主題

정보보호 기술 개발 전략

한국전자통신연구원 조 현 숙

차 례

요 약

정보화 시대의 급속한 진행에 따라 하드웨어에 기반한 기간망의 구축과 함께 다양한 형태의 정보를 안전하게 관리할 수 있는 정보보호 서비스 시스템의 구축이 매우 중요한 시점이다. 세계 시장 경제의 기본 패러다임을 바꾸는 전자상거래 등의 새로운 서비스가 발달함에 따라 정보의 안전과 신뢰를 보장할 수 있는 정보보호 시스템의 필요성은 매우 강조되고 있다. 아직까지 국내의 정보보호 산업은 중소기업 및 벤처기업을 중심으로 제품이 개발되는 초기단계로 볼 수 있다. 지식과 정보를 보호하기 위한 여러 선진국의 노력을 고려할 때, 국제공동연구를 통한 경쟁력 있는 첨단기술을 확보하는 것은 불가능하다. 따라서 지식과 정보 자원의 유출을 막기 위해서 국가적 차원에서 기업, 연구소, 학교가 함께 범국가적인 차원의 독자적인 기술확보가 필요하다. 전자상거래 등의 인터넷에 기반한 다양한 서비스를 위한 정보보호기술의 표준, 정보보호의 핵심 및 기반 기술, 차세대 통신망 정보보호 기술, 시스템 정보보호기술, 해킹 방지 기술 등을 국가적인 차원에서 추진하고 응용서비스 등의 분야는 민간부문에서 추진하는 것이 바람직하다.

I. 서 론

정보보호 기술의 개발 전략의 추진 배경과 기술개발의 필요성을 먼저 살펴보면 먼저 통신상의 중요 정보의 기밀성 확보를 통한 안전한 정보사회의 기반을 구축하는 것이 매우 중요하다.

국가의 안보나 외교상의 정보 등의 국가의 안위를 위해 필요한 정보를 보호하고, 재산적 가치가 있는 기업 등의 민간정보 보호, 개인의 프라이버시를 보호하는 개인정보 보호 등을 위한 기술을 구현함으로써 신뢰할 수 있는 정보사회의 기반이 구축된다.

현재 추진중인 "Cyber Korea 21" 사업과 초고속 정보통신망, 차세대 인터넷 사업의 성공을 위해 시기 적절한 정보보호 기술을 개발하는 것이 필요하다.

현재 항바이러스 및 일부 암호화 제품을 제외한 분야에서 국내 자체개발된 정보보호 관련 핵심기술을 대부분 외국회사에 의존하고 있기 때문에 국내의 정보보호 산업체의 부가가치성 증대 및 수입대체 효과를 위해서 정보보호기술 개발이 요구된다.

국내 기술에 의한 정보보호 기틀을 마련함으로써 정보 주권국의 위치를 유지하며 세계 정보사회에서의 우위를 차지할 수 있다. 최근에 발생한 주요 인터넷 사이트에 대한 해킹공격과 같이 개방형 정보통신망의 확산에 따라 정보통신시스템의 보안상 취약성이 가중되고 있는 환경변화에 효과적으로 대처하기 위해서 비인가 사용자에 의한 시스템 접근, 사용, 데이터 위조 및 변조, 데이터 파괴 등의 대처수단을 확보해야 한다.

전자상거래 및 전자화폐 등의 새로운 응용서비스를 효과적이고 안전하게 구축하는 데 필요한 사용자 식별 및 인증, 거래내용 확인 등을 위한 정보보호 대책 및 기술을 확보해야 하며 정보화 역기능을 방지하고 순기능을 극대화함으로써 건전한 정보사회를 건설할 수 있다. 이를 통하여 Cyber 경제를 활성화하고, 초고속 멀티미디어 서비스의 안전성을 보장해 줌으로써 향후 새롭게 제공될 전자투표, 사이버뱅크, 주문형 비디오 서비스 등의 출현을 촉진할 수 있다.

새롭게 등장하고 있는 차세대 인터넷 보안 시스템, 차세대 IC 카드, IMT-2000 및 무선 인터넷 정보보호 시스템, JAVA 보안 기술 개발 등의 시장을 확보하기 위해 암호, 인증, 전자서명 등의 기술개발을 통해 국내 정보보호 산업의 대외 경쟁력을 강화하고 통신망에서의 정보보호를 기반으로 새로운 고부가가치 서비스를 제공함으로써 신규 서비스 도출의 발판을 마련해야 한다.

