Journal of The Korea Society of Computer and Information
Vol. 19, No. 3, March 2014
www.ksci.re.kr
http://dx.doi.org/10.9708/jksci.2014.19.3.163

국가 사이버안전 관리 법제의 개정방향에 관한 소고

오 태 곤*, 성 관 실*

Consideration on the Revision Direction of National Cyber Security Management Legislation

Tae-Kon Oh*, Gwan-Sil Seoung*

요 약

사이버공간은 시공간을 초월하여 범세계적으로 상호 밀접한 관계를 맺고 있으며, 이미 우리 생활의 가장 중요한 영역 중 하나로 자리 잡았다. 그러나 과거 1·25 인터넷 대란과 같은 전국적 규모의 국가 주요 정보통신망 마비사태 등에서처럼 국내 또는 해외로부터의 조직적인 사이버테러가 발생한다면 국가기밀 및 첨단기술의 유출 등 우리 사회 전반에 중대한 해악을 미칠 수 있는 사이버위기의 발생 가능성이 날로 증대하고 있다. 그러나 우리는 아직까지 국가적 차원에서 사이버안전 관리 업무를 체계적으로 수행할 수 있는 법제도적인 절차가 정립되어 있지 않아, 사이버위기 발생 시에 국가적 또는 개인적 측면에 막대한 손해를 끼칠 가능성이 높다. 이에 이 연구에서는 우리의 사이버안전 관련 입법례를 살펴보고, 주요국의 관련 법제에 대한 비교법적 검토를 통해 우리의 사이버안전 관리 규정의 개정방향에 관한 시사점을 제시하고자 한다.

▸ Keywords : 사이버공간, 1·25 인터넷 대란, 정보통신망, 사이버테러, 사이버안전

Abstract

Cyberspace is closely related with one another, transcending the spacetime throughout the world, and is already located in the most important area of our lives. However, if the organizational cyber terror happens like the national paralysis crisis of major information network such as the previous 1.25 the Internet crisis, the possibility of cyber crisis highly damaging our whole society such as the leakage of the national secrecy and advanced technology is increasing. But we haven't set up the institutional procedure systematically performing the national cyber security management affairs yet. So, in case of cyber crisis, this is highly likely to damage the aspects of national and personal level. On this point, this study

•제1저자 : 오태곤, 교신저자 : 성관실
•투고일 : 2013. 11. 28, 심사일 : 2013. 12. 11, 게재확정일 : 2013. 12. 19.
* 조선대학교 법과대학(College of Law, Chosun University)

looks into the examples of legislation related to our cyber security, and suggests the implication on the revision direction of national cyber security management regulations through relative examination about the examples of legislation in major countries.

▸ Keywords : Cyberspace, 1.25 the Internet Crisis, Information Network, Cyber Terror, Cyber Security

I. 서 론

오늘날 진화되는 IT관련 기술은 관련 하드웨어와 소프트웨어의 비약적인 발전 및 월드와이드웹 시스템을 통해 범세계적으로 상호 밀접한 관계를 형성하였으며, 우리에게 보다 편리하고 행복한 삶을 가능하게 해주고 있다. 그러나 이와 같은 순기능만큼이나 우리에게 끼치는 악기능도 많은 실정이 되었다. 이와 관련하여 최근 10여년 간의 대표적인 피해사례만을 살펴 보더라도, 먼저 2003년 1월 25일 해외로부터 유입된 슬래머웜(Slammer Worm)에 의한 DNS 서버 과부화로 인한 국가적 사이버대란이 일어났으며, 2005년과 2006년에는 리니지 누리집에서 약 26만개의 불법 명의도용 사고가 발생하여 개인사용자들에게 경제적 손실을 입혔으며, 2008년에는 대표적인 인터넷 전자상거래사이트인 옥션의 누리집이 해킹 당해 약 1천1백만명의 개인정보가 유출 되었으며, 2009년 7월 7일에는 DDoS 대란이 발생하여 국내 대부분의 포털사이트, 공공기관, 은행 등의 업무가 마비되었으며, 2011년 7월에는 SK 컴즈의 네이트DB가 해킹되어 약 3천5백만명의 개인정보가 유출된 사고가 있었으며, 2013년에는 3월 20일과 6월 25일에는 주요 방송 및 언론사, 농협, 신한금융 및 청와대, 주요 정부기관에 대한 사이버 공격이 발생하였다.

