

# 정보보호산업동향

이창길대리 | 한국정보통신산업협회 정보화기획팀

## 1. 서론

국내 초고속 인터넷 가입자가 2002년에 1천만명(1,040만명)을 넘어섰고, 인구 100명당 55.1명이 유·무선 인터넷을 이용하는 것으로 집계되었다.<sup>1)</sup>

이와 같은 추세는 국내기업의 사업기반을 인터넷 중심으로 바꾸어놓았을 뿐만 아니라 정보보호문제를 선택이나 조건이 아닌 인터넷의 필수적 기반으로 자리잡도록 만들었다.

〈표1〉 초고속 인터넷가입자 및 이용자수

	초고속인터넷 가입자수(100명 당)	인터넷 이용자수(100명당)
한국 (2002년)	21.8명	55.1명
미국 (2001년)	4.5명	50.0명
일본 (2001년)	2.2명	45.5명

가트너의 한 보고서는 2004년 미국기업의 80%가 사업과정 중 필수적인 부분으로 인터넷을 사용할 것이며, 이들 기업 중 50%는 2004년까지 인터넷과 관련된 사고로 심각한 재정손실을 입을 것이라고 내다봤다.

시장조사업체인 포레스터 리서치는 미 기업들의 보안관련 지출액이 2001년 56억7천만달러에서 2004년에는 1백97억 달러로 3배 가까이 증가할 것으로 전망했다.

최근 「1월 25일 인터넷 대란」으로 기업 정보보안에 대한 인식이 강화되면서 정보보호문제는 기술개발의 문제를 넘어선 거대한 사회조직 문화의 문제로 인식되기에 이르렀다. 네트워크 침해가 곧 사회자체의

1) 한국 eBusiness현황, 환경, 대책 (전자상거래연구조합 2003.3월)

위기가 됨으로써, 정보보호는 기술과 사회과학이 동시에 요구되어지는 것이다. 즉, 특정 기관·단체만의 문제라기 보다는, 보안에 대한 인식이 부족한 모든 기업과 사용자에 의해 파장이 커진 복합적인 사고이며, SQL worm과 같은 지능적인 자동 해킹 공격하에서는 기업이나 개인은 피해자이면서도 가해자(감염되어 타 시스템을 공격했다는 측면에서)가 될 수 있다는 점, 그리고 보안 불감증과 국가적 차원의 비상 관리체계의 중요성을 일깨운 사례라고 할 수 있다.

이에따라 경기침체로 모든 산업이 어려움을 겪고 있지만 보안산업의 미래는 모두의 주목을 끌기에 충분하다.

〈표2〉 최근 해킹 공격의 환경 변화

구분	과 거	현재
공격 형태	단순한 공격 기법	복잡화, 기법의 다양화
공격 툴	직접 프로그램한 툴을 이용	자동화된 해킹툴의 발달
공격대상	서버중심	PC중심
공격지 형태	소규모, 국지적 해킹	대규모 국제적인 해킹 대상의 증가
공격이유	자기과시 및 호기심	정보유출, 웹사이트 파괴 등

## 2. 국내 정보보호산업 특징 : 정보보호제품 및 서비스 시장분석

지난해는 IT 침체에 따른 동반 하락과 투자대비 효과 계량화의 어려움 등으로 인하여 Firewall, IDS, 안티바이러스(AntiVirus) 등 전통적 솔루션(Solution)군의 투자가 감소하고, 시장 포화에 따른 과다 경쟁으로 안티바이러스군의 성장이 둔화돼 이익률이 저조하였다.

또한 보안 컨설팅 시장도 기대 심리 과다 및 경쟁으로 인하여 전반적으로 이익률이 감소하였다고 볼 수 있다. 그러나, 전체 보안 솔루션 수출의 가능성을 확인하는 해 이었으며, 금융권 백업(Backup)망을 시작으로 본격적인 VPN시장이 개방된 해이기도 하다.

### 2.1 보안솔루션 통합화

시장변화 중 큰 특징 하나는 '통합'이라는 이슈를 중심으로, 이를 지원하는 신제품들이 속속 출시되는가 하면, 일부 벤더들은 개별 보안 소프트웨어 업체에서 통합 보안솔루션 프로바이더로 재포지셔닝 하는 등 다이나믹하게 움직이고 있다는 점이다. 이러한 요인은 각 개별 제품의 높은 비용대비 효과가 저조하고, 이기종 솔루션간의 상호보완이 어려우며, 관리 및 기능을 이용자가 쉽게 접근, 관리할 수 없다는 것이다.

