해외 정보보호정책 동향

Information Security Policies of Advanced Countries

박성욱(S.U. Park) 정보기반연구팀 연구원
이현우(H.W. Lee) 정보기반연구팀 책임연구원

컴퓨터 바이러스에 의한 시스템 마비와 해킹을 통한 정보파괴나 도용 등과 같은 직접적인 부작용은 물론 인터넷상의 익명성을 이용한 악의적 정보유포나 개인정보의 유출 등을 포함하는 간접적 피해사례도 급격히 증가하고 있는 추세이다. 이와 같은 정보화 혁명의 부작용은 정보화의 진전에 따라 그 파괴력도 비례적으로 증가하고 있음이 실증적으로 드러나고 있다. 1994년부터 국가적 차원에서 초고속정보통신망 구축을 시작한 이래, 세계적인 인터넷 선도국가로 도약한 우리나라가 1.25 SQL Slammer Worm 대란의 가장 큰 피해국이라는 사실이 단적인 예라고 하겠다. 이에 본 논문에서는 정보보호산업의 선진국인 미국, 유럽, 일본에 대한 정보보호 정책을 살펴봄으로써 향후 우리의 정보보호정책 수립에 도움을 주고자 한다.

I. 서 론

컴퓨팅 기술과 네트워킹 기술의 지속적인 발전은 인터넷의 폭발적인 성장을 가져왔으며 사회전반에 걸친 기반시설 및 공공 인프라, 그리고 산업인프라 및 문화환경을 인터넷기반으로 변화시키는 중요한 역할을 수행해 왔다.

신기술의 도래는 늘 상업적 응용과 함께 범죄에의 악용이라는 예기치 않았던 부작용을 수반했다. 인터넷의 본격적인 활동이 시작된 이후 우리사회에는 새로운 용어(B2B, B2C 등)로 대변되는 변화의 물결이 나타나고 있으며 동시에 해킹(내포적 의미상으로는 크래킹이 적합), 웜 등의 역기능도 함께 나타나고 있다. 즉 오프라인에서나 가능했던 많은 경제활동들이 인터넷상에서 이루어지는 환경에서 2003년 1월 25일 국내에서 발생했던 인터넷침해사고는 우리에게 실로 엄청난 경제적 손실을 안겨준 예라 하겠다.

<표 1>에서처럼 가장 최근의 예를 보아도 인터넷은 정보의 공유나 생산성 향상과 같은 순기능 외에 인터넷대란과 같은 사이버테러나 개인 정보를 악용한 사기, 프라이버시 침해사고와 같은 사이버범죄라는 역기능을 가져 왔다[1]. 이에 대해 신기술에 대한 회의론자들은 목소리를 높여 미래에 대한 불안을 증폭시키고 있다.

따라서 막연한 불안을 해소하는 방안이 필요하다. 이에는 정보보호가 한 몫을 할 것이다. 흔히 정보보호라고 할 때 암호기술, 방화벽과 같은 기술적 측면만이 강조된다. 그러나 진정한 정보보호는 정보환경의 변화와 이에 따른 새로운 수요를 정확히 예측하고 이에 맞춰 법과 제도 등 정책적 해결책과 이를 가

<표 1> 해킹사례와 경향의 변천

	대표적인 해킹사례	해킹의 경향
1980년대	1988년 모리스 웜	개인지식의 과시/실험, 자기복제기술 이용, 컴퓨터의 가용성 파괴
1990년대	1990년 케빈 폴슨의 전화망 해킹 1995년 케빈 미트닉 신용정보 해킹	개인지식의 과시, 경제적 이익, 특정 대상을 향한 해킹
2000년대	스크립트 키드들에 의한 해킹	개인지식의 과시, 경제적 이익, 특정대상을 향한 해킹/게임 사이트, 이웃집 등 자동화된 툴을 이용/취약적 분석 도구 등
2003년	1월 Slammer 웜 8월 MS-Blast 9월 Sobig.F	개인지식의 과시, 불특정 다수를 대상, 자기복제기술, 자동화된 공격대상선정, 해킹+웜의 형태

<자료>: KISA, 정보보호뉴스, 2003. 12.

능하게 하는 기술적 해결책도 함께 추진하는 것이다.

9·11 테러 이후 사이버 보안(cyber security)의 중요성이 부각되면서 주요 선진국에서는 정보보호에 대한 관심이 높아지고 있다. 장기 기술개발계획과 정보보호입법을 통해 국가 인프라 안전확보 차원에서 정보보호기술개발을 추진하고 그에 대한 예산을 늘려가고 있는 실정이다. 이에 본 고에서는 해외에서의 정보보호 대책을 살펴봄으로써 향후 우리의 정보보호대책 수립에 도움을 줄 것이다.

