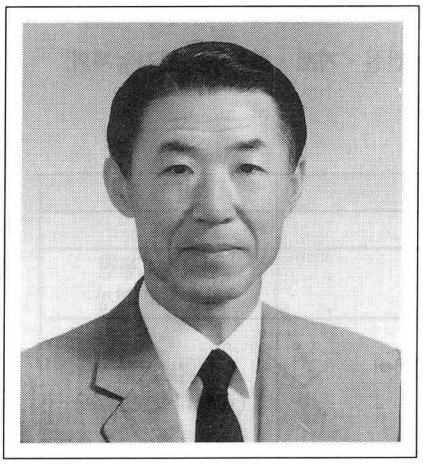
국제 해커 침투의 대응



한국정보보호센터
원 장 이 재 우

우리는 현재 21세기 선진 정보화사회를 향하여 매진하고 있다. 그러나 일부 역기능의 영향으로 큰 장애를 받고 있다. 그 역기능의 하나가 해커에 의한 시스템 침해사고의 피해인 것이다. 피해의 종류에도 여러가지가 있다. 주요정보의 침해나 금융손실 등 직접적인 피해이외에도 그것을 예방하고 방어하는데 소요되는 손실과 대응노력의 낭비가 있다. 분명 해킹의 피해는 정보화사회 촉진을 위해서 하루속히 제거되어야 할 장애요소인 것이다. 더욱 우려스러운 현상은 해커의 침투가 날이 갈수록 국제화되어 국내해킹보다 국제해커로부터의 피해가 증대되고 있다는 데에 또다른 심각성이 있다.

더구나 정보보호의 환경은 더 어려워지고 있다. 전세계 정보기반(GII)의 확산과 함께 발전되고 있는 인터넷의 영향으로 국제 해킹의 기회가 증대되고, 전자화폐나 전자상거래의 보호 등 보호해야할 영역이 확대되고 있다. 또한 정보보호장비의 수입의존으로 암호기반이 취약하며, 대응기술이 개발되면 해커들이 그것을 즉시 역이용함으로써 침투방어는 더욱 곤란해지고 있다. 나아가 해킹기술의 정보전(Information Warfare) 도구화로 산업보안이나 국가보안까지 위협하는 차원에 이르고 있는 것이다.

우리는 이미 국가의 주요 연구소와 기업의 국제해커 침투를 경험한 바 있다. 앞으로는 더 이상 그들의 침투를 허용하거나 값비싼 교훈을 잊어서는 안될 것이다. 그리고 사회적으로도 해커의 행위를 비호하거나 미화시켜서도 안된다. 그들은 결코 컴퓨터 기술의 전문가가 아니다. 다만 국한된 침투수법에 밝은 실정법 위반자일뿐이다. 본래 해커라는 용어자체가 1950년대에 미 MIT 철도모델클럽에서 사용하던 학생들의 은어였다. 오늘날 어느 나라의 해커가 초기 해커들처럼 컴퓨터 전문기술을 개발하여 인류사회에 공헌하고 있다는 말인가.

정보보호란 전문가 몇 사람만의 노력만으로 이루어지는 것이 결코 아니다. 총체적 시스템 접근과 범국민적 대응이 있어야 가능한 것이다. 국제 해커침투를 방어하기 위해서는 더욱 그렇다. 하루속히 범국민적 인식확산이 이루어져야 할 것이다. 정보보호 산업도 조속히 육성되어야 한다. 아울러 정보보호 전문인력도 시급히 양성되어야 한다. 정보보호 장비나 암호 알고리즘이야말로 자국내의 고유한 기술로 제작될 때에 비로소 국제 해커침투의 대응을 보장받을 수 있기 때문이다.

우리나라에는 세계에서 여섯 번째로 설립된 정보보호센터가 있다. 그들은 24시간 해커의 침해사고 대응팀을 운영하고 있으며 시스템 진단 프로그램을 개발하여 연중 기술봉사반 활동을 벌이고 있다. 그들의 적극적인 활용으로 국제 해커침투의 전문적 기술 대응이 있기를 바란다. ◆