안전한 u-Korea 실현을 위한 정보화 역기능 방지 대책 – "Security Belt"

Information Security Strategy for Secure u-Korea – "Security Belt"

최병철 (B.C. Choi)	네트워크보안구조연구팀 연구원
김광식 (K.S. Kim)	네트워크보안구조연구팀 선임연구원
서동일 (D.I. Seo)	네트워크보안구조연구팀 선임연구원, 팀장
장종수 (J.S. Jang)	네트워크보안그룹 책임연구원, 그룹장

목 차

유비쿼터스 코리아(u-Korea) 기본적략에 따르면 우리나라는 정치、사회、문화、의료、복지、교육、노동、외교 등 사회 전반에 걸친 생활문화 혁명이 실현될 것으로 전망된다. 이러한 시점에서 정보보호는 u-Korea 실현의 중요한 핵심 엔진 기술로써 u-Korea 전략 추진의 주요한 장애 요인으로 예상되는 사생활 문제와 지역 간、계층 간 정보격차 문제 등의 정보화 역기능을 해소하는 역할을 수행해야 한다. 본 고에서는 정통부가 추진하고자 하는 u-Korea 기본 전략에 대해서 살펴보고, 안전한 u-Korea 실현을 위해서 구체적인 정보화 역기능 방지 대책을 제안한다. 특히, BcN 인프라 보호 기술, RFID/USN 개인 프라이버시 보호 기술, WiBro 및 DMB 등에서 사용되는 복합단말기용 통합 인증、인가 기술, 안전한 사용자 서비스 제공을 위한 서비스 사용의 익명성과 서비스 관리의 실명성이 제공되는 보안위임서비스 기술 등으로 형성되는 "Security Belt" 정보화 역기능 방지 대책에 대해서 소개한다.

Ⅰ. 서론

향후 미래 사회는 하나의 단말기를 활용해 언제 어디서나 끊김없이(seamless) 다양한 품질보장형 광대역 멀티미디어 서비스를 사용할 수 있는 '컨버전스(convergence)'와 '유비쿼터스(ubiquitous)'를 충족시키는 기술, 제품, 그리고 서비스가 실현될 것이며, 이는 광대역통합망(BcN)을 중심으로 IPv6 주소체계를 기반으로 RFID/USN이 All-IP 망으로 통합되는 유비쿼터스 네트워크 환경을 통해서 실현될 것이다.

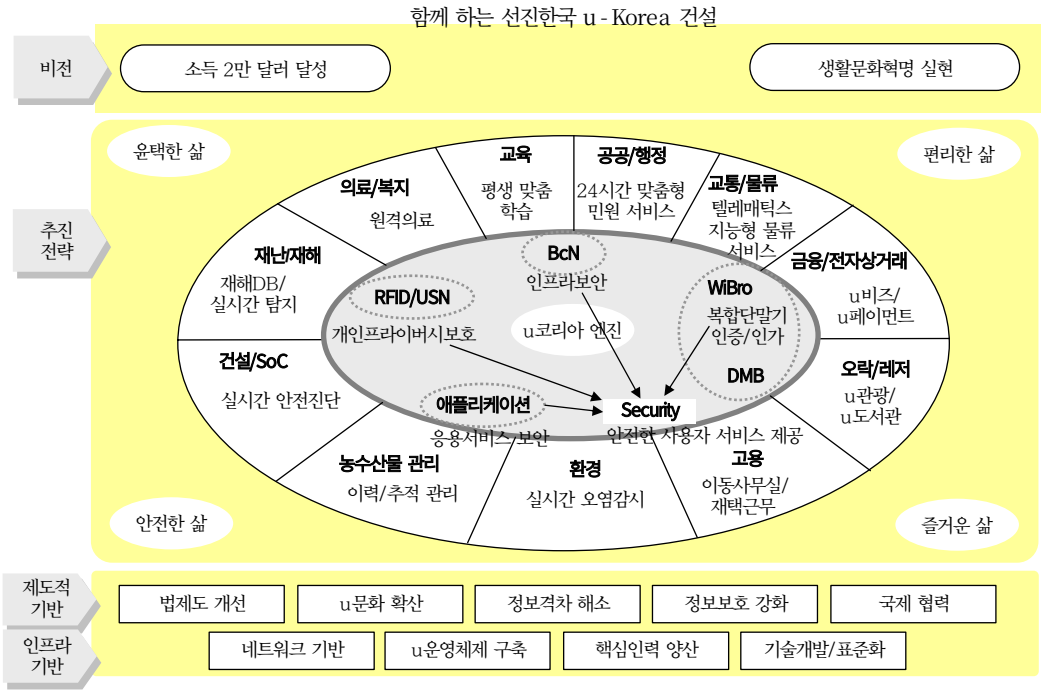
정통부는 이러한 시대적 요구사항을 적극 수용한 유비쿼터스 코리아(u-Korea) 기본전략을 수립하고 있다. u-Korea의 비전은 국민소득 2만 달러 달성과 생활문화혁명 실현을 통한 함께하는 선진한국 u-Korea 건설이다. 추진전략을 살펴보면 국민의 윤택한 삶, 편리한 삶, 안전한 삶, 즐거운 삶을 위해서 IT839 기본 엔진에 정보화 역기능 방지를 위해서 'Security' 분야를 핵심 엔진으로 추가하였다. 또한, 법제도 개선, u문화 확산, 정보격차 해소, 정보보호 강화 등의 제도적 기반과 네트워크 기반, u운영체제 구축, 핵심인력 양성, 기술개발/표준화의 인프라 기반을 바탕으로 추진할 계획이다[1],[2].