Ⅱ. 정보보호 기술

1. 정보보호의 정의

정보보호란 인터넷을 포함한 정보통신망, 단말 등에서 처리되는 음성, 영상, 데이터, 멀티미디어 서비스에서 정보의 유출 및 손상, 시스템파괴, 바이러스 등의 각종 보안위협 요소로부터 정보통신시스템을 보호하고 정당한 사용자의 신분을 확인함으로써 정보공유 및 근거리/원거리 접근 등의 각종 정보 서비스의 가용성을 보장하고 활성화시키기 위한 기술적 활동이다. 아울러 정보보호산업은 정보보호를 위한 하드웨어, 소프트웨어 제품, 서비스를 설계, 개발, 생산, 구축하고 이를 이용한 정보보호대책 마련 및 사후관리 활동을 포함하는 경제활동으로 정의된다.

정보보호 제품 및 서비스의 기능은 다음과 같이 분류된다.

(1) 기밀성 (Confidentiality)
: 송수신되는 데이터 또는 저장된 데이터의 불법적인 유출을 방지

(2) 무결성 (Integrity)
: 송수신 데이터 또는 저장된 데이터의 불법 변경 여부를 검사

(3) 사용자 확인 및 인증 (Identification & Authentication)
: 사용자의 신원과 송수신 데이터의 송수신자를 확인하는 서비스

