국토안보를 위한 미국의 대응 정책 분석 : 국토안보법을 중심으로

김 현 수* · 박 상 서*

요 약

2001년 9.11테러 이후 테러의 피해 당사자인 미국은 그동안 국외 중심의 국가안전보장 전략에서 자국내에서의 안보에 대한 중요성을 재인식하고, 국토안보를 위한 대대적인 정책 변화를 추진하여 왔다. 본 논문에서는 국가차원의 종합적·체계적 대응전략이 미흡한 상태에서 발생한 1.25 인터넷 대란의 교훈을 되새겨 새로운 사이버안보관련 전략 수립이 절실한 시점에서, 911이후 미국의 국토안보를 위한 주요정책, 국토안보법의 성립경과, 국토안보법 중 사이버보안관련 부분을 고찰한다.

Analysis of US policy for Homeland Security

Hyun Soo Kim* · Sang Seo Park*

ABSTRACT

Since the September 11, 2001, the United States has shift their national security policy for homeland from preventing or/and reducing foreign threats to ensuring domestic security.

We learned from recent incident, 1.25 Internet Disaster, that it is urgent to establish cyber security policy for our nation. In this paper; therefore, I analyze the US homeland security policy, the Homeland Security Act of 2002 establishment, and cyber security-related part in this act.

* 국가보안기술연구소

1. 서 론

2001년 9월 11일 미국 본토에서 테러사건이 발생하자 세계 각국은 자국의 테러대응태세를 점검하고 보완책을 추진하였다.

한편 테러사건의 피해 당사자인 미국의 경우, 그동안 국외 중심의 국가안전보장 전략에서 자국내에서의 안보에 대한 중요성을 재인식하고, 국토안보를 위한 대대적인 정책 변화를 추진하여왔다.

테러사건 발생후 약 한달만인 2001년 10월 8일 국토안보국(Office of Homeland Security)을 발족, 자국내에서의 국토안보를 위하여 국무부, 국방부, CIA, FBI 등의 연대활동을 위한 중심기관으로서의 역할을 수행하게 하였다. 이와함께 종래 국가안전보장회의(NSC)에서 수행하던 對테러 정책운영에 관한 책임을 국토안보회의(Homeland Security Council)를 설립하여 이관하는 등 국토안보를 위한 노력을 해 오고 있다.

이러한 미국의 국토안보를 위한 노력은 2002년 11월 국토안보부(Department of Homeland Security) 설립을 위한 국토안보법(Homeland Security Act of 2002)의 제정으로 집대성되었다고 할 수 있다.

본 논문은 국가차원의 종합적·체계적 대응전략이 미흡한 상태에서 발생한 1.25 인터넷 대란의 교훈을 되새겨 새로운 사이버안보관련 전략 수립이 절실한 시점에서, 9.11 이후 미국의 국토안보를 위한 정책의 집대성이라 할 수 있는 '국토안보법' 중 사이버보안 관련 부분을 중심으로 고찰함으로써, 국가차원의 사이버안전보장 전략 수립시 시사점을 제공하고자 한다.

본 논문의 구성은 다음과 같다. 먼저 2장에서는 9.11 이후 미국의 국토안보를 위한 주요정책, 3장에서 국토안보법의 성립경과, 4장에서 국토안보법 중 사이버보안관련 부분을 중심으로 고찰한 뒤, 5장에서 결론을 내리기로 한다.

2. 9.11 이후 국토안보정책 변화

미국은 9.11테러 발생이후 테러 대응 대책 강화를 위하여 연방차원의 중심기관의 설치의 필요성을 인식하고, 이를 위한 각종 제안들을 고려하여 대테러대응정책 강화, 조직 정비, 법제개선 등 다양한 노력을 취하였다.

2.1 대테러대응 정책 강화

테러사건 직후 테러사건의 처리와 향후 테러방지를 위하여 다양한 정책을 시행하였다. 그 중 주요한 것으로는 다음과 같은 것이 있다.

9월 23일 대통령 명령 13224호에 의하여, 테러행위에 관계되거나, 테러를 지지하는 합계 27인의 외국인 및 외국단체·기관의 자산을 동결하는 것과 동시에 테러 행위를 실행하거나, 테러위협이 있는 자의 자산의 동결을 승인했다.

9월 28일 미국은 모든 UN 가맹국에게 일체의 테러리스트에 대한 자금제공을 범죄로 보는 안전보장이사회의 의결을 지지했다.

10월 5일 국무장관은 법무장관 및 재무장관과 협의하여, Al-Qaida를 포함한 25개의 테러조직을 1996년의 「테러 및 유효한 사형에 관한 법률 : Antiterrorism and Effective Death Penalth Act of 1996」에 근거하여, 외국테러 조직으로서 재인정했다. 이러한 외국조직에 유형의 지원 혹은 자원을 제공하는 것은 미국의 법률에서는 중죄로 보게 된다.

10월 12일 대통령명령 13224호에 근거하여, 테러 또는 테러리스트에의 자금제공에 관계되는 개인 및 조직의 리스트에 39개의 개인·조직의 리스트를 추가하였다.

10월 26일 「USA PATRIOT ACT」를 제정하였다. 이 법률은 미국의 법집행기관이 테러행위에 관계되는 개인을 수사하고 소추하는 능력을 크게 확대하였다.

12월 5일 국무장관은 테러를 지원하는 자가 미국내에서 발견된 경우에 미국이 그들을 추방하는 능력을 강화하기 위하여, 새로운 USA PATRIOT ACT에 의하여 수정된 이민·국적법에 근거하여, 39단체를 「테러조직」으로 지정했다.

