네트워크 보안기술 Patent Map 분석

1. 기술의 개요

정보보호 기술이란 정보통신시스템을 통한 정보의 생산, 가공, 유통 과정에서 정보의 비밀성(정보유출 방지)과 무결성(데이터 위·변조 방지)을 유지하고, 각종 정보 서비스의 가용성을 보장하기 위한 기술을 의미한다. 즉, 정보보호 기술은 의도적으로 혹은 우연히 허가받지 않은 형태로 컴퓨터 및 통신망에 접속하여 정보를 누출, 전송, 수정, 파괴하는 등의 행위를 방지함으로써 유무선 통신, 시스템, 생체 등 관련 정보를 안전하게 생성·유통·저장·소비·인식·관리 하도록 하여 안전한 지식정보 사회 구현을 가능하게 하는 정보통신의 핵심 기반기술을 의미한다.

정보기술에 대한 응용 증가, 충분히 검증되지 않은 정보기술, 사이버 공격자의 다양화와 능력 향상으로 인한 위협 양상의 변화와 이에 대응하는 정보보호 기술의 다변화와 개념이 계속해서 진화하고 있는 기술로서, 과거에는 통신망 상의 전송 정보의 비밀성을 유지하기 위한 암호기술 중심의 영역에서 디지털경제 체제의 지식정보의 안전한 흐름을 보장하기 위한 요소기술로 영역이 확대되고 있다.

특히 위험이나 사고 관리, 프라이버시 강화 체계 구축, 국제적 상호연동 가능한 신뢰 프레임워크 조성, 대규모 분산 개방형 시스템·네트워크 환경의 보안관리 등이 중심 기술과제가 될 것으로 보인다.

국방·통신·금융·전력 등 국가주요 인프라의 운영과 인공심장 박동기, 자동차의 ABS 시스템 등 내장형 시스템(Life-critical), 인터넷 TV, 홈뱅킹 등과 같은 네트워크형 시스템 (Business-critical) 등으로 정보기술이 확대되고 있고, 이에 대한 사이버테러 등의 위협 증가에 따라 국가 주요 정보통신 시스템에 대한 정보보호가 주요한 국가·사회적 관심거리가 된다.

미래에는 단순히 정보통신 시스템을 공격으로부터 방어하는 개념에서 정보통신 서비스의 신뢰성을 포괄하는 안전·신뢰성(Dependability) 개념으로 진화할 것으로 보인다. 안전·신뢰성(Dependability)이란 컴퓨터 시스템이 제공하는 서비스에 당연히 부여되어야 하는 믿음으로 정의되며, 보안성(Security)·안전성(Safety)·신뢰성(Reliability)을 포괄하는 개념이다.

시스템 및 네트워크 보안기술에서는 현재는 시스템·네트워크에 대한 침입차단 형태의 단순·수동적인 방어개념이나 앞으로는 시스템·네트워크 자체의 안전성을 실시간 능동적으로 탐지·대응하는 형태의 제품이 대두될 전망으로 보인다.

