

IT839전략과 정보보호

홍도원*, 염용진**, 정교일*, 지성택**

요약

IT839란 새로운 정보통신 서비스를 도입하여 첨단 인프라의 구축을 앞당기고 이를 바탕으로 IT분야의 성장 동력을 이끌어내려는 것으로 정보통신부를 중심으로 추진되는 전략이다. IT839전략은 IT신기술이 국가사회진전에 적용될 수 있도록 하여 지식기반사회보다 한층 고도화된 u-Korea라는 지능기반사회를 구축하기 위한 밑거름이기도 하다. IT839의 성공적인 추진을 위해서는 정보보호 핵심기술의 개발과 제공이 필수적이며 특히 새로운 정보통신 서비스에 대한 정보보호 대책이 적시에 제공되어야 한다.

본고에서는 IT839전략에 필요한 정보보호 관련 요소들을 점검하고 정보보호 핵심기술 개발의 중요성을 강조하고자 한다.

1. 서론

이제 '유비쿼터스'라는 용어는 더 이상 생소하게 느껴지지 않을 만큼 자주 등장하고 있다. 언제 어디에나 존재한다는 개념의 유비쿼터스(ubiquitous)는 컴퓨터의 발전으로 모든 사물이 컴퓨터의 역할을 하며 서로 연동하는 새로운 사회의 모델을 제시하는 핵심어이다^[1].

유비쿼터스 컴퓨팅 기술을 기반으로 국가의 자원을 네트워크 상에서 통합하여 삶의 질을 향상시키고 국가 경제 발전을 추구하려는 u-Korea 전략이 정보통신부를 중심으로 추진되고 있다. u-Korea라는 지능기반사회에 진입하기 위해서는 IT분야의 서비스, 인프라, 기술개발의 3가지 요소가 서로 균형적으로 발전해야 한다는 것이 IT839 전략^[2]의 핵심이다. IT839란 8대 신규 서비스, 3대 첨단인프라, 9대 신성장동력을 뜻하며, 서비스 창출, 인프라 구축, 기술개발을 상호 보완적으로 연계하여 IT산업의 선순환적 구도를 정착시키고 국민소득 2만불 시대를 앞당기는 것이 주요 내용이다^[3].

이 전략이 성공하기 위해서는 적절한 시기에 정보보호 대책이 수립되어야 한다. 새로운 정보통신 서비스의 개발에는 상호 인증, 이용료 과금 등의 문제가 필연적으로 발생하게 된다. 또한, 새로운 인프라의 구축은 새로운 암호 프리미티브의 개발이라는 원천기술 개발까지 요구하게 된다.

다. 예를 들면, 유비쿼터스 센서 네트워크와 같은 새로운 환경에서는 보안 요구사항도 달라지게 되며, 기존의 범용 암호 알고리즘을 수용하기가 어렵다.

지능기반사회인 u-Korea를 이루기 위해서 필요한 기술적인 방안이 IT839전략이며 IT839전략이 성공적으로 추진되기 위한 기반 기술이 정보보호 기술이다. 따라서 관련 정보보호 기술의 개발은 IT839전략의 성공에 필수적이며 최소한의 요구조건이 된다. 본고에서는 IT839의 각 요소에서 필요한 정보보호 기술을 점검하고자 한다.

II. IT839 전략

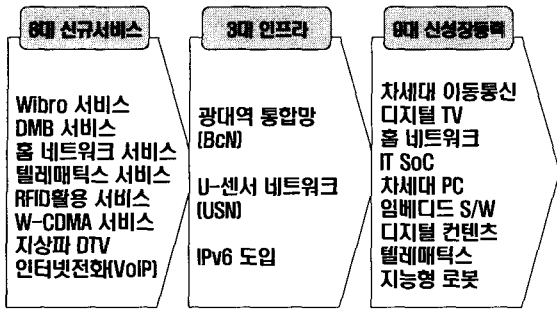
여기서는 IT839전략의 구체적인 내용을 소개하도록 한다. 그림 1과 같이 IT839란 8대 서비스, 3대 인프라, 9대 신성장동력을 의미한다.

1. 추진 배경 및 목표

지난 20여 년간 국내의 IT산업은 세계 강국으로 도약하였으며, 초고속 통신, 이동통신 등에서 세계 최고의 인프라를 보유하게 되었고, 반도체, 이동통신 단말기, 인터넷 게임 등은 세계적인 사업으로 성장하였다. 이러한 성공의 배경에는 새로운 서비스의 도입, 이를 가능케 하는

* 한국전자통신연구원({dwhong, kyoil}@etri.re.kr)

** 국가보안기술연구소({yjyeom, chee}@etri.re.kr)



(그림 1) IT839전략

인프라 구축, 기기제조 능력이 융합되어 있었다. 최근의 IT산업은 산업, 제품의 경계가 점점 모호해지고 신산업이 탄생하는 역동적인 환경을 맞고 있다. 이러한 환경을 성장과 도약의 모멘텀으로 활용하여 새로운 선순환 발전구조로 전화하려는 시도가 바로 IT839이다. 경쟁국보다 한발 앞선 서비스의 도입과 인프라 구축, 제조업의 연계를 통하여 미래 성장동력을 창출하여 IT산업의 발전을 도모하고, 국민소득 2만불 시대를 여는데 IT분야가 핵심적인 역할을 하하고자 하는 것이 IT839전략의 목표이다. 각 세부과제의 내용을 간략히 살펴보도록 한다.

