 판정 필요
  - ※ 재난안전통신망 환경 적용 시 특이사항이 발견된 경우 지원기관은 사용(신청)기관에 추가 자료 및 조치 등을 요청할 수 있음
  - 2차 검증(본 망)에서 모든 항목이 합격한 서비스의 경우 검증위원회를 거쳐 검증서를 발급
- 1차 시험(시험망)과 2차 검증(본 망) 총 2단계 시험검증을 통해 발급되는 시험 성적서 및 검증서의 상세한 발급절차는 아래 [그림 34]와 같음

[그림 34] 시험성적서 및 검증서 발급 절차





## 서비스 검증 대상 및 항목

### ▶ 서비스 검증 대상 및 적용 범위

- ✓ 대상 : 서비스 제공 플랫폼, 단말기 기반 서비스
- ✓ 범위 : 상호운용성, 보안성, 망 적합성



### ▶ 서비스 시험검증 항목

구분	서비스 제공 플랫폼		단말기 기반 서비스	
설정관리	접속관리	5/17항목	앱관리	3/10항목
운영관리	기능관리	3/17항목	기능관리	3/10항목
	연동관리	1/17항목	패키지관리	1/10항목
	패키지관리	2/17항목		
보안성	시큐어코딩	1/17항목	시큐어코딩	1/10항목
	접근제어	5/17항목	접근제어	2/10항목

- ※ 시험항목은 서비스 성격 등에 따라 일부 변동 가능
- ※ 시험/검증 신청 시 국가정보원 보안성 검토 결과 제출 필요

### ▶ 단말기 및 지령장치 시험검증 항목

구분	요구기능	세부기능	항목수
단말기	재난대응성	개별통화, 통화그룹편성, 그룹통화, 지역선택 호출, 긴급통화, 단말위치확인, 주변청취, 복수통화 그룹수신	31/78
	생존.신뢰성	단말이동성	8/78
	보안성	단말제어, 암호화	6/78
	상호운용성	호연결	3/78
	운영.효율성	상황전파메시지, 다자간이중통화, 데이터통신, 녹음/녹화, 발신번호표시, 통화용량확장, 공동통화그룹, 단말등록, 버전갱신, 기본 앱	30/78
지령장치	재난대응성	개별통화, 통화그룹편성, 그룹통화, 지역선택 호출, 긴급통화, 단말위치확인, 주변청취, 복수통화 그룹수신	31/55
	보안성	단말제어, 암호화	5/55
	상호운용성	호연결	2/55
	운영.효율성	상황전파메시지, 다자간이중통화, 데이터통신, 녹음/녹화, 발신번호표시, 통화용량확장, 공동통화그룹	17/55

- ※ 재난안전통신망 지령장치 기본 서비스 시험규격 (TTAK.KO-06.0553/R1, 2022.12.07.)
- ※ 재난안전통신망 단말기의 기본 서비스 시험규격 (TTAK.KO-06.0525/R1, 2022.12.07.)

## 4.4.4. (P3-3) 서비스 개통

## 4.4.4.1. 서비스 개통 절차

- 사용기관은 서비스 개통을 위해 재난안전통신망 운영센터로 서비스 개통을 신청
  - 사용기관은 등록연계신청서를 공문 형식으로 작성·발송하여 서비스 개통을 신청
  - ※ 등록연계신청서는 【붙임 6】 양식을 참조하고 신청 시 검증서와 사용계획서를 첨부하여 제출
- 행정안전부의 서비스 개통이 승인되면 사용기관 또는 개발사는 앱스토어에 등록하고자 하는 서비스(앱)의 기본 등록정보, 성적서와 검증서를 첨부하여 앱스토어 등록을 신청
  - ※ 재난안전통신망 앱스토어에 접속, 등록, 조회와 관련된 내용은 [부록 H] 재난안전통신망 앱스토어 사용자 매뉴얼을 참조

[표 37] 서비스(앱) 기본 등록정보

항목		세부 내용	비고
설치 정보	서비스(앱) 이름	서비스 이름을 입력	-
	지원 OS	지원하는 OS 정보를 입력	-
	필수 설치 여부	앱 설치 필수 여부 선택	-
버전 정보	버전 정보	앱의 버전 정보	-
	버전 설명	앱의 버전 정보에 대한 설명	-
	필수 업데이트	앱이 업데이트 필수 여부 선택	-
	설치 파일(APK)	설치 파일 이름	-
	패키지명	앱의 패키지명	-
	실행 아이콘	앱스토어에 표시될 실행 아이콘	파일 확장자: PNG 크기: 192 x 192
상세 보기	앱 소개	앱의 기능에 대한 설명	2,000자 이내
	앱 스크린	앱의 기능을 설명한 앱의 소개 화면 (4장)	파일 확장자: PNG 크기: 450 x 800

※ 서비스(앱) 등록 이후에도 사용성 개선을 위한 기능 개발, 사용자 요구기능 개발 및 보안 기능 업데이트 등 사후관리가 필요

- 서비스(앱)의 등록·배포 신청은 검증 단계를 포함하여 아래 표 38과 같은 단계로 이뤄지며 최종적으로 서비스(앱) 이용을 위해서는 행정안전부의 최종 배포 승인 후 사용자에게 배포 가능

[표 38] 앱 등록 및 배포

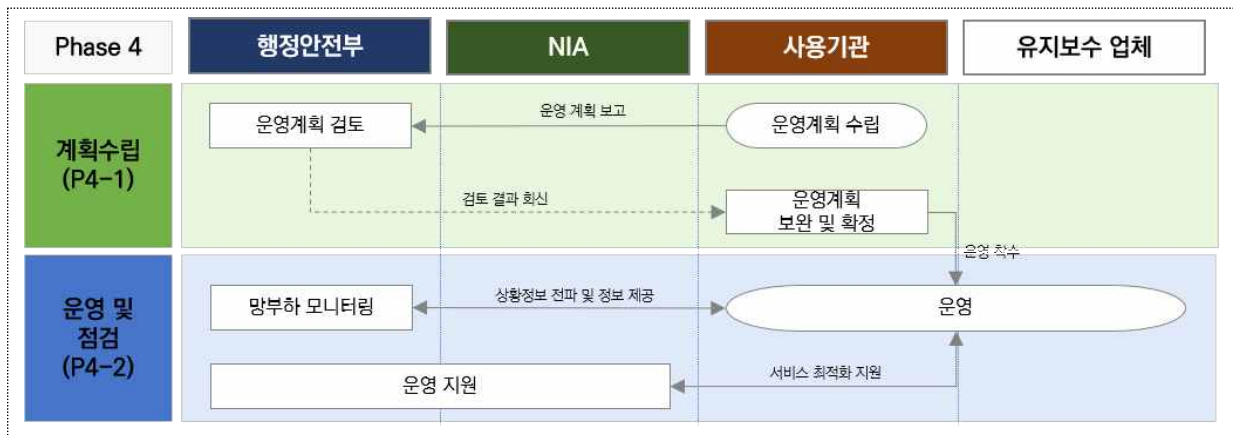
구 분	앱 등록자(사용기관)	운영자(운영센터)	관리자(행안부)	이용자(단말기)
프로세스	<pre> graph LR     A[앱 개발] --&gt; B[앱 기능 검증]     B --&gt; C[검증결과서 다운로드]     C --&gt; D[검증결과서 작성]     D --&gt; E[앱 사용 권한 설정]     E --&gt; F[앱 등록 승인 요청]     F --&gt; G[앱 검증 결과 확인]     G --&gt; H[1차 승인]     H --&gt; I[최종 배포 요청]     I --&gt; J[최종 배포 승인]     J --&gt; K[사용자 다운로드]     K --&gt; L[사용자 설치 및 이용]         </pre>			
설명	1) 사용기관은 앱을 개발하고, 앱 기능 및 성능에 대한 자체 검증을 수행 2) 재난안전통신망 종합지원시스템에서 제공하는 검증 결과서(시험성적서)를 다운 받아, 검증 수행 여부 기입 ※ 2차 검증이 완료되면 최종적으로 현장 이용자에게 배포하기 위해 검증서를 다운 받아 수행 여부 기입 3) 앱스토어를 통해 등록된 앱을 다운 및 사용할 수 있는 조직/사용자/단말 설정 4) 앱 등록과 함께 등록 승인 요청	1) 앱 검증이 정상적으로 수행되었는지 검증 결과서 확인 2) 앱 최종 등록(배포) 요청	1) 앱 검증 및 권한 설정 등 등록된 앱에 대한 최종 확인 후 배포 승인	1) 사용기관 이용자 앱 다운로드 및 설치/이용
To-Do	사용기관별 앱 검증(기능) 및 등록 담당자 필요	- 앱 검증 결과 검토자(운영자) 필요 - 앱 검증 결과서 양식 확정 필요	앱 최종 배포 승인자(관리자) 필요	N/A

## 4.5. 운영 단계

### 4.5.1. (Phase 4) 운영 단계 업무흐름도

- 응용서비스 운영 단계는 계획수립과 운영 및 점검, 총 2단계로 구성
  - (P4-1 계획수립) 사용기관이 서비스 운영을 위한 계획을 수립 및 확정
  - (P4-2 운영 및 점검) 사용기관이 서비스 이용에 따른 운영성과를 분석하고 향후 서비스 계속 운영 여부를 점검

[그림 35] 응용서비스 운영 단계 업무흐름도



### 4.5.2. (P4-1) 계획수립

- 사용기관은 사용기관의 특성을 반영하여 서비스의 운영계획(안)을 수립하여 행정안전부 재난안전통신망과와 협의를 거친 후 최종적으로 운영계획을 마련
  - 사용기관은 서비스 이용환경(이용자 수, 사용주기 등), 이용자 피드백 및 사용기관의 특성을 고려하여 운영계획(안)을 수립

### 4.5.3. (P4-2) 운영 및 점검

- 사용기관은 운영하는 재난안전 응용서비스를 정기 또는 수시로 점검 및 진단하여 미흡한 점을 개선 추진
  - 사용기관은 구축·운영하고 있는 응용서비스에 대하여 매년 운영성과를 측정하고 지속해서 관리

- 사용기관은 재난안전 응용서비스 중 보안에 취약한 서비스가 발견되는 경우 서비스는 즉시 중지하고, 개선 후 재배포를 통해 서비스 재개시

○ 재난안전통신망 운영센터에서는 재난안전 서비스의 운영·관리 및 유사·중복성에 관한 점검 및 진단을 시행

- 재난안전통신망 운영센터는 재난안전통신망의 효율적인 관리를 위하여 사용기관의 서비스 사용 및 운영 실태를 점검 및 확인이 가능

[표 39] 응용서비스의 운영 활동 수행 및 점검

절차	수행 내용
운영 및 사후관리	(사용기관) 로그 파일 분석, 사용자 정보 분석, 사용자 피드백 분석 등 수행 (행정안전부) 재난안전통신망 운영센터에서는 필요하면 재난안전 서비스의 운영·관리 및 유사·중복성에 관한 점검 및 진단을 시행

○ 행정안전부는 각 사용기관의 서비스 이용 확인점검 결과 서비스의 개선·변경 또는 폐기가 필요하다고 인정되는 경우 사용기관에 응용서비스의 정비 또는 폐기를 권고할 수 있으며, 각 사용기관에서는 특별한 사유가 없는 한 이를 수용

※ 응용서비스 업데이트, 정보시스템 교체 등 변동 사항이 있는 경우에는 기술 적합성 재검증 실시 여부에 대하여 행정안전부 재난안전통신망과와 사전협의

○ 행정안전부는 재난안전통신망의 효율적인 사용 및 운영관리를 위하여 필요시 사용기관을 대상으로 교육을 시행



### 응용서비스 운영 시 지원사항

#### ▶ 행정안전부 지원사항

- ✓ 안정적·효율적인 응용서비스 이용을 위해 양질의 서비스 확산 및 불필요 서비스 폐기를 통해 효율적 자원 활용과 운영예산의 절감 방안을 검토

#### ▶ 한국지능정보사회진흥원 지원사항

- ✓ 응용서비스 운영 시 기술적인 문제(연동 문제 등)가 발생할 경우 이에 대한 기술지원을 수행



붙임 1

재난안전통신망 관련 법 · 제도

□ 재난안전통신망법

- 재난관리책임기관 · 긴급구조기관 및 긴급구조지원기관이 공동으로 사용하는 재난안전통신망의 구축, 운영 및 사용 등에 관한 사항 명시

※ 전문은 [부록 E]를 참고

재난안전통신망법

**제8조(재난안전통신망의 운영 · 관리)** ① 행정안전부장관은 재난안전통신망의 운영 · 관리에 관한 사항을 관장하고, 재난안전통신망의 운영 · 관리를 위하여 필요한 인력, 시설, 장비 등을 갖추어야 한다.

② 재난안전 관련기관의 장은 재난안전통신망의 효율적인 운영 · 관리를 위한 행정안전부장관의 요청 등에 적극 응하여야 한다.

③ 재난안전 관련기관은 그가 설치한 관제시설, 지령장치와 그 회선 및 단말기 등의 재난안전통신설비에 대한 유지 · 관리를 담당하며, 재난안전통신설비의 적절한 운영 · 관리를 위하여 필요한 인력, 시설, 장비 등을 갖추도록 노력하여야 한다.

④ 제1항부터 제3항까지에서 규정한 사항 외에 재난안전통신망의 운영 및 관리에 필요한 사항은 대통령령으로 정한다.

**제16조(재난안전통신망의 사용)** ① 재난안전 관련기관은 다음 각 호의 활동을 하는 경우에는 재난안전통신망을 사용하여야 한다.

1. 재난의 대응 및 복구과정에서 재난안전 관련기관 간 상황의 지시, 보고 및 전파
2. 기본법 제37조에 따른 응급조치 등 행정안전부장관이 재난안전통신망의 사용이 필요하다고 정하여 고시하는 활동

② 제1항에서 규정한 사항 외에 재난안전통신망의 사용에 필요한 사항은 대통령령으로 정한다.

**제17조(재난안전통신망 사용 절차 등의 마련)** ① 재난안전 관련기관은 재난안전통신망의 사용에 관하여 행정안전부장관이 정하여 고시하는 절차와 방법을 따라야 한다.

② 행정안전부장관은 재난안전통신망의 사용과 관련하여 재난안전 관련기관에 필요한 재난안전대응 절차를 연구 · 개발하여 보급할 수 있다.

**제18조(재난안전관리 정보서비스 제공)** 행정안전부장관은 대통령령으로 정하는 바에 따라 재난안전통신망과 기본법 제74조제1항에 따른 재난관리정보통신체계 등을 연계하여 재난안전관리에 필요한 정보서비스를 제공할 수 있다.

**제19조(재난안전통신망의 상호 운용성 확보 등)** 행정안전부장관은 재난안전통신망과 주파수 대역을 공동으로 사용하는 공공통신망과의 상호 운용성을 확보하기 위하여 관계 행정기관 또는 공공기관과 협력체계를 구축하는 등 필요한 조치를 하여야 한다.

**제20조(재정적 지원)** 국가는 재난안전통신망의 구축 및 운영과 관련하여 재난안전 관련기관에 필요한 재정의 일부를 지원할 수 있다.

## □ 재난 및 안전관리 기본법

- 정부의 체계적인 재난관리를 위한 재난안전통신망 구축·운영·응용절차 마련 등에 관한 사항을 명시

재난 및 안전관리 기본법	<p>제34조의2(재난현장 긴급통신수단의 마련) ① 재난관리책임기관의 장은 재난의 발생으로 인하여 통신이 끊기는 상황에 대비하여 미리 유선이나 무선 또는 위성통신망을 활용할 수 있도록 긴급통신수단을 마련하여야 한다.</p> <p>② 행정안전부장관은 재난현장에서 제1항에 따른 긴급통신수단(이하 "긴급통신수단"이라 한다)이 공동 활용될 수 있도록 하기 위하여 재난관리책임기관, 긴급구조기관 및 긴급구조지원기관에서 보유하고 있는 긴급통신수단의 보유 현황 등을 조사하고, 긴급통신수단을 관리하기 위한 체계를 구축·운영할 수 있다.</p> <p>제34조의8(재난안전통신망의 구축·운영) ① 행정안전부장관은 체계적인 재난관리를 위하여 재난안전통신망을 구축·운영하여야 하며, <b>재난관리책임기관·긴급구조기관 및 긴급구조지원기관은 재난관리에 재난안전통신망을 사용</b>하여야 한다.</p> <p>② 재난관련기관은 평상시 또는 재난발생 시를 대비하여 <b>재난안전통신망을 활용한</b> 관련기관 간 <b>재난대응 절차를 마련</b>하여야 하며, 행정안전부장관은 재난관련기관에서 필요한 재난대응 절차를 연구·개발하여 보급할 수 있다.</p>
---------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

## □ 재난 및 안전관리 기본법 시행령

- 재난안전통신망 사용의 범위 및 절차·방법에 관한 준수사항을 명시

재난 및 안전관리 기본법 시행령	<p>제43조의12(재난안전통신망의 운영 및 사용) ③ 재난관리책임기관·긴급구조기관 및 긴급구조지원기관은 법 제34조의8제1항에 따라 재난관리에 관한 다음 각 호의 활동에 재난안전통신망을 사용하여야 한다.</p> <ol style="list-style-type: none"> <li><b>1. 재난관리를 위한 상황의 보고 및 전파</b></li> <li><b>2. 응급조치 등 재난 대응의 지시 및 보고</b></li> <li><b>3. 그 밖에 체계적인 재난관리를 위하여 행정안전부장관이 재난안전통신망의 사용이 필요하다고 인정하여 고시하는 활동</b></li> </ol> <p>④ 재난관련기관은 재난안전통신망을 사용할 때 재난안전통신망의 사용에 관하여 행정안전부장관이 정하여 고시하는 절차와 방법을 따라야 한다.</p>
-------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

## □ 재난안전통신망 운영 및 사용에 관한 규정

- 재난안전통신망 사용 신청, 사용 제한, 연계사용, 적합성 검증 등의 운영 및 사용에 관한 준수사항 명시

※ 전문은 [부록 F]를 참고

재난안전통신망 운영 및 사용에 관한 규정	<p><b>제22조(사용 신청)</b> ① 재난안전통신망을 사용하고자 하는 기관의 장은 행정안전부장관에게 사용을 신청하여야 한다.</p> <p>② 행정안전부장관은 제1항의 요청을 받은 경우에는 다음 각 호의 사항을 검토하여 사용 가능 여부를 통보하여야 한다.</p> <ol style="list-style-type: none"> <li>1. 재난관리업무에 사용하거나 통합지휘에 활용하는 등 재난안전통신망 목적에 부합하는지 여부</li> <li>2. 재난안전통신망에서 수용할 수 있는 통신량에 부합하는지 여부</li> <li>3. 재난안전통신망과의 연계와 연동을 위하여 적용하는 기술적 방법이 타당한지 여부</li> <li>4. 재난안전통신망과 중복성 문제가 없는지 여부</li> </ol> <p><b>제23조(사용 해지)</b> 재난안전통신망 사용기관의 장이 사용을 해지하려는 경우에는 행정안전부장관에게 해지를 요청하여야 한다.</p> <p><b>제24조(사용 제한)</b> ① 행정안전부장관은 다음 각 호의 경우에는 통신 속도, 통신망 접속 등 재난안전통신망 사용의 일부를 제한할 수 있다.</p> <ol style="list-style-type: none"> <li>1. 재난안전통신망의 안정적인 품질을 유지하기 어려운 경우</li> <li>2. 일시적인 통신량 폭주 시 장비의 정상적인 동작이 불가능한 경우</li> <li>3. 보안에 피해가 있거나 우려되는 경우</li> <li>4. 상용망 사용요금 등을 장기간 납부하지 않은 경우</li> <li>5. 재난안전 업무와 무관한 인터넷 사이트 등을 접속하는 경우</li> <li>6. 그 밖에 행정안전부장관이 필요하다고 인정하는 사항</li> </ol> <p>② 행정안전부장관은 제1항에 따라 재난안전통신망 사용을 제한하였을 때에는 해당 사용기관에게 그 사실을 통보하여야 한다.</p> <p><b>제25조(장애 신고)</b> ① 사용기관의 장 또는 사용자는 재난안전통신망이 장애가 발생한 것으로 판단하는 경우에는 행정안전부장관에게 그 사실을 지체 없이 신고하여야 한다.</p> <p>② 제1항에 따라 신고를 접수한 행정안전부 담당공무원은 지체 없이 필요한 조치를 하여야 하며 장애처리에 장시간이 소요될 경우에는 사용기관의 장 또는 사용자에게 그 사실을 통보하여야 한다.</p> <p><b>제26조(비용 부담)</b> ① 사용기관이 재난안전통신망을 사용하기 위하여 필요한 비용의 부담에 관한 사항은 다음 각 호와 같다.</p> <ol style="list-style-type: none"> <li>1. 사용기관별 자체 통신서비스를 기간통신사업자의 이동통신망 기지국을 통하여 제공받는 경우에 발생하는 통신요금</li> <li>2. 사용기관에서 자체 장비를 재난안전통신망과 연결하기 위하여 필요한 기간통신사업자의 전용회선 요금</li> <li>3. 그 밖에 행정안전부장관이 필요하다고 인정하는 사항</li> </ol> <p>② 행정안전부장관은 기간통신사업자와 재난안전통신망 사용기관의 비용 절감 등 효율적인 관리를 위한 협약을 체결할 수 있다.</p>
------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

재난안전통신망 운영 및 사용에 관한 규정	<p><b>제27조(연계 사용)</b> ① 사용기관의 장이 자체 정보통신망 또는 정보시스템을 재난 안전통신망과 연계하여 사용하고자 하는 경우에는 행정안전부장관과 상호 협의 하여 국가정보원장의 보안성검토 결과에 따라 구성하여야 한다.</p> <p>② 제1항에 따른 <b>보안성검토는 사용기관의 장이 국가정보원장에게 의뢰</b>하여야 한다.</p> <p><b>제28조(사용 장비 등 도입)</b> ① 사용기관의 장은 단말기, 지령장치 등 재난안전통신망 사용을 위하여 필요한 장비를 도입하는 경우에는 행정안전부장관이 지정한 전문 기관으로부터 <b>기술 적합성 검증</b>을 받은 장비이어야 한다.</p> <p>② 제1항에 따른 기술적합성 검증에 따른 비용은 사용기관의 장이 부담하는 것을 원칙으로 하되, 행정안전부장관이 필요하다고 인정하는 경우에는 예산 범위 내에서 지원 또는 분담할 수 있다.</p> <p><b>제29조(사용 촉진)</b> ① 행정안전부장관은 사용기관의 의견을 수렴하여 재난안전통신망 사용을 촉진하기 위한 관련 정책 및 사업을 추진하고 해당 성과를 사용기관에게 널리 활용 · 확산될 수 있도록 보급할 수 있다.</p> <p>② 행정안전부장관은 재난안전통신망과 관련한 시험 · 검증, 연구개발, 실용화 등의 업무를 자유롭게 수행할 수 있는 개발환경 시스템을 구축하고 산업계, 학계, 연구계에 개방하여야 한다.</p> <p>③ 제2항에 따른 개발환경 시스템은 한국정보화진흥원의 미래네트워크선도시험망 (KOREN) 등 타 관계기관의 개발환경 시스템과 연계하여 공동으로 설치 · 운영 할 수 있다..</p> <p><b>제30조(시행 세칙)</b> 재난안전통신망사업단장은 이 규정의 범위 안에서 <b>재난안전통신망 운영과 사용에 필요한 사항을 따로 정할 수 있다.</b></p>
------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

## □ 국가정보보안 지침

- 재난안전통신망 보호를 위해 재난안전통신망에 도입될 수 있는 정보통신제품과 보안적합성 검증을 명시

국가정보보안 지침	<p><b>제20조(정보통신제품 도입)</b> ① 각급기관의 장은 정보 및 정보통신망 등을 보호하기 위하여 보안기능이 있는 다음 각 호의 정보통신제품을 도입할 수 있다.</p> <ol style="list-style-type: none"> <li>1. 제21조에 따른 안전성 검증필 제품 목록에 등재되어 있는 제품</li> <li>2. 비밀이 아닌 업무자료의 암호화를 목적으로 한 경우 [별표 2] 암호가 주기능인 제품 도입요건을 만족하는 제품</li> <li>3. 제1호 및 제2호에 해당하지 않는 정보통신제품 중에서 국가정보원장이 별도로 공지하는 도입요건을 만족하는 제품</li> </ol> <p>② 제1항제3호에 해당하는 제품은 실제 적용 · 운용 이전에 제2장제5절에 따른 보안적합성 검증을 받아야 한다.</p>
--------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

## 붙임 2

## 재난안전통신망 관련 표준

- 재난안전통신망에 적용된 이동통신기술인 PS-LTE는 이동통신 표준화 기술협력기 3GPP에서 제정한 릴리스 13 표준을 기반으로 하며 관련 TTA 표준 등을 준수
- 그룹통신과 직접통신을 위한 기본 기능들은 릴리스 12에서 이들의 기능향상 및 단독 기지국 운용기능은 릴리스 13에서 표준화 완료

PS-LTE 관련 3GPP 표준 주요 내용

주요기술	구분	설명
MCPTT (Mission Critical Push to Talk)	정의	휴대단말을 사용하여 무전기와 같이 스위치를 누르는 동작만으로 대기시간을 최소화(1초 이내)하여 일대일 또는 그룹통화가 가능한 서비스 (일반 휴대폰은 호 생성 등에 10초 정도 소요)
	기술	기존 그룹 통신을 위한 GCSE_LTE 기술을 사용 근접통신으로 만들어진 ProSe 사용 LMR (TETRA, Project25, TETRAPOL, DMR, GSM-R 등)과 연계 서비스 제공
GCSE (Group Communication system Enablers)	정의	동일한 통신 그룹 소속 단말기들이 상호 간 또는 일대 다수로 통신을 하는 기능 동일 콘텐츠를 기지국을 통해 단말 그룹에 전송하는 방식으로 PTT를 지원하기 위한 핵심 기술
	기술	Unicast 기반 GCSE : 그룹 내 단말들에 동일 콘텐츠를 별도 전송 MBMS 기반 GCSE : 그룹 내 단말들에 동일 콘텐츠를 공통으로 전송
D2D (Device to Device)	정의	재난안전통신망에서 사용자가 음영지역에서 위치하게 되거나 인근 기지국에 접속하기 어려운 상황이 발생하였을 때 단말 간에 직접 통화할 수 있는 통신 기능 음영지역 또는 기지국 부재 시, 단말이 상호 간 망 (기지국)의 개입 없이 직접 통화를 가능하게 하는 기능
	기술	D2D : 네트워크 개입 없이 단말기 간 설정으로 통신환경을 구축하는 방식 (추후 적용 예정) ProSe (Proximity-based Services) : NW(기지국)에서 직접통신 권한을 받는 방식
IOPS (Isolated E-UTRAN Operation for Public Safety)	정의	기지국이 핵심 망과 접속 장애(백 홀 장애, 트래픽폭주 등)로 인해 EPC와 정상적 통신이 어려운 상황에서 임시로 커버리지 확보 및 용량증설을 위해 이동기지국을 사용하는 기술
	기술	기지국 내 그룹통화 유지나 개별통화 유지 인프라 및 이동기지국 주도의 로컬 라우팅 및 제한된 백홀 연결 넓은 범위를 서비스하는 단독기지국 운용 모드 (eNB 또는 이동기지국 구성) 격리된 기지국과 정상적인 기지국 간의 이동성 메커니즘 지원

PS-LTE 관련 TTA 표준 주요 내용

주요기술	구분	설명
통합공공망 주파수 공유 및 상호연동	정의	700MHz 통합공공망 주파수를 공동으로 사용하는 공공망(PS-LTE, LTE-M, LTE-R 등)의 기지국 간 중첩 지역에서 간섭 해소와 연속적인 서비스를 보장하기 위한 네트워크 요구사항
	기술	700MHz 통합공공망 주파수를 공동으로 사용하는 공공망(PS-LTE, LTE-M, LTE-R 등)의 기지국 간 중첩 지역에서 기지국을 공유하고 공유 공공망에 무선자원 각각 할당하여 사용함으로써 간섭을 해소
단말기 규격	정의	PS-LTE 단말기 등 재난안전통신망에서 사용되는 단말기의 호환성 유지를 위하여 필요한 규격
	기술	단말기 기술규격 단말기 시험규격 유선 푸시푸토크 마이크 간 인터페이스 규격 무선 푸시푸토크 마이크 간 인터페이스 규격

붙임 3

사용기관의 응용서비스 적용을 위한 체크리스트(안)

단계	기준1	기준2	항목
프로젝트 설계 및 구현	프로젝트 계획	조사 및 분석	○ 서비스 유형 및 현황(사용성 등) 분석
		일정	○ 적용 일정 고려
	요구사항 정의	정의	○ 사용자 요구사항 반영
	테스트	검증1	○ 평가지표(진단)를 응용한 망 응용도 진단 및 검증 ○ 서비스에 대한 정성적, 정량적 평가 ○ 심의위원회 검증을 통한 최종 승인
		검증2	○ 프로토타입 및 테스트를 통한 적정성 및 적합성 시험·검증
기타 고려사항	정책적 측면	공공성	○ 국민의 생명과 직접적으로 연관이 있는가? ○ 공공의 이익을 창출하는가?
		지속 가능성	○ 장기적 관점에서 봤을 때 향후 지속 가능한 서비스인가? ○ 산업생태계 육성에 기여하는가? ○ 4차 산업혁명 기술과 연계가 가능한 서비스인가?
	기술적 측면	수용 가능성	○ 재난안전통신망에 영향을 미치는 트래픽을 발생하는가? ○ 재난안전통신망 서버 용량, 라이선스 등 수용 가능한가?
		적용 가능성	○ 재난안전통신망의 규격에 부합하는가? ○ 재난안전통신망의 시스템과 상호운용 가능한가?
	비용적 측면	망 사용료 및 기타비용	○ 현재 망 사용료, 서비스 등록비용, 그리고 기타 적용에 필요한 비용이 적절한가?
	보안적 측면	보안사항	○ 국정원 보안적합성 등 법·제도적 규정 및 기술적 규격을 준수하였는가?
			○ 사용기관, 정부부처, 통신사 등 내·외부기관을 통해 데이터 공유가 있는지와 에 저촉되지 않는가?

**붙임 4**

**개발조직의 응용서비스 적용을 위한 체크리스트(안)**

단계	기준1	기준2	항목
사전검토	공통사항	목적성 부합	○ 재난 및 안전관리 기본법 제3조 제11호에 해당되는 경우
		중복성 최소화	○ 재난안전통신망 기본 서비스를 사용 ○ 단, 보안침해 우려, 트래픽 용량 부족 등 명백한 사유가 있는 경우 일부 중복 허용
		타당성 확보	○ 기술적, 경제적, 정책적 타당성 여부를 사전에 자체 검토한 후 행정안전부와 협의
	수용 조건	사용에 대한 검토	○ 재난안전통신망 사용의 일부 제한 조건 준수
		비용 부담	○ 재난안전통신망 비용 부담 조건 준수
		국정원 검토	○ 사용기관 자체 정보통신망 또는 정보시스템을 재난안전통신망과 연계하고자 하는 경우
		기술 적합성 검증	○ 행정안전부장관이 지정한 전문기관으로부터 기술적합성 검증을 득할 것
		무선 커버리지 확장	○ 재난안전통신망 고정기지국의 무선 커버리지 외 지역에서 기관 개별 서비스를 제공하는 경우 사용기관의 부담으로 고정기지국 등 추가 설치
		IP 주소 체계	○ IPv6 주소 체계를 따른다. ○ 불가피한 사유가 있는 경우 NAT 장비를 이용하여 IPv4를 사용할 수 있음
		타 기관 정보 연계	○ 재난안전통신망 내 타 기관의 정보와 연계시 타 기관의 동의를 얻은 후 재난안전망 운영센터와 사전 협의
개발	응용서비스	사용자 인증	○ 허용된 사용자의 식별 수단 제공 필요
		사용 편의성을 우선한 UI 설계	○ 사용 편의성을 고려한 직관적인 UI
		접근권한	○ 과도한 접근권한 허용 금지
		정보보호	○ 중요정보나 개인정보 유출방지
		국정원 보안적합성 인증	○ 공공기관에 도입하는 IT 제품의 안정성을 검증하는 제도
		보안 S/W 연동	○ 백신, MDM 연동
		운영체제 변조 대응	○ 운영체제 변조 상황에 대한 대응
		분실상황 대응	○ 단말기 분실상황에 대한 대응
		리소스 사용	○ 과도한 리소스 사용 방지
		업데이트	○ 추가 기능 개발 및 OS 호환성을 유지하기 위함



단계	기준1	기준2	항목
검증	소스코드검증	입력데이터 검증	○ SQL삽입, 운영체제 명령어 삽입, 오버플로우
		보안기능	○ 취약한 암호화 알고리즘 사용 금지 ○ 중요정보 평문저장 / 평문전송 ○ 하드코드된 비밀번호 사용 금지 ○ 주석문 안에 포함된 시스템 주요정보
		에러처리	○ 오류메시지 및 시스템 정보 노출 ○ 오류 상황 대응 ○ 부적절한 예외 처리
		코드오류	○ Null pointer역참조, 부적절한 자원 해제
		API오용	○ 취약한 API사용 금지
		모바일 환경 특화	○ 민감한 정보 전송을 위한 암시적 intent사용 금지 ○ 접근제어 없이 내 · 외부저장소 사용 금지 ○ 소스코드 난독화 적용 필요
	기능검증	기본기능	○ 제공하려는 서비스 / 기능의 정상동작 확인
		예외상황 동작	○ 정상상태를 벗어난 조건의 정상동작 확인
		자원 소비	○ 데이터 / 전력을 과도하게 소모하지 않는지 확인
		임의기능	○ 명세되지 않은 기능 존재 여부 확인 ○ 악성행위 기능 존재 여부 확인 (불법복음, 임의 데이터 전송, 임의로 위치정보 수집 · 전송 등)

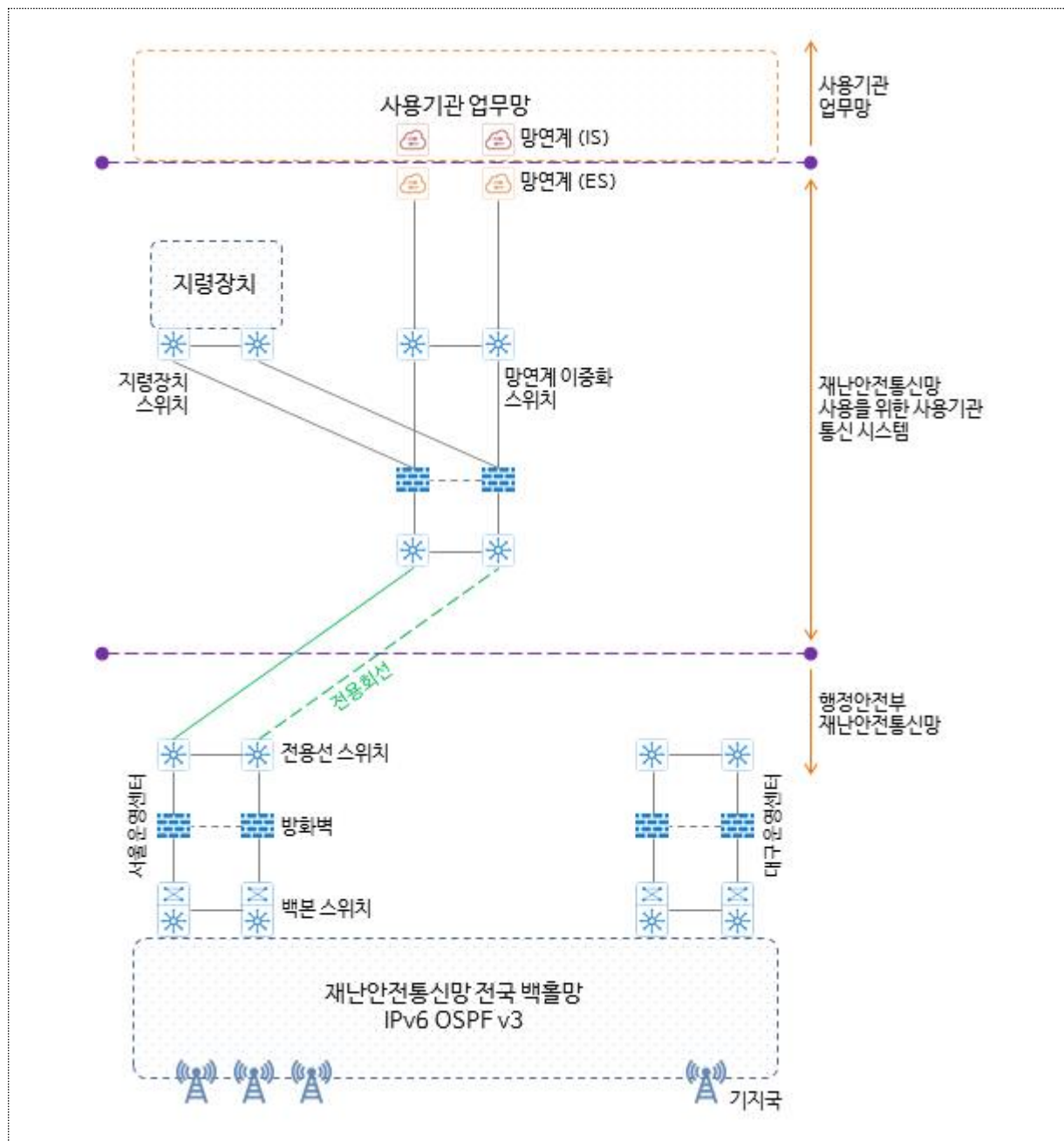
## 붙임 5

## 재난안전통신망 연동 방안

### 1. 전용회선 연동

#### □ 사용기관 유형 #1

- 서울운영센터 또는 대구운영센터 1(개) 운영센터로 회선 연동
  - Routing Protocol : Static Routing Protocol
  - Serial Interface IP Address : 126비트
  - 상세 IP Address : 서울운영센터에 문의
  - Point to Point 방식으로 연동되며, VRRP 방식은 제공하지 않음
    - ※ VRRP(Virtual Router Redundancy Protocol)
- 지령장치 네트워크 구성 : 재난안전통신망 DMZ을 사용기관으로 연장(확대)
  - 지령장치는 재난안전통신망 유선 단말기이며, 사용기관 단말기가 아님
  - SIP, H.265 통신을 위한 IPv6 네트워크 사용
  - 망연계 및 NAT(Network Address Translation) 사용하지 않음
- 외부 인터넷망 또는 소방, 경찰 등 타 기관의 업무망과 연계하는 경우에는 반드시 국가정보원에게 보안성 검토를 의뢰하고 국가정보원의 최종 검토 결과(공문)를 기준으로 구성할 것

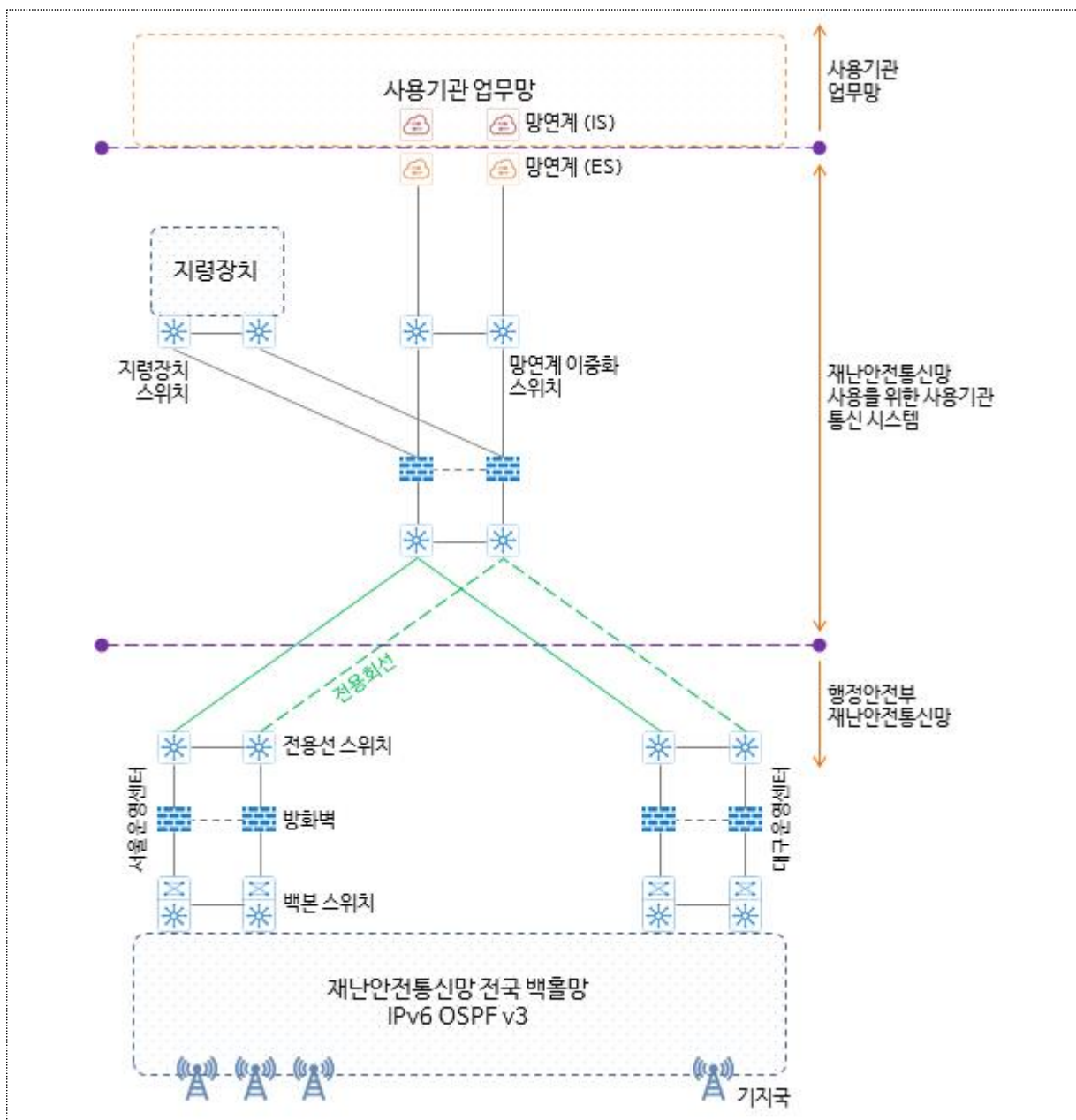


## □ 사용기관 유형 #2

- “사용기관 유형 #1”의 공통 내용 생략
- 서울운영센터 및 대구운영센터 2(개)의 운영센터로 회선 연동
- BGP(Border Gateway Protocol)로 연동

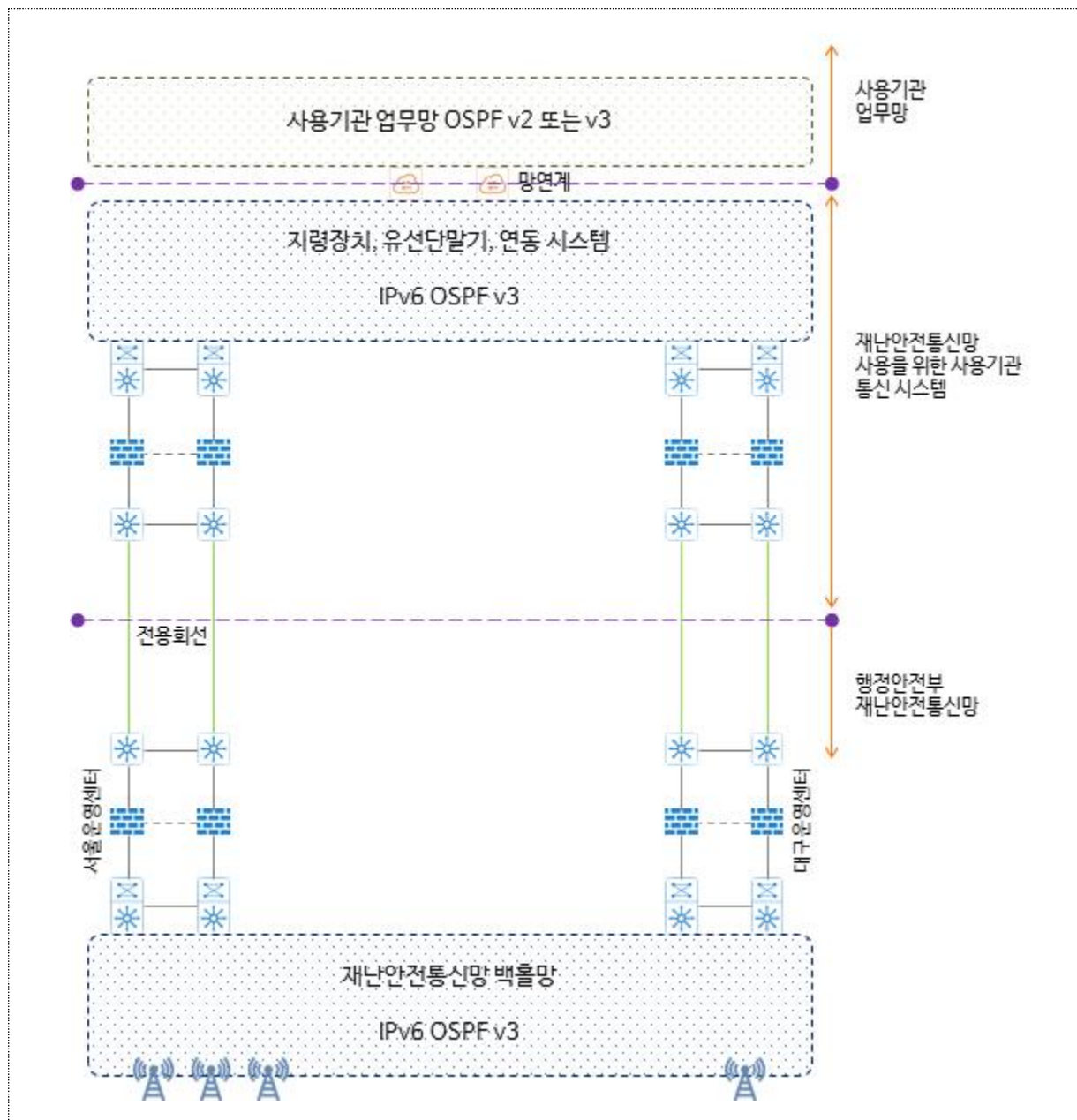
- Serial Interface IP Address : 126비트
- 상세 IP Address : 서울운영센터에 문의
- 망식별 번호(AS : Autonomous System) : 서울운영센터에 문의

※ OSPF(Open Shortest Path First)로 회선 연동은 망안전성 때문에 지양함



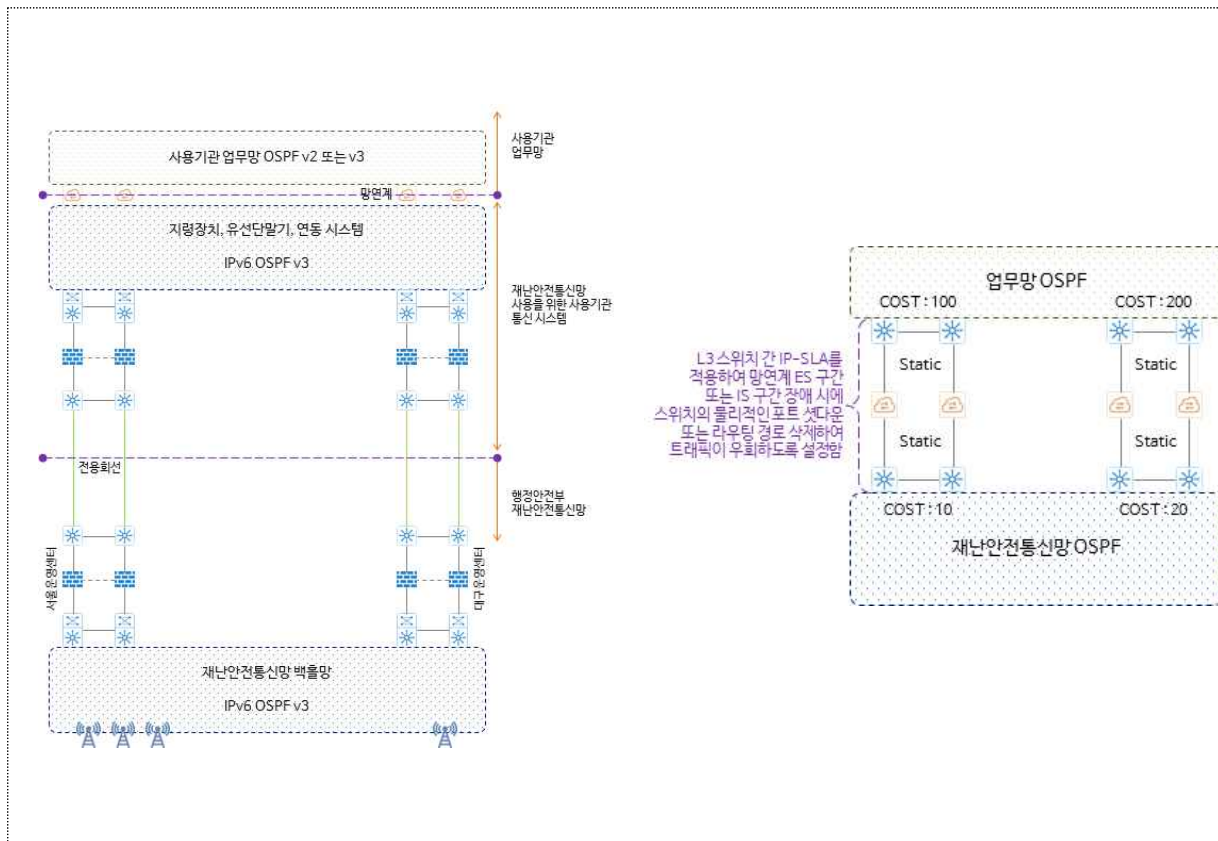
### □ 사용기관 유형 #3

- “사용기관 유형 #1, #2”의 공통 내용 생략
- 이원화된 사용기관 센터에서 서울운영센터 및 대구운영센터로 회선 연동
  - BGP로 연동
  - 사용기관 기준으로 서울운영센터 또는 대구운영센터를 Active로 사용 가능함
  - 사용기관 기준 Routing Table 별로 서울, 대구운영센터를 Active-Active로 사용 가능함
  - 서울운영센터를 Active로 사용하는 Routing Table, 대구운영센터를 Active로 사용하는 Routing Table을 정의하여 서울운영센터에 공문 처리해야 함
- 망연계 사용 구분
  - 사용기관 업무망 시스템과의 통신은 망연계를 사용함
  - 기존 업무망 시스템이 IPv4 Address를 사용하고 있다면, 망연계 External Security 외부에 방화벽(NAT64 : 사용기관이 IPv4망을 운영 중일 때)을 배치하고 IP Header를 변환하여 통신함
  - 망연계 사용 시에 망연계 내부와 외부는 Routing Table이 전달되지 않아 BGP Next Hop 등 Dynamic Routing Protocol을 사용할 수 없으니, 이원화된 재난안전통신망 연동 시에 제약 조건이 있음



## □ 사용기관 유형 #4

- “사용기관 유형 #1, #2, #3”의 공통 내용 생략
- 이원화된 센터에서 망연계 사용
  - 망연계 사용은 이기종 망간 단절을 의미하며, Dynamic Routing Protocol을 사용할 수 없음
  - 망연계 External Security와 Internal Security 간에 재난안전통신망 Routing Table과 업무망 Routing Table 정보가 교환되지 않음
  - Static Routing의 IP-SLA(Service Level Agreement) 등 유사 기능을 사용하여 망연계 ES와 IS 간의 우회 경로를 사용할 것을 권고함