정통부는 u-Korea 실현의 목표를 2007년까지 세계 최초의 지능기반사회에 진입하고, 2015년까지 지능기반사회를 완성하는 것으로 설정하였다. 그러나, 이러한 유비쿼터스 사회의 혜택을 모든 국민이 고루 받으며, 국가적으로 신뢰성을 갖추기 위해서는 개인정보의 침해, 그리고 해킹·바이러스로 인한 폐해 등의 현재 정보화시대에서의 각종 정보화 역기능을 해소하여야 할 것이다.

따라서, 본 고에서는 안전한 u-Korea 실현을 위한 정보화 역기능을 방지 대책을 제안하며, 그 이름을 "Security Belt"라고 명명하였다.

Ⅱ. 정보화 역기능 방지 대책

본 고에서 제안한 "Security Belt" 정보화 역기



(그림 1) u-Korea 추진전략에서의 정보보호의 역할('Security Belt')의 전체 개념도

능 방지 대책은 유비쿼터스 네트워크 인프라의 핵심인 광대역통합망(BcN)에 대한 인프라 보호 기술, 유비쿼터스 환경의 핵심이라고 할 수 있는 RFID/USN에 대한 개인 프라이버시 보호 기술, 개인휴대인터넷(WiBro)과 위성/지상파 DMB를 위한 복합 단말기에 대한 통합 인증·인가 기술, 안전한 사용자 서비스 환경을 제공하기 위한 사이버실명제 기반의 보안위임서비스 기술, 기타 IT839 전략에 포함된 디바이스 및 서비스의 애플리케이션을 위한 응용 서비스 보안 등으로 구성되어 있으며, 본 고에서는 응용 서비스 보안에 대해서는 자세하게 언급하지 않는다. 이에 대한 필요성은 (그림 1)의 u-Korea 추진전략에서의 정보보호의 역할에서 잘 보여주고 있다.

향후 유비쿼터스 환경에서의 보안은 “Security Belt”라는 범주에서 상호 유기적으로 동작하며, 항상 사용자 중심의 서비스 보호를 위해서 어떻게 할 것인가에 대한 해결책 역할을 수행할 것이다.

1. BcN 인프라 보호 기술

세계 최고의 정보통신 인프라를 기반으로 IT 839 전략을 통해 BcN을 기반망으로 하는 유비쿼터스 네트워크 환경으로 진행이 가속화되고 있다. 현재의 인터넷망은 향후 광대역통합망의 구축을 통해 이종망간 끊김없는 멀티미디어 서비스 제공이 가능해짐에 따라 언제, 어디서나, 누구든지 편리하게 서비스를 이용할 수 있는 유비쿼터스 환경으로 진화될 것이다. 안전한 u-Korea 실현을 위해서 기본적으로 인프라에 대한 정보화 역기능을 해소해야 하며, 기존의 인터넷망뿐만 아니라 BcN에 대한 전반적인 보안 기술이 필요하다[3].

가. 위협 분석 및 정보보호의 필요성

유무선 통신망과 방송망의 융합에 따라 개별망 피해가 광대역통합망에 연결된 전체 네트워크의 피해로 확산될 우려가 있다. 즉, 기존의 사이버공격에 취약한 인터넷망에서 발생된 위협이 통신망을 통해 개별망으로 확산되어 음성통신망, 방송망, USN까지 피해 확산이 가능하다.

