情 報 保 護 學 會 誌
第20卷 第4號, 2010. 8

전자적 제어시스템 침해 위협에 따른 법적 대응방안

임 종 인*, 장 규 현**

요 약

최근 기존 폐쇄적 제어시스템 환경에서 네트워크를 통해 연결되는 개방형 제어시스템으로 변화하는 등 전자적 제어시스템의 정보통신기술에 대한 의존도가 더욱 심화되고 있다. 전자적 제어시스템은 효율성을 높이고 사회 전반의 편의성을 증진시켰으나, 정보통신기술의 취약성이 전이됨에 따라 안전하게 보호되어야할 제어시스템은 위협에 노출되고 있는 것이 현재 상황이다. 전자적 제어시스템 침해사고 발생 시 제어시스템의 특성 상 많은 피해 및 사회적 혼란을 초래할 수 있기 때문에, 국가 차원에서 법률적인 보호조치가 필요하다. 국내에서는 2001년 「정보통신기반 보호법」이 시행되어 국가정보통신기반시설에 대한 보호 및 사고 대응을 규정하고 있다. 본 논문에서는 실제 발생한 제어시스템 침해사고를 분석을 통해 전자적 제어시스템의 위협요인 및 이에 따른 대응방안을 모색한다. 또한 제어시스템 위협에 가장 선도적으로 대응하고 있는 미국의 법제 분석을 통해 전자적 제어시스템 침해 위협에 따른 법적 대응방안에 대하여 연구하고자 한다.

Ⅰ. 서 론

정보통신기술(Information Communication Technology)의 발전으로 인하여 사회 전반의 디지털화 및 유비쿼터스 환경이 촉진되고 있는 추세이다. 산업 환경에도 정보통신기술이 적용되어 전자적 제어시스템이 출현하였으며 제어시스템에서 정보통신기술에 대한 의존도가 더욱 심화되고 있다. 최근에는 기존 폐쇄적인 제어시스템 환경이 네트워크로 연결되어 네트워크를 통해 제어시스템을 운영 및 관리하는 개방형 제어시스템이 산업 환경에서 사용되고 있다. 제어시스템에 정보통신기술이 적용됨에 따라 정보통신기술의 취약성은 제어시스템으로 전이되었으며, 이러한 취약성을 통한 사고 사례가 발생하고 있다.

국가기반시설인 전기·발전·교통·통신 분야에도 전자적 제어시스템이 적용되어 널리 사용되고 있다. 국가기반시설에 대한 전자적 침해사고 발생 시에는 기반시설의 마비로 인하여 사회적 혼란 등 많은 피해가 발생할 것으로 예상된다. 이러한 기반시설에 대한 침해 사고의 위험성은 실제로 '2003년 미 북동부 대정전사태'에서 볼 수 있었다. 2003년 발생한 정전사태는 미국 북동부 및 캐나다 온타리오 주 등에서 48시간여 동안 지속되었으며 5500만 명의 사람이 피해를 입었다. 이 사고의 직접적 원인은 송전선의 문제로 밝혀졌지만, CIA는 영국 SANS교육원에서 열린 컨퍼런스에서 사이버공격이 이 정전사태의 원인 중 하나였다고 밝혔다.[1] 이 정전사고로 인하여 수자원 공급이 중단되었으며 교통 및 통신 등에 장애가 발생함에 따라 많은 시민들이 불편을 겪었으며 사회가 마비되어 큰 혼란이 있었다. 이처럼 국가기반시설에 대한 사이버 공격은 사회적으로 큰 혼란을 야기할 수가 있기 때문에 국가기반시설에 대한 보호가 반드시 필요하다.

국가기반시설에 대한 사이버 공격의 위험성은 이미 1990년대 중반에 예견되었으며 각국은 이에 대응하기 위하여 법제 등을 정비하였다. 미국은 가장 선도적으로 사이버공격에 대한 대응을 준비하였으며 2001년 9·11 테러 이후로 더욱 적극적으로 대응하고 있다. 우리나라 역시 2001년 「정보통신기반 보호법」을 제정하여 기반시설에 대한 보호 및 대응을 규정하고 있다. 하지만 2001년 제정 당시와 현재는 환경의 변화에 따라 이를 반영할 필요성이 있으며, 국내외에서 제어시스템의 실제 사고 사례가 발생하였기 때문에 사고 사례 반영의

* 고려대학교 정보경영공학전문대학원 원장 (jilim@korea.ac.kr)
** 고려대학교 정보경영공학전문대학원 석·박사통합과정 (wannab@korea.ac.kr)

필요성이 제기되고 있다.

본 논문에서는 전자적 제어시스템의 주요 침해 사례를 분석하고 미국의 제어시스템 보안 관련 법제와 국내 「정보통신기반 보호법」의 비교를 통하여 전자적 제어시스템 침해 위협에 따른 법적 대응방안에 대하여 알아보고자 한다.

Ⅱ. 전자적 제어시스템 침해 사고 및 대응 사례

2.1 워싱턴주 올림픽 파이프라인 사고(1999)

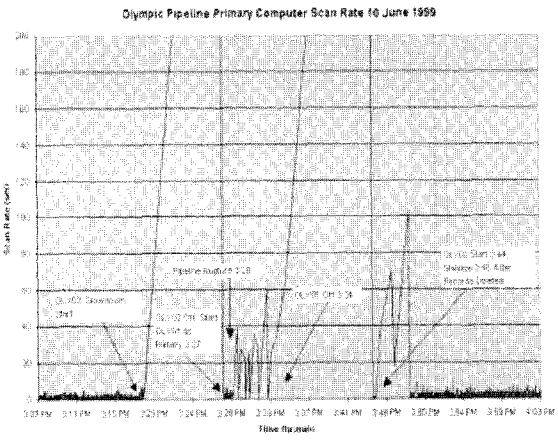
1999년 6월 10일, 미국 워싱턴주 Whatcom Falls Park 지역에서 Olympic Pipeline 社의 16인치 직경의 가솔린 송유관이 파열되어 가솔린이 유출되는 사고가 발생하였다. 유출된 가솔린은 90여 분 후 점화되어 유출지점에서 약 2.5km 떨어진 지점까지 달하는 화재가 발생하였다. 이 유출 및 화재로 인해 3명이 사망하고 8명이 부상을 당했으며 많은 환경 파괴를 일으켰다.[1]

미국 연방교통안전위원회(National Transportation Safety Board)는 2002년 Olympic Pipeline 사고의 조사 결과 발표를 통해 추정 사고원인 5가지를 발표하였다.[2] 이 5가지 원인은 (1) 1994년 IMCO (Intercontinental Manufacturing Company) 社의 폐수처리 플랜트 개선 공사 중 건설현장 근로자에 의한 파이프라인 파손 (2) IMCO 社의 파손에 대한 Olympic Pipeline 社의 부정확한 파이프라인 검사 (3) Bayview 생산 시설과 관련된 모든 안전시설에 대해 예상 작동 환경에서 실험하지 않은 점 (4) Bayview 유입차단밸브의 지속적인 의도치 않는 차단 문제에 대한 Olympic Pipeline 社의 조사 및 개선 실패 (5) 그리고 파이프라인 운영 중 SCADA 시스템 DB 작업을 수행함에 따른 SCADA 시스템 미응답이다.

Olympic Pipeline 社의 SCADA 시스템은 사고 당일 약 90여 분간 응답을 하지 않아 사고의 주요 원인으로 지적이 되었으며, 조사 결과 Olympic Pipeline 社의 SCADA 시스템은 지속적인 문제를 가지고 있던 것으로 밝혀졌다.[3] 1998년 12월 Bayview 터미널이 도입된 이후, 사고가 발생한 1999년 6월 까지 Bayview 지점의 고압으로 인한 총 41번의 예상치 못한 유입차단밸브의 차단이 있었다. 유입차단밸브의 예상치 못한 차단 시 SCADA 운영자는 압력을 분산하였는데 이는 결과적으로 IMCO 社의 공사 중 파손으로 인해 약해진 파이프라인에 높은 압력을 주어 파이프라인이 파열되는 원인이 되었다. NTSB는 사고 당일 높은 압력에 대한 경고 및 유출의 위험성에 대한 통지가 SCADA 시스템에 통보되었다면 사고는 막을 수 있었다고 판단하였으며, 따라서 SCADA 시스템의 미응답은 유출 사고의 잠정 원인으로 판단되었다.

