BcN 정보보호 기술개발 현황

김 국 한　　최 병 철　　유 종 호　　서 동 일

◈ 목 차 ◈

1. 머리말

광대역통합망(BcN: Broadband convergence Network)이란 통신·방송·인터넷이 융합된 품질보장형 광대역 멀티미디어 서비스를 언제, 어디서나, 끊임없이(seamless) 안전하게 이용할 수 있는 차세대 통합네트워크를 말한다(그림 1 참조)[1,2].

이를 기반으로 온라인 근무, 이동 근무와 같은 가상사무실 근무환경과 디지털방송, HD급 VoD 등의 고품질 영상 환경 그리고 원격진료와 같은 건강·복지 환경 등에서 요구되는 다양한 서비스를 제공할 수 있다.

정보통신부는 이러한 시대적인 요구사항을 수용한 유비쿼터스 코리아(u-Korea) 건설을 진행하고 있다. u-Korea의 비전은 국민소득 2만 달러 달성과 생활 문화혁명 실현이다. 이러한 비전을 달성하기 위한 추진전략에는 윤택한 삶, 편리한 삶, 안전한 삶, 즐거운 삶으로 표현되는 IT839 분야의 다양한 엔진이 있고, 이러한 엔진들에서 "정보화 역기능 방지 및 정보격차 해소"는 안전한 u-Korea를 구현하는 핵심 요소인 것이다 [3].

따라서 성공적으로 u-Korea를 실현하기 위해서는 가장 중요한 인프라인 BcN에서의 안전성과 신뢰성이 보장되어야 한다.

기존의 단일 네트워크 환경에서는 각각의 자체 네트워크 취약점에만 영향을 받지만, BcN 네트워크에서는 유·무선 네트워크, 방송·통신망, 데이터·음성 등이 통합한 하나의 네트워크 형태이기에 어느 한 곳에서 발생하는 취약점은 다른 네트워크로 확산될 수 있고 그로 인한 피해 규모는 더욱 커질 위험요소를 내재하고 있다.

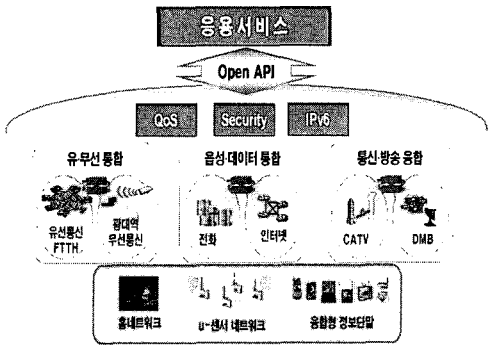
본 고에서는 BcN 인프라의 취약점과 현재 정보보호 시장, 기술 및 표준화 동향을 살펴본 후 이에 대응하기 위한 본 연구단의 5대 정보보호 핵심 기술 개발 현황을 알아본다.

2. BcN 정보보호 필요성

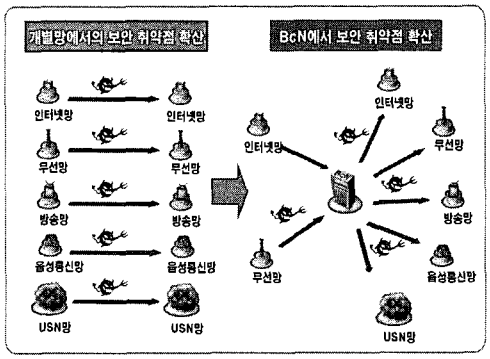
우리나라는 우수한 정보통신 인프라를 가지고 있다. 이를 기반으로 정보통신부는 IT839전략을 통해 BcN을 기반망으로 하는 유비쿼터스 네트워크 환경 구축을 주도하고 있다. 즉, 머지않아 현재의 인터넷망은 이종망간의 융합한 BcN을 통해 언제, 어디서든, 누구나 멀티미디어 서비스를 편리하게 사용할 수 있는 유비쿼터스 환경이 구축되는 것이다.

그러나 BcN 망에서는 웜/바이러스 및 해킹 등과 같은 각종 사이버공격에 취약한 인터넷망을 이용한 공격으로 인해 방송망, 통신망의 장애가 가능하다. 또한 BcN에 연결된 무선망인 WLAN(Wireless Local

* 한국전자통신연구원



(그림 1) BcN 구성 개념도



(그림 2) 광대역통합망에서 보안 취약점의 확산[4]

Area Network), WPAN(Wireless Personal Area Network)등이 사이버 공격에 많은 취약성을 내포하고 있어 공격의 통로로 활용 될 가능성 또한 높다. 그리고 VoIP(Voice of IP)가 일반화 되면 기존의 회선 교환망에서 유·무선 인터넷망으로 전환되었을 때 고려해야 할 보안사항도 여러 가지가 있다 [4]. 즉, BcN의 개별망이 각종 사이버 공격으로부터 침해를 받게 되면, 전체 네트워크의 장애를 발생시키고 이는 2003년 발생한 1.25 인터넷 대란과는 비교할 수도 없는 정도의 큰 규모의 사고로 이어질 수 있다.