2. 8대 신규 서비스

2.1 휴대인터넷 서비스

휴대인터넷(Wibro, Wireless Broadband) 서비스란 정치 및 이동 중에서도 언제, 어디서나 고속으로 무선인터넷 접속이 가능한 휴대인터넷 서비스를 뜻하며, 유·무선 전화시장 및 초고속인터넷 시장이 포화상태를 보임에 따라 통신시장의 차세대 성장동력으로 부상하고 있다. 금년도 휴대인터넷 허가시기 및 사업자 선정방안을 확정하여 '06년도 상용서비스를 개시할 예정이다.

'06년 휴대인터넷 서비스 도입을 통해 '10년까지 가입자 800만명, 3조원의 휴대인터넷 시장 창출이 가능할 것으로 보이며 '10년까지 약 4만명의 휴대인터넷 관련 고용 창출이 기대된다.

2.2 DMB 서비스

DMB(Digital Multimedia Broadcasting) 서비스는 고품질의 음성 및 영상서비스를 언제 어디서나 제공할 수 있는 이동멀티미디어 방송으로, 세계 최초의 상용서비스 도입으로 디지털방송기 산업과 콘텐츠 산업에 활력을 부여하는 차세대 성장동력으로 육성하고자 한다.

위성DMB와 수도권 지상파DMB 본방송은 올 하반기에 제공하고, 기타 지역은 채널이 확보되는 '06년부터 서비스를 시행할 예정이다. 뛰어난 이동수신 특성을 바탕으로 음악·문자·동영상 등 다양한 콘텐츠를 휴대용TV·PDA·휴대폰 등을 통해 제공하고 세계 최초로 지상파 DMB 송수신기술을 개발·상용화함으로써, CDMA단말기처럼 세계적인 경쟁력을 갖춘 산업으로 육성하고 있다.

'04~'12년간 지상파DMB 예상시장 규모는 2조4천억원, 생산유발 효과는 3조4천억원에 이를 것으로 기대되며, 고용유발효과는 4만명에 이를 전망이다. 또한, 이 기간 동안 위성DMB 예상시장 규모는 1조7천억원, 생산유발 효과는 1조8천억원, 고용유발효과는 3만4천명에 이를 전망이다.

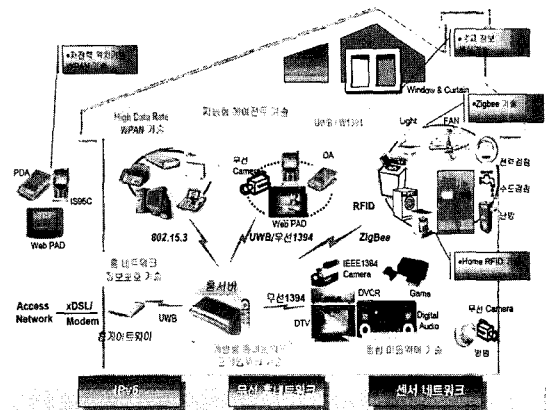
2.3 홈 네트워크 서비스

홈 네트워크는 정보가전이 네트워크로 연결되어 기기·시간·장소에 구애받지 않고 다양한 서비스가 제공되는 미래 가정환경을 제공하고자 하는 서비스로서 통신·방송·건설·가전 및 솔루션 등이 결합되어 연관 산업에 대한 신규 수요창출 효과가 매우 큰 서비스 산업이다.

'04년 50만 가구를 시작으로, '07년에는 전체가구의 60%인 1,000만 가구에 홈 네트워크를 보급할 예정이다.

2.4 텔레매틱스 서비스

텔레매틱스란 위치정보와 무선통신망을 이용하여 교통안내 및 Infotainment 서비스를 제공하는 차량멀티미디어 서비스이다. 텔레매틱스는 유·무선통신 및 방송망을 기반으로 차량을 제3의 인터넷 공간으로 만드는 새로운 개념의 부가가치 서비스로 '07년 시장규모 3.2조원, 단말기 보급률 27%로 확대하여 텔레매틱스 산업 선도국



(그림 2) 홈 네트워크 기술개발 구성도 (4)

가(Top 5)의 진입을 목표로 하고 있다.

제주도에 텔레매틱스 시범도시 구축을 추진('04. 5월~'06. 5월)하고 있으며 텔레매틱스 활성화로 관련 산업의 경쟁력 강화 및 '07년까지 생산유발효과 7조 3,530억원, 부가가치 유발효과 1조원 예상하고 있다.

2.5 RFID 활용 서비스

RFID란 전자칩을 부착하고 무선통신 기술을 이용하여 사물의 정보를 확인하고, 주변 상황정보를 감지하는 센서 기술로 식료품부터 축산물관리, 폐기물관리, 환경관리, 물류·유통, 보안 등에 적용된다. 향후 USN 인프라 구축에 따라 우리 생활의 다양한 분야에 적용될 전망이다.

'04년 RFID용 주파수를 추가 분배하고, '10년까지 전자칩, 리더 및 미들웨어 등 관련 핵심기술 개발을 완료할 예정이며, '05년 수동/능동형 RFID, '07년 센싱형 RFID, '10년 유비쿼터스 센서 네트워크 등 핵심 요소기술 및 시스템 개발을 계획하고 있다.

