인터넷과 더불어 급신장

최근 국내의 CIH 바이러스 사건이나 미국에서의 멜리사 바이러스 등에서 보듯이 정보보호 대책 부재가 사회 전반적으로 다양한 파급효과를 미칠 수 있음을 보여주고 있다. 따라서 이 글에서는 대표적인 정보보호 기술과 국내 정보보호 제품 및 업체 동향를 소개하고 신뢰성 있는 제품 선택 가이드 라인을 제공하려 한다.

노병규/한국정보보호센터 시험평가팀 선임연구원

정보화가 급속도로 진전되고 정보통신기술의 발달로 인하여 공공 및 민간 분야에서의 정보시스템 사용이 증가하고 정보통신망에 대한 의존도가 확대됨에 따라 인터넷 등 개방적인 정보통신망과의 상호접속으로 인한 정보의 유출, 파괴 위·변조 등 각종 해킹 및 컴퓨터 범죄와 같은 정보시스템의 역기능적 측면이 빈번히 발생되고 있다.

또한 보안성이 결여된 전자우편의 사용에 따른 개인의 프라이버시 침해 및 전자우편 주소를 도용한 스팸메일, 메일폭탄 등의 사용에 따라 불필요한 정보를 검색하기 위한 사회적 낭비가 우려할 만한 수준에 이르렀다.

또 정보통신망 기술의 발전으로 인한 웹의 등장으로 새로운 개념적 방법론이 사회적·경제적 패러다임의 변화를 요구하게 되었으며 각 기업들은 자사의 홍보와 상품의 홍보를 위하여 홈페이지를 운영하고, 심지어 개별 인터넷 사용자들까지도 자신들의 홈페이지를 운영하는 등 인터넷의 대중화, 일반화를 촉진시켰다.

그러나 웹을 통한 홈페이지나 정보서비스는 웹서버나 홈페이지를 잘못 구성하거나 관련 CGI(Common Gate Interface)등의 잘못된 구현으로 여러 가지 보안취약점들을 보유하고 있어, 최근 해커들의 주요 공격 대상이 되고 있다. 특히 웹관련 서비스는 불특정 다수를 대상으로 서비스를 제공하므로 한정된 사용자만을 대상으로 하는 안전대책과 보안정책을 수립하기 힘든 형편이다.

최근에는 국내의 CIH 바이러스 사건이나 미국에서의 멜리사 바이러스 등에서 보듯이 하나의 정보보호 대책 부재가 사회 전반적으로 다양한 파급효과를 미칠 수 있음을 보여주었다. 이러한 역기능을 해소하기 위한 대책으로서 사회적인 인식제고를 위한 정책·제도적인 부분, 보안관리자의 관리 능력에 대한 관리적인 부분, 기술적으로 운용될 수 있는 정보보호기술 측면으로 분류할 수 있다.

다행히 최근에는 정부 등에서 이에 대한 중요성을 인식하고 정보보호를 위한 대책수립에 적극적으로 나서고 있으며 기업에서도 정보보호 기술의 중요성이 부각되어 다양한 정보보호제품을 개발하여 이와 관련된 수요도 점차적으로 증가하고 있다.

대부분 수입제품에 의존하던 국내 정보보호제품도 일부 분야에서 중소기업 및 벤처기업을 중심으로 국산제품 개발에 착수하였으며 이미 많은 성과

를 거두고 있다.

사회전반에 걸쳐 정보보호 필요성에 대한 인식을 제고하고 정부나 기업이 정보보호에 대한 문제점에 적극적으로 대처한다면 정보보호 시장이 보다 활성화될 뿐만 아니라 정보보호기술 자체가 최신기술이기 때문에 선진국에 비하여 커다란 격차가 없어 국가 경제적인 측면에서도 국가 경쟁력을 높이는데 커다란 도움이 될 것이다.

