

□사례발표□

국내·외 정보보호 산업현황

김 홍 선[†]

◆ 목 차 ◆

- | | |
|-------------------------|------------------------|
| 1. 서 론 | 4. 국내 정보보호산업 발전을 위한 대책 |
| 2. 국내정보보호산업의 과거, 현재, 미래 | 5. 결 론 |
| 3. 산업의 구성 | |

1. 서 론

새로운 밀레니엄을 맞이하는 시점에서 인터넷을 기반으로 하는 정보화 사회 (Information Society)와 지식기반경제 (Knowledge-based Economy)는 현재와 미래를 규정하는 거시적 패러다임으로 인식되고 있다. 정보화 사회로 이동해 가는 시점에 처해 있는 우리 사회는 농경 사회와 산업 사회의 경제 논리로는 도저히 해석되지 않는 각종 경제 모델들이 끊임없이 제시되고 실현되는 가치 혁명적인 상황을 경험하고 있다.

무엇보다도 이러한 변화의 동인(動因) 역할을 하는 정보통신의 혁신적 발전과 탈 지역화, 글로벌화 경향은 인터넷이라는 핵심적 인프라에 의해 드라이브되고 있다. 인터넷이 기술, 산업, 그리고 문화의 새로운 융합과 발전을 구축하는 중심축이 되고 있는 것은 우리에게서 궁극적으로 무척 다행스러운 일이다. 그만큼 우리는 개방성(openness), 글로벌성(globality), 접근용이성(easy to access)과 같은 혜택을 누릴 수 있기 때문이다.

그러나, 이러한 인터넷의 장점은 정보를 관리하는 측면에서는 근본적인 문제점을 노출한다. 일반 비즈니스의 논리는 철저한 신뢰와 믿음에 근

거하고 있다. 따라서, 비즈니스 논리가 인터넷 환경에서 실현되려면 신뢰의 개념을 사이버 공간에서 구축하는 노력이 전제되어야 한다. 그러나 불행히도 인터넷은 이와 대치되는 특성을 지니고 있다.

첫째, 누구에게도 개방되어 있다는 장점은 다른 각도에서 보면 신뢰할 수 없는 수많은 객체들도 존재한다는 의미를 지닌다. 근본적으로 비즈니스를 구현하기에는 사상이 맞지 않는다. 다시 말해서 인터넷상에서 이루어지는 모든 통신 행위와 정보의 접근은 그대로 제3자에게도 노출되는 취약성을 가지고 있다.

둘째, 글로벌성(globality)의 장점은 위협을 주는 요소도 글로벌하게 존재한다는 단점에 의해 퇴색한다. 기업이나 기관별로 폐쇄성을 지닌 사회에서는 지역적으로나 조직적으로 정보나 자산의 접근을 어느 정도 통제할 수가 있었다. 그러나, 인터넷에 문을 열어두고 있는 이상 전세계의 컴퓨터 범죄자들이 경계의 대상이 된다.

마지막으로 접근 용이성은 기업 네트워크가 여러 곳에 문을 가지고 있음을 가리킨다. 전용선, 케이블, 모뎀에서부터 CDMA, ADSL, 위성통신에 이르기까지 모든 통신사업자들은 인터넷 접속 제공자 (Internet Access Provider)로서 자신들을 정의하고 있다. 여러 곳에 문을 열어 두고 있는 한 각

[†] 정회원 : (주)시큐어소프트 대표이사

기업이나 개인의 정보 시스템에서 관리해야 될 부분도 심각할 정도로 많이 존재한다.

이와 같이 태생적으로 문제점을 지닌 인터넷이지만 각 기업은 경쟁적으로 인터넷 인프라에 기반한 e-business로 자신들의 비즈니스 패러다임을 바꾸고 있다. 인텔의 앤디 그로브 회장이나 GE의 잭 웰치 회장과 같은 세계적 지도자들의 외침은 단순한 권고 이상의 절실함을 지니고 있다. IBM이나 HP같은 전통적인 하드웨어 회사들도 자신들이 인터넷 회사로 불리기를 강력히 바라고 있다. 그만큼 인터넷이 가져다주는 혜택과 매력은 엄청나다.