2.6 W-CDMA 서비스

W-CDMA서비스는 2GHz대역의 주파수를 이용하여 음성뿐 아니라 영상 및 고속 데이터 서비스가 가능한 IMT-2000 서비스이다. 2세대 CDMA를 통해 형성한 무선통신강국 이미지를 3세대까지 지속할 수 있도록 3세대 W-CDMA서비스를 본격적으로 제공할 예정이다.

'04년말까지 서울 및 수도권의 W-CDMA서비스를 안정화시켜 '05년부터 CDMA서비스와의 균형발전을 도모하고자 한다. 통신사업자의 W-CDMA 투자로 '10년까지 생산유발 95,635억원, 부가가치 유발 11,821억원, 고용 창출 효과 약 10만명이 예상된다. 또한, 금년부터 유럽, 일본 등을 중심으로 본격 형성될 세계 W-CDMA시장에 국내업체들의 활발한 진출이 가능할 것으로 전망된다.

2.7 지상파 DTV 서비스

지상파 DTV는 대화면·고화질·입체음향의 고품질 방송을 제공할 수 있는 서비스로 '05년 말까지 전국 방송망 완성을 목표로 하고 있다. 다양한 염가형의 수상기 개발·보급, HDTV 방송시간 확대 및 DTV 수신환경 개선을 통해 디지털방송 활성화를 추진하고 있으며, '04~'08년까지 생산유발효과 229조원, 고용창출 126만명이 예상된다.

2.8 인터넷 전화(VoIP) 서비스

초고속인터넷 보급 확대 및 인터넷백본망 구축 완료에 따라 저렴한 요금으로 전화서비스를 이용할 수 있는 인터넷전화도 등장하였다. 음성신호를 패킷데이터로 변환하여 인터넷망 위에서 전화서비스를 제공하는 인터넷전화는 All-IP기반인 BcN의 주력 응용분야 중 하나이다. '04년 착신번호 부여를 시작으로 인터넷전화도 '10년 BcN 기반의 기초 통신서비스로 발전할 수 있도록 제도정립을 조속히 완료할 예정이다.

세계 최고 초고속인프라를 기반으로 한 인터넷전화서비스 성공을 토대로 장비, S/W 등 인터넷전화산업 경쟁력 강화를 병행 추진하고 있으며 세계 VoIP 기술 및 표준을 주도하고 화상통화, 멀티미디어 및 걸재서비스 등 다양한 형태의 부가서비스를 접목시켜 편리한 통신환경 구축의 중심적 역할을 수행하고자 한다.

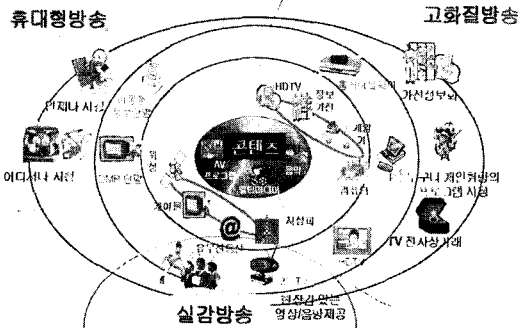
3. 3대 첨단 인프라

3.1 광대역 통합망

우리나라는 '95년부터 초고속정보통신망 구축계획을 적극 추진하여 세계 최고수준의 정보인프라 강국으로 발전하였다. 향후 통신·방송·인터넷의 대통합시대에 대응하고, 신성장동력산업의 발전토대를 마련하기 위해서는 광대역통합망(BcN) 구축이 필요하다.

'10년까지 2천만 유·무선 가입자에게 50~100 Mbps급의 고품질 서비스를 제공하는 광대역통합망을 구축을 목표로 하고 있다. 품질(QoS)이 보장되며, 보안, 새로운 인터넷 주소표준(IPv6) 등이 지원되고 다양한 융합서비스를 제공하는 통신망 확보를 위하여 첨단 연구개발을 구축하여 광대역통합망 관련 핵심기술을 개발·검증하고 시범사업을 추진한다.

광대역통합망 구축을 통해 67조원의 민간투자를 유발할 것으로 기대하며, 통신·방송장비 시장에서의 생산유발효과는 111조원에 이를 것으로 예상된다.



(그림 3) 미래 디지털 방송서비스 환경 [5]

3.2 U-센서 네트워크

u-센서 네트워크(USN)는 모든 사물에 전자태그(RFID)를 부착, 인터넷에 연결하여 정보를 인식 및 관리하는 네트워크로 사물의 정보화를 위한 첫 걸음이며 이는 유비쿼터스 사회 구현을 위한 기반구조이다. 농축산물 관리, 환경, 교통, 유통, 물류 등 u-센서를 이용하여 사업이 가능한 다양한 분야의 비즈니스 모델을 발굴하고

국민생활 및 산업 전반에 파급효과가 큰 응용분야에 대해 시범서비스를 실시하여 초기 시장 창출하며, 보급기간 단축을 위해 서비스와 응용 시스템 개발을 병행하여 추진하고 법·제도 체계를 정비할 예정이다.

