정 보 보 호 학 회 지
제28권 제2호, 2018. 4

사이버보안 위협평가를 통한 원자력시설 등 중요시설 대상 최신 사이버 위협 사례 분석 연구

송 동 훈*, 임 현 종*, 김 상 우*, 류 진 호*, 신 익 현*

요 약

「원자력시설 등의 방호 및 방사능 방재 대책법」(이하 '방사능방재법')에 의거하여 한국원자력통제기술원은 원자력안전위원회로부터 원자력시설의 사이버보안 규제 업무를 위임받아 수행하고 있으며, 그 중 위협평가 업무를 통해 최신 사이버 위협 사례를 분석하여 사이버보안체제의 기준이 되는 설계기준위협을 설정하고 원자력사업자의 이행 여부를 평가하고 있다. 위협평가의 첫 단계로 방사능방재법에 따라 3년 마다 최신 사이버 위협 사례를 조사 및 분석하여야 하며, 사이버 위협 분석 자료는 원자력사업자가 방호해야하는 최대 위협 수준인 설계기준위협 설정에 사용된다. 본 논문에서는 최근 3년간 원자력시설과 같은 중요시설 대상으로 발생한 사이버 위협 사례를 분석하였으며, 향후 분석 자료를 바탕으로 위협평가에 활용하고자 한다.

Ⅰ. 서 론

급격한 정보통신기술의 발전으로 전 세계는 원하는 정보들을 시간·공간적인 한계를 뛰어넘어 언제 어디서나 찾을 수 있게 되었지만, 반대로 사이버 테러를 포함한 사이버 위협이 지속적으로 증가함에 따라 사이버보안의 중요성이 대두되고 있다. 원자력시설과 같은 국가 중요기반시설에도 사이버 테러가 일어나기 시작했으며, 2010년 스턱스넷 악성코드로 인한 이란 원전시설 파괴, 2014년 일본 몬주 원전 해킹 시도, 2014년 원전반대그룹의 한수원 자료 해킹사건, 2015년 우크라이나 발전소 공격에 따른 대규모 정전 등이 대표적인 사이버 공격 사례로 볼 수 있다.

이러한 사이버 위협은 물리적 테러 공격과는 다르게 해킹 기술을 이용하여 비교적 적은 비용으로 큰 피해 효과를 낼 수 있어 해커조직들이 의도적으로 주요 국가 및 시설을 공격하는 계기가 되고 있다. 이와 같이 컴퓨터 및 네트워크 기술 발달과 함께 시대별로 공격의 주체와 목적을 달리하면서 사이버 위협이 발생하고 있으며, 만약 원자력시설과 같이 국가 중요시설이 공격 받을 경우에는 공공 서비스 마비를 넘어 엄청난 경제적 손실로 인해 국민의 안전을 위협할 수 있다.

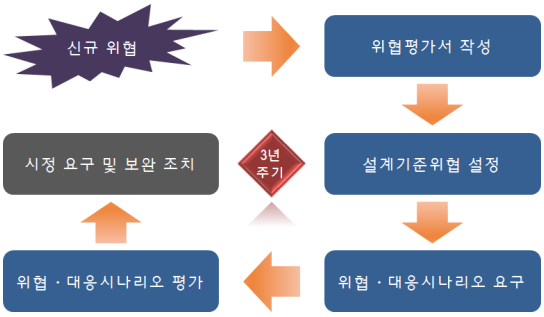
사이버 위협을 방호하기 위해서 방사능방재법 제4조(물리적방호체제의 수립 등)와 동법 시행령 제7조(위협평가 및 물리적방호체제의 수립)에 의거하여 사이버보안 설계기준위협(DBT, Design Basis Threat) 설정을 통해 사이버보안체제를 수립하여야 한다. 이를 위해 3년 마다 최신 사이버 위협의 요인, 발생 가능성, 발생에 따른 결과를 평가하여 사이버보안 설계기준위협 설정을 위한 사이버보안 위협 분석이 필요하다[1].

따라서 본 논문에서는 향후 원자력시설 사이버보안 설계기준위협 재설정 과정에서 활용 가능한 2015년부터 2017년까지의 최신 사이버 위협 사례 중 원자력시설 등 국가 중요시설을 대상으로 하는 해킹, 컴퓨터바이러스, 서비스거부 공격 등 방사능방재법 제2조(정의)에 따른 전자적 침해행위를 상세 분석하고자 한다.

Ⅱ. 사이버보안 위협평가

방사능방재법에 따른 위협평가는 크게 위협평가서 작성, 설계기준위협 설정, 위협·대응시나리오 평가로 구분되며, 사이버보안 설계기준위협은 매 3년마다 위협정

본 연구는 원자력안전위원회의 재원으로 한국원자력안전재단의 지원을 받아 수행한 원자력안전연구사업의 연구결과입니다.
* 원자력통제기술원 사이버보안실 (igiveitashot@kinac.re.kr, silltown@kinac.re.kr, kjoey@kinac.re.kr, halloyu@kinac.re.kr, ihshin@kinac.re.kr)



〔그림 1〕 위협평가 세부 절차

보 수집 및 분석, 위협평가서 작성, 유관기관 자문회의 등의 활동을 거쳐 설정된다. 위협평가에 대한 세부 절차는 그림 1과 같다[2].

