主題

정보보호의 현황과 발전방안

한국정보보호진흥원 원장 김 창 곤

차 례

Ⅰ. 머리말

우리나라의 인터넷 사용인구는 2003년 6월을 기준으로 2,800만명을 넘어섰으며 초고속인터넷 가입자수도 1,100만명을 넘어섰다. 전자정부를 비롯하여 온라인뱅킹, 전자상거래 등 일반국민의 경제 및 사회활동의 많은 부분이 인터넷과 정보통신을 기반으로 하고 있다.

이미 오프라인의 거래를 넘어선 은행의 온라인뱅킹이나 온라인 증권거래의 경우도 이와 유사하다. 2002년 온라인뱅킹의 사용자는 1,700만명을 넘어섰으며 온라인 주식거래 규모는 917조원을 넘어 전체시장의 64.5%가 온라인상에서 거래되고 있다. 가파른 성장곡선을 그리고 있는 전자상거래 시장의 규모 역시 177조원으로 이러한 통계수치들은 대부분 2년 전인 2000년에 비해 대부분 3~4배로 늘어난 수치이다.[1)]

뿐만 아니라 에너지, 운송, 방위산업, 농업 등 국가사회 주요기반시설 또한 인터넷을 비롯한 정보통신을 기반으로 하고 있다.

이제 인터넷을 비롯한 정보통신 인프라를 생각하지 않고는 현대사회를 생각할 수 없을 정도가 되었다. 우리가 인식하지 못하는 동안 인터넷에 대한 사회 전반의 의존도가 너무나 커진 것이다.

그러면 이렇게 생활과 밀접하게 연관되어 있고 국가사회의 주요한 역할을 하고 있는 인터넷은 과연 얼마나 안전한가? 지난 해 1월 25일 국내에서 발생한 인터넷침해사고를 기억하는 사람들은 단 몇 시간 안에 모든 인터넷접속이 차단될 수 있는 가능성을 체험하였을 것이다.

인터넷은 태생적으로 취약한 구조를 가진 시스템이다. 그러나 이러한 취약성을 인식하지도 못하고 준비도 하지 못한 사이, 인터넷은 우리 생활 깊숙이 파고들어 이를 위협하는 기술적 오류나 해커들의 사이버공격에 무방비상태이며, 이로 인한 많은 혼란을 겪을 수 밖에 없다. 더욱이 사회

1) 한국은행, <인터넷뱅킹 서비스 이용현황>

가 고도화되고 다원화될수록 시스템은 더욱 복잡해지고 온라인을 통한 각종 거래규모도 대규모화되어 사소한 보안상의 결함으로도 순식간에 사회 안정이나 국가 신용을 잃을 수 있어 보안의 중요성은 시간이 지날수록 더욱 중요해지고 있다.

최근 국내 상장기업을 대상으로 실시한 설문조사 결과에 따르면 인터넷 기반의 사업에서 가장 큰 장애요인으로 '정보보안' 문제를 꼽고 있다.[2] 이제는 고도화된 정보화의 혜택을 누리기 위해서 반드시 정보화의 역기능까지 생각하고 역기능의 비용까지 TCO(Total Cost of Ownership)비용으로 산정하여야 한다는 주장이 설득력을 얻고 있다.

사이버테러나 해킹과 같은 인터넷 침해사고로 인한 사회적, 국가적 차원의 재산피해와 온라인상의 프라이버시를 위협하여 국민 정신건강에 끼치는 피해 그리고 무작위적인 스팸메일의 발송으로 인한 시스템 낭비와 스팸메일 수신자가 받게 되는 정서적 부담등은 안전한 온라인을 위한 대표적인 저해요소라고 할 수 있다.

최근 정부는 건강한 디지털 안전국가를 위한 국가 차원의 대책을 "e-Secure Korea, e-Privacy Korea, e-Clean Korea"로 압축하여 설명하고 있다. 민·관의 인터넷 대응 시스템을 연계하여 범국가적인 사이버테러 대응체계를 구축하여 e-Secure Korea를 구현하고 누구나 개인정보에 대해 안심하고 신뢰할 수 있는 기반을 조성하여 e-Privacy Korea를 실현하며, 새로운 유형의 스팸 방지 및 불법유해 정보의 유통을 근본적으로 방지할 기술적 대책을 마련하여 사이버 청정구역 e-Clean Korea를 구현하겠다는 의지다.

