선진국 정보보호 정책 동향 분석

김정태, 이현우, 현창희

한국전자통신연구원 정보통신서비스연구단 정보기반연구팀

{acroo,lhwoo,chhyun}@etri.re.kr

요약

대부분의 선진국들이 정보통신사회로 점진적으로 변모함에 따라서, 사회 기반시설이 네트워크를 통해 연결되어 많은 사용자들이 편리하게 이를 이용할 수 있는 환경이 조성되었다. 그러나, 이러한 순기능과 더불어 웜이나 바이러스와 같은 악성코드나 네트워크를 이용한 범죄의 증가로 인해 경제적, 사회적 문제가 대두되기 시작하였고, 사이버테러리즘이 일부 국가에서 나타나고 있는 테러의 수단 중 하나가 될 수 있다는 예상도 잇따르고 있다. 이에, 공공 안전을 위한 중요한 요소의 하나로 정보보호가 부각됨에 따라 미국, 일본 등의 선진국은 정보보호 관련 법안의 제정 및 관련기술의 연구개발이나 투자를 시행하고 있다. 이러한 선진국에서의 정보보호 정책 도입과정에서의 주요 쟁점들에 대해 살펴보고 국내 실정에서 참고할 만한 시사점을 찾아보고자 한다.

키워드: 정보보호, 정책수립, 동향분석

I. 서론

초고속 인터넷, 전자상거래, 모바일 네트워크 등, 정보통신의 보급과 고도화는 편리성을 가져온 한편, 정보보호에 대한 대책 수립의 요구도 증대시키고 있다. 특정 시스템에 대한 보안 대책은, 시스템이 요구하는 서비스, 소프트웨어, 하드웨어, 네트워크 구성, 사용자 정책 등에 따라서 각각의 요소마다 필요해 진다. 시스템의 규모가 증가할수록, 이를 관리·운용하기 위한 보안 대책의 필요성도 증가한다.

네트워크의 이용자 수가 증가하고, 네트워크의 고속화가 이루어짐에 따라서, 악성코드, 스팸메일, 개인정보 유출 등의 정보보호 침해 사례도 지속적으로 증가하고 있다. 이메일을 통한 바이러스의 전파에 이어, 최근 P2P 공유 프로그램을 타고 들어오는 '봇(bot)'류 악성코드의 피해도 확산되고 있는 추세로 P2P의 사용빈도가 높아짐에 따라서 이메일의 첨부파일 외의 신규 경로가 제공되고 있는 셈이다. 또한, 웜 피해 신고 건수는 급속히 증가하고 있는데, 이는 각종 웜의 변종이 지속적으로 출몰하는 것에 따른 결과로 보여 진다. 최근 등장하는 웜은 감염된 시스템에 백도어를 설치하고 향후 공격자가 추가 공격을 할 수 있는 거점을 확보하여, 웜에 감염된 시스템이 사용자 모르게 해킹 툴로 활용될 가능성이 높아지게 된다. 더욱 심각한 문제는 빠르게 진화하는 웜과 달리 대응 능력은 상대적으로 속도가 훨씬 늦다는 점이다. 바이러스와 웜뿐만 아니라, 스파이웨어라고 불리는 프로그램이 증가하고 있다. 대부분 사용자의 부주의한

프로그램 설치로 인해 시스템에 들어오게 되는 것이지만, 시스템 사용자는 그 존재를 충분 인식하고 있지 않는 경우가 많다. 따라서, 시스템 내의 중요 정보가 새어나가는 피해 사례가 빈번히 나타나고 있다.

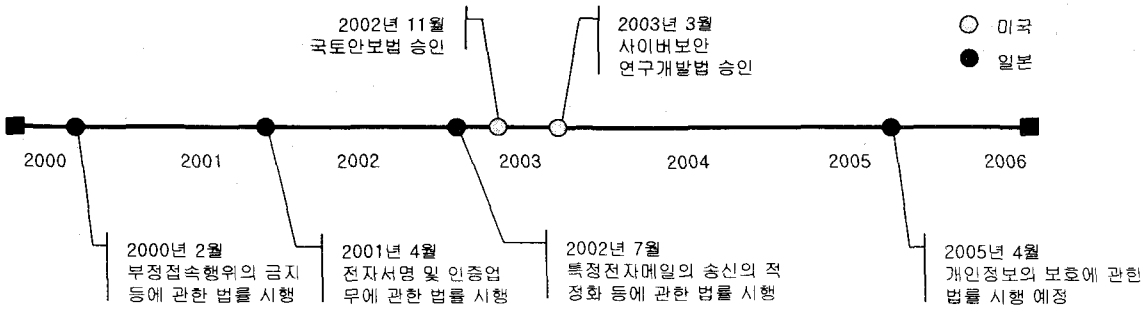
이러한 개인정보 유출 등의 프라이버시 침해 사건들로 인해, 개인정보가 자신이 알지 못하는 사이에 제 3자에 의해 수집되어 부정하게 사용될 수 있거나, 이미 유출되었을 지도 모른다는 사용자들의 불안이 증가하고 있다. 프라이버시의 보호는, 인터넷 이용자가 인터넷을 이용한 때에 느끼는 불안·불만으로 최대의 사유로 되어 있다. 또한, 이용자의 동의를 얻지 않고 광고, 선전, 권유 등을 목적으로 무차별적으로 전자 메일을 보내는 스팸메일이 증가하고 있으나, 현재까지 이와 관련된 뚜렷한 대응책이 마련되지 못한 상황이다.

