주 제

BcN 인프라 정보보호

ETRI 최양서, 장종수

차례

I. 서 론

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, Broadband Convergence Network)을 중심으로 IPv6 주소체계를 기반으로 RFID/USN이 All-IP망으로 통합되는 유비쿼터스 네트워크 환경을 통해서 실현될 것이다.

정보통신부는 이러한 시대적 요구사항을 적극 수용한 유비쿼터스 코리아(u-Korea) 기본전략[1]을 수립하고 있다. u-Korea의 비전은 국민소득 2만 달러 달성과 생활문화혁명 실현을 통한 함께하는 선진한국 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 및 표준화의 인프라 기반을 바탕으로 추진할 계획이다[2,3].

이와 같은 u-Korea 건설을 위한 핵심 기반이 BcN이다. BcN은 향후 유선과 무선, 방송과 통신이 결합되는 새로운 사회의 핵심 기반 인프라로서, 앞으로 세계 최고 수준의 광대역 통합서비스를 제공하고, 디지털 홈, 지능형 서비스로봇, 차세대 이동통신 등 IT 신 산업의 성장기반을 조성하는 기본적인 역할을 할 것이다. 정부도 2010년까지 2,000만 가입자에게 50~100Mbps급 광대역서비스를 제공할 수 있는 BcN 구축을 위해 2005년도에만 핵심기술개발(610억원), 연구개발망구축(94억원), 서비스기반 확충

(28억원) 등에 총 732억원을 투입하고 있다.

이는 앞으로 BcN의 안정성과 신뢰성이 무엇보다도 중요한 요소로서 관리되고 보호되어야 한다는 것을 의미한다. 즉, 아무리 좋은 환경이 제공되더라도 제공된 환경의 안전성과 신뢰성이 보장되지 않는 이상, 단순 기술 개발 이상의 효과를 얻을 수 없게 되는 것이다. 이에, 본 고에서는 차세대 정보통신 환경의 핵심 기반 요소인 BcN 인프라의 구성 및 발전방향에 대해 알아보고, BcN 인프라 정보보호를 위하여 요구되는 정보보호 핵심 포인트를 도출하여 BcN 인프라 정보보호를 위한 기술 개발 방향을 제시하며, 현재 진행중인 BcN관련 표준동향 및 기술개발 동향을 알아보고자 한다.

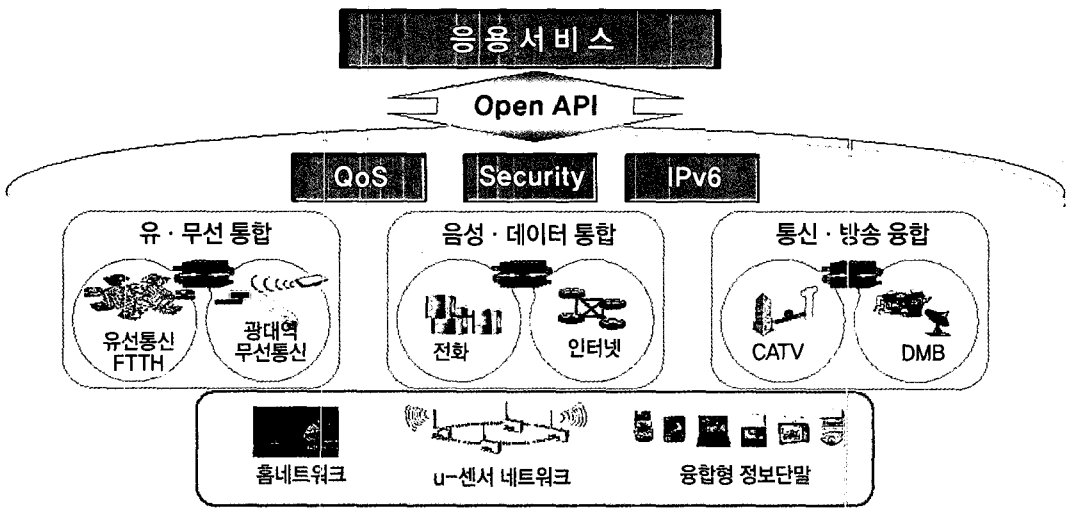
II. BcN 인프라 구성 및 발전 방향

1. BcN 인프라 구성

BcN이란 통신과 방송, 인터넷이 융합된 품질보장형 광대역 멀티미디어 서비스를 언제 어디서나 끊김없이 안전하게 이용할 수 있는 차세대 통합네트워크를 의미한다[1]. 즉, 다양한 서비스를 쉽게 개발하여 제공할 수 있도록 하는 개방형 플랫폼(Open API)을 기반으로 하는 통신망과, 네트워크 단말의 형태에 관계없이 다양한 서비스를 지속적으로 제공할 수 있도록 하는 유비쿼터스 서비스 환경을 지원하는 통신망이 바로 BcN인 것이다.