정보보호 기술 현황

정보보호기술은 접근하고자 하는 정보에 대하여 가용성, 기밀성 및 무결성을 제공하기 위한 수단이다. 이러한 특성을 제공하기 위하여 기본적으로 소요되는 기술은 다음과 같다.

〈표 1〉 국내 침입차단시스템 개발업체

업 체 명	제 품 명
대정정보통신	대정파이어월 (DJFW)'
매직캐슬	'매직캐슬'
시큐어소프트	'수호신' 'SecureShield-Firewall'
어울림정보기술	'시큐어웍스(SecureWorks)'
인젠	'NeoGate'
지란지교소프트	'넷세이프(NetSafe)'
켁신시스템	'화랑'
한국정보공학	'인터가드(Inter-Guard)'

가. 암호화 기술

정보보호기술의 기반기술이며 인가된 사람만이 보유하고 있는 정보를 이용하여 보호하고자 하는 자료를 임의로 변형하여 인가되지 않은 자에 대하여 아무런 정보도 노출시키지 않는 기술이다.

이 기술을 구현하기 위한 방법으로서 키의 형태에 따라 대칭키 암호와 비대칭 암호기술로 분류될 수 있으며 상호 인증, 부인방지, 키분배 및 무결성 등을 제공하기 위한 방법으로써 최근 비대칭 암호를 널리 이용하는 추세이다.

나. 인증 기술

시스템에 접근하고자 하는 사용자의 특성을 이용하여 신분확인을 수행하는 기술로써 아는 것에 대한 인증, 소유하는 것에 대한 인증, 개체의 특징에 의한 인증으로 구분될 수 있다.

아는 것에 대한 인증은 패스워드를 이용하는 단방향 인증, 일회용 패스워드를 이용하는 양방향 인증 등이 있으며 소유하는 것에 대한 인증은 스마트카드, IC 카드, 개인용 토큰 등을 이용하며 개체의 특징에 의한 인증은 지문이나 성문 또는 홍채인식을 이용한 생체 인증기술로 최근 활발히 연구되고 있는 영역이다.

다. 무결성 기술

시스템내의 자료 또는 전송되는 자료가 외부의 의도적인 공격 또는 사고로 의하여 임의로 변경되지 않았음을 보증하는 기술이다. 이러한 무결성을 검사하기 위하여 일반적으로 단방향 함수인 해쉬함수가 널리 사용되며 해쉬함수는 다음과 같은 요구사항들을 최소한 만족하여야 한다.

- 임의의 크기의 입력 데이터에 대하여 적용 가능하여야 한다.
- 일정한 크기의 해쉬 코드를 출력하여야 한다.
- 해쉬함수와 입력 값이 주어졌을 때 계산하기 쉬운 구조를 가져야 한다.
- 해쉬함수와 해쉬코드를 이용하여 역으로 입력 데이터를 추출하는 것이 계산적으로 불가능하여야 한다.

해쉬함수로 많이 사용되는 함수는 MD5(Message Digest), MD4, SHA(Secure Hash Algorithm), DES과 같은 단방향 함수 특성을 가진 것이다.

〈표 2〉 국내 침입차단시스템 개발업체

제 품 명	개 발 국	개 발 업 체	주요공급업체
CyberGuard	미국	CyberGuard Corp.	DST, NICSTECH, 아이네트기술, 한화/정보
Firewall-1	이스라엘	Checkpoint Software Associates	싸이버텍 홀딩스
Gauntlet	미국	TIS	한일정보통신
GUARDIAN	이스라엘	NETguard	삼양데이타시스템
WATCHGUARD	미국	Watchguard Lab	송림시스템, 스탠다드네트워크시스템
AltaVista	미국	Digital Equipment Corp.	한국 디지탈
Eagle	미국	Raptor System Inc.	NetCom, 한국정보공학
Borderware	미국	Border Network Tech.	MJL
GFX	미국	Global Technology Associates	한국엑시스
PIX	미국	Network Translation	Cisco Korea, 한화/정보
IBM Firewall v3.0	미국	IBM	한국 IBM
Firewall/Plus™	미국	Network-1 S&T	교보정보통신
보더메니저	미국	노벨	한국노벨
FIREBOX 11	미국	Watchguard Lab	농심데이타 시스템

라. 접근통제 기술

주어진 자료 또는 자원에 대하여 접근을 할 수 있는 권한을 부여하는 기술이며 접근여부를 결정하므로 써 불법적인 자원에 대한 자료 유출 및 파괴를 방지할 수 있다.

