韓國通信情報保護學會誌
第1卷, 第1號, 1991. 4

정보화사회를 위한 정보보호 대책에 대하여

안 병 성*

1. 서 론

많은 사람들이 앞으로의 사회는 정보화 사회가 될 것이라고 말하고 있다.

그러나 막상 정보화 사회란 어떤 것을 말하는가 정확히 정의된 것을 보지 못했다. 다만, 추측으로 정보산업에서의 생산이 여타 경제활동의 생산액보다 커질 때 이것을 정보화 사회라고 하는 것이 아닐까하고 생각해 본다. 이렇게 생각해 보더라도 정보산업의 범주에 어떤것들이 포함되는 것인지에 대해서는 여러가지 의견이 있을 수 있으며 따라서 언제쯤 정보화 사회가 실현되는 것인지에 대해서도 그 시기를 지정하여 말하기 어려운 입장이다.

그렇더라도 분명히 말 할 수 있는 것은 정보화 사회를 향해 발전해 가고 있으며 정보의 중대성이 점점 증가하고 있다는 점에 대해서는 이의가 있을 수 없다고 생각한다. 과거에는 정보의 대부분이 인쇄매체를 통해 기록, 보관, 전달되었으며 문서가 직접 사물을 지배, 제어하지는 않았으나 정보화 사회에서는 컴퓨터와 통신의 발달로 정보가 직접 사물을 지배, 제어 할 수 있게 되며, 따라서 문서의 관리에 비교해 볼 때 좀더 직접적으로 중대한 문제를 야기할 수 있는 위치에 놓이게 된다.

정보화가 인간생활을 편리하게 하고 생산성을 높이며, 자원의 낭비를 줄이는 좋은 면이 있는 반면 그 역기능으로 범죄의 유발이 용이해지고, 피해의 규모가 커질뿐 아니라 광역화 될 수 있다. 더 더욱 곤란한 것은 문서와는 달리 기록을 소거할 경우 장치내에 그 흔적이 남지 않으며 범죄의 수사에 전문적 기술을 요하게 되어 수사 인력의 확보에 큰 어려움이 예상된다.

이와같은 역기능이 크게 작용하여 사회가 혼란에 빠지며 경제활동에 지장이 온다면 정보화 사회가 아무리 좋은 것이라고 할지라도 실현을 저지 할 수 밖에 없을 것이다. 즉, 정보화 사회의 실현을 위해서는 필연적으로 정보범죄의 예방기술의 개발과 사회제도로 규제장치를 마련하지 않는다면 사상누각으로서의 정보화가 될 것이다.

2. 정보범죄

정보체계에서 발생할 수 있는 문제를 분석해 보기 위해 정보활용 체계를 분석해 보면 그림 1과 같다. 여기서, 정보입수라 함은 외계에서 자료를 사용가능한 형태로 입수하여 활용체계내로 끌어들임을 말하며 변형은 정보의 조합, 분리, 가공, 변화 등 처리를 말하고 검색은 정리, 수색 등 필요시 필요한 정보를 끌어내는 기능이며 통신은 거리의 극복수

* 정회원, 한국전자통신연구소 컴퓨터연구단

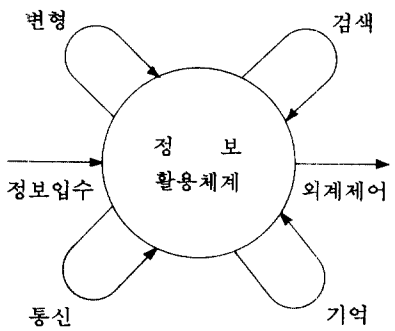

그림 1. 정보활용 체계

단, 기억은 시간의 극복수단이다. 이와같은 모델을 가상할 때 여기서 발생할 수 있는 바람직스럽지 못한 현상들은,

- 정보입수 과정 : 거짓 정보입수, 적시가 아닌 때, 교란정보에 의한 기만
- 거리극복 : 통신차단, 방수, 변조, 위장발신
- 시간극복 : 소거, 변조, 불요 독소 정보의 기록
- 변형처리 : 오조작 유도
- 정리수색 : 기능의 교란
- 외계제어 : 기능차단, 기능변경 교란, 위장발신

같은 것이 있을 수 있다. 이와같은 현상중 일부는 의도적이지 않은 것도 있으나 상당 부분은 인위적으로 발생하는 것들이다.

