THE JOURNAL OF KOREAN INSTITUTE OF ELECTROMAGNETIC ENGINEERING AND SCIENCE. 2013 Aug.; 24(8), 781～790.

http://dx.doi.org/10.5515/KJKIEES.2013.24.8.781
ISSN 1226-3133 (Print) · ISSN 2288-226X (Online)

고출력 전자기파 방호 제도 도입에 관한 연구

A Study on the Introduction of Legal EMP Protection System

정 연 춘

Yeon-Choon Chung

요 약

현대의 국가 핵심 기반 시설은 국제적으로 위협이 증대되고 있는 고출력 전자기파에 대해 매우 취약한 것으로 알려져 있다. 우리나라의 관계 법령에서는 주로 사이버 위협에 대해서만 다루고 있어, 고출력 전자기파 위협에 대해서는 세부시행 관련 규정이 미흡하여 현실적인 대책이 이루어지지 않고 있다. 본 논문에서는 고출력 전자기파 관련 제도의 국내, 외 동향을 살펴보고, 우리나라의 현행 관련 법령의 개정 방향과 구체적으로 법령에 담아야 할 내용에 대해 제안하였다. 그 중에서도 현행 「정보통신기반보호법」을 개정하여, 기밀정보의 보호, 산업육성, 연구 개발 지원, 교육 홍보 강화 등을 포함시키는 방안이 가장 효과적인 것으로 판단된다. 아무튼 본 논문이 우리나라의 효과적인 고출력 전자기파 방호 제도 도입에 도움이 되기를 기대한다.

Abstract

Nowadays, national critical infrastructures have been known to be highly vulnerable to the EMP threats which are internationally growing. But their realistic solutions have been not made by the lack of detailed rules and regulations in current laws, however, which cover most of cyber threats. This paper takes a look at the domestic and overseas trends on the EMP protections, and proposes the revision directives of relevant laws and the contents included into the proposed legislation. Among them, the amendment of the current "Information Infrastructure Protection Act" is considered to be the most effective, including provisions on protected informations, industrial promotions, R&D supports, education, etc. Anyway, this paper is expected to be helpful for introducing an effective legal scheme on the CIP against EMP threats. domestic rule.

Key words : CIP(Critical Infrastructure Protection), EMP Threats, Legal Requirements

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 사회기반구조를 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.

이러한 개별 부문에서의 고장은 자연 재해 및 인

서경대학교 전자공학과(Department of Electronics, Seokyeong University)
· Manuscript received June 17, 2013 ; Revised July 22, 2013 ; Accepted July 23, 2013. (ID No. 20130617-10S)
· Corresponding Author : Yeon-Choon Chung (e-mail : ycchung@skuniv.ac.kr)

적 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.

미국은 물론, 유럽연합 등에서 고출력 전자기파를 국가 안보를 위협하는 대상의 하나로 인식하고, 이에 대한 방호 대책을 강구하고 있다. 우리나라에서도 시급하게 대응책을 마련하고 있으나, 대부분의 법령에서 악성 코드 유포, 해킹 등의 사이버 위협에 대해서만 규정하고 있고, 고출력 전자기파 위협에 대한 규정은 마련되어 있지 않다. 따라서 고출력 전자기파에 대한 위협은 증대되고 있으나, 국가 중요시설에 대한 방호는 관련 법령이 미흡하여 효과적으로 이루어지고 있지 않다.

본 논문에서는 고출력 전자기파에 대한 방호 대책을 위해 필요한 제도의 수립을 위한 제도화 방안을 제안한다. 먼저 외국의 관련 제도를 살펴보고, 우리나라의 현행 관련 법령의 개정 방향과 구체적으로 법령에 담아야 할 내용에 대해 제안하고자 한다. 아무튼 본 논문이 우리나라의 효과적인 고출력 전자기파 방호 제도 도입에 도움이 되기를 기대한다.

Ⅱ. 국내외 관련 법규 분석

2-1 국내 관련 법규 분석

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 정보 통신기반시설로 지정되어 관리되고 있다.

동 법 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.