상품 및 식품관리, 교통, 환경, 의료 등 광범위한 실생활 적용으로 국민생활의 편의성을 증대시키며, 반도체 산업을 기반으로 전자태그, 센서 등 첨단 신산업 창출과 물류체계의 혁신을 선도할 것으로 기대된다.

3.3 차세대 인터넷 프로토콜(IPv6)

현재 우리가 사용중인 인터넷프로토콜(IPv4)은 '06년부터 주소부족 문제를 초래하여 이에 대한 근본적 해결책이 필요하다. 광대역통합망(BcN), 홈 네트워크, 텔레메틱스 등의 구현에 필수적인 핵심요소인 차세대 인터넷 프로토콜(IPv6)을 조기 활성화하여 인터넷 생산강국으로 부상하고자 한다.

'04년 IPv6 시범망 확대 구축, '05년부터 상용서비스 개시, '10년 이후에는 All-IPv6 기반의 서비스 제공을 목표로 한다. BcN, 휴대인터넷, 홈네트워크 구축 등 신규사업에 IPv6를 적용하고, RFID, 3G 이동통신 사업과도 연계하여 추진하여 8조6천억원의 생산유발효과 및 5만3천여명의 고용유발효과 창출이 가능할 것으로 기대된다.

4. 9대 신성장 동력

4.1 차세대 이동통신

차세대 이동통신은 새로운 고속 패킷 무선전송기술 및 IP기반의 이동통신망 기술을 중심으로 통합·발전할 전망이다. 정치 및 이동중에 다양한 형태의 멀티미디어 정보를 기존 이동통신망, 인터넷망 등과 연동하여 고속·고품질로 송수신 하는데 사용된다.

미래 이동통신시장에서 경쟁력 확보에 필수적인 기초·원천기술을 개발하고, 이를 국제표준에 반영하여 미래 핵심 IPR 확보하며 세계 최고의 인프라인 초고속인터넷 기반 위에, 휴대인터넷망을 선도적으로 구축하여 새로운 무선멀티미디어 수요를 창출하는 것을 목표로 한다.

4.2 디지털 TV

지상파 DMB 송수신 단말은 음성·영상, 데이터서비스 등을 이동환경에서 제공하기 위한 기술로 '06년 말까지 상용화를 추진한다. 차량, 휴대환경 등 언제 어디서나 활용가능한 통신·방송 융합서비스를 제공하기 위한 DMB 전송시스템 및 단말기술을 개발한다.

'06년 말까지 양방향 DMB 전송 및 단말시스템 개발을 완료할 예정이며 오디오·비디오와 데이터방송이 가능한 양방향의 단말기를 한국전자통신연구원을 중심으로 산업계, 방송사 등이 공동개발을 추진한다.

지상파 DMB는 '12년 시장규모 2조8천억원, 생산유발효과 3조4천억원 및 고용유발효과('04~'12) 4만명에 이를 전망이다.

4.3 홈 네트워크

홈 네트워크는 정보가전을 제어하는 홈 오토메이션, TV 기반의 홈 엔터테인먼트 서비스 등을 지원하는 핵심요소기술로서 우리나라가 강점인 디지털 TV, 초고속인터넷 기반을 최대한 활용하여 핵심기술 개발과 표준을 선점함으로써 세계시장 선도하는 것을 목표로 하고 있다.

'04년 유무선 통합 홈서버, '05년 통신방송 융합 홈서버, '06년 통신방송게임 융합 홈서버 개발을 완료하며 통신·방송·게임 융합 홈서버의 핵심요소 기술인 개방형 홈 네트워크 프레임워크, 무선 홈 네트워크 및 차세대서버 개발 추진한다.

홈 서버, 정보가전 제품의 국제 경쟁력을 확보할 수 있는 원천 기술 및 유·무선 홈 네트워크 핵심부품 기술을 확보하여 한·중·일 동북아 3국간 홈네트워크 표준화 협력체를 구성하고 세계시장의 표준을 선도하고자 한다.

4.4 IT SoC

IT SoC(System on Chip)는 비메모리 집적회로로서 그 자체로 차세대 성장동력일 뿐 아니라 IT 제품의 경쟁력을 좌우하는 핵심부품이다. 세계 반도체 시장은 SoC가 주도할 전망이다. 국내 반도체 산업은 메모리를 중심으로 성장하여 SoC 분야의 경쟁력이 취약하다.

'04년 휴대폰용 멀티미디어 칩셋을 개발하고, '07년까지 세계 IT SoC 3대 선진국으로 도약하는 것을 목표로 한다. 시장전망이 밝은 이동통신, DTV, 홈 N/W 등과 연계한 핵심 SoC 및 IP(지적자산)를 개발하고 IP DB를 구축하며 대학과 연계한 SoC Architect 교육과정 운영 및 산·학·연 공동 SoC개발로 산업체가 요구하는 이론과 실무를 겸비한 인력 양성을 도모한다.



(그림 4) 차세대 PC 기술개발 진화방향 ^[6]

'07년까지 매출액 1,000억원 규모의 설계전문기업 10여개가 성장하여 1,600억원 규모의 세계 시장에 진출하는 등 IT산업의 경쟁력 확보에 크게 기여할 것으로 전망된다.

