고출력 전자기파 방호제도

정 연 춘

서경대학교 전자공학과

Ⅰ. 서 론

현대의 국가 안보는 군사 분야뿐만 아니라, 비군사 분야를 포함하는 포괄적 안보 개념으로 확대되고 있으며, 따라서 통합 접근법에 따라 국가 위기를 총괄적으로 관리, 통합, 조정할 필요가 있다. 과거의 사회 기반 구조를 구성하는 시스템 및 네트워크는 물리적 및 논리적으로 독립되어 있었고, 각 부문의 상호 연계성도 많지 않았다. 그러나 오늘날에는 기술 발전에 따라 각 부문에 속한 시스템이 컴퓨터와 통신 수단을 이용하여 자동화되고 상호 연계되어, 보다 경제성 있고 효율적으로 운영되고 있지만, 역으로 상호 접속이 강화된 한 개별 부문에서의 고장 영향은 사회 전반으로 파급되어 큰 혼란을 일으킬 수 있는 가능성은 오히려 커졌다[1],[2].

이러한 개별 부문에서의 고장은 자연 재해 및 인적 재난 등으로부터 발생하며, 인적 재난에는 인간의 실수를 비롯하여 사이버 위협 및 물리적 위협을 포함한다. 또한, 물리적 위협에는 다양한 종류의 폭발물의 폭발은 물론, 고출력 전자기파를 포함한 전자기 무기에 의한 위협이 포함된다. 북한의 핵 위협을 비롯하여 국제적으로 고출력 전자기파에 의한 공격으로부터 국가 주요 시설을 방호하는 것은 매우 중요한 이슈로 부각되고 있으며, 이러한 위협으로부터 국가 중요 시설을 조기에 효과적으로 방호하는 방법은 법적 제도를 마련하여 시행하는 것이다.

미국은 물론, 유럽연합 등에서 고출력 전자기파를 국가 안보를 위협하는 대상의 하나로 인식하고, 이에 대한 방호대책을 강구하고 있다. 우리나라에서도 현재 국가기관을 중심으로 관련 기술 기준을 마련하고, 소요 기술 확보를 준비 중이나 국가 주요 시설에 방호대책을 추진할 수 있는 제도(시행령, 규정 등) 및 절차 등 현실적 근거가 미흡하여 시행에 어려움을 겪고 있다. 본 논문에서는 국내, 외의 관련 제도를 살펴보고, 우리나라의 현행 관련 법령의 개정 방향과 구체적으로 법령에 담아야 할 내용에 대해 살펴보고자 한다.

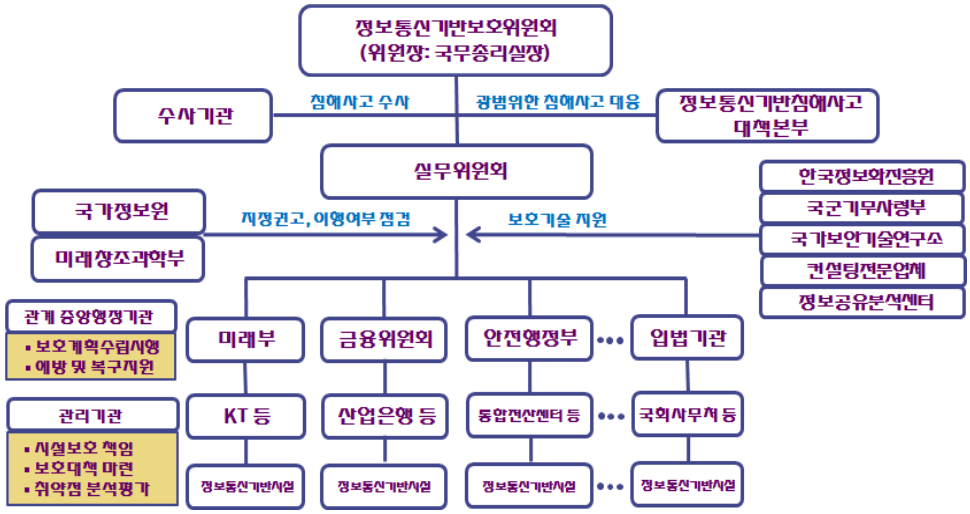
Ⅱ. 국내·외 제도 현황

2-1 국내 제도 현황

2-1-1 정보통신기반보호법

정보통신기반보호법은 해킹, 컴퓨터 바이러스를 비롯하여 고출력 전자기파 등의 “전자적 침해행위”로부터 국가안전보장·행정·국방·치안·금융·방송통신·운송·에너지 등의 업무와 관련된 전자적 제어·관리 시스템과 정보통신망을 보호하는 것을 목적으로 한다. 현재, 사이버 침해 행위 발생 시 국민의 기본생활 및 경제안정에 중대한 영향을 미칠 수 있는 200여개의 정보통신시설을 주요 정보통신기반시설로 지정되어 관리되고 있다.

현행 정보통신기반보호법의 추진 체계는 [그림 1]에서 볼 수 있는 것처럼, KT 등과 같은 관리기관은 시설보호의 책임을 가지며, 관계 중앙행정기관은 보호계획을 수립 시행하고, 예방 및 복구지원을 실시한다. 또한 국가정보원과 미래창조과학부는 각기 공공



[그림 1] 현행 정보통신기반보호법 추진 체계

분야와 민간분야 정보통신기반시설의 지정을 권고하고, 이행 여부를 점검하도록 규정되어 있으며, 정보화진흥원, 국가보안기술연구소, 컨설팅전문업체 등이 보호기술을 지원하도록 규정되어 있다.

동법 제9조에 의해, 관리기관의 장은 대통령이 정하는 바에 따라 정기적으로 소관 주요 정보통신기반시설의 취약점을 분석·평가하여야 하며, 미래창조과학부장관은 관계 중앙행정기관의 장 및 국가정보원장과 협의하여 취약점 분석·평가에 관한 기준을 정하도록 규정하고 있다.

