# 정보사회에서의 정보보안에 관한 연구

## A Study on Information Security in the Information Society

조 찬 식(Chan-Sik Cho)*

목 차

1. 서 론
2. 정보사회와 보편적 서비스
3. Utopia 와 Dystopia
4. 정보보안의 이해
5. 정보침해의 유형
6. 정보보안의 전략
7. 결 론

## 초 록

정보화가 가속되면서 정보의 효과적이고 정확한 전달과 보호에 대한 사회적 관심이 점점 높아가고 있다. 이에 본 논문은 정보사회와 이의 중요한 메카니즘이 되는 보편적 서비스의 개념을 살펴보고, 정보사회에 대한 상반된 두 가지의 이론적 견해를 비교해 본 뒤, 정보보안의 정의, 필요성, 구성요소 등을 분석하고, 다양한 정보 침해의 유형을 조사·설명한 뒤, 정보사회에서의 정보보안 전략을 기술적인 측면과 제도적인 측면으로 나누어 제시함으로서 정보보안의 확립과 정보사회에 대한 이해를 돕는데 일조함에 그 목적이 있다

## ABSTRACTS

As informatization has been accelerated, the secure information flow has become a major social concern. In that, this paper examines the theoretical background of the information society and the concept of universal service; compares the contrasting perspectives on the social meanings of information; analyzes the definition, importance, and components of information security; and suggests some strategies on information security centering around the technical and institutional aspects of it. In so doing, this study aims at establishing the information security and at enhancing our understanding on the information society.

* 동덕여자대학교 문헌정보학과 부교수
접수일자 2000년 3월 1일

## 1. 서 론

정보화가 가속되면서 정보가 하나의 상품이나 자원으로써 가치를 가지게 되었으며 매일의 생활에 꼭 필요한 전략적인 요소로 인식되어 가고 있다. 이러한 정보는 기존 생활방식에 새로운 요소로 작용하고 있으며 효율적인 관리 및 이용은 정보사회에서 꼭 이루어져야 할 과제인 것이다. 특히 보편적 서비스의 확대로 인한 인터넷 등의 정보통신망의 확산이 정보의 생산과 유통을 보다 수월하게 하고 있는 정보사회의 특성상 정보에 대한 다양한 실상 파악과 분석이 이루어질 때 정보사회에서의 삶의 질을 높일 수 있게 되는 것이다.

정보사회에 대한 견해는 낙관론과 비관론으로 나누어 살펴볼 수 있는데 전자의 경우는 정보가 정치, 경제, 문화 등 사회의 모든 면에서 기존의 생활방식을 향상시키며 좀 더 편리하고 안정된 사회로 진행이 되고 있음에 초점을 맞추고 있는 반면, 후자는 개인의 자유와 사회적 행위 전체가 정보기술이나 정보체제를 분배하는 수단을 소유한 사람이나 단체, 기구 등의 불순한 동기에 의해서 서서히 잠식해 가는 것을 주시하며 정보의 복합성과 투과성이 오히려 사회 속의 인간을 통제하는 도구의 필요성과 가능성을 제시하게 된다고 보고 있다.

이러한 정보와 사회의 관계를 보는 관점이 어떻든 정보사회에서 정보가 제대로 전달되기 위한 정보보안은 매우 중요한 의미를 갖게 된다. 이는 정당한 이용자가 원하는 정보를 알 필요성과 인가되지 않거나 부당한 자격을 가진 사람이 그 정보에 접근할 수 없게 함을 의미하는 것으로 이러한 정보보안이 이루질 때 정보의 자유롭고 긍정적인 유통과 소비가 이루어짐으로 해서 정보사회의 진정한 의미를 찾을 수 있게 되는 것이다.

이러한 정보보안은 정보의 누수나 침해에서 그 원인을 찾아볼 수 있다. 정보의 누수나 침해는 정보통신의 개방성과 접근성의 용이함에서 발생되며 그 형태 또한 매우 다양하게 나타나고 있다. 정보침해의 유형을 크게 나누어 보면, 관리자 및 사용자 부주의, 응용프로그램에의 버그, 구성 오류 등에서 비롯되며, 데이터상의 문제점, 시스템적인 측면, 그리고 조직관리 측면에서 살펴볼 수 있다.

이에 본 논문은 정보사회와 보편적 서비스의 이론적 개념을 살펴보고, 정보사회에 대한 상반된 두 가지의 이론적 개관을 비교해본 뒤, 정보보안의 정의, 필요성, 구성요소 등을 분석하고, 다양한 정보 침해의 유형을 조사·설명한 뒤, 이를 바탕으로 정보사회에서의 정보보안 전략을 제시함으로서 정보보안의 확립과 정보사회에 대한 이해를 돕는데 그 목적이 있다.

## 2. 정보사회와 보편적 서비스

정보가 하나의 상품이나 전략적 자원으로 가치를 갖게 되면서 사회의 많은 구성요소가 정보에 영향을 주고받으며 변화하게 된다. 정보사회란 이러한 정보의 가치가 사회의 각 영역에서 인식되고 사회 구성원들 간에 상호작용하는 사회적 총체라고 말할 수 있다.(전석호 1997; 조찬식 1995a; 한상완 1997; Bell 1973) 이러한 정보사회는 정보의 효과적인 유

통을 전제로 하며 이를 달성하기 위한 사회적 장치를 필요로 하게 된다. 보편적 서비스는 사회구성원이 정보에 접하여야 함을 나타내는 사회적 메카니즘으로 정보화의 과정에서 필연적으로 이루어지게 되는 것이다.

정보사회란 정보가 가치를 갖는 사회의 총체를 말한다. 역사의 발전단계를 볼 때 인류는 수렵사회, 농경사회, 산업사회의 형태로 발전되어왔다. 수렵사회는 인간의 수렵활동이 그 사회의 모든 생활방식과 사고를 지배해왔으며, 농경사회에서는 농업, 유목업 등이 그 시대의 중심적 생활형태가 되어왔고, 산업혁명을 통한 기계화와 대량생산으로 규정되어지는 산업사회는 산업활동에 관계되는 행위가 사회유지의 기본이 되는 사회를 유지해 왔다. 따라서 정보사회란 사회구성원의 활동, 인식, 사고가 정보를 중심으로 이루어지는 사회를 가리키며 곧 정보의 혁명으로 야기되는 정보의 대량생산과 대량소비, 즉 정보시대의 도래를 의미한다.

이러한 정보가 영향을 미치는 사회, 즉 정보사회에 대한 이론적 연구는 서구, 특히 미국사회를 중심으로 사회의 구조기능(structural-functionalism)에 입각하여 사회 변화를 연구한데서 그 기원을 찾아볼 수 있다. Daniel Bell (1973)은 지축원리(axial principle)와 사회구조(social structure)의 변화를 이론화하여 현대사회가 과거의 사회들과 그 중에서도 특히 산업사회와는 다른 차원의 후기산업사회로서 도래하고 있음을 예고하였다. Bell은 Marx의 순수자본주의와 산업사회 하에서의 통합조정기능의 과소평가를 비판하며 새로운 금융제도의 발달이 자본의 유통을 조정하고, 중간관리층의 증가와 정신노동위주의 새로운 산업의 등장으로 인한 후기산업사회론의 기초를 확립하였다.

Bell의 후기산업사회론의 요체는 바로 Bell이 말했던 '지적기술' (intellectual technology)이다. Bell에 의하면 기술이란 과학적 지식을 사용하여 일을 반복적으로 할 수 있는 구체적인 방법을 의미한다. 그런 점에서 지적기술이란 기계기술과 달리 직관적인 판단을 통한 문제해결법칙(algorithms)을 의미하는 것이다. 그러므로 기계기술(machine technology)이 산업사회를 주도했듯이 후기산업사회는 지적기술에 의해 유지, 운영되는 것이다. 그럼에도 불구하고 Bell은 초기에는 후기산업사회가 서비스 사회인지, 정보사회인지, 지식사회인지를 명명하지 못했다. 그것은 그 당시만 해도 다분히 주관적인 미래사회의 예고에 불과했기 때문이다.

이러한 후기산업론의 본질은 바로 정보가 하나의 상품이나 자원으로 인식되면서 재조명되었다.(전석호 1997; 정동열 1993) 즉 정보란 현대사회의 효과적인 조정과 기능수행에 기초가 되는 속성들을 가지고 있다고 보는 것이다. 이러한 속성들이란 첫째, 정보가 자원이라는 점이다. 에너지나 자본 또는 노동력처럼 정보가 경제, 정치, 문화적 목적을 달성하기 위하여 이용되는 필요한 자원이란 점이다. 둘째, 정보란 재화란 것이다. 정보가 경제적 또는 다른 보상으로 개인, 조직 또는 국가간에 자주 팔리고 거래되며 교환되는 하나의 재화가 된다는 것이다. 셋째, 정보란 자원의 보존과 생산성 향상에 기여하게 된다는 점이다. 효과적인 정보의 습득과 이용은 다른 자원들을 절약하고 또는 생산적인 이용이 가능케 한다는 점

이다.

이에 따라 정보사회론은 산업화의 심화과정에서 정보의 역할을 창출하는 사회의 다른 힘(social forces)들이 다양하게 작용하면서 산업사회에서 정보사회로 이행해 간다고 추정하고 있다. 이러한 사회적 힘에 의한 사회구조의 변화는 경제적, 정치적, 문화적 조정을 필연케하는 정보에 대한 인식을 재고시켰다. 즉, 정보사회란 새로운 사회적 현상으로서 정보에 의하여 사회구조 및 인간의 생활양태가 재조정되며, 정보산업(information industry)부문의 확대 및 성장으로 기존의 사회적 인식이 정보중심으로 바뀌는 사회변화의 총체를 지칭하기에 이르렀다. 경제적 양식으로 자본주의는 정보의 거래를 가능케 하였으며 사회화의 한 형태로서 산업화는 정보의 생산, 분배, 소비를 가능케 하였다. 그러므로 정보사회란 산업화와 자본주의가 상호작용하는 고도화된 산업자본주의(industrial capitalism)의 한 형태이지만 정보중심의 사회총체라는 특징을 지니고 있다는 점에서 새로운 패러다임의 전환(paradigm-shift)이 이루어지게 되는 것이다.

이러한 정보사회의 가장 두드러진 특징은 정보의 폭 넓은 확산과 효과적인 보급을 위한 정보통신의 발전이다.(조찬식 1995b; Antonelli 1989; Williams 1990) 정보사회에서 사회의 어떤 구성원이라도 정보로부터 자유로울 수 없으며 또한 사회 유기체적 관점에서도 필요한 정보의 습득이란 개인뿐만 아니라 그 사회에 주어진 과제인 것이다. 특히 대량의 메시지(messages)와 경로(channels)가 다양해지면서 대중 전달매체(mass media)의 급속한 발전과 확산은 많은 정보를 다양한 매체를 통하여 개인의 지식축적, 학습용, 업무용 및 여가에까지 널리 이용되게 하였으며 시간과 공간을 초월하여 보다 많은 정보의 교환을 용이하게 하고 있다. 아울러 정보통신기술의 확산은 개인, 조직, 국가들로 하여금 정보를 생산하고 유통시키며 저장하여 이용하는 것을 가능케 하였으며 이러한 정보기술의 확산은 사회환경을 바꾸기도 한다. 예컨대 정보사회의 대표적인 기술결정체인 컴퓨터는 인터넷, 인공위성, 유선방송, 비디오디스크 등과 더불어 현격한 가격하락으로 우리의 생활에 깊이 침투해 있으며 이제는 컴퓨터 또는 인터넷과 같은 정보통신의 영향이 안 미치는 생활은 상상하기도 어렵게 되었다.

