네트워크 및 시스템보안

기술개요

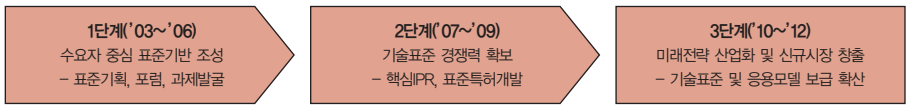
인터넷과 같은 개방형 네트워크 환경에서 전달되는 정보의 위조, 변조, 유출, 무단침입 등을 비롯한 불법 행위로부터 정보를 보호하는 네트워크 보안과, 정보통신 시스템의 안전성과 가용성을 향상시키는데 필요한 정보보호 기술 및 디지털 증거 제공을 위한 기술을 포함한 시스템 보안으로 구성. 네트워크 및 시스템 보안 분야는 유비쿼터스 센서 네트워크(USN) 보안, 휴대인터넷 보안, 홈네트워크 보안, 무선근거리통신망 보안, 이동통신망 보안, 차세대네트워크 보안, 사이버공격 역추적/보안관리, 봇넷대응, 서버 보안, PC 보안, 디지털포렌식 등의 11가지 분야로 구분

표준화의 필요성

정보화의 역기능을 방지하기 위한 정보보호기술의 중요성이 증대됨에 따라 사회 각 분야에서 정보보호에 대한 관심이 매우 고조되고 있고 2006년 6월 CCRA 가입에 따른 공공 보안 시장의 확대를 통해 새로운 형태의 시장 창출을 이루고 있는 시점에서 국내 기술력 및 이를 기반한 IPR 확보는 정보보호 분야의 수명과 공공성 보안 시장의 세계화를 위해서는 표준 기술 개발이 시급히 요구

표준화의 비전 및 목표

정보보호 기술을 적용함으로서, 전자정부의 안전성과 신뢰성 확보, 각종 서버들로 구성되는 공공 분야 정보시스템의 안전성 보장 운영, 정보통신망의 안전한 운영, 개인 PC에 대한 사용자 프라이버시 보호, 기업 정보보호 등을 달성



