情 報 保 護 學 會 誌
第20卷 第4號, 2010. 8

사이버테러 동향과 대응방안

문 종 식*, 이 임 영**

요 약

인터넷 및 컴퓨터 시스템의 급격한 발전으로 인해 네트워크를 통한 서비스 제공이 금융, 교통, 산업, 방송, 의료 등 사회 기반에 전반적으로 사용되고 있다. 이와 함께 네트워크의 취약점을 악용한 사이버 공격이 증가하고 있어 사회 전반적인 부분에 피해를 입힐 수 있는 중대한 위협요인으로 등장하고 있다. 이와 같은 사이버 공격이 테러리즘 등 특정 목적과 결부될 경우 국가 안전보장에 대한 위기를 초래하는 등 심각한 문제가 될 수 있다. 따라서 본 논문에서는 사이버테러의 개요 및 국내·외 사이버테러 동향에 대해 알아보고, 각 국가별 대응방안에 대해 알아본다.

Ⅰ. 서 론

컴퓨터와 인터넷의 급속한 확대로 인하여 고도의 정보화 사회로 들어서고 있다. 컴퓨터의 사용이 금융, 교통, 산업, 방송, 의료 등 사회기반에 전반적으로 확대되면서 이를 악용한 역기능이 발생하고 있다[1,2]. 인터넷 초창기에는 자신의 능력을 과시하기 위해 해킹 실력을 보여주는 것이 사이버 범죄의 주된 유형이었다. 이와 같은 과시욕이 특별한 이념이나 국가적인 목적과 결합하여 국가별 사이버 범죄가 많이 발생하고 있으며 상대국가를 위협하는 하나의 테러 수단으로 사용되고 있다.

이러한 사이버테러는 특정한 정치, 사회적 목적을 가진 개인, 테러집단이나 적성국 등이 해킹, 컴퓨터 바이러스의 유포 등 전자적 공격을 통해 주요 정보기반 시설을 오동작, 파괴하거나 마비시킴으로써 사회혼란 및 국가 안보를 위협하는 행위로 정의되며 현대사회에서 대비되어야 될 새로운 문제로 대두되고 있다.

따라서 본 논문에서는 사이버테러의 개요 및 국내·외 사이버테러 동향에 대해 알아보고 각 국가별 대응방안에 대해 알아본다.

Ⅱ. 사이버테러 개요

사이버테러는 정보통신기술의 발전과 인터넷의 확산으로 인한 유비쿼터스 컴퓨팅 환경이 조성되면서 최근에 많은 이슈를 불러오고 있다. 본 장에서는 이에 대한 개념 및 사이버테러 유형별 특징에 대하여 알아본다.

2.1 사이버테러 정의

사이버테러는 상대방 컴퓨터나 정보기술을 해킹하거나 악성 프로그램을 의도적으로 설치하는 등 컴퓨터 시스템과 정보통신망을 무력화하는 새로운 형태의 테러리즘이다. 그 대상이 개인인가 국가인가를 불문하고 사이버 공간을 이용한 모든 공격 행위 자체를 광의적인 개념으로 사용하는 경우도 있으며 인터넷 사기, 사이버 음란, 사이버 폭력, 사이버 비밀침해 행위 등도 모두 사이버 테러의 개념에 포함 시키고 있다.

2004년 국가 사이버 안전 매뉴얼[3]에서는 특정한 정치·사회적 목적을 가진 개인·테러집단이나 적성국 등이 해킹·컴퓨터 바이러스의 유포 등 전자적 공격을 통해 주요 정보기반 시설을 오동작·파괴 하거나 마비시킴으로써 사회혼란 및 국가안보를 위협하는 행위로 정의하고 있다.