정보체계에 대한 침해 동기를 보면,

- 이익추구형 : 정보의 절취, 매매
  경쟁상대의 무력화
  전략 전술기밀의 취득
  상대방의 약점파악
  위조, 변조에 의한 금전적 이익
- 이념추구형 : 사회혼란 야기
  특정 기능의 마비, 제거
  정보의 절취 및 공개
  시설의 파괴
- 자아도취형 : Hacker의 흥미위주 침입
  Virus의 전파
  시설의 무료사용
  기밀의 절취 및 공개

등이 생각된다.

이와같은 해악을 방지하기 위해서는 법률, 규정 등 사회제도적 측면과 기술적 측면에서 대책을 강구해야 할 것이다.

3. 해악방지를 위한 법적대응

문서상에 기재된 정보의 변조에 대해서는 형법 제 225조부터 제 237조까지에 공문서, 사문서별로 죄와 형벌을 규정하고 있다. 여기에서 보면 공문을 위조 또는 변조한 자, 허위정보를 제공한 자 등을 징역에 처할 수 있게 되어 있다. 그러나 컴퓨터에 기록된 자료 또는 전자적(電磁的=電氣的, 磁氣的, 光利用 等 類似 諸方式) 기록내용에 대해서는 그 정보의 변조, 훼손, 절취, 부정 작출(作出) 등 범죄목적으로 행위가 이루어지더라도 법률상 처벌할 마땅한 조항이 없다. 부분적으로는 전기통신 기본법 제 28조(기술기준) ④에 보면 통신정보 보호기술기준을 제정할 수 있다고 하고 있고, 전산망 보급확장과 이용촉진에 관한 법률 제 22조(전산망의 안전성 등)에 보면 정보의 신뢰성을 확보하기 위한 보호조치를 강구하여야 하며 부당하게 보호조치를 침해, 훼손하여서는 아니된다고 규정하고 있다(처벌규정은 동법 제 29조(벌칙)에 있음).

이와같은 법규정만으로 정보범죄를 막을 가능성은 없는 것으로 생각되며 선진 제 외국의 예와 같이 형법을 개정하거나 별도의 법률을 제정하는 것이 필요하다.

일본의 예를 보면 전자적 기록을 문서와 동격으로 취급할 수 있도록 형법을 개정하여 전자적 공정증서 원본 불실 기록(제 157 조), 불실기록 전자적 공정증서 원본공용(제 158 조), 사적 및 공적 전자적 기록 부정작출 · 공용 · 미수(제 161 조의 2), 전자계산기 손괴등 업무방해(제 234 조의 2), 전자계산기 사용사기(제 246 조의 2), 공용문서 훼기(제 258 조에 추가), 사용문서 훼기(제 259 조에 추가) 등을 보완하고 문서와는 달리 컴퓨터 내부 또는 전자적

기록이 시각적으로 보이지 않으면서 직접적 작용을 미치기 때문에 문서보다도 더 엄격한 규정적용을 할 수 있게 구성된 것으로 보인다.

형벌을 규정하는 기본적인 상위법에서 정보범죄를 방지하기 위한 방안을 강구함과 동시에 정보처리 체계를 구성, 운영하는 주체가 적용해야 할 제반 규정, 표준 등을 작성하고 그 시행을 지도, 감독, 지원할 수 있는 기능을 확보하여야 할 것이다. 이와같은 일을 위해서 정보보호센타 같은 기구를 설립하겨 국가 표준제정 작업을 지원하고 평가 승인 제도를 운영하며, 사용자를 위해서는 지침을 제공하고 교육, 자문에 응하도록 한다.

일반 사용자로서는 정보보호 체계구성을 위한 전문적 지식이 없을 것이므로 그와 같은 용역을 제공할 수 있는 회사를 설립할 수 있도록 법적 뒷받침도 있어야 할 것이다.