동법 및 시행령에 근거하여, 주요 정보통신 기반시설의 관리기관이 자체 전담반을 구성하여 직접 취약점 분석·평가를 수행하거나, 한국인터넷진흥원, 정보공유·분석센터, 전자통신연구원, 지식정보보안 컨설팅전문업체 등과 같은 외부 전문기관에 취약점 분석·평가를 위탁 수행할 수 있다. 취약점 분석·평가 기본 항목은 ① 관리적, ② 물리적, ③ 기술적으로 구분하여, 3단계(상·중·하)로 중요도를 분리하여 "상"인 점검 항목은 필수적으로 점검하고, "중"·"하" 항목은 기관의 사정에 따라 선택 점검하며, 점검 결과를 비밀성·무결성·가용성을 고려하여 위험 등급(상·중·하)을 표시하고, 위험 등급 "상"은 조기 개선, "중"·"하"는 중기 또는 장기 개선토록 요구한다.

이러한 "주요 정보통신기반시설 취약점 분석·평가 기준"은 악성 코드 유포, 해킹 등 사이버 위협에 대한 주요 정보통신기반시설의 취약점을 종합적으로 분석 및 평가·개선하는 일련의 과정을 규정하고 있으나, 고출력 전자기파에 대한 부분은 평가 항목에서 포함되어 있지 않다.

따라서 관련 취약점 분석·평가 기준에 고출력 전자기파와 관련된 구체적 내용과 절차를 추가함으로써 비교적 쉽게 빨리 고출력 전자기파에 대한 주요 정보통신 기반 시설의 방호를 실현할 수 있을 것으로 판단된다. 그러나 현행 분석·평가기준이 사이버 보안에 근거하고 있고, 또한 고출력 전자기파 보안은 사이버 보안과 적용되는 전문 기술도 많이 상이하므로, 별도의 분석·평가 기준을 수립할 필요가 있다. 그러나 궁극적으로는 정보통신기반보호법을 개정하여 기존의 사이버 보안과 차별화된 내용의 제도화하고, 정보 보호, 산업 육성, 연구 개발 지원, 교육 홍보 강화 등에 관한 조항을 신설하는 것이 바람직한 것으로 판단한다.

2-1-2 지능형 전력망 구축 및 이용 촉진에 관한 법률

지능형 전력망 구축 및 이용 촉진에 관한 법률에서 "지능형 전력망"이란 전력망에 정보통신기술을 적용하여, 전기의 공급자와 사용자가 실시간으로 정보를 교환하는 등의 방법을 통하여 전기를 공급함으로써 에너지 이용 효율을 극대화하는 전력망이라고 정의하고 있다. 따라서 지능형 전력망에 고출력 전자기파가 노출될 경우, 큰 위해를 일으킬 수 있는데, 동법 시행 규칙 제2조에서 지능형 전력망의 안정성, 보안성 및 운용 효율을 향상시키는 기술을 "지능형 전력망 기술"로 정의하고, 관련 규정을 명문화하고 있다.

동법 제26조(지능형 전력망 정보의 보호조치 등)에서는 지능형 전력망 사업자는 지능형 전력망 정보의 신뢰성과 안전성을 확보하기 위해 몇 가지의 보호조치를 취해야 하고, 그 하나로 「정보통신기반보호법」 제2조 제2호에 전자적 침해행위의 방지 및 대응을 위한 정보보호 시스템의 설치·운영 등 기술적·물리적 보호조치를 취하도록 규정하고 있다. 또한 동법 제27조(정보보호의 이행 확인 등)에 의해 지능형 전력망 사업자는 매년 지침의 이행 여부를 확인하게 되어 있으며, 동법 시행령 제16조(정보보호 이행확인 대상 사업자)에 의해 「정보통신기반보호법」 제5조의 2에 따라 주요 정보통신 기반 시설 보호대책 이행 확인을 받은 자는 이행 확인 대상 사업자에서 제외하는 것으로 규정되고 있다. 따라서 지능형 전력망의 안정성 및 보안성과 관련된 전자적 침해방지 대책은 「정보통신기반보호법」에 위임되어 이루어지고 있는 것으로 판단할 수 있다.

2-1-3 재난 및 안전관리 기본법

각종 재난으로부터 국토를 보존하고, 국민의 생명·신체 및 재산을 보호하기 위하여 "재난 및 안전관리 기본법"이 시행되고 있으며, 에너지·정보통신 등 그 기능이 마비될 경우, 인명과 재산 및 국가경제에 심각한 영향을 미칠 수 있는 물적·인적 체계로서 지속적으로 관리할 필요가 있다고 인정되는 시설을 동법 제25조 2에 근거하여 "국가기반시설"로 지정하고 있다. 현재 에너지·정보통신·교통수송·금융·보건의료·원자력·환경·식용수 등 9개 분야 250여개 시설이 지정·관리되고 있는 것으로 알려져 있으며, 일부 정보통신 시설은 주요 정보통신기반시설로도 중복 지정되어 있다.

동법에서 정의하고 있는 "재난"에는 태풍·홍수·가뭄·지진·낙뢰·황사·적조 등과 같은 자연현상으로 인해 발생되는 재해는 물론, 화재·붕괴·화생방 사고·환경오염 사고 등과 같은 일정 규모 이상의 피해, 감염 및 가축전염병 확산으로 인한 피해를 비롯하여, 에너지·통신·교통·금융·의료·수도 등 국가 기반 체계의 마비를 포함하고 있다. 동법 및 시행령에는 자연재해 및 인적 재난에 대한 예방조치, 안전점검 및 조치, 응급조치 및 구조, 복구, 보상 등을 규정하고 있으며, 동법에 근거하여 국무총리는 "국가안전관리기본계획"의 수립지침을 작성하여야 하고, 행정안전부장관은 "국가재난관리기준"을 제정하여 운용하도록 되어 있다.