4.5 차세대 PC

차세대 PC란 정보처리, 네트워크 기능을 가지고 의복 등에 내재되어 입을 수 있는 컴퓨터로 미래 유비쿼터스 환경의 핵심 단말이다. 센서, 휴먼인터페이스 기술 등이 집약된 차세대 PC는 이동성과 편의성을 극대화하여 인간 중심의 서비스를 제공하는 것을 목표로 한다.

'04년 차세대 PC 시제품을 개발하고, '06년 표준화 추진 및 기술 확보하여, '07년말까지 입을 수 있는 컴퓨터 개발을 완료할 예정이며 입을 수 있는 컴퓨터 구현에 요구되는 초소형 플랫폼, 휴먼인터페이스 등 핵심기술개발을 '04년도부터 중점 추진한다. 차세대 PC를 미래 전략 산업화하여 350억불에 이르는 세계 시장을 선점할 예정이다.

4.6 임베디드 S/W

임베디드 S/W는 정보가전, 차량, 로봇, 산업기기, 의료기기, SoC 등 차세대 성장동력 분야의 제품에 내장되는 S/W를 뜻하며 H/W제어, 통신, 멀티미디어, 인터넷, 인공지능 등 제품을 스마트하게 만드는 기능을 제공한다.

다양한 규모의 제품개발에 활용이 가능한 임베디드 S/W 플랫폼과 제품별 솔루션을 '07년까지 매년 제공하게 되어 표준형, 마이크로형, 나노형의 범용 임베디드 S/W 플랫폼과 DTV, 스마트폰, 로봇 등에 특화된 솔루션을 개발·보급할 예정이다. 공개소스 채택으로 조기에 국제 수준의 기술력을 확보하고, 이동통신 단말, 디지털 홈 분야에 적용하여 세계기술을 선도하고 산·학·연이 유기적으로 연계된 인력양성 프로그램으로 H/W와 S/W를 모두 다룰 수 있는 고급 엔지니어 양성할 계획이다.

'07년까지 다양한 임베디드 S/W 개발로 생산유발효과

12조원 달성이 가능한 세계 2대 임베디드 S/W 강국으로 도약하는 것을 중장기 목표로 한다.

4.7 디지털 콘텐츠

Digital-Life 시대의 도래로 문화, 교육, 의료 등 다양한 콘텐츠가 IT기술과 결합하여 디지털 형태로 가공 처리된 디지털 콘텐츠(DC)의 중요성이 증대되고 있으며 한계비용이 '0'에 가까운 고부가가치 산업으로 이동통신, DTV, 홈 네트워크 등 다른 신성장 동력산업의 부가가치를 증대시키는 핵심산업이다.

3D 컴퓨터그래픽스, 멀티플랫폼 연동형 온라인게임 엔진, 멀티플랫폼 기반 e-Learning 솔루션 등 차세대 핵심기술을 개발하고 온라인게임, 모바일콘텐츠, e-Learning 등 유망분야를 중심으로 첨단 IT 콤플렉스 건립을 통한 DC 전문집적단지 조성하여 해외시장 진출을 지원하고 글로벌 테스트베드 운영할 계획이다.

온라인게임과 모바일콘텐츠 분야 세계 1위 유지 및 세계 3대 CG 생산기지 구축으로 '07년 생산유발 효과 127억불을 달성할 전망이다.

4.8 텔레매틱스

이동통신과 자동차를 결합하여 차량에서 편리함과 안전 및 즐거움을 제공받도록 하는 서비스로 차량에서도 사무실처럼 콘텐츠, 통신, 상거래를 이용 가능케 하는 핵심 기술 개발을 추진한다.

서비스 사용자, 이동통신 사업자 및 자동차 제조사의 요구사항을 반영한 핵심 기술개발 추진하며 호환성 시험장을 조기에 구축하여 제품 시험 및 인증에 활용하며, 수요기반 확대 및 서비스 고도화를 추진한다. IBM 등 해외 우수 연구소 및 스웨덴 텔레매틱스 벨리와 연구 협력으로 국제 표준화 및 해외시장 조기 진출 추진한다.

4.9 지능형 로봇

언제 어디서나 이용자 요구에 부응한 IT서비스를 제공하는 IT기반의 지능형 서비스 로봇(Ubiquitous Robotic Companion : URC)은 미래핵심 산업으로 기존 로봇에 네트워크기능을 부가하여 저렴한 비용으로 IT서비스 이용을 가능하게 한다.

'05년에 아파트 400가구 및 공공장소(우체국) 200개소에 URC 로봇을 설치하여 초기시장 창출 가능성 타진하며 인간지향 서비스를 중심으로 개발하고, 레고식 기술 개발 전략을 통해 향후 지속적인 기술발전을 선도한다.

지능형서비스 로봇의 상용화로 2,000억불에 이르는 세

계시장을 선점할 계획이며, '13년까지 생산유발효과는 13조원에 이를 전망이다.

III. IT839를 위한 정보보호 이슈

IT839전략의 추진으로 인하여 새로운 서비스와 인프라에 대한 정보보호 기술의 개발이 요구되고 있으며 새로운 정보보호 위협의 증가는 국내 정보보호 산업의 수요 증가와 도약을 위한 기회가 될 수 있다.

