통합적 사이버 위기관리 체계의 필요성에 관한 연구 : 미국과 한국의 제도 및 정책 비교를 중심으로

김민식* · 박상돈* · 권헌영** · 김일환*** · 임종인****

요 약

미국은 국토안보부에서 '국토안보법'에 근거하여 공공과 민간부문 전체에 걸쳐 사이버공격과 그로 인한 위기사태를 예방하고 대응하기 위한 실질적인 조치들을 수행한다. 한국의 경우 공공분야와 민간분야에 따라 또는 주요정보통신기반시설 여부에 따라 적용 법령 및 주관기관이 달라지는 형태를 갖는다. 본 논문에서는 미국의 일원화된 사이버 위기관리 체계의 소개를 통해 우리나라 사이버 위기관리 체계 수립에 있어서 통합적이며 조직적으로 이루어지는 것이 예방의 효율성과 대응의 적시성 등에 있어 바람직함을 일깨우고자 한다.

A Study on the Need of Unified Cyber Crisis Management System : Around Comparison about Policies and Systems of USA and Korea

Min Sik Kim* · Sang Don Park* · Hun Yeong Kwon** · Il Hwan Kim*** · Jong In Lim****

ABSTRACT

According to Homeland Security Act of 2002, DHS in USA is comprehensively responsible for execution of protection methods on the public and private sectors against cyber attack for USA cyber crisis management. There are different laws and organizations according to the sector that is the public, the private, CII(Critical Information Infrastructure, or Non-CII in Korea. In this paper, we show the unified cyber crisis management of USA makes korea realize the importance to integration and systematization for the national cyber crisis management system.

Key words : Cyber Crisis Management, Cyber Security Policy

접수일 : 2008년 12월 28일; 채택일 : 2009년 3월 3일

* ETRI 부설연구소

** 광운대학교 과학기술원학과

*** 성균관대학교 법학과

**** 고려대학교 정보경영공학전문대학원

1. 서 론

정보통신 기술의 발달과 인터넷의 급속적인 보급으로 인해 유비쿼터스 환경이 도래하고 있다.

그러나 이러한 발전과 동시에 컴퓨터 웜·바이러스의 창궐과 사이버 공격이 급증하고 있으며, 사이버공격 기법은 갈수록 지능화되어가고 있다.

또한 사이버 공격은 단순 해킹에서 점진적으로 금전적인 목적을 갖는 해킹이나 국가간의 사이버 전쟁 등의 다양한 형태로 나타나고 있다.

대표적인 예로 2007년 5월에는 러시아 해커들이 에스토니아 전산망을 공격해 에스토니아가 3주간 마비 상태에 빠진 일이 있었으며, 2008년 8월에는 러시아가 사이버 공격을 통해 그루지야의 정부·언론·금융·교통 전산망을 무너뜨려 그루지야가 초토화된 사건이 있었다. 보안 전문가들은 이런 공격이 익명으로, 비교적 적은 비용으로, 그리고 세계 어디서나 이뤄질 수 있다는 점에 주목하고 있다는 것이다.

이처럼 정보통신망에 대한 사이버 공격은 최악의 경우 금융·교통·산업·방송·의료 등의 마비로 국가 전체의 위기를 초래할 수 있으므로 사이버 위기관리의 중요성이 부각됨과 동시에 각 국가는 자국의 사이버 위기관리에 심혈을 기울이고 있다.

사이버 공격의 급증으로 국가차원에서 사이버위기를 효율적으로 관리하고 극복할 수 있는 사이버 위기관리 체계에 대한 관심이 집중되고 있는 현시점에서, 본 논문에서는 사이버 위기관리 체계의 대표적인 모델인 미국의 사이버 위기관리 체계의 동향을 파악함과 동시에 한국의 사이버 위기관리 체계의 발전 방향을 제시하고자 한다.