사고 당일인 1999년 6월 10일, 15시 경에 SCADA 시스템 운영자는 가솔린 전송 시점을 변경하였으며, 이에 대해 OLY-02 시스템 관리자는 이 두 가지 변경을 DB에 입력하였다. 10분 후 SCADA 컴퓨터는 이 DB에 대해 에러 메시지를 출력하였으며, 시스템 관리자는 이 메시지 및 기록에 대해 체크하고 15분 간 자리를 비웠다. OLY-02 SCADA 시스템은 그 후 응답이 불규칙하다가 15시 24분경 연결이 끊어졌으며, 15시 28분에 파이프라인이 유출되었다. 이후 15시 48분 경 문제가 되었던 새로운 DB 입력 값을 삭제하자 OLY-02 SCADA 시스템은 그 다시 정상적으로 운영되기 시작하였으나 16시 29분에야 유출 알람 메시지가 발생되었다. [그림 1][4]은 이 OLY-02 시스템의 주사선변화(Scan rate)를 나타낸 그래프로, SCADA 시스템 응답에 문제가 있었다는 사실을 그래프를 통해서 알 수 있다.

2001년 9월, 연방대배심(Federal Grand Jury)은 Olympic Pipeline 社와 이를 보유한 Equilon Pipeline 社를 기소하였다.[5] 또한 Olympic Pipeline 社의 매니저와 모니터링 직원, 그리고 파이프라인 제어 직원을 「Hazardous Liquid Pipeline Safety Act of 1979」와 「Clean Water Act of 1986」의 위반으로 역시 기소하였다. 2002년 6월 워싱턴주 환경부(Washington



[그림 1] Olympic Pipeline OLY-02 시스템 주사선변화

State Department of Ecology)는 Olympic Pipeline 社와 Equilon Pipeline 社에 대하여 각각 786만 달러의 벌금을 부과하였다. 2002년 5월에는 미국 법무부(U.S. Justice Department)에서 3,700만 달러에 달하는 민사소송을 제기하였다. 2002년 12월 두 회사는 시애틀 지방법원(U.S. District Cout, Seattle)에서 「Hazardous Liquid Pipeline Safety Act of 1979」의 위반과 「Clean Water Act of 1986」의 위반으로 유죄판결을 받았다. 이 유죄판결로 인하여 3,600만 달러의 벌금을 선고받았으며, Equilon 社를 인수한 Shell Oil 社는 자사의 2,100 마일에 달하는 미국 파이프라인에 대하여 파손예방 프로그램 조치의 수행으로 6,100만 달러에 대하여 추가로 투입할 것으로 결정하였다.

2.2 캘리포니아 TCCA 社 운하 제어시스템 해킹 사고 (2007)

2007년 11월 미국 California 주 Willows 지역의 운하를 운영하는 Tehama Colusa Canal Authority 社의 전직 직원이 SCADA 시스템을 침해한 혐의로 기소되었다.[6]

61세의 TCCA 社의 전직 전자 관리자인 Michal Keehn은 2007년 8월 15일 경 TCCA 社의 SCADA 시스템에 권한 없이 접근하여 수로를 관리하는 컴퓨터에 소프트웨어를 설치하여 피해를 입혔다. TCCA 社는 연방 정부에서 관리하는 Colusa 운하와 Corning 운하를 운영하는 회사이다. Michal Keehn은 TCCA 社의 SCADA 시스템에 침입하여 악성소프트웨어를 설치하였으며 이 소프트웨어로 인해 Sacramento River의 수로를 제어하는 컴퓨터가 마비되었다. TCCA 社는 이 마비로 인해 수동으로 제어를 하였으며, 이 침해 사고로 인해 TCCA 社는 $5,000 이상의 손해를 입었다고 美 법무부 차관 Robin Taylor가 밝혔다.

2.3 호주 퀸즈랜드 오폐수 처리 제이시스템 해킹 사고 (2000)

호주 Queensland의 Maroochy Shire Council의 오폐수처리 시설의 제어시스템이 이 제어시스템을 설치한 회사의 전직 직원에 의해 침해당하여 오폐수가 무단으로 방출되는 사고가 발생하였다.[7]

본 사고는 Queensland Maroochy Shire Council의 오폐수처리시설 제어시스템 설비를 설치한 Hunter Watertech 社의 직원이던 Vitek Boden이 제어시스템에 침해하여 발생하였다. Boden은 Hunter Watertech 社에서 2년간 IT/제어시스템 기술 지원으로 근무하다가 회사와의 관계가 껄끄러워지자 사임하였으며, 이후 Maroochy Shire Council에 지원했으나 채용되지 못했다. 이에 Maroochy Shire Council과 Hunter Watertech 社 모두에 적개심을 품고 오폐수처리 제어시스템을 침해한 것으로 밝혀졌다.

Boden은 그의 차에 도난 무선 장비와 컴퓨터 등을 설치하여 Wardriving[1] 방식으로 오폐수처리 제어시스템을 공격하였다. Boden은 특정 하수 처리 시설의 펌프 장치를 제어하는 컴퓨터에 접속하여 악성 프로그램을 설치하여 전자 정보를 교체하는 방식으로 공격을 하였으며 이는 이 장치의 오작동을 야기하였다. 펌프 장치는 가동이 필요할 때 가동되지 못했고, 중앙제어시스템으로 알람이 보고되지 않았으며, 중앙제어시스템과 펌프 장치들 간의 통신이 이루어지지 않았다.

이와 같은 방식으로 2000년 2월 28일부터 4월 23일까지 총 46번 해킹이 이루어졌으며, 이로 인하여 약 80만 리터의 폐수가 무단으로 방출되었으나 이는 탐지되지 않았다. 이렇게 방출된 폐수는 공원, 강, 호텔로 유출되어 환경 파괴 등의 문제를 발생시켰다. Boden은 신호위반으로 경찰에 단속되는 과정에서 우연히 검거되었으며, 그의 차량에서 발견된 노트북 등을 증거로 기소되었다. Boden은 악의적으로 환경을 파괴한 혐의로 12개월형을, 30회 의상의 컴퓨터 해킹 및 절도 등의 혐의로 2년형을 선고받았다.

2.4 시사점

상기에서 분석한 3건의 사고 사례는 제어시스템 사고 중 대표적인 사례로 공통적인 특징은 3건의 사고 모두 외부인의 침입이 아닌, 내부 직원의 실수 및 전직직원에 의한 침해사고라는 것이다. 이는 폐쇄적인 제어시스템의 특성상 외부망과 분리되어 구성되고, 외부 접속에 대한 방화벽 등의 기술적 보호조치가 마련되었기 때문에 외부인의 침입이 쉽지 않았다고 해석할 수 있다.

1) 1983년 영화 'WarGames'에서 유래한 용어로, 주로차량을 이용하여 접속 가능한 무선네트워크 AP를 찾아내 이 AP를 통해 침해하는 해킹 방식

전직 직원의 경우 내부 시스템에 대한 지식이 있어 상대적으로 취약점을 잘 알 수 있다.

Olympic Pipeline 社 유출사고의 경우, 직원의 실수에 의한 오작동 및 제어시스템의 오류 발생에도 자리를 비우는 등 대처에 문제가가 있었다. TCCA 운하 및 퀸즈랜드 오폐수 처리 제어시스템 침해 사고의 경우 내부 시스템에 대한 지식을 갖고 있는 전직 직원에 의한 사고이다. 본 사고들의 분석 결과 내부의 취약성 역시 제어시스템에 있어 중요한 고려 요인이며, 내부 위협에 대한 보호조치의 마련이 필요하다는 것을 알 수 있다.

Ⅲ. 미국의 제어시스템 보안 관련 법제 분석

미국 법체계는 법(Act) · 조약(Treaty) · 행정명령(Executive Order) · 규칙(Rule) 등으로 구성되어 있으며, 미국 법체계에서 효력은 "연방헌법 - 연방법률 · 조약 · 판례 - 연방 행정명령 · 연방 행정규칙 - 주헌법 - 주법률 - 조례"의 순을 갖는다.[8] 따라서 미국의 제어시스템 보안 관련 법제를 분석하기 위해서는 법(Act)뿐만 아니라 전반적인 법제 및 각 법제들의 재정배경과 정책 등에 대한 분석이 필요할 것이다. 본 절에서는 미국의 제어시스템 보안 법제 및 정책의 개관을 살펴보고 세부 법에 대해서 분석하고자 한다.