2.1. 위협평가 세부 기준

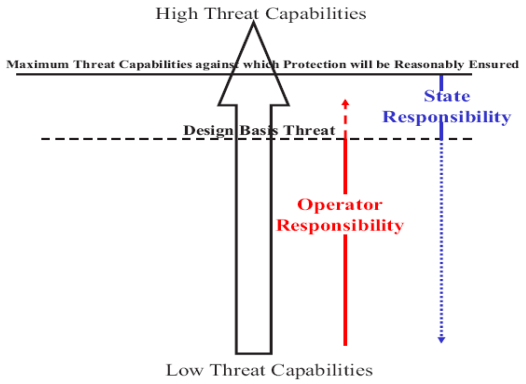
위협평가에 대한 세부 기준은 한국원자력통제기술원의 원자력시설등의 물리적방호 관련 사무편람에 기술되어 있다. 먼저, 사무편람에 의거 위협의 요인, 위협의 발생 가능성, 위협의 발생에 따른 결과를 포함한 위협평가서를 설계기준위협 (재)설정 1년 전까지 작성 완료하여 원자력안전위원회에 제출하여야 한다[2].

또한, 원자력안전위원회로부터 설계기준위협 설정안 제출을 의뢰받은 날로부터 180일 이내에 위협평가서를 활용한 설계기준위협 설정안을 작성하여 제출하여야 한다. 설정된 설계기준위협에 따라 원자력사업자에게 위협·대응시나리오 제출을 요구하여 적합성 여부를 검토하여야 한다. 위협·대응시나리오 관련 서류를 접수 완료하게 되면 15일 이내에 위협·대응시나리오 평가계획서를 원자력안전위원회에 제출하여야 한다[2].

위협·대응시나리오를 검토할 경우, 설계기준위협, 시설의 사이버보안 체계, 시설의 필수디지털자산, 기타 사이버보안에 관한 사항의 포함 여부를 평가하여야 한다. 원자력안전위원회로부터 위협·대응시나리오의 검토의뢰를 받은 날로부터 180일 이내에 처리를 완료하여야 한다[2].

2.2. 설계기준위협

설계기준위협은 불법이전이나 사보타주를 시도하려는 잠재적인 내부자 및 외부 침입자들의 속성과 특성이



〔그림 2〕 설계기준위협에 대한 원자력사업자와 국가의 책임 범위

다. 그림 2와 같이 설계기준위협은 원자력사업자가 대응해야 하는 최대 위협에 해당되며, 이를 초과하는 위협(beyond DBT)에 대해서는 국가차원의 대응이 필요하다[3].

사이버보안 설계기준위협에 포함되어야할 위협은 크게 외부자 위협과 내부자 위협으로 구분할 수 있으며, 각 위협별 특성이 세분화 되어야 한다. 먼저 외부자 위협의 특성은 외부자 유형, 위협 동기, 가용 자원, 공격기법(공격자 능력), 공격시점으로 구분된다. 내부자 위협의 특성으로는 내부자 유형, 위협 동기, 내부자 수, 가용자원, 접속권한, 공격기법(공격자 능력), 공격시점이 포함된다[4].

Ⅲ. 사이버 위협 유형별 동향 및 사례

사이버 위협은 새로운 유형의 테러리즘으로서 물리적 방법이 아니라 사이버 공간을 통해 공격을 감행하는 것이다. 사이버테러는 교통통제시스템, 항공기 관제통제시스템, 금융업무시스템, 식료품 공정 처리 시스템, 의약품 제조공정시스템, 국방관련 통계시스템, 국가전산망 등 현대사회의 핵심 구조를 이루고 있는 전산시스템에 침투하여 전산망을 마비시키거나 정보를 빼내감으로써 상대국을 무력화시키거나 취약점을 공격하기 위한 수단으로 사용된다.

사이버 공격에는 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability) 등에 영향을 줄 수 있는 컴퓨터 기반의 다양한 사건들이 포함된다. 기밀성은 중요한 정보가 허가받지 않은 사람에게 노출되는 것을

막는 것인데, 기밀성 상실은 정보에 대한 미인가된 접근 또는 도청이 있음을 의미한다. 무결성은 정보 또는 소프트웨어가 완전하고, 정확하고, 변경되지 않음을 보장하는 것인데, 무결성 상실은 정보, 소프트웨어, 하드웨어 등에 대한 미인가된 변경이 있음을 의미한다. 가용성은 언제든지 정당한 사용자가 정보와 서비스를 이용할 수 있다는 것을 보장하는 것인데, 가용성 상실은 자료 전송 라인의 차단 또는 시스템의 가동정지를 의미한다.

이러한 사이버 위협의 유형은 각 기관별로 분류가 다소 상이하다. 경찰학사전의 사이버테러 정의에는 컴퓨터해킹, 컴퓨터 바이러스 및 메일폭탄 유포, 사이버 스토킹 등으로 구분되며, 경찰청 사이버안전국에서 정의한 정보통신망 침해 범죄 유형으로는 해킹, 서비스거부 공격, 악성프로그램 및 기타 정보통신망 침해형 범죄로 분류하고 있다. 한국인터넷진흥원의 민간부문 침해사고 대응 안내서에 따르면 바이러스, 트로이잔, 웜, 악성코드 등의 공격, 네트워크 및 시스템의 정상적인 서비스를 마비 또는 파괴시키는 서비스 방해, 네트워크 서비스의 취약점을 이용하여 서비스를 무단 이용하는 비인가된 서비스 이용, 네트워크 정보 수집을 포함한 비인가된 네트워크 정보 접근, 비인가된 시스템 접근 및 파일 접근으로 구분된다.

