네트워크 및 시스템 보안

1. 개요

1.1. 기술개요

1.1.1. 중점기술 및 표준화 대상항목의 정의

○ 중점기술의 정의

○ 인터넷과 같은 개방형 네트워크 환경에서 전달되는 정보의 위조, 변조, 유출, 무단침입 등을 비롯한 불법 행위로부터 정보를 보호하는 네트워크 보안과, 정보통신 시스템의 안전성과 가용성을 향상시키는데 필요한 정보보호 기술 및 디지털 증거 제공을 위한 기술을 포함한 시스템 보안으로 구성

○ 네트워크 및 시스템 보안 분야는 유비쿼터스 센서 네트워크(USN) 보안, 휴대인터넷 보안, 홈네트워크 보안, 무선근거리통신망 보안, 이동통신망 보안, 차세대 네트워크 보안, 사이버공격 역추적/보안관리, 봇넷대응, 서버 보안, PC 보안, 디지털포렌식 등의 11가지 분야로 구분

○ 표준화 대상항목의 정의

- 네트워크 보안 분야의 경우는 USN 보안, 휴대인터넷 보안, 홈네트워크 보안, 무선근거리통신망 보안, 이동통신망 보안, 차세대 네트워크 보안, 사이버공격 역추적/보안관리 등 7개 분야의 표준화 대상항목으로 분류함
- 시스템 보안 분야의 경우는 봇넷대응, 서버 보안, PC 보안, 디지털포렌식 등 4개 분야의 표준화 대상항목으로 분류함

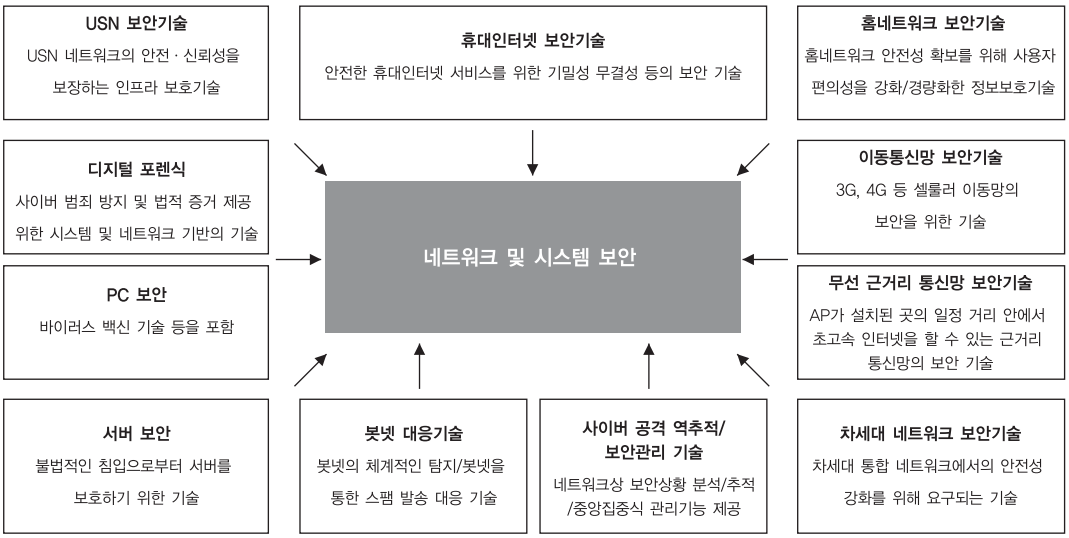
구분	정의	표준화 대상항목	세부표준화 항목	표준화 내용
네트워크 보안	개방형 네트워크 환경에서 전달되는 정보의 위·변조, 유출, 무단 침입 등을 비롯한 불법행위로부터 정보를 보호	USN 보안기술	USN 응용 서비스를 위한 인증 기술	USN 서비스에서 센서네트워크까지의 안전한 서비스 제공을 위한 인증 가이드라인 및 기법을 제공할 수 있도록 표준화 추진
			안전한 라우팅 기술	안전한 서비스를 위한 기밀성, 무결성 등의 보안기술
			USN 미들웨어 보안기술	USN 응용 서비스와 센서네트워크 간 존재하는 미들웨어 계층에서 요구되는 보안 요구사항 및 가이드라인을 제시하고, 보안기법 표준화 추진
			USN 보안 프레임워크	USN 서비스에서 안전한 서비스 제공을 위한 보안 프레임워크
		휴대인터넷 보안기술	이종 네트워크 간 핸드오버를 위한 보안기술	BcN 기반의 인터네트워크 통합 환경에서 이종 네트워크 간 핸드오프를 안전하게 수행하기 위한 보안기술에 대한 표준화 추진
			4G에서의 인증 및 사용자 접근 제어기술	4G 환경에서 휴대인터넷의 보안을 제공하기 위한 인증 및 사용자 접근 제어 등의 보안기술 표준화 추진
		홈네트워크 보안기술	보안제품 간 상호호환성을 위한 보안정책 기술언어	홈네트워크 보안정책을 적용을 위해 홈네트워크 상황에 적합한 문법과 홈네트워크 구성 요소 및 홈네트워크 보안 기능 등에 대한 정의를 표준화함. 향후 새로이 개발된 보안기능을 고려하여 확장성을 제공할 수 있도록 하며 홈네트워크 보안제품 간의 상호호환성을 제공할 수 있도록 표준화를 추진
			홈네트워크 인가 프레임워크	홈네트워크 서비스의 안전한 사용을 위해 홈네트워크 인가 프레임워크에 대한 표준화가 ITU-T SG17에서 진행되고 있으며, 국제표준 제정 시 국내 표준화를 추가적으로 추진할 예정
			홈네트워크 IT 보안과 홈네트워크 물리 보안 간 융합을 위한 융합 보안 프레임워크	사용자 이용 선호도가 가장 높은 홈시큐리티 서비스 활성화를 위해 관련 보안제품 간 효율적인 상호 연동이 이루어질 수 있도록 홈네트워크 IT보안제품과 홈네트워크 물리보안제품으로 구성되는 융합 서비스 환경의 구성모델, 구성요소, 취약점 및 대응기술 등에 관련된 표준화 추진
		이동통신망 보안기술	모바일 단말 보안 및 모바일 백신	이동통신 단말들이 다양한 인터페이스를 수용하고 있고, 전화번호, 동영상, 사진 등의 개인정보를 저장하고 있어서 이러한 개인정보의 보호와 바이러스 등의 침해로 인한 서비스 장애를 예방하기 위한 모바일 환경의 단말 보안 및 모바일 백신 표준화 추진
			이동통신망 보안 관리 프레임워크	이동통신서비스의 종단 간 정보보호를 제공하기 위한 정보보호 구조를 정의하고, 관리평면, 제어평면 그리고 사용자평면에 가해지는 여러 형태의 위협을 대처하기 위한 접근제어, 인증, 부인방지, 데이터 기밀성, 데이터 무결성, 프라이버시 등의 적절한 정보보호 서비스들을 제공하기 위한 정보보호 프레임워크 및 관리 메커니즘에 대한 표준화 추진
			사용자 인증 및 이종망 간 보안 객체 연동기술	이동통신서비스의 끊김이 없는 서비스 제공을 위해 사용자 인증 및 디바이스 인증 정보 등의 보안객체에 대한 연동은 필수적이며 이는 이종망 간의 서비스연동 시에는 더욱 중요한 부분으로 상호호환성, 상호연동성이 보장되어야 하며 이를 ITU-T SG17 모바일 정보보호 Question에서 보안객체 연동기술 표준화 및 3GPP, 3GPP2 모바일 보안 표준화 추진

구분	정의	표준화 대상항목	세부표준화 항목	표준화 내용
네트워크 보안	개방형 네트워크 환경에서 전달되는 정보의 위·변조,유출,무단 침입 등을 비롯한 불법행위로부터 정보를 보호	이동통신망 보안기술	모바일 서비스 및 콘텐츠 보호	이동통신망 응용서비스와 다양한 모바일 콘텐츠 서비스를 위한 종단 간 보안 응용 인터페이스 요구사항 및 응용 가이드라인을 제시하고, 모바일 콘텐츠의 저작권 보호에 대한 표준화 추진
		무선근거리통신망 보안기술	무선랜 인증 및 접근 제어 기술	안전한 무선 근거리 통신망을 보장하기 위해서 사용자 인증 및 권한 관리를 위한 기술의 표준화를 추진
			무선랜 보안 프로파일	표준화가 진행되어 있지만 활용되지 못한 기술들을 위해서 사용자가 활용하기 쉽고 다양한 환경에 적용 가능한 보안 프로파일의 개발
			이종 네트워크로 이루어진 통합 환경에 대한 보안 기술	차후 통합 네트워크 환경에서 이기종 네트워크 간의 보안 기술 연동을 위해서 기반이 되는 기술을 개발해서 서로 다른 네트워크의 핸드오프, 로밍 환경에서도 안전한 네트워크를 보장하기 위해서 관련 기술의 표준화를 추진
			무선랜 위한 효율적인 암호 기술	제한적인 환경에서 활용 가능한 안전한 암호화 기술 개발 및 활용하기 위한 표준화를 추진
		차세대 네트워크 보안기술	차세대 네트워크 보안 구조 및 요구사항	차세대 네트워크 취약점 보호를 위한 보안 구조와 취약점에 대한 대응을 위한 보안 요구사항 등에 관련된 표준화를 추진
			사업자별 통합·분산 인증 기술	안전한 차세대 네트워크 서비스의 접근 제어를 위한 사용자 인증 기술 및 네트워크 및 서비스 사업자 간의 상호 접속을 위한 인증 연동 기술 등에 관련된 표준화를 추진
			융복합 서비스 보안 기술	차세대 네트워크에서 제공되는 융복합 서비스(예, IPTV 등)의 안정성 보장을 위한 단말기 보호 및 콘텐츠 보호 기술 등에 관련된 표준화를 추진
		사이버공격 역추적/보안 관리 기술	공격자 추적 메시지 교환 및 전달 프로토콜	네트워크의 다중 도메인 환경에서 사이버공격이 발생할 경우 침해사고에 대한 관리 도메인 내부에서의 탐지 및 추적뿐만 아니라 타 도메인과 침해사고 정보나 추적 정보를 교환하기 위한 전달 방법을 마련함
			다중 도메인 환경에서의 사이버 공격 추적 프레임워크	다중 도메인 환경에서 협력 기반의 사이버공격 추적을 수행함에 있어 프레임워크의 기본 구조, 사이버공격 추적 프레임워크를 구성하는 구성요소들, 사이버공격 추적 프레임워크의 구성요소 중의 하나인 사이버공격 추적 시스템의 세부구조, 사이버공격 추적 시스템을 구성하는 모듈들, 그리고 사이버공격 추적 시스템의 상황에 따른 여러 추적 메커니즘을 마련함
			침해사고 이벤트 공유 방법	각 관리 도메인에서 발생된 침해사고를 타 도메인에게 상호 간에 공유하기 위한 방법을 마련함
			프라이버시 보호를 위한 가이드 개발	인터넷상에서 사이버공격 및 역추적을 통해 사용자 정보 보호를 위한 프라이버시 가이드를 개발 및 마련함

구분	정의	표준화 대상항목	세부표준화 항목	표준화 내용
시스템 보안	정보통신 시스템의 안전성과 가용성을 향상시키는데 필요한 정보보호 기술 및 디지털 증거제공을 위한 기술	봇넷 대응 기술	봇넷 탐지 및 대응 프레임워크	전 세계적으로 분포된 봇넷에 대한 체계적인 탐지와 ISP 및 도메인 간 공조를 통한 봇넷 대응 프레임워크에 대한 표준화 추진
			봇넷을 이용해 발송되는 스팸 대응 기술	최근 발생하는 대부분의 스팸의 스팸 발송 수단으로 이용되는 봇넷을 통해 발송되는 스팸에 대한 대응 방안에 대한 표준화 추진
		서버보안	접근 통제 및 감사 추적 기술	PC와 서버 로그 기술, 커널기반 접근통제 기술, 보안정책 관리기술 등은 국제 표준화 기구에서 표준 작업을 추진하고 있으므로 국제 표준을 충분히 수용하고 국제 표준 인력을 양성하여 국내 기술로 활용할 수 있는 방안을 마련함. 더 나아가 이종 운영체제에 대한 서버의 보안 정책을 관리하고 통제하는 기술로 발전하여 일부 국제 표준화에 역할을 할 수 있음
			소프트웨어 무결성 검증 기술	서버 보안 및 트러스트 플랫폼 기반 소프트웨어 무결성 검증 기술, 그리고 플랫폼 임의 조작 방지 기술 등은 국제 표준화 기구에 미래 표준 기술 분야로 선행 표준 기술 연구 활동을 적극 추진하여 국제 표준 선점을 위한 국제 표준화 활동을 강화함
			보안 커널 제어 기술	현재 임베디드 시스템에 보안 모듈은 무거워서 장착을 꺼리고 있으나 하드웨어 기술이 발전에 따라 임베디드 시스템을 위한 보안 커널 기술이 필요할 수 있으므로 경량의 보안 커널과 통제 메커니즘에 대하여 국제적 표준화 활동을 할 수 있음
			애플릿 기반 보안 처리 기술	액티브엑스 위주에서 벗어나 자바 애플릿 기반의 전자상거래 및 보안 모듈을 위한 보안 처리 기술을 연구함으로써 국제적 표준화를 주도할 가능성이 있음
		PC보안	통합 PC 보안을 위한 로그 정보 교환 기술	통합 PC 보안이 요구되는 상황에서 통합관리를 위한 PC 보안 제품의 로그를 취합하고 분석, 정리할 수 있고 확장성을 고려할 수 있는 로그 형식 표준화 및 로그 정보 교환 기술 표준화 추진 필요
			통합 관리를 위한 공통 API 기술	통합관리를 위한 PC 보안 제품의 로그 및 환경설정, 개별 기능 컨트롤 등 공통적으로 적용할 수 있는 API 기술 표준화 추진 필요
		디지털 포렌식	컴퓨터 및 휴대폰 포렌식 가이드라인	컴퓨터, 휴대폰과 같은 정보기기 장치에 내장된 디지털 자료를 근거로 삼아 그 장치를 매개체로 발생한 어떤 행위의 사실 관계를 규명하고 증명하고자 함에 있어 법정에서 그 증거력을 인정받기 위해서는 논리적이고 체계화된 분석 절차에 따라야함. 국내 환경 및 디지털 데이터의 특성을 반영한 디지털 증거 분석 절차에 대한 표준화 추진
			디지털 데이터 수집도구 및 분석 도구 요구 사항 및 검증 규격	디지털포렌식 도구는 그 목적이 법정에서 사용될 수 있을만한 신뢰성 있는 증거자료를 도출하는 것이므로 일반적인 응용 프로그램과 달리 신뢰할 수 있는 프로그램인지에 대한 검증이 필요함. 포렌식 도구에 대한 적합성 시험 방법 및 절차에 대한 표준화를 추진
			디지털 데이터 공통 교환 포맷	디지털 데이터의 특성상 원격지에서 수집될 수 있는 디지털 증거의 확보를 위해 기관 간 및 국가 간 수사공조가 요구될 수 있으므로 수집된 증거 파일을 교환할 수 있는 공통 교환 포맷 표준화를 추진
			프라이버시 보호를 위한 가이드 개발	정보기기 장치 및 인터넷에 저장된 개인 정보 보호를 위한 프라이버시 가이드를 개발 및 마련함

1.1.2. 연관기술 분석

○ 연관기술 관계도



○ 연관기술 분석표

연관기술	내 용	표준화 기구/단체		표준화 수준		기술개발 수준	
		국내	국외	국내	국외	국내	국외
USN 보안기술	USN 네트워크의 안전 · 신뢰성을 보장하는 인프라 보호기술	TTA 기술 표준원	IEEE ITU-T	표준기획	표준화 항목승인	설계	시제품/ 프로토타입
휴대인터넷 보안기술	안전한 휴대인터넷 서비스를 위한 기밀성, 무결성 등의 보안기술	TTA 휴대 인터넷포럼	IEEE ITU	표준화 항목승인	표준화 항목승인	시제품/ 프로토타입	시제품/ 프로토타입
홈네트워크 보안기술	홈네트워크의 안전성을 확보하기 위해 편의성이 강화되고 경량화된 정보보호기술	TTA HSNF	ITU	일부표준 제정 일부표준 기획	일부표준 제/개정 일부표준 개발/검토	시제품/ 프로토타입	시제품/ 프로토타입
이동통신망 보안기술	3G, 4G 등의 안전한 이동통신망 서비스를 위한 보안기술	TTA	3GPP 3GPP2	표준안 검토	표준안 검토	설계	설계
무선근거리통신망 보안기술	AP가 설치된 곳의 일정거리 안에서 무선 인터넷을 할 수 있는 근거리 통신망의 보안기술	TTA	IEEE	표준안 개발/검토	표준안 개발/검토	구현	구현
	IEEE 802.11-무선랜 정의	TTA	IEEE	재정	재정	상용화	상용화
	IEEE 802.11i-무선랜 보안기술 정의	TTA	IEEE	재정	재정	상용화	상용화
	IEEE 802.11r-핸드오버 시 보안기능 지원	TTA	IEEE	표준기획	표준안 개발/검토	기술기획	설계

연관기술	내 용	표준화 기구/단체		표준화 수준		기술개발 수준	
		국내	국외	국내	국외	국내	국외
무선근거리통신망 보안기술	IEEE 802.11w-관리프레임 취약점 보완	TTA	IEEE	표준기획	표준안 개발/검토	기술기획	기술기획
차세대 네트워크 보안기술	통신 방송 등 각종 서비스 영역을 통합한 멀티미디어 서비스를 시간과 장소에 구애받지 않고 이용할 수 있는 통합 차세대 네트워크에서의 안전성 강화를 위해 요구되는 기술	TTA	ITU-T IETF	표준안 개발/검토	표준안 개발/검토	설계	설계
사이버공격 역추적/보안관리기술	침입 차단 시스템, 침입 탐지 시스템, 가상 사설망 시스템 등 다양한 종류의 보안 시스템들을 상호 연동하여 각 기능을 통합 관리하며, 네트워크 차원의 보안 상황 분석, 추적, 그리고 대응하는 중앙집중식 관리와 사이버 공격 역추적 기능을 제공 하는 기술	TTA ISTF	ITU-T IETF ISO	표준제정 (보안관리) 표준안 개발/검토 (역추적)	표준제정 (보안관리) 표준안 개발/검토 (역추적)	프로토타입 (역추적)/ 일부상용화 (보안관리)	프로토타입 (역추적)/ 일부상용화 (보안관리)
봇넷 대응기술	다양한 공격의 수단으로 사용되는 봇넷에 대한 대응기술	TTA	ITU-T	표준화 항목승인	표준화 항목승인		
서버 보안	서버 보안은 접근통제 및 감사추적 기술, 트러스트 플랫폼 기반 소프트웨어 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	표준 제/개정	시제품/ 프로토타입	시제품/ 프로토타입
PC 보안	안티바이러스 기술 및 키보드 보안 기술, 내부정보 유출방지 등과 같은 개인용 PC환경에서 개인의 정보를 보호하는 기술	TTA	IEEE ITU-T	표준안 기획	–	설계	기술 일부 적용
디지털포렌식	사이버 범죄 방지 및 수사를 위한 시스템 및 네트워크 기반의 디지털 데이터 수집, 복구 및 분석 기술	TTA	ITU-T ISO NIST	표준화 항목승인	표준화 항목승인	설계	구현

1.2. 추진경과 및 중점 추진방향

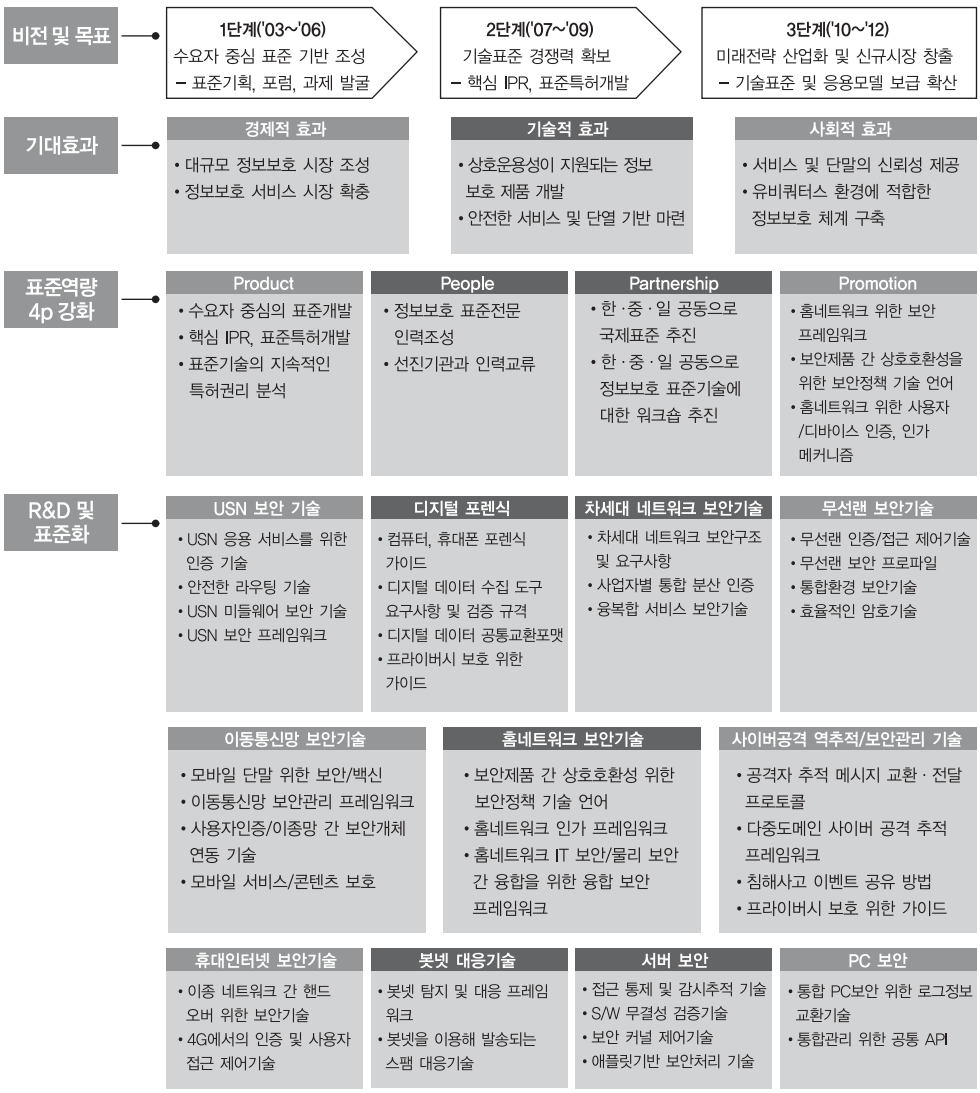
○ 추진경과

- Ver. 2006에는 정보보호 분야의 표준화가 TTA(한국정보통신기술협회)를 통하여 수행되지 않고 한국정보보호진흥원을 통하여 수행되었음
- Ver. 2007에는 정부의 추진 의지가 강한 VoIP 분야를 포함한 응용 서비스 정보보호분야와, 최근 ITU-T와 IETF 등의 국제 표준화 기구에서 활발하게 국제 표준화가 추진 중인 네트워크 정보보호 분야를 중점적으로 정리함
- Ver. 2008에는 네트워크 및 시스템 보안 분야로 정보보호 분야를 세분화하고, 네트워크 분야를 USN 보안 기술, 휴대인터넷 보안기술, 이동통신망 보안기술, 홈네트워크 보안기술, 무선근거리통신망 보안기술, 차세대네트워크 보안기술, 통합보안관리 기술 등으로 분류하여 정리하였고, 시스템 보안 분야는 기존의 서버 보안과 PC 보안 및 디지털포렌식을 정리함
- Ver. 2009에는 Ver. 2008의 네트워크 보안 및 시스템 보안 기술 분류에서 통합보안관리 기술을 사이버 공격 역추적 및 보안관리기술로 변경하여 사이버 공격 역추적 표준화를 강화하고, 봇넷 대응 기술을 신규로 포함하였음

○ 중점 추진방향

- Ver. 2008에는 위와 같이 10 가지로 세분화한 보안 기술 분야 중에서 휴대 인터넷 보안, 홈네트워크 보안 부분을 중점적으로 표준화를 추진하였고, Ver. 2009에는 홈네트워크 보안 기술 및 휴대 인터넷 보안 기술과 통합관리 부분에서는 사이버 공격에 대한 역추적 기술 및 봇넷 대응 기술 등을 포함하여 중점적으로 표준화를 추진하였음
- 중점 표준화 항목은 정부의 정책 주친 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 시스템 보안 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 네트워크 및 시스템 분야의 상호 운용성을 제고하기 위한 정보보호 제품에 대한 표준화 부재는 안전한 전자 정부와 유비쿼터스 사회로의 구현을 위한 커다란 장애

○ 네트워크 및 시스템 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, 네트워크 및 시스템 측면에서 가용성 보장 및 신뢰성 확보가 필수적으로 요구됨

○ 따라서 네트워크 및 시스템 분야의 정보보호 기술은 일반적인 정보보호 기실의 안전성과 신뢰성을 향상시키고, 지식 기반 전자정부의 유용성을 증대시킬 수 있음

○ 또한, 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

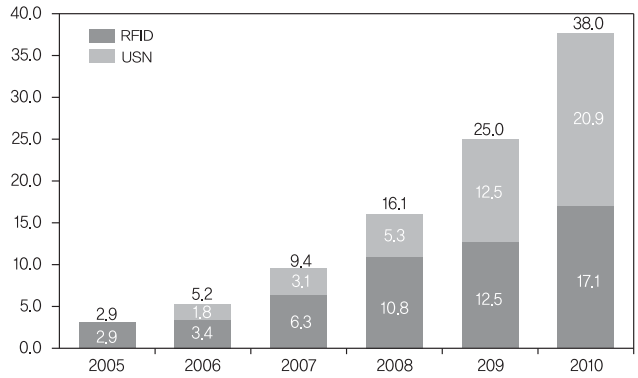
2.1.1. 국내 시장 현황 및 전망

○ USN 보안

- 2010년도에는 국내 3백만 개에서 4백만 개 정도의 시장을 형성할 것으로 예측되며, 이는 USN을 이용한 센서네트워크 활용 시장규모가 매년 150% 이상의 성장률을 기록할 것으로 예상되는 수치임
- 2012년도에는 USN과 4G 등과의 연동을 통한 시너지 효과를 고려하면 센서노드 만으로도 시장규모는 20억 달러 이상의 시장을 형성할 것으로 예측 됨

○ 휴대인터넷 보안

- 2006년 6월 세계 최초로 와이브로 서비스가 우리나라에서 KT, SKT에 의해 상용 서비스됨
- KT
  - 2008년 2분기 기준으로 가입자 수 20만 명을 확보하였으며, 2010년까지 약 400만 명의 가입자 확보를 계획하고 있음
  - 2008년 5월에 서울지역 인빌딩 커버리지 구축을 완료하였고, 2008년 10월 수도권 19개 도시로 커버리지를 확대할 예정이며 2008년 말까지는 84개 도시로 서비스 영역을 확대할 계획에 있음



국내 RFID/USN 시장동향[1)]

(단위: 억 US$)

1) ETRI(한국전자통신연구원)/IDTech/VDC

- 4대 신규 서비스 중 하나로 와이브로를 선정하여 그간 주춤했던 와이브로 관련 설비투자를 2007년 말부터 재개함과 동시에, 국내시장 확대 및 해외시장 개척에 집중할 것으로 전망
- 와이브로 경쟁력 강화를 위해 스마트폰, 모바일 PC, USB 모뎀 등 기존 8종에서 총 17종으로 다양한 형태의 와이브로 단말기 라인업을 늘려 나갈 예정
- 와이브로 확대를 위해 노트북 대여 서비스 및 UICC 개발, 타 사업 영역과 연계한 공동마케팅 등을 추진 중으로 이용률 향상을 위해 영상통화서비스 및 VoIP 등의 부가서비스도 도입 예정

– SKT

- KT보다 상대적으로 와이브로에 대한 투자 및 마케팅 비용을 적게 투입하는 등 와이브로 시장 참여에 소극적이며 2008년 6월 말 기준 가입자 수는 2,000명 정도
- SKT가 시장참여에 소극적인 이유는 절대적인 우위를 차지하고 있는 기존 이동통신 서비스(시장 점유율 50% 이상)에 대해서 와이브로가 경쟁자로 작용할 가능성이 크기 때문
- 2007년 11월, 와이브로 서비스의 경쟁력과 마케팅을 강화하기 위한 전담 조직을 신설하고 커버리지 확대 및 신규 가입 유치 프로모션을 펼치는 등 본격적인 사업 확대 계획
- 서울, 수도권, 광역시 등 23개 도시에 설치되어 있는 56개 핫존(hot zone)을 2009년까지 지방 도청 소재지 등 42개 시 100여 개로 확대할 예정

– 2008년부터 현재 시스템(wave 1)보다 넓은 대역폭과 대용량 전송이 가능한 향상된 와이브로 시스템(wave 2)으로 업그레이드가 예정되어 있어 보다 빠른 데이터 전송속도를 가지는 서비스 제공 예정

– 2007년 10월 와이브로의 3G 이동통신 IMT-2000 기술표준 채택에 따라 기존의 무선인터넷 접속위주의 서비스뿐만 아니라 인터넷 전화를 통한 음성서비스 제공도 가능할 것으로 예상됨

– 2011년 와이브로 가입자는 500만에 달하고, 3G 이동통신 가입자가 1,500만 명에 이를 것으로 예측

– IT 시장조사업체 한국 IDC는 "HSDPA와 와이브로 서비스 시장 분석 및 전망 보고서"에서 HSDPA/HSUPA가 올해 전체 이동통신 가입자 중 7.4%를 차지하고 2011년에는 1,492만 명에 달해 전체 이동통신 가입자의 32.6%에 달할 것으로 전망했으며, 와이브로 역시 올해 0.2%에서 2011년 38.8%로 크게 높아질 것으로 예상

– HSDPA/HSUPA와 와이브로는 각각 독립적인 서비스로 서로 경쟁하기보다는 상호 보완적 관계에서 다양한 결합 서비스 형태로 제공될 것으로 예측

– 또한, 정부는 2010년까지 국내 와이브로 시장 규모를 8조 1000억 원, 장비 시장규모를 5조 8000억, 세계 시장 규모를 24조 원으로 추정했으며, 와이브로 상용화에 따라 6년간 24조 7000억 원의 생산 유발 효과와 12조 원의 부가가치 창출 효과, 27만 명에 이르는 고용 창출이 가능할 것으로 예상[2)]

– 와이브로의 기존 초고속인터넷 서비스 대체 수요는 2015년까지 140만 명에 이를 것으로 추정

2) 방송통신위원회(舊 정보통신부), IT전략 시장전망, 2007.5.31

○ 홈네트워크 보안

- 지능형 홈네트워크 국내 시장규모는 2008년에 10조 2천억 원 규모가 될 것으로 전망되며, 향후 연평균 7.1% 씩 성장하여 2010년에는 11조 2천억 원 규모로 성장할 것으로 전망됨
- 홈네트워크의 활성화 지연 및 보안제품에 대한 인식미비로 현재 구체적인 홈네트워크 보안시장은 형성되지 않고 있으나, 네트워크 시스템 및 서비스 시장 대비 네트워크 보안 시장간 비율을 반영하면 향후 홈네트워크 활성화가 이루어질 경우 홈네트워크 시장의 3% 규모의 홈네트워크 보안 시장이 형성될 것으로 예상됨
- 2010년 홈네트워크 장비 시장 중 정보 가전 시장 비중이 국내 시장의 66%로 가장 큰 부분을 차지할 것으로 전망되면서 가정 내 IT 인프라가 보편화될 것임
- 홈네트워크 서비스가 홈오토메이션 중심에서 홈엔터테인먼트 중심으로 진화되면서 인터넷 접속과 다양한 엔터테인먼트 서비스를 융합하여 제공하는 차세대 홈서버 시장이 빠르게 형성될 것으로 전망됨
- 국내의 경우, 정부 주도하에 적극적인 홈네트워크 활성화 정책을 추진하고 있으나 킬러 서비스의 부재로 실질적인 시장 활성화가 지연되고 있음. 현재 지경부에서는 홈네트워크 산업의 재도약을 위해 적극적인 산업 활성화정책을 계획하고 있으므로 향후 시장 활성화시 새로운 홈네트워크 보안시장의 창출이 예상됨

지능형 홈네트워크 국내 시장[3)]

구분	2004	2005	2006	2007	2008	2009	2010	CAGR '05–'10
홈플랫폼	345	615	954	1,509	2,085	2,505	2,922	36.6%
유무선 홈네트워크	253	206	197	184	195	192	215	0.9%
정보가전	5,516	7,008	8,605	8,180	7,615	7,128	7,444	1.2%
유비쿼터스 컴퓨팅	86	123	170	239	341	475	647	39.4%
총계	6,200	7,952	9,926	10,112	10,236	10,300	11,228	7.1%

지능형 홈네트워크 국내 시장

(단위: 명)[4)]

구분	2007. 11월 말	2007. 12월 말	점유율(12월)
SKT	21,816,140	21,968,169	50.5%
KTF	13,632,228	13,720,734	31.5%
LGT	7,748,249	7,808,638	18.0%
합계	43,196,617	43,497,541	100.0%

3) 2005 In-Stat, 2005 Gartner, 2005 VDC

4) 방송통신위원회(舊 정보통신부), 2007

○ 이동통신망 보안

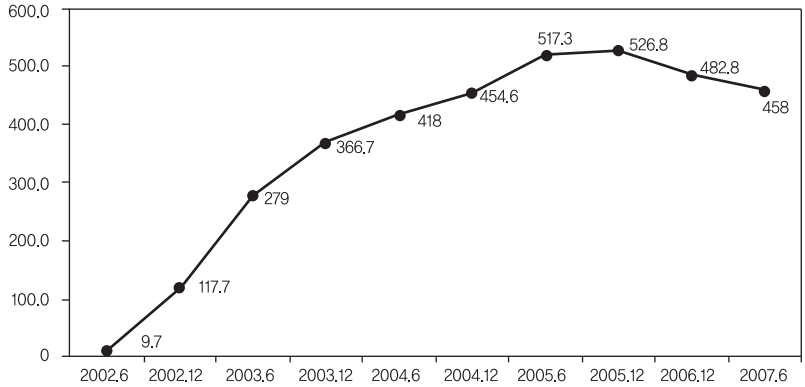
- 이동통신망 보안에 해당하는 솔루션 영역은 크게 이동통신 단말 보안, 이동통신망 사용자 인증 및 이종망간 연동보안, 서비스 및 콘텐츠 보호를 들 수 있음
- 지난 몇 년간 이동통신 단말 시장은 급격하게 변화되었으며, 성숙기를 지나 교체 수요 시장으로 변경됨
- 현재, 국내 이동통신 가입자는 4400만 명에 육박하며 약 90%의 보급률을 보이고 있음
- 최근, 국내 이동통신 단말 휴대폰 판매량은 2008년 계속해서 200만대를 돌파했지만, 연속 하락세를 보이고 있으며, 국내 수요의 경우 대부분이 고가 폰으로의 교체 수요에 해당되며, 이와 같은 국내 판매량이 하락세를 보이는 이유는 이동통신사들의 보조금 축소가 주요 원인으로 보이며, 과열경쟁이 진정되면서 판매량 감소세는 지속될 것으로 예상됨
- 모바일 단말의 보안 시장은 USIM, 모바일 백신 등으로 추정될 수 있으며 최근 모바일 악성코드의 위협으로 앞으로 모바일 백신 시장이 확대될 전망임
- 이동통신망 사용자 인증 및 이종망 간 연동 보안시장은 기존의 AAA 시장에서 IMS 기반 HSS 장비 시장으로 변화되어 성장률이 눈에 띄게 줄어 듦
- 그러나 이동통신환경에서 보안 서비스 및 콘텐츠 보호 시장은 국내의 지상파 DMB 폰, 애플의 I-Phone, 구글의 Android, 노키아의 Windows Mobile 등이 관심을 끌면서 모바일 인터넷 및 위치기반서비스 기술로 진화해가고 있어서 앞으로의 시장은 고성장이 예견되고 있음

○ 무선근거리통신망 보안

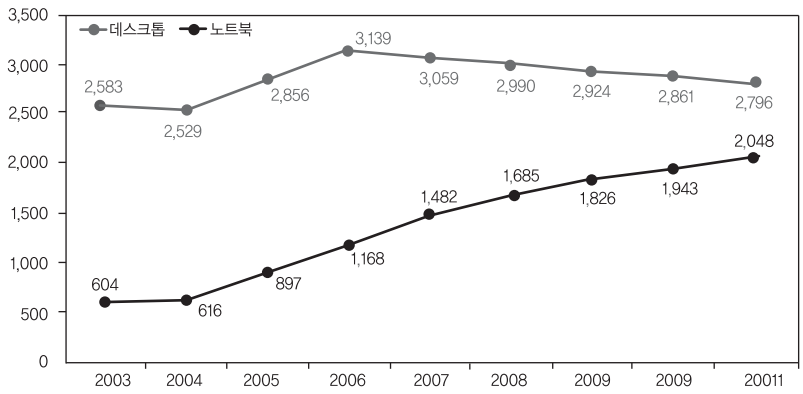
- 2000년대 이후 이동통신, 초고속인터넷으로 양분되어 성숙기 단계에 접어들었던 국내 통신 서비스 시장에서 신규 사업으로 추진되었던 무선랜 서비스는 최초 기대에 만족하지 못하는 상태에서 정체 상태에 직면한 상황으로, 현재는 광대역 휴대 인터넷이라는 서비스의 등장으로 경쟁 상태에 빠져있음
- 시장 상태는 불투명하지만 일반 가정과 기업 사무로 구분되어 독립적인 시장이 구축되어 있고, 최근 대역폭 변경 및 서비스 품질 강화, 전송속도 강화를 추구한 새로운 기술 표준이 제안되면서 새로운 전환기를 맞고 있음
- 차세대 무선랜 기술 규격으로 평가 받고 있는 802.11n은 올해 본격적인 성장세를 맞을 것으로 예상되나 아직 표준화가 완료되지 않은데다 네트워크 인프라 구축이 미흡해 시장 확대에 어려움을 겪고 있음
- 국내의 경우 2.4GHz 대역을 이용한 공중 무선랜 서비스인 KT 네스팟이 중심적인 역할을 수행하고 있음. 2002년 2월 KT와 하나로텔레콤에 의해서 서비스가 시작된 이후, 2007년 6월말 기준 645만 명의 가입자가 이용 중임. 전국 주요도시를 중심으로 IEEE 802.1x 표준 장비를 이용한 16,000개의 핫스팟이 구축되어 있음
- 무선랜 장비 시장은 초기 중소기업들이 유선랜을 무선으로 대체하게 된 대체수요와 의료, 제조, 유통, 학교 등 전통적인 수직 애플리케이션 분야에서 시장창출이 일어났으나, 2005년을 기준으로 일반 가정의 홈네트워킹 수요가 급증하고 공공구역에 대한 핫스팟의 증가와 더불어 기업들의 대대적인 핫스팟 설치에 힘입어 전체 시장이 성장하고 있음

– 2008년 후반기 IPTV와 VoIP의 대대적인 도입으로 관련 기술과 장비들에 관심이 모아지고 있으며 사용자의 기대에 만족시키기 위해서는 상응하는 인프라를 갖추어야 하기 때문에 시장에 대한 기대가 높음. 일례로 지난해 400만대에 달했던 국내 무선랜 공유기 관련 시장은 저가 노트북, 인터넷전화기, IPTV 등의 확산에 따라 올해 500만대를 넘을 것으로 전망

– 이번 년도는 대형 무선랜 사업이 본격화 되는 시기로 도로 공사가 실시간 도로 정보 수집을 위해 전국의 고속도로에 무선랜을 구축하는 사업을 시작했음. 대기업 계열사들이 무선랜 구축에 나서고 있는 등 무선랜의 안정성과 보안 등에 부정적이었던 인식이 바뀌고 있어 하반기가 더욱 시장 활성화가 기대됨



KT 네스팟 가입자 수[5]

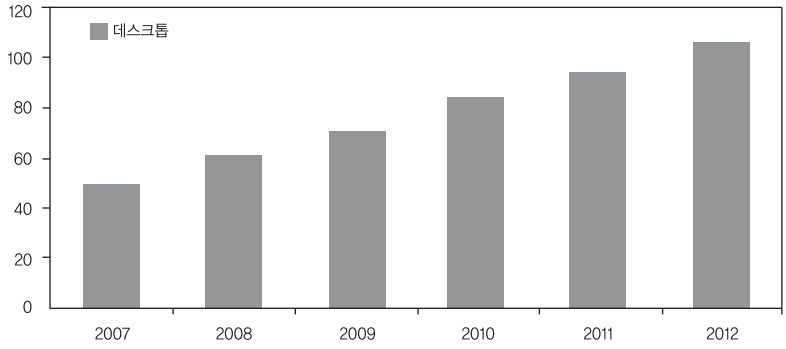


노트북 PC시장 규모

(단위: 천 대, °은 전망)[6]

5) IITA, 2007.09

6) 한국 IDC, 한국일보 2007.10.25



국내 무선랜 장비시장

(단위: 십억 원)[7]