이와 관련하여 2008년 한국정보보호진흥원(KISA)은 2003년 1·25 인터넷 대란의 원인을 "실시간 모니터링 체계미비, 사고발생 시 관련기관 간 긴급 연락체계 미흡, KISA와 ISP 간 공조체계 미흡, 네트워크·서버·인터넷 이용자 PC 등 계층별 보호체계 미흡, 침해사고 대응 관련 조직 및 법·제도 미비 등"을 대응 상의 한계로 지목하며, 이에 대한 대응체계를 체계적으로 구축해, 2003년 이후 5년간 약 5조3000억원의 손실 예방과 전세계 피해액 대비 국내 피해액 비율을 종전 10%수준에서 현재 3%수준으로 감소시켰다고 발표한 바 있다.[1] 하지만 중요한 것은 과거의 피해사례들은 현재까지도 진행 중이라는 사실이며, 2차적·3차적, 추정 불가능한 손해들이 현재까지도 계속되고 있다는 사실이다.

이러한 사이버안전 위협 행위들로 인한 피해들을 최소화 또는 예방하기 위해서는 민·관, 우리 국가를 떠나 전지구적인 대책이 필요함은 부인할 수 없는 사실이며, 무엇보다도 법·제도적인 대책 수립이 선결되어야 할 것이다.

그러나 우리는 아직까지 국가적 차원에서 사이버안전 관리 업무를 체계적으로 수행할 수 있는 법제도적인 절차가 정립되어 있지 않아, 사이버위기 발생 시에 국가적 또는 개인적 측면에 막대한 손해를 끼칠 가능성이 여타국에 비해 높다.

이에 이 연구에서는 우리의 사이버안전 관련 입법례를 살펴보고, 주요국의 관련 법제에 대한 비교법적 검토를 통해 우리의 사이버안전 관리 규정의 개정방향에 관한 시사점을 제시하고자 한다.

II. 이론적 배경

1. 사이버안전

사이버 공간은 어떠한 정보도 국경을 손쉽게 넘을 수 있으며, 개인정보를 비롯하여 민간기업의 영업비밀이나 산업 비밀에서부터 군사 및 국가기밀에 이르기까지 자유롭게 이동하고 있으며, 그 결과 세계 각국의 국가안전을 위한 방어시스템은 사이버기술을 토대로 하여 네트워크 시스템 내로 전략적, 전술적으로 접목하고자 시도되고 있다.[2]

이와 병행하여 정보를 지배하는 자가 국제관계 내지 적대적 관계에 있는 세력을 제압할 수 있는 도구라는 인식이 보편화되면서, 사이버공간에 대한 테러 내지 사이버위협이 국내외적으로 자행되고 있다.[3] 이와 같은 사이버 위협 내지 사이버테러는 정보를 지배하려는 개인이나 단체 또는 적대국가나

세력에 의하여 자신의 정치, 종교적 또는 군사적 목적을 달성하기 위해 특정 대상을 상대로 하거나 무차별적으로 정보의 유통을 마비, 왜곡시키거나 또는 정보를 탈취하여 개인이나 사회 및 국가의 혼란을 야기하는데,[4] 사이버안전은 이상과 같은 사이버위협 내지 사이버테러에 대한 반작용을 의미한다고 할 수 있다.

우리「국가사이버안전관리규정」은 제2조 3호에 "사이버안전"을 '사이버공격으로부터 국가정보통신망을 보호함으로써 국가정보통신망과 정보의 기밀성·무결성·가용성 등 안전성을 유지하는 상태를 말한다.'고 규정하고 있으며, 동조 2호에서는 "사이버공격"은 '해킹·컴퓨터바이러스·논리폭탄·메일폭탄·서비스방해 등 전자적 수단에 의하여 국가정보통신망을 불법침입·교란·마비·파괴하거나 정보를 절취·훼손하는 일체의 공격행위를 말한다.'고, 동조 4호에서는 "사이버위기"는 '사이버공격으로 정보통신망을 통해 유통·저장되는 정보를 유출·변경·파괴함으로써 국가안보에 영향을 미치거나 사회·경제적 혼란을 발생시키거나 국가 정보통신시스템의 핵심기능이 훼손·정지되는 등 무력화되는 상황을 말한다.'고 규정하고 있다.

