미국의 국가안전보장 및 비상대비 통신 체제 발전 동향 분석 시사점

Analysis on National Security Emergency Preparedness Telecommunications Systems of the USA

김성연 (S.Y. Kim) 네트워크품질보증팀 책임연구원
이준경 (J.K. Lee) 네트워크품질보증팀 책임연구원
이경호 (K.H. Lee) 네트워크품질보증팀 책임연구원, 팀장

재해나 재난이 발생하면 물리적 피해는 지리적 지역을 중심으로 한정적으로 발생하나, 통신재난의 경우 일시적 트래픽 폭주 현상은 전국적인 피해를 입히기도 한다. 또한 이로 인하여 재난 대응체계에 치명적인 손상을 입혀 인명이나 재산상의 피해를 늘리기도 하고, 재난 복구에 차질을 빚게 하기도 한다. 본 고에서는 미국의 국가안전 및 비상대비 통신 프로그램에 대하여 정책적인 측면, 추진 조직 측면과 현재 운용중인 서비스 측면으로 나누어 운용 실태를 살펴보고자 한다.

I. 서 론

세계 각국은 네트워크기반의 정보사회로의 급속한 발전에 따라 통신 인프라스트럭처가 가지는 국가적 중요성을 인식하고 이를 국가가 관리하여야 할 중요 기반시설로 지정하여, 이의 효율적이고 안정적인 운영을 위하여 다각적인 노력을 기울이고 있다. 태풍이나 지진, 홍수, 호우, 해일, 폭풍, 화산폭발과 같은 자연재해, 오클라호마 시 청사 폭발과 같은 내국인에 의해 자행되는 테러, 2002년 9월 11일 뉴욕 무역센터 테러와 같은 외국인에 의한 테러 공격, 인간의 실수에 기인하여 발생하는 재난 등 다양한 형태의 재난이 발생하고 있다. 또한 통신분야에서도 자연재해나 재난에 의한 서비스 장애, 사이버 공간에서의 공격 및 테러, 전화국이나 지중관로의 화재, 도로, 수도, 전기 등 기반시설 공사중의 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 기반구조인 네트워크의 상황에 따라 그 피해의 심각성이나 파급을 미치는 영향 정도가 달라지고 있다고 하여도 과언이 아니다. 일반적으로 재난이 발생하면 물리적 피해는 지리적 지역을 중심으로 한정적으로 발생하나, 통신재난의 경우 일시적 트래픽 폭주 현상은 전국적인 피해를 입히기도 한다. 또한 이로 인하여 재난 대응체계에 치명적인 손상을 입혀 인명이나 재산상의 피해를 늘리기도 하고, 재난 복구에 차질을 빚게 하기도 한다.

그러므로 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(National Security/Emergency Preparedness: NS/EP) 프로그램은 쿠바사태 이후 체계화를 추진하였으며, 역사적 이벤트나 사건의 발생에 따라 그때마다 즉각적인 대응을 하면서 발전시켜 왔기 때문에 매우 복잡하고 다양하게 전개되고 있다.

우리나라의 경우 '자연재해대책법'이나 '재난관리법'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 본고에서는 미국의 국가안전 및 비상대비프로그램에 대하여 정책적인 측면, 추진조직 측면과 현재 운용중인 서비스 측면으로 나누어 운용 실태를 살펴보고자 한다.

II. NS/EP 프로그램 관련 조직

미국의 국가안전보장 및 비상대비 통신 시스템은 1961년 쿠바 미사일 위기 시부터 시작한다. 당시 미국, 소련, NATO 및 기타 외국 원수들간의 통신상의 장애가 발생하여 위기를 보다 복잡한 국면으로 접어들게 한 문제가 발생하였다. 케네디 대통령은 쿠바사태 이후 국가안전보장통신망에 대한 조사를 명령하였고, '국가안전보장회의(National Security Council)'[1]는 범 부처적인 검토위원회를 구성하여 통신망 운용 방안 및 관련기구의 기능조정을 검토하였다. 위원회는 국가위기시 대통령, 국방성, 외교 및 정보활동을 원활하게 수행하기 위해서는 단일의 통합된 통신시스템이 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(National Communications System: NCS)'[2]을 설립하였다.[3]

또한, 미국 정부는 1979년 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. 이에 따라 국가안전보장 및 비상대비 통신 프로그램의 정책수립과 관련된 주요 이슈에 대하여 대통령과 국가통신시스템의 자문을 수행하기 위하여 대통령자문위원회로서 '국가안전보장통신자문위원회(National Security Telecommunications Advisory Committee: NSTAC)'가 1982년 9월에 행정명령(executive order) 12382[2]에 의해 설립되었다.