## 2. DNS·GSLB 연동

### □ 재난안전통신망 DNS 및 GSLB

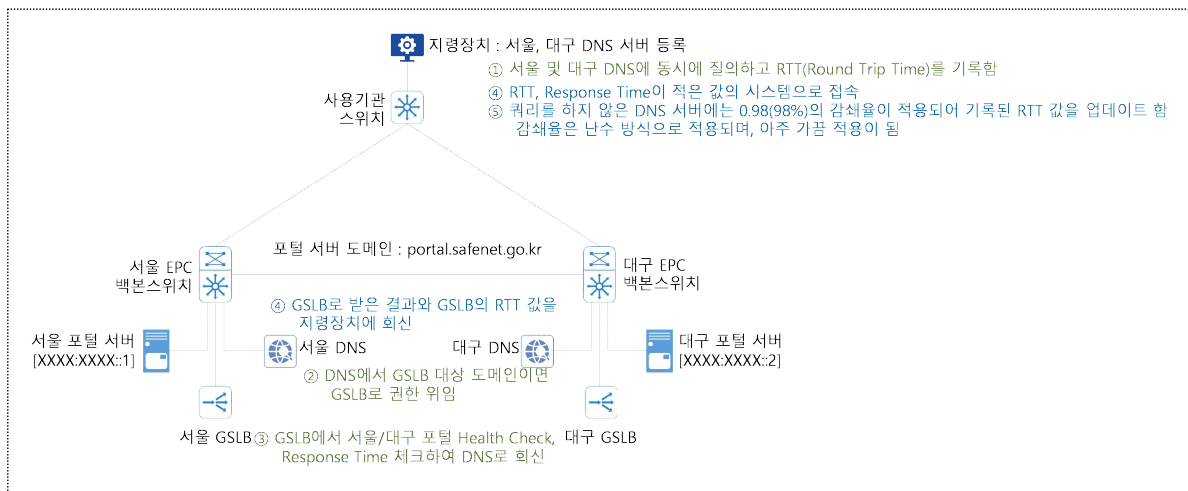
#### ○ DNS 주소

- 서울운영센터 : [ XXXX:XXXX:X110:1000:504::21 ]
- 대구운영센터 : [ XXXX:XXXX:X210:1000:504::21 ]
- 제주운영센터 : [ XXXX:XXXX:X310:1000:504::21 ]

#### ○ Domain Name : \*.safenet.go.kr

#### ○ GSLB(Global Server Load Balancing)

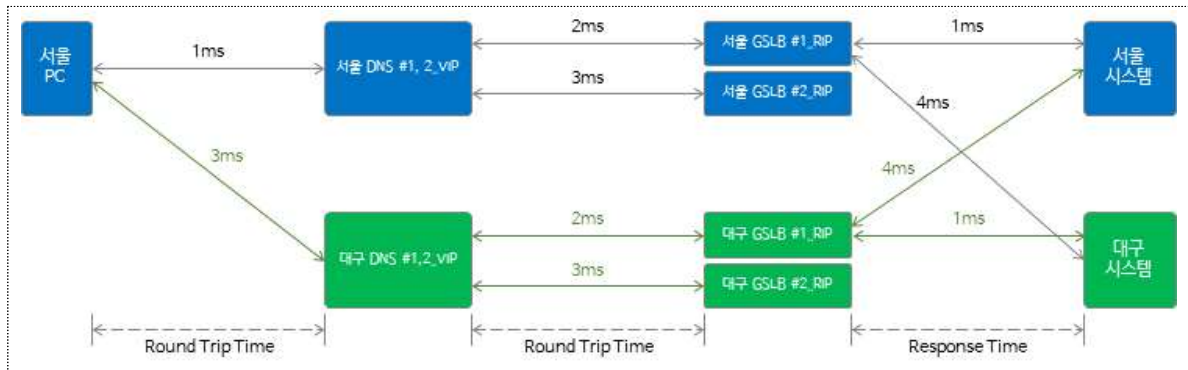
- 재난안전통신망은 삼원화 구조로 단말장치(LTE 단말기, 지령장치)는 코어망, 운영관리, 응용 설비와 도메인 기반으로 통신함
- GSLB 사용으로 센터 간 부하분산 및 단위 센터 장애 시에도 가용성을 보장함
- GSLB 동작방식은 각 시스템에 대한 ① Health Check(장애여부), ② Response Time (응답시간), ③ RTT(Round Trip Time)를 판단하여 단말장치로 회신함
- 재난안전통신망의 가용성 확보를 위해 TTL(Time to Live) 값은 "1초"로 설정되어 있음





○ Response Time 및 Round Trip Time 계산 (예시)

- 구간별 Round Trip Time 및 Response Time은 독립적으로 작동



○ DNS 쿼리 시 서울 시스템으로 접속됨

- RTT + Response Time #1 :  $1\text{ms} + 2\text{ms} + 1\text{ms} = 5\text{ms}$
- RTT + Response Time #2 :  $3\text{ms} + 2\text{ms} + 1\text{ms} = 6\text{ms}$
- 감쇄율(Decay Factor)가 11번 이상 적용이 되면 대구 시스템으로도 접속됨
  - RTT + Response Time #1 : 5ms
  - RTT + Response Time #2 :  $6\text{ms} \times 0.98 \times 0.98 \times \dots \times 0.98 = 4.9\text{ms}$
  - DNS 감쇄율(Decay Factor)는 항상 적용되지 않고, 때때로 가끔 적용이 되며 Windows, Linux, Android 등 OS 제조사 마다 알고리즘이 상이함
- 때문에 데이터 적합성을 요하는 시스템 간 통신 시에 도메인을 사용하는 것을 권고하지 않음
- 시스템 간 DNS 사용으로 인한 데이터 적합성 문제에 대해서 재난안전통신망으로 의뢰 또는 질의 불가함

## □ 재난안전통신망 도메인

○ 도메인명 : \*.safenet.go.kr

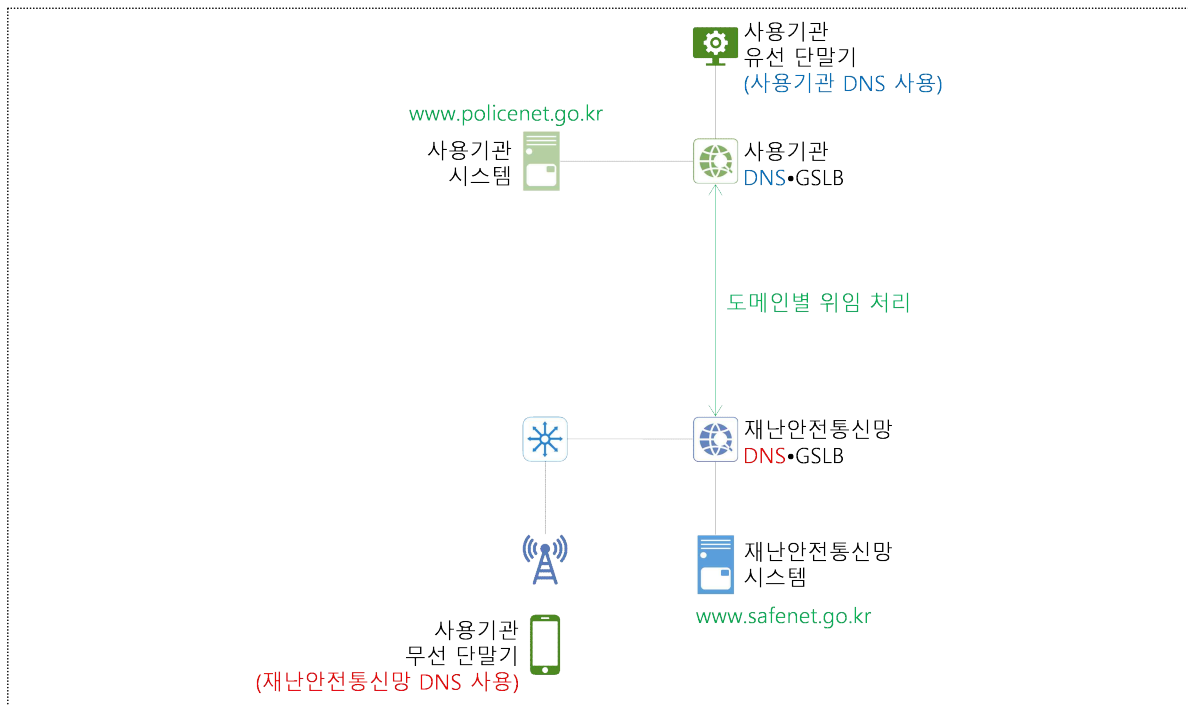
시스템명	GSLB	Domain Name	Health Check				비고
			HTTP	HTTPS	TCP	ICMP	
지도 AP	O	gism.safenet.go.kr	15310, 15410	15313	-	-	지령장치 사용
GIS AP	O	gisc.safenet.go.kr	15310, 15410	15313, 15413	-	-	지령장치 사용
지령 AP	O	cmdap.safenet.go.kr	8080	8443	-	-	지령장치 사용
MDM AP 서버	O	mdm.safenet.go.kr	18443	17443	-	-	지령장치 사용
컨텐츠 전송	O	contents.safenet.go.kr	-	-	10080, 10090	-	지령장치 사용
MMSC	O	mmsc.safenet.go.kr	-	-	50001	-	지령장치 사용
CSC	O	csc.safenet.go.kr	-	-	-	ICMP	지령장치 사용
CSCF	O	cscf.safenet.go.kr	-	-	-	ICMP	지령장치 사용
PC 포털 WEB	O	portal-p.safenet.go.kr	80	443	-	-	지령장치 사용
SSO WEB	O	sso.safenet.go.kr	80	443	-	-	지령장치 사용
Mobile 포털 WEB	O	portal-m.safenet.go.kr	80	443	-	-	
BSS WEB	O	bss.safenet.go.kr	80	443	-	-	
ITSM WEB	O	ism.safenet.go.kr	80	443	-	-	
IAM WEB	O	iam.safenet.go.kr	80	443	-	-	
OpenAPI GW	O	openapig.safenet.go.kr	18080	18443	-	-	
Developer 포털	O	openapid.safenet.go.kr	80	443	-	-	
PUSH AP 서버	O	push.safenet.go.kr	-	17443	-	-	
통계 WAS 서버	O	stat.safenet.go.kr	28080	28443	-	-	
위치제어 WEB	O	lpsp.safenet.go.kr	15443, 15010	15012	-	-	
앱스토어 Mobile WEB	O	astore-m.safenet.go.kr	-	-	23000	-	
앱스토어 PC WEB	O	astore-p.safenet.go.kr	31000	30443	-	-	
챗봇 WEB	O	chb.safenet.go.kr	80	443	-	-	
HSS	O	hss.safenet.go.kr	-	-	-	ICMP	

시스템명	GSLB	Domain Name	Health Check				비고
			HTTP	HTTPS	TCP	ICMP	
영상 WEB	O	strwb.safenet.go.kr	80	443	-	-	
영상 스트리밍	O	strsv.safenet.go.kr	-	-	-	ICMP	
영상 수집	O	strco.safenet.go.kr	-	-	-	ICMP	
NMS AP	O	nms.safenet.go.kr	8080	8443	-	-	
지령 EMS	O	cmdems.safenet.go.kr	8080	8443	-	-	
KT ICS EMS	O	icsems.safenet.go.kr	-	-	9500		
녹음녹화 저장조회 서버	O	rec.safenet.go.kr	80	-			
UMBS 수집	O	umbs.safenet.go.kr	80	443	-	-	
서울운영센터 UMBS AP	X	umbsap-s.safenet.go.kr	-	-	-	-	
대구운영센터 UMBS AP	X	umbsap-d.safenet.go.kr	-	-	-	-	
서울운영센터 FOTA WEB	X	fotawb-s.safenet.go.kr	-	-	-	-	
대구운영센터 FOTA WEB	X	fotawb-d.safenet.go.kr	-	-	-	-	
서울운영센터 LTAS WEB	X	ltas-s.safenet.go.kr	-	-	-	-	
대구운영센터 LTAS WEB	X	ltas-d.safenet.go.kr	-	-	-	-	
서울운영센터 Developer 포털	X	openapia-s.safenet.go.kr	-	-	-	-	
대구운영센터 Developer 포털	X	openapia-d.safenet.go.kr	-	-	-	-	
CBE AP	O	cbeim.safenet.go.kr	8080	8443	-	-	
Heat Map AP	O	gish.safenet.go.kr	15310, 15410	15313	-	-	
메신저 WEB 서버	X	msgwb.safenet.go.kr	-	-	-	-	
메신저 CHAT 서버	X	msgchat.safenet.go.kr	-	-	-	-	

## □ 재난안전통신망 DNS 서버 이용 방법

- 사용기관에 DNS 서버가 없는 경우 재난안전통신망 DNS 서버를 사용함
  - 네트워크 경로상 서울운영센터에 근접 : 기본 설정 DNS 서버(서울운영센터 DNS), 보조 DNS 서버(대구운영센터 DNS)
  - 네트워크 경로상 대구운영센터에 근접 : 기본 설정 DNS 서버(대구운영센터 DNS), 보조 DNS 서버(서울운영센터 DNS)
- 사용기관에 DNS 서버가 있는 경우 재난안전통신망 DNS 서버와 사용기관 DNS 서버를 연동함

- 서울운영센터와 근접한 DNS 서버는 서울운영센터 DNS 서버와 연동함
  - 대구운영센터와 근접한 DNS 서버는 대구운영센터 DNS 서버와 연동함
  - DNS 서버가 Active-Standby 1식일 경우 서울운영센터와 대구운영센터 각각 연동함
- 사용기관 유선 단말기가 사용기관 시스템을 도메인으로 접속 : 사용기관 DNS 서버 및 GSLB에서 직접 처리함
- 사용기관 유선 단말기가 재난안전통신망 시스템을 도메인으로 접속
- 사용기관 DNS 서버에 "\*.safenet.go.kr" 질의 시에 재난안전통신망 DNS 서버로 위임 처리
  - 재난안전통신망 DNS 서버 및 GSLB에서 처리 후에 사용기관 DNS 서버로 회신
- 사용기관 무선 단말기가 재난안전통신망 시스템을 도메인으로 접속 : 재난안전통신망 DNS 서버 및 GSLB에서 처리함
- 사용기관 무선 단말기가 사용기관 시스템을 도메인으로 접속
- 재난안전통신망 DNS 서버에 "\*.police.net.go.kr" 질의 시에 사용기관 DNS 서버로 위임 처리
  - 사용기관 DNS 서버 및 GSLB에서 처리 후에 재난안전통신망 DNS 서버로 회신



### 3. NTP·PTP 연동

#### □ 재난안전통신망 NTP, PTP

##### ○ NTP(Network Time Protocol)

- 패킷 교환, 가변 레이턴시 데이터 네트워크를 통해 시간을 동기화하는 프로토콜
- 시간의 정밀도 : 1/1000초
- 재난안전통신망에서는 네트워크/보안 장비, 서버 및 기타 장치류가 사용함
- LAN 및 WAN 환경에서 사용함

##### ○ PTP(Precision Time Protocol)

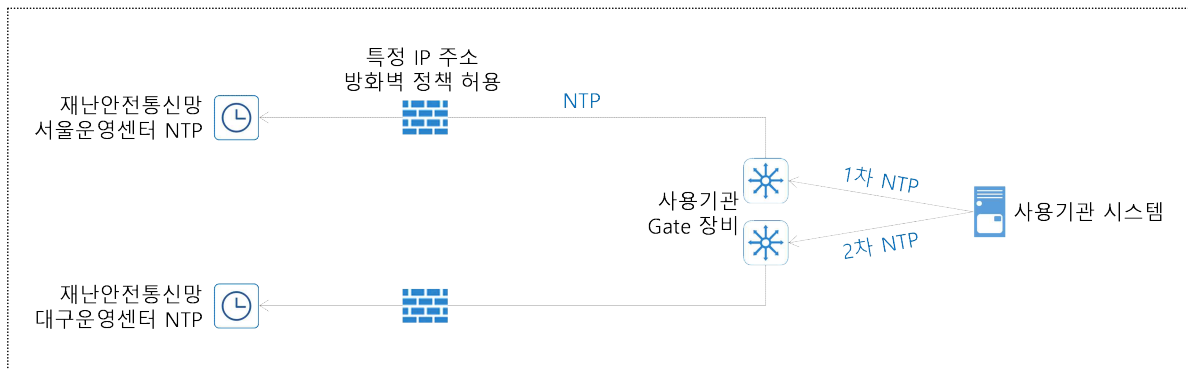
- IEEE 1588 표준으로 네트워크 장치의 클럭을 동기화하는 프로토콜
- 시간의 정밀도 : Hardware Time Stamp를 사용, 1/1,000,000초
- 재난안전통신망에서는 PSLTE 기지국, EPC 장치류, 이동기지국 및 무선단말기 등이 사용함
- LAN 환경에서 사용함

##### ○ 재난안전통신망 NTP, PTP 서버 주소

구분		서울운영센터	대구운영센터	제주운영센터
NTP 서버	1차	[ XXXX:XXXX:X110:1000:501::5 ]	[ XXXX:XXXX:X210:1000:501::5 ]	[ XXXX:XXXX:X310:1000:501::5 ]
	2차	[ XXXX:XXXX:X110:1000:501::6 ]	[ XXXX:XXXX:X210:1000:501::6 ]	[ XXXX:XXXX:X310:1000:502::5 ]
PTP 서버	1차	[ XXXX:XXXX:X110:1000:501::7 ]	[ XXXX:XXXX:X210:1000:501::7 ]	[ XXXX:XXXX:X310:1000:501::7 ]
	2차	[ XXXX:XXXX:X110:1000:501::8 ]	[ XXXX:XXXX:X210:1000:501::8 ]	[ XXXX:XXXX:X310:1000:502::7 ]

## □ 재난안전통신망 NTP 포워딩

- 사용기관이 NTP 서버를 보유하고 있으면 사용기관 NTP 사용
- 사용기관이 NTP 서버를 보유하고 있지 않은 경우 재난안전통신망 NTP 서버 사용
  - 서울운영센터와 대구운영센터 NTP 서버 사용
  - 특정 네트워크 장비 또는 리눅스 서버 중 최대 2 ~ 4대만 접속을 허용함
  - 나머지 시스템 및 장비는 위 장비를 통해 NTP 사용함



## 4. 어플리케이션 연동

### □ 녹음·녹화 시스템

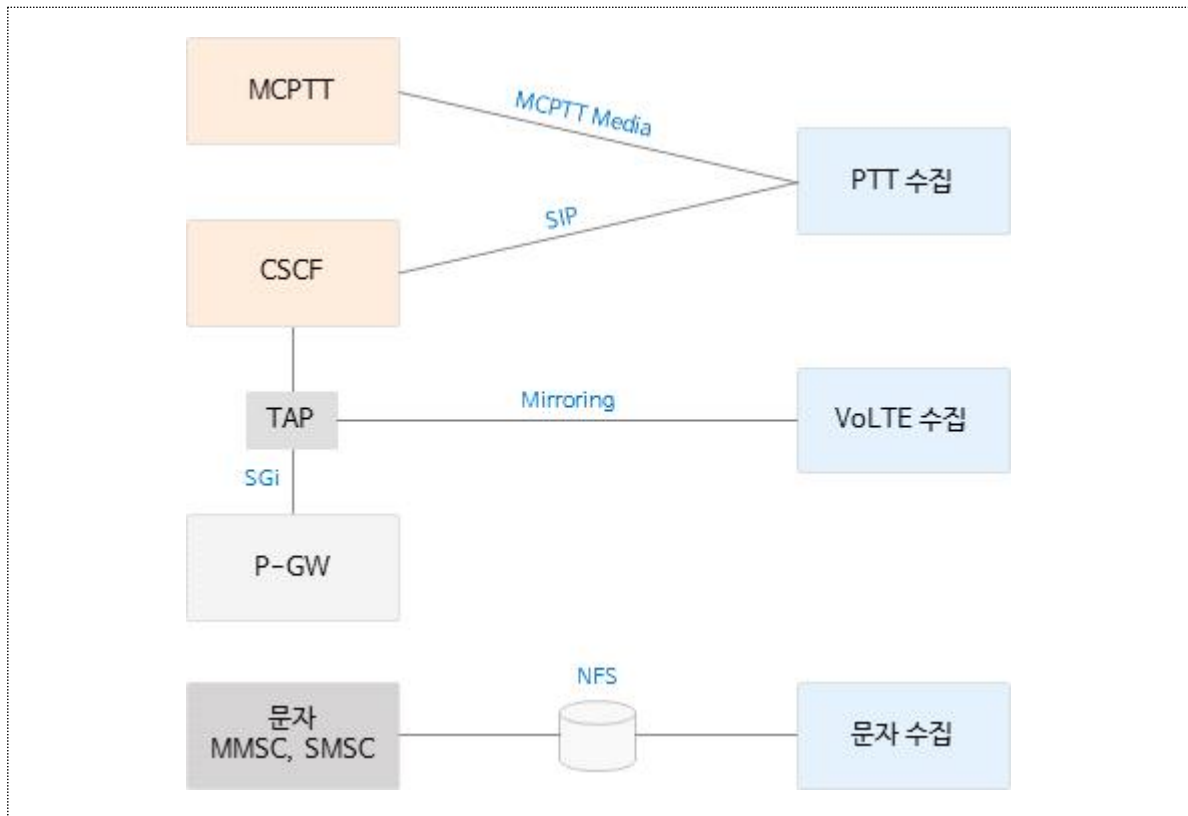
- 녹음·녹화 시스템은 PSLTE 망에서 발생하는 MCPTT 음성, 영상, 문자 등의 데이터에 대한 녹취 및 권한에 따른 녹취, 파일 다운로드 및 재생을 함
  - MCPTT 서비스 녹취
    - MCPTT 서비스 Raw Data 수집/분석
    - MCPTT 서비스 : 음성, 영상, 메시지
  - VoLTE 서비스 녹취
    - VoLTE 서비스 Raw Data 수집/분석
    - VoLTE 서비스 : 음성, 영상
  - 녹음·녹화 저장/조회
    - 수집된 정보의 저장 기능 및 관리자 등급별 메뉴 접근 권한 기능
    - 녹취 WEB 화면을 통한 저장된 정보의 검색 및 재생기능
    - 외부 저장매체 저장 기능 및 PC에서 저장된 정보 확인 기능
    - 장기 보관용 데이터 전송 기능 : WORM 스토리지

### □ 녹취 시스템

- 녹음·녹화 수집 연동
  - PTT 수집
    - 서울, 대구, 제주운영센터 MCPTT 및 CSCF 연동
    - CSCF에 Registration을 확인하고, Registration 되어 있는 경우라면 PTT 서버에서 개별/그룹 호에 대한 Record URI를 정상적으로 입력했는지 확인

시스템명	IP 주소 또는 범위	포트번호	프로토콜	비고
CSCF	•서울운영센터 [ XXXX:XXXX:X110:1000:721::11 ] •대구운영센터 [ XXXX:XXXX:X210:1000:721::11 ] •제주운영센터 [ XXXX:XXXX:X310:1000:721::11 ]	5060, 5080	UDP, TCP	SIP
MCPTT	•서울운영센터 [ XXXX:XXXX:X110:1000:727::13 ~ 72 ] •대구운영센터 [ XXXX:XXXX:X210:1000:727::13 ~ 72 ] •제주운영센터 [ XXXX:XXXX:X210:1000:727::13 ~ 72 ]	10000 ~ 65532	UDP, TCP	Media

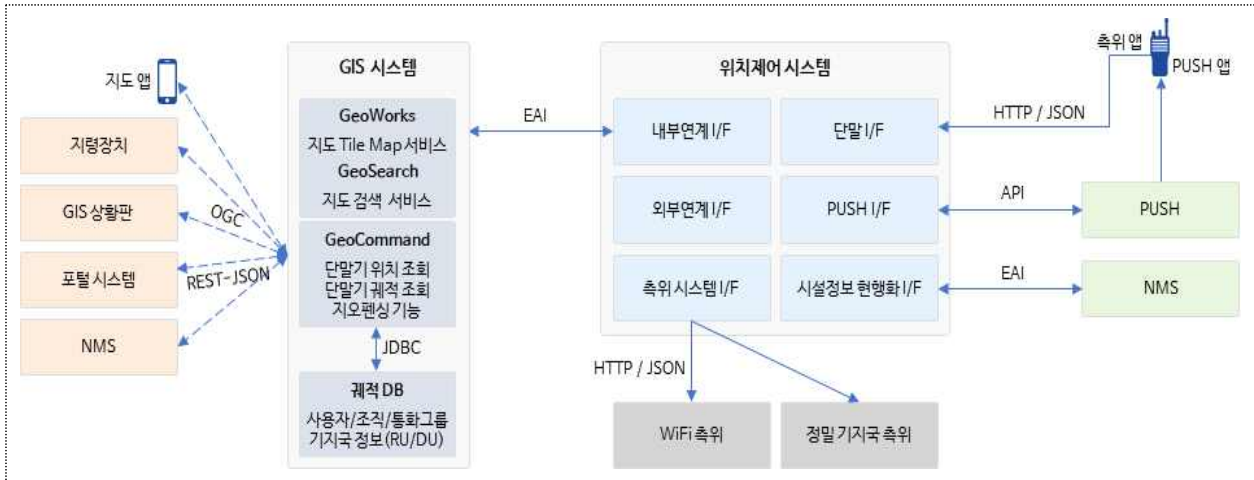
- VoLTE 수집
  - 서울, 대구운영센터 Mirroring 방식으로 수집함
  - 사용기관 시스템에서 직접 수집이 불가함
- 문자 수집
  - 서울, 대구운영 SMSC, MMSC와 연동
  - 운영센터 내에서는 NFS(Network File System)로 연동
  - 현재 재난안전통신망에서 내·외부 시스템으로의 연동은 개발되어 있지 않음
  - 때문에 사용기관에서는 송수신된 문자에 대한 수집 연동 시에 비용 발생함





## □ GIS 및 위치측위 시스템

### ○ GIS 및 위치제어(LPSP) 인터페이스 구조



### ○ GIS 표준 인터페이스 프로토콜

- REST-JSON : API를 제공하는 시스템(GeoSearch, GeoCommand)은 REST서비스를 위해 JSON형태로 입수된 클라이언트의 Data를 API Provider에 전달함
- JDBC : NMS는 사용자/조직, 기지국 데이터를 웨지 DB 서버에 전달하기 위하여 JDBC를 통하여 데이터를 전달
- OGC(Open Geospatial Consortium) : 지도 서비스를 하는 시스템(GeoWorks)는 다양한 시스템에서 활용하기 쉽도록 OGC에서 정의한 GIS 표준 인터페이스 구조를 사용함
  - WMTS(Web Map Tile Service) : 지도의 타일 이미지를 서비스하기 위한 프로토콜
  - WMS(Web Map Service) : 데이터베이스에서 데이터를 사용하기 위해 맵 서버에서 생성된 지도 이미지를 서비스하기 위한 프로토콜
  - WFS(Web Feature Service) : 데이터베이스에서 데이터를 사용하기 위해 맵 서버에서 직접 피쳐(Feature)를 서비스하기 위한 프로토콜

## ○ GIS 인터페이스 설계서

ID	설명	From	To	구분	방식	주기
A3-MSR-IIF-CMD-GIS-00002	CMD 에서 GIS 로 단말의 위치수집 On/Off 및 주기 제어	CMD	GIS	내부연계	Real Time	수시
A3-MSR-DIF-CMD-GIS-00001	CMD 에서 GIS 로 단말 궤적 조회	CMD	GIS	직접연계	Real Time	수시
A3-MSR-DIF-CMD-GIS-00002	단말기 목록 및 위치정보	CMD	GIS	직접연계	Real Time	수시
A3-MSR-DIF-CMD-GIS-00003	기지국 목록 및 위치정보	CMD	GIS	직접연계	Real Time	수시
A3-MSR-DIF-CMD-GIS-00004	단말의 현재 위치 발송 요청	CMD	GIS	직접연계	Real Time	수시
A3-MSR-DIF-CMD-GIS-00005	특정 영역 단말기 검색	CMD	GIS	직접연계	Real Time	수시
A3-MSR-DIF-CMD-GIS-00006	행정구역 (법정도 ) 단말기 검색	CMD	GIS	직접연계	Real Time	수시
A3-MSR-DIF-CMD-GIS-00007	CMD 에서 GIS 로 단말 궤적 조회 (페이징 )	CMD	GIS	직접연계	Real Time	수시
A3-MSR-DIF-통합상황판 -GIS-00001	GIS 통합상황판 단말기 목록 및 위치정보	통합상황판	GIS	직접연계	Real Time	수시
A3-MSR-EIF-GIS-00010	배경 지도 서비스	외부시스템	GIS	직접연계	Real Time	수시
A3-MSR-EIF-GIS-00011	POI 검색	외부시스템	GIS	직접연계	Real Time	수시
A3-MSR-EIF-GIS-00012	주소 검색	외부시스템	GIS	직접연계	Real Time	수시
A3-MSR-EIF-GIS-00004	단말기 위치 표시 (WMS)	외부시스템	GIS	직접연계	Real Time	수시
A3-MSR-EIF-GIS-00005	단말기 위치 표시 (WFS)	외부시스템	GIS	직접연계	Real Time	수시
A3-MSR-EIF-GIS-00006	기지국 위치 표시 (WMS)	외부시스템	GIS	직접연계	Real Time	수시
A3-MSR-EIF-GIS-00007	기지국 위치 표시 (WFS)	외부시스템	GIS	직접연계	Real Time	수시
A3-MSR-EIF-GIS-00008	동적 통화그룹 영역 표시 (WMS)	외부시스템	GIS	직접연계	Real Time	수시
A3-MSR-EIF-GIS-00008	동적 통화그룹 영역 표시 (WFS)	외부시스템	GIS	직접연계	Real Time	수시

## ○ GIS 시스템 IP 주소, 도메인명 및 어플리케이션 포트

ID	설명	From	To	구분	방식
서울 지도 서버 (GIS MAP) #1	gism.safenet.go.kr	XXXXXXX120.2000.101::76	XXXXXXX120.2000.401::75	15310/15313 (GeoSearch ) 15410/15413 (GeoWorks )	HTTP/ HTTPs
서울 지도 서버 (GIS MAP) #2		XXXXXXX120.2000.101::77			
대구 지도 서버 (GIS MAP) #1		XXXXXXX220.2000.101::76	XXXXXXX220.2000.401::75		
대구 지도 서버 (GIS MAP) #2		XXXXXXX220.2000.101::77			
서울 관제 서버 (GIS CAP) #1	gisc.safenet.go.kr	XXXXXXX120.2000.101::72	XXXXXXX120.2000.401::71	15310/15313 15410 (GeoCommand )	HTTP/ HTTPs
서울 관제 서버 (GIS CAP) #2		XXXXXXX120.2000.101::73			
대구 관제 서버 (GIS CAP) #1		XXXXXXX220.2000.101::72	XXXXXXX220.2000.401::71		
대구 관제 서버 (GIS CAP) #2		XXXXXXX220.2000.101::73			
서울 궤적 DB #1	-	XXXXXXX120.2000.103:372	XXXXXXX120.2000.103:370	-	TCP
서울 궤적 DB #2		XXXXXXX120.2000.103:373	XXXXXXX120.2000.103:371		
대구 궤적 DB #1		XXXXXXX220.2000.103:372	XXXXXXX220.2000.103:370		
대구 궤적 DB #2		XXXXXXX220.2000.103:373	XXXXXXX220.2000.103:371		

- GIS 인터페이스 명세 : A3-MSR-IIF-CMD-GIS-00002 (CMD에서 GIS로 단말의 위치수집 On/Off 및 주기 제어)

- Request

프로그램명	패키지							
참조테이블	<a href="https://gisc.safenet.go.kr:15313/api/cmd/deviceConfig.do">https://gisc.safenet.go.kr:15313/api/cmd/deviceConfig.do</a>							
번호	데이터 정의							
	데이터항목 한글명	Table/Structure 명	Column/Field 명	유형	길이	필수여부	기본값	특이사항
1	단말기 목록	deviceList []		Array		Y		설정 대상 단말 목록
2	└ 단말식별번호		deviceId	String		Y		
3	└ 단말 위치수집 여부		posOn	String		Y		Y: ON, N: OFF
4	└ 단말 위치수집 전송 간격		interval	Number		Y		second

- Response

번호	데이터 정의							
	데이터항목 한글명	Table/Structure 명	Column/Field 명	유형	길이	필수여부	기본값	특이사항
1	내부연계 송수신 상태 코드		IIF_TRSMRCV_STTUS_CODE	Char	1	Y		인터페이스 처리 상태코드를 Source 시스템에 전달 (N: 전송 S: 성공 E: 오류)
2	내부연계 상태 메시지		IIF_STTUS_MSSAGE	String	250	N	null	인터페이스 오류 메시지를 Source 시스템에 전달 (Target 시스템에서 처리 중 오류 (E)인 경우 해당 오류 메시지 리턴)
3	트랜잭션 ID		tid	String	20	Y		Async 방식으로 요청했을 시 작업 ID - 위치정보 응답 시 사용

## ○ GIS 인터페이스 명세 : A3-MSR-DIF-CMD-GIS-00001 (CMD에서 GIS로 단말 궤적 조회)

## - Request

프로그램명	패키지							
참조테이블	https://gisc.safenet.go.kr:15313/api/cmd/locationTrace.do							
번호	데이터 정의							
	데이터항목 한글명	Table/Structure 명	Column/Field 명	유형	길이	필수여부	기본 값	특이사항
1	단말식별번호		deviceId	String		Y		
2	조회 시작시간		fromTime	String		Y		yyyyMMddHHmmss
3	조회 종료시간		toTime	String		Y		yyyyMMddHHmmss
4	단말 위치수집 전송 간격		interval	Number		Y		second

## - Response

번호	데이터 정의							
	데이터항목 한글명	Table/Structure 명	Column/Field 명	유형	길이	필수여부	기본값	특이사항
1	내부연계 송수신 상태 코드		IIF_TRSMRCV_STTUS_CODE	Char	1	Y		인터페이스 처리 상태코드를 Source 시스템에 전달 (N : 전송, S : 성공, E : 오류)
2	내부연계 상태 메시지		IIF_STTUS_MESSAGE	String	250	N	null	인터페이스 오류 메시지를 Source 시스템에 전달 (Target 시스템에서 처리 중 오류 (E)인 경우 해당 오류 메시지 리턴)
3	트랜잭션 ID		tid	String	20	Y		Async 방식으로 요청했을 시 작업 ID - 위치정보 응답 시 사용
4	단말식별번호		deviceId	String		Y		
5	위치정보 목록	locations[]		Array		Y		
6	위치 획득 시간		posTime	String		Y		yyyyMMddHHmmss
7	기지국 ID		equip_id	String	20	Y		
8	측위 방식		posMethod	String		Y		CELL:기지국측위, GPS:GPS 측위, WiFi:WiFi 측위
9	경도		longitude	Number		Y		
10	위도		latitude	Number		Y		
11	고도		altitude	Number		N	null	
12	층수		floor	Number		N	null	

## ○ GIS 인터페이스 명세 : A3-MSR-DIF-CMD-GIS-00002 (단말기 목록 및 위치정보)

## - Request

프로그램명	패키지							
참조테이블	https://gisc.safenet.go.kr:15313/api/cmd/getDeviceList.do							
번호	데이터 정의							
	데이터항목 한글명	Table/ Structure 명	Column/Field 명	유형	길이	필수여부	기본값	특이사항
1	검색 영역 최소값 (경도 )		minx	Double		N	null	검색 영역 최소값 (경도 ) - 없을 시 전체 영역 검색
2	검색 영역 최소값 (위도 )		miny	Double		N	null	검색 영역 최소값 (위도 ) - 없을 시 전체 영역 검색
3	검색 영역 최대값 (경도 )		maxx	Double		N	null	검색 영역 최대값 (경도 ) - 없을 시 전체 영역 검색
4	검색 영역 최대값 (위도 )		maxy	Double		N	null	검색 영역 최대값 (위도 ) - 없을 시 전체 영역 검색
5	통화그룹 ID		tel_grp_id	String		N	null	검색 키워드 : 통화그룹 ID
6	단말기 ID		device_id	String	50	N	null	검색 키워드 : 단말기 ID
7	기지국 ID		equip_id	String	20	N	null	검색 키워드 : 기지국 ID
8	조직 ID		grp_id	String		N	null	검색 키워드 : 조직 ID
9	단말 검색 일시		fromTime	String	14	N	null	해당 일시 이후 단말기 검색 (날짜형식 : yyyyMMddHHmmss )
10	검색요청 페이지		page	Integer		N	1	검색 요청 페이지
11	검색결과 건수		limit	Integer		N	10	검색 요청 결과 건수

## - Response

번호	데이터 정의							
	데이터항목 한글명	Table/Structure 명	Column/Field 명	유형	길이	필수여부	기본값	특이사항
1	내부연계 송수신 상태 코드		IIF_TRSMRCV_STTUS_CODE	Char	1	Y		인터페이스 처리 상태코드를 Source 시스템에 전달 (N : 전송, S : 성공, E : 오류 )
2	내부연계 상태 메시지		IIF_STTUS_MESSAGE	String	250	N	null	인터페이스 오류 메시지를 Source 시스템에 전달 (Target 시스템에서 처리 중 오류 (E)인 경우 해당 오류 메시지 리턴
3	응답결과 전체 건수		total_size	Integer		Y		검색 응답 결과 전체 건수
4	단말기 목록	device[]		Array<Map>		Y		단말기 결과 목록
5	└ 단말기 ID		device_id	String	50	Y		단말기 ID
6	└ IMEI		imei	String	50	Y		IMEI 값
7	└ 조직 ID		grp_id	String		Y		조직 ID
8	└ 조직 명칭		grp_nm	String		Y		조직 명칭
9	└ 위치 획득 시간		pos_time	String	17	Y		yyyyMMddHHmmss
10	└ 기지국 ID		equip_id	String	20	N	null	
11	└ 측위 방식		pos_method	String	5	Y		CELL:기지국측위, GPS:GPS 측위, WiFi:WiFi 측위
12	└ 경도		longitude	Number		Y		단말기 위치 (경도 )
13	└ 위도		latitude	Number		Y		단말기 위치 (위도 )
14	└ 고도		altitude	Number		N	null	단말기 고도
15	└ 층수		floor	Number		N	null	단말기가 위치한 건물 현재 층수

○ GIS 인터페이스 명세 : A3-MSR-DIF-CMD-GIS-00003 (기지국 목록 및 위치정보)

- Request

프로그램명	패키지							
참조테이블	<a href="https://gisc.safenet.go.kr:15313/api/cmd/getLTEList.do">https://gisc.safenet.go.kr:15313/api/cmd/getLTEList.do</a>							
번호	데이터 정의							
	데이터항목 한글명	Table/ Structure 명	Column/Field 명	유형	길이	필수여부	기본값	특이사항
1	검색 영역 최소값 (경도 )		minx	Double		N	null	검색 영역 최소값 (경도 ) - 없을 시 전체 영역 검색
2	검색 영역 최소값 (위도 )		miny	Double		N	null	검색 영역 최소값 (위도 ) - 없을 시 전체 영역 검색
3	검색 영역 최대값 (경도 )		maxx	Double		N	null	검색 영역 최대값 (경도 ) - 없을 시 전체 영역 검색
4	검색 영역 최대값 (위도 )		maxy	Double		N	null	검색 영역 최대값 (위도 ) - 없을 시 전체 영역 검색
5	검색 키워드 유형		kwd_typ	String	1	N	1	검색 키워드 유형 - 1 : du_id - 2 : ru_id - 3 : du_nm - 4 : ru_nm - 5 : equip_id
6	검색 키워드		keyword	String	40	N	null	검색 키워드
7	검색요청 페이지		page	Integer		N	1	검색 요청 페이지
8	검색결과 건수		limit	Integer		N	10	검색 요청 결과 건수

## - Response

번호	데이터 정의							
	데이터항목 한글명	Table/ Structure 명	Column/Field 명	유형	길이	필수여 부	기본 값	특이사항
1	내부연계 송수신 상태 코드		IIF_TRSMRCV_STT US_CODE	Char	1	Y		인터페이스 처리 상태코드를 Source 시스템에 전달 (N : 전송 , S : 성공 , E : 오류 )
2	내부연계 상태 메세지		IIF_STTUS_MSSAGE	String	250	N	null	인터페이스 오류 메시지를 Source 시스템에 전달 (Target 시 스템에서 처리 중 오류 (E)인 경 우 해당 오류 메시지 리턴
3	응답결과 전체 건수		total_size	Integer		Y		검색 응답 결과 전체 건수
4	기지국 리스트	lte_info[]						
5	↳ 기지국 ID		equip_id	String	40	Y		
6	↳ DU ID		du_id	String	40	Y		Digital Unit ID
7	↳ Cell 번호		cell_cd	String	20	Y		Cell 번호
8	↳ Sub Cell 번호		sub_cell_cd	String	20	N	null	Sub Cell 번호
9	↳ Local Cell ID		local_cell_id	String	20	N	null	Local Cell ID
10	↳ DU System 번호		du_sys_cd	String	20	N	null	DU System 번호
11	↳ DU 한글명		du_nm	String	100	Y		DU 한글명
12	↳ RU ID		ru_id	String	40	Y		RU ID
13	↳ RU 명칭		ru_nm	String	100	Y		RU 명칭
14	↳ MME 영문명		mme_en_nm	String	40	N	null	MME 영문명
15	↳ MME 한글명		mme_kr_nm	String	60	N	null	MME 한글명
16	↳ Mobile Country Code		mo_cont_cd	String	20	N	null	Mobile Country Code
17	↳ Mobile Network Code		mo_ntw_cd	String	20	N	null	Mobile Network Code
18	↳ Tracking Area Code		trck_ara_cd	String	20	N	null	Tracking Area Code
19	↳ Sector 개수		sector_cnt	Integer		Y		Sector 개수
20	↳ Physical Cell ID		phy_cell_id	String	20	N	null	Physical Cell ID
21	↳ 주파수 도달 평균 반경		freq_radus	Double		Y		주파수 도달 평균 반경
22	↳ 안테나 방향각		antn_dir_angl	Double		Y		기지국 안테나 방향각
23	↳ 안테나 개방각		antn_tilt_angl	Double		Y		기지국 안테나 개방각
24	↳ 운용상태		oper_stts	String	30	Y		기지국 현재 운용상태
25	↳ 제조사 코드		man_cd	String	20	N	null	기지국 제조사 코드
26	↳ 위도		lat	Double		Y		기지국 위치 (위도 )
27	↳ 경도		lon	Double		Y		기지국 위치 (경도 )
28	↳ 고도		alt	Double		Y		기지국 위치 (고도 )
29	↳ 도 구분		sido_cd	String	30	N	null	기지국 주소 구분 (시도 )
30	↳ 시 /군 /구 구분		sgg_cd	String	30	N	null	기지국 주소 구분 (시군구 )
31	↳ 읍 /면 /동 구분		emd_cd	String	60	N	null	기지국 주소 구분 (읍면동 )
32	↳ 번지		bunji	String	80	N	null	기지국 주소 구분 (번지 )
33	↳ 주요 건물		builing	String	50	N	null	기지국 주소 구분 (건물명 )
34	↳ 우편번호		zip_code	String	10	N	null	기지국 주소 구분 (우편번호 )
35	↳ 개통일		regt_dttm	Date		Y		기지국 개통일



○ GIS 인터페이스 명세 : A3-MSR-DIF-CMD-GIS-00004 (단말의 현재 위치 발송 요청)

- Request

프로그램명	패키지							
참조테이블	<a href="https://gisc.safenet.go.kr:15313/api/cmd/getDeviceLocation.do">https://gisc.safenet.go.kr:15313/api/cmd/getDeviceLocation.do</a>							
번호	데이터 정의							
	데이터항목 한글명	Table/Structure 명	Column/Field 명	유형	길이	필수여부	기본값	특이사항
1	단말기 목록	device[]		Array<String>		Y		현위치 조회 단말기 목록
2	단말기 ID		device_id	String	50	Y		단말기 ID

- Response

번호	데이터 정의							
	데이터항목 한글명	Table/Structure 명	Column/Field 명	유형	길이	필수여부	기본값	특이사항
1	내부연계 송수신 상태 코드		IIF_TRSMRCV_STTUS_CODE	Char	1	Y		인터페이스 처리 상태코드를 Source 시스템에 전달 (N : 전송, S : 성공, E : 오류)
2	내부연계상태메세지		IIF_STTUS_MSSAGE	String	250	N	null	인터페이스 오류 메시지를 Source 시스템에 전달 (Target 시스템에서 처리 중 오류 (E)인 경우 해당 오류 메시지 리턴)
3	트랜잭션 ID		tid	String	20	Y		Async 방식으로 요청했을 시 작업 ID - 위치정보 응답 시 사용

## ○ GIS 인터페이스 명세 : A3-MSR-DIF-CMD-GIS-00005 (특정 영역 단말기 검색)

## - Request

프로그램명	패키지							
참조테이블	https://gisc.safenet.go.kr:15313/api/cmd/getBoundaryDevice.do							
번호	데이터 정의							
	데이터항목 한글명	Table/ Structure 명	Column/ Field 명	유형	길이	필수여부	기본값	특이사항
1	검색 영역		device[]	String		Y		WKT 포맷 형태
2	단말 검색 일시		fromTime	String	14	N	null	해당 일시 이후 단말기 검색 (날짜형식 : yyyyMMddHHmmss)
3	검색요청 페이지		page	Integer		N	1	검색 요청 페이지
4	검색결과 건수		limit	Integer		N	10	검색 요청 결과 건수

## - Response

번호	데이터 정의							
	데이터항목 한글명	Table/ Structure 명	Column/Field 명	유형	길이	필수여부	기본값	특이사항
1	내부연계 송수신 상태 코드		IIF_TRSMRCV_STTUS_CODE	Char	1	Y		인터페이스 처리 상태코드를 Source 시스템에 전달 (N : 전송, S : 성공, E : 오류)
2	내부연계 상태 메세지		IIF_STTUS_MESSAGE	String	250	N	null	인터페이스 오류 메시지를 Source 시스템에 전달 (Target 시스템에서 처리 중 오류 (E)인 경우 해당 오류 메시지 리턴)
3	응답결과 전체 건수		total_size	Integer		Y		검색 응답 결과 전체 건수
4	단말기 목록	deviceList[]		Array<Map>		Y		단말기 결과 목록
5	└ 단말기 ID		DEVICE_ID	String	50	Y		단말기 ID
6	└ IMEI		IMEI	String	50	Y		IMEI 값
7	└ 위치 획득 시간		POS_TIME	String	17	Y		yyyyMMddHHmmss
8	└ 기지국 ID		EQUIP_ID	String	20	N	null	
9	└ 측위 방식		POS_METHOD	String	5	Y		CELL:기지국측위, GPS:GPS 측위, WiFi:WiFi 측위
10	└ 경도		LONGITUDE	Number		Y		단말기 위치 (경도)
11	└ 위도		LATITUDE	Number		Y		단말기 위치 (위도)
12	└ 고도		ALTITUDE	Number		N	null	단말기 고도
13	└ 층수		FLOOR	Number		N	null	단말기가 위치한 건물 현재 층수
14	└ 건물 정보		BUILDING_INFO	String		N	null	건물 정보
15	└ 저장일시		REGT_DTTM	String		Y		단말기 저장 일시

## ○ GIS 인터페이스 명세 : A3-MSR-DIF-CMD-GIS-00006 (행정구역(법정동) 단말기 검색)

## - Request

프로그램명	패키지							
참조테이블	https://gisc.safenet.go.kr:15313/api/cmd/getLayerDevice.do							
번호	데이터 정의							
	데이터항목 한글명	Table/Structure 명	Column/Field 명	유형	길이	필수여부	기본값	특이사항
1	검색 타입		type	String		Y		ctprvn : 시도 sig : 시군구 emd : 읍면동 li : 리
2	행정구역 (법정동 ) 코드		code	String		Y		행정구역 코드
3	단말 검색 일시		fromTime	String	14	N	null	해당 일시 이후 단말기 검색 (날짜형식 : yyyyMMddHHmmss)
4	검색요청 페이지		page	Integer		N	1	검색 요청 페이지
5	검색결과 건수		limit	Integer		N	10	검색 요청 결과 건수

## - Response

번호	데이터 정의							
	데이터항목 한글명	Table/Structure 명	Column/Field 명	유형	길이	필수여부	기본값	특이사항
1	내부연계 송수신 상태 코드		IIF_TRSMRCV_STTUS_CODE	Char	1	Y		인터페이스 처리 상태코드를 Source 시스템에 전달 (N : 전송 , S : 성공 , E : 오류 )
2	내부연계 상태 메세지		IIF_STTUS_MSSAGE	String	250	N	null	인터페이스 오류 메시지를 Source 시스템에 전달 (Target 시스템에서 처리 중 오류 (E)인 경우 해당 오류 메시지 리턴
3	응답결과 전체 건수		total_size	Integer		Y		검색 응답 결과 전체 건수
4	단말기 목록	deviceList[]		Array<Map>		Y		단말기 결과 목록
5	단말기 ID		DEVICE_ID	String	50	Y		단말기 ID
6	IMEI		IMEI	String	50	Y		IMEI 값
7	위치 획득 시간		POS_TIME	String	17	Y		yyyyMMddHHmmss
8	기지국 ID		EQUIP_ID	String	20	N	null	
9	측위 방식		POS_METHOD	String	5	Y		CELL:기지국측위 , GPS:GPS 측위 , WiFi:WiFi 측위
10	경도		LONGITUDE	Number		Y		단말기 위치 (경도 )
11	위도		LATITUDE	Number		Y		단말기 위치 (위도 )
12	고도		ALTITUDE	Number		N	null	단말기 고도
13	층수		FLOOR	Number		N	null	단말기가 위치한 건물 현재 층수
14	건물 정보		BUILDING_INFO	String		N	null	건물 정보
15	저장일시		REGT_DTTM	String		Y		단말기 저장 일시

○ GIS 인터페이스 명세 : A3-MSR-DIF-CMD-GIS-00007 (CMD에서 GIS로 단말 궤적 조회(페이징))

- Request

프로그램명	패키지							
참조테이블	https://gisc.safenet.go.kr:15313/api/cmd/locationTracePage.do							
번호	데이터 정의							
	데이터항목 한글명	Table/Structure 명	Column/Field 명	유형	길이	필수여부	기본값	특이사항
1	단말식별번호		deviceId	String		Y		
2	조회 시작시간		fromTime	String		Y		yyyyMMddHHmmss
3	조회 종료시간		toTime	String		Y		yyyyMMddHHmmss
4	페이지 번호		page	Number		Y		

- Response

번호	데이터 정의							
	데이터항목 한글명	Table/Structure 명	Column/Field 명	유형	길이	필수여부	기본값	특이사항
1	내부연계 송수신 상태 코드		IIF_TRSMRCV_STT_US_CODE	Char	1	Y		인터페이스 처리 상태코드를 Source 시스템에 전달 (N : 전송 , S : 성공 , E : 오류 )
2	내부연계 상태 메세지		IIF_STTUS_MSSAGE	String	250	N	null	인터페이스 오류 메시지를 Source 시스템에 전달 (Target 시스템에서 처리 중 오류 (E)인 경우 해당 오류 메시지 리턴
3	트랜잭션 ID		tid	String	20	Y		Async 방식으로 요청했을 시 작업 ID - 위치정보 응답 시 사용
4	단말식별번호		deviceId	String		Y		
5	단말 IMEI		imei	String	20	Y		IMEI
6	페이지 번호		page	Number		Y		
7	페이지내 레코드 수		count	Number		Y		
8	전체 페이지 수		totalPage	Number		Y		
9	전체 레코드 수		totalCount	Number		Y		
10	위치정보 목록	locations[]		Array		Y		
11	└ 위치 획득 시간		posTime	String		Y		yyyyMMddHHmmss
12	└ 기지국 ID		equip_id	String	20	Y		
13	└ 측위 방식		posMethod	String		Y		CELL:기지국측위 , GPS:GPS 측위 , WiFi:WiFi 측위
14	└ 경도		longitude	Number		Y		
15	└ 위도		latitude	Number		Y		
16	└ 고도		altitude	Number		N	null	
17	└ 층수		floor	Number		N	null	

