

# EMP, SF의 무기가 아니라 현실적인 위협입니다

김원배 정보통신용어표준화위원회(WORDSTD) 위원, 전자신문 부장

고출력 전자파(EMP, Electromagnetic Pulse)란 핵폭발에 의해 발생하는 전자기 충격파를 말한다. 흔히 컴퓨터와 전산망 등 모든 전자 기기와 시스템을 물리적으로 파괴시킬 정도의 강력하고 순간적인 전자기적 충격파로 정의한다. 전자기기와 시스템은 물론, 국가 경제·사회에도 영향을 미칠 수 있다.

## 전자기기를 파괴하는 EMP

EMP는 1962년 그 실체 혹은 존재가 확인됐다. 1962년 7월 미국은 태평양의 존스톤 환초에서 핵무기 실험을 수행했다. 그런데 실험 중 섬으로부터 1,500km나 떨어진 하와이에서 일부 전기 시스템을 비롯해 텔레비전과 전화, 신호등이 꺼지고 공습경보 사이렌이 오작동하며 전자 기기에 이상현상이 발생했다. 미국은 이러한 이상현상의 원인이 핵폭발로 인해 발생한 EMP라는 사실을 확인했다. 이후 EMP가 동식물이나 인체에는 별 영향이 없지만 통신, 전력, 교통, 금융 등의 전자기기 및 이에 기반한 시스템을 파괴하거나 무력화할 수 있다는 사실도 밝혀냈다.

EMP의 정체는 이름 그대로 전자기파다. 핵폭발이 일어나면 파장이 매우 짧고 에너지가 큰 방사선인 감마선이 대량으로 쏟아져 나온다. 감마선

은 짧은 시간에 퍼져나가는 강력한 파장인 ‘펄스’의 형태로 폭심지로부터 모든 방향으로 퍼져 나가며 전기를 사용하는 기기에 오작동을 일으킨다.

전자기기에 미치는 영향에 주목한 과학자들은 EMP를 무기로 활용할 수도 있음을 깨달았다. 사람에게는 직접적인 피해를 주지 않으면서도 넓은 지역에 걸쳐 현대사회의 인프라와 첨단 무기를 작동 불가능한 상태로 만들 수 있기 때문이다. 가장 간단한 방법은 핵탄두를 공중 높은 곳에서 폭발시키는 것이었다. 일반적인 폭발과는 달리 지표면보다 30km 이상의 높은 고도에서 폭발할 때 피해가 더 크다. 폭심지 주변의 공기 밀도가 낮아서 감마선이 더 멀리까지 퍼져 나가기 때문이다. 공중폭발한 핵탄두는 순간적으로 강력한 감마선 펄스를 사방에 내뿜으며 각종 전자 기기를 파괴한다.

또 다른 방법은 대규모 코일을 이용하여 순간적으로 강한 전자기 펄스를 내보내는 것이다. 핵폭발보다는 약한 EMP를 생성하지만 반복적으로 EMP를 쏘아내 특정 지역에만 EMP를 일으킬 수 있다. 2003년 이라크전 당시 미국이 이라크 국영방송을 상대로 이같은 방법으로 공격한 것으로 알려졌다.

각종 전산망과 전자기기를 모두 무력화시켜 속

수무책으로 만드는 EMP는 군사적으로 강력한 무기일 뿐 아니라 일상생활을 위협하는 요인이기도 하다. 현대 사회는 첨단 정보통신기술(ICT)을 활용한 전자기기가 고도로 복잡한 네트워크를 이뤄서 전자기기가 파괴되면 사회 전체가 멈출 수 있기 때문이다. ICT 기술에 기반한 현대 사회는 분명 편리하고 효율적이지만 EMP와 같은 예상치 못한 위협요인에 대비하지 않으면 정치·경제·사회의 신명망 시스템이 한순간에 붕괴되거나 짧은 시간에 암흑상태로 전락할 수 있는 잠재적인 위험이 존재하고 있는 것이다. 더욱이 사물인터넷(IoT), 빅데이터, 인공지능(AI) 등 첨단 ICT를 기반으로 하는 4차 산업혁명 시대에 그 위험성은 추정조차 어려울 정도다.

#### 사후 대응이 무의미한 EMP, 표준으로 대비한다

그렇다면 EMP의 위협을 어떻게 막을 수 있을까? 두 가지 방법이 있다. 하나는 전산시설로 EMP가 유입되는 것을 차단해서 EMP 공격을 무력화하는 것, 다른 하나는 EMP에 피해를 입더라도 인프라가 정상적으로 동작할 수 있도록 서비스 가용성을 확보하는 것이다.

EMP 유입 차단은 전산시설 등을 보호하기 위해 차폐 가능한 재료로 밀폐함으로써 유입을 차단하거나 감쇄하는 방법이다. 전산시설 등을 지하 공간에 설치해 지형지물과 암반 등을 자연적인 차폐제로 활용할 수도 있다. 물리적으로 완전하게 보호하기 어려운 전력선이나 통신선 등에는 EMP 차단필터를 설치해서 방어할 수 있다.

서비스 가용성을 확보하는 방안은 원격지에 전산기기 등을 이중으로 구성해 특정 시설이 EMP 공격을 받더라도 다른 시설을 통해 서비스를 정상으로 제공하는 방법이다. 예비기기와 데이터 백업 체계를 마련해 EMP 공격으로 전산시

설이 완전히 파괴될 경우 백업 시스템을 가동해 대처한다.

우리나라에서는 2017년 9월 북한이 조선중앙TV를 통해 EMP 공격 가능성을 언급하면서 대책 마련이 요구됐다. 당시 군의 EMP 방호태세 강화는 물론 주요 국가시설, 민간 시설도 EMP 공격에 대비한 데이터 백업 및 시스템 이중화의 필요성이 제기됐다.

현재 우리나라 EMP 대비 기준은 2009년 제정된 ‘전자파 방호시설 설계 기준’과 2017년 발간된 ‘EMP 침해방지대책 기술 기준’ 등이 있으나, 실효성이 부족하다는 지적이 잇따랐다. 다행히 최근 국가 차원에서 EMP 위협에 대한 선제적 대비가 필요하다는 공감대가 전문가를 중심으로 확산되고 있다. EMP 공격 및 차단 기술이 쉽게 습득하기 어려운 첨단 기술인 만큼 국산화를 서두르고, 지원도 집중해야 한다고 입을 모으고 있다.

이에 국가정보원 주도로 정보통신기반보호법에 따라 공공기관 정보통신기반시설에 대한 EMP 취약점 분석 및 평가 기준을 수립할 계획이다. 그간 공공기관은 주요 국가시설에 대해 자체 EMP 영향 시뮬레이션을 진행하고 관련 복구방안을 수립했지만 이들 대책의 실효성을 판단할 근거가 없었다. 그러나 분명한 기준이 수립되면 공항·철도 등 공공시설의 EMP 대응 실태를 파악하는 동시에 취약점과 개선안 도출이 가능할 것으로 전망된다.

EMP처럼 광범위한 피해를 주는 요인에 대해서는 사후 대응의 의미가 없다. 미리 철저한 방어체계를 세우고 이를 정확하게 분석해야 한다. EMP 관련 표준이 중요한 이유도 여기에 있다. 객관적인 분석툴과 평가 기준은 개발되어야 실효성 있는 EMP 대책이 마련될 수 있을 것이다. 