접근통제 기술은 사용자, 프로세스와 같은 주체나 그룹의 신분에 근거하여 자료와 같은 객체에 접근을 제한하는 임의적 접근통제(Discretionary Access Control), 객체에 포함된 정보의 기밀성과 이러한 정보에 대하여 주체가 갖는 허가권에 근거하여 객체에 대한 접근을 제한하는 강제적 접근통제(Mandatory Access Control) 및 역할기반 접근통제(Role-Based Access Control)등으로 분류될 수 있다. 대량의 자료를 보유하는 데이터베이스 시스템은 사용자에게 주어진 권한에 따라 접근을 제어하는 접근통제기술이 중요한 부분을 차지하고 있다.

〈표 3〉 국내 암호화 제품 자체개발업체

업 체 명	제 품 명
대정정보통신	DJRSA
미래산업 소프트포럼	XecureWeb
시큐어소프트	HASP
이니텍	RSADLX, SecurityGate-128
장미디어 인터렉티브	CEAL '98'
중앙제지	Data Crypto
켁신시스템	화랑동자, SecureXpress, KEEP2'
펜타시큐리티시스템	PACA

〈표 4〉 국내 개발 1백 28비트 대칭키 암호알고리즘

암호알고리즘명	개 발 기 관
SEED	한국정보보호센터, 한국전자통신연구원, 국방과학연구소 공동개발
Keep2'	고려대-켁신시스템 공동개발
PACA	포항공대-펜타시큐리티시스템 공동개발

정보보호 제품 동향

가. 침입차단시스템 (Firewalls)

국내 정보보호시장은 침입차단시스템 소프트웨어 업체들이 초기시장의 주도권을 장악한 가운데 점차로 시스템 보안과 침입탐지 시스템 등 유관분야로 확산되고 있다.

국내 초기 정보보호시장은 침입차단시스템인 Firewall-1(이스라엘 체크포인트사), Gauntlet(미국 TIS사), 'Raptor-Eagle', 'Borderware' 등을 공급하기 시작하면서 활성화되기 시작했다. 이렇게 외국산 제품 중심으로 시장을 주도하는 가운데 독자기술로 사이버게이트인터내셔널, 아이에스에스, 켁신시스템, 한국정보공학 등 국내 소프트웨어 개발업체들이 국내 보안실정에 맞는 자체기술로 개발한 국산 침입차단시스템을 개발해 오면서 활발해지기 시작했으며 지난해 11월에는 국산 침입차단시스템의 양대 업체인 사이버게이트인터내셔널과 아이에스에스가 합병하여 시큐어소프트를 설립함으로서 앞으로 시장점유율과 보유 제품군에서도 상당한 경쟁력을 확보할 것으로 예상된다.

나. 암호화 제품 (Encryption Products)

국내 암호화제품 시장은 이미 국제적으로 암호의 성능이 검증되어 표준으로 정착되어 사용되고 있는 국제 표준 암호 알고리즘들을 순수 국산 기술로 개발하고 있다. 국내 자체 개발한 암호화 제품은 〈표 3〉과 같다.

국내 개발의 128비트 대칭키 암호알고리즘에는 SEED, 킵투세븐, PACA가 있다.

다. 바이러스백신 제품 (Anti-Virus Products)

신종 바이러스들이 날로 증가하는 가운데 이를 치유할 수 있는 바이러스 백신제품도 수요가 증가하고 있다. 국내 백신 소프트업체들은 백신 프로그램과 침입차단시스템 솔루션을 하나로 병합한 별도의 소프트웨어를 개발해 게이트웨이 차원에서 파일과 함께 암호화한 바이러스를 잡아내는 솔루션 개발에 적극 나서고 있다.