BcN은 개방형 망구조 특징 때문에 다양한 경로로 통신망에 쉽게 접근이 용이하고, 이를 이용해 해킹 및 바이러스 유포의 가능성을 가지고 있다. 표 1에서 알 수 있듯이 서비스, 관리/제어, 전달, 접속, 홈/단말 계층마다 각각의 보안 위협 요소들이 존재하고 있다 [5].

따라서 안전한 u-Korea 실현을 위해서는 그 바탕이 되는 BcN에서의 보안은 필수적인 요소라고 할 수 있다. 그림 2는 BcN에서 개별망에서의 보안 취약점이 다른 망으로 쉽게 확산되어 나감을 보여준다.

3. 정보보호동향

BcN 정보보호를 알아보기 위해서는 현재의 정보보호 관련 시장 규모, 기술 및 표준화 동향을 알아봄으로써 흐름을 알 수 있다.

(표 1) BcN 계층별 예측 취약점

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

(표 2) 정보보호 시장 분류

대분류	중분류	세부 항목	
정보보호 H/W	하드웨어 인증	· 생체인식	· 보안 스마트카드
	보안 어플라이언스	· Firewall/VPN (하드웨어 기반)	· SCM (Security Contents Monitoring)
		· IDS & IPS(주로 네트워크 기반의 솔루션)	· UTM (Unified Threats Management)
정보보호 S/W	사용자 인증 및 접근 관리	· PKI (Public Key Infrastructure)	· IAM (Identity and Access Management)
		· SSO (Web & Host 기반)	
	보안 및 취약성 관리	· SIM/SEM (보안 정보/사건 관리)	· 취약성 분석/평가
		· 보안 패치 시스템	· 통합보안관리시스템 (ESM)
	보안 컨텐츠 관리	· 안티 바이러스	· 웹 보안
		· 스팸 차단	· Malware & Crimeware 차단
		· 저작권 보호 (워터마킹 & DRM)	
	위협 관리	· IDS & IPS (주로 호스트 기반의 솔루션)	· Firewall/VPN (소프트웨어 기반)
		· Secure OS	
	무선/모바일 보안	· 무선 PKI	· 무선랜 보안
		· 모바일 디바이스 보안 솔루션 (백신 포함)	
정보보호 서비스	보안관제	· 보안관제 서비스	
	컨설팅이행	· 취약점 진단/분석 서비스	
	보안교육	· 보안교육 서비스	

3.1 정보보호 시장

정보보호 시장은 크게 정보보호 H/W, 정보보호 S/W 그리고 정보보호 서비스 이렇게 3가지 분류로 나눌 수 있다. 표 2에서 보듯이 H/W에서는 하드웨어 인증이나 방화벽 및 IPS 등을 통한 보안 장비 등이고, S/W는 사용자 인증 및 접근 관리, 컨텐츠 및 이벤트 관리, 취약성 관리, 무선/모바일 관리 등이다. 마지막으로 서비스는 보안 관제, 컨설팅, 보안 교육 분야이다 [6].

세계 정보보호시장은 2003년 228억 달러 규모로 파악되며, 향후 연평균 18%로 성장하여 2008년에는 521억 달러에 이를 것으로 전망된다. 부문별로는 정보보호서비스 시장이 연평균 19.8% 성장률로 2008년에는 260억 달러로 전체의 49.8%를 점유하고 소프트웨어 분야가 162억 달러, 하드웨어 부문이 98억 달러에 이를 전망이고, 세계 정보보호 시장에서 2008년까지의 연평균성장률이 가장 높을 것으로 예상되는 부문은 하드웨어 부문이며 21%의 성장률 예상된다. 소프트웨어 단독 제품들이 여러 가지 소프트웨어 기능을 가진 하나의 하드웨어 제품에 통합되어 가는 경향 때문에, 소프트웨어 부문보다 하드웨어 부문의 성장률이 더 높은 것으로 분석된다 [6].

