초고속 정보통신기반 안전성 정책 연구

"정상곤*, 이성우*, 신재호*, 박진섭**, 이민섭***, 송영기****, 인소란****
* 동국대학교 전자공학과 ** 대전대학교 컴퓨터공학과
*** 단국대학교 수학과 **** 한국전자통신연구원 소프트웨어 연구부

A Study on the Security Policy for Information Infrastructure

Sanggon Jung*, Sungwoo Lee*, Jaeho Shin*, Jinsub Park**,
Min-surp Rhee***, Young-kee Song****, So-ran Ine****
* Dongguk Univ. ** Taejon Univ. *** Dankook Univ. **** ETRI

본 연구는 한국전자통신연구원 "초고속정보통신기반 안전성 기술개발" 과제로서 수행중입니다.

요 약

정보사회로의 촉진을 유도하기 위한 초고속 정보통신기반 구축은 다양한 서비스 출현을 예상할 수 있게 하면서 이에 따른 위협요소 및 정보 범죄도 반드시 나타나리라 판단된다. 따라서 안전성 확보를 위한 종합적인 정책 수립이 요구되고 있다. 본 논문에서는 정보보호 위협요소와 정보범죄 실태를 살펴보고, 정보보호 정책 수립 지침을 고찰하면서, 국가적으로 정보보호 정착을 위한 정책 방향을 제시 한다.

Ⅰ. 서 론

인간사회는 농경사회에서 산업사회를 거쳐 정보사회로 발전하는 전환기에 놓여 있다. 농경사회에서는 토지와 노동이, 산업사회에서는 에너지와 자본이 핵심적인 사회구성요소였지만, 이제는 정보와 지식이 사회활동을 좌우하는 핵심요소로 등장하고 있다. 따라서 세계는 지금 정보와 지식의 활용을 최대한 촉진하기 위하여 정치·경제·사회·문화의 전영역에 걸쳐 근본적인 구조혁신을 시도하고 있다.

통신기술과 컴퓨터기술의 급속한 발전이 정보사회로의 촉진을 유도하면서, 초고속 정보통신기반의 시급한 구축을 요구하고 있다. 초고속 정보통신망이란 디지털 정보를 언제, 어디서나 누구든지 저렴한 가격으로 정보를 전송하거나 다양한 정보에 접근하여 이용할 수 있도록 해주는 하나의 거대한 시스템을 말하며, 고속 통신망, 방대한 데이터베이스, 고성능 컴퓨터들로 구성된다.

초고속 정보통신기반은 고도 정보사회에 있어서 국가의 경쟁력과 국민의 생활수준에 결정적인 영향을 미치는 새로운 개념의 사회간접자본으로서, 이를 조기에 고도화하는 것이 국가적 과제로 대두되고 있다. 즉, 정부나 민간사용자에게 교육과 고용기회의 강화, 생산성의 증대, 시민참여의 확대, 정부서비스의 개선과 같은 거대한 경제적, 사회적, 문화적 이익의 확산을 가능케 함으로써 궁극적으로는 국가 경쟁력을 강화하고 국민의 삶의 질을 높이는 순기능적 역할이 있다.

그러나 정보통신망을 통하여 전송된 개인정보가 부적절한 목적 또는 부당한 방법으로 사용될 위험, 다시 말해서 범죄적, 사회적, 문화적, 윤리적 측면의 역기능이 초고속 정보통신기반의 구축과 발전에 장애요인이 되고 있다.

미국에서는 NII의 성공적인 구축을 위하여 NII Security Issue Forum을 통해 안전성 확보를 추구하고 있으며, 유럽의 OECD에서도 시스템 안전성을 위한 기본 원칙 등을 제정하고 있다. 일본에서는 통산산업성이 주축이 되어 국가 정보화를 위한 정책, 법규 등을 책정하여 국가 정보화를 추진하고 있다.[7]

작금 정보통신기반 구축을 둘러싼 법적·제도적 여건은 과거보다 개선되었으며, 정보사회를 열어가기 위한 필요조건도 외견상 충분하게 갖추어져 있다. 그러나 결정된 정책이 효율적이며 성공적으로 집행될

수 있을 것인가는 또 다른 문제로 대두되고 있다.

본 논문에서는 초고속 정보통신기반에서의 정보보호 개념을 살펴보고, 정보보호를 위협하는 요인과 정보범죄의 유형을 고찰하며, 정보보호 정책개발 지침에 대해 서술한다. 그리고 정보화 사회에서 정보보호 정착을 위한 국가적 정책방향을 정리하고자 한다.

Ⅱ. 초고속 정보통신 기반에서의 정보보호

정보화 촉진기본법 제2조 제1호에 "정보라 함은 특정한 목적을 위하여 광 또는 전자적 방식으로 처리하여 부호, 문자, 음성, 음향 및 영상 등으로 표현한 모든 종류의 자료 또는 지식"이라고 정의하고 있는 것처럼 정보화 사회에서는 단순한 자료(data)와 정보(information), 지식(knowledge)사이의 개념이 불분명하다.