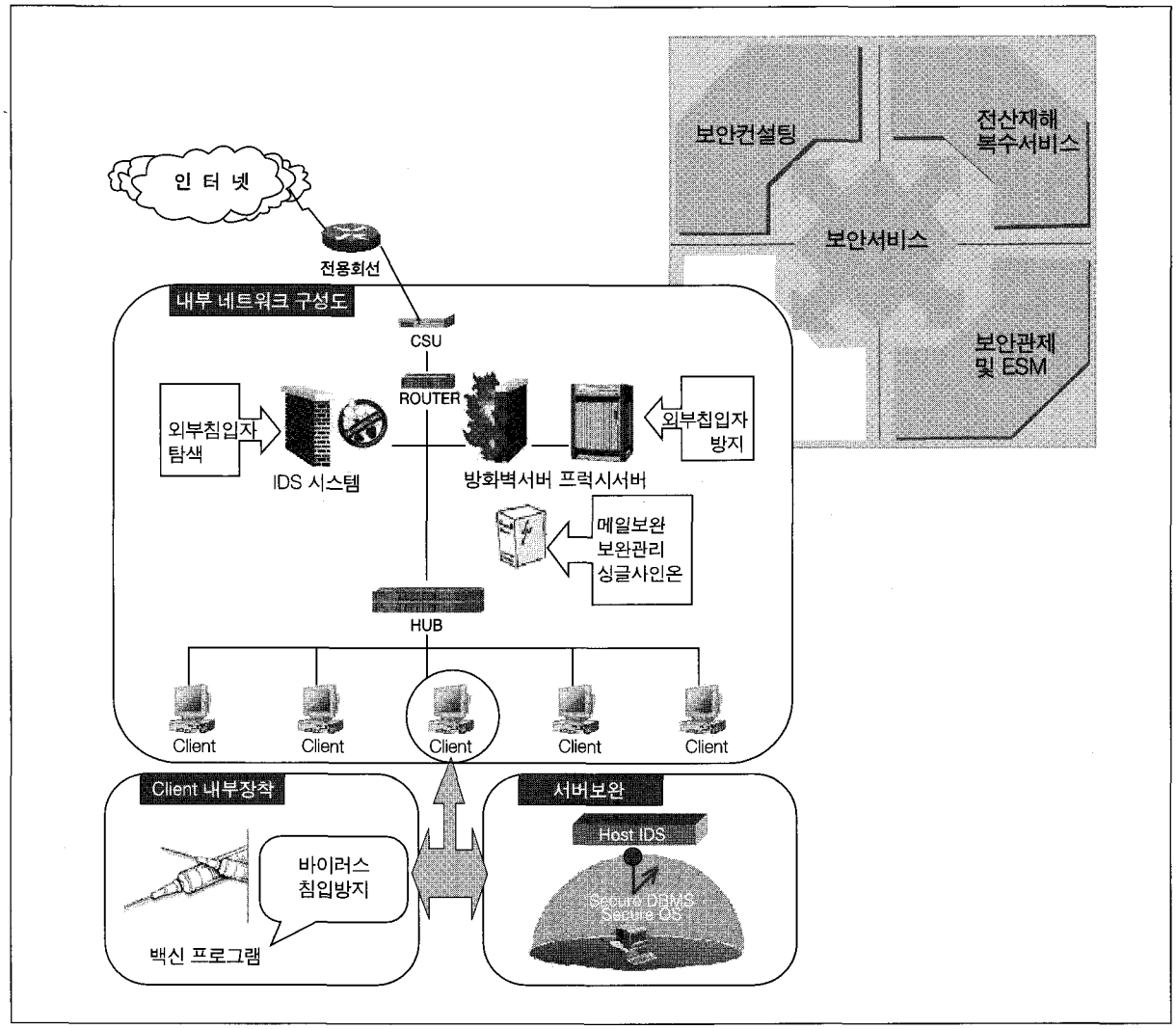
기존 정보통신인프라에 IDS, VPN 등 단위보안기술을 단순 부가시키는 차원이 아니라 자동 면역형 백신 등 시스템과 네트워크 자체의 능동형 탐지기능을 강화시키는 방향으로 발전될 전망이며, 보안 관리 기술은 현재는 ESM 기술이 주류이나 PBNM 기반 ESM기술, 관리성의 효율성이 극대화된 실시간 지능형 보안 관리까지 발전될 전망으로 보인다.

시스템 및 네트워크 보안은 지금까지 암호기반 기술에 의하여 Need to Know 즉 권한이 있는 사람이나 응용만이 해당하는 정보를 접근할 수 있다는 소극적인 방어 및 보호 정책에서 대량의 DDOS 공격과 worm 공격, 물리적인 테러 등에 의한 시스템의 가용성과 무결성을 강조하는 방향으로 이전되고 있다. 결국 정보보안이 물리적, 관리적, 기술적 보안관리 체계로 보았을때 기존의 물리적, 관리적 보안도 막중하지만 기술적인 심각성이 드러나면서 보안관리기술의 자동화, 실시간화가 더욱 중요한 과제로 떠오르고 있으며 기존의 보안 기술로서 침입차단, 침입탐지 등의 기술은 보다

지능화 및 고속화를 시도하고 있는 것이다.