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

이러한 "주요 정보통신 기반시설 취약점 분석·평가기준"은 악성코드 유포, 해킹 등 사이버 위협에 대한 주요 정보통신 기반시설의 취약점을 종합적으로 분석 및 평가·개선하는 일련의 과정을 규정하고 있으나, 고출력 전자기파에 대한 부분은 평가항목에서 포함되어 있지 않다. 따라서 관련 취약점 분석·평가기준에 고출력 전자기파와 관련된 구체적 내용과 절차를 추가함으로써 비교적 쉽게 빨리 고출력 전자기파에 대한 주요 정보통신 기반시설의 방호를 실현할 수 있을 것으로 판단된다. 그러나 현행 분석·평가기준이 너무 사이버 보안에 치우쳐 있고, 사이버 보안과 고출력 전자기파 보안에 적용되는 전문기술도 많이 상이하므로, 별도의 분석·평가기준을 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 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 국가경제

에 심각한 영향을 미칠 수 있는 물적·인적 체계로서 지속적으로 관리할 필요가 있다고 인정되는 시설을 동 법 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 정보통신시설은 주요 정보통신 기반시설로도 중복 지정되어 있다.

동 법에서 정의하고 있는 "재난"에는 태풍·홍수·가뭄·지진·낙뢰·황사·적조 등과 같은 자연현상으로 인해 발생되는 재해는 물론, 화재·붕괴·화생방 사고·환경 오염 사고 등과 같은 일정규모 이상의 피해, 감염병 및 가축전염병 확산으로 인한 피해를 비롯하여, 에너지·통신·교통·금융·의료·수도 등 국가기반 체계의 마비를 포함하고 있다. 동 법 및 시행령에는 자연재해 및 인적 재난에 대한 예방조치, 안전점검 및 조치, 응급조치 및 구조, 복구, 보상 등을 규정하고 있으며, 동 법에 근거하여 국무총리는 "국가안전관리기본계획"의 수립 지침을 작성하여야 하고, 안전행정부장관은 "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 개정되어 고출력 전자기파에 대한 포괄적인 방호 대책 수립이 이루어져야 할 것으로 판단한다.

2-1-3 전파법 개정안

방송통신위원회에서는 전파법을 일부 개정하여 "고출력·누설 전자파 안전성 평가제도"를 신설하는 것을 입법 예고한 바 있는데, 현재는 정부 조직 개편에 따라 미래창조과학부가 담당하고 있다. 개정 법률의 목적은 방호 차폐 시설 또는 장비 보호 시설 등에 대한 안전성 평가를 실시할 수 있는 근거를 마련하고, 미래창조과학부는 안전성 평가 결과가 미흡한 경우 대책을 강구하도록 권고할 수 있도록 하며, 안전성 평가기준·방법 등의 고시 마련 및 수수료 납부 근거를 마련하는 것으로 되어 있다.

그러나 이러한 개정 법률안이 통과되면 방호 차폐시설과 장비 보호시설의 평가와 관련된 기술표준과 안전성 평가기관 등의 제도적 문제가 보완될 것으로 기대되지만, 평가 대상시설에 대한 규정이 법적으로 명확히 뒷받침되지 않아, 법령 시행의 실효성이 의문된다. 특히, 적용기준은 대상 시설의 목적과 설치 환경 등을 종합적으로 고려하여 판단해야 함에도 불구하고, 획일적으로 규정하는 것은 바람직하지 않다. 현재 정보통신기반보호법 및 전파법의 소관 부처가 일원화됨에 따라 포괄적인 보호 규정은 정보통신기반보호법에서 다루고, 전파법에서는 안전성 평가와 관련한 규정을 분리해서 담는 것이 바람직한 것으로 판단된다.

2-1-4 기타

"정보통신망 이용촉진 및 정보보호 등에 관한 법률"에도 고출력 전자기파에 의한 침해 사고를 정의하고 있으나, 정보통신망의 안정성을 확보하기 위해 필요한 구체적인 절차 등은 마련되어 있지 않다. 침해사고의 대응을 위해 한국인터넷진흥원이 침해사고에 관한 정보의 수집·전파, 침해사고의 예보·경보, 침해 사고에 대한 긴급조치 등에 관한 업무를 담당하여 수행하도록 하고 있다. 그러나 대부분 정보보호 업무와 관련되어 있고, 고출력 전자기파 침해 방지와 관련한 업무는 전혀 이루어지지 않고 있는 실정이다.