원자력시설의 사이버 위협은 방사능방재법 제2조 정의의 '전자적 침해행위'에 따라 해킹, 컴퓨터바이러스, 논리·메일폭탄, 서비스거부 등으로 공격 유형이 구분되며, 최근 3년간('15년~ '17년) 사이버 위협 유형별 사건을 상세 분석하였다.

3.1. 해킹 공격

해킹 공격은 컴퓨터 또는 네트워크와 같은 자원에 대해 정당한 접근권한 없이 또는 허용된 접근권한을 초과하여 침입하는 행위를 말하며, 주로 계정도용, 단순침입, 자료유출, 자료훼손 등의 영향을 줄 수 있다. 2015년부터 2017년까지 발생한 주요 해킹 공격 사례는 아래 표 1과 같다[4].

해킹 공격 사건 중 주요 사이버 사건에 대한 분석 내용은 아래와 같다.

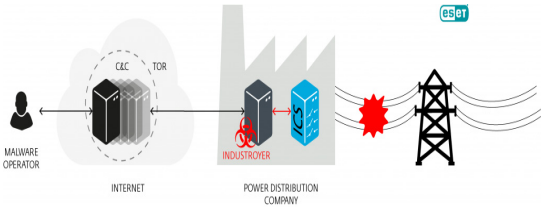
〔표 1〕 2015~2017년 주요 해킹 공격 사례

발생년도	발생국가	주요 사건 명
2015	대한민국	원전반대그룹의 홈페이지 변조
2015	이스라엘	전력공사 해킹 공격으로 2일간 업무 마비
2015	베트남	금융권 해킹 사건
2016	방글라데시	방글라데시 은행 8100만 달러 해킹 사건
2016	대한민국	공군 홈페이지 해킹 사건
2016	인도	인도 은행 1천900억 원 해킹 사건
2016	이란	석유화학 공장 사이버 공격
2016	대한민국	국방부 해킹사건
2016	독일	도이체텔레콤 해킹 공격에 따른 통신 마비
2016	우크라이나	전력 배전 회사 해킹으로 8만명 정전 피해
2016	미국	대선 투표시스템 해킹
2017	대한민국	아시아나항공 홈페이지 변조 사건
2017	북한	북한 미사일 발사 교란 해킹 사건
2017	프랑스	프랑스 대선 후보 해킹 공격
2017	대한민국	국내 웹호스팅 업체 130여 곳 대량 해킹 사태
2017	우크라이나	랜섬웨어로 인한 체르노빌 홈페이지 마비
2017	폴란드	폴란드 은행 사이버 공격 시도
2017	미국	미국 원전 관리 기업, 울프크릭 해킹 사건

3.1.1. [우크라이나] 전력 배전 회사 해킹으로 8만명 정전 피해

본 사건의 공격 목적은 정치적 이유이며, 공격 주체는 러시아 해커 그룹 샌드웜으로 추정된다. 공격 대상은 우크라이나 전력 회사 Ukrenergo의 전력망이며, 공격 경로는 VPN을 이용하였으며, 공격 자원은 Industroyer 악성코드를 사용하였다[5,6].

공격 방법은 Siemens 시스템의 모델에 대한 특정 공격을 수행하여 전력 시스템을 제어하는 원격 터미널 장치를 끄고 정전을 일으켰다. 피해 현황은 키에프 북쪽과 인근 지역에서 1시간 15분 동안 정전이 발생되었으며 관련 사진은 그림 3과 같다[5,6].



〔그림 3〕 우크라이나 전력 배전 회사 해킹으로 8만명 정전 피해 사건 관련 사진

3.1.2. [미국] 미국 원전 관리 기업, 울프크릭 해킹 사건

본 사건의 공격 목적은 정보 탈취이며, 공격 주체는 불분명하나, Energetic Bear라고 불리는 러시아 해커 그룹의 기술을 모방한 것으로 추정된다[5,7].

공격 대상은 울프크릭(Wolf Creek) 원자력 운영회사이며, 공격 경로는 이메일을 이용하였으며, 공격 자원으로 악성 코드가 포함된 Microsoft Word 문서를 사용하였다[5,7].

공격 방법은 Microsoft Word 취약점을 이용하여 악성 코드를 제작한 후, 가짜 이력서로 위장하여 수석 산업 제어 엔지니어에게 전송한 후, 엔지니어가 해당 문서를 열면 네트워크상에 있는 다른 기기에 접속 할 수 있는 자격 증명을 훔칠 수 있도록 설계하였다[5,7].

피해 현황은 원전을 관리하는 컴퓨터 시스템이 기업 네트워크와 분리되어 있고, 제어시스템은 인터넷에 연결되어 있지 않아 피해가 발생되지 않았다[5,7].

3.2. 컴퓨터바이러스 공격

컴퓨터바이러스 공격은 컴퓨터 또는 네트워크와 같은 자원을 정당한 사유 없이 훼손, 멸실, 변경, 위조하거나 그 운용을 방해할 수 있는 바이러스를 전달 또는 유포하는 행위를 말하며, 컴퓨터바이러스는 사용자 몰래 스스로 복제하여 다른 프로그램을 감염시켜 정상 프로그램이나 다른 데이터 파일을 파괴한다. 2015년부터 2017년까지 발생한 주요 컴퓨터바이러스 공격 사례는 아래 표 2와 같다[4].

컴퓨터바이러스 사건 중 주요 사이버 사건에 대한 분석 내용은 아래와 같다.