실제로 BcN은 네트워크 통합 및 서비스의 통합을 통해 새로운 수익 모델을 창출하기 위해 탄생되었다. 즉, BcN은 기존 ISDN/B-ISDN 등과 같이 기술의 발전을 통해 네트워크의 진화가 이루어진 것이 아니라 정보화 사회에서 새로운 시장을 개발하고자 하는 비즈니스 및 사회적인 측면에서 시작된 것이다. 이러한 개념을 잘 표현하고 있는 것이 (그림 2)[4]이다.

그렇다면, BcN 인프라란 무엇인가? 이에 대해서는 다양한 의견이 제시될 수 있다. 그러나, 본 고에서는 BcN 자체가 BcN 인프라는 아니라는 대전제 하



(그림 1) BcN 구성 개념도[1]

에, BcN에서 다양한 가입자들이 통합되는 접속계층(Access G/W)부터, 통합된 트래픽들이 송수신되는 통합전달망을 포함하는 전달계층(통합전달망) 그리고, 전달계층의 상위에서 망 및 서비스를 제어하는 제어계층(Open API G/W, QoS/보안 제어 서버 등)을 포함하는 영역을 BcN의 인프라로 정의한다. 이는 BcN에서 서비스를 제공하는 부분과 서비스를 받는 부분을 제외한 중간계층이라 볼 수 있다.

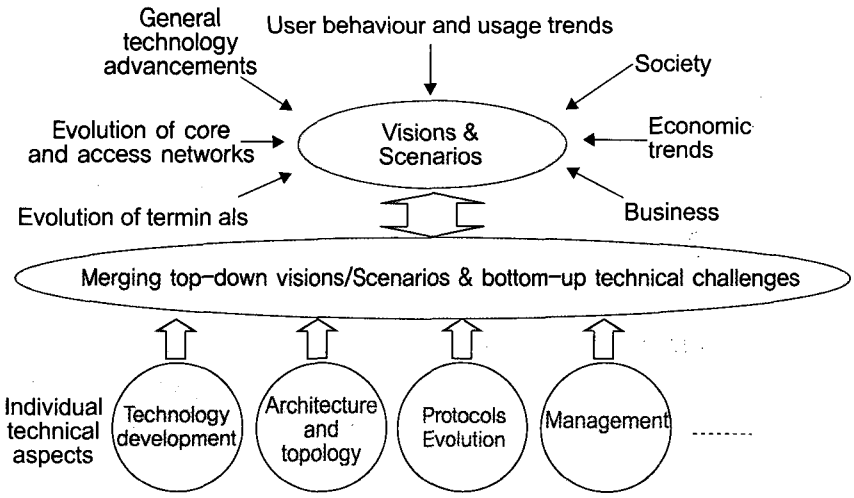
2. BcN 인프라의 발전 방향

정부는 이와 같은 BcN을 구축하기 위해 2010년까지 총 3단계에 걸쳐 BcN의 단계별 목표를 제시하고 있다[1]. 각 단계별 특징을 간단히 살펴보면, 1단계는 유/무선 연동 및 통신/방송망의 초기 융합을 통한 기본 서비스를 제공하는데 있으며, 2단계는 유/무선 통합 및 통신/방송 융합서비스를 본격적으로 제공하고, 3단계에서 광대역 통신/방송/인터넷의 통합망을 완성하는 것이다.

