응용보안/평가인증

1. 개요

1.1. 기술개요

1.1.1. 중점기술 및 표준화항목의 정의

• 중점기술의 정의

- 정보보호기술은 정보통신시스템에서 저장 및 유통되는 정보의 기밀성(정보누출 방지)과 무결성(데이터 위·변조 방지)을 보장하며, 정보통신 시스템의 안전성과 가용성을 향상시키는데 필요한 기술을 의미
- 본 문건에서 고려하는 정보보호기술은 응용보안 및 평가인증의 2가지 분야로 구분될 수 있음

응용보안 및 평가인증 분야의 중점 표준화 내용을 분류하면 다음 〈표1〉와 같음

〈표 1〉 응용보호 및 평가인증 표준화 대상항목

분 야	표준화 대상항목	내 용
응용보안	u지식 보안	유비쿼터스 환경에서 복합콘텐츠에 대한 유통보호 기술, 프로슈머에 의해 창작/수정/가공된 콘텐츠 보호
	VoIP 보안	제어정보보호, 트래픽정보보호, 스팸대응
	응용보안 강화 프로토콜	안전한 패스워드 인증 가이드라인
	안전한 P2P 보안	보안 프레임워크, 보안 메커니즘 및 프로토콜
	IPTV 보안	IPTV 인프라 보호, 응용 서비스 보호, 프라이버시 보장
	신뢰 보안 서비스 (STC: Secure Trusted Computing)	Trusted computing 정보보호, 신뢰보안 프레임워크, 메커니즘, 디바이스/플랫폼 보호, 악성코드 탑재 방지용 IMA (Integrity Measurement Agent) 기술, 임베디드 장치 보호
	차세대 웹 보안	웹 2.0 보안, 시맨틱 웹 보안, 시맨틱 웹서비스 보안, 유비쿼터스 웹 보안, 모바일 웹서비스 보안
	Lawful Interception	통신로상의 암호화된 불법정보 분석
평가인증	정보보호 평가	표준 적합성 시험, 보안성 평가, CMVP 평가(암호모듈검증프로그램)
	보안관리	관리체계 및 성과 측정, 보안관리 모델 및 구축 가이드, Security 거버넌스, 위험관리/위험분석, 운영지침개발, 개인정보 위협 분석 및 대응 (전자거래, 이동환경 등)

• 표준화항목의 정의

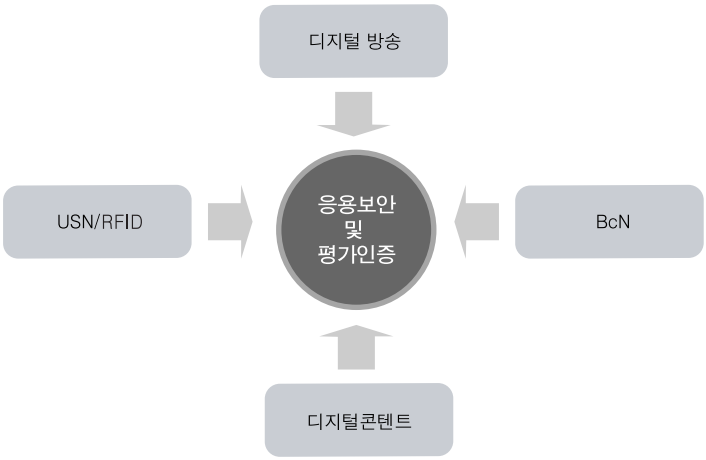
- 금년도 표준화항목은 크게 응용보안과 평가인증 부문으로 구분하였으며, 응용보안 분야의 경우, 전자거래 보안, 전자우편, 전자투표/공증, u지식 보안, 쉘 보안, VoIP 보안, IPTV 보안, 차세대 웹 보안 등이 중점 항목으로 선정되었고, 평가인증 분야의 경우, 정보보호 평가와 보안관리가 중점 항목으로 선정됨

〈표 2〉 응용보호 및 평가인증 표준화항목 정의

구분	정의	대상 표준화항목	표준화 내용
응용보안	응용 레벨을 위한 보호 기능을 제공하기 위한 기술들을 포함함	전자거래 보안	전자구매를 위한 보안 기술 표준화
		전자우편	전자우편을 보호하기 위한 기술, 사용 암호 슈트 등의 표준화 항목 정의 - 도메인키 확인 메일(DKIM), Open PGP, S/MIME 메일보안
		전자투표/공증	전자 투표 및 전자 공증을 위한 보안 기술 표준화
		u지식 보안	유비쿼터스 환경에서 복합콘텐츠에 대한 유통보호 기술 표준화
		쉘 보안	안전한 쉘에 관련 기술 표준화 - 키관리, 보안프로토콜
		VoIP 보안	안전한 VoIP 서비스 제공 기술 표준화 - 제어정보보호, 트래픽보호, 스팸대응
		스팸대책	스팸을 제어하기 위한 대책과 가이드라인 표준화
		응용보안 강화 프로토콜	안전한 응용 보안 프로토콜 표준화
		안전한 P2P 보안	P2P 보안 구조와 관련 프로토콜 표준화 - 보안 프레임워크, 보안 메커니즘
		IPTV 보안	IPTV 인프라 보호, 응용 서비스 보호, 프라이버시 보장 기술 표준화
		신뢰보안서비스 (STC)	신뢰성있는 컴퓨팅 기술 관련 표준화 - 신뢰 · 보안 프레임워크, 신뢰 · 보안 메커니즘, 디바이스 보호/플랫폼 보호, 악성코드 탑재 방지용 무결성 측정 기술, 임베디드 장치 보호 등
		차세대 웹 보안	차세대 웹 보안과 관한 표준화 -웹 2.0 보안, 시맨틱 웹 보안, 시맨틱 웹서비스 보안, 유비쿼터스 웹 보안, 모바일 웹서비스 보안
		Lawful Interception	유무선 통신 매체를 통해 암호화되어 전송되는 음성, 데이터의 합법적 분석기술 표준화 - 시스템(장비), 알고리즘, 프로토콜 등
평가인증	정보보호 시스템에 대한 보안성 평가와 조직에 대한 보안관리, 그리고 암호모듈에 대한 기술을 포함함	정보보호 평가	정보보호시스템의 보안성평가 및 표준적합성 시험을 위한 기준 및 체계의 표준화 - 시험방법론, 세부 보안프로토콜 시험기준 등 - 암호모듈에 대한 구현 적합성 시험 - 표준 적합성 시험, 보안성 평가, CMVP평가(암호모듈검증프로그램)
		보안관리	조직의 목적 및 전략을 지원하기 위해 정보보호를 조직화/제도화 등의 표준화 - 정보보호관리체계 계획, 구현, 운영지원, 감시 및 검토하는 프로세스에 관한 표준화, 지침 및 기법 등 - 정보보호 정책/조직, 위험분석/관리, 정보보호 대책 선정 구현 및 교육/훈련, 사후관리, 관리체계 및 성과측정, 거버넌스 - 위험관리, 위험분석

1.1.2. 연관기술 분석

• 연관기술 관계도



〈그림 1〉 응용보안 및 평가인증 기술 관계도

• 연관기술 분석표

응용보안 및 평가인증 연계기술은 IT839 네트워크 기반기술과 관련하여 (그림 1)과 같이 연관되며, 주요 기반 서비스 및 네트워크는 디지털방송, USN/RFID, 디지털콘텐트, BcN 등임. 이들 연관 기술의 특성은 〈표 3〉과 같음

〈표 3〉 연관기술 분석

연관기술	내 용	표준화기구/단체		표준화수준		기술개발수준	
		국내	국외	국내	국외	국내	국외
디지털방송	디지털방송은 고화질/고음질, 다채널, 양방향서비스, 인터넷접속 등의 특징을 기반으로 하는 차세대 TV 방송을 의미하며, 현재 Internet TV, STB 기반의 IPTV, DMB, Mobile TV, Satellite TV, Cable TV, TV 2.0, Web TV 등의 기술이 혼재되어 있는 상태임. 특히 가장 각광을 받고 있는 것이 상용화가 한창인 IPTV 영역으로써 Download and Play 또는 Real-time Streaming의 두 가지 형태로 서비스되고 있음. IPTV 관련 표준은 ITU-T의 FG을 통해 한국이 주도적으로 표준안 제정을 위해 노력중이며 관련 보안 이슈를 해결하기 위해 CAS를 탑재한 STB를 활용하고 있음. 또한 CAS와 DRM을 통합하고자 하는 시도와 자체 디지털 TV 표준안 제정을 통한 de-factor 선점을 위해 적극적인 표준화 활동이 진행 중임. 커뮤니티 기반의 인터렉티브, 지능형 및 다방향 서비스에 대한 국내 관련 표준 단체 및 기관의 행보는 크게 방송기술영역, 네트워크영역, 디지털방송콘텐트 정보보호 영역으로 나뉘어 이뤄지고 있으나, 대부분 성능개선과 관련한 내용에 치중되어 있고, 디지털 TV 보안부문에 대해서도 종래의 네트워크 보안기술을 중심으로 접근하고 있고, 방송 및 인터넷 그리고 디지털콘텐트 접목에 따라 발생할 수 있는 새로운 보안 취약성에 대해서는 간과하는 측면이 있어 이에 대한 신규 표준안 제정의 노력이 요구됨	TTA, 한국디지털케이블포럼, 차세대디지털방송포럼	ITU-T OpenCable, ATSC, DVB-CA	표준 개발/검토	표준 개발/검토	상용화	상용화

연관기술	내 용	표준화기구/단체		표준화수준		기술개발수준	
		국내	국외	국내	국외	국내	국외
BcN	광대역통합망(BcN)이란 통신을 비롯해 방송 · 인터텟 등 각종 서비스 영역을 통합한 멀티미디어 서비스를 시간과 장소에 구애받지 않고 이용할 수 있는 차세대 통합 네트워크임. 통신 · 방송 · 인터넷의 대통합시대에 대응하고 신성장동력 산업의 발전토대마련을 위해 광대역통합망(BcN) 구축이 필요함. 현재 BcN은 ITU-T SG13에서 금년부터 FG(Focus Group) 구조에 대한 표준화를 진행중임. 아직 보안에 대한 구체적인 표준안은 마련되어 있지 않으나, 지난 7월 제네바 FG 회의에서 집필자의 제안으로 주요 보안 표준화 항목을 채택한바 있어서, 이를 기초로 보안을 위한 표준이 개발될 예정임. 유무선 통합화 및 통신 · 방송 융합화의 네트워크 발전 경향에 부응하는 BcN(Broadband Convergence Network) 정보보호기술의 표준화가 필요함	TTA, BcN 포럼	ITU-T, ETSI	표준 개발/검토	표준 개발/검토	시제품 프로토타입	시제품 프로토타입
USN/RFID	u-센서 네트워크(USN:Ubiquitous Sensor Network))는 모든 사물에 전자태그를 부착, 인터넷에 연결하여 정보를 인식 및 관리하는 네트워크임. u-센서 네트워크(USN)는 사물의 정보화를 위한 네트워크이며, 유비쿼터스 사회구현을 위한 기반구조임. 안전한 u-센서 네트워크 구축을 위한 초경량 정보보호 기술의 표준화가 필요함	TTA, USN 포럼	ISO/IEC JTC1, ITU-T, IEEE	표준 개발/검토	표준 개발/검토	시제품/프로토타입	시제품/프로토타입
디지털콘텐트	현재의 디지털 콘텐트 산업의 수익을 개선하기 위해서는 제공되는 콘텐트의 유료화가 요구되는데, 이것을 지원하기 위해서는 콘텐트에 대한 보안이 필연적으로 뒤따라야 함. 최근 MP3와 같은 디지털 음원에 대한 국내외 분쟁이 본격화되면서 이에 대한 표준화 요구가 더욱 거세지고 있는 실정임 디지털콘텐트의 경우 크게 DRM, Copy Protection, CAS 등으로 대표되는 세 영역으로 나뉘어 MPEG21, OMA 등의 단체에서 표준화가 진행 중임. 최근 콘텐트의 유통이 비단 인터넷뿐만 아니라, P2P, IPTV 등으로 다변화되고 있어 관련 서비스와의 상호운용을 고려한 디지털콘텐트 표준화의 제정이 시급한 실정이나, DRM의 경우 동일콘텐트에 대해 재생기기간에 상호 운용성을 지원하지 않을 뿐만 아니라, 단체별로 상이한 표준을 채택 및 제정하고 있어, 상호 운용성을 보장한 일관된 표준안 제정의 노력이 요구됨	TTA, DRM Forum, MPEGKorea, KODCA, 한국디지털콘텐트미래포럼	IETF, ITU-T, MPEG-21, OMA, CPTWG, 4C Entity - CPPM/CPRM 5CDTCP	표준 개발/검토	표준 최종검토	시제품/프로토타입	상용화

1.2. 추진경과 및 중점 추진방향

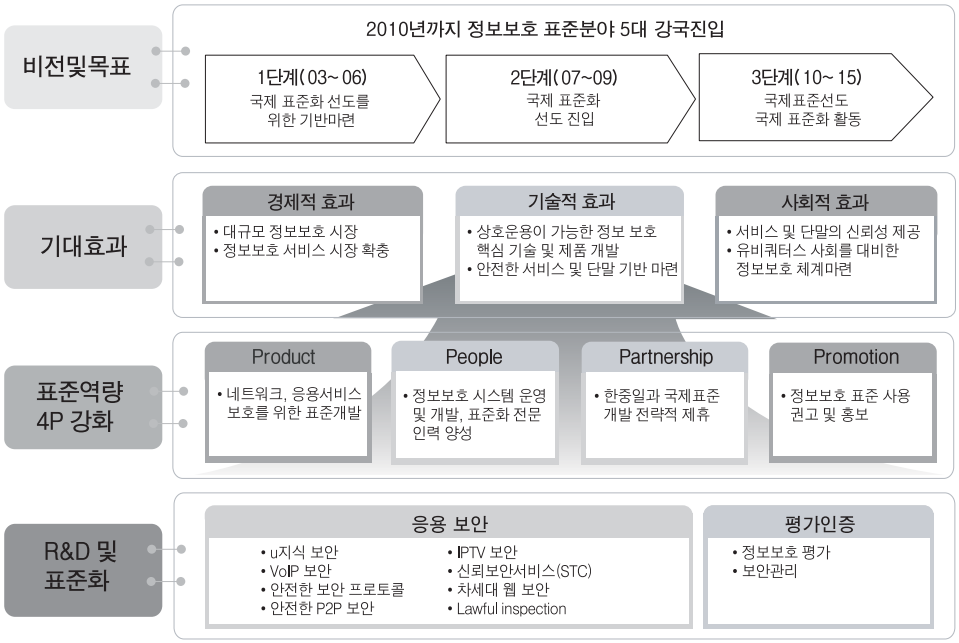
• 추진경과

- 2004년도에는 모든 분야에 대한 표준화 항목을 정리함
- 2005년도에는 TTA를 통하여 수행되지 않고 한국정보보호진흥원을 통하여 수행되었으며, 주로 IT839와 연계된 정보보호 표준 분야를 정리함
- 2006년도에는 정부의 추진 의지가 강한 VoIP 분야를 포함한 응용 서비스 정보보호분야와, 최근 ITU-T와 IETF 등의 국제 표준화 기구에서 활발하게 국제 표준화가 추진 중인 네트워크 정보보호 분야를 중점적으로 정리함
- 2007년도에는 응용보안 분야를 u지식, IPTV, 신뢰보안서비스(STC), 차세대 웹 및 Lawful Interception과 같은 기술이 신규 중점 표준화 기술항목으로 추가하였고, 평가인증 분야에서 정보보호 평가와 보안관리 분야를 중심으로 정리함

• 중점 추진방향

- 중점 표준화 항목은 정부의 정책 추진 의지, 산업체의 요구사항, 국제 표준화 기구의 표준화 동향, 그리고 파급 효과 등을 고려함
- 특히, 응용보안 분야 중 전자거래 보안, 스팸대책, VoIP, IPTV, STC, Web 정보보호 및 Lawful Interception 등에서의 표준안 제정은 보안 산업 및 관련 시장을 통해 실제로 적용되어 상용화될 가능성이 큰 부분임을 감안할 필요성이 있음
- 정보통신부는 미래 기존 전화망을 대체할 가능성이 있는 VoIP 에 대한 정보보호 표준화 로드맵 작업을 2006년 8월부터 12월까지 연구반을 구성하여 추진하고 있음을 고려할 것임
- 응용 보호 기술은 최근 문제가 되고 있고 또 다른 공격을 위한 일차 공격이 되고 있는 스팸 등을 효과적으로 방지할 수 있는 전자메일 보안을 포함하고 있음을 고려함
- 최근 ITU-T는 NGN 보안 요구사항을 2006년 7월에 표준으로 SG13 에서 승인했으며 응용 서비스 보안 등의 표준화가 활발하게 진행되고 있음
- 표준화 추진 방향은 국내 표준 추진 방향과 국제 표준 추진방향으로 구분되며, 국내의 표준 동향과 국제 표준동향을 분석하고, 이를 근거로 국내 표준화 방향을 결정하고, 경쟁력과 효과성이 우수한 국제 표준화 방향을 결정함
- 관련 핵심 기술의 선점 및 독점권 행사를 위해 국내외 등록 및 출원이 진행 중인 특허 현황을 파악하고, 그 추이를 전망하여 응용보안 및 평가인증 표준화 추진에 반영함
- 관련 산업체에서 기 상용화하여 운용중인 시스템 및 장비 현황을 분석하고, 어느 단체 또는 기업의 표준안을 기반으로 하고 있는지를 검토함

1.3. 표준화의 Vision 및 기대효과



〈그림 2〉 표준화 Vision 및 기대효과

1.3.1. 표준화의 필요성

- 최근 정보화의 역기능을 방지하기 위한 정보보호기술의 중요성이 증대됨에 따라 사회 각 분야에서 정보보호에 대한 관심이 매우 고조되고 있고, 따라서 정보보호 제품의 설치가 활발히 진행되고 있음. 그러나 상호 운용성을 제고하기 위한 정보보호 제품에 대한 표준의 부재는 안전한 전자상거래와 전자정부의 구현과 유비쿼터스 사회를 구현하기 위한 커다란 장애가 되고 있음
- 정보보호 분야의 표준화 활동은 크게 국외 표준화 기구에서 채택된 국제 표준을 국내 표준화하는 활동, 국내에서 개발된 고유의 기술을 국제 표준화 기구의 국제 표준으로 상정하는 활동, 국내에서 개발된 기술을 국내 표준화 기관을 통하여 표준화하는 활동 등으로 구분될 수 있음
- 이미 세계 각국은 자신이 개발한 기술을 국제 표준에 반영함으로써, 관련 정보보호 제품에 대한 IPR을 확보하고 관련 제품의 기술경쟁력과 시장지배력을 향상시키고 있는 추세임. 정보보호 분야는 제품의 수명주기가 일반적으로 매우 짧고, 새로운 서비스에 대한 표준 기술의 개발이 요구되고 있음

- 현재까지 정보보호 분야의 표준화는 국제 표준을 국내 실정에 맞게 개정하거나 준용하는 수준에 머물러 있다고 판단됨. 또한, 암호 표준은 주로 알고리즘의 국내 표준화에 초점이 맞추어 수행되었지만, 일부 국내에서 개발된 암호 알고리즘이나 프로토콜의 국제 표준화 노력도 시도되고 있음. 이의 대표적인 사례는 KCDSA 서명 알고리즘과 SEED 알고리즘, AMP 및 C2C-PAKA 키 분배 방식의 ISO/IEC을 통한 표준화 작업과, 고객 식별 방법(SIM : Subscriber Identification Method)의 IETF PKIX 작업반 표준화 작업, 그리고 ITU-T SG17에서의 모바일 보안 표준 등을 들 수 있음
- 그러나, 최근 우리나라는 인터넷 인프라가 세계 정상수준으로 향상되고 있고, 정통부가 의욕적으로 추진하고 있는 IT839에 따른 새로운 서비스나 인프라, 그리고 디바이스에 소요되는 정보보호 기술의 개발이 요구되고 있음. 그런데, 이러한 정보보호 표준은 현재 선진국에서도 개발되지 않음을 고려하면, 이를 위한 정보보호 표준을 개발함으로써 안전한 정보통신 서비스 제공이 가능하며, 관련 정보보호 제품 및 표준의 개발을 통한 기술 경쟁력을 향상할 수 있을 것으로 기대됨
- 정보보호 분야 표준화도 역시 정보기술 분야의 표준화와 마찬가지로 제품간의 상호 연동성 보장이 매우 중요. 이렇게 함으로서, 제품의 시장 규모를 증가시킬 수 있고, 전용 기술의 채택으로 인한 정보보호 제품의 상품화의 위험을 감소시킬 수 있음. 따라서 정보보호 산업의 육성을 위해서도 정보보호 기술의 표준화 작업이 무엇보다도 시급하다고 할 수 있음
- 인터넷 보안 기술 개발 및 표준화 등의 연구와 표준화 작업은 국가의 정책적 지원이 있어야 하며, 국가 및 민간간의 유기적인 협력체제의 구축을 통하여 가능할 것임. 대체적으로 국가적으로 수행되어야 할 정보보호 분야의 표준화는 국가 및 전자정부, 그리고 공공분야에서 요구되는 암호 알고리즘에 대한 개발 및 암호 알고리즘의 표준화 등이 요구되며, 민간과 협력하여 수행되어야 할 표준화는 민간에서 요구되는 상품화가 가능한 다양한 국제 표준의 수용 및 채택을 통한 국내 표준화 작업, 그리고 국내 연구소나 산업체에서 개발된 독자적인 기술을 국제 표준화하는 작업 등으로 구성. 현재까지의 주요 표준화 활동은 국내 알고리즘의 국내 표준화 작업, 국제 표준을 국내 표준으로 채택하는 작업을 주로 수행해 왔으나, 앞으로는 국내 기술의 국제 표준화 작업의 수행도 요구됨. 이를 위해서는 국내 산업체와 국내 연구소의 기술 경쟁력을 향상시키고, 독자적인 정보보호 기술의 개발도 요구되며, 이를 바탕으로 개발된 기술을 국제 표준화하는 방향으로 추진되어야 할 것임
- 특히 응용보안 분야의 경우 이미 거의 모든 인터넷 사용자들이 이용하고 있는 메일, 전자구매 및 전자공증 등의 Web, 멀티미디어 디지털 콘텐츠, 그리고 주요한 콘텐츠 전달의 매체로서 기능할 VoIP, IPTV 등을 그 주요한 영역으로 포함하고 있어, 이의 국제 표준화는 상용 서비스에 직접적으로 적용 및 운용되는 등의 매우 큰 경제적 파급 효과를 기대할 수 있음. 또한 lawful interception의 경우, 정보통신 기술의 사용이 일반화된 현 사회에서 정부의 범죄에 대한 수사권을 확보를 위한 주요한 기능을 수행할 수 있다는 공감대가 국가별로 형성되어 있으며, 이미 유럽표준단체를 중심으로 적극적인 움직임이 포착되고 있는 만큼, 국가차원에서의 기술 규격의 확보가 시급한 실정임
- 평가 및 인증 분야는 응용보안 분야를 비롯한 모든 정보보호 표준안 검토 및 평가의 공통 기준으로 적용될 수 있는 가능성을 내포하고 있음. 즉 특정 인증 수준 이상의 기술 및 제품만이 시장에 진입할 수 있는 권한을 부여받게 되는

등의 보안 기술 등급의 규격화가 요구됨. 더불어 조직의 목적 및 전략을 지원하기 위해서 정보보호관리체계를 계획, 구현, 운영지원, 감시 및 검토하는 프로세스에 고간한 표준 지침 및 기법 등을 포함함

- 향후 정보보호 표준화 정책은 국외 표준화 기구에서 이미 성숙도가 높은 국제 표준을 국내 시장이 필요하면 바로 준용하고, 현재 표준화 논의가 시작되고 있는 분야를 선택하여 국내 기술을 개발하고 관련 IPR을 습득하고, 이를 바탕으로 국제 표준화 작업을 수행하고, 산학연 전문가로 하여금 국제 표준화를 수행하도록 함으로써, 국내 표준화 활동과 국제 표준화 활동을 적극적으로 수행하도록 지원해야 함. 또한 국내 선도기반 기술개발 사업과 국제 표준화 활동이 긴밀하게 연계하여 관련 기술개발과 표준화 활동을 연계하는 정책이 필요함

1.3.2. 표준화의 목표

- 정보통신 및 정보보호 기술은 표준화되어 상호 연동될 수 있는 형태로 발전되어야 함. 통신망 또는 정보시스템에서의 정보보호 표준은 정보보호 프레임워크를 정의하고 관련 프로토콜과 프로토콜 관련 요소들의 구문 등을 정의함으로써, 정보보호 시스템간의 상호 연동을 가능케 하고, 안전하고 신뢰성 있는 통신을 보장하는 핵심 기술
- 정보보호 기술은 금융, 국방, 외교, 기업, 통신 인프라 등의 모든 정보화 부분에 안전성과 신뢰성을 보장하기 위한 필수 기술임. 정보보호 기술을 적용함으로써, 전자정부의 안전성과 신뢰성 확보, 각종 서버들로 구성되는 공공 분야 정보시스템들의 안전적 운용 보장, 정보통신망의 안전한 운영, 개인 PC내의 정보에 대한 보호, 기업 정보보호 등을 달성할 수 있음

- 국내에서는 정부기능을 혁신하기 위한 전자정부 사업을 추진하고 있으며, 이를 바탕으로 민간뿐만 아니라 공공 분야를 망라한 지식을 통합적으로 관리하고 효율적으로 분배하는 지식기반 정보화 사회를 구축하기 위한 노력을 기울이고 있음. 정보화는 가장 필수적인 요소로서 국가 경쟁력 확보와 국가 성장 잠재력 확보를 위하여 반드시 필요. 이러한 정보화는 최근 급속히 확산되고 있는 인터넷과 함께 기존의 정보산업뿐만 아니라 정통 산업의 모든 형태를 변화시키고 있음. 정보통신 시장의 국제적인 개방화와 경쟁화의 추세는 다양한 정보통신 제품들 사이의 상호 연동을 위해 표준의 중요성을 제고하는 계기가 되고 있음
- 상호운용성은 통신기기와 정보통신 시스템 수용을 위한 필수적인 요건이 되어가고 있으며, 표준화는 상호 운용성 확보를 위하여 반드시 필요한 요구사항. 오늘날 정보통신기술의 근간을 이루고 있는 정보보호 기술은 안정적인 정보기술의 활용에 있어 필수적으로 요구되며, 정보보호기술도 다른 정보통신 제품과 마찬가지로 표준화를 통해 상호운용 가능한 형태로 개발되어야 함. 또한 대규모 시장을 형성할 수 있는 동기를 부여함으로써, 국내 정보보호 산업의 국제 경쟁력을 향상할 수 있음
- 구체적인 국제 표준화 및 국내 표준화 목표는 다음과 같음
  - 2008년까지 정보보호 분야의 리드 SG인 SG17을 통하여 응용보안 분야에서 총 6건 이상의 국제 표준화를 완성함을 목표로 함

- 2011년까지 IETF를 통하여 인터넷 분야 정보보호에 대한 국제 표준화를 추진함
- 2011년까지 중요 국제 표준화 기구에서 표준화된 총 60 여건(매년 10여건)의 국제 표준을 우선순위와 국내 필요 표준의 선정을 통하여 국내 표준으로 이전하여 표준화를 추진하고, 또한 국내에서 선도 기반 과제를 통하여 개발된 기술들의 국제표준화를 추진함

• 한편 국가 정보통신 연구개발 사업의 중추로서 IT839를 강력하게 추진하고 있는 국내 실정을 감안하고, 최근 떠오르고 있는 u지식서비스, IPTV, 신뢰 컴퓨팅, P2P, VoIP, 안전한 email 등의 신규 응용 서비스 기술을 고려할 필요성이 있음. 즉 주요한 국가 전략 기조 및 많은 시장성이 예상되는 응용 서비스에 대한 고려가 표준화 활동 및 작업에 반영시키기 위해서는 지금까지 IETF 및 SG17과 같은 일부 표준화 단체에 집중화 된 표준화 노력을 "MPEG-21, OMA, W3C, OASIS" 등의 기관 및 단체로 확대 적용하는 표준화 정책의 다변화가 수반되어야 함

〈표 4〉 연관기술 분석

표준화 기구	현재 국제표준화 추진 중인 권고안 제목	분야	국제 표준화 완료시점
ITU-T	Security Architecture and protocols for peer to peer network	응용 보안	2007
ITU-T	Security architecture and protocols for per to peer network	응용 보안	2008
ITU-T	Guideline on strong password authentication protocols	응용 보안	2008
ITU-T	Guideline on countering e-mail spam	응용 보안	2006
ITU-T	Overview for countering spam for IP multimedia application	응용 보안	2007
ITU-T	Technical means for countering SPAM	응용 보안	2008

1.3.3. Vision 및 기대효과

• 정보보호 기술의 표준화는 기반이 되는 암호 알고리즘 표준화, 이를 이용하는 구현되는 네트워크 및 시스템 정보보호 기술의 표준화, 응용 서비스 기술 표준화, 그리고 평가 및 관리 표준화를 통하여 상호연동이 가능한 정보보호 제품, 대규모 정보보호 시장 형성, 안전하게 동작하는 정보보호 제품을 가능케 하며, 궁극적으로 안전한 정보통신 서비스 및 디바이스를 실현 가능하게 하여 안전한 지식 기반 사회를 구축할 수 있음

• 정보보호기술의 발전은 지식기반 정보화 사회를 유지하기 위한 바탕을 제공하며, 이는 특히 인터넷 망의 가용성과 신뢰성, 그리고 무결성을 제공하는 기술임. 따라서 정보보호 기술은 일반적인 정보통신망의 안전성과 신뢰성을 향상하고, 지식 기반 전자정부의 유용성을 증대할 수 있음. 이렇게 함으로써, 정보 및 통신 시스템의 신뢰성과 안전성을 보장함으로써 신뢰할 수 있는 지식기반 정보화 사회를 달성할 수 있을 것임. 또한 지문 및 홍채 인식, 그리고 스마트 카드 등의 인간 친화적 정보보호 제품을 통하여 원격 가전 제어 및 재택 근무를 가능케 하여 국민 생활의 질을 향상

할 수 있을 것임

- 정보보호 산업은 발전 속도가 매우 빠른 산업분야여서 정보보호 표준화는 정보보호 산업체의 제품의 경쟁력을 향상시킬 수 있을 것이고, 이를 통한 수출 증대 효과를 극대화할 수 있음. 또한, 국내 정보보호 제품의 국제 시장 점유율을 높이는 효과를 갖음. 이를 통해, 국내 고용 창출 효과를 극대화 할 수 있고, 정보보호 기술력을 독자적으로 가짐으로써 IT 강국의 이미지를 고양시킬 수 있음
- 국제 표준화는 ITU-T에서 정보보호 분야의 리드 SG인 SG17을 통하여 추진하고, 완성된 국제 표준 중에서 중요도와 산업체 파급 효과 등을 고려하여 대상 표준을 선정하고 TTA를 통하여 국내 표준화를 추진함
- 정보보호 기술의 표준화는 기반이 되는 암호 알고리즘 표준화, 이를 이용하여 구현되는 네트워크 및 시스템 정보보호 기술의 표준화, 응용 서비스 기술 표준화, 그리고 평가 및 관리 표준화를 통하여 상호동작이 가능한 정보보호 제품, 대규모 정보보호 시장 형성, 안전하게 동작하는 정보보호 제품을 가능케 하여, 궁극적으로 안전한 정보통신 서비스 및 디바이스를 실현 가능하여 안전한 지식 기반 사회를 구축할 수 있음
- 응용서비스를 기반으로 한 정보보호 기술의 표준화는 기술 규격 정립을 통해 산업체의 기술 개발을 위한 적절한 이정표 역할을 제시할 수 있고 또한 동종의 서비스 또는 제품을 생산하는 산업체간의 기술 유동성을 제공할 수 있음. 또한, 표준화는 정보보호 기업이 관련 시장 선점을 하는데 주요한 역할을 수행할 수 있기 때문에 정보보호 산업체의 제품의 경쟁력을 향상시킬 수 있을 것이고, 이를 통한 수출 증대 효과를 극대화할 수 있음. 즉 국내 정보보호 제품의 국제시장 점유율을 높이는 효과를 갖음
- 응용보안 분야의 세부 기술을 위한 공통의 평가 및 인증 방안의 표준화는 세부 기술 규격의 정립을 정확히 평가하는 매우 중요한 도구로써 활용될 가능성이 높기 때문에, 응용보안 표준안을 바탕으로 한 산업체의 시장 진입 및 제품 개발이 활발해질수록 더불어 평가인증 표준안의 정확도의 신뢰성은 높아질 것임. 그러므로 잘 제정된 평가 및 인증 표준안의 도출은 타 기술 표준안의 보편적 채용 가능성 및 우수성을 검증하기 위한 주요한 수단으로 기능할 것이며, 평가 및 인증의 영역 또한 비단 일부 응용서비스에 국한되는 것이 아니라 정보보호 전 분야로 확대 적용될 것으로 예상할 수 있음
- 이렇게 함으로써, 국내 고용 창출 효과를 극대화 할 수 있고, 정보보호 기술력을 독자적으로 가질 수 있어서, IT 강국의 이미지를 고양시킬 수 있음. 구체적으로 2010년까지 정보보호 표준 분야의 세계 5대 강국에 진입을 목적으로 함

2. 국내외 현황분석

2.1. 시장 현황 및 전망

2.1.1. 국내 시장 현황 및 전망

• 국내 정보보호산업 매출 현황

- 정보보호산업은 〈표 5〉와 같이 크게 "시스템 및 네트워크 정보보호 제품" 및 "정보보호서비스"의 두 분야로 구분될 수 있으며, 본 표에서는 2005~2006년의 매출 현황을 보여주고 있음
- 정보보호산업의 2005년도 매출 실적은 6,807억원이며 2006년도 (예상) 매출액은 7,348억원 규모로 전년대비 7.9% 증가할 것으로 조사됨
- 시스템 및 네트워크 정보보호제품 분야는 2005년 매출 총액 5,834억원에서 2006년 매출 (예상)액이 6,252억원으로 약 7.2% 증가할 전망이며, 정보보호 서비스 분야는 2005년 매출 총액 973억원에서 2006년 매출 예상액이 1,096억원으로 약 12.7% 증가할 것으로 나타남

〈표 5〉 정보보호산업의 분류별 매출액 현황 [단위: 백만원]

구분	2005년	2006년	증감률(%)	매출비중(%)
시스템 및 네트워크 정보보호제품	583,423	625,182	7.2	85.1
정보보호서비스	97,282	109,610	12.7	14.9
합계	680,705	734,792	7.9	100.0

(출처) 한국정보보호진흥원, "2006 국내 정보보호산업 통계조사"

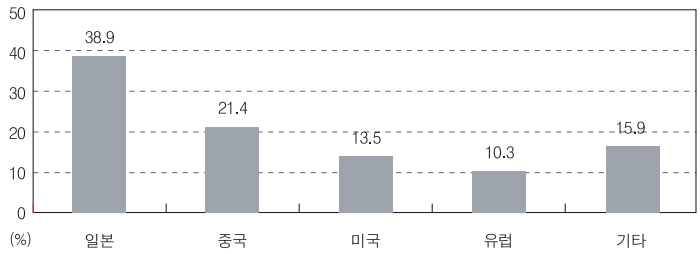
• 국내 정보보호산업 수출입 현황

- 수출 현황
  ◦ 2005년도 수출액 290억원에서 2006년도에 520억원으로 79.6%로 상승할 것으로 전망. 구체적으로 '시스템 및 네트워크 정보보호제품' 분야인 경우 2005년 수출액이 270억원에서 2006년도에는 86.6% 증가한 503억원 규모가 될 것으로 전망되며, '정보보호서비스' 분야는 2005년 수출액이 20억원에서 2006년도에는 17억원으로 14% 감소하는 것으로 조사됨
- 정보보호관련 기업의 주요 수출 국가
  ◦ '일본'이 38.9%로 가장 높게 나타났고, 다음으로 '중국' 21.4%, '미국' 13.5%, '유럽' 10.3%순으로 나타남. 기타 주요 수출국으로는 동남아시아, 멕시코, 브라질 등으로 나타남. 수출은 2006년 520억원으로 2005년도 289억원에 비해 79.6% 증가할 것으로 조사됨
- 수출 전망
  ◦ 2007년도에는 781억원에 이를 것으로 전망됨. 이를 대분류별로 살펴보면, '시스템 및 네트워크 정보보호제품' 분

야는 2005년도 269억원에서 2006년도 503억원으로 86.6%가 증가하여 2007년에 763억원을 이를 것으로 전망되며, '정보보호서비스' 분야는 2005년도 20억원에서 2006년도 17억원으로 14.0%가 감소할 것이지만, 2007년도에는 소폭 성장하여 18억원 규모가 될 것으로 전망

〈표 6〉 정보보호산업의 수출 현황 [단위: 백만원]

구분	2005년	2006년	증감률(%)	매출비중(%)
시스템 및 네트워크 정보보호제품	26,997	50,331	86.8	96.7
정보보호서비스	1,997	1,717	-14.0	3.3
합계	28,974	52,048	79.6	100.0



〈그림 3〉 정보보호산업의 주요 수출국가 현황

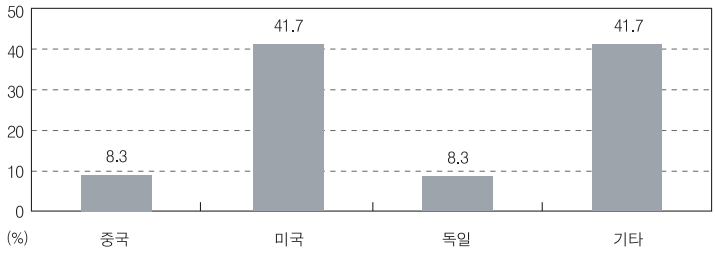
(출처) 한국정보보호진흥원, "2006 국내 정보보호산업 통계조사"

- 수입 현황
  - 2005년도 수입액이 423억원에서 2006년도에는 559억원으로 32.1%가 상승할 것으로 전망. 대분류별로 살펴보면, '시스템 및 네트워크 정보보호제품' 분야인 경우 2005년 수입액이 385억원에서 2006년도에는 35.0%가 증가해 519억원 규모가 될 것으로 전망되며, '정보보호서비스' 분야는 2005년 수입액이 38억원에서 2006년도에는 39억원으로 2.8%가 증가할 것으로 조사
- 정보보호관련 기업의 주요 수입 국가
  - 정보보호관련 기업의 주요 수입국가는 '미국'이 41.7%(15개 기업)로 가장 높게 나타났고, 다음으로 '중국'과 '독일'이 각각 8.3%(각각 3개 기업) 순으로 나타남. 기타 주요 수입국가로는 '이스라엘', '뉴질랜드', '대만' 등으로 나타남
- 수입 현황
  - '시스템 및 네트워크 정보보호제품' 분야의 수입 전망은 2006년에 519억원으로 2007년도에는 35.0%가 증가해 656억원에 이를 것으로 전망되고, '정보보호서비스' 분야의 수입 전망은 2006년에 39억원에서 2007년도에는 2.8%가 증가해 39억원에 이를 것으로 전망

〈표 7〉 정보보호산업의 수출 현황

[단위: 백만원]

구분	2005년	2006년	증감률(%)	매출비중(%)
시스템 및 네트워크 정보보호제품	38,471	51,943	35.09	93.0
정보보호서비스	3,804	3,909	2.8	7.0
합계	42,275	55,852	32.1	100.0



(그림 4) 정보보호산업의 주요 수입국가 현황

(출처) 한국정보보호진흥원, "2006 국내 정보보호산업 통계조사"

• 국내 정보보호산업 매출 전망

- 정보보호산업의 매출액 전망은 2005년도 6,807억원에서 2011년까지 CAGR이 9.64%로 지속적으로 상승하여 2011년에는 1조 1,821억원에 이를 것으로 전망됨. 대분류별 매출 전망을 살펴보면, '시스템 및 네트워크 정보보호 제품' 분야는 CAGR이 9.50%로 꾸준히 성장하여 2011년에는 1조 55억원을 이를 것으로 전망되며, '정보보호서비스' 분야는 CAGR이 10.47%로 2011년도에 1,768억원에 이를 것으로 예상

〈표 8〉 정보보호산업의 매출 전망

[단위: 백만원]

구분	2005년	2006년	2007년	2008년	2009년	2010년	2011년	CAGR(%)
시스템 및 네트워크 정보보호제품	583,423	625,182	713,689	790,940	864,482	935,633	1,005,495	9.50
정보보호서비스	97,282	109,610	123,053	136,495	149,938	163,380	176,823	10.47
합계	680,705	734,792	836,742	927,435	1,014,420	1,099,013	1,182,318	9.64

(출처) 한국정보보호진흥원, "2006 국내 정보보호산업 통계조사"

• 국내 정보보호산업의 분류별 매출 전망

- 〈표 8〉는 2005년부터 2011년까지 "시스템 및 네트워크 정보보호 제품" 및 "정보보호서비스" 분야의 세부적인 매출 예상치를 보여줌

- 구체적으로 정보보호산업의 품목 분류 중 대분류로는 시스템 및 네트워크 정보보호 제품, 정보보호서비스로 크게 2가지 분야로 분류하고 시스템 및 네트워크 정보보호제품분야는 침입차단(방화벽)시스템, 침입방지시스템(IPS), 보안관리, 가상사설망(VPN), 인증제품, Anti-Virus, Anti-Spam, 보안운영체제(Secure OS), PC보안, 컨텐츠

보안, 공개키기반구조(PKI), 접근관리, 무선/모바일 보안, 바이오인식 제품, 기타 제품 등 15개의 소분류로 나누었으며 15개의 소분류에는 총 34개의 제품군으로 세분화 하였음. 정보보호서비스는 인증서비스, 보안관제, 보안컨설팅, 유지보수, 기타서비스 등 5개의 소분류로 나눔

- 시스템 및 네트워크 정보보호 제품

시스템 및 네트워크 정보보호제품 분야의 매출액에 대한 전망을 조사 분석한 결과, '무선/모바일 보안' 분야가 CAGR이 24.34%로 가장 높은 성장세를 보이고 있으며, 다음으로 'Anti-Spam' 14.73%, 'Anti-Virus' 13.10%, '컨텐츠보안' 12.52%, '침입방지 시스템' 11.01% 등의 순으로 성장할 것으로 전망

- 정보보호 서비스

정보보호서비스 분야의 매출 전망을 살펴보면, 2005년 973억원에서 2011년까지 CAGR이 10.47%로 지속적으로 상승하여 1,768억원에 이를 것으로 전망. 소분류별 매출 전망은 '보안관제' 분야의 CAGR이 13.84%로 가장 높은 성장을 보이고 있으며, 그 다음으로 '보안컨설팅' 13.03%, '인증서비스' 10.69%, '유지보수' 6.63%등의 순으로 성장할 것으로 전망

〈표 9〉 기술 분류별 국내 표준화 현황 요약 [단위: 백만원]

대분류	소분류	2005년	2006년	2007년	2008년	2009년	2010년	2011년	CAGR(%)
시스템 및 네트워크 정보보호 제품	침입차단(방화벽)시스템	89,108	94,554	104,896	115,075	125,107	135,006	144,787	8.43
	침입탐지시스템 (IPS)	62,406	71,469	80,532	89,595	98,658	107,721	116,784	11.01
	보안관리	87,957	101,038	112,519	122,767	132,049	140,562	148,455	9.12
	가상사설망	53,776	54,558	64,340	69,622	74,904	80,186	85,468	8.03
	인증제품	56,736	42,691	56,202	68,015	78,981	89,321	99,123	9.75
	Anti-Virus	57,935	68,671	79,681	90,083	100,185	110,386	121,232	13.10
	Anti-Spam	10,756	15,438	18,715	21,010	22,616	23,740	24,527	14.73
	보안운영체제	28,652	29,144	29,636	30,128	30,620	31,112	31,604	1.65
	PC 보안	29,500	32,662	35,824	38,986	42,148	45,310	48,472	8.63
	콘텐츠 보안	27,329	32,554	37,779	42,202 4	6,624	51,047	55,469	12.52
	공개키기반구조 (PKI)	16,085	17,735	19,385	21,035	22,685	24,335	25,985	8.32
	접근관리	11,221	9,087	11,378	13,510	15,501	17,363	19,110	9.28
	무선/모바일 보안	2,516	3,646	4,776	5,906	7,036	8,166	9,296	24.34
	바이오인식 제품	43,195	46,725	51,697	55,864	59,629	63,192	66,655	7.50
	기타 제품	6,251	5,210	6,329	7,142	7,739	8,186	8,528	5.31
	소 계	583,423	625,182	713,689	790,940	864,482	935,633	1,005,495	9.45
정보보호 서비스	인증서비스	6,549	7,465	8,381	9,297	10,213	11,129	12,045	10.69
	보안관제	22,241	26,602	30,963	35,324	39,685	44,046	48,407	13.84
	보안컨설팅	26,331 3	1,093	35,855	40,617	45,379	50,141	54,903	13.03
	유지보수	40,051	43,186	46,321	49,456	52,591	55,726	58,861	6.63
	기타서비스	2,110	1,264	1,533	1,801	2,070	2,338	2,607	3.58
	소 계	97,282	109,610	123,053	136,495	149,938	163,380	176,823	10.47
합 계		690,705	734,792	836,742	927,435	1,014,420	1,099,013	1,182,318	9.64

(출처) 한국정보보호진흥원, "2006 국내 정보보호산업 통계조사"

2.1.2. 국외 시장 현황 및 전망

• 국외 정보보호산업 매출 현황

- 세계 정보보호시장 규모는 2003년에 83억 달러 정도, 2004년도에는 98억달러, 2006년도에 135억 정도에 다다를 것으로 전망. 2002년부터 2006년까지의 시장전망에서는 시장규모가 2005년에는 115억달러 규모로, 그리고 2006년에는 135억달러를 넘는 규모의 시장이 형성되며, 2002년부터 2006년까지 5년간 연평균 17%의 성장이 전망
- IT 시장대비 정보보호시장은 과거 3년간 국내시장이 9.02%, 세계시장이 19.09% 성장하여 IT시장 성장보다 높은 성장을 지속. 그러나 국내정보보호시장은 세계시장에 비해 절반에도 미치지 못하는 성장률을 기록하였으며, 또한 국내 IT시장에서 차지하는 비중은 과거 3년간 약 0.3%로 매우 미약한 상황. 세계 IT시장에서 차지하는 정보보호시장 비중은 매년 꾸준히 증가하여 05년 1.2%로 상승

〈표 10〉 정보보호산업과 IT 산업의 성장률('03년~'05년) 비교 [단위: 억원(국내), 백만달러(세계)]

구 분		2003	2004	2005	3년간 CAGR
국내	정보통신산업 (A)	2,016,230	2,285,251	2,332,089	7.55%
	정보보호산업 (B)	5,862	6,261	6,967	9.02%
	점유비율 (B/A)	0.29%	0.27%	0.30%	
세계	정보통신산업 (C)	2,265,700	2,494,800	2,688,400	8.93%
	정보보호산업 (D)	22,807	27,192	32,344	19.09%
	점유비율 (D/C)	1.01%	1.09%	1.20%	
IT 시장 세계대비 국내비중 (A/C)		8.90%	9.16%	8.67%	
정보보호시장 세계대비 국내비중(B/D)		2.57%	2.30%	2.15%	

(출처) KISA, KAIT 등 관련기관 통계 및 Gartner, IDC의 조사기관 자료 정리

• 국외 정보보호산업의 분류별 매출 현황

- 정보보호 시스템 시장은 보안 소프트웨어와 하드웨어 및 보안 서비스 등 크게 세부문으로 구분. IDC 분석에 따르면 전세계 IT 보안시장은 2001년에 약 169억 달러 규모에서 2006년에는 약 445억 달러 규모에 이르러 CAGR이 21%를 넘어설 것으로 전망
- 각 부문별로는 보안 서비스 시장이 2001년~2006년까지 가장 큰 규모를 차지하겠으나 보안 하드웨어 시장이 동 기간동안 높은 신장률을 보여 2006년에는 소프트웨어 시장과 함께 전체 시장의 절반 이상을 차지할 것으로 봄. 보안 서비스, 보안 하드웨어, 보안 소프트웨어 시장의 2001년~2006년도 CAGR은 각각 24%, 25%, 16%를 나타내어 앞으로 보안시장의 동인이 소프트웨어에서 하드웨어 응용제품으로 옮아갈 것으로 예상. 하드웨어 응용제품들 중에서 특히 방화벽/VPN과 네트워크 침입탐지 응용제품들이 다양한 가격대를 형성함으로써 성장의 견인차 역할을 할 것으로 보임

〈표 11〉 국외 정보보호산업 분류별 매출 현황

대분류	소분류	2003년	2004년	2005년	2006년	CAGR(%) 2001-2006
보안 S/W	암호화	260.0	293.8	332.0	265.2	10.0
	방화벽/VPN	1,015.0	1,136.8	1,261.8	1,388.0	0.2
	침입탐지(IPS)	896.2	1,048.6	1,205.9	1,386.7	17.5
	보안컨텐츠관리(SCM)	3,247.0	3,855.0	4,591.0	5,372.0	21.7
	보안 3A	2,701.0	3,025.0	3,422.0	3,899.0	12.0
합 계		8,119.2	9,289.2	10,812.7	12,411.0	15.8
이동 보안 S/W	암호화	20.8	27.9	38.2	53.0	36.59
	방화벽/VPN	14.2	19.3	26.5	38.2	39.08
	침입탐지(IPS)	6.7	13.1	24.1	41.6	83.80
	보안컨텐츠관리(SCM)	45.5	85.5	165.3	311.6	89.90
	보안 3A	40.5	60.5	119.8	253.4	84.27
합 계		127.7	206.3	379.3	697.7	76.13
보안 H/W	바이오매트릭스	106.5	124.7	146.0	169.5	16.1
	토큰 및 IT인증 스마트카드	642.1	855.8	1,186.1	1,482.7	27.3
	방화벽/VPN 보안제품	1,971.6	2,523.6	3,129.3	3,767.7	24.4
	IPS 보안제품	261.3	326.6	375.5	420.6	23.7
	기타 보안제품	140.8	268.9	390.0	506.9	73.8
	전용 IP VPN	1,410.2	1,693.0	1,982.8	2,251.2	20.7
	암호화 가속기	146.6	187.6	238.6	301.4	26.0
합 계		4,679.1	6,010.2	7,448.3	8,900.0	24.8
보안 서비스	컨설팅	2,431.5	2,886.7	3,700.4	4,606.6	19.9
	설치	5,027.0	6,413.6	7,832.4	9,750.6	24.3
	관리	2,822.0	3,622.3	4,606.6	5,734.8	26.5
	사고대응	445.5	583.6	761.3	947.7	28.6
	교육 및 훈련	1,243.0	1,429.1	1,747.9	2,175.9	21.1
합 계		11,969.0	14,915.4	18,648.5	23,215.7	23.7
총 시장 규모 합계		24,895.0	30,421.1	37,288.8	45,224.4	22.02

(출처) IDC, 2002. 12 및 IITA 자료

- 국외 정보보호산업 매출 전망

- 세계 보안 소프트웨어 시장은 2003년도에 총 매출액 84억달러를 달성하였으며, 이는 2002년도 대비 17.5% 성장한 수치로 기록됨. 최근 IDC 예상에 따르면 보안 소프트웨어 전체 시장은 2008년도에 163억달러에 이를 것이며, 연평균 복합 성장률은 14%에 근접할 것으로 전망 (〈표 12〉 참고)

〈표 12〉 기술 분류별 세계 보안 소프트웨어 매출 전망 [단위: 백만달러]

구분	2003년	2004년	2005년	2006년	2007년	2008년	Share(%) 2003	CAGR(%) 2003-2008	Share(%) 2008
보안콘텐츠관리	3,427	4,206	4,994	5,815	6,665	7,477	40.6	16.9	46.0
인증 및 접근제어	2,213	2,408	2,042	2,904	3,195	3,508	26.2	9.7	21.6
보안/취약성 관리	1,210	1,489	1,809	2,176	2,593	3,043	14.3	20.3	18.7
IDS/IPS	366	374	381	391	402	416	4.3	2.6	2.6
Firewall/VPN	912	982	1,041	1,098	1,153	1,203	10.8	5.7	7.4
그 외 보안기술	307	354	412	476	548	623	3.6	15.2	3.8
합계	8,435	9,813	11,279	12,860	14,555	16,270	100.0	14.0	100.0

(출처) IDC. 2004 - World Security Software Revenue by Market, 2003-2008

- 전체 보안 소프트웨어 시장을 지역별로 구분하면 다음 〈표 13〉와 같음. 보안 서비스 시장은 계속해서 확대될 것으로 예상되며, 특히 아시아/태평양, 라틴 아메리카 그리고 서유럽 등지가 급속한 성장을 보이고 있음
- 보안 서비스 시장의 특성상 고려되어야 할 요소는 기술적 장애물의 극복 능력과 함께 제도적이며 문화적인 장애요소도 간과하지 말아야 한다는 점임. 또한 지역 전문가들과의 전략적 파트너 관계 유지와 보안문제에 대한 국제적 균형에 맞춘 지역화 전략개발이 중요시되고 있음

〈표 13〉 지역별 세계 보안 소프트웨어 매출 전망 [단위: 백만달러]

구분	2003년	2004년	2005년	2006년	2007년	2008년	Share(%) 2003	CAGR(%) 2003-2008	Share(%) 2008
북아메리카	4,133	4,790	5,478	6,180	6,898	7,614	49.0	13.0	46.8
서유럽	2,556	2,983	3,446	3,980	4,585	5,206	30.3	15.3	32.0
아시아/태평양	1,324	1,548	1,787	2,049	2,333	2,619	15.7	14.6	16.1
기타 지역	422	493	568	651	739	830	5.0	14.5	5.1
합계	8,435	9,813	11,279	12,860	14,555	16,270	100.0	14.0	100.0

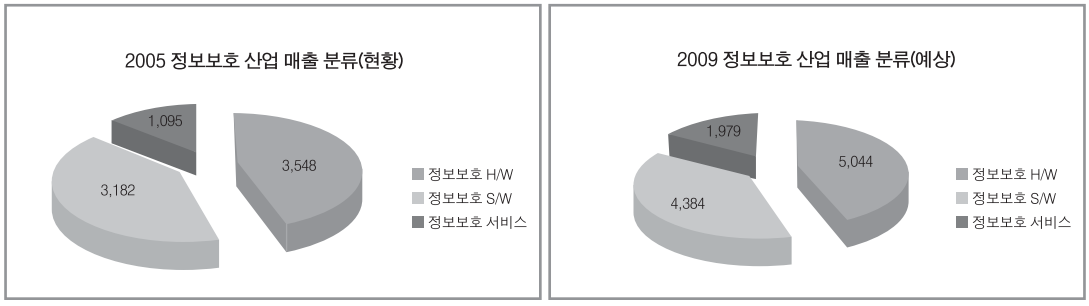
(출처) IDC. 2004 - World Security Software Revenue by Region, 2003-2008

2.1.3. 시장 현황 요약

- 국내 정보보호 시장 현황
  - 국내 정보보호산업 매출은 크게 "정보보호 하드웨어", "정보보호 소프트웨어", "정보보호 서비스"의 3대 분야로 구분하여 고려할 수 있으며 이들 세 분야의 예상 매출액 합산을 정보보호산업의 예상 규모로 잠정 집계할 수 있음
  - 정보보호산업의 매출액 전망은 2005년도 6,807억원에서 2011년까지 연평균복합성장률(CAGR:Compound Annual Growth Rate)이 9.64%로 지속적으로 상승하여 2011년에는 1조 1,821억원에 이를 것으로 전망. 대분류별 매출 전망을 살펴보면, 이중 '시스템 및 네트워크 정보보호제품' 분야는 CAGR이 9.50%로 꾸준히 성장하여 2011년에는 1조 55억원을 이를 것으로 전망되며, '정보보호서비스' 분야는 CAGR이 10.47%로 2011년도에 1,768억원으로 전망

- 정보보호산업의 수출 전망은 2006년 520억원으로 2005년도 289억원에 비해 79.6% 증가할 것으로 조사되어 2007년도에는 781억원에 이를 것으로 전망. 또한, 정보보호산업의 수입 현황은 2005년도 수입액이 423억원에서 2006년도에는 559억원으로 32.1%가 상승할 것으로 전망
- 더불어, KISA의 정보보호산업 매출전망 보고에 따르며 정보보호 하드웨어 분야의 경우 2005년 3,548억원에서 2009년 5,044억원으로, 정보보호 소프트웨어 분야는 2005년 2,634억원에서 2009년 4,384억원으로, 정보보호서비스 분야는 2005년 1,095억원에서 2009년 1,979억원으로 성장할 전망이며 이를 연평균 복합 성장률로 비교하면, 각각 11.01%, 10.73%, 17.75%로 집계될 수 있어, 정보보호서비스 분야가 가장 큰 성장 잠재력을 가지고 있는 것으로 밝혀짐. 즉 (그림 5)와 같이 2009년 총 예상 매출액 11,407억원 중 하드웨어 분야가 44.22%(5,044억원) 소프트웨어 분야가 38.43%(4,384억원), 그리고 정보보호 서비스 분야가 17.35%(1,979억원)을 각각 차지할 것으로 예상

〈그림 5〉 2005, 2009년 정보보호 산업 매출 분류 (참조: KISA)



• 국외 정보보호 시장 현황

- 세계 정보보호 시장은 대형정보보호업체(General Player)와 정보보호전문업체(Niche Player)로의 양극화가 심화되고 있는 실정. 또한 자사 플랫폼(네트워크, OS, 애플리케이션 등)에 관련 보안 제품을 패키지화하는 경향이 있어 세계시장은 글로벌 대형기업 위주로 재편되는 경향이 두드러지게 나타나고 있음. 2001년 세계 10대 보안업체 중 대형기업은 유일무이하게 IBM뿐이었으나, 2005년 Cisco, Junifer, MS 등의 기존 정보통신 대형 벤더들이 사업 영역을 정보보호 분야로 확대함에 따라 〈표 14〉와 같이 총 5개로 증가하게 됨

〈표 14〉 세계 및 국내 주요 정보보호업체 매출 현황 [단위: 억달러]

		2001		2005		02~05 성장률(%)
합계		매출규모	점유율	매출규모	점유율	29.1%
1	Symantec	724.0	12.02%	2,444.6	14.62%	35.6%
2	Cisco	26.1	0.43%	1565.3	9.36%	178.3%
3	McAfee	485.6	8.06%	958.5	5.73%	18.5%
4	CA	435.0	7.22%	698.7	4.18%	12.6%
5	Trend Micro	250.0	4.15%	621.9	3.72%	25.6%
6	IBM	277.0	4.60%	577.6	3.45%	20.2%
7	Check Point	531.0	8.82%	531.5	3.18%	0.02%
8	Junifer	-	-	427.6	2.56%	∞
9	MS	83.8	1.39%	306.2	1.83%	38.3%
10	RSA	165.0	2.74%	292.0	1.75%	15.3%
50	안연구소	20.2	0.34%	37.44	0.22%	16.7%
89	하우리	4.2	0.07%	11.03	0.07%	27.3%
93	어울림정보	0.1	0.00%	9.36	0.06%	211%
95	소프트포럼	3.9	0.06%	8.88	0.05%	22.8%
100	시큐어소프트	0.5	0.01%	6.08	0.04%	86.7%

(출처) IDC, Worldwide IT Security Software, Hardware, and Service 및 KISA, 국내외 정보보호산업 현황 및 주요 정책 진단