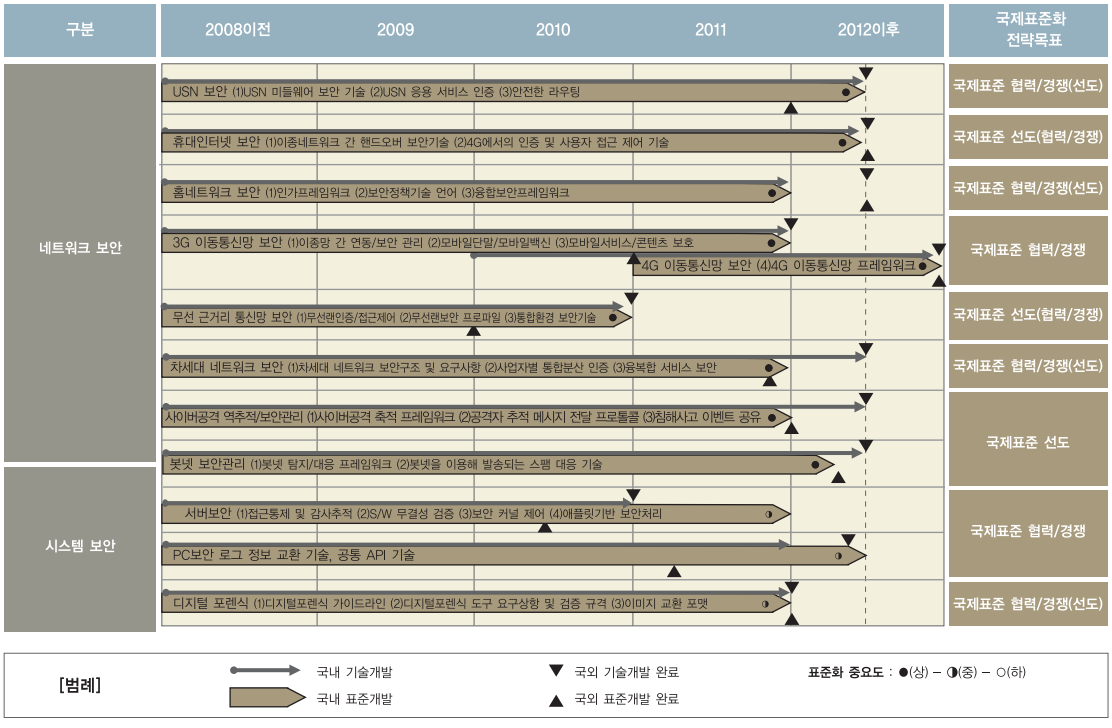
표준화 대상항목

* 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
네트워크 보안	USN 보안기술	– USN 응용 서비스를 위한 인증기술 – 안전한 라우팅 기술	0.84	0.86	IEEE ITU-T	ETRI KISA NIA	TTA 기술 표준원	산업체 연구소 학계
	휴대인터넷 보안기술	– 안전한 휴대인터넷 서비스를 위한 기밀성, 무결성 등의 보안 기술	0.84	0.88	IEEE802.16 ITU	삼성전자 포스데이타 ETRI	TTA PG302	
	홈네트워크 보안기술	– USN 미들웨어 보안 기술/ USN 보안 프레임워크 – 이종 네트워크 간 핸드오버를 위한 보안 기술 – 4G에서의 인증 및 사용자 접근 제어 기술 – 보안제품 간 상호호환성을 위한 보안정책 기술언어 – 홈네트워크 인가 프레임워크	0.72	0.80	ITU-T	ETRI KISA	TTA HNSF	
	이동통신망 보안기술	– 홈네트워크 IT 보안과 홈네트워크 물리 보안 간 융합을 위한 융합 보안 프레임워크 – 모바일 단말 보안 및 모바일 백신 – 이동통신망 보안 관리 프레임워크 – 사용자 인증 및 이종망간 보안 객체 연동기술 – 모바일 서비스 및 콘텐츠 보호	0.76	0.84	3GPP 3GPP2 ITU-R IETF	ETRI KISA	TTA	
	무선근거리통신망 보안기술	– 무선랜 인증 및 접근 제어 기술 – 무선랜 보안 프로파일 – 이종 네트워크로 이루어진 통합 환경에 대한 보안 기술 – 무선랜 위한 효율적인 암호 기술	0.76	0.86	IEEE	ETRI KISA		
	차세대 네트워크 보안기술	– 차세대 네트워크 보안 구조 및 요구사항 – 사업자별 통합 · 분산 인증 및 융복합 서비스 보안 기술	0.86	0.88	ITU-T IETF	ETRI KISA		

