고출력전자기파(EMP) 취약점 시범 분석·평가 서비스

양상운 한국정보통신기술협회 공공안전기반기술팀장

1. 머리말

최근 과학기술의 발전은 4차 산업혁명이라는 거대한 변화의 물결을 만들어 냈다. 4차 산업혁명 사회는 인공지능, 빅데이터 같은 고도화된 지능정보기술을 바탕으로 연결된 사회를 의미한다[1]. 이러한 우리사회의 특징은 정보통신 네트워크와 이를 지원하기 위한 기반시설에 과거보다 더 많이 의존하게 되었음을 의미한다. 이에 따라 기반시설에 대한 안전과 보호를 위한 관심을 더 기울여야 한다.

정보통신 기반시설은 각종 자연재해부터 사회적 재난 또는 테러나 전쟁 등 다양한 요인에 위협받는다. 다양한 위협 요인 중 정보통신 기반시설에 특화된 고유 위협요인은 전자적 침해를 유발하는 공격과 사고이다. 이러한 전자적 침해사고를 유발하는 공격행위를 우리 법에서는 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스거부 행위, 그리고 고출력전자기파 등으로 정의한다[2]. 본고에서는 이러한 다양한 전자적 침해유발 공격행위 중 고출력전자기파(EMP, Electromagnetic Pulse) 공격과 위협을 방호할 때 첫 번째 단계인 취약점 분석평가에 관해 설명하고자 한다.

다음 본문에서는 먼저 EMP를 간략히 설명하고, 이러한 EMP를 이용한 공격이나 위협 대응의 첫 단계인 취약점 분석·평가에 대한 근거 법제도를 설명한다. EMP 관련 법제도 소개를 통해 EMP 방호 필요 대상과 대상선정 기준, 방호를 위한 각종 절차 등을 설명하고, 특히 정보통신기반보호법에 근거한 취약점분석·평가에 대해 자세히 설명한다. 마지막으로는 현재 과학기술정보통신부의 지원을 받아 한국정보통신기술협회가 수행하고 있는 민간분야 취약점 시범 분석·평가 서비스를 소개한다.

2. EMP 취약점 시범 분석·평가 서비스

2.1 EMP란?

EMP 또는 EMP 효과란 물리학적으로는 콤프턴 효과 또는 콤프턴 산란의 원리에 바탕을 둔다. 즉 핵폭발로 발생한 고에너지 감마선 광자가 원자핵과 충돌하면서 방출된 고에너지 전자기 펄스이다. 간단하게 말해 핵폭발 등으로 발생하는 고출력전자파 또는 충격파이다.

1) https://www.4th-ir.go.kr/4ir/list
2) 정보통신기반보호법, 정보통신망 이용촉진 및 정보보호에 관한 법률, 전자금융거래법, 원자력 시설 등의 방호 및 방사능 방재 대책법 등

EMP가 본격적으로 알려지게 된 계기는 미 해군의 핵무기 실험이다. 1962년 미해군이 태평양 상공에서 핵무기 실험을 하였는데, 폭발 시 폭발 장소로부터 무려 1,000km 떨어진 위치의 관측 장비 및 각종 전자시스템이 오동작 또는 작동을 멈추는 이상현상이 발생하였다. 이러한 현상의 원인이 핵폭발 시 발생한 EMP였던 것이다. 이러한 EMP 효과 발견 과정에서 알 수 있듯, 지금까지 EMP에 대한 인식과 관심은 주로 핵에 의한 EMP(NEMP, Nuclear EMP)에 집중되었다. 국내에서는 과거 여러 차례 북한의 핵무기 개발에 의한 직간접적인 위협으로 EMP 공격 가능성과 이에 대한 방호 필요성이 알려져 왔다.

2.2 EMP 관련 국내 법제도 현황

정보통신기반시설에 EMP 공격이나 사고가 발생하면 해당 시설을 운영하는 기관을 넘어 많은 국민에게 상당한 피해를 미칠 수 있다. 이러한 우려에 따라 정부는 법제도를 통해 EMP 방호 대상을 지정하고, 방호대책을 수립하도록 안내하고 있다.