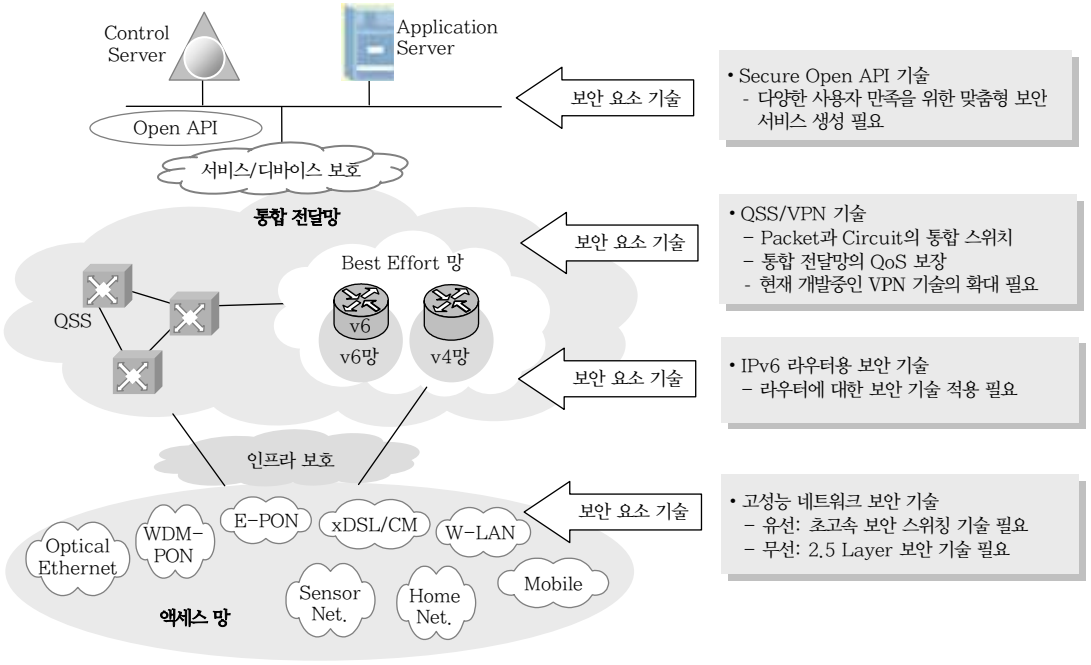
〈표 1〉 광대역통합망 계층별 예측 취약점

계층 이름	주요 이슈
서비스	- 서비스 계층으로의 접근 인증 및 권한 문제 - 개방형 인터페이스 제공 문제 – 서비스 사용자의 개인정보보호 문제 – 반사회·윤리적 정보 유통 문제 – 지적 재산권 보호 문제 – BcN 단위 서비스와 개별 망 서비스 응용 프로그램 사이의 상호 의존성 문제
관리/제어	– 서비스 게이트웨이 서버의 신뢰성 보장 문제 – 소프트스위치의 신뢰성 보장 문제 – BcN 망관리 시스템 보호 문제 – BcN 보안성 확보를 위한 법·제도 정비
전달	– 전달망 관리 측면의 서비스 품질 보장 – BcN 생존성 기능 고도화 – 이종 망간 상호 연동 시 정보보호 문제 – 고성능 정보보호 장비 확보 문제 – 암호화 트래픽의 유해성 여부 판단 문제
접속	– 망 통합으로 인한 취약성 확산 – 악의적인 공격의 위치 다양화 – 비인가자 접속 차단 기능 강화 문제 – 도청, 데이터 위변조 대책
홈/단말	– 홈 게이트웨이 안전성 보장 대책 – 가입자 망 접속 장비의 보안 취약성 – 휴대 단말을 활용한 사이버 공격 위험성 증대 – 이동성 보장에 따른 공격 근원지 추적 난이성 – 무선 단말기, USN 센서노드 보호대책 – 위장 단말기 및 접속장치(AP) 탐지 기능

또한, 광대역통합망은 개방형 망구조를 특징으로 하기 때문에 다양한 경로로 통신망에 쉽게 접근이 가능하여 해킹 및 바이러스 유포 확대의 가능성을 내제하고 있다. 〈표 1〉에서 알 수 있듯이, 서비스, 관리/제어, 전달, 접속, 홈/단말 계층별 다양한 주요 보안 위협이 존재하고 있다.

나. BcN 인프라 보호 기술

기존의 광역망 차원의 네트워크 위협 대응 시스템의 개발이 진행되고 있으며, 이것을 기반으로



(그림 2) BcN 인프라 보호 기술에서의 세부 보안요소기술 적용 개념도

BcN 환경 예측을 통한 secure open API, QSS/VPN, IPv6 라우터용 보안 기술, 고성능 네트워크 보안 기술 등의 전체적인 보안 기술 개발 체계가 필요하다.

BcN 백본 네트워크 인프라의 처리능력은 최고 수십 Gbps 수준인 반면, 현재의 정보보호 장비의 처리능력은 수 Gbps에 불과하여 BcN 인프라에 적용하는 데에는 한계가 있기 때문에 기본적으로 고성능/지능형 네트워크 보안 기술이 필요하다.

(그림 2)는 BcN 인프라 보호 기술에 대한 개념도이며, BcN에서 발생할 수 있는 위협에 대응하기 위해서는 전달망과 접속망을 보호하기 위한 고성능 네트워크 보안 기술뿐만 아니라 IPv6 망의 액세스 및 백본 에지 라우터를 위한 IPv6 라우터용 보안 기술, 패킷과 서킷의 통합 스위치이며 통합 전달망의 QoS를 보장하는 QSS에 고성능 VPN 기술을 결합한 QSS/VPN 기술, 보안성이 고려된 전달망과 서버간의 개방형 표준 인터페이스 제공과 맞춤형 보안 서비스 생성을 위한 secure open API 기술 등이 필요함을 알수 있다.