## ○ GIS 인터페이스 명세 : A3-MSR-DIF-통합상황판-GIS-00001 (GIS 통합상황판 단말기 목록 및 위치 정보)

## - Request

프로그램명	패키지							
참조테이블	<a href="https://gisc.safenet.go.kr:15313/api/cmd/getMainDeviceList.do">https://gisc.safenet.go.kr:15313/api/cmd/getMainDeviceList.do</a>							
번호	데이터 정의							
	데이터항목 한글명	Table/ Structure 명	Column/ Field 명	유형	길이	필수여부	기본값	특이사항
1	검색 영역 최소값 (경도 )		minx	Double		N	null	검색 영역 최소값 (경도 ) - 없을 시 전체 영역 검색
2	검색 영역 최소값 (위도 )		miny	Double		N	null	검색 영역 최소값 (위도 ) - 없을 시 전체 영역 검색
3	검색 영역 최대값 (경도 )		maxx	Double		N	null	검색 영역 최대값 (경도 ) - 없을 시 전체 영역 검색
4	검색 영역 최대값 (위도 )		maxy	Double		N	null	검색 영역 최대값 (위도 ) - 없을 시 전체 영역 검색
5	단말기 ID		device_id	String	50	N	null	검색 키워드 : 단말기 ID
6	기지국 ID		equip_id	String	20	N	null	검색 키워드 : 기지국 ID
7	조직 ID		grp_id	String		Y		검색 키워드 : 조직 ID 대분류 사용기관 ID
8	단말 검색 일시		fromTime	String	14	N	null	해당 일시 이후 단말기 검색 (날짜형식 : yyyyMMddHHmmss)
9	검색요청 페이지		page	Integer		N	1	검색 요청 페이지
10	검색결과 건수		limit	Integer		N	10	검색 요청 결과 건수

- Response

번호	데이터 정의							
	데이터항목 한글명	Table/ Structure 명	Column/Field 명	유형	길이	필수여부	기본값	특이사항
1	내부연계 송수신 상태 코드		IIF_TRSMRCV_STTUS_CODE	Char	1	Y		인터페이스 처리 상태코드를 Source 시스템에 전달 (N : 전송 , S : 성공 , E : 오류 )
2	내부연계 상태 메 세지		IIF_STTUS_MSSAGE	String	250	N	null	인터페이스 오류 메시지를 Source 시스템에 전달 (Target 시스템에서 처리 중 오류 (E)인 경우 해당 오류 메시지 리턴
3	응답결과 전체 건 수		total_size	Integer		Y		검색 응답 결과 전체 건수
4	단말기 목록	device[]		Array< Map>		Y		단말기 결과 목록
5	단말기 ID		device_id	String	50	Y		단말기 ID
6	IMEI		imei	String	50	Y		IMEI 값
7	조직 ID		grp_id	String		Y		조직 ID
8	조직 명칭		grp_nm	String		Y		조직 명칭
9	위치 획득 시간		pos_time	String	17	Y		yyyyMMddHHmmss
10	기지국 ID		equip_id	String	20	N	null	
11	측위 방식		pos_method	String	5	Y		CELL:기지국측위 , GPS:GPS 측위 , WiFi:WiFi 측위
12	경도		longitude	Number		Y		단말기 위치 (경도 )
13	위도		latitude	Number		Y		단말기 위치 (위도 )
14	고도		altitude	Number		N	null	단말기 고도
15	층수		floor	Number		N	null	단말기가 위치한 건물 현재 층수

○ GIS 인터페이스 명세 : A3-MSR-EIF-GIS-00010 (배경 지도 서비스)

- Request

프로그램명	패키지						
참조테이블	https://gism.safenet.go.kr:15413/TMS/GC:[mapType]/[zoom]/[x]/[y].[imgType]						
번호	데이터 정의						
	데이터항목 한글명	Table/Structure 명	Column/Field 명	유형	길이	필수여부	특이사항
1	지도 유형		mapType	String		Y	보고 싶은 지도의 유형 (Path 상에 지도유형 기입 ) - base : 일반지도 - sat : 영상지도 - hybrid : 하이브리드지도
2	줌레벨		zoom	Number		Y	보고 싶은 지도의 줌레벨 (Path 상에 줌레벨 기입 )
3	X 좌표		x	Number		Y	보고 싶은 지도의 X 좌표 (Path 상에 X 좌표 기입 )
4	Y 좌표		y	Number		Y	보고 싶은 지도의 Y 좌표 (Path 상에 Y 좌표 기입 )
5	이미지 유형		imgType	String		Y	각 설정된 이미지 타입 - 일반지도 : png - 영상지도 : jpeg - 하이브리드지도 : png

- Response



○ GIS 인터페이스 명세 : A3-MSR-EIF-GIS-00011 (POI 검색)

- Request

프로그램명	패키지							
참조테이블	<a href="https://gism.safenet.go.kr:15313/search/poi">https://gism.safenet.go.kr:15313/search/poi</a>							
번호	데이터 정의							
	데이터항목 한글명	Table/Structure 명	Column/Field 명	유형	길이	필수여부	기본값	특이사항
1	검색 키워드		keyword	String		Y		
2	페이지 번호		page	Integer		N	1	
3	페이지당 개수		perCount	Integer		N	10	
4	좌표계		crs	String		N	EPSG:4326	EPSG:xxxx 형식
5	검색 포인트 좌표		point	Double[]		N		EPSG:4326 형식의 lon,lat 값 입력 [lon,lat]
6	포인트 반경		dist	Integer		N	500	meter
7	검색 경계		bbox	Double[]		N		EPSG:4326 형식 [left-bottom-lon, left-bottom-lat, right-top-lon, right-top-lat]
8	wkt 형태의 검색 경계		wkt	String		N		EPSG:4326 형식 POLYGON((...))
9	버퍼		buffer	Integer		N	0	meter



- Response

번호	데이터 정의							
	데이터항목 한글명	Table/ Structure 명	Column/Field 명	유형	길이	필수여부	기본값	특이사항
1	결과 정보	result		Object		Y		
2	↳ 결과 코드		code	Integer		Y		
3	↳ 결과 메시지		message	String		Y		
4	페이징 정보	paging		Object		Y		
5	↳ 현재 페이지 번호		page	Integer		Y		
6	↳ 마지막 페이지 번호		pages	Integer		Y		
7	↳ 페이지당 item 수		perCount	Integer		Y		
8	↳ 총 item 수		total	Integer		Y		
9	추가 정보	info		Object		Y		
10	↳ 검색 키워드		orign	String		Y		
11	↳ 세부 검색 키워드		refine	String		N		
12	↳ 좌표계		crs	String		Y		
13	↳ 검색 범위		extent	Double[]		Y		
14	검색 item	items		Object[]		Y		
15	↳ 검색 결과 개수		score	Double		Y		
16	↳ 검색 반경		dist	Double		N		
17	↳ 검색 결과	source		Object		Y		
18	↳ 일련번호		poild	String		Y		
19	↳ 공식 이름		fmyNm	String		Y		
20	↳ 카테고리 정보		category	String		Y		
21	↳ 분류 코드	sortCode		Object		Y		
22	↳ 대분류		lclas	String		Y		
23	↳ 중분류		mlsfc	String		Y		
24	↳ 소분류		sclas	String		Y		
25	↳ 세부 분류		dclas	String		Y		
26	↳ 최소 세부 분류		bclas	String		Y		
27	↳ 우선순위		priort	Integer		Y		
28	↳ 디스플레이 수준		dsplv	String		Y		
29	↳ 주소 정보	adres		Object		Y		
30	↳ 우편 번호		zip	String		Y		
31	↳ 도로 주소		road	String		Y		
32	↳ 법정동 코드		legalCd	String		Y		
33	↳ 지번 주소		lnm	String		Y		
34	↳ 국가 명소 번호		nationSpotNo	String		Y		
35	↳ 추가 정보	adilInfo		Object		N		
36	↳ 전화 번호		telNo	String		N		
37	↳ 참조 정보	refer		Object		Y		
38	↳ 참조 데이터 이름		referNm	String		Y		
39	↳ 참조 데이터 번호		referDtaNo	String		Y		
40	↳ 부모 주소 정보	mhrhlRelate		Object		Y		
41	↳ 부모 Poi 일련번호		parntsPoild	String		Y		
42	↳ 관계 코드		mhrhlCd	String		Y		1 : Comparative facility 2 : Accessory Facility 3 : Entrance
43	↳ 좌표 정보	geometry		Object		Y		
44	↳ 경도		lon	Double		Y		
45	↳ 위도		lat	Double		Y		

## ○ GIS 인터페이스 명세 : A3-MSR-EIF-GIS-00012 (주소 검색)

## - Request

프로그램명	패키지							
참조테이블	<a href="https://gism.safenet.go.kr:15313/search/adres">https://gism.safenet.go.kr:15313/search/adres</a>							
번호	데이터 정의							
	데이터항목 한글명	Table/ Structure 명	Column/ Field 명	유형	길이	필수여부	기본값	특이사항
1	검색 키워드		keyword	String		Y		
2	페이지 번호		page	Integer		N	1	
3	페이지당 개수		perCount	Integer		N	10	
4	좌표계		crs	String		N	EPSG:4326	EPSG:xxxx 형식
5	검색 포인트 좌표		point	Double[]		N		EPSG:4326 형식의 lon,lat 값 입력 [lon,lat]
6	포인트 반경		dist	Integer		N	500	meter
7	검색 경계		bbox	Double[]		N		EPSG:4326 형식 [left-bottom-lon, left-bottom-lat, right-top-lon, right-top-lat ]
8	wkt 형태의 검색 경계		wkt	String		N		EPSG:4326 형식 POLYGON((...))
9	버퍼		buffer	Integer		N	0	meter

- Response

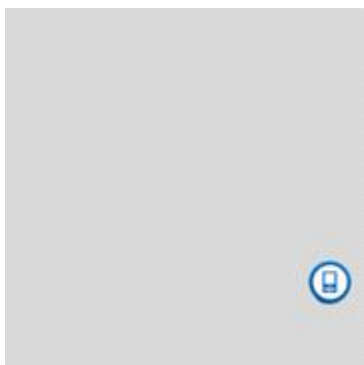
번호	데이터 정의							
	데이터항목 한글명	Table/ Structure 명	Column/Field 명	유형	길이	필수여부	기본값	특이사항
1	결과 정보	result		Object		Y		
2	↳ 결과 코드		code	Integer		Y		
3	↳ 결과 메시지		message	String		Y		
4	페이징 정보	paging		Object		Y		
5	↳ 현재 페이지 번호		page	Integer		Y		
6	↳ 마지막 페이지 번호		pages	Integer		Y		
7	↳ 페이지당 item 수		perCount	Integer		Y		
8	↳ 총 item 수		total	Integer		Y		
9	추가 정보	info		Object		Y		
10	↳ 검색 키워드		origin	String		Y		
11	↳ 세부 검색 키워드		refine	String		N		
12	↳ 좌표계		crs	String		Y		
13	↳ 검색 범위		extent	Double[]		Y		
14	검색 item	items		Object[]		Y		
15	↳ 검색 결과 개수		score	Double		Y		
16	↳ 검색 반경		dist	Double		N		
17	↳ 검색 결과	source		Object		Y		
18	↳ 일련번호		id	String		Y		
19	↳ 건물 관리 번호		buldNo	String		Y		
20	↳ 우편 번호		zip	String		Y		
21	↳ 도로 주소 정보	road		Object		Y		
22	↳ 도로 번호		no	String		Y		
23	↳ 도로 주소 (한국어 )		kor	String		Y		
24	↳ 도로 주소 (영어 )		eng	String		Y		

○ GIS 인터페이스 명세 : A3-MSR-EIF-GIS-00004 (단말기 위치 표시(WMS))

- Request

프로그램명		패키지						
참조테이블		<a href="https://gism.safenet.go.kr:15413/WMS?SERVICE=WMS&amp;VERSION=1.1.0&amp;REQUEST=GetMap&amp;LAYERS=GC:DEVICE_LAST_LOCATION">https://gism.safenet.go.kr:15413/WMS?SERVICE=WMS&amp;VERSION=1.1.0&amp;REQUEST=GetMap&amp;LAYERS=GC:DEVICE_LAST_LOCATION</a>						
번호	데이터 정의							
	데이터항목 한글명	Table/ Structure 명	Column/ Field 명	유형	길이	필수여부	기본값	특이사항
1	이미지 넓이		WIDTH	Number		N	256	리턴되는 이미지 넓이
2	이미지 높이		HEIGHT	Number		N	256	리턴되는 이미지 높이
3	요청 좌표계		SRS	String		Y		Coordinate Reference Systems 사용자가 요청한 좌표의 좌표계 example : EPSG:3857 기준 : EPSG 코드는 <a href="http://spatialreference.org">http://spatialreference.org</a> 참조
4	이미지 요청 경계 영역		BBOX	String		Y		EX) 14129231.804458257, 4439462.602803037, 14130454.79691082, 4440685.595255599
5	이미지 스타일		STYLES	String		N	DEVICE_ DEFAULT_ STYLE	단말기 표출 스타일 - DEVICE_DEFAULT_STYLE : 기본 디바이스 스타일
6	조건 검색		CQL_FILTER	String		N	null	단말기 조건 검색 EX) DEVICE_ID=3904

- Response



## ○ GIS 인터페이스 명세 : A3-MSR-EIF-GIS-00005 (단말기 위치 표시(WFS))

## - Request

프로그램명	패키지							
참조테이블	https://gism.safenet.go.kr:15413/WFS?SERVICE=WFS&VERSION=1.1.0&REQUEST=GetFeature&TYPENAME=GC:DEVICE_LAST_LOCATION							
번호	데이터 정의							
	데이터항목 한글명	Table/ Structure 명	Column/ Field 명	유형	길이	필수여부	기본값	특이사항
1	요청 좌표계		SRS	String		Y		Coordinate Reference Systems 사용자가 요청한 좌표의 좌표계 example : EPSG:3857 기준 : EPSG 코드는 <a href="http://spatialreference.org">http://spatialreference.org</a> 참조 (EX)
2	이미지 요청 경계 영역		BBOX	String		Y		14129231.804458257,4439462.60280 3037,14130454.79691082,4440685.5 95255599
3	조건 검색		CQL_FILTER	String		N	null	단말기 조건 검색 (EX) DEVICE_ID=3904

## - Response

번호	데이터 정의							
	데이터항목 한글명	Table/ Structure 명	Column/Field 명	유형	길이	필수여부	기본값	특이사항
1	응답 유형		type	String		Y		WFS 응답 유형
2	좌표 정보	crs		Object		Y		응답 데이터 좌표 정보
3	└ 정보 유형		type	String		Y		좌표 정보의 속성 유형
4	└ 속성정보	properties		Object		Y		좌표 속성 정보
5	└ 좌표 명칭 정보		name	String		Y		좌표 명칭 정보
6	Feature 정보	features		Array<Object>		Y		단말기 정보
7	└ Feature 유형		type	String		Y		
8	└ 공간정보	geometry		Object		Y		
9	└ 공간정보 유형		type	String		Y		Point
10	└ 좌표정보		coordinates	Array<Double>		Y		arr[0] = longitude arr[1] = latitude
11	└ 속성정보	properties		Object		Y		Feature 의 속성정보
12	└ 단말기 ID		DEVICE_ID	String	50	Y		단말기 ID
13	└ IMEI		IMEI	String		N	null	IMEI
14	└ 위치 획득 시간		POS_TIME	String	17	N	null	yyyyMMddHHmmss
15	└ 기지국 ID		EQUIP_ID	String	20	N	null	
16	└ 측위 방식		POSMETHOD	String	5	N	null	CELL:기지국측위, GPS:GPS 측위, WiFi:WiFi 측위
17	└ 경도		LON	Number		N	null	단말기 위치 (경도)
18	└ 위도		LAT	Number		N	null	단말기 위치 (위도)
19	└ 고도		ALTITUDE	Number		N	null	단말기 고도
20	└ 층수		FLOOR	Number		N	null	단말기가 위치한 건물 현재 층수
21	└ ID		id	String		Y		Feature ID

## ○ GIS 인터페이스 명세 : A3-MSR-EIF-GIS-00006 (기지국 위치 표시(WMS))

## - Request

프로그램명		패키지						
참조테이블		https://gism.safenet.go.kr:15413/WMS?SERVICE=WMS&VERSION=1.1.0&REQUEST=GetMap&LAYERS=GC:LTE_INFO						
번호	데이터 정의							
	데이터항목 한글명	Table/ Structure 명	Column/ Field 명	유형	길이	필수여부	기본값	특이사항
1	이미지 넓이		WIDTH	Number		N	256	리턴되는 이미지 넓이
2	이미지 높이		HEIGHT	Number		N	256	리턴되는 이미지 높이
3	요청 좌표계		SRS	String		Y		Coordinate Reference Systems 사용자가 요청한 좌표의 좌표계 example : EPSG:3857 기준 : EPSG 코드는 http://spatialreference.org 참조
4	이미지 요청 경계 영역		BBOX	String		Y		EX) 14129231.804458257,4439462.60280 3037,14130454.79691082,4440685.5 95255599
5	이미지 스타일		STYLES	String		N	LTE_DEFAULT_STYLE	기지국 표출 스타일 - LTE_DEFAULT_STYLE : 기본 기지국 스타일
6	조건 검색		CQL_FILTER	String		N	null	기지국 조건 검색 EX) DU_ID=39

## - Response



## ○ GIS 인터페이스 명세 : A3-MSR-EIF-GIS-00007 (기지국 위치 표시(WFS))

## - Request

프로그램명		패키지						
참조테이블		https://gism.safenet.go.kr:15413/WFS?SERVICE=WFS&VERSION=1.1.0&REQUEST=GetFeature&TYPENAME=GC:LT E_INFO						
번호	데이터 정의							
	데이터항목 한글명	Table/ Structure 명	Column/ Field 명	유형	길이	필수여부	기본값	특이사항
1	요청 좌표계		SRS	String		Y		Coordinate Reference Systems 사용자가 요청한 좌표의 좌표계 example : EPSG:3857 기준 : EPSG 코드는 http://spatialreference.org 참조
2	이미지 요청 경계 영역		BBOX	String		Y		EX) 14129231.804458257,4439462.602803037,14 130454.79691082,4440685.595255599
3	조건 검색		CQL_FILTER	String		N	null	기지국 조건 검색 EX) DU_ID=39

## - Response

번호	데이터 정의							
	데이터항목 한글명	Table/ Structure 명	Column/Field 명	유형	길이	필수여부	기본값	특이사항
1	응답 유형		type	String		Y		WFS 응답 유형
2	좌표 정보	crs		Object		Y		응답 데이터 좌표 정보
3	└ 정보 유형		type	String		Y		좌표 정보의 속성 유형
4	└ 속성정보	properties		Object		Y		좌표 속성 정보
5	└└ 좌표 명칭 정보		name	String		Y		좌표 명칭 정보
6	Feature 정보	features		Array<Object>		Y		기지국 정보
7	└ Feature 유형		type	String		Y		
8	└ 공간정보	geometry		Object		Y		
9	└└ 공간정보 유형		type	String		Y		Point
10	└└ 좌표정보		coordinates	Array<Double>		Y		arr[0] = longitude arr[1] = latitude
11	└ 속성정보	properties		Object		Y		Feature 의 속성정보
12	└└ 기지국 ID		EQUIP_ID	String	20	Y		

번호	데이터 정의							
	데이터항목 한글명	Table/ Structure 명	Column/Field 명	유형	길이	필수여부	기본값	특이사항
13	└ DU ID		DU_ID	String	20	Y		Digital Unit ID
14	└ Cell 번호		CELL_CD	String	20	Y		Cell 번호
15	└ Sub Cell 번호		SUB_CELL_CD	String	20	N	null	Sub Cell 번호
16	└ Local Cell ID		LOCAL_CELL_ID	String	20	N	null	Local Cell ID
17	└ DU System 번호		DU_SYS_CD	String	20	N	null	DU System 번호
18	└ DU 한글명		DU_NM	String	40	Y		DU 한글명
19	└ RU ID		RU_ID	String	20	Y		RU ID
20	└ RU 명칭		RU_NM	String	20	Y		RU 명칭
21	└ MME 영문명		MME_EN_NM	String	50	N	null	MME 영문명
22	└ MME 한글명		MME_KR_NM	String	50	N	null	MME 한글명
23	└ Mobile Country Code		MO_CONT_CD	String	20	N	null	Mobile Country Code
24	└ Mobile Network Code		MO_NTW_CD	String	20	N	null	Mobile Network Code
25	└ Tracking Area Code		TRCK_ARA_CD	String	20	N	null	Tracking Area Code
26	└ Sector 개수		SECTOR_CNT	Integer		N	null	Sector 개수
27	└ Physical Cell ID		PHY_CELL_ID	String	20	N	null	Physical Cell ID
28	└ 주파수 도달 평균 반경		FREQ_RADUS	Double		N	null	주파수 도달 평균 반경
29	└ 안테나 방향각		ANTN_DIR_ANGL	Double		N	null	기지국 안테나 방향각
30	└ 안테나 개방각		ANTN_TILT_ANGL	Double		N	null	기지국 안테나 개방각
31	└ 운용상태		OPER_STTS	String	10	N	null	기지국 현재 운용상태
32	└ 제조사 코드		MAN_CD	String	20	N	null	기지국 제조사 코드
33	└ 위도		LAT	Double		Y		기지국 위치 (위도 )
34	└ 경도		LON	Double		Y		기지국 위치 (경도 )
35	└ 고도		ALT	Double		N	null	기지국 위치 (고도 )
36	└ 도 구분		SIDO_CD	String	3	N	null	기지국 주소 구분 (시도 )
37	└ 시 /군 /구 구분		SGG_CD	String	5	N	null	기지국 주소 구분 (시군구 )
38	└ 읍 /면 /동 구분		EMD_CD	String	10	N	null	기지국 주소 구분 (읍면동 )
39	└ 번지		BUNJI	String	10	N	null	기지국 주소 구분 (번지 )
40	└ 주요 건물		BUILING	String	20	N	null	기지국 주소 구분 (건물명 )
41	└ 우편번호		ZIP_CODE	String	10	N	null	기지국 주소 구분 (우편번호 )
42	└ 개통일		REGT_DTTM	Date		Y		기지국 개통일
43	└ 변경일		UPDT_DTTM	Date		Y		기지국 정보 수정일
44	└ ID		id	String		Y		Feature ID



## ○ GIS 인터페이스 명세 : A3-MSR-EIF-GIS-00008 (동적 통화그룹 영역 표시(WMS))

## - Request

프로그램명		패키지						
참조테이블		https://gism.safenet.go.kr:15413/WMS?SERVICE=WMS&VERSION=1.1.0&REQUEST=GetMap&LAYERS=GC:TEL_GROUP						
번호	데이터 정의							
	데이터항목 한글명	Table/ Structure 명	Column/ Field 명	유형	길이	필수여부	기본값	특이사항
1	이미지 넓이		WIDTH	Number		N	256	리턴되는 이미지 넓이
2	이미지 높이		HEIGHT	Number		N	256	리턴되는 이미지 높이
3	요청 좌표계		SRS	String		Y		Coordinate Reference Systems 사용자가 요청한 좌표의 좌표계 example : EPSG:3857 기준 : EPSG 코드는 http://spatialreference.org 참조
4	이미지 요청 경계 영역		BBOX	String		Y		EX) 14129231.804458257,4439462.60280 3037,14130454.79691082,4440685.5 95255599
5	이미지 스타일		STYLES	String		N	TEL_GROUP_DEFAULT_STYLE	동적통화그룹 표출 스타일 - TEL_GROUP_DEFAULT_STYLE : 기본 펜스영역 스타일
6	조건 검색		CQL_FILTER	String		N	null	동적통화그룹 조건 검색 EX) TEL_GRP_ID=3904

## - Response



○ GIS 인터페이스 명세 : A3-MSR-EIF-GIS-00009 (동적 통화그룹 영역 표시(WFS))

- Request

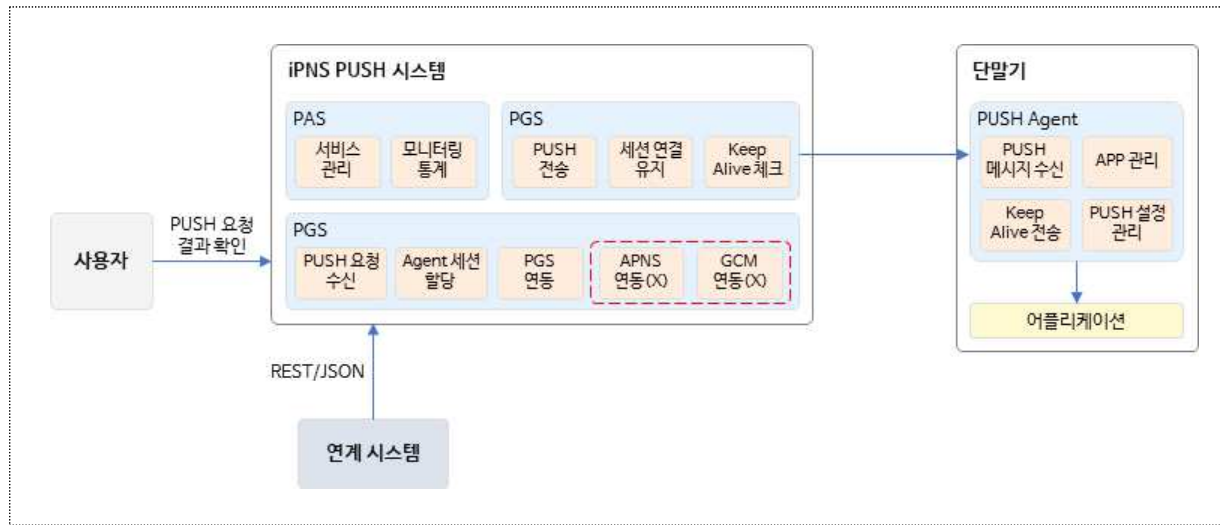
프로그램명		패키지						
참조테이블		https://gism.safenet.go.kr:15413/WFS?SERVICE=WFS&VERSION=1.1.0&REQUEST=GetFeature&TYPENAME=GC:LTE_INFO						
번호	데이터 정의							
	데이터항목 한글명	Table/ Structure 명	Column/ Field 명	유형	길이	필수여부	기본값	특이사항
1	요청 좌표계		SRS	String		Y		Coordinate Reference Systems 사용자가 요청한 좌표의 좌표계 example : EPSG:3857 기준 : EPSG 코드는 http://spatialreference.org 참조
2	이미지 요청 경계 영역		BBOX	String		Y		EX) 14129231.804458257,4439462.602803037,14 130454.79691082,4440685.595255599
3	조건 검색		CQL_FILTER	String		N	null	동적통화그룹 조건 검색 EX) TEL_GRP_ID=3904

- Response

번호	데이터 정의							
	데이터항목 한글명	Table/ Structure 명	Column/Field 명	유형	길이	필수여부	기본값	특이사항
1	응답 유형		type	String		Y		WFS 응답 유형
2	좌표 정보	crs		Object		Y		응답 데이터 좌표 정보
3	└ 정보 유형		type	String		Y		좌표 정보의 속성 유형
4	└ 속성정보	properties		Object		Y		좌표 속성 정보
5	└ 좌표 명칭 정보		name	String		Y		좌표 명칭 정보
6	Feature 정보	features		Array<Object>		Y		통화그룹 정보
7	└ Feature 유형		type	String		Y		
8	└ 공간정보	geometry		Object		Y		
9	└ 공간정보 유형		type	String		Y		Point
10	└ 좌표정보		coordinates	Array<Double>		Y		arr[0] = longitude arr[1] = latitude
11	└ 속성정보	properties		Object		Y		Feature 의 속성정보
12	└ 통화그룹 ID		TEL_GRP_ID	String		Y		통화그룹 ID
	└ 통화그룹 명		TEL_GRP_NM	String		Y		
	└ 통화그룹 이벤트 유형		TEL_GRP_EVT_TYP	String	1	Y		
	└ 최초 등록일자		REGT_DTTM	Timestamp		Y		
	└ 수정일자		UPDT_DTTM	Timestamp		Y		
	└ ID		id	String		Y		Feature ID

## □ PUSH 시스템 서버 연동 가이드

### ○ PUSH 인터페이스 구조



### ○ iPNS 구성 요소

- PIS(Push Interface Server), PGS(Push Gateway Server) : Push 전송 처리
- PAS(Push Admin Site) : Push 메시지 전송 및 서비스 관리
- Push Agent
- 외부 연계 시스템 : API로 호출
- 인증방식 : API Key

### ○ 연동 인터페이스 정의 : Push 요청 시스템은 특정 사용자 또는 App 설치 가입자 전체를 대상으로 사용자의 동의 없이 Push 메시지를 휴대용 단말기에 전송한다.

- 연동 방식 : Http / Https 연동을 통해 데이터를 송수신하며, 데이터 규격은 JSON 포맷으로 한다.

연동 시스템		연동 방식	연동 API
From	To		
요청 시스템	Push I/F 시스템	REST API	<ul style="list-style-type: none"> <li>• Push 요청 등록</li> <li>• Push 요청 취소</li> </ul>

## - 연동 API 상세 정보

Method	POST
Required	Content-Type: application/json; charset=UTF-8
Request Header	-
URI	별도 제공

## ○ 연동 Protocol 정의

## - Push 요청 등록 : Request

프로그램명	PUSH 패키지						
참조테이블	https://push.safenet.go.kr:17443/pis/interface						
번호	데이터 정의						
	이름	타입	Null 허용	크기 (바이트)	설명	예제 기본값	비고
1	SERVICE_ID	char	N	20	서비스 아이디	req(고정 값)	대소문자 구분
2	SERVICE_BEAN	char	N	20	서비스 빈	PushRequest(고정 값)	대소문자 구분
3	CP_ID	char	N	20	CP 아이디	dki	Push 시스템에서 발급
4	AUTH_KEY	char	N	20	CP 인증키	H215S6S7BI	Push 시스템에서 발급
5	REQUEST_TYPE	char	N	2	요청 타입	00	00 : 푸쉬, 01 : APP 전체 공지(예정)
6	PRIORITY	char	Y	1	요청 우선 순위	2	Default '5'
7	APP_ID	char	N	20	APP 아이디	APP ID	Push 시스템에서 발급
8	TEST_YN	char	N	1	테스트 APP 여부	N	
9	PUSH_ID_TYPE	char	Y	2	Push 수신 아이디 유형	00(미입력시 01)	00 : DEVICE_ID (Android ID) 01 : CP_USER_ID (USER ID) 02 : CP_DEVICE_ID (MSISDN) 03 : PUSH_TOKEN
10	PUSH_ID	char	N	100	Push 수신 아이디	4323521, 514123	구분자 ' ; ' 하나 이상일 경우 동보 전송 처리 (최대 1000)
11	RESV_DATE	char	Y	14	예약 전송 일자	20110810133000	공백일 경우 즉시 전송 처리
12	TITLE	char	Y	100	메시지 제목		
13	ALERT	char	Y	300	팝업 메시지		
14	MESSAGE	char	N	4000	Push 요청 메시지		
15	RESV1	char	Y	200	예약 필드		RESV1 ~ RESV6 6개 필드까지 설정 가능

## - Push 등록 요청 : Response

프로그램명	PUSH 패키지						
참조테이블	https://push.safenet.go.kr:17443/pis/interface						
번호	데이터 정의						
	이름	타입	Null 허용	크기 (바이트)	설명	예제 기본값	비고
1	RT	char	N	10	결과	0000	"0000" 아닐 경우 실패
2	RT_MSG	char	N	100	요청 결과 메시지	Success	
3	REQUEST_ID	char	N	20	요청 아이디	123	Push 요청 취소 및 상태 조회 시 활용
4	RESV	char	Y	200	예약 필드		

## - Push 요청 취소 : Request

프로그램명	PUSH 패키지						
참조테이블	https://push.safenet.go.kr:17443/pis/interface						
번호	데이터 정의						
	이름	타입	Null 허용	크기 (바이트)	설명	예제 기본값	비고
1	SERVICE_ID	char	N	20	서비스 아이디	req(고정 값)	대소문자 구분
2	SERVICE_BEAN	char	N	20	서비스 빈	PushRequest(고정 값)	대소문자 구분
3	CP_ID	char	N	20	CP 아이디	dki	
4	REQUEST_ID	char	N	20	요청 아이디	13241234	Push 요청 등록 시 리턴된 REQUEST ID 활용
5	RESV	char	Y	200	예약 필드		

※ 예약 요청일 경우만 요청 취소 가능하며, 진행 중인 Push 요청 건에 대해서는 취소 불가

## - Push 요청 취소 : Response

프로그램명	PUSH 패키지						
참조테이블	https://push.safenet.go.kr:17443/pis/interface						
번호	데이터 정의						
	이름	타입	Null 허용	크기 (바이트)	설명	예제 기본값	비고
1	RT	char	N	4	결과	0000	"0000" 아닐 경우 실패
2	RT_MSG	char	N	100	요청 결과 메시지	Success	
3	RESV	char	Y	200	예약 필드		

## ○ 연동 데이터 샘플

## - Push 요청 등록

Request	
# 즉시 전송 요청 <pre>{   "SERVICE_ID":"req",   "SERVICE_BEAN":"PushRequest",   "CP_ID":"onm",   "AUTH_KEY":"D4FG2L1435560412261",   "REQUEST_TYPE":"00",   "APP_ID":"sampleapp",   "TEST_YN":"N",   "PUSH_ID_TYPE":"01"   "PUSH_ID":"galaxyS5",   "TITLE":"Push Title ",   "ALERT":"Alert Message",   "MESSAGE":"Push Message" }</pre>	# 예약 전송 요청 <pre>{   "SERVICE_ID":"req",   "SERVICE_BEAN":"PushRequest",   "CP_ID":"onm",   "AUTH_KEY":"D4FG2L1435560412261",   "REQUEST_TYPE":"00",   "APP_ID":"sampleapp",   "TEST_YN":"N",   "PUSH_ID_TYPE":"01",   "PUSH_ID":"galaxyS5",   "RESV_DATE":"20180125110505",   "TITLE":"Push Title ",   "ALERT":"Alert Message",   "MESSAGE":"Push Message" }</pre>
# 동보 전송 요청 <pre>{   "SERVICE_ID":"req",   "SERVICE_BEAN":"PushRequest",   "CP_ID":"onm",   "AUTH_KEY":"D4FG2L1435560412261",   "REQUEST_TYPE":"00",   "APP_ID":"sampleapp",   "TEST_YN":"N",   "PUSH_ID":"galaxyS5,gnote4",   "TITLE":"Push Title ",   "ALERT":"Alert Message",   "MESSAGE":"Push Message" }</pre>	# APP 전체 요청 <pre>{   "SERVICE_ID":"req",   "SERVICE_BEAN":"PushRequest",   "CP_ID":"onm",   "AUTH_KEY":"D4FG2L1435560412261",   "REQUEST_TYPE":"01",   "APP_ID":"sampleapp",   "TEST_YN":"N",   "TITLE":"Push Title ",   "ALERT":"Alert Message",   "MESSAGE":"Push Message" }</pre>

※ 주의 사항!! 구축된 Push 서버에서 사전에 등록된 CP\_ID 및 AUTH\_KEY 정보를 사전에 발급 받아 설정해야 하며, APP\_ID 정보는 사전에 등록되어 있어야 함.

Response
<pre>{   "RT":"0000",   "RT_MSG":"Success"   "REQUEST_ID":"1234" }</pre>

- Push 요청 취소

Request

```
{
  "SERVICE_ID":"req",
  "SERVICE_BEAN":"PushRequestCancel",
  "CP_ID":"onm",
  "AUTH_KEY":"D4FG2L1435560412261",
  "REQUEST_ID":"65"
}
```

※ Push 전송 요청 시 리턴된 Request ID 정보를 활용하여 설정

Response

```
{
  "RT":"0000",
  "RT_MSG":"Success"
}
```

## □ PUSH 시스템 Local Push Library 연동 가이드

- (연동 인터페이스 정의) Android의 경우 Library(aar 파일) 파일이 제공되며, 이 라이브러리를 업무용 App 혹은 3rd Party App에 import 하여 Library 내의 API들을 호출하는 방식으로 동작함

### ○ Android용 Library

- Local Push Library는 IpnsLocalLib-<version>-release-<생성일>.aar 파일로 이루어져 있음

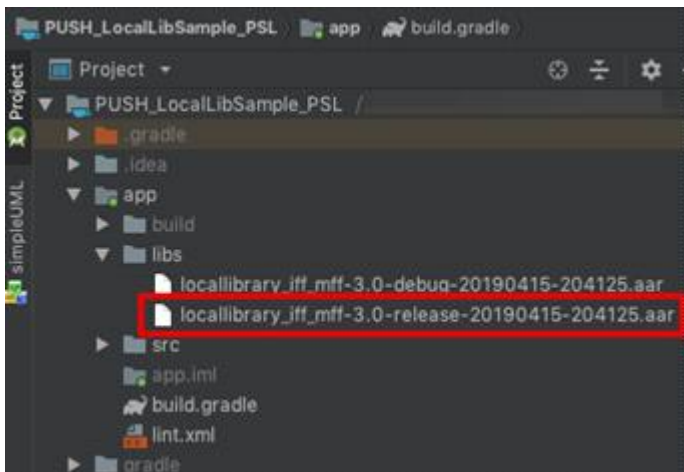
※ Library를 정상적으로 사용하기 위해서는 단말기 상에 Push Agent가 설치되어 있어야 함

※ Local Push Library는 기본적으로 Android Studio Project의 각종 기준 버전에 맞춰서 작성되어 있으므로, 이 가이드의 모든 내용은 기준 버전에서만 정상 작동을 보장함

각종 기준 버전	버전 상세 내용
Android Studio 버전	Android Studio 3.4.1 Build #AI-183.6156.11.34.5522156, built on May 2, 2019 JRE: 1.8.0_152-release-1343-b01 x86_64 JVM: OpenJDK 64-Bit Server VM by JetBrains s.r.o macOS 10.14.6
Gradle 버전	3.4.1(com.android.tools.build:gradle)
buildToolVersion	28.0.3
compileSdkVersion	28
minSdkVersion	14
targetSdkVersion	28
okhttp 버전	com.squareup.okhttp3:okhttp:3.10.0 com.squareup.okhttp3:logging-interceptor:3.8.0

기본 구성물	내용
lpnsLocalLib-<버전>-release-<생성날짜>.aar	3rd party App과 Local Push Agent 가 연동하기 위한 인터페이스 라이브러리.
추가 구성물	내용
PUSH_LocalLibSample	Local Library 사용 Sample App Project(Android Studio)

#### - Local Library 추가 및 Android Studio 설정



그림과 같이 업무용 App의 Android Studio Project 구조 중 libs 디렉토리에 AAR 파일을 추가



```
dependencies {  
    implementation 'com.android.support:appcompat-v7:28.0.0'  
    implementation 'io.realm:android-adapters:2.1.1'  
    implementation 'com.android.support:support-v4:28.0.0'  
    implementation 'com.android.support:design:28.0.0'  
    implementation 'com.android.support:recyclerview-v7:28.0.0'  
  
    implementation 'com.android.support:multidex:1.0.3'  
    androidTestImplementation 'com.android.support:multidex:1.0.3'  
  
    implementation 'com.google.code.gson:gson:2.8.5'  
  
    implementation 'com.squareup.okhttp3:okhttp:3.10.0'  
    implementation 'com.squareup.okhttp3:logging-interceptor:3.8.0'  
    implementation files('libs/localLibrary_fff_mff-3.0-debug-20190415-204125.aar')  
}
```

app레벨의 build.gradle에 붉은색 영역과 같이 dependency 라이브러리를 추가하고, 추가한 libs 밑에 aar도 그림과 같이 추가해 줌(okhttp 라이브러리를 이용해서 http 통신을 하기 때문에 관련 라이브러리 추가가 필수적)

(com.squareup.okhttp3:okhttp:3.10.0, com.squareup.okhttp3:logging-interceptor:3.8.0)

- (Permission 추가) App등록 절차에 앞서 AndroidManifest.xml에 필수 Permission과 Receiver선언 등을 추가해야 하며, AndroidManifest.xml에 선언된 BroadcastReceiver는 java 파일에 구현되어야만 Push 등록 및 수신 등의 결과를 받을 수 있음

## AndroidManifest.xml

```

<uses-permission android:name="android.permission.INTERNET" />
<uses-permission android:name="android.permission.FOREGROUND_SERVICE" />

<application
    ....>
    <receiver
        android:name="com.dkitec.locallibsample.receiver.PushLibraryBRReceiver">
        <intent-filter>
            <action android:name="com.dkitec.pns.ACTION_PUSH_RECEIVED" />
            <category android:name="{applicationId}" />
        </intent-filter>
        <intent-filter>
            <action android:name="com.dkitec.pns.ACTION_PUSH_REGISTERED" />
            <category android:name="{applicationId}" />
        </intent-filter>
        <intent-filter>
            <action android:name="com.dkitec.pns.ACTION_AGENTALIVED" />
            <category android:name="{applicationId}" />
        </intent-filter>
        <intent-filter>
            <action android:name="com.dkitec.pns.intent.CONFIGSET" />
            <category android:name="{applicationId}" />
        </intent-filter>
        <intent-filter>
            <action android:name="com.dkitec.pns.intent.CONFIGGET" />
            <category android:name="{applicationId}" />
        </intent-filter>
        <intent-filter>
            <action android:name="android.intent.action.BOOT_COMPLETED" />
        </intent-filter>
        <intent-filter>
            <action android:name="android.intent.action.PACKAGE_ADDED" />
            <category android:name="android.intent.category.DEFAULT" />
            <data android:scheme="package" />
        </intent-filter>
        <intent-filter>
            <action android:name="android.intent.action.PACKAGE_CHANGED" />
            <category android:name="android.intent.category.DEFAULT" />
            <data android:scheme="package" />
        </intent-filter>
        <intent-filter>
            <action android:name="android.intent.action.PACKAGE_REMOVED" />

```

붉은 색으로 표기된 텍스트는 다른 이름으로 바뀌어도 무방함

※ 위 내용은 Sample Project를 토대로 작성되었고 동일한 코드가 Sample Project 를 통해서 제공되므로, 자세한 내용은 Sample project 소스 코드를 참조

아래에는 위에 선언된 BroadcastReceiver 를 java 파일에 구현한 예제 코드 설명

#### PushLibraryBRReceiver.java

```
public class PushLibraryBRReceiver extends PushLibraryReceiver {
    private final String TAG = PushLibraryBRReceiver.class.getSimpleName();

    @Override
    public void onRegistration(Context arg0, String arg1) {
        Log.d(TAG, "onRegistration : " + arg1);
        if(arg1!=null && arg1.length()>0) {
            if(RegistrationFragment.mRegHandler!=null)
                RegistrationFragment.mRegHandler.sendMessage(0);
        }
    }

    @Override
    public void onMsgReceive(Context context, Bundle bundle) {
        if(bundle!=null && !bundle.isEmpty()){
            //Message ID
            String requestId = "";
            //Alert Title
            String title = "";
            //Alert Message
            String alert = "";
            //Noti 선택 시 App 으로 전달할 Message
            String message = "";
            //Image Link URL
            String imageLink = "";

            if(Build.VERSION.SDK_INT >= Build.VERSION_CODES.HONEYCOMB_MR1){
                requestId = bundle.getString("requestid", "");
                title = bundle.getString("title", "");
                alert = bundle.getString("alert", "");
                message = bundle.getString("message", "");
                imageLink = bundle.getString("linkimage", "");
            }
            else{
                requestId = bundle.getString("requestid");
                title = bundle.getString("title");
                alert = bundle.getString("alert");
                message = bundle.getString("message");
                imageLink = bundle.getString("linkimage");
            }

            Log.d("TEST", "requestId : " + requestId);
            Log.d("TEST", "title : " + title);
            Log.d("TEST", "alert : " + alert);
            Log.d("TEST", "message : " + message);
            Log.d("TEST", "imageLink : " + imageLink);
        }
    }
}
```

※ 위 내용은 Sample Project를 토대로 작성되었고 동일한 코드가 Sample Project 를 통해서 제공되므로, 자세한 내용은 Sample project 소스 코드를 참조

PushLibraryBReceiver는 PushLibrary에 포함된 PushLibraryReceiver를 상속받은 BroadcastReceiver이며, AndroidManifest.xml에 설명된 대로 Class명은 원하는 대로 바뀌어도 상관이 없지만, 반드시 하나의 PushLibraryReceiver를 상속받는 BroadcastReceiver를 구현해야만 등록과 메시지 수신 등의 이벤트를 전달 받을 수 있음

PushLibraryReceiver를 상속받는 경우, onRegistration, onMsgReceive를 반드시 override 해줘야 함

onRegistration으로는 앱 등록의 결과가 전달되고, onMsgReceive는 Push 메시지가 수신되는 부분임(단, 메시지 수신은 App 등록과정이 정상적으로 이루어지고 난 이후부터 가능함)

\* 주의 : PushLibraryReceiver를 상속받을 때, onReceive는 절대로 override하면 안됨 (override하는 경우 선처리 코드가 호출되지 않아 이상 동작 하게 됨)

○ (App 등록) 위 부분에서도 일부 설명되었지만, 3rd party 앱이 Local Push Library의 기능을 정상적으로 이용하기 위해서는 App 등록 절차가 이루어져야 하며, App 등록 절차는 아래와 같은 순서로 진행되어야 함

- (setStart API 호출) Library를 초기화 시켜주는 역할을 하며, AppRegist 등과 같은 PushLibrary의 API 호출전에 반드시 한번은 호출되어야 함

- Parameter

Parameter	필수 여부	설명
context	Y	API 를 호출하는 context (일반적으로 Activity)
serverUrl	Y	iPNS 서버 주소 (http://[아이피 혹은 도메인]:[포트]/pis/interface) ex)http://push.server.com:8080/pis/interface
appId	Y	iPNS 서버 관리자 페이지에 등록된 app id

- (Return Value) 1400이 리턴되는 경우 성공 그렇지 않으면 실패이며, 아래는 setStart 호출 후 정상일 경우 AppRegist를 호출하는 코드 예제임

## setStart 호출 후 AppRegist 호출 코드

```

public boolean registerIPNS()
{
    boolean ret = false;
    ....
    int iRet = PushLibrary.getInstance().setStart(getContext(), svrUrl, appld);
    if(iRet==1400)
    {
        int result = PushLibrary.getInstance().AppRegist(getContext(), new
PushAppRegistListener() {
            @Override
            public void didRegistResult(Context context, Bundle bundle) {
                String rt = bundle.getString("RT");
                String rt_msg = bundle.getString("RT_MSG");
                if (rt != null)
                {
                    Toast.makeText(getContext(), "App Registration 서버 응답 RT : " + rt + "
RT_MSG : " + rt_msg, Toast.LENGTH_LONG).show();
                    Log.d(TAG, "didRegistResult : " + rt + ", msg : " + rt_msg);
                    if(!TextUtils.isEmpty(rt) && "0000".equalsIgnoreCase(rt))
                    {
                        if(MainActivity.realm!=null && !MainActivity.realm.isClosed())
                        {
                            MainActivity.realm.beginTransaction();
                            if(pushSetting==null || !pushSetting.isValid())
                            {
                                pushSetting =
MainActivity.realm.where(PushSetting.class).findFirst();
                            }
                            pushSetting.setbRegistered(true);
                            pushSetting.setInterfaceServerUrl(svrUrl);
                            pushSetting.setUserId(userCn);
                            pushSetting.setAppld(appld);
                            pushSetting.setDeviceCn(deviceCn);
                            MainActivity.realm.commitTransaction();
                            SERVER_ADDRESS = svrUrl;
                            USER_CN = userCn ;
                        }
                    }
                }
            }
        })
    }
}

```

- 위 내용은 Sample Project를 토대로 작성되었으며 일부코드는 생략되어 있고, 동작하는 코드가 Sample Project를 통해서 제공되므로 자세한 내용은 Sample project 소스 코드를 참조

- (AppRegist API 호출) PushLibrary 클래스의 AppRegist를 호출하면 App등록이 요청되며 App등록이 정상적으로 이루어진 경우 iPNS Server에 현재 요청 단말의 정보와 Application정보들을 전달하고 결과값을 Library의 Callback function으로 전달함

- Parameter

Parameter	필수 여부	설명
context	Y	API를 호출하는 context (일반적으로 Activity)
listener	Y	PushAppRegistListener의 didRegistResult로 App 등록 결과가 리턴됨. 일반적으로 MainActivity 혹은 Fragment에 구현합니다.
userCN(cpUserId)	N	사용자의 id. 만약, 입력 값이 없을 경우 Device Id 만으로 앱 등록이 진행됨. (Device Id = Android Id)
cpDeviceId	N	단말 고유 값, 어떤 값을 넣어도 관계 없으나 단말 별로 Unique 한 값이어야 함(예를 들어 전화번호 등)
pushYn	N	Push 수신 여부 값, default 가 "y" 이며 앱 등록은 하나 수신여부를 "n" 으로 전달 시 등에 사용 가능

- (Return Value) API 의 return값은 int값으로 전달되며, 이 값은 AppRegist API 에 대한 정상 호출 여부만을 의미하고 전체 ErrorCode 표 이며 셀 색상이 마킹되어 있는 것만 이 API의 리턴 값으로 전달 가능함(초록색만 정상이며 나머지는 오류)

ErrorCode	Member Variable Name	설명
1400	OK	API 정상 호출
1401	CONTEXT_NOT_VALID	context 파라미터가 유효하지 않음
1402	SERVER_ADDRESS_NOT_VALID	iPNS 서버 주소가 유효하지 않음
1403	APP_ID_NOT_VALID	app id 가 유효하지 않음
1404	DEVICE_ID_NOT_VALID	단말의 DeviceID(Android ID) 가 유효하지 않습니다.
1405	AGENT_NOT_INSTALLED	Push Agent 미설치 상태입니다.
1408	REQUEST_ID_MISSING	request id 가 존재하지 않습니다.
1409	RESULT_DATA_MISSING	result data 가 존재하지 않습니다.
1410	SENDING_MSG_NULL	전송 메시지가 null 입니다.
1411	LISTENER_IS_NULL	listener 가 null 입니다.
1412	HOST_UNREACHABLE	서버 네트워크 연결 실패
1499	UNKNOWN_ERROR	알 수 없는 오류가 발생하였습니다.