본 논문의 구성은 다음과 같다. 제 2장에서는 미국 사이버 위기관리 체계를 살펴보고, 제 3장에서는 한국 사이버 위기관리 체계를 분석하며, 제 4장에서는 미국과 한국의 사이버 위기관리 체계를 비교한 후, 제 5장에서 결론을 내리고자 한다.

2. 미국 사이버 위기관리 체계

2.1 사이버 위기관리 관련 법

2.1.1 관리예산처(OMB : Office of Management and Budget) Circular A-130

관리예산처는 Circular A-130을 발표하여 정보자원의 관리와 정보보안에 있어 요구되는 임무 수행에 필요한 사항들을 기술하고 있다.

OMB Circular A-130의 <부록 Ⅲ>연방정보자원보안(Security of Federal Automated Information Resources)은 연방 정보보안 정책에 필요한 최소한의 통제장치들을 수립, 각 기관들이 정보보안에 대한 책임을 지도록 하면서 각 기관 정보보안 프로그램과 관리통제시스템을 상호 연계시킨다. 세부 내용에 따르면 관리예산처는 연방정보자원 보안정책을 총괄 및 감독하며, 상무부 특히 국립표준기술연구소(NIST : National Institute of Standards and Technology)는 보안 관련 표준 및 지침을 개발하고, 인사관리처(OPM : Office of Personal Management)는 정보보안 교육 및 훈련을 지원하고 각 기관의 침해사고 대응 및 취약성 정보 공유 및 조정 등을 포함한 기타 기관들의 역할을 규정하고 있다[9].

2.1.2 연방정보보안관리법(Federal Information Security Management Act of 2002)

연방정보보안관리법은 2002년 11월에 만료 폐기된 정부정보보안개혁법(Government Information Security Reform Act of 2000)의 한시법 조항을 삭제하고, 전자정부법 2002(e-Government Act of 2002)의 제 3장 정보보안에 삽입된 법이다. 연방정보보안관리법의 목적은 연방정부의 운영 및 자산에 대한 정보보안 통제항목의 효율성을 강화하기 위한 총괄적인 프레임워크 제공, 국가보안 및 법집행기관 전반에 걸친 관련 정보의 보안 위험에 대한 효율적인 관리 및 통제방안 제공,

그리고 연방정부 정보 및 정보시스템 보호를 위한 최소한의 통제 및 유지 방안 개발 등에 있다[8].

연방정보보안관리법의 주요내용에 따르면, 연방정부 정보 및 정보시스템에 대한 정보보안을 강화하고 그 정보보안에 대한 효율성과 적절성을 확보하기 위하여 각 부처의 최고정보화담당과 감사관은 매년 자신들 부처의 정보보안 프로그램을 점검하고 그 결과를 관리예산처에 보고해야 한다.

관리예산처는 각 부처의 보고에 기초하여 각 부처에 대한 정보보안 관련 감독 책임을 다하고 있으며, 각 부처와 독립 감사관들이 제공한 보고서에 기초하여 각 부처의 연방정보보안관리법 실행에 대하여 매년 의회에 보고서를 제출해야 한다.

매년 각 부처는 자신들의 정보보안 프로그램과 관행의 효율성을 측정하기 위하여 이들에 대한 독립적인 평가를 하여야 한다.

추가적으로 연방정보보안관리법에서는 연방 각 부처의 장의 권한 및 책임으로 위험 평가 수행, 정보보안 정책 및 절차 마련, 정보보안 관련 세부 계획 수립, 보안 교육 및 훈련 실시, 정보보안 정책, 절차 및 그 실행에 대한 주기적 평가 실시, 정보보안 정책, 절차 및 실행에 있어서의 문제점을 해결하기 위한 대책 계획, 실행, 평가, 문서화, 대응 조치 실시 등의 절차 마련, 보안사고 탐지, 보고, 대응 절차 마련 등을 규정하고 있다[3].