2. 사이버안전 침해 유형

사이버안전 침해의 유형과 관련하여 국내에서는 주로 사이버침해의 수단 또는 수법과 피해를 중심으로 분류하고 있는데, 이는 학술적인 분류는 아니며 주로 실무적인 관점에서 유형 분류가 이루어지고 있다.[5]

먼저 경찰청 사이버테러대응센터는 정보통신망 자체를 공격대상으로 하는 불법행위로서 해킹, 바이러스유포, 메일폭탄, DoS공격 등 전자기적 침해장비를 이용하여 컴퓨터시스템과 정보통신망을 공격하는 행위를 사이버테러형 범죄로 분류하고, 이를해킹(단순침입, 사용자 도용, 파일등 삭제와 자료유출, 폭탄메일)과 악성프로그램으로 구분한다.[6]

표 1. 경찰청 사이버테러대응센터의 분류
Table 1. National Police Agency, the classification of Cyber Terror Response Center

유형	침해행위	내용
해킹	단순침입	정당한 ① 접근권한 없이 또는 허용된 접근권한을 초과하여 ② 정보통신망에 침입 하는 것
	사용자도용	정보통신망에 침입하기 위해서 타인에게 부여된 사용자계정과 비밀번호를 권한자의 동의 없이 사용하는 것
해킹	파일등 삭제와 자료유출	정보통신망에 침입한 자가 행한 2차적 행위의 결과로, 일반적으로 정보통신망에 대한 침입행위가 이루어진 뒤에 가능함
	폭탄메일	메일서버가 감당할 수 있는 한계를 넘는 많은 양의 메일을 일시에 보내 장애가 발생하게 하거나 메일내부에 메일 수신자의 컴퓨터에 과부하를 일으킬 수 있는 실행코드 등을 넣어 보내는 것
	서비스거부공격	정보통신망에 일정한 시간 동안 대량의 데이터를 전송시키거나 처리하게 하여과부하를 야기시켜 정상적인 서비스가 불가능한 상태를 만드는 일체의 행위
악성프로그램	트로이목마	프로그램에 미리 입력된 기능을 능동적으로 수행하여 시스템 외부의 해커에게 정보를 유출하거나 원격제어기능 수행. 트로이목마처럼 유용한 유틸리티로 위장하여 확산되기 때문에 감염사실 알아채기 어려움
	인터넷웜	시스템 과부하를 목적으로 이메일의 첨부파일 등 인터넷 이용하여 확산됨. 확산시 정상적인 파일이 이메일에 첨부되기도 하기 때문에 개인정보 유출의 위험 내포
	스파이웨어	공개프로그램, 쉐어웨어, 평가판 등의 무료 프로그램에 탑재되어 정보를 유출시키는 기능이 있는 모든 종류의 프로그램

다음으로 국가정보원 사이버안전센터는 사이버공격을 수법에 따라 ① 악성코드공격, ② 서비스거부공격, ③ 비인가접근공격, ④ 복합구성공격의 4가지로 분류한다.[7]

표 2. 국가정보원 사이버안전센터의 분류
Table 2. National Intelligence Service, the classification of Cyber Security Center

유형	침해행위	내용
사이버침해	악성코드공격	컴퓨터바이러스, 웜, 트로이목마, 백도어, 봇(BOT), 스파이웨어 등 악성코드가 사용자의 동의없이 컴퓨터에 설치되어 사용자의 정보를 탈취하거나 컴퓨터를 오작동시키고 네트워크를 마비시키는 행위를 말한다.
	서비스거부공격	시스템에 과도한 부하(負荷)를 유발하여 정상적인 서비스를 차단하거나 성능을 저하시키는 행위를

		말한다.
	비인가접근공격	네트워크, 시스템, 응용프로그램, 데이터 기타 정보자원 등에 인가받지 않은 자가 논리적 혹은 물리적으로 불법 접근하는 행위를 말한다.
	복합구성공격	위의 악성코드공격, 서비스거부공격, 비인가접근공격 등의 요소를 복합적으로 이용하는 공격행위를 말한다.
안보위해공격	국가기밀에 속하는 문서·자재·시설·지역 등을 대상으로 한 공격	국가정보원법 제3조 및 보안업무규정에 따른 국가기밀에 속하는 문서·자재·시설·지역 및 이를 관리하는 인원을 대상으로 한 사이버공격
	반국가단체, 국제범죄조직 및 테러단체에 의한 공격	국가보안법 제2조에 따른 반국가단체, 국가정보원법 제3조에 따른 국제범죄 조직 및 테러단체에 의하여 수행되는 사이버공격
	국가안전보장 관련 주요정보통신기반시설을 대상으로 한 공격	'정보통신기반 보호법' 제7조 제2항에 따른 국가안전보장 관련 주요정보통신 기반시설 및 이를 관리하는 인원을 대상으로 한 사이버공격
	국가핵심기술을 대상으로 한 공격	'산업기술의 유출방지 및 보호에 관한 법률' 제9조에 따른 국가핵심기술 및 이를 취급하는 인원을 대상으로 한 사이버공격