21세기 정보화된 지적사회의 구축을 목적으로 사람들이 초고속 정보통신망을 적극 활용하고 정보의 자유로운 유통과 공유의 혜택을 최대한으로 향유하기 위해서는 사생활(privacy)에 대한 불안이나 전자정보의 안전성, 신뢰성에 대한 불안을 제거해야 한다. 그리고 초고속 정보통신기반의 발전을 위하여 정부나 민간부문은 초고속 정보통신망 사용을 적극 유도, 장려함과 동시에, 개인들의 사생활보호와 정당한 이익들을 보호해 주는 안전장치를 확보해야 한다. 더욱이 정보고속도로를 구축하는 세계적인 추세에 통신망의 지능화, 고속화, 광대역화, 대규모화, 개방화와 유선망, 이동망, 위성망, 방송망등 개별망들의 통합화를 바탕으로 하는 초고속 정보통신망에서 정보의 유실, 파괴, 변조에 따른 각종 안전사고와 시스템의 신뢰성에 대한 문제는 향후 초고속 정보통신기반의 발전에 큰 영향을 주게 될 것이 분명하다.

급속한 정보화의 진전과 함께 정치·경제·사회·문화의 전 영역이 점차 정보시스템에 의존하게 되고, 그 결과 정보시스템의 기능이 정지하거나 불완전하게 되면, 경제활동은 말할 것도 없이 국민생활 전반에 심각한 영향을 끼치게 된다. 이 때문에 정보화 사회가 원활히 기능해 가기 위해서는 정보통신기반에 대한 안전(safety)대책도 충분히 실시되어야 한다.

초고속 정보통신기반에서의 정보보호란 초고속 정보통신기반 구축을 위한 환경정비의 일환으로서, 정보가 내부 또는 외부침입자에 의해 우연 또는 고의에 의해 유출, 변조, 파괴되는 것을 막고, 시스템이 일정 품질이상으로 수준을 유지하면서 지속적으로 수행되어, 정보와 통신서비스를 언제든지 이용할 수 있도록 하며, 정보가 정해진 절차에 의해 그리고 적법한 사람에게만 접속되어 변경될 수 있고, 정보주체가 원하는 대로 비밀을 유지할 수 있게 하는 것을 의미하는 것으로 무결성, 기밀성, 신뢰성, 가용성을 보장 또는 유지하는 것을 말한다. 그리고 권한이 주어진 사용자에게는 정보서비스가 거부되어서도 안되며, 정보변경에 대한 통제, 오류, 태만의 예방도 포함되어야 한다. 그러나 기밀성과 가용성은 상호 배타적인 요소이므로 적절한 균형을 이루어야 한다. 결국 기밀성과 무결성을 보장하면서 가용성을 극대화하도록 대책이 수립되어야 한다. 이러한 정보보호 목표달성을 위한 대책을 분류해 보면 법적·제도적 보안대책, 관리적 보안대책, 기술적 보안대책, 물리적 보안대책 등으로 나눌 수 있다.

Ⅲ. 위협요소와 정보범죄

초고속 정보통신기반에서 예상되는 정보보호 위협요소는 정보통신환경 변화로 더욱 다양해질 것이고, 그 취약성 또한 증대되어, 이에 따른 정보보호 서비스가 더욱 강화되어야 한다.

정보보호를 위협하는 요인은 크게 두가지로 볼 수 있는데, 정보 및 시스템의 노출과 부정한 접속에 따른 인위적인 것과 자연재해에 의한 자연적인 것이 있으며, 인위적 위협에 해킹이나 컴퓨터 바이러스와 같은 공격적 수법과 사생활 침해, 저작권 침해와 같은 불법이용이 포함되고, 자연적 위협에 운영미숙, 고장, 관리소홀, 부실시공과 같은 고장사고와 지진, 홍수, 화재등과 같은 자연재해가 포함된다. 이렇게 정보보

호를 위협하는 요인이 정보범죄형태로 나타나고 있으며, 그 실태를 살펴보면 다음과 같다.[9]

1) 컴퓨터 조작 사기 : 정보통신망을 통해 불법 접근하여 상업, 금융자료의 조작, 프로그램조작을 자행하여, 상업, 금융관련 위조, 조작사건들이 발생한다.
2) 소프트웨어 불법 복제 : 컴퓨터 프로그램 저작권에 대해서도 지적 소유권을 인정하고 불법복제를 금지하고 있으나, 프로그램의 불법복제의 용이성과 복제행위의 적발 곤란성 때문에 근절되지 않고 있다.
3) 컴퓨터 스파이 : 자료유출이나 도청 등의 컴퓨터 스파이가 기업이나 국가의 비밀을 유출시킴으로써 손해를 입히고 있다.
4) 사생활 침해 : 은행, 신용카드회사, 병원, 학교, 행정당국, 세무당국, 수사기관등의 전산망에 수록된 개인신상에 관한 자료들이 인권보호와 관련하여 중요한 의미를 갖고 있으나, 자료의 유출, 오용, 남용으로 인한 피해가 일어나고 있다.
5) 국가적, 사회적 위기조장 : 홍수 통제, 비행관제, 핵시설 통제, 교통 통제, 전력배송 통제, 전화등 통신운용 통제, 무기관리 통제 등에 대한 침입행위는 국가적, 사회적 위기를 조장하고 특별한 경우 전쟁발발의 원인이 될 가능성도 있다.
6) 전통 범죄에의 악용 : 음란물 판매, 마약거래 및 결제, 자금세탁, 도박, 조세포탈, 각종 위·변조, 명예훼손, 물품 판매가장 사기행위 등의 전통적 범죄를 컴퓨터를 이용하여 자행하는 행위가 발생하고 있다.

