主題

재난대비 비상통신 사례 분석

한국전자통신연구원 김 성 연, 남 기 동, 전 덕 중

차 례

Ⅰ. 서론
Ⅱ. 미국의 국가안전보장 및 비상대비(NS/EP) 프로그램 정책
Ⅲ. 재난대비 비상통신 기술 표준화 프로그램
Ⅳ. 시사점 및 맺음말

요약

재해나 재난 발생 시 재난 대비 비상통신시스템의 미비로 인하여 인명이나 재산상의 피해를 늘리기도 하고, 재난 복구에 차질을 빚게 하기도 한다. 따라서 각 국에서는 재난 대비 비상통신시스템을 정부 주도로 정비하여 재난 발생 시 신속한 통신시스템 운용으로 피해를 줄이고자 노력하고 있다. 그리고 표준화 단체를 중심으로 비상통신시스템에 대한 표준을 개발하고 있다. 본 고에서는 외국의 비상대비 통신 프로그램에 대하여 미국의 사례를 중심으로 알아보고, 표준화 기구의 기술개발 동향을 살펴보고 시사점을 도출하고자 한다.

Ⅰ. 서 론

세계 각국은 네트워크기반의 정보사회로의 급속한 발전에 따라 통신 인프라스트럭처가 가지는 국가적 중요성을 인식하고 이를 국가가 관리하여야 할 중요 기반시설로 지정하여, 효율적이고 안정적인 운영을 위한 다각적인 노력을 기울이고 있다. 태풍이나 지진, 홍수, 호우, 해일, 폭풍, 화산폭발과 같은 자연재해, 오클라호마 시 청사 폭발, 2002년 9월 11일 뉴욕 무역센터 테러와 같은 테러 공격, 인간의 실수에 기인하여 발생하는 재난 등 다양한 형태의 재난이 발생하고 있다. 또한 통신 분야에서도 자연재해나 재난에 의한 서비스 장애, 사이버 공간에서의 공격 및 테러, 전화국이나 지중관로의 화재, 도로, 수도, 전기 등 기반시설 공사 중의 통신 케이블 절단 등 각종 통신 재난이 발생하고 있다. 이러한 통신재난은 경우에 따라서는 국가의 안전에 지대한 영향을 미치는 경우도 종종 발생한다. 특히 통신기술의 발달 및 통신서비스 이용의 활성화는 통신 기반구조 인 네트워크의 상황에 따라 그 피해의 심각성이나 파급을 미치는 영향 정도가 달라지고 있

다고 하여도 과언이 아니다.

특히 정보사회로의 성숙도가 높은 국가일수록 재난이나 비상사태에 대비하는 사회적 체계나 시스템 구축에 많은 노력을 기울이고 있다는 사실에 주목할 필요가 있으며, 그 중에서 통신이 차지하는 비중도 점차 확대되고 있음을 주지할 필요가 있다. 방재나 비상대비 통신시스템은 안정적인 서비스 공급을 전제로 하는 공공재적 성격이 강한 서비스라는 특성과 시장 자율기능에만 의존할 수 없다는 특성으로 인하여 각국은 자국의 안전보장과 국민의 재산과 인명 보호를 위하여 다양한 형태의 비상통신 시스템을 운용하고 있다. 미국의 경우 국가안전 및 비상대비(NS/EP: National Security /Emergency Preparedness) 프로그램은 역사적 이벤트나 사건이 발생할 때 마다 즉각적인 대응을 하면서 발전해왔기 때문에 매우 복잡하고 다양하게 전개되고 있다. 또한 무선기술을 이용한 공공안전무선네트워크 시스템은 연방정부 및 각 주, 지자체가 보유한 무선서비스의 상호운용성을 확보하기 위하여 지속적으로 발전되고 있다.

호주의 경우 비상사태 발생 시 PSTN을 이용한 비상접속번호로 000을 가지고 있으며, 각 주별로 GRN (Government Radio Network)[1]을 구축하여 대응하고 있다. 캐나다의 경우 Industry Canada에서 MSAT 비상통신네트워크를 운영하고 있으며, 비상방송, 통신설비 재고 확보, IP기반의 PAD (Priority Access for Dialing), 이동우선접속서비스(CPAS: Cellular Priority Access Service), 복구 우선순위 설정 등을 통하여 대비하고 있다. 그리고 UN에서는 WGET (Working Group on Emergency Telecommunications)를 운영하고 있다.

1) 비상서비스 용으로 450-470MHz을 이용하고 있으며, 2003부터 420-430MHz대역이 비상 무선데이타 통신용으로 할당되었음

우리 나라의 경우 '자연재해대책법', '재난관리법' 및 '전기통신기본법'에서 재해 혹은 재난과 같은 비상사태 발생 시에 대비한 통신 계획을 수립하도록 정하고는 있으나, 아직 본격적인 의미에서 국가안전 및 재난대비 통신 시스템에 대하여 총체적이고 실행 가능한 시스템이 갖추어져 있는 상태라고 보기는 어렵다. 따라서 본 고에서는 미국의 국가안전 및 비상대비프로그램과 PSWN, 그리고 표준화 기구들의 비상통신 표준화 동향을 살펴보고 향후 비상통신의 발전을 위한 시사점을 얻고자 한다.

Ⅱ. 미국의 국가안전보장 및 비상대비 (NS/EP) 프로그램 정책

미국의 국가안전보장 및 비상대비 통신 시스템은 1961년 쿠바 미사일 위기 시부터 시작한다. 당시 미국, 소련, NATO 및 기타 외국 원수들간의 통신상의 장애가 발생 하여 위기를 보다 복잡한 국면으로 접어들게 한 문제가 발생하였다. 케네디 대통령은 쿠바사태 이후 국가안전보장통신망에 대한 조사를 명령하였고, '국가안전보장회의' (NSC: National Security Council)는 범 부처적인 검토위원회를 구성하여 통신망 운용 방안 및 관련기구의 기능조정을 검토하였다. 위원회는 국가위기 시 대통령, 국방성, 외교 및 정보활동을 원활하게 수행하기 위해서는 단일의 통합된 통신 시스템이 필요하다고 권고하였다. 케네디대통령은 위원회의 권고에 따라 국가 재난 시에도 정부 고유 기능을 원활하게 수행하고, 이를 효율적으로 지원할 수 있는 통신 시스템을 구축할 것을 명령[1]하였고 이에 의하여 재난 및 비상대비 통신 전담기구로서 '국가통신시스템' (NCS: National Communications System)을 설립하였다.

또한. 미국 정부는1979년 이래 '국가 안전보장 전기통신 정책' (National Security Telecommunications Policy)을 제정하여 국가 안전보장을 위한 통신설비 이용에 관한 기본방향을 설정하는 등 국가 안전보장과 관련된 통신 정책 입안을 추진하고 있다.[2] 이에 따라 국가안전보장 및 비상대비 통신 프로그램의 정책수립과 관련된 주요 이슈에 대하여 대통령과 국가통신시스템에 자문을 수행하기 위하여 대통령자문위원회로서 '국가안전보장통신자문위원회' (NSTAC: National Security Telecommunications Advisory Committee)가 1982년 9월에 행정명령(Executive Order) 12382 [3]에 의해 설립되었다.

클린턴 행정부에 들어와서는 국가 주요 기반시설을 지정하여 특별한 보호를 하여야 할 필요성을 인지하고 1996년 7월 행정명령 13010 [4]에 의하여 대통령 직속의 위원회인 '국가 주요기반시설 보호에 관한 자문위원회' (PCCIP : President's Commission on Critical Infrastructure Protection)를 설립하였다. 국가주요핵심기반시설은 국방이나 경제 안전에 지대한 영향을 미칠 수 있는 시설이나 시스템으로서, 행정명령 13010에 의하여 지정된 국가주요 기반시설은 통신망, 전력시스템, 가스 및 오일, 은행 및 금융, 운송체계, 수자원 공급, 정부서비스와 긴급비상서비스가 이 범주에 포함되었다[2] . 1997년 10월 PCCIP는 미국의 기반시설을 보호하기 위하여 전 국가적인 노력이 필요함을 역설하였다. 그로부터 7개월 후 1998년 5월 22일 클린턴 당시 대통령은 Presidential Decision Directive 63[6]을 발표하여 국가 주요 기반시설 보호를 위한 정책 기반 및 구체적인 조직을 확립하였다. PDD-63에서는 '국가주요핵심기반시설보증위원회' (Critical Infrastructure Assurance Council)과 '국가주요기반시설보호센터' (NIPC: National Infrastructure Protection Center)의 역할과 기능을 정립하였다.