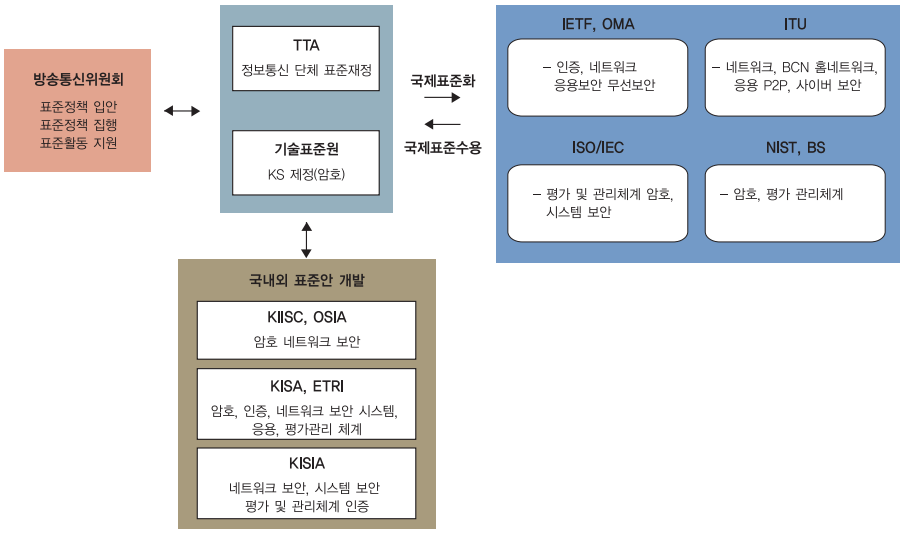
표준화 대상항목 (중점 표준화항목)		정의	전략적 중요도	기술적 파급효과	대응 표준화기구	국내 참여 기관/업체	국내 개발주체	
							표준개발	기술개발
	사이버공격 역추적/ 보안관리 기술	– 공격자 추적 메시지 교환 및 전달 프로토콜 – 다중 도메인 환경에서의 사이버 공격 추적 프레임워크 – 침해사고 이벤트 공유 방법 – 프라이버시 보호를 위한 가이드 개발	0.88	0.80	ITU-T IETF ISO	ETRI 이글루시큐리티 KISA	ISTF TTA	산업체 연구소 학계
시스템 보안	봇넷 대응기술	– 본넷 탐지 및 대응 프레임워크 – 본넷을 이용해 발송되는 스팸 대응 기술	0.76	0.88	ITU-T	KISA	TTA	
	서버보안	– 접근 통제 및 감사 추적 기술 – 소프트웨어 무결성 검증 기술 – 보안 커널 제어 기술 – 애플릿 기반 보안 처리 기술	0.76	0.74	ITU-T ISO/IEC TCPA/WSSN	ETRI 보안업체		
	PC보안	– 통합 PC 보안을 위한 로그 정보 교환 기술 – 통합 관리를 위한 공통 API 기술	0.80	0.82	ITU-T IETF	KISA ETRI		
	디지털포렌식	– 컴퓨터 및 휴대폰 포렌식 가이드라인 – 디지털 데이터 수집도구 및 분석 도구 요구 사항 및 검증 규격 – 디지털 데이터 공통 교환 포맷 – 프라이버시 보호를 위한 가이드 개발	0.88	0.72	ITU-T NIST ASTAP	ETRI KISA TTA		

중점 표준화항목별 중기(3개년) 표준화로드맵



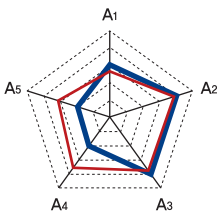
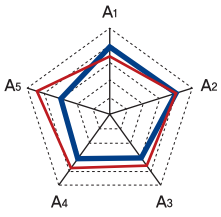
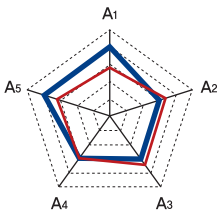
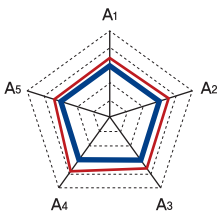
표준화 추진체계