(4) 접근제어 및 모니터링 (Access Control & Monitoring)
: 임의의 시스템에 대해 허가되지 않은 사용의

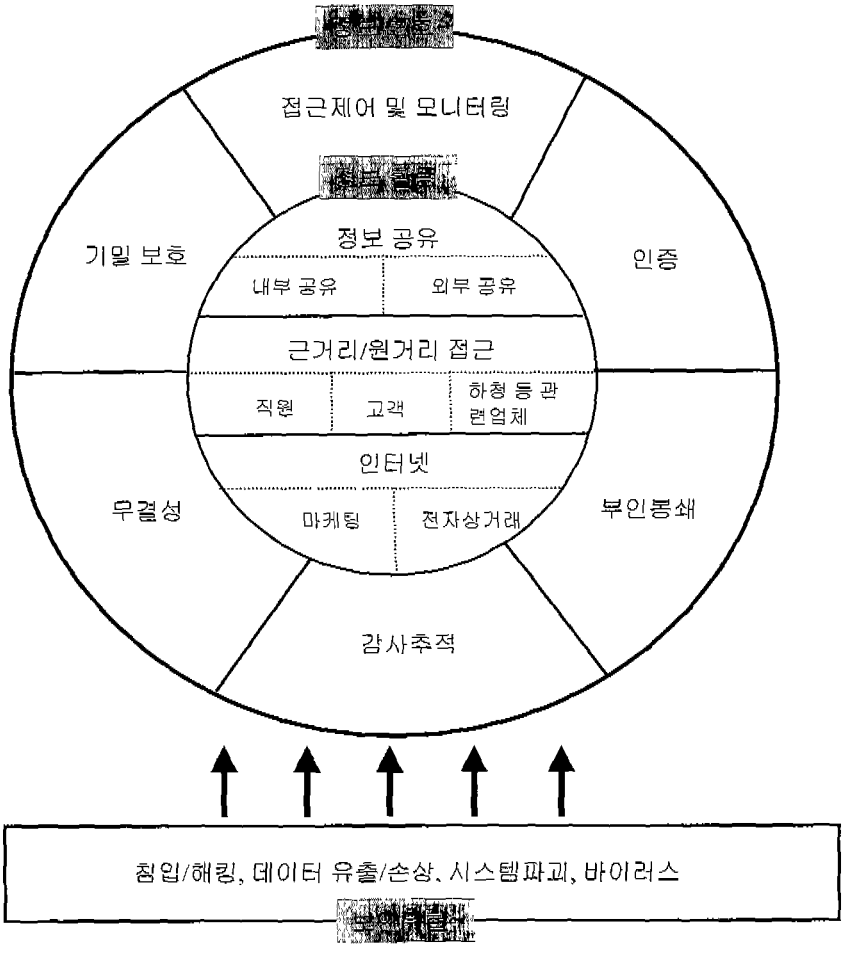

그림 1. 정보보호산업의 활용 및 응용

접근 및 사용을 제어

(5) 부인봉쇄 (Non-repudiation)
: 송수신된 데이터에 대한 분쟁시 제3자가 송수신자 및 송수신 내용을 확인

(6) 감사추적 (Auditing)
: 대상시스템에서 정보보호 관련 사건들을 기록

2. 정보보호 기술의 분류

정보보호 기술은 하드웨어와 소프트웨어로 분류할 수 있으며, 기능 및 소요기술, 시장 점유율 등을 고려할 때 크게 9개의 제품군으로 분류된다. 그러나 정보보호 기술의 발전과 시장성 등을 고려할 때 향후 2003년 경에는 6-7개 군으로 줄어들 전망이다.

3. 정보보호기술의 분류

정보보호 기술은 정보보호의 기초가 되는 기반기술을 개발하는 정보보호기반기술분야와 정보보호기술의 적용 대상에 따른 네트워크정보보호기술분야, 시스템 보호기술분야, 응용서비스보호기술분야와 보안관리분야 그리고 정보보호 표준 및 평가분야로 분류된다.

표 1. 정보보호 기술 분류 및 기능

정보보호 제품	기 능
항바이러스(anti-virus)	- 바이러스 등의 시스템 유해요소의 진입을 차단하고 손상된 시스템을 복구하는 소프트웨어 또는 하드웨어
방화벽(firewall)	- 공공 또는 사설 망으로부터 다른 망으로의 침입을 저지하는 소프트웨어 또는 하드웨어
암호화제품(encryption)	- 특정 정보의 암호화를 통해 사용자가 해독을 위한 적정한 키를 가지고 있지 않으면 사용할 수 없게 하는 제품 - 암호화 알고리즘은 대칭과 비대칭 알고리즘으로 구분됨
가상사설망 (VPN: virtual private network)	- 공공 IP망에서 필요한 두 지점간 안전한 커넥션을 만들어 줌으로써 실질적인 사설망이 가능하도록 하는 제품
공개키기반 (PKI: public key infrastructure)	- 공개키를 이용한 인증을 하는 프레임워크로써 제3자가 전자서명서를 발급하면서 사용자의 신원확인 작업 수행
인증(authentication)	- 사용자의 신원을 확인 - 비밀문자를 이용한 소프트웨어적인 방법과 지문이나 망막등의 개인속성을 이용한 하드웨어적인 방법이 있음 - 인프라가 포함되지 않는다는 측면에서 PKI와 구별됨
보안 IC카드	- 반도체를 포함하는 IC카드에 암호 알고리즘을 이식하여 컴퓨터 접근제어나 사용자 신원확인에 사용
보안관리 (security management)	- 보안관리를 쉽게 하도록 돕는 제품으로서 침입탐지와 검사기구 등을 통해 무결성을 확보하는 작업을 수행
보안시스템(secure system)	- 컴퓨터 운영체제나 DBMS 등의 시스템 프로그램의 기능상 보안 취약성을 보완하여 안전한 전산 환경 제공