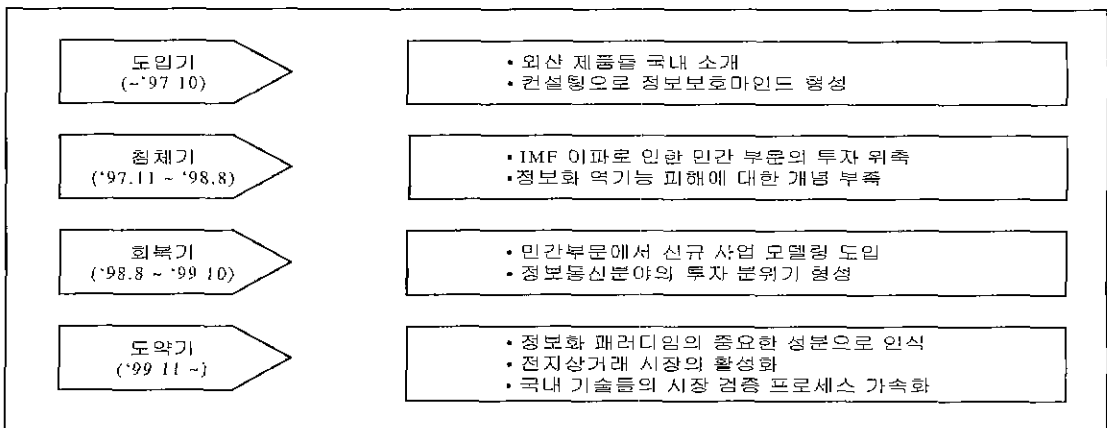
결론적으로 정보 관리나 비즈니스 업무의 폐쇄성과 대치되지만 인터넷 환경으로 사회 공간이 옮겨가고 있는 대체는 거스를 수가 없다. 그렇다면 이러한 약점을 보완하는 기술적 대안은 무엇인가? 바로 이러한 사명을 정보보호산업은 수행한다. 인터넷 사회에서 정보보호기술의 존재는 필수 불가결한 요소이다. 정보보호산업은 각종 위협으로부터 보호하는 방어적 개념에서부터 인터넷 정보통신의 프레임워크를 구성하는 모든 요소를 총망라한다. 바로 그런 점에서 정보보호산업의 성장은 폭발적인 대중화에 기반을 둔 인터넷 산업의 발전과 맥을 같이하고 있다.

국내에서도 정보보호산업은 이 유아기를 벗어나 도약의 발걸음을 힘차게 하고 있다. 이제 정보보호산업도 독자적인 산업으로 굳게 자립매김 하였다. 여타 산업에 끼치는 영향력이 날로 증대하고 있다. 특히 금년도 상반기에 터진 CIH 바이러스의 피해와 최근 연이어 발생하는 해킹위협증대는 정보화의 역기능에 대한 중요성을 크게 부각시켰다.

본 기고에서는 국내 정보보호산업의 현황을 파악하여 그 대책을 제시하고자 한다. 정보보호산업의 위상을 바탕으로 산업체의 목소리도 구체적인 공감대를 잘 형성하고 있다. 이런 점에서 한국정보보호산업협회(KISIA)의 역할도 더 중요해지고 있다. 다른 측면에서는 관련된 기관이나 단체에서도 한국정보보호산업협회가 이 산업을 누구보다 대변하고 있음을 인지하여 올바른 대책 수립이 되어야 할 것으로 생각된다.

2. 국내정보보호산업의 과거, 현재, 미래

보통 새로운 패러다임의 제품이나 기술이 독립적인 산업 분야로 분류될 때에는 산업을 구성하는 기업들의 형태, 시장을 구성하는 고객층, 기술력의 성숙도 등 여러 가지 척도를 이용해 판단한



(그림 1) 국내정보보호발전현황

다. 비록 한국정보보호산업협회가 1997년 9월에 협회회의 형태로 태어나면서 인위적으로 산업의 의미를 부여했지만, 사실상 독립적인 산업의 형태로 자리잡은 것은 최근이라고 보는 것이 적합하다. 정보보호산업의 지나온 역사를 살펴보는 것도 현황을 파악하는데 도움이 되리라 생각된다.

2.1 도입기 (- '97.10)

시장 초기에는 국내 제품으로 안철수컴퓨터바이러스연구소의 V3 백신과 사이버게이트인터넷서널(현 ㈜시큐어소프트)의 수호신 방화벽 제품 정도가 나와 있었지만 그 규모가 크지 않았다. 바이러스 백신은 외산 제품이 약세를 면치 못했지만, 그 이외의 분야에서는 국내 제품보다는 외산 제품들이 비교적 활발하게 소개되고 있었다. 일반적으로 정보보호제품은 영업 사이클이 긴 경향이 있다. 따라서, 이 시기는 고객과 벤더간에 방향을 모색하는 수준이었다고 볼 수가 있다.