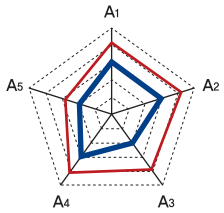
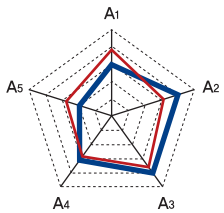
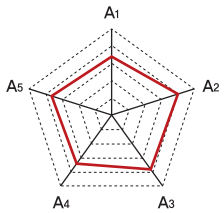
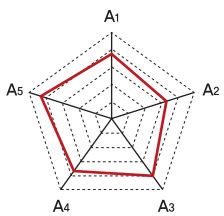
- 네트워크 및 시스템 보안 표준안 개발은 KISA, ETRI, 그리고 정보보호 산업체를 중심으로 국내외 표준(안)을 개발하고, TTA와 IETF, ISO/IEC, 그리고 ITU-T를 통하여 국제 표준화를 추진
- 와이브로 보안 기술은 산업체를 중심으로 TTA를 통하여 국내 표준을 추진하고 ITU-T를 중심으로 국제 표준화를 추진
- 홈네트워크 보안기술은 ETRI, KISA, 학계 및 관련 산업체를 통하여 국내외 표준을 개발하고, 국내의 경우 홈네트워크 시큐리티 포럼 및 TTA를 통하여 수행하고, 국제표준은 ITU-T를 통하여 표준화를 추진하며, 이동통신망 보안 기술은 이동통신 사업자와 정보보호 전문가의 협력에 의한 3GPP, 3GPP2 표준화 주도권 확보가 요구되며 이를 위한 TTA, 지경부의 지원이 절실함. 이동통신 단말업체와 서비스 사업자, 정보보호 전문업체, ETRI, KISA 등을 중심으로 국내외 표준(안)을 개발하고, TTA를 통하여 국내 표준화를 추진하고 3GPP, 3GPP2, ITU-T SG17를 통하여 국제 표준화를 추진함
- 무선 근거리 통신 보안 기술은 ETRI, 학계 및 관련 산업체를 통하여 국내외 표준을 개발하고, 국내의 경우 TTA를 통하여 수행하고, 국제표준은 IEEE를 통하여 표준화를 추진하며, 차세대 네트워크 보안 기술은 BcN 포럼을 통하여 산업체의 표준화 참여를 유도하며, TTA와 ITU-T SG13을 통하여 추진. 사이버공격 역추적/보안관리 기술은 ETRI, 학계 및 관련 산업체를 통하여 국내외 표준을 개발하고, 국내의 경우 TTA를 통하여 수행하고, 국제표준은 ITU-T 를 통하여 표준화를 추진하고 있으며 국제표준 추진을 위해서 해외 유관기관과의 긴밀한 협력을 추구. 봇넷 대응 기술은 KISA를 통하여 국내외 표준을 개발하고, 국내의 경우 TTA를 통하여 수행하고, 국제표준은 ITU-T SG17을 통하여 표준화를 추진. PC 보안 기술은 인터넷보안기술포럼(ISTF)을 통해 산업체 자율적으로 표준화를 추진하되 TTA를 통하여 국내 표준을 추진. 디지털포렌식 기술은 ETRI, 학계 및 관련 산업체를 통하여 국내외 표준을 개발하고, 국내의 경우 TTA를 통하여 수행하고, 국제표준은 ITU-T를 통하여 표준화를 추진함

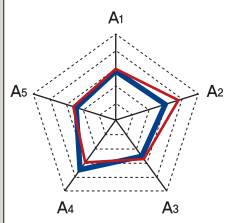
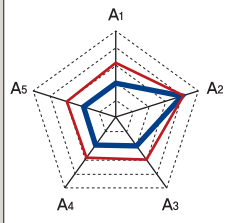
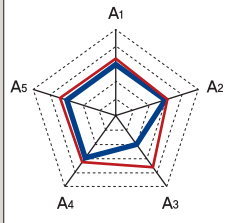


중점 표준화항목별 세부전략(안)