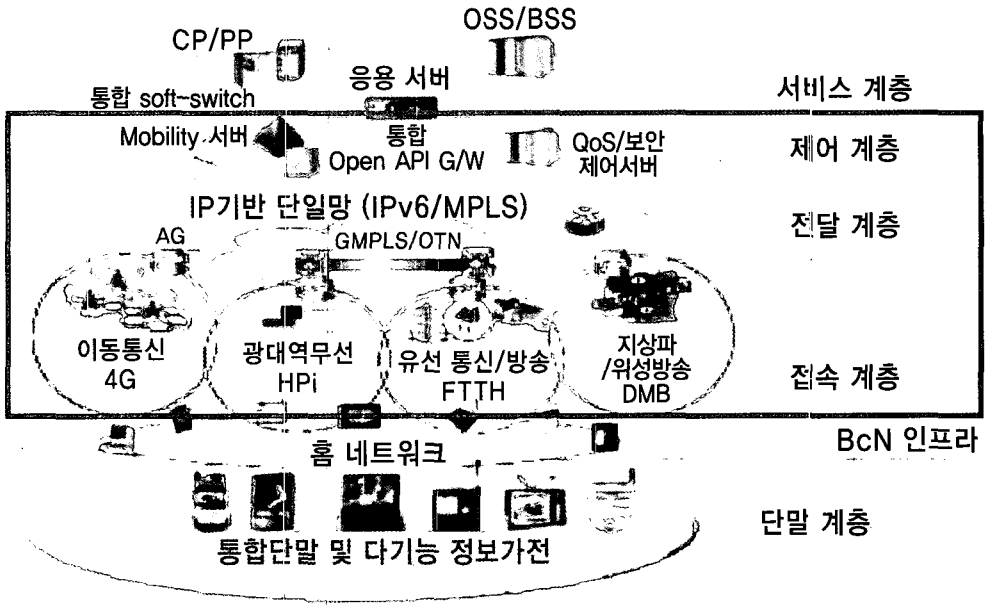
여기서, BcN 인프라 측면에서의 발전 방향을 살펴보면 다음과 같다.

앞서 언급한 BcN의 단계별 목표에 따르면 3단계를 거쳐 2010년에는 유/무선망별 Open API뿐만 아니라 통신/방송이 통합된 Open API Gateway가 도입될 것이며, 모든 계층에 IPv6가 전면적으로 적용되고, QoS 측면에서는 MPLS기반 QoS, Label Switch 기반 QoS를 거쳐 Generalized Label Switch망이 확대되고, 통합 망관리 등을 통한 End-to-End 품질 보장이 가능해지며 OAM 기능이 구비될 것으로 예상되고 있다.

이러한 BcN 인프라의 발전을 바탕으로 결국 BcN은 현재의 각 네트워크의 특성에 따라 사용자의 단말, 단말의 네트워크 접속점, 전달망, 이를 제어하기 위한 제어 방식 및 제공되는 서비스가 결정되는 수평적 구조를 탈피하여 사용자의 단말과 이를 네트워크에 접속하는 접속점들이 전달계층에서 통합(유/무선, 통신/방송, 음성/데이터의 통합)이 이루어지고, 이후 이를 제어하는 제어계층과 이를 바탕으로 제공



(그림 2) BcN 비전 및 시나리오



(그림 3) BcN 인프라의 발전방향

되는 서비스 계층은 Open API를 통해 통합적으로 운영되는 수평적 구조로 발전할 것으로 예상된다. 이와 같은 네트워크의 통합과 구조적인 발전은 보다 안정적으로 다양한 서비스를 제공받을 수 있는 환경을 제공하게 될 것이다.

III. BcN 정보보호 포인트

BcN은 사이버 공간에서의 활동범위를 무한히 넓혀주어, 다양한 서비스를 안정적으로 제공할 것으로 기대되고 있다. 그러나, 이는 어디까지나 네트워크의 안전성과 신뢰성이 보장된다는 가정하에서 가능한 것이다. 실제로 과거 새로운 네트워크 및 서비스의 출현은 새로운 위협 및 침해로 인한 사회적/경제적 손실의 발생을 의미하였다.

따라서, 새로운 사이버 세상의 중추 역할을 할 BcN 역시 이러한 역기능으로 인한 피해로부터 안전하다고 아무도 장담할 수 없는 것이다. 특히, BcN은 기존의 통신망과 프로토콜 및 서비스가 서로 달라 현재까지 개발된 정보보호 기술로는 완전한 보호가 불가능하고, 유무선 통신망과 방송망의 융합에 따라 개별망 피해가 광대역통합망에 연결된 전체 네트워크로 확산되어, 기존의 사이버공격에 취약한 인터넷망에서 발생된 위협이 통합전달망을 통해 개별망으로 확산되어 음성통신망, 방송망, USN까지 피해를 줄 수 있으며, IPv6가 적용됨에 새로운 공격들이 시도될 것으로 예상된다.

