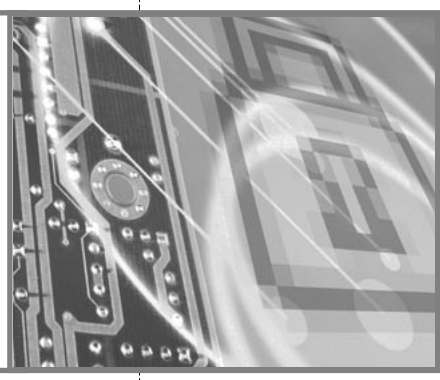
정보보호

염흥열 / TTA 공통기반기술위원회 부의장
순천향대학교 정보보호학과



요약

정보보호 기술은 IT 서비스 및 신성장 동력 산업의 인프라에 해당하는 기술이다. 정보보호 기술을 이용해야 각종 디바이스를 이용한 IT 서비스를 안전하고 편안하게 제공할 수 있어서 궁극적으로 안정되고 지속적인 IT 산업 발전을 도모할 수 있다. 본 고에서는 정보보호 보호 핵심 기술분야의 국내외 기술개발 및 표준화 동향을 살펴보며, 이를 통하여 향후 국내 표준화 추진 전략을 제시하는데 있다.

1. 서론

정보보호기술은 정보통신 시스템에서 저장 및 유통되는 정보의 기밀성과 무결성 그리고 가용성을 보장하여 궁극적으로 정보통신 시스템의 안전성과 신뢰성을 향상시키기 위한 기반 핵심기술이다.

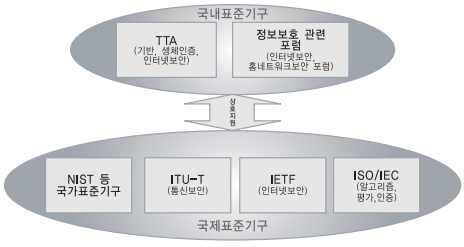


그림 1. 정보보호 분야 국내외 표준화 기구

그림 2. 정보보호 기술

표 1. 국내 제품 경쟁력 분석표

기술 분야	제품분야	경쟁력 격차 (년수)	상대수준 (%)
공통기반 기술	암호제품	3.5	75
	PKI	1.5	85
	생체인식	2.5	80
	IC 카드	2.5	80
시스템 및 네트워크 보호	Firewall/ VPN	1	90
	IDS/IPS	2.5	80
	ESM	2	82
	Security Appliance	3	78
	서버보안	3	72
	바이러스 백신	1.5	85
응용서비스 보호	e-mail 보안	1.5	85
	전자문서 보안	1.5	85
	DRM	1	70
	CAS	2	80

표 2. 국내 정보보호 기술 경쟁력 분석

대분류	중분류	기술격차 (년수)	상대수준 (%)
공통기반 기술	암호기술	3.5	70
	인증기술	2	70
	개인정보보호	2	80
	해킹 · 바이러스 방지 기술	1	85
네트워크 보안기술	BcN/IPv6 보호기술	3	75
	USN 보호	2.5	80
시스템 보호기술	시스템보호기술	1	85
	유해정보차단 기술	2	75
	접근제어기술	2	80
응용보안 기술	전자거래 및 응용서비스 보호 기술	2	80
	IT 서비스 보호기술	2	80
	콘텐츠 보호관리 기술	1	85
	T-Commerce 보안 기술	3	70

정보보호 관련 국제표준화 기구는 정보보호 알고리즘, 보안제품 평가, 관리체계 인증, 생체인식, IC 카드 보안을 중심으로 수행하는 ISO/IEC, 인터넷 관련 사실표준을 주도하는 IETF(Internet Enginering Task Force), 통신보안 구조, 통신 정보보호 관리, 텔리 바이오메트릭, 모바일 보안, 홈네트워크 보안, 스팸메일 보안, 사이버 보안 등에 대한 국제 보안표준을 주도하는 ITU-T SG17, 그리고 미국의 NIST 등의 국가 표준화기구 등이 있다. 국내의 경우 정보통신 단체표준을 주도하는 TTA, 표준 개발 원천기관인 한국정보보호진흥원과 한국전자통신연구원 등의 정보보호 연구기관, 그리고 각종 정보보호 사실표준을 개발하고 있는 인터넷 보안기술 포럼 등이 있다(그림 1)[4-10]. 본 고에서는 정보보호기술의 세부 기술체계를 분류하고, 세부 기술체계에 따른 국내외 기술 및 표준화 동향을 살펴보며, 이를 근거로 향후 국내 표준화 추진전략을 제시한다.

