주 제

IT839 정보보호 표준화 현황과 전망

ETRI 서동일

차례

요 약

최근 정보통신부에서는 IT839 전략 추진을 통하여 국민소득 2만불 시대를 견인하고자 노력하고 있다. 이러한 IT839 전략을 성공적으로 추진하기 위해서는 모든 분야에 공통적으로 필요로 하는 정보보호 기술의 성공적인 개발이 절대적으로 필요할 것으로 판단된다. 이는 IT839 전략 추진시 정보보호 측면의 기술과 개인의 정보를 활용하는 기술이 가장 기초적인 분야를 담당하고 있기 때문이다. 따라서 본 기고문에서는 현재까지 나타나고 있는 IT839 정보보호 요구사항 및 표준화 현황과 전망을 살펴보고자 한다.

I. 서 론

최근 정보통신부에서는 BcN(Broadband Convergence Network), IPv6, USN(Ubiquitous Sensor Network) 이라는 3대 인프라를 중심으로 하여 휴대인터넷, 홈네트워크, 텔레매틱스, 인터넷전화, DMB 등과 같은 8대 신규 서비스를 제공하고, 이를 기반으로 하여 9대 신성장 동력 산업을 활성화시켜 국민소득 2만불 시대를 견인하고자 IT839 전략을 야심차게 추진하고 있다.

더욱이 21세기 지식정보화 사회의 기반은 '컨버전스(Convergence)' 와 ' 유비쿼터스 (Ubiquitous)' 를 충족시키는 광대역통합망(BcN, Broadband Convergence Network)을 중심으로 구축될 것이며, 이러한 광대역통합망은 IPv6 체계를 기반으로 단계적으로 유 · 무선 통신망, 방송망, 인터넷 망과 최종적으로 USN(Ubiquitous Sensor Network)이 All-IP 망으로 통합되는 개념이라고 할 수 있을 것이다. 국내에서는 국가적인 차원에서 이러한 미래 유비쿼터스 환경을 구축하기 위한 노력을 기울이고 있으며, 대표적으로 정보통신부의 IT839전략 추진을 들 수 있을 것이다.

IT839전략의 8대 서비스는 휴대인터넷(WiBro), DMB(Digital Multimedia Broadcasting), 홈네트워크, 텔레매틱스(Telematics), RFID(Radio Frequency IDentification), W-CDMA (Wide-band ode division Multiple Access), 지상파 DTV(Digital TeleVision), 인터넷 전화를 의미한다. 3대 인프라는 앞서 본바와 같은 BcN, IPv6, USN을 의미한다. 9대 신성장동력 산업은 차세대 이동통신, 디지털 TV, 홈 네트워크, IT SoC (System-on-Chip), 차세대 PC, 임베디드 소프트웨어, 디지털 컨텐츠, 텔레매틱스, 지능형 로봇 분야이다[1,2,9].

그러나, 이러한 IT839 전략이 성공적으로 수행되기 위해서는 그 기반이 되는 정보보호 기술의 완성이 필수적으로 요구되고 있다. 이는 모든 개인의 정보들이 IT839 전략 전 분야에 걸쳐서 적극적 혹은 중요한 자원으로 사용되고 있기 때문에 이러한 정보들을 안전하게 보호할 수 있는 대책이 필요하기 때문이다. 따라서, IT839 전략이 추진됨에 따라 발생될 수 있는 사이버 역기능은 매우 광범위하게 나타나게 될 것으로 예측된다.

본 기고문에서는 이러한 IT839 전략 추진을 위한 정보보호 기술의 표준화에 대해서 알아보고자 한다. 제II장에서는 IT839에서의 정보보호 요구사항을 알아본다. 제III장에서는 IT839 전략분야에서의 정보보호 표준화 현황을 분석하고, 마지막으로 결론을 맺도록 한다.

II. IT839 정보보호 요구사항

1. 8대 서비스에서의 보안취약점 및 요구사항

IT 분야의 설비투자를 견인하는 서비스 보급 촉진을 위해 8대 서비스를 선정하여 정책적으로 육성하고, 이러한 서비스를 활성화시키는 정책을 추진중에 있다. 이러한 IT 839 전략에 따른 여러가지 서비스 제공에 대한 위협요소들을 살펴보자. 홈네트워크 서비스에서의 개인 자산에 대한 불법 제어 가능성이 매우 증대될 것이다. 홈네트워크 정보기기에 대한 불법적인 공격은 개인의 프라이버시 침해뿐 아니라 생명 및 재산까지 직접적인 피해를 줄 수 있어 보안 취약성에 대한 대응책 마련이 매우 시급한 실정이다. 텔레매틱스 서비스의 경우, 서비스 임시 사용자에 의한 불법 서비스 도용 및 프라이버시 침해 가능성이 존재하고 있다. 이를 통하여 텔레매틱스 서비스 장애를 유발시키거나 불법 사용에 의한 금전적 피해가 우려되는 상황이다. 또한, 휴대 단말기를 통한 웜 · 바이러스 공격, 불건전 정보의 유통등도 매우 커다란 위협요인으로 대두될 것이다. 디지털 컨텐츠의 불법 복제와 유통 문제도 매우 심각한 역기능 현상이며, 특히 BcN을 통하여 여러 개별망이 통합된 환경에서는 이러한 지적재산권 침해나 유통 문제가 더욱 더 손쉽게 발생될 가능성이 매우 높아질 것이다. 이를 요약하면 〈표 1〉과 같다.

2. 3대 인프라에서의 보안 취약점 및 요구사항

통신 · 방송 · 인터넷을 동시에 수용하는 미래 기간 인프라인 광대역통합망(BcN)과 최근 유비쿼터스 혁명의 총아로 각광 받고 있는 USN, 인터넷 도메인 수를 거의 무한대로 늘릴 수 있는 IPv6 등을 3대 인프라로 정의하여 이의 구축을 본격적으로 추진하고 있다. 이러한 3대 인프라에서의 보안 취약점 및 요구사항을 정리하면 〈표 2〉과 같다.

