응용보안/평가인증

1. 개요

1.1. 기술개요

1.1.1. 중점기술 및 표준화 대상항목의 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 기술로, 응용보안 및 평가인증의 2가지 분야로 구분될 수 있음

- 정보보호 기술측면에서 응용보안 분야의 비중이 점점 확대되고 있는 추세에 있음. 사회의 변화에 힘입어 사이버 공간에서의 정보활동의 중요성과 그 폐해에 대한 위해성이 부각되고 있으므로 이에 대한 기술적, 제도적 장치가 필요한 시점임. 개인의 프라이버시를 보장하여야 하지만 사이버 공간과 더 나아가 사회의 질서를 유지하는 것이 절실히 필요함. 이것은 정보보호 기술이 점점 인간의 사이버 활동과 밀접한 관계를 갖는 상위 개념의 콘텐츠와 그 사용권한에 대한 관리와 같은 문제로 집중됨. 또한 인간 사회활동과 유사한 수준의 상호 신뢰 할 수 있는 사이버공간을 조성이 필요하며 이를 위하여 인간–장비와 장비–장비 간의 신뢰 구축에 대한 기술개발이 부담없이 진행되고 있음
- 정보보호가 과거에는 단순 정보보호의 차원에서 전산시스템에 국한되는 것으로 치부되었지만 현재는 인간 사회 조직의, 더 나아가 국가의 이미지 관리로 이어지며, 보안 관리의 실수로 인한 조직의 사활의 중대한 영향을 미침을 인식하고 이에 대한 연구 및 표준이 박차를 가하고 있음

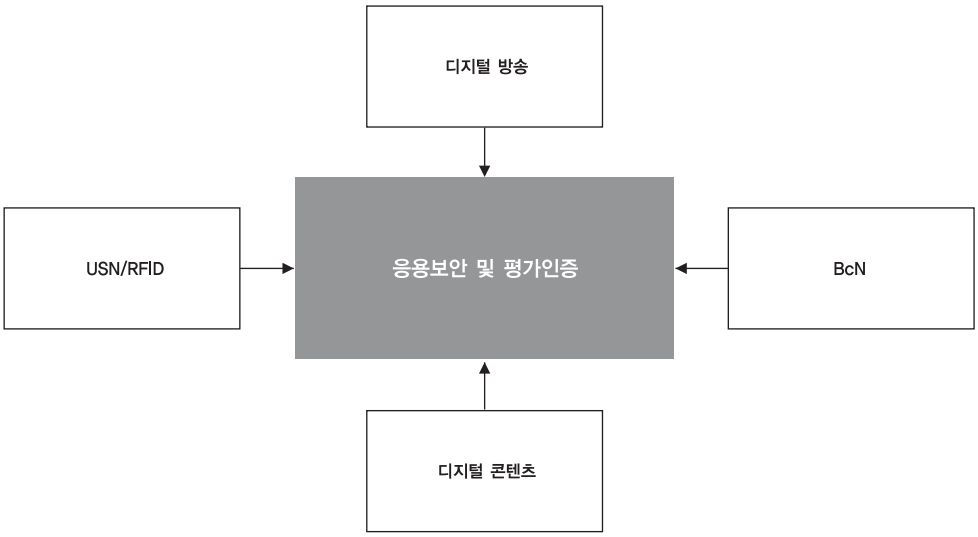
○ 표준화 대상항목의 정의

- 금년도 표준화 대상항목은 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 표준화 대상항목으로 선정되었고, 평가인증 분야의 경우, 정보보호 평가와 보안관리가 표준화 대상항목으로 선정되었음

구분	정의	표준화 대상항목	표준화 내용
응용보안	응용 레벨을 위한 보호 기능을 제공하기 위한 기술들을 포함	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(TPM)	신뢰 컴퓨팅 기술의 관련 표준화 – 신뢰보안 프레임워크, 신뢰보안 메커니즘 – 디바이스/플랫폼 보호, 악성코드 탑재 방지용 무결성 측정 기술 (IMVA: Integrity Measurement and Verification Agent), 임베디드 장치 보호 등
		차세대 웹 보안	차세대 웹 보안에 관한 표준화 – 웹 2.0 보안, SOA 기반 융합서비스 보안, 유비쿼터스 웹 보안, 시맨틱 보안, 모바일 웹 2.0 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 보안 관리, 그리고 암호모듈에 대한 기술을 포함	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 지원하고, 정보자산의 보안 관리를 위한 정보보호의 조직화/제도화 등의 표준화 – 정보보호관리체계 계획 수립 및 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 – 정보자산의 보안 관리 모델 및 지침 등

1.1.2. 연관기술 분석

○ 연관기술 관계도



○ 연관기술 분석표

응용보안 및 평가인증 연계기술은 기반기술과 관련하여 위와 같이 연관됨. 주요 기반 서비스 및 네트워크는 디지털방송, USN/RFID, 디지털콘텐츠, BcN 등임. 이들 연관 기술의 특성은 아래와 같음

연관기술	내 용	표준화기구/단체		표준화수준		기술개발수준	
		국내	국외	국내	국외	국내	국외
디지털방송	디지털방송은 고화질/고음질, 다채널, 양방향서비스, 인터넷 접속 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 정보보호영역으로 나뉘어 이뤄지고 있으나, 대부분 성능개선과 관련한 내용에 치중되어 있고, 디지털 TV 보안부문에 대해서도 종래의 네트워크 보안기술을 중심으로 접근하고 있고, 방송 및 인터넷 그리고 디지털콘텐츠 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 · 인터넷 등 각종 서비스 영역을 통합한 멀티미디어 서비스를 시간과 장소에 구애받지 않고 이용할 수 있는 차세대 통합 네트워크임. 통신 · 방송 · 인터넷의 대통합시대에 대응하고 신성장동력산업의 발전토대마련을 위해 광대역통합망(BcN) 구축이 필요함. 현재 BcN은 ITU-T SG13에서 금년부터 FG(Focus Group) 구조에 대한 표준화를 진행 중임. 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
디지털콘텐츠	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 실정임다. 디지털콘텐츠의 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 디지털콘텐츠 표준화의 제정이 시급한 실정이나, DRM의 경우 동일콘텐트에 대해 재생기기 간에 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, 한국디지털콘텐츠 미래포럼	ISO/IEC JTC1, ITU-T, IEEE	IETF, ITU-T, MPEG-21, OMA, CPTWG, 4C Entity – CPPM/CPRM 5CDTCP	표준 최종 검토	시제품/ 프로토타입	상용화

1.2. 추진경과 및 중점 추진방향

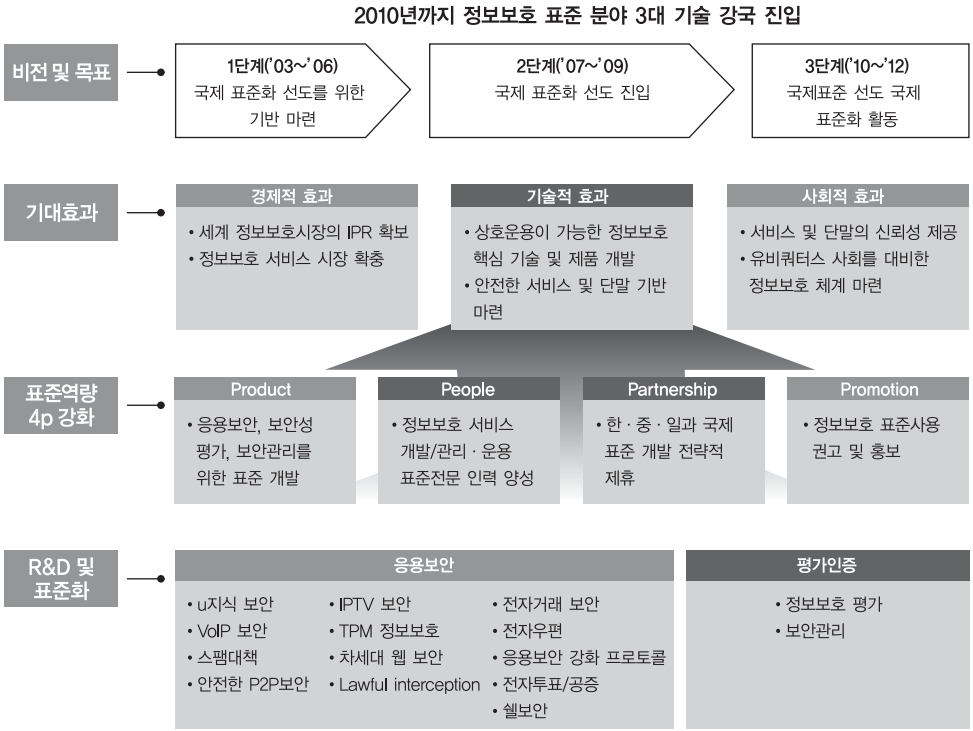
○ 추진경과

- Ver.2005에는 모든 분야에 대한 표준화 항목을 정리함
- Ver.2006에는 TTA를 통하여 수행되지 않고 한국정보보호진흥원을 통하여 수행되었으며, 주로 IT839와 연계된 정보보호 표준 분야를 정리함
- Ver.2007에는 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
- Ver.2008에는 응용보안 분야를 u지식, IPTV, 신뢰보안서비스(TPM), 차세대 웹 보안 및 Lawful Interception 과 같은 기술이 신규 중점 표준화 기술항목으로 추가하였고, 평가인증 분야에서 정보보호 평가와 보안관리 분야를 중심으로 정리함
- Ver.2009에는 IPTV 및 평가분야를 중점적으로 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, 신뢰보안서비스(TPM), 차세대 웹 보안 및 Lawful Interception 등에서의 표준안 제정은 보안 산업 및 관련 시장을 통해 실제로 적용되어 상용화될 가능성이 큰 부분임을 감안할 필요성이 있음
- 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
- 평가인증 분야 중 정보보호 평가 부분은 평가기준과 방법론에 대한 표준화가 선진국 중심으로 매우 활발히 진행되고 있는 상황으로, 국내에서도 적극적으로 참여하여 우리나라의 입지 강화를 통한 자국의 이익을 대변할 필요가 있음. 더불어 보안관리 분야의 ISMS에 대한 국제표준 제정으로 인한 관심 증대 및 관리체계 인증의 활성화로 국내 보안관리의 선진화 및 경쟁력을 제고 하는 차원에서 추진할 필요성이 있음
- 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 운용 중인 시스템 및 장비 현황을 분석하고, 어느 단체 또는 기업의 표준안을 기반으로 하고 있는지를 검토함

1.3. 표준화의 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 진행 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, 홈네트워크 보안, RFID/USN, P2P, 모바일 웹서비스 보안 표준 등을 들 수 있음

○ 그러나, 최근 우리나라는 인터넷 인프라가 세계 정상수준으로 향상되고 있고, 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 제품 간의 상호 연동성 보장이 매우 중요함. 이렇게 함으로써, 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 민간 간의 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 구성됨. 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 있으

며, 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 정보보호 관리체계를 계획, 구현, 운영지원, 감시 및 검토하는 프로세스에 관련한 표준 지침 및 기법 등을 포함함

○ 향후 정보보호 표준화 정책은 국제 표준화 기구에서 이미 성숙도가 높은 국제 표준을 국내 시장이 필요에 따라 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 국내의 선도 기반 기술 개발 사업과 국제 표준화 활동을 긴밀히 연계하여 관련 기술개발과 표준화 활동을 추진하는 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 시스템 간의 상호 연동을 가능케 하고, 안전하고 신뢰성 있는 통신을 보장하는 핵심 기술로, 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 PC 내의 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 필요함. 이러한 정보화는 최근 급속히 확산되고 있는 인터넷과 함께 기존의 정보산업뿐만 아니라 정통산업의 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 운

용성 확보를 위하여 반드시 필요한 요구사항임. 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

- 2012년까지 정보보호 분야의 리드 SG인 SG17을 통하여 응용보안 분야에서 총 6건 이상의 국제 표준화를 완성함을 목표로 함
- 2014년까지 IETF를 통하여 인터넷 분야 정보보호에 대한 국제 표준화를 추진함
- 2014년까지 중요 국제 표준화 기구에서 표준화된 총 60여 건(매년 10여 건)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 분야로서 최근 떠오르고 있는 u지식서비스, IPTV, 신뢰보안서비스(TPM), P2P, VoIP, 스팸대책 등의 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

〈추진 중인 국제표준〉

표준화 기구	현재 국제표준화 추진 중인 권고안 제목	분야	국제 표준화 완료시점
ITU-T	Functional Requirements and Architecture for IPTV Security Aspects	응용 보안	2008
ITU-T	Key management framework for secure IPTV communications	응용 보안	2010
ITU-T	Requirements and mechanisms for secure transcodable scheme of IPTV	응용 보안	2010
ITU-T	Security framework for ubiquitous sensor network	응용 보안	2009
ITU-T	Framework for combating e-mail spam via Botnet	응용 보안	2011
ITU-T	Information security governance framework	보안 관리	2010
ITU-T	OTP(One Time Password) based Security Service-Generic Architecture and Service Requirement	응용 보안	2010
ITU-T	Security Architecture for Message Security in Mobile Web Services	응용 분야	2007
ITU-T	Security framework for enhanced Web based telecommunication services	응용 분야	2010

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 스마트카드 등의 인간 친화적 정보보호 제품을 통하여 원격 가전 제어 및 재택근무를 가능케 하여 국민 생활의 질을 향상할 수 있을 것으로 판단

○ 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 평가인증 및 보안관리 표준화를 통하여 상호동작이 가능한 정보보호 제품, 대규모 정보보호 시장 형성, 안전하게 동작하는 정보보호 제품 개발, 종합적이고 체계적인 조직의 정보자산의 보안 관리를 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 국

내 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 가능할 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 아래와 같이 크게 "시스템 및 네트워크 정보보호 제품" 및 "정보보호서비스"의 두 분야로 구분될 수 있으며, 본 표에서는 2006~2007년의 매출 현황을 보여주고 있음
- 정보보호산업의 2006년도 매출 실적은 705,247백만 원에서 5.4%인 37,907백만 원이 증가하여 2007년도에 743,154백만 원으로 조사되었음
- '시스템 및 네트워크 정보보호 제품' 분야의 총 매출액은 2006년 611,606백만 원에서 2007년 628백만 원으로 28% 증가하였다. '정보보호 서비스' 분야의 총 매출액은 2006년 93,641백만 원에서 2007년 114,549백만 원으로 22.3% 증가하였음
- 한편, 2007년도 정보보호산업의 매출 총액의 비중을 비교해 보면, '시스템 및 네트워크 정보보호 제품' 분야는 84.6%, '정보보호 서비스' 분야는 15.4%로 양자 간 매출비중의 차이가 있음을 알 수 있음

〈정보보호산업의 분류별 매출액 현황〉

(단위: 백만 원)

구분	2006년	2007년	증감률(%)	매출비중(%)
시스템 및 네트워크 정보보호제품	611,606	628,605	2.8	84.6
정보보호서비스	93,641	114,549	22.3	15.4
합계	705,247	743,154	5.4	100.0

(출처: 한국정보보호협회, "2007 국내 정보보호산업 시장 및 동향조사")

○ 국내 정보보호산업 수출입 현황

- 수출 현황
  - 2007년도 수출액이 53,197백만 원으로 2006년도 수출액 34,997백만 원 보다 18,200백만 원(52.0%) 증가한 것으로 조사되었음 구체적으로 '시스템 및 네트워크 정보보호제품' 분야인 경우 2006년도 수출액 34,105백만 원에서 2007년 51,984백만 원으로 17,879백만 원(52,4%) 증가하였음. '정보보호서비스' 분야의 수출액은 2006년 892백만 원에서 2007년 1,213백만 원으로 321백만 원(36.0%) 증가하였음. 수출비중을 살펴보면, '시스템 및 네트워크 정보보호 제품'이 아직까지 절대적인 우위를 차지하고 있음을 알 수 있음
- 정보보호관련 기업의 주요 수출 국가
  - 정보보호산업의 국가별 수출 현황을 조사한 결과, '일본'에 수출하는 기업 수가 가장 많은 52개(45.2%)로

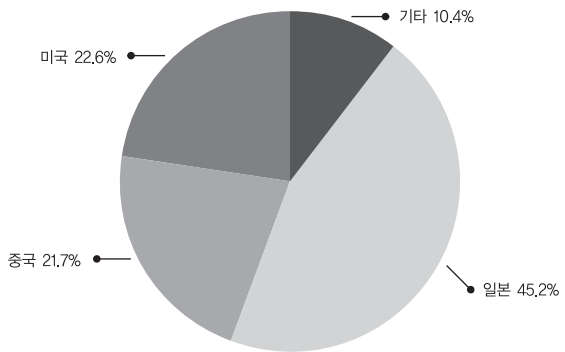
전체 수출액의 55.9%를 차지하는 것으로 나타났고, 다음으로 '미국'에 수출하는 기업은 26개(22.6%)로 수출액 비중 19.4%임. '중국'에 수출하는 기업 수는 25개(21.7%)로 수출액 비중 16.4%로 조사되었음. 기타 국가(유럽, 말레이시아 등)에 수출하는 기업은 12개(10.4%)이며 수출액 비중은 8.3%임

- 수출 전망
  - 2008년도 총 수출액은 62,297백만 원으로 예상되는데, 이는 2007년도 총 수출액 53,197백만 원에 비해 17.1% 증가한 것이다. 대분류별로 살펴보면, '시스템 및 네트워크 정보보호 제품' 분야는 2007년 수출액 51,984백만 원에서 2008년에는 17.2% 증가한 60,924백만 원으로 예산됨. '정보보호 서비스' 분야의 수출액은 2007년 1,213백만 원에서 13.2% 증가하여 2008년도에는 1,373백만 원에 이를 것으로 전망됨

〈정보보호산업의 수출 현황〉

(단위: 백만 원)

구분	2006년	2007년	증감률(%)	매출비중(%)
시스템 및 네트워크 정보보호제품	34,105	51,984	52.4	97.7
정보보호서비스	892	1,213	36.0	2.3
합계	34,997	53,197	52.0	100.0



〈정보보호산업의 주요 수출국가 현황〉

(출처: 한국정보보호협회, "2007 국내 정보보호산업 시장 및 동향조사")

- 수입 현황
  - 2007년도 수입액은 61,838백만 원으로 2006년도 수입액 61,114백만 원 보다 724백만 원 증가하여 1.2% 증가율을 보이고 있음
  - '시스템 및 네트워크 정보보호제품' 분야의 수입액은 2006년 55,912백만 원에서 2007년 56,399백만 원으로 0.9% 증가한 것으로 나타났다. '정보보호 서비스' 분야의 수입액은 2006년 5,202백만 원에서 2007년 5,439백만 원으로 4.6% 증가하였음

– 정보보호관련 기업의 주요 수입 국가

• 정보보호관련 기업의 주요 수입 국가를 조사한 결과, '미국'으로부터 수입하는 기업은 총 21개 기업(63.6%)으로 전체 수입액의 72.1%를 차지하고 있는 것으로 나타났음. 다음으로, '일본'에서 수입하고 있는 기업은 6개(18.2%)로 수입액 비중은 15.6%, '중국'은 3개 기업(9.1%)으로 수입액 비중은 6.7%로 조사되었음. '기타 국가(유럽 등)'에서 수입하고 있는 기업은 3개 기업(9.1%)으로 수입액은 전체 수입액의 5.6%를 차지하는 것으로 분석되었음

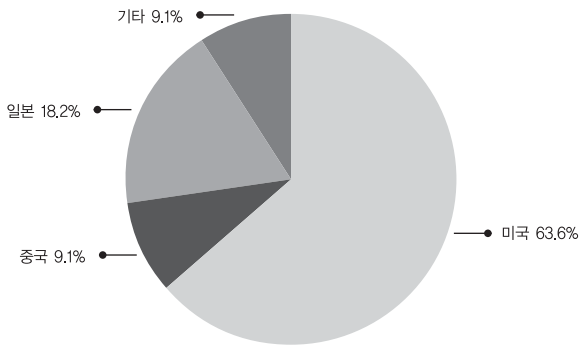
– 수입 전망

• 2008년도 수입액은 62,200백만 원으로 2007년도 수입액 61,838백만 원에 비해 0.6% 증가할 것으로 예상됨. '시스템 및 네트워크 정보보호제품' 분야의 수입액은 2007년도에 비해 0.4% 증가하여 2008년도에는 56,643백만 원에 이를 것으로 추정되며, '정보보호 서비스' 분야의 수입액은 2007년도 5,439백만 원에서 2008년 5,557백만 원으로 2.2% 증가할 것으로 전망됨

〈정보보호산업의 수입현황〉

(단위: 백만 원)

구분	2006년	2007년	증감률(%)	매출비중(%)
시스템 및 네트워크 정보보호제품	55,912	56,399	0.9	91.2
정보보호서비스	5,202	5,439	4.6	8.8
합계	61,114	61,838	1.2	100.0



〈정보보호산업의 주요 수입국가 현황〉

(출처: 한국정보보호협회, "2007 국내 정보보호산업 시장 및 동향조사")

○ 국내 정보보호산업 매출 전망

– 정보보호산업의 매출액 전망은 2007년도 총 매출액 743,154백만 원으로 전년도 매출액 705,247백만 원 보다 37,907백만 원(5.4%) 증가하였음. 향후 정보보호산업 전체의 매출액을 추정한 결과, 2008년도 매출액은

824,469백만 원까지 증가할 것으로 예상되며, 2006년 705,247백만 원에서 2012년까지 7년간의 연평균성장률(CAGR)이 7.4%로 매출액이 지속적으로 상승하여 2012년에는 1,083,797백만 원에 이를 것으로 전망됨

〈정보보호산업의 매출전망〉

(단위: 백만 원)

구 분	2006년	2007년	2008년	2009년	2010년	2011년	2012년	CAGR(%)
시스템 및 네트워크 정보보호제품	611,606	628,605	698,551	752,280	806,008	859,737	913,465	6.9
정보보호서비스	93,641	114,549	125,918	137,021	148,125	159,228	170,332	10.5
합계	705,247	743,154	824,469	889,301	954,133	1,018,965	1,083,797	7.4

(출처: 한국정보보호협회, "2007 국내 정보보호산업 시장 및 동향조사")

○ 국내 정보보호산업의 분류별 매출 전망

– 아래 표는 2006년부터 2012년까지 "시스템 및 네트워크 정보보호 제품" 및 "정보보호서비스" 분야의 세부적인 매출 예상치를 보여주고 있음

– 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, 콘텐츠 보안, 공개키기반구조(PKI), 접근관리, 통합보안시스템(UTM), 바이오인식 제품, 기타 제품 등 15개의 소분류로 나누었으며 15개의 소분류에는 총 34개의 제품군으로 세분화하였음. 정보보호서비스는 인증서비스, 보안관제, 보안컨설팅, 유지보수, 기타서비스 등 5개의 소분류로 나누었음

– 시스템 및 네트워크 정보보호 제품

시스템 및 네트워크 정보보호제품 분야의 매출액에 대한 전망을 조사 분석한 결과, '통합보안시스템(UTM)' 분야가 CAGR이 9.4%로 가장 높은 성장세를 보이고 있으며, 다음으로 보안운영체제)와 '바이오인식제품' 의 CAGR이 9.3%, '가상사설망' 분야가 8.4% 등의 순으로 성장할 것으로 전망됨

– 정보보호 서비스

정보보호서비스 분야의 매출 전망을 살펴보면, 가장 높은 19.3%의 CAGR을 보이고 있는 '인증서비스' , 다음으로 '보안관제' 분야의 CAGR이 12.0%이며, '기타 서비스' 11.9%, '유지보수' 9.7%, 마지막으로 '보안컨설팅' 이 6.9%의 증가세를 보일 것으로 전망됨

〈기술 분류별 정보보호산업 매출 전망〉

대분류	소분류	2006년	2007년	2008년	2009년	2010년	2011년	2012년	CAGR(%)
시스템 및 네트워크 정보보호 제품	침입차단(방화벽)시스템	72,830	73,767	83,966	91,850	99,733	107,617	115,500	8.0
	보안관리	65,008	65,226	75,105	82,157	89,210	96,262	103,315	8.0
	가상사설망	50,501	50,611	58,402	64,272	70,143	76,013	81,884	8.4
	인증제품	19,647	19,763	22,485	24,524	26,562	28,601	30,639	7.7
	Anti-Virus	72,082	75,122	76,742	78,162	79,682	81,202	82,722	2.3
	Anti-Spam	10,610	11,917	12,571	13,224	13,878	14,531	15,185	6.2
	보안운영체제	22,121	22,143	26,031	28,953	31,874	34,796	37,717	9.3
	PC 보안	35,662	36,574	39,786	42,423	45,060	47,697	50,334	5.9
	콘텐츠 보안	57,585	59,315	65,573	70,309	75,045	79,781	84,517	6.6
	공개키기반구조(PKI)	22,081	22,462	22,653	22,843	23,034	23,224	23,415	1.0
	접근관리	17,296	17,369	19,796	21,418	23,040	24,662	26,284	7.2
	통합보안시스템(UTM)	29,950	30,249	35,449	39,423	43,398	47,372	51,347	9.4
	바이오인식 제품	56,697	63,169	71,198	77,582	83,966	90,350	96,734	9.3
	기타 제품	10,351	10,380	11,143	11,679	12,212	12,748	13,281	4.2
	소 계	611,606	628,605	698,551	752,280	806,008	859,737	913,465	6.9
정보보호 서비스	인증서비스	4,875	7,500	8,813	10,125	11,438	12,750	14,063	19.3
	보안관제	29,270	37,391	41,452	45,512	49,573	53,633	57,694	12.0
	보안컨설팅	27,045	29,821	32,123	34,161	36,198	38,236	40,273	6.9
	유지보수	24,360	29,526	32,109	34,692	37,275	39,858	42,441	9.7
	기타서비스	8,091	10,311	11,421	12,531	13,641	14,751	15,861	11.9
	소 계	93,641	114,549	125,918	137,021	148,125	159,228	170,332	10.5
합 계		705,247	743,154	824,469	889,301	954,133	1,018,965	1,083,797	7.4

(출처: 한국정보보호협회, "2007 국내 정보보호산업 시장 및 동향조사")

2.1.2. 국외 시장 현황 및 전망

○ 국외 정보보호산업 매출 현황

- 2008년 Gartnet 조사에 따르면, 2007년 세계 정보보호 시장은 전년도에 비하여 뚜렷한 감소세를 보이지 않고 약 20% 성장세를 유지하였음. 2007년 주요 업체별 매출규모를 보면, Symantec과 MaAfee가 각각 26.6%와 11.8%의 시장 점유율을 보이면서 선두를 유지하고 있고, EMC는 기업 인수합병에 힘입어 세 자리 수의 성장률을 보이고 있음

〈국외 정보보호 소프트웨어 주요 업체별 매출 현황〉

(단위: 백만 달러)

Company	2007 Revenue	2007 Market Share(%)	2006 Revenue	2006 Market Share(%)	2006~2007 Growth(%)
Symantec	2,768.5	26.6	2,564.3	29.5	8.0
McAfee	1,225.7	11.8	1,072.9	12.3	14.2
Trend Micro	809.6	7.8	701.5	8.1	15.4
IBM	607.9	5.8	465.1	5.3	30.7
CA	419.0	4.0	431.1	5.0	-2.8
EMC	414.6	4.0	121.8	1.4	240.5
Others	4,170.5	4.0	3,338.2	38.4	19.8
Total	10,415.8	100.0	8,694.9	100.0	19.8

(출처: Gartner, 2008)

○ 국외 정보보호산업 매출 전망

- 국외정보보호 시장은 정보보호 하드웨어와 소프트웨어 및 정보보호 서비스 등 크게 세 부문으로 구분되어 질 수 있음. IDC 분석에 따르면 전 세계 IT 보안시장은 2006년에 약 384억 달러 규모에서 2009년에는 약 600억 달러 규모에 이르러 CAGR이 16.9%로 성장이 예상됨
- 각 부분별로는 '정보보호 하드웨어' 시장은 통합위협관리(17%), 콘텐츠보안관리(47%)의 급성장이 예상되고, 방화벽/VPN(-5%)은 감소할 것으로 전망되어 하드웨어 전체 시장은 2009년까지 연평균성장률이 17%를 유지하여 총 117억 달러가 될 것으로 보임
- '정보보호 소프트웨어' 부문에서는 보안 및 취약점관리(18%), 콘텐츠보안관리(16%)가 빠른 성장을 보이고 있으며, 2009년까지 연평균 성장률 14%로 총 192억 달러규모의 매출이 예상됨
- '정보보호 서비스' 부문은 전반적으로 높은 성장률(19%)을 보이는 가운데 관리(20%)와 구현(19%)에서 빠른 성장이 예상됨

〈국외 정보보호산업 분류별 매출 전망〉

대분류	소분류	2006년	2007년	2008년	2009년	CAGR(%)
정보보호H/W	콘텐츠보안관리	580	990	1,335	1,728	47.3
	방화벽/VPN	1,490	1,412	1,348	1,318	-4.8
	IDS/IPS	879	1,060	1,226	1,343	22.0
	통합위협관리	947	1,232	1,870	2,364	47.9
	SSL-VPN 어플라이언스	470	635	762	899	34.9
	HW 인증토큰	589	662	745	764	9.5
	콘텐츠 및 애플리케이션	290	310	320	330	7.0
	기타	2,067	2,353	2,669	3,016	14.2
합 계		7,413	8,703	10,275	11,761	17.6
정보보호S/W	콘텐츠보안관리	6,938	7,950	8,872	9,707	16.1
	인증 및 접속관리	2,875	3,221	3,589	3,980	11.3
	보안 및 취약점관리	1,910	2,266	2,663	3,105	17.8
	위협관리	1,553	1,553	1,778	1,892	7.1
	기타	413	452	494	538	9.5
합 계		13,689	15,552	17,396	19,222	14.0
정보보호 서비스	컨설팅	5,125	6,093	7,230	8,513	18.5
	구현	7,230	8,654	10,326	12,188	19.4
	관리	3,021	3,601	4,309	5,281	19.7
	교육훈련	1,907	2,242	2,656	3,019	16.5
합 계		17,284	20,590	24,521	29,002	18.9
총 시장 규모 합계		38,386	44,845	52,192	59,985	16.9

(출처: IDC, 2005)

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 수립하였음
- 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 하고 있음
- 최근 IPTV 등 신규 응용서비스 분야의 기술 확산이 급속도로 진전되면서, 응용서비스 보안 분야에서 u-지식 보안, 차세대 웹 보안, VoIP 보안, IPTV 보안, P2P 보안, 신뢰보안서비스(TPM), Lawful Interception 등의 핵심 요소기술 고도화를 추진 중이며, 이러한 신규 응용 분야 제품의 보안성 평가 및 관리체계 인증을 위한 평가인증 분야의 표준화를 추진하고 있음

○ 국내 기술개발 현황 및 전망

- 응용보안
  - 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 수준
    - 콘텐츠의 다양한 활용은 하나의 콘텐츠를 하나의 사용자나 기기, 한정된 서비스를 제공하던 기존의 형태에서 다양한 사용자, 기기, 서비스로 유통되고 안전하게 관리되어지도록 요구되고 있으며, 이를 위해 OsMu(One Source Multi Use) 개념을 도입함으로써 다양한 환경에서 활용할 수 있는 기술 및 보안, 유통 기술 문제의 해결을 위한 DRM 기술 간 연계 및 통합 기술, 디지털 콘텐츠의 저작권 보호관리 기술,

CAS(Conditional Access System)와 DRM(Digital Rights Management) 연동 관리 기술 등을 통한 정보보호 및 관리 방안에 대한 전반적인 연구가 요구되고 있음

· 이것은 콘텐츠 인식, 보호, 유통 관리 기술 및 CAS와 DRM 연동을 통한 통합 서비스 미들웨어 및 플랫폼 구현 기술, OsMu 기반의 콘텐츠 검색, 추적, 보호, 재구성 관리 기술에 대한 연구의 필요성을 의미함

– VoIP 보안

- 2008년 1월 VoIP 번호이동제의 시행으로 가입자가 증가할 것으로 예상됨. VoIP는 기존 공중전화망(PSTN; Public Switched Telephone Network) 대신 인터넷으로 음성 통화 서비스를 제공하기 때문에 보안 측면에서 위험성이 높음. VoIP 서비스의 서버를 DDoS 공격해 서비스를 중단하거나 서버의 데이터를 위변조할 가능성이 있음. 또한 전송되는 데이터를 도감청할 수 있으며 스팸의 또 다른 채널로 악용할 가능성도 매우 큼
- 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 지점 간 안전한 통화선로를 설정하는 VPN은 불특정 다수와 착발신 통화를 해야 하는 일반 전화서비스 성격에는 적합하지 않음
- 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
- 최근, 불법도청으로부터 인터넷전화 사용자의 통화내용을 보호할 수 있는 음성, 데이터 암호화 기술을 기반으로 VoIP 암호기술과 키관리 기술이 적용된 인터넷전화기가 개발되어 상용화를 앞두고 있음. 이 인터넷전화기에서는 인터넷 사용자간 통화내용을 보호할 수 있는 종단간 암호통신과 인터넷 전화 사용자가 휴대폰 등으로 통화할 때 인터넷 구간의 통화내용을 보호할 수 있는 일부 구간 암호통신, 일반통화 도중에 암호통화로 전환할 수 있는 기능을 제공함

– 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 실정
- 005년 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, 가입

1) Internet Protocol Security
2) Virtual Private Network

자 증가에 따른 오류율 증가와 다양한 형태의 스팸에 대응하기 어려운 한계를 지지고 있음

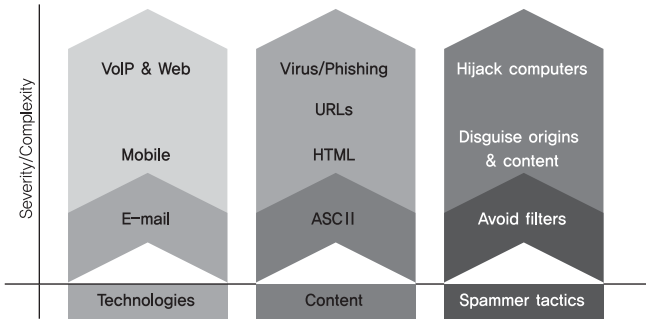
- 최근, 키워드 필터링과 같은 기존의 기술 외에 합법적으로 등록된 서버를 통한 통화요청은 연결하되, 등록되지 않은 서버를 통한 통화요청은 사업자망에서 차단하는 등록서버 인증기능과, 스팸으로 의심되는 통화요청 허용치를 초과하는 통화요청은 차단하는 그레이리스트(Gray list) 관리 기능이 포함된 VoIP 스팸대응 기술이 개발되어 상용화를 앞두고 있음

– 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
- 최근, 대량의 비정상적인 전화통화 요청을 차단하며, 사업자망을 외부로부터 숨겨 VoIP 서비스 장비를 보호할 뿐만 아니라 사설 IP환경에서 IP주소가 변동돼도 통화를 유지하는 기능을 제공하는 보안세션제어기술이 개발된 바 있음

– 스팸대책

- 원치 않는 또는 관련 없는 대량의 데이터(Unsolicited Bulk Data) 전송을 특징으로 하는 스팸은 기존 이메일뿐만 아니라, VoIP, 전화, 휴대폰 텍스트 메시지, P2P 파일, 팩스, 메신저, 웹 게시판, 블로그, 팝업 페이지 등 다양한 응용 매체 및 경로를 통해 그 불법적 유통의 범위를 더욱 확대하고 있는 실정. 또한 스팸의 제작 및 발송 역시 단순 광고/홍보 전달에서부터 치명적인 보안적 결함을 유발시키는 Warm 유포, 바이러스 전파, 악성코드 설치/실행, Phishing 등 보다 적극적인 공격유형를 보이고 있음. 이를 통해 스팸 전파의 목적이 사내 PC 감염(좀비PC), 시스템 원격 제어, 개인/신용정보 유출, 기업 기밀정보 유포 등의 경제적 문제를 야기할 수 있는 형태로 크게 변모하고 있음. 2008년 (주)옥션의 고객정보 유출의 사례의 결정적 원인으로 스팸이 지목되는 것도 이와 같은 맥락에서 해석될 수 있음



〈스팸의 기술적 고도화 추세〉

(출처: OECD Task Force on Spam)