- App 등록에 대한 실제 결과 값은 비동기로 전달되는데, 이는 2개의 메소드로 전달됨(첫번째는 파라미터인 PushAppRegistListener의 interface인 didRegistResult이며, 나머지 하나는 PushLibraryReceiver 를 extend 한 BroadcastReceiver의 onRegistration 메소드)
- 상세 결과 값은 파라미터인 Bundle 클래스로 전달되며, RT값이 "0000"이면서 RT\_MSG값이 "Success"이면 성공 그렇지 않으면 실패를 의미함

Parameter	필수 여부	설명
RT	Y	0000 인 경우 정상 그 이외에는 처리실패
RT_MSG	Y	성공인 경우 성공 메시지, 실패된 경우 실패 사유 등을 전달

- (Push 메시지 수신) 위에서 명시된 BroadcastReceiver의 onMsgReceive 메소드로 Push 메시지가 전달됨(메시지는 Bundle 클래스를 통해 전달되며, 각 Extra 값들을 추출해 내는 방법은 아래 코드를 참조)

## PushLibraryBRReceiver.java

```

public class PushLibraryBRReceiver extends PushLibraryReceiver {

    @Override
    public void onMsgReceive(Context context, Bundle bundle) {
        if(bundle!=null && !bundle.isEmpty()){
            //Message ID
            String requestId = "";
            //Alert Title
            String title = "";
            //Alert Message
            String alert = "";
            //Noti 선택 시 App 으로 전달할 Message
            String message = "";
            //Image Link URL
            String imageLink = "";

            if(Build.VERSION.SDK_INT >= Build.VERSION_CODES.HONEYCOMB_MR1){
                requestId = bundle.getString("requestid", "");
                title = bundle.getString("title", "");
                alert = bundle.getString("alert", "");
                message = bundle.getString("message", "");
                imageLink = bundle.getString("linkimage", "");
            }
            else{
                requestId = bundle.getString("requestid");
                title = bundle.getString("title");
                alert = bundle.getString("alert");
                message = bundle.getString("message");
                imageLink = bundle.getString("linkimage");
            }

            Log.i("TEST", "requestid : " + requestId);
            Log.i("TEST", "title : " + title);
            Log.i("TEST", "alert : " + alert);
            Log.i("TEST", "message : " + message);
            Log.i("TEST", "imageLink : " + imageLink);

            Intent receiveIntent = new Intent();
            receiveIntent.putExtras(bundle);
            receiveIntent.setClass(context, PushReceiveIntentService.class);
            receiveIntent.setPackage(context.getPackageName());
            if (Build.VERSION.SDK_INT >= Build.VERSION_CODES.O) {
                context.startForegroundService(receiveIntent);
            } else {
                context.startService(receiveIntent);
            }
        }
    }
}

```



- Android 운영 체제는 기본적으로 BroadcastReceiver에서는 간략한 작업만 수행할 것을 권장하는데, 만약 BroadcastReceiver에서 Network, GPS 그리고 File I/O 등 단말 리소스를 소비하는 작업을 수행할 경우 정상적으로 처리가 되지 않을 수 있음
- 따라서 Sample Project는 Receiver에서는 별다른 처리를 하지 않고(Bundle에서 변수들을 추출하는 법은 예제일 뿐임) PushReceiverIntentService로 Bundle을 넘겨서 처리하도록 구현함
- 비슷한 구조로 사용하는 것을 권장하며, Android O(8.0) 이상부터는 Broadcast Receiver로 부터 시작되는 Background Service는 자동으로 차단될 수 있기 때문에 startForegroundService를 호출해서 IntentService를 실행하는 것 또한 권장함

※ Push Library는 서버로부터 메시지 수신을 해서 전달까지만 책임짐(Notification을 생성한다거나, Alert popup 을 띄우는 등의 UI 관련 항목 그리고 메시지의 저장 등은 App 에서 구현해야 함)

- (Push 설정 값 Server 전달 및 조회) Push Library 의 SetPushConfig/GetPushConfig API로 App 의 Push 수신 여부, 가능 시간 등을 서버에 저장 및 조회할 수 있음
- (설정 전달(SetPushConfig)) Push 등록 이후 SetPushConfig API를 호출할 수 있으며 파라미터는 아래와 같음

Parameter	필수 여부	설명
context	Y	API를 호출하는 context (일반적으로 Activity)
listener	Y	PushSetConfigListener의 instance, 이 리스너의 didSetConfigResult로 결과가 리턴됨
pushYn	N	앱 등록 시에 정보만 올려놓고 Push 수신은 하지 않는 등의 경우에 사용됨 Y : Push 수신 허용(default) N : Push 수신 차단
userCN(userId)	N	사용자의 id 값 : 변경을 원할 때 사용됨
CpDeviceId	N	단말 고유 값, 어떤 값을 넣어도 관계 없으나 단말 별로 Unique 한 값이어야 함(예를 들어 전화번호 등) : 변경을 원할 때 사용됨
startTime	N	Push 수신 가능 시작시간, default : 0000 (00시 00분) * startTime, endTime 은 pushYn 이 Y 인 경우에만 유효함
endTime	N	Push 수신 가능 종료시간, default : 2359 (23시 59분) * startTime, endTime 은 pushYn 이 Y 인 경우에만 유효함

## - Return Value

ErrorCode	Member Variable Name	설명
1400	OK	API 정상 호출
1401	CONTEXT_NOT_VALID	context 파라미터가 유효하지 않음
1402	SERVER_ADDRESS_NOT_VALID	iPNS 서버 주소가 유효하지 않음
1403	APP_ID_NOT_VALID	app id 가 유효하지 않음
1404	DEVICE_ID_NOT_VALID	단말의 DeviceID(Android ID) 가 유효하지 않습니다.
1405	AGENT_NOT_INSTALLED	Push Agent 미설치 상태입니다.
1408	REQUEST_ID_MISSING	request id 가 존재하지 않습니다.
1409	RESULT_DATA_MISSING	result data 가 존재하지 않습니다.
1410	SENDING_MSG_NULL	전송 메시지가 null 입니다.
1411	LISTENER_IS_NULL	listener 가 null 입니다.
1412	HOST_UNREACHABLE	서버 네트워크 연결 실패
1499	UNKNOWN_ERROR	알 수 없는 오류가 발생하였습니다.

- 처리 결과 값은 첫번째 파라미터인 PushSetConfigListener의 interface인 did SetConfigResult로 비동기 전달됨
- 이 API의 파라미터인 Bundle값으로 상세 결과가 전달되며
- RT값이 "0000"이면서 RT\_MGS값이 "Success"이면 성공, 그렇지 않으면 실패를 의미함

Parameter	필수 여부	설명
RT	Y	0000 인 경우 정상 그 이외에는 처리실패
RT_MSG	Y	성공인 경우 성공 메시지, 실패된 경우 실패 사유 등을 전달

- 아래는 Server로 설정값을 전달 및 결과를 수신하는 방법임

## SetPushConfig

```

//setStart 후 SetPushConfig 호출 부분
int result = -1;
if (PushLibrary.getInstance().getContext() == null || PushLibrary.getInstance().getAppId() == null ||
PushLibrary.getInstance().getSvrAddress() == null) {
    result = PushLibrary.getInstance().setStart(getContext(), pushSetting.getInterfaceServerUrl(),
pushSetting.getAppId());
} else {
    result = 1400;
}
if (result == 1400) {
    result = PushLibrary.getInstance().SetPushConfig(getContext(), new PushSetConfigListener() {
        @Override
        public void didSetConfigResult(Bundle bundle) {
            if (bundle != null) {
                String rt = bundle.getString(PushLibraryConstant.EXTRA_RT);
                String rtMsg = bundle.getString(PushLibraryConstant.EXTRA_RT_MSG);
                Log.d(TAG, "rtMsg : " + rtMsg);
                if (rt != null && rt.equals("0000")) {
                    //Successful!
                    if(pushSetting==null || !pushSetting.isValid()) {
                        pushSetting = MainActivity.realm.where(PushSetting.class).findFirst();
                    }
                    if (pushSetting != null) {
                        MainActivity.realm.beginTransaction();
                        pushSetting.setbPushAllowed(isChecked);
                        pushSetting.setUserId(userCnStr);
                        pushSetting.setStartTime(localStartTime);
                        pushSetting.setEndTime(localEndTime);
                        MainActivity.realm.commitTransaction();
                    } else {
                        Log.w(TAG, "PushSetting should exist...");
                    }
                } else if (rt == null) {
                    //Something's wrong.
                } else {
                    //See RT Code.
                }
            }
        }
    }, isChecked ? "Y" : "N",TextUtils.isEmpty(userCnStr) ? USER_CN : userCnStr, deviceCnStr, localStartTime,
localEndTime);
    if(result==1400)

```

- (설정 조회(GetPushConfig)) Push등록 이후에 GetPushConfig를 호출하면 서버에 저장되어 있는 해당 단말의 설정값을 가져올 수 있음

- Parameter

Parameter	필수 여부	설명
context	Y	API를 호출하는 context (일반적으로 Activity)
listener	Y	PushSetConfigListener의 instance, 이 리스너의 didSetConfigResult로 결과가 리턴됨

- Return Value

ErrorCode	Member Variable Name	설명
1400	OK	API 정상 호출
1401	CONTEXT_NOT_VALID	context 파라미터가 유효하지 않음
1402	SERVER_ADDRESS_NOT_VALID	iPNS 서버 주소가 유효하지 않음
1403	APP_ID_NOT_VALID	app id 가 유효하지 않음
1404	DEVICE_ID_NOT_VALID	단말의 DeviceID(Android ID) 가 유효하지 않음
1405	AGENT_NOT_INSTALLED	Push Agent 미설치 상태
1408	REQUEST_ID_MISSING	request id 가 존재하지 않음
1409	RESULT_DATA_MISSING	result data 가 존재하지 않음
1410	SENDING_MSG_NULL	전송 메시지가 null임
1411	LISTENER_IS_NULL	listener 가 null임
1412	HOST_UNREACHABLE	서버 네트워크 연결 실패
1499	UNKNOWN_ERROR	알 수 없는 오류가 발생함

- 처리결과에 대한 리턴 값은 첫번째 파라미터인PushGetConfigListener의 interface인 didGetConfigResult로 전달됨

Parameter	필수 여부	설명
RT	Y	0000 인 경우 정상 그 이외에는 처리실패
RT_MSG	Y	성공인 경우 성공 메시지, 실패된 경우 실패 사유 등을 전달
PUSH_YN	Y	Push 메시지 수신 여부, Y 인 경우 수신이며 N 인 경우 수신거부
PUSH_STIME	Y	Push 수신 가능 시작 시간 (0000 - 2359 까지)
PUSH_ETIME	Y	Push 수신 가능 종료 시간 (0000 - 2359 까지)

- 이 API의 파라미터인 Bundle값으로 상세 결과가 전달되며
- RT값이 "0000"이면서 RT\_MGS값이 "Success"이면 성공, 그렇지 않으면 실패를 의미함
- 상세 설정 값은 아래 예제를 참조
- 다음은 Push Server로부터 단말의 개별 설정값을 조회하는 방법임

#### GetPushConfig

```
PushLibrary.getInstance().GetPushConfig(new PushGetConfigListener() {  
    @Override  
    public void didGetConfigResult(Bundle bundle) {  
        String rt = bundle.getString("RT");  
        String rt_msg = bundle.getString("RT_MSG");  
        if (rt != null && rt.equals("0000")) {  
            String pushYn = bundle.getString("PUSH_YN");  
            String startTime = bundle.getString("PUSH_STIME");  
            String endTime = bundle.getString("PUSH_ETIME");  
        } else if (rt == null) {  
            //fail  
        } else {  
            //fail  
        }  
    }  
});
```

## □ MDM 시스템

### ○ MDM 인터페이스 구조



### ○ MDM 통제 기능

- 하드웨어(카메라, 마이크)
- 통신 경로(USB, WiFi, Bluetooth, NFC, 적외선)
- 소프트웨어 설치 및 실행 제어
- 데이터 보호(원격 잠금, 원격 삭제)
- 상태 정보 감시(운영체제 변조, 통신 불가) 등

### ○ 기본 MDM 정책 : 국가정보원 보안성 검토 준수

- 기본 탑재 앱 : 국가정보원 보안성 검토 준수 및 앱 검증완료 이후 MDM에서 정책 허용
- 이용 기관 추가 탑재 앱 : NIA에서 앱 검증 이후 운영센터로 MDM 정책 허용에 대한 공문 발송
- WiFi, 블루투스, 테더링 등 국가정보원에 허용하지 않은 기능 : 사용기관에서 사전 국가정보원 보안성 검토를 득하고 재난안전통신망 관리과의 협의가 완료된 이후 MDM 정책을 반영함

## ○ MDM 인터페이스 명세 : A2-MSR-DIF-CMD-MDM-00001 (단말 통제 요청)

## - Request

프로그램명	MDM 패키지							
참조테이블	https://mdm.safenet.go.kr:8443/mdm/api/control/request							
번호	데이터 정의							
	데이터항목 한글명	Table/Structure 명	Column/Field 명	유형	길이	필수여부	기본값	특이사항
1	시스템 아이디		systemId	String	20	Y		MDM 서버 발급
2	인증키		authKey	String	20	Y		MDM 서버 발급
3	단말 아이디 유형		devIdType	String	2	Y		00 : IMEI 01 : MSISDN
4	단말 아이디		devId	String	20	Y		단말 아이디 유형에 따라 설정 (01312341234)
5	액션 코드		actCd	String	20	Y		LOCK : 단말 잠금 UNLOCK : 잠금 해제 RESET : 공장초기화 CONTROL : 장치 제어
6	예약 전송 일시		resvDt	String	14	N		공백일 경우 즉시 전송 처리 (YYYYMMDDHHMMSS)
7	잠금 메시지		lockMsg	String	300	N		액션코드가 'LOCK'일 경우 옵션
8	통제 데이터		controlData	Object	-	N		액션코드가 'CONTROL'일 경우 옵션
9	카메라		Camera	String	5	N	Allow	Allow : 허용 / Deny : 차단
10	마이크		Mic	String	5	N	Allow	이하 상동
11	GPS		GPS	String	5	N	Allow	
12	와이파이		Wifi	String	5	N	Allow	
13	블루투스		Bluetooth	String	5	N	Allow	
14	USB		USB	String	5	N	Allow	
15	NFC		NFC	String	5	N	Allow	
16	테더링		Tethering	String	5	N	Allow	
17	화면캡처		Screenshot	String	5	N	Allow	
18	브라우저		Browser	String	5	N	Allow	
19	OS 업그레이드		OTAUpgrade	String	5	N	Allow	
20	공장초기화		FactoryReset	String	5	N	Allow	
21	시간변경		TimeChange	String	5	N	Allow	
22	추가 필드		extra	String	1024			
23	카메라		Camera	String	5	N	Allow	
24	마이크		Mic	String	5	N	Allow	
25	GPS		GPS	String	5	N	Allow	

## - Response

번호	데이터 정의							
	데이터항목 한글명	Table/Structure 명	Column/Field 명	유형	길이	필수여부	기본값	특이사항
1	요청 일련번호		reqSeq	String	20			
2	결과 코드		returnCode	String	4	Y		요청 수신 결과 코드 ('0000'일 경우 성공)
3	결과 메시지		returnMessage	String	100	Y		결과 메시지 또는 실패 사유

- MDM 인터페이스 명세 : A2-MSR-DIF-CMD-MDM-00002 (단말 유/무효화 요청 상태 조회)

- Request

프로그램명	MDM 패키지							
참조테이블	https://mdm.safenet.go.kr:8443/mdm/api/control/request/status							
번호	데이터 정의							
	데이터항목 한글명	Table/Structure 명	Column/Field 명	유형	길이	필수여부	기본값	특이사항
1	시스템 아이디		SYSTEM_ID	String	20	Y		MDM 서버 발급
2	인증키		AUTH_KEY	String	20	Y		MDM 서버 발급
3	요청 일련번호		REQ_SEQ	String	20	Y		단말 유/무효화 요청 시 회신된 요청 일련번호

- Response

번호	데이터 정의							
	데이터항목 한글명	Table/Structure 명	Column/Field 명	유형	길이	필수여부	기본값	특이사항
1	요청 상태정보		STTUS_CD	String	3	Y		000 : Stand By 001 : Processing 007 : Success 008 : Fail 009 : Cancel
2	처리 일시		EXEC_DT	String	14	N		STTUS_CD 정보가 002, 003, 009 일 경우 제공
3	추가 필드		EXTRA	String	1024	N		



## ○ MDM 인터페이스 명세 : A2-MSR-DIF-CMD-MDM-00003 (단말 잠금 상태 조회)

## - Request

프로그램명	MDM 패키지							
참조테이블	https://mdm.safenet.go.kr:8443/mdm/api/devicelock/status							
번호	데이터 정의							
	데이터항목 한글명	Table/Structure 명	Column/Field 명	유형	길이	필수여부	기본값	특이사항
1	시스템 아이디		SYSTEM_ID	String	20	Y		MDM 서버 발급
2	인증키		AUTH_KEY	String	20	Y		MDM 서버 발급
3	단말 아이디 유형		DEV_ID_TYPE	String	2	Y		00 : IMEI 01 : MSISDN
4	단말 아이디		DEV_ID	String	20	Y		단말 아이디 유형에 따라 설정

## - Response

번호	데이터 정의							
	데이터항목 한글명	Table/Structure 명	Column/Field 명	유형	길이	필수여부	기본값	특이사항
1	단말 상태 코드		DEV_STTUS_CD	String	20	Y		LOCK : 단말 잠금 UNLOCK : 잠금 해제
2	추가 필드		EXTRA	String	1024			

## ○ MDM 인터페이스 명세 : A2-MSR-DIF-CMD-MDM-00004 (단말 통제 상태 조회)

## - Request

프로그램명	MDM 패키지							
참조데이터	https://mdm.safenet.go.kr:8443/mdm/api/peripheral/status							
번호	데이터 정의							
	데이터항목 한글명	Table/Structure 명	Column/Field 명	유형	길이	필수여부	기본값	특이사항
1	시스템 아이디		systemId	String	20	Y		MDM 서버 발급
2	인증키		authKey	String	20	Y		MDM 서버 발급
3	단말 아이디 유형		devIdType	String	2	Y		00 : IMEI 01 : MSISDN
4	단말 아이디		devId	String	20	Y		단말 아이디 유형에 따라 설정

## - Response

번호	데이터 정의							
	데이터항목 한글명	Table/Structure 명	Column/Field 명	유형	길이	필수여부	기본값	특이사항
1	결과 코드		returnCode	String	4	Y		요청 수신 결과 코드 ('0000'일 경우 성공 )
2	결과 메시지		returnMessage	String	100	Y		결과 메시지 또는 실패 사유
3	통제 데이터		controlData	Object	-	N		결과코드가 '0000'일 경우 옵션
4	카메라		Camera	String	5	N		Allow : 허용 / Deny : 차단
5	마이크		Mic	String	5	N		상동
6	GPS		GPS	String	5	N		
7	와이파이		Wifi	String	5	N		
8	블루투스		Bluetooth	String	5	N		
9	USB		USB	String	5	N		
10	NFC		NFC	String	5	N		
11	테더링		Tethering	String	5	N		
12	화면캡처		Screenshot	String	5	N		
13	브라우저		Browser	String	5	N		
14	OS 업그레이드		OTAUpgrade	String	5	N		
15	공장초기화		FactoryReset	String	5	N		
16	시간변경		TimeChange	String	5	N		



## [부 록]

## [부록 A] 용어

○ 4G<sup>2)</sup>

4세대 이동통신이며, 제3세대 이후 3GPP 릴리스 14까지를 의미한다. 3GPP의 상표명은 엘티이(LTE), 엘티이 어드밴스트(LTE-Advanced), 엘티이 어드밴스트 프로(LTE-Advanced Pro)이다.

○ 5G<sup>3)</sup>

국제 전기 통신 연합(ITU)에서 정한 공식 명칭은 아이엠티 2020(IMT-2020)이지만, 이동통신 시장에서는 세대로 구분하여 5세대(5G) 용어를 사용하며, 3GPP 릴리스 15부터 해당한다.

## ○ Non Mission Critical(논 미션크리티컬)

미션크리티컬에 반대되는 용어이며, 재난안전통신망 등을 위하여 정해진 요구사항을 만족하는 수준이 되지 않는 것을 의미한다. 그러므로 QoS 관리, 매우 높은 신뢰성 등이 필요로 하지는 않는다.

## ○ UE 또는 Terminal(단말기)

일반적으로 단말기란 다음과 같은 두 가지의 의미가 있다:

① 디지털 자료전송 시스템에서 자료를 만들거나 보기 위한 기기. 혹은 자료를 보내거나 받기 위한 기능을 수행하는 기기로서 사람과 직접 대면하게 되는 자료 처리의 기본 기기이다.

② 정보가 통신망에서 입출력되는 지점. 재난안전통신망에서는 음성 및 영상통화, 비상시 통화, 그룹 통화, 데이터 통신, eMBMS, 단말 간 통화, 단말 위치 제공 등과 같이 재난안전 업무에 특화된 서비스 기능을 갖춘 단말기를 말한다. 휴대용, 차량용, 고정용 단말기로 구분된다. 사물인터넷 단말기를 포함한다.

## ○ App(모바일 앱)

스마트폰 등 모바일 기기 운영체제(OS)에 최적화되어 단독으로 실행될 수 있도록 개발된 애플리케이션(application)을 말한다. 애플리케이션 스토어(Application Store)를 통해 필요한 모바일 앱을 구매·내려받고 스마트폰 등 모바일 기기에 설치하여 이용할 수 있다.

## ○ Mission Critical(미션크리티컬)

재난안전통신망 등을 위하여 정해진 요구사항을 만족한 수준을 의미한다. 이를 위하여는 QoS 관리, 매우 높은 신뢰성 등이 필요하다.

2) [http://terms.tta.or.kr/dictionary/dictionaryView.do?word\\_seq=166870-6](http://terms.tta.or.kr/dictionary/dictionaryView.do?word_seq=166870-6)

3) [http://terms.tta.or.kr/dictionary/dictionaryView.do?word\\_seq=166870-6](http://terms.tta.or.kr/dictionary/dictionaryView.do?word_seq=166870-6)

○ Server(서버)

통신망 상에서 다른 컴퓨터에 대하여 그 통신망의 전부 또는 일부에 대한 접속과 그 통신망의 자원(디스크 장치, 파일, 프린터 등)에 대한 접속을 제어하는 관리 소프트웨어를 운용하는 컴퓨터나 장치 또는 프로그램이다. 응용서비스를 구현하기 위해서는 중심에 위치하는 서버와 종단에 위치하는 단말기로 구성된다.

○ Software Development Kit(소프트웨어 개발 키트) SDK<sup>4)</sup>

응용프로그램의 개발을 간편하고 쉽게 하도록 제공되는 특정 환경이나 플랫폼 기반의 종합 개발 도구. 원래는 마이크로소프트사가 윈도우 응용프로그램을 개발하는 프로그래머들을 위해 만든 고급 응용프로그램 인터페이스(API: Application Programming Interface)를 의미했으나 개발 도구 및 라이브러리, 관련 문서 세트 등을 의미하는 일반 용어로도 사용된다.

○ 신규 서비스

사용기관들이 재난안전통신망에서 기본적으로 받는 서비스 이외에 사용기관별로 재난안전 업무를 효율적으로 수행하기 위해 신규로 도입하는 서비스를 말한다.

○ 싱글사인온

단 한 번의 로그인만으로 여러 서비스에 접속하게 해주는 보안 응용 솔루션이다.

○ 애플리케이션 스토어(Application Store)

개발된 모바일 앱을 모아두고 자유롭게 사고팔 수 있는 온라인장터(Marketplace)를 뜻하며, 통상 앱스토어(App Store)로 줄여서 통칭한다.

○ OPEN Source(오픈소스)<sup>5)</sup>

일정한 이용 조건을 지키면 누구나 개량하고, 재배포할 수 있도록 무상으로 공개되는 소스 코드(source code)이다. 소스 코드를 비밀로 유지하려는 독점(사유)의 반대되는 운동으로, 소스 코드나 표준을 공개하여 자유로운 개작, 재배포 등을 허용하면서도 저작권자의 권익을 보호하고, 공동 개발을 장려하는 소프트웨어업계의 뚜렷한 하나의 제도화된 흐름이다. 공개 소스 저작자는 저작권은 소유하나 일반 공중 라이선스(GPL: General Public License), BSD(Berkeley Software Distribution) 라이선스, 또는 이를 준용한 라이선스 형태로 소스 코드를 공개하여 자유로운 개선, 개작 및 재배포를 허용하며, 그 결과물 또한 라이선스 규정에 따르도록 규정된다. 1998년 11월에 결성된 오픈 소스 이니셔티브(OSI: Open Source Initiative)가 공개 소스의 보급, 검증 및 인증 업무를 주관하고 있다.

4) [http://terms.tta.or.kr/dictionary/dictionaryView.do?word\\_seq=056171-2](http://terms.tta.or.kr/dictionary/dictionaryView.do?word_seq=056171-2)

5) [http://terms.tta.or.kr/dictionary/dictionaryView.do?word\\_seq=051000-4](http://terms.tta.or.kr/dictionary/dictionaryView.do?word_seq=051000-4)

○ OneM2M one Machine-To-Machine(원엠투엠)<sup>6)</sup>

사물 통신(M2M) 분야 글로벌 표준화 협력체이다. 원엠투엠(oneM2M)에는 세계 표준화 단체인 한국정보통신기술협회(TTA), 유럽전기통신협회(ETSI), 미국 통신정보 표준협회(ATIS)와 통신산업협회(TTA), 중국통신표준협회(CCSA), 일본 전파산업협회(ARIB)가 중심이 되고 이에 속한 수많은 기업과 연구기관, 대학 등이 참여하고 있다. 협력체는 공통 M2M 서비스 플랫폼 표준 개발을 위한 사용 예(Use Case) 및 요구 사항, 단 대단(End-to-End) M2M 아키텍처 및 서비스 계층(플랫폼) 표준, M2M 단말·모듈 측면의 공통 사용 예 및 인터페이스, API(Application Programming Interface) 등의 업무를 추진한다.

○ 응용 앱

응용서비스를 구현하기 위하여 작성된 애플리케이션을 말한다.

○ 사용기관

「재난 및 안전관리 기본법」제3조에 따른 재난관리책임기관, 긴급구조기관, 긴급구조 지원기관 중에서 재난안전통신망을 사용하는 기관을 말한다.

○ 재난안전통신망

「재난 및 안전관리 기본법」제3조에 따른 재난관리책임기관·긴급 구조기관이나 긴급 구조지원기관이 재난관리업무에 사용하거나 재난 현장에서의 통합지휘에 활용하기 위하여 구축·운영하는 무선통신망을 말한다. 소방·경찰·군·지방자치단체 등 재난 대응 기관들이 각기 독립적으로 운용하는 무선통신망을 단일망으로 통합하여 재난 현장에서 일사불란한 지휘·협조 체제를 통해 움직일 수 있도록 하는 통합 재난안전통신 망을 말한다.

○ 재난안전통신망용 모바일 앱

재난안전통신망 응용서비스를 사용기관에서 평시 또는 재난 시 실제 업무에서 사용하기 위한 앱으로서 재난안전통신망 전용 단말기에서 설치되며, 재난안전통신망을 이용하여 공공안전을 위한 기능들을 제공하도록 개발된 애플리케이션(Application)이다.

○ 전환 서비스

사용기관들이 이미 운영 중인 자체 통신망 또는 상용 통신망 기반의 재난안전 서비스를 재난안전통신망으로 전환하여 사용하고자 하는 서비스를 말한다.

6) [http://terms.tta.or.kr/dictionary/dictionaryView.do?word\\_seq=050809-3](http://terms.tta.or.kr/dictionary/dictionaryView.do?word_seq=050809-3)

### ○ Zig Bee(지그비)<sup>7)</sup>

저속, 저비용, 저전력의 무선망을 위한 기술. 주로 양방향 무선 개인 영역 통신망(WPAN) 기반의 홈 네트워크 및 무선 센서망에서 사용되는 기술로 지그비 얼라이언스(zig bee alliance)에서 IEEE 802.15.4 물리 계층(PHY, MAC) 표준 기술을 기반으로 상위 프로토콜 및 응용 프로파일을 표준화하였다. 버튼 하나의 동작으로 집안 어느 곳에서나 전등 제어 및 홈 보안 시스템을 제어 관리할 수 있고, 인터넷을 통한 전화 접속으로 가정 자동화를 더욱 편리하게 달성하려는 것에서부터 출발한 기술이다. 지그비(ZigBee)는 세계 대부분 지역에서 ISM(Industrial Scientific Medical band) 밴드인 2.4 GHz 무선 주파수 대역에서 동작하지만, 무선랜(WLAN), 블루투스(Bluetooth)와 같이 동일 주파수 대역을 사용하는 무선기술들과의 간섭을 피하려고 868MHz, 915MHz 주파수 대역도 사용된다. 변조 방식은 직접 시퀀스 확산 스펙트럼(DS-SS) 방식이며, 데이터 전송 속도는 20~250kbps이다.

### ○ 지령장치

재난 관련 기관의 상황실과 현장에 간 지휘·명령, 상황 보고 등의 통신 업무를 효율적으로 수행하기 위한 지휘자용 관제 장치

### ○ Z-Wave(지웨이브)<sup>8)</sup>

젤 시스(Zensys) 사가 주축이 된 지웨이브 얼라이언스(Z-Wave Alliance)에서 제정한 가정 자동화(home automation) 무선 전송 방식 표준. 900MHz대 주파수로 10~40kbps의 전송속도를 갖는 무선 RF 기술로 양방향 통신을 지원하는 무선 메시 기술을 사용하며 지그비(ZigBee)에 비해 전력 효율이 우수하다.

### ○ NB-IOT, NarrowBand-Internet of Things(협대역 사물 인터넷)<sup>9)</sup>

엘티이(LTE) 기술 기반으로 사물인터넷을 효율적으로 제공하는 저전력 광역 통신 표준 기술이다. 180kHz의 좁은 대역으로 최대 250kbps의 데이터 전송 속도와 10km 이상의 광역 서비스를 지원하고, 이동성은 지원하지 않는다. 수도·가스·온도·전기 등 검침 센서, 스마트 조명, 위치추적 기기 등과 같이 원거리에 있고 데이터 사용 빈도와 전력 소비가 적으며 이동성이 없거나 낮은 사물인터넷(IoT) 기기에 적합하다.

7) [http://terms.tta.or.kr/dictionary/dictionaryView.do?word\\_seq=078206-1](http://terms.tta.or.kr/dictionary/dictionaryView.do?word_seq=078206-1)

8) [http://terms.tta.or.kr/dictionary/dictionaryView.do?word\\_seq=060594-4](http://terms.tta.or.kr/dictionary/dictionaryView.do?word_seq=060594-4)

9) [http://terms.tta.or.kr/dictionary/dictionaryView.do?word\\_seq=081014-5](http://terms.tta.or.kr/dictionary/dictionaryView.do?word_seq=081014-5)

- Adaptive Multi-Rate Wideband, AMR-WB (광대역 적응형 다중 속도 음성 코덱)<sup>10)</sup>  
 적응형 다중 전송률 광대역 음성 부호화 방식. 적응형 다중 속도 음성 코덱(AMR) 또는 협대역 음성 코덱용 AMR-NB(AMR-narrowband)의 다음 버전이다. AMR-NB가 300 ~ 3,400Hz로 좁은 대역만을 지원하는 반면, AMR-WB는 50 ~ 7,000Hz로 광대역을 지원한다. 대수 부호 여진 선형 예측(ACELP: Algebraic Code Excited Linear Prediction) 기술을 쓰며, 6.6 ~ 23.85kbps 사이의 아홉 개 비트율을 제공한다. 이동 통신 3GPP나 유선 ITU-T G.722.2에서 표준으로 택하고 있다.
- Android(안드로이드)<sup>11)</sup>  
 구글이 공개한 개방형 모바일 운영체제. 안드로이드는 운영체제(OS)와 미들웨어, 사용자 인터페이스(UI), 브라우저, 애플리케이션 등으로 구성되어 있고, 터치스크린 기능, 쿼티(QWERTY) 자판, 웹 서핑, 지도 검색, 온라인 인스턴트 메신저 등 다양한 기능을 제공하여 스마트폰과 태블릿 PC 같은 모바일 기기에 사용된다.
- Cat.M1<sup>12)</sup>  
 LTE Category M1의 약어. LTE Cat.M1 표준은 속도를 높여 데이터 전송량을 늘렸다. 전송속도는 300kbps로, 사물 이동통신(IoT) 표준 기술인 로라(LoRa, 5.5kbps)보다 50배 이상, 협대역 사물인터넷(NB-IoT, 최고 27kbps)보다 10배 이상 빠르다. 저용량 동영상, 고화질 사진과 음성 전송, 인증 및 결제 서비스 등이 가능하다. LTE Cat.M1을 적용하면 전력 소비가 적어 이동성이 증가한다. 전력 소비효율은 초기 LTE 기반 IoT 기술인 LTE-M보다 수십 배 높다. 배터리 수명도 수년까지 길어진다. 대규모 사물인터넷에 최적화됐다는 평가이다.
- Cellular Internet of Things, CloT  
 EC-GSM-IoT, LTE-M 및 NB-IoT를 망라하는 셀룰라 시스템에서의 IoT를 의미한다.
- Configuration Management(구성관리)<sup>13)</sup>  
 그룹 관리와 관련이 없는 미션크리티컬 서비스 애플리케이션을 구성관리하는 기능이다. 3GPP 릴리스 14부터 미션크리티컬 PTT, 미션크리티컬 비디오 및 미션크리티컬 데이터 모두에 공통으로 이용될 수 있는 공통적인 구조로 변경되었다. 재난안전통신망이 이러한 구조로 업그레이드되면 응용서비스에서도 이를 활용할 수 있게 될 것이다.

10) [http://terms.tta.or.kr/dictionary/dictionaryView.do?word\\_seq=035444-2](http://terms.tta.or.kr/dictionary/dictionaryView.do?word_seq=035444-2)

11) [http://terms.tta.or.kr/dictionary/dictionaryView.do?word\\_seq=035882-3](http://terms.tta.or.kr/dictionary/dictionaryView.do?word_seq=035882-3)

12) [http://terms.tta.or.kr/dictionary/dictionaryView.do?word\\_seq=168453-4](http://terms.tta.or.kr/dictionary/dictionaryView.do?word_seq=168453-4)

13) 3GPP TS 23.280 V14.6.0 cl.7.4.2.2.2



- Dynamic Host Configuration Protocol, DHCP (동적 호스트 설정 통신 규약)<sup>14)</sup>

프로토콜로서 동적 호스트 설정 통신 규약(DHCP) 서버는 DHCP 클라이언트의 요구에 따라서 IP 주소를 할당하는 한편, BOOTP는 서버/클라이언트 간에 주고받는 것을 담당한다. 초기 적재 통신 규약을 확장한 통신 규약으로서 할당된 IP 주소에 임대 기간을 설정할 수 있는 점이 초기 적재 통신 규약과 다르다.
- D2D  
Device to Device의 약어이며, 망의 기지국을 경유하지 않는 단말기 간의 직접통신을 의미한다.
- EMS  
네트워크 환경에서 재난안전통신망 교환장비(EPC, IMS, MCPTT eMBMS) 등 통신망 장비를 원격으로 감시 및 제어
- ESM  
MCPTT 플랫폼 등 보안기기들을 효율적으로 운영하기 위해 중앙에서 통합 관제 기능을 한다.
- Event(이벤트)
  - ① 프로그램이 반응하도록 사용자가 생성시키는 동작 또는 일(사건)의 발생. 키보드의 키를 누르는 것이 대표적이다. 마우스 버튼을 클릭하는 것, 마우스를 이동하는 것 등이 있다. ② 프로그램이나 태스크의 수행에 영향을 미치는 동작 또는 일의 발생. 프로그램 주행 중의 입출력 동작의 완료 등이 있다.
- FOTA  
Firmware Over The Air의 약어이며, 재난안전통신망 단말기 하드웨어를 제어하는 펌웨어(Firmware)의 설치/실행에 대한 통제 기능을 한다.
- GBR  
비트률이 보장된다는 의미이며, GBR 베어러란 데이터 네트워크 상에서 예약된(보증된) 비트률의 리소스를 갖는 IP 네트워크 상의 베어러를 말한다.
- Group Management(그룹 관리)<sup>15)</sup>

미션크리티컬 서비스를 위하여 지원되는 그룹 관리기능이며 주로 단말기의 그룹 구성에 적용된다. 3GPP 릴리스 14부터 미션크리티컬 PTT, 미션크리티컬 비디오 및 미션크리티컬 데이터 모두에 공통으로 이용될 수 있는 공통적인 구조로 변경되었다. 재난안전통신망이 이러한 구조로 업그레이드되면 응용서비스에서도 이를 활용할 수 있게 될 것이다.

14) [http://terms.tta.or.kr/dictionary/dictionaryView.do?word\\_seq=042069-1](http://terms.tta.or.kr/dictionary/dictionaryView.do?word_seq=042069-1)

15) 3GPP TS 23.280 v14.6.0 cl 7.4.2.2.4

○ Identity Management(식별 관리)<sup>16)</sup>

미션크리티컬 서비스 ID의 인증 관리 기능이다. 3GPP 릴리스 14부터 미션크리티컬 PTT, 미션크리티컬 비디오 및 미션크리티컬 데이터 모두에 공통으로 이용될 수 있는 공통적인 구조로 변경되었다. 재난안전통신망이 이러한 구조로 업그레이드되면 응용 서비스에서도 이를 활용할 수 있게 될 것이다.

○ intent(인텐트)

수행될 동작의 내용

○ iOS

애플이 생산하는 제품 중 모바일 기기에 탑재되는 운영체제. Android와 달리 비개방형이다.

○ IPv4<sup>17)</sup>

IPv4는 인터넷 프로토콜의 4번째 판이며, 전 세계적으로 사용된 첫 번째 인터넷 프로토콜이다. IPv4의 주소체계는 총 12자리이며 네 부분으로 나뉜다. 각 부분은 0~255까지 3자리의 수로 표현된다. IPv4 주소는 32bit로 구성되어 있으며, 현재 인터넷 사용자의 증가로 인해 주소 공간의 고갈에 대한 우려가 커지고 있다. 이에 따라 대안으로 128bit 주소체계를 갖는 IPv6가 등장하였다.

○ IPv6<sup>18)</sup>

IPv6(Internet Protocol version 6)는 인터넷 프로토콜 스택 중 네트워크 계층의 프로토콜로서 버전 6 인터넷 프로토콜(version 6 Internet Protocol)로 제정된 차세대 인터넷 프로토콜을 말한다. 인터넷(Internet)은 IPv4 프로토콜로 구축됐으나 IPv4 프로토콜의 주소가 32bit라는 제한된 주소 공간 및 국가별로 할당된 주소가 거의 소진되고 있다는 한계점으로 인해 지속적인 인터넷 발전에 문제가 예상되어, 이에 대한 대안으로서 IPv6 프로토콜이 제안되었으며, 국제 표준이 RFC를 통해서 확정되었고, 실제로 IPv6 주소는 휴대전화나 컴퓨터에 할당되어 적용되고 있다.

○ Key Management(키 관리)<sup>19)</sup>

키 관리 기능이며, 주로 단말기에 적용된다. 3GPP 릴리스 14부터 미션크리티컬 PTT, 미션크리티컬 비디오 및 미션크리티컬 데이터 모두에 공통으로 이용될 수 있는 공통적인 구조로 변경되었다. 재난안전통신망이 이러한 구조로 업그레이드되면 응용 서비스에서도 이를 활용할 수 있게 될 것이다.

16) 3GPP TS 23.280 v14.6.0 cl 7.4.2.2.6

17) <https://ko.wikipedia.org/wiki/IPv4>

18) <https://ko.wikipedia.org/Wiki/IPv6>

19) 3GPP TS 23.280 v14.6.0 cl 7.4.2.2.8

○ Location Management(위치 관리)<sup>20)</sup>

단말기의 위치 정보에 대하여 관리하는 기능이다. 3GPP 릴리스 14부터 미션크리티컬 PTT, 미션크리티컬 비디오 및 미션크리티컬 데이터 모두에 공통으로 이용될 수 있는 공통적인 구조로 변경되었다. 재난안전통신망이 이러한 구조로 업그레이드되면 응용 서비스에서도 이를 활용할 수 있게 될 것이다.

○ Land Mobile Radio, LMR

브로드밴드 기술이 적용되기 이전의 무전 통신을 의미하며, 주파수 공유(트렁킹) 방식과 비주파수 공유(논트렁킹) 방식

○ LoRa(Long Range, 로라)<sup>21)</sup>

사물 간 통신(IoT)을 위한 저전력의 장거리 통신(LPWA, Low Power Wide Area) 기술

○ Low Power Wide Area, LPWA

사물 간 통신(IoT)을 위한 LoRa, Sigfox 등 저전력의 장거리 통신의 통칭

○ LTE

Long Term Evolution의 약자이며, 3GPP에서 추진한 4세대 이동통신 명칭이다.

○ LTE-M<sup>22)</sup>

LTE for Machine의 약자이며 기기와의 통신하는 분야의 LTE를 의미한다. 이에는 Category M1과 M2가 있다.

○ LTE-M1

LTE Category M1의 약어이며 eMTC (Enhanced Machine-Type Communication) 라고도 함. 기타 내용은 Cat.M1을 참조

○ LTE-Maritime, LTE-M.

해상통신에 이용하는 엘티이이다. 현재 700MHz 대역의 통합공공망 주파수를 재난 안전통신망과 함께 사용하며 재난안전통신망과 연동이 되어 있으며 일부 기지국을 RAN Sharing하고 있다.

○ LTE-Railway, LTE-R

철도통신에 이용하는 엘티이이며, 이를 기반으로 철도통합무선망이 구축되고 있다. 현재 700MHz 대역의 통합공공망 주파수를 재난안전통신망과 함께 사용하며, 전파 간섭 및 상호운용성 확보를 위해 재난안전통신망과 기지국 공유(RAN Sharing)하고 있다.

---

20) 3GPP TS 23.280 v14.6.0 cl 7.4.2.2.10

21) [http://terms.tta.or.kr/dictionary/dictionaryView.do?word\\_seq=173889-2](http://terms.tta.or.kr/dictionary/dictionaryView.do?word_seq=173889-2)

22) <https://en.wikipedia.org/wiki/LTE-M>

○ MCPTT

Mission Critical Push To Talk의 약자이며, 재난안전통신을 위한 엘티이(LTE) 기반의 푸시투토크(PTT) 서비스이다. MCPTT는 재난안전을 위해 특화된 기능을 제공한다. 주요 기능으로 단말기 간 개별, 그룹 및 비상 통화, 원격에 있는 특정 사용자 단말의 주변 소리를 임의로 청취, 긴급상황 시 운영센터에서 강제적으로 통화를 재발신하는 기능 등이 있다.

○ Mission Critical Service, MCS(미션크리티컬 서비스)

미션크리티컬 서비스 요구사항(QoS, KPI, 신뢰성 등)을 만족하는 서비스를 의미하며, Mission Critical PTT, Mission Critical Data 및 Mission Critical Video를 통칭한다.

○ Mobile Device Management, MDM

단말기에 설치하는 소프트웨어(S/W)의 설치/실행에 대한 통제 및 재난안전통신망 정책관리를 하는 기능을 한다.

○ Mesh

N/W 스스로 네트워크 환경을 인지, 통신하는 자가 통제 네트워크로, 다른 국을 향하는 모든 호출이 중계에 의하지 않고 직접 접속되는 그물(mesh) 모양의 네트워크이다.

○ Message Queuing Telemetry Transport, MQTT<sup>23)</sup>

사물 통신(M2M: Machine to Machine), 사물인터넷(IoT: Internet of Things)과 같이 대역폭이 제한된 통신환경에 최적화하여 개발된 푸시 기술(push technology) 기반의 경량 메시지 전송 프로토콜. 엠큐티티(MQTT) 프로토콜은 푸시 기술(push technology)에서 일반적으로 사용되는 클라이언트/서버 방식 대신, 메시지 매개자(broker)를 통해 송신자가 특정 메시지를 발행(publish)하고 수신자가 메시지를 구독(subscribe)하는 방식을 사용한다. 즉, 매개자(broker)를 통해 메시지가 송수신된다. 메시지 길이가 가장 짧게는 2바이트까지 가능하고, 초당 1,000단위의 메시지 전송이 될 수 있어 가볍고 빠르다는 장점이 있다. 따라서 원격 검침, 원격 의료 등 다양한 분야에 효율적으로 사용될 수 있다. MQTT는 아이비엠(IBM)사와 유로테크(Eurotech)가 공동 개발하였으며 2014년 국제 민간 표준 기구인 오아시스(OASIS) 표준으로 제정되었다.

23) [http://terms.tta.or.kr/dictionary/dictionaryView.do?word\\_seq=076451-6](http://terms.tta.or.kr/dictionary/dictionaryView.do?word_seq=076451-6)

○ Network Address Translation, NAT (네트워크 주소 변환)<sup>24)</sup>

사내의 개별 주소와 정식 IP 주소를 상호 변환하는 기능. 이러한 기능에 의해 개별 주소가 할당되지 않은 노드에서도 인터넷에 접속할 수 있다. TCP/IP의 전송 계층(transport layer)이나 응용 계층의 통신 규약에 대한 변환을 하여 특정 TCP/IP 응용을 이용하도록 한다. 패킷 헤더에 있는 발신원 주소와 IP 주소만 식별할 수 있으므로 개별 주소와 IP 주소의 대응은 항상 1:1이 되어야 한다. 그러므로 1개의 IP 주소를 사용해서 외부에 접속할 수 있는 노드는 어느 시점에서 1개만으로 제한되는 문제가 있으나, IP 매스커레이드(IPM: IP masquerade)를 이용하면 된다.

○ NB-IoT<sup>25)</sup>

전력 소모를 줄이기 위해 전력 절약 모드(PSM: Power Saving Mode)와 단말의 불연속 수신 향상 기술(eDRX: enhanced Discontinuous Reception) 등을 지원한다. 그리고 프로토콜의 복잡도를 낮추기 위해 이동성을 지원하지 않는다. NB-IoT 주파수 대역으로는, GSM 대역의 일부를 NB-IoT용으로 변경한 대역(standalone 모드), LTE 주파수 대역의 일부(in-band 모드) 또는 보호 대역(guard-band 모드) 등이 사용될 수 있다.

※ 정부 NB-IoT 기술 기준(2017): LTE 주파수인 800MHz 대역에서 829~849MHz(업로드) 및 874~894MHz(다운로드), 1.8GHz 대역에서 1735~1755MHz(업로드) 및 1830~1850MHz(다운로드)를 NB-IoT 주파수로 활용

## ○ Network Management System, NMS

재난안전통신망 장비의 장애, 구성, 계정, 성능, 보안 등의 관리정보를 수집·보관·분석

## ○ Non-GBR

특정 패킷을 전송 함에 있어서의 QoS 등급 구분이며, 리소스 형태, 패킷 지연 규격, 패킷 오류율로 특성을 정의한다.

## ○ Non-Mission Critical Service(논미션크리티컬 서비스)

미션크리티컬 서비스와 반대되는 개념으로써, 미션크리티컬 서비스 요구사항(QoS, KPI, 신뢰성 등)을 만족하지 않는 일반 서비스를 의미한다.

○ Open API<sup>26)</sup>

Open Application Programming interface의 약어이며, 누구나 사용할 수 있도록 공개된 API를 의미한다. 임의의 응용프로그램을 쉽게 만들 수 있도록 준비된 프로토콜, 도구 같은 집합으로 프로그램 개발자는 운영 상세한 기능은 몰라도 공개된 몇 개의 API만으로도 쉽게 응용프로그램을 개발할 수 있다.

24) [http://terms.tta.or.kr/dictionary/dictionaryView.do?word\\_seq=050110-1](http://terms.tta.or.kr/dictionary/dictionaryView.do?word_seq=050110-1)

25) [http://terms.tta.or.kr/dictionary/dictionaryView.do?word\\_seq=081014-5](http://terms.tta.or.kr/dictionary/dictionaryView.do?word_seq=081014-5)

26) [http://terms.tta.or.kr/dictionary/dictionaryView.do?word\\_seq=050924-1](http://terms.tta.or.kr/dictionary/dictionaryView.do?word_seq=050924-1)

예를 들어 구글이 제공하는 구글맵 API를 활용하면 개인의 웹 페이지에서도 구글맵과 같은 지도 서비스를 구현할 수 있다.

#### ○ Push<sup>27)</sup>

인터넷에서 클라이언트 측 사용자의 검색 조작에 의하지 않고 서버의 작용으로 서버상에 있는 정보를 클라이언트로 자동 배포(전송)하는 것이다. 클라이언트 측 사용자의 조작으로 서버로부터 정보를 검색하는 풀(pull)과 대칭된다.

#### ○ QoS class identifier(QCI)

특정 패킷을 전송 함에 있어서의 QoS 등급 구분이며, 리소스 형태, 패킷 지연 규격, 패킷 오류율로 특성을 정의한다.

#### ○ REST(레스트)<sup>28)</sup>

Representational state transfer의 약어이며, 웹서비스에 사용되는 일련의 제약을 정의하는 소프트웨어 아키텍처의 스타일이다. 확장성 마크업 언어(XML) 파일로 된 웹 페이지를 읽어서 원하는 정보를 수집하는 기능이다. 웹 페이지를 만드는 사람은 주기적으로 내용을 개정하고 사용자는 그 페이지의 URL만 알면 웹 브라우저로 읽어서 정보를 얻을 수 있다. 하이퍼텍스트 전송 규약(HTTP)과 XML을 포함한 웹 기술 및 프로토콜을 사용하는 구조적 형태로서 단순 객체 접근 통신 규약(SOAP)보다 사용이 간편하고, 사이트 내용을 기술하는 RSS(RDF Site Summary)의 정보 편집 기능과 유사하다. REST 아키텍처 스타일을 만족하는 웹서비스를 RESTful 웹서비스라 칭하며, 인터넷상에서 컴퓨터 시스템 간의 상호호환성을 제공한다.

#### ○ SigFox<sup>29)</sup>

2009년 설립된 프랑스 기업으로 사물 인터넷망의 효시가 된 기업이다. 시그폭스는 UNB(Ultra Narrow Band) 기술을 사용하며, 배터리 교체 없이 몇 년간 사용할 수 있는 저전력 기반의 사물 인터넷망 서비스를 제공하고 있다. 특히 주파수 사용료가 없는 비면허 주파수 대역을 사용하고 있다는 점이 특징이다.

#### ○ VoLTE<sup>30)</sup>

Voice over LTE의 약어이다. 엘티이(LTE: Long Term Evolution)와 아이엠티 어드밴스트(IMT-Advanced, 4세대 이동통신) 기술인 엘티이 어드밴스트(LTE-Advanced)의 IP 데이터망으로 음성 통화서비스를 제공하기 위한 기술.