이러한 정보범죄는 컴퓨터 범죄의 대표적인 범행수법으로 컴퓨터 해킹(hacking), 컴퓨터통신과 전화에 대한 도청, 전화시스템의 교란과 도용, 암호해독, 컴퓨터 바이러스 등이 있으며, 이런 것들의 단독 또는 결합된 형태로 범행이 이루어진다.

암호는 원래 국가 비밀을 보호할 목적으로 군사, 외교분야에서 사용되기 시작하였지만, 금융기관에서 전자자료 이동에 널리 사용되면서 경제, 금융분야에서 확고한 자리를 잡은 이래, 통신시스템, 특정 보안시설, 중요한 비밀장치등에 대한 사용, 또는 출입이 승인된 사람을 확인하기 위한 동일성의 인증(authentication), 암호화 키에 대한 관리(key management), 디지털 서명(digital signature), 신원확인(identity verification) 등에 널리 이용된다. 특히 컴퓨터 통신에 대한 도청기술이 급속히 발전함에 따라 개인이나 기업들에게는 개인사생활 보호나 산업비밀을 지키기 위한 암호화의 필요성이 높아지면서 암호화 기법은 사회 전영역에서 다양하게 이용된다. 그러나 범죄집단에서도 그들의 통신에 암호를 사용함으로써 범인 검거나 증거 채취에 어려움이 가중되어 공공의 안녕과 사회질서유지의 위협대상으로 등장하였다.

암호해독이라 함은 해독행위자가 암호문만을 가지고 평문에 대한 해독을 감행하는 방법이 아니라, 평문의 암호화에 사용된 알고리즘의 종류, 사용된 운영체제등 시스템에 대한 모든 정보를 알고 있는 상태이면서 암호화에 사용된 키(key)만 모르는 경우에 그 키를 찾아내어 암호문을 평문으로 해독하려는 행위를 지칭한다.

컴퓨터 해킹이란 컴퓨터를 이용하여 타인의 컴퓨터 통신망에 침입하거나 기술적인 방법으로 타인의 컴퓨터가 수행하고 있는 기능이나 전자 정보에 함부로 간섭하는 일체의 행위를 가리킨다.

폰 프리킹(phone phreaking)은 교환기가 전자식으로 교체되면서 UNIX운영체제를 이용하게 되자 컴퓨터 해킹을 통하여 전화망을 교란하거나 요금계산에 관한 기본원리를 악용하여 전화를 도용하는 행위를 가리킨다.

도청이란 다른 사람의 통신에 간섭하여 통신중에 있는 정보의 내용을 함부로 수신하는 행위를 가리키며, 컴퓨터 통신에 대한 도청은 컴퓨터를 연결하는 케이블 또는 무선전송로에 대한 간섭으로 이루어진다.

컴퓨터 바이러스란 다른 컴퓨터 프로그램 또는 사용자가 실행할 수 있는 전자기록의 집합, 예컨데 오버레이 파일(overlay file), 장치구동기(device driver), 운영체제(OS), 부팅에 필요한 기록(Boot record)등

에다 자신 또는 그 변형을 복제하도록 고의로 제작된 프로그램의 일종이다.

Ⅳ. 정보보호 정책 개발 지침

1. 정보보호 정책의 개념[10]

정보보호정책이란 정보보호행위의 기본 구성요소로서, 어떤 조직이 정보보호를 위해 어떻게 수행해야 하는지를 나타내는 관리지령이며, 전형적으로 목표, 목적, 의무, 책임 등의 일반사항을 포함하고, 이러한 것들을 취하는 일반적 방법, 즉 절차를 수반한다.

정책, 지침, 표준은 대상자들이 반드시 따라야 할 길잡이이며, 조직의 구성이나 주위상황, 기술발전에 따라 수시로 재검토하고, 개정, 확장, 대체되어야 하는 것들이다. 정책은 일반적 사항을 서술한 일종의 명령으로서, 각 항목이 "하지 않으면 안된다"로 표현되어 대상자들의 의사결정지표가 되며, 여기에 반하는 행위를 취해야 할 경우는 특별한 승인이 요구된다. 지침은 선택사항이거나 권고사항으로서, 각 항목이 "해야 한다"로 표현된다. 표준은 기술, 방법론, 구현과정 및 기타 세세한 요소들을 상세히 언급한다. 그렇기 때문에 표준은 수년 이내에 자주 검토되고 변경되어야 하지만, 정책은 비교적 장기간 유지되어야 한다.

2. 정보보호 정책의 필요성

1) 적절한 통제 수단

임시방편으로 정보보호처리를 실시하고자 할 때 주로 정보보호 제품을 구입, 설치하는 경우가 많지만, 대체로 희망하는 결과가 나오지 않아 실망하게 된다.