2.2 사이버테러 유형

사이버 공격 기법은 갈수록 점차 지능화되어가고 있

* 순천향대학교 컴퓨터학부 (jsmoon@sch.ac.kr)
** 순천향대학교 컴퓨터학부 (imylee@sch.ac.kr)

〔표 1〕 침해 주체에 따른 침해 위협

구 분	개인적침해 위협	조직적침해 위협	국가적침해 위협
주 체	해커 및 사이버 범죄자	산업스파이, 테러리스트, 조직화된 범죄집단	국가정보기관, 사이버전사
목 적	금전획득, 영웅심발휘, 명성획득	범죄조직의 이익달성, 정치적 목적달성, 사회·경제적 혼란 초래	국가기능 마비, 국가 방위 능력 마비
대 상	민간사설망, 전자상거래망, 개인용 컴퓨터	기업망, 금융, 항공, 교통 등 정보통신망	국방, 외교, 공안망 등
방 법	컴퓨터 바이러스, DDoS, 해킹 등	유·무선 도청, 정보통신망 스니핑, 통신망 교환 시스템 공격	첨단도청 및 암호해독, 전자공격무기 등

참고자료 : 2004 국가정보보호백서

다. 특히, 최근의 사이버 공격 형태는 단순 자기과시에서 벗어나 금전적인 이득추구로 본격화되고 있으며 정보유출을 목적으로 한 악성코드가 크게 증가하고 있고, 피싱 등 여러 사회공학적 방법과 유기적으로 결합한 사이버 공격 수법이 나날이 증가되고 있다. 이러한 사이버 테러는 침해 주체, 침해 목적, 침해 대상, 공격 방법에 따라 분류 할 수 있으며, 국가정보보호백서에서는 침해 주체에 따른 침해 위협을 분류 하고 있다. 개인적 침해 유형으로는 컴퓨터 바이러스, 해킹, 서비스 거부 공격이 있고, 조직적 침해 유형으로는 개인적 공격 방법을 포함하여 유·무선 도청, 통신망 교환 시스템 동작마비 공격 등이 있으며, 국가적 침해 유형으로는 개인·조직적 공격방법을 포함하여 첨단도청 및 암호해독, 전자공격무기 등이 있다. [표 1]은 침해 주체에 따른 위협에 대한 내용이다[4].

Ⅲ. 사이버테러 동향

사이버테러는 컴퓨터의 보급을 시작으로 현재까지 지속적으로 발생하고 있으며, 본 장에서는 국내·외 사이버테러 동향에 대해 알아본다.

3.1 국외 사이버테러 동향

국외 사이버테러 동향은 국가차원의 테러와 주요시설 및 국가기관의 네트워크 공격을 목적으로 해킹 및 DDoS 공격을 수행하고 있다. 주로 중국 및 러시아발 해킹이 발생하고 있는 것으로 보이며, IT가 발달한 선진 국가에게 공격을 행하는 것으로 보인다. 이 절에서는 에스토니아, 미국, 그루지야, 브라질 등의 사례를 분석한다.

3.1.1 에스토니아 사이버테러 사례

해킹 중심의 초창기 사이버테러는 시간이 흘러 첩보활동 중심의 사이버테러 양상을 보이고 있으며 피해 규모 역시 확대되고 있다. 2007년 일어난 에스토니아 사이버테러 사건은 러시아의 공격으로 3주간 대통령 궁, 의회, 정부기관, 은행, 이동통신 네트워크 등 국가 시스템이 마비되는 초유의 사태가 발생하였다. 해커들은 여러 대의 컴퓨터로 특정 사이트를 일제히 공격해 단시간에 시스템을 마비시키는 DDoS 수법을 이용하였다. 이같이 피해가 커진 이유는 에스토니아 사회가 인터넷 무선 접속이 비교적 자유롭고 인구의 절반 이상이 인터넷 뱅킹을 하는 IT강국이어서 피해규모가 더 심각하였다.