- 2008년도에 주목 받은 사안은 국방 BcN[8] 구축사업임. 지난해 연말부터 시작된 국방 BcN 구축사업은 열악한 야전부대의 정보통신 인프라를 개선하고 네트워크 중심전 등 미래 전에 대비할 수 있도록 초고속 · 대용량 국방 BcN을 임대형 민자 사업 방식으로 구축하는 것임. 현재 임대형 민자 사업 참가 업체들이 모두 기준을 통과하지 못한 것으로 결론이 났고, 최근 다시 진행했으나 아직 사업의 향배가 어떻게 될지는 불투명한 상황이지만 국가적인 프로젝트가 진행되고 있다는 점에서 실질적인 예로 들 수 있음
- 무선랜과 직접적으로 관련이 있는 노트북 PC 시장의 경우 전체적인 PC 시장이 정체기에 접어들었음에도 불구하고 기술개선 및 사용자의 요구에 맞는 폼팩터 제품 출시 비중이 높아지고 있으며 대부분의 노트북 PC들은 무선 통신의 단말로 활용되고 있음
- 무선랜 장비시장은 802.11a/b/g 통합 모듈이 탑재된 액세스 포인트와 컨트롤러의 확산, 기업 시장과 소호 부문에서의 장비 도입에 따라 2007년 약 518억 원 규모로, 전년도 437억 원 보다 18.5% 증가한 추세를 보임. 한국 IDC는 전망 기간 동안 무선랜 시장은 메시 네트워크의 성장과 802.11n 지원 장비의 출시에 따라 향후 5년간 연평균 15.4%로 성장, 2012년에는 1천억 원을 상회하는 규모로 성장할 것으로 예상함

7) 출처: IDC, 2008

8) Broadband Convergence Network, 광대역통합망

국가별 무선랜 이용 순위[9]

	2H07 SESSIONS	SESSION LENGTH (MIN)	% OF WORLDWIDE TOTAL	2H06 SESSIONS	ANNUAL GROWTH FROM 2H06
미국	1,109,468	88	51%	692,232	60%
영국	291,325	86	13%	131,546	121%
독일	217,706	90	10%	63,496	243%
스위스	83,282	76	4%	37,443	122%
네덜란드	74,827	82	3%	36,342	106%
프랑스	68,978	70	3%	20,712	233%
일본	50,785	53	2%	33,887	50%
호주	35,778	90	2%	12,346	190%
벨기에	22,764	102	1%	9,608	137%
브라질	22,363	47	1%	6,226	259%

PC 시장 규모

(단위: 천 대, *은 전망)[10]

구분	2003	2004	2005	2006	2007	2008*	2009*	2010*	2011*
데스크톱	2,583	2,529	2,856	3,139	3,310	2,990	2,924	2,861	2,796
노트북	604	616	897	1,168	1,482	1,685	1,826	1,943	2,048

○ 차세대 네트워크 보안

– Firewall/VPN 보안시장 현황

• 국내 업체는 상위 3사(시큐아이닷컴, 어울림정보기술, 퓨쳐시스템즈)가 대다수의 시장을 차지하고 있으며, 초기 설비투자비용으로 진입장벽이 존재하는 것으로 판단됨

• Firewall 분야는 점차 고성능화 되어 가고 있으며, 시장 흐름에 따라서 점차 UTM[11]으로 전환 예상되고 있음

– IDS/IPS 보안시장 현황

• IDS 제품으로는 윈스테크넷의 Sniper IDS, 인젠의 Neowatcher, 펜타시큐리티의 Siren 등이 있음

• LG 엔시스는 중소기업 시장을 위한 네트워크 통합보안제품인 세이프 IPS-U를 출시함. 세이프 IPS- U는 IDS, IPS, 방화벽, 안티바이러스, 안티스팸, 웹 콘텐츠 필터링 등 복합 기능을 통합 지원함

– UTM 보안시장 현황

• LG 엔시스의 네트워크 통합보안제품인 세이프 IPS-U는 기존의 IDS[12] 및 IPS[13] 기능에서부터 방화벽, 안

9) USA iPass의 전화 조사 결과

10) 한국 IDC, 한국일보 2007.10.12

11) Unified Threat Management, 통합보안관리

12) Intrusion Detection Service, 침입탐지시스템

13) Intrusion Prevention Service, 침입방지시스템

티바이러스, 안티스팸, 웹콘텐츠 필터링 기능을 한대의 장비로 지원

- 어울림정보기술에서 UTM을 준비 중으로 향후 UTM 시장에 참여하는 기업이 늘어날 것으로 전망됨

○ 사이버공격 역추적/보안관리

– 사이버공격 역추적 관련 분야와 TMS[14], ESM[15], PMS[16], 로그관리 및 분석 도구, 취약점 분석도구 등을 포함하는 보안관리 분야는 보안 컨설팅 분야의 약진 및 정책적 보안관리 인식 강화 등에 힘입어 향후에도 꾸준히 팽창할 것으로 기대되는 분야임[17]

- 2007년도의 매출규모는 65,226백만 원에서 기존에 설치된 제품들의 꾸준한 업그레이드 및 패치사업이 계속되고 공공기관을 중심으로 대규모 프로젝트가 예상되어 보안관리 시장의 향후 매출전망은 상승세를 이어나갈 것으로 보이며, 2012년에는 그 규모가 103,315백만 원에 이를 것으로 전망됨

– 통합보안 관리 툴, 로그분석, 및 취약점 분석에 대한 툴 등을 포함하는 보안관리 소프트웨어 분야는 보안컨설팅분야의 약진 및 정책적 보안관리 인식 강화 등에 힘입어 향후에도 꾸준히 팽창할 것으로 기대되는 분야임

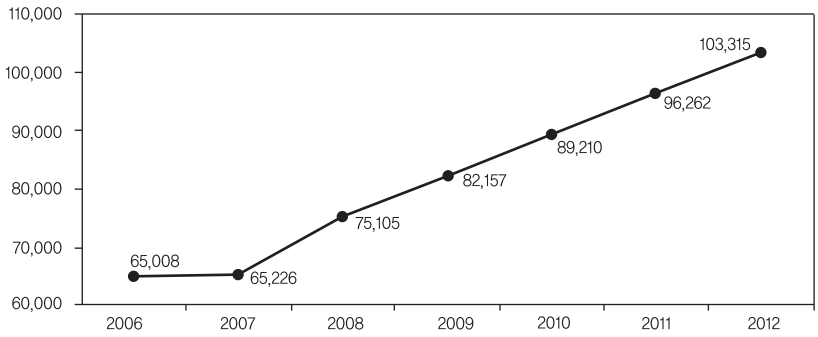
- 최근 기업들은 전사적인 인프라 구축 및 통합 작업과 연계하여 보안 솔루션을 도입하고 있는 추세이며, 보안 서비스에 대한 관심으로 이어지면서 ESM 솔루션 수요와 함께 통합 인프라 관리 및 보안 관제 서비스 시장이 동반 확대되고 있는 추세를 반영한다면 매출이 지속적인 증가 전망
- TMS는 네트워크 취약점, 악성코드 등을 탐지하여 적절한 대응에 필요한 의사결정을 지원하는 시스템으로 향후 공공기관을 중심으로 매출신장이 이루어질 것으로 전망이며, 다만 여러 가지 보안관리 도구 틈에서 아직 자리를 잡지 못한 상황을 감안하면 매출액 규모는 크지 않을 것으로 예상되는 성장세는 빠르게 이루어질 전망
- PMS는 일반 보안관리 도구나 백신 시장에 비해 그 필요성에 대한 인식이나 수요처가 한정되어 있다는 것도 시장규모가 확산되는 것을 저해하는 원인이 될 수 있지만, 웜이나 바이러스에 항상 노출되어 있는 일반 PC를 기준으로 패치에 대한 중요성의 인식이 확산된다면 향후 시장규모는 크게 성장할 것으로 예상
- 로그 관리 및 분석 도구는 다양한 디지털범죄가 날로 증가되고 광범위 화되면서 사전예방 못지않게 꾸준한 상승이 기대되며, 공공기관은 물론 일반 기업에서도 수요는 꾸준히 늘어날 전망
- 취약점 분석 도구는 정보통신기반보호법 시행으로 주요 정보통신 시설에 대한 안전진단이 의무화되면서 많은 보안 제품들은 도입해 활용했던 공공기관과 금융, 기업들이 보안수준을 파악하고 이에 대한 대책을 제시해 주는 보안 취약점 분석 도구를 도입하기 위해 예산을 편성하는 열기에 힘입어 시장규모는 크지 않아도 꾸준한 상승세를 보일 것으로 전망

14) Threat Management System, 위협 관리 시스템

15) Enterprise Security Management

16) Patch Management System

17) 2007년 국내 정보보호산업 시장 및 동향 조사, KISA(한국정보보호진흥원)



보안관리의 매출 전망

보안관리 분야별의 매출 전망

(단위: 백만 원)

구분	2006년	2007년	2008년	2009년	2010년	2011년	2012년	CAGR(%)
ESM	29,114	30,002	32,841	35,192	37,543	39,884	42,245	6.4
TMS	14,008	13,016	15,424	16,982	18,540	20,098	21,656	7.5
PMS	8,121	11,410	13,055	14,699	16,344	17,988	19,633	15.8
로그관리분석 툴	10,861	8,056	10,195	11,098	12,001	12,904	13,807	4.1
취약점분석 툴	2,904	2,742	3,590	4,186	4,782	5,378	5,974	12.8
합계	65,008	65,226	75,105	82,157	89,210	96,262	103,315	8.0

국내 정보보호 시장 전망

(단위: 백만 원)

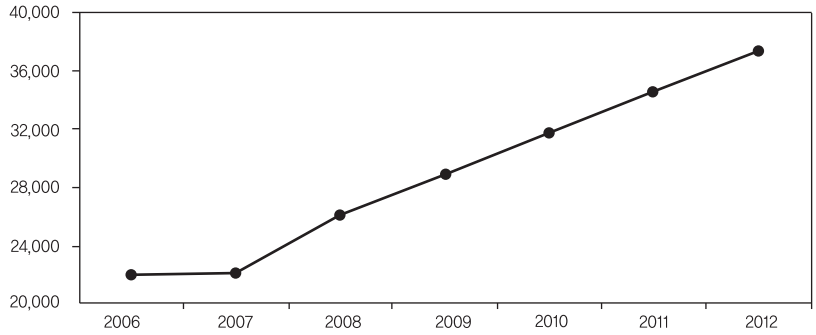
구분	2005	2006	2007	2008	2009	2010	2011	CAGR(%)
시스템 및 네트워크 정보보호 제품	583,423	625,182	713,689	790,940	864,482	935,633	1,005,495	9.50
정보보호서비스	97,282	109,610	123,053	136,495	149,938	163,380	176,823	10.47
합계	680,705	734,792	836,742	927,435	1,014,420	1,099,013	1,182,318	9.64

– 향후 ESM 제품의 주요 요소기술로는 취약점관리시스템과 실시간 상관관계 분석 기능이 연계되는 제품이 주요 이슈가 될 전망되면서 제품 간 · 출시업체 간 연동성을 제고하는 시장이 형성될 것으로 추정

- 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[18]

- 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 이상 상황에 따른 거시적 관점의 사이버 공격 감시 기술은 시각화 및 지능형 에이전트와 같이 매우 높은 수준이지만, 세부적 관점의 사이버공격 감시는 개척 단계로서 기술혁신 상태의 제품이 출현할 것으로 예상됨
- 또한 사이버공격 역추적 기술은 현재 각 자사제품위주의 사이트 운영을 통해 제한적이고 수동적인 역추적 기능을 제공하거나 또는 특정 응용 포트에 국한하여 각 응용 서비스 추적 제품을 개발하여 적용하고 있는 단계이나, 향후 주요 능동적인 대응을 위한 제품 기능으로 도입될 것으로 전망됨
  - 전자금융거래법에 따른 각 금융기관의 웹 기반의 금융 트랜잭션에 대한 보호 및 입증을 위해 웹 기반의 역추적 기술은 일부 시장 개척단계로 초기 상태의 제품이 출현하였으며, 보다 강력한 역추적 기술이 출현할 것으로 예상됨
  - 금융기관 및 해외 진출 기업을 중심으로 IT 거버넌스 및 리스크 관리를 위해 준수해야할 보안 관리 요건이 늘면서 보안 정책 관리 및 컴플라이언스 관리에 대한 예산을 확대
  - 핵심 기술 유출 및 영업기밀 유출을 통한 피해를 사전에 예방하기 위해 전사적인 보안 관리 체계를 고도화하고 있는 추세이며, 보안 감사 및 전자적 증거개시(e-Discovery)를 위한 사이버 포렌식 등의 사후 대응 방안에 대한 관심이 증대



보안 운영체제의 매출 전망

(단위: 백만 원)

18) 디지털 데일리(2005.12)

○ 봇넷 대응

– 국내 봇넷 침입 탐지 및 대응 기술 또한 연구 초기 단계로 아직 시장이 형성되지 않았기 때문에, 정보보호 제품 시장 규모를 참고하여 2005년 6,807억 원 규모에서 2011년에는 1조 1,821억 원 규모에 이를 전망이며 연평균 9.64%의 성장률을 보일 것으로 예측

○ 서버 보안

– 서버 보안(보안운영체제) 분야의 시장규모는 2007년도 매출액 221억 원으로 전년도와 크게 변화가 없으나 문제점 보안과 제품 인증으로 2008년 이후부터는 연평균성장률이 9.3%로 2012년 377억 원까지 이를 것으로 전망하고 있음[19)]

– 새로운 기술보다는 기존 기술을 개량하여 접근 제어 메커니즘의 제한을 극복하는 등의 방안을 고려하는 서버 보안 솔루션이나 키 관리와 소프트웨어 무결성 확인을 위한 트러스트 플랫폼용 운영체제에 대한 요구가 증가할 것으로 예상됨

○ PC 보안

– PC 보안에 해당하는 솔루션 영역은 안티바이러스(안티스파이웨어), 개인방화벽/침입탐지, 내부정보 유출방지(통합PC 보안), 패치관리, 유해정보차단, 데이터복구 등을 들 수 있음. 2007년 시장조사를 보면 PC 보안 관련 제품 또는 서비스의 연평균 성장률이 10%근처로 예상되었지만 2008년 시장자료는 그 수치가 많이 떨어져 5%대이며 안티바이러스나 PC 방화벽 시장은 2.3%, 3.0%로 예상될 정도로 시장 자체의 성장률이 눈에 띄게 줄어들었음

– 이중 안티바이러스 시장은 개인방화벽/침입탐지를 포함한 인터넷 보안 제품으로 진화해나가고 있고, 이에 대한 전문 시장조사기관의 시장 전망 자료가 존재하고 있으나 내부정보 유출방지(통합 PC 보안), 유해정보차단, 데이터복구 시장 등은 아직 그 규모가 미미하여 신빙성 있는 기관의 보고가 이루어지고 있지 않아 안티바이러스 시장의 현황 및 전망을 중심으로 기술함

19) KISIA, 2007년 11월

서버 보안 관련 제품의 매출 전망[20]

(단위: 백만 원)

구분	2006년	2007년	2008년	2009년	2010년	2011년	2012년	CAGR(%)
보안운영체제 (Secure OS)	22,121	22,143	26,031	28,953	31,874	34,796	37,717	9.3
방화벽	69,185	70,538	77,751	83,461	89,171	94,881	100,591	6.4
IPS	72,830	73,767	83,966	91,850	99,733	107,617	115,500	8.0
로그 관리/분석 툴	10,861	8,056	10,1951	1,098	12,001	12,904	13,807	4.1
취약점 분석 툴	2,904	2,742	3,590	4,186	4,782	5,378	5,974	12.8
DB 보안	16,512	15,124	19,823	23,000	26,177	29,354	32,531	12.0

○ 안티바이러스 시장 현황 및 전망

- 2007년부터 논의가 되었던 무료 백신과 대형 IT 기업의 시장 진입으로 인해 2008년의 안티바이러스 시장은 새로운 변화가 있을 것으로 예상되나 악성코드는 불행하게도 더욱 지능화, 고도화 되어가고 있고 그 수가 기하급수적으로 증가하고 있음
- 각종 웜 및 바이러스, 트로이목마와 더불어 다양한 스파이웨어 및 애드웨어로 인한 위협이 증가하고 있어서 안티바이러스 시장에 대한 수요가 갑자기 줄어들지는 않을 것으로 예상됨. 안티스파이웨어 시장과 합쳤을 경우 2006년도에 720억 원, 2007년도 751억 원 크기의 시장을 만들고 있고, 약 4.3%의 성장률이지만 무료 백신의 등장으로 개인시장은 2008년도에 더 많은 타격을 받을 것으로 예상됨

○ 안티바이러스 시장은 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 상황으로 최근 개인 사용자용 무료 백신의 등장으로 유료 개인 시장이 급격히 줄고 있는 상황임

- 기술적으로 발전되고 시장의 크기가 커지는 방향으로의 건전한 경쟁구도가 아닌 하나의 마케팅의 일환으로 시장을 축소시키는 것은 지양되어야 할 것이지만 보안 전문 업체의 역할이 더욱 필요하게 될 것이며 보안이라는 관점에서의 대응 체제가 더욱 중요한 역할을 하게 될 것임

○ 안티바이러스 시장 발전의 긍정적 요소

- 인터넷 사용 증가와 더불어 새롭고 다양한 바이러스, 웜이 지속적인 위협요소로 작용하고 있고 그 피해가 늘어나고 있음

20) 국내 정보보호산업 시장 및 동향조사, KISIA, 2007.11

– 성숙된 시장이지만 1회성 구매에 그치지 않고, 연 단위 계약 및 업데이트가 일반화 되어 꾸준한 시장이 창출되고 있음
– 단순한 안티바이러스 기능에서 개인방화벽, 개인정보보호 기능까지 포괄하는 등, 통합 솔루션 공급 일반화로 매출 단가 상승에 대한 시도가 지속되고 있음
– 특정 목적을 타깃으로 하는 공격으로 인해 변종이 많아지고 있으며 지역별 공격형태 및 악성코드의 피해가 다르게 나타나고 있음

PC 보안 관련 제품의 매출전망[21]

(단위: 백만 원)

	2006	2007	2008	2009	2010	2011	CAGR(%)
안티바이러스	60,556	62,920	64,102	65,284	66,466	67,648	2.2%
안티스파이웨어	11,526	12,202	12,540	12,878	13,216	13,554	3.2%
PC 방화벽	11,989	10,947	12,059	12,633	13,206	13,780	3.0%
패치 관리	8,121	11,410	13,055	14,699	16,344	17,988	5.8%
기타 PC 보안	35,662	36,574	39,786	42,423	45,060	47,697	5.9%
합계	127,854	134,053	141,542	147,917	154,292	160,667	4.02%

○ 안티바이러스 시장 발전의 부정적 요소
– 불확실한 경기 전망은 기업들에게 전반적인 IT 투자, 특히 보안 부분에 대한 투자규모 축소를 요청하고 있으며 상반기 공공기관의 통폐합으로 수요가 하반기로 연기된 건도 많음
– 다수의 신규 벤더가 등장함에 따라 경쟁이 심화되고 있으며, 저가 수주현상이 일반화 되어가고 있고 마이크로소프트의 등장으로 가속화될 것으로 예상됨
– 저가 전쟁이 더욱 심화되며 그나마 커지고 있던 개인시장이 없어지고 있으며 그 영향이 중견중소기업 시장에 미치고 있음

○ 기타 PC 보안 시장 현황
– 2003년 1.25 인터넷 대란 이후 웜 공격이 끊이지 않았고, 이에 대한 근본적인 해결책으로 패치관리 솔루션이 시장에 소개되어 현재는 공공시장을 필두로 금융권을 비롯한 국내 주요 대기업이 이미 패치관리 솔루션을 도입해 운영하고 있는 등 시장 규모가 확대되고 있는 추세며 패치관리의 향후 발전 가능성에 대해서는 패치의 범위가 확장될 것이라는 안과 기업용 안티바이러스 솔루션의 구성요소로 편입 될 것이라는 두 가지 예측이 존재함
– 고객정보 유출 방지를 위한 DBMS에 대한 접근 제어 솔루션, DB 암호화 등 DB 보안 제품, 내부 정보의 무단

21) 국내 정보보호산업 시장 및 동향 조사, KISA, 2007

반출에 대한 대응책인 엔터프라이즈 DRM과 USB 등 외부 매체 장치를 무단으로 사용할 수 없게 만드는 제품 등 다양한 솔루션이 공급되고 있고 주로 대기업 및 공공기관을 발판으로 시장의 확산을 꾀하고 있지만 기술적, 관리적 문제로 인하여 실제 효용성은 낮은 수준이나 법안 계류 중인 개인정보보호법이 통과되면 본격적인 시장의 확산이 예상됨

○ 디지털포렌식

- 기업들의 보안 관리의 중요성이 강조되면서 단순 로그관리에 그치는 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
- 국내사건 대응 서비스 시장은 세계시장의 5% 수준으로 예측하여 2011년 3,550억 원에 이를 것으로 추정됨
- 미국에서 디지털 정보의 미제출로 인한 벌금 부과의 사례가 있었으며, 소송증거 확보를 위해 디지털포렌식 도구의 사용이 의무화됨에 따라 업체에서 자체적으로 솔루션을 도입 및 운영하려는 추세가 확대되고 있음

2.1.2. 국외 시장 현황 및 전망

○ USN 보안

- ETRI 보고서에 따르면 2010년도에는 440억 달러 이상의 시장이 형성 될 것으로 전망

○ 휴대인터넷 보안

- 모바일 와이맥스 전 세계 시장규모는 2011년까지 가입자 기준으로 2억 1천만 명에 이를 것으로 추정
- 전 세계 와이맥스 장비 시장은 2010년까지 연평균 70%의 고속 성장을 지속할 전망[22]
  - 고정형 와이맥스 및 모바일 와이맥스 장비 시장은 오는 2010년 46억 달러 규모로 예측됨
  - 2010년에 이동형 장비가 전체 와이맥스 시장의 66% 차지할 전망
- 2007년 전 세계 와이맥스 시장 규모는 2006년(9억 3,900만 달러)에 비해 70.18% 증가한 15억 9,800만 달러에 달할 것으로 추산되고 있으며, 2008년에는 245개 텔레콤 업체가 와이맥스에 30억 9,600만 달러 이상을 투자할 것으로 예측됨
- 정보통신컨설팅 업체인 대만의 MIC[23]에 따르면 2006~2008년 동안 와이맥스 네트워크 구축에 대한 세계 총 투자 규모는 52억 달러에 이르고, 연평균 성장률은 150%에 달할 것으로 예측됨
  - 2006~2008년 동안 미국은 약 30억 달러를 투자하여 최대 투자국이 될 것으로 예상되고 대만은 6억 6,400만 달러로 2위 투자국이 될 것이며, 한국은 총 6억 4,100만 달러를 투자할 것으로 전망됨

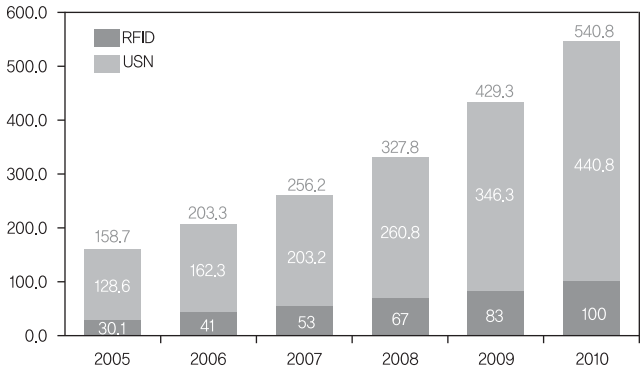
22) 인포네틱스리서치, 2007.6

23) Market Intelligence Center

– 와이브로 세계 시장은 향후 5년간 급속히 성장하여 2012년 약 38조 원에 이르는 등 향후 약 5년간 약 94조 원의 시장을 형성할 것으로 예상됨

– 이에 따라 향후 5년간 장비수출 30조 원 이상, 생산유발효과 15조 원, 부가가치 유발효과 7조 원, 고용창출효과 7만 6천여 명에 달할 것으로 전망

– 2006년 한국, 일본, 미국, 영국, 프랑스 등 24개 나라에서 와이맥스 네트워크가 상용화 단계에 접어들기 시작하였으며, 대만도 2007년 7월 6개의 와이맥스 자격증을 발급



세계 RFID/USN 시장동향[24]

(단위: 억 US$)

○ 미국

– 2008년 말까지 미국 전역에 와이맥스 서비스 상용화를 목표로 추진 중이나, 미국 메이저급 이동통신사인 LTE[25]를 지지하는 쪽으로 방향을 급선회할 가능성이 있어 전망이 다소 불투명

– 스프린트 넥스텔

- 미국 내 3위 이동통신사로 다양한 전략적 제휴를 통해 미국 전역에서 모바일 와이맥스 상용화를 계획하고 있음
- 경쟁업체인 클리어와이어와 제휴를 맺고 와이맥스 망을 공동 구축키로 합의
- 구글과 제휴하여, 모바일 와이맥스 서비스를 위해 구글이 무선인터넷 검색, 소셜 네트워크 사이트, 인스턴트메신저, 이메일 등의 응용 애플리케이션 부분 담당키로 함
- 2008년까지 모바일 와이맥스 서비스에 25억 달러를 투자하고 시카고, 볼티모어, 워싱턴 D.C, 3개 도시에서 상용화 서비스 돌입 계획(볼티모어와 워싱턴 D.C는 삼성전자가 망과 장비를 공급할 예정)

24) ETRI/IDTech/VDC

25) Long Term Evolution

• 최근 와이브로 사업을 자회사 형태로 분리하는 계획 추진 중이어서 서비스 제공이 연기될 우려가 있음

– AT&T

• 2.3GHz에 대한 면허 획득, 이르면 오는 2008년 2분기부터 와이맥스 서비스 시작 예정

– 버라이즌 커뮤니케이션즈

• 미국 내 2위 통신사업자이며, 4세대 이동통신 표준으로 와이맥스가 아닌 GSM 계열의 LTE를 채택하여 내년부터 시험 테스트 실시 계획

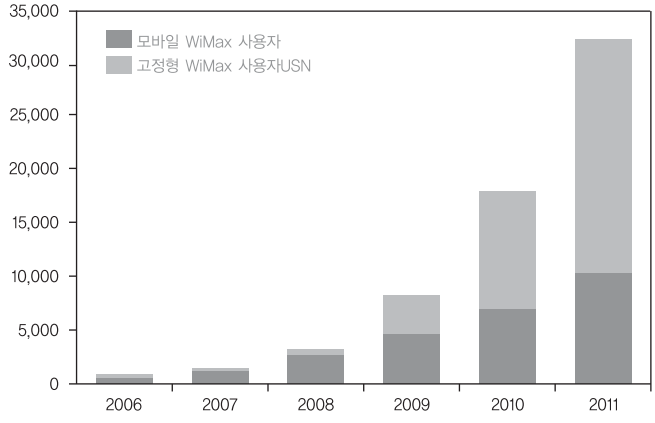
• AT&T가 버라이즌을 따라 LTE 진영으로 이동 가능성에 대한 우려 제기되고 있음

○ 유럽

– 3G LTE 기술과의 경쟁으로 모바일 와이맥스 도입이 가장 어려운 시장으로 인식되고 있음. 유럽 주요 국가들은 모바일 와이맥스 관련 주파수 할당 검토 단계에 있으며, 기술검토 및 업체선정 소요기간을 감안할 때 상용화까지 상당한 시간이 소요될 것으로 예상됨

– 보다폰

• 최근 와이맥스 포럼에 주요 협력사로 합류. 지금까지는 4G 기술로 3G LTE를 채택하겠다는 입장이었으나, 3G LTE 기술이 상용화까지 상당한 시간이 소요될 것으로 예상되어 3G 통신기술인 UMTS(WCDMA) 이후 통신 기술로 와이맥스를 채택하려는 것으로 보임



전 세계 와이맥스 가입자 증가 추이[26]

26) Ovum 2007

○ 독일은 2006년 12월 3.5 GHz 주파수대의 무선 브로드밴드 라이선스 경매 진행. 와이브로의 국제표준 채택 시 반대의사를 표했던 국가로 와이브로에 대한 부정적인 시작이 지배적임

○ 이탈리아는 모바일 와이맥스에 사용될 3.4~3.6 GHz 대역 주파수 입찰 계획을 공개하고 총 35개 사업자에 라이선스를 발급할 계획임. 낙찰자는 15년간 지속적인 허가권을 갖게 될 예정이며, 입찰가는 4500만 유로(약 6385만 달러)부터 시작될 예정

○ 일본은 2.5 GHz 주파수 대역 모바일 와이맥스는 2007년 9월 총무성이 2개 사업자 선정하여 면허를 교부하고 기존 3세대 이동통신사업자(NTT 도코모, KDDI, 소프트뱅크)에 면허를 할당하지 않을 방침이며, 간이휴대전화(PHS) 사업자인 윌콤의 선정이 유력시 되고 있는 가운데, Wireless Broadband Planning[27] 진영과 아카네트웍스를 내세운 NTT 도코모/소프트뱅크 진영의 치열한 경쟁이 예상됨

○ 중국은 자국의 이동통신 기술인 TDS-CDMA에 대한 육성정책 등의 이유로 모바일 와이맥스 상용화가 지연되고 있음. 청도에 중국 기간통신사업자로는 최초로 차이나모바일이 모바일 와이맥스 망을 구축함

○ 우리나라 정부 및 민간 산업체의 협력으로 해외 로드쇼 및 국제포럼을 개최 후 전 세계 5개국 6개 사업자에서 와이브로 시험 서비스를 제공 중이며, 6개국 7개 사업자는 와이브로 상용서비스를 제공할 예정

- 시험장비 운영국가: 5개국 6개 사업자
  - 일본: KDDI(2005년 3월), NTT 도코모(2006년 5월)
  - 영국: BT(2005년 8월)
  - 아랍에미레이트: 에티살랏(2006년 9월)
  - 미국: 뉴파라(2007년 2월)
  - 남아프리카공화국: 알텍(2007년 7월)

3G 표준 채택 이후의 와이브로 세계시장 규모 전망[28]

(단위: 억 원)

구분		2008년	2009년	2010년	2011년	2012년	합 계
3G 표준 채택 전		38,000	66,000	116,000	176,000	248,000	644,000
시장규모 증가분	기존 시장 확대	1,602	2,799	4,947	7,566	10,743	27,656
	추가 시장 발생	0	5,828	42,895	96,977	121,423	267,123
	소계	1,602	8,627	47,842	104,542	132,166	294,779
3G 표준 채택 후		39,602	74,627	163,842	280,542	380,166	983,779

27) KDDI, 인텔, 동일본여객철도, 교세라, 다이와, 도쿄미쓰비시 은행이 와이맥스 사업권 취득을 위해 공동 출자하여 설립한 신규 법인
28) ETRI 신기술정책 연구팀. 2007

표준 채택에 따른 경제적 파급효과[29]

(단위: 억 원)

구분	2008년	2009년	2010년	2011년	2012년	합 계
생산유발효과	796	4,287	23,773	51,947	65,673	146,476
부가가치유발	398	2,145	11,896	25,994	32,863	73,296
고용창출(M/Y)	407	2,192	12,157	26,564	33,583	14,903

– 해외 상용서비스 추진예정 국가: 6개국 7개 사업자

- 브라질: TVA(2007년 4월)
- 이탈리아: TI(미정)
- 베네수엘라: 옴니버전(2007년 상반기)
- 크로아티아: 포르투스(2007년 상반기)
- 미국: 아리아링크(2007년 상반기), 스트린트 넥스텔(2008년 2분기)
- 사우디아라비아: 바아낫(2007년 7월)

전 세계 와이맥스 추진 현황[30]

국 가	형 태	주 파 수 (GHz)	추 진 현 황
한국	모바일	2.3	상용화
일본	모바일	2.5	모바일은 검토 중 고정형은 4.9로 상용화
호주	고정형	3.4 ~ 3.5	상용화
사우디아라비아	고정형	2.5 + 3.5	검토 중
중국	고정형	3.5	검토 중
싱가포르	모바일 & 고정형	2.3 & 2.5	검토 중
필리핀	고정형	3.4	검토 중
인도네시아	모바일	2.3	검토 중
말레이시아	모바일	2.3	검토 중
대만	모바일	2.3 + 2.5	검토 중
뉴질랜드	모바일	2.3 + 3.5	검토 중
인도	고정형	3.4 ~ 3.5	검토 중
태국	고정형	2.5 + 3.5	검토 중
네덜란드	고정형	3.5	상용화
덴마크	고정형	3.5	상용화
크로아티아	모바일	3.5	검토 중

29) ETRI 신기술정책 연구팀. 2007

30) 방송통신위원회(舊 정보통신부)

국 가	형 태	주 파 수 (GHz)	추 진 현 황
이탈리아	모바일	2.5	검토 중
영국	모바일 & 고정형	2.5 & 3.5 + 5.8	검토 중
아일랜드	고정형	3.5 + 5.8	검토 중
스페인	고정형	3.4	검토 중
프랑스	고정형	3.5	검토 중
독일	고정형	3.5	검토 중
스웨덴	고정형	3.5	검토 중
러시아	고정형	2.5 + 3.5	검토 중
노르웨이	모바일	2.5	검토 중
미국	모바일 & 고정형	2.3 + 2.6 & 2.5	고정형은 상용화 모바일은 검토 중
캐나다	고정형	2.5 + 3.5	상용화
브라질	모바일	2.5	상용화
베네수엘라	모바일	2.5	검토 중
멕시코	고정형	2.5 + 3.5	검토 중

- KT는 미국 뉴파라 사에 와이브로 서비스 기술 컨설팅을 제공하고 있고 와이브로 관련 사업자들의 글로벌 협의체인 WMC[31] 의장과 와이맥스 포럼 이사회 임원과 글로벌로밍 워킹그룹 의장으로 활동하며 와이브로 세계 시장에서 주도적인 역할을 하고 있음
- 삼성전자는 2006년 8월 미국의 주요 통신사업자인 스프린트사와 전격 와이브로 상용화 계약을 체결하면서 3.5 G를 이끌어가는 선두주자로 급부상했으며, 미국, 이탈리아, 브라질 등 23개국 35개 사업자와 와이브로 사업을 추진 중

○ 홈네트워크 보안

- 지능형 홈네트워크 세계시장 규모는 2008년에 852억 달러로 전망되며, 향후 연평균 10%씩 성장하여 2010년에는 936억 달러 규모로 성장할 것으로 전망됨
- 홈네트워크의 활성화 지연 및 보안제품에 대한 인식미비로 현재 구체적인 홈네트워크 보안시장은 형성되지 않고 있으나, 네트워크 시스템 및 서비스 시장 대비 네트워크 보안시장간 비율을 반영하면 향후 홈네트워크 활성화가 이루어질 경우 홈네트워크 시장의 3% 규모의 홈네트워크 보안시장이 형성될 것으로 예상됨

31) Wibro-Mobile WiMAX Community

지능형 홈네트워크 세계시장[32]

(단위: 백만 달러)

구분	2004	2005	2006	2007	2008	2009	2010	CAGR '05-'10
홈플랫폼	4,554	8,768	13,434	20,946	27,786	31,315	35,133	32.0%
유무선 홈네트워크	3,327	2,935	2,795	2,558	2,582	2,415	2,336	-4.5%
정보가전	36,840	44,022	47,873	48,593	48,996	47,558	47,084	1.4%
유비쿼터스 컴퓨팅	1,754	2,397	3,326	4,542	5,932	7,526	9,139	30.7%
총계	46,475	58,122	67,428	76,639	85,295	88,814	93,692	10.0%

휴대폰 업체별 출하량 실적과 전망[33]

(단위: 천대, %)

구분	2005년	2006년	2007년(E)	2008년(E)
노키아	264,900(32.4)	347,500(34.1)	437,100(38.5)	465,000(37.9)
모토롤라	146,000(17.9)	217,400(21.3)	154,200(13.7)	165,200(13.5)
삼성전자	102,900(12.6)	113,760(11.2)	159,900(14.2)	201,050(16.4)
소니 에릭슨	21,000(6.2)	74,830(7.3)	103,600(9.2)	109,000(8.9)
LG 전자	54,900(6.7)	64,400(6.3)	79,661(7.1)	91,623(7.5)
기타	197,420	200,700	192,479	194,969
합계	817,120	1,018,590	1,126,940	1,226,272

- 2010년 홈네트워크 장비 시장 중 정보가전 시장 비중이 세계시장의 50%로 가장 큰 부분을 차지할 것으로 전망되면서 가정 내 IT 인프라가 보편화될 것임
- 홈네트워크 서비스가 홈오토메이션에서 홈엔터테인먼트 중심으로 진화되면서 인터넷 접속과 다양한 엔터테인먼트 서비스를 융합하여 제공하는 차세대 홈서버 시장이 빠르게 형성될 것으로 전망됨
- 홈네트워크 확산에 따라 디지털홈 주요 장비인 홈서버 · 홈게이트웨이는 연평균 48%의 높은 성장이 기대됨

○ 이동통신망 보안

- 세계 이동통신 가입자는 2006년 말 기준으로 27억 5,000만 명을 넘어섰으며 2007년에는 16.8% 증가한 32억 2,000만 명, 2008년에는 36억 5,000만 명, 2009년에는 39억 6,000만 명을 웃돌 것으로 추정됨에 따라 전체 세계인구 대비 이동통신 보급률은 2006년 42.2% 수준에서 2007년 48.7%, 2008년 54.6%가 될 것으로 전망됨
- 세계 휴대폰 시장은 2002년부터 다양한 휴대폰 기능들이 업그레이드되면서 교체수요 시장이 빠르게 성장하고 있으며, 특징으로는 컬러폰, 카메라폰, 뮤직폰 등으로, 구조 측면에서는 폴더형, 슬라이드형, 슬림형으로, 기술적 측

32) 005 In-Stat. 2005 Gartner. 2005VDC

33) 키움증권, 2007.11.21., 중앙일보, 2008.1.26.