정보보호 업무를 효과적으로 수행하기 위해서는 업무의 대상과 지향하는 업무방향이 설정되어야 하고, 조직관리자로부터의 지원 확보와 효과적이고 명백한 정책을 보유하고 있어야 한다. 관리자의 지원이 없이는 정보보호업무를 위한 예산배정이 어렵고, 조직원들을 통제할 수 없다.

그러므로 응용시스템 통제 설계, 사용자 접근권한 확립, 위험분석 수행, 컴퓨터범죄 수사, 보안위반에 대한 징계 등 광범위하고 다양한 정보보호 행위 즉 통제의 기준으로 정보보호 정책이 사용된다.

조직적 기반을 구축하기 위해, 모든 조직은 문서화된 정책, 지침, 표준, 절차 등을 구비하고 조직상의 책임 설정, 보안대책 집행절차, 관리감독, 위험평가 및 정보보호 기획방법 등을 구축해야 한다.

2) 보안제품 선택과 개발공정 유도

대부분의 조직들은 아무것도 없는 상태에서부터는 정보보호 통제를 설계하고 구현할 수 있는 능력이나 자원을 갖고 있지 않기 때문에, 상용 보안제품을 엄선하여 구입하고, 그 통제에 맞춰 조직의 정책, 지침, 표준, 절차를 책정하려 한다. 그러나 이러한 과정은 조직의 정보자산이나 정보보호의 목적, 목표를 충분히 이해하지 못한 상태에서 실행되어 조직에 필요한 결과를 얻지 못하는 경우가 많다.

정보보호의 목표를 기술한 정책은 전조직원이 시스템을 적절히 선정하고 개발하고 구현하도록 유도하고 보장하는 방법이다.

3) 조직관리자의 지원 확보

관리자를 포함한 대부분의 사람들은 현재 직면한 정보보호 위험의 범위나 정도를 알지 못하며, 또한 전문지식이 없기 때문에 어떤 위험에 대한 통제 조치의 필요성조차 평가할 능력이 없다.

정보자산의 중요성, 정보보호 조치의 필요성을 관리자가 인식하고 전 조직원에게 정보보호에 주의를 기울이도록 지시하도록 하는데 정보보호 정책이 결정적인 방법이며, 조직원들이 정보원을 보호(protect)하는데 소홀하지 않도록 하는 환경 조성에도 중요하다.

정책수립은 관리자가 적법한 행동을 정의하고 관심을 나타내며, 어떤 행동의 타당/부당 여부를 명시하

므로써 비용을 크게 들이지 않는 적법한 방법이다.

4) 책임회피

정보보호에 관한 법적 판례는 조직원 특히 관리자들이 정보보호에 관한 부적절한 행위에 책임을 부과하고 있음을 알려준다. 이 책임부과는 부주의 (무관심, 태만), 의무위반, 보안대책 실패 등이 원인인데, 관리자로서도 책임회피의 목적으로 정보보호 행위에 지원하게 되고, 관련 정책을 수립하는데 동의하지 않을 수 없게 된다.

5) 일관성 있고 완전한 보안 실시

조직내 부서간 업무가 서로 다르기 때문에 정보보호가 필수적인 부서도 있지만, 오히려 짐이 되는 부서도 있게 마련이다. 그러나 정보보호 분야의 중요한 문제 중 하나가 단편적이고 상호 모순된 정보보호 행위이다. 비록 복잡한 정보보호 행위에 전 조직원이 숙달되도록 만드는 것은 실행가능하지도 바람직하지도 않지만, 적어도 최소한의 정보보호 행위에는 동의하도록 하는 것이 중요하다. 즉 정책은 최소보호수준을 정의하는데에도 사용된다.

3. 정책의 개발 절차

1) 주요 참고자료 수집

정보보호 정책을 개발할 때에는 현재 조직에서 정보보호가 꼭 필요함은 나타내는 위험분석 결과를 참고해야 한다. 더 많은 관심을 필요로 하는 영역을 확인한다는 관점에서 실패의 기록도 도움이 되며, 소송, 불평불만, 분쟁도 정보보호 정책 개발의 참고 자료가 될 수 있다. 응용시스템 개발 정책, 컴퓨터장치 도입 정책, 인적자원 정책, 물리적 보안정책 등의 관련 정책도 유용한 배경정보를 제공해 준다. 만약 어떤 조직이 타 조직의 종속조직이거나 계열조직이면 상위 조직의 정책을 반드시 참고해야 한다.

2) 정책 골격 정의

참고 자료들을 검토, 편집한 후, 당장 적용할 정책이나 차츰 적용해 나갈 정책을 포함해서, 새로이 책정될 포괄적인 정보보호 정책에서 취급할 모든 논제들의 목록을 준비하고, 몇 번에 걸쳐 정정해 나간다. 그리고 해당 조직에서 정책을 표현하고 사용하는 방법을 정의해야 한다.