3.1.2 미국의 사이버테러 사례

2003년 7월 미국 뉴욕에서는 사상 최대의 정전사태가 발생했다. 미국과 캐나다 국경에서 발생한 국지적 정전사태가 번져, 7개주에 걸치는 대규모 정전사태로 확대된 것이다. 처음의 원인은 송전선에 걸쳐진 나뭇가지로 시작된 것이었으나, 모든 배전 분전 시스템이 컴퓨터망으로 연결되어 있는 미국에서는 '블래스터 웜'에 의해 더욱 더 심각한 상태로 확대되었다.

또한 2009년 7월 미국의 백악관을 비롯해 한국의 주요 웹 사이트들이 사이버공격을 받았다. 최근 유행하고 있는 DDoS공격을 통해 미국의 백악관 및 검색엔진인 '에스크 닷컴'이 공격받았고, 24시간동안 서비스가 제공되지 못했다. DDoS공격의 문제점은 다수의 사이트를 대상으로 하고 있어 추적이 어렵고, 공격의 근원지인 악성코드 감염경로나 공격대상 목록 및 그 변형과정을 파악하기가 쉽지 않다. 따라서 미국에서는 백악관 컴퓨터 보안 책임자를 신설, 외부 사이버 공격에 대한 방어태세를 강화할 계획을 세우고 있고, 신규 온라인 보안

시스템을 갖추는데 총 170억 달러를 투입한다는 목표를 제시하고 있다[5,6].

3.1.3 그루지야의 사이버테러 사례

2008년 8월 영토분쟁으로 무력 충돌이 확산되고 있는 그루지야의 주요 정부 인터넷 사이트(의회, 국방부, 외교부)가 러시아로부터 무차별 공격을 당했다. 그루지야 사이버테러 사건은 그루지야의 정부, 언론, 금융, 교통을 마비시킨 후 오프라인 군대에 의한 전쟁이 일어난 사건으로 사이버테러가 전쟁의 초기 공격이 될 수 있음을 보여주는 사건이다. 공격방법은 미국의 유명 소셜네트워킹 사이트인 페이스북과 트위터 등을 해킹해 미국민들의 개인정보를 이용하여 마이크로소프트의 소프트웨어와 연결해 그루지야 정부의 사이트를 공격한 사건으로 이전의 해킹 및 DDoS 공격과는 다른 기법을 이용하여 공격하였다. 이 사례는 소셜네트워크가 사이버테러에 악용될 수 있음을 보여주고 있다.

〔표 2〕 국외 사이버테러 현황

연 도	내 용
1986	소련, 미국 미사일 방어체계 정보 입수 위해 관련 연구소 침입 시도
1990	미국, 이라크로 수출하는 프린터 장치에 컴퓨터 바이러스 이식 이후 1991년 걸프전 당시 이라크 방공망 완전 마비
2000	이스라엘-팔레스타인 4개월간 해킹 전 이스라엘 텔아비브 증권거래소와 은행 등 40여개 사이트 파괴
2001	미국 정찰기와 중국 전투기가 충돌한 사건 이후 미-중 해킹전 시작 백악관 사이트 일시 마비
2004	중국 해커들, 한국 국방연구소·원자력연구소·외교부·주요 언론사 웹사이트 집중 공격
2005	일본 방위청·경찰청 컴퓨터 시스템 해킹 흔적 발견
2007	중국 해커들, 미국 국방부 동아태국 집중 공격해 초토화, 로버트 게이츠 국방장관 컴퓨터까지 침입
2007	러시아 해커들, 에스토니아 정부·언론·방송·은행전산망 일제공격
2008	그루지야 러시아 해커들이 정부·은행 DDoS 공격
2009	키르기스스탄 러시아 해커 공격으로 정부 전산망 불통
2009	7.7 DDoS대란, 한국 주요사이트 및 미국 사이트 DDoS공격

