

## □ 특별기고 □

## 정보보호와 안전한 사회

이 철 수<sup>†</sup>

며칠전에 '개인정보보호 지침' 제정을 위한 공청회를 열었다. 지침제정의 필요성에 대해서는 참석자 모두가 공감대를 이루었다. 그러나 시행에 있어서 사업자는 개인정보보호를 너무 강화하면 사업에 애로가 있다는 것을 주장했고 일반인들은 구체적인 구체절차와 피해보상방법등이 강화되어야 한다는 주장이었다. 한국정보보호센터에서 조사한 역기능 실태조사에 의하면 허락없는 개인정보의 유통 및 매매를 원치 않는 사람이 응답자의 70%에 이르고 있고, 전자상거래 등 인터넷의 활용을 이러한 이유로 꺼리고 있는 것으로 조사되었다. 최근에 미국에서 CNN, Yahoo등의 web이 해킹을 당하여 미국정부가 범인을 색출하기 위해서 노력한다는 보도와 함께 이런 행위를 방지할 수 있는 대책을 마련한다는 발표가 있었다. 해킹을 통한 정보의 유출, 이미지 손상등은 고려하지 않더라도 시스템의 마비, 파괴로 인해서 사업을 중단할 수 밖에 없어 발생하는 경제적 손실은 상상을 초월한다는 것이다.

21세기는 사이버 공간의 확대, 선점이 곧 국가의 경쟁력이고 국력이 될 것이다. 그러므로 선진 각국은 사이버 공간의 구축에 총력을 기울이고 유수 기업들은 국적에 관계없는 제휴와 M&A를 추구하며 e-business로 영역을 확대해 가고 있다. 그러나 사이버 공간에 대한 각종 침해사고가 빈발하고 발생할 뿐 아니라 점차 발생빈도가 많아지고 그 침해 사이버공간이 위협 받고 있다.

지금까지 우리나라는 국가 안보를 위한 보안정책을 펼쳐왔다. 국토방위가 국가의 안위를 위한 가장 중요한 목표였다. 물론 국토라는 개념에는 국토위에 존재하는 국민을 비롯한 모든 재화, 자연물들을 포함하고 있는 개념이다. 그러나 사이버 공간에는 국경이 없고 선점하고 활용하는 사람이 있을 뿐이다. 사이버 공간의 우리의 영역을 확보하고 이를 활용하는 보안정책의 수립이 필요한 시기이다. 그런면에서 어찌면 국토의 방위를 확대한 사이버 공간에서의 활동의 주체가 되는 국민의 보호가 절대적으로 필요한 시기이다. 그러므로 종래의 보안의 개념이 물리적이고 고정적이며 가시적인 것이라면, 앞으로의 보안은 추상적이고 유동적이며 비가시적인 영역을 확대되어야 한다. 지금까지 국토방위를 위한 보안에서 국민활동과 국민활동에 의한 정보로 까지 보안의 영역을 확대해야 한다.

사이버 공간에서의 보안에는 몇가지 특징이 있다. 사이버 공간에서 보안의 핵심은 정보와 정보를 저장·처리하는 정보시스템과 정보를 유통하는 통신망이다. 기밀성만 중요시하면 특정시스템을 폐쇄적으로 운영하거나 분리시켜 운영할 수도 있다. 그러나 분리되는 순간 사이버 공간으로서의 의미를 상실하게 된다. 즉 사이버 공간은 가용성과 무결성을 유리하면서 기밀성을 지킬수 있는 보안대책이 마련되어야 한다. 다음은 정보에 대한 가치판단의 기준이다. 냉전하에서의 주요 정보는 국가의 기밀, 군에 관련된 군사배치, 무기체제, 작정등에 관한 정보였다. 그러나 지식 정보사회에서의 정보가치는 경제적 가치가 더 중요시 되고