국내 EMP 관련 규제와 기준을 직간접적으로 명시하고 있는 법령은 「정보통신기반보호법」 및 「원자력 시설 등의 방호 및 방사능 방재 대책법」, 「전파법」, 「정부기관 비상대피시설 설치에 관한 규정」 등에 산재되어 있다. 「정보통신기반보호법」과 「원자력 시설 등의 방호 및 방사능 방재 대책법」은 EMP 침해를 규정하고 대책을 명시한다. 「전파법」은 EMP로부터 주요 정보통신시설을 보호하기 위한 방호시설 성능 기준을 규정하고, 성능 확인을 위한 시험방법을 제시한다. 또한 「정부기관 비상대피시설 설치에 관한 규정」(행자부 훈령)은 비상 대피시설 설치 시 EMP 방호시설을 설치하고 관련 성능시험을 수행하도록 세부 시행 기준을 정한다. 「EMP 침해방지대책기술기준」은 핵과 비핵을 포함하여 현재 국내에 서 가장 앞선 EMP 방호 기준을 명시한다.

산재된 EMP 관련 법령 중, EMP 방호의 첫 단계라 할 수 있는 취약점 분석·평가는 정보통신기반보호법의 관련 조항에 근거한다. 「정보통신기반보호법」은 전자적 침해행위에 대한 대책으로 2001년 1월 제정됐다. 해당 법에는 공공기관 및 민간시설을 포함한 주요 정보통신기반시설을 지정하고 관리하는 내용을 담았다. 참고로, 현재 19개 관계중앙행정기관과 약 220여 개 관리기관에 대해 약 400개의 주요 정보통신기반시설이 지정되어 관리 중이다. 이러한 기반시설은 정보통신분야부터 방송, 금융, 교통, 에너지, 원자력, 식·용수, 의료, 보건복지, 지리정보, 기타 등이 있다. 주요 정보통신기반시설의 지정은 다섯가지 기준을 따른다.

- 첫 째 관리기관이 수행하는 업무의 국가적, 사회적 중요도
- 둘 째 관리기관 업무가 정보통신기반시설에 의존하는 정도
- 셋 째 타 정보통신기반시설과의 상호 연계성
- 넷 째 침해사고 발생 시 국가안전과 경제 사회에 미치는 피해 규모와 범위
- 다섯째 침해사고의 발생가능성과 사고 발생 시 복구의 용이성 등

이러한 기준에 의해 지정한 주요 정보통신기반시설은 해킹, 컴퓨터 바이러스 등과 함께 고출력전자기파에 의한 전자적 침해행위에 대비하여 보호계획을 수립하고 시행하여야 한다. 이때 보호대책의 일환으로 본 법령에 근거하여 정기적으로 취약점을 분석하고 평가하여야 한다.

물론 취약점 분석·평가를 위한 근거 법령이 있음에도 불구하고, EMP 위협에 대한 취약점 분석평가는 여전히 시범단계이다. 「정보통신기반보호법」은 EMP를 포함한 주요 전자적 침해행위에 대한 취약점 분석·평가를 수행하기 위한 명시적 근거이고, 구체적인 기준과 절차 등 수행방법은 하부 고시에 있다(주요정보통신기반시설취약점 분석·평가 기준 미래창조과학부 고시 제2013-37호).

<표 1> 정보통신기반보호법 주요 내용

제1조(목적) 이 법은 전자적 침해행위에 대비하여 주요정보통신기반시설의 보호에 관한 대책을 수립·시행함으로써 동 시설을 안정적으로 운용하도록 하여 국가의 안전과 국민생활의 안정을 보장하는 것을 목적으로 한다.