IT839전략의 기본 인프라는 IPv6를 기반으로 한 광대역통합망(BcN)이며, 최종적으로는 USN까지 확대 적용될 것이다. 이러한 BcN 에서의 향후 위협요소를 별도로 상세히 알아 보면 아래와 같다.

〈표 1〉 8대 서비스에서의 보안취약점 및 요구사항

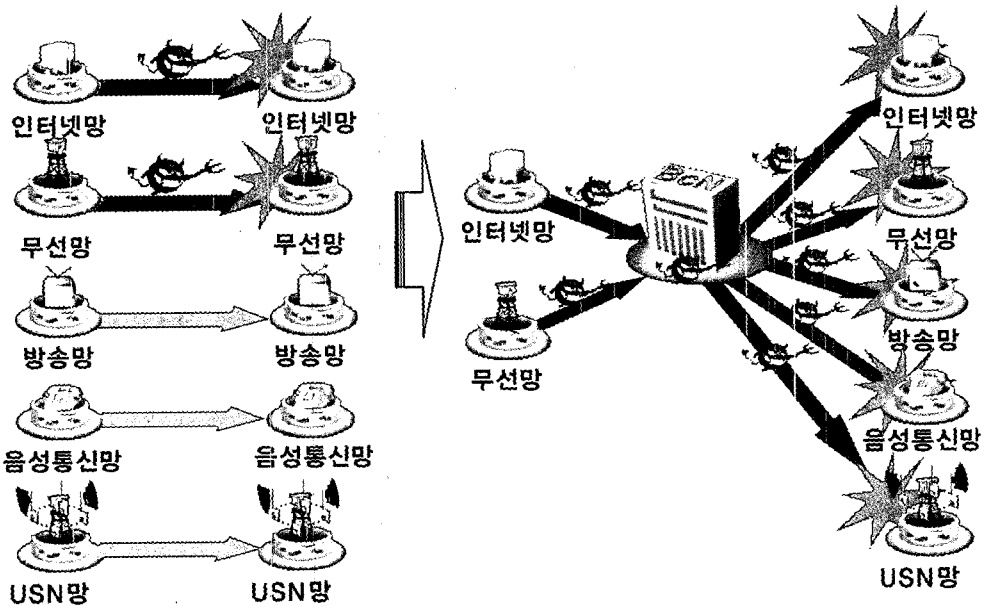
분류	주요 보안취약점 및 보안요구사항
2.3GHz 휴대인터넷	- 휴대인터넷용 단말기 보안 및 인증 기술이 필요 - 고속의 휴대인터넷 컨텐츠 보호기술이 필요 - 휴대인터넷에서의 통합 인증, 권한 검증, 과금 기술이 필요 - 무선 구간에서 발생하는 도청, 변조, 삽입, 삭제 등의 침해 위협 - 휴대 단말기를 통한 웜/바이러스 공격 - 불건전 정보의 유통 - 디지털 컨텐츠의 불법 복제와 유통 - 개인정보보호 및 프라이버시 보장
위성/지상파 DMB	- 전송 매체에서 나타날 수 있는 도청, 변조 등의 위협 - 고품질화를 위해서 보안기술을 접목한 secure DMB 단말기, Secure DMB 게이트웨이, 서비스 서버 보안기술 개발이 필요 - 청소년에게 유해정보 유출이 되지 않도록 내용기반 자동등급 분류 기술 개발이 필요 - 허용된 방송 시청자만 수신하도록 하는 제한 수신 기술 필요
홈네트워크	- 홈 디바이스에 대한 불법제어 - 유무선 도청 가능으로 인한 사용자 프라이버시 정보침해에 취약 - Rouge Middleware로 인한 정보 유출의 취약 - 홈네트워크 시스템 및 단말 해킹, 바이러스 공격, - 내부 불법침입, 콘텐츠 위변조, 정보유출, 프라이버시 침해
전파식별 (RFID)	- 제3자의 타인 정보 유출 위협 - 개인 정보보호 침해 및 신용 정보 해킹 - 정보의 위변조 용이성 - 불법적인 리더기 사용 W-CDMA - 복제 단말기에 의한 서비스 도용 - 무선 링크에 대한 도청 - W-CDMA 단말기에 대한 통합 인증, 권한 검증, 과금 기술이 필요 - 고속 이동에 따른 멀티미디어 정보 훼손에 대한 보증기술이 필요 - 개인정보보호와 프라이버시 침해 텔레매틱스 - 위치정보에 대한 프라이버시 보호기술 개발 필요 - 상황 식별및 인증 기술 개발이 필요 - 불법적인 서비스 도용 - 서비스 장애 유발 공격 지상파 DTV - 방송통신망 연동 기술 및 지능형 방송 서비스 기술 개발 필요 - 유통 컨텐츠 보호를 위한 사용자, 기기 인증 기술 개발 필요 - 유료 서비스의 불법 사용 - 방송 컨텐츠 지적재산 보호 - PSTN과는 달리 체계적인 보안 관리가 어려움
인터넷전화 (VoIP)	- 트래픽 폭주로 인한 데이터 손실과 적체현상, 인터넷 전화의 음질 저하 및 불통 등의 문제점 - 불법적인 서비스 도용 - 사용자의 위치 정보 침해 (개인 프라이버시 침해)