그리고 2002년 3월 12일 국토안보국 Tom Ridge 국장이 미국내에서의 테러대책·예방을 위하여 국토안보상황보고 시스템(Homeland Security Advisiory System)을 창설한다고 발표하였다. 이 시스템은 현재의 연방정부, 주, 지방자치체에 대한 테러의 위협을 근거로 그 대책 수준을 다음과 같이 5단계로 발표한 것이다.

<표 1> HSAS의 등급과 조치내용

수 준	대 용
GREEN (저위협)	예방책의 책정, 훈련의 실시 등
BLUE (요경비)	특정기관과의 연락체제의 체크, 긴급대응계획의 검증 등
YELLOW (위협증대)	요경비대상시설의 감시강화, 연방기관과의 긴급대응계획의 조정 등
ORANGE (고위협)	군, 사법당국과의 필요한 보안활동의 조정, 수요시설에의 진입금지
RED (위협상태)	긴급대응팀·책임자의 임명, 공공시설·정부시설의 폐쇄 등

2.2 테러대응을 위한 조직 정비[1]

테러사건 발생 후 부시대통령은 2001년 10월 8일, 대통령 명령 13228[2]을 발표하여 국토안보국(Office of Homeland Security)을 발족시키고, 국토안보에 대한 대통령 명령 제1호[3]에 의해 2001년 10월 29일 테러범의 위협과 공격으로부터 미국을 수호하고, 잠재적인 테러 공격을 감소시키고, 공격 발생시 피해를 최소화하기 위해 연방, 주, 지방 부처에 대한 총괄적 조정 강화 필요성에 따라 국토안보회의(Homeland Security Council)를 설립하였다.

한편 정보시스템 보안을 위한 각 부처 및 연방 정부, 지방 정부의 활동을 총괄 조정하고, 침해사고 발생시 그 복구를 총괄하며 주요정보통신시설을 운용하고 있는 민간 분야와의 업무를 조정하고 협의하는 역할을 담당할 사이버 보안담당 대통령 특별보좌관(Special Advisor to President for Cyberspace Security)을 임명하는 등 조직적 정비에도 노력하였다.

2.3 테러대응을 위한 법제도 정비

2.3.1 USA Patriot Act

同法은 정보의 수집이나 정부기관에 의한 공유, 이민의 구속, 테러협력자의 취조, 테러조직과 관련된 은행구좌나 자산의 동결 등에 관한 법집행기관이나 첩보기관의 권한을 확대한 것으로 2002년 10월 16일 성립하였고, 주요내용은 다음과 같다.

① 종래 용의자와 관련된 전화번호를 법집행기관이 기록하는 권한을 전자통신(인터넷이나 휴대전화를 포함)으로 확대하고, DCS 1000 (통칭 '카니보어') 등에 의한 IP 어드레스 등의 기록을 인정(단, 통신내용의 기록은 인정하기 않음)한다.

② 사람의 생명 등에 관한 긴급시에 인터넷 서비스 프로바이더가 법집행기관에 고객의 통신기록(통신내용을 포함)을 개시하는 것을 위법으로 하지 않는다.

③ 컴퓨터에 해킹하는 침입자를 모니터하기 위하여 피해자(컴퓨터 소유자)가 법집행기관에 통신감청을 의뢰할 수 있도록 한다.

2.3.2 사이버보안연구개발법[4]

同法의 주요내용은 국립과학재단(NSF)과 국립표준 기술원(NIST)에 새로운 연구 프로그램을 신설하는 것이다.

NSF는 사이버 보안에 관한 혁신적 사고를 장려하기 위하여 새로운 학문적 연구센터(academic center)와 장학금 제도를 신설하고, NIST는 산업계와의 공동연구 능력을 고려하여, 정부, 연구계, 산업계간의 상호작용을 강화하기 위한 새로운 연구 보조금(grant) 프로그램을 신설하는 등 2003년부터 2007년까지 약 8억 7000억불을 투입하여 사이버보안 관련 연구개발을 촉진하게 된다.

3. 국토안보부 설립경과

3.1 국토안보부 설립경위

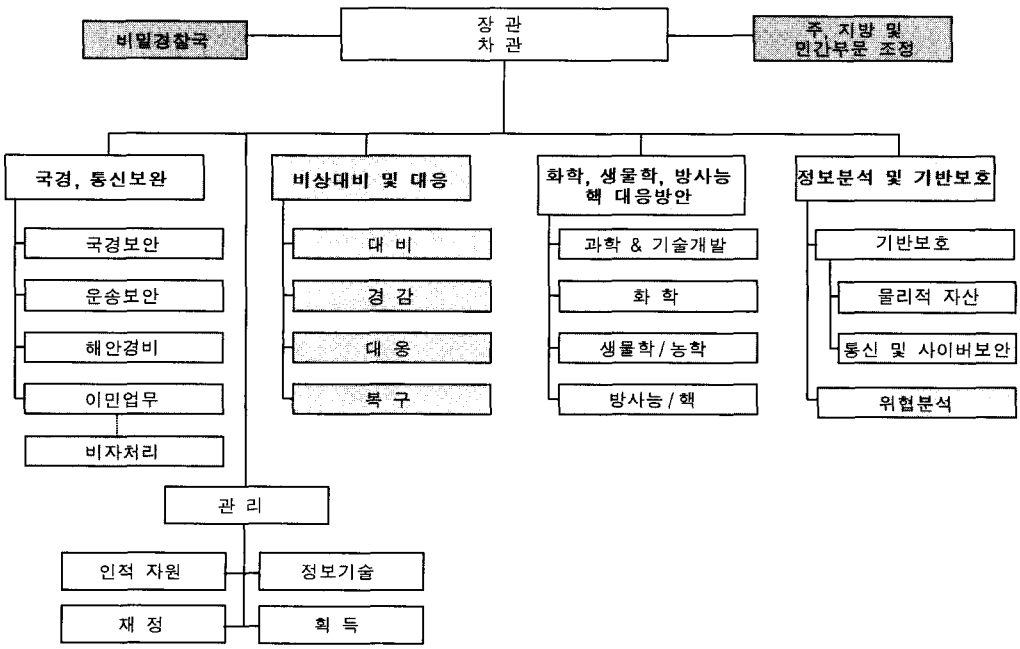
부시 대통령은 2002년 6월 6일 테러대책을 총괄하는 새로운 부서로서 「국토안보부(Department of Homeland Security)」의 창설을 발표하고, 국토안보부 설립을 위한 제안서를 공표하였다[5].