이러한 정보통신의 발달로 인한 정보와 통신의 수렴(convergence)과 상호연관성(interconnectedness) 그리고 모든 사람들이 필요로 하는 각종 정보를 가장 신속하고 효율적으로 수집, 처리, 전달하는데 중요한 하부구조(infrastructure)가 되는 정보통신기술의 발전은 통신서비스의 공공화를 초래하게 되었다. 초기의 통신서비스의 개념은 주로 개인적 재산의 성격이 강하였으나 정보화가 가속되면서 정보통신에의 접근은 좀더 일반적인 개념으로 변화되었으며, 통신서비스의 공공화 즉 정보통신시설이 모든 사회구성원을 위한 사회적 수단이 된다는 것은 중요한 의미를 가지며 어느 지역의 그 누구도 통신서비스가 가져오는 이익으로부터 배제되어선 안 된다는 것이다. 다시 말해서 통신서비스의 이용이 모든 사회구성원의 사실적 권리가 되어야 한다는 점에서 정보사회의 통신서비스의 중요성이 부각되고 있는 것이다.

통신서비스의 일반화 개념은 보편적 서비스(universal service)에서 구체화되었다(조찬식 1999a; Dordick, Rife 1991; Hills 1989). 보편적 서비스란 용어는 1910년 당시 미국 AT&T사의 사장이었던 Theodore Vail에 의해 처음 통신부문에 사용되었으며, 그 후 1934년 미국 통신법(Communication Act)에서 보다 구체화되고 있다. 이 법에 따르면 보편적 서비스를 "가능한 한 모든 국민에게 전국적인 유무선 통신서비스를 적절한 설비와 합리적인 가격으로 제공될 수 있도록..." 하는 것으로 규정하고 있다. 통신서비스에 대한 이와 같은 시각은 마치 누구나 교육과 의료혜택을 당연히 받을 수 있듯이, 정보이용을 위한 통신서비스도 '누구나', '어디에서든지', 그리고 '언제나' 접근될 수 있어야 한다는 것이다.

초기의 보편적 서비스의 개념은 음성을 통한 전화중심의 통신서비스였으나 정보사회의 도래로 인한 사회환경의 변화는 유선을 이용한 전화서비스가 더 이상 공공의 기본권리를 보장할 수 없음을 시사하고 있다. 즉, 많은 사람들이 정보의 가치와 다양한 형태를 인식하면서 정보의 유통과정에 관여하고 있다는 사회적 총체는 단순히 사람과 사람 또는 조직과 조직 사이의 연결성에 중점을 두었던 통신서비스가 이제는 정보의 일반화를 통하여 필요한 정보전달의 기능으로 점점 변화되어야 하며 이러한 통신산업의 발달과 정보의 중요성은 결국 통신과 정보의 수렴(convergence)으로 이어지는 것이다. 이는 정보사회에서의 국민의 권리란 개인간의 단순한 '연결'에서 끝나는 것이 아니라 민주주의 사회의 시민으로서 필요한 정보를 제공함으로서 사회적 환경에 대응하 수 있도록 사회보장의 차원에서 이루어지느냐의 중요한 의미를 갖게되는 것이다.

보편적 서비스는 정책적인 배려를 바탕으로 평등과 효율이 균형을 이룰 때 그 효과를 기대할 수 있다. 물이나 전기 등의 공공시설과 같이 정보통신시설의 보급도 효과적인 서비스를 위한 국가적 지원과 정책적인 배려를 바탕으로 한다. 국가적인 지원과 정책적인 배려는 시대와 상황, 그리고 사회적 특성을 반영하고 사회적 변화에 능동적으로 대처할 수 있도록 마련되었을 때 비로소 사회의 일체감, 동질성 그리고 상호교류 등의 극대화를 꾀할 수 있는 것이다. 실로 이러한 보편적 서비스의 개념은 미국의 유선 통신서비스를 포화(saturation)시켰고 정보사회에 맞는 다양한 정보서비스를 제공할 수 있게 되었으며, 우리나라의 경우도 이러한 보편적 서비스의 개념이 1980년대부터 채용되어 정보화를 가속시켰으며 우리사회의 정보화에 견인차 역할을 담당해 왔다.(Dordick, Rifㄷ 1991; Kim, Lee 1991)

정보통신기술의 발전과 보편적 서비스의 확대는 새로운 정보문화를 창출하였으며 PC통신, 인터넷, 전자우편(e-mail), 전자상거래(EC: Electronic Commerce) 등 매일매일의 생활 속에 정보의 유통을 가능케 하였으며 시간과 공간을 초월한 가상의 세계를 현실화하였다.(Cronin 1994) 이러한 정보통신의 발전은 정치, 경제, 문화의 모든 면에서 기존의 생활방식과 다른 사회상을 초래하였으며 초국가적으로 영향을 미치게 되었다. 특히 새로운 통신기술의 발달로 정보를 사실상 어느 곳이나 보내고 받을 수 있게 되었으며 농촌과 도시 등지에서도 같은 정보를 공유할 수 있게 함으로써

정보사회의 구성원간에 상호 연관성과 일체감을 갖게 될 수 있는 것이다.

요컨대 정보사회란 사회적 구조와 정보가 상호작용하는 발전된 사회의 형태이다. 즉 사회의 모든 분야에 정보가 '만연'되어 있고 가치를 갖게 되어 사회 구성요소와 서로 영향을 끼치는 성숙한 산업사회의 사회 양태인 것이다. 그런 의미에서 정보사회란 정보와 관련된 부분만의 단순한 변화가 아니라 정보의 역할과 가치의 변화에 따른 사회의 총체적인 변화를 지칭한다고 할 수 있다. 보편적 서비스는 정보사회에 필요한 정보의 제공을 전제로 한 통신서비스의 개념으로 발전되어 일면 정보화를 더욱 가속시키며 일면 기술의 발전에 영향을 받아 정보의 유통을 원활하게 하는 정보사회의 중심축이 되는 것이다. 그러므로 정보사회란 사회의 총체(configuration, totality)를 나타내는 것이며 보편적 서비스란 이를 위한 사회적 메카니즘이라 할 것이다.

## 3. 유토피아(Utopia)와 디스토피아(Dystopia)

정보사회의 도래에도 불구하고 정보와 사회의 근본적인 관계에 대한 논란은 계속되고 있다. 물론 정보란 사회의 산물이며 재화나 자원으로서의 가치에 대해서는 전반적인 공감대가 형성되어 있으나 그러한 정보와 사회의 관계는 아직도 보는 관점에 따라 논쟁의 대상이 되고 있으며 사회학적 이론의 틀에서 나타나는 유토피아적 견해의 자유주의적 접근과 디스토피아적 견해의 막스(Marx)주의적 접근에서 사회와 그 산물, 즉 정보에 대한 이해를 구할 수 있는 것이다.(전석호 1997; 조찬식 1995a; 한상완 1997) 이 두 개의 사상적 기반은 물론 모든 관점을 다 대변하는 것이 아니며 사회와 정보와의 관계의 일정한 면만을 강조하는 것이다. 그러나 위의 두 사상적 기반은 전후 사회발전의 이해에 가장 유용한 잣대로 쓰여져 왔던 것이다.

### 3. 1 유토피아적 견해

자유주의적 전통은 정보와 사회의 관계를 낙원(utopia)과 연계시켰다. 정보의 역할이 증대되면서 인간은 새로운 기술혁명의 이점을 취하고 그 가운데 삶의 질(quality of life)이 향상된다고 보았다. 벨(Bell 1973, 488)에 의하면 "후기산업사회란 새로운 낙원주의(utopianism)의 도래를 말한다. 인간은 재생되고 해방되며 그들의 행위와 의식은 변화되며 과거의 제약들은 소멸되고 마는 것이다."

이러한 자유주의적 전통은 낙관적인 미래주의적 성격을 나타내며 정보가 기존의 사회발전에 장애를 극복하고 정치, 경제, 문화적 발전에 기여하는 점을 강조하며 단조롭고 위험한 작업들이 사라지고 인간의 생활이 점점 지식과 정보의 가공과 유통 그리고 활용을 통하여 새로운 사회로 진입하게 되며 정보통신의 발달로 인한 생활의 향상, 대의 민주주의의 실현 등을 주장하고 있다.

이를 좀 더 구체적으로 살펴보면 첫째, 사회적으로는 사회조직의 원리가 경직된 수직적 또는 피라미드형 구조에서 네트워크형으로 전환되어 가며 자연의 통제와 관리보다는 인간

과 인간의 서비스관리에 더 비중을 두게 되어 정보사회는 궁극적으로는 인간 중심의 그리고 변화에 대응하는 현장적응형의 사회조직 형태가 이루어지게 되며 평등한 전문성을 지닌 지식근로자들 중심의 사회체제로 가게 되어 기존의 위계적 관료체제나 중앙통제식의 인간 또는 사회구조에서 벗어나게 된다는 것이다.

이러한 사회구조 및 가치의 변화는 도시화, 사회제도, 직업구조, 가족관계, 교육 등 사회 전반에 걸쳐 영향을 미치게 되며 이러한 인간 중심의 사회구조 변화야말로 유토피아에 접근하는 전제조건이라 보았다. 예컨대 여성의 고학력화로 인한 여성고용의 확대, 정보네트워크의 발전과 도시와 지방간의 격화 완화로 인한 대도시로의 인구 유입 둔화 등으로 정보사회에서는 각 계층간의 격차가 줄어들고, 사회조직은 대체로 평등한 관계에서 조직되며, 개인이나 조직원의 지위는 지식과 기술을 기초로 하기 때문에 갈등은 줄어들게 된다고 보았다.

둘째, 정치적으로 웨버(Weber)의 관리주의(bureaucracy)가 기술관료주의(technocracy)로의 변화이다. 기술적으로나 합리성으로나 우세해왔던 관료주의는 지식과 정보기술이 급속히 변동하는 정보사회의 전부를 설명하기가 어렵게 되며 정보사회에서의 정치·경제·사회조직은 적응적이고 급속히 변하는 일시적 체계(adhocracy)가 된다. 이에 권력의 원천은 지식이 되며 정보와 기술의 소유가 곧 정치적인 영향력과 직결이 되는 새로운 정치체계로 이행된다는 것이다.

이러한 권력에의 접근 방법은 교육이며 정보사회에서의 정치체계는 많은 정보를 소유하고 그 정보처리능력이 뛰어나고 또한 많은 지식과 기술을 소유한 사람, 즉 테크노크라트들이 정치에 결정적인 영향을 미치게 된다. 이에 따라 정치참여, 정치제도, 정치적 안정 등의 개념이 과거의 권위주의적 구조에서 좀 더 자발적이고 안정된 정치참여가 이루어 과거의 권위주의적 구조에서보다 좀 더 자발적이고 안정된 정치참여가 이루어지며 이를 위한 기술과 교육이 따름으로 해서 보다 민주적인 정치적 안정을 구가할 수 있다는 것이다.

셋째, 경제적으로는 대부분 추출산업(extractive industry)에 종사하던 과거와는 달리, 또한 상품생산에 주로 종사하던 산업사회와 달리 정보사회에서는 지식에 의한 지식을 위한 서비스에 종사하는 구조적 변화를 가져옴으로써 육체적 노동이나 에너지보다 정보가 더 중요시된다. 이러한 정보사회의 경제시스템의 특징은 사회와 경제발전의 중심 축인 정보가 정보유틸리티에 의해 생산되며, 사용자에 의한 정보의 자체생산과 정보의 축적이 증가되고, 축적된 정보가 공동의 생산과 공유를 통하여 확대되며, 교환경제로부터 협동경제(synergetic economy)로의 구조적인 변화가 이루어지게 됨을 의미한다.