〈표 2〉 3대 인프라에서의 보안취약점 및 요구사항

분류	주요 보안취약점 및 보안요구사항
BcN	- 단위 네트워크에서의 위협이 BcN 전체 네트워크로 확산될 수 있음 - IPv4/IPv6 혼합망에서의 취약점 - 개인 정보보호 및 프라이버시 침해 - ISP망의 Ingress Point에서 네트워크 위협을 능동적으로 탐지하고 대응할 수 있는 통합 보안 관리 기술이 필요 - ISP망의 발전속도를 고려한 고성능 네트워크 위협 대응 기술이 필요 - 알려진 침입공격에 대한 탐지 기술과 알려지지 않은 침입에 의한 과다 트래픽 탐지 기술이 필요 - 유해트래픽에 대한 차단 및 대역폭 제어 기술이 필요
IPv6	- IPv4/IPv6 변환용 네트워크 노드에 대한 보안 기술이 필요 - IPv6 프로토콜 자체에 대한 옵션 처리 미적용으로 인한 공격을 방지할 수 있는 보안 게이트웨이 기술이 필요 - Mobile IPv6용 인증/인가/접근제어 기술이 필요
USN	- 악의적인 공격자가 태그의 정보를 얻고자 시도하는 공격을 막는 인증 기술이 필요 - 정상적인 Reader와 Tag 사이의 데이터를 공격자가 엿듣는 경우를 방어하는 도청 방지 기술이 필요 - 공격자가 정상적인 데이터를 위조하는 Reader 또는 Tag를 혼란시키는 공격을 방어하는 데이터 기밀성과 무결성 보장 기술이 필요 - DoS Tolerant RFID/USN 네트워킹 기술, RFID/USN 네트워크 노드 간의 상호 인증 기술이 필요 - 센서 신호의 Jamming 회피 기술이 필요 - 개인정보보호 및 프라이버시 침해

첫째는, 개별 통신망에서의 위협이 전체 BcN 통신망으로 확산되기 쉬워진다는 점이다.따라서, 현재의 네트워크 보안은 소규모 네트워크 차원에서 단순 모니터링 및 보안 정책을 적용하는 형태이나, 향후의 BcN 네트워크 보안은 네트워크 전체를 보안 관리 영역으로 확장할 필요가 있을 것이다. 이는 BcN 구성요소 개개의 보안성을 고려하기 보다는 체계성을 갖추어 통합 관리함으로써, 신속한 대응환경을 구성하는 것이 필요하기 때문이다.

상기와 같은 광대역 차원의 네트워크 침입 대응이 필요한 결정적인 이유는 BcN의 구성이 여러가지 기존의 네트워크들이 통합되어 있다는 점에 기인한다. 즉, (그림 1)과 같이 사이버 공격에 취약한 기존의 인터넷 망에서 발생된 위협이 BcN을 통하여 각각의 개별망으로 확산되어 음성통신망, 방송망, USN까지 그 피해가 확산될 것이기 때문이다. 다시 말해서 음성통신방식이 VoIP 기술등을 이용하여 기존의 회선교환망에서 유 · 무선 인터넷 망으로 전환되는 경우 음성통신도 기존의 인터넷과 동일하게 웜, 바이러스



(그림 1) BcN 에서의 사이버 위협 확산

등 사이버 공격에 노출되는 것이다. 또한, BcN은 개방형 망구조(Open API)를 이용하여 다양한 서비스를 창출하고 이를 다양한 경로로 사용자에게 서비스하는 것이 가능한데 이는 곧 해킹과 웜 · 바이러스 유포 확대에도 사용될 소지가 매우 높기 때문이다.

지금까지 살펴본 대표적인 BcN 에서의 새로운 사이버 위협을 포함하여 BcN 각 계층별 취약점을 예측하여 보면 (표 3)과 같다.

두번째, BcN 위협 요소는 BcN이 기본적으로 IPv6를 기반으로 할 것이기 때문에 발생되는 문제이다. 즉, IPv6 기능의 취약점을 이용한 새로운 형태의 공격이 발생될 가능성이 상존한다. 기존의 인터넷은 IPv4를 기반으로 하고 있으며, 이때 발생되었던 여러가지 사이버

〈표 3〉 BcN 에서의 각 계층별 취약점 예측

계 층	주요 취약점 이슈	비 고
서비스 계층	- 서비스 계층으로의 접근 인증 및 권한문제 - Open API 제공 문제 - 서비스 사용자의 개인정보보호 문제 - 불건전 정보 및 반사회적 정보의 유통문제 - 지적 재산권 보호 문제	
제어 계층	- 서비스 게이트웨이 신뢰성 보장문제 - 소프트스위치의 신뢰성 보장 문제 - 관리 · 제어 정보의 보호 문제	
전달 계층	- 전달망 측면에서의 서비스 품질 보장 문제 - BcN 생존성 보장 문제 - 이종망간 상호 연동시 정보보호 문제	- 유선 · 무선 통합 - 통신 · 방송 융합
접속 계층	- 망 통합으로 인한 취약성 확산 방지 문제 - 악의적 공격의 위치 다양화 및 역추적 문제 - 비인가자 접속 차단 문제 - 도청, 데이터 위변조등의 문제	- 각 개별망 접속
단말 계층	- 홈 게이트웨이 안전성 보장 문제 - 가입자 망접속 장비의 정보보호 취약성 문제 - 이동성 보장에 따른 공격자 역추적 난이성 문제 - 위장 단말기 탐지 문제	- 홈네트워크 - USN 센서

공격 형태를 포함하여 새롭게 IPv6에 신규로 추가된 자동환경설정 기능이나 근접노드 탐색기능, 이동 IP 등의 기능은 기존 공격 형태와는 다르게 변형된 새로운 공격이 발생될 소지가 매우 높은 것이다. 또한, 완전한 IPv6 전환 이전에 과도기적으로 IPv4와 IPv6를 병행하여 사용해야 하므로 종단대종단(end-to-end) 네트워크 차원의 정보보호가 매우 어렵게 될 소지가 높을 것이다.

세번째, BcN 위협 요소는 최종적으로 BcN과 연결될 것으로 예측되는 USN 에서의 취약점이다. USN에서는 이동단말이나 센서와 같은 장비들에서 사용되는 CPU, 배터리의 용량이 매우 적기 때문에 이러한 자원들에 대한 집중적인 공격으로 보유 자원을 급격히 소모시키는 공격을 받을 경우 일반 사용자들은 전체 서비스가 중단될 위협에 노출될 수가 있을 것이다. 또한, USN 무선망의 경우에는 중앙 집중형 보안 기능이 상대적으로 취약한 Ad-hoc 네트워크 구조를 취하고 있으므로 이동형 단말기기에 대한 통제가 어려워 사이버 공격에 대해 취약성이 상당 부분 증대될 것으로 보인다.