또한, 정보통신부 산하 인터넷침해대응센터는 침해사고를 ① 웜·바이러스, ② 해킹, ③ 악성 봇(Bot)으로 분류하고, 해킹을 다시 스팸 릴레이, 피싱 경유지, 단순침입시도, 홈페이지 변조, 기타 해킹으로 나눈다.[8]

표 3. 정보통신부 인터넷침해대응센터의 분류
Table 3. Ministry of Information and Communication, the classification of Computer Emergency Response Center

유형	침해행위	내용
웜 바이러스	웜	독립적으로 자기복제를 실행하여 번식하는 빠른 전파력을 가진 컴퓨터 프로그램 또는 실행 가능한 코드
	바이러스	컴퓨터 프로그램이나 메모리에 자신 또는 자신의 변형을 복사해 넣는 악의적인 명령어들로 조합하여 불특정 다수에게 피해를 주기 위한 목적으로 제작된 모든 컴퓨터 프로그램 또는 실행 가능한 코드
해킹	스팸릴레이	스팸 메일 발신자 추적을 어렵게 하기 위하여 타 시스템을 스팸 메일발송에 악용
	피싱경유지	정상적인 웹서버를 해킹하여 위장 사이트를 개설한 후, 인터넷 이용자들의 금융 정보 등을 빼내는 신종 사기수법으로 Bank Fraud, Scam이라고도 함
	단순침입시도	시스템에 침입하려고 시도하거나, 취약점 정보의 수집을 위해 스캔하는 등의 행위
	홈페이지변조	—
	기타 해킹	—
악성 봇	봇(Bot)	운영체제 취약점, 비밀번호의 취약성, 웜·바이러스의 백도어 등을 이용하여 전파되며, 해킹명령 전달 사이트와의 백도어 연결 등을 통하여 스팸메일 전송이나 DDoS 공격에 악용이 가능한 프로그램 또는 실행 가능한 코드

III. 사이버안전 관련 법령

1. 정보통신기반보호법

정보통신기반보호법은 전자적 침해행위에 대비하여 주요정보통신 기반시설의 보호에 관한 대책을 수립·시행함으로써 동 시설을 안정적으로 운용하도록 하여 국가의 안전과 국민생활의 안정을 보장하는 것을 목적으로 하는 법으로서(제1조), 중앙행정기관의 장으로 하여금 소관분야의 정보통신기반시설 중 당해 정보통신기반시설을 관리하는 기관이 수행하는 업무의 국가 사회적 중요성 등을 고려하여 전자적 침해행위로부터의 보호가 필요하다고 인정되는 정보통신기반시설을 주요정보통신기반시설로 지정하도록 하고(제8조), 지정된 주요정보통신기반시설의 보호에 관한 사항을 심의하기 위하여 국무총리 소속하에 정보통신기반보호위원회를 두고 있다(제3조). 이때 중앙행정기관은 전자적 침해행위로부터의 보호가 필요하다고 인정되는 정보통신기반시설을 주요정보통신기반시설로 지정하여 정보통신기반보호위원회의 심의를 거쳐 고시한다. 주요정보통신기반시설에 대한 침해행위는 누구에게나 금지되며, 현재 공공부문과 민간부문에 걸쳐 다양하게 지정되어 있는데, 이에 대하여 관계중앙행정기관장은 보호지침을 제정하고 주요정보통신기반시설 관리기관의 장에게 그 준

수를 권고할 수 있으며, 보호에 필요한 조치를 명령 또는 권고할 수 있다. 이 법에서는 주요 정보통신기반시설 침해에 대한 대응조치 및 관련 민간부문과의 협력 등도 규정되어 있다.