4. 기술적 방어대책

정보체계에 가해지는 여러 종류의 해악을 시설의 기능이라는 측면에서 보면 시설을 파괴하여 기능을 마비시키는 경우를 제외하면 대부분 시설의 기능은 유지시키면서 전체 시스템으로서의 기능에 이상을 가져오거나 정보 자체에 대해 행하여지는 조작으로 볼 수 있다. 즉, 체계가 가지고 있는 소프트웨어나 데이터 등 정보에 대한 조작으로 볼 수 있으며 이와같은 조작을 위해서는 범죄자가 전체 체계내에서 정보가 취급하는 과정을 상세히 알아야만 한다. 즉, 범죄자가 알 수 없는 체계에 대해서는 공격을 할 수 없거나 극히 어렵게 한다.

그와 같은 대책으로 가장 유력한 수단이 정보의 암호화이다. 암호화 하므로서 범죄자가 체계내의 사정을 파악할 수 없게 할 뿐 아니라 절취할 정보가 어느것인지, 절취한 정보의 내용이 무엇인지 알 수 없게 하여 범죄의지를 좌절시킬 수 있다.

그러나 암호화 한다고 하더라도 체계내의 모든 정보를 소거, 훼손시킬 경우에는 대책이 없으며 체계와는 별도로 정보의 복사물을 가지고 있어야만 원상회복이 가능하다.

역사적으로 볼 때 암호는 상당히 먼 옛날부터 군사목적으로 사용되었으며 따라서, 암호라고 하면 일반인들은 첩보나 첩자 등 어두운 면을 연상하게 되는데 그와같은 연상은 구시대적 상식에 바탕을 둔 것으로 앞으로의 정보화 사회에서는 암호의 사용이 일상생활 주변으로 확산될 것으로 보인다. 우선 당장 생각되는 것이 은행 예금통장과 연관한 암증 번호도 훌륭한 암호체제로 우리 생활에 암호가 침투한 증거라 할 것이다.

암호기술은 수학의 발전에 힘입어 장족의 발전을 이루었으며 주요한 암호 기술을 분류하면 표 1과

표 1. 암호의 분류와 특성

	祕密 Key 暗號		公開 Key 暗號
原 理	暗號化 Key=復號化 Key (祕密) (祕密)		暗號化 Key=復號化 Key (公開) (祕密)
祕密 Key 配送	必 要(X)		不 要(O)
祕密 Key의 數	많 다(X) 通信相對의 數만큼 必要		적 다(O) 自身의 復號 Key 한개
安全한 認證	곤 란(X)		용 이(O)
暗號化 速度	고 속(O)		저 속(X)
暗號化 仕樣	祕 密	公 開	公 開
具 體 例	Vernam	DES, FEAL	RSA, ElGamal 暗號
主 用 途	外交 軍事用	商 業 用	公衆通信網用 等

小山： 電子情報通信學會誌, Vol. 73, No. 5, pp.516(1990).

같다.

암호의 활용이라는 측면에서 보면 통신과 같이 방수가 용이한 체계에 적용하는 경우와 컴퓨터 내부에서 사용하는 경우에는 각각의 경우에 적합한 방식이 사용된다.

암호의 취급에서 가장 문제로 생각되는 것은 Key의 배송, 관리문제이다.

통신의 경우는 신호를 원격지로 보내기 때문에 어떤 형태로든 수신자가 해독을 위한 Key를 가지고 있어야만 전달된 정보를 입수할 수 있게 되며 Key를 절취당하면 그 암호체계는 사용할 수 없게 된다.

컴퓨터 내부에서는 Key를 암호화된 다른 정보 속에 같이 보관하더라도 정보를 절취한 자는 어느 부분이 Key인지 알 수 없게 구성할 수 있기 때문에 통신에서 발생하는 문제는 관련이 없어진다. 반면에 컴퓨터 시스템인 경우 여러 계층의 사람이 사용하게 되며 이 사용자들은 시스템에 대해 조작할 수 있는 권한의 등급이 있어서 가장 큰 권한을 가진 자는 암호화 내지 복호화하는 부분까지 지배할 수 있는 권한이 있다. 이와같은 시스템에서 실제로 권한을 부여받지 못한 사람이 권한이 있는 사람을 가장하여 체계를 공격할 경우 권한을 가진 자와 위장한 자의 구분 방법에서 어려운 문제가 발생한다.

