네트워크 및 시스템보안

1. 개요

1.1. 기술개요

1.1.1. 중점기술 및 표준화대상항목의 정의

• 중점기술의 정의

- 네트워크 및 시스템보안 분야는 인터넷과 같은 개방형 네트워크 환경에서 전달되는 정보의 위조, 변조, 유출, 무단침입 등을 비롯한 불법 행위로부터 네트워크를 통한 정보를 보호하는 네트워크 보안과, 정보통신 시스템의 안전성과 가용성을 향상시키는데 필요한 정보보호 기술 및 디지털 증거 제공을 위한 기술을 포함한 시스템 보안으로 구성
- 네트워크 및 시스템보안 분야는 유비쿼터스 센서 네트워크(USN) 보안, 휴대인터넷 보안, 홈네트워크 보안, 무선근거리통신망 보안, 이동통신망 보안, 차세대네트워크 보안, 통합보안관리, 서버보안, PC보안, 디지털 포렌식 등의 10가지 분야로 구분

• 표준화 대상항목의 정의

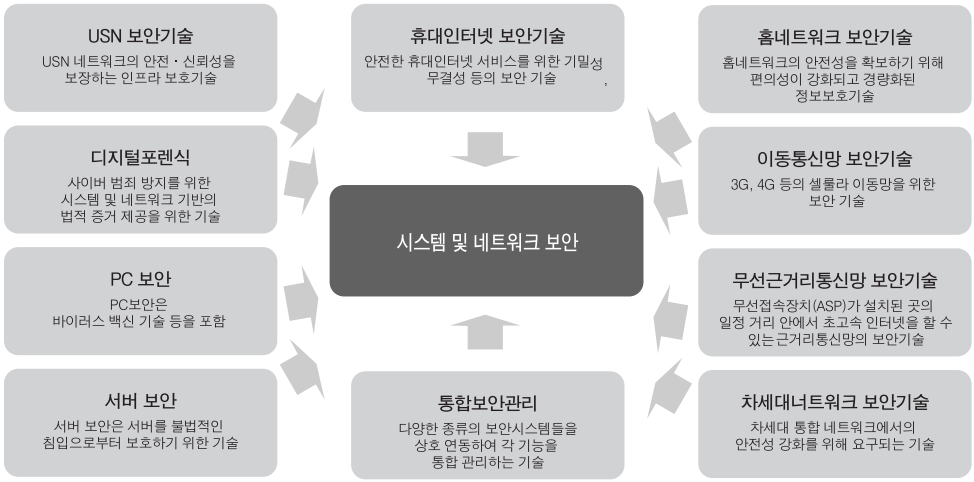
- 네트워크 보안 분야의 경우는 USN 보안, 휴대인터넷 보안, 홈네트워크 보안, 무선근거리통신망 보안, 이동통신망 보안, 차세대 네트워크 보안, 통합보안관리 등 7개 세부 분야의 대상 표준화 항목으로 분류함
- 시스템 보안 분야의 경우는 서버보안, PC보안, 디지털 포렌식 등 3개 세부 분야의 대상 표준화 항목으로 분류함

구분	정의	대상 표준화항목	표준화 내용
USN 보안기술	USN 네트워크의 안전 · 신뢰성을 보장하는 인프라 보호기술	USN 용 경량 암호 및 인증을 위한 키 관리 기법	TTA 의 RFID/USN 프로젝트 그룹에 보안 WG 혹은 분리된 프로젝트 그룹을 만들어 운영하며, 경량의 암호 및 인증을 위한 키관리 기술, 안전한 라우팅 기술, 안전한 배치 기술등이 USN활성화를 위해 표준화 항목으로 추진
		안전한 라우팅 기술	
		안전한 센서 배치 기술	
휴대인터넷 보안기술	안전한 휴대인터넷 서비스를 위한 기밀성, 무결성 등의 보안 기술	IPv6 적용에 따른 보안기술	와이브로 기술을 IMT2000 표준기술로 진입시켜 기존 이동통신서비스와 동등한 위치를 확보한 후, 와이브로 서비스에서의 보안기술에 대한 국제 표준활동 강화
		인증 및 접근제어 기술	
홈네트워크 보안기술	홈네트워크의 안전성을 확보하기 위해 편의성이 강화되고 경량화된 정보보호기술	홈네트워크를 위한 보안프레임워크	ITU-T SG17에서 표준화가 활발히 진행되고 있으며, 국내에서도 홈네트워크 보안 프레임워크 구조, 인증, 인가 메커니즘 등의 분야에서는 기술개발이 활발히 진행되고 있어 국내 선도의 가능성이 높음
		보안제품간 상호호환성을 위한 보안정책 기술언어	
		홈네트워크를 위한 사용자 인증, 인가 메커니즘	

구분	정의	대상 표준화항목	표준화 내용
이동통신망 보안기술	3G, 4G 등의 셀룰라 이동망을 위한 보안 기술	모바일 바이러스 대응 기술	ITU-R을 중심으로 향후 4세대 사용될 주파수 논의가 이루어지고 있고 ITU-T SG17에서는 이동통신 보안 기술 로드맵 작업이 이루어지고 있음
		단말 불법복제 탐지 기술	
무선근거리 통신망 보안 기술	무선접속장치(AP)가 설치된 곳의 일정 거리 안에서 초고속 인터넷을 할 수 있는 근거리통신망의 보안 기술	무선랜을 위한 인증 및 접근제어 기술	프로토콜 수준에서의 보안 기술 표준화 문제가 일단락되면, 네트워크 측면에서 유무선 통합보안 기술에 대한 표준화 예상
		AP 위장 방지용 인증 기술	
		무선랜 보안 프로파일	
차세대네트워크 보안 기술	차세대 네트워크 보안 기술은 방송인터넷 등 각종 서비스 영역을 통합한 멀티미디어 서비스를 시간과 장소에 구애받지 않고 이용할 수 있는 차세대 통합 네트워크에서의 안전성 강화를 위해 요구되는 기술	메쉬노드용 협업 상호호환 기술	인터넷 및 BcN 망 입구에서의 위협방어 보안 표준화 및 이종 사업자/네트워크 사이의 보안 인터페이스 표준화 추진
		서비스별 및 통합 · 분산 인증 기술	
		차세대네트워크 보안 프레임워크	
통합보안 관리	침입차단시스템, 침입탐지시스템, 가상사설망 시스템 등 다양한 종류의 보안시스템들을 상호 연동하여 각 기능을 통합 관리하며, 네트워크 차원의 보안상황 분석, 추적, 그리고 대응하는 중앙집중식 관리와 네트워크 노드의 접근제어 기능을 제공하는 기술	공격자 추적 메시지 교환 및 전달 프로토콜	현재 일관성 있는 침해사고 방지를 위한 네트워크 보안 제어 정책프레임워크 문제가 진행되고 있으며, 향후에는 일관성 있는 네트워크 접근제어 정책 서버 및 프록시 프레임워크와 네트워크 노드 인증에 대한 표준으로 확장될 것으로 예상되며, 최근 공격자 추적 메시지 교환 및 전달 프로토콜, 보안 프로파일 정의가 강력히 대두되고 있음
		네트워크 보안 프로파일	
		네트워크 접근제어 정책 서버 및 프록시 기술	
		네트워크 노드 인증 기술	
서버보안	서버 보안은 접근통제 및 감사추적 기술, 트러스트플랫폼 기반 S/W 무결성 검증 기술, 그리고 플랫폼 임의 조작 방지 기술 등과 같이 서버에 대한 불법적인 침입으로부터 보호하기 위한 기술	접근통제 및 감사추적 기술	서버 보안 및 트러스트 플랫폼 기반 S/W 무결성 검증 기술, 그리고 플랫폼 임의 조작 방지 기술 등은 국제 표준화 기구에 미래 표준기술 분야로 선행 표준 기술 연구 활동을 적극 추진하여 국제 표준 선점을 위한 국제 표준화 활동을 강화함
		S/W 무결성 검증 기술	
		플랫폼 임의 조작 방지 기술	
PC보안	PC 보안은 바이러스 백신 기술 및 키보드 보안 기술 등과 같이 개인용 PC 환경에서 개인의 정보를 보호하는 기술	통합 PC 보안을 위한 로그정보 교환 기술	통합 PC보안이 요구되고 있는 시장 상황에 맞추어 각 업체별로 중복 투자되거나 통합화하는데 장애요인인 로그 형식에 대해 기존 침입방지/탐지 시스템의 로그형식 표준화를 참조하여 통합관리를 위한 로그 형식 표준화 추진이 필요함.
		통합관리를 위한 공통 API 기술	
디지털 포렌식	사이버 범죄 방지를 위한 시스템 및 네트워크 기반의 법적 증거 제공을 위한 데이터의 복구, 분석 기술과 디지털데이터의 관리 기술	컴퓨터 및 휴대폰 포렌식 가이드라인	IT 기술 환경 변화에 따른 다양한 디지털 포렌식 요구사항을 만족하는 기술을 개발하여 IPR 확보 및 국내외 표준화 추진
		컴퓨터 포렌식을 위한 디지털 데이터 수집도구 요구사항	
		디지털 데이터 분석도구 요구사항 및 수집/분석 도구에 대한 검증 규격	

1.1.2. 연관기술 분석

• 연관기술 관계도



• 연관기술 분석표

연관기술	내용	표준화기구/단체		표준화수준		기술개발수준	
		국내	국외	국내	국외	국내	국외
USN 보안기술	- USN (Ubiquitous Sensor network) 네트워크의 안전 - 신뢰성을 보장하는 인프라 보호기술	TTA,USN 포럼	IEEE, ISO	표준기획	표준화 항목승인	설계	시제품/ 프로토타입
휴대인터넷 보안기술	- 안전한 휴대인터넷 서비스를 위한 기밀성, 무결성 등의 보안 기술	TTA, 휴대인터넷 포럼	IEEE	표준화 항목승인	표준화 항목승인	시제품/ 프로토타입	시제품/ 프로토타입
홈네트워크 보안기술	- 홈네트워크의 안전성을 확보하기 위해 편의성이 강화되고 경량화된 정보보호기술	TTA, HNSF	ITU-T	표준안 개발/검토	표준안 개발/검토	시제품/ 프로토타입	시제품/ 프로토타입
이동통신망 보안기술	- 3G, 4G 등의 셀룰라 이동망을 위한 보안 기술	TTA	3GPP 3GPP2	표준안 개발/검토	표준안 개발/검토	시제품/ 프로토타입	시제품/ 프로토타입
무선근거리통신망 보안기술	- 무선접속장치(AP)가 설치된 곳의 일정 거리 안에서 초고속 인터넷을 할 수 있는 근거리통신망의 보안 기술	TTA	IEEE	표준안 개발/검토	표준안 최종검토	구현	구현
차세대네트워크 보안기술	- 차세대 네트워크 보안 기술은 방송인터텟 등 각종 서비스 영역을 통합한 멀티미디어 서비스를 시간과 장소에 구애받지 않고 이용할 수 있는 차세대 통합 네트워크에서의 안전성 강화를 위해 요구되는 기술	TTA	ITU-T IETF	표준안 개발/검토	표준안 개발/검토	설계	설계
통합보안관리	- 침입차단시스템, 침입탐지시스템, 가상사설망 시스템 등 다양한 종류의 보안시스템들을 상호 연동하여 각 기능을 통합 관리하며, 네트워크 차원의 보안상황 분석, 추적, 그리고 대응하는 중앙집중식 관리와 네트워크 노드의 접근 제어 기능을 제공하는 기술	TTA ISTF	ITU-T IETF	표준안 항목승인	표준안 개발/검토	시제품/ 프로토타입	시제품/ 프로토타입
서버보안	- 서버 보안은 접근통제 및 감사추적 기술, 트러스트플랫폼 기반 S/W 무결성 검증 기술, 그리고 플랫폼 임의 조작 방지 기술 등과 같이 서버에 대한 불법적인 침입으로부터 보호하기 위한 기술	TTA	ITU-T ISO TCPA	표준안 항목승인	표준제/ 개정	시제품/ 프로토타입	시제품/ 프로토타입
PC보안	- PC 보안은 바이러스 백신 기술 및 키보드 보안 기술 등과 같이 개인용 PC 환경에서 개인의 정보를 보호하는 기술	TTA	ITU-T IETF	표준화 항목승인	표준안 개발/검토	시제품/ 프로토타입	시제품/ 프로토타입
디지털포렌식	- 사이버 범죄 방지를 위한 시스템 및 네트워크 기반의 법적 증거 제공을 위한 디지털 포렌식 기술 - 하드디스크, 스토리지서버와 휴대용 기기 등 디지털기기에 저장된 디지털 데이터의 복구, 분석 기술과 디지털데이터의 관리 기술	TTA	IETF ITU-T NIST	표준기획	표준기획	기술기획	기술기획

1.2. 추진경과 및 중점 추진방향

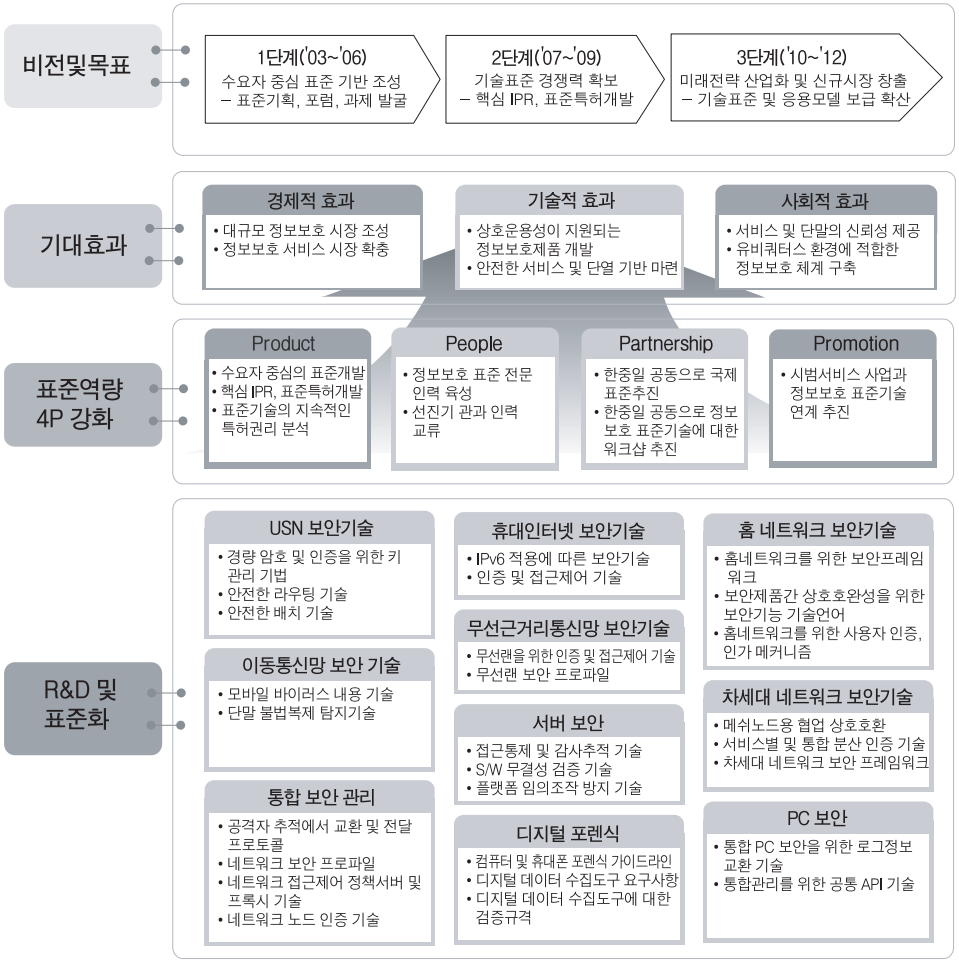
• 추진경과

- 2004년도에는 모든 분야에 대한 표준화 항목을 정리하였음
- 2005년도에는 TTA를 통하여 수행되지 않고 한국정보보호진흥원을 통하여 수행되었으며, 주로 IT839와 연계된 정보보호 표준 분야를 정리하였음
- 006년도에는 정부의 추진 의지가 강한 VoIP 분야를 포함한 응용 서비스 정보보호분야와, 최근 ITU-T와 IETF 등의 국제 표준화 기구에서 활발하게 국제 표준화가 추진 중인 네트워크 정보보호 분야를 중점적으로 정리함
- 2007년도에는 네트워크 및 시스템 보안 분야로 정보보호 분야를 세분화하고, 네트워크 분야를 USN 보안기술, 휴대인터넷 보안기술, 이동통신망 보안기술, 홈네트워크 보안기술, 무선근거리통신망 보안기술, 차세대네트워크 보안기술, 통합보안관리 기술 등과 같이 통신기술의 분류에 따라 분류하고 차세대 인터넷 프로토콜 기술을 포함한 통합보안관리 기술을 포함시켰으며, 시스템 보안 분야는 기존의 서버 보안과 PC 보안 외에 최근 화두가 되고 있는 디지털포렌식을 포함하였음

• 중점 추진방향

- 중점 표준화 항목은 정부의 정책 추진 의지, 산업체의 요구사항, 국제 표준화 기구의 표준화 동향, 그리고 파급 효과 등을 고려함
- 표준화 추진 방향은 국내 표준 추진 방향과 국제 표준 추진방향으로 구분되며, 국내의 표준 동향과 국제 표준 동향을 분석하고, 이를 근거로 국내 표준화 방향을 결정하고, 경쟁력과 효과성이 우수한 국제 표준화 방향을 결정함

1.3. 표준화의 Vision 및 기대효과



- 네트워크 및 시스템보안 기술의 표준화는 유비쿼터스 환경의 기반이 되는 USN을 비롯하여 최근 이슈가 되고 있는 휴대인터넷, 차세대 이동통신의 표준화, 응용 서비스 기술 표준화, 그리고 통합보안 관리 표준화를 통하여 상호동작이 가능한 정보보호 제품, 대규모 정보보호 시장 형성, 안전하게 동작하는 정보보호 제품을 가능케 하여, 궁극적으로 안전한 정보통신 서비스 및 디바이스를 실현 가능하여 안전한 지식 기반 사회 구축 지원할 수 있도록 추진

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
- 그러나 시스템/네트워크 분야의 상호 운용성을 제고하기 위한 정보보호 제품에 대한 표준화 부재는 안전한 전자

정부와 유비쿼터스 사회로의 구현을 위한 커다란 장애

- 시스템 네트워크 보안 분야의 표준화 활동은 크게 국외 표준화 기구의 국제표준으로 상정하는 활동 및 국내 개발된 기술을 국내 표준화 기관들을 통하여 표준화하는 활동 등으로 구분
- 특히, 세계 각국은 자신이 개발한 보안 기술을 국제 표준에 반영함으로써, 관련 정보보호 제품에 대한 IPR을 확보하고 관련 제품의 기술 경쟁력과 시장 지배력을 향상시키고 있는 추세
- 우리나라도 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

1.3.2. 표준화의 목표

- 국내에서는 정부기능을 혁신하기 위한 전자정부 사업을 추진하고 있으며, 이를 바탕으로 민간뿐만 아니라 공공분야를 망라한 지식을 통합적으로 관리하고 효율적으로 분배하는 지식기반 정보화 사회를 구축하기 위한 노력을 기울이고 있음
- 정보화 사회 구현을 위한 가장 핵심적인 요소는 국가 경쟁력 확보와 국가 성장 잠재력 확보를 위해 반드시 요구
- 이러한 시점에서 최근 급속히 확산되고 있는 정보 산업은 모든 형태를 변화시키고 있으며, 정보통신 시장의 국제적인 개방화와 경쟁력 추세는 다양한 정보통신 제품들 사이의 상호 연동을 위해 표준의중요성을 제고하는 계기가 되고 있음
- 정보보호 기술은 금융, 외고, 기업, 통신 인프라 등의 모든 정보화 부분에 안전성과 신뢰성을 보장하기 위한 필수 요구 기술
- 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 할 수 있음

1.3.3. Vision 및 기대효과

- 정보보호기술의 발전은 지식기반 정보화 사회를 유지하기 위한 바탕을 제공하며, 이는 특히, 시스템/네트워크 측면에서 가용성 보장 및 신뢰성 확보가 필수적으로 요구
- 따라서, 시스템/네트워크 분야의 정보보호 기술은 일반적인 정보보호 기실의 안전성과 신뢰성을 향상시키고, 지식기반 전자정부의 유용성을 증대시킬 수 있음
- 또한, IT839로 대표되는 정보화산업 진흥에 따른 구체적인 실현을 위해서 인간 친화적 정보보호 제품 개발과 이를 통한 국민 생활의 질을 향상
- 국제 표준화는 ITU-T에서 정보보호 분야를 리드하고 있는 SG17을 통하여 추진하고, 완성된 국제 표준 중에서 중요도와 산업체 파급 효과 등을 고려하여 대상 표준을 선정하고 TTA를 통하여 국내 표준화를 추진

2. 국내외 현황분석

2.1. 시장 현황 및 전망

2.1.1. 국내 시장 현황 및 전망

• USN 보안

- 2010년도에는 국내 3백만 개에서 4백만 개 정도의 시장을 형성할 것으로 예측되며, 이는 USN 이용한 센서네트워크 활용 시장규모가 매년 150% 이상의 성장률을 기록할 것으로 예상되는 수치임

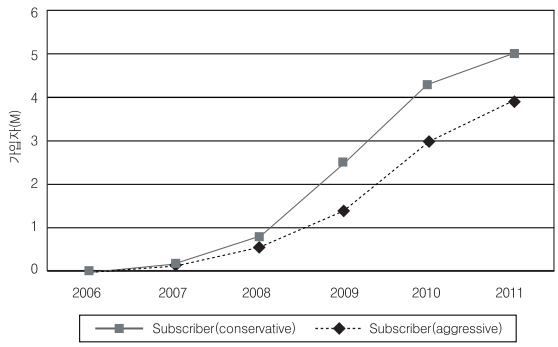
(단위 : 천개)

구분		2006	2007	2008	2009	2010	CAGR
보수적	세계	2,539	6,532	17,663	48,572	126,797	166%
	국내	61	157	424	1,166	3,043	166%
낙관적	세계	3,042	8,146	22,922	65,876	184,759	179%
	국내	73	196	550	1,581	4,434	179%

주1) 게이트웨이 이외의 USN 네트워킹 소프트웨어 및 하드웨어를 포함
주2) 세계 경제규모(상위 13개국의 경제규모를 합산) 중 국내 경제규모가 차지하는 비중 적용
자료 : On World(www.onword.com), "Wireless Sensor Networds : Growing Markets, Accderating Demand", 2005, IMF, "세계 경제 보고서"

• 휴대인터넷 보안

- 2006년 6월 와이브로 서비스는 세계 최초로 우리나라에서 KT, SKT가 상용서비스를 제공하고 있으며, 서비스 초기에는 와이브로 모뎀에서의 배터리 소모문제, 기지국간 이동시 끊김 현상, 핵심 응용서비스 부재로 가입자 증가가 정체되어 있었으나, 2007년 8월 현재 KT의 활발한 마케팅에 힘입어 가입자가 3만 명을 돌파
- 서울 일부지역에서만 제공되던 서비스가 2007년 4월 서울 전역으로 확대되고, 2007년 6월 와이브로 전용 USB 모뎀이 출시되면서 가입자가 빠르게 늘어나고 있으며, KT는 연말까지 상하향 전송속도가 지금보다 2배정도 빠르게 개선된 서비스를 선보일 예정



Source:IDC. 2007

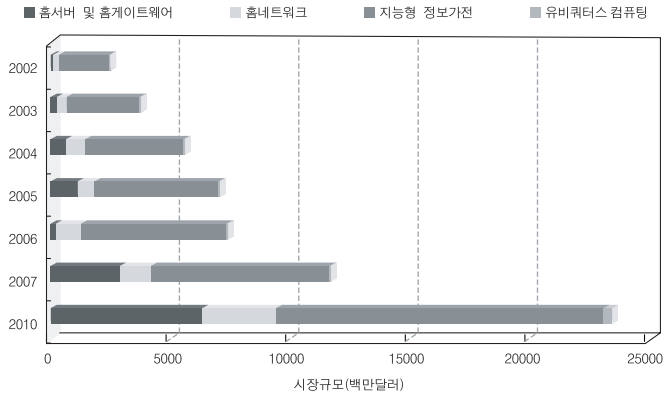
〈 와이브로 시장전망 〉

- 2011년 와이브로 가입자는 500만에 달하고, 3G 이동통신 가입자가 1,500만명에 이를 것으로 예측
- IT 시장조사업체 한국IDC는 "HSDPA와 와이브로 서비스 시장 분석 및 전망 보고서 '를 통해 HSDPA/HSUPA가 올해 전체 이동통신 가입자 중 7.4%를 차지하고 2011년에는 1,492만명에 달해 전체 이동통신 가입자의 32.6%에 달할 것으로 전망했으며, 와이브로 역시 올해 0.2%에서 2011년 38.8%로 크게 높아질 것으로 IDC는 예상
- HSDPA/HSUPA와 와이브로는 각각 독립적인 서비스로 서로 경쟁하기보다는 상호 보완적 관계에서 다양한 결합 서비스 형태로 제공될 것으로 예측
- 또한, 정부는 2010년까지 국내 와이브로 시장규모를 8조1000억원, 장비 시장규모를 5조8000억, 세계시장 규모를 24조원으로 추정했으며, 와이브로 상용화에 따라 6년간 24조7000억원의 생산유발 효과와 12조원의 부가가치 창출 효과, 27만명에 이르는 고용 창출이 가능할 것으로 예상(2007년 5월31일, MIC IT전략 시장전망결과).

• 홈네트워크 보안

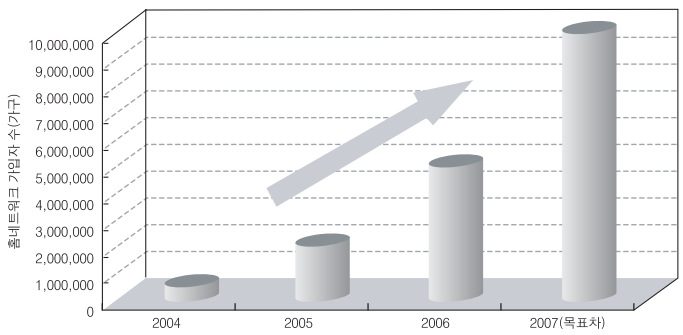
- 홈 네트워크 산업의 국내 시장규모는 2002년 25억 1,000만 달러, 2003년 37억 8,000만 달러, 2004년 56억 달러, 2005년에는 70억 8,000만 달러에 이를 것으로 추정, 이는 세계 홈 네트워크 산업 시장의 9.2%를 점유하는 규모이며, 향후 연평균 32.2%씩 급성장하여, 2010년에는 234억 5,000만 달러에 이를 것으로 전망
- 국내 시장도 세계와 마찬가지로 홈서버와 홈게이트웨이 시장의 연평균 61.2%의 고속 성장이 기대되며, 유비쿼터스 컴퓨팅 시장 또한 연평균 52.3%씩 성장할 전망
- 국내 홈네트워크 가입자 수는 초기적인 PC 중심의 홈네트워킹 사용자와 인터넷 접속 공유, 원격검침, 가스화재 감지, CCTV 원격 감시, 가전기기 원격조정 서비스 등 다양한 형태의 홈 네트워킹과 인텔리전트 아파트 등을 포함
- 기본 전제사항으로 국내 2004년 초고속 인터넷 보급률은 76.7%를 기준으로 하였으며, 초고속 인터넷 가입자 수의 3.8%인 45만 8천여 가구가 홈네트워크 가입자 시장규모로 도출. 여기에 정통부 시범아파트 1,300여 가구, 기존 고급 인텔리전트 아파트의 홈네트워크 사용자 가구로 추정된 40,000여 가구를 합해, 2004년 총 500,000 가구로 시장규모를 산출
- 2007년까지 정통부 가입목표치를 기준으로 할 때, 2005년 2백만 가구, 2006년 8백만 가구 , 2007년 10백만 가구의 홈네트워크 가입자 규모를 예상

국내 홈 네트워크 산업의 시장동향



자료 : Gartner Group, In-Stat 2003, R&DBIZ 재가공

홈 네트워크 가입자 전망



자료 : 정통부, R&DBIZ

• 이동통신망 보안

- 2007년 5월 휴대폰 수출은 전년 동월 대비 1.8% 감소한 16억 4,200만 달러, 5월 누적으로는 전년동기 대비 5.4% 증가한 85억 8,740만 달러 기록

◦ 2007년 5월 기술방식별 수출을 보면 CDMA 방식은 전년 동월 대비 4.7% 감소한 3억 7,250만 달러, GSM 방식은 2.3% 감소한 11억 1,760만 달러, WCDMA 방식은 16.8% 증가한 1억 4,670만 달러 기록

◦ 5월 누적 기준 기술방식별 수출 비중은 CDMA 28.4%, GSM 59.0%, WCDMA 12.4%임

◦ 유럽지역의 3G 서비스 확대로 WCDMA 방식의 수출은 2006년 5월에 1억대를 돌파한 이후 지속적으로 성장하여 2007년 5월 누적으로는 전년 동기 대비 173.3% 증가한 10억 6,370만 달러를 기록

◦ CDMA 방식의 수출은 미국(14.6억 달러, 21.3%↑) 및 홍콩(5.0억 달러, 28.3%↑)의 수출 증가로 인해 5월 누적으로 전년동기 대비 14.9% 증가한 24억 4,080만 달러를 기록

◦ 2007년 5월 CDMA WLL 수출은 전년동월 대비 1.6% 감소한 2,200만 달러, 5월 누적으로는 50.5% 감소한 7,760만 달러를 기록

〈표3〉 이동통신 수출동향

(단위 : 백만달러, %)

구분		2006			2007			증감률	
		합계	5월	1~5월	4월	5월	1~5월	전년동월	1~5월
휴대폰	CDMA	5,215,0	390,7	2,123,3	447,8	372,5	2,440,8	-4,7	14,9
	GSM	13,009,2	1,143,7	5,574,8	1,043,4	1,117,6	5,067,0	-2,3	-9,1
	WCDMA	1,619,4	125,5	389,2	191,9	146,7	1,063,7	16,8	173,3
	휴대폰 합계	19,966,2	1,672,2	8,150,9	1,684,2	1,642,0	8,587,4	-1,8	5,4
CDMA WLL		335,2	22,3	156,6	10,4	22,0	77,6	-1,6	-50,5
이동통신 시스템		252,6	23,1	62,1	33,7	21,2	126,7	-8,5	104,0
이동통신 부분품		3,775,6	296,9	1,469,7	348,5	338,4	1,441,0	13,2	-2,0

• 무선근거리통신망 보안

- 2000년대 이후 성숙기 단계의 국내 통신 서비스 시장에 신규 수종 사업으로 기대를 모았던 무선랜 서비스는 가입자 정체의 캐즘 상태에 직면하였으며 향후 휴대인터넷이라는 경쟁 서비스의 등장으로 잠재시장 잠식이라는 어려운 위기상황에 처해 있음. 시장전망은 불투명한 상태이지만 꾸준한 성장을 보이면서 향후 무선랜 서비스는 5GHz 대역으로 주파수 대역 변경을 통한 서비스 품질 강화와 전송속도 강화를 통하여 독자적인 생존과 성장을 모색할 것으로 전망
- 국내에서 무선랜은 의료, 유통등의 특정한 분야를 중심으로 발전하다가 공중 무선랜 서비스(KT Nespot등)의 등장과 노트북에 무선랜 어댑터 기본으로 장착되면서 대중에게도 익숙한 서비스가 되었음
- 무선랜 시장은 매년 20%이상의 고성장을 기록하면서 서비스 포화 상태로 침체기에 빠진 네트워크 시장의 돌파구로 인식
- 2004년 1월에 Gartner에서 발표한 네트워크 장비시장전망에 따르면 무선랜 장비는 2007년까지 평균 22.4%의 성장을 달성하여, 한 자리 수 성장에 머무르고 있는 다른 네트워크 장비분야와는 달리 성장의 원동력이 될 것으로 예상
- 무선랜 장비 시장은 초기 중소기업들이 유선랜을 무선으로 대체하게 된 대체수요와 의료, 제조, 유통 등 전통적인 수직 애플리케이션 분야에서 시장창출이 일어났으나, 2003년도에는 일반 가정의 홈네트워킹 수요와 핫스팟의 증가에 힘입어 일반 소비자들을 대상으로 시장이 점점 커지고 있음

• 차세대네트워크 보안

- 국내 정보보호시장은 2005년 6,967억원 규모에서 2010년에는 1조 1,544억원 규모에 이를 전망이며 연평균 10.64%의 성장률을 보일 것으로 예측
  - 성장률 측면에서는 정보보호서비스 분야가로 연평균 19.88%의 성장으로 2010년에는 시장규모가 약 2,148억원에 이를 것으로 전망
  - 정보보호 하드웨어 및 소프트웨어 분야는 각각 2010년도에 시장 규모가 5,386억원 및 4,009억원에 이를 것으로 전망되며 연평균 성장률은 각각 8.84% 및 9.28%로 예측됨(KISIA, 2005.12.)
  - 세계시장 전망과 비교하여 보면 전반적으로 하드웨어 분야의 성장률이 낮게 나타남

〈국내정보보호 시장전망〉 (단위: 백만원)

구분	2005	2006	2007	2008	2009	2010	CAGR(%)
정보보호 H/W	352,675	387,912	425,594	463,275	500,958	538,639	8.84
정보보호 S/W	257,289	286,573	315,274	342,708	372,105	400,946	9.28
정보보호 서비스	86,755	113,645	138,734	162,427	188,919	214,823	19.88
합계	696,719	788,130	879,602	968,410	1,061,982	1,154,408	10.64

출처 : 국내 정보보호산업 통계조사(2005-2010), KISIA, 2005.12.