국내 정보보호시장은 2004년도 6,500억원에서 2009년에는 1조 1,400억원 규모에 이를 전망이며 연평균 11.9%의 성장률을 보일 것으로 예측된다. 성장률이 가장 높은 분야는 정보보호서비스 분야로 연평균 17.74%의 성장을 거듭하여 2009년에는 시장규모가 1,970억원에 이를 것으로 전망되고, 정보보호 H/W 및 S/W 분야는 각각 2009년도에 시장규모가 5,040억원 및 4,380억원에 이를 것으로 전망되며 연평균 성장률은 각각 11.01% 및 10.72%를 보이는 것으로 분석된다[7].

표 3, 4와 같이 소프트웨어 분야에서는 보안/취약성 관리기술이 강세를 보이고 있고, 하드웨어 분야는 "침입 탐지/방지 기술"이 강세다 [6,7].

(표 3) 세계시장 주요 보안제품 동향 (단위:백만달러)

	2003	2004	2005	2006	2007	2008	2003~2008 CAGR(%)
Software							
보안, 취약점 관리	1,210	1,488	1,808	2,175	2,592	3,043	20.30
침입 탐지/방지 (S/W)	365	373	380	391	402	415	2.60
방화벽/VPN	911	982	1,041	1,098	1,152	1,203	5.70
Hardware							
침입 탐지/방지 (장비)	222	356	499	624	717	825	29.90
방화벽/VPN	1,479	1,667	1,791	1,804	1,623	1,462	0.20

(표 4) 국내시장 주요 보안제품 동향 (단위:백만원)

	2004	2005	2006	2007	2008	2009	2004~2009 CAGR(%)
Software							
보안관리 S/W	63,547	77,763	89,630	98,905	105,622	110,220	11.71
침입탐지 S/W	27,369	28,474	29,257	29,759	30,077	30,275	2.10
Hardware							
침입차단	69,534	75,032	77,996	79,366	79,990	80,271	2.91
침입 탐지/방지 (장비)	43,238	54,125	61,515	66,345	69,502	71,565	10.60
VPN	82,201	97,500	111,977	124,968	136,627	147,089	12.34

3.2 정보보호 기술

과거 방화벽으로부터 시작한 네트워크 정보보호 기술같이 단일 보안 솔루션으로는 최근 발생하는 다양한 문제점에 대응하기 어렵다. 특히 단일 네트워크에서 통신·방송·인터넷이 융합되어 다양한 컨텐츠와 서비스를 제공할 수 있는 통합망으로 진화해 가면서 그 위험 요인은 더욱 다양해지고 취약성도 높아진다는 것을 앞서 이야기 했다.

여기서는 BcN 인프라에서 필요한 기술이 무엇인가를 알기 위해 최근 네트워크 보안에서 요구되는 변화를 알아보고, 세계적인 IP 시장 조사 기관인 가트너 그룹에서 발표한 최신 기술동향과 마지막에 BcN 계층별로 요구되는 기술을 살펴본다.

근래 네트워크 보안요구 사항의 변화를 보면 크게 Contents Security, No Signature IPS, Internal Network Security 이렇게 3가지로 나눌 수 있다[8].

첫째, 다양한 서비스(WWW, E-mail, P2P, 인스턴트 메시지 등) 정보에 유해 및 불법 정보를 다량 포함한 공격 형태(Phishing & Pharming, Spam, Malicious codes, Social Engineering Attacks 등)가 증가하고 있다. 이에 대응하기 위해서는 컨텐츠 기반 보안이 요구된다. 즉 보호하고자 하는 해당 어플리케이션의 프록시 형태로 컨텐츠 필터링 기능을 추가하여 새로운 알고리즘이 필요하다.

두 번째, 2004년 국내 정보보호 제품의 최대 관심사는 IPS(Intrusion Prevention System)이었다. 기존의 IDS(Intrusion Detection System)는 실패한 개념이 되었고 그에 대한 대안으로 IPS가 각광을 받고 있다. 그러나 IPS는 기존의 IDS가 지니고 있는 Signature기반에 유해 트래픽을 차단하는 기능을 추가한 정도의 기술이 제공 되었는데 이는 급속하게 증가하는 웜 트래픽에 대한 Signature 활성에 걸리는 시간과 비용 문제, 네트워크 성능저하, False

Positive 문제를 가지고 있다. 따라서 이에 대응 할 수 있는 No Signature IPS의 연구가 더욱 필요하다.