- 따라서 국내 스팸 메일 차단 시스템의 경우, 스팸메일 인지 및 차단은 물론, 메일로부터 바이러스, 악성코드 및 개인정보 유출 유무를 탐지하고, Inbound/Outbound 메일 트래픽의 감시 및 관리하며, 이메일 보안 정책 제공 및 메일 서버 보호하는 등의 다각적인 기술을 상용 제품화하여 시장을 공략하고 있음. 현재 국내 안티스팸 시장은 200억 원대로 예측되고 있으며, 국내 스팸 차단 전문 업체로는 (주)지란지교소프트(스팸스나이퍼), (주)컴트루테크놀로지(클린스팸), (주)모비젠(크레디메일), (주)다우기술(메일와쳐), 크리니티社(SpamBreaker) 등이 대표적임. 또한 Sophos, Symantec, Spamhaus 등의 해외 솔루션이 국내 시장에서도 널리 유통되고 있으며, 웹 메일 및 메신저 서비스의 경우 해당 기업 고유의 스팸 필터링 기술을 개발하여 이용자들에게 제공하고 있음
- 국내의 경우 이미 전체 메일 유통량의 90% 이상이 스팸인 것으로 조사된 바 있으며, 한국은 2005년 2위(18.43%)의 스팸 발송국에서, 2006년에 3위(9.8%)로 순위가 하락한 바 있으나 이것은 중국이 상대적으로 제 2의 스팸메일 발송국(21.9%)으로 등장하고 있기 때문인 것으로 분석되었음
- 한편 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 진행함. 한편 IETF에서는 SIP 관련 기술 표준화를 진행하는데 초점을 맞추고 있음. 정보통신망법 개정에 따라 국내에서는 정통부와 한국정보보호진흥원이 공동으로 스팸방지 가이드라인을 2006년도에 이미 공표한 있음

– 안전한 P2P 보안

- 파일 공유로부터 시작한 P2P 아키텍처는 장점과 위협을 동시에 가지는 기술 분야로, 보안기술은 이 두 가지 특성에 맞게 다각화하여 개발할 필요가 있음. 순기능적 측면에서 P2P 보안은 네트워킹 또는 메시징 목적으로 P2P 아키텍처를 채택함으로써 얻는 잠재적인 이익을 보장하기 위한 방안을 마련하는데 그 목적이 있음. P2P 순기능을 활용한 대표적인 국내 P2P 관련 프로젝트로는 한국과학기술정보연구원(KISTI)에서 2002년 시작된 P2P 기반 분산 컴퓨팅에 관한 프로젝트인 코리아앳홈(Korea@home)이 있음. 또한 기업을 중심으로 다양한 분야에 P2P 아키텍처가 도입되고 있는 추세임. 가트너(Gartner)는 '2008년 10대 기

술전략'을 발표한 바 있는데, 이 중 통합커뮤니케이션(unified communications) 분야는 기업 IT 인프라에 대한 혁신을 의미하는 것으로 메신저, 블로그, 전화, 인터넷 전화, 휴대전화 등을 하나로 통합하는 기술에 관한 것임. 이러한 통합 커뮤니케이션 환경을 위해서는 P2P 인프라가 매우 중요한 역할을 할 것임

- 현재까지 국내에서는 P2P 아키텍처를 도입하는 기업이 증가하는 만큼 P2P 보안 기능을 교육하는 데 상당히 주안점을 두고 있음. 비교적 작은 회사인 기업 어플리케이션을 위한 보안이 필요한데, 이러한 환경은 직원 실명 확인 등이 가능하므로 아이디/패스워드, VPN, 인증서 등 전통적인(인터넷) 보안 기술이 채용되고 있음. 이러한 환경에서 P2P를 위한 신규 기술 개발은 저조한 상태임. (주)아라기술과 (주)소만사는 메신저를 통한 정보의 외부 유출을 막는 등의 기능을 제공하는 기업 메신저 보안 솔루션을 제공하고 있음
- 실명을 사용하지 않는 개방된 환경에서의 P2P 아키텍처를 위한 보안 기술은 ETRI를 중심으로 진행되었으며, 2005년부터 수행된 '유무선 IPv6 기반 P2P 네트워크 정보보호 기술개발' 과제가 대표적. 실명을 이용하지 않는 P2P의 경우 사용자 ID 조작을 토대로 한 많은 위협을 가할 수 있음. 대표적인 P2P 공격 유형 및 대응기술 목록을 아래와 같이 정리함

〈P2P 공격 유형 및 대응 기술〉

공격유형	대응기술
Whitewashing	– 영속성 있는(Persistent) 피어 ID 보장 – Strict Model(Central Trusted Authority) 활용 – Reputation Model을 통한 Cost vs. Penalty 기법 적용
ID Spoofing	– 접근 제어(Access Control) 기법 활용 – Packet Filtering을 통한 접근제어 – 취약점 서비스 사용의 제거 – 암호화 프로토콜 활용
MITM	– 상대 객체에 대한 안전한 인증 서비스 – 인증된 객체만이 패킷을 복호화 함 – 교환되는 메시지의 수정 여부 탐지 – 각 객체마다 Firewall, Anti-Virus 탑재 – 등록된 데이터의 위치 정보 오류 탐지
Privacy	– 공개키 기반 구조(PKI) – 분산 환경에 적합한 자치적 관리구조
Join	– 노드 ID 생성 시 IP 주소 또는 공개키 등 부가정보 이용 – Trust Authority(CA) 활용
Sybil	– 노드 ID 생성에 따른 과금 징수 – 노드 ID와 사용실체를 실검 증하는 방안
Message Routing	– 다중 해쉬(hash) 함수 사용하여 Key 분산복제 – (예: PKI 기반의 전자서명 활용)

- P2P 역기능은 불법적인 공유에 의한 지적재산권 침해가 대표적임. 2008년 현재 국내 P2P 파일공유 업체는 나우콤(피디박스 클럽박스), KTH(아이디스크), 소프트라인(토토디스크 토토팸), 미디어네트웍스(엠파

일), 한국유비쿼터스기술센터(엔디스크), 유즈인터렉티브(와와디스크), 아이서브(폴더플러스), 이지원(위디스크) 등이 대표적임. 구 정통부는 2007년 불법 · 유해정보 기술 · 관리적 차단 가이드라인을 발표한 바 있으나, 불법 공유를 근절하기 위한 기술개발은 부족한 상태

- 그밖에 역기능으로 P2P 트래픽 과다를 들 수 있음. P2P 트래픽은 2000대 중반부터 이미 전체 네트워크 트래픽의 50% 이상을 차지하고 있으며, 기업 네트워크에 다량의 트래픽을 유발하여 업무에 지장을 초래하기도 함. 이에 대해 (주)아라기술, (주)소만사, (주)라오넷 등이 패킷 필터링 기술에 기반한 P2P 트래픽을 수집 · 분석 · 차단 · 제어 솔루션을 제공하고 있음

– IPTV 보안

- IPTV(Internet Protocol Television)란 초고속인터넷망(NGN, BcN 및 IMS)을 이용하여 실시간 방송채널, 주문형 비디오(VOD) 및 TV Banking, T-commerce를 포함하는 양방향 데이터서비스 등을 단말기를 통하여 가입자에게 제공하는 대표적인 방송 · 통신 융합서비스임. 2007년 12월 국회에서 인터넷멀티미디어방송법의 통과로 법적인 근거가 마련되었고, 2008년에는 방송위원회와 舊 정보통신부를 통합한 방송통신위원회 조직이 구성되어 IPTV 산업의 활성화를 주도하고 있음
- IPTV 구조는 선택한 초고속망의 구조와 진화유형에 따라서 Non-NGN IPTV, NGN non-IMS IPTV 및 NGN-IMS IPTV 구조로 분류될 수 있음. Non-NGN IPTV 구조는 기존의 IPTV 망 구성요소와 프로토콜, 인터페이스를 기반으로 한 구조로서, 현재 일부 통신사업자들이 서비스하고 있는 Pre-IPTV 서비스 및 사업초창기의 Full-IPTV 서비스의 구조가 될 것임. NGN non-IMS IPTV 구조는 NGN 프레임워크 참조 구조의 구성요소를 이용하며 필요할 경우에 다른 NGN 서비스와 연동이 가능하고, NGN-IMS 기반의 IPTV 구조는 IMS 구성요소를 이용하며 필요할 경우에 다른 IMS 서비스와 연동이 가능함
- IPTV 보안은 기존의 유료방송시스템(CATV, 위성방송, 위성 DMB 등)의 연속으로 보는 시각이 강하며, 방송통신위원회는 산하기관인 전파연구소를 통하여 CATV 셋톱박스(STB)의 경우 수신제한(CAS) 모듈의 분리를 의무화하고 있는 것과 동일하게, IPTV 단말장치에서 가입자 시청제한 및 불법 복제방지를 위한 수신제한(CAS) 모듈을 분리 또는 교환이 가능하도록 규정하는 "인터넷멀티미디어 방송설비에 관한 기술기준"을 마련 중임. IPTV 가입자를 확인하고 과금할 수 있는 CAS 모듈을 휴대폰의 USIM처럼 STB에서 분리하여 가입자들이 특정사업자에 얽매이지 않고 원하는 디자인이나 기능을 보유한 STB를 자유롭게 구매해 사용할 수 있도록 하는 장점이 있음. 이러한 정책은 그동안 IT산업을 사업자 중심에서 이용자 중심으로 전환하고자 하는 정부의 의지와, 특정업체의 CAS기술에 종속되어가는 산업계의 우려가 함께 반영된 것으로 보임
- IPTV 미들웨어와 관련하여 한국전자통신연구원(ETRI)은 2006년부터 舊 정보통신부 및 국내 셋톱박스 제조업체들과 'ACAP 기반 IPTV용 미들웨어' 기술 개발을 추진하여 왔음. IPTV 미들웨어 분야의 국내 표준을 마련하기 위하여 지상파방송용으로 만들어진 ACAP(Advanced Common Application Platform)와 MHP(Multimedia Home Platform) 방식을 변환하여 IPTV 전용의 미들웨어 규격인 ACAP-J를 개발하

는데 목표를 두고 있음. 현재는 Java기반 및 HTML기반의 두 가지 표준문서가 별도로 존재하며, 향후 ITU-T IPTV-GSI의 요구사항을 만족하는 Browser 기반의 미들웨어의 표준화 작업을 위하여 TTA를 중심으로 각계의 전문가들이 함께 노력하고 있음

- 수신제한시스템(CAS)은 유료방송을 시청할 권한을 부여하거나 제한하는 시스템으로 기존의 위성방송과 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 횟수 제한 등의 기능을 제공함. 하나TV는 셀런 제품을 LG데이콤은 코어트러스트 제품을 채택했음
- 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 밸류캐스팅 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 했으며, 국내 5개 개발업체(LG CNS, 디지캡, LG전자, 엑스크립트, 코어트러스트)와 컨소시엄을 구성하여 "KCTA 2008 디지털케이블쇼"에서 D-CAS의 소개 및 시연을 하였음
- 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[3] 중 대표적이라고 할 수 있는 주스트(Joost)의 경우 이미 이러한 커뮤니티 서비스를 TV 채널과

3) 인터넷을 통한 동영상 스트림 서비스를 인터넷 TV와 IPTV로 구분지을 수 있는데, 인터넷TV는 인터넷 포털 형태의 VoD를 제공하는 서비스를 의미하고 IPTV는 NGN상에서 통신 사업자 중심의 서비스를 의미한다. 국내 인터넷TV의 예로 곰TV, 아프리카TV, 판도라TV 등을 들 수 있고 IPTV의 예로 하나로TV, 메가TV등이 있다.

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 · 부가서비스 및 커뮤니티 서비스에 적용하기 위한 추가 연구가 필요한 상황

- 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 진행되었음. 이에 반하여 국외 인터넷TV 분야의 연구 개발은 NGN을 기반으로 하기 보다는 응용 계층에서의 멀티캐스트를 대상으로 하는 경우가 대부분임. 이에 따라 최근에 ITU-T FG-IPTV에는 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

– 신뢰보안서비스(TPM: Trusted Computing Module)

- 신뢰보안 서비스(TPM)는 사용자의 중요한 정보 자산(데이터, 암호, 키, 서비스 등)이 외부의 소프트웨어 공격, 물리적인 공격 및 물리적인 도난 등 유해한 환경으로부터 보호될 수 있도록 하는 기술들을 의미함. 이 기술은 기존의 소프트웨어 기반 정보보호에서 나아가 하드웨어를 기반으로 하는 정보보호 기술을 요구하는 새로운 패러다임으로 각광받으며 활발히 연구 개발되고 있음
- 그 중 가장 대표적인 활동은 TCG(Trusted Computing Group)로 알려진 국제 산업 표준화 단체를 통해서임. TCG는 다양한 플랫폼, 주변 장치와 기기에 걸쳐 하드웨어 구성 요소와 소프트웨어 인터페이스를 포함하여 신뢰할 수 있는 하드웨어 지원 컴퓨팅 및 보안 기술에 대한 개방형 표준을 개발, 정의 및 촉진하기 위해 결성된 비영리 조직임. HP, IBM, MS 등 대형 IT 업체들이 주축으로 활동하고 있는 TCG는 시스템의 신뢰성을 지원하기 위해 하드웨어 보안 칩인 TPM(Trusted Platform Module)을 신뢰 기반으로 함. 이미 많은 PC와 노트북 등에 이를 위한 하드웨어 및 소프트웨어 기술들이 장착되어 출시되고 있으며 점점 더 많은 제품에서 TCG 규격을 수용하고 있는 추세. 이들이 추구하는 신뢰 컴퓨팅 기술이란 컴퓨터가 당초 의도된 대로 동작할 수 있도록 신뢰성을 부과하는 것으로서, 하드웨어 기반의 보안 칩(TPM)을 모든 기기들에 공통으로 적용하도록 하고 이를 위한 소프트웨어를 개방형 표준으로 제공하고자 하는 기술
- 국내에서도 차세대 단말 환경에서의 신뢰보안 요구가 증대되고 있음에 따라 기밀정보 유출, 위장, 불법 사용, 정상적인 서비스 방해, 프라이버시 방해 등을 방지하기 위한 정보보호 요소 기술의 개발의 필요성이 점점 높아지고 있는 상황임. 하지만, 현재 국내에서는 이러한 기술 개발에 대해 적극적인 대처는 하고 있지 않은 상황임

– 국내 기술 개발 현황을 요약하면 다음과 같음

- ETRI 정보보호연구본부에서는 2006년부터 TPM에 관한 연구 개발을 진행해 오고 있음. 이 중에서도 차

세대 모바일 단말기에서의 모바일 단말에 신뢰 보안 서비스를 적용하기 위한 핵심 모듈인 STPM(Secure and Trusted Platform Module)을 개발하고 있음

- 삼성전자는 TPM 에 대해서는 검토하는 단계이며, 오히려 자체적인 신뢰 컴퓨팅 기술 개발에 주력하고 있음. 삼성전자는 TCG 회원사이지만, TCG에 적극적인 활동은 거의 하지 않고 있음
- 이동통신 사업자의 경우는 하드웨어 기반의 신뢰 컴퓨팅 기술에 대해 관심을 가지고 있지만, 기술 개발보다는 자사 제품에 빨리 적용할 수 있는 상용 기술을 찾고 있는 상황임
- 전체적으로, 국내 산업계는 TPM에 대해서 아직 본격적인 움직임은 없는 상태이며, 국내외의 진행 상황, 특히 기술의 시장성이나 TCG의 표준화 추이를 지켜본 후 시장성과 표준이 어느 정도 성숙되었을 때 본격적으로 개발을 시작할 전망

– 차세대 웹 보안

- 초기의 웹 기술은 주로 비즈니스 분야에서 다양한 응용에 대한 통합의 도구로서 이용되어 왔으나, 현재는 유무선 통합 응용 서비스, 정보 가전, 홈네트워킹, 임베디드 환경 등 다양한 분야에서 핵심 연동 기술로 그 활용 범위가 빠르게 확산되고 있음
- 특히 최근 웹 2.0 기술 및 SOA(Service Oriented Architecture) 기반의 융합 서비스가 확산되고 있으며, 웹 기술이 다양한 디바이스에까지 적용되기 시작하면서 웹 기술을 기반으로 한 다양한 서비스 및 콘텐츠, 디바이스들의 융복합이 가속화 되고 다양한 사용자 참여형 서비스가 등장하는 등 웹 환경이 급속히 변화하고 있음
- 이러한 차세대 웹 기반 서비스에서는 서로 다른 도메인에 속하는 이질적인 서비스 간의 연동이 빈번하게 발생하는 등 기존의 웹 환경보다 더 많은 보안 취약점이 존재하며, 이를 해결할 수 있는 보안 표준 기술 개발이 요구되고 있음
- 차세대 웹 보안 기술은 다양한 서비스 및 디바이스들로 구성된 차세대 웹 기반 서비스에 대한 안전성을 보장해 줄 수 있고 이들 간의 안전한 서비스 연동을 제공해 줄 수 있는 정보보호 기술로, 웹 2.0 보안 기술, SOA 기반의 융합 서비스 보안 기술, 유비쿼터스 웹 보안 기술, 시맨틱 보안 기술, 모바일 웹 2.0 보안 기술 등을 포함함
- 웹 2.0 보안 기술은 다양한 서비스 및 리소스들이 다양한 형태로 결합되고 재창출되는 웹 2.0 서비스 환경에서의 보안 취약점을 해결하기 위한 정보보호 기술로, SOA 기반 융합서비스 보안 기술은 웹서비스(Web Services) 등의 SOA 기술을 기반으로 다양한 응용 서비스의 안전한 융합을 가능하게 해주는 정보보호 기술로 정의함
- 유비쿼터스 웹 보안 기술은 웹 기술이 적용된 다양한 디바이스 기반 서비스들이 안전하게 서로 연동되도록 해주는 정보보호 기술
- 시맨틱 보안 기술은 시맨틱 정보를 기반으로 보다 사용자 친화적이고 지능적인 보안 연동을 가능하게 해주는 정보보호 기술

- 모바일 웹 2.0 보안 기술은 웹 2.0 기술을 모바일 환경까지 적용한 모바일 웹 2.0 서비스의 안전성 보장을 위한 정보보호 기술
- 기존의 전자거래 등 비즈니스 영역에서의 웹서비스 정보보호 기술들은 기술 보급이 상당히 이루어지고 있는 단계이나, 향후 기술 수요가 증가하리라고 예상되는 차세대 웹 기반 서비스에 대한 안전성을 보장해 줄 수 있는 차세대 웹 보안 기술은 아직 기술 개발 초기 단계
- 비즈니스 응용을 위한 XML 정보보호 및 웹서비스 정보보호 기술 개발은 이미 국내에서도 많이 이루어지고 있으며, 웹 2.0 보안 기술은 기존의 웹 방화벽 제품 개발이 주를 이루고 있고 이외의 웹 2.0 보안 관련 기술 개발은 별로 이루어지지 않고 있음. 향후 웹 2.0 보안 기술에 대한 수요가 증가하리라고 예상되어 이에 대한 기술 개발이 시급하다고 판단됨. 시맨틱 보안, 모바일 웹 2.0 보안, 유비쿼터스 보안 관련 기술 개발은 아직 초기 단계로 파악되며 향후 이들 기술에 대한 개발도 필요하리라고 예상
- 최근 ITU-T SG17의 다음 회기에 대한 구조조정 작업이 진행되면서 기존 Q.9의 후속 Question인 Secure Application Services Question에서 SOA 기반 서비스를 비롯한 안전한 응용 서비스를 위한 보안 메커니즘, 웹 2.0 및 매쉬업 등의 웹 기반 융합서비스에 대한 보안 메커니즘이 향후 표준화 범위에 포함되었으며, 2008년 하반기에 차세대 웹기반 통신 서비스를 위한 보안 프레임워크에 대한 신규 표준화 항목이 Q.9에서 채택되어 표준 개발이 시작되었음. Q.9의 또다른 후속 Question인 Secure Ubiquitous Communication Services Question에서 유비쿼터스 환경에서의 웹 기술을 이용한 안전한 통신 및 인터워킹 메커니즘과 프로토콜 등을 향후 표준화 범위에 포함시켰고, 신규 Question인 SOA Question에서 SOA 기반 안전한 통신 및 정책 디스커버리, SOA 기술에 대한 보안 보증 메커니즘 및 보안 평가 기술 등을 향후 표준화 범위에 포함시켜 향후 국내에서도 이러한 기술 개발 방향을 반영한 차세대 웹 보안 기술 및 SOA 보안 기술 개발이 필요할 것으로 보임
- 차세대 웹 보안과 관련된 국내 기술 개발 현황은 다음과 같음
- 웹서비스(Web Services) 및 SOA 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 기술을 개발하여 2007년 ITU-T SG17을 통해 표준화를 완료하였음(ITU-T X.1143)
- ETRI에서는 웹 2.0 보안 기술, 유비쿼터스 웹 보안 기술 등 차세대 웹 보안 관련 기술 국제 표준화를 추진하고 있으며, 2008년 상반기에 ITU-T SG17에서 차세대 웹서비스 보안 표준화 로드맵을 수립하였고 2008년 하반기부터 차세대 웹기반 융합서비스 보안에 대한 국제 표준(ITU-T X.websec-4)을 개발하고 있음
- KISA에서는 KT와 함께 웹 사용자의 프라이버시 보호를 위한 P3P(Platform for Privacy Preferences) 소프트웨어를 개발한 바 있음

- 웹서비스(Web Services) 보안과 관련하여 이니텍, 비씨큐어, STI Security 등에서 XML 전자서명 및 XML 암호 기술을 구현한 제품을 출시한 바 있음
- 웹 2.0 보안과 관련된 개발은 주로 웹 애플리케이션 취약점 분석툴 및 웹 방화벽 개발 쪽에 집중되어 있으며, 펜타시큐리티, 듀얼 시큐리티 등에서 웹 방화벽 제품을 개발하였음. 이외의 다른 웹 2.0 보안 관련 기술들은 아직 개발이 시작되지 않았지만, 국내 웹 2.0 서비스 확산 속도를 볼 때 곧 수요가 급속히 증가하리라고 예상됨
- 모바일 환경을 위한 웹 2.0 보안 제품 국내 개발 사례는 아직 드문 실정이며, 또한 유비쿼터스 웹 환경을 위한 보안 제품 개발도 드묾
- KT, K4M 등에서 시맨틱 웹 상용 기술을 개발하고 있으나 아직 이를 위한 보안 기술 개발이나 시맨틱 기반의 정보보호 기술 개발은 이루어지지 않고 있음

– Lawful Interception

- Lawful Interception과 관련하여 국내 기술 개발 현황은 ETRI BcN 사업단에서 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 ETRI 외에 공적인 목적으로 국정원이 유선중계통신망 감청장비를 도입하여 보유하다가 폐기하였고, 1998 및 1999년 자체 개발 장비를 통해 이동망 감청에 활용한 것으로 보고된 바 있음
- 2007년 6월 통신비밀보호법 개정안이 국회 법제사법위원회를 통과된 상태임. 그 주요 내용은 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 국회 본회의에 통과될 경우 기지국 이동교환기에 감청설비를 설치해 특정번호를 입력, 이 번호로 송수신되는 모든 통화내역을 녹음하는 방식으로 수행되는 별도의 소프트웨어나 카드가 개발될 것으로 예상됨
- 한편 통신비밀보호법 개정안의 확대로 기존 유선망뿐만 아니라 휴대전화 및 인터넷을 포함한 모든 통신서비스에 감청이 가능해지면 인터넷 망을 통하는 음성통화의 경우 인터넷에서의 보안문제가 그대로 적용되는 문제점이 있어 보안 서비스 적용이 보편화 될 것임. 하지만 감청이 도입될 경우 감청기관의 암호화된 통신 내용 복호화를 위한 키 관리기능이 요구되어 이에 대한 연구가 병행되어야 할 것으로 예상됨
- 지금까지는 도청 및 감청에 대한 법적 소고 및 인문사회학적 의미에서의 도청의 법적 규제에 관한 고찰과 같은 작업이 주로 이루어졌음. 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

○ 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 마련하였음. 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 확대하였음

〈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

- 2002년 CC를 도입하면서, 업체의 평가제출물 작성 지원을 위하여 보호프로파일 및 보안목표명세서 작성 가이드(ISO 15446)에 기반한 제품별 세부 평가기준인 보호프로파일(PP: Protection Profile)을 개발하여 공고하고 있음. 현재 국내에서는 CC 버전 2.3과 버전 3.1 모두 사용하고 있는데, 한국의 인증기관 역할을 담당하고 있는 국가정보원 IT보안인증사무국(http://www.kecs.go.kr)에 등재된 PP는, 2008년 7월 15일 기준으로 총 24개가 있음. 이 중 침입차단시스템 등 8종의 보호프로파일은 기존의 CC 버전 2.3 기반의 PP를 등급 조정과 함께 CC 버전 3.1로 전환하여 개발되음. 무선랜 및 통합보안관리 PP도 3.1로 전환 중이며, 웹 응용프로그램 침입차단시스템 및 전자문서 유출방지시스템 PP도 3.1로 개발 중으로 2008년 하반기에 모두 완료될 예정임

〈보호프로파일 현황('08. 7. 15 기준)〉

보호프로파일명	최종 등재일	등급
(CC v3.1) 네트워크 침입방지시스템 보호프로파일 V2.0	2008. 04	EAL3
(CC v3.1) 네트워크 스팸메일차단시스템 보호프로파일 V2.0	2008. 04	EAL2
(CC v3.1) 지문인식시스템 보호프로파일V2.0	2008. 04	EAL2
(CC v3.1) 개방형 스마트카드 플랫폼 보호프로파일 V2.0	2008. 04	EAL4+
(CC v3.1) 등급기반 접근통제시스템 보호프로파일 V2.0	2008. 04	EAL3
(CC v3.1) 가상사설망 보호프로파일 V2.0	2008. 04	EAL3
(CC v3.1) 침입탐지시스템 보호프로파일 V2.0	2008. 04	EAL3
(CC v3.1) 침입차단시스템 보호프로파일 V2.0	2008. 04	EAL4
(CC v3.1) 보안토큰 보호프로파일 V1.0	2008. 01	EAL4
(CC v2.3) 전자여권 보호프로파일 V1.0	2008. 01	EAL4+
(CC v2.3) 무선랜 인증시스템 보호프로파일 V1.0	2008. 01	EAL4
(CC v2.3) 통합 보안관리시스템 보호프로파일 V1.0	2007. 01	EAL3
(CC v2.3) 안티 바이러스 소프트웨어 보호프로파일 V1.0	2007. 01	EAL3
(CC v2.3) 네트워크 스팸메일차단시스템 보호프로파일 V1.0	2007. 01	EAL3
(CC v2.3) 국가기관용 가상사설망 보호프로파일 V1.2	2006. 05	EAL3+
(CC v2.3) 국가기관용 침입탐지시스템 보호프로파일 V1.2	2006. 05	EAL3+
(CC v2.3) 국가기관용 등급기반 접근통제시스템 보호프로파일 V1.1	2006. 05	EAL3+
(CC v2.3) 국가기관용 침입차단시스템 보호프로파일 V1.2	2006. 05	EAL3+
(CC v2.3) 국가기관용 지문인식시스템 보호프로파일 V1.1	2006. 05	EAL2+
(CC v2.3) 국가기관용 개방형 스마트카드 플랫폼 보호프로파일 V1.1	2006. 05	EAL4+
(CC v2.3) 국가기관용 침입차단시스템 · 가상사설망 통합 보호프로파일 V1.1	2006. 05	EAL2
(CC v2.3) 역할기반 접근통제시스템 보호프로파일 V1.0	2006. 03	EAL4
(CC v2.3) 네트워크 침입방지시스템 보호프로파일 V1.1	2005. 12	EAL4
(CC v2.1) 국가기관용 게이트웨이형 가상사설망 보호프로파일 V1.1	2003. 04	EAL3+

- 평가제도를 운영하기 시작한 이래 현재 연 25개 이상의 제품 및 보호프로파일을 평가하고 있으며 2008년 7월 15일 기준으로, 185개를 평가하였음. 또한 우리나라에서 평가한 결과가 해외에서도 인정받을 수 있도록 2004년 9월 국제 공통평가기준 상호인정협정 가입 신청서를 제출하였으며 20개월만인 2006년 5월 9일 11번째 인증서발행국으로 가입. 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 높아짐. 더불어 국내 업체가 해외에서 평가받기 위한 수수료 및 제출물의 번역 등 예산을 절감할 수 있으며 업체의 기술을 해외 유출로부터 보호할 수 있음

〈국내 평가완료 현황('08. 7. 15 기준)〉

구 분	2004	2005	2006	2007	2008	합계
침입차단시스템	7	2	0	4	0	13
침입탐지시스템	2	6	6	4	1	19
통합제품	11	3	4	4	3	25
운영체제보안시스템	0	10	5	2	2	19
침입방지시스템	0	2	3	11	1	17
기타 정보보호제품	0	2	2	4	9	17
보호프로파일	0	1	5	1	9	16
합계	20	26	25	30	25	126

※ 통합제품: "침입차단시스템+가상사설망", "침입차단시스템+가상사설망+침입탐지시스템", "침입차단시스템+침입탐지시스템", "침입차단시스템+가상사설망+침입방지시스템" 등 2개 이상 제품이 통합된 제품

※ 기타 정보보호제품: 가상사설망, 지문인식, 스마트카드, 통합보안관리, 웹 보안, 안티바이러스, 자료유출방지, DB 보안 등

- 2006년 1월 우리나라는 국가/공공기관에 납품되는 모든 정보보호제품에 대한 평가를 강제화함에 따라, 평가신청이 급증하여 평가대기기간이 장기화되는 문제가 발생하였음. 이를 해결하기 위하여 2007년 8월 한국기술시험원과 한국시스템보증 2개 회사가 평가기관으로 승인되어, 우리나라는 현재 한국정보보호진흥원을 포함한 총 3개의 정보보호제품 평가기관을 보유하게 됨
- 또, 한편으로 단일사 유사한 제품을 1건으로 평가하는 일괄 평가제도를 도입하여 시행하였고, 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 방안
- 2008년에는 3개의 평가기관에서 인력 추가 확보 및 집중 교육을 통하여 2008년 말에는 평가대기기간 장기화 문제가 어느 정도 해소될 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 인증 제도를 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 이슈는 기존 정보보호 패러다임이 정보보호관리 관점에서 정보보호 거버넌스로 변화되고 있는 추세이므로 이에 따른 체계적인 정보보호 거버넌스 연구가 필요하나, 국내의 선행 연구 등의 노력이 부족한 실정임

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

- 응용보안
  - 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 것으로, 방송콘텐츠 보호에 사용되던 CAS 역시 기존의 HW(케이블 카드 및 셋탑) 중심에서 SW 형태로 다운로드하여 단말 트러스트를 제공하는 지식 보안 기술이 미국의 오픈케이블랩 중심으로 개발 중. 그리고 MS를 중심으로 새로운 DRM 기술로 연계되는 기기에서의 OsMu 활용 기술 등 기존의 독립적인 콘텐츠의 활용에서 다양한 확장성 및 연동성 확보를 위한 노력이 진행 중에 있으며, 미쓰비스와 NHK는 디지털 영화의 불법 복제 및 유통 방지를 위한 전자 워터마크 기술의 공동 개발하는 등 저작권 관리 및 콘텐츠에 대한 관리 정보 운용 방안과 유통 관리를 수행하기 위한 연구를 진행하고 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/RTCP에 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 종단 간 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
  · 일부 외국사업자들이 표준을 준용하지 않고 자체 암호통신 기술을 적용함으로써 해당 사업자 간의 통화 시에만 보안 통화를 제공하는 문제점을 나타내고 있음
  · 최근 해외에서 접속설정프로토콜(SIP) 기반 응용서비스에 대한 침입방지시스템이 출시된 사례가 있으며, 이 사례에서 알 수 있듯이 VoIP 응용 프로토콜을 악용하는 사이버 공격을 탐지하고 대응할 수 있는 VoIP서비스에 특화된 정보보호 제품도 필요하게 될 것으로 보임

– 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

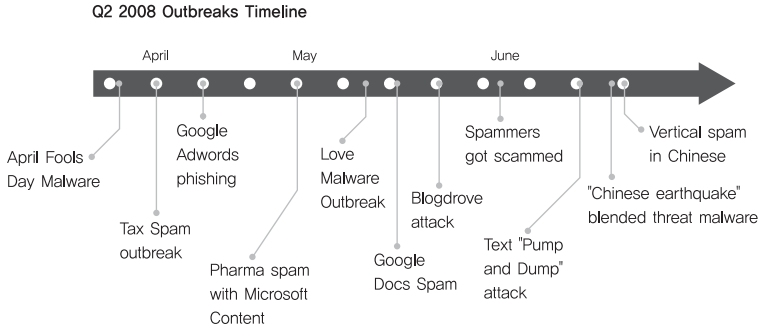
– VoIP 보안 세션제어 기술 및 사용자 프라이버시 보호 기술

- 국외 SBC 기술은, 다양한 환경을 경유하는 과정에서 세션을 제어하여 원활하게 서비스가 제공되도록 프로토콜 및 프로파일간의 연동(SIP/H.323/MGCP[4] 등 VoIP 프로토콜 간 호환성, IPv4/IPv6 연동 등) 및 QoS 보장을 위한 트래픽 모니터링/Traffic shaping/Call admission control, NAT/FW[5] 통과문제 해결을 위한 B2BUA/B2BGK/B2BGW[6], 사용자 인증 등의 기능을 제공함
- 현재 SBC 장비는 standalone 형태로 제공되고 있으며 일부 SBC 업체는 IMS[7] 장비 업체와 제휴를 통해 IMS 기능과 연계하여 동작하는 SBC를 제공하고 있으며, 향후 세계적인 주요업체의 IMS 장비, FW 장비, MPLS[8] 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 콘텐츠와 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

4) Media Gateway Control Protocol
5) Firewall
6) Back to Back User Agent/Back-to-Back Gatekeeper/Back-toBack Gateway
7) IP Multimedia Subsystem
8) Multi-Protocol Label Switching

– 스팸대책

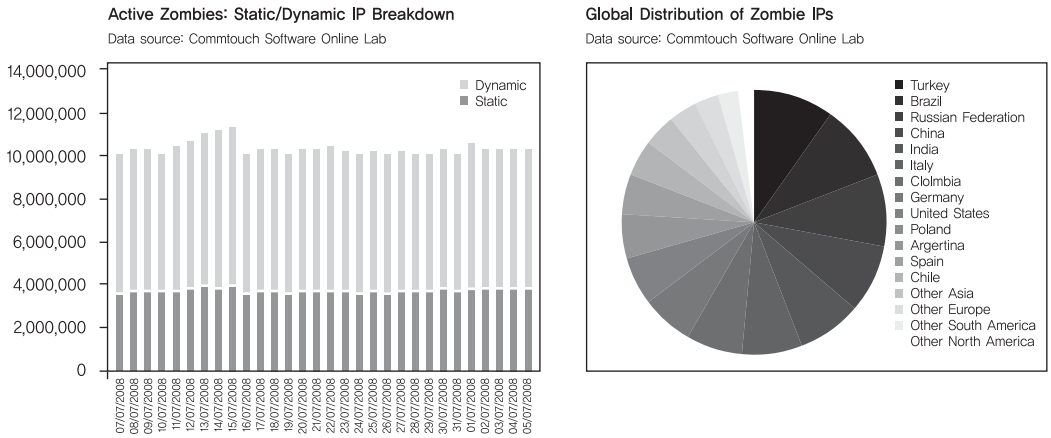
• 2006년 말 이후 PDF 스팸을 통해 예상외의 저조한 공격성과를 보이자, 스패머들은 전통적인 플레인 텍스트나 HTML 포맷 메시지를 이용한 공격성향을 보이고 있는데, 큰 사회적 반향 또는 개인적 관심을 불러일으킬만한 제목이나 내용(의약 46%, 성인물 22%, 복제 21%)을 이메일, 블로그, Google Docs 등에 기재하여 특정 파일의 실행 또는 사이트로의 접속을 유도하고 있음. 아래 그림은 2008년도 2분기의 주요 이메일 스팸의 유형을 제공함



〈Spam 발생 유형 정리〉

(Source: Commtouch Lab)

• 특히, 스팸을 통해 악성 웹 사이트로의 사용자 접속을 유도하는 공격이 성행하고 있는데, 이와 공격의 많은 부분이 접속 PC를 좀비(Zombie)로 만들기 위한 목적을 갖고 있음. 즉, 수백에서 수백만 대에 이르는 좀비 PC를 Botnet으로 연결하고 공격자는 이를 통해 경제적 수익을 창출할 수 있는 구조가 이미 현실화되었기 때문임. Commtouch Lab의 "2008년 2분기 Email 보안 위협 트렌드 보고서"에 따르면 전 세계 이메일 스팸은 평균적으로 77% 추이를 보이고 있으며, 최소 64%에서 최대 94%에 이르는 실정으로 분석됨. 또한 일평균 1,000만 개의 좀비 IP 주소가 활성화 되어있으며 이러한 IP 주소는 거의 대부분이 ISPs의 소유 주소로 알려져 있음. 또한 Static IP 주소와 Dynamic IP 주소의 활성화 비율은 35%:65% ~ 30%:70%의 수준으로 조사되었음. 국가별 좀비 발생 순위는 터키, 브라질, 러시아 순이었으며, 미국은 9위를 차지하는 것으로 밝혀졌음