면에서는 2.5세대(CDMA1x, GPRS), 3세대(EV-DO, W-CDMA), 3.5세대(HSDPA)로 빠르게 이동하고 있음

- 특히, WCDMA방식의 3G 휴대폰 시장이 전체 휴대폰 시장에서 차지하는 비중은 2005년 5%, 2006년 9%에서 2007년 15%, 2008년 25%로 가파르게 성장할 것으로 예상됨
- 이와 함께 2000년대 초반부터 보급이 급격히 확대되고 있는 카메라폰, MP3 폰 등 컨버전스 제품의 추이를 살펴보면, 세계 휴대폰 시장 내 카메라폰의 비중은 2004년 23%에서 2008년에는 59%로 확대되고, 동 기간 중 MP3 폰은 9%에서 61%로 증가할 것으로 전망됨
- 터치스크린폰(스마트폰/PDA 폰 포함)의 경우, 2006년 5,100만대에서 2007년에는 6,500만대, 2008년에는 1억 900만대, 2009년에는 1억 9,300만대로 점차 증가할 것으로 전망되며, 전체 휴대폰 시장에서 차지하는 비율도 2006년 5.0%에서 2007년에는 5.7%, 2008년 8.9%, 2009년 14.6%로 그 비중이 점차 증대할 것으로 예상됨
- 세계 휴대폰 시장 규모는 2008년은 작년 대비 15% 성장한 13.0억 대 규모가 될 것으로 예상되며, 구글과 아이폰이 신제품을 출시하여 판도 변화의 주요 요인이 되고 있음

○ 무선근거리통신망 보안

- 전 세계적으로 일일 공중 무선랜 이용자는 89% 증가하였으며, 특히 유럽 지역의 이용은 9% 증가하여 전체의 40%를 차지하였음. 미국이 차지하는 비율은 8% 감소한 51%가 되었음. 도시별로 런던이 전년대비 56% 증가하여 전년에 이어 1위로 선정되었고 제2위는 싱가포르이며, 도쿄는 18% 증가하여 뉴욕을 제치고 세계 제3위에 랭크되었음
  - 일본은 랜을 중심으로 발전하고 있고 아직 무선랜 시장은 규모가 크지 않은 편이지만, 서비스 제공업체들의 부가가치 옵션으로 매우 중요한 역할을 하고 있으며, 실제로 소프트뱅크 그룹의 재팬 텔레콤이 맥도날드와 협력해 일본 내 맥도날드 매장의 70%에 무선랜 서비스를 공급하고 있음. IDC Japan의 2008년 2월 발표한 무선랜 기기 시장동향에 따르면, 일본 내 무선랜 기기 시장은 액세스 포인트와 무선랜 컨트롤러/스위치를 맞추어 최종 사용자 매출액 124억 7,500만 엔으로 추정함. 그 중 무선랜 컨트롤러/스위치와 AP 집중관리형 무선랜 시스템이 약 68%를 차지함. 2006년~2011년까지 연평균 성장률은 무선랜의 편리성, 고밀도 및 광대역 환경 구축, IEEE802.11n의 이용 진전 등으로 14.2%의 고성장이 전망되며, 2011년 일본 내 무선랜 기기 시장은 242억 엔에 이를 것으로 전망됨
  - 중국은 모든 다국적 기업들이 노리는 거대시장이라는 점을 활용하여 독자 기술표준 전략을 더욱 강화하고 있으며 중국 독자 기술 표준의 효율성 및 안정성이 국제표준에 비해 떨어지더라도 밀어붙일 경우 국제 표준이 될 가능성이 높다고 생각됨
    - ISO에서 실시된 ISO 가맹국 투표에서 미국이 개발한 IEEE 802.11i에 밀려 국제 표준화를 실패한 이후 자국 내 산업화를 강화하는데 초점을 맞추고 있으며 지난 7월 세계 첫 WAPI 휴대용 단말기가 출시됨에 따라 중국이 WAPI[34] 산업화를 시키는데 탄력이 붙게 되었음

34) 중국의 독자적인 무선랜 암호화 표준

· 올해부터 베이징, 상하이, 주쟝, 창쟝 지역에서 모바일 도시 구축 프로젝트를 본격적으로 시작하기 때문에 WAPI 산업은 거대한 상업 기회를 맞이하게 될 전망이며 이와 함께 WAPI 관련 업체들은 중국 대도시들의 모바일 도시 구축을 계기로 WAPI 제품 개발에 박차를 가하고 있으며 중국 정부도 이를 적극적으로 지원하고 있는 상황임

– 현재 무선랜을 활용한 MAN[35] 구축 프로젝트가 속속 등장하고 있으며 세계 여러 나라들은 유비쿼터스 사회 구축의 일환으로 무선랜을 통해 도시 전체를 아우르는 무선 MAN 구축 프로젝트를 진행하고 있음[36]

- 일본 라이브도어의 D-Cubic은 무선랜으로 동경 JR선 야마노테센 열차가 지나는 지역의 80%를 커버하며, 이용요금은 525엔이 될 것으로 알려져 있음. 이외, 노무라 종합 연구소와 인텔이 주도하고 있는 디지털시티 오사카 프로젝트는 오사카시 남쪽 항구 코스모스퀘어 일대를 무선랜으로 커버하려는 계획을 수립, 사업을 진행 중이며, 공중 무선랜 서비스 무선랜 클럽을 운영하고 있는 NTT 브로드밴드 플랫폼(NTTBT)도 이와 유사한 서비스를 시작했음
- 미국의 필라델피아시와 아리조나주 템프시 등이 시내 전체를 무선랜으로 커버하려는 프로젝트를 진행했음
- 대만에서는 세계 최대의 무선랜 프로젝트가 진행 중으로 대북시에 약 1만개의 AP를 설치해 도시 전체를 커버하는 '망로(網路-중국어로 네트워크를 뜻함)신도(新都)'를 진행 중인 이 프로젝트는 2006년 말까지 대북시 인구의 90%에게 무선랜 서비스 제공을 목표로 하고 있음
- 구글이 마운틴 뷰 도시 전체에 Wifi 무료 서비스를 시작하였음

– Wifi 시장 동향을 장비 시장과 칩셋시장으로 분리해서 살펴보면 아래와 같음

- 장비 시장: 무선랜 장비 시장은 05년~10년간 생산대수 기준으로 연평균 4.4%의 마이너스 성장이 예상되며, 매출시장 역시 -0.1%의 성장이 예상됨. 무선랜 카드 시장은 급속한 단가 하락으로 매출 시장이 감소 추세인 반면, AP 시장은 '05년~' 10년까지 연평균 3.8%의 성장을 통해 12.4억 달러의 시장을 형성할 것으로 전망됨. 특히 AP 시장은 개인보다는 기업이 시장을 주도할 것으로 전망됨. 기업별 시장점유율을 살펴보면, 시스코는 급성장하고 있는 기업용 무선랜 장비 분야에서 확고한 1위를 차지하고 있으며 Symbol이 2위, Aruba와 Trapeze가 공동 3위를 기록, 시스코는 서비스 프로바이더용 무선랜 장비 시장 매출에서도 62%의 점유율로 1위를 차지하였으며, 주거용 제품 분야에서는 Linksys가 1위, NETGEAR가 2위를 차지함

35) Metro Ethernet Network

36) 특정 도시에 다수의 무선랜 AP를 설치해 그 지역을 무선랜 전파로 모두 연결하는 것을 의미함

주요 산업기술의 국제표준 대 중국표준

기 술 분 야	국제표준	중국표준
3세대 이동통신	WCDMA, CDMA-2000	TD-SCDMA
차세대 DVD	블루레이, HD-DVD	EVD
무선LAN	802.11i	WAPI
홈네트워크	DLNA	IGRS
영상압축기술	MPEG	AVS
RFID	EPC	NPC

무선랜 장비 시장 전망[37]

(단위: 백만 달러)

구분	2005	2006	2007	2008	2009	2010	CAGR('05-'10)
NIC	366	256	205	169	138	113	-20.9%
AP	1,027	1,066	1,101	1,159	1,198	1,239	3.8%
스위치/콘트롤러	386	498	541	556	488	428	2.1%
합계	1,779	1,820	1,864	1,884	1,824	1,766	-0.1%

도시별 무선랜 이용 순위[38]

	2H07 SESSIONS	SESSION LENGTH(MIN)	% OF WORLDWIDE TOTAL	2H06 SESSIONS	ANNUAL GROWTH FROM 2H06
런던	28,720	72	1.3%	11,203	156%
싱가포르	9,925	66	0.5%	5,764	72%
도쿄	9,591	77	0.4%	4,395	118%
뉴욕	7,929	54	0.4%	5,729	38%
시카고	5,920	44	0.3%	5,615	5%
휴스턴	5,372	50	0.2%	4,422	21%
샌프란시스코	4,889	51	0.2%	4,282	14%
댈러스	4,426	54	0.2%	4,039	10%
뮌헨	4,186	24	0.2%	2,203	90%
새노제	4,156	53	0.2%	2,990	39%

- 칩셋 시장: IDC에 따르면 세계 Wifi 칩셋 시장은 2009년에 2,931 백만 달러로 추정되는데 Wifi의 다양한 표준 중 802.11/a,b,g 칩셋의 시장규모는 모두 점진적으로 줄어들지만, 802.11n MIMO 칩셋은 CAGR 155%의 성장률을 가지며, 2009년에는 759.8백만 달러 규모로 전체 WiFi 칩셋의 26%에 해당함. 또한 듀얼 밴드 칩셋의 시장규모도 연 69%의 높은 성장률로 커질 것으로 예상됨

37) Gatner, 2005 보고서

38) USA iPass의 전화조사 결과

- 2009년에 세계 무선랜 장비 시장 매출은 36억 달러에 달할 전망으로 부문별로는 2사분기 무선랜 장비 매출 중 기업용 제품이 47%를 차지하였으며 주거용 제품은 45%, 서비스 프로바이더용 제품은 8%를 차지하였고 2009년까지 무선랜 시장에서 기업용 제품이 차지하는 비중은 67%까지 늘어날 전망
- 지역별 매출 구성을 보면, 북미 지역이 2사분기 무선랜 장비 매출의 48%를 차지하였으며 EMEA 지역은 30%, 아시아/태평양 지역은 20%, 중남미 지역은 2%를 차지

○ 차세대 네트워크 보안

- 방화벽/VPN 보안시장 현황
  - 시장조사 전문 기관인 Frost & Sullivan이 발표한 아시아 태평양 네트워크 보안 시장 조사결과에 따르면, 시스코 시스템즈가 하드웨어 방화벽/VPN 시장에서는 27.9%를 차지하는 것으로 조사되는 등 아시아 태평양 지역 최대의 네트워크 보안업체로 나타났으며(시장점유율 23.4%), 시스코의 뒤를 이어 주니퍼가 아시아 태평양 네트워크 보안시장에서 11.9%의 점유율로 2위를 차지했고, 3위는 소프트웨어 업체인 체크포인트가 차지함
- IDS/IPS 보안시장 현황
  - 현재 세계적인 IDS 제품은 Realsecure, Netprowler, Dragon, Blackce, PIX 등이 있으며, 3Com의 TippingPoint IPS, Radware의 DefensePro 제품 등이 있음
- UTM 보안시장 현황
  - 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

○ 사이버 공격 역추적/보안관리

- 세계 보안관리 시장은 타 보안 분야보다 가장 높은 성장률을 보이고 있으며, 특히 미국 내에서는 사이버공격에 대한 보안 관제를 위해 지출되고 있는 비용이 높은 증가율을 보임[39)]
  - 보안 관리 및 취약점 관리 시장은 보안 컴플라이언스에 대응하고 보안인프라의 복잡성을 관리하기 위한 수요가 증가
  - 콘텐츠 보안 및 위협관리 영역은 다양한 복합 공격이 출현하면서 호스트, 네트워크단을 불문하고 방화벽, VPN에 다양한 콘텐츠 보안 기술이 접목되어 통합 솔루션 형태의 시장 접근이 두드러지고 있음
- 사이버 보안 동향
  - 미국인의 70%가 인터넷 및 컴퓨터 보안에 대한 우려하고 있으며, 미국인의 74%가 인터넷상의 그들의 개인정보가 도난 되어 악용될 것을 우려하고 있는 것으로 조사됨

39) IDC 2007

• 미국인의 74%가 전화네트워크 혹은 발전소 등과 같은 국가 주요 인프라에 대한 테러리스트들의 사이버 공격이 있을지 모른다고 우려하는 것으로 미국 정보기술협회[40]와 Tumbleweed Communications Corp.의 공동조사결과 나타남

○ 봇넷 대응

– 봇넷 침입 탐지 및 대응 기술은 연구 초기 단계로 아직 시장이 형성되지 않았기 때문에, 국외 시장 규모는 정보보호 제품 시장 규모를 참고하여 '05년 323억 달러 규모로 파악되며, 연평균 15.6%로 성장하여 '10년 666억 달러에 이를 것으로 전망됨

○ 서버 보안

– IDC에 따르면 2005년 아시아/태평양 지역의 보안 응용 서버 시장은 5.5억 달러에 이르고 이 시장은 해마다 39%정도씩 성장해왔음

– UTM 시장은 많은 기능을 가진 제품이 출시되어 가속도가 붙고 있고 방화벽 및 VPN은 단일 제품으로 판매되며 보안 응용 서버 시장의 53%에 해당하고 있으나 몇 몇 고객들은 UTM으로 옮겨가고 있음

– IPS 부분은 보안 응용 서버 시장에서 겨우 두 자리 수를 차지하는 정도임

– IDC는 고객들이 네트워크 하부구조와 필수적 사업을 보호하기 위해 서버 보안의 필요성으로 보안 응용 서버 분야가 2010년까지 성장 곡선을 유지한다고 예상하고 있으며 특히 아시아/태평양 지역의 보안 응용 서버 시장이 15.6% CAGR로 성장하여 2010년에는 11.34억 달러에 이를 것이라고 전망함

– NSA에서는 Linux를 기반으로 기존의 보안 구조(Flask Architecture)를 통합한 SELinux[41]를 개발하였고, 현재 Linux 커널에 기본 기능이 탑재되어 보안 서버 시장에 변화를 주고 있으며, SELinux를 활용하는 방법도 활발히 연구됨

○ PC 보안

– 해외 시장을 보면 꾸준히 성장이 예상되지만 안티말웨어 시장은 서서히 하향추세를 보이며 새로운 패러다임의 변화가 필요한 시점으로 보이나, PC 보안 전체로 보았을 때 위협에 대한 시장은 커지고 있는 것으로 예상하고 있으며 안티말웨어 시장이 그 자체는 줄어들고 있지만 오히려 다른 분야로 확대되고 있다는 것으로 해석될 수 있음

40) ITAA, Information Technology Association of America

41) Secure Enhanced Linux

세계 정보보호 시장 전망

(단위: 백만 달러)

구분	2005	2006	2007	2008	2009	2010	CAGR(%)
정보보호 H/W	6,045	7,346	8,793	10,435	12,141	13,589	17.6
정보보호 S/W	11,802	13,598	15,404	17,088	18,714	20,492	11.7
정보보호 서비스	14,484	17,170	20,283	23,865	27,981	32,595	17.6
합계	32,331	38,114	44,480	51,388	58,837	66,677	15.6

○ 디지털포렌식

- 전 세계 사건 대응 시장은 2007년 46억 달러에서 연평균 17.8%씩 증가하여 2011년에는 86억 달러에 이를 것으로 추정됨[42]
- 최근 미국의 경우 디지털포렌식 서비스 시장 규모는 15억 달러 이상으로 추정되며, 최근 3년간 60% 이상의 급속한 성장을 지속하고 있음[43]

World security product and service revenue by segment[44]

(단위: $백만 달러)

	2006	2007	2008	2009	2010	2011	2006-2011 CAGR(%)
Identity and access management	2,989	3,370	3,770	4,152	4,548	4,975	10.7
Secure content and threat management	13,237	15,119	17,160	19,191	21,166	23,125	11.8
Security vulnerability management	1,886	2,269	2,706	3,202	3,757	4,386	18.4
Other security products	593	736	897	1,049	1,200	1,350	17.9
Security services	16,981	20,171	23,824	27,980	32,708	37,938	17.4
Total	35,686	41,668	48,357	55,574	63,379	71,773	15.0

U.S. Managed Security Services 2008~2012 Forecast and Analysis[45]

	2007	2008	2009	2010	2011	2012	CAGR(%)
Spending	1,281	1,520	1,795	2,111	2,456	2,838	· 17.2
Growth(%)	NA	18.7	18.1	17.6	16.3	15.6	

42) IDC, 2007
43) Guidance Software, CEIC 2006
44) IDC #210018
45) Doc#213551, IDC 2008

Worldwide Corporate Endpoint Security Revenue by Submarket[46]

(단위: US $M)

	2006	2007	2008	2009	2020	2011	CAGR(%)
Antimalware	1,397.6	1,350.0	1,294.1	1,226.1	1,226.1	1,151.5	–5.3
Endpoint threat management	318.9	355.3	390.0	390.0	419.2	448.1	8.3
Security suites	363.5	544.5	766.6	766.6	1,005.8	1,258.3	33.3
Other	319.0	442.2	545.7	545.7	657.7	767.1	22.1
Total	2,399.0	2,692.0	2,996.3	3,308.8	3,625.0	3,941.5	10.4

디지털 포렌식 분야 세계 시장의 성장 추세[47]

(단위: US $M)

구분		2006	2007	2008	2009	2010	2011	CAGR(%)
Digital Forensic(Discovery & Litigation Support)	SW	280	366	451	536	611	698	20.0
	HW	328	423	532	756	756	856	21.1
	서비스	3,207	3,839	4,598	5,406	6,228	7,101	17.2
	소계	3,815	4,628	5,581	6,605	7,594	8,654	17.8

46) IDC, 2007

47) IDC, 2007

2.2. 기술개발 현황 및 전망

2.2.1. 국내 기술개발 현황 및 전망

○ USN 보안

– 정부정책기조

• 행정안전부 산하 한국정보사회진흥원(NIA)을 통해 USN 활용 산업 기술 저변을 확대하고 있음. 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

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

– USN 응용 서비스를 위한 인증 기술, 공격탐지, Secure Routing 등이 USN 보안 표준화의 중요 쟁점 사항이며 국내외에서 기술 개발에 박차를 가하고 있는 상황임

– 현재 20여 건 정도의 USN 관련 특허가 최근 등록되었으며, USN 보안 관련 특허는 3건으로 미약하나 증대될 것으로 사료됨

○ 휴대인터넷 보안

– 국내기술 현황

• KT 와이브로는 2007년 4월 서울 전 지역으로 서비스 지역을 확대했으며, 2007년 6월 IMS 기반의 통합커뮤니케이션 서비스 플랫폼을 국내 최초로 구축하여 HSDPA 사용자와 영상통화가 가능하고, 지상파 DMB 방송사 U1 미디어와 협력하여 와이브로를 통해 실시간으로 방송에 참여할 수 있게 됨

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

USN 관련 특허 현황

특허명	등록번호	등록일	출원인
센서 노드 간 통신 보안 방법 및 그 시스템	10-2006-0122553(출원)	2006.12.05(출원일)	ETRI
센서 네트워크에서 공간 효율적인 결정적 비밀키 분배 방식	10-2005-0129205	2005.12.24	중앙대학교 산학협력단
센서네트워크 환경에 적합한 센서 인증 시스템 및 방법	10-2005-0027303	2005.03.31	니츠

○ 홈네트워크 보안

- 현재 국내 홈네트워크 산업은 가전제어, 엔터테인먼트 서비스, 보안 서비스 등 다양한 서비스를 구축해서 제공하고 있지만, 시장규모가 매년 소폭 상승하고 있고 킬러 기술의 부재로 인하여, 본격적인 활성화가 이루어지지 못하고 있음
- 단순 보안 및 제어 서비스 중심의 홈오토메이션 시장에서 네트워크와 센서 기술이 추가된 홈네트워크로 발전하고 있으며, 앞으로는 유비쿼터스 환경 중심의 지능형 홈네트워크로 발전할 전망
- 안전한 홈네트워크 구축을 위해 ETRI 및 일부 보안업체를 중심으로 홈네트워크 보안기술이 개발되었음
  - 정부주도의 홈네트워크 시범사업에 참여했던 소프트포럼은 KT 컨소시엄에 참여하여 전송망 보안을 위한 XecureConnector를 개발하였으며, 이니텍은 SKT 컨소시엄에 참여하여 홈네트워크 시범사업의 전송망 보안을 위한 INIsafe을 개발하였음
  - ETRI에서는 기존 홈네트워크 서비스의 보안기능을 강화하고 사용자 관점에서의 편리성을 제공하기 위한 사용자 인증기술, 접근제어기술, 홈디바이스 인증기술, 홈디바이스 인가기술 등을 개발하였음

○ 이동통신망 보안

- IEEE 802 계열의 무선망에 대한 가입자 인증 및 키 분배 등 관련 보안 기술은 개발, 상용화 되었으며, IP 기반 멀티미디어 서비스를 위한 SIP 기술과 연계하여 인터넷 폰 등의 형태로 개발되어 급속히 확산되고 있음
- 차세대 이동통신으로 IMT-Advanced 이동통신 기술은 고속이동 환경에서 최대 100 Mbps, 고정 또는 저속 이동 환경에서 최대 1 Gbps의 데이터 전송속도로 비대칭/대칭적 패킷 서비스와 방송 서비스를 포함한 다양한 서비스를 IP 기반으로 통합 제공하는 기술을 의미하며 현재까지 IMT-Advanced 관련 보안기술은 진행되고 있지 않음
- 보안 측면에서, IMT-Advanced 시스템뿐만 아니라 다양한 무선통신 시스템과 통합되는 형태로서 기존의 2G, 3G 뿐만 아니라 와이브로, 무선랜 등 다양한 무선망 환경과 2010년 상용화 되는 새로운 IMT-Advanced 망 간의 안전한 서비스 연동 환경에 대한 보안기술개발이 요구 될 것으로 예상됨
- CDMA 휴대 단말기의 무선 인터넷 표준 플랫폼으로 WIPI 2.0이 제정되었으며, 최근 WIPI 플랫폼에서 와이브로, DMB, RFID 서비스 제공을 위한 WIPI 개선 방안이 논의되었으나 WIPI 탑재의 의무화 규정은 구글폰 등 기술적 진화에 대한 영향으로 퇴색되고 있는 상황임
  - 모바일 플랫폼이 최근 급격하게 발전되고 있으므로 망 개방 및 융 · 복합 서비스 등장으로 인하여 악성코드로부터 플랫폼을 보호하는 보안 이슈가 현안으로 등장함
- 현재 국내 이동통신사는 CDMA 방식의 2G 및 3G 인증 시스템을 구축하고 있으며 W-CDMA 방식의 3G에 USIM을 적용한 인증 보안 서비스와 와이브로에 PISIM을 적용한 인증 보안 서비스를 제공하여 단말, 기지국, 교환기, 인증 서버를 운용하고 있음
- 3세대 이동통신시스템 이후를 대비하여 2005년 ~ 2006년까지 ETRI를 중심으로 LTE 시스템을 개발. 관련

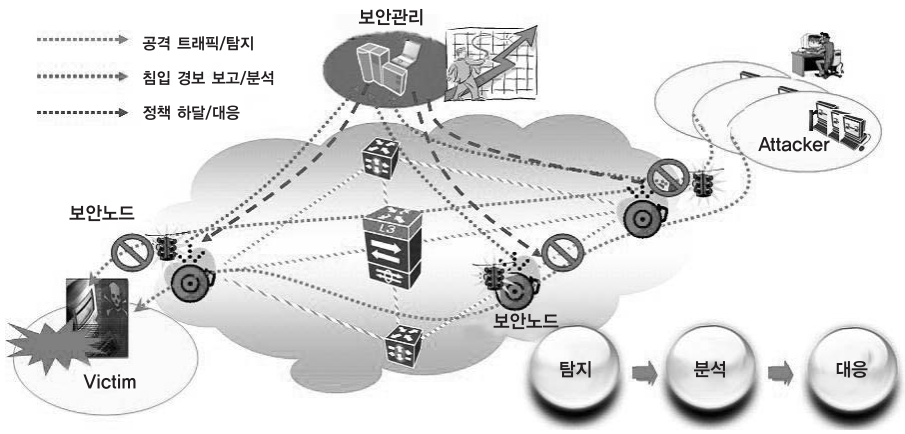
기업에 기술이전을 하였으나, LTE/SAE 시스템에 보안기능이 없어서, 상용화를 위해서는 추가로 Security를 추가적으로 개발 보완하여야 할 상황임

○ 무선근거리통신망 보안

- 무선 인터넷 보안 분야는 국내나 국외나 아직까지 많은 발전 가능성이 있고, 현재에도 꾸준히 연구되고 있는 분야임. 또한, 현재 사용자들의 높은 욕구에 발맞추어 다양한 기술이 선을 보이고 있지만, 그 보안 상태는 아직 미지수로 남아있는 상황임. 무선 인터넷의 보안 문제는 앞으로 네트워크가 통합되는 환경인 FMC와 다양한 사업자가 존재하는 MVNO 환경에서는 더욱 중요하나 문제로 다루게 될 것임
- 국내에서는 주로 데이터 송수신시의 암호화 키 생성과 불법 장비 탐지에 관한 특허가 주를 이루고 있고 무선 인터넷을 위한 보안 프로토콜 모듈을 개발하는 움직임이 활발하게 이루어지고 있으나, 이러한 보안 프로토콜의 근간이 되는 암호 알고리즘에 대한 기술을 직접 보유하고 있는 업체가 적고, 많은 업체들이 외국의 암호 알고리즘 라이브러리를 가져와 개발하는 경우가 많은 것으로 알려져 있고 보안 관련 모듈을 개발했다고 발표를 하더라도 그 제품에 대한 공개적인 성능 평가 내지는 같은 규격의 다른 제품과 상호 연동 테스트가 거의 없어 그 제품에 대한 정확한 평가가 어려움
- 국내 업체들 사이에 자체적인 핵심 기술 개발 및 무선 인터넷용 보안 제품의 개발이 많이 이루어져야 한다고 생각되고 많은 제품의 개발이 이루어져야 업체 간의 선의의 경쟁도 이루어지고, 제품의 공개적인 성능 평가 혹은 상호 연동 테스트가 자연스럽게 이루어질 것이며 특히 보안 기술이 외국 업체에 종속됨으로써 생길 수 있는 문제를 피할 수 있을 것으로 예상됨

○ 차세대 네트워크 보안

- 차세대 네트워크 보안 기술 운영 현황
  - 이기종 망 간 통합 및 여러 사업자 간 연동이 이루어지는 BcN 통합 환경에서 체계적으로 침해사고에 대처하기 위한 통합 정보보호 관리체계 구축과 침해사고 예방 및 대응체계의 고도화 기술임
  - 1.25 인터넷 침해사고 이후 인터넷 침해사고 대응지원센터를 설립하여 긴급대응 및 시스템을 구축하였으며, 민 · 관공조의 침해사고 긴급대응체계 구성 · 운영하고 있음



고성능 네트워크 종합 위협 대응 시스템 개념도

– 차세대 네트워크 보안 기술 개발 현황

- 현재 네트워크 보안은 소규모 네트워크 차원에서 단수 모니터링 및 보안정책을 적용하는 형태이나 향후의 네트워크 보안은 네트워크 전체를 보안 관리 영역으로 확장
- BcN 백본 인프라의 처리능력이 최고 수십 Gbps 수준인 반면 현재의 정보보호 장비의 처리능력은 시장 규모 형성에 맞춰 진행되고 있는 관계로 아직까지 수 Gbps에 불과하여 BcN에 적용하는데 애로점이 있을 수 있음
- BcN 광대역 환경에 적합한 고성능 네트워크 보안장비 개발

– 이상 트래픽을 감지 · 차단 · 대응하는 고성능 네트워크 통합 보안장비와 RFID/USN 환경에 적합한 초경량 암호모듈 및 시큐어 센서 노드 개발 중

○ ETRI를 중심으로 2006년 실시간 하드웨어 기반 100만 세션 동시 처리가 가능하고, 패턴 매칭 · 비정상행위분석 기반의 침입탐지가 가능한 20 Gbps 처리량의 고성능 침해 대응 시스템 개발 완료

○ LG 엔시스, 윈스테크넷, 시큐아이닷컴 등 중소 보안 전문 업체 중심으로 수 기가급 침입 방지 시스템, 방화벽 등의 보안 장비 개발 및 보급

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

○ 국내 무선랜과 와이브로망에 대한 개별접속 보안기술이 개발되었으며, 모바일 RFID 단말기, 무선랜 + 와이브로 단말기, CDMA + 무선랜 단말기 등과 같이 멀티-무선 링크를 지원하는 융 · 복합 단말기 기술이 개발되고 있음

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

○ 사이버공격 역추적/보안관리

– 정부정책기조

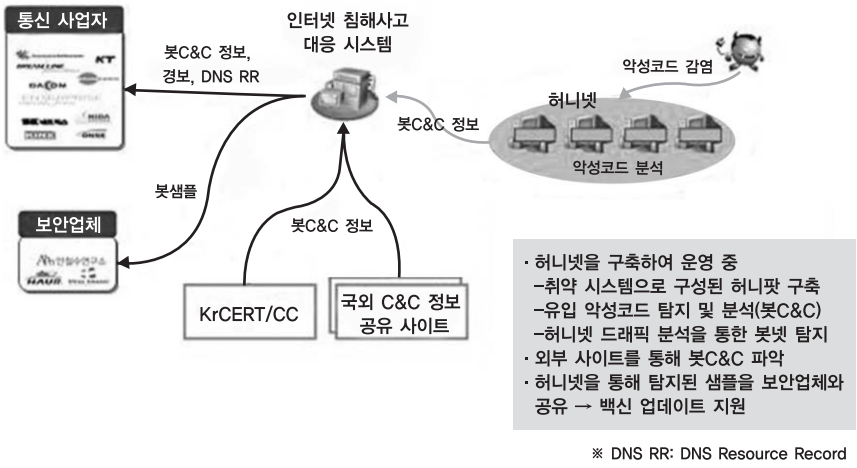
- 기업 IT 인프라의 안전성 보장 및 책임 소재 여부에 관한 규정이나 개인 정보 보호 지침이 강화되면서 보안 서버, 통합 인증 시스템 및 리스크 관리 등 컴플라이언스 관리 기술 개발 및 구축이 확대될 것으로 전망됨
- 주요 정보통신시설에 대한 안전진단의 의무화는 취약점 분석이나 로그 분석과 같은 보안관리 솔루션의 지속적인 수요와 신규 기능의 요구사항 증대

– 국책연구소, 산업계, 학계의 기술개발 현황

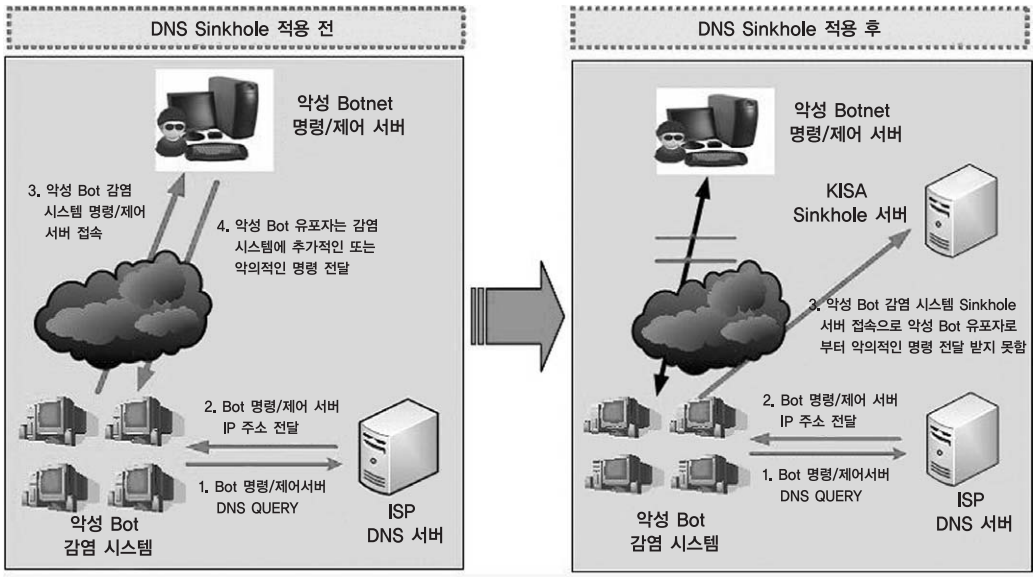
- 보안관리기술은 침입차단시스템, 침입탐지시스템, 가상사설망 시스템 등 다양한 종류의 보안시스템들을 상호 연동하여 각 기능을 통합 관리하는 중앙집중식 관리체계로서, 보안관제서비스 업체, 보안 시스템 개발 업체들 간에 컨소시엄 형태나 독립적인 보안관리 시스템으로 개발되고 있음
- 보안관리기술 수준은 현재 자사 제품에 대한 모니터링 기능이 구현되어 있지만, 앞으로는 보안프로토콜의 표준화를 통해 타사 제품을 포함한 이기종 보안 시스템에 대한 모니터링 기능을 가지도록 발전하고 있으며, 소규모 네트워크 차원에서 단수 모니터링 및 보안정책을 적용하는 형태이나, 향후의 보안관리기술은 네트워크 전체를 보안 관리 영역으로 확장될 것으로 예상
- 단순하게 보안장비를 통합적으로 관리하는 범주에서 벗어나 점차 네트워크 장비 및 시스템까지 연계하여 관리해주는 시스템으로 진화 발전할 것으로 전망되고 있음
- 유무선 통합망의 백본 IP 코아망 인프라의 고성능 처리능력에 비해 현재의 정보보호 장비의 처리능력은 미흡하며, 현재 차세대 네트워크 보안은 소규모 네트워크 차원에서 단수 모니터링 및 보안정책을 적용하는 형태를 초월하여 향후의 네트워크 보안은 네트워크 전체를 보안 관리 영역으로 확장이 전망됨

– 사이버 보안 동향

- 핵심 기술 유출 및 영업 기밀 유출을 통한 피해를 사전에 예방하기 위해 전사적인 보안 관리 체계를 고도화하고 있는 추세
- 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



KISC의 봇넷 대응 프로세스



KISC의 DNS 싱크홀 기술

○ 봇넷 대응

– 기술 동향

• 안철수 연구소와 국방과학 연구소에서는 메모리 감시를 이용하여 봇 서버의 행위를 지속적으로 모니터링

하고 자동 분석하는 봇넷 역추적 기술을 제안했으나 아직 구현 및 검증이 수행되지 않음

- 논문으로 통하여 봇넷 탐지 및 대응 기술이 연구 목적으로 제안되고 있지만, 전문적인 대응 솔루션은 전무한 실정
- KISA를 중심으로 신종 봇넷 능동형 탐지 및 대응 기술이 개발되어 질 것으로 전망

– 봇넷 대응 현황

- KISA의 인터넷침해사고대응지원센터(KISC)에서는 악성 봇 명령 또는 제어 서버로 이용되는 도메인 네임에 대하여 DNS 싱크홀 시스템을 적용, 좀비 PC 조종에 악용되는 봇넷 C&C 서버로의 연결을 차단하고, 허니넷을 통해 탐지된 샘플을 보안업체에 전달, 백신 업데이트를 지원하고 있음
- KISA의 봇넷 대응은 국제적인 Best Practice로 받아들여지고 있음. 그 대응을 살펴보면, Honeynet DNS 로그, 악성코드 수집시스템, 외부 사이트, 사고분석(KrCERT/CC)를 통해 봇C&C 정보를 수집하고, 이를 업체 및 사업자와 공유하고 있으며, DNS 싱크홀을 운영하여 C&C 서버와 봇 좀비간의 통신을 단절시켜 공격에 악용되는 것을 방지하고 있음

○ 서버 보안

– 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 구축 의무화로 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 FreeBSD에서 서버형태로 사용할 수 있는 접근제어, 사용자인증, 암호화 파일 시스템 등의 보안기술을 개발하고 국내업체를 대상으로 기술이전을 통한 상용화를 추진한 바 있으며, 최근 들어 업체를 통해 은행권과 정부 기관의 서버 보안 사업을 수주함
- 2006년부터 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 특허 출원 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, 소프트웨어 무결성 제공 기술에 대응할 수 있는 특허권을 확보함으로써 시장 선점 노력

– 국내 보안운영체제 제품 현황

• TOSS WG/FG(시큐브), RedOwl SecuOS(티에스온넷), Hizard(안랩 시큐브레인), RedCastle(레드게이트) 등이 국내에서 접근통제 기능을 강화한 보안 운영체제로 개발되어 판매되고 있음

○ PC 보안

– 기술 개발

• 안티바이러스 대응기술: 2000년 이전까지 도스용에서 윈도우용까지 컴퓨터 바이러스가 주된 PC 보안 대응기술이었고 네트워크의 발달로 더 이상 파일 매개체를 이용한 바이러스의 감염 방법보다는 네트워크를 통하여 시스템을 감염시키는 웜의 피해로 인한 대응기술로 변화하는 추세로 관련 기술도 이런 악성코드의 변화에 따라 발전하였음. 금전적 목적을 위해 개인정보 유출 피해가 늘고 있으며 UCC와 웹2.0의 확산과 함께 PC 사용자의 피해가 늘고 있음. 보안 업데이트는 필수이고 신뢰할 수 없는 ActiveX와 코덱 등 주의가 필요하며 USB 등 이동식 저장 장치를 악성코드가 전파수단으로 사용하고 있으며 ARP 스푸핑을 이용한 악성코드 유포 및 Packer를 이용 및 변종한 공격 등을 대응할 수 있는 기술로 발전하고 있음

• 안티스파이웨어 대응 기술: 2003년 이후 악성코드뿐만 아니라 PC 보안 분야에서 새로운 공격 형태를 보이는 것이 스파이웨어로 2007년에는 허위 안티스파이웨어 제품들이 전 세계적으로 기승을 부리고 있어서 스파이웨어만큼 피해를 주고 있는 실정임. 안티바이러스 기술과 비슷한 기술로 대응할 수 있으나 별개의 진단법, 치료법등으로 운영되고 있었으며 제품 자체도 안티바이러스 제품과 합쳐지고 있기 때문에 엔진 자체도 통합되고 있는 추세임. 악성코드도 웜이나 트로이목마 등이 별개로 존재하는 것이 아니라 스파이웨어나 애드웨어 등과 결합된 형태로 공격하는 것들도 늘어나고 있기 때문에 하나의 기술로 대응하기엔 역부족임

• 개인 방화벽은 악성코드에 의한 정보 유출 사례가 많아지고 있음에 따라 PC에서 접근제어를 하는 침입차단시스템으로 해킹 위협에 노출되는 것을 방지해줌. 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. 최근 ARP 스푸핑으로 인한 피해가 늘어남에 따라 안티바이러스 기술과 함께 개인방화벽을 이용하여 공격하는 시스템을 확인하고 공격을 받고 있다는 것을 사용자에게 알려주어 추가적인 피해를 줄이는 기술이 결합되고 있음

• 특정 목적, 특히 금전적인 목적을 위해 정보를 유출하는 악성코드 등 보안 위협이 증가함에 따라 내부 정보를 보호하고 유출 방지를 위한 내부정보 유출 방지 기술은 정보의 이동을 제어하는 것으로 내부자의 부정 행동을 감시, 통제하며 도구로 사용될 수 있는 모든 매체(외부 저장 장치, 메일 등)를 감시, 차단하는 역할을 하고 있음. 크게 인쇄를 통한 정보 유출 감시, 저장 장치를 통한 유출 방지, 네트워크를 통한 유출 방지 등으로 구분됨

○ 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

• 지식경제부는 IT 신성장동력 사업의 일환으로 ETRI가 주관이 되어 산학연이 협력하여 국산 파일에 특화된 기능을 내장한 디지털포렌식 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 모의실험, 기업 간 법적 분쟁, 기업 내 기술유출 등의 영역에서 포렌식 솔루션 및 서비스 도입이 활발해 지고 있음

2.2.2. 국외 기술개발 현황 및 전망

○ USN 보안

– USN 주요국가의 정책기조

• 미국은 NITRD[48] 주관의 8개 분야로 나누어 연간 20억 달러 규모의 거대 연구가 DARPA, UC Berkeley에서 진행 중이며 각종 비즈니스 및 서비스 모델 개발에 전 부처가 박차를 가하고 있는 중임

• EU의 IST[49] 프로그램이 주축이 되어 복지 서비스를 목표로 Bio-MEMS 기술 등에 R&D가 이루어지고 있음

• 일본은 산학이 중심이 되어 2010에 UNS(Ubiquitous Network Society) 구현을 목표로 센싱 기술 개발에 많은 역량을 투입하고 있는 것으로 보고됨

○ 휴대인터넷 보안

– 와이브로는 무선 접속기술에 있어서 4G 무선 전송 기술로 채택이 확실히 되고 있는 OFDMA 기술을 이동통신 시스템으로는 최초로 도입하였으며, 스마트 안테나 기술과 다중안테나(MIMO)기술을 적용해 경쟁 시스템들보다 구축비용 대비 최고의 데이터 전송 속도 구현 가능

– 2006년부터 OFDMA, MIMO 등 핵심 기술을 상용 서비스 과정에서 검증을 통해 안정화를 이루었기 때문에 향후 4G 이동통신 표준화 시 3GPP LTE, 3GPP2 UMB 등 경쟁 기술들에 비해 유리한 고지 점령

– 와이브로의 시스템 경쟁력 확보를 위해 정부출연연구소와 민간산업체에서 2006년부터 고속 이동 환경에서

48) Network and IT R&D

49) Network and IT R&D

40MHz 대역폭 사용해 최대 400Mbps 데이터 전송을 가능해 하는 와이브로 진화기술, 와이브로 에볼루션 기술 개발을 추진 중. 이는 ITU 4G 기준 만족시킬 수 있으며, 2008년까지 개발 완료하여 2010년 예정인 ITU 4G(IMT-Advanced)표준에 반영 추진 예정

- 미국 기술개발 현황 및 전망
  - 미국은 전역에 와이맥스 서비스를 상용화 할 계획
  - 2008년 말까지 Sprint와 Clearwire는 미국 전역에 와이맥스 망을 공동 구축하기로 합의했으며, 이를 위해 각자 담당지역에서 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, 인스턴트 메신저, 이메일 등 애플리케이션을 제공
  - 이에 따라 2010년에는 총 1억 2500만 명이 와이맥스 서비스를 사용할 수 있을 것으로 전망
- 일본 기술개발 현황 및 전망
  - 일본 역시 2007년 5월 도시바와 노텔이 와이맥스 기지국을 공동 개발
  - 2010년 40억 달러로 추산되는 와이맥스 기지국 시장에 대응하기 위해 제휴를 맺고 일본 내 사업은 도시바가, 해외사업은 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 4억 달러로 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

- 가정 내 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 홈 서버로 제공하기 위한 기술개발을 진행 중
- 마이크로소프트, 인텔, 소니, 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
- UWB 및 무선 1394와 같은 광대역 무선 기술과 지그비 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 OFDM와 Dual-band DSSS 중 표준안을 선택하는 작업이 진행 중
- 유비쿼터스 홈컴퓨팅 분야는 MIT, IBM, 마이크로소프트, 소니, 파나소닉, ESPRIT 등 선진기관에서 주변 환경에 따라 다양한 가전기기들을 동적으로 연결하여 서비스를 제공할 수 있는 상황 적응형 미들웨어 기술 개발을 진행 중이며, 시장 활성화를 위한 장비 및 소프트웨어 업체간의 결속 등 DLNA 표준 활동을 통한 기기 간 상호운용성 기술과 유비쿼터스 홈 구축을 위한 상황 적응형 미들웨어로 발전할 전망
- 지능형 정보가전 분야는 홈센서 간 정보 교환이 가능하도록 홈센서가 지능화되고 착용 가능한 형태로 발전하고, RFID 및 유비쿼터스 ID를 기반으로 다양한 정보를 제공할 수 있도록 발전할 전망이며, AT&T, 마이크로소프트, 인텔, HP, MIT의 미디어 랩 등에서 광대역의 저전력 무선 칩셋을 이용한 유비쿼터스 컴퓨팅 기술 개발을 강화
- 홈네트워크 보안기술은 홈 게이트웨이 플랫폼을 통한 보안성 확보에 연구가 집중되고 있음
  - 홈 게이트웨이 플랫폼에 VPN, 방화벽 기술을 적용하여 외부 망과 홈 게이트웨이 사이의 보안성을 확보하기 위한 상용제품이 개발되었음
- 미국의 케이블회사들이 주축이 되어 개발된 CableHome 기술은 홈 게이트웨이 장치 인증, 컨트롤 데이터 및 다운로드 소프트웨어의 암호화 제공, 원격 홈 게이트웨이의 방화벽 기능 등을 지원함
- 일본 NTT 데이터, 후지쯔, 미쯔비시, 도쿄공업대를 중심으로 개인키를 포함한 스마트카드를 이용하여 원격지에서 홈네트워크를 관리하는 방안 연구 중임
- 사용자 인증, 정보가전기기 인증, 접근권한 제어, 정보의 무결성과 기밀성을 지원하는 HAVi, UPnP, Jini, OSGi 미들웨어 정보보호 기술이 연구되고 있음

○ 이동통신망 보안

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

– 최근 CDMA + RFID, 무선랜 + 와이브로, CDMA + 무선랜 단말기 등과 같이 무선 멀티-링크 간 융?복합 보안 서비스 기술을 미국, 유럽에서 연구개발 중

– 미국은 IEEE802 무선 네트워크(802.11, 802.15, 802.16, 802.20)간 상호 연동 및 융?복합, IEEE 802 무선망과 이동 인터넷 간 연동 기술을 개발

– 차세대 이동통신망 보안 기술 현황

  • 차세대 이동 통신 시스템의 보안 위협으로 휴대 단말, 기지국 및 관리 서버의 공격을 통한 사용자 기밀정보 유출, 위장, 불법 사용, 정상적인 서비스 방해를 방어하기 위한 지속적 보안 기술 개발 필요함

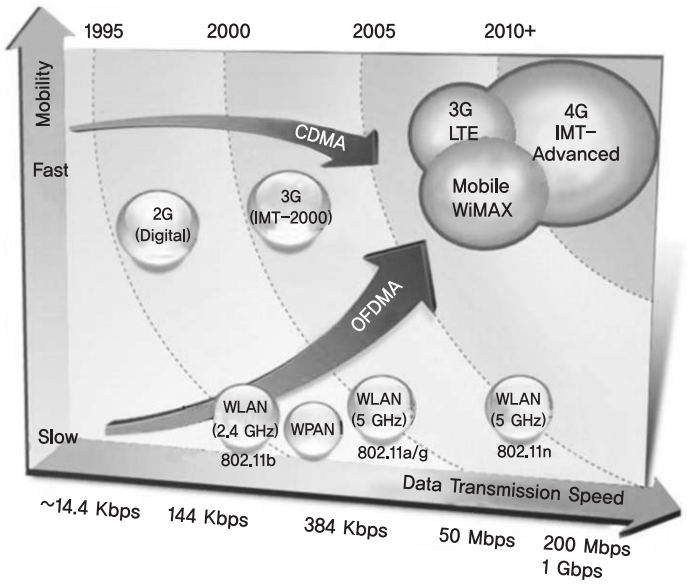
  • LTE 시스템은 3G와 하위호환성[50]을 가지고 있으므로 공유키 방식을 적용하고 있는 3G 표준과 인증 보안을 유지한 채로 IP환경에 적합한 인증(예: EAP-AKA)을 추가하여 제공해야 하며, 보완적으로 공개키 기반으로 보안 기법 제공과 보안 정책 서버를 추가하는 등의 안전성 강화가 요구됨