이에 따라 정보사회에서의 산업구조면에서 보면 기술의 진보 및 자유시간의 증대 등에 의한 국민요구의 고도화·다양화에 따라 제조업에서는 가공조립산업이 비제조업에서는 서비스산업이 발전하고 전체적으로 소프트화의 경향이 현저하며 그 중에서도 정보의 생산·유통에 관계된 산업과 같이 소위 창조성의 발휘를 기초로 한 지식집약형 및 고부가가치형 산업구조로의 전환이 이루어지며 이를 기초로한 고부가·고소득의 경제체제가 이루어지게 된다.

이와 같이 정보사회에서는 정보와 사회의 관계가 기존의 사회와는 다른 좀더 이상적인 방향으로 흐른다는 것이 자유주의적 관점에서의 주장이다. 이러한 정치, 문화, 경제적 변화는 정보의 영향을 받음과 동시에 정보에 영향을 미치면서 좀더 편안하고 안정된 사회로의 진행을 유도한다는 것이며 이러한 변화 가운데 개인과 조직 그리고 사회가 하나로 연결되는 새로운 사회가 바로 정보사회인 것이다.

### 3. 2 디스토피아적 견해

정보사회에 대한 이미지가 유토피아적 낙관론만 존재하는 것은 아니다. 막스(Marx)주의적 전통은 정보와 사회의 관계를 오웰린(Owellian)의 관점에서 디스토피아와 연계시켰다. 이러한 관점은 개인의 자유와 사회적 행위 전체가 정보기술이나 정보체제를 분배하는 수단을 소유한 사람이나 단체, 기구 등의 불순한 동기에 의해서 서서히 잠식해져 가는 것을 주시하였다. 이 관점에 의하면 정보의 복합성과 투과성이 오히려 사회 속의 인간을 통제하는 도구의 필요성과 가능성을 제시하게 된다는 것이다.

이러한 막스주의적 전통은 비관적인 현실을 들어 정보와 기술의 발전이 인간 또는 사회 전체를 분열시키는데 앞장선다고 보았다. 정보사회의 구조적 변화에 따라 생기는 사회구조와 개인별 역할 구조간의 갈등, 정치체계상의 관리문제, 기존의 전통적인 문화적 성향에 도전 등과 새로운 기술과 매체의 등장에 따른 사회 경제적 격차가 오히려 기존의 사회체제보다 불안하고 불편한 상황으로 유도되고 있다는 점을 주시하며 이는 궁극적으로 인간의 예속화를 초래한다고 보고 있다.

이러한 정보사회의 비판적 견해를 구체적으로 몇 가지 살펴보면, 첫째, 개인정보의 유출과 사생활 침해의 문제이다. 국민개개인의 정보가 국가나 기업·단체·사회집단에 의해 광범위하게 수집되어 컴퓨터에 수록되고, 자기도 모르는 사이에 누설되거나 부당하게 이용된다면 개인의 사생활을 보호받기가 어려운 것이다. 이러한 사생활 침해가 의도적으로 이루어지거나 단순한 착오에 의한 것이든지 간에 인간들이 고도로 발달된 커뮤니케이션 수단에 의해 철저히 감시 받게 되면 인간의 존엄성과 개인적 비밀이 유지되기 어렵게 되며 신종범죄의 증가를 초래하게 된다.

둘째, 사회를 구성하고 있는 개인간 또는 국가간 정보격차의 문제이다. 정보격차(information gap)란 정보에의 접근, 정보처리 및 전달 기술의 차이, 그리고 이러한 정보를 처리할 수 있는 능력의 차이 등 복합적인 의미를 내포하고 있다. 예컨대 정보사회가 컴퓨터와 통신의 결합으로 이루어진 새로운 매체를 기저로 한다고 볼 때, 사회경제적 지위에 따라 뉴미디어를 수용할 수 있는 시기성의 차이, 운영의 수준차이 등이 생기게 되며 이들의 격차는 산업사회의 그것보다 훨씬 크며 위험한 것이다. 이러한 정보격차는 국가간에도 같이 적용되며 정보사회란 바로 이러한 격차에서 비롯된 갈등을 의미하게 되는 것이다.

셋째, 정보화의 심화에 따른 비인간화의 문제이다. 정보사회에서 인간들의 중요한 문제는 정보부족 현상보다 인간에게 쏟아지는 정보를 어떻게 조직하고 처리하며 통제하는가 하는 것이다. 이러한 결과는 정보기술과 발전

으로 이어지게 되며 효율과 결과를 중시하는 사회적 구조에서 결국 인간성의 상실을 초래하게 된다. 또한 정보화·기계화는 자칫 대인 커뮤니케이션의 소홀로 이어지면서 비인간화의 현상을 부채질하게 되는 것이다. 또한 가상공간의 확대로 인한 현실도피와 비인간화도 경계하여야 할 과제로 떠오르게 되는 것이다.

넷째, 과잉정보에 관한 문제이다. 정보사회에서는 유용한 정보를 대량생산하여 공급함으로써 개인들의 선택의 폭을 넓혀주어 의사 결정에 큰 몫을 담당하지만 이러한 정보를 모두 소화시키지 못한 결과 발생하는 정보과잉 현상을 야기한다. 이러한 정보공해의 결과 정보에 지배되고 압박 받는 수동적 인간상이 제조될 수 있으며 정보에의 무감각·무기력 사태를 야기하여 결국은 정치·사회적인 문제로의 역기능을 초래할 수도 있다. 더욱이 이러한 정보의 진단이 창조적 소수(creative minority)에 의한 채널로 전달될 때 과잉정보의 문제점의 심각성이 있는 것이다.

다섯째, 정보와 커뮤니케이션 기술을 비롯한 과학기술의 비약적 발달로 인해 인간은 기술의 발달속도에 적응할 수 없게 된다. 이러한 문화지체는 사회구성원간의 심리적·사회적 괴리감을 조성하게 되며 발전된 과학기술의 열매가 사회에 공평히 분배되지 못하는 문제점을 야기한다. 다시 말해서 새로운 정보기술의 발달은 사회구성원의 의식을 깨우쳐 삶의 욕망을 불러일으키지만 지나친 기대상승은 개인이나 사회전체의 좌절을 초래할 수도 있게 된다. 나아가 극단적인 견해는 개인이나 사회해체의 가능성을 암시하기도 한다.

여섯째, 국가간 정보유통 분쟁의 문제이다. 정보통신의 발달은 지구촌(global village)을 형성하는데 기여해왔다. 그러나 그 이면에는 선진국들의 기술안보의 주력과 후진국의 시장방어의 갈등이 숨어져 있으며 각국은 정부와 기업이 공동의 힘을 극대화시켜 기술 시장 점유경쟁에 전력을 다할 것이며 이는 국가간의 전쟁으로 간주되는 문제이기도 하다. 이러한 문제는 정보가 지닌 특성상 국가들이 밀집되어 있는 지역에서 특히 심각한 문제가 되는 것이다.

이와 같이 정보사회는 낙관론만이 아닌 많은 문제점을 내포하고 있다. 간략히 살펴보았듯이 이러한 양대 사상적 견해의 논쟁은 각각 서로 단면적이며 한 견해의 주장이 다른 관점의 문제점이 되는 것이다. 즉 각각의 주장은 어느 정도의 타당성이 있으나 정보사회에서의 정보와 사회의 관계를 일반적으로 설명하지 못하고 있는 것이다. 그것은 정보와 사회의 관계를 이해하는 사상과 분석의 시각차이에서 오는 것이지 정보의 내재적 구조에서 기인하는 것은 아니다. 그러므로 정보와 사회의 관계는 위의 두 가지 사상적 기반 위에 같이 통합하여 볼 때 전체적인 이해로 구하게 되는 것이며, 정보사회의 이해에 관한 위의 두 가지 관점은 상호보완적이어야 하며 배타적일 수가 없는 것이다.

## 4. 정보보안의 이해

정보사회의 도래에 따른 이해와 관점이 어떻든지 정보사회에서 중요한 사안 중의 하나가 정보보안의 문제이다.(송인애 1998; 조찬식 1999b) 정보는 원래 적정보고(敵精報告)의

가운데 두 자를 줄여서 표현한 것으로, 결국 그 정보의 내용을 알아야 하는 사람이 있고, 알아서는 안 될 사람, 즉 첩자로부터 보호되어야 한다는 보안이라는 측면을 내포하고 있다. 이는 정당한 사용자가 필요한 정보를 알 필요성과 인가되지 않은 자는 그 정보에 접근할 수 없게 보호되어야 한다는 당위성에 기초한 의미를 말하는 것으로 진정한 정보사회의 성패는 바로 이 정보보안의 문제에서 비롯된다고 할 수 있다.

이러한 정보보안의 원인은 정보통신기술의 발달과 급격한 보급으로 인한 정보누수와 정보침해에서 찾아볼 수 있다. 정보사회에서 정보통신에의 접근성(accessibility)이 높아짐에 따라 정보의 이용이 용이해졌으며 이에 따른 정보의 노출이 불가피하게 되었다. 과거에는 특정 계층만이 정보통신에 접할 수 있었으나 보편적 서비스의 개념 정립과 이의 실현은 정보통신의 이용이 정치적, 상업적, 문화적으로 가능케 하였으며 이에 따라 사회의 다양한 정보가 공개되어 지고 있다. 이러한 정보통신의 대중성과 개방지향성은 정보의 유출과 침해를 용이하게 할 뿐만 아니라 추적도 어렵게 만들어 놓고 있다. 아울러 망(network)의 개념으로 형성된 정보통신체계는 각종 정보원의 공개가 자연스럽게 이루어지고 이에 따른 정보침해나 해킹(hacking) 그리고 각종 버그의 발생과 확산을 가능케 하고 있다.(정용섭 1995; Strebe, Perkins and Moncur, 1999) 또한 이렇게 만연된 정보통신을 이용하고 활용하는 인적자원의 정보보안에 대한 인식과 관리 능력의 부족은 정보보안의 문제를 증폭시키고 있다.

그러므로 바람직한 정보사회의 정립을 위하여 필요한 정보는 보호되어야 하며, 이러한 정보보안은 유통되는 정보나 데이터의 보호뿐만 아니라 이들을 작동하는 각종 소프트웨어 및 정보유통을 가능케하는 정보통신시스템, 정보통신 네트워크 등에 대하여 광범위하게 이루어져야 하며 내부 사용자나 일반 이용자에 대한 관리와 교육을 통한 의식과 능력의 변화 등 근본적이고 체계적으로 실현될 때 효과적으로 이루어질 수 있는 것이다.

이러한 정보보안의 기본요소는 비밀성과 무결성 그리고 가용성 등 세 가지로 나누어 설명할 수 있다.(Farley, Stearns and Hsu 1997) 첫째, 비밀성(confidentiality)은 보안공격으로부터 전송자료를 보호하기 위하여 전송 또는 보관중인 정보를 비인가자가 부정한 방법으로 입수하더라도 그 내용을 알 수 없도록 보호하는 것이다. 가장 일반적인 비밀성 서비스는 두 사용자 사이의 모든 전송자료를 일정기간 보호하는 것과 전송되는 메시지내의 특정 필드에 대한 보호 등이다. 비밀성을 보장하기 위해서는 운영절차 및 지침, 접근제어, 정보암호와 기법, 인증시스템, 보안소프트웨어 등으로 위험에서 안전하게 보장받을 수 있다.

