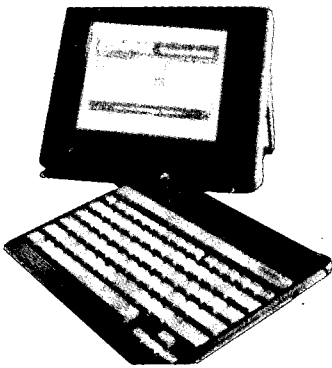


정보관리의 허와 실

1. 정보관리 안전인가?
2. 국내의 정보 안전관리 현황
3. 정보안전관리 대책

김 세 현 (한국과학기술원 경영학과 교수)



우 리 나라의 경우 공공기관은 정보보안에 관한 자체 규정을 갖고 보안관련통제를 수행하고 있으며 또 관련기관으로부터 보안감사를 받고 있다. 그러나 이 보안감사는 국가안전에 관련된 정보의 관리상태에 대한 감사가 주된 목적으로서 정보화 사회에서 새롭게 대두되고 있는 개인프라이버시 침해, 컴퓨터 금융범죄 및 기업경영정보에 대한 산업스파이 문제등은 주된 대상이 되지 못한다. 뿐만 아니라 과거부터 수행되어온 문서의 보안에 초점을 두고 있는 보안통제규정으로 인하여 전산망의 보안통제에 대해서는 좀 더 보강하여야 할 것 같다. 최근에는 총무처, 과학기술처, 체신부등에서 전산망관련 보안규정등을 제정하고 있으나 적절히 운영되고 있는지는 미지수이다.

민간부문중 금융기관의 경우에는 자체적인 필요에 의해서 상당한 수준의 보안통제를 수행하고 있는 것으로 보인다. 실제로 81년 부터 지속적으로

로 발생하고 있는 컴퓨터 범죄의 규모가 수 억원에서 수십 억원대에 이르자 특히 은행에서는 강력한 보안 시스템의 구축을 추진해 왔다. 경비원에 의해 물리적인 통제가 일차적으로 이루어지고 있으며 기관장은 담당직원들의 신상파악과 동향변화를 수시로 점검하는 행정적 통제에 관심을 갖게 되었다. 또 업무처리의 인허가 과정보도 철저히 분리되어 수행되고 있으며 단말기의 사용도 이중 점검 제도를 쓰고 있다. 그러나 그럼에도 불구하고 컴퓨터 범죄는 지속적으로 발생하고 있다.

현재 금융기관의 경우 보안문제에 관하여 가장 필요한 것은 보안에 대한 의식개혁과 보안에 대한 적절한 교육일 것으로 생각된다. 현행의 보안대책들은 대부분 외국에서 시행되고 있는 것을 그대로 모방하였기 때문에 귀찮은 이중점검을 왜 해야하는지에 대한 이해가 부족하다고 할 수 있다. 어떠한 정보를 왜 비밀로 유지해야 하는지, 어떠한 위험이 존재하는지, 보안이 제대로 이루어지지 못할 때 조직 구성원 각자에게 어떠한 위험이 돌아올 수 있는지 등에 관한 인식이 제대로 되어 있지 못하면 보안을 위한 모든 규정들은 불편하기만 하고 때로는 생략해도 무방할 것처럼 인식되기 쉽다.

금융기관을 제외한 민간부문의 경우에는 정보시스템 보안의 중요성을 크게 느끼고 있지는 못하나 부분적인 관리는 하고 있는 상황이다. 한국정보산업연합회가 92년 11월에 실시한 설문조사에 의하면 대상기업(금융기관 포함)의 79.1%가 [시스템의 안전관리 기준을 자체적으로 마련하여 실시]하고 있다고 응답하였으며 18.6%는 [안전관리를 실시하거나 별도의 규정을 가지고 있지 않다]고 응답하였다. 현재 실시중인 안전관리대책의 적정성에 대해서는 [대책이 매우 불충분한 실정이며 잘 이루어지지 않고 있다]가 46.0%, [충분한 대책이 되고 있다]는 33.0%가 되어 충분한 대책이 이루어지고 있지는 못한 것으로 보인다. 또 비용지출에 관해서는 [별도 비용설정없이 전

산예산에서 필요에 따라 소요 경비를 지출하는 것]의 경우가 48.8%에 달해 체계적인 안전관리 지원 예산이 미흡한 것으로 나타났다.