이에 따라 6월 24일부터 의회에서 본 법안이 검토되기 시작하였고, 2002년 11월 19일 상원통과, 11월 22일 하원을 통과하여, 11월 25일 대통령이 서명함으로써 성립되었다.

3.2 국토안보부 설립 제안서 주요내용

제안서에 나타난 바에 의하면, 국토안보부에 통합되는 것은 연방재난관리국(FEMA), 해안경비대, 교통안전국(TSA), 세관국, 이민국(INS), 국경경비대, 비밀검찰국(Secret Service), 주요기반보장국(CIAO), 미국준비센터(NDPO : National Domestic Preparedness Center), 연방보호국(Federal Protective Service), 연방컴퓨터침해사고대응센터(FedCIRC), 동식물검사국, 에너지부나 보건복지부내의 기관이다. 국토안보부내에서 이름이 남는 것은 해안경비대와 Secret Service로 다른기관은 기능에 따라 국토안보부내에 통합되는 것으로 된다.

국토안보부의 임무는 ① 미국내의 테러공격을



(그림 1) 국토안보부 설립제안서에서의 조직구성(2002.6)

방어, ② 미국내의 취약성을 경감, ③ 테러공격이 발생한 경우 피해의 최소화 및 복구로 볼 수 있다. 국토안보부는 이들 임무를 수행하기 위하여 크게 4개의 기능으로 조직된다.

3.2.1 국경·교통 안전

국토안보부는 미 국경·해역·교통 시스템의 보전에 관계되는 연안경비대, 세관국, 이민국, 국경경비대, 교통안전국, 동물검사국, 주요 연방기관 모두의 권한을 총괄 한다. 국토안보부는 비자발행을 포함하여, 국경관리업무를 중앙으로 일괄 집중관리한다.

3.2.2 긴급사태에 대한 대응

연방 비상관리국이 해온 업무를 중심으로 연방 대응계획(Fedreal Response Plan), 국내 긴급사고대응 계획(National Contingency Plan), 미국정부기관 연대에 의한 국내테러 대책 작전계획(US Government Interagency Domestic Terrorism Concept of Operations Plan), 연방방사선 대응 계획(Federal Radiological Response Plan) 등 연방정부의 다양한 긴급대응계획을 하나의 정부전체의 계획에 통합한다. 또 국내 즉시대응 Traing Program에 대한 연방정부 수준에서의 지원이나, 재해대응활동의 조정도 행한다. 국토안보부는 핵긴급수색 팀이나, 국내 약품보관에 관련한 긴급대응권한도 가지게 된다.

3.2.3 화학·생물·핵병기 테러 대책

국토안보부는 CBRN 병기를 사용한 테러에 대한 연방수준에서의 대책·대응을 조직화한다. CBRN 테러 공격에의 대책·대응에서는 국가정책이나, 주·지방정부에의 가이드라인 책정, 연방·주·지방 각 수준의 대응팀에 대한 교육·훈련을 지휘해 나간다. 국토안보부은 치료·백신·해독제 등 일련의 대책을 국가수준에서 개발해 나가는 것을 목표로 하고 있다.

3.2.4 정보분석·기반시설 보호

국토안보부는 정보분석·기반시설보호국을 통해서, 국토안보부에 관계되는 다양한 정보기능을 융합하는 중앙 허브적인 역할을 담당한다. 특히, 중앙정보부(CIA), 연방수사국(FBI), 이민국, 마약국(DEA : Drug Enforcement Agency), 세관국 등 다수의 기관사이에서 정보를 공유하는 연결고리를 제공한다. 국토안보부는 또한 현재 및 장래의 위협을 평가특정하고 해당하는 취약성에 대비하여 국토안보자문 시스템(HSAS)를 통하여 권고를 발하고, 보호·예방조치를 강구한다. 주요 기반시설의 취약성을 평가하는 권한도 함께 가진다.

4. 국토안보법[6-8]

4.1 정의 및 구성

국토안보법에서 사용되고 있는 용어 중 주요한 것으로는 '국토'와 '테러리즘'에 대한 정의라고 할 수 있다.

먼저 본 법에서 의미하는 '국토'는 미국을 의미하고, 지리적 의미로 사용되는 때에는 미국의 모든 주(State), 특별 행정구, 푸에르토리코, 버진제도, 괌, 아메리칸 사모아, 북 마리아나 제도, 미국이 관할하는 영해 등을 의미한다.

한편 '테러리즘'에 대하여 본 법에서는 「인명에 위험하거나 주요기반시설 또는 핵심자원을 파괴할 잠재적인 행위와 미국의 모든 주 또는 기타 세부행정구역의 형법에 대한 위반행위를 포함하고, 일반국민을 협박하거나 위압하려는 의도, 협박이나 위압을 통하여 정부정책에 영향을 미치고자 하는 의도, 대량파괴, 암살 또는 납치 등을 통하여 정부의 업무수행에 영향을 미치고자 하는 의도를 나타낸다」고 정의하고 있다.