2.1.3 국토안보법(Homeland Security Act of 2002)

2002년에 제정된 국토안보법에 따르면 국토안보부는 미국에 대한 위협과 테러에 대한 취약점을 경감시키며, 공격에 의한 피해복구 지원 및 위험을 최소화하기 위한 임무를 수행하도록 규정하고 있다. 세부 내용에 따르면, 국토안보부의 역할에는 미국내 테러 위협에 대한 취약성 제거, 미국내 테러 발생시 피해 최소화 및 복구 지원, 미국내 주요기반시설 및 자산의 취약성 평가, 위험평가 수행, 주요기반시설 및 자산 보호를 위한 국가전략 수립 등을 포함하고 있다[6].

2.1.4 사이버 보안연구개발법(Cyber Security Research and Development Act)

사이버 보안연구개발법은 사이버 보안 관련 연구수행의 절대 부족, 사이버 보안 연구를 지원하는데 있어 선도적 역할을 수행할 정부기관 부재, 사이버 보안 연구 수요를 해결할 수 있도록 준비된 과학자의 절대부족 등의 문제를 해결하고자 2002년 11월에 제정되었다. 사이버 보안연구개발법의 상세 내용에 따르면 국립과학재단(NSF : National Science Foundation)과 국립표준기술연구소에 새로운 연구프로그램을 신설하도록 규정하고 있다[7].

2.2 사이버 위기관리 관련 대통령령

HSPD-3(국토안보경보 시스템 : Homeland Security Advisory System)은 2002년 3월에 테러 위험과 관련된 정보를 공유하고 이를 사전에 경고할 수 있는 시스템 창출을 규정하고 있다[5].

HSPD-5(국내 사고관리 : Management of Domestic Incidents)는 2003년 2월에 미국내 사고 발생시 정부간 및 민간영역과의 효율적 협력을 통해 관리할 수 있도록 체계를 규정하고 있다. 同 명령에 따라 국토안보부(DHS : Department of Homeland Security)는 연방 국내사고 관리의 총 책임자로 지명되었으며 테러 공격, 주요 재난 발생 등과 같은 비상사태의 예방, 준비, 대응 및 복구를 위한 연방자원 배분 및 업무조정의 책임을 부여받았다[5].

HSPD-7(주요기반 식별, 우선순위 설정 및 보호 : Critical Infrastructure Identification, Prioritization, and Protection)은 2003년 12월에 테러 행위로부터 보호해야할 주요 기반시설/자산을 식별하고 보호활동의 우선순위를 설정하며 보호활동을 수행할 수 있는 프레임워크 구성을 규정하여 국토안보부 및 연방과 지방정부 등 기반시설 보호를 위한 참여자들의 책임과 역할을 정하고 있다[5].

HSPD-8(국가준비 : National Preparedness)은 2003년 12월에 미국의 테러활동에 대한 예방, 보호,

대응 및 복구를 강화할 수 있는 준비태세 강화 정책을 수립하도록 규정하고 있다[5].

HSPD-23/NSPD-54는 2008년 1월에 연방정부 사이버보안에 대해 커다란 전략적 변화를 꾀하고자 美 정부 전산망을 적극적으로 감시하는 정책을 수립하도록 규정하고 있으나, Classified Document로 분류되어 비공개 자료로 관리된다. HSPD-23/ HSPD-54의 요구에 의해 국토안보부 내에 국가 사이버 안전센터(NCSC : National Cyber Security Center)가 설립되었으며 국가 사이버 안전 센터의 미션은 연방 기관들간의 협력을 통해 사이버 위협으로부터 美정부의 컴퓨터와 통신 시스템을 보호하는 것으로 알려지고 있다[4].