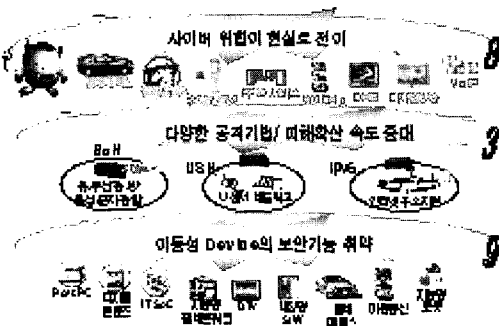
여기서는 정보보호 요구사항을 기반요소, 인프라보호, 디바이스보호, 방송콘텐츠보호의 4개 분야로 나누어 정리하고자 한다.

1. 기반요소

IT839의 새로운 서비스와 인프라 구축에 필요한 기반 기술로는 암호설계, 개인정보보호, 인증 및 ID관리 등이 있다.

새로운 정보 인프라 구축에 따른 정보보호 서비스를 위해서는 새로운 암호 알고리즘의 개발이 요구되고 있다. 유비쿼터스 센서 네트워크(USN) 분야와 BcN 등의 새로운 환경에는 기존의 알고리즘을 적용하기에 무리가 있다. 따라서 초경량, 저전력 환경에 대비한 암호 알고리즘의 개발이 필수적이다. 이를 위해 다양한 서비스에 적합한 알고리즘의 요구사항 분석도 병행되어야 한다.

급속한 정보화의 진전은 개인정보의 누출과 같은 사회 문제를 야기하고 있으며 RFID/USN 환경에서는 특히 개인정보보호와 익명성보호 등이 중요하며 이를 위해서는 기술 개발 뿐만 아니라 새로운 패러다임에 적합한 법, 제도의 정비도 함께 다루어져야 한다. 개인과 기업 등 정보 사회의 주체가 법으로 보장되는 자유와 권리를 사이버 공간에서 안전하게 누릴 수 있는 정보보호 환경의 조성이 중요하게 부각될 것으로 예상된다.



(그림 5) IT839전략의 위협요인^[7]

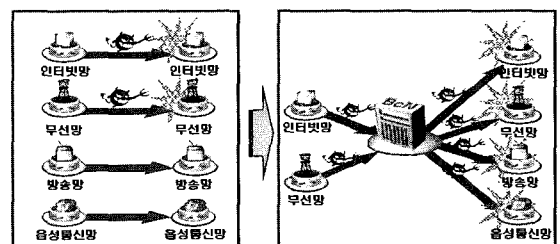
인터넷 기반의 안전한 전자거래를 위하여 사용되는 인증 및 ID관리 기술은 서비스의 다양화에 따라 그 중요성이 더욱 증대할 것이며 새로운 인프라 구축에 따라 다양한 인증 기술이 개발되어야 한다. 유럽의 ECRYPT 프로젝트^[8]에서도 다자간 프로토콜 기술이 비중있게 다루어지고 있으며 일대일이 아닌 다자간 통신환경이 주를 이룰 새로운 환경에 대비한 기술개발이 확대될 것으로 예상된다. 또한, 생체인식 기술은 개인인증에 있어서 최선의 수단으로 인식되고 있으며 이에 대한 투자도 활발히 전개될 것으로 판단된다.

2. 인프라 보호

통신, 방송, 인터넷이 융합된 차세대 통합 네트워크에서는 위협을 능동적으로 탐지하고 대응할 수 있는 통합 보안 관리 기술이 요구된다. 초고속 망에서의 고성능 네트워크 위협 대응 기술과 침입에 의한 과대 트래픽 감지 기술이 필요하며 공격자에 대한 능동적 대응을 위하여 역추적 기술도 크게 부각될 것이다. 또한 IPv6의 연동에 따른 보안 대책도 수립되어야 한다. 기존의 IPv4와 IPv6간의 변환용 네트워크 노드에 대한 보안 기술과 보안 게이트웨이 기술이 필요하며 mobile IPv6용 인증, 접근제어 등의 기술이 필요하다.

유비쿼터스 센서 네트워크(USN) 분야는 새로운 보안 요구사항이 가장 많이 필요한 인프라이다. 초경량, 저전력 환경은 강력한 보안대책을 적용하기에 어려움이 있으며 주요 서버에 대한 트래픽의 관리도 필요하다. RFID와 USN 관련 정보보호 기술은 세계적으로도 초기 단계이며 미국, 일본 등에서는 개인정보보호를 위한 법제도의 마련을 동시에 추진하고 있다. 기존의 보안기술로는 RFID를 사용하는 USN에 대한 새로운 위협에 대처하지 못하며 USN 전용의 보안기술과 보안 인프라 구축이 필요하다.