국토안보법은 총 17장으로 구성되어 있으며, 각 장의 제목은 다음과 같다.

<표 2> 국토안보법의 구성

Title 1.	국토안보부	Title 10.	정보보호
Title 2.	정보분석 및 기반시설 보호	Title 11.	법무부 부서
Title 3.	국토안보 지원에 있어서의 과학기술	Title 12.	항공회사 전쟁위험 보험 법령
Title 4.	국경 및 교통안전국	Title 13.	연방 노동력 개선
Title 5.	비상대비 및 대응	Title 14.	테러대응을 위한 항공기 조종사의 무장
Title 6.	미국과 기타 정부조직들의 군대구성원을 위한 자선기금	Title 15.	전 환
Title 7.	관리	Title 16.	항공교통 안전과 관련된 기존 법률
Title 8.	비연방실체들과의 조정	Title 17.	관련 규정 및 기술적 개정
Title 9.	국토안보회의		

4.2 국토안보부의 임무

국토안보법 제2장에서는 국토안보부의 임무, 국토안보부 장관과 관련 공무원 등 신설되는 국토안보부의 조직구조에 관하여 규정하고 있다.

SEC. 101에서 국토안보부의 임무에 관하여 규정하고 있으며, 내용은 다음과 같다.

- 미국내에서의 테러리스트 공격 억지
- 테러리즘에 대한 미국의 취약성을 감소
- 미국 내에서 발생한 테러리스트의 공격으로부터 손상을 최소화하고, 복구를 지원
- 자연적·인위적 위기와 비상계획에 관하여 중심으로서의 활동을 포함하여, 국토안보부로 이관된 실체들의 모든 직무를 수행
- 국토안보에 직접적으로 관련되지 않은 국토안보부내 기관 및 산하부서의 직무가 명시적인 특정명령에 의하여 축소되거나, 예외로 간과되지 않도록 보증
- 국토안보를 목적으로 한 노력, 활동 및 프로그램에 의하여 미국 전체의 경제안보가 축소되지 않도록 보증
- 불법 마약 거래와 테러리즘간의 연계를 감시하고, 당해 연계를 단절시키기 위한 노력을 조정하며, 기타 불법마약거래를 금지하기 위한 노력에 기여

4.3 정보분석 및 기반보호

4.3.1 임무와 정보접근

9.11 테러 사건 이전 미국에서는 외국정보 수집을 담당하는 CIA와 같이 국내의 위협 등을 분석하는 첩보기능이 미약하였다. 이에 따라 국토안보부는 국내 위협요인을 적절하고 세밀하게 분석하여, 관련 정보를 기반으로 경보발령 등 테러공격에 적절히 대처하기 위하여 CIA, FBI, NSA 등 첩보기관 및 각급 기관들과의 파트너쉽 강화를 주요기능의 하나로 규정하고 있다.

이를 위하여 국토안보부는 정보분석 및 기반보호를 위하여 담당 차관을 두고, 그 아래 다시 정보분석 담당 차관보와 주요기반보호 담당 차관보를 두게되고 본국에서 수행하는 임무에 관하여 규정하고 있고 주요한 것들로는 다음과 같은 것이 있다.

- 첩보기관 등 각급기관의 정보에 접근, 수신, 분석, 통합, 배포를 위한 협력 강화
- 테러리스트 공격에 대비한 위험평가, 핵심자원·주요 기반시설에 대한 포괄적인 취약성 평가
- 각급기관에 대한 보호 및 지원대책에 대한 우선 순위 식별을 위하여, 관련 정보분석,

취약성 평가 등을 통합
- 핵심자원 및 주요 기반시설의 안전을 확보하는 국가계획 개발
- 핵심자원 및 주요 기반시설을 보호하기 위하여 각급기관과 조정, 대책 권고
- 국가자문 시스템(Homeland Security Advisory System) 관리
- 정보분석 및 주요 기반보호 임무수행을 위하여 데이터 마이닝 및 기타 첨단 분석 툴을 포함한 안전한 통신 및 정보기술 기반 확립, 활용
- 각급 기관에 대한 교육 및 기타 지원을 조정

그리고 정보분석 및 기반보호를 위하여 국토안보법은 연방기관이 수집하는 미국에 대한 테러리즘의 위협과 관련 보고서, 분석서, 미평가첩보 등을 포함한 모든 정보와, 테러리즘에 대한 미국의 기반시설이나 기타 취약성에 관한 모든 정보에 대하여 당해 정보의 분석여부와 관계없이 필요한 경우에 접근할 수 있다. 또한 2001년 미국테러 방지법(The USA PATROIT ACT of 2001), 미 연방법령집 Title 18, Section 2517(6), 연방형사소송규칙(Federal Rules of Criminal Procedure) 6(e)(3)(C)에 따라 CIA에 제공될 필요가 있는 법 집행기관들로부터의 모든 정보를 제공받게 된다.

이러한 임무를 위하여 국무부, CIA, FBI, NSA, 국립영상지리원(NIMA), 국방정보국(The Defense Intelligence Agency)과 기타 기관의 인원이 분석 및 관련 직무의 수행을 지원하기 위하여 국토안보부로 파견된다.

한편 아래와 같은 기관들의 직무, 인원, 자산, 책임 등은 국토안보부로 이관된다.