그리고 1999년 7월 14일 행정명령 13130[7] 및 PDD-63에 의하여 기반시설에 대한 전문지식을 보유한 민간, 주정부 및 지자체에서 추천되는 30인 이내의 대통령 지명직 위원으로 구성되는 NIAC (National Infrastructure Assurance Council)[3] 를 설립하였다.

또한 '국가핵심기반시설보증국' (CIAO: Critical Infrastructure Assurance Office)은 2000년 1월에는 '정보시스템 보호에 관한 국가계획'(National Plan for Information System Protection)을 PDD-63의 실행 전략 프로그램의 일환으로 제시하였다. 그리고 2001년 9월 11일 뉴욕 세계무역센터에 가해진 테러 직후 부시대통령은 행정명령13231 '정보사회에서의 주요 기반시설 보호'[8]에 의하여 '국가 핵심 기반시설 보호를 위한 대통령 자문위원회' (CIPB: President's Critical Infrastructure Protection Board)를 2001년 10월에 설치하였다. 또한 뉴욕 테러의 여파로 2001년 10월 8일 행정명령 13228[9]에 의하여 '본토안전보장국' (Office of Homeland Security)을 설치하고, **Homeland Security Presidential Directive-1[10]**에 의해 '본토안전보장위원회' (Homeland Security Council)을 설치하였으며, **"Homeland Security Act of 2002"[11]**에 의거 '본토안전보장성' (Department of Homeland Security)이 설치되었다. 그리고 2002년에는 행정명령 **13260[12]**에 의해 '본토안전보장자문위원회' **(Homeland Security Advisory Council)**이 설립되었다.

2002년에 발표된 본토안전을 위한 국가전략 (National Strategy for Homeland Security)에 의

2) 2002년 발표된National Strategy for Homeland Security [5]에 정의된 핵심기반시설분야는 농업, 식료품, 수자원, 공중보건, 긴급비상서비스, 정부부문, 국방산업, 정보통신, 에너지, 수송, 금융, 화학산업, 우정분야로 정의되어 있음.

3) NIAC는 행정명령13231에 의거 2003년 10월까지 운영 예정임

하면 비상대비 및 대응(Emergency Preparedness and Response) 분야의 전략 중의 하나로 비상사태 발생 시 초기 대응을 위한 1단계 대응 책임자들간의 단절 없는 통신을 확보하는 것의 중요성을 인식하여, 그 들간의 통신을 위한 장비 및 기술, 절차, 프로세스 등을 정립하기 위한 '국가비상통신계획'(National Emergency Communications Plan)을 수립하며, 또한 관련 장비를 2003년부터 본토안전성에서 우선적으로 확보하는 것을 목표로 계획을 수립하고 있다.

1. 주요 국가안전보장 및 비상대비 서비스

국가통신조정센터에서는 고도지능망서비스, 비상조정네트워크서비스, 정부비상통신서비스, 통신자원공유프로그램, 우선순위통신서비스, 우선접속서비스 등을 제공하고 있다. 본 절에서는 국가통신조정센터에서 제공하고 있는 주요 서비스를 중심으로 설명한다.

1) ACN (Alerting and Coordination Network)

ACN은 국가안전보장 및 비상대비 서비스를 지원하기 위하여 서비스 제공 사업자의 비상운용센터 (EOC: Emergency Operations Center)와 네트워크운용센터(NOC: Network Operations Center) 간의 안정적인 비상 음성 서비스 제공과 통신망의 복구를 위한 기관간 업무 조정, 통신요구사항 및 우선순위의 전송을 목적으로 구성한 비상용 네트워크 이다. 공중망이 혼잡 상태이거나, 네트워크 성능이 현저히 저하되는 상황 발생 시, 혹은 공중망이 운용불능 상태 등일 때 사고보고를 위한 용도로 활용되는 등 평상시 또는 비상시 국가통신조정센터를 지원하기 위하여 24시간 상시 운용되고 있다.

2) 정부 비상 통신 서비스 (GETS: Government Emergency Telecommunications Service)

정부비상통신서비스는 국가 안전과 긴급 상황 발생 시 국가안전보장 및 비상대비 관계자들이 보다 원활하게 주어진 사명을 달성할 수 있도록 지원하기 위한 목적으로 개발된 통신서비스로서, 국가통신시스템 사무국에서 관장하고 미국전역에 걸쳐 서비스가 제공되고 있는 특수 . 서비스이다.[13] 정부비상통신서비스는 대통령 지도통신, 비상시 정부운용의 지속성 확보, 외교 및 국방목적의 국제전화, 특수기관의 필수적인 비상사태 수행 기능, 비상시 방송시스템과의 연동, 각 주의 비상운용센터 지원기능, 재해에의 신속한 대응 기능들이 제공되고 있다.

정부비상통신서비스는 긴급 상황, 재해, 혹은 전쟁 상황 하에서도 가용한 통신자원을 최대한 활용하여 국가, 공공기관, 국방 등에서 그 기능을 유지하기 위하여 필요로 하는 일정한 수준을 상시 제공할 수 있도록 하기 위하여 설계되었다. 정부비상통신서비스 이용자는 국가통신시스템 회원기관들을 대상으로 제공되며, 연방기관, 각 주, 지방행정기관 등에서의 근무자가 이용자가 될 수 있다. 일반적으로 정부비상통신서비스 이용자는 다음과 같은 네 가지의 범주로 구분하고 있다.

- 제1범주: National Security Leadership

위기 상황에서 정부 및 국가 통치의 지속성 확보를 위한 대통령지도통신 및 외교적 협상 관계자

- 제2범주: National Security Posture and U.S. Population Warning

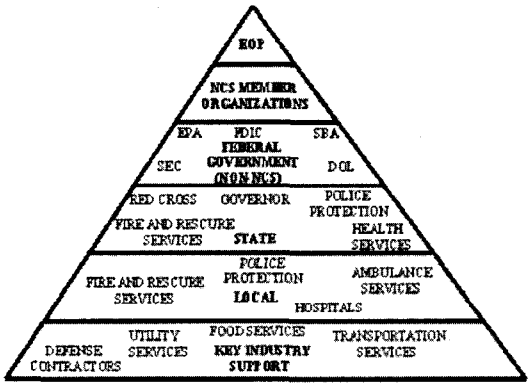
국가 비상사태 전, 중, 후의 연방업무의 지속적 수행과 이를 지원하기 위한 주, 지방행정기관 필수 요원

- 제3범주: Public Health, Safety, and Maintenance of Law and Order

전국 혹은 지역, 지방의 비상사태 발생 시 법을 수호하고 국민을 보호하기 위하여 필요한 국가안전보장 및 비상대비 기능 수행에 필요한 인력으로서 보건, 수송, 통신, 전력 등 기간 필수 서비스 제공 관련자를 포함

• 제4범주: Public Welfare and Maintenance of Economic Posture

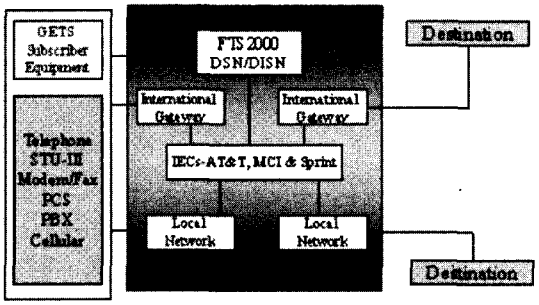
재해 발생 시 식료품 및 생활필수품 조달, 금융시스템의 유지, 전략 물자 및 에너지의 생산 및 유통 통제, 재해의 방지 및 통제 등을 행하는 인력



(그림 1) 정부비상통신서비스 이용자 그룹

정부비상통신서비스에서는 주요 장거리 사업자 네트워크, 유무선 지역 전화 사업자 네트워크, FTS[4], 국방정보네트워크 (DISN: Defense Information System Network) 등을 포함하는 정부 보유 자가망 등을 이용하여 서비스 하고 있다.