클린턴 행정부에 들어와서는 국가 주요 기반시설을 지정하여 특별한 보호를 하여야 할 필요성을 인지하고 1996년 7월 행정명령 13010[3]에 의하여 대통령 직속의 위원회인 '국가 주요기반시설 보호에 관한 자문위원회(President's Commission on Critical Infrastructure Protection: PCCIP)'를 설립하였다. 국가주요핵심기반시설은 국방이나 경제 안전에 지대한 영향을 미칠 수 있는 시설이나 시스템으로서 지정된 국가주요 기반시설은 통신망, 전력시스템, 가스 및 오일, 은행 및 금융, 운송체계, 수자원 공급, 정부서비스와 긴급비상서비스가 이 범주

1) 대통령이 주재하며, 부통령, 국무장관, 재무장관, 국방장관, 국가안전보좌관이 참석하며 합참의장이 국방관련 자문역을, 중앙정보국장이 정보자문역을 수행한다.

2) 의장은 국방장관이, 매니저는 DISA(Defense Information Systems Agency)의 장이 겸직하고 있다.

3) NCS 회원기관은 국무성, 재무성, 국방성, 법무성, 내무성, 농림성, 상무성, 보건성, 운수성, 에너지성, 보훈성, CIA, FEMA, The Joint Staff, GSA, NASA, NRC, NTIA, NSA, USPS, FRB, FCC 22개 기관임.

에 포함되었다.[4] 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[4]을 발표하여 국가 주요 기반시설 보호를 위한 정책 기반 및 구체적인 조직을 확립하였다. PDD-63에서는 '국가주요핵심기반시설보증위원회(Critical Infrastructure Assurance Council)'와 '국가주요기반시설보호센터(National Infrastructure Protection Center: NIPC)'의 역할과 기능을 정립하였다.

그리고 1999년 7월 14일 행정명령 13130[5] 및 PDD-63[4]에 의하여 기반시설에 대한 전문지식을 보유한 민간, 주정부 및 지자체에서 추천되는 30인 이내의 대통령 지명직 위원으로 구성이 되는 NIAC(National Infrastructure Assurance Council)[5] 를 설립하였다.

또한 '국가핵심기반시설보증국(Critical Infrastructure Assurance Office: CIAO)'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 부시 대통령은 행정명령 13231[6]에 의하여 '국가 핵심 기반시설 보호를 위한 대통령 자문위원회(President's Critical Infrastructure Protection Board: CIPB)'를 2001년 10월에 설치하였다. 또한 뉴욕 테러의 여파로 2001년 10월 8일 행정명령 13228[7]에 의하여 '본토안전보장국(Office of Homeland Security)'을 설치하고, Homeland Security Presidential Directive-1[8]에 의해 '본토안전보장위원회(Homeland Security Council)'을 설치하였으며, "Homeland Security Act of 2002"[9]에 의거 '본토안전보장성(Department of Homeland Security)'이 설치되었다. 그리고 2002년에는 행정명령 13260[10]에 의해 '본토안전보장자문위원회(Homeland Security Advisory Council)'이 설립되었다.

2002년에 발표된 본토안전을 위한 국가전략[11]에 의하면 비상대비 및 대응(emergency preparedness and response) 분야의 전략 중의 하나로 비상사태 발생시 초기 대응을 위한 1단계 대응 책임자들간의 단절 없는 통신을 확보하는 것의 중요성을 인식하여 그들간의 통신을 위한 장비 및 기술, 절차, 프로세스 등을 정립하기 위한 '국가비상통신계획'을 수립하고, 또한 관련 장비를 2003년부터 본토안전성에서 우선적으로 확보하는 것을 목표로 계획을 수립하고 있다.