2. 전자정부법

전자정부법은 행정업무의 전자적 처리를 위한 기본원칙·절차 및 추진방법 등을 규정함으로써 전자정부의 구현을 위한 사업을 촉진시키고, 행정기관의 생산성·투명성 및 민주성을 높여 지식정보화 시대의 국민의 삶의 질을 향상시키는 것을 목적으로 하는 법으로(제1조), 국회·법원·헌법재판소·중앙선거관리위원회 및 행정부에 대해 "전자정부의 구현에 요구되는 정보통신망과 행정정보 등의 안전성 및 신뢰성 확보를 위한 보안대책을 마련할 의무"를 부여하고 있다(제56조). 또한 전자정부 구현을 위한 시책 등의 추진을 위해 행정기관등의 장에게 전자정부의 구현·운영 및 발전을 위한 사업의 추진 의무를 부여하며, 안전행정부장관에게 행정적·재정적·기술적 지원 등 필요한 지원을 할 수 있도록 규정하고 있으며(제64조), 국가 및 지방자치단체는 지역의 경쟁력 강화 및 지역주민의 삶의 질 향상을 위하여 "지역의 역사·문화·복지·환경 등의 지역정보서비스 개발과 보급, 정보시스템 구축 및 지역의 정보화기반 조성, 정보화 낙후지역의 집중 지원 등"의 지역정보화사업을 추진할 수 있다고 규정하고 있다(제65조).

3. 정보통신망 이용촉진 및 정보보호 등에 관한 법률

정보통신망 이용촉진 및 정보보호 등에 관한 법률은 정보통신망의 이용을 촉진하고 정보통신서비스를 이용하는 자의 개인정보를 보호함과 아울러 정보통신망을 건전하고 안전하게 이용할 수 있는 환경을 조성하여 국민생활의 향상과 공공복리의 증진에 이바지함을 목적으로 하는 법으로(제1조), 정부는 정보통신망의 이용촉진 및 안정적 관리·운영과 이용자의 개인정보보호 등을 통하여 정보사회의 기반을 조성하기 위한 시책을 마련하여야 하고(제4조), 이를 위해 미래창조과학부장관과 방송통신위원회가 전기통신사업자, 정보통신서비스 제공자, 나아가 정보통신망을 이용하는 모든 사람에게 일정한 조치의무를 부과하고 이행명령을 발하는 등 안전성 확보 업무 수행의 법적 근거를 두고 있다(제45조, 제47조 등).

4. 국가정보화기본법

국가정보화기본법은 국가정보화의 기본 방향과 관련 정책의 수립·추진에 필요한 사항을 규정함으로써 지속가능한 지식정보사회의 실현에 이바지하고 국민의 삶의 질을 높이는 것을 목적으로 하는 법으로(제1조), 정부에 암호기술의 개발과 이용을 촉진할 의무를 부여함과 아울러 정보보안과 관련하여 미래창조과학부장관에게 관계기관의 장과 협의하여 정보보호시스템의 성능과 신뢰도에 관한 기준을 정하여 이를 고시하고, 정보보호시스템을 제조하거나 수입하는 자에 대하여 이 기준의 준수를 권고할 권한을 부여하고 있다(제37조, 제38조).

5. 국가사이버안전관리규정

대통령 훈령인 국가사이버안전관리규정은 국가사이버안전에 관한 조직체계 및 운영에 대한 사항을 규정하고 사이버안전업무를 수행하는 기관간의 협력을 강화함으로써 국가안보를 위협하는 사이버공격으로부터 국가정보통신망을 보호함을 목적으로 하는 법으로(제1조), 이 규정은 중앙행정기관, 지방자치단체 및 공공기관의 정보통신망(정보통신기반보호법 제8조의 규정에 의하여 지정된 주요정보통신기반시설에 대하여는 적용 제외)을 대상으로 하는 대통령 훈령으로, 사이버공격에 대한 국가차원의 종합적이고 체계적인 대응을 위하여 국가정보원장 소속으로 국가사이버안전센터를 두고(제8조), 국가사이버안전에 관한 중요사항을 심의하기 위하여 국정원장 소속하에 국가사이버안전전략회의를 두며(제6조), 중앙행정기관의 장 등은 보안관제센터를 구축·운영(제10조의2)하도록 하는 등이 있다. 하지만 이 법령은 그 형식상 국가 및 공공기관에만 적용되는 대통령훈령으로서 사이버안전의 위협 행위에 대해 종합적이고 체계적인 대응의 근거 법령으로서는 다소 미흡하며, 민간 기업이나 이용자 등에게 의무를 부과하거나 그에 따라 벌칙을 두는 것은 불가능하다는 한계가 있다.