금융기관을 제외한 민간기업의 경우에는 보안을 필요로 하는 자료의 양이 별로 많지 않다고 보고 중요한 자료는 문서의 형태로 비밀 관리를 따로 하는 데에 큰 불편을 느끼지 못하고 있는 듯하다. 그러나 앞으로 보안이 필요한 정보의 종류와 양이 증가하게 되면 정보시스템 보안관리의 필요성을 더욱 느끼게 될 것으로 보인다. 사실 현재 정보시스템에 입력되어 있는 많은 자료 중에는 이미 보호를 필요로 하는 정보가 많이 있음에도 불구하고 그 필요성을 덜 느끼고 있는 것으로 보인다.

개인 프라이버시 침해 문제나 컴퓨터 범죄의 심각성이 본격적으로 거론되기 시작한 것은 제 6 공화국 출범 이후라 할 수 있다. 이러한 점에서 볼 때 우리 나라에서 민간정보보안의 중요성을 인식하게 된 것은 상당히 최근이라 할 수 있고 이에 따라 전산망보안에 관련된 제도도 뒤늦게 준비되었다. 여러가지 제도가 마련되었으나 이러한 일련의 제도마련은 선언적인 의미는 있었다고 할 수 있으나 이것이 구체적인 보안대책의 수립을 촉진시키기에는 미흡하였다. 또 이러한 규정에서 언급된 보안대책을 구현하기 위한 관리적, 기술적 보안대책의 구체적인 추진은 형식적인 수준에 머물러 있었다고 보아진다.

민간 정보보안 문제의 중요성에 대하여서는 학계의 일각에서 먼저 깨닫기 시작하였으며 관심 있는 학자들 사이에 개별적인 연구가 수행되어 오던중 1990년에 “통신정보보호학회”가 정식으로 설립되어 정보보안분야의 연구, 교육 및 정책제안등의 업무를 수행해 오고 있다. 이 학회 이전에도 전자통신연구소가 주관하여 정보보안에 관련된 워크샵이 전문가들 사이에 비공개로 개최되기도 하였다. 또 1991년 사단법인으로 등록된 “한국정보시스템감사인협회”는 정보시스템 감사의 초점인 “무결성”과 “가용성”에 대한 감사

이외에도 “비밀성”에 대한 비중을 높여가면서 전산망의 보안감사에 관련된 활동을 해오고 있다. 아직은 우리 나라 자체적인 감사인자격제도가 없으나 미국의 감사인자격(CISA)을 획득한 요원들이 부분적인 활동을 하고 있다.

우리 나라에서 적절한 정보보호제도를 정착시키는데 있어서 가장 어려운 점은 정보 보호에 대한 인식의 부족을 꼽을 수 있다. 최근까지도 정보보안이란 국가기밀이나 관련된 내용이며 정부의 특수관련부서만의 소관사항이라는 고정적 사고방식이 지배적이다. 따라서 대부분의 공공기관에서는 정보보안을 특수관련부서의 강제적인 지시에 따라 할 수 없이 수행하는 귀찮은 업무로만 생각해 오고 있다. 정보의 보안이 왜 필요하고 이것이 적절히 이루어지지 못할 때 어떠한 피해가 돌아오게 될 것인가 등에 대한 충분한 홍보와 교육이 부족하였다고 보인다. 마찬가지로 정보보안 문제를 관리하고 있는 관련부서에서는 정보보안업무를 폐쇄적인 시각으로 보고 있다는 점이 지적되어야 할 것이다. 정보보안관련 업무는 그 정책을 공개하거나 홍보를 통한 협조요청을 할 성질의 업무가 아니며 일방적인 지시와 규정에 따라 관련부서에서 요구하는 대로 일반부서에서는 쫓아주기만 하면 된다는 일방적인 사고방식은 정보보안에 대한 인식의 부족을 초래하여 자칫 형식적인 보안업무에 그치게 되기 쉽다.

민간부문에서는 개인신상정보를 보호해야 하는 정보로 인식하지 못하고 컴퓨터 금융범죄는 재수가 없어서 당한 사고이며 기업의 경영 비밀은 극소수 경영층에게만 문서를 통해 제공함으로써 보안 문제가 해결된다고 생각하고 있다. 그러나 이제 인권의 신장과 더불어 개인신상정보를 보호하여야 하며, 재수가 없어 당한 사고로 치부하기에는 컴퓨터 범죄가 너무 자주 발생하며, 앞으로 전개될 각국의 경제전쟁 속에서 중요경영정보를 제대로 보호하지 않고는 외국기업들과의 경쟁에서 이겨나가기 힘들 것이므로 이 문제에 대한 인식이 높아져야 할 것이다.