III. NS/EP 프로그램 정책

미국의 국가안전 및 비상대비 통신 정책은 통신에 관한 분야, 정보정책에 관한 분야,[6] 최근 들어서는 본토안전[7]에 관한 분야로 크게 나누어 생각할 수 있다. 국가 안전보장 전기통신정책은 국가의 안전보장을 확보하는 데 필요한 전기통신방안, 특히 비상시 연방정부의 전기통신 시스템의 운용관리 방안으로 국가안전보장회의, 국가안전보장통신자문위원회, 국가통신시스템 등이 중심이 되어 정책의 입안 및 실시에 관여하고 있다. 미국 정부의 안전보장과 관련한 기본적인 목표는 다음과 같다.

- 연방정부의 전기통신 시스템은 정부의 소유시설, 전기통신 사업자의 전용선 임대 또는 공중통신망을 이용한 구축 모두가 국가의 안전보장 정책

4) 2002년 발표된 National Strategy for Homeland Security[11]에 정의된 핵심기반시설분야는 농업, 식료품, 수자원, 공중보건, 긴급비상서비스, 정부부문, 국방산업, 정보통신, 에너지, 수송, 금융, 화학산업, 우정분야로 정의되어 있음.

5) NIAC는 행정명령 13231에 의거 2003년 10월까지 운영 예정임.

6) 정보정책분야에 관하여는 D.D. Steinauer, S.M. Radack, and S.W. Katzke, U.S. Government Activities to Protect the Information Infrastructure, NIST[12] 참조.

7) 본토안전에 대한 정책은 Office of Homeland Security, National Strategy for Homeland Security, July 2002[11] 참조.

의 기본적인 요소이다.

- 연방정부의 전기통신 시스템을 뒷받침하는 민간 통신사업자의 존립 유지 및 신뢰성 확보를 도모한다.
- 긴급사태 시 연방정부의 통신시스템에 대한 기본적인 방침 제시
- 긴급사태 시 연방정부의 통신시스템에 대한 계획 및 관리지침 제시
- 연방정부의 통신시스템에 대한 통일성 확보의 핵심이 되는 국가통신시스템 운영방침 입안
- 국가통신시스템 운영을 관리

행정명령 12472[13]에서는 상기와 같은 방침을 효율적으로 수행하기 위하여 대통령 보좌관들의 임무를 전시와 비전시로 구분하여 정의해 놓고 있다.

○ 전시 비상 임무

국가안전보장회의는 통신법 606조에 따라 전시 전쟁 수행을 위한 훈련 정책 지침을 제공하여야 하며, 과학기술정책국(Office of Science and Technology Policy: OSTP)장은 대통령의 전쟁 수행을 위한 훈련 정책 지침에 따라 훈련을 지도한다.

○ 비전시 비상 임무

국가안전보장회의는 국가 통신 자원 사용, 배정, 확인을 위한 연방정부의 정책개발, 계획수립, 프로그램개발, 표준개발을 통해 대통령을 권고, 지원하고, 또한 대통령의 비전시 비상 통신 기능의 훈련 지침을 제공한다.

과학기술정책국장은 위기상황이나 비상사태 시 통신 자원의 공급, 관리, 배정에 관한 책무를 지며, 대통령이나 연방 부처 및 기관들에게 정보를 제공하고, 자문이나 권고 등의 지원을 한다.

계획수립과 관리책임 측면에서 국가안전보장회의는 첫째, 상용망, 정부 보유망, 자가망 등 통신자원의 동원 및 활용을 위한 정책, 계획, 프로그램, 표준을 개발하고, 둘째, 국가통신시스템의 활동에 대한 정책 감사를 하며, 셋째, 연방 정부 기관에 부여된 비상통신 책무 수행 여부를 감사한다.

과학기술정책국장은 국가 안전 및 비상 대비 통신 시스템, 네트워크와 설비에 관한 시험, 훈련, 평가에 관해 권고한다. 또한 국가 안전 및 비상 대비 통신 기능 수행을 위하여 주파수 자원 스펙트럼 활용의 우선순위를 설정한다.

국가 안전과 비상 대비 통신 요구사항은 국가안전보장회의, 과학기술정책국장, 그리고 OMB(Office of Management and Budget) 국장 책임 하에 수립한다.

대통령 보좌관들은 연방 정부 기관들과 국가안전 및 비상 대비 통신에 관한 제반 사항들을 협의하여야 하며, 또한 임무 수행에 필요한 예산지원을 하여야 한다.