2. 본론

2.1 정보보호 기술 분류

표 3. 정보보호 기술 분류

대분류	요소기술	설 명
공통기반 기술	암호기술	암호기술은 기밀성, 무결성, 메시지 인증, 사용자 인증, 부인방지 등의 서비스를 제공하기 위한 기본 프리미티브이다. 암호 알고리즘은 대칭형 암호 알고리즘, 공개키 암호 알고리즘, 키분배 알고리즘, 해쉬 알고리즘, 전자서명 알고리즘, MAC(Message Authetication Code) 알고리즘으로 분류될 수 있다.
	인증기술	인증기술은 크게 공개키 기반구조(PKI, Public Key Infrastructure) 기술과 권한관리 기반구조(PMI, Previledge Management Infrastructure) 기술, identity 관리, 무선망을 위한 공개키 기반구조, 생체인식 등으로 분류될 수 있다. PKI 기술은 공개키 인증서를 이용하여 사용자 공개키의 무결성과 인증성을 제공하는 기술이며, PMI 기술은 속성 인증서 등을 이용하여 사용자에 대한 권한을 관리하기 위한 기술이고, Identity 관리는 조직과 회사가 연합하여 생성된 표준과 공통의 플래폼을 이용하여 싱글사이언 기능을 효율적으로 제공하기 위한 기술이며, 생체 인식은 지문 등의 인간의 생체 특성을 이용하여 사용자의 신원을 확인하는 기술이다.
시스템 및 네트워크 보호기술	시스템 보호 기술	시스템 보호기술은 각종 불법 행위로부터 조직 혹은 개인의 컴퓨터의 정보를 안전하게 보호하는 기술이며, PC 보안기술과 서버 보안기술 등으로 구성된다. PC 보안은 바이러스 백신 기술 등을 포함하며, 서버 보안기술은 사용자에 대한 접근 제어기술 등을 포함한다.
	네트워크 보호기술	네트워크 보호기술은 해킹이나 바이러스로부터 네트워크를 보호하기 위한 침입차단 기술과 침입탐지 기술로 구성되는 침해대응 기술, VPN(Virtual Privacy Network)을 위한 IP 보안기술(IPSec), 다수의 사용자에게 멀티미디어 정보를 전달하기 위한 멀티캐스트 보안, 종단간 보안기능을 제공하기 위한 전송계층 보안(TLS 보안), 네트워크 보안 장치간의 관리를 자동화하기 위한 통합 보안관리, DDOS(Distributed Dinial of Service) 공격 등으로 부터 네트워크 요소를 보호하기 위한 차세대 네트워크 보안, 그리고 USN(Ubiquitous Sensor Network), WPAN(Wireless Personal Area Network), 4G 망 등으로 구성되는 IT839 네트워크 기반기술 등으로 구성된다.
응용서비스 보호기술	공공부문	공공부문 응용서비스 보호는 전자정부 관련 보안과 전자투표 및 전자공증 서비스를 포함하고 있다.
	일반부문	일반부문 응용 서비스 보호 기술은 전자우편 보안, 디지털 콘텐츠 보안 등을 포함하고 있다.
정보보호 평가 · 관리 기술	정보보호 평가	정보보호평가 기술은 정보보호 시스템의 보안성 평가 및 개발환경 보증을 평가하기 위한 기준 및 체계를 의미하며 구체적으로는 시험방법론, 세부 보안프로토콜 시험기준 등을 포함한다.
	정보보호 관리체계	정보보호 관리기술은 조직의 목적 및 전략을 지원하기 위해 정보보호를 조직화/제도화할 필요가 있으며 이를 위한 정보보호 관리체계를 계획, 구현, 운영지원, 감시 및 검토하는 프로세스에 관한 표준, 지침 및 기법 등을 포함한다.

정보보호 기술은 표 3과 같이 공통 기반기술, 시스템 및 네트워크 보호기술, 응용서비스 보호기술, 그리고 정보보호 평가 · 관리 기술의 4개 기술 분야로 나눌 수 있다. 표 3은 정보보호 분야의 핵심 요소기술 분야를 나타내고 있다[1-3].

2.2 국내외 정보보호 기술수준 비교

국내 정보보호 제품과 선진국과의 격차(표 1)는 평균 2.5년의 제품경쟁력 격차와 81%의 상대수준 격차가 존재하고 있다. 국내 정보보호 기술과 선진국과의 격차(표 2)는 평균 2.5년의 기술격차, 75%의 상대수준 격차가 존재한다. 이 기술격차 및 상대수준은 국내전문가 136명을 대상으로 한 설문조사(2003년 11월 19일 ~ 28일) 결과를 바탕으로, 평가기준 항목 가운데 중요성이 보통 이상으로 응답한 항목을 대상으로 통계분석한 결과이다.[3]

2.3 표준화 대상 기술현황

가. 암호기술

시장 현황 및 전망	국내	– SEED, DES, 3DES, AES 등 정보보호 제품에 탑재된 정보보호 제품이 출시 중 – ECDSA 등이 무선 PKI 적용을 위한 상용 제품으로 사용되고 있음 – 국내 공인 인증서비스 확대와 더불어 전자서명 알고리즘을 중심으로 사용이 급속히 증가할 것으로 예측됨 – IDC Korea에 따르면 공인 인증, 사설 인증, 보안을 대상으로 한 국내 PKI 솔루션 시장은 2005년 1,000억원이 넘을 것으로 예상됨
	국외	– 인증기술, 시스템, 네트워크 정보보호 기술, 응용 정보보호 기술은 모두 기반기술인 암호기술에 의존하고 있음 – 정보보호 시장의 제품이 점차 토털 솔루션의 형태로 발전하고 있으나, 암호 제품에 대한 독자적인 시장이 형성되고 있음 – 독자적인 암호 모듈 제품이 여러나라에서 평가되고 있고, 상용화되고 있으며, 독자적인 시장을 형성하고 있음
개발 현황 및 전망	국내	– KISA가 2001년 암호 키 관리 시범 시스템을 구축함 – 대칭키 암호 분야는 민간 표준으로 사용하기 위한 블록 암호 SEED를 개발하였고, 2004년 ARIA 알고리즘이 개발되었음 – 공개키 암호 연산 고속화 분야에서는 지수승 알고리즘, 유한체 연산 기법, 타원곡선 연산 속도 개선 알고리즘을 발표함 – 패스워드 인증 및 키공유, 특수 전자서명 알고리즘 등의 분야, DES 등의 암호해독 분야에서 주목할 만한 연구 실적이 있으나, 공개키 암호 알고리즘 설계 분야에서 연구 실적이 미미함 – SEED, ARIA 등 대칭형 암호 알고리즘을 개발했으나, 공개키 암호를 위한 암호해독 및 암호 알고리즘 설계 분야가 다소 뒤떨어짐 – USN을 위한 암호 알고리즘이 2005년도에 개발될 예정임
	국외	– 대칭키 암호 알고리즘은 1970년대 중반 미 연방 표준 암호 알고리즘으로 DES가 채택된 이후로 IDEA, MISTY 등을 비롯한 다양한 블록 암호가 개발되었음 – 현재 대칭키 암호 분야의 연구는 AES의 실용화에 대비한 다양한 안전성 분석, 운영 모드, MAC 등을 비롯한 블록 암호 응용기술 분야에서 연구가 진행됨