이와 같은 위협을 감소시키고 안전한 BcN 구축 및 운영을 위해 필요한 정보보호 포인트를 BcN 인프라의 보호를 위한 네트워크 가용성 및 안전성 측면과 BcN을 기반으로 제공되는 서비스를 보호하기 위한 네트워크 서비스의 무결성 및 기밀성 측면에서 살펴보도록 한다.

1. BcN 인프라 보호를 위한 네트워크의 가용성 및 연속성 측면

BcN의 핵심 인프라는 다양한 형태의 단말들이 접속되어 서비스 계층과 연결되는 통합전달망이라 할 수 있다. 이러한 BcN의 통합전달망은 말 그대로 연결된 모든 형태의 네트워크로 데이터의 전달이 가능한 형태를 갖는다. 그렇다면, 네트워크에서의 가용성 및 연속성이 보장된다는 것은 무엇을 의미하는가? 이는 가입자망에서 어떠한 형태의 트래픽 및 데이터들이 통합전달망을 통해 송수신되더라도 정당한 트래픽이 끊김없이 안정적으로 송수신될 수 있도록 네트워크가 운영될 수 있어야 한다는 것을 의미한다.

이를 위해서는 먼저 송수신 되는 모든 트래픽을 모니터링하고, 이를 바탕으로 트래픽의 이상 유무를 예측하고 판단하여 침해를 유발할 수 있는 트래픽에 대해 실시간으로 대응함으로써 네트워크 가용성을 확보할 수 있어야 한다. 즉, 신속한 침입의 탐지와 차단이 이루어질 수 있어야 하는 것이다. 따라서, BcN 인프라 보호를 위해서는 BcN의 다양한 위치에서 트래픽에 대한 정보를 수집할 수 있는 환경이 필요하고, 이를 통합적으로 관리/운영할 수 있는 프레임워크가 마련되어야 한다.

그러므로, 전체 네트워크 정보를 수집하여 상황을 판단하고 이에 대한 대응을 지시할 수 있는 중앙 집중식 제어 및 관리시스템과, 네트워크 상의 적재적소에 배치되어 관리 시스템으로 네트워크 상황을 보고하고, 관리 시스템으로부터 네트워크 상황에 따른 제어 신호를 받아 지시된 기능(트래픽 차단, 필터링, 모니터링 등)을 수행할 수 있는 보안 노드가 필요한 것이다. 여기서 가장 중요한 것은 다양한 형태의 단말들의 특징을 잘 반영하여 제어가 가능하도록 하는 접속계층에서의 보안 노드로서 가입자 특성에 따라 다양한 형태로 적용될 수 있을 것이다.

이를 위해서는 BcN인프라 전체에 대한 보안 프레임 워크가 정의되어야 하며, 정의된 보안 프레임워크를 기반으로 제공되는 서비스 및 단말의 특징을 적용한 보안 제어 및 관리 서비스 시나리오가 정의되어야 하고, 정의된 서비스 시나리오를 실현하기 위한 보안 메커니즘과, 프로토콜이 정의되어야 하며, 이러한 요소들은 용이한 확장성과 체계적인 관리를 위해 표준화된 Information Modeling 기법이 적용되어야만 한다.

상기된 사항들이 BcN의 특성에 맞게 적용되어야만 다양한 환경에서 발생 가능한 침해 상황을 신속히 분석하여 대응할 수 있게 되고, 상황에 따라 위험도가 높은 네트워크를 통합전달망으로부터 분리, 고립이 가능해진다. 이것이 가능해야만 네트워크의 가용성 및 연속성이 보장될 수 있게 되는 것이다.