3.1 미국 제어시스템 보안 관련 정책 개관

3.1.1 클린턴 정부

미국은 1996년 Computer Fraud and Abuse Act(18 U.S.C. § 1030)의 개정 법률인 「National Information Infrastructure Protection Act of 1996」 제정을 통해 국가 정보시스템에 대한 보호를 규정하기 시작하였다.[9] 동 법은 미국 정부의 행정명령 · 주 정부의 보호 정보 등에 대한 권한이 없거나 권한을 초과하는 접근(without authorization or exceeding authorized access) 등을 규제하고 있다.

같은 해 7월, 동 법과 컴퓨터 보안 관련 상원 청문회(Senate Hearings on Computer Security)의 결과 등을 바탕으로 클린턴 대통령은 주요기반시설에 대한 컴퓨터 기반 공격에 대한 대응을 위해 「Executive Order No.13010. Critical Infrastructure Protection」에 서명하였다. 이 명령을 통하여 주요기반시설에 대하여 연구하며, 광범위한 분야의 위협에 대하여 결정하고 장기적인 보안 정책을 대하여 제시하는 기구인 주요기반시설 대통령자문위원회(President's Commission on Critical Infrastructure Protection, PCCIP)가 설립되었다. PCCIP는 1997년 "Critical Foundations : Protecting America's Infrastructures"라는 리포트를 통해 피해를 입기 전 사이버 위협으로부터 기반시설을 보호하기 위한 방법론 개발의 필요성을 역설하였다.[10]

이 리포트를 기반으로 1998년 클린턴 대통령은 「Presidential Decision Directive 63, (PDD63)」을 공표하였다.[11] PDD63은 美 행정부(Executive Branch)로 하여금 국가주요기반시설에 대한 위협을 평가하고 연방 및 주 정부로 하여금 책임을 지도록 하고 있다. 또한 PDD63은 국가기반시설보호센터(National Infrastructure Protection Center, NIPC), 중요정보기반보장국(Critical Infrastructure Assurance Office, CIAO), 국가기반보장위원회(National Infrastructure Assurance Council, NIAC) 및 민간 분야의 정보공유분석센터(Information Sharing and Assessment Centers, ISAC)의 설립 등을 통하여 주요기반시설의 각 부문에서 사용되는 시스템의 보호 및 정보의 공유에 대하여 규정하고 있다.

2000년 1월 백악관은 PDD63에 대한 노력의 일환으로 「National Plan for Information System Protection」을 발표하였다. 이는 주요기반의 보호를 위해 필요한 안전장치(Safeguard)를 만들기 위한 종합적인 계획으로 정부와 민간의 협력을 강조하고 있다. 이 프로그램들은 주요기반시설의 자산 및 위협을 식별하여 공격을 탐지하고 이에 대응하며, 이를 위하여 기술의 연구 및 개발 · 교육 · 인식 제고 · 법률 정비 · 프로그램에 있어 자국민의 프라이버시 보호 등을 담고 있다.

3.1.2 조지 W. 부시 정부

미국 정부의 제어시스템 보호에 대한 노력은 2001년 조지 W. 부시 정부 하에서 9·11 테러를 기점으로 급격한 변화를 맞이한다.[12] 2001년 10월 부시 대통령은 「Executive Order 13228, Establishing the Office of Homeland Security and the Homeland Security Council」과 「Executive Order No.13231. Critical Infrastructure Protection in the Information Age」을 잇달아 승인하였다. EO13228은 테러로부터 자국을 보

호하기 위한 정책을 담당하는 대통령실산하국토안보실(Executive Office of the President an Office of Homeland Security)과 국토보안위원회(Homeland Security Council)를 설립하도록 명시하였다. 또한 EO13231은 주요기반시설 보호 관련 정책을 조정하는 대통령 직속 주요기반시설보호위원회(President's Critical Infrastructure Protection Board)를 설립하도록 하여 정보시스템 보호 프로그램을 조정하고 정책을 권고하는 역할 등을 명시하였다.

이는 「Homeland Security Act of 2002」 입법으로 이어졌으며, 동 법을 통해 국토안보부(Department of Homeland Security, DHS)를 창설하여 분산 된 테러 대응 역량을 국토안보부에 집중시켰다. 또한 「Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001」을 통해 테러에 대응하기 위한 정보기관들의 정보 수집의 제약 및 정보기관 간의 정보 공유의 제약을 없앴으며, 테러 방지 및 주요기반시설을 위한 정보공유센터 설립을 규정하였다. 국토안보부는 주요기반시설보호와 관련한 일련의 전략 및 계획(Strategy & Plan)을 발표하였으며 이는 [표 1]과 같다.

〔표 1〕 국토안보부의 주요기반시설보호 관련 전략 및 계획

Strategy/Plan	주요기반시설보호 관련 내용
National Strategy for Homeland Security (2002)	각종 위협으로부터 국토의 안전과 자국민의 보호를 위한 적극적 대응 전략 주요기반시설을 연결하고 제어하는 정보 및 통신 부분의 중요성 강조 주요기반시설의 물리적·사이버 보호를 위하여 국토안보부의 책임 명시 제어시스템 관련 '내부자(Insider)'와 관련된 위협을 명시하였으며, 내부자 위협을 방지하기 위하여 보증인 프로그램 · 심사 및 배경 조사 국가 표준 제안 등 명시
National Strategy for the Physical Protection of Critical Infrastructure and Key Assets (2003)	물리적 공격으로부터 국가 주요기반시설과 핵심 자산을 보호하여 테러에 노출되는 국가 취약점 줄이기 위함 다음의 전략적 목적 명시 · 공중보건과 안전, 지배구조, 경제-국가적 안보, 공공 신뢰를 위한 국가적 중요성 측면에서 가장 주요한(crucial) 것으로 여겨지는 기반시설과 자산을 식별하고 이들에 대한 보호를 보장하는 것. · 적시에 경고를 해주는 것. · 시간이 흐르면서 테러리스트들의 목표물이 될 수도 있는 다른 기반 시설들과 자산들의 보호를 보장하는 것
National Strategy to Secure Cyberspace (2003)	사이버공간 방어를 위한 단일대응체계 구축 등 사이버 보안 관련 5대 현안과 이에 대응하는 권고조치를 내용으로 함 미국의 주요기반시설에 대한 사이버 공격 예방, 사이버 공격에 대한 국가적 취약점 감축, 사이버 공격 발생 시 피해 및 복구기간 최소화가 목표 5대 현안은 다음과 같음 · 국가 사이버공간 방어 대응체계 구축 · 국가 사이버 위협 제거 및 취약점 보완 · 국가 사이버공간 방어 관련 인식 제고 및 교육 프로그램 · 정부 부문 사이버공간 방어 · 국가 안보 및 국제 사이버 방어 협력 강화 상기 현안에 대한 정부의 대응방안은 다음과 같음 · 엔터프라이즈 아키텍처 구축 · 위협 및 취약점에 대한 지속적 평가 · 연방시스템 이용자에 대한 인증 및 유지관리 · 연방 무선 LAN 보안 · 아웃소싱 및 조달의 보안 강화 기관의 보안성 검증을 위한 구체적 기준 마련
National Infrastructure Protection Plan (2006)	「Homeland Security Presidential Directive 7」에 의해 2006년 수립, 2008년 업데이트 및 2009년 개정 미국 내 테러 위협 및 기타 위협에 대한 정보 공유 및 이해 증진, 주요기반시설 및 핵심 자산(Critical Infrastructure and Key Assets, CI/KA) 보호 프로그램 실시를 위한 안전한 정보공유 파트너쉽 수립, 장기적인 위험 관리 프로그램 실시, 효율적 주요기반시설 및 핵심 자산 보호를 위한 자원의 최대 활용 등을 목표 국가 주요기반시설 보호를 위한 연구개발 계획 수립 및 로드맵 작성 국가 주요기반시설 및 핵심 자산을 대표하는 17개 부문 관련 연방·주·지역·기관의 대표자들로 구성된 정부부처조정위원회(Government Coordinating Council) 구성 및 주요자산의 소유자-운영자 대표 또는 민간 영역 대표자로 구성되는 부문조정위원회(Sector Coordinating Council)의 자발적 구성을 장려 2009년 개정 된 주요 내용은 다음과 같음 · 부문별 세부 계획 발표 · 지역 컨소시엄 조정위원회 포함 부문별 파트너쉽 모델 확장 · 기반시설 정보 수집 시스템과 기반시설 데이터 웨어하우스로 국립 자산 데이터베이스 진화 · 위험 관리 프레임워크 구현을 위한 프로그램·접근방식·도구 개발 · 교육·훈련·복지 프로그램 등의 검토 · 국가대응계획으로부터 국가대응프레임워크로 진화

2008년 부시 대통령은 NSPD-54/HSPD-23(National Security Presidential Directive 54/Homeland Security Presidential Directive 23)을 기반으로 국가사이버보안 종합계획(Comprehensive National Cybersecurity Initiative, CNCI)을 발표하였다. CNCI는 사이버 위협에 대하여 분석하고 미래 사이버보안 환경을 강화 등이 목적이며 이를 위하여 주요기반시설 보안을 포함한 12가지 세부 계획(Initiative)을 수립하였다.