특히, Firewall 시장은 통합 보안솔루션으로 재편성됨에 따라 개별시장에서는 비중이 감소하고 있는 반면 그동안 보안시장을 선도해왔던 안티바이러스를 포함하고 있는 SCM(Secure Contents Management) 시장은 여전히 지속적인 성장을 보이고 있다.

또한, VPN, IDS 등의 3A 시장도 지속적인 성장률을 기록하고 있는 추세이다. 인터넷보안산업은 크게 방화벽, 암호, 바이러스, 3A 등 5가지 시장으로 구분할 수 있는데, 3A란 Authentication(인증), Authorization(권

한부여), Administration(관리) 등 세 분야를 통칭하는 말로, 기업들이 고객이나 파트너와의 신뢰기반을 만들어 주는 핵심보안기술을 지칭하고 있다.

〈표3〉 3A의 개념 및 제품군

3A	개념	제품
Authentication인증	이용자 확인과정	PKI, VPN
Authorization권한부여	작업가능대상 확인과정	SSO(Single Sign-On)
		EAM(Extranet Access Management)
		PMI(Privilege Management Infrastructure)
Administration관리	보안솔루션 통합관리	ESM(Enterprise Security Management)



## 2.2 보안업계의 구조조정 필요성 대두

지난해에는 경기회복 둔화와 더불어 보안 소프트웨어에 대한 투자가 감소함에 따라 벤더(Vendor)간 경쟁은 무분별한 가격 경쟁으로 치달아 벤더의 수익 구조가 악화되는 부정적인 모습을 보여주기도 하였다. 이는 시장 규모에 비해 벤더가 너무 많아서 생기는 문제로 업계에서 구조조정이 일어나지 않는 한 이런 악순환은 계속될 것이다. 국내 보안 소프트웨어 시장의 발전을 위해 M&A 및 퇴출이 요구된다.

또한 한국IDC는 거의 비슷한 기술 수준을 보이고 있는 국내 기업들이 보안 소프트웨어 시장에서 더 많은 시장점유율을 확보하기 위해서는 제품 및 서비스의 차별화, 모바일 보안 강화, SMB 시장을 공략해야 한다고 제안하고 있다.

## 3. 정보보호산업 전망



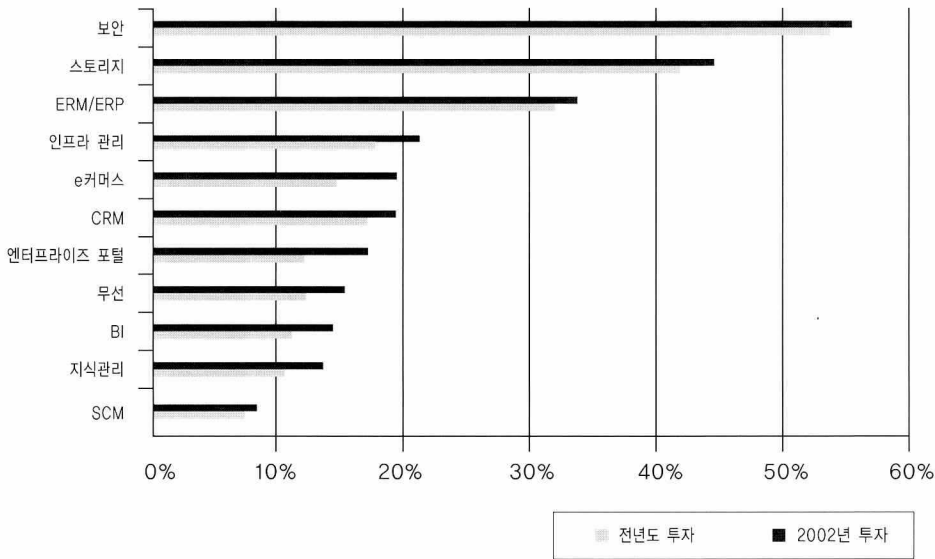
### 3.1 아·태 시장규모

일본을 제외한 아시아 태평양 지역 12개 국가의 CIO들이 2002년 집행한 IT투자에서 우선순위 1위로 보안 솔루션을 꼽았다고 IDC가 발표하였다. 아시아 태평양 지역 2,850개 기업을 대상으로 실시한 이번 조사 결과, 조사 대상 기업의 56%가 보안 솔루션 부문에 신규 투자를 한 것으로 나타났고, 스토리지 솔루션과 ERM솔루션에 각각 45%, 34%의 기업이 신규 지출을 한 것으로 응답하였다.

“이번 조사에 의하면, 2002년도 투자 성향은 보안, 백오피스 애플리케이션 등에 집중됨으로써 소위 ‘방어적,수비적(Defensive)’인 면에 치중해 있었음을 알 수 있다”고 IDC 아/태지역의 소프트웨어 및 서비스 리서치 부문을 총괄하고 있는 푸니 라자(Puni Rajah) 부사장은 전했다.”