- 미국, 일본 등을 비롯한 주요 경제 지표 국가들의 오랜 경기 침체에도 불구하고 타 정보통신 분야에 비해 상대적으로 보안 시장이 호조를 띈 것은 긍정적인 측면으로 사료됨. 일례로 과거 2001~2002년에 많은 IT 시장이 붕괴 또는 퇴조의 모습을 보인 바 있으나 주요 기업과 공공기관이 정보통신 관련한 지출에서 보안부문을 최우선적으로 고려하고 있음이 밝혀진 바 있음
- 근래에는 ID관리와 웹 서비스에 참여하고 있는 벤더들이 향후 IT 보안 제품과 서비스 시장의 성장에 활력소 역할을 담당하고 있으며, 이 주류는 향후에도 어느 정도 지속될 것으로 전망. 그러나 보안 시장의 확대 및 성숙을 유지하기 위해서는 보안 응용제품과 서비스가 함께 기능하도록 조화를 이루고 설계되도록 할 필요성이 있다는 점을 간과해서는 안 될 것임
- 세계 경기의 회복에 따른 정보보호 시장은 다음과 같은 세 가지 요인의 힘을 받아 고속 성장을 지속할 것으로 전망
  - 국가 및 기업의 정보보호에 대한 투자 증대
  - 세계 최대시장인 미국을 중심으로 정보보호 관련 관심 증대 및 규제 강화
  - 인터넷 응용 서비스 관련 침해 사고 증대
- 또한 국외 정보보호 응용 시장의 잠재적인 성장을 이끌 것으로 예상되는 주요 요인은 다음과 같이 고려될 수 있음
  - 보안 관리 · 운영 활동이 활발해짐에 따라 기존의 보안 AAA (Administration, Authentication, and Authorization) 소프트웨어가 다시금 중요한 솔루션으로 고려될 것이며, ID 관리와 웹 서비스 보안이 AAA 기술에

대한 광범위한 소비를 가져옴으로써 보안 AAA 솔루션 증가를 촉진시킬 것으로 기대

◦ 공격 유형 또한 지금보다 더 큰 파괴력으로 무장한 "혼합 공격"이나 "하이브리드 웜" 바이러스들이 출현할 것으로 예상되며, 또한 무선망 및 이동통신망에 대한 해킹과 웜 공격이 빈번할 것으로 발생할 것으로 전망. 특히 기업 컴퓨터 시스템을 대상으로 한 유무선을 넘나드는 인지 및 방어가 어려운 형태의 공격이 감행될 것이며, 네트워크에서의 다양한 취약성을 대상으로 한 복합 공격이 유행할 것으로 판단

◦ 전통적으로 보안 서비스 시장의 수요는 기업에서 비롯되었으며 그 영향력은 향후 상당 기간 계속될 것으로 예상. 특히 기업들이 직원, 고객, 파트너, 공급자 등이 구성하는 기업내부프로세스를 신뢰성 있는 환경을 기반으로 운영하기 위한 모델을 경영 전략의 일부로 채택하게 될 것임

◦ IT 시장에서 개인 부문 수요는 20%를 차지하는 반면에, 정보보호 부문은 약 7%에 그치고 있는 것이 현 실정. 그러나 향후 우수한 컴퓨팅 능력을 제공하는 모바일 단말의 확산이 이미 진행 중에 있고 유비쿼터스 환경의 큰 주축으로 가능할 것이라 전망되고 있어, 개인 맞춤형 보안 제품 및 서비스의 개발을 통한 시장 개척이 주요한 정보보호 이슈로 떠오를 것임

2.2. 기술개발 현황 및 전망

2.2.1. 국내 기술개발 현황 및 전망

■ 정부정책기조

- 정부는 선도적 정보화정책을 통해 이룩한 세계최고의 IT인프라가 해킹, 바이러스, 개인정보 침해, 스팸메일 등 정보화 역기능 문제로 인해 침해당하는 것에 적극적으로 대응하고, 안전하고 신뢰할 수 있는 미래 유비쿼터스 환경 실현의 초석이 될 안정적인 지식정보사회를 구축하기 위한 중장기 정보보호 로드맵을 수립
- 중장기 정보보호 로드맵은 네트워크 융합, 신규 IT 서비스 등 유비쿼터스 환경에 적합한 새로운 정보보호 프레임웍을 구축한다는 취지하에 BcN 등 첨단 인프라의 안전성 확보, 신규 IT 서비스 신뢰체계 구축, 인터넷 침해사고 예방, 개인 프라이버시 보호 등을 핵심 목표로 함
- 최근 온라인 전자거래가 급증하고, VoIP/IPTV 등 신규 응용서비스 분야의 기술 확산이 급속도로 진전되면서, 응용서비스 보안 분야에서 전자거래 보안, 전자우편/차세대 웹 보안, 전자투표/공증, 디지털콘텐츠보호, 쉘보안, VoIP/IPTV 보안, P2P 보안, 신뢰 컴퓨팅 보안, lawful intereception 등의 핵심 요소기술 고도화를 추진 중이며, 이러한 신규 응용 분야 제품의 보안성 평가 및 관리체계 인증을 위한 평가인증 분야 표준화를 추진하고 있음

■ 국내 기술개발 현황 및 전망

가) 응용보안

- 전자우편

  전자우편 소프트웨어의 경우 운영체제에서 기본적으로 제공하거나 웹 브라우저 안에 포함되어 있어 그 개발에 대한 수요가 많지 않은 편임. 그리고 독립적인 전자우편 클라이언트에서 MIME을 지원해야 할 경우, 다양한 MIME 객체의 처리 기능이 구현되어야 하므로 많은 개발 노력을 요하게 됨. 이와 같은 이유로 국내에서 완전한 기능을 갖춘 전자우편 소프트웨어의 개발은 많이 이루어지고 있지는 않음. 반면에, 웹 메일 소프트웨어의 개발은 활발한 편이며, 특히 S/MIME, PGP 또는 별도의 전자우편 보안프로토콜을 이용한 웹 메일 솔루션들이 개발되어 있음

- 전자투표/공증

  전자투표는 기존의 종이 투표의 문제점인 투표 참여율의 감소, 투개표과정의 오버헤드 등을 극복하기 위해 전세계적으로 관심의 대상이 되고 있으며 이러한 전자투표는 크게 3가지 형태로 분류할 수 있음. 첫째, 지정된 투표소에서 전자투표기를 이용하는 방식, 둘째, 임의의 투표소에서 전자투표기를 이용하는 방식으로 유권자 인증이 가장 중요한 요소기술임. 셋째, 인터넷 혹은 휴대폰을 이용하는 원격 전자투표로 인증 및 보안기술의 적용으로 안전한 투표가 이루어져야 함. 현재로는 인터넷 등을 이용한 원격 전자투표는 매표 가능성이나 네트워크 취약점 등으로 인해 아직은 실험적인 단계에 머물러 있거나 해외 부재자 투표 등 극히 제한적인 환경에서만 실시되고 있음

  국내에서는 중앙선거관리위원회가 전자투표 사업추진단을 설치하여 정보화전략계획을 수립하고, 2005년 5월부터

전자투표기 및 인터넷 투표시스템의 개발 중. 선관위는 전자투표시스템의 도입을 위해서 해킹이나 시스템다운 등의 비상사태에 대비해 분산된 방식의 중앙처리시스템을 구축하고 선거기간동안 모든 시스템에서 안정적으로 자료가 실시간으로 저장될 수 있는 백업시스템을 개발. 또 중복투표 방지를 위한 통합선거인명부 확인시스템과 키오스크(Kiosk)를 사용하는 전자투표 시스템, 실시간 검증이 가능하고 개표상황의 실시간 체크와 후보자 자신이 자신의 득표에 대한 역추적이 가능하도록 하는 시스템도 개발 중. 이런 전자투표시스템은 개인 인증이 가능한 스마트카드를 도입하거나 인터넷 등 원격으로 투표가 가능한 시스템을 도입하여 운영될 계획. 한편 선관위는 유권자의 개인정보가 담겨있는 통합선거인명부를 온라인화하되 전자투표기는 오프라인으로 구성하여 유권자가 전국의 어느 투표소에서든 투표가 가능하도록 할 계획. 2008년 국회의원 총선부터는 전자투표를 전면적으로 적용하여 확대하고, 2012년에서는 집에서 모든 투표가 가능하도록 하는 것이 선관위 전자투표계획의 주요 골자임

• o u-지식 보안

한미FTA 체결로 개정 저작권법에서 P2P나 웹하드와 같은 온라인서비스사업자는 불법저작물 전송을 차단하는 기술적 조치를 의무화함으로써, 저작권 및 콘텐츠 보호 등의 u-지식 보안 기술 개발 필요성을 인식하고 있음. 콘텐츠에 저작자 정보를 삽입하여 저작권을 보호하는 워터마킹 분야에서 많은 경험과 기술을 축적하고 있으며, SW 및 실명ID 기반의 DRM, CAS 등의 콘텐츠 보호 솔루션을 개발/상용화를 진행하고 있음. 다만, 전용 디바이스 단위로 권한관리를 추구하는 DRM 콘텐츠 보호 솔루션으로 자신 소유의 타 디바이스로 구매 지식의 이동 불가로 사용자 불편이 있으며, 사업자들이 사용자의 이용 내역을 모니터링 등의 프라이버시 침해에 대한 일부 우려가 있음. 또한 새롭게 등장한 UGC 등의 프로슈머형 콘텐츠 보호를 위한 사용자 창작/수정/재가공 지식에 대한 지재권보호 및 지분표현 기술은 미약한 수준임. 따라서 익명성을 기반으로 한 u-지식 보안 기술 개발이 필요

• 쉘 보안

쉘 보안 관련하여 국내에서는 SFTP(Secure Shell File Transfer Protocol)를 이용한 파일전송 프로그램과 같이 소규모의 응용 기술개발만이 이루어지고 있으며, 독자적인 쉘 보안에 대한 국책연구소, 산업계에서의 기술개발 사례는 없음. 현재 쉘 보안은 독자적으로 사용되기 보다는, 다른 여러 보안 요소 기술들과 통합된 형태로 활용되고 있는 상황임

• VoIP 보안

VoIP와 관련된 기술개발은 크게 암호화 및 키관리 기술, 스팸 대응 기술, 보안 세션 제어 및 사용자 프라이버시 보호 기술로 분류할 수 있으며, 각 분야별 국내 기술 개발 현황은 다음과 같음

- VoIP 암호 및 키관리 기술
  ◦ 국내에서는 VoIP 암호화 장비로 IPSec[1] 기반 VPN[2] 기능을 갖는 VoIP 보안 제품이 주로 시장에 출시되었으나, 본점과 지점간 안전한 통화선로를 설정하는 VPN은 불특정 다수와 착발신 통화를 해야 하는 일반 전화서비스

1) Internet Protocol Security
2) Virtual Private Network

성격에는 적합하지 않음

– 최근 해외에서 SIP 서버 및 SRTP 툴킷을 포함한 SIP 툴킷을 개발한 바가 있으며, 국내에서도 암호 통화를 수행할 수 있는 비화용 휴대전화기 개발 사례가 있으나, 아직 국내에서는 VoIP 서비스를 위한 암호/키관리 API 모듈에 연구 개발이 미흡한 실정임

- VoIP 스팸 대응 기술
  - ◦ 국내에서는 2006년 2월, 인터넷전화 발신자번호를 조작하여 휴대폰 소액결제 사기범죄가 발생하였고, 대형기간사업자망에서 이동통신망으로 VoIP 스팸이 발생한 사례가 최근 불법스팸대응센터에 접수되는 등 VoIP 스팸이 사회적 문제로 등장하고 있으나, 국내 관련 기술 개발은 미비한 실정임
  - ◦ 2005년 7월부터 070 음성전화 상용 서비스를 제공 중인 일부 별정사업자들은 스팸 대응을 위한 기술적 조치로 호당 일정 수준이상 트래픽 발생을 차단하는 초보적인 스팸 대응 메커니즘을 적용하고 있으나, 가입자 증가에 따른 오류율 증가와 다양한 형태의 스팸에 대응하기 어려운 한계를 지님
- VoIP 보안 세션제어 기술 및 사용자 프라이버시 보호 기술
  - ◦ VoIP 서비스가 점차로 확대됨에 따라서 SBC 수요가 급속히 증가하고 있는 상황에서 국내 기간/별정사업자들은 외산장비 고가의 외산장비 수입을 고려하고 있으며, 극히 일부에서는 시급하게 NAT/FW 통과문제만을 해결할 수 있는 기능만을 구현하고 있음
  - ◦ 국내 사업자들은 SBC의 필요성은 인식하고 있으나 고가장비라는 점에서 쉽게 투자하지 못하고 있으며, 이로 인해 일부 외산장비를 도입 · 운영하는 환경을 제외한 사업자들의 망 환경이 외부에 노출되는 문제점을 지니며, SBC를 도입하더라도 SBC 시스템에 대한 DoS 위협이 대두됨에 따라 SBC에 대한 정보보호 기능이 점차 중요하게 요구되고 있음

• 스팸대책

원하지 않는 데이터를 다량으로 전송하는 것을 특징으로 하는 스팸 분야는 과거 이메일에만 국한되던 것이 최근 등장하고 있는 신규 IT 서비스를 대상으로 하고 있으며, 음성, 영상, 텍스트 등 다양한 형태를 띠고 있고, 휴대폰, 이메일, 팩스, 메신저, 팝업 등 다양한 매체를 통해 전송되고 있음. 최근 스팸 관련 국내외 기술 개발은 주로 VoIP를 중심으로 진행되고 있음. 숭실대, KISA, ETRI에 관련 기술 및 표준화를 진행중에 있으며, 삼성네트웍스는 브로드소프트사의 브로드웍스 라는 IP centric server와 주니퍼 SBC 장비인 보이스플로우를 이용한 탐지 및 차단 솔루션을 제공하고 있음. 이 솔루션은 하나의 VoIP 콜에서 일정 수준 이상의 트래픽을 발생시키거나, 하나의 IP에서 발생하는 초당 VoIP 콜의 수를 측정하여 필터링하는 방식이며, 초당 20개 이상의 VoIP 콜이 발생할 경우 스팸으로 규정하고 있음

스팸 분야에서는 VoIP 스팸을 제외하면 기술개발 보다는 정책적인 측면에서의 스팸 방지 대책을 세우는 형태에 있으며, 이에 따라 ITU-T SG17에서 스팸 방지 가이드라인과 관련된 표준화를 진행하고, IETF에서 SIP 관련 기술 표준화를 진행하는데 초점을 맞추고 있음. 정보통신망법 개정에 따라 국내에서는 정통부와 한국정보보호진흥원이 공동으로 스팸방지 가이드라인을 공표하였음 (2006년). 이 가이드라인에서는 정보통신서비스 제공자 측면에서

스팸 전송자에 대한 서비스 규제, 자료 열람 및 제출 요구 권한, 사업장 출입통제, 과태료 부과 기준, 자율 규제 등 항목을 제시하고 있으며, 광고전송자 측면에서는 이메일, 전화, 팩스 등 다양한 매체를 이용한 광고전송시 준수할 사항을 제시하고 있음

- 응용보안 강화 프로토콜

응용보안 강화 프로토콜 분야에서는 전송계층의 보안프로토콜인 TLS 그리고 패스워드 인증 프로토콜에 대한 기술 개발이 진행 중에 있음

패스워드 인증 기술의 경우 키 로밍 서비스, 인터넷 뱅킹 서비스, 망 관리 서비스와 같은 응용 보안 시스템에 부분적으로 응용되고 있으나 현재 독자적인 제품으로 개발된 사례는 없음

TLS 프로토콜은 국내에서 기술개발이 완료되어 다양한 상용시제품이 출시된 상황임. 보안 웹메일을 위해 TLS를 사용하고 있는 제품으로는 3R소프트의 보안 웹메일 솔루션인 엣시큐어와 소프트 이그제큐티브의 Merak 등이 존재함. 국내에서 TLS를 제공하기 위한 선보이고 있는 toolkit 제품들로는 ECC 알고리즘을 적용함으로써 PC는 물론 PDA나 휴대폰에서도 사용 가능하도록 개발한 IA시큐리티의 IA-TLS, 협우인포테크의 Dundas TCP/IP Secure Edition, 무선 인터넷 정보보호를 위한 장미디어 인터랙티브의 JX-WTLS 등이 존재함. 그 외에 SEENODE는 VoIP 솔루션에 사용자 등록 및 인증/권한 부여를 위해 TLS를 사용하고 있으며, 셋탑박스 업체인 이미지네트는 Magatainment VOD 서비스에서 셋탑박스 브라우저를 통한 데이터 암복호화를 위해 TLS를 사용하고 있음. 마지막으로 Rainbow 코리아는 이러한 SSL, TLS 사용의 급증으로 인한 서버의 과부하를 줄이기 위한 SSL/TLS 가속기인 CryptoSwift와 NetSwift2012 제품을 선보고 있음. 무선인터넷에서의 전자서명과 PKI 기술의 실용화에서는 활성화된 이동통신을 배경으로 빠른 속도로 표준개발이 이루어지고 있으며, 운용 경험에 있어서도 앞서 나갈 수 있을 것으로 평가되지만, 구현기술 등에서는 상당한 노력이 필요할 것임. 일부 상용 서비스 분야에서 상당한 기술력을 갖고 있는 것으로 판단되나, WIM, 암호 API 등의 기술 개발이 요구됨

- 안전한 P2P 보안

국내 주요 연구기관의 P2P 기술 관련 프로젝트로는 KISTI에서 수행중인 P2P 기반 분산 컴퓨팅에 관한 프로젝트인 Korea@home이 있으며, ETRI에서 수행중인 유무선 IPv6 기반 P2P 네트워크 정보보호 기술개발 과제가 있음. 산업계에서는 삼성종합기술원에서는 P2P기술이 가진 지적재산권, 확장성 문제와 IPv6와의 결합문제 등에 관하여 연구를 진행하고 있고, (주)대우정보시스템은 P2P 애플리케이션을 기업의 기간시스템, 특히 지식관리 시스템과 연동하는 프로젝트를 추진하고 있으며. (주)피어컴은 SK Mobile 지원으로 P2P 연구 선도 과제를 수행 중임

그밖에 소리바다, 프루나, 피투피아 등 여러 업체에서 P2P 파일 공유 서비스를 제공하고 있으며, P2P 보안 관련 기술 분야에서는 (주)아라기술과 (주)소만사 등이 패킷 필터링 기술에 기반한 P2P 트래픽을 수집 · 분석 및 제어하는 솔루션을 구축하고 있음

- PTV 보안

IPTV 서비스는 NGN 상에서 운용되는 고용량의 스트림 데이터 전송을 요하는 서비스인 동시에, 영상(VoD), 음성

(VoIP), 데이터(Internet), 그리고 다양한 부가 서비스를 핵심으로 하는 융합 서비스임. 따라서 IPTV 보안 기술 역시 상기 요소들의 유기적으로 결합을 전제로 하여 개발되어야 함. 국내외적으로 볼 때 현재까지는 이러한 요소들의 유기적 결합을 위한 보안 기술에 대한 논의는 전무한 상태임. IPTV 보안은 크게 유니캐스트/멀티캐스트 전송을 포함하는 NGN 보안, 복제방지/저작권 보호 등을 포함하는 IPTV 데이터 보안, 부가 서비스 보안 영역으로 구분 지을 수 있고, 이들은 다시 보안 기술이 탑재되는 위치에 따라 Head-end용, 중간노드(라우터 등)용, 셋톱박스(STB)용으로 구분됨

NGN 보안과 부가서비스 보안은 기존의 연속으로 보는 시각이 강하며, 국내 IPTV 보안 기술 분야에서는 IPTV 전송 데이터 보안 부분에서 콘텐츠 제공자의 우선 고려 사항인 DRM이나 수신제한시스템(CAS)을 이용하는 보안 기술만이 이슈가 되고 있음. DRM과 관련하여서도 기존의 멀티미디어 콘텐츠 보호에 이용되던 DRM을 IPTV에 적용하기 위해 변환하는 경우가 주를 이루고 있으며, CAS의 경우 기존의 공중파 방송이나 케이블TV에서 이미 국외 핵심 기술을 채용하고 있었기 때문에, 기술 개발 보다는 서비스 운용에 초점을 맞추고 있음. 이러한 점은 비디오 스트림 자체를 암호화/복호화 하는데 소요되는 시간을 줄이기 위한 연구 개발이 진행되고 있는 국외 기술 기발 현황과 비교해 볼 때 IPTV 보안 핵심 기술에서 또다시 국외 기술에 종속적인 형태를 가져올 수 있는 부분임. 참고로 국외에서는 공간/주파수 도메인 암호화, 선택적 암호화 등에 대한 기초 연구가 학계를 중심으로 진행되고 있으며, 논문 형태의 결과물이 도출되고 있고 아직까지 IPTV 서비스에 직접 적용되지는 않고 있음. 또한 visual 암호화, 암호화된 영상의 투명성(transparency) 보장[3] 등 신규 보안 기능에 대한 기초연구가 진행되고 있음.

IPTV 미들웨어와 관련하여 한국전자통신연구원(ETRI)은 2006년부터 정보통신부 및 국내 셋톱박스 제조업체들과 'ACAP 기반 IPTV용 미들웨어' 기술 개발을 추진하고 있음. 정통부와 ETRI가 함께 추진하는 프로젝트인 아이코드(i-code)는 IPTV 미들웨어 분야의 국내 표준을 마련하기 위한 것인데, 케이블방송과 지상파방송용으로 만들어진 ACAP(Advanced Common Application Platform)와 MHP(Multimedia Home Platform) 방식을 변환하여 IPTV 전용의 미들웨어를 개발하는데 목표를 두고 있음. 여기에 기존의 ACAP 및 MHP와 차별화를 위해 CAS, DRM과 같은 기술을 적용하는 연구를 진행 중에 있음

수신제한시스템(CAS)은 유료방송을 시청할 권한을 부여하거나 제한하는 시스템으로 기존의 공중파 방송과 케이블 TV와 같은 광대역 TV 전송에 사용되던 것이 IPTV의 멀티캐스트 스트리밍 보호를 위해 이용되고 있음. 수신제한은 IPTV 성공의 핵심 요소로 인식되고 있어 보안성과 안정성이 중요 이슈가 되고 있음. 국내에서는 이데토코리아, NDS코리아, 나그라비전 등 외산 CAS 업체가 주를 이루고 있으며, 엑스크립트, 코어트러스트, 싸이퍼캐스팅 등 국내 CAS 업체가 자체 기술을 제공하고 있음. KT의 IPTV 서비스인 메가TV는 현재 실시간 스트리밍 방식의 전송에 NDS코리아의 수신제한시스템(CAS)을 탑재하고 있음

IPTV의 주문형 비디오(VoD) 보호를 위해서는 DRM에 의존할 수밖에 없음. KT는 2007년 후반기부터 IPTV 서비스에 국내 업체인 코어트러스트의 제품을 채용하여, 불법복제 방지 · 사용자 및 장치 인증 · 콘텐츠 재생 기간 및

3) 암호화된 영상의 투명성(transparency)은 암호화된 데이터의 특성을 조정하기 위한 것인데, 기존의 암호화 기법은 암호화된 데이터의 주파수 특성을 확산시켜 노이즈처럼 보이게 만드는 데에 중점을 두고 있었음. 그러나 IPTV 전용의 암호화 기법에서는 암호화된 영상 데이터의 특성 중 일부(예를 들면, 사람의 움직임, 건물 외형 등)를 시청자가 인식할 수 있도록 하는 것이 투명성임. 투명성은 유료 TV 채널에 적용이 되어, 이를 보는 시청자로 하여금 채널 구매욕을 높이는 효과가 있기 때문에 IPTV 활성화에 매우 중요한 역할을 할 수 있는 기술임. 아날로그 공중파 방송이나 케이블 TV에서는 CAS 스크램블링에 의해 손쉽게 구현되었지만, 암호화에 의존하는 디지털 방송과 IPTV 분야에서는 새로운 암호화 방식에 의해서만 실현할 수 있음

횟수 제한 등의 기능을 제공함. 하나TV와 LG데이콤도 IPTV 서비스에 DRM을 적용할 예정임

IPTV의 특성상 DRM과 CAS가 동시에 적용될 수밖에 없는데, 최근에는 CAS와 DRM을 통합한 솔루션이 개발되고 있음. 하나TV는 셋톱박스 전문업체 셀런이 개발한 셀크립(CelCrypt)을 채용하였는데, 이것은 '실시간 DRM' 방식으로 주문형 콘텐츠의 저작권보호 뿐 아니라 IPTV 수신제한 및 가입자 관리도 DRM 하나로 실현한 제품임. 이 밖에도 이데토코리아의 'CA+DRM' 솔루션, NDS코리아의 비디오가드, 싸이퍼캐스팅의 델리캐스팅 등 제품이 있음

현재 CAS의 또 다른 기술개발 트렌드는 다운로더블 CAS(D-CAS)임. 즉 하드웨어(HW)와 소프트웨어(SW)를 결합한 기존 CAS와 달리 브로드밴드 등을 통해 셋톱박스에 내려 받는 방식임. SW 방식이 보안성을 저하한다는 우려가 있기는 하지만, 이는 양면성을 가진 문제라는 인식이 있고, 방송사업자 측면에서는 D-CAS가 셋톱박스 가격을 하락시키고 고장 발생률을 낮춘다는 장점을 갖고 있음. 국내 케이블 TV 업계에서 외산 CAS가 주류를 이루었던 점 때문에 D-CAS 분야의 기술 개발은 많은 관심을 모으고 있음. 한국디지털케이블연구원(K랩스)은 2007년에 북미 복수종합유선방송사업자(MSO) 3사가 D-CAS 개발을 위해 설립한 '폴리싸이퍼'와 D-CAS 공동 개발에 협력키로 함. LG전자는 CES 2006에서 북미 최대 케이블 사업자인 컴캐스트, CAS 업체인 나그라비전(NagraVision)과 공동으로 다운로더블 CAS(DCAS. Downloadable Conditional Access System)를 공개 시연한 바 있음.

IPTV 부가 서비스 분야에서는 IPTV 동일 채널 시청자들 간에 메시징, 채팅, 등급 지정(rating), 평가(reputation), 감상평, 채널 공지 등의 커뮤니티 활동이 활성화 될 것으로 예상됨. 현재 서비스 되고 있는 인터넷TV[4] 중 대표적이라고 할 수 있는 주스트(Joost)의 경우 이미 이러한 커뮤니티 서비스를 TV 채널과 동시에 제공 하고 있음. 이를 위하여 N:N 커뮤니티 환경에서의 사용자 데이터에 대한 암 · 복호화, 신뢰성(trust) 문제에 대한 기술 개발이 필요함. 한국전자통신연구원(ETRI)은 이에 대한 기반 연구로 P2P (Peer-to-Peer) 커뮤니티에서 보안 기술에 대한 연구를 진행 중에 있고 이러한 연구 결과를 IPTV 양방향 · 부가 서비스 및 커뮤니티 서비스에 적용하기 위한 추가 연구가 필요한 상황임

IPTV 네트워크와 관련하여서는 현재 NGN을 기반으로 한 유니캐스트와 멀티캐스트 방식만이 주요 전송 메커니즘으로 고려되고 있는 상황임. 국내에서는 한국과학재단(KOSEF) 지원으로 한국과학기술원(KAIST)에서 안정적인 IPTV 백본 네트워크에 대한 연구가 진행됨. 이에 반하여 국외 인터넷TV 분야의 연구 개발은 NGN을 기반으로 하기 보다는 응용 계층에서의 멀티캐스트를 대상으로 하는 경우가 대부분임. 이에 따라 최근에 ITU-T IPTV FG에는 오버레이(Overlay) 기반 멀티캐스트와 P2P 네트워크를 이용하는 스트리밍 전송에 대한 표준 기고서가 상정되고 있음. 특히 오버레이 기반 멀티캐스트는 ETRI가 중심이 되어 추진하고 있는 분야임

그러나 오버레이 기반 멀티캐스트를 위한 보안 기술에 대해서는 아직까지 구체적으로 논의되고 있지 않음. 이에 ETRI는 보안 이슈 및 메커니즘을 추가로 제안할 계획임

4) 인터넷을 통한 동영상 스트림 서비스를 인터넷TV와 IPTV로 구분 지울 수 있는데, 인터넷 TV는 인터넷 포털 형태의 VoD를 제공하는 서비스를 의미하고, IPTV는 NGN 상에서 통신 사업자 중심의 서비스를 의미함. 국내 인터넷 TV의 예로 곰TV, 아프리카 TV, 판도라TV 등을 들 수 있고, IPTV의 예로 하나로 TV, 메가TV 등이 있음

• STC (Secure TC)

신뢰 · 보안 서비스는 신뢰성의 개념을 시스템에 적용함으로써 해킹이나 유해한 환경으로부터 보호하는 목적으로 나온 패러다임으로, 많은 PC와 노트북 등에서는 이를 위한 디바이스들이 이미 장착되어 출시되고 있음. 이러한 현상은 시간이 지남에 따라 더욱 증가될 것으로 예측됨. HP, IBM, MS 등 여러 대형 업체들을 중심으로 산업표준인 TCG (Trusted Computing Group)을 만들어 이와 관련한 표준화를 진행하고 있음. 그러나 아직 국내에서는 이에 대한 적극적인 수용이나 개발 활동은 이루어지고 있지 않음. 향후 통신 환경이 모바일 형태로 흡수되어질 것으로 예측되므로 이를 위한 정보보호 기능의 제공이 더욱 필요할 것으로 예측됨

- 차세대 단말 환경에서의 신뢰보안 요구가 증대되고 있음.(기밀정보 유출, 위장, 불법 사용, 정상적인 서비스 방해, 프라이버시 침해 등을 방지하기 위한 정보보호 요소 기술의 개발이 필요함)
- SW 기반 정보보호에서 나아가 HW 기반 정보보호를 제공하기 위한 연구 개발 진행
- HP, IBM 등 대형 업체들은 TCG(Trusted Computing Group)을 통하여 신뢰보안 컴퓨팅에 관한 표준화를 진행 중이고 신뢰보안 서비스를 제공하는 기술을 개발 중임
- 국내는 현재 검토 중인 단계임

STC 관련 국내 기술 개발 현황은 다음과 같음

- ETRI 정보보호연구단에서는 2006년부터 STC에 관한 연구 개발을 진행 중임. 이 중에서도 차세대 모바일 단말기에서의 신뢰 보안 서비스를 위한 핵심 모듈인 STPM (Secure and Trusted Platform Module)을 개발하고 있음.
- 삼성전자의 시스템 LSI 사업 부문에서 스마트카드 기술은 년간 1억 개 이상 수출하는 수준이지만, 아직 TPM 에 대해서는 검토하는 단계임. 삼성전자는 TCG 회원사이지만, 적극적인 활동은 거의 하지 않고 있음
- 국내 산업계는 STC에 대해서 아직 검토하는 단계임. TCG의 표준화 상태를 더 관찰한 후 표준이 어느 정도 성숙되었을 때 개발을 시작할 전망임
- DAA (Direct Anonymous Attestation), 암호화 모듈, 보증(attestation) 등 TPM 기술과 관련하여 부분적인 접근을 시도하고 있음

• 차세대 웹 보안

차세대 웹서비스 정보보호 기술은 유비쿼터스 환경하에서의 다양한 서비스와 디바이스, 리소스 들의 안전한 통합 및 연동을 가능하게 해주는 정보보호 기술로, 웹 2.0 보안 기술, 시맨틱 웹서비스 보안 기술, 유비쿼터스 웹서비스 보안 기술, 모바일 웹서비스 보안 기술 등을 포함함

- 웹 2.0 보안 기술은 다양한 서비스 및 리소스의 결합에 의해 발생하는 웹 2.0 서비스 환경에서의 보안 위협을 해결하기 위한 정보보호 기술을 말함
- 시맨틱 웹서비스 보안 기술은 시맨틱 정보를 기반으로 보다 지능적이고 안전한 서비스 연동을 가능하게 해주는 정보보호 기술을 말함

- 유비쿼터스 웹서비스 보안 기술은 다양한 단말로 구성된 유비쿼터스 서비스들을 안전하게 연동시키기 위한 정보보호 기술을 말함
- 모바일 웹서비스 보안 기술은 웹서비스 기술을 모바일 환경까지 적용한 모바일 웹서비스의 안전성 보장을 위한 정보보호 기술을 말함

정통부에서는 웹서비스를 소프트웨어인프라에서 서비스 연동을 위한 핵심 기술로 채택한 바 있으며, 전자정부를 비롯한 공공부문에서는 웹서비스 기술을 범정부 시스템의 연계 통합을 위한 표준 기술로 채택하였음

기존의 유선 환경에서의 전자거래 등 비즈니스 서비스 영역에서의 웹서비스 정보보호 기술들은 기술 보급이 시작된 단계이나, 향후 기술 수요가 증가하리라고 예상되는 유비쿼터스 환경하에서의 다양한 서비스 및 디바이스 연동 및 통합을 위한 차세대 웹서비스 정보보호 기술은 아직 기술 개발 초기 단계임

◦ 국책 연구소

- 웹서비스 (Web Services) 보안과 관련하여 ETRI가 XML 전자서명, XML 암호, WS-Security, SAML (Security Assertion Markup Language), XACML (eXtensible Access Control Markup Language), XKMS (XML Key Management Specification) 등의 기술을 구현한 바 있음
- ETRI는 유무선 웹서비스를 위한 보안 표준 기술들을 개발하였으며, 이중 모바일 웹서비스 메시지 보안 구조 표준 기술은 ITU-T SG17을 통해 표준화를 추진중임
- ETRI는 웹 2.0 보안 기술, 시맨틱 웹 및 시맨틱 웹서비스 보안 기술, 시맨틱 기반의 보안 기술 등에 관한 개발을 준비중이며 이와 관련된 구체적인 기술개발은 아직 이루어지지 않고 있음
- KISA에서 KT와 함께 웹 사용자의 프라이버시 보호를 위한 P3P (Platform for Privacy Preferences) 소프트웨어를 개발한 바 있음

◦ 산업계

- 웹서비스 (Web Services) 보안과 관련하여 이니텍, 비씨큐어, STI Security 등에서 XML 전자서명 및 XML 암호 기술을 구현한 제품을 출시하였음
- 유선 환경에서는 웹서비스 보안 기술의 적용이 점차 확산되고 있으나 무선 환경을 위한 웹서비스 보안 상용 제품 국내 개발 사례는 아직 드문 실정임. 또한 유비쿼터스 웹 환경을 위한 보안 제품 개발도 전무함
- 웹 2.0 보안 기술은 주로 웹 어플리케이션 취약점 분석툴 및 웹방화벽 개발쪽에 집중되어 있으며, 펜타시큐리티, 듀얼 시큐리티 등에서 웹 방화벽 제품을 개발하였음
- KT, K4M 등에서 시맨틱 웹 상용 기술을 개발하고 있으나 아직 이를 위한 보안 기술 개발이나 시맨틱 기반의 정보보호 기술 개발은 이루어지지 않고 있음

◦ 학계

- 웹 2.0 보안 기술, 웹 프라이버시 보호 기술 등에 관한 연구가 이루어지고 있음

• Lawful Interception

ETRI BcN 사업단은 음성과 데이터의 통합화, 유무선 서비스의 통합화와 같은 통신환경의 융합의 일환으로 VoIP 기술 등에 관한 연구를 수행하고 있으며, 주로 망 융합, 망 관리, QoS 보장, 신규 서비스 적용, 기능 구현 등에 초점을 맞추고 있는 것으로 알려져 있음. ETRI는 BcN 기술 중 NGN 보안 영역의 일부로써 ETSI와 같은 표준화 단체의 LI 동향을 파악하고 분석하고 있는 실정이며 이와 관련된 구체적인 기술개발은 이루어지지 않고 있음. 다만 공적인 목적으로 국정원이 유선중계통신망 감청장비를 도입하여 보유하다가 폐기하였고, 1998 및 1999년 자체 개발 장비를 통해 이동망 감청에 활용한 것으로 보고된 바 있음

통신비밀 보호법 개정안이 정기국회에 올해 9월 제출될 예정인데, 그 주요 내용이 수사기관의 요청 등이 있을 경우 전기통신사업자에 감청을 위탁 또는 협조를 요청할 수 있도록 하는 것, 휴대전화의 감청이 가능하도록 할 것, 또한 이동통신 업체들은 2년, 그 외 전기통신사업자는 4년 내에 감청장비를 의무적으로 갖출 것 등의 내용을 담고 있어 LI 관련 장비 개발이 크게 요구될 것으로 전망됨. 이동통신 및 전기통신사업자들을 중심으로 1990년대 중반부터 감청과 관련된 특허 기술들이 본격적으로 출원되었으며, 구체적인 감청장비 제작은 공식적으로 없는 것으로 알려져 있음. 개정 법안이 통과될 경우 기지국 이동교환기에 감청설비를 설치해 특정번호를 입력, 이 번호로 송수신되는 모든 통화내역을 녹음하는 방식으로 수행되는 별도의 소프트웨어나 카드가 개발될 것으로 예상됨

지금까지는 도청 및 감청에 대한 법적 소고 및 인문사회학적 의미에서의 도청의 법적 규제에 관한 고찰과 같은 작업이 주로 이루짐. 최근 VoIP와 같은 IP 기반의 통신이 일반화 되면서 통신 채널에서의 "Wiretapping 또는 Electronic Surveillance" 라는 공학적 의미의 연구가 진행되고 있음. 국내의 경우 그동안 "합법적 감청"이라는 연구 주제보다는 "IP Telephony Networks 보안"와 같이 좀 더 광범위한 해석을 바탕으로 연구자들의 참여가 있었던 것으로 보임

나) 평가인증

• 정보보호 평가

1998년 우리나라 고유 평가기준인 K-기준에 기반한 정보보호시스템 평가는 정보보호시스템 공통평가기준(ISO 15408) 제정과 세부 평가절차를 명시한 정보보호시스템 평가 · 인증 지침(2002.8)을 개정 고시하면서 국제 수준의 평가제도로 도약하기 위한 기반을 마련함. ISO는 공통평가기준 버전 2.3을 3.1로 대체하였으며 국제 공통평가기준 상호인정협정(CCRA)에서는 2008년 4월부터 공통평가기준 버전 3.1의 사용을 강제한다는 정책을 수립하여 추진 중에 있음

정보보호시스템 평가대상은 1998년 침입차단시스템, 2000년 침입탐지시스템을 시작으로 가상사설망, 운영체제보안시스템 등으로 확대해 오다 2005년에는 정보보호기능이 구현된 모든 IT 제품으로 그 대상을 확대함

〈표 15〉 평가기준 및 평가대상 제품군 확대 연혁

평가기준	연도	평가대상 제품군 확대
K-기준	1998. 2	침입차단시스템
	2000. 7	침입탐지시스템
CC	2002. 8	가상사설망
	2003. 11	운영체제보안시스템, 지문인식시스템, 스마트카드
	2004. 10	침입방지시스템
	2005. 5	모든 정보보호제품군으로 확대

업체의 평가제출물 작성 지원을 위하여 보호프로파일 및 보안목표명세서 작성 가이드(ISO 15446)에 기반한 제품별 세부 평가기준인 보호프로파일을 개발하여 공고하고 있음. 현재까지 한국정보보호진흥원이 11개를 국가보안기술연구소가 3개의 보호프로파일을 개발하는 등 총 14개의 보호프로파일이 개발됨. 2007년 현재 전자여권, 하드웨어 토큰, 웹 방화벽, 어플리케이션 보안 등 4개 보호프로파일을 개발 중에 있으며 공통평가기준 버전 2.3이 3.1로 대체됨에 따라 기존의 14개 보호프로파일을 버전 3.1 기반으로 개정 작업 중에 있음

〈표 16〉 개발 보호프로파일 내역

보호프로파일명	최초등재일	개발 주체
국가기관용 게이트웨이형 가상사설망 보호프로파일 V1.1	2003. 4	NSRI
국가기관용 침입탐지시스템 보호프로파일 V1.2		KISA
국가기관용 가상사설망 보호프로파일 V1.2		
국가기관용 침입차단시스템 보호프로파일 V1.2		
국가기관용 지문인식시스템 보호프로파일 V1.1	2004. 2	
국가기관용 등급기반 접근통제시스템 보호프로파일 V1.1		
국가기관용 침입차단시스템 · 가상사설망 통합 보호프로파일 V1.1		
국가기관용 개방형 스마트카드 플랫폼 보호프로파일 V1.1	2004.12	
네트워크 침입방지시스템(IPS) 보호프로파일 V1.1	2005. 5	
역할기반 접근통제시스템 보호프로파일 V1.0	2006. 3	
안티 바이러스 소프트웨어 보호프로파일 V1.0	2007. 1	
네트워크 스팸메일차단시스템 보호프로파일 V1.0		
통합보안관리시스템 보호프로파일 V1.0		NSRI
무선랜 인증시스템 보호프로파일 V1.0		
웹 방화벽	개발중	
어플리케이션 보안		
전자여권		KISA
하드웨어 토큰		

평가제도를 운영하기 시작한 이래 현재 년 25개 이상의 제품을 평가하고 있으며 현재까지 145개의 제품을 평가하

였음. 또한 우리나라에서 평가한 결과가 해외에서도 인정받을 수 있도록 2004년 9월 국제 공통평가기준 상호인정협정 가입 신청서를 제출하였으며 20개월만인 2006년 5월 9일 11번째 인증서발행국으로 가입함. 따라서, 국내 업체가 우리나라에서 평가받으면 국제 공통평가기준 상호인정협정의 24개 회원국에서 동일한 효력을 가질 수 있으며 평가받은 제품의 사용이 회원국에서 강제 또는 권고됨에 따라 국산 제품의 해외진출을 위한 국제 경쟁력이 높아졌음. 더불어 국내 업체가 해외에서 평가받기 위한 수수료 및 제출물의 번역 등 예산을 절감할 수 있으며 업체의 기술이 해외 유출로부터 보호할 수 있음

〈표 17〉 평가완료 현황('04년부터 ' 07년7월까지)

구분	2004	2005	2006	2007	합계
침입차단시스템	7	2	-	4	13
침입탐지시스템	2	6	6	4	18
통합제품	11	3	4		18
운영체제보안시스템	-	10	5	1	16
침입방지시스템	-	2	3	5	10
기타 정보보호제품		2	2	1	5
보호프로파일	-	1	5	-	6
합계	20	26	25	15	86

※ 통합제품 : "침입차단시스템+가상사설망", "침입차단시스템+가상사설망+침입탐지시스템", "침입차단시스템+침입탐지시스템", "침입차단시스템+가상사설망+침입방지시스템" 형태의 통합제품
※ 기타 정보보호제품 : 가상사설망, 지문인식시스템, 스마트카드, 통합보안관리, 웹 보안, 안티바이러스 제품

2006년 1월 우리나라는 국가/공공기관에 납품되는 모든 정보보호제품에 대한 평가를 강제화하여 평가신청이 급증하여 2007년 8월 현재 41개 제품이 평가대기 중이며 평균 대기기간이 7.1개월에 달함. 따라서 평가적체해소를 위한 대책으로 우리나라 유일한 평가기관인 한국정보보호진흥원 외에 평가기관을 추가 지정한다는 정책을 수립하였으며 이를 위한 정보화촉진기본법 시행령 개정(2007년 8월 예정)을 추진 중에 있음. 추가 지정되는 평가기관은 한국기술시험원과 한국시스템보증 2개 회사가 평가기관 신청을 한 상태임

평가적체 해소를 위하여 단일사 유사한 제품을 일괄 평가신청하고, 국내용과 국제용으로 평가신청을 분리하여 평가기간을 단축시킬 수 있도록 제도를 개선하였음. 일괄평가는 하드웨어 사양 또는 운영체제의 버전의 변경이 미비한 제품을 단일 제품으로 평가신청하던 것을 일관적으로 평가신청하여 문서 평가는 1개로하되 시험 및 취약성 평가만을 분리함으로써 평가기간을 단축시키는 방안임. 국제용 평가는 해외 시장을 겨냥하여 평가신청하는 경우로써, CCRA에서 요구하는 수준의 평가산출물 및 결과물이 요구되나 국내용은 국내 시장을 타겟으로 함으로써 평가산출물 및 결과물에 대한 수준을 대폭 감소시켜 평가기간을 단축시키는 방안임

하지만, 신규 평가기관이 정착되고 평가자를 확보하여 정상적으로 운영되어 평가적체 해소에 기여하기에는 향후 몇 년이 소요될 것으로 분석됨

• 보안 관리

국내 환경에 적합한 정보보호관리 모델을 개발 · 보급하기 위해서 국내 정보보호관리체계 인증제도에 대한 연구를 2000년부터 진행하여 관련 법률(2001.7)을 개정, 인증심사기준을 고시(2002.5)하였고, 세부 심사기준 및 업무지침 등을 마련하여 2005년 11월부터 인증제도를 본격 시행하였고 위험분석 방법론 개발, 정보보호관리체계 수립 가이드 등을 개발 · 배포하고 있음. 유사 제도인 ISO27001(예전 BS7799)의 기준을 모두 포괄하고 있을 뿐만 아니라 문서 중심이 아닌 기술적 관점으로 구성되어 있는 등 우수성을 인정받고 있지만, 최근 IT 환경의 급속한 환경 변화 개인정보보호 등 신규 이슈 등 기존 정보보호 패러다임이 정보보호관리 관점에서 정보보호 거버넌스로 변화되고 있는 추세이므로 이에 따른 체계적인 정보보호 거버넌스 연구가 필요하나, 국내의 선행 연구 등의 노력이 부족한 실정임

■ 국내 특허출원 현황 및 전망

가) 응용보안

• 전자우편

전자우편 관련 출원건수는 꾸준한 증가세를 나타내고 있는 가운데, 초기에는 응용에 관한 기술과 사용의 편의성 증대 및 멀티미디어 메일 관련 특허 기술이 주를 이루고 있으며, 전자우편 보안관련 특허가 그 뒤를 따르고 있음. 이후 전자우편의 꾸준한 이용증가에 따라 다양한 역기능 방지 기술들이 출원됨. 스팸메일 차단에 관한 특허출원이 지속적으로 증가하고 있으며, 기존의 해킹과 바이러스의 경계가 무너지고 각종 웜 바이러스가 고도화 · 지능화되어 기승을 부리면서, 바이러스 관련 기술과 함께 전자우편 기술이 출원되고 있음

• 전자투표/공증

전자투표 관련 특허는 1997년부터 약 120여건이 국내에 출원 · 등록되어있음. 인터넷, 전자우편, 디지털 텔레비전 등의 미디어를 이용하는 방법, 사용자 인증, 전자 개 · 검표, 계수 및 기록 방법 등에 관한 내용이 주를 이루고 있음. 현재 전자투표의 이용이 옵티컬 스캔이나 터치스크린을 통한 독립적 투표기기에 직접 기록하고 취합되는 보안 측면에서 안전한 형태의 전자투표가 대부분이나 점차 유선 및 무선(휴대폰 등의 단말)을 포함하는 전자투표에 관한 특허로의 발전이 예상됨

• o u-지식 보안

한국 출원인인 SAMSUNG이 스트리밍/다운로드 콘텐츠 복제방지기술 분야에서 가장 많은 출원건을 보유하고 있으며, ETRI는 u-지식 보안 관련 다양한 분야에 걸친 특허출원이 이루어지고 있음. 콘텐츠 저작권 보호 툴킷에 대한 일부 특허는 있으나, 참여 저작자들의 지분표현 등 프로슈머형 지식 관련 특허는 없는 것으로 파악되어, 이 분야에서의 핵심 IPR 확보가 필요할 것임. 세부 기술별로 익명성 기반 u-지식 보안 기술 분야 기술 혁신 리더를 살펴보면 한국과 미국에서 주요 출원인들의 일치하는 부분이 거의 없음을 알 수 있음

• 쉘 보안

무선 환경을 고려한 쉘 보안 등 일부 특허가 존재하나 매우 적은 특허가 출원되었음. 쉘 보안 분야의 특허는 미국을 제외하고는 관련 특허 출원 실적이 비교적 적은 상황이므로, 쉘 보안기술의 응용 기술 등 다양한 형태의 개량 및

우회 특허 추진이 충분히 가능할 것으로 보임

• VoIP 보안

VoIP 관련 국내 특허는 1999년부터 증가하기 시작하여 약 800여건이 등록되어 있음. 이러한 특허 동향은 VoIP 관련 기술의 개발이 외국에 비해 늦었음을 의미함. 국내 특허는 주로 채팅서비스, 컨퍼런스폰 시스템 등 VoIP 응용 분야의 출원이 많이 되고 있는 것으로 조사됨

• 스팸대책

스팸과 관련하여 약 350여건의 특허가 등록되어 있으며, 이 중 대부분은 이메일 스팸 또는 휴대폰 스팸과 관련된 기술임

• 응용보안 강화 프로토콜

신뢰적인 제 3기관을 통한 보안 프로토콜, 이동 통신 시스템에서의 패스워드 인증 관련 특허 등 약 50여개 이상의 특허가 출원됨. 현재 국외의 경우 패스워드 인증에 대한 다양한 형태의 특허가 다수 출원되고 있는 상황이므로. 기술 개발을 통한 응용 특허 또는 기존 특허에 대한 우회특허 또는 개량 특허의 도출을 통한 IPR 확보가 요구됨

• 안전한 P2P 보안

P2P 관련 국내특허는 현재까지 30여 건이 등록되었으며, 국내 P2P 응용 서비스 이용 규모에 비해서 특허 건수는 상대적으로 적은 편임. 현재 출원/등록된 주요 P2P 보안기술 관련 국내특허는 아래와 같음

- 네트워크의 유해 P2P 트래픽 선별 차단 방법 및 장치 (ETRI)
- 네트워크의 유해 P2P 트래픽 선별 차단 방법 및 장치 (ETRI)
- P2P 트래픽 분류 시스템 및 그 분류 방법 (ETRI)
- P2P 유해 정보 차단 시스템 및 방법 (아라기술)
- 보안이 유지되고 액세스 제어된 P2P 자원 공유 방법 및 장치 (IBM)
- 피어-투-피어 환경에서의 네트워크 트래픽 제어 (IBM)

• IPTV 보안

IPTV 보안 관련 기술은 고용량의 스트림 데이터 전송(VoD), 음성(VoIP), 데이터(Internet), 그리고 다양한 부가서비스를 핵심 요소로 하고 있어, 네트워크, 시스템, 응용 보안 기술이 광범위하게 포함되는 분야임

인터넷 방송 (IPTV, 인터넷TV 등)과 관련하여 국내에서 출원된 특허는 약 600건에 달하며 이중 한국인이 출원한 특허 는 590여건에 달함. 그리고 IPTV를 키워드로 하는 특허는 178건이었으며, 시스템(서비스) 운용상의 이유로 사용자 인증을 포함하는 경우는 있지만, 직접적으로 IPTV 보안을 위한 식별, 인증, 과금, 접근제어와 관련된 특허는 전무함

IPTV 네트워크와 관련된 특허는 10여건으로 홈네트워크에서의 서비스 운용과 관련된 특허가 주를 이루고 있음

IPTV의 주요 코딩 기법인 H.264/MPEG-4 AVC와 관련된 특허는 160여건으로 대부분 스트림 처리 또는 운용 방법에 관한 것이며, 암호화/복호화 관련 특허는 없는 것으로 조사됨

국내에서 출원된 DRM 관련 특허는 총 280여 건에 달하며 이중 120여 건(한국인 출원수: 90건)이 영상 데이터 관

련 특허로 IPTV용 DRM 기술과 직접적으로 관련이 있으며, CAS 관련 특허의 총 수는 137여 건인데 반해 한국인 출원 수는 70여 건으로 나타나 DRM에 비해 그 수가 상대적으로 적은 것으로 조사됨

• STC (Secure TC)

STC 기술과 관련한 국내외 특허들은 암호기술, 인증기술, 키 관리기술, 하드웨어 및 소프트웨어 기술들을 포함하여 1600건 정도에 달함. 현재 국내에서 STC와 관련되어 등록 또는 출원되어 있는 주요 특허는 10건 넘게 되지만, 7건 정도는 후지쯔, MS 등 국외 대형 업체임. ETRI에서는 2006년 STC 관련 과제를 진행하면서 출원한 특허들이 다수 개 있음

〈표 18〉 국내 주요 등록 특허

대분류	세부 분류	출원 번호	출원 일자	등록 번호	공고 일자	출원인	발명의 명칭	진행 상태	비고
STCf	서명	20070007021				IBM	컴퓨터 프로그램 소자, 컴퓨터 프로그램 매체, 사용자입증 - 서명 값 생성용 입증 값 발행 방법 및 시스템		
	Boot	2005-0110058				MS	하드웨어 보안 모듈을 구비한 컴퓨터를 보안 부팅하기 위한 시스템, 방법 및 컴퓨터 판독 가능 매체		
	Boot	20060047897				MS	상태 검증을 사용하여 보호된 오퍼레이팅 시스템 부팅을 위한 시스템 및 방법		
	Device	20047014195				프리시젼	식별 장치		
	Physical presence	20050123152				IBM	신뢰할 수 있는 플랫폼에서의 물리적 존재 판정 방법		
	Tamper-proof	2004-7018757				톰슨	키 전송 탬퍼 보호		
		2006-0095007				ETRI	LED를 가지는 RFID 태그		
		2006-0102249				ETRI	센서 신호 처리 및 응용 장치		
		2006-0059845				ETRI	임베디드 시스템용 저전력 AES 암호 장치 및 방법		
		2006-0120732				ETRI	효율적인 모듈러 곱셈 장치 및 방법		
		2006-0120697				ETRI	효율적인 TPM 명령어 처리 방법		
		2006-0120344				ETRI	TPM의 PCR을 이용한 원격 인증 방법		
		2006-0120455				ETRI	보안 모듈을 이용한 네트워크 서비스 보안 개선 방법		
		2006-0120840				ETRI	플랫폼 무결성 정보를 이용한 안전한 네트워크 인증 장치 및 방법		
		2006-0120783				ETRI	TPM을 사용한 모바일 플랫폼의 안전한 부팅 방법		
		2006-0096571				ETRI	컴퓨팅 플랫폼의 설정 정보를 은닉하면서 무결성 보증을 제공하는 방법		
		2006-0120453				ETRI	신뢰 컴퓨팅 환경에서 각 참여자 상호 보증 기능을 갖는 인터넷 전자투표		
총 계		13 건							

• 차세대 웹 보안

현재까지 웹 및 웹서비스와 관련하여 다수의 특허가 출원되었지만, 보안과 관련한 특허는 그 수가 극히 적다고 볼 수 있음. 현재까지의 주요 특허 목록은 아래와 같음. (2007. 9 기준)

〈표 19〉 웹 정보보호 관련 주요 특허

대분류	세부 분류	출원 번호	출원 일자	등록 번호	공고 일자	출원인	발명의 명칭	진행 상태	비고
웹서비스 (Web Services)	보안	10-2004-0064371	2004-08-16	10-0622086-0000	2006-09-13	한국신용정보 주식회사	개인 식별을 위한 인증키 제공 시스템 및 방법	등록	
		10-2004-0059560	2004-07-29	10-0690452-0000	2007-03-09	연세대학교 산학협력단	웹서비스 기반 의료정보의 보안 접근제어 시스템	등록	
		10-2003-0070551	2003-10-10	10-0549504-0000	2006-01-27	ETRI	서명 암호화를 이용한 웹서비스 보안에서의 SOAP 메시지 생성 및 검증 방법	등록	
		10-2002-0059178	2002-09-28	10-0566634-0000	2006-03-24	주식회사 케이티	웹서비스를 이용한 우편번호 제공 시스템 및 그 방법	등록	
웹 2.0	웹 2.0 보안	10-2003-0076785	2003-10-31	10-0562357-0000	2006.03.20	(주)와이즈그램	블로그 서비스 제공 시스템 및 블로그 서비스 제공 방법	등록	
		10-2004-0042145	2004-06-09	10-0462158-0000	2004-12-16	엔에이치엔(주)	익명의 메시지 전달 방법	등록	
		10-2006-0018059	2006-02-24	10-2007-0087999(공개)	2007-08-29	(주)뱅크타운	미니홈피 또는 블로그 뱅킹 서비스	공개	
시맨틱 웹	시맨틱 웹 기반 서비스	10-2007-0015735	2007-02-15	10-0751292-0000	2007-08-23	(주)헤리트	시맨틱 웹 기반의 서비스 제공 방법	등록	
		10-2004-0040077	2004-06-02	10-0704285-0000	2007-04-10	인하대학교	자원 디스크립션 프레임워크를 사용하여 제품 데이터온톨로지를 구성하는 장치 및 방법	등록	
웹 프라이버시	프라이버시 보호	10-1998-0016142	2000-05-06	10-0263894-0000	2000-08-16	삼성전자	홈 네트워크 시스템에서의 사용자 액세스 제한 방법	등록	
		10-2004-0109131	2004-12-21	10-0599937-0000	2006-07-13	ETRI	인터넷 개인정보 관리 및 보호 시스템 및 방법	등록	
		10-2004-0061672	2004-08-05	10-0609701-0000	2006-08-09	ETRI	전자 거래 내역에 대한 프라이버시를 보호하는 거래 인증방법 및 시스템	등록	
유비쿼터스 웹	웹서비스	10-2004-0098002	2004-11-26	10-0653266-0000	2006-12-01	삼성SDS	홈네트워크 디바이스의 제어장치 및 사용자 인터페이스 생성 방법	등록	
		10-2005-0096200	2005-10-12	10-0694155-0000	2007-03-12	삼성전자	웹서비스를 통해 홈 네트워크 기기의 서비스를 홈 네트워크 외부에 제공하는 방법 및 장치	등록	
		10-2005-0007247	2005-01-26	10-0657793-0000	2006-12-14	삼성SDS	홈 네트워크 디바이스의 제어 방법 및 장치	등록	
총 계		15 건							

- 웹서비스 보안과 관련한 특허는 웹서비스에 대한 연구와 도입이 상당히 진행된 만큼, 다수의 특허가 출원되었음. 현재까지 284건의 관련 특허가 제출되었으나, 90여건 정도만 등록되었음. 웹서비스 보안에 대한 특허는 기존의 네트워크 서비스에 웹서비스를 도입하려는 과정에서 발생하는 보안 문제를 해결하기 위한 목적으로 제출된 다수이며, 각 서비스의 특성에 맞는 보안 적용 방법에 대한 특허를 제출함
- 웹 2.0과 관련하여 검색 결과 90여건 정도의 관련 특허가 일부 등록되어 있으나, 웹 2.0 보안과 관련한 특허는 현재까지 등록 현황이 미비함. 웹 2.0 보안과 관련한 특허는 블로그 정보 보호 방법, 커뮤니티내에서의 메시지 전달 및 보호 방법 등과 같이 서비스 특징적인 것들이 대다수임. 웹 2.0 보안과 관련한 특허는 NHN, SK 텔레콤과 같

이 블로그, 미니홈피 등과 같은 웹 2.0을 서비스하는 업체들이 주도하고 있음. 하지만, 국내 웹 2.0의 서비스 발전 현황과 비추어 보았을 때, 보안 특허는 매우 미비하다고 할 수 있음

- 시맨틱 웹 및 시맨틱 웹서비스와 관련한 보안 특허는 현재까지 찾아 볼 수 없음. 시맨틱 웹과 관련한 특허 또한 서비스 제공을 위한 기반 구조에 대한 특허가 대부분임. 국내 시맨틱 웹의 도입 및 발전 현황에 비추어 보았을 때, 보안 관련 특허가 등록되기 까지는 상당한 시일이 소요될 것으로 판단됨
- 웹 2.0과 웹서비스의 발전으로 프라이버시 보호에 대한 요구가 상당히 커짐. 현재까지의 특허 등록 현황으로 보았을 때, 아직까지는 연구소에서 기반 기술을 연구하는 단계임. 프라이버시 보호의 중요성이 증대됨에 따라 웹 또는 웹서비스에서의 프라이버시 보호 관련 특허 등록이 늘어날 가능성이 있음
- 홈네트워크, 유비쿼터스 컴퓨팅 등의 발전과 더불어 웹 기술이 디바이스 환경에까지 적용되고 있음. 삼성전자 및 삼성SDS와 같은 대기업을 중심으로 유비쿼터스 웹에 대한 개념을 정리하고 있는 단계로 파악됨. 현재까지 등록된 특허는 홈네트워크를 기반으로 하는 디바이스 웹 또는 웹서비스의 서비스 구조에 대한 것이 대부분임. 하지만, 각 특허 내용에서 보안의 중요성에 대해서 언급하고 있으며, 일부 보안 서비스의 개념을 제시하였음