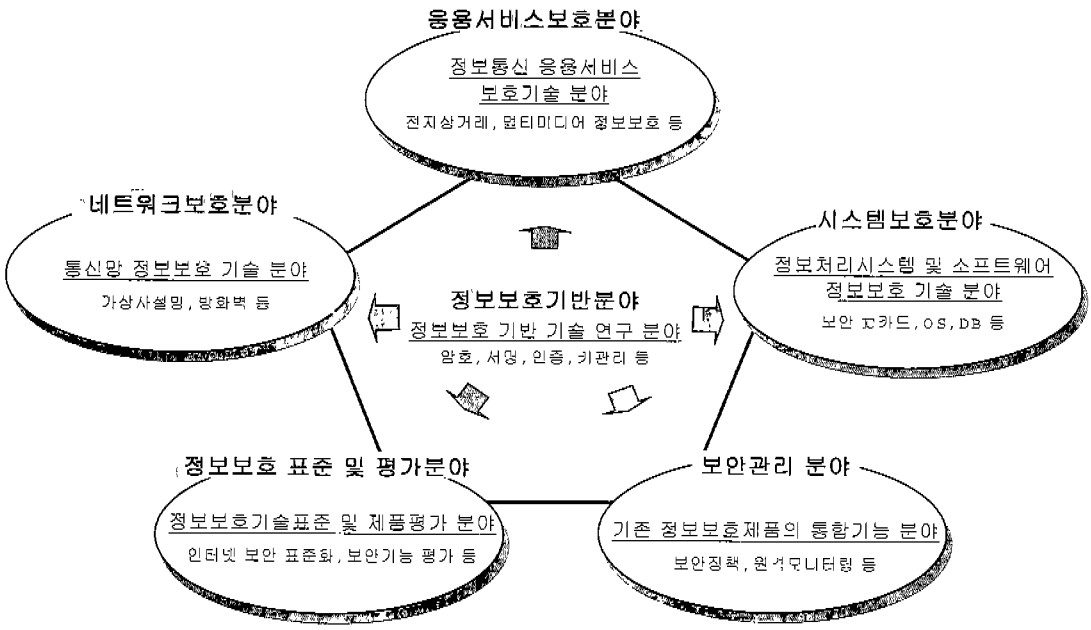

그림 2. 정보보호 기술분야

4. 정보보호 서비스 분류

정보보호 서비스산업이란 전체 시스템의 보안 최적화를 위한 정보보호 제품의 통합 및 효율적인 활용방안을 수립하는 활동을 의미한다. 정보보호 제품의 경우 패키지 형태의 단순구매가 아닌 시스템차원의 보안 컨설팅과 고객과 업체간의 기술적 협력이 필요한 경우가 대부분이다.

5. 정보보호 기술의 특징

정보보호기술의 특징을 살펴보면 다음과 같다.

(1) 국가안보상의 특수성

국가 주요 정보기반구조 보호와 안전을 위하여 필수적으로 육성이 요구되는 전략 산업이며, 타 산업과는 달리 단순한 시장경쟁의 원리에 의한 기술개발을 기대하기 힘들며 국가가 직접 산업육성 및 기술개발을 추진해야 한다.

(2) 독자성

국내의 기간망을 포함한 정보통신망의 보안환경을 외국제품으로 구축하기에는 많은 부작용과 어려움이 발생하며, 국제사회의 글로벌화에 따른 국내 정보유출 우려가 있으므로 독자적인 기술개발이 절실히 요구된다.

표 2. 정보보호 서비스 분류 및 기능

정보보호 서비스	기능
전문서비스 (professional service)	- 초기 보안 시스템 디자인, 선정 및 구축 - 최적 보안 프로세스 리엔지니어링 - 사용자 및 관리자 교육
시스템 통합 (system integration)	- 새로운 보안제품과 기존 시스템과의 통합 - 새로운 보안정보제공
보안관리 서비스 (security administration)	- 위험 및 취약성 분석 - 보안시스템 평가, 점검 및 감리
인증 서비스 (CA service)	- 인증사업자(CA)의 인증서비스 - 정보보안검색 공증서비스, 기타 인증서비스

(3) 사회성

사이버 공간에서의 활동 증가에 따른 개인 프라이버시의 보장과 정보 범죄의 차단 등 안전 신뢰성을 확보하고, 독자적으로 침해사고 대응 환경을 구축하고, 필요에 따른 상호협력 관계 유지가 요구된다.

(4) 고 부가가치성

전자상거래, 차세대 인터넷 등 새로운 정보환경 내에서 정보활동의 신뢰성 및 실효성을 확보하고 미래 정보통신 산업의 지속성장을 보장하기 위한 핵심 산업으로 고 부가가치를 부여할 수 있는 산업이다.

(5) 고속 성장산업

정보통신의 발전과 정보의 자산적 가치가 크게 증대됨에 따라 정보보호에 대한 관심과 수요가 지속적으로 증가되는 추세이다.

(6) 정보화와 동반 발전하는 산업

정보화의 진전에 따라 정보통신시스템의 안전, 신뢰성을 보장할 필요성이 증대되어 정보보호산업은 정보통신산업과 동반 성장할 것으로 예상되며 정보보호가 필수적인 전자상거래, 전자 화폐 등 새로운 서비스의 출현이 정보보호산업 발전을 촉진한다.