참고자료 : '국가 전산망 사수작전', 서울신문 2008.4

3.1.4 브라질 사이버테러 사례

2001년 6월 브라질해커 그룹인 'Prime Suspectz'는 채 1시간도 되지 않는 시간 동안 보안이 완벽하다고 여겨졌던 feeds.mobile.msn.com 등 4개의 MS 사이트를 해킹하여 홈페이지를 변조하였다. 이후에도 2003년 브라질 해커그룹 'drwxr'이 미 NASA 홈페이지를 해킹하여 이라크 반전문구를 삽입하는 사례가 발생하였다. 또한 브라질 소프트웨어 개발자 'Marcos Velasco'가 심비안 운용체제의 블루투스 휴대폰에 적용되는 악성코드를 제작, 공개하여 변종 발생 등이 우려되고 있는 등 브라질의 해커들의 전 세계를 대상으로 하는 무차별적인 사이버공격은 현실적인 위협이 되고 있다.

최근에는 해킹 사건의 발원지로 대부분 중국이 지목되고 있으며, 국내에도 중국발 해킹, 바이러스, 스팸메일 등이 지속적으로 증가하고 있다. 중국 인터넷 정보센터(CNNIN)에 따르면, 홍커(Red Hacker)라고 불리는 약 100만명 정도의 해커가 중국 내에서 활동 중인 것으로 추정되고 있다. 그 외 국외 사이버테러현황은 [표 2]와 같다.

3.2 국내 사이버테러 동향

국내 경찰청 사이버테러 대응센터인 NETAN[7]에서는 사이버테러 범죄 중에서 전자상거래 사기나 프로그램 불법복제, 개인정보 침해 등과 같이 사이버공간이 범죄의 수단으로 사용되는 범죄 유형인 일반 사이버범죄와 구분하여, 해킹, 바이러스 유포와 같이 고도의 기술적인 요소가 포함되어 정보통신망 자체에 대한 공격행위를 통해 이루어지는 범죄를 사이버테러형 범죄로 규정하고 있다. [표 3]에서는 2008년까지의 사이버범죄 발생 및 검거현황을 나타내고 있다[8].

〔표 3〕 사이버테러형 범죄 발생, 검거현황

구분 / 연도	발생건수	검거건수
2003	14,241	8,891
2004	15,390	10,339
2005	21,389	15,874
2006	20,186	15,979
2007	17,671	14,037
2008	20,022	16,953

참고자료 : 경찰청 사이버테러대응센터

우리나라는 지난 2003년 1월 25일 일어난 '인터넷 대란' 사고와 2009년 7월 7일 일어난 '7.7 DDoS 대란' 사고에서 볼 수 있듯이 정보 기반이 잘 구축되어 있어 국가적으로 전자정부 서비스 확산과 금융·통신 등 국가 핵심 전산망의 인터넷 연동 등의 추세에 따라 국가·사회 기능의 전산시스템 의존도 높은 만큼 이에 대한 사이버테러의 위협에 취약할 수밖에 없다[9].

3.2.1 국내 사이버테러 사례

국내의 사이버테러 사례를 보면, 2001년 4월 한 해커가 국내 유명 신용카드 회사 및 금융전산망과 전용망으로 연결되어 신용카드 거래 승인·결제 업무를 수행하고 있는 신용카드정보처리 전문 업체의 시스템을 해킹해 약 47만 명가량의 주민번호, 신용카드 번호 등 중요 신용정보를 유출하여 판매하려다 경찰청 사이버테러대응센터에 검거된 바 있다.

또한, 같은 해 한 해커가 방화벽을 우회하여 약 700만 명의 개인정보를 유출하였다가 경찰청 사이버테러대응센터에 검거된 바 있다. 테러 대상 업체의 네트워크 시스템은 보안을 위해 많은 투자를 아끼지 않았고, 방화벽을 이용하여 내부전산망과 외부전산망을 구분하였으며, 웹서버는 외부망에 위치하도록 하는 등 다양한 보안기술을 접목시켰다. 그러나 해커는 방화벽과 DB 서버 사이의 취약점을 이용하여 공격에 성공하였다.