USN 에서의 또 다른 위협 요소로는 개인정보보호 문제와 프라이버시 침해 위험이 매우 높아진다는 점을 들 수 있다. 즉, USN에서는 도처에 설치된 센서를 통하여 사용자의 위치 정보라든지 여러가지 서비스 이용정보들을 수집하고 있으므로, 이렇게 수집된 정보가 오 · 남용될 경우 이용자에 대한 24시간 감시 시스템 역할을 할 수가 있게 되어 개인의 사생활 침해 문제가 매우 심각해 질 것으로 보인다.

3. 9대 신성장동력에서의 보안 취약점 및 요구사항

국내외 시장성, 기술, 국내 역량 등을 고려하여 국내외적인 경쟁력이 있고, 고성장이 예상되는 분야를 9대 신성장 동력으로 선정하여 중점 육성하고자 추진하고 있다. 이러한 9대 신성장 동력에서의 보안 취약점 및 요구사항은 〈표 4〉와 같다.

〈표 4〉 9대 신성장동력에서의 보안취약점 및 요구사항

분류	주요 보안취약점 및 보안요구사항
차세대 이동통신	- 초고속 무선 LAN 및 2.3 GHz 휴대 인터넷의 전송 기술, 무선망 보호 및 이동성 보안 기술의 개발이 필요 - W-CDMA에서의 IPv6 적용을 통한보안 기술 개발이 필요 - 불법 단말기에 의한 서비스 도용, 불법 도청 - 이동기기에 대한 원공격 및 스팸 공격 - 단말기 불법 복제
DTV	- 방송통신망 연동 기술 및 지능형 방송 서비스 기술 - 유통 컨텐츠 보호 위한 사용자, 기기 인증 기술 개발 필요 - 불법 사용자에 의한 서비스 도용
홈 네트워크	- 사용자 및 정보 가전기기의 인증기술 - 데이터 유출 및 위 · 변조 방지 기술 - 침입방지 보안기술 개발 필요
IT SoC	- 사용자 식별, 생체인식, 고비도 암호처리와 같이 많은 연산 처리, 하드웨어 안전성 활용 등의 security 기술을 효과적으로 점목하기 위한 보안 SoC 개발이 필요 - 경량화된 보안 기능
차세대 PC	- 오감 센싱을 통한 사용자 인증 생체인식 처리 기술 및 생체정보 보호/위변조 탐지 기술 개발이 필요 - 차세대 PC 자체의 보호기술 - 개인 프라이버시 침해
임베디드 S/W	- Secure OS 기술 및 사용자 단말 인식 기술 개발이 필요 - 경량화된 정보보호 기술개발이 필요(안전한 운용체제 기술)
디지털 콘텐츠	- 불법 유통 추적 및 콘텐츠 내용제어 기술 개발이 필요 - 디지털 지적재산권 보호 기술 필요 - 유료 컨텐츠 과금 및 지불 방법
텔레매틱스	- 위치정보에 대한 프라이버시 보호기술 필요 - 상황 식별 및 인증 기술 개발이 필요 - 사이버 공격에 의한 서비스 장애 - 불법적인 서비스 도용
지능형 로봇	- 적법한 사용자의 명령을 인증하고 처리정보의 비밀성과 무결성 보장을 위한 정보보호 기술 개발이 필요 - 개인정보보호 보호

III. IT839 정보보호 표준화 현황

1. 8대 서비스

8대 서비스는 휴대인터넷(WiBro), DMB, 홈네트워크, 텔레매틱스, RFID, W-CDMA, 지상파 DTV,

인터넷 전화 등을 의미한다.

RFID 기술은 판독기를 통하여 직접적인 접촉 없이 Air Interface 기술로서 태그의 정보를 판독하거나 기록하는 무선 주파수 인식기술로서 리더와 태그 기술을 포함하는 하드웨어 기술과 소프트웨어를 포함하는 미들웨어 기술을 요소기술로 갖는다[3,6].

RFID 기술에서는 정보보호를 위해 RFID 태그와 센서 노드들로부터 적절한 정보를 주고 받는 기술이 필요하다. 이용자의 권리 이상의 정보 제공을 제한하고 문제가 있는 정보의 유입을 막기 위해 인증과 보안에 관한 기술이 연구되고 있다. 최근에는 RFID 프라이버시보호 가이드라인 표준이 TTA를 중심으로 하여 제정되고 있다. RFID 자체에 대한 여러 규격들은 ISO/IEC JTC1 SC31과 SC17을 중심으로 제정되고 있다. 이외에도 EPCglobal, uID센터(Ubiquitous ID Center)등이 있다[6].

디지털 방송 서비스는 기존의 아날로그 방송을 통해 서비스되고 있는 비디오나 오디오를 디지털로 바꿈으로써 고선명 영상과 고품질 음향의 방송 콘텐츠를 언제, 어디서나, 사용자가 원하는 형태로 선택하여 시청할 수 있도록 하는 다양한 형태의 부가 서비스를 제공하는 방송 서비스이다. 디지털 위성 방송, 지상파 디지털 방송, 디지털 유선 방송 형태로 디지털 데이터 방송 서비스, 디지털 맞춤형 서비스, 방송/통신 융합 서비스 등을 제공한다. 또한, DMB 기술이란 고품질의 음향/영상/데이터를 고정 및 이동/휴대 환경에서 수신하는 단방향 서비스와 통신망과의 연동을 통한 양방향 서비스를 통칭하는 이동멀티미디어방송 기술을 의미한다[3].

국내에서는 TTA PG308과 차세대방송표준포럼에서 TV Anytime 분과위원회를 구성하여 맞춤형 방송을 위한 국내표준 초안을 제정하였고, 규격작업과 정합 시험을 진행하고 있다. 맞춤형 디지털방송으로 방송 · 통신 융합 서비스를 위한 기술개발과 이를 위한 표준 활동이 전개되고 있다. 디지털 컨버전스에 대비한 차세대 통신 네트워크에서 방송 · 통신 융합 서비스를 제공하려는 방안이 연구 중에 있다. 정보보호와 관련하여서는 차세대방송표준포럼에서 DMB 제한수신을 위한 CAS 관련 표준을 작업중에 있다.

