응용보안/평가인증

기술개요

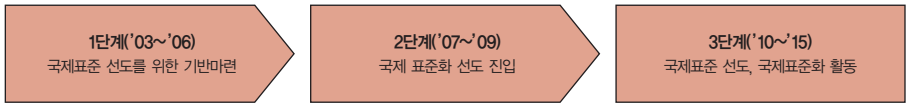
정보보호기술은 정보통신시스템에서 저장 및 유통되는 정보의 기밀성(정보누출 방지)과 무결성(데이터 위 · 변조 방지)을 보장하며, 정보통신 시스템의 안전성과 가용성을 향상시키는데 필요한 기술을 의미하는 것으로, 응용보안은 전자거래 보안, 전자우편, 전자투표/공증, u지식 보안, 쉘 보안, VoIP 보안, IPTV 보안, 차세대 웹 보안으로 분류되며, 평가인증은 정보보호 평가와 보안관리로 구분됨

표준화의 필요성

정보화의 역기능을 방지하기 위한 정보보호기술의 중요성이 증대됨에 따라 사회 각 분야에서 정보보호에 대한 관심이 매우 고조되고 있고, 따라서 정보보호 제품의 설치가 활발히 진행되고 있으나, 상호 운용성을 제고하기 위한 정보보호 제품에 대한 표준의 부재는 안전한 전자상거래와 전자정부의 구현과 유비쿼터스 사회를 구현하기 위한 커다란 장애가 되고 있어 기술경쟁력과 시장지배력을 향상을 위한 표준기술 개발이 요구됨

표준화의 비전 및 목표

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 구축



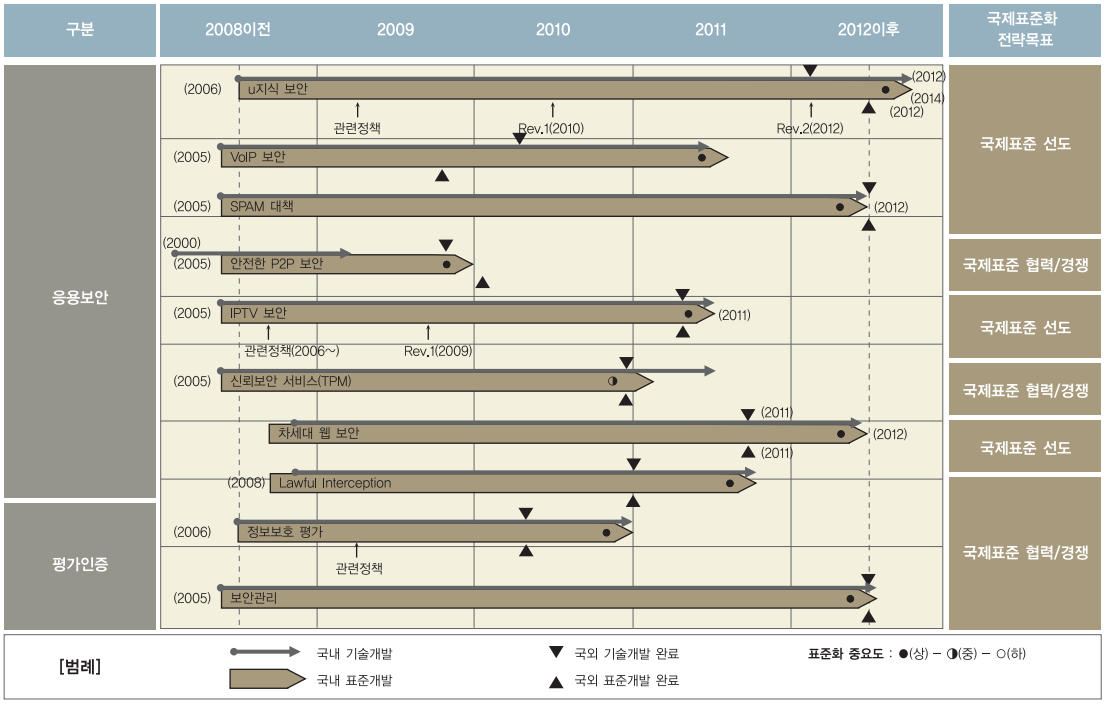
표준화 대상항목

* 0 (매우 낮음) 〈 "전략적 중요도 및 기술적 파급효과" 〈 1 (매우 높음)