악의적인 공격자가 RFID 태그의 정보를 얻는 것을 막는 인증기술과 도청방지 기술이 필요하며 데이터의 기



(그림 6) 통합 네트워크(BcN)의 위협 요인^[7]

[표 1] 디바이스 보호 관련 보안 요구사항¹⁰⁾

구분	분야	보안 요구사항
8대 서비스	홈 네트워크	- 원격관리 및 제어에 따른 사용자 권한 인증 - 가전 단말 및 사용자에 대한 접근 제어
	휴대 인터넷	- 기밀성 보장 및 인증 - 경량화된 무선 해킹방지
	VoIP/W-CDMA	- 도감청 방지 - 침해탐지, 대응
	DMB/DTV	- 불법복제 방지 및 유통관리 - 유료 콘텐츠의 과금문제
	텔레매틱스	- 위치정보에 대한 개인정보 유출 문제 - 정보 DB 보호기술
9대 신성장 동력	지능형 로봇	- 로봇 및 관리자에 대한 접근 제어 - 로봇간의 상호 인증
	임베디드 S/W	- 임베디드 보안 S/W(암호, 인증, 키관리, 접근제어 등)
	IT SoC	- 고속 보안 SoC - 이동통신용 보안 SoC
	차세대 PC	- 사용자 인터페이스에 대한 인증 - 경량화, 저전력화된 침해 탐지 및 대응
	디지털 콘텐츠	- 콘텐츠 보호관리 - 유해정보 차단 기술

밀성과 무결성을 보장하는 방법이 연구되어야 한다. 또한, 태그는 그 정보를 추출하려는 부채널 공격에 대한 내성을 가지도록 설계되어야 한다.

각 서비스에 대하여 디바이스 보호 측면에서의 보안 요구사항을 간략히 정리하면 표 1과 같다.

3. 디바이스 보호

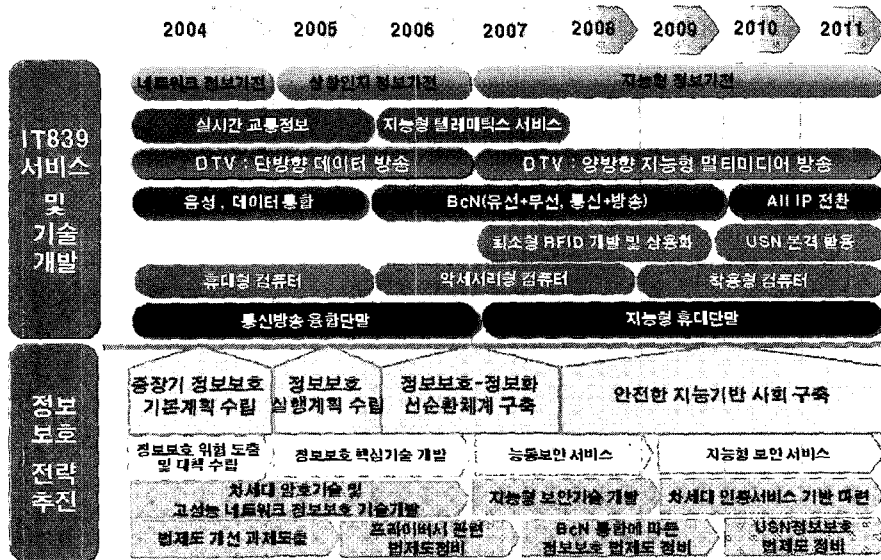
유무선 통신, 방송, 인터넷 등 인프라의 통합화와 휴대 인터넷, 홈 네트워크, DMB 등 다양한 멀티미디어 서비스의 증가로 통합보안 서비스에 대한 요구가 증가하고 있다. 현재 각 분야에서 사용되는 정보기기는 지능화되고 통합되어 디지털 컨버전스 디바이스로 발전하는 추세이다. 컨버전스의 가속화로 컴퓨팅 기능이 내장된 단말기가 확산됨에 따라 저전력 보안기술에 대한 요구도 증대되고 있다.

8대 서비스에서의 대표적인 위협요소는 휴대인터넷 기반의 전자거래에서의 정보도용, VoIP, W-CDMA에서의 도·감청 문제, 텔레매틱스 기반의 위치정보 유출 등이 있다. 9대 신성장 디바이스에서는 지능형 로봇의 기기인증 문제, 한정된 자원을 사용하는 임베디드 S/W에서의 침입방지, 차세대 PC의 다양한 인터페이스에서의 인증과 접근제어, 디지털 콘텐츠의 불법 유통방지 등이 있다.

4. 방송콘텐츠 보호

방송매체의 경우 그 특성상 시청 권한을 관리하고 불건전 정보를 차단할 수 있는 기술이 필요하며 양방향 서비스의 제공에 따라 다자간 통신 프로토콜 기술이 요구된다. 서비스 과금의 문제와 콘텐츠의 불법 복제 및 재배포 방지를 위한 대책이 수립되어야 한다. 이 분야는 디지털 저작권 문제와 밀접한 관련이 있으며 기술적으로 기본적인 암호화 기능 외에도 워터마킹이나 핑거프린팅 기술이 필요하다. 사용자에게 불편을 주지 않으면서 콘텐츠를 보호하는 것은 서비스의 성공을 결정하는 매우 중요한 요소가 되며 기술의 발전과 법제도의 정비가 병행되는 것이 바람직하다.

최근 불법적인 MP3파일의 유통과 MP3폰 문제의 경우를 보면 원칙적으로는 다수의 동의를 얻어 내는 해법이 존재하지만 기술적 대안의 부재로 합리적인 유통구조를 만들 수 없었고, 저작권을 보호하는 솔루션이 사용자의 불편을 초래하는 사례가 발생하였다. 실제 사용자의 요구



(그림 7) IT839전략과 정보보호 기본계획과의 연계¹⁾

가 반영되고 기술적인 성숙과 사회전반의 합의가 도출 되어야 성공적인 서비스의 활성화가 가능할 것으로 판단된다.