이처럼 안철수-시큐어소프트, 하우리-세넥스, 시만텍, 트랜드-사이버텍홀딩스 등의 백신 업체들과 침입차단시스템 업체와의 전략적인 제휴는 인터넷과 같은 네트워크 환경이 확산됨에 따라 네트워크의 불법 침입을 탐지하는 침입차단시스템과 컴퓨터 백신 프로그램을 통합해 사용하려는 요구가 커짐에 따른 것이다.

라. 접근통제 제품 (Access Control)

외부의 불법적인 침입을 막기 위한 침입차단시스템(Firewall)에 이어 침입차단시스템 안에 있는 사내 비인가자들의 해킹 행위를 방지하기 위한 사내 보안 소프트웨어들도 등장하고 있다.

〈표 5〉 국내 바이러스 백신 개발업체

업 체 명	제 품 명
시큐어소프트	'바이러스 월'
안철수컴퓨터바이러스연구소	'V3시리즈'
하우리	'바이로봇'

〈표 6〉 기타 바이러스 백신업체

업체명	제 품 명
트렌드	PC-Cillin, Server Protect, InterScan VirusWall, ScanMail, VSAPI(virus scan API), TVCS(Trend Virus Scan System)
시만텍	한글Norton AntiVirus, 한글Norton Utilities

〈표 7〉 내부 침입자 접근통제 소프트웨어

공급업체명	제 품 명
사이버텍홀딩스	이스라엘 보안 소프트웨어업체인 멤코사의 멀티플랫폼 유닉스 오픈시스템 보안 소프트웨어인「SeOS」공급
한국휼래티뉶	「오토시큐어」공급
브이플러스	이스라엘 핀잔사의 자바 어플릿 보안 소프트웨어인 「서핑게이트(서버용)」와 「서핑쉴드(클라이언트)」공급

터(ECRC) 등으로 대형 프로젝트 발주가 잇따르고 있으며 증권, 은행 등 금융권의 사이버뱅킹 시스템 도입도 늘어나고 있다.

이에 따라 전자상거래 종합솔루션 업체인 한국오라클, 한국IBM, 마이크로소프트 등이 대형 사이트를 중심으로 치열한 수주경쟁을 벌이는 한편 싸이버텍홀딩스의 웨브로마트, 다우기술, 이네트정보통신, 파이언소프트 등 국내 쇼핑몰 저작도구 전문업체들도 중소시장을 중심으로 경쟁대열에 가세하고 있다.

인터넷 사용자의 진위여부를 판별하는 CA제품은 전자서명법, 전자거래법 등 EC환경을 위한 제도정비와 맞물려 대중화 단계에 접어들 것으로 예상된다. 인터넷 쇼핑몰 등 EC환경에서는 단일 보안용도의 제품이 전자지갑, 지불게이트웨이 등과 결합되면서 '통합지불보안솔루션'이 각광받을 것으로 보인다.

바. 인증제품 (Authentication)

인증은 사이버뱅킹, 전자상거래, 보안정보접근 등 사용자 암호확인이 필요한 모든 곳에 적용된다. 최근 사이버 금융고객이 증가하고 전자상거래가 확산되면서 시장잠재력이 엄청나게 커지고 있다. 올해부터 은행들도 인증시스템을 도입하고 있다.

사용자들이 상거래를 포함한 모든 전자적거래와 문서교환을 신뢰할 수 있도록 정부가 전자 서명법으로 그 효력과 안전을 보장함으로써 현재 시범서비스와 특정분야에 한정돼 있는 전

마. 전자상거래 제품

국내 전자상거래 시장은 기업과 소비자간 거래규모만 집계해볼 때 지난 '97년 63억원에서 지난해 150억원 규모의 시장을 형성, 100%이상의 성장률을 나타냈다고 한다. 특히 최근 전자상거래 관련 보안기술이 급성장, 신용카드 결제에 대한 불안감이 해소되면서 소비자들의 이용이 급증하고 있다. 또한 기업의 전자상거래(EC) 도입이 본격화하면서 솔루션업체 간의 수주경쟁이 한층 가열되고 있다.