- 연방 수사국(컴퓨터 수사 및 운용 섹션 이외의)의 국가 기반 보호 센터(NIPC)
- 국방부의 국가통신 시스템(NCS)
- 상무부의 주요 기반 보장국(CIAO)
- 에너지부의 국가 기반 시뮬레이션 및 분석 센터(The National Infrastructure Simulation and Analysis Center)와 에너지부의 에너지 안보 및 보장 프로그램 및 활동
- 총무청(General Services Administration)의 연방 컴퓨터 침해사고 대응 센터(Federal Computer Incident Response Center)

4.3.2 주요 기반정보

국토안보를 위하여 연방, 주 또는 법률을 위반하거나, 각 주 사이의 상거래에 대한 위해, 공중보건이나 안전을 위협하는 것으로서, 물리적 공격, 컴퓨터 기반 공격 또는 기타 유사한 행위에 의한 주요기반시설이나 보호시스템에 대한 현재, 잠재적 또는 임박한 공격, 손상 또는 무력화 등[1]과 관련된 정보를 주요기반정보라고 규정하고 있다.

이러한 정보가 각급 기관으로부터 자발적으로 국토안보부로 제공된 경우, 당해 정보는 형법상 수사나 기소, 의회나 위원회 관련 문제, 회계감사원(GAO)의 임무수행과정과 관련된 경우를 제외하고는 미연방 법령집 Title5의 SEC. 552(정보공개법)에 의한 공개로부터 면제된다.

이에 위반하여 고의로 공표, 누설, 공개 또는 고지한 자는 벌금부과, 1년 이하의 징역 등에 처해질 수 있다.

4.3.3 정보보호, 사이버보안 강화

정보보호에 있어서 국토안보부는 정보의 보안 및 기밀성 등을 보장하도록 하는 정보공유 절차, 프라이버시 보호 관련 업무를 수행하는 프라이버시 책임자, 지역 사회의 정보시스템 및 전기 통신 망에 대한 공격으로부터의 대응 및 복구를 지원하기 위하여 과학 및 기술의 해당 분

1) Title 2, Sub Title B, SEC. 212, (3).

야에 전문 지식을 갖고 있는 자원 봉사자의 지역 팀으로 구성된 「NET GUARD」라는 국가 기술 경비대(national technology guard)의 창설을 규정하고 있다. 한편 SEC. 225에는 사이버보안 강화법(Cyber Security Enhancement Act of 2002)이 삽입되어 규정하고 있다.

4.4 사이버 보안 강화법[9]

공격에 대한 효율적인 정보수집을 위하여 법집행기관의 정보수집 능력을 강화하기 위하여 사이버 보안 강화법 제정이 대두되었고. 별도의 법률안으로 법제정이 추진되었으나, 2002년 11월 국토안보법안을 통과시킬 때 동 법안의 통과에 앞서 사이버 보안 강화법(Cyber Security Enhancement Act : CSEA)을 국토안보법에 삽입하여 통과시켰다.

제2장 SEC. 225에는 사이버보안 강화법은 총 10개의 세부항목으로 구성되어 있으며, 주요한 것으로는 양형위원회(Setencing Commision)[2] 관련 내용, 긴급 공개 예외(Emergency Disclosure Exception), 선의예외(Good Faith Exception), 불법장치의 인터넷 광고, 형벌강화, 프라이버시 보호 등이 있다.

4.4.1 양형위원회의 가이드라인 수정

먼저 양형위원회와 관련해서는 컴퓨터 사기 및 남용에 관한법(CFAA : Computer Fraud and Abuse Act)인 미연방법령집 Title. 18 §1030과 관련하여, 공격의 심각성, 공격의 증가발생율, 효과적인 억제 및 적절한 처벌에 대한 필요성을 반영하도록 양형 가이드라인을 수정하도록 하고 2003년 5월 1일 이전에 관련 보고서를 의회에 제출토록 하고 있다.

4.4.2 긴급시 공개 예외 규정

9.11 이전 연방 전자통신 프라이버시법(ECPA : Electronic Communication Privacy Act)에서는 일반 공중에 대하여 전자통신 서비스를 제공하는 자(예컨데 ISP)가 저장된 고객의 통신들(예컨데 voicemail, e-mail, 첨부물)을 고의로 누설하는 것은 일반적으로 금지되어 있었다. 예를 들어 정부가 SEC. 2703.(Requirements for governmental access) 규정에 따라 181일 미만 동안 보관되어 있던 e-mail 내용을 확보하기 위해서는 상당한 이유를 제시하고 이에 따른 사법적 판단이 요구되는 수색 영장(search warrant)이 필요했었다.

이러한 것이 9.11 테러 사건 이후 10월 26일에 「USA Patriot Act」가 제정되면서 ECPA의 공개 금지 규정에 긴급시 예외 조항이 만들어지게 되었다. 즉, 서비스 제공자는 '어떤 사람에 대한 급박한(immediate) 생명의 위험이나 심각한 신체의 상해를 수반하는 긴급상황이, 지체없는 당해 정보의 공개(disclosure of information)가 필요하다고 합리적으로 신뢰[3]한때에는 법집행기관에게 이러한 contents를 제공할 수 있도록' 하고 있다.

서비스 제공자에게 긴급시 영장없이 자신이 제공하는 서비스 관련 통신 내용들을 제공할 수 있게 되었으나, 사이버보안 강화법은 이러한 긴급시 공개 예외 규정을 대폭 강화하여, '제공자가 어떤 사람에 대한 생명의 위협이나 심각한

2) 1984년 양형개혁법(Sentencing Reform Act)에 의거 사법부 산하의 독립 연방 기구로서 설립되었으며, 연방법원의 양형기준 개발, 범죄와 양형에 관련된 정보수집, 범죄와 양형에 대하여 의회, 행정부, 사법부에 자료제공 등을 임무로 하고 있다.