II. 민간 부문에 대한 규제 및 지원

미국 등 주요 선진국은 정보통신기반의 보호를 위해 민간과의 유기적 협력체계의 수립을 확립하고 있고 민·관의 협조적 관계 속에서 자율적 규제를 추진하는 기조이다.

1. ISP

미국은 2002년 소프트웨어 업체, 네트워크 업체, ISP 등이 참여하는 인터넷 보안기구(The Organization for Internet Safety)를 조직하여 네트워크 운용과 소프트웨어의 취약점을 공개하고 이에 공동대처하고 있다[2]. 또한 기반시설 보호와 관련된 정책 이슈들을 논의하기 위해 8개 분야의 60여 개 관련 기업·연합회 및 13개 연방정부가 참여하는 주요기반시설보호 파트너십(Partnership for Critical Infrastructure Security: PCIS)을 구성·운영중에 있다. PCIS는 상무성(DOC) 내의 주요기반보호사무국(Critical Infrastructure Assurance Office: CIAO)과 함께 분야별 주요 기반시설 보호계획을 심의하고 있다[3].

EU 이사회는 바이러스 유포, 시스템 방해, 온라인 사기 등을 범죄행위로 규정하고 ISP 업체의 통신기록 보존·수사협조를 의무화하고 있다.

영국은 2001년 12월 정부와 민간이 참여하는 대규모 보안연합회인 'SAINT'를 결성하여 사이버 범죄에 대한 협조체계를 구축하고 있다. 그리고, 독일은 '정보통신서비스법(IuKDG)을 통해 불법 및 유해정보의 유통에 대해 ISP에 책임을 부여하고 있다[4].

2. 서비스 사업자

미국은 사이버 위협 예방을 위하여 2002년 2월 'NIST Special Publication 800-42'에서 침입심사기법에 대한 가이드라인을 제공하고 있으며, 침입심사를 통해 발견한 취약 사항을 미리 법적으로 명시할 것을 제안했다[5].

일본의 내각관방은 시스템 관리자 배치, 시큐리티 감시 등에 관한 모범사례(best practice)를 제시하고 있으며, 정보보호설비를 도입하는 민간사업자에 대한 세제상의 우대조치를 실시하고 있다[6]. 일본은 정보통신기반의 적정한 이용을 위한 법제를 정비하면서(2002년 11월) 포털사이트 운영자에게 인터넷상의 권리 침해에 대한 방지의무를 부과하고 스팸메일 대량전송에 대한 처벌규정을 신설하였으며, 정보통신업자들은 '정보통신사업운영에 대한 윤리강령'과 'PC 통신서비스이용자규범'이라는 정보통신 윤리강령을 자체적으로 제정했다[7].

3. 일반사용자 및 정보보호산업체

미국은 2002년 9월 발표한 '사이버 공간 보호에 대한 국가전략(The National Strategy to Secure Cyberspace)'의 초안에서 가정 내 이용자와 소규모 기업에 대해 ① 방화벽 소프트웨어를 우선적으로 설치하고 주기적으로 업데이트 할 것, ② 바이러스 백신을 주기적으로 업데이트 할 것, ③ 스팸메일을 차단하는 소프트웨어의 사용을 고려할 것, ④ OS의 보안패치를 주기적으로 업데이트할 것 등을 권고했다[8]. 또한, 미국의 '사이버 공간 보호에 대한 국가전략'은 정보보호산업체에게 보안소프트웨어의 업데이트를 시의적절하게 자동으로 업데이트 해주도록 권고했다.

III. 국가차원의 정보보호 기반 및 모니터링 체계 구축

미국은 국가기반시설보호라는 관점에서 정보통

신 기반시설 보호체계를 수립하고 있으며, EU와 일본도 정보보호 기반 및 모니터링 체계 구축을 중장기 국가과제로 추진하고 있는 실정이다.

1. 미국

2000년 'National Plan for Information System Protection'을 수립하여 사이버 공격에 대한 대응기반 구축을 추진하고 있다. 따라서, 정보통신 인프라의 보호를 대통령의 직접 관할에 두고 있으며, 연방부처 및 기구들에게 정보통신 인프라의 보호의무를 부여하고, 민간부문과의 파트너십 구축을 추진하고 있다. 동 계획에서는 민간자율의 ISAC(Information Sharing and Analytic Center) 구축을 권고하였으며, 이후 7개 분야에서 ISAC이 운영되고 있다[9].