  • ETRI는 2008년 1월 삼성전자 · KTF와 함께 세계최초로 3GPP LTE 이동 통신 시스템을 개발

– 노텔, 에릭슨은 LTE 시스템 장비를 선보이고 4G를 구현할 수 있는 세계 최고 속도의 장비를 시연하였으나 보안기술에 대하여는 아직 추가 개발 없는 상태임

  • LTE 시스템은 단말기간의 성능이 하향링크 105Mbps, 상향링크 65 Mbps 임

  • 향후 상용제품이 완성되면 실제 차량이 3Km/h의 저속 이동 중 100 Mbps, 고속인 120Km/h로 이동 중에도 30 Mbps의 표준규격을 만족하는 초고속 멀티미디어 서비스 제공 가능



이동통신의 기술 발전 방향

50) backward compatibility

○ 무선근거리통신망 보안

- 무선랜을 위한 보안 기술은 IEEE 802.11i로 정의되어 사용되고 있음. WiFi 에서 제안한 WPA, WPA2와 인증 서버를 활용하는 802.1x, 인증서를 활용하는 기법, 기존 802.11 표준의 WEP[51]을 모두 포함하고 있음. 요구 보안 정도에 따라 단계별로 적용 가능한 보안 표준으로 설계되었지만 초기 무선랜을 바탕으로 하였기 때문에 부분적으로 취약점이 발생함. 이에 따른 후속 조치로 다양한 워킹그룹이 구성되어 운용되고 있음
- 무선랜의 보안 문제점은 성장을 더디게 하는 부정적인 면으로 인식되어 왔음. 최근 무선랜을 통한 해킹이 급속히 확산되는 등 사회 문제로 인식되면서 관련 연구들이 진행되고 있음
- 무선랜 연구의 방향은 현재 제안된 표준안의 취약점을 보안하는 방향 및 애드혹 네트워크를 발전시킨 메쉬 네트워크로의 발전 방향, 유선 네트워크에 서비스되고 있는 다양한 보안기법을 무선 네트워크로 전환시키는 방향으로 진행되고 있음
- 무선랜 보안과 관련된 표준은 ITU와 IEEE가 양분해서 가지고 있지만 실질적인 주도권은 IEEE 802.11이 가지고 있음. IEEE 802.11은 표준의 취약점을 보완하기 위해서 802.11i 이후 서브 그룹을 통해서 관리 프레임의 보호, 이종 네트워크와의 핸드오프, 메쉬 네트워크의 보호, 로밍 환경에서의 키 구조개선 등을 목적으로 연구를 진행하고 있음
- 차세대 네트워크의 실질적인 모델로 인식되고 있는 메쉬 네트워크로의 발전을 위해서 IETF의 MANET과 IEEE의 802.11s의 두 가지 연구 그룹이 진행되고 있음
- 기존의 유선 네트워크의 보안 기법은 크게 방화벽과 침입탐지시스템 그리고 인증시스템으로 볼 수 있음. 현재 무선랜에 이러한 기법을 도입하기 위한 연구가 진행되고 있음. 강력한 보안 기능을 요구되고 무선랜 자체의 성능이 발전함에 따라 유선랜과 상응하는 보안 기술이 활용할 수 있게 되었음. 모든 연구들은 무선랜의 환경에 적합한 기술을 개발하기 위해서 진행되고 있으며 대표적으로 무선 VPN과 무선 PKI가 있음
- 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 편임
- 무선 PKI는 기업의 내부행정, 전자결제, 그룹웨어 등을 휴대폰 및 PDA로 처리할 수 있는 모바일오피스, 제조 및 도소매 유통에 필요한 업무 프로세스를 무선 환경을 통해 구현한 물류정보 서비스, 무선 환경에서의 시스템 관리 및 원격제어가 가능한 원격제어 · 검침서비스, 전자결제를 통한 무선 전자상거래 등의 기업정보 보호 등에 적용

○ 차세대 네트워크 보안

- 차세대 네트워크 보안 기술 운영 현황
  - 미국은 통신망 보안 이슈에 대한 조사와 통신망 보안을 위한 권고사항 작성, 사이버 보안을 위한 국가 전

51) Wireless Equivalent Privacy

략발표, 국토안보부 신설, GEWIS[52] 구축 추진 등 사이버 보안활동을 활발히 추진 중

- EU의 경우 사이버 보안을 위한 국가 간 정보보호 협력체계 구축하고 있으며 유럽 네트워크 및 정보보호 기구를 설립하여 정보보호 주체간의 협력을 강화하고 있음
- 일본의 경우 정보보호대책 추진실을 설치하여 정보보호 대책의 기획 및 입안, 기술자문, 사이버공격대응 등의 업무를 수행

– 차세대 네트워크 보안 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

- 통합 유무선 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

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

○ 사이버공격 역추적/보안관리

– 주요국가의 정책기조

- 미국은 1991년 말 정보통신 기술개발과 응용을 촉진하기 위해 고성능 컴퓨터 법을 제정하였으며, 1993년에는 이 법에 따라 미국 경제의 경쟁력을 높이고 세계의 주도권을 확보하기 위하여 미국의 국가적인 정보화 전략[53]을 발표했으며, 그에 따라 네트워크 보안기술 및 컴퓨터 시스템 보안기술의 정책 마련
- 중국은 컴퓨터 바이러스에 의한 테러가 원자탄을 사용하는 것보다 효율적인 전략 방법이라는 판단 하에 1999년 해커부대를 창설하였고 대만을 대상으로 2000년 8월 7만 2000건의 사이버 테러 감행
- 일본의 경우 사이버 테러 전에 대비 2000년 말 사이버부대를 창설하고, 테러공격을 방어하기 위해 1억 4000만 엔의 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 보안관리기술 관련 연구프로젝트는 전

52) Global Warning Information System

53) NII, National Information Infrastructures

세계적으로 2004년 전후에 시작하여 개별적으로 점점 확대되어 SIFT[54], NVAC[55]등에서 활발히 진행 중임

- 보안관리기술 중 사이버공격 추적 기술 실현을 위해 전 세계적으로 연구가 초기 단계에 있으며, 현재 이와 관련하여 DETER[56], EMIST[57], ARDA[58]의 Network Attacks Traceback 연구가 매우 활발히 진행되고 있음
- 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

○ 봇넷 대응

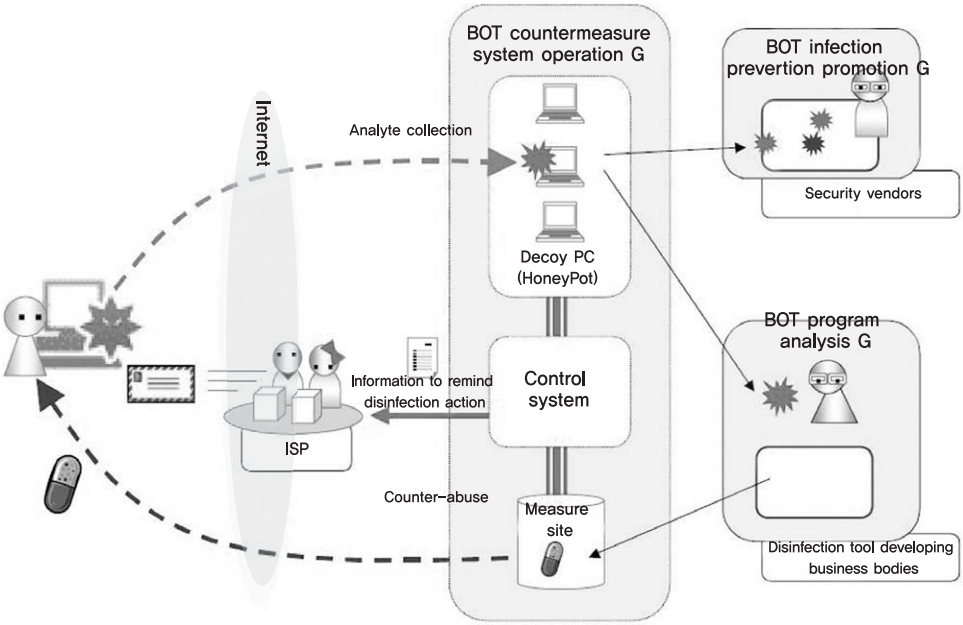
– 기술 동향

- IRC, HTTP, P2P 봇넷 대응을 위해 호스트 및 네트워크 각각에서 시그니처 및 행위 기반 탐지 솔루션이 연구 · 개발되고 있음
- McAfee, Trend Micro, FireEye, Damballa, Arbor 등에서 솔루션이 개발되었음
- Georgia 공대, 노스캐롤라이나 대학, 암스테르담 대학 등에서 봇넷 대응 수단이 연구되었으며, 관련 컨퍼런스로 USENIX SRUTI, USENIX HOTBOT 등이 있음
- 과거 네트워크 기반의 시그니처 분석 탐지 방법은 초기 IRC 봇넷이 가지는 특정 포트 사용, 특정 DNS 주소를 C&C 서버로 사용하는 경우에 효과적인 탐지 및 차단이 가능했지만, 최근 지능화된 봇넷은 암호통신, C&C 인증, Fast-flux 등의 회피기술을 사용하기 때문에 기존의 시그니처 기반 방법으로는 신종 봇넷에 대한 대처가 어려움. 따라서 능동적으로 신종/변종 봇넷의 탐지와 대응을 위해서는 네트워크 기반의 이상행위 탐지 시스템 개발이 요구됨
- 최근 OS와 애플리케이션의 서비스 패치가 활발하게 이루어짐으로써 애플리케이션이 가진 취약점을 이용해 유입되는 악성코드보다는 이메일, 메신저, 웹서비스를 통한 유입이 더욱 증가하는 추세이므로 기존의 탐지 방법으로는 한계가 있기 때문에, 호스트 기반 Packing, 압축, 암호화를 통한 악성코드의 다양한 변종 바이너리 생성 방법에 대한 연구 및 분석이 필요함

– 봇넷 대응 현황

- 일본의 봇넷 대응
  · 최근 급증하고 있는 봇넷, 악성코드 등 역기능방지 · 예방을 위한 활동을 목적으로 경제산업성과 공동으로 CCC(Cyber Clean Center)를 2006년 12월 오픈

54) Security Incident Function Tools
55) National Visualization and Analytics
56) Cyber Defense Technology Experimental Research
57) Evaluation Methods for Internet Security Technology
58) Advanced Research and Development Activity



CCC의 봇넷 대응 프로세스

- 총무성과 경제산업성의 공동사업으로 일반국민을 대상으로 악성봇에 관한 정보제공
- 봇에 감염된 PC의 IP를 식별하고 ISP와 협력하여 봇 제거 툴 무료다운로드를 실시하여 감염된 PC를 치료하는데 초점을 두고 있음
- 사이버클린센터는 총무성과 경제산업성이 운영하는 사이버클린센터 운영위원회를 중심으로 IPA, JPCERT, Telecom-ISAC이 실무를 담당

• 중국의 봇넷 대응

- CNCERT/CC의 봇넷 대응은 크게 봇넷을 모니터링하여 제거하고, 정보를 공유하는 대응체계를 구축하고 있음.

• 유럽의 봇넷 대응(ENISA(네트워크 및 정보 보호 기구))

- 봇넷 특징, 동향, 위협요인, 대응방안 제시함.

• 인도의 WAZ

- 인도 CERT는 윈도우 플랫폼에서 실행되는 악성 봇의 DDoS 공격을 막는 안티 DDoS 툴을 개발하였으나 아직 상용화 되지 않았음

○ 서버 보안

– 주요국가의 정책기조

- 미국은 정부 차원에서 보안 운영체제를 개발하고 있으며, 기존의 마이크로 커널 기반으로 개발하던 정책을 최근에는 공개 운영체제인 리눅스를 기반으로 연구를 진행하고 있음
- 특히 NSA 주도로 개발된 SELinux가 기존 리눅스 운영체제 커널로 장착됨에 따라 보안 운영체제 시장에 변화를 가져오고 있으며, SELinux의 활성화를 위한 정부와 민간 차원의 연구가 활성화되고 있음
- 유럽은 미국 TCSEC과 통합된 국제공통평가표준(CC)에 맞게 PP 등을 개발하고 그에 알맞은 기술 연구가 진행 중에 있음
- 일본에서는 리눅스를 기반으로 한 많은 보안 운영체제가 개발되었고 SELinux에 대한 연구도 병행되고 있음

– 기술 개발 현황

- 미국의 NSA[59] 주도하에 정부차원으로 국가정보기반 구조를 구축하고 국방용으로 사용하기 위해 1992년부터 DTMach 시스템 연구를 시작으로 보안 구조를 연구하였고 이러한 연구를 계승하여 Fluck/Flask 프로젝트를 수행하여 보안 정책의 유연성과 높은 보안 수준을 제공하는 보안 구조를 개발함
- NSA에서 개발한 Flask 구조를 리눅스에 적용하여 SELinux를 개발하여 현재 리눅스 커널에 기본으로 탑재함

– 주요 국가별 특허 출원 동향

- 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(RBAC) 방법, 강제적 접근제어(MAC)가 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

○ PC 보안

– 외국의 경우 악성코드의 숫자가 기하급수적으로 늘어남에 따라 행위기반에 대한 연구가 가속화되고 있으며 시그니처 기반 진단을 보완하고 있음

– 기술주기가 약 1년에서 1.5년 정도 빠르게 진행되고 있고 악성코드의 변화와 플랫폼의 변화에 밀접한 연구를 하고 있으며 가상화에 대한 연구 진행 중

– 가상화란 악성코드 자체가 가상화 환경에서 동작할 수 있기 때문에 그에 대한 대비와 반대로 가상 환경에서 악성코드를 판단하는 기술 등이 연구 중

59) National Security Agency

– 악성코드에 대한 자동 분석 시스템, 자동 분류 시스템 등의 연구 및 운영을 하고 있으며 자동 시그니처에 의해 처리되고 있음

○ 디지털포렌식

– 주요국가의 정책기조

• 미국: 1990년대 초부터 이미 디지털포렌식을 도입되어 FBI를 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 디지털포렌식 활용으로 2006년 12월부터 발효된 개정 미국연방민사소송법률안 ESI에 대한 내용이 추가됨에 따라 기업의 입장에서 포렌식 툴을 이용한 전자적 증거물인 ESI[60]에 대한 관리 및 빠른 식별의 중요성이 증대됨[61]

· 유럽에서는 1995년에 포렌식 관련 지식 및 포렌식 수사 경험을 공유하기 유럽의 포렌식 연구 협회인 ENFSI[62]가 결성되어 정기적인 포렌식 세미나와 공동 연구를 추진하고 있음. 또한 네덜란드의 NFI[63]는 포렌식 관련 수사 및 연구 개발을 추진하며 포렌식 교육과 전문 인력을 양성하고 있음

– 기술개발 현황 및 전망

• 디지털포렌식 툴을 상용화한 국가 중 가장 큰 기술력과 시장규모를 가지고 있는 나라는 미국이며, 영국, 프랑스, 러시아 등도 분야별로 디지털포렌식 기술을 독자 개발 중에 있음

• 상용 컴퓨터 포렌식 툴은 Guidance Software사의 Encase, AccessData사의 FTK 등이 출시되어 있으며, 최근에는 대용량 데이터에 대한 고속 검색 및 분석 기술, 다양한 모바일 폰에 대한 포렌식 기술, 기업의 중요 데이터에 대한 관리 및 검색을 위한 e-Discovery용 포렌식 기술 개발이 활발히 진행되고 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 Software사도 Neutrino라는 모바일 포렌식 제품을 개발하고 있음

2.2.3. 국내외 IPR 보유현황 및 확보 가능분야

○ USN 보안 기술

– 주요 국가별 센서네트워크 관련 특허 출원 동향

• 미국: 20여 건 정도만 다보유 출원인인 경우 조사되어 있음

60) Electronically Stored Information

61) ESI의 민사소송 개시를 보통 e-Discovery라 함

62) European Network of Forensic Science Institutes

63) Netherlands Forensic Institute

- 유럽: 2건
- 일본: 한국 RFID/USN협회에 따르면 200여 개의 특허가 출원 및 등록되어 있으며, 주로 기업이 출원인으로 재산권을 확보해 좋은 상태 임

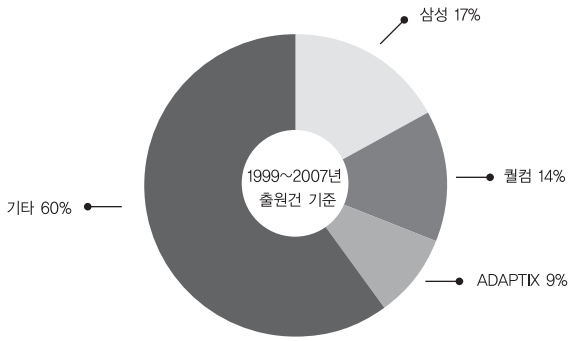
○ 휴대 인터넷 보안 기술

– 국내 특허 출원 현황 및 전망

- 2.3 Ghz 대역을 활용한 와이브로를 위한 국내 표준화에 포함되는 특허 출원 분석을 위해 TTA 홈페이지, 2.3 Ghz 대역을 활용한 휴대인터넷을 위한 국내 표준특허 기술 리스트를 조사한 결과, 삼성전자, SKT, KT, ETRI, 하나로통신 및 KTF를 포함하는 공동출원이 많은 것으로 나타났으며, 와이브로와 관련된 특허 출원은 아래(아래) 그림에서 보듯이 다중접속 및 듀플렉스 기술(37%), 자원관리 및 효율증대(26%), 무선링크제어 기술(18%)순으로 물리계층과 매체접속 제어계층에 대한 출원 내용이 많이 포함
- ETRI에 의해 와이브로가 세계 표준으로 채택돼 2024년까지 6,800달러의 기술료 수입 전망

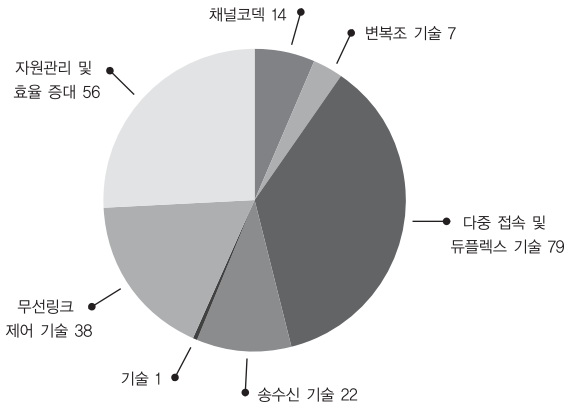
– 국외 특허 출원 현황 및 전망

- 와이브로 특허권 문서에 대한 권리를 삼성전자가 22%, 미국 인텔이 15% 보유[64]



OFDMA 핵심기술 관련 미국 특허 등록 현황

64) 한경, 2007/10/19



와이브로 국내 특허 출원현황[65]

- 와이브로 국제표준특허
  - · 국내 와이브로 국제표준특허 21건, 예상 로열티 47.8백만 불[66]
  - · 삼성전자 와이브로 특허비중 25%
  - · 삼성전자는 휴대인터넷 분야에서 203건의 특허를 출원, 출원건수 세계 1위, 2위는 미국 루슨트테크놀로지(135건)가 차지했고 한국전자통신연구원(78건)임[67]
- 와이브로의 ITU 3G IMT-2000 공식 표준명 OFDMA[68] 핵심기술에 대한 미국 특허 등록 현황
- 한국은 와이브로 필수기술 항목인 무선링크 제어, 다중접속, 듀플렉스 기술에서 미국, 일본, 유럽에 비해 강점을 보이고 있음
- 특히 핵심기술인 OFDM 기술은 미국, 일본, 유럽에서 출원된 전체 특허 중 삼성전자, ETRI 등이 출원한 특허가 51% 차지

○ 홈네트워크 보안 기술

– 국내 특허 출원 현황 및 전망

- 홈네트워크 보안 분야에서는 인증 및 접근제어 분야에 대한 특허가 가장 많으며, 그 외 홈네트워크 보안관리, 홈시큐리티, 홈서비스 보안 등에 대한 특허가 출원 및 등록된 상황임

65) 특허청 전기전자심사본부, 와이브로 기술 분야 특허 출원현황
66) 방송통신위원회(구 정통부)
67) 특허청
68) 직교주파수분할 다중접속방식, Orthogonal frequency division multiple access

- 2002년경부터 홈네트워크 보안 특허가 출원되기 시작하였으며 본격적으로 2004년부터 꾸준히 증가하고 있는 추세임. LG 전자와 ETRI 등이 가장 활발히 특허 출원을 하고 있음

– 주요 국가별 특허 출원 동향

- 국내와 마찬가지로 홈네트워크 보안 분야에서는 인증 및 접근제어 분야에 대한 특허가 가장 많으며, 그 외 홈네트워크 보안관리, 홈시큐리티, 홈서비스 보안 등에 대한 특허가 출원 및 등록된 상황임
- 미국이 가장 많은 특허를 출원 및 등록하였으며, 그 뒤를 따라 유럽, 중국 등에서 출원한 특허가 많음. 일본의 경우는 상대적으로 적은 특허 출원 현황을 보이고 있음

○ 이동통신망 보안 기술

– 국내 특허 출원 현황 및 전망

- 전체 특허 동향에 있어서 IMT-2000이후 이동통신 전반의 연구개발 활동이 위축된 상태이며 4G에 해당하는 기술의 출원으로 연결되는 과도기로서 전체 특허가 주춤하는 시기임
- 4G의 다중접속기술에 대한 특허 출원은 초기 단계이며, 기존 셀 간 간섭 및 완화 기술 등 적용관련 특허 및 MIMO 관련 특허는 포화 상태임
- 삼성전자 및 LG전자는 2세대, 3세대에서의 성공을 발판으로 차세대 원천/핵심특허의 확보를 위해 이동통신 분야의 ETRI 등과 협력하여 4G(IMT-Advanced)에 대한 특허 출원 활발하게 추진되고 있으나 상대적으로 보안 기술에 대한 핵심 특허는 저조한 실정임
- 이동통신망 보안관련 특허에서는 이동통신망 자체에 대한 핵심 특허 보다는 통신망간 연동 보안 특허, 이동단말의 USIM 관련 특허, 모바일 뱅킹 등 이동통신 보안 응용 서비스에 대한 특허가 활발히 출원되고 있음
- 한국에 출원한 이동통신 보안관련 특허는 SK텔레콤, ETRI, 삼성, LG 등으로 이루어져 있음

– 주요 국가별 특허 출원 동향

- 전체적으로 미국의 특허 건수가 가장 많고 특허 증가세로만 놓고 볼 경우, 한국이 가장 높으며, 일본과 유럽의 출원 건수는 비교적 적은 수준임
- 미국, 일본 유럽에서는 다중접속 및 듀플렉싱 기술 분야의 출원이 활발하며, 무선링크 제어 기술은 한국에서 가장 활발히 출원되고 있음
- 이동통신망 보안 기술 관련해서, 아직 4G 관련 보안기술의 특허 출원은 미미한 수준이며, 이동단말의 보안기술, 멀티미디어 서비스 응용 보안기술, 망간 연동을 위한 보안기술이 대부분을 차지하고 있음

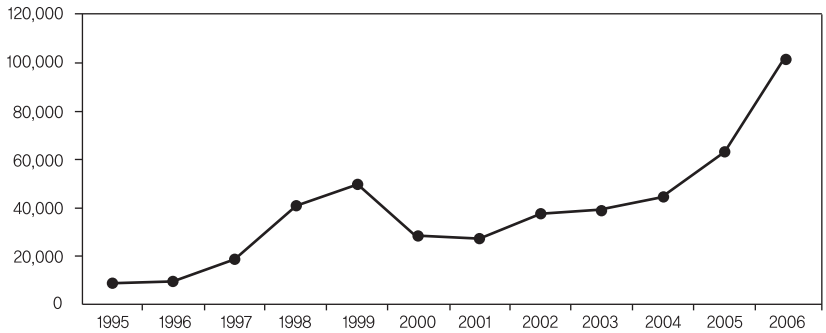
○ 무선근거리 통신망 보안 기술

– 국내 특허출원 현황 및 전망

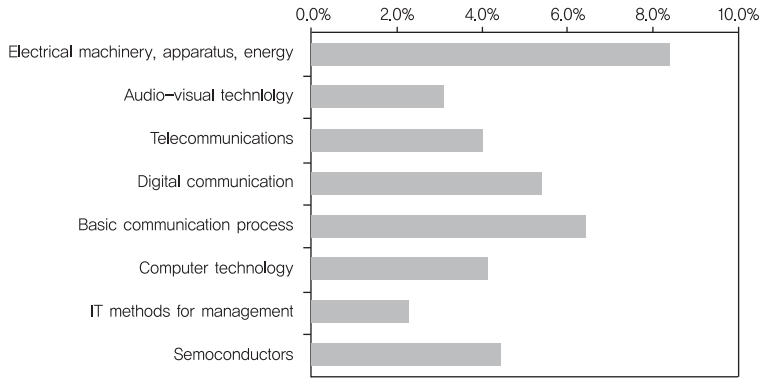
- 전체 특허 출원 동향은 802.11n draft 2.0 출현 이후로 다소 주춤한 실정임. 물리 계층의 효율성을 높이기 위한 스마트 안테나, MIMO 기술이 특허의 대부분을 차지하고 있음. 단말의 인증 방법, 접속 제어 기술 등

이 주로 다루어지고 있고 보안 관련 기술은 미진함. 특허의 대부분을 삼성전자, LG전자와 같은 대형 기업과 ETRI와 같은 연구기관에서 주도하고 있음

- 현재 802.11n의 draft를 기준으로 많은 제품이 시장에 나와 있는 상태로 차후 실제 표준이 제안됨에 따라서 관련 기술이 연구될 것으로 예상됨. 802.11 무선랜의 취약점을 분석하고 보완하기 위한 표준들이 제안되면 그 표준들에 기준한 연구들 또한 활발해질 것으로 예상됨



한국인의 국내외 특허 등록 건수[69]



전기공학 계열의 세부 분야별 세계 대비 한국인 특허 등록 비율(2001~2005년)

– 주요 국가별 특허출원 동향

- 국내에 출원된 기술의 대부분이 미국에도 출원되어있는 것으로 알려져 있음. 관련 기술이 널리 보급됨에 따라 관련 기술 분쟁이 증가하고 있음

69) WIPO

○ 차세대 네트워크 보안

– 국내 특허 출원 현황 및 전망

- 노드들 간 메시지 인증 방법, 이기종망 간 빠른 핸드오버 서비스 제공 방법, 비디오 뱅킹 등 고도의 보안을 요하는 서비스 등을 위한 트래픽 암호화 방법, 사용자 인증 메시지 보호 및 이를 위한 보안키 생성 방법, 암호화된 초고속 광대역 신호의 송/수신 방법 등으로 현재 특허 출원이 되어 있음
- 차세대 네트워크 보안 자체에 대한 특허 기술은 많이 공개되고 있으나, 보안과 연계된 특허는 그렇게 많이 보이지 않고, 특히 국내에서는 출원 기관으로 판단해 보면 주로 ETRI, 삼성전자, KT 등이 주도를 하고 있음
- 현재 대부분의 서비스가 모바일 환경이 주가 되고 있는 상황을 반영하듯, BcN 보안 역시 모바일 환경에서의 서비스 및 기존의 유선환경에 연동하는 부분이 많이 고려되고 있어 공통보안 플랫폼, 구조와 서비스에 대한 특허가 출원될 것으로 예상

– 주요 국가별 특허 출원 동향

- 국내에 출원된 기술이 대부분 미국에 출원되어 있으며 특이한 점은 국내와 다르게 광대역 네트워크를 위한 프로세서 모듈 자체의 보안과 광대역 시스템을 위한 시스템의 메모리 보호와 같은 네트워크망이 아닌 적용되는 시스템 구조 및 시스템 보안 구조에 대한 특허들도 다소 있음
- 차세대 네트워크 보안 기술에 대한 특허는 미국을 제외하고는 찾아보기 힘들며, 국내와 비슷한 수준으로 특허가 출원되어 있는 것 같음

○ 사이버공격 역추적/보안관리

– 주요 국가별 특허 출원 동향

- 1992.1.1~2005.5.26 기간 중 한국/미국/일본을 대상으로 검색
- 기술별 등록 특허 추세 관점에서 보안 이벤트 시각화 기반의 분석 기술은 2000년도부터 특허 출원이 시작되었으며, 특허 출원 완료 예상기간이 2년 정도의 소요됨을 고려하면 2003년 기준으로 타 분야 대비 출원 완료가 급증 추세에 있음
- 국가별 보안관리기술의 등록특허 동향에 관한 그래프로 미국, 한국, 일본, 유럽 순위로 나타나고 있으며, 이는 보안관리기술의 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 것

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

○ 봇넷 대응

– 주요 국가별 특허 출원 현황 및 전망

• 연도별 특허출원의 동향

- 봇은 웜, 바이러스, 백 도어, 루트 킷 등 다양한 악성 코드 등의 특성을 복합적으로 지니고 있는데, 봇을 포함하는 악성코드에 대한 탐지 기술의 국가별 출원 추이는 한국/미국/일본/유럽 모두 2000년부터 2002년 사이 관련된 출원 건이 가장 많음. 이러한 특허 출원의 급성장은 2000년도 이후 초고속 인터넷망 보급과 맞물려 여러 가지 변종 바이러스에 대한 문제가 제기 되면서 이를 방지 및 치료 하는 기술에 대한 연구 활동이 활발해진 것이 주요 원인으로 분석됨
- 미국이 1992년부터 관련 기술을 출원하기 시작하여 372건으로 가장 많은 출원건수를 보여주고 있으며, 일본이 216건, 한국이 147건을 출원하였으며, 한국은 해당 분야에 대한 연구가 꾸준히 늘고 있는 것으로 보임
- 전체 출원건이 2004년 이후에는 출원량이 2000년도 보다는 점차 줄고 있기는 하나 해마다 꾸준한 출원량이 있는 것으로 보아 늘어나는 신종 악성 봇에 대한 연구가 지속적으로 이루어지고 있는 것으로 보임

• 기술별 특허출원의 동향

- 기술별 출원 추이를 살펴보면 2000년도에서 2002년까지는 호스트 기반 악성코드 탐지 기술에 대한 출원이 많았으나 2003년을 기점으로 IRC/HTTP 봇넷 관련 네트워크 기반의 탐지 기술의 출원이 점점 더 많아지고 있음
- 미국과 일본은 IRC/HTTP 봇넷 관련의 기술을 많이 출원한 반면 한국은 호스트 기반의 악성코드 탐지 방법에 대한 특허 출원이 많은 것으로 나타났음

봇넷 대응 기술 분류 체계에 따른 국가별 특허 보유 건수

대분류	중분류	검색건수					
		유럽	일본	한국	미국	PCT	합 계
신종봇넷 탐지 및 대응기술	IRC/HTTP 봇넷 능동 탐지/분석기술 개발	22	122	63	203	43	453
	P2P 봇넷 능동 탐지/분석 기술 개발	–	1	2	–	–	3
	호스트 기반 악성코드 탐지 기술 개발	23	93	87	169	31	403
합 계		45	216	152	372	74	859

- 출원인별 특허출원의 동향
  - · 봇을 포함하는 악성코드에 대한 탐지 기술의 주요 출원인을 알아보면 후지쯔가 45건으로 가장 많은 출원을 하였고, IBM이 40건, TrendMicro Inc.가 32건, 히타치가 32건을 출원하였으며, 그 뒤로 Network Associates Inc., Mcafee, Inc. ETRI가 출원을 많이 했음. 출원인의 업종별 특징을 살펴보면, 각 국의 대표 컴퓨터 회사와 네트워크 통신 업체가 주를 이루고 있음
  - · 봇을 포함하는 악성코드에 대한 탐지 기술의 주요 출원인은 후지쯔가 45건으로 가장 많았고, IBM이 40건, TrendMicro Inc.가 32건, 히타치가 32건을 출원하였음
  - · 최근 3년간의 주요 출원인 출원 현황을 보면 여전히 후지쯔가 가장 많고, 국내에서는 한국전자통신연구원의 특허활동이 활발함

○ 서버 보안

– 국내외 IPR 보유 현황

- WIPO에 따르면 한국인이 국내외 특허로 등록한 건수는 IMF 시절이 지나면서 줄었던 특허가 2005년 이후에 급격히 증가하고 있음
- WIPO에 따르면 전기공학 계열의 8가지 세부 분야의 경우 2001년부터 2005년까지 세계 대비 한국인이 등록한 특허의 비율은 컴퓨터 기술과 IT 관리 기술 분야가 전체적으로 낮게 나타남
- 2001년부터 2005년 까지 전기공학 계열에 대한 특허 등록 수에 있어 통신과 컴퓨터 기술에 대하여 특허가 많이 나왔으나 세계적인 추세에 비하면 적은 편이라는 것을 알 수 있음

– 서버 보안 관련 IPR 확보 가능성

- 보안 운영체제 표준화와 관련된 특허는 미국을 중심으로 확보되어 있는 상황이며 국내 업체나 연구소에서 보안 운영체제의 특수한 기능을 중심으로 특허를 보유하고 있음
- 서버 보안 분야에서 운영체제 커널 기술의 경우 국내에서 보유한 경우가 매우 적으며 그에 관련된 특허도 산출되기 힘든 상황이며, 국가 간의 경쟁력도 매우 약해진 상황임. 특히 마이크로소프트와 유닉스 서버뿐만 아니라 리눅스 분야까지 중국이나 일본에 밀리고 있는 상황임

• 국내에서는 서버 운영체제 자체보다는 운영체제 위에 탑재된 응용 기술에 더 관심을 기울이고 있으며 그러한 분야에서 특허의 경쟁력이 있을 것으로 보임

○ PC 보안

– 국내 특허출원 현황 및 전망

• 각 산업체별로 PC 보안과 관련한 기술에 대해 특허 출원을 강화하고 있는 추세로 점점 더 많은 특허 출원이 이루어질 것으로 예상

• 안티바이러스나 안티스파이웨어 분야는 진단방법에 대한 연구, 엔진 배포 등 업데이트에 대한 연구, 가상화에 대한 연구, 진단 속도 및 메모리 사용량 등에 대한 연구 및 특허를 진행

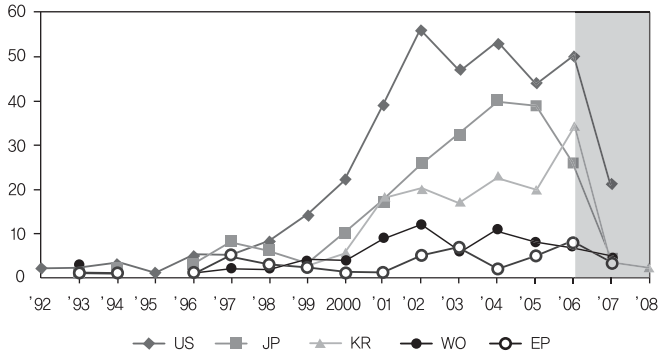
○ 디지털 포렌식

– 국내 특허 출원 현황 및 전망

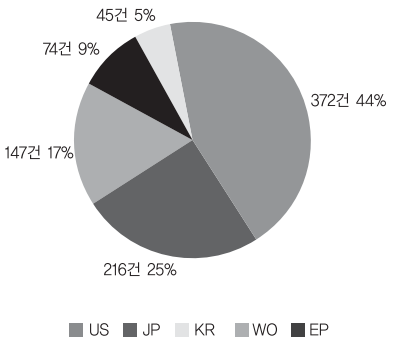
• 컴퓨터 포렌식을 중심으로 한 디지털포렌식 분야 특허 중 한국은 약 20%의 관련 특허를 출원 중에 있으며, 향후 모바일 포렌식 분야 특허가 활발해 질 것으로 전망됨

– 주요 국가별 특허 출원 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

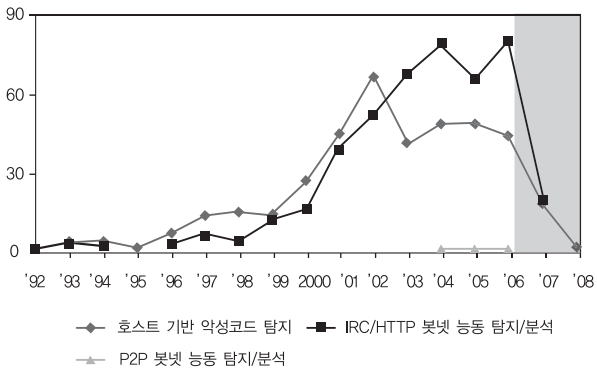


국가별 출원 추이

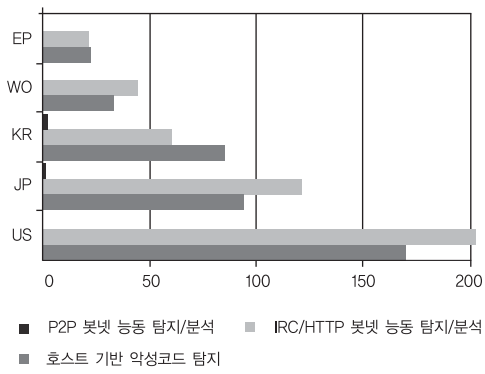


국가별 출원 건수

연도별 특허 출원 동향

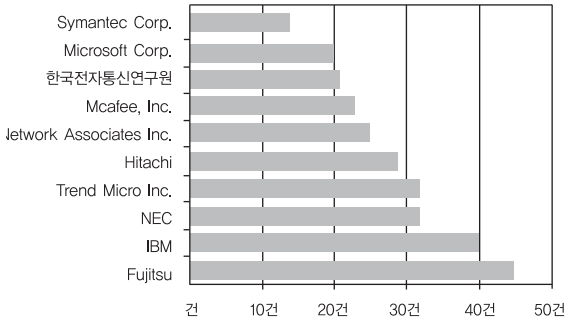


국가별 출원 추이

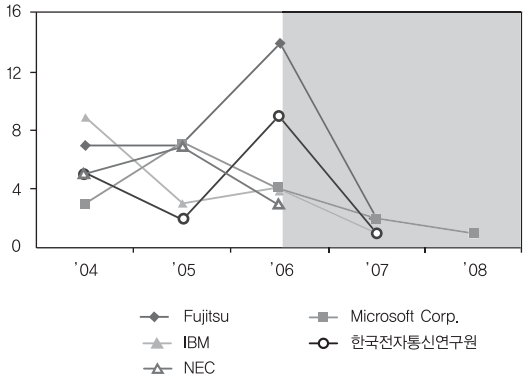


국가 기술별

기술별 특허 출원 동향



주요출원인 출원현황



최근 3년간 주요출원인 출원현황

출원인별 특허 출원 동향

2.3. 표준화 현황 및 전망

2.3.1. 국내 표준화 현황 및 전망

○ USN 보안

– 국내 표준화 현황

- 국내에서 센서 네트워크 보안과 관련되어 발표된 표준은 없으나, ETRI에서 RFID/USN 표준화 연구를 수행하면서 관련 연구를 시작하여 2006년 하반기부터 표준화 요구사항 분석이 이루어져 2007년부터 표준 초안이 작성되어 TTA의 RFID/USN 프로젝트 그룹에서 검토 및 표준화를 추진했고 2008년도부터는 TTA의 TC5(정보보호기술위원회)내 PG504[70] 프로젝트 그룹에서 센서 노드간의 인증 및 키 분배 프로토콜 등 14개의 표준화 아이템을 가지고 표준 제정이 진행 중임
- ICT 표준화 로드맵(2008)의 내용에서 알 수 있듯이 현재 국내 USN 표준화 진행은 미비한 상태로 현재 국내 RFID/USN 표준화 추진체계는 TTA가 활동을 지원하는 RFID/USN 포럼 내에 4개의 분과(기술, 응용, 네트워크, 정보보호)로 구성하며 정부출연기관인 ETRI, NCA, KRNIC, KISA가 하나씩 표준화 분과를 주도적으로 맡아 TTA 단체표준을 추진하고 있으며 TTA에서 채택된 단체표준을 관련 국제 표준화 기구에 제안하고 있고 표준화 포럼은 국제표준화 활동을 적극적으로 지원하며 일차적으로 RFID/USN에 관련된 용어표준화를 추진하고 있음
- 기술 분과는 시스템기술, 미들웨어, 시험인증, USN 미래기술, 시스템기술 등 4개의 워킹그룹으로 구성
  - 시스템기술 워킹그룹은 국제표준을 수용하고 국내 기술개발과 연계하여 900 MHz/433 MHz RFID 시스템 국내표준을 개발하고 국제표준을 수용하여 국내실정에 맞게 식별코드 및 ID표준을 제정함
  - 미들웨어 워킹그룹은 국제기술동향을 파악하여 리더/호스트/응용 데이터 인터페이스 국내표준을 개발하고 능동형 비즈니스 프로세스 자동화를 위한 이벤트 규칙표현방식에 대한 표준 기술의 국내표준 제정 및 국제표준을 제안하며 RFID 객체정보 표현 언어 표준 기술의 국내표준 제정 및 국제표준을 제안함
  - 시험인증 워킹그룹은 RFID 리더/태그 국내 기술기준시험표준을 개발한고 국제표준을 수용하며 국내 기술개발과 연계하여 900/433 MHz RFID 시스템 프로토콜 시험인증 기술을 개발할 뿐만 아니라 RFID시스템에 의한 인체영향 및 EMI 기술기준을 개발함
  - USN 미래기술 워킹그룹은 국제 기술동향을 파악하여 센서와 태그 통합 등에 대한 표준 기술을 개발하여 국내표준 및 국제표준과 태그간 새로운 통신방식 표준의 국제표준, 및 기존 통신망과 연계한 새로운 서비스 기술을 개발하여 국제표준을 제안하고 능동형 RFID 기술을 이용한 RTLS 표준을 개발함
- 응용분과는 물류/유통, 사회/문화, 교통/환경 등 3개의 워킹그룹으로 구성
  - 물류/유통 워킹그룹은 조달, 국방, 우편 등 물류분야를 담당