그러나 고출력 전자기파 위협이 에너지·통신·교통·금융·의료·수도 등 국가 기반 체계를 마비시킬 수 있음에도 불구하고, 재난의 원인으로 분류되어 있지 않음에 따라 고출력 전자기파에 대한 구체적인 내용도 포함되어 있지 않다. 특히, 국제적으로 고출력 전자기파에 대한 전력망 및 통신망 보호가 시급하게 강구되고 있음을 고려할 때, 장기적으로는 재난 및 안전관리 기본법이 정하고 있는 국가적 재난의 한 유형으로 고출력 전자기파이 포함되어야 한다. 현행 정보통신기반보호법으로 고출력 전자기파에 의한 재난을 예방하고, 대비하는 것은 가능하지만, 사후 대응하고, 복구하는 데는 한계를 가질 것으로 판단한다. 따라서 장기적으로 재난 및 안전관리법에서 정한 인적 재난의 한 유형으로 고출력 전

자기파를 규정하여 국가적 재난 및 안전관리체계에 포함시킬 필요가 있을 것으로 판단한다.

2-1-4 기타 법령

“정보통신망 이용 촉진 및 정보보호 등에 관한 법률”에도 고출력 전자기파에 의한 침해 사고를 정의하고 있으나, 정보통신망의 안정성을 확보하기 위해 필요한 구체적인 절차 등은 마련되어 있지 않다. 침해 사고의 대응을 위해 한국인터넷진흥원이 침해 사고에 관한 정보의 수집・전파, 침해 사고의 예보・경보, 침해 사고에 대한 긴급 조치 등에 관한 업무를 담당하여 수행하도록 하고 있다. 그러나 대부분 정보보호 업무와 관련되어 있고, 고출력 전자기파 침해방지와 관련한 업무는 전혀 이루어지지 않고 있는 실정이다.

또한 국제적으로 전력망 보호는 국가 기반 시설의 상호 의존성을 고려할 때, 가장 중요하게 다루어지고 있다. 또한, 미래의 지능형 전력망에서는 고출력 전자기파에 매우 취약한 컴퓨터와 감시 제어 데이터 수집(SCADA: Supervisory Control And Data Acquisition) 시스템이 보다 중요한 역할을 하므로, 이에 대한 방호는 매우 중요하다. “전기사업법”에서 송・배전 전기설비의 안전관리를 규정하고 있다. 그러나 관련 세부 기술 기준은 마련되어 있지 않을 뿐만 아니라, 전기 안전에 관한 조사・연구・기술 개발 및 홍보, 검사・점검 업무를 담당하는 한국전기안전공사 등에 관련 전문가가 부재하므로, 관련 업무 진행에 어려움이 있을 것으로 판단한다.

2-2 외국 제도 현황

2-2-1 미국

미국은 국가의 핵심 기반 시설 방호를 국토안보부가 국가기반 시설 보증 계획(NIAP: National Infrastructure Assurance Plan)을 수립하여 주관하고 있으며, <표 1>에 보인 것처럼 8개 부처 18개 부문에서 수행할 특별방호계획(SSP: sector specific plan)을 각각 제정하여 시행하고 있다[3]~[5]. 여기에서, 핵심 기반 시설은 고도로 상호 의존적으로 함께 작동하는 인적 자산, 물리적 시스템, 사이버 시스템을 포함한다[6]. 클린턴 정부시절, 국가 핵심기반 시설 방호는 사이버 위협이 주 관심사였으나, 911 테러를 겪은 부시 정부에서부터 물리적 위협에 대한 보안을 포함한 보다 강화된 방호 개념을 수립 시행하고 있다.

미국은 국가 핵심기반 시설 방호에 관한 대통령자문위원회 보고서에서 네트워크로 연동된 정보시스템(networked information systems)에 대한 위협으로 물리적 위협과 사이버 위협으로 구분하고, 또 물리적 위협을 폭발물과 전자적 무기로 세분하며, 전자적 무기에 고출력 전자기파와 누설 전자파(TEMPEST)를 규정하고 있다. 또한, 국립소방협회(NFPA: National Fire Protection Association)의 업무 연속성을 위한 재난관리표준인 NFPA 1600에서는 고출력 전자기파와 지자기 폭풍을 인적 재난 및 자연재난으로 분류하고 있으며[7], 국토안보부 산하 연방위기관리청(FEMA: Federal Emergency Management Agency)은 고출력 전자기파로부터 중요 인프라 시설을 보호하는 업무를 담당하고, 방어 가이드라인(CPG 2-17: Electromagnetic Pulse Protection Guidance - 비공개)을 제정, 운영하고 있다.

<표 1>에 보인 각각의 국가 핵심 기반 시설과 자원(CIKR: Critical Infrastructure and Key Resource)에 대한 특별 방호 계획에는 대개 다음과 같은 내용을 포함한다.