또한 국제적으로 전력망 보호는 국가 기반시설의 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. 특히, "지능형 전력망의 구축 및 이용촉진에 관한 법률"에서는 「정보통신기반 보호법」 제2조 제2호에 따른 전자적 침해행위의 방지 및 대응을 위한 정보보호시스템

의 설치 · 운영 등 기술적 · 물리적 보호조치에 대해 규정하고 있다. 그러나 관련 세부 기술기준은 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 외국의 관련 법규 분석

2-2-1 미국

미국은 핵심 기반 시설(critical infrastructure)을 포함한 심각한 사고의 대비와 대응과 관련한 개념을 CIP(Critical Infrastructure Protection)라 부르며, 국가의 중요 책무로 여기고 있다. 여기에서, 핵심 기반시설은 고도로 상호 의존적으로 함께 작동하는 인적 자산, 물리적 시스템, 사이버 시스템을 포함한다[1]. 1998년 5월에 클린턴 대통령의 행정명령(Presidential Decision Directive) PDD-63[2]에 따라 CIP에 대한 구체적인 조치가 강구되었는데, 그 당시에는 주로 사이버 위협이 주요 관심사였다. 그러나 2001년 911 테러를 겪은 후, 2003년 12월에 부시 대통령에 의한 국토 안보 행정 명령(Homeland Security Presidential Directive) HSPD-7[3]에서 물리적 위협에 대한 보안을 포함한 보다 강화된 CIP 개념을 수립 시행하고 있다[4],[5].

2007년 5월에 국토안보부는 HSPD-7에 따라 국가의 핵심기반과 주요 자원(CIKR: Critical Infrastructure and Key Resource)에 대한 국가기반시설 보증 계획(NIPP: National Infrastructure Assurance Plan)을 수립하도록 하였다[6]. 현재 표 1에 보인 것처럼 8개 부처 18개 부문에서 수행할 특별방호 계획(SSP: sector specific plan)을 각각 제정하여 시행하고 있다.

각 부문의 특별방호 계획에는 대개 다음과 같은 내용을 포함한다:

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

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.

미국은 국가 핵심 기반시설 방호에 관한 대통령자

표 1. 미 정부 부처별 담당 국가 핵심기반시설
Table 1. The American sector specific agencies and critical infrastructure and key resources.

정부부처	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 공중보건
내무부	· 국가 기념물 및 상징물
재무부	· 은행 및 재정
환경보호청[b)]	· 음용수 및 정수처리체계
국토안보부	
기반시설보호사무국[c)]	· 상업시설 · 기반제조시설 · 응급서비스 · 원자로, 핵연료, 핵폐기물 · 댐 · 화학
사이버보안 및 통신사무국[d)]	· 정보기술 · 통신
수송안전관리청[e)]	· 우편 및 해운
수송안전관리청 및 연안경비대[f)]	· 수송체계
연방방호서비스국[g)]	· 정부시설

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

문위원회 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 1600[7]에서는 고출력 전자기파와 지자기 폭풍을 인적 재난 및 자연재난으로 분류하고 있으며, 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.

특히, 미국은 1963년에 쿠바의 미사일 위기와 같은 국가적 재난에 대비하기 위해 47 CFR 215, “Federal Government focal point for electro magnetic pulse (EMP) information”에 근거하여 NS(National Security) 및 EP(Emergency Prepareness)를 담당하는 NCS(National Communications System)를 설립하였으며, 2012년 8월에 NCS가 폐지되고, 그 기능이 국토안보부 산하의 재난통신사무국(Office of Emergency Communications)으로 이관되어 고출력 전자기파를 포함한 국토 안보 업무가 모두 국토안보부로 집중되었다.

2010년에 입안되어 상원에서 자동 폐기된 Grid Act[HR 5026]에 포함된 사이버 보안을 제외하고, 핵, 비핵, 지자기 폭풍에 의한 고출력 전자기파 보안으로 대상을 축소한 일명 방패법(안), SHIELD(Secure High-voltage Infrastructure for Electricity from Lethal Damage) Act, HR 668[8]를 2011년 2월에 상정하여 심의 중에 있다. Grid Act에서 관할권 및 비상시국에서의 신뢰성 표준 신속처리 등의 문제[9]로 반대했던 연방전기신뢰성위원회(FERC: Federal Electric Reliability Commission)가 지지함에 따라 곧 가결될 것으로 기대한다.