한편 이 시기에 4대 기업들을 중심으로 외국 컨설팅업체로부터 보안 컨설팅을 받는 사례가 나오기 시작했다. 일단 상위 계층(high level)의 컨설팅이어서 구체적으로 구현되지는 않았지만 보안에 대한 개념을 잡아가기 시작했고 각 기업별로 정보 보안팀을 구성해가기 시작했다. 또한 정보통신부는 1997년 9월에 정보보호산업 발전대책을 수립해서 이 산업에 대한 정부의 의지를 표명하였다.

2.2 침체기 ('97.11 - '98.8)

1,2년의 시장 형성기를 거쳐서 본격적 산업으로 도약하려는 시점에서 정보보호산업은 IMF라는 산업적 충격을 받았다. 이 시기의 특성은 다음과 같이 요약된다.

첫째, 매출의 성장세가 크게 둔화되었다. 비교적 산업이 안정화되어 있던 다른 IT(Information Technology) 분야의 경우도 타격은 마찬가지로 받

았지만 비즈니스 관성에 의해 그 충격이 점차적으로 하강 곡선을 그려 가는 형태였다. 그러나, 정보보호산업은 시장이 막 형성되려는 시점에 IMF가 터졌기 때문에 충격의 여파가 아주 컸다. 특히 주요 시장을 형성해야 하는 민수 분야의 부진은 충격이 컸는데, 정보보호산업의 주고객인 기업, 금융 기관들은 자체의 구조 조정 과정 때문에 여력이 있다고 보기 힘들었다. 또한 산업의 구성원이 벤처 기업들 위주로 형성되어 있어서 투자 자급에 대한 수요가 높았던 것도 어려움을 겪었던 이유이었다.

둘째, 정보화 역기능에 대비책에 대한 마인드가 거의 형성되지 않았다. 정보화를 위한 투자 자체도 위축되었지만, 설사 계획이 있다 하더라도 정보보호의 순위는 최하위에 위치하였다고 해도 과언이 아니다. 안전 불감증이라는 한국 국민의 고질적 병폐와 전시 위주의 운영 방식도 정보화 역기능에 대한 대책이 소홀하게된 원인이 되었다.

셋째, 정보보호산업 업체들은 재정비를 하고 인력 보강을 하는 계기를 삼을 수가 있었다. IMF덕에 고급 인력들의 수혈이 가능했고, 이들을 중심으로 내실을 다지는 기반을 마련했다. 정보보호산업협회에 등록된 업체들의 현황을 보면 이 시점에 어떻게 준비했는가에 따라 그 후 위상에 큰 변화가 있는 것을 목격할 수가 있다.

어려운 상황에서 투자를 정보보호분야에 집중했던 기업들은 그 다음 시기인 시장 회복기에 발전의 계기를 마련했고, 다른 분야로 전업하거나 우선 순위를 낮춘 기업들은 그 후 약화되거나 없어지는 것을 볼 수가 있다. 그런 점에서 이 시기는 한국의 정보보호산업으로서 가장 암흑기였지만 전환점이 되었다고 하겠다.

2.3 시장회복기 ('98.9 - '99.10)

IMF의 여파는 '98년 상반기까지의 모든 투자를 얼어붙게 했다. 그런데 이 시기를 지나면서 조심

스레 시장에서 가능성이 보이기 시작했다. 특히 해가 바뀌어 99년을 맞으면서 정보보호산업을 본격적으로 형성할 수가 있는 사건들이 발생했다.

첫째, CIH 바이러스의 발생으로 정보화의 역기능에 대한 적신호가 울렸다. 직접적인 피해가 피부에 와 닿으면서 정보화 역기능에 대한 우려의 목소리가 높아졌다. 마침 불법 소프트웨어 단속도 이루어져 바이러스 백신업체는 가장 큰 수혜자로서 급성장의 피치를 올렸다. 바이러스 피해에 이어 '백오리피스 2000'과 같은 해킹 위협이 세계적으로 부각되면서 인터넷 해킹 문제가 일반인들에게 전파되는 인식의 전환이 일어났다.