† 정회원 : 한국정보보호센터 원장

있다. 경제 활동에 이용될 수 있는 것이라면 개인 정보, 기술정보, 기업정보 등 무엇이든 활용하고자 하는 사람의 활용목적에 따라 정보의 가치가 결정된다는 것이다. 따라서 특정 정보시스템만이 침해나 공격의 대상이 되는 것이 아니라 불특정한 정보시스템이 그때 그때의 상황에 따라 공격이나 침해의 대상이 될 수 있다. 또한 사이버 공간은 접속되어 있는 모든 사람에게 공개되어 있는 공간이다. 지역과 거리, 시간의 개념이 존재하지 않는다. 따라서 언제, 어디서, 누가, 어떤 경로를 통해서 누구를 공격할 것인지를 예측하기 어렵다. 특히 공격 경로에 있어서는 직접 공격보다 우회 공격의 수단을 사용하는 것이 일반적인 형태이다. 또한 공격을 위해서 공격 대상을 선정하고 사전에 공격대상이 되는 정보시스템에 대한 취약성 조사를 한 후 취약점이 발견되면 수초 이내에 공격을 하여 상황이 종료된다. 이러한 상황으로부터 사이버 공간을 보호하여야 하는 것이 정보사회에서의 보안개념이다.

어느 사회이든 사회가 안정되지 못하면 국민의 경제활동은 물론 삶의 불편을 초래하게 된다. 지식정보사회에서 사이버 공간은 그 자체가 정치, 경제, 사회, 문화등의 기본적 생활 공간이다. 따라서 이를 보호하지 않으면 안정된 정보사회 구축은 불가능하다. 정보보호의 대상이 특정국가기밀에 국한되지 않고 국민의 개인정보, 사생활보호, 기업정보, 주요 사회기반에 대한 정보 등으로 확대되었다. 막대한 보호의 대상을 효율적으로 보호하기 위해서는 국민 각자와 기업등의 적극적인 참여가 반드시 필요하다. 따라서 종래의 보안에 관한 인식과 조직, 법·제도의 틀을 벗어나 국민의 생활과 기업의 경제 활동을 보호하면서 국가 안보를 지키는 민간과 공조하는 새로운 제도와 처치가 마련되어야 한다. 이를 단순히 지금의 정부부처의 역할이나 기능 중심으로 판단하여 추진해서는 안된다. 개방된 사이버 공간에서의 정보보

호는 물리적시설에 의존하기 보다 기술적 대응체계의 구축이 중심이 되어야 한다. 뿐만 아니라 침해와 공격행위간 순간적으로 일어나 상황이 끝나고 이를 추적, 적발하는 데는 기술력이 없으면 불가능하다. 그러기에 사전예방, 사전정보등의 노력이 정보보호의 중심이 되어야 한다. 이를 위해서는 고도의 기술개발을 위한 연구가 과감히 이루어져야 하고 관련 산업을 육성해야 한다. 뿐만 아니라 기술을 중심으로 한 정보보호가 되어야 하는 만큼 보안의 중심인력이 정보통신기술에 바탕을 둔 정보보호 전문가이어야 한다. 아직 우리는 정보보호에 대한 개념의 정립도 미흡할 뿐 아니라 정보보호 기술개발 능력, 정보보호 전문가의 육성등도 체계적으로 이루어지지 못하고 있는 실정이다.

정보보호 기술은 두가지 측면에서 고려가 되어야 한다. 첫째는 보호대상 측면에 따른 기술과 보호대상에 대한 예방측면의 사전점검에서부터 복구 내지는 공격적 방어 기술까지 공격과 침해 활동에 대한 단계적 보호 기술 측면을 고려하여야 한다. 따라서 정보보호 대상에 따라, 정보통신망의 구성요소에 따라, 정보통신기술의 응용분야에 따라 기술의 특화가 가능한 다양한 기술개발 분야가 존재한다. 나아가서 기존의 산업구조를 정보통신기술을 이용한 환경으로 전환하므로써 이에 응용할 수 있는 산업구조를 정보통신기술을 이용한 환경으로 전환하므로써 이에 응용할 수 있는 기술분야가 많다. 그럼에도 전세계적으로 아직도 크지 않다는 특징을 가지고 있다. 요소기술 분야로 보아도 단순히 정보통신기술 분야만 필요한 것이 아니라 수학, 물리등 기초기술분야의 응용이 절실히 요구되고 감성공학, 생체기술등과 접목이 필요하다. 또 암호, 인증 등 전자상거래, 전자문서 교환 등에 필요한 정보보호 기술은 점차 국제적 표준화 되지 않으면 시스템의 상호 운영이 결여되어 많은 불편을 초래하게 될 것이다. 따라서 각국은 이들 기술의 표준화에 역점을 두고 있다. 따