그리고 행정명령 12656[14]에는 국가안전보장과 관련한 비상대비 정책 방향과 책무 내용을 정해 놓고 있다.

- 정부 기관은 어떠한 형태의 국가 안보 비상 사태가 발생하더라도 필수적인 방어태세와 민간에서의 요구를 충족할 수 있도록 충분한 능력을 갖추고 있어야 한다. 국가안전보장 및 비상대비 정책은 대통령에 의해 수립되며, 국가안전보장회의는 관련 정책을 개발하고, 관리한다.
- 국가 안전 보장 및 비상 대비 계획 수립 시 필수 요구사항:
  - 비상사태 발생 시 수행되어야 할 기능들
  - 이러한 기능들을 수행하기 위한 세부계획
  - 세부 계획들을 집행하기 위한 능력수준

국가안전 보장 및 비상 대비 체제에 대한 관리 체계는 다음과 같다.

- 국가안전보장회의는 국가안전 보장 및 비상 대비 관련하여 의회와 연방 사법부의 연락 책임자를 지정하여야 한다.
- FEMA 청장은 국가안전 보장 및 비상 대비 이슈와 관련하여 국가안전보장회의에 자문역으로

서 조력하여야 한다.
- 여러 기관들에 의해 수행되어야 하는 국가안전보장 및 비상 대비 기능들은 주 책임을 담당하고 있는 연방정부 기관장에 의해 조정되며, 관련기관은 협조하여야 한다.
- 모든 관련 연방정부 기관은 국가안전 보장 및 비상 대비 훈련을 하여야 한다.
- 모든 계획과 절차는 대통령의 비상 시 활동에 최대한의 유연성을 제공할 수 있도록 고안되고, 개발되어야 한다.

미국의 국가안전보장 및 비상대비 프로그램은 임무나 기능의 중요도와 파급효과에 따라 다섯 가지 범주를 설정하여 운영하고 있다[15].

① 국가 안전에서의 리더십

이는 핵 위협이나 공격이 발생하였을 시 국가의 존립과 관련된 임무를 수행하는 범주이다. 따라서 신속하고도 효율적인 서비스 공급이나 복구가 이루어져야 하는 기능으로서 다음과 같은 기능들이다.

- 다른 국가안전보장 및 비상대비 기능을 지원하기 위한 주요한 회선이나 통제 서비스
- 정부와 국가 안전을 위한 리더십의 지속에 필수적인 대통령 지원 기능
- 국가 보존을 위하여 국방 지휘 및 통제를 지원하는 국가지휘기구(National Command Authority) 관련 기능
- 대혼란을 야기할 수 있는 잠재적 공격에 대한 경고 관련 정보 기능
- 범죄자의 체포나 적대 국가의 세력을 제한하는데 중요한 외교 협상 지원 기능

② 국가안보사태 및 공습에 대한 경고

위기 상황 전후를 막론하고 최적의 방위, 외교 혹은 정부기능의 유지를 위한 기능으로서 국가 비상사태뿐만 아니라 국제적인 위험이나 위기까지를 포함하는 기능이다.

- 위협에 대한 평가 및 공격에 대한 경고 기능
- 외교 기능
- 정보의 수집, 처리 및 배포 기능
- 군사력에 대한 지휘 및 통제 기능
- 군 이동 기능
- 위기상황 시 연방정부의 유지 기능
- 국가 비상사태 시 주 및 지방정부 유지 기능
- 위기 상황 종료 시 주요 국가 기능의 복구와 관련된 기능
- 국가적인 우주 계획 추진과 관련된 기능

③ 공중보건, 안전 및 법질서의 유지

- 공습경보를 제외한 대국민 경고 기능
- 법 집행 기능
- 주 및 지방자치단체의 유지 기능
- 병원 및 의료 물자 분배 기능
- 병참 기능 및 국가 공익 서비스 제공 기능
- 민간 항공 통제 기능
- 민간에 대한 군사 지원 기능
- 주요 민간 시설에 대한 방위 및 보호 기능
- 일기예보 서비스 제공 기능
- NS/EP 기능 제공에 필요한 수송 기능

④ 공중 후생 및 국가경제의 유지

- 식량 및 기타 필수물자의 제공 기능
- 국가 금융 시스템 유지 기능
- 물가, 임금, 지대 안정화 유지 기능
- 전략 물자 및 에너지 공급의 생산 및 분배 통제 기능
- 환경 위험이나 손실에 대한 예방 및 통제 기능
- NS/EP 제공에 필요한 수송 기능