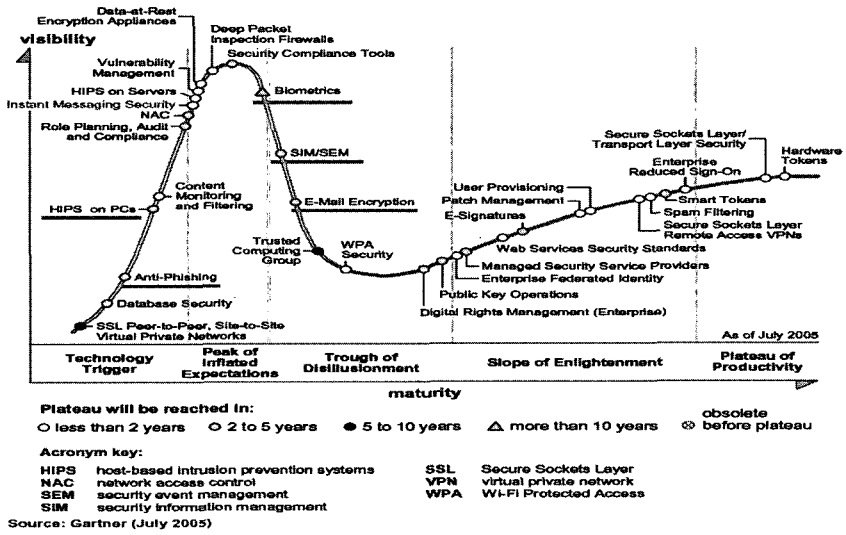
마지막 세 번째, 현재까지의 네트워크 보안은 내부망과 외부 인터넷망과 연결된 사이에 존재하며 내부 IT 자원을 보호하기 위한 차단과 탐지가 주목적이었다. 그러나 내부 LAN의 피해를 입히는 웜의 발생으로 이해 발생할 큰 피해를 조기에 통제하고 예방할 수 있는 방안이 요구된다. 그러한 기술이 Internal Network Security(Incident Response System)이다. INS 기술은 다양한 LAN 프로토콜의 지원과 취약성 점검 및 클라이언트 격리 기능을 포함한다.

다음으로는 그림 3과 같이 2005년 7월 가트너 그룹에서 발표한 정보보호 관련 기술 동향을 알아보겠다[9].

우선 최근에 발생하고 있는 기술을 보면, 개인 PC간의 연결을 위해 SSL(Secure Sockets Layer)을 이용하여 P2P 통신을 하거나 라우터 없이도 VPN (Virtual Private Network)을 emulate 할 수 있는 SSL Peer-to-Peer, Site-to-Site VPN 기술. e-메일을 통해 잘 알려진 금융 사이트를 가장하여 개인 정보를 유출하는 피싱(Phishing) 공격에 대응하기 위해 e-메일 필터링, URL 차단과 같은 서비스를 IPS, e-메일 Provider, 은행에 제공하는 Anti-Phishing 기술이 있다. 그리고 악성 코드를 모니터링 하고 signature를 생성하는 HIPS(Host-based Intrusion Prevention System) on PCs 기술이 있다. 이외에도 인스턴트 메신저 보안, 취약점 관리, NAC(Network Access Control)등이 있다.

그리고 손가락이나 손의 스캔, 홍체 스캔, 키보드 탄도, 안면 인식 등과 같은 생체 정보를 이용하여 신원확인이나 인증을 하는 Biometrics, 실시간 이벤트 관리와 히스토리 분석를 위해 다양한 소스로부터 보안 정보를 뽑아내어 모으고 통합하는 SIM/SEM (Security Information Management & Security Event Management) 기술, 개인의 프라이버시와 중요한 정보를 보호하기 위해 Person-to-Person 메시지 전송에 암호화를 사용하는 E-Mail Encryption같이 중요한 기술이 있다. 위와 같이 다양한 정보보호 기술들이 요구되고 그에 따른 대응 기술들이 필요하다.

마지막으로 BcN 환경이 내재하고 있는 계층별 위협 요소들에 대응하는 기술을 살펴보면 우선 서비스 계층에서는 다양한 사용자 만족을 위한 맞춤형 보안 서비스 생성 제공하는 Secure Open API (Application Programming Interface) 기술, Service



(그림 3) Hype cycle Security Information 2005

(표 5) FG NGN Working Groups

WG	Area	Deliverables
WG1	SR(Service Requirement)	NGN Scope, Release 1/ General Requirements, Service and Capability, Mobility Services and Capabilities
WG2	FAM (Functional Architecture, and Mobility)	Req. and Architecture, Functional Req. for NGN Mobility, Functional Req. for Soft Router
WG3	QoS	TR 123.qos, TR msnniqos, TR NGN.qos, TR NGN.NHNperf, TR e2eqos.1, TR enet, TR atmipa, TR racs, TR ipaqos
WG4	CSC(Control & Signaling)	TRQ.IP.QOS.SIG.CS1
WG5	SeC(Security Capability)	NGN Security Framework
WG6	Evol (Evolution)	Evolution of Networks to NGN, PSTN evolution to NGN
WG7	FPBN(Future Packet based Bearer Network)	Future Packet Network Requirements