〔표 2〕 2015~2017년 주요 컴퓨터바이러스 공격 사례

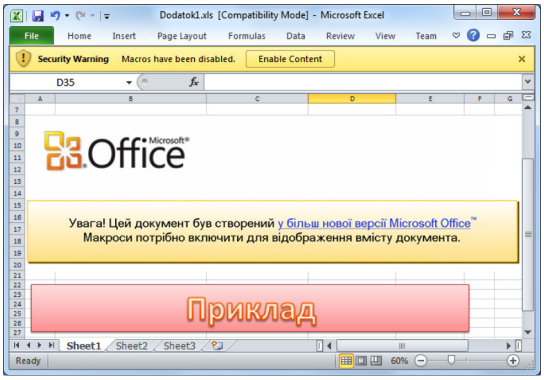
발생년도	발생국가	주요 사건 명
2015	우크라이나	악성코드 감염에 따른 22만명 정전 사태
2016	미국, 뉴질랜드	의료 시설 랜섬웨어 감염
2016	독일	독일 병원 랜섬웨어 감염
2016	캐나다	오타와 병원(Ottawa Hospital) 랜섬웨어 감염
2016	미국 등	랜섬웨어 감염
2016	미국	전력, 석유 파이프라인, 수도 등 주요 인프라시스템 악성코드 감염
2016	독일	원전 연료취급시스템 악성코드 감염
2017	전 세계	WannaCry
2017	대한민국	인터넷나야나 랜섬웨어 감염

3.2.1. [우크라이나] 악성코드 감염에 따른 22만명 정전 사태

본 사건의 공격 목적은 사회 혼란이며, 공격 주체는 러시아 해킹 그룹 샌드웜으로 분석됐다. 공격 대상은 우크라이나에 위치한 3개의 전력 배전 회사이며, 공격 경로는 이메일을 사용하였고, 공격 자원은 피싱 메일을 통해 악성 매크로를 포함하는 Microsoft Word문서, BlackEnergy, KillDisk 악성코드 및 전화회선 DoS를 이용하였다[5,8].

공격 방법은 보낸 사람 주소를 우크라이나 의회로 위장하여 악성 매크로 첨부파일을 실행하도록 유도하는 내용이 포함된 메일을 전송하여 피해자가 첨부파일을 실행하면 시스템에 BlackEnergy 악성코드가 다운로드 되도록 하였으며, BlackEnergy는 KillDisk 악성코드를 다운로드하도록 설계됐다. KillDisk를 이용하여 감염된 시스템의 중요 구성 요소를 제거하고, 마스터 부트 레코드(MBR)를 손상시켜 시스템이 작동하지 못하게 한 후, 차단기를 열어 정전을 일으켰으며, 발전소 직원이 정전 보고를 받지 못하도록 전화 회선에서 서비스 거부 공격을 수행하였다[5,8].

피해 현황은 22만 명의 고객이 약 8시간 동안 정전의 영향을 받았으며, 발전소의 중요 장치에 펌웨어를 덮어써서, 새로운 장치를 가져와 통합할 때까지 복구할 수 없어 차단기를 수동으로 제어해야 했다. 사건 관련 사진은 그림 4와 같다[5,8].



〔그림 4〕 우크라이나 악성코드 감염에 따른 22만명 정전 사건 관련 사진

3.2.2. [독일] 원전 연료취급시스템 악성코드 감염

본 사건의 공격 목적은 사회 혼란이며, 공격 주체는 불분명하다. 공격 대상은 Gundremmingen 원자력 발전소로, 공격 경로는 알려지지 않았다[5,9].

공격 자원은 W32.Ramnit, Conficker 악성코드를 사용하였으며, 공격 방법은 W32.Ramnit 악성코드를 이용하여 로그인 자격 증명을 도용하고, 해커에게 원격으로 액세스할 수 있도록 백도어 기능을 제공하였으며, Conficker 악성코드를 이용하여 사용자 자격 증명 및 개인 재무 데이터를 훔치고, 감염된 컴퓨터를 봇으로 만들어 분산 서비스 거부(DDoS) 공격을 수행하려고 시도하였다[5,9].

피해 현황은 발전소의 운영 체제와 별도로 유지 관리되는 사무실 컴퓨터의 18개 저장장치(대부분 USB)와, 원전연료취급시스템에서 악성코드가 발견되었으며, 감시시스템이 인터넷에서 격리되어 있어 악성코드가 C&C 서버에 접속할 수 없었기 때문에, 발견 당시까지 활성화되지 않아 시설 운영에 위협이 되지는 않았다[5,9].

3.3. 논리·메일폭탄 공격

논리·메일폭탄 공격은 사용자의 이메일 프로그램을 마비시키거나 정당한 메시지의 수신을 방해할 의도로 사용자의 이메일 주소로 엄청난 양의 이메일 데이터를 발송하거나 논리폭탄을 이용하는 행위를 말하며, 해킹 공격이나 컴퓨터바이러스 등을 유포하기 위한 수단으로 사용된다. 2015년부터 2017년까지 발생한 주요 논리·메일폭탄 공격 사례는 아래 표 3과 같다[4].