⑤ 재난 복구

- 의료 시설에 수용중인 환자, 장비, 인력과 같은 의료 자원의 관리 기능
- 대피소 구축 및 저장, 상세 피해 분석 및 평가 등과 같은 조정 관련 활동 및 기능

IV. 주요 NS/EP 서비스

국가통신조정센터는 고도지능망서비스, 비상조정네트워크서비스, 정부비상통신서비스, 통신자원공유프로그램, 우선순위통신서비스, 우선접속서비스 등을 제공하고 있다.

1. ACN

ACN(Alerting and Coordination Network)은 국가안전보장 및 비상대비 서비스를 지원하기 위하여 서비스제공 사업자의 비상운용센터(Emergency Operations Center: EOC)와 네트워크운용센터(Network Operations Center: NOC) 간의 안정적인 비상 음성 서비스를 제공하는 것을 목적으로 별개로 구성한 비상용 네트워크이다. ACN은 통신망의 복구를 위한 기관간 업무 조정, 통신 요구사항 및 우선순위의 전송을 목적으로 구성된 네트워크이다. 또한 공중망이 혼잡 상태이거나, 네트워크 성능이 현저히 저하되는 상황시, 혹은 공중망이 운용불능 상태 등일 때 사고보고를 위한 용도로도 활용된다. 그러므로 ACN은 국가통신조정센터를 지원하기 위하여 24시간 상시 운용되고 있다.

2. 정부비상통신서비스(GETS)

정부비상통신서비스(Government Emergency Telecommunications Service: GETS)는 국가 안전과 긴급 상황발생 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[15]. 정부비상통신서비스는 대통령지도통신, 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 전쟁상황 하에서도 가용한 통신자원을 최대한 활용하여 국가, 공공기관, 국방 등에서 그 기능을 유지하기 위하여 필요로 하는 일정한 수준을 상시 제공할 수 있도록 하기 위하여 설계되었다. 자연재해 혹은 인위적인 재해 발생 시– 즉 화재, 동력원의 차단, 선로장애, SW 문제 발생 등– 네트워크 장애는 재해 발생지역 뿐만 아니라 전 지역에 영향을 미친다. 그리고 여러 가지 요인으로 인한 통신의 단절, 통화량 폭주 등으로 인한 공중전화망의 접속의 어려움 등이 발생하여 피해를 증가시키기도 한다. 이러한 상황하에서 국가안전에 영향을 미치는 긴급 상황이 발생하면 우선적으로 수행되어야 할 공공기관의 업무에 차질이 생길 우려가 있으므로 이를 미연에 방지하기 위한 서비스로서 정부비상통신서비스가 개발되었다.

정부비상통신서비스 이용자는 국가통신 시스템 회원기관들을 대상으로 제공되며 연방기관, 각 주, 지방행정기관 등에서의 근무자, 그리고 산업계도 필요에 따라서는 이용자가 될 수 있다. 이러한 국가통신시스템 비회원 기관들의 정부비상통신서비스 이용자는 각 개별 기관들의 책임 하에 관리되고 있으며, 국가통신시스템 사무국의 허가를 득하여 관련 국가통신시스템 회원기관에 신청하면 된다.

그리고 정부비상통신서비스에서 이용하고 있는 네트워크는 주요 장거리 네트워크와 국제 전화 서비스, 지역 네트워크, FTS, DISN 등 정부 임차 네트워크 등을 사용하고 있다.

정부비상통신서비스는 정부비상통신서비스 고유 접속번호와 개인식별번호를 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 지역서비스 사업자들에게도 정부비상통신서비스 이용자

들이 보다 쉽게 정부비상통신서비스의 서비스를 이용할 수 있도록 ELS(Essential Line Service), DTP(Dial Tone Priority)와 같은 서비스를 제공토록 하고 있다. 접속 후 개인 개인식별번호와 전화번호를 등록하여 적법한 이용자인지 여부를 확인하고, 일단 이용이 승인된 후에는 국가안전보장 및 비상대비 통신 이용자로 분류되어 라우팅과 우선 순위에서 특별 취급을 받게 된다.