27) [http://terms.tta.or.kr/dictionary/dictionaryView.do?word\\_seq=053314-1](http://terms.tta.or.kr/dictionary/dictionaryView.do?word_seq=053314-1)

28) [http://terms.tta.or.kr/dictionary/dictionaryView.do?word\\_seq=054309-3](http://terms.tta.or.kr/dictionary/dictionaryView.do?word_seq=054309-3),  
[https://en.wikipedia.org/wiki/Representational\\_state\\_transfer](https://en.wikipedia.org/wiki/Representational_state_transfer)

29) [http://www.hellot.net/\\_UPLOAD\\_FILES/magazine/source\\_file/source\\_1481774801.pdf](http://www.hellot.net/_UPLOAD_FILES/magazine/source_file/source_1481774801.pdf)

30) [http://terms.tta.or.kr/dictionary/dictionaryView.do?word\\_seq=059831-7](http://terms.tta.or.kr/dictionary/dictionaryView.do?word_seq=059831-7)

## [부록 B] 약어

3GPP	3rd Generation Partnership Project(쓰리지피피)
AI	Artificial Intelligence(인공 지능)
AMR	Adaptive Multi-Rate
API	Application Programming Interface(응용 프로그래밍 인터페이스)
APP	Application(응용)
BLE	Bluetooth Low Energy(저전력 블루투스)
BSS	Business Support Systems
DHCP	Dynamic Host Configuration Protocol
DMR	Digital Mobile Radio
DMZ	Demilitarized Zone
DNS	Domain Name System/ Domain Name Server
eMBMS	Enhanced Multimedia Broadcast Multicast Service
EMS	Entity Management System
eMTC	Enhanced Machine-Type Communication
EPC	Evolved Packet Core
ESM	Enterprise Security Management
FOTA	Firmware Over-The-Air
GBR	Guaranteed Bit Rate
GIS	Geographical Information System(지리 정보 시스템)
G/W	Gateway
HD	High Definition
IAM	Identity and Access Management(식별/접근 관리)
ICT	Information and Communications Technology(정보통신기술)
IMS	IP Multimedia Subsystem
IoT	Internet of Things(사물인터넷)
IT	Information Technology(정보 기술)
ITSM	Information Technology Service Management(정보 기술 서비스 관리)
LMR	Land Mobile Radio
LPWA	Low Power Wide Area
LPWAN	Low Power Wide Area Network
LTE	Long Term Evolution(엘티이)

LTE-M1	LTE Category M1
MDM	Mobile Device Management
MMS	Multimedia Messaging Service(멀티미디어 메시징 서비스)
MQTT	Message Queuing Telemetry Transport
NAT	Network Address Translation
NB	Narrow Band
NB-IoT	Narrow Band IoT
NMS	Network Management System(망 관리시스템)
NTP	Network Time Protocol(네트워크 타임 프로토콜)
N/W	Network
OS	Operating System
PS-LTE	Public Safety-LTE(피에스 엘티이)
QCI	QoS class identifier
SMS	Short Message Service(문자 메시지 서비스)
SQL	Structured Query Language(구조화 질의 언어)
SWB	Super Wide Band
S/W	Software
TCP	Transmission Control Protocol(전송 제어 프로토콜)
UE	User Equipment(단말기)
UI	User Interface(사용자 인터페이스) <sup>31)</sup>
UX	User Experience(사용자 경험) <sup>32)</sup>
UID	Unique Identifier
UMC	User Modified Content(사용자 변환 콘텐츠) <sup>33)</sup>
UTF-8	Unicode Transformation Format(유니코드 변환 형식)- 8
WB	Wide Band

31) [http://terms.tta.or.kr/dictionary/dictionaryView.do?word\\_seq=059271-1](http://terms.tta.or.kr/dictionary/dictionaryView.do?word_seq=059271-1)

32) [http://terms.tta.or.kr/dictionary/dictionaryView.do?word\\_seq=059261-1](http://terms.tta.or.kr/dictionary/dictionaryView.do?word_seq=059261-1)

33) [http://terms.tta.or.kr/dictionary/dictionaryView.do?word\\_seq=059279-1](http://terms.tta.or.kr/dictionary/dictionaryView.do?word_seq=059279-1)



## [부록 C] 참고 문헌

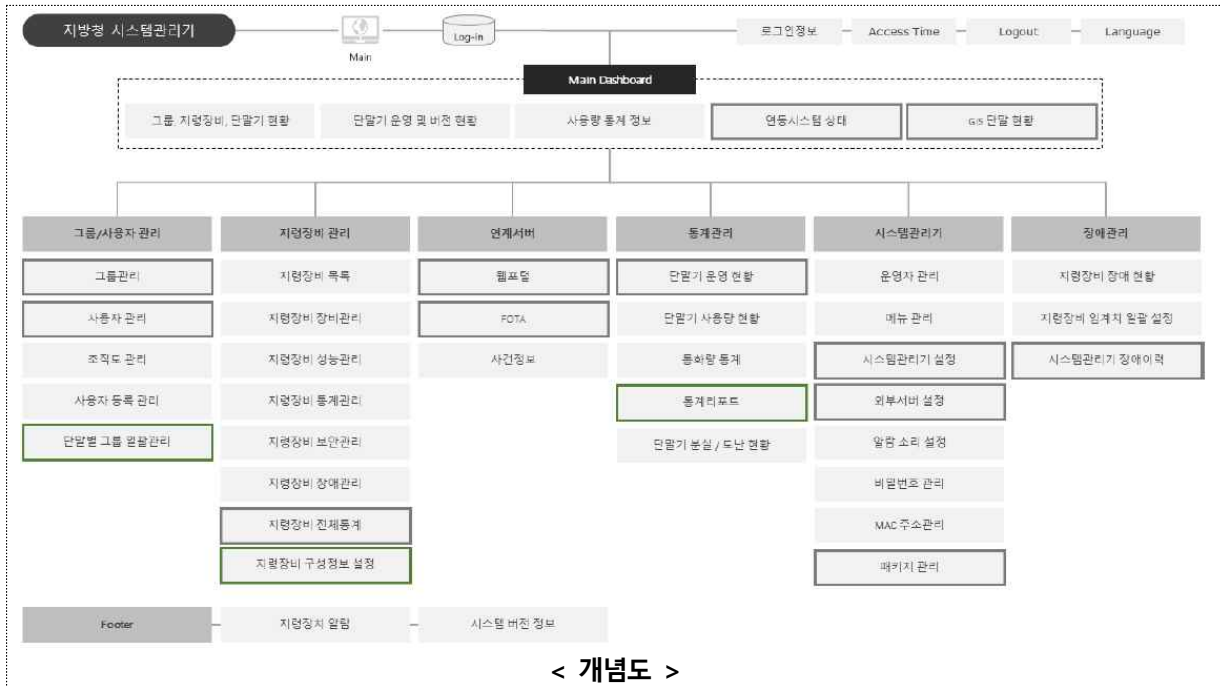
- [1] "FirstNet Developer Program," firstnet.com, 2020. [Online]. Available: <https://www.firstnet.com/apps/app-developer-program.html>.
- [2] "FirstNet IoT Solutions," firstnet.com, 2020. [Online]. Available: <https://www.firstnet.com/industry-solutions/iot.html>.
- [3] "FirstNet 모바일 앱," firstnet.com, 2020. [Online]. Available: <https://apps.firstnet.att.com/?auth=false>.
- [4] "KT API Link," KT, 2020. [온라인]. Available: <https://apilink.kt.co.kr/apilInfo/mvInfoView.do>.
- [5] "SKT IoT Portal," SKT, 2020. [온라인]. Available: <https://www.sktiot.com/iot/main/index>.
- [6] "SKT Open API," SKT, 2020. [온라인]. Available: <https://openapi.sk.com/>.
- [7] "정부사물인터넷 도입 가이드라인," 2019.
- [8] "IPv4/IPv6 변환기술", TTA 저널 79호, 2002
- [9] "TTAK.KO-06.0496 재난안전통신망 단말기 기술 규격", TTA, 2019

## [부록 D] 재난안전통신망 활용 장비·서비스 도입 사례

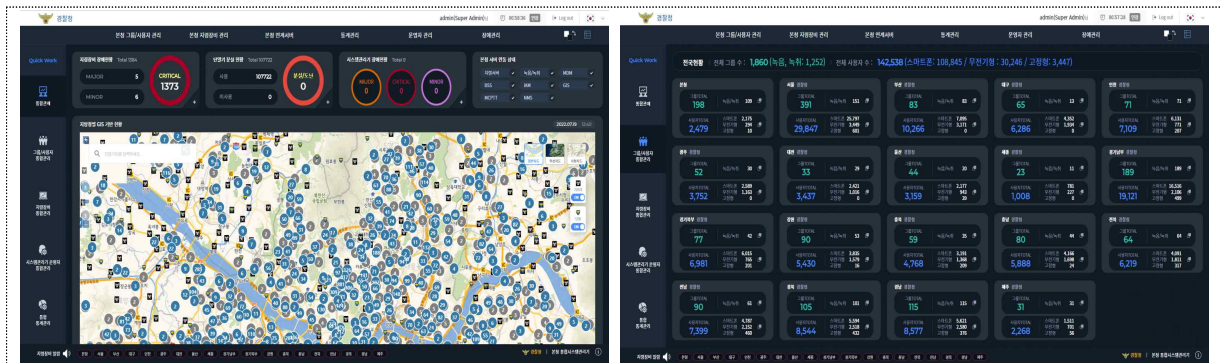
### D-1) 시스템 관리기

- 경찰청 본청의 지령서버, 통합시스템관리기, 행안부 운영센터와 연결하여 지방청 시스템관리기 통합 관제

※ 출처 : 행정안전부



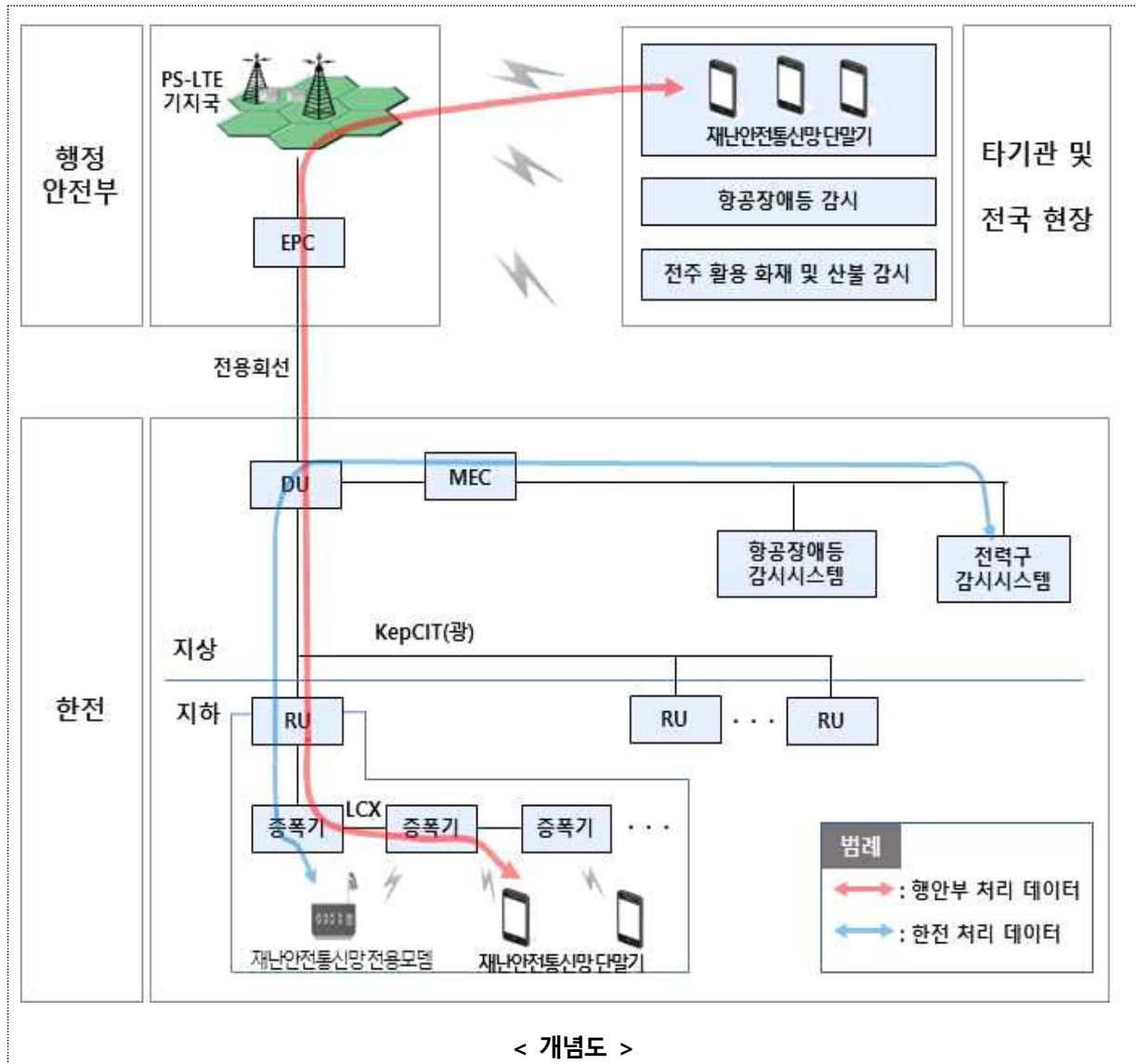
기능명	설명
그룹/사용자 관리	• 그룹, 사용자(단말), 조직도에 대한 정보를 상세보기 및 등록, 수정, 삭제
외부연동 관리	• 조직 별 단말 상태 통계, 앱(FOTA) 연동, 사건정보 설정
통계 관리	• 조직별 단말기 운영현황, 사용자 현황, 통화량 통계, 통계리포트 보기/출력, 단말기 변경이력에 대한 현황 출력
시스템관리기 관리	• 계정 등록, 수정 삭제 및 메뉴 권한설정, 환경설정을 통해 관리
장애관리	• 지령장비 장애현황, 임계치 설정, 시스템관리기 장애 현황 파악
지령장비 관리	• 지령장비에 대한 장비, 성능, 통계, 보안, 장애 관리



## D-2) 재난안전통신망을 활용한 지하전력구 무선통신망 시설

- 지하전력구 내 재난안전 감시정보 취득용 전용모뎀을 활용하여 LTE 방식 기반 고속데이터 전송 서비스 활용
  - 재해재난 상황 대비 관련 기관(지자체·경찰·소방 등)과의 통신수단 확보
  - 전력설비 장애 시 신속한 고장복구 지원 위한 무선통신수단 신뢰성 확보
  - 일반업무 및 긴급상황 발생시 음성 + 영상통화 가능
  - 현재 다양한 음성단말기 종류를 재난안전통신망 단말기로 일원화 가능
  - 전력구 내 다양한 신기술 현장 적용을 위한 무선인프라 제공

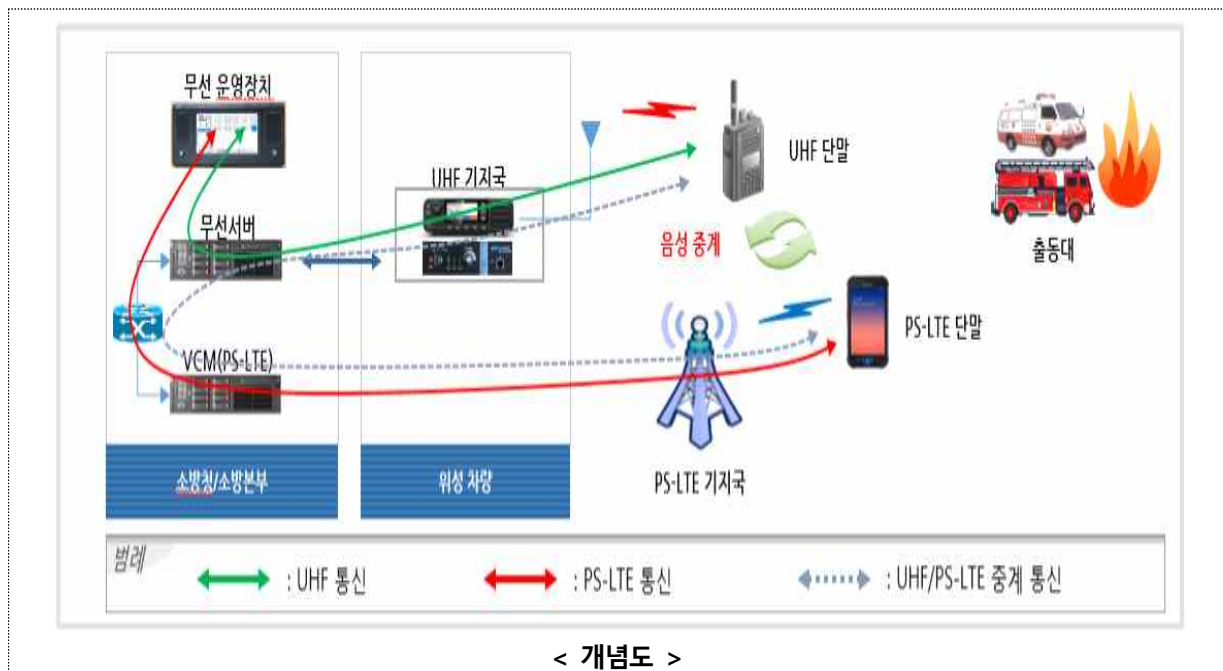
※ 출처 : 한국전력공사



### D-3) 소방 UHF 통신망과 재난안전통신망 통합운영시스템

- 기존 소방 UHF통신망과 재난안전통신망을 연동하여 현장 출동대 간의 원활한 그룹 통신 대책을 구비하고 통합 작전체계 제공
- '재난안전통신망 전환 운용'에 따라 기존 소방UHF 무선망간의 연동을 통한 통합 작전 수행
- 소방 119상황실 무선지령대에서 소방 UHF 및 재난안전통신망 동시 운영

※ 출처 : 소방청



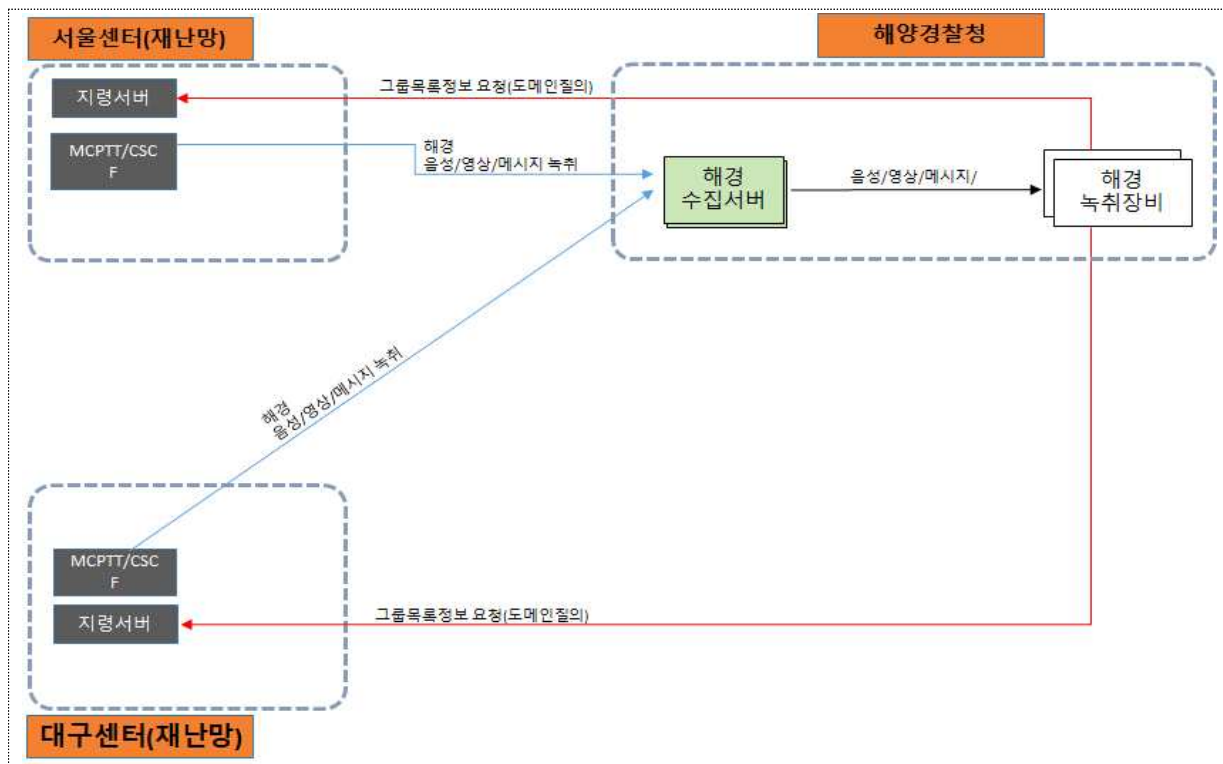
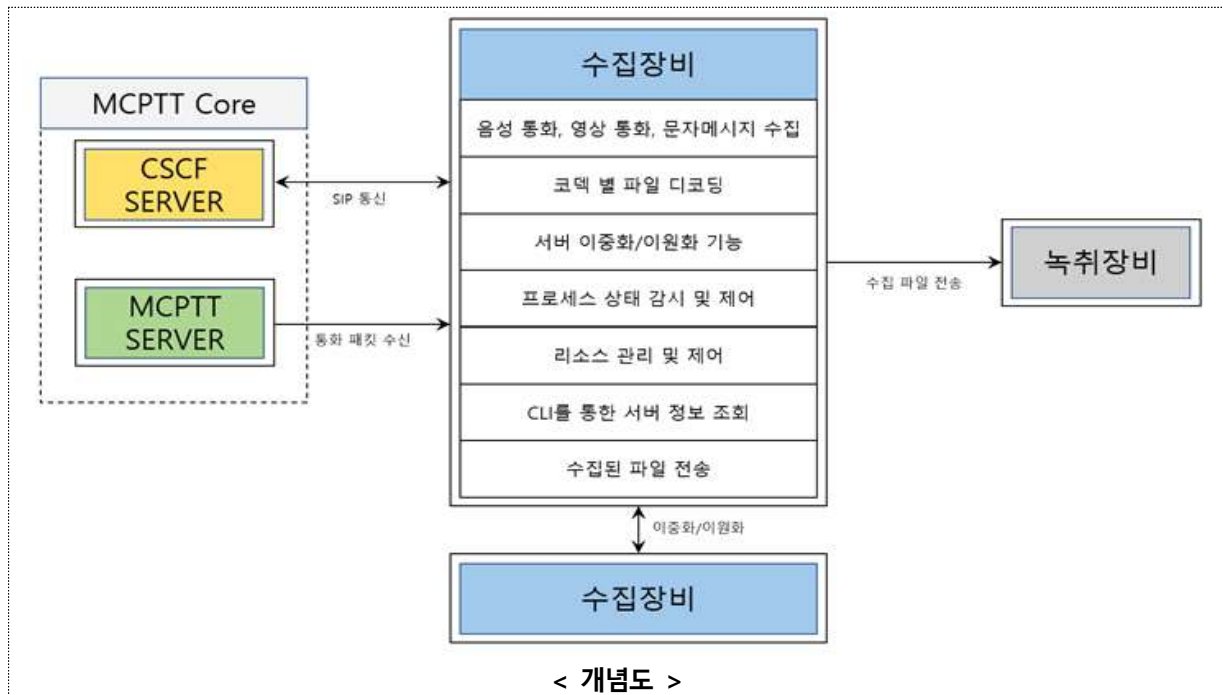
기능명	설명
소방통신망 단말기 관리	• 소방통신망 단말기 추가, 삭제, 통신 및 채널변경
재난안전통신망 단말기 관리	• 재난안전통신망 단말기 추가, 삭제, 통신
통신망 연계	• 소방통신망 및 재난안전통신망을 연동하여 상호통신

## D-4) 재난안전통신망 연계 녹취장비

○ 재난망 MCPTT 녹취, 녹화 수집 및 조회, 해경 녹취그룹 수신

- 해경 녹취조회 시 재난안전통신망 센터에 문의하여 조회하는 불편함을 해결하고, 해양경찰청 전용으로 재난안전통신망 MCPTT수집 및 조회

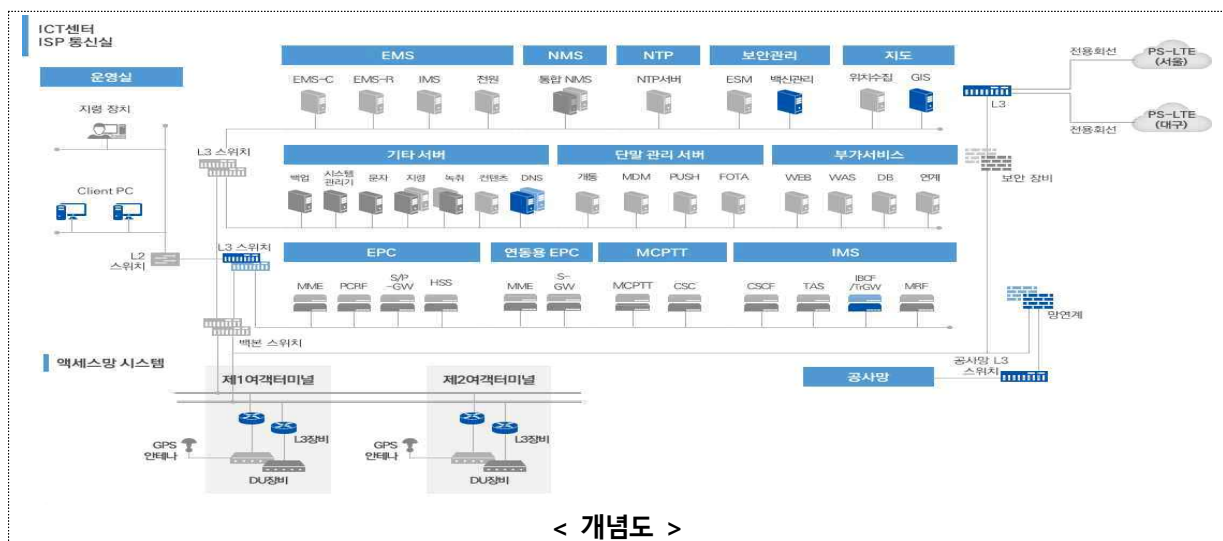
※ 출처 : 해양경찰청



## D-5) 재난안전통신망 연동 서비스

- 인천공항운영 이외 공항 지역 재난 발생 시 재난안전통신망과의연계를 통해 데이터, 사진, 동영상 등 다양한 멀티미디어 활용으로 신속·정확한 재난상황 파악 및 전달
- (코어망 설비) 단말기가 요청하는 통신서비스를 제공하기 위한 통화로 제어, 영상·음성통화, 데이터 전송, 연동접속 기능 구성
- (운영관리설비) 전체 장비의 구성, 성능 및 장애 등 운영 상태 통합 관리와 원격 제어
- (응용설비) LTE 통합공공망 응용서비스에 필요한 다양한 통신 부가서비스 및 통합플랫폼 기능 제공
- (액세스망 시스템) 무선 송·수신, 전파신호 출력세기 제어 등 무선 구간 전파 통신 기능, 무선통신에 적합한 형태로 데이터 변환(변·복조), 단말 핸드오버 등 기지국의 디지털 신호처리 기능, 무선구간 통신을 위하여 전기적 신호를 무선 신호로 변환하여 공중으로 전파를 송·수신
- (지령장치) 상황실과 현장 간 지휘, 명령 및 상황보고 등의 무선통신 업무를 효과적으로 수행
- (부가서비스) 인천공항 내 안전사고 증가에 따른 안전 예방 활동, 데이터 기반 예방점검 활동, 안전을 우선한 정확한 예방점검 확인, 업무환경 개선
- (단말기) 안드로이드 기반의 통합공공망 표준 휴대용 단말기로 스마트폰형, 무전기형, 차량형 단말기로 구성

※ 출처 : 인천국제공항

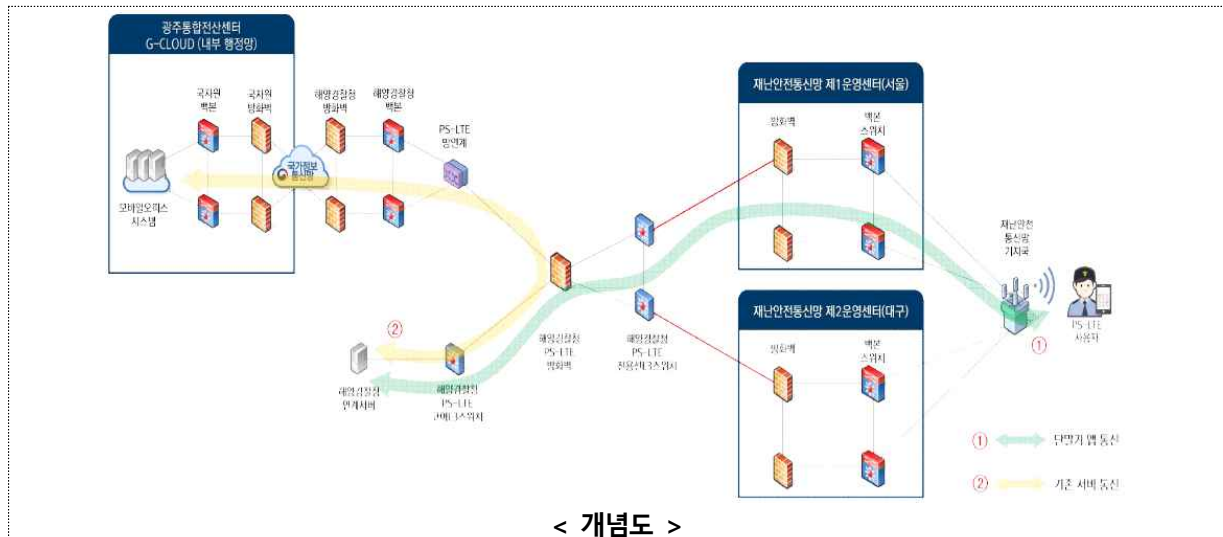




## D-6) 모바일오피스 서비스

- 해양경찰청에서 기존에 운영하던 모바일 오피스 앱 서비스에 재난안전통신망을 도입/운영하여 현장에서 재난상황보고 등을 통한 신속한 대처성 제고

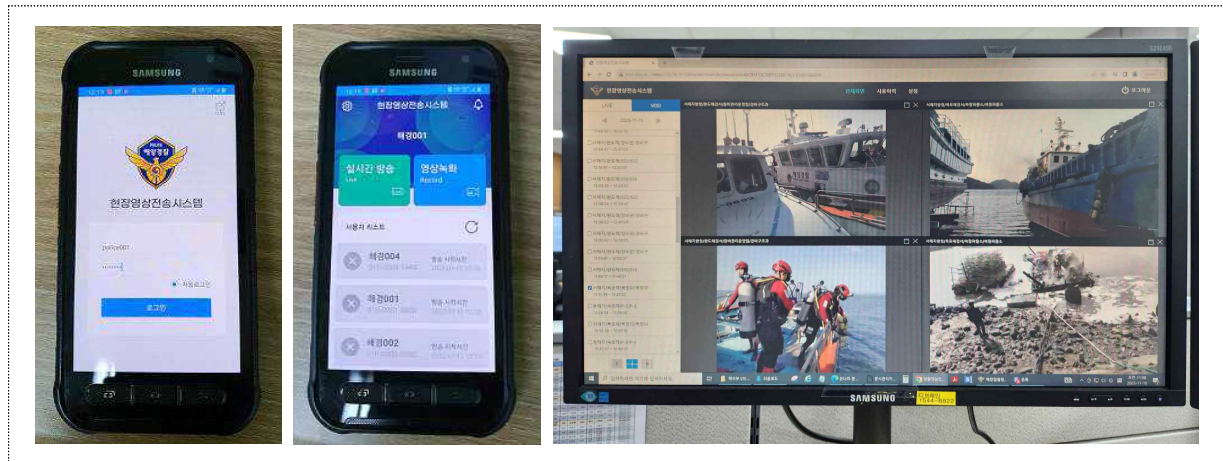
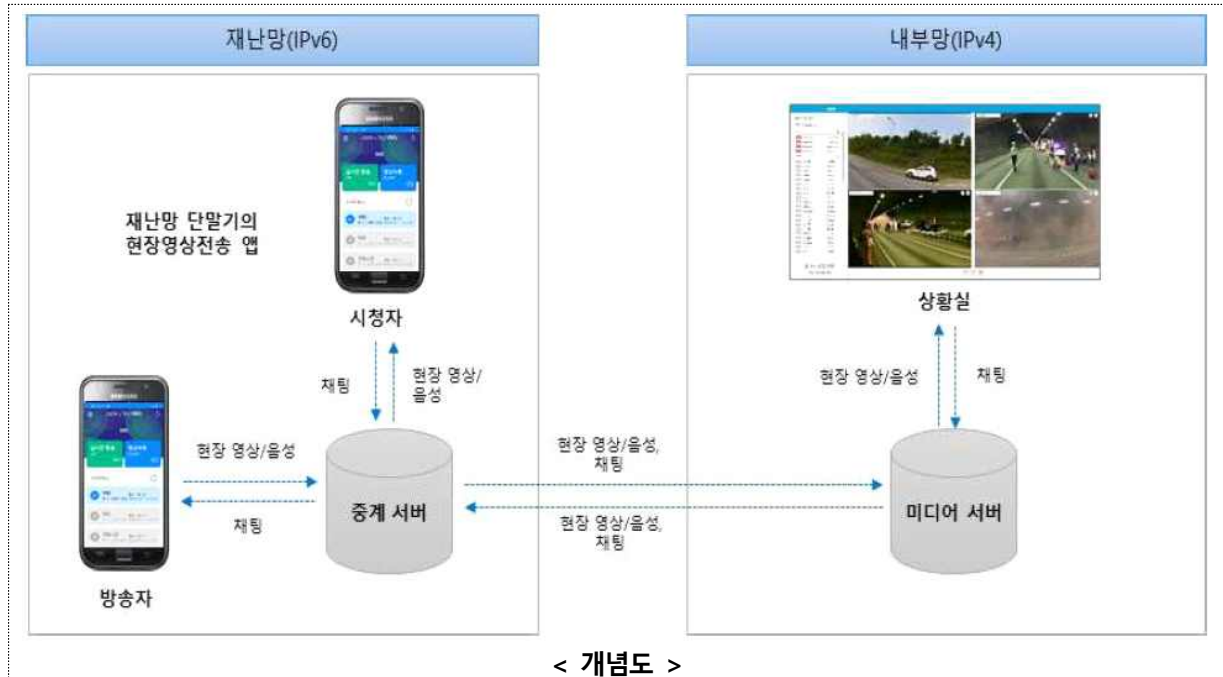
※ 출처 : 해양경찰청



## D-7) 현장영상전송시스템 서비스

- 재난안전통신망 단말의 현장영상전송시스템 서비스를 이용하여 240P, 480P, 720P 해상도의 영상을 실시간으로 전송

※ 출처 : 해양경찰청





## [부록 E] 재난안전통신망법 [법률 제18206호]

### 제1장 총칙

제1조(목적) 이 법은 「재난 및 안전관리 기본법」 제34조의8에 따라 재난관리 책임기관·긴급구조기관 및 긴급구조지원기관이 공동으로 사용하는 재난안전통신망의 구축, 운영 및 사용 등에 관한 사항을 정함으로써 신속하고 정확한 의사소통을 지원하고 재난의 예방·대비·대응·복구와 안전관리가 효과적·체계적으로 이루어지도록 하는 것을 목적으로 한다.

제2조(정의) ① 이 법에서 사용하는 용어의 뜻은 다음과 같다.

1. “재난안전통신”이란 「재난 및 안전관리 기본법」 (이하 “기본법”이라 한다) 제3조제3호에 따른 재난관리 및 같은 조 제4호에 따른 안전관리(이하 “재난안전관리”라 한다)에 사용하기 위하여 유선·무선·광선이나 그 밖의 전자적 방식으로 모든 종류의 부호·문언(文言)·음향 또는 영상을 송신하거나 수신하는 것을 말한다.
2. “재난안전통신설비”란 재난안전통신을 하기 위한 기계·기구·선로(線路)와 그 밖에 재난안전통신에 관련된 설비를 말한다.
3. “재난안전 관련기관”이란 기본법 제3조제5호에 따른 재난관리책임기관, 같은 조 제7호에 따른 긴급구조기관 및 같은 조 제8호에 따른 긴급구조지원기관을 말한다.
4. “재난안전통신망”이란 기본법 제3조제11호에 따른 재난안전통신망을 말한다.

② 제1항에서 정한 사항 외에 이 법에서 사용하는 용어의 뜻은 기본법에서 정하는 바에 따른다.

제3조(다른 법률과의 관계) ① 재난안전통신망의 구축 및 운영 등에 관하여 이 법에서 정한 사항이 「전기통신사업법」, 「전파법」 등 다른 법률과 다른 경우에는 이 법에서 정하는 바에 따른다.

② 재난안전통신망의 구축 및 운영 등에 관하여 이 법에서 규정한 것을 제외하고는 「전기통신사업법」 및 「전파법」을 준용한다.

## 제2장 재난안전통신망의 구축 및 운영에 관한 기본계획 등

제4조(재난안전통신망의 구축 및 운영에 관한 기본계획) ① 행정안전부장관은 재난안전통신망을 효과적·체계적으로 구축 및 운영하기 위하여 5년마다 재난안전통신망의 구축 및 운영에 관한 기본계획(이하 “기본계획”이라 한다)을 수립하여야 한다.

② 기본계획에는 다음 각 호의 사항이 포함되어야 한다.

1. 재난안전통신망 정책의 기본방향 및 목표
2. 재난안전통신망 구축 및 고도화
3. 재난안전통신망의 운영 및 이용
4. 재난안전통신망의 통화권 확대
5. 재난안전통신망의 보호 및 안전성 확보
6. 재난안전통신 관련 기술·서비스의 개발
7. 재난안전통신 관련 기술·서비스의 국외 진출 및 국제협력
8. 그 밖에 재난안전통신망의 구축 및 운영에 필요한 사항

③ 행정안전부장관은 기본계획을 수립하려면 다음 각 호의 재난안전 관련기관의 장과 미리 협의하여야 한다.

1. 과학기술정보통신부장관
2. 경찰청장
3. 소방청장
4. 해양경찰청장
5. 그 밖에 대통령령으로 정하는 재난안전 관련기관의 장

④ 행정안전부장관은 기본계획을 수립하거나 변경하려는 경우에는 기본법 제9조에 따른 중앙안전관리위원회의 심의를 거쳐야 한다. 다만, 대통령령으로 정하는 경미한 사항을 변경하려는 경우에는 그러하지 아니하다.

⑤ 제1항부터 제4항까지에서 규정한 사항 외에 기본계획의 수립 등에 필요한 사항은 대통령령으로 정한다.

제5조(재난안전통신망의 구축 및 운영에 관한 시행계획) ① 행정안전부장관은 기본계획을 시행하기 위한 시행계획을 매년 수립·시행하여야 한다.

② 제1항에 따른 시행계획에는 다음 각 호의 사항이 포함되어야 한다.

1. 기본계획의 해당 연도 시행을 위한 세부 실행계획

2. 재난안전통신망의 이용·보급 확대를 위한 장비 및 시설의 도입·교체 등에 관한 단계별 추진 계획
3. 그 밖에 재난안전통신망의 구축 및 운영에 필요한 세부 추진 사항

제6조(재난안전 관련기관의 재난안전통신망 활용계획) ① 재난안전 관련기관으로서 대통령령으로 정하는 기관의 장은 매년 재난안전통신망을 효과적으로 사용하기 위한 기관별 활용계획을 수립·시행하여야 한다.

② 제1항에 따른 활용계획에는 다음 각 호의 사항이 포함되어야 한다.

1. 재난안전통신망 활용을 위한 단말기 등의 신규 도입·교체
2. 재난안전통신망을 활용한 기관별 재난대응절차의 수립 및 보완
3. 재난안전통신망과 재난안전 관련기관의 정보시스템과의 연계 및 정보의 공동이용
4. 재난안전통신망 사용자 교육·훈련
5. 재난안전통신설비의 공동사용 및 관리
6. 재난안전통신망 통화권 확대
7. 그 밖에 재난안전통신망 사용에 필요한 사항

③ 제1항에 따라 재난안전통신망 활용계획을 수립하는 기관의 장은 제1항에 따른 활용계획을 수립하기 전에 미리 행정안전부장관과 협의하여야 한다.

### 제3장 재난안전통신망의 구축 및 운영

제7조(재난안전통신망의 구축 등) ① 행정안전부장관은 체계적인 재난안전관리를 위하여 재난안전통신망을 구축하여야 한다.

② 행정안전부장관은 무선통신기술의 발전과 재난안전통신과 관련된 국제 표준의 변화 등을 고려하여 재난안전통신망을 지속적으로 고도화하여야 한다.

③ 행정안전부장관은 재난안전통신망의 구축을 위하여 필요하다고 인정하는 경우에는 다른 행정기관 및 공공기관의 장에게 해당 기관이 운영하는 정보통신망 또는 정보통신설비 등과의 연계를 요청할 수 있다. 이 경우 요청을 받은 행정기관 및 공공기관의 장은 특별한 사유가 없으면 이에 응하여야 한다.

제8조(재난안전통신망의 운영·관리) ① 행정안전부장관은 재난안전통신망의 운영·관리에 관한 사항을 관장하고, 재난안전통신망의 운영·관리를 위하여 필요한 인력, 시설, 장비 등을 갖추어야 한다.

- ② 재난안전 관련기관의 장은 재난안전통신망의 효율적인 운영·관리를 위한 행정안전부장관의 요청 등에 적극 응하여야 한다.
- ③ 재난안전 관련기관은 그가 설치한 관제시설, 지령장치와 그 회선 및 단말기 등의 재난안전통신설비에 대한 유지·관리를 담당하며, 재난안전통신설비의 적절한 운영·관리를 위하여 필요한 인력, 시설, 장비 등을 갖추도록 노력하여야 한다.
- ④ 제1항부터 제3항까지에서 규정한 사항 외에 재난안전통신망의 운영 및 관리에 필요한 사항은 대통령령으로 정한다.

제9조(전기통신사업자 등에 대한 전기통신설비 등의 사용·제공 요청 등) ① 행정안전부장관은 재난안전통신망의 효율적인 구축·운영을 위하여 필요한 경우에는 「전기통신사업법」에 따른 전기통신설비 또는 도로, 철도, 지하철도, 상·하수도, 전기설비, 전기통신회선설비 등을 건설·소유·운용·관리하는 자(이하 “전기통신사업자등”이라 한다)에 요청하여 전기통신설비 또는 관로(管路)·공동구(共同溝)·전주(電柱)·케이블이나 국사(局舍) 등의 시설 또는 설비(이하 이 장에서 “전기통신설비등”이라 한다)를 사용하거나 제공받을 수 있다.

- ② 행정안전부장관은 제1항에 따라 전기통신설비등을 사용하거나 제공받으려면 그 대가·범위·절차·방법 등에 관하여 전기통신사업자등과 업무협약을 체결하여야 한다. 다만, 행정안전부장관은 재난이 발생하거나 발생할 우려로 미리 업무협약을 체결할 수 없는 급박한 사정이 있는 경우에는 제1항에 따라 전기통신설비등을 사용하고 사후에 그 대가 등에 대하여 협의할 수 있다.
- ③ 제1항 및 제2항에 따른 전기통신설비등의 사용·제공과 업무협약 체결 등에 필요한 사항은 대통령령으로 정한다.

제10조(무선통신시설의 공동이용) ① 행정안전부장관과 전기통신사업자등은 업무협약을 체결하여 상호 간에 무선통신시설을 공동으로 이용할 수 있다.

- ② 행정안전부장관과 전기통신사업자등은 제1항에 따라 무선통신시설을 공동이용하려는 경우에는 미리 무선통신시설 공동이용의 대가·범위·절차·방법 등에 관하여 업무협약을 체결하여야 한다.
- ③ 제1항 및 제2항에 따른 무선통신시설의 공동이용과 업무협약 체결 등에 필요한 사항은 대통령령으로 정한다.

제11조(재난안전통신설비의 접속) ① 행정안전부장관과 전기통신사업자들은 상호 간에 통신역무의 제공이 가능하도록 재난안전통신설비와 전기통신설비를 접속할 수 있다.

② 행정안전부장관과 전기통신사업자들은 제1항에 따라 재난안전통신설비와 전기통신설비를 접속하려면 전기통신사업자등과 접속의 대가·범위·절차·방법 등에 관하여 업무협약을 체결하여야 한다.

③ 제1항 및 제2항에 따른 재난안전통신설비와 전기통신설비와의 접속과 업무협약 체결 등에 필요한 사항은 대통령령으로 정한다.

제12조(기술정보의 제공) ① 행정안전부장관은 다음 각 호의 어느 하나에 해당하는 경우에는 해당 전기통신사업자등에게 관련 기술정보의 제공을 요청할 수 있다.

1. 제9조에 따른 전기통신설비등의 사용·제공

2. 제10조에 따른 무선통신시설의 공동이용

3. 제11조에 따른 재난안전통신설비와 전기통신설비와의 접속

② 행정안전부장관은 제1항에 따라 기술정보를 제공받으려면 전기통신사업자등과 기술정보 제공의 대가·범위·절차·방법 등에 관하여 협의하여야 한다.

③ 누구든지 제2항에 따라 제공받은 기술정보를 제공받은 목적 외의 용도로 사용하거나 제3자에게 제공해서는 아니 된다.

④ 제2항에 따른 기술정보의 제공 절차, 방법과 업무협약 체결 등에 필요한 사항은 대통령령으로 정한다.

제13조(건물과 토지에의 출입 등) ① 재난안전통신설비의 설치·보수, 재난안전통신설비 설치를 위한 조사·측량에 종사하는 사람은 그 설치·보수나 조사·측량을 위하여 필요할 때에는 타인의 건물 또는 토지에 출입하거나 그 토지에 표지물을 설치할 수 있다. 이 경우 출입하려는 곳이 주거용 건물인 경우에는 거주자의 승낙을 받아야 한다.

② 제1항에 따라 타인의 건물 또는 토지에 출입하려는 사람은 대통령령으로 정하는 바에 따라 권한을 표시하는 증표를 지니고 점유자나 관계인에게 보여 주어야 한다.

제14조(토지 등의 사용) ① 행정안전부장관은 재난안전통신설비를 설치하거나 보수하는 데에 필요한 경우에는 국유·공유 또는 사유(私有)의 토지와 그 토

지에 붙어 있는 인공구조물이나 수면·수저(水底) 또는 공공시설물(이하 “토지등”이라 한다)을 사용할 수 있다.

② 제1항에 따라 토지등을 사용할 때에는 토지등의 관할 관청과 소유자 또는 점유자와 미리 협의하여야 한다. 이 경우 토지등의 소유자 또는 점유자의 주소나 거소가 분명하지 아니하여 협의할 수 없을 때에는 그 사용 목적 및 기간과 그 밖에 필요한 사항을 대통령령으로 정하는 바에 따라 공고하여야 한다.

③ 행정안전부장관은 제2항에 따른 협의가 성립되지 아니하거나 협의를 할 수 없으면 「공익사업을 위한 토지 등의 취득 및 보상에 관한 법률」에서 정하는 바에 따라 타인의 토지등을 사용할 수 있다.

제15조(인공구조물의 제거 등) ① 행정안전부장관은 이동할 수 있는 인공구조물·매설물(埋設物)·기기(器機)·죽목(竹木)이나 그 밖의 식물(이하 “인공구조물등”이라 한다)이 재난안전통신설비를 설치하는 데에 장애가 되거나 재난안전통신의 전파장애를 일으키는 경우에는 그 소유자 또는 점유자에게 철거·상태변경·벌채(伐採) 또는 이식(이하 “제거”라 한다)을 요구할 수 있다.

② 행정안전부장관은 인공구조물등의 소유자 또는 점유자가 제1항에 따른 요구에 따르지 아니하거나 인공구조물등을 제거할 수 없는 부득이한 사유가 있을 때에는 그 소유자 또는 점유자에게 미리 통지하고 인공구조물등을 제거할 수 있다. 이 경우 국가 또는 지방자치단체가 소유 또는 점유하는 대통령령으로 정하는 인공구조물등에 대해서는 미리 관계 행정기관의 장과 협의하여야 한다.

③ 제1항 및 제2항의 경우에 인공구조물등의 소유자 또는 점유자의 주소나 거소가 분명하지 아니할 때에는 인공구조물등의 제거에 관한 사항을 대통령령으로 정하는 바에 따라 공고하여야 한다.

#### 제4장 재난안전통신망의 사용

제16조(재난안전통신망의 사용) ① 재난안전 관련기관은 다음 각 호의 활동을 하는 경우에는 재난안전통신망을 사용하여야 한다.

1. 재난의 대응 및 복구과정에서 재난안전 관련기관 간 상황의 지시, 보고 및 전파
2. 기본법 제37조에 따른 응급조치 등 행정안전부장관이 재난안전통신망의 사



용이 필요하다고 정하여 고시하는 활동

② 제1항에서 규정한 사항 외에 재난안전통신망의 사용에 필요한 사항은 대통령령으로 정한다.

제17조(재난안전통신망 사용 절차 등의 마련) ① 재난안전 관련기관은 재난안전통신망의 사용에 관하여 행정안전부장관이 정하여 고시하는 절차와 방법을 따라야 한다.

② 행정안전부장관은 재난안전통신망의 사용과 관련하여 재난안전 관련기관에 필요한 재난안전대응 절차를 연구·개발하여 보급할 수 있다.

제18조(재난안전관리 정보서비스 제공) 행정안전부장관은 대통령령으로 정하는 바에 따라 재난안전통신망과 기본법 제74조제1항에 따른 재난관리정보통신체계 등을 연계하여 재난안전관리에 필요한 정보서비스를 제공할 수 있다.

제19조(재난안전통신망의 상호 운용성 확보 등) 행정안전부장관은 재난안전통신망과 주파수 대역을 공동으로 사용하는 공공통신망과의 상호 운용성을 확보하기 위하여 관계 행정기관 또는 공공기관과 협력체계를 구축하는 등 필요한 조치를 하여야 한다.

제20조(재정적 지원) 국가는 재난안전통신망의 구축 및 운영과 관련하여 재난안전 관련기관에 필요한 재정의 일부를 지원할 수 있다.

## 제5장 재난안전통신망의 보호 및 개발촉진

제21조(재난안전통신망의 보호조치) ① 행정안전부장관 및 재난안전 관련기관의 장은 재난안전통신망의 안정적 운영을 위하여 다음 각 호의 보호조치를 하여야 한다.

1. 정당한 권한이 없는 자가 재난안전통신설비 또는 재난안전통신망에 접근·침입하는 것을 방지하거나 대응하기 위한 방안을 마련할 것
2. 재난안전통신망용 단말기의 분실·도난 및 정보유출·변조·삭제 등을 방지하기 위한 방안을 마련할 것
3. 재난안전통신망에 장애가 발생한 경우에는 신속하게 복구하고 재발방지를 위한 방안을 마련할 것

② 재난안전통신 사무에 종사하고 있거나 종사하였던 사람은 직무상 알게 된 비밀을 누설해서는 아니 된다.

③ 누구든지 재난안전 관련기관이 취급 중에 있는 재난안전통신의 비밀을 침해하거나 누설해서는 아니 된다.

제22조(재난안전통신의 보호) ① 누구든지 재난안전통신설비를 파손하여 그 기능에 장애를 일으키거나 재난안전통신을 방해해서는 아니 된다.

② 누구든지 재난안전통신설비에 물건을 던지거나 동물·배 또는 멧목 따위를 매는 등의 방법으로 재난안전통신설비를 더럽히고 손상하거나 재난안전통신설비의 표지물 등을 훼손해서는 아니 된다.

제23조(재난안전통신망 기술 등의 개발·발전의 촉진 등) ① 행정안전부장관은 재난안전통신, 재난안전통신설비 및 재난안전통신망과 관련된 기술(이하 이 조에서 “재난안전통신망기술등”이라 한다)의 개발 및 발전을 촉진하기 위하여 다음 각 호의 사항을 추진할 수 있다.

1. 재난안전통신망기술등의 개발 및 발전전략 수립
2. 개발된 재난안전통신망기술등의 권리 확보, 실용화 및 이용 활성화
3. 재난안전통신망기술등의 국내외 협력 및 정보교류
4. 재난안전통신망기술등의 운영, 유지·보수, 관련 인력 양성 및 교육
5. 재난안전통신망기술등의 적합성 확보
6. 그 밖에 재난안전통신망기술등의 개발 및 발전에 필요한 사항

② 행정안전부장관은 재난안전통신망의 효과적인 구축 및 운영을 위하여 재난안전통신망기술등의 표준화가 필요한 경우 과학기술정보통신부장관에게 다음 각 호의 사항을 요청할 수 있다.

1. 재난안전통신망기술등에 관한 표준의 제정·개정 및 폐지와 보급
2. 재난안전통신망기술등의 국내외 표준의 조사·연구 및 개발
3. 그 밖에 재난안전통신망기술등의 표준화에 필요한 사항

제24조(자료의 수집) ① 행정안전부장관은 재난안전통신망의 효율적 운영 및 관리를 위하여 재난안전 관련기관의 재난안전통신망 사용 현황에 관한 자료를 수집·분석할 수 있다.

② 행정안전부장관은 재난안전 관련기관의 장에게 자료 수집·분석에 필요한 협조를 요청할 수 있다. 이 경우 재난안전 관련기관의 장은 특별한 사정이 없으면 요청에 응하여야 한다.



## 제6장 보칙

제25조(업무의 위탁) 이 법에 따른 행정안전부장관의 업무는 대통령령으로 정하는 바에 따라 그 일부를 관련 기관이나 법인 또는 단체에 위탁할 수 있다.

제26조(원상회복의 의무 및 손실보상) ① 행정안전부장관은 제13조에 따른 표지물의 설치 및 제14조에 따른 토지등의 사용 시 더 이상 재난안전통신 업무에 제공할 필요가 없게 되면 지체 없이 그 토지등을 원상으로 회복하여야 하고, 원상으로 회복하지 못하는 경우에는 그 소유자나 점유자가 입은 손실에 대하여 정당한 보상을 하여야 한다.

② 행정안전부장관은 다음 각 호의 사유로 발생한 손실에 대하여 정당한 보상을 하여야 한다.