정보화의 역기능에 대한 사회·국가적 차원의 노력은 이제 선택이 아닌 필수 사항이 되고 있는 것이다.

그러면 앞에서 말한 정보화사회를 위협하는 인터넷 역기능들의 원인은 무엇이고 그 대책은 없는 것인가? 정보화 사회를 위협하는 인터넷의 구조적 취약점과 이를 이용한 해킹, 인터넷의 이용자들 스스로 자정의 노력을 하지 않아 생기는 문제점이라고 할 수 있는 개인정보의 침해와 스팸메일의 현황과 해결방안을 살펴보고자 한다. 인터넷의 역기능을 알리고 그로 인한 폐해가 얼마나 위험한 것인가를 소개하는 것도 매우 중요한 일이다. 그러나 현실적으로 개인, 사회, 국가는 현실생활에서 어떻게 정보보호를 해야하는지는 더 중요한 일이다. 각각의 단계, 상황마다 필요한 정보보호의 수준이 있고 그에 따른 비용이 있는데, 필요에 따른 정보보호 시스템을 제공하고 컨설팅을 해주는 것은 그 나라의 정보보호 기업들의 몫이다. 따라서 정보보호 시스템을 생산하는 정보보호 기업들이 경쟁력을 갖추기 위해 필요한 민·관 차원의 노력도 함께 논함으로써 국가 정보보호의 발전방안을 보다 구체적으로 제시하고자 한다.

Ⅱ. 정보보호의 현황 및 문제점

1) 인터넷의 구조적 취약성

■ 인터넷 구조적 특징에 따른 문제점

정보통신 인프라는 기존의 메인프레임 환경에서 시작하여 Client-Server 환경을 거쳐 인터넷 환경으로 진화해왔다. 과거 폐쇄적인 메인프레임 기반의 정보통신 환경에서는 정보에 접근할 수 있는 사람은 매우 제한적이었기 때문에 정보유출의 위험성은 그만큼 적었다. 정보가 유출된다 하더라도 네트워크 환경이 취약했기 때문에 유출된 정보의 전파도 매우 제한적이었다. 이러한 환경

2) '국내 e-비즈니스 투자 효과 분석'(KISDI 이슈리포트)

프레임을 180도 바꾸어 놓은 것이 바로 '인터넷'이다. 인터넷의 특징으로 복잡성, 개방성, 확장성을 들 수 있으며 이 세 단어 모두 '보안'과는 배치되는 개념이라고 할 수 있다.

< 복잡성 >

인터넷망은 상호의존성이 높고, 구조적으로 복잡한 네트워크 구조를 가지고 있다. 노드의 증가와 노드사이의 링크가 기하급수적으로 늘어나는 복잡한 구조를 가지고 있는 인터넷 네트워크망은 시간이 지나면서 노드사이의 링크가 소멸과 생성을 반복하면서 진화의 과정을 겪게 된다. 결국 하나의 네트워크에 수많은 서로 다른 성격의 노드들이 연결되어 있어 전체 네트워크를 파악하기 어려워지고 인터넷상 문제가 발생하였을 때 근원지가 어디인지조차 파악하기 어려워지는 것이다. 인터넷 네트워크의 구조적 특징으로 발생한 과도한 양의 패킷간 경쟁은 패킷 손실과 전송 지연을 유발하여 서비스 품질과 네트워크 성능을 저하시키는 취약점을 갖는다.

< 개방성 · 확장성 >

인터넷은 개방형 프로토콜로 개발되었으며 네트워크 성능향상을 위한 멀티캐스트 등의 기법을 이용하고 있어 짧은 시간 안에 엄청난 수의 컴퓨터와 네트워크를 마비시키는 데 좋은 환경을 제공한다. 서비스의 품질은 염두에 두지 않고 무수하게 많은 패킷들이 네트워크의 노드에서 노드로 전달되는 과정에서 병목현상이 생기고 이것은 인터넷 접속장애를 일으키게 된다. 인터넷의 개방적인 특징은 인터넷에서 사고가 발생했을 경우 이를 총체적으로 제어하고 관리할 통제조직이 없다는 것이며 이것은 인터넷 사용자의 사소한 실수가 대규모 인터넷 장애로 확산될 가능성이 있음을 의미한다.