	– RSA, ECC, Rabin, ElGamal, XTR, NTRU 등 다양한 공개키 암호가 개발되었으나, 현재는 RSA와 ECC 만이 실용적으로 널리 이용되고 있음 – AES, 가변 길이 해쉬 알고리즘이 개발되는 등 핵심 암호 알고리즘 설계 및 암호 분석 분야에 대한 연구가 활발히 추진되고 있음 – Crypto2004에서 MD5와 SHA1에 대한 암호 해독 가능성을 제시함으로써, 이 분야에 대한 해독과 이를 회피할 수 있는 새로운 해쉬 알고리즘의 개발이 활발히 수행될 예정임 – 미국의 경우 독자적인 암호모듈의 평가를 시행하고 있음
국내외 표준화 동향	– 암호 알고리즘은 ISO/IEC SC27 WP2, IEEE, IETF PKIX WG에서 주로 표준화되고 있음 – 현재 일본은 CryptoRec 사업을 통하여 전자정부에 필요한 암호 알고리즘을 표준화 하였고, 유럽의 경우도 NISSIE 사업을 통하여 암호 알고리즘 표준화 사업을 수행하고 있는바, 각 나라는 개별적으로 암호 알고리즘에 대한 표준을 재정할 것으로 예측됨 – 우리나라의 경우도 암호 모듈 평가에 대비한 안전성이 검증된 암호 알고리즘을 선정하고, 이를 탑재한 암호 모듈의 평가를 2005년부터 시행할 예정이어서 암호 제품시장에 큰 영향을 줄 것으로 판단됨 – 국외 표준화 단체의 경우, 여러 알고리즘을 시스템 특성에 따라서 선택적으로 협상을 통하여 사용할 수 있도록 하는 암호 알고리즘 스위트의 국제 표준화를 진행 중에 있음, 이의 대표적인 경우가 IPSec, TLS, 전자보안을 위한 SMIME 암호 스위트, 그리고 PKIX에서의 표준 암호 스위트를 들 수 있음 – 우리나라가 제안한 SEED가 ISO/IEC JTC1에서 공식 위원회 표준으로 200년도 4월에 확정되었음 – 키 분배 프로토콜은 ISO/IEC JTC1 에서 대칭키 기반과 공개키 기반의 다양한 프로토콜을 국제 표준으로 규정한 이후 많은 연구가 이루어지고 있음 – IETF의 경우 ECC 알고리즘을 포함한 다양한 암호 알고리즘에 대한 확인자 등의 표준을 개발하고 있고, 관련 보안 프로토콜의 기반 알고리즘으로 활용하고 있음 – ITU-T의 경우, 접근제어 프레임워크, 부인방지 프레임워크, 키관리 프레임워크 등의 다양한 프레임워크를 개발 완료하였음

나. 인증기술

시장 현황 및 전망	국내	– CA, RA, OCSP, SCVP 서버가 개발되고 있음 – 무선 PKI 시스템을 위한 제품이 상용화되고 있음 – 2004년도부터 개인용 상호연동용 인증서가 유료화 됨에 따라 인증시장의 규모가 증가할 것으로 기대됨 – 2033년도부터 전자입찰 업무의 활성화에 기인한 기업용 인증서의 활용이 점차로 증대하고 있음 – 2004년도부터 신분 관리 시스템이 시장 도입기에 들어갈 것으로 예측됨 – 주민등록 대체 수단에 익명 인증서의 활용이 예상되고 있음
	국외	– PKI 제품이 주로 지금까지 상용화되어 서비스되고 있으나, 앞으로는 PMI 관련 제품의 개발이 이루어질 것으로 예측되며, 홈네트워크 등에서 각종 디바이스 인증 제품에 대한 수요가 증가할 것으로 예측됨 – 2004년, PKI 시장은 1억 달러, ID 관리 시장은 19억 달러가 될 것으로 예측되고 있음
	국내	– 국내에서도 ETRI, 관련 산업체(케이사인, 드림시큐리티, 비시큐어 등)에서 많은 유형의 PKI 제품을 개발하고 있음 – Identity 관리 분야의 경우, ETRI에 의하여 2004년부터 시작되어 2005년부터 관련 제품과 표준이 개발될 예정임 – 많은 PKI 관련 산업체에서 IETF PKIX에서 표준화되고 있는 프로토콜을 이용한 제품을 개발하고 있고, 대부분 IETF 표준에 호환성이 있는 제품을 개발하고 있음