SHIELD Act는 의회의 EMP 위원회 보고서에 근거하여 기존의 Federal Power Act, Part 2, Section 215 뒤에 새로운 Section 215A를 추가하는 개정 법률(안)으로서 제안된 Section 215A의 내용은 다음과 같다.

(a) 용어의 정의
(b) 비상대응수단
  (1) 전력망 보안 위협 대책 권한
  (2) 의회 통지
  (3) 협의
  (4) 적용
  (5) 중지
  (6) 비용 보전
(c) 전력망 보안 취약성 대책 수단
  (1) 위원회 권한
  (2) 철회
  (3) 지자기 폭풍과 고출력 전자기파
  (4) 대용량 변압기 입수 가능성
(d) 방호에 치명적인 시설
  (1) 지정
  (2) 위원회 권한
  (3) 비용 보전
(e) 정보 보호
  (1) 보호 정보의 공개 금지
  (2) 정보 공유
  (3) 정보의 의회 제출
  (4) 비보호 정보의 공개
  (5) 지정 기간
  (6) 지정의 취소
  (7) 지정의 사법적 검토
(f) 사법적 검토
(g) 전력망 보안 방호 요구 산업체 지원 규정
  (1) 전문지식과 자원
  (2) 전문지식의 공유
  (3) 보안 증명과 통신
(h) 특정 연방 독립체

위의 방패법의 주요 내용에는 다음과 같은 사항이 포함되어 있다.

- 위원회는 고출력 전자기파의 위협이 예상되어 전기 기반시설의 보안이 시급할 때 비상대응책을 수립, 시행하여야 한다.
- 전기 에너지의 발전, 송전, 배전과 관련한 전기 기반시설의 소유자, 운영자, 사용자는 비상대응책에 따라 대책을 수립해야 한다.
- 국가적으로 방호가 필요하다고 판단되는 주요

시설은 대상 시설로 지정되며, 반드시 비상대응책에 따라 대책을 수립해야 한다.
- 전기기반시설의 소유자, 운영자, 사용자가 수립한 대책의 신뢰성에 문제가 있을 때, 위원회는 비상대응책의 실시를 요구할 수 있다.
- 전기기반시설의 소유자, 운영자, 사용자는 개별적으로 또는 연합하여 대용량 변압기를 비축하여 조기에 복구가 될 수 있도록 해야 한다.
- 대책 수립에 감당하기 어려운 정도의 과도한 비용이 들어갈 경우, 위원회는 비용 복구 방안을 강구해야 한다.
- 고출력 전자기파 방호 대책과 관련한 보호 정보는 지정되어 일정기간 공개 금지되어야 하며, 비보호 정보는 관련 기관 간의 정보 공유를 촉진하여 원활한 방호가 이루어질 수 있도록 해야 한다.

2-2-2 유럽연합

유럽연합도 “New European Approaches to Counter Terrorism” 보고서를 통해 대테러 방안에 고출력 전자기파 방호를 포함시켰으며, 2006년에 EU COM (2006) 786에 따라 핵심 기반시설 방호를 위한 유럽 프로그램(EPCIP: European Program for Critical Infrastructure Protection)을 회원국의 법령으로 채택하도록 하였다. 또한, 유럽연합에서는 2012년 7월부터 2015년 6월까지 3년 동안 12개의 산업체와 대학이 공동으로 STRUCTURES 라는 제목의 유럽 공동 프로젝트를 추진하고 있다. STRUCTURES라는 명칭은 Strategies for The impRovement of critical infrastrUCTUre Resilience to Electro magnetic attackS의 약어로 부르는 용어이다. 프로젝트는 의도성 전자파장해(고출력 비핵 전자기파) 관련 연구를 공동 수행하고, 핵심기반시설에 대한 위해도 분석, 방호 및 탐지, 최종 사용자 및 정책 입안자를 위한 가이드 라인 제공, 프로젝트 수행동안 최종 사용자와의 긴밀한 협력을 목적으로 하고 있다.