둘째, 한국정보보호센터의 침입차단시스템 평가를 획득한 제품들이 시장에 출시되었다. 민간기업에서는 이미 침입차단시스템 제품이 도입되고 있었지만, 공공기관에서는 부진한 상태이었다. 평가과정이 끝나면서 공공 기관에서도 차입차단시스템이 확산되는 계기가 되었다. 그리고, 국내 제품이 권위 있는 정부 기관에 의해 검증이 되었다는 점이 정보보호산업의 큰 획을 긋는 계기가 되었다고 하겠다.

셋째, 전자서명법의 발효로 공인인증기관들이 준비를 하면서 전자상거래 시대를 맞이하는 정보보호 인식이 크게 확장되었다. 인증 솔루션을 준비해온 업체들이 인증기관이나 기업 전산 시스템에 자신들의 기술을 구축하면서 자신들의 기술을 검증해 갔다. 전자상거래가 인증 기반으로 이루어진다는 마인드의 확산도 자연스레 이루어졌다.

넷째, 분야별로 구조조정이 이루어지면서 인터넷 기반의 IT 인프라에 투자가 이루어지기 시작했다. 인터넷 인프라의 확산과 정보보호산업의 발전은 비례관계에 있어서 이는 아주 바람직한 현상으로 지적된다. 금융권에서는 경쟁 서비스를 위해 사이버 금융을 강화하면서 본격적인 해킹 방대책으로서 정보보호제품을 도입하기 시작했다.

한 마디로 말해서 이 시기는 민간 부문의 투자

분위기 회복이라는 점이 시장 성장에 기폭제 역할을 했다. 각 분야별로 인터넷 사업의 각종 모델들이 제시되고 있었고 e-business가 주요 패러다임으로 정착하면서 대기업을 중심으로 IT에 대한 투자가 이루어지기 시작했다. 정보통신산업에 종사하는 기업들이 전반적인 성장을 하게 된 것도 투자 분위기 유도에 도움이 되었다.

특히 정보보호 문제가 민감한 사안이 되는 통신업체, 금융기관 등의 인터넷 프로젝트들은 정보보호 분야가 상당한 비중을 차지하고 있다. 정보보호업체들의 입장에서는 자신들의 기술이 검증되고 더욱 도전적인 서비스를 개발할 수가 있어서 상당한 기술 향상을 기할 수 있는 계기가 되었다.

2.4 도약기 ('99.11 -)

이러한 준비기를 거쳐서 '99년도 하반기부터는 본격적인 도약을 하고 있다. 방화벽, 바이러스 백신 분야에서는 시장별로 판도가 이미 드러나고 있고, 인증 솔루션, 침입탐지, 시스템 보안 분야도 크게 인식이 확산되고 있다. 한편 IT 전반적으로 컨설팅이 높은 부가가치로 등장하는 것도 주목할 만한 추세이다. 무엇보다도 정보화 패러다임의 핵심 요소로 정보보호가 간주되는 것은 팔목할만한 개념의 변화이다.

또한 인터넷 전자상거래 산업이 급성장하는 것은 정보보호산업으로서는 청신호이다. 전자상거래에서 가장 중요한 정보기술이 정보보호 분야일 뿐만 아니라, 정보보호 측면에서도 전자상거래 구축을 위해서는 모든 기술과 솔루션이 총동원되기 때문이다. 그런 점에서 전자상거래가 안전하고 신뢰할 수 있는 환경이 구축될 수 있도록 도와주어야 하는 막중한 임무가 정보보호산업에 종사하는 이들에게 주어졌다고 해도 과언이 아니다.

아울러 국내 정보보호 업체들의 기술들이 시장에서 검증되어가고 있다. 정부의 보호막이 없는

시장에서도 경쟁하고 있다는 것은 그만큼 우리의 기술력이 성장해가는 표징이 되고 있다. 한편 아시아권에서는 우리 나라가 독자적인 정보보호 제품이나 기술을 가지고 있는 리더쉽을 가지고 있다는 사실은 앞으로의 잠재력을 보여주고 있다.

그러나, 아직 정보보호 산업이 제대로 정착하려면 정보보호의 중요성이 더 확실하고 강력하게 사회 전반적으로 각인되어야 한다. 필요한 성분이지만 그 규모가 미약하다면 산업이 성장하기에 충분한 동기부여가 되지 않는다. 그리고, 정보보호는 어중간한 솔루션은 통하지를 않는다. 모든 상황에 대해 치밀하게 대비책이 형성되어야 한다. 그런 점에서 일단 동기는 부여되었지만 아직 인터넷 산업의 탄탄한 인프라의 모습으로 갖추어지기에는 극히 초보 단계로 보는 것이 합당하다.