2002년 12월 국내 모 보안회사 타이거팀 연구원 10여명이 보안컨설팅 수주를 목적으로 국내 금융기관 등 80여 개 사이트를 조직적으로 해킹하여 정보를 유출, 영업목적으로 사용해오다 경찰청 사이버테러대응센터에 전원 검거되는 조직적인 공격 사례도 발생한 바 있다.

2005년 발생했던 1.25 인터넷 대란 사건의 경우는 이전의 사이버테러 공격 유형과는 다른 사례로써, 특정 대상을 공격한 것이 아닌 불특정 대다수를 노린 공격이었다. 주공격 기술로 사용된 슬래머 웜은 15분 만에 전 세계적인 대규모 트래픽을 발생시켰으며, 국내 인터넷 대부분이 마비되는 결과를 가져왔다.

최근 사이버테러 공격 사례 중 이슈가 되는 분산서비스 거부공격(DDoS)의 경우 지난 2001년 2월, 국내 초등학교 해킹 사건을 수사하는 과정에서 분산서비스 거부공격 도구인 Starcheldraht 마스트 프로그램을 발견하여 역추적해 본 결과, 네덜란드의 한 해커가 국내 26곳,

〔표 4〕 국내·외 제어시스템 피해 사례

연도	발생국	피해내용	비고
1999	미국	▪ 워싱턴 주 올림픽 파이프라인사의 석유 송유관 제어시스템 DB 수정 후 송유관이 폭발 ▪ 3명 사망, 피해액 4,500만 달러, 786만 달러 벌금 부과 ▪ http://seattletimes.nwsource.com/html/opinion/2009319747_guest10goltz.html	석유
2000	호주	▪ 퀸즈랜드주 오폐수 처리 제어시스템을 전직 직원이 무선통신 해킹 ▪ 3달 동한 46차례에 걸쳐 오폐수 방출 ▪ http://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage	환경
2003	미국	▪ 미국 오하이오주의 Davis-Besse 원자력 발전소의 사설 컴퓨터 네트워크에 슬래머웜이 침투 ▪ 안전 감시시스템이 5시간 동안 정지 ▪ http://www.nrc.gov/reading-rm/doc-collections/news/2003/03- 108.html	원자력
2003	한국	▪ ISP의 DNS 등이 슬래머웜에 감염 ▪ 수 시간동안 인터넷 접속 마비 ▪ http://www.krcert.or.kr/index.jsp	통신
2003	미국	▪ 동부지역의 철도신호시스템이 소빅-F 웜에 감염 ▪ 수 시간 동안 운행 중단 ▪ http://www.cbsnews.com/stories/2003/ 08/21/tech/main569418.s html	교통
2007	미국	▪ DHS 주관 미국 발전소 제어시스템을 모의해킹 ▪ 발전기 가동 사이클을 변경하여 발전기 파괴 ▪ http://www.cnn.com/2007/US/09/26/power.at.risk/index.html#cnnSTCTText	전력
2007	미국	▪ 전직 직원이 캘리포니아주의 TCCA 운하 제어시스템에 악성프로그램을 설치 ▪ 운하 운영 마비 ▪ http://www.computerworld.com.au/article/198630/insider_charged_hacks-into-citys-tram-system.html	수자원
2008	폴란드	▪ 14세 소년이 TV리모컨을 개조하여 트램 교차로를 불법 조작 ▪ 4대의 트램 탈선 및 12명 부상 ▪ http://www.telegraph.co.uk/newSWorldnews/1575293/Schoolboy-hacks-into-citys-tram-system.html	교통
2008	미국	▪ 회계감사원(GAO) 주관 미국 최대 국립전력회사인 TVA사 제어시스템을 모의해킹 ▪ 발전소 제어시스템 침투 성공 ▪ http://www.cnn.com/2008/US/05/21/cyber.attack/index.html	전력
2009	러시아	▪ 수력발전댐의 터빈 제어시스템 장애 ▪ 발전기 터빈 폭발, 75명 사망 ▪ http://en.wikipedia.org/wiki/2009_Sayano-Shushenskaya_hydro_accident	수자원

참고자료 : 2010 국가정보보호백서

국외 299곳 등 총 325개의 시스템을 해킹, 데몬 프로그램을 설치하였다가 발견된 적이 있었다. 분산서비스 거부 공격은 2000년 이후 급속히 발전한 공격기법으로 인터넷 등 전체 네트워크를 마비시키는 경우보다는 특정한 목표를 정해서 공격하는 경우에 많이 사용된다.