- 네트워크 보안시장 현황
  - Firewall/VPN : 국내 업체는 상위3사(시큐아이닷컴, 어울림정보기술, 퓨쳐시스템즈)가 대다수의 시장을 차지하고 있으며, 초기 설비투자비용으로 진입장벽이 존재하는 것으로 판단됨
  - IDS/IPS/UTM : IDS 제품으로는 윈스테크넷의 Sniper IDS, 인젠의 Neowatcher, 펜타시큐리티의 Siren 등이 있으며, LG엔시스는 중소기업 시장을 위한 네트워크 통합보안제품인 '세이프 IPS-U' 를 출시함. 세이프 IPS-U는 침입탐지시스템(IDS), 침입방지시스템(IPS)기증은 방화벽, 안티바이러스, 안티스팸, 웹 콘텐츠 필터링 등 복합기능을 통합 지원
- 차세대네트워크 인프라는 정부의 u-City 투자 계획, 미래인터넷의 새로운 네트워크 인프라 요구에 따라 무선 메쉬 네트워크 시장이 가장 뚜렷한 인덱스가 될 것으로 판단됨
  - 국내 주요 지자체 및 도시의 u-City 사업투자, 예산 및 계획이 활발히 추진[1]되고 있으며, 주요 u-City 투자계획을 근거로 2010년까지 50조~60조원으로 예측자료를 제시
  - 메쉬 네트워킹은 물리적인 계층을 무선통신에 크게 의존하므로 근본적으로 보안 이슈가 매우 큰 관심을 끌 것임
  - 또한 구체적인 침해 사례가 발생하지 않아도 무선통신의 감청에 의한 개인정보 유출, 도용에 대한 우려가 존재하고, 이에 따른 보안에 대한 시장요구가 나타나는 단계가 매우 빠를 것으로 예상됨

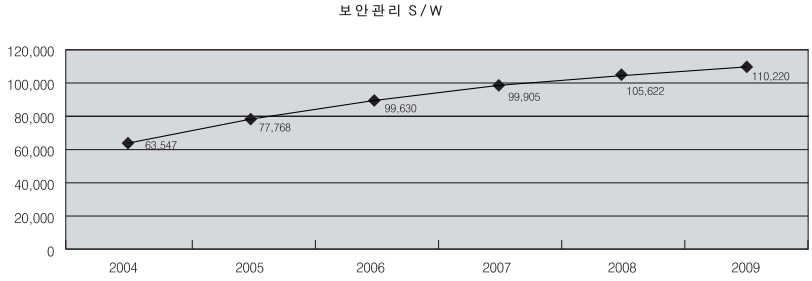
1) 자료 : ETR(2005), 전자부품연구원(2005), 가트너(2004), 일본 총무성(2004), 김신배(2004), 맥킨지(2004) 자료를 재구성함

- 보안 이벤트 시각화 및 공격자 추적 : 주요 업체 및 제품은 이글루 시큐리티의 SPiDER-X 가 유일하며 국내 시장을 개척하고 있으며, 아이자이어의 웹기반 응용서비스 추적 제품인 (웹시큐어TM)가 현재 시장을 주도 하고 있음

• 통합보안관리

- 통합보안 관리 툴, 로그분석, 및 취약점 분석에 대한 툴 등을 포함하는 통합보안관리 S/W 분야는 보안컨설팅분야의 약진 및 정책적 보안관리 인식 강화 등에 힘입어 향후에도 꾸준히 팽창할 것으로 기대되는 분야임

◦ 2004년도의 매출규모는 63,547백만원에서 2009년에는 그 규모가 110,220백만원에 이를 전망



〈2003년도 국내 12개 주요 ISP의 시설투자계획 및 ETRI의 국내외 정보보호시장 전망(* 03. 3월)에 근거〉

◦ 향후 ESM 제품의 주요 요소기술로는 취약점관리시스템과 실시간 상관관계분석기능이 연계되는 제품이 주요 이슈가 될 전망이며, 인트라넷 정보 및 보안관리를 총체적으로 제공하는 통합형 제품개발이 필요하며, 제품간 · 출시업체간 연동성을 제고하는 제품개발이 요구되고 있음

◦ 산업계에서는 알려지지 않은 네트워크 공격특성 인자를 자동으로 추출하여 표현하는 메커니즘과 보안이벤트에 대한 시각화를 통해 직관적 모니터링이 가능한 보안이벤트 시각화 기술이 가장 주목을 받을 것이라고 예상하고 있으며 향후 미래 시장을 형성할 것으로 전망됨

※위협관리 기술의 고도화, "보안이벤트에 대한 시각화를 통해 직관적 모니터링이 가능한 보안이벤트 시각화 기술이 가장 주목", 디지털데일리 (2005.12)

※미국 Georgia Institute of Technology의 Greg. Conti는 전 세계의 언더그라운드 해커들이 모여 발표하는 수준 높은 행사인 BlackHat과 Defcon에서 2004년과 2005년에 걸쳐 네트워크 보안상황의 시각화에 대한 중요성을 매우 강조하였으며, 향후 사이버공격 감시 기술은 보안이벤트 시각화 기술임을 강조하고 있음

◦ 특히 보안 측면의 유무선 네트워크 이상상황에 따른 거시적 관점의 사이버공격 감시 기술은 시각화 및 지능형 에이전트와 같이 매우 높은 수준이지만, 세부적 관점의 사이버공격 감시는 개척 단계로서 기술혁신 상태의 제품이 출현할 것으로 예상됨

◦ 통합보안관리 기술 중 사이버공격 추적 기술은 현재 각 자사제품위주의 사이트 운영을 통해 제한적이고 수동적인 역추적 기능을 제공하거나 또는 특정 응용 포트에 국한하여 각 응용서비스 추적 제품을 개발하여 적용하고 있는 단계이나, 향후 주요 능동적인 대응을 위한 제품 기능으로 도입될 것으로 전망됨

- NAC 기술은 네트워크와 엔트포인트를 융합해서 관리하기 위한 솔루션으로 적절한 권한을 가진 사용자가 보안 검증이 된 안전한 PC로 사내 네트워크 자원에 접속할 수 있도록 통제하는 네트워크 접속 통제 기술임 인증 및 정책 관리 기술, 접속 정책 실행 기술 들이 아우러져 사내망 또는 정부공공망 등의 IT 관리자들이 그 내부망 보호와 보안을 보다 손쉽게 관리 운용할 수 있는 추세임

- 통합보안 관리 툴, 로그분석, 및 취약점 분석에 대한 툴 등을 포함하는 통합보안관리 S/W 분야는 보안컨설팅분야의 약진 및 정책적 보안관리 인식 강화 등에 힘입어 향후에도 꾸준히 팽창할 것으로 기대되는 분야임

- 사이버보안 동향

  ◦ 갈수록 늘어나는 보안 장비와 다양한 수법들에 대처하기 위한 장비 관리의 어려움과 전문 인력의 부재로 보안 장비가 설치되어 있어도 외부로부터의 침입에 적절하게 대응을 하지 못하는 경우가 많기 때문에 설치된 보안 장비들을 관리하기 쉽고 운용을 간단하게 하려는 노력들이 진행

  ◦ 다른 한편으로는 보안관리를 전문으로 하는 아웃소싱형태의 업체들이 생겨난 것이 그 예라고 볼 수 있음.

  ◦ 그리고 한 가지 솔루션만이 독자적으로 설치되어 운용되는 것이 아니라 각 보안장비들을 통합해서 취약점을 보완한 형태의 통합 솔루션들과 관리 솔루션들이 개발 출시

  ◦ 대표적인 것으로는 보안장비들을 중앙에서 감시하고 로그들을 분석해서 현재 상태를 감시할 수 있는 통합보안관리 시스템(ESM)과 인증과 접근제어를 연계한 통합인증 및 권한관리(Extranet Access Management: EAM)

• 서버보안

- 국내 정보보호시장은 연평균 9.64% 성장률로 2011년에 1조 1,821억원 규모에 이를 것으로 전망 (출처 - IDC & KISIA, 2006.11.)

〈국내정보보호 시장전망〉

구분	2005년	2006년	2007년	2008년	2009년	2010년	2011년	CAGR(%)
시스템 및 네트워크 정보보호 제품	583,423	625,182	713,689	790,940	864,482	935,633	1,005,495	9,50
정보보호 서비스	97,282	109,610	123,053	136,495	149,938	163,380	176,823	10,47
합계	680,705	734,792	836,742	927,435	1,014,420	1,099,013	1,182,318	9,64

출처 : 국내 정보보호산업 통계조사(2005-2010), KISIA, 2006.11.

- 서버 보안(보안 운영체제) 분야의 시장 규모는 2005년도 매출액 286억원에서 2006년 매출액 291억원으로 조사되어, 2005년 대비 2006년 성장률은 1.7%의 증가를 보이고 있으며, 연평균 1.65% 성장률로 2011년에 316억원 규모에 이를 것으로 전망 (출처 - KISIA 2006. 11)

〈서버 보안 분야 시장전망〉 (단위: 백만원)

구분	2005년	2006년	2007년	2008년	2009년	2010년	2011년	CAGR(%)
보안운영체계 (Secure OS)	28,652	29,144	29,636	30,128	30,620	31,112	31,604	1,65

- 새로운 기술보다는 기존 기술을 개량하여 접근 제어 메카니즘의 제한을 극복하는 등을 고려하는 서버 보안 솔루션이나 키관리와 S/W 무결성 확인을 위한 트러스트 플랫폼용 운영체제에 대한 요구가 증가할 것으로 예상됨

• PC보안

- PC보안에 해당하는 솔루션 영역은 Anti-Virus(Anti-Spyware), 개인방화벽/침임탐지, 매체제어, 패치관리, 유해정보차단, 데이터복구 등을 들 수 있음
- 이중 Anti-Virus 시장은 개인방화벽/침입탐지를 포함한 Internet Security 제품으로 진화해나가고 있고, 이에 대한 전문 시장조사기관의 시장 전망 자료가 존재하고 있으나, 매체제어, 유해정보차단, 데이터복구 시장등은 아직 그 규모가 미미하여 신빙성 있는 기관의 보고가 이루어지고 있지 않음
- Anti-Virus 시장 현황 및 전망
  - 갈수록 지능화, 고도화 되가는 새로운 각종 웜 및 바이러스와 다양한 스파이웨어 및 애드웨어 등의 등장에 따른 위협 증가와 대응 노력의 확대, 그리고 지속적인 업데이트 수요에 힘입어 2005년도 580억원, 2006년도 630억원 크기의 시장을 만들고 있으며, 약 12%의 견조한 상승세를 지속
  - Anti-Virus시장은 전통적으로 보안 소프트웨어 시장에서 가증 큰 비중을 차지하고 있는 영역으로 도입율 역시 높아 신규 수요확대의 어려움이 예상되지만, 상대적으로 여전히 높은 성장을 기록하며 보안 소프트웨어 시장을 견인하고 있는 상황
  - 최근 시장 성장의 특징은 그간 불법소프트웨어의 온상이었던 Consumer Market의 유료화가 높아지고 있다는 것
- AV시장 발전의 긍정적 요소
  - 인터넷 및 네트워크 신규 위협 증가 : 인터넷 사용 증가와 더불어 새롭고 다양한 바이러스, 웜이 지속적인 위협요소로 작용
  - 연단위 계약 및 업데이트의 일반화 : 성숙된 시장이지만 1회성 구매에 그치지 않고, 연단위 계약이 일반화 되어 꾸준한 시장이 창출
  - 통합 솔루션 공급 일반화 : 단순한 Anti-Virus 기능에서 개인방화벽, 개인정보보호 기능까지 포괄하여, 매출 단가 상승에 대한 시도가 지속
- AV시장 발전의 부정적 요소
  - 지속적인 경기 침체 : 불확실한 경기 전망은 기업들에게 전반적인 IT 투자, 특히 보안 부분에 대한 투자규모 축소를 요청
  - 경쟁심화에 따른 가격 하락 : 다수의 신규 벤더가 등장함에 따라 경쟁이 심화되고 있으며, 저가 수주현상이 일반화

단위 : 백만원

	2005	2006	2007	2008	2009	2010	CAGR
시장크기	57,390	63,456	71,325	79,884	88,831	98,958	11.5%

출처 : SCM Software Forecate 2006-2010, IDC 2006

- 기타 PC 보안 시장 현황

◦ 패치관리 : 2002년 인터넷 대란 이후 웜 공격이 끊이지 않았고, 이에 대한 근본적인 해결책으로 패치관리솔루션이 시장에 소개되어 현재는 약 60억 정도의 시장이 유지되고 있는 것으로 추정. 패치관리의 향후 발전 가능성에 대해서는 패치의 범위가 확장될 것이라는 안과 기업용 Anti-Virus 솔루션의 구성요소로 편입 될 것이라는 두가지 예측이 존재

◦ 매체제어 관리 : 내부 정보의 무단 반출에 대한 대응책으로 USB등 외부 매체 장치를 무단으로 사용할 수 없게 만드는 제품이 공급. 주로 대기업 및 공공기관을 발판으로 시장의 확산을 꾀하고 있지만 기술적, 관리적 문제로 인하여 실제 효용성은 현저히 낮은 수준. 법안 계류중인 "개인정보보호법"이 통과되면 본격적인 시장의 확산이 예상

단위 : 백만원

	2005	2006	2007	2008	2009	2010	CAGR(%)
Anti-Virus	41,139	51,327	61,515	70,684	78,936	86,364	14.57%
Anti-Spyware	16,796	17,344	18,166	19,399	21,249	24,023	9.01%
PC방화벽	5,385	5,782	6,179	6,576	6,973	7,370	6.29%
패치관리	9,450	12,884	15,288	16,970	18,148	18,973	12.88%
기타 PC보안	29,500	32,662	35,824	38,986	42,148	45,310	8.63%
합계	102,270	119,999	136,972	152,615	167,454	182,040	10.276%

출처 : 한국정보보호진흥원, 2006 국내 정보보호산업 통계조사, 2006

• 디지털포렌식

- 기업들의 보안 관리의 중요성이 강조되면서 단순 로그관리에 그치는 통합보안관리(ESM) 솔루션보다 한 차원 높은 분석 및 대응책을 제시하는 컴퓨터 포렌식 솔루션에 대한 관심이 증가
- 금융, 제조업체 및 사이버 수사기관을 중심으로 포렌식 시장이 형성되어 가고 있음
- 국내 사건 대응 서비스 시장은 세계시장의 5% 수준으로 예측하여 2010년 2,644억원에 이를 것으로 추정됨
- 미국에서 디지털 정보의 미제출로 인한 벌금 부과의 사례가 있었으며, 소송증거 확보를 위해 디지털 포렌식 도구의 사용이 의무화됨에 따라 업체에서 자체적으로 솔루션을 도입 및 운영하려는 추세가 확대되고 있음

2.1.2. 국외 시장 현황 및 전망

• USN 보안

- 한국정보사회진흥원 보고서에 따르면 2010년도에는 83억달러 이상의 시장이 형성 될 것으로 전망

구분		2006	2007	2008	2009	2010	CAGR
보수적	세계	333,348	691,461	1,845,996	3,514,578	8,339,155	124%
	국내	8,000	16,595	44,304	84,350	200,140	124%
낙관적	세계	395,460	855,330	1,994,214	4,677,196	12,009,335	135%
	국내	9,491	20,528	47,861	112,253	288,224	135%

주1) 게이트웨이 이외의 USN 네트워킹 소프트웨어 및 하드웨어를 포함
주2) 세계 경제규모(상위 13개국의 경제규모를 합산) 중 국내 경제규모가 차지하는 비중 적용
자료 : On World(www.onword.com), "Wireless Sensor Networds : Growing Markets, Accderating Demand", 2005, IMF, "세계 경제 보고서"

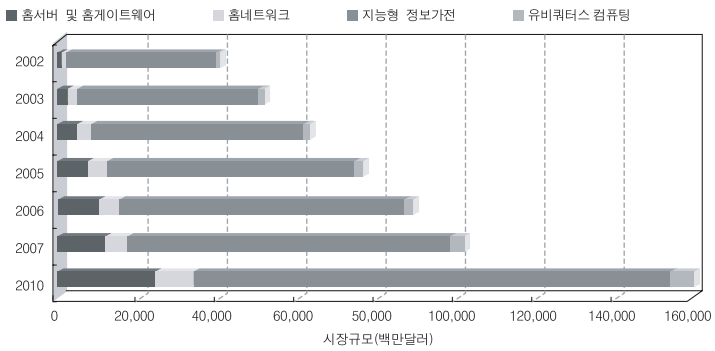
• 휴대인터넷 보안

- 국내 와이브로 사업자인 KT에 이어 브라질에서의 옴니비전, 미국에서의 스프린트 넥스텔, 이탈리아에서 상용서비스를 개시할 예정이고 최근에는 일본과 대만에서 사업자 선정계획을 발표하는 등 와이브로 도입국가가 확대
- KT는 미국 뉴파라사에 와이브로 서비스 기술 컨설팅을 제공하고 있고 와이브로 관련 사업자들의 글로벌 협의체인 WMC(WIBRO-Mobile WiMAX Community) 의장과 와이 맥스(WiMAX) 포럼 이사회 임원과 글로벌로밍 워킹그룹 의장으로 활동하며 와이브로 세계 시장에서 주도적인 역할
- 삼성전자는 2006년 8월 미국의 주요 통신사업자인 스프린트사와 전격 와이브로 상용화 계약을 체결하면서 3.5G를 이끌어가는 선두주자로 급부상했으며, 미국, 이탈리아, 브라질 등 23개국 35개 사업자와 와이브로 사업을 추진중
- 또한, 향후 2010년까지 전세계 와이맥스(WiMAX) 장비 시장은 연평균 70%의 고속 성장을 거듭할 것으로 전망
- 통신서비스와 장비, 모바일 기술분야 전문 시장조사기관인 인포네틱스리서치는 고정 및 이동형 와이맥스 장비 시장은 2010년 46억달러 규모에 이를 것으로 예상했으며, 이중 이동형 와이맥스 장비시장 규모가 66%를 차지할 것으로 예상

• 홈네트워크 보안

- 홈 네트워크 산업의 세계 시장규모는 2002년 407억 달러, 2003년 518억 달러, 2004년 638억 달러, 2005년에는 768억 달러에 이를 것으로 추정
- 또한, 2002년에서 2010년까지 복합연평균성장률(CAGR)이 18.8%로 성장하여, 2010년에는 1,620억 달러에 이를 것으로 전망
- 특히, 홈서버와 홈게이트웨이는 연평균 47.2%의 급성장이 기대. 홈서버는 기능이 융합된 방송통신 융합형 홈서버로 발전될 전망

세계 홈 네트워크 산업의 시장동향



자료 : Gartner Group, In-Stat 2003, R&DBIZ 재가공

- 주요 벤더별 동향은 MS는 최근 AV 등 엔터테인먼트 기능을 강화한 미디어 센터 PC를 통해 홈네트워크 시장을 공략하고 있으며, 향후 홈네트워크 게이트웨이 목적으로 콘솔 게임기 시장에 진입
- Sony는 Ubiquitous Value Network 전략의 일환으로 TV, 게임기, PC, PDA 4개 제품을 하나로 통합 시키려는 시도를 하고 있음
- Matsushita는 Home, Car, Mobile 세 분야의 유기적인 네트워크 연결에 중점을 두고 있으며, 또한 메모리 카드, DVD, DTV 등 새로운 홈네트워크 가전기기 출시를 준비 중
- 기타 Nokia, IBM, Intel 등도 홈 게이트웨이, 칩 집적기술 등 R&D에 모든 전략적 에너지를 투입

〈세계 홈 네트워크 산업 시장규모〉

단위 : 백만달러

	홈서버 및 홈게이트웨어	홈네트워크	지능형 정보가전	유비쿼터스 컴퓨팅	합 계
2002	1,100	1,500	37,300	800	40,700
2003	2,400	2,500	45,700	1,200	51,800
2004	5,000	3,500	53,700	1,600	63,800
2005	7,900	4,300	62,600	2,000	76,800
2006	10,300	4,900	71,700	2,500	69,400
2007	12,400	5,400	81,300	3,500	102,600
2010	24,300	10,000	120,000	7,700.	162,000
CAGR(%)	47.2%	26.8%	15.7%	32.7%	18.8%

※ 지능형 정보가전은 DVD플레이어, 인터넷 오디오, 비디오 게임기, 이동 및 고정형 단말기 등을 말함, 자료 : Gartner Group, In-Stat 2003, R&DBIZ 재가공

• 이동통신망 보안

- 2007년 5월 누적 기준 미국은 최대 휴대폰 수출국으로 프리미엄 제품의 호조로 인해 전년동기 대비 23.7% 증가한 18억 9,124만 달러를 기록하여 전체 수출국가 중 22%의 비중 차지

- 중국(2위)과 홍콩(3위)은 전년동기 대비 각각 59.4%, 2.2% 증가한 11억 5,628만 달러, 6억 1,068만 달러를 기록하여 휴대폰 수출에 견인하고 있으며, 중국과 홍콩을 포함한 휴대폰 수출은 전년동월 대비 33.6% 증가한 17억 6,699만 달러로 머지않아 최대 수출국인 미국을 앞지를 전망
- 이탈리아(2.7억 달러, 41.8%↓), 독일(4.0억 달러, 15.6%↓) 등의 마이너스 성장으로 인해 EU는 전년동기 대비 12% 감소한 24억 3349만 달러를 기록
- 또한 러시아(3.4억 달러, 504.3%↑), 중동(2.6억 달러, 45.8%) 등의 신흥시장은 신규 수요 증가로 인해 수출이 꾸준히 증가 추세

• 무선근거리통신망 보안

- 가까운 일본에서는 무선 근거리통신망(LAN)을 중심으로 발전하고 있고 아직 무선랜 시장은 규모가 크지 않은 편이지만, 서비스 제공업체들의 부가가치 옵션으로 매우 중요한 역할을 함. 실제로 소프트뱅크 그룹(Softbank Group)의 재팬 텔레콤(Japan Telecom)이 맥도날드와 협력해 일본 내 맥도날드 매장의 70%에 무선랜 서비스를 공급
- 대만의 ICT 산업 연구기관 마케 인텔리전스 센터(MIC)는 2006년 4/4분기 대만 WLAN 업계의 WLAN 네트워크 인터페이스 카드(NIC) 출하량이 전년 동기 대비 16.4% 증가한 4천 62만 개에 달할 전망이며, 대만 업계의 AP 출하량은 10.1%감소한 136만 개에 이를 것으로 발표
- 무선랜 시장과 직접적으로 관련이 있는 전 세계 노트북 PC 시장은 2006년 상반기 동안에는 다소 침체되었지만 3/4분기에 다시 높은 성장률을 기록한 후, 2007년 1/4분기에는 인텔의 새로운 무선랜 기술이 적용된 산타 로사(Santa Rosa) 플랫폼과 마이크로소프트의 윈도 비스타(Window Vista) 운영시스템이 선보이면서 WLAN NIC와 노트북 출하량이 모두 상승세를 탈 것으로 기대

• 차세대네트워크 보안

- 세계 정보보호시장은 2004년 274억 달러 규모로 파악되며, 향후 연평균 16.9%로 성장하여 2009년에는 600억 달러에 이를 것으로 전망
  - 부문별로는 정보보호서비스 시장이 연평균 18.9% 성장률로 2009년에는 전체의 약 50%를 점유함으로서 가장 큰 시장을 형성할 전망이며 소프트웨어 분야가 192억 달러, 하드웨어 부문은 117억 달러에 이를 전망
  - 2009년까지 연평균 성장률 측면에서는 정보보호 서비스 부문이 약 19%의 성장률로 가장 높을 것으로 전망되고 소프트웨어 분야는 14%의 성장률 전망
  - 소프트웨어의 단독 제품들이 여러 가지 소프트웨어 기능을 가진 하나의 하드웨어 제품에 통합되어 가는 경향 때문에, 소프트웨어 부문보다 하드웨어 부문의 성장률이 더 높은 것으로 분석됨

〈세계정보보호 시장전망〉 (단위: 백만달러)

구분	2004	2005	2006	2007	2008	2009	CAGR(%)
정보보호 H/W	5,237	6,309	7,413	8,703	10,275	11,761	17.6
정보보호 S/W	10,000	11,852	13,689	15,552	17,396	19,222	14.0
정보보호 서비스	12,210	14,488	17,284	20,590	24,521	29,002	18.9
합계	27,447	32,649	38,386	44,845	52,192	59,985	16.9

출처 : IDC, Worldwide IT Security Software, Hardware, and Services 2005-2009 Forecast : The Big Picture

- 네트워크 보안시장 현황

◦ Firewall/VPN : 시장조사 전문 기관인 Frost & Sullivan이 발표한 "아시아 태평양 네트워크 보안 시장" 조사결과에 따르면, 시스코 시스템즈가 하드웨어 Firewall/VPN 시장에서는 2 7.9%를 차지하는 것으로 조사되는 등 아시아 태평양 지역 최대의 네트워크 보안업체로 나타났으며(시장점유율 23.4%), 시스코의 뒤를 이어 주니퍼(Juniper)가 아시아 태평양 네트워크 보안시장에서 11.9%의 점유율로 2위를 차지했고, 3위는 소프트웨어 업체인 체크포인트(Check Point)로 나타남

◦ IDS/IPS : 현재 세계적인 IDS 제품은 Realsecure, Netprowler, Dragon, Blackce, PIX 등이 있으며, 3Com의 TippingPoint IPS, Radware의 DefensePro 제품 등이 있음

◦ UTM : 현재 UTM 보안 장비 시장분야에는 포티넷을 필두로 시만텍, 시큐어컴퓨팅, 서브게이트, 주니퍼(넷스크린) 등이 시장에 진출해 치열한 경쟁을 보이며, 향후 UTM 보안 장비를 공급하는 업체가 더욱 늘어날 것으로 예상됨

◦ 보안패치시스템 : 미국의 애버딘(Aberdeen) 그룹은 전 세계 보안패치 시스템 시장이 지난해 20억 달러 규모를 기록하며 급성장했고, 향후 매년 50% 이상의 성장을 보이며 2007년에는 약 60~70억 달러 규모로 성장할 것으로 전망

◦ 보안 이벤트 시각화 : 미국 NASA로부터 우주항공 구성요소들의 추적 기술을 전수받은 HighTower 사의 제품과 DARPA 연구 프로젝트 참여자로 구성된 SecureDecisions 사의 DecisionScopeTM 제품이 2002년 전후부터 HD 시각화 기반의 미래 시장을 개척하고 있음

◦ 공격(자) 역추적 : 시만텍의 해커 유인용 Honeypot 위장 서버(맨트랩, ManTrap)와 해커 자동 역추적 탐지 소프트웨어(맨헌트, ManHunt)가 있음

◦ 무선 메쉬 네트워크 : 국내에 비해 인프라 전개 속도의 예상 수준은 낮으나 미국 등 선진국의 경우 국내에 비해 기술적 연구 수준이 뛰어나며, 통신 장비 등 요소 기술의 수준이 국내에 비해 매우 뛰어나므로 시장 요구가 있을 경우 대응하는 속도가 즉각적이고 빠를 것으로 예상됨

• 통합보안관리

- 세계 통합보안관리 기술은 네트워크 장비 업체(CISCO, NOKIA 등)를 중심으로 UTM (Unified Threat Management) 어플라이언스, ITSoC 및 보안모듈 형태로 네트워크 장비에 통합하는 추세임
  ◦ 시장조사업체 「데이터모니터」에 따르면 오는 2003년 네트워크 보안시장 규모는 미국시장이 46억 8000만 달러, 유럽 24억 6,000만 달러, 기타 지역이 9억 6,000만 달러에 이를 것으로 전망되며, 국내 보안 시장의 규모는 매년 연평균 약 100% 이상의 성장률을 보여 2007년 약 2억불(2,300억원)에 이를 것으로 예상
- 벤더별로 제공하는 제품에는 다소 차이가 있지만 일반적으로 NAC는 사용자 PC 에이전트, 인증 및 접속 정책 관리 장비, 접속 정책 실행 장비로 구성되며, 제품으로는 CISCO 네트워크 입장 통제(Network Admission Control), 마이크로소프트사의 NAP(Network Access Protection), 그리고 TCG의 TNC(Trusted Network Connect) 등이 주도하는 추세임
- 사이버보안 동향
  ◦ 미국인의 70%가 인터넷 및 컴퓨터 보안에 대한 우려하고 있으며, 미국인의 74%가 인터넷상의 그들의 개인정보가 도난되어 악용될 것을 우려하고 있는 것으로 조사
  ◦ 그리고 미국인의 74%가 전화네트워크 혹은 발전소 등과 같은 국가 주요 인프라에 대한 테러리스트들의 사이버 공격이 있을지 모른다고 우려하는 것으로 미국 정보기술협회(Information Technology Association of America ; ITAA)와 Tumbleweed Communications Corp.의 공동조사결과 나타남

• 서버보안

- 세계 정보보호시장은 2004년 274억 달러 규모로 파악되며, 향후 연평균 16.9%로 성장하여 2009년에는 600억 달러에 이를 것으로 전망

〈세계정보보호 시장전망〉 (단위: 백만달러)

구분	2004	2005	2006	2007	2008	2009	CAGR(%)
정보보호 H/W	5,237	6,309	7,413	8,703	10,275	11,761	17.6
정보보호 S/W	10,000	11,852	13,689	15,552	17,396	19,222	14.0
정보보호 서비스	12,210	14,488	17,284	20,590	24,521	29,002	18.9
합계	27,447	32,649	38,386	44,845	52,192	59,985	16.9

출처 : IDC, Worldwide IT Security Software, Hardware, and Services 2005-2009 Forecast : The Big Picture, 2005.12

- IT 서비스간 연동 및 융 · 복합화 추세에 따라 향후 2010년 정보보호공통플랫폼 산업 및 시장 규모가 2조 9,603억 원으로 확대될 전망 (출처- IITA, 2006. 8)
- NSA에서는 Linux를 기반으로 기존의 보안 구조(Flask Architecture)를 통합한 Secure Enhanced Linux를 개발하였고, 현재 Linux 커널에 보안 기본 기능이 탑재된 운영체제가 시장을 주도할 것으로 전망

• PC보안

- Worldwide Client Antivirus Revenue, 2005- 2010($M)

	2005	2006	2007	2008	2009	2010	CAGR
Rev	2,837.7	3,225.2	3,572.5	3,860.9	4,032.9	4,202.3	8.2%

(출처 : Worldwide Antivirus 2006-2010 Forecast Update and 2005 Vendor Analysis, IDC, 2006)