특히, 영국에서는 2012년 2월에 하원 국방위원회에서 “Developing Threats: Electro-Magnetic Pulses (EMP)”라는 제목의 보고서[10]를 출간하였는데, 고고도 핵 전자기파와 고출력 비핵 전자기파, 지자기 폭풍에 대한 위협이 대두되고 있으며, 국가 핵심 기반시설에 대한 방호, 특히 전력망에 대한 고출력 전자기파 방호를 강조하고 있다. 또한, 2012년 12월에 재무부에서 국가 기반시설 방호 계획을 보완하여 발간한 바 있다.

2-2-3 러시아

러시아에서는 2007년에 기존의 정보보호 관련 규정, GOST R 50922 및 51275 규격에 추가하여 고출력 비핵 전자기파(의도성 전자파장해)에 대한 자동화 시스템의 보호를 위한 GOST R 52863 규격[11]을 발표한 바 있다. 이 규격은 다음과 같은 6개의 절과 6개의 부속절로 이루어져 있다.

1) 범주
2) 참조 기준
3) 정의 및 약어
4) 의도성 전자파 장해에 대한 안정성 요구사항
5) 시험 강성도(degree of stiffness)
6) 방호 자동화시스템에 대한 요구사항

A-1) 방호 자동화 시스템의 동작조건 분류의 정량적 특성
2) 의도성 전자파 장해 모의장치의 주요 특성에 대한 요구사항
3) 의도성 전자파 장해 모의장치의 통신/감결합 기기의 주요 특성
4) 시험 절차
5) 의도성 전자파 장해 시험 패턴
6) 평가 판단기준

2-2-4 기타

노르웨이는 NORFO SL 238 & 239 규격을 적용하고 있고, 일본에서는 신정보시큐리티기술연구회(IST: Information Security Technology study group)에서 작성한 “전자파 시큐리티 가이드라인”을 적용하고 있다.

Ⅲ. 취약성 및 리스크 평가 기법

리스크(risk) 관리의 중요성은 미국의 911 테러와

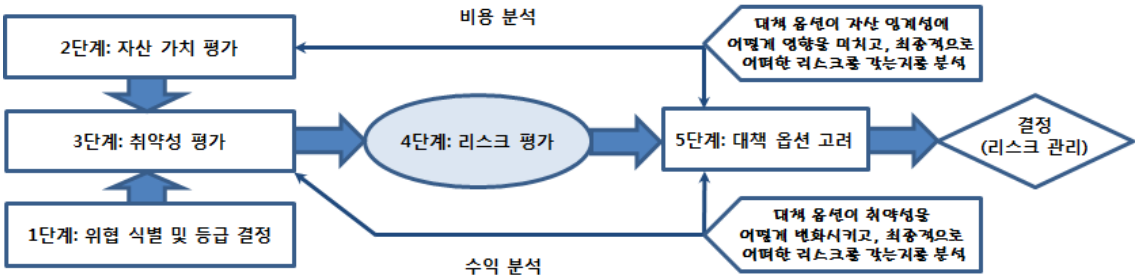

그림 1. FEMA 452에 근거한 리스크 평가 과정
Fig. 1. Risk assessment process model by FEMA 452.

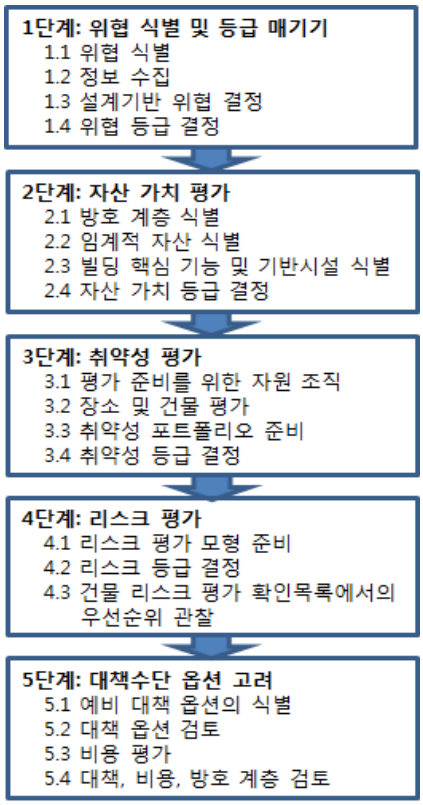

그림 2. FEMA 452에 근거한 리스크 평가과정의 각 단계별 세부 과업
Fig. 2. Steps and their tasks based on FEMA 452.