이와 같이 국내 공공 및 민간분야에서 많은 사이버테러 사례가 소개되었으나, 2004년에 주요 국가기관이 해킹당하는 사건이 발생하였다. 위장된 악성프로그램을 국가기관 직원을 사칭하여 e-mail 등에 첨부하고 유포함으로써 방화벽 내부의 소수 시스템을 장악하고 이를 통해 내부에서 다수의 시스템을 직접 해킹한 후 저장된 파일 및 e-mail 정보 등 주요 정보를 유출하는 치밀한 수법이 사용되었으며 국회, 원자력연구소, 해양경찰청, 국방연구원 등 10여개 기관의 220여 대의 시스템이 해킹 피해를 입은 것으로 밝혀졌다. [표 4]는 국내·외 제어시스템의 사이버테러 사례이다[10].

Ⅳ. 사이버테러 대응방안

사이버테러가 지능화됨에 따라 각 국가에서는 사이버테러에 대한 대비책을 마련하고 있다. 이 장에서는 국가별 사이버테러 대응방안에 대해 알아본다.

4.1 미국

미국의 경우 테러관련 22개 부처를 통합한 국토안보부(DHS)가 사이버테러 및 정보전에 대한 범국가적 대응활동을 조정, 통제하고 있으며, 전략사령부는 컴퓨터 네트워크 공격 및 방어와 관련된 군의 활동을 총괄 조정, 통제하고 있다. 또한 사이버 지휘부대 창설 및 사이버 전쟁 모의훈련 등을 실시하여 사이버테러에 대응하고 있다. 루이지애나 주 박스데일 공군기지에 '사이버 지휘부대'를 만들고, 통신 보안과 시설감시, 도메인 장악, 인프라 보안 등의 방어기술을 개발하고 국토 안보부에서는 매년 사이버전쟁 모의훈련을 실시하고, 산하에 사이버보안 및 통신실을 설치하여 사이버 공격 위협분석, 취약점 보완, 사이버 위협 경고전파, 사이버 공격 대응활동 조정 등을 실시하고 있다[11].

4.2 일본

일본의 경우 2001년 33억 엔을 들여 사이버전 연구계획을 수입한 뒤 시험용 바이러스 및 해킹 기술의 독자개발을 추진하고 있으며 2006년 사이버 전투부대를 창설하였다. 2005년 '정보시큐리티센터의 설치에 관한 규칙(내각총리대신결정)'에 의거하여 설립한 '내각관방 정보보호센터(NISC, National Information Security Center)'에서 2009년 1월부터 중앙 성청에 대해 24시간 해킹·웜바이러스 등 사이버위협징후에 대한 모니터링을 실시하고 있으며, 탐지된 위협에 대해서는 공격자 정보, 공격시간, 공격방법 등을 분석하여 해당 성청에 지원하는 업무를 수행중이다[12].

4.3 EU(유럽)

EU는 정보보안에 대한 유럽 각국의 초국가적 협력을 위해 2004년 유럽 네트워크정보보안청(ENISA)을 설립해 공동으로 대응하고 있으며 ENISA는 보안사고 처리를 위한 데이터 수집 프레임워크 및 신뢰지수 측정방안 개발, 보안정보 공유 및 경고시스템의 실행가능성을 검토 등 수행하고 있다. 또한 유럽 각국에 컴퓨터 비상대응팀(CERT) 구축을 지원하고, 각국의 수준에 맞는 컨설팅을 실시, 우수 CERT 활동 사례등을 전파하고 있다[11].