근래, 개인이나 개별기업의 보안 침해뿐만 아니라, 정보통신 네트워크 전체를 위협한 침해 사례도 발생하고 있다. 사회 경제 전반에 있어 정보통신 네트워크에의 의존도가 늘고 있고, 일단 정보통신 네트워크의 안전성·신뢰성이 손상된 경우에는 막대한 피해가 발생할 우려가 있다. 일본 등의 일부 국가에서 지진과 같은 자연재해에 의하여 정보통신 네트워크의 안전성·신뢰성이 위협받는 경우도 있어 왔으나, DDoS 공격이나 사이버 테러 등의 인위적인 위협에 의하여 정보통신 네트워크의 안전성·신뢰성이 침해받는 사례가 보다 빈번해지고 있다.

본고에서는 선진 각국이 정보통신 네트워크의 안전성·신뢰성에 대한 위협에 대응하기 위해 마련하고 있는 정보보호 관련 정책, 조직 정비 현황, 기술개발 투자동향 등을 차례로 살펴보고자 한다.

II. 정보보호 분야 법제정비

정보통신 네트워크의 안전성 및 신뢰성의 확보를 위한 정책으로, 여러 선진국에서는 정보보호 분야의 법제를 정비하여 대응하고 있다. 미국의 경우 국토안보 영역 중 정보 네트워크와 시스템들에 대한 중요한 전자 기반시설을 보호하는 사이버보안을 중요시 하고 있어, 사이버보안 연구개발법과 국토안보법 등을 통하여 사이버보안에 대한 적극적인 연구개발을 시행하고자 한다. 일본 또한, 'e-Japan 전략' 중점계획의 하나인 '고도 정보통신 네트워크의 안정성 및 신회성의 확보' 달성을 위한 방안의 하나로서 2000년 이후부터 꾸준하게 정보보안 법제를 정비하고 있다.



<그림 1> 미국과 일본의 정보보호분야 법제정비 현황

1. 미국의 정보보호 법제정비

1) 사이버보안 연구개발법

컴퓨터 및 네트워크 보안에 관한 연구개발의 촉진과 인재육성을 목적으로 하는 미국의 '사이버보안 연구개발법(Cyber Security Research and Development Act, HR 3394, 이하 HR 3394)'은 2002년 11월에 상정되었으며, 의회는 2003년 3월에 이 법안을 승인했다. 이 법안은 컴퓨터 시스템이나 네트워크를 보호하기에는 현재의 정보보호 기술이 충분하지 못하며, 새로운 방법을 개발하기 위한 연구개발의 규모가 다른 연구 분야와 비교해 볼 때 충분하지 못하다는 것에서 시작되었으며, 구체적으로 다음과 같은 문제점들을 제기하고 있다.

- 민간 부문은 신속함과 편리함만을 중시하므로 사이버보안에 투자하는 비중이 작음
- 연방 정부의 사이버보안에의 투자가 부족함
- 강력한 사이버보안 연구를 수행할 행정 부처가 존재하지 않음
- 사이버보안 연구가 부족하여 사이버보안에의 기본적 대응이 어려움
- 자금과 연구자가 적어 사이버보안에 관심을 가지는 학생이 적음

이러한 사항들을 해소하기 위해, 국립과학재단(NSF)과 국립표준기술원(NIST)은 새로운 연구 및 교육 프로그램을 신설하였다. 이 프로그램의 목적은, 정부 또는 민간의 컴퓨터에 대한 테러리스트로부터의 공격을 예방하거나 차단하기 위해, 사이버보안 분야에서의 혁신적인 연구를 촉진하며 이 분야로 새로운 인력을 유도하거나 육성해 나가는 것이다. 이에, NSF는 다음과 같은 목적을 지닌 프로그램을 실시하기 시작하였다.

- 대학이 단독 또는 타대학이나 산업계나 정부 연구소와 협력해, 복수의 학술 영역에 걸치는 컴퓨터 및 네트워크보안 연구 센터를 설립함
- 대학이 사이버보안에 관한 학사 및 석사 프로그램을 개설 또는 개선함
- 박사 과정 학생이 네트워크보안 전공으로 학위를 취득하기 위한 연구 지원금을 지급함
- 대학원 학생이 박사 학위 취득 직후 사이버보안 분야의 학문적 발전을 추구할 수 있도록 능력향상을 위한 연습생 과정을 마련함

또한, NIST에서도 다음과 같은 목적을 달성하기 위한 프로그램을 개설중이다.

- 산학 제휴에 의해 산업계의 관심에 응하기 위한 연구 센터를 설립함
- 관련 분야의 상급 연구자가 사이버보안에 관한 연구를 실시함
- Post-Doc이 사이버보안에 관한 연구의 기회를 이용함

2) 국토안보법

국가안보의 약점을 보완하기 위한 미국의 '국토안보법(Homeland Security Act, HR 5005, 이하 HR 5005)'이 2002년 7월 발표되어, 2002년 11월 의회에서 통과되었다. 이 법률

에 의해 산하에 22개 연방정부기관과 18만 명의 직원을 거느리는 초거대 부처인 국토안보부(Department of Homeland Security, 이하 DHS)가 설립되게 되었다.