개발 현황 및 전망		– 이 분야의 기술수준은 국내도 상당한 수준이라고 평가되며, 특히 무선 공개키 기반구조 분야의 경우, 세계 선진 수준과 견줄만 하다고 판단됨
	국외	– 미국의 경우 150개 이상의 조직이 결합한 Liberty alliance라는 프로젝트를 통하여 연합된 네트워크 구조를 이용한 싱글사인에 대한 표준과 공통의 플래폼을 개발하고 있음. – 대용량 생체인식 기술과 결합된 공개키 기반구조 제품이 개발되고 있음 – 속성 인증서와 인가 인증서에 기반을 둔 PMI 기술에 대한 제품이 현재 개발되고 있음 – 미국의 리버티얼라이언스는 identity 연합을 위한 표준과 공통의 플랫품 기술을 개발하고 있음 – 키복구 기술의 경우 키전달, 키위탁, 키복구 등 다양한 방식이 개발되어, 관련 기술의 상용화가 진행 중에 있음
국내외 표준화 동향		– 국내 인증기술의 표준화는 주로 IETF에서 개발된 사실 표준을 근거로 TTA에 의한 정보통신단체 표준이 개발되고 있음 – IETF의 경우, 기존의 하나의 작업반인(PKIX) 외에 4개의 새로운 작업반(IPSec을 위한 PKI, 안전한 크리덴셜 저장 및 전달 프로토콜, 초기 등록 등)이 만들어져 관련 표준을 개발하고 있음 – OMA의 경우 무선 인증서 관련 프로파일을 개발하고 있음 – OASIS는 PKI 활성화 방안을 마련하고 전자서명 및 공개키 기반구조 관련 표준을 개발하고 있음 – IETF에서 인터넷을 위한 공개키기반구조에 대한 표준을 PKIX 작업반에서, IPSec을 위한 PKI에 대한 표준은 PKI4IPSEC 작업반에서 수행하고 있음 – 공개키 기반구조에 대한 표준은 ITU-T SG17에서도 디렉토리 연구과제에서 표준 유지보수 작업을 수행되고 있음 – 공개키 기반구조에 대한 표준화는 거의 성숙상태에 있으나, IETF PKIX 작업반, ITU-T 디렉토리 연구반, 그리고 OMA에서 무선 공개키 기반구조에 대한 표준화가 지속적으로 추진될 것으로 예측됨

다. 시스템 보호기술

시장 현황 및 전망	국내	– 서버 보안 시장의 경우 인터넷 사용의 확산과 더불어 2003년도에 327억 시장을 형성할 것으로 예측됨 – 2004년도 서버 보안 제품에 대한 평가 인증제도의 적용으로 인한 공공시장의 규모가 증대될 것으로 예측되며, 본격적인 해외 시장개척이 시작되고 있음 – 2005년도에는 금융권 및 군, 그리고 공공분야에 서버 보안 제품의 도입이 활발히 추진될 것으로 예측됨 – PC 보안시장의 경우, PC 사용자의 보안인식이 강화되면서 정보보호 제품이 탑재된 PC 번들제품이 나오기 시작하였고, 2005년도에 295억 정도의 시장이 형성될 것으로 예측됨 – 금융권을 중심으로 PC보안 제품의 수요가 증대될 것임
	국외	– 앤티 바이러스의 경우 2004년도에 약 20억 달러를 형성할 것으로 예측되며, 연평균 14%의 성장률을 기록할 것으로 예측됨 기술
개발 현황 및 전망	국내	– 국내 시스템 보안 제품은 바이러스 감지, 개인 파일보호, PC 방화벽, 서버 접근제어, 서버 로그제어, 암호화 기술, 보안 OS, 취약성 분석도구, 서버용 방화벽, 통합 보안 솔루션 제품 등이 있음 – 보안 OS의 경우 일부 산업체가 2004년도에 CC 평가를 대비하고 있고, 고등급 보장을 위한 제품들이 개발되고 있음 – PC 보안기술은 바이러스 백신 툴 관리 시스템 개발, 전자증거 수집 교환 형식, 접근 통제를 위한 사용자 인증기술 등이 있음. – 바이러스 이름에 대한 부여 표준이 KISA를 중심으로 개발되었으나, 이의 시행이 요구되고 있음

	국외	– 바이러스 백신 툴의 경우, 시그너처 관련 기술은 이미 성숙기를 넘어섰고, 알려지지 않은 바이러스를 탐지하기 위한 다양한 기술들이 개발되고 있음 – 서버 보안기술은 로그 저장 형식과 접근 제어 모델 기술 등을 개발하고 있음.
국내외 표준화 동향		– 바이러스 명명법, 보안 운영체제를 위한 로그 형식, 로그 형식교환 프로토콜, 그리고 접근제어 모델에 대한 표준이 국내외적으로 사실표준으로 개발될 전망임