3.1.3 오바마 정부

2009년 1월 취임한 오바마 대통령 역시 사이버보안을 미국이 직면한 가장 심각한 과제라고 밝히고, CNCI를 수용하였으며 CNCI는 오바마 정부의 「Cyberspace Policy Review」의 주요 정책을 달성하기 위한 핵심적인 요소라 밝혔다.

오바마 대통령은 취임 전 국제전략연구소(Center for Strategic and International Studies, CSIS)의 사이버보안 임무에 관한 보고서(Commission on Cybersecurity for the 44th Presidency) 등을 통하여 사이버보안에 대한 정책을 준비하였다. 오바마 대통령은 취임 이후 사이버 보안 예산 증액, 정보보안 총괄을 위한 사이버보안조정관(Cybersecurity Coordinator)의 임명, 그리고 「Cyberspace Policy Review」를 발표와 같은 일련의 행보를 이어나갔다. 「Cyberspace Policy Review」의 주요 내용에는 주요기반시설 보호를 위한 내용이 포함되어 있다.

3.2 미국 제어시스템 보안 관련 법제 분석

3.2.1 Homeland Security Act of 2002

미국의 테러 대응이 과거 물리적 테러 대응에 초점이 맞추어져 있었다면 최근의 테러 대응 정책은 화·생·방의 고위험물질의 사용과 함께 최첨단 기술을 이용한 테러에 대비하기 위한 종합적 대응전략에 초점을 두고 있다. 또한 최근 IT기술의 발전에 따라 IT 기술을 이용한 이른바 '사이버 테러'에 대한 대응책도 종합적 테러 대비책의 일환으로 자리 잡아 가고 있다. 이를 위하여 미국은 2002년 6월 6일, 테러대책을 총괄하는 국토안보부(DHS)의 창설이 논의되었고, 2002년 11월 「Homeland Security Act of 2002」를 제정하여 조직 설립에 대한 법적 근거를 확보하였다. 동 법의 주요 내용을 살펴보면 다음과 같다.

먼저, 국토안보부(DHS) 장관을 보좌하기 위하여 정보분석및기반시설보호국(Information Analysis & Infrastructure Protection, 이하 IAIP)을 설치하여 각각 차관에 해당하는 이를 임명하여야 하고, 정보분석 담당 차관보와 기반시설보호 담당 차관보를 두어 차관을 보좌하도록 하고 있다. 정보분석 및 기반시설보호 차관은 장관의 명령 및 통제 하에 미 국토에 대한 테러리스트의 위협의 본질 및 범위를 식별하고 평가, 미국에 대한 테러리즘의 위협을 감지하고 식별 그리고 국토의 현재 취약성과 잠재적인 취약성에 비추어 당해 위협을 이해하는 업무에 대하여 책임을 진다.

또한 전력 생산, 발전 및 배전 시스템, 정보통신기술 및 전기 통신 시스템(위성 포함), 전자 재정 및 재산기록 저장소 및 전송 시스템, 비상 대비 통신 시스템, 그리고 당해 시스템을 지원하는 물리적 자산 및 기술 자산을 포함한 미국의 핵심 자원 및 주요 기반을 안전하게 하기 위한 포괄적인 국가 계획을 개발하도록 하였다. 그리고 연방 정부의 다른 기관들과 조정하고, 주 및 지방 정부 기관과 당국, 민간 영역, 기타 실체 등과의 협력에 있어서 미국의 핵심 자원 및 주요 기반을 보호하기 위하여 필요한 대책을 권고할 수 있다. 한편, 정보분석 및 기반시설 보호 담당 차관에 대한 할당을 위하여, 연방수사국(FBI)의 국가기반시설보호센터(National Infrastructure Protection Center, 이하 NIPC), 국방부(DOD)의 국가통신시스템(National Communications System, 이하 NCS), 상무부(DOC)의 주요기반시설보장국(Critical Infrastructure Assurance Office, 이하 CIAO), 에너지부(DOE)의 국가기반시설시뮬레이션분석센터(NISAC)와 안보 및 보장 프로그램 및 활동 등과 관련한 직무, 인원, 자산 책임 등이 장관에 이관되도록 하고 있다.

동 법에서 주요기반시설 및 제어 시스템의 보호에 대한 법 규정은 TitleⅡ Information Analysis and Infrastructure Protection 및 TitleⅧ의 Subtitle G. Support Anti-Terrorism by Fostering Effective Technology Act of 2002 에서 살펴 볼 수 있다. 이 두 부분은 각각 「Critical Infrastructure Information Act of 2002」 및 「Support Anti-Terrorism by Fostering

Effective Technology Act of 2002 」로 독립적인 법으로 언급되고 있기 때문에 3.2.2절 및 3.2.3절에서 살펴보도록 한다.

3.2.2 Critical Infrastructure Information Act of 2002

「Critical Infrastructure Information Act of 2002」(CIIA)는 「Homeland Security Act of 2002」 Title Ⅱ의 Subtitle B에 명시되어 있는 법률로, 공공영역에 속하지 않은 주요기반시설에 대한 정보의 수집, 획득 및 이용 등에 관하여 규정하고 있다.

동 법에서 정의되는 '주요기반시설 정보(Critical Infrastructure Information, CII)'라 함은 주요기반시설이나 기반시설보호 시스템의 보안과 관련된 정보로서 다음과 같다.

- 연방, 주 또는 지방 법률을 위반하거나, 미국의 주간 상거래(Interstate Commerce)에 위해를 가하거나, 공중 보건이나 안전을 위협하는 정보를 의미한다. 물리적 공격은 물론 컴퓨터 기반 공격 또는 기타 유사한 행위에 의한 주요기반시설이나 기반시설 보호 시스템에 대한 현재적, 잠재적, 또는 임박한 간섭, 이에 대한 공격, 손상 또는 무력화와 관련된 정보
- 침해·손상·무력화에 대항하는 주요기반시설이나 기반시설 보호 시스템의 능력과 관련된 정보로 보안 테스트·위험 평가·위험 관리 계획·위험 감사를 비롯한 주요기반시설 및 기반시설 보호 시스템의 취약성과 관련된 평가·예측·추정과 관련 된 정보
- 또한 간섭, 손상 또는 무력화와 관련된 범위에 대한 수리, 복구, 재건, 대비, 또는 연속성을 포함하여, 주요기반시설이나 기반시설 보호 시스템에 관한 계획되었거나 과거의 운용 문제 또는 해결책 등과 관련된 정보

정보 공유 및 분석 조직은 어떠한 공식 혹은 비공식적으로 정부 혹은 민간에 의한 조직 및 공동체로 다음의 목적에 의해 생성 혹은 임명된다.

- 가용성, 무결성 및 신뢰성 보증을 위하여 주요 기반시설 및 기반시설 보호 시스템과 관련된 보안 문제와 상호 의존에 대한 이해를 발전시켜야 하며, 이를 위하여 주요기반시설 정보를 수집 및 분석 목적
- 주요기반시설 및 기반시설 보호 시스템과 관련된 침해 등을 예방·탐지·경감·복구 하도록 도움을 줄 수 있는 주요기반시설 정보에 대한 통신 및 공개 목적
- 회원 그리고 주·지역·연방 정부, 혹은 다른 상기 항목에 도움을 줄 수 있는 다른 단체에 대하여 주요기반시설 정보에 대한 자발적 전파 목적

동 법에서 논의되는 기반시설 보호 시스템은 주요기반시설의 취약성에 직접적으로나 간접적으로 영향을 미치는 서비스, 물리적 또는 컴퓨터 기반 시스템, 프로세스 또는 절차 등을 의미하며, 컴퓨터, 컴퓨터 시스템, 컴퓨터 또는 전기통신망 또는 그것의 모든 컴포넌트 하드웨어나 요소, 소프트웨어 프로그램, 처리 명령, 또는 송신 매체나 저장 매체를 불문하고 송신 또는 저장되는 정보나 데이터를 포함하여, 물리적 또는 컴퓨터 기반 시스템을 포함한다.