• 디지털포렌식

- 전 세계 사건 대응 시장은 2005년 $22억에서 연평균 19.2%씩 증가하여 2010년에는 $53억에 이를 것으로 추정됨 (IDC, 2006)
- 최근 미국의 경우 디지털 포렌식 서비스 시장 규모는 $15억 달러 이상으로 추정되며, 최근 3년간 60% 이상의 급속한 성장을 지속하고 있음 (Guidance Software, CEIC 2006)

〈표〉 디지털 포렌식 세계 시장의 성장 추세 (단위: US $M)

구분		2005	2006	2007	2008	2009	2010	성장율
Digital Forensic (e-discovery)	SW	429	557	686	824	939	1002	18.5
	HW	45	55	71	82	106	109	19.4
	서비스	1,725	2,128	2,544	3,086	3,632	4,177	19.3
	소계	2,199	2,740	3,301	3,991	4,677	5,288	19.2

※ Worldwide Legal Discovery and Litigation Support Infrastructure 2006-2010 Forecast, IDC, 2006

2.2. 기술개발 현황 및 전망

2.2.1. 국내 기술개발 현황 및 전망

• USN 보안

- 정부정책기조

◦ USN 공공부문: 정보통신부 산하 한국정보사회진흥원(NIA)을 통해 USN 활용 산업 기술 저변확대 중. 그 분야로는 항만, 물류관리, 도시건축, 환경, 국방 및 보건 산업 등에 이미 시범과제를 통해 이미 600억 이상의 시장이 확보되었고 또한 활용 가능성 및 수출에도 어느 정도의 시장이 확보됨. 2007년부터 R&D에 투자를 늘릴 계획이며 송도에 연구단지 조성 계획이 이를 뒷받침 함. RFID 의 적극 개발 활용으로 원가 하락을 이미 확보함

◦ 그러나 보안 기술이 기반이 되지 않을 경우 USN 의 활용에는 많은 제약이 따르므로 경량의 USN 보안 기술 개발에 연구가 KISA, ETRI, NIA 등에서 진행 중임

- USN 보안 표준화 항목 : 인증 및 Key 관리, 공격탐지, Secure Routing, Secure Localization 등이 중요 쟁점 사항이며 국내외에서 기술 개발에 박차를 가하고 있는 상황임

- 국내 특허출원 현황 및 전망 : 현재 19건 정도의 USN관련 특허가 최근 등록되었으며, USN 보안 관련 특허는 2건으로 미약하나 증대될 것으로 사려됨

특허명	등록번호	등록일	출원인
센서 네트워크에서 공간 효율적인 결정적 비밀키 분배 방식	10-2005-0129205	2005.12.24	중앙대학교산학협력단
센서네트워크 환경에 적합한 센서 인증 시스템 및 방법	10-2005-0027303	2005.03.31	니츠

• 휴대인터넷 보안

- 국내기술 현황

◦ KT 와이브로는 2007년 4월 서울 전지역으로 서비스 지역을 확대했으며, 2007년 6월 IMS 기반의 통합커뮤니케이션 서비스 플랫폼을 국내 최초로 구축하여 HSDPA 사용자와 영상통화가 가능

◦ 또한, 지상파 DMB 방송사 U1 미디어와 협력하여 와이브로를 통해 실시간으로 방송에 참여할 수 있게 됨

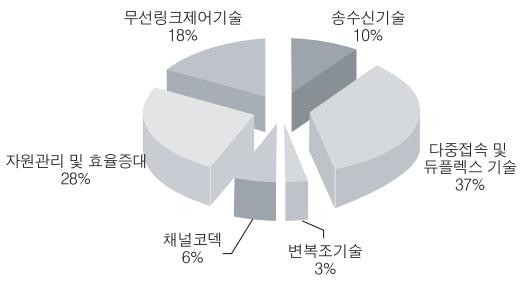
◦ 한편 SKT는 사업활성화에 적극적으로 나서고 있지 않는데, 이는 와이브로가 SKT가 보유하고 있는 2G, 3G 사업 분야를 잠식할 우려가 있기 때문

- 국내 특허출원 현황 및 전망

◦ 2.3Ghz 대역을 활용한 와이브로를 위한 국내 표준화에 포함되는 특허출원 분석을 위해 TTA 홈페이지, 2.3Ghz 대역을 활용한 휴대인터넷을 위한 국내 표준특허 기술 리스트를 조사한 결과, 삼성전자, SKT, KT, ETRI, 하나로통신 및 KTF를 포함하는 공동출원이 많은 것으로 나타났으며, 와이브로와 관련된 특허출원은 아래 그림에서 보듯이 다중접속 및 듀플렉스 기술(37%), 자원관리 및 효율증대(26%), 무선링크제어 기술(18%)순으로 물리계층과 매체접속 제어계층에 대한 출원 내용이 많이 포함

기술분류	개수
송수신기술	22
다중접속 및 듀플렉스 기술	79
변복조기술	7
채널코덱	14
자원관리 및 효율증대	56
무선링크제어기술	38
응용서비스기술	1
총 계	217

〈와이브로 국내특허 출원현황〉



(특허청 전기전자심사본부, 와이브로 기술분야 특허출원현황)

• 홈네트워크 보안

- 홈네트워크 기술은 크게 무선 홈네트워크 기술과 유선 홈네트워크 기술 형태로 나뉨
- 무선 홈네트워크 기술에는 Bluetooth 기술, UWB 기술, Zigbee 기술, Home RF 기술 등으로 분류
  - Bluetooth 기술은 근거리 무선 통신에 기반을 두고 근거리, 일대다, 음성과 데이터 전송을 위한 무선 방식을 채택하면서 보통 10m 이내 거리의 통신이 가능하고 최대 100m까지도 확장이 가능
  - UWB 기술은 통신이나 레이더 등에 주로 응용되는 무선 시스템으로 광대역 에너지를 수신하여 신호를 검출하므로 협대역 통신 신호에 의한 간섭 특성이 우수하고 보안 통신에 적합한 기술
  - Zigbee 기술은 인터넷을 통한 전화 접속으로 홈오토에이션의 편리성을 위해 출발한 기술로서 버튼 하나의 동작으로 집안 어느 곳에서나 전동제어 및 홈 보안 시스템, VCR On/Off 등이 가능
  - Home RF 기술은 데이터 및 음성 트래픽을 모두 지원하는 시스템으로 2.4㎓ 대역을 사용하여 가정 내의 PC를 중심으로 가전기기와 연결하는 홈 네트워킹을 구성하는 기술
- 유선 홈네트워크 기술에는 IEEE1394, Home PNA, PLC, USB 등으로 분류
  - IEEE1394는 차세대 홈 네트워크 인터페이스 기술로 주목. 전송속도가 매우 빠른 점을 이용하여 동화상 정보를 실시간 처리하거나 디지털카메라 등과 멀티미디어 주변기기를 연결하여 사용할 수 있을 뿐만 아니라, PC를 통한 화상회의 등 응용분야에서 기능의 우수성을 발휘하고 있음. 향후 다양한 홈 디지털 서비스를 편리하게 이용될 수 있는 표준화 기술 확보가 중요한 시장 선점의 관건으로서, IP 기반 기술과 무선 기술이 시장 활성화에 큰 역할을 할 것으로 기대

• 이동통신망 보안

- 국내 WLAN과 Wibro 망에 대한 개별 접속 보안 기술이 개발되었으나, WLAN-WLAN, Wibro-Wibro, WLAN-Wibro간 연동 및 핸드오프 관련 보안 기술은 아직 개발되지 않음
  - IEEE802 무선망 가입자 인증 및 키분배 기술로 IEEE802.1x (port based network access control)와 EAP(Extended Authentication Protocol) 기술이 개발됨

◦ 현재, 전용 무선단말기를 이용하여 WLAN, Wibro, CDMA 등 무선 보안 서비스가 일부 제공되고 있으나, 아직까지 정부에서 개인영역 무선망(WPAN)에 대한 보안 기술을 개발한 사례는 없음

◦ 초기 무선 접속망에서 제공받은 보안 강도의 손상없이, 새로운 무선 접속망으로 빠르게 보안 접속점을 이동하는 서비스, 무선 DoS, 무선단말기 ID추적, 위장 공격 등으로부터 정당한 사용자와 무선 인프라를 보호하는 기술은 기초 연구 단계 수준임

- CDMA 휴대 단말기의 무선 인터넷 표준 플랫폼으로 WIPI2.0이 제정되었으며, 최근 WIPI 플랫폼에서 Wibro, DMB, RFID 서비스 제공을 위한 WIPI개선 방안이 논의 중임

◦ 현재, WIPI 플랫폼은 사업자가 인증한 모바일 코드만 실행되게 되어 있는데, 망개방 및 융 · 복합 서비스 등장으로 인하여 악성코드로부터 플랫폼을 보호하는 보안 이슈가 현안으로 등장함

- 모바일 인터넷과 무선랜의 연동을 위한 다양한 시도가 이루어지고 있음. KT의 무선랜과 KTF의 CDMA 1x, EV-DO를 결합한 NESPOT Swing이 서비스 중이며, 이는 듀얼-모드 PDA를 이용하고 있음

• 무선근거리통신망 보안

- 무선 인터넷 보안 분야는 국내나 국외나 아직까지 많은 발전 가능성이 있고, 현재에도 꾸준히 연구되고 있는 분야임. 또한, 현재 사용자들의 고속화 고용량화 등의 높은 욕구에 발맞추어 WiMAX등의 기술이 선을 보이고 있지만, 그 보안 상태는 아직 미지수로 남아있는 실정. 무선인터넷 보안기술의 발전은 무선인터넷 부분에서의 시장 확대뿐만 아니라 전체 보안 산업의 발전을 가져올 것으로 기대. 뿐만 아니라, 무선인터넷의 지속적인 발전은 유 · 무선 통합 환경의 등장으로 이어질 것으로 예상

- 한국은 이동 음성시장의 성장이 포화상태로 접어들면서 무선 데이터, 모바일 부가서비스 등의 시장이 성장기에 접어들었음. 특히 국내 시장의 경우 증권거래, 은행거래, 회사의 인트라넷업무, 게임, 전자상거래, 티켓예매, 채팅 등 다양한 무선 응용 서비스가 활발하게 구축 및 운영되고 있어 이 같은 무선 데이터 서비스들을 안심하고 이용할 수 있는 보안이 어느 나라보다 중요. 국내 무선보안 시장은 세계적 추세와 마찬가지로 무선랜 보안과 무선PKI 두 가지측면에서 전개되고 있음. 그외에 휴대폰용 안티바이러스 제품, 위피용 보안 솔루션 등이 틈새시장을 공략

- 한국정보보호산업협회(KISIA)에 따르면 무선인터넷보안 분야는 2002년 사업자체의 활성화 부족으로 시장규모가 40억원으로 미비한 시장을 형성. 하지만 2003년 63억원에 이어 2005년에는 시장규모가 100억원 정도에 이르고 2007년에는 시장규모가 140억원까지 확대될 것으로 전망

- 국내에서는 주로 데이터 송수신시의 암호화 키 생성과 불법 장비 탐지에 관한 특허가 주를 이루고 있으며, 국제적으로 새로운 표준이 개발 중이여서 앞으로 많은 특허 출원이 이루어질 전망

• 차세대네트워크 보안

- 주요국가의 정책기조

◦ 정부는「유비쿼터스 정보보호 기본전략」(2006.12)을 수립하여 안전한 정보인프라 구축을 위한 BcN 통합안전관리

체계 구축

· 휴대폰, PDA 등 차세대 지능형 단말기 보급증가에 따른 신종 웜 · 바이러스 예방대책 마련

· 신규 사이버 공격에 대해 국가 대응체계를 강화하고, 침해사고 예방 · 대응 기술 고도화를 위해 「BcN 환경을 고려한 침해사고 조기 예 · 경보 시스템」개발 추진

· 개별 서비스 장애나 침해사고 발생시 피해가 전체망으로 확산되는 것을 방지하기 위한 침해사고 격리 메커니즘 개발 추진

◦ BcN 주요 인프라 및 서비스에 대한 지속적인 안전성과 신뢰성 확보를 위한 법 · 제도적 개선방안 마련

· VoIP 등 신규 서비스의 상용화에 따라 서비스 게이트웨이 등 BcN 인프라에 대한 기반시설 지정 추진

· BcN 서비스 제공자에 대한 안전진단 대상으로 지정하고 ISMS 수검을 유도하여 자발적인 보호대책 수립 · 적용을 위한 제도 개선추진

· BcN 인프라 보호를 위한 정보보호 필수항목 및 가이드라인 개발 · 적용 추진

※ BcN 시범사업주관기관 및 BcN 컨소시엄 참여사 등의 정보보호 협의체를 구성하여 필수항목 도출 및 적용

◦ 메쉬 네트워크 기술 적용이 가능한 u-City와 관련된 다양한 프로젝트가 진행 중임

· 행정중심복합도시의 u-City 프로젝트가 2007.7부터 시작될 예정

· u-City 법제도 정비 (u-City 건설지원법 마련, 2007년 확정 · 공포 예

· 현재 정통부, 건교부, 지자체 등이 공동 참여하는 u-City구축추진 TFT에서 추진 중임

– 국책연구소, 산업계, 학계의 기술개발 현황

◦ BcN 광대역 환경에 적합한 고성능 네트워크 보안장비 개발

· 이상트래픽을 감지 · 차단 · 대응하는 고성능 네트워크 통합 보안장비와 RFID/USN 환경에 적합한 초경량 암호 모듈 및 시큐어 센서노드 개발 중

· ETRI 중심으로 2006년 실시간 H/W기반 100만 세션 동시 처리가 가능하고, 패턴매칭 · 비정상행위분석 기반의 침입탐지가 가능한 20Gbps throughtput의 '고성능 침해대응 시스템' 개발 완료

· LG엔시스, 윈스테크넷, 시큐아이닷컴 등 중소 보안전문업체 중심으로 수기가급 침입방지시스템, 방화벽 등의 보안장비 개발 및 보급

◦ 이동 무선 환경이 상용화되고 있으나 유무선 통합 환경을 고려한 보안 기술에 대한 연구는 초기단계

· 국내 WLAN과 Wibro 망에 대한 개별접속 보안기술이 개발되었으며, 모바일 RFID 단말기, WLAN + WiBro 단말기, CDMA + WLAN 단말기 등과 같이 멀티-무선 링크를 지원하는 융 · 복합 단말기 기술이 개발되고 있음

· 이동 무선 환경은 국내 업체가 WiBro, HSDPA 등을 세계 최초로 상용 서비스를 시작할 정도로 가장 높은 수준에 있으나, 유무선 통합 환경을 고려한 보안기술 개발은 초기단계

◦ 무선 매쉬 네트워크에 대한 연구는 미래 인터넷 인프라 구축 및 서비스 제공을 위한 연구 분야에서 활발히 이루어지고 있으나 이의 보안에 대한 연구는 거의 전무한 상태임

· 현재 KT와 기상청이 공동으로 기상/해양 관측을 위한 메쉬 네트워크 시험망을 구축하거나, 무선 메쉬 네트워크

구축과 상용 서비스 제공을 위한 기술 개발에만 초점

· 보안 기술의 적용 가능성 검증을 위한 요구사항 정립단계

• 통합보안관리

- 정부정책기조

◦ 차세대 네트워크 보안솔루션의 다양한 요구사항을 충족할 수 있는 고성능 네트워크 위협대응 기술이 개발되어 상용화 시도 중임

◦ IT 839 전략을 핵심엔진으로 하는 u-Korea 유비쿼터스 사회의 인프라를 안전하게 유지하고 네트워크에 대한 사이버테러에 강력하게 대응할 수 있도록, 네트워크 인프라에 대한 정보보안을 강화한 고성능 네트워크 통합보안관리 시스템 개발 및 구축될 것으로 전망됨

- 국책연구소, 산업계, 학계의 기술개발 현황

◦ 통합보안관리(ESM: Enterprise Security Management) 기술은 침입차단시스템, 침입탐지시스템, 가상사설망 시스템 등 다양한 종류의 보안시스템들을 상호 연동하여 각 기능을 통합 관리하는 중앙집중식 관리체계로서, 보안 관제서비스 업체, 보안 시스템 개발 업체들간에 컨소시움 형태나 독립적인 통합보안관리 시스템으로 개발되고 있음

◦ 통합보안관리 기술 수준은 현재 자사 제품에 대한 모니터링 기능이 구현되어 있지만, 앞으로는 보안프로토콜의 표준화를 통해 타사 제품을 포함한 이기종 보안 시스템에 대한 모니터링 기능을 가지도록 발전하고 있으며, 소규모 네트워크 차원에서 단수 모니터링 및 보안정책을 적용하는 형태이나, 향후의 통합보안관리 기술은 네트워크 전체를 보안 관리 영역으로 확장될 것으로 예상

◦ 단순하게 보안장비를 통합적으로 관리하는 범주에서 벗어나 점차 네트워크 장비 및 시스템까지 연계하여 관리해 주는 시스템으로 진화 발전할 것으로 전망되고 있음

◦ 유무선 통합망의 백본 IP Core 망 인프라의 고성능 처리능력에 비해 현재의 정보보호 장비의 처리능력은 미흡하며, 현재 차세대네트워크보안은 소규모 네트워크 차원에서 단수 모니터링 및 보안정책을 적용하는 형태를 초월하여 향후의 네트워크 보안은 네트워크 전체를 보안 관리 영역으로 확장이 전망됨

- 사이버보안 동향

◦ 라우터와 스위치를 개발하던 한아시스템에서 다양한 보안 제품을 개발 출시 예정. 기존의 네트워킹 장비 회사들의 보안 시장 진입도 많이 나타남

◦ 앞으로는 단순히 네트워킹 기능뿐만이 아니라 보안 기능이 필수적으로 제공되는 장비들이 시장을 주도하게 될 것이며, 그리고 점차로 수동적인 방어 위주보다는 역추적과 공격 등 대응 개념이 들어간 능동 보안 개념의 제품들이 개발되어 질 것으로 전망

• 서버보안

- 정부정책기조

◦ 2007년 3월부터 시행된 정보통신법 개정안에 따라 인터넷상에서 ID와 비밀번호, 연락처 등 개인 정보를 수집 활용하는 정보통신 서비스 제공자들은 고객의 개인 정보를 보호하기 위해 보안 서버 구축을 의무화 함으로 인해 보안 서버 인증서가 활성화 되며, 기능 업그레이드를 위한 보안 운영체제 및 웹서비스용 분산 클러스터 시스템의 보안 기능 등이 개발될 전망

- 기술 개발

◦ 1991~1992년 ETRI에서 "정보통신 시스템 기반보호를 위한 안전한 운영체제 기술 연구"를 통하여 리눅스 및 FreeBSD 에서 서버형태로 사용할 수 있는 접근제어, 사용자인증, 암호화 파일 시스템등의 보안기술을 개발하고 국내업체를 대상으로 기술이전을 통한 상용화를 추진한 바 있으며, 최근들어 업체를 통해 은행권과 정부 기관의 서버 보안 사업을 수주함

◦ 2006년 부터 3년 계획으로 ETRI에서 "임베디드 보안 운영체제 기술 개발" 과제를 수행중이며, 분산 클러스터 시스템에서 플랫폼의 무결성 제공을 위한 "분산 클러스터 보안 미들웨어 기술 개발" 과제도 2007년부터 5년 계획으로 수행 중임

- 국내 특허출원 현황 및 전망

◦ DAC, MAC, RBAC 등 접근 제어 기술과 신뢰채널 기술에 대한 특허들을 다수 확보하고 있으며, 최근에는 개선된 접근 제어 기술에 대한 특허와 웹서비스 환경에서의 인증 기법 등과 같은 특허들이 출원될 전망

◦ 최근에는 플랫폼 무결성 차원에서의 신뢰 플랫폼 기술에 대한 특허를 다수 확보하고 있으며, 신뢰 플랫폼 모듈 기반의 키관리, SW 무결성 제공 기술에 대응할 수 있는 특허권을 확보함으로써 시장 선점 노력

• PC보안

- PC보안 분야를 주도하고 있는 Anti-Virus(Anti-Spyware)에서 악성 코드는 크게 바이러스, 웜, 트로이목마로 정의되고 있고 최근 스파이웨어나 스팸 메일, 피싱등의 대응책도 통합되어 가고 있는 추세이며 각각의 악성 행위에 대응하기 위한 관련 연구가 지속적으로 연구되어 별도로 구현된 제품들이 통합된 형태로 발전하고 주목받고 있음

- 항상 변화하는 악성코드에 따라 방지 지침이 지속적으로 Update되어야 할 것이며 접근 통제는 서버에서 사용되던 기술들이 개인 컴퓨터에 적용되고 그 기술 또한 발전하고 있으며 통합되는 형태로 제품화가 이루어지고 있기 때문에 관리적인 측면에서 표준화가 필요

- Anti-Virus대응기술

◦ 2000년 이전까지 도스용에서 윈도우용까지 컴퓨터바이러스가 주된 PC보안 대응기술이었고 네트웍의 발달로 더 이상 파일 매개체를 이용한 바이러스의 감염 방법보다는 네트워크을 통하여 시스템을 감염시키는 웜의 피해로 인한 대응기술로 변화하였고 최근에는 웹을 통한 트로이목마로 인한 피해가 증가하고 있는 추세로 관련 기술도 이런 악성코드의 변화에 따라 발전해 나갔으며 기존 PC안에서 파일단위로 대응하던 기술에서 사용자의 조작 없이 스스로 번식하는 웜이나 네트워크나 인터넷을 통해 연결된 컴퓨터에 쉽게 감염될 수 있기 때문에 인터넷을 통해 받은 파일들의 실시간 검사, 주기적인 업데이트 및 공격방법을 알아내어 취약점을 알려주고 의심스러운 파일들을

사전에 차단하는 기술들이 연구되고 있음

◦ Signature관련 기술은 Anti-Virus분야에서 앞으로도 계속 사용될 기술이지만 현재 DB의 양이 커짐에 따라 DB사이즈나 리소스 사용, 속도와 관련하여 개선하는 연구가 이루어지고 있으며 병행하여 행위기반이나 휴리스틱 진단 등 진단법 자체가 많은 변종과 새로운 공격 형태에 대응할 수 있는 기술들이 지속적으로 연구가 이루어지고 있으나 오진 등의 문제로 인해 사용자들에게는 제한적으로 그 기능들이 활용

◦ 최근에는 PC 뿐만 아니라 모바일 기기를 대상으로 한 악성 프로그램들이 발견되고 있고 아직은 심비안(Symbian) 운영체제로 제한적이기는 하지만 관련 기술개발도 연구

- Anti-Spyware 대응 기술

◦ 2003년 이후 악성코드 뿐만 아니라 PC보안분야에서 새로운 공격형태를 보이는 것이 스파이웨어

◦ 이것은 전세계적으로 아직 정의가 다르고 법/제도에서 적절하게 대응할 기준이 없는 틈새를 타고 전세계 사용자들에게 피해를 주고 있음.

◦ 스파이웨어는 웹서버나 개인 컴퓨터에 사용자 몰래 설치되거나 적절한 동의 절차없이 설치되어 컴퓨터 내의 정보들을 유출시키거나 광고를 보여주고 사용자가 원하지 않는 행위를 하여 불편하게 하는 류의 프로그램을 뜻하며 악성코드 범위로 포함하는 추세

◦ 스파이웨어는 초기에는 정보 수집에 도움을 주는 목적으로 제작되었으나 점차적으로 정보 유출 등의 악의적인 목적으로 사용되었으며, 최근에는 범죄에도 활용되는 것으로 분석되고 있으며 기존 바이러스나 웜, 트로이목마와 통합된 형태로 배포되는 형태도 나타남

◦ 또한, 최근에는 스파이웨어 차단 프로그램으로 가장한 허위 안티스파이웨어프로그램으로 인한 피해도 많은 실정

◦ Anti-Virus기술과 비슷한 기술로 대응할 수 있으나 조금 다른 형태를 가지고 있는 것은 스파이웨어를 위해 별도 진단기술이 있어야 하고 스파이웨어를 제거하는 기술도 Anti-Virus기술만으로는 대응이 복잡한 형태도 있었기 때문에 초기 Anti-Virus업체들이 별도 제품으로 대응하다 최근엔 통합하여 하나의 제품으로 대응

- Personal Firewall 대응 기술

◦ 개인 방화벽은 개인이 사용하는 컴퓨터용 방화벽을 의미

◦ 2000년 이후 웜이나 트로이목마와 같은 악성 프로그램에 의한 정보 유출 사례가 증가함하고 악성코드의 감염이 취약점을 통하여 이루어짐에 따라 네트워크 전체의 접근제어 용도로 사용되었던 기능을 개인 컴퓨터에서 사용 가능한 형태로 배포한 것

◦ 개인 방화벽 소프트웨어들은 프로그램별로 인터넷 접속 통제 기능을 제공하여 허용되지 않은 프로그램이 인터넷에 접속하거나 자기 시스템으로의 접근을 방지하여 사용자가 원하지 않는 인터넷 접속이 시도되는 것을 확인할 수 있으며 컴퓨터에 설치된 악성 프로그램의 외부 연결 시도와 침투를 통제할 수 있음

◦ 국내의 경우 초기 은행 사이트에서 ActiveX 컨트롤을 이용한 개인 방화벽에서 시작하여, 특정 윈도우 버전에서 기본 탑재되어 널리 사용하게 되었으며, 보안 관련 회사에서도 개인 방화벽 소프트웨어를 제공

◦ 최근에는 Anti-Virus 소프트웨어, 패치관리시스템(PMS: Patch Management System)등과 함께 하나의 기능

으로 통합되어 서비스를 제공하는 형태로 변화

- 국내 특허출원 현황 및 전망
  - 각 산업체별로 PC보안과 관련한 기술을 특허 출원을 강화하고 있는 추세로 점점 더 많은 특허출원이 이루어질 것으로 예상

• 디지털포렌식

- 정부정책기조
  - 검찰, 경찰, 국정원, 기무사 등 국가 수사기관은 한국의 IT 환경에 적합한 디지털포렌식 도구의 필요성을 절감하고 있으며, 일부 기관은 자체 개발 및 개발 중이나 통합 포렌식 도구를 개발하기에는 역부족임
  - 정보통신부는 IT 신성장동력 사업의 일환으로 한국전자통신연구원이 주관이 되어 산학연이 협력하여 국산 파일에 특화된 기능을 내장한 디지털 포렌식 도구 개발을 2007년 3월부터 시작하였음
- 기술개발 현황 및 전망
  - 국내의 포렌식 기술 개발은 최근까지 학교 및 몇몇 산업체를 중심으로 기본 기능 및 초기 수준의 기술 개발을 진행하였지만, 2007년부터는 출연연과의 협력을 통한 본격적인 개발에 착수함
  - 최근 국내 기업들도 자체 감사, 외부 감사 모의 실험, 기업간 법적 분쟁, 기업 내 기술유축 등의 영역에서 포렌식 솔류션 및 서비스 도입이 활발해 지고 있음
- 국내 특허출원 현황 및 전망
  - 컴퓨터 포렌식을 중심으로 한 디지털 포렌식 분야 특허 중 한국은 약 20%의 관련 특허를 출원 중에 있으며, 향후 모바일 포렌식 분야 특허가 활발해 질 것으로 전망됨

2.2.2. 국외 기술개발 현황 및 전망

• USN 보안

- USN 주요국가의 정책기조
  - 미국 : NITRD(Network and IT R&D) 주관의 8개 분야로 나누어 연간 20억달러 규모의 거대 연구가 DARPA, UC Berkeley에서 진행 중이며 각종 비즈니스 및 서비스 모델 개발에 전 부처가 박차를 가하고 있는 중임.
  - 유럽 : EU의 IST(Information Society Technology) 프로그램이 주축이 되어 복지 서비스를 타겟으로 Bio-MEMS 기술 등에 R&D 가 이루어지고 있음.
  - 일본 : 산학이 중심이 되어 2010에 UNS(Ubiquitous Network Society) 구현을 목표로 센싱기술 개발에 많은 역량을 투입하고 있는 것으로 보고됨.
- 주요 국가별 특허출원 동향
  - 미국 : 20여건 정도만 다보유 출원인인 경우 조사되어 있음.
  - 유럽: 정보 없음.

◦ 일본: 한국 RFID/USN협회에 따르면 200여개의 특허가 출원 및 등록되어 있으며, 주로 기업이 출원인으로 재산권을 확보해 좋은 상태

• 휴대인터넷 보안

- 미국 기술개발 현황 및 전망

◦ 미국은 전역에 와이맥스 서비스를 상용화 할 계획

◦ 2008년 말까지 Sprint와 Clearwire는 미국전역에 와이맥스망을 공동 구축하기로 합의했으며, 이를 위해 각자 담당 지역에서 네트워크를 구축하고 상호로밍이 가능하도록 진행할 계획

◦ 부정적인 시각을 가지고 있던 시스코 역시 와이맥스 시장에 참여할 예정이며, 관망하고 있던 노키아지멘스도 모바일 와이맥스에 주력할 예정

◦ 이러한 시장변화에 따라 구글도 스프린트와 모바일 와이맥스 서비스를 제휴

◦ 구글은 무선인터넷 검색과 소셜 네트워크 사이트, 인스턴트메신저, e메일 등 어플리케이션을 제공

◦ 이에 따라 2010년에는 총 1억 2500만명이 와이맥스 서비스를 사용할 수 있을 것으로 전망

- 일본 기술개발 현황 및 전망

◦ 일본 역시 2007년 5월 도시바와 노텔이 와이맥스 기지국을 공동 개발

◦ 2010년 40억달러로 추산되는 와이맥스 기지국 시장에 대응하기 위해 제휴를 맺고 일본내 사업은 도시바가, 해외 사업은 노텔이 맡기로 함

◦ 도시바가 보유한 고주파 증폭기술과 노텔의 직교주파수다중분할(OFDM) 입출력 기술을 접목할 계획이며 도시바가 라디오 모듈 분야를, 노텔은 기지국용 디지털 모듈을 개발

◦ 도시바는 2010년 4억달러로 예상되는 일본 와이맥스 시장에서 25%를 점유할 계획으로 추진

- 유럽 기술개발 현황 및 전망

◦ 유럽에서는 2007년 8월 가장 큰 이동통신사 중 하나인 보다폰이 3세대 통신인 UMTS 이후의 통신기술로 와이맥스를 채택하고, 와이맥스 포럼에 주요 협력사로 참여할 예정

◦ 보다폰은 지금까지 3G 이후에 4G 기술로 3G LTE를 선택하겠다는 입장으로 진행하여 왔으나, 3G LTE 기술이 상용화까지 상당한 시간이 걸릴 것으로 예상되어 방향을 전환

• 홈네트워크 보안

- 해외에서는 유 · 무선 통합화와 디지털 컨버전스의 급속한 진전으로 FTTH 등의 차세대 초고속 유무선 인터넷과 연계되어 가정에서 다양한 통신 · 방송 · 게임이 융합된 서비스 제공을 위한 가정용 디지털 허브로서의 홈서버 기능이 부각

- 선진 외국의 각 사가 우위를 점하고 있는 제품을 기반으로 홈플랫폼을 구축함으로써 홈네트워크 조기 시장 선점을 위한 경쟁이 가속화되고 있으며, 홈게이트웨이는 다양한 홈 네트워킹 기술을 지원하고 홈네트워크 서비스를 지원할

수 있도록 홈서버 기능이 통합되는 형태로 진화

- 가정내 다양한 가전기기들에 대한 홈네트워크 보안 기술의 중요성이 빠르게 확산되고 있으며, 홈게이트웨이 플랫폼을 통한 정보보호 및 보안성 확보에 연구가 집중되고 있으며, 마이크로소프트에서는 가정에 있는 모든 플랫폼에서 Embedded Windows를 수행할 수 있게 하거나 PC 형태의 장비를 가정 제어 등을 위한 홈서버로 제공하기 위한 기술개발을 진행중
- 마이크로소프트, Intel, SONY, 삼성전자를 중심으로 결성된 DLNA에서는 UPnP를 이용한 다양한 장비의 상호운용성 해결에 많은 노력을 기울이고 있으며, Windows XP는 UPnP가 탑재된 최초의 마이크로소프트의 운영체제로서 UPnP가 지원되는 장비로는 홈 데이터 라우터가 포함
- 이외에 디지털 컨버전스의 가속화로 통신, 방송 및 게임 등 엔터테인먼트 서비스를 제공할 수 있는 개방형 서비스 프레임워크 및 서비스 통합 관리 솔루션 확보를 위한 기술 개발이 활발히 추진
- 유 · 무선 네트워킹 분야는 초고속 인터넷과 연계한 이더넷, 가전기기 제어를 위한 전력선 통신, AV 기기를 위한 IEEE1394 등 유선 기술과 Wi Media 및 IEEE의 WPAN 등 무선 홈네트워크 기술의 표준 경쟁이 심화되고 있으며, DS2에서 OFDM방식의 200Mbps급 전력선 통신 핵심 칩이 발표되었으며, 미국 HPPA에서는 200Mbps급 고속 전력선 모뎀 규격(V2.0) 작업을 진행중
- UWB 및 무선1394와 같은 광대역 무선 기술과 ZigBee 등 위치기반의 저속 센서 기술이 등장하는 등 유선보다는 무선 기술이 시장을 지배할 것으로 전망되며, IEEE 802.15.3은 고속 WPAN의 물리층과 MAC층 표준을 완료하였으며, MAC층 표준은 UWB 물리층과 함께 사용될 것이고, 현재 Multi-band OFDM 안과, Dual-band DSSS안 중 표준안을 선택하는 작업이 진행중
- 유비쿼터스 홈컴퓨팅 분야는 MIT, IBM, MS, Sony, Panasonic, ESPRIT 등 선진기관에서 주변 환경에 따라 다양한 가전기기들을 동적으로 연결하여 서비스를 제공할 수 있는 상황 적응형 미들웨어 기술개발을 진행중이며, 시장 활성화를 위한 장비 및 소프트웨어 업체간의 결속 등 DLNA 표준활동을 통한 기기간 상호운용성 기술과 유비쿼터스 홈 구축을 위한 상황 적응형 미들웨어로 발전할 전망
- 지능형 정보가전 분야는 홈센서간 정보 교환이 가능하도록 홈센서가 지능화되고 착용 가능한 형태로 발전하고, RFID 및 유비쿼터스 ID를 기반으로 다양한 정보를 제공할 수 있도록 발전할 전망이며, AT&T, MS, Intel, HP, MIT의 미디어 랩 등에서 광대역의 저전력 무선 칩셋을 이용한 유비쿼터스 컴퓨팅 기술 개발을 강화

• 이동통신망 보안

- 이동 무선 환경은 국내 업체가 WiBro, HSDPA 등을 세계 최초로 상용 서비스를 시작할 정도로 가장 높은 수준에 있으므로, 유무선 통합 환경을 고려한 보안 기술 개발은 기술과 시장 선점의 효과가 있음
- 무선 네트워크는 셀의 크기, 통신 특성, 지향하는 타겟 서비스 환경에 따라서 각기 다른 링크 액세스 보안 기술이 개발됨
  ◦ 현재, 무선랜, Wibro, CDMA 등 개별 무선 IT서비스는 전용 단말기를 이용하여 보안 서비스 제공
    ※ WCDMA의 경우 USIM을 이용한 AKA(Authentication and Key Agreement) 기술 을 상용화하여 무선

데이터 통신 보안

※ 도청 방지, 비인가자 망 접속 차단, 위장 단말 및 기지국 차단, 무선 데이터 위변조 차단, 무선 침입탐지 등을 제공하는 전용 암호, 인증 및 보안 프로토콜을 연구

◦ 최근에는 동종 무선망간 핸드오프 또는 보안구조가 서로 상이한 이종망간 핸드오프시 지연시간을 최소화시키는 핸드오프 보안 기술이 미국을 중심으로 활발하게 연구 중임

※ 최근 CDMA + RFID, WLAN + Wi-bro, CDMA + WLAN 단말기 등과 같이 무선 멀티-링크간 융 · 복합 보안 서비스 기술을 미국, 유럽에서 연구개발 중

※ 미국은 IEEE802(Wireless Network) 무선 네트워크(802.11, 802.15, 802.16, 802.20)간 상호 연동 및 융 · 복합, IEEE 802 무선망과 이동 인터넷간 연동 기술을 개발

※ EU은 FP6의 FET(Future Emerging Technology)사업 일완으로 이종 무선망 (WLAN, CDMA, Wi-MAX)간의 융 · 복합 표준 인터페이스(Unified Link-Level API) 기술을 개발함 (GOLLUM 프로젝트, 2006. 3.)