최근 전자상거래를 도입한 주요 사이트는 삼성물산의 삼성쇼핑몰, 한국정보통신진흥협회의 사이버쇼핑엑스포, 정보통신부의 우체국전자상거래사업, SK그룹의 전자상거래사업, 전자상거래 교육기관인 전자상거래지원센

〈표 8〉 국내 개발 접근통제 제품

업 체 명	제 품 명
미래산업 소프트포럼	OnceID & OASIS, Xecure IC 1.0, XecureWeb 3.0
삼성에스디에스	MagicGuard
세넥스테크놀로지스	X-Filer
시큐어소프트	수호신 VPN, 수호신 Remote
에스제이아이앤씨	Secure UNISQL (?)
인터넷시큐리티코리아	SecureServer, SecureToken, SecureCard, SecureSoft
퀵신시스템	화랑 파수병, 화랑동자

〈표 9〉 '세계보안표준(SET)'을 바탕으로 한 전자상거래서비스 (사이버쇼핑몰)

업 체 명	홈페이지 주소
삼성물산	www.sism.co.kr
쌍용정보통신	www.s-mart.co.kr
LG소프트	hishop.lgsoft.com/hishop
한국통신	www.Mall21C.co.kr
한솔텔레콤	shopping.HanQ.net

※ SET (Secure Electronic Transaction) : 별도의 패스워드를 사용, 구매자가 정당한 고객이라는 것을 확인하고 거래내용을 암호화함으로써 안전한 전자상거래를 가능하게 하는 보안솔루션

자상거래가 일반화, 대중화될 것이란 전망이다. 이처럼 전자서명이 법적으로 유효해짐에 따라 관련 전문업체들은 전자상거래의 주체인 인증(CA: Certification Authority)시장이 큰 규모로 성장할 것으로 보고 있다.

전자서명법 제3조 1항에 따르면 전자서명을 이용할 사용자는 전자서명이 당사자에 의한 것임과 서명 송신 후 서명 사실을 임의로 부인할 수 없도록 당국이 인정한 인증기관의 인증을 받아야 한다. 당초 법안에서는 인증관련 기술을 확보한 업체를 인증기관으로 '허가' 한다고 규정했으나 의결된 법령에서는 '인정' 하는 것으로 하향 조정했다.

그간 인터넷 보안 솔루션을 개발해 온 관련업체들이 직접 CA서비스를 제공할 의사를 밝히는가 하면 공공기관에서는 CA서비스를 시범 실시 중에 있거나 사업계획을 세운 것으로 알려져 CA서비스 시장 붐이 크게 형성될 전망이다. 한편 CA솔루션 시장도 함께 활기를 띠고 있다. 인증기관이 자유롭게 설립되고 CA서비스가 확대 실시되면 CA솔루션 수요 역시 늘어날 것이란 기대 때문이다.

특히 국내 업체들의 시장 전망은 매우 밝은 편이어서 전자서명 인증(CA) 시장은 올해 새로운 수요 창출을 유도, 센세이션을 불러일으킬 것으로 예상되고 있다.

사. 침입탐지 (Intrusion Detection)

침입차단시스템의 국산화가 잇따르고 있어 내년 상반기부터는 침입차단시스템과 함께 침입탐지시스템이 국내 보안 솔루션 시장을 주도하는 핵심 솔루션으로 자리잡아 가고 있다.

그 동안 국내 침입탐지시스템 시장에는 몇몇 외산 제품만이 출시된 상태였지만 내년 상반기부터 잇따라 국산 침입탐지시스템을 출시할 계획이어서 이 시점이 되면 본격적으로 시장이 형성될 전망이다.