허리케인 카트리나 이후에 크게 부각되었다. 911 테러와 같은 사건은 극히 예외적이고, 잘 알려져 있지도 않았으며, 발생 가능성도 낮았지만 일단 발생되고 나면 엄청난 파급 효과를 초래한다. 이러한 리스크 평가는 시스템 임계성(criticality)은 물론, 작동하는 위협, 시스템의 취약성을 평가하는 과정을 포함한다.

리스크란 ISO Guide 73-2009에 의해 “목적 실현에 대한 불확실한 영향”으로 정의된다. 이러한 리스크 관리의 대표적인 규격은 ISO 31000인데, 효과적인 리스크 관리를 위한 원칙 수립, 리스크 관리를 위한 경영 프로세스 수립, 조직이 운영 중인 관리 프로세스와의 연동을 위한 프레임웍 제공을 목적으로 하며, 다양한 형태의 조직에서 효과적인 리스크 관리를 위해 범용으로 적용되고 있다. 리스크 관리의 기본 프로세스는 “의사소통과 자문” 및 “모니터링과 검토”를 통해서, 상황을 설정하고, 리스크를 식별하며, 리스크를 분석하고, 리스크를 평가하며, 리스크를 처리하는 과정이다.

“건물에 대한 테러 공격을 어떻게 완화시킬 수 있는가”를 정리한 FEMA 452 가이드[12]에 근거한 고출력 전자기파 위협에 대한 리스크 평가 절차는 그림 1과 같으며, 그림 2에 각 단계에서 이루어져야 하는 세부 과업을 보였다. 이러한 가이드는 고출력 전자기파 방호와 관련하여 리스크 관리에 유용하게 활용될 수 있을 것으로 판단하며, 본 논문도 이러한 과정에 근거하였다.

3-1 취약성 분석 방법

고출력 전자기파 위협은 지상 30 km 이상의 고도에서의 핵폭발에 의해 발생하는 고 고도 핵 전자기파와 E-bomb을 비롯한 고출력 전자파 테러 등에 의한 고 출력 비핵 전자기파로 구분되며, 위협의 공간적인 커버리지, 노출 전계강도, 전송선로로의 유기전류, 시간 영역 특성, 주파수 스펙트럼 등에서 차이가 있다. 즉, 고 고도 핵 전자기파는 매우 넓은 지역,

우리나라로 볼 때 범국가적인 문제인 반면에, 고출력 비핵 전자기파는 전자기적 무기가 동작하는 위치(지상 또는 저 고도)에 따라 영향 범위가 다르지만 제한된 지역의 문제이다.

특히, 위협의 세부적인 특성은 방호하고자 하는 체계의 취약성을 평가하는데 중요한 요소이며, 보다 엄밀한 자료의 수집이 요구된다. 고 고도 핵 전자기파의 특성은 군사규격 Mil-Std-2169에 상세하게 기술되어 있는 것으로 알려져 있으나, 비밀문서로 분류되어 공개되고 있지 않다. 공개된 자료로서 고 고도 핵 전자기파의 복사 특성에 대한 IEC 61000-2-9 규격, 고 고도 핵 전자기파의 전도 특성에 대한 IEC 61-000-2-10 규격, 고출력 비핵 전자기파의 환경 분류에 대한 IEC 61000-2-11 규격, 고출력 비핵 전자기파의 복사 및 전도 특성에 대한 IEC 61000-2-13 규격이 중요한 참고자료로 활용될 수 있다. 반면에 비핵 전자기파 발생장치는 지속적으로 소형화되고, 고출력화되고 있으므로 관련 국제학술회의 및 학술저널 등에 발표되는 논문을 추적하여 최신 정보를 확보해야 한다.