2. BcN 인프라에서 네트워크 서비스의 무결성 및 기밀성 측면

네트워크 서비스의 무결성 및 기밀성을 서비스 측면이 아닌 BcN 인프라 측면에서 살펴본다면, 결국 무결성 및 기밀성은 송수신 데이터에 대한 정당성을 확보하는 기술과 정보 노출을 방지하는 기술로 귀결될 수 있다. 즉, BcN의 특성상 매우 다양한 형태의 네트워크에서 송수신되는 데이터가 정당한 시스템 및 사용자에 의해 생성된 것임을 어떻게 증명할 것인가에 관한 것과, 그 정보에 대한 프라이버시를 어떻게 보호할 것인가에 대한 것이다.

실제로 앞으로는 다양형태의 단말이 사용되면서, 단말의 Computing Power 부족으로 인해 현재 인터넷 상에서 사용하고 있는 암호 및 인증 메커니즘이 동일하게 사용될 수 없는 상황이 발생할 것이다. 이와 같은 상황에서 이를 해결하는 방법은 물론 light-weight한 암호 및 인증 알고리즘을 개발하여 사용할

수도 있지만, BcN 인프라 차원에서도 이러한 문제를 극복할 수 있는 방안이 제시되어야 한다. 이를 극복하기 위해 유/무선 통합 VPN, 음성/데이터 통합 VPN, 통합전달망에서 QoS를 보장하는 QSS와 고성능 VPN기술이 통합된 QSS/VPN 등이 제시되고 있는 것이다.

3. 세부 보안 요소 기술

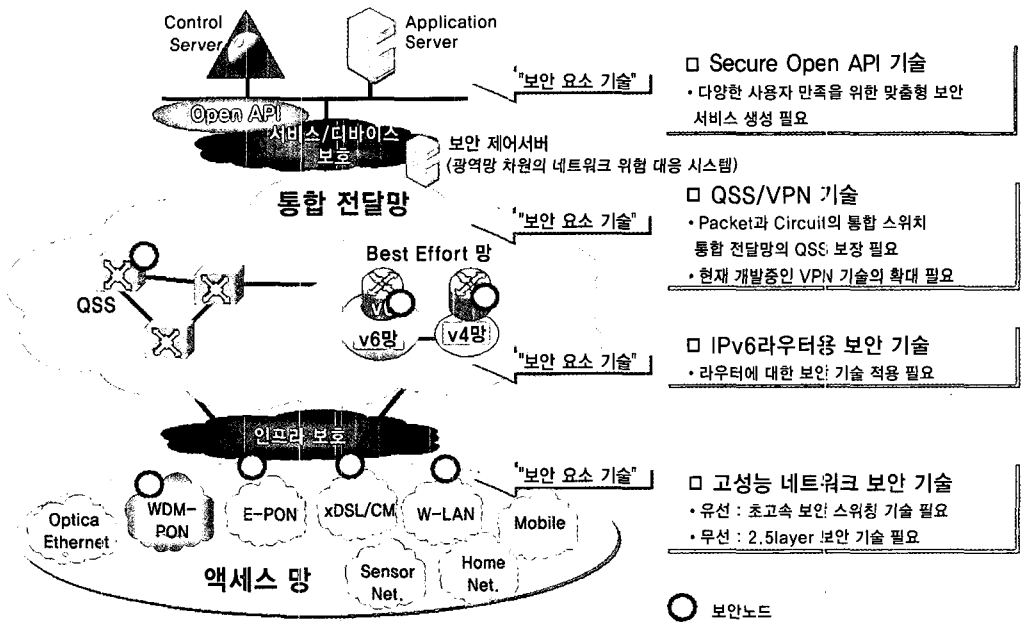
앞서 제시한 정보보호 포인트를 구현하기 위해서는 다양한 정보보호 기술이 요구된다. 이를 구체적으로 살펴보면 다음과 같다.

먼저, 다양한 네트워크 상의 정보를 활용하여 신속한 침입 탐지 및 대응을 수행하기 위한 광역망 차원의 네트워크 위협 대응 시스템이 필요하다. 또한 이것을 기반으로 BcN 환경 예측을 통한 Secure Open API, 무결성 및 기밀성 제공을 위한 QSS/VPN, IPv6 라우터용 보안 기술 등이 필요하다. 특히, BcN 백본 네트워크 인프라의 처리능력은 최고 수십 Gbps 수준인 반면, 현재의 정보보호 장비의 처리능력은 수 Gbps에 불과하여 BcN 인프라에 적용 하는데 한계가 있기 때문에 기본적으로 이를 극복할 수 있는 고성능 네트워크 보안기술이 필요하다. 이를 그림으로 살펴보면 (그림 4)와 같다.