1. 부문별 목표 및 세부 목적
2. 보호하고자 하는 자산, 체계, 망의 식별
3. 리스크 평가
4. 기반 시설에서의 우선처리(prioritization)
5. 보호 프로그램과 복구 전략의 수립 시행
6. 효율성 판단
7. 핵심 기반 및 주요 자원 보호 연구개발 협력

〈표 1〉 미 정부 부처별 담당 국가 핵심 기반 시설

정부 부처	담당 핵심기반 및 자원
농무부/식품의약청[a]	· 농업 및 식품(육류, 가금류, 난제품 포함/제외)
국방부	· 방위산업기지
에너지부	· 에너지(석유 및 가스 생산, 정유, 저장, 유통 포함) 및 전력(상업용 핵 전력설비 제외)
보건사회복지부	· 의료 및 공중 보건
내무부	· 국가 기념물 및 상징물
재무부	· 은행 및 재정
환경보호청[b]	· 음용수 및 정수 처리 체계
국토안보부	
기반 시설보호사무국[c]	· 상업 시설 · 기반 제조 시설 · 응급서비스 · 원자로, 핵연료, 핵폐기물 · 댐 · 화학
사이버보안 및 통신사무국[d]	· 정보기술 · 통신
수송안전관리청[e]	· 우편 및 해운
수송안전관리청 및 연안경비대[f]	· 수송 체계
연방방호서비스국[g]	· 정부 시설

참조 : [a] Food and Drug Administration,
[b] Enviromental Protection Agency,
[c] Office of Infrastructure Protection,
[d] Office of Cyber Security and Communitions,
[e] Transportation Security Administration,
[f] U.S. Coast Guard,
[g] Federal Protective Service

8. 부문별 책임의 관리 및 협력

이러한 업무의 총괄은 국토안보부 내의 NPPD(National Protection & Programs Directorate)가 주관하고 있으며, NPPD 내에서는 IP(Infrastructure Protection)가 담당하고 있다. 또한 각 부문에서의 리스크 평가는 관련 연방기구의 인력이 포함된 NISAC(National Infrastructure Simulation and Analysis Center)에서 지원되며, Sandia National Laboratories와 Los Alamos National Laboratory가 주요 역할을 수행하고 있는 것으로 판단된다.

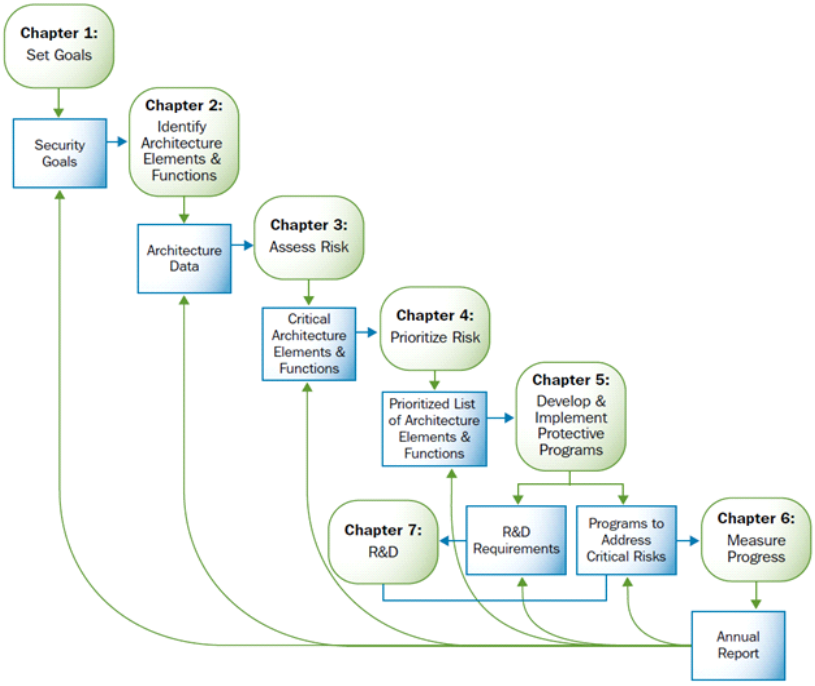
[그림 2]는 18개 부문 중에서 통신 부문에서 작성된 특별 방호계획의 목차이다[8]. 통신 부문에서의 특별 방호계획을 수립하는데 NIPP에 입각하여, 핵심기반 부문은 비용-편익 평가(cost-benefit assessment)에 근거하여 다양성, 용장성, 그리고 복구 가능성(recoverability)을 적절히 혼합하여 통신 복구(resilience)을 달성할 책임이 있다.

통신 부문에는 다음과 같은 원칙이 적용된다.

· 용장성(redundancy): 다중도(multiplicity), 여분(spares)
· 다양성(diversity): 다중 경로(multiple routes), 다수 공급자
· 민첩성(agility): 빠르게 천이 및 이동하는 능력
· 적응성(adaptability): 빠르게 다시 조정하는 능력
· 우선 순위(prioritization): 전용 또는 공유 자원을 활용
· 지리적 특성: 분산성(diversity), 근접성(proximity)
· 방호(힘, 자연재해, 전자기 펄스에 대한)
· 보안(사이버 보안 및 물리적 보안 모두)

또한 복구 평가(resilience assessments)를 수행할 때, 다음 사항을 포함하여 고려하는 것이 중요하다.

· 필수 비즈니스 기능(essential business functions)
· 각각의 필수 기능의 시간적 민감도(time sensitivity)
· 기능과 기능에 의존하는 서비스의 연속성에 대한 위협
· 위협 저감에 대한 옵션
· 비용-편익 분석(cost-benefit analysis)
· 저감 전략(mitigation strategy)
· 시행(implementation)



[그림 2] 미국 통신부문의 특별 방호계획의 목차

· 시험 검사(testing)

· 정보 공유(information sharing)

또한 미국 하원에는 국토안보위원회(Committee on Homeland Security)가 있고, 그 산하에 6 개의 소위원회가 운영되고 있는데, 그 중의 하나가 사이버보안, 핵심기반 시설 방호, 보안기술 소위원회(Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies)이다. 이 소위원회에서 고출력 전자기파와 관련된 법안을 검토하며, 다양한 종류의 청문회를 개최하고 있다. 2012년 9월 12일에 개최된 소위원회 청문회보고서에 의하면, 2012년 9월까지 17개의 연방 재난경보체계 무선국(National level Emergency Alert System radio stations)에 EMP 방호를 완료하고, 2013년에 20개의 연방 재난경보체계 무선국에 추가 투자를 계획하고 있음을 보고하고 있다[9]. 이러한 보고서를 통해 미국은 이미 재난경보체계에 대한 고출력 전자기파 방호를 투자하고 있음을 알 수 있다.