둘째, 무결성(integrity)은 전송 또는 보관중인 정보가 인가되는 방법으로 위조 또는 변조할 수 없도록 보호하는 것으로서 메시지 스트림, 단일메시지, 또는 메시지 특정 필드에 적용할 수 있으며, 연결형과 비연결형의 두 가지가 있다. 연결형 무결성 서비스는 메시지가 원래 송신된 그대로 수신되었음을 확인하는 것이며 전송되는 자료에 대한 파괴와 위해 및 불법수정과 서비스부인도 이에 포함된다. 비연결형 무결성 서비스는 개인 메시지만을 대

상으로 하며 일반적으로 메시지 불법변경으로부터 보호하는 것이며 이 서비스는 복구를 포함하는 경우와 포함하지 않는 경우가 있으며 적극적으로 공격과 연관되기 때문에 예방보다는 발견이 더 중요하다.

셋째, 가용성(availability)은 정당한 사용자가 인가된 방법으로 적시에 정보시스템에 접근하여 이용할 수 있는 것을 의미한다. 이러한 가용성을 확보하기 위한 통제 수단으로는 데이터의 백업(backup), 중복성 유지, 물리적 위험요소로부터의 보호 등이 있다.

이러한 정보보안의 필요성은 다음과 같이 다섯 가지 측면에서 살펴볼 수 있다.(한상완 1997) 첫째, 정상적인 정보의 기능유지 측면에서 볼 때 정보는 고유한 사용 목적과 기능을 유지해야하고 필요한 장소, 필요한 사람, 필요한 시점에 정확히 전달되어야 한다. 그러나 정보자체가 무결성이나 비밀성 등을 보장하지 못하며 무용지물이 될 소지가 많으므로 정상적인 정보의 기능 유지를 위해 정보보안이 필요하다.

둘째, 자산의 보호측면에서 정보는 정보에 관련된 모든 자산, 즉 하드웨어, 소프트웨어, 데이터 등의 손실과 왜곡으로 막대한 재정적 손실을 초래할 수 있으므로 정상적인 정보통신망 운영과 정보에 관련된 모든 재산권 보호를 위해 정보보안이 필요하다.

셋째, 개인정보의 보호측면에서 정보는 정보통신망의 확대와 컴퓨터 보급확장 등으로 인한 정보의 집중화를 가져왔고, 정보의 수집과 이용이 활성화 다양화되어 가고 있다. 이에 따른 개인정보의 침해 가능성도 증가되어 가고 있어 개인의 프라이버시(privacy)보호를 위해서 정보보안이 필요하다.

넷째, 국가안전에 관한 측면에서 정보는 정보통신망을 통한 국가기밀정보의 유출, 파괴, 훼손의 가능성이 매우 크고, 정보통신망의 보안 헛점으로 인한 국가기밀정보의 위협은 국가경쟁력 약화까지 초래할 수 있으므로 국가의 안전보장을 유지하기 위해서 정보보안이 필요하다.

다섯째, 정보윤리의 확보측면에서의 정보의 건전한 유통질서와 안전한 거래를 보장할 수 있는 유통질서 확립과 정보의 역기능을 예방·방지할 수 있는 정보윤리의 확보를 위해 정보보안이 필요한 것이다.

## 5. 정보침해의 유형

정보의 유통 방법과 경로가 활발해지고 다양해지면서 정보보안이 더욱 중요해 지는 것은 그만큼 정보의 침해와 누수가 확산되어가고 있음에 기인하는 것이며 전술한 정보통신의 특성상 정보침해의 수법이나 기술은 점점 지능화 되어가고 있는 실정이다. 정보사회에서의 정보보안의 확립은 이렇게 다양한 정보침해에 대한 이해를 기초로 이루어져야 하며 이러한 정보침해에 대한 연구와 분석이 계속적으로 진행되어져야 할 것이다.

정보침해, 즉 정보시스템에 대한 공격방법에는 몇 가지 유형을 살펴볼 수 있는데, 하드웨어에 손상을 주는 것과 같이 직접 시스템에 접근하여 손상을 입히는 물리적인 공격과 정보 또는 소프트웨어에 손상을 주는 것으로 전산망이나 기타 전산장비를 사용하여 시스템 내부에 침투하는 기술적인 공격이 있다. 또한

정상적이지 않은 방법을 통해 시스템에 침투하여 보안에 손상을 주는 유형으로 '해킹(Hacking)'과 '크래킹(Cracking)'이 있는데, 해킹은 정상적인 규칙을 따르지 않고서도 하고자 하는 일을 하는 것인 반면, 크래킹은 불법적인 수단으로 시스템에 침투해 시스템을 파괴하는 것으로 요즘은 쉐어웨어(Shareware) 등의 락(Lock)을 해체하여 사용하는 행위를 가리키기도 한다. 시스템에 어느 정도의 손상을 주는지 여부에 따라 해킹과 크래킹을 구별하기도 하지만 둘 다 정상적인 방법이 아니란 점에서 대책이 마련되어야 하는 것이다.(김태봉 1997; 김태헌 1997)

일반적으로 인지된 정보침해의 유형 몇 가지를 살펴보면 다음과 같다.(유승렬 1998; 조찬식 1999b) **트로이 목마**(Trojan Horse): 그리스 로마 신화에 나오는 이야기로 상대방이 눈치채지 못하게 몰래 숨어드는 것을 의미하듯이, 정상적인 프로그램에 트로이 목마라는 부정 루틴(routine)이나 명령어를 삽입해 정상적인 작업을 수행하나 부정 결과를 얻어내고 즉시 부정 루틴을 삭제하기 때문에 발견이 어렵다. 주로 주프로그램이 미작동시에 해당 통신망의 정보를 유출시킨 후 가입자들의 통신망에 접속할 때 누르는 첫 12자를 따로 복사해 두었다가 후에 정보를 넘기는 양식으로, 시스템 프로그래머, 프로그램 담당 관리자, 오퍼레이터, 외부 프로그램 용역자가 저지르며 시스템 로그인 테이프와 운용 기록이 있는 프로그램 리스트를 확보한 후 정상적인 프로그램 실행 결과와 의심스런 프로그램 결과를 비교하는 것이 예방책이다.

**취약점 공격**(Exploits): 주로 호스트 프로그램상의 오류나 서비스 방해공격이 불법적으로 이루어지며 시스템 버그를 이용하여 이를 보안 취약점(Security Hole)으로 활용하는 경우로, 프로그래머 자신이 프로그램을 만들던 시점에 생긴 버그를 기억해내거나 우연히 버그를 알게 되었을 때 발생하여 상당히 빠르게 시스템을 공격하며 일단 공격을 받게되면 회복이 매우 어렵다. 시스템의 취약점을 이용한 공격에 대비하기 위해서는 시스템 개발 시 보안기법의 구현이 요구되며, 시스템의 버그가 침입하지 못하도록 보안 취약점은 새로운 버전의 수정 프로그램으로 시스템 변환이 이루어져야 한다.

**구조적 공격**(Infrastructure Attack): 시스템이나 네트워크 프로토콜의 구조적인 문제점을 단순히 호스트의 어드레스를 바꾸는 방법으로 공격하는 수법으로 도메인 네임 스푸핑(Domain Name Spoofing), 쏘스라우팅(Source Routing), TCP Squence, Guessing 등이 이에 해당되며 매우 복합적으로 사용되고 있다. 스푸핑은 '속이다' 또는 '사기치다'란 뜻으로 보안이 잘되어 있는 호스트 사이에서 한 쪽의 어드레스로 침투하여 호스트를 잠시 상실케 한 뒤 상대방 호스트로 위장전입하여 필요한 정보를 빼어내 오는 방법으로 정밀한 인증체계를 실행함으로서 이러한 구조적 공격에 대응할 수 있다.

**사용자 도용**(Impersonation): 정당한 사용자의 ID를 도용하는 경우로서, 네트워크의 한 호스트에서 실행되어 그 주위를 지나다니는 패킷을 엿보는 프로그램인 스니퍼(Sniffer)를 이용하여 네트워크 접근시의 ID와 패스워드 등을 도용하는 방법을 가리킨다. 또한 최근에는 비합리적인 패스워드를 통해 시스템에 접

근하자는 목적에 의해 만들어진 프로그램인 크랙(Crack)을 이용해 손쉽게 비밀번호를 추출해 내기도 한다. 이와 같은 사용자도용은 모두 ID나 패스워드의 제작이나 보안의 허술함에서 비롯되며 이를 방지하기 위해서는 패스워드의 추측이 가능하면 어렵게 하거나, 패스워드를 만드는 프로그램을 사용하여 정기적으로 바꾸어 주며, 좀 더 확실한 보안을 위해서는 물리적인 사용자를 확인하거나 암호화를 강화하는 방법을 생각할 수 있다.

**서비스 방해공격**(Denial of Service Attack) : 시스템의 정상적인 동작을 방해하는 공격 수법으로 대량의 데이터 패킷을 네트워크로 보낸다든가, 전자우편으로 보내는 식의 공격이 많으며, 각종 메일 폭탄을 전송하여 시스템의 서비스를 혼란케 하는 경우이며, 이와 같이 전형적인 메일 폭탄 사건은 이미 세계적인 추세로 나타나고 있다. 이러한 서비스 방해공격에 대한 대응책은 스팸메일이 도착했을 경우 리스트를 설정해 다음부터 스팸메일을 보내는 전자우편 주소로부터는 메일을 받지 않도록 스팸메일을 차단하거나, 수신되는 메일의 크기, 범위, 수준 등을 제한하여 문제가 되는 메일 폭탄을 차단하거나, 시스템의 배치를 바꾸어 메일 폭탄이 도착했을 때 대처하는 방법 등의 대책을 마련할 수 있다.

이상의 정보침해 경우 외에도 통신 출입구가 전자적 또는 기계적으로 잠겨 있어 자유롭게 접근할 수 없는 경우에 불법 단말기를 설치하여 물리적으로 출입구를 여는 방법인 피기백, 목표 호스트가 신뢰하는 시스템이나 네트워크로 잠시 위장하여 침입하는 시스템 위장(Transitive Trust), 컴퓨터 시스템내에서 프로그램을 파괴시킬 수 있는 프로그램을 침투시킨 후 정해진 조건이 되면 자동적으로 논리적 폭탄효과를 얻는 컴퓨터 바이러스(Compute Virus)나 논리파괴 폭탄(Logic-Destructive Bombing), 그리고 보통 케이블 및 와이어, 지상 마이크로파 시스템, 통신용 인공위성 등 통신의 약점이라 알려진 통신회선 부분에 누수를 위한 장치를 부착하여 컴퓨터간의 통신내용이 간파되는 것으로 A와 B가 통신하고 있는 내용을 C가 엿보는 도청 등을 포함한 전자적 누수 또는 통신 누수 등 정보침해의 종류와 유형 매우 다양하며 광범위하다.

이러한 정보침해의 유형들은 대략 시스템이나 네트워크 중심으로 발생되고 있으며 아래 〈표 1〉과 같이 요약해 볼 수 있다.

〈표 1〉 정보 침해의 유형

| 분 류 | 예 | 설 명 |
|---|---|---|
| 시스템 | 관리자 및 사용자 부주의 | 추측이 쉬운 패스워드 사용,<br>부주의한 시스템 신뢰관계 설정,<br>사용자/퇴직자 미확인 또는 관리 부주의 |
| | 응용프로그램 버그 | 응용프로그램의 보안 관련 버그 |
| | 구성 오류 | 응용프로그램 구성상의 보안 관련 오류 들 |
| 네트워크 | 구조적 취약점 | 프로토콜 설계상의 보안 취약점 |
| | 응용프로그램 버그 | 네트워크 서비스 프로그램의 보안관련 버그들 |
| | 구성 오류 | 네트워크 서비스 구성상의 보안관련 오류 들 |

지금까지 살펴본 바와 같이 정보화의 심화는 정보통신에의 접근을 용이하게 하였으며 이에 따른 정보침해의 방법은 매우 복잡하며 다양하다. 사회의 구조가 정보와 이를 유통시키는 통신에 가치를 두고 이들을 중심으로 변화하는 시점에서 이러한 정보침해나 정보의 누수란 건전한 정보사회의 질서를 파괴하고 나아가 사회의 기본구조마저도 붕괴시킬 수도 있는 것이다. 그러므로 진정한 정보사회의 성패는 이러한 정보침해 또는 정보누수를 어떻게 해결하느냐에 달려있다 해도 지나침이 없는 것이다.