70) 응용보안 및 평가인증

- 사회/문화 워킹그룹은 교육, 문화, 엔터테인먼트 등을 담당함
- 교통/환경 워킹그룹은 교통, 환경 분야를 담당한다. 시범서비스 및 테스트베드를 통해 국민생활과 밀접한 분야의 ARP[71]를 개발하여 국내표준 제정 및 국제표준을 제안하고 있으며 센싱 및 네트워크 융합 등 USN 발전단계에 맞추어 BM[72]발굴 및 응용표준 개발을 선도함

• 정보보호 분과는 RFID 보안 워킹그룹, USN 보안 워킹그룹 등 2개의 워킹 그룹으로 구성

- RFID 보안 워킹그룹은 RFID 태그 등 초 경량 환경에 적합한 암호 프리미티브(블록 암호, 스트림 암호, 해시 함수)를 개발하여 국내 표준 제정 및 국제 표준을 제안. 또, RFID 태그/리더 간 상호인증을 위한 경량화 된 인증기술을 개발하여 국내표준 제정 및 국제표준을 제안. 이 외에, RFID 사용자의 개인정보 및 위치정보 프라이버시 침해방지를 위한 기술을 개발하여 국내표준 제정 및 국제표준을 제안
- USN 보안 워킹그룹은 USN 환경에서의 라우팅 프로토콜 보호 메커니즘을 개발하여 국내표준 제정 및 국제표준을 제안하고 있으며, 애드혹 네트워크, USN 등에서의 인증을 위한 기술을 마련하여 국내표준 제정 및 국제 표준을 제안함

USN 표준화 대상 항목

구분	표준화 대상항목	표준화 내용
USN Service	Application에 따른ARP/SRP	응용 서비스에 따른 센서 노드 요구 사항 정리
	USN directory service	USN 서비스를 위한 서비스 검색 기술
	USN database API	데이터베이스에 대한 API정의
USN Middleware	Service Registration	USN 서비스 등록 방법에 대한 정의
	Sensor Data Processing	센서 데이터 처리를 위한 기술
	Application layer interface	응용 계층에 대한 인터페이스 정의
	Network layer interface	네트워크 계층에 대한 인터페이스 정의
	Middleware API	미들웨어에 대한 API 정의
	Context-Awareness	상황인지 기술
	GIS 연계 기술	위치 정보 서비스와의 연동 기술
	Security	USN 보안기술
USN Networking	PHY / MAC	에너지 효율적인 통신을 위한 기술
	Routing	에너지 효율적인 통신을 위하 라우팅 기술
	위치인식기술	센서 노드의 위치를 알기 위한 위치 인식기술
	Short Addressing	센서 노드의 주소를 나타내기 위한 기술
	Lightweight TCP/IP profile	TCP 연동을 위한 기술
	Multicasting	효율적인 멀티캐스트를 위한 기술
	QoS Support	센서네트워크에서 QoS를 지원하기 위한 기술
	Mobility Support	센서 노드의 이동성을 지원하기 위한 기술
	Gateway Discovery	센서 네트워크에서 게이트웨이를 찾기 위한 기술

71) Application Requirement Profile

72) Business Model

구분	표준화 대상항목	표준화 내용
USN Networking	Gateway MIB	게이트웨이에 필요한 정보 정의
	IP Access망 연동	기존 IP망과의 연동을 위한 기술
	Bootstrapping procedure	센서가 처음 동작할 대 필요한 부팅 과정 정의
	USN Network Management	센서 네트워크를 관리 하기 위한 기술
Sensor Node	Sensor Interface	센서 표준 인터페이스 정의
	Sensor Node Architecture	센서 노드의 구조 정의
	Sensor OS API	센서 노드 OS에 대한 API
	Sensor Node MIB	센서 노드에 필요한 정보 정의

- 국내 표준화 전망 및 표준대상
  - TTA에서는 USN의 표준화 부분을 위 표처럼 분류하여 항목별 표준 대상을 지정하여 전략적으로 접근하고 있으므로 표준화가 매우 활발할 것으로 예상됨
  - 2008년 현재 국내에서도 USN 표준화를 위한 활동이 활발히 이루어지고 있으며 현재까지 국내에서 TTA를 중심으로 진행된 표준화의 내용을 살펴보면 2004년부터 각종 USN 현장 시험이 이루어지면서 센서 네트워크 인터페이스, 메타데이터 디렉터리 서비스, 미들웨어 플랫폼 참조 모델 등 센서 네트워크의 서비스 적용에 필요한 부분에 대한 표준화가 진행되었음. 특히 USN 서비스 제공을 위해서는 보안과 관계된 표준이 가장 중요하나 현재 보안이나 인증에 대한 표준은 전무한 상태임
  - 다양한 응용에서 센서 네트워크에 대한 보안 관리를 수행하는 경우, 해당 응용은 적합한 인증 및 접근 제어 기술이 필요함. 센서 개별노드와 네트워크, 게이트웨이 등에 대한 보안 미들웨어 및 보안관리 프로토콜에 대한 기술 개발과 선행 표준화가 시급한 상황임

○ 휴대인터넷 보안

- 2003년 1월 휴대인터넷이라는 이름하에 와이브로 기술개발 착수하여 2004년 6월 TTA 휴대인터넷 표준 제정 완료
- 와이브로 국내 표준은 IEEE에서 추진하는 국제표준과 유사
- 최근 TTA PG210[73] 산하의 PG 2103[74]은 PG302[75] 산하의 PG 3022[76]의 협력 하에 와이브로 네트워크에서의 IPv6 기술 적용 표준화를 추진
- 국내 표준화 전망
  - TTA PG302에서는 와이브로에서 UMTS로 PS HO, 댁내 RAS 및 비즈니스 형 와이브로, 와이브로에서 UMTS로 PS 핸드오버 등의 표준을 추진할 예정

73) IPv6 프로젝트 그룹
74) IPv6 over wibro 실무반
75) 휴대인터넷 프로젝트 그룹
76) 서비스 및 네트워크 실무반

○ 홈네트워크 보안

– 국내 표준화 현황

- TTA의 PG501[77]과 HNSF[78]를 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 PG501에 제출되었고, 2006년 12월 표준으로 제정
- 홈네트워크를 위한 보안기술 프레임워크에 관한 표준안이 TTA PG501에 제출되었고, 2006년 12월 표준으로 제정
- TTA PG501에서 "홈네트워크 등에 적용 가능한 디바이스 인증서 프로파일" 표준안이 2007년 12월 표준으로 제정

– 국내 표준화 전망

- ITU-T에서 표준화 중인 홈네트워크인가 표준이 2008년에 제정되면 TTA PG501을 통해 국내표준화를 추진할 예정임
- 홈네트워크 방범/방재를 위한 영상보안제품은 홈네트워크 IT보안제품과 연계되어 한층 강화된 보안 서비스를 제공하는 형태로 발전할 것이므로, 이를 고려하여 홈네트워크 보안제품간의 연동 및 안전성을 강화하기 위한 홈네트워크 융합보안프레임워크에 대한 표준화가 필요

○ 이동통신망 보안

– 국내 표준화 현황

- TTA PG701 및 PG703에서 완료된 정보보호 관련 표준
  - IMT-2000 3GPP-개선된 MMD 보안
  - IMT-2000 3GPP-(U)SIM 어플리케이션 툴킷을 위한 보안 메커니즘(R7)
  - IMT-2000 3GPP-선호하는 암호화 프로파일
  - IMT-2000 3GPP2-CDMA 카드 응용 툴킷을 위한 보안 패킷 구조(Release 0)
  - IMT-2000 3GPP-무선 특성 기술, 가입자 기밀
  - IMT-2000 3GPP-무선 특성 기술, 음성 프라이버시
  - IMT-2000 3GPP2-UMB 무선접속의 보안 기능(Release 0)

77) 정보보호기반 프로젝트 그룹
78) 홈네트워크시큐리티포럼

· IMT-2000 3GPP-무선 특성 기술, 강화된 보안 서비스
· IMT-2000 3GPP2-IP 기반 위치 서비스 보안성 프레임워크
· IMT-2000 3GPP2-GBA를 이용한 보안 구조
· IMT-2000 3GPP-Diameter 응용, 3GPP 특성코드와 식별자(R7)
· IMT-2000 3GPP-3G 보안, 합법적 감청 구조 및 기능(R7)
· IMT-2000 3GPP-Generic 인증 구조(GAA)-HTTPS를 이용한 망용용 기능에의 접속(R7)
· IMT-2000 3GPP-3GPP 기밀과 보전 알고리즘 규격, 문서2-kasumi 알고리즘 규격(R7)
· IMT-2000 3GPP-3G 보안, MILENAGE 알고리즘 세트의 규격, 3GPP 인증과 키 생성 기능 f1. f1*, f2. f3, f4, f5, f5*의 예시 알고리즘 세트, 문서4, 디자인 순응 데이터(R7)
· IMT-2000 3GPP-통신 관리, 통합참조점을 위한 보안 서비스, CORBA 솔루션(R7)
· IMT-2000 3GPP-통신 관리, 보안관리 개념과 요구사항(R7)

- 국내 표준화 전망
  - TTA TC5(정보보호) 및 TC3(이동통신)의 프로젝트 그룹에서 이동단말 간 보안 상황 정보교환, 모바일 단말 보안강화 등 단말 관련 보안표준 등을 추진할 예정

○ 무선근거리통신망 보안

- 국내 표준화 현황
  - TTAE.IE-802.11a: 무선랜 매체접근제어 및 물리계층. 5GHz대역의 고속 물리계층
  - TTAE.IE-802.11f IEEE 802.11: 분산 시스템에서 다중 사업자 AP 상호 운용성을 위한 AP간 프로토콜
  - TTAE.IE-802.11i: 무선랜 매체접근제어 및 물리계층의 보안기능 향상
  - TTAS.KO-06.0069: 무선랜 매체접근제어 계층 보안기능 향상을 위한 그룹 키 갱신 및 설정. 본 표준은 IEEE 802.11 기반의 무선랜 매체접근제어 계층 보안기능 향상을 위한 그룹 키 갱신 및 그룹 키 설정 동작을 규정하는 것을 목적으로 하며, WPA 단말기와 non-WPA 단말기가 공존하는 혼합 모드 무선랜 시스템의 구축 시 본 표준이 적용될 수 있음
  - TTAS.KO-06.0081: 고속무선랜(IEEE 802.11g) 상호운용성 시험 규격
  - TTAS.KO-06.0086: IAPP에서 스테이션 보안 콘텍스트
  - TTAS.KO-06.0099: AP간 프로토콜에서 안전한 통신 보장을 위한 RADIUS-Diameter 연동 규약
  - TTAS.OT-06.0045: 무선랜(IEEE 802.11b) 상호운용성 시험규격
  - TTAS.KO-06.0025/R1, TTAS.IE-P1489/R1, TTAS.IE-P1488/R1, TTAS.IS-DIS15662, TTAS.KO-06.0034: 5.8 GHz 대역 노변 기지국과 차량 단말기가 근거리 전용 무선통신 교통정보 및 제어시스템[79] 서

79) TICS: Transport Information and Control System

비스를 지원하기 위한 5.8GHz 대역의 ITS 전용 단거리 무선통신[80] 표준 중 개방형 시스템 간 상호접속 참조모델[81]을 기준하여 물리 계층과 데이터링크 계층, 그리고 응용 계층에 대하여 기술

- TTAS.OT-12.0001: 무선 인증서 관리 프로토콜
- TTAS.KO-12.0016, TTAS.KO-12.0017: 무선 전자서명 인증서 프로파일 표준, 무선 전자서명 인증서 효력정지 및 폐지 목록 프로파일 표준
- TTAS.KO-12.0019: 무선 WTLS 인증서 프로파일 표준
- TTAS.KO-12.0031: 안전한 무선랜 사용을 위한 가이드

– 국외 표준화 전망

- IEEE 802.11e 관련 무선랜 QoS 보장을 위한 MAC 기능 연구 예정
- IEEE 802.11r, 802.11k, 802.11u 관련 무선랜 망간 서비스연동 규격 연구 예정
- IEEE 802.11s 관련 무선랜 메쉬 네트워크 규격에 관한 표준을 추진할 예정
- IEEE 802.11w 관련 무선랜 관리 프레임 보호 규격에 관한 표준을 추진할 예정
- IEEE 802.11n에 대한 무선랜 관련 기술기준 작업이 진행 예정
- 2.4GHz 대역은 간섭의 영향이 많으므로, 5 GHz 대역에서 무선랜을 적용하는 것에 대한 검토

○ 차세대 네트워크 보안

– 국내 표준화 현황

- 차세대네트워크 보안 분야는 Broadband, Mobility, QoS, IPv6 등에 이르기까지 매우 다양한 분야에 걸쳐있어 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 PG503[82]에서 인터넷 보안 및 NGN 보안 기술 관련 표준 개발, 사이버 보안 기술(스팸대응, 악성코드 대응 등) 관련 표준 개발, 사이버 범죄 대응 기술(IP 역추적, 디지털포렌식 등) 관련 표준 등 개발 중이며, NGN 보안에 관련된 표준화 활동도 포함되어 있으나 구체적인 활동이 미미함
  - TTA PG204[83]에서는 BcN 일반요구사항, 참조모델, 통합연동기술 등을 연구하고 있으며, 2008년도부터 BcN의 보안 분야의 표준화 활동이 시작된 상태임

– 국내 표준화 전망

- TTA PG503에서 서비스거부공격 소스추적 기술, 암호 메시지 규격, 암호화 알고리즘의 사용, 홈네트워크를 위한 보안기술 프레임워크 표준 등을 추진할 예정
- TTA PG204에서는 BcN 보안 요구사항, BcN 사용자 인증 기술 등에 관한 표준을 추진할 예정

80) DSRC: Dedicated Short Range Communication
81) OSI: Open System Interconnection
82) 사이버 보안 프로젝트그룹
83) NGN 프로젝트그룹

○ 사이버공격 역추적/보안관리

– 국내 표준화 현황

• 국내 사이버공격 역추적 및 보안관리 일반 표준은 인터넷 보안기술 포럼과 TTA에서 추진함

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

· 침입차단시스템, 침입탐지시스템, 가상사설망 시스템 로그 표준을 정의한 국내 인터넷 보안기술 포럼(KISA, ETRI, 정보보호산업체 등에서 참여)에서 표준화된 정보보호 일반 관련 표준과 TTA에서 확정된 정보보호 표준은 아래와 같음

• 현실 망에서 활용 가능한 멀티 도메인 간 협업 기반의 사이버공격 역추적 보안이벤트 포맷 및 프레임워크에 대한 표준화 작업이 진행 중임

– 국내 표준화 전망

• 현재, 보안장비의 보안이벤트 로그 포맷 이외에도 보안관점의 네트워크 트래픽 현황에 정형화된 형식에 대한 표준화가 추진 중이며, 효율적인 보안관리 가이드라인을 제공을 위해 직관적인 보안관리 인터페이스에 대한 표준화가 진행될 것으로 예상

• 현실 망에서 활용 가능한 멀티 도메인 간 협업 기반의 공격 추적 수행을 위해 각 도메인간의 침해사고 데이터 형식과 이를 교환하기 위한 프로토콜에 대한 표준화가 추가적으로 요구될 것임

사이버공격 역추적 및 보안관리 관련 제정 및 진행 중인 표준 목록

관련분야	표준 번호	표준 내용	제정년도	개정현황
보안관리	ISTF-004/R	침입차단시스템 로그형식 표준	2003	개정
	ISTF-005/R	침입탐지시스템 로그형식 표준	2003	개정
	ISTF-020	보안시스템의 통합관리를 위한 API 표준	2003	–
	TTAS.IS-17799	정보보호관리 표준	2002	–
	TTAS.KO-12.0036	정보보호관리체계 수립 지침	2006	–
	TTAS.OT-12.0003	정보보호제품 표준적합성 시험방법	2004	–
사이버공격 역추적	TTAE.IT-X.1036	네트워크 보안 정책의 생성, 저장, 분배 및 실행을 위한 프레임워크	2007	–
	TTAS.KO-12.0060	사이버공격 추적 이벤트 교환 포맷	2007	–
	–	사이버공격 추적을 위한 정보보호 요구 사항	2008 진행 중	–
	–	다중 도메인 환경에서의 사이버공격 추적프레임워크		–
	–	침해사고 이벤트 교환 포맷		–
	–	시스코시스템즈 넷플로우 서비스 전송 버전 9		–

○ 봇넷 대응

– 광범위하게 분포한 봇넷의 대응을 위해서 ISP 및 도메인 간 공조 요구됨

– TTA 정보보호 기술위원회(TC5) 산하 사이버 보안 프로젝트 그룹(PG503)에서 봇넷 대응에 관한 과제 제안 상태

○ 서버 보안

– TTA TC5 PG501에서 서버 보안에 대한 과제 추진

– 국내 서버 보안 업체들의 경우 CC 인증 기준에 맞추어 제품을 개발하는 형태이며 서버 보안 제품에 대한 표준화에는 크게 노력을 기울이고 있지 않음

– 삼성, LG, 소니, IBM 등의 세계 유수의 가전 및 임베디드 리눅스 업체들이 모여 결성한 CELF[84]에서 임베디드 리눅스 솔루션 및 표준 플랫폼 제정을 위해 활동 중이며 산하 기구인 보안워킹그룹을 통해 기술적인 접근을 하고 있음

○ PC 보안

– 국내 정보보호 일반 표준은 ISTF[85]과 TTA에서 추진되고 있지만 특별히 활성화 되어 있지 않은 것으로 보고 있으며 PC 보안과 관련되어 추진된 표준은 2000년에 제정된 악성코드 방지 지침이 있고 침입차단/방지 시스템 로그형식 표준처럼 악성코드 처리 로그도 표준화 대상이지만 타 분야에 비해 그 필요성이 적음

– PC 보안기술과 관련하여 국내에 표준화가 이루어진 것은 2000년에 악성코드 방지 지침이 있으며 2006년 보완되었음

– 관리적인 요구사항에 맞추어 업체별로 로그 형식 표준화가 되어 있지만 업체 간의 표준화까지는 이루어지고 있지 않음

○ 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

• 2007년부터 TTA를 통해 디지털포렌식 가이드라인 및 수집도구 검증을 위한 요구사항에 대한 표준화가 추진되었음

– 국내 표준화 전망

• 향후에는 TTA를 통해 데이터 수집, 분석, 복구에 관한 검증 방법 및 절차에 대한 표준안과 디지털 증거에 대한 교환 포맷 표준안을 개발하고 표준화를 추진하려 하고 있음

84) Consumer Electronics Linux Forum

85) 인터넷 보안기술 포럼

2.3.2. 국외 표준화 현황 및 전망

○ USN 보안

- IEEE 802.15.4: 지그비 보안 요소 정의 및 구체적 메커니즘(마스터키, 링크키, pair-wise 키, global 키) 들이 제정되어 있고 6LoWPAN에서 계속 경량화 보안 기술 적용을 위한 연구 진행 중
- ITU-T SG17: WP2(보안)그룹에서 센서네트워크 관련 미들웨어 및 보안 프레임 워크 표준 진행 중
- IETF Security 분야의 17개 작업반을 두어, IPSEC, TLS 등의 표준을 담당
- ISO/IEC JTC1 의 SC27의 IT 보안기술 연구반에서 USN 관련 프라이버시, 요구사항 등을 진행
- W3C: 센서 관련 콘텐츠의 표준화(SensorML: 센서 데이터 인코딩 기술의 표준)

○ 휴대인터넷 보안

- 와이맥스는 IEEE 802.16x 표준에 기반을 두고 있으며, 고정형 와이맥스인 IEEE 802.16-2004와 모바일 와이맥스인 IEEE 802.16e 두 가지 버전 존재
- 초기에는 고정형 광대역 AP를 목표로 표준화가 진행되어 왔으나 2003년부터 한국의 고유 기술에 의한 와이브로 사업추진에 자극을 받아 와이맥스 포럼은 모바일 와이맥스 표준화 작업에 착수하였고, 기존의 고정형 와이맥스 표준 규격을 2004년 6월에 조기 마무리
- 고정형 와이맥스는 초기에 IEEE 802.16d로 명명되다가 2004년 7월 IEEE 802.16-2004로 승인
- 2004년 3월 와이브로 개발을 주도하는 국내 개발 기관과 모바일 와이맥스 개발을 주도하는 인텔간의 기술협의와 사업자의 동의하에 와이브로 기술규격과 모바일 와이맥스 기술규격을 일치시키기로 합의
- 2005년 12월 국제표준인 IEEE 802.16e에 와이브로 규격 반영
- 2007년 10월 ITU에서 3G(IMT-2000) 표준 채택
- 와이브로 기술이 국제 표준안으로 채택됨에 따라 우리나라는 2010년경에 기술 표준이 확정될 예정인 4G(IMT-Advanced) 표준채택에 있어서 유리한 고지 선점

○ 홈네트워크 보안

- 홈네트워크 보안에 대한 국외 표준화는 ISO에서 2005년에 표준안이 한 건 있었고, ITU-T에서 는 총 4건의 표준이 제정 또는 표준화가 진행 중임
- 홈네트워크 보안에 대한 국외 표준화는 현재 한국 주도로 이루어지고 있음
- ITU-T에서 진행 중인 표준안들은 SG17의 Question 9에서 진행 중
  - 2007년 2월 홈네트워크 보안프레임워크에 대한 표준이 X.1111로 제정
  - 2007년 11월 홈디바이스 인증을 제공하기 위한 인증서 프로파일에 관한 표준이 X.1112로 제정
  - 2007년 11월 홈네트워크 서비스를 위한 사용자 인증 메커니즘에 관한 표준이 X.1113으로 제정

- 홈네트워크인가 프레임워크에 관한 표준 과제인 X.homesec-4가 진행 중이며, 2008년 하반기에 표준 제정이 예상됨

– 홈네트워크 보안제품간의 연동 및 안전성을 강화하기 위한 홈네트워크 융합보안프레임워크에 대한 표준화를 국내표준화와 병행하여 추진 예정

○ 이동통신망 보안

– 3GPP를 중심으로 IMT-Advanced 기술에 대한 표준화를 활발하게 추진하고 있으며, 보안관련 부분은 Network Access Security, Network Domain Security, User Domain Security, Application Domain Security의 4가지 구간으로 나누어 진행됨

– 현재, 4세대 시스템으로 LTE 시스템이 가장 유력하게 대두되고 있으나, 현재 LTE 시스템을 위한 Security 부분은 기존의 표준안과 차이가 있는 부분을 위주로 고려하고 있어 별도 활발하게 추진되지는 않는 상태임

– 3GPP LTE 표준화는 매우 활발하여 유럽을 넘어 미국과 일본 등 확산되고 있음. 미국 2위 이동통신사업자인 버라이즌도 LTE를 채택하기로 하였고, 모바일 와이맥스를 도입키로 한 일본의 KDDI가 복수 표준을 지원하고자 하고 있음

– 이동통신망의 연동 게이트웨이의 경우, 3GPP와 Non-3GPP 타망 연동을 위한 표준을 무선랜에서 모바일 와이맥스까지 수용하고 IP Networked Internet Device까지 수용하도록 확장되어 기존 IPsec 수준으로 Network Domain Security를 추가로 진행하고자 하고 있으며, 인증 정보 및 키 배포에 대하여 Key hierarchy가 새로이 표준화됨

– 차세대 이동통신관련 표준화는 3GPP에서 LTE와 타망(3GPP2/Mobile-WiMAX)과의 상호연동에 대한 논의 결과, LTE와 타 망과의 상호연동을 표준화 아이템으로 채택하여 2008년 12월까지 표준화를 추진키로 결정함

○ 무선근거리통신망 보안

– 현재 프로토콜의 보안 결함을 강화시키는 측면에서 IEEE와 IETF가 상호 협력아래 표준화를 진행

– EAP[86]를 이용한 사용자 인증 프로토콜과 보안키의 계층적 구성 방안은 IETF의 EAP 워킹그룹에서, 공개키 인증서, ID/패스워드 등 다양한 사용자 인증 방법에 대해서는 PPPEXT 워킹그룹에서, 그리고 글로벌 로밍 가입자에 대한 권한제어, 과금, 분산 인증 프레임워크는 AAA 워킹그룹에서 표준화를 추진

– 프로토콜 수준에서의 보안 기술 표준화 문제가 일단락되면, 네트워크 측면에서 유무선 통합보안 기술에 대한 표준화가 예상

– 또한, 최근 기존 무선랜의 한계를 극복하기 위해 다양한 새로운 기술 동향 중 무선 메쉬 네트워크 기술이 등장하였으며, 현재 IEEE 802.11에서는 TGs에서 표준화를 다루고 있으며 홈네트워킹 분야의 IEEE 802.15에서는 TG5에서 무선 메쉬 네트워크 표준화를 다룸

86) Extensible Authentication Protocol

– IEEE에서 진행되고 있는 Tasking 그룹과 Study 그룹 중 무선랜 보안에 관련한 부분을 요약하면 〈표 27〉과 같음

– IEEE 802.11 워킹그룹별 기술 동향

• TGn

· 2007년도 3월부터 WFA에서 시작된 "WI-Fi CERTIFIEDTM 802.11n Draft 2.0" 인증을 통해 현재까지 180가지가 넘는 제품이 출시되고 있는 가운데 이러한 시장의 상황을 반영하듯 IEEE 802.11n이 현재 최대 이슈로 등장하고 있음. 하지만 ITU-R WP8F에서 IMT-Advanced에서 요구하고 있는 기준을 만족시키지 못하고 있기 때문에 후속 기술에 대한 Study 그룹이 2007년 5월 정식으로 만들어져 작업에 들어갔음

· 2008년 3월 27일에 Draft IEEE 802.11n D4.00을 발표하고 letter ballot에 들어간 IEEE 802.11n은 2009년 7월에 최종 발간하는 것을 목표로 현재 Sponsor ballot을 준비하고 있음

· IEEE 802.11n은 MIMO, LDPC, Aggregation 등의 핵심기술을 활용하여 기존 IEEE 802.11a에 비해 PHY에서의 최대 성능을 54 Mbps에서 600 Mbps로 11배 가까이 끌어 올렸으며, 더불어 동작 범위를 대폭 늘렸고 신호의 품질 또한 향상 시켰음. 이러한 비약적인 성능 발전에 대한 시장의 기대를 반영해 Wi-Fi Alliance는 2007년 3월부터 IEEE 802.11n D2.0을 기반으로 인증을 부여하기 시작했으며 현재까지 180 개가 넘는 제품에 인증을 부여함

• TGp

· WAVE라고도 불리는 TGp는 802.11을 개선시켜 10ms의 짧은 latency를 가지게 하고, 최소 200km/h의 속도에서 반경 1km를 커버하며, 큰 빌딩들 사이의 멀티패스 환경에서 운송수단과 길거리의 장치 또는 운송수단 간에 5 GHz의 주파수 대역을 사용한 통신을 지원하는 ITS 응용 시스템의 PHY 및 MAC 표준을 연구

IEEE의 표준화 작업

표준화	내용
802.11s	메쉬 네트워크
802.11p	Vehicular 환경에서의 무선 통신
802.11e	802.11 네트워크의 QoS 향상
802.11z	확장된 데이터링크
802.11i	802.11 네트워크의 보안 향상(인증 측면)
802.11w	802.11 네트워크의 보안 향상(통신 프레임 측면)
802.11h	Spectrum 측정을 위한 MAC & PHY 정의
802.11j	지역 표준(일본)
802.11y	3,650~3,700MHz 주파수 대력 서비스 제공
802.11d	지역 간 로밍용 확장기술
802.11m	각 무선랜 규격의 잘못을 수정

표준화	내용
802.11t	802.11 장비 및 시스템 제조업체와 판매자 평가 측정
802.11v	무선 네트워크 관리
802.11k	무선 자원측정
802.11a	5 GHz 주파수 대역에서 OFDM을 적용한 물리계층 정의
802.11b	DSSS를 이용한 2Mbps, CCK를 통해 5.5, 11 Mbps 전송 지원
802.11g	2.4 GHz 주파수 대역에서 OFDM을 적용한 물리계층 정의
802.11n	차세대 무선랜 요소 기술 정의
802.11r	빠른 로밍
802.11f	AP 간 프로토콜
802.11u	IETF, 3GPP, 3GPP2 상호 작용

- TGr
  - Fast roaming을 제공하기 위한 것으로 빠른 BSS 전환을 추구. 원래 TGr은 셀룰러 망을 사용하는 대신에 무선 인터넷 망에서 이동전화기를 가지고 VoIP와 같은 응용서비스를 실시간으로 지원하기 위한 목적으로 시작. 이러한 응용 서비스의 핸드오프는 최대 50ms 이상을 초과할 수 없는데, 현재의 802.11의 로밍 지연은 평균 수백 ms가 걸리고 있음. 이러한 문제점을 개선하기 위해 TGr은 802.21과도 연계하여 현재 draft 6.0에 대한 수정작업 중이며, 공식적인 표준화 일정은 2008년 4월까지로 정해져 있음
- TGs
  - TGs는 기존 802.11에 메시 네트워킹을 추가한 것으로, 애드혹 망에서 무선 디바이스들이 상호 통신을 하도록 정의함. AP 간에 브로드캐스트/멀티캐스트와 유니캐스트를 지원함. TGs에서는 기본적으로 HWMP 라우팅 프로토콜을 제공하며, 다른 벤더에서 제공하는 RA_OLSR과 같은 라우팅 프로토콜의 사용도 허락하고 있음. 현재 draft 초안 작업 중이며, 공식적인 표준화 일정은 2009년 4월까지로 정해져 있음
- TGu
  - TGu에서는 기존의 802.11 표준에 외부 망과의 상호 연동성을 향상시키기 위한 기능을 추가하는 작업을 하고 있음. 현재의 802.11망은 사전에 인증을 받은 사용자만이 이용 가능한 망이나, 802.11u는 사전에 인증을 받지 않은 사용자도 망의 사용이 가능하도록 함. 즉, 외부 망 이용자가 현재의 망에 들어오게 할 수 있는 방법이라든가 비상 호출 시에 망에 접근을 허락하게 하는 방법 등을 제안하고 있음. 현재 802.11과 3GPP SA2와의 상호 연동 방안을 논의 중이며, 공식적인 표준화 일정은 2009년 3월까지로 정해져 있음

– IEEE 802.11 SG별 기술 동향

- VTS SG
  - 대용량 고속전송 물리 계층의 발전으로 최근 제품에서는 최대 200 Mbps 이상의 속도를 가지는 무선랜 제품들이 출현하고 있음. 이러한 제품들은 802.11n의 고속 PHY 계층과 이를 지원하기 위한 MAC 계층을 이용하며, 이들은 데이터 전송속도를 효율적으로 높이기 위한 방법을 사용하고 있지만 비디오 전송을

주된 목적으로 802.11을 사용하는 경우 여러 문제가 발생함. 우선순위에 대한 제한된 정의, 각 내부 계층 간의 정보공유 부재, 부족한 QoS 파라미터, 그리고 영상 콘텐츠에 특화된 전송 방법 부재 등 다양한 문제점을 가지게 됨. 이러한 다양한 문제점을 802.11e에서 제공하는 EDCA, HCCA, CFBs, BA와 DLS 기능을 이용하면 서비스 품질의 증가를 가져올 수 있지만, HD급 또는 Blue-Ray 급의 고화질을 전송하는 경우에는 비디오 전송에 최적화된 MAC을 개발할 필요가 있음

- QSE SG
  - Wi-Fi alliance가 WMM 규격을 만들 때 산업체의 의견을 받아 802.11e의 Draft 버전을 기반으로 만든 후 IEEE 위원회에서 802.11e를 WMM의 superset으로 승인을 했으며, 이로 인해 WMM의 규격과 802.11e의 규격(프레임 구조)의 차이로 인한 호환성에 문제가 발생하여 통합 필요성이 제기됨
- DLS SG
  - 802.11e에서 이미 정의된 DLS는 BSS 안에서 스테이션 간의 직접적인 통신을 지원하도록 하는 기능으로 802.11e AP는 DLS 기능을 처리해야 하나 기존 AP의 경우 DLS 기능이 없어 지원할 수 없는 문제가 있음. 이를 해결하기 위해서 DLS 요청 관련 프레임을 데이터 프레임 내에 캡슐화하여 보내는 방법이 검토되고 있음
- VHT SG
  - VHT SG는 현재 802.11n이 지원하는 300Mbps 또는 600Mbps의 속도를 넘어서 무선으로 1Gbps 이상의 고속 처리율을 제공하자는 목적으로 2007년 3월 회의에서 SG로 승인되었음
  - 1Gbps 처리를 위해서 다양한 의견들을 취합하고 있음. 특히 IMT-advanced와의 관계를 유념하며 VTS-SG와의 관계 협조를 강조하고 있으며, 2010년 이후에 표준화 완성을 목적으로 하고 있음

○ 차세대 네트워크 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 진행하고 있음
- TU-T NGN[87] 네트워크 보안 기술 표준 활동
  - SG11에서, NGN 사용자 접근을 위한 보안 프로토콜 기술에 대한 국제 표준을 개발하였으며, 망간 상호접속을 위한 인증 프로토콜 연동 기술에 대한 표준화가 추진되고 있음
  - SG13에서, NGN 보안 요구사항 및 인증 기술에 대한 국제 표준을 개발하였으며, 사용자 접근제어를 위한 표준안과 보안 메커니즘에 대한 표준화가 추진되고 있음
- IETF에서 네트워크 보안 기술 표준 활동
  - 보안기술 표준화와 관련된 작업은 여러 영역에서 수행 중
  - 보안 영역에는 20개 작업반이 구성되어 관련 표준화를 수행

87) Next Generation Network

- 보안 영역 밖의 일부 작업반은 보안과 관련을 갖는 활동 수행

– ISO/IEC JTC1에서 네트워크 보안 기술 표준 활동

- SC27(IT Security Techniques)은 보안서비스를 위한 일반적인 요구사항과 보안기술과 메커니즘 개발, 보안 지침의 개발 및 보안 관리기법 등 개발을 주요 업무로 함
- 워킹그룹 1(요구사항, 보안 서비스, 가이드라인), 워킹그룹 2(보안 기술과 메커니즘), 워킹그룹 3(보안 평가 기준) 등 3개의 그룹으로 나뉘어 활동하고 있음

○ 사이버공격 역추적/보안관리

– 국내 표준화 전망국제표준화기구 및 산업체 중심의 보안 관리를 위한 표준화 현황은 국내 표준보다 활발하게 진행되고 있으며, 특히 ITU-T SG17는 정보통신 보안에 관한 표준을 선도하는 그룹으로 WP2 산하에 보안 관리, 안전한 통신 서비스 등의 7개 보안연구과제가 구성되어 있음

– ITU-T에서는 2007년 9월에 5개국이 참여한 역추적 관련 국제표준화를 2008년 4월부터 진행하기로 결정하였고 관련 표준화에 대하여 한국의 국제 표준전문가가 co-editor로 선정되었으며 ITU-T SG17 국제 표준 규격화 시도를 위한 사전단계로 ASTAP에서 검토가 수행됨

– IETF ID[88] 워킹그룹은 침입탐지시스템 구성 요소들, 대응 시스템, 관리 시스템 사이의 정보 공유를 위한 데이터 포맷과 교환 절차를 표준으로 정의하고 있으며 현재 Tunnel Profile(RFC 3620)이 표준으로 제정되어 있음

– 또한 IETF INCH[89] 워킹그룹은 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 규정하고 있음

– 350개 이상의 각 분야 톱 벤더가 제공하는 솔루션과 통합 및 상호연동을 실현하는 프레임워크 OPSEC[90] 표준이 제정되었으며, OPSEC에서는 CheckPoint 사를 중심으로 컨텐츠 보안, 인증 및 권한 관리, 침입탐지시스템, 사건 분석 및 리포팅, 디렉터리 서버분야의 프레임워크 파트너를 구성하기 위한 표준을 제정함

– IETF iTrace 워킹그룹에서 ICMP 메시지를 이용하여 공격 경로 정보를 제공하는 표준화 작업을 진행하여 2000년에 첫 드래프트를 발간하기도 하였으나 2003년 이후로 작업을 종료함

88) Intrusion Detection
89) extended INCident Handling
90) Open Platform for Security

ITU-T Study Group 17에서의 통합보안관리 관련 Question 및 이슈

연구과제	연구과제 제목	이슈
Q.5	Security architecture and framework	통신보안 솔루션에 대한 보안구조 신규 솔루션 및 모바일 환경을 위한 보안구조 종단 간 사용자 보안을 위한 구조 NGN, IP기반 네트워크, 개방형 시스템 보안구조
Q.6	Cyber Security	취약 또는 위협정보의 분배 및 공유 방법 사이버 공간에서 침해사고 처리를 위한 운용 방법 중요 네트워크 인프라의 보호 정책
Q.7	Security Management	통신 시스템에서 정보자산 및 보안위협의 확인/관리 통신보안에서 정보보안 관리의 구축 방법 보안사건 발생에 대한 처리 관리

ITU-T Study Group 17에서의 통합보안관리 관련 '08년도 신규 Question 및 이슈

연구과제	연구과제 제목
Q.6	New work item proposal for the scenarios and requirements of IP trace-back
	Proposed a study skeleton for new work item about IP trace-back

ASTAP에서의 통합보안관리 관련 Question 및 이슈

분야	기고서 제목	표준 기구명
Information Security Group	Framework for Tracing a Cyber attack at the Multiple Domains Environment	ASTAP
	Security Requirement for Cyber Attack Traceback	ASTAP

통합보안관리 관련 IETF INCH RFC 및 진행 표준

분야	IETF INCH RFC 및 진행 표준
INCH	The Incident Object Description Exchange Format(IODEF, RFC5070) Requirements for the Format for Incident Information Exchange(FINE) Real-time Inter-network Defense(RID) IODEF/RID over SOAP Extensions to the IODEF-Document Class for Phishing, Fraud, and Other Crimeware

IDWG 분야 표준안

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

○ 봇넷 대응

- 국제적인 봇넷 분포 현황 및 공조 대응 체계가 요구됨에 따라 봇넷 정보 공유 데이터와 공조체계에 대한 표준화 필요
- 봇넷 관련 국제 표준화 활동이 미비하기 때문에 기술개발 초기부터 표준안 개발을 추진하여 국내 우위 기술 전파와 관련 분야 시장성 및 주도권 확보할 수 있음
- ITU-T SG17 보안 그룹에서 봇넷 탐지 및 대응 프레임워크와 봇넷을 이용해 발송되는 스팸 대응 수단에 대한 표준화 추진

○ 서버 보안

- ISO/IEC는 유럽의 ITSEC과 미국의 TCSEC을 통합한 국제공통평가표준 CC를 버전 2.3에 이어 3.1을 2007년 9월에 발표하였고, 특히 세 개의 파트로 나누어 표준 문서를 발표하였으며 CCRA의 멤버 조직에서는 인증 레벨인 EAL을 정의하고 있음
- CC/CEM에서는 지속적으로 보안 평가 부분을 갱신하고 있음. CCRA에 의해 전체적으로 관리되며 CCDB에서는 CC/CEM의 관리와 개발에 대한 기술 프로그램을 운용하고 있으며 CCMB에서는 CP(Change Proposal)를 처리함. ISO/IEC에서는 제안된 자료를 검토함으로써 CC/CEM의 표준화를 지원함
- 현재 NIAP과 NIST를 중심으로 PP, ST 등의 표준화가 진행 중임
- TCPA[91]는 PC 기반의 산업 플랫폼, 운영체제, 응용 등의 보안규격을 개발이 목표임. 표준규격인 TCPA 1.0의 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 중임

○ PC 보안

- 악성코드 분야에서 국제 표준화 활동은 미비한 편이며 명명법, 분류법에 최근 테스트 방법론에 대한 토론이 이루어지고 있지만 미비한 편임
- 1991년 CARO[92]의 멤버들이 CARO 바이러스 명명법 관례라는 기준안을 제시했으나 AV 업체들이 가이드라인 정도로 부분적으로 이 규칙을 적용하여있어서, Virus Bulletin에서 VGrep이라고 각 AV 벤더들의 악성코드 이름을 비교해 주는 도구를 만들어 운영하고 있으며 각 벤더들의 도움을 받아 서비스하고 있지만 많은 악성코드와 실시간으로 DB가 업데이트되지 않기 때문에 운영상의 어려움이 있음
- AMTSO[93]이 2007년에 결성되었고 AV 벤더들이 모여서 안티말웨어 제품의 테스팅에 대한 표준을 위해 2008년에 결성되어 운영 중에 있으며 Generic Testing, Dynamic Testing, Static Testing 등에 대한 표준 및 가이드라인 등이 논의되고 있음

91) Trusted Computing Platform Alliance
92) Computer Antivirus Researchers Org.
93) Anti-Malware Testing Standards Organization

○ 디지털포렌식

- 미국 NIST는 CFTT 프로젝트[94]를 운영하여 포렌식 도구 기능 검증을 국가적으로 주도하고 있음
  - 디지털 증거의 무결성 훼손 없는 수집, 분석을 통한 법적 근거 있는 결과를 도출하기 위해 사용되는 디지털포렌식 기능을 검증하고 그 결과를 공표하고 있음
  - CFTT에서는 디지털포렌식 툴의 검증 및 평가 방안을 제시하고, 평가 결과 보고서는 NIS[95]와 함께 공동으로 발간하여 일반인들도 쉽게 열람할 수 있도록 하고 있음. 컴퓨터 범죄 수사관들은 이 보고서를 참조하여 디지털포렌식 툴의 선정 기준을 확립하며, 변호사와 검사들은 디지털 증거의 객관성을 증명하기 위한 자료로 활용하고 있음
- 미국 NIST는 NSRL 프로젝트[96]를 운영하여 획득된 증거 조사 분석 시 효율적인 파일 검색을 위한 참조 데이터 셋을 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 ITL[97]에서는 Special Publication 800-series를 통해 컴퓨터 포렌식 및 모바일 포렌식에 대한 가이드라인을 발표하는 등 포렌식 분야의 표준화를 진행 중임
  - 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
- 최근 ITU-T SG17에서 2009년부터 시작되는 신규 회기에 사이버 범죄 추적 관련 표준화를 기존 WG6의 새로운 범위로 포함시켰으므로, 여기에서 관련되는 포렌식 표준화가 이루어질 전망임