Ⅳ. 주요국의 사이버안전 관리 법제

1. 미 국

미국의 사이버안전 관련 최초법률은 1987년 제정된 '컴퓨터보안법'(Computer Security Act)이다. 이 법은 미국국립표준기술연구소(NIST)를 중심으로 정부에서 사용되는 컴퓨터보안에 기준 프로그램을 제공함과 동시에 연방정부 컴퓨터시스템을 운용하는 정부 관련자의 교육을 목적으로 한다.[9]

애국법(USA PATRIOT ACT of 2001)은 9·11테러 직후 계속되는 테러 위협에 대응하기 위한 수사력 강화와 국가안보 확립을 목적으로 한 법률로서 인터넷이나 휴대전화를 포함한 모든 전자통신에 대해 DCS1000에 의해 IP주소 등을 기록하며, 테러 혐의자에 대한 감청 허용요건과 영장주의를 완화하고 테러조직과 관련된 은행계좌나 자산의 동결 등을 규

정하였다. 또한, 테러범죄자들이 미국으로 입국하는 것을 막고 미국 내 테러용의자들의 추방을 쉽게 하기 위하여 구금 및 추방의 요건을 대폭 완화하는 한편, 테러행위에 대한 처벌도 과거 사이버테러시 초범은 5년 이하의 징역, 상습범에게는 10년 이하의 징역이 최고형이었지만, 이 법은 최고 형량을 초범 10년, 상습범 20년까지로 강화하였을 뿐만 아니라 국방이나 국가안보와 관련한 컴퓨터에 피해를 야기한 경우에는 손실을 증명할 수 없어도 처벌할 수 있도록 하였다.[10] 이후 애국법은 2006년에 '애국법의 개선 및 권한 재부여 법(USA PATRIOT Improvement and Reauthorization Act of 2005)'과 '애국법의 부가적 권한 재부여에 관한 수정안(USA PATRIOT Act Additional Reauthorizing Amendment Act of 2006)'으로 개정되었다.[11]

국토안보법(Homeland security Act of 2002)은 미국 내 테러대책을 총괄하는 국토안보부의 창설을 위해 2002년 11월 총17장으로 제정되었다.[12] 이 법은 특히 제2장의 정보분석 및 기반시설 보호(IAIP : Information Analysis and Infrastructure Protection)에 관한 규정과 제10장의 정보보안(Information Security)에 관한 규정을 통해 사이버안전 관리에 대해 규정하고 있다.

이 외에도 연방정보보안정책에 필요한 최소한의 통제장치들을 수립하고, 각 기관들이 정보보안에 대한 책임을 지도록 하면서 각 기관 정보보안프로그램과 관리통제시스템을 상호연계시키도록 규정하고 있는 관리예산처 지침, 사이버보안연구개발법, 2009 사이버보안법안 등이 있다.

2. 영 국

영국의 사이버안전 관련 법제로는 컴퓨터부정사용방지법(Computer Misuse Act 1990)을 들 수 있다. 이 법은 허가 받지 않고 컴퓨터자료에 접근하는 행위(제1조), 추가적인 범죄행위를 실행하거나 그 실행을 돕기 위한 목적으로 허가 받지 않고 접근하는 행위(제2조), 허가 받지 않고 컴퓨터의 자료를 변경하는 행위(제3조) 등을 처벌하고 있다. 즉, 모든 컴퓨터소프트웨어의 불법복제금지 등 비인가자에 의한 컴퓨터 접속을 금지하고 있는데, 여기에는 일반인의 취미활동이나 테스트를 위한 접속도 포함되어 이를 위반하는 경우 6개월의 구금, 혹은 5000파운드의 벌금형을 부과한다. 또한 사기 및 도용 등 범죄를 목적으로 한 비인가 된 접속을 금지하며, 범죄를 목적으로 한 행위에 해킹을 포함하고 있어 이를 위반한 경우 5년간 구금 혹은 벌금형을 부과한다. 뿐만 아니라 바이러스 등의 유포행위를 포함, 컴퓨터 소프트웨어나 데이터에 대한 불법 수정행위를 금지하며 이를 위반한 경우 5년간 구금 혹은 무한대의 벌금형이 부과될 수 있다. 이와 함께 사이버테러와 관련해서는 기존의 테러방지법과 테러법(Terrorism Act 2000)을 대신하여, 9·11 테러 발생 이후 보다 강력한 법적 대처를 위해 2001년 12월 14일 제정된 '대테러범죄 및 안전보장법'(Anti-terrorism, Crime and Security Act 2001)을 들 수 있다. 이 법은 총 14개 장으로 이루어져 있는데, 이 법 제11편에 통신 데이터(전화, 인터넷 및 우편내용 등) 보전을 위한 권한 관계를 규정하고 있다. 이 외에도 통신감청과 일반인 모니터를 위한 조사권한규제법(RIPA : Regulation of Investigatory Power Act of 2000)과 정보보안관리에 대한 표준(BS 7799) 등이 있다.[13]