Security가 있고, 관리/제어계층에서는 통합 전달망의 QoS(Quality of Service) 보장과 VPN 기술 확대를 위한 QSS(Quality Security Service)/VPN 및 BcN 보안관리 기술이 요구된다. 그리고 전달 계층에서는 IPv4/IPv6가 혼재하는 인프라 구축용 보안 기술과 IPv6 인프라 구축용 통합보안 기술이 필요하다. 또한 접속 계층에서는 고성능 네트워크 보안 기술이 필요하고, 마지막으로 홈/단말 계층에서는 Privacy 보장 기술 등의 기술이 요구된다.

3.3 BcN 표준화

현재 BcN과 관련되어 국제 표준화가 진행되는 대표적인 조직이 ITU-T의 FG-NGN(Focus Group-Next Generation Network)이다. FG-NGN 은 2004년 6월 시작된 NGN Focus Group으로서 2005년까지만 한시적으로 운영된다.

(표 6) ITU T SG17 Working Party 2

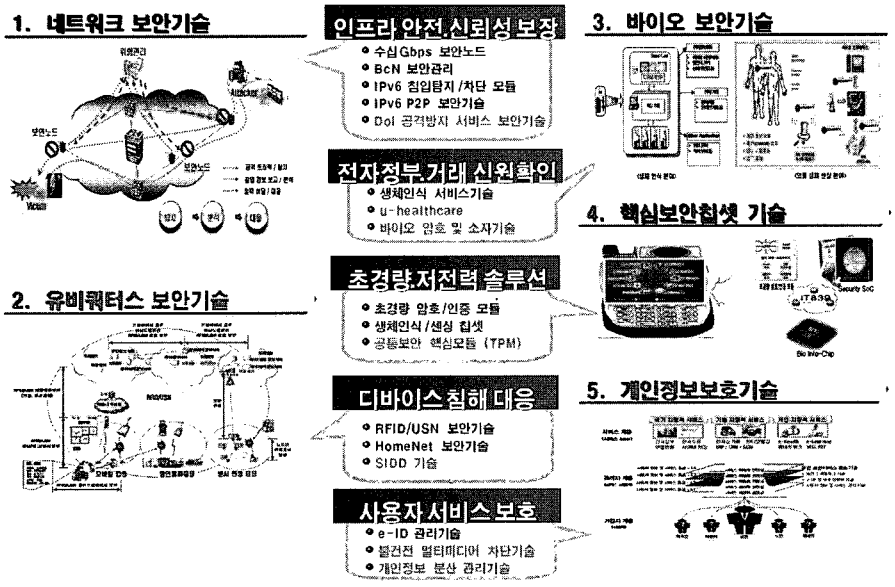
Working Party	Questions	Title
WP 2/17 Telecommunication Security	4/17	Communications Systems Security Project
	5/17	Security Architecture and Framework
	6/17	Cyber Security
	7/17	Security Management
	8/17	Telebiometrics
	9/17	Secure Communication Services

FG-NGN에서는 SR(Service Requirement), FAM (Functional Architecture and Mobility), QoS, CSC (Control and Signaling), Evolution, PBN(Future Packet-based Bearer Network) 등과 같은 분야로 나뉜 7개 Working Group으로 구성되어 있으며, 표 5에서와 같이 "NGN Security Framework" 표준화는 WG5에서 진행하고 있다 [10].

2005년 6월 중국 베이징에서 열린 제 7차 FG-NGN 미팅에서는 "Guidelines for NGN Security"와 "NGN security requirements for release 1"이 제출되었다. 다음 미팅은 2005년 8월 스위스 제네바에서 열린다.

ITU-T SG13은 NGN에 대한 전반적인 사항에 대한 표준화를 진행하는 Study Group이다. SG13은 총 4개의 Working Party가 있고, 각 WG마다 "관련 Question"에 대해 표준화를 진행한다. "NGN Security" 표준화를 진행하는 Q15/13의 주요 임무는 NGN 보안 프레임워크, NGN 보안 구조, 기타 보안 이슈들을 논의와 NGN 환경에서 X.805 권고안을 적용하기 위한 연구를 진행, 그리고 NGN 환경에서 요구되는 AAA(Authentication, Authorization, and Accounting) 기술 개발을 한다.

그리고 ITU-T SG17에서는 "보안, 언어, 소프트



(그림 4) 5대 정보보호 핵심기술 개발

웨어" 분야의 표준화가 진행되고, 표 6에서와 같이 WG2/17 (Telecommunication Security)의 Q5/17에서 "Security Architecture and Framework"에 대한 표준화가 진행되고 있다 [10].