2.3 사이버 위기관리 관련 전략

국토안보 국가전략(National Strategy for Homeland Security)은 2002년에 발표된 것으로 주요 기반시설 및 자산 보호 강화 및 위기상황에 대한 준비태세 및 대응능력 강화 내용을 포함한다. 국토안보 국가전략 세부내용을 살펴보면 주요 기반시설 및 자산 보호를 위한 사이버 공간 보호를 위한 프로젝트 실시, 국토안보부가 주요 기반시설 보호를 총괄하도록 업무조정, 주요기반시설 및 자산에 대한 정확하고 완벽한 평가, 위협으로부터 주요 기반시설과 자산 보호, 국제공동체와 협력하여 국가간 주요 기반시설 보호 강화 등을 포함하고 있다.

2003년에는 사이버 공간 보호를 위한 국가전략(National Strategy to Secure Cyberspace)이 발표되었다. 사이버공간 보호를 위한 국가전략은 사이버 보안의 비전을 설정하고 주요 기반시설 및 주요 자산의 사이버 보안 지침으로 활용되고 있으며, 주요 내용을 보면 5대 주요 프로그램으로 국가 사이버공간 보안 대응 시스템(National Cyberspace Security Response System), 국가 사이버보안 위협 및 취약성 감소 프로그램(National Cyberspace Security Threat and Vulnerability Reduction Program), 사이버보안 인식 및 훈련 프로그램(National Cyberspace Security Awareness and Training Program), 정부영역의 사이버보안 강화(Securing Government Cyberspace), 국가보안 및 국제 사이버보안과의 협력강화(National Security and International Cyberspace Security Cooperation) 등을 언급하고 있다.

2004년에는 국가 사고 관리 시스템(NIMS : National Incident Management System)을 통해 연방, 주 및 지역정부간 사고대응 단일 체계 수립 및 표준화된 관리계획이 국토안보부에 의하여 발표되었다[1]. 테러 발생 예방, 국토안보 보장, 주요 기반시설 및 핵심자산 보호 및 복구 등의 목적으로 사고관리 절차 및 모범사례를 통합해 단일화된 구조로 재구성한 국가 대응 계획(NRP : National Response Plan)도 같은 해 발표되었으며, 국가 대응 계획은 2008년 국가 대응 프레임워크(NRF : National Response Framework)로 대체되었다.

2006년 6월 국토안보부는 핵심 정보보호전략으로 국가 기반 구조와 주요자원 보호 프로그램을 구현하기 위한 것을 목표로 하는 국가 기반 보호 계획(NIPP : National Infrastructure Protection Plan)을 발표하였다.

2008년 1월 Bush 대통령이 “NSPD-54/ HSPD-23”을 승인함으로서 이를 바탕으로 한국가 사이버 보안 종합전략(CNCI : Comprehensive National Cyber Security Initiative)이 수립되었다. 이는 신 사이버 보안을 위해 결정한 비밀정책이다. 이것이 의미하는 바는 지금까지는 각각의 침입사고에 대한 사후 대응에 비중이 높았다면, 이제 사전대응 체계 구축으로 사이버안보를 달성하겠다는 것으로 향후 美 연방정부에서 국내외 침입 및 미래의 위협에 대해 방어할 수 있도록 컴퓨터 시스템을 안전하게 만드는 새로운 모델을 만들 것으로 보인다[10-14].

3. 한국의 사이버 위기관리 체계

한국의 현행 관련 법률에 따른 사이버 위기관리체

계는 분야별・보호대상별로 별개의 법령이 적용되고 있다. 현재 공공부문과 민간부문을 막론하고 주요정보통신기반시설에 대하여는 「정보통신기반보호법」이 적용되며, 그 외에는 공공부문은 「국가사이버안전관리규정」이 적용되고, 민간부문은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」이 적용된다. 이와 같이 내용이 상이한 법률이 적용됨에 따라 각 부문마다 사이버 위기관리체계가 별도로 이루어진다. 각 부문의 세부 내용을 살펴보면 다음과 같다.

3.1 공공부문의 주요정보통신기반시설

정보통신기반보호위원회는 주요 정보통신기반시설의 보호에 관한 사항을 심의한다. 위원장은 국무총리실장이며, 위원은 대통령령이 정하는 중앙행정기관의 차관급 공무원 및 위원장이 위촉하는 자로 한다.