절차나 표준과 같은 여타 관리지령과 정책간의 연계 뿐 아니라, 기존 정책이 작성된 스타일(style), 특정 용어의 사용, 정책기록의 전통적 포맷(format), 정책항목의 번호매김이나 명명법 등에 대해서도 연구해야 한다. 그리고 정책문을 어느 정도 상세하게 표현할 것인가에 대한 검토도 수반된다.

3) 적용대상 확인

여러 대상을 적용 상대로 하는 정책을 책정할 때는 정책초안이 작성되기 전에 적용대상 확인과정을 거치는 것이 좋으며, 적용표를 작성하여 확인하는 것이 효율적이다. 적용표란 행에는 적용대상, 열에는 필요한 정책 종류(category)를 나열하여, 각 교차되는 셀에 어떤 정책항목이 필요한지 명시해 주는 것이다.

서로 다른 대상에 대해서는 서로 다른 정책문이 마련되어야 하지만, 대체로 각 대상간의 정책문에는 중복되는 것이 매우 많기 때문에, 시간절약책으로 하나의 대상에 대한 정책문을 먼저 작성하고 점차 이를 기초로 하여 확대 적용시킨다.

4) 효과적인 검토, 승인, 집행

정보보호 정책 초안이 일단 작성되면, 주위의 여러 동료들에게 검토를 의뢰한다. 견해가 다른 여러 사람들의 검토결과에 따라 더욱 명백하고 간략하게 정책을 수정할 수 있고, 기존의 조건에 부응하도록 만들

어 간다.

조직의 대표자에게 검토 및 승인을 요청하기 전에 정책의 실행가능성, 비용과 이익의 관계, 내부 정략에의 관련 등의 관점에서 정책을 검토, 평가한다. 정보보호 정책을 준비하면서 그 정책의 집행과정을 결정해야 하는데, 정책이 있으면서 집행되지 않는 것은 조직원들의 위선이나 부당행위에 대한 관용을 가르치는 꼴이 된다.

새로운 정책의 공표에 앞서 감사의 인준을 받아야 한다. 그리고 조직원들에게 어떤 행위가 정보보호 정책에 위배되고, 어떤 처벌을 받게 되는지를 알려주는 홍보, 교육 프로그램 실시하는 것이 바람직하다. 사업정보가 재산이며, 복제, 수정, 삭제되어서는 아니 되고, 승인 없이 타 목적에 사용되어서는 아니 된다는 것을 이 교육 프로그램으로 명백히 인식시켜 준다.

V. 정보보호 정착을 위한 정책방향

정보화는 최소의 비용으로 교육, 문화 기반의 확충, 쾌적한 생활환경을 조성하여 삶의 질을 획기적으로 높이고, 지역, 계층간 격차를 완화할 수 있는 수단이 된다. 21세기 정보사회에서 우리나라가 세계일류국가로 도약하기 위해서는 정보화를 범국가적 차원에서 적극 추진하여 국가 경쟁력을 선진국수준으로 끌어 올려야 한다.

정보와 지식이 돈이 되고 힘이 되는 정보화 시대로 들어서고 있는 시점에 국가적으로 정보화를 촉진시키고 초고속 정보통신기반 구축을 서두르고 있다. 건전한 정보사회를 구축하기 위해서는 다음과 같은 정보이용의 규범적 원칙이 지켜지도록 해야 한다.[6]

1) 자율성의 원칙(principle of autonomy)
   정보의 제공, 공개, 활용, 처분은 그 정보주체의 자유의사, 자율성에 맡겨야 하는데, 인격의 존엄성과 자율성으로부터 도출되는 원칙이다.
2) 해악회피의 원칙(principle of nonmaleficence)
   정보처리 기술을 이용하는 경우 누구에게도 해악을 입혀서는 안된다는 원칙으로서, 기술활용에 대한 최소한의 도덕적 요구를 나타낸다. 법을 도덕의 최소한이라고 한다면, 이 요구는 곧 국가 강제력 개입의 근거와 한계를 설정하고 있다.
3) 설명제공을 통한 동의의 원칙(principle of informed consent)
   정보사회에서 정보통신시스템의 관리자와 일반인과의 관계를 규정하는 원칙으로서, 어떤 목적을 위하여 수집된 정보가 다른 목적을 위하여 사용되기 위해 요구되는 정보주체의 동의는 반드시 충분한 설명을 통하여 이루어져야 함을 뜻한다. 즉 우월한 지위의 정보처리자가 정보통신 체계를 일방적으로 남용할 수 없도록 규정한다.

현재 우리나라의 정보화 사업의 장애요인으로는 첫째 정보활용수준이 낙후되어 있으며, 둘째 정보통신기술수준이 선진국과 격차가 있고 전문기술인력이 부족하며, 창의적인 중소기업의 활동이 부진하다는 것이다. 셋째로 고도 정보통신기반구축이 늦어지고 있으며, 넷째로 지적 소유권, 정보보호, 사생활보호등에 대한 사회적 인식과 법·제도 정비가 미흡하여 정보화 촉진의 장애요인으로 작용하고 있다.