3. 산업의 구성

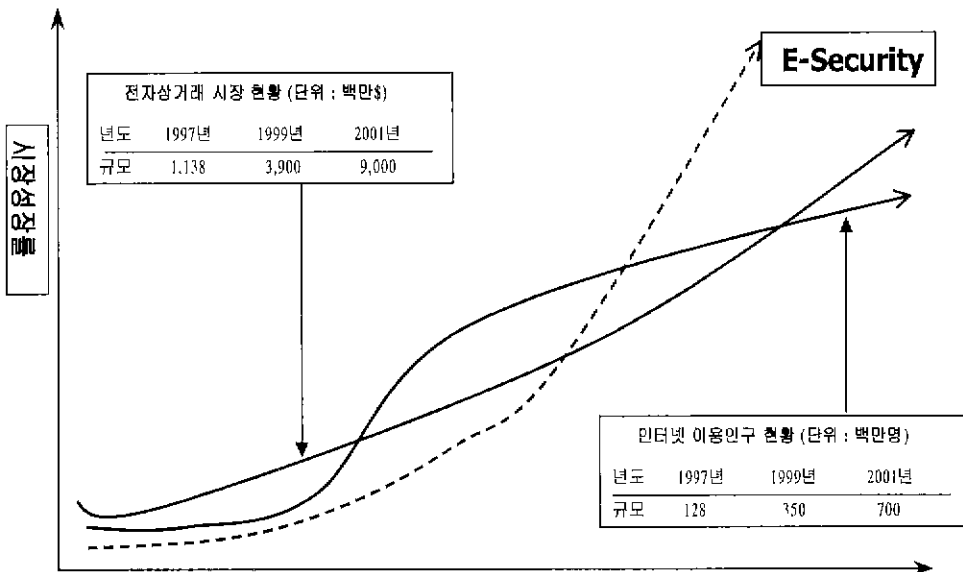
전세계적으로 인터넷 산업이 성장하는 것과 비례해서 정보 보호 시장 또한 폭발적인 성장을 거듭하고 있다. 그림 1은 시장 예측 자료로서 인트

라넷에서 전자상거래 서비스로 발전하면서 시장 규모는 기하급수적으로 성장하는 것을 볼 수가 있다. 이는 보안상의 위협성이 증가할수록 필요한 보안 기술과 서비스를 더 필요로 한다는 지극히 상식적인 가정만으로도 쉽게 예측할 수 있다. 인터넷 전문지인 인터넷월드(Internet World)에서 선정한 1998년 말에 급성장한 50개의 인터넷 상장 회사 중에서 8개가 보안 분야인 것만 보아도 보안 시장의 성장을 낙관할 수가 있다.

3.1 제품별 분류

정보 보호 산업은 제품적으로 보아서 크게 다음과 같이 분류할 수가 있다.

- √ 침입차단시스템(방화벽, Firewall)
- √ 바이러스 백신
- √ 시스템 보안
- √ PKI
- √ 침입탐지시스템
- √ Assessment & 컨설팅
- √ 기타 : PC 보안, 메일 보안



(그림 2) E-Security 시장 양적 성장

현재 시장 규모에 있어서는 침입차단시스템과 바이러스 백신 시장이 전년도 대비 2-3배로 커져서 가장 큰 규모를 차지하고 있다. 다른 분야도 규모가 계속 커지고 있는 추세이어서 향후 전체 정보보호산업은 연 2배 이상으로 커져 나갈 것으로 예상된다.

제품별로 유통 경로는 다소 차이가 있는데, 표 1은 주요 제품별로 유통되는 형태를 표시하고 있다. 여기서 SI 대리점은 시스템이나 네트워크 장비와 더불어 SI 형태로 납품하는 기업을 의미하며, 유통대리점은 PC 소프트웨어 유통망을 의미한다.