① 다이얼링 계획(Dialing Plan)

국가안전 및 비상대비를 목적으로 지역번호로 710이 배정되어 있다. 이 특정 국가안전보장 및 비상대비 통신의 지역번호는 장거리전화사업자, 지역전화사업자, 이동전화사업자에게 적용되며 심지어 외국 사업자들에게도 적용하고 있다. 이용자들의 접속방법은 각 이용자들이 가입한 장거리 전화사업자의 정부비상통신서비스 접속번호(1-710-NCS-GETS)를 다이얼링함으로써 접속할 수 있다. 접속이 안되는 경우에는 타 장거리전화사업자를 통해 접속한 후 정부비상통신서비스 접속번호를 돌림으로써 연결이 가능하다. 이 경우 AT&T에는 1010288, MCI에는 1010222, Sprint에는 1010333이 배당되어 있다. FTS2000[8]/2001, 국방정보시스템네트워크, 기타 정부기관의 설비를 통해서도 정부비상통신서비스에의 접속은 가능하다.

② 개인식별번호를 통한 액세스 제어

정부비상통신서비스 이용자는 정부비상통신서비스 접속번호를 통해 접속한 후, 자신의 식별번호와 원하는 서비스 번호를 누르면 된다. 적절하지 않은 개인식별번호를 세 번 입력하면 접속이 자동으로 끊어지게 되도록 설계되어 있다.

③ 강화된 라우팅(Enhanced Routing)

지역전화사업자, 이동전화사업자, 외국 사업자들은 GETS호가 들어오면 3개의 장거리전화사업자에게로 호를 라우팅 시킨다. AT&T는 자사의 네트워크에서 710호를 라우팅 시키는 서비스를 이미 구현하여 운용중이며, MCI, Sprint와 지역전화 사업자들은 라우팅 서비스의 편익과 비용효과성에 대하여 평가중에 있다.

④ 우선순위 처리(Priority Treatment)

정부비상통신서비스 트래픽은 여타 트래픽보다 우선순위가 높고, 또한 제어 호 완성도(High Probability of Completion: HPC)의 제고를 통해 혼잡한 네트워크 상에서 국가안전보장 및 비상대비 호의 완성도를 높이게 된다.

⑤ 국제 호(International Calling)

국제 게이트웨이 스위치에 호를 라우팅 시켜 국제 호 서비스를 이용할 수 있도록 하고 있다. 미국 외의 지역에서 미국으로 들어오는 호인 경우, 외국 사업자가 협약에 따라 미국의 장거리전화사업자에게 호를 연결시켜 주고, 이 호가 미국에 있는 게이트웨이 스위치에 도착한 다음에는 개인식별번호 확인을 거쳐 원하는 상대와 연결이 된다.

⑥ 타 네트워크와의 상호운용성

FTS나 국방정보시스템네트워크를 통해 정부비상통신서비스에 접속하는 경우 FTS나 국방정보시스템네트워크 교환기는 자동으로 정부비상통신서비스에 호를 라우팅하여 준다. 이것이 지역전화 네트워크의 혼잡을 막고 또한 지역전화 네트워크의 장애발생 시 이를 피하는 중요한 방법이다.

⑦ 전송 증대와 복구

위기발생 시에도 CPS 및 우선순위통신서비스 연결성과 네트워크 관리 서비스를 제공하고 있다.

⑧ 번호전환을 통한 액세스

이런 서비스를 요하는 이용자에게는 번호전환 서

8) FTS(Federal Telecommunications Service)의 자세한 내용에 대하여는 김성연 외, 미국의 연방통신서비스 동향, 주간기술동향 98-42[16] 참조.

비스를 제공

⑨ 기록 보호

액세스 통제 기능을 이용하여 특수한 소수인원에게만 접근을 제한함으로써 이용자들의 개인식별번호 데이터베이스와 호 기록 정보를 보호하고 있다.

3. 통신자원 공유(SHARES) 프로그램

통신시스템이 파괴되었거나, 통신망을 이용하여 국가안전보장 및 비상대비 관련 정보를 전송할 수 없을 경우 HF 무선 자원을 이용하여 기관간 비상메시지를 처리하는 것을 목적으로 행정명령 12472에 의해 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 있고, 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. 운용 수준의 변경은 SCN (SHARES Coordination Network) 운용수준변경 고시를 각 무선국에 통보하고, 또한 SHARES 홈페이지와 BBS에도 공지된다.