HR 5005에 의해 연방 수사국의 국가 기반시설 보호 센터(NIPC), 국방부의 국가 통신 시스템(NCS), 상무성의 중요 기반시설 보전국(CIAO), 에너지성의 분석 센터, 연방 컴퓨터 사건 대책 센터(FedCIRC) 등 중요한 기반시설의 보호를 담당하고 있던 기존의 여러 조직들이 DHS에 통합되었다. 또한, 국방부 산하의 고등연구 계획국(DARPA)을 표본으로 하는 국토안전 고등연구 계획국(HSARPA)이 설립되었다. HSARPA의 역할은 국토안전에 공헌하는 신기술의 혁신을 재촉하고 기술개발을 진행시켜, 국가의 취약성을 보완하는 기술의 실용화와 도입을 촉진하는 것이다.

DHS의 주요 임무는 미국에 대한 테러공격을 예방하고 국민을 보호하는 것이며, 이를 위해 △정보 분석과 기반시설 보호 △화학, 생물, 방사능, 핵 등에 대한 대응조치 △국경 및 수송부문 보안 △비상시 대처 및 대응조치 △연방 주 지방 정부 부서 및 민간부문과 공조 등 5가지 기능을 수행한다. 다음과 같은 구체적 조항이 HR 5005에 포함되어 있다.

- 정보기술, 금융 네트워크, 위성 등을 포함한 미국의 중요 자원 및 기반시설을 보호하기 위한 포괄적인 국가 계획을 작성함
- 컴퓨터 범죄를 수사하기 위한 도구, 인증 등을 취급하는 기술 분야 기관을 설립함
- 컴퓨터 범죄의 방지에 임하는 주 경찰이나 지방 경찰을 지원하기 위한 도구의 개발자금을 제공함
- 중앙정보국, 국방부, 국가 안전 보장국을 포함한 모든 정부기관에 대해, 미국의 기반시설의 취약성에 관한 정보를 DHS에 제공하는 것을 의무화함
- 개인 사생활보호 및 인권문제를 담당하는 부서를 설치해, DHS에 대해 개인정보의 이용, 수집, 개시에 있어서의 개인 사생활보호를 철저하게 함
- DHS는 중요한 정보 시스템을 운영하는 기업에 대해 기술 지원을 제공하여 취약성에 대해 경고함
- 지역사회가 정보 시스템 및 통신 네트워크에의 공격에 대처해 복구를 꾀하는 것을 지원하기 위해서 전국에서 자원봉사 단체를 조직함
- 시스템 및 취약성 분석, 전화망이나 인터넷 등의 기반시설의 취약성에 대해 시뮬레이션과 모델링을 수행하는 국토 안전 연구소(Homeland Security Institute)를 설치함

2. 일본의 정보보호 법제정비

1) 부정 접속 행위의 금지 등에 관한 법률

일본 총무성은 부정 접속 행위의 금지 및 처벌에 관하여 규정하고, 시스템에 대해 방어 조치를 실시하도록 하는 의무를 관리자에게 부과한 법률을 2000년 2월부터 시행하고 있다. 이와 동시에, 재발 방지를 위한 행정기관의 지원 조치 등을 정하여, 전기통신 회선을 통하여 행해지는 범죄의 방지 및 접근 제어 기능을 통해 전기통신에 관한 질서의 유지를 도모하고, 이를

통해 고도 정보 통신 사회가 건전하게 발전하는 것을 목적으로 한다.

2) 전자 서명 및 인증 업무에 관한 법률

일본 총무성은 전자 서명에 일반 문서상의 서명이나 날인과 동일한 법적 근거를 줌과 동시에, 인증 업무에 대한 인정 제도를 도입한 법률을 2001년 4월부터 시행하고 있다. 전자 서명에 관하여, 전자적 기록의 성립의 추정, 특정 인증 업무에 관한 인정 제도 및 그 밖에 필요한 사항을 정하고 있다. 전자 서명의 원활한 이용의 확보에 의한 정보의 전자적 방식으로의 유통 및 정보 처리의 촉진을 도모하고, 이를 통해 국민생활의 향상 및 국민 경제가 건전한 발전에 기여하는 것을 목적으로 한다.

3) 특정 전자 메일의 송신의 적정화 등에 관한 법률

이용자의 동의를 얻지 않고 광고, 선전 또는 권유 등을 목적으로 한 전자 메일을 송신할 때에는 '미 승낙 광고※'라고 표시하여야 하며, 수신 거부자에 대해서는 송신을 금하는 것을 골자로 하는 법률이 2002년 7월부터 시행되고 있다. 다수의 이용자에 대해 동시에 대량의 전자 메일을 송신하는 등에 의한 전자 메일의 송수신상의 지장을 방지하기 위해, 전자 메일 송신의 적정화를 위한 조치 등을 규정하고, 전자 메일의 이용에 관한 양호한 환경의 정비를 도모하는 것을 목적으로 한다.

4) 개인정보의 보호에 관한 법률

2003년 5월, 총무성은 개인정보의 보호에 관한 법률을 제정하고, 2005년 4월 시행을 앞두고 있다. 이 법률에서는 정보 통신 사회의 진전을 통해 개인정보의 유통, 축적 및 이용이 급속히 증가함에 따라, 개인정보의 적정한 취급에 대해 기본이 되는 사항을 규정하고 개인정보의 유용성을 고려하여 개인의 권리이익 보호를 포함하도록 유도하고 있다. 개인정보는 개인의 인격 존중의 이념 하에 신중히 취급되어야 하며, 개인정보를 다루는 자는 개인정보를 취급함에 있어서 다음의 원칙들을 지키도록 권고하고 있다.