정보와 지식의 정당치 못한 생산, 유통, 활용은 사회체제 뿐 아니라 개인 생활에 치명적인 악영향을 미치게 되어 사회적 퇴보를 초래할 위험성을 내포하고 있다. 따라서 정보화 사업은 지적소유권, 정보보호, 사생활보호, 정보의 윤리성등 여러 문제점에 대해 신속한 대응방안이 강구될 수 있도록 철저한 준비체제를 갖춰 정보사회의 역기능에 적절히 대응할 수 있도록 하여야 할 것이다.

초고속 정보통신기반상에서 수립되어야 할 정보보호 정책 방향은 먼저 응용서비스별 요구사항을 파악하고, 정보보호 기본원칙과 정보시스템에 대한 기본원칙을 정의하여 정보보호 체제(framework)를 설정하

는 것이다. 그런 다음 정보보호 체제를 바탕으로 상호역할을 정립하고 법적·제도적 측면의 통제와 실행에 대해 준비하고, 기술적 측면, 관리적 측면에서 준비해 나가야 한다.

본 논문에서는 현재까지 정보보호 정책방향에 대한 제안 [1,2,3,4,8]들에서 정리된 논리적인 정책방향을 참고하여, 실제로 실행에 옮겨야 할 정책 방향들을 항목별로 정리해 보고자 한다.

1. 정보문화 확산

정보사회로 들어서서 예컨데 정부, 기업, 병원, 학교 등 대부분의 조직에서 정보시스템을 사용하게 되었지만, 정보나 컴퓨터시스템을 이해하고 각자의 업무에 필요한 것을 스스로 개발할 능력을 보유한 사람들이 매우 적다. 그래서 국가적 차원에서 정보화에 대한 범국민적 공감대 형성과 정보의 건전한 이용능력 향상을 위해 다양한 홍보·계몽·교육활동을 추진해 나가야 한다. 특히 전국민을 대상으로 정보보호의 중요성을 인식시키고, 어겼을 때는 처벌된다는 사실을 철저히 인지시켜야 하며, 특히 도덕·윤리적으로 판단하여 불건전한 정보의 이용을 자제하도록 유도하여야 한다. 이러기 위해서는 사회지도층에서부터 도덕 재무장, 윤리바로세우기에 앞장서야 할 것이다.

정보보호에 대한 전반적 국민의식수준 제고와 사회적 분위기를 조성하기 위한 홍보·계몽·교육활동의 대상으로는 전 국민의 대부분을 차지하는 일반 사용자(end-user)뿐 아니라, 기관사용자(관공서, 법인, 기업체등)의 경영자, 시스템관리자도 포함되어야 한다. 특히 국가 정보화의 주축이 되는 공무원, 그리고 청소년들이나 일반인들을 가르치는 위치에 있는 교사 및 교육자들에 대한 교육을 더욱 강화하여 의식개혁에 앞장 세워야 한다. 그리고 정보통신 관련 사업자 즉 네트웍 서비스 사업자, 소프트웨어 개발·공급자, 하드웨어 개발·생산·공급자들에 대한 계몽·교육도 소홀히 해서는 안될 것이다.

2. 국가적 관리체제 확립

정보보호 업무를 국가적으로 관리하기 위하여 부문별 책임소재가 명확한 전문기관을 설립하고, 부처별, 기관별 협조체제를 강화하여 여러 정책들의 상충으로 인해 일반 국민들의 혼돈을 유발케 해서는 아니된다. 또한 각 분야별, 부문별 담당자, 연구자, 개발자, 교육자, 관리자들을 총괄관리하여 국가적으로 모든 정보보호 업무를 일사분란하게 통합하는 기능을 담당해야 한다. 각 분야별, 부문별 담당자들은 전체를 파악하지 못하고 자신들의 업무만 생각하는 경향이 있기 때문이다.

침해사고 대응팀과 검경수사팀의 긴밀한 협조하에 국내 모든 전산망을 상시 감시하여 부정접근을 방지하며, 부정접근 사고가 발생했을 때는 즉각적으로 대응 및 복구하고, 해커를 추적하여 조치함으로써 재발을 방지해야 한다. 그리고 컴퓨터 바이러스 감염사고나 해킹 침해사고를 당한 일반사용자 및 시스템 관리자들의 신고를 접수하여 즉시 구제책을 조치해 주고, 신고 접수상황을 수시로 발표함으로써 주위를 환기시킨다.

또한 암호제품의 인증을 통해 상호운용성을 확립하면서, 신뢰하고 사용할 수 있도록 인증마크부여제도를 창설해야 한다.

그리고 정책 개발에 대해서도 국가적 차원의 정책 뿐 아니라 개별조직 차원의 정책수립에 근간이 되는 표준정책 문안을 개발해 줌으로써, 범 국가적으로 각 조직의 정책들이 일관성이 있고 각 조직에서는 비용을 적게 들이면서도 쉽고도 빠르게 정책을 수립할 수 있고, 대상자들이 쉽게 정책을 이해하고 준수할 수 있도록 해 주어야 한다. 또한 수시로 정책을 재검토하여 항상 최신 보안기술을 수용하고 국제적 규범에 정합할 수 있도록 개정해 나가야 한다.

3. 법·제도 정비

정보사회에 대비한 법·제도적 장애요인을 정비·개선함으로써 정보화의 확산과 정보사회의 조기정착의 여건을 조성하고, 국가적으로 정보보호업무가 원활히 추진될 수 있도록 한다.