컴퓨터 시스템 보안기술은 미 국방성이 제정한 TCSEC(Trusted Computer System Evaluation Criteria)에 근거하여 커널 후킹 기법을 이용한 서버 보안 제품이 상용보안서버 기술로서 각광을 받기 시작하고 있으며, 또한 네트워크를 경유하여 침입한 사용자에 대한 공격을 탐지하고 막기 위한 호스트기반 침입탐지 및 침입방지시스템(Intrusion Prevention System)이 한 축을 이루고 있다. 그리고 가장 중요하게 시장에서 축을 이루는 것은 안티바이러스시스템 기술이다. 안티바이러스는 기존에 알려진 바이러스 패턴을 가지고 분석하는 고전적인 방법에서 알려져 있지 않은 바이러스를 탐지하는 기법이 점차 널리 채용될 것이며, 악성소프트웨어 검출을 위한 스캐너 기술도 점차 중요하게 이해되고 있다. 또한 PC에 대한 해킹을 막고 탐지 및 관리를 하는 PC보안제품도 알려지기

▶ [그림 1] 시스템 보안, 네트워크 보안 및 보안 서비스 구성도



시작하고 있다.

네트워크보안은 네트워크에 대한 접근을 허용하는 싱글사인온(Single Sign On), 침입차단시스템으로 널리 알려진 방화벽시스템, 침입탐지기술로 알려진 IDS(Intrusion Detection System), 인터넷을 이용한 터널링 방식으로 사설망을 구축하는 가상사설망, 스팸메일을 막고 차단하기 위한 기술, 무선망 보안기술로서 무선LAN 보안과 무선보안기술이 최근 나타나고 있다. 또한 많은 보안제품을 기업이 가진 하나의 보안정책에 의하여 효율적으로 분산, 관리하도록 하는 보안관리기술은 정책기반 보안관리기술이 있으며, 또한 실시간으로 온라인 위협과 취약점을 관리하는 실시간위험관리 기술이 타나나고 있다.

또 하나의 보안기술로서 산업적으로 각광받는 것은 서비스 산업이다. 서비스 산업은 보안컨설팅, 대행서비스인 ESM(Enterprise Security Management) 기술 등이 각광을 받고 있다. 컨설팅은 재래적 방식에 의한 위험분석과 대책을 강구하는 컨설팅이며, ESM은 고객의 IT 자산을 대신하여 보호, 감시 및 탐지, 대응하는 기술을 지원하는 것이다.

여기에서는 네트워크 보안기술을 컴퓨터 시스템보안, 네트워크 보안, 보안서비스로 분류하였으며, 각각에 대해 세부기술로 또 다시 분류하였다. 분석대상 데이터는 1982년~2001년 사이에 출원된 해당특허 중에서 출원공개 또는 등록공고된 것이며, 한국의 경우 KIPRIS를 미국, 일본의 경우에는 Delphion의 DB를 활용하였다.

2. 산업 및 시장동향

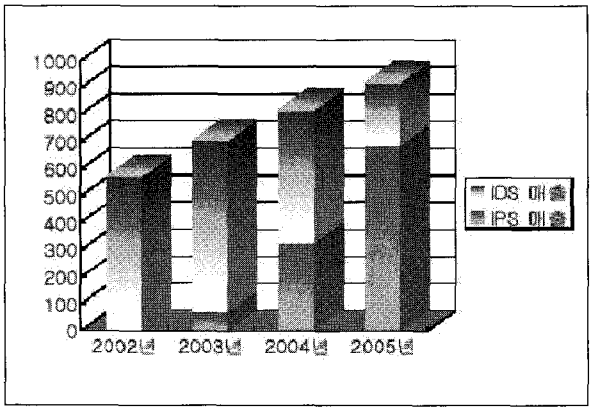
현대 리서치의 2002년 9월 자료에 따르면 국내 보안시장의 무선 인터넷 보안 분야는 2003년까지 성장률 279%가 증가한 546억원의 시장 규모를 예상하였으며, 정보 보호 컨설팅의 166% 성장률을 비롯하여 대부분의 보안 시장이 50% 이상의 성장률을 보일 것

▶ [표 1] 국내 보안시장 현황

(단위 : 억원, 출처 : 현대 리서치 2002.9)

구 분		2000	2001	2002	2003	성장률
기존 보안 시장	VPN	468	878	1,571	2,357	71%
	인증, 지불	230	483	874	1,477	86%
	암호화	150	308	554	841	78%
	바이러스 백신	205	350	543	895	63%
	방화벽	220	352	489	641	43%
	PKI	40	210	441	750	166%
	침입 탐지	60	150	285	490	101%
	정보 보호 컨설팅	35	90	198	376	121%
	소계	1,313	2,581	4,472	6,961	74%
신규 보안 시장	통합관리 서비스	60	168	353	635	120%
	무선 인터넷 보안	10	90	266	546	279%
	인증서비스	20	110	209	334	156%
	소계	185	608	1,311	2,381	134%
총 계		1,498	3,189	5,783	9,342	84%

▶ [그림 2] 전세계 IDS/IPS 시장



(자료 : 가트너 2002. 8)

으로 예상하였다.