현재 네트워크 인프라 보호 기술 분야에 있어서 국내 제품은 외국 제품에 비해 기능과 성능 면에서 열세에 있고, 국내 업체의 기술 역량이 다소 취약한 실정이다. 이는 예산 및 인력의 부족과 BcN 네트워크 인프라의 현실적인 불확실성 때문이라고 판단된다. 따라서, 국가적 차원에서 인력양성 및 예산확보를 통하여 안정적이고 장기적인 연구 개발이 수행될 수 있도록 기틀을 마련하여야 할 것이다.

안전한 u-Korea 실현을 위한 국가 기반망의 보안성 확보를 위한 기술 개발 투자는 모든 정보화 역기능 방지 대책의 기본이 될 것이며, 1차적으로는 2003년 1월에 발생한 1.25 인터넷 침해사고와 같은 대재앙을 막을 수 있으며, 2차적으로는 “Security Belt” 완성의 기틀이 될 것이다.

2. RFID/USN 개인 프라이버시 보호 기술

유비쿼터스 코리아 완성을 위한 꽃이라고 할 수 있는 RFID/USN 환경에서의 공격/침해 대상은 기존 환경의 컴퓨터에 저장된 정보 또는 통신 정보만

이 아닌, 사물이나 신체 등 개인의 모든 정보가 되며, 공격 범위는 개인의 컴퓨터에 국한되지 않고 개인의 사적인 모든 공간이 될 것이다. 따라서, RFID/USN 환경에서는 개인 프라이버시 문제가 심각할 것이며, 이를 해결하는 것이 필요할 것으로 판단된다.

향후 모든 사물에 전자태그/센서를 부착하고 인터넷에 연결하여 자동인식·추적·센싱·제어·관리 서비스 제공을 가능케 하는 RFID/USN 환경이 될 것이며, 전자태그/센서 정보의 무단 누출 및 위변조, 오동작, 개인 추적 정보의 불법 수집·유통 등과 같은 새로운 보안 위협으로부터 개인 프라이버시와 RFID/USN 서비스를 안전하게 제공하는 데 필요한 초경량 객체 정보보호 핵심기술 및 시스템 개발이 필요하다[4]-[7].

가. 위협 분석 및 정보보호의 필요성

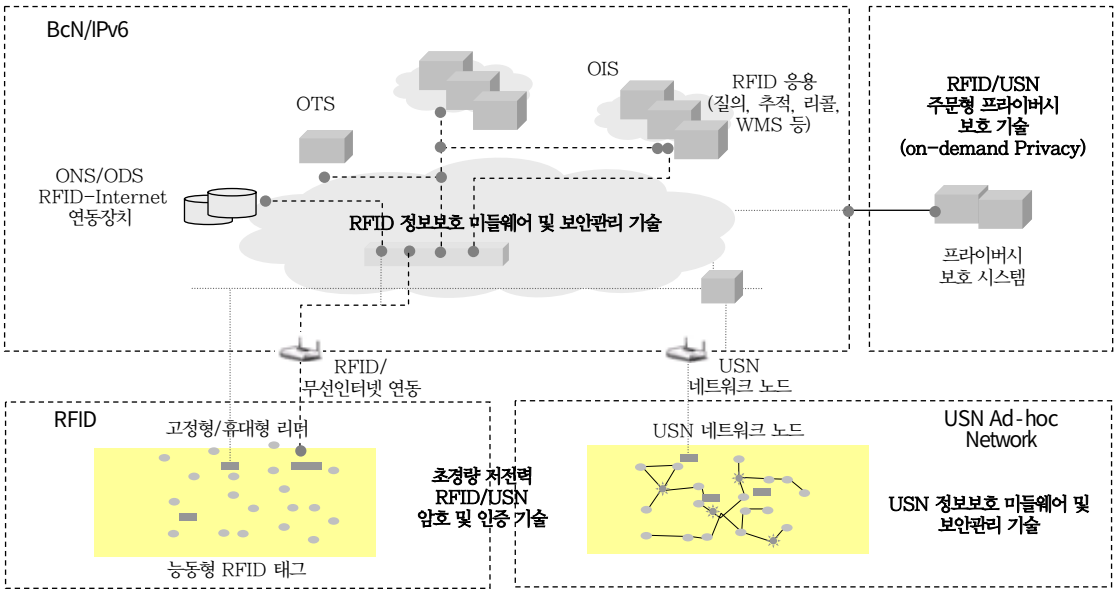
현재의 RFID 기술은 정보보호 기술을 포함하고 있지 않아, 태그 정보의 위변조, 위장리더, DoS/DDoS 공격, 네트워크에서 개인 추적 정보 유출 등의 위협에 노출될 것이다. 또한, RFID/USN 환경에서는 개인이 소유한 모든 물체 단위까지 침해 범위가 확대되며, 이는 RFID/USN 서비스 활성화에 심각한 장애 요인으로 작용할 것이다.