• Lawful Interception

합법적 감청과 도청은 기술에 있어 도청과 합법적 감청은 동일한 것을 판단되고 있으며, 단 출원서 상의 기재로 보아 사용용도가 도청일 경우, 특허법 제32조에 의거 공공의 질서를 문란하게 하는 기술(도청 기술)은 특허 받을 수 없도록 되어 있음. 1990년 이후 2005년 8월까지 통신 감청장비 관련 특허는 총 35건이 출원되었고 그 중 13건이 등록됨 (2007.8)

2005년까지의 등록기술은 무선구간이 아닌 교환기(유선구간)에서 일반 전화기 또는 휴대폰 통화를 감청할 수 있는 기술임. 그러나 2006년부터 휴대폰 단말기를 무선구간에서 직접 감청하는 특허기술의 출원 및 등록 사례가 등장하기 시작함

- 국내업체의 감청기술 특허출원 · 등록과 도 · 감청 실시여부
  - ◦ 국내업체는 교환기(유선구간)에서의 감청기술을 특허출원 하였으며 이에 대한 실시가 가능하여 등록된 것임
- 교환기(유선구간)에서 제3자가 불법적 감청 여부
  - ◦ 특허등록 된 감청기술이라도 통신비밀보호법에 의해 허가받은 자가 정식절차에 의하여 통제된 장소 내에서만 감청할 수 있음. 따라서 기술적 활용의 적법성 여부는 사법기관의 판단 사항임
- 감청 관련 특허 출원 · 등록 기술공개 여부
  - ◦ 특허법에 의해 모든 특허는 출원 1년 6개월이 지나면 공개하고 특허등록 된 기술은 등록공보를 통해 별도의 조치 없이 공개
  - ◦ 출원공개 · 등록공보는 법률로 규정하고 있으며 정통부, 국정원 등 타 기관과 협의하지 않음
- 감청 관련 특허의 불법적인 도청에 활용될 여지
  - ◦ 특허등록 된 교환기(유선구간) 감청기술은 모두 통신사업자가 통신망의 운용 및 가입자 관리를 목적으로 하는 것임

- 휴대폰의 불법도청 방지기술의 특허 출원현황
  - 휴대폰 도청방지 기술은 크게 시스템 보안방식인 '코드암호화 및 인증' 기술과 가입자 보안방식인 '음성비화' 기술이 출원됨('90년 ~ '05년 79건)
- 국내 주요 등록 특허
  - 합법적 감청을 주요 내용으로 다룬 등록 특허만을 선별함
  - 2005. 8월까지의 등록현황을 기준으로 함
  - 통신비밀보호법 개정안 통과가 예상되고 있으며, 또한 다양한 휴대 이동 단말의 사용이 이미 성숙기에 접어든 만큼, 이와 관련된 감청 및 도청 특허가 출원이 폭등할 것으로 예상됨

〈표 3〉 Lawful interception 관련 국내 특허 현황

대분류	세부 분류	출원 번호	출원 일자	등록 번호	공고 일자	출원인	발명의 명칭	진행 상태	비고
교환기 분야	유선망 교환기	10-1992-0012578	1992-07-15	특허 0116201	1997-03-08	(주)LG	전전자교환기 가입자 전화기의 감청시험방법	등록	
		10-1993-0030058	1993-12-27	특허 0136390	1998-06-01	(주)LG	전전자 교환기에서의 가입자 전화기 감청시험방법 및 그 장치	등록	
		10-1995-0069204	1995-12-30	특허 0195062	1999-06-15	(주)대우	전전자 교환기를 이용한 지정번호 감청 장치 및 그 방법	등록	
		10-1996-0033010	1996-08-08	특허 0233490	1999-12-01	(주)대우	전전자교환기에서 지역 가입자의 착신 감청서비스장치 및 방법	등록	
		10-1996-0033011	1996-08-08	특허 0215970	1999-08-16	(주)대우	전전자교환기에서 지역 가입자의 발신 감청서비스장치 및 방법	등록	
		10-1996-0033012	1996-08-08	특허 0215971	1999-08-16	(주)대우	전전자교환기에서 타지역간 가입자의 감청서비스방법	등록	
		10-1996-0042624	1996-09-25	특허 0210763	1999-07-15	(주)대우	국설 전전자 교환기에서의 안내대 감청 제어장치및 방법	등록	
		10-1997-0009465	1997-03-20	특허 0222414	1999-10-01	(주)삼성	가입자 감시/감청 동시 수행방법	등록	
		10-2000-0061343	2000-10-18	특허 0435782	2004-06-12	(주)LG	사설 교환기 가입자의 정보 및 음성 감청장치	등록	
	이동망 교환기	10-1999-0015971	1999-05-04	특허 0318965	2002-01-04	(주)삼성	교환기 시스템에서 가입자의 감시와 감청을 위한 시스템 및 방법	등록	
		10-1999-0017874	1999-05-18	특허 0320422	2002-01-16	(주)LG	통신망에서의 특정 번호의 호에 대한 감청 방법	등록	
	기타 교환기 (위성.데이터)								
일반 전화기 분야	유선 방식	20-1999-0014942	1999-07-24	실용신안 0164775	2000-02-15		시그널 방식 전화 감청 녹음장치	등록	음성 녹음기
	무선 방식	10-1994-0031675	1994-11-29	특허 0121964	1997-11-19	(주)대우	단말기의 음성 신호를 감청하는 방법	등록	유럽 방식
휴대폰 무선 분야	휴대폰								
총 계		13 건							

2.2.2. 국외 기술개발 현황 및 전망

■ 주요국가의 정책기조

- EU IST에서는 2010년 이후의 정보보호 중점 연구 방향으로, 디지털 사회의 취약성 및 위협 대응; 디지털 프라이버시; 객관적, 자동화된 정보보호 기반; 디지털 세계에서 기술 간의 융합에 따른 새로운 정보보호 이슈; 등 4대 중장기 과제를 주요 연구방향으로 제시하였음. ("정보보호 미래연구 전략 2010 (ICT Security & Dependability Research beyond 2010: Final Strategy)" 참고) 이는 2015년까지 디지털 컨버전스의 확장 및 글로벌화에 따른 정보보호 문제에 대한 기술적, 계량적, 공학적 발전을 시도한 것으로, 개인적 차원에서의 정보보호 뿐만 아니라 사회 전체의 보안에 대한 대책을 수립하고자 한 것임

■ 국외 기술개발 현황 및 전망

가) 응용보안

- 전자우편

  전자우편 보안 제품은 기본적인 암호 서비스로 메시지 암호화와 디지털 서명을 제공하는 제품에서부터 여러 형태로 보안 기능을 강화시킨 제품들이 발표되고 있음. 암호 기술을 응용한 기능들 중에서는 기본 기능인 메시지 기밀성, 송신자 인증, 메시지 무결성 외에도 부인방지, 발신 사실 증명, 보안 메일링 리스트, 도메인 보안 서비스 등이 있음. 그리고, 비암호 보안 기능인 스팸 메일 방지 기능과 바이러스 방지/검색 기능도 현재의 전자우편에서는 아주 중요한 보안 기능이지만, 이들 서비스에 관련된 기술은 개별 소프트웨어의 기능이며 표준과 관련된 의미는 갖지 않음. 부인봉쇄는 송신자 부인봉쇄와 수신자 부인봉쇄로 나누어지는데, 송신자 부인봉쇄는 공개키 기반구조와 디지털 서명으로 이루어지며, 수신자 부인봉쇄는 수신자로 하여금 수신된 메시지에 대해 서명된 영수증을 발행하도록 함으로써 달성됨. 발신 사실 증명은 신뢰할 수 있는 제3의 기관을 통해 메시지를 전달함으로써 달성될 수 있음. 보안 메일링 리스트는 메일링 리스트를 통해 암호화된 메시지를 제공할 수 있게끔 하자는 기능이며, 이는 전자우편에서 일반적으로 사용되는 암호화 서비스가 수신자의 공개키를 필요로 하는데, 메일링 리스트 가입자들의 경우 최종 수신자가 메시지 송신자에게 알려지지 않는 경우가 많기 때문에 별도의 메커니즘을 필요로 함. S/MIME 버전 3에서는 보안 메일링 리스트를 하나의 사용자로 간주하여 공개키를 갖게 하고, 보안 메일링 리스트로 하여금 수신된 암호 메시지를 복호화하고 다시 개별 수신자들을 위해 다시 암호화해서 전달하는 방법을 제안하고 있음. 도메인 보안 서비스는 암호화와 디지털 서명을 개별 사용자를 대신하여 도메인 수준의 메일 게이트웨이나 관리 에이전트가 수행하자는 방안임

- 전자투표/공증

  전자투표는 이미 외국의 여러 나라에서 다양한 형태의 투표로 실행되고 있음. 미국에서는 2000년 3월 Arizona주 민주당 예비선거에서는 전통적인 투표소에서 투표용지에 기입하는 방법, 투표소에서 전산투표방식, 우편을 통한 부재자 투표방식 그리고 원거리 인터넷 투표방식 등 4가지 투표방식을 사용하였는데 전체 투표자의 40% 이상이 원거리 인터넷 투표를 하였음. 캘리포니아 주정부에서는 2008년 대통령 예비선거에서 전자투표를 사용하기로 하

고 현재 보안 취약점을 점검 중에 있음. 최근에 발견된 보안 취약점으로는 전자투표 관리시스템에서 사용된 윈도우 OS에서 시스템 로그 기록 방해, 펌웨어에 덮어쓰기, 시스템 록 통과, 서버에 무선기기의 은밀한 설치 등 15가지에 이르고 있으나 이런 문제점들의 개선을 통해 안전한 전자투표 시스템 구축에 노력하고 있음. 일본의 경우 2002년 6월 23일 오카야마현 니미시의 지방선거에 최초로 전자투표가 도입됨. 시내 43곳에 113대의 투표기를 설치하여 부재자 투표를 제외한 전체 선거를 전자투표 방식으로 진행하였는데 1만5천명의 시민이 투표에 참여하였고 과거 4시간 정도 걸리던 개표 시간이 25분만에 완료되었으며 무효표가 단 한 표도 발생하기 않았음. 이에 따라 일본 정부는 전자투표 시스템 구축을 본격적으로 추진 중에 있음

전자투표의 성공적인 도입을 위해서는 무엇보다 보안 문제가 우선적으로 해결되어야 함. 전자투표가 해킹이나 바이러스 공격을 견뎌낼 수 있을 정도로 안전해야 하며, 유권자의 컴퓨터를 떠난 데이터는 서버까지 안전하게 배달되어야 하고 개인 단말기, 네트워크 그리고 서버 차원의 보안까지 완벽해야함. 한편 전자투표시스템은 투 · 개표의 조작 가능성을 파악하여 전송과정에서 조작을 목적으로 공격을 방어할 수 있어야 하고 투표 및 개표의 모든 과정에 대한 객관적인 외부감사가 가능해야 함. 결국 전자투표의 모든 과정은 투명하게 공개되어야 하고 외부의 공격까지도 막아낼 수 있는 보안시스템을 구축해야 함. 투표의 결과는 한 치의 오차도 없이 정확히 계산되어야 하고 컴퓨터나 전자기기에 대한 일반적 상식을 가진 유권자라면 누구나 사용할 수 있을 정도로 쉬워야 함. 외부로부터 선거에 대한 의문이나 요청이 있을 경우, 언제든지 재검표 할 수 있어야 하고 자료로서의 보전 및 재생 또한 가능해야 하기 때문에 전자투표는 보안 이론상 매우 어려운 분야로 간주되고 있음

• o u-지식 보안

음악 재생용 MP3를 콘텐츠 판매와 보호로 세계적인 제품으로 자리 잡은 애플의 iPod는 하나의 디바이스에서만 재생을 허용하는 중심의 권한 관리 방식이 아닌 사용자 도메인 내에서는 지식의 이동을 자유롭게 허용하는 Non-DRM 방식(Protected Contents 개념)의 지식을 제공하여 큰 성공을 거두고 있음. 또한 일부 콘텐츠 제공자(EMI 등)들은 DRM이 적용되지 않은 콘텐츠 제공을 선언함으로써 u-지식 보안 기술에 있어 새로운 전환점이 필요할 것임. 또한 방송콘텐츠 보호에 사용되던 CAS 역시 기존의 HW(케이블카드 및 셋탑) 중심에서 SW 형태로 다운로드하여 단말 트러스트를 제공하는 지식 보안 기술이 미국의 오픈케이블랩 중심으로 개발 중임

• 쉘 보안

쉘 보안은 IETF에서 표준화와 더불어 기술 개발을 진행하고 있음. IETF에서는 쉘 보안을 위해 SSH 프로토콜을 개선하고 표준화하기 위한 작업을 진행하고 있음. SSH 프로토콜은 안전한 원격 로긴, 안전한 파일 전송, 안전한 TCP/IP와 X11 전달을 지원하는 프로토콜임. 쉘 보안 기술은 이미 성숙기에 이른 기술이며, 현재 다음과 같은 요구사항을 충족시키는 형태의 기술개발이 진행 중임

- 암호해독, 프로토콜 공격 등에 강한 보안성 제공
- 글로벌 키 관리나 certificate infrastructure 없이도 잘 동작하는 구조 제공
- DNSSEC, SPKI, X.609와 같은 현존하는 certificate infrastructure와 통합하는 경우 호환성 제공
- 탑재 용이성, 구현 용이성 제공
- SSH 동작을 위한 사용자의 수동 작업 최소화

산업체에서는 RSA Security사에서 SSH2와 RSASecurID 솔루션을 통합한 제품을 개발하였고, SSH 커뮤니케이션스 시큐리티사, 마이크로소프트, 썬마이크로시스템즈와 같은 주요 소프트웨어 업체에서도 관련 제품을 개발하고 있으며, 현재 SSH Secure Shell은 정부 조직, 민간 조직, 기업, 금융기관 등에서 안전한 원격접속을 위해 일부 사용되고 있음

• VoIP 보안

VoIP와 관련된 기술개발은 크게 암호화 및 키관리 기술, 스팸 대응 기술, 보안 세션 제어 및 사용자 프라이버시 보호 기술로 분류할 수 있으며, 각 분야별 국외 기술 개발 현황은 다음과 같음

- VoIP 데이터 보호를 위한 암호 및 키관리 기술

  VoIP 데이터 보호를 위한 암호 및 키관리 기술은 표준화를 중심으로 개발

  ◦ SIP(Session Initiation Protocol, RFC 3261)

- 세션 설정 과정에서의 관련 데이터를 보호하기 위해 HTTP(Hypertext Transfer Protocol), TLS(Transport Layer Security), S/MIME(Secure/Multipurpose Internet Mail) 등 기존의 보안 메커니즘을 적용

  ◦ SRTP(Secure RTP, RFC 3711)

- VoIP 미디어 스트림의 기밀성을 보장하기 위한 IETF(Internet Engineering Task Force) 표준 프로토콜로, H.235와 SIP 기반 VoIP 음성정보를 전달하는 RTP/RTCP[5]에 대한 암호화 기술로 적용

  ◦ MIKEY(Multimedia Internet KEYing, RFC3830)

- 기존의 키 관리 프로토콜인 IKE(Internet Key Exchange), TLS 등이 멀티미디어 트래픽에 적용하기 부적합한 문제점을 해결하기 위해 제안되었으며, VoIP에서 멀티미디어 세션을 위한 키관리 프로토콜로 제안됨

  ◦ VoIP 관련 업체 및 사업자의 암호화 및 키관리 기술 적용 현황

- 대형 국외 장비업체들은 단말에서 SRTP 프로토콜 스택을 추가하여 출시하고 있지만, 실제 서비스에는 시그널 및 미디어 트래픽별 암호화 및 종단간 복잡한 키관리의 상호운용성 부족, 암호화로 인한 QoS 저하 등의 이유로 운용상의 실용화 문제가 존재함

- 표준에서는 VoIP 키관리 규격으로 MIKEY를 권고하고 있으며, 이에 따라 이스라엘의 대표적인 VoIP 프로토콜 툴킷 업체인 Radvision사에서 2006년도 초에 MIKEY를 지원하는 API를 출시

  ◦ 국외 VoIP 관련 업체 및 사업자들의 암호 및 키관리 기술 개발과 적용은 초기 시작단계로써, VoIP 암호 기술의 적용을 활성화하기 위해 SRTP/MIKEY 등 표준화된 기술에 대한 API 개발이 시급함

- 암호화 실용성 제고를 위해 서로 다른 키관리 기술 간에도 상호 운용성 있는 키관리 기술을 개발할 필요가 있음

- 또한 유해한 트래픽 차단을 위해서 트래픽 모니터링을 위한 기존의 키위탁(Key Escrow) 등의 기술이 보완될 필요가 있음

5) Realtime Transport Protocol/Realtime Transport Control Protocol

- VoIP 스팸 대응 기술
  - VoIP 스팸은 호 형태의 SPIT(Call Spam, Spam over Internet Telephony)과 메신저 서비스 기반의 SPIM(IM Spam, Spam over Instant Messaging), 프레즌스 서비스 기반의 Presence Spam의 종류로 나누며, 기존의 이메일 · 휴대폰 스팸 대응 기술을 벤치마킹한 대응 기술이 U. North Texas, BorderWare, Facetime, Antepo 등 학계 및 산업계 중심으로 연구 중임
  - SIP 기반의 VoIP 서비스는 아직 초기 단계로 서비스를 준비 중에 있으며, VoIP 스팸으로 인한 폐해를 최소화하기 위해 사전에 스팸 발생을 근본적으로 차단하는 방안을 망 구축단계부터 적용하는 것을 고려중임
  - 따라서 VoIP 스팸 대응은 Inbound/Outbound spam별 다단계 탐지 및 대응과 정책적 대응을 통한 차단율을 높이기 위해 경로 추적 및 사용자 간편신고 기능이 부가적으로 요구됨. 또한 현재 망 구축 단계부터 VoIP 스팸 발생을 근절할 수 있는 발신자 인증 기술이 보완되어야 함
- VoIP 보안 세션제어 기술 및 사용자 프라이버시 보호 기술
  - 국외 SBC 기술은, 다양한 환경을 경유하는 과정에서 세션을 제어하여 원활하게 서비스가 제공되도록 프로토콜 및 프로파일간의 연동(SIP/H.323/MGCP[6] 등 VoIP 프로토콜간 호환성, IPv4/IPv6 연동 등) 및 QoS 보장을 위한 트래픽 모니터링/Traffic shaping/Call admission control, NAT/FW[7] 통과문제 해결을 위한 B2BUA/B2BGK/B2BGW[8], 사용자 인증 등의 기능을 제공함
  - 현재 SBC 장비는 standalone 형태로 제공되고 있으며 일부 SBC 업체는 IMS[9] 장비 업체와 제휴를 통해 IMS 기능과 연계하여 동작하는 SBC를 제공하고 있으며, 향후 세계적인 주요업체의 IMS 장비, FW 장비, MPLS 라우터 장비에 SBC 기능을 탑재한 지능형 시스템 형태로 제공될 수 있을 것으로 일부 예상됨
  - SBC에 대한 정보보호 기능이 점차 중요하게 요구됨에 따라, 기존의 SBC 기능에 VoIP 서비스의 취약점을 악용하는 공격과 SBC 자체에 대한 공격을 막기 위한 보안기능이 탑재된 SBC 장비가 개발될 것으로 예상됨
  - 공익의 목적을 위한 Lawful Interception(LI)을 위하여 SBC에서 Call 컨텐츠와 Call 정보를 LI로 전송하는 기능을 제공하고 있으며, 미국의 경우를 살펴보면 CALEA(Communications Assistance for Law Enforcement Act) 법적 근거에 따라 SBC 장비에서 LI 기능을 제공
  - VoIP 사용자의 프라이버시 보호 기술은 아직 초계 단계로 SIP를 위한 프라이버시 메커니즘이 표준으로 제공되고 있고, VoIP 프라이버시 정책에 의거 프라이버시 서비스가 제공되어야 한다고 정의하고 있으나, 그 구현 방법 등은 명시되어 있지 않으며 시장에서도 적용된 바를 찾기 어려움
  - 사용자의 물리적, 논리적 위치정보를 다루는 VoIP 긴급통화 및 프레즌스 서비스 등 다양한 VoIP 부가서비스가 등장하고 있으나, 사용자의 위치정보 노출로 인한 프라이버시 침해 위협에 대한 고려는 매우 부족한 상황임

6) Media Gateway Control Protocol
7) Firewall
8) Back to Back User Agent/Gack-to-Back Gatekeeper/Back-to-Back Gateway
9) IP Multimedia Subsystem
10) Multi-Protocol Label Switching

• 스팸대책

국내와 유사하게 국외에서도 VoIP (또는 SIP) 스팸 분야에 대한 연구개발이 진행 중이나, 이외의 다른 형태의 스팸 분야에서는 기술개발 보다는 스팸 방지 정책을 수립하고, 가이드라인을 제시하는 측면에 관심이 집중되고 있음. VoIP 이외의 스팸 방지 분야의 기술적인 측면에 대한 논의는 IRTF의 ASRG (Anti-Spam Research Group)이 전무한 상태임. 2003년에 설립된 ASRG는 스팸 문제에 대한 기술적 솔루션에 대한 논의를 진행하고 있으나, 활동이 활발하지는 않음

IETF의 SIPPING WG는 SIP 또는 SIP 응용 서비스와 관련된 요구사항을 표준화 하고 있고, SIP WG는 SIP 프로토콜과 관리 분야의 표준화를 진행 중에 있음. 이에 반하여 ITU-T는 NGN security 가이드라인 내에 스팸에 대한 언급이 있으며 SG 17내에 스팸 대응 가이드라인을 포함한 다수의 표준화가 진행중에 있음

Qovia는 call pattern 분석 및 발신자의 행위분석에 대한 scoring을 통해 스팸 콜을 차단하는 기법에 대한 연구를 수행하였음. North Texas 대학에서는 VoIP 스팸을 탐지하는 추론 기법에 관한 연구를 진행함. Fraunhofer Institut Fokus에서는 reputation 기반의 SIP 스팸 탐지 기술을 연구하였으며, 예일 대학에서는 발신자 인증을 위해 identity, identity-info 헤더를 확장하는 방안에 대한 기고서를 제안하였음. Koyote Networks는 발신자 인증 헤더 삽입을 통한 SPIT 차단 기술을 연구하였음

국외 산업계 역시 VoIP 분야에서만 활동이 왕성한 편인데, VoIP Security Alliance는 비영리 VoIP 보안 관련 단체로, 사업자, 사용자, 제조사 등에 기술 자료를 제공하여 VoIP 서비스를 확산하는데 기여하고 있음. Qovia.inc는 VoIP 스팸 대응 기술이 포함된 제품을 판매하고 있으며, 단일 소스에서 다량의 VoIP 콜 전송을 분석하는 방법과 관련된 특허를 보유하고 있음. BorderWare의 SIPassure는 ID 스푸핑 공격, 화이트리스트(whitelist), 블랙리스트(blacklist), SIP DoS 공격 방지 기능 등을 제공하는 최초의 SIP 화이어월 장비임. Facetime의 IMAuditor는 실시간 콘텐츠 필터링 장비임

• 응용보안 강화 프로토콜

응용보안 강화 프로토콜 분야에서는 전송계층의 보안프로토콜인 TLS, 패스워드 인증 프로토콜에 대한 기술 개발이 진행 중에 있음

패스워드 인증 프로토콜과 관련하여서는 IETF, ITU-T 등에서 표준화와 더불어 기술 개발을 진행 하고 있음

산업체의 경우 현재로는 패스워드 인증 프로토콜에 대한 독자적인 제품개발이 이루어지고 있지는 않지만, 통신망 보안, 금융망 보안 시스템 개발에 일부 응용되어 적용되고 있는 상황임. 현재 많이 사용되는 평문의 아이디와 패스워드를 이용하는 인증방식은 통신로의 중간에 있는 공격자가 패스워드를 획득하고, 획득된 패스워드를 이용해 추후에 그 사용자를 가장할 수 있는 중간자 공격에 취약한 단점이 있음. 그러나 안전한 패스워드 인증 프로토콜은 중간자 공격으로부터 안전하고, 사람이 기억하기 쉬운 패스워드를 이용하며, 쉽게 구현할 수 있고, 사용이 용이하다는 특징이 있음. 안전한 패스워드 인증 프로토콜은 대표적인 키 공유 프로토콜인 DH (Diffie-Hellman) 프로토콜을 이용하며, 이 프로토콜의 수행 결과로, 통신 상대에 대한 상호 인증과 동시에 추후 세션에서 사용될 공통의 세션 키가 공유됨

안전한 패스워드 인증 프로토콜은 키 로밍 서비스, 인터넷 뱅킹 서비스, 망 관리 서비스 등에서 인증 및 키 분배 방

식으로 활용 될 수 있을 것으로 기대됨. 안전한 패스워드 인증 프로토콜은 평문의 패스워드를 직접적으로 교환하지 않고 상호 인증을 수행할 수 있어서, 결과적으로 중간자 공격을 막을 수 있고, 공격자가 패스워드를 데이터베이스에 미리 저장했다가 비교함으로써 사전 공격(dictionary attack)을 막을 수 있음. 또한 하나의 세션에서 교환된 정보를 후에 다른 세션에서 재사용하는 방식의 재생 공격에 취약하지 않음. 특히 클라이언트와 서버 측에 낮은 부하로 구현될 수 있어서 계산량과 메모리에 제한을 갖는 이동 전화기를 포함한 PDA, 그리고 PC 등에 효율적으로 설치될 수 있으며, 암호 토큰이나 PKI 같은 외부 인프라의 도움이 필요가 없어서 금융 보안과 고객 애플리케이션에 매우 효과적이라고 할 수 있음

TLS를 사용하는 경우의 대부분은 안전한 웹서비스를 제공하기 위해 개발된 HTTPS(HTTP/TLS) 프로토콜을 사용하는 것으로 Apache와 OpenSSL을 결합해서 만든 Apache-SSL, 마이크로소프트사에서 개발한 IIS(Internet Information Services), 넷스케이프사의 Netscape Enterprise Server가 대표적임. HTTPS를 지원하기 위해서는 웹브라우저 또한 TLS를 지원해야 하는데 현재 개발된 대부분의 웹브라우저는 SSL v2.0, SSL v3.0, TLS v1.0을 지원하고 있음. 이러한 안전한 웹서비스를 이용하는 분야로는 금융분야, 전자상거래 및 보안 웹메일 등이 대표적임. 또한 요즘에는 ID와 패스워드를 암호화하여 전송함으로써 안전한 로그인을 수행하기 위해 TLS를 사용하고 있음. 이러한 TLS를 제공하는 toolkit에는 SSLeay를 이용하여 제작한 오픈 소스의 OpenSSL, RSA Security사에서 Planet SSL이 대표적이며, 인터넷 또는 인트라넷에서 암호화 통신을 제공하는 Dart Communications사의 PowerTCP SSL Tool이 존재함. 그 외에 TLS를 지원하는 제품으로는 안전한 텔넷서비스 제공을 위한 InterSoft Internal사의 SecureNetterm과 안전한 ftp 서비스 제공을 위한 IPSWITCH사의 ws-ftp 프로그램 등이 대표적임

- 안전한 P2P 보안

미국의 Microsoft가 2001년부터 매우 가용적, 신뢰적이며 안전한 파일 공유 시스템 제공을 목적으로 하는 Farsite(Federated, Available, and Reliable Storage for an Incompletely Trusted Environment) 라는 연구를 진행 중이며, 최근에는 윈도우즈 운영체제 "비스타"(2006년)에 컴퓨터간 연결 및 검색이 자유로운 P2P 기술을 탑재하여, P2P 응용을 통해 이용자의 행동을 완전히 포괄할 수 있는 MS 세계 구축을 추진하고 있음

SUN Microsystems는 2001년부터 JXTA 라는 프로젝트를 진행하고 있는데, 이는 휴대전화, PDA, PC 및 서버 등과 같이 네트워크에 연결된 다양한 디바이스들이 P2P 형태로 서로 통신, 협업할 수 있도록 하는 프로토콜의 개발을 목적으로 함. JXTA는 2006년 현재 J2SE용 버전의 개발이 거의 완료된 상태이며, C/C++용 버전 및 J2ME용 버전의 개발은 성숙 단계에 있음

이 외에도 인텔, 휴렛패커드, 노키아 등 세계 유수한 IT 기업들이 P2P 관련 연구를 진행 중임

P2P 보안 관련기술 분야에서는 시만텍, 포티넷, 시큐어컴퓨팅, 주니퍼 등 보안장비 업체들이 P2P 트래픽 제어 기능이 포함된 UTM 솔루션을 제공하고 있음

학계에서는 UC Berkeley가 P2P 기반 분산 컴퓨팅을 통하여 외계 생명체의 존재를 찾기 위한 막대한 양의 계산을 수행하는 SETI@home이라는 프로젝트를 진행하고 있으며 그밖에 MIT, Purdue, UC Berkeley, Rice University 등에서 여러 구조적 분산형 P2P 네트워크(Chord, CAN, Pastry, Tapestry)의 개발을 진행해오고 있음

그밖에 일본 Gnutella 사용자 모임이 핸드폰을 이용한 Gnutella 서비스를 목적으로 하는 Mog 라는 프로젝트를 진행하고 있음

• IPTV 보안

2006년 현재 세계적으로 280여개 이상의 사업자가 IPTV 시범 및 상용서비스를 제공하고 있지만 서비스 제공자별로 독자적 기술을 채용하고 있어 다양하게 존재하는 IPTV 서비스 간에 상호 운용성을 기대하기 힘든 상황임. 특히 CAS와 DRM 기술은 IPTV에 적용되기 이전부터 상호 호환성이 결여되어 있기 때문에 IPTV에 적용되더라도, 이러한 현상이 계속될 것으로 예상됨. ITU-T IPTV FG의 IPTV 보안 관련 표준화 작업 문서에서는 IPTV 스트림 데이터가 CAS 또는 DRM에 의해서 보호되어야 한다는 요구사항을 정의하고 있음

IPTV 스트림 데이터 보호를 위해서 기존의 DRM 또는 CAS 기술이 거론되고 있긴 하지만, HD급의 고화질 디지털 방송을 지원할 수 있는 보안 기술에 대한 요구 및 연구개발이 학계를 중심으로 끊임없이 일고 있어 IPTV 전용 암·복호화 (또는 스크램블링) 기술 분야에 대한 기초·응용 연구가 진행 중임. 특히, 투명성(transparency), transcodability, 공간/주파수 도메인 암호화, 선택적 암호화 등과 같은 IPTV에 특화된 요구사항을 만족하기 위한 기술 개발이 주를 이루고 있음

최근 NDS, 이데토 등 업계를 중심으로 고성능의 암호화 제품이 출시되고 있으나, 기술의 우열을 가늠하기 힘들며, 아직까지는 기술 향방을 논할 수 있는 정도는 아님. 공간/주파수 도메인 암호화, 선택적 암호화 등에 대한 기초 연구는 Connecticut 대학, City University of New York, North Carolina State University 등 학계를 중심으로 진행되고 있으며, 논문 형태의 결과물이 도출되고 있을 뿐 아직까지 IPTV 서비스에 직접 적용되지는 않음

Tokyo 대학, 이스라엘의 Weizmann Institute 등에서 Visual 암호화를 이용한 투명성(transparency) 보장에 대한 기초 연구가 진행 중에 있으나, 동영상 데이터에 대해 연구된 것이 아니므로 IPTV에 이러한 특성을 제공하기 위해서는 추가 연구가 필요함

NGN 보안과 부가서비스 보안은 국내와 마찬가지로 기존의 네트워크 또는 서비스 보안 기술의 연속으로 보는 시각이 강하며, IPTV를 대상으로 한 구체적인 연구는 진행되지 않음. 이에 대하여 국외 인터넷TV 분야의 연구 개발은 NGN을 기반으로 하기 보다는 응용 계층에서의 멀티캐스트를 대상으로 하는 경우가 대부분임. NGN 기반의 IPTV 서비스 방식에서는 모든 라우터가 멀티캐스트를 지원해야 하고, VoD (유니캐스트)와 실시간 방송(멀티캐스트)을 동시에 제공하는 다채널 서비스의 특성[11]이 강하여 다수의 스트림 세션을 동시에 제공해야 하는 문제가 발생하기 때문에 결국 네트워크 및 서버의 부담이 증가할 수밖에 없음. 학계에서는 이러한 단점들을 보완하거나 대체할 수 있는 방안으로 오버레이(Overlay) 또는 P2P(Peer-to-Peer) 방식으로 불리는 새로운 방식을 이용하고 있음

11) 최근 IPTV와 같이 VoD와 실시간 방송 서비스를 다채널로 지원하는 서비스에서 다수의 시청자가 채널을 선택하는 특성을 연구한 결과에 따르면, 거듭제곱법칙(Power Law)의 특성을 보인다는 결과가 나오고 있음. 이것은 매우 적은 수의 인기 있는 채널과 매우 많은 수의 비인기 채널이 동시에 존재한다는 것으로, 몇몇 채널을 멀티캐스트로 제공함과 동시에 대부분의 채널들을 유니케스트로 제공해야 하므로, NGN 상에서 멀티케스트를 이용한다 하더라도 네트워크 및 서버의 부담은 크게 줄지 않는다는 것임(참고:Nishith Sinha and R뮤 Oz, "The Statistics of Switched Broadcast," in Proc. SCTE Conference on Emerging Technologies, Huntington, CA, January 2005)

오버레이 방식은 IP 계층에서 라우터의 멀티캐스트 기능을 이용하는 것이 아니라, 응용 계층에서의 멀티캐스트 기능을 지원할 수 있도록 고정된 중간 노드들을 두는 것임. 이에 따라 모든 라우터가 IP 멀티캐스트를 지원하지 않더라도 서비스가 가능하게 됨. P2P 방식은 여기에서 더 나아가 사용자의 단말(또는 셋톱)이 이러한 중간자의 역할을 할 수 있도록 다이나믹 토폴로지를 갖는 서비스 망을 응용 계층에서 구성한다는 것임. 이러한 서비스에 대한 연구와 개발은 많은 진척을 보이고 있으며, Joost, PPStream, PPTV, CoolStream 등 서비스가 이루어지고 있음. 그러나 이러한 네트워크 계층의 변경은 많은 추가 위협을 낳을 수밖에 없는데, 현재까지는 대부분 안정적인 서비스에만 중점을 두고 있어, 이에 대한 추가 연구가 필요함

프라이버시에 대해서는 homomorphic 암호화 기법을 중심으로 하여 다양한 형태의 기초 연구가 학계를 중심으로 진행되었는데, 이러한 기술을 IPTV 환경에서의 사용자 (프로슈머) 프라이버시 보호를 위해 적용한 사례는 아직 없음. 카네기멜론 대학, Rovira i Virgili 대학, Aarhus 대학 등에서 homomorphic 암호화에 대한 연구가 진행 중에 있으나, 자체적인 기초 연구 형태로 진행되고 있고, 논문 형태의 결과물만을 내고 있음

IPTV 서비스 프레임워크 분야에서는 마이크로 소프트를 비롯한 업계에서 IPTV (통합) 솔루션을 제공하고 있으며, ITU-T 등에서 표준화 노력이 진행되고 있으나 현재까지는 연구 분야로 인식 되지는 않고 있음. 이 분야에서의 보안 기술로는 이데토가 사용자/디바이스 인증, 콘텐츠 보호, STB 보안 등의 IPTV 통합 보안 솔루션을 출시하였음. 그러나 IPTV를 구성하는 '종적' (계층별) 보안 취약성 분석 (브로드캐스트 망, 멀티캐스트 전송 프로토콜, 스트림 패키타이징 (MPEG-2 TS), 비디오 코딩 (MPEG-2, H.264) 등)이 필요하고, LAN/WLAN/Wibro 등 서로 다른 전송망에서의 '횡적' 서비스 제공시 보안 취약성 분석이 요구됨. 이와 별도로 IPTV 양방향 또는 부가서비스 제공시 서비스 간 보안 기술 필요하며, 이러한 보안 기능을 제공할 때 QoS와 QoE를 우선 보장하면서 안전한 IPTV 서비스망을 구축이 용이해야 함

- STC (Secure TC)

신뢰 · 보안 관련해서는 TCG의 표준을 준수하는 TPM (Trusted Platform Module)이라는 칩을 탑재한 많은 제품들이 출시되고 있고 이러한 증가는 앞으로 더욱 두드러질 것으로 예측됨. MS사는 WindowVista에 이러한 장치를 탑재하기 시작했고 IBM 등 많은 노트북 제품들도 TPM 칩이 탑재되어 나옴. 무선 통신 기술 및 장비의 발달로 모바일 장치의 보급이 더욱 증가하면 향후 이를 겨냥한 많은 서비스 시장이 창출될 것으로 판단되며 이에 관련한 보안 문제는 신뢰 · 보안 서비스로 해결을 할 수 있을 것으로 판단됨

- 현재 MS, IBM, HP 등 많은 업체들이 STC에 대한 연구 개발을 진행 중임
- STC 기술(TCG 표준 준수)을 탑재한 제품을 출시하고 있는 회사가 10개 이상되고 170 개 이상의 회사가 STC 표준화 작업에 참여 중임
- 이 중 칩 제조사는 Atmel 등 4개사, 보안 제품에 적용 중인 회사는 Verisign 외 10여개 회사 등이 있고, 노트북과 PC에도 관련 기술이 탑재되어 있음

〈표 21〉 STC 관련 활동 참여 업체

분류	참가 기업
반도체 벤더	Atmel, Broadcom, Infineon? Sinosun,STMicroelectronics, National Semiconductor,Texas Instruments, Renesas Technology Corp, Intel? AMD
PC 부품 벤더	Intel, Seagate Technology, Phoenix
PC 플랫폼 벤더	Dell, Fujitsu Limited, Fujitsu Siemens Computers,NEC, Hitachi, Ltd., Lenovo,Toshiba,Hewlett-Packard, IBM
소프트웨어 보안 벤더	RSA Security, Certicom,Enforce,Funk Software,Wave Systems VeriSign,Network Associates,Sygate,Symantec,Trend Micro,Utimaco Safeware
휴대전화 벤더	Nokia Motorola,Vodafone, Siemens etc.
네트워크 장치 벤더	Juniper Networks,Enterasys Networks,Extreme Networks,Foundary Networks

• 차세대 웹 보안

- 국책 연구소
  ◦ 웹서비스 정보보호 관련 기술 개발은 주로 산업계에서 이루어짐
  ◦ 유럽의 ITEA (Information Technology European Advancement)가 SODA (Service Oriented Device and Delivery Architecture) 프로젝트를 통해 디바이스 간의 연동을 용이하게 해주는 도구를 개발중임
- 산업계
  ◦ 웹서비스 (Web Services) 보안과 관련하여, IBM, MS, Verisign, Baltimore, RSA, Phaos 등은 XML 전자서명 및 XML 암호에 대한 상용 제품을 개발 완료하였으며, Apache에서는 XML 전자서명 및 XML 암호의 공개 버전을 선보임
  ◦ 또한 Entegrity의 AssureAccess, HP의 Select Access, Computer Associates의 eTrust SSO, Entrust의 GetAccess 등이 SAML을 기반으로 하여 SSO를 제공하는 솔루션을 개발하였고, Parthenon Computing, Sun Microsystems, Lagash Systems 등에서는 XACML 지원 제품을 개발하였으며, IBM의 WSDK, MS의 .NET Framework에서 WS-Security가 지원됨
  ◦ IBM의 WebSphere DataPower XS40 XML Security Gateway는 XML/SOAP Filtering, Field Level XML 보안, SAML, XACML, WS-Security 기술을 통한 접근제어 기능 등을 제공함
  ◦ 웹 2.0 보안 기술은 웹 어플리케이션 취약점 분석툴 및 웹방화벽 개발이 주로 이루어지고 있으며, 넷컨티넘, 임퍼바 등에서 웹방화벽을 개발함. Apache에서는 ModSecurity라는 무료 웹 방화벽을 공개하였음.
  ◦ Nokia 에서는 모바일 환경에서 XML 및 SOAP을 지원하고 기본적인 보안 기능 및 Liberty Alliance의 ID관리 기술을 구현한 Nokia Web Services Framework를 개발하였음
  ◦ 유비쿼터스 웹 기술과 관련하여, MS는 웹서비스 기반의 디바이스 간의 연동을 위해 'Devices Profile for Web Services' 명세를 개발하고 이를 기반으로 한 제품을 개발하였으며, 메시지 보호를 위해 HTTPS를 사용함. UPnP 포럼에서는 디바이스 간 연동시의 보안을 위해 XML 기반의 보안 스펙을 개발하였음.
  ◦ MIT CSAIL과 Nokia Research Center Cambridge는 공동으로 SwapMe라는 프로젝트를 추진중이며, Mobile Ecosystem을 위한 시맨틱 웹 어플리케이션 플랫폼을 개발하고 있음

〈표 22〉 웹서비스 보안 제품 업체

Company	Functionalities Provided by Product
IBM WebSphere	WS-Security, WS-Policy
MS WSE 3.0	WS-Security, WS-Policy
Apache XML Security	XML 전자서명, XML 암호
Apache ModSecurity	웹 방화벽
IAIK XML Security	XML 전자서명, XML 암호
IBM XML Security Suite	XML 전자서명, XML 암호
IBM WebShere DataPower	XML 보안 게이트웨이, WS-Security
Entegrity AssureAccess	SAML, SSO
HP Select Access	SAML, SSO
Entrust GetAccess	SAML, SSO
Parthenon Computing	XACML
Sun Microsystems	XACML
Nokia Web Services Framework	Liberty ID 관리 기술
STG Security	웹어플리케이션 취약성 분석, 웹 어플리케이션 파이어월
TEROS	웹어플리케이션 보안 게이트웨이
체크포인트 Connectra	웹 보안 게이트웨이

- 학계
  - ◦ AJAX, Mashup 등 웹 2.0 기술들에 대한 보안 기술에 관한 연구가 시작되고 있음
  - ◦ 시맨틱 웹 서비스를 위한 보안, 프라이버시, 트러스트에 대한 연구가 수행되고 있음
  - ◦ IHMC (Institute for Human and Machine Cognition)에서 KAoS라는 시맨틱 웹 언어를 이용한 보안 정책 기술을 개발하고 있으며, Kagal et al.에 의해 Rei라는 시맨틱 웹 언어를 이용한 보안 정책 기술이 연구되고 있음

• Lawful Interception

LI Plugteststm 시험이 2006년 3월 6일부터 10일까지 ETSI 구내에서 실시됨. 테스트 영역은 크게 "Handover of intercepted IP and e-mail traffic" 및 "Delivery of Interception Related Information (IRI) and Call Content (CC)"으로 구분됨. 구체적으로 다음과 같은 기술 규격의 적합성 및 유효성에 대한 실험이 이루어짐

〈표 23〉 LI Plugteststm 주요 평가 내역

ETSI TS 102 232 v.1.3.1	Handover of intercepted IP Traffic
ETSI TS 102 233 v.1.2.1	Service specific details for E-mail services
ETSI TS 102 234 v.1.4.1	Service specific details for Internet Access services

해당 실험에 참여한 업체 리스트는 다음과 같음

〈표 24〉 LI Plugteststm 시험 참여 업체 리스트

Company	Tested
Atis	Monitoring Facility equipment
Cisco Systems	Cisco 7200 router with Service Independent Intercept capability
Home Office UK	Interception equipment, Monitoring Facility equipment
Verint	Interception equipment, Monitoring Facility equipment
Utimaco Safeware AG	Interception equipment
Nice	Monitoring Facility equipment
Penlink	Monitoring Facility equipment
Narus	Interception equipment
Pine Digital Security	Interception equipment, Monitoring Facility equipment

Cisco는 2006년 현재 Cisco 12000 시리즈 라우터 ISE Line Cards에 LI 기능을 탑재하여 출시하고 있으며, Cisco의 LI 기술은 SII(Service Independent Intercept) 아키텍처 및 SNMPv3(Simple Network Management Protocol Version 3) 제공 아키텍처를 기반으로 하고 있음. 특히 Cisco는 RFC3924(Cisco Architecture for Lawful Intercept In IP Networks) 및 Cisco Lawful Intercept Control MIB 와 같은 자체 기술력을 바탕으로 제품화 하고 있는 실정임. Cisco의 라우터시리즈는 다음과 같은 두 가지 형태의 LI를 수행할 수 있게 설계됨

- Lawful Intercept for Voice over IP (VoIP) calls
- Lawful Intercept for dial-up calls

또한 Cisco SII 아키텍처는 모든 IP 네트워크를 위한 표준 구조를 지원하고 있으며, Call control equipment 대신에 Mediation device를 통해 감청 제어를 수행함. 즉 LI control은 Call control가 별개로 운용되는 구조를 갖게 됨. SII는 Call control 파트너사 및 Mediation device를 위한 공통 인터페이스 제공함. 더불어 이러한 SII 구조 하에서 동작하는 Cisco 12000 시리즈 라우터는 SNMPv3를 이용하여 VoIP 및 Dial-up 연결에 대한 감청 기능을 제공하며, 감청된 정보를 Mediation device로 전달하는 기능을 수행할 수 있음. 이를 위해 LI MIB (CISCO-TAP-MIB, Version 1)을 사용하고 있으며, UDP(User Datagram Protocol) encapsulation 기능, 그리고 SNMPv3 LI provisioning 인터페이스를 활용함

- 구체적으로 VoIP call 감청은 Media gateway local IP 및 UDP port number에 기반하여 수행되고 이때 MGCP(Media Gateway Control Protocol) 프로토콜이 이용됨
- Dial-up call 감청은 account session ID에 기반하여 수행되며, PPP, multi-link PPP, Exec/TCP-clear 등의 세션을 위해 사용될 수 있음

이러한 기능은 AS5350, AS5400, AS54500HPX, AS5400XM, AS5850와 같은 Universal Gateway 제품군에도 동일하게 탑재되어 있음

CableLabs는 2006년 10월 "Control Point Discovery Interface Specification (PKT-SP-CPD-I02- 061013)"와

은 자체적인 기술 규격을 정의하고 사용하는 등의 기술적 우위를 확보하고 있음

대당 33만 5천달러의 가격에 판매되고 있는 것으로 알려진 CCS 인터내셔널사의 CDMA 감청장비는 MIN(가입자번호)과 ESN(단말기일련번호)의 정보를 획득, 암호화된 코드를 해체하여 압축음성을 풀어서 음성을 재생하는 기능을 수행함. 이는 이동통신 회사의 별도의 협조가 필요 없으며 통화자는 자신의 전화가 도청당하고 있는지 전혀 알 수 없음.

이미 1996년도부터 GSM 휴대전화에 대한 감청장비를 개발하여 판매하고 있으며, 시스템과 연결하여 감청하는 장비(GSM1000)와 공중에서 전파를 수신하여 감청하는 휴대용장비(GMS2000)의 두 가지 모델이 있음

〈표 25〉 주요 LI 관련 서비스 제공 업체

Company	Service Area	Functionalities Provided by Product
Fiducianet	USA	Lawful interception and lawful access (subpoena processing)
GTEN	Germany	Lawful interception
TSI	USA	Lawful interception (announced)
VeriSign	Global	All lawful interception and lawful access (subpoena processing), including transnational requirements

〈표 26〉 주요 LI 관련 제품 개발 업체

Company	Functionalities Provided by Product
Accuris	Multiple intercept products and capabilities
Acecom	Collection systems
AcmePacket	IP border acquisition systems
Aqsacom	Multiple intercept products and capabilities
Arpege	Collection systems
Bartec	Collection systems
Cetacean	Collection systems
Cisco	LI enable access devices
Codem	SIGENT solutions
EDI	Collection systems
ETI	Collection systems
JSI	Collection systems
Marconi	Integrated government systems
NICE Systems Ltd	Multiple intercept products and capabilities
NikSun	
Pen-Link Ltd	Collection systems
Pine	Multiple intercept products and capabilities
Raytheon	Collection systems
Roke Manor Research Limited	Tracking and intelligence
Septier Communications, Ltd	SS7 mediation equipment
Siemens	Multiple intercept products and capabilities
Soghi Communications Ltd	Multiple intercept products and capabilities

Company	Functionalities Provided by Product
SS8 Networks	Mediation and collection systems
Syborg	Collection systems
Telcordia	
Teletron	
TopLayer	Ultra high performance IP intercept devices
Urmet	
Utimaco Safeware AG	Intercept software products and services
Verint	Multiple intercept products and capabilities

학계에서는 H.323 기반의 IP 전화 네트워크에서의 LI 방법론에 대한 연구가 진행되고 있는 것으로 보고되었으며, Electronic Surveillance 관련 이슈에 대한 연구가 국내에 비해 보다 먼저 진행되어 왔음. VoIP와 같은 환경에서 LI 자체 구조 또는 이의 수행을 돕는 분산 시스템 또는 모니터링 아키텍처에 대한 연구가 활발히 이루어지고 있음

나) 평가인증

• 정보보호 평가

평가선진국인 미국, 영국, 독일, 프랑스, 캐나다, 호주 등은 일찍히 자체 평가기준을 개발하여 정보보호제품을 평가하여 왔음. 미국은 1983는 TCSEC(Trusted Computer System Evaluation Criteria)을, 영국은 1987년 Green Book을 독일과 프랑스는 Blue-White-Red Book을, 캐나다는 1989년 CTCPEC(Canadian Trusted Computer Product Evaluation Criteria)을 개발하여 정보보호제품 평가를 시작하였음

이들은 각 국에서 평가한 제품을 타 국가에서 사용하기 위해서는 해당 국가로부터 다시 평가받아야 하는 불편함이 있어 각 국가에서 평가한 결과를 상호인정하기 위한 평가기준을 개발하였음. 초기에는 유럽 국가들이 ITSEC(Information Technology Security Evaluation Criteria)을 개발하였으나 미국과 캐나다가 참여하면서 공통평가기준 (CC : Common Criteria for Information Technology Security Evaluation)을 개발하여 현재 국가들이 사용하고 있음

더불어 이들 국가들은 평가결과를 상호 인정하는 국제 공통평가기준 상호인정협정(CCRA)을 체결하였으며, '07. 3월 현재 CCRA에는 총 24개 국가가 회원국으로 활동하고 있으며 회원국가는 다시 인증서 발행국(CAP : Certificate Authorizing Participant)과 인증서 수용국(CCP : Certificate Consuming Participant)으로 구분됨. CAP 국가는 자국에 평가 · 인증 제도를 구축하여 운영하고 있으며 CCRA에서 인정되는 인증서를 발급하는 국가임. CCP 국가는 CAP 국가에서 발행한 인증서를 수용하는 국가를 의미함

〈표 27〉 인증서발행국 및 수용국 현황

구분	설명	가입국명
인증서발행국 (12개국)	자국의 인증서가 회원국으로부터 인정받는 국가	미국, 캐나다, 영국, 프랑스, 독일, 호주, 뉴질랜드, 일본, 네덜란드, 노르웨이, 대한민국, 스페인
인증서수용국 (12개국)	인증서발행국의 인증서를 인정하는 국가	이탈리아, 그리스, 핀란드, 이스라엘, 스웨덴, 오스트리아, 터키, 헝가리, 체코슬로바키아, 싱가폴, 인도, 덴마크

CCRA는 CCRA 관리위원회(MC : Management Committee), CCRA 집행위원회(ES : Executive Sub-Committee), CC 개발위원회(DB : Development Board), CC 개발실무위원회(MB : Management Board)로 구성됨

- CCRA MC : 모든 회원국에서 2명이 참여할 수 있으며 년 1회 회의를 개최함. 이들은 신규 회원국 가입, CCRA의 사업계획, 새로운 버전의 평가기준 및 평가방법론, CCRA 인정범위 등 모든 업무에 대해 최종 결정권을 행사함
- CCRA ES : CAP 국가 또는 MC의 승인을 득한 CCP국가에서 2명이 참여할 수 있으며 년 2회 회의를 개최함. 이들은 CCRA 사업계획 및 절차 수립, 신규 회원국의 평가 · 인증 능력 심사, 회원국 정기심사, 기술적 이견을 해소하며 보안성 평가 홍보를 담당함
- CC DB : CAP 국가에서 2명과 MC의 승인을 득한 전문가가 위원 자격으로 CCP 국가에서는 2명까지 관찰자 자격으로 참여할 수 있으며 년 2회 회의를 개최함. 이들은 CC와 CEM 개발을 관리하고 모든 회원국이 동일하게 이를 적용할 수 있도록 지원하며 ISO 표준화를 위한 연락관 역할을 수행함
- CC MB : 관심을 가지고 있는 모든 회원 국가에서 참여할 수 있으며 CC 및 CEM을 실제 개발하고 각 국가에서 제기한 의문사항에 대한 해설서를 작성함

〈표 28〉 CCRA 위원회별 업무 내역

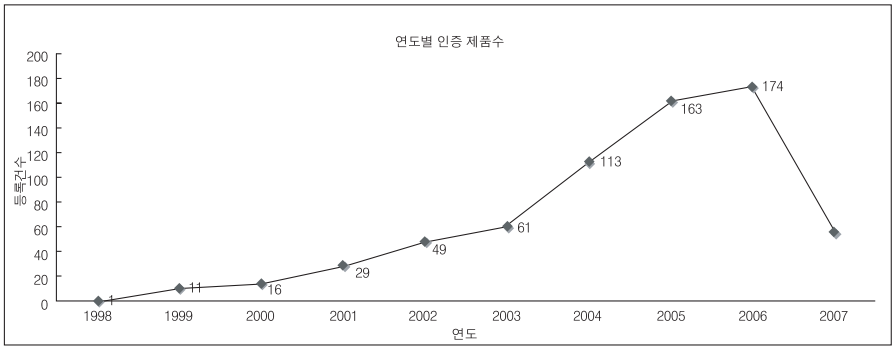
위원회 명	업무
CCRA 관리위원회 (CCRA Management Committee)	CCRA 모든 업무에 대한 최종 결정
CCRA 집행위원회 (CCRA Executive Subcommittee)	CCRA 사업계획 수립 CAP 회원국 정기 심사 및 신규 회원국가 심사 기술적이견 해소, 평가 홍보
CC 개발위원회 (CC Development Board)	인증제품 사후관리, 개발환경 평가기준/방법론 적용, ISO 표준화
CC 개발실무위원회 (CC Management Board)	평가기준 및 방법론 개발 실무

CCRA에서는 보안성 평가와 관련된 문서들을 개발하고 ISO를 통하여 표준화를 추진함. CCRA는 공통평가기준 및 공통평가방법론을 시작으로 보호프로파일 및 보안목표명세서 작성 가이드, Probablistic 평가 방법론, 인증보고서 양식, 보안성 평가 tools & techniques, 개발환경 보안실사, 지문인식 평가 가이드, 제출물 작성 가이드 등 다양한 문서들을 개발 중에 있으며 그 중, 공통평가기준 및 공통평가방법론, 보호프로파일 및 보안목표명세서 작성 가이드 등은 이미 ISO에 전달되어 표준화 중에 있으며 Probablistic 평가 방법론을 2007년 11월 ISO 제출할 예정임

2007년 4월 우리나라를 제외한 11개의 CCRA 인증서발행국에서 인증된 제품은 총 672개 제품에 달하며 매년 인증 제품 수가 증가하고 있는 추세임

〈표 29〉 CCRA의 연도별 인증제품 수 ('07년 4월말 기준)

연도	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	계
인증제품 수	1	11	15	29	49	61	113	163	174	56	672
누적 수	1	12	27	56	105	166	279	442	616	672	-



(그림 6) CCRA의 연도별 인증제품수 추이

그중 스마트카드가 190개 제품으로 전체의 30%에 달하며 이어 데이터보호제품 12%, 운영체제시스템 및 침입차단시스템 10% 순임

〈표 30〉 제품 군별 인증 제품 수 ('07년 4월말 기준)

제품군	Access Control	Anti-Virus	Biometric	Data Protection	DB	Firewall	IDS/IPS	Network Device	Network Mngt.	Wireless LAN
인증제품 수	35	1	2	76	28	62	23	7	12	2
제품군	OS	PKI/KMI	Secure Messaging	Security Mngt.	Smartcard	VoIP	VPN	Web	Misc.	계
인증제품 수	62	42	18	17	190	1	13	15	66	672

인증제품의 등급을 비교하면 스마트카드 제품 평가의 수요로 인하여 4+ 등급이 202개 제품으로 30%를 차지하며 2,3 등급이 128개, 70개 제품으로 19%와 11%로 그 뒤를 이음

〈표 31〉 보안 등급 별 인증 제품 수 ('07년 4월말 기준)

보증등급	EAL1	EAL1+	EAL2	EAL2+	EAL3	EAL3+	EAL4	
인증제품 수	24	19	128	48	70	60	63	
보증등급	EAL4+	EAL5	EAL5+	EAL6	EAL6+	EAL7	EAL7+	계
인증제품 수	202	8	48	0	0	0	2	672

• 보안관리

정보보호관리체계 인증기술의 경우, 영국의 BSI(British Standard Institute)에서 만들어진 BS7799 영국 표준이 최초의 정보보호관리 표준이며, 1993년 처음 정보보호 관리실무에 대한 지침을 개발되어 1995년 처음 BS7799 Part 1이 공포되고 1998년에는 Part 1에 기반한 인증 기준으로서 Part 2가 개발됨. BS7799가 ISO(17799, 27001) 표준으로 제정되었으며, 유럽과 일본을 중심으로 활성화 되어 있음. 인증기술에 대한 표준을 ISO/IEC JTC1 SC27/WG1에서 ISMS 구현가이드, ISMS 평가 방법론, 정보보호 위험관리 등 ISO27000 시리즈를 지속적으로 표준으로 제정하기 위한 작업을 진행중에 있음

■ 주요 국가별 특허출원 동향

가) 응용보안

• u-지식 보안

미국특허에서는 Microsoft와 Digimarc가 콘텐츠 저작권 보호 툴킷 분야에서 가장 많은 출원을 보이고 있음. Intel은 지식 보안 단말플랫폼 분야를 비롯한 다양한 분야에서 연구 활동이 이루어짐을 알 수 있었음. 유럽특허에서는 Intertrust Technologies와 Microsoft, SONY와 MATSUSHITA, 삼성 등 비유럽인에 의한 u-지식 보안 분야 특허 출원이 이루어지고 있으며, 대부분 콘텐츠 복제방지기술 분야에서 특허 출원이 많았음. 아울러 일본은 익명ID 발급/검증 분야에서 NTT가 가장 많은 출원건수를 보유하고 있는 것으로 조사되었으며, NTT, HP, TOSHIBA, MATSUSHITA, SONY는 콘텐츠 복제방지기술 분야에서 특허 출원을 보이고 있음. 콘텐츠 복제방지 기술 관련기술은 특허 출원이 많이 이루어진 분야로, u-지식 보안 기술 개발시 타 공백기술에 대한 IPR 확보에 중점을 둘 필요가 있음

• 쉘 보안

미국 특허 중에 쉘 보안을 위한 호스트 키 습득 방법, 채널 보호, 보안 쉘 접근 프로토콜 접근 제어에 대한 특허가 일부 존재하나 관련 특허 출원 건수가 10개 이내로 많지 않은 것으로 조사됨

유럽 역시 쉘 보안 관련 특허가 매우 적으며, 쉘 보안 기술을 포함한 응용 보안 분야의 특허가 일부 존재하는 것으로 조사됨

일본 역시 쉘 보안 관련 특허가 매우 적으며, 쉘 보안 자체보다 쉘 보안 기술을 포함 또는 응용한 형태의 보안 시스템에 대한 특허가 일부 존재함

• 응용보안 강화 프로토콜

미국 특허는 Graphical 패스워드 인증, 임시 패스워드를 이용한 세션 인증, 패스워드 인증 정책, 경량의 패스워드 인증, 서버의 dictionary 공격 대응 방법 등 50여건 이상의 다양한 형태의 특허가 출원되었으며, 2003년 이후에 관련 특허 출원이 급증하는 추세를 보임