텔레매틱스는 자동차에 정보단말기(이동통신) 및 위치추적시스템(GPS)을 탑재하여, 자동차 사고 통보, 교통정보/길안내, 원격진단, 무선인터넷 등을 제공하는 자동차용 차세대 종합정보 서비스 사업이며, 컴퓨터 하드웨어 기술, 통신기술, ITS(Intelligent Transport Systems) 기술, GIS(Geographic Information System) 기술, LBS(Location Based Services) 기술 및 컨텐츠 관련기술 등 다양한 요소기술을 활용하는 요소기술 통합 프레임워크 표준 및 개방형 플랫폼 표준이다[3]. 텔레매틱스 분야에서의 정보보호는 아직까지 뚜렷한 움직임을 보여주고 있지 못한 현실이다. 단지, 위치기반서비스(LBS)는 통신망 또는 통신 설비 등을 이용하여 사람이나 사물의 위치를 파악하고, 이를 활용하는 응용시스템 및 서비스이므로, 이를 악용할 수 없도록 개인정보보호 측면에서의 가이드라인 제정을 추진하고 있다.

인터넷 전화는 VoIP 기술을 사용하며, 음성을 패킷으로 전달하여 통신하는 기술을 의미한다. VoIP 관련 정보보호 표준화는 별도로 진행되고 있지 않으며, 기존의 ITU-T, IETF 에서 제정된 VoIP 관련 표준 문서를 그대로 사용하고 있다. 그러나, 인터넷 전화는 개인의 프라이버시 보호 문제가 매우 중요한 관건이 될 것이므로 관련된 정보보호 표준화가 별도로 진행될 필요가 있을 것으로 보인다.

2. 3대 인프라

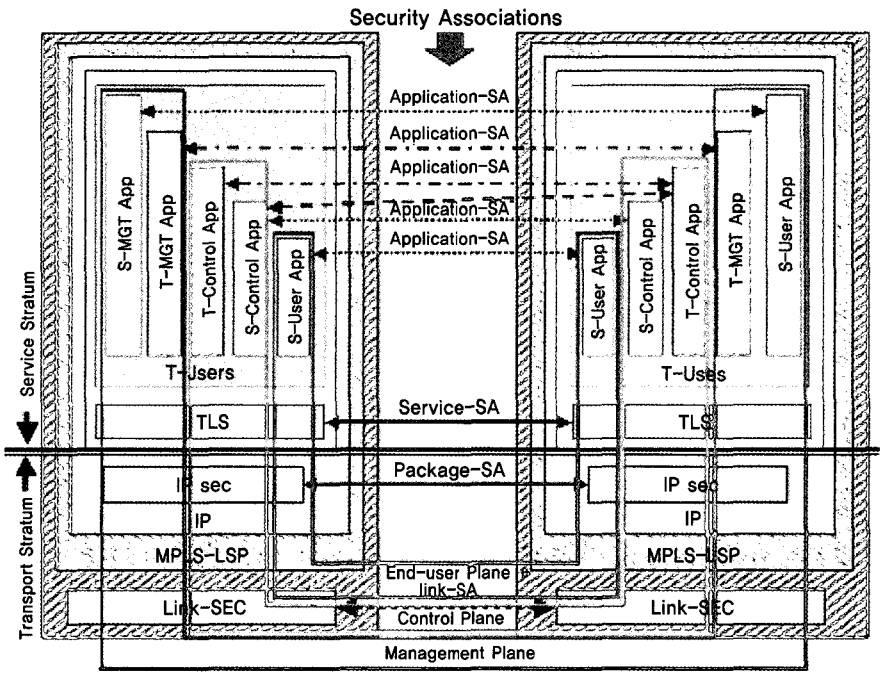
3대 인프라는 광대역통합망(BcN), USN, IPv6이며, 최근에는 IPv6를 BcN에 통합하고 대신에 소프트

웨어를 추가하여야 한다는 의견이 대두되고 있는 상황이다.

광대역 통합 네트워크(BcN)는 진보된 패킷 기반의 네트워크 기술을 활용하여 유선과 무선 통신망, 방송과 통신, 인터넷 등 모든 종류의 통신망을 통합 수용하는 기술로, 모든 서비스의 융합 및 고품질 서비스를 제공할 수 있는 통합 네트워크를 의미한다[3]. 이러한 광대역 통합 네트워크는 기본적으로 국제적인 정의에 따르는 차세대 네트워크(NGN, Next Generation Network) 기술인 패킷 기반의 통합 기술에 기반하고 있다. NGN 에서는 일반적으로 응용 서비스 계층과 통신망의 제어 계층, 그리고 전달망 계층이 분리되며, 각 계층이 독립적으로 단계적인 진화가 가능한 구조를 가지고, 이들 계층간에는 표준화된 개방형 인터페이스가 정의되어 사용된다.

BcN 환경에서의 위협 요소로는 앞장에서 살펴 보았듯이, 첫째, 여러가지 개별망이 통합되므로써 각 개별망에서의 위협이 전체 네트워크로 확산될 수 있다는 점과, 두번째, IPv6를 기반으로 하기 때문에 새롭게 발생될 수 있는 위협요소가 있다는 점, 세번째로는 USN 에서의 새로운 위협과 개인의 프라이버시 보장 문제 등이 크게 부각되고 있는 점이 있다.

이러한 위협요소들에 대해 현재 국내 TTA에서는 PG101 (정보보호기반), PG204 (NGN) 그룹이 연구하고 있으나, 구체적인 BcN 정보보호 표준화 노력이 부족한 실정이다. 또한, 정보통신부를 중심으로 하여 2005년 6월 BcN 표준전략 협의회가 구성되었으며, 이를 중심으로 하여 BcN 관련 국내 표준을 검토할 예정으로 있으며, 동 협의회 산하 실무분과로써 보안분야가 구성되어 있다.