94) Computer Forensic Tool Testing, http://www.cftt.nist.gov

95) 미국 국가 법무연구소

96) National Software Reference Library, http://www.nsrl.nist.gov

97) Information Technology Laboratory

2.3.3. 표준화 대상항목별 현황분석

구분		네트워크 보안			
표준화 대상항목		USN 보안기술	휴대인터넷 보안기술	홈네트워크 보안기술	이동통신망 보안기술
시장현황 및 전망	국내	600억 원(보안시장 열려있음)	현재 상용서비스 초기단계에 있지만, 서비스 지역 및 품질 개선으로 향후 서비스가 활성화 될 것으로 예상됨	연평균 7.1%씩 성장하여 2010년에는 3천4백억 원 규모로 성장이 예상됨	최근, 국내 이동통신 단말 휴대폰 판매량은 2008년 계속해서 200만대를 돌파했지만, 연속 하락세를 보이고 있으며, 국내 수요의 경우 대부분이 고가 폰으로의 교체수요에 해당됨
	국외	120억$(보안시장 열려있음)	세계 30여 개국에서 와이브로 서비스 도입을 준비하고 있어 향후 서비스가 활성화 될 것으로 예상됨	연평균 10%씩 성장하여 2010년에는 28억 달러 규모로 성장이 예상됨	세계 이동통신 가입자는 2006년 말 기준으로 27억 5,000만 명을 넘어섰으며 2007년에는 16.8% 증가한 32억 2,000만 명, 2008년에는 36억 5,000만 명, 2009년에는 39억 6,000만 명을 웃돌 것으로 추정됨
기술개발 현황 및 전망	국내	키관리 및 인증기술 일부 확보	IMS기반 기술개발 등을 통해 WCDMA와의 영상통화 및 다양한 부가서비스 개발되고 있음	사용자 인증 및 접근제어, 홈디바이스 인증 및 인가기술 등이 개발되었음	ETRI를 중심으로 LTE 시스템을 개발. 관련 기업에 기술이전을 하였으나, LTE/SAE 시스템에 보안기능이 없어서, 상용화를 위해서는 추가로 보안을 추가적으로 개발 보완예정임
	국외	주파수 및 기본 스펙에 중점 SPINS.u-TELSA 등 프레임워크 개발	미국, 유럽, 일본 등에서 서비스 도입을 위해 활발한 와이브로 기술개발이 이루어지고 있음	VPN, Firewall 기능이 탑재된 홈게이트웨이 제품이 개발되었음	노텔, 에릭슨은 LTE 시스템 장비를 선보이고 4G를 구현할 수 있는 세계 최고 속도의 장비를 시연하였으나 보안 기술에 대하여는 아직 추가 개발 없는 상태임
기술개발 수준	국내	설계	시제품/프로토타입	시제품/프로토타입	설계
	국외	시제품/프로토타입	시제품/프로토타입	시제품/프로토타입	설계
	기술격차	별로 없음	세계최고 수준	별로 없음	별로 없음
	관련제품	한백전자 Ubicoin, ZigBeX, 하이버스 Hmote 등	기지국, 제어국 시스템, 안테나, 와이브로 모듈	홈게이트웨이, 홈서버, 월패드 등에 탑재되는 보안소프트웨어(인증 및 접근제어, 침입대응) 홈디바이스용 보안소프트웨어(인증 및 접근제어)	차세대 이동통신 단말, HSS시스템
IPR 보유현황	국내	20여 건	217여 건	20여 건	해당사항 없음
	국외	500여 건 예상(주로 하드웨어)	915여 건	100여 건	해당사항 없음
IPR확보 가능 분야		USN 키관리 및 인증기술(S/W), Secure Routing 기술, 경량 IDS 기술	와이브로에서 이종 네트워크로의 핸드오버 시 인증 기술, 4G(IMT-Advanced) 보안 기술	홈네트워크 보안관제 기술, 홈네트워크 융합보안기술	해당사항 없음
IPR 확보 가능성		매우 높음(S/W)	매우 높음(S/W)	매우 높음(S/W)	해당사항 없음
표준화 현황 및 전망		현재 미흡하나 활성화 가능성이 매우 높음	와이브로 기술이 IEEE802.16e에 반영되었으며, ITU 3G(IMT-2000) 표준으로 채택됨, 2010년 예정인 ITU 4G(IMT-Advanced) 표준 반영 추진 예정	ITU-T SG17의 Question9에서 표준안 진행	정보보호 분야의 활동은 미흡한 상태
표준화 기구/단체	국내	TTA, 기술표준원	TTA PG302	TTA, HNSF	TTA
	국외	IEEE, ITU-T	IEEE 802.16, ITU	ITU-T	3GPP, 3GPP2, ITU-R, IETF
	국내참여 업체 및 기관현황	ETRI, KISA, NIA	삼성전자, 포스데이타, ETRI 등	ETRI, KISA	ETRI, KISA
	국내기여도	적극 활동 시작	크게 기여하고 있음	적극 활동	높음

구분		네트워크 보안			
표준화 수준	국내	표준기획	표준화 항목승인	일부표준 제/개정 일부 표준 기획	표준안 개발/검토
	국외	표준화 항목승인	표준화 항목승인	일부표준 제/개정 일부 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	높음

구분		네트워크 보안			시스템보안
표준화 대상항목		무선근거리통신망 보안기술	차세대 네트워크 보안기술	사이버공격 역추적/보안관리 기술	봇넷 대응 기술
시장현황 및 전망	국내	시장규모는 차후 2010년까지 평균 22.4%의 성장이 예상됨. 기간망으로 활용될 가능성이 높음	차세대 네트워크는 방송 및 통신의 융복합에 따른 안정성 보장을 위한 IDS/UTM 등의 네트워크 보안 장치에 대한 수요가 급증할 것으로 예측됨	보안컨설팅분야의 약진 및 정책적 보안관리 인식 강화 등에 힘입어 향후에도 꾸준히 팽창할 것으로 기대되는 분야임	봇넷 탐지 및 대응 기술은 연구 초기 단계로 시장이 형성되지 않았지만, 봇넷으로 인한 피해 확산 및 대응 요구에 따라 관련 분야 시장 형성 및 성장이 예상됨. 시장 규모는 2005년 6,807억 원 규모에서 2011년에는 1조 1,821억 원 규모에 이를 전망이며 연평균 9.64%의 성장률을 보일 것으로 예측됨
	국외	장비 업체가 표준 기관보다 앞장서서 트렌드를 주도하는 상황이 발생. 홈네트워크와 기업네트워크를 위한 장비 시장의 성장이 예상. 차후 국가규모의 대형 프로젝트가 시장을 주도할 것으로 예측	네트워크 장비 업체(시스코, 노키아 등)를 중심으로 UTM(Unified Threat Management) 어플라이언스, ITSoC 및 보안모듈 형태로 네트워크 장비에 통합하는 추세임	ESM, TMS, RMS 등과 같이 다양한 형태로 개발되고 있으나 각각이 뚜렷한 차별성을 갖지 못하고 단지 ESM을 고객의 요구에 맞게 일부 수정한 형태로 나타나고 있으며, 사이버공격에 대한 원천봉쇄 효과 및 원인규명을 위해 역추적 필요성만이 제기되고 있음	봇넷 탐지 및 대응 기술은 연구 초기 단계로 시장이 형성되지 않았지만, 봇넷으로 인한 피해 확산 및 대응 요구에 따라 관련 분야 시장 형성 및 성장이 예상됨. 시장 규모는 '05년 323억 달러 규모로 파악되며, 연평균 15.6%로 성장하여 '10년 666억 달러에 이를 것으로 전망됨
기술개발 현황 및 전망	국내	사용자의 높은 요구에 따라서 이종 네트워크와의 통합이 추진되고 있음. 통합 네트워크에서 발생하는 보안 문제점들에 대한 해결책이 제안되고 있지만 아직 성능이 확인되지 않았음	광대역 환경에 적합한 고성능 네트워크 보안장비 개발되고 있으나, 이동 무선 환경이 상용화되고 있으나 유무선 통합 환경을 고려한 보안 기술에 대한 연구는 초기단계	현재 보안프로토콜의 표준화를 통해 타사 제품을 포함한 이기종 보안 시스템가의 연동 기술로 발전하고 있으며, 향후네트워크 전체를 보안관리 영역대상으로 확장될 것으로 예상되며, 다중 도메인 간의 침해사고 공유 및 공격 위치 추적을 위한 기술개발이 진행되고 있음	봇넷 역추적 기술 및 봇넷 탐지와 대응과 관련된 기술이 연구목적으로 제안되고 있으나 검증이 되지 않은 상태이며, 봇에 감염된 PC에 의한 C&C 서버로의 접속을 차단하는 DNS 싱크홀을 이용한 봇넷에 대응하는 시스템이 가동되고 있음
	국외	전 세계적으로 이동통신망, 무선랜, 광대역 통신 간의 경합이 일어나고 있고, 서로 장단점을 가지고 있기 때문에 상호 보완적으로 통합될 것으로 예상됨	BcN 보호를 위한 보안장비도 기가급 제품 및 10G 이더넷 제품의 출시가 진행 중이며, 통합 유무선 네트워크 기술 및 기반기술 개발이 활발하게 이루어지고 있음	장비 및 인프라의 공격상황을 직관적인 파악과 추적기술을 포함하려는 요구사항과 이를 실현하려는 연구개발이 진행되고 있음	IRC, HTTP, P2P 봇넷 대응을 위해 호스트 및 네트워크 각각에서 시그니처 및 행위 기반 탐지 솔루션이 연구 개발되고 있으며, 일본 등에서 봇넷 대응 시스템이 가동되고 있음
기술개발 수준	국내	구현	설계	시제품/프로토타입-구현	설계
	국외	구현	설계	시제품/프로토타입-구현	설계
	기술격차	1.1	1.9	1.1	거의 없음
	관련제품	AP, Wireless LAN Card(NIC), 무선공유기, 무선 스위치	고속 침입방지시스템	보안관리, 시각화 기반의 이상 징후 분석, 웹 또는 이메일 서비스에서의 역추적 기술	침입탐지시스템, 백신
IPR 보유현황	국내	스마트 안테나 분야의 소수의 특허	트래픽 암호화 방법, 사용자 인증 메시지 보호 및 이를 위한 보안키 생성 방법, 암호화된 초고속 광대역 신호의 송/수신 방법 특허 다수	보안이벤트 시각화 및 보안이벤트 간의 상호연관성 분석 관련 다수 특허 확보	호스트 기반 악성코드 대응 관련 특허를 다수 확보하고 있으며, 꾸준히 증가세를 보임
	국외	라우터 간의 라우팅 정보 보안 기술 관련 특허 확보. 802.11 기반의 PHY 기반 특허, OFDM, MIMO 관련 특허	특허는 미국을 제외하고는 찾아보기 힘들며, 국내와 비슷한 수준으로 특허가 출원되어 있는 것 같음	침해사고 추적 관련 다수 특허 확보	봇을 포함한 악성코드 대응과 관련하여 미국, 일본 순으로 특허를 많이 보유하고 있으며, IRC/HTTP 봇넷 관련 특허를 많이 확보하고 있음
IPR확보 가능분야		현재 Draft가 진행되고 있는 표준에 대한 새로운 기준 제시, 차세대 이종 네트워크 간의 연동 기술 분야	이종망 간의 연동 보안 기술, 차세대 네트워크 침해사고 대응	침해사고 공유, 보안이벤트 상호연관성 분석, 보안이벤트 시각화	신종 봇넷 능동형 탐지 및 대응
IPR확보 가능성		보통	높음	높음	높음
표준화 현황 및 전망		현존하는 표준의 취약점에 대한 보안 기술들이 빠른 속도로 개발되고 있음. 차세대 기술의 도입으로 인한 시장 주도화에 표준화가 뒤늦게 따라가는 추세임	차세대 네트워크 보안 요구사항 및 참조모델, 통합연동 사용자 인증기술 등을 연구하고 있으며, 향후 융합서비스 분야에 대한 정보보호 기술 등이 표준화되고 있는 추세임	멀티 도메인 간 침해사고 데이터 형식과 이를 교환하기 위한 프로토콜에 대한 표준화가 추가적으로 요구될 것임	봇넷을 이용한 보안 위협의 증가 및 봇넷의 진화에 따라 체계적인 봇넷 대응 기술에 대한 표준이 요구되고 있음. 봇넷 탐지 및 대응 프레임워크 및 봇넷을 이용해 발송되는 이메일 스팸 대응 방안에 대한 표준 개발 작업이 진행 중에 있음

구분		네트워크 보안			시스템보안
표준화 기구/단체	국내	TTA	TTA	ISTF, TTA	TTA
	국외	IEEE	ITU-T, IETF	ITU-T, IETF, ISO	ITU-T
	국내참여 업체	ETRI, KISA	ETRI, KISA	ETRI, 이글루시큐리티, KISA	KISA
	국내기여도	표준화에 적극적으로 참여하지 않음	높음	높음	높음
표준화 수준	국내	표준안 개발/검토	표준안 개발/검토	표준안 개발/검토	표준화 항목승인
	국외	표준안 개발/검토	표준안 개발/검토	표준 제/개정	표준화 항목승인
국내표준화의 인프라수준		높음	높음	매우 높음	높음

구분		시스템 보안		
표준화 대상항목		서버 보안	PC 보안	디지털포렌식
시장현황 및 전망	국내	새로운 기술보다는 기존 기술을 개량하여 접근제어 메커니즘의 제한을 극복하는 등을 고려하는 서버 보안 솔루션이나 키관리와 소프트웨어 무결성 확인을 위한 트러스트 플랫폼용 트러스트 운영체제에 대한 요구가 증가할 것으로 예상됨	2008년부터 보안시장 전체적으로 저조한 성장률 예상. 안티바이러스 시장은 무료백신과 경쟁 심화로 인해 2.3% 성장률 예상. 단순한 안티바이러스 기능에서 개인방화벽, 개인정보보호 기능까지 포괄하는 통합 솔루션 공급 일반화. 내부정보 유출 방지 솔루션 시장이 활성화되고 있음	국내사건 대응 서비스 시장은 2011년 4,300억원에 이를 것으로 추정됨.(IDC 전 세계 시장 예측 규모 중 5%) 과학 수사 분야뿐만 아니라, 기업의 민 형사 분쟁 발생 시 관련 자료의 추출을 위한 기업 보안 포렌식 분야 시장이 활성화 되고 있음
	국외	NSA에서는 SELinux를 개발하였고, Linux 커널에 탑재되어 보안 서버 시장을 주도할 것임	안티바이러스 분야는 2008년도에 13억 달러 시장 예상	전 세계 사건 대응 서비스 시장은 2007년 $46억에서 연평균 17.8%씩 증가하여 2011년 %86억에 이를 것으로 추정(IDC, 2007)
기술개발 현황 및 전망	국내	기존의 서버 보안 운영체제의 기능을 개선하는 측면의 보안 기술 확보. RBAC과 MAC이 적용된 보안 운영체제에서의 신뢰채널 접근 제어 관련 특허를 ETRI와 산업체 중심으로 소유함	안티바이러스(Anti- Spyware), 개인방화벽/침임탐지, 내부정보 유출방지, 패치관리, 유해정보 차단, 데이터 복구 등 별개 기술로 개발되어 왔고 통합되는 추세임. 행위기반 등 새로운 진단법 연구. 속도 개선 및 경량화 연구. Generic Unpacking 연구	2007년부터 국가출연연을 중심으로 국산 파일에 특화된 기능을 내장한 통합 포렌식 도구 개발을 시작하였음
	국외	미국은 정부 차원에서 SELinux를 개발하여 공개 운영체제인 리눅스를 기반으로 연구를 진행하고 있음. 유럽은 국제공통평가표준(CC)에 맞게 PP 등을 개발하고 그에 알맞은 기술 연구가 진행중에 있음	장기적 측면의 미래 기술 연구. 시그니처 기반 진단법 개선 중.(양적 팽창 및 리소스, 퍼포먼스 등 고려) 행위기반 및 알려지지 않은 악성코드 기술 연구. 가상화 연구	디지털포렌식 산업의 잠재력에 대한 인식제고로 국가기관에서의 범죄수사 분야를 넘어 활용분야가 민간으로 확대되고 있으며 각국 기술개발 경쟁이 고조되는 상황임. 현재 디지털포렌식 도구를 상용화한 국가 중 가장 큰 기술력 및 시장규모를 가진 국가는 미국이며, 영국, 프랑스, 일본, 러시아 등도 분야별로 디지털포렌식 기술을 독자 개발 중에 있음
기술개발 수준	국내	시제품/프로토타입	설계	설계
	국외	구현 또는 상용화	시제품/프로토타입	시제품/프로토타입
	기술격차	2년	1 ~ -1.5년	미국-3년
	관련제품	접근제어 소프트웨어, 키관리 및 소프트웨어 무결성 검증	안티바이러스(Anti-Spyware), PC방화벽, 내부정보 유출방지, 패치관리, 유해정보 차단, 데이터 복구	컴퓨터 포렌식 도구, 모바일 포렌식 도구, 네트워크 포렌식 도구, e-Discovery 도구
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		디스트 이미징 및 데이터 분석
IPR확보 가능분야		보안 운영체제의 개선된 접근제어, 키관리 및 소프트웨어 무결성 검증 등. 운영체제 위에 탑재된 응용 기술에 대한 경쟁력 확보	악성코드 탐지 기술	고속 검색 분야
IPR확보 가능성		보통	낮음	보통
표준화 현황 및 전망		국내: TTA에서 리눅스 보안 표준규격 개발 국외: TCPA는 PC 기반의 산업 플랫폼, 운영체제, 응용 등의 보안규격을 개발	악성코드 명명법, PC 보안 로그 형식 표준, 패치관리	미국 NIST는 Special Publication 800 – series를 통해 컴퓨터 포렌식 및 모바일 포렌식에 대한 가이드라인을 발표하는 등 포렌식 분야의 표준화를 진행 중이며, CFTT 프로젝트를 운영하여 포렌식 도구 기능 검증을 국가적으로 주도하고 있음
표준화 기구/단체	국내	TTA	TTA	TTA
	국외	ITU-T, ISO/IEC, TCPA, WSSN 등	ITU-T, IETF	ITU-T, NIST, ASTAP
	국내참여 업체	ETRI 및 보안산업체	KISA, ETRI	ETRI, KISA, TTA
	국내기여도	높음	낮음	부분 선도
표준화 수준	국내	표준안 항목승인	표준안 기획	표준안 기획
	국외	표준 제/개정	표준안 최종/검토	표준안 기획
국내표준화의 인프라수준		높음	보통	보통

3. 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 하드웨어의 용량(CPU, Memory, Power 등)이 매우 제한적이어서 기존에 개발된 보안 인프라(공개키 기반의 인증 및 암호, IDS, NMS, IPSec 등) 적용이 불가능할 것으로 판단되며 국제 표준도 아직 초기 단계라 방향을 이끌고 갈 인력 및 기술력 필요함. 또한 인증 부분이 매우 중요한데 특히 암호 혹은 인증키의 선택에 따라 USN 적용 여부가 결정된다고 할 수 있음. 특히 브로드캐스팅 기반의 무선네트워킹 기술로 인한 각종 공격의 위협이 다양하게 존재 하고 있어 표준화된 기술의 정의가 어려운 부분도 많이 있음

○ 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

○ 홈네트워크 보안의 경우, 킬러 서비스의 부재로 홈네트워크가 활성화되지 못하고 있어 홈네트워크 보안 제품에 대한 수요가 없었으나 지경부를 중심으로 홈네트워크 활성화에 대한 적극적인 정책지원이 예상되고 있어 홈네트워크 보안제품의 활용성이 높아질 것으로 예상됨. 향후 홈네트워크 보안제품의 활성화에 대비하여 다양한 홈네트워크 보안취약성을 해결하는 보안제품간의 연동성을 고려한 보안기술 표준화가 요구되며 특히, 아파트에서의 신변안전에 대한 수요가 급증할 것으로 생각됨에 따라 홈네트워크 IT보안과 홈네트워크 물리보안을 융합하는 홈네트워크 융합보안프레임워크에 대한 표준 기술 개발에 적극적인 투자가 필요한 상황임

○ 차세대 이동통신 기술 분야는 IMT-2000 표준화 그룹 중에서 유럽중심의 3GPP는 LTE 및 LTE- Advanced를 구성하여 IMT-Advanced로 표준화를 활발하게 추진하고 있음. 3GPP2 진영은 UMB, 1X, DO의 진화를 추진하는 의견과 보완차원으로 추진하는 논의가 진행 중이나 활발하게 추진되고 있지 않은 실정이고 국제적 표준으로 진행되는 상황이므로 산업계 차원에서의 국제적 이동통신관련 내용과 보안관련 내용을 모두 숙지하는 표준 전문가가 절대적으로 부족하고, 실적을 달성할 수 있는 가시적 표준화 활동이 어려우므로 중장기적인 정부차원의 지원 노력이 필요함

○ 무선 근거리 통신망 보안

- 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 무선 근거리 통신망이 더욱 더 활발히 보급되어 보안 취약성이 대두 될 것으로 전망되고 있으며 이에 따라 국제적으로 논의되고 있는 보안 표준 제정에 발맞추어 국내 기술이 이 분야에서 뒤처지지 않도록 해야 함
- 현 시점에서 통신의 발전 경향은 기존의 기술을 배제한 채 새로운 기술을 도입하는 방향으로 진행되었다면 앞으로의 발전은 기존에 구축이 완료된 망을 바탕으로 통합, 융합을 추구하는 방향으로 이루어질 것임. 이 때 현재 구축되어 있는 시스템을 활용하기 위해서는 현존하는 취약점에 대한 분석 및 적절한 해결책이 제시되어야 함. 이미 완성된 기술이기 때문에 제외하는 것이 아니라 완성된 기술로 만들기 위한 준비와 투자가 필요함
- 근거리 통신 기술이 매우 다양하게 보급되고, 또 기업들에 의해서 적극적으로 서비스가 되고 있지만 국내 수요에 비해 과잉 경쟁이 이루어지고 있기 때문에 각각의 서비스의 통합을 통한 효율적인 서비스 제시를 위해서 연구가 필요하고 국내 시장이 아닌 더 넓은 세계로의 방향 전환을 위해서는 국제 표준에 대한 적극적인 관심과 연구가 병행되어야 함
- 대형 기업들과 미국의 IEEE에 의해서 모든 표준화가 진행되고 있기 때문에 표준 자체가 지나치게 편향적으로 설계될 수 있으며 차세대 표준에서 이점을 확보하기 위해서는 표준의 전개에 참여 필요함

○ 차세대 네트워크의 경우, 연관된 표준화 그룹이 상호 기술적, 정책적으로 토의하고 조율 할 수 있는 협력이 필요하나, 국내외 표준화 활동이 그룹 내의 활동에 머물고 있음

- 차세대 네트워크 기술 분야가 융 · 복합화됨에 따라 일관되고 안정적으로 적용할 수 있는 국가적 표준기술 개발이 필요한 반면에, 기술개발 인력과 표준화 인력과의 유기적인 협력이 이루어지지 못해, 표준 기술이 시스템 개발에 빠르게 적용되지 못하고 있음
- 또한 산업계 차원에서의 표준 전문가가 절대적으로 부족하고, 개선을 위한 적극적 지원이나 인력 양성을 위한 투자가 기업체에서는 미미한 실정이므로 정부차원의 지원 노력이 필요함

○ 사이버공격 역추적/보안관리 기술의 경우, 각 업체별로 자사 제품 시장을 위해 현실적인 보안제어 표준 규격 적용 여건 부족이나, 향후 도래할 다중 관리 도메인 환경에서의 공격자 추적 기술과 표준화에 대한 필요성이 대두될 것이며 이에 대한 적극적인 투자가 필요한 실정임

○ 봇넷 대응 기술

- 기술 특성 상 국제적인 협력이 요구되나 현재 관련 표준화 활동은 미비한 편임
- 현재 국내에서는 KISA에 의해 봇넷 대응이 이루어지고 있음

- 이상적이고 실용 가능한 기술 및 표준 개발을 위해서는 각국의 봇넷 대응 시스템을 운영 중인 유관기관과의 협력을 통한 표준화 추진이 필요함
- 봇넷 탐지 및 대응을 위해서는 봇에 감염된 피해자의 트래픽 정보에 대한 수집 및 공유를 가정하고 있는데, 사용자의 트래픽을 다루는 문제에 대해서 신중한 접근이 필요함
- 기술 개발 및 운영 인력 그리고 표준화 추진 인력간의 유기적인 협력이 필요함
- 국제적인 봇넷 대응의 필요성을 인식하고 ITU-T SG17 보안 그룹에서 봇넷 대응을 위한 표준화 추진을 결정하였고, 개발이 착수됨

○ 서버 보안 기술
- 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
- 서버 보안 부분에 대한 표준화를 주도하고 있으며 서버 보안 관련 국내 특허를 가장 많이 보유하고 있는 곳은 ETRI임. 표준화와 제품 개발이 병행되어야 이상적인 표준화 추진이 되겠지만, 업체에서의 표준화 활동은 미비한 실정임
- 정부에서는 CC인증을 확대하고 제품 구입을 활성화함으로써 업체의 제품 개발 및 표준화 활동을 적극적으로 유도할 수 있음
- 몇 년 전보다 오히려 격차가 벌어진 운영체제 커널 기술에 대한 정부의 투자를 확대하고 국가 표준의 보안 운영체제를 구축할 수 있는 기회를 제공하여 국제 경쟁력을 확보하고 나아가 국제 표준화 활동을 주도할 필요가 있음
- 운영체제 커널 외에 서버 응용 기술의 경우 국내 기술이 경쟁력이 있으므로 웹서버 보안 기술, 소프트웨어 무결성 검증 기술, 접근통제 및 감사추적 기술, 플랫폼 임의조장 방지 기술 등에 대한 표준안을 마련하고 기술력을 보유한 산업체와 정부가 협력하여 표준화를 추진한다면 국제적으로 이 분야에 대한 표준화를 선도할 수 있음

○ PC 보안의 경우, 표준화 추진 의지 낮고 업체 간 경쟁 심화 및 정보 공유 필요성 없음
- 각 업체별로 자사 제품을 관리하는 제품을 보유하고 있음
- 경쟁적인 상황에서 타사 제품을 반영 필요성 낮음
- 통합관리 요구로 로그 형식 등 표준화가 요구되고 있으나 추진 의지도 낮고 현실적인 어려움이 존재함

○ 디지털포렌식
- 범죄 수사와 관련된 부분은 각 국의 사법 환경을 반영한 가이드라인 및 증거 수집 절차 등의 제정이 우선적

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

- 현재 미국은 NIST에서 디지털포렌식 관련 프로젝트 및 가이드라인 등의 표준을 제정하고 있으며, 최근 ITU-T SG 17, ISO/IEC JTC1 SC27 WG4 등의 국제 표준화 기구에서도 포렌식 조사 등의 내용으로 표준화 추진 초기 단계에 있음

3.1.2. SWOT 분석 및 표준화 추진방향

국내역량요인 / 국외환경요인			강 점 요 인 (S)	약 점 요 인 (W)
		시장	– 네트워크 보안 시장의 확대로 보안 시장이 증가하고 있으며 세계 최초로 상용서비스를 시작하여 서비스 시장에 앞장서 있음 – 개인정보보호법 제정에 따른 시장 활성화 예상 – 연 계약에 의한 지속적인 시장창출 – 국내 원천 기술 보유	시장 – 네트워크 보안 시장에 대한 상대적 투자 미흡하고 경기 침체에 따른 기업 투자비용 감소 – 국외 산업과 유사하게 유선 인터넷 보호 위한 특정 기술 분야에 집중되어 있음에도 불구하고, 외산 장비가 시장 주도권을 쥐고 있는 상태임 – 우리보다 기술개발이 앞선 외산 장비가 시장 주도권을 가지고 있는 상태
		기술	– 보안운영체제에 대한 연구개발 성과에 대한 기대 – 통합화 추세에 각 요소기술 보유 – 학계 및 산업계가 협력하여 핵심 기술 개발 – 특히 융·복합 기술이 주목받고 있음	기술 – IT 환경 변화에 따른 다양한 기술 요구 사항 만족시키기 위한 투자 및 연구가 부족 – 보안 장비 분야는 국외와 유사하게 고성능 산업적 토대는 미약한 상태
		표준	– 네트워크 보안 분야는 시작단계로 발굴 대상 항목이 많고 특히 융·복합 기술이 주목받고 있음. 또, 국내 표준이 국제 표준과 유사하며 국내 전문가가 국제 표준을 주도하고 있음 – 시스템 보안은 시작단계이고 절차 및 기술적 관점에서 표준화 진행	표준 – 보안 역량 인프라에 대한 투자 미흡 – 네트워크 보안 관련 표준을 IETF 및 ITU-T에서 진행하고 있으나 IPR 확보 노력이 필요 – 시스템 보안 분야의 국내 표준화는 시작 단계이며, ITU-T 등에서의 국제 표준화를 위한 IPR 확보가 아직 미비함 – 산업체의 인식 부족
기회요인 (O)	시장	– 미국, 유럽 및 일본이 기반 기술의 확보에 주력하므로 보안 기술 시장에 대한 기회 – 개인정보보호법 제정에 따른 수요 확대 – 개인인터넷환경의 지속적인 발전 – 전 세계 사건대응 시장의 급속한 증가에 따른 포렌식 신규시장에 대한 기회	**현황분석에 의한 우선순위: 1** – 많은 USN 활용 분야에 시장 확보가 우선 필요 – 표준화 역량 강화에 인력 육성 – 세계 최초로 와이브로 상용서비스 시작하여 도입을 준비하는 타 국가에 비해 앞서가고 있음 – 고정형 와이맥스 기술보다 와이브로 기인 이동형 와이맥스 기술 시장규모가 더 클 것으로 예상 – 이동통신과 달리 국내에서 다수 특허를 보유 하고 있어 로열티 등을 지급하지 않아도 됨 – 국내 표준전문가가 국제 표준 주도하고 있음 – 유무선 통합망 환경에 적용할 수 있는 IT 서비스를 위한 정보보호 기술 개발 – 보안 가용도 극대화를 위한 공통 보안관리 프레임워크 표준화 추진 – 우선적인 국내 표준화 추진 및 ITU-T, ISO/IEC JTC1 등의 표준화 단체를 통한 적극적인 표준화 추진 – 휴대 인터넷 보안 및 홈네트워크 보안, 사이버 공격 역추적 및 보안 관리 분야에 대한 기술 개발 및 표준화에 중점을 둘 필요 있음	**현황분석에 의한 우선순위: 2** – 와이브로 상용서비스를 시작하고 있으나, WCDMA 등 유사 서비스와의 경쟁으로 여전히 서비스 활성화 초기 단계에 있으므로, 국내 와이브로 서비스를 활성화를 통해 성공적인 모델을 제시 – ITU-T와 IETF에서 표준화를 수행하고 있으므로, 이 표준화기구의 표준화 동향을 근거로 관련 제품과 서비스 개발 – 중장기적인 전략으로 국제 표준화 활동 통한 해외 의존도 트러스트 플랫폼 모듈 기반의 트러스트 서버용 보안 운영체제 기술 확보 – 우선적인 국내 표준화 추진 및 ITU-T, ISO/IEC JTC1 등의 표준화 단체를 통한 적극적인 표준화 추진 – USN 보안 분야 및 PC 보안 분야는 국내 표준 개발이 기술 개발을 앞서 있어서 국제 표준을 선도할 수 있음
	기술	– 네트워크 분야의 보안 기술의 격차는 거의 없으므로 선점시 기술의 표준 가능성 증대 – 네트워크 장비 보안기능 탑재하여 고성능화 – 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	– 보안 표준화 항목 발굴이 현재 미흡하므로 적극적인 참여 및 투자로 항목 발굴에 유리 – 네트워크 보안 영역에서의 기술 표준화 진행 가속화 – 연구개발 확대로 인한 기술 확보		
			SO전략: 공격적 전략(강점사용–기회활용)	SO WO WO전략: 만회 전략(약점극복–기회활용)
			ST전략: 다각화 전략(강점사용–위협회피)	전략 ST WT WT전략: 방어적 전략(약점최소화–위협회피)
위협요인 (T)	시장	– 네트워크 보안 분야 국내 기반기술의 약화로 인한 수익성 저하(Royalty) – 유·무선 통합용 네트워크 인프라 방어용 보안 시장 미비 – 기업 보안 관리 제품들이 민사소송의 e-Discovery 분야의 경쟁 기술이 될 수 있음	**현황분석에 의한 우선순위: 3** – R&D에 많은 투자를 통한 기반 기술 확보 – 시장 발굴에 따른 보안 시장의 육성 – ISO/IEC 등 선도 표준 기구의 진입을 위한 국제 표준 전문가 그룹과의 연대를 통한 국제 표준의 협력 및 서버 보안 기술의 경쟁력 확보 – 새로운 포렌식 분야에 대한 R&D 투자 통한 기반 기술 확보 – 적극적인 투자 및 기술 개발을 통한 디지털 포렌식 핵심 기술 개발	**현황분석에 의한 우선순위: 4** – 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 – 산학연 표준 협력 체계 구축으로 국제 표준화 활동의 지속적인 참여를 통한 기존 표준과의 호환성 유지 및 표준 전문 인력양성
	기술	– 보안 기술 개발 회사의 투자 미흡 – 국제 경쟁력 심화 및 장기 대응 기술 미비 – 새로운 형태의 공격 등장 – 투자 미흡으로 원천기술의 IPR 확보 미흡		
	표준	– 표준 역량 인프라 투자 미흡시 표준 기술 외국이 점령 가능 – 타 사업자와의 관리정보 연동 부재에 따른 보안연동성 부재		

○ 현황분석을 통한 우선순위

- 1순위-SO 전략: 휴대 인터넷, 홈네트워크, 사이버 공격 역추적 및 보안 관리 분야는 미국, 유럽, 일본 등 해외에서 기반기술 확보에 주력하고 있고, 향후 관련 시장이 확대될 것으로 예상되며, 국내에서 관련 원천 기술 및 표준을 보유하고 있어 이 분야에 대한 중점 표준화를 통해 국제표준을 선도할 필요가 있음
- 2순위-WO 전략: 기술 개발대비 표준화가 상대적으로 미비하여 약점/기회요인으로 분석된 USN 보안 분야는 향후 시장이 확대되고 IPR 확보 가능성도 높아 기업들의 표준 활동 참여를 강화할 필요가 있음
- 3순위-ST 전략: 기업 보안관리 제품들이 민사소송의 e-discovery 분야의 경쟁기술이 될 수 있으므로 다양한 전자 매체의 디지털 증거 수집 가이드라인, 디지털 증거 수집 및 분석 규격, 이미징 규격 등 디지털포렌식 분야의 R&D 투자 확대를 통한 기반기술 확보 및 시장 발굴이 필요함
- 4순위-WT 전략: PC 보안 로그 표준화의 필요성은 있으나 국내 기업 간 경쟁 심화로 현실적 문제가 있으나, 최근 각 안티바이러스 업체들이 테스팅에 대한 표준화 논의가 되고 있기 때문에 글로벌 테스팅 표준화에 국내 업체도 참여하여 그 움직임에 따라 기술 개발과 대응책을 마련할 필요가 있음

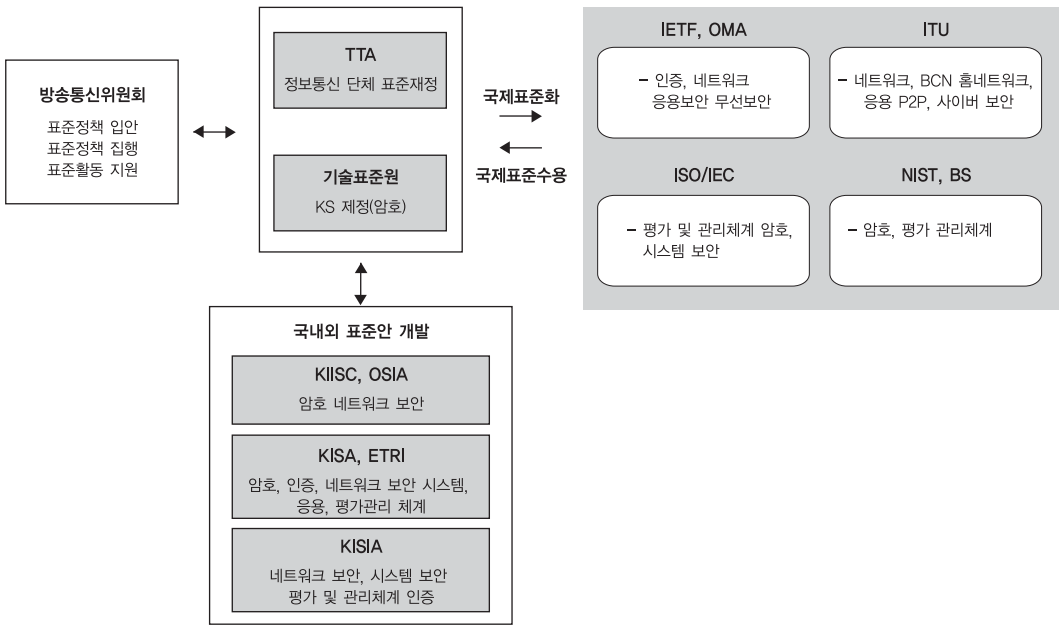
○ 표준화 추진방향

- 정부는 USN 보안 문제를 해결하기 위한 기술 로드맵 및 항목별 연구반을 만들고 장기적인 표준화 로드맵의 개발이 필요함
- 시장 규모가 급속히 확대될 것으로 예측되므로 ISO SC27에 적극 참여할 수 있는 인력 선정과 IPR 확보를 위한 현실적인 지원을 보고 할 것임
- 2008년부터 TTA의 정보보호 기술위원회(TC5)를 신설 분리 운영하도록 보다 적극적인 체계를 갖추었으며 PG504 프로젝트 그룹에서 USN 관련 표준화 작업을 적극 운영하며 R&D와 표준화가 연동되어 활동 하도록 R&D Fund 조성을 유도 할 것임
- 와이브로 서비스가 활성화되면 기존 무선랜 환경에서 발생했던 단말/기지국에 대한 서비스거부공격, 세션하이재킹, 인증우회 등 와이브로에서 발생 가능한 보안 취약성에 대한 대비가 필요함
- 와이브로 기술을 IMT2000 표준 기술로 진입시켜 기존 이동통신서비스와 동등한 위치를 확보한 후, 와이브로 서비스에서의 보안기술에 대한 국제 표준 활동 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
- 국제 표준 수용과 프로파일 표준 개발 작업을 추진함에 있어 산업체의 제품 경쟁력과 관련이 깊은 핵심 기술

과 트러스트 플랫폼 기술에 대해서는 선행 시제품 개발을 병행하여 추진함으로써 표준 개발의 품질 제고 및 확보되는 핵심표준 기술을 산업체에 제공하여 개발 표준이 조기 상용화되도록 추진

- 서버 보안 및 트러스트 플랫폼 기반 소프트웨어 무결성 검증 기술 및 플랫폼 임의 조작 방지 기술 등은 국제표준화 기구에 미래 표준 기술 분야로 선행 표준 기술 연구 활동을 적극 추진하여 신규 표준화 분야에 대한 국제 표준 선점을 위한 국제 표준화 활동을 강화함
- 통합 PC 보안이 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
- IT 기술 환경 변화에 따른 다양한 디지털포렌식 요구사항을 만족하는 기술 및 포렌식 도구의 신뢰성을 확보할 수 있는 검증 방안을 개발하여 IPR 확보 및 국내외 표준화 추진
- 각 안티바이러스 업체들이 테스팅에 대한 표준화 논의가 되고 있기 때문에 국내 업체도 참여하여 그 움직임에 따라 기술 개발과 대응책을 마련해야 함

3.1.3. 표준화 추진체계



○ 전체에 대한 추진 체계로 재작성(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)

○ 와이브로 보안 기술은 산업체를 중심으로 TTA를 통하여 국내 표준을 추진하고 ITU-T를 중심으로 국제 표준화를 추진

○ 홈네트워크 보안기술은 ETRI, KISA, 학계 및 관련 산업체를 통하여 국내외 표준을 개발하고, 국내의 경우 홈네트워크시큐리티포럼 및 TTA를 통하여 수행하고, 국제표준은 ITU-T를 통하여 표준화를 추진

○ 이동통신망 보안 기술은 이동통신 사업자와 정보보호 전문가의 협력에 의한 3GPP, 3GPP2 표준화 주도권 확보가 요구되며 이를 위한 TTA, 지경부의 지원이 절실함

○ 이동통신 단말업체와 서비스 사업자, 정보보호 전문업체, ETRI, KISA 등을 중심으로 국내외 표준(안)을 개발하고, TTA를 통하여 국내 표준화를 추진하고 3GPP, 3GPP2, ITU-T SG17를 통하여 국제 표준화를 추진함

○ 무선 근거리 통신 보안 기술은 ETRI, 학계 및 관련 산업체를 통하여 국내외 표준을 개발하고, 국내의 경우 TTA를 통하여 수행하고, 국제표준은 IEEE를 통하여 표준화를 추진함

○ 차세대 네트워크 보안 기술은 BcN 포럼을 통하여 산업체의 표준화 참여를 유도하며, 국내표준은 TTA를 통하여 추진하며, 국제표준은 ITU-T SG13을 통하여 추진함

○ 사이버공격 역추적/보안관리 기술은 ETRI, 학계 및 관련 산업체를 통하여 국내외 표준을 개발하고, 국내의 경우 TTA를 통하여 수행하고, 국제표준은 ITU-T 를 통하여 표준화를 추진하고 있으며 국제표준 추진을 위해서 해외 유관기관과의 긴밀한 협력을 추구함

○ 봇넷 대응 기술은 KISA를 통하여 국내외 표준을 개발하고, 국내의 경우 TTA를 통하여 수행하고, 국제표준은 ITU-T SG17을 통하여 표준화를 추진함.