라. 네트워크 보호기술

시장 현황 및 전망	국내	– 방화벽 및 VPN 관련 시장이 점차 확대되고 있으며, 웹 서비스 기반의 보안시장 형성 확대 – 방화벽, VPN 등의 네트워크 보안 장치들을 모두 통합한 통합보안제품 개발이 이루어지고 있음 – 네트워크 속도의 향상으로 인하여 고속 동작이 가능한 네트워크 보안 장치에 대한 수요가 급증할 것으로 예측됨 – 홈네트워크 보안 제품이 2004년도부터 개발되기 시작하여 2006년 정도에 시장도입이 시작될 것임 – 휴대 인터넷 보안 제품은 망 자체 보안 제품과 응용 서비스 보안제품으로 상용화 될 것으로 예측됨 – 편재형 네트워크 보안, 휴대 인터넷 보안, BcN(Broadband Convergence Network) 보안, 4G 보안 제품에 대한 시장은 아직 태동기에 있으며, 이들 기반 네트워크가 정상적으로 동작할 것으로 예측되는 2010년도 이후에 본격적인 시장이 열릴 것으로 예측됨.
	국외	– 통합 보안관리 등의 서비스 시장이 형성되고 있으며, 향후 다중 서비스가 급증할 것으로 예상됨 – 멀티캐스트 보안 응용 서비스에 대한 상용화가 진행될 것으로 예상됨 – 새로운 통신환경에 따른 정보보호 기술 및 서비스에 대한 요구사항이 다양하고, 이에 따른 정보보호 표준 개발이 동시에 이루어지고 있음 – 특히 홈네트워크 기술의 경우 인터넷 장비, 이동통신기기, 가전기기 등의 다양한 IT 매체의 통합인 만큼 장비간의 호환과 서비스의 안전성을 보장하기 위한 표준 제정이 활발히 이루어지고 있음 기술
개발 현황 및 전망	국내	– 방화벽, VPN, 고속 네트워크 보안 장치 등에 대한 기술개발과, 새로운 네트워크에 대한 보안 기술들이 개발될 전망임. – 최근 무선 환경에서의 TLS 기능을 제공하는 방식에 대해 상용화가 진행 중 – 현재 ETRI를 중심으로 40Gbps 급의 차세대 네트워크 보안 장치를 개발하고 있음 – IT839 추진과 더불어, 홈네트워크, 이동통신망, 무선 통신망, BcN, 그리고 편재형 네트워크에서 소요되는 보안 기술들이 정의되고 있고, 이에 대한 보안기술들이 핵심 기술과제를 통하여 개발될 예정임 – BcN의 경우, 서비스 및 시스템 보안구조에 대한 연구를 2005년부터 KISA를 중심으로 수행하고 있음 – 홈네트워크 보안제품은 홈네트워크의 핵심 기술로써, 인터넷 정보가전용 미들웨어의 경우 개발 초기 단계로, 가전3사에서는 이를 위한 다양한 표준 기술을 연구하고 있는 실정이고, 한국홈네트워크보안기술포럼, KISA, ETRI가 함께 2003년도부터 보안 프레임워크 개발, 미들웨어 보안 기술 개발, 그리고 인증 및 인가 기술을 개발하고 있고, 여러 국내 업체에서 이에 대한 자체 기초 연구와 실용화 연구를 시작하고 있는 실정임
	국외	– 멀티캐스트 보안의 경우, 시장형성 초기 단계이며, 상용화/제품화 초기 단계에 있음 – 홈네트워크와 무선 근거리통신망(IEEE 802.11i)에 대한 보안제품이 일부 상용화되고 있음 – NGN 보안제품은 NGN 보안 프레임워크 및 세부 기술표준이 완료된 시점에서 개발될 예정임 – 홈네트워크 보안기술은 현재 ITU-T SG17, UPnP, CableLab 등의 표준화 기구를 통한 보안 프레임워크와 인증 및 인가 기술들이 개발되고 있음.

국내외 표준화 동향	– 휴대 인터넷 보안과 무선 근거리통신망 보안은 IEEE 802.11 위원회에서 주로 수행되고 있음 – IETF에서는 네트워크계층 보안 프로토콜, 전송망 보안 프로토콜, IDS를 위한 정보교환 형식 등에 대한 표준을 개발하고 있음 – ITU-T에서 홈네트워크 보안, NGN 보안에 대한 보안표준을 개발할 예정임 – OMA와 ITU-T SG17에서는 무선망을 위한 응용 레벨 보안표준이 개발하고 있음 – 침입대응기술 관련 기술개발의 경우 IETF IDWG에서는 IDS 관련 요소들 간의 정보공유를 위한 IDS 요소 시스템간에 데이터 형식과 교환절차에 대한 프로토콜을 개발하고 있음. IETF INCH에서는 침해 대응 조직 간에 침해 데이터의 교환 및 데이터 형태, 그리고 데이터 언어, 침해 보고와 관련된 샘플 집합을 정의하고 있음. 또한 IETF SYSLOG 작업반에서는 네트워크 이번트와 네트워크 로깅을 위한 사실상의 표준인 BSD 시스로그를 정보 RFC로 표준화하였고, 여러 수준의 보안 메커니즘에 대한 권고안을 개발하고 있음

마. 공공부문 응용보호 기술

시장 현황 및 전망	국내	– 웹서비스 보안기술이 초기 태동기임 – 전자투표의 경우, 비시큐어 등의 회사에서 일부 제품이 상용화되었다고 발표되었으나, 아직 시장 초기단계임
	국외	– 웹서비스 보안은 OASIS 표준에 근거한 많은 보안 제품이 개발되어 표준적합성 시험을 받고 있음 – 전자투표 시장은 초기 상태에 있어서 시장현황 정보는 없는 것으로 판단됨기술
개발 현황 및 전망	국내	– 전자정부법과 전자서명법을 제정하였으며 공인인증기관을 통해 발급된 공인인증서를 이용하여 일부 민원 발급 업무에 대해서는 실용화 추진 중 – 웹서비스 보안(SAML, XACML) 기술이 ETRI를 중심으로 개발되고 있음
	국외	– 웹 서비스 보안표준이 OASIS를 중심으로 개발되어 관련 기술이 웹서비스 제품에 포함되고 있음 – 2000년 3월 미국 Arizona주 민주당 예비선거에서 인터넷 투표를 시행하고, 일본은 터치-패널 스크린 (touch-panel screen) 방식의 전자투표 도입함 – 2003년 영국 : 18개 지자체, 정부에서의 다양한 전자투표
국내외 표준화 동향		– OASIS에서 개발된 웹 서비스 보안 표준이 국내 표준으로 수용될 예정임 – ITU-T SG17에서 통신망 응용서비스를 위한 웹서비스 보안에 대한 표준화를 진행할 예정임 – 대규모 전자투표방식에 대한 기술개발과 표준화가 진행될 것으로 예측됨