* 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)
USN보안		국제표준화 전략목표: 국제표준 협력/경쟁(Ver.2008) → 국제표준 협력/경쟁(선도)(Ver.2009) – USN보안 분야에 대한 표준화를 주도적으로 추진하고 있어, 표준화 선도할 수 있는 전략이 요구 – 국외 대비 국내 표준화 수준은 대등한 수준에 있으므로 좀 더 적극적인 지원을 통한 국제 표준 기술 선점에 집중할 필요가 있으며, 또한 IPR 확보 가능성이 매우 높으므로 기업의 표준 활동 참여를 강화할 필요가 있고, 이를 위해 국내 표준 활동 강화에 기업 홍보에 심혈을 기울여야 할 것임 IPR확보가능분야 | USN 키관리 및 인증기술, Security Routing, 경량 IDS기술
휴대 인터넷보안		국제표준화 전략목표: 국제표준 선도(Ver.2008) → 국제표준 선도(협력/경쟁)(Ver.2009) – 3G환경에서의 와이브로 표준을 국제표준으로 채택시키는 등 와이브로 분야는 국외 대비 국내표준화 및 국외대비 국내개발 수준은 선도영역에 위치하고 있으며, 계속적으로 선도적 위치로서 통합네트워크 및 4G환경을 고려한 와이브로 보안 기술의 개발 및 표준화 유도 필요 – 와이브로 기술에 대한 국내 표준화 인프라 수준 및 국제표준화 기여도, IPR 확보의 노력이 협력/경쟁 영역에 미루어 볼 때, 국내 기술개발 수준에 비해 국외 대비 표준 기술 및 IPR확보를 위한 활동을 적극적으로 전개해야 할 것임 – 따라서 IMT-2000환경뿐만 아니라, IMT-Advanced 환경에 적합한 와이브로 보안에 적합한 인증 및 접근제어 기술, 이종 네트워크간의 핸드오버 시의 보안기술 등에 관한 표준화 추진노력이 필요 IPR확보가능분야 | 와이브로 핸드오버 시 인증기술, 4G보안기술
홈네트워크 보안기술		국제표준화 전략목표: 국제표준 협력/경쟁(Ver.2008) → 국제표준 협력/경쟁(선도)(Ver.2009) – 국내 기술개발이 활발히 진행되고 있으며 국제 표준화 기구에서도 많은 활동을 하고 있어, 국내 선도의 가능성이 높은 분야임. 홈네트워크 방범/방재용 영상보안감시시스템과 홈네트워크 IT 보안시스템 간의 통합화 추세를 반영, 홈네트워크 융합보안프레임워크에 대한 국제 표준화를 추진하여 국제표준을 선도할 필요가 있음 – 한국이 ITU-T SG17을 중심으로 국제 표준화를 주도하고 있으므로 관련 제품의 국제경쟁력 강화를 위해서는 계속적인 국내 표준화와 병행 추진이 요구됨 – 다양한 아파트 단지형 홈네트워크 구축 경험을 갖고 있는 국내 산업체의 해외 진출 활성화를 위해 해외 홈네트워크 구축환경을 고려한 요구사항이 표준에 반영될 수 있도록 함 IPR확보가능분야 | 홈네트워크 보안관제, 홈네트워크 융합보안 기술
이동통신망 보안기술		국제표준화 전략목표: 국제표준 협력/경쟁(Ver.2008) → 국제표준 협력/경쟁(Ver.2009) – UICC 기반 SIM 인증 보안 기술의 표준화 등 TTA 중심으로 활발히 이루어지고 있으나, 보안 측면에서는 아직 미흡하므로 3GPP 보안, 3GPP2 보안을 중점적으로 표준화를 추진함으로써 국제표준과 협력, 경쟁할 필요가 있음 – 차세대 이동통신 분야에 적용할 수 있는 단말의 보안 프레임워크, 신뢰컴퓨팅 등 단말 관련된 기술에 대한 표준화를 중점적으로 추진 – 차세대 이동통신에서 국내 삼성, ETRI 등에서 활발하게 추진하고 있으며, 이동환경을 위한 단말 보안기술 위주로 표준 선점이 가능하며, 이를 이용하여 국제 표준으로 연결될 수 있도록 추진 IPR확보가능분야 | 차세대 이동통신 단말, HSS시스템