○ PC 보안 기술은 인터넷보안기술포럼(ISTF)을 통해 산업체 자율적으로 표준화를 추진하되 TTA를 통하여 국내표준을 추진함

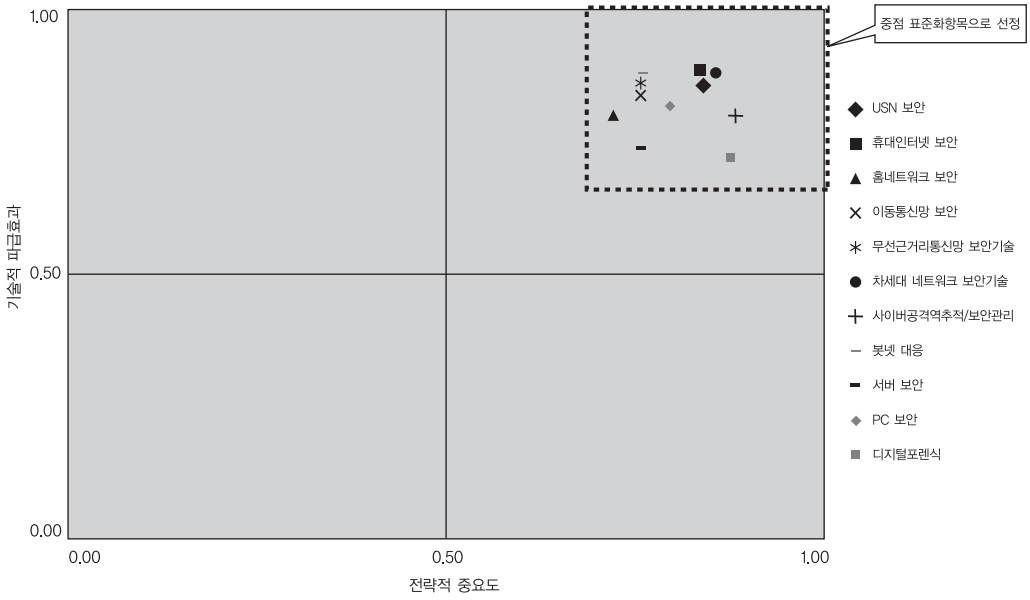
○ 디지털포렌식 기술은 ETRI, 학계 및 관련 산업체를 통하여 국내외 표준을 개발하고, 국내의 경우 TTA를 통하여 수행하고, 국제표준은 ITU-T를 통하여 표준화를 추진함

3.2. 중점 표준화항목 선정

3.2.1. 중점 표준화항목 선정방법

중점기술 후보별 전략적 중요도 및 기술적 파급효과 분석

평가지표	전략적 중요도(Priority)						기술적 파급효과(Effect)					
	P1 정부 및 산업체 의지(국가 산업 전략과의 연관성, 국내기업의 표준화 참여 및 관심도 등)	P2 공공성(사용자 편리성, 중복투자 방지 등)	P3 적시성	P4 기술적 선도 가능성(국제표준 경쟁력, IPR확보 등)	P5 국제표준화 이슈정도	PI (Priority Index)	E1 기술적 중요도(원천성 등)	E2 타 기술에 파급효과(연관성, 활용성 등)	E3 시장파급성 및 상용화 가능성(구현가능성 등)	E4 산업적 파급효과(산업화로 인한 이득, 국내 관련 산업 규모 및 성숙도 등)	E5 미래 영향력(미래 표준항목에의 적용/응용성)	EI (Effect Index)
평가지표의 중요도 / 표준화 대상항목	0.19	0.19	0.21	0.21	0.20	–	0.20	0.20	0.20	0.20	0.20	–
USN 보안	8.00	9.00	7.00	9.00	9.00	**0.84**	8.00	8.00	9.00	9.00	9.00	**0.86**
휴대인터넷 보안	9.00	9.00	8.00	8.00	8.00	**0.84**	8.00	9.00	9.00	9.00	9.00	**0.88**
홈네트워크 보안	6.00	8.00	8.00	8.00	6.00	**0.72**	8.00	8.00	8.00	8.00	8.00	**0.80**
이동통신망 보안	8.00	9.00	8.00	6.00	7.00	**0.76**	6.00	9.00	9.00	9.00	9.00	**0.84**
무선근거리통신망 보안기술	8.00	8.00	8.00	7.00	7.00	**0.76**	7.00	9.00	9.00	9.00	9.00	**0.86**
차세대 네트워크 보안기술	9.00	9.00	8.00	8.00	9.00	**0.86**	8.00	9.00	9.00	9.00	9.00	**0.88**
사이버공격역추적/보안관리	7.00	9.00	9.00	10.00	9.00	**0.88**	9.00	9.00	7.00	7.00	8.00	**0.80**
봇넷 대응	8.00	8.00	8.00	7.00	7.00	**0.76**	8.00	9.00	9.00	9.00	9.00	**0.88**
서버 보안	8.00	9.00	8.00	6.00	7.00	**0.76**	7.00	8.00	7.00	7.00	8.00	**0.74**
PC 보안	9.00	9.00	8.00	7.00	7.00	**0.80**	8.00	7.00	10.00	9.00	7.00	**0.82**
디지털포렌식	9.00	10.00	9.00	8.00	8.00	**0.88**	7.00	7.00	8.00	7.00	7.00	**0.72**



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, 기술 개발 시 국내외적으로 시장경쟁력을 확보할 수 있는 분야를 중심으로 도출된 표준화 대상 항목을 모두를 중점 표준화항목으로 선정하였음. 네크워크 보호 기술과 응용 보안은 정보보호산업에 커다란 파급 효과를 갖는 분야임. 이와 같은 기준에 따라 USN 보안기술, 휴대인터넷 보안기술, 홈네트워크 보안기술, 이동통신망 보안기술, 차세대네트워크 보안기술, 사이버공격 역추적/보안관리 기술, 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
- 홈네트워크 보안 분야는 홈네트워크 서비스에 대한 선호도 설문 결과, 사용자의 선호도가 가장 높은 서비스였으므로, 사용자의 요구사항을 반영한 홈네트워크 융합보안서비스가 개발될 경우 새로운 홈네트워크 킬러 서비스로 부상될 수 있는 분야임
- 이동통신망의 경우, 국내외적으로 이동통신의 의존도가 높아지고 있으므로 해당 원천기술의 전략적 선점 및 표준화 주도를 통하여 이동통신 기술로 인한 로열티 부담을 줄이고, 표준 특허로 인한 로열티 수익의 발생을 통한 경제적 부가가치 및 생산 유발 효과를 유도함

- 무선근거리통신망 보안기술은 국내외 기술격차는 거의 없지만 표준화 진행에서 큰 차이를 보여주고 있음. 표준 선도 가능성은 낮지만 현존하는 표준과 개발되는 표준들을 정확히 적용하기 위해서 국내 표준의 도입의 중요성이 높음. 다수의 대중들을 위해서 안전한 네트워크를 제공하기 위해서는 근거리 무선 통신 기술의 공공성을 크게 판단
- 차세대 네트워크 보안은 공공성이 크고, 새로운 융복합 서비스의 안정성 보장을 위한 네트워크 보안 장비 산업 분야의 경제적 파급 효과가 크며, 국내외 기술 격차가 적어 국제 표준을 선점할 수 있는 분야임
- 사이버공격 역추적/보안 관리는 공공기관 및 민간기관의 각 중앙행정기관 및 지방행정기관, 민간 침해대응센터, 정보보호 솔루션업체 등과 같은 기관으로부터 보안 강화를 통해 민간 산업 분야로의 파급 효과를 갖는 분야임
- 봇넷 대응 기술 분야는 전 세계적으로 우수한 사례라고 인정받고 있는 대응 체계를 KISA가 구축하고 있으며, 표준화 활동이 미비한 실정에서 관련 기술 표준화를 주도하고 있음
- PC 보안 분야가 국내 보안 소프트웨어 시장을 주도하고 있으며, 전체 위협의 대부분이 악성코드와 관련이 있음. PC의 경우, 취약점을 이용한 공격이 많아지고 있기 때문에 패치관리, 백신, 정보 유출 등 PC 보안 분야에 대한 연구 필요
- 디지털포렌식 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 분야로, 공공성이 크고 새로운 보안 서비스 시장 창출할 수 있음

○ 중점 표준화항목별 선정사유

- USN 보안기술
  - TTA의 정보보호기술위원회(TC5)에 PG504 프로젝트 그룹에서 응용 서비스 보안 표준개발을 주 항목으로 하여 이미 USN 관련 보안 표준을 제정하였고, 점차 확산되는 USN 서비스의 안전한 활용과 정착을 위해 USN 서비스를 위한 인증 기술, 안전한 라우팅 기술, 경량 침입탐지 기술 등이 표준화 항목으로 우선 진행될 필요성을 공감 하고 과제 제안 및 표준제정을 위해 노력하고 있음
- 휴대인터넷 보안기술
  - 와이브로는 IMT-Advanced 환경에 적합하도록 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, 이기종 네트워크 간의 이동성 제공에 있어서도 인증 기술 등이 요구되므로 중점 표준화 항목으로 선정함
- 홈네트워크 보안기술
  - 우리나라가 홈네트워크 보안에 관한 표준화 활동이 가장 활발하고, 국제표준 또한 우리나라가 이끌어 가고 있음. 홈네트워크 및 홈네트워크 보안에 관한 종주국으로 내세우기에 손색이 없게 더욱 활발한 표준화 활동이 이루어질 수 있도록 지원이 필요함. 따라서 ITU-T SG17 Q.9에서의 표준화 활동을 지원하고 현재

국내 표준화가 완료되거나 진행 중인 표준들을 ITU-T에서 표준화가 이루어 질 수 있도록 홈네트워크 융합보안 프레임워크를 중점 표준화 항목으로 선정함

- 이동통신망 보안기술
  - 3GPP 보안, 3GPP2 보안을 중심으로 활발한 표준화 활동이 예상되며, 특히 이러한 NGN 및 단말보안기술 위주로 ITU-T SG17에서 보안기술 로드맵 작업이 이루어지고 있는 등 활발한 표준화 활동이 예상되므로 이를 중점 표준화 항목으로 선정함
- 무선근거리통신망 보안기술
  - TTA의 RFID/USN 프로젝트 그룹에 보안 워킹그룹 혹은 분리된 프로젝트 그룹을 만들어 운영하며, 경량의 암호 및 인증을 위한 키관리 기술, 안전한 라우팅 기술, 안전한 배치 기술 등이 USN 활성화를 위해 표준화 항목으로 선정함
  - 무선랜의 표준화는 일정 부분 완성되었다고 평가되나 안전한 기술을 적절히 활용하기 위한 대안이 제시되지 못하고 있기 때문에 관련 연구가 요구되고 있음
  - 현존하는 네트워크도 그 수가 매우 다양하여 앞으로의 미래 환경에서 다양한 기술을 융합해서 효율적으로 사용하기 위해서는 통합 환경에서 적용 가능한 표준 기술 개발이 선행되어야 함
  - 기존의 암호 기술들은 무선 환경을 가정하지 않은 기술이 많음. 현재 관련 기술들이 개발되고 다수의 알고리즘들이 제안되고 있지만 확실한 솔루션은 제안되지 않았음. 무선을 기반한 통신을 대상으로 하는 효율적인 암호 기술에 대한 요구가 증가하고 있음
- 차세대 네트워크 보안기술
  - 차세대 네트워크 구축 초기단계에서부터 사이버공격에 대한 상호연동이 가능한 조기 예방 및 대응체계를 구축하고, 사업자별 정보보호 대책 마련의 중요성 부각
  - 개별망 및 연동망 환경 발생할 수 있는 새로운 위협을 찾아내어 차세대 네트워크 보안 분야에 공통으로 적용할 수 있는 보안 프레임워크, 사업자별 통합、분산 인증, 융복합 서비스 보호 기술을 중점 표준화 항목으로 선정함
- 사이버공격 역추적/보안관리
  - 네트워크 차원의 보안관리 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 중점 표준화 항목으로 선정함
- 봇넷 대응 기술
  - TTA에서 관련 기술에 대한 표준 항목을 제안하여 채택되었고, 기술 특성 상 국제적인 협력이 요구되는데

반해 관련 분야 표준화가 미비한 상태였고, 전 세계적으로 우수하다고 평가되는 대응 체계를 국내에서 보유하고 있어, 관련 분야 표준화 주도 가능성이 높기 때문에 중점표준화 항목으로 선정함. 국제 표준화 기구인 ITU-T SG17 보안 그룹에서 봇넷 탐지 및 대응 프레임워크 개발과 봇넷을 이용해 발생되는 이메일 스팸 차단 기술에 대한 표준 개발을 착수하여 국내 연구진의 주도 하에 진행되고 있음

– 서버 보안

- 웹서버 보안 기술, 트러스트 플랫폼 기반 소프트웨어 무결성 검증 기술, 접근통제 및 감사추적 기술, 그리고 플랫폼 임의조장 방지 기술 등은 국제 표준화 기구에서 미래 표준 기술 분야로 선행 표준 기술 연구 활동을 적극 추진하여 국제 표준 선점을 위한 국제 표준화 활동을 강화하기 위해 중점표준화 항목으로 선정함
- 마이크로소프트사에서 액티브엑스를 윈도우즈에서 추후에 없앤다고 발표하였고 국내 인터넷에서 액티브엑스의 의존도가 높은 만큼 액티브엑스 위주에서 벗어나 자바 애플릿 기반의 전자상거래 및 보안 모듈을 위한 보안 처리 기술을 연구함으로서 국제적 표준화를 주도할 가능성이 있으므로 중점 표준화 항목으로 선정함

– PC 보안

- 통합 PC 보안이 요구되고 있는 시장 상황에 맞추어 각 업체별로 중복 투자되거나 통합화하는데 장애 요인인 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

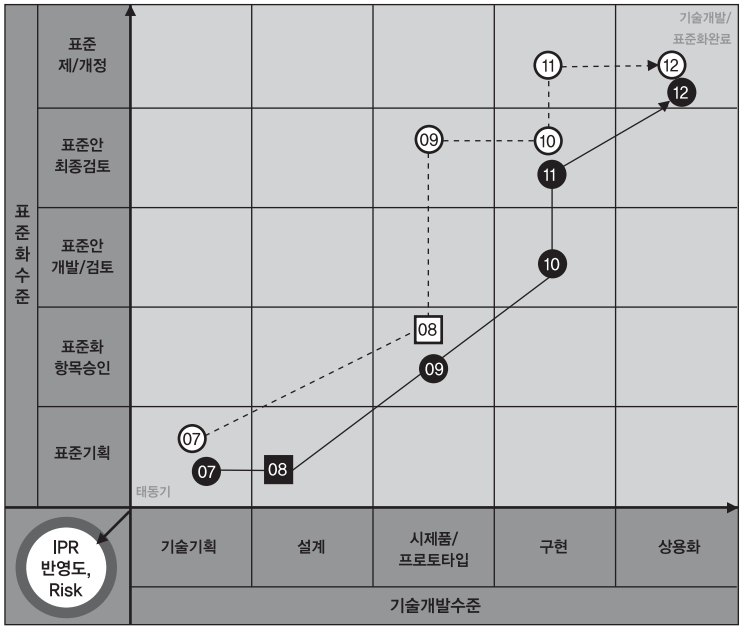
– 디지털포렌식

- 국내 사법 환경에 적합한 디지털포렌식 가이드라인 등의 국내 표준화가 제정됨에 따라, 디지털포렌식을 위한 디지털 데이터 수집도구 요구사항, 디지털 데이터 분석도구 요구사항 및 수집/분석 도구에 대한 검증 규격, 디지털 데이터 교환 포맷 등을 중점표준화 항목으로 선정함

3.3. 중점 표준화항목별 세부전략(안)

3.3.1. USN 보안

○ 표준상태전이도(표준화 & 기술개발 연계분석)

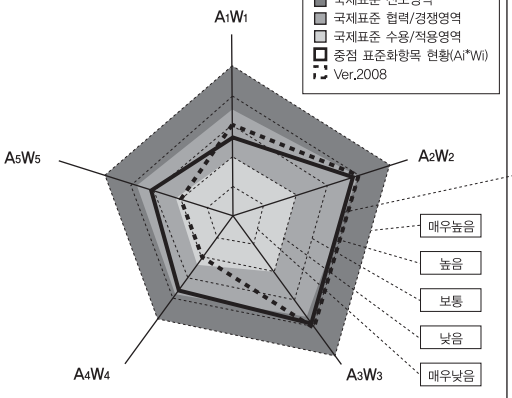


표준화 중요도	국내개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★★★	TTA	ETRI, KISA, 삼성전자	ITU-T, IETF

범례

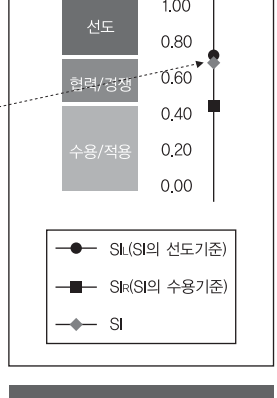
- 08 중점 표준화항목의 국내상태
- 08 중점 표준화항목의 국제상태
- → 중점 표준화항목의 국내 표준상태전이
- -▸ 중점 표준화항목의 국제 표준상태전이
- ↑ 선행표준(선 표준화 후 기술개발)
- ↗ 동시표준(표준화 & 기술개발 동시추진)
- → 후행표준(선 기술개발 후 표준화)

○ 국제표준화 전략목표 도출



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

SI(표준화 전략지수)	
SI_L (SI의 선도기준)	0.73
SI_R (SI의 수용기준)	0.43
SI	0.68



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

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

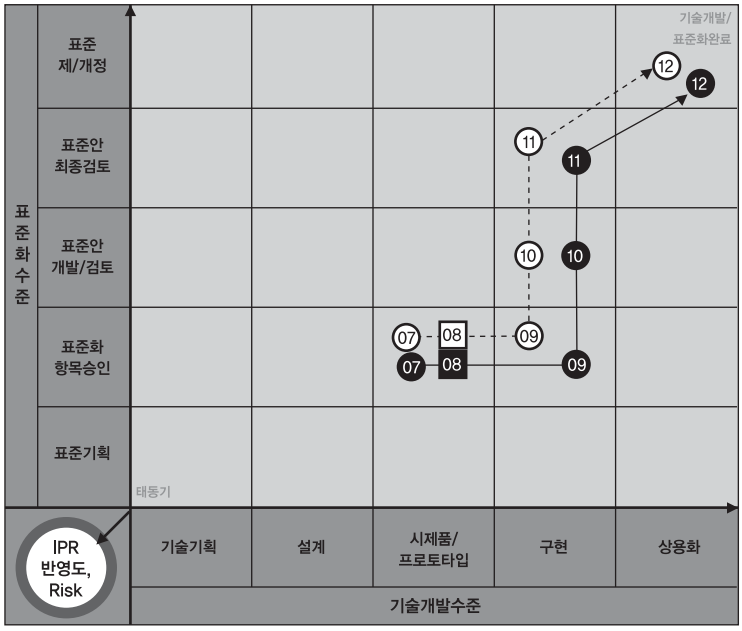
국제표준협력/경쟁(Ver.2008)
↓
국제표준협력/경쟁[선도](Ver.2009)

○ 세부전략(안)

- USN 보안 표준화와 관련하여 표준화 선도 기준 값 0.73에 근접한 0.68이 도출되었으나, 현재 한국이 USN 보안 분야에 대한 표준화를 주도적으로 추진하고 있어, 표준화 선도할 수 있는 전략이 요구됨
- 국외 대비 국내 표준화 수준은 대등한 수준에 있으므로 좀 더 적극적인 지원을 통한 국제 표준 기술 선점에 집중할 필요가 있음
- 또한 IPR 확보 가능성이 매우 높으므로 기업의 표준 활동 참여를 강화할 필요가 있으며 이를 위해 국내 표준 활동 강화에 기업 홍보에 심혈을 기울여야 할 것임
- 국제 표준화 기여 부분이 현재 매우 높게 예상되므로 적극적인 활동이 필요함

3.3.2. 휴대인터넷 보안

○ 표준상태전이도(표준화 & 기술개발 연계분석)

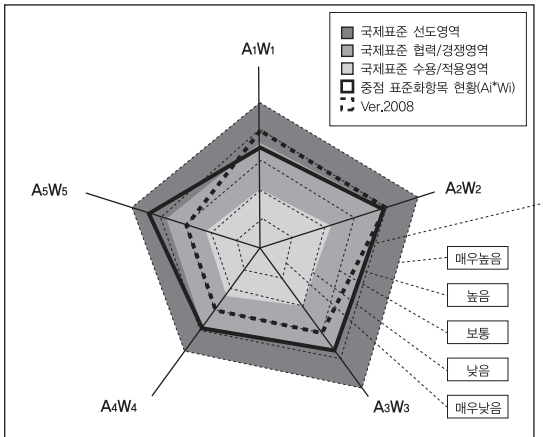


표준화 중요도	국내개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★★★	TTA, 휴대인터넷 포럼	삼성전자, 포스데이타, ETRI 등	IEEE, ITU

범례

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

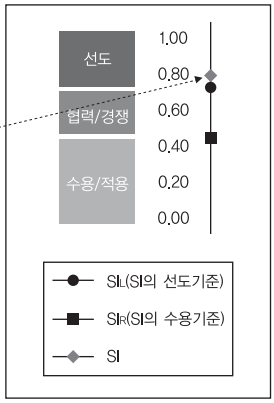
○ 국제표준화 전략목표 도출



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

SI(표준화 전략지수)	
SI_L (SI의 선도기준)	0.73
SI_R (SI의 수용기준)	0.43
SI	0.77

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



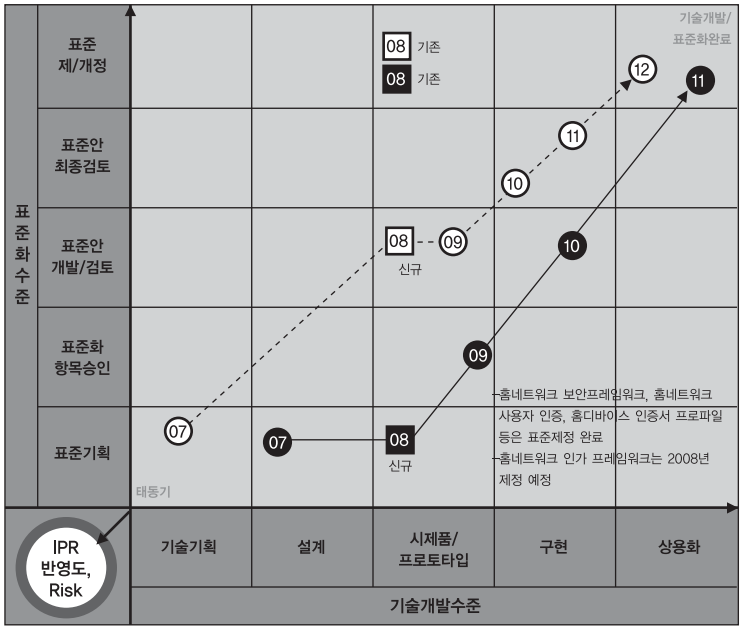
국제표준 선도(Ver.2008)
⬇
국제표준 선도(협력/경쟁)
(Ver.2009)

○ 세부전략(안)

- 3G환경에서의 와이브로 표준을 국제표준으로 채택시키는 등 와이브로 분야는 국외 대비 국내표준화 및 국외대비 국내개발 수준은 선도영역에 위치하고 있으며, 계속적으로 선도적 위치로서 통합네트워크 및 4G환경을 고려한 와이브로 보안 기술의 개발 및 표준화 유도 필요
- 와이브로 기술에 대한 국내 표준화 인프라 수준 및 국제표준화 기여도, IPR 확보의 노력이 협력/경쟁 영역에 미루어 볼 때, 국내 기술개발 수준에 비해 국외 대비 표준 기술 및 IPR확보를 위한 활동을 적극적으로 전개해야 할 것임
- 따라서 IMT-2000환경뿐만 아니라, IMT-Advanced 환경에 적합한 와이브로 보안에 적합한 인증 및 접근제어 기술, 이종 네트워크간의 핸드오버시의 보안기술 등에 관한 표준화 추진노력이 필요

3.3.3. 홈네트워크 보안기술

○ 표준상태전이도(표준화 & 기술개발 연계분석)

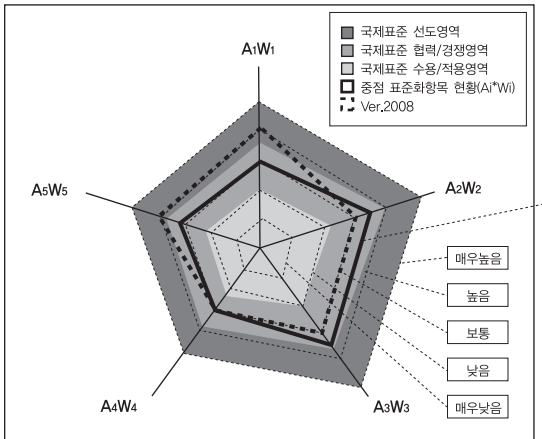


표준화 중요도	국내개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★★★	TTA, HNSF	ETRI, 각 산업체	ITU-T

범례

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

○ 국제표준화 전략목표 도출

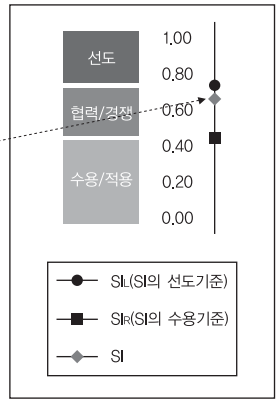


A1 : 국외대비 국내표준화수준
A2 : 국외대비 국내기술개발수준
A3 : IPR확보가능성
점선 : Ver.2008현황
A4 : 국내표준화 인프라수준
A5 : 국제표준화 기여도
Wi : Ai의 가중치

SI(표준화 전략지수)	
SI_L (SI의 선도기준)	0.73
SI_R (SI의 수용기준)	0.43
SI	0.64

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

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



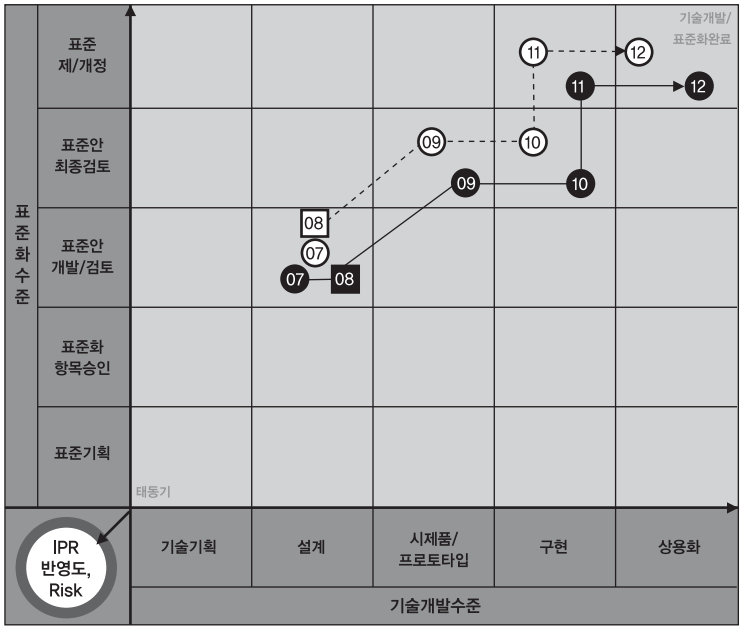
국제표준협력/경쟁(Ver.2008)
⬇
국제표준협력/경쟁[선도] (Ver.2009)

○ 세부전략(안)

- 홈네트워크 보안 분야는 국내 기술개발이 활발히 진행되고 있으며 국제 표준화 기구에서도 많은 활동을 하고 있어, 국내 선도의 가능성이 높은 분야임. 홈네트워크 방범/방재용 영상보안감시시스템과 홈네트워크 IT 보안시스템간의 통합화 추세를 반영, 홈네트워크 융합보안프레임워크에 대한 국제 표준화를 추진하여 국제 표준을 선도할 필요가 있음
- 한국이 ITU-T SG17을 중심으로 국제 표준화를 주도하고 있으므로 관련 제품의 국제경쟁력 강화를 위해서는 계속적인 국내 표준화와 병행 추진이 요구됨
- 다양한 아파트 단지형 홈네트워크 구축 경험을 갖고 있는 국내 산업체의 해외 진출 활성화를 위해 해외 홈네트워크 구축환경을 고려한 요구사항이 표준에 반영될 수 있도록 함
- 해외 업체와의 동등한 기술수준을 갖고 있는 국내 산업체의 적극적인 IPR 확보를 위해 관련 포럼을 중심으로 한 기술교류 및 정보교환이 활성화 될 수 있도록 적극적인 지원이 이루어져야 함
- 국내 표준화 인프라 수준의 강화를 위해 산 · 학 · 연 간 기술교류 및 정보공유가 이루어질 수 있도록 관련 학회 및 포럼에 대한 정책적인 지원이 필요함
- 계속적인 국제표준화 주도를 위해 홈네트워크에서의 보안기술 융합화 추세를 반영한 융합보안프레임워크 표준에 대한 추진이 필요

3.3.4. 이동통신망보안기술

○ 표준상태전이도(표준화 & 기술개발 연계분석)

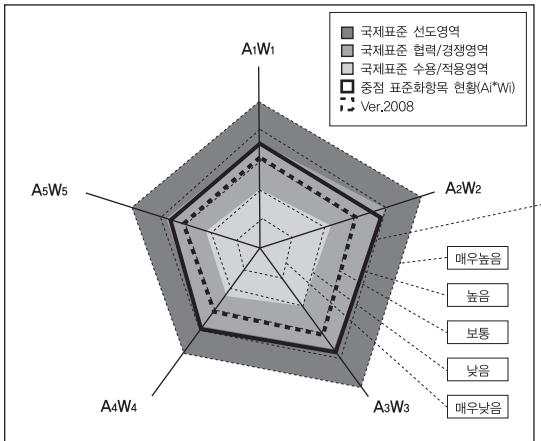


표준화 중요도	국내개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★★	TTA, HNSF	ETRI, 삼성전자, LG전자 등	3GPP, 3GPP2, ITU-T

범례

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

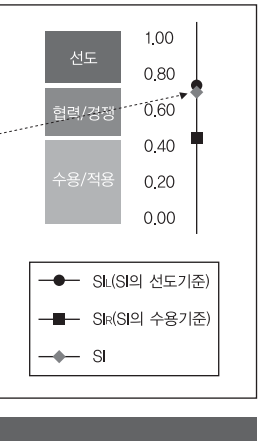
○ 국제표준화 전략목표 도출



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

SI(표준화 전략지수)	
SI_L (SI의 선도기준)	0.73
SI_R (SI의 수용기준)	0.43
SI	0.71

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



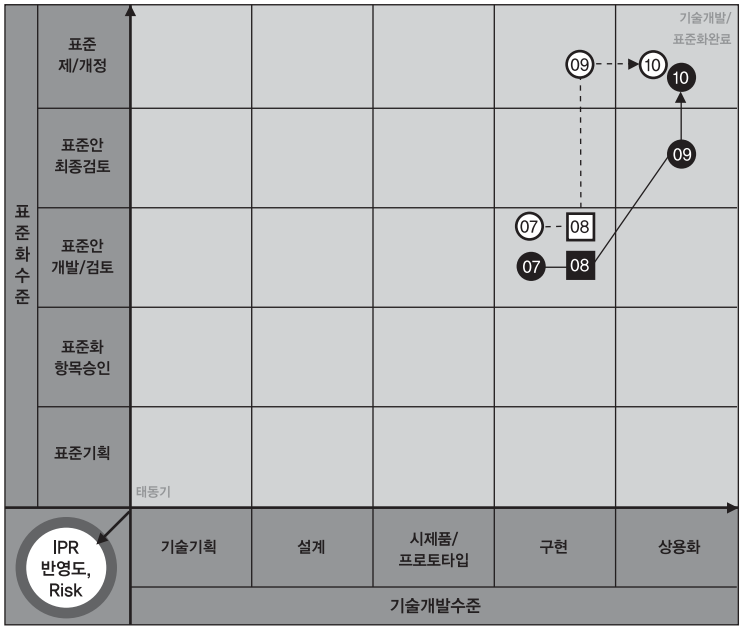
국제표준협력/경쟁(Ver.2008)
⬇
국제표준협력/경쟁(Ver.2009)

○ 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
- 국내외 표준화 현황분석에 따른 전략
  - 차세대 이동통신 분야에 적용할 수 있는 단말의 보안 프레임워크, 신뢰컴퓨팅 등 단말 관련된 기술에 대한 표준화를 중점적으로 추진
- 국내외 기술개발 현황분석에 따른 전략
  - 차세대 이동통신에서 국내 삼성, ETRI 등에서 활발하게 추진하고 있으며, 이동환경을 위한 단말보안기술 위주로 표준 선점이 가능하며, 이를 이용하여 국제 표준으로 연결될 수 있도록 추진

3.3.5. 무선근거리통신망 보안기술

○ 표준상태전이도(표준화 & 기술개발 연계분석)

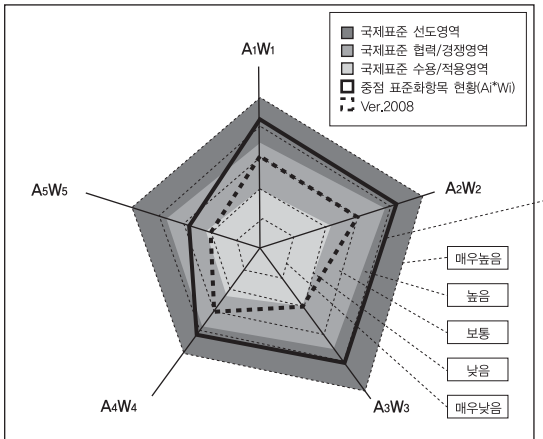


표준화 중요도	국내개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★★★	TTA	ETRI, 각 산업체	IEEE

범례

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

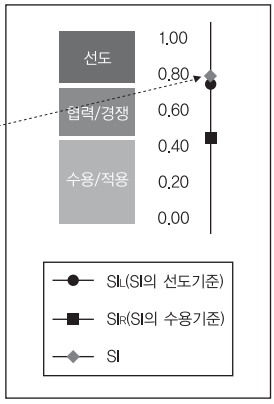
○ 국제표준화 전략목표 도출



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

SI(표준화 전략지수)	
SI_L (SI의 선도기준)	0.73
SI_R (SI의 수용기준)	0.43
SI	0.78

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



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

○ 세부전략

– 국내외 표준화 현황분석에 따른 전략

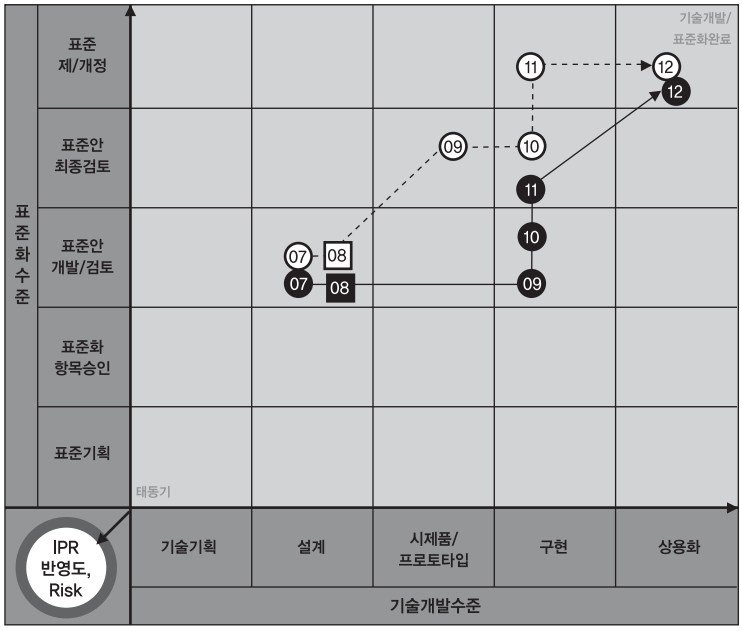
- 무선근거리통신망 보안과 관련하여 프로토콜 수준에서의 보안 기술 표준화 문제가 일단락되면, 네트워크 측면에서 유무선 통합보안 기술에 대한 표준화 예상됨
- 무선랜을 위한 인증 및 접근제어 기술, AP 위장 방지용 인증 기술, 차세대 통합 네트워크에 대한 보안 기술 및 무선랜 보안 프로파일 등에 대한 표준화를 중점적으로 추진함으로써 국제표준과 협력, 경쟁할 필요가 있음
- 국내 표준의 수준이 국외 표준에 미치지 못하고 뒤쫓아 가는 형상이기 때문에 와이브로의 경우와 같이 앞선 기술의 사전 준비를 통한 표준화 과정 추진이 반드시 필요함

– 국외 기술개발 현황분석에 따른 전략

- 무선근거리통신망이 발전 과정에서 휴대인터넷 및 이동통신망의 기술을 참조하는 경향이 나타나고 있기 때문에 관련 기술을 확보한 국내 기업들의 기술 개발 선도 가능성이 높음
- 무선근거리통신망은 향후 통합 네트워크 환경에서 핵심 네트워크로 사용될 가능성이 매우 높기 때문에 관련 기술의 사전 확보가 중요한 과제로 예상됨

3.3.6. 차세대 네트워크 보안

○ 표준상태전이도(표준화 & 기술개발 연계분석)

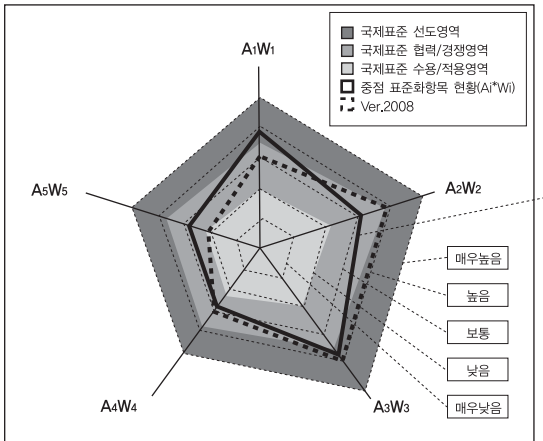


표준화 중요도	국내개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★★★	TTA	ETRI	ITU-T, IETF

범례

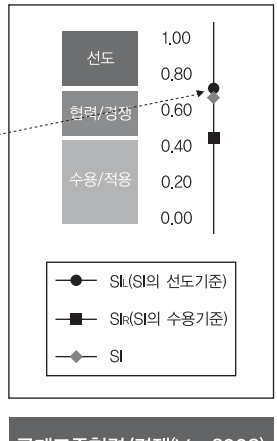
- 08 중점 표준화항목의 국내상태
- 08 중점 표준화항목의 국제상태
- → 중점 표준화항목의 국내 표준상태전이
- -▸ 중점 표준화항목의 국제 표준상태전이
- ↑ 선행표준(선 표준화 후 기술개발)
- ↗ 동시표준(표준화 & 기술개발 동시추진)
- → 후행표준(선 기술개발 후 표준화)

○ 국제표준화 전략목표 도출



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

SI(표준화 전략지수)	
SI_L (SI의 선도기준)	0.73
SI_R (SI의 수용기준)	0.43
SI	0.67



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

국제표준협력/경쟁(Ver.2008)
⬇
국제표준협력/경쟁[선도] (Ver.2009)

○ 세부전략(안)

– 국내외 표준화 현황분석에 따른 전략

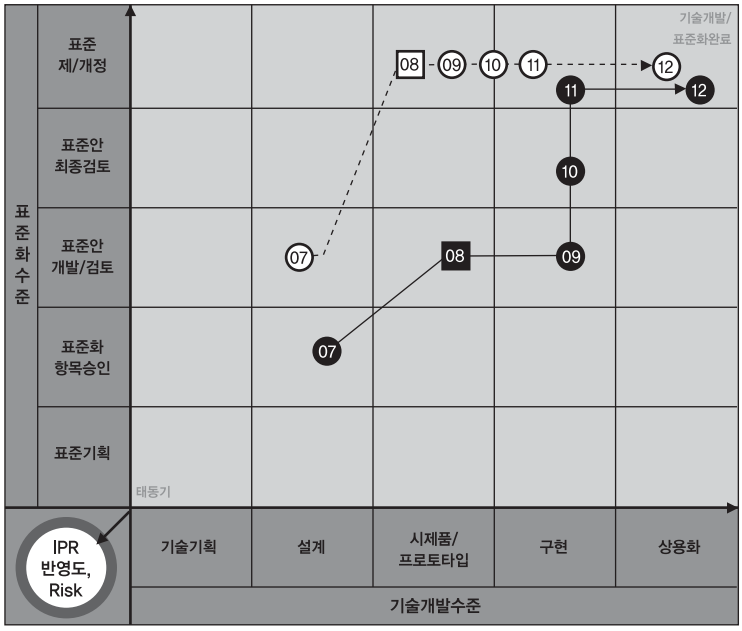
• 차세대 네트워크 분야에 공통으로 적용할 수 있는 보안 프레임워크, 절차 및 보안 요구사항 정의와 관련된 기술에 대한 표준화를 중점적으로 추진

– 국내외 기술개발 현황분석에 따른 전략

• 차세대 휴대 인터넷 서비스 시작이 국내 기술이 세계 선두이므로 유 · 무선 통합 환경에서의 보안 위협과 이에 대한 대응 기술은 표준 선점이 가능하며, 이를 이용하여 국제 표준으로 연결될 수 있도록 추진

3.3.7. 사이버공격 역추적/보안관리

○ 표준상태전이도(표준화 & 기술개발 연계분석)