중앙행정기관은 전자적 침해행위로부터의 보호가 필요하다고 인정되는 정보통신기반시설을 주요정보통신기반시설로 지정하여 정보통신기반보호위원회의 심의를 거쳐 고시한다. 주요정보통신기반시설은 현재 공공부문과 민간부문에 걸쳐 다양하게 지정되어 있다. 행정안전부, 국가정보원 등은 필요하다고 판단되는 시설에 대하여 중앙행정기관에 주요정보통신기반시설의 지정을 권고할 수 있다.

주요정보통신기반시설을 관리하는 역할을 하는 관리기관은 취약점 분석・평가를 실시한다. 관리기관은 한국전자통신연구원, 한국정보보호진흥원, 정보공유・분석센터, 정보보호컨설팅전문업체에 취약점 분석・평가를 위탁할 수 있다. 관리기관은 주요정보통신기반시설 보호대책을 수립・시행하고, 중앙행정기관은 주요 정보통신기반시설 보호대책을 취합하여 주요 정보통신기반시설 보호계획을 수립・시행한다.

행정안전부와 국가정보원은 보호대책의 이행여부를 확인한다. 그리고 국가정보원, 행정안전부, 국군기무사령부, 한국전자통신연구원 부설연구소, 한국정보보호진흥원, 정보보호컨설팅전문업체가 보호활동을 지원한다.

주요 정보통신기반시설에 대하여 관계중앙행정기관장은 소관분야 주요 정보통신기반시설 보호지침을 제정하고 주요 정보통신기반시설 관리기관의 장에게 그 준수를 권고할 수 있으며, 보호에 필요한 조치를 명령 또는 권고할 수 있다. 주요 정보통신기반시설에 대한 침해행위는 누구에게나 금지된다.

이 외에도 주요 정보통신기반시설 침해에 대한 대응조치 및 관련 민간부문과의 협력 등이 규정되어 있다. 침해사고에 대비하여 중앙행정기관은 소관분야 보호지침을 제정하고, 관리기관에 보호조치를 명령・권고할 수 있다. 관리기관은 침해사고 발생시 관계 행정기관, 수사기관 또는 한국정보보호진흥원에 그 사실을 통지하고, 신속한 대응・복구조치를 시행하여야 한다. 관계중앙행정기관의 장 또는 한국정보보호진흥원의 장은 관리기관에 필요한 지원을 제공한다.

정보통신기반보호위원회는 정보통신기반침해사고대책본부를 설치・운영하며, 정보공유・분석센터는 취약점・침해요인 관련정보를 제공하고 실시간 경보・분석체계를 운영한다[15].

3.2 공공부문의 주요 정보통신기반시설 외

사이버안전 관련 정책의 총괄・조정은 국가정보원장이 담당한다. 그리고 국가정보원장 소속하에 국가 사이버 안전전략회의, 국가 사이버 안전대책회의, 국가 사이버 안전센터를 설치・운영한다.

국가 사이버 안전전략회의는 국가 사이버 안전체계의 수립 및 개선에 관한 사항, 국가 사이버 안전 관련 정책 및 기관간 역할조정에 관한 사항, 국가 사이버 안전 관련 대통령 지시사항에 대한 조치방안 등 공공부문의 국가 사이버 안전에 관한 중요사항을 심의한다.

국가 사이버 안전전략회의의 의장은 국가 정보원장이며, 위원은 관계 중앙행정기관의 차관급 공

무원으로 한다.

그리고 국가 사이버 안전전략회의의 효율적 운영을 위하여 국가 사이버 안전대책회의를 둔다. 국가 사이버 안전대책회의의 의장은 국가정보원의 사이버 안전업무를 담당하는 차장이며, 위원은 국가 사이버 안전전략회의의 위원이 속하는 기관의 실·국장급 공무원으로 한다.