따라서, 태그 리더 영역, 미들웨어 영역, 서비스 인프라 영역에서 RFID/USN 서비스의 안전성을 제공할 수 있는 핵심 정보보호 기술이 개발되어야 한다. 특히, 보안 침해의 역작용이 큰 홈네트워크, 교통, 병원환자, 전자지불, 재난관리 등 안전 관련 영역에서 정보보호 기능이 없는 RFID/USN을 기반으로 하는 유비쿼터스 서비스 제공은 거의 불가능하다고 판단된다.

국내외적으로 연구 초기 단계에 있는 RFID/USN 정보보호 핵심 기술을 조기에 개발함으로써 2007년 191억 불(IDtechEx 추정, 2004. 1.)로 추정되는 RFID/USN 국내외 시장에서 경쟁력을 확보할 수 있을 것이며, 무엇보다도 안전한 u-Korea 실현을 위한 요소 기술이 될 것이다.

나. RFID/USN 정보보호 기술

RFID/USN 환경에서 개인 프라이버시를 적극적으로 보호하고, 사물의 자동식별·이력추적 등



(그림 3) RFID/USN 정보보호 기술 적용 개념도

RFID/USN 서비스를 안전하게 제공할 수 있는 초경량 정보보호 핵심 기술 및 시스템 개발이 필요하다.

RFID/USN 정보보호 기술은 크게 RFID/USN용 초경량 암호 칩/태그 기술, 멀티홉 객체 보안 관리 및 경량 정보보호 미들웨어 기술, 착탈형 프라이버시 보호 서비스 기술 등이 있으며, 이것의 주된 목적은 안전한 유비쿼터스 서비스 제공을 위한 개인 프라이버시 보호가 주 목적이다.

(그림 3)은 RFID/USN 정보보호 기술 적용 개념도이며 RFID와 USN Ad-hoc 네트워크를 위한 초경량 저전력 RFID/USN 암호 및 인증 기술, RFID/USN 정보보호 미들웨어 및 보안관리 기술, RFID/USN 주문형 프라이버시 보호 기술에 대해서 BcN/IPv6 망과의 연관성과 함께 표현하였다.

이러한 정보보호 기술은 RFID/USN 환경에서 사용자의 개인 프라이버시를 보호 및 관리할 수 있어서 안심하고 편리하게 RFID/USN 관련 서비스를 이용할 수 있도록 한다. 예를 들면, RFID를 이용한 고액상품, 유가 증권 등의 전자지불 서비스에 있어서 위변조 방지 및 부정 사용 방지에 활용될 수 있다. 특히, 국내 실정에 맞는 개인 프라이버시 보호 서비스 제공에 중요한 역할을 할 것으로 기대되며, RFID/USN 산업 활성화의 걸림돌인 보안 위협성을 해결할 것으로 예상된다.

3. 복합단말기용 통합 인증·인가 기술

유비쿼터스 통신·방송 융합형 신규 IT 서비스 환경에서 다양한 디바이스들이 네트워크 노드로 상호 연결되어 구성됨으로써 새로운 공격목표나 공격에 활용될 가능성이 높아지므로, 복합 단말기의 안전성 보장을 위한 복합 단말기 보안 기술 개발이 필요할 것으로 예상된다[4],[5],[7].

가. 위협 분석 및 정보보호의 필요성

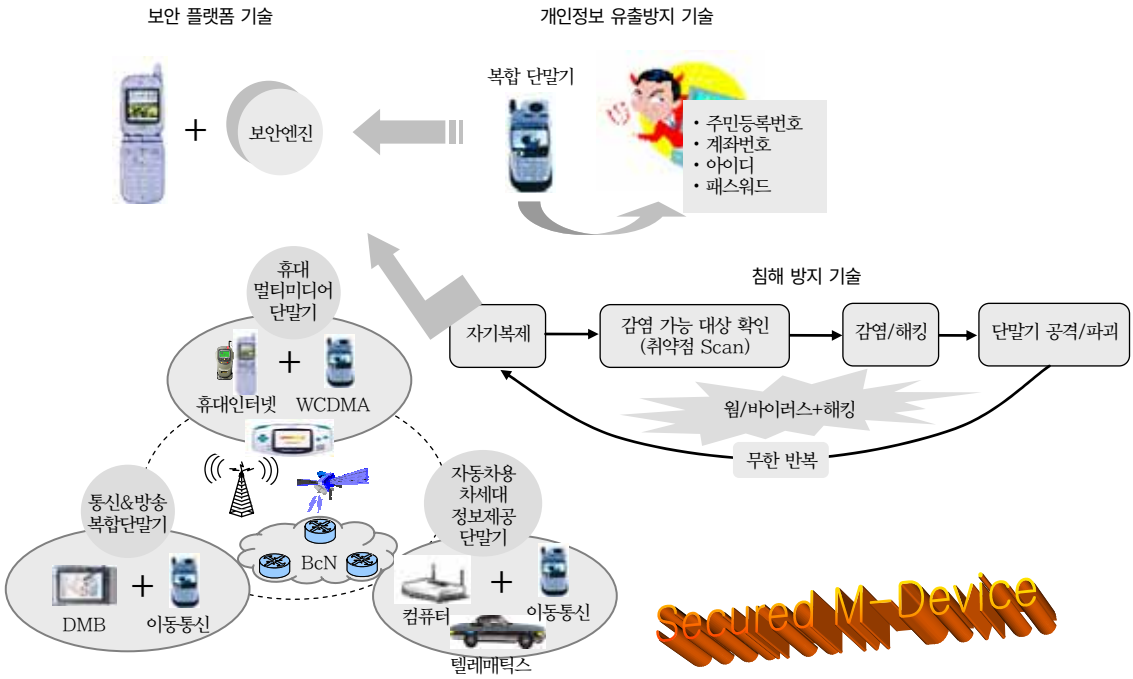
유·무선 통신망, 방송망, 인터넷 등 사이버 인프라 통합 환경 출현에 따른 신규 IT 융합형 서비스가 증대되고, 이러한 다양한 신규 융합 서비스를 지원하기 위해서 이동통신 및 휴대단말기로의 적용이 확산되어, 멀티미디어를 지향하는 복합단말기들이 출현하고 있으므로, 안전한 단말기 보안 플랫폼 기술 개발이 필요하다.