4.4 NATO(북대서양조약기구)

NATO는 사이버 전쟁에 대한 연구 수행 및 대응을 위해 에스토니아에 사이버 방어센터를 설립하였고 독일, 이탈리아, 라트비아, 리투아니아, 슬로바키아, 스페인 등 6개국은 사이버 방어센터를 위한 예산과 전문요원을 지원하고, 미국은 참관국 자격으로 동참하였다. 사이버 방어센터는 사이버 테러 방어 관련 연구·협의·훈련 등의 프로젝트를 수행하고 있다[8].

4.5 중국

중국은 1999년 바이러스 해커부대를 창설, 실전에 배치하고 넷포스(Net Force)를 운영 중으로 사이버체계 구축을 신국방전략의 핵심으로 삼고 있다. 또한 공안부는 국무원의 지휘 하에 국가 전체에 대한 공안 업무를 담당하고 있으며, 중국 내의 컴퓨터 및 네트워크 보안 정책과 기술 개발에 관여를 하면서 국가 기밀을 보호하는데 있어 핵심적인 역할을 수행하고 있다[13].

4.6 북한

북한은 1989년부터 사이버전 전담인력을 매년 100명이상 양성하고 있으며, 미 국방부 자체 모의 실험결과 태평양사령부 지휘통제소를 마비시키고 미 본토 전력망 피해를 유발시킬 절도의 사이버전 역량을 갖추고 있는 것으로 알려졌다.

4.7 한국

우리나라의 사이버테러 대응체계는 국가안전보장회의(NSC) 사이버안전 정책조정회의를 중심으로 민간 부분에는 정보통신부와 한국인터넷진흥원의 '인터넷침해사고대응지원센터'가 담당하고, 국방 분야는 국방부와 기무사, 정부 공기관은 국가정보원과 경찰청 사이버테러대응센터 등이 담당하며 비상시 유기적으로 결합하도록 하고 있다. 발달한 IT 수준만큼 다양하고 앞선 사이버테러형 범죄가 발생함에 따라 외국에서 사이버 테러형 범죄 수사기법을 벤치마킹하여 대응하고 있으며, 국가간 공조를 위해 관련분야에서의 주도적 역할로 원활한 협력체계의 마련 및 강화를 하고 있다.

이 밖의 대응책으로는 민·관 보안관제의 기술정보를 교류해야 하며, 국가사이버안전센터와 민간 보안관제 서비스 업체 간의 사이버 안전 약량을 강화해야 한다. 이는 해킹 등 사이버공격의 조기 탐지 및 대응을 위한 것으로 상호 원활한 정보교류가 선행되어야만 한다.

또한 최근 일반적인 해킹뿐만 아니라 개인정보 유출 및 기업 핵심 기술 유출 등의 내부 정보 유출이 급격하게 증가하고 있다. 그러나 현재 일반 기업의 경우 정보보호에 대한 개념과 이해가 매우 부족한 상황이며, 정보보호에 관심을 가지고 있는 기업이라도 실질적인 예산 책정이 어려워 이에 대한 대응책이 필요한 실정이다. 따라서 기업경영자의 보안에 대한 인식 마련이 최우선이며 보안 전담 인력 및 부서가 필요하고 시스템에 대한 보안뿐만 아니라 관리자의 정보보호 의식 고취가 필요하다.

전 세계적으로 발생한 사건에 대해서는 기민하고 끈질긴 수사로 즉시 해결하여 전 국민이 사이버 공간에서 안심하고 자유롭게 정보를 습득 및 공유할 수 있도록 하여야 한다. 그러나 정작 중요한 것은 시스템 운영자나 개개인이 모두 보안에 늘 신경 써야 하며, 자신이 공격당하면 모두가 피해 입을 수 있다는 생각으로 보안에 신경 쓰는 것이 중요하다[11].