〈Zombie PC IP 주소 통계〉

(Source: Commtouch Lab)

- IBM Research는 IBM Lotus와 함께 IETF 활동을 통해 Anti-Spam 공개 표준화를 위한 노력을 기울이고 있으며, Spam Filtering 기술 개발을 위해 IBM Internet Security Systems 자회사를 운용하여 고객 요구에 대응하는 신속한 지원 체계를 갖추고 있음. 또한 대단위 이메일 관리를 위해 GECS(Global E-Mail Cleansing Service) 및 EPAL(Enterprise Privacy and Authorization Language)와 같은 연구 프로젝트를 진행한 바 있으며, EPAL의 경우 이미 2003년에 W3C로 관련 문건이 제출된 바 있음. 특히 SpamGuru라는 Anti-Spam Filter 테스트베드를 이용하여 기존의 다양한 Filtering 알고리즘을 적용시키고 있는데, 그 주요한 기술로는 "JClassifier, Chung-Kwei, Plagiarism Dectection, Spoof Detection, Intelligent Rendering, Classifier Aggregation" 등이 알려져 있음. 본 기술은 인공지능적 메일 필터의 근간을 이루고 있으며, IBM의 차세대 메시징 & 협업 프레임워크인 Lotus Worksplace 2.0에 탑재되어 있음. MessageLabs, Symantec, Proofpoint, Secure Computing 등의 주요 Anti-Spam 보안 기업은 웹, 이메일, 인스턴트 메시지 서비스를 스팸, 바이러스, 웜 등으로부터 보호하기 위해 "메시지 통합 보안 솔루션" 제공하고 있는 추세. 또한 스팸 차단을 위한 전용 솔루션의 개발보다는 콘텐츠 사용과 관련된 Inbound/Outbound 트래픽을 통제/관리할 수 있는 전용 게이트웨이에 다양한 보안 솔루션을 구현하는 방향으로 관련 보안 기업의 움직임이 포착되고 있음. 학계에서는 스팸과 관련한 다양한 학술행사가 2001년도 SpamCon 2001을 시작으로 국제학술회의, 세션, 워크숍, 심포지엄 등의 형태로 꾸준히 개최되고 있음. 대표적으로 "Spam Conference, Inbox/Outbox, EU Spam Symposium, Usenix LISA, INBOX, Spam Conference, APCAUCE Meeting, Messaging Anti-Abuse General Meeting" 등이 지속적인 활동을 보이고 있음. 특히 MIT 스팸 컨퍼런스 2008에 제출된 관련 논문연구 주제로 Zombile Botnets이 단연 강세를 보이고 있으며, Multilayer Filtering, Blacklisting, SMTP Session Abort, Image Spam 등와 같은 전통적인 Anti-Spam 분야의 연구 노력도 지속적으로 이뤄지고 있는 것으로 판단됨

• 국외의 경우 다양한 Anti-Spam 단체들이 활동 중에 있는데, 이들 중 일부는 원치 않는 상업용 이메일에 대한 법적 규제를 목적으로 논의하고 있으며, 또 다른 단체들은 최근 산업체들이 겪고 있는 스팸 홍수에 대한 경험을 바탕으로 스팸 차단/방지를 위한 회의 및 논의를 진행하고 있음. 이를 정리하면 아래 표와 같음

〈Anti-Spam Organizations〉

대분류	기술 개발 현황	URL
국제단체	StopSpamAlliance	http://stopspamalliance.org/
	OECD Task Force on Spam	http://www.oecd-antispam.org/
	London Action Plan	http://www.londonactionplan.org/
	CAUCE(Coalition Against Unsolicited Commercial Email)	http://www.cauce.org/
ISP Industry	IRTF Anti-Spam Research Group(ASRG)	http://www.irtf.org/charter.php?gtype=rg&group=asrg
	RIPE Anti-Spam WG	http://www.ripe.net/ripe/wg/anti-spam/
	ITU Activities on Countering Spam	http://www.itu.int/osg/spu/spam/
	ISIPP	http://www.isipp.com/
	IIA Spam Virtual Taskforce	http://www.iia.net.au/index.php?option=com_content&task=section&id=4&Itemid=35
	Anti-Spam Technical Alliance	http://postmaster.info.aol.com/asta/
	Anti-Spam Projects: Information and Resources	http://www.oecd-antispam.org/article.php3?id_article=191
Email Industry	EEMA	http://www.eema.org/
	Email Service Provider Coalition	http://www.espcoalition.org/
	Messaging Anti-Abuse Working Group	http://www.maawg.org/home
	The Open Group Messaging Forum	http://archive.opengroup.org/messaging/spam/

– 안전한 P2P 보안

• 미국의 Microsoft가 2001년부터 가용성, 신뢰성이 뛰어난 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 컴퓨터 간 연결 및 검색이 자유로운 P2P 기술을 탑재, 오피스 제품군에 그루브(Groove) 추가 등 P2P 응용의 범위를 넓혀가고 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. JXTA 라이브러리는 2008년 현재 J2SE, C/C++, J2ME 등 다양한 버전이 완성되었거나 개발 중에 있음

• 이 외에도 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 제공하고 있음

- Skype는 P2P 기반의 VoIP 솔루션을 제공하면서 보안을 위해 X.509 인증서 기반의 사용자 인증 기술을 이용하고 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

- IPTV 서비스는 OECD 가입국 대부분에서 제공되고 있으며, 전 세계적으로 211개 사업자(북미 136개, 유럽 45개, 아시아 21개 등)가 IPTV서비스를 상용화했거나 준비 중에 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 FG-IPTV의 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 않고 있음
- 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 필요
- NGN 보안과 부가서비스 보안은 국내와 마찬가지로 기존의 네트워크 또는 서비스 보안 기술의 연속으로 보는 시각이 강하며, IPTV를 대상으로 한 구체적인 연구는 진행되지 않았음. 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(유니

캐스트)와 실시간 방송(멀티캐스트)을 동시에 제공하는 다채널 서비스의 특성[9]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. 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 셋톱박스)이 이러한 중간자의 역할을 할 수 있도록 다이내믹 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 필요

- 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, Rovirai 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 마이크로소프트를 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. 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 제공 시 보안 취약성 분석이 요구됨. 이와 별도로 IPTV 양방향 또는 부가서비스 제공 시 서비스 간 보안 기술 필요하며, 이러한 보안 기능을 제공할 때 QoS와 QoE를 우선 보장하면서 안전한 IPTV 서비스망의 구축이 용이해야 함

9) 최근IPTV와 같이 VoD와 실시간 방송서비스를 다채널로 지원하는 서비스에서 다수의 시청자가 채널을 선택하는 특성을 연구한 결과에 따르면 거듭제곱법칙(Power Law)의 특성을 보인다는 결과가 나오고 있음. 이것은 매우 적은 수이 인기있는 채널과 매우 많은 수의 비인기 채널이 동시에 공종한다는 것으로 몇몇채널을 멀티캐스트로 제공함과 동시에 대부분의 채널들을 유니캐스트로 제공해야 함으로 NGN상에서 멀티캐스트를 이용한다 하더라도 네트워크 및 서버의 부담은 크게 줄지 않는다는 것임.(참고: Nishith Sinha and R뮤 Oz "The Statistics of Switched Broadcast," in Proc. of SCTE Conference on Emerging Technologies, Huntington Beach, CA, January 2005)

– 신뢰보안서비스(TPM)

- TPM 기술에 대해 국제적으로는 TCG를 중심으로 신뢰 컴퓨팅에 관한 표준화와 기술 개발이 동시에 활발히 이루어지고 있음
- TCG TPM 표준 spec을 ISO/PAS의 Public 표준 스펙으로 금년 1월 제안하여 ISO SC27의 과제 승인을 받았고 현재 ISO format으로 별도로 변환을 진행하고 있음. 이는 TCG 표준이 ISO의 공개 표준으로 되어 널리 적용토록 하는 의미이며 TCG 집행부에서 진행
- TCG는 TPM 칩을 신뢰성 제공의 기반으로 정의하고 있음. 인피니온사가 만든 TPM 칩은 이미 PC나 노트북 등 많은 상용화 단말에 내장되어 있음
- 인텔사는 TCG에서 TPM 규격화 작업에 핵심 에디터로 참여하고 있을 뿐만 아니라 TXT(Trusted Execution Technology) 프로젝트를 통하여 신뢰 컴퓨팅 기술 개발 연구를 활발히 진행하고 있음. ARM사는 TPM이라는 별도의 하드웨어 보안 칩이 아니라 메인 프로세스 안에 보안 기능을 탑재하는 방법을 채용함. 이미 상용화된 Trust Zone이라는 기술을 사용하여 메인 프로세스를 normal mode와 secure mode 등 2중 모드로 분리하여 정보를 보호하는 방법을 사용하고 있음. 그러나 별도의 칩을 사용하는 방법보다는 보안에 취약할 수밖에 없음
- 중국은 Huawei Technologies 사 등을 중심으로 TCG의 표준화 상황을 주시하면서 자체적인 기술 개발에 주력하고 있음. 중국은 국가의 지원 하에 TC260이라는 표준화 그룹을 만들어 TCM(Trusted Computing Module)이라고 명명된 TPM과 같은 칩을 개발하고 있음. 국가 정책 차원에서 TCG의 TPM은 중국 국민이 사용할 장비에는 탑재시키지 못하도록 하고 대신 TCM을 장착하여 신뢰 컴퓨팅 기술을 확산시키는 방향으로 유도하고 있음
- 독일의 경우, 전 세계 스마트카드 시장의 75% 이상, 반도체 시장의 50% 이상이 독일에서 만들어지고 있고 국내의 인터넷 사용자 수도 기하급수적으로 증가하고 있는 점을 고려하여 정부도 신뢰보안서비스 기술에 많은 관심을 가지고 있고 TCG와도 긴밀한 협력 관계를 유지하고 있으며 기술 개발 활동에 많은 지원을 아끼지 않고 있음. Open TC(Trusted Computing)라는 그룹에서는 TCG의 규격들을 기반으로 다양한 소프트웨어 기술들을 실험하고 있음. 이 그룹을 실제적으로 이끌고 있는 것은 HP인데, HP는 TCG에서도 TC로 활동하고 있고 Bochum 대학과 업체들을 Tests suite나 TSS 개발 용역을 통하여 끌어들임으로써 발빠르게 움직이고 있음
- 일본은 후지쯔, 히타치, 파나소닉 사 등 많은 업체들이 TCG 활동에 적극적임. 2008년 2월에는 JRF(Japan Regional Forum)라는 조직을 만들어서 TCG의 규격들을 연구하고 이들을 사용해 시장을 만들 수 있도록 다양한 응용을 개발함으로써 일본 내 신뢰 컴퓨팅 기술을 확산시키기 위해 노력하고 있음. 그들은 일본과는 달리 TCG에 적극 동조하여 기술을 빨리 서비스에 적용함으로써 이 기술 분야에서도 주도권을 잡기 위해 노력함. 후지쯔는 노트북에 인피니온사에서 만든 TPM을 장착하여 출시하고 있고, 파나소닉의 경우 소프트웨어적인 MTM 기능 구현에 주력을 하고 있음

- 미국의 경우, IBM, Intel, Motorola, MS, Juniper 등 많은 대형 단말업체가 TCG에 활발히 활동하고 있음. 특히 Intel의 경우는 TCG 내에서 TPM 규격 작업에 적극적으로 동참하는 동시에 TXT 프로젝트를 통하여 신뢰 컴퓨팅 관련 자체 기술 개발에 주력하고 있음. Remote attestation 관련 기술을 개발하는 것이 이 프로젝트의 주요 목적임. MS는 Windows Vista에 신뢰보안 기술을 탑재하여 출시하고 있으며 IBM 등 노트북에도 TPM 칩이 장착되어 출시되고 있음
- 이 외에도 Nokia, Vodafone 등의 모바일 단말업체나 프랑스 텔레콤 등 이동통신 사업자, Freescale과 같은 반도체 회사들도 TCG 활동에 매우 적극적으로 참여하고 있고 참여 업체 수는 점점 늘어나고 있는 추세
- 무선 통신 기술 및 장비의 발달로 모바일 장비의 보급이 더욱 증가하면 향후 이를 겨냥한 많은 서비스 시장이 창출될 것으로 판단되며 이에 관련한 보안 문제는 TPM로 해결될 수 있을 것으로 판단됨. 그 결과 TPM의 탑재 범위는 더욱 광범위해질 것으로 예측됨
- TPM 기술(TCG 표준 준수)을 탑재한 제품을 출시하고 있는 회사가 10개 이상 되고 150여 개 회사가 TCG 표준화 그룹 활동을 통하여 표준화 작업에 참여 중임. 이 중 칩 제조사는 Atmel 등 4개 사, 보안 제품에 적용 중인 회사는 Verisign 외 10여 개 회사 등이 있고, 노트북과 PC에도 관련 기술이 탑재되어 있음. 이 외에도 TCG 활동과 병행하여 자체적인 TPM 솔루션을 만드는 업체들도 점차 증가하고 있음. 중국의 화웨이, ARM사가 대표적임

〈TPM 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

- 비즈니스 응용을 위한 XML 정보보호 및 웹서비스 정보보호 기술 개발은 이미 많이 이루어져 상용화 수준이며, 웹 2.0 보안 기술은 기존의 웹 방화벽 제품 개발이 주를 이루고 있고 이밖의 웹 2.0 보안 관련 기술 개발은 아직 활발하게 이루어지지는 않고 있으며 매쉬업 보안 기술 등에 대한 연구가 진행되고 있음. SOA 및 웹 2.0 기반의 융합서비스 개발이 활발히 이루어지기 시작하여 이를 위한 보안 기술에 대한 수요가 발생하리라고 전망됨. 시맨틱 보안, 모바일 웹 2.0 보안, 유비쿼터스 보안 관련 기술 개발은 국외에서도 아직 초기 단계로 파악되며 향후 이들 기술에 대한 개발도 필요하리라고 예상됨

- ITU-T SG17에서 2008년 하반기부터 차세대 웹기반 융합서비스 보안에 대한 국제 표준(ITU-T X.websec-4) 개발이 시작되었으며, 2009년부터 SOA 기반 서비스를 위한 보안 메커니즘, 유비쿼터스 환경에서의 웹기반 안전한 통신 및 인터워킹 메커니즘과 프로토콜, 안전한 통신 및 정책 디스커버리, SOA 기술에 대한 보안 보증 메커니즘 및 보안 평가 기술 등에 대한 표준화가 활발하게 진행될 전망으로, 이와 관련된 기술 개발이 많이 이루어지리라고 예상됨
- 차세대 웹 보안과 관련된 국외 기술 개발 현황은 다음과 같음
- 웹서비스(Web Services) 및 SOA 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 제공함
- 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
- 웹서비스(Web Services) 및 SOA 보안과 관련하여 IBM의 WebSphere DataPower XS40 XML Security Gateway는 XML/SOAP Filtering, Field Level XML 보안, SAML, XACML, WS-Security 기술을 통한 접근제어 기능 등을 제공
- 웹 2.0 보안 기술은 웹 애플리케이션 취약점 분석툴 및 웹 방화벽 개발이 주로 이루어지고 있으며, 넷컨티넘, 임퍼바 등에서 웹방화벽을 개발하였으며, STG Security에서 웹 애플리케이션 취약성 분석 툴 및 웹 애플리케이션 파이어월을 개발하였으며, TEROS, 체크포인트 등에서 웹 애플리케이션 보안게이트웨이를 개발하였음
- Layer 7의 XML Data Screen은 SOAP, REST, AJAX 등의 XML 메시지 형태를 갖는 유해하거나 인가받지 않은 메시지를 필터링 할 수 있음. 오픈 소스 기반의 웹 방화벽으로 Apache의 ModSecurity 2.5가 있으며, 애플리케이션 레벨의 방화벽으로 유해한 메시지를 필터링 할 수 있음
- 오픈 소스 기반의 웹 취약성 분석툴로는 OWASP에서 프로젝트를 진행하고 있는 Sprajax가 있으며, Ajax 기반의 웹 어플리케이션에 대한 보안 취약점을 점검할 수 있음
- 클라이언트에서의 매쉬업 보안을 위해 IBM에서 SMash 라는 기술을 개발하였음
- Nokia에서는 모바일 환경에서 XML 및 SOAP을 지원하고 기본적인 보안 기능 및 Liberty Alliance의 ID 관리 기술을 구현한 Nokia Web Services Framework를 개발하였음. 또한 iPhone과 Nokia N810에 Ajax가 구현되어 탑재되기 시작하였음
- 유비쿼터스 웹 기술과 관련하여, MS는 웹서비스 기반의 디바이스 간의 연동을 위해 'Devices Profile for Web Services' 명세를 개발하고 이를 기반으로 한 제품을 개발하였음
- UPnP 포럼에서는 디바이스 간 연동시의 보안을 위해 XML 기반의 보안 스펙을 개발하였음

- MIT CSAIL과 Nokia Research Center Cambridge는 공동으로 SwapMe라는 프로젝트를 추진 중이며, Mobile Ecosystem을 위한 시맨틱 웹 애플리케이션 플랫폼을 개발하고 있음
- 유럽의 ITEA(Information Technology European Advancement)가 SODA(Service Oriented Device and Delivery Architecture) 프로젝트를 통해 디바이스 간의 연동을 용이하게 해주는 도구를 개발 중
- 지능형 보안 기술은 주로 비정상 행위 탐지(anomaly detection)를 위한 침입탐지 시스템 및 대응 기술에 적용되고 있음
- 시맨틱 보안에 대한 연구는 주로 학계에서 수행되고 있으며, 지능형 보안정책을 위해 KAoS, Rei, Ponder 등의 정책 표현 및 추론 언어가 연구되고 있음
- 국내외적으로 Myspace, Facebook, SecondLife, Cyworld 등 100여 개 Social Networking Site에 수백만 명의 회원이 있는 실정이나, IDS, IPS 등의 기존 네트워크 보안 장비를 이용하는 수준이며 Social Networking Site를 위한 보안 기술은 아직 개발 초기 단계
- Parlay에 의해 유무선 통신망에 대한 웹서비스 API인 Parlay X가 표준화되고 있으며, Parlay-X 게이트웨이가 개발되고 있음
- BT에서는 Web21C SDK라고 불리는 웹 2.0기반의 API를 개발하였으며, 개발자는 이 API를 이용해 통신사업자 네트워크를 손쉽게 제어할 수 있음

〈웹 보안 제품 업체 현황〉

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	웹 애플리케이션 취약성 분석, 웹 애플리케이션 파이어월
TEROS	웹 애플리케이션 보안 게이트웨이
체크포인트 Connectra	웹 보안 게이트웨이
Layer 7 XML Data Screen	유해 XML 메시지 필터링
OWASP Sprajax	웹 취약점 점검

– Lawful Interception

- 합법적인 감청에 대한 법제화는 국내보다 일찍이 외국에서부터 시행되었거나 준비단계에 있으며 연구 및 표준화 또한 국내에 비하여 앞선 상태로 파악됨. 다음은 유럽 및 북미 각국에서의 법제화 현황
- 미국에서는 다양한 통신환경에서의 효과적인 감청을 위하여 1994년 10월 통신사업자에게 감청수행을 위한 기능구비 의무를 부과하는 것을 주요 골자로 하는 CALEA(Communications Assistance for Law Enforcement Act)를 제정하였음. CALEA에서는 전기통신사업자로 하여금 전기통신사업제로 하여금 전기통신의 감청을 수행하기 위한 능력을 갖추도록 규정하고 있는데 여기에서 전기통신 사업자란 PSTN기반 유선전화 서비스 제공업자 뿐만 아닌 PCS 서비스, 셀룰러 서비스, 위성이동통신 등을 포함하는 무선통신서비스 제공업자를 포함함
- 네덜란드 에서는 형사소송법, 국가보안법, 통신법 등에서 감청수행과 관련된 사항을 규정하고 있으며 이메일을 비롯한 IP 서비스에 대한 감청은 2001년부터, 인터넷 전화에 대한 감청은 2004년부터 시작되었음
- 영국에서는 1985년에 IOCA(Interception of Communication Act)를 제정하여 통신 서비스에 대한 감청을 시작하였음. 하지만 IP 서비스가 발전함에 따라 IOCA기반의 감청에 어려움이 있어 2000년 RIPA 2000(Regulation of Investigatory Powers Act 2000)을 제정하였음. 이는 기술 중립적으로 제정되어 다양한 통신 기술에 대한 감청이 가능하도록 하고 있음
- 호주에서는 통신산업부 및 법무부에서 감청 규제를 담당하고 있는데 호주 내 모든 CSP 와 ISP는 사업 허가의 조건으로 감청기능을 제공해야 하며, 따라서 IP 기반 통신 서비스, 위성통신서비스, 데이터통신 서비스 등 모든 종류의 공공전기통신 서비스가 감청의 대상이 될 수 있는 상태임
- 한편, 기술 측면에서는 LI Plugteststm 시험이 2006년 3월 6일부터 10일까지 ETSI 구내에서 실시되었다. 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 이루어졌음

〈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

〈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

- 이 실험은 종료 후 기술 규격에 12가지의 개선사항을 추가 하였으며 기대에 미치는 안정적인 성능을 발휘하여 성공적으로 평가되었음
- 산업분야측면에서 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 실정. Cisco의 라우터시리즈는 다음과 같은 두 가지 형태의 LI를 수행할 수 있게 설계되었음
- 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 같은 자체적인 기술 규격을 정의하고 사용하는 등의 기술적 우위를 확보하고 있음. 대당 33만 5천 달러의 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 모델

〈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

〈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
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, 모니터링 구조에 대한 연구가 활발히 이루어지고 있음
- 이와 같이 통신망의 범위가 PSTN망뿐만 아니라 데이터 네트워크로 확장되면서 음성 및 영상 정보가 암호

화되어 전송되기도 함. 따라서 암호화된 통신의 감청 또한 필요로 하게 되는데 3GPP및 ATIS등의 표준문서에서는 통신 내용 및 관련 정보과 암호화되어 전송되거나 압축되어 전송될 경우 감청 시 암호화 키 및 알고리즘 등을 전달할 것을 명시하고 있지만 자세한 사항에 대하여는 기술하고 있지 않음. 이에 관련하여 감청을 수행하는 기관에서는 암호화된 통신내용을 복호화 하기 위하여 키 복구 기술을 필요로 하게 됨

– 키 복구 기술은 사용자의 비밀키를 위탁하는 키 위탁 방식과 키 복구 정보를 암호화된 데이터와 함께 전송하는 키 캡슐화 방식, 제 3자를 두어 사용자의 비밀키를 생성하고 보관하는 역할을 맡기는 TTP(Trusted Third Party) 기반의 방식이 있음. 장단점은 아래 표와 같음

〈키 복구 기술의 비교〉

	장점	단점	비고
키 위탁 방식	사용자의 비밀키를 위탁하는 방식으로 확실한 키 복구를 보장	비밀키 노출에 대한 사용자의 거부감이 심함	최근에는 키 복구기관의 복구 능력을 제어함으로써 사용자 거부감을 줄일 수 있는 방식들이 제안되고 있음
키 캡슐화 방식	사용자의 비밀키가 아닌 데이터 암호키를 위탁하므로 비밀키 노출에 대한 거부감이 적음	키 복구를 보장하지 못하는 경우가 있음 (다른 방식에 비해 키 복구 능력이 떨어짐)	최근까지 연구된 기술은 모두 안전성(키 복구 능력)에 문제가 있음
TTP 방식	가장 확실하게 키 복구를 보장하며, 다른 도메인과의 확장이 용이	사용자의 비밀키 노출에 대한 거부감이 가장 심하며, 복구기관의 키 관리 부담이 큼	유럽 중심의 방식

이와 관련된 각국의 암호화된 통신의 키 복구를 위한 정책은 다음과 같음

– 미국의 키 복구 정책
  • 1993년 4월 skipjack 암호알고리즘이 내장된 클리퍼칩으로만 암복호화를 해야한다는 내용의 클리퍼 정책으로 시작
  • 클리퍼칩에 대한 불신 및 키위탁기관이 모두 국가기관인 점, 암복호화의 비용이 많이 든다는 이유로 반발
  • 1994년 고어부통령이 상업적이고 자발적인 위탁기관 설립을 골자로 하는 클리퍼 II 제안
  • 1996년 5월 OMB(Office of Management and Budget , 관리예산청)는 정부와 산업계가 공동으로 강력한 암호를 사용하는 키관리 기반구조(KMI)를 구축할 것을 제안하는 OMB 보고서 발표
  • 1997년 KMI의 창설과 키복구시스템의 사용을 강제하는 내용의 전자데이터 보호법안(EDSA) 입법
– 영국의 키 복구 정책
  • 1995년 집권당인 노동당은 미국의 클리퍼 정책에 반대입장 표명
  • 법 집행기관 등에 영장에 의하여 복호화를 요구할 수 있는 권한을 부여하고자 1997년 통상산업부(DTI)는 TTP 제도 도입을 추진
  • 1998년 자발적인 TTP 제도 도입 허가

- 최근 TTP에 키위탁이나 키 복구의 의무를 부과하지 않는 새로운 방안 모색

– 프랑스의 키 복구 정책

- 1996년 TTP 제도 승인
- 1999년 허가된 TTP만 운영해야 한다는 사항을 폐지하고 법원 요구시 평문을 제출해야 한다는 법 제정
- 최근 키복구 정책의 자유화 추친

– 일본의 키 복구 정책

- 1998년 3월 키 복구 정책 기본계획 발표

○ 평가인증

– 정보보호 평가

- 평가선진국인 미국, 영국, 독일, 프랑스, 캐나다 등은 일찍이 자체 평가기준을 개발하여 정보보호제품의 안전성을 평가하여 왔음. 미국은 1983년 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
- 한편, 이들은 각 국에서 평가한 제품을 타 국가에서 사용하기 위해 해당 국가에서 다시 평가받아야 하는 불편함을 해소하기 위하여 각 국가에서 평가한 결과를 상호인정하기 위한 평가기준을 개발하였음. 초기에는 유럽 국가들이 ITSEC(Information Technology Security Evaluation Criteria)을 개발하였으나 미국과 캐나다가 참여하면서 이들 국가 모두 사용할 수 있는 공통평가기준(CC: Common Criteria for Information Technology Security Evaluation)을 개발하였음
- 더불어 이들 국가들은 평가결과를 상호 인정하는 국제 공통평가기준 상호인정협정(CCRA)을 체결하였으며, '08년 6월 기준으로 CCRA에는 총 25개 국가가 회원국으로 활동하고 있음. CCRA 회원국은 크게 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

〈인증서발행국 및 수용국 현황〉

구분	설명	가입국명
인증서발행국 (13개국)	자국의 인증서가 회원국으로부터 인정받는 국가	미국, 캐나다, 영국, 프랑스, 독일, 호주, 뉴질랜드, 일본, 네덜란드, 노르웨이, 대한민국, 스페인, 스웨덴
인증서수용국 (12개국)	인증서발행국의 인증서를 인정하는 국가	이탈리아, 그리스, 핀란드, 이스라엘, 오스트리아, 터키, 헝가리, 체코슬로바키아, 싱가포르, 인도, 덴마크, 말레이시아

- 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 담당
  - · 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 수행
  - · CC MB: 관심을 가지고 있는 모든 회원 국가에서 참여할 수 있으며 CC 및 CEM을 실제 개발하고 각 국가에서 제기한 의문사항에 대한 해설서를 작성

〈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 – 기술적 이견 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 추진한다. 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 표준으로 제정되었거나 진행 중에 있음
- 특히, CC의 경우 이전 버전의 문제점 및 시장의 요구사항을 반영한 개정 작업이 지속적으로 이루어지고 있음. 현재 통용되는 CC의 버전은 3.1이 사용되고 있는데, 정보보호제품 개발자가 보다 쉽게 CC에 접근하고, 평가기간을 단축하는 등 CC 효율성을 높이기 위하여 CC 버전 4 개정을 위한 5개의 작업반이 구성되어 올해부터 본격적으로 진행될 예정에 있음

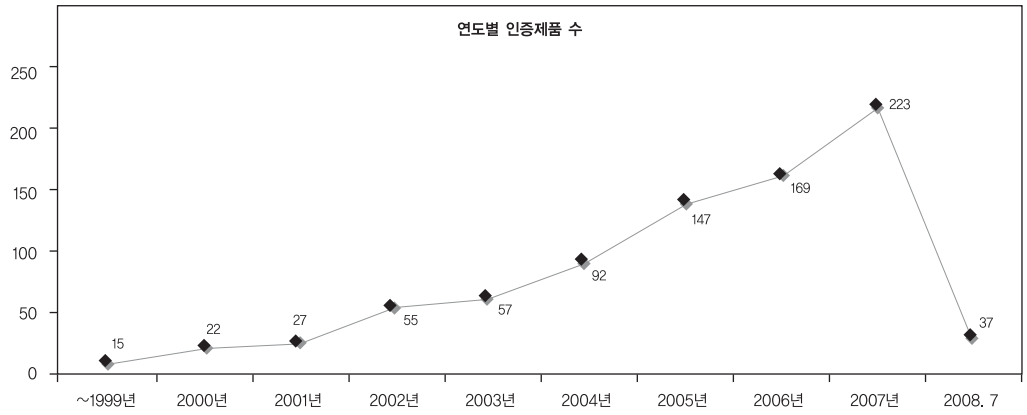
〈CC 버전 4 개정 작업반〉

작업 그룹		주도국	참여국
WG1	Evidence Based Approach(실제 개발자 산출문서 적용 방안)	스웨덴, 미국	영국, 호주, 독일, 프랑스, 한국, 캐나다, 일본, 노르웨이, 스페인
WG2	Skills and Evaluator Interaction(평가자/외부전문가 자격 부여 및 평가기관 간 의견 교류 활성화)	영국, 미국	스페인, 독일, 캐나다, 프랑스, 한국
WG3	Predictive Assurance(제품 변경 시 인증효력 유지)	독일	영국, 미국, 스페인, 노르웨이, 한국
WG4	Detalied Reports(인증보고서/평가보고서 활용도 제고)	캐나다	영국, 미국, 스페인, 호주, 독일, 노르웨이
WG5	Tools to Support Evaluator(평가 효율성 제고를 위한 평가자 도구 활용)	영국, 스페인	미국, 프랑스

- CCRA(http://www.commoncriteriaportal.org)에 따르면, CCRA 인증서발행국에서 인증된 제품은 2008년 7월 15일 기준으로, 총 842개 제품에 달하며 매년 인증제품 수가 증가하고 있는 추세

〈CCRA의 연도별 인증제품 수('08. 7. 15 기준)〉

연도	~1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	계
인증제품 수	15	22	27	53	57	92	147	169	223	37	842
누적 수	15	37	64	117	174	266	413	582	805	842	–



〈CCRA 연도별 인증제품수 추이〉

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

〈제품군별 인증 제품 수('08. 7. 15 기준)〉

제품군	Access Control	Data Protection	Detection Device	Key Mgmt.	OS	Digital Signature	Boundary Protection	DB	IC chip, Smart card	Network Device	Other	합계
인증제품 수	31	31	18	22	78	42	89	36	208	68	234	842

• 인증제품의 등급을 비교하면 스마트카드 제품 평가의 수요로 인하여 EAL4+ 등급이 250개 제품으로 29.7%를 차지하고 있으며, EAL2, EAL3 등급이 각각 158개, 100개 제품으로 18.8%와 12.0%를 차지하며 그 뒤를 잇고 있음

〈보안 등급 별 인증 제품 수('08. 7. 15 기준)〉

보증등급	EAL1	EAL1+	EAL2	EAL2+	EAL3	EAL3+	EAL4	EAL4+	EAL5	EAL5+	EAL6	EAL6+	EAL7	EAL7+	합계
인증제품수(개)	30	19	158	63	101	74	83	250	7	55	0	0	1	1	842
비율(%)	3.6	2.3	18.8	7.5	12.0	8.8	9.9	29.7	0.8	6.5	0	0	0.1	0.1	100.0

– 보안관리

• 정보보호관리체계 인증의 경우, 영국의 BSI(British Standard Institute)에서 만들어진 BS7799 영국 표준이 최초의 정보보호관리 표준이며, 1993년 처음 정보보호 관리실무에 대한 지침으로 개발되어 1995년

처음 BS7799 Part 1이 공포되고 1998년에는 Part 1에 기반한 인증 기준으로서 Part 2가 개발되었음

- BS7799가 ISO(17799, 27001) 표준으로 제정되었으며, 유럽과 일본을 중심으로 활성화 되어 있음. 인증에 대한 표준을 ISO/IEC JTC1 SC27/WG1에서 ISMS 구현가이드, ISMS 평가 방법론, 정보보호 위험관리 등 ISO27000 시리즈를 지속적으로 표준으로 제정하기 위한 작업이 진행 중에 있음

2.2.3. IPR 보유현황 및 확보 가능분야

○ 응용보안

– u-지식 보안

- 한국 출원인인 삼성이 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 있었음
- 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 특허출원이 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 개발 시 타 공백기술에 대한 IPR 확보에 중점을 둘 필요가 있음. 그러나 여전히 국내에서는 사용권한 제어, 워터마킹, CAS 등 한정된 분야에서의 특허를 중점적으로 연구하고 있으며 기업 간의 기술 협력이나 특허의 활용 방안이 한정적으로 콘텐츠의 연동, 유통, 관리 방안과 서비스 구현을 위한 시스템, 기술 활성화에 대한 연구나 특허 출원이 필요한 상황임

– VoIP 보안

- VoIP 관련 국내 특허는 1999년부터 증가하기 시작하여 약 1,036여 건이 등록되어 있다. 이러한 특허 동향은 VoIP 관련 기술의 개발이 외국에 비해 늦었음을 의미. 국내 특허는 주로 채팅서비스, 컨퍼런스폰 시스템 등 VoIP 응용 분야의 출원이 많이 되고 있는 것으로 조사되었음. 현재까지 출원/등록된 주요 VoIP 보안기술 관련 국내특허는 30건 정도가 있으며, 주요 특허의 정보는 아래와 같음

〈VoIP 보안 관련 주요 특허〉

대분류	세부 분류	출원 번호	출원 일자	등록 번호	공고 일자	출원인	발명의 명칭	진행 상태	비고
VoIP 보안		10-2007-0141231	2007.12.31			소시에떼 프랑세즈 뒤 라디오텔레폰	데이터 스트림 보안 방법	공개	
		10-2006-0070516	2006.07.27			지용구 외 1인	복합 기능을 구현할 수 있는 휴대형 유에스비 메모리 장치	공개	
		10-2007-0067669	2007.07.05			브로드콤 코포레이션	브이오아이피 및 보안 아이피를 결합하는 고객 주문형반도체	공개	
		10-2006-0060703	2006.06.30			주식회사 윈아이티	VoIP 수신자 전화번호 기반의 보안 시스템 및 그 방법	공개	
		10-2005-0079357	2005.08.29			주식회사 케이티	VoWLAN 시스템에서 VoIP 서비스를 위한 로밍 및 보안 기능 제공 시스템 및 방법	공개	
		10-2005-0041332	2005.05.17	10-0728277-00-00	2007.06.13	삼성전자주식회사	동적 네트워크 보안 시스템 및 방법	등록	
		10-2005-0013571	2005.02.18			(주) 오른기술	유에스비 메모리 인터넷 폰 및 통화 시스템	공개	
		10-2006-0048646	2006.05.30	10-0768150-00-00	2007.10.17	(주)아이티솔텍	유선 장비를 무선화하는 통합형 전환 시스템	등록	
		10-2005-7022083	2005.11.18			에이티 앤드 티 날리지 벤처스,엘.피.	가상 사설 네트워크를 사용하는 보이스 오버 인터넷프로토콜 텔레포니를 위한 방법 및 장치	공개	
		10-2004-0047424	2004.06.24			최성원	네트워크 통합 관리 시스템	공개	
		10-2007-0023908	2007.03.12	10-0845229-00-00	2008.07.09	주식회사 케이티네트웍스	유무선통합 기업 통신망 환경에서의 CUG / VPN기반모바일 VoIP 서비스 시스템	등록	
		10-2007-0015692	2007.02.15	10-083 8811-00-00	2008.06.19	한국정보보호진흥원	안전한 VoIP 서비스를 위한 보안 세션 제어 장치	등록	
		10-2006-0048646	2006.05.30	10-0768150-00-00	2007.10.17	(주)아이티솔텍	유선 장비를 무선화하는 통합형 전환 시스템	등록	
		10-2006-0009862	2006.02.01	10-0738567-00-00	2007.07.11	삼성전자주식회사	동적 네트워크 보안 시스템 및 그 제어 방법	등록	
		10-2006-0000807	2006.01.04	10-0729628-00-00	2007.06.19	삼성전자주식회사	통합 홈게이트웨이 장치	등록	
		10-2005-0041332	2005.05.17	10-0728277-00-00	2007.06.13	삼성전자주식회사	동적 네트워크 보안 시스템 및 방법	등록	
		10-2006-0010880	2006.02.03	10-0656481-00-00	2006.12.11	삼성전자주식회사	동적 네트워크 보안 시스템 및 그 제어 방법	등록	
총 계		18 건							