복합단말기들이 데스크톱 PC에 맞먹는 성능으로 진화하고 있으며, 바이러스나 웜 등이 휴대폰과 PDA 등 복합단말기들을 통해 네트워크와 24시간 서로 그물처럼 연결되어 있는 융합 환경으로 단숨에 확산될 수 있는 위협이 존재하고 있다. 따라서, 모바일 웜·바이러스 형태의 새로운 위협으로부터 복합단말기에 대한 침해 방지 기술이 필요하다. 모바일 웜·바이러스의 실례로는, 2004년 6월 GSM 방식 휴대폰의 카비르 웜 등장, 2004년 8월 마이크로소프트(MS)의 휴대용 개인단말기(PDA) '포켓 PC'의 취약점을 공격하는 '더츠'라는 신종 웜·바이러스가 등장했다.

통신·방송의 융합형 복합단말기를 통한 M-Commerce, T-Commerce의 전자거래가 크게 증대될 것이며, 이는 다양한 기기 간 통신이 가능한 인터페이스를 제공하기 때문에 불법적인 접근에 의한 개인 정보 유출의 위협이 존재하므로, 이를 위한 복합단말기용 개인 정보 유출 방지 기술이 필요하다. 개인 정보 유출 사례로는, 2004년 2월 노키아, 소니, 에릭슨의 블루투스 휴대폰 기종에서 공공장소에서 단말기의 블루투스 스위치를 켜놓을 시 개인 정보 유출 피해 가능성에 대한 보고가 있었다.

나. 복합단말기 통합 정보보호 기술

유비쿼터스 IT 서비스에서의 이러한 보안위협 방지를 위한 복합단말기 통합 정보보호 기술은 WiBro(휴대인터넷), DMB, 텔레매틱스 서비스를 위한 사용자와 기기간 인증기술 및 인증되지 않은 휴대단말기에의 불법접근제어 및 개인정보 유출방지를 위한 보안 컴포넌트 기술, 신규 IT 서비스에 적합한 복합단말기 안전성 보장 기술, 이종 무선 통신망(3G/PWLAN/휴대인터넷)간 USIM/PKI 기반의 상호보안 연계 서비스를 위한 보안 플랫폼 기술이 필요하며, (그림 4)는 유비쿼터스 IT 복합단



(그림 4) 유비쿼터스 IT 복합단말기를 위한 정보보호 기술 개념도

말기를 위한 정보보호 기술에 대한 개념도이다.

이러한 복합단말기와 정보보호 기술의 접목으로 보다 안전하고 신뢰하는 고품질 복합단말기의 상품화를 토대로 국내 산업기반 구조개선, 초경량 정보보호 기술 개발에 따른 정보보호 산업 육성, 고용창출과 수출증대의 경제적 효과가 기대된다.

또한, 안전한 통신·방송 융합형 복합단말기를 이용하여 언제 어디서나, 안전하고 신뢰하는 IT 서비스의 보급화와 고속 인터넷 활용이 증대됨에 따라 사이버 공간이 제2의 생활 공간으로 자리잡게 될 것이고, 각종 전자거래 등의 확대로 복합적인 멀티미디어 서비스 이용이 증대될 것으로 기대된다.

4. 안전한 사용자 서비스 제공을 위한 보안 위임서비스 기술

유비쿼터스 코리아 기본전략에서 ‘security’의 중요한 역할은 개인의 사생활 문제와 지역 간·계층 간 정보격차 문제의 해소를 통한 정보화 역기능 방지가 주요한 내용이다. 이것을 충족해 줄 수 있는 ‘Security Belt’ 정보보호 전략이 바로 안전한 사용자 서비스 제공을 위한 사이버실명제 기반의 보안 위임 서비스 기술이다. 즉, 모든 사람들이 쉽고, 안전하게 유비쿼터스 IT 서비스를 받도록 할 수 있는 기술 및 제도이다.