〔표 3〕 2015~2017년 주요 논리·메일폭탄 공격 사례

발생년도	발생국가	주요 사건 명
2016	대한민국	청와대 사칭 악성 이메일 발송 사건
2016	미국	미국 국토 안보부 인사정보탈취 사건
2016	미국	대선 후보 스피어 피싱
2017	영국	영국 의회에 이메일 피싱 공격

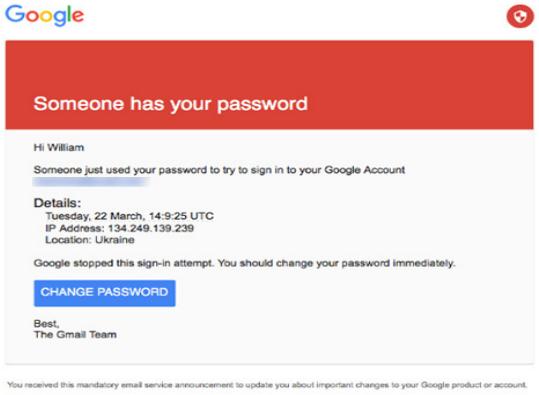
논리·메일폭탄 공격 중 주요 사이버 사건에 대한 분석 내용은 아래와 같다.

3.3.1. [미국] 대선 후보 스피어 피싱

본 사건의 공격 목적은 러시아 정부의 정치적 이익을 위한 것이며, 공격 주체는 APT28이다. 공격 대상은 힐러리 클린턴 캠프 관계자 및 직원들이며, 공격 경로로 이메일을 사용하였으며, 공격 자원으로 피싱 메일을 활용하였다[5,10].

공격 방법은 Bitly계정을 사용하여 Gmail 계정 사용자 이름을 Base64로 인코딩한 값을 포함하는 악성 URL을 단축해 전자 메일에 링크를 첨부하여 보냈으며, 링크 클릭 시 사용자 이름 입력란에 이메일 주소가 미리 채워진 가짜 Google 계정 로그인 페이지가 표시되도록 하여 입력된 자격 증명을 사용해 Gmail 계정의 내용에 액세스하였다[5,10].

피해 현황은 힐러리 클린턴 대선 후보의 캠페인 일정에 대한 정보 등이 유출되었다. 사건 관련 사진은 그림 5와 같다[5,10].



〔그림 5〕 미국 대선 후보 스피어 피싱 사건 관련 사진

3.3.2. [영국] 영국 의회에 이메일 피싱 공격

본 사건의 공격 목적은 정보 탈취이며, 공격 주체는 러시아 해커로 추정된다. 공격 대상은 영국 의회 이메일 시스템이며, 공격 경로로 이메일을 사용하였으며, 공격 자원은 피싱 메일을 활용하였다[5,11].

공격 방법은 정치인과 10명 미만의 의원에게 자신의 컴퓨터에 액세스할 수 있게 해주는 가짜 피싱 이메일을 보냈으며, 네트워크 상의 9000개 이상의 의회 이메일 사용자의 계정에 대한 지속적인 무차별 대입 공격을 통해 액세스를 시도하였다[5,11].

피해 현황은 취약한 로그인 자격 증명을 사용한 90명의 의회 전자 메일 계정이 탈취되었다[5,11].

3.4. 서비스거부 공격

서비스거부 공격은 네트워크 기능을 마비시킬 목적으로 서버가 처리할 수 있는 능력 이상의 것을 요구하거나 해당 요구 사항만 처리하게 만듦으로써 다른 서비스를 정지시키거나 시스템 자체를 다운시키는 행위를 말하며, 다수의 시스템을 통해 분산 서비스 공격이 주로 사용된다. 2015년부터 2017년까지 발생한 주요 서비스 거부 공격 사례는 아래 표 4와 같다[4].

서비스거부 공격 중 주요 사이버 사건에 대한 분석 내용은 아래와 같다.

〔표 4〕 2015~2017년 주요 서비스거부 공격 사례

발생년도	발생국가	주요 사건 명
2015	대한민국	금융업체에 대한 서비스거부 공격
2015	폴란드	폴란드 항공 DDoS 공격으로 5시간 마비
2015	스위스	ProtonMail DDoS 사건
2016	미국	FirstEnergy사 대규모 DoS공격
2017	대한민국	시간당 10만원 디도스 공격-사이버 청부테러
2017	대한민국	금융업체 DDoS 위협 사건

3.4.1. [대한민국] 금융업체에 대한 서비스거부 공격

본 사건의 공격 목적은 금전적 이익 추구이며, 공격 주체는 DD4BC(DDoS for Bitcoin)이다. 공격 대상은 대구, 부산, 전북은행, 미래에셋증권, 한국투자증권 등이다. 공격 경로는 네트워크를 이용하였으며, 공격 자원으로 SSDP(Simple Service Discovery Protocol) 프로토콜 패킷을 사용하였다[5,12].

공격 방법은 SSDP 프로토콜 취약점을 악용하여 50GB이상의 트래픽을 발생시켜 DDoS 공격을 수행하였으며, 초기 공격을 수행한 후 해커들은 더 높은 강도의 DDoS 공격을 수행할 것이며 공격을 멈추고 싶으면 비트코인을 지불하고, 요구를 무시하면 가격이 더 올라갈 것이라는 협박 메시지를 보냈다[5,12].

피해 현황은 금융권과 금융보안원, 한국인터넷진흥원의 공동 대처로 큰 장애가 발생하지 않았고 비트코인 또한 지불되지 않았다. 사건 관련 사진은 그림 6과 같다[5,12].


To: redacted
Hello,

To introduce ourselves first:

https://blogs.akamai.com/2014/12/dd4bc-anatomy-of-a-bitcoin-extortion-campaign.html

http://bitcoinbountyhunter.com/bitalo.html

http://cointelegraph.com/news/113499/notorious-hacker-group-involved-in-exc=oin-theft-owner-accuses-ccedk-of-withholding-info

Recently we were DDoS-ing Neteller:

https://twitter.com/neteller/status/583363894665715712

Yes, our attacks are powerful.

So, it=E2=80=99s your turn!