미국은 2003년 3,000만 달러를 투입하여 주요기반시설의 보호를 위한 정보수집 및 조기경보체계 구축을 목적으로 하는 '사이버경보정보망(CWIN)'을 추진했다. 9·11 테러 이후 정보통신망의 보호를 더욱 강화하기 위하여 대통령 행정명령 'Critical Infrastructure Protection in the Information Age'을 통해 '주요기반시설보호위원회(President's Critical Infrastructure Protection Board)'를 신설하여 민간지원, 정보의 공유, 사고협력과 위기대응, 보안전문가 양성, 연구개발, 국가 보안요소에 대한 법 시행 협력, 국제 정보기반시설 보호, 법률, 국가보안사무국과 협력 등의 기능을 수행하며, 사고협력과 위기대응, 정보기반시설 보호, 보안전문가 양성 등 이외에도 정보보호기술의 연구개발을 위해 NSF(National Science Foundation), DARPA(Defese Advanced Research Project Agency) 등과 협조·조율하는 임무를 부여받고 있다[3]. 또한, 미국의 대통령 직속 주요기반시설보호위원회는 2002년 9월 사이버 공간의 안전한 이용을 목표로 하여 '사이버 공간 보호에 대한 국가전략(The National Strategy to Secure Cyberspace)'의 초안을 발표했는데 이 초안의 내용은 연방 및 주 정부, 업계, 학계의 의견수렴을 거쳐 사이버 공간의 인프라를 보호하기 위한 로드맵의 성격이었다. 사이버보안을 위해 인식과 정보(awareness and information), 기술과 도구(technology and tools), 훈련과 교육(training and education), 역할과 협력(roles and partnership), 연방정부 지도력(federal leadership), 조정과 위기관리(coordination and crisis management)의 6가지 도구를 제시하고, 정보보호 기술확보을 위한 단기·중기·장기의 기술개발계획의 수립을 강조하고 있으며, 민간과 정부간·국제간의 공동연구의 필요성을 제기하고 있다[8].

9·11 테러 이후 신설된 국토안보국(Homeland Security Department)은 사이버 공간의 안보를 위해 정보통신 인프라 보호를 위한 포괄적인 명령을 수행할 수 있으며, 산하에 컴퓨터 범죄에 대처하기 위한 기관을 두고 있고, 개인 정보보호 정책을 홍보하는 역할까지도 담당하고 있다. 국토안보국은 연방정부 차원에서의 정보의 분석 및 공유, 주요기반보호의 사령부 역할을 맡게 되는데, 주요 정보통신기반 보호를 위한 실천전략으로서 ① 국가기반보호센터(National Infrastructure Protection Center: NIPC)의 확대·강화, ② 무선망 접근에의 우선권 확보(Priority Wireless Access), ③ 국가기반 시뮬레이션 분석센터의 확대·강화(National Infrastructure Simulation and Analysis Center), ④ 안전한 정부망 연구(Secure 'GovNet' Feasibility Study), ⑤ 고등 암호표준(Advanced Encryption Standard), ⑥ 사이버 정보보호 장학제도(Cybercorps Scholarship for Service) 등을 제시하고 있다[10].

2. EU

EU는 eEurope 2005 프로젝트에서 안전한 정보기반설비 구축을 목표로 기술개발은 6th Framework Programme for Research and Technological Development를 통해 지속하며, 사이버보호대책반(CDTF) 운영, 정보보호문화운동 시행, 공공서비스간 안전한 정보전송 환경조성을 추진한다[11]. 또한, 유럽의회는 네트워크 보안, 개인정보보

호, 해킹·바이러스 경보 시스템 도입, 관련 기술개발, 법제 정비, 국제협력 강화의 추진을 제안했다[12]. EU는 '안전한 인터넷 환경조성을 위한 실행계획(The Safer Internet Action Plan)'을 시행중에 있으며 이 계획에서는 2003년~2004년에 2단계로 비회원국까지 포괄하는 광범위한 협력체제를 운영하면서 ① 불건전정보에 대한 핫라인의 구축, ② 이용자 친화적 등급시스템 구축, ③ 인식제고를 추진중이며, 안전한 웹 서핑기술, 안전한 인터넷 접속기술, 스마트카드를 이용한 접근제어기술, 콘텐츠 필터링 기술 등의 연구개발을 추진하고 있다[13].