3. 독 일

독일은 2004년 정보통신법(TKG)을 제정하여 정부기관이 기밀누설 방지, 데이터의 안전성 확보 및 네트워크 침해사고 방지를 위해 인터넷통신 사업자와 정보통신서비스 제공하는 모든 책임자에게 고객 정보에 대한 정부의 접근 요청시 이를 지원해 주도록 하고 있으며, 이러한 데이터는 정부의 감시기관이 직접 접근할 수 있도록 규정하고 있다. 특히 제7장(비밀, 정보보호 및 공공안전)에서 공공안전을 위해 사업자들이 긴급전화가 가능하도록 할 의무, 기술적 보호대책과 감시가 가능한 방법을 마련할 의무 및 정보제공 의무를 지게 하여 국가 본연의 기능을 수행할 수 있도록 사업자 등에 대한 자료요구 권한, 사업자들의 관련 시설지원 의무 등을 구체화하고 있다. 한편 '정보보안책임자'를 임명하여 '정보보안에 관한 계획'을 수립하여 정보보안계획의 내용과 유지는 연방통신망청의 통제를 받도록 제도화되어 있다. 이와 함께 사이버테러와 관련해서는 2001년 9·11 테러를 계기로 한층 강화된 테러대책을 수립하였는데, 그 주요 내용은 테러대책을 위한 재정확보, 법 개정을 통한 효율적인 테러기관의 권한 강화, 신원확인, 주요시설의 보안 강화 등이다. 이에 따라 국제테러대책법(Gesetz zur Bekämpfung des internationlen Terrorismus)이 제정되어 2002년 1월 1일부터 발효되었다. 그 주요내용은 외국 테러 단체에 대한 처벌의 확장이었다. 이 외에도 정보통신 안전영역에 있어서 가장 대표적인 기관인 연방정보기술안전청의 설립 근거법인 연방정보기술안전청설치법(BSIG) 등이 있다.[14]

4. 일 본

일본은 고도 정보통신 네트워크 사회 형성 기본법(高度情報通信ネットワーク社會の形成に關する基本方針を定めた法律), 일명 'IT기본법'을 통해 사이버안전 측면에서 최근 문제

가 되고 있는 정보통신 네트워크 안전성 확보를 위하여 국민이 안심하고 네트워크를 이용하기 위한 네트워크 안전성 및 신뢰성 확보 등에 관한 조치가 선행되어야 함을 규정하고 있다(제21조). '고도 정보통신네트워크 사회 추진전략 본부'로 하여금 정보통신 네트워크의 안전성 및 신뢰성 확보 시책에 대한 중점 계획을 작성토록 하는 등 우리의 국가정보화기본법과 유사한 지위를 지닌다. 이와 함께 전기통신사업법(電氣通信事業法)은 1984년 12월 법률 제86호로 제정되어 2006년 6월 법률 제50호로 개정되었는바, 이 법은 전기통신사업의 공공성에 비추어 적정하고 합리적인 운영을 꾀함과 동시에 그 공정한 경쟁을 촉진하고 전기통신서비스의 원활한 제공을 확보하여 이용자의 이익을 보호하는 한편, 전기통신의 건전한 발달 및 국민편의를 도모하여 공공복리를 증진하는 것을 목적으로 하고 있다.〔15〕 일본의 사이버안전 관련 법제에서 특이한 점은 일본의 발달된 IT기술 수준에 비해 대응 법체계는 미약하다는 것이다.