제2조(정의) 이 법에서 사용하는 용어의 정의는 다음과 같다.
1. "정보통신기반시설"이라 함은 국가안전보장·행정·국방·치안·금융·통신·운송·에너지 등의 업무와 관련된 전자적 제어·관리시스템 및 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제1호의 규정에 의한 정보통신망을 말한다.
2. "전자적 침해행위"라 함은 정보통신기반시설을 대상으로 해킹, 컴퓨터바이러스, 논리·메일폭탄, 서비스거부 또는 고출력 전자기파 등에 의하여 정보통신기반시설을 공격하는 행위를 말한다.
3. "침해사고"란 전자적 침해행위로 인하여 발생한 사태를 말한다.

제9조(취약점의 분석·평가) ① 관리기관의 장은 대통령령이 정하는 바에 따라 정기적으로 소관 주요정보통신기반시설의 취약점을 분석·평가하여야 한다. ⑤과학기술정보통신부장관은 관계중앙행정기관의 장 및 국가정보원장과 협의하여 제1항 및 제2항에 따른 취약점 분석·평가에 관한 기준을 정하고 이를 관계중앙행정기관의 장에게 통보하여야 한다.

그런데 이 고시의 내용이 악성코드 유포, 해킹등 사이버 위협에 대한 내용 위주로 작성되어 있어 EMP로 인한 전자적 침해 위협에 대한 취약점 분석·평가를 할 수 없는 상황이다. 전자적 침해행위의 요인으로 EMP가 가장 최근에 포함되었기에 발생한 제도적 빈자리이긴 하나, EMP 침해 시 발생할 수 있는 피해 규모를 고려하면 서둘러 해당 고시에 EMP에 위협에 대한 취약점분석·평가 기준과 절차를 보완할 필요가 있다. 이러한 제도적 미흡함을 개선하기 위해 과학기술정보통신부 국립전파연구원은 2018년 주요 정보통신기반시설 EMP 취약점분석·평가기준을 제작하여 지정시설 관리·운영기관에 배포했다. 이 기준은 EMP 취약점 분석·평가가 공식 적용되기 전 시범수행에 활용하고 시범수행 중 파악된 세부절차 및 각종 미비점을 파악하여 제도보완에 활용할 예정이다. 다음 장에서 설명할 과기정통부의 민간 분야 EMP 취약점 분석·평가서비스(명확하게는 시범 분석·평가) 역시 해당기준을 근거한다.

2.3 민간 주요 정보통신기반시설 대상 EMP 취약점 시범 분석·평가

EMP 취약점 분석·평가는 용어 그대로 고출력전자기파로 발생하는 전자적 침해위협에 대한 시설의 취약점을 분석하고 평가하는 일련의 과정이다. 이러한 과정은 크게 세 단계 또는 네 단계로 구별된다. 계획수립과 대상선별을 합치느냐, 또는 구별하느냐의 차이다.

간단하게 세 단계로 구별하여 살펴보자. 첫째 단계는 '계획 수립 및 대상목록 산출'로 EMP 공격이나 사고 위험성을 분석하고 분석 대상을 선정하는 과정이다. EMP 방호는 여전히 많은 비용과 시간이 필요하다. 따라서 취약점 분석평가의 첫 번째 절차는 해당 시설이 EMP 공격에 대응하는 방호가 필요한지 판단하는 과정이다. 물론 주요 정보통신기반시설로 지정된 기관의

시설은 EMP 방호대책의 필요성이 검토됐다고 가정할 수 있다. 그리고 해당 시설이 EMP 공격에 대응하는 방호가 필요하다고 판단한 경우, 대상 시설 내 설비와 세부 시설, 더 자세하게는 시설 내세부 기능을 구별하여 취약점 분석 대상을 선별한다. 선별한 대상목록에 대해 EMP 공격에 의한 피해규모를 추정하고, 이를 통해 중요도를 판단한다.