순전히 학문적 관점에서 발신자 또는 조작자의 신분을 확인하는 방법으로 서명방식, 발신자의 비밀을 노출시키지 않고 신원을 확인하는 영지식 증명(零知識 證明) 등이 연구 개발되고 있으나 실용화 시키기에는 문제가 있다.

신원확인을 위해서는 결국 법률적 행위의 주체인 인간을 확인해야 하며 사람이 가지고 있는 물적 수단을 확인하는 것은 의미가 없다. 물품의 경우 절취, 분실 등으로 인해 다른 사람이 부정한 방법으로 사용할 수 있기 때문이다. 그러나 사람의 경우에는 복잡한 수십자리의 난수를 기억하기도 어렵고 순서정연하게 컴퓨터를 조작하기도 어렵기 때문에 학문적 성과에도 불구하고 행위의 주체로서의 사람을 최종 확인하는 단계에서 실용성이 문제가 된다. 컴퓨터 및 인식기술이 더욱 발전하여 지문, 성문(声文), 얼굴화상 등을 분석하여 특정인을 정확히 인식하는 단계가 되면 신원확인 문제가 해결될지도 모르겠으나 암호기술만으로는 신원확인을 하는 데에는 제약이 있다.

그렇더라도 정보를 보호하기 위한 수단으로 암호기술은 대단히 중요한 것으로 고도의 특수기술을 가진 범인이 어려운 조작을 통해 컴퓨터 또는 통신정보를 절취, 해독하는 경우를 제외하면 일반적으로는 보호해야 할 정보를 암호화 하므로서 보통의 범죄 의도를 가진 사람들로부터 정보를 보호할 수 있으며 체계의 악의적 조작으로부터 시스템을 보호할 수 있다.

5. 결 언

정보화 사회가 산업사회보다 발전된 형태이며 자원의 절약과 생산성의 향상, 편리성의 증대 등을 가져올 것이라고 믿는 것은 당연한 일이다. 하지만 정보화 사회의 실현을 위해서는 정보에 대한 의식이 현재와는 다르게 바뀌어야 할 것으로 생각된다. 우리는 현재 재물을 보유하기 위해서 절취당하지 않고 파손되지 않게 보호하는 수단을 가지고 있으며 주의를 기울이고 있고, 법률적으로 범죄를 규정하여 위반할 경우 처벌하는 제도를 가지고 있다.

정보화 사회에서는 정보에 대해 같은 생각을 가져야 할 것이다. 정보가 경제적 가치를 갖게 되며, 정보를 통해 부정한 방법으로 금전적 이익을 취할 수 있는 이상 정보가 보호되고 관리되지 않으면 사회가 경제적으로 대혼란에 빠지게 될 것이며 정보화 사회가 인간에게 쾌적한 사회가 아니라 불행을 가져다 주는 결과가 될 것이다.

이와같은 문제를 해결하기 위해 법적, 제도적 방지 장치를 만들어야 하며 물적 재화를 창고 또는 보관시설에 넣고 보호하듯이 정보도 보관 보호시설을 갖춘 체계속에서 취급되어야만 할 것이다. 결론적으로 두가지 문제를 적시해야 할 것으로 생각된다.

1. 정보를 부정한 방법으로 조작하지 못하게 하기 위하여 각종 문서의 수준 이상으로 보호하며, 재화를 보호하는 수준의 법적 제도적 장치를 마련하기

위한 연구활동을 조속히 시작해야 할 것이다.

2. 정보를 보호하기 위한 강력한 수단인 암호기술 및 연관기술의 이론적 및 실용적 기법의 연구를 강화하여 정보화 사회에서 야기될 수 있는 제반 역기능의 방지를 위한 기반을 조성해야 할 것이다.

□ 著者紹介

安 柄 星(正會員)

1935年 9月 10日生
仁荷工大 電氣科(學士)
仁荷工科大學 大學院 電氣科(碩士)
仁荷工科大學 大學院 電子科(博士)
原子力廳 原子力研究所 電子工學研究室 研究官
韓國科學技術研究所 電子工學研究部 室長/韓國通信技術研究所 副所長
대영電子工業(株) 副社長, 研究所長/韓國電子通信研究所 無線通信開發團 團長
韓國電子通信研究所 컴퓨터研究團 團長, 韓國通信情報保護學會 副會長