Your site is going under attack unless you pay 25 Bitcoin.

Pay to 198Qaeuj6oMeuan2p5gyDx75odweMWzNXH

Please note that it will not be easy to mitigate our attack, because
our current UDP flood power is 400-500 Gbps, so don't even bother. At
least, don't expect cheap services like CloudFlare or Incapsula to
help...but you can try. :)

Right now we are running small demonstrative attack.
Don't worry, it will not be that hard (it shouldn't crash your site)
and it will stop in 1 hour. It's just to prove that we are serious.
Check UDP traffic. :)

We are aware that you probably don't have 25 BTC at the moment, so we
are giving you 24 hours.

Find the best exchanger for you on
https://localbitcoins.com or
http://howtobuybitcoins.info
You can pay directly through exchanger to our BTC address, you don't
even need to have BTC wallet.

Current price of 1 BTC is about 230 USD, so we are cheap, at the

〔그림 6〕 금융업체 해킹을 통한 악성코드 유포 관련 사진

3.4.2. [미국] FirstEnergy사 대규모 DoS공격

본 사건의 공격 목적은 사회 혼란이며, 공격 주체는 불분명하다. 공격 대상은 FirstEnergy사 컴퓨터 네트워크로, 공격 경로인 네트워크를 이용하였으며, 공격 자원에 대한 알려진 정보는 없다[5,13].

공격 방법은 FirstEnergy의 컴퓨터 네트워크에 악성 트래픽을 전송하여 대규모 서비스 거부(DoS) 공격을 수행하였다[5,13].

피해 현황은 FirstEnergy의 방화벽이 악성 트래픽을 차단하여 피해가 발생되지 않았다[5,13].

Ⅳ. 국내외 사이버 위협 분석

국내의 사이버보안 규제 대상 원자력시설은 현재 19

개 사업소로, 여기에는 한국수력원자력 원자력발전소(13개 발전사업소/25호기), 한국원자력연구원 연구용 원자로(하나로), 한전원자력연료 핵연료가공시설, 한국원자력환경공단 방사성폐기물 관리시설(월성 환경관리센터, 대전 RI폐기물관리시설/2개 사업소), 대단위 방사선조사시설(그린피아기술(주), ㈜소야그린텍/2개 사업소)이 포함된다.

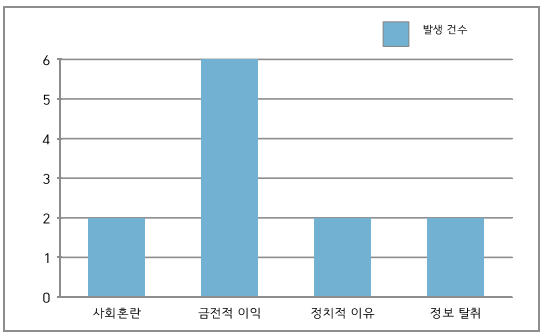
잠재적으로 국내 원자력시설에 위협을 가할 수 있는 세력으로는 북한 테러 조직, 해외 테러 조직, 국내 불만 세력 등을 들 수 있으며, 특히 2014년 12월 원자력발전소 대상 사이버 위협이 대대적으로 발생하여 사회혼란을 야기한 사례로 보아 원자력시설 대상 사이버 위협은 매우 현실적임을 알 수 있다.

이에 따라, 3장에서 분석된 사이버 위협 유형별 사건 41건을 국내와 국외로 구분하여 심층 분석하였다.

4.1. 국내 사이버 공격 행위 분석

2015년에서 2017년 사이 발생한 국내 주요 사이버 사건은 총 12건이다. 2015년에 발생한 사이버 사건은 총 2건으로 해킹 1건과 서비스거부 공격 1건으로 분석되었으며, 2016년에 발생한 사이버 사건은 총 4건으로 해킹 2건, 컴퓨터바이러스 1건, 논리·메일폭탄 1건으로 분석되었다. 2017년은 주요 사이버 사건이 가장 많이 발생되었으며, 총 6건의 세부 유형으로는 해킹 2건, 논리·메일폭탄 2건, 서비스거부 공격 2건으로 분석되었다 [4].

국내에서 발생된 주요 사이버 사건을 정밀히 분석하기 위해 공격 목적, 공격 경로, 공격 자원에 대한 통계 자료를 작성하였다. 먼저 공격 목적은 사회 혼란, 금전적 이익, 정치적 이유, 정보 탈취로 구분되며, 자세한 현황은 그림 7과 같다.



〔그림 7〕 국내 주요 사이버 사건에 대한 공격 목적 분석

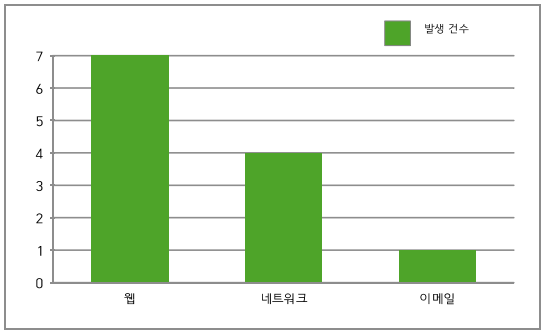
공격 목적 중 금전적 이익을 목적으로 가장 많은 사이버 사건이 발생되었으며, 특히 비트코인을 이용한 금전 갈취가 대표적인 공격 목적으로 분석되었으며, 기타 공격 목적으로 사회혼란, 정치적 이유, 정보 탈취가 각 2회씩 분석되었다.