국내 BcN 관련 표준화 연구 동향은, 한국정보통신기술협회(TTA)에서 Security & Lawful Interception과 관련하여 PG101(정보보호기반), PG204 (NGN) 그룹이 있으나 구체적인 논의 진행은 이루어지지 않은 상태이고, 정보통신부를 중심으로 하여 2005년 6월 BcN 표준전략 협의회가 구성되었으며, 이를 중심으로 하여 NGN과 관련 국내 표준을 검토할 예정이다 [11].

4. ETRI 정보보호 기술개발 현황

정보통신부가 추진하고 있는 u-Korea 실현 목표는 2007년까지 세계 최초의 기능지반사회 진입, 2015년까지 지능기반사회 완성하는 것이다. 이런 목표를 성공적으로 이루기 위해서는 필연적으로 그 기반을 이루는 BcN에서의 정보화 역기능 방지를 할 수 있는 요소기술들이 제공 되어야 한다.

ETRI(한국전자통신연구원) 정보보호연구단은 이와 관련하여 그림 4의 "5대 정보보호 핵심기술 개발"을 수행하고 있다. 개발 분야는 최초 u-Korea 건설의 추진 전략 분야의 여러 가지 엔진들을 아우를 수 있는 5대 핵심 분야를 선정하여 향후 융합(Convergence)이 가능하도록 타 분야의 Seed 역할을 수행하도록 한다 [12].

5대 정보보호 핵심 분야는 네트워크 보안기술, 유비쿼터스 보안기술, 바이오 보안기술, 핵심보안 칩셋 기술, 개인정보보호기술이다 [5].

유무선 통신망과 방송망의 융합에 따라 개별망 피해가 광대역통합망에 연결된 전체 네트워크로 확산 될 우려가 있다. 여기에 대응하는 네트워크 보안 기술은 인프라 안전 및 신뢰성 보장을 위한 기술로서 통합 네트워크 보안 프레임워크를 기반으로 정보보호를 제공하는 기술이다. 광역망 차원의 네트워크 위협 대응 시스템 개발을 기반으로 Secure Open API, QSS/VPN, IPv6 라우터용 보안기술, 고성능 네트워크 보안 기술 등 BcN 네트워크 인프라 전반에 걸친 보안 기술 개발 체계가 필요하다. 현재 본 연구단에서는 "고성능 네트워크 정보보호 시스템 기술개발" 사업에서 그러한 요구사항에 대해 일부

진행 중이고, 수십 Gbps급 보안노드, BcN 보안관리, IPv6 침입탐지/차단 모듈 개발, DoI (Denial of Information) 공격방지 서비스 보안기술 등을 목표로 하고 있다. 사업 추진 실적으로는 20G급 보안게이트웨이 원천기술 확보 및 상용화 추진, 10G급 라우터용 보안기술 개발 및 사용화 추진, 고성능 침해방지용 보안관리 시스템 핵심기술 확보 및 기술이전 계획 등이 있다 [12].

u-Korea 완성을 중심이라고 할 수 있는 RFID/USN (Radio Frequency Identification & Ubiquitous Sensor Network) 환경에서는 기존 컴퓨터 정보통신뿐 아니라 개인의 사적인 공간 및 정보도 공격대상이 된다. 따라서 RFID/USN 환경에서 모든 사물에 부착하여 사용하는 전자태그/센서 정보의 무단 누출 및 위·변조, 오동작, 개인 프라이버시 문제를 해결하기 위해 초경량 객체 정보보호 기술 및 시스템 개발이 필요하다. 특히 교통, 의료/복지, 재난/재해와 같은 안전관련 분야에서는 위급한 상황에서 신속한 대처가 요구되므로 정보보호 기능이 없는 유비쿼터스 서비스 제공이 어렵다. 따라서 유비쿼터스 핵심 인프라의 프라이버시 강화를 위해 유비쿼터스 환경에서의 프라이버시 강화를 위한 정보보호 기술이 필요하다. 현재 본 연구단에서는 "RFID/USN 정보보호 기술 개발" 사업을 중심으로 유비쿼터스 보안 기술개발이 진행 중이며, 홈 네트워크 인증/접근제어 기술, 3G/WAN 통합 보안 연동기술 사업도 진행 중이고, RFID/USN 보안, 홈 네트워크 보안, SIDD (Smart IDentity Device) 보안 기술이 주요 사업목표이다. BcN 인프라를 주요 기반으로 하는 유비쿼터스 환경에서 개인의 다양한 서비스를 안전하게 사용 할 수 있도록 하는 원천기술 분야는 생체인식, 생체 센싱, Bio-Networking, 생체 면역에 관련된 바이오 보안 분야이다. 유비쿼터스 환경에서는 생체인증을 통해 전자정부 보호, 전자거래 및 의료/복지 분야의 서비스가 가능하다. 따라서 개인의 생체 정보는 아주 중요하고 안전하게 관리 되어야 한다. 본 연구단에서는 u-Korea에서 정부 주도형 서비스의 안전성을 제공하기 위해 "생체 인식 기술 개발" 사업을 진행 중이며, "생체 센싱 기술 및 Bio-Networking 기술 개발" 사업이 계획 중이다.