〈표 1〉 정보보호제품의 유통체계

	직판	SI 대리점	유통 대리점
침입차단시스템	●	●	
바이러스 백신	●	□	●
시스템 보안	●	□	
PKI	●	□	
침입탐지시스템	●	□	
Assessment & 컨설팅	●		

3.2 시장 구성

국내에서 시장 규모를 판단하는 데에는 상당한 어려움이 따른다. 대부분의 벤더들이 비상장 기업이어서 매출의 규모를 검증하는 것이 불가능하기 때문이다. 그러나, 전반적인 경향과 추세에 대해서는 예측이 가능하다.

민수시장의 경우 인트라넷과 전자상거래 시장으로 구분할 수가 있는데, 인트라넷의 경우 대기업을 중심으로 한 시장이 가장 먼저 형성이 되었다. 대기업들은 초기 투자 이후 그 규모를 확장하고 있는 추세이며, 중소기업들은 아직 제품 도입이 미미한 실정이다.

금융 시장의 경우 최근 은행, 증권을 비롯한 금융 시장에서 활발히 도입이 이루어지고 있는

현상이 고무적이다. 인터넷 뱅킹, 가상 은행, 사이버 트레이딩 서비스들이 조속시 준비되고 있으며, 여기에서 정보보호기술은 요소 기술로 취급되고 있다.

EC 쇼핑몰을 비롯한 시장에서는 '99년도 하반기부터 점진적인 성장의 곡선을 그리게 될 것으로 예상된다. 앞으로 전자상거래 시장은 인증기관이 얼마나 빠른 속도로 정착하느냐가 시장 형성의 변수가 될 것이다.

공공시장의 경우 '99년도부터 성장하기 시작했다. 그러나, 공공시장은 고객 숫자는 증대하지만 매출 규모는 그리 크게 성장하지는 않는 특성을 지니고 있다. 그 이유는 공공 시장의 구매 포인트가 가격이 최우선이고, 대부분 가격 입찰을 거치기 때문이다. 그러나, 보급이 타부분에 비해 다소 덜된 편이어서 앞으로 잠재성이 큰 시장으로 예측된다.

수출에 있어서는 아직 성과가 나타나지 않고 있다. 그러나, 정보보호산업의 역사가 아주 짧았고 현재 많은 업체들이 열심히 이를 준비하고 있는 것을 상기하면 2000년도에는 수출 실적이 나타날 것으로 기대한다.

4. 국내 정보보호산업 발전을 위한 대책

이제 국내 정보보호산업은 본격적인 도약의 길을 걷고 있는 것은 확실하다. 그 배경에는 폭발적으로 성장하는 인터넷 산업이 있는 것도 명약관화하다. 일부에서는 인터넷 산업의 거품성을 걱정하는 목소리가 크지만, 정보보호산업은 그 특성상 일과성이 되는 성격이 아니다. 정보보호산업은 고급 기술과 경험이 그 밑바탕이 되고 있다는 점이 거품의 가능성이 있는 여타 인터넷 서비스나 어플리케이션 분야와는 차원이 틀리다.

이렇게 어렵게 정착해온 정보보호산업을 우리나라 인터넷 정보화 산업 구축의 기반으로 삼기

위해서는 다음과 같은 대책이 마련되고 수행되어야 할 것이다.

4.1 정보보호에 대한 의지

앞에서 수차 지적되었듯이 인터넷 산업의 발전과 정보보호산업의 발전은 같은 맥락에 놓여있다. 어떻게 보면 정보보호산업은 인터넷 산업의 가장 핵심적인 요소로서 인터넷 산업의 정착에 성패를 좌우한다고 해도 과언이 아니다. 정보보호가 무너진 전자상거래가 어떻게 번창할 수가 있겠는가? 현재는 초기 단계이어서 별 문제가 아니지만 사이버 공간으로 모든 산업이 이동한다고 생각해 볼 때에 단순한 역기능의 문제로 구분하기에는 정보보호산업의 위상이 너무나도 크다.

그럼에도 불구하고 아직 많은 이들이 마치 정보보호산업은 별개로 존재하는 산업으로 인식하는 데에는 안타까움이 많다. 미국의 시장 조사나 산업 연구기관의 연구 결과에 따르면 모두가 인터넷 정보 보호 분야는 인터넷 솔루션 및 서비스의 핵심분야로서 분류하고 있다. 따라서, 인터넷 산업, 더 나아가 IT 산업의 전체 패러다임의 맥락에서 정보 보호를 보는 시각이 필요로 하다.