국가 사이버 안전센터는 국가 사이버 안전정책의 수립, 전략회의 및 대책회의의 운영에 대한 지원, 사이버 위협 관련 정보의 수집·분석·전파, 국가정보통신망의 안전성 확인, 국가 사이버 안전매뉴얼의 작성·배포, 사이버 공격으로 인하여 발생한 사고의 조사 및 복구 지원, 외국과의 사이버위협 관련 정보의 협력 등 국가 사이버 안전 관련 업무를 수행한다.

중앙행정기관의 장은 소관분야의 사이버 안전대책을 수립·시행하고, 지도·감독한다. 중앙행정기관의 장, 지방자치단체의 장 및 공공기관의 장은 국가정보원에 사이버 공격 관련 정보를 통보한다. 국가정보원장은 제공받은 정보 관련 대응 조치를 강구한 후 그 결과를 해당 기관에 통지한다.

국가정보원장은 사이버 공격을 탐지한 경우 사이버공격경보를 발령한다. 이를 통보받은 관계 중앙행정기관의 장은 소관기관에 경보를 전파한다. 사이버공격 발생 시 중앙행정기관의 장은 대응조치를 취하고 국가정보원장에 공격사실을 통보하고, 지방자치단체의 장 및 공공기관의 장은 대응조치를 취하고 관계 중앙행정기관의 장에게 공격사실을 통보하며, 관계 중앙행정기관의 장은 이를 다시 국가정보원장에게 통보한다.

국가 정보원장은 사고조사 및 지원활동을 수행한다. 또한 국가정보원장은 사이버 안전관련 연구개발에 필요한 시책을 추진하며, 한국전자통신연구원 부설연구소에 연구개발 수행을 위임할 수 있다.

국방부문은 별도의 체계에 따른다. 안전성 확인, 경보발령, 사고통보, 사고조사 등을 국방부가 담당하여 수행한다[16].

3.3 민간부문의 주요 정보통신기반시설

앞에서 논한 공공부문 중 주요정보통신기반시설의 경우와 동일한 체계이다. 공공부문과 마찬가지로「정보통신기반보호법」이 적용되기 때문이다[15].

3.4 민간부문의 주요 정보통신기반시설 외

정보통신 서비스 제공자는 정보통신망의 안정성 및 정보의 신뢰성을 확보하는 조치를 실시하여야 한다. 방송통신위원회는 구체적인 정보보호지침을 고시한다.

사이버 위기관리와 특히 관련성이 큰 부분은 집적정보통신시설 등 대규모의 정보통신시설의 보호에 관한 것이다. 타인의 정보통신 서비스 제공을 위하여 집적된 정보통신시설을 운영·관리하는 사업자는 정보통신시설을 안정적으로 운영하기 위한 보호조치를 하여야 하며, 집적정보통신시설의 멸실, 훼손, 그 밖의 운영장애로 발생한 피해를 보상하기 위한 보험에 가입하여야 한다. 방송통신위원회가 지정한 안전진단 수행기관은 대규모 정보통신망 및 집적정보통신시설에 대하여 안전진단을 실시한다.

정보통신 서비스 제공자 및 집적정보통신시설사업자는 침해사고가 발생 시에는 즉시 그 사실을 방송통신위원회 또는 한국정보보호진흥원에 신고하여야 한다. 방송통신위원회 및 한국정보보호진흥원은 인터넷침해사고대응지원센터를 운영하여 침해사고정보 수집·전파, 경보, 긴급조치 등을 수행하며, 정보통신 서비스 제공자의 정보통신망에 중대한 침해사고가 발생한 때에는 민·관합동조사단을 구성하여 당해 침해사고의 원인분석을 할 수 있다[17].