- 개방형 무선(SDR: Software Defined Radio) 단말 및 기지국 기술, 멀티모드 지원 IT 컨버전스 단말기와 모바일 플랫폼 보안 기술 연구가 활발히 진행 중

• 무선근거리통신망 보안

- 대표적인 무선랜 전용 보안 기술들로는 WEP(Wireless Equivalent Privacy), 802.1x 등이 있으며, 현재 IEEE 802.11i 워킹 그룹을 중심으로 WPA(Wi-Fi Protected Access) 표준을 제정, 진화 · 발전되고 있는 상황. 그동안 무선랜 보안은 시장의 성장을 더디게 하던 부정적인 힘이었지만, 와이파이협회(Wi-Fi Alliance)에서 WPA(Wi-Fi Protected Access)를 발표한 이후에는 무선랜 보안이 무선랜 시장 성장의 원동력이 될 것으로 기대
- 사실 일부 벤더에서는 WPA가 발표되기 전인 2002년 중반부터 RrK(Rapid re-Keying)나 LEAP(Light EAP)등의 이름으로 엔터프라이즈급의 무선랜 보안솔루션을 보유 하고 있었지만 시장 활성화에는 큰 영향을 미치지 못함. 하지만 지금은 엔터프라이즈 급의 무선랜 보안이 필요한 시장에서 WPA라는 표준기술을 사용 할 수있는 기반이 마련돼 그동안 무선랜이 활성화 되지 못했던 금융시장이나 공공 시장 등에서도 무선랜의 적극적인 검토가 이루어지고 있음
- 하지만 아직 무선랜을 위한 보안 기술은 계속적으로 보완과 발전이 이루어지고 있는 현재 진행형 상태라 볼 수 있으며, 이러한 현실상의 공백을 채워주는 기술이 바로 무선(Wireless) VPN 기술
- 무선 VPN 기술은 이미 시장에서 존재하며 어느 정도 검증된 VPN 기술을 무선랜 기술과 결합시킨 것으로 현재 국내 및 해외 시장에서 무선 VPN은 가장 강력한 무선 보안 솔루션으로 인식. 이에 기존 VPN 솔루션 공급 업체의 움직임이 매우 활발한 편
- 특히 북미 지역의 많은 신생 네트워크 장비 업체들이 무선랜 스위치 시장에 도전장을 내밀고 VPN 기능을 기본적으로 갖추고 있으며 무선랜 관련 기능을 한층 강화시킨 새로운 개념의 장비들을 출시하고 있는 상황
- 무선 VPN은 현재 VPN 기술을 수용하면서 무선랜에 특화된 다양한 인텔리전스를 지닌 무선랜 보안 스위치와 같은 새로운 네트워크 장비의 영역을 만들어 내고 있음. 사실 2002년 초기만 하더라도 기업에서 VPN을 통해서 무선

랜 보안을 보강해야 하는 것이 비용적인 부담이 되었지만 소호에서의 VPN은 기존의 PC와 공유기나 보안 라우터에서 추가 비용 없이 적용 할 수도 있게 됨. 그리고 엔터프라이즈용 무선랜 보안 부분은 일부 벤더들에 의해서 WEP키를 다이나믹하게 갱신하는 무선랜장비의 기능이 구현 되면서 그 부담을 대폭 경감

- 2006년 15억 달러 시장이 기대되는 무선PKI는 기업의 내부행정, 전자결제, 그룹웨어 등을 휴대폰 및 PDA로 처리할 수 있는 모바일오피스, 제조 및 도소매 유통에 필요한 업무 프로세스를 무선환경을 통해 구현한 물류정보 서비스, 무선환경에서의 시스템 관리 및 원격제어가 가능한 원격제어 · 검침서비스, 전자결제를 통한 무선 전자상거래 등의 기업정보보호 등에 적용

• 차세대네트워크 보안

- 주요국가의 정책기조

◦ 미국은 9 · 11 테러를 계기로 국토안보부를 신설하여, 국가 사이버 공간 보호전략(National Strategy to Secure CyberSpace)을 수립

· 정보보호 위협 및 취약점 감소를 위하여 사이버 공격 예방 및 국가적인 취약점 평가절차 구축, 사이버 시스템 및 통신 설비에 대한 물리적 보안 개선 등 8가지 계획 수립

· 국가안보 및 국제 사이버 보안 협력 강화를 위한 미국 국가 안보 공동체 내의 사이버 공격 대응 조정 개선 등 5가지 계획 수립

※ 유비쿼터스 사회의 도입에 따른 정보보호 대책에 관해 기업, 연구소 등에서 활발한 연구 진행 중

◦ EU의 경우, '리스본 전략'과 'i2010' 전략을 성공적으로 추진하기 위한 기반으로서 정보보호 정책을 수립하여 추진

· EU 집행위의 정보보호 전략과 ENISA의 행동계획을 발표하고, '정보보호 문화 실현'을 위한 관련정책 강화하여 추진

· 2007년부터 2013년까지 추진될 제7차 Framework Programme에서 90억 유로를 연구개발에 투자할 계획을 세우는 등, IT 및 정보보호 경쟁력 확보를 위한 노력 진행 중

◦ 일본의 경우, 2005년 4월에 '유비쿼터스 시대에 있어서 우주통신의 기본방향에 관한 연구회'를 설치하고 유비쿼터스 스페이스넷 프로그램(Ubiquitous Space-Net Program) 발표

※ 'UNS 전략 프로그램'이란 유비쿼터스 네트워크 사회를 지향한 보편적커뮤니케이션 기술, 차세대 네트워크 기술, ICT 보안 · 안전 기술 등 3가지 중점연구개발 전략부문에 대한 첫 글자에서 따온 약자임

· ICT 보안 · 안전(Security and Safety) 기술개발 전략에서는 사이버 공격이나 대규모 재해에도 장애 없는 ICT 인프라를 실현하기 위한 기술개발 전략 수립

◦ 유비쿼터스 무선 네트워크와 관련해서 매쉬네트워크 기술을 적용시키는 사례가 학계에서 보고되고 있음

· National Taiwan University(타이완), Taipei시 전체

· University of Arkansas

· Nortel 본사, NASA 등

- 국책연구소, 산업계, 학계의 기술개발 현황

◦ 향후 백본에서 단말로 점차 기가급 환경이 보편화되고 10G 이더넷의 활용이 확대됨에 따라 BcN 보호를 위한 보안장비도 기가급 제품 및 10G 이더넷 제품의 출시가 진행 중

· 포티게이트, 티핑포인트, 라드웨어 등은 10G 인터페이스를 지원하는 보안장비를 시장에 출시

◦ 메쉬 네트워크 기술 및 기반기술 개발이 활발하게 이루어지고 있음

· "Adhoc Peer to Peer Muti-Hopping"기술이 모토로라를 중심으로 제품화 되고 있음

· QDMA(Quadrature Division Multiple Access : 모토로라 고유의 무선통신방식)으로 FDMA, TDMA, CDMA, DSMA/CA+의 결합기술이 발전됨

· 2.4GHz 비 면허 주파수 대역 활용과 끈김 없는 이동성 보장, 동적 패널선택으로 강력한 간섭 회피, 최적화된 주파수 이용, 고밀도 데이터 이용과 무선랜 대비 확장성이 우수한 것으로 진화하고 있음

• 통합보안관리

- 주요국가의 정책기조

◦ 미국은 1991년 말 정보통신 기술개발과 응용을 촉진하기 위해 고성능 컴퓨터 법을 제정하였으며, 1993년에는 이 법에 따라 미국 경제의 경쟁력을 제고 시키고 세계의 주도권을 확보하기 위하여 NII(National Information Infrastructures)라는 미국의 국가적인 정보화 전략을 발표했으며, 그에 따라 네트워크 보안기술 및 컴퓨터 시스템 보안기술의 정책 마련

◦ 중국은 컴퓨터 바이러스에 의한 테러가 원자탄을 사용하는 것보다 효율적인 전략 방법이라는 판단하에 1999년 해커부대를 창설하였고, 대만을 대상으로 7만2000건의 사이버 테러(2000년 8월)를 감행

◦ 일본의 경우 사이버테러전에 대비 2000년말 사이버부대를 창설하고, 테러공격을 방어하기 위해 1억4000만엔의 예산을 책정하여 강화

◦ 북한의 사이버전 능력은 미 국방부에서 모의 실험한 결과, 태평양사령부 지휘소를 마비시키고 미 본토 전산망과 전력망에 피해를 줄 수 있는 정도로 상당한 수준에 이른 것으로 추측

- 국책연구소, 산업계, 학계의 기술개발 현황

◦ 전술적 네트워크 운용 및 전략적인 네트워크의 직관적인 제어를 위한 통합보안관리 기술 관련 연구프로젝트는 전 세계적으로 2004년 전후에 시작하여 개별적으로 점점 확대되어 SIFT (Security Incident Fution Tools), NVAC (National Visualization and Analytics) 등에서 활발히 진행 중임

◦ 통합보안관리 기술 중 사이버공격 추적 기술 실현을 위해 전 세계적으로 연구가 초기 단계에 있으며, 현재 이와 관련하여 DETER (Cyber Defense Technology Experimental Research), EMIST (Evaluation Methods for Internet Security Technology), ARDA (Advanced Research and Development Activity)의 Network Attacks Traceback 연구가 매우 활발히 진행되고 있음

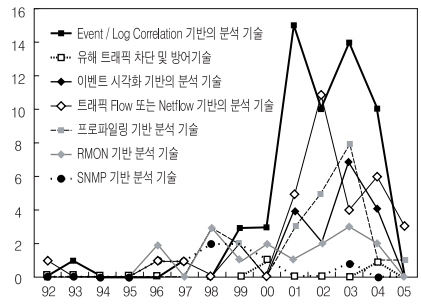
◦ NAC는 CISCO, MS사 그리고 TCG 등이 PC NAC 에이전트, 인증 및 접속 정책 장비, 정책 실행 장비 등의 기술을 개발하여 출시하고 있음

◦ 또한 보안장비의 고성능 및 기능 통합화는 성장곡선에서 성장기 말기에 접어드는 추세이지만, 장비 및 인프라의 공격상황을 직관적으로 파악하려는 요구사항은 향후 국내외적으로 강력히 출현될 것으로 기대되며, 이를 위한 연구개발이 중점적으로 진행될 것으로 예상됨

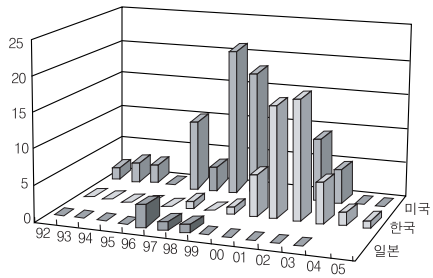
◦ 차세대 네트워크는 다양한 통신망과 서비스가 통합 운영되므로 개별망이 갖고 있던 보안의 취약성뿐만 아니라 통합에 따른 광범위한 보안 문제를 해결하는 쪽으로 연구가 이루어지고 있으며, 대표적으로 라우터간의 라우팅 정보 보안 기술이 개발되고 있음

- 주요 국가별 특허출원 동향

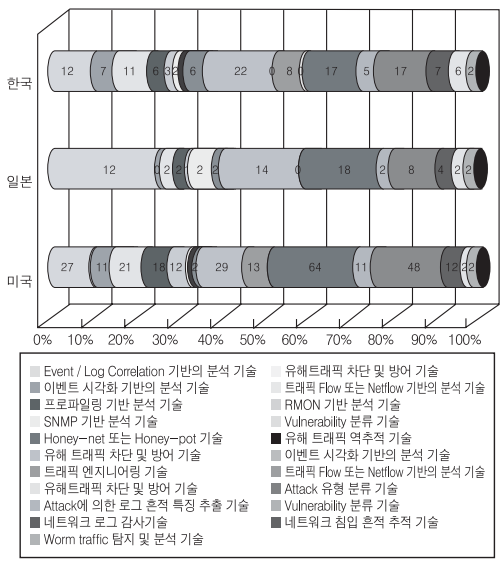
◦ 1992.1.1~2005.5.26 기간 중 한국/미국/일본을 대상으로 검색



〈기술별 등록 특허 추세〉



〈국가별 등록특허 동향〉



〈국가별 기술별 특허 현황〉

◦ 기술별 등록 특허 추세 관점에서 보안 이벤트 시각화 기반의 분석 기술은 2000년도부터 특허 출원이 시작되었으며, 특허출원 완료 예상기간이 2년 정도의 소요됨을 고려하면 2003년 기준으로 타 분야 대비 출원완료가 급증 추세에 있음

◦ 국가별 통합보안관리 기술의 등록특허 동향에 관한 그래프로 미국, 한국, 일본, 유럽 순위로 나타나고 있으며, 이는 통합보안관리 기술의 역사와 맥을 같이 하는 것으로 볼 수 있음

· 미국은 1992년부터 특허 등록이 되었으며 높은 등록을 보인 시기는 1998년에 21건의 특허가 등록된 것으로

나타남

· 한국은 다른 국가들 보다 다소 늦은 1997년에 특허 등록을 보였으며 2002년부터 가장 많은 17건의 특허 등록이 된 것으로 나타나고 있음

· 일본은 1996년~1998년에 5건의 등록을 이루어진 것을 볼 수 있음

◦ 국가별 특허 현황은 각 기술별 강점과 취약점을 갖고 있음

· 유해 트래픽 차단 및 방어 기술의 비율을 보면 미국과 일본은 출원이 없는 반면 한국에서는 출원을 한 것으로 나타나고 있음

· 한국은 네트워크 침입 흔적추적 기술도 미국과 일본보다 강점을 가지고 있지만 반면 Event / Log Correlation 기반의 분석 기술은 미국과 일본에 비하여 취약한 점을 나타내고 있음

· 미국은 전반적으로 모든 특허 출원에서 강점을 가지고 있으며 특히 이벤트 시각화 분석기술, 트래픽 Flow 또는 Netflow 기반 분석 기술, Vulnerability 분류 기술 강점을 가지고 있는 것으로 나타나고 있음

· 일본은 모든 부분에서 특허 출원(등록)이 미국과 한국에 비교하여 적게 출원(등록)한 것으로 나타나고 있으며 유해 트래픽 차단 및 방어 기술에 취약한 것으로 보여짐

· 또한 보안 이벤트 시각화 기반의 분석 기술은 2000년도부터 특허 출원이 시작되었으며, 특허출원 완료 예상기간이 2년 정도의 소요됨을 고려하면 2003년 기준으로 타 분야 대비 출원완료가 급증 추세에 있음

– 사이버보안 동향

◦ 미국은 '9.11 동시다발테러' 이후 사이버보안을 연방정부 R&D 분야에서 최우선프로그램 중 하나로 선정하고 연구개발 정책을 강화

◦ '사이버보안연구개발법' (2002년) 제정, '국가 사이버공간 방어전략' (2003년) · 「사이버보안:우선순위의 위기」 (2005년) · 「연방 사이버보안 및 정보보증 연구개발 계획」(2006년) 발표

◦ 네트워킹 장비에서는 보안 기능이 추가된 제품군들이 개발되고 있으며 엔터라시스 네트웍스에서는 방화벽 기능과 VPN 기능이 기본 제공되는 "시큐리티 라우터"를 내놓고 있으며, 네트워크 장비 개발 업체인 노텔에서는 Firewall-1 소프트웨어를 탑재해서 고속의 ASF(Altelon Switched Firewall)을 개발하였으며, 탑레이어사에서는 7계층 switch인 appswitch 제품을 전문 기능화하여 출시하고 있음

• 서버보안

– 주요국가의 정책기조

◦ 미국, 유럽, 일본

· 미국은 정부 차원에서 보안 운영체제를 개발하고 있으며, 기존의 마이크로 커널 기반으로 개발하던 정책을 최근에는 공개 운영체제인 리눅스를 기반으로 연구를 진행하고 있음

· 유럽은 미국 TCSEC과 통합된 국제공통평가표준(CC)에 맞게 PP 등을 개발하고 그에 알맞은 기술 연구가 진행중이며, 일본은 리눅스를 기반으로 한 많은 보안 운영체제 연구가 진행되고 있음

- 기술 개발 현황
  - 미국의 NSA (National Security Agency) 주도하에 정부차원으로 국가정보기반구조 구축과 국방용으로 사용하기 위하여 1995년부터 보안 운영체제를 개발 중임
  - 최근에는 Linux를 기반으로 Secure Enhanced Linux를 개발 진행 중이며, 현재 Linux Kernel의 기본 기능으로 탑재되어 있음
- 주요 국가별 특허출원 동향
  - 미국, 유럽, 일본
    - 기존의 서버용 보안 운영체제의 기능을 개선하는 차원에서 새로운 접근 제어 메커니즘, 성능 및 안정성 측면의 보안 기술에 대한 특허의 다수 확보하고 있으며, 고속이나 기능 개선 등에 대응할 수 있는 특허권을 확보함으로써 시장 선점
    - 역할 기반 접근 제어 방법, 강제적 접근제어가 적용된 보안 운영체제에서의 신뢰 채널 제공 장치 및 방법 등 보안 운영체제 관련 특허 들이 ETRI와 산업체 중심으로 미국, 일본 등의 등록 특허를 소유하고 있음

• PC보안
- 국내에서의 기술개발 현황과 비슷한 동향이라고 보면 되지만 기술주기가 약 1년에서 1.5년정도 빠르게 진행되고 있고 단기적인 대응 기술외에 장기적인 연구가 활발히 이루어지고 있으며 여러 가지 요인이 있겠지만 기술 인력의 숫자적인 차이로 인해 국내는 장기적인 측면보다는 단기적인 대응에 투입할 수밖에 없어 이의 개선이 시급한 실정임

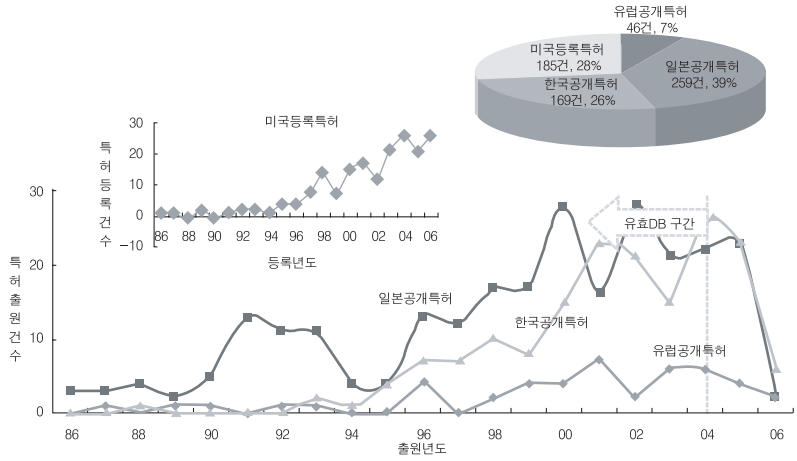
• 디지털포렌식
- 주요국가의 정책기조
  - 미국: 1990년대 초부터 이미 디지털 포렌식을 도입되어 FBI(미연방수사국)를 중심으로 사이버 범죄 수사에 널리 이용하고 있으며, 미 국방성은 사이버 범죄에 대응하여 DoD Cyber Crime Center를 운영하며 사이버 범죄 연구, 디지털 증거 획득 및 분석, 수사관 교육을 하고 있음
    - 민간 분야의 디지털 포렌식 활용으로 2006년 12월부터 발효된 개정 '미국연방민사소송법률안' ESI(Electronically Stored Information)에 대한 내용이 추가됨에 따라 기업의 입장에서 포렌식툴을 이용한 전자적 증거물인 ESI에 대한 관리 및 빠른 식별의 중요성이 증대됨 (ESI의 민사소송 개시를 보통 e-Discovery라 함)
  - 유럽: 1995년에 포렌식 관련 지식 및 포렌식 수사 경험을 공유하기 유럽의 포렌식 연구 협회인 ENFSI (European Network of Forensic Science Institutes)가 결성되어 정기적인 포렌식 세미나와 공동 연구를 추진하고 있으며, 또한 네덜란드의 NFI(Nederlands Forensic Institute)는 포렌식 관련 수사 및 연구 개발을 추진하며 포렌식 교육과 전문인력을 양성하고 있음
- 기술개발 현황 및 전망

◦ 현재 상용화되어 있는 컴퓨터 포렌식 제품은 Guidance Soft사의 EnCase, Technology Pathways 사의 ProDiscover, AccessData 사의 ForensicToolkit, ASR Data 사의 SMART 등이 있으며, 그 중 EnCase Edition이 가장 높은 시장 점유율을 차지하고 있음

◦ 휴대전화를 포함한 휴대용 전자기기에 대한 포렌식 도구로는 Paraben 사의 Cell Seizure, Oxygen Software 사의 Oxygen Phone manager, Radio Tactics 사의 ForensicSIM Toolkit 등의 상용 제품이 있으며, Guidance Software 사도 Neutrino라는 모바일포렌식 제품을 개발하고 있음

- 주요 국가별 특허출원 동향

◦ 컴퓨터 포렌식 분야는 미국이 현재 가장 많은 특허를 보유하고 있으며, 모바일 및 네트워크 포렌식 분야는 미국, 유럽, 일본 등이 비슷하게 특허를 보유하고 있지만 특허 출원 건수는 컴퓨터 포렌식 분야에 비해 아직 많지 않은 상황임



〈그림〉 디지털 포렌식 세계 특허 출원 추세

2.3. 표준화 현황 및 전망

2.3.1. 국내 표준화 현황 및 전망

- USN 보안
  - 국내 표준화 현황
    - TTA PG311 RFID/USN 프로젝트 그룹에서는 "안전한 모바일 RFID 리더를 위한 WIPI API 보안등급", "안전한 모바일 RFID 리더를 위한 접근 권한 관리 API" 등 RFID/USN 응용서비스 및 관련 정보보호 기술 표준화 추진중에 있으며, OS 및 기본 인프라 보호 표준화는 PG101 정보보호 프로젝트그룹에서 추진중임. 한편, RFID 관련 주파수 규약 등에 표준화는 산업자원부 기술표준원에서 추진중에 있음
  - 국내 표준화 전망
    - TTA PG311내 WG3113에서는 "RFID 서비스 보안 요구사항", "모바일 RFID 프라이버시 보호 프레임워크" 등에 대한 RFID/USN 정보보호 표준을 추진할 예정

- 휴대인터넷 보안
  - 국내 표준화 현황
    - 와이브로 국내 표준은 IEEE에서 추진하는 국제표준과 유사
    - 최근에 TTA IPv6 프로젝트 그룹(PG 210) 산하의 IPv6 over WiBro 실무반(PG 2103)은 휴대인터넷 프로젝트 그룹(PG302) 산하의 서비스 및 네트워크 실무반(PG 3022)의 협력 하에 와이브로 네트워크에서의 IPv6 기술 적용 표준화를 추진
  - 국내 표준화 전망
    - TTA PG302에서는 "WiBro에서 UMTS로 PS HO", "댁내 RAS 및 비즈니스 형 WiBro", "WiBro에서 UMTS로 PS Handover" 등의 표준을 추진할 예정

- 홈네트워크 보안
  - 국내 표준화 현황
    - TTA의 정보보호기반 프로젝트 그룹(PG101)과 HNSF을 중심으로 표준화가 진행
    - 2004년 홈네트워크에서의 사용자 인증메커니즘에 관한 표준안이 HNSF에 제출된 것을 시작으로 홈네트워크 보안에 관한 국내 표준화 활동이 시작
    - 홈네트워크에서의 사용자 인증 메커니즘에 관한 표준은 그 후 검토회의를 거쳐 2005년 TTA와 HNSF에서 표준으로 제정
    - 2006년에는 홈네트워크 보안 정책 기술 언어에 관한 표준안이 HNSF과 TTA PG101에 제출되었고, 2006년 12월 표준으로 제정

◦ 홈네트워크를 위한 보안기술 프레임워크에 관한 표준안이 TTA PG101에 제출되었고, 2006년 12월 표준으로 제정

- 국내 표준화 전망

◦ TTA PG101에서 "홈네트워크 등에 적용 가능한 디바이스 인증서 프로파일" 등의 정보보호 표준을 추진할 예정

• 이동통신망 보안

- 국내 표준화 현황

◦ TTA PG301에서 완료된 정보보호 관련 표준

· IMT-2000 3GPP2 - IP-기반 위치 서비스 보안성 프레임워크
· IMT-2000 3GPP2 - GBA를 이용한 보안 구조
· IMT-2000 3GPP2 - 개선된 암호화 알고리즘
· IMT-2000 3GPP2 - 공통 보안
· IMT-2000 3GPP2 - IMS 보안 프레임워크
· IMT-2000 3GPP - (U)SIM 어플리케이션 툴킷을 위한 보안 메커니즘(R99)
· IMT-2000 3GPP2 - 공통 보안 알고리즘 v1.0
· IMT-2000 3GPP2 - 브로드캐스트-멀티캐스트 서비스 보안 프레임워크

- 국내 표준화 전망

◦ "휴대전화기 키패드 접근성 지침"에 관한 표준을 추진할 예정

· 신체적인 제약으로 인해 휴대전화기 활용에 어려움을 겪는 사용자가 불편함이 없이 사용할 수 있도록 휴대전화기 키패드 인터페이스 제작 및 제공 등에 필요한 사항을 규정한 표준안

• 무선근거리통신망 보안

- 국내 표준화 현황

◦ TTA PG303에서 완료된 정보보호 관련 표준

· AP간 프로토콜에서 안전한 통신 보장을 위한 RADIUS-Diameter 연동 규약
· IAPP에서의 스테이션 보안 콘텍스트
· 무선 LAN 매체접근제어(MAC) 계층 보안기능 향상을 위한 그룹 키 갱신 및 설정
· 무선 LAN 매체접근제어(MAC) 및 물리계층(PHY) : 보안기능 향상

- 국내 표준화 전망

◦ "무선 LAN QoS 보장을 위한 MAC 기능 연구", "무선랜 망간 서비스연동 규격", "무선 LAN 메쉬네트워크 규격" 등에 관한 표준을 추진할 예정

◦ 802.11n에 대한 무선랜 관련 기술기준 작업이 진행 예정

· 2.4GHz 대역은 간섭의 영향이 많으므로, 5GHz 대역에서 무선랜을 적용하는 것에 대한 검토

• 차세대네트워크 보안

- 국내 표준화 현황

◦ 차세대네트워크보안 분야는 Broadband, Mobility, QoS, IPv6 등에 이르기까지 매우 다양한 분야에 걸쳐있으므로 국내에서의 다양한 프로젝트 그룹 및 워킹 그룹이 형성되어 표준화가 진행 하고 있으며, 각 분야의 보안 기술 및 연동 환경의 보안 기술은 개별 분야에서 표준화를 진행

· TTA PG102(인터넷보안 프로젝트그룹)에서 무선랜 침해사고 방지 지침, 인터넷 접속시 보안관리를 위한 지침, IPsec AH/ESP 표준적합성 시험규격, IPv6 IPsec IKE 표준적합성 시험표준 등을 개발 중이며, NGN Security에 관련된 표준화 활동도 포함되어 있으나 단지 구체적인 활동이 없음

· TTA PG204(NGN 프로젝트그룹)에서는 BcN 일반요구사항, 참조모델, 통합연동기술 등을 연구하고 있으며, 정보보호 분야의 활동은 미흡한 상태임

- 국내 표준화 전망

◦ TTA PG101(정보보호기반 프로젝트그룹)에서 서비스거부공격 소스추적 기술, 암호메세지 규격, 암호화 알고리즘의 사용, 홈네트워크를 위한 보안기술 프레임워크 표준 등을 추진할 예정

◦ TTA PG204(NGN 프로젝트그룹)에서는 BcN 일반요구사항, 참조모델, 통합연동기술 등에 관한 표준을 추진할 예정

• 통합보안관리

- 국내 표준화 현황

◦ 국내 통합보안관리 일반 표준은 인터넷 보안기술 포럼과 TTA에서 추진함

· 사실 표준화 단체의 표준 초안 개발과 TTA에서의 정보통신 단체표준으로 개발되거나, TTA에서의 표준초안 개발과 관련 PG를 통하여 최종 표준을 확정하는 방법으로 표준을 추진

· 참고로, 침입차단시스템, 침입탐지시스템, 가상사설망 시스템 로그 표준을 정의한 국내 인터넷보안기술 포럼(정보보호진흥원, 한국전자통신연구원, 정보보호산업체 등에서 참여)에서 표준화된 정보보호 일반 관련 표준과 TTA에서 확정된 정보보호 표준은 다음과 같음

관련분야	표준 번호	표준 내용	제정년도	개정현황
보안 관리	ISTF-004/R	침입차단시스템 로그형식 표준	2003	개정
	ISTF-005/R	침입탐지시스템 로그형식 표준	2003	개정
	ISTF-020	보안시스템의 통합관리를 위한 API 표준	2003	초안
	TTAS.IS-17799	정보보호관리 표준	제정완료	2002
	-	정보보호제품 표준적합성 시험방법	제정완료	2004.