유럽의 경우, 패스워드 인증 자체에 대한 특허보다 패스워드 인증 방식을 포함한 보안 시스템에 대한 특허가 일부 존재하며 출원 건수가 10여개 이내로 비교적 적은 편임

일본의 경우, OTP(One Time Password) 관련 특허, 패스워드 인증 디바이스, IC 카드 또는 셀룰러 폰을 위한 패스

워드 관리 방법 등 특정 장치에 특화된 형태의 패스워드 인증 방식에 대한 특허등 약 100여개 정도의 많은 특허가 출원되고 있음

- VoIP 보안

미국과 일본의 특허는 1500여건으로 2000년 이전부터 등록되고 있어, 기술 개발이 국내보다 빨랐음을 보여주고 있음. 이중 대부분은 데이터 처리 장치, 호출 제어 장치, 어댑터 장치 등 기술 특허로, 응용 서비스 분야에 주를 이루는 국내 특허와 대비됨

- 스팸대책

미국 특허는 약 560여건이 등록되어 있으며, 이 중 기술 특허는 대부분 스팸을 탐지하는 방법, Blacklist/Whitelist 관리 방법, 스팸 방지를 위한 인증 방법 등에 관한 특허임. VoIP 또는 SIP에 국한된 특허는 10건 미만으로, 이들 분야가 스팸 관련 기술적 이슈 보다는 관리, 정책적인 이슈와 표준화에 국한되어 있음을 나타내는 것으로 해석됨

- 안전한 P2P 보안

미국에서 Microsoft, Sun Microsystems, Intel, McAfee, HP를 포함한 많은 기업들이 1,000여건을 등록/출원했으며, 일본에서는 KDDI, Microsoft, NEC, Onkyo, Fuji, Hitachi 등의 기업들이 100여건의 특허를 출원/등록한 상태임. 한편 유럽에서는 Nokia, Qualcomm, Siemens, Microsoft, Philips, British Telecom, France Telecom, Deutsche Thomson-Brandt GMBH, International Business Machines Corporation 등에서 200여건의 특허를 출원/등록해오고 있음. 특히 최근 2-3년간 P2P 기술 관련 국제특허가 급증했으며, 향후 P2P 응용 서비스가 더욱 확산 되면서 P2P 관련 특허도 지속적으로 증가할 것으로 전망됨

- IPTV 보안

미국 특허 중 IPTV를 핵심 키워드로 하고 있는 특허는 100여 건 정도이며, 이 중 암호화, 보안, 인증 등을 주제로 하는 특허는 10여 건 이내로 저조하며, 대부분 codec 및 서비스에 대한 특허임. 인터넷TV를 포함할 경우 그 수는 190건 이상으로 증가함. 동일한 검색에 조건에 의해 유럽은 20여 건, 일본은 40여 건으로 조사됨

DRM 관련 특허 중 미국 특허는 800건 이상으로, 출원인 별 분류에서는 마이크로소프트 124건, 인터트러스트 52건, 콘텐트가드 홀딩스 50건, 삼성전자 35, 노키아 24건, 소니 15건, IBM 14건 등으로 조사되었음. 출원 연도별로는 1996년부터 증가하기 시작하여 2005년에 140건까지 증가하였으나 2006년에는 70이 출원되는데 그침. 일본 특허는 112건으로 이 중 마이크로소프트 20건, 삼성전자 14건, 소니 13건, 마쓰시다 전기 7건 등으로 조사되었음. 유럽 특허는 200건으로 이 중 마이크로소프트 31건, 삼성전자 25건, 노키아 9건 등으로 조사됨

CAS 관련 특허 중 미국 특허는 660건 이상으로, 이 중 마이크로소프트 84건, 디지마크 42건, 소니 26건, 삼성전자 15건, 사이언티픽 아틀란타 15건 등으로 조사되었음. 출원 연도별로는 1994년부터 증가하기 시작하여 2000년을 전후하여 많은 출원 건수를 보이고 있으며, 2000년 이후 계속 감소 추세에 있음. 유럽 특허는 229건으로 필립스 25건, 사이언티픽 아틀란타 16건, 톰슨 멀티미디아 13건, 나그라비젼 12건, 삼성전자 12건, 프랑스텔레콤 9건 등으로 조사됨. 일본 특허는 61건으로 이 중 마쓰시다 전기 12건, 소니 10건, 사이언티픽 아틀란타 7건, 도시바 5건 등으로 조사되었음

• STC (Secure Trusted Computing)

STC와 관련하여 외국에서 출원된 특허들은 동작환경, 서명, 응용, 보증(attestation), 부트, certificate, key, physical presence, RNG(Random Number Generator), SW, T-agent, tamper-proof, TCB, TPM 등 다양한 기술들에 대한 특허들이 있음

STC 관련하여 핵심 특허들을 분석해 보면, 아래 표와 같이 IBM(27건), MS(8), Broadcom(2), TOSHIBA(2), Fujitsu(2), Sony(2), Intel(2), HP(2), 톰슨(1), SHARP(1), NTT(1), 프리시젼(1), Adventest(1), Citibank(1), HITACHI(1), 기타(18)로 나뉠 수 있음. 이를 국가별로 보면 미국이 51건으로 가장 많음. 유럽은 4건, 일본 10건, 한국은 7건임

〈표 32〉 업체별 STC 관련 특허 출원 현황

출원처	건수	출원국	출원처	건수	출원국
IBM	27	EP(1)/JP(2)/KR(3)/US(21)	톰슨	1	KR(1)
MS	8	EP(1)/KR(2)/US(5)	SHARP	1	JP(1)
Broadcom	2	EP(1)/US(1)	NTT	1	JP(1)
TOSHIBA	2	JP(2)	프리시젼	1	KR(1)
Fujitsu	2	JP(1)/US(1)	Advantest	1	EP(1)
Sony	2	US(2)	Citibank	1	US(1)
Intel	2	US(2)	HITACHI	1	JP(1)
HP	2	US(2)	기타(개인)	18	JP(2)/US(16)

• 차세대 웹 보안

웹 또는 웹서비스라는 공통된 분야에 대해서는 다수의 특허가 존재하는 것으로 파악되지만, 각 분야의 특성에 맞는 보안 관련 특허는 극히 미비한 것으로 밝혀짐. 현재까지의 주요 특허 목록은 아래와 같음 (2007. 9 기준)

〈표 33〉 차세대 웹 보안 관련 주요 특허

대분류	세부분류	출원번호	출원일자	등록번호	공고일자	출원인	발명의 명칭	진행상태	비고
웹서비스 (Web Servivces)	Security	US20040038862	2004-11-19	2005067202 (공개)	2005-07-21	ELECTRONIC DATA SYSTEMS CORPORATION	SECURE FILE TRANSFER FOR WEB SERVICE	공개	WO A1
		US20030031262	2003-10-01	2004036426 (공개)	2004-04-29	AMERICA ONLINE, INCORPORATED	WEB SERVICE SECURITY FILTER	공개	WO A1
		20040025375	2004-12-29	20050251853 (공개)	2005-11-10	MS	Automatically generating security policies for web services	공개	US A1
		20040849487	2004-05-19	20060041669 (공개)	2006-02-23	Lucent Technologies	Securing web services	공개	US A1
Web 2.0	Security	EP2006000367	2006-01-17	2006077075 (공개)	2006-07-27	GIESECKE & DEVRIENT GMBH	SUBSCRIBER CARD FOR INTERNET WEB LOG SERVICES	공개	WO A1
		US20050034141	2005-09-21	2006036785 (공개)	2006-04-06	GOOGLE, INC.	IMAGE DISTORTION FOR CONTENT SECURITY	공개	WO A1 EP A1
Semantic Web	Ontology	KR20030002896	2003-12-30	2005052720 (공개)	2005-06-09	ETRI	KNOWLEDGE MODELING SYSTEM AND METHOD USING ONTOLOGY	공개	WO A2
Web Privacy	Privacy Protection	20050072143	2005-03-04	20050172120 (공개)	2005-08-04	MS	System and method for protecting privacy and anonymity of parties of network communications	공개	USA1 외 2건 (2003, 2006)
		19991066620	1999-04-14	2000076189 (공개)	2000-03-14	CITICORP DEV CENTER INC	SYSTEM AND METHOD FOR CONTROLLING TRANSMISSION OF STORED INFORMATION TO INTERNET WEB SITE	공개	JP
Ubiquitous Web Services	Security	2002315663	2002-10-30	2004151942 (공개)	2004-05-27	RICOH CO LTD	WEB SERVICE PROVIDING DEVICE, WEB SERVICE PROVIDING METHOD AND WEB SERVICE PROVIDING PROGRAM	공개	JP
		2004319692	2004-11-02	2005166024 (공개)	2005-06-23	RICOH CO LTD	AUTHENTICATION SERVICE PROVIDING DEVICE, WEB SERVICE PROVIDING DEVICE, USER TERMINAL DEVICE, AUTHENTICATION SERVICE PROVIDING METHOD, WEB SERVICE PROVIDING METHOD, WEB SERVICE UTILIZING METHOD, AUTHENTICATION SERVICE PROVIDING PROGRAM, WEB SERVICE PROVIDING PROGRAM, WEB SERVICE UTILIZING PROGRAM, AND RECORDING MEDIUM	공개	JP
Mobile Web Service	Security	KR20000001059	2000-09-21	2001026280	2001-04-12	G.MATE, INC.	SECURITY SYSTEM AND METHOD USING MOBILE COMMUNICATION NETWORK	공개	WO A1
		2004253084	2004-05-26	1494429	2007-04-11	Nokia INC.	Method for implementing secure corporate communication	공개	EP A3
		2004253083	2004-05-26	1494428	2005-01-05	Nokia INC.	Method and apparatus for implementing secure VPN access via modified certificate strings	공개	EP A1
		20000584605	2000-05-31	07206803	2007-04-17	International Business Machines Corporation	Method and apparatus for controlling access to the contents of web pages by using a mobile security module	등록	US B1
	Mobile Web 2.0	IB2004003236	2004-10-05	2005033828	2005-04-14	Nokia INC	METHOD AND APPARATUS FOR AUTMATICALLY UPDATING A MOBILE WEB LOG (BLOG) TO REFLECT MOBILE TERMINAL ACTIVITY	공개	WO A2
총 계		16 건							

- 웹서비스 보안과 관련하여 58건 정도의 관련 특허가 있음. 등록된 특허는 웹서비스를 구축하기 위한 기반구조라기 보다는 응용 보안 서비스의 대한 내용이 대부분임
- 웹 2.0과 관련하여 다수의 특허가 존재함. 대부분의 특허는 블로그, AJAX 등의 웹 2.0 서비스와 기술 등에 대한 것임. 웹 2.0 보안과 관련한 특허는 극히 미비하며, 개념적인 제시 단계에 머물러 있음. 향후 웹 2.0 관련 특허가 다수 등록되는 만큼. 보안 관련 특허도 늘어날 것으로 예상됨. 현재까지는 구글과 아마존이 웹 2.0과 관련한 다수의 특허를 제출하고 있음
- 시맨틱 웹 및 시맨틱 웹서비스와 관련된 특허는 찾아보기 힘듦. 아직까지는 시맨틱 웹 자체가 개념적인 제시 단계에 머물러 있기 때문이라고 판단됨. 시맨틱 웹의 한 기술인 온톨로지 분야에서 약간의 특허가 검색됨
- 웹 프라이버시 보호와 직접적으로 관련된 특허를 MS에서 3건을 등록함. 이외의 다른 특허는 매우 미비하며, 웹 프라이버시에 대한 관련 특허는 찾아볼 수 없음
- 디바이스 상에서 웹서비스를 제공하고 또한, 보안 서비스를 제공하기 위한 방법에 대한 특허를 RICOH에서 JP로 등록하였음. 이외의 다른 특허는 찾아 볼 수 없음
- 모바일 웹과 관련한 특허의 출원은 대부분이 모바일 웹과 모바일 디바이스간의 통신 보안에 편중되어 있음. Nokia에서 관련 특허를 몇 건 출원하였으며, 모바일 웹과 관련한 특허 현황이 국내와 비교하여 다양하지 못한 실정임. 모바일 웹 2.0과 관련한 특허는 국내와 마찬가지로 블로그를 대상으로 서비스 특허 출원 단계에 있음

• Lawful Interception

직접적으로 LI를 특허 제목으로 지정하여 출원된 미국 특허는 총 29건이며, 이중 9건이 등록된 것으로 파악됨. 그러나 LI, Electronic Surveillance, Wiretapping 등과 같은 보다 일반적인 도청 및 감청의 범주에서의 관련 특허는 총 900여건으로 이중 600여건 등록되어 있음

LI 관련 371건 정도의 유럽 특허가 출원되어 있으며, 명시적으로 LI 자체를 다루고 있는 특허는 대략 23건 정도인 것으로 분석됨

일본특허는 광의적 의미에서의 IP 네트워크, 통신채널 상에서의 보안 관련 특허는 100여건 이상 존재하지만, LI와 직접적으로 연계성을 갖는 특허는 극히 적은 것으로 판단되며, 등록 건수는 역시 미비한 것으로 조사되었음

2.2.3. 기술개발 현황 요약

• 국내외 기술개발 관련 사항을 정리하면 다음 〈표 34〉와 같이 요약할 수 있음

〈표 34〉 기술 개발 현황 요약

구분	기술 분류	기술 개발 현황	
		국내	국외
응용보안	전자우편	운영체제 또는 웹브라우져에 탑재되어 제공되므로, 개발에 대한 수요가 많지 않음, S/MIME, PGP 등을 이용한 웹 메일 S/W 개발은 활발한 편임	기본적인 암호 서비스로 메시지 암호화 및 디지털 서명을 제공하는 제품에서부터 다른 형태로 보안 기능을 강화시킨 제품들이 출시되고 있음, S/MIME v3 및 DKIM 등의 개념을 이용한 전자우편 보안 메커니즘이 제안 및 개발되고 있는 실정임
	전자투표/공증	인터넷을 이용한 원격투표는 네트워크 취약성 등의 문제로 실험적인 단계에 머물러 있거나, 제한적인 환경에서만 실시되고 있는 상태임, 2010년 집에서 모든 투표가 가능하도록 하는 선관위 전자투표 계획이 추진 중임	이미 미국에서는 2000년 3월 아리조나주 민주당 예비선거에서 40% 이상의 인터넷 투표율을 기록한 바 있으며, 2008년 캘리포니아 주정부에서는 대통령 예비선거에서 전자투표를 활용한 계획임, 그러나 단말기, 네트워크, 서버 차원에서의 통합적인 보안 및 외부감사 요청 시 재검토 및 자료의 보전/재성 또한 가능해야하므로 매우 어려운 보안서비스 영역으로 간주되고 있음
	u지식 보안	한미 FTA 체결 이후, DRM, CAS 등의 콘텐츠 보호 솔루션 개발 및 상용화를 진행 중임, 전용 디바이스 단위로 권한 관리가 되는 DRM의 문제점 및 UCC와 같은 새로운 콘텐츠에 대한 지재적 보호 및 지분표현 기술은 미약한 수준임, 익명성 기반의 u-지식보호 기술이 필요한 실정임, 프로슈머형 지식 관련 ?허는 전무한 것으로 파악되며, 익명성 기반 u지식 보안 기술에 대한 IPR 선점이 필요함	애플사의 iPod 제품에서 재생되는 MP3 파일의 경우 DRM이 적용되고 있으나, 단일 단말에서의 재생이 허용되는 문제점으로 인해, 애플사 스스로 Non-DRM 방식으로의 전환을 시도 중이며, CAS의 경우 기존 케이블카드 또는 STB 중심에서 SW 형태로 다운로드 가능한 CAS 솔루션에 대한 연구를 OpenCable 수행하고 있음

〈표 34〉 기술 개발 현황 요약 - 계속

구분	기술 분류	기술 개발 현황	
		국내	국외
응용보안	쉘 보안	SFTP를 이용한 파일전송 프로그램과 같이 소규모의 응용 기술개발만이 이뤄짐, 독자적인 쉘 보안에 대한 개발 사례 없음, 매우 적은 수의 관련 특허가 출원된 상태임	IETF에서 관련 표준화와 더불어 SSH 프로토콜을 개선하기 위한 기술개발을 병행 중임, 쉘 보안은 이미 성숙단계에 접어든 기술이며, 강한 보안성/호환성, 구현용이성 및 수동 작업 최소화 등을 위한 추가적인 개발 작업이 이뤄지고 있음, RSA Security社에서 SSH2와 RSASecurID 솔루션 통합 제품을 개발하였고, SSH 커뮤니케이션 시큐리티社, MS, Sun Microsystems와 같은 기업에서 관련 제품을 개발 및 판매 중임
	VoIP 보안	VoIP 암호 및 키관리 기술과 관련하여 VoIP 암호화 장비로 IPSec 기반 VPN 기능을 갖는 VoIP 보안 제품이 주를 이룸. 국내에서는 2006년 2월, 인터넷전화 발신자번호를 조작하여 휴대폰 소액결제 사기범죄가 발생하였고, 대형기간사업자망에서 이동통신망으로 VoIP 스팸이 발생한 사례가 최근 불법스팸대응센터에 접수되는 등 VoIP 스팸이 사회적 문제로 등장하고 있으나, 국내 관련 기술 개발은 미비한 실정임	VoIP 데이터 보호를 위한 암호 및 키관리 기술은 표준화를 중심으로 개발 (SIP, SRTP, MIKEY 등). 대형 국외 장비 업체들은 단말에서 SRTP 프로토콜 스택을 추가하여 출시. 표준에서는 VoIP 키관리 규격으로 MIKEY를 권고. VoIP 스팸은 호 형태의 SPIT와 메신저 서비스 기반의 SPAM, 프레즌스 서비스 기반의 Presence Spam의 종류로 나누며, 기존의 이메일 · 휴대폰 스팸 대응 기술을 벤치마킹한 대응 기술이 U. North Texas, BorderWare, Facetime, Antepo 등 학계 및 산업계 중심으로 연구 중임
	스팸대책	최근 스팸 관련 국내외 기술 개발은 주로 VoIP를 중심으로 진행됨. 숭실대, KISA, ETRI에 관련 기술 및 표준화를 진행중에 있으며, 삼성네트웍스는 브로드소프트사의 브로드웍스 라는 IP centric server와 주니퍼 SBC 장비인 보이스플로우를 이용한 탐지 및 차단 솔루션을 제공. VoIP 스팸을 제외하면 기술개발 보다는 정책적인 측면에서의 스팸 방지 대책을 세우는 형태에 있으며, 이에 따라 ITU-T SG17에서 스팸 방지 가이드라인과 관련된 표준화를 진행하고, IETF에서 SIP 관련 기술 표준화를 진행하는데 초점을 맞추고 있음	VoIP 스팸 분야에 대한 연구개발이 진행 중이나, 이외의 다른 형태의 스팸 분야에서는 기술개발 보다는 스팸 방지 정책을 수립하고, 가이드라인을 제시하는 형태. VoIP 이외의 스팸 방지 분야의 기술적인 측면에 대한 논의는 IRTF의 ASRG (Anti-Spam Research Group)이 전무. 기술 특허는 대부분 스팸을 탐지하는 방법, Blacklist/Whitelist 관리 방법, 스팸 방지를 위한 인증 방법 등임
	응용보안 강화 프로토콜	TLS, 패스워드인증기술에 대한 기술이 개발중에 있음, TLS는 이미 기술개발이 완료되어 상용화된 실정임, 대략 50여건의 관련 특허가 출원중이며, 우회특허 및 개량특허 도출을 통한 IPR 확보가 요구됨	TLS의 경우 HTTPS(HTTP/TLS)를 이용한 안전한 웹서비스 제공을 위해 필수적인프로토콜로서 Apache-SSL, MS IIS, Netscape Enterprise Server 등이 이를 채용한 대표적인 제품군임, 현재 개발된 대부분의 웹브라우져는 SSL v2, SSL v3., TLS v1을 지원하고 있음, 패스워드 인증 프로토콜 관련하여 IETF, ITU-T 등에서 표준화와 더불어 기술 개발을 진행 중임

〈표 34〉 기술 개발 현황 요약 - 계속

구분	기술 분류	기술 개발 현황	
		국내	국외
응용보안	안전한 P2P 보안	KISTI, ETRI, SAIT, (주)대우정보시스템, (주)피어컴 등에서 P2P 관련 분산컴퓨팅, IPv6 기반 정보보호, 지적재산권, 모바일 등의 기술개발 연구를 수행 중임, 그 외 소리바다, 푸르나, 피투피아 등의 업체에서 파일 공유 서비스를 제공 중이며, (주)아라전자, (주)소만사에서 패킷 필터링 기술 솔루션을 제공하고 있음	MS는 2001년부터 안전한 파일공유 시스템 제공을 목적으로 Farsite라는 연구를 진행 중이며 2006년 Windows Vista에 P2P 기술을 탑재함, Sun Microsystems는 네트워크 상의 여러 디바이스를 지원하기 위한 범용 P2P 프레임워크인 JXTA를 개발하여 현재 성숙단계에 접어들고 있음, P2P 트래픽 제어와 관련하여 시만텍, 포티넷, 시큐어컴퓨팅, 주니퍼 등 보안장비 업체에서 UTM 솔루션을 제공함, 학계의 경우 UC Berkeley가 SETI@home 프로젝트를 수행하고 있으며, MIT, Purdue, Berkeley, Rice Univ.,에서 Chord, CAN, Pastry, Tapestry의 개발을 진행 중에 있음
	IPTV 보안	현재, 하나로, KT 등에서 IPTV 상용 서비스를 제공, 그러나 IPTV의 특성을 유기적으로 결합하여 반영한 보안기술에 대한 논의는 전무한 실정, 현재 DRM 적용 노력 및 CAS 채용하고 있으므로, 기술개발 보다는 서비스 운용에 초점을 맞추고 있음, 이미 NDS의 CAS 솔루션이 국내 시장을 점유하고 있는 실정이며, 이데토코리아, NDS코리아 등의 업체가 DRM과 CAS를 결합한 개발 및 시제품 출시를 진행 중, 2006년부터 ETRI에서 'ACAP 기반 IPTV용 미들웨어' 기술 개발 진행 중이며, KAIST에서 안정적인 IPTV 백본 네트워크에 대한 연구를 진행 중임, N:N 커뮤니티 환경 및 다방향 부가서비스 그리고 오버레이 기반 멀티캐스트를 지원하기 위한 추가 연구가 요구되고 있음, 현재까지 30여건의 특허가 출원 중임	2006년 세계적으로 280여개 이상의 사업자가 IPTV 서비스를 제공하고 있음, 그러나 독자적 기술 채용으로 인하여 상호 운용성을 기대하기 어려운 실정이므로, DRM 및 CAS를 적용한 보안 서비스 역시 상호 호환성이 매우 떨어지는 것으로 판단됨, HD급 고화질 서비스를 지원할 수 있는 보안기술에 대한 요구 및 연구가 진행 중임, 특히 비디오 스트림 자체를 암/복호화하는데 걸리는 시간을 줄이기 위한 노력, 공간/주파수 도메인 및 선택적 암호화 등에 대한 기초 연구가 이뤄지고 있음, 또한 Visual 암호화 및 Transparency 보장 등의 신규 보안에 대한 연구가 진행 중이나, 실제 IPTV에 적용은 이뤄지고 있지 않음
	차세대 웹 보안	웹서비스 보안과 관련하여 ETRI가 XML 전자서명, XML 암호, WS-Security, SAML , XACML, XKMS 등의 기술을 구현한 바 있음. ETRI는 유무선 웹서비스를 위한 보안 표준 기술들을 개발하였으며, 이중 모바일 웹서비스 메시지 보안 구조 표준 기술은 ITU-T SG17을 통해 표준화를 추진중임. 유선 환경에서의 웹서비스 보안 기술은 점차 확산되고 있으나 모바일 웹서비스 보안 상용 제품은 아직 드문 실정이며, 디바이스 웹서비스를 위한 보안 제품 개발은 이루어지지 않고 있음. 웹 2.0 보안 기술은 웹방화벽 개발쪽에만 집중되어 있음. 학계에서는 웹 2.0 보안 기술, 웹 프라이버시 보호 기술 등에 관한 연구가 이루어지고 있음	웹 2.0 보안 기술은 웹 어플리케이션 취약점 분석툴 및 웹방화벽 개발이 주로 이루어지고 있으며, 넷컨티넘, 임퍼바 등에서 웹방화벽을 개발함. Apache에서는 ModSecurity라는 무료 웹 방화벽을 공개하였음. Nokia 에서는 모바일 환경에서 XML 및 SOAP을 지원하고 기본적인 보안 기능 및 Liberty Alliance의 ID관리 기술을 구현한 Nokia Web Services Framework를 개발하였음. 유비쿼터스 웹 기술과 관련하여, MS는 웹서비스 기반의 디바이스 간의 연동을 위해 'Devices Profile for Web Services' 명세를 개발하고 이를 기반으로 한 제품을 개발하였으며, UPnP 포럼에서는 디바이스 간 연동시의 보안을 위해 XML 기반의 보안 스펙을 개발함. MIT CSAIL과 Nokia Research Center Cambridge는 공동으로 SwapMe라는 프로젝트를 추진중이며, 모바일 환경을 위한 시맨틱 웹 어플리케이션 플랫폼을 개발중임

〈표 34〉 기술 개발 현황 요약 - 계속

구분	기술 분류	기술 개발 현황	
		국내	국외
응용보안	신뢰 보안 서비스 (STC)	이미 HP, IBM, MS 등 여러 대형 벤더를 중심으로 Desktop과 Laptop 등의 컴퓨터 시스템을 해킹이나 유해환경으로 보호하기 위해 디바이스를 장착하여 출시되고 있으나, 국내의 경우 STC 관련 기술 개발이 이뤄지고 있지 않음	신뢰 보안과 관련하여 TCG(Trusted Computing Group)의 표준을 준수하는 TPM(Trusted Platform Module)이라는 칩을 탑재한 많은 제품들이 출시되고 있으며, 더욱 가속화될 것으로 전망됨, MS의 Windows Vista에 이러한 장치가 탑재되고 있으며, IBM 역시 자사의 노트북 TPM 칩을 장착하여 판매하고 있음, 모바일 컴퓨팅 장치에 대한 매우 효과적인 보안 방안으로 부상 중임
	Lawful Interception	ETRI에서 BcN 기술 중 NGN 보안 영역의 일부로써 ETSI와 같은 표준화 단체의 동향을 파악하고 있는 실정임, 국정원와 같은 국가기관에 공적인 목적으로 해외 감청 장비를 도입한 사례가 있음, 올해 9월 통신비밀보호버버 개정안이 국회를 통과할 경우 전기사업자 및 이통사는 수사기관의 요청을 대비하여 의무적으로 감청 시스템을 개발하여 갖추고 있어야 함, 2005년까지 총 13건의 LI 관련 특허가 등록됨, 특히 무선 및 이통통신 영역에 대한 기술개발 및 특허확보가 요구될 것으로 전망됨	ETSI 및 Atis, Cisco, Home Office UK, Verint, Utimaco Safeware AG, Nice, PenlilInk, Narus, Pine Digital Security 등의 주요 업체의 참여한 LI PlugtestsTM 시험이 2006년 3월 시행되어 표준안 유효성 검증을 수행한 바 있음, Cisco에서는 12000 Router 시리즈와 AS 5xxx 시리즈 Gateway 제품에 VoIP을 대상으로 합법적 감청을 지원하는 기능을 탑재하여 출시하고 있으며, CableLabs社 등에서는 자체 기업 기술규격을 정의하여 상용 시제품에 사용하는 등의 기술적 우위 확보를 위한 노력이 진행 중임, 또한 GSM 및 CDMA 감청 장비가 CCS International社에 의해 1996년에 시제품으로 개발/판매됨
평가인증	정보보호 평가	1998년 정보보호시스템 공통평가기준(ISO15408) 제정 및 2002년 8월 세부 평가절차를 명시한 정보보호시스템 평가/인증 지침을 개정 고시한 바 있음, 업체에서 평가제출물 작성 시 이를 가이드라인으로 삼을 것을 권고 하고 있음, 현재까지 IITA (11) 및 국가보안연구소 (3)에서 총 14개의 보호프로파일을 개발하였고, 공통평가 기준 버전 이 2.3에서 3.1으로 변경됨에 따라, 개정 작업을 진행하고 있음, 2006년 5월 국제 공통평가기준 상호인증협정국으로 가입하였고, 현재까지 총 145개의 제품을 평가한 바 있음	미국, 영국, 독일, 프랑스, 캐나다, 호주 등이 정보보호 평가 관련 선진국으로 고려될 수 있음, 미국과 캐나다 주도로 공통평가기준(CC)가 개발되어 24개 회원국에서 사용 중임 (2007년 3월), 또한 국제 공통평가기준 상호인정협정(CCRA)을 체결한 바 있음, 이를 통해 현재까지 총 672개의 보안 제품이 평가 및 인증됨, CCRA는 내부 4개 위원회(관리/집행/개발/개발실무)를 통해 보안성 평가와 관련된 문서를 개발하고 이를 ISO 표준으로 상정하려는 노력을 기울이고 있음
	보안관리	국내 환경에 적합한 정보보호관리 모델을 개발·보급하기 위해서 국내 정보보호관리체계 인증제도에 대한 연구를 2000년부터 진행하여 관련 법률(2001.7)을 개정, 인증심사기준을 고시(2002.5)하였고, 세부 심사기준 및 업무지침 등을 마련하여 2005년 11월부터 인증제도를 본격 시행. 위험분석 방법론 개발, 정보보호관리체계 수립 가이드 등을 개발·배포함. 이 가이드는 유사 제도인 ISO27001(예전 BS7799)의 기준을 모두 포괄하고 있을 뿐만 아니라 문서 중심이 아닌 기술적 관점으로 구성되어 있는 등 우수성을 인정받고 있지만, 최근 IT 환경의 급속한 환경 변화 개인정보보호 등 신규 이슈 등 기존 정보보호 패러다임이 정보보호관리 관점에서 정보보호 거버넌스로 변화되고 있는 추세이므로 이에 따른 체계적인 정보보호 거버넌스 연구가 필요하나, 국내의 선행연구 등의 노력이 부족한 실정임	정보보호관리체계 인증기술의 경우, 영국의 BSI(British Standard Institute)에서 만들어진 BS7799 영국 표준이 최초의 정보보호관리 표준임. BS7799가 ISO(17799, 27001) 표준으로 제정되었으며, 유럽과 일본을 중심으로 활성화 되어 있음. 인증기술에 대한 표준을 ISO/IEC JTC1 SC27/WG1에서 ISMS 구현가이드, ISMS 평가 방법론, 정보보호 위험관리 등 ISO27000 시리즈를 지속적으로 표준으로 제정하기 위한 작업을 진행중

2.3. 표준화 현황 및 전망

2.3.1. 국내 표준화 현황 및 전망

• 응용보안

- 전자우편

국내외 전자우편 보안 시스템간 호환성을 보장하는 표준이 인터넷보안기술포럼을 통해 6건(암호 메시지 규격, S/MIME 버전 3 인증서 운영 규격, 안전한 전자우편을 위한 보안서비스 확장, CMS에서 CAST-128 암호화 알고리즘의 사용, Diffie-Hellman 키합의 방식, S/MIME 메시지 명세서)이 제정되었으며 한국정보통신기술협회(TTA)의 단체표준으로 상정되었음. 현재 이를 기반으로 관련된 전자우편 보안 기술이 상정되고 있음. S/MIM3 관련 표준은 전자우편 보안에서 공개키기반구조(PKI)기반 인증서를 활용하여 전자서명, 암호화 서비스가 이루어지도록 PKI 관련 인증서 처리, 인증서 폐지 목록 처리 등의 기술을 명시하고 있음. 또한, '안전한 전자우편을 위한 보안서비스 확장' 표준은 우수한 보안 서비스를 제공하기 위해 서명된 영수증 (signed receipts), 보안 레이블 (security labels), 보안 메일 리스트 (secure mailing lists), 서명 인증서 (signing certificates)를 내용을 정의하고 이를 사용하기 위한 지침을 기술함으로써 전자우편을 사용하기 위한 향상된 보안 서비스를 규정하고 있으며, 이를 통해 국내외 전자우편 보안 표준과의 호환성을 확보하고 있음

- 전자투표/공증

전자투표에 관한 국내 표준이 정해진 바는 없으나 중앙선거관리위원회 및 전자선거추진협의회를 중심으로 개발되어 시험되어지고 있음. 2008년 제 18대 총선에 전자투표가 도입될 예정이며 이를 위해 선관위에서는 터치스크린 방식의 전자투표기를 총 2만대로 늘릴 예정임. 유권자의 투표편의를 획기적으로 개선시키기 위해 선거인명부가 전국망으로 공유되어 유권자들은 주소지를 벗어나 전국 어디에서나 투표할 수 있을 것으로 예상됨

- o u-지식 보안

디지털 콘텐츠 보호 기술은 서비스 도메인별로 다른 지재권 보호 체제(DRM, mDRM, CAS, CP, COI/UCI, 전자문서 보관소 등)로 운용되고 있음. 국내 DRM 표준화 활동으로는 TTA 단제 표준으로 EXIM을 표준화하여 DRM간 데이터 교환으로 상호연동이 가능한 인터페이스 규격을 제정하였으나, 서비스 사업자간 호환성과 과금 방식에 이견이 있는 상태임. 또한 KTF, SKT 등의 이동통신 사업자는 OMA DRM 2.0 기반 저작권 보호 서비스를 제공 중이나 각기 다른 도메인 간 DRM 연동과 로열티 부담의 문제가 있음

- 쉘 보안

쉘 보안 분야는 국내 독자 표준 없이 바로 국외 표준에 따라 제품 개발을 하기 때문에 현재 쉘 보안 관련 국내표준화는 진행되지 않고 있으며, 기술/제품 성숙에 따라 추가적인 표준화 요구도 없음

- 응용보안 강화 프로토콜

현재 국내에서 추진 중인 패스워드 인증 프로토콜관련 표준은 없음. 그러나, 현재 한국에서 패스워드 인증 프로토콜 가이드라인 표준을 ITU-T SG17에서 추진하고 있으며, 이 표준이 완료되면, 국내 환경에 맞게 조정하는 작업을 거

쳐 국내 표준으로 들여올 계획을 가지고 있음

TLS 보안 기술의 경우, 국내에서는 TTA에서 전송계층보안 구조의 적용 및 확장을 위한 보안 표준으로 제시하였음. 특히 무선 환경에서의 WTLS 인증서 프로파일 표준 등에 관한 내용이 표준으로 채택되었음. 그러나, 전반적으로 국내 표준인 경우 TLS에 대해서는 비교적 표준화가 미진한 상태임. 이는 국내 독자 표준 없이 바로 제품 개발이 이루어지고 있다고 판단될 수 있음

〈표 35〉 TLS 표준화 현황

구분	문서명	문서이름	제정년도	상태
TLS	TTAS.IF-RFC2830	LDAPv3 : 전송계층보안(TLS)을 위한 확장		표준
	TTAS.KO-12.0019	무선 WTLS 인증서 프로파일 표준		표준

- 스팸대책

스팸과 관련한 국내 표준화는 ETRI PEC의 활동이 중심이며, ITU-T SG17에서 스팸 대응을 위한 국제 표준화에 주력하고 있음. 현재까지 국내에서 개발하고 있는 ITU-T 국제 표준 기고서는 다음과 같음

〈표 36〉 스팸 관련 ITU-T 표준화 현황

구분	문서명	문서이름	제정년도	상태
스팸	X.gcs	Guidelines on Countering E-mail SPAM		진행
	X.ocsip	Overview of Countering SPAM for IP Multimedia Applications		진행
	X.tcs	Technical Means for Countering SPAM		진행
	X.fcs	Technical Framework for Countering E-mail SPAM		진행
	X.csreq	Requirement for Countering SPAM		진행

- 안전한 P2P 보안

현재까지 P2P 관련 국내 표준은 전무한 상태임. 이미 국내 P2P 응용 서비스 사용자 수가 수백만 명에 달하는 현실을 감안할 때, P2P의 취약한 보안성과 과다 트래픽 유발 등의 보안 문제점들을 해결하기 위해서 P2P 보안 관련 표 준 제정이 시급하다고 볼 수 있음

- IPTV 보안

최근 신규 IT 응용 분야로 급부상하고 있는 IPTV(인터넷프로토콜TV) 분야는 세계적인 표준화 가 급속도로 진행되고 있어 국내에서도 이러한 변화에 적극 대응해야 한다는 목소리가 높아지고 있음. 또한 KT, 하나TV 등이 시범 및 상용서비스를 실시하고 있고 LG는 서비스를 준비 중에 있지만, 각 IPTV 사업자별로 별도의 기준(기술)을 채택하고 있어 표준화 추진이 요구되고 있음

국내 IPTV 표준화 움직임은 ITU-T의 IPTV FG 설립과 함께 발 빠르게 진행되고 있음. 한국정보통신기술협회(TTA) 산하에 IPTV 프로젝트 그룹(PG)을 두고 IPTV 표준화 문제를 다루고 있음. IPTV 관련 표준은 비디오 및 오디오 코딩, 전송 네트워크 프로토콜, 코덱, 스트리밍 전송, 콘텐츠 보안, 맞춤형 방송 등 IPTV 서비스 전반적인 분야

에 걸쳐 진행되고 있는데, TTA는 IPTV 구조 및 시나리오 실무반, IPTV 수신기 규격 실무반, Mobile IPTV 실무반으로 구성되며, 서비스 요구사항 및 서비스 제공구조 표준화, 서비스 제공을 위한 관련 기술표준 연구, 세부 기술표준 개발, 상호 운용성 증진을 위한 표준 개발 등에 중점을 두고 있음

IPTV관련 표준화 추진체계는 정보통신부 산하 ITU-T IPTV FG 및 TTA IPTV PG를 중심으로 활발히 활동 중이며, 국내 IPTV관련 사업자, 제조업체, 학계 전문가들이 대거 참여하고 있음. 1차 ITU-T 제네바 회의에서부터 한국의 IPTV 표준화 방향 및 전략을 반영하여 국제 표준으로 상정하고자 지속적으로 노력하고 있으며, 국가 대표단을 구성하여 국가적 차원의 기고서를 제출하며, 해외 단체 및 사업자 기고서 분석을 통해 대응방안을 모색하고 전략을 수립하고 있음. 이러한 노력의 결과로 국내에서는 법령 미비로 IPTV의 도입이 지연되고 있는 상황에서도 한국의 IPTV 관련 기술은 국제표준으로 채택이 추진되고 있음. 2007년 5월에 개최된 5차 FG 회의에서 우리나라가 기고한 개방형 응용프로그램 인터페이스(오픈 API)등 IPTV관련 표준 52건 중 46건이 반영되었으며, 이에 따라 우리나라는 5차에 걸친 FG 회의에서 총 210건의 기술을 제안하여 이 중 199건이 반영되는 실적을 올렸음. ITU-T IPTV FG 작업문서와 living list로 남아있는 문서 33개 중 6개의 문서를 한국인 에디터가 작성하고 있음

〈표 37〉 ITU-T IPTV FG의 기고서

문서명	문서이름	제출자	제출일
FG IPTV-C-0823	Proposal for Retransmission of Digital Broadcasting Services over IPTV	ETRI	2007.07
FG IPTV-C-0821	Proposal for updated text of EPG Implementation Guideline	ETRI	2007.07
FG IPTV-C-0755	Description and use cases of the integrated internet services in IPTV	ETRI	2007.07
FG IPTV-C-0754	Updates on the use case of the VoD services in IPTV	ETRI	2007.07
FG IPTV-C-0753	Updates on the use case of the linear broadcast TV services in IPTV	ETRI	2007.07
FG IPTV-C-0746	Service Scenario of Service Information Guide(SIG)	ETRI	2007.07
FG IPTV-C-0744	Updated text for the definition of Presence Service on FG IPTV-DOC-0085	ETRI	2007.07
FG IPTV-C-0743	Requirements to support Multiple Service Securities	ETRI	2007.07
FG IPTV-C-0742	Proposal for Conceptual Reference Model in WG6	ETRI	2007.07
FG IPTV-C-0741	Proposal of metadata syndication capability on figure 5.3 in Service Navigation Systems (FG IPTV-DOC-0098)	ETRI	2007.07
FG IPTV-C-0688	Proposal for content delivery procedure in IPTV architecture	ETRI	2007.07
FG IPTV-C-0687	Proposed modifications to figure 18 and 19 of FG IPTV-DOC-0092	ETRI	2007.07
FG IPTV-C-0686	Requirement on Multicast VPN in IPTV Network Control Aspects	ETRI	2007.07
FG IPTV-C-0685	Addition of Annex A of Working Documents: IPTV Multicast Framework (FGIPTV-DOC-0092)	ETRI	2007.07
FG IPTV-C-0653	Considerations on personal IPTV broadcast service scenario with WG5	ETRI	2007.07
FG IPTV-C-0651	Considerations on personal IPTV broadcast service scenario with WG2	ETRI	2007.07
FG IPTV-C-0649	Detailed Architecture for the Content Preparation	ETRI	2007.07

〈표 38〉 ITU-T IPTV FG의 기고서

문서명	문서이름	제출자	제출일
FG IPTV-C-0820	Reporting Quality Scores	Korea	2007.07
FG IPTV-C-0819	Terminal Requirements for Hybrid Perceptual/Bit-Stream Models	Korea	2007.07
FG IPTV-C-0819	Requirements for Hybrid Perceptual/Bit-Stream Models	Korea	2007.07
FG IPTV-C-0817	Metadata for Hybrid Perceptual/Bit-Stream Models with embedded video quality scores	Korea	2007.07
FG IPTV-C-0816	Proposal for physical configuration of IPTV architecture	Korea	2007.07
FG IPTV-C-0815	Draft of "13 Overlay Networking" in FG IPTV-DOC-0091	Korea	2007.07
FG IPTV-C-0814	Overlay Networking Capabilities in IPTV Functional Architecture at ANNEX A (FG IPTV-DOC-0084).	Korea	2007.07
FG IPTV-C-0813	Updated proposal of personal IPTV broadcast service	Korea	2007.07
FG IPTV-C-0812	Proposed Multicast Functionalities for IPTV Multicast Framework	Korea	2007.07
FG IPTV-C-0811	Proposal of Reconstructing FG-IPTV Multicast Framework WD	Korea	2007.07
FG IPTV-C-0810	Proposed requirements for interoperability amongst multiple IPTV security technologies	Korea	2007.07
FG IPTV-C-0809	Consideration on QoE requirements for VoD trick mode in IPTV service	Korea	2007.07
FG IPTV-C-0808	Comments on the working document FG IPTV-DOC-0085	Korea	2007.07
FG IPTV-C-0807	Proposed multicast scenarios for IPTV service solutions	Korea	2007.07
FG IPTV-C-0806	Overlay multicast scheme for Internet streaming service (FYI)	Korea	2007.07
FG IPTV-C-0805	Proposed updates on Web-based IPTV Portal service scenario	Korea	2007.07
FG IPTV-C-0804	Proposal on Section 6.3 Multicast in FG IPTV-DOC-0087	Korea	2007.07
FG IPTV-C-0803	Application support functions for IPTV	Korea	2007.07
FG IPTV-C-0802	Additions to IPTV Functional Architecture for 3rd Party Application	Korea	2007.07
FG IPTV-C-0801	Updated texts for IPTV Multicast in Core Node on FG IPTV-DOC-92	Korea	2007.07

〈표 39〉 ITU-T IPTV FG의 기고서

문서명	문서이름	제출자	제출일
FG IPTV-C-0731	Proposed Text for Network Performance Monitoring	ICU	2007.07
FG IPTV-C-0727	Discussion issues about Web-based IPTV Portal service scenario with WG6	ICU	2007.07
FG IPTV-C-0726	Discussion issues about Web-based IPTV Portal service scenario with WG5	ICU	2007.07
FG IPTV-C-0725	Discussion issues about Web-based IPTV Portal service scenario with WG4	ICU	2007.07
FG IPTV-C-0724	Discussion issues about Web-based IPTV Portal service scenario with WG3	ICU	2007.07
FG IPTV-C-0723	Discussion issues about Web-based IPTV Portal service scenario with WG2	ICU	2007.07
FG IPTV-C-0652	Considerations on personal IPTV broadcast service scenario with WG4	ICU	2007.07
FG IPTV-C-0735	Requirement on the locator for IPTV	hanarotelecom, TVSTORM	2007.07
FG IPTV-C-0734	Proposal for a gap analysis among the existing middleware standards	TVSTORM	2007.07
FG IPTV-C-0733	Proposal for integrated service navigation system as a realization reference model	TVSTORM	2007.07
FG IPTV-C-0732	Comments on FG IPTV- DOC-0097	hanarotelecom	2007.07
FG IPTV-C-0779	Additional Proposal on Presentation Engines in IPTV Service Requirements	Samsung Electronics	2007.07
FG IPTV-C-0634	Additional Proposal on TD-HN interface of IPTV end systems	Samsung Electronics	2007.07

〈표 40〉과 〈표 41〉은 ITU-T IPTV FG의 작업문서와 living list로 남아있는 문서 중 2007년 7월 현재 한국인 에디터가 작성하고 있는 문서 목록임

〈표 40〉 ITU-T IPTV FG의 작업문서 (2007년 7월)

문서명	문서이름	에디터
FG IPTV-DOC-0124	IPTV multicast frameworks	Yeong-il Seo (KT) Juyoung Park (ETRI) YoungHwan Kwon (ICU)
FG IPTV-DOC-0146	Working Document: IPTV Multimedia Application Platforms	Kyunghee Ji (TVSTORM)

〈표 41〉 ITU-T IPTV FG의 living list (2007년 7월)

문서명	문서이름	에디터
FG IPTV-DOC-0133	IPTV service requirements	Jun Kyun Choi (ICU)
FG IPTV-DOC-0135	Service scenarios for IPTV	Hyojin Park
FG IPTV-DOC-0141	IPTV network control aspects	Dae Gun Kim (KT) Peilin Yang (Huawei, 중국)
FG IPTV-DOC-0142	IPTV multicast frameworks	Shin-Gak Kang (ETRI)

TTA는 Mobile IPTV 국내 및 국제표준화 작업도 진행 중에 있는데, Mobile IPTV란 기존 IPTV 개념에 이동성 기능

을 추가시킨 개념으로서, 다양한 무선기술을 이용하여 이동 환경에서도 텔레비전/비디오/텍스트/그림 등의 양방향 멀티미디어 서비스를 자유롭게 제공하는 기술을 말함. 여기에는 삼성전자를 주축으로 LG전자, 디지캡, 알티캐스트, 넷앤티비 등의 관련사에서 표준화 작업에 참여하고 있음

〈표 42〉 ITU-T IPTV FG에 제안된 Mobile IPTV 관련 기고서

문서명	문서이름	제출자	제출일
FG IPTV-C-0636	Requirements for supporting Mobility	Samsung Electronics	
FG IPTV-C-0635	Requirements for Mobile IPTV Terminal Devices	Samsung Electronics	2007.07
FG IPTV-ID-0038	IPTV: Mobile Scenario and Architecture	Samsung Electronics	2006.07

- STC (Secure TC)

국내에서는 현재까지의 활동은 없었고, 무선인터넷포럼과 TTA를 통하여 2007년부터 연구를 시작할 예정임

◦ 표준화 작업 주요 참여 기업 및 기관

· ETRI

· (스프레드텔레콤, 프롬투)

· (표준화가 본격적으로 추진되면 보다 많은 업체들이 참여할 것으로 예상됨)

◦ STC 관련 국내 표준화 문건

· 지금까지 신뢰 보안 서비스에 관해 국내 표준화는 진행된 바가 없음.

- 차세대 웹 보안

국내는 웹서비스 보안과 관련하여 TTA가 주요한 표준화 기구로서 활동 중이며, 이밖에 전자상거래 표준화 통합 포럼 (ECIF), 유비쿼터스 웹 포럼 등에서도 관련 표준화를 추진하고 있음.

◦ TTA의 웹 프로젝트 그룹 (PG401)에서는 시맨틱 웹, 웹서비스, XML 등의 웹 기반 기술 표준 개발, 모바일 웹 및 유비쿼터스 웹 응용 표준 개발, 웹 2.0 기술 표준 개발 등을 수행하고 있음

◦ TTA의 전자거래 프로젝트 그룹 (PG403)에서는 전자거래 메시징 기술 표준 개발, 전자거래 협업 프로토콜 기술 표준 개발, 전자거래 적합성 및 상호운용성 기술 표준 개발 등을 수행하고 있음.

◦ TTA의 인터넷 보안 프로젝트 그룹 (PG102)은 전자우편 및 전자상거래 보안 기술 표준 개발, 네트워크 레벨 정보보호 표준 개발, 응용 레벨 정보보호 표준 개발 등을 수행하고 있음.

◦ 유비쿼터스 웹 포럼은 TTA의 IT 표준화 전략포럼의 일환으로 웹서비스 및 SOA에 대한 기술, 표준, 정책 연구와 협의를 수행하고 있음.

◦ 전자상거래 표준화 통합 포럼 (ECIF) 산하 전자거래기반 기술위원회에서는 보안인증 워킹 그룹을 구성하여 XML 및 웹서비스 정보보호 기술의 표준화 현황 파악과 기술 개발, 산업 분야 적용을 논의하고 있음.

◦ 2005년부터 ETRI에서는 유비쿼터스 웹서비스 표준화 연구를 통해 유비쿼터스 웹서비스 핵심 표준 기술, 유비쿼터스 웹서비스 연동 표준 기술, 모바일 웹서비스 핵심 표준 기술, 유무선 웹서비스 보안 표준 개발 등을 수행하고 있음.

〈표 43〉 웹서비스 보안 관련 국내 표준화 문건

구분	표준화 기구	문서번호	문서이름	상태	발표월일
웹서비스 정보보호	TTA	TTAS.IF-RFC3075	확장성 생성 언어 전자서명 구문과 처리	V1.0.0	2004.12.23
		TTAS.IF-RFC3076	정규 XML 버전 1.0	V1.0.0	2004.12.23
		TTAS.IF-RFC3741	배제 정규 XML 버전 1.0	V1.0.0	2004.12.23
		TTAS.KO-10.0214	웹서비스 메시지 보안 제품에 대한 평가 가이드라인	V1.0.0	2006-12-27
		TTAS.OT-10.0075	웹서비스 보안: SAML 토큰 프로파일 1.1	V1.0.0	2006-12-27
		TTAS.OT-10.0076	웹서비스 보안: 첨부를 갖는 SOAP 메시지 프로파일 1.1	V1.0.0	2006-12-27
		TTAS.KO-10.0168	XML Signature/Encryption 적합성 및 상호운용성 평가	V1.0.0	2004-12-23
		TTAS.KO-10.0166	XACML 적합성 및 상호운용성 평가	V1.0.0	2004-12-23
		TTAS.KO-10.0167	XKMS 적합성 및 상호운용성 평가	V1.0.0	2004-12-23
		TTAS.KO-10.0185	확장성 생성언어 암호 구문과 처리	V1.0.0	2005-12-21
		TTAS.OT-10.0042	SAML 구문과 프로토콜	V1.0.0	2005-12-21
		TTAS.KO-10.0187	확장성 생성언어 전자서명을 위한 복호화 변환	V1.0.0	2005-12-21
		TTAS.OT-10.0041	SAML 바인딩과 프로파일	V1.0.0	2005-12-21
		TTAS.KO-10.0186	확장성 생성언어 암호 요구사항	V1.0.0	2005-12-21
		TTAS.OT-10.0040	확장성 접근제어 생성언어	V1.0.0	2005-12-21
		TTAE.OT-12.0005	웹 서비스 보안 : SOAP 메시지 보안 1.1	V1.1.0	2006-12-27
		TTAE.OT-12.0006	웹 서비스 보안 X.509 인증 토큰 프로파일 1.1	V1.1.0	2005-12-21
		TTAE.OT-12.0004	웹 서비스 보안 유저네임토큰 프로파일 1.1	V1.1.0	2005-12-21

2005년부터 ETRI에서는 유비쿼터스 웹서비스 표준화 연구를 통해 유비쿼터스 웹서비스 핵심 표준 기술, 유비쿼터스 웹서비스 연동 표준 기술, 모바일 웹서비스 핵심 표준 기술, 유무선 웹서비스 보안 표준 개발 등을 수행하고 있음. 아직까지 웹 2.0 보안, 시맨틱 웹 및 시맨틱 웹서비스 보안, 유비쿼터스 웹 보안 등에 관한 표준화가 이루어지지 않았음

- Lawful Interception

국내는 합법적인 감청과 관련하여 TTA가 주요한 표준화 기구로서 활동 중임. 한국 대표 표준화 기관으로 TTA는 GSC(Global Standards Collaboration)이라는 이름으로 90년대 초반 미국, 유럽, 일본, 호주, 한국, 캐나다 등 6개국이 참여 중인 표준화 기구(PSO: Participating Standardization Organization)에 참가하고 있으며, 특히 NGN(Next Generation Networks)와 관련된 사항들 중 주요협력분야(HIS: High Interest Subject)로서 Lawful/legal interception에 대한 초기적인 논의가 제7차 GSC 회의에서 진행된 바 있음. 본 세부분야에서 논의된 작업범위는 다음과 같음

◦ Target network and law enforcement agency간의 새로운 Packet based transport handover interface 정의

◦ Signaling과 Multimedia stream을 포함한 새로운 데이터 요소를 포함하기 위한 기존의 Intercept related information의 개선

◦ 모든 관련 이슈들에 대한 Technical solutions 고려

현재 TTA에 LI와 관련하여 국내 표준으로 상정 또는 채택한 문건은 IMT2000(W-CDMA)과 관련된 총 3건이며 본 문건들은 ETSI, 3GPP 등의 국제 표준화 단체의 표준 문건을 국내 표준으로 채택하였거나 이를 바탕으로 작성된 문건임

◦ IMT2000 3GPP - 그룹 서비스와 시스템 형태; 보안; 합법적 도청 요구사항

◦ IMT2000 3GPP - 보안 - 합법적 감청 구조 및 기능

◦ IMT2000 3GPP - 그룹 서비스와 시스템 gudxol 보안; 합법적 도청을 위한 Handover Interface

〈표준화 작업 주요 참여 기업 및 기관〉

◦ LG전자(주), 전파연구소, (주)LG텔레톰, (주)머큐리, (주)현대시스콤, SK텔레콤

◦ 루슨트테크놀러지스(주), 삼성전자(주), 한국전자통신연구원, KTF(주), (주)새롬기술

◦ KTICOM(주), 한국퀄컴, 데이콤, 한국통신, LG정보통신, 대우통신, 모토로라반도체통신

◦ 신세기통신, 하나로통신, 한국통신프리텔, 한솔엠닷컴, LG정보통신, LG텔레컴, SK텔레컴

〈표 44〉 LI 관련 국내 표준화 문건

구분	표준화 기구	문서번호	문서이름	상태	발표월일
LI	TTA	TTAE.3G-33.106	Technical Specification Group Services and System Aspects; 3G Security; Lawful Interception Requirements	V5.0.0	2002.10.28
		TTAE.3G-33.107	Security-Lawful Interception Architecture and Functions	V3.0.0	2000.7.13
		TTAE.3G-33.108	Technical Specification Group Services and System Aspects; 3G Security; Handover Interface for Lawful Interception	V5.0.0	2002.10.28

지금까지 IMT2000 영역에 편중된 표준화 작업만이 이루어져, IP 기반의 VoIP, email 등과 같은 서비스 환경에 대한 LI 표준안 부재의 문제점을 안고 있음

• 평가인증

- 보안관리

국내 보안관리 관련 표준 또는 지침 작성은 한국정보통신기술협회(TTA)에서 제정하는 정보통신단체표준, 정보통신부에서 제정하는 한국정보통신표준(KICS), 기술표준원에서 제정하는 한국산업규격(KS)로 구성되어 있음. TTA에서는 정보보호관리와 관련하여 정보보호관리표준, 위험분석방법론 모델, 정보시스템 구축준비 단계의 보안지침서, 정보시스템 비상계획 및 재해복구에 관한 지침서, 컴퓨터 바이러스 방지 지침 등 5건의 단체표준을 고시하였음. 정보보호평가와 관련하여 국제공통평가기준 1, 2, 3부를 표준화하였고 보호프로파일 및 보안목표명세서 작성법을 제정 중에 있음. KICS에서도 정보보호관리 관련 7 종의 보안관리 지침서를 제정하였으나 대부분 1996년도 이전에 작성된 것임. KS에서는 정보보호관리 관련 국제표준인 ISO13335의 1-4부를 KS화 하였고, ISO17799 역시 KS화 하여 총 5건의 KS가 있음. 정보보호평가 관련하여 CC 1-3부를 KS화 하여 총 3건의 KS가 있음

2.3.2. 국외 표준화 현황 및 전망

• 응용보안

- 전자우편

IETF smime 작업반은 RSA 사의 주도로 만들어진 인터넷 전자우편 보안 표준인 S/MIME 버전 2를 수용하여 RFC로 발표하고, 바로 이어 메시지 양식, 처리 절차, 보안성 등을 개선하고 새로운 기능을 추가하기 위한 버전 3 개발 작업에 착수한 이래, S/MIME 메시지 형식과 처리, 인증서 처리, 추가로 도입되는 암호 알고리즘들(IDEA, SKIPJACK, PBE, CAST-128), Diffie-Hellman 알고리즘 관련 사항, 강화된 보안 서비스, 전자서명 정책, 도메인 보안 서비스 등을 규정하고 있음. S/MIME은 안전한 MIME 데이터를 송수신할 수 있는 일관성 있는 방법을 제공함. S/MIME는 기존의 메일 사용자 에이전트에 의하여 사용되며, 송수신되는 메일에 암호학적 부가 기능을 제공할 수 있음. CMS는 암호학적 메시지 구문으로써, 이 구문은 임의의 메시지 내용을 암호화하고, 인증하고, 서명하고, 메시지 다이제스트 하는데 사용됨. CMS는 데이터를 보호하기 위한 캡슐화 구문을 제공하며, 디지털 서명과 암호를 지원함. 이 구문은 다중의 캡슐화를 지원하며, 서명 시간과 같은 다양한 속성을 지원함. 또한 다양한 인증서 기반 키 관리를 위한 구조를 지원함. 표준 문서는 암호 및 인증 알고리즘, 메시지 타입, 인증서 처리, 보안, 정책, 공격 등으로 구분됨. 한편, ITU-T SG17 연구과제 17에서는 스팸메일에 관한 표준을 ETRI 주도하에 개발하고 있음

〈표 45〉 스팸메일 표준 문서

권고번호	권고명 (주제)	에디터
X.csreq	Requirement on countering spam	H.W. Luo,J. Chen
X.fcs	Technical framework for countering e-mail spam	K. Yang
X.gcs	Guideline on countering e-mail spam	S.G. Kang, Y.X. Li
X.ocsip	Overview for countering spam for IP multimedia application	S.G. Kang
X.tcs	Technical means for countering SPAM	TBD

〈표 46〉 S/MIME 표준 문서

구분	문서명	문서이름	발표월일
암호 및 인증 알고리즘	RFC 4490	Using the GOST 28147-89, GOST R 34.11-94,GOST R 34.10-94, and GOST R 34.10-2001 Algorithms with Cryptographic Message Syntax (CMS)	2006
	RFC 4056	Use of the RSASSA-PSS Signature Algorithm in Cryptographic Message Syntax (CMS)	2005
	RFC 4010	Use of the SEED Encryption Algorithm in Cryptographic Message Syntax (CMS)	2005
	RFC 3565	Use of the Advanced Encryption Standard (AES)Encryption Algorithm in Cryptographic Message Syntax (CMS)	2003
	RFC 3657	Use of the Camellia Encryption Algorithm in CMS	2004
	RFC 3560	Use of the RSAES-OAEP Key Transport Algorithm in Cryptographic Message Syntax (CMS)	2003
	RFC 3537	Wrapping a Hashed Message Authentication Code (HMAC) key with a Triple-Data Encryption Standard (DES) Key or an Advanced Encryption Standard (AES)Key	2003
	RFC 3394	Advanced Encryption Standard (AES) Key Wrap Algorithm	2002
	RFC 3370	Cryptographic Message Syntax (CMS) Algorithms	2002
	RFC 3278	Use of ECC Algorithms in CMS	2002
	RFC 3211	Password-based Encryption for SMS	2001
	RFC 3185	Reuse of CMS Content Encryption Keys	2001
	RFC 3217	Triple-DES and RC2 Key Wrapping	2001
	RFC 2984	Use of the CAST-128 Encryption Algorithm in CMS	2000
	RFC 2631	Diffie-Hellman Key Agreement Method	1999
	RFC 3058	Use of the IDEA Encryption Algorithm in CMS	2001
	RFC 2876	Use of the KEA and SKIPJACK Algorithms in CMS	2000
메시지 타입, 암호학적 구문, 메시지 명세	RFC 4853	Cryptographic Message Syntax(CMS) Multiple Signer Clarification	2007
	RFC 4134	Examples of S/MIME Messages	2005
	RFC 3852	Cryptographic Message Syntax (CMS)	2004
	RFC 3851	S/MIME Version 3.1 Message Specification	2004
	RFC 3274	Compressed Data Content Type for Cryptographic Message Syntax (CMS)	2002
	RFC 3369	Cryptographic Message Syntax	2002
	RFC 2633	S/MIME Version 3 Message Specification	1999
	RFC 2630	Cryptographic Message Syntax	1999
	RFC 2311	S/MIME Version 2 Message Specification	1998
	RFC 2440	OpenPGP Message Format	1998
	RFC 3126	Electronic Signature Formats for long term electronic signatures	2001
강화된 보안 서비스	RFC 2634	Enhanced Security Services for S/MIME	1999
	RFC 3183	Domain Security Services using S/MIME	2001
	RFC 3156	MIME Security with OpenPGP	2001
인증서 처리	RFC 4262	X.509 Certificate Extension for Secure/Multipurpose Internet Mail Extensions (S/MIME) Capabilities	2005
	RFC 3850	S/MIME Version 3.1 Certificate Handling	2004
	RFC 2632	S/MIME Version 3 Certificate Handling	1999
	RFC 2312	S/MIME Version 2 Certificate Handling	1998
정책	RFC 3114	Implementing Company Classification Policy with the S/MIME Security Label	2002
	RFC 3125	Electronic Signature Policies	2001
공격	RFC 3218	Preventing the Million Message Attack on CMS	2001
	RFC 2785	Methods for Avoiding the 'Small-Subgroup' Attacks on the Diffie-Hellman Key Agreement Method for S/MIME	2000
객체 전달	RFC 3855	Transporting S/MIME Objects in X.400	2004
	RFC 3854	Securing X.400 Content with S/MIME	2004

- 전자투표/공증

전자투표에 대해서는 아직 국 · 내외적으로 표준화된 바는 없으나 현재 각국에서 실험적으로 개발 및 시행되고 있음. 표준화에 대한 연구는 IEEE 산하 SCC 38 위원회(Standard Coordinating Committee 38)에서 진행 중이며, 표준화 과제를 크게 두 개로 나뉘어(P-1622: Voting Equipment Electronic Data Interchange standard, P-1583: Voting Equipment Standard) 진행 중이지만 2005년 이후로 새로운 활동이 없어 표준화 노력은 미미하다고 할 수 있음

- o u-지식 보안

국제 디지털 콘텐츠 보호 기술 (지재권보호 기술)은 DRM, CAS, 복제 방지(CP) 분야에 대해서는 현재 MPEG, OMA 등 국제 표준화 단체를 중심으로 기술표준화가 진행중임

◦ 저작권 보호기술 분야는 MPEG-21, OMA, DVB-CPCM, DHWG, TV-Anytime, IDRM, SDMI, OeBF, XrML, ODRL에서 추진중

◦ 디지털 방송 & 셋탑박스 분야 (CAS 포함)는 OpenCable POD Copy Protection (케이블방송), ATSC CA (지상파), DVB-CA, ISMACrypt 에서 추진중

- 쉘 보안

IETF secsh 작업반은 원격 로그인, 파일 전송, X11 세션, 기타 TCP/IP 세션을 안전하게 지원하기 위한 보안 쉘인 SSH 프로토콜을 개량하고 표준화하는 것을 목표로 작업해 왔음. 보안 셸은 rsh, rlogin, rcp, telnet, rexec, rcp, ftp 등을 대치하며, 모든 트래픽을 암호화하고 다양한 수준의 사용자 인증 기능을 제공함. 현재는 SSH 버전 2 프로토콜에 대해 강한 보안성 제공과 확장성(scalability) 향상, 기존 인증서 구조 활용, 명료하고 구현하기 쉬운 명세서 개발, TCP/IP나 다른 전송 프로토콜 상에서도 작동 등을 목표로 작업 중임. 현재 13개의 RFC가 완료된 상태이며, "SSH File Transfer Protocol" 에 대한 1개의 internet draft가 상정된 상태임

〈표 47〉 쉘 보안 관련 국외 표준, IETF secsh WG

구분	문서명	문서이름	상태	발표월일
SSH	RFC 4250	The Secure Shell (SSH) Protocol Assigned Numbers	표준	2006.1.
	RFC 4256	Generic Message Exchange Authentication For The Secure Shell Protocol (SSH)	표준	2006.1.
	RFC4255	Using DNS to Securely Publish Secure Shell (SSH) Key Fingerprints	표준	2006.1.
	RFC 4254	The Secure Shell (SSH) Connection Protocol	표준	2006.1.
	RFC 4253	The Secure Shell (SSH) Transport Layer Protocol	정보	2006.1.
	RFC 4252	The Secure Shell (SSH) Authentication Protocol	표준	2006.1.
	RFC 4251	The Secure Shell (SSH) Protocol Architecture	표준	2006.1.
	RFC 4344	The Secure Shell (SSH) Transport Layer Encryption Modes	표준	2006.1.
	RFC 4335	Secure Shell (SSH) Session Channel Break Extension	표준	2006.1.
	RFC 4419	Diffie-Hellman Group Exchange for the Secure Shell (SSH) Transport Layer Protocol	표준	2006.3.
	RFC 4462	Generic Security Service Application Program Interface (GSS-API) Authentication and Key Exchange for the Secure Shell Protocol	표준	2006.5.
	RFC 4716	The Secure Shell (SSH) Public Key File Format	표준	2006.11.
	RFC 4819	Secure Shell Public-Key Subsystem	표준	2007.3.