3. 일본

일본 정부는 2001년 '사이버테러 대책에 관한 특별행동계획'을 발표하였으며, 제153회 정기국회에서는 사이버테러에 대한 대책으로서 ① 사이버테러 대책의 보완·강화, ② 사이버 공격에 대한 대처 수단 등 연구, ③ 사이버테러 방지를 위한 고성능 네트워크 보안 시스템 정비, ④ 부정 액세스·컴퓨터 바이러스 등에 관한 정보 제공 강화 등을 의결했다. 2001년 긴급 사태에 대응하기 위한 긴급대응지원팀(National Incident Response Team: NIRT) 편성 프로젝트를 발족하였으며, 2002년 긴급대응지원팀을 발족시켰다[14]. 2001년 4월 정보통신국에 기술대책과를 설치하고 경찰청 기술센터를 설치하고 기동적 기술 부서로서 사이버 포스를 창설했는데, 사이버 포스는 24시간 사이버 테러의 조기인지를 통한 긴급대처체계 강화에 주력하고 있으며, 민간의 최첨단 기술의 습득이나 외국 수사기관 등과의 정보교류, 긴급대처 기술의 고도화를 도모하고 있다[15]. 2002년 4월 내각관방 정보보호대책회의에서 정보보호에 대한 근본적인 인식전환이 필요함을 지적하면서, ① 각 정부기관의 정보보호 대응체계 강화, ② 침입감시체계와 복구대책의 정비, ③ 정보보호 예산의 확충, ④ 긴급 대응체계의 강화, ⑤ 관련 법제의 정비, ⑥ 인적·기술적 기반의 정비 등의 정책추진을 결정하였다[16]. 2000년 범정부 차원에서 고도정보통신사회추진본부 산하에 '정보보호대책 추친위원회'를 설치하였으며, 2002년 4월 총리실 산하에 민·관이 함께 참여하는 사이버테러 대책기구'를 구성하였다.

Ⅳ. 정보보호 기반 구축을 위한 투자

9·11 테러 이후 사이버 보안의 중요성이 부각되면서 주요 선진국은 중장기계획과 정보보호입법을 통해 국가 인프라 안전확보 차원에서 정보보호기술 개발과 정보보호 기반 구축을 추진하였다.

1. 미국

미국은 정보통신 주요 기반시설 보호를 위한 중장기 계획으로서 2000년 발표한 'National Plan for Information System Protection'에서 정보통신 기반시설 보호를 위해 장기적 예산지원의 근거를 마련하였다[17]. 미국은 IT 분야의 7가지 주요 기술개발 과제의 하나로서 HCSS(High Confidence Software and Systems) 계획을 추진하고 있다. HCSS 계획은 Reliability, Security, and Safety for Mission-Critical Systems의 구축을 목표로 국가 인프라로서의 네트워크 보호를 위한 기술개발과제를 수행하고 있는데 HCSS 계획에는 2003년 예산으로 1억 2,800만 달러가 요청되었다[18].

미국의 정보보호기술개발은 NITRD에서 관장하는 일반 정보통신기술개발 외에, 국가안보기술개발의 일환으로서 DARPA에서 추진되고 있으며, 9·11 테러 이후 국토 안보 차원에서 별도의 예산이 할당되어 있는 실정이다.

<표 2>에서 처럼 미국의 DARPA는 Information

<표 2> Information Assurance and Survivability 예산 배정 (단위: 백만 달러)

	2001	2002	2003	2004	2005	2006	2007	합계
예산	70.908	77.738	51	65.555	86.183	100.82	105.537	557.741

<자료>: DARPA, Fiscal Year 2003 Budget Estimates, 2002. 2.[19]

<표 3> Cyber Security R&D Act에 의한 예산배정

(단위: 백만 달러)

	2003	2004	2005	2006	2007	합계
NSF	73.0	105.25	123.25	129.25	137.25	568
NIST	32.06	47.29	61.40	76.60	94.80	312.15
합계	105.06	152.54	184.65	205.82	232.05	880.15

<자료>: American Association for the Advancement of Science, R&D Funding, 2002.[20]

Assurance and Survivability 계획에 2001년부터 2007년까지 총 5억 557.7만 달러의 예산을 배정하였다. 동 계획은 시스템·네트워크의 신뢰성을 보장하기 위한 기술개발계획으로서, Intrusion Tolerant System, Fault Tolerant Network, Fundamentals of Computer Network Defense, High Assurance Trusted System, 상호간 안전한 인증을 위한 Dynamic Coalition 등의 정보보호 기술개발을 연구과제로 하고 있다.

9·11 테러 이후 <표 3>과 같이 Cyber Security Research and Development Act(2001. 12.)에 의해 별도의 네트워크 정보보호 기술개발 및 정보보호 교육 예산을 할당하고 있는데 Cyber Security Research and Development Act에 의해 NSF와 NIST(National Institute of Standards and Technology)에 5년간 총 8억 8천만 달러의 예산이 배정되어 있다.