정부비상통신서비스는 정부비상통신서비스 고유 접속번호와 개인식별번호 (PIN: Personal Identification Number)를 통해 정부비상통신서비스 긴급 액세스, 시내.외 및 국제 전화 네트워크에서의 국가안전 및 비상대비를 위한 특정 프로세스 제공이 주요 내용이다. 정부비상통신서비스에의 접속은 일반 음성용 전화서비스 접속 도구(표준 데스크 세트, STU-III, 팩스, 모뎀, 셀룰러)를 사용하여 정부비상통신서비스 접속번호인 '1-710-NCS-GETS'를 통해 액세스하면 된다. 이를 위하여 국가통신시스템 사무국에서는 각 기관의 구내교환시설에 710을 식별할 수 있도록 조치하고 있으며 지역 서비스 사업자들에게도 정부비상통신서비스 이용자들이 보다 쉽게 정부비상통신서비스 서비스를 이용할 수 있도록ELS (Essential Line Service), DTP (Dial Tone Priority)와 같은 서비스를 제공토록 하고 있다. 접속 후 개인 개인식별번호와 전화번호를 등록하여 적법한 이용자인 여부를 확인하고, 일단 이용이 승인된 후에는 국가안전보장 및 비상대비 통신 이용자로 분류되어 라우팅과 우선순위에서 특별 취급을 받게 된다.



(그림 2) 정부비상통신서비스 구조

정부비상통신서비스에서는 네트워크의 각종 장애에 대처하기 위하여 다음과 같은 기능들을 보유하고 있다.

1) 비상통신 전용 다이얼링 계획
   • 710
   • 장거리사업자별 비상통신전용 접속 번호[5]
2) 개인식별번호를 통한 액세스 제어

4) FTS(Federal Telecommunications Service)의 자세한 내용에 대하여는 김성연 외, 미국의 연방통신서비스 동향, 주간기술동향 98-42[14] 참조,

5) AT&T에는 1010288, MCI에는 1010222, Sprint에는 1010333이 배당되어 있다.

3) 강화된 라우팅(Enhanced Routing)
4) 트래픽 제어에 의한 우선순위 처리
5) 개인식별번호에 의한 국제 호 접속 서비스
6) FTS, DISN 등 타 네트워크와의 상호운용성 제고
7) 위기발생 시에도 향상된 연결성 제공 서비스
   • CPS(Cellular Priority Service):
   • 우선순위통신서비스(Telecommunications Service Priority)
8) 번호전환을 통한 액세스
9) 통화 기록 보호 및 접근 제한

3) 통신자원 공유 (SHARES: SHAred RESources) 프로그램

통신시스템이 파괴되었거나, 통신망을 이용하여 국가안전보장 및 비상대비 관련 정보를 전송할 수 없을 경우 HF(High Frequency) 무선 자원을 이용하여 기관간 비상 메시지를 처리하는 것을 목적으로 개발되었다. SHARES 네트워크는 현재 1073개의 HF 무선국으로 구성되어 있으며, 85개 연방기관, 주정부, 민간기업이 참가하고 있다. 무선국들은 각 주와 16개 해외지점에 배치되어 있다.

SHARES 프로그램은 국가통신조정센터가 운용 및 관리를 책임지고 있으며, 프로그램의 원활한 운영을 위하여 SHARES HF 상호운용성 워킹 그룹을 상설위원회로 운영하고 있으며, 94개 기관에서 143명이 회원으로 참가하고 있다.

10개 주파수를 이용하여 운용하며, 그 중 2개의 주파수는 음성용으로, 6개의 주파수는 디지털 전송용으로, 2개의 주파수는 SHARES BBS용으로 할당된다. 운용 수준은 3개 수준으로 정의되어 있으며, 수준 3은 평시상태, 수준 2는 잠재적 비상사태, 수준 1은 비상사태로 정의한다.

4) 우선순위 통신 서비스(TSP: Telecommunications Service Priority) 시스템

우선순위통신서비스는 비상사태 혹은 위기상황 발생 시 다른 어떠한 서비스보다도 국가중요통신 서비스의 우선순위를 보장하여줌으로써, 국가안전보장 및 비상대비 이용자들에게 서비스 안정적 이용을 보장하여 주며, 또한 서비스 제공사업자에게는 우선순위통신서비스 대상 서비스를 우선 복구함에 따른 법적, 제도적 보호를 하기 위해 개발된 서비스이다. 즉 우선순위통신서비스 프로그램은 검증된 국가안전보장 및 비상대비 통신 서비스의 우선순위 설정에 따른 제도적, 행정적, 운용적 측면에서의 서비스 운용체계라고 할 수 있다. [15]

우선순위통신서비스 대상 서비스는 기간통신사업자가 제공하는 주간(interstate) 및 주내(intrastate)통신서비스, 외국에서 제공하고 있는 통신서비스, 정부기관 보유 자가 통신망이나 비기간통신사업자 네트워크로서 기간통신사업자 네트워크에 접속되어 있는 서비스로서 우선순위통신서비스의 우선순위가 할당되어 있는 서비스를 대상으로 한다. 또한 국가안전보장 및 비상대비 이용자가 요구하는 특별한 경우에는 정부기관 자가망이나 비기간통신사업자 네트워크로서 기간통신사업자 네트워크에 접속되지 않은 서비스 중 우선순위통신서비스의 우선순위 특약이 되어 있는 서비스, 외국 기관이나 공관에 제공되고 있는 국제 서비스의 일부도 대상 서비스가 될 수 있다.

우선순위통신서비스 프로그램은 서비스 복구(restoration) 및 서비스 제공(provisioning)이라는 두 가지 요소로 구성된다. 복구 우선순위는 사고나 장애발생 이전에 복구에 관하여 우선순위를 요청한 경우에 한하여 적용된다. 사업자들은 서비스 장애 발생 시 다른 어떤 서비스들보다도 먼저 우선순위통신서비스의 적용대상 서비스 복구에 우선순위를 두어 복구하여야 한다.

그리고 서비스 제공 측면에서는 비상(emergency)

서비스와 필수(essential) 서비스로 구분되어 제공된다. 비상서비스는 우선순위통신서비스 범주 중 비상으로 분류된 서비스 기능을 제공하는 것으로 이 서비스는 제공 비용에 관계없이 무엇보다도 우선적으로 제공되어야 하는 서비스이다. 반면 필수 서비스는 사업자의 정상적인 프로세스에도 불구하고 지정된 일자까지 반드시 제공되어야 하는 서비스이다.

우선순위통신서비스 프로그램은 다음 <표 2>와 같은 5개의 서비스 범주가 있다. 서비스 범주 중 A, B, C, D는 필수서비스로 구분된다. 그리고 서비스 프로파일별 요소는 이용자 단말 및 구내망 배선 상태에 따라 다음과 같은 여섯 개의 요소그룹으로 구분된다.

- 요소그룹 A: 단말 (CPE)
- 요소그룹 B: 구내 배선(CPW)
- 요소그룹 C: 운용
- 요소그룹 D: 기술적 통제 설비/장애검색/분리
- 요소그룹 E: 서비스 테스팅
- 요소그룹 F: 초기 서비스 및 루트 다양성
- 요소그룹 G: 설비 및 사이트 접속성

서비스 프로파일 요소 정보는 복구 서비스와 제공서비스에 따라 다음과 <표 1>와 같이 구분된다.