두 번째 단계는 '취약점 분석' 단계로 EMP 방호필요성을 분석하고, 구체적인 점검항목을 도출하여 분석하는 과정이다. EMP 방호필요성을 분석하기 위해서는 EMP 공격 시 중단 또는 오동작하는 서비스의 범위, 중요한 데이터의 손실 가능성, 그리고 침해발생 시 복구가능시간 등을 고려하여야 한다. 도출한 점검항목에 대한 취약점 분석은 관리적, 물리적, 기술적 세 가지 측면을 고려한다. 관리적 측면은 EMP 방호를 위한 내부 정책과 관리시스템, 그리고 방호교육 및 대응교육 여부 등을 점검하고, 물리적 측면은 EMP 방호에 영향을 미치는 시설환경을 분석한다. 예를 들어 대상 시설에 일반인의 접근이 통제되거나 접근이 가능하더라도 즉각 파악이 가능한 감시장치가 있을 경우에는 테러와 같은 비핵 EMP 공격에 대한 취약점이 낮게 분석된다. 통상적으로 알려진 비핵 EMP 발생장치를 대상시설 주변 어딘가에서 구동시켜야 하는데, 이러한 공격시나리오 가능성이 물리적 환경에 의해 낮아지기 때문이다.

세 번째 기술적 분석은 EMP 방호가 필요한 설비와 장치 자체의 내성부터 설비와 장치를 보호하고 있는 차폐랙, 차폐실, 더 크게는 건물의 내성을 분석하는 과정이다. 주요 정보통신기반시설 내 여러 가지 대상목록들은 기능과 형태에 따라 일부는 차폐랙이나 차폐실 안에 있을 수 있고 또한 해당 시설의 위치가 건물 지하나 높은 층 등 위치가 다르다. 이러한 시설 내 자체 차폐환경과 분석대상이 위치한 건물의 구성재료(콘크리트, 철골, 유리 등), 그리고 건물 내 위치에 따른 전파진행 경로상의 환경은 해당 시설이 자체적으로 보유한 차폐 내성이다. 기술적 분석은 이러한 기반시설 건물과 환경에 의한 차폐내성을 분석하고, 이를 취약점 평가에 반영하기 위함이다. 이러한 관리적, 물리적, 기술적 분석을 통한 취약점 분석결과는 궁극적으로는 적절한 수준의 EMP 방호레벨을 판단하고, 효율적인 방호방법을 검토할 때 고려해야 하는 중요한 요소이다.

마지막 '취약점 평가' 단계는 앞서 분석한 대상목록에 대한 취약점 전반을 평가하고 위험등급을 부여한다. 현재 과학기술정보통신부에서 제시하는 주요 정보통신기반시설 대상 EMP 취약점 분석·평가기준에 의하면 위험등급은 1부터 3등급으로 표시하며, 1등급부터 각각 조기개선, 중기개선, 장기개선과 같이 조치를 취해야 하는 시급함의 단계를 의미한다. 이렇게 진행한 취약점 분석·평가를 통해 파악한 취약점에 대해서는 해당 시설의 관리기관이 보호대책을 수립할 때 반영하여야 한다.

물론 앞서 언급한 대로 EMP에 대한 취약점 분석·평가는 세부 적용규정 미비로 인해 아직 의무가 아니므로 현재 관리기관에서 보호대책수립 시 EMP 취약점 분석·평가를 반드시 시행하지는 않는다. 사실 EMP 취약점 분석·평가 절차는 계획수립-대상선정-분석-평가라는 큰 틀에서 기존의 사이버침해 위협에 대한 취약점 분석·평가와 유사하다. 단, 위협의 요인이 다르므로 위험 대상목록이 다르고, 대상목록에 대한 취약점분석방법과 평가, 그리고 개선방향의 내용이 모두 다를 뿐이다. 사이버와 비교한 EMP 취약점 분석·평가에 대해 요약하면 <표 2>와 같다.