또한 특별위원회로서 EMP Commission이 운영되고 있다. 본 위원회는 고 고도 핵 전자기파 공격으로부터 군사시설은 물론, 민간시설의 방호능력을 평가하기 위해 2001년도에 설립되었으며, 2004년과 2008년에 보고서를 출판하였는데, 고 고도 핵 전자기파의 위협과 미국의 핵심기반 시설의 취약성이 어떠한지를 이해하는데 큰 도움이 된다. 2004년 보고서는 전체 보고서의 요약보고서만 공개되고 있으며, 다른 3권의 보고서는 기밀로 분류하고 있다[1],[2].

미국 국토안보부 산하 연방재난관리청(FEMA: Federal Emergency Management Agency)은 민간에 대한 국가적 재난의 전주기적 과정(예방 · 대비 · 대응 · 복구)을 관리하고 있다. 특히, 연방재난관리청에서는 다음과 같은 고출력 전자기파에 대한 민간의 대응 가이드(CPG: Civil Preparedness Guides) 제작, 활용하고 있는데, 기밀문서로 취급되어 그 내용을 파악하기 어렵다.

- CPG 2-17 Feb-91 Electromagnetic Pulse Protection Guidance Volume 1
- CPG 2-17 Feb-91 Electromagnetic Pulse Protection Guidance Volume 2
- CPG 2-17 Feb-91 Electromagnetic Pulse Protection Guidance Volume 3

또한 국가의 핵심기반 시설의 방호와 관련한 교육과 홍보를 위해 해군대학원 내에 국토안보센터(CHDS: Center for Homeland Defense and Security)를 설치하여, 석사학위 과정과 다양한 형태의 단기강좌를 운영하고 있다. 또한 George Mason 대학에 핵심기반 시설 방호 프로그램을 운영하고 있으며, 연방재난관리청을 비롯한 여러 산하 단체에서 다양한 형태의 교육 강좌를 개설하여 운영하고 있다.

2-2-2 기타 국가

유럽연합에서도 “New European Approaches to Counter Terrorism” 보고서를 통해 대테러 방안에 고출력 전자기파 방호를 포함시켰으며, 2006년에 EU COM (2006) 786에 따라 핵심기반 시설 방호를 위한 유럽 프로그램(EPCIP: European Program for Critical Infrastructure Protection)을 회원국의 법령으로 채택하도록 하였다. 특히, 영국에서는 2012년 2월에 하원 국방위원회에서 “Developing Threats: Electro-Magnetic Pulses (EMP)”라는 제목의 보고서, HC 1552를 출간하였는데, 고 고도 핵 전자기파와 고출력 비핵 전자기파, 지자기 폭풍에 대한 위협이 대두되고 있으며, 국가 핵심 기반 시설에 대한 방호, 특히 전력망에 대한 고출력 전자기파 방호를 강조하고 있다[10]. 또한, 2012년 12월에 재무부에서 국가 기반 시설 방호계획을 보완하여 발간한 바 있다.

또한 러시아에서는 2007년에 기존의 정보보호 관련 규정, GOST R 50922 및 51275 규격에 추가하여 고출력 비핵 전자기파(의도성 전자파 장해)에 대한 자동화 시스템의 보호를 위한 GOST R 52863 규격을 발표한 바 있다[11]. 노르웨이는 NORFO SL 238 & 239 규격을 적용하고 있고, 일본에서는 신정보시큐리티기술연구회(IST: Information Security Technology study group)에서 독립행정법인 정보통신연구기구(NICT)의 협력을 얻어 “전자파 시큐리티 가이드라인”을 작성하여 적용하고 있다.

Ⅲ. 국내 현황의 문제점 및 발전 방향

3-1 국방 분야

현재 우리나라에서 군사적 목적으로 많은 수의 방호시설이 소요 제기되고 있는 것으로 알려져 있다. 보다 자세한 내용은 보안에 저촉될 수 있으므로 생략한다. 다만, 필자가 2013년 11월 22일에 국방부 국방시설본부에서 개최한 2013 방호시설 발전세미나에서 발표한 내용에 근거하여 현안 문제점과 개선 방향을 언급하고자 한다.

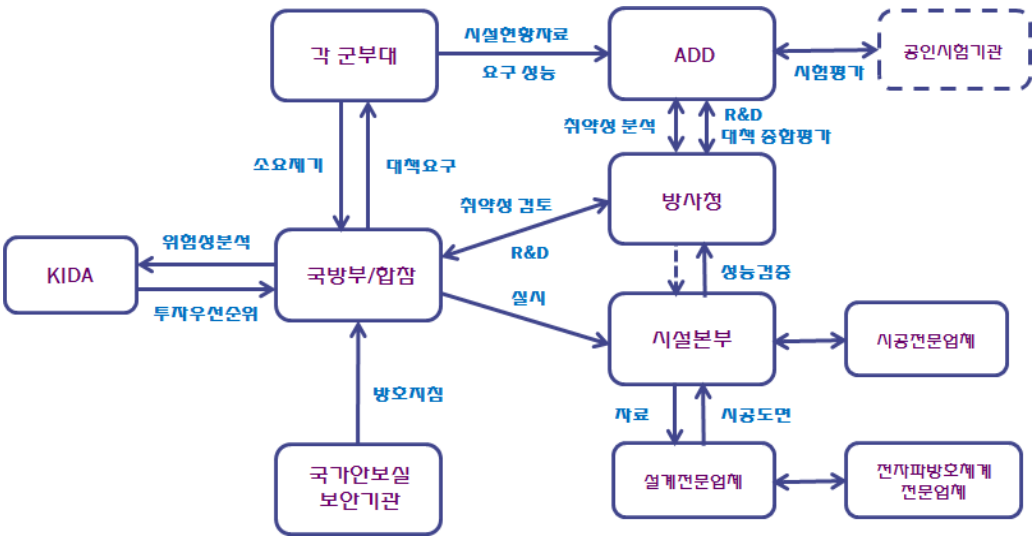
주요한 문제점은 고출력 전자기파 방호시설 구축사업이 건설 분야에 크게 치우쳐 진행되고 있다는 점이다. 고출력 전자기파 방호시설은 시설 내에서 운용되고 있는 체계 및 장비를 보호하기 위해 구축되며, 외부 전자기파에 의해 노출되는 위협 레벨과 장비와 체계가 견딜 수 있는 레벨의 차이를 시설에서 방호대책을 수립하는 것이다. 따라서 장비에서부터, 함체, 쉘터, 건물의 순서로 대책이 강구되어야 경제적 비용을 절감할 수 있다. 그러나 시설 내에서 운용되는 체계 및 장비에 대한 면밀한 분석이 없고, 체계 및 장비 운용자가 방호시설 성능 기준 작업에 참여하지 않는 등, 단순히 대규모 건설공사의 한 형태로 이루어지는 경향이 없지 않다. 또한 용접 방식의 전자파 차폐를 세부 시행 방법으로 규정하고 있어, 기존 건물 내부에서의 전자파 방호를 어렵게 하고 있음은 물론, 사용공간의 축소 등으로 인해 경제성이 크게 악화되고 있다.