9·11 테러 이후 국토안보법은 신설된 국토안보국의 ① 사이버 공간 감시, ② 컴퓨터 범죄 수사, ③ 네트워크 보안을 위한 정보센터 설립, ④ 국가안보 관련 정보보호를 위해 연간 5억 달러의 예산을 배정하고 있다[10].

2. EU

EU는 <표 4>에서 처럼 제5차 R&D 프로그램(1998~2002)에 의해 IT 분야에 총 36억 유로를 투자하고 있으며 시스템 및 네트워크 보호가 주요 기술개발 내용으로 포함되어 있는 "New methods of work and electronic commerce" 부문에 전체의 15%인 5억 4천만 유로를 투자하고 있다.

<표 4> 유럽연합의 정보보호 관련 연구개발 예산

(단위: 백만 유로)

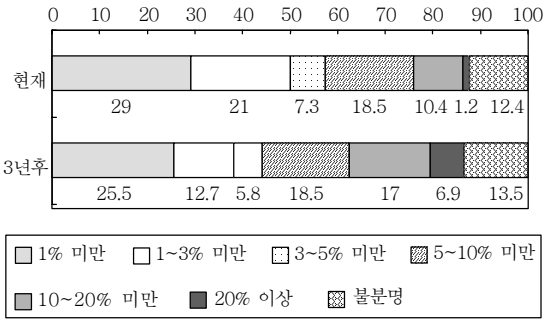
연구분야	투자액	비율(%)
Systems and services for the citizen	646	18
New methods of work and electronic commerce	547	15
Multimedia content and tools	564	16
Essential technologies and infrastructures	1,363	38
Future and emerging technologies	319	9
Research networking	161	4
합계	3,600	100

<자료>: European Parliament, The Fifth Framework Programme for Research and Technological Development, 2002.[21]

EU의 제6차 R&D 프로그램(2002~2006)에서는 Information Society Technology 개발 계획에 36억 2천 5백만 유로를 배정하고 있는데, 동 계획은 4가지의 주요 과제 중 정보보호 기술개발을 최우선으로 제시하고 있다[22].

3. 일본

일본 (社)정보서비스산업협회[23]에 의하면 (그림 1)에서 처럼 정보보호 확보를 위한 예산이 정보처리 관계 모든 경비가 차지하는 비율은 「1% 미만」이라는 회답이 현재와 3년 후 모두 최대 다수이다. 단,



<자료>: (주) 정보서비스산업협회, 정보시스템화와 미래 동향 조사 (대기업: 정보시스템부문편), 2001.[24]

(그림 1) 정보처리 관계 제경비에서 정보보호 예산이 차지하는 비율

<표 5> 2002년과 2003년 일본 IT 예산의 비교

(단위: 억 엔)

분 류	2003년	2002년
1. 세계 최고수준의 고도정보통신네트워크 형성 촉진	2,220	2,278
2. 교육 및 학습의 진흥과 인재육성	1,125	1,173
3. 전자상거래 등의 촉진	67	96
4. 행정의 정보화	5,759	5,372
5. 공공분야의 정보통신기술 활용	3,286	3,523
6. 고도정보통신네트워크의 안전성 확보 등	264	249
7. 연구개발의 추진	1,990	2,028
8. 국제적인 협조 및 공헌	29	30
9. 기타	618	1,013
총 액	15,358	15,762

<자료>: 일본 IT 전략본부, 2003년 일본 IT 예산, 2003.[25]

5% 미만의 합계는 현재부터 3년간 13.5포인트 감소하고「10~20%」「20% 이상」의 합계가 현재부터 3년간 12.3포인트 증가한다.

일본은 e-Japan 중점계획에서 중점정책 분야의 하나로서 '고도정보통신네트워크의 안전성 및 신뢰성 확보'를 제시하고 있다. <표 5>에서 처럼 '고도정보통신네트워크의 안전성 및 신뢰성 확보' 계획에는 2002년 249억 엔의 예산이 배정되었으며 2003년 264억 엔의 예산이 배정되어 있다[25].

일본의 2003년 IT 예산은 2002년 대비 2.6% 감소했으나, '고도정보통신네트워크의 안전성 및 신뢰성 확보' 계획의 예산은 6% 증가하였다. 2003년 IT 예산 세부내역은 <표 6>과 같다.