동 법에서는 제어 시스템을 포함하는 기반시설에 대한 보호 등을 명시하고 있는데, 그 중 주요기반시설에 관련된 '정보' 에 초점을 두고 있다. 특히 정보의 공유 및 분석을 정보보호에 있어서 중요한 요소로 강조하고 있으며, 이들 기능의 수행을 위한 조직 및 협력의 근거를 제공하고 있다.

3.2.3 Support Anti-terrorism by Fostering Effective Technologies Act of 2002

SAFETY Act로 소위 알려진, 「Support Anti-terrorism by Fostering Effective Technologies Act of 2002」는 「Homeland Security Act of 2002」 TitleⅧ의 Subtitle G에 명시되어 있는 법률이다. 동 법은 적합한 테러 방지 기술(Qualified Anti-Terrorism Technology, QATT) 제공자에 대한 법률적 책임으로 부터의 보호를 규정하는 법률이다. SAFETY Act의 목적은 테러 방지 기술 개발 및 제공 업체를 책임으로부터 보호하여 테러 방지를 위한 새롭고 창의적인 기술의 개발을 장려하는 것으로 주요 내용은 다음과 같다.

동 법에서는 "소송 관리(Litigation Management)" 및 "위험 관리(Risk Management)" 시스템을 통해 테러 방지 기술을 개발 및 적용하는 제공자들을 보호한다. 동 법은 상기의 위험 관리 시스템에 의하여 보호될 수 있는 테러 방지 기술의 7가지 요건[2]에 대해서 규정하며

이 요건은 다음과 같다.

- 기존 미국 정부에서 사용하였거나 효과적이라고 평가된 기술
- 즉시 공공 및 민간에 적용 가능한 기술
- 테러 방지 기술의 판매자나 기타 제공자가 막대한 책임에 노출될 위험이 존재할 경우
- 위험 관리 차원에서 동 법 등에서 보호가 이루어지지 않을 경우 테러 방지 기술이 적용되지 않을 것 이라 예측되는 기술
- 테러 대응 기술이 적용되지 않을 경우 위험에 대한 노출의 위험성이 큰 기술
- 예상되는 위험 요인을 예방할 수 있다는 과학적 평가가 가능한 기술
- 테러 행위에 대해 효율적으로 방어·예방·타파·대응을 수행할 수 있는 기술

소송 관리[3]는 테러 발생 시 적합한 테러 방지 기술(QATT)이 테러에 대응하였을 경우 제조물 책임 등으로 인하여 판매자(Seller)에게 발생하는 소송 관련 손해와 관련된 조항이다. 이와 같은 QATT 관련 소송 발생 시 연방의 소송 사유(Federal Cause of Action) 가 있어야 하며 지방법원(District Court of the United States)이 관할권을 갖도록 하고 있다.

위험 관리[4]는 적합한 테러 방지 기술 제공업체의 법률적 책임을 경감 혹은 면제를 위한 책임보험(Liability Insurance)을 의미한다. 연방 혹은 비연방 정부에 테러 방지 기술을 제공하는 업체는 책임보험을 보유하여야 하며, 제3자의 청구(Third Party Claims)발생 시 책임보험을 통해서 보장할 수 있다.

3.2.4 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001

소위 애국법 으로 알려진 USA PATRIOT Act는 2001년 10월 6일 조지 W. 부시 대통령에 의해 승인된 법으로 「Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001」의 표제(Short Title)이다. 2001년 9.11 테러 이후 테러 방지를 위해 이 법은 사법 기관의 전화, 이메일, 의료, 금융 등의 감시에 대한 권한을 높이는 등의 내용을 담고 있다.

본 법은 다른 법률에 많은 변화를 야기하였다. Foreign Intelligence Surveillance Act of 1978, the Electronic Communications Privacy Act of 1986, 그리고 Money Laundering Control Act of 1986 등이 변경된 주요 법률들이다. 본 법은 10개의 세부 조항으로 구성되어 있으며 전자적 제어시스템 보안과 관련된 조항 및 주요 내용은 다음 [표 2]와 같다.

〔표 2〕 전자적 제어시스템 보안 관련
USA PATRIOT Act 조항 및 주요 내용

Title	주요 내용
Title I: Enhancing Domestic Security against Terrorism	테러에 대한 위협에 대비하고 국토 안보를 증대시키기 위한 각종 조치들에 대해 규정 대테러 활동과, FBI의 기술지원센터를 위한 자금 확보 방안을 정립 무기와 대량 살상 무기가 관련된 상황 시 국방장관의 요청에 따라 군이 도움을 줄 수 있도록 승인 핵심기반시설 등을 위협 등 전자범죄를 예방하고 탐지하고 수사하기 위한 국가 전자 범죄 TF확대
Title VII: Increased information sharing for critical infrastructure protection	핵심기반시설을 위협하는 테러에 대한 대응을 위한 조항 Omnibus Crime Control and Safe Streets Act of 1968 개정 여러 관할권에 걸쳐 테러 음모 및 활동을 하는 단체에 대한 수사 및 기소 등을 장려하기 위한 정보 공유 시스템 도입 및 운영 Bureau of Justice Assistance (BJA)에 상기 시스템 운영 권한 및 예산 부여
Title VIII: *Strengthening* the criminal laws against terrorism	테러리즘에 대한 정의를 변경 및 테러에 대응하기 위해 새로운 정의에 따른 규정 확립 "국내 테러"에 대해서 대량 파괴뿐만 아니라 암살 혹은 납치까지 테러 활동으로 넓은 범위에서 규정 "미국 연방과 모든 주의 어떤 법을 위반하는 행위 중 인명에 위해를 끼치는 행위"로 "민간인들을 위협, 강압함", "위협, 강압을 통해 정부의 정책에 영향을 미치기 위해", "대량 파괴, 암살, 납치 등을 통해 정부의 행동에 영향을 미치기 위함" 등을 테러리즘으로 정의
Title X: Miscellaneous	SEC.1016 Critical Infrastructure Protection 으로 Critical Infrastructures Protection Act of 2001로 명칭 됨

2) SEC. 862. Administration. (b)
3) SEC. 863. Litigation Management
4) SEC. 864. Risk Management

Title	주요 내용
	정부의 기반시설 정보화에 따른 보안문제로 국가적 차원의 노력의 필요성에 의해 입법 주요기반시설의 대테러 활동, 위협 평가 그리고 위험 완화 등의 보호를 위하여 국가기반시설 모의실험 및 분석 센터(National Infrastructure Simulation and Analysis Center, NISAC)의 설립 NISAC의 활동으로 (1) 주요기반시설의 시스템 관련 모델링, 시뮬레이션 그리고 분석 (2) 주요기반시설의 일반적 시스템 모델링 위한 주 및 지방 정부 등으로 부터의 정보 수집 (3) 주요기반시설 보호 관련 정책 수립 담당자에 대한 교육 제공 (4) 주요기반시설의 보호 및 안전성 위해 정책 수립 담당자 · 연방 정부 기관 · 민간 분야 등에 제공하기 위한 모델링·시뮬레이션·분석 결과의 이용 등을 명시 보안위협감축기구(Defense Threat Reduction Agency)에 NISAC 활동을 위하여 국방성(Department of Defense)에 예산 부여

3.3 소결

미국은 가장 선도적으로 사이버공격에 대한 대응을 준비하였으며 2001년 9·11 테러 이후 사이버공격에 더욱 적극적으로 대응하고 있다. 전담기구인 국토안보부를 설치하여 국가주요기반시설 등 자국 내 테러 방지를 위한 역량을 집중시켰으며, 기반시설 보호 기술 개발, 분야별 기반보호 법 제정 및 전략 수립 등 다양한 노력을 기울이고 있다.

다음 [표 3]은 미국의 사이버보안 관련 법·정책에서 볼 수 있는 제어시스템 보안 관련 세부 대응 전략이다.