<표 1> 프로파일 요소 정보 일람

서비스복구	A1	• 서비스제공자의 복구대응기간 내 CPE에 대한 현장 복구 서비스
	A2	• 백업용 여유 단말이 가용 한 상태
	B1	• 서비스제공자의 복 대응기간 내 CPW에 대한 현장 복구 서비스
	C1	• 이용자 설비의 24시간/일 운용 또는 hot-standby 상태 유지
	D1	• 문제를 격리하거나 서비스 테스트를 하는데 24시간/일 가용
	D2	• 자동 서비스 손실 경고 표시 및 담당자에게 경고 발송 얼람 기능
	E1	• 품질이나 신뢰성 테스트를 주기적으로 실시
	F1	• 서비스 포인트간의 중요 서비스
	F2	• 다른 우선순위통신서비스 복구를 위한 루트 다원화 기능 제공
	G1	• 이용자가 24시간/일 사이트에 접속 가능
	G2	• 이용자가 사전에 지정된 시간에 사이트에 접속 가능
	G3	• 이용자가 익일 접속 가능
서비스제공	A3	• 서비스 요구일자까지 단말 가용
	B2	• 서비스 요구일자까지 구내배선 가능
	C1	• 이용자 설비의 24시간/일 운용 또는 hot-standby 상태 유지
	D1	• 문제를 격리하거나 서비스 테스트를 하는데 24시간/일 가용
	D2	• 자동 서비스 손실 경고 표시 및 담당자에게 경고 발송 얼람 기능
	F1	• 서비스 포인트간의 중요 서비스제공에 필요한 경로 존재
	F2	• 다른 우선순위통신서비스 제공을 위한 루트 다원화 기능 제공
	G1	• 이용자가 24시간/일 사이트에 접속 가능
	G2	• 이용자가 사전에 지정된 시간에 사이트에 접속 가능
	G3	• 이용자가 익일 접속 가능

<표 2> 서비스복구 우선순위 수준 표

서비스범주		서비스 프로파일 요소				
A	국가안보	A1/A2 B1	A1/A2 B1	A1/A2 B1	A1/A2 B1	A1/A2 B1
B	국가안보 사태 및 공습경보	A1/A2 B1	A1/A2 B1 C1 G1,G2 or G3	A1/A2 B1 C1 D1/D2 E1 G1 or G2	A1/A2 B1 C1 D1/D2 E1 F1 or F2 G1 or G2	

C	공중보건, 안전 및 법질서 유지	A1/A2 B1	A1/A2 B1 C1 G1,G2 or G3	A1/A2 B1 C1 D1/D2 E1 G1 or G2		
D	공공 후생 및 국가경제 유지	A1/A2 B1	A1/A2 B1 C1 G1,G2 or G3			
우선순위 수준		5	4	3	2	1

<표 3> 서비스제공 우선순위 수준표

서비스 범주	서비스 프로파일 요소						
A	국가안보	A3 B2	A3 B2	A3 B2	A3 B2	A3 B2	
B	국가안보 사태 및 공습경보	A3 B2 G1 or G2	A3 B2 C1 G1 or G2	A3 B2 C1 D1/D2 G1 or G2	A3 B2 C1 D1/D2 F1 or F2 G1 or G2		
C	공중보건, 안전 및 법질서 유지	A3 B2 G1 or G2	A3 B2 C1 G1 or G2	A3 B2 C1 D1/D2 G1 or G2			
D	공공 후생 및 국가경제 유지	A3 B2 G1 or G2	A3 B2 C1 G1 or G2				
E	비상사태						
우선순위 수준	5	4	3	2	1	E	

국가안전보장 및 비상대비 관련 업무를 수행하는 기관은 국가통신시스템의 우선통신 사무국(OPT: Office of Priority Telecommunications)으로부터 우선순위통신서비스 사용자 지정을 받아야만 한다 OPT는 이용자에게 각 서비스별로 2년간 유효한 우선순위통신서비스 권한 코드(TSP authorization code) 를 부여하고, 이용자는 우선순위통신서비스 권한코드를 가지고 서비스 제공업자에게 서비스 신청을 함으로써 서비스가 개시된다.

우선순위통신서비스의 우선순위 배정은 다음 <표 4>와 같은 비율로 배정하여 동일 우선순위에 많은 기관이 집중되는 현상을 피하고 있다.

<표 4> 우선순위통신서비스 운선순위 배정 표

서비스 범주	우선순위				
	5	4	3	2	1
A	N/A	N/A	N/A	N/A	100%
B	35%	30%	20%	15%	
C	50%	30%	20%		
D	70%	30%			

FCC의 우선순위통신서비스 시스템 룰에 의해, 서비스 제공사업자는 국가안전보장 및 비상대비 통신 서비스를 기타 서비스보다 먼저 제공해야 한다. 기존 우선순위통신서비스를 복구하는 것이 새로운 우선순위통신서비스를 제공하는 것보다 앞서며 다음과 같은 우선순위에 의하여 진행하여야 한다.

- 복구 우선순위 1인 서비스의 복구
- 비상(Emergency) 우선순위통신서비스의 제공 (제공 우선순위 'E')
- 복구 우선순위 2,3,4,5에 의한 서비스 복구
- 서비스 제공 우선순위 1,2,3,4,5에 의한 우선 순위통신서비스의 제공

우선순위통신서비스 시스템에서 발생하는 여러 가지 문제를 식별하고, 검토하고, 해결방안 등을 제시하기 위하여 1990년 7월 우선순위통신서비스 감독 위원회(Oversight Committee)를 설립

하였다. 위원들은 19인[6] 으로 구성되어 있으며 연 2회 회의를 개최한다.

5) 우선 접속 서비스(PAS: Priority Access Service)

자연 재해 발생 시 셀룰러 이동전화가 긴급 통신 상황에서 유용함이 여러 차례 입증되었다. 재난이나 비상사태가 발생하면 일시적으로 셀룰러 이동통신 트래픽이 급증하는 문제가 발생하고, 이로 인하여 긴급구조 요원들이 통신을 하기가 무척 어려워지며, 또한 긴급 상황에서 재난구호 사무국으로 호가 몰리는 상황이 발생할 가능성이 크다. 이미 언급한 바와 같이 국가안전보장 및 비상대비 통신 서비스는 상시 사용 가능한 상태로의 유지가 이루어져 있음으로써 발생 사건이나 혹은 위험에 대하여 즉각적인 대응과 관리를 할 필요가 있다. 따라서 비상사태 상황에서 국가안전보장 및 비상대비 관련 긴급비상통신을 해야 할 경우 우선적으로 공중무선망에 접속할 수 있도록 할 필요가 있다.

우선접속서비스 이용 대상자는 국가안전 및 비상사태 대응과 관련한 업무 수행자 모두가 이용할 수 있는 서비스는 아니고, 국방성, FEMA, 소방본부의 긴급의료서비스(Emergency Medical Service) 등 주요 기관의 핵심 인사만이 이 서비스를 이용할 수 있다. 서비스 신청은 연방기관의 이용자는 기관을 통하여 신청하면 되나, 주정부나 지방정부의 이용자는 관련 연방기관을 통하여 신청할 수 있다. 그리고 이용 시에는 반드시 상용무선네트워크에 혼잡이 발생하여 접속이 불가능하거나 어려운 상태이며, 긴급사태 관련 업무 수행 중이어야 한다.

서비스 제공 사업자는 별도로 지정하지 않으며, 이동전화 허가를 보유한 사업자는 원하는 경우 서비스를 제공할 수 있으며, 이 경우 FCC가 지정한 프로토콜을 이용하여야 한다.

서비스 제공 우선순위는 정부비상통신서비스 국가안전보장 및 비상대비 판단기준에서 제시한 바와 유사하게 다섯 가지 범주로 나누어 지정된다.

(1) 국가 안전에서의 리더쉽
(2) 재난 대응 및 군의 지휘 및 통제
(3) 공중보건, 안전 및 법질서의 유지
(4) 공공 서비스, 국가기간서비스 및 공중 후생
(5) 재난 복구

2. 공공 안전 무선 네트워크 서비스

미국 연방 정부는 공공의 안전을 효율적으로 유지하기 위한 통신 수단을 확보하고, 지자체, 주정부, 연방 정부 들 간의 상호운용성을 확보하기 위하여 다양한 무선통신서비스를 이용하고 있다. 연방재난관리청(Federal Emergency Management Agency)에서는 MERS (Mobile Emergency Response Support)를 운용하고 있으며, 법무성은 JWN (Justice Wireless Network), 연방통신위원회 (FCC: Federal Communications Commission)에서는 공공 안전 무선 네트워크(PSWN: Public Safety Wireless Network) 프로그램을 1996년부터 운용하여 오고 있다.