<표 6> 2003년 IT 예산 세부내역

(단위: 천 엔)

분류	고도정보통신 네트워크형성	교육, 학습진흥, 인재육성	전자상거래 등의 촉진	행정의 정보화	공공분야의 IT 기술 활용	정보통신 네트워크 안전성 확보 등	연구개발의 추진	국제적인 협조 및 공헌	기타	합계
내각관방				254,971	65,215,761	1,504,743			114	66,975,589
내각법제국						43,794				43,794
내각부			150,625	5,454,911	2,857,743	69,790	421,076		9,345,321	18,299,466
궁내청				436,562						436,562
경찰청				12,427,989	17,762,387	1,277,428	9,739		5,469	31,483,012
방위청				137,211,774		20,566,558				157,778,332
금융청				2,050,998						2,050,998
총무성	23,971,997	597,161	1,904,268	26,635,932	14,811,795	636,262	60,370,368	1,324,356	1,929,615	132,181,754
공해조정 위원회				22,050						22,050
공정거래 위원회			9,631	258,718						268,349
법무성				80,020,384		14,884			31,367	80,066,635
외무성		61,296		23,295,993	85,047	63,419		4,188	1,904	23,511,847
재무성	1,022,524			107,919,962				1,159,000	880	110,102,366
문부과학성		102,290,657	95,754	5,039,636	1,853,722		98,481,273	130,000	3,850	207,894,892
후생노동성		7,014,413		96,230,595	111,745,280			61,089	45,541,075	260,592,452
농림수산성	3,749,732	838,549	1,315,778	12,132,196	6,802,605		2,491,656	9,198	261,556	27,601,270
경제산업성		1,626,215	3,227,879	46,217,341	5,481,872	2,207,477	34,612,093		4,506,958	97,879,835
국토교통성	193,221,560			19,041,493	100,413,284	4,990	2,604,661	239,511	146,308	315,671,807
환경성		86,172		1,275,213	1,586,153					2,947,538
합계	221,965,813	112,514,463	6,703,935	575,926,718	328,615,649	26,389,345	198,990,866	2,927,342	61,774,417	1,535,808,548

<자료>: 일본 IT 전략본부, 2003년 일본 IT 예산, 2003.[25]

V. 정보유통 참여자에 관한 정보보호 정책

주요 선진국은 정보유통의 전과정에서 정보보호를 도모하고 있다. 특히, 정보보호 가이드라인의 제시와 정보보호교육을 통한 정보보호의식의 고양을 중시, OECD도 정보보호 가이드 라인을 지속적으로 개정하고 있다.

미국은 정부 주도의 '주요시설 보호계획'에서 10개 부문의 주요 정보통신 인프라 보호 프로그램 중 2개 부문을 교육과 정보보호 인식환산에 관한 프로그램으로 설정하고 있으며, CyberCitizen 프로그램을 통해 초·중·고생을 대상으로 정보보호 윤리 및 통신망의 올바른 사용교육을 실시하고 있다. 또한, CITE(Centers for Information Technology Excellence) 프로그램을 통해 공무원들을 대상으로 업무수행에 필요한 지식과 정보보호의 필요성을 지속적으로 교육하고 있으며 SafeGuide를 활용하여 민간과 유기적인 연합을 통해 국가 중요시설에 대한 정보보호의 중요성을 확산시키고 있다[3].

EU는 '개인정보의 자유로운 유통에 관한 개인정보지침'을 채택하고 회원국에의 이행요구 및 역외국가에 대한 상호주의를 요구하여 협상이 진행되었다. 2000년 7월 EU와 미국, 헝가리, 스위스가 협의를 완료하였고, 2002년부터 캐나다, 호주 등이 EU와 협의했다[4].

일본은 2000년 7월 정보보호 정책에 관한 가이드라인을 책정하였는데, 동 가이드라인은 ① 정보보호정책의 책정·도입·운용·평가를 반복함으로써 높은 보안수준을 실현할 것, ② 긴급대처 및 연구개발에 관련한 민·관의 협력체계를 강화할 것, ③ 물리적 보안·인적 보안·기술적 보안·시스템 운용의 종합적 관점에서 정보보호를 확보할 것 등의 지침을 제시했다[15]. 일본의 2001년 정보보호현황 보고서는 <표 7>에서 처럼 경영자, 시스템 관리자, 최종 이용자의 각각에 대한 정보보호대책 가이드라인을 제시하고 있다.

또한 일본은 민간부문의 정보보호 대책을 향상시키기 위해 <표 8>에서 처럼 경찰청, 총무성 등이 분담하여 정보보호대책을 지원하고 있다.