〔표 3〕 미국 제어시스템 보안 대응 전략 관련 세부 전략 및 근거 법·정책

대응 전략		세부 전략 및 근거 법·정책
사전 대응	기반시설 보호 관련 권한 및 예산 부여	국토안보부 창설 및 테러 대응 역량 집중 - Homeland Security Act of 2002 주요기반시설 부문별 주요지휘기관 지정(국토안보부:정보통신·운송·우편선박·긴급구난·정부연속성, 환경보호부:수자원·화학산업 등) - National Strategy to Secure Cyberspace 국가기반시설보호센터(National Infrastructure Protection Center, NIPC), 중요정보기반보장국(Critical Infrastructure Assurance Office, CIAO), 국가기반보장위원회(National Infrastructure Assurance Council, NIAC) 설립 - PDD 63 대통령 직속 주요기반시설보호위원회(President's Critical Infrastructure Protection Board) 설립 - EO13231 Cybersecurity Coordinator를 통한 리더쉽 발휘 - Obama's Cyberspace Policy Review
	분석센터 설립	국가기반시설시뮬레이션및분석센터(National Infrastructure Simulation and Analysis Center) 설치 - Critical Infrastructure Protection Act of 2001
	보호프로그램 수립	주요기반시설 보호 프로그램의 수립 - Critical Infrastructure Information Act of 2001, National Plan for Information System Protection, National Strategy for the Physical Protection of Critical Infrastructure and Key Assets, National Strategy to Secure Cyberspace, National Infrastructure Protection Plan
	취약점 분석	주요기반시설 등에 대한 취약점 분석 및 감축 - National Strategy to Secure Cyberspace 주요기반시설 및 핵심자산 보호를 위한 위험평가 및 취약점 분석 - National Infrastructure Protection Plan
	인식제고 및 교육	2009년 12월을 "Critical Infrastructure Protection Month"로 지정 - President's Proclamation 인식 제고 프로그램 및 교육 장려 - National Strategy to Secure Cyberspace
	기술개발	테러 방지 기술 개발 업체에 대한 위험 관리 제공 - SAFETY Act of 2002 사이버보안 관련 전략적 기술개발 계획 등에 예산 지원 및 표준 개발 - (Bill) Cybersecurity Enhancement Act of 2010
실시간 침해 대응	침해위협 및 침해사실 통지	기반보호전담반(Infrastructure Protection Task Force)은 침해의 위협이 있을 경우 위협 및 경고 통지(Threat & Warning Notice) - EO13010
	침해대응을 위한 정보공유	국토안보부 산하 US-CERT(Computer Emergency Readiness Team)를 설립하여 사이버보안 조정 · 준비 · 사이버공간 보안 계획 수행 관련 정부의 주춧돌 역할, US-CERT는 연방/주 정부 및 ISAC 들과 정보 교환 등과의 협력을 통해 정보 공유 및 취약점 분석, CII Act에 의거하여 보호되는 정보들의 민간과 정부의 공유위한 PCII(Protected Critical Infrast Information) Program - Homeland Security Act of 2002, Critical Infrastructure Information Act of 2002, National Strategy

대응 전략		세부 전략 및 근거 법·정책
		to Secure Cyberspace 민간의 정보공유분석센터(Information Sharing and Analysis Center, ISAC)의 설립 장려 - PDD63, Critical Infrastructure Information Act of 2001 법무부 사법원조국(Bureau of Justice Assistance)에 여러 관할권 걸친 테러 음모에 대한 수사 및 기소 등을 장려하기 위한 정보공유 시스템 운영 권한 및 예산 부여 - USA PATRIOT Act of 2001
침해 사후 대응	처벌 규정	정보시스템에 대한 비인가 혹은 권한 초과하는 접근 등에 대한 형사 처벌 규정 - National Information Infrastructure Protection Act of 1996 컴퓨터 관련 범죄 관련 양형위원회(Sentencing Commission)에 형량의 가이드라인 정하도록 함, 컴퓨터 해킹 등을 통해 고의적으로 상해를 입힐 경우 20년 이하의 징역, 사망을 일으켰을 경우 종신형 이하의 징역 등으로 처벌 수준 확대 - Cyber Security Enhancement Act of 2002
	복구	주요기반시설 등에 대한 사이버 침해사고 발생 시 복구 기간 최소화 노력 - National Strategy to Secure Cyberspace

[표 3]과 같이, 국가주요기반시설 관련 법제 및 정책은 크게 사전대응 · 실시간 침해대응 · 사후 대응으로 분류할 수 있다. 사전대응은 기반시설보호관련 권한 및 예산 부여 · 보호프로그램 수립 · 취약점 분석 · 인식제고 및 교육 · 기술개발로 분류할 수 있으며, 실시간 침해대응은 침해위협 및 침해사실의 통지 · 침해대응을 위한 정보공유로, 침해 사후 대응은 처벌 · 복구로 분류할 수 있다. 미국은 각 법률 및 정책을 통해 세부 전략별로 구체적으로 대응하고 있음을 알 수 있다.

또한 미국은 연방 정부, 주 정부, 그리고 민간 영역으로 분산 된 주요기반시설의 보호 및 관리와 국토안보부, NSA 등에 분산된 대응 체계 등을 관리하기 위한 소통 및 테러대응 기술의 개발, 보호프로그램 수립 및 분석센터 설립 등으로 제어시스템 침해의 사전 대응에 중점을 두고 있음을 알 수 있다.

Ⅳ. 한국의 법제 현황 및 개선점 도출

4.1 「정보통신기반 보호법」 개관

국내 제어시스템 보안 관련 법제 논의는 1996년 미국의 「National Information Infrastructure Protection Act of 1996」의 입법에 따라 국내에도 기반시설 보호를 위한 법제의 필요성이 인식되면서 시작되었다.[13] 주요기반시설 등에 대한 사이버위협은 현실화되고 있지만 당시 이를 규제할 수 있는 법률은 국가정보원법 · 전기통신기본법 · 정보통신망이용촉진등에관한법률 · 보안업무규정 등으로 산재되어 있었다. 이에 2000년 2월 국무총리 주재로 <사이버테러 방지 관계 장관회의>가 개최되어 연내 「정보통신기반보호법」을 제정하기로 하였으며, 동해 3월 정보통신기반보호법 제정위원회가 구성되어 법제 준비를 하였다.[14] 2000년 7월 초안이 마련되어 공청회 등을 거쳐 2000년 12월 국회에서 통과가 되어 「정보통신기반 보호법」은 2001년 7월 시행되었다. 이후 일부 개정 및 타법 개정 등을 거쳐, 현재 행정안전부 소관 법률로 시행되고 있다.

「정보통신기반 보호법」은 주요정보통신기반시설의 보호체계구축, 주요정보통신기반시설 보호지원, 취약점 분석, 침해사고 대응, 기술지원 및 민간협력, 벌칙 등으로 구성되어 있다. 동 법에서 나타난 제어시스템 보안 관련 세부 대응 전략은 다음 [표 4]와 같이 분류할 수 있다.

[표 4] 정보통신기반 보호법의 세부 대응 전략

대응 전략		세부 전략 및 근거 법·정책
사전 대응	기반시설 보호 관련 권한 및 예산 부여	정보통신기반보호위원회 설립 및 공공공분야와 민간분야를 각각 담당하는 실무위원회 설립 - 제3조 제1항, 제4항 등
	분석 센터 설립	분야별 정보통신기반시설을 보호하기 위하여 정보공유·분석센터를 구축·운영 - 제16조 제1항 등
	보호 프로그램 수립	주요정보통신기반시설 관리기관의 장은 취약점 분석·평가의 결과에 따라 물리적·기술적 대책을 포함한 관리대책을 수립·시행하여야 함 - 제5조 제1항 등 관계중앙행정기관의 장은 주요정보통신기반시설보호대책을 종합·조정하여 소관분야에 대한 주요정보통신기반시설에 관한 보호계획을 수립·시행하여야 함 - 제6조 제1항 등
	취약점 분석	전자적 침해행위로부터의 보호가 필요하다고 인정되는 정보통신기반시설을 주요정보통신기반시설로 지정할 수 있음 - 제8조 제1항 등 관리기관의 장은 대통령령이 정하는 바에