- 이용 목적에 의한 제한: 개인정보는 그 이용 목적이 명확해짐과 동시에 해당 이용 목적의 달성에 필요한 범위 내에서 취급되어야 함
- 적정한 방법에 의한 취득 및 목적의 통지: 개인정보는 적법한 방법에 의해 취득 된 것이어야 하며, 개인정보를 취득한 경우 이용 목적의 통지 또는 공표하여야 함
- 내용의 정확성의 확보: 개인정보는 그 이용 목적의 달성에 필요한 범위 내에서 정확하고 최신의 내용으로 유지해야 함
- 안전 보호조치의 실시: 개인정보는 적절한 안전 보호조치를 강구한 뒤 취급되어야 함
- 제3자 제공의 제한: 본인의 동의 없이 개인 데이터를 제3자에게 제공하는 것을 금지함

3. EU의 정보보호 법제정비

EU에 있어서는, 2002년 6월에 채택된 'eEUROPE 2005 액션 플랜' 가운데에서, 2005년까지 달성할 목표 중 하나로 안전한 정보 인프라 구축을 위해 사이버보안 태스크포스의 설치,

보안 문화의 현실화, 행정 정보교환을 위한 안전한 통신 환경의 조사를 추진해 가는 것으로 결정하였다.

또한, 사이버범죄를 범유럽 차원에서 대응하기 위해 전담기구를 설립하였다. 유럽의회는 EU 15개 국가가 사이버 범죄에 공동으로 대처, 전담기구를 설립하도록 한 법안을 승인했다. '범유럽 네트워크 및 정보 보안청(ENISA, European Network and Information Security Agency)'이라고 명명된 이 기구는 2004년 1월부터 5년간 2,430만 유로의 예산으로 운영된다. 18명으로 이뤄진 이 기구의 관리위원에는 정부측 관계자는 물론 산업계와 민간단체 대표들도 참가하는데 EC 위원회와 유럽이사회에서 각각 5명, 유럽의회 2명, 산업계 4명, 소비자단체 2명 등으로 구성된다. 이 기구는 또 관리위원회 이외에 업계, 소비자단체, 과학계를 대표하는 9명의 인물로 구성된 자문위원회도 갖췄다.

4. OECD의 정보보호 법제정비

2001년, OECD는 각국의 정보보호 확보의 지침으로서 1992년에 정한 'OECD 정보 시스템의 보안·지침'을 개정하여, 2002년 8월에 '정보 시스템 및 네트워크의 보안을 위한 지침(Guideline for the Security of Information Systems and Networks: Towards a Culture of Security)'을 발표하였다. 새로운 지침에서는 '보안 문화'를 제창하고, 정보 시스템이나 네트워크의 이용이나 개발에 즈음하여 보안 의식을 높일 필요성을 강조하고 있다. 또, 네트워크의 관점에서 정보보호를 문제 삼고, 정보보호 확보에 관한 원칙들을 내세우고 있다.

개정 가이드라인은 법적인 구속력을 가지지 않지만 OECD 회원국들이 목표로 하는 보안 수준과 이를 달성하기 위한 OECD 회원국들의 공통적인 접근방식을 제시하고 있다. OECD는 향후 관련 회의에서 개정 가이드라인의 실천 방안을 중점적으로 논의할 예정이며 개정 가이드라인의 홍보, 회원국사이의 정보공유 체계 구축 등 OECD 차원에서의 가이드라인 실천방안들을 수행할 계획이다.

III. 정보보호 기구의 정비

정보보호이나 정보통신 네트워크에 대한 위기에 대처하기 위해, 선진 각국에서는 종합적인 정보보호 강화 대책을 책정하고 실시하고 있다. 미국이나 EU 등은, 9·11 테러 등을 계기로 국가 안전 확보에 대한 의식이 높아지고 있고, 정보보호 정책이 강화되고 있다. 일본에서는, IT 전략 본부 담당 조직을 설치하고 관련 법률의 개정, 기술 개발 등을 수행하고 있다. 또한, 정보보호와 관계된 정보의 집약, 전달, 축적 및 관민으로의 공유 등을 행하기 위해 공공기관뿐만 아니라 민간단체 차원에서의 보안 대응 기구의 결성도 이루어지고 있으며, 관계기관간의 연계를 강화하기 위해 협의회와 같은 자리를 통해 공조해 나가고 있다.

1. 미국의 정보보호 기구 정비

1) IAIP의 설립

HR 5005와 NSSC가 발표된 이후, DHS는 연구개발 활동에 중점을 맞춘 사이버보안 연구

개발 센터인 정보분석 및 기반시설보호(Information Analysis Infrastructure Protection, 이하 IAIP) 부문을 설립하였다. IAIP는 △사이버보안에 관련된 연구 및 평가 촉진 △공공 및 사설기관과의 의견교환과 조율, 확고한 사이버 기반시설을 마련하기 위한 국가적×국제적 협력 촉진 △IAIP의 윤용 상의 요구 지원 △참여 대학과의 교육 프로그램 개설을 촉진하기 위한 NSF와의 협력 등 네 가지 주요 기능과 역할을 담당한다.