이처럼 침입탐지시스템이 침입차단시스템에 이은 차세대 보안 솔루션으로 부각되는 주된 이유는 침입차단시스템이 해킹됐을 경우 이에 따른 피해를 최소화하고 네트워크 관리자 부재시에 시스템 자체적으로도 해킹 등에 대응할 수 있는 보안 솔루션에 대한 요구가 늘고 있는 상황에서 침입탐지시스템이 이 같은 요구를 해결할 수 있는 솔루션이기 때문이다.

보안 관련 전문가들은 "침입차단시스템의 도입이 이뤄지고 나면 침입차단시스템이 해킹된 이후의 문제를 처리할 수 있는 좀더 신뢰성 있는 보안 솔루션이 요구되고 이의 대안이 곧 실시간 침입탐지시스템"이라며 침입탐지시스템의 시장 형성 자체를 기정 사실화하고 있다.

국내 침입탐지시스템 개발 업체로는 펜타시큐리티시스템이 지난 8월 싸이렌을 발표한 이후 인젠의 네오와처, 대정아이앤씨의 DJ IDS, 세넥스테크놀로지의 어슈어디텍션(개발코드명), 시큐어소프트의 수호신 IDS 등이 있다.

이 업체들은 내년 상반기부터 본격적인 침입탐지시스템 시장이 형성될 것으로 전망하며 약 100억원대

〈표 10〉 국내 사용자인증시스템 개발업체

업 체 명	제 품 명
금향정보통신	OneToOne
대정정보통신	대정파이어월 (DJFW)
미래산업 소프트포럼	OneID, SFCA
인터넷시큐리티코리아	SecureServer, SecureToken, SecureCard, SecureSoft
켁신시스템	화랑, 화랑파수병

〈표 11〉 국내 CA솔루션 개발업체

업 체 명	제 품 명
삼성 SDS	트러스트 프로(Trust Pro)
소프트포럼	국내 처음으로 인증서 발급관리 솔루션인 SFCA' 개발
시큐어소프트	수호신CA
LG-EDS	스마트CA
이니텍	이니텍 CA 서버
장미디어 인터렉티브	JMI Certification Authority (자바로 개발한 인증기관 구축서버인 JCA 서버 2.0'을 버전업, 또 전자메일에 필요한 전자서명과 데이터암호화 기능을 제공하는 전자우편 보안솔루션인 TSmail'을 JCA와 연동시키는 기술인프라 선보임)
펜타시큐리티시스템	ISSAC

〈표 12〉 국내 침입탐지시스템 개발 제품

업 체 명	제 품 명
대정아이씨앤씨	DJIDS
세넥스테크놀로지	어슈어디텍션(개발코드명) 개발중
시큐어소프트	수호신IDS
인젠	네오와처 (NeoWatcher)
지씨텍	넷킵이
펜타시큐리티시스템	싸이렌 (Siren)
한양AGO	소도98

〈표 13〉 국내 침입탐지시스템 개발 제품

업 체 명	제 품 명
네트워크어쏘시에이츠 코리아	'사이버캅' 발표
타이타게이트인터내셔널	'OmniGuard/ITA' 수입
동부정보기술	'SessionWall-3', 'Elron Internet Manager' 수입
시큐어소프트	미국 ISS로부터 'RealSecure' 도입, 국내 공급 추진
아이빌소프트	Cisco사의 'NetRanger', 'NetSonar' 도입, 판매
퀵신시스템	아비넷사의 'SessionWall-3' 도입, 판매

이상의 시장 규모를 보일 것으로 예상한다.

아. 일회로그인 (Single-Sign-On)

일회로그인(Single-Sign-On)이란 클라이언트서버, 인트라넷 등 다른 기종의 여러 시스템을 사용할 때 시스템마다 서로 다른 ID와 비밀번호(Password)를 입력하지 않고 한 번의 인증만으로 전 시스템을 하나의 시스템처럼 사용할 수 있는 기술을 말한다.