- 미국과 일본의 특허는 1500여 건으로 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

- 현재 국내에 대략 350여 건의 스팸 관련 특허가 등록되어 있으며, 이 중 대부분은 이메일 스팸 또는 휴대폰 스팸과 관련된 기술
- 미국 특허는 약 560여 건이 등록되어 있으며, 이 중 기술 특허는 대부분 스팸을 탐지하는 방법, Blacklist/Whitelist 관리 방법, 스팸 방지를 위한 인증 방법 등에 관한 특허. 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

- 현재까지 P2P와 관련하여 네트워킹, 스트리밍, 인터넷 뱅킹, 파일 공유, 검색 등 다양한 응용 분야에서 다수의 특허가 출원되었지만, 국내 P2P 응용 서비스 이용 규모에 비해서 보안 특허 건수는 상대적으로 적은 편임. 현재 출원/등록된 주요 P2P 보안기술 관련 국내특허는 아래와 같음
- 미국에서 Microsoft, Sun Microsystems, Intel, McAfee, HP를 포함한 많은 기업들이 1,000여 건을 등록/출원했으며, 일본에서는 KDDI, Microsoft, NEC, Onkyo, Fuji, Hitachi 등의 기업들이 100여 건의 특허를 출원/등록한 상태임. 한편 유럽에서는 Nokia, Qualcomm, Siemens, Microsoft, Philips, British Telecom, France Telecom, Deutsche Thomson-Brandt GMBH, International Business Machines Corporation 등에서 200여 건의 특허를 출원/등록해오고 있음. 특히 최근 3~4년간 P2P 기술 관련 국제특허가 급증했으며, 향후 P2P 응용 서비스가 더욱 확산 되면서 P2P 관련 특허도 지속적으로 증가할 것으로 전망됨

〈안전한 P2P 보안 관련 주요 특허〉

대분류	세부 분류	출원 번호	출원 일자	등록 번호	공고 일자	출원인	발명의 명칭	진행 상태	비 고
P2P 보안	유해정보차단	10-2004-0064371	2004-08-16	10-0622086-0000	2006-09-13	ETRI	네트워크의 유해 P2P 트래픽 선별 차단 방법 및 장치	등록	
		10-2004-0059560	2004-07-29	10-0690452-0000	2007-03-09	ETRI	네트워크의 유해 P2P 트래픽 선별 차단 방법 및 장치	등록	
		10-2003-0070551	2003-10-10	10-0549504-0000	2006-01-27	ETRI	P2P 트래픽 분류 시스템 및 그 분류 방법	등록	
		10-2002-0059178	2002-09-28	10-0566634-0000	2006-03-24	아라기술	P2P 유해 정보 차단 시스템 및 방법	등록	
		10-2003-0076785	2003-10-31	10-0562357-0000	2006-03-20	IBM	보안이 유지되고 액세스 제어된 P2P 자원 공유 방법 및 장치	등록	
		10-2004-0042145	2004-06-09	10-0462158-0000	2004-12-16	IBM	피어-투-피어 환경에서의 네트워크 트래픽 제어	등록	
		10-2005-0107040	2005-11-09	10-0799558-0000	2008-01-24	ETRI	P2P 네트워크에서의 유해 파일 추적 장치 및 방법	등록	
		10-2004-0077730	2004-09-30	10-0628306-0000	2006-09-19	ETRI	네트워크의 유해 피투피 트래픽 선별 차단 방법 및 장치	등록	
		10-2004-0041692	2004-06-08	10-0609839-0000	2006-07-31	(주)파인핸즈인터넷	유해정보 접촉 관제방법	등록	
	저작권/유통보안	10-2005-0093292	2005-10-05	10-0747147-0000	2007-08-01	문종섭	콘텐츠 유통에 있어서, 저작권자와 네트워크 운영자 그리고, 유통자 모두에게 수익을 보장해주고, 통신상의 보안을 제공해주는 피투피 시스템	등록	
		10-2004-0111109	2004-12-23	10-0670765-0000	2007-01-11	포항공과대학교	P2P 환경에서 수정 가능한 디지털 자료에 대한 저작권 및 콘텐츠 보호 시스템 및 방법	등록	
	인증, 신뢰성	10-2007-0045195	2007-05-09			ETRI	P2P 네트워크에서 피어간 간접 신뢰 바인딩 형성 방법	공개	
		10-2007-0045194	2007-05-09	10-0834580-0000	2008-05-27	ETRI	피어 투 피어 네트워크에서의 아이디 검증 방법	등록	
		10-2008-7004149	2008-02-21			마이크로소프트	피어-투-피어 동기화 애플리케이션에서의 보안	공개	
		10-2008-7006978	2008-03-21			메시네트웍스	노드 간 인증을 위한 무선 네트워크에서의 EAPOL프록시	공개	
		10-2007-7030535	2007-12-27			마이크로소프트	보안 인스턴트 메시징	공개	
		10-2007-7023983	2007-10-18			마이크로소프트	피어-투-피어 인증 및 허가	공개	
		10-2005-0102410	2005-10-28	10-0756308-0000	2007-08-31	리서치 인 모션 리미티드	안전한 피어 투 피어 메시징 초대 구조	등록	
		10-2004-0056365	2004-07-20			마이크로소프트	피어 투 피어 네트워크에서의 안전한 계층적 이름 공간	공개	
		10-2005-7009769	2005-05-30	10-0781725-0000	2007-11-27	IBM	피어 투 피어 인가를 위한 방법 및 시스템	등록	
총 계		15 건							

– IPTV 보안

- IPTV 보안 관련 기술은 고용량의 스트림 데이터 전송(VoD), 음성(VoIP), 데이터(Internet), 그리고 다양한 부가 서비스를 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 590여 건에 달했음. 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 10여 건으로 홈네트워크에서의 서비스 운용과 관련된 특허가 주를 이루고 있음
- IPTV의 주요 코딩 기법인 H.264/MPEG-4 AVC와 관련된 특허는 160여 건으로 대부분 스트림 처리 또는 운용 방법에 관한 것이며, 암호화/복호화 관련 특허는 없는 것으로 조사되었음
- 국내에서 출원된 DRM 관련 특허는 총 280여 건에 달하며 이중 120여 건(한국인 출원 수: 90건)이 영상 데이터 관련 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 조사되었음
- 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 조사되었음
- DRM 관련 특허 중 미국 특허는 800건 이상으로, 출원인 별 분류에서는 마이크로소프트 124건, 인터트러스트 52건, 콘텐츠가드 홀딩스 50건, 삼성전자 35, 노키아 24건, 소니 15건, IBM 14건 등으로 조사되었음. 출원 연도별로는 1996년부터 증가하기 시작하여 2005년에 140건까지 증가하였으나 2006년에는 70이 출원되는데 그쳤음. 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 조사되었음
- AS 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 조사되었음. 일본 특허는 61건으로 이 중 마쓰시다 전기 12건, 소니 10건, 사이언티픽 아틀란타 7건, 도시바 5건 등으로 조사되었음
- IPTV 표준화 추진 전략을 통해 국내 기술이 국제 표준으로 채택될 경우 IPTV 지적재산권 확보를 비롯하여 해외시장 선점의 계기가 될 개연성은 충분하며 방송 · 통신 서비스 사업자와 장비 · 단말기 사업자 간

접속 및 호환이 가능하여 IPTV를 포함한 새로운 방송통신융합 산업의 성장이 전망됨

- 특히 IPTV 보안분야에서는 기존의 해외업체가 주도하고 있는 CAS나 DRM분야의 경쟁개발보다는 사업자의 수익모델을 다양화와 이용자의 편익을 함께 증진시킬 수 있는 CAS와 DRM의 연동기술을 집중적으로 개발할 경우 IPR 확보 가능성이 높다고 할 수 있음

– 신뢰보안서비스(TPM)

- 신뢰보안서비스(TPM)의 국내 IPR 보유 현황은 아래와 같음

〈국내 IPR 보유 현황〉

대분류	세부 분류	출원 번호	출원 일자	등록 번호	공고 일자	출원인	발명의 명칭	진행 상태	비고
TPM	Device	2006-0102249				ETRI	센서 신호 처리 및 응용 장치	등록	
	Crypto	2006-0059845				ETRI	임베디드 시스템용 저전력 AES 암호 장치 및 방법	등록	
	Crypto	10-2004-0044340				삼성	보안키의 복구가 가능한 컴퓨터 및 제어 방법	출원	
	IMV	10-2006-0047232				삼성	자기 수정 코드의 무결성 검증 장치 및 방법	등록	
	Crypto	2006-0120732				ETRI	효율적인 모듈러 곱셈 장치 및 방법	출원	
	Command	2006-0120697				ETRI	효율적인 TPM 명령어 처리 방법	출원	
	Attestation	2006-0120344				ETRI	TPM의 PCR을 이용한 원격 인증 방법	출원	
	crypto	2006-0120455				ETRI	보안 모듈을 이용한 네트워크 서비스 보안 개선 방법	출원	
	authentication	2006-0120840				ETRI	플랫폼 무결성 정보를 이용한 안전한 네트워크 인증 장치 및 방법	출원	
	Boot	2006-0120783				ETRI	TPM을 사용한 모바일 플랫폼의 안전한 부팅 방법	출원	
	IMV	0823738				ETRI	컴퓨팅 플랫폼의 설정 정보를 은닉하면서 무결성 보증을 제공하는 방법	등록	
	Application	2006-0120453				ETRI	신뢰 컴퓨팅 환경에서 각 참여자 상호 보증 기능을 갖는 인터넷 전자투표	출원	
총 계		12 건							

- 국내 IPR 확보 관련하여, 신뢰보안서비스에 대해서는 인텔 등 외국 업체들이 많이 특허를 출원하고 있고, 삼성과 ETRI 등 국내에서도 다수가 출원하고 있음. IPR 확보 가능한 분야는 device authentication, attestation, IMV 등 신뢰보안서비스에 관한 구현 기술, 암호 기술, 칩 기술, 소프트웨어 기술 등 신뢰보안

서비스 기술과 관련한 거의 모든 분야에서 확보 가능함. 또한 신뢰보안서비스 기술이 적용될 수 있는 응용 분야에 대한 IPR 확보도 중요한 요소로 고려하여야 함

- TPM와 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
- TPM 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. 단, 이 표에 나타낸 수치는 2006년도에 조사한 내용으로써, 현재의 특허 출원 상태는 보다 많은 회사들이 보다 많은 관련 특허들을 출원 중

〈업체별 TPM 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

- 현재까지 국내에서도 웹서비스와 관련하여 다수의 특허가 출원되었지만, 주로 웹 기반의 서비스 및 방법에 관한 특허로, 차세대 웹 보안과 직접 관련된 특허는 그 수가 많지 않음. 특히 기존의 웹 및 웹서비스 보안과 관련한 특허는 다수 있으나, 웹 2.0 보안, 시맨틱 웹 보안, 유비쿼터스 웹 보안, 모바일 웹 2.0 보안 등의 분야에서의 국내 특허 출원은 현재까지 드물어 이에 대한 특허 확보가 필요함. 차세대 웹 보안 관련 국내 특허 동향은 다음과 같음
  - 웹서비스 보안과 관련한 특허는 웹서비스에 대한 도입이 상당히 진행된 만큼, 국내에서도 다수의 특허가 출원되어있는 상태임. SOA(Service Oriented Architecture)와 관련된 특허로는, ETRI에서 출원한 SOAP 메시지 보안에 관한 특허 및 연세대에서 출원한 웹서비스 기반 의료정보 보안 접근제어 시스템 등이 있으며, MS에서 국내에 출원한 웹서비스를 위한 신뢰되는 제3자 인증, 웹서비스에 대한 제3자 확장의 안전하고 안정적인 호스팅 등 다수의 특허가 있음
  - 기존의 웹 보안 기술과 관련해서도 많은 국내 특허가 출원되고 있으며, 웹 해킹 방지 기술에 관한 것이

주를 이루고 있음. 한양대에서 출원한 실시간 웹 무결성 검증 시스템, MS가 국내에 출원한 웹서비스 구성의 보안 검사 방법, 트리니티소프트에서 출원한 웹서버의 업로드 파일의 검증 방법 및 장치, 모니터랩에서 출원한 프로파일링 기반 웹서비스 보안 시스템 및 방법 등의 특허가 있으며, 이밖에 실시간 웹로그 수집을 통한 웹해킹 대응 방법, 웹보안 시스템 및 방법 등 많은 특허가 출원되고 있음

- 웹 2.0 서비스와 관련하여 조선대에서 출원한 웹 2.0에서 감성기반 동영상 전자우편 시스템 등 다수의 특허가 있으나, 웹 2.0 보안과 직접 관련된 특허는 현재까지 등록된 것이 그다지 많지 않음
- 웹 2.0 보안과 관련이 있는 특허로는 블로그 정보보호 방법, 커뮤니티 내에서의 메시지 전달 및 보호 방법 등과 같이 사용자 커뮤니티 서비스에 특징적인 것들이 대다수임. 이밖에 아주대에서 출원한 커뮤니티 컴퓨팅 보안 시스템 및 방법에 대한 특허가 있으며, 웹 2.0 보안과 관련한 특허는 NHN, SK텔레콤과 같이 블로그, 미니홈피 등과 같은 웹 2.0을 서비스하는 업체들이 주도하고 있음
- 시맨틱 웹과 관련된 특허로는, ETRI에서 출원한 시맨틱 UDDI 레지스트리 시스템 및 검색 방법이 있으며, 시맨틱 웹 어노테이션을 위한 웹 문서의 자동 의미정보 추출 방법 및 시스템, ebXML 레지스트리 정보 모델에서 웹 온톨로지 처리 등에 대한 특허가 있음. 하지만 시맨틱 웹 기반 보안 기술과 관련된 특허는 거의 없으며, 주로 기존의 웹 서비스에 대한 시맨틱 웹 기술 적용 등에 대한 특허가 대부분임
- 유비쿼터스 웹과 관련된 특허로는, ETRI에서 출원한 웹서비스 기반의 규칙 처리를 위한 디바이스 방법, 이종의 SOAP 전송 프로토콜을 사용하는 노드 간 웹서비스 연동 방법 등의 특허가 있으며, 삼성전자에서 출원한 웹브라우저가 없는 장치를 위한 웹서비스 제공 시스템 및 방법, 홈네트워크 기능을 갖는 웹 페이지 제공 시스템 및 홈네트워크 디바이스 제어 방법 등의 특허가 있음
- 삼성전자와 같은 대기업 및 ETRI를 중심으로 유비쿼터스 웹에 대한 개념을 정리하고 있는 단계로 파악되며, 현재까지 등록된 특허는 디바이스 기반 웹서비스의 서비스 구조에 대한 것이 대부분이며, 유비쿼터스 웹 보안과 직접 관련된 특허는 아직까지 드뭄
- 기존의 모바일 웹과 관련된 국내 특허는 삼성전자, LG 전자 등 휴대 단말 제조업체를 중심으로 많은 특허가 출원 혹은 등록되고 있음. 삼성전자가 출원한 복수 개의 웹브라우저를 사용하는 이동 단말과 웹 서버 간의 통신 방법, 인프라웨어에서 출원한 휴대 인터넷상에서 웹페이지를 신속하게 보여주는 방법 및 시스템 등의 특허가 있음
- 모바일 블로그를 중심으로 하는 모바일 웹 2.0 관련 특허가 출원된 바 있으며, 이동통신 단말기에서의 위치정보 획득 및 이를 이용한 이동통신 단말의 영상 및 사진, 문자를 인터넷 지도에 표시, 등록하기 위한 단말 응용 기술 및 서비스 시스템에 관한 특허가 출원 중임
- 기존의 모바일 웹 보안과 관련된 특허는 LG 전자가 출원한 웹사이트 유효성 검증 기능을 구비한 이동통신 단말기 및 웹사이트 유효성 검증 방법 및 웹사이트 유효성 검증 시스템 등의 특허가 있으나, 모바일 웹 2.0 보안과 관련한 특허는 현재까지 출원된 것이 거의 없는 것으로 분석됨

• 국외에서는 웹 보안 분야에 대해서 많은 특허가 존재하는 것으로 파악되고 있으며, 특히 웹서비스 보안은

MS, IBM 등의 업체에서 다수의 핵심 특허를 보유하고 있음. 하지만 웹 2.0 보안, 시맨틱 웹 기반 보안, 유비쿼터스 웹 보안, 모바일 웹 2.0 보안 등 차세대 웹 보안과 직접 관련된 특허는 국외에서도 아직 그 숫자가 많지 않음. 차세대 웹 기반의 서비스 구조 및 방법에 대한 특허가 지속적으로 출원되고 있는 것으로 볼 때 차세대 웹 보안 관련 특허 출원도 증가하리라고 예상되며, 이 분야에 대한 전략적인 기술 개발 및 특허 확보가 필요하다고 판단됨. 차세대 웹 보안 관련 국외 특허 동향은 다음과 같음

- 웹서비스 보안 기술과 관련하여 많은 특허가 존재하며, 특히 웹서비스 보안 기술 개발을 세계적으로 주도하고 있는 IBM, MS 등에서 많은 특허를 등록하였음. IBM에서는 Security mechanisms in a Web server, System and method for providing physical Web security, Security profile for Web browser 등의 특허를 보유하고 있고, MS에서는 Checking the security of Web services configuration, Web application security framework 등 다수의 특허를 보유하고 있음
- 웹 2.0과 관련하여 다수의 특허가 등록되어 있으나, 대부분의 특허는 블로그, AJAX 등의 웹 2.0 서비스와 기술 등에 대한 것이며 웹 2.0 보안과 직접 관련된 특허는 국외에서도 아직 많지 않은 것으로 분석됨. 웹 2.0 관련 특허가 다수 등록되고 있는 실정이므로, 웹 2.0 보안 관련 특허도 늘어날 것으로 예상됨. 현재까지는 구글과 아마존이 웹 2.0과 관련한 다수의 특허를 제출하고 있음
- 시맨틱 웹과 관련된 특허로는, 독일에서 출원한 A method and a system for integrating semantic Web services into a existing Web service infrastructure, A method and a system to organize and manage a semantic Web service discovery, 프랑스에서 출원한 Method for finding Web services described by respective semantic descriptions in different languages or forms 등의 특허가 있음
- 시맨틱 웹 관련 특허는 주로 기존의 웹 서비스에 대한 시맨틱 웹 기술 응용 등에 대한 특허로, 시맨틱 웹 기반 보안 기술에 대한 특허는 아직 국외에서도 미미한 실정임
- 미국에서 Remote control of wireless electromechanical device using a web browser, Generating and communicating web content from within an implantable medical device 등 웹 기술을 디바이스 환경에 적용하는 방법에 대한 특허를 출원하였으며, 국외에서는 유비쿼터스 웹 서비스에 대한 개념이 도입되고 있는 단계로 파악됨
- 현재까지 등록된 유비쿼터스 웹 관련 특허는 디바이스 기반 웹서비스의 서비스 구조에 대한 것이 대부분으로 분석됨. 일본 RICOH에서 디바이스 상에서 웹서비스를 제공하는 기술과 함께 보안 서비스를 제공하기 위한 방법에 대한 특허를 등록하였으며, 이외의 유비쿼터스 웹 보안과 직접 관련된 특허는 아직까지 별로 없는 것으로 파악됨
- 기존의 모바일 웹과 관련하여 많은 특허가 존재하며, 특히 Nokia가 상당수의 특허를 보유하고 있음. Nokia는 Web Services push gateway, Mobile Web Services, System and method for location based Web Services, Terminal based device profile Web Service, System, Apparatus, and method for

providing Web Services on mobile devices 등의 모바일 웹서비스 관련 핵심 특허를 다수 보유하고 있음

- 기존의 모바일 웹 보안과 관련하여 Nokia가 Method and apparatus for implementing secure VPN access via modified certificate strings 특허를 등록하였고, IBM에서 Method and apparatus for controlling access to the contents of web pages by using a mobile security module 등의 특허를 등록하였음. 또한 삼성에서 Internet access control method in a mobile communication terminal with a built-in web browser라는 국제 특허를 출원하였음
- 하지만 모바일 웹 2.0 보안과 관련된 특허는 아직 국외에서도 별로 없으며, 보안 이외의 모바일 웹 2.0 관련 특허로 Nokia에서 Method and apparatus for automatically updating a mobile Web log(Blog) to reflect mobile terminal activity 등의 특허를 몇 건 출원하였고, 국외에서도 모바일 웹 2.0과 관련한 특허는 국내와 마찬가지로 블로그를 대상으로 서비스 특허 출원 단계에 있음

– Lawful Interception

- 국내에서는 합법적 감청과 도청은 기술에 있어 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 21건이 출원되었고 그 중 9건이 등록됨.(2008.8). 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 시작하였음

〈Lawful Interception 관련 국내 특허 현황〉

출원 번호	출원일자	등록번호	공고일자	출원인	발명의 명칭	진행 상태
1019970009465	1997.03.20	1002224140000	1999.10.01	삼성전자주식회사	가입자 감시/감청 동시 수행방법	등록
1019970077687	1997.12.30	1002578090000	2000.06.01	주식회사 신세기통신	코드분할 다중접속 아날로그 이중모드 단말기에서의 단말기 복제에 의한 감청 방지 방법	등록
1019990015971	1999.05.04	1003189650000	2002.01.04	삼성전자주식회사	교환기 시스템에서 가입자의 감시와 감청을 위한 시스템 및 방법	등록
1019990017874	1999.05.18	1003204220000	2002.01.16	엘지정보통신주식회사	통신망에서의 특정 번호의 호에 대한 감청 방법	등록
1020000061343	2000.10.18	1004357820000	2004.06.12	엘지전자 주식회사	사설 교환기 가입자의 정보 및 음성 감청장치	등록
1020010087329	2001.12.28			주식회사 머큐리전전자	교환기에서의 가입자 감청 시험 방법	공개
1020020049469	2002.08.21			엘지노텔 주식회사	사설교환기의 복수가입자 감청 및 감독기능 제공 장치 및 방법	공개
1020020071980	2002.11.19	1005563550000	2006.03.03	엘지전자 주식회사	패킷 데이터 감청 기능을 갖는 이동통신 패킷 교환국 및 이를 이용한 호 감청 방법	등록
1020030011169	2003.02.22			주식회사 케이티	차세대망에서 콜 믹서 기능을 이용한 감청기능 구현 방법	공개
1020040007845	2004.02.06	1008241670000	2008.04.21	주식회사 케이티	NGN에서의 음성 통화 감청 시스템 및 방법	등록
1020040074267	2004.09.16			주식회사 케이티	차세대 통신망에서의 감청시스템 및 방법	공개
1020060102358	2006.10.20			삼성전자주식회사	이동통신 시스템에서 패킷 데이터 감청을 위한 장치 및 방법	공개
1020060119146	2006.11.29			엘지노텔 주식회사	이동 단말기 감청 시스템 및 감청 방법	공개
1020070014244	2007.02.12	1007991930000	2008.01.29	삼성전자주식회사	이동통신 시스템에서 감청을 위한 장치 및 방법	등록
1020070119164	2007.11.21	1008521460000	2008.08.13	한국정보보호진흥원	제 3 신뢰기관을 이용한 VoIP 보안 통신에서의 감청시스템 및 감청 방법	등록

- 국외에서는 직접적으로 LI를 특허 제목으로 지정하여 출원된 미국특허는 총 29건이며, 이중 9건이 등록된 것으로 파악됨. 그러나 LI, Electronic Surveillance, Wiretapping 등과 같은 보다 일반적인 도청 및 감청의 범주에서의 관련 특허는 총 900여 건으로 이중 600여 건 등록되어 있음. LI 관련 371건 정도의 유럽 특허가 출원되어 있으며, 명시적으로 LI 자체를 다루고 있는 특허는 대략 23건 정도인 것으로 분석됨. 일본 특허는 광의적 의미에서의 IP 네트워크, 통신채널 상에서의 보안 관련 특허는 100여 건 이상 존재하지만, LI와 직접적으로 연계성을 갖는 특허는 극히 적은 것으로 판단되며, 등록 건수는 역시 미비한 것으로 조사되었음
- 현재 발표된 국내외의 LI 관련 특허 전반과 특히 무선구간 및 암호화된 통신 등과 관련한 특허는 현재 미비한 상태이며 앞으로 많은 분야에서 출원 가능할 것으로 보임

2.3. 표준화 현황 및 전망

2.3.1. 국내 표준화 현황 및 전망

○ 응용보안

– 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 단체 표준으로 EXIM을 표준화하여 DRM간 데이터 교환으로 상호연동이 가능한 인터페이스 규격을 제정하였으나, 서비스 사업자 간 호환성과 과금 방식에 이견이 있는 상태. 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. 또한 우리나라에서 진행되고 있는 표준 단체 및 연구에서는 DRM, CAS, 핑거프린팅 등 개별적인 표준화는 국제 표준 단체와 연계를 통해 활용되고 있으나 아직까지 이러한 기술에 대한 연계 방안이나 콘텐츠 재활용성이나 다양한 유통 방안에 대한 모색이 부족한 실정

– 스팸대책

• 스팸 관련 국내 표준화는 ETRI(PEC: Protocol Engineering Center)가 중심이 되어 ITU-T SG17/Q17에서 이뤄지고 있음. 2008년 3월까지 논의된 주요 표준 기고서는 다음과 같음

〈ITU-T 스팸 관련 표준 기고서 현황〉

구분	문서명	문서이름	제정년도	상태
ITU-T SG17/Q17	X.1244(X,ocsip)	Overall aspects of IP Multimedia Application Spam	–	**
	X.fcsip	Framework for countering IP multimedia spam	–	*
	X.csreq	Requirement on countering spam	–	진행
	X.fcs	Technical framework for countering e-mail spam	–	진행
	X.gcs	Guideline on countering e-mail spam	–	승인예정
	X.ssf	Short Message Service(SMS)spam filtering system based on users' rules	–	*
	X.tcs	Technical means for countering spam	–	진행
	X.tcs-1	Interactive countering spam gateway system	–	*

* Draft Recommendations planned for consent or dertermination at the September 2008 SG 17 Meeting
** Recommendation planned for approval at the September 2008 SG 17 Meeting

– 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 표준 제정이 시급하다고 볼 수 있음

– IPTV 보안

- 국내 IPTV 표준화 움직임은 ITU-T의 FG-IPTV 설립과 함께 진행되고 있음. 한국정보통신기술협회(TTA) 산하에 IPTV 프로젝트 그룹(PG219)과 동 그룹산하 4개 실무반(WG)을 통해 총 11건의 TTA표준을 작성 중에 있음. IPTV 관련 표준은 비디오 및 오디오 코딩, 전송 네트워크 프로토콜, 코덱, 스트리밍 전송, 콘텐츠 보안, 맞춤형 방송 등 IPTV 서비스 전반적인 분야에 걸쳐 진행되고 있는데, 특히 IPTV 보안 표준은 과제번호 "2007-086"으로 채택된 "IPTV Security 기술"이란 과제명으로 단체표준이 작성 중에 있음
- TTA는 IPTV 구조 및 시나리오 실무반, IPTV 수신기 규격 실무반, Mobile IPTV 실무반, IPTV 보안 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. 특히 IPTV 보안 실무반(WG2194)에서는 IPTV 콘텐츠 보호기술, IPTV 서비스 보호기술, IPTV 단말기 보호기술, IPTV 가입자 보호기술 및 방송서비스 보호기술과 콘텐츠 보호기술간의 연동기술 등 5가지 세부기술로 나누어 표준화 작업을 추진 중에 있으나 현재까지 눈에 띄는 진전을 보이고 있지는 않은 실정임
- IPTV관련 표준화 추진체계는 舊 정보통신부 산하 ITU-T IPTV-GSI 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 법령의 지연으로 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 작성하였음
- 아래 표 둘은 ITU-T IPTV FG의 작업문서와 living list로 남아있는 문서 중 2007년 7월 현재 한국인 에디터가 작성하고 있는 문서 목록

〈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

〈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

〈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

〈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)

〈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 기능을 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

〈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

- 신뢰보안서비스(TPM)의 국내 표준화 현황
  - 국내에서는 TTA의 PG504를 통하여 신뢰보안서비스에 대한 표준화 작업을 진행하고 있음. 2007년에 PG504에서 신뢰보안서비스가 중요한 표준화 아이템 중 하나로 정해졌으며, 2008년에 본격적인 표준화 작업을 진행하고 있음
- 표준화 작업 주요 참여 기업 및 기관
  - ETRI
  - (스프레드텔레콤, 프롬투)
  - (표준화가 본격적으로 추진되면 보다 많은 업체들이 참여할 것으로 예상됨)
- TPM 관련 국내 표준화 문건
  - 신뢰 보안 서비스에 관한 국내 표준화는 2007년부터 진행되고 있음

〈국내 표준화 진행 상황〉

표준화기구명	문서이름	제출자	제출일
TTA(PG504)	모바일 플랫폼용 신뢰보안모듈(MTM) 인터페이스	ETRI	진행 중
TTA(PG504)	차세대 모바일 플랫폼에서의 신뢰보안모듈(MTM) 서비스 시나리오	ETRI	진행 중
무선인터넷표준포럼	PKCS#11의 WIPI API 확장	ETRI	진행 중
무선인터넷표준포럼	WIPI용 Security API 확장	ETRI	진행 중

- 차세대 웹 보안
  - 국내에서는 웹 보안과 관련하여 TTA가 주요한 표준화 기구로서 활동 중이며, 이밖에 전자상거래 표준화 통합 포럼(ECIF), 유비쿼터스 웹 포럼, 모바일 웹 2.0 포럼 등에서도 관련 표준화를 추진하고 있음
  - TTA의 응용보안 및 평가인증 그룹(PG504) 에서는 안전 응용 보안 표준, 보안성 평가 기술 및 보안관리 표준, 신뢰보안 모듈 기술 표준 등을 개발하고 있으며, 웹 보안 관련 표준 개발도 담당하고 있음
  - TTA의 웹 프로젝트 그룹(PG605)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

- 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
- 모바일 웹 2.0 포럼에서는 응용 WG, 단말정보 WG, 시험인증 WG, 콘텐츠 WG 과 함께 모바일OK TF를 구성하여, 각각의 세부적인 표준안들을 개발하는 작업을 진행하고 있음
- 2005년부터 2007년까지 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 수행한 바 있으며, 2008년부터 차세대 웹 보안 관련 표준화 연구를 수행하고 있음
- ETRI에서는 2008년부터 인터넷 인프라 보안 표준 개발 표준화 과제를 통해 차세대 웹 보안 기술 표준 기술을 개발하고 있으며, 2008년 상반기 ITU-T SG17에서 차세대 웹서비스 보안 표준화 로드맵을 수립하였고, 2008년 하반기부터 SG17에서 차세대 웹기반 통신 서비스를 위한 보안 프레임워크(X.websec-4) 표준 개발을 진행하고 있음
- 국내에서는 주로 웹서비스 보안 및 SOA 보안 관련 표준이 많이 개발되었으며, 아직까지는 웹 2.0 보안, SOA 기반 융합 서비스 보안, 유비쿼터스 웹 보안, 시맨틱 보안, 모바일 웹 2.0 보안 등 차세대 웹 보안에 관한 표준은 개발되지 않고 있음
- 향후 차세대 웹 기반 서비스의 확산에 따라 이를 위한 보안 기술에 대한 수요도 증가하리라고 예상되며, TTA PG504 등을 중심으로 차세대 웹 보안 기술 국내 표준화가 진행되리라고 예상

〈웹 보안 관련 국내 표준화 문건〉

구분	표준화 기구	문서번호	문서이름	상태	발표월일
웹서비스 보안	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	2004-12-23
		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	V1.0.0	2006-12-27
		TTAE.OT-12.0006	웹 서비스 보안 X.509 인증 토큰 프로파일 1.1	V1.0.0	2005-12-21
		TTAE.OT-12.0004	웹 서비스 보안 유저네임토큰 프로파일 1.1	V1.0.0	2005-12-21
		TTAS.OT-10.0133	확장성 생성언어 키 관리(XKMS 2.0) 요구사항	V1.0.0	2007-12-26
		TTAS.OT-10.0134	확장성 생성언어 키 관리 명세(XKMS 2.0)	V1.0.0	2007-12-26
		TTAS.OT-10.0132	확장성 생성언어 키 관리 명세 바인딩 2.0	V1.0.0	2007-12-26
		TTAS.KO-10.0246	웹서비스 응용을 위한 통합 보안 모델 가이드라인	V1.0.0	2007-12-26
		TTAS.KO-10.0245	모바일 웹서비스 보안 평가 가이드라인	V1.0.0	2007-12-26
		TTAS.KO-10.0244	웹서비스 보안 정책 적용 가이드라인	V1.0.0	2007-12-26
		TTAS.KO-10.0243	웹서비스 보안 정책 모델	V1.0.0	2007-12-26
		TTAS.OT-10.0040/R1	확장성 접근제어 생성언어 2.0	V1.0.0	2007-12-26

– 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 agency 간의 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. 이것은 IMT2000 영역에 편중된 표준화 작업만이 이루어져, IP 기반의 VoIP, email 등과 같은 서비스 환경에 대한 LI 표준안 부재의 문제점을 안고 있음
  - 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 작업에 참여한 주요 기업및 기관의 목록은 다음과 같음
  - 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, SK 브로드밴드, 한국통신프리텔, 한솔엠닷컴, LG정보통신, LG텔레컴, SK텔레컴

〈LI 관련 국내 표준화 문건〉

표준화 기구	문서번호	문서이름	상태	발표월일
TTA	TTAT.3G-33.106	IMT-2000 3GPP-3G 보안; 합법적 감청 요건	V7.0.1	2008.4.9
	TTAT.3G-33.107	IMT-2000 3GPP – 3G 보안; 합법적 감청 구조 및 기능	V7.6.0	2008.4.9
	TTAT.3G-33.108	IMT-2000 3GPP – 3G 보안; 합법적 감청에 대한 핸드오버 인터페이스	V7.8.0	2008.4.9

○ 평가인증

– 정보보호 평가

- 보안성 평가와 관련하여 상호인정협정(CCRA)에서 공통평가기준으로 사용되는 CC 1, 2, 3부가 버전 2.1에 대하여 TTA 단체 표준으로 2001년 제정되었으며, 이는 기술표준원의 한국산업규격(KS X ISO/IEC 15408-1/2/3)으로도 표준화가 추진되어 현재 CC V2.3까지 개정 완료된 상태임
- 또한, 어떤 제품 또는 구현물이 표준에 부합하는지 시험하는 표준적합성 시험 분야에 있어서도, 전체적인 시험방법과 절차 및 도구를 다루는 문건에서부터, 생체인식, IPSEC VPN 등 사례를 적용한 문건까지 표준화가 진행되었음
- 한편, 암호와 관련하여 SEED, AES 등 암호알고리즘 자체를 다루는 부분에서부터, 암호 메시지 규격, 인증서 등 일부 응용 분야까지 TTA의 단체표준으로 제정된바 있으며, 암호모듈 평가와 관련된 표준화는 크게 암호모듈 보안 요구사항(KS X ISO/IEC 19790)과 시험 요구사항(KS X ISO/IEC 24759)으로 기술표준원의 한국산업규격(KS)에서 다루고 있음

〈정보보호 평가 관련 표준화 현황〉

구분		문서명	문서이름	제/개정일	상태
정보보호 평가	TTA	TTAE.CC-99.031(CC-1v2.1)	국제공통평가기준 – 제1부: 소개 및 일반모델	2001-12-19	표준
		TTAE.CC-99.032(CC-2v2.1)	국제공통평가기준 – 제2부: 보안 기능 요구사항	2001-12-19	표준
		TTAE.CC-99.033(CC-3v2.1)	국제공통평가기준 – 제3부: 보안 보증 요구사항	2001-12-19	표준
		TTAS.KO-12.0023	낮은 위험수준을 위한 보증패키지	2003-12-18	표준
		TTAS.KO-12.0026	침입탐지시스템 기능패키지	2003-12-18	표준
		TTAS.OT-12.0003	정보보호제품 표준적합성 시험방법	2004-12-23	표준
		TTAS.OT-10.0001	BioAPI 표준적합성 시험방법 및 절차(K-CTS)	2004-12-23	표준
		TTAS.KO-12.0032	IPv6 IPsec AH/ESP 표준적합성 시험	2005-12-21	표준
		TTAS.KO-12.0033	IPv6 IPsec IKE 표준적합성 시험	2005-12-21	표준
		TTAS.KO-11.0061	표준적합성 평가도구 요구사항	2006-12-27	표준
		TTAS.KO-11.0077	소프트웨어 표준적합성 평가절차	2007-12-26	표준
	KS	KS X ISO/IEC 15408-1	정보기술 – 보안기술 – 정보기술보안 평가기준 – 제1부: 개요와 일반모델	2006-12-26	표준
		KS X ISO/IEC 15408-2	정보기술 – 보안기술 – 정보기술보안 평가기준 – 제2부: 보안기능 요구사항	2006-12-26	표준
		KS X ISO/IEC 15408-3	정보기술보안 평가기준 – 제3부: 보안보증 요구사항	2006-12-26	표준