4. 미국과 한국의 사이버 위기관리체계 비교

미국의 경우, '전자정부법'의 일부인 '연방정보보

안관리법'에 따라 각 연방기관은 예산 제정 절차의 일환으로서 미국 백악관 관리예산처에 정보보호 대책의 상황을 보고하도록 하여 정보보호 정책과 예산을 연계시킨 형태로 분석될 수 있다. 미국 백악관 관리예산처는 '연방정보보안관리법'에 근거하여 전자정부에서 각 연방기관의 정보보호조치를 감독하고 이를 예산집행 등에 반영함으로써 공공부문 정보보안 일반에 대한 실질적인 평가 역할을 수행하지만 직접 정보보호조치를 집행하지는 않는다.

한편 국토안보부는 '국토안보법'에 근거하여 공공과 민간부문 전체에 걸쳐, 그리고 물리적 위협이든 사이버공격이든 그 형태를 막론하고 보호조치를 총괄적으로 집행한다. 국토안보부는 연방정부의 정보보호 정책을 실시할 책임을 지고 있으며, 이것에 대한 실례로, 2002년에 발표된 "국토안보 국가전략"에서 국토안보부의 주요기반시설 보호를 총괄하는 역할을 명시, 2003년에 제시된 "사이버공간 보호를 위한 국가전략"에서는 연방정부의 각 기관이 완수해야 할 정보보호의 포괄적인 틀을 제시, 2004년부터 "국가 사고 관리 시스템"을 통한 사고대응 단일 체계 수립 및 표준화된 관리 계획 제시 등을 언급할 수 있다.

또한 국토안보부는 "국가 대응 프레임워크", "국가 기반 보호 계획", "국가 사이버 공간 대응 시스템", "사이버 위험 관리 프로그램" 등의 전략과 프로그램의 진행으로 사이버 공격을 예방하고 대응하기 위한 실질적인 조치들을 수행하고 있으며 최근의 경우 "국가 사이버보안 종합전략"에 의해 美정부 전산망을 적극적으로 감시하는 임무를 맡아 사이버침해 사고에 대한 사후 대응측면보다는 사전 대응체계를 수립하는데 큰 역할을 맡고 있다.

한국의 경우 공공분야와 민간분야에 따라 적용법령이 다르고 추가적으로 주요 정보통신 기반시설 여부에 따라 적용 법령이 또 달라지는 형태이다. 더구나 공공부문 중 주요 정보통신기반시설이 아닌 경우는 법률이 아닌 대통령령을 적용하기 때문에 분야간 불균형 문제 또한 존재하는 형태를 보인다. 따라서 미국과는 달리 사이버 위기관리 체계가 통합적이면서 단일화된 구성을 이루지 못하고 있다. 주요 정보통신기반 보호는 행정안전부가 주관하여 담당하고, 그 외의 부분은 공공부문은 국가 정보원이, 민간부문은 방송통신위원회가 각각 주관한다.

그러나 오늘날 정보통신망의 연동으로 인하여 그러한 분야별 구분은 무의미하다. 개인용 PC를 감염시킨 컴퓨터 바이러스가 정보통신망을 타고 주요 정보통신기반에 피해를 줄 수도 있는 것이고, 민간 정보통신시설에 대한 사이버 공격이 공공 정보통신시설로 확산될 수도 있는 것이다. 따라서 현재와 같은 체계는 적용할 법을 결정하고 그에 따른 주관부서를 정함에 있어 혼란을 야기할 수 있고, 사이버위기관리를 국가차원에서 총체적으로 지휘할 수 있는 기관이 불분명하여 전문적이면서 일관성 있는 대응이 어렵다.

따라서 미국 국토안보부와 같이 공공과 민간부문 전체에 걸쳐, 그리고 물리적 위협이든 사이버 공격이든 그 형태를 막론하고 보호조치를 총괄적으로 집행하는 기구가 필요하다. 이를 위하여 관계 법령의 정비가 시급한 실정이라고 할 수 있다.