이러한 투자 성향은 불안한 글로벌 정치 경제 상황에 따라 2003년에도 계속될 것으로 IDC는 예상하고 있다.

〈IDC Continuum 2003 Survey〉



### 3.2 국내 시장규모

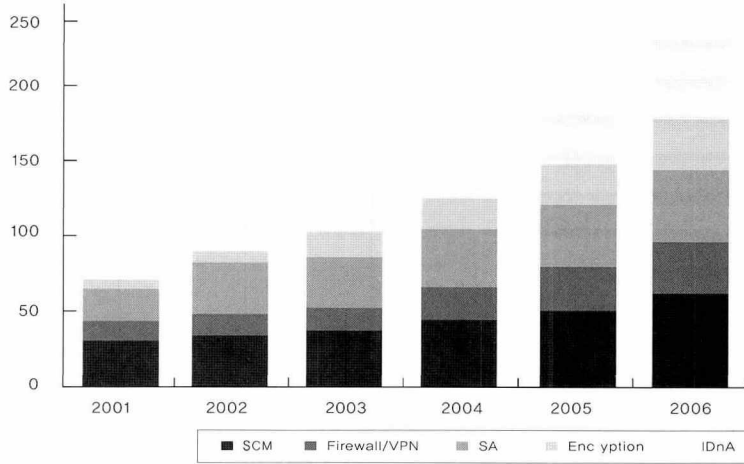
미래의 시장규모를 예측하는 것이 결코 쉬운 일은 아니지만, 정보보호산업이 성장할 것임은 아무도 부정할 수 없을 것이다. 한국IDC가 최근 발표한 ‘한국 보안 소프트웨어 시장 동향 및 전망보고서, 2002-2006’에 따르면, 국내 보안 소프트웨어 시장은 전년대비 24.8% 성장한 1억 천 2십만 달러에 달할 것이라고 밝혔다.

한국IDC에서 분류하는 5가지 세부 시장 중 가장 큰 시장은 안티바이러스가 포함된 SCM(Secure Content Management)으로 전년 대비 13.7% 성장한 3천 2백 4십만 달러에 이를 전망이며, 두번째로는 3A가 14.9% 성장한 2천 5백 4십만 달러 규모의 시장을 형성할 것으로 보인다.

IDS 및 취약점분석 소프트웨어 시장이 46.4%라는 가장 높은 성장률을 보이면서 2천 4백 6십만 달러 규모의 시장이 예상된다. 반면에 Firewall/VPN시장은 하드웨어 Appliance, Firewall/VPN 통합 Appliance 시장으로 급속히 옮겨감에 따라 전년에 비해 불과 1% 정도 성장한 1천 6백 2십만 달러에 이를 전망이다.

또한 안티바이러스, Firewall, PKI 등 몇 가지로 국한되었던 보안 소프트웨어의 종류도 SSO(Single-Sign On), ESM(Enterprise Security Management), Secure OS, 취약점분석 소프트웨어 등으로 보다 다양해지면서 보안의 적용 범위가 확대되어 시장의 성장을 돕고 있다.

[그림1] 국내 보안 소프트웨어 시장 규모 예측, 2001~2006



#### 4. 결론

그 동안 인터넷 사용의 확산으로 높은 성장세를 유지했던 보안산업은 투자대비 효과가 계량화되지 못하여 보안분야에 대한 투자가 미흡하였다.

2002년 선진국 보안투자 규모는 IT투자 대비 5.7% 수준인데 비해 우리나라는 2% 미만인 실정이다. 그러나 기업들의 모바일 인프라 구축 확장, 보안 적용 분야 확대, 정부정책 등과 맞물려 앞으로는 높은 성장이 예상된다.

IT 경기 하락에도 불구하고 전체 전년대비 약 25%의 성장을 예상하고 있으며, VPN, Giga Solution과 같이 신규 니즈(needs)에 의한 시장도 성장하며, 기존 솔루션의 다양화, 다각화에 따라 지속적인 성장을 가능하게 하고 있다.

궁극적으로 정보보호산업 활성화의 기반은 대중적 정보보호의식 수준의 제고에서 찾을 수 있을 것이다. 사회적 맥락 속에 정보보호문제를 끌어당겨 공감대를 형성하도록 하는 것이 중요하다.

훌륭한 정보보호기술이 개발되었더라도 기술 단독으로는 보안수준을 높이기 어렵다. 공공기관을 중심으로 정보보호마인드가 확산되어야 하고 또 관련 교육도 지속적으로 이루어져야 할 것이다.