<표 7> 일본의 정보보호대책 가이드라인

구분	정보보호대책 가이드라인
경영자	• 회사 전반의 정보보호 보안레벨을 균등화하는 통일적인 정보보호 정책을 실시할 것 • 완벽한 정보보호는 사실상 불가능하므로 정보보호와 관련한 포트폴리오를 작성할 것
시스템 관리자	• 시스템 관리자는 서버를 요새화 하여야 하며, 이용자 인증, 방화벽, 암호화, IDS, 바이러스 대책 툴 등을 이용하여 인트라넷을 보호할 것 • 시스템 자산에 관한 정보를 일원화하고, 정기적으로 이용자의 이용현황을 점검할 것 • 수시로 보안정책을 수집하고, 부정접속을 감시할 것 • 최종이용자의 정보보호 교육을 도모할 것
최종 이용자	• 클라이언트 단의 정보보호 솔루션을 사용할 것 • 비상 시에 대비해 파일을 백업하며, ID/패스워드 관리에 유의할 것 • 긴급상황 시의 대처요령을 숙지할 것

<자료>: 일본 IT 전략본부, 일본 제7차 IT 전략본부회의, 2001. 10. 10.[14]

<표 8> 일본의 민간에 대한 정보보호 지원

내용	지원 기관
정보보호의식 고양	경찰청
산업계와의 연대강화	경찰청, 총무성, 경제산업성
신뢰성 향상시설 등의 도입 지원	총무성
네트워크 정보보호 평가방법 확립	총무성
전기통신사업 정보보호대책 인정	총무성
부정접속·바이러스 대책에 관한 정보제공	경찰청
정보보호관리 규격 보급계발	경제산업성

<자료>: 총무성, e-Japan 중점계획, 2002.[26]

OECD는 정보통신인프라에 대한 위협에 대처하기 위한 '정보시스템과 네트워크의 보호를 위한 가이드라인(OECD Guidelines for the Security of Information Systems and Networks)'을 이사회 권고로 채택하고 있다. 동 가이드라인에서는 정보통신인프라에 관여하는 모든 참여자에게 정보시스템과 네트워크를 보호하는 수단으로서 9개의 정보보호원칙(① Awareness, ② Responsibility, ③ Response, ④ Ethics, ⑤ Democracy, ⑥ Risk assessment, ⑦ Security design and implementation, ⑧ Security management, ⑨ Reassessment)을 제시하고 있다[23]. OECD는 2002년 7월

<표 9> WPISP의 정보보호문화 이행방안

구분	정보보호문화 이행방안
정부	• 각종 교육·훈련·캠페인을 통해 정보보호문화를 장려 • 각 분야의 성공사례를 공공교육 프로그램, 웹페이지, 기타 기술교육을 통해 홍보 • 정보시스템과 네트워크에 대한 정책에 OECD의 정보보호 가이드라인 포함, 새로운 정책 수립
기업	• 제품과 서비스의 안전성 보장 • 새로운 디자인이나 시스템 개발시 다른 요소보다 보안을 중시 • 사용자가 제품이나 서비스의 보안기능에 대해 충분히 이해할 수 있도록 정보 제공
사용자	• 잠재적 보안위험에 대해 인지하고 가능한 한 시스템의 안전장치를 점검 및 유지/보수

개정한 정보보호 가이드라인의 효과적인 이행 및 확산을 위해 개인·기업·정부 등이 자신의 역할에 맞는 정보보호 책임을 이행하는 정보보호문화운동을 전개하고 있으며, OECD 정보보호작업반(WPISP)은 2002년 10월 22~23일 파리회의에서 구체적인 이행방안을 마련하고 이를 정보통신정책위원회(ICCP)에 제출하였다. WPISP가 마련한 정보보호문화 이행방안은 크게 정부와 기업, 사용자, 기타 영역으로 구분되어 있다.

WPISP는 <표 9>에서 처럼 정부·기업 모두에게 ① 정보보안 영역의 연구개발(R&D)을 장려하며, ② 정보시스템과 네트워크 보안에 대한 실제적인 정보를 알리기 위한 정보수집 및 출판 등의 노력을 경주하고, ③ 위협과 취약성을 경고하고 적절한 대응법을 조언하기 위해 연락처와 정보를 공유할 것을 권고하고 있다[23].

VI. 결 론

기술선진국들 대부분은 정보보호기술 전반에 걸쳐 고르게 개발이 이루어지고 있으며, 사이버공격으로 인한 정보통신 인프라의 중요성이 부각되고 있어 네트워크 보안기술 및 정보침해 대응기술 분야에 대한 집중적인 기술개발이 추진되고 있다. 이렇게 미국, 유럽, 일본의 정보보호 대책에 대해 살펴보았는데 우리에게 주는 시사점은 다음과 같다.