2004년, IAIP는 주요 자산을 식별하고, 취약점을 파악하고, 위험 분석을 수행하는 것에 초점을 두고 있다. 중요한 기반시설은 정부에 의해 소유되거나 운용되고 있지 않으며, 효과적인 보호를 위해 정부와 사설업체의 협력을 요구하며, 중요한 기반시설의 보안담당자, 소유자, 운용자와 함께 작업한다. 2005년에는 주요 자산의 식별과 측량을 지속할 것으로 보인다. IAIP 산하의 팀들은 기반시설의 소유주와 운영자를 돕기 위해 현장을 방문하여 취약성을 식별하고 감소시키는 일을 수행해 나가며, 주요한 자산을 사이버 테러리스트의 공격으로부터 보호하기 위한 취약점 파악과 대처방안을 권고하는 역할을 지속할 것이다.

2) NCSD의 설립 및 운영

2003년 6월, DHS는 모든 정부 부처의 정보보호 기능을 집중시키기 위해 범국가적 사이버보안 센터인 NCSD(National Cyber Security Division)를 설립하였다. 이 조직은, NSSC에 의거해 설립된 것으로 IAIP의 감독 아래 놓여진다. NCSD는 DHS 창설 당시 DHS로 이관되었던 NIPC, NCS, CIAO, FedCIRC 등의 조직들의 기능을 총괄하고 있으며, 다음의 역할들을 담당하는 3개의 부문으로 나누어져 있다.

- 정부나 민간 부문의 사이버 자산의 취약성 파악 및 대응
- 인터넷상의 사건 검지 및 대응, 잠재적 위협과 취약성 추적, 여러 협력 기관들과의 공조 등의 통합된 기능을 담당하는 CSTARC(Cyber Security Tracking, Analysis, and Response Center)에 대한 감독
- 관련 기관들과 공동으로 사이버보안 경고 발령 및 교육 프로그램 개발

2004년 1월, NCSD는 사이버보안 관련정보 및 경고를 국민에게 제공하는 National Cyber Alert System(이하 NCAS)의 운용을 시작하여, 미국의 일반 시민이나 기업 및 정부조직의 기술자에게 보안 관련문서나, 지침서, 위협에의 대응책 등을 제공하고 있다. NCAS는 컴퓨터의 취약성이나 보안상의 문제에 대해 분석 및 분류를 실시하며, 관리 및 운영은 NCSD와 민간기업의 협력 조직인 US-CERT가 담당하고 있다. NCAS가 제공하는 정보는 △일반 컴퓨터 유저를 대상으로 하는 보안 문제의 대책 정보, △보안 문제, 취약성의 정보, 피해 상황, 리스크 관리 정보, △신속한 대응이 필요한 보안 정보 등이다.

2. 일본의 정보보호 기구 정비

1) 정보보안 대책 추진실

2000년, 내각관방 산하에 설립된 정보보안 대책 추진실은, 관계 각 부처와의 연휴·협력과 동시에 관민의 정보보안 전문가로 구성된 비상근 팀의 조언을 얻으면서, 전자 정부의 정보보

안 확보나 중요한 기반시설에 대한 사이버 테러 대책 등, 관민에 있어서 정보보안 확보를 위한 정책 추진에 몰두하고 있다. 또, 고도 정보통신 네트워크 사회 추진 전략 본부의 하에 설치되고 있는 정보보안 대책추진 회의 및 정보보안 전문 조사회의 사무국을 담당하고, 각 부처와의 종합 조정 등을 행하고 있다.

정보보안 대책 추진실에서는, '해커 대책 등의 기반 정비에 관계된 행동 계획'을 기초로, 주로 두 가지의 정책을 민간 전문가, 기업, 각 정부 부서 등의 협력을 통해 진행해 왔다. 그 중 하나는, 전자 정부 및 자치단체의 보안 확보에 있고, 또 다른 하나는 사이버 테러로부터 금융, 전력, 철도 등 중요한 기반시설을 보호하는 대책이다. 최근, 조사 및 연구 활동으로 보안 강화 소프트웨어의 조사와 오픈 소스 소프트웨어의 평가 연구도 중요한 대상이 되고 있다.

2) 긴급 대응 지원 팀

2002년 3월의 정보보안 대책 추진회의에서의 결정사항으로, 전자 정부나 민간에 중요한 기반시설을 대상으로 하는 사이버 테러 등의 대책 입안에 필요한 조사·조언 등을 행하는 기구의 설립을 결정하였다. 이에 따라, 2002년 4월 내각관방 정보보안 대책 추진실에 '긴급 대응 지원팀(NIRT, National Incident Response Team)'이 설치되었다. 사이버 공격 등에 의한 전자 정부나 민간의 중요한 정보통신 사업자 등의 정보 시스템에 관계된 장애의 발생에 대해 정부차원의 위기 관리 대응이 필요한 사안해지는 사안을 활동 대상으로 삼고 있다. 이를 위해, △사안의 정확한 파악, △피해 확대 방지, 복구, 재발 방지하기 위한 기술적 대응책의 검토, △대책의 실시에 관계된 지원 등의 활동을 담당하고 있다.