- VoIP 보안

VoIP 보안과 관련된 표준화는 ITU-T와 IETF를 중심으로 진행 중이며, 각 단체의 활동 내역은 다음과 같음

◦ ITU-T 표준그룹의 VoIP 보안 관련 표준화 현황

· H.235에서 H.245 logical channel signaling procedure를 사용하는 모든 H-series protocol (H.310, H.323, H.324)에서 사용 가능한 전반적인 보안에 관한 프레임웍을 규정하고, 호환성을 위한 프로파일을 제공. 현재 버전 3(2003년 5월 표준화)까지 나왔으며, 관련된 보안 프로파일들은 다음과 같음

· Baseline security profile : 일반적인 H.323 시스템의 보안을 정의하고 기본적인 인터넷전화 기능을 갖는 단말(SET: Simple Endpoint Type)의 보안 기능 제시

· Signature security profile : PKI(Public Key Infrastructure)를 기반으로 X.509 인증서 및 전자서명 방식을 이용함

· Hybrid security profile : 전자의 두 가지 방식을 혼합한 형태

◦ 미디어 스트림의 기밀성을 보장하기 위한 Voice encryption option은 Baseline/Signature security profile과 함께 적용될 수 있음. 이 방식에서는 H.225.0 채널을 통해 키를 교환하게 되고 H.245 호 제어 채널을 통해 키 분배를 하게 됨

◦ 보안을 담당하는 Q.17/17에서는 SG17 내에 연구주제로 스팸을 선정(05.10)하여 Q.15/13 NGN security WG과 결과물을 공유할 예정이며, 2006년 연내에는 이메일 스팸에 대한 대응 가이드라인을 제시하기로 하였으며, 향후 VoIP 스팸으로 영역을 확장할 것으로 보임[12)]

◦ ITU-T SG17

· X.ocsip : Overview of Countering spam for IP multimedia application

· X.fcsip : Framework of countering IP multimedia spam

◦ IETF 표준그룹의 VoIP 보안 관련 표준화 현황

· H.323과 달리 SIP 프로토콜 자체는 IP 기반의 멀티미디어 통신을 위한 완벽한 시스템 기능을 정의하지는 않고 있으며, 새로운 기술을 개발하기보다는 기존의 보안 메커니즘을 적용하고 있음

· SIP에서 제공하는 정보보호 기술로 사용자 인증을 위한 HTTP 인증, 홉간 보안을 위한 TLS, 양단간 보안을 위한 S/MIME 등을 사용하며, 미디어 트래픽 보호를 위해 SRTP 기술을 쓰는 추세이며, 키 관리를 위해서는 MIKEY가 표준화 진행 중임 (〈표 48〉 참조)

12) ITU-TSG17 / Q국제 표준 개발 로드맵 : Guideline for countering email SPAM(Xgcs) : '06년까지 개발할 예정

〈표48〉 SIP 보안 기술

구분	기술 설명	보안 기능
HTTP 인증	HTTP에서 사용되는 인증방법으로 Digest 인증만을 사용하며, 재사용 공격방지와 인증 기능을 제공함 (RFC 2617)	사용자 인증
TLS (Transport Layer Security)	- SIP 메시지에 대한 암/복호화를 통하여 홉간 신뢰구간을 형성하며 SIP 메시지의 기밀성과무결성을 제공함 - SIP 서버에서는 TLS 기능을 반드시 지원해야 하나 단말은 옵션임 - TLS는 TCP 기반 SIP에만 적용가능하며, IPSec은 TLS 대신 (RFC 2401) 사용해도 되지만 TLS처럼 의무사항은 아님 (RFC 2246, RFC 3546)	홉간 보안
S/MIME (Secure/ Multipurpose Internal Mail)	- 종단간 SIP 사용자에게 보안기능을 제공하고, 메시지에 대한 기밀성, 무결성과 상호 인증 기능을 제공함 (RFC 2633, RFC 3261)	양단간 보안

· SRTP(Secure RTP, RFC 3711)

- VoIP 미디어 스트림의 기밀성을 보장하기 위한 IETF 표준 프로토콜로, H.235와 SIP 기반 VoIP 음성정보를 전달하는 RTP/RTCP에 대한 암호화 기술로 적용
- SRTP는 RTP/RTCP payload에 대한 암호화 기능을 지원하며, 전체 RTP 패킷에 대한 인증 기능을 수행함으로써 RTP 패킷에 대한 재생 공격(Replay Attack)을 방지할 수 있음
- SRTP 프로토콜 내에서 암호화를 수행하기 위한 알고리즘은 AES를 사용하며, Counter Mode를 적용하여, 실시간 암호화 패킷 전송을 지원함
- SRTP 패킷 전송을 위한 암호화 키는 MIKEY 키관리 프로토콜을 적용하여 양 단말 간에 공유하지만, MIKEY 키관리 프로토콜은 표준 초안 단계로써 실용화를 위해서는 검증이 필요함

· MIKEY(Multimedia Internet KEYing, RFC3830)

- 기존의 키 관리 프로토콜인 IKE, TLS 등의 문제점을 해결하며, VoIP에서 멀티미디어 세션을 위한 IETF 키관리 프로토콜로 현재 거의 표준완료 단계임
- 실시간 멀티미디어 어플리케이션을 위한 안전한 키 관리 기법으로 일대일 통신, 그룹 통신에서 이용되며, 유무선 통합 환경의 실시간 데이터 전송에 적합하게 설계되었음
- MIKEY에서는 4가지 키관리 모드로, Null(no encryption), Pre-shared Key, PKI, Diffie-Hellman 가 있으며, Pre-shared Key와 Diffie-Hellman 방식을 결합한 방식과 SIP call forwarding 시나리오에 적합한 방식, ECC(Elliptic Curve Cryptography)을 지원하는 방식 등이 Draft로 나와 있음

· DTLS(Datagram TLS, RFC 4347)

- 기존의 TLS가 TCP에서 동작하는데 비해, UDP 데이터그램 전송에 적합하도록 고안됨
- 기존의 TLS은 TCP 기반으로 신뢰성은 제공하나, 지연시간을 유발하는 반면, UDP 기반의 DTLS은 실시간 보안통신에 적합하며, 아직까지 국내 VoIP 장비는 TCP보다는 UDP기반으로 동작하고 있음
- 서비스 거부 공격방지를 위해서 상태가 없는 쿠키(stateless cookie) 교환이 이루어지고 메시지 단편화 및 재조합이 제공됨

· ZRTP(Extensions to RTP for Diffie-Hellman Key Agreement for SRTP)

- SRTP 세션을 수립하는데 필요한 Diffie-Hellman 키 교환 방법을 위한 RTP헤더의 확장으로 현재 IETF에서

표준화 작업 진행 중

- 공개키 알고리즘임에도 불구하고 PKI(Publick Key Infrastructure)를 필요로 하지 않으며, 짧은 인증 스트링을 사용하여 Man-in-the-middle 공격을 차단함

· SIPPING WG과 SIP WG에서 VoIP 스팸 관련 정의와 기술적 대응범위를 정의하고 있으며, 스팸을 근절하기 위한 근본적 대책으로 SIP 프로토콜 인증헤더 확장을 통한 발송자 인증 기술에 대해 활발히 논의 중임

- 'Framework for anti-spam in SIP(Draft-ietf-sipping-spam-01)' 에서는 SIP 기반 VoIP 스팸 대응이 단일 솔루션만으로 해결하기 어려우며, 강력한 인증방식(HTTP Digest authentication, TLS, Private Extensions to SIP for Asserted Identity within Trusted Networks, Draft-ietf-sip-identity-05) 기반의 화이트 리스트 및 동의 기반 시스템 연계를 통한 대응 방법을 권고하고 있음
- SIP 헤더의 From 필드 값 조작을 통한 발신자 익명성 문제를 근본적으로 차단하여 VoIP 스팸 발생을 근절하는 방안을 위한 표준화 논의가 IETF SIP WG에서 진행 중임

· Starting with SPITSTOP BoF(January, 2007)

- Signaling to Prevent SPIT Reference Scenario
- SIP Extensions for SPIT Identification
- Authorization Policies for Preventing SPIT
- A Document Format for Expression Anti-SPIT Authorization Policies

· IRTF ASRG (Internet Research Task Force, Anti-Spam Research Group)

- IRTF 내 스팸 대응을 위한 TF로써, 2003년 3월 시작됨
- 스팸 대응을 위한 기술적 방안을 논의하고 이를 IETF 표준화로 제정하는 역할

· Privacy mechanism for SIP(RFC 3323)

- 사용자 레벨과 네트워크 레벨의 프라이버시 서비스를 정의하고 있으며, 프라이버시 보호를 위해 익명성, 메시지 암호화, 네트워크 구조 은닉, 인증 등의 기술을 적용할 것을 권고
- 프라이버시 보호를 위한 고려사항 및 기존기술의 활용에 중점을 두고 있으며, 프라이버시 정책 운용 및 관리에 대한 규격이 미흡하여 실제 환경에 적용하기에는 어려움

· IETF geopriv(Geographic Location/Privacy) WG에서 물리적 위치에 데이터 포맷, 위치정보 전달 절차, 위치정보에 대한 프라이버시 보호 표준화를 추진 중임

- RFC 3693, Geopriv requirements
- RFC 3694, Threat analyusis of the geopriv protocol
- RFC 3825, Dynamic Host Configuration Protocol Option for Coordinate-based Location Configuration Information
- RFC 4079, Presence Architecture for the Distribution of GEOPRIV Location Object
- RFC 4119, A Presence-based GEOPRIV Location Object Information Format

· 최근까지 업체 주도로 다양한 형태의 제품이 개발되어 왔으나, 2006년 3월 IETF speermint(Session Peering for

Multimedia Interconnect) WG이 창설되어 SBC에 대한 표준화 활동을 시작

- draft "SPEERMINT Requirement and Terminology" : SIP 기반 세션 peering 요구사항과 용어정의
- draft "SPEERMINT Peering Architecture"
- draft "SPEERMINT Routing Architecture Message Flows"
- draft "SPEERMINT Requirements for SIP-based VoIP Interconnection"
- draft "SPEERMINT Terminology"
- draft "SIP Peering Use Case for VSPs(VoIP service providers)"

· SBC의 주요기능 중 하나인 NAT/FW 통과 해결을 위한 관련된 국제 표준에는 STUN, TURN, ICE, MIDCOM 등이 있으나, 시장에서의 적용은 매우 미흡한 실정임

- 스팸대책

IETF의 SIPPING WG는 SIP 또는 SIP 응용 서비스와 관련된 요구사항을 표준화 하고 있고, SIP WG는 SIP 프로토콜과 관리 분야에서 음성 스팸 차단 관련 표준화를 진행중에 있음

〈표 49〉 IETF SIPPING 관련 문서

구분	문서이름	상태
IETF SIPPING	Signaling to Prevent SPIT Reference Scenario	진행
	SIP Extensions for SPIT Identification	진행
	Authorization Policies for Preventing SPIT	진행
	A Document Format for Expression Anti-SPIT Authorization Policies	진행

IETF MARID(Mail Transfer Authorization Records in DNS) WG는 메일 전송자를 검증하기 위한 DNS 기반의 메커니즘 관련 표준화임. 현재 활동이 중단되었으며, 다수의 기고서가 있고 산출된 RFC는 없음

〈표 50〉 IETF MARID 관련 문서

구분	문서이름	상태
IETF MARID	SMTP Service Extension for Indicating the Responsible Submitter of an E-mail Message	ID
	Sender ID: Authenticating E-Mail	ID
	Client SMTP Validation (CSV)	ID
	Client SMTP Authorization (CSA)	ID
	Domain Name Accreditation (DNA)	ID
	Behind The Curtain: An Apology for Sender ID	ID
	The SPF Record Format and Test Protocol	ID
	The SPF Record Format and Sender-ID Protocol	ID
	Purported Responsible Address in E-Mail Messages	ID
	Authorizing Use of Domains in MAIL FROM	ID

ITU-T는 NGN security 가이드라인 내에 스팸에 대한 언급이 있으며 SG 17내에 스팸 대응 가이드라인을 포함한 다수의 표준화가 진행중에 있음

- 응용보안 강화 프로토콜

응용보안 강화 프로토콜에 대한 표준화는 ITU-T SG17 WP2에서 연구과제 5와 9에서 추진되고 있음. ITU-T SG17 연구과제 9에서는 안전한 패스워드 인증 프로토콜(SPAK: Secure Password-based Authentication protocol with Key Exchange) 가이드라인에 대한 표준화가 추진 중에 있음. 연구과제 5에서는 SPAK 프로토콜 중의 하나인 PAK(Password-Authenticated Key Exchange)에 대한 표준화와 EAP기반의 인증 및 키관리 프레임워크(Framework for EAP-based authentication and key management) 에 대한 표준화가 진행 중임

SPAK 가이드라인에 대한 표준은 2005년 10월 제네바 회의에서 "안전한 패스워드 인증 프로토콜 가이드라인"에 대한 기고서가 한국에서 제안되어 권고안 후보로 채택됐고, 이후 표준화 작업이 진행 중에 있음. 안전한 패스워드 프로토콜 가이드라인의 경우, 표준의 범위는 일반 요구사항, 프로토콜 요구사항, 취약성 분석, 선택 기준, 그리고 안전성 분석 등으로 구성돼 있음

PAK 표준은 연구과제 5에서 미국 루슨트에서 PAK에 대한 기고서가 2006년 1월 SG17 WP2 인터림 회의에 제출되어 표준화 항목으로 채택되었고, 2007년 4월 회의에서 표준화 제정이 완료됨. PAK 표준은 프로토콜의 구체적인 동작 과정과 이 프로토콜이 갖는 특성을 다루고 있음. PAK 프로토콜은 상호 인증과 세션키 공유가 가능한 프로토콜이며, 중간자 공격을 막을 수 있고, 재생 공격을 예방할 수 있지만, 서버 타협 공격을 막을 수 없는 단점이 있음. 그러나 이 표준 역시 다양한 보안 수준을 요구하는 애플리케이션에 이용될 수 있음

현재 ITU-T 외에 ISO/IEC, IETF에서도 관련 표준화가 진행 중임. One-Time Password의 경우는 IETF에서 표준화가 진행 중에 있으며, 현재 관련 RFC 3건이 등록되어 있음

〈표 51〉 응용보안 강화 프로토콜 관련 국제 표준

구분	표준기구	문서명	문서이름	상태	발표월일
패스워드 인증	ITU-T	X.1035		표준	2007.4.
	ITU-T	X.sap-1	Guideline on secure password-based authentication protocol with key exchange (updated 1st draft recommendation)	표준	2007.4.
	IEEE	P1363.2	The PAK suite: Protocols for Password-Authentication Key Exchange	표준	2002.4
	IETF	internet-draft	Password-Authenticated Diffie-Hellman Exchange (PAK)	표준	2007.7
	IETF	RFC1938/2289	A One-Time Password System	표준	1997.11
	IETF	RFC2243	OTP Extended Responses	표준	1998.2
	IETF	RFC2444	The One-Time-Password SASL Mechanism	표준	1998.10

IETF의 tls 작업반은 트랜스포트 계층 상위에서의 기밀성, 인증, 무결성 구현 방법 제공을 목표로 표준화 작업을 수행하고 있으며, 넷스케이프 SSL을 기초로 하고 있음. 이 작업반은 기존의 TLS 프로토콜을 진화시키며, 다양한 암호 알고리즘이 TLS에 사용되도록 각종 암호 스위트들을 규정하고 있음

〈표 52〉 TLS 표준 문서

구분	문서번호	제 목	발표월일	상 태
프로토콜	RFC 2246	The TLS Protocol Version 1.0	1999	Proposed Standard
	RFC 2817	Upgrading to TLS Within HTTP/1.1	2000	Proposed Standard
	RFC 2818	HTTP Over TLS	2000	Informational
	RFC 3456	Transport Layer Security Extension	2003	Proposed Standard
	RFC 3749	Transport Layer Security Protocol Compression Methods	2004	Proposed Standard
	RFC 4346/2246	The Transport Layer Security (TLS) Protocol Version 1.1	2004.4.	표준
	RFC 4346/3546	Transport Layer Security (TLS) Extensions	2006.4.	표준
사이퍼스위트	RFC 2712	Addition of Kerberos Cipher Suites to Transport Layer Security (TLS)	1999	Proposed Standard
	RFC 3268	AES Ciphersuites for TLS	2002	Proposed Standard
	RFC 3749	Transport Layer Security Protocol Compression Methods	2004.5.	표준
	RFC 4132	Addition of Camellia Cipher Suites to Transport Layer Security (TLS)	2005.7.	표준
	RFC 4279	Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)	2005.12.	표준
	RFC 4492	Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)	2006.5.	정보

- 안전한 P2P 보안

P2P 관련 표준화 활동은 IETF와 ITU-T와 같은 국제 표준화 기구들과 Sun Microsystems와 같은 기업들을 중심으로 이루어지고 있음

우선, ITU-T SG-17의 Question 9/17에서는 2005년에 시작된 두 개의 P2P 보안 분야의 표준화 프로젝트, X.p2p-1과 X.p2p-2가 현재까지 진행 중에 있음. X.p2p-1은 P2P 보안을 위한 요구사항에 관한 것으로 일본 측에서 수행하고 있으며, X.p2p-2는 P2P 보안을 위한 세부 기술에 관한 것으로 ETRI에서 담당하고 있음. 양 프로젝트에서 한국, 중국, 일본의 적극적인 참여 속에 표준화 작업이 꾸준히 진행되고 있음

〈표 53〉 P2P 보안 관련 국제 표준 - ITU-T

구분	표준기구	문서명	문서이름	상태	발표월일
P2P 보안	ITU-T	X.p2p-1	Security requirements for P2P communications	진행	
	ITU-T	X.p2p-2	Security architecture and operations for peer-to-peer network	진행	

IETF에서는 XMPP, SIMPLE, P2PSIP 등의 워킹그룹들이 P2P 관련 표준화 작업을 진행하고 있거나 종결한(XMPP) 상태이며, IRTF의 P2PRG 연구그룹에서도 표준화 작업의 기초를 제공하기 위한 연구를 진행하고 있음. 그러나 P2P 정보보호 기술에 대한 것은 초보적인 단계로 기존 정보보호 프로토콜을 적용하는 단계에 머무르고 있는 실정임

XMPP(Extensible Messaging and Presence Protocol)는 인스턴트 메신저의 표준을 제정하기 위한, 현재는 종료된 워킹그룹으로써 인스턴트 메시징과 현재 위치인식을 지원하기 위한 XML 기반의 프로토콜의 표준화 작업을 수행하

였음. 인스턴트 메신저에 채널 및 개체 암호를 지원하기 위한 security 기능이 추가된 프로토콜을 개발하여 4건의 RFC를 등록하였음

〈표 54〉 P2P 보안 관련 국제 표준 - IETF XMPP WG

구분	표준기구	문서명	문서이름	상태	발표월일
P2P 보안	IETF	RFC 3920	Extensible Messaging and Presence Protocol(XMPP): Core	제정	2004
	IETF	RFC 3921	Extensible Messaging and Presence Protocol(XMPP): Instant Messaging and Presence	제정	2004
	IETF	RFC 3922	Mapping the Extensible Messaging and Presence Protocol(XMPP) to Common Presence and Instant Messaging(CPIM)	제정	2004
	IETF	RFC 3923	End-to-End Signing and Object Encryption for the Extensible Messaging and Presence Protocol(XMPP)	제정	2004

SIMPLE(SIP for Instant Messaging and Presence Leveraging Extensions)은 인스턴트 메신저 서비스의 표준화를 위해 구성된, 현재 진행 중인 워킹그룹으로 SIP를 이용하여 인스턴트 메신저 서비스를 제공할 수 있도록 하는 관련 표준 작업을 수행하고 있음. 현재까지 등록된 14건의 RFC는 다음과 같음

〈표 55〉 P2P 보안 관련 국제 표준 - IETF SIMPLE WG

구분	표준기구	문서명	문서이름	상태	발표월일
P2P 보안	IETF	RFC 3856	A Presence Event Package for the Session Initiation Protocol (SIP)	제정	
	IETF	RFC 3857	A Watcher Information Event Template-Package for the Session Initiation Protocol (SIP)	제정	
	IETF	RFC 3858	An Extensible Markup Language (XML) Based Format for Watcher Information	제정	
	IETF	RFC 3994	Indication of Message Composition for Instant Messaging	제정	
	IETF	RFC 4481	Timed Presence Extensions to the Presence Information Data Format (PIDF) to Indicate Status Information for Past and Future Time Intervals	제정	
	IETF	RFC 4480	RPID: Rich Presence Extensions to the Presence Information Data Format (PIDF)	제정	
	IETF	RFC 4482	CIPID: Contact Information in Presence Information Data Format	제정	
	IETF	RFC 4479	A Data Model for Presence	제정	
	IETF	RFC 4662	A Session Initiation Protocol (SIP) Event Notification Extension for Resource Lists	제정	
	IETF	RFC 4661	An Extensible Markup Language (XML) Based Format for Event Notification Filtering	제정	
	IETF	RFC 4660	Functional Description of Event Notification Filtering	제정	
	IETF	RFC 4827	An Extensible Markup Language (XML) Configuration Access Protocol (XCAP) Usage for Manipulating Presence Document Contents	제정	
	IETF	RFC 4826	Extensible Markup Language (XML) Formats for Representing Resource Lists	제정	
	IETF	RFC 4825	The Extensible Markup Language (XML) Configuration Access Protocol (XCAP)	제정	

P2PSIP(Peer-to-Peer Session Initiation Protocol)는 중앙서버보다는 단말 집합체에 의해서 세션의 설치 및 관리가 처리되는 SIP 세션 이용을 위한 메커니즘과 가이드라인을 제정하기 위하여 표준화 작업을 진행중에 있음. 아직까지 RFC는 나오지 않았고 현재 등록된 드래프트 1건으로 아래와 같음

〈표 56〉 P2P 보안 관련 국제 표준 - IETF P2PSIP WG

구분	표준기구	문서명	문서이름	상태	발표월일
P2P 보안	IETF		Concepts and Terminology for Peer to Peer SIP	진행	2007

P2PRG(P2P Research Group)는 P2P 네트워크 구성, 확장성, 상호 운용성, 보안성 등의 광범위한 P2P 주제에 대한 연구를 수행하기 위한 포럼을 제공함. 향후 IETF에서 P2P 관련 워킹그룹을 구성할 수 있도록 연구결과를 제공하는 것을 목적으로 함

한편 Sun Microsystems에서 개발 중인 공개 P2P 프로토콜 프레임워크인 JXTA는 2002년 IETF에서 표준화 시도가 불발되었지만, 현재도 누구나 참여할 수 있는 공개된 개발 환경 하에서 지속적인 연구가 진행되고 있음

- IPTV 보안

2006년 조사에 따르면, 세계적으로 280여개 이상의 사업자가 IPTV 시범 및 상용서비스를 제공하고 있지만 현재 각 IPTV 사업자별로 별도의 기준을 채택하고 있어 ITU-T를 비롯 여러 표준화단체들이 각 분야별 표준 기술을 추진하고 있음

현재 가장 활발하게 움직임을 보이고 있는 표준단체는 ITU-T로 AT&T, NTT 등 통신사업자뿐 아니라 루슨트, 노텔, 시스코 등의 벤더들이 글로벌 표준화를 요구함에 따라 2006년 4월 첫 미팅을 거쳐 IPTV 포커스그룹(FG)를 설립했음. 이후에 IPTV FG는 IPTV에 적용될 수 있는 표준 전반에 대해 검토한 뒤 2007년 7월 현재까지 5번의 회의를 열어 IPTV 표준화를 진행하고 있음. 2007년 7월까지 800여개의 기고서가 상정되었으며, 이를 통하여 20개의 작업문서가 제정되었으며 (〈표 56〉 참고), 13개의 문서가 living list로 남아있는 상태임 (〈표 58〉 참고). 이 포커스그룹은 1년 정도 활동하면서 기본적 요구사항, 서비스 시나리오, 정책 및 표준화 방향, IP망 기능구조, 시스템 운용 및 과금/인증, 응용서비스 및 코덱, 구현방법과 QoS에 대한 표준화 작업을 수행하는 것을 목표로 하고 있음. 보안 관련 문서로는 "IPTV Security Aspects (FG IPTV-DOC-0140)"가 유일한데, 이 문서에서는 일반적인 보안 요구사항과 아키텍처를 정의하고 있으며, 구체적인 보안 메커니즘은 TBD로 남아있음. IPTV 서비스에 따른 요구사항의 구체화, 아키텍처의 세분화, 그리고 보안 메커니즘의 정의는 향후 SG13/SG17을 통해 완료될 예정에 있음

〈표 57〉 ITU-T IPTV FG의 작업문서 (2007년 7월)

문서명	문서이름	에디터
FG IPTV-DOC-0114	IPTV services requirements	Mr. Clive Miller (Acting), Royal National Institute of Blind People
FG IPTV-DOC-0115	IPTV architecture	Mr. Jincheng LI, Huawei Mr. Kai WEI, CATR
FG IPTV-DOC-0116	Service scenarios for IPTV	Mr. Mingdong LI, ZTE
FG-IPTV-DOC-0117	Gap analysis	Mr. Julien Maisonneuve, Alcatel-Lucent
FG IPTV-DOC-0118	Quality of experience requirements for IPTV	Mr. Akira Takahashi, NTT
FG IPTV-DOC-0119	Traffic management mechanism for the support of IPTV services	Mr Osama Aboul-Magd, Nortel
FG IPTV-DOC-0120	Application layer reliability error recovery mechanisms for IPTV	Mr. Thomas Stockhammer, Digital Fountain
FG IPTV-DOC-0121	Performance monitoring for IPTV	Mr. Danny Wilson, Pixelmetrix Corporation
FG IPTV-DOC-0122	IPTV security aspects	Ms. Wei XIE, CATR
FG IPTV-DOC-0123	IPTV network control aspects	Linli Lu, Alcatel Shanghai Bell Mr. Peilin Yang, Huawei
FG IPTV-DOC-0124	IPTV multicast frameworks	Mr.Yeong-il Seo, KT Mr. Juyoung Park, ETRI Mr. YoungHwan Kwon, ICU
FG IPTV-DOC-0125	Aspects of IPTV end system ? terminal device	Mr. Michael Shannon, Scientific Atlanta
FG IPTV-DOC-0126	Aspects of home network supporting IPTV services	Mr. Gale N. Lightfoot, Jr., Scientific Atlanta Mr. Yoshinori Goto, NTT Mr. Jianting Meng, China Telecom
FG IPTV-DOC-0127	Working Document: IPTV Middleware, Applications, and Content Platforms	Mr. Christian Bertin, France Telecom
FG IPTV-DOC-0128	Working Document: Toolbox for Content Coding	Mr. Richard Nicholls, Dolby Laboratories
FG IPTV-DOC-0129	Working Document: IPTV Middleware	Quan Wang, UTStarcom Damien Alliez, NDS France
FG IPTV-DOC-0130	Working Document: Service Navigation System	Menghua Tao, China Netcom Group Hongqi Liu, China Netcom Group
FG IPTV-DOC-0131	Working Document: IPTV Metadata	Yasuaki Yamagishi, Sony
FG IPTV-DOC-0146	Working Document: IPTV Multimedia Application Platforms	Ms. Kyunghee Ji, TVSTORM
FG IPTV-DOC-0132	IPTV vocabulary of terms	Mr. Ghassem Koleyni, Nortel

〈표 58〉 ITU-T IPTV FG의 living list (2007년 7월)

문서명	문서이름	에디터
FG IPTV-DOC-0133	IPTV service requirements	Mr. Jun Kyun Choi, ICU
FG IPTV-DOC-0134	IPTV architecture	Mr. Jincheng LI, Huawei Mr. Kai WEI, CATR
FG IPTV-DOC-0135	Service scenarios for IPTV	Ms. Hyojin Park
FG IPTV-DOC-0136	Quality of experience requirements for IPTV	Mr. Kenneth Toney, Tektronix
FG IPTV-DOC-0137	Traffic management for IPTV	Mr. Ning Zong, Huawei
FG IPTV-DOC-0138	Application layer reliability solutions for IPTV	Mr. Thomas Stockhammer, Digital Fountain
FG IPTV-DOC-0139	Performance monitoring for IPTV	Mr. Danny Wilson, Pixelmetrix Corporation
FG IPTV-DOC-0140	IPTV security aspects	Ms. Wei XIE, CATR
FG IPTV-DOC-0141	IPTV network control aspects	Mr. Dae Gun Kim, KT Mr. Peilin Yang, Huawei
FG IPTV-DOC-0142	IPTV multicast frameworks	Mr. Shin-Gak Kang, ETRI
FG IPTV-DOC-0143	Aspects of IPTV end system ? terminal device	Mr.Gale N. Lightfoot, Jr., Scientific Atlanta Mr. Yoshinori Goto, NTT Mr. Jianting Meng, China Telecom
FG IPTV-DOC-0144	Aspects of home network supporting IPTV services	Mr. Gale N. Lightfoot, Jr., Scientific Atlanta Mr. Yoshinori Goto, NTT Mr. Jianting Meng, China Telecom
FG IPTV-DOC-0145	IPTV middleware, application and content platforms	Mr. Christian Bertin, France Telecom

1993년부터 정식 활동을 시작한 디지털 방송 표준인 DVB 프로젝트는 2000년부터 방통 융합 표준화를 시작하여 2005년 3월에 IP망을 이용한 통신 및 방송 서비스에 관한 규정을 ETSI TS 102 034문서로 공시바 있음. DVB의 IPTV 표준은 가전사, 시스템/서비스/네트워크 제공자 등을 중심으로 한 상업분과 (CM; Commercial Module) 서브 그룹에서 요구사항을 도출하고, 기술분과 (TM; Technical Module) 서브 그룹에서 표준화를 담당함. 이중 CM계열의 CM-IPTV (sub-group on IP Television)와 TM계열의 TM-IPI(IP Infrastructure)가 대표적인 IPTV 워킹 그룹이며, IETF, DLNA(Digital Living Network Alliance), TVA (TV Anytime Forum), Pro-MPEG Forum, 그리고 ATIS와 같은 단체와 동맹하여 최적화된 표준안을 도출하고 있음

이외에도 IETF에서 멀티캐스트 전송 및 보안, MPEG에서 코덱 및 멀티미디어 프레임워크, ISMA에서 인터넷 스트리밍, TVA에서 맞춤형방송 등의 표준화 단체들도 각 분야별 기술의 표준화를 추진하고 있음

- STC (Secure TC)

TCG에서 IBM, HP, MS, 후지쯔 등 대형 업체를 중심으로 이와 관련한 표준화를 진행하고 있음. TCG에서 진행하고 있는 워킹그룹들은 TPM, Mobile, TNC (Trusted Network Connect), Server, Storage, PC Client, Hard Copy, TSS (TCG Software Stack) 등 많은 분야를 포함함. 현재 TPM 관련한 표준은 TPM v1.2까지 제정되어 있는 상황임

◦ TCG (Trusted Computing Group)는 TPM (Trusted Platform Module)이라는 하드웨어를 기반으로 신뢰 컴퓨팅 및 보안 기술에 대한 산업 표준을 개발, 정의 및 활성화하는 표준화 기구임

◦ 1999년 Intel, AMD, IBM, HP 및 MS가 단말 사용자의 데이터를 보호하고, 네트워크에서 신뢰성있는 거래의 확보를 위해 하드웨어를 기반으로 하는 안전한 컴퓨팅 환경 개발을 목표로 TCPA (Trusted Computing Platform Alliance)를 설립함

◦ 최근 컴퓨팅 기술의 발전, 개방형 네트워크 기술의 발전에 따라 사용자 컴퓨터의 위협 요인은 더욱 증가하는 추세이며, 더욱 신뢰성있는 컴퓨팅 환경의 요구에 따라 더욱 많은 컴퓨터 회사와 소프트웨어 회사들이 TCPA의 제안을 수용함으로써 2003년에 TCG로 확대됨

◦ 현재 Promoter(8), Contributor(84), Adopter(62) 를 포함하여 154개의 회원을 가지고 있고, 매년 증가하는 추세임. ETRI는 Contributor로 회원 가입이 되어 있음. 국내에서는 ETRI와 삼성이 Contributor로 등록은 되어 있지만, 삼성은 현재 적극적인 활동은 하고 있지 않은 상태임

◦ TCG는 TPM WG, MP WG, Authentication WG, TSS WG, Storage WG, TNC WG 등 다양한 분야에서의 신뢰보안을 위한 표준화를 진행 중임

〈표 58〉 STC 관련 국제 표준화 기구별 기술 문건

구분	표준화 기구	문서번호	문서이름	상태	발표월일
STC	TCG	-	TPM Design Principles		
		-	Structures of the TPM		
		-	TPM Commands		
		-	TCG Software Stack Specification		
		-	TCG TNC Architecture for Interoperability		
		-	TCG TNC IF-IMC Specification		
		-	TCG TNC IF-IMV Specification		
		-	TCG Mobile Reference Architecture		2007.6.
		-	Mobile Trusted Module Specification		2007.6.
		-	TCG Credential Profiles Specification		
		-	Security Qualities Schema Specification		
		-	Verification Result Schema Specification		
		-	TCG Storage Architecture Core Specification		2006.9.
		-	TCG EFI Protocol Specification		
		-	TCG EFI Platform Specification		

- 차세대 웹 보안

차세대 웹 보안 표준화와 관련하여 주요하게 활동 중인 표준화 단체는 아래와 같이 요약될 수 있음

◦ ITU-T (International Telecommunication Union)

◦ OASIS (Organization for the Advancement of Structured Information Standards)

◦ W3C (World Wide Web Consortium)

◦ OMA (Open Mobile Alliance)

대표적인 국제 표준화 기구인 ITU-T SG17의 Q.9에서 웹서비스 정보보호 표준화를 수행하고 있으며, X.1141 (SAML 2.0), X.1142 (XACML 2.0)에 대한 표준화를 2006년 완료하였음

ITU-T SG17에서 2007년 4월에 모바일 웹서비스를 위한 메시지 보안 구조 (X.websec-3)에 대한 표준 문서 개발이 승인되어 개발되고 있으며, 2007년말 승인 예정임. 따라서 모바일 단말을 포함한 다양한 디바이스로 구성된 환경에서의 보안 서비스가 웹서비스 보안 기술 기반으로 개발될 것으로 전망됨

웹서비스 보안의 기반이 되는 Web Services Security: SOAP Message Security 1.1 (WS-Security 2004) 명세가 2006년 OASIS에서 표준화가 완료되었으며, 산업체의 공동 작업을 통해 개발된 WS-SecurityPolicy, WS-SecureConversation, WS-Trust 등의 명세들이 OASIS에 상정되어 표준화 되고 있음

W3C에서는 XML 전자서명, XML 암호, XKMS (XML Key Management Specification) 의 표준화를 완료하였으며, WS-Policy 1.5, P3P 1.1의 표준화를 진행하고 있음

◦ W3C의 시맨틱 웹 워킹그룹에서 시맨틱 웹 관련 표준 개발을 담당하고 있으나, 시맨틱 웹 보안, 시맨틱 웹서비스 보안 등의 표준화는 아직 시작되지 않았음

◦ W3C의 유비쿼터스 웹 어플리케이션 워킹그룹에서는 유비쿼터스 웹 보안 관련 표준화를 담당하고 있으나 아직 유비쿼터스 웹 보안 기술 표준화는 진행되지 않고 있음

OMA는 WAP Forum, SyncML Initiative 등 여러 모바일 관련 단체를 통합하여 2002년에 설립된 조직으로, 모바일 서비스를 위한 표준화 작업을 수행함. OMA의 Mobile Web Services WG에서는 무선 디바이스가 OMA 아키텍처 상에서 웹서비스 응용을 수행할 수 있도록 하기 위해 관련 연구와 표준화 작업을 진행 중으로, OMA Web Services Enabler (OWSER) Core Specification 1.1, OMA Web Services Enabler (OWSER) Network Identity Specification 1.0 등에 모바일 웹서비스 보안을 위한 기본적인 명세가 포함되어 있음

웹 2.0 보안과 관련하여 OWASP (Open Web Application Security Project)에서 Ajax를 비롯한 Rich Interface 기술들에 대한 보안 가이드라인을 개발하고 있으며, 웹 2.0 보안과 관련된 표준화 활동은 세계적으로 아직 시작 단계임

〈표 60〉 국제 표준화 기구별 기술 문건 - ITU-T

구분	표준화 기구	문서번호	문서이름	상태	발표월일
웹서비스 보안	ITU-T	X.1141 (X.websec-1)	Security Assertion Markup Language 2.0 (SAML 2.0)	제정	2006.4
		X.1142 (X.websec-2)	eXtensible Access Control Markup Language 2.0 (XACML 2.0)	제정	2006.4
		X.websec-3	Security Architecture for message security in mobile Web Services	Final Draft	2007.9

〈표 61〉 국제 표준화 기구별 기술 문건 - OASIS

구분	표준화 기구	문서번호	문서이름	상태	발표월일
웹서비스 보안	OASIS	-	Web Services Security: SOAP Message Security 1.1	제정	2006.
		-	WS-SecurityPolicy v1.2	제정	2007
		-	Web Services Federation Language (WS-Federation) 1.2	Draft	2007
		-	WS-SecureConversation 1.3	제정	2007
		-	WS-Trust 1.3	제정	2007
		-	XACML 2.0 Core: eXtensible Access Control Markup Language (XACML) Version 2.0	제정	2005.2
		-	Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0	제정	2005.3
		-	Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0	제정	2005.3
		-	Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0	제정	2005.3

〈표 62〉 국제 표준화 기구별 기술 문건 - W3C

구분	표준화 기구	문서번호	문서이름	상태	발표월일
웹서비스 보안	W3C	-	XML-Signature Syntax and Processing	제정	2001
		-	Canonical XML 1.0	제정	2001.3
		-	Exclusive XML Canonicalization Version 1.0	제정	2002.7
		-	XML Encryption Syntax and Processing	제정	2002.12
		-	Decryption Transform for XML Signature	제정	2002.12
		-	XML Key Management Specification (XKMS 2.0)	제정	2005.06
		-	XML Key Management Specification (XKMS 2.0) Bindings 2.0	제정	2005.06
		-	Web Services Policy 1.5 ? Framework	제정	2007
		-	Web Services Policy 1.5 ? Attachment	제정	2007
		-	The Platform for Privacy Preferences 1.1 (P3P1.1) Specification	Working Group Note	2006

〈표 63〉 국제 표준화 기구별 기술 문건 - OMA

구분	표준화 기구	문서번호	문서이름	상태	발표월일
모바일 웹서비스 보안	OMA	-	OMA Web Services Enabler (OWSER):Core Specifications, Approved Version 1.1	Standard	2006
		-	OMA Web Services Enabler (OWSER):Overview, Approved Version 1.1	Standard	2006
		-	OMA Web Services Enabler (OWSER) Best Practices: WSDL Style Guide	Standard	2006

- Lawful Interception

합법적 감청 분야에서 주요하게 활동 중인 표준화 단체는 아래와 같이 요약될 수 있음

◦ ETSI(European Telecommunications Standards Institute)

◦ ATIS(Alliance for Telecommunications Industry Solutions)

◦ TIA(Telecommunications Industry Association)

◦ 3GPP(3rd Generation Partnership Project)

◦ IETF(Internet Engineering Task Force), CISCO

ETSI 등 국제 표준기구 및 미국 ATIS 등 국가 표준기구에서는 사용자의 개인 통신 비밀이 보장되는 환경에서 이러한 국가의 요구를 수용할 수 있도록 장비 제조업자와 서비스 공급자들이 표준 기술 개발을 위하여 노력하고 있음. 현재 국제 표준기구로는 ETSI가 주도적 역할을 하며 LI에 관한 표준을 개발 중임

ETSI는 보안 문제를 다루는 TC SEC(Security)에서 LI 작업반을 두어 표준을 개발중에 NGN(Next Generation Network)으로의 발전, 이동/무선망의 고려 등 기술적 이슈가 많아지자, TC SEC LI를 TC LI로 독립시켜 표준개발을 진행하고 있음. TC LI는 3GPP나 TETRA(TErrestrial Trunked RAdio) 등 특정 망 서비스에 대한 LI 이슈들을 각 그룹들과 협력하여 풀고 있음. ETSI 표준 문건은 크게 다음과 같이 세 가지 유형으로 분류 될 수 있음

1) LI 전반적인 요구사항 정의 관련 표준

2) Handover Interface 및 기능 모듈 관련 표준

3) Network & Service Specific 기능 관련 표준

미국의 LI 표준을 주도하는 ATIS PTSC의 표준화가 NGN 망에서의 이슈 해결 방향으로 진행되고 있음

IETF는 자체적으로 "IETF Policy on Wiretapping (RFC2804)"문건을 2000년 5월 달에 출판한 바 있음. Cisco는 자사 라우터 및 게이트웨이에 LI 기능을 탑재하는 작업과 동시에 IETF 표준화 작업을 2003년도에 활발히 진행한 바 있는데, 이때 "Cisco Architecture for Lawful Intercept in IP Networks (RFC3924)"가 10월에 출판되었으며, SNMPv3를 위한 MIB를 정의한 "Draft-baker-slem-mib-00.txt"을 제안되었음. Cisco의 상기 문건은 IP 네트워크에서 운용되는 장비에 LI 지원 메커니즘을 탑재하기 위한 방법론을 기술하고 있음

〈표64〉 국제 표준화 기구별 기술 문건 1

구분	표준화 기구	문서번호	문서이름	상태	발표월일
LI	ETSI	TS 102 232	Telecommunications security; Lawful interception; Handover specification for IP delivery	V1.1.1	2004.2
		TS 102 233	Telecommunications security; Lawful interception; Service specific details for E-Mail delivery	v1.1.1	2004.2
		TS 102 234	Telecommunications security; Lawful interception; Service specific details for Internet Access Services	v1.1.1	2004.11
		TS 101 671	Telecommunications security; Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic	V2.8.1	2003.11
		TS 101 331	Telecommunications security; Lawful Interception (LI); Requirements of Law Enforcement Agencies	V1.1.1	2001.8
		TS 133 106	Universal Mobile Telecommunications System (UMTS); 3G Security; Lawful interception Requirements	V5.1.0	2002.9
		TS 133 107	Universal Mobile Telecommunications System (UMTS); 3G Security; Lawful interception Architecture and Functions	V5.6.0	2003.9
		TS 133 108	Universal Mobile Telecommunications System (UMTS); 3G security; Handover interface for Lawful Interception (LI)	V5.6.0	2003.12
		EG 201 040	Terrestrial Trunked Radio (TETRA); Security; Lawful Interception (LI) interface; Feasibility study report	V1.1.1	1998.4
		EG 201 781	Intelligent Networks (IN); Lawful Interception	V1.1.1	2000.7
		EN 301 040	Terrestial Trunked Radio (TETRA); Security; Lawful Interception (LI) interface	V2.0.0	1999.6
		ES 101 909-20.1	Cable IP Handover for Voice and Multimedia	V0.0.11	2002.11
		ES 101 909-20.2	Cable IP Handover for data		
		ES 201 158	Telecommunications Security; Lawful Interception (LI); Requirements for Network Functions	V1.2.1	2002.4
		ES 201 671	Telecommunications Security; Lawful Interception (LI); Handover Interface for the Lawful Interception of Telecommunications Traffic (revised version).	V2.1.1	2001.9
		ES 201 733	Electronic Signature Formats	V1.1.3	2000.5
		ETR 331	Security Techniques Advisory Group (STAG); Definition of user requirements for lawful interception of telecommunications; Requirements of the law enforcement agencies		1996.12
		ETR 363	Digital cellular telecommunications system; Lawful Interception requirements for GSM (GSM 10.20 version 5.0.1)		1997.1
		TR 101 514	Digital Cellular telecommunications sytem (Phase 2+); Lawful Interception requirements for GSM (GSM 01.33 version 7.0.0 Release 1998)	V8.0.0	2001.5
		TR 101 750	Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Security; Studies into the Impact of lawful interception	V1.1.1	1999.11
		TR 101 772	Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; Service independent requirements definition; Lawful interception - top level requirements	V1.1.2	2001.12
		TR 101 876	Telecommunications security; Lawful Interception (LI); Description of GPRS HI3	V1.1.1	2001.1
		TR 101 943	Telecommunications Security; Lawful Interception (LI); Concepts of Interception in a Generic Network Architecture.	V1.1.1	2001.7

〈표 65〉 국제 표준화 기구별 기술 문건 2

구분	표준화 기구	문서번호	문서이름	상태	발표월일
LI	ETSI	TR 101 944	Telecommunications Security; Lawful Interception (LI); Issues on IP Interception.	V1.1.2	2001.12
		TR 102 053	Telecommunications security; Lawful Interception (LI); Notes on ISDN lawful interception functionality	V1.1.2	2001.12
		TR 141 033	Digital cellular telecommunications system (Phase 2+); Lawful Interception requirements for GSM (3GPP TR 41.033 version 5.0.0 Release 5)	V5.0.0	2002.6
		TS 101 040	Terrestrial Trunked Radio (TETRA); Security; Lawful Interception (LI) interface	V1.1.1	1997.5
		TS 101 507	Digital cellular telecommunications system (Phase 2+); Lawful Interception - Stage 1 (GSM 02.33 version 7.3.0 Release 1998)	V8.0.1	2001.6
		TS 101 509	Digital cellular telecommunications system (Phase 2+); Lawful interception; Stage (GSM 03.33 version 8.1.0 Release 1999)	V8.1.0	2000.12
		TS 101 861	Time Stamping Profile	V1.2.1	2002.3
		DTS/TIPHON-03020	TIPHONTM Release 4; Functional Entities, Information Flow and Reference Point Definitions; Lawful Interception	V1.0.1	2002.11
	IETF	RFC3924	Cisco Architecture for Lawful Intercept In IP Networks	V.0.2	2003.10
		-	Cisco Lawful Intercept Control MIB (draft-baker-slem-mib-00)	Expired	2003.4
		RFC2804	IETF Policy on Wiretapping	-	2000. 5

〈표 66〉 국가 표준화 기구별 기술 문건

구분	표준화 기구	문서번호	문서이름	국가	발표월일
LI	RtP	TR F (v 4.0)	Technical Directive setting forth Requirements relating to the Implementation of Legal Measures for the Interception of Telecommunications	Germany	2003.4
	EZ	TIIT-V1.0.0	Transport of Intercepted IP Traffic	Netherlands	2002.9
	Home Office	NHIS-V1.0	National Handover Interface Specification	United Kingdom	2002.3
	Cable Labs	PKT-SP-ESP-I02-030815	PacketCable™ Electronic Surveillance Specification	USA	2003.8.15
	ATIS	T1.678-2004	Lawfully Authorized Electronic Surveillance(LAES) for Voice over Packet Technologies in Wireline Telecommunications Networks	USA	2004.1
		T1.724-2004	UMTS Handover Interface for Lawful Interception	USA	2004.1
	TIA	TIA/EIA/IS-J-STD-025-A	Lawfully Authorized Electronic Surveillance	USA	2003.2
	PCIA	Standard 1 (V.1.3)	CALEA Specification for Traditional Paging	USA	2000.5.24
		Standard 2 (V.1.3)	CALEA Specification for Advanced Messaging	USA	2000.5.24
		Standard 3 (V.1.3)	CALEA Specification for Ancillary Services	USA	2000.5.24
	SCTE	DSS-01-08	IPCablecom Electronic Surveillance Standard	USA	2001.5.22

RtP: Regulatory Authority for Telecommunications and Posts
EZ: Ministry of Economic Affairs-Directorate-General for Telecommunications and Post

- 평가인증

◦ 정보보호 평가

국외의 정보보호시스템 평가 관련 표준 현황은 ISO/IEC JTC1 SC27에서 활발하게 진행되고 있음. SC27 내의 WG3에서는 IT 보안성 보증 및 평가에 관한 표준에 대한 제정 작업을 하고 있으며, 국제 상호인정협정 회원국이

주로 참여하고 있음. 최근 동향을 살펴보면, 암호 모듈 평가를 위한 요구사항 문서가 2006년 3월에 국제 표준으로 승인되었고, 공통평가기준의 범위를 확장하여 인적, 관리적 부분을 평가에 포함하는 운영시스템 보안성 평가가 기술문서로 발간됨. 2007년 10월 IT 보안성 보증 프레임워크가, 2008년 5월에는 IT 보안성 평가기준 버전 3.1이, 11월에는 바이오 인식 보안성 평가 프레임워크가 표준으로 등록될 예정임

〈표 67〉 IT 보안성 보증 및 평가에 관현 표정 제정 작업 현황

권고번호	완료시점	권고명 (주제)	국내표준
ISO/IEC 19790	2006.3.	암호 모듈보안 요구사항	-
ISO/IEC 19791	2006.5.	운영시스템 보안성 평가	-
ISO/IEC 15408	2008.5.	IT 보안성 평가 기준 개정판	-
ISO/IEC 18045	-	IT 보안성 평가 방법론 개정판	-
ISO/IEC 15443	2007.10.	IT 보안성 보증 프레임워크(※ 15443-3: 보증방법분석 표준화 진행 중, 2007-10월 완료예정)	-
ISO/IEC 15446	-	보호 프로파일 및 보안목표명세서 작성 가이드라인 개정판(※ 2007.9 2nd Working Draft 완료예정)	-
ISO/IEC 19792	2008.11.	바이오 인식 보안성 평가 프레임워크	-
ISO/IEC 24759	-	암호 모듈 시험 요구사항	-

- 보안관리

국외의 정보보호관리 표준 현황은 ISO/IEC JTC1 SC27, ITU-T, NIST 등에서 활발하게 진행되고 있음. SC27 내의 WG1에서는 ISO13335의 4개 파트가 국제표준으로 작성되었으며 또한 BS7799를 ISO17799로 수용하여, 2000년에 국제표준으로 제정하였고 현재 개정 작업 중에 있음. 최근 ISO회의에서 27007 Guidenlines for ISMS Auditing이 새롭게 추가되었고 27004 (ISM measurements)는 현재 CD상태이고 내년에 표준이 될 예정, 27011(ISM guidelines for Telecommunications)은 현재 FCD상태이며, 27011~이후의 번호들은 통신분야, 자동차분야, 헬스, 복권 등에 특화된 ISMS를 개발할 예정임

〈표 68〉 국외 정보보호관리 표준화 현황

권고번호	완료시점	권고명 (주제)	국내표준
ISO/IEC 27000	-	Overview & Vocabulary	-
ISO/IEC 27001	-	ISMS Requirement	-
ISO/IEC 27002	-	Code of practice for information security management(ISO/IEC 1799)	-
ISO/IEC 27003	-	ISMS Implementation guidelines	-
ISO/IEC 27004	-	ISMS measurements	-
ISO/IEC 27005	-	Information Security Risk management	-
ISO/IEC 27006	-	Requirement for the accreditation of bodies providing certification of ISMS	-

2.3.3. 표준화 현황 요약

• 국내 표준화 현황

국내 정보보호 일반 표준은 인터넷 보안기술 포럼과 TTA에서 추진되고 있음. 두 가지 방법으로 표준화가 추진 중에 있으며, 한 가지 방법은 사실 표준화 단체가 표준 초안을 개발하고, TTA에서 정보통신 단체표준으로 개발되는 방법이고, 다른 방법은 TTA에서 표준초안이 개발되고 관련 PG를 통하여 최종 표준을 확정하는 방법으로 표준안이 개발되는 방법임. 참고로, 국내 인터넷 보안 기술 포럼에서 표준화된 정보보호 일반 관련 표준과 TTA에서 확정된 정보보호 표준은 다음과 같음. 사실표준인 인터넷 보안기술포럼은 정보보호진흥원, 한국전자통신연구원, 정보보호산업체 등에서 참여하고 있는 국내 사실표준단체라고 볼 수 있음

TTA의 보안관련 조직은 다음과 같음. TTA의 TC1 산하에 3개의 보안관련 기술위원회가 존재함

〈표 69〉 TTA 정보보호를 위한 조직 구성

기술위원회	PG 이름	활동영역
TC1 (공통기반기술)	PG101 (정보보호기반)	- TC2/TC3/TC4 분야의 공통기반 요소 표준화 - 신성장동력 품목 수용(타 TC 분야 외) - 공통기반 분야의 표준적합/상호운용/성능시험 표준 마련 - 관련 국제표준화기구 동향분석 및 대응 - ITU-T SG17(정보보호), SG2(재난복구) 대응업무 - 공통기반 관련 표준 유지보수 추진
	PG102 (인터넷보안)	- 전자우편 및 전자상거래 보안 기술 표준 개발 - 네트워크 레벨 정보보호 표준 개발 - VPN, IDS 등 네트워크 보안 기술 표준 개발 - 응용 레벨 정보보호 표준 개발
	PG103 (바이오인식)	- 바이오인식 관련 표준화 및 기술개발 로드맵 제안 - 동종/이종 바이오인식 기법간 호환을 위한 표준화 동향 분석 - BioAPI 적합성 시험규격 등 상호운용 관련 표준화 추진