– 보안관리

- 국내 보안관리 관련 표준 또는 지침 작성은 한국정보통신기술협회(TTA)에서 제정하는 정보통신단체표준, 舊 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 지

침 등 5건의 단체표준을 고시하였음. KICS에서도 정보보호관리 관련 7 종의 보안관리 지침서를 제정하였으나 대부분 1996년도 이전에 작성된 것임. KS에서는 정보보호관리 관련 국제표준인 ISO13335의 1-4부를 KS화 하였고, ISO17799 역시 KS화하여 총 5건의 KS가 있음

2.3.2. 국외 표준화 현황 및 전망

○ 응용보안

- 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 진행 중임
    - DRM 표준 정립을 위해 SDMI, AAP, OeBF, DVD Forum, IRTF의 IDRM, DOI, OPIMA, MPEG-21 등 다양한 표준화단체들이 2000년을 전후로 대거 등장하였으며, 각자 독자적인 DRM 표준기술 준비 이후 W3C, ISMA, TV-Anytime, OMA, DHWG, DMP 등 새로운 단체 등장
    - 저작권 보호기술 분야는 MPEG-21, OMA, DVB-CPCM, DHWG, TV-Anytime, IDRM, SDMI, OeBF, XrML, ODRL에서 추진 중
    - 디지털 방송 & 셋탑박스 분야(CAS 포함)는 OpenCable POD Copy Protection(케이블방송), ATSC CA(지상파), DVB-CA, ISMACrypt 에서 추진 중
- 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[10]

- 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

- IETF에서는 VoIP에 대한 보안 서비스를 제공하기 위하여 다양한 연구에 대한 표준작업을 진행하고 있음. 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
- SIP는 시그널링을 위한 프로토콜로 세션 설정과정에서의 관련 데이터 보호를 위한 여러 보안 메커니즘을 제공하고 있음. 사용자 인증으로는 HTTP 인증, 홉 간 보안을 위해 TLS(Transport Layer Security), 양자 간 보안을 위한 S/MIME(Secure/Multipurpose Internet Mail) 등 기존 보안 메커니즘을 그대로 이용함. 멀티미디어 데이터를 전송하는 프로토콜인 RTP(Real-time Transport Protocol)는 멀티미디어 데이터의 기밀성 및 무결성 보장을 위해 SRTP(Secure RTP)를 이용함. 또한 VoIP에서는 멀티미디어 데이터 암호화를 위한 키 관리 프로토콜로 MIKEY(Multimedia Internet KEYing)를 사용하고 있음

〈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 기밀성과 무결성을 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)	홉 간 보안
S/MIME(Secure/ Multipurpose Internal Mail)	– 종단 간 SIP 사용자에게 보안기능을 제공하고, 메시지에 대한 기밀성, 무결성과 상호 인증 기능을 제공함(RFC 2633, RFC 3261)	양단 간 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 AES[11]를 사용하며, Counter Mode를 적용하여, 실시간 암호화 패킷 전송을 지원함

10) ITU-T SG17/Q.17 국제 표준 개발 로드맵: Guideline for countering email SPAM(X.gcs): '06년까지 개발할 예정임

- SRTP 패킷 전송을 위한 암호화 키는 MIKEY 키관리 프로토콜을 적용하여 양 단말 간에 공유하지만, MIKEY 키관리 프로토콜의 적용은 표준 초안 단계로써 실용화를 위해서는 검증이 필요함
  - MIKEY(Multimedia Internet KEYing, RFC3830)
  - MIKEY는 실시간 멀티미디어 통신(SIP 호 교환 및 RTSP세션, 스트리밍, 유니캐스트, 멀티케스트 등을 위한 키 관리 메커니즘으로 이기종망 통신환경에서 안전한 멀티미디어 세션 통신을 위한 키 관리 및 갱신 등에 대한 규격을 제시함
  - 기존의 키 관리 프로토콜인 IKE, TLS 등의 문제점을 해결하며, VoIP에서 멀티미디어 세션을 위한 IETF 키관리 프로토콜로 현재 거의 표준완료 단계임
  - MIKEY에서는 3가지 키관리 모드로, 사전 공유키 기반 키 공 공유방법(Pre-shared Key), 공개키 암호 기술을 이용한 키 공유 방법(Public-key encryption), Diffie-Hellman기반의 키 공유방법(Diffie-Hellman key exchange)이 있음. 2006년에는 RFC 3830를 새로운 MIKEY RSA모드인 MIKEY RSA-R 모드로 update한 RFC 4738가 승인되었음. 이외에도 ECC(Elliptic Curve Cryptography)을 지원하는 방식 등이 Draft로 나와 version 3(draft-ietf-msec-mikey-ecc-03)까지 진행되었으나 2007년 6월 이후 진행이 되지 않고 있음
  - 기본적인 키 전송 암호화는 AES counter mode이며, RFC 2014에 따른 HMAC SHA-1 160비트 인증 태그를 사용함. 공개키 분배 방식일 경우는 공개키 암호화와 전자서명을 위한 X.509v3 인증서를 기반으로 함
  - 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
  - RTP(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
  - AVT(Audio/Video Transport) WG에서 ZRTP와 관련된 기고서는 다음과 같음("Media Path Key Agreement for Secure RTP"(draft-zimmermann-avt-zrtp-07)
  - 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

11) Advanced Encryption Standard

- "Framework for anti-spam in SIP Draft-ietf-sipping-spam-05, RFC5039)"서는 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
- SIPPING WG에서 인터넷 전화상에서의 스팸 방지(SPam over Internet Telephony(SPIT) prevention)와 관련된 기고서는 다음과 같음

• "Signaling TO Prevent SPIT(SPITSTOP) Reference Scenario"(draft-niccolini- sipping-spitstop-01)"
• "Requirements for Authorization Policies to tackle Spam and Unwanted Communication for Internet Telephony"(draft-froment-sipping-spit-requirements-03)
• "A Framework to tackle Spam and Unwanted Communication for Internet Telephony"(draft-tschofenig-sipping-framework-spit-reduction-04)
• "A Document Format for Expressing Authorization Policies to tackle Spam and Unwanted Communication for Internet Telephony"(draft-tschofenig-sipping-spit-policy-03)
• 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
• IETF의 Geopriv WG, SIMPLE WG, ieprep WG 및 ecrit WG을 중심으로 VoIP를 이용한 위치정보 활용 서비스의 개발을 진행 중임
• IETF geopriv(Geographic Location/Privacy) WG에서 물리적 위치에 데이터 포맷, 위치정보 전달 절차, 위치정보에 대한 프라이버시 보호 표준화를 추진 중임
  - Geopriv WG의 주요과제는 지리적 위치 정보를 전달하기 위해 만족되어야 하는 인증(authentication), 완전성(integrity), 프라이버시 요구사항을 평가하고 에이전트를 통한 그러한 정보의 표현 및 동개를 인증하는 것임
  - 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 시작하였음

· IETF의 SPEERMINT(Session PEERing for Multimedia INTerconnect) WG은 실시간 통신호의 라우팅, 시그널링 등을 위한 구조에 관한 그룹으로, 주로 실시간 세션 라우팅 구조들에 관하여 초점을 두고 있음. 두 개 이상의 IP 네트워크 기반 도메인들 간 동등접속이 가능하도록 SIP 시그널링 프로토콜을 사용하는 것으로 가정하고 있음

· SPEERMINT WG 에서는 SIP기반의 VoIP 서비스에 있어서 VoIP 사업자 간 Peering 이슈를 다루고 있음. SPEERMINT에서는 아래의 internet draft에서 VoIP Peering 구조 및 federation 기반 peering 모델에서의 메시지 흐름 등에 대해 설명하고 있음

· draft "SPEERMINT Terminology": SPEERMINT 에서 사용하는 용어의 정리

· draft "SPEERMINT Requirements for SIP-based Session Peering": 일반적인 요구사항 및 Session Peering을 위한 Signaling과 Media 가이드라인 정의

· draft "SPEERMINT Peering Architecture": 멀티미디어 상호접속 세션에서 참조할 수 있는 구조모델을 정의

· draft "SPEERMINT Routing Architecture Message Flows"

· draft "Presence & Instant Messaging Peering Use Cases"

· draft "VoIP SIP Peering Use Cases": VoIP 만을 고려하였을 때 SIP 기반 동등접속 환경의 구조, 구성요소에 대한 설명

• SBC의 주요기능 중 하나인 NAT/FW 통과 해결을 위한 관련된 국제 표준에는 STUN[12], TURN[13], ICE[14], MIDCOM[15] 등이 있으나, 시장에서의 적용은 매우 미흡한 실정임

– 스팸대책

• IETF DKIM(Domain Keys Identified Mail) WG는 인터넷을 통해 전달되는 메시지와 해당 메시지의 신원증명(Identity) 사이의 연계관계(Association)의 유효성을 검증하는 것에 초점을 맞추고 있음. 이를 위해 암호학적 메커니즘을 제공하고 있으며, 공개키 암호화 기법을 이용하는 이메일 및 키 서버 기술을 위해 도메인 레벨의 인증 프레임워크(Domain-Level Authentication Framework)를 정의함

12) Simple Traversal of UDP through NATs

13) Traversal Using Relay NAT

14) Interactive Connectivity Establishment

15) Middlebox Communications

〈IETF DKIM WG 관련 문서〉

구분	문서이름	상태
IETF DKIM WG	Analysis of Threats Motivating DomainKeys Identified Mail(DKIM)	RFC 4686
	DomainKeys Identified Mail(DKIM) Signatures	RFC 4871
	Requirements for a DomainKeys Identified Mail(DKIM) Signing Practices Protocol	RFC 5016
	DomainKeys Identified Mail(DKIM) Service Overview	진행
	DKIM Author Domain Signing Practices(ADSP)	진행
	DomainKeys Identified Mail(DKIM) Development, Deployment and Operations	진행

- IETF MARID(Mail Transfer Authorization Records in DNS)는 메일 전송자를 검증하기 위한 DNS 기반의 메커니즘 관련 작업그룹(WG)임. 현재 활동이 중단되었으며, 다음과 같은 Internet Drafts(I-D)만이 결과물로서 존재함

〈IETF MARID WG 관련 문서〉

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

- IEFT SIEVE(Sieve Mail Filtering Language)은 이미 RFC 3028 및 RFC 3421, 3598, 3685, 3894에 기술되어 있는 Sieve Mail Filtering Language에 관한 표준 규격을 개정하거나 갱신하기 위한 목적으로 설립되어 운영 중임. 특히 Spamtest/Virustest와 관련한 RFC 3685의 경우 이의 확장버전 격인 RFC5235에 의해 그 실효성을 상실하였음. 본 WG의 표준 기고서는 다음과 같이 요약할 수 있음

〈IETF SIEVE WG 관련 문서〉

구분	문서이름	상태
IETF SIEVE WG	Sieve: An Email Filtering Language	RFC 5228
	SIEVE Email Filtering: Spamtest and Virustest Extensions	RFC 5235
	Sieve Email Filtering: Variables Extension	RFC 5229
	Sieve Email Filtering: Vacation Extension	RFC 5230
	Sieve Email Filtering: Relational Extension	RFC 5231
	SIEVE Email Filtering: IMAP4flag Extension	RFC 5232
	Sieve Email Filtering: Body Extension	RFC 5173
	Sieve Email Filtering: Editheader Extension	I-D
	Sieve Email Filtering: Reject and Extended Reject Extensions	I-D
	SIEVE Email Filtering: Extension for Notifications	I-D
	Sieve Notification Mechanism: mailto	I-D
	Sieve Notification Mechanism: xmpp	I-D
	Sieve Email Filtering: MIME part Tests, Iteration, Extraction, Replacement and Enclosure	I-D

- IETF SIPPING WG는 SIP(Session Initiation Protocol) 또는 SIP 응용 서비스와 관련된 요구사항을 표준화 하고 있음. 음성 스팸 차단과 관련하여 표준화 문건은 다음과 같음

〈IETF SIPPING WG 관련 문서〉

구분	문서이름	상태
IETF SIPPING WG	The Session Initiation Protocol(SIP) and Spam	RFC 5039
	Requirements for End-to-Middle Security for the Session Initiation Protocol(SIP)	RFC 4189

- IRTF ASRG(Anti-Spam Research Group)는 스팸과 관련한 문제점을 분석하고 다양한 해결 방안의 제안 및 솔루션을 적절성을 평가하기 위한 목적으로 2003년부터 56회 IETF 회의를 기점으로 정식 활동을 시작하였으나, 2004년 60회 IETF 회의를 이후 공식적인 연구 활동의 정도가 미비한 실정임. 최근 아래 표와 같은 Internet Draft가 기고되고 있음

〈IRTF ASRG 스팸 관련 표준 기고서 현황〉

구분	문서이름	작성자	상태
IRTF ASRG	DNS Blacklists and Whitelists draft-irtf-asrg-dnsbl-06	J. Levine, Taughannock Networks.	Publication Requested 2008-07-30
	Guidelines for Management of DNSBLs for Email draft-irtf-asrg-bcp-blacklists-04	C.Lewis, Nortel Networks./M. Sergeant, MessageLabs, Inc.	I-D Exists 2008-07-28

- ITU-T SG17/Q17에서 스팸메일에 관한 표준화에 주력하고 있으며 특히 ETRI가 표준 제안의 주도권을 확보하고 있음. 그 외 참여 국가로는 중국, 스페인, 인도, 미국, 일본 등의 순으로 활동을 보이고 있으며, 기업으로는 Huawei Technologies, ZTE Corporation, China Mobile, MII, SETSI, Lucent Technolgies, Nokia Siemens Networks이 있으나 활동의 빈도가 낮은 편임
- 한편, 이메일 중 80% 이상이 스팸일 가능성에 무게가 실리면서, 스팸에 기인한 ISPs의 직간접적 생산성 저하 및 비용 증가 문제가 대두되자, OECD 회원국 간의 협력을 통한 정부규제, 산업정책, 기술적 솔루션 조율의 필요성이 제기되었음. 현재 OECD Task Force on Spam 활동을 통해 2006년 4월 "Anti-Spam Toolkit of Recommended Polices and Measures" 보고서가 발간되었음. 본 활동은 표준적 성격보다는 OECD 회원국 간에 다자적 협력을 법적, 정책적 측면에서 도모하고자 하는 목적에 보다 초점을 맞추고 있음
- 그밖에 Messaging Anti-Abuse Working Group(MAAWG), Email Authentication Submit, Anti-Publishing Working Group(APWG), Coalition Against Unsolicited Commercial Email(CAUSE) 등에서 단체 표준 활동을 수행 중에 있음

– 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 Q.9/17에서는 2005년에 시작된 두 개의 P2P 보안 분야의 표준화 프로젝트, X.1161(X.p2p-1)과 X.1162(X.p2p-2)가 2008년 9월 완료를 목표로 진행 중에 있음. X.1161은 P2P 보안을 위한 요구사항에 관한 것으로 일본에서 편집을 맡고 있으며, X.1162는 P2P 보안을 위한 세부 기술에 관한 것으로 ETRI에서 편집을 맡고 있음. 양 프로젝트에서 한국, 중국, 일본의 적극적인 참여 속에 표준화 작업이 꾸준히 진행되고 있음

〈P2P 보안 관련 국제 표준-ITU-T〉

구분	표준화 기구	문서명	문서이름	상태	발표월일
P2P 보안	ITU-T	X.1161(X.p2p-1)	Framework for secure P2P(Peer-to-Peer) communications	진행	2008.09(예정)
		X.1162(X.p2p-2)	Security architecture and operations for peer-to-peer network	진행	2008.09(예정)

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

〈P2P 보안 관련 국제 표준–IETF XMPP WG〉

구분	표준화 기구	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

〈P2P 보안 관련 국제 표준–IETF SIMPLE WG〉

구분	표준화 기구	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 진행 중에 있음. 아직까지 RFC는 나오지 않았고 현재 등록된 드래프트 1건으로 아래와 같음

〈P2P 보안 관련 국제 표준–IETF P2PSIP WG〉

구분	표준화 기구	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 개발이 진행되었음

– IPTV 보안

• 2006년 조사에 따르면, 세계적으로 280여 개 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 FG-IPTV는 IPTV에 적용될 수 있는 표준 전반에 대해 검토한 뒤 2007년 7월 현재까지 5번의 회의를 열어 IPTV 표준화를 진행하고 있음. 2007년 7월까지 800여 개의 기고서가 상정되었으며, 이를 통하여 20개의 작업문서가 제정되었으며, 13개의 문서가 living list로 남아있는 상태임. 이 포커스 그룹은 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

• IPTV의 국제 표준화는 ITU-T의 SG(Study Group)13에서 주도하고 있음. SG13은 주로 NGN(Next Generation Network)을 연구하고 있는 그룹으로 IPTV 관련 국제표준화를 추진하고 있는 ITU의 모 그룹임. 지난 2006년 4월 ITU-T TSB국장의 요청에 의해 소집된 IPTV 표준화 자문회의 결의에 따라 구성된 FG(Focus Group)-IPTV에서 2007년 12월까지 총 7차 회의를 개최하여 IPTV 요구사항, 구조 및 보안 분야 등에 대한 표준 초안 문서 20건을 작성하였고 ITU-T 권고로 채택하기 위한 후속 표준화 작업의 효율적인 추진을 위해 2007년 12월 몰타에서 개최된 마지막 FG-IPTV회의에서 IPTV-GSI를 구성하기로 하였음. 2008년 1월 제1차 IPTV-GSI회의가 서울에서 개최되었으며 2008년 12월까지 4차례의 회의를 추가로 개최할 예정임. IPTV-GSI는 ITU_T 내 다수의 연구반에 속한 라포터들이 상호 협력하여 표준화 권고안을 효율적으로 끌어내기 위해 관련 라포터들이 함께 모여 회의하는 Joint Rapporteur Group(JRG)회의를 말함

• IPTV-GSI에서 IPTV 보안분야의 요구사항 초안이 작성 중에 있으며, 세부내용은 일반적인 IPTV 보안, 콘텐츠 보안, 서비스 보안, 네트워크 보안, 단말 보안 및 가입자 보안 등으로 분류하여 진행 중임

• 미국은 ATIS IIF(IPTV Interoperability Forum) 중심으로 산하에 5개 태스크포스팀(Architecture, Test & Interoperability, QoS, DRM, Metadata)을 통해 상호운용성 확보를 위한 표준확보에 주력하고 있으며

DRM IOP 요구사항, 구조 요구사항, QoS 등 6건 표준개발을 완료하고 주로 QoS/QoE(WG) 및 Contents와 이용자 보호, 보안분야(WG3)의 표준화에 중점을 두고 있음. 미국의 Cisco는 Cable기반의 IPTV 표준화를 위해 노력 중이며 ITU-T SG9 중심으로 진행되고 있는 Cable 기반의 IPTV 표준화를 위해 심혈을 기울이고 있음

- 유럽의 ETSI는 DVB CM(Commercial Module)그룹과 TM-IPI(Technical Module-IP Infrastructure) 그룹을 구성하여 IPTV 미들웨어 등 표준화에 주력하고 있고 DVB 규격을 IPTV 표준으로 적용하기 위해 심혈을 기울이고 있으며 IMS기반의 IPTV규격화를 위한 요구사항 및 구조정립 등 WG1활동에 집중하고 있음. TM-IPI에서는 IPTV Phase I v1.2까지 완료하였으며, v1.4까지 진행할 계획임
- 중국은 CCSA에서 IPTV 표준화연구특별위원회(TC1 SWG2)를 신설하고 IPTV 기술요구사항, STB와 IPTV 서비스 플랫폼 간 인터페이스 등 6건의 표준안을 승인 중이며 추가 15개의 표준안도 작성 중에 있음. 또한, 로열티를 지불해야 하는 표준기술에 대해서는 자체 기술개발 및 국제표준화 제안 등의 형태로 대응하고 있으며, H.264 대신 자체 개발한 AVS코덱을 FG-IPTV를 통해 국제 표준으로 반영하고 "ChinaCrypto"를 중국의 CAS 단일 표준으로 내세워 기술료 지불 문제를 해결하고 있음. 중국의 Huawei는 전 분야에 참여하여 IMS를 기반으로 기존 활용기술의 표준화를 추진 중임
- 일본은 총무성 주도로 IPTV 표준화규격을 작성 중에 있으며, 국제표준화는 NTT가 주도적으로 추진하여 국제표준으로 제안할 예정임. 통신기반, 방송기반, Cable기반의 IPTV표준이 서로 대치중에 있었으나 방송 · 통신 · 가전업계 주요 15개사가 참가하는 IPTV 포럼을 발족하여 공통사양의 IPTV 표준규격을 마련하고 이용자는 이 표준규격에 대응한 TV나 단말을 가지고 있으면 모든 IPTV 사업자의 서비스를 받을 수 있게 됨
- 프랑스의 Alcatel은 기술적으로 IMS기반의 IPTV표준화에 관심이 있음

〈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 MetadataYasuaki	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

〈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 공시한 바 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. 이 중 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

– 신뢰보안서비스(TPM)의 국외 표준화 현황

- TCG에서는 IBM, HP, MS, 후지쯔 등 대형 업체를 중심으로 신뢰 컴퓨팅과 관련한 표준화를 진행하고 있음. TCG에서 진행하고 있는 워크그룹들은 TPM, Mobile, TNC(Trusted Network Connect), Server, Storage, PC Client, Hard Copy, TSS(TCG Software Stack), Virtualized Platform 등의 분야를 포함. 현재 TPM 관련한 표준은 TPM v1.2까지 표준으로 공표되어 있음. TPM의 다음 버전인 TPM.Next는 2007년도부터 규격화를 진행 중에 있음

- 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 신뢰성 있는 컴퓨팅 환경의 요구에 따라 더욱 많은 컴퓨터 회사와 소프트웨어 회사들이 TCPA의 제안을 수용함으로써 2003년에 TCG로 확대됨
- 2008년 7월 현재, Promoter(11), Contributor(90), Adopter(49) 를 포함하여 총 150개 정도의 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, MPWG, Authentication WG, TSS WG, Storage WG, TNC WG, Virtualized Platform WG 등 14개의 워크그룹을 만들어 신뢰 보안을 위한 표준화를 진행 중임
- TCG는 표준화 결과물을 공인된 표준 기구인 ISO의 표준으로 발전시키기 위해 노력 중임

〈TPM 관련 국제 표준화 기구별 기술 문건〉

구분	표준화 기구	문서명	문서이름	상태	발표월일
TPM	TCG	문서번호없음	TCG TPM Specification Version 1.2 Revision 103: Design Principles, Structures of the TPM, TPM Commands	공표	2007.10.
		문서번호없음	TCG Software Stack(TSS) Specification Version 1.2	공표	2007.3.
		문서번호없음	TCG Platform Reset Attack Mitigation Specification, Version 1.0	공표	2008.5.
		문서번호없음	TCG Physical Presence Interface Specification, Version 1.0	공표	2007.4.
		문서번호없음	TCG EFI Platform Specification, Version 1.2	공표	2006.6.
		문서번호없음	TCG EFI Protocol Specification, Version 1.2	공표	2006.6.
		문서번호없음	TCG PC Specific Implementation Specification, Version 1.1	공표	2003.8.
		문서번호없음	TCG PC Client Specific TPM Interface Specification(TIS), Version 1.2	공표	2005.7.
		문서번호없음	TCG PC Client Specific Implementation Specification for Conventional Bios, Version 1.2	공표	2005.7.
		문서번호없음	TCG Protection Profile PC Client Specific Trusted Platform Module, TPM Family 1.2, Level 2, Version 0.94	공표	2008.3.
		문서번호없음	TCG Mobile Reference Architecture, Version 1.0	공표	2007.6.
		문서번호없음	TCG Mobile Trusted Module Specification, Version 1.0	공표	2007.6.
		문서번호없음	Mandatory and Optional TPM Commands for Servers, Version 1.0	공표	2005.3.
		문서번호없음	TCG Generic Server Specification, Version 1.0	공표	2005.3.
		문서번호없음	TCG TNC Architecture for Interoperability, Version 1.3	공표	2008.4.
		문서번호없음	TCG TNC IF-MAP Bindings for SOAP, Version 1.0	공표	2008.4.
		문서번호없음	TCG TNC IF-IMC Specification, Version 1.2	공표	2008.4.
		문서번호없음	TCG TNC IF-IMV Specification, Version 1.2	공표	2007.2.
		문서번호없음	TCG TNC IF-PEP: Protocol Bindings for RADIUS, Version 1.1	공표	2007.2.
		문서번호없음	TCG TNC IF-T: Protocol Bindings for Tunneled EAP Methods, Version 1.1	공표	2007.2.
		문서번호없음	TCG TNC IF-TNCCS: Protocol Bindings for SoH, Version 1.0	공표	2007.5.
		문서번호없음	TCG Credential Profiles Specification, Version 1.1	공표	2007.5.
		문서번호없음	Security Qualities Schema Specification, Version 1.1, Revision 7	공표	2007.5.
		문서번호없음	Verification Result Schema Specification, Version 1.0, Revision 1.0	공표	2007.5.
		문서번호없음	Core Integrity Schema Specification, Version 1.0.1, Revision 1.0	공표	2007.5.
		문서번호없음	Integrity Report Schema Specification, Version 1.0, Revision 1.0	공표	2007.5.
		문서번호없음	Reference Manifest(RM) Schema Specification, Version 1.0, Revision 1.0	공표	2007.5.

(주: TCG는 정형화된 문서 번호 체계를 가지지 않음)

– 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)

· OpenAjax Alliance

· 대표적인 국제 표준화 기구인 ITU-T SG17에서 웹서비스 정보보호 표준화를 수행하고 있으며, OASIS에서 개발한 웹서비스 보안 표준을 수행하여 X.1141(SAML 2.0), X.1142(XACML 2.0)에 대한 표준화를 2006년 완료하였음

· ITU-T SG17에서 2006년 4월에 모바일 웹서비스를 위한 메시지 보안 구조(X.websec-3)에 대한 표준 문서 개발을 한국 주도로 시작했으며, 2007년 말 승인 완료되었음(X.1143)

· ITU-T SG17 Q.9에서는 2008년 상반기에 차세대 웹 보안 표준화 로드맵을 수립한 바 있으며, 이를 기반으로 2008년 하반기부터 차세대 웹 보안 표준 개발을 진행하고 있음. 차세대 웹 보안 표준화 로드맵에는 SOA 기반 통신 서비스를 위한 보안 프레임워크 및 보안 서비스 시나리오, 웹 2.0 기반 통신 서비스를 위한 보안 프레임워크 및 보안 서비스 시나리오, 유비쿼터스 웹 서비스를 위한 보안 프레임워크, 다양한 디바이스 연동을 위한 보안 서비스 시나리오 등이 포함되어 있음

· ITU-T SG17의 다음 회기에 대한 구조조정 작업이 진행되면서 기존 Q.9의 후속 Question인 Secure Application Services Question에서 SOA 기반 서비스를 비롯한 안전한 응용 서비스를 위한 보안 메커니즘, 웹 2.0 및 매쉬업 등의 웹 기반 융합서비스에 대한 보안 메커니즘이 향후 표준화 범위에 포함되었으며, 또 다른 후속 Question인 Secure Ubiquitous Communication Services Question에서 유비쿼터스 환경에서의 웹 기술을 이용한 안전한 통신 및 인터워킹 메커니즘과 프로토콜 등을 향후 표준화 범위에 포함시켰고, 신규 Question인 SOA Question에서 SOA 기반 안전한 통신 및 정책 디스커버리, SOA 기술에 대한 보안 보증 메커니즘 및 보안 평가 기술 등을 향후 표준화 범위에 포함시켜 이에 대한 구체적인 표준 개발이 진행되리라고 예상됨

· ITU-T SG17에서 2008년 9월부터 차세대 웹기반 통신 서비스를 위한 보안 프레임워크(X.websec-4)에 대한 표준 문서 개발이 한국 주도록 시작되었음

· 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 1.2, WS-SecureConversation 1.3, WS-Trust 1.3 등의 명세들이 OASIS에서 표준화되었음

· SAML 2.0과 XACML 2.0은 OASIS에서 표준화 완료된 후 ITU-T SG17에서 표준으로 채택되었으며,

OASIS에서는 현재 XACML 3.0을 표준화하고 있으며 Working Draft 상태임

- W3C의 Web Application Formats Working Group은 클라이언트 측의 웹 애플리케이션 개발을 위한 언어를 표준화하고 있으며, 'Access Control for Cross-site Requests'를 표준화하고 있음. 이 표준은 클라이언트 측에서의 도메인 간 콘텐츠 억세스 제어를 가능하게 해주는 표준 기술로, 현재 워킹 드래프트 상태임
- Web API Working Group에서는 클라이언트 측의 웹 애플리케이션을 위한 표준 API를 개발하고 있으며, 'Network Communication API'를 표준화하고 있음. 현재 에디터 드래프트 상태이며, 드래프트 문서에 보안 부분도 일부 포함되어 표준화되기 시작했음
- W3C에서는 웹 프라이버시 보호를 위해 P3P(Platform for Privacy Preferences) 프로젝트를 수행 중이며, 현재 P3P 1.1 버전 스펙을 개발하고 있고 Working Group 노트 상태이임
- 웹서비스 보안 정책과 관련하여 WS-Policy 1.5가 표준화 완료되었으며, XML Encryption 및 XKMS(XML Key Management Specification) 도 현재 표준화 완료된 상태임. XML 전자서명 표준은 W3C와 IETF가 공동으로 개발하고 있으며, 'XML Signature Syntax and Processing' Second Edition이 개발 중으로 현재 Proposed Recommendation 상태임. Canonical XML 1.1은 2008년 5월 표준화 완료되었음
- 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 애플리케이션 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 수행하고 있음. OMA의 Mobile Web Services WG에서는 무선 디바이스가 OMA 아키텍처상에서 웹서비스 응용을 수행할 수 있도록 하기 위해 관련 연구와 표준화 작업을 진행하였음
- 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
- OpenAjax Alliance는 BEA, 구글, IBM, Oracle, Sun Microsystems 등 개방적이고 상호운용 가능한 Ajax 기반의 웹 기술을 성공적으로 적용하고자 하는 벤더들의 연합으로, Ajax 상호운용성과 관련된 명세서와 오픈 소스 소프트웨어 등을 개발하고 있음
- 다수의 Ajax 라이브러리가 동일한 웹 페이지에 사용될 때의 상호운용성 문제를 해결하기 위해 OpenAjax Hub 1.1 명세를 개발하고 있으며, 보안 TF에서Ajax 및 매쉬업 보안과 관련된 화이트 페이퍼 및 유스 케이스를 개발하고 있음. 또한 Mobile TF에서 모바일 디바이스 API를 개발하면서 이에 대한 보안 명세도 개발하고 있음

· 이밖에, OWASP(Open Web Application Security Project)는 응용 소프트웨어의 보안성 향상을 목적으로 한 오픈 커뮤니티이며, 웹 보안을 위한 가이드라인과 오픈 소스를 개발하고 있음. 웹 어플리케이션 보안의 10가지 보안 취약점에 대한 가이드라인인 Top Ten을 개발하고 있으며, Web 2.0 프로젝트 및 AJAX 응용에 대한 보안 이슈와 이에 대한 보안 방안을 다루는 AJAX Security 프로젝트도 시작 단계임. Sprajax 프로젝트에서는 AJAX 보안 스캐너 공개 소스를 개발하고 있음

- 세계적으로 ITU-T, W3C, OASIS 등에서 웹 보안 관련 표준화를 주도하고 있으며, 국외에서도 웹 2.0 보안은 기술 개발 및 표준화가 시작된지 얼마되지 않았고, 유비쿼터스 웹 보안, 시맨틱 보안, 모바일 웹 2.0 보안 등에 관한 표준 개발은 국외에서도 아직 개발 초기 단계임
- 향후 차세대 웹 기반 서비스의 확산에 따라 이를 위한 보안 표준 기술에 대한 수요도 증가하리라고 예상되며, 차세대 웹 보안 기술 표준화는 향후 ITU-T, W3C 등에서 계속 주도할 것으로 예상됨
- 특히 ITU-T SG17에서 2008년 하반기부터 차세대 웹기반 융합서비스 보안에 대한 국제 표준(ITU-T X.websec-4) 개발이 시작되어 관련 표준화가 활발하게 진행되리라고 예상되며, 2009년부터 ITU-T SG17의 Secure Application Services Question 및 SOA Security Question 등에서 SOA 기반 서비스를 비롯한 안전한 응용 서비스를 위한 보안 메커니즘, 유비쿼터스 환경에서의 웹기반 안전한 통신 및 인터워킹 메커니즘과 프로토콜, SOA 기반 안전한 통신 및 정책 디스커버리, SOA 기술에 대한 보안 보증 메커니즘 및 보안 평가 기술 등 차세대 웹 보안 관련 표준화가 더욱 활발하게 진행될 것으로 전망됨

〈국제 표준화 기구별 기술 문건 – ITU-T〉

구분	표준화 기구	문서명	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.1143(X.websec-3)	Security Architecture for message security in mobile Web Services	제정	2007.11
		X.websec-4	Security framework for enhanced Web based telecommunication services	신규 표준화 항목 채택	2010.11

〈국제 표준화 기구별 기술 문건 – OASIS〉

구분	표준화 기구	문서명	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	2007.11
		–	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

〈국제 표준화 기구별 기술 문건 – W3C〉

구분	표준화 기구	문서명	문서이름	상태	발표월일
웹서비스 보안	W3C	–	XML-Signature Syntax and Processing(Second Edition)	제정	2008
		–	Canonical XML 1.0	제정	2001.3
		–	Exclusive XML Canonicalization Version 1.0	Draft	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

〈국제 표준화 기구별 기술 문건 – OMA〉

구분	표준화 기구	문서명	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 개발 중에 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
  - LI 전반적인 요구사항 정의 관련 표준
  - Handover Interface 및 기능 모듈 관련 표준
  - 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 있다. 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

〈국제 표준화 기구별 기술 문건〉

표준화기구	문서번호	문서이름	상태	발표월일
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
	TR 101 944	Telecommunications Security; Lawful Interception(LI); Issues on IP nterception	V1.1.2	2001.12

표준화기구	문서번호	문서이름	상태	발표월일
ETSI	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) nterface	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
	RFC2803	IETF Policy on Wiretapping	–	2000.5

〈국가 표준화 기구별 기술 문건〉

표준화기구	문서번호	문서이름	국가	발표월일
RtP	TR FÜV(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 발간되었음. 2007년 10월 IT 보안성 보증 프레임워크가, 2008년 5월에는 IT 보안성 평가기준 버전 3.1이 11월에는 바이오 인식 보안성 평가 프레임워크가 표준으로 등록될 예정임

〈IT 보안성 보증 및 평가에 관련 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. 또한 정보보호 거버넌스 분야는 새로운 이슈로 활발한 표준 개발이 예상됨

〈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 대상항목별 현황분석

구분		응용보안
표준화 대상항목		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 – UCC 등 개인화 콘텐츠 및 온라인을 통한 급격한 콘텐츠 시장에 활성화에 따라 음악, 영화 및 동영상 등에 대한 유통 및 저작권 관리, 콘텐츠 재가공/활용성에 대한 검증, 추적, 관리 기술에 대한 요구가 증가
	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 – 불법 콘텐츠에 대한 추적 기술 및 복제 방지 기술과 저작권 보호 기술 등에 대한 상용화가 진행 중
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)
기술개발 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
IPR보유 현황	국내	– 익명 PKI 분야 2건, 불법복제 78건, 지식보안 단말플랫폼 분야 11건, 복합지식 콘텐츠저작권 보호 툴킷 4건 등의 유효 특허 파악됨 – 불법복제를 제외한 타분야에 IPR 확보 집중할 필요 있음
	국외	– 미국 Microsoft와 Digimarc Intel: 지식보호 기술 전분야 다출원 404건 – 유럽 Intertrust Technologies와 Microsoft, SONY와 MATSUSHITA, 삼성 등 비유럽 특허출원(복제방지기술 분야 다수) 28건 – 일본 NTT 익명ID 발급/검증 분야와 불법복제 분야 출원특허 중심으로 83건 유효 특허
IPR확보 가능분야		– 사용자 익명 ID 제공 기술 및 Downloadable-TPM 기반 지식보안 단말, 프로슈머 유통구조를 갖는 계층적 지재권 보호 핵심 IPR 확보 가능
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, OpenCableLab 등
	국내참여 업체 및 기관현황	– ETRI, 삼성전자 등 – SK텔레콤, KT
	국내기여도	– 거의 없음
표준화 수준	국내	– 국외표준 수용 및 표준안 기획
	국외	– 표준안기획 및 표준안항목승인
국내표준화의 인프라 수준(시장요구정도 및 참여도)		– 높음 – 연구소, 학계 및 산업체의 기술 개발 및 표준화 참여가 증가하고 있음