- 국내 표준화 전망
  - 향후, 보안장비의 보안이벤트 로그 포맷 이외에도 보안관점의 네트워크 트래픽 현황에 정형화된 형식에 대한 표준화가 필요함
  - 또한 현실 망에서 활용가능한 멀티 도메인간 협업 기반의 공격 추적 수행을 위해 각 도메인간의 침해사고 데이터 형식과 이를 교환하기 위한 프로토콜에 대한 표준화가 추가적으로 요구될 것임

• 서버보안
- 국내 표준화 현황
  - TTA PG101 정보보호 프로젝트 그룹에서는 정보보호 기반기술 표준, Secure OS 표준 등 총 16건의 표준화 과제 수행
- 국내 표준화 전망
  - 삼성, LG, 소니, IBM 등의 세계 유수의 가전 및 임베디드 리눅스 업체들이 모여 결성한 CELF(Consumer Electronics Linux Forum)에서 임베디드 리눅스 솔루션 및 표준 플랫폼 제정을 위해 활동 중이며 산하 기구인 Security Working Group 을 통해 기술적인 접근을 하고 있음

• PC보안
- 국내 표준화 현황
  - 국내 정보보호 일반 표준은 인터넷 보안기술 포럼(ISTF)과 TTA에서 추진
  - PC보안과 관련되어 추진된 표준은 2000년에 제정된 "악성코드 방지 지침"이 유일하며 "침입차단/방지 시스템 로그형식" 표준이 서버에서 PC로 적용되면서 로그에 적용할 표준으로 볼 수 있음
- 국내 표준화 전망
  - PC 보안기술과 관련하여 국내에 표준화가 이루어진 것은 2000년에 악성코드 방지 지침 정도이며 관리적인 요구사항에 맞추어 각 기업별로 내부적으로 로그 형식 표준화가 되어 있지만 업체간의 표준화까지는 이루어지고 있지 않은 실정

• 디지털포렌식
- 국내 표준화 현황
  - 국내의 디지털 증거 수집 과정에서는 수사 매뉴얼, 가이드라인과 같은 지침서가 없거나 있어도 각 기관마다 별도의 지침을 담고 있으며 국가적으로 표준화된 수사기법은 정형화되지 않음
  - 디지털 증거의 법적 효력을 확보하고, 정확한 조사/분석을 위해, 증거 수집, 이송, 분석, 보고, 보관 절차를 확립하고 명문화하는 절차를 표준화 단체에 의해 규격화되어야 하나 아직 이에 관한 활동은 미미함
- 국내 표준화 현황

◦ 2007년부터 TTA를 통해 데이터 수집, 분석, 복구에 관한 검증절차 권고안 및 디지털포렌식 가이드라인에 대한 표준안을 개발하고 표준화를 추진하려 하고 있음

2.3.2. 국외 표준화 현황 및 전망

• USN 보안

- IEEE 802.15 WG: bluetooth, 휴대용 멀티미디어 단말간의 연동, WPAN 구성을 위한 표준화
- ISO/IEC JTC1/SC27: 정보 보호 표준화 그룹으로 현재 센서네트워크 관련 표준을 진행 중임.
- W3C : 센서 관련 컨텐츠의 표준화 (예, SensorML : 센서 데이터 인코딩 기술의 표준)

• 휴대인터넷 보안

- 지난 2005년 12월 국제전기전자학회(IEEE)에서 와이브로의 핵심기술이 포함된 광대역 무선 이동통신 접속규격인 802.16e가 국제 표준으로 확정된 데 이어 최근 차세대이동통신인 IMT-2000의 기술 표준으로의 채택이 급물살을 타고 있어 와이브로가 명실상부한 세계 표준으로 자리잡고 있음
- 그러나, 중국과 유럽의 일부 이동통신사업자가 모바일 와이맥스를 여섯 번째 3세대 이동통신(IMT2000) 국제 표준으로 채택하자는 우리나라의 제안에 반대하여, 지난 6월 국제전기통신연합 전파통신 연구반(ITU-R SG) 제네바회의에서 '기술 요건(스펙) 미비'를 이유로 모바일 와이맥스의 IMT2000 표준화 문제가 하위 작업반(WP8F)회의에 반려되었음
- 정보통신부는 'WP8F 모바일 와이맥스 특별회의' 결과물을 토대로 10월 제네바에서 열릴 세계전파통신회의(WRC) 2007'로 모바일 와이맥스의 IMT2000 표준 진입 여부가 확정될 예정임. IMT2000 표준 진입은 와이브로가 기존 이동통신서비스와 동등한 위치에서 경쟁할 수 있는 토대가 되고, 글로벌 로밍이 가능한 주파수 확보가 용이해질 뿐만 아니라 비동기 4G 표준화 작업에도 동등한 자격으로 참여할 수 있어 성장 동력을 확보
- 미국을 위시한 30여개국이 이미 와이브로를 채택하기로 한 것은 이미 기술적 문제가 없다는 것을 의미하는 것이므로, 국제표준화는 가능할 것으로 예상

• 홈네트워크 보안

- 홈네트워크 보안에 대한 국외 표준화는 ISO에서 2005년에 표준안이 한 건 있었고, ITU-T에서 진행중인 표준안이 3건
- ITU-T에서 진행중인 표준안들은 SG17의 Question9에서 진행중
  ◦ Question9은 X-homesec-1, X-homesec-2, Xhomesec-3의 세 부분으로 나뉘어져 있고, Xhomesec-1은 "Framework of security technologies for home network", X-homesec-2는 "Device certificate profile for the home network", X-homesec-3는 "User authentication mechanism for home network service"라는 제목 아래

표준화가 진행중

• 이동통신망 보안
- 3GPP에서는 WLAN 망과 3G 망을 연동시키는 것이 가능한지 여부에 관한 연구를 진행하였으며(TR 22.934), 이를 가능하게 하기 위한 구조 및 6단계 시나리오를 상위 수준에서 정의함. (TR 22.934, TR 23.934, TS 23.234)
- ETSI BRAN(Broadband Radio Access Network)에서는 IEEE 802.11a와 유사한 무선 기술인 HIPERLAN/2와 3G 망을 연동시키기 위한 요구사항 및 구조 명세에 관한 표준을 정의함. (TR 101 957)
- 동기식 이동통신 정보보호 표준화는 3GPP2, TIA, CDG를 중심으로 표준규격이 제정되고 있고, 비동기식은 GSM, 3GPP를 통하여 진행되고 있음
- ITU-R을 중심으로 향후 4세대 사용될 주파수 논의가 이루어지고 있고 ITU-T SG17에서는 이동통신 보안 기술 로드맵 작업이 이루어지고 있음
- 3GPP2에서는 이종망간의 로밍 및 이동성 지원을 위해 Mobile IP를 고려하고 있으나, 아직 3G-무선랜 연동 관련 표준화 작업을 추진하고 있지는 않으며, 현재까지 아키텍쳐 정의 및 시나리오 설정에 치중되어 있으므로 보안 문제를 이슈화하여 무선 네트워크의 연동을 위한 표준화를 추진함

• 무선근거리통신망 보안
- 현재 무선랜은 프로토콜의 보안 결함을 강화시키는 측면에서 IEEE와 IETF가 상호 협력아래 표준화를 진행
- EAP(Extensible Authentication Protocol)를 이용한 사용자 인증 프로토콜과 보안 키의 계층적 구성 방안은 IETF EAP WG에서, 공개키 인증서, ID/패스워드 등 다양한 사용자 인증 방법에 대해서는 IETF PPPEXT WG에서, 그리고 글로벌 로밍 가입자에 대한 권한제어, 과금, 분산 인증 프레임워크는 IETF AAA WG에서 표준화를 추진
- 프로토콜 수준에서의 보안 기술 표준화 문제가 일단락 되면, 네트워크 측면에서 유무선 통합보안 기술에 대한 표준화가 예상
- 예를 들면 무선랜 보안과 Mobile IP 보안을 연계함으로써 인증에 따른 지연시간을 최소화하는 문제나 임시주소와 임시포트를 사용하는 이동 단말기로부터 내부망 해킹 시도에 대응하기 위한 실시간 유무선 통합보안 솔루션이 중요시
- 또한, 최근 기존 무선LAN의 한계를 극복하기 위해 다양한 새로운 기술 동향 중 무선 메쉬 네트워크(Wireless Mesh Network) 기술이 등장하였으며, 현재 IEEE 802.11에서는 TGs에서 표준화를 다루고 있으며 홈네트워킹 분야의 IEEE 802.15에서는 TG5에서 무선 메쉬 네트워크 표준화를 다룸
- 무선 메쉬 네트워크는 기존의 점대 점, 점대 다점의 무선통신 방식과는 달리, 유선망의 메쉬형태의 네트워크 구조를 무선망에서도 같은 구조를 가짐으로써 망의 신뢰도 및 적은 출력을 이용한 무선망의 확장 등의 장점을 가지고하는 기술

〈표〉 표준화기구에서의 표준화 진행 이슈

	MANET(IETF)	IEEE 802.11TGs
라이팅 레이어	IP 레이어	Subnet 레이어 (MAC과 IP사이)
IEEE 802.11 구조 분류	IBSS	ESS
관련 MAC 기능	DCF, EDCF	DCF, PCF, EDCF, HCF
동기	비동기 프로토콜	동기 프로토콜

- 현재 IEEE 802.11 TGs는 2004년 5월 TGs로 승인을 받어 잠정 표준화를 위해 표준화 개발 단계에 있으며, 2004년 5월 회의에서 효율적 표준화 개발을 위해 사용 모델과 용어 정의를 우선적으로 하고 이에 대한 기술기고를 받고자 합의
- IEEE 802.15 TG5도 2004년 5월 회의에서 TG5를 위한 PAR(프로젝트 형식 요청서) 작업과 5개 기준안 작성을 위해 결성되었고, 특히 한국 삼성전자의 이명 박사가 부의장으로 선출

• 차세대네트워크 보안

- 국내 동향과 마찬가지로 국외 동향도 다양한 프로젝트 그룹 및 워킹 그룹이 형성되어 표준화가 진행 하고 있으며, 각 분야의 보안 기술 및 연동 환경의 보안 기술은 개별 분야에서 표준화를 진행
  - ITU-T SG13, SG11(NGN : Next Generation Network)에서, 보안관련 표준권고(안)을 제정하여 NGN 정보보호 요구사항과 가이드라인을 도출하였으며, 기타 이슈에 대한 표준화를 추진하고 있음
- IETF에서 IPv6 관련 워킹 그룹은 IPv6, MIP6, DHC, MANET, MAGMA, DNSop, DNSext, NEMO, v6ops 등이 있음
  - IPv6는 IPv6 프로토콜에 대한 표준화와 명세를 담당
  - MIP6는 Mobile IPv6에 대한 표준화를 담당. Mobile IPv6는 특히 WiBro 등의 무선 단말에 대한 IPv6 기반 3계층 이상의 표준 프로토콜로서 BcN 유무선 통합 환경에 중요한 역할을 수행
  - v6ops는 IPv6 네트워크를 도입하기 위한 기술 및 시나리오 가이드라인을 제시. 3GPP나 IPv4와 IPv6가 혼재되어 있는 경우에 대한 고려가 이루어짐
- 메쉬네트워크와 관련된 표준화는 broadcast/multicast를 지원하는 architecture와 protocol의 정의를 통해 IEEE 802.11 MAC의 상호 운용성 문제 해결을 목표로 하고 있으나, 메쉬네트워크 정보보호 표준화 진행은 전무함

• 통합보안관리

- 현재 통합보안관리를 위한 표준화 현황은 국제표준화기구 중심과 산업체 중심으로 활발히 진행되고 있음
  - ITU-T SG17에서는 정보통신 보안에 관한 표준을 선도하는 그룹으로 WP2 산하에 보안 관리, 바이오인식, 안전한 통신 서비스, 기술적인 스팸대응 등의 7개 보안연구과제가 구성되어 있으며, 현재 진행되고 있는 현황을 아래와 같음

연구과제	연구과제 제목	이슈
Q.5/WP2	Security architecture and freamework	- 통신보안 솔루션에 대한 보안구조는 무엇인가? - 새로운 보안 솔루션을 구축하기 위하여 보안구조에 적용할 수 있는 보안 프레임워크는 무엇인가? - 기존의 보안 솔루션을 평가하기 위한 보안 구조와 프레임워크는 무엇인가? - 사용자간 보안을 위한 구조는 무엇인가? - 모바일 환경을 위한 보안 구조는 무엇인가? - NGN 보안구조는 무엇인가?
Q.6	Cyber Security	- 사이버 공간에서의 취약 또는 위협정보를 어떻게 분배하고 공유할 것인가? - 사이버 공간에서 사건처리를 위한 운용방법은? - 중요 네트워크 인프라를 보호할 수 있는 정책은?
Q.7	Security Management	- 통신장비에서 보안위협을 어떻게 관리할 것인가? - 통신보안에서 정보보안 관리를 어떻게 구축할 것인가? - 보안평가 수행은 어떻게 처리하나? - 보안사건 발생에 대한 처리 관리는?

◦ 이기종 보안 장비간의 상호연동성을 제공을 위해 체크포인트사의 Firewall-1/VPN을 중심으로 컨텐츠 보안, 인증 및 권한 관리, 침입탐지시스템, 사건 분석 및 리포팅, 디렉토리 서버분야의 프레임워크 파트너를 구성하는 OPSEC(Open Platform for Security) 표준을 제정함

◦ IETF IDWG(Intrusion Detection Working Group)는 침입탐지시스템 구성 요소들, 대응 시스템, 관리 시스템 사이의 정보 공유를 위한 데이터 포맷과 교환 절차를 정의함

분야	표준안
IDWG	The TUNNEL Profile (RFC 3620), IETF, 2003, 초안, TTA/ISTF

◦ INCH 작업반은 컴퓨터 침해 대응에 관한 작업반으로써, 침해 대응 조직 간의 침해사고의 교환을 위하여 침해사고를 다른 조직 간에 교환되어야 할 데이터 형태에 대한 교환 수준의 요구사항, 이 요구사항을 만족하는 데이터 포맷을 기술하는 침해사고 데이터 언어, 그리고 침해사고 데이터 언어로 표현된 침해사고 보고와 연관 표현에 대한 샘플 집합을 규정하는 것을 목표로 하여 표준화 진행

분야	논의 중인 표준초안
INCH	- The Incident Object Description Exchange Format Data Model and XML Implementation - Requirements for the Format for Incident Information Exchange (FINE) 〈draft-ietf-inch-requirements-08.txt〉 - Incident Handling: Real-time Inter-network Defense - Extensions to the IODEF-Document Class for Phishing, Fraud, and Other Crimeware - draft-ietf-inch-phishingextns-03

- TCG는 컴퓨팅 환경을 보다 안전하게 만들기 위한 비영리 업계 표준화 기구로 TCG 내부에 8개의 워킹 그룹을 통해 컴퓨팅 환경 전반에 대한 표준화 작업을 진행 중에 있으며 삼성과 MS 등 시스코를 제외한 120개 글로벌 회사들이 NAC 기술을 포함한 표준화에 참여하고 있음
- 특히 TCG 그룹의 TNC(Trusted Network Connect) 개방형 표준은 NAC 기술을 위한 표준 규격을 지원하며 이를 준수하면 벤더 종속에서 탈피할 수 있으므로, 시만텍-주니퍼 등과 같은 NAC 후발 업체들이 CISCO-MS 등을 이어 시장을 잡겠다고 함

• 서버보안

- ISO/IEC 에서는 유럽의 ITSEC과 미국의 TCSEC을 통합한 국제공통평가표준인 Common Criteria Ver. 2.1을 세 개의 파트로 나누어서 표준 문서로 채택되었으며, 현재는 NIAP과 NIST를 중심으로 PP, ST 등의 표준화가 진행 중임
- TCPA(Trusted Computing Platform Alliance)는 PC 기반의 산업 플랫폼, 운영체제, 응용 등의 보안규격을 개발이 목표임. 표준규격인 TCPA 1.0 의 범위는 안전한 저장매체, 플랫폼 인증 등의 전형적인 보안 기능 블록과 BIOS의 자가 진단, 마스터 부트 레코드, OS 부트 로더 등의 플랫폼 무결성 확인 표준화 진행 중

• PC보안

- 1991년 CARO(Computer Antivirus Researchers Org.)의 멤버들이 'CARO 바이러스 명명법 관례' 라는 기준안을 제시했지만 AV업체들은 가이드라인 정도로 업체마다 부분적으로 이 규칙을 적용하여 명명하기도 하지만 절대적인 영향을 주고 있지는 못함

• 디지털포렌식

- 미국 NIST는 CFTT(Computer Forensic Tool Testing, http://www.cftt.nist.gov) 프로젝트를 운영하여 포렌식 도구 기능 검증을 국가적으로 주도하고 있음
  - 디지털 증거의 무결성 훼손없는 수집, 분석을 통한 법적 근거 있는 결과를 도출하기 위해 사용되는 디지털 포렌식 기능을 검증하고 그 결과를 공표하고 있음
  - CFTT에서는 디지털 포렌식 툴의 검증 및 평가 방안을 제시하고, 평가 결과 보고서는 미국 국가 법무연구소(NIS: National Institute of Justice)와 함께 공동으로 발간하여 일반인들도 쉽게 열람할 수 있도록 하고 있음. 컴퓨터 범죄 수사관들은 이 보고서를 참조하여 디지털 포렌식 툴의 선정 기준을 확립하며, 변호사와 검사들은 디지털 증거의 객관성을 증명하기 위한 자료로 활용하고 있음
- 미국 NIST는 NSRL(National Software Reference Library , http://www.nsrl.nist.gov) 프로젝트를 운영하여 획득된 증거 조사 분석시 효율적인 파일 검색을 위한 참조 데이터 셋(RDS: Reference Data Set)을 구축함
  - 조사/분석에 소요되는 시간을 단축시키기 위해서는 준비된 참조 데이터 셋을 사용하여 잘 알려진 파일은 검색대상에서 제외하고 검색범위를 축소해서 조사 우선순위를 부여하는 것이 중요함
  - 미국에서는 이러한 Hashed Search 기술을 활성화하고 일반 수사관들도 쉽게 사용할 수 있게 하기 위해서, 잘 알려진 파일들의 표준 해쉬셋을 NIST에서 제작하여 무상으로 배포하는 NSRL 프로젝트를 실시하고 있음
- NIST Information Technology Laboratory(ITL)에서는 Special Publication 800-series를 통해 컴퓨터 포렌식 및 모바일 포렌식에 대한 가이드라인을 발표하는 등 포렌식 분야의 표준화를 진행중임
  - "Guidelines on PDA Forensics", Special Publication 800-72
  - "Guide to Integrating Forensic Techniques into Incident Response", Special Publication 800-86
  - "Guidelines on Cell Phone Forensics", DRAFT, Special Publication 800-101

2.4. 표준화 대상항목별 현황 분석표

구분		네트워크 보안			
표준화대상항목		USN 보안기술	휴대인터넷 보안기술	홈네트워크 보안기술	이동통신망 보안기술
시장 현황 및 전망	국내	- 600억원 (보안시장열려 있음)	- 현재 상용서비스 초기단계에 있지만, 서비스 지역 및 품질 개선으로 향후 서비스가 활성화 될 것으로 예상됨	- 연평균 32.2%씩 급성장하여, 2010년에는 234억 5,000만 달러에 이를 것으로 전망	- 2007년 5월 휴대폰 수출은 전년동월 대비 1.8% 감소한 16억 4,200만 달러, 5월 누적으로는 전년동기 대비 5.4% 증가한 85억 8,740만 달러 기록
	국외	- 120억$(보안시장열려 있음)	- 세계30여개국에서 와이브로 서비스 도입을 준비하고 있어 향후 서비스가 활성화 될 것으로 예상됨	- 2010년에는 1,620억 달러에 이를 것으로 전망되고, 특히 홈서버와 홈게이트웨이는 연평균 47.2%의 급성장이 기대	- 2007년 5월 누적 기준 미국은 최대 휴대폰 수출국으로 프리미엄 제품의 호조로 인해 전년동기 대비 23.7% 증가한 18억 9,124만 달러를 기록
기술 개발 현황 및 전망	국내	- 키관리 및 인증기술 확보	- IMS기반 기술개발등을 통해 WCDMA와의 영상통화 및 다양한 부가서비스 개발되고 있음	- Bluetooth 기술, UWB 기술, Zigbee 기술, Home RF 기술, IEEE1394, Home PNA, PLC 등 개발	- 모바일 인터넷과 무선랜의 연동을 위한 다양한 시도가 이루어지고 있음
	국외	- 주파수 및 기본 스펙에 중점	- 미국, 유럽, 일본등에서 서비스 도입을 위해 활발한 와이브로 기술개발이 이루어지고 있음	- 홈게이트웨이 플랫폼을 통한 정보보호 및 보안성 확보에 기술개발을 진행중	- 동종 무선망간 핸드오프 또는 보안구조가 서로 상이한 이종망간 핸드오프시 지연시간을 최소화시키는 핸드오프 보안기술이 미국을 중심으로 활발하게 연구 중임
기술 개발 수준	국내	- 설계	- 시제품/프로토타입	- 시제품/프로토타입	- 시제품/프로토타입
	국외	- 시제품/프로토타입	- 시제품/프로토타입	- 시제품/프로토타입	- 시제품/프로토타입
	기술격차	- 별로 없음	- 세계최고수준	별로없음	- 별로없음
	관련제품	- 한백전자 Ubicoin, ZigBeX, 하이버스 Hmote등	- 기지국, 제어국 시스템 - 안테나, 와이브로 모듈	- 홈게이트웨이, 홈서버	- 기지국, 제어국 시스템
IPR 보유현황	국내	- 20여건			
	국외	- 500 여건 예상 (주로 H/W)			
IPR확보 가능분야		- USN 키관리 및 인증기술 (S/W)			
IPR확보 가능성		- 매우 높음(S/W)			
표준화 현황 및 전망		- 현재 미흡하나 활성화 가능성이 매우 높음	- IEEE802.16 국제표준으로 승인되었으며, IMT2000 표준진입을 위한 작업을 진행하고 있음	- ITU-T SG17의 Question9에서 표준안 진행	- 국내는 UICC 기반 SIM 인증 보안 기술 표준화를 TTA를 중심으로 이루어지고 있으며 국외는 핵심 기술의 표준화를 GSM과 CDMA 표준화 기구를 통하여 진행하며 ETSI와 3GPP/3GPP2가 중심임
표준화 기구/ 단체	국내	- TTA, 기술표준원	- TTA PG302	- TTA, HNSF	- TTA
	국외	- IEEE, ISO	- IEEE 802.16	- ITU-T	- 3GPP, 3GPP2
	국내참여 업체 및 기관현황	- 한국전자통신연구원, - 한국정보보호연구원, - 한국정보사회진흥원	- 삼성전자, 포스데이타, ETRI등	- 한국전자통신연구원	- 한국전자통신연구원
	국내기여도	- 적극 활동 시작	- 크게 기여하고 있음	- 적극 활동	- 적극 활동
표준화 수준	국내	- 표준기획	- 표준화 항목승인	- 표준안 개발/검토	- 표준안 개발/검토
	국외	- 표준화 항목승인	- 표준화 항목승인	- 표준안 개발/검토	- 표준안 개발/검토
국내표준화의 인프라수준 (시장요구정도 및 참여도)		- 기술 개발에 중점을 두어 표준화에 다소 미흡한 현실이나 시장의 확대를 위해서는 보안기술의 표준이 절실히 요구되므로 표준화 인프라 구축이 절실함.	- 현재 일부지역만 와이브로 서비스를 위한 인프라를 제공하고 있음	- 국내 선도 가능성이 높음	- 보안 기술에 대한 요구가 많음

구분		네트워크 보안		
표준화항목		무선근거리통신망 보안기술	차세대네트워크 보안기술	통합보안관리
시장 현황 및 전망	국내	- 2007년까지 평균 22.4%의 성장을 달성	차세대 네트워크는 속도의 향상으로 인하여 고속 동작이 가능한 네트워크 보안 장치에 대한 수요가 급증할 것으로 예측됨	보안컨설팅분야의 약진 및 정책적 보안관리 인식 강화 등에 힘입어 향후에도 꾸준히 팽창할 것으로 기대되는 분야임
	국외	- 2006년 4/4분기 대만 WLAN 업계의 WLAN 네트워크 인터페이스 카드(NIC) 출하량이 전년 동기 대비 16.4% 증가한 4천 62만 개에 달할 전망	네트워크 장비 업체(CISCO, NOKIA 등)를 중심으로 UTM (Unified Threat Management) 어플라이언스, ITSoC 및 보안모듈 형태로 네트워크 장비에 통합하는 추세임	ESM, TMS, RMS 등 처럼 다양한 형태로 개발되고 있음. 그러나 각각이 뚜렷한 차별성을 갖지 못하고 단지 ESM을 고객의 요구에 맞게 일부 수정한 것에 불과함
기술 개발 현황 및 전망	국내	- 고속화 고용량화 등의 높은 욕구에 발맞추어 WiMAX등의 기술이 선을 보이고 있지만, 그 보안 상태는 아직 미지수로 남아있는 실정	BcN 보안 제품은 BcN 프레임워크에 대한 표준화가 완료된 시점에서 개발될 예정임	현재 보안프로토콜의 표준화를 통해 타사 제품을 포함한 이기종 보안 시스템가의 연동 기술로 발전하고 있으며, 향후네트워크 전체를 보안 관리 영역으로 확장될 것으로 예상
	국외	- 북미 지역의 많은 신생 네트워크 장비 업체들이 무선랜 스위치 시장에 도전장을 내밀고 VPN 기능을 기본적으로 갖추고 있으며 무선랜 관련 기능을 한층 강화시킨 새로운 개념의 장비들을 출시하고 있는 상황	라우터간의 라우팅 정보 보안 기술 등과 같이 통합에 따른 광범위한 보안 문제를 해결하는 쪽으로 연구가 이루어지고 있음	장비 및 인프라의 공격상황을 직관적인 파악과 추적기술을 포함하려는 요구사항은 향후 국내외적으로 강력히 출현될 것으로 예상됨
기술 개발 수준	국내	- 구현	설계	시제품/프로토타입
	국외	- 구현	설계	시제품/프로토타입
	기술격차	- 별로없음	1.9	1.1
	관련제품	- AP, Wireless LAN Card	고속 침입방지시스템	통합보안관리, 시각화 기반의 이상징후 분석
IPR 보유현황	국내		해당사항 없음	보안이벤트 시각화 및 보안이벤트 간의 상호연관성 분석 관련 다수 특허 확보
	국외		라우터간의 라우팅 정보 보안 기술 관련 특허 확보	침해사고 추적 관련 다수 특허 확보
IPR확보 가능분야			이종망 간의 연동 보안 기술, 차세대네트워크 침해사고 대응	침해사고 공유, 보안이벤트 상호연관성 분석, 보안이벤트 시각화
IPR확보 가능성			높음	높음
표준화 현황 및 전망		- 무선랜과 와이맥스는 서비스 영역이 다르기 때문에 공존하는 형태로 발전할 것으로 보이나 무선랜이 와이맥스의 많은 영역을 커버할 수 있을 것으로 예상	BcN 일반요구사항, 참조모델, 통합연동기술 등을 연구하고 있으며, 정보보호 분야의 활동은 미흡한 상태임	멀티 도메인간 침해사고 데이터 형식과 이를 교환하기 위한 프로토콜에 대한 표준화가 추가적으로 요구될 것임
표준화 기구/ 단체	국내	- TTA	TTA	ISTF, TTA
	국외	- IEEE	ITU-T, IETF	ITU-T, IETF
	국내참여 업체 및 기관현황	- 한국전자통신연구원	ETRI, KISA	ETRI, 이글루시큐리티, KISA
	국내기여도	- 적극 활동	높음	높음
표준화 수준	국내	표준안개발/검토	표준안개발/검토	표준화 항목승인
	국외	표준안개발/검토	표준안개발/검토	표준안개발/검토
국내표준화의 인프리수준 (시장요구정도 및 참여도)		- 보안 기술에 대한 요구가 많음	높음	매우 높음

구분		시스템 보안		
표준화항목		서버보안	PC보안	디지털포렌식
시장 현황 및 전망	국내	새로운 기술보다는 기존 기술을 개량하여 접근 제어 메카니즘의 제한을 극복하는 등을 고려하는 서버 보안 솔루션이나 키 관리와 S/W 무결성 확인을 위한 트러스트 플랫폼용 트러스트 운영체제에 대한 요구가 증가할 것으로 예상됨	- Anti-Virus 기능에서 개인방화벽, 개인정보보호 기능까지 통합 솔루션 공급 일반화되고 있으며 매년 약 12%의 상승세 지속 - 법안 계류중인 "개인정보보호법"이 통과되면 매체제어 관리기술이 본격적인 시장의 확산이 예상됨.	- 국내 사건 대응 서비스 시장은 2010년 2,644억원으로 증가할 것으로 추정 (IDC 전 세계 시장 예측 규모 중 5%)
	국외	NSA에서는 Secure Enhanced Linux를 개발하였고, 현재 Linux 커널에 보안 기본 기능이 탑재된 운영체제가 시장을 주도할 것으로 전망	- Anti-Virus분야는 2007년도에 36억달러 시장 예상	- 전 세계 사건 대응 서비스 시장은 2005년 $22억에서 연평균 19.2%씩 증가하여 2010년에는 $53억에 이를 것으로 추정(IDC, 2006)
기술 개발 현황 및 전망	국내	ETRI에서 "임베디드 보안 운영체제 기술 개발"과 분산 클러스터 시스템에서 플랫폼의 무결성 제공을 위한 "분산 클러스터 보안 미들웨어 기술 개발" 과제를 수행중임	- Anti-Virus(Anti-Spyware), 개인방화벽/침임탐지, 매체제어, 패치관리, 유해정보차단, 데이터복구등이 통합되는 추세임. - 행위기반등 새로운 진단법 연구	- 국내의 포렌식 기술 개발은 2007년부터 국가 출연연을 중심으로 국산 파일에 특화된 기능을 내장한 통합 포렌식 도구 개발을 시작하였음
	국외	최근에는 Linux를 기반으로 Secure Enhanced Linux를 개발 진행 중	- 시그니쳐 기반 진단법 개선중(양적팽창 및 리소스, 퍼포먼스등 고려) - 행위기반 및 알려지지 않은 악성코드 기술 연구	- 디지털 포렌식 산업의 잠재력에 대한 인식제고로 국가기관에서의 범죄수사 분야를 넘어 활용분야가 민간으로 확대되고 있으며 각국의 기술개발 경쟁이 고조되는 상황임 - 현재 디지털 포렌식 도구를 상용화한 국가 중 가장 큰 기술력 및 시장규모를 가진 국가는 미국이며, 영국, 프랑스, 일본, 러시아 등도 분야별로 디지털 포렌식 기술을 독자 개발 중에 있음
기술 개발 수준	국내	시제품/프로토타입	시제품/프로토타입	기술기획
	국외	시제품/프로토타입	시제품/프로토타입	기술기획
	기술격차	1년	1 - 1.5년	미국-3년
	관련제품	접근제어 S/W, 키관리 및 S/W 무결성 검증	- Anti-Virus(Anti-Spyware), PC방화벽, 매체제어, 패치관리, 유해정보차단, 데이터복구	- 컴퓨터 포렌식 도구, 모바일 포렌식 도구, 네트워 포렌식 관련 제품
IPR 보유현황	국내	DAC〈 MAC, RBAC 등 접근제어 기술, 신뢰 채널 등 보안 서버 기술 등 다수 확보		- 데이터 복구 분야
	국외	고속 및 기능개선 등에 대응할 수 있는 특허권을 확보함으로써 시장 선점		- 디스크 이미징 및 데이터 분석
IPR확보 가능분야		개선된 접근제어, 키관리 및 S/W 무결성 검증 등	- 악성코드 탐지 기술	- 고속 검색 및 모바일 포렌식 분야
IPR확보 가능성		보통	부분 선도	보통
표준화 현황 및 전망		- 국내 : TTA에서 리눅스 보안 표준 규격 개발 - 국외 : TCPA는 PC 기반의 산업 플랫폼, 운영체제, 응용 등의 보안규격을 개발	- 악성코드 명명법, PC보안 로그 형식 표준, 패치관리	- 미국 NIST는 Special Publication 800-series를 통해 컴퓨터 포렌식 및 모바일 포렌식에 대한 가이드라인을 발표하는 등 포렌식 분야의 표준화를 진행중이며, CFTT 프로젝트를 운영하여 포렌식 도구 기능 검증을 국가적으로 주도하고 있음
표준화 기구/단체	국내	TTA	TTA	TTA
	국외	ITU-T, ISO, TCPA 등	ITU-T, IETF	IETF, ITU-T, NIST
	국내참여 업체 및 기관현황	ETRI, Secuve 등	KISA, ETRI	ETRI, KISA, TTA
	국내기여도	높음		
표준화 수준	국내	표준안 항목승인	표준화 항목승인	표준기획
	국외	표준제/개정	표준안 개발/검토	표준기획
국내표준화의 인프라수준 (시장요구정도 및 참여도)		높음	보통	보통