정보통신부의 "정보화 촉진 기본법"을 위시해서 "컴퓨터 프로그램 보호법", "전기통신기본법", 통상산

업부의 상행위관련법, 총무처의 사무관리규정, 정보처리관련 법률, 행정절차법, 재정경제원의 금융, 증권관련법, 교육부의 교육법, 법무부의 형법, 상법, 민법, 내무부의 세법등 정보화에 대비하여 재정비해야 할 법률, 규정을 전반적으로 검토·개정해 나가야 할 것이며, 서로 다른 유권해석이 나오지 않도록 연구하고 협조하여야 한다. 이러한 정보정책의 발전 방안으로는 정책 목표와 정책 수단간의 접합성을 유지하고, 정책참여자간 상호 적응의 제도화, 정책내용의 전달 체계로서 정책 결정 구조와 집행 체제간에 일관성 확보, 정책 대상 집단 및 국민적 관심과 참여의 제고 등을 고려하여야 한다.

이러한 법규 재정비는 해킹, 컴퓨터 바이러스, 개인사생활 침해, 저작권 침해, 불건정정보유통과 같은 정보범죄에도 대비해야 하겠지만, 자연재해에 대비하는 안전성(safety)이나, 감사, 평가인증, 표준화에 관련된 법규도 시급히 마련되어야 할 것이다.

4. 정보보호 전문인력 양성

국가적 정보보호 업무를 원활히 추진하기 위해서는 무엇보다도 전문인력 양성이 시급하다. 보안기술 연구나 보안제품개발의 기술인력뿐 아니라 정보보호 전문성을 보유한 시스템 관리 인력, 감리인력, 시험·평가인력, 표준화 및 정책개발 인력, 침해사고 대응인력, 법조계 및 검경수사인력 등도 시급히 양성되어야 하며, 무엇보다도 이러한 인력 양성을 위한 교육인력 양성이 앞서야 한다. 그러기 위해서 전문기관에서 공무원 및 일반인 대상으로 교육을 강화하여 전문 인력양성에 공헌함과 동시에 정보통신전문대학원, 일반대학원에 정보보호학과를 신설하고 지원해야 한다. 다만 인력수급상황을 원활히 조절하기 위하여 지원 대학수를 제한해야 한다.

5. 정보보호 기술개발 및 연구지원

일반적 첨단기술은 우선 선진국기술을 도입하여 제품생산부터 시작할 수 있지만, 정보보호 분야는 기술적 선진국 예속화에다가 국가 전반에 걸친 정보의 예속화가 이루어지기 때문에 정보보호 기술만은 독자적인 기술을 개발할 수 있도록 국가적 차원에서 연구지원을 아끼지 않아야 한다. 전문연구기관, 전문업체, 전문학회에 대한 연구비 지원 뿐 아니라 교육과 연구를 겸하고 있는 대학의 기초연구에 대해 지원하면 인력 양성과 이론적 기초연구 양쪽 효과를 얻을 수 있다.

6. 정보보호 관련 기업육성 및 지원

정보보호관련 기업육성은 전문인력 양성과 함께 국가 정보보호 사업의 핵심과제이다. 정보보호관련 산업은 노동집약적 산업이므로 새로운 아이디어가 쉽게 기업화될 수 있고 기술력 있는 중소기업으로 성장해 갈 수 있도록 지원해 주어야 한다.

7. 표준화, 감리 및 평가제도 개선

일반적인 첨단기술과 마찬가지로, 급격히 발전하고 있는 암호관련 기술에 관한 표준화 분야의 선진국 동향 분석 및 신속한 대응으로 국가 표준을 마련해야 한다. 우리나라의 문화적, 정서적 정보통신 환경에 적응하고 기술적 능력등을 감안하여 표준안을 마련하고 국제 표준화에 적극 참여하여 관철해 나가면서, 국가간 상호 인정을 위한 협조체제를 굳건히 해야 한다.

그리고 정보보호 제품이나 시스템의 개발, 생산, 판매, 관리업무 전반에 대한 감리 및 평가제도도 조속히 개선, 확립해야 한다.

8. 국제 협력의 촉진

암호기술 뿐 아니라 표준화, 정책, 제도등 전반적으로 선진국 동향분석을 통하여 신속히 대응하고, 제외국 정보보호기관간의 정보교환을 수행함으로써 상호인정하는 평가·인증제도를 확립하여, 국가간 상호인정의 실시 기반을 추진해야 한다.

범세계 전산망(global network)의 확산과 함께 국제적인 정합성을 갖는 해킹, 바이러스 대책을 실시하여 국제적인 대책실시 체제구축에 공헌해야 한다.

9. 정보보호 소프트웨어 개발 및 보급

정보범죄의 예방과 대응·신속복구를 목적으로 국가 전문기관 또는 민간업체에 의뢰하여 바이러스 대책기술이나 부정접근 방지기술 등을 개발하고, 정보보호 소프트웨어를 개발하여 유료·무료로 보급해야 한다.