특히, 고출력 비핵 전자기파 발생장치는 종류가 다양하고 소형이므로 취약성 평가에도 세부적인 분석이 요구된다. 먼저 고출력 전자기파 발생장치를 1) 위협 레벨, 2) 이동성(mobility), 3) 기술 수준(technological challenge)으로 분류되며, 독일의 F. Sabath 등이 제시한 모델[13]이 유용하게 활용될 수 있다. 다음으로 방호하고자 하는 시설은 1) 수용성(receptivity), 2) 민감도(sensitivity), 3) 잉여성(redundancy)을 고려하여 분류될 수 있는데, 스웨덴의 D. Månsson 등이 제시한 모델[14]이 유용하게 활용될 수 있을 것으로 판단한다. 최종적으로 이러한 위협요인과 방호시설의 특성을 고려하여 실제 위협이 가해졌을 때의 결과를 방호시설 자체 손상은 물론, 연계된 다른 부문으로의 피해 파급성을 고려하여 판단해야 한다.

3-2 리스크 평가 방법

미국의 Sandia National Laboratories에서 물리적 보안에 대해 다음과 같은 리스크 평가 방법을 제안한 바 있다[15].

$$Risk = C \times P_A \times (1-P_E) \quad (1)$$

여기에서, C는 공격에 따른 손실 결과, P_A는 악의적인 공격 가능성, P_E는 보안시스템의 유효성, 즉 $(1-P_E)$는 악의적 공격의 성공 가능성이다. 또한, 미국의 의회 연구소 보고서[16]에 의하면 기대 손실(expected loss)은 다음과 같이 평가될 수 있다.

$$Expected\ loss = C \times P_A \times P_B \times P_C \quad (2)$$

여기에서, C는 공격에 따른 손실 결과, P_A는 공격이 일어날 확률, P_B는 공격자가 해당 위협을 사용할 조건 확률, P_C 는 해당 공격이 성공할 조건 확률이다. 실제 이러한 리스크 평가를 통해 방호 시설의 투자 우선순위를 정하는데 활용하고 있다.

C. Manto의 보고서[17]에 따르면 미국의 볼티모어-워싱턴-리치몬드 지역을 대상으로 고 고도 핵 전자기파에 의한 경제적 손실을 평가하였는데, 전력시설과 통신시설의 피해가 가장 심각하고, 따라서 전력망과 통신망의 복구 정도에 따라 피해 규모는 달라지는 것으로 판단하였다. 이러한 피해는 직접적인 피해는 물론, 정전으로 인해 파급되는 간접적인 피해, 예를 들면, 음식품의 손상, 생산 중단에 따른 손해, 초과 근무에 따른 임금 등을 포함한 비용이며, 미국 인구의 1/7 정도 이상이 이와 관련된 비용의 부담이 발생될 것으로 예상하고 있다. 평가된 누적 피해규모는 약 342억 달러에서 최악 7,708억 달러, 복구기간은 4개월에서 최악 33개월 정도 소요되는 것으로 추산하였으며, 사전에 방호 대책을 수립하면 피해 규모를 약 90억 달러에서 최악 5,860억 달러 정도로 줄일 수 있는 것으로 예상하고 있다.

Ⅳ. 국내 제도 도입 방안 및 결론

현대의 국가 핵심 기반구조는 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.

미국과 유럽연합 등에서 고출력 전자기파를 국가 안보를 위협하는 대상의 하나로 인식하여, 관련 방호 대책에 관한 법령제도를 마련하고 있다. 우리나라에서도 정보통신기반보호법 등에서 관련 규정을 포함하고 있으나, 악성 코드 유포, 해킹 등의 사이버 위협에 대해서만 규정하고 있고, 고출력 전자기파 위협에 대해서는 세부시행 관련 규정이 미흡하여 현실적인 대책이 이루어지지 않고 있다.