V. 결 론

컴퓨팅 시대가 발전하면서 일반 테러활동에서 사이버환경을 이용한 테러가 주요한 위치를 차지하게 되었다. 인터넷의 확산으로 짧은 시간에 가장 큰 피해를 입힐 수 있는 사이버 테러는 갈수록 지능화 되어가고 있다. 각 국은 2001년 9월 일어난 미국 9.11테러사건이후 사이버 테러에 대한 대응방안을 세워 사이버테러에 대비하고 있다. 우리나라는 이러한 사이버테러의 대비하기 위하여 국가기관과 민간기관과의 협력체계를 구성하고 있으며, 국가적 대처뿐만 아니라 개인적 대응을 위한 다양한 방안을 마련하고 있다. 또한 사이버테러 대응을 위한 기술적 방안, 법률적 방안, 교육적 방안을 기반으로 국가 사이버테러 대응체계를 확고히 해나가고 있다. 앞으로 국내·외 적으로 사이버테러 대응을 위해 국가간 공조를 통한 대응 시스템 구축이 필요할 것으로 사료된다.

참 고 문 헌

[1] 박영우, "사이버범죄방지협약의 국내법적 수용문제," 정보보호학회지, 13(5), pp. 70-75, 2003년 10월.

[2] 이기혁, 이철규, "사이버 환경에서의 침해사고대응을 위한 위험도 산정 및 실시간 경보생성에 대한 연구," 정보보호학회지, 18(5), pp. 112-124, 2008년 10월.

[3] 국가사이버안전센터, "국가사이버안전매뉴얼," 2005년 10월.

[4] 2004 국가정보보호백서, pp. 14-32 , 2004년 5월.

[5] 오일석, 김소정, 고재영, "미국과 프랑스 정부의 사이버조기 경보 체계," 정보보호학회지, 15(1), pp. 1-8, 2005년 2월.

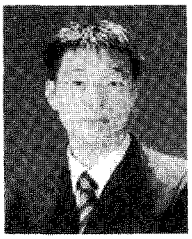
[6] 이철수, "침해사고 국가 대응 체계 - National security system for countering information incidents," 정보보호학회지, 15(1), pp. 33-40, 2005년 2월.

[7] 사이버테러 대응센터, http://www.netan.go.kr/cyber/division.jsp

[8] 사이버테러대응센터 NETAN, "사이버 범죄 현황",

http://netan.go.kr/cyber/graph01.jsp
[9] 최정호, "사이버테러리즘의 변천방향과 한국의 대응", 국방안보학술회의, pp. 155-172 , 2008년 4월.
[10] 2010 국가정보보호백서, pp. 58-59 , 2010년 4월.
[11] 한국정보화진흥원, "국가 사이버테러 현황과 대응동향", CIO 리포트, pp. 1-7 , 2008년 9월.
[12] 김영진, 이수연, 권헌영, 임종인, "국가 전산망 보안관제업무의 효율적 수행방안에 관한 연구," 정보보호학회논문지 19(1), pp. 103-111, 2009년 2월.
[13] 국가사이버안전센터, http://service1.nis.go.kr/ PDS/Pub.jsp?pdsKD=PUB1

〈著者紹介〉



문 종 식 (Jong-Sik Moon)
정회원

2006년 2월: 순천향대학교 정보기술공학부 졸업
2008년 2월: 순천향대학교 컴퓨터학과 석사
2008년 3월~현재: 순천향대학교 컴퓨터학과 박사과정
<관심분야> AAA, IPTV 보안, 디바이스 인증

이 임 영 (Im-Yeong Lee)
종신회원

1981년 2월: 홍익대학교 전자공학과 졸업
1986년 2월: 오사카대학 통신공학전공 석사
1989년 2월: 오사카대학 통신공학전공 박사
1985년~1994년: 한국전자통신연구원 선임연구원
1994년~현재: 순천향대학교 컴퓨터학부 교수
<관심분야> 암호이론, 정보이론, 컴퓨터 보안