구분		응용보안
표준화 대상항목		VoIP 보안
시장 현황 및 전망	국내	– 2008년 1월 VoIP 번호이동제의 시행으로 가입자가 증가할 것으로 예상됨 – 인터넷전화(VoIP) 도청이나 불법스팸, 서비스거부(DoS) 공격을 막을 수 있는 VoIP 정보보호 기술이 개발돼 올해부터 단계적으로 상용화됨 – 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 단계에 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 키워드 필터링과 같은 기존의 기술 외에 합법적으로 등록된 서버를 통한 통화요청은 연결하되, 등록되지 않은 서버를 통한 통화요청은 사업자망에서 차단하는 등록서버 인증기능과, 스팸으로 의심되는 통화요청 허용치를 초과하는 통화요청은 차단하는 그레이리스트(Gray list) 관리 기능이 포함된 VoIP 스팸대응 기술이 개발되어 상용화를 앞두고 있음
	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)) – 최근 접속설정프로토콜(SIP) 기반 응용서비스에 대한 침입방지시스템이 출시된 사례가 있으며, 이 사례에서 알 수 있듯이 VoIP 응용 프로토콜을 악용하는 사이버 공격을 탐지하고 대응할 수 있는 VoIP서비스에 특화된 정보보호 제품도 필요하게될 것으로 보임
기술개발 수준	국내	– 국내에서는 VoIP 암호화 장비로 본점과 지점간 안전한 통화선로를 설정하는 VPN은 불특정 다수와 착발신 통화를 해야 하는 일반 전화서비스 성격에는 적합하지 않음 – 최근, 불법도청으로부터 인터넷전화 사용자의 통화내용을 보호할 수 있는 음성, 데이터 암호화 기술을 기반으로 VoIP 암호기술과 키관리 기술이 적용된 인터넷 전화기가 개발되어 상용화를 앞두고 있음. – 대량의 비정상적인 전화통화 요청을 차단하며, 사업자망을 외부로부터 숨겨 VoIP 서비스 장비를 보호할 뿐만 아니라 사설 IP환경에서 IP주소가 변동돼도 통화를 유지하는 기능을 제공하는 보안세션제어기술이 개발된 바 있음
	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 진행 중 – 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)
IPR보유 현황	국내	– VoIP 관련 국내 특허는 1999년부터 증가하기 시작하여 약 1000여건이 등록. 이러한 특허 동향은 VoIP 관련 기술의 개발이 외국에 비해 늦었음을 의미 – 국내 특허는 주로 채팅서비스, 컨퍼런스폰 시스템 등 VoIP 응용 분야에 집중됨 – 현재까지 출원/등록된 주요 VoIP 보안기술 관련 국내특허는 30건 정도가 있음
	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 및 표준 개발/검토
	국외	– 표준기획, 표준 제정/개정
국내표준화의 인프라수준 (시장요구정도 및 참여도)		– 높음 – 연구소, 학계 및 산업체의 기술 개발 및 표준화 참여가 증가하고 있음

구분		응용보안
표준화 대상항목		스팸 대책
시장 현황 및 전망	국내	– 스팸은 이제 모든 메시지기반 서비스에서 발생할 수 있는 대표적이고 강력한 공격 수단으로 변모하고 있으며, 내부 PC 감염, 기밀/개인 정보의 유출 등의 치명적 문제를 유발하고 있어 이를 적극적으로 방지할 수 있는 기술적 대책 및 제도적 장치가 크게 요구됨
	국외	– 스팸은 이제 모든 메시지기반 서비스에서 발생할 수 있는 대표적이고 강력한 공격 수단으로 변모하고 있으며, 내부 PC 감염, 기밀/개인 정보의 유출 등의 치명적 문제를 유발하고 있어 이를 적극적으로 방지할 수 있는 기술적 대책 및 제도적 장치가 크게 요구됨
기술 개발 현황 및 전망	국내	– 서비스 업계 별로 고유의 스팸 방지기술 채용
	국외	– MessageLabs, Symantec, Proofpoint, Secure Computing, RSA Security, SSH 커뮤니케이션스, 마이크로소프트, attachmate 등에서 관련 제품을 개발함 – OpenSSH 등의 공개된 소스의 제품도 존재함 – 당 기술은 성숙/적용 단계임
기술개발 수준	국내	– 서비스별 고유 기술 개발
	국외	– 프로토타입 및 일부기술별 성숙단계
	기술격차	– 0~1년
	관련제품	– 지란지교소프트: 스팸스나이퍼 – 컴트루테크놀로지: 클린스팸 – 모비젠: 크레디메일 – 다우기술: 메일와쳐, – 크리니티: 스팸브레이커 – Qovia.inc: VoIP 스팸 대응 기술이 포함된 제품 판매 – BorderWare: SIPassure – Facetime: IMAuditor
IPR보유 현황	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 DKIM WG는 도메일 레벨의 인증 프레임워크 관련된 사항을 표준화 – IETF의 SIEVE WG는 이메일 필터링 언어와 관련된 규격을 표준화 – IETF의 SIPPING WG는 SIP 또는 SIP 응용 서비스와 관련된 요구사항을 표준화 – IETF의 SIP WG는 SIP 프로토콜과 관리 분야의 표준화 – ITU-T SG17/Q17에서는 스팸 방지 관련 가이드라인 표준화
표준화 기구/단체	국내	– ETRI(PEC)
	국외	– IETF, ITU-T
	국내참여 업체 및 기관현황	– ETRI, KISA
	국내기여도	– 높음
표준화 수준	국내	– 국외표준 준용
	국외	– 표준기획, 항목승인, 표준제정/개정국내
국내표준화의 인프라수준 (시장요구정도 및 참여도)		– 높음

구분		응용보안
표준화 대상항목		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 장비 업체들이 P2P 트래픽 제어 시장을 주도하고 있음
기술 개발 현황 및 전망	국내	– 소리바다, 프루나, 피투피아 등 여러 업체에서 P2P 파일 공유 서비스를 제공 – KISTI에서 P2P 기반 분산 컴퓨팅에 관한 프로젝트인 Korea@home가 수행 중 – ETRI에서 유무선 IPv6 기반 P2P 네트워크 정보보호 기술개발 과제 수행 – P2P 보안 관련 기술 분야에서는 (주)아라기술, (주)소만사 등이 패킷 필터링 기술에 기반한 P2P 트래픽을 수집 · 분석 및 제어하는 솔루션을 구축
	국외	– Microsoft는 2001년부터 안전한 파일 공유 시스템 제공을 목적으로 하는 Farsite라는 연구를 진행 중, 또한 최근 Vista에 PC 간 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
기술개발 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
IPR보유 현황	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 1,000여 건을 등록/출원했으며, 일본에서는 KDDI, Microsoft, NEC, Onkyo, Fuji, Hitachi 등의 기업들이 100여 건의 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	– 표준기획 단계
	국외	– 표준안 개발/검토
국내표준화의 인프라수준 (시장요구정도 및 참여도)		– 높음 – 연구소, 학계 및 산업체의 기술 개발 및 표준화 참여가 증가하고 있음

구분		응용보안
표준화 대상항목		IPTV 보안
시장 현황 및 전망	국내	– KT, 하나TV가 IPTV 시범 및 상용 서비스를 개시하였고, LG에서 서비스를 준비 중에 있음 – IPTV 보안은 DRM과 CAS만 고려되고 있음 – DRM/CAS 핵심 기술은 외산이 주를 이루고 있음
	국외	– 전 세계적으로 280여 개의 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 진행 중 – 오버레이 또는 P2P 방식의 멀티캐스트에 대한 기초연구 진행 중
	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)
기술개발 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 진행 중
	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 3년 이상
	관련제품	– 마이크로소프트, NDS, 이데토, 나그라비전, 셀런
IPR보유 현황	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 FG 내에서 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
표준화 대상항목		신뢰보안서비스(TPM: Trusted Computing Module)
시장 현황 및 전망	국내	– TPM 기술에 대해서 필요성은 인지하고 있지만 기술 개발을 적극적으로 추진하고 있는 상태는 아님 – TPM이 장착된 노트북이나 데스크탑 등은 많이 사용하고 있는 상태임 – 이동통신사업자들은 ARM사의 TrustZone같은 기술을 단말에 탑재해 보안 문제에 대응하고 있음. 삼성전자는 자체적인 기술 개발을 진행 중이지만, 상품으로서의 가시화는 아직 미지수인 상황임
	국외	– HP, IBM, MS 등 대형 단말 업체들은 이미 TPM이 탑재된 상용 제품들을 판매함. Infineon사는 많은 TPM 칩을 생산해 이들 단말 업체들에 판매해 오고 있는 상황임 – 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
기술개발 수준	국내	– TPM 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
	관련제품	– IBM에서 생산하는 노트북 제품 – MS사의 WindowsVista – 데스크탑, 노트북 등에 탑재되어 출시되고 있고 그 양이 점점 증가하고 있음
IPR보유 현황	국내	–
	국외	–
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, MTM에 대한 표준화 추진 필요
표준화 기구/단체	국내	– TTA
	국외	– TCG – ISO, 3GPP, OMTP
	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
표준화 대상항목		차세대 웹 보안
시장 현황 및 전망	국내	– 전자거래 등 비즈니스 응용 서비스를 위한 웹서비스 정보보호 기술은 이미 활발히 적용되고 있어 시장이 확대되고 있음 – 국내에서 차세대 웹 기반 서비스가 급속히 확산되고 있고 보안 문제에 대한 심각성이 커지고 있어 향후 관련 시장이 성장하리라고 예상됨 – 국내 웹방화벽 시장은 2006년 100억 규모를 형성하였으며, 2008년도는 320억 규모로 예상되고 있음(2008, 보안뉴스) – 국내 모바일 웹 2.0 보안 기술은 아직 시장이 태동기이나 웹 2.0 기술이 모바일 환경으로 확산되리라고 예상되고 있어 향후 시장이 성장하리라고 예상됨
	국외	– 웹 2.0 기술이 급속히 확산되고 있고 보안 문제에 대한 심각성이 커지고 있어 시장이 성장하리라고 예상됨. 특히 비즈니스 영역 뿐 아니라 통신 사업자 영역에서의 서비스, 모바일 디바이스 서비스 등에도 웹 2.0 기술이 확산되고 있어 이와 관련된 시장이 성장하리라고 예상됨 – 모바일 디바이스 보안 시장은 2011년 연평균성장률이 35%로 예상되고 있음(IDC). 모바일 웹 2.0 보안 기술 시장도 이와 비례하여 성장하리라고 예상됨 – 차세대 웹 보안 기술이 속하는 분야인 웹 애플리케이션 보안 분야에 대한 수요가 전체 정보보호 제품 수요의 20%로 예상됨(IDC) – 웹 애플리케이션 보안 분야는 매년 전년대비 50% 이상 성장할 것으로 예상됨(Frost & Sullivan, 2006) – 모바일 웹 2.0 보안 기술은 아직 시장이 크지는 않지만 웹 2.0 기술이 모바일 환경으로 확산되리라고 예상되므로 향후 시장이 더욱 커지리라고 예상됨 – 유비쿼터스 웹, 시맨틱 보안 기술은 기술 개발 초기 단계로 시장 형성에 다소 시간이 걸릴 것으로 예상되나 유비쿼터스 컴퓨팅 환경으로의 전환에 따라 궁극적으로 수요가 증가하리라고 예상됨
기술 개발 현황 및 전망	국내	– 국내에서도 비즈니스 응용을 위한 주요 XML 및 웹서비스 보안 기술은 ETRI 등에서 개발하였음 – 웹 2.0 보안에 대한 요구사항이 증가하고 있으나 웹 2.0 보안 기술 개발은 웹 방화벽 개발 위주로 이루어지고 있어 아직 기술 개발이 부족한 실정임 – 시맨틱 보안 기술, 유비쿼터스 웹 보안 등의 기술 개발은 아직 이루어지지 않고 있음
	국외	– 비즈니스 영역을 위한 웹서비스 보안 기술은 이미 상용화 수준임 – 통신 사업자 영역에서의 서비스를 위해 SOA, 웹 2.0 기술 도입이 이루어지고 있어 이를 위한 보안 기술 개발이 필요함 – 모바일 웹 2.0 기술은 Nokia 등에서 개발하고 있으며 MS 등에서 디바이스 웹서비스 관련 기술을 개발하고 있음 – 시맨틱 웹 보안 기술 제품 개발은 이루어지고 있지 않으며 웹 2.0 기술 개발은 웹 방화벽 개발에 치중되어 있음
기술개발 수준	국내	– 비즈니스 영역을 위한 웹서비스 보안 기술 및 웹 방화벽 기술은 비교적 높은 편임 – 웹 2.0 보안 기술, 유비쿼터스 웹 보안 기술, 시맨틱 보안 기술은 기술 초기 단계임
	국외	– 비즈니스 영역을 위한 웹서비스 보안 기술 및 웹 방화벽 기술은 비교적 높은 편임 – IBM 등에서 매쉬업 보안 기술 등을 개발하고 있으며, 곧 웹 2.0 보안 기술이 활발히 개발되리라고 예상됨 – 모바일 웹서비스 보안 기술은 기술 성장 단계이며, 모바일 웹 2.0 보안 기술도 아직은 초기 단계이지만 곧 성장하리라고 예상됨 – 시맨틱 보안, 유비쿼터스 웹 보안 기술은 기술 개발 초기 단계임
	기술격차	– 2~3년
	관련제품	– BT Web21C SDK, Parlay-X Gateway – Nokia Web Services Framework – TEROS 웹 애플리케이션 보안 게이트웨이
IPR보유 현황	국내	– 비즈니스 영역에서의 웹서비스 보안은 상당수의 특허 보유 – 웹 2.0 보안 관련 특허는 소수 있지만 시맨틱 보안, 유비쿼터스 웹 보안 관려 특허는 거의 없음
	국외	– 비즈니스 영역에서의 웹서비스 보안은 상당수의 특허 보유 – 웹 2.0 보안 관련 특허는 소수 있지만 시맨틱 보안, 유비쿼터스 웹 보안 관려 특허는 별로 없음
IPR확보 가능분야		– 모바일 웹 2.0 보안 기술, 웹 기반 디바이스 보안 연동 기술, 시맨틱 보안 기술 등
IPR확보 가능성		– 높음
표준화 현황 및 전망		– ITU-T, W3C, OASIS 주도의 표준화 활동이 지속될 것으로 전망됨 – 기존의 비즈니스 영역에서의 웹서비스 정보보호 기술은 이미 성숙된 상태이며, 웹 2.0 보안, SOA 기반 융합 서비스 보안, 유비쿼터스 웹 보안, 시맨틱 보안 등은 아직 국제 표준화도 초기단계에 있어 이에 대한 표준화를 중점적으로 추진
표준화 기구/단체	국내	– TTA, 유비쿼터스 웹 포럼, 모바일 웹 2.0 포럼
	국외	– ITU-T, W3C, OASIS
	국내참여 업체 및 기관현황	– ETRI, KISA, TTA
	국내기여도	– 국내에서 개발하여 제안한 모바일 웹서비스 보안 표준이 ITU-T에서 국제 표준화 완료되었음(X.1143) – 차세대 웹기반 융합서비스 보안 신규 표준화 항목이 ITU-T에서 채택되어 국제 표준 개발중(X.websec-4)
표준화 수준	국내	– 표준기획
	국외	– 표준안 항목승인
국내표준화의 인프라수준 (시장요구정도 및 참여도)		– 높음

구분		응용보안
표준화 대상항목		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 판매 중임
기술개발 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
IPR보유 현황	국내	– 10여 건의 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 – SK텔레콤, KT – 대우통신, 데이콤 – 하나로통신, 머큐리 – KTF, 현대시스콤
	국내기여도	– 거의 없음
표준화 수준	국내	– 국외표준 수용
	국외	– 표준안 기획 – 표준안 항목승인
국내표준화의 인프라수준(시장요구정도 및 참여도)		– 높음 – 통신비밀 보호법 개정안 통과 예상 – 암호화된 데이터에 대한 합법적인 분석방법에 대한 표준화 요구 증대

구분		평가인증
표준화 대상항목		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)
기술개발 수준	국내	– 한국정보보호진흥원(KISA), 한국산업기술시험원(KTL), 한국시스템보증(KOSYAS)에서 정보보호 평가
	국외	– 기준, 가이드 개발
	기술격차	– 1년
	관련제품	–
IPR보유 현황	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/초안 개발 및 검토
	국외	– 권고/초안 개발 및 검토
국내표준화의 인프라수준 (시장요구정도 및 참여도)		– 보통

구분		평가인증
표준화 대상항목		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, 전 세계적으로 인증 발급 건수가 2천여 건이 넘고 있음
기술 개발 현황 및 전망	국내	– 보안관리 관련 지침은 한국정보통신기술협회(TTA)에서 제정하는 정보통신단체표준, 舊 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 개발 중에 있음 – ISO 27000 시리즈의 국제 표준 제정으로 보안관리 분야의 관심 증대와 기술개발이 활성화되고 있으며, 조직의 정보보호 활동을 강화하기 위한 거버넌스 이슈가 새롭게 논의되기 시작하고 있음
기술개발 수준	국내	– 보안관리에 관련하여 다양한 지침, 가이드 등을 개발 · 보급 중에 있고, 보안관리에 관련된 국내표준을 2002년부터 개발하여 실무에 적용하고 있음 – TTA에서 보안관리 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	–
IPR보유 현황	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 개발된 평가와 관리체계 인증에 대한 표준은 모든 분야에 적용될 수 있는 표준으로, 앞으로는 특정 분야에 적용될 수 있는 평가와 보안관리 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/초안 개발 및 검토
	국외	– 권고/초안 개발 및 검토
국내표준화의 인프라수준 (시장요구정도 및 참여도)		– 보통

3. 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 네트워크(BcN, USN) 환경을 기반으로 하므로 이러한 기술에 대한 상호 협력이 필요함

○ 즉, 서비스 및 네트워크 기술과의 원활한 조화를 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 역 검증 할 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 SG17에 국내에서 제출된 기고서를 중심으로 표준화를 진행하고 있음

○ 기존의 IETF, ITU-T SG17 표준화 단체를 중심으로 한 표준화 활동의 추진은 현재까지 다수의 표준 개발의 성과를 낳았으며, 현재 추가적인 표준화 항목의 선정이 요구되고 있는 실정. 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, TPM, 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 개발을 병행하여 수행하는 것이 요구됨

3.1.2. SWOT 분석 및 표준화 추진방향

국내역량요인 / 국외환경요인			강 점 요 인 (S)	약 점 요 인 (W)
		시장	– 고속 인터넷 액세스망 구축으로 다양한 응용서비스가 출현하여 신규 시장이 창출되고 있음 – 일반 기업의 정보보호에 대한 지속적인 투자 확대	시장 – 상대적 협소한 정보보호 시장 – 국내업체간 출혈경쟁 구도
		기술	– 사이버공간에서의 개인정보보호의 정책적 중요성이 부각되어, 이에 부합되는 정보보호 기술개발의 필요성 대두 – ETRI를 통한 선도 기술개발을 통한 핵심 기술 확보 가능	기술 – 기술개발 고급 인력 부족 – 정보보호 기능이 미비한 응용 위주의 IT 제품 생산 – 정보보호 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	**현황분석에 의한 우선순위: 1** – (시장) 잘 정비된 고속 인터넷 인프라를 이용한 IPTV, P2P, VoIP 등의 서비스의 상업화 및 수익창출이 가능 – (기술1) u지식, TPM, 차세대 웹서비스 등의 신규 서비스에 대한 신속한 연구개발을 통해 관련 기술규격 정립 및 상용화 추진 – (표준1) ITU-T, ISO/IEC JTC1, IETF 등을 통한 활발한 정보보호 국제 표준화 활동 역량 강화 – (표준2) IPTV 보안 국제 표준화를 ITU-T를 통하여, VoIP보안은, IETF를 통하여 표준화 추진	**현황분석에 의한 우선순위: 2** – (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 – (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, TPM, VoIP, P2P, SPAM 차단, 차세대 웹서비스 등의 IT 서비스에 대한 보안기술 개발 필요성 증가 – u지식 및 TPM의 경우 아직까지 국내외에서 구체적 성과물 전무 – 핵심 응용서비스를 지원할 수 있는 관련 기술 및 인프라가 확보된 상태임		
	표준	– IPTV 표준안 제정 활동이 ITU-T 에서 한국 주도로 진행 중임 – 디지털콘텐트는 MPEG-21, OMA, OASIS 등을 중심으로 진행 중이나 u지식 정보보호에 대한 활동 및 전문 표준화단체는 전무함		
			SO전략: 공격적 전략(강점사용-기회활용)	SO WO 전략 WT ST WO전략: 만회 전략(약점극복-기회활용)
			ST전략: 다각화 전략(강점사용-위협회피)	WT전략: 방어적 전략(약점최소화-위협회피)
위협요인 (T)	시장	– 기술종속으로 인하여 해외 보안 시장 진입 장벽을 넘지 못함 – 지나치게 폐쇄적인 시장구조	**현황분석에 의한 우선순위: 3** – (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	**현황분석에 의한 우선순위: 4** – (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	– 자본과 기술력을 갖고 있는 비정보보호 장비 및 기술 사업자들이 통합 정보보호 제품 개발 및 출시 등에 의한 국내 시장 잠식 – 응용보안을 관련한 원천 핵심 기술력 부족(세계 100대 보안기업중 국내기업이 5개뿐인 실정)		
	표준	– 국내 정보보호 전문 인력의 부족 – 국제표준안 수용 등의 수동적인 전략으로 자체 IPR 확보가 미비 – 주요 IT벤더들의 적극적인 표준안 제정 참여 및 자체 Alliance 또는 전문단체를 구성하는 추세		

○ 현황분석을 통한 우선순위

- 응용보안 분야로 “u지식정보보호, VoIP 보호, 스팸대책, 안전한 P2P 보안, IPTV 정보보호, 신뢰보안서비스(TPM), 차세대 웹 보안, Lawful Interception” 등의 총 8개의 중점 표준화 항목을 선정함
- 더불어 평가인증 분야로 “정보보호 평가, 보안관리”등의 2개의 중점 표준화 항목을 추가 선정함

○ 표준화 추진방향

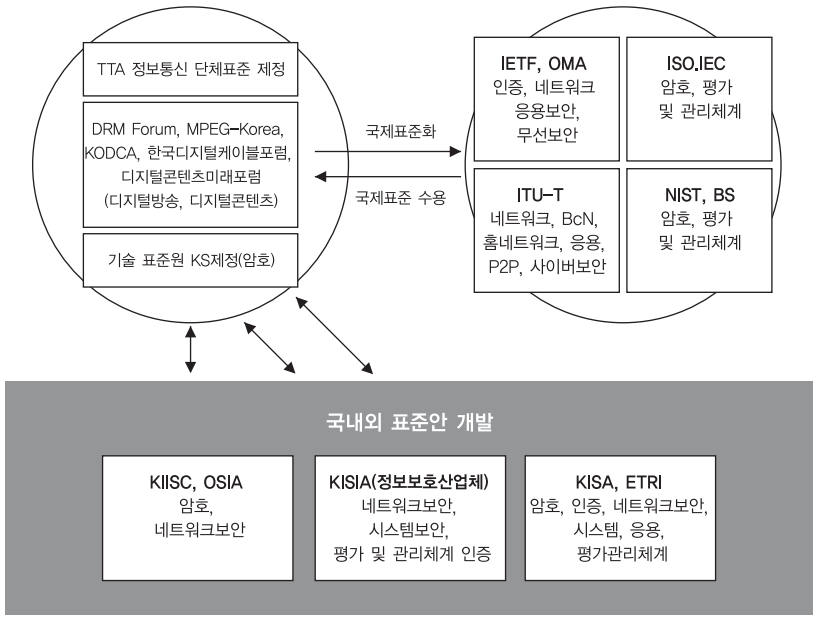
- “u지식, IPTV, P2P, VoIP, TPM, SPAM대책” 등과 같이 시장성이 확대 및 발굴된 응용서비스에 대해서는 아직까지 국제 표준단체의 제정 노력이 일관되지 않은 실정이며, 적극적인 표준화 활동이 미비한 것으로 판단되므로 이를 신규 응용보안 분야로 지정하여 신규 표준 개발에 주력할 필요성이 있음. 이는 기존에 잘 알려지거나 상업용으로 상당히 진전된 기술력을 바탕으로 성숙된 시장을 가진 응용 서비스에 대한 표준화 노력에 비해 상대적으로 주도적 활동을 이끌 수 있을 것으로 기대됨. 이를 위해서는 다음과 같이 전략적이고 신속한 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
- (안전한 P2P 보안) 이미 인터넷 사용자의 대다수가 사용할 정도의 넓은 이용 층을 확보하고 있는 P2P 응용 프로그램 및 네트워크의 보안에 대한 표준화 논의가 ITU-T SG17의 작업반 Q.9에서 X.1161(X.p2p-1)과 X.1162(X.p2p-2) 두 개의 프로젝트로 나뉘어 수행되었음, 또한 IETF의 XMPP, SIMPLE. P2PSIP 작업반과 IRTF의 P2PRG 연구그룹이 관련 표준화를 진행하고 있음
- (IPTV 보안) ITU-T의 IPTV FG에서 이미 800여 개의 기고서가 상정되었고, 이 중 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
- (TPM) 국외 TPM 기술 표준은 이미 완성도가 매우 높으며, 일부 분야에서 표준 개발이 진행중에 있음. 따라

서 국내에서는 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 SOA 및 웹서비스 정보보호 기술 표준은 이미 성숙된 상태이나, 향후 기술 수요가 증가하리라고 예상되는 유비쿼터스 환경하에서의 다양한 서비스 및 디바이스 연동 및 통합, 텔레커뮤니케이션 서비스에서의 융합 서비스를 위한 차세대 웹 보안 기술은 아직 기술 개발 초기 단계임. 따라서 웹 2.0 보안 기술, SOA 기반의 융합서비스 보안 기술, 유비쿼터스 웹 보안 기술, 모바일 웹 2.0 보안 기술 등의 차세대 웹 보안 기술들에 대한 국제 표준화를 적극적으로 추진하는 노력이 필요함
- 특히 2008년 하반기부터 ITU-T SG17에서 차세대 웹기반 융합서비스 보안에 대한 국제 표준 개발이 우리나라 주도로 시작되어 이에 대한 지속적인 활동이 필요하며, 2009년부터 ITU-T SG17의 Secure Application Services Question 및 SOA Security Question 등에서 SOA 기반 서비스를 비롯한 안전한 응용 서비스를 위한 보안 메커니즘, 유비쿼터스 환경에서의 웹 기술을 이용한 안전한 통신 및 인터워킹 메커니즘과 프로토콜, SOA 기반 안전한 통신 및 정책 디스커버리, SOA 기술에 대한 보안 보증 메커니즘 및 보안 평가 기술 등 차세대 웹 보안 관련 표준이 활발하게 진행될 것으로 예상되어 이에 대한 적극적인 표준화 참여 및 대응이 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
- (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. 보안관리 분야는 현재 ISO/IEC JTC1 SC27에서 ISO27000 시리즈를 중심으로 국제 표준화 작업이 한창 진행 중이며, 각국의 많은 보안관리 분야 전문가들이 관심을 갖고 참석하고 있음. 또한 정보보호 거버넌스, 기반시설 등 신규 이슈에 대한 발굴 및 활발한 논의가 진행 중에 있어 국내 보안관리 분야의 경쟁력 강화를 위해서는 전략적 접근을 통한 표준화 작업에 참여할 필요가 있다고 사료됨
- ITU-T의 네트워크 및 응용보안 분야의 완성도가 높은 기존 표준을 선정하여, 국내 표준화를 적극적으로 추진함

3.1.3. 표준화 추진체계

○ 응용보안 및 평가인증 분야



○ 응용보안 표준은 ETRI, KISA, 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 추진

○ 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 개발

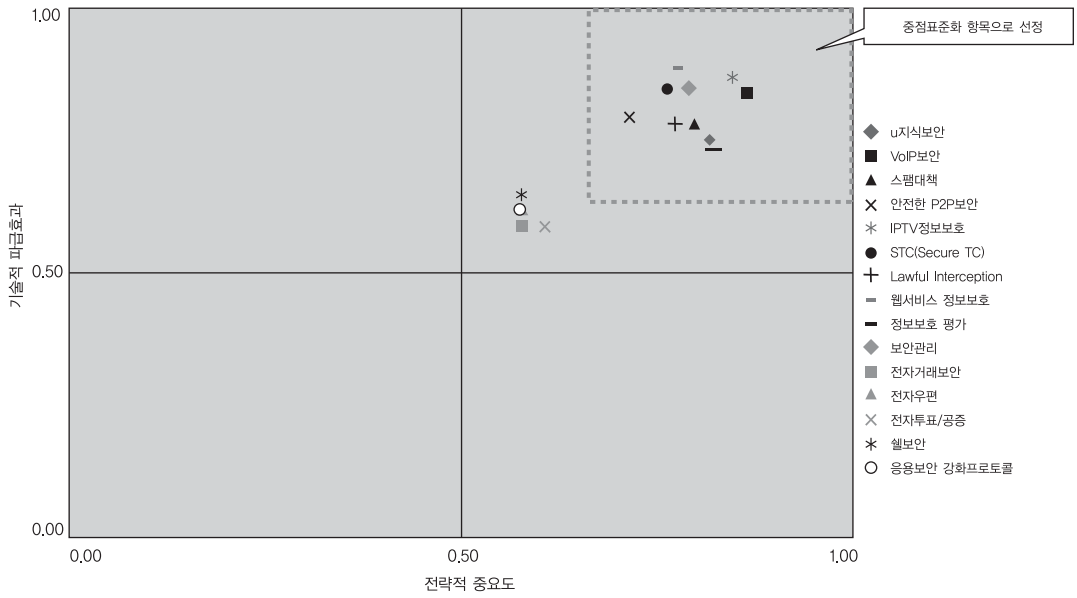
○ 국내 표준 개발절차는 ETRI, KISA, KIISC, 그리고 정보보호 산업체에서 국내 표준안이 개발되며, 이들 중 시기가 긴박한 표준은 ISTF를 통하여 사실표준화를 추진하고, 이후 TTA를 통하여 정보통신단체 표준으로 개발함. 암호 알고리즘은 기술표준원의 KS 표준화함. 정보통신 단체 표준은 TTA TC1 위원회를 통하여 추진

3.2. 중점 표준화항목 선정

3.2.1. 중점 표준화항목 선정방법

중점기술 후보별 전략적 중요도 및 기술적 파급효과 분석

평가지표	전략적 중요도(Priority)						기술적 파급효과(Effect)					
	P1 정부 및 산업체 의지 (국가 산업 전략과의 연관성, 국내기업의 표준화 참여 및 관심도 등)	P2 공공성(사용자 편리성, 중복투자 방지 등)	P3 적시성	P4 기술적 선도 가능성 (국제표준 경쟁력, IPR확보 등)	P5 국제표준화 이슈정도	PI (Priority Index)	E1 기술적 중요도(원천성 등)	E2 타 기술에 파급효과 (연관성, 활용성 등)	E3 시장파급성 및 상용화 가능성(구현가능성 등)	E4 산업적 파급효과(산업화로 인한 이득, 국내 관련산업 규모 및 성숙도 등)	E5 미래 영향력(미래 표준항목에의 적용/응용성)	EI (Effect Index)
평가지표의 중요도 / 표준화 대상항목	10.00	10.00	10.00	10.00	10.00	–	10.00	10.00	10.00	10.00	10.00	–
u지식보안	8.43	8.14	8.00	9.14	7.43	**0.82**	8.29	8.71	8.71	8.71	9.00	**0.87**
VoIP보안	9.29	8.43	9.43	8.14	8.71	**0.88**	8.71	8.29	9.14	8.86	8.14	**0.86**
스팸대책	9.14	8.14	8.86	7.86	7.29	**0.83**	8.00	7.71	8.71	8.43	8.00	**0.82**
안전한 P2P보안	6.86	7.71	8.43	8.00	6.71	**0.75**	8.29	8.14	8.43	8.14	8.14	**0.82**
IPTV정보보호	8.57	8.00	9.29	8.86	8.57	**0.87**	8.71	8.57	9.14	9.29	8.71	**0.89**
신뢰보안서비스(TPM)	7.43	8.14	8.43	7.71	7.86	**0.79**	8.71	8.86	8.57	8.29	8.86	**0.87**
Lawful Interception	7.29	8.43	8.14	7.86	8.57	**0.81**	8.57	8.00	8.14	8.00	8.00	**0.81**
웹서비스 정보보호	8.57	8.14	8.86	7.00	7.86	**0.81**	8.43	8.86	9.43	9.43	8.86	**0.90**
정보보호 평가	8.86	9.00	8.14	8.43	7.86	**0.85**	8.00	7.57	7.43	8.00	8.00	**0.78**
보안관리	8.86	8.86	8.71	7.43	8.29	**0.84**	7.86	7.43	8.00	8.29	8.00	**0.79**
전자거래보안	6.00	6.00	6.00	6.00	6.00	**0.60**	6.00	6.00	6.00	6.00	6.00	**0.60**
전자우편	6.00	6.00	6.00	6.00	6.00	**0.60**	6.00	6.00	6.00	7.00	6.00	**0.62**
전자투표/공증	6.00	7.00	6.00	6.00	6.00	**0.62**	6.00	6.00	6.00	7.00	5.00	**0.60**
쉘보안	6.00	6.00	6.00	6.00	6.00	**0.60**	6.00	6.00	6.00	7.00	7.00	**0.64**
응용보안 강화프로토콜	6.00	6.00	6.00	6.00	6.00	**0.60**	6.00	6.00	6.00	6.00	7.00	**0.62**



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

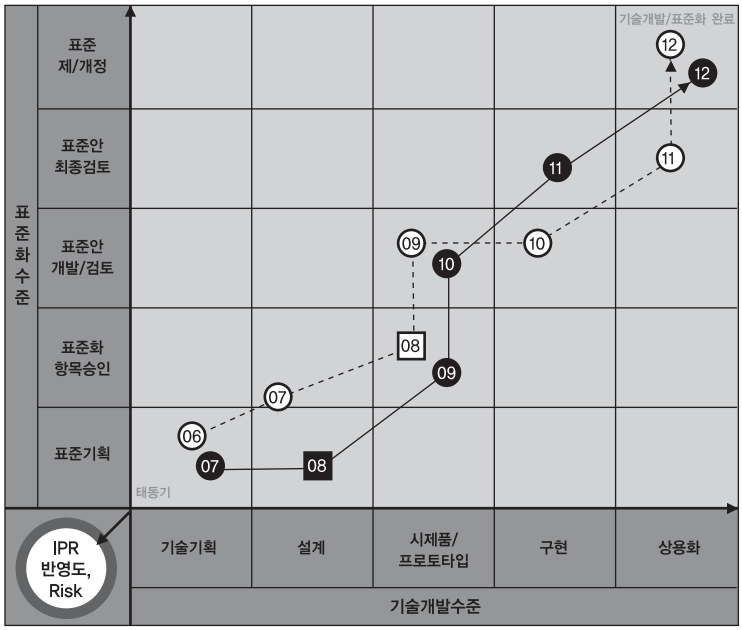
○ 중점 표준화항목별 선정사유

- 응용보안 분야의 경우, 분야별로 다양한 서비스 및 제품에 밀접한 관련이 있어 파급효과가 지대함
- VoIP, IPTV, P2P, 차세대 웹, TPM 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)

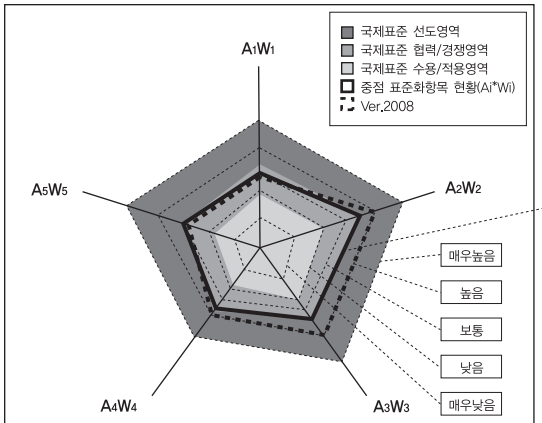


표준화 중요도	국내개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★★★	TTA	ETRI	ITU-T, DVB, OMA

