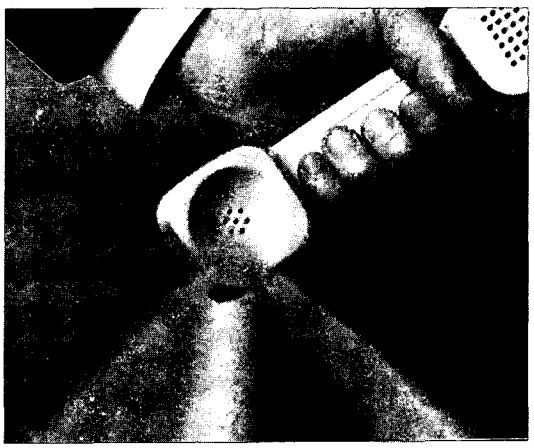
정보관리의 허와 실

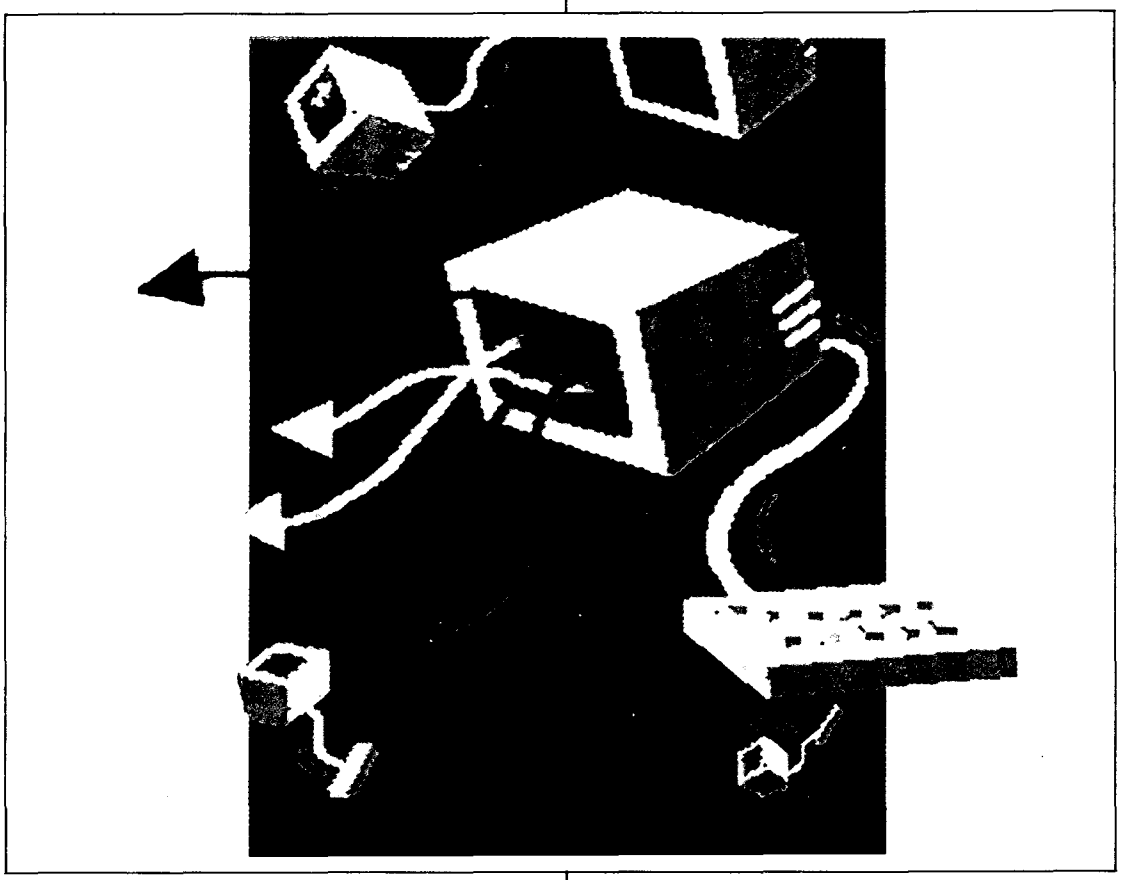
김세헌 / 한국과학기술원 경영학과 교수



전산망에서의 정보보안의 문제는 과거의 문서보안의 문제와 근본적인 몇가지 차이를 갖고 있다. 첫째, 문서보안의 경우에는 신체적 접근을 통제하는 물리적 통제만으로 대부분 해결되었음에 반하여 전산망은 통신망으로 연결되어 있기 때문에 물리적 통제만으로는 해결되지 않는다. 옥외를 통할 수 밖에 없는 통신망은 정보보안에 매우 취약하여 메세지의 노출 및 내용변조의 가능성이 매우 높다.

둘째, 한사람이 접근할 수 있는 정보의 범위가 전산망에서는 매우 광역화되었다는 점이다. 종이를 기록매체로 쓰는 경우 각 업무의 담당자가 취급하는 자료는 자신의 업무영역으로 자연스럽게 한정되게 된다. 그러나 컴퓨터로 사무처리를 하게 됨에 따라 각종 업무의 자료가 중앙 컴퓨터에 집중되고 여기에 연결된 단말기를 통해 접근할 수 있는 자료의 범위는 자신의 담당업무영역을 벗어나 사무전반으로 확대된 것이다. 이에 따라 정보 유출의 가능성이 크게 높아졌고 또 대량의 정보유출사고의 발생가능성도 높아졌다.

셋째, 개별적으로 개발된 여러 정보시스템을 종합적으로 이용할 수 있게 됨으로써 개인 프라이버시 침해 문제가 심각해 진다. 같은 자료라 하더라도 문서로 보관될 때에는 한곳에서 종합하기 어려우나 이 자료들이 전산화되면 손쉽게 모