2002년 전세계 보안상의 결함은 4,129건으로 전년 대비 69.4%가 증가한 수치이다.[3] 최근 피해사례를 살펴보면 MS사의 운영체제의 취약성을 이용한 해킹 피해규모가 점점 커지고 있는데 이것은 인터넷에 연결된 대부분의 컴퓨터들이 MS사의 소프트웨어를 사용하고 있기 때문이다. 이것은 인터넷의 구조적 특징과 함께 최근 인터넷 취약성을 특징짓는 가장 중요한 원인의 하나가 결함이 있는 소프트웨어의 사용이라는 점을 말해준다.

■ 인터넷 공격유형과 해킹 · 바이러스 피해현황

공격방법이 점차 복잡해져서 백신이나 침입탐지시스템을 이용하여 공격의 흔적을 찾기가 어려워지고 있으며 분산서비스거부공격(DDoS)이 다양한 공격형태와 결합하면서 엄청난 피해를 야기하고 있다.

또한 지난 1년 동안 발생한 인터넷침해사고를 보면 인터넷웜에 의한 공격이 일반화되고 있음을 알 수 있다. 인터넷웜은 자가복제, 고속전파, 서비스 거부 등의 성격을 가진 공격기법으로 에이전트화[4], 분산화[5], 자동화[6]의 특징을 지닌다.

2003년 1월 25일 한국은 '인터넷 마비'라는 사상 초유의 침해사고를 겪게 되는데 이것은 슬래머웜(Slammer Worm)이라는 미국산 신종 웜 바이러스 때문이었다.

국내 유명 ISP를 통해 처음 국내 유입된 슬래

---

3) www.cert.org
4) 원격으로 조정가능한 에이전트형 백도어를 설치하고 이를 이용하여 다른 시스템을 공격하는 방법 사용. 이는 공격자가 매번 로그파일에서 자신의 흔적을 지우지 않아도 되며 분산공격에 매우 효과적임
5) 침입탐지시스템 등의 보안 시스템을 우회하기 위해 많은 수의 시스템에서 단일 혹은 다수 시스템을 공격하는 방법 사용
6) 인터넷웜 및 윈도우용 공격도구에서 발견되는 자동공격 스크립트의 증가는 공격도구들이 자동화되고 있음을 의미

머웜은 초당 1만~5만개의 공격패킷을 대량으로 만들어 패치를 하지 않은 취약한 윈도우서버를 공격하였다. 공격당한 서버는 다시 같은 속도로 패킷을 생성하여 다른 서버를 공격하게 되고 이러한 연쇄반응으로 급기야 인터넷을 사용할 수 없게 되었다.

이어 8월에는 블래스터(Blaster), 웰치아(Welchia), 소빅F웜(Sobig.F) 바이러스 공격으로 전세계적으로 한달 동안 328억불에 달하는 피해 규모를 기록하였다. 다행히 우리나라는 1.25 인터넷침해사고 이후 발빠른 대응으로 큰 피해는 없었지만 인터넷상 웜바이러스의 위험은 해를 거듭할수록 커지고 있다.

2) 정보이용 환경의 신뢰성 부족

안전한 인터넷 환경을 만들기 위해 해킹이나 바이러스와 같은 온라인 침해사고로부터 각자는 자신의 컴퓨터를 지킬 수 있어야 한다. 웜바이러스가 개인의 컴퓨터에 감염되면 자신도 모르게 피해자에서 가해자의 신분으로 바뀔 수 있기 때문에 취약성을 가진 소프트웨어는 항상 패치하는 습관이 필요하다.

인터넷을 '정보의 바다'라고 흔히 말한다. 특히 최근 화두가 되고 있는 '지식검색'이나 고도화된 알고리즘으로 제작된 검색엔진은 보다 정교하고 정확한 정보를 손쉽게 얻을 수 있게 한다. 개인에겐 중요한 프라이버시나 사회적으로 문제가 되는 음란한 정보, 불법적인 정보의 거래도 이렇게 손쉽게 거래된다. 인터넷이 생활을 편리하게 만드는 도구로 사용될 뿐 아니라 악용할 수 있는 도구라는 점은 이제 곳곳에서 나타나는 폐해를 통해 알 수 있다.