방호시설의 성능 기준은 위협이 되는 외부 전자기

파 환경의 특성과 방호하고자 하는 체계 및 장비의 특성에 따라 다르게 적용되어야 한다. 그러나 우리 군에서 현재 적용하고 있는 "전자파 방호시설 설계 기준"은 미국의 군사규격, Mil-Std-188-125-1/2를 준용한 것으로서, 고 고도 핵 전자기파로부터 지상의 C^4I 체계의 보호를 목적으로 한다. 따라서 고출력 비핵 전자기파 및 TEMPEST(누설전자파에 의한 정보 유출) 위협에 대해 적용하고, 또한 C^4I 체계가 아닌 경우와 체계 내에 상용 기성품이 포함될 경우에 대해서도 현행 기준을 적용하는데 한계가 있다.

따라서 전자기파 방호체계를 이해하고 있는 조직 기본 설계 및 실시 설계에 반드시 참여하고, 시설 내에서 운용되는 체계 및 장비 운용자가 성능 기준 작업에 참여함으로써 보다 효과적인 방호시설 구축사업이 이루어질 것으로 판단한다. 이러한 현행 문제점을 보완하기 위해 필자가 동 세미나에서 제안한 추진 체계는 [그림 3]과 같다.

국가안보정책실이나 국군기무사에서 효과적인 방호지침을 마련하고, 국방부 및 합참에서는 방호지침에 따라 각 군 부대에 대책을 요구하거나, 또는 각 군 부대에서 제기되는 소요를 국방부 및 합참에서 모두 취합하여 국방연구원에서 위험성을 분석하고, 그 결과에 근거하여 투자 우선 순위를 결정한다. 필요한 경우, 국방부 및 합참은 방사청에 국방과학연으로 하여금 각 군부대의 시설현황자료를 바탕으로 취약성 검토를 실시하도록 한다(필요한 경우, 공인시험기관의 시험 평가 자료가 요구될 수 있다). 이러한 위험성 분석 및 취약성 평가·분석 자료에 근거하여 당장 실시가 가능한 분야는 시설본부가 주관하여 전자파 방호체계 전문 업체의 도움을 받아 설계 전문 업체에서 시공 도면을 작성하도록 하고, 연구 개발이 필요한 분야는 방사청으로 하여금 연구 개발을 추진하도록 한다. 제작된 설계도면을 시공 전문업체에 제공하여 효과적으로 시공토록 하고, 성능 검증은 방사청의 협조로 국방과학연(또는 국방기술품질원)이 주관하는 것이 바람직하다. 성능 검증은 몇 가지의 시험 검사로 이루어지는 것이 아니라, 취약성 검토 결과에 근거하여 종합적인 엔지니어링을 통해 완결되기 때문이다. 특히, 방호시설 구축사업은 "창과 방패" 개념에서 보안이 매우 중요하다. 각 군부대에서 제공되



[그림 3] 제안된 국방 전자파 방호시설 추진 체계(안)

는 시설현황 자료는 물론, 국방과학연에서 수행하는 취약성 분석 자료, 시설본부에서 주관하는 설계 도면 등에 관한 정보는 반드시 기밀 유지가 이루어져야 한다. 따라서 외부 민간기관의 도움을 최소로 하고, 가능한 한 국방 관련 기관 또는 정부 관련 기관에서 동 사업을 추진하는 것이 바람직하다.