공격 경로는 웹, 네트워크, 이메일로 구분되며, 자세한 현황은 그림 8과 같다.

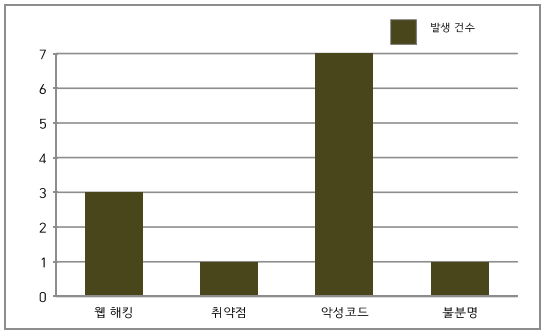
공격 경로 중 웹을 통한 사이버 공격이 가장 많이 발생되었으며, 네트워크를 이용한 사이버 공격도 4회로 분석되었으며, 이메일을 통한 사이버 공격은 1회로 분석되었다.

공격 자원은 웹 해킹, 취약점, 악성코드로 구분되며, 자세한 현황은 그림 9와 같다.

공격 자원 중 악성코드를 이용한 사이버 공격이 총 7회로 가장 많이 발생되었다. 또한, 웹 해킹을 이용한 사이버 공격도 3회로 분석되었으며, 취약점 및 공격 자원을 분석할 수 없는 사건이 각 1회로 분석되었다.



〔그림 8〕 국내 주요 사이버 사건에 대한 공격 경로 분석



〔그림 9〕 국내 주요 사이버 사건에 대한 공격 자원 분석

4.2. 국외 사이버 공격 행위 분석

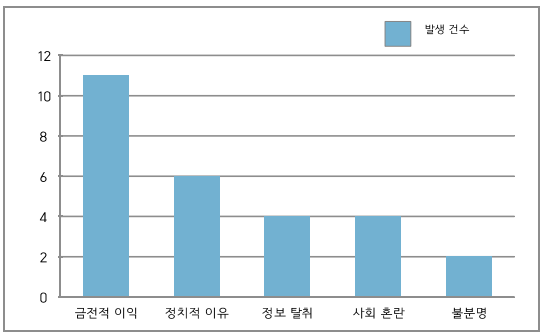
2015년에서 2017년 사이 발생한 국외 주요 사이버 사건은 총 27건이다. 2015년에 발생한 사이버 사건은 총 5건으로 해킹 2건, 컴퓨터바이러스 1건, 서비스거부 공격 2건으로 분석되었다. 2016년은 주요 사이버 사건이 가장 많이 발생되었으며, 총 15건의 세부 유형으로는 해킹 6건, 컴퓨터바이러스 6건, 논리·메일폭탄 2건, 서비스거부 공격 1건으로 분석되었다. 2017년에 발생한 사이버 사건은 총 7건의 세부 유형으로는 해킹 5건, 컴퓨터바이러스 1건, 논리·메일폭탄 1건으로 분석되었다[4].

국외에서 발생된 주요 사이버 사건을 정밀히 분석하기 위해 공격 목적, 공격 경로, 공격 자원에 대한 통계 자료를 작성하였다. 먼저 공격 목적은 금전적 이익, 정치적 이유, 정보 탈취, 불분명으로 구분되며, 자세한 현황은 그림 10과 같다.

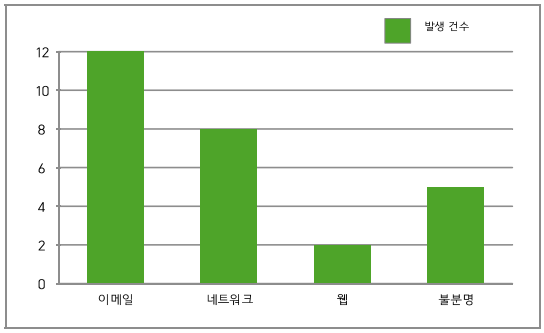
공격 목적 중 금전적 이익을 목적으로 발생한 사이버 사건이 11회로 가장 많았으며, 금전적 이익의 주요 목적은 비트코인을 이용한 금전 갈취가 대표적으로 분석되었다. 또한 정치적 이유로 6건의 사이버 사건이 발생되었으며, 정보 탈취와 사회 혼란 목적으로 각 4건의 사이버 사건이 발생되었다. 또한, 공격 목적이 불분명한 사이버 사건이 2회로 분석되었다.

공격 경로는 이메일, 네트워크, 웹, 불분명으로 구분되며, 자세한 현황은 그림 11과 같다.

공격 경로 중 이메일을 통한 사이버 사건이 총 12회로 가장 많이 발생되었으며, 네트워크를 이용한 사이버 사건이 8회로 다음으로 많이 발생되었다. 또한, 웹을 통한 사이버 사건이 2회 발생되었고 공격 경로가 불분명한 사이버 사건도 총 5회로 분석되었다.



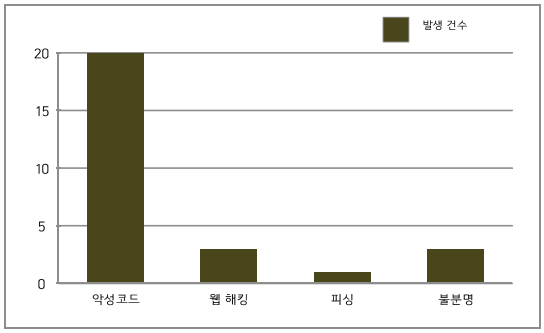
〔그림 10〕 국외 주요 사이버 사건에 대한 공격 목적 분석



〔그림 11〕 국외 주요 사이버 사건에 대한 공격 경로 분석

공격 자원은 악성코드, 웹 해킹, 피싱, 불분명으로 구분되며, 자세한 현황은 그림 12와 같다.