3) Telecom-ISAC Japan

'Telecom-ISAC Japan'은 정보통신 사업자들이 제공중인 네트워크와 같은 기반시설의 보호를 위해 전기통신사업자 협회, 일본 인터넷 제공자 협회, 텔레콤 서비스 협회, 전기통신사업자 등이 2002년 7월에 설립한 조직이다. 사업자들이 제공중인 통신 서비스의 보안 수준을 평가하고, 다른 중요한 기반시설에 대한 정보보안 상의 영향이 예상되는 보안 침해 사안에 관한 대처 및 예방조치 등을 상호 연계를 통해 수행하려는 목적을 지니고 있다.

또한, △인터넷 서비스 제공자를 중심으로 하는 네트워크의 각 거점에 보안 정보를 수집하기 위한 기기 배치 △집중 센터에 보안 정보를 신속하게 수집·분석 △각 거점에 있어서 사이버 테러에 의한 오염 상황·피해 상황을 실시간으로 파악 △상호 정보의 공유를 할 수 있는 연구 개발의 기반 정비 등의 역할을 담당하고 있다.

4) 사이버 포스

경찰의 수사는 본래, 사건이 일어나고 나서 수사를 시작하는 사후 수사의 성격이 강하지만, 사이버 테러는 사회에 대한 영향이 크기 때문에, 사전에 전조를 파악해 미리 예방하는 것이 요구됨에 따라, 경찰청은 2001년 4월에, 시스템의 취약성의 검사나 사이버 공격에의 대처 기술의 연구를 담당할 기관으로 사이버 포스(Cyber Force)를 설립하였다. 경찰청의 정보통신 기술자로부터 선발된 60명이, 도쿄도내의 민간 빌딩에 있는 '사이버 포스 센터' 등 전국 57개소의 거점으로부터, 경찰 네트워크에의 해킹 행위를 24시간 체제로 감시하며, 정보통신이나

은행·증권거래소 등 금융 관계, 철도·항공, 전력·가스 등의 사회의 중요 기반시설에 대해서도 방호를 수행하고 있다. 네트워크를 사용한 범죄에 대한 각급 경찰의 수사를 기술 측면에서 지원하는 것도 중요한 임무이다.

사이버 포스는 사이버 공격 또는 그 징조가 파악되면, 대책 요원이 현장에 출동하고 피해 확대의 방지, 범인의 추적 등을 행한다. 또, 광범위하게 수집된 정보로부터 보안에 관한 정보를 제공하고 있다. 또한, 공격 수법에 관한 연구, 사이버 테러의 대책의 연구·개발 등도 수행하고, 향후 점점 고도화한 공격 수법에의 대응책을 준비하고 있다.

IV. 정보보호 기술 연구개발 투자

1. 미국의 정보보호 연구개발 투자 동향

미국 연방 정부의 연구개발 동향을 살펴보면, 연구개발 전략의 구성이 시대와 함께 변화하였고, 필요에 따라서는 국책의 우선순위의 변화를 반영해 왔다는 것을 알 수 있다. 이러한 국가의 우선 과제의 변화는 과학기술 분야의 각 기관에 대한 예산의 증감으로 나타난다. 예산관리국(OMB)에서 발표하는 국방부, 에너지부, 법무부, 보건복지부, 항공우주국 등의 20여 정부 기관들에 할당된 정보기술 분야와 정보기술 보안 분야에서의 지출액 합계를 나타낸 <표 1>을 살펴보면, 9·11 테러 이후 정보기술 보안 분야의 비중이 2.81%에서 5.56% 수준으로 급증하여 정보기술 보안 분야에 적극적으로 투자가 이루어지고 있음을 알 수 있다.

	FY 2001	FY 2002	FY 2003 (예상)	FY 2004 (예상)	FY 2005 (예상)
정보기술	46.1	48.6	52.6	59.3	59.8
정보기술 보안	1.3	2.7	4.2	4.7	N/A
보안 비중	2.81 %	5.56 %	7.98 %	7.93 %	N/A

<표 1> 미국 연방 정부기관의 정보기술 예산 동향

HR 3394의 발표로 인해 미국 정부는 대학들의 보안센터 설립과 연구비 보조를 위해 2003년부터 5년간 약 9억 달러를 지원하게 되었다. HR 3394에 대한 2003~2007년도 예산으로 인가된 액수는 <표 2>와 같다.

프로그램		FY 2003	FY 2004	FY 2005	FY 2006	FY 2007	합계
NSF Research	Computer and Network Security Research	35	40	46	52	60	233
	Computer and Network Security Research Centers	12	24	36	36	36	144
	Computer and Network Security Capacity Building	15	20	20	20	20	95

	Community Colleges	1	1.25	1.25	1.25	1.25	6
	Graduate Traineeships in Computer and Network Security Research	10	20	20	20	20	90
	Cyber Security Faculty Development	5	5	5	5	5	25
NIST	NIST Extramural Research	25	40	55	70	85	275
	Computer Security Review, Public Meetings, and Information	1.06	1.09				2.15
	Intramural Security Research	6.0	6.2	6.4	6.6	6.8	32
	National Academy of Sciences Study on Computer and Network Security in Critical Infrastructures	0.7					0.7
합계		110.8	157.5	189.7	210.9	234.1	902.9

<표 2> HR 3394 관련 예산 동향

이상과 같이, HR 3394의 성립으로 인해 미국은 사이버보안에 관한 연방정부 지출을 기존의 연간 약 6천만 달러 수준으로부터 급격히 증가시켜, 연구개발과 인재육성 부문에 많은 노력을 기울이기 시작하였다.