중점 표준화항목	현황분석 (파란색: Ver.2008, 빨간색: Ver.2009)	세부전략(안)
무선근거리 통신망 보안기술		국제표준화 전략목표: 국제표준 협력/경쟁(Ver.2008) → 국제표준 선도(협력/경쟁)(Ver.2009) – 무선근거리통신망 보안과 관련하여 프로토콜 수준에서의 보안 기술 표준화 문제가 일단락되면, 네트워크 측면에서 유무선 통합보안 기술에 대한 표준화 예상됨 – 무선랜을 위한 인증 및 접근제어 기술, AP 위장 방지용 인증 기술, 차세대 통합 네트워크에 대한 보안 기술 및 무선랜 보안 프로파일 등에 대한 표준화를 중점적으로 추진함으로써 국제표준과 협력 및 경쟁이 요구되며, 국내 표준의 수준이 국외 표준에 미치지 못하고 뒤쫓아 가는 형상이기 때문에 와이브로의 경우와 같이 앞선 기술의 사전 준비를 통한 표준화 과정 추진이 반드시 필요함 – 무선근거리통신망이 발전 과정에서 휴대인터넷 및 이동통신망의 기술을 참조하는 경향이 나타나고 있기 때문에 관련 기술을 확보한 국내 기업들의 기술 개발 선도 가능성이 높음 – 무선근거리통신망은 향후 통합 네트워크 환경에서 핵심 네트워크로 사용될 가능성이 매우 높기 때문에 관련 기술의 사전 확보가 중요한 과제로 예상됨 IPR확보가능분야 | 차세대 이종 네트워크 간의 연동기술분야
차세대 네트워크 보안		국제표준화 전략목표: 국제표준 협력/경쟁(Ver.2008) → 국제표준 협력/경쟁(선도)(Ver.2009) – 차세대 네트워크 분야에 공통으로 적용할 수 있는 보안 프레임워크, 절차 및 보안 요구사항 정의와 관련된 기술에 대한 표준화를 중점적으로 추진 – 차세대 휴대 인터넷 서비스 시작이 국내 기술이 세계 선두이므로 유 · 무선 통합 환경에서의 보안 위협과 이에 대한 대응 기술은 표준 선점이 가능하며, 이를 이용하여 국제 표준으로 연결될 수 있도록 추진 IPR확보가능분야 | 이종망 간의 연동봉안기술, 차세대네트워크 침해사고 대응
사이버공격 역추적/보안관리		국제표준화 전략목표: 국제표준 선도 – 사이버 공격 감시 및 추적기술은 국내 각 정부 및 민간 기관별 침해대응센터의 고도화에 해당되는 것으로서 상호호환성이 절대적으로 필요하며, 국내에서는 추적 메시지에 대한 표준 교환 포맷을 TTA에서 정의하였으며, 향후에 제시될 다양한 방향에 대한 기술 검증과 더불어 실용적인 추적 메시지 교환 전달프로토콜과 추적 메시지 교환 시 안전성 제공을 위한 보안 프로파일에 대한 체계적인 국내 고유 표준 개발을 추진 – 약간의 표준 인프라(인력 및 정책 등)만 있어도 충분히 선도가능하며, 현재의 표준 대상의 기술에 대한 검증을 통해 국내표준 시도 추진 – 사이버공격의 글로벌화로 국제적 상호 호환성이 중요해지고 세계시장의 단일화로 세계 표준화 여부가 수출 산업화에 핵심 관건이 되고 있음 – 따라서 국내 시장 중심의 표준화와 더불어 세계 시장 중심의 기술과의 격차가 크지 않아 지속적인 기술의 완성도에 대한 검증을 역점에 두면서 표준을 적극 추진 – 사이버공격 역추적 분야는 국제 기여도가 매우 높은 상태인 관계이며, 따라서 실용적인 기술 검증과 함께 현재 미흡한 국제표준을 선도하는 상황에 역점을 두어 관련 국제 표준을 선도 IPR확보가능분야 | 침해사고 공유, 보안이벤트 상호연관성 분석, 보안이벤트 시각화
봇넷 대응기술		국제표준화 전략목표: 국제표준 선도 – 국내 표준의 경우 2008년 TTA를 통해 봇넷 탐지 및 대응 프레임워크에 대한 표준 제안이 이루어졌으며, 신규 표준 항목으로 채택되어 표준 문서 개발이 진행 중임 – 향후 프레임워크를 기반으로 동작하는 봇넷 탐지 및 대응 체계 운영 가이드라인과 봇넷 탐지 및 대응 프레임워크에 적용되는 상세 스키마 및 프로토콜 등에 대한 표준안이 개발되어야 함 – ITU-T SG17에서 봇넷 탐지 및 대응 프레임워크에 대한 표준 항목을 제안해 채택된 상태이며, 국내 주도 하에 표준 문서 개발 중 – 효율적이고 높은 상호 운용성을 제공하기 위해서 다른 나라 유관기관과의 협력이 필요함 IPR확보가능분야 | 신종 봇넷 능동형 탐지 및 대응