## 6. 정보보안의 전략

정보사회에서의 정보보안은 가장 우선시되어야 하는 과제이다. 즉, 필요한 정보가 생성되고, 유통되어, 이용되기까지 공개된 정보통신의 환경에서 어떻게 보호받느냐 하는 것이 정보사회를 정착시키는 중요한 요소 중의 하나인 것이다.(임휘선 1997; 최종욱 1997) 따라서 정보침해 및 누수에 따른 문제점을 극복하고 정보보안을 유지하여 정보사회의 기초를 확립하는 방안이 체계적으로 강구되어야 할 것이며, 이러한 정보보안의 전략은 기술적인 측면과 법적, 제도적 측면으로 구분되어 연구·분석될 수 있다.

### 6. 1 기술적 측면에서의 정보보안

정보사회에서의 정보보안을 기술적인 측면에서 살펴보면 비밀성(confidentiality), 인증(authentication), 무결성(integrity), 부인방지(non-repudiation)를 전제로 한 인증체계와 암호화를 이룸과 동시에 방화벽(firewall)을 구축하는 등 다각적인 시스템적 접근에서 이해할 수 있다.

#### 6. 1. 1 암호화 기법

암호화(Encryption)는 데이터를 특정한 처리를 통해서 침입자 혹은 파괴자가 데이터를 입수하더라도 그 내용을 알 수 없도록 만드는 것을 말한다. 전자메시지를 암호화하는데는 다음 다섯 가지의 원칙을 따라야 한다.(조찬식 1999b) 첫째, 신원 확인(Identification)이란 메시지를 보낸 사람이 실제로 그 사람인지를 확인하는 과정이다. 암호화에서는 봉인을 하고 인장을 찍을 장소가 없기 때문에 신원확인은 코딩된 정보를 통해 확실하게 출처를 밝힌다는 개념에 의존하고 있다. 둘째, 인증(Authentication)이란 암호문의 원래 전송자를 확인하고 메시지 전문이 제대로 전달이 되었는지를 확인하는 절차를 말한다. 공용키 체계에서의 인증 절차에는 디지털 서명이 필요하다. 인증과정에서 공용키는 개인키로 암호화된 메시지 암호를 해독하는데 사용된다. 셋째, 발신자 확인(Non-repudiation)으로 메시지이나 파일을 보낸 사람이 그것을 부인할 수 없도록 만드는 보안체계이다. 넷째, 확인(Verification)으로 어떤 암호화된 통신과정에서 신원확인과 인증을 한 번에 처리하는 것이다. 이 두 가지가 모두 사실로 판명돼야만 메시지를 완전히 믿을 수 있다. 다섯째, 개인정보 보호(Privacy)로 정보 전달 시 해킹으로부터 보호하기 위한 암호 시스템 기능이다.

암호화를 수행하기 위해서는 일반적으로 키(key)가 사용된다. 암호화된 데이터를 원상으로 복구하는 것을 복호화(Decryption)라고 하는데 이 과정에서도 일반적으로 키를 사용하게 된다. 암호화 방법은 정보를 보내는 사람과 받는 사람이 사용하는 키의 상이 여부에 따라 단일키(비밀키, 대칭적) 암호시스템과 이중키(공개키, 비대칭적) 암호시스템으로 구분된다. 단일키 암호기법은 일 대 일의 이용자 서로가 같은 키를 소유하고 송신자가 비밀키를 이용하여 암호화한 것을 수신자가 비밀키를 이용하여 복호화 하는 방식이고, 이중키 암호기법은 암호화할 때와 복호화할 때 사용하는 키가 서로 다른 방식으로 하나를 비밀키라고 하고 나머지를 공개키라 하며 주로 일 대 다수의 이용자간에 사용된다.

이러한 암호화의 몇 가지 기법을 살펴보면 다음과 같다.(신일순 1998; 조찬식 1999b) 첫째, DES(Data Encryption Standard)는 1970년대에 IBM에 의해 개발된 NBS(National Bureau of Standards)의 유명한 데이터 암호화 알고리즘이다. 64비트 데이터 블록 단위로 암호화를 하며 이 과정에서 56비트의 키를 사용하게 된다. 이 방식은 동일한 키로서 암호화, 복호화를 수행한다. 따라서 새로운 사람과 통신하고자 할 때는 키가 전달되어야 하는 과정의 보안이 힘들고 키의 보관 역시 어려운 면이 있다. 그럼에도 불구하고 공개키 알고리즘에 비해 훨씬 간단하므로 암호화하는 속도가 월등히 빠르고 크기가 작아서 경제적이다.

둘째, RSA(Rivest, Shamir, Adleman)는 암호화와 사용자 인증을 동시에 수행하는 공개키(Public Key) 기반의 암호화 기법으로서 1977년에 Ron Rivest, Adi Shamir, Leonard Adleman이 개발하였고, RSA는 이들의 머리글자를 따서 만든 이름이다. 이 방식에서는 공개키(Public Key)와 비밀키(Private Key)를 사용하는데 공개키는 일반에 공개되는 반면에 비밀키는 본인만이 알고 있게 해서, 데이터의 암호화는 물론이고 수신된 데이터의 부인봉쇄(Non-Repudiation)의 기능까지도 하게 된다. 이러한 공개키 암호 방식은 한 개의 키를 누구에게나 알려주어도 무방하므로 공개적으로 전달할 수 있다. 또한 비밀키 암호 방식처럼 통신을 할 때 비밀키를 전달할 필요가 없기 때문에 필요한 키의 수도 줄어들 뿐만 아니라 키 관리의 보안 문제가 쉬워진다. 이러한 방식은 비밀키 방식에서는 불가능한 디지털 서명과 같은 기능을 가지고 있다. 그러나 사용하는 키의 크기가 크고 알고리즘이 복잡하여 실행 속도가 느리고 구현하기가 힘들다는 단점이 있다.

셋째, PEM(Privacy Enhanced Mail)을 살펴보면, 전자우편을 사용할 때 우편은 SMTP(Simple Mail Transfer Protocol)을 통해서 전송된다. 그러나 이 프로토콜에서는 우편을 텍스트 형식으로 전송하므로 전송 경로 중간에서 가로채어 그대로 해석할 수 있다. 우편을 암호화된 형태로 보내기 위해서는 암호화에 사용된 키를 수신자에게 어떻게 보낼 것인가 하는 것은 또 다른 문제가 된다. PEM은 RSA를 사용하는데 우편을 전송하기 전에 미리 자동으로 암호화하여 전송 도중에 데이터가 유출되더라도 암호화된 우편의 내용을 알아볼 수 없게 된다.

넷째, PGP(Pretty Good Privacy)는 미국의

Philip Zimmermann이 일반 사람들에게 비싼 암호 체계의 혜택을 받을 수 있도록 하기 위해서 개발하였다. 사용하기 쉽고 우수한 성능으로 초기에는 공개된 PGP 프로그램을 많은 사람들이 사용하였으나 40비트를 초과하는 긴 키를 사용하기 때문에 미국의 무기 수출법에 저촉되어 미국 이외에서는 사용할 수 없게 되었다. 요즘에는 미국 이외의 국가에서도 사용할 수 있도록 키의 길이를 제한하는 방법으로 프로그램이 제공되고 있다. 메일을 암호화하여 도청을 방지할 수 있으며 공개키 암호방식을 이용한 전자 서명 장치를 채용하고 있기 때문에 함부로 고치는 것도 방지할 수 있다.

정보보안에 있어서 암호화 알고리즘과 키의 길이가 매우 중요하지만 또 한가지 중요한 요소는 바로 보안프로토콜이다. 암호화 알고리즘 기술은 이미 상당한 수준으로 연구가 진행되어 있다. 그러나 자료가 암호화되었다고 무조건 다 안전한 것은 아니다. 강한 알고리즘으로 암호화되었다고 하더라도 여전히 보안침해의 가능성은 많이 있다. 이런 것을 막아주는 것이 보안프로토콜이다. 예를 들면 WWW보안에는 SSL(Secure Socket layer), SHTTP 등, 전자우편에는 PEM, S/MIME 등과 같은 보안프로토콜이 있다. 이렇듯 안전한 정보교환을 위한 정보보안시스템에도 암호화 알고리즘뿐 아니라 보안프로토콜이 매우 중요한 요소가 된다. 따라서 인터넷의 특성인 개방형 네트워크상에서 인증, 키교환, 암호화, 무결성 등 보안 서비스를 구현하기 위한 네트웍 차원의 보안 프로토콜에 대한 표준에는 PTP(Point-to-Point, Tunneling Protocol), IPSEC(IP Security), SSL 등이 대표적이다. SSL은 넷스케이프가 웹서버와 클라이언트간의 안전한 통신을 위해 전송단계에서 공개키 암호화 기술을 활용하여 개발한 프로토콜로서 범용적으로 많이 활용되고 있다.

6. 1. 2 인증서비스

인증시스템이라는 것이 아직은 새로운 개념이기는 하지만, 기존의 계약 서류에 날인을 하고 인감증명서를 첨부하는 것과 같은 개념으로 생각한다면 쉽게 이해가 될 것이다. 이와 같은 인증은 일반적으로 두 가지 의미로 요약할 수 있다. 첫째, "Authentication"으로 사용자 인증이나 메시지 인증을 의미하는 것이고, 둘째가 "Certification"으로 비대칭형(공개키) 암호방식으로 공개키의 무결성을 보장하기 위해 인증기관에서 발행하는 인증서의 의미로 나누어 생각할 수 있다. 일반적으로 이 두 개념은 혼용되어 사용되고 있으나, 최근에 이슈가 되고 있으며 사용되는 인증의 의미는 인증기관으로부터 파생되는 "Certification" 서비스를 지칭하게 되었다.(안혜연 1999; 허금 1998)

이러한 인증서비스의 필요성은 공개키 암호화를 사용하는데서 시작된다. 안전한 정보통신환경의 구축을 위해서는 인증, 무결성, 비밀성, 부인봉쇄 등의 정보보호 서비스가 요구되며 이의 실현은 전자서명 기술을 활용함으로써 해결이 가능하다. 현재 안전성을 유지시킬 수 있는 공개키 암호 방식의 전자서명 기술이 가장 우수하다고 알려져 있으며 실제 적용을 위해서는 인증서비스가 필요하다. 따라서 인증기관은 전자서명을 이용하고자 하는 사용자들에 대해 인증서 발급 서비스를 제공해주고 이윤을 창출하거나 기업내 안전한 전산망 구축을 담당하는 하나의 조직이라 할 수 있다.

여기서 인증 서비스란 인증기관이 제공해주는 인증서 발급, 인증서 관리 등 일련의 인증 관련 서비스를 통칭하는 것이다.

이와 같은 인증서비스는 인증을 받는 사용자와 관리자가 올바른 이해가 필수적이며, 사용자들은 인증의 신청 절차, 획득 방법, 인증서의 사용 범위, 폐기 및 재발급 절차, 암호화 및 전자서명 key의 관리, 개인의 보안통제 기준 등을 이해하고 있어야 하며 또한 권한과 책임에 대해서도 올바른 의미를 파악하고 있어야 할 것이다. 같은 의미로 공증사무소(CA: Certificate Authority) 관리자들도 인증을 발급 받을 사용자의 식별과 키의 생성, 보증 등급의 부여, 확장 필드의 정의, 폐기의 처리 등 정책상의 물리적·기술적 보안 통제의 기준 등을 사전에 파악하고 있어야 한다.