1. 제13조제1항에 따른 출입 또는 표지물의 설치
2. 제14조제1항에 따른 토지등의 사용
3. 제15조에 따른 인공구조물등의 제거

③ 제1항 및 제2항에 따른 손실보상의 청구는 손실이 있음을 안 날부터 1년 또는 손실이 발생한 날부터 3년 이내에 하여야 한다.

④ 행정안전부장관은 제3항에 따른 손실보상 청구를 받았을 때에는 청구를 받은 날부터 3개월 이내에 보상금액을 결정하여 청구인에게 서면으로 통지하여야 한다.

⑤ 제1항부터 제4항까지에서 규정한 사항 외에 손실보상의 기준 및 절차 등은 대통령령으로 정한다.

## 제7장 벌칙

제27조(벌칙) ① 제22조제1항을 위반하여 재난안전통신설비를 파손하여 그 기능에 장애를 일으키거나 재난안전통신을 방해한 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.

② 제21조제2항을 위반하여 재난안전통신 사무에 종사하고 있거나 종사하였던 사람이 직무상 알게 된 비밀을 누설하였을 때에는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처한다.

③ 다음 각 호의 어느 하나에 해당하는 자는 2년 이하의 징역 또는 2천만원 이하의 벌금에 처한다.

1. 제12조제3항을 위반하여 제공받은 기술정보를 제공받은 목적 외의 용도로 사용하거나 제3자에게 제공한 자
2. 제13조 및 제14조에 따른 재난안전통신설비의 설치·보수 또는 조사·측량을 정당한 사유 없이 방해한 자
3. 제21조제3항을 위반하여 재난안전통신의 비밀을 침해하거나 누설한 자
- ④ 제22조제2항을 위반하여 재난안전통신설비를 더럽히고 손상하거나 재난안전통신설비의 표지물 등을 훼손한 자는 300만원 이하의 벌금 또는 과료(科料)에 처한다.

제28조(미수범) 제27조제1항·제2항 및 같은 조 제3항제2호·제3호의 미수범은 처벌한다.

제29조(과태료) ① 제13조제1항에 따른 건물 또는 토지에의 출입을 정당한 사유 없이 방해한 자에게는 3천만원 이하의 과태료를 부과한다.

② 제1항에 따른 과태료는 대통령령으로 정하는 바에 따라 행정안전부장관이 부과·징수한다.

#### 부칙

제1조(시행일) 이 법은 공포 후 6개월이 경과한 날부터 시행한다.

제2조(다른 법률의 개정) 재난 및 안전관리 기본법 일부를 다음과 같이 개정한다.

제3조제11호 중 “재난관리업무”를 “재난 및 안전관리업무”로, “무선통신망”을 “통신망”으로 한다.

제34조의8제2항을 삭제하고, 같은 조 제3항 중 “대통령령으로”를 “다른 법률로”로 한다.

## [부록 F] 재난안전통신망 운영 및 사용에 관한 규정

[행정안전부고시 제2023-50호]

### 제1장 총칙

제1조(목적) 이 규정은 「재난안전통신망법」(이하 ‘법’이라 한다) 제8조 및 제16조, 같은 법 시행령(이하 ‘령’이라 한다) 제4조 및 제13조에 따라 재난안전통신망의 효율적인 운영 관리와 사용에 필요한 세부 사항을 규정함을 목적으로 한다.

제2조(용어의 정의) 이 규정에서 사용하는 용어의 정의는 다음 각 호와 같다.

1. "재난안전통신망"이란 법 제2조제1항제4호에 따른 재난안전통신망을 말한다.
2. "사용기관"이란 법 제2조제1항제3호에 따른 재난안전 관련기관 중에서 재난안전통신망을 사용하는 기관을 말한다.
3. "재난현장지휘관"이란 법 제2조제1항제3호에 따른 재난안전 관련기관의 장 및 재난 관련 부서장 등 현장 지휘 책임이 있는 자를 말한다.
4. "공통 통화그룹"이란 재난현장 및 비상상황에서 사용기관간 협업 업무를 수행하기 위하여 모든 단말기가 공통으로 사용할 수 있는 통화그룹을 말한다.
5. "기관 통화그룹"이란 사용기관 고유 업무를 수행하기 위하여 해당 사용기관 소속의 단말기만 자체적으로 사용할 수 있는 통화그룹을 말한다.
6. "임시 통화그룹"이란 사용기관 등에서 특별한 수요에 따라 지령장치 등에서 통화그룹을 임시 생성하여 해당 단말기에서 일시적으로 사용할 수 있는 통화그룹을 말한다.
7. "변경 관리"란 재난안전통신망을 통해 제공되는 통신서비스의 품질 개선을 위하여 구성요소를 변경하는 절차를 관리하는 활동을 말한다.

제3조(적용범위) 재난안전통신망을 사용하는 각급기관(행정안전부를 포함한다)의 운영 및 관리에 관한 사항은 다른 법령에 특별한 규정이 있는 경우를 제외하고는 이 규정이 정하는 바에 따른다.

### 제2장 재난안전통신망 운영 · 관리

제4조(재난안전통신망 운영센터의 설치) ① 영 제4조에 따른 재난안전통신망 운영센터(이하 ‘운영센터’라 한다)의 위치 및 관할구역은 별표1과 같다.

② 행정안전부장관은 재난안전통신망의 효율적인 운영 관리를 위하여 제1항에 따른 운영센터 하위에 운영지소를 설치·운영할 수 있다.

제5조(관리 체계) ① 「행정안전부와 그 소속기관 직제 시행규칙」 제18조제12

항에 따른 재난안전통신망과장은 재난안전통신망 운영업무를 총괄한다.

② 지역별 운영센터장은 재난안전통신망장이 지정한 지역별 운영센터 내 소관 업무를 관장한다.

③ 지역별 운영센터 근무자는 운영센터 상황실 내에서 이루어지는 재난안전통신망의 장애 감시 · 접수 및 보고, 초동조치, 민원접수 및 처리와 제2조제6호에 따른 변경 관리 업무를 수행한다.

제6조(근무 체계) ① 운영센터 및 운영지소의 근무체계는 재난안전통신망 통신 서비스를 365일 24시간 운영하기 위하여 4교대를 원칙으로 한다.

② 운영센터장 및 운영지소장은 교대근무자를 매월 편성하여 재난안전통신망과장의 승인을 얻어 시행하되 영 제4조제2항에 따라 재난안전통신망 무선국 운영에 필요한 무선종사자 기술자격을 소지한 자를 우선 배치하여야 한다.

③ 재난안전통신망과장은 재난안전통신망의 효율적 운영을 위하여 사용기관에 상주 연락관 파견을 요청할 수 있다.

제7조(번호 관리) ① 행정안전부장관은 「전기통신사업법」 제48조 및 과학기술정보통신부고시 「전기통신번호관리세칙」, 「이동전화망번호관리기준」, 「신호점번호관리기준」 등에 따라 재난안전통신망의 번호자원을 관리하여야 한다.

② 재난안전통신망의 식별번호 이후의 국번호와 가입자 개별번호 체계에 대한 기준은 행정안전부장관이 정하여 과학기술정보통신부장관의 승인을 받아야 한다.

③ 제2항에 따른 번호관리의 효율성을 위하여 행정안전부장관은 국번호와 가입자 개별번호를 다음 각 호의 사용기관에게 부여하고, 사용기관은 부여된 국번호와 가입자 개별번호를 자체 번호사용계획에 따라 자율적으로 운영한다.

1. 중앙행정기관 : 해당 기관의 소속기관 및 산하기관, 기타 관리감독 대상 기관을 포함

2. 광역자치단체(특별시, 광역시, 특별자치시, 도, 특별자치도) : 해당 지역의 기초자치단체(시, 군, 구)를 포함한 소속기관 및 산하기관, 기타 관리감독 대상 기관을 포함

제8조(통화그룹 관리) ① 행정안전부장관은 공통 통화그룹에 재난현장 및 비상 상황에서 사용기관간 협업 업무를 수행하기 위하여 필요한 모든 단말기가 참여할 수 있도록 관리하여야 하며, 전국, 광역(특별시, 광역시, 특별자치시, 도, 특별자치도), 기초자치단체(시, 군, 구) 등에 따라 배정한다.

② 행정안전부장관은 기관 통화그룹에 해당 사용기관 소속의 단말기만 참여할

수 있도록 관리하여야 하며, 배정 체계는 재난안전통신망에서 수용할 수 있는 수준을 고려하여 행정안전부장관과 사용기관의 장이 상호 협의하여 정한다.

③ 행정안전부장관은 임시 통화그룹에 운영센터 또는 사용기관이 지령장치 등에서 참여할 단말기를 자율적으로 입력할 수 있도록 관리하여야 하며, 배정 체계는 재난안전통신망에서 수용할 수 있는 수준을 고려하여 행정안전부장관과 사용기관의 장이 상호 협의하여 정한다.

제9조(주파수 관리) ① 행정안전부장관은 과학기술정보통신부의 재난안전통신망 관련 전파지정기준 등에 따라 주파수를 관리하여야 한다.

② 사용기관의 장이 재난안전통신망의 주파수를 사용하는 무선국을 직접 설치·운용하고자 하는 경우에는 행정안전부장관과 사전 협의 후 재난안전통신망과 연계하여 타 사용기관과 공동으로 사용할 수 있어야 한다.

제10조(서비스 수준 관리) 행정안전부장관은 재난안전통신망 운영과 관련한 서비스 수준 관리 협약을 용역 수행업체와 체결하여 관리하여야 한다.

제11조(통화내용 관제) ① 행정안전부장관은 다음 각 호에 해당하는 통화내용에 대하여 관제할 수 있다.

1. 공통 통화그룹
2. 사용기관에서 동의한 기관 및 임시 통화그룹
3. 장애 및 통화량 증가로 인하여 보수가 필요한 통화그룹
4. 고객센터 상담업무를 위한 통화내용

② 제1항에 따른 통화그룹에 대하여 녹취할 수 있으며 녹취한 정보는 3개월간 저장·관리하여야 한다.

③ 제2항에 따른 운영 관리는 「통신비밀보호법」 및 「개인정보 보호법」을 준수하여야 한다.

제12조(장비 관리) ① 재난안전통신망과장은 재난안전통신망 운영에 필요한 장비가 정상 작동하도록 주기적인 점검을 실시하고 필요한 조치를 하여야 한다.

② 재난안전통신망과장은 국무총리훈령 「긴급통신수단 관리지침」에서 정하는 바에 따라 장비를 관리하여야 한다.

제13조(장애 관리) ① 재난안전통신망과장은 재난안전통신망의 장애에 대비하여 주요 장비를 이중화로 구축·운영하여야 한다.

② 재난안전통신망에 장애가 발생한 경우에는 장애시간을 최소화하고 조속히 정상 복구될 수 있도록 응급복구와 장애보고 체계를 마련하고 그 밖에 필요한 조치를 취하여야 한다.

③ 재난안전통신망을 정상 복구한 후 장애원인을 분석하여 해당 공사 또는 용

역 업체에게 개선이나 시정 조치를 지시할 수 있으며 재발 방지를 위한 이행 결과를 확인하여야 한다.

제14조(통계 관리) ① 재난안전통신망과장은 재난안전통신망 운영 및 사용과 관련한 통계를 주기적으로 분석하여 기능 및 성능 개선정책에 반영하도록 노력하여야 한다.

② 제1항에서 규정한 사항 외에 필요한 사항은 행정안전부훈령 「행정안전부 통계관리 규정」에서 정하는 바에 따른다.

제15조(품질 관리) ① 행정안전부장관은 재난안전통신망 구축 및 운영 단계에서 해당 업체가 제시한 목표 품질이 유지되고 있는지에 대하여 매년 1회 이상 평가하고 미흡한 경우에는 해당 업체에게 만회 조치를 요구하고 이행결과를 확인하여야 한다.

② 제1항에 따른 평가 업무를 「지능정보화 기본법」 제12조 및 영 제17조에 따라 예산의 범위에서 한국지능정보사회진흥원에 출연하거나 위탁할 수 있다.

제16조(물품 관리) ① 재난안전통신망과장은 디지털예산회계시스템의 물품 취득원장과 일치하도록 물품을 관리하여야 한다.

② 제1항에서 규정한 사항 외에 필요한 사항은 「물품관리법」 및 「공유재산 및 물품 관리법」에서 정하는 바에 따른다.

제17조(보안 관리) ① 행정안전부장관은 운영센터 상황실 등 필요한 장소를 「행정안전부 보안업무규정 시행세칙」 제43조제1항에 따라 제한구역으로 설정하여 출입자 명부를 비치하고 고정출입자 이외의 출입상황을 기록 유지하여야 한다.

② 제1항에서 규정한 사항 외에 필요한 사항은 행정안전부훈령 「행정안전부 정보보안지침」에서 정하는 바에 따른다.

제18조(자료 관리) 재난안전통신망과장은 재난안전통신망 운영과 관련한 자료를 「공공기록물 관리에 관한 법률」에서 정하는 바에 따라 관리하여야 한다.

제19조(공동 운영 등) ① 행정안전부장관이 재난안전통신망을 효율적으로 운영하기 위하여 필요하다고 인정하는 경우에는 사용기관 또는 관계기관과 공동으로 운영하거나 「재난 및 안전관리 기본법」 제78조제1항에 따라 행정안전부장관 권한의 일부를 시·도지사에게 위임할 수 있다.

② 제1항에 따라 공동으로 운영하기 위하여 필요한 비용은 사용기관 또는 관계기관이 부담하여야 한다.

③ 제2항에도 불구하고 행정안전부장관이 필요에 의하여 사용기관 또는 관계기관에게 공동 운영을 요청하는 경우에는 행정안전부장관이 관련 비용을 부담



할 수 있다.

제20조(점검 및 확인) ① 행정안전부장관은 재난안전통신망의 효율적인 관리를 위하여 사용기관의 사용 및 운영 실태를 점검할 수 있다.

② 행정안전부장관은 제1항에 따른 점검 및 확인 결과를 사용기관에 통보할 수 있다.

제21조(교육 및 훈련) ① 행정안전부장관은 재난안전통신망의 효율적인 사용 및 운영 관리를 위하여 사용기관을 대상으로 교육을 실시할 수 있다. 이 경우 사용기관은 특별한 사유가 없는 한 행정안전부장관의 교육 실시 요청에 따라야 한다.

② 행정안전부장관은 재난 발생 시 재난안전통신망의 원활한 사용 및 운영을 위하여 사용기관을 대상으로 합동훈련을 실시할 수 있다. 이 경우 사용기관은 특별한 사유가 없는 한 행정안전부장관의 합동훈련 실시 요청에 따라야 한다.

③ 재난안전통신망과장은 제6조제2항에 따른 무선종사자의 양성을 위하여 과학기술정보통신부장관이 지정한 교육기관에 행정안전부 소속 공무원을 대상으로 자격검정 교육을 의뢰할 수 있으며, 해당 교육 이수자 및 자격 취득자에게 해당 비용을 지원하여야 한다.

### 제3장 재난안전통신망 사용

제22조(사용 신청) ① 재난안전통신망을 사용하고자 하는 기관의 장은 별지 제1호 서식에 따라 행정안전부장관에게 신청하여야 한다.

② 행정안전부장관은 제1항의 요청을 받은 경우에는 다음 각 호의 사항을 검토하여 사용 가능 여부를 통보하여야 한다.

1. 재난 및 안전관리업무에 사용하거나 통합지휘에 활용하는 등 재난안전통신망 목적에 부합하는지 여부
2. 재난안전통신망에서 수용할 수 있는 통신량에 부합하는지 여부
3. 재난안전통신망과의 연계와 연동을 위하여 적용하는 기술적 방법이 타당한지 여부
4. 재난안전통신망과 중복성 문제가 없는지 여부

제22조의2(재난안전통신망의 사용) ① 재난현장지휘관은 재난 시 상황 관리를 위하여 단말기를 상시 소지 및 사용하여야 한다.

② 지방자치단체의 장은 재난안전 관련기관 간 신속한 재난상황의 지시, 보고 및 전파를 위하여 다음 각 호의 조치를 하여야 한다.

1. 상황실 및 당직실(이하 "재난상황관리부서"라 한다)에 재난안전통신망 단

말기 비치 및 통신상태 점검

2. 재난상황관리부서 근무자에 대한 재난안전통신망 사용 요령 교육

③ 재난상황관리부서 상황근무자는 소속 시·도 및 시·군·구 공통통화그룹에 상시 참여하여 통신상황을 청취하고 재난 상황을 전파하여야 한다.

④ 안전한국훈련, 을지연습 등 중앙행정기관 및 지방자치단체의 장이 유관기관과 합동으로 실시하는 훈련에는 재난안전통신망을 적극 활용하여야 한다.

제23조(사용 해지) 재난안전통신망 사용기관의 장이 사용을 해지하려는 경우에는 별지 제2호 서식에 따라 행정안전부장관에게 신청하여야 한다.

제24조(사용 제한) ① 행정안전부장관은 영 제13조제1항에 따라 다음 각 호의 경우에는 재난안전통신망 사용의 일부를 제한할 수 있다.

1. 재난안전통신망의 안정적인 품질을 유지하기 어려운 경우

2. 일시적인 통신량 폭주 시 장비의 정상적인 동작이 불가능한 경우

3. 보안에 피해가 있거나 우려되는 경우

4. 상용망 사용요금 등을 장기간 납부하지 않은 경우

5. 재난안전 업무와 무관한 인터넷 사이트 등을 접속하는 경우

6. 그 밖에 행정안전부장관이 필요하다고 인정하는 사항

② 행정안전부장관은 제1항에 따라 재난안전통신망 사용을 제한하였을 경우에는 영 제13조제2항에 따라 해당 사용기관의 장에게 서면(전자문서를 포함한다), 팩스, 전화, 문자메시지 등 가장 빠른 방법으로 즉시 통보해야 한다.

제25조(장애 신고) ① 사용기관의 장 또는 사용자는 재난안전통신망이 장애가 발생한 것으로 판단하는 경우에는 행정안전부장관에게 그 사실을 지체 없이 신고하여야 한다.

② 제1항에 따라 신고를 접수한 행정안전부 담당공무원은 지체 없이 필요한 조치를 하여야 하며 장애처리에 장시간이 소요될 경우에는 사용기관의 장 또는 사용자에게 그 사실을 통보하여야 한다.

제26조(비용 부담) ① 사용기관이 재난안전통신망을 사용하기 위하여 필요한 비용의 부담에 관한 사항은 다음 각 호와 같다.

1. 사용기관별 자체 통신서비스를 기간통신사업자의 이동통신망 기지국을 통하여 제공받는 경우에 발생하는 통신요금

2. 사용기관에서 자체 장비를 재난안전통신망과 연결하기 위하여 필요한 기간통신사업자의 전용회선 요금

3. 그 밖에 행정안전부장관이 필요하다고 인정하는 사항

② 행정안전부장관은 기간통신사업자와 재난안전통신망 사용기관의 비용 절감



등 효율적인 관리를 위한 협약을 체결할 수 있다.

제27조(연계 사용) ① 사용기관의 장이 자체 정보통신망 또는 정보시스템을 재난안전통신망과 연계하여 사용하고자 하는 경우에는 행정안전부장관과 상호 협의하여 국가정보원장의 보안성검토 결과에 따라 구성하여야 한다.

② 제1항에 따른 보안성검토는 사용기관의 장이 국가정보원장에게 의뢰하여야 한다.

제28조(사용 장비 등 도입) ① 사용기관의 장은 단말기, 지령장치 등 재난안전통신망 사용을 위하여 필요한 장비를 도입하는 경우에는 행정안전부장관이 지정한 전문기관으로부터 기술 적합성 검증을 받은 장비이어야 한다.

② 제1항에 따른 기술적합성 검증에 따른 비용은 사용기관의 장이 부담하는 것을 원칙으로 하되, 행정안전부장관이 필요하다고 인정하는 경우에는 예산 범위 내에서 지원 또는 분담할 수 있다.

③ 제1항에 따른 기술적합성 검증을 받은 장비 등을 도입하고자 하는 경우에는 별지 제2호 서식에 따라 행정안전부장관에게 신청하여야 한다.

제29조(사용 촉진) ① 행정안전부장관은 사용기관의 의견을 수렴하여 재난안전통신망 사용을 촉진하기 위한 관련 정책 및 사업을 추진하고 해당 성과를 사용기관에게 널리 활용·확산될 수 있도록 보급할 수 있다.

② 행정안전부장관은 재난안전통신망과 관련한 시험·검증, 연구개발, 실용화 등의 업무를 자유롭게 수행할 수 있는 개발환경 시스템을 구축하고 산업계, 학계, 연구계에 개방하여야 한다.

③ 제2항에 따른 개발환경 시스템은 한국지능정보사회진흥원의 초연결 지능형 연구개발망(KOREN) 등 타 관계기관의 개발환경 시스템과 연계하여 공동으로 설치·운영할 수 있다.

## 제4장 보칙

제30조(시행 세칙) 재난안전통신망과장은 이 규정의 범위 안에서 재난안전통신망 운영과 사용에 필요한 사항을 따로 정할 수 있다.

제31조(재검토 기한) 행정안전부장관은 이 고시에 대하여 2021년 1월 1일을 기준으로 매 3년이 되는 시점(매 3년째의 12월 31일까지를 말한다)마다 그 타당성을 검토하여 개선 등의 조치를 하여야 한다.

## 부칙

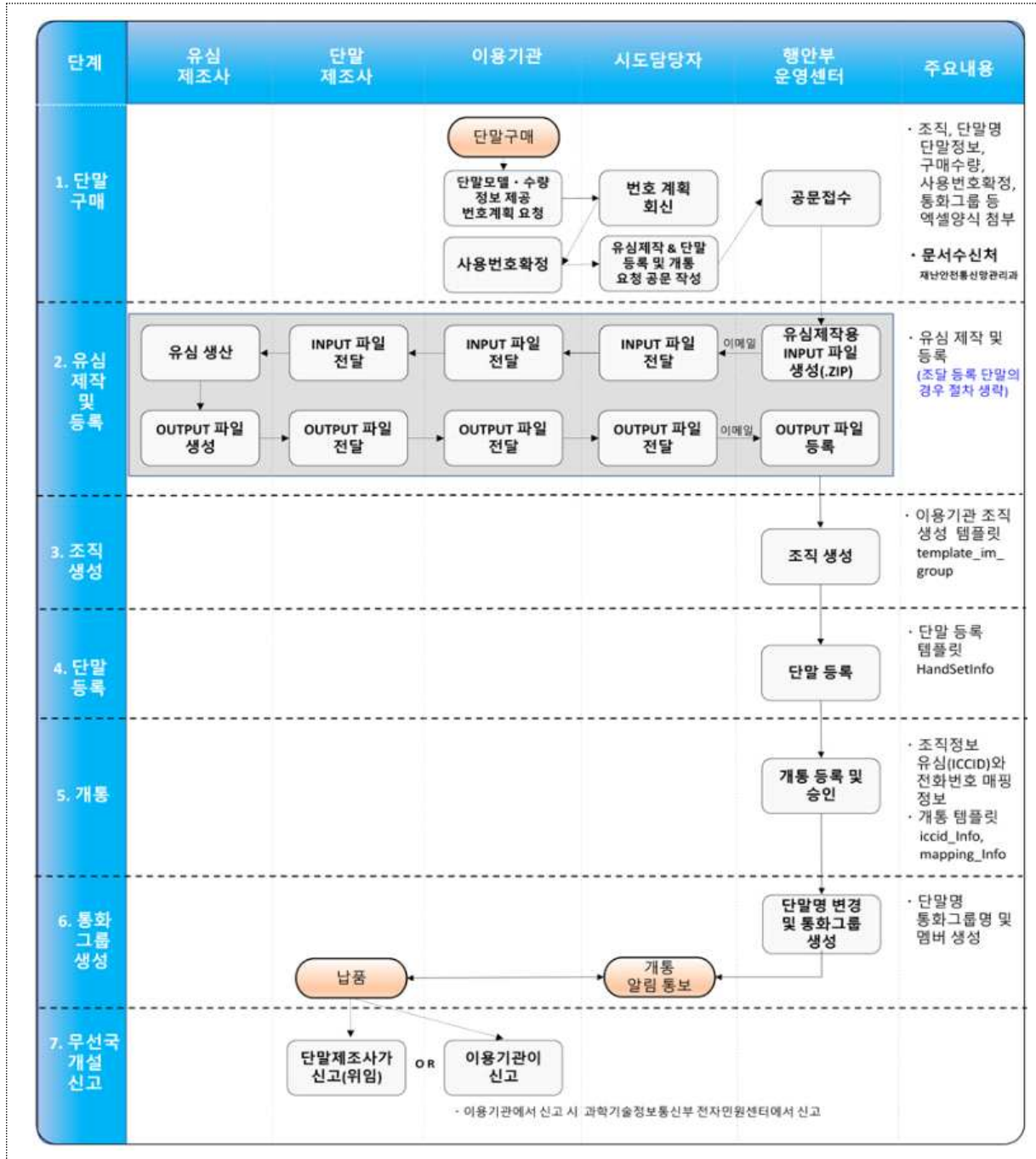
제1조(시행일) 이 고시는 발령한 날부터 시행한다.

## [부록 G] 재난안전통신망 단말기 개통 절차

※ 이 문서는 2021년 11월 현재의 버전을 참고로 첨부한 것이며, 변경 사항 등 최신버전에 대하여는 재난안전통신망 웹 포털을 참조하거나 운영센터에 문의

### G-1) 단말기 개통에 대한 담당 기관

- 사용기관이 SIM 등록, 단말기 등록 및 단말기 개통을 하고자 할 때는 다음의 절차에 따라 재난안전통신망 웹 포털을 통하여 재난안전통신망 운영센터에 신청을 한다.



※ 별도 공지 전까지 공문과 offline 협의를 통해 진행

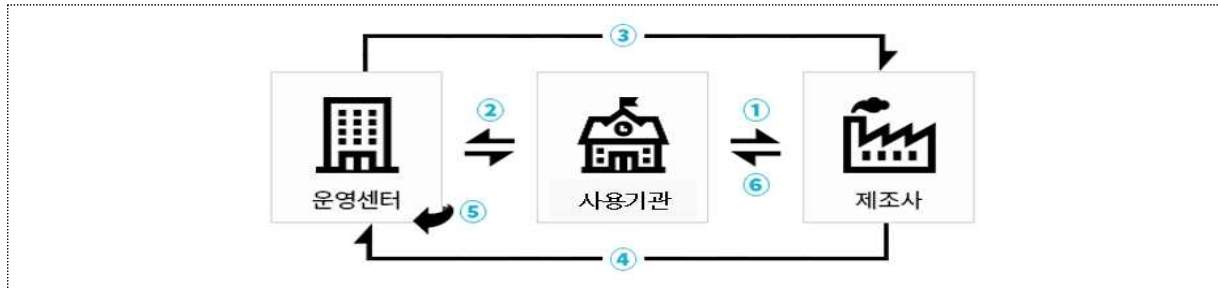
※ 과학기술정보통신부 전자민원센터 전자민원 신청 접속([https://www.emsit.go.kr/cp/cv/Cp1440000\\_0041\\_01Reg.do](https://www.emsit.go.kr/cp/cv/Cp1440000_0041_01Reg.do))

## G-2) 자원 관리 (참고)

- 단말기 관리시스템에서 관리되는 자원은 SIM, 단말기, 전화번호를 의미한다. 각 사용기관이 운영센터로 자원등록 서비스 요청을 하면 운영센터에서 자원을 등록한 이후에 각 사용기관에서 사용할 수 있다. 단말기 관리시스템으로의 자원등록 흐름은 아래와 같다.



## G-3) SIM 등록 절차



- SIM 등록을 하고자 하는 사용기관은 제조사와 SIM 계약 후 포털에서 등록신청을 하며, 운영센터는 제조사에게 요청정보(input file)를 전달 후 생성정보(output file)를 받아 등록한다. 단계별 절차는 다음과 같다.

- ① 계약 : 사용기관이 SIM 제조사와 계약
- ② 등록신청(포털) : 사용기관이 운영센터에 SIM 등록 신청
- ③ 요청정보(input file) : 운영센터에서 SIM 제조사에 SIM 제작 요청정보(ICCID Prefix 및 IMSI 정보, 수량)를 전달
- ④ 생성정보(output file) : SIM 제조사가 운영센터에 SIM 정보 전달
- ⑤ 등록 : 운영센터에서 SIM 등록
- ⑥ SIM 전달 : SIM 제조사가 사용기관에 SIM 전달

## G-4) 단말기 등록 절차

- 단말기 등록을 하고자 하는 사용기관은 제조사와 단말 계약 후 실물과 단말 정보를 받아 포털의 자원등록 신청 메뉴를 통해 신청한다. 단계별 절차는 다음과 같다.

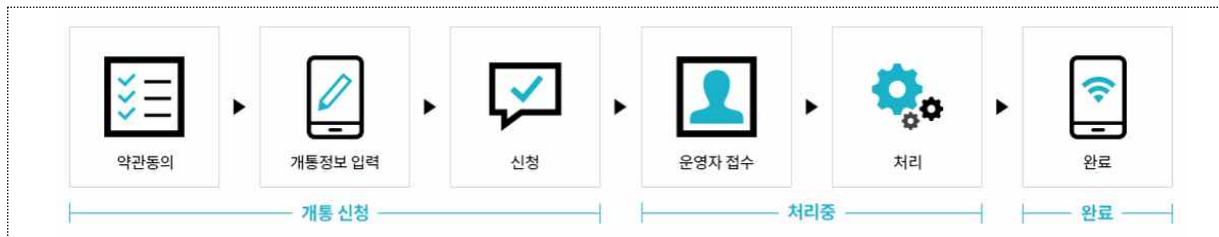


- ① 계약 : 사용기관이 단말제조사와 계약
- ② 실물 & 정보 파일 : 제조사가 사용기관에 단말기와 정보파일을 제공
- ③ 등록신청 : 사용기관이 공문 또는 협의를 통해 단말기 정보 등록을 신청 (단말기 유형 코드, 제조사 코드, 모델명, Serial No, IMEI)
- ④ 등록 : 운영센터에서 요청정보를 단말 가입/해지 시스템에 등록

## G-5) 단말기 개통/변경 업무 절차

- 사용기관은 향후 재난안전통신망 포털 사이트를 통해서 개통/변경(해지, 부가서비스) 신청을 할 수 있으며 센터운영자는 신청된 신청서를 확인 후 센터승인권자로부터 승인을 받는다. 개통요청의 경우 승인과 동시에 장비 연계되어 단말기를 사용할 수 있다.

- 개통 순서



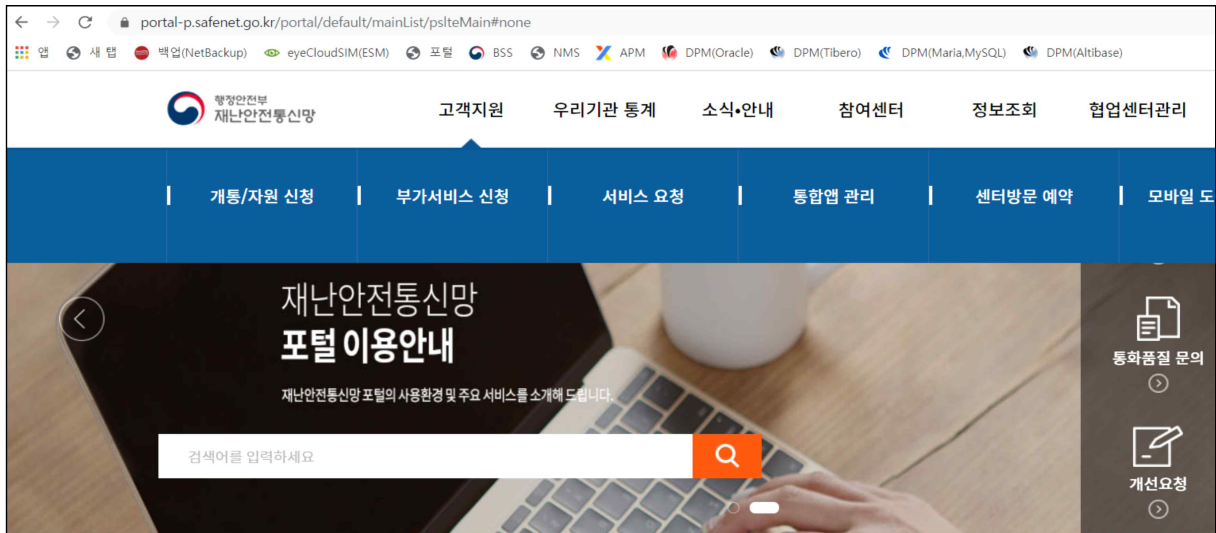
- 개통 업무 흐름



## [부록 H] 재난안전통신망 앱스토어 사용자 매뉴얼

### H-1) 앱스토어 접속

- “https://sso.safenet.go.kr/nls3/clientLogin.jsp” URL에 접속하여 로그인한다.




### H-2) 앱 등록

- 앱을 등록하고자 할 때는 아래 그림과 같이 “고객지원”, “통합앱 관리”, “앱등록” 메뉴를 차례로 선택하여, 앱등록 화면에 들어간다.
- 앱등록 화면에서 등록하고자 하는 앱에 대한 정보를 입력하여 등록시키고, “등록” 버튼을 누른다.







통합안전통신망

고객지원    우리기관 통계    소식·안내    참여센터    정보조회    협업센터관리    기관별 협업센터

### 통합앱 관리

총 2건 (1/1)

번호	앱 명	소속	앱 등록구분	현재버전	승인상태	배포상태	권한	수정일시
1	TEST-APP02	운영센터	신규	1.0.4	<a href="#">업등록</a>	비협동	미설정	2020-02-27
2	TEST-APP-1	운영센터	신규	1.0.4	<a href="#">업등록</a>	비협동	미설정	2020-02-26

### 통합앱 관리

총 2건 (1/1)

소속기관    앱(서비스)명    지원OS    모델번호

소속기관: 운영센터    앱(서비스)명: TEST-APP-1    지원OS: 9.0    모델번호: SM-G889N

버전    배포 버전    앱 버전 코드    패키지명    설치파일(apk)    실행아이콘

버전: 1.0.4    배포 버전: 1.0.4    앱 버전 코드: 104    패키지명: kr.co.ejbt.gis.3    설치파일(apk): GIS\_v1.0.4.apk    실행아이콘: GIS\_첨두자료\_앱 실행아이콘.png

상세정보

앱 소개: test용입니다    앱 스크린 이미지: GIS\_첨두자료\_스크린샷1.png

등록    삭제    목록

### H-3) 앱 목록 조회

- 통합 앱 관리 화면에서 앱 목록이 조회된다. 앱 목록은 앱명, 소속, 앱 등록구분, 현재 버전, 승인상태, 배포상태, 권한, 수정일시가 표시되어 나열되며, 전체상태, 활동, 비활동 중 선택하여 조회할 수 있다.

#### H-3.1) 앱 상세 조회

- 앱을 클릭하면 앱의 상세 내역이 조회된다.

- 버전 업데이트 등 수정이 필요한 경우 '수정' 버튼을 선택하여 내용을 변경하고 '저장' 버튼을 누른다.

## H-3.2) 앱 사용권한 관리

※앱 승인신청을 위해 사전에 권한 설정 필요

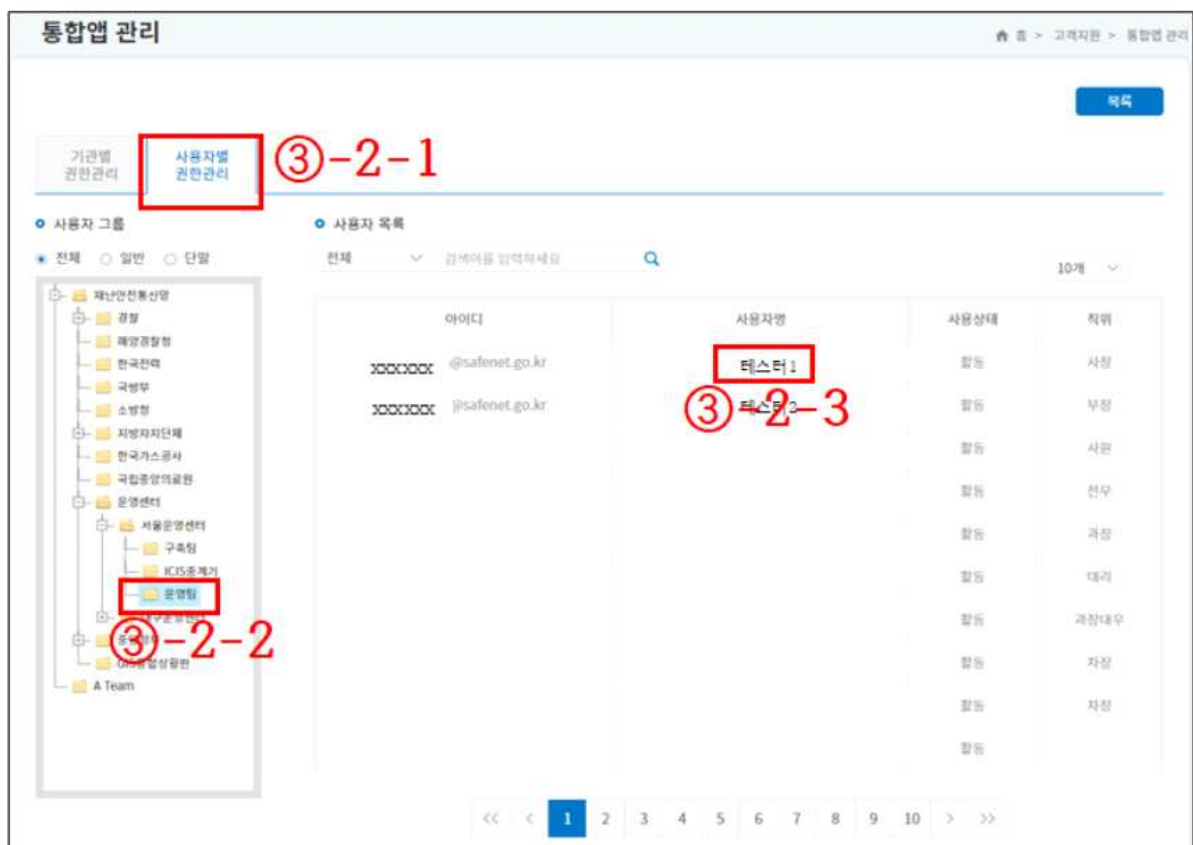
### H-3.2.1) 기관별 권한 관리





※ 권한 삭제 시, 권한 부여된 사용자 목록에서 삭제할 리스트를 선택한 다음 '권한제거' 버튼을 클릭

### H-3.2.2) 사용자별 권한 관리



통합앱 관리

기관별 권한관리 사용자별 권한관리

앱 권한 관리

[아이디: xxxxxxxx@safenet.go.kr] - [이름: 테스트1]

목록 저장 ③-2-5

<input type="checkbox"/>	앱(서비스)	앱설명	현재버전	버전설명
<input type="checkbox"/>	현장영상	현장영상	1.0.09	1009
<input type="checkbox"/>	지도		1.1.09	1109
<input checked="" type="checkbox"/> ③-2-4	WEAR	1. 스마트폰과 귀종품역 분실물 ...	1.0.13	1.0.13
<input checked="" type="checkbox"/>	TEST-APP-1	kr.co.ejbt.gjskr.co.ejbt.gjs	1.0.4	배포 버전
<input type="checkbox"/>	AR설비교육	AR설비교육자원 앱은 백팩형 무...	1.0.07	1007
<input type="checkbox"/>	TEST-APP02	앱 등록 테스트 - 앱 등록 테스트 - ...	1.0.4	배포 버전

### H-3.3) 앱 승인

#### H-3.3.1) 앱 승인신청

※ 권한신청 완료 후 승인신청 가능

통합앱 관리

승인상태

등록 승인요청 배포요청 배포(승인/반려)

④-5

승언여력 승인요청 목록

검증보고서 양식

앱 해시코드 ABCDEFGHIJKLMNOPQRSTU ④-1

내용 ④-2

버전 1.0.4

④-3 검증보고서 ④-4 ITSM CSR 처리결과서

XXXXXXX.pdf \* 검증보고서는 pdf/hwp 파일 형식으로 등록 가능합니다.

XXXXXXX.png \* 연혁이칭 관련 서버등록 처리 완료 이미지

파일찾기

파일찾기

검증

앱사용 승인요청 드립니다.

### H-3.3.2) 앱 승인 상세조회

① 앱 승인 시 첨부한 검증보고서 다운로드 가능

② 앱 승인 시 첨부한 ITSM CSR 처리 결과서 미리 보기 및 다운로드 가능

### H-3.4) 앱 배포상태 변경

※ 배포 승인 완료 후 변경 가능


번호	앱명	소속	앱 등록구분	현재버전	승인상태	배포상태	권한	수정일시
1	TEST-APP02	운영센터	신규	1.0.4	승인완료	비활용	미설정	2020-02-27
2	TEST-APP-1	운영센터	신규	1.0.4	승인완료	비활용	설정완료	2020-02-26

번호	앱명	소속	앱 등록구분	현재버전	승인상태	배포상태	권한	수정일시
1	TEST-APP02	운영센터	신규	1.0.4	승인완료	비활용	미설정	2020-02-27
2	TEST-APP-1	운영센터	신규	1.0.4	승인완료	활용	설정완료	2020-02-26

## [부록 I] 재난안전통신망 개발자 포털의 API

- 재난안전통신망 개발자 포털에서 볼 수 있는 API 목록이며, 추가 내용이나 갱신된 내용은 향후 개발자 포털 또는 운영센터를 통해 확인

### I-1) APIs

<div>  <span>행정안전부</span> </div> <div> <span>개발자 포털</span> </div> <div> <input type="text"/> <input type="button" value="Q"/> </div>																																																																																										
<div> <span>홈</span> <span>APIs &amp; 플랜</span> <span>API 문서</span> </div>																																																																																										
<div> <span>APIs &amp; 플랜</span> </div>																																																																																										
<div> <span>APIs</span> <span>플랜</span> </div>																																																																																										
<div> <h4>APIs</h4> <table> <tr> <th>API 이름</th><th>유형</th><th>인증</th><th>가시성</th><th>상태</th><th>버전</th><th>앱</th></tr> <tr> <td>[BSS] A3-MSR-EIF-BSS-0001_단말 기사용량조회</td><td>REST</td><td>API 키</td><td>공개(Public)</td><td>활성화됨</td><td>1</td><td></td></tr> <tr> <td>[CMD] A1-MSR-EIF-CMD-0001_통 화그룹목록조회</td><td>REST</td><td>API 키</td><td>공개(Public)</td><td>활성화됨</td><td>1</td><td></td></tr> <tr> <td>[CMD] A1-MSR-EIF-CMD-0002_통 화그룹단말목록조회</td><td>REST</td><td>API 키</td><td>공개(Public)</td><td>활성화됨</td><td>1</td><td></td></tr> <tr> <td>[CMD] A1-MSR-EIF-CMD-0003_통 화그룹생성</td><td>REST</td><td>API 키</td><td>공개(Public)</td><td>활성화됨</td><td>1</td><td></td></tr> <tr> <td>[CMD] A1-MSR-EIF-CMD-0004_통 화그룹사용자추가</td><td>REST</td><td>API 키</td><td>공개(Public)</td><td>활성화됨</td><td>1</td><td></td></tr> <tr> <td>[CMD] A1-MSR-EIF-CMD-0005_재 난발생등록</td><td>REST</td><td>API 키</td><td>공개(Public)</td><td>활성화됨</td><td>1</td><td></td></tr> <tr> <td>[CMD] A1-MSR-EIF-CMD-0006_재 난종결설정</td><td>REST</td><td>API 키</td><td>공개(Public)</td><td>활성화됨</td><td>1</td><td></td></tr> <tr> <td>[CMD] A1-MSR-EIF-CMD-0007_재 난변경설정</td><td>REST</td><td>API 키</td><td>공개(Public)</td><td>활성화됨</td><td>1</td><td></td></tr> <tr> <td>[CMD] A1-MSR-EIF-CMD-0008_통 화그룹사용자삭제</td><td>REST</td><td>API 키</td><td>공개(Public)</td><td>활성화됨</td><td>1</td><td></td></tr> <tr> <td>[CMD] A1-MSR-EIF-CMD-0009_통 화그룹정보변경</td><td>REST</td><td>API 키</td><td>공개(Public)</td><td>활성화됨</td><td>1</td><td></td></tr> <tr> <td>[CMD] A1-MSR-EIF-CMD-0010_통 화그룹삭제</td><td>REST</td><td>API 키</td><td>공개(Public)</td><td>활성화됨</td><td>1</td><td></td></tr> </table> </div>							API 이름	유형	인증	가시성	상태	버전	앱	[BSS] A3-MSR-EIF-BSS-0001_단말 기사용량조회	REST	API 키	공개(Public)	활성화됨	1		[CMD] A1-MSR-EIF-CMD-0001_통 화그룹목록조회	REST	API 키	공개(Public)	활성화됨	1		[CMD] A1-MSR-EIF-CMD-0002_통 화그룹단말목록조회	REST	API 키	공개(Public)	활성화됨	1		[CMD] A1-MSR-EIF-CMD-0003_통 화그룹생성	REST	API 키	공개(Public)	활성화됨	1		[CMD] A1-MSR-EIF-CMD-0004_통 화그룹사용자추가	REST	API 키	공개(Public)	활성화됨	1		[CMD] A1-MSR-EIF-CMD-0005_재 난발생등록	REST	API 키	공개(Public)	활성화됨	1		[CMD] A1-MSR-EIF-CMD-0006_재 난종결설정	REST	API 키	공개(Public)	활성화됨	1		[CMD] A1-MSR-EIF-CMD-0007_재 난변경설정	REST	API 키	공개(Public)	활성화됨	1		[CMD] A1-MSR-EIF-CMD-0008_통 화그룹사용자삭제	REST	API 키	공개(Public)	활성화됨	1		[CMD] A1-MSR-EIF-CMD-0009_통 화그룹정보변경	REST	API 키	공개(Public)	활성화됨	1		[CMD] A1-MSR-EIF-CMD-0010_통 화그룹삭제	REST	API 키	공개(Public)	활성화됨	1	
API 이름	유형	인증	가시성	상태	버전	앱																																																																																				
[BSS] A3-MSR-EIF-BSS-0001_단말 기사용량조회	REST	API 키	공개(Public)	활성화됨	1																																																																																					
[CMD] A1-MSR-EIF-CMD-0001_통 화그룹목록조회	REST	API 키	공개(Public)	활성화됨	1																																																																																					
[CMD] A1-MSR-EIF-CMD-0002_통 화그룹단말목록조회	REST	API 키	공개(Public)	활성화됨	1																																																																																					
[CMD] A1-MSR-EIF-CMD-0003_통 화그룹생성	REST	API 키	공개(Public)	활성화됨	1																																																																																					
[CMD] A1-MSR-EIF-CMD-0004_통 화그룹사용자추가	REST	API 키	공개(Public)	활성화됨	1																																																																																					
[CMD] A1-MSR-EIF-CMD-0005_재 난발생등록	REST	API 키	공개(Public)	활성화됨	1																																																																																					
[CMD] A1-MSR-EIF-CMD-0006_재 난종결설정	REST	API 키	공개(Public)	활성화됨	1																																																																																					
[CMD] A1-MSR-EIF-CMD-0007_재 난변경설정	REST	API 키	공개(Public)	활성화됨	1																																																																																					
[CMD] A1-MSR-EIF-CMD-0008_통 화그룹사용자삭제	REST	API 키	공개(Public)	활성화됨	1																																																																																					
[CMD] A1-MSR-EIF-CMD-0009_통 화그룹정보변경	REST	API 키	공개(Public)	활성화됨	1																																																																																					
[CMD] A1-MSR-EIF-CMD-0010_통 화그룹삭제	REST	API 키	공개(Public)	활성화됨	1																																																																																					

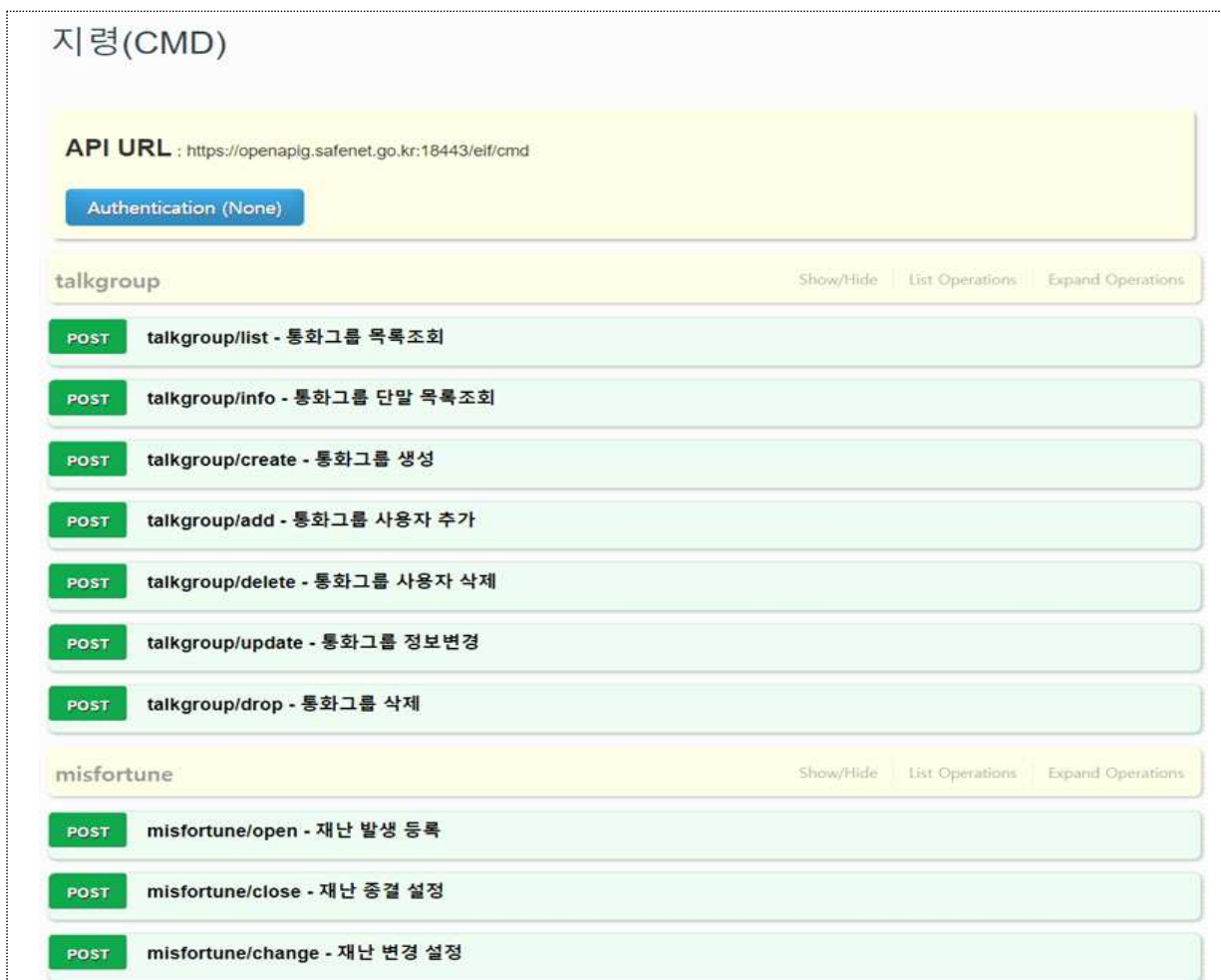
[GIS] A1-MSR-EIF-GIS-0001_단말 기 목록 및 위치정보	REST	API 키	공개(Public)	활성화됨	1	
[GIS] A1-MSR-EIF-GIS-0002_기지 국 목록 및 위치정보	REST	API 키	공개(Public)	활성화됨	1	
[GIS] A1-MSR-EIF-GIS-0003_단말 기 위치 정보	REST	API 키	공개(Public)	활성화됨	1	
[GIS] A1-MSR-EIF-GIS-0004_단말 기 위치 표시(WMS)	REST	API 키	공개(Public)	활성화됨	1	
[GIS] A1-MSR-EIF-GIS-0005_단말 기 위치 표시(WFS)	REST	API 키	공개(Public)	활성화됨	1	
[GIS] A1-MSR-EIF-GIS-0006-기지국 위치 표시(WMS)	REST	API 키	공개(Public)	활성화됨	1	
[GIS] A1-MSR-EIF-GIS-0007_기지 국 위치 표시(WFS)	REST	API 키	공개(Public)	활성화됨	1	
[GIS] A1-MSR-EIF-GIS-0008_동적 통화그룹 영역 표시(WMS)	REST	API 키	공개(Public)	활성화됨	1	
[GIS] A1-MSR-EIF-GIS-0009_동적 통화그룹 영역 표시(WFS)	REST	API 키	공개(Public)	활성화됨	1	
[GIS] A1-MSR-EIF-GIS-0010_배경 지도 서비스	REST	API 키	공개(Public)	활성화됨	1	
[GIS] A3-MSR-EIF-GIS-0011_POI검 색	REST	API 키	공개(Public)	활성화됨	1	
[GIS] A3-MSR-EIF-GIS-0012_주소 검색	REST	API 키	공개(Public)	활성화됨	1	
[ISM] A3-MSR-EIF-ISM-0001_나의 CSR목록수신	REST	API 키	공개(Public)	활성화됨	1	
[ISM] A3-MSR-EIF-ISM-0002_나의 CSR상세수신	REST	API 키	공개(Public)	활성화됨	1	
[LPS] A1-MSR-EIF-LPS-0001_단말 위치조회	REST	API 키	공개(Public)	활성화됨	1	
[LPS] A1-MSR-EIF-LPS-0002_위치 반경제어	REST	API 키	공개(Public)	활성화됨	1	
[LPS] A1-MSR-EIF-LPS-0003_단말 궤적조회	REST	API 키	공개(Public)	활성화됨	1	
[POT] A3-MSR-EIF-POT-0001_통화 그룹생성개별승인요청	REST	API 키	공개(Public)	활성화됨	1	
[POT] A3-MSR-EIF-POT-0001_통화 그룹생성개별승인요청	REST	API 키	공개(Public)	활성화됨	1	
[POT] A3-MSR-EIF-POT-0002_통화 그룹생성일괄승인요청	REST	API 키	공개(Public)	활성화됨	1	
[POT] A3-MSR-EIF-POT-0004_승인 상태확인요청	REST	API 키	공개(Public)	활성화됨	1	
[PSH] A3-MSR-EIF-PSH-0001_휴대 용단말기에Push전송요청	REST	API 키	공개(Public)	활성화됨	1	
[REC] A1-MSR-EIF-REC-0001 음성 목록조회	REST	API 키	공개(Public)	활성화됨	1	
[REC] A1-MSR-EIF-REC-0002 영상 목록조회	REST	API 키	공개(Public)	활성화됨	1	
[REC] A1-MSR-EIF-REC-0003 문자 전송내역조회	REST	API 키	공개(Public)	활성화됨	1	

## I-2) API 문서

○ API 문서는 다음과 같은 것들이 있다.