(7) 첨단기술산업

암호알고리즘기술, 인증기술, 고집적 칩 개발기술, 고속연산기술 등 첨단기술에 대한 의존도가 높은 산업이며, 암호기술 등 핵심분야 첨단기술 및 컴퓨터, 통신, 반도체 등의 분야에서 원천기술을 보유한 미국 등 선진국이 시장을 주도하고 있다.

(8) 수출입규제 등 국가정책에 의한 영향이 큰 산업

선진국은 정보보호 핵심분야인 암호기술 및 제품의 수출을 규제하고 있다.

(9) 패키지의 단순구매형태보다는 컨설팅 등 복합적 형태의 제품이 많음

항바이러스, 방화벽 등이 주로 패키지 형태의 사

표 3. 분야별 핵심 정보보호기술

기술분야	핵심기술	기술내용	대상사업 (제품 및 서비스)	시장출현 예상시점
정보보호 기반기술	암호설계 기술	- 차세대 핵심 암호 알고리즘 설계기술	- 정보보호 원천기술 개발	2001년
	인증기술	- 출입 접근제어 - 인증기관 개발 - 상호인증 - 생체특성 활용기술	- 정보보호 원천기술 개발	2001년
	키관리 기술	- 공개키기반 기술 - 디렉토리 서버 개발 기술 - 안전한 API 개발 기술 - 멀티캐스팅 키관리	- 공개키기반	2002년
네트워크 보호	방화벽기술	- 다른 네트워크로의 불법침입 저지	- 방화벽	2000년
	가상사설망	- IP망에서 안전한 커넥션을 구축	- 가상사설망	2000년
	차세대 인터넷보안	- IP security(IPsec) - IPv6	- 차세대인터넷 정보보호	2002년
시스템 보호	보안 IC카드	- 안전성 강화를 위한 IC카드 구조 설정 및 설계 - 비대칭형 암호 방식 적용	- 차세대 IC카드	2002년
	보안 OS	- 컴퓨터 운영체제에 대한 각종 해킹으로 부터 시스템을 보호	- 보안 OS 개발	2003년
	보안 DBMS	- DB질의어의 접근 통제 - 부적당한 질의어에 대한 정보의 흐름방지	- 보안 DBMS 개발	2001년
응용 서비스 보호	전자상거래 정보보호	- 전자문서 공증 - 안전한 전자 입찰 - 전자화폐 보안 - 전자상거래공용 플랫폼 보안	- 전자문서 공증시스템 - 전자상거래 보안서비스	2001년
정보보호 표준 및 평가	표준화	- 인터넷 보안 표준화 - 공개키 기반 구조 표준화 - 암호 메카니즘 표준화	- 정보보호 표준화 기술개발	1999년
	평가기준	- 정보보호시스템 평가 방법	- 국제공통 평가기준 상호인증 기반 구축	2000년
	평가기술	- 보안기능 평가 기술 - 보증성 평가 기술	- 정보보호 제품 평가기술 개발	2001년
보안관리 기술	보안형상 관리기술	- 네트워크내 보안요소의 형상관리 - 안전 네트워크 형상 관리	- 보안관리시스템 개발	2002년
	원격모니터링 기술	- 운용시스템에 대한 원격 보안관리 - 보안 정보수집 및 침해탐지	- 감사경보체계구축	2002년
	보안정책 기술	- 보안정책 설정 - 보안 정책 유포 및 강제 집행	- 보안정책서버개발	2001년

업이지만 국내에서는 시스템 구매, 설치시 컨설팅과 동시에 제공하고 있으며, 정보보호 제품은 단독 제품이 아닌 시스템 기반의 전문적인 컨설팅과 고객과 업체간의 기술적 협력이 필수적이다.

(10) 다른 제품이나 기술의 기반적 요소가 강함

인터넷 등 네트워크의 개방화에 따른 대부분의 시스템 및 소프트웨어에 정보보호기술이 필수적인 핵심요소이다.

(11) 기술 및 제품의 병합을 위한 산업체간 급속한 M&A가 빈번함

정보보호시장은 인터넷의 시장과 더불어 동적인 시장 특성을 가지며 정보통신기술에 접목되므로 활발한 기술제휴와 회사간 합병이 빈번하다.