인증서비스의 분류는 인증기관이 발급하는 인증서의 응용 분야에 따라서 나뉘어 진다. 현재 정보통신망과 컴퓨터 네트웍 기술의 발전으로 말미암아 대부분의 영역에서 정보보호 필요성이 대두되어 있으며, 이것에 대한 해결책으로서 암호기술의 사용이 권장되고 있다. 이중에서도 공개키 암호화 알고리즘을 이용한 전자서명 기술의 활용은 인증, 무결성, 부인방지 등의 정보보호 서비스를 제공해 주는 효과적인 기법으로 자리잡고 있다. 이러한 현황으로 인하여 컴퓨터 네트웍 보안과 관련된 많은 국제 표준화 단체나 개발 업체들이 공개키 암호 기술이 적용된 프로토콜이나 제품들을 출시하고 있는 상태이며, 이것은 상업적 목적을 갖는 인증기관 탄생의 기반이 되었다.

일반적으로 인증서비스는 두 가지 분류로 나뉘어진다. 첫번째는 앞에서 언급한 바와 같이 범용적인 보안 프로토콜의 확산으로 인해 요구되는 인증서비스이다. 이 경우 인증기관은 각 객체들에 대해 인증서를 발급하고, 이에 대한 수수료를 받음으로써 경제적 이득을 취하게 된다. 두번째는 안전한 인트라넷, 익스트라넷, 기업망, 폐쇄 네트워크 시스템 등의 구축을 위해 요구되는 인증서비스로서, 이 경우 사업자는 인증서 발급에 대한 수수료를 목적으로 하는 것이 아니라 자사의 안전한 네트웍 환경 구축을 목적으로 하고 있다.

### 6. 1. 3 방화벽 (Firewall)

정보사회에서의 정보보안에 필요한 방화벽의 개념을 살펴보면, 방화벽은 인터넷의 보안 문제로부터 특정 네트워크를 격리시키는데 사용되는 시스템이다.(Siyan and Hart 1996) 즉 문제시되는 외부의 불법적인 침입으로부터 내부를 보호한다는 뜻이다. 일반적으로 방화벽 자체는 중요한 정보를 갖고 있지 않으며, 외부로부터의 접근도 대부분 봉쇄되어 해킹 위험으로부터 보호되기 때문에 보안의 구멍은 보완을 위한 방화벽 기술의 주목을 부추기고 있으며, 보안을 안전하게 유지하기 위해서는 방화벽을 효과적으로 운영 및 관리해야 하는데 이를 부적절하게 운영 관리함으로써 많은 보안 문제가 발생하게 된다.

그러나 일면 방화벽은 완벽한 보안능력을 발휘하지는 못한다. 왜냐하면 방화벽은 외부로부터의 공격을 막는 역할만 하기 때문에 내부에서 자행되는 해킹 행위에는 속수무책이기 때문이다. 하지만 현재 보안시스템에서 가장 널리 사용되는 방화벽은 크게 두 가지의 목적을 갖는다. 첫째, 외부로 나가는 네트워크의 IP

주소를 위장하여 그것이 마치 방화벽에서 발생한 것처럼 하는데 사용된다. 이를 위해서는 네트워크에 포함되어 있는 모든 클라이언트들은 반드시 방화벽을 거쳐서 외부 네트워크로 나가도록 해야만 한다. 이렇게 하는 이유는 특정 네트워크에서 외부로 나가는 데이터들을 감시하고 있는 해커가 결국 해당 네트워크에서 사용되는 개별 IP 주소를 알게되고, 해커가 클라이언트처럼 가장해서 접근할 수 있기 때문이다. 둘째, 해당 네트워크로 들어오는 패킷에 대한 IP 필터링(filtering)을 하는 것이다. 즉 자신의 네트워크에 이유없이 접근하는 IP 주소를 걸러낼 수 있도록 한다.

방화벽의 보호메커니즘의 종류는 방화벽이 운용되는 프로토콜 계층의 위치에 따라 구분되며, 대부분의 방화벽은 네트워크 레벨이나 어플리케이션 레벨에서 동작한다. 네트워크 계층 방화벽은 보통 소스 어드레스, 목적지 어드레스, 그리고 포트 번호를 가지고 트래픽 통과를 필터링하는 전형적인 하드웨어인 라우터를 포함한다. 만약 패킷이 정당한 IP 주소를 가진다면 라우터는 패킷을 다음 목적지로 보낸다. 요즘의 라우터는 의심스러운 패킷을 정밀하게 조사함으로써 좀 더 지능적으로 진화하고 있다. 어플리케이션 레벨 방화벽은 대개 네트워크 레벨 방화벽보다 더 견고한 보안을 제공한다. 어플리케이션 레벨 방화벽은 그것을 통해 지나가는 트래픽을 좀더 정밀하게 조사하는 소프트웨어로 되어있어 패킷들을 보낼지 차단할지를 결정하는데 필요한 더 많은 정보를 제공하기 위해서 특정 어플리케이션 패킷상의 헤더 부분을 해석할 수 있다. 어플리케이션 방화벽은 좀 더 비싸고, 네트워크 상에서 각 어플리케이션마다 특정 프로그램이 필요하기 때문에 설정하기가 더욱 힘들다.

방화벽은 네트워크의 출입로를 단일화함으로써 보안 관리 범위를 좁히고 접근제어(access control)를 효율적으로 할 수 있으며 외부에서 불법으로 네트워크에 침입하는 것을 방지하면 내부의 사용자는 네트워크를 자유롭게 사용할 수 있다. 또한 방화벽에는 역추적 기능이 있어서 어떠한 네트워크 접근이라도 그 흔적을 찾아 역추적이 가능하여 시스템의 보안이 가능하게 되는 것이다. 그러므로 기업의 네트워크 관리자는 사내 네트워크에 방화벽의 보호없이 인터넷에 연결하는 일의 위험성을 인식해야하며, 인터넷상에서 사업을 하기 위해서는, 조직은 먼저 웹을 연결시키고 이를 보호하기 위해 네트워크 내에 방화벽을 설치해 관리해야 한다.

### 6. 2 제도적 측면에서의 정보보안

정보사회에서의 정보보안의 문제는 시스템적 정보보안 뿐만 아니라 제도적인 측면에서도 그 대책을 찾아 볼 수 있다. 제도적 측면에서의 정보보안 대책은 우선 법적인 측면에서의 정보보안이 이루어져야 하며, 전문인력의 양성 및 확보, 윤리적 의식의 확산, 전담기구의 설치 및 운영, 인력관리 및 교육, 정부의 역할 등으로 살펴볼 수 있으며 또한 이들은 상호 연계되어 있으므로 거시적 안목으로 분석되어야 하며 아울러 매우 구체적으로 실행될 때 진정한 정보보안을 유지할 수 있으며, 나아가 정보사회에서의 활발하고 효과적인 정보유통의 자리매김을 통한 정보화의 가속화를 이

루어 나갈 수가 있게 되는 것이다.

6. 2. 1 법적 측면

정보사회에서 정보보안을 위해서는 통일되고 명확한 법의 재정비와 이를 보호하기 위한 강력한 법적 조치가 확보되어야 하며 이러한 법적 재정비는 국내뿐만 아니라 국가간의 통일된 법안까지 포함되어 이루어져야 한다. 그리고 정보통신 이용시 개인의 프라이버시가 보장되고 유통되는 정보전달의 신뢰성을 구축하기 위한 법적 노력도 병행될 때 정보보안의 효과를 높일 수 있는 것이다.

현행 정보보안과 관련된 법규는 「컴퓨터프로그램보호법」, 「컴퓨터프로그램저작권법」, 「통신비밀보호법」, 그리고 「공공기관의 개인정보보호에 관한 법률」 등이 있다. 그러나 이러한 규정들은 그 내용과 범위에 있어서 불확실하고 애매모호한 면이 내포되었으며 법 집행의 강제성이 미약한 실정이다. 예를 들어 위의 법들은 원활한 전자상거래를 위하여 개인정보를 제공하는 것을 규정하고 있다. 그러나 어느 법규에서도 개인정보의 내용과 범위를 구체적으로 명시하지 않아 각각 전자상거래 상에서 제공하여야 할 정보가 달라질 수 있게 된다. 이렇게 제공되는 정보내용의 불확실성은 전자상거래상의 판매자나 구매자에게 정보 교환시 혼란을 초래하게 되어 심리적인 위축으로 인하여 전자상거래의 활성화를 저해하는 요인으로 작용하게 될 수 있다. 또한 전자상거래시 이렇게 다양하게 제공되는 개인정보는 도용 및 남용의 소지를 안고 있는 것이다.

또한 「공공기관의 개인정보보호에 관한 법률」에 의하면 이러한 개인정보를 보호하는 주체를 공공기관으로 한정하고 있다. 그러나 구체적으로 살펴보면 프라이버시의 침해의 구제에 대한 강제성을 가지지 않는다. 즉, 개인정보를 처리하는 행정기관에 대하여는 책임의무를 부여하고 있고 배상의 책임을 명시하고 있으나 기관에 대한 강제적인 시정명령이나 처벌의 규정이 없기 때문에 실제적인 면에서는 소극적인 보호정책을 택하고 있어서 보호의 실효성에 의문이 있다. 그러므로 안정된 정보유통을 위하여 법적으로 제공되어야 할 정보의 내용과 범위가 구체적으로 규정되어야 하며 공공기관으로 한정되어있는 법률의 한계가 사적인 부분까지 확대되어야 할 것이다. 아울러 이러한 정보 침해에 관한 폭넓은 교육과 함께 강경한 사후조치를 법률에 명시하여야할 것이다.

또한 정보유통의 국제화에 따른 초국가적 정보교환에 관한 기술문제가 종종 거론되고는 있지만 중요한 법률문제가 아직 해결되지 않은 채로 있어 세계적인 정보통신시스템의 운용에 걸림돌이 되고 있다. 국제적 정보통신시스템이 지속적으로 활기를 띨 것인지 여부는 국내·외 법규를 급속히 발전하고 있는 네트워크 인프라에 어떻게 전향적으로 적용할 것인지에 달려 있다. 많은 경우 현행 법규를 유추 적용할 수도 있겠지만, 발전하고 있는 기술에 비추어 충분히 검토되지 않은 기존 법규를 적용하는 것은 부적절한 결론을 이끌어낼 수 있기 때문이다. 이러한 법규의 파급효과에 대한 충분한 고려없이 기존 산업사회의 법을 바탕으로 한 법규를 국제적 정보화 문제에 적용한다면 명확성이 떨어져 국제적 정보통신시스템의 구현에 큰 해를 끼치게 될 것이다.

마찬가지로 국내적으로 정보화를 촉진하기 위한 각국의 입법 노력이 서로 상충된다면 전 세계적으로 일관성 있는 법제의 수립에 방해가 될 것이다. 이러한 우려는 한 나라 지역간의 일관성은 물론 국제적인 일관성에도 해당되므로 통일되고 조화로운 입법 노력이 긴요하게 요구된다. 국가간의 실체법이나 절차법이 불일치할 경우 국제적인 정보유통에 있어서 매우 복잡하고 예측할 수 없는 상황을 야기할 수 있는 것이다. 따라서 국경을 뛰어넘는 이용자들의 상호작용을 촉진하는 인터넷과 같은 개방 네트워크의 중요성이 증가함에 따라 보장(ensuring)에 관한 국제적 법률제도의 개발을 위한 통일된 노력이 요구되며 국제적으로 일관되고 통일된 규제법안을 마련해야 할 것이다.