초고속 정보통신망에서의 해킹사고를 사전에 예방하고 해킹 사고 발생시 해커 추적을 용이하게 하는 소프트웨어나, 컴퓨터 바이러스 감염검사 및 복구 소프트웨어, 인터넷 불건전정보차단 소프트웨어등을 시급히 개발·보급해야 한다.

10. 특허제도 개선

현행 특허제도로는 급격히 발전하는 첨단 기술분야에서 우리나라 자체 기술이 살아남기 힘들다. 특허취득에 시간이 많이 소요되어, 실제 특허를 취득한 시점에는 벌써 그 기술이 낡은 것이 되기 쉽다. 정보보호 기술의 경우도 마찬가지 현상이므로, 특허제도의 개선으로 참신한 아이디어가 짧은 시일내 특허로 등록되어 지적 재산권으로 보호될 수 있도록 하여야 한다.

이러한 정보보호 정책방향을 감안하여 조속히 정비해야 할 초고속 정보통신기반 안전성 정책들은 다음과 같이 정리할 수 있다.

1) 국가 정보통신기반 보호 대책
2) 컴퓨터 바이러스 대책
3) 컴퓨터 부정접근 대책
4) 정보시스템 안전 대책
5) 시스템 감사 대책
6) 사생활 보호 대책(개인정보보호법)
7) 소프트웨어 관리 대책
8) 지적재산권 보호 대책
9) 암호기술 개발 및 응용 대책
10) 정보보호 감리, 평가인증 대책
11) 정보보호기술 표준화 대책
12) 정보보호 산업육성 대책
13) 정보보호 인력양성 대책
14) 인터넷 보안관리 대책

Ⅵ. 결 론

본 논문에서는 초고속 정보통신기반에서 정보보호 업무를 원활히 추진하기 위해 국가적 차원에서 시행해야 할 정책방향을 제시하였다. 초고속 정보통신기반 구축과 국가 정보화에 장애요인이 되고 있는 범죄적, 사회적, 문화적, 윤리적 측면의 역기능에 대처하기 위해 정보보호의 개념을 살펴보고 정보범죄의 실태와 내용을 고찰했으며, 정보보호 정책을 개발하는데 고려해야 할 지침을 기술하였다.

정보화에 대한 범국민적 공감대 형성과 정보의 건전한 이용능력 향상, 정보보호의 중요성 인식 및 처벌사실의 인지, 그리고 불건전 정보이용 자제를 유도하기 위한 홍보·계몽·교육이 우선이 되어야 한다.

또한 정보보호 업무를 책임행정으로 일관성있게 추진할 국가적 관리체제 확립과 법·제도 정비에도 관심을 쏟아야 하며, 특히 정보보호 전문인력 양성과 정보보호 기술개발 및 연구지원, 정보보호 관련 기업육성 및 지원이 국가 정보화를 성공적으로 이끌 수 있는 시책이라고 본다. 그리고 표준화, 감리, 평가제도 및 특허 제도 개선도 매우 중요하고, 국제적 협력도 빠뜨릴 수 없는 시책이며 조직 차원의 정책수립을 도와 주기 위한 표준정책 문안 개발이나 정보보호 소프트웨어 개발 및 보급도 국가에서 시급히 시행해야 할 것이다.

21세기 정보사회의 문턱에서 초고속 정보통신망 구축 및 운용의 환경 조성 일환으로 정보보호 정책수립은 필수 요소인데, 대체로 충분한 정보보호 지식을 갖지 못한 일반 국민들이나 이익 추구가 목적인 기업보다는 국가를 운영하는 정부 및 공무원 개개인의 의식 개혁이 우선이 되어야 하며, 정보문화 확산을 위한 사회적 분위기 조성에 앞장서야 한다.

참고문헌

1] 박정현, 이상호 "초고속 정보통신기반에서의 안전성 대책방향과 정부 역할", 정보처리학회지, 제4권, 제2호, 1997.3.

2] 한세억, "우리나라 정보정책의 현상분석과 발전방안", Telecommunications Review, 제7권, 제1호, 1997.1.

3] 강휘원, 현창희, "정보 프라이버시 보호를 위한 정책방향", Telecommunications Review, 제7권, 제1호, 1997.1.

4] 송주석, "정보전대비 전문인력 양성해야", 세계일보, 1997.9.24.

5] 문필주, 고병도, 전문석, 이철희, "초고속 정보통신망과 인터네트의 접속에 따른 통신망 보안", 통신정보보호학회지, 제5권, 제4호, 1995.12.

6] 정보통신부 정보화기획실, "정보화에 관한 연차 보고서", 1996.9.

7] 박춘식, "OECD, 프라이버시 그리고 시큐리티", 통신정보보호학회지, 제6권, 제3호, 1996.9.

8] 박정현, "초고속정보통신기반하에서 시큐리티 프레임워크", 통신정보보호학회지, 제6권, 제3호, 1996.9.

9] 최영호, "정보범죄의 추세와 대처 방안". 통신정보보호학회지, 제6권, 제3호, 1996.9.

10] Charles Cresson Wood, et. al., *Information Security Policies Made Easy-ver.5*, Baseline Software Inc., 1996.