타인의 주민등록번호를 도용하여 재산상의 피해를 주는 사례는 계속 늘어가고 있으며 음란한 정보를 담은 스팸메일이 어린 자녀에게까지 배달이 되는 광경은 흔히 볼 수 있다. 이것은 인터넷이 없던 시절에는 볼 수 없었다. 이제 인터넷 이용자 스스로 안전하고 건강한 온라인 환경을 만드는 노력이 필요한 것이다.

■ 개인정보 침해의 유형과 피해 현황

'프라이버시'는 '혼자 있을 권리'라는 개념에서 출발했다. 개인정보가 자기 자신의 권리를 남으로부터 능동적으로 지킬 권리로 확대된 배경에는 개인정보가 돈이 된다는 마케팅의 개념과 이를 시스템 측면에서 뒷받침한 인터넷의 기능을 무시할 수 없다.

정보화의 역기능을 묻는 설문조사에서 이용자들은 개인정보와 프라이버시의 침해로 심한 정신적 피해를 입고 있는 것으로 나타났으며 한국정보보호진흥원의 개인정보침해 신고·상담건수를 살펴봐도 잘 나타난다.

개인정보침해는 2001년에 388건에 비해 4배 가까운 증가를 보이고 있으며 침해유형도 이용자의 이용추세에 따라 보다 조직적이고 지능화되어 가고 있음을 알 수 있다. 2002년 가장 많은 침해유형이 '법정대리인의 동의없는 개인정보 수집'이었던 반면, 2003년에는 '타인정보의 훼손·침해·도용'으로 타인의 주민등록을 이용하여 재산상의 피해를 입히는 상황이 전개되고 있다.

민간기업의 개인정보 문제뿐 아니라 의무적으로 개인의 정보를 수집·관리하는 공공기관의 개인정보보호에 관한 문제도 첨예한 이슈이다.

지난 2002년에는 전자정부 주요 시스템의 개통으로 전자정부가 출범하였으나 정부의 중점사업 중 하나인 교육행정정보시스템(NEIS)이 개인정보를 부당하게 수집·관리할 가능성이 높다는 지적으로 전자정부 사업전반에 대한 검토가 요구되기도 하였다. 이처럼 개인정보는 지식정보사회

의 근간으로 정부와 기업의 경쟁력을 높이고 서비스의 품질을 향상하는데 필수적이지만 엄격하게 관리되지 않으면 개인의 안전과 삶의 질을 위협하는 수단이 될 수 있는 것이다. 특히 개인정보의 침해는 단순한 침해행위로 끝나는 것이 아니라 타인의 정보를 도용해 사기 등 다른 범죄에 악용되는 경우가 많기 때문에 개인정보 침해에 따른 피해는 더 심각하다고 말할 수 있다.

■ 스팸메일로 인한 피해현황

2003년 한국정보보호진흥원이 조사한 '정보화 역기능 실태조사'에 따르면 인터넷 이용자들이 가장 피해를 많이 입은 정보화 역기능으로 '스팸메일(50.4%)'이 가장 높게 나타났다. 또한 대부분의 인터넷 이용자들은 정보화가 진행될수록 개인정보 침해나 스팸메일과 같은 정보화 역기능의 정도가 심하다고 응답했으며 인터넷을 많이 사용하는 사람일수록 스팸메일로 인한 정신적 피해가 크다고 말한다. 한국정보보호진흥원의 스팸메일 신고·상담건수를 살펴보면 2001년에 비해 2003년에는 156배 증가한 것을 알 수 있다.

스팸메일은 전자우편을 이용하는 이용자들에게는 많은 시간과 비용을 낭비하게 하며 웹메일 서비스업자들에게는 인터넷 가중 및 통신저하 등 유·무형의 피해가 증가하고 있다. 불법 스팸메일으로 인한 피해규모는 국내의 경우 2조6천억, 미국의 경우 89억 달러, 유럽의 경우는 25억 달러로 추산되고 있다. 더욱이 불법 스팸메일의 88%가 음란성 광고메일인 점을 감안할 때 청소년들에게 미치는 영향이 매우 커 사회적인 차단장치 도입이 시급한 실정이다.

실태조사 결과에 따르면 인터넷 이용자의 90%가량이 음란물을 접한 적이 있거나 접하고 있는 것으로 나타난다. 마음만 먹으면 언제 어디서나 음란물을 접할 수 있으며 이러한 정보는 아직 미성숙한 청소년들에게 무방비상태로 노출되고 있다.