3. 중점 표준화항목의 표준화 추진전략

3.1. 중점기술의 표준화 환경분석

3.1.1. 표준화 추진상의 문제점 및 현안사항

- USN의 경우 단순히 센서를 통한 소량의 정보 수집 및 이를 전달하는 것이므로 H/W 의 용량이 (CPU, Memory, Power)이 매우 제한적임. 따라서 기존에 개발된 보안 인프라(공개키 기반의 인증 및 암호, IDS, NMS, IPSec) 적용이 불가능할 것으로 판단됨. 따라서 현재 랜덤빌 기반의 키관리 기술이 대세를 이루고 있지만 아직 표준화에는 초기 단계임. 또한 센서가 사람에게 부착되어 있는 경우 개인정보(privacy) 보호를 어떻게 다룰 것인 가에 대한 법적 해결책이 선행되어져야 함
- 와이브로의 경우 USIM 카드를 사용하여 인증 및 접근제어를 하고 있고 상용화 초기단계이므로 문제점이 없었으나, 서비스가 활성화 될 경우 보안취약성이 발생할 우려가 있으므로, 안전성 확보를 위한 보안대책 마련이 요구되며, 와이브로에 대한 국제 표준화는 국내전문가들이 주도적으로 진행하고 있지만, 보안 측면에서는 표준에 대한 전문가가 부족한 실정이므로 적극적인 지원이나 투자가 필요한 실정임
- 차세대 네트워크의 경우, 독자적인 국제표준화기구에 따른 표준화 업무 부담 증가

  - 차세대 네트워크 기술 분야가 다양화 · 복합화됨에 따라 일관되고 안정적으로 적용할 수 있는 국가적 표준기술 개발이 필요한 반면에, 산업계 차원에서의 표준 전문가가 절대적으로 부족하고, 개선을 위한 적극적 지원이나 인력 양성을 위한 투자가 기업체에서는 미미한 실정이므로 정부차원의 지원 노력이 필요함
- 통합보안 관리 기술의 경우, 각 업체별로 자사 제품 시장을 위해 현실적인 보안제어 표준 규격 적용이 미비하며, 이에 따라 일관성있는 네트워크 접근제어를 위해서는 정책 분배 서버 및 프록시의 상호호환성 적용이 요구되며, 향후 도래할 다중 관리 도메인 환경에서의 공격자 추적 기술과 표준화에 대한 필요성이 대두될 것이며 이에 대한 적극적인 투자가 필요한 실정임
- 서버 보안 기술의 경우 국내 관련 산업의 인프라가 비교적 양호한 기술 분야이나, 기술에 대한 관심과 업체 표준화 노력이 부족하므로 정부차원의 지원이 필요하며, 개방형 표준을 수용한 구현 기술에 대한 국내 고유 표준 개발을 추진한 후에 이를 바탕으로 국제 표준을 추진할 필요가 있음
- PC보안의 경우, 업체간 경쟁 심화 및 정보 공유 필요성 없음

  - 악성코드 명명법의 표준화 필요성은 높았으나 현실적으로 각 업체마다 표준화를 적용할 여건이 안되며 시간적으로 같은 이름으로 발표할 수 없음. 각 업체별로 고유한 명명법의 차이로 인해 공통표준안은 가이드라인 수준으로 운영되고 있음
- 디지털포렌식의 경우, 미국은 NIST에서 디지털 포렌식 관련 프로젝트 및 가이드라인 등의 표준을 제정하고 있으며, 최근 ITU-T SG 17, ISO/IEC JTC1 SC27 WG4 등의 국제표준화 기구에서도 포렌식 조사 등의 내용으로 표준화 추진 초기 단계에 있음
- 디지털 포렌식 분야에서 범죄 수사와 관련된 부분은 각 국의 사법 환경을 반영한 가이드라인 및 증거 수집 절차 등의

제정이 우선적으로 이루어져야 하므로, 관련 분야에 대한 국내 표준화를 우선적으로 추진하고 관련된 국제 표준을 주도적으로 선도할 필요가 있음

- 무선랜 근거리 통신망 보안의 경우 국제적으로 기존 802.11의 보안 결함을 보완하기 위한 여러 가지 그룹들이 존재하고, 그 논의가 활발히 진행되고 있음. 비록 국내 기술과 산업이 표준을 선도하고 있지는 않지만 앞으로 무선랜 근거리 통신망이 더욱 더 활발히 보급되어 보안 취약성이 대두 될 것으로 전망됨. 이에 따라 국제적으로 논의되고 있는 보안 표준 제정에 발맞추어 국내 기술이 이 분야에서 뒤처지지 않도록 해야 함.

3.1.2. SWOT 분석 및 표준화 추진방향

- 네트워크 보안

<table>
<tr><th colspan="3" rowspan="2">국내역량요인
국외환경요인</th><th colspan="2">강 점 요 인 (S)</th><th colspan="2">약 점 요 인 (W)</th></tr>
<tr><td>시장</td><td>- 전체적 시장의 확대로 보안 시장의 증가
- 세계 최초로 상용서비스를 시작하여 서비스 시장에 앞장서 있음</td><td>시장</td><td>- 보안 시장에 대한 상대적 투자 미흡 가능
- 국외 산업과 유사하게 유선 인터넷 보호를 위한 특정 기술 분야에 집중되어 있음에도 불구하고, 외산 장비가 시장 주도권을 쥐고 있는 상태</td></tr>
<tr><td></td><td></td><td>기술</td><td>- IT839의 인프라 기술로 R&D 활성화
- 소프트 인프라웨어가 u-IT839에 포함되면서 u-IT 서비스의 연동 및 융복합화가 가속화 될 것으로 예상</td><td>기술</td><td>- 국외 기술의 모방
- 보안 장비 분야는 국외와 유사하게 고성능 산업적 토대는 미약한 상태</td></tr>
<tr><td></td><td></td><td>표준</td><td>- 시작단계 이고 발굴 대상 항목이 많음
- 국내표준이 국제표준과 유사하며, 국내 전문가가 국제표준을 주도하고 있음</td><td>표준</td><td>- 보안 역량 인프라에 대한 투자 미흡
- 네트워크보안 관련 표준을 IETF 및 ITU-T에서 진행하고 있으나 IPR 미비로 미진함</td></tr>
<tr><td rowspan="3">기회요인 (O)</td><td>시장</td><td>- 미국, 유럽 및 일본이 기반기술의 확보에 주력하므로 보안 기술 시장에 대한 기회
- 정보보호 유선 기반 네트워크 보안산업 연 13.6% 성장</td><td colspan="2" rowspan="3">- 많은 USN 활용 분야에 시장의 확보가 우선 필요
- 표준화 역량 강화에 인력 육성
- 세계 최초로 상용서비스를 시작하여 와이브로 도입을 준비하는 타 국가에 비해 앞서가고 있음
- 이동통신과 달리 국내에서 다수의 특허를 보유하고 있어 로열티 등을 지급하지 않아도 됨
- 국내 표준전문가가 국제 표준을 주도하고 있음
- 유무선 통합망 환경에 적용할 수 있는 IT 서비스를 위한 정보보호 기술 개발
- 보안 가용도 극대화를 위한 공통 보안관리 프레임워크 표준화 추진
- 각각의 네트워크/서비스 유형에 의존적인 공격 특징 인자들을 대체할 수 있는 적응형 공격 탐지 기술 개발</td><td colspan="2" rowspan="3">- 보안 시장 발굴
- 보안 인프라 역량 강화
- 상용서비스를 시작하고 있으나, WCDMA 등 유사서비스와의 경쟁으로 여전히 서비스 활성화 초기단계에 있으므로,
- 국내 와이브로 서비스를 활성화를 통해 성공적인 모델을 제시
- 국제 표준전문가 양성
- ITU-T와 IETF에서 표준화를 수행하고 있으므로, 이 표준화기구의 표준화 동향을 근거로 관련 제품과 서비스 개발</td></tr>
<tr><td>기술</td><td>- 보안 기술의 격차는 거의 없으므로 선점시 기술의 표준 가능성 증대
- 네트워크 장비에 보안기능을 탑재하여 고성능화</td></tr>
<tr><td>표준</td><td>- 보안 표준화 항목 발굴이 현재 미흡하므로 적극적인 참여 및 투자로 항목 발굴에 유리
- 네트워크 보안 영역에서의 기술 표준화 진행 가속화</td></tr>
<tr><td colspan="3">SO전략 : 공격적 전략(강점시장-기회활용)</td><td colspan="2">SO WO 전략 ST WT
WO전략 : 만회전략(약점극복-기회활용)</td><td colspan="2">ST전략 : 다각화 전략(강점시장-위협회피)
WT전략 : 방어적 전략(약점최소화-위협회피)</td></tr>
<tr><td rowspan="3">위협요인 (T)</td><td>시장</td><td>- 국내 기반기술의 약화로 인한 수익성 저하(Royalty)
- 유 · 무선 통합용 네트워크 인프라 방어용 보안시장 미비</td><td colspan="2" rowspan="3">- R&D에 많은 투자를 통한 기반 기술확보
- 시장 발굴에 따른 보안 시장의 육성
- IMT2000 표준진입이 성공할 경우, 이동통신과 동일한 위치에서 경쟁할 수 있어 와이브로 서비스는 활성화 될 수 있을 것으로 예상
- 고정형 와이맥스 기술보다 와이브로 기술인 이동형 와이맥스 기술의 시장규모가 더 클 것으로 예상
- 서비스장애 발생시에 보안 가용자원 활용 가능 기술 개발
- 융 · 복합 Shared Information 표준 인터페이스 구축 및 프로세스 자동화
- 실감형 보안이벤트 시각화 기술 개발 및 유 · 무선 통합망 환경의 공격(자) 역추적 기술 개발
- 유비쿼터스 환경에 적용할 수 있는 보안관제 프로토콜 개발</td><td colspan="2" rowspan="3">- 센서기술의 부가 서비스에 비중을 늘림
- 국내 표준으로 USN 활용
- 와이브로 서비스가 활성화 될 경우, 보안 취약성이 발생할 수 있음
- 발생 가능한 보안취약성을 사전에 대응하여 서비스 활성화에 걸림돌이 되지 않도록 진행
- All-IP기반 차세대 네트워크 QoS 및 무결성 보장 보안 서비스를 위한 공통 가이드라인 규정
- NGN 보안관리 프레임워크 및 보안성 고도화를 위한 프레임워크 적용
- 알려지지 않은 공격에 대한 자동 대응을 위한 핵심기술 개발
- 알려지지 않은 공격에 대한 자동 대응과 보다 능동적인 대응을 위한 핵심 기술 개발
- 유 · 무선 환경에서의 공격 특성인자를 추출하여 사전에 방지하여 침해사고 역기능 발생을 최소화</td></tr>
<tr><td>기술</td><td>- 보안 기술 개발 회사의 투자 미흡
- 보안 이벤트의 대용량화에 따른 직관적인 인터페이스 미흡</td></tr>
<tr><td>표준</td><td>- 표준 역량 인프라 투자 미흡시 표준 기술 외국이 점령 가능
- 타 사업자와의 관리정보 연동 부재에 따른 보안연동성 부재</td></tr>
</table>

- 현황분석을 통한 우선순위

◦ 많은 활용분야에 시장의 확보가 우선 필요

◦ 표준화 역량 강화에 인력 육성

◦ R&D에 많은 투자를 통한 기반기술 확보

◦ 시장 발굴에 따른 보안 시장의 육성

◦ 국내기술로 개발된 와이브로는 우리나라가 국제표준을 선도하고 있어 보안 분야에서도 국제표준 선도가능

◦ 시스템 및 네트워크 등의 다양한 리소스에 대한 위험관리, 시험 및 평가, 통합 보안 관리를 포함하는 보안관리 기술 항목 및 개별적으로 운용되는 이기종의 보안시스템(방화벽, IPS, VPN 등)을 원격에서 통합 관리하여 조직의 보안 효율성을 극대화 시키는 보안관리 기반 기술 항목

◦ 실감형 보안이벤트 시각화 기술 및 유 · 무선 통합망 환경의 공격(자) 역추적 기술 및 차세대 네트워크 보안의 표준화 항목

- 표준화 추진방향

◦ 정부는 USN 보안 문제를 해결하기 위한 기술 로드맵 및 항목별 연구반을 만들고 2008년까지 장기적인 표준화 로드맵의 개발이 필요함

◦ 시장 규모가 급속히 확대될 것으로 예측되므로 ISO SC27에 적극 참여할 수 있는 인력 선정과 현실적인 지원을 요청.

◦ TTA 의 RFID/USN 프로젝트 그룹에 보안 WG 혹은 분리된 프로젝트 그룹을 만들어 운영하며 R&D와 표준화가 연동되어 활동 하도록 R&D Fund 조성을 유도.

◦ 와이브로 서비스가 활성화되면 기존 무선랜 환경에서 발생했던 단말/기지국에 대한 서비스거부공격, 세션하이재킹, 인증우회 등 와이브로에서 발생 가능한 보안 취약성에 대한 대비가 필요하며,

◦ 와이브로 기술을 IMT2000 표준기술로 진입시켜 기존 이동통신서비스와 동등한 위치를 확보한 후, 와이브로 서비스에서의 보안기술에 대한 국제 표준활동 강화

◦ 차세대 네트워크 보안솔루션의 다양한 요구사항을 충족할 수 있는 고성능 네트워크 위협대응 기술과 인터넷 및 BcN 망 입구에서의 위협방어 보안 기술에 대한 표준화 추진 필요

◦ 현재 일관성 있는 침해사고 방지를 위한 네트워크 보안제어 정책프레임워크 표준이 진행되고 있으며, 향후에는 일관성 있는 네트워크 접근제어 정책 서버 및 프록시 프레임워크와 네트워크 노드 인증에 대한 표준으로 확장될 것으로 예상됨에 따라 국내 제품의 수출 및 국내 시장 보호를 위해 국제 또는 외국의 표준을 면밀히 분석하여 추진

• 시스템보안

국외환경요인 / 국내역량요인			강점 요인 (S)	약점 요인 (W)
		시장	- 개인정보보호법 제정에 따른 시장 활성화 예상 - 연 계약에 의한 지속적인 시장창출 - 국내 원천 기술 보유	시장 - 경기 침체에 따른 기업 투자비용 감소 - 우리보다 기술개발이 앞선 외산 장비가 시장 주도권을 가지고 있는 상태
		기술	- 보안 운영체제에 대한 연구개발 성과에 대한 기대 - 통합화 추세에 각 요소기술 보유 - ETRI를 중심으로 학계 및 산업계가 협력하여 핵심 기술 개발	기술 - IT 환경 변화에 따른 다양한 기술 요구 사항을 만족시키기 위한 투자 및 연구가 부족 - 단기 기술 대응 수준
		표준	- 시작단계이고 절차 및 기술적 관점에서 표준화 진행	표준 - 국내 표준화는 시작 단계이며, ITU-T 등에서의 국제 표준화를 위한 IPR확보가 아직 미비함 - 산업체의 인식 부족
기회요인 (O)	시장	- 개인정보보호법 제정에 따른 수요 확대 - 개인인터넷환경의 지속적인 발전 - 전세계 사건대응 시장의 급속한 증가에 따른 포렌식 신규시장에 대한 기회	- ITU-T SG17 정보보호 표준화 경험 활용을 통한 보안미들웨어 및 트러스트 운영체제 기술의 국제 표준 선점 - PC보안 로그 형식 표준화 추진 - PC 보안 제품의 공통 API 표준화 추진 - 다양한 전자 매체에 대한 디지털 증거 수집, 분석 절차 및 기술에 대한 표준개발 - 표준화 역량 강화에 위한 인력 육성	- 중장기적인 전략으로 국제 표준화 활동을 통한 해외 의존도 트러스트 플랫폼 모듈 기반의 트러스트 서버용 보안 운영체제 기술 확보 - 산업체 공동으로 추진할 수 있는 과제 발굴 및 추진 - 우선적인 국내 표준화 추진 및 ITU-T, ISO/IEC JTC1 등의 표준화 단체를 통한 적극적인 표준화 추진
	기술	- 트러스트 플랫폼에 대한 연구개발 확대 - 악성코드 대응 기술인력 증가로 장기 대응 기술 연구 가능 - 다양한 전자매체에 대한 디지털 증거 확보 및 분석 기술의 요구 증대		
	표준	- 연구개발 확대로 인한 기술 확보 - 침입탐지/방지 로그 형식 표준 참조 가능 - 보안 표준화 항목 발굴이 현재 미흡하므로 적극적인 참여 및 투자로 항목 발굴에 유리	SO전략 : 공격적 전략(강점사용-기회활용) / WO전략 : 만회전략(약점극복-기회활용)	
위협요인 (T)	시장	- 연구개발 초기단계로 인한 상용제품의 경쟁력 낮음 - 기업 보안 관리 제품들이 민사소송의 e-Discovery 분야의 경쟁 기술이 될 수 있음	ST전략 : 다각화 전략(강점사용-위협회피) / WT전략 : 방어적 전략(약점최소화-위협회피)	
	기술	- 국제 경쟁력 심화 - 장기 대응 기술 미비 - 새로운 형태의 공격 등장 - 투자 미흡으로 원천기술에 대한 IPR 확보 미흡	- ISO/IEC 등 선도 표준 기구의 진입을 위한 국제 표준 전문가 그룹과의 연대를 통한 국제 표준의 협력 및 서버 보안 기술의 경쟁력 확보 - 이종 제품 간의 통합 제품 개발을 지원하는 공통 API 표준화 추진 - 새로운 포렌식 분야에 대한 R&D 투자를 통한 기반 기술확보	- 산학연 표준 협력 체계 구축으로 국제 표준화 활동의 지속적인 참여를 통한 기존 표준과의 호환성 유지 및 표준 전문 인력 양성 - 이종 제품 간의 통합 제품 개발을 지원하는 공통 API 표준화 추진 - 적극적인 투자 및 기술 개발을 통해 IT 환경 변화에 따른 디지털 포렌식 핵심 기술 개발
	표준	- 글로벌 표준에 적극적 참여를 못하고 정보 공유 수준 - 표준 역량 인프라 투자 미흡시 표준 기술 외국이 점령 가능		

SO WO
전략
ST WT

– 현황분석을 통한 우선순위

◦ 기술성숙도와 시장잠재력이 우수한 서버 보안 기술은 국내 관련 산업의 인프라가 비교적 양호한 기술 분야로 국내 산업의 강점을 최대한 활용하여 국제 표준 협력/경쟁을 할 필요가 있으나, 보안 서버 인증서 등과 같은 일부 인프라 측면에서의 기술은 국제 표준 선도 가능

◦ 기술 의존도가 높고 원천기술 확보가 취약한 트러스트 플랫폼 모듈 기반의 트러스트 서버용 보안 운영체제 분야는 TCPA 등과 같은 국제 표준을 수용하여 국내 관련 산업의 기술 기반 마련

◦ 다양한 전자 매체의 디지털 증거 수집 가이드라인, 디지털 증거 수집 및 분석 규격, 이미징 규격 등이 우선적인 디지털 포렌식 분야의 표준화 항목

- 표준화 추진방향

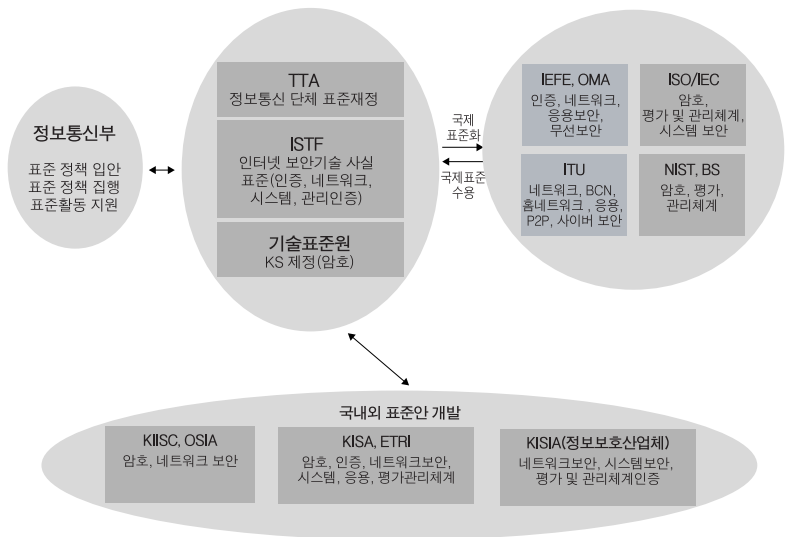
◦ 국제 표준 수용과 프로파일 표준 개발 작업을 추진함에 있어 산업체의 제품 경쟁력과 관련이 깊은 핵심 기술과 트러스트 플랫폼 기술에 대해서는 선행 시제품 개발을 병행하여 추진함으로써 표준 개발의 품질 제고 및 확보되는 핵심표준기술을 산업체에 제공하여 개발 표준이 조기 상용화되도록 추진

◦ 서버 보안 및 트러스트 플랫폼 기반 S/W 무결성 검증 기술 및 플랫폼 임의 조작 방지 기술 등은 국제 표준화 기구에 미래 표준기술 분야로 선행 표준 기술 연구 활동을 적극 추진하여 신규 표준화 분야에 대한 국제 표준 선점을 위한 국제 표준화 활동을 강화함

◦ 통합 PC보안이 요구되고 있는 시장 상황에 맞추어 각 업체별로 중복 투자되거나 통합화하는데 장애요인인 로그형식에 대해 기존 침입방지/탐지 시스템의 로그형식 표준화를 참조하여 통합관리를 위한 로그 형식 표준화 추진이 필요함

◦ IT 기술 환경 변화에 따른 다양한 디지털 포렌식 요구사항을 만족하는 기술을 개발하여 IPR 확보 및 국내외 표준화 추진

3.1.3. 표준화 추진체계

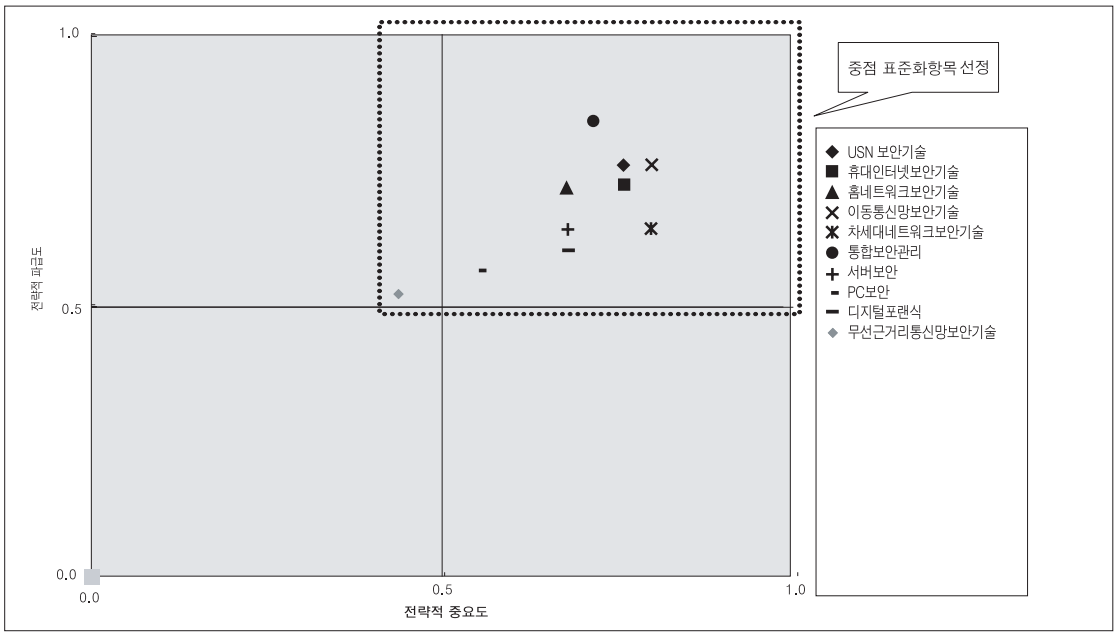


- 네트워크 및 시스템 보안 표준안 개발은 KISA, ETRI, 그리고 정보보호 산업체를 중심으로 국내외 표준(안)을 개발하고, 국내 표준의 경우 TTA를 통하여 국내표준화를 추진하며, 국제표준인 경우 IETF, ISO/IEC, 그리고 ITU-T를 통하여 국제 표준화를 추진
- PC보안 기술은 인터넷보안기술포럼(ISTF)을 통해 산업체 자율적으로 표준화를 추진하되 TTA를 통하여 국내 표준을 추진함
- 디지털 포렌식 기술은 ETRI, 학계 및 관련 산업체를 통하여 국내외 표준을 개발하고, 국내의 경우 TTA를 통하여 수행하고, 국제표준은 ITU-T 를 통하여 표준화를 추진함

3.2. 중점 표준화항목 선정

3.2.1. 중점 표준화항목 선정방법

표준화 대상항목에서 중점 표준화항목 도출을 위한 데이터입력												
	전략적 중요도						전략적 파급도					
고려요소	P1 산학연 관심도 (투자 등)	P2 정부 관심도 (정책 등)	P3 표준선도가능성(표준 투자정도)	P4 표준(기술) 개발의 시급성	P5 기술(표준) 격차	PI (Priority Index)	E1 타 산업 파급효과	E2 경제적 파급효과	E3 국내외시장 규모	E4 IPR 확보가능성 (로얄티수입)	E5 사용자편의 (호환성/공공성 등)	EI (Effect Index)
고려요소별 가중치(합계1)	0.2	0.2	0.2	0.2	0.2	1	0.2	0.2	0.2	0.2	0.2	1
USN 보안기술	4.0	4.0	4.0	4.0	3.0	0.8	4.0	4.0	4.0	4.0	3.0	0.8
휴대인터넷 보안기술	4.0	4.0	3.0	4.0	4.0	0.8	4.0	4.0	3.0	4.0	3.0	0.7
홈네트워크 보안기술	4.0	4.0	3.0	3.0	3.0	0.7	4.0	4.0	4.0	3.0	3.0	0.7
이동통신망 보안기술	4.0	4.0	4.0	4.0	4.0	0.8	4.0	4.0	4.0	4.0	3.0	0.8
무선근거리통신망 보안기술	3.0	2.0	2.0	2.0	2.0	0.4	3.0	3.0	3.0	2.0	2.0	0.5
차세대네트워크보안기술	4.0	4.0	4.0	3.0	5.0	0.8	3.0	3.0	3.0	4.0	3.0	0.6
통합보안관리	4.0	4.0	4.0	3.0	3.0	0.7	4.0	4.0	4.0	4.0	5.0	0.8
서버보안	4.0	3.5	3.0	3.5	3.0	0.68	4.0	3.0	3.0	3.0	3.0	0.64
PC보안	4.0	3.0	2.0	3.0	2.0	0.6	3.0	3.0	2.0	2.0	4.0	0.6
디지털포렌식	4.0	5.0	2.0	3.0	3.0	0.7	3.0	3.0	3.0	2.0	4.0	0.6



3.2.2. 중점 표준화항목 선정사유

• 전략적 중요도 및 기술적 파급효과의 요소
- 최근 ITU-T, ISO 등 국제표준화기구를 중심으로 진행되고 있는 시스템 및 네트워크 기술 표준화 동향을 중심으로 표준화 대상 항목을 선정하였음
- 또한, 국제적으로 우리나라가 표준화를 주도하거나, 주도 할 잠재력을 가진 분야, 기술개발시 국내외적으로 시장경쟁력을 확보할 수 있는 분야를 중심으로 표준화 대상 항목을 선정하였음
- 네크워크 보호 기술과 응용 보안은 정보보호 산업에 커다란 파급 효과를 갖는 분야임
- 이와 같은 기준에 따라 USN 보안기술, 휴대인터넷 보안기술, 홈네트워크 보안기술, 이동통신망 보안기술, 차세대 네트워크 보안기술, 통합보안관리, 서버 보안, PC 보안, 디지털포렌식의 표준화 대상항목을 선정하였음
- 와이브로는 차세대 이동통신기술로 서비스가 활성화 될 경우, 국내 고유의 기술로 개발되어 로열티 등의 지불이 없고, 상당한 경제적 부가가치 및 생산, 고용유발 효과를 지니고 있음
- 디지털 포렌식 기술은 검찰 및 경찰, 국정원 등의 국가 수사기관에서 활용되며, 중장기적으로는 내부 정보 유출 방지, 회계 감사 등의 내부 보안 강화를 위해 민간 산업 분야로의 파급 효과를 갖는 분야임
- 디지털 포렌식 분야의 경우, 공공성이 크고 새로운 보안 서비스 시장 창출할 수 있음
- 무선근거리 통신망 보안기술은 국내외 기술격차가 거의 없고 표준선도 가능성이 낮으며, IPR 확보가능성도 낮아 보이는 등 전략적 중요도와 파급도 측면에서 낮은 점수를 받아 중점 표준화항목에서 제외되었음

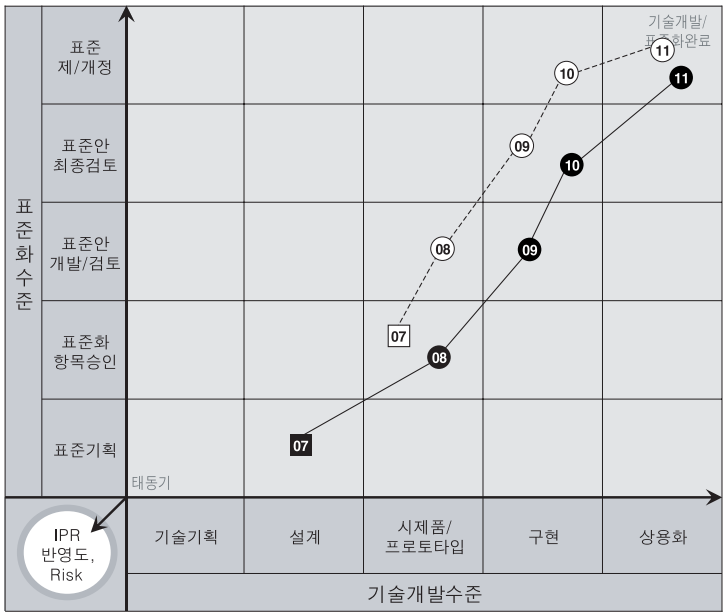
• 중점 표준화항목별 선정사유
- USN 보안기술
  ◦ TTA 의 RFID/USN 프로젝트 그룹에 보안 WG 혹은 분리된 프로젝트 그룹을 만들어 운영하며, 경량의 암호 및 인증을 위한 키관리 기술, 안전한 라우팅 기술, 안전한 배치 기술 등이 USN활성화를 위해 표준화 항목으로 선정함
- 휴대인터넷 보안기술
  ◦ 와이브로는 IEEE 802.11에서 발생했던 보안 취약성인 서비스거부공격 및 세션가로채기 등이 발생할 수 있어 서비스 초기단계인 와이브로 활성화에 장애요소가 될 수 있으므로, 가입자단에서의 인증 및 접근제어 기술에 대한 보안대책 마련이 필요하며, 이동성 제공에 있어서도 바인딩 업데이트 등에서의 서비스거부공격이 발생할 수 있으므로 중점 표준화 항목으로 선정함
- 홈네트워크 보안기술
  ◦ 우리나라가 홈네트워크 보안에 관한 표준화 활동이 가장 활발하고, 홈네트워크 보안에 관한 표준을 이끌어 가고 있음. 홈네트워크 및 홈네트워크 보안에 관한 종주국으로 내세우기에 손색이 없도록 더욱 활발한 표준화 활동이 이루어지고, 현재 ITU-T SG17 Q9에서 표준화 과정에 있는 표준안들이 표준으로 발표될 수 있도록 보안프레임워크, 보안기능기술언어, 인증 · 인가 메커니즘을 중점 표준화 항목으로 선정함