3) reasonable belief는 합리적 인식 또는 합리적 확신으로, 사실을 오인한 것이 통상인(reasonable man)이라면 그만둘 수 없었음을 이유로 정당화되는 경우의 기준을 말한다. 형사소송법에서는 영장없는 체포·수색·압수가 정당화되기 위하여 필요한 요건이 충족되었다고 할 수 있는 합리적 확신을 말한다.

신체적 상해를 수반하는 긴급상황이, 이와 관련된 통신의 지체없는 공개가 필요하다는 것을 선의로 믿는 경우 연방, 주, 또는 지방정부 기관에 대하여' 이러한 contents를 공개할 수 있도록 하고 있다.

이는 「USA Patriot Act」에서의 규정보다 ISP의 정보공개(disclosure of information)의 요건을 크게 세 가지 점에서 강화했다고 할 수 있다.

첫째, 가장 중요한 것으로 contents의 공개 대상이 더 이상 법집행기관으로 한정되지 않는다는 것이다. 즉, 비상상황의 경우에는 정부기관이면 누구나 ISP에게 관련 contents의 제공요구를 할 수 있게 된 것이다.

둘째, ISP에게 더 이상 사실에 대한 객관적 판단 기준인 합리적 확신(reasonable belief)을 요구하지 않는다는 것이다. 사이버보안 강화법에서는 단순히 ISP에게 주관적인 확신인 선의의 확신(good-faith belief)만을 요구한다는 것이다.

셋째, 비상상황에 더 이상 생명에 대한 **'급박한(immediate)'** 위험이라는 요소가 필요치 않고, 단지 애매한 시간에 '생명에 대한 위험' 만을 그 요소로 하고 있다.

한편 이러한 contents를 수신한 정부기관은 당해 공개 이후 90일 이내에 공개가 이루어진 근거규정인 Section의 Paragraph, 공개일, 공개가 이루어진 대상인 기관, 공개된 정보와 관련된 고객이나 신청자의 수, 통신의 수를 진술한 보고서를 법무부 장관에게 제출하여야 하며, 법무부 장관은 모든 당해 보고서를 본 법의 제정일 1년 후에 의회에 제출할 단일의 보고서로 만들어 공표하여야 한다.

4.4.3 선의의 예외[4] 규정

이 조항 역시 「USA Patriot Act」에 의하여 규정된 '컴퓨터 침입자(computer trespasser)' 예외를 이용하는 ISP에게 감청의 예외를 확대시켜 주는 것이다.

ECPA에서는 일반적으로 유선이나 전자통신(electronic communication)의 감청이 금지되어 있고, 예외적으로 자신의 권리나 재산을 보호하기 위하여 컴퓨터 소유자에게 자신의 기계장치에 대한 활동을 모니터하는 것을 허용하고 있었다.

9.11 테러 사건이후 「USA Patriot Act」에서는 '컴퓨터 침입자'를 '권한없이 보호되어 있는 컴퓨터에 접근하거나, 보호되는 컴퓨터에 전해지거나, 이를 통하여 전달되거나, 이로부터 전달되는 어떠한 통신에서 프라이버시에 대한 합리적인 기대를 할 수 없는 자'를 의미한다. 그러나 컴퓨터 침입자는 '보호되는 컴퓨터 소유자나 운영자와 당해 컴퓨터의 전부 또는 일부에 대한 접근을 위하여 현재 계약상 관계를 가지는, 보호되는 컴퓨터의 소유자나 운영자가 알고 있는 자'[5]는 명백하게 제외된다.

「USA Patriot Act」는 컴퓨터의 소유자나 운영자가 타인에게 법적 외관(주법의 행위)으로 이러한 컴퓨터 침입자라고 믿을 수 있는 자의 통신을 감청할 수 있도록 하고 있다. 또한 그렇게 감청을 행하는 자는 자신이 감청하는 컴퓨터 침입자 통신의 contents가 적법한 수사와 관련될 것이라고 믿는데 합리적인 근거를 가져야 한다[6].

---

4) 1970년대 후반에 들어서면서 위법수집 증거배제법칙에 대한 전면적 폐지론과 불합리성 및 무효성이 현저한 부분에 한하여 배제를 요구하는 '선의의 예외'이론이 나타났다.
'선의의 예외이론'은 증거배제 법칙을 실질적 절차위반의 경우에는 적용하고 중대사법이나 어떤 가이드라인을 정하여 절차위반이 사소한 경우에는 그 적용을 배제하자는 것인데, 1984년의 Leon 사건과 Sheppard 사건에서 확립되어 연방대법원의 판례로서의 지위를 취득하였다. 위 이론의 채용은 위법수집증거를 피고인의 유죄 입증을 위한 본증에 재공하는 것을 금지하는 배제법칙의 중핵 부분에 제약을 가한 것으로 종래의 배제법칙에 대한 질적변화를 인정한 것으로 볼 수 있다.

5) 예를 들면 ISP의 고객과 같은 경우는 본 조항의 '컴퓨터 침입자'가 될 수 없다.

6) 이렇게 법원의 사전영장을 발부 받지 않고, 통신감청을 행할 수 있게 되는 예의의 경우를 EFF 등

사이버보안강화법에서는 이러한 컴퓨터 소유자나 운영자가 선의의 경우에는 감청을 의뢰한 경우 민사상, 형사상 책임이 면제되는 것으로 하고 있다.