표준화 대상항목 (중점 표준화항목)		정의	전략적 중요도	기술적 파급효과	대응 표준화기구	국내 참여 기관/업체	국내 개발주체	
							표준개발	기술개발
응용보안	전자거래 보안	– 전자구매를 위한 보안 기술 표준화	0.60	0.60	–	–	–	–
	전자우편	– 전자우편을 보호하기 위한 기술, 사용 암호 슈트 등의 표준화 항목 정의 – 도메인키 확인 메일(DKIM), Open PGP, S/MIME 메일보안	0.60	0.62				
	전자투표/공증	– 전자 투표 및 전자 공증을 위한 보안 기술 표준화	0.62	0.60				
	u지식 보안	– 유비쿼터스 환경에서 복합콘텐츠에 대한 유통보호 기술 표준화	0.82	0.87	MPEG-21 OMA DVB-CPCM DHWG TV-Anytime	ETRI 삼성전자 SKT KT	TTA	산업체 연구소 학계
	쉘 보안	– 안전한 쉘에 관련 기술 표준화 – 키관리, 보안프로토콜	0.60	0.64	IETF ITU-T	KISA ETRI 숭실대		
	VoIP 보안	– 안전한 VoIP 서비스 제공 기술 표준화 – 제어정보보호, 트래픽보호, 스팸대응	0.88	0.86				
	스팸대책	– 스팸을 제어하기 위한 대책과 가이드라인 표준화	0.83	0.82				
	응용보안 강화 프로토콜	– 안전한 응용 보안 프로토콜 표준화	0.60	0.62		KISA, ETRI ICU, 소만사 VI소프트		
	안전한 P2P 보안	– P2P 보안 구조와 관련 프로토콜 표준화 – 보안 프레임워크, 보안 메커니즘	0.75	0.82				
	IPTV 보안	– IPTV 인프라 보호, 응용 서비스 보호, 프라이버시 보장 기술 표준화	0.87	0.89	ETSI, ITU-T IETF, DVB ATSC 케이블랩스 ATIS IIF TV-Anytime	TTA ETRI KISA 삼성전자 ICU		

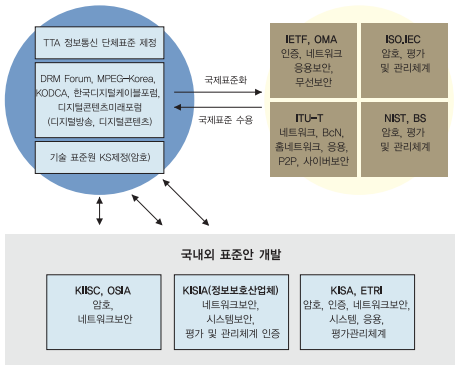
표준화 대상항목 (중점 표준화항목)		정의	전략적 중요도	기술적 파급효과	대응 표준화기구	국내 참여 기관/업체	국내 개발주체	
							표준개발	기술개발
	신뢰보안서비스(TPM)	– 신뢰 컴퓨팅 기술의 관련 표준화 – 신뢰보안 프레임워크, 신뢰보안 메커니즘 – 디바이스/플랫폼 보호, 악성코드 탑재 방지용 무결성 측정 기술(IMVA: Integrity Measurement and Verification Agent), 임베디드 장치 보호 등	0.79	0.87	ISO 3GPP OMTP	ETRI 삼성스프레드T 프롬투	TTA	산업체 연구소 학계
	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	0.81	0.90	ITU-T W3C OASIS	ETRI KISA TTA		
	Lawful Interception	– 유무선 통신 매체를 통해 암호화되어 전송되는 음성, 데이터의 합법적 분석기술 표준화 – 시스템(장비), 알고리즘, 프로토콜 등	0.81	0.81	ETSI ATIS TIA 3GPP IETF	ETRI 전파연구소 LG, 삼성 SKT, KT 대우, 데이콤 하나로 머큐리 KTF, 현대		
평가인증	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 (암호모듈검증 프로그램)	0.85	0.78	ISO/IEC JTC1 SC27 ITU-T	KISA ETRI 중앙대		
	보안관리	– 조직의 목적 및 전략을 지원하고, 정보자산의 보안 관리를 위한 정보보호의 조직화/제도화 등의 표준화 – 정보보호 관리체계 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	0.84	0.79				

중점 표준화항목별 중기(3개년) 표준화로드맵



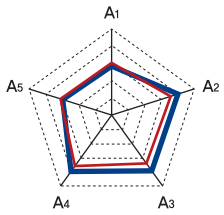
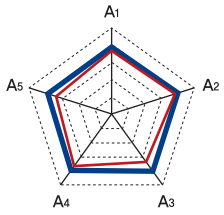
표준화 추진체계