4. 우선순위통신서비스(TSP) 시스템

우선순위통신서비스(Telecommunications Service Priority: TSP)는 FCC 명령 88-341에 의해 1988년 11월 17일 개설된 서비스이다. 우선순위통신서비스는 비상사태 혹은 위기상황 발생 시 다른 어떠한 서비스보다도 국가중요통신 서비스의 우선순위를 보장하여 줌으로써, 국가안전보장 및 비상대비 이용자들에게 서비스의 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[17].

우선순위통신서비스 대상 서비스는 기간통신사업자가 제공하는 주간 및 주내통신서비스, 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 서비스들 보다도 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 NS/EP 기준의 5개 서비스 범주가 있으며, 서비스 프로파일별 요소는 이용자 단말 및 구내 망 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

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

우선순위통신서비스 권한 코드는 TSP 컨트롤 ID와 TSP 우선순위 수준으로 구성되며, 일반적인 형태는 TSP0A2M6C-03과 같은 형태이다. 전반부가 9자리 ID 코드이며, 후반 2자리 숫자는 우선순위 수준을 표현한다. 후반 2자리 숫자 중 앞의 숫자는 서비스 제공 우선순위를 표현하며, 다음 숫자는 복구 우선순위를 나타낸다. 서비스 제공 우선순위는 E,1,2,3,4,5,0으로 표현되며, 복구 우선순위는 1,2,3,4,5,0으로 표시된다. 여기서 0은 서비스 해당사항이 없음을 표시한다.

연방정부기관이 아닌 기관[9]으로서 국가안전보장 및 비상대비 기능을 수행하는 경우 우선순위통신서비스를 신청하고자 할 때 관련 연방기관의 지휘감독을 받아야 신청할 수 있다. 일반적으로 우선순위통신서비스의 우선순위 배정은 OPT에서 수행하며, <표 1>과 같은 비율로 배정하여 동일 우선순위에 많은 기관이 집중되는 현상을 피하여야 한다.

9) 주정부, 지방정부, 외국정부기관 및 일반 기업도 포함된다.

<표 1> 우선순위통신서비스 우선순위 배정표

서비스범주	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
- 비상우선순위통신서비스 제공(우선순위 'E')
- 복구 우선순위 2,3,4,5에 의한 서비스 복구
- 서비스 제공 우선순위 1,2,3,4,5에 의한 우선순위통신서비스의 제공

우선순위통신서비스 시스템에서 발생하는 여러 가지 문제를 식별하고, 검토하고, 해결방안 등을 제시하기 위하여 1990년 7월 우선순위통신서비스 감독 위원회를 설립하였다. 위원들은 19인[10]으로 구성되어 있으며 연 2회 회의를 개최한다.

5. 우선접속서비스(PAS)

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 재난 구호 사무국으로 호가 몰리는 상황이 발생할 가능성이 크다. 이미 언급한 바와 같이 국가안전보장 및 비상대비 통신 서비스는 상시 사용 가능한 상태로의 유지가 이루어져 있음으

10) 연방기구 소속 7명, 기업체 7명, 주정부 소속 2명, OPC 대표, FCC 대표, 그리고 연방정부관리 1명으로 구성된다.

로써 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.

국가안전보장통신자문위원회에서는 무선 우선 서비스의 필요성을 파악, 클린턴 대통령에게 국가안전 및 비상대비로 취급할 것을 건의, 1995년 1월, 국가통신시스템에게 정부, 산업과 협동하여 무선 우선 서비스를 제공하도록 지시하였다. 국가안전보장통신자문위원회는 무선 서비스 전담팀 산하에 이동 우선접속서비스 하위그룹을 두고 방안을 연구하도록 하였다. 국가안전보장통신자문위원회와 국가통신시스템은 우선 대기 능력을 이용한 기술적 솔루션을 개발함으로써 NS/EP 이용자를 위한 셀룰러 우선 서비스를 제공하는 방안을 수립하였다. 2000년 7월 FCC 00-242[18]에 의하여 우선접속서비스(Priority Access Services: PAS)로 개칭되면서 서비스가 시작되었다.