범례

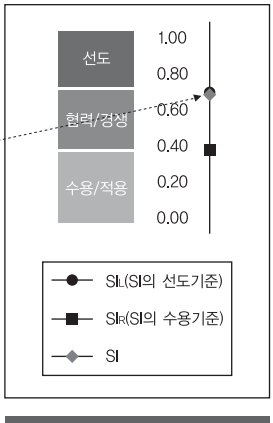
- 08 중점 표준화항목의 국내상태
- 08 중점 표준화항목의 국제상태
- 중점 표준화항목의 국내 표준상태전이
- 중점 표준화항목의 국제 표준상태전이
- 선행표준(선 표준화 후 기술개발)
- 동시표준(표준화 & 기술개발 동시추진)
- 후행표준(선 기술개발 후 표준화)

○ 국제표준화 전략목표 도출



A1 : 국외대비 국내표준화수준
A2 : 국외대비 국내기술개발수준
A3 : IPR확보가능성
점선 : Ver.2008현황
A4 : 국내표준화 인프라수준
A5 : 국제표준화 기여도
Wi : Ai의 가중치

SI(표준화 전략지수)	
SI_L (SI의 선도기준)	0.68
SI_R (SI의 수용기준)	0.37
SI	0.68



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

국제표준 선도(Ver.2008)
⬇
국제표준 선도(Ver.2009)

○ 세부전략(안)

– 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 현황분석에 따른 세부 전략

- MPEG-21, OMA에서는 DRM 표준화를 추진하였고, 국내 표준화를 위해서 TTA에서 DMB-CAS, EXIM 표준화를 추진
- CAS를 SW 형태로 다운로드하여 단말 트러스트를 제공하는 지식보안 기술 표준화와 관련하여 오픈케이브랩스에서 표준화를 추진 중에 있으므로, 국제 표준화에 적극 참여. 음악 보호 파일에 대한 상호연동을 위해 EXIM을 표준화하였으나, 서비스 사업자 간 호환성과 과금 방식에 추가 표준화가 필요한 상태임
- CAS와 DRM 등 개별 기술에 대한 표준화는 제정되어 있으나 연동 측면에서의 고려는 부족하기 때문에 transcoding 기법 역시 고려되어 있지 않으므로 CAS와 DRM의 연동을 위한 인터페이스, 콘텐츠 및 정보에 대한 저작권과 리스트에 대한 관리 방안 및 기기 및 서비스, 사용자에 따른 지능적 Transcoding 기술에 대한 표준화 계획 및 제정이 요구

– 국내외 기술개발 현황분석에 따른 세부 전략

- 국내에서는 SW 및 실명ID 기반의 DRM, CAS 등의 지식보호 솔루션을 개발 및 상용화를 진행하고 있으나, 복합지식 보호 및 프라이버시 보호기술 표준화가 요구
- 전용 디바이스 단위로 권한관리를 추구하는 음악지식(MP3)에 대한 보호 솔루션은 있으나, 자신 소유의 타 디바이스로 구매 지식의 이동 불가로 사용자 불편을 초래하고 있어, 이에 대한 기술 개발과 더불어 표준화가 요구됨
- 사용자 창작/수정/재가공 지식에 대한 지재권보호 및 지분표현 기술 분야 개발이 미약한 수준이므로, 기술개발과 표준화를 동시에 추진
- DRM과 CAS에 급격한 개발과 연구 이후에 시장이나 연구가 둔화되고 있는 상황에서 기술적 연동은 시장의 확산과 기술적인 확장, 서비스의 개발로 이어질 것이며 이를 위해서는 현재 기술들에 대한 표준과 기술의 기업 간의 상호 연계가 수행되어야 하며 이에 대한 정부에서의 정책적 지원이나 관리가 요구됨

– 국내 IPR 보유 현황분석 및 확보가능성 분석에 따른 세부 전략

- 콘텐츠 불법복제 분야는 이미 많은 국외 IPR이 확보된 분야로 볼법복제를 제외한 타분야에 IPR 확보 집중할 필요가 있음
- 미국 Microsoft 등에서 지식보호 기술 전 분야 출원이 400건을 넘고있으므로, 사용자 익명 ID 제공 기술 및 Downloadable-TPM 기반 지식보안 단말, 프로슈머 유통구조를 갖는 계층적 지재권 보호 등의 분야에

서 핵심 IPR 확보를 위해 기술개발을 추진

- CAS, DRM에 대한 IPR은 존재하고 활용되고 있으나 기술적인 부재와 연동을 위한 기업 간의 기술 교류의 부족으로 현재 연동을 통한 기술적 요소, Transcoding 기술 등의 연동을 위한 기술 요소에 대한 IPR은 기술 융복합화와 함께 다양한 분야에서 생성이 가능할 것으로 기대

– 국내 표준화 인프라 수준 분석에 따른 세부 전략

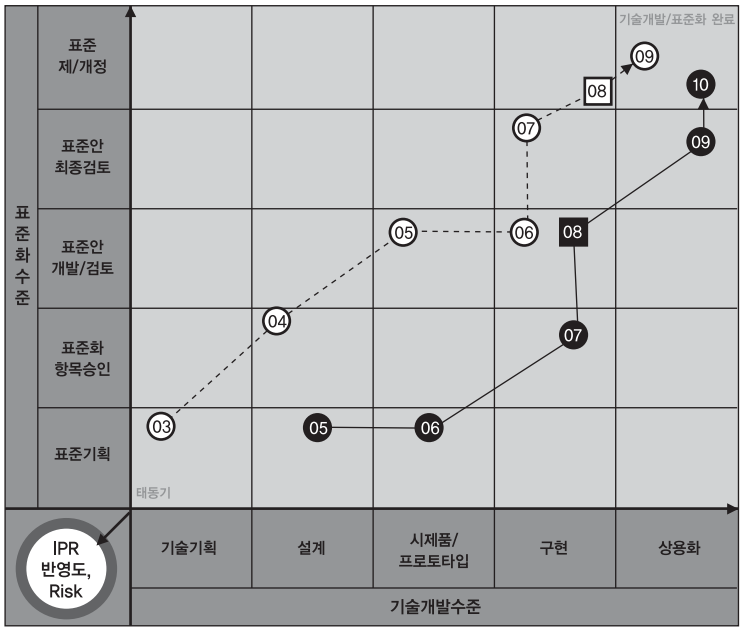
- 국내 인터넷 인프라는 세계 최고 수준이므로, 이를 잘 활용하여 새로운 지식 서비스 산업 및 다양한 비즈니스 모델이 발굴될 수 있도록 기술 개발 및 표준화가 요구됨
- 유무선 네트워크 및 지능형 기기, 사용자 정보에 기반한 통합 시스템이 다양하게 발전되어 있는 상태이므로 연동 기술의 개발과 적용을 통해서 충분히 세계 시장과 표준에 적용이 가능한 상태까지 발전이 가능할 것으로 전망되며 따라서 기술의 융합과 적용을 위한 정책적인 지원이 필요

– 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 추진
- 콘텐츠 산업의 비약적인 발전과 콘텐츠 유통 인프라의 급격한 형성에도 불구하고 유통에 대한 지능적인 관리나 시스템, 기기, 서비스 간의 연동 및 생성에 대한 기술과 표준이 부족하여 현재 CAS나 DRM에 대한 발전이 저해되고 있으므로 이러한 기술의 융복합화는 국제 표준의 선도적인 역할을 수행하도록 진행

3.3.2. VoIP 보안

○ 표준상태전이도(표준화 & 기술개발 연계분석)

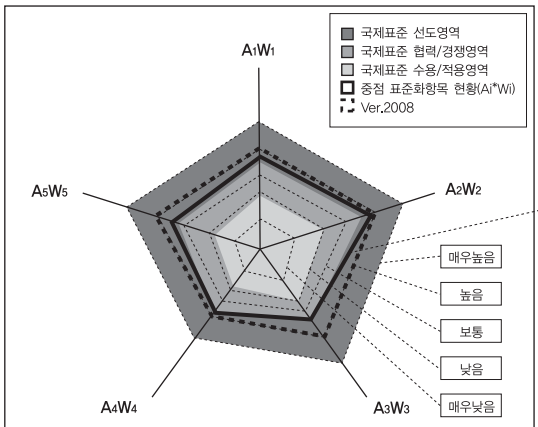


표준화 중요도	국내개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★★	ETRI PEC	ETRI/KISA /숭실대	IETF/ITU-T

범례

- 08 중점 표준화항목의 국내상태
- 08 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)

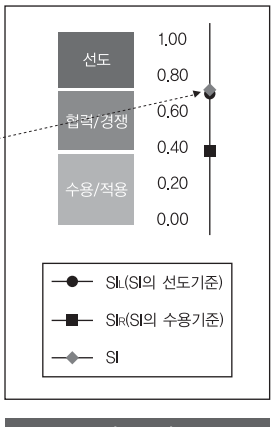
○ 국제표준화 전략목표 도출



A_1 : 국외대비 국내표준화수준
A_2 : 국외대비 국내기술개발수준
A_3 : IPR확보가능성
점선 : Ver.2008현황
A_4 : 국내표준화 인프라수준
A_5 : 국제표준화 기여도
W_i : A_i의 가중치

SI(표준화 전략지수)	
SI_L (SI의 선도기준)	0.68
SI_R (SI의 수용기준)	0.37
SI	0.72

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



국제표준선도
일부수용(Ver.2008)
⬇
국제표준 선도(Ver.2009)

○ 세부전략(안)

– 많은 부분 이미 개발되어 있는 표준을 수용하되, 스팸 대응책 등 분야에서 ITU-T SG17를 통하여 국제 표준화 지속 활동 요구됨

• 프라이버시 보호 메커니즘, 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 참여

• 인증된 아이덴터티 관리, SIP SAML, SIP 스팸 대책 등 신규 항목에 대한 기술개발 및 표준화 추진이 필요

– 국내외 기술개발 현황분석에 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 진행 중

• 국내에서는 VoIP 서비스를 위한 암호/키관리 API 모듈에 연구 개발이 미흡한 실정이므로 기술 개발 및 표준화를 추진

• 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 요구

• 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, 콘퍼런스폰 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 메커니즘, 인증된 아이덴터티 관리, SIP SAML, SIP 스팸 대책 등 신규 분야의 IPR 확보에 집중함

– 국내 표준화 인프라 수준 분석에 따른 세부 전략

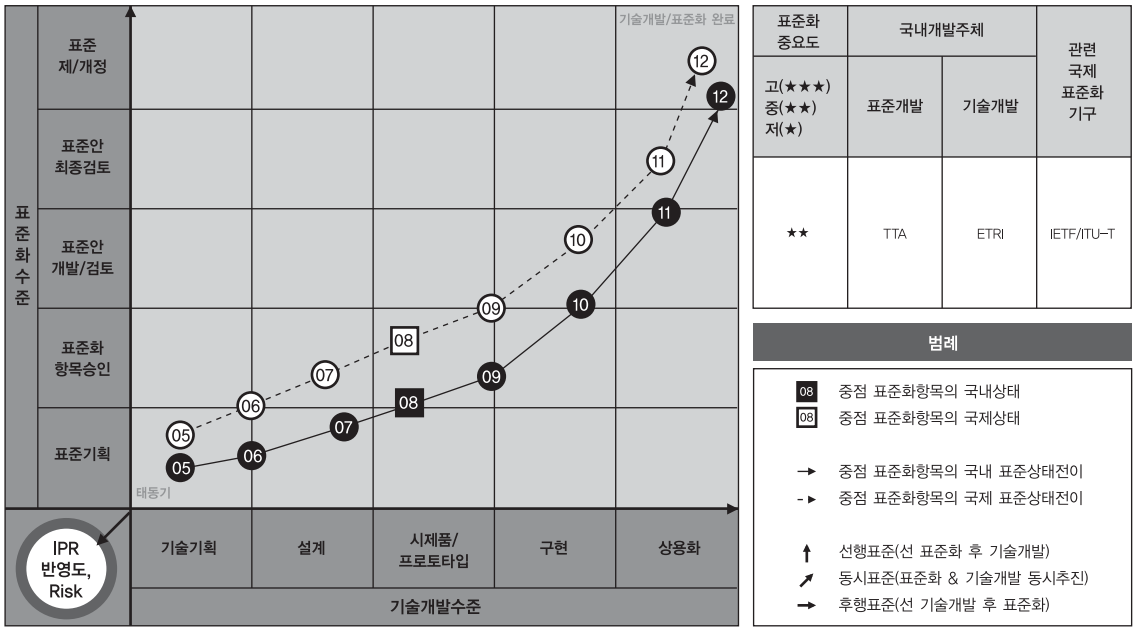
• VoIP 관련 다양한 영역에서 활동하고 있는 산학연 표준전문가들이 스팸 대응책 등 분야에서 ITU-T SG17를 통하여 국제 표준화 활동을 지속적으로 추진함

– 국제표준화 기여도 분석에 따른 세부 전략

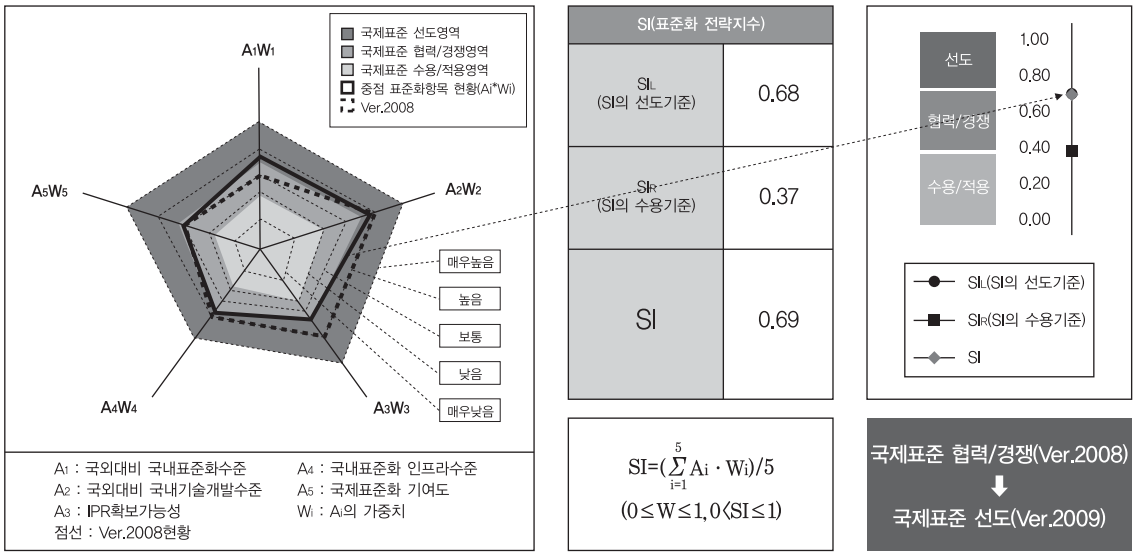
• 많은 부분 이미 개발되어 있는 표준을 수용하되, 스팸 대응책 등 분야에서 ITU-T SG17를 통하여 국제 표준화를 진행

3.3.3. 스팸 대책

○ 표준상태전이도(표준화 & 기술개발 연계분석)



○ 국제표준화 전략목표 도출



○ 세부전략(안)

– SIP, DNS, Domain, Filtering Language 관련 표준은 그 추이를 지켜보고 수용하되, 스팸을 이용한 신규 공격에 대한 스팸 대응책의 분야는 ITU-T SG17를 통하여 국제 표준화 추진이 요구됨

○ 항목별 전략

– 국내외 표준화 현황분석에 따른 세부 전략

- IETF는 SIP, DNS, Domain, Filtering Language 등과 관련된 스팸 이슈에 초점을 맞추고 있으며, 꾸준히 표준안이 최종 승인(RFC)된 바 있으므로, 지속적인 추적을 통한 일부 표준안의 국내 수용이 적절할 것으로 판단
- ITU-T SG17에서는 스팸 관련 Requirement, Framework, Guideline, Filtering System 등의 분야에서 표준 선도를 위해 지속적인 활동이 요구됨. 특히 최신 스팸 공격에 대한 대응 솔루션을 신규 표준 아이템으로 발굴하는 노력이 추가될 수 있을 것으로 기대됨

– 국내외 기술개발 현황분석에 따른 세부 전략

- Anti-Spam 기술 개발 및 상용화는 IBM, MessageLabs, Symantec, Proofpint, Secure Computing, Cloudmark 등을 통해 활발히 진행되고 있음
- 국내의 경우 Spam의 심각성을 인식하고 스팸 차단 전문 업체를 중심으로 시장이 점차 확대되고 있으나, 스팸 발송국 세계 2, 3위를 기록하는 국내 현황과 중국발 스패머의 급속한 신장세를 고려한다면 이에 대응하기 위한 지속적인 기술 개발 및 표준화가 요구됨
- 특히 기업의 산업정보 및 개인 기밀정보의 유출로 스팸이 광범위하게 활용되고 있는 추세이기 때문에, 스팸을 통한 PC 감염 및 자료 유출과 관련한 표준안 신규 제정의 노력이 필요

– 국내 IPR 보유 현황분석 및 확보가능성 분석에 따른 세부 전략

- IPR은 주로 Email 또는 휴대폰 관련 스팸에 집중되어 있어, 신규 매체 및 최신 공격 유형(예: Botnet, Blog, VoIP)을 반영한 IPR 확보를 위한 노력이 요구됨

– 국내 표준화 인프라 수준 분석에 따른 세부 전략

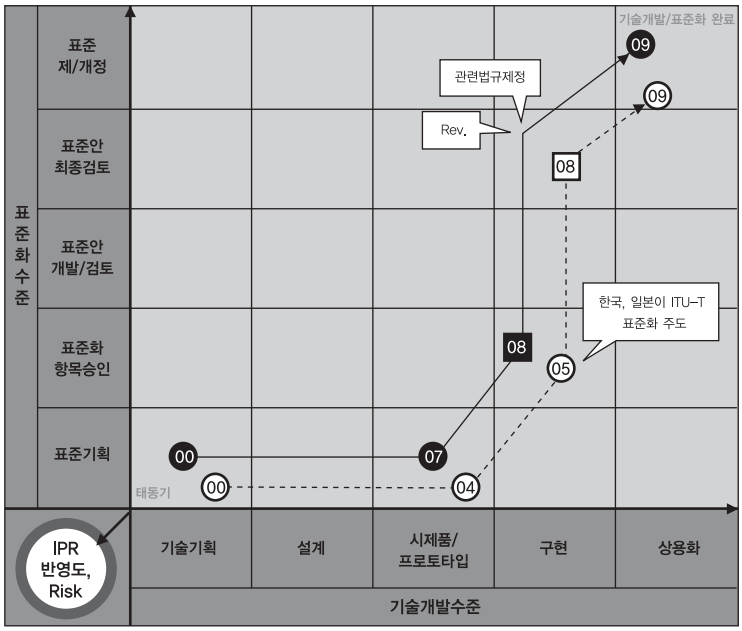
- 이미 바이러스, 악성코드 및 개인정보 유출을 탐지하는 Anti-Spam 통합 보안솔루션 상용화를 통한 시장 진출이 이뤄지고 있으나, ITU-T 및 IETF 스팸 관련 표준 활동은 상대적으로 저조하므로, 지속적으로 표준안 추적을 진행할 필요성이 있음

– 국제표준화 기여도 분석에 따른 세부 전략

- SIP, DNS, Domain, Filtering Language 분야에서의 스팸 관련 표준안은 이미 수년간 진행된 바 있어 국내 표준으로 수용하는 것이 바람직하며, ITU-T SG17을 중심으로 최근 스팸 공격의 특성(예: Zombie PC)을 반영한 신규 표준 아이템의 발굴을 진행함

3.3.4. 안전한 P2P 보안

○ 표준상태전이도(표준화 & 기술개발 연계분석)

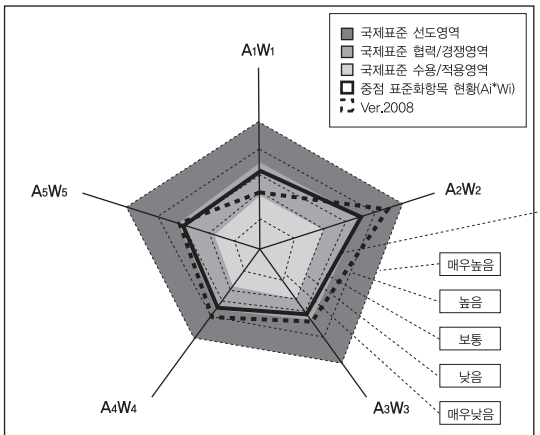


표준화 중요도	국내개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★★	TTA	ETRI	IETF/ITU-T

범례

- 08 중점 표준화항목의 국내상태
- 08 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)

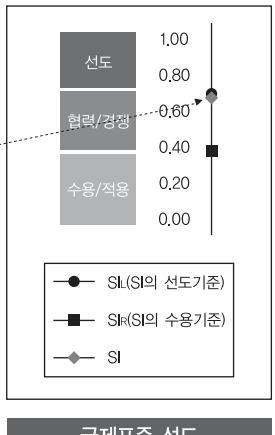
○ 국제표준화 전략목표 도출



A1 : 국외대비 국내표준화수준
A2 : 국외대비 국내기술개발수준
A3 : IPR확보가능성
점선 : Ver.2008현황

A4 : 국내표준화 인프라수준
A5 : 국제표준화 기여도
Wi : Ai의 가중치

SI(표준화 전략지수)	
SI_L (SI의 선도기준)	0.68
SI_R (SI의 수용기준)	0.37
SI	0.66



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

$$(0 \le W \le 1, 0 < SI \le 1)$$

국제표준 선도
일부수용(Ver.2008)
⬇
국제표준 협력/경쟁(Ver.2009)

○ 세부전략(안)

– IM(Instance Message)관련 표준화는 IETF에서 완료가 되었고, 보안 프레임워크 분야는 ITU-T SG17에서 범용 표준 개발이 진행 중에 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 현황분석에 따른 세부 전략

• IM(Instance Message)관련 표준화는 IETF에서 완료가 되었고, 보안 프레임워크 분야는 ITU-T SG17에서 보안 요구사항, 프레임워크를 중심으로 표준화 진행 중에 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 필요

– 국내외 기술개발 현황분석에 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 요구

• 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 필요

– 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 확보

• P2P기반 IPTV 보안 기술 분야와 같이 신규 응용 서비스에 적용 가능한 P2P 보안 기술을 개발하여 IPR을 확보

– 국내 표준화 인프라 수준 분석에 따른 세부 전략

• ITU-T 표준화 활동을 주도하고 있지만, IETF 활동은 저조한 상태이다. 활발한 국내 표준전문가 활용이 필요

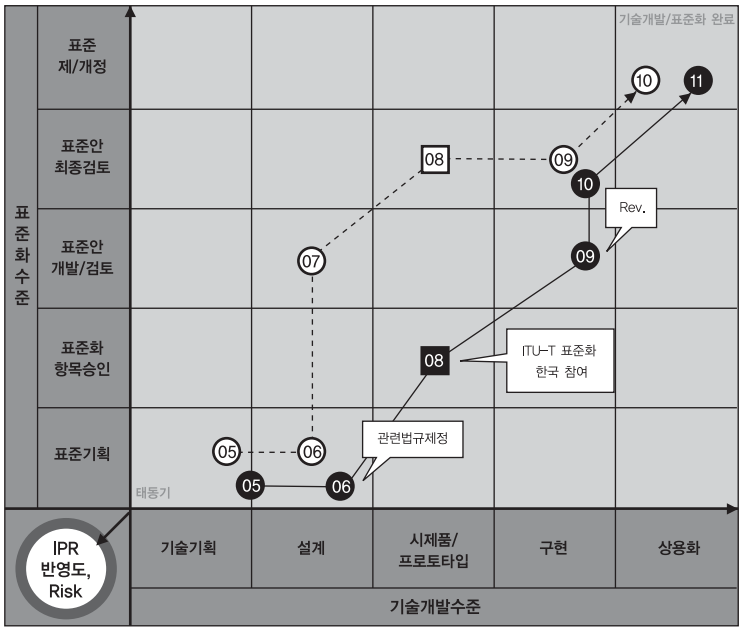
– 국제표준화 기여도 분석에 따른 세부 전략

• ITU-T의 표준화에 기여가 매우 높으므로, 국내 표준전문가의 활동을 장려하고 아이디 보안 등 신규 분야에 표준화를 지속적으로 추진

• 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 필요

3.3.5. IPTV 보안

○ 표준상태전이도(표준화 & 기술개발 연계분석)

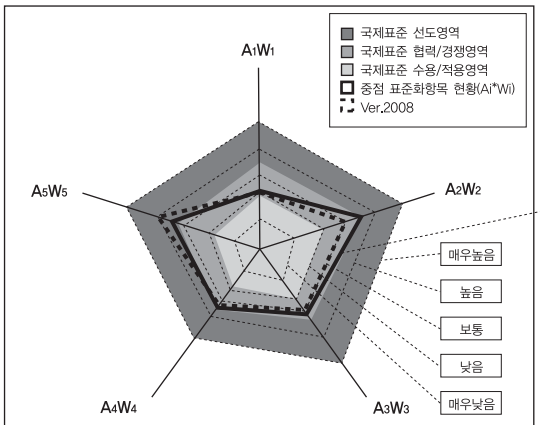


표준화 중요도	국내개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★★	TTA	ETRI	ITU-T

범례

- 08 중점 표준화항목의 국내상태
- 08 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)

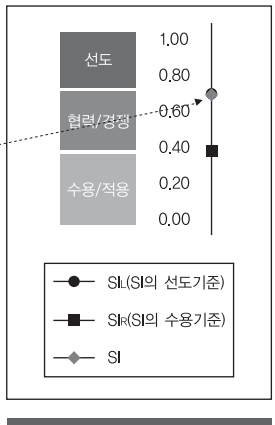
○ 국제표준화 전략목표 도출



A1 : 국외대비 국내표준화수준
A2 : 국외대비 국내기술개발수준
A3 : IPR확보가능성
점선 : Ver.2008현황
A4 : 국내표준화 인프라수준
A5 : 국제표준화 기여도
Wi : Ai의 가중치

SI(표준화 전략지수)	
SI_L (SI의 선도기준)	0.68
SI_R (SI의 수용기준)	0.37
SI	0.68

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



국제표준 선도
협력/경쟁(Ver.2008)
⬇
국제표준 선도(Ver.2009)

○ 세부전략(안)

– ITU-T FG-IPTV에 이어 IPTV-GSI에서도 표준화 활동이 전개됨

– 전통적 보안 기술을 IPTV 보안 표준으로 적용 및 보완 활동 필요함

– ITU-T SG17을 통한 표준 활동이 요구됨

- 코드 상호연동 보안 및 프라이버시 보장 메커니즘
- 콘텐츠 보안기술 및 서비스 보안기술의 상호연동 메커니즘

○ 항목별 전략

– 국내외 표준화 현황분석에 따른 세부 전략

- 한국은 ITU-T FG-IPTV에 이어 IPTV-GSI에서 서비스, 망 구조 등 분야를 주도하고 있어 IPTV 보안 분야의 표준화가 필요함. 현재까지는 IPTV 보안 요구사항만 도출된 상태
- IPTV를 위한 암호화, 프라이버시 등 신규 보안 기술 분야의 표준화가 미흡하기 때문에 기술개발과 함께 ITU-T에서 표준화를 추진
- ITU-T에서 오버레이 또는 P2P 방식의 멀티캐스트를 IPTV에 적용하기 위한 기술 표준화가 진행되고 있으므로, 보안 요구사항 및 보안 메커니즘 표준화에 참여가 필요

– 국내외 기술개발 현황분석에 따른 세부 전략

- 국내의 IPTV 응용, 서비스 기술은 뛰어나나 보안 기술 분야에서는 뒤쳐져 있는 상태로, CAS/DRM의 핵심 요소 기술은 외산을 채용하고 있는 실정임. 최근 CAS+DRM 통합과 Downloadable CAS와 같은 분야의 기술개발과 함께 ITU-T에서 표준화를 추진
- IPTV를 위한 암호화, 프라이버시 등 신규 보안 기술 분야의 기초연구가 전무한 상태이므로, 기술개발과 표준화를 동시에 진행
- 국외에서는 여러 분야의 보안 기술들이 개발되고 있으므로 다양한 기술들 간의 상호호환성을 제공하는 표준의 개발이 필요하며, 오버레이 또는 P2P 방식의 멀티캐스트를 IPTV에 적용하기 위한 보안기술 개발도 필요

– 국내 IPR 보유 현황분석 및 확보가능성 분석에 따른 세부 전략

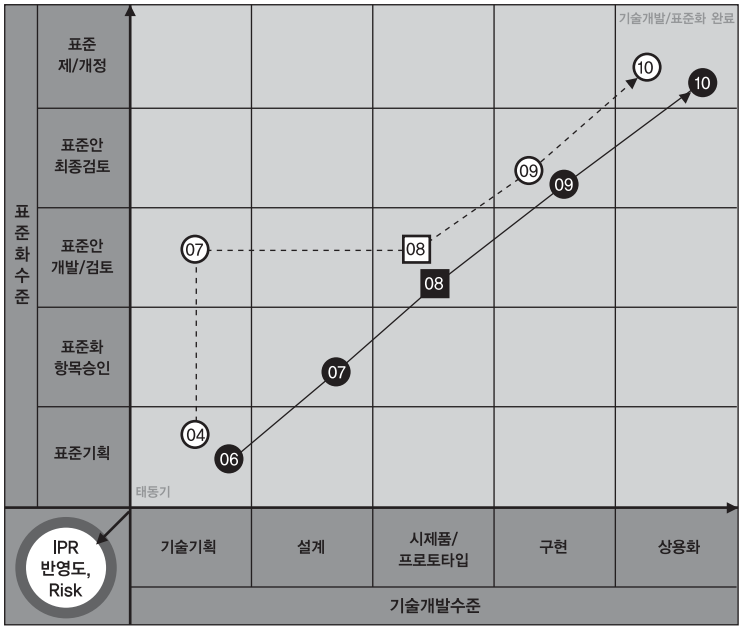
- 국내에서는 IPTV 서비스 및 응용 기술 특허를 다수 보유하고 있으며, 전송망, 인증, 과금, 식별 등 IPTV 보안 특허는 매우 적고, CAS/DRM 특허 중 일부를 보유하고 있음. 국외에서는 IPTV 서비스 및 응용 기술 관련 특허를 다수 보유하고 있으므로, 전송망, 인증, 과금, 식별 등 IPTV 보안 관련 분야의 IPR 확보에 주력
- 투명성, transcodability, 공간/주파수 도메인 암호화, 선택적 암호화 등 보안기술 분야와 프라이버시 보호분야의 IPR 확보에 주력
- IPTV 보안 분야에서는 기존의 CAS/DRM 분야의 경쟁개발보다는 CAS+DRM 연동기술 분야의 집중개발

로 IPR 확보에 주력

- 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 상태이므로, 다양한 보안기술간의 상호호환을 지원하는 표준보안플랫폼 개발을 위하여 산.학 협동을 통한 활발한 국내 표준 전문가 활용이 필요
- 국제표준화 기여도 분석에 따른 세부 전략
  - IPTV 보안 표준화에 기요도가 높은 ITU-T 뿐만 아니라 ATIS IIF, DVB-CM/TM-IPI 등을 통하여 코드 상호연동 보안 메커니즘, 프라이버시 보장 메커니즘 및 상호 호환 보안플랫폼 등 신규 분야에 대한 표준화를 지속적으로 추진
  - 국내 IPTV 서비스사업자와의 긴밀한 협력을 통하여 IPTV 서비스가 원활하게 제공될 수 있는 보안 프레임워크 및 기능 구조를 설계하여 국내 및 국제 표준화에 기여

3.3.6. 신뢰 보안 서비스(TPM)

○ 표준상태전이도(표준화 & 기술개발 연계분석)

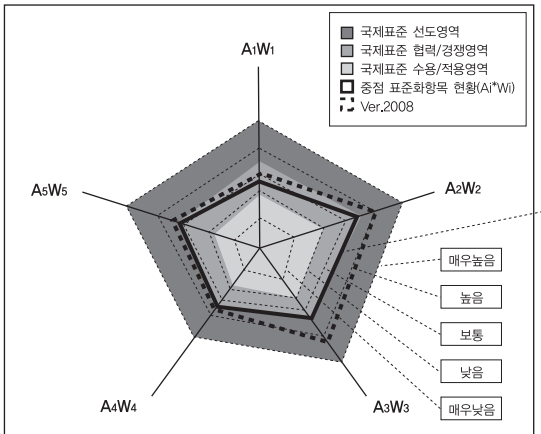


표준화 중요도	국내개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★★	유비쿼터스 씨큐리티 포럼	ETRI	TCG/IETF /3GPP

범례

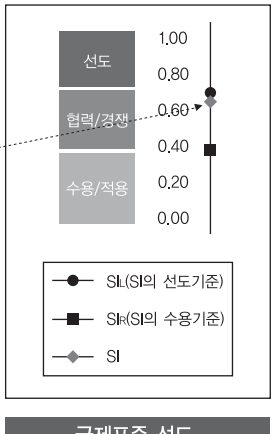
- 08 중점 표준화항목의 국내상태
- 08 중점 표준화항목의 국제상태
- → 중점 표준화항목의 국내 표준상태전이
- -▸ 중점 표준화항목의 국제 표준상태전이
- ↑ 선행표준(선 표준화 후 기술개발)
- ↗ 동시표준(표준화 & 기술개발 동시추진)
- → 후행표준(선 기술개발 후 표준화)

○ 국제표준화 전략목표 도출



A1 : 국외대비 국내표준화수준
A2 : 국외대비 국내기술개발수준
A3 : IPR확보가능성
점선 : Ver.2008현황
A4 : 국내표준화 인프라수준
A5 : 국제표준화 기여도
Wi : Ai의 가중치

SI(표준화 전략지수)	
SI_L (SI의 선도기준)	0.68
SI_R (SI의 수용기준)	0.37
SI	0.63



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

국제표준 선도
협력/경쟁(Ver.2008)
⬇
국제표준 협력/경쟁(Ver.2009)

○ 세부전략(안)

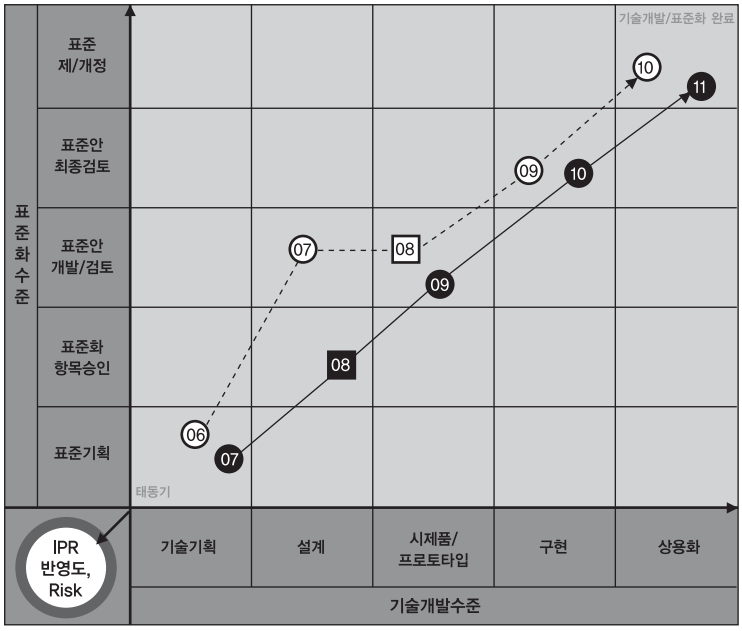
- TCG에서 보다 적극적인 표준화 활동이 요구됨
  - 신뢰보안 프레임워크, 신뢰보안 메커니즘
  - 디바이스/플랫폼 보호, 악성코드 탑재 방지용 무결성 측정 기술(IMVA: Integrity Measurement and Verification Agent), 임베디드 장치 보호 등

○ 항목별 전략

- 국내외 표준화 현황분석에 따른 세부 전략
  - 국내에서는 무선인터넷포럼과 TTA를 통하여 2007년부터 표준화를 진행하고 있으며, TCG의 활동 분야 중 TPM와 mobile phone 분야 등의 표준화를 주도하여 국제표준화를 선도
- 국내외 기술개발 현황분석에 따른 세부 전략
  - 국내에서 모바일용 TPM을 개발하고 있고, 타 업체는 아직 검토 단계이므로, 기술개발 시기에 맞추어 표준화를 진행할 필요가 있음
  - 노트북이나 PC에는 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 추진
- 국내 IPR 보유 현황분석 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 주력
- 국내 표준화 인프라 수준 분석에 따른 세부 전략
  - 국내에서는 이미 기술개발 경험이 풍부한 전문 인력을 확보하고 있으므로, 이를 적극 활용하여 TCG에서 표준화에 참여
- 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 저조. TTA를 통한 국내 표준화 활성화와 함께 ETRI, 삼성, 스프레드텔레콤, 프롬투 등 국내 산,학,연 공동의 표준화 참여가 요구