중점 표준화항목	현황분석 (파란색: Ver.2008, 빨간색: Ver.2009)	세부전략(안)
서버 보안		국제표준화 전략목표: 국제표준 협력/경쟁(Ver.2008) → 국제표준 협력/경쟁(Ver.2009) – 웹서버 보안 기술, 트러스트 플랫폼 기반 소프트웨어 무결성 검증 기술, 접근통제 및 감사추적 기술, 그리고 플랫폼 임의조장 방지 기술 등은 TCG의 트러스트 플랫폼 환경에서 플랫폼 임의 조작 및 침해확산을 방지하는 트러스트 플랫폼 및 네트워크의 신뢰성을 제공하는 TNC(Trusted Network Connection) 규격을 수용하고, 2009년 구현 기술에 대한 국내 고유 표준 개발을 추진함 – 트러스트 플랫폼에 대한 기술은 국외에서 표준화되어 앞서가는 기술이므로 트러스트 플랫폼 환경에서 감사추적, 웹서버 보안, 전자상거래 기술, 보안 커널 제어 등의 기술을 접목하는 분야에서 국제 표준화 활동을 수행함 – 트러스트 플랫폼에 대한 운영체제 기술은 ISO 표준 규격을 바탕으로 트러스트 플랫폼용 보안 운영체제 국제 표준을 추진함으로 협력 경쟁 관계를 유지함 – 침해 확산 방지형 도메인 분리 기술은 새로운 개념의 분리 커널 표준화 분야로, CC를 기반으로 ISO에서 국제 표준화 및 IPR 확보를 추진하며, 애플릿 기반 전자 상거래 및 보안 모듈을 연구함으로써 국제 표준화와 IPR 확보를 추진함 IPR확보가능분야 | 보안 운영체제의 접근제어, 신뢰 채널 등 보안 서버 기술
PC 보안		국제표준화 전략목표: 국제표준 협력/경쟁(Ver.2008) → 국제표준 협력/경쟁(Ver.2009) – 안티바이러스 분야에서는 글로벌하게 표준화하여 아직 독점을 하거나 사업을 주도하는 부분이 적으므로 표준화 동향의 주시가 필요. 다만, 통합관리 요구를 수용하기 위해 국내에서 PC 보안 로그 형식 표준화를 추진이 요구됨 – 또한, 각 안티바이러스 업체들이 테스팅에 대한 표준화 논의가 되고 있기 때문에 글로벌 테스팅 표준화에 국내 업체도 참여하여 그 움직임에 따라 기술 개발과 대응책을 마련해야 함 IPR확보가능분야 | 악성코드 탐지 기술
디지털포렌식		국제표준화 전략목표: 국제표준 협력/경쟁(Ver.2008) → 국제표준 협력/경쟁(선도)(Ver.2009) – 국내 사법 환경에 적합한 절차 가이드라인 및 수집, 분석 도구 검증 규격 등의 국내 표준화가 필요하며, 디지털 데이터 분석도구 요구사항 및 수집/분석 도구에 대한 검증 규격, 데이터 교환 포맷 등의 표준안이 개발되어야 함 – 아직 주도적인 국제 표준화 기구가 결성되지 않았으므로, 표준항목을 개발하여 ITU-T 등을 통한 국제 표준화 선도가 가능함하며, – ITU-T SG17에서 2009년부터 시작되는 신규 회기에 사이버 범죄 추적 관련 표준 작업 그룹에 포렌식 관련 표준항목을 준비하여, 주도적인 표준안 제안을 통해 국제 표준을 선도해 나가는 것이 필요하며, ITU-T가 중점적으로 추진할 것으로 예상되는 네트워크 및 모바일 포렌식 분야의 국제 표준을 선도 개발함 IPR확보가능분야 | 고속검색분야