PSWN 프로그램은 법무성(Department of Justice)과 재무성(Department of Treasury)이 공동으로 후원하고 있으며, 공공의 안전과 관련된 지자체, 주정부, 연방정부 기관들간의 통신상의 상호운용성 증진을 위한 이슈들을 주로 다루고 있다.

즉 향상된 상호운용성을 바탕으로 국민의 생명과 재산을 안전하고, 효과적이고, 효율적으로 보호할 수 있는 단절없고(seamless), 조정(coordinated) 및 통합이 이루어진 공중 안전 통신망을 구축하는 것을 비전으로 설정하고 있다.

6) 연방기구 소속 7명, 기업체 소속 7명, 주정부 소속 2명, OPC대표, FCC대표, 그리고 연방정부관리 1명으로 구성

PSWN 프로그램의 현재 비전은 공공 안전 관련 기관들이 지금까지 사용하여 오고 있던 서로 통신이 불가능한 고립된 연통형(stovepipe) 통신 시스템을 극복하여 모든 시스템들을 통합하여 네트워크를 형성하는 것이다.

모든 정부기관은 보다 나은 서비스를 위해 더욱 효과적이고, 효율적이며 비용 측면에서도 효과적인 통신을 하기를 원하고 있다. 부시 정부는 이 임무를 효과적으로 추진하기 위하여 국가적인 차원에서 공공안전의 요구사항을 충족시키는 무선 네트워크 간의 상호운용에 대한 조정과 계획을 수립하는 것을 본토 안전 전략의 중요한 우선사항으로 비준하였다.

미국의 공공 안전 무선 네트워크 프로그램과 관련된 구성요소는 다음과 같다.

- PSWN 이용자 그룹 (FLEWUG: Federal Law Enforcement Wireless User Group)
- PSWN 자문위원회 (PSWAC: Public Safety Wireless Advisory Committee)
- PSWN 프로그램

이용자 그룹은 1994년 공공의 안전 확보를 위한 통신과 관련된 주파수, 상호운용성, 그리고 관련 이슈들을 다룰 조직으로 FLEWUG를 출범되었다. 이용자 그룹은 연방 정부의 법 집행 및 공공 안전 유지 책임을 지닌 30개 기관의 무선관련 담당자들로 구성되어 있으며, 이용자 그룹의 주요 기능은 지상이동무선(LMR: land mobile radio)기술의 표준 개발, 연방정부 및 지자체, 주 등 서로 다른 공공안전무선시스템과의 상호운용성 확보, 경제성 분석 등의 기능을 수행한다.

1994년에 FCC와 NTIA는 2010년까지 지방, 주, 연방의 공공안전기관들이 요구하는 무선통신 요구기능을 파악하고, 이와 관련된 문제점 분석 및 가용한 솔루션 제안을 위하여 자문위원회를 구성하였다. 자문위원회에는 지방, 주, 연방의 공공안전 담당자, 공공서비스제공자, 장비공급업체, 상용서비스 제공자 등을 망라하여 구성하고 있다. 1996년에는 PSWAC 보고서를 통하여 공공안전을 위한 이슈들을 정리하여 발표하였다.

PSWN 프로그램은 각 정부기관이 보유하고, 운용 중인 무선 네트워크들 간의 상호 연동성에 문제가 되는 부분을 도출하고, 이의 해결을 위한 개발을 지원하는 것이 주요 임무 이다. PSWN 프로그램에서는 국가적인 구매, 구축, 관리 및 자금 지원에는 직접 관여하지 않고 있으며, PSWN과 관련된 장비들의 규격, 상호 연동 시 고려되어야 할 사항 및 성공 사례(Pilot Project)들을 공표 및 홍보함으로써 문제를 해결하려는 각 기관들이 참고할 수 있도록 하는데 주안점을 두고 있다.

PSWN에서 운용 중인 파이롯 프로젝트는 상호 운용성의 구현 및 지원을 위한 프로젝트로서, 현재 10개의 파이롯 솔루션을 제공하고 있다. 파이롯 프로젝트는 상호운용성 해결을 위해 도입된 기술 및 방법을 프로젝트화 하여, 상호운용성을 해결하려는 기관들이 참고할 수 있도록 하기 위한 것으로서, 일부는 아직도 수행 중에 있다. 이러한 파일롯 솔루션은 상호운용을 위한 주파수 자원, 시스템 비용, 기술 성능, 주요 기능, 조직 특성 등의 요소를 고려하여 제공되고 있다. [17]

1) Console-console patch Project

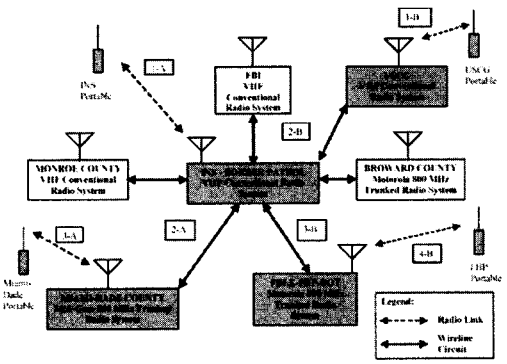
본 프로젝트의 목적은 대규모 난민 처리 시 발생하는 기관간 통신 상호운용성을 검증하기 위한 것이다.

이 프로젝트는 이동통신과 고정통신을 동시에 이용하는 것으로서, 고정통신은 LCIDC (Leased Circuit Interconnection of Dispatcher Console)을 이용하여 참여 기관의 dispatch console간을

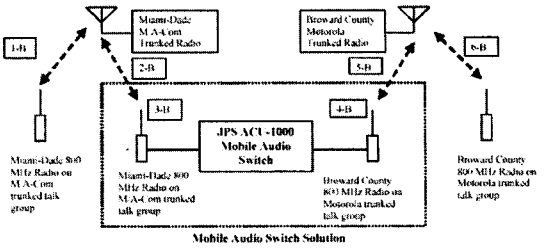
4개의 음성 circuit를 연결하여, 이종의 시스템을 이용하고 있는 각 기관 이용자들의 직접 연결을 가능하게 하는 것이다. 각 기관(7개 기관) [7]

들은 INS(Immigration and Naturalization Service's, 이민관리국) dispatch center에 연결되어 있으며, Border Patrol의 console electronic switch를 hub로 이용하여 상호 연결한다. 이동통신은 재난현장에서의 상호 연동을 위한 것으로서 3개의 county마다 하나씩 제공된 MASS(Mobile Audio Switching System)를 이용한다. MASS는 12개의 무선 인터페이스, 2개의 POTS를 제공하여 현장에서의 다양한 무선 환경의 게이트웨이 역할을 담당한다. LMR 시스템에 따라 subscriber unit을 MASS에 직접 연결, 또는 LMR 리피터와 연결하여 현장 요원들의 직접 통화를 가능하게 한다.

LCIDC 구성 및 MASS 구성은 다음과 같으며, 2001년 8월 상호운용성 시험을 완료하였다



(그림 3) LCIDC 구성도



(그림 4) MASS 구성도

2) Console-console Radio Frequency Link

원격에 있는 이종의 TRS간 상호운용성을 검증 하는 것을 목적으로, 이종의 TRS간 연동을 무선주파수링크를 이용하여 직접 연결하는 것이다.

각 지역의 TRS 유닛들은 지역trunked desktop radio에 연결 신청을 하고, 각 desktop radio는 remote control을 통해 CCRFL을 생성하고, Dispatch supervisor는 agency간 talk group을 연결시켜 직접 통화 가능하도록 한다 [8]. 이때 CCRFL은 Intercity VHF를 통해 연결 된다. 이 시험에서는 두 시스템은 액세스 프로토콜을 TDMA, FDMA로 달리 사용하였다.

3) Interstate Interoperability

이종의 LMR을 이용하는 기관들간의 상호운용성을 검증하기 위한 것이다. 대상은 Vermont주와 New Hampshire주로서 이들은 각각 UHF와 VHF 시스템을 자가망으로 운용하고 있다. Microwave system은 각 LMR 사이트를 연결하는 백본 역할을 담당한다.