또한 '스팸릴레이'로 인한 폐해도 만만치 않다. 스팸메일 발송자가 실제 발송지를 감추거나 스팸메일 필터링 시스템을 통과하기 위해 타인의 메일서버를 이용, 스팸메일을 발송하는 행위를 스팸릴레이라고 하는데 2001년 65건을 기록한 이후 80배 이상 증가하여 2003년에는 72,00건을 기록하였다. 이렇듯 스팸메일로 인한 폐해는 이제 국가·사회적으로 매우 심각한 수준으로 제도적인 보완이 필요한 실정이다.

3) 정보보호산업의 글로벌 경쟁력 미흡

■ 업체간 경쟁심화에 따른 출혈경쟁

국내 정보보호 산업은 업체간 경쟁구도 심화에 따른 출혈경쟁 양상을 띠고 있다. 현재의 과도한 경쟁구도는 산업 발전에 따른 과도기적 현상으로만 보기에는 도를 넘어서는 수준에 이르렀으며 특정분야에 국한되지 않고 산업전반에 일어나는 현상이라는 점이 더욱 우려스럽다. 그 배경에는 물론 수익성 낮은 영세업체의 난립이 있다. 한국정보보호진흥원이 실시한 "2003 정보보호산업 통계조사"에 따르면 정보보호산업협회의 회원사로 등록되어 있는 업체 수만 해도 200개가 넘고 이 중 절반이 넘는 64.5%의 업체가 '종업원 30명 이하'의 규모인 것 나타났다. 이처럼 대다수 업체의 규모가 영세하고 비슷한 수준의 제품과 서비스를 제공함에 출혈경쟁이 심화되고 있다. 영세한 규모에 이러한 가격경쟁까지 더하여 대부분의 업체들이 마케팅이나 R&D 등 글로벌 환경에서 생존하기 위한 투자에는 여력이 없다는 점이 심각한 문제이다.

■ 핵심기술 확보 미흡

대다수의 정보보호 업체들의 경우 핵심 기술 확보가 미흡하다는 점 또한 문제점으로 지적될 수 있다. 국내 정보보호 업체들의 경우 응용연구 수준은 일정부분 세계적인 수준에 이르렀다고 평가되고 있다. 하지만 핵심원천기술이나 상품화 능력 부분에서는 세계수준과 많은 격차를 보이고 있다. 이러한 핵심원천기술이나 상품화 능력 부족 등은 앞서 언급한 기업 규모의 영세성과 맞물려 산업 전체의 수익성 악화로 이어지고 있는 실정이다.

Ⅲ. 정보보호 대응책 및 개선방향

1) 정보보호를 위한 국가 차원의 노력

첫째, 정보보호 예방체계를 더욱 고도화해야 한다. 이를 위해 정부는 한국정보보호진흥원 내 '인터넷침해사고대응지원센터'를 구축하여 운영하고 있다. 이러한 대응지원센터가 보다 효과적으로 운영되기 위해서는 민·관 협조체제를 더욱 공고히 할 필요가 있다. 인터넷서비스업체나 관련 기관과의 협조체제를 보다 확대하여 지속적으로 인터넷침해 사고에 대한 대응 능력을 향상시켜 나가야 한다. 또한 해외 정부 및 침해사고대응기관, 국제단체 등과 실질적인 공조체제를 구축하고 침해사고 발생 시 상황전파, 대응현황 등의 정보를 공유하는 것도 반드시 필요하다.

둘째, 인터넷의 구조적 문제를 기술적으로 보완해 나가야 한다. 인터넷 기반구조는 특정노드에 트래픽이 집중되도록 구성되어 있기 때문에 특정노드에 대한 의존도가 매우 크다. 따라서 네트워크의 특정 단일지점 공격에도 취약하여 전체 네트워크의 속도 저하로 이어질 수 있다. 이러한 네트워크의 취약점을 최소화하기 위해 트래픽 집중을 억제하고 단일지점 취약점을 제거하는 노력이 필요하다.

이와 더불어 차세대 인터넷 주소체계인 IPv6를 위한 정보보호 기술을 개발하고 안전한 시스템 운영을 위한 Secure OS를 개발하는 등 기반구조 보호를 위한 기술개발에 노력을 기울여야 한다. 그리고 침입에 대한 탐지·대응 등의 기능을 수행할 수 있는 Secure 엔진과 이를 탑재한 Secure 노드 등으로 구성된 차세대 네트워크 정보보호 기술개발을 함께 진행하여야 할 것이다.