3-2 공공 및 민간 분야

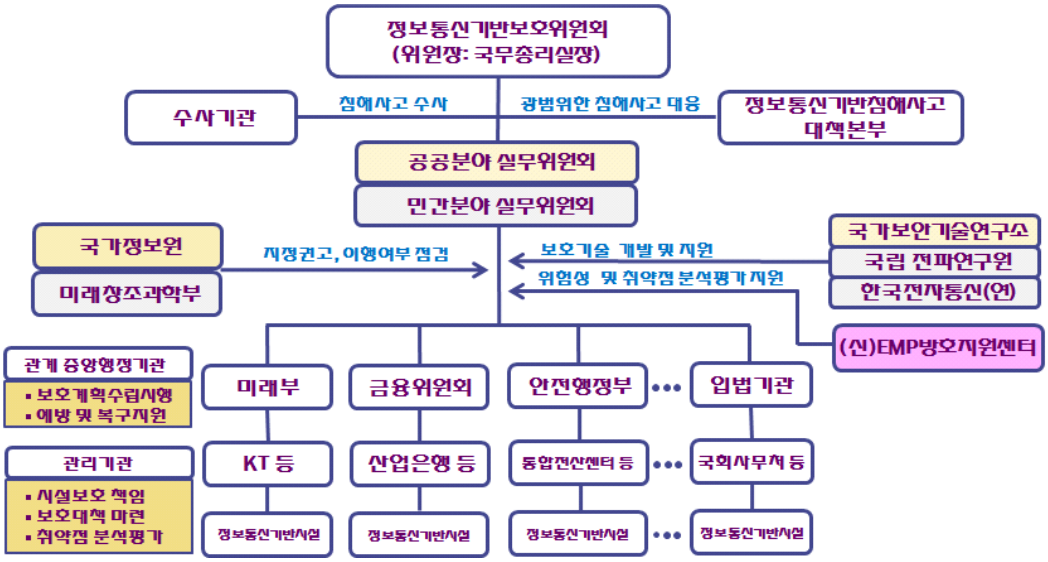
현행 정보통신기반보호법 등에서 고출력 전자기파에 대한 방호를 명시적으로 규정하고 있으나, 실제의 세부 규정에서는 악성 코드 유포, 해킹 등의 사이버 위협에 대해서만 규정하고 있다. 따라서 효과적인 고출력 전자기파 위협에 대한 대책을 위해서 다음과 같은 몇 가지의 관련 제도 개선 방안이 강구될 수 있을 것으로 판단한다.

- 현행 "주요 취약점 분석·평가기준"을 개정 보완하는 방안으로, 이 방안은 "정보통신기반보호법"의 개정 없이 현행 기준을 개정하여 고출력 전자기파 부분을 보완토록 함으로써 관련 제도의 조속한 시행이 가능하다는 장점이 있는 반면에, 현행 육안 검사 등으로 고출력 전자기파의 취약점을 분석·평가하는데 한계가 있다는 점과 관련 시험검사 및 엔지니어링 산업의 육성 근거가 미약하다는 단점이 있다.
- 현행 "정보통신기반보호법"을 개정하는 방안이다. 이 방안은 기존의 사이버 보안과 차별화된 내용의 제도화가 가능하고, 정보 보호, 산업 육성, 연구 개발 지원, 교육 홍보 강화 등을 제도에 포함시킬 수 있는 장점이 있는 반면에, 법률 개정을 위해 많은 절차나 협의가 요구될 수 있어 번거로울 수 있다는 단점이 있다.
- 현행 "재난 및 안전관리 기본법"을 개정하는 방안으로, 이 방안은 전력망 등, 국가 핵심기반 시설 전반에 대한 고출력 전자기파 방호를 실현할 수 있다는 장점이 있는 반면에, 많은 정부 부처 간의 업무 협조와 조정이 필요하여, 법률 개정에 큰 어려움이 예상되는 단점이 있다.
- 필자는 "주요 정보통신 기반 시설의 취약점 분석·평가기준"에 고출력 전자기파 항목을 추가 신설하여 고출력 전자기파 방호제도를 조속히 시행하는 것이 가능하지만, 근거 법령인 "정보통신기반보호법"이 사이버 보안을 중심으로 기술되어 있어 적용하는데 여러 가지 한계를 노출할 수 있다고 생각한다. 고출력 전자기파 보안은 사이버 보안과 적용기술이 상이하고, 방호대상도 명확히 구분되므로 규정 적용에 혼란을 일으킬 여지가 크다. 따라서 보다 적극적으로 정보통신기반보호법을 개정하여 기존의 사이버 보안과 차별화된 내용으로 제도화하고, 정보 보호, 산업 육성, 연구 개발 지원, 교육 홍보 강화 등에 관한 조항을 신설하는 것이 바람직한 것으로 판단된다.

따라서 이러한 개정된 "정보통신기반보호법"에 근거하여 별도의 "주요 (고출력 전자기파)의 취약점 분석·평가 기준"를 제정하여 시행하는 것이 효과적이다. 이는 현행 분석·평가 기준으로 고출력 전자기파 보안을 확립하는데 문제가 있고, 접근 방법에 있어서 근본적인 차이가 있으므로 두 분야를 분리하여 별도의 분석·평가 기준을 수립할 필요가 있기 때문이다.

정보통신기반보호법 개정(안)에 포함시켜야 할 효과적 추진 체계를 [그림 4]와 같이 제안한다. 현재의 국내 관련 기관의 현황과 활동을 살펴볼 때, 전문적인 설계 및 시공, 시험 검사 지원 등은 가능하다고 판단되지만, 종합적인 위험성 분석 및 취약점 분석·평가, 그리고 국가 핵심기반 시설의 주요 정보에 대한 기밀 유지 등을 위해 "(가칭)고출력 전자기파 방호 지원센터"의 설립은 필요하다.

또한 장기적으로는 "재난 및 안전관리 기본법"에 정의된 인적 재난의 범주에 고출력 전자기파를 국가적 재난의 한 유형으로 포함시켜 재난 관리의 전주기



[그림 4] 정보통신기반보호법 개정을 통한 효과적 고출력 전자기파 방호업무 추진 체계의 제안

과정(예방・대비・대응・복구)이 이루어질 수 있도록 하고, 구체적 제도 시행은 정보통신기반보호법에 근거하도록 규정할 필요가 있다. 이러한 추가적인 제도 외에도 국가위기관리기본지침에 근거한 “EMP 위기관리(표준, 실무) 매뉴얼”을 작성하여 유관기관에 배포, 활용토록 할 필요가 있다.