유비쿼터스 통신·방송 융합형 신규 IT 서비스 환경에서 다양한 디바이스들이 네트워크 노드로서 구성됨으로 새로운 공격 목표나 공격에 활용될 가능성이 높다. 이런 디바이스들은 데스크 탑과 대등한 성능으로 발전하고 있으며, 그물처럼 연결된 융합 환경에서 순식간에 바이러스나 웜 등이 휴대폰이나

(그림 5) 사업 추진 전략

PDA를 통해 확산될 수 있는 가능성을 가지고 있다. 따라서 복합 단말기의 안정성 보장을 위한 복합 단말이 보안 기술 개발이 필요할 것으로 예상된다 [13,14,15]. 현재 본 연구단에서는 IT 디바이스 보호를 위한 초경량/저전력 보안 솔루션을 위해 DMB(Digital Multimedia Broadcasting), WiBro (Wireless Broadband Internet), 텔레메틱스 서비스를 위한 사용자와 기기간의 인증기술 및 인증되지 않은 휴대단말기의 불법접근제어 및 개인정보 유출 방지를 위한 바이오 칩셋과 같은 보안 컴포넌트 기술, 신규 IT 서비스에 적합한 복합단말기 안정성 보장을 위한 보안 칩셋 기술, 이기종 무선 통신망 (3G/ PWLAN/휴대인터넷)간 USIM/PKI(Universal Subscriber Identify Module & Public Key Infrastructure) 기반의 상호보안 연계 서비스를 위한 보안 SoC(System on Chip) 기술이 필요하다. 즉, DMB, WiBro 등의 복합단말기용 핵심보안 IP/SoC 요소 기술을 위해 "생체인식 칩 셋 개발" 사업을 중심으로 진행 중이며, 차세대 암호/인증 칩셋, 생체 센싱 칩셋, 공통보안 핵심모듈(TPM: Trusted Platform Module) 기술 개발" 사업이 계획 중이다.

마지막으로, u-Korea 기본전략에서 "Security"의 중요한 역할은 서비스 사용자의 프라이버시 제공 및 지역간·계층간 정보격차 문제 해소를 통한 정보화 역기능 방지가 주요한 내용이다. 이를 해소하기 위해서는 안전한 사용자 서비스 제공을 위한 사이버 실명제 기반의 보안 위임서비스 기술이 요구된다. 이 기술은 인터넷의 익명성을 해결하고, 개인 사생활 보호 및 지역간·계층간 정보격차 문제 해결할 수 있다[5]. 본 연구단에서는 "e-ID 기술, 유해정보 차단기술" 사업을 중심으로 진행 중이며, 향후 "인프라, 서비스, 사용자의 관점의 융합 보안 서비스 기술" 사업이 계획 중이다.

5. 추진전략

u-Korea의 실현을 위한 근간이 되는 안전한 BcN 인프라를 구축하기 위해서는 서비스계층, 관리/제어 계층, 전달망 계층, 접속 계층, 홈/단말 계층에서 각각 요구되는 위협대응 기술들이 계층별로 추진되어야 하며, 또한 본연구단에서 진행 중인 5대 정보보호 핵심기술 개발이 성공적으로 마무리해야 한다. 즉, 안전한 BcN 인프라 구축을 조기에 실현하고 정보보호 기술 개발의 완성도 및 산업화 극대화를 위해서는 현 진행 중인 사업을 계획대로 잘 추진해야 하고, 그림 5와 같이 각계 관련 기관과 효과적인 우호협력 네트워크를 구축하여 기술의 완성도를 향상시켜나가야 할 것이다 [12].

6. 맺음말

본 고에서는 현재 정보통신부를 중심으로 진행 중인 u-Korea 건설에서 BcN이 차지하는 위치와, BcN에서의 정보보호 필요성을 알아보았고, 그에 따른 현 시장, 기술, 표준화 동향을 살펴보았다. 그리고 BcN 정보보호에 필요한 대응 기술로 한국전자통신연구원 정보보호연구단에서 진행 중인 BcN 관련 "5대 정보보호" 핵심 기술에 대해 살펴보았다.