대응 전략		세부 전략 및 근거 법·정책
		따라 정기적으로 소관 주요정보통신기반시설의 취약점을 분석·평가하여야 함 - 제9조 제1항 등
	인식 제고 및 교육	N/A
	기술 개발	정보통신기반시설을 보호하기 위하여 필요한 기술의 개발 및 전문인력 양성에 관한 시책을 강구할 수 있음 - 제24조 제1항 등
실시간 침해대응	침해 위협 및 침해 사실 통지	관리기관의 장은 침해사고가 발생하여 소관 주요정보통신기반시설이 교란·마비 또는 파괴된 사실을 인지한 때에는 관계 행정기관 등에 그 사실을 통지하여야 함 - 제13조 제1항 등
	침해 대응을 위한 정보 공유	주요통신기반시설에 대하여 침해사고가 광범위한 경우 그에 필요한 응급대책, 기술지원 및 피해복구 등을 수행하는 정보통신기반침해사고대책본부를 둘 수 있음 - 제15조 제1항 등
침해 사후 대응	처벌 규정	주요통신기반시설을 교란·마비 또는 파괴한자는 10년 이하의 징역 또는 1억원 이하의 벌금에 처함 - 제28조 제1항 등
	복구	관리기관의 장은 해당 정보통신기반시설의 복구에 필요한 조치를 신속히 취해야 함 - 제14조 제1항 등 피해복구 등을 수행하는 정보통신기반침해사고대책본부를 둘 수 있음 - 제15조 제1항 등

동 법에 따라 2010년 현재까지 주요정보통신기반시설을 지정하여 보호대책을 수립하고 있으며, 2010년 1월 현재 10개 관계중앙행정기관 90개 관리기관 126개 기반시설이 지정·관리되고 있다. 분야별 주요정보통신기반시설 현황은 다음 [표 5][15]와 같다.

〔표 5〕 분야별 주요정보통신기반시설 현황

분야	주요정보통신기반시설 현황
행정	행정업무시스템 등
방송통신	인터넷 접속망 등
금융	인터넷뱅킹 시스템 등
에너지	감시·제어 및 자료취득시스템(SCADA) 등
건설·교통	운항관리 시스템 등
사회복지	보험관리 시스템 등
기타	보험 전산망 등

4.2 정보통신기반 보호법의 문제점 및 이에 따른 개선 방안 도출

4.2.1 제어시스템의 특수성 반영 필요성

현행 「정보통신기반 보호법」의 대상은 국가안전보장·행정·국방·치안·금융·통신·운송·에너지 등의 업무와 관련된 전자적 제어·관리시스템 및 정보통신망을 대상으로 하고 있다. 동 법의 대상은 [표 5]와 같이 에너지 및 교통 분야의 제어시스템 부분과, 방송통신 분야의 전산망 그리고 행정·금융 분야의 정보시스템으로 분류할 수 있다. 즉, 정보통신기반 보호법에서 통신망 · 정보시스템 · 제어시스템 3가지 서로 다른 대상에 대한 보호를 다루고 있다.

정보시스템과 제어시스템은 사용 목적 상 여러 항목에서 차이가 있는 시스템으로 이 차이는 다음 [표 6][16]에서 확인할 수 있다.

정보시스템은 행정정보·금융정보·개인정보를 처리하는 시스템으로 기밀성이 가장 중요한 요구사항이며, 상대적으로 사고 발생 시 피해 및 파급 효과가 제어시스

〔표 6〕 IT시스템과 제어시스템의 차이점

항목	IT시스템	제어시스템
응답 요구시간	적당히 빠른 응답시간 (인간중심)	실시간 응답 (기계 중심)
서비스 제공시간	서비스 대부분은 시급성이 요구되지 않음	한시라도 멈춰서는 안 됨
시스템 보안관리	백신·패치 등의 설치가 자유로움	백신·패치 설치 어려움 (설치로 인한 오작동 및 유지보수 문제)
소프트웨어 문제점 수정	운영 S/W 문제점 발견 시 즉시 수정 가능	문제점이 발견되어도 시스템 안전성 충분히 검토 후 수정 가능
유지·보수	유지·보수 문제점 발생 가능성 낮음	개발 및 설치 업체만이 유지·보수 가능
보호 대상	IT 시스템	제어시스템 및 제어기기
중요 요구사항	기밀성, 가용성	가용성, 무결성
사고 피해 파급효과	업무 불편 및 지연	국가기반시설 마비로 인한 사회적 혼란
원격 유지보수 및 업데이트	원격 유지보수 및 백신 등 자동업데이트 가능	실제 시스템에서 유지보수 및 자동 업데이트 불가

템에 비하여 적다. 반면 정보통신기반 보호법에서 보호하고자 하는 제어시스템의 경우 국가기반과 관련된 시설로 마비 등을 일으켰을 경우 사회적 혼란 등 심각한 문제가 발생할 수 있다. 따라서 가용성이 최우선 요구사항이며 적법하지 않은 권한을 가진 사용자가 이에 접근하여 정보를 수정하는 침해 상황이 발생할 경우 큰 위험성이 있으므로 무결성 역시 중요한 요구사항이다. 두 시스템은 여러 면에서 상이한 시스템으로 보호조치 및 침해사고 발생 시 대응방안 등에 있어서 일괄적인 현재 규정보다는 각 시스템의 특수성을 고려하여 규정해야할 것이다.

4.2.2 미국 법제와의 비교에 따른 보완 필요성

현행 「정보통신기반 보호법」은 제정 당시 국가기반시설 보호와 관련한 법 제정을 가장 적극적으로 진행하고 있던 미국의 입법례를 많이 참고[17]하였다. 미국과 우리나라의 세부전략을 비교한 [표 3]과 [표 4]를 비교해보면 유사한 대응을 하고 있다는 것을 알 수 있다. 미국이 2001년 이후 법제에 많은 변화가 있었던 것과 달리, 우리 법은 2번의 개정과 3번의 타법개정 등 변화가 크지 않았다. 이로 인하여 각 세부 전략의 구체성에 있어서는 많은 차이를 보이고 있다.

미국은 국토안보부를 신설하여 분산된 대테러 역량을 집중시켰으며, FBI와 NSA 등 타 부처와의 협조를 위하여 백악관 산하에 사이버보안조장관을 두었다. 또한 민간에서 주요기반시설을 관리하고 있는 특성 상 민간 정보공유분석센터(ISAC)의 설립을 장려하였으며, US-CERT와 같은 분석센터 등을 통해 취약점 분석 및 민간과 정부 기구들과의 정보교류를 장려하였다. 또한 컴퓨터 해킹 등 전자적 침해에 의한 형량을 상해의 경우 20년, 사망에 이를 경우 종신형 등으로 확대하였다. 또한 제어시스템에 대한 테러방지 기술의 개발을 위하여 기술 개발 업체에게 민·형사 소송 리스크를 관리하기 위한 법안을 제정하여 기술개발을 장려하며, 관련 기술 연구 장려 및 인력 양성에 예산을 지원하는 법안이 통과를 앞두고 있다.

우리 기반보호법의 경우 현재 행정안전부 소관 법률로 행정안전부, 국정원, 국방부, 한국인터넷진흥원에서 주요정보통신기반시설의 보호를 담당하고 있다. 대상에 있어 민간영역의 정보통신기반시설의 보호조치 및 사고대응 등에 있어 관할문제가 발생할 수 있다. 또한 민간의 정보공유분석센터의 부재와 소관부처 등과 정보를 공유 등의 조정할 수 있는 기구가 부재한다. 기술 개발 역시 구체적인 예산 · 시행 계획이 없이 '기술의 개발 및 전문인력 양성에 관한 시책을 강구할 수 있다'고 추상적으로 명시하고 있다. 벌칙 조항의 경우 침해사고의 위협에 비하며 낮은 수준의 벌칙을 규정하고 있으며, 주요정보통신기반 시설의 물리적 침해에 대한 벌칙은 적용이 불가능한 문제가 있다.

따라서 민간 분야 제어시스템의 보호 관할 정비 및 정보공유 방안의 수립, 구체적인 인력양성 및 기술개발 규정, 그리고 제어시스템 보호의 중요성에 대응하는 침해 시 처벌 규정의 개정 등이 필요하다.