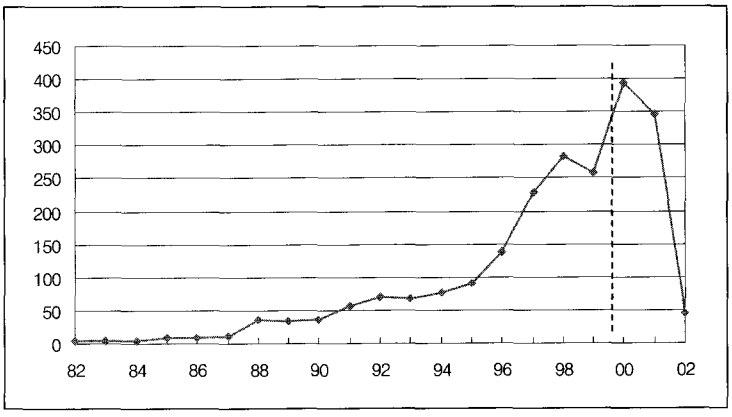
한편 세계 보안산업 시장은 정보기술 산업 성장이 느리게 진행됨에도 불구하고 급성장하여, 2001년 170억달러에서 오는 2006년 450억달러 규모로 팽창할 것이라고 시장 조사기업 IDC가 2003년 2월에 밝혔다. 또한 차세대 보안솔루션으로 주목을 받고 있는 침입방지시스템(IPS) 시장이 본격적으로 열리고 있음에 따라 2003년 상반기까지 개념 차원에 그쳤던 것과는 달리 2003년 하반기에 접어들어 국내외 보안업체들의 침입방지시스템 제품의 출시와 더불어 이에 대한 시장 점유율이 높아질 것으로 예상된다.

현재 네트워크 보안분야에서는 네트워크 상의 모든 정보보호 솔루션이 유기적으로 연계되어 해킹 등의 사이버테러를 사전에 탐지하고 차단할 뿐 아니라, 이를 역추적 · 복구까지 지원하는 능동형 통합 솔루션이 등장하고 있다. 지금까지는 방화벽과 VPN을 결합한 통합이 대세였으나 이제는 방화벽과 VPN을 기본으로 IDS/IPS, 바이러스월, IP 공유, 유해사이트 차단, 인터넷 트래픽 제어, 인터넷 응용 프로그램 통제 등 통합의 범위가 전방위로 확산될 전망이다.

3. 특허출원현황

1991년 말 미국은 정보통신 기술개발과 응용을 촉진하기 위해 고성능컴퓨터법을 제정하였으며, 1993년에는 이 법에 따라 미국 경제의 경쟁력을 제고시키고 세계 경제의 주도권을 확보하기 위하여 NII(National Information Infrastructure)라는 미국의 국가적인 정보화 전략을 발표했으며, 그에 따라 네트워크 보안기술 및 컴퓨터 시스템 보안기술의 중요성이 대두되었다. 일본은 1990년대 초반까지 세계 경제의 주도권을 쥐고 있었으나 사회가 고령화되고 일본 경제의 구조적 문제가 누적되면서 정보화를 통해 돌파구를 찾아야 한다는 공감대가 형성되었다. 이러한 분위기와 미국의 NII정책이 함께 작용하여 1994년 5월 '21세기 지적사회로의 개혁을 위하여 정보통신기반정비 프로그램'을 발표했다. 미국 · 일본 그리고 유럽연합의 정보화 정책은 1990년대 중반 이후 우리나라 정보화 정책에 지대한 영향을 끼쳤다. 이에 따라, 1995년 8월 정보화촉진기본법이 제정되고, 1999년 Cyber Korea 21을 수립, 추진하면서 인터넷 이용자