V. 결 론

이상으로 국가 사이버안전 대응과 관련된 기본 이론과 우리나라의 법제도 및 주요국의 관련법에 대해 살펴봤다. 현재 국가 사이버안전 관리와 관련하여 국회에 2개의 법률안이 계류 중이다. 2013년 3월 26일 하태경 의원이 대표 발의한 "국가 사이버안전 관리에 관한 법률안"과 2013년 4월 9일 서상기 의원이 대표 발의한 "국가 사이버테러 방지에 관한 법률안"이 바로 그것이다. 양 법률안은 서상기 의원안이 공공부문과 주요민간부문을 포함한 '사이버테러 방지 및 위기관리 책임기관'에게 각종 책임과 의무를 부여하고 이에 따른 벌칙 규정을 둔 반면 하태경 의원안은 이러한 책임과 의무를 주로 중앙행정기관, 지방자치단체 및 공공기관에 부여하고 있다는 차이점이 있지만, 양 법률안 모두 사이버공격 또는 테러에 대한 국가차원의 종합적인 대응체계를 구축하도록 하고, 이를 통하여 테러 또는 공격을 사전에 탐지하여 사이버위기 발생 가능성을 조기에 차단하는 등 사이버안전을 확보하려는 목적에서, "공공과 주요 민간을 포함한 책임기관 규정, 사이버안전센터와 보안관제센터 설치, 사이버테러 방지 및 위기관리 또는 사이버안전관리에 대한 기본계획의 수립 및 이행, 사이버위기경보, 사고 발생시 통보·복구·조사·처리, 인프라 구축에 관련한 사항을 두고 있다는 점에서 공통점이 있다. 하지만 양 법률안 모두 나날이 진화, 흉폭화 되어 가는 사이버안전 위협 사태에 대응하기에는 역부족이며, IT강국으로 자처하는 우리의 실무 현실을 법제도가 뒷받침 해주지 못하고 있는 것이다. 이는 앞서 살펴본 바와 같이 미국, 영국, 독일 등 주요 국가들이 사이버안전 관리와 관련된 국가 차원의 법적·제도적 시스템을 도입하고 있는 현실을 감안해보더라도 더욱 그렇다.

현재 우리 사회의 모든 영역에서의 급속한 정보화로 사이버 공간과 실제 공간 간의 경계가 모호해졌으며, 이에 따라 향후 사이버안전을 위협하는 행위는 더욱 증대될 것이다. 따라서 발생 가능한 사이버안전 위협 상황 등을 사전에 방지하기 위해서는 국가 전체의 사이버안전 관리를 총괄할 수 있는 법·제도적인 체계를 구축할 필요성이 있을 것이다.

하지만 이 경우에도 간과하지 말아야 할 중요한 사항은 이러한 법·제도의 정비 시에 핵심조정기관의 역할을 하게 될 기관에 대한 민주적인 감시와 견제 장치까지를 제도화해야 한다는 것이다.

참고문헌

〔1〕 http://www.mt.co.kr/view/mtview.php?type=1&no=2008011817260290355&outlink=1

〔2〕 Changyoung Lee, 『New Terrorism and National Crisis Management』, Dae Young Book, 2007, p.139.

〔3〕 Junhyeon Jeong, "Problems of the Legal Systems on the national Cyber-security and A Suggestion", Journal of National Intelligence Studies Vol.4. No.2., 2012, pp.10-11.

〔4〕 Hongsuk Kim, "Cyber Terror and National Security", 『Justice』 Vol.121., 2010.12., p.324.

〔5〕 Kang, Seok Ku et al., "A Study on the Construction of Efficient System for Safe Cyber space", Korean Institute of Criminology, 2010, p.40.

〔6〕 http://www.netan.go.kr

〔7〕 http://service1.nis.go.kr

〔8〕 http://www.krcert.or.kr

〔9〕 Kang, Seok-Ku et al., "A Study on the Construction of Efficient System for Safe Cyber space", Korean Institute of Criminology, 2010, pp.173-174.

〔10〕 *Supra Note 9*, pp.169-170.

〔11〕 http://www.usdoj.gov/olp/pdf/usa_patriot_improvement_and_reauthorization_act.

〔12〕 Homeland security Act of 2002, SEC. 2. DEFINITIONS (15).

〔13〕 *Supra Note 9*, pp.182-184.

〔14〕 *Supra Note 9*, pp.188-190.
〔15〕 *Supra Note 9*, pp.205.

저 자 소 개

오 태 곤
2001: 조선대학교
법과대학 법학과 법학사.
2003: 조선대학교
대학원 법학과 법학석사.
2005: 조선대학교
대학원 법학과 법학박사
현 재: 조선대학교
법과대학 외래교수
관심분야: IT Convergence
Email : t6713@naver.com

성 관 실
2013: 조선대학교
대학원 법학과
법학박사 과정
현 재: 새얼문화재단
운영위원
관심분야: 경영정보
Email : sks5317@naver.com