IV. BcN 정보보호 동향

1. 표준화 동향

현재 BcN과 관련되어 표준화가 진행되는 대표적인 것이 ITU-T의 FG-NGN이다. FG-NGN은 2004년



(그림 4) 세부 보안요소기술이 적용된 BcN 인프라 보호 개념도

6월에 발족된 NGN Focus Group으로서 2개월을 주기로 회의를 진행중에 있다. FG-NGN은 Functional & Nomadicity Architecture, QoS, Security Capability, NGN Control and Signaling Capability 그리고 Evolution from CGN to NGN에 대한 표준화를 진행중이다. 특히 보안과 관련되어서는 ITU-T FG-NGN의 WG5에서 수행하고 있다. FG-NGN WG5에서는 Network Security Framework에 대한 표준화 작업을 수행하고 있는데, 주로 개념적인 모델을 제시하는데 초점이 맞춰져 있다. 단, FG-NGN은 2005년까지만 한시적으로 운영되고 Closed될 예정이다.

FG-NGN은 〈표 1〉과 같이 이루어져 있다.

〈표 1〉 FG-NGN Working Groups[12]

WG	Area	Deliverables
WG 1	SR(Service Requirement)	NGN Scope, Release 1/ General Requirements, Service and Capability, Mobility Services and Capabilities
WG 2	FAM (Functional Architecture, and Mobility)	Req. and Architecture, Functional Req. for NGN Mobility, Functional Req. for Soft Router
WG 3	QoS	TR-123.qos, TR-msnniqos, TR-NGN.qos, TR-NGN.NHNperf, TR-e2eqos.1, TR-enet, TR-atmipa, TR-racs, TR-ipaqos
WG 4	CSC(Control & Signaling)	TRQ.IP.QOS.SIG.CS1
WG 5	SeC(Security Capability)	NGN Security Framework
WG 6	Evol(Evolution)	Evolution of Networks to NGN, PSTN evolution to NGN
WG 7	FPBN(Future Packet-based Bearer Network)	Future Packet Network Requirements

〈표 2〉 ITU-T SG13 Working Party & Questions[12]

Working Party	Questions	Title
WP 1/13 Project management and coordination	1/13	Project coordination and release planning for NGN
	11/13	General network terminology
	13/13	Public data networks
WP 2/13 Functional architecture and mobility	3/13	Principles and functional architecture for NGN
	6/13	NGN mobility and fixed-mobile convergence
	9/13	Impact of IPV6 to an NGN
	10/13	Interoperability of satellite with terrestrial and Next Generation Networks (NGNs)
	15/13	NGN security
WP 3/13 Service requirements and scenarios	2/13	Requirements and implementation scenarios for emerging services in NGN
	7/13	Network and service interworking in NGN environment
	8/13	Service scenarios and deployment models of NGN
	12/13	Frame Relay
	14/13	Protocols and service mechanisms for Multi-service Data Networks (MSDN)
WP 4/13 QoS and OAM	4/13	Requirements and framework for QoS for NGN
	5/13	OAM and network management for NGN

〈표 3〉 ITU-T SG17 Working Party 2[12]

Working Party	Questions	Title
Working Party 2/17 Telecommunication Security	4/17	Communications Systems Security Project
	5/17	Security Architecture and Framework
	6/17	Cyber Security
	7/17	Security Management
	8/17	Telebiometrics
	9/17	Secure Communication Services

ITU-T SG13에서는 NGN에 대한 전반적인 사항에 대해 표준화를 진행하고 있는 Study Group이다.

최근에는 Softswitch기반 NGN에 대한 것이 FGNGN에서 거부되었으나, SG13의 Q.7/13에서 Call server 기반 PSTN/ISDN Emulation으로 연동 측면에서 기존 전화망을 NGN에 접속하기 위한 방안을 제시한 Y.csem(TD25, WP3/13)이라는 새로운 권고안 작업을 시작하기로 하였다. SG13은 총 4개의 Working Party가 구성되어 있는데, 주요 업무는 〈표 2〉와 같다.