Ⅳ. 결 론

국제적으로 고출력 전자기파에 대한 위협은 국방분야에서 주로 다루어져 왔으나, 점차 민간 분야로 확대되고 있다. 현대의 국가 핵심기반 구조는 과거와 달리 포함된 시스템과 네트워크가 컴퓨터와 통신 수단을 이용하여 사회의 다른 부문과 상호 연계되어 있다. 따라서 이러한 상호 연계성은 전력 및 통신 기반시설과 같은 한 개별 부문에서의 고장 영향이 사회 전반으로 파급되어 큰 혼란을 일으킬 수 있다. 개별 부문에서의 고장은 자연 재해는 물론, 사이버 위협 및 물리적 위협으로부터 발생하며, 이러한 물리적 위협에 고 고도 핵 전자기파 및 고출력 비핵 전자기파에 의한 위협이 포함된다.

고출력 전자기파 방호는 “국가핵심기반 시설 방호” 개념에서 다루어지고 있으며, 위험성 분석 및 취약점 평가・분석에 근거하여 투자 우선 순위가 결정되고 있다. 국가의 핵심 기반 시설 중에서 전력망, 정보통신망이 가장 취약하고, 따라서 이 분야 투자가 우선 이루어지고 있는 것으로 파악된다. 우리나라의 고출력 전자기파에 대한 방호제도화는 현행 “주요 취약점 분석・평가 기준”을 개정하여 고출력 전자기파 항목을 추가하면 제도 시행은 가능할 것으로 생각된다. 그러나 현행 정보통신기반보호법 및 하위 법령이 사이버 보안을 중심으로 규정되어 “정보 보호” 개념을 “고출력 전자기파 방호” 개념으로 확대시킬 수 있는지는 의문이다. 따라서 현행 “정보통신기반보호법”을 개정하여 고출력 전자기파 관련 사항을 추가, 보완하는 것이 바람직한 것으로 판단된다.

현행 “정보통신기반보호법”의 개정과 관련하여 주요하게 검토되어야 할 사항은 다음과 같다.

・현행 정보통신기반보호법은 사이버 보안을 중심으로 규정되어 있고, 또한 고출력 전자기파 방호는 적

용 기술과 적용 범위가 구분될 수 있으므로, 법 규정에서의 혼돈을 개선할 필요가 있다.

- 주요 에 대한 전자기적 침해행위에서 주요 중 고출력 전자기파 평가 대상을 지정하고, 취약점을 분석 평가하는 사항
- 위험성 분석 및 취약성 평가·분석의 효율성과 보안성을 제고하기 위해 “(가칭)고출력 전자기파 방호지원센터”를 신설하는 사항
- 고출력 전자기파에 대한 취약점 평가 대상 의 물리적 정보 및 전담반에 의한 정보 유출방지 사항
- 고출력 전자기파 침해방지기술 개발과 관련한 정부의 인력 양성과 연구 개발 지원 규정의 신설
- 신설된 규정에 따른 시행령 규정 보완

근래에 들어 국제적으로 고출력 전자기파는 국가의 존망을 위협하는 재난으로 인식되고 있다. 북의 핵 위협이 엄연히 존재하는 우리나라의 상황에서 국가의 핵심기반 시설을 고출력 전자기파 위협으로부터 보호해야 함은 명확하다. 따라서 정부는 관계법령을 정비하고, 나아가서 고출력 전자기파 재난에 의한 피해 예방을 위한 “상황관리체계”를 구축하고, 국가위기관리기본지침에 근거하여, “고출력 전자기파 위기관리(표준, 실무) 매뉴얼”을 작성하여 유관기관에 배포, 활용토록 할 필요가 있다.

참 고 문 헌

[1] EMP Commission, "Report of the commission to assess the threat to the United States from electromagnetic pulse (EMP) attack", Volume 1: Executive Report, 2004.

[2] EMP Commission, "Report of the commission to assess the threat to the United States from electromagnetic pulse (EMP) attack, critical national infrastructures", 2004. 4.

[3] J. D. Moteff, "Critical infrastructures: Background, policy and implementation", RL30153, *CRS Report for Congress*, Jul. 2011.

[4] G. W. Bush, "The national strategy for the physical protection of critical infrastructures and key assets", Washington D.C., The White House, Feb. 2003.

[5] M. Chertoff, "National infrastructure protection plan", Dept. of Homeland Security, 2009.

[6] R.T. Marsh, "Critical foundations; Protecting America’s infrastructures", *The President’s Commission on Critical Infrastructure Protection*, Oct. 1997.

[7] NFPA 1600, *Standard on Disaster/Emergency Management and Business Continuity Programs*, National Fire Protection Association, 2007.

[8] Dept. of Homeland Security, "Communications sector-specific plan, an annex to the national infrastructure protection lan", 2010.

[9] Homeland Security Digital Library, "EMP threat: Examining the consequences", U. S. House of Representatives, Sep. 12, 2012.

[10] House of Commons Defense Committee, "Developing threats: Electro-magnetic pulses (EMP)", HC 1552, *Tenth Report of Session 2010-12*, Feb. 2012.

[11] GOST R 52863-2007, Protection of the Information. Protective automatically systems. Testing for stability to intentional power electromagnetic influence. General requirements, Jul. 2008.

[12] 정연춘, "고출력 전자기파 방호정책 동향", 2014 방호시설 발전세미나, 국방시설본부, pp. 3-10, 2013년 11월.

≡ 필자소개 ≡

정 연 춘

1984년 2월: 경북대학교 물리학과 (이학사)
1986년 2월: 경북대학교 물리학과 (이학석사)
1999년 8월: 충남대학교 전자공학과 (공학박사)
1985년 12월~2001년 5월: 한국표준과학연구원 전자기환경그룹 그룹장, 책임연구원
2000년 3월~2001년 2월: Univ. of York, Visiting Academics
2001년 6월~2002년 2월: (주)익스팬전자 중앙연구소장
2002년 2월~현재: 서경대학교 전자공학과 교수
[주 관심분야] EMI/EMC 측정 및 대책 기술, 전자파 재료