이 경우 우선 가입자 장비를 dual mode로 교체(Vermont 기관원들의 단말을 VHF LMR에 연결 가능토록 함)하고, microwave baseband 시스템을

7) 대상 은 Florida주의Monroe County, Dade County, and Broward County 3군데이며, 7개 참여기관은 Florida Highway Patrol (FHP), Florida Department of Law Enforcement (FDLE), Broward County Sheriff's Office, Miami-Dade Police Department, Monroe County Sheriff's Office, U.S. Coast Guard (USCG), Federal Bureau of Investigation (FBI), Immigration and Naturalization Service (INS), and Border Patrol 임

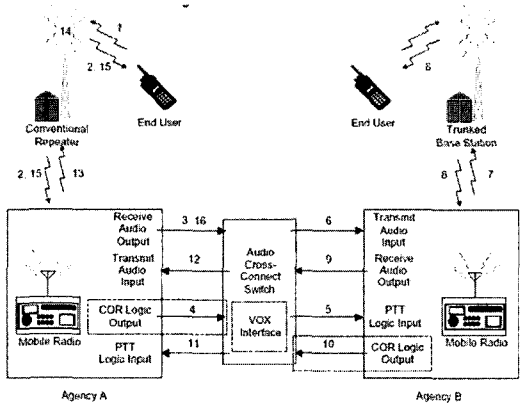
8) 대상 장비는 EDACS (Ericsson Enhanced Digital Access and Control System), trunked radio system (Las Cruces, New Mexico), Motorola SmartNet trunked radio system (El Paso, Texas)이 이용된다.

이용하여 두 주 사이의 연결을 구성하는 형태이다.

4) Transportable Communication System

TCS (Transportable Communication System) 시스템은 MCV (Mobile Command Vehicles)에 탑재하여, 비상 지역에서의 기관간 상호 연동을 담당한다. TCS는 ACU-1000 스위치와 무선 인터페이스 등으로 구성되어 있으며, 최대 24 무선 인터페이스 연결이 가능하고, 12개 주파수 대역을 지원한다.

운용은 Mobilemobile, MobilePSTN, 그룹통화, PSTN dialout from TCS 형태가 가능하다. San Diego 지역에서 운용 중인 TCS 구성도는 다음과 같다.



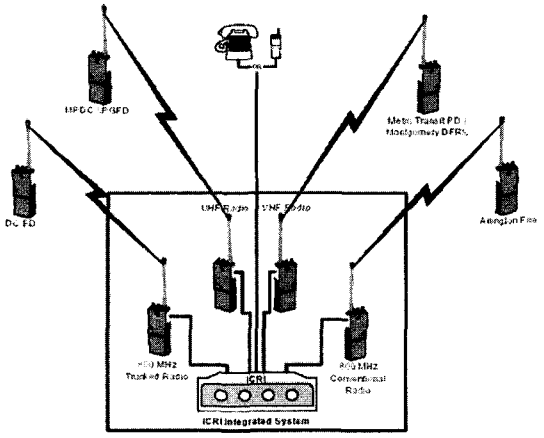
(그림 5) TCS 구조도

5) In-tunnel Interoperability

지하철과 같은 유효 주파수 확보가 어려운 지역에서, 이동형 장비를 통한 기관간 상호 무선 통신을 지원하기 위한 솔루션이다.

운용은ICRI(Incident Commanders Radio Interface) 유닛을 이용하고, 포터블 장비[9] 를 이용한다. 장비 구성 요소는 4개 표준 무선인터페이스, 하나의 remote 무선인터페이스, 하나의 전화 인터페이스 포트와 배터리 팩으로 구성되어 있다. 현장에 있는 팀과 터널 밖의 기관들과도 ICRI의 연결을 통해 통신이 가능하다.

이 솔루션을 활용하고 있는 지역은 District of Columbia Fire and Rescue Department (DCFD), Washington DC Metro railway 등에서 현재 8개 시스템을 운용하고 있다.



(그림 6) In-Tunnel 상호운용성 구조도

6) Cross-System Interconnect

2002년 Salt Lake 동계 올림픽 진행을 위한 기관간 상호 운용을 위한 솔루션으로 개발된 것으로서, JWN (Justice Wireless Network) [10], Integrated Treasury Network[11], USCS[12] (United State Customer Service), USSS[13] (United State Secret Service), Utah Communication Agency 시스템[14] , Salt Lake

9) Communications-Applied Technologies에서 개발

10) 디지털 무선시스템으로 연결 기관은 BOP, FBI, INS, DEA, USMS, OIG 등이다.

11) VHF 디지털 양방향 무선 시스템으로, 연결 기관은 USSS, USCS,IRS, BATF 임.

12) VHF 아날로그 무선 시스템으로서, 임무특정적 목표를 수행한다.

13) LMR(VHF 디지털 협대역 무선시스템으로, 17개의 encrypted 무선 채널 제공

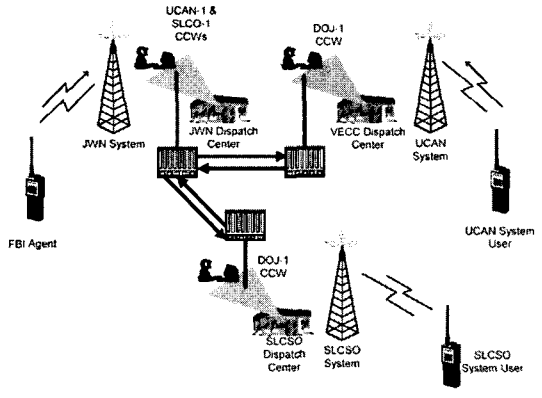
14) 800Mhz 디지털 협대역 TRS로서, 90개 정부기관 들이 연결되어 있음

카운티 통신시스템[15] 등이 참여하고 있다.

상호운용성 솔루션으로는 CSI (Cross-System Interconnect)를 활용한 3개 중요 시스템간 상호운용을 위한 solution (UCAN system, JWN system, SLCSO system), CEB (central electronics banks)내 BIM (base interface module)을 cross-connecting 하여 agency간 연결로를 확보하는 개념이다. 각 기관-대-기관 링크는 3개의 patch들로 구성 되어 있다.

현장에서의 무선 통신은 JPS ACP-1000을 이용한다. 다양한 무선 인터페이스를 가진 오디오 스위치를 활용하여 현장에서 소속이 다른 기관원들간의 통신을 가능하게 한다.

USSS에서 제공되는 유선라인은 4개의 데이터라인, 4-8개의 트렁크라인, 현장용 1라인으로 구성되어 있으며, 위성통신은 산림청에서 제공하는 26개의 GlobalStar 위성 전화를 활용하였다. 이동형 장비는 ACU-1000과 같은 이동형 장비는 고속 이동이 가능한 다목적 차량에 탑재하여 이용되었으며, 올림픽 기간 동안 정보 교환 및 백업 통신용으로 비화 양방향 페이저[16]가 활용되었다.



(그림 7) CSI 구조도

15) 800Mhz 디지털 협대역 TRS (Motororа SmartZone)로서, 안전 및 법 집행 지원이 목적

16) FBI, Treasury's WPO, UCAN, DPS, SLCSO, USSS, USCS, and Federal Law Enforcement Training Center 인력들이 사용

7) Consolidated Communication Site

각 기관들이 기관별 무선 통신을 위해 설치한 안테나 및 운용국을, 공동의 타워 및 운용국으로 전환하여 비용효율성을 높이고자 하는 프로젝트이다. 즉 하나의 타워에 각 기관들의 무선통신을 지원하기 위한 안테나들을 설치하고, 타워의 전원 및 통신 시설을 위한 운용국을 공동으로 구축, 활용하는 형태이다. Montana Public Safety Communications Association (PSCA)에서 구축된 사례이다.

8) 기타 사례

이 외의 사례로는 해변 주위에서 두 지역간 무선통신을 위한 상호운용성 사례 및 고밀도 지역에서의 무선통신에 대한 상호운용성 프로젝트가 진행 중에 있다. 특히 고밀도 지역에서의 상호운용성 확보 프로젝트는 주파수 자원의 한계로 인하여 계획을 재설정하고 있다. 또한 음성 위주의 무선통신에 대한 보완수단으로 비화 양방향 페이저 활용방안에 대한 프로젝트가 진행 중에 있다.