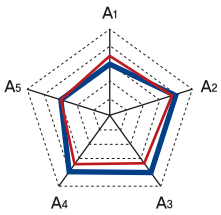
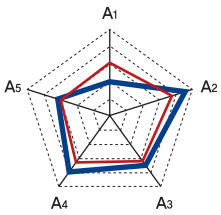
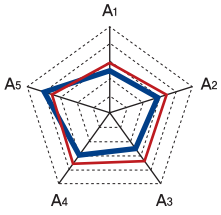
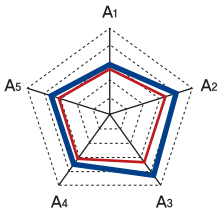
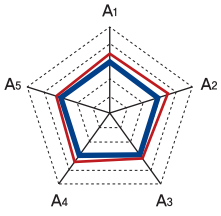
- 응용보안 표준은 ETRI, KISA, KISIA(정보보호산업체)가 표준을 개발하고, 국내 표준은 TTA 및 DRM Forum, MPEG-Korea 등의 디지털방송 및 콘텐트 관련 단체를 통하여, 국제 표준은 IETF, ITU-T, ISO/IEC를 통하여 표준화를 추진
- 평가 및 관리체계 인증 표준은 ISO/IEC, ITU-T를 통하여 국제 표준을 수용하거나 추진하며, BS 표준을 참조하며, TTA를 통하여 국내 표준을 추진하고, KISA와 정보보호 산업체를 통하여 국내 표준을 개발
- 국내 표준 개발절차는 ETRI, KISA, 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

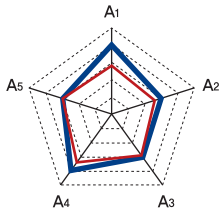
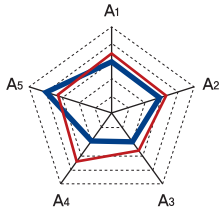
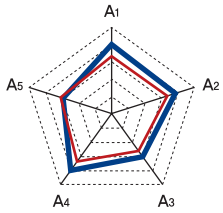


중점 표준화항목별 세부전략(안)

* A_1: 국외대비 국내 표준화 수준, A_2: 국외대비 국내 기술개발 수준, A_3: IPR 확보 가능성, A_4: 국내 표준화 인프라 수준, A_5: 국제표준화 기여도

중점 표준화항목	현황분석 (파란색: Ver.2008, 빨간색: Ver.2009)	세부전략(안)
u-지식보안		국제표준화 전략목표: 국제표준 선도(Ver.2008) → 국제표준 선도(Ver.2009) - 유비쿼터스 환경에서 융복합 콘텐츠 보호 서비스를 제공하기 위한 지식 보호 기술은 선 국내 표준화 추진 후, ITU-T SG17 에서 표준화 요구 - u-지식 보안 기술은 OMA, DVB 등에서 모바일 및 IPTV 등의 지식보호 관련한 De factor 표준화 요구되며, CAS와 DRM 등 개별 기술에 대한 표준화는 제정되어 있으나 연동 측면에서의 고려는 부족, 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 - 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 참여하고, TTA에서 국내 표준화를 진행한 후, ITU-T SG17을 통한 국제표준화를 추진 IPR확보가능분야 | 사용자 익명 ID 제공기술, Downloadable TPM기반 지식보안 단말
VoIP보안		국제표준화 전략목표: 국제표준 선도(일부수용)(Ver.2008) → 국제표준 선도(Ver.2009) - 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, 국제 표준화 활동에 적극 참여 - 인증된 아이덴티티 관리, SIP SAML, SIP 스팸 대책 등 신규 항목에 대한 기술개발 및 표준화 추진이 필요하며, 많은 부분 이미 개발되어 있는 표준을 수용하되, 스팸 대응책 등 분야에서 ITU-T SG17를 통하여 국제 표준화를 진행 IPR확보가능분야 | -