우선접속서비스 이용 대상자는 국가안전 및 비상사태 대응과 관련한 업무 수행자 모두가 이용할 수 있는 서비스는 아니고, 국방성, FEMA, 소방본부의 긴급의료서비스 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 상용무선 네트워크에 혼잡이 발생하여 접속이 불가능하거나 어려운 상태이며, 긴급사태 관련 업무 수행중이어야 한다. 서비스 제공 사업자는 별도로 지정하지 않으며, 이동전화 허가를 보유한 사업자는 원하는 경우 서비스를 제공할 수 있고, 이 경우 FCC가 지정한 프로토콜을 이용하여야 한다.

V. 맺음말

통신재난의 중요성은 통신기술의 발전과 이용 활성화에 따라 그 중요성이 점점 커지고 있으며, 재난 발생 시 피해 규모도 점차 확대되는 경향을 보이고 있다. 선진 각국에서는 국가안전 및 비상 대비 통신 체계를 국가 주도로 우선적으로 확보하여 운용하고 있다. 재난대비 통신 시스템은 공공재적 성격이 강하고, 민간의 자율에 의존해서는 해결되기 어렵다는 특성 때문에 정부 부문이 직접 개입하고 있다. 본 고에서는 미국의 사례를 정책적인 측면, 추진 조직 측면, 국가안전 및 비상대비 통신서비스 측면으로 나누어 살펴보았다.

NS/EP 통신서비스 제공자는 민간부문이기는 하나 서비스 기획이나 계획은 정부부문에서 수립하고, 서비스 이용자도 정부기관 중심이라는 특성이 있다. 즉 서비스 요구사항은 정부의 필요에 따라 계획되나, 운용측면에서는 비용 효율성 측면에서 민간의 자원을 활용한다는 점이다.

또한 국가안전 및 비상대비 통신 시스템 체계가 점점 복잡해지고 있다는 사실이다. 초기에는 자연재해 등 재난 발생 시 재난지역의 비상통신과 복구를 위한 통신서비스 중심이었으나, 점차 방재영역에서의 통신 기능도 증대되고 있고, 특히 9.11 뉴욕 테러와 같은 재난에서는 구조 및 복구 요원들간의 통신 장애가 문제점으로 대두되었다. 또한 데이터 통신의 활성화에 따라 사이버 공간에서의 테러 문제도 대두되고 있으며, 이에 따라 정보 보호 자체 뿐만 아니라 네트워크 보호에 관한 방안까지도 포함하여 운용되고 있는 등 점차 복잡해지고 있는 경향이다.

그리고 기술적인 측면에서도 네트워크의 생존성 증대 문제, 음성전화 위주의 서비스에서 데이터 통신 서비스로의 전환 문제, 데이터 통신에서의 정보 보안, 네트워크 보안 등의 문제들은 아직 해결하여야 할 과제로 남겨져 있다.

우리나라의 경우에도 자연재해나 재난관리 계획 수립 시 미국의 사례에서 드러난 한계점들을 해결하는 방향을 강구해야 할 필요가 있다.

참 고 문 헌

[1] National Security Action Memorandum No. 252,

Establishment of National Communications System, July 11, 1963.
[2] Executive Order 12382, Sep. 13, 1982.
[3] Executive Order 13010, July 15, 1996.
[4] Presidential Decision Directive 63, May 22, 1998.
[5] Executive Order 13130, July 14, 1999.
[6] Executive Order 13231, Oct. 16, 2001.
[7] Executive Order 13228, Oct. 8, 2001.
[8] Homeland Security Presidential Directive-1, Oct. 29, 2001.
[9] Homeland Security Act of 2002.
[10] Executive Order 13260, Mar. 19, 2002.
[11] Office of Homeland Security, National Strategy for Homeland Security, July 2002.
[12] D.D. Steinauer, S.M. Radack, and S.W. Katzke, U.S. Government Activities to Protect the Information Infrastructure, NIST.
[13] Executive Order 12472, Apr. 3, 1984.
[14] Executive Order 12656, Nov. 18, 1988.
[15] OMNCS, GETS Planning Guide, Aug. 23, 2000.
[16] 김성연, 원세호, 정충영, 미국의 연방통신서비스 동향, 주간기술동향 98-42, pp. 1 - 13.
[17] OMNCS, Service User Manual for the TSP System, NCS Manual 3-1-1, May 5, 2000.
[18] FCC, PAS Second Report and Order, FCC 00-242, July 13, 2000.