<표 2> 사이버와 EMP에 대한 취약점 분석평가 제도 현황 비교표

구분	사이버 취약점분석평가	EMP 취약점분석평가
위협 종류	악성코드 유포, 메일폭탄, 해킹 등 사이버 침해 위협	핵/비핵 고출력전자파(EMP) 등 전쟁, 테러, 범죄 등의 실제 침해 위협
관련 법령	정보통신기반보호법 제2조, 제9조 근거, 세부규정 마련(전문기관 존재)	정보통신기반보호법 제2조, 제9조 근거, 세부규정 없음(전문기관 없음)
관련 고시	2013년 8월, 미래창조과학부 고시 제2013-37호, 취약점 분석·평가 기준 발효	현재 기준 마련 및 확정을 위한 시범사업 진행 中 (`18년 개시)
추진 방법	신규 지정 후 6개월 이내 실시 매년 1회 취약점 분석·평가 시행 中	- 신규 지정 후 6개월 이내 실시 - 매년 1회 취약점 분석·평가 제도 마련 中

2.4 한국정보통신기술협회(TTA)의 EMP 취약점 시범 분석·평가 서비스

과학기술정보통신부는 민간분야 EMP 방호유도와 EMP 방호와 관련된 국내 산업활성화를 위해 2018년부터 기반조성사업[3]을 진행 중이다. 해당 과학기술정보통신부의 기반조성사업은 한국정보통신기술협회(TTA)가 수행기관으로 지정되었으며, 한국정보통신기술협회는 크게 두 가지 내용(EMP 방호 기술지원과 EMP 방호 인식제고)으로 세부사업을 한다.

EMP 방호 기술을 지원하기 위해서는 취약점시범 분석·평가 서비스와 전파특성 성능검증시험 서비스를 제공하며, EMP 방호 인식을 제고하기 위해서는 EMP 관련 교육프로그램 운영 및 EMP 방호포럼 운영을 지원한다. TTA의 EMP취약점 시범 분석·평가 서비스는 위에서 설명한 과학기술정보통신부의 취약점 분석·평가기준을 바탕으로 시행한다. TTA의 취약점 시범 분석·평가 서비스의 절차 역시 앞서 설명한 취약점 분석·평가 기준의 절차와 대동소이하나, 도식화하여 요약하면 다음 <표 3>과 같다.

TTA의 취약점 분석·평가 서비스의 차별점은 취약점 분석 작업에서 좀 더 자세한 기술적 분석을 한다는 것이다. TTA는 EMP 측정을 위한 장비(신호발생기, 신호분석기, 안테나 등)와 더불어자체 개발한 EMP 신호 제어프로그램을 활용한다. 또한 대상 시설이 위치한 건물과 주변 환경의 내성 수준을 더 정확하게 측정하고 이를 취약점평가에 반영하여 최대한 효율적인 수준의 방호대책 수립을 하도록 지원한다.

민간분야 주요정보통신기반시설을 보유한 기관들은 대부분 기업들로, 대부분의 기업이 취약점 분석평가가 자기의 영업활동에 미치는 영향을 우려한다. 이러한 우려를 해소하기 위해, TTA는 주말이나 야간시간대 등 영업 외 시간을 집중 활용하여 현장분석 및 실측을 진행한다. 또한 실측 진행 시, EMP 신호의 세기와 측정지점을 적절하게 판단하여, 기업의 다른 시설과 장치에 절대 영향을 미치지 않도록 주의를 기울이고 있다.

또한, 건물이나 시설의 내성을 실측하려면 시설이나 건물에 대한 EMP 공격 시나리오를 가정한지점에서 전파를 쏘고 이를 내부에서 측정하여야 하는데, 이러한 건물 내부 또는 건물 외부 주변 위치를 확보하는 게 현실적으로 불가능할 수 있다. 이러한 경우를 위해 TTA는 EMP 내성측정을 시뮬레이션하여 기술적 분석을 진행하기도 한다. 물론 이를 위해서는 대상 기업이 기반시설이 위치한 건물이나 시설에 대한 도면정보 제공하는 것 같은 협조가 필요하다.