본 논문에서는 고출력 전자기파에 대한 효과적인 방호 대책을 위해 먼저 적절한 제도의 수립 및 시행이 필요하다고 인식하고, 관련 제도의 국내, 외 동향을 살펴보고, 우리나라의 현행 관련 법령의 개정 방향과 구체적으로 법령에 담아야 할 내용에 대해 제안한다. 고출력 전자기파에 대한 우리나라의 국가 핵심 기반시설의 방호를 위해서 몇 가지 관련 현행 법령의 개선 방안을 다음과 같이 제안하고자 한다:

- 현행 「주요정보통신기반시설 취약점 분석·평가기준」을 개정 보완하는 방안. 이 방안은 「정보통신기반보호법」의 개정 없이 현행 기준을 개정하여 고출력 전자기파 부분을 보완토록 함으로써 관련 제도의 조속한 시행이 가능하다는 장점이 있는 반면에, 현행 육안검사 등으로 고출력 전자기파의 취약점을 분석·평가하는데 한계가 있다는 점과 관련 시험검사 및 엔지니어링 산업의 육성 근거가 미약하다는 단점이 있다.
- 현행 「정보통신기반보호법」을 개정하는 방안. 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 방안이다. 이 방안은 전력망 등, 국가 핵심 기반시설 전반에 대한 고출력 전자기파 방호를 실현할 수 있다는 장점이 있는 반면에, 많은 정부부처 간의 업무 협조와 조정이 필요하여 법률 개정에 큰 어려움이 예상되는 단점이 있다.

이러한 방안 중에서 현행 「정보통신기반보호법」을 개정하여 필요한 절차 및 제도를 포함하는 것이 고출력 전자기파 방호 제도 도입에 가장 효과적이라 판단된다.

본 논문에서는 국제적으로 고출력 전자기파의 위협이 증대되고 있음을 인식하고, 국가 핵심 기반시설의 고출력 전자기파에 대한 방호를 위해 관련 국내, 외 제도를 살펴보았다. 또한, 외국의 국가 핵심 기반시설 방호 업무의 큰 틀을 이해하고, 구체적 시행 절차 등을 검토하여, 우리나라의 현행 관련 법령의 개정 방향과 구체적으로 법령에 담아야 할 내용에 대해 검토하였다. 아무튼 본 논문이 우리나라의 효과적인 고출력 전자기파 방호 제도 도입에 도움이 되기를 기대한다.

References

[1] Robert T. Marsh, "Critical foundations; protecting America's infrastructures", *The President's Commission on Critical Infrastructure Protection*, Oct. 1997.

[2] Presidential Decision Directive PDD-63 (http://www.fas.org/irp/offdocs/pdd/pdd-63.htm).

[3] Homeland Security Presidential Directive HSPD-7 (http://georgewbush-whitehouse.archives.gov/news/releases/2003/12/20031217-5.html).

[4] John D. Moteff, "Critical infrastructures: background, policy, and implementation", *RL30153*, *CRS Report for Congress*, Jul. 2011.

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

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

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

[8] H. R. 668, "Secure high-voltage infrastructure for electricity from lethal damage act", *112th Congress 1st Session*, Feb. 2011.

[9] Homeland Security Digital Library, "EMP threat: Examining the consequences", *U. S. House of Representatives*, Sep. 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] FEMA 452, *Risk Assessment*, *A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings*, Federal Emergency Management Agency, Jan. 2005.

[13] F. Sabath, H. Garbe, "Risk potential of radiated HPEM environments", *Proc. of IEEE EMC Symp.*, Austin TX, pp. 226-231, Aug. 2009.

[14] D. Månsson, R. Thottappillil, and M. Bäckström, "Methodology for classifying facilities with respect to intentinal EMI", *IEEE Trans. Electromagn. Compat.*, vol. 51, no. 1, pp. 46-52, Feb. 2009.

[15] John D. Moteff, "Risk management and critical infrastructure protection: Assessing, integrating, and managing threats, vulnerabilities and consequences", *RL32561*, *CRS Report for Congress*, Feb. 2005.

[16] C. Martin, "Protecting america's critical infrastructure: Making our program more effective", *U.S. Army War College*, Mar. 2006.

[17] C. Manto, "Initial economic assessment of Electromagnetic Pulse(EMP) impact upon the Baltimore-Washington-Richmond region", *Instant Access Networks*, LLC, 2007.

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)익스펜전자 중앙연구소장
2002년 2월～현재: 서경대학교 전자공학과 교수
[주 관심분야] EMI/EMC 측정 및 대책 기술, 전자파 재료