(그림 2) NGN Security Model

ITU-T 에서는 그동안 NGN security 관련하여 FG-NGN WG5에서 기술문서 개발을 진행하였으며, BT, Lucent, ZTE, NEC등이 주로 참여 하였고, FGNGN의 WG2의 NGN 아키텍쳐(FRA)를 기반으로 보안 요구사항 및 가이드라인을 반영하고 있다. 현재까지 생성된 문서는 아래의 2가지가 있으며, 추후 좀더 보강한 다음 최종적으로는 SG17 security WP로 기고할 예정으로 있다.

- FGNGN-OD-00132(6th FGNGN, Stable): NGN security Requirements for Release 1
- FGNGN-OD-00173(7th FGNGN, Draft): Guidelines for NGN security

(그림 2)는 OD-173 문서에서 제시하고 있는 NGN Security Model 이다. 여기에서 보는 것처럼 NGN Security는 Management Plane, Control Plane, End-user Plane으로 나뉘어 있다. 이는 기존의 ITU-T X.805 권고안에서 제시하고 있는 보안평면과 동일하다. 그러나, 보안계층은 기존의 X.805에서 제시하고 있는 Infrastructure Security Layer, Service Security Layer, Application Security Layer와는 다르게, OD-173 에서는 Application Layer, Service Layer, Package Layer, Link Layer로 구분하고 있다. 이 외에 Security Dimension은 X.805에서 제시하고 있는 8개 항목을 그대로 수용하고 있다. 이들 항목은 access control, authentication, non-repudiation, data confidentiality, communication security, data integrity, availability, privacy를 의미한다[7].

ITU-T Q.15/13 on NGN Security 가 2005년 5월 신설 승인이 되었으며, 기존의 FGNGN WG5 활동을 이어받아 아래와 같은 추가적인 NGN security 표준화 작업을 진행할 예정으로 있다.

- NGN 보안프레임워크, NGN 구조, 기타 보안 이슈들
- NGN 환경에서 X.805 권고안을 적용하기 위한 연구
- NGN 환경에서 요구되는 Authentication, Authorization, and Accounting (AAA) 기술 개발

이외에 보안분야에서 ITU-T Lead Study Group은 SG17이며, WP2에서 주로 다루고 있다. 관련 Question으로는 Q4/17 (Communications Systems Security Project), Q5/17 (Security Architecture and Framework), Q6/17 (Cyber Security), Q7/17 (Security Management), Q8/17 (Telebiometrics), Q9/17 (Secure Communication Services), Q17/17 (proposed) (Countering SPAM)이 있으며, ITU-T 모든 SG 그룹은 보안과 관련된 자신들의 연구 활동 결과를 SG17로 연락하여야 한다. ITU-T SG16, Q25 (Multimedia Security in NGN)에서는 멀티미디어 NGN 보안 이슈들을 논의하고 있다.

USN(Ubiquitous Sensor Network)은 인간의 생활공간, 생활기기, 기계 등 모든 사물에 컴퓨팅 기능과 네트워크 기능을 부여하여, 환경과 상황의 자동인지를 통해 인간에게 최적의 기능을 스스로 창출 제공함으로서, 인간 생활의 편리성과 안전성을 고도화한다. 바코드나 RFID와 달리 사용자의 개입이 필요하지 않고, 센서 노드들 사이에서 능동적으로 정보의 교환이 이루어지는 장점이 있다[3].

USN을 기반으로 하는 유비쿼터스의 의미가 모든 사물의 통신을 뜻하고 이는 곧 모든 사물, 개인의 정보 또한 안전하지 못하다는 의미가 된다. 작은 리더기를 숨겨두고 이용하여 공개되기 원하지 않는 정보까지 유출이 가능하므로 이런 역기능을 방지하기위한 기본적인 암호, 인증 기법은 물론 외부의 공격에

대응하는 기술개발이 함께 진행 중이며, 개인 정보의 유출을 막기 위한 구조적인 문제 또한 해결해 나가고 있다. USN기반 PKI 기술, 키관리 기술, 보안 라우팅 기술 등 기반 정보보호기술과 디지털인증체계가 필요하다. 이외에도 USN 표준화 포럼을 통하여 USN 보안 및 RFID 보안 문제를 중점적으로 연구하고 있다. IPv6란 현재 사용하고 있는 IPv4의 32비트 주소체계를 확장하여, 민간국제표준화기구인 IETF (Internet Engineering Task Force)가 1996년에 표준화한 128비트 차세대인터넷 주소체계를 지칭한다[3]. 현재까지 IPv6 정보보호와 관련된 직접적인 표준화 동향은 보이고 있지 않으며, 관련된 기술개발이 진행되고 있다. 그러나, IPv6는 향후 유비쿼터스 시대의 기반망으로 구축될 광대역통합망(BcN)의 기반 기술로써 사용될 예정이므로 별도의 정보보호 표준화 작업이 필요할 것으로 판단된다.

3. 9대 신성장동력

9대 신성장동력 산업은 차세대이동통신, 디지털 TV, 홈 네트워크, IT SoC, 차세대 PC, 임베디드 S/W, 디지털 컨텐츠, 텔레매틱스, 지능형 로봇 분야를 의미한다.

차세대 이동통신 기술은 고속이동환경에서 최대 100Mbps, 고정 또는 저속이동 환경에서 최대 1Gbps의 데이터 전송속도로 비대칭/대칭적 패킷 서비스와 방송 서비스를 포함한 다양한 서비스를 IP 기반으로 통합 제공하는 기술을 의미하며, 셀룰러 이동통신 뿐만 아니라 다양한 무선통신 기술이 통합되는 형태로 실현될 것으로 예상하고 있다[3].

차세대 이동통신 분야에서의 정보보호는 소프트웨어 보안 및 인증기술이 필수적으로 필요하며, 이는 다운로드 프로토콜을 불법으로 사용하는 것을 방지하고 도청 및 간섭을 막기 위한 기술이다. 국내에서는 TTA를 중심으로 과제를 기획하고 있으며, 국제적으로는 SDRF(Software Defined Radio Forum)에서 표준화 작업을 진행하고 있다.