한편, DHS 및 DHS의 산하 조직인 IAIP와 NCSD의 예산을 살펴보면, DHS의 경우 부처가 설립된 2003년을 기점으로 예산이 급증한 것을 알 수 있다. 증가된 예산은 다른 부처로부터 관련 프로그램의 예산이 이관되기 이전인 2002년에 비해서 80% 가량 증가한 것인데, 이러한 증가의 원인은 DHS 내에 신설된 HSARPA의 예산 배정에서 기인한 것이다.

IAIP의 경우에도, 부문이 설립된 2004년부터 편성된 금액이 급증하였다. IAIP가 설립되어 연방기관을 통한 기반시설 보호 활동을 조정하고, 테러로부터 국가의 기반시설에 대한 취약점을 줄이기 시작한 2004년에는 예산이 전년대비 350% 가량 대폭 증가하였으며, 2005년 예산은 9·11 테러 이전의 7배에 달하는 8억 6천 5백만 달러를 요구하고 있다. 특히, IAIP에 대한 예산 중에서 주요 기반시설을 감정하고 이러한 시설에서의 보안이 향상되는 것을 보장하기 위해 필요한 단계를 지원하는 부분에 5억 달러 이상이 할당되어 있다. IAIP 산하의 NCSD에 대한 재원은 2005년 예산에서 증가하여, 7천 9백 8십만 달러가 요청된 상태이다.

2. 일본의 정보보호 연구개발 투자 동향

부정 접속 기술, 바이러스나 웜 등의 악성코드의 위력, 암호 해독 기술 등은 끊임없이 진화 계속되고 있고, 이를 지키기 위해서는 부단한 연구 개발이 불가결하다. 산업계가 추진하기 어려운 연구나 비용이 큰 연구 등에 대해서는, 국가가 직접·간접적으로 연구 개발을 추진할 필요가 있다. 암호 기술, 정보보안 평가 기술 등의 기반 기술의 개발을 행하고, 국방·치안 관련 기술에 관하여는 지장이 없는 범위 내에서 정부의 기타 기관 또는 민간에도 공개한다는 방침을 가지고 있다. 정보보안과 관련된 기반 기술의 개발을 담당하는 기관으로는 총무성, 경제산업성, 방위청, 경찰청, 문부과학성 등이 있다.

총무성은, 2004년도 예산의 5가지 중점 추진안 중에서 '일본발의 신 IT사회의 구축'을 통

해 정보보호 전략의 종합적 추진을 꾀하고 있다. 이에 신설된 '정보통신 보안 인재육성센터 개설 지원사업' 분야에 2억 4천 엔, '보안 기술기반의 형성' 분야에 38억 1천 엔을 책정하여 연구 개발에 투자하고 있다.

연구 분야	FY 2003	FY 2004
네트워크 보안 기반 기술의 추진 (2001년부터)	26.0	24.7
고도 네트워크 인증 기반 기술에 관한 연구 개발 (2004년부터)	-	10.4
컴퓨터 바이러스 등에 관한 연구 기반의 구축 (2003년부터)	1.8	1.8
타임스탬프 플랫폼 기술의 연구 개발 (2003년부터)	2.7	1.7
합계	30.5	38.1

<표 3> 총무성의 정보보호 분야 연구개발 예산

경제 산업성에서는, 컴퓨터 바이러스나 부정 접속 등에 의해 정보 처리 시스템이 받는 위협의 상황이나 그것에 대한 방어 조치에 관한 기술 개발을 추진해 오고 있으며, 2004년 연구개발예산으로 '정보보호 문제에 대한 대응' 분야에 24.8억 엔의 예산을 배정하였다.

연구 분야	FY 2002	FY 2003	FY 2004
전자정부의 보안기술 개발	10.0	5.0	6.0
정보보안 평가·인증기반 정비사업	2.1	2.3	-
정보보안 대책연구 개발 평가사업	3.5	3.5	5.0
EC기반의 상호운용성에 관한 조사연구	2.7	2.4	1.8
정보보안 매니지먼트 이용 촉진사업	-	0.8	1.5
전자서명·인증제도 이용 촉진사업	0.9	0.8	0.8
부정접속행위 등 대책 업무	1.5	6.5	6.7
전력분야의 사이버 테러 대책 촉진사업	-	-	3.0
합계	20.7	21.3	24.8

<표 4> 경제 산업성의 정보보호 분야 연구개발 예산

방위청에서는, 사이버 공격에 대한 대처 수법의 실증적 연구 및 컴퓨터 시스템 등의 안전성 확립을 위한 운용 지침에 관한 조사 연구를 추진 중이다. 사이버 공격의 위협에 정확하게 대응하기 위해서는 정보 보안의 기반을 정비함과 동시에, 사이버 공격에 대한 방어·대처 능력이나 체제를 확보하는 것이 필요하다. 이 때문에, 정보 보안 방침의 개선, 사이버 공격에 대한 대처 수법의 연구, 보안 시스템의 운용 평가 등의 정책을 진행하고 있다. 경찰청은, 네트워크상의 부정 접속 자동 검지에 관한 조사 연구, 고도의 보전 기술에 대응하는 요소 기술의 연구 등을 실시하고 있다.