4.2.3 내부자에 의한 침해 및 오작동 방지 고려

2장에서 분석한 전자적 제어시스템 침해사고 사례에서 볼 수 있는 사실은 직원의 실수에 의한 오작동 및 전직직원의 침해가 문제였다는 사실이다. 국가기반시설의 전자적 제어시스템의 경우 대부분 인터넷 등 네트워크 접속을 차단하였으며 내부망에서도 접속 지점을 한정하고 방화벽 등으로 보호하고 있다. 하지만 정당한 접근권한을 가진 내부자, 내부 사정을 잘 알고 있는 전직직원, 내부자와의 공모 그리고 실수 등에 의한 오작동(Malfunction)을 막기는 힘들다는 문제점이 있다.

미국의 경우 「National Strategy for Homeland Security」에서 제어시스템의 '내부자(Insider)'와 관련된 위협을 명시하였으며, 내부자 위협을 방지하기 위하여 보증인 프로그램 · 심사 및 배경 조사 국가 표준 제안 등을 마련할 것을 명시하고 있다. 반면 우리나라의 현행 정보통신기반보호법 제27조의 '비밀유지의무' 외에는 내부의 취약성으로부터 제어시스템을 보호할 수 있는 규정이 전무하며, 이 역시 실제 사고 사례에서 발생한 상황을 막을 수는 없다. 정보통신기반보호법에서 규정하고 있는 취약점 분석은 내부 전담반 및 「정보통신산업진흥법」 상의 지식정보보안컨설팅전문업체 등에 의하여 이루어지고 있으며, 이 프로세스는 주요정보통신기반시설의 특성상 취약점 탐지도구 등을 이용한 일반적인 기술적 취약점 분석 이상의 결과를 도출하기는 힘들 것으로 보인다.

내부자에 의한 침해 및 실수 등을 통한 오작동을 막

기 위해서는 행동지침(Code of conduct), 내부통제, 교육·훈련, 실수 제어 등의 정책적 보호조치의 마련이 필요할 것이다. 정보통신기반보호법에는 주요정보통신기반시설 소관 관리기관의 장으로 하여금 이러한 정책적 보호조치 마련을 요구하도록 해야 할 것이다. 또한 주요정보통신기반시설을 운영하는 자의 신원을 확인하고 보증할 수 있도록 미국의 보증인 프로그램 · 심사 및 배경조사 국가 표준 제안 등의 마련 역시 필요할 것이다.

V. 결 론

제어시스템 및 기반시설 등의 정보기술에 의한 자동화는 효율을 높이고 사회 전반의 편의성을 증진시켰다. 하지만 정보기술의 취약성이 전이됨에 따라 안전하게 보호되어야 할 기반시설은 위협에 노출되고 있는 것이 현재 상황이다. 우리나라의 경우 현재까지 보고된 전자적 제어시스템에 대한 침해사고는 없지만, 지난 2009년 발생한 7·7 DDoS 공격에서 금융사이트 접속이 마비되는 등 주요정보통신기반시설에 대한 침해 위협은 점차 현실화되고 있다. 전자적 제어시스템은 멈추어서는 안되며 사고가 발생할 경우 사회적 혼란을 야기할 수 있기 때문에 전자적 제어시스템 침해 위협에 따른 보호대책 및 침해사고 발생 시 대응 방안이 필요하다.

최근 개방형 제어시스템이 등장하고 있는 추세에 따라 취약점은 증가하고 있으며 네트워크를 통한 침해 위협은 더욱 증가하고 있다. 「정보통신기반 보호법」은 국가주요기반시설 등의 보호에 대해 규정하고 있는 법으로서 사회 안전을 위하여 기반시설의 침해위협에 대응할 수 있도록 구비되어야 한다. 현행 기반보호법은 보호대상의 특성에 따른 구분 없이 정보시스템 · 전산망 · 제어시스템을 포괄하여 규제하고 있는 문제, 민간 분야의 제어시스템 보호 및 정보공유 문제, 기술개발 및 인력양성 조항 등의 추상적인 문제, 낮은 처벌 수준의 문제 등이 문제점으로 지적될 수 있다. 따라서 제어시스템의 특성을 고려한 보호조치 및 사고 대응, 민간 분야 제어시스템의 보호 관할 정비 및 정보공유 방안의 수립, 구체적인 인력양성 및 기술개발 규정, 그리고 제어시스템 보호의 중요성에 대응하는 침해 시 처벌 규정의 개정 등이 필요하다.

또한, 주요 사고사례 분석에서 나타난 것과 같이 실제 사고는 예상하고 대응조치를 마련하였던 외부의 침입이 아니었으며, 내부의 실수로 인한 오작동 및 내부 시스템에 대한 지식이 있는 전직 직원에 의한 소행이었다. 따라서 내부로부터의 위협을 줄이기 위한 정책적 보호조치 마련이 필요하며, 소관 관리기관의 장으로 하여금 정책적 보호조치 수립을 의무화하는 방안이 필요할 것이다.

참 고 문 헌

[1] CNET NEWS, "CIA: Cyberattack caused multiple-city blackout," Jan. 2008. http://news.cnet.com/CIA-Cyberattack-caused-multiple-city-blackout/2100-7349_3-6227090.html

[2] Pipeline Rupture and Subsequent Fire in Bellinham, Washingtom. June 10, 1999, p.V NTSB, 2002.

[3] Marsheall Abrams, Joe Weiss, Bellingham, Washinton, Control System Cyber Security Case Study, NIST, pp. 8-9, 2007.

[4] Marsheall Abrams, Joe Weiss, 상게 보고서, pp. 11, 2007

[5] SEATTLE POST-INTELLIGENCER, "In deal, Olympic Pipe Line, 3 workers admit guilt in blast,, Dec. 2002. http://www.seattlepi.com/local/99588_olympic12.shtml

[6] PC World, "California Canal Management System Hacked", Dec. 2007. http://www.pcworld.com/article/140190/california_canal_management_system_hacked.html

[7] Marsheall Abrams, Joe Weiss, Malicious Control System Cyber Security Attack Case Study - Maroochy Water Services, Australia, NIST, pp. 8-9, 2008.

[8] 권태웅 "미국의 입법절차와 사법심사," 법제(법제처), 통권 제599호, pp. 63, 2007년.

[9] 정찬모, 유지연, 조용혁, "정보통신기반보호법 제정 관련 기초연구," 정책연구, 정보통신정책연구원, pp. 36-41, 2000년.

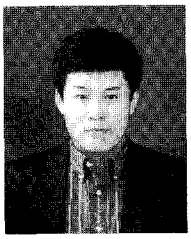
[10] Critical Foundations: Protecting America's Infrastructures, The Report of the President's Commission on Critical Infrastructure Protection, 1997.

[11] John Arquilla, David Ronfeldt, "Networks and Netwars : The Future of Terror, Crime, and Military," pp. 285-287, 2001.
[12] 김도승, "사이버위기 대응을 위한 법적 과제", 방송통신정책, 21(17), pp. 39, 2009.
[13] 강경근, "인터넷 사회에서의 개인정보보안과 정보기반보호," 인터넷법률, 창간호, pp. 44-45, 2000년 7월.
[14] 홍봉화, "정보통신기반보호법 제정," 국가기록원 http://contents.archives.go.kr/next/content/listSubjectDescription.do?id=001989
[15] "2010 국가정보보호 백서," pp. 61, 2010년
[16] 서정택, "국외 제어시스템(SCADA) 보안기술 동향," SIS2008 발표자료
[17] 백광훈, "사이버테러리즘에 관한 연구", 한국형사정책연구원, pp. 225, 2001년

〈著者紹介〉

임 종 인 (Jong-in Lim)
종신회원

1980년 2월 : 고려대학교 수학과 졸업
1982년 2월 : 고려대학교 수학과 석사
1986년 2월 : 고려대학교 수학과 박사
現 고려대학교 정보경영공학전문대학원((구)정보보호대학원) 원장 (고려대학교 정보보호연구원 원장 겸임), 대검찰청 디지털수사자문위원회 위원장, 금융보안연구원 보안전문기술위원회 위원장, 행정안전부 정책자문위원회 위원 등
<관심분야> 정보법학, 디지털포렌식, 개인정보보호, 전자정부보안, 융합기술보안 등



장 규 현 (GyeHyun Jang)

2009년 8월 : 고려대학교 산업시스템정보공학과 공학사
2009년 9월~현재 : 고려대학교 정보경영공학전문대학원 석·박사통합과정
<관심분야> 정보법학, 모바일 시큐리티, 융합기술보안 등