외국의 여러업체들이 'Single-Sign-On' 관련제품을 개발, 출시하고 있으나 이는 해당업체의 하드웨어, 소프트웨어 환경에서만 작동하고 있는 가운데, LG-EDS 시스템사가 다양한 이기종 시스템에서 통일적으로 적용할 수 있는 통합사용자인증시스템(Single-Sign-On)제품을 출시했다.

Secure 운영체제 및 Secure DBMS

가. Secure 운영체제

다중 등급(Top Secret, Secret, Confidential, Sensitive But Unclassified)의 비밀 자료를 처리하는 주요 기관에서 사용될 수 있는 것이 다중 등급 구조(Multi Level Structure)를 갖는 운영체제이다. 각 등급을 위한 영역은 논리적으로 완전히 분리되어 있어 운영체제의 허가 권한 없이는 상호간섭이 불가능하다.

접근통제 정책은 기본적으로 하위등급사용자는 상위등급의 내용을 읽을 수 없고(No Read Up) 상위등급의 사용자는 하위등급의 자료에 쓸 수 없는(No Write Down) 강제적 접근통제 특성을 보유한다. (만일 이러한 특성이 없다면 어떠한 일이 발생하는지 상상해보라!)

또한 이러한 접근정책은 자료의 보관을 위한 저장소뿐만 아니라 운영체제 전반에 걸쳐 자료 이동시 권한이 부여되지 않은 불법접근 또는 불법 유출을 막기 위해 CPU, 메모리, 프로세스, 공유데이터, 메모리/프로세스 관리자, 라이브러리, 감사기록, 논리적인 파이프, 포트 등 모든 자원에 대하여 통제정책을 수행한 후 사용권한을 획득한다. 모든 객체의 등급 변화는 사용자에 의해 변경 불가능하고 오직 관리자에 의해 부여된 보안 정책에 의해서만 변경 가능하다.

최근에는 다양한 사용자 보안 요구사항에 맞도록 운영체제 내에 원하는 모듈이나 서버를 추가하거나, 삭제할 수 있는 구성의 유연성과 모듈성을 갖도록 하기위해 마이크로 커널 구조에 대한 연구가 활발히 이루어지고 있다. 즉, 다양하게 요구되는 보안기능을 갖는 안전한 운영체제를 만들기 위해서 최소의 신뢰성 있는 마이크로 커널을 기반으로 그 위에 운영체제의 다른 서비스 기능을 서버 형태로 구성하는 추세이다.

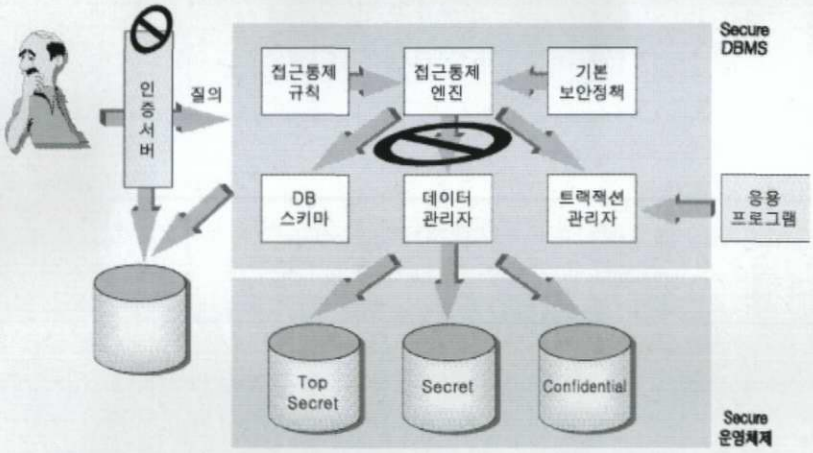
이는 다양한 사용자의 보안정책에 대처할 수 있는 유연성(Flexibility), 사용자에 적용 여부를 모르게 자동적으로 처리되는 투명성(Transparency), 다른 모듈 혹은 서버들과의 독립적인 평가가 가능하며, 분해될 수 있는 모듈성(Modularity), 가능한 한 위협을 여러 단계에서 막을 수 있는 계층적 보안(Layered security) 등의 디자인 원칙을 운영체제에 사용자 레벨의 서버로서 적용하는 것이 가능하다.