미국에서 CIO(Chief Information Officer)에 이어 CISO(Chief Information Security Officer)의 개념이 도입되고 정보보호대응체계가 대통령의 직접 관심사가 되는 것은 결코 일회성의 기술이 아닌, 정책적인 요소임을 말하고 있다. 정보보호는 최고위층에서 정책적인 차원에서 고려해야 하는 전략적 성분이다.

4.2 전문인력의 확보

정보보호 전문인력의 부족은 고질적인 문제이다. 사실 세계적으로도 정보보호 전문가는 그 수요를 따라가지 못하고 있다. 기술 인력만 놓고 보았을 때에는 크게 개발자와 컨설턴트의 두 가지 분야로 분류할 수가 있다.

개발자의 경우 전반적으로 하부 구조 인력이 취약한 점을 무시할 수가 없다. 정보보호 기술은 시스템 및 네트워크 기술에 기반을 하고 있기 때문에 시스템 관리, C 언어, 네트워크 프로그래밍을 기초로 한다. 이러한 기초가 어느 정도 바탕이 되어야 어플리케이션이나 서비스 분야의 제품 개발에 기여할 수가 있다.

컨설팅 분야에 대해서는 IT 전반 즉, 네트워크, 데이터베이스, Tool 등을 보는 경험이 필요하다. 물론 해킹 기법 등 공격 기술에 대한 전문가들도 컨설팅의 중요한 요소이다. 오히려 정보관리의 전반적인 체계를 이해하고 이들의 인프라를 구축해주는 상위 개념의 컨설팅이 우선적으로 자리잡아야 한다.

앞으로 이러한 전문인력들을 체계적으로 양성해 나가고 이들을 산업체에 공급해주는 정책이 수립되어야 한다. 아직 인력 양성의 초점 측면에서 잘 맞지 않는 경향이 있는데, 이에 대해 지속적으로 협의해 나아가야 바람직한 방향이 모색될 것이다.

4.3 정보보호에 대한 마인드 확산

정보보호는 우리가 정보화 사회에서 필수적으로 갖추어야 할 덕목이다. 문화적으로 여기에 적용할 수가 없다면 이미 사이버 공간에서 산업을 구축한다는 우리의 비전은 환상으로 끝날 수도 있다. 그만큼 정보의 가치에 대한 인식과 사이버 비즈니스에 대한 개념이 전제되어야 하는 것이다.

아직 국내에서 전체 기관이나 기업 중에서 기본적인 정보보호 인프라를 구축한 곳은 극히 일부분이다. 그리고, 설사 구축되었다 하더라도 이에 대한 지속적인 관리 체계가 잘 이루어지지 않고 있다. 이는 소비자층의 기술적 성숙도와 정보보호제품에 대한 기대 심리가 다양하게 존재하는 데에도 그 원인이 있다. 앞으로 산업계나 정부는 합심해서 정보보호의 마인드가 더 확산되어 나갈

수 있도록 노력을 경주해야 할 것이다.

4.4 산학(産學) 및 산연(産研)간의 역할 분담

2-3년 전의 상황과 달리 현재 정보보호기술 분야는 나름대로 잘 정의되어 있다. 확고한 솔루션 제품으로부터 그 근저를 이루는 기술 성분까지 기초 프레임워크는 정연하게 정리되어 있다. 따라서, 이제 기술 개발 측면에서 산학(産學) 과 산연(産研)간에 확고한 역할 분담을 필요로 하는 시점이라고 생각한다.

이미 국내 정보보호산업은 현재 서비스를 위해 필요한 제품을 공급할 수 있는 능력들을 갖추고 있다고 생각한다. 따라서, 앞으로 2년 내에 상품이나 솔루션으로서 갖추어야 하는 분야는 현재 시장을 알고 있는 기업들의 업무라고 생각한다.

그러나, 우리가 장기적으로 연구개발에 투자해야 하는 분야는 나날이 기술이 바뀌는 체제에서 경쟁하는 기업들로서는 역부족이다. 따라서, 3-5년을 내다보는 분야는 장기적인 안목에서 학교와 연구소를 중심으로 추진되어야 할 것으로 생각한다.

특히 이러한 프로젝트들은 기초 학문인 수학과 네트워크 이론, 운영 체제, 물성론 등에 기반하고 있다. 이 연구결과는 앞으로 암호 서비스, 스마트 카드, 차세대 네트워크 보안 제품, 위험 분석 시스템 등 다양한 제품에 적용될 수 있을 것으로 예상된다. 앞으로 이 방향에 대한 지속적인 협의를 통해 연구 개발의 역할 분담은 물론 인력의 양성 측면에서도 긍정적인 방향으로 정책이 설정될 것으로 예상된다.