5. 결 론

미국의 사이버 위기관리 체계의 사례는 우리에게 많은 점을 시사해준다. 국토안보법에 근거하여 국토안보부가 미국의 사이버 위기관리를 위한 컨트롤 타워의 역할을 하듯이 사이버 위기관리 체계는 여러 갈래로 나누어져서는 안되며, 통합적으로 이루어지는 것이 예방의 효율성과 대응의 적시성 등에 있어 바람직하다. 한국의 사이버 위기관리 체계의 경우 사이버 위기관리에 대해 명확히 규정하는 법률 부재와 각 부처간 역할과 책임소재가 불분명하며 2개 이상의 기관 및 부문이 연루되어 사이버 위기 발생 시 효과적인 대응에 어려움이 존재한다. 그렇다면 한국의 사이버 위기관리 체계 역시 단일

화된 법률, 제도 및 정책을 중심으로 통합적으로 재구성하여야 한다. 즉, 사이버 위기관리를 조직적이며 전문적으로 대응할 수 있도록 국가차원에서 법규로 설립근거를 갖는 하나의 기관이 컨트롤 타워가 되어 일원화된 위기관리 체계의 구축이 가능하도록 해야 한다.

참 고 문 헌

[1] www.dhs.gov/xlibrary/assets/NIMS-90-web.pdf.

[2] www.whitehouse.gov.

[3] Federal Information Security Management Act of 2002.

[4] Responses of Chairman Lieberman's and Senator Collin's Questions Regarding the National Cyber Secuirty Center, July 18, 2008.

[5] www.fas.org.

[6] Homeland Security Act of 2002.

[7] Cyber Security Research and Development Act.

[8] 김대호, 오일석, "미국 전자정부 정보보안 법제동향", 한국정보보호학회지, 2003년 6월, pp. 23-30.

[9] OMB circular A-130.

[10] http://www.cdi.org/program/document.cfm?DocumentID=4345 and from_page=../index.cfm, "The Murky Waters of the White House's Cybersecurity Plan", July 23, 2008.

[11] Letter by Senators Joe Lieberman, I-Conn., and Ranking Member Susan Collins, R-Maine, to Secretary of Homeland Security Michael Chertoff, May 1, 2008.

[12] http://www.nist.gov/public_affairs/factsheet/cyber2009.html, "Comprehensive National Cyber Security Initiative : Leap-Ahead Security Technologies", Feb 1, 2008.

[13] http://www.washingtonpost.com/wp-dyn/content/article/2008/07/20/AR2008072001641.html, "Cybersecurity Will Take A Big Bite of the Budget", July 21, 2008.

[14] http://news.cnet.com/8301-13578_3-10004266-38.html, "DHS stays mum on new 'Cyber Security' center", July 31, 2008.

[15] 정보통신기반보호법.

[16] 국가 사이버 안전관리규정.

[17] 정보통신망 이용촉진 및 정보보호 등에 관한 법률.

김 민 식

2000년 한양대학교 전기공학과(학사)
2003년 한양대학교 전자통신전파공학과(석사)
2007년~현재 고려대학교 정보경영공학전문대학원 (박사과정)
2003년~현재 ETRI 부설연구소 근무

박 상 돈

2002년 성균관대학교 법학과(학사)
2004년 성균관대학교 법학과(석사)
2008년~현재 성균관대학교 법학과(박사과정)
2008년~현재 ETRI 부설연구소 근무

권 헌 영

2005년 연세대학교 법학과(박사)
2008년~현재 광운대학교 법학대학 과학기술법학과 조교수

김 일 환

1988년 성균관대학교 법학과 (학사)
1990년 성균관대학교 법학과 (석사)
1995년 독일 만하임(Mannheim) 대학교 법과대학(박사)
현재 성균관대학교 법학전문대학원 부교수

임 종 인

1980년 고려대학교 수학과
1982년 고려대학교 수학과 (석사)
1986년 고려대학교 수학과 (박사)
2000년 고려대학교 자연과학대학 정교수

현재 고려대학교 정보경영공학전문대학원
고려대학교 정보보호기술연구센터 센터장