지능형 로봇 분야는 복합적인 하드웨어 기술로 구성된 로봇에 지능을 부여하여 인간과 상호작용을 통하여 인간의 명령 및 감정을 이해하고, 반응하며 정보통신 기술을 바탕으로 인간에게 다양한 서비스를 제공하는 기술이다. 이를 위해 기능실현과 지능 구현을 위한 소프트웨어 플랫폼, 네트워크 기능, 인간과의 커뮤니케니션 및 서비스, 보안/인증 등과 같이 네트워크 로봇 실현을 위한 기술이 필요하다.

현재까지 로봇분야에서의 정보보호는 구체적으로 표준화되고 있지 못한 실정이다. 미래 유비쿼터스 사회에서는 많은 인간친화형 로봇들이 인간과의 상호작용을 통하여 사용될 것으로 예측되고 있는 상황에서 이러한 정보보호에 대한 표준화 노력이 미흡하다는 것은 매우 위험한 상황으로 판단되며, 좀더 적극적인 정부의 관심이 필요한 부분이다.

홈네트워크 기술은 가정 내의 모든 정보가전기기가 유 · 무선 홈네트워크로 연결되어 누구나 기기, 시간, 장소에 구애받지 않고 다양한 홈디지털서비스를 제공받을 수 있는 미래지향적인 가정 환경을 제공함으로써 국민의 삶의 질을 향상시키고 국민의 정보수요 격차를 해소하기 위한 수단을 제공하는 기술로서, 액세스망과 홈네트워크를 연결하기 위한 홈서버 · 홈게이트웨이 기술, 사용자의 편의성 제공을 위한 미들웨어기술, 그리고 가정정보화 인프라 구축을 위한 유 · 무선 홈네트워크 기술 표준 등을 포함하고 있다[3].

홈 네트워크는 광대역통합망의 하부 구조로서 미래 유비쿼터스 사회에서는 매우 친숙한 환경이 될 것이다. 이러한 홈 네트워크는 가정의 모든 환경을 네트워크를 통하여 제어가 가능하다는 점에서 관련 정보를 보호해야 하는 것은 매우 중요한 문제이다. 현재까지 이러한 홈네트워크 정보보호는 인증 문제를

중심으로 TTA와 ITU-T SG17에서 표준화가 진행중에 있다[8].

임베디드 S/W 기술은 운영체제, GUI, 미들웨어, 멀티미디어, 개발도구 등 임베디드 시스템을 동작시키기 위한 임베디드 소프트웨어 플랫폼 전반을 포함한다[3]. 임베디드 소프트웨어 분야에서의 정보보호 표준화는 아직까지 뚜렷한 움직임이 없는 실정이다.

디지털콘텐츠는 특성상 무한히 반복하여 사용해도 품질의 저하가 발생하지 않고, 수정과 복사가 편리하며, 통신망을 통해 대용량의 콘텐츠를 짧은 시간에 전송과 배포가 가능하다는 특징을 가지고 있다. 이러한 특성은 디지털콘텐츠의 배포 용이와 손쉬운 접근 환경을 제공함으로써 누구든지 쉽게 콘텐츠를 이용할 수 있는 순기능을 제공하기도 하지만, 불법복제와 같은 사례로 인해 저작권자들의 권익이 심각하게 위협받는 역기능의 원인이 되기도 한다. 따라서, 디지털콘텐츠의 불법복제방지와 저작권을 보호하기 위하여 여러 가지 기술적 대안들이 제시되었지만 그중에서 암호화 기술을 기반으로 한 DRM이 최적의 기술로 평가되고 있으며, 이러한 기술을 기반으로 디지털 뮤직, 영화, e-Book, e-Learning, 문서보안 등 다양한 분야에서 DRM의 응용기술이 사용되고 있다.

이러한 DRM은 협의적 의미로 단순히 콘텐츠의 불법복제를 방지하는 요소기술로 정의되기도 하지만 광의적 의미로 디지털콘텐츠 전체 라이프 사이클에 걸쳐 투명하고 신뢰성을 보장해주기 위한 기술과 서비스체계를 통틀어 말할 수도 있다. 이를 위해 DRM은 불법복제로부터 디지털콘텐츠에 대한 지적재산권을 지속적으로 보호해주는 패키징 기술과 허가된 사용자만이 허가된 권한으로 콘텐츠를 이용할 수 있도록 권리를 부여하는 라이센스 관리 기술, 그리고 이렇게 부여된 권한이 지속적으로 보호되는 환경에서 콘텐츠의 이용이 이루어질 수 있도록 하는 권한통제 기술등이 사용된다. 또한 DRM은 이러한 기술 요소들이 디지털콘텐츠 유통 체계에 통합되어 콘텐츠의 생산, 분배, 거래규칙, 이용규칙, 과금, 거래내역의 관리 및 보고, 정산 등 디지털콘텐츠의 전체 라이프 사이클에 걸쳐 투명성과 신뢰성을 보장하는 신뢰기반의 유통 체계를 제공한다. DRM 기반의 유통체계를 구성하는 세부 구성요소는 디지털콘텐츠의 식별체계, 메타데이터 관리체계, 거래내역 관리체계, 그리고 거래 쌍방간의 신뢰를 보장해주는 인증관리체계 등이며, 이러한 구성요소는 디지털콘텐츠의 유통에 참여하는 모든 참여주체들에게 투명성과 신뢰성을 제공해주는 기반 서비스로 제공된다.

이와 같은 DRM 관련 기술들 중에서 현재 국내에서 표준화가 진행되고 있는 부분은 TTA(DRM포럼, MPEG Korea 포럼, 인터넷 식별자 포럼 등)를 통하여 콘텐츠 식별체계나 디바이스 인증기술, 암호화 기술, 메타데이터 분야이다. 기타 나머지 분야들에 대한 국내 표준화 움직임은 아직까지 없는 실정이다. 국제적으로는 MPEG21, OMA(Open Mobile Alliance), XrML, CPTWG, DMP(Digital Media Project), IETF, W3C 등에서 관련 표준화를 진행하고 있다. 특히, 여러 표준화 단체들 중에서 DRM 표준기술 사양의 개발을 위해 OMA 와 MPEG-21이 현재 가장 활발한 활동을 보이고 있다.