4.5 글로벌 확장

궁극적으로 국내 정보 산업이 바라는 만큼의 성장을 하려면 국내 시장만으로는 한계가 있다. 따라서, 기술적인 자신감이 갖추어지면 글로벌하게 나아가는 비전을 수립해야 한다.

지금까지 정부의 보호 정책 하에 국내 정보보

호산업은 어느 정도 선진업체와의 격차를 줄여갈 수가 있었다. 그러나, 글로벌화 되어 가는 경제 속에서 지역적인 안도감만으로는 충분하지가 않다. 더구나, 인터넷 산업은 글로벌 스탠다드를 지향한다는 측면에서 보는 정책은 나라의 정보화 발전을 위해서도 바람직하지가 않다.

따라서, 앞으로 국내 산업의 활성화를 위해서 글로벌 경쟁 체제 분위기를 성숙시켜야 한다고 생각한다. 이미 몇몇 분야는 치열한 경쟁을 벌이고 있는데, 이는 기술과 발전과 시장의 확장을 위해서는 고무적인 현상으로 지적된다. 이는 치열한 생존 분위기에서만 세계 수준의 기술이 만들어질 수가 있다는 평범한 인식에 기인한다.

그만큼 국내 정보보호산업 업체들의 위상이 올라갔다는 것은 우리에게 좋은 신호이며, 이러한 현실 인식을 바탕으로 우리가 앞으로의 글로벌 성장 전략을 같이 그려갈 시점이라고 생각한다.

5. 결 론

미국에서의 정보보호산업은 이미 분야별로 안정기에 접어들어 10개 이상의 관련업체가 주식공개에 성공하여 그 규모가 확장되었다. 일단 주식공개가 되었다는 점은 만인이 인정할 수 있는 기업으로, 나름대로 성공한 기업으로 평가될 수 있음을 의미한다. 미국의 경우 Fortune 500 회사들이 인터넷 환경으로 급속도로 이동했고, 금융이나 공공 기관에서 팔목할만한 소비 계층을 형성하고 있어 시장 형성에 어려움이 없었다.

야후와 아마존으로 대표되는 인터넷 포털 사이트나 쇼핑몰들은 완벽한 정보보호시스템을 갖추고, 이 분야에 철저한 관리를 하고 있다. 이 과정에서 네트워크 보안이나 인증 시스템 같은 분야가 전반적으로 발전할 수 있는 계기가 되었다.

국내에서도 인터넷 기반으로 IT 인프라를 구성하여 정보화 사회를 지향한다는 것을 산업적으로

나 국가적인 지상 과제로 삼고 있다. 그런 점에서 정보보호산업의 위상은 크게 향상될 것으로 예상된다. 이제 정보보호가 정보화 사회에서 필수적인 기본기라는 인식이 일반인에게 확산된다면, 기술과 산업의 앞날은 밝다고 하겠다.

한편 해킹이나 바이러스는 국경 없이 발생하는 위협 행위이다. 따라서, 국내 인터넷 IT 산업도 국내의 위협만으로 경계 대상을 삼아서는 안 된다. 앞으로 글로벌한 경쟁력을 갖지 못한 정보보호기술이나 제품은 생존할 수가 없음을 이 분야에 종사하는 기업들은 잘 인식하고 있다. 그래서 앞으로 정보보호산업이 국내는 물론 세계 어느 곳에 나아가서도 경쟁한 산업으로 성장할 것을 기대한다.



김 홍 선

서울대학교 전자공학과 학사
서울대학교 전자공학과 석사
Purdue University 컴퓨터공학 박사학위 취득
1990년-1994년 삼성전자주식회사 선임연구원

1994년-1996년 TSI, Inc. 연구원
1995년 아이에스에스(주) 대표이사
1998년 ㈜시큐어소프트 대표이사
1997년-1998년 국제정보처리학술회의, NETSEC-KR 97/98, CONCERT 등 학회에서 프로그램 전문위원 및 운영 위원장 역임
관심분야 : 시스템 및 네트워크 보안, 정보보호시스템 평가, 정보보호표준화, 전자상거래 보안, 전자서명 인증, 공개키 기반구조(PKI)