- 이동통신망 보안기술
  - ITU-T SG17에서 이동통신 보안기술 로드맵 작업이 이루어지고 있는 등 활발한 표준화 활동이 예상되므로 3GPP 보안, 3GPP2 보안을 중점 표준화 항목으로 선정함
- 차세대 네트워크 보안기술
  - 차세대 네트워크 구축 초기단계에서부터 사이버공격에 대한 상호연동이 가능한 조기 예방 및 대응체계를 구축하고, 사업자별 정보보호 대책 마련의 중요성 부각
  - 차세대 네트워크에서 발생할 수 있는 새로운 위협을 찾아내어 각각의 개별 환경 및 연동 표준화 과정에서 총괄적인 차세대 네트워크 보안 프레임워크 미흡으로 차세대 네트워크 분야에 공통으로 적용할 수 있는 보안 프레임워크, 메쉬노드용 협업 상호호환 기술, 서비스별 및 통합 · 분산 인증 기술을 중점 표준화 항목으로 선정함
- 통합보안관리
  - 네트워크 차원의 통합보안관리 기능 중 사이버 공격 감시 및 추적기술은 국내 각 정부 및 민간 기관별 침해대응센터의 고도화에 해당되는 것으로서 상호호환성이 절대적으로 필요하고, 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 추진하며, 일관성 있는 네트워크 접근제어 정책 서버 및 프록시 프레임워크와 네트워크 노드 인증에 대한 표준으로 확장될 것으로 예상됨에 따라 중점표준화 항목으로 선정함
- 서버보안
  - 접근통제 및 감사추적 기술, 서버 보안 및 트러스트 플랫폼 기반 S/W 무결성 검증 기술, 그리고 플랫폼 임의 조작 방지 기술 등은 국제 표준화 기구에서 미래 표준기술 분야로 선행 표준 기술 연구 활동을 적극 추진하여 국제 표준 선점을 위한 국제 표준화 활동을 강화하기 위해 중점표준화 항목으로 선정함
- PC보안
  - 통합 PC보안이 요구되고 있는 시장 상황에 맞추어 각 업체별로 중복 투자되거나 통합화하는데 장애요인인 로그 형식에 대해 기존 침입방지/탐지 시스템의 로그형식 표준화를 참조하여 통합관리를 위한 로그 형식 표준화 추진이 필요함에 따라 로그정보 교환 및 공통 API를 중점표준화 항목으로 선정함
- 디지털포렌식
  - 국내 사법 환경에 적합한 절차 가이드라인 및 수집, 분석 도구 검증 규격 등의 국내 표준화가 필요함에 따라, 컴퓨터 및 휴대폰 포렌식 가이드라인과 컴퓨터 포렌식을 위한 디지털 데이터 수집도구 요구사항, 디지털 데이터 분석도구 요구사항 및 수집/분석 도구에 대한 검증 규격을 중점표준화 항목으로 선정함

3.3. 중점 표준화항목별 세부전략(안)

3.3.1. USN 보안

• 표준상태전이도 (표준화 & 기술개발 연계분석)

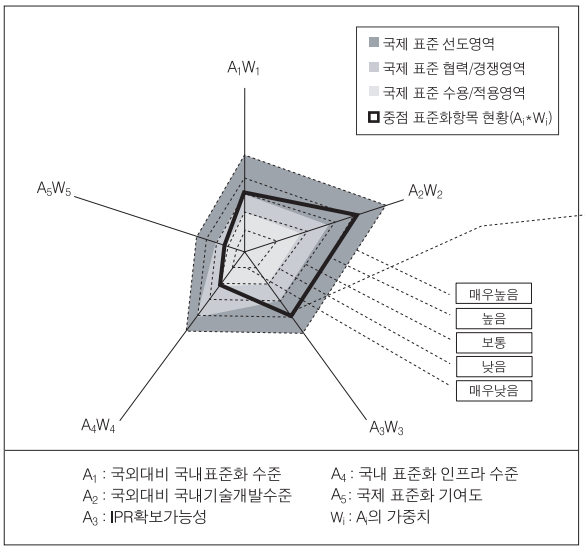


표준화 중요도	국내 개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★★★	TTA	삼성전자, 니츠 등	IEEE, ISO/IEC JTCI/SC27 W3C

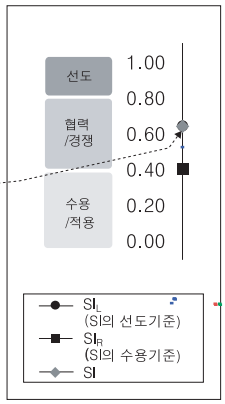
범 례

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

• 국제표준화 전략목표 도출



SI (표준화 전략지수)	
SI_L (SI의 선도기준)	0.64
SI_R (SI의 수용기준)	0.40
SI	0.64



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

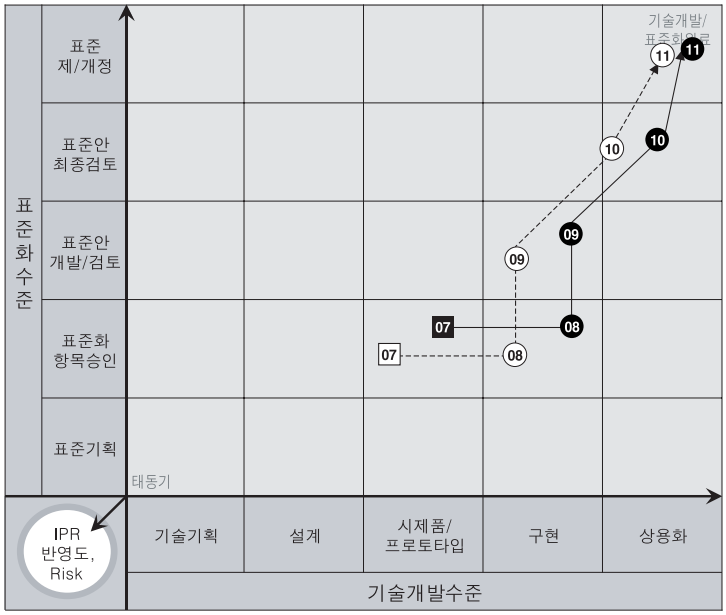
국제표준 협력/경쟁

• 세부전략(안)

- USN 보안과 관련하여 국내외 시장, IPR 확보가능성 등을 분석해 본 결과 매우 양호한 현실과 전망을 갖고 있음
- 하지만 국내 표준화 인프라 역량면에서 매우 미흡한 정도를 보이고 있어 이는 결국 국제표준화 참여 및 표준 제정 및 국내 표준화 활동에도 저조한 결과를 초래 하고 있음
- 따라서, TTA의 RFID/USN 프로텍트 그룹의 보안 WG등을 통하여 경량의 암호 및 인증을 위한 키관리 기술, 안전한 라우팅 기술, 안전한 배치 기술 등에 대한 표준화를 통하여 USN 활성화를 촉진시킴

3.3.2. 휴대인터넷 보안

• 표준상태전이도 (표준화 & 기술개발 연계분석)

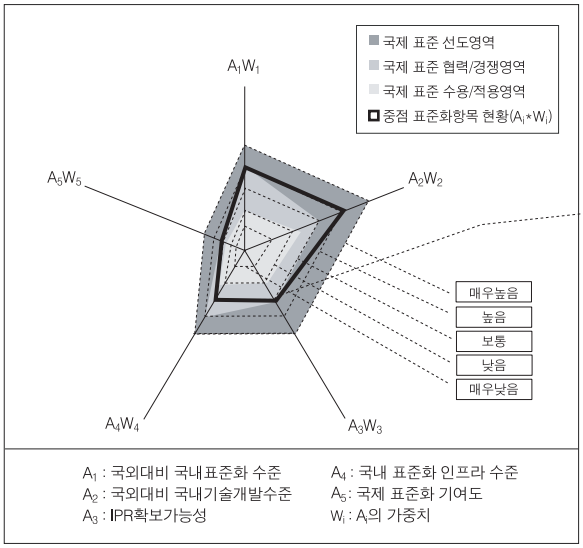


표준화 중요도	국내 개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★★	TTA	삼성전자, 포스데이타, ETRI 등	IEEE, ITU-T

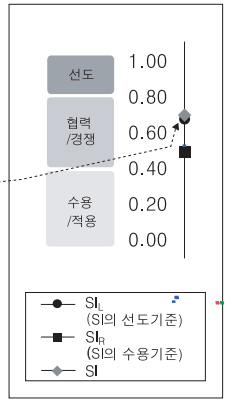
범 례

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

• 국제표준화 전략목표 도출



SI (표준화 전략지수)	
SI_L (SI의 선도기준)	0.68
SI_R (SI의 수용기준)	0.50
SI	0.70



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

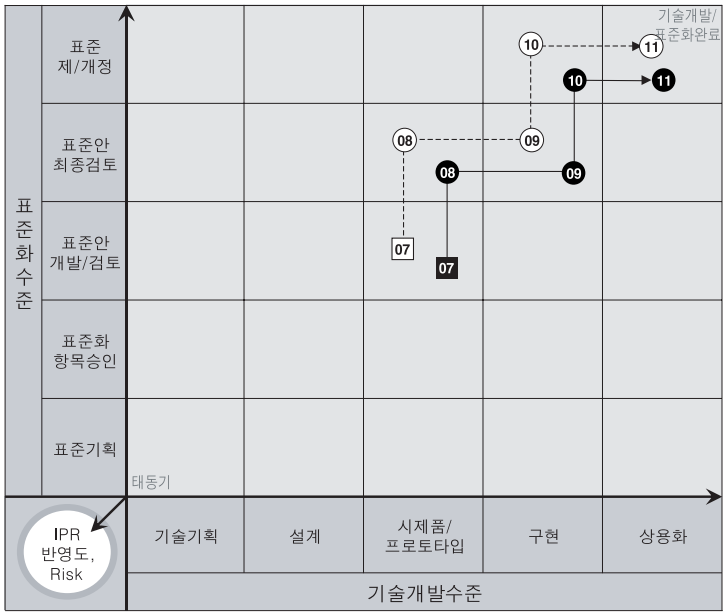
국제표준 선도

• 세부전략(안)

- 와이브로 보안 관련하여 국외대비 국내기술수준, 국외대비 국내표준화 수준, IPR 확보가능성 등 대부분의 항목에서 국제수준에 근접해 있음
- 와이브로 표준화는 초기부터 적극적으로 참여하고 산업화까지 연계되어 국제표준을 주도할 수 있을 것으로 예상됨
- 그러나, 와이브로 보안 측면에서는 활발한 활동이 이루어지고 있지 않으므로, 인증 및 접근제어 기술, IPv6 도입에 따른 보안기술 등에 관한 표준화 추진노력이 필요

3.3.3. 홈네트워크 보안기술

- 표준상태전이도 (표준화 & 기술개발 연계분석)



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

범 례

07 : 중점 표준화항목의 국내상태

07 : 중점 표준화항목의 국제상태

→ : 중점 표준화항목의 국내 표준상태전이

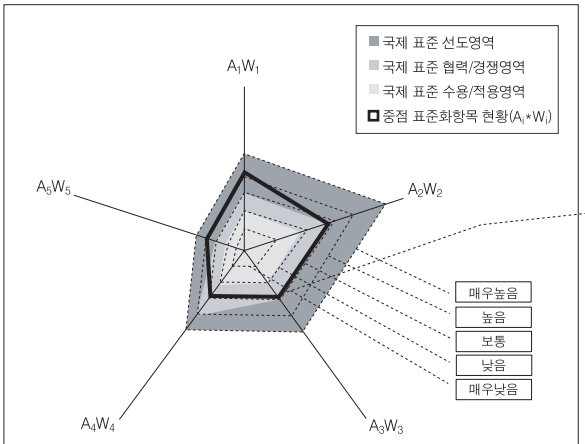
-→ : 중점 표준화항목의 국제 표준상태전이

↑ : 선행표준(선 표준화 후 기술개발)

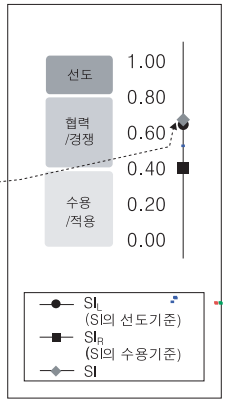
↗ : 동시표준(표준화&기술개발 동시추진)

↓ : 후행표준(선 기술개발 후 표준화)

- 국제표준화 전략목표 도출



SI (표준화 전략지수)	
SI_L (SI의 선도기준)	0.64
SI_R (SI의 수용기준)	0.40
SI	0.66



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

$$(0 < W_i < 1, 0 < SI \leq 1)$$

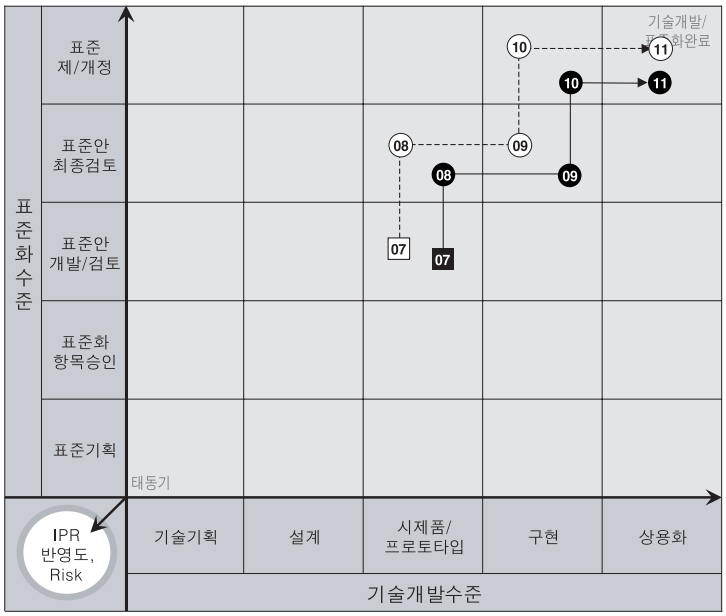
국제표준 선도

• 세부전략(안)

- 홈네트워크 보안 분야는 국내 기술개발이 활발히 진행되고 있고, 국제 표준화 기구에서도 많은 활동을 하고 있어, 국내 선도의 가능성이 높은 분야로 보안 프레임워크, 보안기능 기술언어, 인증, 인가 메커니즘에 대한 표준화를 추진하여 국제표준을 선도 및 협력, 경쟁할 필요가 있음

3.3.4. 이동통신망보안기술

• 표준상태전이도 (표준화 & 기술개발 연계분석)

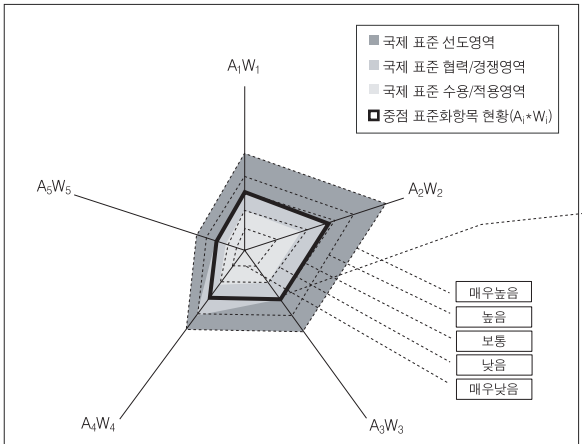


표준화 중요도	국내 개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★★	TTA	E TRI, 각 산업체	3GPP 3GPP2

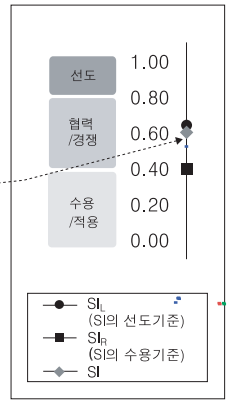
범 례

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

• 국제표준화 전략목표 도출



SI (표준화 전략지수)	
SI_L (SI의 선도기준)	0.64
SI_R (SI의 수용기준)	0.40
SI	0.60



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

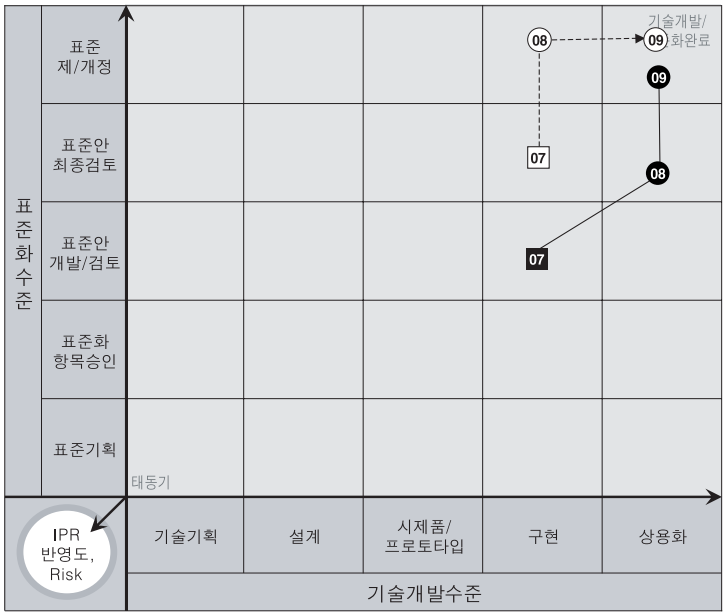
국제표준 협력/경쟁

- 세부전략(안)

  - 이동통신망 보안과 관련하여 국내에서 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

3.3.5. 무선근거리통신망 보안기술

- 표준상태전이도 (표준화 & 기술개발 연계분석)



표준화 중요도	국내 개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★★	TTA	ETRI, 각 산업체	IEEE

범 례

07 : 중점 표준화항목의 국내상태

07 : 중점 표준화항목의 국제상태

→ : 중점 표준화항목의 국내 표준상태전이

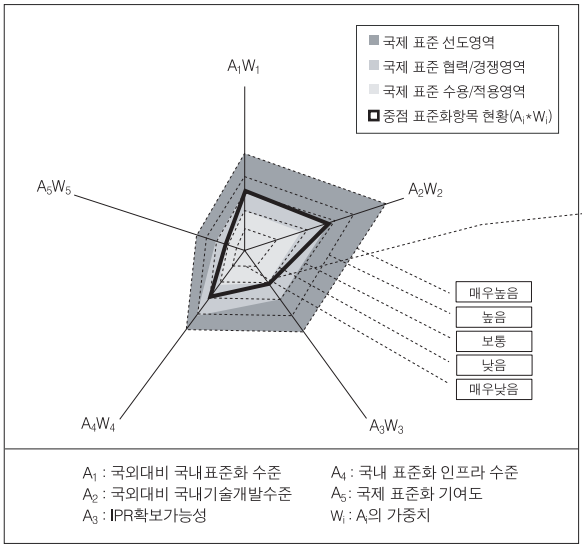
⇢ : 중점 표준화항목의 국제 표준상태전이

↑ : 선행표준(선 표준화 후 기술개발)

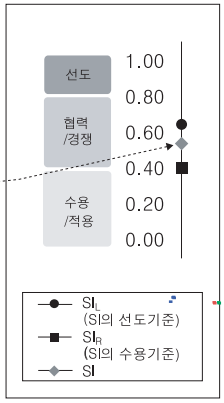
↗ : 동시표준(표준화&기술개발 동시추진)

↓ : 후행표준(선 기술개발 후 표준화)

- 국제표준화 전략목표 도출



SI (표준화 전략지수)	
SI_L (SI의 선도기준)	0.64
SI_R (SI의 수용기준)	0.40
SI	0.54



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

$$(0 < W_i < 1, 0 < SI \leq 1)$$

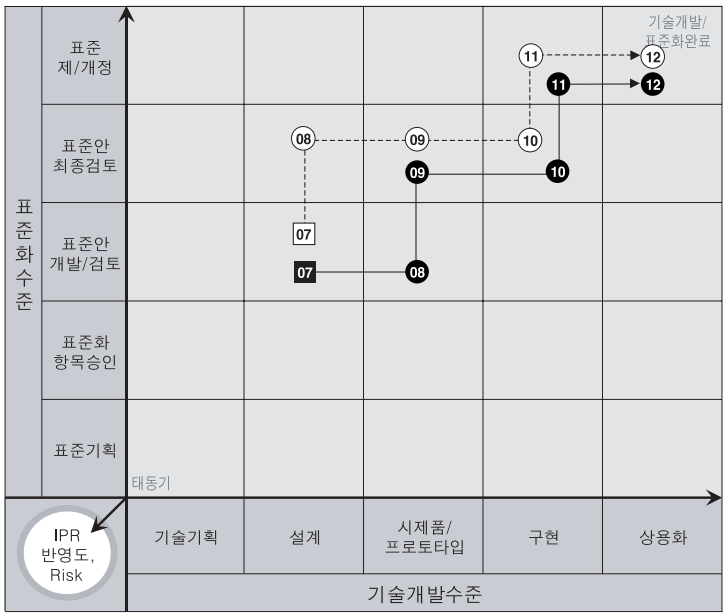
국제 표준 협력/경쟁

- 세부전략(안)

  - 무선근거리통신망 보안과 관련하여 프로토콜 수준에서의 보안 기술 표준화 문제가 일단락되면, 네트워크 측면에서 유무선 통합보안 기술에 대한 표준화 예상되며, 무선랜을 위한 인증 및 접근제어 기술, AP 위장 방지용 인증 기술, 무선랜 보안 프로파일 등에 대한 표준화를 중점적으로 추진함으로써 국제표준과 협력, 경쟁할 필요가 있음

3.3.6. 차세대네트워크 보안

• 표준상태전이도 (표준화 & 기술개발 연계분석)

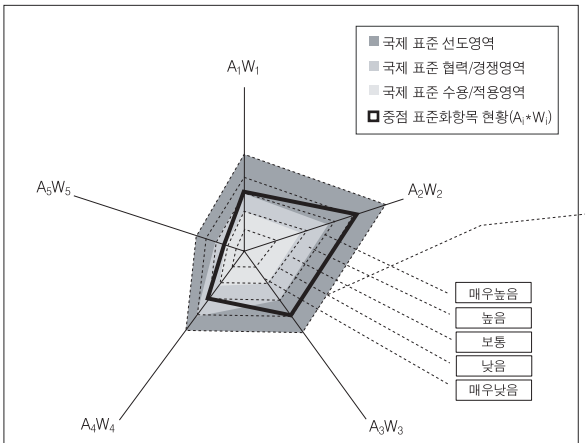


표준화 중요도	국내 개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★★★	TTA	ETRI	ITU-T, IETF

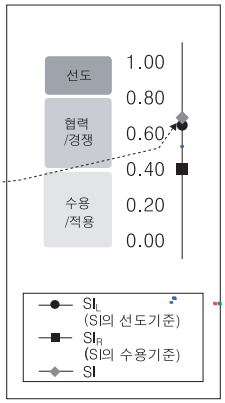
범 례

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

• 국제표준화 전략목표 도출



SI (표준화 전략지수)	
SI_L (SI의 선도기준)	0.64
SI_R (SI의 수용기준)	0.40
SI	0.68



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

국제표준 협력/경쟁 [일부선도]

• 세부전략(안)

- 국내외 표준화 현황분석에 따른 전략

◦ 차세대네트워크 분야는 Broadband, Mobility, QoS, IPv6 등에 이르기까지 매우 다양한 분야에 걸쳐있으므로 국내 · 외적으로도 다양한 프로젝트 그룹 및 워킹 그룹이 형성되어 표준화가 진행 중이며, 각 분야의 보안 기술 및 연동 환경의 보안 기술은 개별 분야에서 표준화를 진행하고 있음

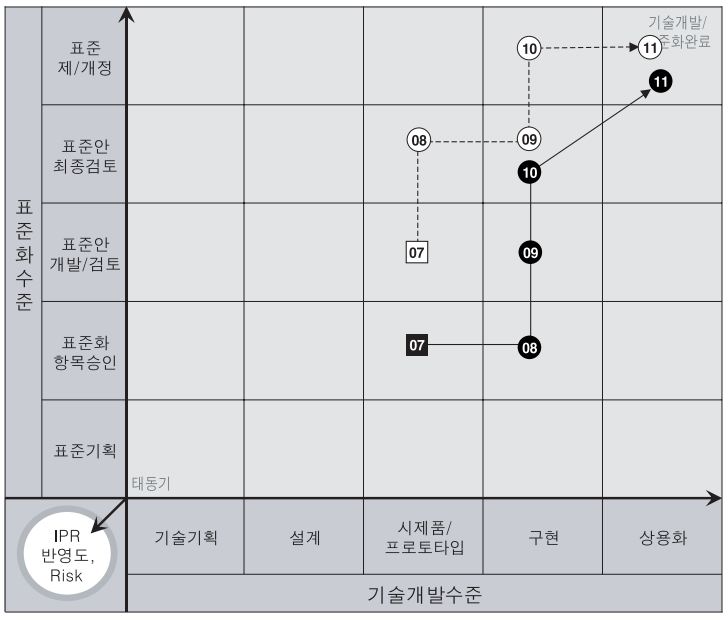
◦ 그러나 총괄적인 차세대 네트워크 보안 프레임워크 미흡으로 차세대 네트워크 분야에 공통으로 적용할 수 있는 보안 프레임워크, 절차 및 보안 요구사항 정의와 관련된 국내 · 외 표준 제정이 신규로 동시에 추진

- 국내외 기술개발 현황분석에 따른 전략

◦ 차세대 휴대 인터넷 서비스 시작이 국내가 세계 선두이므로 유 · 무선 연동 환경에서 나타날 수 있는 보안 위협과 이에 대한 보안 기술은 기술 선점이 가능하며, 이를 이용하여 국제 표준으로 연결될 수 있도록 추진

3.3.7. 통합보안관리

• 표준상태전이도 (표준화 & 기술개발 연계분석)

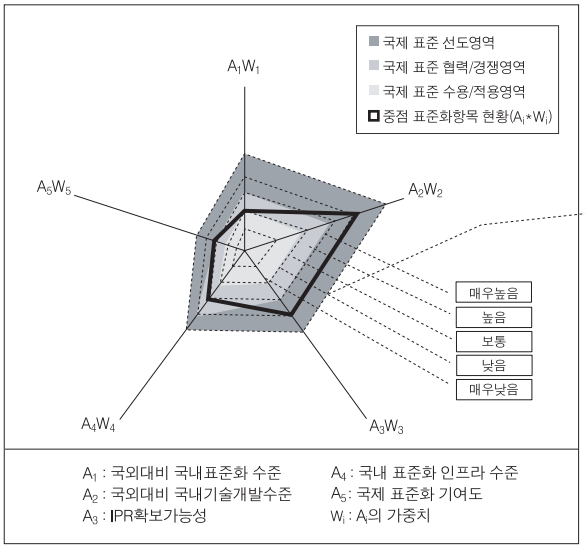


표준화 중요도	국내 개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★★★	TTA	ERTI, 이글루시큐리티, 인젠 등	ITU-T, IETF

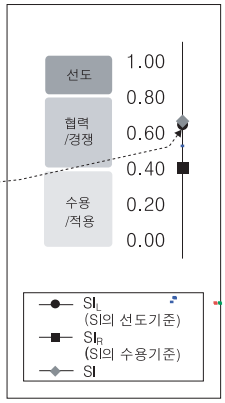
범 례

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

• 국제표준화 전략목표 도출



SI (표준화 전략지수)	
SI_L (SI의 선도기준)	0.64
SI_R (SI의 수용기준)	0.40
SI	0.66



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

국제표준 협력/경쟁 [일부선도]

• 세부전략(안)

- 국내외 표준화 현황분석에 따른 전략

◦ 네트워크 차원의 통합보안관리 기능 중 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 TTA PG102 그룹에서 정의하고 있으며, 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 추진하며, 실용적인 측면에서의 기술 검증 완성도와 함께 현재 미흡한 국제표준을 선도하는 상황에 역점을 두어 관련 국제 표준을 선도

◦ 현재 일관성 있는 침해사고 방지를 위한 네트워크 보안제어 정책프레임워크 표준이 진행되고 있으며, 향후에는 일관성 있는 네트워크 접근제어 정책 서버 및 프록시 프레임워크와 네트워크 노드 인증에 대한 표준으로 확장될 것으로 예상됨에 따라 국내 제품의 수출 및 국내 시장 보호를 위해 국제 또는 외국의 표준을 면밀히 분석하여 추진

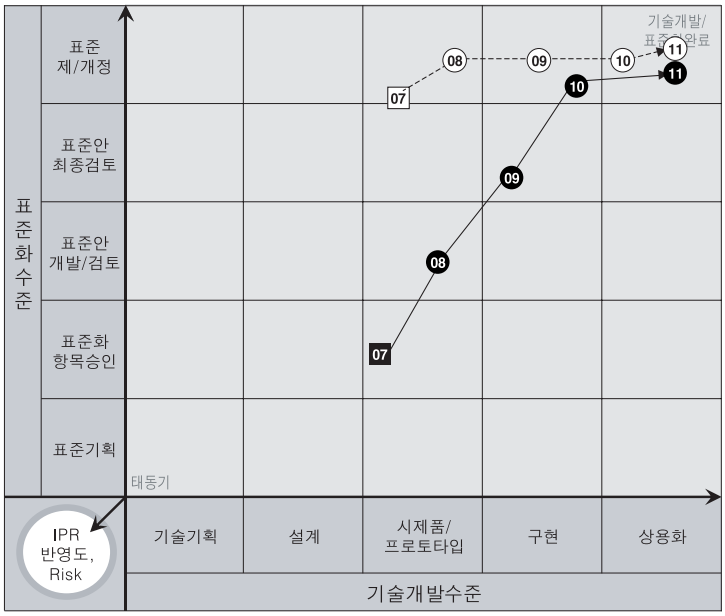
- 국내외 기술개발 현황분석에 따른 전략

◦ 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 표준기술 개발에도 중점을 두고 추진해야 함

3.3.8. 서버 보안

• 표준상태전이도 (표준화 & 기술개발 연계분석)

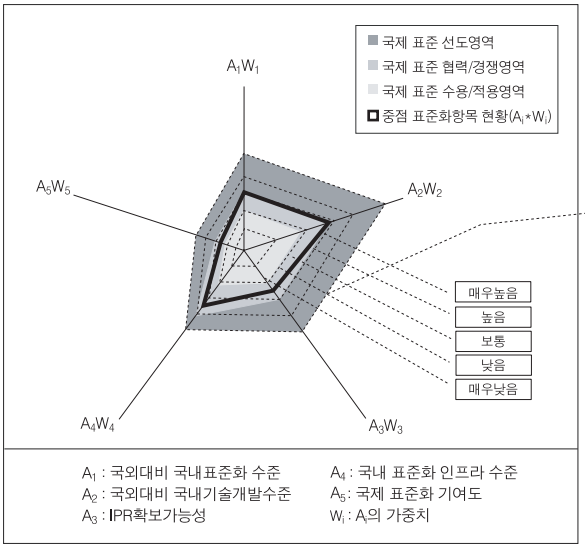


표준화 중요도	국내 개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★★	TTA	ETRI, Secuve 등	ITU-T, ISO, TCPA