3.3.7. 차세대 웹 보안

○ 표준상태전이도(표준화 & 기술개발 연계분석)

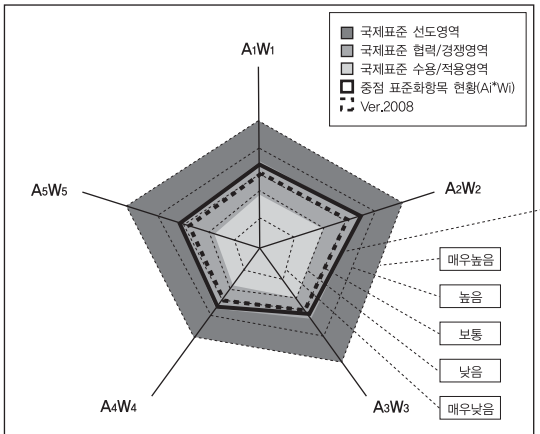


표준화 중요도	국내개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★★★	TTA	ETRI	ITU-T/ W3C/OASIS

범례

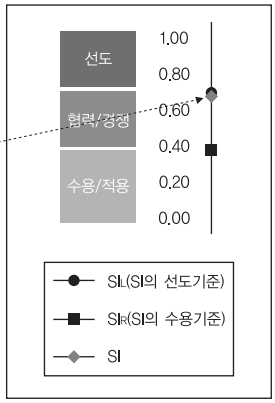
- 08 중점 표준화항목의 국내상태
- 08 중점 표준화항목의 국제상태
- → 중점 표준화항목의 국내 표준상태전이
- -▸ 중점 표준화항목의 국제 표준상태전이
- ↑ 선행표준(선 표준화 후 기술개발)
- ↗ 동시표준(표준화 & 기술개발 동시추진)
- → 후행표준(선 기술개발 후 표준화)

○ 국제표준화 전략목표 도출



A1 : 국외대비 국내표준화수준
A2 : 국외대비 국내기술개발수준
A3 : IPR확보가능성
점선 : Ver.2008현황
A4 : 국내표준화 인프라수준
A5 : 국제표준화 기여도
Wi : Ai의 가중치

SI(표준화 전략지수)	
SI_L (SI의 선도기준)	0.68
SI_R (SI의 수용기준)	0.37
SI	0.68



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

국제표준 선도
일부수용/적용(Ver.2008)
⬇
국제표준 선도(Ver.2009)

○ 세부전략(안)

– ITU-T SG17 및 W3C를 통하여 국제 표준화 선도가 요구됨

• 차세대 웹 기반 융합 서비스 보안 프레임워크, SOA 기반 융합서비스 보안, 유비쿼터스 웹 보안 프레임워크, 시맨틱 보안 서비스, 모바일 웹 2.0 보안, SOA 기반 안전한 통신 및 정책 디스커버리, SOA 기술에 대한 보안 보증 메커니즘 등

○ 항목별 전략

– 국내외 표준화 현황분석에 따른 세부 전략

• ITU-T, W3C, OASIS 주도의 표준화 활동이 지속될 것으로 전망됨

• ITU-T에서는 SG17에서 웹서비스 보안 표준화를 담당하고 있으며, 국내에서 개발한 모바일 웹서비스 보안 구조가 표준화가 완료되었고 2008년 하반기부터 차세대 웹기반 융합서비스 보안에 대한 국제 표준(ITU-T X.websec-4)을 우리나라 주도로 개발하고 있어 차세대 웹 보안 분야 표준화 추진에 유리한 위치에 있음

• ITU-T SG17에서는 2009년부터 시작되는 새로운 회기 동안 차세대 웹 보안, SOA 보안 등에 관한 표준 개발이 본격적으로 추진되리라고 전망됨

• 따라서, ITU-T에서 차세대 웹기반 융합서비스 보안 표준에 대한 지속적인 주도적 개발 및 웹 2.0 보안, SOA 기반 융합서비스 보안, 유비쿼터스 웹 보안 등의 차세대 웹 보안 분야에 대한 신규 표준화 항목 추가 발굴 및 적극적인 국제 표준화 추진이 필요함

– 국내외 기술개발 현황분석에 따른 세부 전략

• 비즈니스 응용에서의 웹서비스 보안 기술 및 웹 방화벽 기술 등은 비교적 기술 개발 결과가 많은 편이나, 차세대 웹 및 SOA 기반 융합서비스 보안 기술, 모바일 웹 2.0 보안 기술, 유비쿼터스 웹 보안 기술, 시맨틱 보안 기술 등은 국내외 적으로 기술 개발 초기 단계이므로, 이러한 분야의 기술개발 및 표준화를 추진

– 국내 IPR 보유 현황분석 및 확보가능성 분석에 따른 세부 전략

• 국내외적으로 비즈니스 영역에서의 웹 보안 기술은 상당수의 특허가 출원되어 있으나, 웹 2.0, 유비쿼터스 웹, SOA 기반 융합서비스, 시맨틱 웹 분야에서의 보안 관련 특허 건수가 많지 않은 실정임

• 따라서 위의 분야에 대한 보안 기술 개발 및 IPR 확보에 주력

– 국내 표준화 인프라 수준 분석에 따른 세부 전략

• 국내 기술 개발 및 표준화는 ETRI, KISA, TTA 등에서 이루어지고 있으며, ITU-T를 통해 국제 표준화를 추진하고 있음

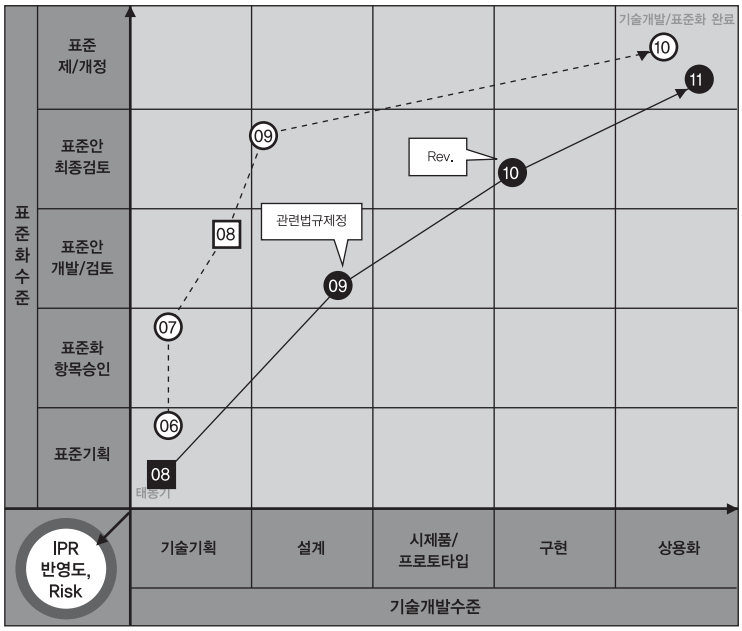
• 우리나라는 세계적으로 인터넷 인프라가 발달하였으며, 웹기반 서비스가 널리 활용되고 있지만 그에 비해 웹 보안 분야에 대한 표준화 전문 인력은 아직 많지 않아 향후 산학연 웹 보안 전문가의 더욱 활발한 표준화 참여가 필요함

– 국제표준화 기여도 분석에 따른 세부 전략

- XML 보안 및 웹 보안, SOA 보안 핵심 기술 들은 W3C 및 OASIS, ITU-T 등에서 활발히 표준화가 진행되어 이미 다수의 표준이 승인된 상태임
- 하지만 세계적으로 웹 2.0 보안, SOA 기반 융합 서비스 보안, 유비쿼터스 웹 보안, 시맨틱 보안 기술 등 차세대 웹 보안 관련 기술은 표준화 초기 단계에 있기 때문에 ITU-T, W3C, OASIS 등에서 보다 적극적으로 표준화에 참여하여 국제 표준화를 추진하는 전략이 필요함
- 특히 국내에서 주도적으로 개발하고 있는 차세대 웹기반 융합서비스 보안 표준에 대한 지속적인 주도적 개발 및 신규 표준화 항목 추가 발굴 필요

3.3.8. Lawful Interception

○ 표준상태전이도(표준화 & 기술개발 연계분석)

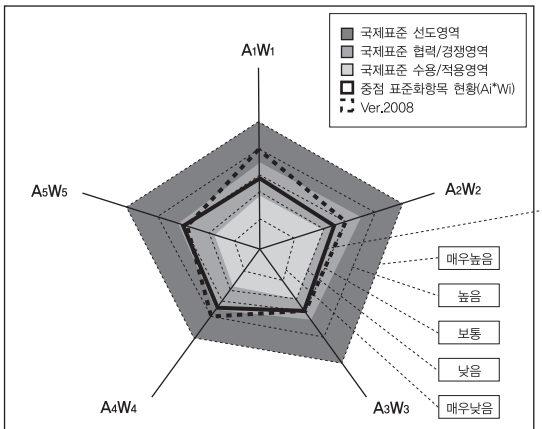


표준화 중요도	국내개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★★	TTA	ETRI	ITU-T

범례

- 08 중점 표준화항목의 국내상태
- 08 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)

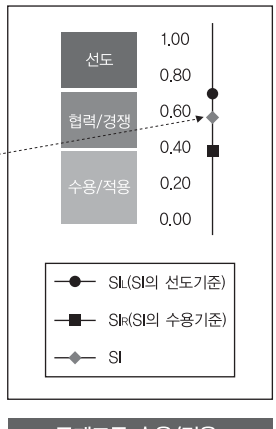
○ 국제표준화 전략목표 도출



A_1 : 국외대비 국내표준화수준
A_2 : 국외대비 국내기술개발수준
A_3 : IPR확보가능성
점선 : Ver.2008현황

A_4 : 국내표준화 인프라수준
A_5 : 국제표준화 기여도
W_i : A_i의 가중치

SI(표준화 전략지수)	
SI_L (SI의 선도기준)	0.68
SI_R (SI의 수용기준)	0.37
SI	0.59



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

$$(0 \le W \le 1, 0 < SI \le 1)$$

국제표준 수용/적용
일부선도(Ver.2008)
⬇
국제표준 협력/경쟁(Ver.2009)

○ 세부전략(안)

– 암호화된 정보에 대한 분석 분야에 있어서 ITU-T SG17을 통한 국제 간(아시아 권역) 표준 개발이 요구됨

○ 항목별 전략

– 국내외 표준화 현황분석에 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 추진

– 국내외 기술개발 현황분석에 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 주력

– 국내 표준화 인프라 수준 분석에 따른 세부 전략

• 인터넷 인프라의 확대와 더불어 국내외적으로 암호화된 정보에 대한 합법적인 분석 기술에 대한 요구가 높으며, 시기적절한 표준의 제정이 뒤따르지 않으면 상용화 시기의 선점을 위해 해외 선도 업체의 기술을 그대로 도입할 가능성이 높음

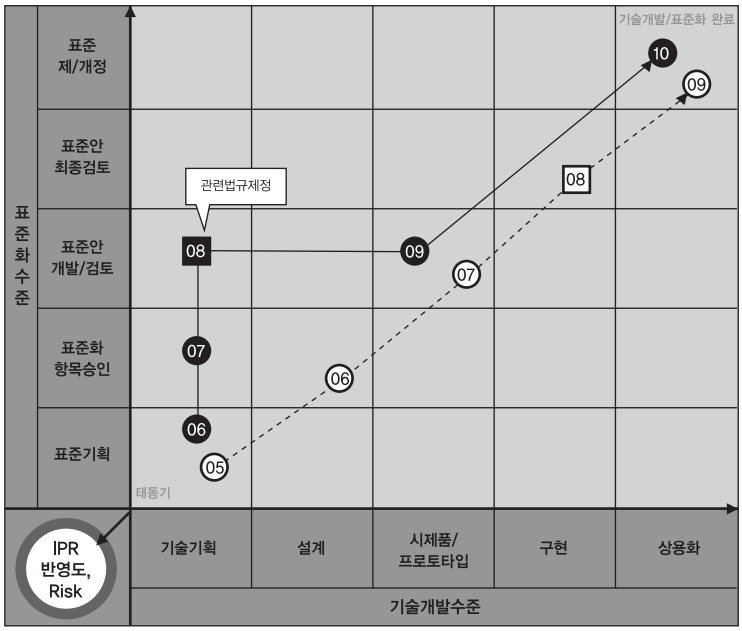
• 수 년 전까지 국제표준화의 중요성이 상대적으로 작았던 것이 사실이나 최근(아시아 권역에서) 국제표준화의 중요성 부각과 함께 국가 간 연동이 가능한 표준 개발이 요구되고 있어, 관련 분야의 시장성이 매우 큰 만큼 국내표준화인프라의 양적인 확장뿐만 아니라 질적인 성장이 필요한 시점으로 판단됨. 따라서 국내표준의 선행활동을 활발히 전개 하고 이를 국제표준으로 연계하는 형태로 체제의 전환이 필요

– 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)

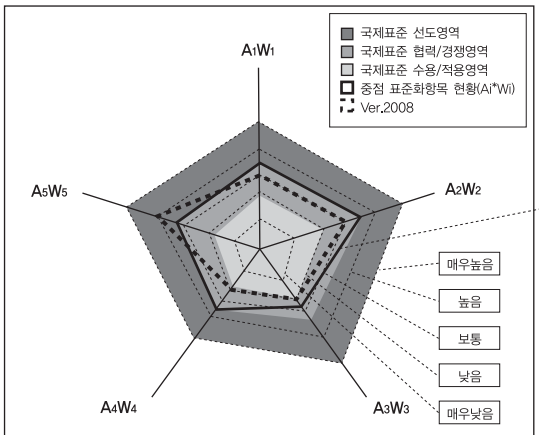


표준화 중요도	국내개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★★	TTA/기술표준원	KISA/ETRI	ITU-T

범례

- 08 중점 표준화항목의 국내상태
- 08 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)

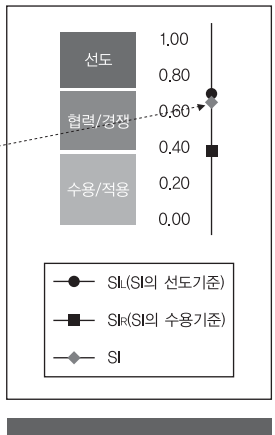
○ 국제표준화 전략목표 도출



A_1 : 국외대비 국내표준화수준
A_2 : 국외대비 국내기술개발수준
A_3 : IPR확보가능성
점선 : Ver.2008현황

A_4 : 국내표준화 인프라수준
A_5 : 국제표준화 기여도
W_i : A_i의 가중치

SI(표준화 전략지수)	
SI_L (SI의 선도기준)	0.68
SI_R (SI의 수용기준)	0.38
SI	0.65



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

국제표준 수용/적용(Ver.2008)
↓
국제표준 협력/경쟁(Ver.2009)

○ 세부전략(안)

– 현재 ISO에서 국제 표준화가 진행되고 있으며, 이에 대한 국제 표준의 주시가 필요하며, 개발된 표준의 국내 수용이 필요함

○ 항목별 전략

– 국내외 표준화 현황분석에 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 현황분석에 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 유리

• 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 현황분석 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 가능

– 국내 표준화 인프라 수준 분석에 따른 세부 전략

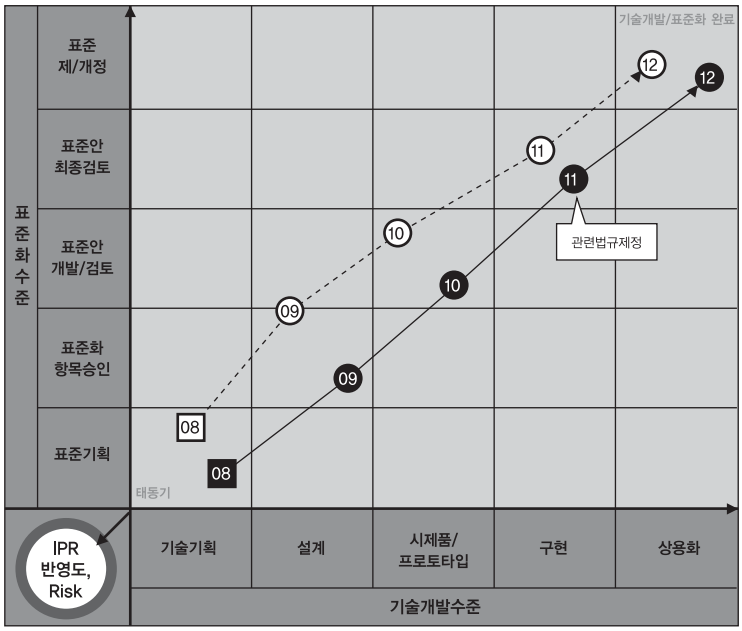
• 기존 국내외 표준 제정 인프라는 충분히 확충되어 있으므로, 통신 분야 및 무선 통신 분야에 적용될 수 있는 정보보호 평가 기술 표준과 제도 정비에 전문 인력을 충분히 활용할 수 있을 것임. 그러나 평가 서비스 운용을 위해 관련 기술 표준에 대한 요구가 매우 높으며, 시기적절한 표준의 제정이 뒤따르지 않으면 해외 선도 업체의 기술을 그대로 도입할 가능성이 높음

– 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 필요

3.3.10. 보안관리

○ 표준상태전이도(표준화 & 기술개발 연계분석)

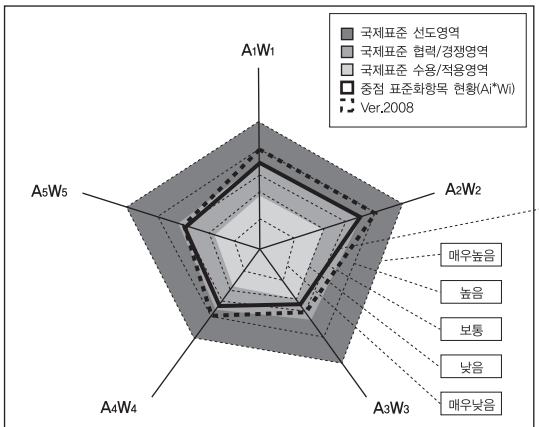


표준화 중요도	국내개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★★	TTA/기술표준원	KISA/ETRI /중앙대	ISO/ITU-T

범례

- 08 중점 표준화항목의 국내상태
- 08 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)

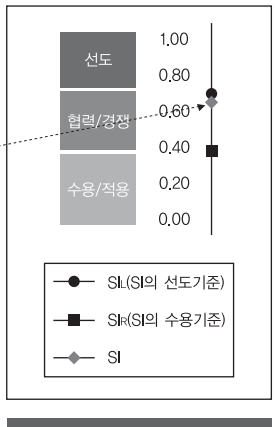
○ 국제표준화 전략목표 도출



A_1 : 국외대비 국내표준화수준
A_2 : 국외대비 국내기술개발수준
A_3 : IPR확보가능성
점선 : Ver.2008현황

A_4 : 국내표준화 인프라수준
A_5 : 국제표준화 기여도
W_i : A_i의 가중치

SI(표준화 전략지수)	
SI_L (SI의 선도기준)	0.68
SI_R (SI의 수용기준)	0.37
SI	0.63



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

국제표준 수용/적용(Ver.2008)
↓
국제표준 협력/경쟁(Ver.2009)

○ 세부전략(안)

– ISO/IEC, ITU-T를 통한 세부항목 표준 활동이 요구됨

• 정보관리, 거버넌스, 유비쿼터스 환경 분야

○ 항목별 전략

– 국내외 표준화 현황분석에 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 요구됨

• 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 현황분석에 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 요구

– 국내 IPR 보유 현황분석 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 반영함으로써 국제 경쟁력을 갖출 수 있음. 이를 위해서는 관련 국제표준 제정에 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 필요

– 국내 표준화 인프라 수준 분석에 따른 세부 전략

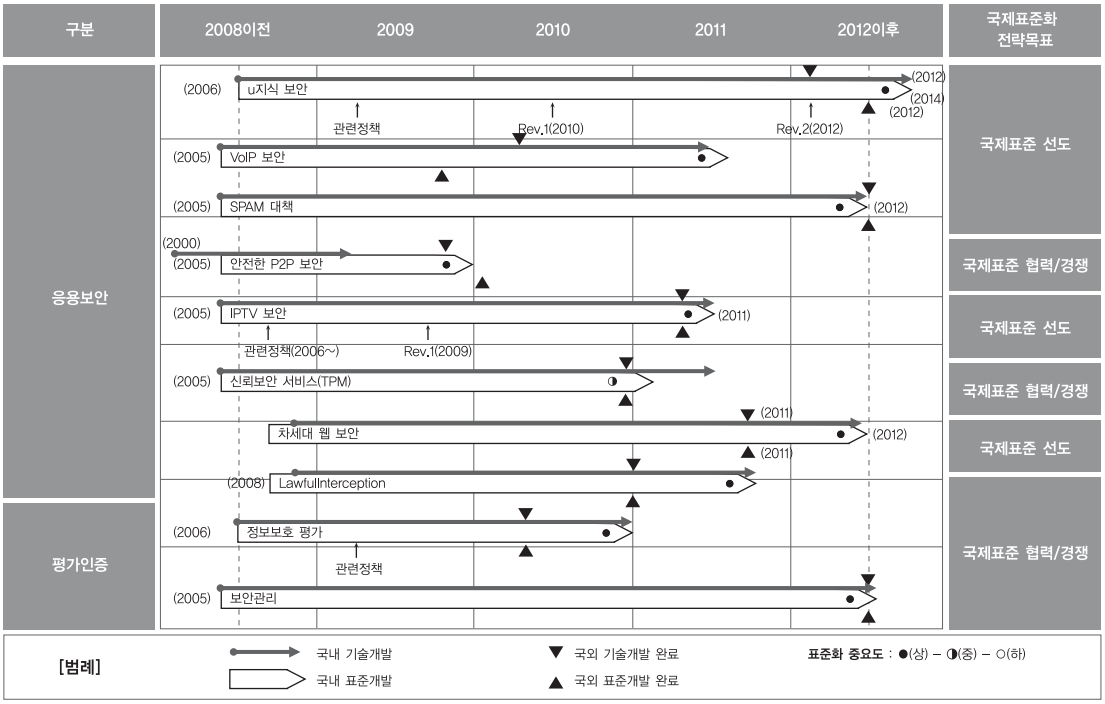
• 상대적으로 국내표준화 인프라 수준이 높은 편으로 평가되나 일부 주요 기술의 표준화를 제외하고 국제표준화 활동 대비 국내 단체 표준제정을 위한 활동이 미미한 상황임. 최근 국제표준화의 중요성 부각과 함께 국내표준화 인프라의 양적인 확장뿐만 아니라 질적인 성장이 필요한 시점으로 판단됨. 따라서 국내표준의 선행 활동과 이를 국제표준으로 연계하는 전략이 필요

– 국제표준화 기여도 분석에 따른 세부 전략

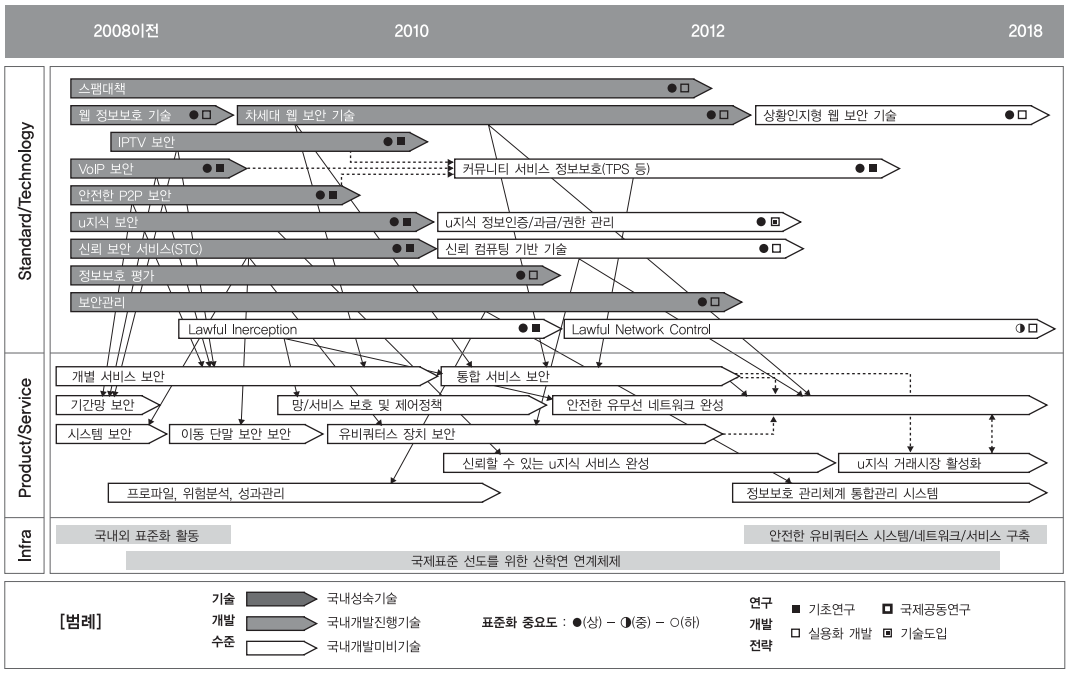
• 국제표준화기여도 분석에 따른 전략으로 보안관리 관련 국제표준회의에서 우리나라의 활동이 저조한 현황임. 최근 IT 환경의 급속한 환경 변화 개인정보보호 등 신규 이슈 등 기존 정보보호 패러다임이 정보보호관리 관점에서 정보보호 거버넌스로 변화되고 있는 추세이므로 이러한 기회를 통해 국내 기술이 국제표준에 반영되도록 하기 위한 국제표준전문가의 활동이 필요

3.4. 중장기 표준화로드맵

3.4.1. 중기('09~'11) 표준화로드맵



3.4.2. 장기 표준화로드맵(10년 기술예측)



[국내외 관련표준 대응리스트]

구분	표준화항목	표준명	기구(업체)	제정연도	재개정 현황	국내 관련표준	국내 추진기구
응용 보안	스팸 대책	Overall aspects of IP Multimedia Application Spam	ITU-T		**		
		Framework for countering IP multimedia spam	ITU-T		**		
		Requirement on countering spam	ITU-T		진행		
		Technical framework for countering e-mail spam	ITU-T		진행		
		Guideline on countering e-mail spam	ITU-T		승인예정		
		Short Message Service (SMS)spam filtering system based on users' rules	ITU-T		*		
		Technical means for countering spam	ITU-T		진행		
		Interactive countering spam gateway system	ITU-T		*		
	안전한 P2P 보안	Framework for secure peer-to-peer 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		

구분	표준화항목	표준명	기구(업체)	제정연도	재개정 현황	국내 관련표준	국내 추진기구
응용보안	안전한 P2P 보안	Timed Presence Extensions to the Presence Information Data Format(PIDF) to Indicate Status Information for Past and Future Time Intervals	IETF		제정		
		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		
	IPTV 보안	IPTV security aspects	ITU-T	2007	진행		
	TPM	TCG TPM Specification Version 1.2 Revision 103: Design Principles, Structures of the TPM, TPM Commands	TCG	2007.10.	진행	없음	TTA
		TCG Software Stack(TSS) Specification Version 1.2	TCG	2007.3.	진행	없음	TTA
		TCG Platform Reset Attack Mitigation Specification, Version 1.0	TCG	2008.5.	진행	없음	TTA
		TCG Physical Presence Interface Specification, Version 1.0	TCG	2007.4.	진행	없음	TTA
		TCG EFI Platform Specification, Version 1.2	TCG	2006.6.	진행	없음	TTA
		TCG EFI Protocol Specification, Version 1.2	TCG	2006.6.	진행	없음	TTA

구분	표준화항목	표준명	기구(업체)	제정연도	재개정 현황	국내 관련표준	국내 추진기구
응용 보안	TPM	TCG PC Specific Implementation Specification, Version 1.1	TCG	2003.8.	진행	없음	TTA
		TCG PC Client Specific TPM Interface Specification(TIS), Version 1.2	TCG	2005.7.	진행	없음	TTA
		TCG PC Client Specific Implementation Specification for Conventional Bios, Version 1.2	TCG	2005.7.	진행	없음	TTA
		TCG Protection Profile PC Client Specific Trusted Platform Module, TPM Family 1.2, Level 2, Version 0.94	TCG	2008.3.	진행	없음	TTA
		TCG Mobile Reference Architecture, Version 1.0	TCG	2007.6.	진행	없음	TTA
		TCG Mobile Trusted Module Specification, Version 1.0	TCG	2007.6.	진행	없음	TTA
		Mandatory and Optional TPM Commands for Servers, Version 1.0	TCG	2005.3.	진행	없음	TTA
		TCG Generic Server Specification, Version 1.0	TCG	2005.3.	진행	없음	TTA
		TCG TNC Architecture for Interoperability, Version 1.3	TCG	2008.4.	진행	없음	TTA
		TCG TNC IF-MAP Bindings for SOAP, Version 1.0	TCG	2008.4.	진행	없음	TTA
		TCG TNC IF-IMC Specification, Version 1.2	TCG	2007.2.	진행	없음	TTA
		TCG TNC IF-IMV Specification, Version 1.2	TCG	2007.2.	진행	없음	TTA
		TCG TNC IF-PEP: Protocol Bindings for RADIUS, Version 1.1	TCG	2007.2.	진행	없음	TTA
		TCG TNC IF-T: Protocol Bindings for Tunneled EAP Methods, Version 1.1	TCG	2007.5.	진행	없음	TTA
		TCG TNC IF-TNCCS: Protocol Bindings for SoH, Version 1.0	TCG	2007.5.	진행	없음	TTA
		Security Qualities Schema Specification, Version 1.1, Revision 7	TCG	2007.5.	진행	없음	TTA
		Verification Result Schema Specification, Version 1.0, Revision 1.0	TCG	2007.5.	진행	없음	TTA
		Core Integrity Schema Specification, Version 1.0.1, Revision 1.0	TCG	2007.5.	진행	없음	TTA
		Integrity Report Schema Specification, Version 1.0, Revision 1.0	TCG	2007.5.	진행	없음	TTA

구분	표준화항목	표준명	기구(업체)	제정연도	재개정 현황	국내 관련표준	국내 추진기구
응용보안	TPM	Reference Manifest(RM) Schema Specification, Version 1.0, Revision 1.0	TCG	2007.5.	진행	없음	TTA
	차세대 웹 보안	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		
		확장성 생성언어 키 관리(XKMS 2.0) 요구사항	TTA	2007	제정		
		확장성 생성언어 키 관리 명세 (XKMS 2.0)	TTA	2007	제정		
		확장성 생성언어 키 관리 명세 바인딩 2.0	TTA	2007	제정		
		웹서비스 응용을 위한 통합 보안 모델 가이드라인	TTA	2007	제정		
		모바일 웹서비스 보안 평가 가이드라인	TTA	2007	제정		
		웹서비스 보안 정책 적용 가이드라인	TTA	2007	제정		
		웹서비스 보안 정책 모델	TTA	2007	제정		

구분	표준화항목	표준명	기구(업체)	제정연도	재개정 현황	국내 관련표준	국내 추진기구
응용 보안	차세대 웹 보안	확장성 접근제어 생성언어 2.0	TTA	2007	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	제정		
		Security framework for enhanced Web based telecommunication services	ITU-T	2010 예정	진행		
		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		
		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		

구분	표준화항목	표준명	기구(업체)	제정연도	재개정 현황	국내 관련표준	국내 추진기구
응용보안	차세대 웹 보안	Web Services Policy 1.5 ? Framework	W3C	2007	제정		
		Web Services Policy 1.5 ? Attachment	W3C	2007	제정		
		The Platform for Privacy Preferences 1.1(P3P1.1) Specification	Working Group Note	2006	진행		
		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		

구분	표준화항목	표준명	기구(업체)	제정연도	재개정 현황	국내 관련표준	국내 추진기구
응용 보안	Lawful Interception	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		
		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	1999	제정		

구분	표준화항목	표준명	기구(업체)	제정연도	재개정 현황	국내 관련표준	국내 추진기구
응용보안	Lawful Interception	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	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		

구분	표준화항목	표준명	기구(업체)	제정연도	재개정 현황	국내 관련표준	국내 추진기구
보안 평가	정보보호 평가	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		진행		
		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		진행		
		ISMS Requirement	ISO/IEC	2005	제정		
		Code of practice for information security management(ISO/IEC 1799)	ISO/IEC	2007	제정		
		ISMS Implementation guidelines	ISO/IEC	2007	진행		
		ISMS measurements	ISO/IEC		진행		
		Information Security Risk management	ISO/IEC		진행		
		Requirement for the accreditation of bodies providing certification of ISMS	ISO/IEC	2007	제정		
		ISMS Auditor Guidelines	ISO/IEC		진행		
		x.1051 – Information security management system Requirements for telecommunications(ISMS-T)	ITU-T	2004	제정		
		Security incident management guidelines for telecommunications	ITU-T		진행		
		Risk Management and Risk Profile Guide	ITU-T		진행		
		Information Security Governance framework	ITU-T		진행		
		정보보호관리체계 수립 지침	TTA	2002	제정		
				2006	개정		
		조직의 정보보호 정책 수립 가이드	TTA	2008	진행		

[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 3

편“, ITU-T SG17, COM17-D193~6-E, April 2006.

[78] ITU-T Recommendation X.1141, “X.1141: Security Assertion Markup Language(SAML 2.0)”, ITU-T SG17, June 2006.

[79] ITU-T Recommendation X.1142, “X.1142: eXtensible Access Control Markup Language Version 2.0 (XACML 2.0)”, ITU-T SG17, June 2006.

[80] ITU-T Recommendation X.1143, “X.1143: Security Architecture for Message Security in Mobile Web Services”, ITU-T SG17, November 2007.

[81] 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.

[82] 염흥열, “ITU-T 모바일 보안 표준 분석 및 전망”, TTA IT Standard Weekly, 2004.4.

[83] 오흥룡, 염흥열, “ITU-T SG17 정보보호 표준화 동향과 Mobile Security 표준 분석”, 한국정보보호진흥원, 2004.12.

[84] 염흥열, “ITU-T SG17 WP2 Q.9(안전한 통신 서비스) 표준화 동향 및 향후 전망”, 한국정보보호진흥원, 2005.12.

[85] 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.

[86] 염흥열, ITU-T가 홈 네트워크 보안 표준을 주도할 수 있을까?”, TTA IT Standard Weekly, 2005.5.

[87] 진병문, 오흥룡, 염흥열, 정교일, “ITU-T SG17 모스크바 회의”, TTA 저널, 99호, 2005.6.

[88] 진병문, 오흥룡, 염흥열, 정교일, “ITU-T SG17 제네바 회의”, TTA 저널, 102호, 2005.12.

[89] 진병문, 오흥룡, 염흥열, 강신각, “2005년 ITU-T SG17 연구동향”, TTA, ITU-T 연구활동 보고서, 2005.12.

[90] TCG 홈페이지, http://www.trustedcomputinggroup.org.

[91] Open TC 홈페이지, http://www.opentc.org.

[92] http://spamlinks.net/

[93] http://domino.research.ibm.com/comm/research_projects.nsf/pages/spam.index.html

[94] http://www.research.ibm.com/spam/links.html

[95] http://www.commtouch.com/Site/Resources/ZombieMonitor.asp

[96] 염흥열, 이재승, “웹 2.0 보안 기술 동향 및 표준화 추진 방향”, TTA 저널, 117호, 2008.5.

[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
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
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
OASIS	Organization for the Advancement of Structured Information Standards
OMA	Open Mobile Alliance
PAN	Personal Area Network
PDA	Personal Digital Assistants
PKI	Public Key Infrastructure
PKI Forum	Public Key Infrastructure Forum
PMI	Privilege Management Infrastructure
RBAC	Role-Based Access Control
RFID	Radio Frequence Identification
RSA	Rivest-Shamir-Adelman)
RSA-OAEP	RSA-Optimal Asymmetric Encryption Padding
SAML	Security Assertion Markup Language
SET	Secure Electronic Transaction
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol

SSL	Secure Socket Layer
SSO	Single Sign-on
TCG	Trusted Computing Group
TCSEC	Trusted Computer System Evaluation Criteria
TLS	Trnansport Layer Security
TPM	Trusted Platform Module
TTA	Telecommunications Technology Association
VPN	Virtual Private Network
W3C	World Wide Web Consortium
WPAN	Wideband Personal Area Network
XACML	eXtensible Access Control Markup Language
XML	eXtensible Markup Language