3) 2018년 EMP방호기반조성사업, 2019년 이후 고출력전자파 침해 대응산업 활성화사업(사업명 변경)

<표 3> TTA 취약점 시범분석평가 서비스 절차 요약

단계구분	수행 업무내용	예상 소요기간
사전협의	• 세부 방법 및 일정 협의 • 제공자료 내역 및 보안관리 방안 협의 • 취약점 분석 평가 지원인력 및 범위 정의 • 결과물에 대한 통보방법 및 결과물의 활용 범위 협의	3~4주
대상시설 EMP 방호 필요성 분석	• 법률 등으로 부여된 운용 및 서비스 제공 의무범위 • 대상 시설의 운용 목적과 피해 규모 산정 • 전시 및 평시 각 상황별 EMP 방호 필요성 여부 검토	3~4주
분석·평가 대상목록 작성	• 시범분석 대상 범위 선정 • 기능레벨 분류 수행 • 설비레벨 분류 수행	3~4주
EMP 취약점 평가 수행	• 작성된 설비 목록에 대해 방호대책 평가 • 방호대책 선정과 취약점 평가 수행 • 방호대책 적용 필요성 분석을 통해 방호대책 선정	3~4주
결과보고서 작성	• 결과보고서 작성 및 통보방법 등 협의 - 자문위원회 의견 검토 - 피평가기관 의견 검토	3~4주

3. 맺음말

지금까지 EMP 침해는 주로 북한의 핵무기 공격 시 발생하는 사고로 간주해 왔다. 따라서 남북관계가 좋아지거나 나빠짐에 따라 EMP 방호 필요성과 관심의 온도가 가변적이었다. 그러나 EMP는 핵무기가 아닌 다른 비핵 발생장치로도 막대한 피해를 유발할 수 있다. 근래 들어서는 소형화한 비핵 EMP 발생장치를 차량이나 드론 같은 이동수단에 탑재하여 테러수단으로 활용하는 가능성이 제기되기도 하였다. 단순히 핵무기 위협 감소와 현실적인 테러발생 가능성이 낮다는 생각으로 EMP 방호의 필요를 가볍게 보는 것은 매우 위험하다. 또한 서론에서 언급한 대로, 정보통신기술을 기반으로 초연결된 우리 사회의 특성으로 정보통신기반시설을 위협하는 전자적 침해 행위에 대한 대비와 대응은 점점 더 중요하다. 우리나라는 여러 법령을 통해 산업별 주요정보통신기반시설의 EMP 방호를 유도하고 있다.

이러한 제도적 정비에도 불구하고, 정보통신기반시설의 EMP 방호 현황은 매우 열악한데, 이는 EMP 방호를 구축하는 데 여전히 많은 비용이 들기 때문이다. 비용 효율적인 EMP 방호계획을 수립하기 위해서는 가장 먼저 EMP의 취약점을 정확하게 파악하고 자체 방호역량을 잘 활용하여야 한다. 본고에서 소개한 EMP 취약점 분석평가가 민간분야 기반시설 담당자들에게 효과적이고 효율적인 EMP 방호계획을 수립하는 데 잘 활용되기를 기대한다.

※ 본 연구는 2020년 '전파기반 신산업 창출 및 중소기업 육성 세부사업'의 '고출력전자파 침해대응산업 활성화 내역사업'의 일환으로 수행됨

[참고문헌]
[1] 국가정보원·과학기술정보통신부, 2020 '주요정보통신기반시설 EMP 취약점 분석·평가기준'
[2] 권혁진, 이호성, 차동철, 김륙완, 정명원, & 김세현. (2019). '민간 주요시설에서 고출력 전자파 환경차폐특성 측정방법'. 한국통신학회 학술대회논문집, 487-488.
[3] 민병길, 안우근, & 서정택. (2014). '사이버보안 위협 변화에 따른 취약점 분석 방안'. 정보보호학회지, 24(1), 7-12.
[4] 정연춘. (2013). '고출력 전자기파 방호 제도 도입에 관한 연구'. 한국전자파학회논문지, 24(8), 781-790.

※ 출처: TTA 저널 제190호
(코로나 이슈로 각 표준화기구의 표준화회의가 연기・취소됨에 따라 TTA 저널로 대체합니다)