두를 한 곳에 모을 수 있다.

넷째, 컴퓨터 바이러스 및 악의적인 해커에 의한 시스템 파괴 및 노출의 문제이다. 문서관리체계에서는 상상할 수 없었던 일이다. 이러한 근본적인 차이로 인하여 전산망의 보안문제는 문서보안의 시각에서 시작해서는 안되며 완전히 새로운 관점에서 출발하여야 한다. 이러한 어려움을 슬기롭게 극복하고 건전한 정보화사회를 건설하기 위해서는 적절한 대책마련이 필수적이다.

먼저, 정부차원에서의 정책방향으로는 첫째로 정보보안센타의 설치가 필요하다. 5대 기간 전산망 뿐만 아니라 민간의 각종 정보시스템에서도 정보보안이라는 공통된 문제를 안고 있으므로 정보보안에 관한 기술습득 및 전산망간의 기술이전을 원활히 하고 연구개발의 중복된 투자를 방지하기 위해서는 국가차원의 종합적인 정보보안센타를 설립할 필요가 있다.

둘째로는, 정보정책 자문위원회의 설립이다. 정부에서는 국가안보기밀보호, 국민의 프라이버시 침해보호, 컴퓨터 범죄, 기업의 정보보호 문제등에 관련된 여러 가지 정책 및 제도의 수립을 총괄하고 촉진하며 적절히 조정하는 기능을 수행하기 위한 정책자문위원회가 필요하다.

셋째로는, 전산감리제도 활성화이다. 공공부문에 대한 정보시스템 감사 제도는 법적으로 감사원이나 전산원등에서 수행하고 있으나, 민간부문

의 정보시스템의 감사는 각종 감사에서 제외되어 왔기 때문에 아직 관심의 정도가 낮다. 일본 및 구미제국에서와 같이 정보시스템에 대한 감사기능을 강화함으로써 안전/신뢰성을 높이는 것이 바람직하다.