가. 위협 분석 및 정보보호의 필요성

최근 보안 위협들을 분석해 보면 보안 취약점이 발견되고 해당 패치가 공표되는 기간이 단축되고 있으며, 해커들의 reverse engineering을 통한 공격 발생의 가속화로 인하여 적극적 대응이 어려운 현실이다. 이러한 보안위협의 기본적인 이유는 인터넷이 사용자에 대한 익명성을 지원하기 때문이며, 이러한 문제 때문에 향후 유비쿼터스 IT 서비스 환경에 대한 전망이 그리 밝지 못하다. 이것을 해결하는 기본은 바로 서비스 사용의 익명성과 서비스 관리의 실명성 제공이며, 이를 사용자의 편리성과 안전성 측면을 고려하여 사용자 정보관리 사업자 또는

대리인을 이용하는 보안 위임 서비스 기술 및 제도가 필요하다.

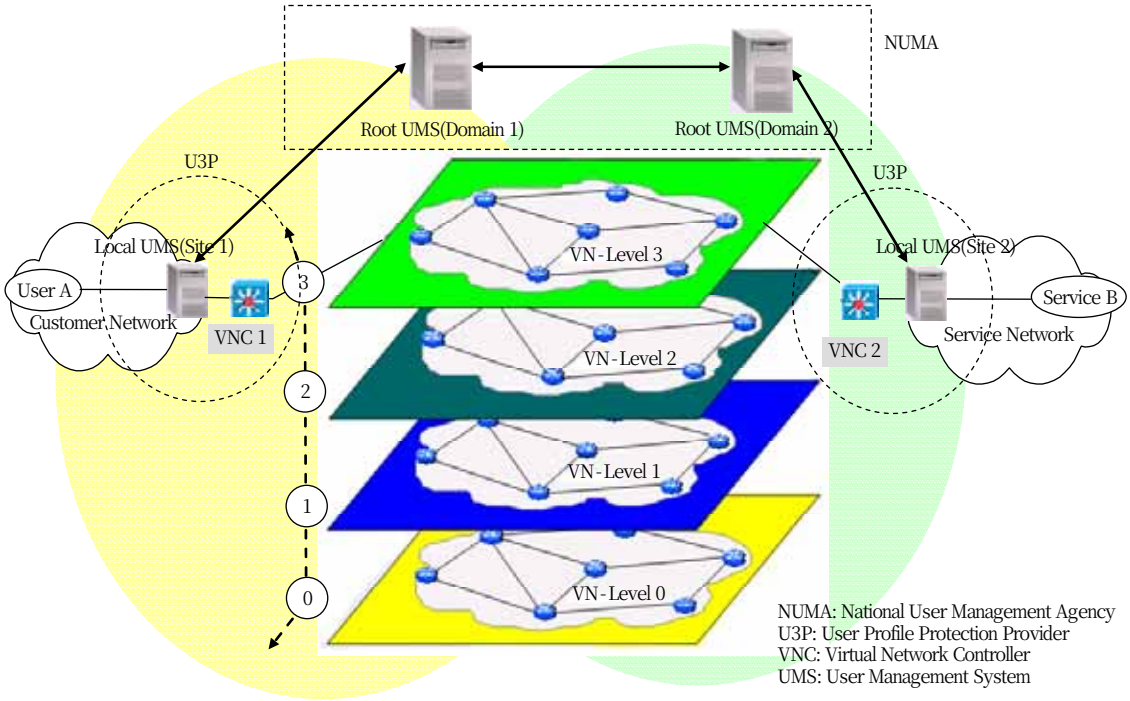
나. 보안위임서비스 기술

안전한 사용자 서비스 제공을 위한 서비스 사용의 익명성과 서비스 관리의 실명성이 제공되는 보안위임서비스 기술은 인터넷의 익명성의 근본적인 문제점을 해결하고, 개인 사생활 보호 및 지역 간、계층 간의 정보격차 문제를 한꺼번에 해결할 수 있는 기술이다.

이것은 현재 인터넷의 보안 취약성을 극복하기 위한 사용자 중심의 QoS 보장형 보안 프레임워크인 GUMF와 GUMF를 구현하기 위한 UMS, VNC 등의 시스템 기술이 필요하며, 이를 운영하기 위한 U3P 서비스 사업자와 국가적 차원의 사용자 관리국인 NUMA가 필요하다. 또한, 현재의 전자서명법의 개정 및 신규 법제의 제안 등의 관련 법제 정비가 필수적으로 수행되어야 한다. 이에 대한 상세한 개념도를 (그림 5)에서 표현하였다.

이러한 보안위임서비스 기술의 실현을 통하여 개인정보를 안전하고 효율적으로 관리함으로써 정보화 역기능을 최소화하여 안전한 u-Korea 실현이 가능하고, 안전한 사이버 환경을 통한 세계적으로 기업하기 가장 좋은 환경 실현이 가능하여 국가 신임도 및 시장 경쟁력 강화의 계기가 될 것이다. 또한, 현재 ISP와 NSP 사업자의 새로운 이윤 창출 아이템이 없는 현실에서 U3P 서비스 사업자 모델은 기업 및 국가, 그리고 국민 모두에게 수익 모델이 될 수 있으며, 개인은 안전하게 사이버상의 활동을 할 수 있을 것이다.