〈표 1〉 세계 정보보호산업의 시장규모 및 전망

(단위 : 백만 달러)

구분	1998년	1999년	2000년	2001년	2002년	2003년	인평균 증가율
제품	2,417 (40%)	3,395 (40%)	4,608 (36%)	6,013 (30%)	7,659 (27%)	9,407 (23%)	31%
서비스	3,119	4,598 (47%)	6,476 (41%)	8,284 (27%)	10,284 (25%)	12,494 (19%)	32%
총계	5,536	7,993 (44%)	11,084 (39%)	14,261 (29%)	17,943 (26%)	21,901 (22%)	32%

라서 정보보호 분야의 기술개발을 위한 집중적인 투자가 지금 이루어져야 할 시기이다.

정보보호산업은 기술이 아직 초기단계에 있으므로 그 시장규모가 적지만 <표 1>에서 보는 바와 같이 년 평균 31%의 고속성장을 하고 있다. 특히 아시아의 인터넷 시장과 이용수가 연간 40%씩 급성장할 것으로 전망됨에 따라 아시아에서의 인터넷과 관련된 보안제품의 큰 성장이 예상되고 있다. 정보보호 전망산업은 제품의 생산판매부분과 서비스부분으로 구분할 수 있는데 제품은 항바이러스, 방화벽, 인증등이 주를 이루고 있고, 암호, 공개키기반, 보안관리, 보안IC카드 등의 시장은 향후 규모가 커질 것으로 전망된다. 정보보호의 특성상 정보보호서비스 부문은 아직은 그 규모가 적지만 정보화의 진전, web호스팅서비스, ASP사업등의 활성화와 더불어 사업영역이 확대되어 갈 것으로 전망된다. 세계 정보보호 시장의 53%를 미국이 점유하고 있고 전문 보안업체가 대형컴퓨터 업체나, 통신업체들과 제휴하는 현상이 두드러지고 있다. 우리나라 1999년도 정보보호업체의 매출액은 1000억 규모로 세계 정보보호산업 시장규모의 1%미만 수준에 불과하다. 현재 국내에는 총 100여개의 정보보호 산업체가 있으며 대부분 중소벤처기업으로 구성되어 있다. 이중 스스로 제품을 개발하여 판매하는 업체는 40개 정도에 불과하며 대부분 외국 제품의 수입 판매를 하고 있다. 최근에 정보보호 서비스 업체도 4~5개 창업을 하여 향후 정보보호 서비스 산업의 발전

을 예고하고 있다.

정보보호산업은 정보통신분야에서는 새롭게 형성되는 산업분야 일 뿐만 아니라 향후 시장의 규모 팽창이 급속히 이루어질 전망이며 또 사이버 공간상에서의 생활이 보편화되면 될 수록 그 중요도가 커질수 밖에 없는 유망산업이다. 따라서 범정부적 차원에서 정보보호산업의 육성지원이 시급히 요구되고 있다. 정보보호산업의 육성을 위해서는 첫째가 시장의 창출이다. 아직 국내에서는 정보보호에 대한 인식 확신이 미흡하고, 특히 공공부문에서 정보보호에 대한 구체적인 방안 수립만 실천을 하지 못하여 많은 위험을 노출시키고 있다. 사이버테러 대책등을 정부가 마련하고 있지만 사후의 대책보다 사전의 방호가 침해를 사전 방지하지 않으면 안된다. 따라서 제도적으로 정보보호를 의무화하여 안전한 사회를 만들면서 정보보호 산업의 수요를 창출하는 노력을 하여야 할 것이다.

최근 벤처열풍으로 유망한 정보보호업체에 벤처자금이 물리고 있다. 바람직한 현상이다. 그러나 신규기술 개발, 기초기술개발등의 투자를 벤처가 모두 감당한다는 것은 현실적으로 어려운 형편이다. 따라서 정부는 보다 과감한 정보보호 기술 개발 투자를 대학, 연구소, 민간기업 등에 함으로서 정보보호 기술개발력을 조성하여 조기에 시장을 점유할 수 있도록 지원하고 부족한 전문인력을 함께 양성할 수 있도록 하여야 할 것이다. 특히 정보보호 전문인력은 <표 2>에서 보는것과

같이 수급의 불균형이 심각한 형편이다. 정부는 인력 양성을 위한 계획을 마련하고 있다. 정보보호에 대한 전공교육을 실시하는 대학(원)에 적극적인 지원을 하여 대학(원)을 근간으로 하는 인력 양성과 더불어 국외학술연구 및 활동을 지원하여 선진기술을 습득하여 조기에 정보보호 전문가를 양성하려 한다.