3. E-911서비스

911서비스는 미국 및 캐나다의 비상통신서비스로서, 긴급통화를 누르면 PSAP(Public Safety Answering Point)에 접속해 주는 서비스이다. 911서비스는 Wireless Communications and Public Safety Act of 1999 에서 정의된 것으로서 기존의 다양한 비상호출번호를 911로 통합하였다. 'Enhanced 911(E911)'이란 개정된 통신법 제 222조의 내용으로서 긴급구조의 경우 고객의 동의 없이도 위치정보를 활용할 수 있으며, 유선에서 긴급 비상통신(911)을 호출하는 경우 발신자의 위치 및 발신번호를 자동으로 PSAP에 알려주는 서비스를 말한다.

네트워크기술의 발전 및 GPS 등 위치확인기

술이 발전함에 따라 공공의 안녕과 국민의 생명 보호를 강화하기 위하여 FCC에서는 2000년부터 이동휴대전화에서의 위치확인서비스 도입을 적극 추진하여 왔다. 휴대폰에서 발신된 비상호출에 대하여 이동통신 업체들이 휴대폰 가입자의 위치를 확인하여 PSAP에 알려주면 이를 소방서, EMS(Emergency Medical Service) 등 긴급 구조기관에 연결시켜 주는 것을 의무화 하고자 하는 것이다. 최근 미국의회에서도 미국내 6개 이동통신업체들에게 위치정보서비스 공을 의무화하는 법안을 제정하기로 했다.

FCC Wireless 911 Requirements[18]에 의하면 제공하는 가입자 정보 및 위치정보에 대해서는 발신자 확인(911 호출자의 전화번호)과 911호출을 수신한 셀 사이트 또는 기지국 정보를 제공하는 1단계와 1단계를 포함하여 경위도 좌표에 의한 911호출자의 위치 정보를 제공하도록 하는 2단계로 구성되어 있으며, 현재 2단계 구현이 의무화 되고 있다.

요구되는 위치정보 정밀도는 단말기반 방식에서 호출의 67%에 대하여 50미터, 95%에 대해서 150 미터, 네트워크 기반 방식에서 호출의 67%에 대해 100 미터, 95%에 대해서 300 미터 정밀도를 제공하도록 규정하고 있다. 초기 법령의 발효 시에는 2001년을 목표로 하였으나, 무선 기술의 어려움과 통신사업자들의 비용부담 등 현실적인 문제로 인하여 최종 구현일자를 2005년으로 연기하였다.

- PSAP(Public Safety Answering Position)의 요구와 관계없이, 망사업자들은
- 2001.10. 1: ALI (Automatic Location Identification) 가능한 단말판매 및 서비스개시
- 2001. 12.31: 신규개통단말의 25% ALI가능
- 2002. 6. 30: 신규개통단말의 50% ALI 가능
- 2002. 12.31: 신규개통단말의 100% ALI 가능
- 2005.12.31: 모든 가입자의 95%에 ALI가능 단말보급
- PSAP(Public Safety Answering Position)의 요구가 있을 경우 6개월 이내 또는 2001.10. 1부터
- 2단계 E911 서비스 제공이 가능한 네트워크 업그레이드 완료
- 2단계 요구사항을 충족하는 E911 서비스를 PSAP에 제공

E-911 서비스는 최근 미국 이동통신 서비스업체들이 막대한 투자비용 등의 이유 때문에 보급에 차질을 빚었던 휴대폰 위치정보서비스 및 위치정보 측위 기술의 상용화를 앞당기며 GPS수신기를 장착한 휴대 단말의 보급을 촉진시키는 등 위치기반 관련 산업 활성화의 계기를 제공할 것으로 기대된다.

위치정보에 있어서 공익적 활용이라는 측면과 아울러 프라이버스 보호라는 측면에서 심각한 고려가 필요하다는 인식 하에 통신법 222조를 일부 수정하여 프라이버시 보호를 강화하고자 "Wireless Privacy Protection Act of 2003"이라는 법안이 발의되어 있는 상태이다.

Ⅲ. 재난대비 비상통신 기술 표준화 프로그램

재난 발생 시 통신 기술을 활용한 인명이나 재산상의 피해를 줄이기 위한 기술개발 노력은 ITU, TIA, ETSI 등 표준화 기구를 중심으로 연구되고 있다.

ITU에서는 TDR(Telecommunications for Disaster Relief) 프로그램이 진행되고 있다.[19] 비상사태 발생 시 통신네트워크에는 과부하가 일어나 효율적인 통신이 어렵게 된다. 긴급 구조 활동에서는 경찰, 소방대, 의료지원 요원 등 구조요원들 간의 통신이 필수적이다. 이러한 긴급통

신 지원을 위하여는 통신자원에 대한 접근성 및 사전에 준비된 가용성 정도에 따라 긴급구조 활동의 효율성이 결정된다는 인식 하에 비상통신서비스의 표준화 필요성이 제기되어 TDR이 결성되었다. 이러한 TDR 활동은 과거에는 PSTN 등 회선기반의 서비스가 주를 이루고 있었으나, 최근에는 IP기반, 멀티미디어 서비스를 중심으로 공중망과 사설망과의 완전한 상호운용성 확보를 목표를 국제 표준화 하는 방향으로 발전하고 있다. SG2에서는 운용측면에서의 이슈를 주로 다루고 있으며, E.106 및 E.TDR이 검토되고 있다. SG3에서는 법,제도적인 측면에서의 이슈들을 다루고 있으며, SG4에서는 TMN을 포함한 망관리 관련 이슈들을 다루고 있다. SG9에서는 J.et에서 CATV 망을 이용한 비상통신을 다루고 있으며, SG16에서는 F.706에서 E.106을 멀티미디어 서비스로 발전시키는 표준을 준비하고 있다.

ETSI에서는 EMTEL (Emergency Telecommunications) 프로그램을 중심으로, TIPHON, E112, SPAN, SES, MESA, TETRA(TErrestrial Trunked Radio), 3GPP 등이 연구되고 있다.[20]

TIPHON 프로젝트에서는 IP기반 네트워크를 이용한 비상통신 서비스 제공 기술 및 방식에 관한 표준화가 진행 중이며, SPAN에서는 국제 비상통신 체계 및 ELP(Emergency Location Protocol) 기반의 멀티미디어 비상통신 서비스에 대한 표준을 개발하고 있다. E112에서는 모든 통신사업자들이 112호에 대한 위치 정보를 제공할 수 있는 기술적 가능성 및 표준을 개발하고 있다. TETRA에서는 공공 안전 응용서비스를 위한 광대역 디지털 TRS 통신서비스에 대한 표준을 개발하고 있으며, 현재 기존 대비 10배 이상의 데이터 처리가 가능하고, 기존 무선통신망과의 연동이 가능한 구조를 목표로 하는 릴리즈2가 개발중이다. 3GPP에서는 GSM방식이나 W-CDMA에서의 호 우선처리 기능 및 위치 서비스를 위한 표준을 개발하고 있다.

TIA와 ETSI 간에는 MESA[17] 라는 공동연구 프로젝트가 2001년부터 추진 중 이다. MESA 프로젝트에서는 공공보호 및 구호를 위한 원격환자 모니터링, 무선로보틱스, 광대역위성접속 등 2Mbps 이상의 광대역 디지털 무선 응용 서비스 개발과 이와 관련된 기술표준을 개발하고 있다.

표준화 활동과는 별개로 미국 정부에서는 PSWN을 보다 발전시키기 위하여 전자정부 프로젝트[18] 추진의 일환으로 FEMA를 중심으로 SAFECOM (wireless public SAFEty interoperable COMmunications) 프로젝트 [19]를 추진하고 있다[21]. SAFECOM에서는 비상사태 발생 시 공공의 안전을 위하여 종사하는 있는 요원들이 다른 지자체, 주, 연방정부의 요원들과 통신을 할 수 있도록 하는 것이다. 앞서 설명한 PSWN이 연방정부기관과 주의 기관들간의 상호운용성을 보장하기 위한 노력이라면, SAFECOM은 연방정부기관들간의 상호운용성을 확보하기 위한 노력이다. 그리고 SAFECOM은 광대역 무선 전송기술을 활용하는 방안으로 더욱 발전시킬 계획이다.