4.4.4 감청 설비의 전자적 광고 금지

ECPA에서는 오랫동안 감청설비에 대하여 장비의 디자인이 유선, 음성, 전자 통신의 비밀 감청이 본래의 목적인 것을 나타내는데 유용하다는 것을 알거나 알아야 할 설비의 제조, 배포, 소유 또는 광고가 금지되었다[7]. 그러나 광고는 '신문, 잡지, 광고지 또는 기타 출판물(other publication)에 속하는 것에 한하였다.

사이버보안 강화법에서는 광고의 제한에 대하여 두 가지 변화가 있었다. 먼저 '기타 출판물' 뒤에 '또는 전자적 수단에 의한 배포(or dissenminates by electronic means)'를 삽입하여, 전자적 수단에 의한 감청설비의 광고를 제한하였다. 그리고 광고를 하는 자가 광고의 내용을 알아야 한다는 내용을 삽입하여 구체적으로 명시하고 있다[8].

4.4.5 컴퓨터 범죄에 관한 처벌의 강화

미국의 연방 컴퓨터 법률인 컴퓨터 사기 및 남용에 관한 법률(18 U.S.C. §1030)에서는 고의로 프로그램, 정보, 명령(command)의 전송하고 그 결과로서 보호되고 있는 컴퓨터에 대하여 권한없이 손해를 야기한 행위를 불법으로 처벌하고 있다[9]. 9.11 테러 사건이전에는 이러한 범죄를 야기한 자에 대한 처벌이 초범의 경우에는 5년 이하의 징역, 상습범의 경우에는 10년 이하의 징역이 최고형이었다. 그러나 9.11 테러 사건 이후 「USA Patriot Act」 제정으로 보호되는 컴퓨터에 대한 손해를 가한 해커에 대한 최고 형량을 초범에게 10년, 상습범에게는 최고 20년형으로 상향 조정하였다.

그러던 것이 금번의 사이버보안 강화법에서는 새로운 처벌 조항이 신설되었다. 즉, 공격자가 고의 또는 부주의로 Subsection (a)(5)(A)(i)의 위반행위로부터 심각한 신체적 상해를 유발하거나 시도하는 경우, 본 Title에서 정한 벌금이나 20년 이하의 징역 또는 이를 병과하거나, 공격자가 고의적 또는 부주의로 Subsection (a)(5)(A)(i)의 위반행위로부터 사망을 유발하거나 유발하고자 시도하는 경우 벌금이나 유기 또는 무기징역이나 또는 이를 병과라고 규정하여, 신체의 상해나 생명의 위험과 관련된 컴퓨터 범죄의 처벌을 강화하였다.

4.4.6 조력자에 대한 책임 면제

ECPA는 정부의 통신 감시에 조력하거나, 정보를 제공하는 통신 서비스 제공자에게 책임을 면제하고 있다[10]. 사이버보안 강화법에서는 책임을 면제하는 이러한 두 가지의 경우에 모두 법적 인증(statutory authorization)을 추가하여, 정부기관으로 하여금 법적 인증만으로 통신감청시 정보제공이나 조력을 강제할 수 있도록 하였다.

4.4.7 긴급시 pen-trap 권한

미국에서는 일반적으로 누구도 법원의 명령

프라이버시 옹호단체들은 비난하고 있다.

7) 미연방법령집 Title 18. §2512. Manufacture, distribution, possession, and advertising of wire, oral, or electronic communication intercepting devices prohibited.

8) 일부에서는 광고의 제한과 관련된 변화 중 첫 번째에 대한 내용에 대하여 '기타 출판물'이라는 기존의 요건으로도 전자적 수단에 의한 배포를 확대해석할 수 있는데도 불구하고, 요건을 추가한 것이라는 불필요성을 제기하고 있다.

9) 미연방법령집 Title 18. §1030(a)(5)(A)(i).

10) (미연방법령집 Title 18. §2703(e), 법원의 명령, 영장, 소환장, 증명에 따라 정보, 시설, 조력의 제공); (미연방법령집 Title 18. § 2511(2)(a)(ii), 그러한 조력을 지시하는 법원의 명령 또는 특정 공무원에 의한 서면의 증명서).

없이는 pen register나 trap-and-trace 장비를 사용할 수 없다[11]. 그러나 긴급시의 경우 지정된 법집행기관 공무원은 pen/trap 장비를 법원의 명령없이 사용할 수 있지만, 48시간 이내에 법원의 명령을 획득하여야 한다[12]. 여기서 '긴급시(emergency)'라 함은 '어떤 사람의 생명에 대한 급박한 위험이나 심각한 신체적 상해'와 '조직범죄의 특징인 공모활동'의 경우를 포함하는 것이다.

USA Patriot Act에서는 긴급시에 관한 규정이 변화하지 않았다. 그러나 USA Patriot Act에서는 명백하게 pen/trap의 권한 범위를 확대하여 카니보어(Carnivore)와 같은 패킷스니핑(packet-sniffing) 기술의 사용을 확대하였다.

사이버보안 강화법에서는 긴급시의 정의를 확대하여, '국가 안보이익에 대한 직접적인 위협' 또는 '1년 이상의 징역에 처할 수 있는 범죄의 성질을 갖는(Section 1030에서 정의된 바와 같은) 보호되는 컴퓨터에 대하여 진행 중인 공격'의 경우도 긴급시에 포함시켜 pen/trap 사용의 예외의 경우를 확장하였다.

4.5 정부 정보보안 관리법[10]

컴퓨터보안법(Computer Security Act of 1987), 문서감축법(Paperwork Reduction Act of 1995), 행정명령 13011 등의 위임에 의하여 미국 연방정부의 컴퓨터보안을 포함한 정보자원관리의 중심기관은 OMB이다. OMB는 이러한 업무를 수행하기 위하여 Circular A-130의 부록 3에서 연방정보보안정책에 필요한 최소한의 통제장치들을 수립, 각 정부기관들이 정보보안에 관한 책임을 지도록 요구하고 있고, 각 기관들의 정보보안 프로그램과 기관관리통제 시스템을 상호 연계시키고 있었다.