이를 경제적인 가치로 환산해 보면, BcN이 현실화되는 2010년에는 2천만 명(유무선가입자)×월 1만 원×12개월(2.4조 원)의 수익을 올릴 수 있는 모델로 분석될 수 있다. 이외에 국가 신용도 증대로 인한 투자 유치 증대는 부가적이지만 매우 중요한 효과로 기대된다.



(그림 5) GUMF를 이용한 사이버실명제 기반 보안위임서비스 개념도

Ⅲ. IT839 정보보호 중장기 기술 계획 vs.u-Korea “Security Belt”

안전한 IT839 전략을 위한 정보보호 기술 대책으로 발표한 정보보호 중장기 기술개발 계획(안)에 따르면, 정보통신인프라 보호기술, IT 디바이스 보호기술, 정보보호 기반기술로 구분되어 있다[4], [5]. 이는 IT839 전략 관점에서 분류한 기준이며, u-Korea 기본 전략의 정보화 역기능 해소 방안을 전체적으로 반영하지 못하였다. 즉, 사용자 측면의 보안 서비스 관점의 기술이 언급되지 않았다. 따라서, 본 고에서 제안한 보안위임서비스 기술 개발은 향후 정보보호 중장기 기술 개발 계획에 반영되어야 할 것이다. 따라서 다음과 같이 기술 개발 분류 기준을 제안한다.

- 정보보호 기반 핵심기술

  구현기술 분야에 공통적으로 적용되는 암호, 인증, 보안 프로토콜 기술 분야

- 정보통신 인프라 보호기술

  유비쿼터스 시대 핵심 인프라인 BcN, IPv6, USN 네트워크 보호 분야

- 복합 단말 보호기술

  WiBro, DMB 등 복합단말기를 위한 인증、인가 기술

- 응용 서비스 보호기술

  8대 주요 서비스 및 기타 응용서비스에 대한 서비스 안전성 제공 기술

- 사용자 서비스 보호기술

  보안위임서비스와 같은 사용자 중심의 보안 서비스 기술

미래의 보안(security)은 공급자를 위한 것이 아니라 사용자를 위한 서비스가 될 것이며, 개인의 안전한 삶을 영유하기 위한 생활 필수품이 될 것이다. 본 고에서 제안한 안전한 u-Korea를 위한 “Security Belt” 정보화 역기능 방지대책은 공급자 및 사용자 서비스를 모두 고려한 기술이다.

Ⅳ. 결론

본 고에서는 안전한 유비쿼터스 코리아(u-Korea) 실현을 위해서 BcN 인프라 보호 기술, RFID/USN 개인 프라이버시 보호 기술, WiBro 및 DMB 등에서 사용되는 복합단말기용 통합 인증 、인가 기술, 안전한 사용자 서비스 제공을 위한 서비스 사용의 익명성과 서비스 관리의 실명성이 제공되는 보안위임서비스 기술 등으로 형성되는 “Security Belt” 정보화 역기능 방지 대책을 제안하였다.

‘Security Belt’ 정보보호 기술은 안전한 u-Korea 실현의 중요한 역할을 수행할 것으로 기대되며, 안전한 유비쿼터스 서비스 환경을 제공함과 동시에 사이버 상에서의 안전한 경제 활동이 가능함으로 인하여 국가 신용도 증대 및 투자 유치 확대의 시너지 효과도 창출할 것으로 예상된다. 또한, 국민소득 2만 불 시대의 가속화 및 정보 강국의 위상 향상 등의 부가적인 효과도 기대된다.

약어 정리

BcN	Broadband convergence Network
DMB	Digital Multimedia Broadcasting
GUMF	Global User Management Framework
ODS	Object Discovery Service
OIS	Object Information Service
ONS	Object Naming Service
OTS	Object Tracking Service
PKI	Public Key Infrastructure
QSS	Quality of Security Service
RFID	Radio Frequency Identification
UMS	User Management System
USIM	Universal Subscriber Identify Module

USN Ubiquitous Sensor Network
Wibro Wireless Broadband Internet

참 고 문 헌

[1] 전자신문, u-Korea 관련기사, 2005. 1. 17일자(1면, 5면)
[2] 정보보호뉴스, u-Korea 추진전략과 정보보호, 2005년 1월호, http://www.kisa.or.kr
[3] IT 집중 육성 품목 자료 DB, http://library.etri.re.kr
[4] 정통부, 정보보호 중장기 기본전략 보고서, 2005. 1.
[5] 정통부, 정보보호 중장기 실무협의회 보고서, 2004. 12.
[6] TTA 저널 제95호, RFID/USN 정보보호 기술, http:// www.tta.or.kr
[7] Gartner Symposium ITXPO 2004, The Future of Information Security & The Future of Network Security & Evolution of Security Architecture, http://www3.gartner.com