Ⅳ. 시사점 및 맺음말

자연재해, 인위적인 실수 혹은 고의에 의한 재난이거나 비상사태 발생 시 국민의 생명과 재산을 보호하기 위한 구호활동의 효율성을 높일 필요성은 오랜 기간 제기되어 왔다. 본 고에서는

17) http://www.projectmesa.org/home.htm 참조

18) 현재 24개의 전자정부 응용 프로젝트가 추진 중임.

19) 2002.5.31.부터 FEMA가 SAFECOM 프로젝트를 관장하고 있으며, SAFECOM에는 Strategic Planning, Program Management, First Responder Interoperability, Federal Interoperability, Enterprise Architecture, Industry Liaison 등 6개의 워킹그룹이 있다.
PSWN Program Up date, Summer 2002

정보통신기술 및 네트워크기술의 발전을 활용하여 구호활동의 효율성 및 재난 발생 시 피해 규모를 줄이기 위한 여러 가지 노력들이 있음을 미국의 사례와 비상통신 관련 기술 표준 개발 동향을 중심으로 살펴보았다. 선진 각 국에서는 국가 안전 및 비상 대비 통신 체계를 국가 주도로 우선적으로 확보하여, 운용하고 있다. 이는 911 사태 등 재난 대처 사례에서 구호 요원들 간의 현장통신과 지휘통신의 중요성이 부각되었으며, 또한 이러한 재난대비 통신 시스템은 민간의 자율에 의존할 수 없는 공공재적 성격이 강하기 때문이다.

앞서 살펴본 사례에서 조직측면, 서비스측면, 기술개발측면으로 나누어 시사점을 살펴보면 다음과 같다.

우선 미국의 사례에서 알 수 있는 바와 같이 재난대비 비상통신은 정부주도로 이루어진다는 것이다. 이러한 통신 시스템은 수익성을 위주로 하는 민간 부문이 운용하기 어렵다는 서비스 특성, 서비스 이용자들이 공공부문에 있다는 점, 사태 발생이 비주기적이며 수시로 발생한다는 특성, 서비스의 안정적 공급이 중요하고, 비상 시 최단 시간 내 복구를 위하여 경우에 따라서는 공익성이 사적재산권에 우선되어야 하는 특성 등이 있기 때문이다. 정부 주도로 비상 대비 통신 서비스가 준비되기는 하나, 운용 적인 측면에서는 다양한 대안이 있을 수 있다. 비상 통신 서비스 기획이나 계획은 정부부문에서 수립하고 운용측면에서는 비용 효율성 측면에서 민간의 자원을 활용하는 방안과 운용까지도 정부부문이 직접 수행하는 경우가 있을 수 있다. 자가망을 운용하는 경우, 커버리지, 용량, 보안, 통신서비스 우선권 설정 등 네트워크 자원에 대한 통제가 용이하다는 장점이 있는 반면, 구축과 운용 및 유지보수에 소요되는 비용이 많이 들고, 시스템 운용이 비탄력적이며, 기술 발전에 대응하기가 쉽지 않으며, 타 망과의 상호운용성이 용이하지 않다는 문제가 발생할 수 있다. 그러나 상용망을 이용하면 비용 측면에서는 장점이 있으나, 네트워크 자원에 대한 통제, 보안성, 비상사태 발생 시 현장 설치 및 운용의 문제, 상용망에서의 장애로 인한 비상통신 서비스 차질 야기 가능성 등이 단점으로 대두된다. 따라서 비상통신 서비스 설정 시 무엇을 중시할 것인가의 정책적 판단에 따라 운용 주체를 결정하여야 할 것이나, 공익성을 중시하는 관점에서 살펴본다면 캐나다나 호주의 사례처럼 정부가 주체가 되는 자가망이 유리할 것이다. 자가망을 선택하는 경우에는 운용 주체에 대한 문제가 대두되는 데, 정부기관 내에서 운용하는 경우와 별도의 전담기구를 신설하는 경우로 나누어 생각할 수 있다. 일반적으로는 별도의 전담기구를 신설하여 전문성을 확보하는 방향이 바람직 할 것이다.

서비스 측면에서는 비상대비 통신 시스템 체계가 점점 복잡해지고 있으며, 정보통신기술의 발전에 따라 유무선 통합 서비스 제공 방향으로 발전하고 있다는 사실이다. 비상통신 기능 측면에서는 초기에는 음성전화에서의 라이프라인서비스, 자연재해 등 재난 발생 시 재난지역의 비상통신과 복구를 위한 통신서비스 중심이었으나, 점차 방재영역에서의 통신 기능도 증대되고 있다. 제공 서비스 기술 측면에서는 회선기반의 통신에서 IP 기반, 멀티미디어 기반의 서비스로 발전하고 있다. 또한 유무선 기술의 발달에 따라 무선E911에서 보는 바와 같이 무선을 이용한 위치기반서비스가 확대되고 있다.

기술적인 측면에서는 911 뉴욕 테러와 같은 재난에서는 구조 및 복구 요원들간의 통신 장애가 문제점으로 대두됨에 따라 네트워크 및 서비스의 상호운용성 확보가 무엇보다도 중요한 이슈로 인식되고 있다. 따라서 국가 내 기관간 상호운용성 측면 뿐만 아니라 국제적으로도 상호운용

성 확보를 위한 다양한 기술개발 및 표준화가 진행되고 있다.

참고문헌

[1] National Security Action Memorandum No. 252, Establishment of National Communications System, Jul. 11, 1963

[2] 김성연,이준경,이경호, 미국의 국가안전보장 및 비상대비 통신 체제 발전 동향 분석, 전자통신동향분석, 제17권 제6호, 2002.12.

[3] Executive Order 12382,: President's National Security Telecommunications Functions Advisory Committee, Sep. 13, 1982

[4] Executive Order 13010, President's Commission on Critical Infrastructure Protection, July 15, 1996

[5] Office of Homeland Security, National Strategy for Homeland Security, July 2002

[6] Presidential Decision Directive 63: The Clinton Administration's Policy on Critical Infrastructure Protection, May 22, 1998

[7] Executive Order 13130, National Infrastructure Assurance Council, July 14, 1999

[8] Executive Order 13231, Critical Infrastructure Protection in the Information Age, Oct. 16, 2001

[9] Executive Order 13228, Establishing the Office of Homeland Security and the Homeland Security Council, Oct. 8, 2001

[10] Homeland Security Presidential Directive-1, October 29, 2001

[11] Homeland Security Act of 2002

[12] Executive Order 13260, Establishing the President's Homeland Security Advisory Council and Senior Advisory Committees for Homeland Security, Mar. 19, 2002

[13] OMNCS, GETS Planning Guide, Aug. 23, 2000

[14] 김성연,원세호,정충영, 미국의 연방통신서비스 동향, 주간기술동향 98-42

[15] OMNCS, Service User Manual for the Telecommunications Service Priority (TSP) System, NCS Manual 3-1-1, May 5, 2000

[16] FCC, PAS Second Report and Order, FCC 00-242, Jul. 13, 2000

[17] PSWN, Local and Regional Inter-operability Solution Map, Feb. 2003

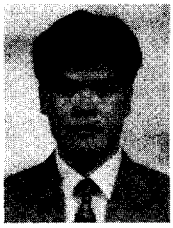
[18] FCC, FCC Wireless 911 Requirements, Jan. 2001

[19] Probst, P.A., ITU-T Project on TDR, Workshop on TDR, 2003

[20] Heidrich, W., ETSI EMTEL Initiative, Workshop on TDR, 2003

[21] FWUG, Project SAFECOM, 2002

김 성 연
1984.2. 고려대학교 통계학 석사
1983.12~ 한국전자통신연구원
네트워크진화팀 팀장



남 기 동
1992.2. 인하대학교 전산학 석사
1992.1.~ 한국전자통신연구원
네트워크진화팀 선임연구원

전 덕 종
2002.2. KAIST 산업공학 석사
2002.5.~ 한국전자통신연구원
네트워크진화팀 연구원