11) 미연방법령집 Title 18. §3121(a).
12) 미연방법령집 Title 18. §3125.

그러나 OMB의 지침성격을 가진 Circular A-130으로는 급증하고 있는 새로운 보안침해 및 기술에 대하여 충분한 대응을 할 수 없다는 인식하에 기존의 연방정부의 보안정책에 대한 보완의 필요성이 제기되었다. 이에 따라 정보 및 시스템에 대한 기밀성·무결성·인증·부인방지 확보, 정보보안 정책 수립 집행, 보안침해에 대한 탐지·보고·대응 절차, 감사관 및 수사관 등에 대한 통보·자문 절차, 보안 프로그램 관리자의 매년 기관자체 정보보안 프로그램 평가, 예산·정보자원관리·성과관리 등과 관련하여 정보보안 프로그램 관리와 평가 측면을 강조하기 위하여 2000년 10월 정부 정보보안 개혁법(Government Information Security Reform Act)이 제정되었다.

그러나 정부 정보보안 개혁법이 2002년 10월까지 유효한 한시법적 형태를 가지고 있는 반면, 연방정부의 정보보안관리 강화의 필요성은 계속되었다. 이에 따라 정부 정보보안 개혁법을 영구화할 수 있는 방안으로 연방 정보보안 관리법(Federal Information Security Management Act)안이 제출되었고, 2002년 11월 국토안보법의 일부로서 제정되었다.

연방 정보보안 관리법은 2000년의 정부 정보보안 개혁법의 기본적인 내용에 정보보안과 관련하여 정보시스템의 무결성, 기밀성, 가용성을 보장하기 위하여 각급기관들이 'best practices'를 이용하게 하고, 최소한의 정보보안 통제를 위한 표준과 기준의 개발 및 유지에 있어 국립표준기술원(NIST)의 역할을 강화하는 등 몇몇 조치가 부가되었다.

4. 결 론

9.11 테러 이후 부시 행정부의 '테러와의 전쟁'의 일환으로 추진된 국토안보부 설치 근거법인 국토안보법안은 공무원의 고용 안정이 불안해질

수 있다는 민주당의 반대로 초기에는 법안 성립에 어려움을 겪었다. 그러나 2002년 11월 13일 하원에서 찬성 299, 반대 121의 압도적 표차로 가결된 뒤 상원 표결도 통과한 이 법안은 부시 대통령의 서명으로 결국에는 성립하게 된다.

국토안보부의 설립을 통하여 미국은 향후 다양한 시스템의 통합·조정, 비즈니스 프로세스의 재구축, 연락조정, 리더쉽의 통제 등 다양한 부문에서 전례 없었던 시도를 하게될 것이다.

국토안보부의 창설과 운영을 위한 미국의 노력은 단순히 하나의 부서를 새롭게 창설했다는 것 이상의 의미를 가질 것으로 생각된다. 국토안보부는 행정적 모델의 효율적 수행을 위하여 첨단기술의 적절한 활용을 시도하고 있다. 결국 여기서 얻은 경험이 현재 진행중인 각 전자정부 프로젝트에 반영되는 등 미국 전체의 전자화·효율화가 가속화될 것이 예상된다.

이는 사이버보안 부분에 있어서도 마찬가지이다. 지난 1.25 인터넷대란에서 알 수 있듯이 국내의 사이버보안 수준은 아직까지 보완할 점이 많은 것으로 판단된다.

이러한 시점에서 정보화분야의 최강국인 미국이 사이버안보를 국토안보의 일환으로 인식하고, 이에 대한 효율성을 강화하기 위하여 취하는 노력은 우리에게 주는 시사점이 크다 할 것이며, 향후 국내에서 논의되는 정보보안 및 정보보호 정책수립에 있어 국가안보 수호차원에서 접근하는 시각을 갖추는 것이 필요한 시점이라 할 것이다.

참 고 문 헌

[1] 김현수 외 2인, 9.11 테러이후 미국·일본의 대응동향, Security Issue 2002-4, 2002. 6.

[2] Establishing the Office of Homeland Security and the Homeland Security Council, Executive Order 13228 of October 8, 2001.

[3] Homeland Security Presidential Directive-1, October 29, 2001.

[4] Cyber Security Research and Development Act.

[5] George W. Bush, The Department of Homeland Security, 2002. 6.

[6] Homeland Security Act of 2002.

[7] Whitehouse, Analysis for the Homeland Security Act of 2002. 2002. 6.

[8] The Brookings Institution, Assessing the Department of Homelan Security, 2002. 7.

[9] Cyber Security Enhancement Act of 2002.

[10] Federal Information Security Management Act of 2002.

김 현 수

1997년 부산대학교 사법학과 법학학사
1999년 부산대학교 대학원 법학과 법학석사
2000년~2001년 한국정보보호진흥원 연구원
2001년~ 현재 국가보안기술연구소 연구원

박 상 서

1991년 중앙대학교 전자계산학과 공학사
1993년 중앙대학교대학원 전자계산학과 공학석사
1996년 중앙대학교대학원 컴퓨터공학과 공학박사
1996년~1998년 국방정보체계연구소 선임연구원
1998년~1999년 국방과학연구소 선임연구원
2000년~현재 국가보안기술연구소 선임연구원
2001년~현재 한국사이버테러정보전학회 이사