바. 일반부문 응용보호 기술

시장현황 및 전망	국내	– 전자메일 시장이 웹 보안기술을 중심으로 개발되고 있음
	국외	– SMIME 보안표준을 준용한 전자메일 제품이 상용화되고 있음
개발 현황 및 전망	국내	– ETRI와 KISA 등에서 암호 및 PKI 기술을 주도하고 있으며, 이를 기초로 하는 전자우편 보안이 상용화되고 있음 – 국내 전자우편 시장의 경우, 독립적인 전자우편 클라이언트 프로그램에서 MIME을 지원할 경우 다양한 MIME 처리 객체를 구현해야 하므로, 많은 노력이 요구됨. 따라서 웹 메일 소프트웨어 개발이 주로 이루어지고 있으나, SMIME 버전 2나 PGP를 이용한 웹 메일 솔루션이 개발되고 있음
		– ETRI와 KISA는 SMIME 버전 2에 기반을 둔 웹 메일 제품에 대한 상호운용성 시험기술을 개발하고 있음. – 디지털 콘텐츠 보안의 경우, 저작권 보호 시스템과 서비스 분야에 많은 경험과 기술을 축적하고 있으며, 여러 DRM 전문업체가 독자적인 기술을 개발하거나 외국 전문 기술을 도입하여 국내 시장을 개척하고 있다.

		최근에는 독자적인 기술을 개발하여 이를 상용화하여 서비스를 제공하고 있음
	국외	– 미국과 유럽을 중심으로 전자우편 보안기술이 개발 및 상용화되고 있음 – 디지털 콘텐츠 보호기술은 Intertrust, ContentGuard 등 선도 기술을 보유한 DRM 전문업체가 기술개발을 주도적으로 수행했으나 최근 MS, Adobe 등의 업체들이 기존의 제품에 DRM 기능을 부여함으로써, DRM 시장을 장악하고 있음. 국외의 경우 DRM 제품 시장과 서비스 시장이 분야되어 발전해 가고 있는 실정임.
국내외 표준화 동향		– 콘텐츠 보안은 MPEG 포럼에서 주로 수행되고 있으며, 2005년도에 초안 개발이 완료되었음 – 전자우편의 경우, IETF SMIME WG에서 국제 표준이 개발되고 있으며, 대부분의 표준이 성숙 단계에 있어, 앞으로는 보완적인 표준의 개발이 추진될 예정임 – 2005년부터 ITU-T에서 스팸메일 보안 대책에 대한 제도적, 기술적 대책 연구가 시작되었음

사. 평가 및 관리체계 인증

시장 현황 및 전망	국내	– 국내 평가 및 관리체계는 정보보호진흥원에 의하여 수행되므로, 평가제품이 다양하지 않고 관리체계에 대한 인식이 아직 부족하여 산업체를 위한 시장의 규모가 크지 않으나, 인식 확산과 더불어 급격한 성장이 예상되고 있음
	국외	– 공인 및 사설 평가기관에 의하여 이루어지므로, 외국 시장이 매우 크다고 볼 수 있음 – 각 나라마다 인정되고 있는 국제공통 평가기준에 의한 시험기관과 영국의 BSI사에 의한 관리체계 인증이 독자적인 정보보호 시장을 형성하고 있음
개발 현황 및 전망	국내	– 기존의 위험분석 표준을 새로운 환경에 적합하도록 개보수 작업이 필요하며 정보보호 구조, 성과측정 등 새로운 지침 및 표준개발이 요구됨 – 평가 도구 개발은 아직 초기 단계를 벗어나지 못하고 있는 실정임 – 정보보호 제품 평가의 경우, 지금까지는 K 시리즈 기준과 CC가 공동 기준으로 평가되어 왔음으나, 향후는 CC로만 평가를 수행할 예정임 – 정보통신부는 2004년도에 정보보호 제품 평가를 방화벽, IDS, VPN에서 지문, 보안 OS, 스마트카드 분야까지 확대하였고, 다시 이를 전체 IT 제품으로 확대할 것이라고 2005년도에 발표함. – 국가정보원은 공통 평가를 위한 국제 기구인 CCRA 가입을 2004년도에 요청했고, 2005년도에 심사 과정을 거칠 예정임
	국외	– 정보보호 관리기술은 ISO/IEC 표준화 기구에서 지침 및 기준 등을 개발하고 있으며 특히 정보보호 컨설팅 업체를 중심으로 위험분석 도구개발을 중심으로 기술개발이 이루어지고 있음 – 정보보호 평가의 경우 미국은 1883년도부터 TCSEC 기반의 평가를 실시하였고, 1998년 상호인정협정 가입후 CC기반으로 정보보호 제품을 평가하고 있으며, 관련 인증기관으로는 NIST와 NSA가 공동으로 운영하는 NIAP가 있으며, 6개의 민간 분야 평가기관도 지정되어 운영되고 있음. 지금까지는 TCSEC과 CC를 동시에 인정하였으나, 최근 CC만을 공식 평가기준으로 인정하고 있음
국내외 표준화 동향		– ISO/IEC SC27에서 개발된 평가(WP3)에 대한 표준은 ISO/IEC 15408이며, 관리체계 인증(WP1)에 대한 표준은 ISO/IEC 17799이다. 평가와 보안관리 체계에 대한 표준이 ITU-T, ISO/IEC JTC1에서 추진되고 있음 – 2005년도에 ISO/IEC에서 평가기준을 위한 ISO/IEC 15408 버전 3 문서가 발표되었음 – 국내에서도 최근 공통평가평가 기준 ISO/IEC 표준이 버전 2.2을 수용하기 위한 절차가 진행되고 있음 – 또한 2005년 6월 관리체계 인증에 대한 ISO/IEC 17799에 대한 표준이 개정되어 이에 대한 국내 표준으로의 반영이 요구됨