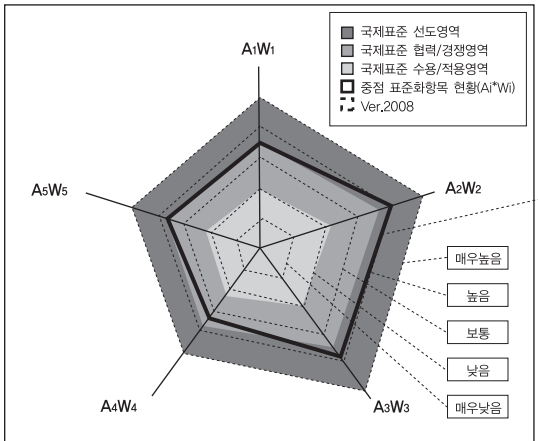


표준화 중요도	국내개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★★★	TTA	ETRI, 이글루시큐리티, 인젠 등	ITU-T, IETF

범례

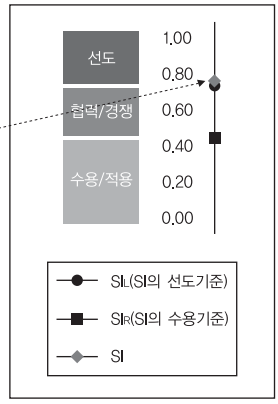
- 08 중점 표준화항목의 국내상태
- 08 중점 표준화항목의 국제상태
- → 중점 표준화항목의 국내 표준상태전이
- -▸ 중점 표준화항목의 국제 표준상태전이
- ↑ 선행표준(선 표준화 후 기술개발)
- ↗ 동시표준(표준화 & 기술개발 동시추진)
- → 후행표준(선 기술개발 후 표준화)

○ 국제표준화 전략목표 도출



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

SI(표준화 전략지수)	
SI_L (SI의 선도기준)	0.73
SI_R (SI의 수용기준)	0.43
SI	0.75



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

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

국제표준 선도(Ver.2009)

○ 세부전략(안)

– 국외대비 국내표준화 현황분석에 따른 전략

• 사이버 공격 감시 및 추적기술은 국내 각 정부 및 민간 기관별 침해대응센터의 고도화에 해당되는 것으로서 상호호환성이 절대적으로 필요하며, 국내에서는 추적 메시지에 대한 표준 교환 포맷을 TTA에서 정의하였으며, 향후에 제시될 다양한 방향에 대한 기술 검증과 더불어 실용적인 추적 메시지 교환 전달프로토콜과 추적 메시지 교환 시 안전성 제공을 위한 보안 프로파일에 대한 체계적인 국내 고유 표준 개발을 추진

– 국내표준화 인프라 현황분석에 따른 전략

• 약간의 표준 인프라(인력 및 정책 등)만 있어도 충분히 선도가능하며, 현재의 표준 대상의 기술에 대한 검증을 통해 국내표준 시도 추진

– 국외대비 국내개발수준 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 기술과의 격차가 크지 않아 지속적인 기술의 완성도에 대한 검증을 역점에 두면서 표준을 적극 추진

– 국제표준화 기여도 현황분석에 따른 전략

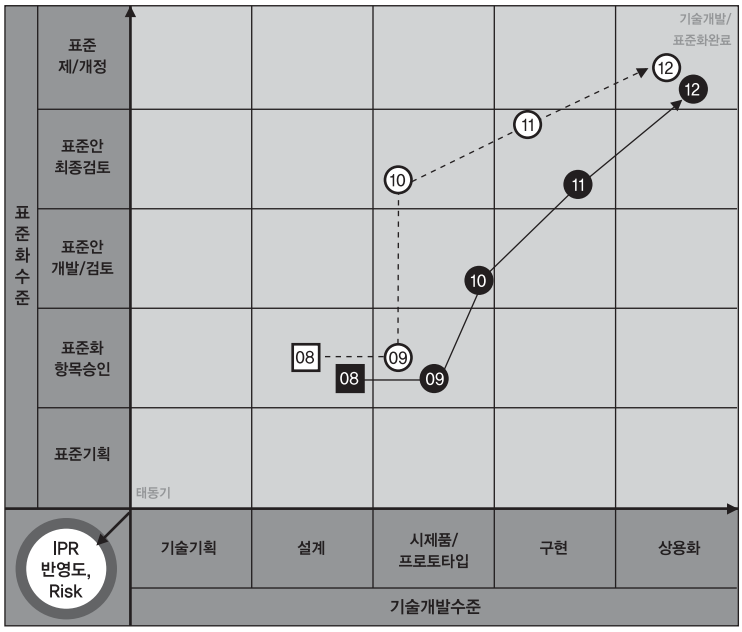
• 사이버공격 역추적 분야는 국제 기여도가 매우 높은 상태인 관계이며, 따라서 실용적인 기술 검증과 함께 현재 미흡한 국제표준을 선도하는 상황에 역점을 두어 관련 국제 표준을 선도

– IPR 확보 가능성 현황분석에 따른 전략

• 사이버공격 역추적 분야는 국제 기여도가 매우 높으며, 또한 IPR 확보 가능성이 높아야 국제표준 선도 가능성이 높은 관계로, 추적 메시지 교환 전달프로토콜과 추적 메시지 교환 시 안전성 제공을 위한 보안 프로파일 등에 대한 국내외 IPR 확보를 적극적 확보 시도

3.3.8. 봇넷 대응 기술

○ 표준상태전이도(표준화 & 기술개발 연계분석)

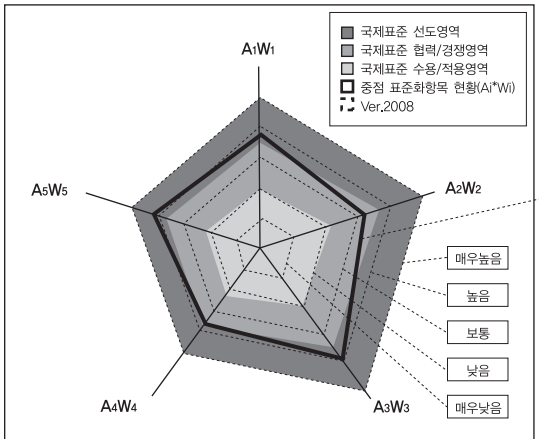


표준화 중요도	국내개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★★★	TTA	ETRI, KISA, 각 산업체	ITU-T

범례

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

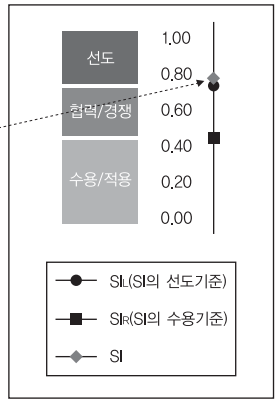
○ 국제표준화 전략목표 도출



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

SI(표준화 전략지수)	
SI_L (SI의 선도기준)	0.73
SI_R (SI의 수용기준)	0.43
SI	0.76

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



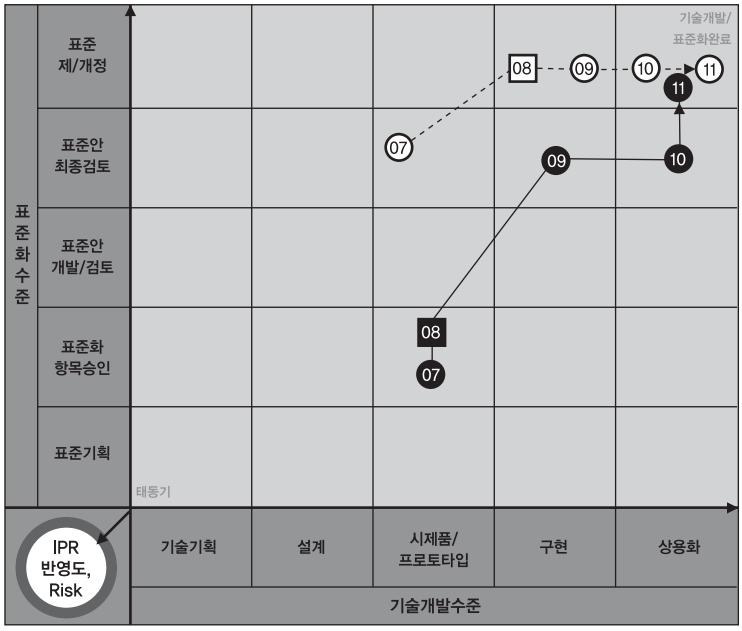
국제표준 선도(Ver.2009)

○ 세부전략(안)

- 체계적인 봇넷 탐지 및 대응을 위해 전반적인 프레임워크에 대한 국내 표준화가 필요
  - 국내 표준의 경우 2008년 TTA를 통해 봇넷 탐지 및 대응 프레임워크에 대한 표준 제안이 이루어졌으며, 신규 표준 항목으로 채택되어 표준 문서 개발이 진행 중임
  - 향후 프레임워크를 기반으로 동작하는 봇넷 탐지 및 대응 체계 운영 가이드라인과 봇넷 탐지 및 대응 프레임워크에 적용되는 상세 스키마 및 프로토콜 등에 대한 표준안이 개발되어야 함
- 봇넷 탐지 및 대응을 위해서 국제적인 협력이 요구되며, 이를 위해 국제 표준화가 필요
  - ITU-T SG17에서 봇넷 탐지 및 대응 프레임워크에 대한 표준 항목을 제안해 채택된 상태이며, 국내 주도하에 표준 문서 개발 중
  - 효율적이고 높은 상호 운용성을 제공하기 위해서 다른 나라 유관기관과의 협력이 필요함

3.3.9. 서버 보안

○ 표준상태전이도(표준화 & 기술개발 연계분석)

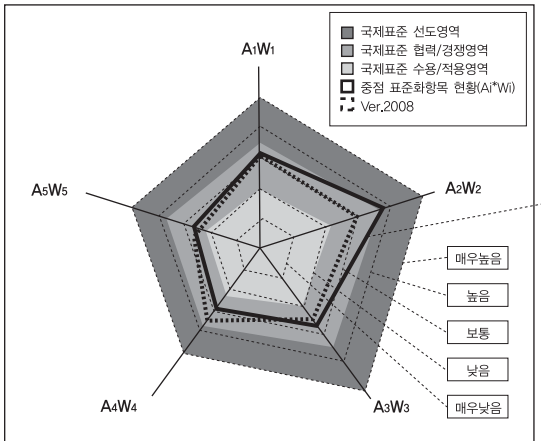


표준화 중요도	국내개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★★	TTA	ETRI, 보안서버 개발업체	ITU-T, ISO, TCPA

범례

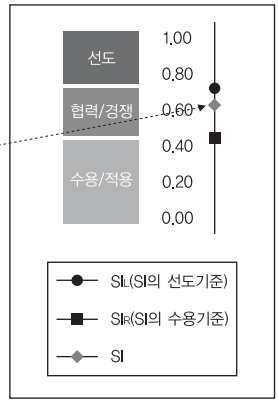
- 08 중점 표준화항목의 국내상태
- 08 중점 표준화항목의 국제상태
- → 중점 표준화항목의 국내 표준상태전이
- -▸ 중점 표준화항목의 국제 표준상태전이
- ↑ 선행표준(선 표준화 후 기술개발)
- ↗ 동시표준(표준화 & 기술개발 동시추진)
- → 후행표준(선 기술개발 후 표준화)

○ 국제표준화 전략목표 도출



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

SI(표준화 전략지수)	
SI_L (SI의 선도기준)	0.73
SI_R (SI의 수용기준)	0.43
SI	0.62



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

국제표준협력/경쟁(Ver.2008)
⬇
국제표준협력/경쟁(Ver.2009)

– 국제 표준에 대한 협력 경쟁관계 유지

- 2008년에 비하여 국내 기술개발 수준은 향상되었고 IPR 확보 가능성도 증가한 것으로 분석됨
- 국내 표준화 인프라는 국제 표준을 선도하기에는 낮은 수준으로 국제 표준에 대한 협력 경쟁관계를 유지하기 위해 서버 보안 분야에서 우리가 선도적인 기술을 보유하고 있는 웹서버 보안, 전자성거래 기술, 보안 커널에 대한 접근통제 부분에서 차별화된 특허 가능한 기술 개발을 추진함

○ 세부전략(안)

– 표준화 추진

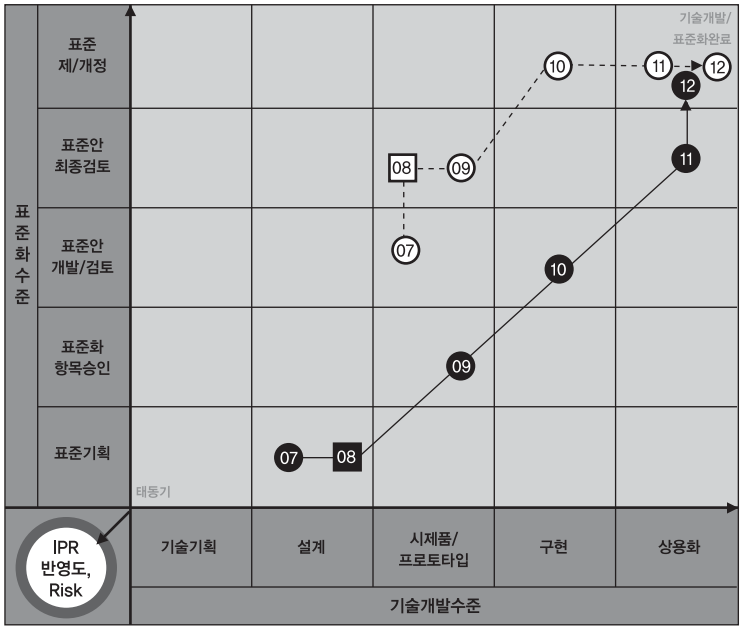
- 웹서버 보안 기술, 트러스트 플랫폼 기반 소프트웨어 무결성 검증 기술, 접근통제 및 감사추적 기술, 그리고 플랫폼 임의조장 방지 기술 등은 TCG의 트러스트 플랫폼 환경에서 플랫폼 임의 조작 및 침해확산을 방지하는 트러스트 플랫폼 및 네트워크의 신뢰성을 제공하는 TNC(Trusted Network Connection) 규격을 수용하고, 2009년 구현 기술에 대한 국내 고유 표준 개발을 추진함
- 트러스트 플랫폼에 대한 기술은 국외에서 표준화되어 앞서가는 기술이므로 트러스트 플랫폼 환경에서 감사추적, 웹서버 보안, 전자상거래 기술, 보안 커널 제어 등의 기술을 접목하는 분야에서 국제 표준화 활동을 수행함
- 트러스트 플랫폼에 대한 운영체제 기술은 ISO 표준 규격을 바탕으로 트러스트 플랫폼용 보안 운영체제 국제 표준을 추진함으로 협력 경쟁 관계를 유지함

– IPR 확보 방안

- 침해 확산 방지형 도메인 분리 기술은 새로운 개념의 분리 커널 표준화 분야로, CC를 기반으로 ISO에서 국제 표준화 및 IPR 확보를 추진함
- 국내에서 액티브엑스 기술이 전 세계적으로 발전한 만큼 이 기술을 자바 애플릿으로 적용하여 애플릿 기반 전자 상거래 및 보안 모듈을 연구함으로써 국제 표준화와 IPR 확보를 추진함

3.3.10. PC 보안

○ 표준상태전이도(표준화 & 기술개발 연계분석)

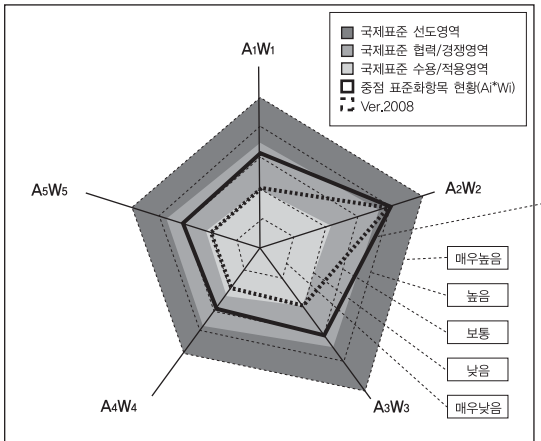


표준화 중요도	국내개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★	TTA, ISTF	ETRI, 각 산업체	ITU-T, IETF

범례

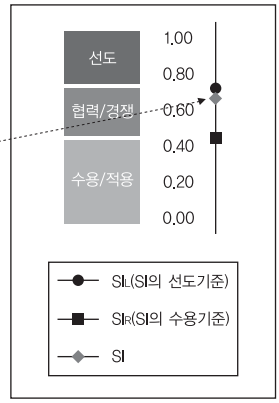
- 08 중점 표준화항목의 국내상태
- 08 중점 표준화항목의 국제상태
- → 중점 표준화항목의 국내 표준상태전이
- -▸ 중점 표준화항목의 국제 표준상태전이
- ↑ 선행표준(선 표준화 후 기술개발)
- ↗ 동시표준(표준화 & 기술개발 동시추진)
- → 후행표준(선 기술개발 후 표준화)

○ 국제표준화 전략목표 도출



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

SI(표준화 전략지수)	
SI_L (SI의 선도기준)	0.73
SI_R (SI의 수용기준)	0.43
SI	0.65



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

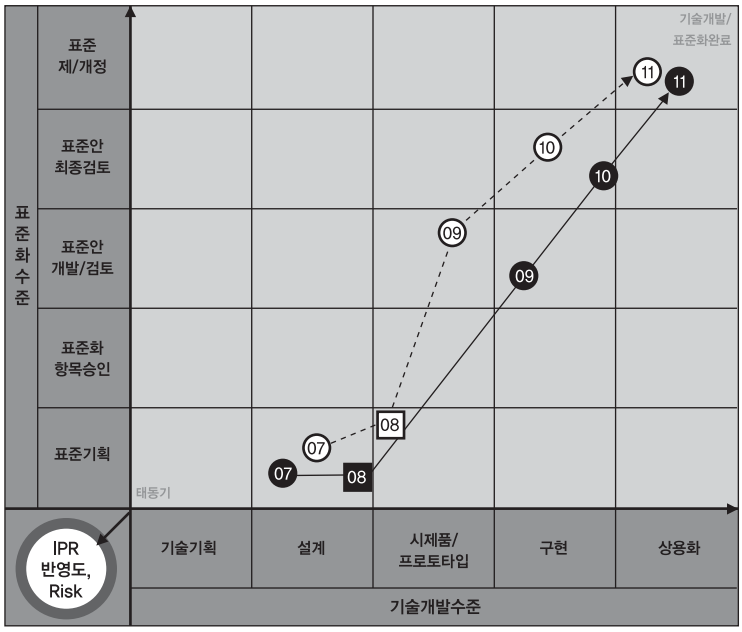
국제표준협력/경쟁(Ver.2008)
⬇
국제표준협력/경쟁(Ver.2009)

○ 세부전략(안)

- 안티바이러스 분야에서는 글로벌하게 표준화하여 아직 독점을 하거나 사업을 주도하는 부분이 적으므로 표준화 동향의 주시가 필요
- 다만, 통합관리 요구를 수용하기 위해 국내에서 PC 보안 로그 형식 표준화를 추진이 요구됨
- 또한, 각 안티바이러스 업체들이 테스팅에 대한 표준화 논의가 되고 있기 때문에 글로벌 테스팅 표준화에 국내 업체도 참여하여 그 움직임에 따라 기술 개발과 대응책을 마련해야 함

3.3.11. 디지털포렌식

○ 표준상태전이도(표준화 & 기술개발 연계분석)

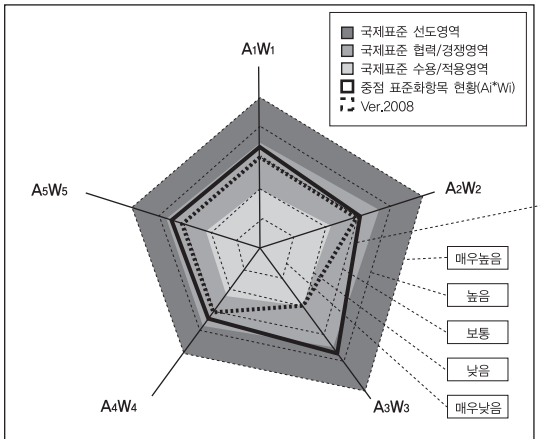


표준화 중요도	국내개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★★	ETRI, TTA	ETRI	ITU-T, ISO/IEC

범례

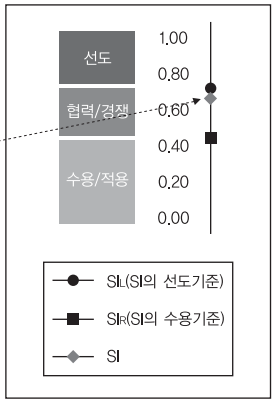
- 08 중점 표준화항목의 국내상태
- 08 중점 표준화항목의 국제상태
- → 중점 표준화항목의 국내 표준상태전이
- -▸ 중점 표준화항목의 국제 표준상태전이
- ↑ 선행표준(선 표준화 후 기술개발)
- ↗ 동시표준(표준화 & 기술개발 동시추진)
- → 후행표준(선 기술개발 후 표준화)

○ 국제표준화 전략목표 도출



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

SI(표준화 전략지수)	
SI_L (SI의 선도기준)	0.73
SI_R (SI의 수용기준)	0.43
SI	0.68



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

국제표준협력/경쟁[선도] (Ver.2009)

○ 세부전략(안)

– 국내 사법 환경에 적합한 절차 가이드라인 및 수집, 분석 도구 검증 규격 등의 국내 표준화가 필요

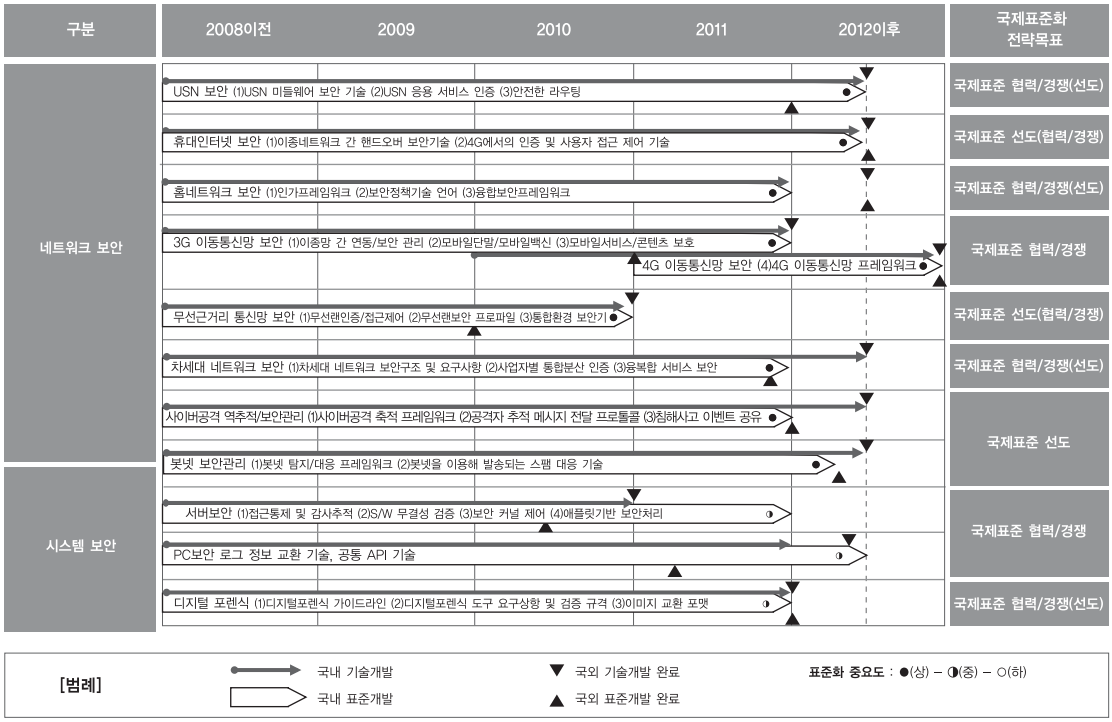
- 국내 표준의 경우 2007년 TTA를 통해 컴퓨터 및 휴대폰 포렌식 가이드라인과 컴퓨터 포렌식을 위한 디지털 데이터 수집도구 요구사항 표준안이 작성되었음
- 향후 디지털 데이터 분석도구 요구사항 및 수집/분석 도구에 대한 검증 규격, 데이터 교환 포맷 등의 표준안이 개발되어야 함

– 아직 주도적인 국제 표준화 기구가 결성되지 않았으므로, 표준항목을 개발하여 ITU-T 등을 통한 국제 표준화 선도가 가능함

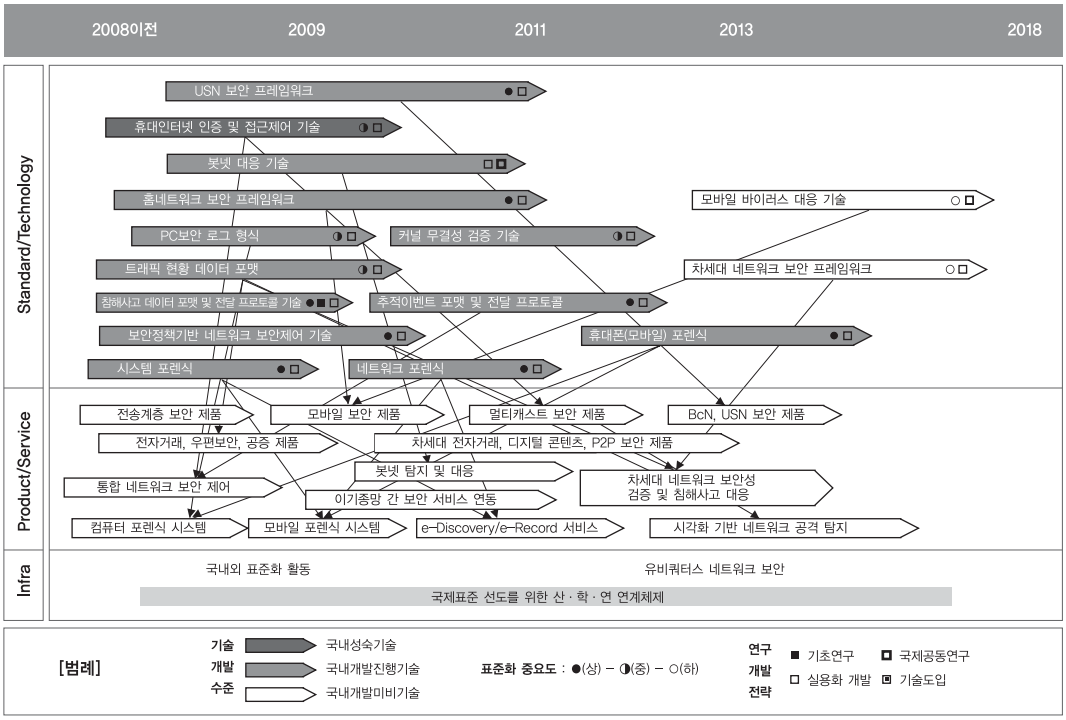
- ITU-T SG17에서 2009년부터 시작되는 신규 회기에 사이버 범죄 추적 관련 표준 작업 그룹에 포렌식 관련 표준항목을 준비하여, 주도적인 표준안 제안을 통해 국제 표준을 선도해 나가는 것이 필요함
- ITU-T가 중점적으로 추진할 것으로 예상되는 네트워크 및 모바일 포렌식 분야의 국제 표준을 선도 개발함

3.4. 중장기 표준화로드맵

3.4.1. 중기('09~'11) 표준화로드맵



3.4.2. 장기 표준화 로드맵(10년 기술예측)



[국내외 관련 표준 대응리스트]

구분	표준화 항목	표준명	기구(업체)	제정 연도	재개정 현황	국내 관련표준	국내 추진기구
네트워크 보안	USN 보안 기술	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		
	휴대인터넷 보안기술	IEEE Std 802.16e-2005	IEEE	2005	제정	2.3 GHz 휴대인터넷 상호인증 메커니즘	TTA
						2.3 GHz 휴대인터넷 표준 (물리계층 및 매체접근제어계층)	
						2.3 GHz 휴대인터넷 서비스 및 네트워크 요구사항	
	무선근거리 통신망 보안기술	IEEE 802.11	IEEE	1997	O	X	TTA
		IEEE 802.11-1999		1999	O	X	
		IEEE 802.11-2007		2007	X	X	
		IEEE 802.11i-2004		2004	X	X	
		IEEE 802.11r		Draft	X	X	X
		IEEE 802.11w		Draft	X	X	X
	차세대 네트워크 보안기술	Next Generation Networks? Security	ITU-T SG13	2007	제정		
		NGN Authentication and Authorization Requirements		2008	제정		
		EAP-based security signalling protocol architecture for network attachment	ITU-T SG17	2007	제정		
		Authentication Protocols based on EAP-AKA for Interworking among 3GPP, WiMax, and WLAN in NGN		2008	제정		
	사이버공격 역추적 및 보안관리	IPsec-NAT Compatibility Requirements(RFC 3715)	IETF	2004	초안		TTA/ISTF
		A Traffic-Based Method of Detecting Dead IKE Peers(RFC 3706)		2004	초안		
		Using AES Counter Mode With IPsec ESP(RFC 3686)		2004	초안		
		The AES-XCBC-PRF-128 algorithm for IKE(RFC 3664)		2004	초안		
		The AES-CBC Cipher Algorithm and Its Use with IPsec(RFC 3602)		2003	초안		
		IP Security Policy Requirements(RFC 3586)		2003	초안		
		IPsec Configuration Policy Information Model(RFC 3585)		2003	초안		
		The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec(RFC 3566)		2003	초안		

구분	표준화 항목	표준명	기구(업체)	제정 연도	재개정 현황	국내 관련표준	국내 추진기구
네트워크 보안	사이버공격 역추적 및 보안관리	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)		2003	초안		
		The Use of HMAC-RIPEMD-160-96 within ESP and AH(RFC 2857)		2000	초안		
		RFC 2451 The ESP CBC-Mode Cipher Algorithms		1998	초안		
		RFC 2410 The NULL Encryption Algorithm and Its Use With IPsec		1998	초안		
		RFC 2409 The Internet Key Exchange(IKE)		1998	초안	ISTF-003	
		RFC 2408 Internet Security Association and Key Management Protocol(ISAKMP)		1998	초안	ISTF-003	
		RFC 2407 The Internet IP Security Domain of Interpretation for ISAKMP		1998	초안	ISTF-003	
		RFC 2406 IP Encapsulating Security Payload(ESP)		1998	초안	TTAS.KO-12.0014	
		RFC 2405 The ESP DES-CBC Cipher Algorithm With Explicit IV		1998	초안		
		RFC 2404 The Use of HMAC-SHA-1-96 within ESP and AH		1998	초안		
		RFC 2403 The Use of HMAC-MD5-96 within ESP and AH	IETF	1998	초안		TTA/ISTF
		RFC 2402 IP Authentication Header		1998	초안	TTAS.KO-12.0014	
		RFC 2401 Security Architecture for the Internet Protocol		1998	초안	ISTF-003, TTAS.KO-12.0014	
		RFC 2085 HMAC-MD5 IP Authentication with Replay Prevention		1997	초안		
		RFC 1825 Security Architecture for the Internet Protocol		1995	초안	TTAS.KO-12.0014	
		RFC 1826 IP Authentication Header		1995	초안		
		RFC 1827 IP Encapsulating Security Payload(ESP)		1995	초안	TTAS.KO-12.0014	
		RFC 1828 IP Authentication using Keyed MD5		1995	초안		
		RFC 1829 The ESP DES-CBC Transform		1995	초안		
		The TUNNEL Profile		2003	초안		
		The Incident Object Description Exchange Format		2008	초안		
		The Intrusion Detection Exchange Protocol(IDXP)		진행 중	-		
		RFC 3749 Transport Layer Security Protocol Compression Methods		2004	초안		
		RFC 3546 Transport Layer Security(TLS) Extensions		2003	초안		
		RFC 3268 AES Ciphersuites for TLS		2002	초안		
		RFC 2818 HTTP Over TLS		2000	초안		
		RFC 2817 Upgrading to TLS Within HTTP/1.1		2000	초안		
		RFC 2712 Addition of Kerberos Cipher Suites to Transport Layer Security(TLS)		1999	초안		
		RFC 2246 The TLS Protocol Version 1.0		1999	초안		
		Incident Handling: Real-time inter- network Defense		진행 중	-	TTAS.KO-12.0060	
		네트워크 보안 정책의 생성, 저장, 분배 및 실행을 위한 프레임워크	ITU-T	2007	제정	TTAE.IT-X.1036	TTA
		사이버공격 추적 이벤트 교환 포맷	-	2007	제정	TTAS.KO-12.0060	

구분	표준화 항목	표준명	기구(업체)	제정 연도	재개정 현황	국내 관련표준	국내 추진기구
네트워크 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)"		2003	제정		
		Information Technology – Portable Operating System Interface(POSIX)	ISO/IEC	2003	제정		
		System Administration – Part 2: Software Administration First Edition; ANSI/IEEE Std 1387.2					
		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		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		
		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		
		Portable operating system interface(POSIX) part 2: shell and utilities		2005	제정	POSIX–PART 2: 쉘과 유틸리티 표준 – ISO/IEC 9945–2	TTA
		A Standard for portable operating system interface(POSIX)		2005	제정	개방형 운영체제 인터페이스(POSIX.1) 표준	
		Portable operating system interface(POSIX) part 1 system application programming interface(API) [C language]		2005	제정	POSIX–PART 1: C 언어를 위한 시스템 응용 프로그래밍 인터페이스(API) 표준 – ISO/IEC 9945–1	
		Sensor Operating System API Framework for USN		2005	제정	USN용 센서 운영체제 API 프레임워크	

[참고문헌]

[1] http://www.cftt.nist.gov.

[2] http://www.nsrl.nist.gov.

[3] http://www.trustedcomputinggroup.org/, Trusted Computing Group(TCG) Main Specification Version 1.1b.

[4] 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.

[5] A. Belenky, N. Ansari, On IP Traceback IEEE Communication Magazine, vol. 41, pp. 142 – 153, July 2003.

[6] 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.

[7] Arkoudi-Vafea Aikaterini, Security of IEEE 802.16.

[8] BcN 포럼, http://www.bcnforum.or.kr.

[9] BcN 포럼, BcN 표준모델 v2.0, 2006.

[10] BcN 포럼, 광대역통합망(BcN) 기술 워크숍, 2004.

[11] Common Criteria, http://www.commoncriteriaportal.org/thecc.html.

[12] Common Criteria for Information Technology Security Evaluation(aligned with ISO/IEC International Standard(IS) 15408), Version 2.1, August 1999, http://www.radium.ncsc.mil/tpep/library/ccitse/, http://csrc.nist.gov/cc/ccv20/ccv2list.htm#CCV21.

[13] Common Criteria Part: Security functional requirements, Aug 1999, Ver.2.1.

[14] 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, Mar. 2000.

[15] David Johnston, Jesse Walker, Overview of IEEE 802.16 Security, THE IEEE Computer Society, 2004.

[16] Don Cohen and K. Narayanaswamy, Survey/Analysis of Levels I, II, and III Attack Attribution Techniques, Cs3, Inc., Apr. 2004.

[17] ETSI, http://www.etsi.org.

[18] 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.

[19] Gartner Dataquest, Worldwide Switching Market Share and Forecast, 2003

[20] 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

[21] IDC Korea, IDC Market Analysis: Korea Security Software 2008-2012.

[22] IDC, Worldwide Standalone VOIP Gateways Forecast and Analysis, 2002.

[23] IEEE 802.11b Wireless LAN Medium Access Control(MAC) and Physical Layer(PHY) Specification, IEEE Standard 802.11b, 1999.

[24] IEEE P1520, http://www.ieee-pin.org.

[25] IETF, http://www.ietf.org.

[26] IITA, 정보보호 기술로드맵(ITRM 2012), 2007.

[27] Igor Faynberg, etc. Converged Networks and Services, John Wiley & Sons Inc., 2000.

[28] IST, http://www.cordis.lu/ist/.

[29] ITU-T, http://www.itu.int/ITU-T/.

[30] ITU-T FGNGN Ouput Documents, http://ties.itu.int/fgngn/fgngn.

[31] Korean Intellectual Property Office(KIPO), http://www.kipo.go.kr/.

[32] L. Blunk, J. Vloobrecht, PPP Extensible Authentication Protocol(EAP), IETF RFC2284, 1998. 3.

[33] Micah Adler, Tradeoffs in probabilistic packet marking for IP traceback, STOC 2002, pp. 407-418.

[34] Ovum, Market Strategies for Telcos and ISPs, 2000.

[35] Port-based Network Access Control, IEEE Standard 802.1x, 2001.

[36] Protection Profile for Multilevel Operation Systems in Environments Requiring Medium Robustness, version 1.22, NSA, May 2001.

[37] Protection Profile for Singlelevel Operation Systems in Environments Requiring Medium Robustness, version 1.22, NSA, May 2001.

[38] R&D 특허센터, http://www.ipr-guide.org/.

[39] 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.

[40] Sen Xu Manton Matthews Chin-Tser Huang, Security Issues in Privacy and Key Management Protocols of IEEE 802.16, ACM SE'06, 2006, Melbourne, Florida, USA.

[41] 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.

[42] TCG Software Stack(TSS) Specification Version 1.0.
[43] Tom Katygiannis, Les Owens, Draft Wireless Network Security, National Institute and Technology(NIST), 2002.
[44] Trusted Computing Group(TCG) Design Philosophies and Concepts Version 1.0
[45] Trusted Computing Group(TCG) Main Specification Version 1.1b, http://www.trustedcomputinggroup.org/, Feb. 2002(also known as Trusted Computing Platform Alliance(TCPA) Main Specification Version 1.1b).
[46] World Intellectual Property Organization(WIPO), http://www.wipo.int/.
[47] 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.
[48] 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.
[49] NIA, 2005 국가정보화 백서, 2005.
[50] ETRI, 유비쿼터스 서비스를 위한 BcN 기술 워크숍, 2004.
[51] KISA, 2007년 국내 정보보호산업 시장 및 동향 조사, 2008.
[52] KISA, 무선랜 안전운영가이드, 2004.
[53] KISA, IPv6 보안기술해설서, 2005.
[54] TTA, TTA 정보보호 표준화 로드맵, 2006.
[55] TTA, 정보통신 중점기술 표준화로드맵 종합보고서,(Ver. 2005).
[56] (주)KRG, 국내 무선보안 동향 보고서, 전자정보센터(EIC), 2004.
[57] 강유성, 사용자 중심의 무선랜 이동보안 기술 표준화 논의 본격화, TTA, IT Standard Weekly 2005-04호, 2005.
[58] 김상훈, 무선랜 칩셋 동향, 전자정보센터(EIC), 2005.
[59] 박용우, 무선랜 장비시장 현황 및 국내시장에의 시사점, 정보통신정책 제16권 5호 통권 343호, 2004.
[60] 밸류애드, 무선랜카드(WLAN) 시장 동향, 전자정보센터(EIC), 2007.
[61] 이석규, 무선랜 표준화: IEEE802.11의 워킹그룹이 주도적 역할: 글로벌시대의 키워드 'IT표준화, 2004.
[62] 임선희, 이옥연, 전성익, 한진희, EAP-AKA를 적용한 WiBro 무선네트워크의 인증구조 연구, 한국통신학회 논문지, 2006.
[63] 정병호, 무선랜 보안 기술 표준화 동향, TTA, 2003.
[64] 정보통신부, Dynamic u-Korea 건설을 위한 광대역 통합망(BcN) 구축 기본 계획 II, 2006.
[65] 정보통신부, 광대역통합망 구축 기본계획, 2004.

[66] 정찬형, 유비쿼터스 환경을 위한 무선 메쉬 네트워크 기술 동향, 한국정보산업연합회(FKII), IT Issue 2004.
[67] 지경용, 강충구, 조용수, 휴대인터넷의 이해, 2006.
[68] 지경용, 김문구, 오동섭, 무선랜 서비스 이용 현황 및 시장 확대 방향, 2005.

[약어]

3GPP	3rd Generation Partnership Project
AAA	Authentication, Authorization and Accounting
AP	Access Point
BA	Block Acknowledgement
BcN	Broadband Convergence Network
DLS	Direct Link Setup
HCCA	HCF Controlled Access
CC	Common Criteria
CFB	Cipher Feedback)
CFTT	Computer Forensic Tool Testing
CDMA	Code Division Multiple Access
DBMS	Database Management System
DoD	Department of Defense
DRM	Digital Rights Management
Dual-band DSSS	Dual-band Direct Sequence Spread Spectrum
EDCA	European Network of Forensic Science Institutes
ENFSI	European Network of Forensic Science Institutes
ESI	Electronically Stored Information
ESM	Enterprise Security Management
FMC	Fixed Mobile Convergence
FTTH	Fiber To The Home
GSM	Global System for Mobile communications
HNSF	Home Network Security Forum
HSDPA	High Speed Downlink Packet Access
HSS	Home Subscriber Services
IDS	Intrusion Detection Service
IMS	IP Multimedia Subsystem
IPR	Intellectual Property Rights
IPS	Intrusion Prevention System
LTE	Long Term Evolution

LTE/SAE	Long Term Evolution/Service Architecture Evolution
MVNO	Mobile virtual network operator
NFI	Netherlands Forensic Institute
NIST	National Institute of Standards and Technology
NSRL	National Software Reference Library
NGN	Next Generation Network
OFDM	Orthogonal Frequency Division Multiplexing
OFDMA	Orthogonal frequency division multiple access
PMS	Patch Management System
PS	Policy Store
PSIM	Professional Services Information Management
RAS	Remote Access Server
RDS	Reference Data Set
RFID	Radio Frequency Identification
RID	Real-time Inter-network Defense
RTLS	Real-Time Locating Service(System)
QDMA	Quadrature Division Multiple Access
QoS	Quality of Service
SMB	Small & Medium Business
TMS	Threat Management System
UMTS	Universal Mobile Telecommunication System
USIM	Universal Subscriber Identity Module
UTM	Unified Threat Management
VoIP	Voice over IP
VPN	virtual private network
WCDMA	Wideband Code Division Multiple Access
WiBro	Wireless Broadband
WIPI	Wireless Internet Platform for Interoperability
WLAN	Wireless Local Area Network
WPA	Wi-Fi protected access
WPA2	Wi-Fi protected access 2