셋째, 차세대 정보통신 환경변화를 고려할 때 이제는 정보통신 서비스 보급단계부터 정보보호 기술이 고려되어야 한다. 정부는 2010년까지 100Mbps급 이상의 구내 통신망 구축과 디지털 홈네트워크 보급을 통해 유비쿼터스 접속환경을 구현할 계획이다. 이렇듯 차세대 정보통신 환경은 더욱 빨라지고 유선과 무선 등 경로는 더욱 다양해지겠지만 정보통신망 사고로 인한 파급효과는 더욱 커질 것이다. 변화된 정보통신 환경에서 정보를 더욱 안전하게 사용하려면 차세대 정보통신 서비스를 위한 정부차원의 계획안에 정보보호를 위한 로드맵을 함께 작성하여 정보화 추진단계에서부터 정보보호를 고려해야 할 것이다.

넷째, 정보보호는 제도적, 기술적 노력도 중요하지만 일반 PC 사용자 개인의 정보보호의식 또한 매우 중요하다. 2003년 8월에 발생했던 블래스터웜으로 인한 피해 사례에서 볼 수 있듯이 일반 PC의 미흡한 보안관리로 인해 전체 네트워크가 피해를 겪을 수 있다. 블래스터웜의 경우 취약점에 대한 내용과 이에 대한 보안패치 권고가 1년 전부터 공지되었지만 일부 보안패치를 하지 않은 사용자들로 인해 전체 네트워크의 피해로 이어졌다. 블래스터웜에 감염당한 PC는 다시 공격을 시도하게 되어 인터넷 이용자는 피해자인

동시에 가해자가 되었다. 결국 소수의 보안이 취약한 PC로 인해서도 전체 네트워크가 마비될 수 있는 것이다. 이러한 네트워크 마비사태와 같은 사고의 재발을 막기 위해서는 정부, 인터넷서비스업체, 서버 관리자 등의 역할이 필수적이지만 일반 PC 사용자의 주의도 매우 중요하다. 일반 PC 사용자들의 경우 정품소프트웨어 사용, 백신엔진 및 보안 패치 업데이트, 그리고 비밀번호 관리라는 3가지 원칙만 잘 지켜도 해킹·바이러스의 피해를 90% 이상 막을 수 있다는 분석이 있을 정도로 정보보호는 일부 전문가들의 전유물이 아닌 국민 모두가 함께 풀어야 할 숙제이다.

2) 관련 산업 발전을 위한 제언

정보보호산업은 산업 초기단계에서 국가 보안이나 국방 측면에서 활용하던 암호기술 등을 중심으로 발전하여 산업 초기에는 전적으로 국가 주도로 발전되는 특성을 보여왔다. 하지만 최근 인터넷 환경의 확산으로 민간에서도 정보보호기술의 활용과 수요가 높아졌기 때문에 민간 기업들의 역할이 더욱 중요해지고 있다. 정보보호 업체들은 기술연구 및 제품개발을 통해서 국가의 정보보호 수준에 직접적으로 영향을 미치기 때문에 정보보호산업 육성은 국가 정보보호 수준 제고를 위해서 반드시 필요하다.

또한 정보보호산업은 향후 몇 년간 다른 IT 산업 분야에 비해 약 2.5배 이상의 고성장을 기록할 것으로 전망되는 유망산업이기 때문에 국가 성장동력으로서의 가치도 지니고 있다.

정보보호산업 육성에 있어 정부의 시장개입은 불가피할 것이다. 그렇지만 과거와는 달리 이제는 어디까지나 정부는 시장 조성자(market maker)와 시장 창출자(market initiator)로서의 역할에 머물러야 한다. 과거와 같은 국가 주도의 산업 발전보다는 효율적인 시장창출에 중점을 두는 수준에서 정부의 부분적 개입이 바람직할 것이다.