또한 ITU-T SG17에서는 "보안, 언어, 소프트웨어"분야의 표준화가 진행되고 있는데, 특히 보안 구조 및 프레임워크에 관해서는 WP2(Telecommunication Security)의 Q.5에서 "Security Architecture and Framework"에 대한 표준화가 진행되고 있다. ITU-T SG17의 Q.5에서는 NGN Security Question의 연구사항과 중첩되는 부분에 대한 영역 구분이 진행될 예정이다. ITU-T SG17의 WP2는 〈표 3〉과 같이 구성되어 있다.

국내에서는 BcN 포럼의 BcN 표준모델 전담반을 중심으로 BcN 표준 모델에 대한 논의가 진행중이며, 2004년 12월 현재 "BcN 표준 모델 Draft 2.2"가 제시되어 있다.

본 모델에는 BcN 구축 목표를 실현하기 위한 망 구조 및 기술규격, 서비스 제공 기준 등에 대한 가이드라인 등이 제공되고, 단계별 망진화에 따른 BcN의 구조 및 기술규격, 서비스 제공 기준을 4계층(서비스 계층, 전달망 계층, 가입자망계층, 홈 및 단말 계층)으로 나누어 제시하고 있다.

BcN표준모델전담반은 본 드래프트 문서를 조정하여 연내에 BcN 1차 표준모델로 최종 확정할 계획이다. 또한 2005년도에는 BcN표준화협의회라는 명칭으로 국제 표준화 활동에 참여하고 있다.

2. 기술개발 동향

현재 BcN 기술들은 전체 네트워크를 서비스 및 제어계층, 전달망 계층, 가입자망 계층으로 분류되어 각 계층별로 기술개발을 추진중이다. 이중 BcN의 서비스 및 IPv6, QoS 등에 대한 기술개발은 매우 활발히 이루어지고 있다. 현재 서비스제어를 위한 Open API의 시제품이 완성되었고, IPv6 홈 라우터를 개발 완료하여 IPv6 Ready Logo를 획득하였으며, 중형 IPv6 라우터를 개발 시험 운영중에 있다.

또한 BcN의 핵심인 QoS 보장을 위해 해외 업체들과 공동개발이 추진되고 있으며, 가입자망에서 사용되는 E-PON 개발이 완료되었고 WDM-PON 개발이 추진중에 있다.

정보보호 관련 기술개발과 관련해서는 먼저 ETRI에서는 지난 2002년부터 시작된 광역 네트워크 보호를 위한 "고성능 네트워크 정보보호 시스템 개발"과제가 2004년에 1단계 마무리가 이루어지면서 10G급 고성능 보안 게이트웨이 기술과 기가급 IPSec VPN 기술 개발을 마치고 기술이전에 들어갔다.

또한 각 정보보호 업체들도 기존의 IPv4용 정보보호 제품들을 IPv6용으로 개발하고 있으며, 퓨쳐시스템[13]의 경우 ETRI와 공동 개발한 IPv6용 VPN장비에 IPv6 레디 로고를 획득하는 등, BcN 정보보호를 위한 기술 및 제품 개발 역시 활발히 진행중이다.

V. 결 론

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 것이

며, 이는 광대역통합망(BcN, Broadband Convergence Network)을 중심으로 IPv6 주소체계를 기반으로 RFID/USN이 All-IP망으로 통합되는 유비쿼터스 네트워크 환경을 통해서 실현될 것이다.

그러나, BcN은 서비스 및 네트워크 기술만으로는 절대 성공할 수 없다. 이는 과거 새로운 기술 및 제품의 발전은 새로운 역기능의 출현으로 이어졌음을 보면 쉽게 알 수 있다. 따라서, 안전한 BcN의 운영과 구축을 위해 다양한 정보보호 기술이 함께 개발되어야 한다. 정부에서도 이를 위해 "안전한 u-Korea 구현을 위한 중장기 정보보호 로드맵(안)"을 작성하여 토론회를 개최하기도 한 것이다.

이에 본 고에서는 차세대 정보통신 환경의 핵심 기반 요소인 BcN 인프라의 구성 및 발전방향에 대해 알아보고, BcN 인프라 정보보호를 위하여 요구되는 정보보호 핵심 포인트를 도출하여 BcN 인프라 정보보호를 위한 기술 개발 방향을 제시하며, 현재 진행중인 BcN관련 표준동향 및 기술개발 동향을 알아보았다.