• 국외 표준화 현황

국외 정보보호 분야의 표준화는 다양한 기관에서 이루어지며, 이들 중 인터넷 보안과 관련하여 대표적인 기구들은 IETF, ISO/IEC JTC1/SC6 & SC27, ITU-T, NIST, ATIS, ETSI, OASIS, W3C, 3GPP 등이 있음. IETF에서의 보안 기술 표준화와 관련된 작업은 여러 영역에서 수행되고 있음. 이를 크게 구분한다면, 보안 영역의 17개의 작업반과 기타 영역의 여러 작업반으로 구분됨. IETF 보안 영역은 다음과 같은 작업반들이 표준화 작업을 수행하고 있음

〈표 70〉 IETF security area 표준화 작업반 (2007.8.14)

작업반	관련 내용
BTNS	Better-Than-Nothing Security
DKIM	Domain Keys Identified Mail
EMU	EAP Method update
HOKEY	Handover Keying
ISMS	Integrated Security Model for SNMP
KEYPROV	Provisioning of Symmetric Keys
KITTEN	Kitten(GSS API Next Generation)
KRB-WG	Kerberos WG
LTANS	Long-term Archive and Notary Service
MSEC	Multicast Security
NEA	Network Endpoint Assessment
OPENPGP	An Open Specification for Pretty Good Privacy
PKIX	Public Key Infrastructure (X.509)
SASL	Simple Authentication and Security Layer
SMIME	S/MIME Mail Security
SYSLOG	Security Issues in Network Event Logging
TLS	Transport Layer Security

ITU-T SG17에서는 정보통신 보안에 관한 표준을 선도하는 그룹으로 WP2 산하에 통신 시스템 보안 프로젝트, 보안 구조 및 프레임워크, 사이버 보안, 보안 관리, 바이오인식, 안전한 통신 서비스, 기술적인 스팸대응 등의 7개 연구과제로 구성되어 보안 표준들을 추진하고 있음. 각 연구과제별로 개요 및 연구영역은 〈표 71〉와 같음

〈표 71〉 ITU-T SG17 WP2 연구과제 개요

연구과제	연구과제 제목	기 개발된 표준
4/17	통신 시스템 보안 프로젝트(Communications systems security project)	
5/17	보안 구조 및 프레임워크(Security architecture and framework)	X.800, X.802, X.803, X.805, X.810, X.811, X.812, X.813, X.814, X.815, X.816, X.830, X.831, X.832, X.833, X.834, X.835, X.841, X.842, X.843
6/17	사이버 보안 (Cyber security)	E.409
7/17	보안 관리 (Security management)	X.1051
8/17	텔리바이오메트릭 (Telebiometrics)	X.1081
9/17	안전한 통신 서비스 (Secure communication services)	X.1121, X.1122, X.1141, X.1142
17/17	기술적인 SPAM 대응 (Countering SPAM by technical means)	-

응용보호와 정보보호 평가 및 관리체계 인증 분야를 대상으로 한 국내외 표준화 현황을 요약한 내용은 〈표 72〉와 같음

〈표 72〉 기술 분류별 국내외 표준화 현황 요약

구분	기술 분류	표준화 활동 현황	
		국내 동향	국외 동향
응용보안	전자우편	인터넷보안기술포럼 또는 TTA TC1에서 표준안을 작성하고 TTA에서 이를 확정하는 형태로 추진됨	RSA社가 주도하는 IETF SMIME 작업그룹에서 S/MIME v2를 수용하여 RFC를 발표한 바 있음
	전자투표/공증	국내외 모두 표준화된 바 없는 것으로 판단됨.	IEEE 산하 SCC 38 위원회에서 진행 중이고 P-1622, P-1583 두 과제로 나뉘어 개발되고 있음
	u지식 보안	URI 분야는 한국인터넷정보센터, URI포럼, 한국디지털콘텐츠포럼 등을 중심으로 추진됨. DRM 분야는 디지털콘텐츠포럼 및 DRM 포럼	MPEG21, OMA를 중심으로 진행 중임
	쉘 보안	쉘 보안에 대한 국내 표준화 활동이 없는 것으로 판단됨, 국외 제품 규격을 수용하여 국내 제품을 양산하기 때문인 것으로 사료됨	IETF SECSH 작업반에서는 SSH v2의 보안성 강화 및 확장성 제공을 위한 작업이 진행 중, 총 13건의 RFC 문서 완료, 1건의 Draft 문건이 진행 중임
	VoIP 보안	ITU-T를 중심으로 국제 표준화 활동	ITU-T, IETF 에서 표준 개발 중임.
	스팸대책	ITU-T를 중심으로 국제 표준화 활동	ITU-T, IETF 에서 표준 개발 중임.
	응용보안 강화 프로토콜	관련 표준안은 제정된 바 없으나, 현재 ITU-T SG17에서 패스워드 인증 프로토콜 가이드라인 표준 작업을 추진 중임	ITU-T SG17의 Q9에서 SPAK 표준화를 진행 중이고, Q5에서 PAK의 표준화를 4월 회의에서 완료함, IETF에서는 OTP 관련 RFC가 3건 등록된 상태임
	안전한 P2P 보안	사용자 수가 수백만에 이르는 대표적인 서비스임에도 불구하고 국내 표준이 전무한 상태임	ITU-T SG17 Q9에서 X.p2p-1과 X.p2p-2와 두 프로젝트가 진행 중이고, IETF에서 XMPP, SIMPLE, P2PSIP, IRTF P2PRG 연구그룹이 표준화 연구를 진행 중에 있음
	IPTV 보안	ITU-T IPTV FG 및 TTA IPTV PG를 통해 활발하게 활동 중, 5차 FG회의에서 46건의 표준안이 반영된 바 있음	ITU-T, AT&T, NTT 표준화 단체 및 루슨트, 노텔, 시스코 등 벤더가 가장 활발한 움직임을 보임, IPTV FG에서 7월까지 800여개의 기고서가 상정되었고, 이중 20개의 작업문서가 제정됨, DVB, IETF, MPEG, ISMA, TVA 등에서도 관련 표준화 활동이 있음
	신뢰 보안 서비스 (STC)	국내의 경우 STC 관련 표준안에 대한 적극적인 수용이나 개발이 이뤄지고 있지 않음, 2007년부터 무선인터넷포럼과 TTA를 통해 연구가 시작될 예정임	이미 HP, IBM, MS 등 여러 대형 벤더를 중심으로 산업표준인 TCG(Trusted Computing Group)을 결성하여 관련 표준화를 진행 중이며 TPM v1.2이 대표적 표준화 성과임
	차세대 웹 보안		
	Lawful Interception	TTA에서는 IMT2000(W-CDMA)와 관련하여 3GPP의 표준안을 국내 표준으로 3건 채택한 바 있음	유럽의 ETSI 주도로 합법적 감청에 대한 표준화가 활발히 진행되고 있음, 현재 진행 중인 문건은 총 31건에 이르며, 표준안 검토를 위한 자체 검증실험도 진행됨, IETF에서는 시스코 주도로 1건의 RFC가 2003년 채택된 바 있음
평가인증	정보보호 평가	TTA에서 제정하는 정보통신단체표준(5건), MIC에서 제정하는 한국정보통신표준(7종), 기술표준원에서 제정하는 한국산업규격(8건)으로 구성됨.	ISO/IEC JTC1 SC27, ITU-T, NIST 등에서 활발하게 표준안 제정이 진행 중임
	보안관리		

2.4. 표준화항목별 현황 분석표

구분		응용보안
표준화항목		전자우편 보안
시장 현황 및 전망	국내	- 보안프로토콜을 이용한 기밀성 서비스 보다는 스팸차단, 안티바이러스 등의 유해정보차단 중심으로 시장형성이 되고 있음
	국외	- 현재 많은 안티바이러스 및 스팸 차단 업체들이 스팸과 피싱 차단기술, 안티바이러스 기술을 통합한 솔루션을 통해 전자우편 보안이 제공되어 활용도가 높음
기술 개발 현황 및 전망	국내	- 국내 독자적인 스팸메일 차단 기술을 개발하고 있으며((주)자란지교소프트, 테라스테크놀로지 등) - 안철수 연구소의 V3와 같은 안티바이러스 기술의 일부로 전자우편을 통한 바이러스 및 피싱등의 기술개발이 이루어지고 있음.
	국외	- Microsoft, Trend Micro, McAfee, Sophos, Kaspersky, IronPort Systems 등에서 관련 제품을 개발함 - 독자적인 전자우편 보안 솔루션이 아닌 자사 제품의 기술중 하나로 제공되어지고 있음(Microsft-Exchange Hosted Services, Sophos, McAfee 등의 안티 바이러스 및 게이트웨이 하드/소프트 웨어)
기술 개발 수준	국내	- 기술 성숙단계
	국외	- 기술 성숙단계
	기술격차	- 없음
	관련제품	- (주)지란지교소프트, 스팸스나이퍼 - Microsoft Exchange server - McAfee Secure Messaging Gateway
IPR 보유현황	국내	- 다수의 관련 특허 보유
	국외	- 미국에서 다수의 관련 특허 보유 - 미국 IETF에 관련 표준문서 다수 존재
IPR확보 가능분야		- 특허, 논문 - 전자우편과 보안솔루션과의 통합 등
IPR확보 가능성		- 보통
표준화 현황 및 전망		- IETF에서 확장성을 고려한 전자우편 보안 관련 표준화가 거의 완료되어 있음. 41개의 RFC 및 4가지 권고문
표준화 기구/ 단체	국내	- ISTF, TTA
	국외	- IETF
	국내참여 업체 및 기관현황	- KISA
	국내기여도	-
표준화 수준	국내	- 국외표준 수용
	국외	- 표준기획, 표준제정/개정
국내표준화의 인프라수준 (시장요구정도 및 참여도)		- 높음

구분		응용보안
표준화항목		전자투표
시장 현황 및 전망	국내	- 키오스크 방식(터치스크린 시스템)의 전자투표 시스템을 2008년까지 2만대로 늘릴 예정.
	국외	- 현재 주 이상 규모의 공식 선거에 전자투표를 전면적으로 적용하고 있는 국가는 인도, 벨기에, 브라질 호주 등 4개국에 불과하지만 점차적으로 도입되어 활용도가 높아질 것으로 예상됨.
기술 개발 현황 및 전망	국내	- 국내 실정에 적합한 전자투표 시스템을 개발하여 도입중 - 현재 키오스크 방식(터치스크린)의 전자투표 시스템을 도입중이지만 원격 전자투표로 기술개발이 이루어 질것으로 예상됨.
	국외	- 미국 : 옵티컬 스캔, 마크 센스기술을 이용 - 일본 : 터치스크린 방식을 도입중 - 각 국가별 적합한 전자투표 시스템을 개발 · 도입하고 있음 - 당 기술은 성숙/적용 단계임
기술 개발 수준	국내	- 기술 개발 단계
	국외	- 기술 개발/성숙 단계
	기술격차	- 2~3년
	관련 제품	- 다이볼드 일렉션 시스템(Diebold Election Systems) 애큐보트-TS - 세콰이어(Sequoia) 보팅 시스템 - ES&S - (주)인터콘웨어
IPR 보유현황	국내	- 120여건의 관련 특허 보유
	국외	- 국가별 관련 특허 보유
IPR확보 가능분야		- 특허, 논문, 시스템/서비스 - 원격 전자투표 시스템/서비스, 인증 방법, 호환성, 다양한 미디어 이용 방법 등
IPR확보 가능성		- 보통
표준화 현황 및 전망		- IETF 산하 SCC 38위원회에서 표준 작업 진행중이지만 현재는 미비한 실정 - 다양한 방식의 전자투표 기술의 표준화의 진행이 필요
표준화 기구/ 단체	국내	- 중앙선거관리위원회, 전자선거추진협의회
	국외	- IETF
	국내참여 업체 및 기관현황	-
	국내기여도	- 거의 없음
표준화 수준	국내	- 거의 없음
	국외	- 거의 없음
국내표준화의 인프라수준 (시장요구정도 및 참여도)		- 높음

구분		응용보안
표준화항목		u-지식 보안
시장 현황 및 전망	국내	- 한미FTA 체결로 개정 저작권법에서 P2P나 웹하드와 같은 온라인서비스사업자는 불법저작물 전송을 차단하는 기술적 조치를 의무화함. - KTF, SKT 등의 이동통신 사업자는 OMA DRM 2.0 기반 저작권 보호 서비스를 제공 중이나 높은 로열티 문제가 있음 - 국내 지식산업 인프라가 확대되어 감에 따라 DRM 상호호환성 보장 및 DRM/CAS 등 지재권 보호 기술들 간의 연동 요구 증가 - 지식제공자의 투명한 지식 유통 파악을 위한 추적 요구가 있음.
	국외	- 자유로운 사용이 보장된 지식에 대한 사용자 요구 증가와 지식보호 솔루션의 과다한 관리 비용으로, 일부 콘텐츠 사업자(EMI, UMG 등)와 서비스제공자(애플, MS)는 DRM-free 서비스 선언
기술 개발 현황 및 전망	국내	- 서비스 도메인별로 다르게 요구된 지재권 보호 기술을 개발 - 전용 디바이스 단위로 권한관리를 추구하는 지재권 보호 기술로 자신 소유의 타 디바이스에서 구매 지식의 이동 불가로 사용자 불편 - 서비스 사업자들이 사용자의 이용 내역을 모니터링 등의 프라이버시 침해 우려
	국외	- 단일 도메인용 디지털 컨텐츠의 지재권 보호 기술이 상용화 수준 - 인증서가 아닌 익명/가명 ID 기반의 익명성 제공 기술에 대한 연구 진행(EU PRIME 등) - 사용자 도메인 내에서 지식의 이동을 자유롭게 허용하는 Non-DRM 방식의 지식을 제공함.(애플 iPod의 Protected Contents)
기술 개발 수준	국내	- SW 및 실명ID 기반의 DRM, CAS 등의 지식보호 솔루션을 개발/상용화를 진행하고 있으나, 복합지식 보호 및 프라이버시 보호 없음 - 전용 디바이스 단위로 권한관리를 추구하는 음악지식(Mp3)에 대한 보호 솔루션은 있으나, 자신 소유의 타 디바이스로 구매 지식의 이동 불가로 사용자 불편
	국외	- 사용자 창작/수정/재가공 지식에 대한 지재권보호 및 지분표현 기술은 미약한 수준임. - 기술 성장 단계
	기술격차	- 1년
	관련제품	- 없음
IPR 보유현황	국내	- 익명 PKI 분야 2건, 불법복제 78건, 지식보안 단말플랫폼 분야 11건, 복합지식 콘텐츠저작권 보호 툴킷 4건 등의 유효 특허 파악됨.
	국외	- 미국 Microsoft와 Digimarc Intel : 지식보호 기술 전분야 다출원 404건
IPR확보 가능분야		- 사용자 익명 ID 제공 기술 및 Downloadable-TPM 기반 지식보안 단말, 프로슈머 유통구조를 갖는 계층적 지재권 보호 핵심 IPR 확보
IPR확보 가능성		- 높음
표준화 현황 및 전망		- MPEG-21, OMA에서는 DRM 표준화 추진 - 국내 TTA에서 DMB-CAS, EXIM 표준화 - 방송콘텐츠보호솔루션인 CAS를 SW 형태로 다운로드하여 단말 트러스트를 제공하는 지식보안 기술 표준화 (미국 OpencableLab) - 음악 보호 파일에 대한 상호연동을 위해 EXIM을 표준화하였으나, 서비스 사업자간 호환성과 과금 방식에 이견이 있는 상태
표준화 기구/ 단체	국내	- TTA
	국외	- MPEG-21, OMA, DVB-CPCM, DHWG, TV-Anytime, OpenCableLab등
	국내참여 업체 및 기관현황	- ETRI, 삼성전자 등 - SK텔레콤, KT
	국내기여도	- 거의 없음
표준화 수준	국내	- 국외표준 수용
	국외	- 표준안기획 및 표준안항목승인
국내표준화의 인프라수준 (시장요구정도 및 참여도)		- 높음 - 연구소, 학계 및 산업체의 기술 개발 및 표준화 참여가 증가하고 있음.

구분		응용보안
표준화항목		쉘 보안
시장 현황 및 전망	국내	- 외국제품을 수입하여 사용하고 있음.
	국외	- 체적인 시장자료는 없으나, 현재 국가, 기업, 금융망 등에 안전한 원격접속을 위해 많이 사용되고 있으며, 통합 보안 시스템의 일부 기능으로 활용도가 높음.
기술 개발 현황 및 전망	국내	- 외국의 제품을 국내에 공급하는 수준이며, - SFTP(Secure Shell File Transfer Protocol)를 이용한 파일전송 프로그램과 같이 소규모의 응용 기술개발이 이루어지고 있음.
	국외	- RSA Security사, SSH 커뮤니케이션스, 마이크로소프트, attachmate 등에서 관련 제품을 개발함. - OpenSSH 등의 공개된 소스의 제품도 존재함. - 당 기술은 성숙/적용 단계임
기술 개발 수준	국내	- 프로토타입 구현 수준
	국외	- 기술 성숙단계
	기술격차	- 1~2년
	관련제품	- SSH SecShell Toolkit - RSA Communication Security - Reflection for Secure IT
IPR 보유현황	국내	- 관련 특허 출원 실적 없음
	국외	- 미국에서 다수의 관련 특허 보유 - 미국 IETF에 관련 표준문서 다수 존재
IPR확보 가능분야		- 특허, 논문 - SSH 확장성, 호환성, 편의성, 키교환 방법 등
IPR확보 가능성		- 보통
표준화 현황 및 전망		- IETF에서 SSH관련 표준화가 거의 완료단계에 있음. 13개의 RFC, 1개의 internet draft 상정
표준화 기구/ 단체	국내	- 없음
	국외	- IETF
	국내참여 업체 및 기관현황	- KISA, ETRI
	국내기여도	- 거의 없음
표준화 수준	국내	- 국외표준 수용
	국외	- 표준기획, 표준제정/개정
국내표준화의 인프라수준 (시장요구정도 및 참여도)		- 높음

구분		응용보안
표준화항목		VoIP 보안
시장 현황 및 전망	국내	- 국내에서는 VoIP 암호화 장비로 IPSec 기반 VPN 기능을 갖는 VoIP 보안 제품이 주로 시장에 출시됨 - 초고속 인터넷 망과 휴대통신망의 발전으로 VoIP 관련 다양한 형태의 서비스가 등장하고 있으며, 이에 대한 기술적, 정책적 보호 대책이 필요함.
	국외	- SIP 기반의 VoIP 서비스는 아직 초기 단계로 서비스를 준비 중에 있음 - 초고속 인터넷 망과 휴대통신망의 발전으로 VoIP 관련 다양한 형태의 서비스가 등장하고 있으며, 이에 대한 기술적, 정책적 보호 대책이 필요함.
기술 개발 현황 및 전망	국내	- 암호 통화를 수행할 수 있는 비화용 휴대전화기 개발 사례가 있음 - 최근 불법스팸대응센터에 접수되는 등 VoIP 스팸이 사회적 문제로 등장하고 있으나, 국내 관련 기술 개발은 미비한 실정임
	국외	- IP 서버 및 SRTP 툴킷을 포함한 SIP 툴킷을 개발한 바가 있음 - VoIP 데이터 보호를 위한 암호 및 키관리 기술은 표준화를 중심으로 개발됨. (SIP(RFC 3261), SRTP(RFC 3711), MIKEY(RFC3830))
기술 개발 수준	국내	- 국내에서는 VoIP 암호화 장비로 본점과 지점간 안전한 통화선로를 설정하는 VPN은 불특정 다수와 착발신 통화를 해야 하는 일반 전화서비스 성격에는 적합하지 않음. - 국내에서는 VoIP 서비스를 위한 암호/키관리 API 모듈에 연구 개발이 미흡한 실정임 - 프라이버시 보호 메카니즘, 암호 요구사항 등 기술 개발 필요함
	국외	- VoIP 스팸은 호 형태의 SPIT(Call Spam, Spam over Internet Telephony)과 메신저 서비스 기반의 SPIM(IM Spam, Spam over Instant Messaging), 프레즌스 서비스 기반의 Presence Spam의 분야로 나뉘어 학계 및 산업계 중심으로 연구 진행중 - VoIP 사용자의 프라이버시 보호 기술은 아직 초계 단계로 SIP를 위한 프라이버시 메커니즘이 표준으로 제공되고 있고, VoIP 프라이버시 정책에 의거 프라이버시 서비스가 제공되어야 한다고 정의하고 있으나, 그 구현 방법 등은 명시되어 있지 않음. - 사용자의 물리적, 논리적 위치정보를 다루는 VoIP 긴급통화 및 프레즌스 서비스 등 다양한 VoIP 부가서비스가 등장하고 있으나, 사용자의 위치정보 노출로 인한 프라이버시 침해 위협에 대한 고려는 매우 부족한 상황임 - 프라이버시 보호 메카니즘, 암호 요구사항 등 기술 개발 필요함
	기술격차	- 2~3년
	관련제품	- Radvision(VoIP 프로토콜 툴킷)
IPR 보유현황	국내	- VoIP 관련 국내 특허는 1999년부터 증가하기 시작하여 약 800여건이 등록. 이러한 특허 동향은 VoIP 관련 기술의 개발이 외국에 비해 늦었음을 의미 - 국내 특허는 주로 채팅서비스, 컨퍼런스폰 시스템 등 VoIP 응용 분야에 집중됨
	국외	- 미국에서 다수의 관련 특허 보유 - 데이터 처리 장치, 호출 제어 장치, 어댑터 장치 등 기술 특허로, 응용 서비스 분야에 집중됨
IPR확보 가능분야		- Consent framework, Black/White list 관리, 필터링, reputation, 추론기법, 인증방법, 패턴 분석 등
IPR확보 가능성		- 보통
표준화 현황 및 전망		- IETF의 SIPPING WG는 SIP 또는 SIP 응용 서비스와 관련된 요구사항을 표준화 - IETF의 SIP WG는 SIP 프로토콜과 관리 분야의 표준화 - ITU-T는 스팸 방지 관련 가이드라인 표준화 - 인증된 아이덴터티 관리, SIP SAML, SIP 스팸 대책 등 표준화 추진 필요
표준화 기구/ 단체	국내	- ETRI PEC
	국외	- IETF, ITU-T
	국내참여 업체 및 기관현황	- KISA, ETRI, 숭실대학교
	국내기여도	- 보통
표준화 수준	국내	- 국외표준 준용
	국외	- 표준기획, 표준제정/개정
국내표준화의 인프라수준 (시장요구정도 및 참여도)		- 높음. - 연구소, 학계 및 산업체의 기술 개발 및 표준화 참여가 증가하고 있음.

구분		응용보안
표준화항목		스팸대책
시장 현황 및 전망	국내	- 초고속 인터넷 망과 휴대통신망의 발전으로 다양한 형태의 스팸이발생하고 있으며, 이에 대한 기술적, 정책적 대책이 필요함.
	국외	- 초고속 인터넷 망과 휴대통신망의 발전으로 다양한 형태의 스팸이발생하고 있으며, 이에 대한 기술적, 정책적 대책이 필요함.
기술 개발 현황 및 전망	국내	- 서비스 업계 별로 고유의 스팸 방지기술 채용
	국외	- RSA Security사, SSH 커뮤니케이션스, 마이크로소프트, attachmate 등에서 관련 제품을 개발함. - OpenSSH 등의 공개된 소스의 제품도 존재함. - 당 기술은 성숙/적용 단계임
기술 개발 수준	국내	- 서비스별 고유 기술 개발
	국외	- 기술 성숙단계
	기술격차	- 0~1년
	관련제품	- Qovia,inc: VoIP 스팸 대응 기술이 포함된 제품 판매 - BorderWare: SIPassure - Facetime: IMAuditor
IPR 보유현황	국내	- 없음
	국외	- 미국에서 다수의 관련 특허 보유 - 미국 IETF, ITU-T에서 표준화 진행
IPR확보 가능분야		- Consent framework, Black/White list 관리, 필터링, reputation, 추론기법, 인증방법, 패턴 분석 등
IPR확보 가능성		- 보통
표준화 현황 및 전망		- IETF의 SIPPING WG는 SIP 또는 SIP 응용 서비스와 관련된 요구사항을 표준화 - IETF의 SIP WG는 SIP 프로토콜과 관리 분야의 표준화 - ITU-T는 스팸 방지 관련 가이드라인 표준화
표준화 기구/ 단체	국내	- ETRI PEC
	국외	- IETF, ITU-T
	국내참여 업체 및 기관현황	- KISA, ETRI, 숭실대학교
	국내기여도	- 높음
표준화 수준	국내	- 국외표준 준용
	국외	- 표준기획, 표준제정/개정
국내표준화의 인프라수준 (시장요구정도 및 참여도)		- 높음

구분		응용보안
표준화항목		응용보안 강화 프로토콜
시장 현황 및 전망	국내	- 통신망, 금융망 보안에 일부 활용되고 있음.
	국외	- 통신망, 금융망 보안 등에 일부 활용되고 있으며, 단독 제품보다는 여러 보안 기술을 통합한 형태의 제품이 출시됨
기술 개발 현황 및 전망	국내	- 국내의 경우 진행 중인 기술개발은 없으며, 학술적 연구위주로 진행하고 있음
	국외	- IETF, ITU-T 등에서 표준화와 더불어 기술 개발을 진행 하고 있음. 산업체의 경우 패스워드 인증을 포함한 보안 제품 개발이 진행 중에 있으며, 주로 통신망 보안, 금융망 보안에 활용도가 높을 것으로 기대됨
기술 개발 수준	국내	- 프로토타입/테스트베드 구현
	국외	- 프로토타입/테스트베드 개발완료
	기술격차	- 1~2년
	관련제품	- 금융망 보안 솔루션 - 망 관리 솔루션
IPR 보유현황	국내	- 신뢰적인 제 3기관을 통한 보안 프로토콜, 이동 통신 시스템에서의 패스워드 인증 관련 특허 등 보유
	국외	- 미국, 일본을 중심으로 다수의 특허 보유 - 패스워드 인증에 대한 다양한 기술분야의 특허가 다수 출원 - 미국을 중심으로 국외표준문서 다수 존재
IPR확보 가능분야		- 기술 개발을 통한 응용 특허 또는 기존 특허에 대한 우회특허 또는 개량 특허의 도출을 통한 IPR 확보가 요구
IPR확보 가능성		- 높음
표준화 현황 및 전망		- IETF, ITU-T 등에서 표준화가 진행 중에 있음 - ITU-T의 국제표준화가 완료되면, 국내 표준으로 수용될 예정임
표준화 기구/ 단체	국내	- 없음
	국외	- ITU-T, IETF, IEEE
	국내참여 업체 및 기관현황	- KISA, ETRI, 순천향대학교
	국내기여도	- ITU-T 국제 표준화 추진 중
표준화 수준	국내	- 표준기획-권고/초안검토
	국외	- 표준기획, 표준제정/개정
국내표준화의 인프라수준 (시장요구정도 및 참여도)		- 높음 - 연구소, 학계 및 산업체의 기술 개발 및 표준화 참여가 증가하고 있음

구분		응용보안
표준화항목		안전한 P2P 보안
시장 현황 및 전망	국내	- 국내에서 P2P로 인한 기밀유출 및 과다 트래픽 문제가 심각해짐에 따라 P2P 트래픽 제어와 P2P 응용 보안기술의 수요가 증가하고 있음
	국외	- 시만텍, 포티넷, 시큐어컴퓨팅, 주니퍼 등, 세계의 유수한 보안 장비업체들이 P2P 트래픽 제어 시장을 주도하고 있음
기술 개발 현황 및 전망	국내	- KISTI에서 P2P 기반 분산 컴퓨팅에 관한 프로젝트인 Korea@home가 수행 중 - ETRI에서 유무선 IPv6 기반 P2P 네트워크 정보보호 기술개발 과제 수행 중 - 삼성종합기술원에서 P2P기술이 가진 지적재산권, 확장성 문제와 IPv6와의 결합문제 등에 관하여 연구 진행 - (주)대우정보시스템은 P2P 애플리케이션을 기업의 기간시스템, 특히 지식관리 시스템과 연동하는 프로젝트를 추진 - (주)피어컴은 SK Mobile 지원으로 P2P 연구 선도 과제를 수행 중 - P2P 보안 관련 기술 분야에서는 (주)아라기술, (주)소만사 등이 패킷 필터링 기술에 기반한 P2P 트래픽을 수집 · 분석 및 제어하는 솔루션을 구축 - 소리바다, 프루나, 피투피아 등 여러 업체에서 P2P 파일 공유 서비스를 제공
	국외	- Microsoft는 2001년부터 안전한 파일 공유 시스템 제공을 목적으로 하는 Farsite라는 연구를 진행 중, 또한 최근 Vista에 PC간 연결 및 검색이 자유로운 P2P 기술을 탑재. - SUN Microsystems는 2001년부터 다양한 디바이스들이 P2P 형태로 서로 통신, 협업할 수 있도록 하는 프로토콜의 개발을 목적으로 하는 JXTA 라는 프로젝트를 진행 중. - 인텔, 휴렛패커드, 노키아 등 세계 유수한 IT 기업들이 P2P 관련 연구를 진행 중 - P2P 보안 관련기술 분야에서는 시만텍, 포티넷, 시큐어컴퓨팅, 주니퍼 등 보안장비 업체들이 P2P 트래픽 제어 기능이 포함된 UTM 솔루션을 제공 - UC Berkeley가 P2P 기반 분산 컴퓨팅을 통하여 외계 생명체의 존재를 찾기 위한 막대한 양의 계산을 수행하는 SETI@home이라는 프로젝트를 진행 중 - MIT, Purdue, UC Berkeley, Rice University 등에서 여러 구조적 분산형 P2P 네트워크(Chord, CAN, Pastry, Tapestry)의 개발을 진행 중 - 일본 Gnutella 사용자 모임이 핸드폰을 이용한 Gnutella 서비스를 목적으로 하는 Mog 라는 프로젝트를 진행 중
기술 개발 수준	국내	- 패킷 탐지 분야에 일부 기술 개발이 있으며, 피어 검색, 자원 분산 등의 핵심 기술 분야에 기술개발은 전무한 상태
	국외	- 폐쇄 환경에서 피어검색, 자원분산 등 핵심 기술 분야에 상용화 제품 출시되고 있으나 개방 환경에서의 보안 기술은 미흡함
	기술격차	- 1.5년
	관련제품	- P2P 보안 프레임워크, P2P 트래픽 제어 시스템 - 아라기술, 소만사
IPR 보유현황	국내	- P2P 관련 국내특허는 현재까지 30여 건이 등록되었으며, 국내 P2P 응용 서비스 이용 규모에 비해서 특허 건수는 상대적으로 적은 편
	국외	- 미국에서 Microsoft, Sun Microsystems, Intel, McAfee, HP를 포함한 많은 기업들이 1,000여건을 등록/출원했으며, 일본에서는 KDDI, Microsoft, NEC, Onkyo, Fuji, Hitachi 등의 기업들이 100여건의 특허를 출원/등록한 상태
IPR확보 가능분야		- P2P 트래픽 분석 및 제어 기술 - 개방 환경에서의 피어검색 보안, 자원 분산 보안 등 - P2P 아이디 보안 기술 - P2P기반 IPTV 보안 기술
IPR확보 가능성		- 보통
표준화 현황 및 전망		- ITU-T SG-17의 Question 9/17에서는 X.p2p-1과 X.p2p-2, 두 개의 P2P 보안 분야의 표준화 프로젝트가 현재 진행 중 - IETF에서는 XMPP, SIMPLE, P2PSIP 등의 워킹그룹들이 P2P 관련 표준화 작업을 진행 또는 완료(XMPP)한 상태임 - XMPP는 인스턴트 메신저에 채널 및 개체 암호를 지원하기 위한 security 기능이 추가된 프로토콜의 표준화를 추진하여 4건의 RFC를 등록 - SIMPLE은 인스턴트 메신저 서비스의 표준화를 위해 구성된 워킹그룹으로 현재까지 14건의 RFC를 등록 - P2PSIP는 P2P 기반 SIP 세션 이용을 위한 메커니즘과 가이드라인을 제정하기 위하여 표준화 작업을 진행 중 - IRTF의 P2PRG 연구그룹에서도 표준화 작업의 기초를 제공하기 위한 연구를 진행 중 - 아이디 보안 분야 등에서 신규 표준화가 필요함 - P2P 기반 기술을 IPTV 등 신규 응용 분야에 적용하기 위한 요구사항 및 프레임워크 표준화가 필요함
표준화 기구/ 단체	국내	- 없음
	국외	- ITU-T, IETF
	국내참여 업체 및 기관현황	- KISA, ETRI, ICU, 소만사, VI소프트
	국내기여도	- 높음.
표준화 수준	국내	- 진행중인 표준화 작업 없음
	국외	- 표준안개발/검토
국내표준화의 인프라수준 (시장요구정도 및 참여도)		- 높음 - 연구소, 학계 및 산업체의 기술 개발 및 표준화 참여가 증가하고 있음

구분		응용보안
표준화항목		IPTV 보안
시장 현황 및 전망	국내	- KT, 하나TV가 IPTV 시범 및 상용 서비스를 개시하였고, LG에서 서비스를 준비중에 있음 - IPTV 보안은 DRM과 CAS만 고려되고 있음 - DRM/CAS 핵심 기술은 외산이 주를 이루고 있음
	국외	- 전 세계적으로 280여개의 사업자가 IPTV 시범 및 상용 서비스를 제공 하고 있음 - DRM/CAS 분야에 전통적으로 강세를 보이고 있음
기술 개발 현황 및 전망	국내	- 네트워크 및 부가 서비스 보안은 기존의 보안 기술의 연속으로 보는 시각 - DRM/CAS에 주력하고 있으나, 기술개발은 부진하고 외산 DRM/CAS 핵심 기술을 채용하여 셋톱박스를 구현하는 형태 - Downloadable CAS 분야에 강세 - DRM + CAS 통합 제품 개발 - IPTV커뮤니티 보안을 위한 기초연구 진행중 - 오버레이 또는 P2P 방식의 멀티캐스트에 대한 기초연구 진행중
	국외	- IPTV 스트림 보호를 위해 DRM과 CAS를 이용하는 방안이 적극 고려됨 - 학계를 중심으로 HD급 고화질 암호화 연구 진행 - 투명성, transcodability, 공간/주파수 도메인 암호화, 선택적 암호화 등 신규 보안 기술 분야 연구 - 오버레이/P2P 기반 IPTV 기술 연구 - P2P 기반 인터넷TV 서비스 제공(Joost, PPstream, PPTV, Coolstream등)
기술 개발 수준	국내	- IPTV 응용, 서비스 기술은 뛰어나나 보안 기술 분야에서는 뒤쳐짐 - 응용 기술은 뛰어나나 DRM/CAS의 핵심 요소 기술은 외산을 채용 - DRM+CAS 통합과 Downloadable CAS와 같은 분야에서 강세 - IPTV를 위한 신규 보안 기술 분야의 기초연구 없음 - 오버레이 또는 P2P 방식의 멀티캐스트를 IPTV에 적용하기 위한 보안기술 개발이 필요함
	국외	- DRM/CAS 분야의 기술은 포화된 상태이며, 상용제품이 출시되고 있음 - 학계를 중심으로 IPTV를 위한 신규 보안 기술 분야의 기초연구 활발히 진행중
	기술격차	- 응용서비스 분야는 대등한 기술수준임 - 수신제한(CAS) 분야의 격차는 1년 이상 (초기 기술격차에 의한 시장 잠식이 문제) - DRM 분야는 국내기술이 우수하나 IPTV 전용 DRM 개발이 필요함. - IPTV를 위한 암호화, 프라이버시 등 신규 보안 기술 분야의 격차는 3년이상.
	관련제품	- 마이크로소프트, NDS, 이데토, 나그라비젼, 셀런
IPR 보유현황	국내	- IPTV 서비스 및 응용 기술 특허 다수 보유 - 전송망, 인증, 과금, 식별 등 IPTV 보안 특허는 매우 적음 - DRM/CAS 특허 일부 보유
	국외	- IPTV 서비스 및 응용 기술 특허 다수 보유 - 전송망, 인증, 과금, 식별 등 IPTV 보안 특허는 매우 적음 - DRM/CAS 특허 다수 보유
IPR확보 가능분야		- DRM/CAS 분야는 국내뿐만 아니라 국외에서도 이미 기술이 포화된 상태임 (2005년 이후 특허 수 급격히 감소) - 투명성, transcodability, 공간/주파수 도메인 암호화, 선택적 암호화 등 신규 보안 기술 분야 IPR 확보 가능 - 전송망, 인증, 과금, 식별 등 IPTV에 특화된 보안 기술 IPR 확보 가능 - 프라이버시 보호 분야에 IPR 확보 가능
IPR확보 가능성		- 높음
표준화 현황 및 전망		- 한국은 ITU-T IPTV FG에서 서비스, 망 구조 등 분야를 주도하고 있음. - 디지털 방송 분야는 이미 표준화가 완료된 상태 - IPTV 보안 기술 분야 표준화는 요구사항만 도출된 상태 - IPTV를 위한 암호화, 프라이버시 등 신규 보안 기술 분야 - 오버레이 또는 P2P 방식의 멀티캐스트를 IPTV에 적용하기 위한 요구사항 및 기술 표준화 필요
표준화 기구/ 단체	국내	- TTA
	국외	- ETSI, ITU-T, IETF, DVB, ATSC, 케이블랩스, ATIS IIF, TV Anytime
	국내참여 업체 및 기관현황	- TTA, ETRI, KISA, Samsung, ICU 등
	국내기여도	- ITU-T IPTV FG내에서 서비스, 망 구조 등 분야 주도
표준화 수준	국내	- 국내 표준화 추진 - 국제 표준 상정에 주력
	국외	- 표준기획, 제정/개정
국내표준화의 인프라수준 (시장요구정도 및 참여도)		- 높음 - 연구소, 학계 및 산업체의 기술 개발 및 표준화 참여 활발함.

구분		응용보안
표준화항목		STC (Secure Trusted Computing)
시장 현황 및 전망	국내	- STC 기술에 대해서는 아직 검토 단계임 - TPM이 장착된 노트북이나 데스크탑 등 많은 외국 제품들이 있지만, 국내 업체는 아직 관망 단계임.
	국외	- HP, IBM, MS 등 대형 단말 업체들은 이미 TPM이 탑재된 상용 제품들을 판매 - 보안의 중요성이 부각되면서 TPM 탑재 제품은 더욱 증가하는 추세며, 표준화 진행도 더욱 광범위해질 것으로 예측
기술 개발 현황 및 전망	국내	- ETRI에서 모바일용 TPM을 개발하고 있음. 타 업체는 아직 검토 단계임. - 유비쿼터스 환경에서는 TPM에 대한 필요성이 더욱 커질 것으로 예상
	국외	- 노트북이나 데스크탑에는 이미 TPM 장착된 상용 제품들이 출시되고 있음. - TPM을 장착한 모바일 단말 제품은 아직 출시되지 않음. - TCG의 표준화 진행과 업체들의 관련 기술 개발이 동시에 이루어지고 있음.
기술 개발 수준	국내	- STC 관련한 기술 개발은 아직 검토 중임. - 기술 초기 단계
	국외	- 상용 제품을 판매하고 있고 시장 영역이 점점 확대되고 있음. - 기술 성장 단계
	기술격차	- 2~3년
	관련 제품	- IBM에서 생산하는 노트북 제품 - MS사의 WindowVista - 데스크탑, 노트북 등에 탑재되어 출시되고 있고 그 양이 점점 증가하고 있음.
IPR 보유현황	국내	-
	국외	- TCG에 다수의 표준문서 존재(TPM, TSS, MTM 등)
IPR확보 가능분야		- 국내/국제 특허, 논문 - 모바일 TPM 개발에 사용된 다수의 기술들
IPR확보 가능성		- 보통
표준화 현황 및 전망		- TCG 위주의 표준화 활동이 앞으로 더욱 활발해질 것으로 예측됨.(TCG 가입업체가 점점 증가하고 있음) - TCG의 활동 분야 중 TPM 등 분야의 표준화 추진 필요
표준화 기구/ 단체	국내	- TTA
	국외	- TCG - 3GPP, IETF
	국내참여 업체 및 기관현황	- ETRI, 삼성 - 스프레드텔레콤, 프롬투
	국내기여도	- 거의 없음
표준화 수준	국내	- 아직 표준화 진행 사항 없음
	국외	- TCG에서 표준화를 활발히 진행 중임 - 3GPP, OMA, ITU-T와도 liaison을 통한 표준화 추진 예정
국내표준화의 인프라수준 (시장요구정도 및 참여도)		- 높음 - 연구소, 학계 및 산업체의 기술 개발 및 표준화 참여 예상됨

구분		응용보안
표준화항목		차세대 웹 보안
시장 현황 및 전망	국내	- 유선 환경에서의 전자거래 등 비즈니스 응용 서비스를 위한 웹서비스 정보보호 기술은 이미 적용이 시작되어 시장이 확대되리라고 예상됨 - 국내 모바일 웹서비스 보안 기술은 아직 시장이 태동기이나 웹기술이 모바일 환경으로 급속하게 확산되고 있어 향후 시장이 커지리라고 예상됨 - 국내에서 웹 2.0 기술이 급속히 확산되고 있고 보안 문제에 대한 심각성이 커지고 있어 시장이 성장하리라고 예상됨 - 유비쿼터스 웹, 시맨틱 웹 보안 기술은 기술 개발 초기 단계로 시장 형성에 다소 시간이 걸릴것으로 예상되나 유비쿼터스 사회로의 전환에 따라 궁극적으로 수요가 증가하리라고 예상됨
	국외	- 모바일 디바이스 보안 시장은 2011년 연평균성장률이 35%로 예상되고 있음 (IDC) - 웹어플리케이션 보안 분야에 대한 수요가 전체 정보보호 제품 수요의 20%로 예상 (IDC) - 유선 환경에서의 비즈니스 응용 서비스를 위한 웹서비스 정보보호 기술은 이미 시장이 상당히 형성된 상태임 - 모바일 웹서비스 보안 기술은 아직 시장이 크지는 않지만 웹기술이 모바일 환경으로 급속하게 확산되고 있어 향후 시장이 더욱 커지리라고 예상됨 - 웹 2.0 기술이 급속히 확산되고 있고 보안 문제에 대한 심각성이 커지고 있어 시장이 성장하리라고 예상됨 - 유비쿼터스 웹, 시맨틱 웹 보안 기술은 기술 개발 초기 단계로 시장 형성에 다소 시간이 걸릴것으로 예상되나 유비쿼터스 사회로의 전환에 따라 궁극적으로 수요가 증가하리라고 예상됨
기술 개발 현황 및 전망	국내	- 국내에서도 유선 환경을 위한 주요 웹서비스 보안 기술은 ETRI 등에서 개발하였거나 개발중임 - 모바일 웹서비스 보안 기술은 ETRI에서 표준화만 진행하고 있음 - 웹 2.0 보안에 대한 요구사항이 증가하고 있으나 웹 2.0 보안 기술 개발은 웹 방화벽 개발 위주로 이루어지고 있어 기술 개발이 부족한 실정임 - 시맨틱 웹 보안 기술, 유비쿼터스 웹 보안 등의 기술 개발은 아직 이루어지지 않고 있음
	국외	- 유선 환경을 위한 웹서비스 보안 기술은 이미 상용화 수준임 - 모바일 웹서비스 보안 기술은 Nokia 등에서 개발하고 있음 - 시맨틱 웹 보안 기술 제품 개발은 이루어지고 있지 않음 - 웹 2.0 기술 개발은 웹방화벽 개발에 치중되어 있음 - MS 등에서 디바이스 웹서비스를 위한 보안 기술을 개발하고 있음
기술 개발 수준	국내	- 유선 웹서비스 보안 기술 및 웹 방화벽 기술은 비교적 높은 편임 - 모바일 웹서비스 보안 기술, 시맨틱 웹 보안 기술은 기술 초기 단계임
	국외	- 유선 웹서비스 보안 기술 및 웹 방화벽 기술은 상용화 수준임 - 모바일 웹서비스 보안 기술은 기술 성장 단계이며, 시맨틱 웹 보안, 유비쿼터스 웹 보안 기술은 기술 개발 초기 단계임
	기술격차	- 2~3년
	관련 제품	- IBM WebSphere, MS WSE 3.0 - Nokia Web Services Framework - TEROS 웹어플리케이션 보안 게이트웨이
IPR 보유현황	국내	- 유선 환경에서의 웹서비스 보안은 상당수의 특허 보유 - 웹 2.0 보안 관련 특허는 소수 있지만 시맨틱 웹서비스 보안, 유비쿼터스 웹 보안 특허는 없음
	국외	- 유선 환경에서의 웹서비스 보안은 상당수의 특허 보유 - 웹 2.0 보안 관련 특허는 소수 있지만 시맨틱 웹서비스 보안, 유비쿼터스 웹 보안 특허는 없음
IPR확보 가능분야		- 웹서비스 기반의 디바이스 및 서비스간 보안 연동 기술, 시맨틱 기반 보안 연동 기술, 웹 2.0 보안 프로토콜 등
IPR확보 가능성		- 높음
표준화 현황 및 전망		- ITU-T, W3C, OASIS 위주의 표준화 활동이 지속될 것으로 전망됨 - 기존의 유선 환경에서의 비즈니스 서비스를 위한 웹서비스 정보보호 기술은 이미 성숙된 상태이며, 유비쿼터스 웹서비스 보안, 웹 2.0 보안, 시맨틱 웹서비스 보안 등의 아직 국제 표준화가 초기 단계에 있는 웹서비스 정보보호 기술에 대한 표준화를 중점 추진
표준화 기구/ 단체	국내	- TTA, 유비쿼터스 웹 포럼
	국외	- ITU-T, W3C, OASIS, OMA
	국내참여 업체 및 기관현황	- ETRI, KISA, TTA
	국내기여도	- 모바일 웹서비스 보안 표준이 ITU-T에서 국제 표준화 되고 있음
표준화 수준	국내	- 표준기획-권고/초안개발및검토
	국외	- 표준기획-권고/초안최종검토및승인
국내표준화의 인프라수준 (시장요구정도 및 참여도)		- 높음

구분		응용보안
표준화항목		Lawful Interception
시장 현황 및 전망	국내	- LI 국내 시장이 형성되어 있지 않은 실정이고, 불법적인 감청 위주의 법제도화로 인해 수입 역시 어려운 상황임 - 비밀통신보호법 개정안 통과 시 LI 관련 국내 시장이 국외 제품에 의해 잠식 가능성 있는 것으로 판단됨
	국외	- 미국 및 유럽 주요 국가를 중심으로 LI 관련 법제화가 이미 이루어짐 - IPTV 및 VoIP(Skype)의 대중적 사용으로 인해 국가별 합법적 감청의 필요성이 증대하고 있음 - 아시아 권역에서 암호화된 데이터에 대한 합법적인 분석방법에 대한 기술 수요 증대
기술 개발 현황 및 전망	국내	- 필요에 따라 국가기관에서 장비를 구입하여 사용함 - 국정원에서 공적인 목적으로 개발을 주도하여 사용한 바 있음
	국외	- ETSI 및 주요 기업들은 이미 자체 표준 기술 규격에 대한 검증 작업을 착수하여 성공적인 결과를 도출하고 있는 실정임 - Cisco 일부 router 및 gateway 장비에 LI 기능이 탑재되어 판매되고 있음 - 이외 다수의 장비업체가 LI 기능 및 서비스를 제공하는 상용 제품을 판매중임
기술 개발 수준	국내	- 유선 및 이동 단말에 대한 감청 프로토타입 장비/소프트웨어 구현 가능 수준임 - 기술 초기 단계
	국외	- LI 관련 메커니즘 및 아키텍처를 상용제품화 시킬 수 있는 수준임 - 암호화된 데이터에 대한 분석 방법에 대한 기술 개발 미흡 - 기술 성장 단계
	기술격차	- 2~3년
	관련제품	- Cisco 12000 series router - Cisco AS series universal gateway- CCS CMDA, GSM 감청장비 - 그 외 Collection system 등
IPR 보유현황	국내	- 10여건의 유선 감청 특허 등록 - 3건 미만의 이동 감청 특허 출원
	국외	- ETSI에 관련 표준문서 다수 존재 - 암호화된 데이터에 대한 분석 방법에 대한 기술 개발 미흡
IPR확보 가능분야		- 국내/국제 특허, 논문 - BcN 기반의 신규 서비스망에서 암호화된 데이터의 합법적인 분석 방법 및 구조 등
IPR확보 가능성		- 보통 (BcN 환경 고려)
표준화 현황 및 전망		- ETSI 위주의 표준화 활동이 지속될 것으로 전망됨 - 기존 기술은 유선망에서의 감청 분야에 집중되어 있으므로, BcN 기반의 신규 서비스망에서 암호화된 데이터에 대한 합법적인 분석 방법 및 구조 분야에 표준화 필요
표준화 기구/ 단체	국내	- TTA
	국외	- ETSI, ATIS, TIA - 3GPP, IETF
	국내참여 업체 및 기관현황	- ETRI, 전파연구소 - LG전자, 삼성전자 - SK텔레컴, KT - 대우통신, 데이콤 - 하나로통신, 머큐리 - KTF, 현대시스콤
	국내기여도	- 거의 없음
표준화 수준	국내	- 국외표준 수용
	국외	- 표준안기획 - 표준안항목승인
국내표준화의 인프라수준 (시장요구정도 및 참여도)		- 높음 - 통신비밀 보호법 개정안 통과 예상 - 암호화된 데이터에 대한 합법적인 분석방법에 대한 표준화 요구 증대

구분		평가인증
표준화항목		정보보호 평가
시장 현황 및 전망	국내	- 정보보호 평가에 대한 인식이 부족하나 최근 중요성을 인식하고 시장의 확대되고 있는 추세임
	국외	- 유럽, 일본 등을 중심으로 정보보호 평가 분야가 급속히 활성화 됨.
기술 개발 현황 및 전망	국내	- 기존의 위험분석 표준을 새로운 환경에 적합하도록 개보수 작업이 필요하며 정보보호 아키텍처, 성과측정 등 새로운 지침 및 표준개발이 요구됨 - 정보보호 관리기술은 정보보호 관련 전문 공공기관 및 민간기업에서 여러 지침 및 기준 등을 개발하고 있으며 특히 정보보호컨설팅 업체를 중심으로 위험분석 도구개발을 중심으로 기술개발이 이루어지고 있음
	국외	- 암호 모듈 평가를 위한 요구사항 국제 표준으로 승인 (2006년 3월) - 인적, 관리적 부분을 평가에 포함하는 운영시스템 보안성 평가 기술문서 발간 (2006년 3월) - IT 보안성 보증 프레임워크 (2007년 10월, 예정) - IT 보안성 평가기준 버전 3.1(2008년 5월, 예정) - 바이오 인식 보안성 평가 프레임워크 (2008년 11월, 예정)
기술 개발 수준	국내	- 한국정보보호진흥원(KISA), 한국산업기술시험원(KTL), 한국시스템보증(KOSYAS)에서 정보보호 평가
	국외	- 기준, 가이드 개발
	기술격차	- 1년
	관련제품	-
IPR 보유현황	국내	
	국외	
IPR확보 가능분야		- 통신 분야 및 무선 통신 분야의 정보보호 평가 체계의 개발을 통한 도구를 통하여 IPR 확보가 가능함
IPR확보 가능성		- 수용/적용
표준화 현황 및 전망		- 정보보호시스템 평가 관련 표준 현황은 ISO/IEC JTC1 SC27에서 활발하게 진행 - 기존 표준의 완성도를 향상하기 위한 표준들이 개발될 예정임 - ISO/IEC JTC1에서 개발된 정보보호 평가에 대한 표준은 모든 분야에 적용될 수 있는 표준으로, 앞으로는 특정 분야에 적용될 수 있는 정보보호 평가에 대한 표준이 ITU-T, ISO/IEC JTC1에서 추진될 예정임
표준화 기구/ 단체	국내	- TTA, 기술표준원
	국외	- ISO/IEC JTC1 Sc27, ITU-T
	국내참여 업체 및 기관현황	- KISA, ETRI
	국내기여도	
표준화 수준	국내	- 권고/초안개발및검토
	국외	- 권고/초안개발및검토
국내표준화의 인프라수준 (시장요구정도 및 참여도)		- 보통

구분		평가인증
표준화항목		보안관리
시장 현황 및 전망	국내	- 보안관리에 대한 인식이 부족하나 최근 정보보호관리체계의 중요성을 인식하고 시장의 확대되고 있는 추세이며, IT거버넌스 중심으로 하여 최근 급속히 이슈화되고 있음
	국외	- 유럽, 일본 등을 중심으로 정보보호관리체계 인증이 급속히 활성화 되어, 전세계적으로 인증 발급 건수가 2천여건이 넘고 있음
기술 개발 현황 및 전망	국내	- 보안관리 관련 지침은 한국정보통신기술협회(TTA)에서 제정하는 정보통신단체표준, 정보통신부에서 제정하는 한국정보통신표준(KICS), 기술표준원에서 제정하는 한국산업규격(KS)로 구성됨 - 기존의 위험분석 표준을 새로운 환경에 적합하도록 개보수 작업이 필요하며 정보보호 아키텍처, 성과측정 등 새로운 지침 및 표준개발이 요구됨 - 정보보호 관리기술은 정보보호 관련 전문 공공기관 및 민간기업에서 여러 지침 및 기준 등을 개발하고 있으며 특히 정보보호컨설팅 업체를 중심으로 위험분석 도구개발을 중심으로 기술개발이 이루어지고 있음
	국외	- ISO를 중심으로 기존 ISO13335 기존을 ISO27000 시리즈로 편입하여 보안관리 시리즈를 계속 개발 · 보급하고 있으며, 보안관리에 관련된 각종 지침, 가이드를 개발중에 있음
기술 개발 수준	국내	- 보안관리에 관련하여 다양한 지침, 가이드 등을 개발 · 보급 중에 있고, 보안관리에 관련된 국내표준을 2002년부터 개발하여 실무에 적용하고 있음 - TTA에서 정보보호관리와 관련하여 정보보호관리표준, 위험분석방법론 모델, 정보시스템 구축준비 단계의 보안지침서, 정보시스템 비상계획 및 재해복구에 관한 지침서, 컴퓨터 바이러스 방지 지침 등 5건의 표준 제정
	국외	- 기준, 가이드 개발
	기술격차	- 1년
	관련제품	-
IPR 보유현황	국내	
	국외	
IPR확보 가능분야		- 통신 분야 및 무선 통신 분야의 정보보안 관리체계의 개발을 통한 도구를 통하여 IPR 확보가 가능함
IPR확보 가능성		- 수용/적용
표준화 현황 및 전망		- 기존 표준의 완성도를 향상하기 위한 표준들이 개발될 예정임 - ISO/IEC JTC1에서 개발 · 평가와 관리체계 인증에 대한 표준은 모든 분야에 적용될 수 있는 표준으로, 앞으로는 특정 분야에 적용될 수 있는 평가와 보안 관리 체계에 대한 표준이 ITU-T, ISO/IEC JTC1에서 추진될 예정임
표준화 기구/ 단체	국내	- TTA, 기술표준원
	국외	- ISO/IEC JTC1 Sc27, ITU-T
	국내참여 업체 및 기관현황	- KISA, ETRI, 중앙대학교
	국내기여도	
표준화 수준	국내	- 권고/초안개발및검토
	국외	- 권고/초안개발및검토
국내표준화의 인프라수준 (시장요구정도 및 참여도)		- 보통

3. 중점 표준화항목의 표준화 추진전략

3.1. 중점기술의 표준화 환경분석

3.1.1. 표준화 추진상의 문제점 및 현안사항

- 응용보안 영역에서의 표준화를 선도하기 위해서는 신규 응용 서비스에 대한 표준 개발에 주력해야 하며, 표준화 추진 시 기술 개발을 병행하여 적극적인 검증 및 적용 가능성을 타진해야 함. 특히 응용보안 영역은 IT839에서 추진 중인 주요 응용 서비스, 네트워크 (BcN, USN) 등의 환경을 기반으로 하므로 이러한 기술에 대한 상호 협력이 필요함
- 즉, 서비스 및 네트워크 기술과의 원활한 조유를 위해서는 해당 기술과 관련한 보안 표준이 명확히 제시되어 있어야 하는데 이는 표준안을 바탕으로 병행적으로 개발된 결과물의 직접적인 연동을 통해 응용보안 표준안 및 개발 성과 그리고 연동에 대한 검증 및 결과분석이 체계적으로 진행될 수 있기 때문임. 이를 통해 표준안 기반의 제품의 실적용 가능성을 정확히 타진할 수 있어, 표준안 자체의 Quality를 역검증할 수 있는 좋은 방안이 됨
- 국내에서 제안하고 있는 정보보호 분야의 표준화는 응용보안의 경우 IETF를 중심으로 진행되고 있고, 통신망 보안의 경우 ITU-T SG17을 중심으로 추진하고 있음. IETF에서 보안 분야 표준화의 경우, 인터넷 응용분야 보안을 중심으로 활동하며, 통신망 보안의 경우 ITU-T SG17에서 많은 국내에서 제출된 기고서를 중심으로 표준화를 진행하고 있음
- 기존의 IETF, ITU-T SG17 표준화 단체를 중심으로 한 표준화 활동의 추진은 현재까지 약 8개의 RFC 개발이라는 성과를 낳았으며, 현재 추가적인 표준화 항목의 선정이 요구되고 있는 실정임. 즉, 두 단체에서의 집중화된 표준화 활동은 국제 표준화 참여를 위한 주요한 도약의 계기를 마련해 주는 강력한 역할을 수행하고 있음
- NGN 보안에 관한 경우, ITU-T SG13 Q.15를 중심으로 추진되고 있고, 현재 보안 요구사항에 대한 표준이 완성되어 있는바, 여타 분야의 표준 개발을 통한 참여가 요구되고 있음
- 즉, "u지식, IPTV, P2P, VoIP, STC, SPAM대책" 등과 같은 신규 응용 서비스의 창출 및 이에 따른 보안 환경의 다변화 그리고 새로운 보안 요구사항의 등장은 기존에 국제 표준안의 국내 수용내지는 일부 참여만으로 그친 국내 표준화 활동의 수준을 표준화 Leader의 입지로 변모시킬 수 있는 좋은 기회를 부여하고 있어 기존 표준화 전략에 시사하는 바가 크다고 할 수 있음
- 또한 신규 응용 서비스 영역의 발굴 및 기존 영역의 확대 적용에 따라, 관련 기술 규격의 표준안 선점을 시도하기 위해 상호 운용성 확보 및 통합의 명목을 들어 "ETSI, OASIS, W3C, 3GPP, OMA, MPEG-21" 등의 비교적 신생의 전문적 영역에 관련한 국제 표준화 단체가 설립되고 있지만. 이에 대한 적극적인 참여 IETF 및 ITU-T SG17에 비해 다소 미흡한 것으로 판단됨. 더불어 "ISO/IEC JTC1/SC6 & SC27, NIST, ATIS" 등의 국제 표준화 기구에 대한 현황 파악 및 동향 분석이 추가적으로 요구됨
- 이와 같이 현재 시급하게 표준화가 필요한 분야가 응용보안 분야와 평가인증 분야임. 따라서 이들 분야에 대한 표준화는 IETF, ITU-T 및 관련 전문 표준화 단체를 중심으로 추진해야 하며, 과제 발굴을 통해 국제 표준화 활동 및 개발 병행하여 수행하는 것이 요구됨