2.4 국내외 표준화 추진전략

본 절에서는 지금까지 분석을 토대로 국내외 표준화를 위한 전략을 제시한다.

분 야	국내외 표준화 추진 전략
암호	– USN을 위한 대칭형 암호 알고리즘과 해쉬 알고리즘에 대한 개발을 통하여 자체적인 국내 표준화를 수행하고, 이를 국제 표준화에 반영하는 전략이 필요함 – 암호 기술의 경우 안전성이 입증된 국외 사실 표준을 수용하고, 장기적으로는 고비도/고속 암호 알고리즘과 양자 암호 알고리즘을 개발하여 국내외 표준화를 수행해야 함. – IETF를 통한 국내 대칭형 암호 알고리즘인 SEED의 TLS, SMIME 프로토콜의 암호 스위트로 채택되기 위한 국제 표준화 활동이 지속적으로 요구됨 – 국가정보원이 시행중인 암호모듈 평가를 위한 표준 암호 스위트 선정 및 표준적합성 시험 표준 개발이 요구됨
인증	– 국제 표준화 기구의 범용 표준안 중 산업체에 필요성, 시급성, 중요성, 파급효과 등을 고려하여 대상 표준을 엄선하여 국내 표준화를 추진함. 이를 위하여 IETF에서 RFC 상태에 있는 사실 표준들 중 산업체가 필요로 하는 표준과 OMA에서 표준화되고 있는 무선 PKI 관련 표준 중 무선망을 위한 암호 API 관련 표준을 국내 표준화할 필요가 있음 – 홈네트워크를 위한 디바이스 인증 체계와 프로파일의 국내 표준 개발이 요구되고 있음 – identity 관리를 위하여 리버티 얼라이언스 관련 표준화 동향을 파악하고, 핵심 국제 표준을 국내 표준으로 수용할 필요가 있음 – IETF 표준 중 인증서 확장자 표준, 인증서 관리 및 운영 프로토콜, 인증서 정책 프로토콜, 온라인 인증서 상태 검증 프로토콜, 대리 인증서 검증 프로토콜, SIM 표준, 커버로스 관련 프로토콜 등의 국내 표준화가 요구되며, PKCS 관련 표준 중 타원곡선 관련 표준과 토큰 인터페이스 표준, 그리고 토큰 내의 정보 교환 분야의 국내 표준화가 필요함 – 새로 표준 이슈가 필요하여 구성되고 있는 국제 표준화 기구의 작업반에 초기에 참여하여 미래 활용가치가 높은 인증 분야의 국제표준화 활동의 강화가 필요함. IETF의 경우 IPsec을 위한 PKI, 안전한 크리덴셜 저장 및 전달 프로토콜, SNMP를 위한 인증 확장, 디지털 엔터테인먼트 콘텐츠를 안전하게 관리하기 위한 프로토콜 등이며, ITU-T의 경우 홈네트워크을 위한 인증/인가와 모바일 보안을 위한 인증기술 등을 들 수 있음.
시스템 보안	– 이 분야의 국내 표준은 앤티바이러스 업계 및 인터넷보안 기술포럼 참여 산업체 중심으로 독자 국내 표준 개발이 요구됨. – 바이러스 및 해킹 관련 정보교환을 위한 표준은 IETF 표준을 근거로 포럼을 통한 국내 사실 독자 표준의 개발이 요구됨 – 시스템 보안의 경우, 바이러스 이름 명명 및 호스트 기반 IDS의 데이터 교환 형태 및 API를 표준화해야 함
네트워크 보안	– 기존 IETF 표준 중에서 IP 계층 보안기술, 전송계층 보안기술, 멀티캐스트 보안기술, 이동 IP 보안기술, 침입탐지시스템 연동 보안, 통합 보안관리, AAA 보안 등에서 조속한 국내 표준화가 필요함 – 선도기술개발 과제를 수행하고 있는 홈네트워크 보안, USN 보안 프로토콜, 휴대 인터넷 보안기술, BcN 보안 기술 분야의 경우, 표준과 기술개발이 동시에 수행되도록 하는 정책적 유도가 필요함