첫째, 산업을 발전을 위하여 가장 시급하고 중요한 것은 적절한 수요 기반을 만들고 확대해 나가는 일이다. 국내 정보보호산업이 협소한 시장에서 과다한 업체들의 난립으로 영세성을 면치 못하고 있는 점을 고려할 때 이는 더욱 절실하다. 이를 위해 우선 공공기관의 선도적 투자를 이끌어 내도록 해야 할 것이다. 우리나라 정부부처, 공공기관의 정보보호 투자는 선진국에 비해 턱없이 부족하다. 대체로 정보화 예산의 5% 내외 수준으로 이는 선진국의 절반 수준이다. 따라서 공공부문의 예선편성 기준을 개선하여 정보보호 투자비율을 정보화 예산의 10% 이상으로 높여 나갈 것을 제안한다. 정부는 지난해 처음으로 '공공기관 정보보호 수준제고 사업'을 실시하여 중앙행정기관과 광역 자치단체 등 60개 기관에 정보보호시스템 구축 및 컨설팅 사업을 지원한 바 있다. 이 사업은 공공기관의 정보보호 수준 제고는 물론 국내 정보보호시장 기반을 제공했다는 점에서 매우 긍정적인 평가를 받고 있다. 정규 예산 편성이 어렵다면 지난해와 같이 기금을 활용한 특별사업을 통해서라도 국내 수요기반을 확대해 나가도록 해야 할 것이다. 또한 보호장비의 기준 제정, 표준화 등도 수요 기반 조성 차원에서 중요하다. 과거 이동통신산업은 초기 단계에서 정부가 주도적으로 기술을 개발하고, 표준을 제정하고, 적기에 사업을 허가함으로써 효과적으로 시장을 조성할 수 있었다. 정보보호산업의 경우에도 네트워크의 보호기준을 제정하고 표준화하고 IDC 등 정보통신 관련 직접시설의 안전기준을 만들어주어야 한다. 정부는 가급적 조기에 기준과 표준을 제정해 주어야 시장이 조성되고 기업의 생산활동을 전개할 수 있을 것이다.

둘째, 핵심기술의 확보 또한 산업의 발전을 위

해 중요한 요소이다. 특히 기능이 급속하게 복합화, 첨단화되고 있어 이에 대한 대응이 시급하다. 뒤떨어진 국내 기업의 기술수준을 높이기 위해서는 R&D 투자가 확대되어야 한다. 이를 위한 정부의 적극적인 지원대책이 요구된다. 국책기관을 중심으로 기업과 콘소시움을 구성하여 대형과제, 필수과제를 공동으로 개발하고 이를 정부가 적극 지원하는 것이 좋은 방안일 것이다. 과거 TDX나 CDMA 개발과 같은 대형국책과제를 발굴하여 산학연이 공동으로 추진하는 방안을 검토해볼 것을 제안한다. 특히 하루가 다르게 첨단화되고 복합솔루션화되는 발전추세를 고려할 때 국내기업의 기술수준을 획기적으로 제고시킬 특단의 대책이 필요하다. 국내외 대기업과 전략적 제휴를 통해 소요 기술과 판로를 확보하는 것도 좋은 방안이다. 정보보호업체는 대기업과의 파트너쉽 구축을 통해 대기업의 해외 판매망을 활용할 수 있고 대기업은 정보보호 업체의 제품을 판매할 수 있을 것이다.

셋째, 중소업체가 대부분인 국내 정보보호산업의 현실을 고려할 때 기업간에 M&A를 하는 방안을 적극 제안하고 싶다. 세계적으로 IT산업의 경우 경기침체에도 불구하고 선도기업들을 중심으로 M&A가 활발하게 이루어져 왔다. 시만텍, 넷스크린 등 해외 유수 보안업체들은 잇달아 다른 보안업체를 인수·합병함으로써 규모의 경제 실현은 물론 통합보안솔루션 개발의 전초기지를 구축해 왔다. 마이크로소프트나 IBM도 지난 5년간 꾸준히 중소전문업체를 M&A하여 경쟁력을 키워왔다.

물론 국내 시장에서 M&A가 활성화되기 위해서 선결되어야할 과제들이 많다. 회계 투명성 확보를 통한 기업의 객관적인 가치평가가 선행되어야 한다. 또 전통적인 자산이나 수익가치 평가방식에서 탈피하여 M&A를 통해 얻을 수 있는 시너지효과까지 포괄하는 새로운 평가방식의 정착도 필요하다. 무엇보다 피인수기업의 패배의식 등 부정적 인식부터 개선되어야 할 것이다. 미국에서 벤처기업 투자자금의 회수방법 중 M&A를 통한 규모는 나스닥 상장의 10배 이상이다. 우리나라도 그 많은 벤처기업이 코스닥 상장을 통해 자본을 회수할 수는 없다. M&A가 활성화되어야 한다.