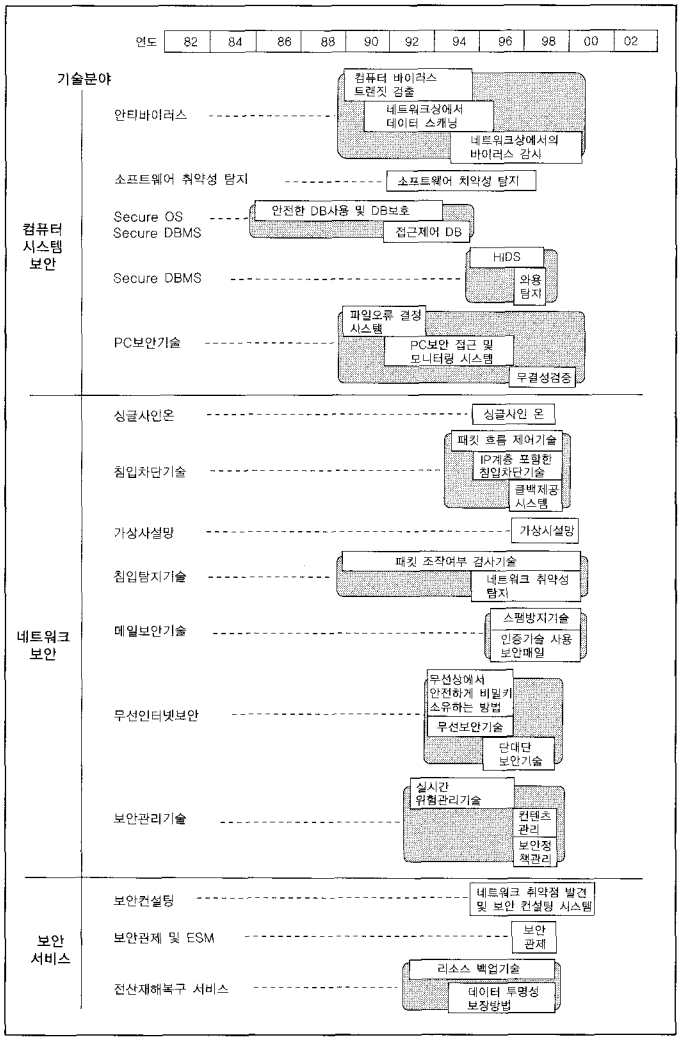
▶[그림 3] 전체 출원연도별 특허출원(등록) 동향



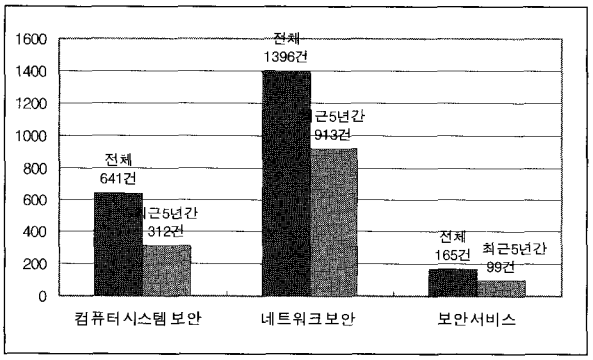
수 뿐만 아니라 전자상거래 규모도 확대되면서 해킹이나 바이러스와 같은 정보화 위협 요소들이 등장하였으며, 2001년에는 1월부터 6월까지 즉 상반기에만 총 7,422건의 사이버 범죄가 발생하였는데 이 중 2,206건이 사이버테러 사건이었다는 통계적 수치를 볼 때 컴퓨터 시스템 보안 및 네트워크 보안 분야에 대한 관심도가 급속도로 높아졌음을 알 수 있다. 따라서, 특허 출원 동향도 각 국가별 정보화 정책과 연계되어 나타남을 알 수 있다.

전체 출원건수/최근 5년간(98~2002년) 특허출원 동향을 살펴보면, 네트워크 보안, 컴퓨터 시스템 보안 및 보안서비스 모두 최근 5년간(98~2002년) 특허 출원이 폭발적으로 활발하게 이루어졌음을 알 수 있으며, 이는 컴퓨터 시스템에 관련된 운영체제 및 바이러스는 1970년대부터 등장하기 시작하였으며, 그에 따라 컴퓨터 시스템 보안에 대한 인식이 확산되었으며 다른 보안 기술에 비해 일찍 국가정보기반구조 구축과 국방용으로 정부기관과 군사기관들이 사용하기 위해 정부차원에서 기술개발을 진행하였기 때문인 것으로 해석할 수 있다.