〈표 2〉

연도	2000	2001	2002	2003
신규수요(명)	3,988	6,251	5,653	5,386

\* 정보통신분야 신규고용수요(정보통신정책연구원, 1999.12)의 5%로 추정

최근에 미국등의 나라에서 암호 제품의 수출에 관한 규제를 완화하고 있다. 그동안 암호제품의 특성상 세계각국이 규제 정책을 추진하여 왔으나 개인정보보호, 기업정보보호등 민간부문의 암호 활용도가 점차 높아 지므로서 규제는 완화하고 있고 전략적 수출 상품화 하고 있다. 따라서 우리나라도 암호 활용에 관한 법을 제정하여 민간의 암호개발, 상품화, 활용분야의 개척등을 활성화해야 할 것이다. 또한 날로 심각해지는 해킹, 바이러스 침해등에 대한 사고를 사전에 방지하고 이를 예방하기 위한 제도적 장치가 있어야 할 것이다. 특히 이는 민·관·군이 공통으로 활동할 수 있도록 제도화 하여야 할 것이다. 개인정보보호에 대한 인식도를 향상시키고 정부 뿐만아니라 민간기업도 개인정보를 보호 할 수 있도록 제도화하여야 한다. 전자상거래등이 국제적으로 이루어 지기 위해서는 자국민의 개인정보는 물론 우리의 상품과 서비스를 공급받는 외국인에 대한 개인정보도 보호할 수 있는 제도가 되어야 우리의 상품과 서비스의 신뢰도가 높아 질수 있을 것이다. 또한 정보보호 제품을 다른 정보통신 제품과 달리 제품자체의 안전도가 제품의 질을 가름하는 척도가 되고 있다. 따라서 선진국에서는 제품의 평가

제도를 시행하고 있고 국가가 상호 인증을 시행 중에 있다. 우리나라도 98년부터 평가제도를 시행하고 있으나 제도외 제도 운영상의 문제로 산업체에게 실질적인 도움을 주지 못하고 있다. 국제 상호인증제도의 도입등 제도 개선을 하여야 한다. 그외에도 전자서명법의 제정으로 안전한 전자상거래를 보장 받을 수 있는 공인인증제도가 수립되어 공인인증기관이 서비스를 개시하였으나 아직은 일반 국민에게 충분한 홍보가 되지 못해 이용도가 낮다. 이를 위한 기술의 표준화, 제품의 평가등이 조속히 이루어지고 홍보되어 안전한 전자상거래 기반이 조기에 확립되어야 할 것이다.

지식정보사회에서는 국민 생활, 국민의 활동 등에 관한 모든 것이 중요한 국가 자선이며 보호되어야 할 지분이다. 이를 보호하지 못한다면 국가의 경쟁력은 물론 국가의 자본이 유출되거나 침해 받는 것과 같다. 정보보호는 선진국, 후발국 할 것 없이 이제 시작하는 단계이다. 보안에 대한 개념을 바르게 하여 국가의 주요한 정보, 지식 자원을 보호하고 산업도 육성하는 획기적인 전환점을 마련해야 할 시점이 지금이다.



**이 철 수**

- 1964년-1968년 육군사관학교 졸업
- 1970년-1972년 서울대 수학과 졸업
- 1975년-1977년 한국과학기술원  
전산학과 석사
- 1977년-1980년 한국과학기술원  
전산학과 박사

- 1980년 육군본부 전산위원
- 1981년-1982년 서울지하철공사 연구위원
- 1982년 한국데이터통신(주) OA개발연구부부장
- 1985년 한국데이터통신(주) 올림피아사업단 단장
- 1987년 한국데이터통신(주) 행정전산사업본부 본부장
- 1989년 한국데이터통신(주) 상무이사
- 1991년-1993년 (주)데이콤 종합연구소장(상무이사)
- 1993년-1998년 한국전산원 원장
- 현재 한국정보보호센터 원장