넷째, 세계 시장의 글로벌화에 대비해야 한다. 세계시장은 국경간 무역장벽이 없어지고 급속히 글로벌화되고 있다. 국내 정보보호시장도 머지않아 대외에 개방될 것이다. 이와 같은 세계 시장의 개방화 추세에 대비하여 국내 시장을 보호하고 해외 진출을 활성화할 수 있도록 능력을 배양해야 할 것이다. 우선 정보보호장비의 평가기준을 세계 공통 평가기준인 CC(Common Criteria) 기준으로 전환할 것을 제안한다. 그리고 평가결과를 상호인정할 수 있는 공통기준상호인증제도(CCRA)에 조속히 가입해야 할 것이다.

또한 해외시장 진출이 반드시 대기업만 가능할 것이라는 인식은 버려야 한다. 휴맥스와 같은 전문성을 가진 중소기업들이 해외시장에서 많은 성공을 거두고 있다. 무엇보다 선진국 제품을 압도할 수 있는 성능과 품질을 가지는 제품을 확보하는 것이 급선무다. 정부차원에서는 국내 업체의 제품과 기술력을 해외시장에 알릴 수 있는 기술 세미나와 제품 전시회 등 홍보 행사를 지원하는 것도 좋은 방안이다. 또한 정부부처 간의 긴밀한 협력체제 구축을 통하여 기업간에 교류협력 환경을 적극 조성하는 것도 중요하다.

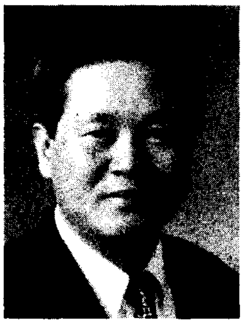
Ⅳ. 맺음말

지난 2003년 4월 한국정보보호진흥원이 실시한 '2003년도 정보보호 실태조사 보고서'에 따르면 사회 전반의 정보보호 수준은 여전히 낮은 수

준에 머물고 있는 것으로 조사되었다. 1.25 인터넷 마비사태에도 불구하고 정보보호에 대한 사회적 인식이나 투자는 크게 개선되지 않고 있는 것으로 나타나 다시 한 번 정보보호가 취약한 정보통신 강국의 모습을 드러내고 있다. 정보보호가 병행되지 않는 정보화 사회는 사상누각이다. '사이버 시대(cyber age)'를 뒤로하고 '안전한 사이버 시대(secure cyber age)'를 후손에게 물려주는 것은 우리 시대가 이뤄야 할 의무이다. 이를 위한 노력은 하루라도 늦출 이유가 없다.

참고자료

1. 중장기 정보보호 기본계획, 정보통신부, 2002/8
2. 국내 정보보호산업 통계조사, 한국정보보호진흥원, 2003/12
3. 2003년도 정보보호 실태조사 보고서, 한국정보보호진흥원, 2003/4
4. 2003 한국인터넷백서, 한국전산원, 2003/3
5. 2003 한국인터넷통계집, 한국인터넷정보센터, 2003/10
6. 2002년 개인정보보호백서, 한국정보보호진흥원, 2003/2
7. 2003년 인터넷 침해사고 유형분석, 한국정보보호진흥원, 2003/12
8. 인터넷침해사고대응지원센터 CERT-CC 통계자료, 한국정보보호진흥원, 2003/12
9. 개인정보침해신고센터 개인정보침해 통계·사례분석자료, 한국정보보호진흥원, 2003/12
10. OECD Guidelines for the Security of Information Systems and Networks, OECD, 2002/7



김 창 곤

한양대학교 전자공학과 졸업
한양대학교대학원 전자공학 박사
제12회 기술고등고시 합격
체신부 통신정책실 기술심의관
미국 콜롬비아대학 정보통신연구소 초빙연구원
정보통신부 전파방송관리국장
정보통신부 정보통신진흥국장
정보통신부 정보통신정책국장
정보통신부 기획관리실장
정보통신부 정보화기획실장
現 한국정보보호진흥원(KISA) 원장
現 아시아 PKI 포럼 의장
現 한국통신학회 부회장
現 한국정보과학회 부회장
現 고려대학교 공과대학 겸임교수