### I-2.1) 지령(CMD)



## I-2.2) 지도(GIS)

지도(GIS)			
API URL : https://openapig.safenet.go.kr:18443/elf/gis			
Authentication (None)			
Toggle All			
getDeviceList	Show/Hide	List Operations	Expand Operations
GET	getDeviceList - 단말기 목록 및 위치정보		
getLTEList	Show/Hide	List Operations	Expand Operations
GET	getLTEList - 기지국 목록 및 위치정보		
getDeviceLocation	Show/Hide	List Operations	Expand Operations
GET	getDeviceLocation - 단말기 위치 정보		
wms	Show/Hide	List Operations	Expand Operations
GET	wms/device - 단말기 위치 표시(WMS)		
GET	wms/station - 기지국 위치 표시(WMS)		
GET	wms/fence - 동적 통화그림 영역 표시(WMS)		
wfs	Show/Hide	List Operations	Expand Operations
GET	wfs/device - 단말기 위치 표시(WFS)		
GET	wfs/station - 기지국 위치 표시(WFS)		
GET	wfs/fence - 동적 통화그림 영역 표시(WFS)		
tms	Show/Hide	List Operations	Expand Operations
GET	tms/{mapType}/{zoom}/{x}/{y}.{imgType} - 배경 지도 서비스		
search	Show/Hide	List Operations	Expand Operations
GET	search/poi - POI 검색		
GET	search/adres - 주소 검색		



### I-2.3) 위치측위(LPS)

#### 위치측위(LPS)

**API URL** : https://openapig.safenet.go.kr:18443/elf/lps

Authentication (None)

currentLocation

Show/Hide | List Operations | Expand Operations

**POST** currentLocation - 단말현재위치조회

deviceConfig

Show/Hide | List Operations | Expand Operations

**POST** deviceConfig - 단말제어

locationTracePage

Show/Hide | List Operations | Expand Operations

**POST** locationTracePage - 단말궤적조회

### I-2.4) 녹음녹화(REC)

#### 녹음녹화(REC)

**API URL** : https://openapig.safenet.go.kr:18443/elf/rec

Authentication (None)

Toggle All

voices

Show/Hide | List Operations | Expand Operations

**POST** ptt/voices - 녹음/녹화 음성 목록 조회

videos

Show/Hide | List Operations | Expand Operations

**POST** ptt/videos - 녹음/녹화 영상 목록 조회

messages

Show/Hide | List Operations | Expand Operations

**POST** ptt/messages - 녹음/녹화 문자 전송 내역 조회



## I-2.5) 포털(POT)

포털(POT)

API URL : https://openapig.safenet.go.kr:18443/elf/pot

Authentication (None)

Toggle All

talkGrp

Show/Hide

List Operations

Expand Operations

POST

talkGrp/getTalkGrpStatus - 통화그룹 생성 개별 승인 요청

POST

talkGrp/setTalkGrpFile - 통화그룹 생성 일괄 승인 요청

POST

talkGrp/getTalkGrpStatus - 승인상태 확인요청

## I-2.6) 운영서비스관리(ISM)

운영서비스관리(ISM)

API URL : https://openapig.safenet.go.kr:18443/elf/ism

Authentication (None)

Toggle All

csrList

Show/Hide

List Operations

Expand Operations

POST

csrList - CSR목록수신

csrPotDetail

Show/Hide

List Operations

Expand Operations

POST

csrPotDetail - CSR상세수신

## I-2.7) 단말개통(BSS)

### 단말개통(BSS)

**API URL** : <https://openapi.g.safenet.go.kr:18443/eif/bss>

Authentication (None)

Toggle All

pot

Show/Hide

List Operations

Expand Operations

**POST** pot/usageList - 단말기 사용량 조회

## I-2.8) 푸시전송(PSH)

### 푸시전송(PSH)

**API URL** : <https://openapi.g.safenet.go.kr:18443/eif/pus>

Authentication (None)

Toggle All

interface

Show/Hide

List Operations

Expand Operations

**POST** interface - Push전송요청

## I-3) API 문서 내역 예시

### I-3.1) GetDeviceList – 단말기 목록 및 위치정보

getDeviceList
Show/Hide
List Operations
Expand Operations

GET
getDeviceList - 단말기 목록 및 위치정보

단말기 목록 및 위치정보

요청 파라미터

파라미터	유형	필수	설명
minx	number	N	검색 영역 최소값(경도)
miny	number	N	검색 영역 최소값(위도)
maxx	number	N	검색 영역 최대값(경도)
maxy	number	N	검색 영역 최대값(위도)
tel_grp_id	string	N	통화그룹 ID
device_id	string	N	단말기 ID

maxx	number	N	검색 영역 최대값(경도)
maxy	number	N	검색 영역 최대값(위도)
tel_grp_id	string	N	통화그룹 ID
device_id	string	N	단말기 ID
equip_id	string	N	기지국 ID
grp_id	string	N	조직 ID
fromTime	string	N	단말검색일시
page	string	N	검색요청 페이지
limit	string	N	검색결과 건수

```
// Request URL
https://openapig.safenet.go.kr:8443:/eif/gis/getDeviceList?EIF_INTFR_ID=GeoCommandTestAPI&EIF_INTFR_SNO=GeoCommandTestAPI&EIF_TRANSMIT_DT=20190402143524998&minx=126.16545&miny=36.2354898&maxx=127.951895&maxy=37.6654898&tel_grp_id=999999&device_id=DEVICE_506&equip_id=test_equip_1234&grp_id=org_0001&page=1&limit=10
```

## Parameters

Parameter	Value	Description
EIF_INTFR_ID	(required)	외부연계인터페이스아이디
EIF_INTFR_SNO	(required)	외부연계인터페이스등록순서
EIF_TRNSMIT_DT	(required)	외부연계전송일시
minx	0	검색 영역 최소값(경도)
miny	0	검색 영역 최소값(위도)
maxx	0	검색 영역 최대값(경도)
maxy	0	검색 영역 최대값(위도)
device_id	0	단말기ID
equip_id	0	기자국ID
grp_id	0	조직ID
page	0	검색요청 페이지
limit	0	검색결과 건수

POS_METHOD	string	측위 방식(CELL:기자국측위, GPS:GPS측위, WiFi:WiFi측위)
LONGITUDE	string	경도
LATITUDE	string	위도
ALTITUDE	number	고도
FLOOR	number	층수

```
// JSON Response Data
{
  "EIF_TRSMRCV_STTUS_CODE" : "S",
  "EIF_STTUS_MESSAGE" : "",
  "total_size" : 1,
  "device" : [ {
    "GRP_ID" : "org_0001",
    "POS_TIME" : "20190521095518",
    "LONGITUDE" : 127.3932698288816,
    "GRP_NM" : "조직1",
    "EQUIP_ID" : "test_equip_1234",
    "DEVICE_ID" : "DEVICE_506",
    "LATITUDE" : 37.21032067562426
  } ]
}
```

## Response Messages

HTTP Status Code	Reason	Response Model
Add Parameter	Try it out!	

## I-3.2) getDeviceLocation – 단말기 위치 정보

GET
getDeviceLocation - 단말기 위치 정보

단말기 위치 정보

요청 파라미터

파라미터	유형	필수	설명
device_id	string	Y	단말기 ID

```
// Request URL
https://openapi.safenet.go.kr:8443:/eif/gis/getDeviceLocation?EIF_INTFR_ID=GeoCommandTestAPI&EIF_INTFR_SNO=GeoCommandTestAPI&EIF_TRNSMIT_DT=20190402143524998&device_id=device_111
```

응답 파라미터

파라미터	유형	설명
EIF_TRSMRCV_STTUS_CODE	string	외부연계송수신상태코드(N : 전송, S : 성공, E : 오류)
EIF_STTUS_MSSAGE	string	외부연계상태메세지
DATA	object	단말기 정보
DEVICE_ID	string	단말기 ID
IMEI	string	사용자 ID
POS_TIME	string	위치 획득 시간
EQUIP_ID	string	기지국 ID
POSMETHOD	string	측위 방식(CELL: 기지국측위, GPS: GPS측위, WiFi: WiFi측위)
LON	string	경도
LAT	string	위도
ALTITUDE	number	고도
FLOOR	number	층수

```
// JSON Response Data
{
  "EIF_TRSMRCV_STTUS_CODE" : "S",
  "DATA" : {
    "REGT_DTTM" : "20190607182005887",
    "FLOOR" : 3,
    "POSMETHOD" : "CELL",
    "IMEI" : "4019283748291",
    "EQUIP_ID" : "test_equip_1234",
    "LON" : 127.2156,
    "POSTIME" : "20190517160900",
    "BUILDINGINFO" : "건물정보",
    "ALTITUDE" : 8.23,
    "DEVICE_ID" : "device_111",
    "LAT" : 36.65987
  },
  "EIF_STTUS_MSSAGE" : ""
}
```

### Parameters

Parameter	Value	Description
EIF_INTFR_ID	(required)	외부연계인터페이스아이디
EIF_INTFR_SNO	(required)	외부연계인터페이스등록순서
EIF_TRANSMIT_DT	(required)	외부연계전송일시
device_id	(required)	단말기 ID

### Response Messages

HTTP Status Code	Reason	Response Model
<div> <div>Add Parameter</div> <div>Try it out!</div> </div>		

### Add Parameter

Name

Value

Parameter Type

☐ Template
 ☐ Header
 ☒ Query

Cancel

Add

## [부록 J] 재난안전통신망 IPv6 주소체계 및 도입현황

### J-1) IPv6 개요 및 구조

#### □ IPv6 개요

- IPv4의 주소 길이는 32비트, IPv6의 주소 길이는 128비트이며 사용할 수 있는 주소 개수는 아래와 같다.

- IPv4 = 4,294,967,296(개)
- IPv6 = 340,282,366,920,938,463,463,374,607,431,768,211,456(개)

- IPv4 주소와 IPv6 주소 비교

구분	IPv4	IPv6
주소 길이	32 비트	128 비트
주소 개수	약 43 억개	약 43 억 x 43 억 x 43 억 x 43 억개
주소 할당	<ul style="list-style-type: none"> <li>•A, B, C 등 Class 단위의 비순차적 할당</li> <li>•IP 주소 관리가 어려움</li> </ul>	<ul style="list-style-type: none"> <li>•네트워크 규모 및 단말기 수에 따른 순차적 할당</li> <li>•IP 주소 관리가 용이함</li> </ul>
보안 기능	IPSec 프로토콜 별도 설치	확장 기능에서 IPSec 기본 제공
Mobile IP 주소 관리	상당히 어려움	용이함

- IPv6의 라우팅 성능

- IPv4의 불필요한 Header를 제거해서 오버헤드를 줄임
- Checksum Filed를 기본 Header에서 Extension Header로 이동시킴
- 기본적으로 Checksum을 하지 않음 : TCP, UDP에서 Checksum 함
- MTU Size를 맞추기 위해 IPv4는 Fragmentation, IPv6는 Packet 분할함

- IPv6의 장점

- 주소의 규모가 무대han이며, 주소를 설정하는 방식이 매우 단순함
- 주소의 코드화 및 계층화로 IP주소의 할당 및 관리가 용이
- 자동적인 주소 부여 기능 (Stateless Auto Configuration)
- 모바일 및 IoT 주소 체계를 설계하기에 용이함

## ○ IPv6 주소 신청

- 한국인터넷진흥원(KISA)에 독립사용자로 IPv6 주소 신청
  - 참조 URL : <https://krnic.or.kr/jsp/business/management/ipv6Reg.jsp>
  - 전화 번호 : 1433-25(수신자 요금 부담)
  - 신청 자격 : 두개 이상의 서로 다른 망과 연동하거나, 연동할 계획이 있는 경우
  - AS번호 미보유 기관의 경우 AS번호를 선 확보하신 후 IP주소 할당 신청을 해야 함
- 한국인터넷진흥원(KISA)의 관리 대행자에 IPv6 할당 신청
  - 관리 대행자 참조 URL : <https://krnic.or.kr/jsp/business/management/isCurrentIpv6.jsp>

## □ IPv6 구조

## ○ 기본 Header

- IPv6의 헤더는 기존 IPv4의 헤더보다 단순해짐으로써 성능이 향상되고 효율적인 라우팅이 가능함
- IPv6의 기본 헤더의 크기는 총 40바이트로 IPv4 헤더의 크기인 20바이트의 두 배임
- 가장 큰 차이점이라면 기존 IPv4 헤더에 있던 체크섬(header checksum)필드가 IPv6 헤더에서 삭제되었으며, 이 기능은 하위계층과 상위계층 프로토콜에서 진행함

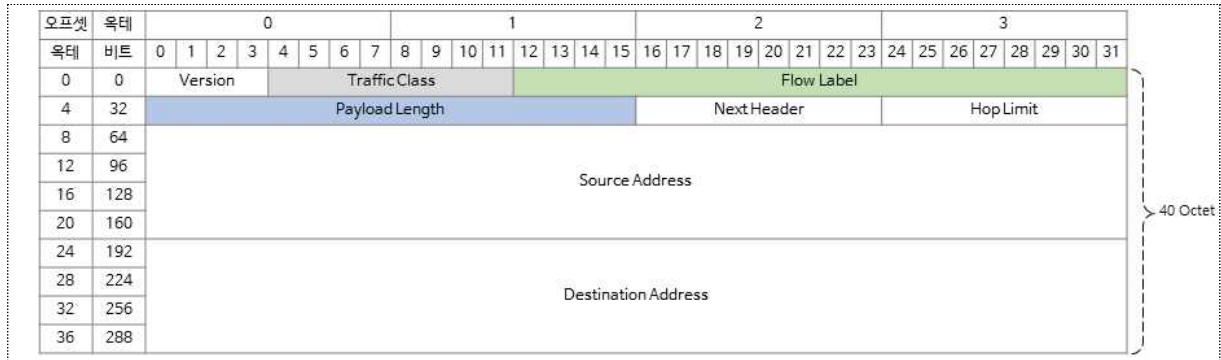
## ○ IPv4와 IPv6 Header 비교

- IPv4 Header

오프셋	옥테	0								1								2								3								
옥테	비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
0	0	Version				Hd Len				Type of Service								Total Length																} 20 Octet
4	32	Identification																Flags				Fragment Offset												
8	64	Time to Live								Protocol								Header Checksum																
12	96	Source Address																																
16	128	Destination Address																																
20	160	Options																																} 가변 길이
24	192																																	
28	224																																	
32	256																																	



- IPv6 Basic Header



- Header 기능 차이

- Traffic Class : Type Of Service 기능을 수행(Quality of Service)
- Payload Length : 전체 길이 필드가 사라지고 Payload 길이만 표시(4계층부터 Data길이)
- Next Header : Protocol 기능을 수행
- Hop Limit : TTL(Time To Live) 기능을 수행
- Flow Label : IPv4는 단편화 했을 경우 첫 번째 패킷만 QoS 기능을 수행, IPv6는 Flow Label을 통해서 모든 패킷에서 확인 가능
- IPv6는 패킷의 크기가 항상 40바이트로 고정 되어있기 때문에 헤더 길이 필드 (IHL)가 필요 없음

○ 확장 Header1

- 패킷을 전송할 때 평상시에는 IPv6 기본 헤더만으로 구성된 패킷을 사용
- 필요시 용도에 맞는 확장 헤더를 기본 헤더 뒤에 추가하며 확장 헤더 옵션은 아래와 같음
  - Hop-by-Hop : Path 상의 각 Hop에서, 배달 또는 전달 처리 옵션을 지정하기 위해 사용
  - Destination : Packet의 목적지에서, 배달 또는 전달 처리 옵션을 지정하기 위해 사용
  - Routing : IPv6 Source Node가 Packet이 Destination에 가는 동안 경유해야 할 라우터들을 지정
  - Fragmentation : 요청한 페이로드가 MTU보다 크면 IPv6 Source에서 페이로드를 조각내고, Fragmentation Option Header를 사용하여 리어셈블 정보를 제공하여 Destination Node가 재결합
  - Authentication : IPSec의 인증 헤더
  - Encapsulating Security Payload : IPSec의 인증 및 암호화 헤더

## J-2) IPv6의 주소표기 및 통신방식

### □ IPv6 주소 표기 방법



#### ○ 규칙 #1

- 16진수로 표시하며, 16진수 4개를 쓰고 Colon(:)으로 구분
- 2401:400A:0CA0:0001:0000:0000:0000:0D0B

#### ○ 규칙 #2

- Colon(:) 내의 앞쪽에 오는 "0"은 생략할 수 있음
- 2XXX:XXXX:CA0:1:0:0:0:D0B

#### ○ 규칙 #3

- "0"이 연속으로 나올 때는 Double Colon(::)으로 축약할 수 있음
- 2XXX:XXXX:CA0:1::D0B

### □ 프리픽스

- IPv6 주소의 "프리픽스"는 IPv4 주소의 '서브넷'과 유사한 개념으로 네트워크 규모 (길이) 또는 네트워크 주소로 표현됨

- 2001:4007:DB8::/48 (네트워크 주소 길이 : 48비트, 호스트 주소 길이 : 80비트, 라우팅 Table은 48비트)  
[ 2001:4007:0DB8:0000:0000:0000:0000:0000 ~ 2001:4007:0DB8:FFFF:FFFF:FFFF:FFFF:FFFF ]
- 2001:4007:DB8::/112 (네트워크 주소 길이 : 112비트, 호스트 주소 길이 : 16비트, 라우팅 Table은 48비트로 표현 가능함)  
[ 2001:4007:0ABA:0000:0000:0000:0000:0000 ~ 2001:4007:0ABA:0000:0000:0000:0000:FFFF ]

## □ IPv6 통신 방식

### ○ IPv4 vs IPv6 주소 종류

구분	IPv4	IPv6	비고
유니캐스트	O	O	
멀티캐스트	O	O	
브로드캐스트	O	X	네트워크에 불필요한 트래픽을 유발하여 IPv6에서는 사용하지 않음
애니캐스트	X	O	동일한 애니캐스트 주소를 가진 목적지 중 가장 근접한 Node로 Packet 전달

### ○ IPv4 vs IPv6 주소 관계

구분	IPv4	IPv6
멀티캐스트	224.0.0.0/4	FF00::/8
링크 로컬	169.254.0.0/16	FE80::64
브로드캐스트	•255.255.255.255 또는 •호스트 주소의 모든 Bit 가 1 인 경우	해당 사항 없음
루프백	127.0.0.1	::1/128
공인 IP	공인 IP 주소	Global Unicast Address
사설 IP	10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16	없음
멀티캐스트	O	O
브로드캐스트	O	X
애니캐스트	X	O

### J-3) ICMPv6

#### □ ICMPv6

##### ○ ICMPv6 개요

- ICMPv6는 ICMP 보다 더 많은 기능이 있음
- IPv4의 ICMP 기능에 PMTUD, MLD, NDP, 주소 자동설정 기능이 추가됨
- IPv6의 경우 ARP 역할을 ND(Neighbor Discover)가 수행하고 IGMP 역할을 MLD가 수행

##### ○ PMTUD(Path MTU Discovery)

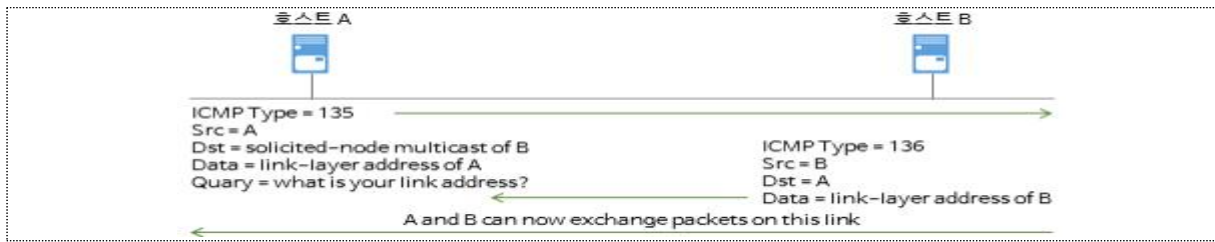
- PMTUD란 목적지로 가는 경로상에 존재하는 링크들 중 MTU 값이 가장 적은 링크의 MTU 값을 확인하는 과정
- IPv6에서는 오직 출발지 장비만이 IPv6 패킷을 분할할 수 있도록 규정함
- 그 이유는 IPv4에서 목적지로 가는 경로상의 중간 라우터들이 무분별한 분할을 수행함으로 인해 발생했던 라우팅 속도 저하를 막기 위함



- 위 그림에서 IPv4 네트워크에서의 출발지 호스트는 패킷을 전송할 때 자신의 링크 MTU 값에 패킷을 크기를 맞추어 전송함
- 아래 그림에서 IPv6 네트워크에서의 출발지 호스트는 목적지까지의 MTU 값을 확인 후 최소 MTU 값으로 패킷을 호스트 A에서 분할하여 전송함



- MLD(Multicast Listener Discovery) : MLD는 IPv4에서의 IGMP(internet group management)와 유사한 기능을 수행하는 프로토콜로서, 연결된 링크 상에 멀티캐스트 그룹에 소속되어 있는 호스트가 존재하는지의 여부를 확인하거나, 멀티캐스트 그룹에 소속되어 있는 호스트들의 관리를 목적으로 사용함
  - MLQ(Multicast Listener Query)
    - 멀티캐스트 그룹에 소속된 호스트가 존재하는지 여부를 확인하기 위한 ICMPv6 메시지
    - 메시지 전송 시, 출발지 주소는 자신의 링크 로컬 주소를 사용, 목적지는 all node multicast를 사용
  - MLR (Multicast Listener Report)
    - MLQ메시지를 받은 대상이 응답을 위해 사용하는 ICMPv6 메시지
    - 메시지 전송 시 출발지 주소는 자신의 링크 로컬 주소를 사용, 목적지는 MLQ 메시지를 보낸 상대방의 링크 로컬 주소를 사용
  - MLD(Multicast Listener Done)
    - 특정 멀티캐스트 그룹에서 탈퇴할 경우 라우터에게 보내는 ICMPv6 메시지
    - 메시지 전송 시 출발지 주소는 자신의 링크 로컬 주소를 사용, 목적지는 all router multicast 주소를 사용, ICMPv6는 ICMP 보다 더 많은 기능이 있음
- NDP(Neighbor Discovery Protocol) : NDP는 IPv4에서의 ARP와 유사 역할을 수행함. IPv6를 통해 MAC 주소를 알아내고 또한, 상대방과의 통신을 가능하게 함
  - A는 B와 통신하기 위하여 상대방의 MAC 및 링크 로컬 주소를 알아야 하기 때문에 A는 B에게 자신의 링크 로컬 주소를 기반으로 Solicited Node Multicast 그룹으로 NS 메시지를 전송함
  - B는 NS 메시지를 전송 받은 후 A에서 요청한 MAC 및 링크 로컬 주소를 NA 메시지를 통하여 응답함. 이때 B는 A의 링크 로컬 주소를 알고 있기 때문에 출발지를 자신으로, 목적지를 A의 주소로 설정하여 메시지를 전송함
  - A와 B가 서로의 정보를 모두 주고 받으면 IPv6 neighbor 정보에 MAC과 링크 로컬 주소가 등록되어 서로 통신이 가능함



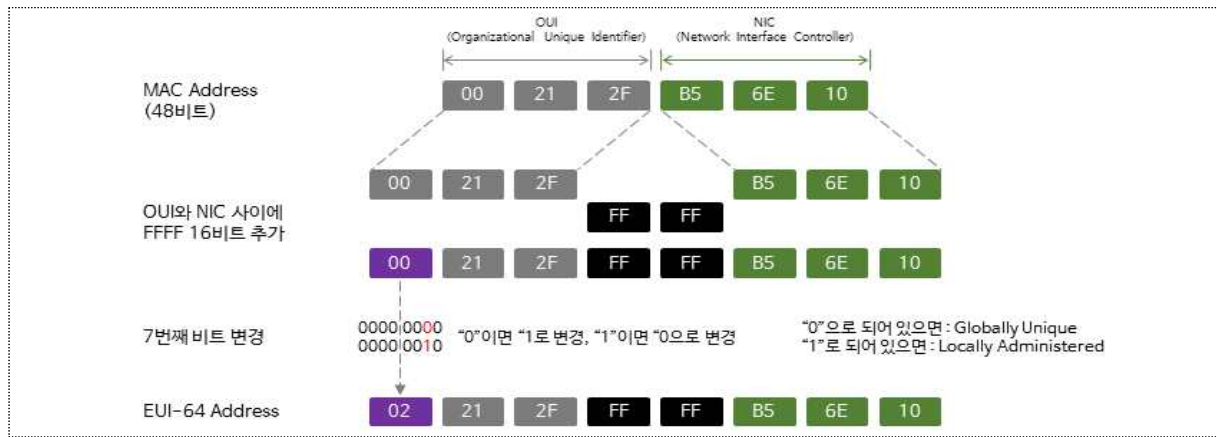
○ DAD(Duplicate Address Detection) : 처음 인터페이스가 활성화된 호스트는 자신과 인접한 라우터의 존재 유무를 확인하고 해당 라우터와 통신하기 위해 스스로 링크 로컬주소를 생성함. 이때 호스트는 링크상에 자신이 사용할 주소와 동일한 주소를 사용하는 장비가 존재하는지 확인하는 과정을 DAD 과정이라고 함

- 호스트 A는 EUI-64 Format으로 링크 로컬 주소를 생성하고 이 주소에 대한 DAD 과정을 수행하기 위해 NS 메시지를 전송함
- NS 메시지의 출발지 IPv6는 '::'(미 지정 주소)를 사용하며, 목적지 주소는 자신이 부여할 FE80::2:260:8FF:FE52:F9D8를 기반으로 한 FF02::1:FF52:F9D8 solicited node multicast 주소를 보냄
- 링크 상에 동일한 주소를 사용하고 있는 장비가 없을 경우 응답 메시지가 전송되지 않으며, 동일 주소가 존재하는 장비가 있다면 NS 메시지에 대한 응답으로 NA 메시지를 전송



○ EUI(Extended Unique Identifier)-64 : IEEE 표준으로, 링크 계층상에서 유일 식별성을 갖추기 위한 주소 형식

- 48비트인 MAC 주소에 "FFFE" 16비트를 결합하여 IPv6 하위 64비트 부분인 인터페이스 ID정보를 생성하는 방식
- RS, RA 메시지를 이용한 /64의 프리픽스와 EUI-64 방식은 인터페이스 ID부분이 결합하여 IPv6 주소 설정



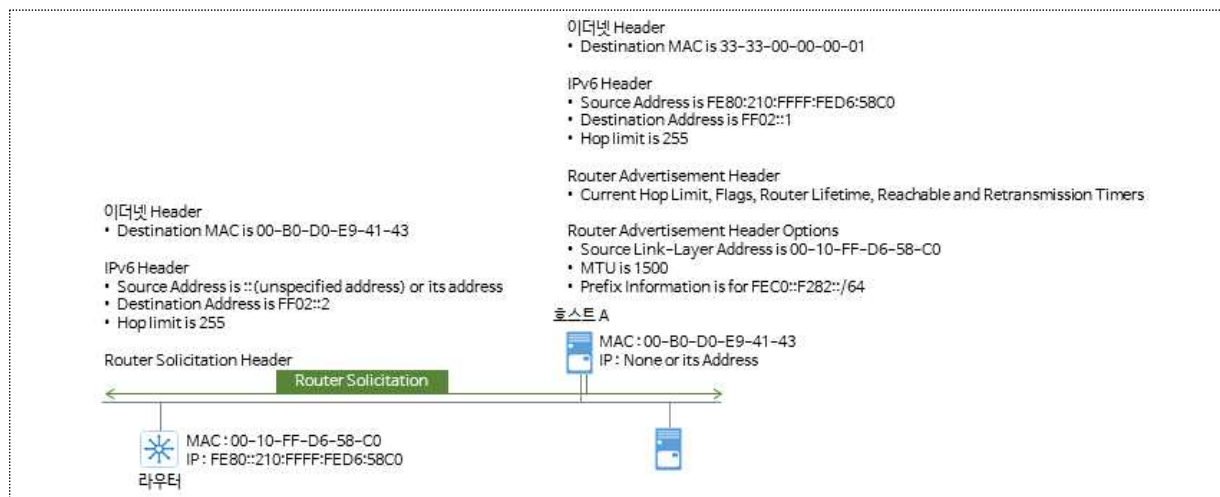
○ Stateless Auto Configuration : Stateless Auto Configuration은 DHCP와 같이 별도의 설정이 없더라도 라우터와의 상호 작용으로 자동으로 글로벌 주소를 획득할 수 있는 기능. RS, RA의 메시지로 이루어지며 EUI-64 포맷을 기반 동작함

- RS(Router Solicitation)

- 글로벌 주소를 생성하기 위하여 현재 라우터가 사용하고 있는 글로벌 프리픽스를 요청하는 메시지
- 출발지 주소는 자신의 링크 로컬 주소 혹은 미 확정 주소(::)를 이용하며 목적지 주소는 all router multicast 주소를 사용

- RA(Router Advertisement)

- RS 메시지에 대한 응답메시지로 라우터 인터페이스에 설정된 글로벌 /64의 프리픽스 정보를 포함한 정보들을 제공
- 출발지 주소는 자신의 링크 로컬 주소를 이용하며, 목적지 주소는 all node multicast 주소를 사용



## J-4) IPv6 전환 기술

### □ IPv6 전환 기술

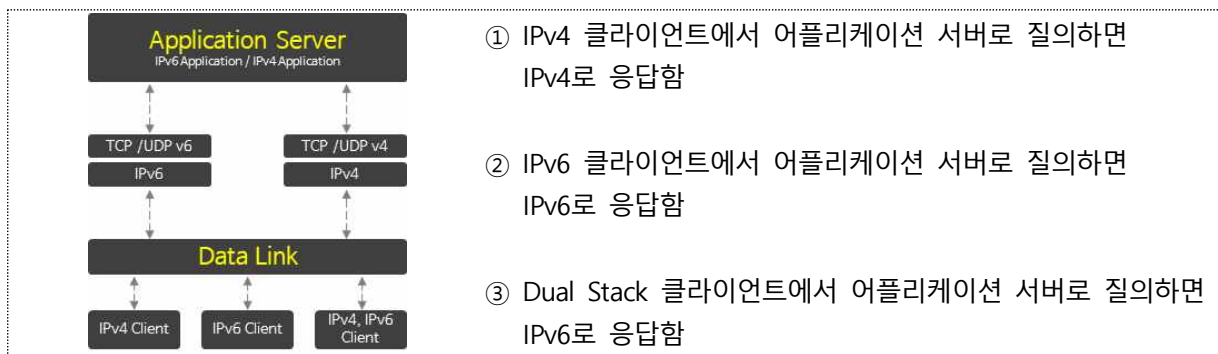
#### ○ 재난안전통신망 인프라 아키텍처 기준

- 코어망 설비, 운영관리 설비, 응용 설비 통신 규격 : All IPv6
- 단말 통신 규격 : All IPv6
- 단, 타망 연동 등으로 인하여 불가피한 경우에 한하여 IPv6 점점 기술 사용
  - 상용망 및 공공망 RAN Sharing : 연동용 스위치 및 EPC 장비만 Dual Stack 적용함
  - 행정 전화망 : IPv4 신호를 MGCF SBC(Session Border Controller)에서 IP Header 및 Payload 최적화
  - 선박형 이동기지국 시범 사업 : 해양경찰청 위성 백홀이 IPv4 이기 때문에, IPSec VPN Tunneling을 통하여 EPC 장비와 기지국 장비 간 통신함
- 재난안전통신망 코어 백본스위치에 IPv4 Routing Table은 존재하지 않음

#### ○ IPv4 전환 기술이란? IPv6가 레거시인 IPv4와 통신하기 위한 기술

#### ○ Dual Stack

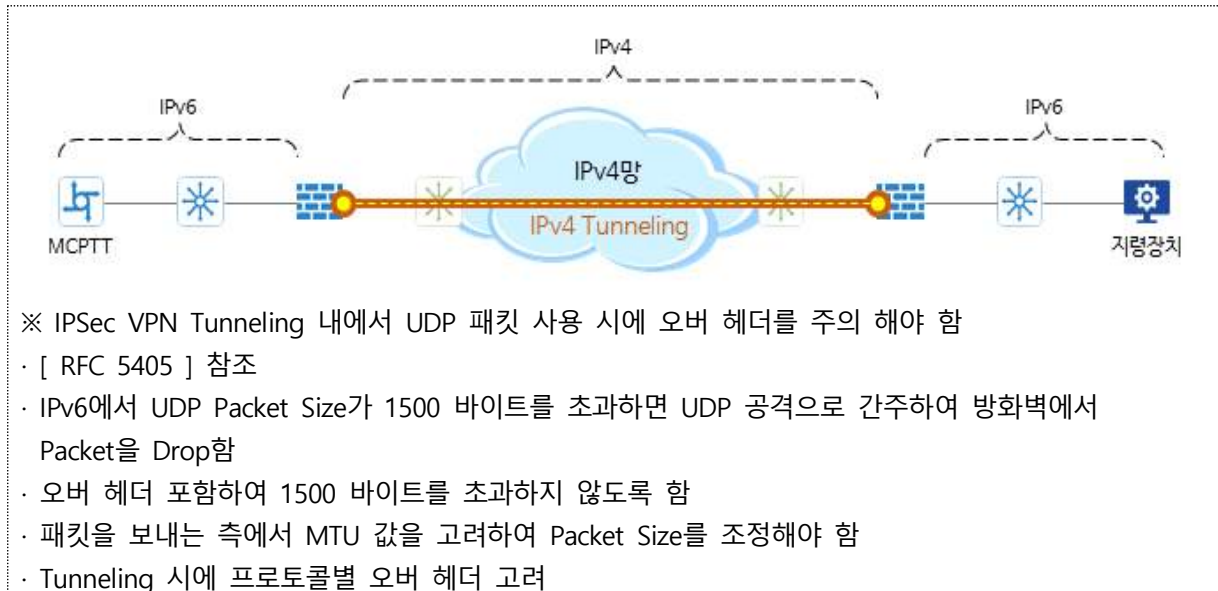
- 가장 일반적인 IPv6 전환 기술
- 어플리케이션 서버와 어플리케이션 서버, 어플리케이션 서버와 클라이언트 간 End to End 정의됨
- 통신망 내에서 IP Node가 IPv4, IPv6 Network을 동시에 가지고 있기 때문에 통신하는데 별다른 특이사항이 없음
- IPv4 주소 고갈에 도움이 되지 않으며, Dual Stack은 IPv6 보다는 IPv4망이라고 판단하는 것이 적합함





## ○ Tunneling

- IPv4 위성 백홀망, 국가정보통신 업무망, 기존 IPv4 업무망에서 재난안전통신망과 PTT, VoLTE 통신
- 재난안전통신망은 VoLTE, PTT를 위해서 표준 SIP를 사용하고 있음
- SIP의 특성상 IPv4 Hop을 제거해야 음성 및 영상 통신이 가능함



## ○ Translation

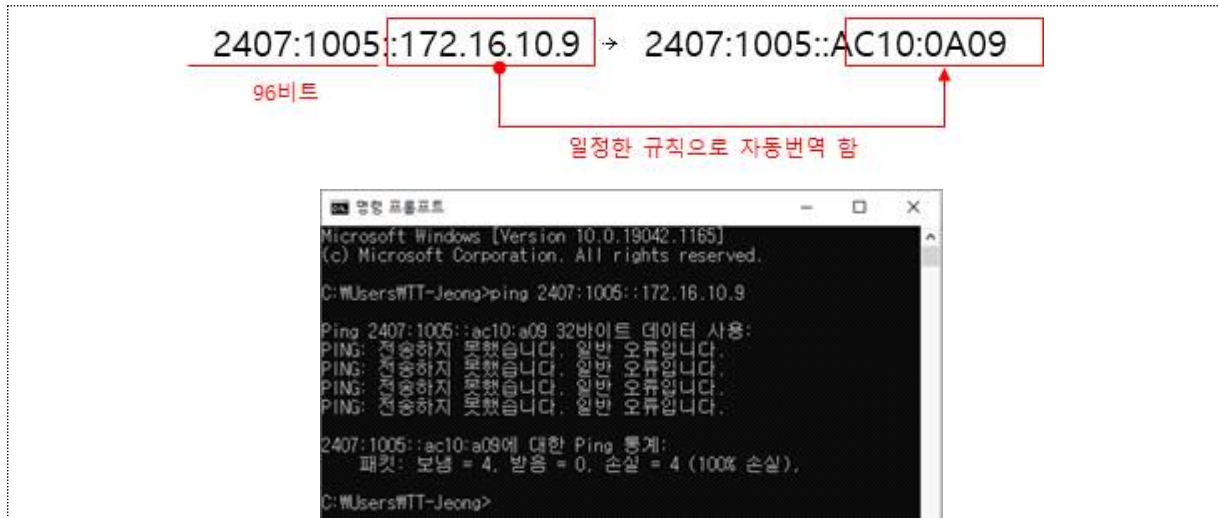
- IPv4 Header를 IPv6 Header로 변환 또는 IPv6 Header를 IPv4 Header로 변환
- Payload는 변환할 수 없음
- SIP, RTP, SCTP 등 Real Time 프로토콜은 Payload에 민감하여 IP 프로토콜 변환 시에 음성/영상 통신이 되지 않음



- NAT 6 to 4
  - IPv6 Real IP Address를 IPv4의 Virtual IP로 Mapping하기 위한 방법
  - "1 : 1", "N : 1" Mapping이 가능함
  - 진화된 프로토콜이 레거시 프로토콜이 변환되기 때문에 비교적 제약사항이 없음

- NAT 4 to 6

- IPv4 Real IP Address를 IPv6의 Virtual IP로 Mapping하기 위한 방법
- IPv4의 "0.0.0.0" 네트워크 개수와 IPv6의 "/96" 개수가 동일하며, 서로 간의 주소 체계가 사전 Mapping 되어 있음
- "1 : 1" Mapping이 기본이며, 제조사에 따라 "N : 1" Mapping도 가능함



## J-5) IPv6 주소 체계화

## □ 센터, 백홀, 단말기 등 구분

2XXX:XXXX:X000:0000:0000:0000:0000:0000

재난안전통신망 프리픽스: 36비트

설비, 네트워크 구분	
번호(4bit)	용도
0	N/A
1	서울운영센터
2	대구운영센터
3	제주운영센터
4	이동기지국, 위성백홀
5	LTE 단말기
6	미할당
7	IoT 단말기
8	미할당
9	7 대 사용기관
A	A 사업구역 Backhaul
B	B 사업구역 Backhaul
C	C 사업구역 Backhaul
D	미할당
E	미할당
F	지방자치단체

## ○ IPv6 주소 체계화 방법

- 프리픽스 앞자리부터 코드화
- 재난안전통신망은 36비트 프리픽스를 갖추고 있어, 40비트부터 IPv6 주소 설계를 진행함
- 40비트에서 센터, 단말기, 사용기관 코드를 부여하여 IP 중복(충돌) 방지
- 프리픽스만으로도 IP 주소 추적이 가능함

## ○ 센터 구분

- 서울운영센터 : [ 2XXX:XXXX:X100::/40 ]
- 대구운영센터 : [ 2XXX:XXXX:X200::/40 ]
- 제주운영센터 : [ 2XXX:XXXX:X300::/40 ]

## ○ 광역 백홀 구분

- A 사업구역(서울, 대구, 대전, 세종, 경북, 충남, 제주) : [ 2XXX:XXXX:XA00::/40 ]
- B 사업구역(광주, 경기, 강원, 전북, 전남) : [ 2XXX:XXXX:XB00::/40 ]
- C 사업구역(부산, 인천, 울산, 충북, 경남) : [ 2XXX:XXXX:XC00::/40 ]
- 이동기지국, 위성 : [ 2XXX:XXXX:X400::/40 ]

## ○ 단말기 구분

- LTE 단말 : [ 2XXX:XXXX:X500::/40 ]
- IoT 단말 : [ 2XXX:XXXX:X700::/40 ]

## ○ 사용기관 구분

- 경찰, 소방, 국방부, 해양경찰청, 가스, 전기, 의료 : [ 2XXX:XXXX:X900::/40 ]
- 지방자치단체 : [ 2XXX:XXXX:XF00::/40 ]

## □ 서울운영센터 설비 구분

2XXX:XXXX:X100:0000:0000:0000:0000:0000

재난안전통신망 프리픽스: 36비트

설비 구분	
번호(4bit)	용도
0	N/A
1	코어망 설비
2	응용 설비
3	운영관리 설비
4	미할당
5	미할당
6	미할당
7	미할당
8	네트워크 설비
9	미할당
A	미할당
B	미할당
C	미할당
D	미할당
E	미할당
F	미할당

- 44비트에서 센터 설비를 코드화 함
- 서울운영센터 설비 IP 주소 코드화가 완료되면, 대구 및 제주운영센터 IP 주소 설계는 센터 프리픽스만 변경하면 됨
- 서울센터 설비 구분
  - 코어망 설비(EPC, IMS, MCPTT 등) : [ 2XXX:XXXX:X110::/44 ]
  - 응용 설비(포털 등 어플리케이션) : [ 2XXX:XXXX:X120::/44 ]
  - 운영관리 설비(NMS, 과금, ESM 등) : [ 2XXX:XXXX:X130::/44 ]
  - 네트워크 설비(스위치, 방화벽 등) : [ 2XXX:XXXX:X180::/44 ]

## □ 서울운영센터 설비 구분

[ IPv6 주소 체계화 : 네트워크 기능 구분 ]

2XXX:XXXX:X180:0000:0000:0000:0000:0000

재난안전통신망 프리픽스 : 36비트

12비트 : 네트워크 ID

[ 규모에 맞는 프리픽스 선언 ]  
Loopback : 128비트  
Point to Point : 126비트  
VRRP : 124비트

네트워크 기능 구분	
번호(4bit)	용도
0	N/A
1	Loopback
2	Backhaul I/F
3	Interlink
4	방화벽 I/F
5	스위치 I/F
6	전용회선 I/F
7	C 사업자 I/F
8	미할당
9	미할당
A	미할당
B	미할당
C	미할당
D	미할당
E	미할당
F	미할당

- 48비트에서 네트워크 기능을 코드화 함
  - 코드화는 48비트이지만, 프리픽스는 128비트, 126비트 등 네트워크 규모에 따라 선언함
  - IP 주소를 확인해서 End to End로 트러블 슈팅이 가능
  - 라우팅 Table 연동은 최종 선언된 프리픽스로 설계함
- 네트워크 기능 구분
  - 네트워크 장비 루프백 : [ 2XXX:XXXX:X181::/128 ]
  - 재난안전통신망 코어 백본스위치 ~ 광역 집선 스위치 시리얼 I/F : [ 2XXX:XXXX:X182::/126 ]
  - 네트워크 장비 인터링크 : [ 2XXX:XXXX:X183::/126 ]
  - 방화벽 ~ 스위치 I/F : [ 2XXX:XXXX:X184::/124 ]
  - 스위치 ~ 스위치 I/F : [ 2XXX:XXXX:X185::/126 ]
  - 전용선 스위치 ~ 사용기관 스위치 I/F : [ 2XXX:XXXX:X186::/126 ]
  - C 사업자 스위치 I/F : [ 2XXX:XXXX:X187::/126 ]
- 예시
  - EPC 백본스위치 #1 루프백 : [ 2XXX:XXXX:X181::1/128 ]
  - MGMT 백본스위치 #1 루프백 : [ 2XXX:XXXX:X181::55/128 ]
  - EPC 백본스위치 #1과 MMSC L3 스위치 #1 Point to Point : [ 2XXX:XXXX:X185:1340::1/126 ]
  - DMZ 백본스위치와 DMZ 방화벽 VRRP : [ 2XXX:XXXX:X184:4810::1/124 ] ~ [ 2XXX:XXXX:X184:4810::6/124 ]

## □ 네트워크 위치 구분

**2XXX:XXXX:X000:0000:0000:0000:0000:0000**  
재난안전통신망 프리픽스: 36비트

시스템 위치 구분	
번호(4bit)	용도
0	N/A
1	EPC Zone
2	SF Zone
3	DMZ Zone
4	MGMT Zone
5	미할당
6	미할당
7	미할당
8	미할당
9	미할당
A	미할당
B	미할당
C	미할당
D	미할당
E	미할당
F	미할당

- 운영센터 내 코어망, 응용, 운영관리 등 위치를 52비트 프리픽스로 코드화 함
  - 방화벽으로 영역을 분리함
  - 센터 내의 설비 IP 주소 체계와 조합하여 IP 중복을 한번 더 회피함
  - IPv6 주소 체계의 보조 역할을 담당하여 프리픽스 선언 및 라우팅 설계와는 무관함
- 네트워크 위치 구분
  - EPC, IMS, 문자 등 LTE 통신 처리를 하는 장비들의 Zone : [ 2XXX:XXXX:XXXX:1000::/52 ]
  - 응용/운영관리 설비, 클라우드 플랫폼 등이 있는 서버팜 Zone : [ 2XXX:XXXX:XXXX:2000::/52 ]
  - WEB, 통신 Gateway 등이 위치하는 DMZ Zone : [ 2XXX:XXXX:XXXX:3000::/52 ]
  - NAC, DLP 및 운영자 단말 등 관리를 위한 Management Zone : [ 2XXX:XXXX:XXXX:4000::/52 ]

## □ 어플리케이션 IP 배치(예시)



- 직관화를 위하여 VLAN ID를 코드화
  - 시스템 : VLAN 101 ~ 999 사용
  - 네트워크 : VRRP VLAN 또는 시리얼 ID 1001 ~ 4094 사용
- 시스템 규모를 산정하여 프리픽스 선언
  - 124비트 : [ 2XXX:XXXX:XXXX::0000 ] ~ [ 2XXX:XXXX:XXXX::000F ]
  - 120비트 : [ 2XXX:XXXX:XXXX::0000 ] ~ [ 2XXX:XXXX:XXXX::00FF ]
  - 116비트 : [ 2XXX:XXXX:XXXX::0000 ] ~ [ 2XXX:XXXX:XXXX::0FFF ]
  - 112비트 : [ 2XXX:XXXX:XXXX::0000 ] ~ [ 2XXX:XXXX:XXXX::FFFF ]
- 라우팅 Table 설계
  - 시스템 프리픽스는 124 ~ 112비트이지만 VLAN ID에서 구분이 가능하기 때문에 80비트로 설계함
- 예시
  - BSS WAS 서버 #1 : [ 2XXX:XXXX:X120:2000:101::11/112 ]
    - X120 : 서울운영센터 응용 설비
    - 2000 : 시스템의 위치는 SF Zone에 있음
    - 0101 : VLAN 101을 사용함
    - 0011/112 : 프리픽스는 112비트이며, 호스트 IP 주소는 "11"임

시스템 VLAN ID와 매핑 (예시 )

번호 (12 bit)	용도
0	N/A
101	클라우드 APP •WAS 서버 그룹 #1
102	클라우드 APP •WAS 서버 그룹 #2
103	클라우드 DB 서버
121	UMC, OFCS
122	NMS, LTAS
201	WEB •Gateway 서버
301	DLP, NAC, WIPS
302	운영자동화 서버
303	화상회의
305	콜센터 (Help Desk)
306	운영자 •관리자 PC
311	관제 시스템 •PC
401	클라우드 L4 VIP
501	NTP •PTP
502	MRF, IBCF, TrGW
503	CSC
504	DNS
505	지령 서버
506	MMSC, SMSC, CBMC
507	MGCF
508	녹음녹화
700 ~ 799	EPC, MCPTT 등
800 ~ 899	C 사업자 (SKT) 시스템

## J-6) 사용기관 IPv6 주소할당

### □ 경찰청, 소방청, 해양경찰청, 국방부 등

2XXX:XXXX:X900:0000:0000:0000:0000:0000  
재난안전통신망 프리픽스: 36비트

사용기관 구분	
번호 (4 bit)	용도
0	N/A
1	경찰청
2	소방청
3	해양경찰청
4	미할당
5	국방부
6	전기
7	가스
8	의료
9	재난안전통신망 외부
A	미할당
B	미할당
C	미할당
D	미할당
E	미할당
F	미할당

### □ 소방청, 시도 소방본부

[ 이용기관 IPv6 주소 할당 : 소방청, 시도 소방본부 ]

2XXX:XXXX:X920:0000:0000:0000:0000:0000  
재난안전통신망 프리픽스: 36비트

소방청 구분	
번호 (4 bit)	용도
0	시도 소방본부
1	소방청 (세종)
2	중앙 119 구조본부 (대구)
3	미할당
4	미할당
5	미할당
6	미할당
7	미할당
8	미할당
9	미할당
A	미할당
B	미할당
C	미할당
D	미할당
E	미할당
F	미할당