아울러 정보사회에서 프라이버시 문제는 정보 이용자의 보호를 위한 수단으로 작용할 수 있기 때문에 매우 중요하다. 정보통신에 접근하기 위해서는 상대방 또는 대중에게 개인의 정보는 물론이고 소속기관에 관한 정보, 금융정보 등을 제공해야 하기 때문에 인터넷상에서 이용되는 정보망에 해킹이나 정보보안의 부주의로 개인정보가 인증되지 않은 타인에게 유포된다면, 이때 경제적, 정신적 피해는 상당할 것이다. 특히 정보사회에서의 프라이버시는 기존의 프라이버시 문제가 국내에 한정된 문제였지만, 개인정보가 통신망을 통하여 외국으로 유통되어질 수 있는 정보의 국제적인 유통(TDF : Transborder Data Flow)과 밀접한 관련이 있다고 할 수 있다. 정보의 국제 유통에 대한 개념을 둘러싸고 많은 견해들이 존재하나 대체로 '전세계적인 컴퓨터 통신망을 통한 국제적 정보유통'으로 이해되고 있는 실정에서 이러한 국제정보유통에서 정보가 선진국의 통신을 이용하게 되기 때문에 외국의 서버에 축적된다는 점이다. 따라서 정보자원을 외국을 통하여 쉽게 이용할 수 있게 된다면, 정보산업 자체가 발전할 수 없게 되며, 정보의 국제적인 종속도 아울러 가져오게 되는 문제가 있다. 따라서 정보사회의 정보보안 대책시 고려해야 하는 것은 이러한 개인정보를 외국에서 불법적인 사용을 금할 수 있는 방안들을 모색하여야 한다.

이와 같이 정보보안을 위한 법적인 면은 정보보안을 위한 법률 자체의 내용과 형식뿐만 아니라, 이러한 법규가 적용되고 영향을 미치는 범위 또한 매우 넓고 복잡하다. 정보통신의 활용이 우리의 매일매일의 생활구조마저도 바꾸어 놓는 오늘날에 있어서 정보보안의 정의와 관리를 위한 법적인 장치의 확립과 실현은 선결되고 항상 새롭게 유지되어야 하는 것이다.

### 6. 2. 2 제도적 측면

정보사회의 정보보안의 방안은 제도적 측면에서도 살펴 볼 수 있는데 이를 위하여 정보보안에 관한 전문인력의 양성 및 확보, 윤리적 의식의 확산, 전담기구의 설치 및 운영, 정보보안을 위한 인력관리 및 교육의 강화 등이 정부의 정책적 노력과 병행되어질 때 그 효과를 극대화 할 수 있는 것이다.

첫째, 정보보안 전문인력의 양성 및 확보의 노력이다. 정보보안상 중요한 문제점의 하나로 기술부족과 인력부족이 지적되는 이유는 전문적인 능력을 가진 전문가의 부족현상으로

실질적으로 안전하게 활동할 수 있는 시스템을 개발하지 못하고 외부로부터의 침입시 문제해결의 능력이 부족하거나 나아가 정보의 생산, 유통, 및 이용에 대한 시스템적 이해가 부족하기 때문이다.

이러한 전문 인적자원의 육성이란 많은 시간이 요하고 사회구조적인 측면에서의 교육이 병행되어야 하기 때문에 장기적인 안목을 가지고 임하여야 한다. 왜냐하면 이러한 정보보안의 전문인력이란 단순한 기술자나 이론적 자문인력이 아니고 정보보안의 중요성과 의미를 인식하고, 정보보안의 관리상의 문제점을 파악하고, 전자상거래 각 구성요소간의 상호관계를 파악하며, 정보통신시스템에 대한 표준화의 개발과 평가, 분석에 의하여 정보보안에 접근하는 능력을 필요로 하기 때문이다.

이러한 정보보안 전문인력의 양성은 체계적이고 지속적인 교육을 전제로 한다. 예를 들어, 인터넷에서 사용하고 있는 규약(protocol)은 그 원리가 공개되고 있으며 이러한 규약을 분석한 자료란 어디에서나 구할 수 있어 정보침입의 수법과 내용이 날로 다양해지는 상황에서 정보보안의 교육은 보다 광범위하게 이루어져야 하며 이러한 교육내용으로는 정보의 의미, 정보보안의 구성요소, 정보침해의 원인 및 유형과 효과, 정보범죄에 대한 법적, 윤리적 내용 등을 포함하여야 한다. 아울러 정보통신의 구조적 이해 및 분석과 평가능력을 배양하는 내용을 포함하는 포괄적인 교육이 이루어 질 때 정보사회에서의 정보보안 문제해결에 접근하게 되는 것이다.

둘째, 정보보안의 윤리적 의식 확산방안의 강구이다. 체계적이고 인간적인 정보보안을 위해서는 정보보안에 관한 정규교육 외에도 정보보안에 관한 윤리적 교육 나아가 정보화에 관한 윤리교육이 시행되어야 한다. 정보와 정보기술의 필요성이 대두된 이래, 학교 등을 비롯한 제도적인 교육기관에서 이를 수용하려 해왔다. 그러나 이러한 교육들은 정보의 이용과 기술의 사용법 교육만을 강조해온 경향이 있다. 즉, 정보나 정보기술에 대한 자세나 태도는 유의하지 않고 조작기술이나 응용능력만을 중시해 온 것이다. 이는 정보나 기술에 대한 기술만 익힐 뿐 이에 대한 가치관이나 철학을 갖지 못한 원인이 되고 있는 것이다.

정보보안에 대한 윤리적 의식이란 정보 및 정보사용의 의미에 대한 올바른 인식과 정보를 보존, 보호할 수 있는 책임감, 그리고 정보의 가치를 이해하는 것으로 이러한 정보보안의 윤리의식이란 문제의식과 좋은 사회관, 그리고 폭 넓은 안목 등을 바탕으로 발생하는 의식변화를 가르친다. 이러한 윤리의식의 확산은 정보통신에의 접속이 일반화되고 해킹의 내용이나 방법 등이 매우 다양해짐에 따라 더욱 강조되어 지고 있다. 그러므로 이러한 정보윤리의식은 가정, 정규교육기관 뿐만 아니라, 언론 등을 비롯한 사회제도에서 강조되어 질 때 효과가 있는 것이다.

아울러 인터넷 등 정보통신 시스템의 개방지향적 특성상 정보침해나 컴퓨터 바이러스 제작의 의미가 호기심의 단계를 이미 지나 사회적, 경제적, 정치적으로 문제로 대두되고 있는 실정에서 정보통신의 정보범죄가 지니는 의미는 폭탄보다 더 큰 파급효과를 초래할 수 있는 것이다. 이러한 정보범죄에 대한 윤리적, 사회적 의식을 심어주지 못한다면 정보사회에

서의 정보보안은 영원히 요원해 질 것이다.

셋째, 정보보안을 위한 전담기구의 설치 및 운영이다. 정보와 통신의 본질상 사회의 여러 구성요소들과 연관이 되며 이러한 구성요소는 정보의 생산자와 소비자 외에도 정부기관, 통신 관련 기관, 시스템 관련 기관 등 매우 다양하다. 사회적 차원에서의 정보보안 역시 이러한 관련 기관들이 상호 연계되어 있으며 정보보안의 문제가 어떠한 형태로 발생하는 지를 예견하기가 매우 어려운 것이다. 그러므로 정보사회에서의 정보보안의 문제는 이러한 관련 요소들을 조정·통제할 때 비로소 가능해지는 것이다.

이러한 의미에서 사회적 차원에서 정보보안을 위한 전담기구의 설치가 필요하다. 이러한 전담기구의 역할은 개방 지향적인 정보통신의 구성요소들을 통합 관리하고 각 분야별로 잔재해 있는 정보보안 요소들이 분석·평가되기 어려우므로 정보유통상의 일련의 과정을 조정·관리하는 것이다. 그러므로 정보보안 전담부서의 설치 및 전문화란 일종의 수사기능을 포함하는 것으로 엄격한 법적 절차와 규제하에서 기능이 수행될 수 있도록 하여야 한다. 물론 이러한 기구의 종사자는 오랜 기간의 전문적인 교육훈련과 경험을 필요로 한다.

이러한 전담부서는 중앙에 통제기구를 두어 종합적인 교육훈련과 수사대책, 버그방지대책, 시스템 관리 및 보안 등을 수립·시행하고 각 지역에는 최소한의 전문인력을 배치하여 균형있고 탄력적인 운영을 해나가는 것이 필요하다. 아울러 인터넷이나 전자상거래의 범위를 고려해 볼 때 국제적인 즉시 공제체제의 구축이 필요하다.

넷째, 정보보안을 위한 인력관리 및 교육의 강화이다. 정보사회의 정보보안을 위해서는 관련자에 대한 엄격한 관리와 감시장치가 필요하다. 정보보안이 중요한 것은 정보사회에서 많은 정보의 정치적, 경제적, 문화적 가치가 점점 커지고 있고, 정보통신망의 발전으로 이러한 사회적 가치의 정보가 한군데 모여있기 때문에 오용과 도용의 기회가 많아졌기 때문이다. 더구나 이러한 정보는 도난과 방출에 면역성이 약하여 정보보안의 여부가 잘 드러나지 않으며 정보의 내용이 바뀐다해도 인지하기가 상당히 어렵다. 그렇기에 정보관련자에 대한 엄격한 관리가 정보보안을 위하여 필수적으로 이루어져야 한다.

이러한 정보보안 관련자에 대한 인력관리는 관련자간의 업무를 적절히 분산시키고 상호견제의 효과를 유지할 필요가 있다. 즉 수시로 실험데이터의 자료와 실제 작업결과의 비교 등을 효과있게 하는 감사기법의 도입, 주요 직무를 수행하는 관련자 동태 등의 일반사항에 대한 감독 및 책임제도의 강화, 주요직무의 수행시에는 반드시 감독자의 입회를 요건으로 하는 대처방안의 수립 등이 필요하다. 이외에도 보안수칙을 제정하고 각 시스템별로 사용자와 사용시간, 사용내용 등을 모두 자동으로 실명 표시하는 기능을 채택하고 중요 정보사항을 다루는 작업은 정보통신망과 격리된 독립 정보시스템에서 다루도록 해야 할 것이다.

또한 정보보안을 위한 인력관리는 관련 종사자에게 정보보안의 필요성과 중요성을 통한 정보보안의 책임과 동기부여를 유발시키고 나아가 정보보안의 홍보를 할 수 있도록 지속적인 교육과 보상제도가 병행될 때 더 큰 효과

를 얻을 수 있게 된다. 더욱이 전자상거래가 갈수록 개방화되는 현시점에서 정보보안에 대한 자부심을 갖고 업무에 임할 수 있는 환경의 조성이란 노력여하에 따라 오히려 수월하게 이루어 질 수도 있는 것이다.

다섯째, 정보보안을 위한 정부의 역할과 이의 실현이다. 정보사회에서의 정보보안을 위해서는 정부의 역할이 필수적인 것은 정부도 이러한 정보보안 및 정보침해의 당사자가 될 뿐만 아니라, 이제 모든 사회 구성원의 생활 가운데 자리매김 하고 있는 정보화의 원활한 운영과 진행을 위한 기반조성의 책임이 있기 때문이다. 정보화의 심화에 주요 매체인 인터넷은 이미 각 개인이나 기업의 차원에서 통제될 수 없는 그야말로 세계적인 정보의 바다이다. 그러므로 정부가 할 수 있는 가능한 범위 내에서 일관적이고 지속적인 통합적인 정책지원이 이루어져야 한다.