넷째로는, 법령의 정비이다. 현재 정보시스템의 안전/신뢰성에 관하여 여러 부서에서 준비된 몇가지 법령들이 제정되었으나 상호균형을 이루고 못하고 있으며 포괄적인 선언에 그치고 있다. 이에 대한 종합적인 정비가 필요하다.

마지막으로는, 안전/신뢰성의 현황을 파악하기 위한 실태조사이다. 우리 나라의 경우 안전/신뢰성에 관한 실태파악이 거의 되어있지 못하므로 앞으로 우리 나라의 정책을 수립하기 위해서는 무엇보다도 현황파악을 하기위한 실태조사가 필요하다.

한편 개별 전산망에서는 다음의 대책을 도입하여야 한다. 첫째는 정보의 기밀등급 분류이다. 공공 또는 민간부문의 개별 전산망에서는 그 안에 내장된 정보들 중 보호가 필요한 정보가 어느 정도 들어 있는지에 대한 평가가 우선 이루어져야 한다. 이에 따라 어느 정도의 보호수준을 유지해야 할 것인지가 결정된다. 둘째는, 전산망시스템의 리스크 분석이다. 현재의 전산망에 어떠한 취약점이 존재하는 지에 대한 평가가 이루어 져야 한다. 취약점이 발견되면 이를 보강하기 위한 대책의 제시와 이를 위한 비용의 평가가 가능해진다.

셋째로는, 전산망 관리조직의 정비이다. 정보의 안전/신뢰성이 중요한 전산망에서는 안전/신뢰성 업무를 종합적으로 담당할 시큐리티 부서와 정보처리부문을 상호조화있게 유지하기위한 목적으로 시큐리티대책협의회의 구성이 바람직하다. 이 이외에도 관리적인 대책으로는 정보 보안에 관한 교육 및 홍보, 직무순환 및 정기적 휴가제도, 신뢰성 있는 직원의 채용 및 직원의 신상 파악등이 있다. 또한, 건물 및 중요부서에 대한 출입통제, 중요자료 보관을 위한 안전장치, 화재 등의 자연재해에 대한 안전관리등의 물리적보안대책, 액세스 자격 부여 및 관리, 사용자 신분 증명, 패스워드 관리등의 사용자 자격관리등이 있다.

기술적 대책으로는 특히 암호법이 있다. 암호법은 전산망이 침투당한 경우에도 정보의 노출을 막을 수 있는 매우 경제적인 방법이다. 미국에서 정보보호를 위해 가장 널리 사용하고 있는 암호법으로 DES(Data Encryption Standard)가 있다. 이는 1977년 NIST(당시 NBS)가 Unclassified 데이터를 보호하기 위하여 제정한 암호법 표준으로서 80년 ANSI 표준이 되었다. 초기에는 정부기관 및 관련기관을 대상으로 하였으나 그후 금융분야에서 많이 사용함으로써 널리 사용되고 있다. 이 암호방식은 정보를 비밀로 유지하기 위한 목적으로 개발된 single-key 암호법에 속한다.

1970년대 후반에 제안된 two-key 암호법은 인증 및 서명을 가능하게 하여 암호법의 새로운 응용영역을 열어 놓았다. 특히 최근에 널리 보급되고 있는 smart card 와 더불어서 앞으로 기대되는 신기술 분야라고 평가된다. 이에 따라 이 분야에 관련된 학술적 연구 활동이 국제적으로도 매우 활발하다.

또, 해킹에 대한 기술적 대책으로 call-back system이 있다. 한 사용자가 공공통신망을 통하여 단말기를 호스트 컴퓨터에 접속시키려 시도할 때에 호스트 컴퓨터는 이 사용자가 정당한 사용자인 가를 확인해야 한다. 이때 가장 널리 쓰이는 방법이 패스워드인데 이는 인증(Authentication) 기능이 취약하다는 단점이 있다. 부정한 사용자가 남의 패스워드로 접속을 시도하는 것을 막기 위한 장치로 call-back 시스템이 최근 외국에서 널리 쓰이고 있다.