누구나, 언제, 어디서든 다양한 정보와 서비스를 이용할 수 있는 환경을 구축 하는 u-Korea의 비전은 국민소득 2만 달러 달성과 생활 문화혁명 실현이다. u-Korea를 구현하기 위해서는 기반이 되는 다양한 추진전략 분야에서의 "정보화 역기능 방지와 정보격차 해소"가 필연적으로 제공되어야 한다. 이런 의미에서 안전한 u-Korea 건설의 주요 핵심 기반 인프라인 BcN에서의 정보보호는 매우 중요하다 할 수 있다.

따라서 BcN 인프라 각 계층별로 예상되는 취약점 발굴과 대응하는 요소기술들의 개발은 안전한 유비쿼터스 서비스 환경 제공과 다양한 경제활동을 가능하게 함으로서 국가 신용도 증대 및 투자유치 확대의 시너지 효과를 창출 할 수 있다는데 있어서 매우 중요한 역할을 할 것 이라 사료된다.

참 고 문 헌

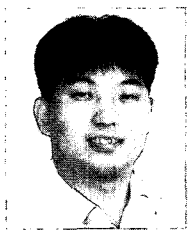
[1] BcN구축기획단, "정보통신 일등국가 실현을 위한 BcN 구축 기본계획(안)", 정보통신부,

2003.11.
[2] 이홍섭, "u-Korea 추진전략과 정보보호", 정보보호뉴스, 2005.1.
[3] 장종수, 박상훈, "안전한 u-Korea 실현을 위한 5대 정보보호 기술기획 방향", 한국전자통신연구원, 주간기술동향 통권1179호, 2005.1.
[4] 김정윤, 이응용, 김인호. "유비쿼터스 환경의 보안 위협과 대응 방안", 한국정보보호진흥원, 정보보호뉴스 2004.10.
[5] 최병철, 김광식, 서동일, 장종수, "안전한 u-Korea 실현을 위한 정보화 역기능 방비 대책-Security Belt", 한국전자통신연구원, 전자통신동향분석 제 20권 2호, 2005.4.
[6] IDC, "Worldwide IT Security Software, Hardware, and Services 2004-2008 Forecast: The Big Picture", 2004. 12.
[7] KISIA, "국내 정보보호산업 전망(2004-2009)", 2004.12.
[8] 美 CSI 2004(Computer Security Institute) 2004.11.
[9] Gartner, "Hype Cycle for Information Security 2005", 2005.7. http://www3.gartner.com
[10] ITU-T, http://www.itu.int
[11] 서동일, "ITU-T NGN Security 표준화 동향 및 전개방향", 제 7회 정보통신표준화 워크숍, 2005.8.
[12] 손승원, "BcN 정보보호 기술개발 현황", 제 1차 BcN 정보보호 실무협의회, 2005.8.
[13] 정통부, "정보보호 중장기 기본전략 보고서", 2005.1.
[14] 정통부, "정보보호 중장기 실무협의회 보고서", 2004.12.
[15] Gartner Symposium ITXPO 2004, "The Future of Information Security & The Future of Network Security & Evolution of Security Architecture", http://www3.gartner.com

◐ 저 자 소 개 ◑

김 국 한

2000년 한양대학교 물리학과 (이학사)
2003년 경희대학교 정보통신망관리공학과 (공학석사)
2000년~2001 삼성전자 디지털미디어총괄 컴퓨터시스템사업부 사원
2003년~2005 한국과학기술정보연구원 슈퍼컴퓨팅센터 초고속연구망개발실 연구원
2005년~현재 한국전자통신연구원 정보보호연구단 네트워크보안구조연구팀 연구원



최 병 철

1999년 서울시립대학교 제어계측공학과 (공학사)
2001년 서울시립대학교 전자전기공학부 (공학석사)
2001년~현재 한국전자통신연구원 정보보호연구단 네트워크보안구조연구팀 연구원

유 종 호

1998년 순천향대학교 전자공학과 (공학사)
2000년 순천향대학교 전기·전자공학과 (공학석사)
2004년 순천향대학교 전기·전자공학과 (공학박사)
2004년~현재 한국전자통신연구원 정보보호연구단 네트워크보안구조연구팀 연구원

서 동 일

1989년 경북대학교 전자공학과 (공학사)
1994년 포항공과대학교 정보통신공학과 (공학석사)
2004년 충북대학교 전자계산학과 (이학박사)
1994년~현재 한국전자통신연구원 정보보호연구단 네트워크보안구조연구팀장 선임연구원
2001년~현재 ASTAP Forum Information Security 의장