공격 자원 중 악성코드를 이용한 사이버 사건이 총 20회로 가장 많이 발생되었으며, 주로 랜섬웨어를 이용한 사이버 공격으로 분석되었다. 또한, 웹 해킹을 이용한 사이버 사건은 3회로 분석되었으며, 피싱을 이용한 사이버 사건은 1회로 분석되었다. 공격 자원을 분석할 수 없는 사이버 사건이 총 3회로 분석되었다.



〔그림 12〕 국외 주요 사이버 사건에 대한 공격 자원 분석

Ⅴ. 결 론

본 논문은 2015년부터 2017년 사이에 발생한 사이버 위협 사례 중 방사능방재법의 전자적 침해행위의 유형에 따라 해킹 공격, 컴퓨터바이러스 공격, 논리·메일폭탄 공격 및 서비스거부 공격에 해당하는 사이버 사건을 분석하였다.

나아가 국내·외 사이버보안 위협 분석을 위해 2015년부터 2017년까지 주요 사이버 사건 41건에 대해 국내(12건)와 국외(27건)로 구분하여 분석하였으며, 공격 목적, 공격 경로 및 공격 자원을 심층 분석하였다.

특히 취약점을 이용해 전 세계적으로 피해를 일으킨 랜섬웨어, 우크라이나 대규모 정전을 일으킨 악성코드 등과 같이 주요 사이버 사건들에 대한 분석 자료를 활용하여 현재 설정된 사이버보안 분야 설계기준위협의 적절성을 평가할 수 있다. 또한, 향후 개정될 사이버보안 분야 설계기준위협 재설정 과정에서 분석 자료를 활용하여 위협 속성을 추가 보완할 수 있을 것으로 기대된다.

참 고 문 헌

[1] 한국원자력통제기술원, “원자력시설 등의 방호 및 방사능 방재 대책 법령집”, pp. 1-11, 2017.

[2] 한국원자력통제기술원, “원자력시설등의 물리적방호 관련 사무편람”, pp. 6-10, 2016.

[3] IAEA, “Development, Use and Maintenance of the Design Basis Threat,” pp. 3-7, 2009.

[4] 한국원자력통제기술원, “핵물질 및 원자력시설 위협평가서”, pp. 155-283, 2017.

[5] 한국원자력통제기술원, “연도별 사이버 사건 분석보고서”, pp. 22-111, 2017.

[6] Reuters, "http://www.reuters.com/article/us-ukraine-crisis-cyber-attacks-idUSKBN1491ZF", 2016.

[7] News1, "http://news1.kr/articles/?3042189", 2017

[8] ICS-CERT, "https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01", 2016

[9] Arstechnica, "https://arstechnica.com/security/2016/04/german-nuclear-plants-fuel-rod-system-swarming-with-old-malware/", 2016

[10] Secureworks, "https://www.secureworks.com/research/threat-group-4127-targetshillary-clinton-presidential-campaign", 2016

[11] UK Parliamentary, "http://www.parliament.uk/business/news/2017/june/cyber-incident/", 2017

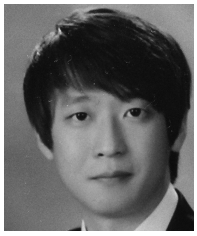
[12] CCN, "https://www.cryptocoinsnews.com/dont-pay-bitcoin-ransoms-south-korean-govt-tells-banks-facing-ddos-threats/", 2017

[13] E&E News, "https://www.eenews.net/stories/1060026735", 2015

〈저 자 소 개〉

송 동 훈 (SONG DONG HOON)
정회원

2012년 2월 : 부산대학교 전자전기공학부 졸업
2012년 1월~2015년 8월 : 한국전력기술 기술원
2015년 8월~현재 : 한국원자력통제기술원 사이버보안실 연구원
관심분야 : 사이버보안, EMP 방호



임 현 종 (LIM HYUN JONG)
정회원

2014년 8월 : 고려대학교 방사선학과 졸업
2016년 8월 : 고려대학교 바이오융합공학과 석사
2016년 7월~현재 : 한국원자력통제기술원 사이버보안실 전문연구원
관심분야 : 제어시스템 보안, 네트워크 보안

김 상 우 (KIM SANG WOO)
정회원

2013년 2월 : 충남대학교 컴퓨터공학과 졸업
2015년 2월 : 충남대학교 컴퓨터공학과 석사 졸업
2015년 2월~현재 : 한국원자력통제기술원 사이버보안실 연구원
관심분야 : 제어시스템 보안, 네트워크 인증

류 진 호 (RYU JIN HO)
정회원

2015년 8월 : 서울대학교 원자핵공학과 졸업
2017년 8월 : 서울대학교 원자핵공학과 석사 졸업
2017년 8월~현재 : 한국원자력통제기술원 사이버보안실 연구원
관심분야 : 해체원전 사이버보안, 제어시스템 보안

신 익 현 (SHIN ICK HYUN)
정회원

2004년 8월 : 뉴욕 시립대학교 컴퓨터 사이언스학과 졸업
2014년 8월 : KAIST 정보보호대학원 석사 졸업
2005년 8월~현재 : 한국원자력통제기술원 사이버보안실 선임연구원

관심분야 : 제어시스템 보안, 기반보호 정책, 사이버보안 전략