3.1.2. SWOT 분석 및 표준화 추진방향

국외환경요인 \ 국내역량요인			강점 요인 (S)		약점 요인 (W)	
			시장	- 고속 인터넷 액세스망 구축으로다양한 응용서비스가 출현하여 신규 시장이 창출되고 있음 - 일반 기업의 정보보호에 대한 지속적인 투자 확대	시장	- 상대적 협소한 정보보호 시장 - 국내업체간 출혈경쟁 구도
			기술	- 정부의 확고한 지원 정책(IT839) 추진으로 인한 새로운 정보보호 서비스와 새로운 정보보호 장치 개발의 필요성 대두 - ETRI를 통한 선도 기술개발을 통한 핵심 기술 확보 가능	기술	- 기술개발 고급 인력 부족 - 정보보호 기반 기술 확보 미흡 - 정보보호 기능이 미비한 응용 위주의 IT 제품 생산 - 정보보호 기술부설연구소 및 연구개발 전담부서의 운영 미비
			표준	- KISA에 의한 CC 평가 확대 및 암호 모듈 평가 검증제도의 시행	표준	- 표준 전문가의 부족 - 보안기업의 표준 추진 의지 미진
기회요인 (O)	시장	- IPTV 가입자 유치 확대로 시장규모가 급속히 증가될 전망임 - 중국, 미국 등에서 정보보호 제품에 대한 수요 증가 추세임 - 웹 2.0 등장과 관련 시장 확산		- (시장) 잘 정비된 고속 인터넷 인프라를 이용한 IPTV, P2P, VoIP 등의 서비스의 상업화 및 수익창출이 가능 - (기술1) ETRI 등의 국책 연구기관에서 개발된 선도 기술의 국제화 추진 - (기술2) u지식, STC, 차세대 웹서비스 등의 신규 서비스에 대한 신속한 연구개발을 통해 관련 기술 규격 정립 및 상용화 추진 - (표준1) BcN, RFID/USN, 디지털방송, 디지털콘텐트 등의 국내 독자 IPR 개발 및 이를 바탕으로 국제 표준화를 추진하는 전략적 활동을 추진 - (표준2) ITU-T, ISO/IEC JTC1, IETF 등을 통한 활발한 정보보호 국제 표준화 활동 역량 강화 - (표준3) IPTV 보안 국제 표준화를 ITU-T를 통하여, VoIP보안은, IETF를 통하여 표준화 추진 - (표준4) 표준화를 통한 기술규격 제정 시 응용 적용 가능성을 적극적으로 고려해야 함	- (시장1) 중장기적인 보안시장 개방을 통해 열악한 대외의존도를 탈피하고 국내 기업의 보안기술 경쟁력 확보 - (시장2) 응용 서비스 보호 및 평가인증 분야에 대한 지속적인 R&D 투자액 증가를 통해 산업 활성화 도모 - (기술1) IPTV 신규 보안 요구사항을 발굴하고 대응책을 연구개발하여 CAS 중심의 보안기술 종속에서 탈피 - (기술2) 안전하고 신뢰성 있는 환경 구축을 위한 P2P 응용보안 기술개발 - (표준1) 자체 응용보안 IPR을 확보하고 이를 준수한 국내제품을 출시하여 세계 정보보호 시장을 개척함 - (표준2) 기존 IETF, ITU-T에 편중되어 있는 표준화 노력을 전문 국제 표준화 단체(MPEG-21, OMA, P3P, ETSI, W3C)로 확대하는 신규전략이 요구됨
	기술	- u지식, IPTV, STC, VoIP, P2P, SPAM 차단, 차세대 웹서비스 등의 IT 서비스에 대한 보안기술 개발 필요성 증가 - u지식 및 STC의 경우 아직까지 국내외에서 구체적 성과물 전무 - 핵심 응용서비스를 지원할 수 있는 관련 기술 및 인프라가 확보된 상태임				
	표준	- VoIP 표준개발이 활발히 추진됨 - IPTV 표준안 제정 활동이 ITU-T FG에서 한국 주도로 진행 중임 -디지털콘텐트는 MPEG-21, OMA, OASIS 등을 중심으로 진행 중이나 u지식정보보호에 대한 활동 및 전문 표준화단체는 전무함				
위협요인 (T)	시장	- 기술종속으로 인하여 해외 보안 시장 진입 장벽을 넘지 못함 - 지나치게 폐쇄적인 시장구조 (정보보호 부문 대외의존도 15%)				
	표준	- 표준화 지연으로 응용보안 기반의 서비스개발이 지연될 가능성 - 국제표준안 수용 등의 수동적인 전략으로 자체 IPR 확보가 미비 - 해외 지적재산권 확보가 미흡 - 주요 IT벤더들의 적극적인 표준안 제정 참여 및 자체 Alliance 또는 전문단체를 구성하는 추세		- (시장) 정보보호 수요가 큰 해외 시장을 대상하여 중장기적으로 마케팅 전략을 수립 - (기술1) 지속적인 정보보호 고급 인력 양성을 통한 자체 기반 기술 확보및 국내제품 경쟁력 강화 - (표준화1) 신규 응용서비스에 대한 정보보호 표준화를 통해 원활한 서비스 및 장치 제공 - (표준화2) 정부의 표준 전문가 양성 프로그램의 확대를 통한 정보보호 산업체 인사의 표준 개발 참여 확대	- (시장1) 전략 분야의 선정 및 전문화된 분야의 기술개발을 통한 외국 선진 기업에 의한 정보보호 시장 잠식의 최소화 - (시장2) 투자대 환수의 개념를 탈피한 잠재 피해 계산 개념을 적용한 정책적 지원을 통한 정보보호 제품 구매 확대 정책 시행 - (기술) MS 등의 대형 벤더와 보안 기술 개발 및 표준화를 공조하여 추진하고 관련 기술인력 양성에 협력함 - (표준1) 국제 표준 적극 수용 및 해외 표준 전문가 영입하여 표준 활성화
	기술	- 막강한 자본과 기술력을 갖고 있는 CISCO 등의 네트워크 회사 및 MS 등의 운영체제 회사의 통합 정보보호 제품 개발 및 출시 등에 의한 국내 시장 잠식 - 응용보안을 관련한 원천 핵심 기술력 부족 (세계 100대 보안기업중 국내기업이 5개뿐인 실정)				

SO전략 : 공격적 전략(강점사용-기회활용)
WO전략 : 만회전략(약점극복-기회활용)
ST전략 : 다각화 전략(강점사용-위협회피)
WT전략 : 방어적 전략(약점최소화-위협회피)

• 현황분석을 통한 우선순위

- 응용보안 분야로 "u지식정보보호, VoIP 보호, 응용보안 강화 프로토콜, 안전한 P2P 보안, IPTV 정보보호, STC 정보보호, 차세대 웹 보안, Lawful Interception" 등의 총 7개의 표준화 항목을 선정함
- 더불어 평가인증 분야가 표준화 영역으로 선정됨

• 표준화 추진방향

- "u지식, IPTV, P2P, VoIP, STC, SPAM대책"등과 같이 시장성이 확대 및 발굴된 응용서비스에 대해서는 아직까지 국제 표준단체의 제정 노력이 일관되지 않은 실정이며, 적극적인 표준화 활동이 미비한 것으로 판단되므로 이를 신규 응용보안 분야로 지정하여 신규 표준 개발에 주력할 필요성이 있음. 이는 기존에 잘 알려지거나 상업용으로 상당히 진전된 기술력을 바탕으로 성숙된 시장을 가진 응용 서비스에 대한 표준화 노력에 비해 상대적으로 주도적 활동을 이끌 수 있을 것으로 기대됨. 이를 위해서는 다음과 같이 전략적이고 신속한 표준화 움직임이 요구됨
- (u지식 보안) 디지털 콘텐츠의 제작/유통/관리/보호 등에 대한 관심이 높아지고 있으며, MP3와 같은 일부 멀티미디어 콘텐츠에 대해서 DRM 등의 보호기법이 적용되고 있는 실정임, 그러나 디지털 콘텐츠 표준 기술 규격이 채택된 바 없으며, MPEG21, IRTF/IETF, W3C 등에서 상의한 표준안을 바탕으로 치열한 선점 양상이 벌어지고 있음, 또한 UCC와 같은 신규 매체의 등장, 디바이스 상호 운용성, N:N 네트워크 환경, 콘텐츠 전달의 다방향성 및 익명성 등을 고려한 표준화 노력은 극히 미비한 것으로 판단되어 이 부분에 대한 국내 연구계의 노력이 요구됨
- (VoIP 보안) 정부는 최근에 VoIP 보안 문제를 해결하기 위한 로드맵 완성을 위한 연구반을 만들고, 금년 말까지 장기적인 차원의 보안 문제를 대처하려 하고 있으므로, 2008년까지 장기적인 표준화 로드맵의 개발이 필요함
- (응용보안 강화 프로토콜) ITU-T SG17의 Q.9에서 SPAK[18] 표준화를 진행 중이고, Q.5에서 PAK의 표준화를 올해 4월 회의에서 완료한 바 있음, IETF에서는 OTP[19] 관련 RFC 3건이 등록된 상태임, 향후 통신망 보안 및 금융망 보안을 위한 기반 패스워드 인증 프로토콜로 이용될 가능성이 있으므로, 표준의 활용성이 매우 높을 것으로 예측됨
- (안전한 P2P 보안) 이미 인터넷 사용자의 대다수가 사용할 정도의 넓은 이용 층을 확보하고 있는 P2P 응용프로그램 및 네트워크의 보안에 대한 표준화 논의가 ITU-T SG17의 작업반 Q.9에서 X.p2p-1와 X.p2p-2와 같은 두 개의 프로젝트로 나뉘어 수행되고 있음, 또한 IETF의 XMPP, SIMPLE. P2PSIP 작업반과 IRTF의 P2PRG 연구그룹이 관련 표준화를 진행하고 있음
- (IPTV 보안) ITU-T의 IPTV FG에서 이미 800여개의 기고서가 상정되었고, 이중 20개의 작업문서가 제정된 바 있음, AT&T, NTT, Lucent Technologies, Notel, Cisco 등의 다국적 기업에서도 활발한 표준화 활동을 보이고 있음, 국내의 경우 BcN과 관련하여 IPTV 표준을 주도하고 있으나, 유비쿼터스 네트워크의 단일화된 콘텐츠 전달 게이트웨이로 부상하고 있는 IPTV의 다양한 특성을 반영한 보안에 대한 검토 및 이의 표준화는 미비한 것으로 판단됨, 기존의 DRM 및 CAS를 활용한 방안 이외의 보안성 검토 작업이 적극적으로 요구됨
- (STC) 국외 STC 기술 표준은 이미 완성도가 매우 높으며, 일부 분야에서 표준 개발이 진행중에 있음. 따라서 국내

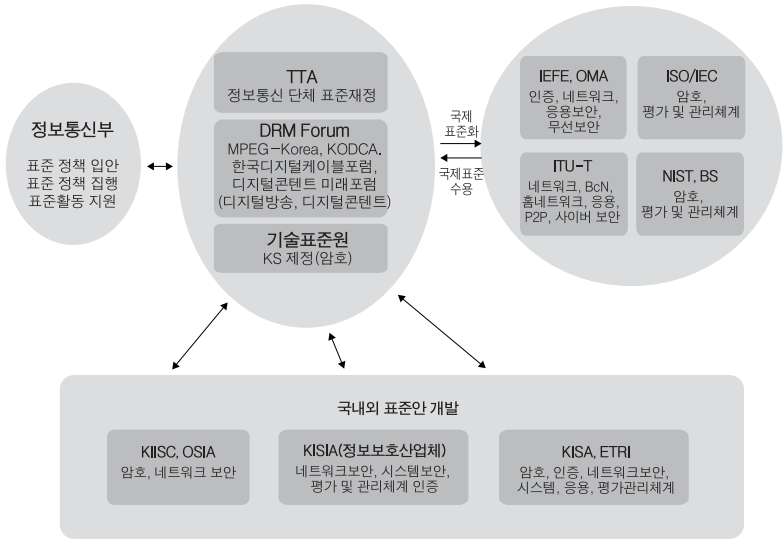
18) Secure Password-based Authentication Protocol with Key exchange
19) One Time Password

에서는 이미 성숙된 국제 표준을 국내 표준으로 준용함과 동시에, 기술 우위에 있는 일부 분야에서는 국제 표준화에 적극 참여하는 전략이 요구됨

- (차세대 웹 보안) 기존의 유선 환경에서의 비즈니스 응용 서비스를 위한 웹서비스 정보보호 기술 표준은 이미 성숙된 상태이나, 향후 기술 수요가 증가하리라고 예상되는 유비쿼터스 환경하에서의 다양한 서비스 및 디바이스 연동 및 통합을 위한 차세대 웹서비스 정보보호 기술은 아직 기술 개발 초기 단계임. 따라서 유비쿼터스 웹서비스 보안, 모바일 웹서비스 보안, 시맨틱 웹서비스 보안, 웹 2.0 보안 기술 등의 차세대 웹서비스 정보보호 기술들에 대한 국제 표준화를 적극적으로 추진하는 노력이 필요함
- (Lawful Interception) 유럽의 ETSI 주도로 합법적 감청에 대한 표준화가 진행되고 있으며, 이미 31건의 표준화 문건이 제정되어 작업이 진행되고 있음, IETF의 경우 Cisco 주도로 한건의 RFC가 2003년도에 채택된 바 있음, 국내의 경우 공공의 목적 또는 수사권 확보를 위한 무선 및 이동통신망에서의 합법적 감청에 대한 요구가 현실화되고 있는 시점이므로, 기술적 종속을 회피하기 위해서는 적극적인 무선 및 이동통신망에서의 감청 장비 및 시스템에 대한 표준화 노력이 필요한 것으로 사료됨
- ITU-T의 네트워크 및 응용보안 분야의 완성도가 높은 기존 표준을 선정하여, 국내 표준화를 적극적으로 추진함.
- (정보보호 평가 및 보안관리) 현재 국제 공통평가 기준 상호인정협정에 따라 공통평가 버전을 2.3에서 3.1로 대체하는 작업을 수행 중이며, 인증서 발행국으로 활동하고 있어, 특정제품군 또는 보안영역에 대한 평가 및 인증 지배권을 강화할 필요성 있음

3.1.3. 표준화 추진체계

- 응용보안 및 평가인증 분야



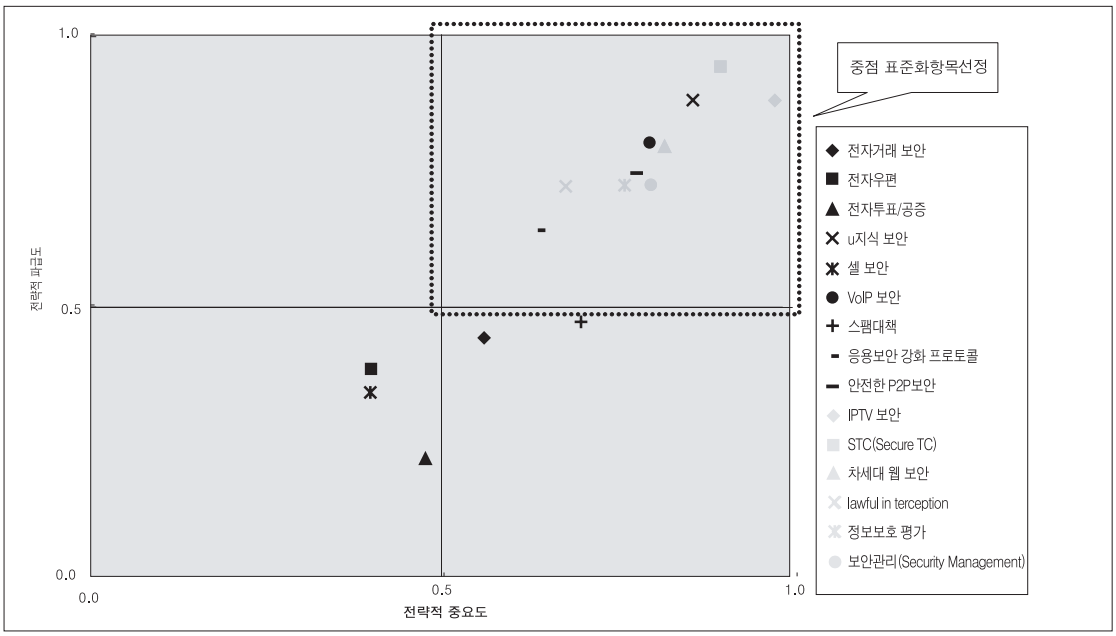
〈그림 7〉정보보호기술 표준 추진 체계

- 응용보안 표준은 KISA, ETRI, KISIA(정보보호산업체)가 표준을 개발하고, 국내 표준은 TTA 및 DRM Forum, MPEG-Korea 등의 디지털방송 및 콘텐트 관련 단체를 통하여, 국제 표준은 IETF, ITU-T, ISO/IEC를 통하여 표준화를 추진함
- 평가 및 관리체계 인증 표준은 ISO/IEC, ITU-T를 통하여 국제 표준을 수용하거나 추진하며, BS 표준을 참조하며, TTA를 통하여 국내 표준을 추진하고, KISA와 정보보호산업체를 통하여 국내 표준을 개발함
- 국내 표준 개발절차는 ETRI, KISA, KIISC, 그리고 정보보호 산업체에서 국내 표준안이 개발되며, 이들중 시기가 긴박한 표준은 ISTF를 통하여 사실표준화를 추진하고, 이후 TTA를 통하여 정보통신단체 표준으로 개발함. 암호 알고리즘은 기술표준원의 KS 표준화함. 정보통신 단체 표준은 TTA TC1 위원회를 통하여 추진함

3.2. 중점 표준화항목 선정

3.2.1. 중점 표준화항목 선정방법

표준화 대상항목에서 중점 표준화항목 도출을 위한 데이터입력												
	전략적 중요도						전략적 파급도					
고려요소	P1 산학연 관심도 (투자 등)	P2 정부 관심도 (정책 등)	P3 표준선도 가능성(표준투자정도)	P4 표준(기술) 개발의 시급성	P5 기술(표준) 격차	PI (Priority Index)	E1 타 산업 파급효과	E2 경제적 파급효과	E3 국내외시장규모	E4 IPR 확보가능성 (로얄티수입)	E5 사용자편의 (호환성/공공성 등)	EI (Effect Index)
고려요소별 가중치(합계1)	0.2	0.2	0.2	0.2	0.2	1	0.2	0.2	0.2	0.2	0.2	1
전자거래보안	4.0	3.0	2.0	2.0	3.0	0.56	3.0	2.0	2.0	1.0	3.0	0.44
전자우편	2.0	1.0	1.0	1.0	5.0	0.40	1.0	1.0	2.0	0.0	5.0	0.38
전자투표/공증	2.0	3.0	3.0	1.0	3.0	0.48	1.0	1.0	1.0	0.0	2.0	0.22
u지식 보안	5.0	5.0	4.0	4.0	3.0	0.86	4.0	5.0	4.0	4.0	4.0	0.88
셀보안	2.0	1.0	1.0	1.0	5.0	0.40	1.0	1.0	1.0	1.0	4.0	0.34
VoIP보안	4.0	4.0	3.0	5.0	4.0	0.80	4.0	3.0	4.0	4.0	5.0	0.80
스팸대책	3.0	4.0	3.0	4.0	4.0	0.72	3.0	2.0	2.0	2.0	3.0	0.48
응용보안 강화 프로토콜	3.0	3.0	3.0	3.0	4.0	0.64	3.0	3.0	3.0	3.0	4.0	0.64
안전P2P보안	3.0	4.0	5.0	4.0	4.0	0.80	4.0	3.0	3.0	4.0	4.0	0.72
IPTV보안	4.0	5.0	5.0	5.0	5.0	0.98	4.0	4.0	4.0	4.0	4.0	0.88
STC(Secure TC)	4.0	5.0	5.0	5.0	3.0	0.90	4.0	5.0	4.0	5.0	4.0	0.94
차세대 웹 보안	4.0	4.0	4.0	4.0	4.0	0.82	4.0	4.0	4.0	4.0	4.0	0.80
lawful interception	3.0	4.0	2.0	4.0	3.0	0.68	2.0	4.0	2.0	4.0	5.0	0.72
정보보호 평가	3.0	5.0	3.0	4.0	4.0	0.76	3.0	4.0	4.0	3.0	4.0	0.72
보안관리(Security Management)	4.0	4.0	4.0	4.0	4.0	0.80	4.0	4.0	4.0	3.0	3.0	0.72



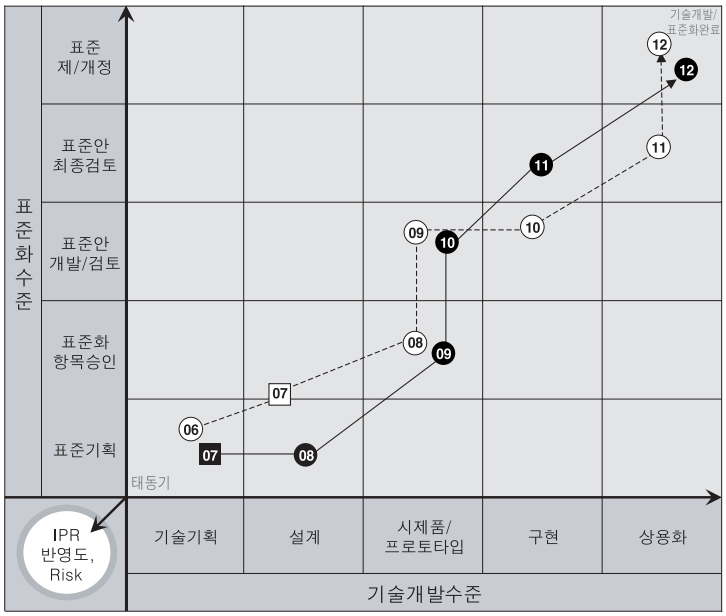
3.2.2. 중점 표준화항목 선정사유

- 전략적 중요도 및 기술적 파급효과의 요소
  - 인터넷 활성화를 기반으로 다양한 응용서비스 창출로 인하여 응용보안 분야의 중요성이 급증하며, 새롭게 출시되는 정보보호 관련 제품 및 서비스를 평가하고 관리할 수 있는 체계적 표준화는 IT산업 전체에 커다란 파급 효과를 갖는 분야임
  - 응용 서비스 산업과 긴밀하게 연계되어 있음
  - 국민의 편리성과 대중성을 만족시킬 수 있음
- 중점 표준화항목별 선정사유
  - 응용보안 분야의 경우, 분야별로 다양한 서비스 및 제품에 밀접한 관련이 있어 파급효과가 지대함
  - VoIP, IPTV, P2P, 차세대 웹, STC 등 최근 국제 표준화 기구에서 활발하게 표준화가 추진되고 있는 신규 응용보안 분야를 선정함
  - 정보화 육성을 위한 정부의 추진 의지가 매우 큰 만큼 응용 서비스 정보보호와 평가인증 분야의 표준화가 시급
  - 신규응용의 경우, 국민의 생활과 긴밀하게 연계되어 있음

3.3. 중점 표준화항목별 세부전략(안)

3.3.1. u-지식 보안

- 표준상태전이도 (표준화 & 기술개발 연계분석)

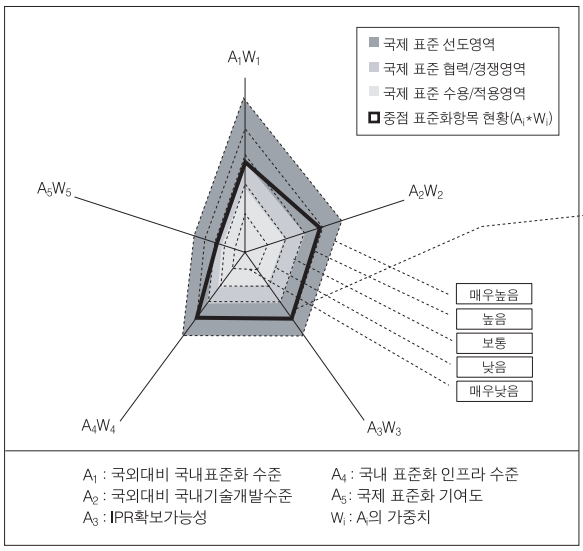


표준화 중요도	국내 개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★★★	TTA	ETRI	ITU-T, DVB, OMA

범 례

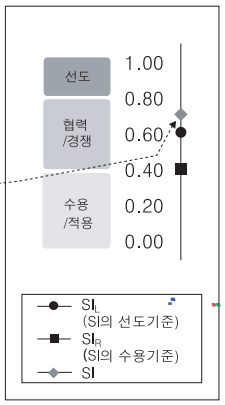
07 : 중점 표준화항목의 국내상태
07 : 중점 표준화항목의 국제상태
→ : 중점 표준화항목의 국내 표준상태전이
⇢ : 중점 표준화항목의 국제 표준상태전이
↑ : 선행표준(선 표준화 후 기술개발)
↗ : 동시표준(표준화&기술개발 동시추진)
↓ : 후행표준(선 기술개발 후 표준화)

- 국제표준화 전략목표 도출



A1 : 국외대비 국내표준화 수준
A2 : 국외대비 국내기술개발수준
A3 : IPR확보가능성
A4 : 국내 표준화 인프라 수준
A5 : 국제 표준화 기여도
Wi : Ai의 가중치

SI (표준화 전략지수)	
SI_L (SI의 선도기준)	0.60
SI_R (SI의 수용기준)	0.40
SI	0.72



$$SI = (\sum_{i=1}^{5} A_i \cdot W_i) / 5$$
$$(0 < W_i < 1, 0 < SI \leq 1)$$

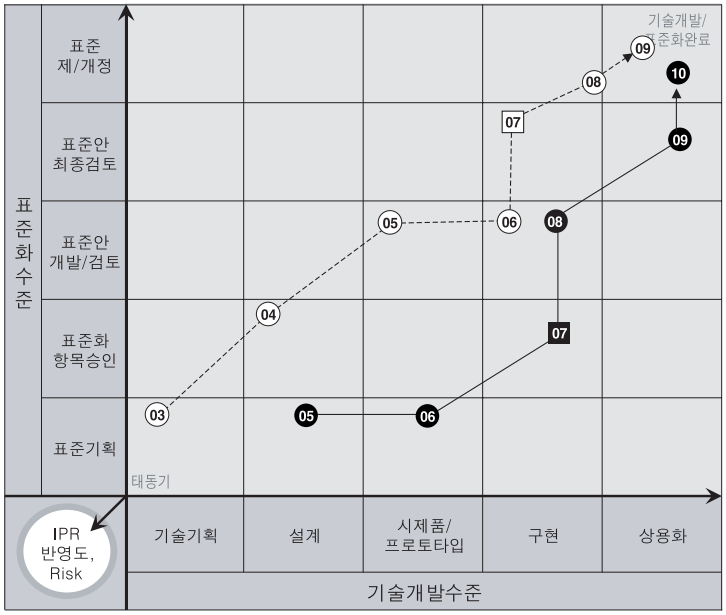
국제표준 선도

• 세부전략(안)

개 요		- 유비쿼터스 환경에서 융복합 콘텐츠 보호 서비스를 제공하기 위한 지식 보호 기술은 선 국내 표준화 추진 후, ITU-T SG17 에서 표준화 요구됨 - u-지식 보안 기술은 OMA, DVB 등에서 모바일 및 IPTV 등의 지식보호 관련한 De factor 표준화 요구됨
항목별 전략	국내외 표준화 현황 분석에 따른 세부 전략	- MPEG-21, OMA에서는 DRM 표준화를 추진하였고, 국내 표준화를 위해서 TTA에서 DMB-CAS, EXIM 표준화를 추진하였음 - CAS를 SW 형태로 다운로드하여 단말 트러스트를 제공하는 지식보안 기술 표준화와 관련하여 오픈케이브랩스에서 표준화를 추진중에 있으므로, 국제 표준화에 적극 참여함 - 음악 보호 파일에 대한 상호연동을 위해 EXIM을 표준화하였으나, 서비스 사업자간 호환성과 과금 방식에 추가 표준화가 필요한 상태임
	국내외 기술개발 현황 분석에 따른 세부 전략	- 국내에서는 SW 및 실명ID 기반의 DRM, CAS 등의 지식보호 솔루션을 개발 및 상용화를 진행하고 있으나, 복합지식 보호 및 프라이버시 보호기술 표준화가 요구됨 - 전용 디바이스 단위로 권한관리를 추구하는 음악지식(MP3)에 대한 보호 솔루션은 있으나, 자신 소유의 타 디바이스로 구매 지식의 이동 불가로 사용자 불편을 초래하고 있어, 이에대한 기술 개발과 더불어 표준화가 요구됨 - 사용자 창작/수정/재가공 지식에 대한 지재권보호 및 지분표현 기술 분야 개발이 미약한 수준이므로, 기술개발과 표준화를 동시에 추진함
	국내 IPR 보유 현황분석 및 확보가능성 분석에 따른 세부 전략	- 콘텐츠 불법복제 분야는 이미 많은 국외 IPR이 확보된 분야로 불법복제를 제외한 타분야에 IPR 확보 집중할 필요가 있음 - ' 미국 Microsoft 등에서 지식보호 기술 전분야 출원이 400건을 넘고있으므로, 사용자 익명 ID 제공 기술 및 Downloadable-TPM 기반 지식보안 단말, 프로슈머 유통구조를 갖는 계층적 지재권 보호 등의 분야에서 핵심 IPR 확보를 위해 기술개발을 추진함
	국내 표준화 인프라 수준 분석에 따른 세부 전략	- 국내 인터넷 인프라는 세계 최고 수준이므로, 이를 잘 활용하여 새로운 지식 서비스 산업 및 다양한 비즈니스 모델이 발굴될 수 있도록 기술 개발 및 표준화가 요구됨
	국제표준화 기여도 분석에 따른 세부 전략	- MPEG-21, OMA, DVB-CPCM, DHWG, TV-Anytime, OpenCableLab등에서 관련 분야의 표준화가 진행되고 있거나 시작되고 있으며, 향후 상용화를 위한 보다 상세한 규격화가 예상되므로, de factor 기술 분야에 표준화에 적극 참여하여야 함 - 일부 분야에서는 TTA에서 국내 표준화를 진행한 후, ITU-T SG17을 통한 국제표준화를 추진함

3.3.2. VoIP 보안

- 표준상태전이도 (표준화 & 기술개발 연계분석)

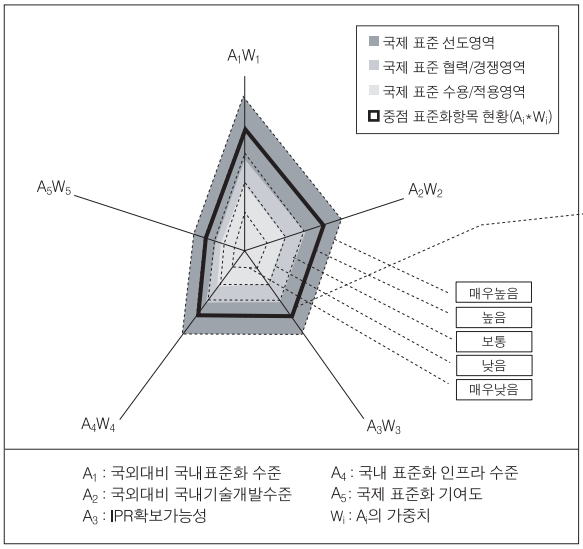


표준화 중요도	국내 개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★★	TTA	ETRI	IETF

범 례

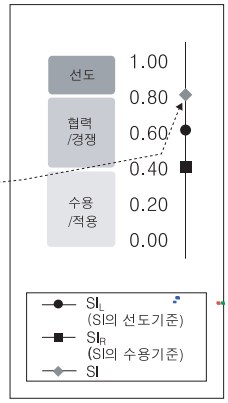
- 07 : 중점 표준화항목의 국내상태
- 07 : 중점 표준화항목의 국제상태
- → : 중점 표준화항목의 국내 표준상태전이
- ⇢ : 중점 표준화항목의 국제 표준상태전이
- ↑ : 선행표준(선 표준화 후 기술개발)
- ↗ : 동시표준(표준화&기술개발 동시추진)
- ↓ : 후행표준(선 기술개발 후 표준화)

- 국제표준화 전략목표 도출



A_1 : 국외대비 국내표준화 수준
A_2 : 국외대비 국내기술개발수준
A_3 : IPR확보가능성
A_4 : 국내 표준화 인프라 수준
A_5 : 국제 표준화 기여도
W_i : A_i의 가중치

SI (표준화 전략지수)	
SI_L (SI의 선도기준)	0.60
SI_R (SI의 수용기준)	0.40
SI	0.80



$$SI = (\sum_{i=1}^{5} A_i \cdot W_i) / 5$$
$$(0 < W_i < 1, 0 < SI \leq 1)$$

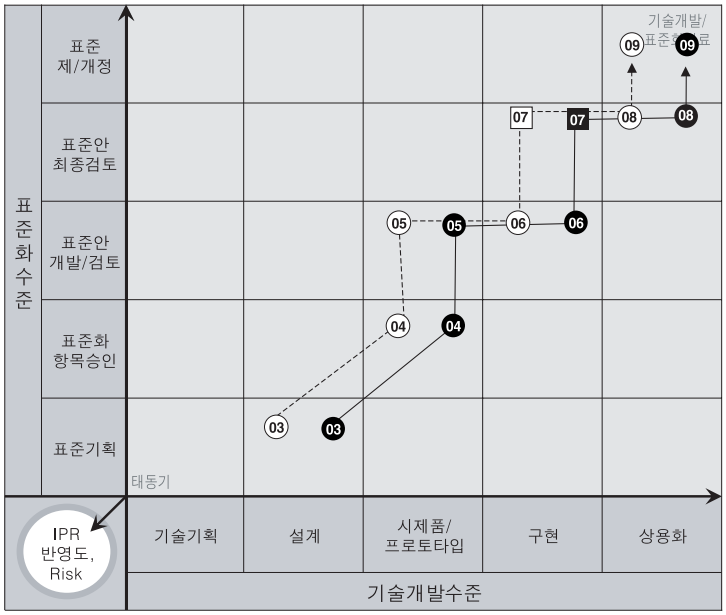
국제표준선도 (일부수용)

• 세부전략(안)

개 요		- 많은 부분 이미 개발되어 있는 표준을 수용하되, 스팸 대응책 등 분야에서 ITU-T SG17를 통하여 국제 표준화 지속 활동 요구됨 - 프라이버시 보호 메카니즘, 인증된 아이덴터티 관리, SIP SAML, SIP 스팸 대책, 암호 요구사항 등
항목별 전략	국내외 표준화 현황분석에 따른 세부 전략	- IETF의 SIPPING WG는 SIP 또는 SIP 응용 서비스와 관련된 요구사항을 표준화, SIP WG는 SIP 프로토콜과 관리 분야의 표준화, 그리고 ITU-T는 스팸 방지 관련 가이드라인 표준화 중점을 두고 있으므로, 이들 표준화 기구의 국제 표준화 활동에 적극 참여함 - 인증된 아이덴터티 관리, SIP SAML, SIP 스팸 대책 등 신규 항목에 대한 기술개발 및 표준화 추진이 필요함
	국내외 기술개발 현황 분석에 따른 세부 전략	- VoIP 스팸은 호 형태의 SPIT(Call Spam, Spam over Internet Telephony)과 메신저 서비스 기반의 SPIM(IM Spam, Spam over Instant Messaging), 프레즌스 서비스 기반의 Presence Spam의 분야로 나뉘어 학계 및 산업계 중심으로 연구 진행중 - 국내에서는 VoIP 서비스를 위한 암호/키관리 API 모듈에 연구 개발이 미흡한 실정이므로 기술 개발 및 표준화를 추진함 - VoIP 사용자의 프라이버시 보호 기술은 아직 초계 단계로 SIP를 위한 프라이버시 메커니즘이 표준으로 제공되고 있고, VoIP 프라이버시 정책에 의거 프라이버시 서비스가 제공되어야 한다고 정의하고 있으나, 그 구현 방법 등은 명시되어 있지 않으므로 표준화가 요구됨 - 사용자의 물리적, 논리적 위치정보를 다루는 VoIP 긴급통화 및 프레즌스 서비스 등 다양한 VoIP 부가서비스가 등장하고 있으나, 사용자의 위치정보 노출로 인한 프라이버시 침해 위협에 대응하기 위한 기술 개발 및 표준화기 요구됨
	국내 IPR 보유 현황분석 및 확보가능성 분석에 따른 세부 전략	- 국내 특허는 주로 채팅서비스, 컨퍼런스폰 시스템 등 응용 분야에 집중되어 있는데 반해 국외 특허는 데이터 처리 장치, 호출 제어 장치, 어댑터 장치 등 핵심 기술 분야에 집중되어 있으므로, 프라이버시 보호 메카니즘, 인증된 아이덴터티 관리, SIP SAML, SIP 스팸 대책 등 신규 분야의 IPR 확보에 집중함
	국내 표준화 인프라 수준 분석에 따른 세부 전략	- VoIP 관련 다양한 영역에서 활동하고 있는 산학연 표준전문가들이 스팸 대응책 등 분야에서 ITU-T SG17를 통하여 국제 표준화 활동을 지속적으로 추진함
	국제표준화 기여도 분석에 따른 세부 전략	- 많은 부분 이미 개발되어 있는 표준을 수용하되, 스팸 대응책 등 분야에서 ITU-T SG17를 통하여 국제 표준화를 진행함

3.3.3. 응용보안 강화 프로토콜

- 표준상태전이도 (표준화 & 기술개발 연계분석)

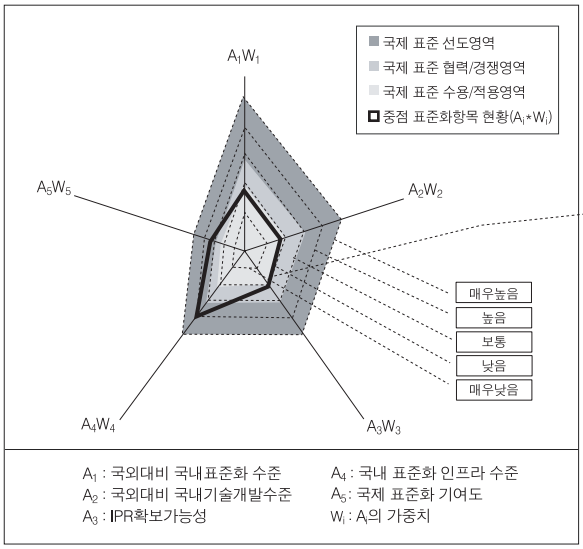


표준화 중요도	국내 개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★★	TTA	ETRI	ITU-T

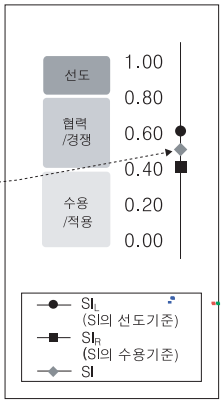
범 례

07 : 중점 표준화항목의 국내상태
07 : 중점 표준화항목의 국제상태
→ : 중점 표준화항목의 국내 표준상태전이
⇢ : 중점 표준화항목의 국제 표준상태전이
↑ : 선행표준(선 표준화 후 기술개발)
↗ : 동시표준(표준화&기술개발 동시추진)
↓ : 후행표준(선 기술개발 후 표준화)

- 국제표준화 전략목표 도출



SI (표준화 전략지수)	
SI_L (SI의 선도기준)	0.60
SI_R (SI의 수용기준)	0.40
SI	0.51



$$SI = (\sum_{i=1}^{5} A_i \cdot W_i) / 5$$
$$(0 < W_i < 1, 0 < SI \leq 1)$$

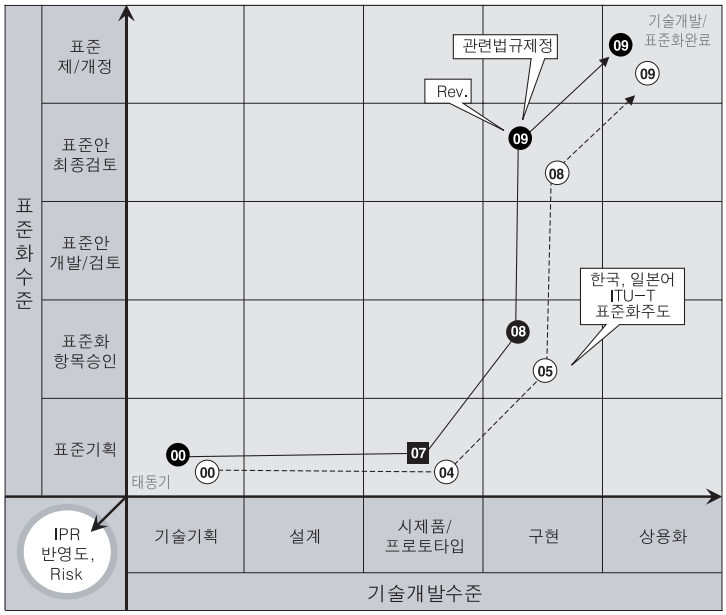
국제표준 선도 (일부수용)

• 세부전략(안)

개 요		- ITU-T SG17 을 통하여 국제 표준화의 선도가 요구됨 . 패스워드 인증 프로토콜 가이드라인, 제3의 신뢰기관을 이용한 안전한 프로토콜 등
항목별 전략	국내외 표준화 현황분석에 따른 세부 전략	- IETF, ITU-T 등에서 표준화가 진행 중에 있어 적극적인 참여가 요구되며, ITU-T의 국제표준화가 완료되면, TTA를 통해서 국내 표준으로 수용함. 주요 활동 분야는 패스워드 인증 프로토콜 가이드라인, 제3의 신뢰기관을 이용한 안전한 프로토콜 등임
	국내외 기술개발 현황분석에 따른 세부 전략	- 국내의 경우 진행 중인 기술 개발은 전무하며, 학술적 연구 위주로 진행하고 있으므로 기술 개발과 함께 표준화가 요구됨 - 국외는 IETF, ITU-T 등에서 표준화와 더불어 기술 개발을 진행 하고 있고, 산업체의 경우 패스워드 인증을 포함한 보안 제품 개발이 진행 중에 있으며, 주로 통신망 보안, 금융망 보안에 활용도가 높을 것으로 기대됨에 따라 연구소, 하계, 산업체의 보다 활발한 활동이 요구됨
	국내 IPR 보유 현황분석 및 확보가능성 분석에 따른 세부 전략	- 국내에서는 신뢰적인 제 3기관을 통한 보안 프로토콜, 이동 통신 시스템에서의 패스워드 인증 관련 특허 특허를 보유하고 있고, 국외에서는 미국, 일본을 중심으로 다수의 특허 보유하고 있으며 패스워드 인증에 대한 다양한 기술분야의 특허가 다수 출원되어 있는 상태이므로, 기술 개발을 통한 응용 특허 또는 기존 특허에 대한 우회특허 또는 개량 특허의 도출을 통한 IPR 확보가 요구됨
	국내 표준화 인프라 수준 분석에 따른 세부 전략	- ITU-T 표준화 활동을 주도하고 있지만, 활발한 국내 표준전문가 활용이 필요함
	국제표준화 기여도 분석에 따른 세부 전략	- ITU-T의 표준화에 기여가 매우 높으므로, 국내 표준전문가의 활동을 장려하고 패스워드 인증 프로토콜 가이드라인, 제3의 신뢰기관을 이용한 안전한 프로토콜 등 신규 분야에 표준화를 지속적으로 추진함

3.3.4. 안전한 P2P 보안

• 표준상태전이도 (표준화 & 기술개발 연계분석)



표준화 중요도	국내 개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★★	TTA	ETRI	ITU-T, IETF

범 례

07 : 중점 표준화항목의 국내상태

07 : 중점 표준화항목의 국제상태

→ : 중점 표준화항목의 국내 표준상태전이

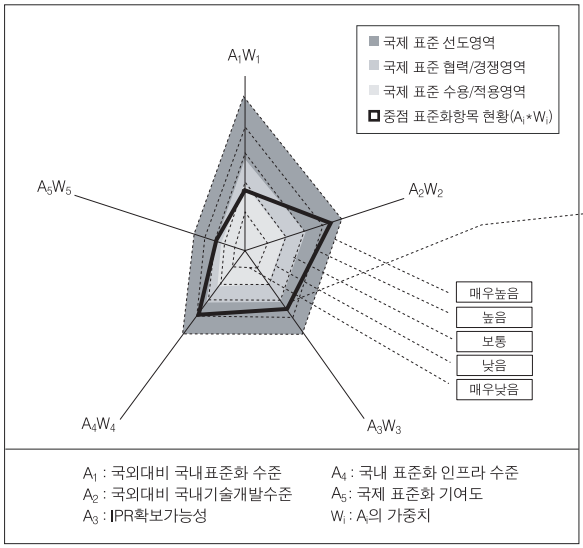
-→ : 중점 표준화항목의 국제 표준상태전이

↑ : 선행표준(선 표준화 후 기술개발)

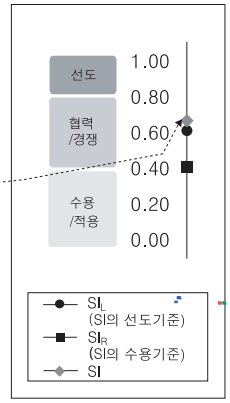
↗ : 동시표준(표준화&기술개발 동시추진)

↓ : 후행표준(선 기술개발 후 표준화)

• 국제표준화 전략목표 도출



SI (표준화 전략지수)	
SI_L (SI의 선도기준)	0.60
SI_R (SI의 수용기준)	0.40
SI	0.66



$$SI = (\sum_{i=1}^{5} A_i \cdot W_i) / 5$$
$$(0 < W_i < 1, 0 < SI \leq 1)$$

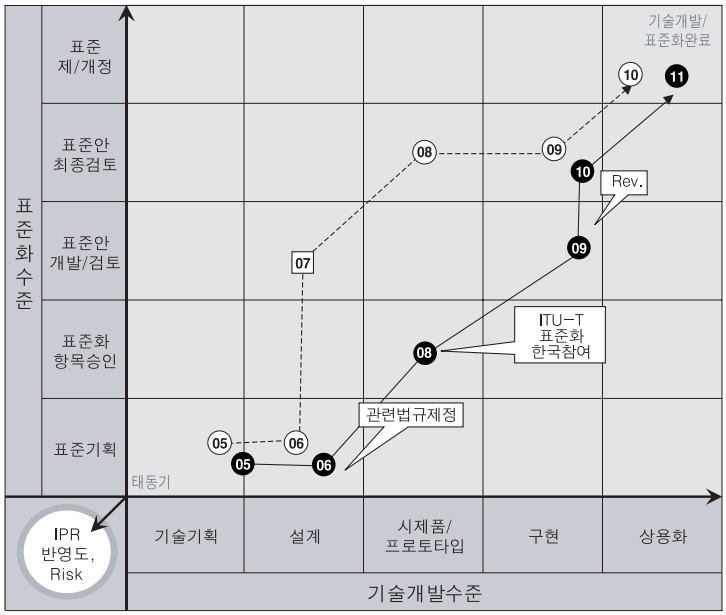
국제표준선도 (일부수용)

• 세부전략(안)

개 요		- IM (Instance Message)관련 표준화는 IETF에서 완료가 되었고, 보안 프레임워크 분야는 ITU-T SG17에서 범용 표준 개발이 진행중에 있으므로, 표준 완료를 위해 기존 표준화 분야에 집중하고, 신규 표준화 아이템을 발굴함 ◦P2P 보안 요구사항, P2P 보안 프레임워크, P2P 아이디 보안, P2P 기반 IPTV 보안 기술 등
항목별 전략	국내외 표준화 현황 분석에 따른 세부 전략	- IM (Instance Message)관련 표준화는 IETF에서 완료가 되었고, 보안 프레임워크 분야는 ITU-T SG17에서 보안 요구사항, 프레임워크를 중심으로 표준화 진행중에 있으므로, 표준 완료를 위해 기존 표준화 분야에 집중하고, P2P 아이디 보안 등 신규 표준화 아이템을 발굴함 - 아이디 보안 분야 등에서 신규 표준화가 필요하므로, ITU-T를 통한 표준화를 추진함 - P2P 기반 기술을 IPTV 등 신규 응용 분야에 적용하기 위한 요구사항 및 프레임워크 표준화가 필요함
	국내외 기술개발 현황 분석에 따른 세부 전략	- 국내의 P2P 보안 제품은 시제품 수준이며 패킷 탐지 분야에 일부 기술 개발이 있으며, 피어 검색, 자원 분산 등의 핵심 기술 분야에 기술개발은 전무한 상태이므로, 핵심 기술 개발과 함께 표준화 추진이 요구됨 - 국외기술은 폐쇄 환경에서 피어검색, 자원분산 등 핵심 기술 분야에 상용화 제품 출시되고 있으나 개방 환경에서의 보안 기술은 미흡한 상태이므로, 기술개발 추진과 표준전문가 활동을 통한 표준개발이 필요함
	국내 IPR 보유 현황분석 및 확보가능성 분석에 따른 세부 전략	- P2P 관련 국내특허는 현재까지 30여 건이 등록되었으며, 국내 P2P 응용 서비스 이용 규모에 비해서 특허 건수는 상대적으로 적은 편이므로, P2P 트래픽 분석 및 제어 기술, 개방 환경에서의 피어검색 보안, 자원 분산 보안 기술, P2P 아이디 보안 기술 등 분야에 기술개발로 IPR을 확보함 - P2P기반 IPTV 보안 기술 분야와 같이 신규 응용 서비스에 적용 가능한 P2P 보안 기술을 개발하여 IPR을 확보함
	국내 표준화 인프라 수준 분석에 따른 세부 전략	- ITU-T 표준화 활동을 주도하고 있지만, IETF 활동은 저조한 상태임. 활발한 국내 표준전문가 활용이 필요함
	국제표준화 기여도 분석에 따른 세부 전략	- ITU-T의 표준화에 기여가 매우 높으므로, 국내 표준전문가의 활동을 장려하고 아이디 보안 등 신규 분야에 표준화를 지속적으로 추진함 - 국내 BcN 등 표준화 분야에서 진행하고 있는 신규 응용 서비스 분야에 P2P 기술을 접목하는 방안 및 기술 개발이 시급히 요구됨. 특히 P2P 기반 기술을 IPTV에 적용하기 위한 요구사항 및 프레임워크 표준화가 필요함

3.3.5. IPTV 보안

• 표준상태전이도 (표준화 & 기술개발 연계분석)

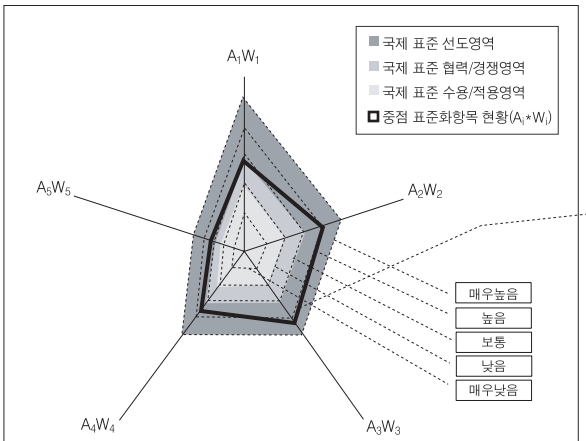


표준화 중요도	국내 개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★★	TTA	ETRI	ITU-T

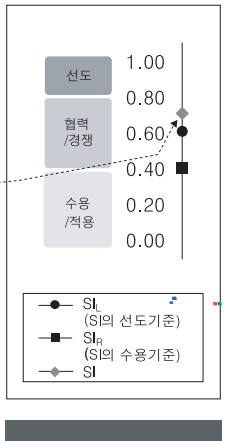
범 례

07 : 중점 표준화항목의 국내상태
07 : 중점 표준화항목의 국제상태
→ : 중점 표준화항목의 국내 표준상태전이
⇢ : 중점 표준화항목의 국제 표준상태전이
↑ : 선행표준(선 표준화 후 기술개발)
↗ : 동시표준(표준화&기술개발 동시추진)
↓ : 후행표준(선 기술개발 후 표준화)

• 국제표준화 전략목표 도출



SI (표준화 전략지수)	
SI_L (SI의 선도기준)	0.60
SI_R (SI의 수용기준)	0.40
SI	0.72



$$SI = (\sum_{i=1}^{5} A_i \cdot W_i) / 5$$
$$(0 < W_i < 1, 0 < SI \leq 1)$$

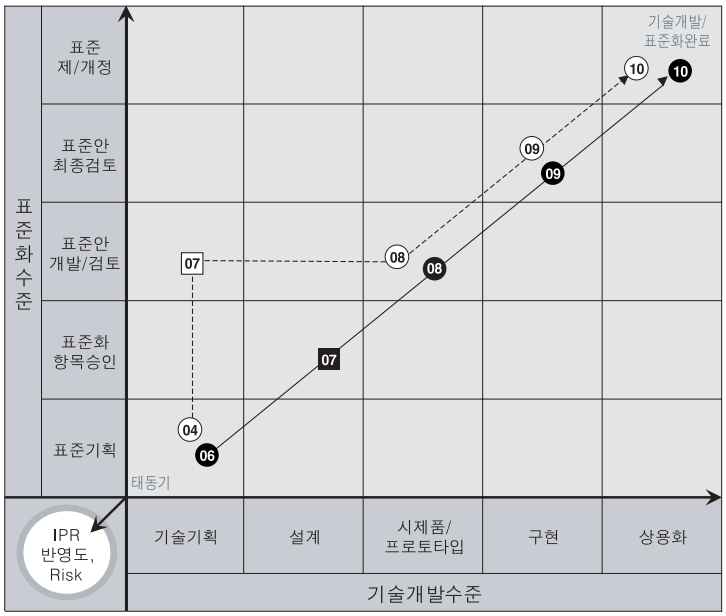
국제표준선도
협력/경쟁

• 세부전략(안)

개 요		- ITU-T FG-IPTV 에서 표준 활동이 완성하게 전개됨 - 전통적 보안 기술을 IPTV 보안 표준으로 적용 및 보완 활동 필요함 - ITU-T SG17을 통한 표준 활동이 요구됨 ◦코드 상호연동 보안 메커니즘 ◦프라이버시 보장 메커니즘
항목별 전략	국내외 표준화 현황 분석에 따른 세부 전략	- 한국은 ITU-T IPTV FG에서 서비스, 망 구조 등 분야를 주도하고 있어 IPTV 보안 분야의 표준화가 필요함.현재까지는 IPTV 보안 요구사항만 도출된 상태임 - IPTV를 위한 암호화, 프라이버시 등 신규 보안 기술 분야의 표준화가 미흡하기 때문에 기술개발과 함께 ITU-T에서 표준화를 추진함 - ITU-T IPTV FG에서 오버레이 또는 P2P 방식의 멀티캐스트를 IPTV에 적용하기 위한 기술 표준화가 진행되고 있으므로, 보안 요구사항 및 보안 메커니즘 표준화에 참여하 필요함
	국내외 기술개발 현황 분석에 따른 세부 전략	- IPTV 응용, 서비스 기술은 뛰어나나 보안 기술 분야에서는 뒤쳐져 있는 상태로, DRM/CAS의 핵심 요소 기술은 외산을 채용하고 있는 실정임. 최근 DRM+CAS 통합과 Downloadable CAS와 같은 분야에서 강세를 보이고 있으므로, 기술개발과 함께 ITU-T에서 표준화를 추진함 - IPTV를 위한 암호화, 프라이버시 등 신규 보안 기술 분야의 기초연구가 전무한 상태이므로, 기술개발과 표준화를 동시에 진행함 - 오버레이 또는 P2P 방식의 멀티캐스트를 IPTV에 적용하기 위한 보안기술 개발이 필요함
	국내 IPR 보유 현황 분석 및 확보가능성 분석에 따른 세부 전략	- 국내에서는 IPTV 서비스 및 응용 기술 특허를 다수 보유하고 있으며, 전송망, 인증, 과금, 식별 등 IPTV 보안 특허는 매우 적고, DRM/CAS 특허 중 일부를 보유하고 있음. 국외에서는 IPTV 서비스 및 응용 기술 관련 특허를 다수 보유하고 있으며, 전송망, 인증, 과금, 식별 등 IPTV 보안 특허는 매우 상태임. 따라서, 전송망, 인증, 과금, 식별 등 IPTV 보안 관련 분야의 IPR 확보에 주력함 - 투명성, transcodability, 공간/주파수 도메인 암호화, 선택적 암호화 등 신규 보안 기술 분야 IPR 확보에 주력함 - IPTV 전용 프라이버시 관련 기술 개발이 미흡하므로, 프라이버시 보호 분야에 IPR 확보에 주력함
	국내 표준화 인프라 수준 분석에 따른 세부 전략	- 국내 BcN 등 관련 단체가 ITU-T에서 활발히 응용 분야 표준화에 참여하고 있으나 IPTV 보안 분야의 활동은 저조한 상태임. 활발한 국내 표준전문가 활용이 필요함
	국제표준화 기여도 분석에 따른 세부 전략	- ITU-T의 표준화에 기여가 매우 높으므로, 국내 표준전문가의 활동을 장려하고 코드 상호연동 보안 메커니즘, 프라이버시 보장 메커니즘 등 신규 분야에 표준화를 지속적으로 추진함

3.3.6. 신뢰 보안 서비스(STC)

• 표준상태전이도 (표준화 & 기술개발 연계분석)

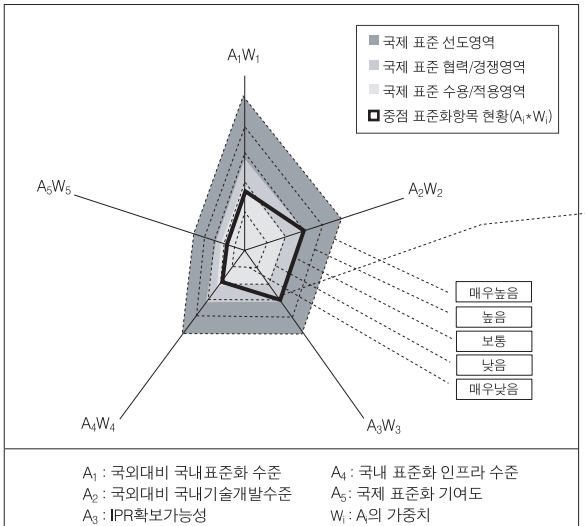


표준화 중요도	국내 개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★★	유비쿼터스 시큐리티 포럼	ETRI	TCG IETF 3GPP

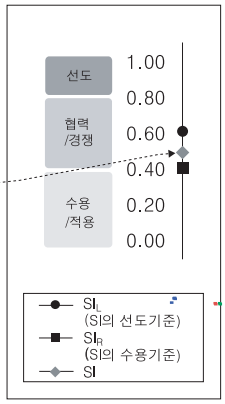
범 례

07 : 중점 표준화항목의 국내상태
07 : 중점 표준화항목의 국제상태
→ : 중점 표준화항목의 국내 표준상태전이
⇢ : 중점 표준화항목의 국제 표준상태전이
↑ : 선행표준(선 표준화 후 기술개발)
↗ : 동시표준(표준화&기술개발 동시추진)
↓ : 후행표준(선 기술개발 후 표준화)

• 국제표준화 전략목표 도출



SI (표준화 전략지수)	
SI_L (SI의 선도기준)	0.60
SI_R (SI의 수용기준)	0.40
SI	0.48



$$SI = (\sum_{i=1}^{5} A_i \cdot W_i) / 5$$
$$(0 < W_i < 1, 0 < SI \leq 1)$$

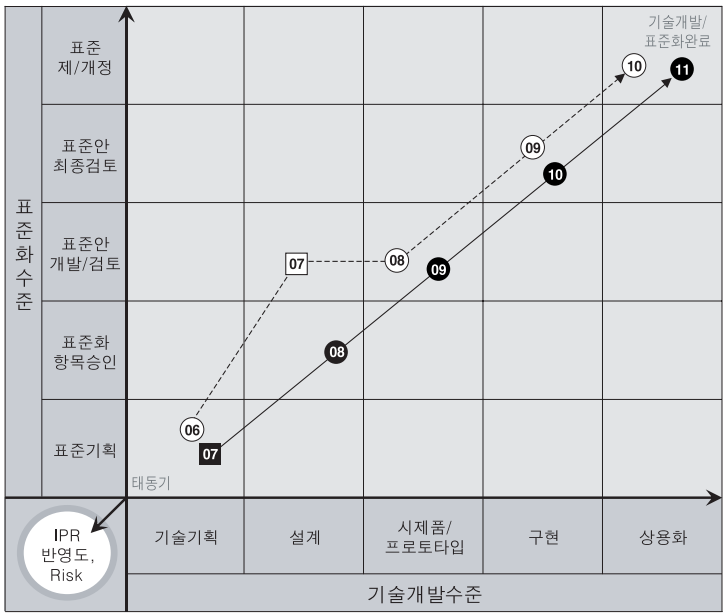
국제표준선도 협력/경쟁

• 세부전략(안)

개 요		- TCG 에서 TPM (Trusted Platform Module) 표준화 요구됨
항목별 전략	국내외 표준화 현황 분석에 따른 세부 전략	- 국내에서는 현재까지의 활동은 없었고, 무선인터넷포럼과 TTA를 통하여 2007년부터 연구를 시작할 예정이므로, 이미 표준화를 진행하고 있는 TCG의 활동 분야 중 TPM 등 분야의 표준화를 주도하여 국제표준화를 선도함
	국내외 기술개발 현황 분석에 따른 세부 전략	- 국내에서 모바일용 TPM을 개발하고 있고, 타 업체는 아직 검토 단계으므로, 기술개발 시기에 맞추어 표준화를 진행할 필요가 있음 - 노트북이나 데스크탑에는 이미 TPM 장착된 상용 제품들이 출시되고 있으나, TPM을 장착한 모바일 단말 제품은 아직 출시되지 않고 있음. TCG의 표준화 진행과 업체들의 관련 기술 개발이 동시에 이루어지고 있으므로, 기술개발과 함께 표준화를 추진함
	국내 IPR 보유 현황 분석 및 확보가능성 분석에 따른 세부 전략	- TCG에 다수의 표준문서 존재(TPM, TSS, MTM 등) 하고 있음. 국내에서는 이미 국내/국제 특허와 논문을 확보하고 있으며, 모바일 TPM 개발에 사용된 다수의 기술들의 IPR 확보에 주력함
	국내 표준화 인프라 수준 분석에 따른 세부 전략	- 국내에서는 이미 기술개발 경험이 풍부한 전문 인력을 확보하고 있으므로, 이를 적극 활용하여 TCG에서 표준화에 참여함
	국제표준화 기여도 분석에 따른 세부 전략	- 관련 표준화는 TCG에서 표준화를 활발히 진행 중이고, 3GPP, OMA, ITU-T와도 liaison을 통한 표준화 추진 예정에 있으나, 국내 표준 전문가의 기여는 매우 저조함. TTA를 통한 국내 표준화 활성화와 함께 ETRI, 삼성, 스프레드텔레콤, 프롬투 등 국내 산,학,연 공동의 표준화 참여가 요구됨

3.3.7. 차세대 웹 보안

• 표준상태전이도 (표준화 & 기술개발 연계분석)

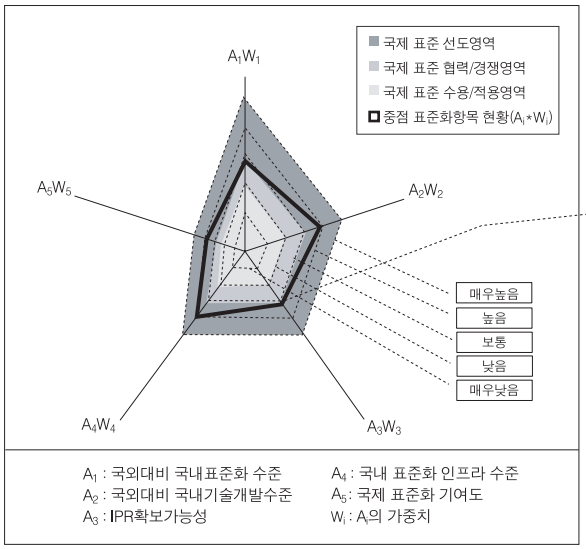


표준화 중요도	국내 개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★★★	TTA	ETRI	ITU-T, W3C OASIS

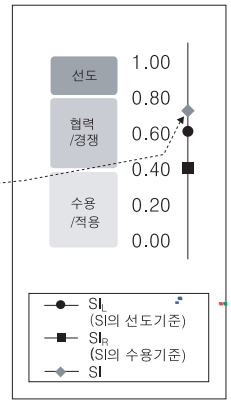
범 례

07 : 중점 표준화항목의 국내상태
07 : 중점 표준화항목의 국제상태
→ : 중점 표준화항목의 국내 표준상태전이
-→ : 중점 표준화항목의 국제 표준상태전이
↑ : 선행표준(선 표준화 후 기술개발)
↗ : 동시표준(표준화&기술개발 동시추진)
↓ : 후행표준(선 기술개발 후 표준화)

• 국제표준화 전략목표 도출



SI (표준화 전략지수)	
SI_L (SI의 선도기준)	0.60
SI_R (SI의 수용기준)	0.40
SI	0.70



$$SI = (\sum_{i=1}^{5} A_i \cdot W_i) / 5$$
$$(0 < W_i < 1, 0 < SI \leq 1)$$

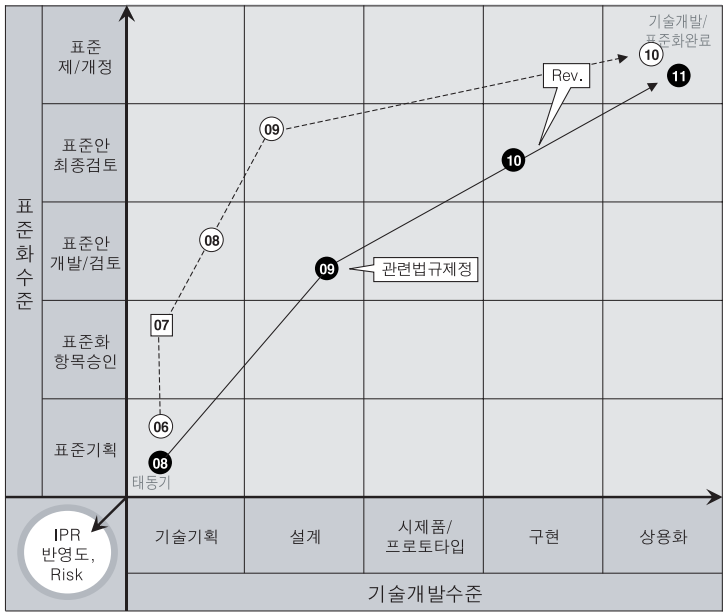
국제표준선도 (일부수용/적용)

• 세부전략(안)

개 요		- ITU-T SG17 및 W3C를 통하여 국제 표준화의 선도가 요구됨 ◦웹 2.0 보안, 시맨틱 웹서비스 보안, 유비쿼터스 웹 보안, 웹 환경에서 프라이버시, 융복합 서비스를 위한 웹서비스 보안 프로파일 등
항목별 전략	국내외 표준화 현황 분석에 따른 세부 전략	- ITU-T, W3C, OASIS 위주의 표준화 활동이 지속될 것으로 전망됨에 따라, 국내 표준전문가의 적극적인 표준화 활동이 요구되며, 웹 2.0 정보보호 분야, 시맨틱 웹, 유비쿼터스 웹 보안 분야 등 신규 분야의 표준화가 필요함
	국내외 기술개발 현황 분석에 따른 세부 전략	- 유선 웹서비스 보안 기술 및 웹 방화벽 기술은 비교적 높은 편이나, 모바일 웹서비스 보안 기술, 시맨틱 웹 보안 기술은 국내외 적으로 기술 초기 단계이므로, 이러한 분야의 기술개발 및 표준화를 추진함
	국내 IPR 보유 현황분석 및 확보가능성 분석에 따른 세부 전략	- 국내외적으로 유선 환경에서의 웹서비스 보안은 상당수의 특허가 출원되어 있으므로, 향후 웹 2.0 보안, 시맨틱 웹 서비스 보안, 유비쿼터스 웹 보안 등의 분야에 기술개발로 IPR 확보에 주력함
	국내 표준화 인프라 수준 분석에 따른 세부 전략	- 국내 기술 개발 및 표준화는 ETRI, KISA, TTA, 유비쿼터스 웹 포럼 등에서 활동하고 있으며, 산,학,연 전문가의 적극적인 참여가 요구됨
	국제표준화 기여도 분석에 따른 세부 전략	- 세계적으로 웹 2.0 보안, 시맨틱 웹 및 시맨틱 웹서비스 보안, 유비쿼터스 웹 보안 등에 관한 표준화는 초기 단계에 있기 때문에 ITU-T, W3C, OASIS, OMA 등에서의 표준화 활동을 보다 강화해야 함.