시도 소방본부 구분	
번호 (8 bit)	용도
00	N/A
01	서울소방재난본부 (SU)
02	부산소방재난본부 (BS)
03	대구소방안전본부 (DG)
04	인천소방본부 (IC)
05	광주소방안전본부 (GJ)
06	대전소방본부 (DJ)
07	울산소방본부 (US)
08	세종소방본부 (SJ)
09	경기남부소방재난본부 (GGN)
10	경기북부소방재난본부 (GGB)
11	강원소방본부 (GW)
12	충북소방본부 (CB)
13	충남소방본부 (CN)
14	전북소방본부 (JB)
15	전남소방본부 (JN)



## □ 지방자치단체 (1/2)

2XXX:XXXX:X F00:0000:0000:0000:0000:0000

재난안전통신망 프리픽스: 36비트

광역시도 구분	
번호 (8 bit)	용도
00	N/A
01	서울특별시
02	부산광역시
03	대구광역시
04	인천광역시
05	광주광역시
06	대전광역시
07	울산광역시
08	세종특별자치시
09	경기도
10	강원도
11	충청북도
12	충청남도
13	전라북도
14	전라남도
15	경상북도
16	경상남도
17	제주특별자치도

광역시도	프리픽스	시군구 구분	프리픽스
서울특별시	2XXX:XXXX:F01::/48	서울특별시(내부)	2XXX:XXXX:F01:1000::/56
		종로구	2XXX:XXXX:F01:1100::/56
		중구	2XXX:XXXX:F01:1200::/56
		용산구	2XXX:XXXX:F01:1300::/56
		성동구	2XXX:XXXX:F01:1400::/56
		광진구	2XXX:XXXX:F01:1500::/56
		동대문구	2XXX:XXXX:F01:1600::/56
		중랑구	2XXX:XXXX:F01:1700::/56
		성북구	2XXX:XXXX:F01:1800::/56
		강북구	2XXX:XXXX:F01:1900::/56
		도봉구	2XXX:XXXX:F01:2000::/56
		노원구	2XXX:XXXX:F01:2100::/56
		은평구	2XXX:XXXX:F01:2200::/56
		서대문구	2XXX:XXXX:F01:2300::/56
		마포구	2XXX:XXXX:F01:2400::/56
		양천구	2XXX:XXXX:F01:2500::/56
		강서구	2XXX:XXXX:F01:2600::/56
		구로구	2XXX:XXXX:F01:2700::/56
		금천구	2XXX:XXXX:F01:2800::/56
		영등포구	2XXX:XXXX:F01:2900::/56
		동작구	2XXX:XXXX:F01:3000::/56
		관악구	2XXX:XXXX:F01:3100::/56
		서초구	2XXX:XXXX:F01:3200::/56
		강남구	2XXX:XXXX:F01:3300::/56
		송파구	2XXX:XXXX:F01:3400::/56
		강동구	2XXX:XXXX:F01:3500::/56

광역시도	프리픽스	시군구 구분	프리픽스
부산광역시	2XXX:XXXX:F02::/48	부산광역시 (내부 )	2XXX:XXXX:F02:1000::/56
		중구	2XXX:XXXX:F02:1100::/56
		서구	2XXX:XXXX:F02:1200::/56
		동구	2XXX:XXXX:F02:1300::/56
		영도구	2XXX:XXXX:F02:1400::/56
		부산진구	2XXX:XXXX:F02:1500::/56
		동래구	2XXX:XXXX:F02:1600::/56
		남구	2XXX:XXXX:F02:1700::/56
		북구	2XXX:XXXX:F02:1800::/56
		해운대구	2XXX:XXXX:F02:1900::/56
		사하구	2XXX:XXXX:F02:2000::/56
		금정구	2XXX:XXXX:F02:2100::/56
		강서구	2XXX:XXXX:F02:2200::/56
		연제구	2XXX:XXXX:F02:2300::/56
		수영구	2XXX:XXXX:F02:2400::/56
		사상구	2XXX:XXXX:F02:2500::/56
		기장군	2XXX:XXXX:F02:2600::/56
대구광역시	2XXX:XXXX:F03::/48	대구광역시 (내부 )	2XXX:XXXX:F03:1000::/56
		중구	2XXX:XXXX:F03:1100::/56
		동구	2XXX:XXXX:F03:1200::/56
		서구	2XXX:XXXX:F03:1300::/56
		남구	2XXX:XXXX:F03:1400::/56
		북구	2XXX:XXXX:F03:1500::/56
		수성구	2XXX:XXXX:F03:1600::/56
		달서구	2XXX:XXXX:F03:1700::/56
		달성군	2XXX:XXXX:F03:1800::/56
인천광역시	2XXX:XXXX:F04::/48	인천광역시 (내부 )	2XXX:XXXX:F04:1000::/56
		중구	2XXX:XXXX:F04:1100::/56
		동구	2XXX:XXXX:F04:1200::/56
		남구	2XXX:XXXX:F04:1300::/56
		연수구	2XXX:XXXX:F04:1400::/56
		남동구	2XXX:XXXX:F04:1500::/56
		부평구	2XXX:XXXX:F04:1600::/56
		계양구	2XXX:XXXX:F04:1700::/56
		서구	2XXX:XXXX:F04:1800::/56
		강화군	2XXX:XXXX:F04:1900::/56
		옹진군	2XXX:XXXX:F04:2000::/56
광주광역시	2XXX:XXXX:F05::/48	광주광역시 (내부 )	2XXX:XXXX:F05:1000::/56
		동구	2XXX:XXXX:F05:1100::/56
		서구	2XXX:XXXX:F05:1200::/56
		남구	2XXX:XXXX:F05:1300::/56
		북구	2XXX:XXXX:F05:1400::/56
대전광역시	2XXX:XXXX:F06::/48	광산구	2XXX:XXXX:F05:1500::/56
		대전광역시 (내부 )	2XXX:XXXX:F06:1000::/56
		동구	2XXX:XXXX:F06:1100::/56
		중구	2XXX:XXXX:F06:1200::/56
		서구	2XXX:XXXX:F06:1300::/56
		유성구	2XXX:XXXX:F06:1400::/56
울산광역시	2XXX:XXXX:F07::/48	대덕구	2XXX:XXXX:F06:1500::/56
		울산광역시 (내부 )	2XXX:XXXX:F07:1000::/56
		중구	2XXX:XXXX:F07:1100::/56
		남구	2XXX:XXXX:F07:1200::/56
		동구	2XXX:XXXX:F07:1300::/56
		북구	2XXX:XXXX:F07:1400::/56
		울주군	2XXX:XXXX:F07:1500::/56

광역시도	프리픽스	시군구 구분	프리픽스
세종특별자치시	2XXX:XXXX:F08::/48	세종특별자치시 (내부 )	2XXX:XXXX:F08:1000::/56
경기도	2XXX:XXXX:F09::/48	경기도 (내부 )	2XXX:XXXX:F09:1000::/56
		수원시	2XXX:XXXX:F09:1100::/56
		고양시	2XXX:XXXX:F09:1200::/56
		성남시	2XXX:XXXX:F09:1300::/56
		용인시	2XXX:XXXX:F09:1400::/56
		부천시	2XXX:XXXX:F09:1500::/56
		안산시	2XXX:XXXX:F09:1600::/56
		남양주시	2XXX:XXXX:F09:1700::/56
		안양시	2XXX:XXXX:F09:1800::/56
		화성시	2XXX:XXXX:F09:1900::/56
		평택시	2XXX:XXXX:F09:2000::/56
		의정부시	2XXX:XXXX:F09:2100::/56
		시흥시	2XXX:XXXX:F09:2200::/56
		파주시	2XXX:XXXX:F09:2300::/56
		김포시	2XXX:XXXX:F09:2400::/56
		광명시	2XXX:XXXX:F09:2500::/56
		광주시	2XXX:XXXX:F09:2600::/56
		군포시	2XXX:XXXX:F09:2700::/56
		오산시	2XXX:XXXX:F09:2800::/56
		이천시	2XXX:XXXX:F09:2900::/56
		양주시	2XXX:XXXX:F09:3000::/56
		안성시	2XXX:XXXX:F09:3100::/56
		구리시	2XXX:XXXX:F09:3200::/56
		포천시	2XXX:XXXX:F09:3300::/56
		의왕시	2XXX:XXXX:F09:3400::/56
		하남시	2XXX:XXXX:F09:3500::/56
		여주시	2XXX:XXXX:F09:3600::/56
		양평군	2XXX:XXXX:F09:3700::/56
경기도	2XXX:XXXX:F09::/48	동두천시	2XXX:XXXX:F09:3800::/56
		과천시	2XXX:XXXX:F09:3900::/56
		가평군	2XXX:XXXX:F09:4000::/56
		연천군	2XXX:XXXX:F09:4100::/56
강원도	2XXX:XXXX:F10::/48	강원도 (내부 )	2XXX:XXXX:F10:1000::/56
		춘천시	2XXX:XXXX:F10:1100::/56
		원주시	2XXX:XXXX:F10:1200::/56
		강릉시	2XXX:XXXX:F10:1300::/56
		동해시	2XXX:XXXX:F10:1400::/56
		태백시	2XXX:XXXX:F10:1500::/56
		속초시	2XXX:XXXX:F10:1600::/56
		삼척시	2XXX:XXXX:F10:1700::/56
		홍천군	2XXX:XXXX:F10:1800::/56
		횡성군	2XXX:XXXX:F10:1900::/56
		영월군	2XXX:XXXX:F10:2000::/56
		평창군	2XXX:XXXX:F10:2100::/56
		정선군	2XXX:XXXX:F10:2200::/56
		철원군	2XXX:XXXX:F10:2300::/56
		화천군	2XXX:XXXX:F10:2400::/56
		인제군	2XXX:XXXX:F10:2500::/56
		고성군	2XXX:XXXX:F10:2600::/56
		양양군	2XXX:XXXX:F10:2700::/56

광역시도	프리픽스	시군구 구분	프리픽스
충청북도	2XXX:XXXX:F11::/48	충청북도 (내부 )	2XXX:XXXX:F11:1000::/56
		청주시	2XXX:XXXX:F11:1100::/56
		충주시	2XXX:XXXX:F11:1200::/56
		제천시	2XXX:XXXX:F11:1300::/56
		보은군	2XXX:XXXX:F11:1400::/56
		옥천군	2XXX:XXXX:F11:1500::/56
		영동군	2XXX:XXXX:F11:1600::/56
		증평군	2XXX:XXXX:F11:1700::/56
		진천군	2XXX:XXXX:F11:1800::/56
		괴산군	2XXX:XXXX:F11:1900::/56
		음성군	2XXX:XXXX:F11:2000::/56
		단양군	2XXX:XXXX:F11:2100::/56
충청남도	2XXX:XXXX:F12::/48	충청남도 (내부 )	2XXX:XXXX:F12:1000::/56
		천안시	2XXX:XXXX:F12:1100::/56
		공주시	2XXX:XXXX:F12:1200::/56
		보령시	2XXX:XXXX:F12:1300::/56
		아산시	2XXX:XXXX:F12:1400::/56
		서산시	2XXX:XXXX:F12:1500::/56
		논산시	2XXX:XXXX:F12:1600::/56
		계룡시	2XXX:XXXX:F12:1700::/56
		당진시	2XXX:XXXX:F12:1800::/56
		금산군	2XXX:XXXX:F12:1900::/56
		부여군	2XXX:XXXX:F12:2000::/56
		서천군	2XXX:XXXX:F12:2100::/56
		청양군	2XXX:XXXX:F12:2200::/56
		홍성군	2XXX:XXXX:F12:2300::/56
		예산군	2XXX:XXXX:F12:2400::/56
		태안군	2XXX:XXXX:F12:2500::/56
전라북도	2XXX:XXXX:F13::/48	전라북도 (내부 )	2XXX:XXXX:F13:1000::/56
		전주시	2XXX:XXXX:F13:1100::/56
		군산시	2XXX:XXXX:F13:1200::/56
		익산시	2XXX:XXXX:F13:1300::/56
		정읍시	2XXX:XXXX:F13:1400::/56
		남원시	2XXX:XXXX:F13:1500::/56
		김제시	2XXX:XXXX:F13:1600::/56
		완주군	2XXX:XXXX:F13:1700::/56
		진안군	2XXX:XXXX:F13:1800::/56
		무주군	2XXX:XXXX:F13:1900::/56
		장수군	2XXX:XXXX:F13:2000::/56
		임실군	2XXX:XXXX:F13:2100::/56
		순창군	2XXX:XXXX:F13:2200::/56
		고창군	2XXX:XXXX:F13:2300::/56
		부안군	2XXX:XXXX:F13:2400::/56

광역시도	프리픽스	시군구 구분	프리픽스
전라남도	2XXX:XXXX:F14::/48	전라남도 (내부 )	2XXX:XXXX:F14:1000::/56
		목포시	2XXX:XXXX:F14:1100::/56
		여주시	2XXX:XXXX:F14:1200::/56
		순천시	2XXX:XXXX:F14:1300::/56
		나주시	2XXX:XXXX:F14:1400::/56
		광양시	2XXX:XXXX:F14:1500::/56
		담양군	2XXX:XXXX:F14:1600::/56
		곡성군	2XXX:XXXX:F14:1700::/56
		구례군	2XXX:XXXX:F14:1800::/56
		고흥군	2XXX:XXXX:F14:1900::/56
		보성군	2XXX:XXXX:F14:2000::/56
		화순군	2XXX:XXXX:F14:2100::/56
		장흥군	2XXX:XXXX:F14:2200::/56
		강진군	2XXX:XXXX:F14:2300::/56
		해남군	2XXX:XXXX:F14:2400::/56
		영암군	2XXX:XXXX:F14:2500::/56
		무안군	2XXX:XXXX:F14:2600::/56
		함평군	2XXX:XXXX:F14:2700::/56
		영광군	2XXX:XXXX:F14:2800::/56
		장성군	2XXX:XXXX:F14:2900::/56
경상북도	2XXX:XXXX:F15::/48	완도군	2XXX:XXXX:F14:3000::/56
		진도군	2XXX:XXXX:F14:3100::/56
		신안군	2XXX:XXXX:F14:3200::/56
		경상북도 (내부 )	2XXX:XXXX:F15:1000::/56
		포항시	2XXX:XXXX:F15:1100::/56
		경주시	2XXX:XXXX:F15:1200::/56
		김천시	2XXX:XXXX:F15:1300::/56
		안동시	2XXX:XXXX:F15:1400::/56
		구미시	2XXX:XXXX:F15:1500::/56
		영주시	2XXX:XXXX:F15:1600::/56
		영천시	2XXX:XXXX:F15:1700::/56
		상주시	2XXX:XXXX:F15:1800::/56
		문경시	2XXX:XXXX:F15:1900::/56
		경산시	2XXX:XXXX:F15:2000::/56
		군위군	2XXX:XXXX:F15:2100::/56
		의성군	2XXX:XXXX:F15:2200::/56
		청송군	2XXX:XXXX:F15:2300::/56
		영양군	2XXX:XXXX:F15:2400::/56
		영덕군	2XXX:XXXX:F15:2500::/56
		청도군	2XXX:XXXX:F15:2600::/56
		고령군	2XXX:XXXX:F15:2700::/56
		성주군	2XXX:XXXX:F15:2800::/56
		칠곡군	2XXX:XXXX:F15:2900::/56
		예천군	2XXX:XXXX:F15:3000::/56
		봉화군	2XXX:XXXX:F15:3100::/56
		울진군	2XXX:XXXX:F15:3200::/56
		울릉군	2XXX:XXXX:F15:3300::/56

광역시도	프리픽스	시군구 구분	프리픽스
경상남도	2XXX:XXXX:F16::/48	경상남도 (내부 )	2XXX:XXXX:F16:1000::/56
		창원시	2XXX:XXXX:F16:1100::/56
		진주시	2XXX:XXXX:F16:1200::/56
		통영시	2XXX:XXXX:F16:1300::/56
		사천시	2XXX:XXXX:F16:1400::/56
		김해시	2XXX:XXXX:F16:1500::/56
		밀양시	2XXX:XXXX:F16:1600::/56
		거제시	2XXX:XXXX:F16:1700::/56
		양산시	2XXX:XXXX:F16:1800::/56
		의령군	2XXX:XXXX:F16:1900::/56
		함안군	2XXX:XXXX:F16:2000::/56
		창녕군	2XXX:XXXX:F16:2100::/56
		고성군	2XXX:XXXX:F16:2200::/56
		남해군	2XXX:XXXX:F16:2300::/56
		하동군	2XXX:XXXX:F16:2400::/56
		산청군	2XXX:XXXX:F16:2500::/56
		함양군	2XXX:XXXX:F16:2600::/56
		거창군	2XXX:XXXX:F16:2700::/56
		합천군	2XXX:XXXX:F16:2800::/56
제주특별자치도	2XXX:XXXX:F17::/48	제주특별자치도 (내부 )	2XXX:XXXX:F17:1000::/56
		제주시	2XXX:XXXX:F17:1100::/56
		서귀포시	2XXX:XXXX:F17:1200::/56

## □ 지방자치단체 (2/2)

<div> <div>2XXX:XXXX:X700:0000:0000:0000:0000:0000</div> <div>재난안전통신망 프리픽스: 36비트</div> </div>			
사용기관 구분			
번호 (8 bit)	용도	번호 (8 bit)	용도
00	N/A	14	전라남도
01	서울특별시	15	경상북도
02	부산광역시	16	경상남도
03	대구광역시	17	제주특별자치도
04	인천광역시	A1	경찰청
05	광주광역시	A2	소방청 , 시도 소방본부
06	대전광역시	A3	해양경찰청
07	울산광역시	A4	미할당
08	세종특별자치시	A5	국방부
09	경기도	A6	전기
10	강원도	A7	가스
11	충청북도	A8	의료
12	충청남도	A9	행정안전부 재난안전통신망
13	전라북도		

## [부록 K] 재난안전통신망 포털 서비스 이용


### K-1) 인터넷망에서 접속 시 신청서 작성

- 재난안전통신망 홈페이지에 접속하여 신청서 파일 다운로드
- 재난안전통신망 포털 접속 신청서 작성 후 서울운영센터 담당자 이메일(jeil2000@korea.kr)로 송부
  - 사용기관명, 담당자, 연락처, 이메일, 접속 PC MAC-Address 정보

사용기관명 (예시 )	담당자	연락처	이메일	PC MAC Address	비고
재난안전통신망 서울운영센터	제경일	010-0000-0000	jeil2000@korea.kr	8C-B0-AA-AA-AA-AA	
재난안전통신망 서울운영센터	이창호	010-0000-0001	yich828@korea.kr	18-67-AA-AA-AA-AA	

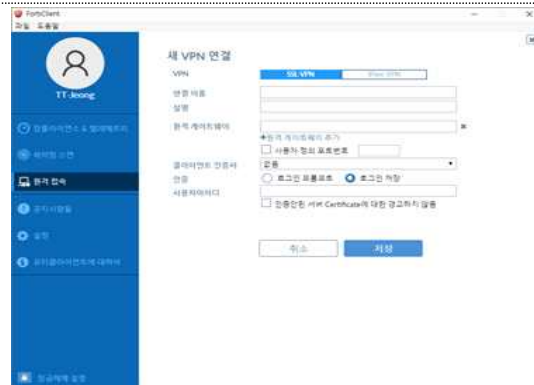
- 서울운영센터 담당자 회신 메일 송부
  - SSL VPN Gateway에 대한 IP Address 정보
  - 담당자별 SSL VPN 계정 및 비밀번호
  - 포털 시스템 외 어플리케이션 계정 및 비밀번호
- 인터넷으로 SSL VPN 접속 방법
  - SSL VPN Client 다운로드 경로
    - 32비트 OS : <https://drive.google.com/file/d/118cbTWJvBicPPLDHd1EPYBvxwGFOuu-M/view?usp=sharing>
    - 64비트 OS : <https://drive.google.com/file/d/1Qyo7cabYMC5PCG0XWISc68OACfWFNzxa/view?usp=sharing>
  - FortiClient 설치
    - "Yes, I Have read and accept the"를 체크하고 다음(Next) 버튼 클릭
    - "Secure Remote Access"를 체크하고 다음(Next) 버튼 클릭
    - "설치 폴더를 지정"하고 다음(Next) 버튼을 클릭하고 설치(Install) 버튼을 클릭하면 설치 진행이 완료됨

## ○ 인터넷으로 SSL VPN 접속 방법

- FortiClient 아이콘 실행 
- SSL VPN 설정

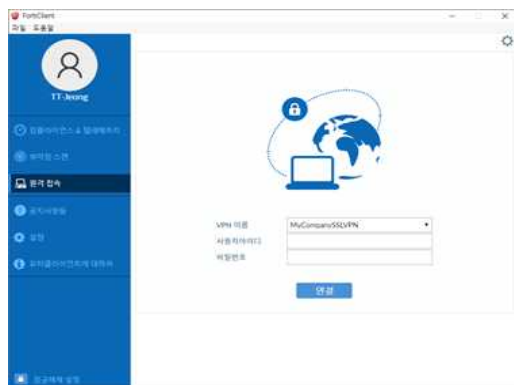


원격 접속 클릭하고 VPN 설정 선택



빨간색 체크 및 내용 기입한 후 저장 선택

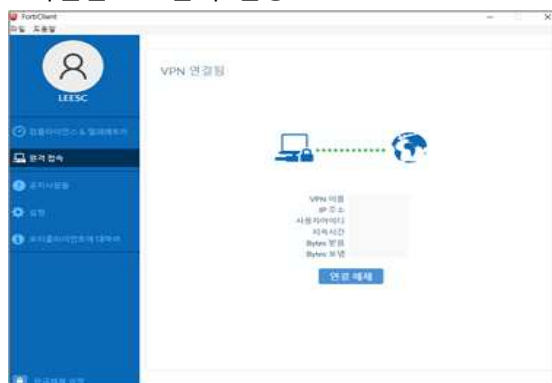
- 연결 이름 : 문자 발송
- 원격 게이트웨이 IP Address : 문자 발송
- 사용자 정의 포트번호 : 문자 발송
- 사용자 아이디 : 문자 발송



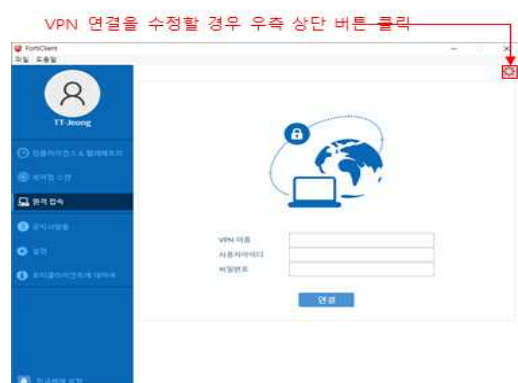
이전 Page 입력 및 클릭 완료 후 저장을 선택하면 위 화면이 나타남  
비밀번호 입력 완료 후 연결 클릭  
· 비밀번호 : 문자 발송



상태가 40%에서 멈출 경우 작업표시줄에 보면 보안 경고창이 생성되어 있음  
보안 연결을 진행하기 위해 "예"를 클릭



VPN 연결이 완료됨





## K-2) 국가정보통신망 업무망에서 접속 시 신청서 작성

- 재난안전통신망 홈페이지에 접속하여 신청서 파일 다운로드
- 재난안전통신망 포털 접속 신청서 작성 후 서울운영센터 담당자 이메일(jeil2000@korea.kr)로 송부
  - 사용기관명, 담당자, 연락처, 이메일, 접속 PC MAC-Address 정보

사용기관명 (예시 )	담당자	연락처	이메일	PC MAC Address	비고
재난안전통신망 서울운영센터	제경일	010-0000-0000	jeil2000@korea.kr	8C-B0-AA-AA-AA-AA	
재난안전통신망 서울운영센터	이창호	010-0000-0001	yich828@korea.kr	18-67-AA-AA-AA-AA	

- 서울운영센터 담당자 회신 메일 송부
  - 재난안전통신망 망연계 정책 적용 완료
  - 포털 시스템 외 어플리케이션 계정 및 비밀번호
  - 국가정보통신망상에 방화벽이 있을 경우 사용기관별로 방화벽 포트 허용 정책 적용

### □ 포털 및 연동 시스템 도메인 정보

시스템명	접속 URL	비고
서울운영센터 포털	https://portal-p.safenet.go.kr	
서울운영센터 SSO	https://sso.safenet.go.kr	
서울운영센터 ITSM	https://ism.safenet.go.kr	
서울운영센터 통계	https://stat.safenet.go.kr:28443	
서울운영센터 앱스토어	https://astore-p.safenet.go.kr:30443	
서울운영센터 IAM	https://iam.safenet.go.kr	
서울운영센터 LTAS	https://ltas-s.safenet.go.kr:8443	

- ※ 인터넷망에서 접속할 경우 DNS 서버 정보를 PC에 등록할 필요 없음
- ※ 국가정보통신망 업무에서 접속할 경우 국가정보통신망 DNS 서버를 사용함

**[부록 L] FirstNet의 응용서비스 목록****L-1) FirstNet API**

○ FirstNet에 등록된 API와 SDK 목록은 현재 [표 M-1]과 같다.<sup>34)</sup>

[표 M-1] FirstNet API/SDK 목록

(2021.11 기준)

번호	API 명칭	분류
1	ZSDK 단말기 고도 측정(안드로이드)	통신, IoT 인에블먼트, 분석, Z축 능력의 향상된 위치
2	API_NEON 위치정보 서비스	통신, IoT 인에블먼트, 분석, 지도/GIS, GPS 거부 개인 추적, 3D 실내 위치
3	ArcGIS Runtime SDK (안드로이드, iOS, 자바스크립트, .NET, Qt) (5종)	IoT 인에블먼트, 지도/GIS, 플랫폼, 분석, 위치 지능
4	AT&T IoT Data Plan	통신, IoT 인에블먼트
5	호 관리(Call Management)	통신, 접근과 인증, 음성통화
6	EPTT 연계 API	통신
7	EPTT 모바일 (웹 클라이언트) API	통신
8	EPTT 웹서비스 API	통신
9	FirstNet 앱 우선순위(App Priority)	통신, QoS
10	FirstNet PTT 웹 API (CAD 지령대, 지령대 및 녹음 애플리케이션에 FirstNet PTT를 통합시킬 수 있음)	FirstNet 전용, FirstNet 네트워크 API
11	모바일용 싱글 사인온(Single Sign-On - Mobile)	접속과 인증
12	단말기 최고순위 상향조정(First Priority Device Uplift)	통신
13	IOS ZSDK	통신, IoT 지원, 분석, Z축 기능을 통한 향상된 위치
14	유선전화 문자(Landline Texting)	통신
15	위치 서비스(Location Services)	지도/GIS, 위치 지능
16	멀티미디어 사건정보 획득(Multimedia Incident Retrieval)	통신, 미션크리티컬 및 논미션크리티컬 통신
17	브라우저용 싱글 사인온(Single Sign-On - Browser Apps)	접근과 인증
18	SMS (앱에서 SMS 발송)	통신
19	Sonim SPCC (소임 단말기용)	통신 플랫폼, 하드웨어 API
20	911로 문자(Text-to-911)	통신, 미션크리티컬 통신
21	TrafficLand API	IoT 인에블먼트, 지도/GIS, 분석, 위치 지능, 교통 정보, 도로 카메라, 동영상, 실시간 화상, Geo 위치
22	양방향 문자 플러스(Two-Way Text)	통신, 미션크리티컬 통신
23	양방향 문자(Two-Way Text Plus)	통신, 미션크리티컬 및 논미션크리티컬 통신

34) <https://developer.firstnet.com/firstnet/apis-sdks>

## L-2) FirstNet IoT

- FirstNet에 등록된 IoT 제품은 [표 M-2]<sup>35)</sup>와 같으며, 임베디드(Embedded) IoT 솔루션과 차량관리 솔루션 및 알람 솔루션이 있다.

[표 M-2] FirstNet IoT 제품 목록

(2021.11 기준)

번호	종류	제품명	기능
1	Embedded 솔루션	Axon Body 3	바티캠으로 무기가 사용될 때 실시간 경보를 발송하여 기관에서 대응. 한편, Axon Evidence (Evidence.com)로 오디오와 영상을 스트리밍할 수 있고, 관련자나 지령자가 실시간으로 영상을 당겨 봄
2		Allerio Mobile Hub	PS-LTE를 WiFi로 핫스팟을 제공하여 모바일 허브이며 연결된 장치에서 PS-LTE 데이터 서비스를 이용
3		ISC LTE Camera	PS-LTE망을 이용하는 비밀(코버트, covert) 형 카메라
4		Swymed elemedicine Backpack	카메라와 음향이 지원되는 백팩 형태의 원격 의료 솔루션으로 원격 데스크톱 제어가 가능. PS-LTE를 통하여 의사와 연결하여 환자에게 모바일 케어를 제공
5		Dejero Gateway	차량 또는 모바일 환경에서 음성, 비디오 및 데이터를 포함한 범용에플리케이션에 안정적인 연결을 제공하고 고정 위치에 무선 연결을 추가하는 장치
6		Digi-Talk+ 9751	건물내의 사용자와 미국 전역의 모바일 인력이 긴급상황에서 버튼 하나만 누르면 거의 실시간으로 연결되어 통신이 가능
7		Motorola APX NEXT™ All-Band P25 Smart Portable Radio	군용 표준에 맞게 설계되고 목적에 맞게 제작되어 VHF, UHF, 700/800MHz 대역은 물론 LTE, Wi-Fi, Bluetooth 및 NFC를 지원하는 미션크리티컬 P25 무전기
8		RATT Ihtch-Mount Teleopic Mast	특별 이벤트, 중대 사건, 모바일 비디오 감시, 수색 및 구조, 열화상을 위한 이동형 기지국
9		ThirdEye Gen Respond Eye MR X2 Glasses	증강 현실 원격 의료 솔루션으로 핸드프리 UI가 있는 웨어러블 장치로 머리동작, 오디오 및 행동을 제어
10	차량관리 솔루션	AT&T Fleet Management GO9 Telematic	사고 감지와 통보 기능을 갖는 차량 관리 솔루션
11		AT&T Fleet Complete Fleet Tracker 2	위치, 차량의 상태 및 운전 형태를 모니터링하여 현장 대원을 제어할 수 있게 하고 위기관리를 향상하는 솔루션
12		AT&T Fleet Complete AT1 Asset Tracker	FirstNet용 LTE-M으로 IP67 방수 및 방진이 되어 외부 온도 탐지, 점화 감지 및 외부전원감지를 지원
13	알림 솔루션	DMP Alarm Communicator	경보 신호의 중계 또는 재전송 없이 모든 DMP 모니터링 센터 수신기에 직접 보고하는 알람 장치
14		Kings III M90	Primary Path Cell/IP VoLTE 상용 긴급 전화 통신기로 VoLTE 기술로 엘리베이터 및 비상 전화용 휴대폰 음성 통신 솔루션은 최대 4개의 POTS 회선을 대체하며, 비상 상황 또는 엘리베이터 갇힘 중에 교환원이 승객과 양방향 음성 통신
15		StarLink Fire LTE	이중 경로 셀/IP LTE 상업용 화재 경보 커뮤니케이터로 FACP당 2개의 POTS 회선을 대체하며, 긴급 구조원에게 필요할 때 언제 어디서나 전용 및 지속적인 음성, 데이터 및 비디오에 우선적으로 액세스 지원

35) <https://www.firstnet.com/industry-solutions/iot.html>

### L-3) FirstNet 앱

○ FirstNet에서는 안드로이드 또는 iOS에서 지원되는 다양한 모바일 앱이 등재되어 있으며 현재 그 현황은 [표 M-3]과 같다.

[표 M-3] FirstNet 앱 목록 (2021.11 현재)

번호	앱 명칭	공급자	주요 기능	안드로이드	iOS
1	10-21 Police Phone	Callyo	무료 콜백을 위해 지역 전화번호를 통해 개인에게 장교 전화 통화 지원	L	-
2	10-21 Video	Callyo	피어 튜인 및 은폐 기능이 있는 스마트 폰을 통한 주문형 녹화 또는 라이브 스트리밍 비디오	L	L
3	AccessMyLAN	Asavie Technologies	네트워크 연결 및 장치 액세스를 관리하기 위해 주문형 액세스를 제공하는 FirstNet 독점 앱	C	C
4	ActiveAlert	Active911	자동 지도 경보 위치를 지원하며, 필수적인 상세 내역으로 통화로 빠르게 대응하게 해줌	L	L
5	Actual Live	Southern Stars Network	장소, 이벤트 및 공공장소를 위한 위험 인텔리전스 및 동적 커뮤니케이션	L	L
6	ArcAngel	Patrocinium Systems	비상시 모든 앱 사용자 및 응답자에 대한 위치 기반 통신 및 시각화	L	L
7	ArcGIS Explorer	Esri	마크업과 측정 도구를 포함하는 검색 가능 지도	L	L
8	AskRail	American Railroads	철도 사고 발생시 첫 번째 대응자를 위한 위험 물질 안전 도구	L	-
9	AT&T Business Messenger	AT&T	빠르고 안전한 양방향 그룹 및 개별 통신 가능	C	C
10	AT&T Enhanced Push-to-Talk	AT&T	PTT 음성 통신, 메시징, 위치 및 LMR과의 상호 운용성 제공	C	C
11	AT&T WFM Shield	AT&T	Workforce Manager Shield는 기본 및 확장 기본 엔터티를 위한 종단 간 데이터 수집 플랫폼입니다	C	C
12	Automatic Injury Detection	DataSoft	응답자 착용 센서 패널이 뚫린 경우 자동 경고 및 보고	L	L
13	BeamFirst	BeamLive Inc.	클라우드 기반 솔루션으로 문자, 오디오/비디오, 1초 미만의 GPS 연결, 공유, 프로파일링, GPS 위치기록되는 IoT 콘텐츠 및 미디어를 포함한 통신기능 제공	L	-

## 재난안전통신망 장비 · 서비스 도입 · 개발 가이드

번호	앱 명칭	공급자	주요 기능	안드로이드	iOS
14	Better app	The Better App Company	더 나은 삶과 수면을 위해 필요한 정보를 제공하는 정신 건강 앱	L	-
15	Better Stop Suicide	The Better App Company	편안한 숙면을 통한 자살 방지 앱	L	-
16	Bridge4PS	NP Strategies	메시징, 그림, 영상 및 파일 공유 솔루션으로 재난안전기관 이용자들 간의 협력 플랫폼	L	L
17	Buidling Safe	Building Safe	비상 위기 시에 건물 내 인원들과 재난 담당자들에게 비상 상황을 통보	L	L
18	CampusGuard911	Guard911, LLC	대학 교직원들을 위한 패닉 버튼 앱으로써, 교내에서 총기 사건 시에 선생이나 교직원이 CampusGuard 패닉 버튼을 눌러 즉각적으로 911에 전화를 걸고, 동시에 가까이 있는 모든 연방, 주 및 지방 경찰의 스마트폰에 경보가 발송됨	L	L
19	Cordico	Cordico INC	스트레스를 많이 받는 직업군(법집행관, 소방관, 파견원, 교도관 등)의 비밀이 보장되는 사전 예방적 건강 지원 앱	L	-
20	Corrate	Corrata Ltd.	이동 기지국 솔루션	L	L
21	CrisisGo	CrisisGo, Inc.	비상 상황에 대비하고 대응하기 위한 디지털 안전 및 위기 대응 플랫폼	L	L
22	Defender Body Worn	Defender LLC	향상된 공간 인지력을 위해 지리정보가 있는 비디오를 스트리밍하는 웨어러블 카메라 앱	L	-
23	DragonForce 3.5	Drakontas, LLC	공유 그룹, 매핑, 미디어, 화이트 보드 및 보안 메시지를 갖춘 중요한 협업 도구	L	-
24	DragonForce 3.6	Drakontas, LLC	공유 그룹, 매핑, 미디어, 화이트 보드 및 보안 메시지를 갖춘 중요한 협업 도구 최신버전	-	L
25	e-Bridge	GD	응급 및 의료진 간의 실시간 원격 진료, 프로토콜 워크 플로우, 정보 및 멀티미디어 공유	L	L
26	eAUXFOG	DHS - CISA	DHS '보조 커뮤니케이션 현장 운영 가이드'에 대한 오프라인 액세스, 모바일 버전	L	L
27	EMOS1	Nikatec	개인적 관리(직원, 업체, 자원봉사자, 고객, 스폰서..), 자격, 통신, 장비 추적 등 행사의 조직적인 사항을 다루는 종합 시스템	L	L
28	EMResource	Juvaré	자원 가용성 및 사고에 실시간으로 액세스	L	L
29	EMTrack	Juvaré	사건이나 사건에서 환자, 사람, 애완동물 및 인구를 수집하고 추적	L	-
30	EnforceNet	DigitalBlue Software	화재, EMS 및 법 집행을 위해 설계된 Blue Force 앱	L	L
31	eNIFOG	DHS - CISA	비상통신 계획과 재난대응에 사용될 단말기들을 책임지는 무선기술자를 위한 기술 참고로서 NIFOG 정보를 쉽게 접근할 수 있게 함	L	L
32	ERinfoPRO	ERinfo Inc.	의사소통이 불가능한 피해자의 얼굴 인식을 통해 신원, 긴급연락처 등 확인이 가능한 앱	C	-

## 재난안전통신망 장비 · 서비스 도입 · 개발 가이드

번호	앱 명칭	공급자	주요 기능	안드로이드	iOS
33	ESChat (Push-to-Talk)	ESChat	PTT 음성, 텍스트, 이미지 및 실시간 위치 공유 기능이 있는 셀룰러 앱을 통한 푸시 투 토크	C	C
34	Esper Device Management	Esper.io, Inc.	새로운 앱 버전을 쉽게 테스트하고 배포할 수 있는 오픈 소스 SDK로 구성된 Android 앱 및 기기 관리 플랫폼	L	-
35	EVERYWHERE App	EVERYWHERE Communications, Inc.	현장 근무자를 위한 앱	L	L
36	FirstNet Assist	AT&T	50마일의 상호 지원 사건을 볼 수 있는 FirstNet 앱, 지원 요청 / 승인 및 모바일 액세스 지원	C	C
37	FirstNet Cybersecurity Aware	AT&T	FirstNet 사이버 보안 인식 및 초동 조치자에 대한 교육	C	C
38	FirstNet Messaging	AT&T	일대일 채팅, 그룹 채팅을 할 수 있으며 동료에게 메시지를 브로드캐스팅 가능한 모바일 메시징 도구	C	C
39	FirstNet Push-to-Talk	AT&T Services, Inc.	FirstNet Push-to-Talk	C	-
40	FirstNet Single Sign-on	AT&T	FirstNet SSO 가능 앱 및 시스템에 단일 서명 액세스를 제공하는 앱	C	C
41	FleetComplete	Fleet Complete, Inc.	차량 정보 및 현장 실시간 GPS 추적 및 관리가 가능한 앱	C	C
42	FLORIAN	3AM Innovations Inc.	최초 대응자를 위한 현장 상황 추적 솔루션	L	-
43	GammaPix Pro Command Center	Image Insight Inc.	스마트 폰 카메라로 이온화 방사선을 자동 감지	L	-
44	GammaPix Training Simulator	Image Insight Inc.	GammaPix Command Center 앱과 함께 사용하여 실시간 가상 트레이닝 연습을 구성 및 실행	L	-
45	Geoteamz City	Zco Corporation	Automate and connect every department in your city	-	L
46	GovSecure	EchoPTT Inc.	인증된 암호화 표준으로 뒷받침되는 정부를 위한 안전한 음성 및 메시징 앱	-	L
47	Groupdolists	Centrallo Corporation	대응 팀을 즉시 동원하고 실시간 중앙 집중식 조정을 위한 대응 계획을 활성화	L	L
48	Guard911	Guard911, LLC	교내에서 총기 사건 시에 Guard911 패닉 버튼을 눌러 911에 즉각적으로 전화를 걸고, 동시에 가까이 있는 모든 연방, 주 및 지방 경찰의 스마트폰에 경보가 발송됨	L	L
49	HAAS Alert	HAAS, Inc.	인근 운전자에게 실시간 비상 차량 / 기기 안전 경보	-	L
50	Hazmat Radar	Zco Corporation	코로나바이러스 감염 장소 근처에 있으면 경고음을 알리는 앱	-	L
51	Hero911	Guard911, LLC	교내에서 총기 사건 시에 발송되는 경보 앱이며, 연방, 주 및 지방 경찰 담당자들로 이용이 제한됨	L	L

## 재난안전통신망 장비 · 서비스 도입 · 개발 가이드

번호	앱 명칭	공급자	주요 기능	안드로이드	iOS
52	Hiplink Mobile	Hiplink Mobile	중요한 텍스트 및 알림을 위한 안전한 통신; 최초 대응자를 위한 현장 도구	C	C
53	IBM MaaS360	IBM	원격장치관리를 위한 모바일 데이터 관리 솔루션	L	L
54	ImageWare Authenticator	ImageWare Systems, Inc	액세스 보안의 추가 계층으로 클라우드 기반 생체 인증을 MFA에 제공하는 확장성이 뛰어난 인증자	L	-
55	Intelligent Hub	VMWare	모바일 장치(이전의 Airwatch Agent)에서 빠른 사용자 온 보딩 및 정책 시행 지원	L	L
56	JPS VIA	JPS Interoperability Solutions, Inc.	연동 게이트웨이를 갖는 JPS VIA PTT 솔루션	C	C
57	Kansas eFOG	DHS - CISA	캔자스 주 필드 운영 가이드에 대한 오프라인 액세스, 모바일 버전	L	L
58	Lighthouse Health & Wellness	Lighthouse Health & Wellness PBC	최초 대응자, 공공 안전 기관 및 지원하는 사람들에게 기존 건강 및 웰빙 프로그램에 대한 익명 액세스를 제공하고, 최신 교육 건강 및 웰빙 정보 및 도구 라이브러리를 제공	L	L
59	Lookout for Work	Lookout Inc.	맬웨어 방지, 백업 및 원격 관리 기능을 갖춘 사용하기 쉬운 엔터프라이즈 모바일 보안 솔루션	L	L
60	LR Responder	AGIS, Inc.	모든 스마트폰, 태블릿 및 PC 사용자 사이에 실시간 상황 인식을 제공하는 저대역 위성 통신 네트워크의 지역 및 참가자의 위치를 표시	-	L
61	MissionKeeper Mobile	KSI Data Sciences	낮은 레이턴스를 갖는 스트리밍의 동영상과 검침을 제공	-	L
62	Mobile@Work	MobileIron	회사 네트워크에 보안으로 접속하여 이메일이나 다른 업무 자원에 접근할 수 있게 함	L	-
63	MobileIron Go	MobileIron	회사 네트워크에 보안으로 접속하여 이메일이나 다른 업무 자원에 접근할 수 있게 함	L	L
64	MobileIron Mobile@Work Client	MobileIron	단말기를 사용기관의 네트워크에 연결하게 해줌	-	L
65	MPTS	Nikatec Ilc	EMOS1의 의료 환자 추적 데이터에 접근할 수 있는 클라이언트 앱	L	L
66	Mutualink Edge	Mutualink	최초 응답자 그룹 통신을 위한 실시간 라디오, 비디오 및 텍스트 상호 운용성	L	L
67	Mutualink Edge @Team	Mutualink	완전한 기능을 갖춘 PTTtoC : 최초 응답자 통신을 위한 실시간 라디오, 비디오 및 텍스트 상호 운용성	L	L
68	NetMotion Mobility	NetMotion	최적화, WAN 가속화 및 적응형 정책 제어를 위한 지능형 VPN	L	L
69	OnGuard Lone Worker/ OnGuard	Sens-Net Canada Ltd.	종합적인 고독 작업자 안전, 모니터링 및 통신 서비스	L	L

## 재난안전통신망 장비 · 서비스 도입 · 개발 가이드

번호	앱 명칭	공급자	주요 기능	안드로이드	iOS
70	Orion Push to Talk	Orion Labs, Inc.	Onyx PTT 웨어러블을 통한 확장 지원을 통한 푸시 투 토크	-	C
71	PocketCop	Caliber Public Safety	공공안전의 상황 인식과 전체 이동성을 위하여 미션크리티컬 데이터를 제공하는 모바일 앱	-	C
72	Private Safety Network	Mooseworks Software, LLC	실시간 정보를 송수신하고 긴급 상황, 테러리스트 또는 안전 이벤트 발생 시 대량 알람을 배포할 수 있는 종합 통신 시스템	L	L
73	PTS Dialer	GDIT	전화통화를 걸 수 있게 도와주는 다이얼러 모바일 앱	L	-
74	Pulsara	CommuniCare Technology, Inc.	오디오, 비디오, 메시징 및 이미지로 환자 관련 통신	L	L
75	PulsePoint AED	PulsePoint Foundation	커뮤니티에서 공용 AED 레지스트리를 구축하는 데 도움이 되는 도구	L	C
76	PulsePoint Respond	PulsePoint Foundation	심폐 소생술 교육을 받은 시민 / 공무원 전문가에게 심장 응급 상황을 알리는 디스패치 인터페이스	L	C
77	QS Team Responder	QuantaSTAT Inc.	응급 의료 대응자가 분류 시간을 단축하고 환자를 추적하며 실시간으로 관련 상황 정보에 액세스	-	L
78	QuantaSTAT for Teams	QuantaSTAT	팀원들이 자신들의 증상을 집에서 쉽게 자체 보고하고 공유되는 앱	-	L
79	Radio-IP Armade Mobile VPN	Radio IP Software	공공 안전 표준을 사용하여 이동성이 높은 인력을 위한 통신 보안	L	-
80	Radio-IP Armade VPN	Radio IP Software	공공 안전 표준을 사용하여 이동성이 높은 인력을 위한 통신 보안	-	L
81	RapidDeploy Nimbus	RapidDeploy, Inc	Nimbus CAD 플랫폼에서 실시간으로 상황을 받을 수 있게 해주는 모바일 앱	L	L
82	Rave Guardian	Rave Mobile Safety	비상 시에 소속 기관과 신속하고 주도적으로 통신할 수 있게 하며, 기관별로 구성함	L	L
83	Rave Panic Button	Rave Mobile Safety	버튼을 눌러 911 비상 통화를 걸러 줌	L	L
84	ResponderRel8	TchTnk, LLC dba iRel8	동료와 통화를 가능하게 해줌	L	L
85	Response for FirstNet	Intrepid Networks	팀과 사용자 그룹이 조정, 협업 및 의사 소통을 할 수 있는 FirstNet 독점 앱	C	C
86	RumbleUp	RumbleUp	비상 상황에서 양방향 문자입력을 지원함	-	L
87	SAFEBUS by Predictable Ryde	Predictable Ride Inc.	학교 버스, 탑승자 및 차량조사를 지원하는 버스 운전자 앱	L	-
88	SafetyDrone	Drone Analytics	UAV 운영 및 규정 준수를 추적하기 위한 전용 앱으로 공공 안전을 제공	L	L



## 재난안전통신망 장비 · 서비스 도입 · 개발 가이드

번호	앱 명칭	공급자	주요 기능	안드로이드	iOS
89	SchoolGuard	Guard911, LLC	K-12(초·중·고) 학교 교직원들을 위한 모바일 패닉 앱이며, 교내에서 총기 사건이 발생했을 때, 교사나 교직원이 SchoolGuard 패닉 버튼을 눌러 즉각적으로 911 에 전화를 걸고, 동시에 가까이 있는 모든 연방, 주 및 지역 경찰 대원의 스마트폰으로 경보가 발송됨	L	L
90	Sectra Mobile VPN	Sectra Communications	경찰관과 응급 구조대원에게 스마트폰이나 태블릿 컴퓨터에서 공공 안전 기록 확인을 위한 안전하고 중단 없는 무선 액세스를 제공	-	L
91	SES Remote Access Control	Security Enhancement	현장 기술자들이 원격 SES 보안 사이트에 접근할 수 있게 하며, 업무상 매우 중요한 자산들을 보호함	L	L
92	ShieldForce	Tyler Technologies	경찰의 안전을 지원하는 앱	-	L
93	Sonim Scan	Sonim Technologies	Sonim XP8 장치를 바코드 스캐너로 전환	C	-
94	Sonim SOS	Sonim Technologies	Sonim XP5s 또는 XP8 물리적 알람 키로 알람을 발생시키면 911 또는 비상연락처 전화걸기 및 카메라에서 자동으로 사진 보내기 등이 가능한 앱	C	-
95	Tactical Performance	O2X Human Performance	식단 추천, 맞춤형 운동 프로그램 및 목표 중심의 정신 성과 계획을 통해 매일 건강한 선택을 하도록 권장하고, 운동 및 건강한 요리법 등 제공	-	L
96	Tango Tango	Tango Tango, Inc.	모바일 PTT 및 무선 통합 : 상호 운용 가능한 통신, 전체 범위 및 교차 채널 가시성	C	C
97	TASSTA T.Flex	TASSTA	3GPP EPS(Evolved Packet System) 서비스를 기반으로 미션 크리티컬 시나리오에 적합한 향상된 PTT 서비스를 지원	C	-
98	TBL Universal Reporting	TBL Systems, Inc.	TBL Systems의 모바일 보고와 지령 시스템	-	L
99	TeamConnect PTT	TeamConnect, LLC	셀룰러 모바일 인력 관리 솔루션을 통한 혁신적인 PTT	L	-
100	TULU PRO	Qnexis, Inc.	비상 통신 관리자로 하여금 비상 경보를 신속하고 용이하게 발령하고 이용자들의 위치를 파악하고 통신하게 해줌	L	L
101	TX eFOG	DHS - CISA	Texas 현장 운영 가이드 문서에 오프라인으로 접속할 수 있게 해주는 모바일 앱	L	L
102	USPDhub	LogicTree IT Solutions	대행사 알림, 게시판, 캘린더 등을 위한 모바일 커뮤니케이션 허브	L	-
103	VALOR Officer Safety	Institute for Intergovernmental Research	다양한 교육 자료를 통해 이동중인 경찰관이 정신적, 육체적으로 임무에 대비할 수 있도록 도와주는 앱	L	L
104	Visual 911+	Southwest Synergistic	GPS 위치 및 경고 상태를 정의된 사용자 / 그룹과 공유하는 기능, 시각적 신호 포함	L	L
105	Visual Labs for FirstNet	Visual Labs Inc.	바디캠, 디지털 카메라 및 오디오 레코더, 라이브 스트리밍 및 위치 분석	C	-

## 재난안전통신망 장비 · 서비스 도입 · 개발 가이드

번호	앱 명칭	공급자	주요 기능	안드로이드	iOS
106	Vitals First Responder	Vitals™ Aware Services	경찰과 초동 대응자가 취약한 개인을 식별하고 효과적으로 참여하도록 지원	L	L
107	VizSafe	VizSafe, Inc.	사건보고, 커뮤니케이션 및 라이브 캠을 갖춘 실시간 상황 인식 플랫폼.	L	L
108	Voyager Query	Salient CRGT	승인된 법집행 공무원에게 CJIS 및 NCIC와 같은 주, 지방 및 연방 데이터베이스에 대한 액세스 권한을 제공	L	L
109	Voyager SAFE	Salient CRGT	학생과 교사가 비상 상황을 이유와 설명 및 위치정보를 추가하여 담당직원에게 개인적으로 알릴 수 있는 앱	L	L
110	WAVE Push-to-Talk	Motorola Solutions Inc.	3GPP MCPTT(Mission Critical Push-To-Talk) 표준을 기반으로 모든 네트워크/장치에서 빠르고 안전하며 안정적인 광대역 PTT 통신을 제공	L	L
111	what3words Lite	what3words ltd	전 세계의 모든 위치를 10ft x 10ft 정사각형에 고유한 주소를 부여하여 위치를 제공하는 앱	L	L
112	WorkerSafety Pro?Safety Alerts	Tidyware, LLC	위험한 일을 하는 작업자(고소작업, 위험한 환경, 혼자 작업 등)를 보호하기 위한 앱	L	L
113	WV eFOG	DHS - CISA	West Virginia 주 운영 가이드에 대한 오프라인 액세스, 모바일 버전	L	L
114	ZIMPERIUM Mobile	Zimperium	이용자, 장치 및 기관을 위협으로부터 방어하는 보안 솔루션	L	L

L: 등록 (Listed), C: 인증 (Certified)

96

88