네트워크 보안	– ETSI 표준과 MPEG 보안 표준을 근거로 DMB 분야 한정수신 표준과 콘텐츠 보안표준의 국내 독자 표준 개발이 필요함 – IEEE 표준을 기본으로 하여 휴대 인터넷과 공중망 무선랜을 위한 독자 표준 개발이 요구되고 있음. 다시 말해, 무선 인터넷을 위한 보안기술은 무선 근거리통신망 보안기술의 경우 IEEE 802 표준안을 수용하고, 이중 패스워드 기반 인증 및 키교환 프로토콜은 독자 국내 표준 개발이 필요한 분야임 – 현재 IETF의 IDWG에서는 침입탐지시스템, 대응시스템과 관리시스템 간의 정보를 공유하기 위한 데이터 포맷 및 교환 절차에 대한 표준을 개발하고 있으므로, 이를 반영하여 다기종 침입탐지시스템 간의 상호연동을 위한 국내 표준의 개발이 필요함 – 2005년에 IETF 표준으로 채택될 예정인 IPSec을 위한 키분배 프로토콜인 IKEv2 프로토콜에 대한 조속한 국내 표준 수용이 필요함 – 홈네트워크 보안, NGN 보안, 사이버 보안 등의 국제 표준화는 ITU-T SG17, SG13에서 2005년도부터 각각 국제 표준화 작업을 시작했으므로, 이곳을 통한 국제 표준의 개발이 필요함 – USN 보안의 경우, 국제 표준이 초기상태에 있으므로 이에 대한 국내외 표준개발의 동시 추진이 필요한 분야이며, ITU-T를 통한 표준개발이 요구되고 있음
공공부분 응용보안	– 전자투표 분야의 기술개발을 통한 IPR 확보가 가능하며, 이를 통한 국제 표준화 추진이 요구됨 – 웹서비스 보안의 경우 전자정부에 활용하기 위하여 기존 OASIS 표준(SAM, XACML)의 조속한 국내 표준 개발이 요구되고 있음
일반부분 응용보안	– 전자우편 보안기술의 경우, 기존 IETF의 표준 중 필요한 분야를 국내 표준으로 수용할 필요가 있음. 이를 위하여 패스워드 기반 인증, 타원곡선 암호방식의 사용 등의 표준과 인증서 처리 규격과 메시지 명세서, 그리고 각종 암호 알고리즘의 대한 수용에 대한 국내 표준 개방이 필요함 – 스팸메일 보안의 경우, ITU-T SG17을 통한 통제를 위한 제도 및 국내외 동시 표준 개발이 요구됨 – IETF SMIME 전자우편 암호 스위트로의 한국 암호 알고리즘(SEED) 채택을 위한 국제 표준화 활동이 요구되고 있음 – 콘텐츠 보안의 경우, 독자 기술개발을 통한 국내 표준을 추진하거나, MPEG 포럼에서 개발된 표준을 고려한 국내 표준 개발이 필요하며, 국내외 표준 개발을 동시에 수행해야 할 것임
평가 및 관리체계 인증	– 보안성 평가의 경우, ISO/IEC SC27 표준화 동향에 적극 대처함과 동시에, 국제공통 평가기준 관련 보증 방법론 등의 기술을 TTA/TC1을 통해 적극적으로 표준화를 추진해야 함. – 2005년도에 개정된 공통평가 기준 버전 3의 기준 국내 표준으로의 반영이 요구되고 있음 – 정보보호 관리체계 인증의 경우, 2005년 6월 개정된 ISO/IEC 17799 표준적합성과 관련된 시험 방법론 등을 TTA을 통해 국내 표준화 개발의 필요가 있음 – 2003년도에 ITU-T에서 개발된 통신망을 위한 관리체계인증 표준을 분석하여 국내 표준안으로의 반영이 필요함 – 통신망을 위한 관리체계 인증의 경우, ITU-T SG17을 통하여 국내외 표준 동시 개발이 요구되고 있음

3. 결론

정보보호 기술은 정보보호 제품간의 상호연동성과 이를 위한 표준적합성을 위하여 표준 개발과 함께 기술개발이 이루어져야 할 분야이다. 정보보호 기술 표준화는 국제표준화 기구에서 성숙도가 높은 표준 중에서 산업체에서 요구되는 핵심 표준에 대한 국내 표준화가 수행되어야 하고, 새로운 서비스와 신성장 산업 분야의 표준화는 국내외 표준화가 동시에 수행되어야 할 것이며, 국내 정보보호 기술중에서 강점이 있고 시장 규모가 크며, 파급효과가 우수하며, IT 강국의 위상에 걸 맞는 기술에 대한 국제 표준화에 대한 노력이 수행되어야 할 것이다. 국제 표준화 활동을 위한 정보보호 분야 인력양성 대책과 현실성 있는 지원책 마련이 요구되고 있는 시점이다. 본 고에서는 정보보호 기술을 세부 핵심 기술분야로 구분하고, 각 분야의 국내외 기술개발 및 표준 현황을 살펴보고, 이를 근거로 국내외 표준화 전략을 제시하였다. 본 고에서 제시된 결과는 IT839 정보보호 기술의 요소기술이므로, 이를 위한 정보보호기술 표준화 로드맵을 작성하기 위한 기반 문서로 활용 가능하다.

참고문헌

[1] 염흥열, 2004년도 정보보호일반 표준화 로드맵, TTA, 2004.

[2] KISA, 정보보호 표준화 로드맵, 2004.7.

[3] MIC, 정보보호 중장기 기술개발 로드맵, 2004.12.

[4] IETF, http://www.ietf.org/, IETF, PKIX, IPSec, S/MIME, MSEC 등의 작업반 홈페이지, 2003.

[5] OMA, http://www.wapforum.org/, OMA 홈페이지, 2003.

[6] ITU, http://www.itu.int/home/index.html, ITU 홈페이지, 2003.

[7] NIST, http://www.nist.gov/, NIST 홈페이지, 2003

[8] ISO/IEC JTC1, http://www.jtc1.org/, ISO 홈페이지, 2003

[9] TTA, http://www.tta.or.kr, TTA홈페이지, 2003.

[10] MIC, http://www.mic.go.kr/index.jsp, MIC 홈페이지, 2003. TTA