V. 결론

인터넷이 경제뿐만 아니라 사회 전반에 필수적인 존재로 자리 잡은 지금, 완전무결한 보

안은 어디에도 존재하지 않게 됐다. 만약 그것을 추구한다면, 외부와의 접속을 차단할 수밖에 없다. 그러나, 다른 네트워크나 시스템과의 접속 없이 기능을 수행할 수 있는 시스템이 경제활동을 발전시키기는 힘들 것이다. 특정 조직의 시스템에 적용하여야 하는 보안 수준은, 외부와의 접속을 단절시키는 최고 수준에서부터 무제한적 접속을 허용하는 최저 수준 사이의 어딘가에 반드시 존재하여야 한다. 보안 수준의 미비로 인해, 2003년 1월, 우리나라를 중심으로 대규모 인터넷 장애가 발생하여 시민 생활에 큰 영향을 주었다. 이 사건은, 다음의 사실들을 명확하게 하고 있다. △현대 사회는 정보통신 네트워크에 크게 의존하고 있고, 이것에 장애가 있으면 큰 사회적 혼란이 발생함, △세계에서 가장 초고속 인터넷이 보급되었던 한국에서의 피해가 가장 컸으며, 정보통신의 진전이 역으로 큰 피해를 가져옴, △이용자가 프로그램 패치를 충실히 하는 것으로 피해를 차단할 수 있었지만, 일반적인 피해자들이 자신이 알지 못하는 사이에 대규모 사고의 가해자가 됨 등이다.

정보통신에 관계된 모든 이들이 정보보호의 필요성과 대응책을 인식할 수 있는 '보안 문화'를 속히 정착시켜야 할 필요가 있다. 보안 수준을 정하는 것은, 이익과 위험성의 트레이드오프라고 생각하는 것이 당연한 만큼, 어디까지 정보보호 분야에 비용을 투자할 것인가에 대한 보다 깊은 고찰이 필요하며, 이러한 비용을 개인과 기업이 부담하기 어려운 경우에는 정책적인 지원을 통해 해결해 나가야 할 것이다.

또한, 정보보호 침해 사례의 원인을 살펴보면 상당 부분이 각 시스템 사용자 또는 운영자의 보안 지식 부족에 따른 정보보호 대책을 실시하지 않음에서 기인함을 알 수 있다. 정보보호 대책을 실시하지 않는 이유에 관하여 정보보호 대책 미실시자의 대다수가 구체적인 대책 방법을 알지 못함을 이유로 들고 있다. 향후, 개인의 정보보호 대책을 진척시켜 나가는 데에, 정보보호에 관한 지식의 향상이 최우선 과제로 되어야 할 것이다. 기업이 강구하고 있는 정보보호 대책 상황으로서는, 정보보호 관련 시스템의 구축이 가장 우선적으로 이루어지고 있다. 그렇지만, 하드웨어나 소프트웨어의 정비와 비교하여, 정보보호를 조직적으로 확보한 데에 필수적인 '사원 교육', '보안 방침의 책정', '보안 감사' 등을 실시하고 있는 기업의 비율은 기업의 규모가 작을수록 잘 이루어지지 못하고 있는 실정이다. 개인과 기업들이 정보보호와 관련된 지식을 갖출 수 있는 체계적인 교육과 홍보가 요구되고 있다.

미국, 일본 등의 선진국의 정보보안 의식이나 정보보안 정책의 수준은, 인터넷 대중화 초기의 정보기술 분야의 발전 추이를 따라가지 못했던 우리나라의 전철을 따르고 있다. 근래 발표된 법률에서는 표현의 모호함으로 인해 해석의 융통성에 따라서 적용 범위가 크게 달라질 수 있으며, 이러한 법률들의 강제성의 부족과 유도 요인의 빈약함으로 인해 실효성에 의문이 제기되고 있는 만큼, 보다 적극적인 법률의 운용과 기술개발의 노력이 필요할 것이다.

참고문헌

[1] The White House, "National Strategy for Homeland Security," 2002. 7.
[2] House Committee on Science, "Summary of H.R. 3394 - The Cyber Security Research and Development Act," 2001

[3] Homeland Protection Institute, "Key CBR Technology-Related Provisions of House Bill HR5005," 2002
[4] The White House, "The National Strategy to Secure Cyberspace," 2003. 2.
[5] National Science and Technology Council, "Supplement to the President's Budget for FY 2002," 2001
[6] National Science and Technology Council, "FY 2003 - Supplement to the President's Budget," 2002. 7.
[7] National Science and Technology Council, "FY 2004 - Supplement to the President's Budget," 2003
[8] GOP.gov, "H.R. 3394 - Cyber Security Research and Development Act," 2002
[9] Office of Management and Budget, "Budget of the United States Government, Fiscal Year 2005," 2004
[10] 총무성, 부정 접속 행위의 금지 등에 관한 법률, 2000년 2월
[11] 총무성, 전자 서명 및 인증 업무에 관한 법률, 2001년 4월
[12] 총무성, 특정 전자 메일의 송신의 적정화 등에 관한 법률, 2002년 4월
[13] 수상관저, 개인정보의 보호에 관한 법률, 2003년 5월
[14] 총무성, 행정기관 등 개인정보 보호법, 2003년 5월
[15] 경제 산업성, 2004년 '정보보안 정부예산안 경제 산업성 개요' 등, 2003년 12월
[16] 내각총리대신, 정보보안 대책 추진실의 설치에 관한 규칙, 2000년 2월