6. 정보보호 기술의 발전 전망

표 4. 정보보호기술 발전전망

기술 분야		발전 전망
정보보호 기반	암호	- 정보를 암호화하는데 필요한 새로운 암호논리 설계 기술 개발/보급 - 민간분야의 수요를 위하여 고속 대칭키 암호 알고리즘 개발 증대 - 새로운 공개키 paradigm 개발로 인하여 새로운 공개키 암호 알고리즘 개발 보급 - 암호알고리즘과 범용인터페이스를 동시에 개발 보급
	인증	- 다양한 기능을 가진 다수의 정보시스템이 통신망에 연결 운영됨에 따라 복합적인 보호 기능의 접근통제 시스템 등장 - 복합적인 기능을 제공하는 형태로 발전 - IC카드 및 생체인식 기술 개발 가속화
	키 관리	- 다양한 사용자에게 키 분배기능을 가진 멀티캐스팅 키 관리 시스템 개발 보급 - 다양한 연산기능을 가진 스마트 카드를 이용한 키 저장 및 분배 제공 - 키 복구 기능 시스템 개발을 적극 추진 중
네트워크 보호	가상 사설망	- 보안성 및 상호운용성 개선의 방향으로 진행되고 있으며, 인터넷 기반의 extranet VPN의 구현이 당면 목표
	방화벽	- 침입차단 시스템을 비롯해 암호화 알고리즘, 일회용 로그인, 인증 관련 제품 등으로 다양화 되고 있는 추세
	IPSec	- 단기적으로는 소규모 사용자들간의 VPN 서비스가 주종을 이룰 것이나 장기적으로는 2005년경 IPv6로의 전환에 따라 IPsec에 대한 수요가 급증할 것으로 예상됨
시스템 보호분야	보안 IC카드	- 공개 플랫폼 기반 IC 카드로 발전 - 키관리가 내장된 보안 IC 카드로 발전

Ⅲ. 맺음말

정보보호와 관련한 유망기술은 암호기술, 인증 기술, 키관리 기술, 가상 사설망, 차세대 인터넷 보안 기술, 보안 IC카드, 보안관리기술 등이며 암호설계에 관한 연구는 창조성이 풍부한 출연연구기관과 대학 인력을 활용하는 것이 필요하다. 상호 인증의 경우 여러 공인 및 민간 인증기관의 이해 상충으로 국가정책과 일관성 있게 진행되기 어려움이 있다. 키관리를 위한 공개키 기반기술은 국가적 공개키 연동을 고려해야 하기 때문에 외국의 경우 국가 차원의 기술 개발과 표준이 정해지고 민간이 이에 따르는 방식으로 진행된다. 보안 관리는 역기능 및 정보전에 대한 대처기반을 구축하기 위한 기술이며 국가 보안과도 밀접한 관련성을 갖고 있어 독자적인 개발이 매우 중요하다.

정보보호기술의 우선 위에 따라 공통 핵심기술인 유망기술을 중심으로 시스템을 개발하되 정부, 출연연구기관, 학계가 주축이 되며 상업적 성격이 큰 분야에 대해서는 산업체와 공동으로 참여하는 것이 매우 중요하다.

※ 참고문헌

[1] ESPRIT (1996) Electronic Commerce - Introduction (http://www.cordis.lu/esprit/src/ecomint.htm).

[2] 정보보호산업 육성을 위한 기술개발 추진 전략(안), 한국전자통신연구원 기술경제연구부, 1999.8.30.

[3] 국내 정보보호산업 동향, 정보보호 21C, 1999.

[4] 정보보호산업발전대책(1998-2002), 정보통신부, 1977.

[5] 정보보호기술개발 중장기 계획(안), 한국전자통신연구원 정보보호기술연구본부, 1999.

[6] Warwick Ford, Computer Communication Security, Prentice Hall, 1944.

[7] Checkpoint Software Technology Ltd, Virtual Private Network Security Components, March 23, 1996.

[8] David Naccache, David MRaihi, "Cryptographic Smart Cards", IEEE Micro, pp.14 - 24, June 1996.

조 현 숙

1979년 전남대학교 수학교육과(학사)
1991년 충북대학교 대학원 전산학과(석사)
1999년 충북대학교 대학원 전산학과(박사과정수료)
1992년 충북대학교 전산학과 시간강사
1982년 ~ 현재 한국전자통신연구원 책임연구원 정보보호기술연구본부장