특히, 안전한 BcN 운영을 위한 정보보호 포인트를 2가지 측면에서 살펴보았다. 먼저 BcN 인프라 보호를 위한 네트워크의 가용성 및 연속성 측면에서는 안전한 BcN의 구축 및 운영을 위해서는 BcN인프라 전체에 대한 보안 프레임 워크가 정의되어야 하며, 정의된 보안 프레임워크를 기반으로 제공되는 서비스 및 단말의 특징을 적용한 보안 제어 및 관리 서비스 시나리오가 정의되어야 하고, 정의된 서비스 시나리오를 실현하기 위한 보안 메커니즘과, 프로토콜이 정의되어야 하며, 이러한 요소들은 용이한 확장성과 체계적인 관리를 위해 표준화된 Information Modeling 기법이 적용되어야만 한다는 것을 강조하였다. 그리고 BcN 인프라에서 네트워크 서비스의 무결성 및 기밀성 관점에서는 BcN 인프라를 통해 송수신되는 데이터의 무결성에 대하여 강조하였다.

앞으로 안전한 BcN 구축을 위해 제안된 핵심 정보보호 포인트를 기본 개념으로 활발한 정보보호 기술 개발이 이루어지게 되면, 안전한 u-Korea 실현의 중요한 역할을 수행할 것으로 기대되며, 안전한 유비쿼터스 서비스 환경을 제공함과 동시에 사이버 상에서의 안전한 경제활동이 가능함으로 인하여 국가 신용도 증대 및 투자 유치 확대의 시너지 효과도 창출할 것으로 예상된다.

[참 고 문 헌]

[1] Bcn구축기획단, "정보통신 일등국가 실현을 위한 BcN 구축 기본계획(안)", 정보통신부, 2003. 11.

[2] 장종수, 박상훈, "안전한 u-Korea 실현을 위한 5대 정보보호 기술기획 방향", 한국전자통신연구원, 주간기술동향 통권1179호, 2005. 1.

[3] 이홍섭, "u-Korea 추진전략과 정보보호", 한국정보보호진흥원, 정보보호뉴스, 2005. 1.

[4] 최준균, "BcN 기술 동향", IITA 기술정책정보단, www.itfind.or.kr

[5] 박준석, 권경인, "BcN 주요 요구사항별 기술 및 활동 동향", IITA 기술정책정보단, www.itfind.or.kr

[6] 박상훈, "BcN 추진현황 및 향후 계획", 정보과학회지 제23권 제2호, 2005. 2.

[7] 김윤정, "안전한 u-Korea 구현을 위한 중장기 정보보호 로드맵 수립의 의의와 과제", 정보보호뉴스, 한국정보보호진흥원, 2005. 6.

[8] 함진호, "BcN 요구사항 및 워크샵 Outline", BcN 합동 표준화 워크샵, 2005. 4.

[9] 최준균, "국제표준화회의 참가보고 ITU-T SG13", TTA저널 통권 99호, 2005. 6.

[10] 진병문, 오홍룡, 염홍열, 정교일, "국제표준화 회의 참가보고 ITU-T SG17 모스크바 회의", TTA저널 통권 99호, 2005. 6.
[11] 정보통신부, "안전한 u-Korea 구현을 위한 중장기 정보보호 로드맵(안)", 정보통신부, 중장기 정보보호로드맵 정책토론회, 2005. 3.
[12] http://www.itu.int
[13] http://www.future.co.kr

최양서

1996년 강원대학교 전자계산학과 이학사
2000년 서강대학교 컴퓨터공학과 공학석사
2000년 ~ 현재 한국전자통신연구원 네트워크보안 구조연구팀 선임연구원
관심분야 : 정보보호, 네트워크보안, BcN, 포렌식, 침입분석

장종수

1984년 경북대학교 전자공학과 공학사
1986년 경북대학교 전자공학과 공학석사
2000년 충북대학교 컴퓨터공학과 공학박사
1989년 ~ 현재 한국전자통신연구원 네트워크보안 그룹장 (책임연구원)
한국정보보호학회 이사, 학회지 편집위원장, 한국정보처리학회 논문지 편집위원, 한국정보과학회 논문지 편집위원, 한국통신학회 회원
관심분야 : 정보보호, 네트워크보안, 웹서비스보안, Traffic Management, IDS/IPS