예를 들어, 정보통신을 이용하는 사회구성요소들을 구분 · 분류하고 그들이 사용하는 정보시스템에 대한 중앙조정기구를 설치하여 정보유통의 원활화와 수사망을 통한 보안유지 및 이용자별, 업무별, 지역별 특성화에 맞는 시스템과 서비스 제도의 실시, 국가 초고속 정보통신망의 활용을 통한 정보보안 대책 수립, 개인, 조직, 사회간의 협동체제 확립을 통한 정보보안의 유지, 강화 등 좀 더 폭 넓고 적극적인 범 사회적 정보보안 대책을 강구하여야 할 것이다.

아울러 이러한 정보보안이 기업이나 개인 그리고 정부에게 주는 의미나 중요성 그리고 효과에 대한 홍보와 체계적 교육의 확립을 통해서 보다 활성화된 정보유통이 이루어지도록 유도해야 할 것이다. 이에 따른 정보보안 마인드의 확산과 이에 대한 정보통신의 운영을 선도하여 정보의 이용 및 활용에 대한 회의적 또는 부정적 인식에 대한 변화를 촉발하여야 할 것이다. 이러한 일련의 정부의 역할은 단순한 정보이용만을 위한 정보보안이 아닌 정보사회의 총체적인 유지를 위한 정보보안 정책의 커다란 틀 속에서 이해되고 실행되어야 할 것이다.

## 7. 결 론

본 연구는 정보사회에서 정보보안이 갖는 중요성을 바탕으로 정보통신상의 정보보안을 이해 분석하고 대책을 마련하여 정보통신을 이용한 정보화의 활성화에 기여할 목적으로 수행되었다. 이에 본 연구에서는 정보사회 및 그 사회적 의미 그리고 정보침해와 정보보안의 이론적 바탕을 살펴보았고 전자상거래상의 문제점을 분석하고 이에 따른 정보보안 전략을 알아보았다.

정보사회란 사회적 구조와 정보가 상호변화, 작용하는 발전된 사회형태를 말한다. 즉 사회의 모든 분야에 정보가 하나의 상품이나 전략적 자원으로서 가치를 갖게되어 사회 구성요소와 서로 영향을 미치는 성숙한 산업사회인 것이다. 따라서 정보사회란 정보와 관련된 부분만의 단순한 변화가 아니라 정보의 역할과 가치의 변화에 따른 사회의 총체적 변화를 지칭하는 것이다.

이러한 정보사회에서 정보보안이 갖는 의미는 자못 각별하다 할 것이다. 왜냐하면 정보사

회의 기본적 전제는 자유로운 정보의 생산과 유통, 그리고 이용이기 때문에 정보의 오용과 남용 그리고 오류에 의해 정보의 흐름에 장애가 생긴다면 좀더 부정적 의미를 담은 정보와 사회의 관점으로만 설명이 되는 것이다. 그러므로 정보보안을 위한 정보침해와 정보누수에 대한 대책의 마련이 시급한 것이다. 컴퓨터의 확산과 통신망의 발달 그리고 이의 대량 보급으로 인해 가능해진 정보침해는 정보통신상의 문제란 의미를 넘어 사회적 문제라는 개념으로 확대되어 기업이나 정부기관과 같은 독립된 조직간 또는 개인간의 정보교환 및 정보유통에 다양한 형태로 그리고 사회적으로도 광범위한 개념으로 자리잡아가고 있다.

정보통신시스템을 이용한 정보침해는 사회와 기술의 발전에 따라 포괄적인 개념으로 자리잡아 가고 있으며, 유기적인 측면과 정보기술적 측면을 가지고 있고, 그 행위 주체에 따라 여러 가지 유형으로 나타나며 그 효과 또한 다양하게 나타나고 있다. 이러한 정보침해는 이미 국제적인 추세이며 우리나라에서도 그 중요성과 의미 그리고 현실성을 바탕으로 이의 활성화에 노력하고 있으며 이를 위한 법적 정책적 정비에 전력을 다하고 있는 실정이다. 그러나 정보통신시스템의 복합성과 개방성은 이미 많은 피해사례를 나타내고 있으며 국내 외적으로 그 수법의 다양성과 대담성 그리고 기술적인 발전은 정보사회의 의미를 쇠퇴시키고 있는 실정이다.

이러한 정보보안의 문제점들을 조정·해결하기 위한 전략을 살펴보면 다음과 같다. 먼저 기술적인 측면에서 살펴보면, 첫째 메시지 보안의 측면이다. 즉 이용자 인증, 무결성, 비밀성, 부인방지 등이 보장되어 정보유통과 정보교환의 신뢰성 확보가 가능하도록 기술적인 측면에서의 점검이 이루어져야하며 이를 위해서 개인정보의 저장, 전달 방법이 마련되어야 할 것이다. 이는 정보의 훼손이나 변조를 막고 세계적으로 개방되어 있는 네트워크상의 정보침해에 대한 정보보안 체제가 마련됨은 의미하는 것이다. 이에 정보통신시스템 또는 네트워크에의 침입자 혹은 파괴자가 데이터를 입수하더라도 그 내용을 알 수 없도록 하기 위하여 DES와 RSA와 같은 암호 기법과 보안프로토콜을 이용한 암호화 기법이 적용되어야 한다.

둘째 인증서비스의 강화이다. 인증서비스는 인증서를 발급하는 인증기관의 체계화가 이루어져야 한다. 그러나 현재 관련 법안이 통과된 지 얼마 되지 않아 인증기관의 체계화 작업이 아직 초기단계이다. 그러므로 공공성을 갖춘 운영 주체를 선정하여 정보통신과 관련된 정부 기관과의 협의 속에서 인증기관의 설립을 추진해야 한다. 또한 정보사회에 맞는 인증시스템의 확보와 목적에 맞는 인증서를 정확히 활용하여 인증서비스의 신뢰도를 높이는 것이 필요하다.

세째 방화벽의 구축이다. 외부의 불법적인 침입으로부터 내부를 보호하기 위해서 설치되는 방화벽은 설치뿐만 아니라 효과적인 운영 및 관리가 뒤따라야 한다. 그러기 위해서는 네트워크의 출입로를 줄이고, 단일화하고 역추적 기능을 강화하고 방화벽의 구축을 통한 정보보안의 수립이 필요하다. 또한 방화벽 자체가 외부로부터의 공격 방어의 역할만 수행하기 때문에 조직내부자의 정보 유출은 무방비

상태이다. 따라서 이를 방지하기 위해서는 직원의 교육에 대한 고려가 뒤따라야 한다.

이러한 기술적 측면이외에도 법적, 관리적 측면에서의 정보보안을 살펴보면, 첫째 법적 측면에서의 정보보안이다. 정보보안에 관한 법의 재정비 및 강화 그리고 구체적인 법의 규정과 적용은 안정된 정보교환을 유지하는 기틀을 마련하게 되며 나아가 국가간의 통일 법안의 제정으로 국가간의 원활한 정보유통이 이루어질 수 있는 것이다. 또한 정보통신상에서 소홀하기 쉬운 개인의 프라이버시의 보장과 전자문서의 신뢰성 구축 등도 법적인 차원에서 해결되도록 해야 할 것이다.

둘째 관리적 측면에서의 정보보안이다. 정보보안은 기술적으로나 제도적으로 고도의 기술과 훈련을 필요로 하기 때문에 이를 위한 정보보안 전문인력의 양성 및 확보와 정보보안 예방을 위한 정보보안 윤리의식의 확산, 그리고 이러한 정보사회에서의 정보보안을 포괄적으로 관장할 정보보안 전담기구의 설치 및 운영, 일반 이용자에 대한 관리 및 교육의 제도적 노력이 정부의 역할과 같이 이루어질 때 정보보호와 정보보안이 훨씬 분명히 보장될 수 있을 것이다.

정보사회에서 정보교환이 갖는 의미는 단순한 정보통신망을 이용한 정보교류가 아닌 정치, 경제, 문화의 모든 분야에 영향을 미치는 사회적 현상인 것이다. 그러므로 정보사회의 정보보안 역시 단순히 정보기술적 문제가 아닌 사회전반에 걸쳐서 관심을 가지고 이루어내야 하는 것이다. 더구나 정보사회에서의 정보보안은 정보통신 분야에만 해당되는 것이 아니고 이와 관련된 모든 사회구성 요소와 직결되어 있기에 이러한 문제의 중요성이 있는 것이다. 그러므로 정보보안의 문제는 정보통신 분야에만 국한되는 것이 아니라 정보사회 전 분야에서 연구되어야 할 사안이며 정보사회의 여러 분야와 여러 측면들이 좀더 깊이 연구 조사되어 본 연구와 비교 분석될 때 우리는 정보사회의 정보보안 뿐만 아니라 정보사회를 살아가는 최선의 길을 찾아 볼 수 있게 되는 것이다.

## 참 고 문 헌

김태봉. 1997.『해커와 보안』. 서울: 문화전사.

김태헌. 1997.『인터넷보안과 해킹』. 서울: 청암미디어.

송인애. 1998.『정보보안 평가용 구축체계 개발』. 석사학위논문, 한국과학기술원.

신일순. 1998.『정보통신 보안을 위한 암호 체계 관련 정책 연구』. 서울: 통신개발연구원.

안혜연. 1999. 인증시스템 현황과 적용모델.『경영과 컴퓨터』, 3: 279-281.

유승렬. 1998.『누드해킹: 해킹의 모든 것』. 서울: 삼각형.

임휘선. 1997. 정보침해 이렇게 준비하자.『데이타베이스월드』, 6: 35-39.

전석호. 1997.『정보사회론』. 서울: 나남.

정동열. 1993. 정보사회 측정을 위한 사회지표

개발에 관한 연구. 『한국문헌정보학회지』, 24: 221-261.

정용섭. 1995. 『네트워킹 해킹의 사례분석과 보안 대책에 관한 연구』. 석사학위논문, 성균관대학교.

조찬식. 1995a. 정보화 사회의 문제점: 개념과 측정을 중심으로. 『한국정보관리학회 학술대회 논문집』, 2(1): 167-170.

_____. 1995b. 통신서비스의 정보화: 그 현황 및 개선 방향. 『정보관리연구』, 26(4): 1-27.

_____. 1999a. Universal Service in the Age of Information. 『산업연구』, 5(1): 181-199.

_____. 1999b. 『전자상거래 정보보안』. 서울: 대한상공회의소.

최종욱. 1997. 인터넷의 보안문제. 『금융』, 5: 74-79.

한상완. 1997. 『정보사회의 전개와 정보이용』. 서울: 구미.

허 금. 1998. 전자상거래 인증체계. 『경영과 컴퓨터』, 11: 176-181.

Antonelli, C. 1989. "The diffusion of information technology and the demand for telecommunication services. *Telecommunication Policy,* 13(3): 255-264.

Bell, D. 1973. *The Coming of Post-industrial Society: A Venture in Social Forecasting*. New York: Basic.

Cronin, B. 1994. "The internet and competitive intelligence: A survey of current practice." *International Journal of Information Management,* 14(3)

Dordick, H. S. and M. D. Rife. 1991. "Universal service in post-divestiture USA." *Telecommunication Policy,* 15 (2): 119-128.

Farley, M., T. Stearns. and J. Hsu. (1997). *Data Integrity and Security.* 강동성(역). 서울: 삼각형프레스.

Hills, J. 1989. "Universal service: Liberalization and Privatization of telecommunications." *Telecommunication Policy,* 13(2): 129-144.

Kim, J. C., and M. H. Lee. 1991. "Universal service policy in Korea: Past and future." *Telematics and Infomatics,* 8(1/2), 31-40.

Siyan, K. and C. Hart. 1996. *Internet Firewalls and Network Security.* 이제엄 등 (공역). 서울: 이한출판사.

Strebe, M., C. Perkins, and M. G. Moncur. 1999. *Network Security.* 윤대원(역). 서울: 삼각형프레스.

Williams, F. 1990. *The New Telecommunications: Infrastructure for the Information Age.* New York: Free Press.