첫째, 국내에서도 정보화와 정보보호의 균형발전을 추진하여 세계 최고수준의 정보화에 부합하는 세계 최고수준의 정보보호체제를 구축하여 안심하고 인터넷을 활용할 수 있는 환경을 조성해야 한다.

둘째, 사회 각 주체들이 정보보호의 중요성을 올바르게 인식하고 상호협력을 통해 자신의 역할에 맞는 정보보호를 실천하는 정보보호 문화(culture of security)의 정착을 추진해야 할 것이다.

셋째, 해킹·바이러스 등의 사이버공격으로 정보통신 인프라가 마비될 수 있음을 인식하여 국가정보인프라의 신뢰성 보장기술과 개인정보보호를 위한 정보침해 대응기술 개발에 대한 정책적인 지원이 이루어져야 할 것이다.

넷째, 가장 중요한 정보보호 예산의 확충이 필요하다. 국내의 경우 정보통신부의 2003년 예산 중 정보보호와 직결된 정보화 역기능 방지 대책부문의 예산은 2002년의 257억 8,700만 원보다 12.7% 증가한 292억 6,200만 원이다. 또한 정보보호산업 국제경쟁력 강화부문 예산은 정보보호제품 표준적합 및 상호운용성 시험평가환경 구축 2억 1,900만 원, 정보보호 기반기술체계 구축에 1억 3,400만 원, 정보보호산업지원센터 예산 중 산업체 마케팅 지원항목으로 3억 원이 책정되어 정보화 역기능만 치중하고 정보보호산업 육성 및 지원부문은 상대적으로 등한시되어 있다. 그리고 정보보호에 대한 투자는 초고속인터넷 인프라 1위 국가와는 대조적으로 저조한 실정이다. 1995년부터 2000년까지 초고속통신망 구축을 위한 1·2단계 사업에 민간과 정부자금 등 11조 7,500억 원 투자, 2001년부터 2005년까지 19조 8,600억 원을 투자했고 초고속통신망 구축을 위해 투자한 액수가 총 30조 원에 이른다. 하지만 정보보호투자는 2002년 전체 정보화예산 편성 중 5.2%로 주요 선진국 평균 15%대에 비해 1/3에 불과하다.

참 고 문 헌

[1] KISA, 정보보호뉴스, 2003. 12.
[2] http:///www.vnunet.com
[3] President's Critical Infrastructure Protection Board,

'Critical Infrastructure Protection in the Information Age,' 2001. 10. 16.
[4] 정보통신부, 중장기 정보보호 기본계획, 2002. 8.
[5] NIST Special Publication 800-42, 2002. 2.
[6] 총무성, e-Japan 중점계획, 2001. 8.
[7] 일본 IT 전략본부, 제15차 일본 IT 전략본부회의, 2002. 11. 7.
[8] The White House, The National Strategy to Secure Cyberspace, 2002. 9.
[9] The White House, National Plan for Information System Protection, 2000.
[10] http://www.whitehouse.gov/homeland /
[11] http://europa.eu.int
[12] Network and Information Security; Proposals for a European Policy Approach, European Parliament
[13] http://europa.eu.int/ISPO/iap /
[14] 일본 IT 전략본부, 일본 제7차 IT전략본부회의, 2001. 10. 10.
[15] 일본 정보처리 진흥협회, 2001 정보보호현황, 2002.
[16] 내각관방 정보보호대책추진실, 2002. 4. 9.
[17] The White House, National Plan for Information System Protection, 2002.
[18] NITRD, Supplement to the President's Budget; Strengthening National, Homeland, and Economic Security, 2002.
[19] DARPA, Fiscal Year 2003 Budget Estimates, 2002. 2.
[20] American Association for the Advancement of Science, R&D Funding, 2002.
[21] European Parliament, The Fifth Framework Programme for Research and Technological Development, 2002.
[22] European Parliament, The Sixth Framework Programme for Research and Technological Development, 2003.
[23] (주)정보서비스산업협회, 정보시스템화 현황과 미래동향 조사(대기업: 경영기획부문편), 2001.
[24] KISA, 정보시스템과 네트워크의 보호를 위한 OECD 가이드라인: 정보보호 문화를 향하여의 이행계획, 2003. 5. 26.
[25] 일본 IT 전략본부, '2003년 일본 IT 예산,' 2003.
[26] 총무성, e-Japan 중점계획-2002, 2002. 5.