IT SoC는 IP 재사용 설계 또는 플랫폼(platform) 기반 설계 방법을 사용하는 SoC (system-on-chip)의 설계 및 개발 방법을 의미한다[3].

IP 재사용이 확산되기 위해 필수적인 문제인 기술보호에 대한 정보제공을 목적으로 하여 VSIA DWG(Development Working Groups)에서는 IP Protection DWG 활동이 전개되고 있다. IP 소스코드 보호를 위해 보안강화는 필수적이지만 보안을 강화하면 유통은 어려워지는 문제가 발생한다. 이러한 문제점들에 대한 해결책을 제시하기위해 표준안 및 Example Tagging Program, IP Tracking

Methodology, Identification and Tracking for Foundry Customer and IP Partners 등의 가이드라인 정보들을 제공한다. 국내에서는 TTA, SIPAC를 중심으로 하여 관련 표준화에 관심을 갖기 시작하는 단계이다.

차세대 PC는 정보이용환경과 사용 목적에 따라 특화된 기능과 형태를 가지는 네트워크 기반의 차세대 디지털정보기기를 총칭한다[3]. 차세대 PC 분야에서의 정보보호 표준화는 아직까지 뚜렷한 움직임이 없는 실정이다.

IV. 결 론

지금까지 IT839전략 추진시 요구되는 각종 정보보호 요구사항과 함께, 현재까지 추진되고 있는 IT839 관련 정보보호 표준화 현황을 살펴 보았다. 이러한 IT839 전략 추진에 따른 정보보호 기술은 기본적으로 다단계 지능형 정보보호 기능이 요구될 것이다. 즉, 기존의 단일 기능의 보안 기능 제공에서 다단계의 지능적인 정보보호 기능이 요구되고 있는 것이다. 더욱이 광대역네트워크를 기반으로 하는 유비쿼터스 환경에서는 하나의 네트워크에서 피해가 발생하게 되면 모든 다른 네트워크로 그 피해가 확대 재생산될 여지가 매우 높기 때문에 이를 방어하기 위해서도 다단계 정보보호 기능의 제공은 필수적인 요소 기능이 될 것이다.

이러한 다단계 정보보호 기능은 접근제어(Access Control), 침입방어(Intrusion Preven-tion), 침입탐지(Intrusion Detection), 침입감내(Intrusion Tolerant) 기능을 의미할 것으로 판단된다.

현재 정보통신부에서 추진하고 있는 IT839 전략의 추진에 따라 그려지는 미래 정보통신 서비스는 유비쿼터스와 컨버전스환경을 그 기반으로 할 것이며, 이러한 환경에서는 수많은 개인의 사적 · 공적인 정보들이 네트워크상에서 혼재되어 사용될 것이다. 그러나, 이러한 정보들을 악의적인 뜻으로 활용하는 경우 그 파급효과는 개인의 사적인 피해뿐만 아니라 국가적인 차원의 대재앙으로까지 발전할 것이다. 따라서, IT839 전략의 성공적인 수행을 위해서는 이러한 개인정보들과 공적인 정보들을 보호하기 위한 기능들이 전적으로 신뢰할 수 있는 수준으로 제공되어야 만이 가능할 것으로 판단된다.

마지막으로, 본 기고문에서 살펴본 바와 같이 현재까지 IT839 전략에서의 정보보호 표준화 현황은 매우 미흡한 실적을 보이고 있다. IT839전략의 성공적인 추진을 위해서는 이러한 정보보호 표준화가 신속정확히 추진되어야 하며, 이를 위해서는 산 · 학 · 연 · 관이 상호 역할 분담 및 긴밀한 연계를 통하여 IT839 전략의 성공적인 추진을 위한 정보보호 기술개발및 표준화에 노력하여야 할 것이다.

[참 고 문 헌]

[1] 서동일, "IT839를 위한 정보보호 기술," ETRI CEO Information 17호, 2004. 11. 17.

[2] 서동일, 김광식, 장종수, 손승원, "IT839 전략 추진을 위한 정보보호 기술개발 방향", 전자통신동향분석, 통권91호, 제20권 제1호, pp. 1 ~ 8, 2005. 2.

[3] 한국정보통신기술협회(TTA), "IT839전략 표준화로드맵 (Ver. 2005)," 2004. 12.

[4] 한국정보보호진흥원(KISA), "국내 정보보호 산업 통계조사," KISA, 2004. 11.

[5] 염흥렬, "IT839 정보보호 기술의 현재와 미래", 정보보호학회지, 제15권 제3호, pp.1~12, 2005. 6.

[6] 고현봉, 오영철, 유승화, "RFID 표준화 동향", Telecommunications Review, 제15권2호, pp.244~256, 2005. 4.
[7] 전용희, 장종수, "BcN 인프라 정보보호", 정보보호학회지, 제15권 제3호, pp.13~28, 2005. 6.
[8] 박광로, "홈 네트워크 표준화와 시장전망", TTA Journal, No.99, pp.20~26, 2005. 5~6.
[9] 송정희, "IT839 전략과 정보보호과제", Information Security Review, 제1권 3호, 2004. 9.

서동일

1998년 경북대 전자공학과 졸업
1994년 포항공대 정보통신공학과 졸업
2004년 충북대 전자계산학과 이학박사
1989년 ~ 1992년 삼성전자(주) 종합연구소
1994년 ~ 현재 한국전자통신연구원 정보보호 연구단 팀장
1994년 ~ 현재 ITU-T SG13, SG17 표준 전문가 활동
2001년 ~ 현재 ASTAP Forum 정보보호 전문가그룹 의장
2001년 ~ 현재 정보통신부지정 IT 국제 표준 전문가
2002년 ~ 현재 TTA TC1 부의장
관심분야 : 정보보호, 컴퓨터 통신, 네트워크 관리