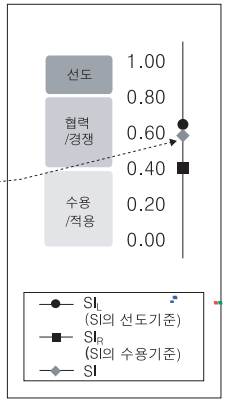
범 례

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

• 국제표준화 전략목표 도출



SI (표준화 전략지수)	
SI_L (SI의 선도기준)	0.64
SI_R (SI의 수용기준)	0.40
SI	0.59



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

국제표준 협력/경쟁 [일부선도]

• 세부전략(안)

- 표준화 추진

◦ 플랫폼 임의 조작 방지기술, 커널 무결성 검증기술 과 침해 확산 방지형 도메인 분리 기술은 TCG의 트러스트 플랫폼 환경에서 플랫폼 임의 조작 및 침해확산을 방지하는 TP(Trusted Platform) 및 네트워크의 신뢰성을 제공하는 TNC(Trusted Network Connection) 규격을 수용하고, 2009년 구현 기술에 대한 국내 고유 표준 개발을 추진함

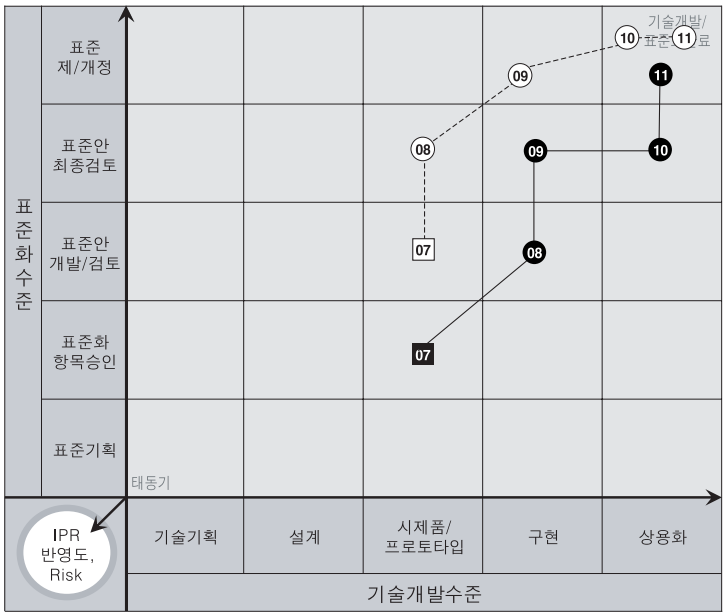
◦ 2008년 트러스트 운영체제 기술은 ISO 표준 규격을 바탕으로 트러스트 플랫폼용 보안 운영체제 국제 표준을 추진함으로 표준화 선도

- IPR 확보 방안

◦ 침해 확산 방지형 도메인 분리 기술은 새로운 개념의 분리 커널 표준화 분야로, Common Criteria를 기반으로 ISO에서 국제 표준화 및 IPR 확보를 추진함

3.3.9. PC 보안

• 표준상태전이도 (표준화 & 기술개발 연계분석)

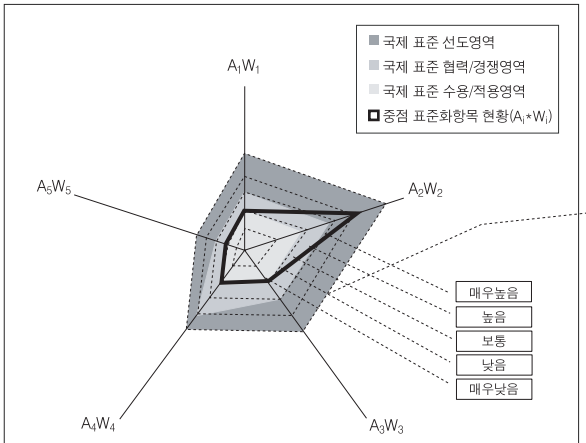


표준화 중요도	국내 개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★★	TTA ISTF	삼성전자, 각 산업체	ITU-T IETF

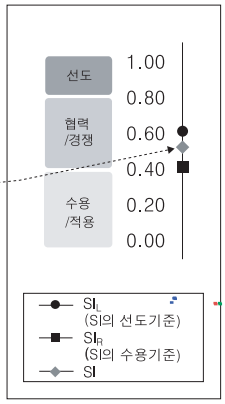
범 례

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

• 국제표준화 전략목표 도출



SI (표준화 전략지수)	
SI_L (SI의 선도기준)	0.60
SI_R (SI의 수용기준)	0.40
SI	0.52



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

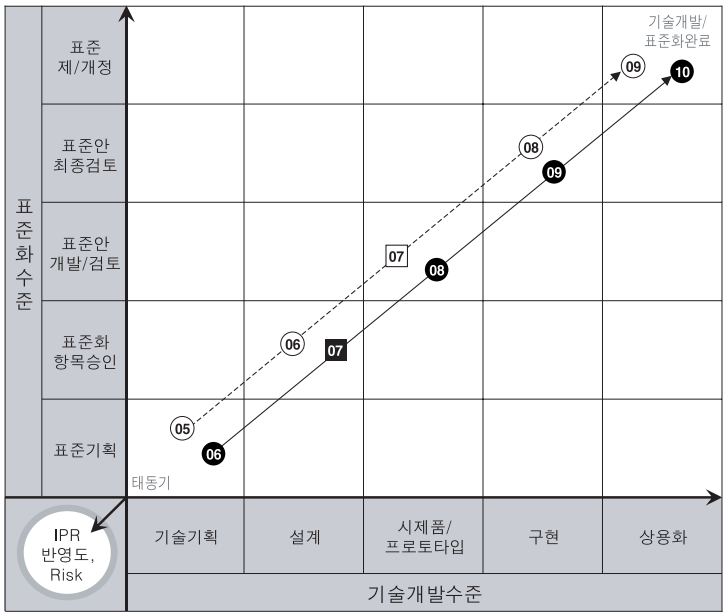
국제표준 협력/경쟁

• 세부전략(안)

- Anti-Virus분야에서는 글로벌하게 표준화하여 아직 독점을 하거나 사업을 주도하는 부분이 적으므로 표준화 동향의 주시가 필요
- 다만, 통합관리 요구를 수용하기 위해 국내에서 PC보안 로그 형식 표준화를 추진이 요구됨

3.3.10. 디지털포렌식

- 표준상태전이도 (표준화 & 기술개발 연계분석)

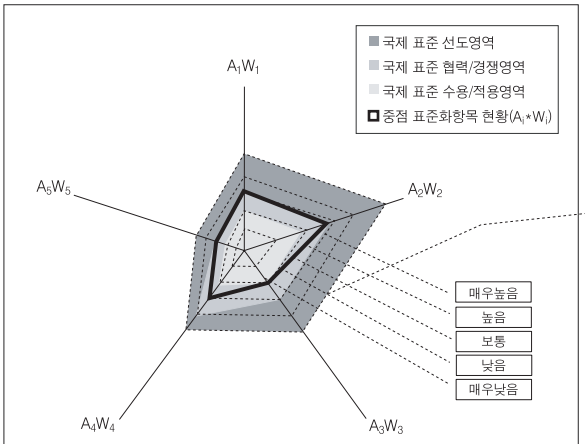


표준화 중요도	국내 개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★★	ETRI TTA	ETRI	ITU-T ISO/IEC JTC1/SC27

범 례

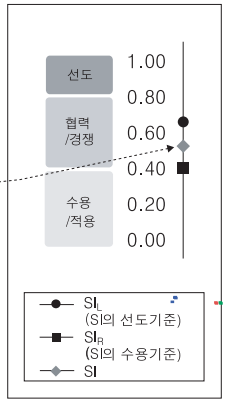
07 : 중점 표준화항목의 국내상태
07 : 중점 표준화항목의 국제상태
→ : 중점 표준화항목의 국내 표준상태전이
⇢ : 중점 표준화항목의 국제 표준상태전이
↑ : 선행표준(선 표준화 후 기술개발)
↗ : 동시표준(표준화&기술개발 동시추진)
↓ : 후행표준(선 기술개발 후 표준화)

- 국제표준화 전략목표 도출



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

SI (표준화 전략지수)	
SI_L (SI의 선도기준)	0.66
SI_R (SI의 수용기준)	0.40
SI	0.56



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

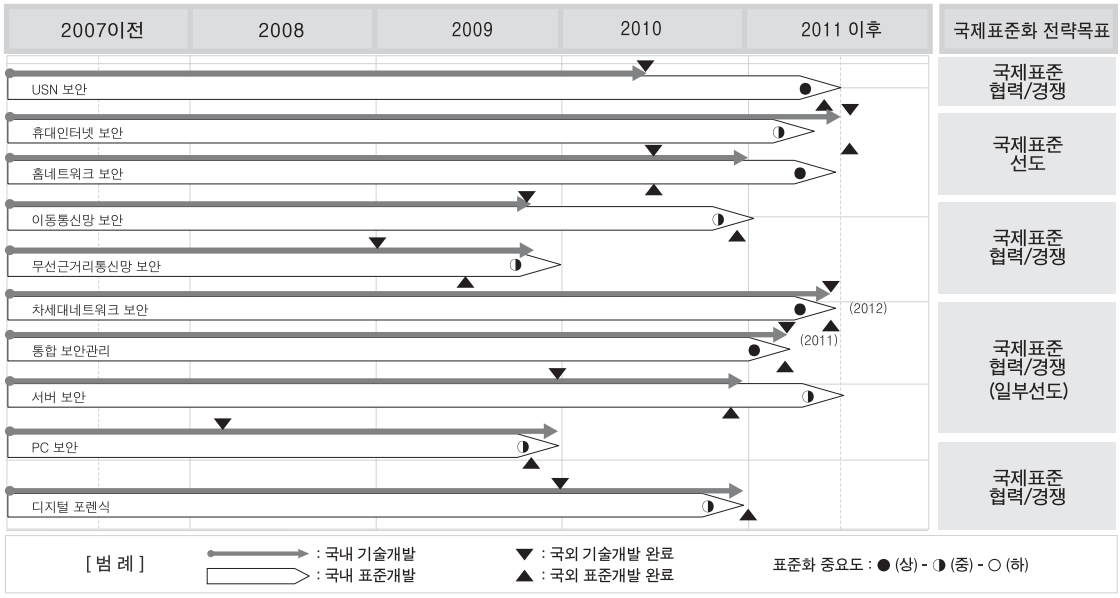
국제표준 협력/경쟁

• 세부전략(안)

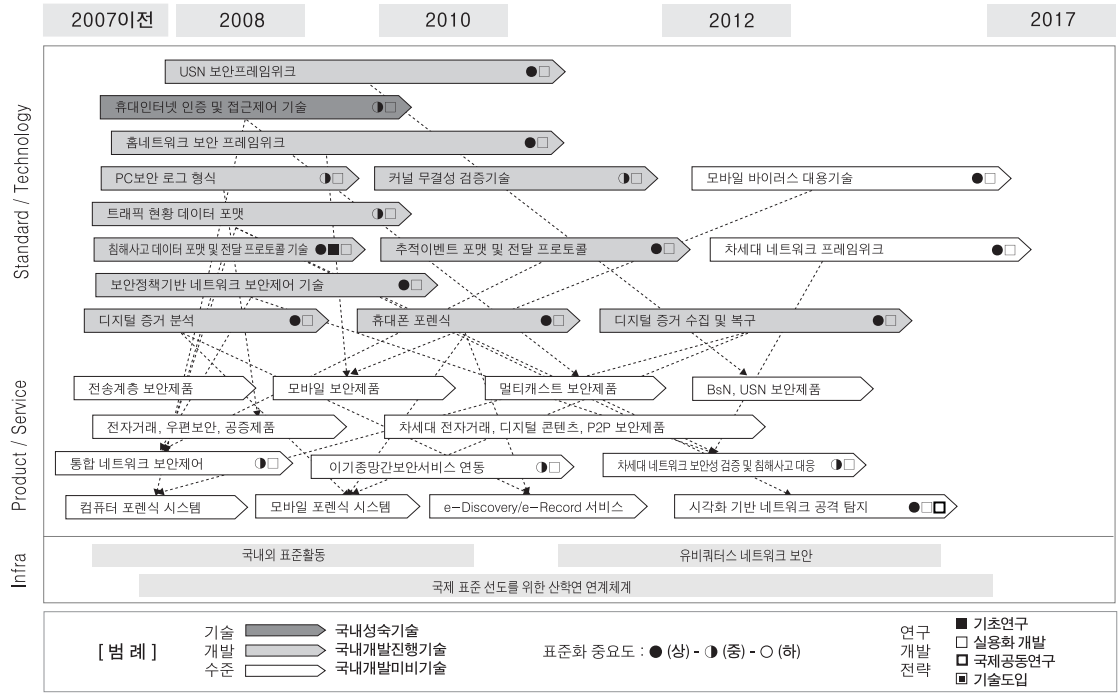
- 국내 사법 환경에 적합한 절차 가이드라인 및 수집, 분석 도구 검증 규격 등의 국내 표준화가 필요
  - 현재 국내 표준의 경우 TTA를 통해 컴퓨터 및 휴대폰 포렌식 가이드라인과 컴퓨터 포렌식을 위한 디지털 데이터 수집도구 요구사항 표준안이 작성 중에 있음
  - 향후 디지털 데이터 분석도구 요구사항 및 수집/분석 도구에 대한 검증 규격 등의 표준안이 개발되어야 함
- 아직 주도적인 국제 표준화 기구가 결성되지 않았으므로, 표준항목을 개발하여 ITU-T 등을 통한 국제 표준화 선도가 가능함
  - 2008년에 ITU-T SG17에서 포렌식 관련 표준항목을 준비하여, 2009년부터 주도적인 표준안 제안을 통해 국제 표준을 선도해 나갈 것임

3.4. 중장기 표준화로드맵

3.4.1. 중기('08~'10) 표준화로드맵(3개년)



3.4.2. 장기 표준화로드맵(10년 기술예측)



국내외 관련표준 대응리스트]

구분	표준화항목	표준명	기구 (업체)	제정 연도	재개정 현황	국내 관련표준	국내 추진기구
네트워크 보안	USN 보안	Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs)	IEEE	2003	제정		
		Systems Security Engineering Capability Maturity Model (SSE-CMM	ISO/IEC	2002	제정		
		IT network security ? Part 4: Securing remote access	ISO/IEC	2005	제정		
		Prime number generation	ISO/IEC	2005	제정		
		Random bit generation	ISO/IEC	2005	제정		
		Encryption algorithms - Part 4: Stream ciphers	ISO/IEC	2005	제정		
		Sensor Operating System API Framework for USN	ISO/IEC	2005	제정	USN용 센서 운영체제 API 프레임워크	TTA
		Information technology - Security techniques - IT network security ?Part 3: Securing communications between networks using security gateways	ISO/IEC	2005	제정		
	와이브로 보안	IEEE Std 802.16e-2005	IEEE	2005	제정	2.3GHz 휴대인터넷 상호인증 메커니즘	TTA
						2.3GHz 휴대인터넷 표준(물리계층 및 매체접근제어계층)	TTA
						2.3GHz 휴대인터넷 서비스 및 네트워크 요구사항	TTA
	통합 보안관리	IPsec-NAT Compatibility Requirements (RFC 3715)	IETF	2004	초안		TTA/ISTF
		A Traffic-Based Method of Detecting Dead IKE Peers (RFC 3706)	IETF	2004	초안		TTA/ISTF
		Using AES Counter Mode With IPsec ESP (RFC 3686)	IETF	2004	초안		TTA/ISTF
		The AES-XCBC-PRF-128 algorithm for IKE (RFC 3664)	IETF	2004	초안		TTA/ISTF
		The AES-CBC Cipher Algorithm and Its Use with IPsec (RFC 3602)	IETF	2003	초안		TTA/ISTF
		IP Security Policy Requirements (RFC 3586)	IETF	2003	초안		TTA/ISTF
		IPsec Configuration Policy Information Model (RFC 3585)	IETF	2003	초안		TTA/ISTF
		The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec (RFC 3566)	IETF	2003	초안		TTA/ISTF
		On the Use of Stream Control Transmission Protocol (SCTP) with IPsec (RFC 3554)	IETF	2003	초안		TTA/ISTF
		More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE) (RFC 3526)	IETF	2003	초안		TTA/ISTF
		The Use of HMAC-RIPEMD-160-96 within ESP and AH (RFC 2857)	IETF	2000	초안		TTA/ISTF
		RFC 2451 The ESP CBC-Mode Cipher Algorithms	IETF	1998	초안		TTA/ISTF
		RFC 2410 The NULL Encryption Algorithm and Its Use With IPsec	IETF	1998	초안		TTA/ISTF
		RFC 2409 The Internet Key Exchange (IKE)	IETF	1998	초안	ISTF-003	TTA/ISTF
		RFC 2408 Internet Security Association and Key Management Protocol(ISAKMP)	IETF	1998	초안	ISTF-003	TTA/ISTF
		RFC 2407 The Internet IP Security Domain of Interpretation for ISAKMP	IETF	1998	초안	ISTF-003	TTA/ISTF
		RFC 2406 IP Encapsulating Security Payload (ESP)	IETF	1998	초안	TTAS.KO-12.0014	TTA/ISTF
		RFC 2405 The ESP DES-CBC Cipher Algorithm With Explicit IV	IETF	1998	초안		TTA/ISTF
		RFC 2404 The Use of HMAC-SHA-1-96 within ESP and AH	IETF	1998	초안		TTA/ISTF

구분	표준화항목	표준명	기구 (업체)	제정 연도	재개정 현황	국내 관련표준	국내 추진기구
네트워크 보안	통합 보안관리	RFC 2403 The Use of HMAC-MD5-96 within ESP and AH	IETF	1998	초안		TTA/ISTF
		RFC 2402 IP Authentication Header	IETF	1998	초안	TTAS.KO-12.0014	TTA/ISTF
		RFC 2401 Security Architecture for the Internet Protocol	IETF	1998	초안	ISTF-003, TTAS.KO-12.0014	TTA/ISTF
		RFC 2085 HMAC-MD5 IP Authentication with Replay Prevention	IETF	1997	초안		TTA/ISTF
		RFC 1825 Security Architecture for the Internet Protocol	IETF	1995	초안	TTAS.KO-12.0014	TTA/ISTF
		RFC 1826 IP Authentication Header	IETF	1995	초안		TTA/ISTF
		RFC 1827 IP Encapsulating Security Payload (ESP)	IETF	1995	초안	TTAS.KO-12.0014	TTA/ISTF
		RFC 1828 IP Authentication using Keyed MD5	IETF	1995	초안		TTA/ISTF
		RFC 1829 The ESP DES-CBC Transform	IETF	1995	초안		TTA/ISTF
		The TUNNEL Profile	IETF	2003	초안		TTA/ISTF
		Intrusion Detection Mesage Exchange Requirements	IETF	진행중	-		TTA/ISTF
		Intrusion Detection Message Exchange Format Data Model and Extensible Markup Language (XML) Document Type	IETF	진행중	-	ISTF-004/R, ISTF-005/R, ISTF-019, ISTF-020	TTA/ISTF
		The Intrusion Detection Exchange Protocol (IDXP)	IETF	진행중	-		TTA/ISTF
		RFC 3749 Transport Layer Security Protocol Compression Methods	IETF	2004	초안		TTA/ISTF
		RFC 3546 Transport Layer Security (TLS) Extensions	IETF	2003	초안		TTA/ISTF
		RFC 3268 AES Ciphersuites for TLS	IETF	2002	초안		TTA/ISTF
		RFC 2818 HTTP Over TLS	IETF	2000	초안		TTA/ISTF
		RFC 2817 Upgrading to TLS Within HTTP/1.1	IETF	2000	초안		TTA/ISTF
		RFC 2712 Addition of Kerberos Cipher Suites to Transport Layer Security(TLS)	IETF	1999	초안		TTA/ISTF
		RFC 2246 The TLS Protocol Version 1.0	IETF	1999	초안		TTA/ISTF
시스템 보안	서버 보안	Standard for Information Technology Portable Operating System Interface (POSIX) Part 26: Device Control Application Program Interface (API) [C Language] IEEE Computer Society Document	IEEE	2003	제정		
		"Standard for Information Technology - Portable Operating System Interface (POSIX) IEEE Computer Society Document; Includes Vol 1-Base Definitions, Vol 2-System Interfaces, Vol 3-Shell and Utilities, Vol 4-Rationale (Informative)"	IEEE	2003	제정		
		Information Technology - Portable Operating System Interface (POSIX) System Administration - Part 2: Software Administration First Edition; ANSI/IEEE Std 1387.2	ISO/IEC	2003	제정		
		Information technology Portable Operating System Interface (POSIX) Test methods for measuring conformance to POSIX Part 2: Shell and utilities First Edition; IEEE Std 2003.2-1996	ISO/IEC	2003	제정		
		Information technology - Portable Operating System Interface (POSIX) - Part 2: System Interfaces Third Edition; IEEE Std 1003.1:2003; Corrigendum 1: 9/15/2004	ISO/IEC	2004	제정		

구분	표준화항목	표준명	기구 (업체)	제정 연도	재개정 현황	국내 관련표준	국내 추진기구
시스템 보안	서버 보안	Information Technology - Portable Operating System Interface (POSIX) - Part 1: Base Definitions Fourth Edition; IEEE 1003.1; Corrigendum 1: 9/15/2004	ISO/IEC	2005	제정		
		PROTABLE OPERATING SYSTEM INTERFACE (POSIX) PART 2 : SHELL AND UTILITIES	ISO/IEC	2005	제정	POSIX - PART 2 : 쉘과 유틸리티 표준 - ISO/IEC 9945-2	TTA
		A STANDARD FOR PORTABLE OPERATING SYSTEM INTERFACE(POSIX)	ISO/IEC	2005	제정	개방형 운영체제 인터페이스(POSIX.1) 표준	TTA
		PORTABLE OPERATING SYSTEM INTERFACE(POSIX) PART 1 : SYSTEM APPLICATION PROGRAMMING INTERFACE(API) [C LANGUAGE]	ISO/IEC	2005	제정	POSIX - PART 1 : C 언어를 위한 시스템 응용 프로그래밍 인터페이스(API) 표준 - ISO/IEC 9945-1	TTA
		Sensor Operating System API Framework for USN	ISO/IEC	2005	제정	USN용 센서 운영체제 API 프레임워크	TTA

[참고문헌]

〔1〕 Common Criteria for Information Technology Security Evaluation (aligned with ISO/IEC International Standard (IS) 15408), Version 2.1, August 1999.The CC consists of four volumes available at, e.g., http://www.radium.ncsc.mil/tpep/library/ccitse/, and at http://csrc.nist.gov/cc/ccv20/ccv2list.htm#CCV21.

〔2〕 Protection Profile for Multilevel Operation Systems in Environments Requiring Medium Robustness, version 1.22, NSA, May 2001

〔3〕 Protection Profile for Singlelevel Operation Systems in Environments Requiring Medium Robustness, version 1.22, NSA, May 2001

〔4〕 Common Criteria Public Knowledge Base, http://niap.nist.gov/tools/CCTB60f-Documentation/CC_PKB/Reports/, http://niap.nist.gov/tools/CCTB60f-Documentation/CC_PKB/User_Guide/, NIAP, March 2000

〔5〕 Trusted Computing Group(TCG) Design Philosophies and Concepts Version 1.0

〔6〕 Trusted Computing Group(TCG) Main Specification Version 1.1b, http://www.trustedcomputinggroup.org/, February 2002 (also known as Trusted Computing Platform Alliance(TCPA) Main Specification Version 1.1b)

〔7〕 TCG Software Stack(TSS) Specification Version 1.0

〔8〕 Common Criteria Part : Security functional requirements, Aug 1999, Ver.2.1

〔9〕 〔200404lan.pdf〕 박용우, 무선랜 장비시장 현황 및 국내시장에의 시사점, 정보통신정책 제16권 5호 통권 343호, 2004.

〔10〕 밸류애드, 무선 LAN카드(WLAN) 시장 동향, 전자정보센터(EIC), 2007.

〔11〕 김상훈, 무선랜 칩셋 동향, 전자정보센터(EIC), 2005.

〔12〕 지경용, 김문구, 오동섭, 무선랜 서비스 이용 현황 및 시장확대 방향, 한국전자통신연구원(ETRI), 2005.

〔13〕 (주)KRG, 국내 무선보안 동향 보고서, 전자정보센터(EIC), 2004.

〔14〕 이석규, 무선랜 표준화 :IEEE802.11의 워킹그룹이 주도적 역할 :글로벌시대의 키워드 'IT표준화', 한국전자통신연구원(ETRI), 2004.

〔15〕 정병호, 한국정보통신기술협회(TTA), 무선 LAN 보안 기술 표준화 동향, 2003.

〔16〕 Zhiqi Tao and A.B. Ruighaver, Detecting Rogue Access Points that endanger the Maginot Line of Wireless Authentication, Proceedings of the 3rd Australian Information Security Management Conf..

〔17〕 강유성, 사용자 중심의 무선랜 이동보안 기술 표준화 논의 본격화, 한국정보통신기술협회(TTA), IT Standard Weekly 2005-04호, 2005.

〔18〕 정찬형, 유비쿼터스 환경을 위한 무선 메쉬 네트워크 기술 동향, 한국정보산업연합회(FKII), IT Issue 2004.

〔19〕 Stefan Savage, David Wetherall, Anna Karlin and Tom Anderson, Practical Network Support for IP Traceback, Technical Report UW-CSE-00-02-01, Department of Computer Science and Engineering, University of Washington, Seattle

〔20〕 Micah Adler: Tradeoffs in probabilistic packet marking for IP traceback, STOC 2002: pp. 407-418

〔21〕 A. Belenky, N. Ansari, "On IP Traceback" IEEE Communication Magazine, vol. 41, pp. 142 - 153, July 2003.

〔22〕 S.C. Lee and C. Shields, "Tracing the Source of Network Attack: A Technical, Legal and Societal Problem", Proc. of the IEEE Workshop on Information Assurance and Security, June 2001, West Point, NY

〔23〕 Don Cohen and K. Narayanaswamy, "Survey/Analysis of Levels I, II, and III Attack Attribution Techniques", Cs3, Inc., April 27, 2004.

〔24〕 A. D' Amico and M. Kocka, "Information Assurance Visualizations for Specific Stages of Situational Awareness and Intended Uses: Lessons Learned", Proc. of VizSEC'05, IEEE, pp. 107-112, Oct. 2005.

〔25〕 Y. Livnat, J. Agutter, S. Moon, and S. Foresti, "Visual Correlation for Situational Awareness", Proc. of IEEE 2005 Symposium on Information Visualization (InfoVis'05), Oct. 2005.

〔26〕 G. Conti, J. Grizzard, M. Ahamad and H. Owen, "Visual Exploration of Malicious Network Objects Using Semantic Zoom, Interactive Encoding and Dynamic Queries", Proc. of VizSEC'05, IEEE, pp. 83-90, Oct. 2005.

〔27〕 정보통신연구진흥원, "정보보호 기술로드맵(ITRM 2012)," 2007.1.

〔28〕 정보통신부, "Dynamic u-Korea 건설을 위한 광대역 통합망(BcN) 구축 기본 계획 II," 2006. 2.

〔29〕 BcN 포럼, "BcN 표준모델 v2.0," 2006. 2.

〔30〕 정보통신부, "광대역통합망 구축 기본계획," 2004.2

〔31〕 Igor Faynberg, etc. "Converged Networks and Services," John Wiley & Sons Inc., 2000

〔32〕 IDC, "Worldwide Standalone VOIP Gateways Forecast and Analysis," 2002. 3

〔33〕 Ovum, "Market Strategies for Telcos and ISPs," 2000

〔34〕 Gartner Dataquest, "Worldwide Switching Market Share and Forecast," 2003.5

〔35〕 Igor Faynberg, etc. "Converged Networks and Services," John Wiley & Sons Inc., 2000

〔36〕 BcN포럼, "광대역통합망(BcN) 기술 워크샵," 2004.6

〔37〕 한국전자통신연구원, "유비쿼터스 서비스를 위한 BcN 기술 워크샵," 2004.9

〔38〕 ITU-T: http://www.itu.int/ITU-T/

〔39〕 IEEE P1520: http://www.ieee-pin.org

〔40〕 ETSI: http://www.etsi.org

〔41〕 ITU-T FGNGN Ouput Documents: http://ties.itu.int/fgngn/fgngn

〔42〕 IETF: http://www.ietf.org

〔43〕 IST: http://www.cordis.lu/ist/

〔44〕 광대역통합네트워크(BcN) 포럼: http://www.bcnforum.or.kr

〔45〕 한국전산원, "2005 국가정보화 백서," 2005.8

〔46〕 TTA, "정보통신 중점기술 표준화로드맵 종합보고서," (Ver. 2005)

〔47〕 Arkoudi-Vafea Aikaterini, SECURITY OF IEEE 802.16

〔48〕 Sen Xu Manton Matthews Chin-Tser Huang, "Security Issues in Privacy and Key Management Protocols of IEEE 802.16", ACM SE'06, March 10-12, 2006, Melbourne, Florida, USA

〔49〕 DAVID JOHNSTON AND JESSE WALKER, "Overview of IEEE 802.16 Security", THE IEEE COMPUTER SOCIETY, 2004

〔50〕 H. Honkasalo, K, Pehkonen, M.T. Niemi, and A.T. Leino, "WCDMA and WLAN for 3G and beyond", IEEE Wireless Communications Magazine, vol. 9, pp 14-18, 2002. 4

〔51〕 3GPP, "3GPP TR 22.234 v6.2.0, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Feasibility study on 3GPP system to Wireless Local Area Network (WLAN) Interworking (Release 6)", 2003. 9

〔52〕 Tom Katygiannis, Les Owens, "Draft Wireless Network Security", National Institute and Technology(NIST), 2002

〔53〕 "IEEE802.11b Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification", IEEE Standard 802.11b, 1999

〔54〕 "Port-based Network Access Control", IEEE Standard 802.1x, 2001. 6

〔55〕 L. Blunk, J. Vloobrecht, "PPP Extensible Authentication Protocol (EAP), IETF RFC2284, 1998. 3

〔56〕 지경용, 강충구, 조용수, "휴대인터넷의 이해", 2006.3

〔57〕 임선희, 이옥연, 전성익, 한진희, "EAP-AKA를 적용한 WiBro 무선네트워크의 인증구조 연구", 한국통신학회논문지, 2006.4

〔58〕 "무선랜 안전운영가이드", 한국정보보호진흥원, 2004.12

〔59〕 "IPv6 보안기술해설서", 한국정보보호진흥원, 2005.10

〔60〕 "TTA 정보보호 표준화 로드맵", TTA, 2006

[약어]

3GPP	3rd Generation Partnership Project
ACL	Access Control List
AES	Advanced Encription Standard
AKA	Authentication and Key Agreement
AKA	Authentication and Key Agreement
API	Application Program Interface
ARDA	Advanced Research and Development Activity
AV	Anti-Virus
BcN	Broadband Convergence Network
CACS	Common Access Control Service
CARO	Computer Antivirus Researchers Org.
CDMA	Code division multiple access
CFTT	Computer Forensic Tool Testing
CRTM	Core Root of Trust Measurement
DAC	Discretionary Access Control
DES	Data Encryption Standard
DETER	Cyber Defense Technology Experimental Research
DHC	Dynamic Host Configuration
DNSext	Domain Name System Extensions
DNSop	Domain Name System Operations
DoD	Department of Defense
EMIST	Evaluation Methods for Internet Security Technology)
ENFSI	European Network of Forensic Science Institute
ENISA	European Network and Information Security Agency
ESI	Electronically Stored Information
ESM	Enterprise Security Management
F/W	Firewall
FBI	Federal Bureau of Investigation
FINE	Format for Incident Information Exchange
HSDPA	High Speed Downlink Packet Access
HSUPA	High Speed Uplink Packet Access

ICT	Information and Communications Technology
IDWG	Intrusion Detection Working Group
IMS	IP Multimedia Subsystem
IPS	Intrusion Prevention System
ISMS	Information Security Management System
MAC	Mandatory Access Control
MIP6	Mobility for IPv6
NEMO	Network Mobility