중점 표준화항목	현황분석 (파란색: Ver.2008, 빨간색: Ver.2009)	세부전략(안)
스팸대책		국제표준화 전략목표: 국제표준 협력/경쟁(Ver.2008) → 국제표준 선도(Ver.2009) – 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 요구된다. 특히 최신 스팸 공격에 대한 대응 솔루션을 신규 표준 아이템으로 발굴하는 노력이 추가될 수 있을 것으로 기대 – ITU-T SG17을 중심으로 최근 스팸 공격의 특성(예: Zombie PC)을 반영한 신규 표준 아이템의 발굴을 진행 IPR확보가능분야: Consent Framework, Black/White List 관리, 필터링, 추론기법, 인증방법, 패턴분석
안전한 P2P보안		국제표준화 전략목표: 국제표준 선도(일부수용)(Ver.2008) → 국제표준 협력/경쟁(Ver.2009) – 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 신규 응용 분야에 적용하기 위한 요구사항 및 프레임워크 표준화가 필요 IPR확보가능분야: P2P 트래픽 분석 및 제어기술, 개방환경에서의 피어검색 보안, 자원분산 보안
IPTV보안		국제표준화 전략목표: 국제표준 선도(Ver.2008) → 국제표준 선도(Ver.2009) – ITU-T FG-IPTV에 이어 IPTV-GSI에서도 표준화 활동이 전개되고 있으며, 전통적 보안 기술을 IPTV 보안 표준으로 적용 및 보완 활동 필요함 – 코드 상호연동 보안 및 프라이버시 보장 메커니즘, 콘텐츠 보안기술 및 서비스 보안기술의 상호연동 메커니즘 등 ITU-T SG17을 통한 표준 활동이 요구 IPR확보가능분야: 투명성, Transcodability, 공간/주파수 도메인 암호화, 선택적 암호화 등 신규 보안 기술분야/전송망, 인증, 과금, 식별 등 IPTV에 특화된 보안기술
신뢰보안서비스		국제표준화 전략목표: 국제표준 협력/경쟁(일부선도)(Ver.2008) → 국제표준 협력/경쟁(Ver.2009) – 신뢰보안 프레임워크, 신뢰보안 메커니즘, 디바이스/플랫폼 보호, 악성코드 탑재 방지용 무결성 측정 기술(IMVA: Integrity Measurement and Verification Agent), 임베디드 장치 보호 등TCG에서 보다 적극적인 표준화 활동이 요구 – 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 IPR확보가능분야: 모바일 TPM 개발 분야
차세대웹보안		국제표준화 전략목표: 국제표준 선도(일부수용)(Ver.2008) → 국제표준 선도(Ver.2009) – 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 ITU-T SG17 및 W3C를 통하여 국제 표준화 선도가 요구됨 IPR확보가능분야: 모바일 웹2.0 보안기술, 웹 기반 디바이스 연동기술, 시맨틱 보안기술

중점 표준화항목	현황분석 (파란색: Ver.2008, 빨간색: Ver.2009)	세부전략(안)
Lawful Interception		국제표준화 전략목표: 국제표준 수용/적용(일부선도)(Ver.2008) → 국제표준 협력/경쟁(Ver.2009) – 암호화된 정보에 대한 분석 분야에 있어서 ITU-T SG17을 통한 국제간(아시아 권역) 표준 개발이 요구 – 기존의 감청 분야에서는 통신망 운용 형태에 따른 감청이 주를 이루었으나, 암호화된 데이터가 네트워크를 통해 전송되는 부분에 대해서는 기술 개발 및 표준화가 전무한 상태임으로 기술 개발과 함께 국제 표준화 단체(ITU-T)를 통한 표준 제안을 활발히 추진 IPR확보가능분야 | 암호화된 데이터의 합법적인 분석 방법 및 구조
정보보호 평가		국제표준화 전략목표: 국제표준 수용/적용(Ver.2008) → 국제표준 협력/경쟁(Ver.2009) – 현재 ISO에서 국제 표준화가 진행되고 있으며, 이에 대한 국제 표준의 주시가 필요하며, 개발된 표준의 국내 수용 및 협력/경쟁하는 전략이 필요 – 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 예정 – 새로운 IT 환경을 위한 표준과 제도의 개보수 작업이 진행 중에 있으므로, 적극적으로 표준화에 참여하여 국내기술을 표준에 반영하도록 하는 전략이 필요 IPR확보가능분야 | 정보보호 평가 체계 개발을 통한 도구
보안관리		국제표준화 전략목표: 국제표준 수용/적용(Ver.2008) → 국제표준 협력/경쟁(Ver.2009) – 정보관리, 거버넌스, 유비쿼터스 환경 분야ISO/IEC, ITU-T 를 통한 세부항목 표준 활동이 요구됨 – 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 IPR확보가능분야 | 정보보안 관리체계의 개발을 통한 도구