나. Secure DBMS

Secure DBMS는 많은 자료를 보유하고 있는 데이터베이스에 각 자료가 다중 등급(Top Secret, Secret, Confidential, Sensitive But Unclassified)으로 분류되어 해당되는 등급의 사용자에게 부여된 등급 자료에 접근할 수 있는 기능을 가지도록

설계된 DBMS이며 기존 DBMS에 이러한 접근통제 정책을 수행할 수 있는 통제규칙과 통제엔진을 탑재하여 구성한다.

사용자는 최초에 인증서버를 통하여 인증을 수행하고 Secure DBMS에 접근할 수 있다. 자료에 접근하기 위한 온라인 질의 및 응용프로그램에 의한 발생된 트랜잭션은 Secure DBMS에 전달이 되고 접근통제를 위한 Secure DBMS 내부의 통제엔진은 보안정책과 보안규칙을 참조하여 해당 등급의 자료에 대한 접근권한을 부여한다. 자료의 검색 또는 저장은 운영체제의 파일 매니저에 의하여 수행되며 보안성을 강화하기 위하여 Secure 운영체제를 이용할 수 있다. 인증과정 및 접근통제에 관련된 모든 사항은 감사추적을 위해 로그된다.



〈그림〉 Secure DBMS 구성도

〈표 14〉 침입차단시스템 평가 제품 현황

구 분	수 량	제 품 명	등 급	비 고
평가 완료	2	SecureShield-Firewall V1.0	K4	'98. 11. 종료
		SecureWorks V1.0	K4	'99. 2. 종료
평가진행	5	화랑 V1.5	K4E	
		인터가드 V1.5	K4	
		매직캐슬 V1.0	K4	
		화랑 V2.0	K4	
		SecureShield-수호신 V2.0	K4E	
평가 철회	1	수호신 Internet V1.0	K4E	신청 업체의 평가 철회
자문 진행	7	DJFW	K4	
		넷세이프	K4E	
		네오게이트	K4	
		태극진	K4	
		외국제품 3건	K3	

〈표 15〉 국외 Secure DBMS 평가현황

평가기준	등급	제 품 명	제품수
TDI (미국)	B1	Sybase Inc.의 Secure SQL Server Version 11.0.6외 5종	8종
	C2	Informix Software Inc.의 INFORMIX-Online/ Secure 5.0외 1종	
ITSEC (영국)	E3	Oracle Corporation의 Oracle 7 and Trusted Oracle 7 Release 7.0.13.6외 1종	2종

※ TDI : Trusted DBMS Interpretation Of The TCSEC
※ ITSEC : Inforrmation Technology Security Evaluation Criteria

5. 정보보호 제품 평가

보안기능에 대한 성능 및 신뢰도가 검증된 정보보호시스템 보급 촉진을 위하여 정보통신부에서는 '99년 2월 정보통신망 침입차단시스템 평가기준 및 평가지침서를 고시하였으며 한국정보보호센터에서는 '98. 2월 23일부터 평가제도를 시행하고 있고 현재 평가중 또는 평가진행중인 제품은 다음 〈표 14〉와 같다.

또한 한국정보보호센터에서는 안전 · 신뢰성 있는 정보보호 환경 구축을 위하여 각종 정보통신망에 사용되는 침입탐지시스템, 인증제품, 접근통제제품, Secure 운영체제 및 Secure DBMS 등 모든 정보보호제품군에 대한 기준을 개발하고 있으며 기준 개발과 동시에 평가를 시행하기 위한 준비과정에 있다.

참고로 미국과 유럽에서 평가 완료된 Secure DBMS는 〈표 15〉와 같다.