3.3.8. Lawful Interception

• 표준상태전이도 (표준화 & 기술개발 연계분석)



표준화 중요도	국내 개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★★	TTA	ETRI	ITU-T

범 례

07 : 중점 표준화항목의 국내상태

07 : 중점 표준화항목의 국제상태

→ : 중점 표준화항목의 국내 표준상태전이

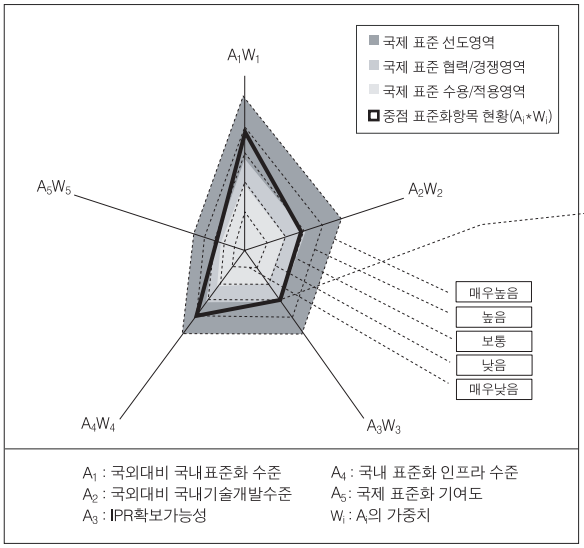
--→ : 중점 표준화항목의 국제 표준상태전이

↑ : 선행표준(선 표준화 후 기술개발)

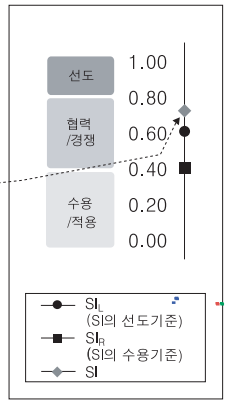
↗ : 동시표준(표준화&기술개발 동시추진)

↓ : 후행표준(선 기술개발 후 표준화)

• 국제표준화 전략목표 도출



SI (표준화 전략지수)	
SI_L (SI의 선도기준)	0.60
SI_R (SI의 수용기준)	0.40
SI	0.70



$$SI = (\sum_{i=1}^{5} A_i \cdot W_i) / 5$$
$$(0 < W_i < 1, 0 < SI \leq 1)$$

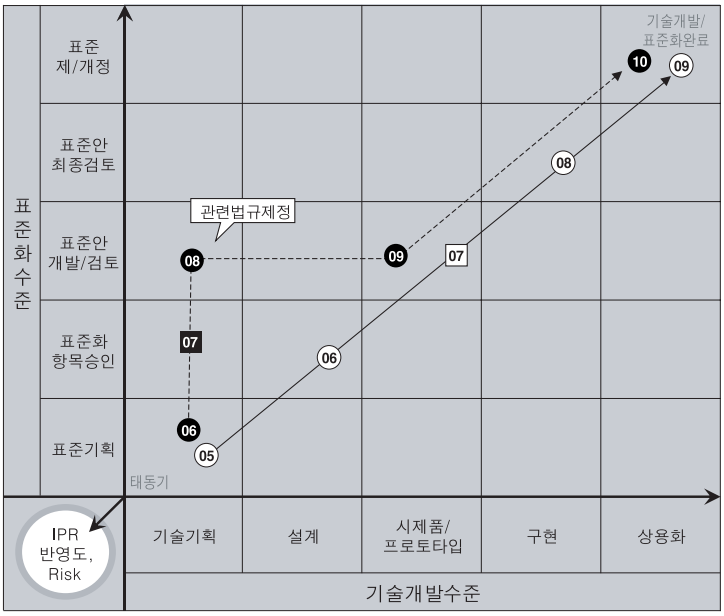
국제표준 수용/적용 (일부선도)

• 세부전략(안)

개 요		- 암호화된 정보에 대한 분석 분야에 있어서 ITU-T SG17을 통한 국제간(아시아 권역) 표준 개발이 요구됨
항목별 전략	국내외 표준화 현황 분석에 따른 세부 전략	- 기존의 감청 분야에서는 통신망 운용 형태에 따른 감청이 주를 이루었으나, 암호화된 데이터가 네트워크를 통해 전송되는 부분에 대해서는 기술 개발 및 표준화가 전무한 상태임. 기술 개발과 함께 국제 표준화 단체 (ITU-T)를 통한 표준 제안을 활발히 추진함
	국내외 기술개발 현황 분석에 따른 세부 전략	- 라우터 장비 등에서 감청은 이미 성숙기에 있지만, 암호화된 데이터에 대한 분석은 아직 초기단계에 머무르고 있으므로, 이 분야에서의 표준화 활동에 집중해야 함
	국내 IPR 보유 현황분석 및 확보가능성 분석에 따른 세부 전략	- ETSI에 관련 표준문서 다수 존재하고 유선망에서의 감청 분야 기술은 포화된 상태이므로, BcN 기반의 신규 서비스망에서 암호화된 데이터에 대한 합법적인 분석 방법 및 구조 분야에서 IPR 확보에 주력함
	국내 표준화 인프라 수준 분석에 따른 세부 전략	- 인터넷 인프라의 확대와 더불어 국내외적으로 암호화된 정보에 대한 합법적인 분석 기술에 대한 요구가 높으며, 시기 적절한 표준의 제정이 뒤따르지 않으면 상용화 시기의 선점을 위해 해외 선도 업체의 기술을 그대로 도입할 가능성이 높음 - 수 년 전까지 국제표준화의 중요성이 상대적으로 작았던 것이 사실이나 최근 (아시아 권역에서) 국제표준화의 중요성 부각과 함께 국가간 연동이 가능한 표준 개발이 요구되고 있어, 관련 분야의 시장성이 매우 큰 만큼 국내표준화 인프라의 양적인 확장뿐만 아니라 질적인 성장이 필요한 시점으로 판단됨. 따라서 국내표준의 선행활동을 활발히 전개 하고 이를 국제표준으로 연계하는 형태로 체제의 전환이 필요함
	국제표준화 기여도 분석에 따른 세부 전략	- 이 분야에서의 국제 표준화는 유선망에서의 감청 분야에 중점을 두고 있어 암호화된 정보에 대한 분석 분야의 기술 개발 및 표준화는 상대적으로 활동이 적은 편임. 이와 더불어 국내 연구 개발 활동도 매우 저조하여 국제 표준화기여도는 매우 낮게 평가되고 있음. 따라서 기술적인 유사성을 근거로 하여 기존 국제 표준을 일부 수용하되, 암호화된 정보 분석을 위한 국제 표준을 선도할 필요가 있음

3.3.9. 정보보호 평가

• 표준상태전이도 (표준화 & 기술개발 연계분석)

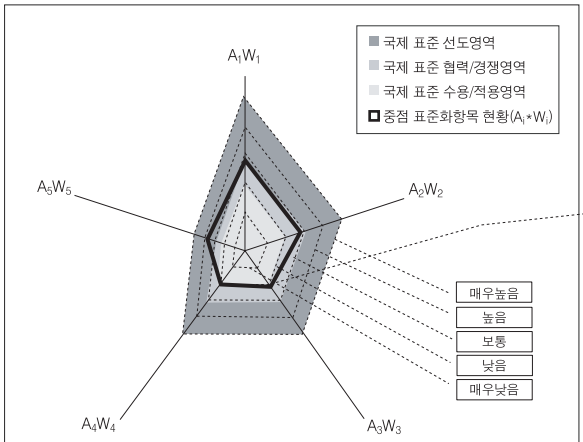


표준화 중요도	국내 개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★★	TTA	ETRI	ITU-T

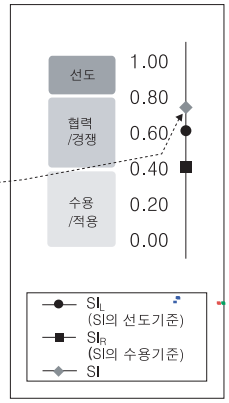
범 례

07 : 중점 표준화항목의 국내상태
07 : 중점 표준화항목의 국제상태
→ : 중점 표준화항목의 국내 표준상태전이
--→ : 중점 표준화항목의 국제 표준상태전이
↑ : 선행표준(선 표준화 후 기술개발)
↗ : 동시표준(표준화&기술개발 동시추진)
↓ : 후행표준(선 기술개발 후 표준화)

• 국제표준화 전략목표 도출



SI (표준화 전략지수)	
SI_L (SI의 선도기준)	0.60
SI_R (SI의 수용기준)	0.40
SI	0.54



$$SI = (\sum_{i=1}^{5} A_i \cdot W_i) / 5$$
$$(0 < W_i < 1, 0 < SI \leq 1)$$

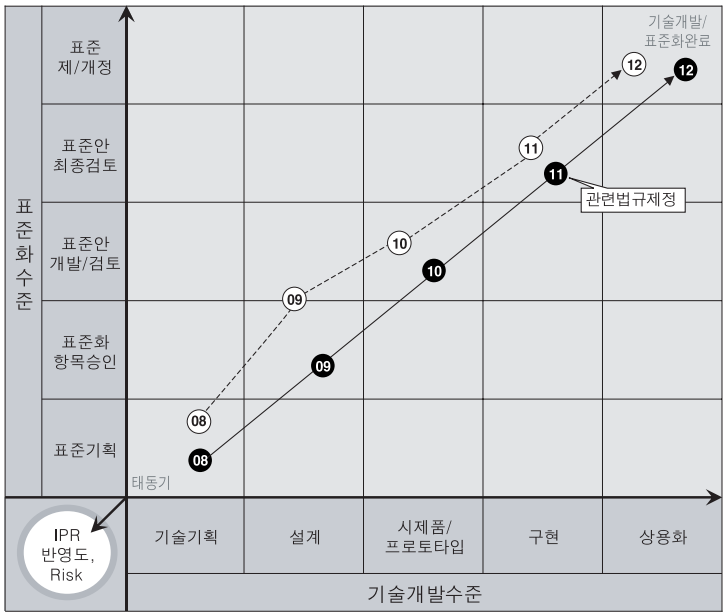
국제표준 수용/적용

• 세부전략(안)

개 요		- 현재 ISO에서 국제 표준화가 진행되고 있으며, 이에 대한 국제 표준의 주시가 필요하며, 개발된 표준의 국내 수용이 필요함
항목별 전략	국내외 표준화 현황 분석에 따른 세부 전략	- 기존 표준의 완성도를 향상하기 위한 표준들이 개발될 예정에 있고, ISO/IEC JTC1에서 개발된 정보보호 평가에 대한 표준은 모든 분야에 적용될 수 있는 범용 표준으로, 향후 특정 분야에 적용될 수 있는 정보보호 평가에 대한 표준이 ITU-T, ISO/IEC JTC1에서 추진될 예정에 있음. 따라서 표준 기술의 차별성을 부여할 수 있는 관련 기술 분야의 IPR을 확보하기 위한 좋은 시기임. 따라서 범용 표준화 부분에서 국제 표준을 수용/적용하되 일부 분야에서 국내의 관련 기술을 국제표준으로 상정하고, 표준화 결과에 따라 국내표준을 빠르게 제정하여 국내의 앞선 인프라를 기반으로 상용화까지 추진, 시장을 선점을 도모할 필요가 있음
	국내외 기술개발 현황 분석에 따른 세부 전략	- 기존에 완성되어 있는 위험분석 표준을 새로운 IT 환경에 적합하도록 개보수 작업이 필요하며 정보보호 아키텍처, 성과측정 등 새로운 지침 및 표준개발이 요구됨에 따라서 기술 업그레이드 및 표준 제/개정이 필요한 시기임 - 정보보호 관리기술은 정보보호 관련 전문 공공기관 및 민간 기업에서 여러 지침 및 기준 등을 개발하고 있으며 특히 정보보호컨설팅 업체를 중심으로 위험분석 도구개발을 중심으로 기술개발이 이루어지고 있으므로, 국내 및 국제 표준기술 확보에 매우 유리함 - 본격적인 평가 서비스가 시작되기 위해서는 관련 표준과 법률 제정이 뒷받침 되어야 하므로 평가 기술 표준의 제정과 밀접한 연관을 갖고 진행하는 것이 좋으며, 국내기술의 국제표준화 뿐만 아니라 표준제정 직후 상용화 시기의 선점을 위한 집중적인 기술개발이 함께 진행되어야 함
	국내 IPR 보유 현황 분석 및 확보가능성 분석에 따른 세부 전략	- 표준 기술의 제/개정에 따른 차별성을 부여할 수 있는 관련 기술 분야의 IPR을 확보하기 위한 좋은 시기로, 통신 분야 및 무선 통신 분야의 정보보호 평가 체계의 개발 및 평가 도구 개발 등 분야에서 IPR 확보가 가능할 것임
	국내 표준화 인프라 수준 분석에 따른 세부 전략	- 기존 국내외 표준 제정 인프라는 충분히 확충되어 있으므로, 통신 분야 및 무선 통신 분야에 적용될 수 있는 정보보호 평가 기술 표준과 제도 정비에 전문 인력을 충분히 활용할 수 있을 것임. 그러나 평가 서비스 운용을 위해 관련 기술 표준에 대한 요구가 매우 높으며, 시기적절한 표준의 제정이 뒤따르지 않으면 해외 선도 업체의 기술을 그대로 도입할 가능성이 높음
	국제표준화 기여도 분석에 따른 세부 전략	- 새로운 IT 환경을 위한 표준과 제도의 개보수 작업이 진행 중에 있으므로, 적극적으로 표준화에 참여하여 국내기술을 표준에 반영하도록 하는 전략이 필요함

3.3.10. 보안관리

• 표준상태전이도 (표준화 & 기술개발 연계분석)

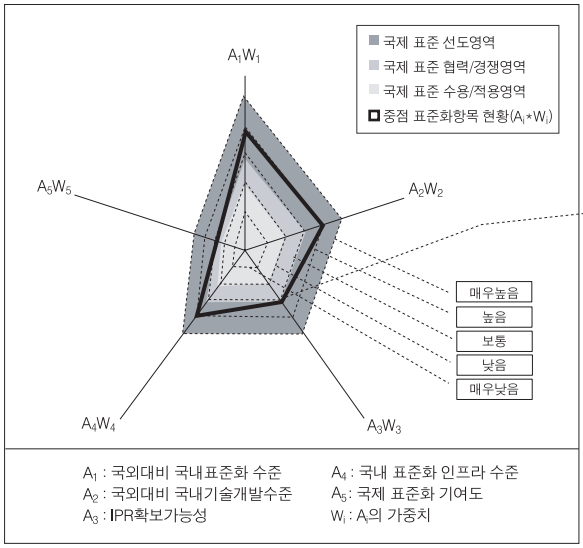


표준화 중요도	국내 개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★★	KISA	KISA	ISO, ITU-T

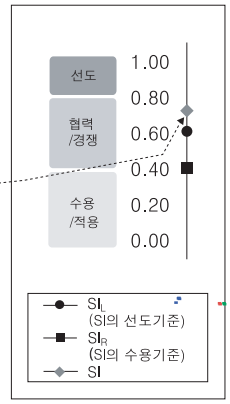
범 례

07 : 중점 표준화항목의 국내상태
07 : 중점 표준화항목의 국제상태
→ : 중점 표준화항목의 국내 표준상태전이
-→ : 중점 표준화항목의 국제 표준상태전이
↑ : 선행표준(선 표준화 후 기술개발)
↗ : 동시표준(표준화&기술개발 동시추진)
↓ : 후행표준(선 기술개발 후 표준화)

• 국제표준화 전략목표 도출



SI (표준화 전략지수)	
SI_L (SI의 선도기준)	0.60
SI_R (SI의 수용기준)	0.40
SI	0.74



$$SI = (\sum_{i=1}^{5} A_i \cdot W_i) / 5$$
$$(0 < W_i < 1, 0 < SI \leq 1)$$

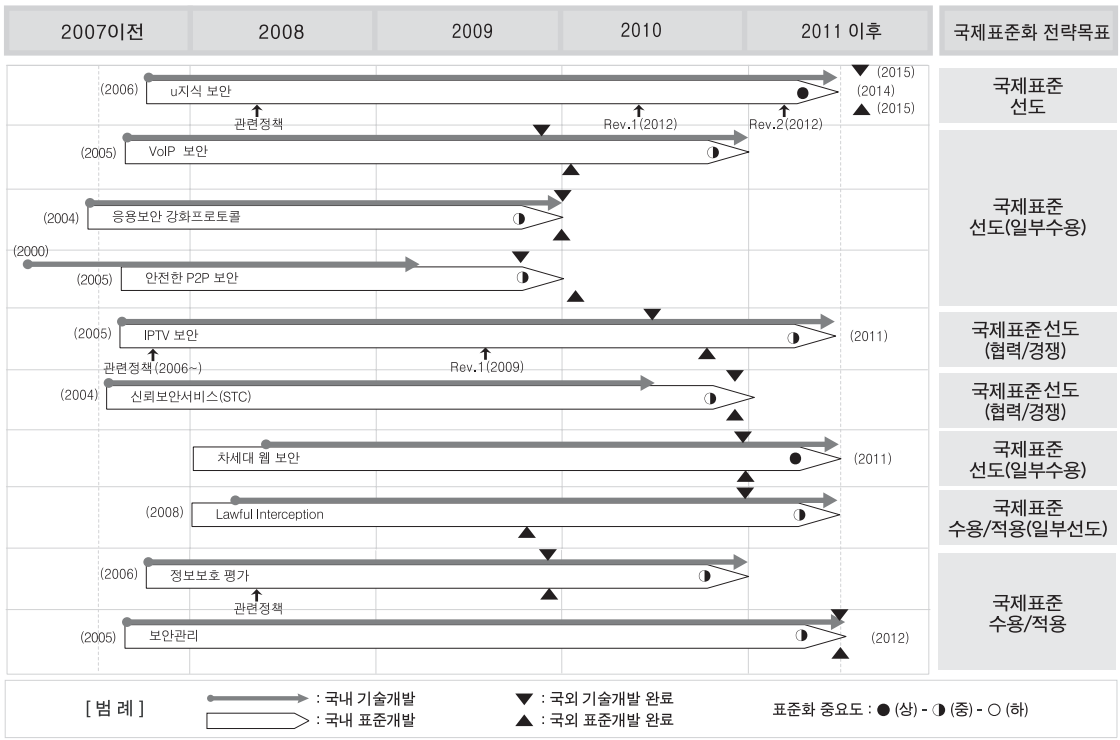
국제표준 수용/적용

• 세부전략(안)

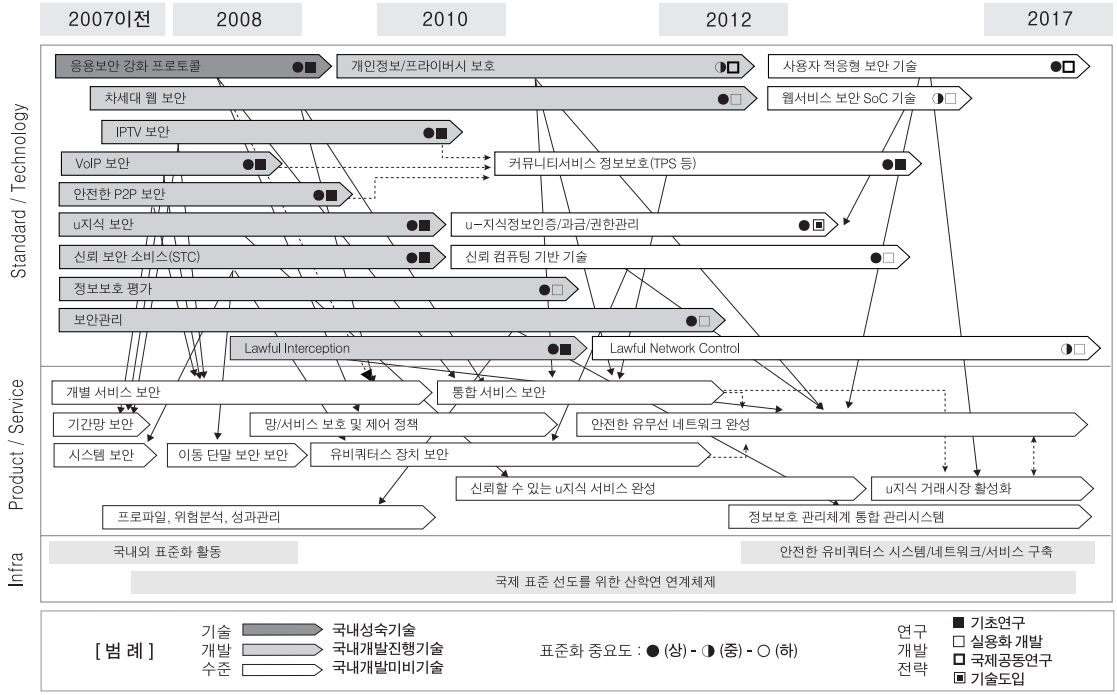
개 요		- ISO/IEC, ITU-T 를 통한 세부항목 표준 활동이 요구됨 ◦거버넌스, 유비쿼터스 환경 분야
항목별 전략	국내외 표준화 현황 분석에 따른 세부 전략	- 최근 IT 환경의 급속한 환경 변화 개인정보보호 등 신규 이슈 등 기존 정보보호 패러다임이 정보보호관리 관점에서 정보보호 거버넌스로 변화되고 있는 추세이므로 이에 따른 체계적인 정보보호 거버넌스 연구 및 표준 제정이 필요함 - 현재 국내에서 보유하고 있는 기술을 기반으로 보안관리 업체들과 협력체계를 구축하고 기술의 시장 적용을 통한 상용화 추진과 표준화에 대한 요구사항을 도출하도록 함 - ISO/IEC와 ITU-T의 보안관리 분야 국제 표준 개발에 집중할 필요가 있음
	국내외 기술개발 현황 분석에 따른 세부 전략	- 유비쿼터스 환경 진입에 따라 보안관리 분야의 새로운 패러다임이 요구되고 있음. 즉 광범위해지는 정보자산 위협요인과 사이버 공격의 파급효과 증대 등으로 인하여 보안관리 프로세스의 자동화, 실시간 보안관리 체계 수립 등 신규 분야의 기술 개발이 요구됨. 이를 위한 국내 기술개발을 추진함에 있어 국내표준을 조기에 확정하고 국제표준으로 반영함과 동시에 국제표준에 준하는 기술개발이 이루어질 수 있도록 하는 추진 전략이 요구됨
	국내 IPR 보유 현황 분석 및 확보가능성 분석에 따른 세부 전략	- 본 항목에서 IPR 보유 및 확보가 차지하는 비중이 낮은 편인데, 실질적인 기술개발 및 적용의 경험을 토대로 IPR을 확보하고 이를 국제표준에 반영함으로 써 국제 경쟁력을 갖출 수 있음. 이를 위해서는 관련 국제표준제정에 주도적인 역할을 수행할 수 있어야 하며 따라서 Editorship 및 Rapparteur와 같은 의장단을 확보하여 전략적으로 국내 관련기술의 IPR을 반영할 수 있도록 산,학,연,관의 긴밀한 협력 및 체계적인 접근이 필요함
	국내 표준화 인프라 수준 분석에 따른 세부 전략	- 상대적으로 국내표준화 인프라 수준이 높은 편으로 평가되나 일부 주요 기술의 표준화를 제외하고 국제표준화 활동 대비 국내 단체 표준제정을 위한 활동이 미미한 상황임. 최근 국제표준화의 중요성 부각과 함께 국내표준화 인프라의 양적인 확장뿐만 아니라 질적인 성장이 필요한 시점으로 판단됨. 따라서 국내표준의 선행 활동과 이를 국제표준으로 연계하는 전략이 필요함
	국제표준화 기여도 분석에 따른 세부 전략	- 국제표준화기여도 분석에 따른 전략으로 보안관리 관련 국제표준회의에서 우리나라의 활동이 저조한 현황임. 최근 IT 환경의 급속한 환경 변화 개인정보보호 등 신규 이슈 등 기존 정보보호 패러다임이 정보보호관리 관점에서 정보보호 거버넌스로 변화되고 있는 추세이므로 이러한 기회를 통해 국내 기술이 국제표준에 반영되도록 하기 위한 국제표준전문가의 활동이 필요함

3.4. 중장기 표준화로드맵

3.4.1. 중기('08 ~ '10) 표준화로드맵(3개년)



3.4.2. 장기 표준화로드맵(10년 기술예측)



[국내외 관련표준 대응리스트]

구분	표준화항목	표준명	기구 (업체)	제정연도	재개정 현황	국내 관련표준	국내 추진기구
응용보안	스팸 대책	Guidelines on Countering E-mail SPAM	ITU-T		진행		
		Overview of Countering SPAM for IP Multimedia Applications	ITU-T		진행		
		Technical Means for Countering SPAM	ITU-T		진행		
		Technical Framework for Countering E-mail SPAM	ITU-T		진행		
		Requirement for Countering SPAM	ITU-T		진행		
	응용보안 강화 프로토콜	Lightweight Directory Access Protocol (v3): Extension for Transport Layer Security (RFC 2830)	IETF	2000	제정	TTAS.IF-RFC2830	TTA
		Password-authenticated key exchange (PAK) protocol	ITU-T	2007	제정		
		Guideline on secure password-based authentication protocol with key exchange (updated 1st draft recommendation)	ITU-T	2007	제정		
		The PAK suite: Protocols for Password-Authentication Key Exchange	IEEE	2002	제정		
		Password-Authenticated Diffie-Hellman Exchange (PAK)	IETF	2007	제정		
		A One-Time Password System	IETF	1997	제정		
		OTP Extended Responses	IETF	1998	제정		
		The One-Time-Password SASL Mechanism	IETF	1998	제정		
	안전한 P2P 보안	Security requirements for P2P communications	ITU-T		진행		
		Security architecture and operations for peer-to-peer network	ITU-T		진행		
		Extensible Messaging and Presence Protocol(XMPP): Core	IETF	2004	제정		
		Extensible Messaging and Presence Protocol(XMPP): Instant Messaging and Presence	IETF	2004	제정		
		Mapping the Extensible Messaging and Presence Protocol(XMPP) to Common Presence and Instant Messaging(CPIM)	IETF	2004	제정		
		End-to-End Signing and Object Encryption for the Extensible Messaging and Presence Protocol(XMPP)	IETF	2004	제정		
		A Presence Event Package for the Session Initiation Protocol (SIP)	IETF		제정		
		A Watcher Information Event Template-Package for the Session Initiation Protocol (SIP)	IETF		제정		
		An Extensible Markup Language (XML) Based Format for Watcher Information	IETF		제정		
		Indication of Message Composition for Instant Messaging	IETF		제정		
		Timed Presence Extensions to the Presence Information Data Format (PIDF) to Indicate Status Information for Past and Future Time Intervals	IETF		제정		
	안전한 P2P 보안	RPID: Rich Presence Extensions to the Presence Information Data Format (PIDF)	IETF		제정		
		CIPID: Contact Information in Presence Information Data Format	IETF		제정		
		A Data Model for Presence	IETF		제정		
		A Session Initiation Protocol (SIP) Event Notification Extension for Resource Lists	IETF		제정		
		An Extensible Markup Language (XML) Based Format for Event Notification Filtering	IETF		제정		
		Functional Description of Event Notification Filtering	IETF		제정		
		An Extensible Markup Language (XML) Configuration Access Protocol (XCAP) Usage for Manipulating Presence Document Contents	IETF		제정		
		Extensible Markup Language (XML) Formats for Representing Resource Lists	IETF		제정		
		The Extensible Markup Language (XML) Configuration Access Protocol (XCAP)	IETF		제정		

구분	표준화항목	표준명	기구 (업체)	제정 연도	재개정 현황	국내 관련표준	국내 추진기구
응용보안	IPTV 보안	IPTV security aspects	ITU-T	2007	진행		
	STC	TPM Design Principles	TCG				
		Structures of the TPM	TCG				
		TPM Commands	TCG				
		TCG Software Stack Specification	TCG				
		TCG TNC Architecture for Interoperability	TCG				
		TCG TNC IF-IMC Specification	TCG				
		TCG TNC IF-IMV Specification	TCG				
		TCG Mobile Reference Architecture	TCG	2007			
		Mobile Trusted Module Specification	TCG	2007			
		TCG Credential Profiles Specification	TCG				
		Security Qualities Schema Specification	TCG				
		Verification Result Schema Specification	TCG				
		TCG Storage Architecture Core Specification	TCG	2006			
		TCG EFI Protocol Specification	TCG				
		TCG EFI Platform Specification	TCG				
	차세대 웹 정보보호	확장성 생성 언어 전자서명 구문과 처리	TTA	2004	제정		
		정규 XML 버전 1.0	TTA	2004	제정		
		배제 정규 XML 버전 1.0	TTA	2004	제정		
		웹서비스 메시지 보안 제품에 대한 평가 가이드라인	TTA	2006	제정		
		웹서비스 보안: SAML 토큰 프로파일 1.1	TTA	2006	제정		
		웹서비스 보안: 첨부를 갖는 SOAP 메시지 프로파일 1.1	TTA	2006	제정		
		XML Signature/Encryption 적합성 및 상호운용성 평가	TTA	2004	제정		
		XACML 적합성 및 상호운용성 평가	TTA	2004	제정		
		XKMS 적합성 및 상호운용성 평가	TTA	2004	제정		
		확장성 생성언어 암호 구문과 처리	TTA	2005	제정		
		SAML 구문과 프로토콜	TTA	2005	제정		
		확장성 생성언어 전자서명을 위한 복호화 변환	TTA	2005	제정		
		SAML 바인딩과 프로파일	TTA	2005	제정		
		확장성 생성언어 암호 요구사항	TTA	2005	제정		
		확장성 접근제어 생성언어	TTA	2005	제정		
		웹 서비스 보안 : SOAP 메시지 보안 1.1	TTA	2006	제정		
		웹 서비스 보안 X.509 인증 토큰 프로파일 1.1	TTA	2005	제정		
		웹 서비스 보안 유저네임토큰 프로파일 1.1	TTA	2005	제정		
		Security Assertion Markup Language 2.0 (SAML 2.0)	ITU-T	2006	제정		
		eXtensible Access Control Markup Language 2.0 (XACML 2.0)	ITU-T	2006	제정		
		Security Architecture for message security in mobile Web Services	ITU-T	2007	Final Draft		
		Web Services Security: SOAP Message Security 1.1	OASIS	2006	제정		
		WS-SecurityPolicy v1.2	OASIS	2007	제정		
		Web Services Federation Language (WS-Federation) 1.2	OASIS	2007	진행		
		WS-SecureConversation 1.3	OASIS	2007	제정		

구분	표준화항목	표준명	기구 (업체)	제정 연도	재개정 현황	국내 관련표준	국내 추진기구
응용보안	차세대 웹 정보보호	WS-Trust 1.3	OASIS	2007	제정		
		XACML 2.0 Core: eXtensible Access Control Markup Language (XACML) Version 2.0	OASIS	2005	제정		
		Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0	OASIS	2005	제정		
		Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0	OASIS	2005	제정		
		Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0	OASIS	2005	제정		
		XML-Signature Syntax and Processing	W3C	2001	제정		
		Canonical XML 1.0	W3C	2001	제정		
		Exclusive XML Canonicalization Version 1.0	W3C	2002	제정		
		XML Encryption Syntax and Processing	W3C	2002	제정		
		Decryption Transform for XML Signature	W3C	2002	제정		
		XML Key Management Specification (XKMS 2.0)	W3C	2005	제정		
		XML Key Management Specification (XKMS 2.0) Bindings 2.0	W3C	2005	제정		
		Web Services Policy 1.5 ? Framework	W3C	2007	제정		
		Web Services Policy 1.5 ? Attachment	W3C	2007	제정		
		OMA Web Services Enabler (OWSER):Core Specifications, Approved Version 1.1	OMA	2006	제정		
		OMA Web Services Enabler (OWSER):Overview, Approved Version 1.1	OMA	2006	제정		
		OMA Web Services Enabler (OWSER) Best Practices: WSDL Style Guide	OMA	2006	제정		
	Lawful Interception	Telecommunications security; Lawful interception; Handover specification for IP delivery	ETSI	2004	제정		
		Telecommunications security; Lawful interception; Service specific details for E-Mail delivery	ETSI	2004	제정		
		Telecommunications security; Lawful interception; Service specific details for Internet Access Services	ETSI	2004	진행		
		Telecommunications security; Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic	ETSI	2003	제정		
		Telecommunications security; Lawful Interception (LI); Requirements of Law Enforcement Agencies	ETSI	2001	제정		
		Universal Mobile Telecommunications System (UMTS); 3G Security; Lawful interception Requirements	ETSI	2002	제정		
		Universal Mobile Telecommunications System (UMTS); 3G Security; Lawful interception Architecture and Functions	ETSI	2003	제정		
		Universal Mobile Telecommunications System (UMTS); 3G security; Handover interface for Lawful Interception (LI)	ETSI	2003	제정		
		Terrestrial Trunked Radio (TETRA); Security; Lawful Interception (LI) interface; Feasibility study report	ETSI	1998	제정		
		Intelligent Networks (IN); Lawful Interception	ETSI	2000	제정		
		Terrestial Trunked Radio (TETRA); Security; Lawful Interception (LI) interface	ETSI	1999	제정		
		Cable IP Handover for Voice and Multimedia	ETSI	2002	제정		
		Cable IP Handover for data	ETSI		제정		
		Telecommunications Security; Lawful Interception (LI); Requirements for Network Functions	ETSI	2002	제정		
		Telecommunications Security; Lawful Interception (LI); Handover Interface for the Lawful Interception of Telecommunications Traffic (revised version).	ETSI	2001	제정		

구분	표준화항목	표준명	기구 (업체)	제정 연도	재개정 현황	국내 관련표준	국내 추진기구
응용보안	Lawful Interception	Electronic Signature Formats	ETSI	2000	제정		
		Security Techniques Advisory Group (STAG); Definition of user requirements for lawful interception of telecommunications; Requirements of the law enforcement agencies	ETSI	1996	제정		
		Digital cellular telecommunications system; Lawful Interception requirements for GSM (GSM 10.20 version 5.0.1)	ETSI	1997	제정		
		Digital Cellular telecommunications sytem (Phase 2+); Lawful Interception requirements for GSM (GSM 01.33 version 7.0.0 Release 1998)	ETSI	2001	제정		
		Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Security; Studies into the Impact of lawful interception	ETSI	1999	제정		
		Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; Service independent requirements definition; Lawful interception - top level requirements	ETSI	2001	제정		
		Telecommunications security; Lawful Interception (LI); Description of GPRS HI3	ETSI	2001	제정		
		Telecommunications Security; Lawful Interception (LI); Concepts of Interception in a Generic Network Architecture.	ETSI	2001	제정		
		Telecommunications Security; Lawful Interception (LI); Issues on IP Interception.	ETSI	2001	제정		
		Telecommunications security; Lawful Interception (LI); Notes on ISDN lawful interception functionality	ETSI	2001	제정		
		Digital cellular telecommunications system (Phase 2+); Lawful Interception requirements for GSM (3GPP TR 41.033 version 5.0.0 Release 5)	ETSI	2002	제정		
		Terrestrial Trunked Radio (TETRA); Security; Lawful Interception (LI) interface	ETSI	1997	제정		
		Digital cellular telecommunications system (Phase 2+); Lawful Interception - Stage 1 (GSM 02.33 version 7.3.0 Release 1998)	ETSI	2001	제정		
		Digital cellular telecommunications system (Phase 2+); Lawful interception; Stage (GSM 03.33 version 8.1.0 Release 1999)	ETSI	2000	제정		
		Time Stamping Profile	ETSI	2002	진행		
		TIPHONTM Release 4; Functional Entities, Information Flow and Reference Point Definitions; Lawful Interception	ETSI	2002	제정		
		Cisco Architecture for Lawful Intercept In IP Networks	IETF	2003	제정		
		IETF Policy on Wiretapping	IETF	2000	제정		
보안평가	정보보호평가	암호 모듈보안 요구사항	ISO/IEC	2006	제정		
		운영시스템 보안성 평가	ISO/IEC	2006	제정		
		IT 보안성 평가 기준 개정판	ISO/IEC	2008	개정		
		IT 보안성 평가 방법론 개정판	ISO/IEC		개정		
		IT 보안성 보증 프레임워크	ISO/IEC		진행		
		보호 프로파일 및 보안목표명세서 작성 가이드라인 개정판	ISO/IEC		진행		
		바이오 인식 보안성 평가 프레임워크	ISO/IEC	2008	진행		
		암호 모듈 시험 요구사항	ISO/IEC		제정		
		Overview & Vocabulary	ISO/IEC				
		ISMS Requirement	ISO/IEC				

구분	표준화항목	표준명	기구 (업체)	제정 연도	재개정 현황	국내 관련표준	국내 추진기구
보안평가	정보보호평가	Code of practice for information security management(ISO/IEC 1799)	ISO/IEC				
		ISMS Implementation guidelines	ISO/IEC				
		ISMS measurements	ISO/IEC				
		Information Security Risk management	ISO/IEC				
		Requirement for the accreditation of bodies providing certification of ISMS	ISO/IEC				

[참고문헌]

〔1〕 KISA, 국내외 정보보호산업 현황 및 주요 정책 진단, 2007

〔2〕 KISA, OECD 개인정보보호 논의 동향: 정보보호작업반(WPISP)의 프라이버시와 정보보호 관련 논의를 중심으로, 2006

〔3〕 KISA, 개인정보 영향평가 제도 최근 동향 및 활성화 방안, 2006

〔4〕 KISA, 개인정보보호백서, 2003

〔5〕 국가정보원, 정보통신부, 국가정보보호백서, 2006

〔6〕 TTA, 정보보호 표준화 로드맵, 2006

〔7〕 TTA, 정보보호 표준화 로드맵, 2005

〔8〕 KISA, 정보보호기술 국제표준화 추진 및 동향 분석, 2005

〔9〕 KISA, 정보보호 표준화 로드맵, 2004.7.

〔10〕 염흥열, 2003년도 정보보호일반 표준화 로드맵, TTA, 2003.

〔11〕 KISA, http://www.kisa.or.kr/, 정보보호 표준화 목록, 2003.

〔12〕 IETF, http://www.ietf.org/, IETF, PKIX, IPSec, S/MIME, MSEC 등의 작업반 홈페이지, 2003.

〔13〕 OMA, http://www.wapforum.org/, OMA 홈페이지, 2003.

〔14〕 ITU, http://www.itu.int/home/index.html, ITU 홈페이지, 2003.

〔15〕 NIST, http://www.nist.gov/, NIST 홈페이지, 2003

〔16〕 ISO/IEC JTC1, http://www.jtc1.org/, ISO 홈페이지, 2003

〔17〕 TTA, http://www.tta.or.kr, TTA홈페이지, 2003.

〔18〕 MIC, http://www.mic.go.kr/index.jsp, MIC 홈페이지, 2003.

〔19〕 MIC, 정통부 정보보호 중장기 기술개발계획서, 초안, 2003

〔20〕 MIC, 정통부 정보보호 중장기 기술개발계획서, 2002.

〔21〕 이계상, 류재철, 이광수, 이재광, 염흥열, 정수환, 채기준, IETF 정보보호 표준화 동향 분석에 관한 연구, 한국정보보호진흥원, 2002.12.

〔22〕 과기처, 정보보호분야 국가기술지도 맵, 김홍근, 염흥열, 이희조, 2003.7.

〔23〕 Rivest, R., "The MD5 Message-Digest Algorithm", RFC 1321, April 1992.

〔24〕 Eastlake, D. and P. Jones, "US Secure Hash Algorithm 1 (SHA1)", RFC 3174, September 2001.

〔25〕 Housley, R., Ford, W., Polk, W. and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", RFC 3280, April 2002.

〔26〕 Housley, R., Ford, W., Polk, W. and D. Solo "Internet X.509 Public Key Infrastructure: Certificate and CRL Profile", RFC 2459, January, 1999.

〔27〕 Myers, M., Ankney, R., Malpani, A., Galperin, S. and C. Adams, "X.509 Internet Public Key

Infrastructure Online Certificate Status Protocol - OCSP", RFC 2560, June 1999.

[28] Pinkas, D., Ross, J. and N. Pope, "Electronic Signature Policies", RFC 3125, September 2001.

[29] Pinkas, D., Ross, J. and N. Pope, "Electronic Signature Formats for long term electronic signatures", RFC 3126, September 2001.

[30] Housley, R. and P. Hoffman, "Internet X.509 Public Key Infrastructure. Operational Protocols: FTP and HTTP", RFC 2585, May 1999.

[31] Boeyen, S., Howes, T. and P. Richard, "Internet X.509 Public Key Infrastructure Operational Protocols LDAPv2", RFC 2559, April 1999.

[32] Hoffman, P., "Enhanced Security Services for S/MIME", RFC 2634, June 1999.

[33] Kent, S., "Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management", RFC 1422, February 1993.

[34] Balenson, D., "Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes, and Identifiers", RFC 1423, February 1993.

[35] Bradner, S., "Key Words for Use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[36] Kaliski, B., "PKCS #1: RSA Encryption Version 1.5", RFC 2313, March 1998.

[37] US National Computer Security Center, "Department of Defense Trusted Computer System Evaluation Criteria", DoD 5200.28-STD, US Department of Defense, Ft. Meade, MD., December 1985.

[38] US National Computer Security Center, "Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria", NCSC-TG-005, Version 1, US Department of Defense, Ft. Meade, MD., 31 July 1987.

[39] Haller, N., and R. Atkinson, "On Internet Authentication", RFC 1704, October 1994.

[40] Harkins, D., and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

[41] SDNS Secure Data Network System, Security Protocol 3, SP3, Document SDN.301, Revision 1.5, 15 May 1989, published in NIST Publication NIST-IR-90-4250, February 1990.

[42] Shacham, A., Monsour, R., Pereira, R., and M. Thomas, "IP Payload Compression Protocol (IPComp)", RFC 2393, August 1998.

[43] Thayer, R., Doraswamy, N., and R. Glenn, "IP Security Document Roadmap", RFC 2411, November 1998.

[44] John Ioannidis and Matt Blaze, "Architecture and Implementation of Network-layer Security Under Unix", Proceedings of USENIX Security Symposium, Santa Clara, CA, October 1993.

[45] Kent, S., and R. Atkinson, "IP Authentication Header", RFC 2402, November 1998.

[46] Kent, S., and R. Atkinson, "IP Encapsulating Security Payload (ESP)", RFC 2406, November 1998.

〔47〕 Kent, S., "US DoD Security Options for the Internet Protocol", RFC 1108, November 1991.

〔48〕 Maughan, D., Schertler, M., Schneider, M., and J. Turner, "Internet Security Association and Key Management Protocol (ISAKMP)", RFC 2408, November 1998.

〔49〕 Orman, H., "The OAKLEY Key Determination Protocol", RFC 2412, November 1998.

〔50〕 Piper, D., "The Internet IP Security Domain of Interpretation for ISAKMP", RFC 2407, November 1998.

〔51〕 ITU-T X680, Abstract Syntax Notation One (ASN.1): Specification of Basic Notation, ITU-T Recommendation X.680 (1997) | ISO/IEC International Standard 8824-1:1998.

〔52〕 ITU-T X690, ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules(DER), ITU-T Recommendation X.690 (1997)| ISO/IEC International Standard 8825-1:1998.

〔53〕 CCITT Recommendation X.208: Specification of Abstract Syntax Notation One (ASN.1), 1988.

〔54〕 ITU-T Recommendation X.660 Information Technology -ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER), 1997.

〔55〕 X9.62-1998, "Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)", January 7, 1999.

〔56〕 ISO/IEC 9594-8/ITU-T Recommendation X.509, "Information Technology - Open Systems Interconnection: The Directory: Authentication Framework", 1997 edition.

〔57〕 ISO/IEC JTC1/SC6, Network Layer Security Protocol, ISO-IEC DIS 11577, International Standards Organisation, Geneva, Switzerland, 29 November 1992.

〔58〕 Federal Information Processing Standards Publication (FIPS PUB) 180-1, Secure Hash Standard, 17 April 1995.

〔59〕 Federal Information Processing Standards Publication (FIPS PUB) 186, Digital Signature Standard, 27 January 2000. 〔Supersedes FIPS PUB 186-1 dated 15 December 1998.〕

〔60〕 ANSI X9.42-2000, "Public Key Cryptography for The Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography", December, 1999.

〔61〕 ANSI X9.63-2001, "Public Key Cryptography For The Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography", Work in Progress.

〔62〕 IEEE P1363, "Standard Specifications for Public-Key Cryptography", 2001.

〔63〕 Bruce Schneier, Applied Cryptography, Section 8.6, John Wiley & Sons, New York, NY, 1994

〔64〕 ITU-T Recommendation X.1121, "X.1121: Framework of security technologies for mobile end-to-end data communication", ITU-T SG17, March 2004.

〔65〕 ITU-T Recommendation X.1122, "X.1122: Guideline for implementing secure mobile systems based on

PKI", ITU-T SG17, March 2004.

〔66〕 ITU-T Recommendation J.190 "Architecture of MediaHomeNet that supports cable based services" defines a reference model of home network based on cable network and describes security requirements for the reference model.

〔67〕 ITU-T Recommendation J.192 "Residential Gateway to support the delivery of cable data services" describes home gateway security.

〔68〕 Heung-Youl Youm, Heung-Ryong Oh, "Updated first draft Recommendation X.homesec-1: Framework of security technologies for home network", ITU-T SG17, COM17-D172-E, April 2006.

〔69〕 Dong-Young Yoo, Gang-Shin Lee, Jae-IL Lee, Heung-Youl Youm, "Draft text on X.homesec-2 : Device certificate profile for the home network", ITU-T SG17, COM17-D173-E, April 2006.

〔70〕 Hyung-Kyu Lee, Hong-IL Ju, Yun-Kyung Lee, Jong-Wook Han, Kyo-IL Chung, Heung-Youl Youm, "Proposal for the first draft of X.homesec-3 User authentication mechanism for home network services", ITU-T SG17, COM17-D176-E, April 2006.

〔71〕 Jianyoung Chen, Feng Zhang, "First draft—General security service (policy) for secure mobile end to end data communication, X.msec-3", ITU-T SG17, TD2330, Arpil 2006.

〔72〕 Zheng Zhibin, Wei Jiwei, "Revised text of X.msec-4 from the Editor", ITU-T SG17, COM17-187-E, April 2006.

〔73〕 Liu Shuling, Wei Jiwei, Zheng Zhibin, "New draft text of X.crs: Correlative reacting system in mobile data communication", ITU-T SG17, COM17-189Rev.1-E, April 2006.

〔74〕 Heung-Youl Youm, Young-Man Park, "New Draft Text of X.sap-1: Guideline on secure password-based authentication protocol with key exchange", ITU-T SG17, COM17-D171-E, April 2006.

〔75〕 Tadashi KAJI, "Proposal on the process model of secure communications for X.sap-2", ITU-T SG17, COM17-D143-E, April 2006.

〔76〕 Yutaka Miyake, "Proposal of Recommendation X.p2p-1 structure", ITU-T SG17, COM17-D144-E, April 2006.

〔77〕 Hyeok-Chan Kwon, Jae-Hoon Nah, Jong-Soo Jang, "Secure Routing on P2P Overlay Networt 외 3편", ITU-T SG17, COM17-D193~6-E, April 2006.

〔78〕 Abbie Barbir, "ITU-T Candidate Recommendation X.websec-1 – Security Assertion Markup Language (SAML)", ITU-T SG17, TD2273Rev.2, April 2006.

〔79〕 Abbie Barbir, "Extensible Access Control Markup Language Version 2.0 (XACML)", ITU-T SG17, TD2278Rev.3, April 2006.

〔80〕 Jae-Seung Lee, Ki-Yoong Moon, Kyo-IL Chung, "Guideline on Security Architecture for Message Security in Mobile Web Services", ITU-T SG17, COM17-D174—E, April 2006.

〔81〕 염흥열, "ITU-T 모바일 보안 표준 분석 및 전망", TTA IT Standard Weekly, 2004.4.
〔82〕 오흥룡, 염흥열, "ITU-T SG17 정보보호 표준화 동향과 Mobile Security 표준 분석", 한국정보보호진흥원, 2004.12.
〔83〕 염흥열, "ITU-T SG17 WP2 Q.9(안전한 통신 서비스) 표준화 동향 및 향후 전망", 한국정보보호진흥원, 2005.12.
〔84〕 염흥열, ITU-T SG17 종단간 이동 통신 보안을 위한 보안 정책 및 홈 네트워크 보안 프레임워크에 관한 표준화 동향 , TTA IT Standard Weekly, 2005.1.
〔85〕 염흥열, "ITU-T가 홈 네트워크 보안 표준을 주도할 수 있을까?", TTA IT Standard Weekly, 2005.5.
〔86〕 진병문, 오흥룡, 염흥열, 정교일, "ITU-T SG17 모스크바 회의", TTA 저널, 99호, 2005.6.
〔87〕 진병문, 오흥룡, 염흥열, 정교일, "ITU-T SG17 제네바 회의", TTA 저널, 102호, 2005.12.
〔88〕 진병문, 오흥룡, 염흥열, 강신각, "2005년 ITU-T SG17 연구동향", TTA, ITU-T 연구활동 보고서, 2005.12.

[약어]

3GPP	3rd Generation Partnership Project
AAA	Authentication, Authorization, Accounting
AES	Advanced Encryption Standard
AP	Access Point
API	Application Program Interface
ASP	Application Service Provider
BcN	Broadband Convergence Network
CA	Certification Authority : 인증기관
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CERT	Computer Emergency Response Team
CMVP	Cryptographic Module Validation Program
CRYPTREC	CRYPTography Research and Evaluation Committee
DARPA	Defense Advanced Research Projects Agency
DDoS	Distributed Denial of Services
DES	Data Encryption Standard
EAL	Evaluation Assurance Level
ECC	Elliptic Curve Cryptosystem
ETRI	Electronic Telecommunications Research Institute
ETSI	European Telecommunications Standards Institute
FIPS	Federal Information Processing Standards
FIRST	Forum of Incident Response and Security Teams
HAS-160	160-bit Hash Algorithm Standard
IDS	Intrusion Detection System : 침입탐지시스템
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPS	Intrusion Protection System
IPSec	Internet Protocol Security

ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
ISAC	Information Sharing & Analysis Center
ISP	Internet Service Provider
ITU-T	Intgernational Telcommunication Union-Telecommunication
KCDSA	Korea Certificate-based Digital Signature Algorithm
KIISC	Korea Institute on Information Security and Cryptology
KISA	Korea Information Security Agency
MLS	Multi Level Security
NCSC	National Computer Security Center
NESSIE	New European Schemes for Signatures, Integrity, and Encryption
NIIPS	National Information Infrastructure Protection Secretariat
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Accreditation Program
OMA	Open Mobile Alliance
PAN	Personal Area Network
PDA	Personal Digital Assistants : 개인 휴대 단말기
PKI	Public Key Infrastructure
PKI Forum	Public Key Infrastructure Forum
PMI	Privilege Management Infrastructure : 권한관리 기반구조
RBAC	Role-Based Access Control
RFID	Radio Frequence Identification
RSA	Rivest-Shamir-Adelman)
RSA-OAEP	RSA-Optimal Asymmetric Encryption Padding
SET	Secure Electronic Transaction
SSL	Secure Socket Layer
SSO	Single Sign-on
TCSEC	Trusted Computer System Evaluation Criteria
TLS	Trnansport Layer Security
TTA	Telecommunications Technology Association
VPN	Virtual Private Network : 가상 사설망
W3C	World Wide Web Consortium
WPAN	Wideband Personal Area Network