▶[그림 5] 기술발전도



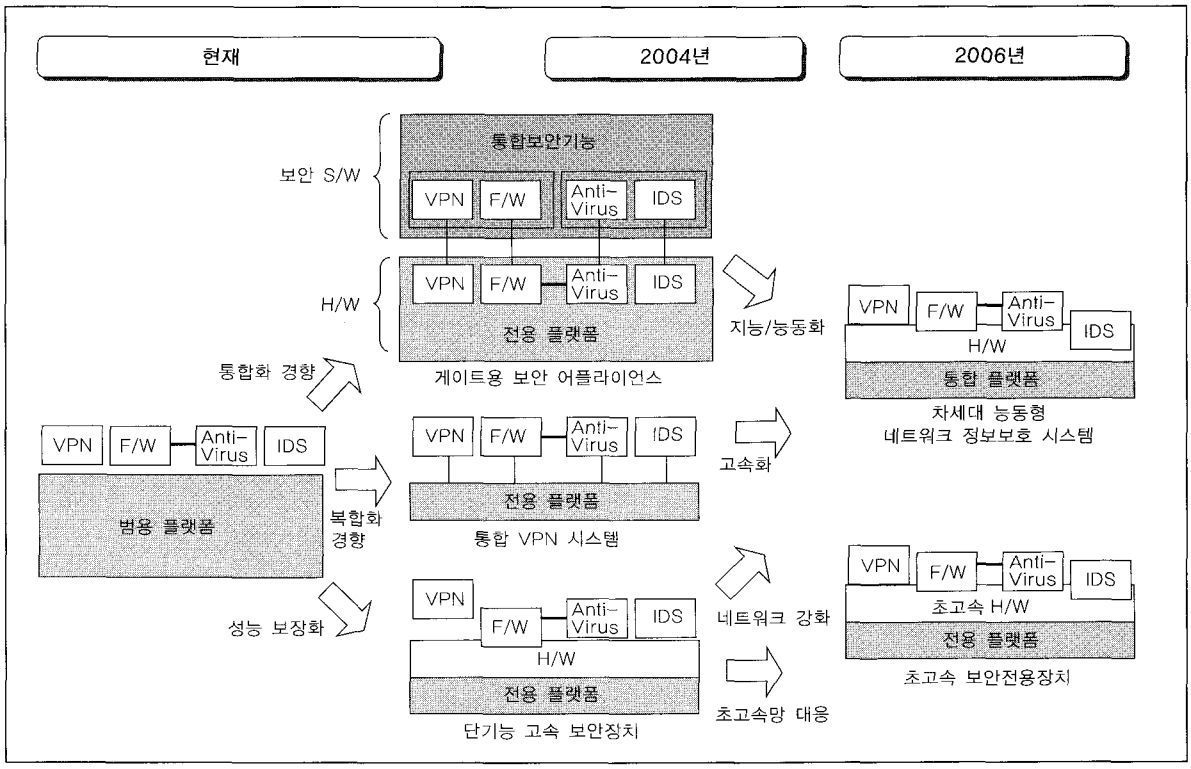
▶ [그림4] 전체국가의 기술별 최근 5년간[98~2002년]



4. 결 론

(그림 5)에서 시스템 보안기술은 네트워크 보안 기술이나 보안 서비스 기술에 비해 기술 발전이 일찍 시작되었음을 알 수 있다. Secure DBMS의 경우에는 80년도 초반부터 기술이 발전하기 시작하여 다른 기술에 비해 일찍 기술이 개발되었음을 알 수 있다. 네트워크 보안 기술 중 침입탐지기술을 제외한 다른 기

▶ [그림 6] 보안시스템의 발전방향



술들은 90년대 중반부터 발전되기 시작하였으며, 보안 서비스의 경우에는 가장 최근인 90년대 후반부터 발전되기 시작되었음을 알 수 있으며, 향후 인프라 공격에 대한 대응이 네트워크 중심의 자동 대응 패러다임으로 교체되는 것이 불가피하여 "자동 공격, 자동 대응(automatic response to automatized attack)"이 공격과 방어의 패러다임으로 자리 잡을 것이라 판단된다.

네트워크 보안기술의 경우 데이터 처리속도의 향상으로 인하여 기가비트를 넘어 초 기가비트 시대로 진입하면서 능동형 솔루션이 빛을 발할 전망이다.