IV. 결 론

IT839전략은 80년대 TDX 전자교환기, 90년대 CDMA의 뒤를 이을 새로운 IT발전 전략으로 추진되고 있으며 국민소득 2만불 시대를 주도할 기술개발 전략이다. 또한, 정보화 사회, 지식기반 사회로부터 더 나아가 지능기반 사회를 구축하려는 u-Korea전략의 핵심이기도 하다.

과거 정보통신 인프라 구축과 별도로 뒤늦게 정보보호가 추진되어 야기되었던 어려움과 혼란을 더 이상 되풀이 하지 않으려면 정보보호 기술이 인프라 구축, 서비스 개발과 동시에 진행되어야 한다. 이번 IT839전략 추진에서는 새로운 서비스, 인프라의 개발과 관련된 정보보호에 대한 연구가 초기부터 함께 고려되어야 할 것이다. 정보보호 분야는 정보통신 환경에서의 부가적인 기능을 수행하는 소극적인 기여에서 새로운 정보보호 기술의 개발이 새로운 서비스 개발에 직결될 수 있는 적극적인 기여를 하여야 할 것이다.

본고에서는 IT839전략을 성공적으로 추진하기 위하여 필요한 정보보호 기술을 간략히 살펴보았다. 아직은 각 서비스와 인프라에 대한 세부적이고 정량적인 보안 요구사항이 정립되지 않았기 때문에 다소 피상적인 접근이 되지 않았나하는 우려가 된다. 세부적인 분야에서 구체적인

정보보호 기술 개발을 추진하기 위해서는 서비스 및 기술 개발과 지속적으로 상호 연동하여야 하며 동시에 관련 법제도의 정비도 함께 이루어져야 그 효과를 극대화 할 수 있을 것으로 판단된다.

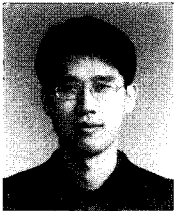
참 고 문 헌

- [1] 사카무라 겐, *유비쿼터스 컴퓨팅 혁명*, 동방미디어, 2002.
- [2] 정보통신부, "국민소득 2만불로 가는 길 IT839전략", 2004.
- [3] 정보통신부, "IT분야 신성장동력, u-Korea 추진 전략", 2004.
- [4] 박광로, "홈 네트워크 사업 소개", IT839 정보보호 중장기 기술개발 계획수립을 위한 실무협의회 워크샵, 2004.
- [5] ETRI 디지털방송연구단, "디지털TV: 방송콘텐츠 보호관리 기술", IT839 정보보호 중장기 기술개발 계획수립을 위한 실무협의회 워크샵, 2004.
- [6] 장병태, "텔레매틱스 기술 개발", IT839 정보보호 중장기 기술개발 계획수립을 위한 실무협의회 워크샵, 2004.
- [7] 정보통신부, "IT839전략 구현을 위한 중장기 정보보호 기본계획", 2004.
- [8] ECRYPT, "European Network of Excellence for Cryptology", www.ecrypt.org.

eu.org, 2004.

- [9] 장병준, "RFID/USN 기술 개요 및 정보보호 요구 사항", IT839 정보보호 중장기 기술개발 계획수립을 위한 실무협의회 워크샵, 2004.
- [10] ETRI 정보보호연구단, "정통부 정보보호 중장기 기술개발 계획-보안요구사항", IT839 정보보호 중장기 기술개발 계획수립을 위한 실무협의회 워크샵, 2004.

〈著者紹介〉



홍도원(Dowon Hong)

1994년 2월 : 고려대학교 이과대학 수학과(학사)
 1996년 2월 : 고려대학교 수학과(석사)
 2000년 2월 : 고려대학교 수학과(박사)
 2000년 4월~현재 : 한국전자통신연

구원 팀장

〈관심분야〉 암호 이론, 정보보호 이론, 이동통신 정보보호

염용진(Yongjin Yeom)

1991년 2월 : 서울대학교 자연과학대학 수학과(학사)
 1994년 2월 : 서울대학교 자연과학대학 수학과(석사)
 1999년 2월 : 서울대학교 자연과학대

학 수학과(박사)

2000년 4월~현재 : 국가보안기술연구소 팀장

〈관심분야〉 암호 이론, 정보보호



정교일 (Kyoil Chung)

1981년 2월 : 한양대학교 전자공학과 졸업
 1983년 8월 : 한양대학교 산업대학원 전자계산학과 석사
 1997년 8월 : 한양대학교 대학원 전

자공학과 박사

1980년 12월~1981년 11월 : 엠시스템즈 사원

1981년 12월~1982년 2월 : 한국전기통신연구소 위촉연구원

1982년 3월~현재 : 한국전자통신연구원 정보보호기반연구그룹장/책임연구원

〈관심분야〉 IC Card, Security, Biometrics, 국가기반보호, 신호처리

지성택 (Seongtaek Chee)

1985년 2월 : 서강대학교 수학과 학사
 1987년 2월 : 서강대학교 수학과 석사
 1999년 2월 : 고려대학교 수학과 박사
 1989년 10월~1999년 12월 : 한국전자통신연구원 정보보호연구본부 선

임연구원

2000년 1월~현재 : 국가보안기술연구소 책임연구원

〈관심분야〉 암호론, 부울합수