주 제

초고속 정보기반 확산에 따른 정보보안의 주요이슈와 대응전략

한국정보보호진흥원 원장 **이홍섭**

차 례

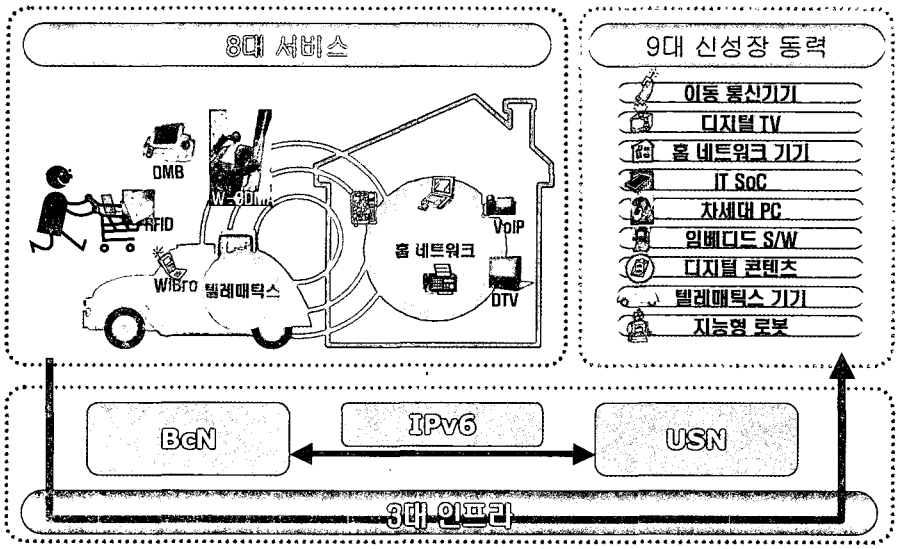
Ⅰ. 서 론

정부는 우리 경제의 주요 기반인 IT산업을 경쟁력 높은 미래형으로 끌어올리기 위해 IT839 전략을 수립하여 추진하고 있다. IT839 전략은 (그림 1)에서 보여주듯이 8개 핵심 서비스와 3대 핵심 인프라 그리고 9대 신성장 동력 산업을 정의하고, 각각에 대한 보급시기, 기술개발 방법 및 목표 등을 포함한 중 · 장기 계획을 수립하여 적극적으로 추진하고 있다.

3대 인프라 분야의 추진경과를 간략하게 살펴보면, 정부 및 산 · 학 · 연과의 유기적인 협력을 통해 2005년 전국 12개 지역 총 2076가구에 대하여 BcN 시범서비스를 개통하였고, 공공기관에 우선적으로 IPv6를 보급하는 등의 IPv6 보급촉진 정책을 시행하고 있으며, 다양한 분야에 RFID/USN 시범서비스를 확대하여 추진하고 있다. 8대 서비스 분야를 살펴보면, 홈네트워크, VoIP, DMB, RFID 서비스는 이미 상용화 단계에 접어들었으며, WiBro 서비스는 올해 상용화 단계에 접어들 예정이다. 금년부터는 이제까지 추진된 인프라와 서비스 분야의 노력을 통합하여 시너지를 높일 수 있도록 u-City 및 u-Work 사업을 추진하여 입체적으로 유비쿼터스 사회로의 진입을 가속화 시킬 계획이다.

하지만, 인터넷뱅킹의 해킹사고, 다양한 변종의 웜 · 바이러스 등장, 휴대폰용 웜 · 바이러스 출현 등에서 볼 수 있듯이, 정보사회의 발전과 병행하여 다양한 정보화 역기능이 증가하고 있는 것이 현실이다. 2005년까지 순기능 중심으로 IT839 전략이 추진되었다면, 이제부터는 3대 인프라 및 여러 신규서비스의 상용화에 발맞추어 보안을 함께 고려하여 안전한 서비스를 제공하는 것이 중요하다. 이를 통해 사용자 신뢰를 확보하고 서비스가 보다 원활하게 보급될 수 있는 선순환 구조를 만들어 나가야 할 것이다.

따라서, 본 고에서는 유비쿼터스 사회로 가기 위한



(그림 1) IT839 전략

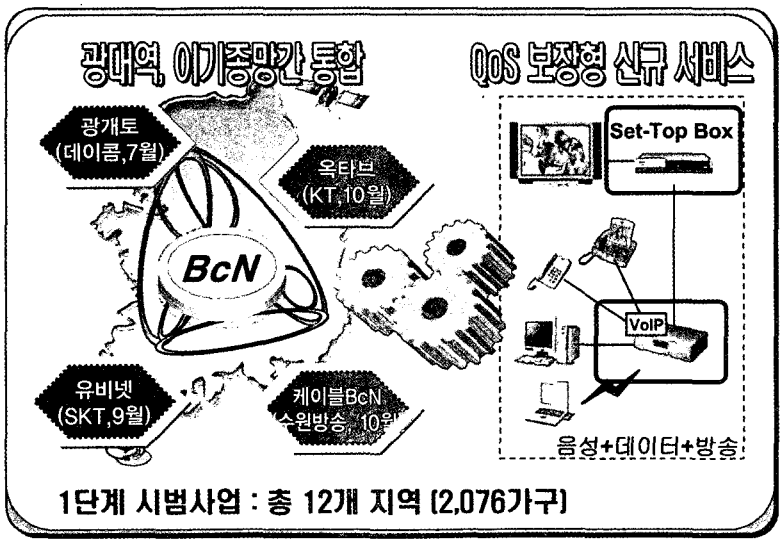
초고속 정보기반 환경의 변화를 살펴보고 예상되는 정보보호 위협요소를 도출한 후, 정보보호 위협에 대비한 정보보호 추진방향을 제언하고자 한다. IT839 전략의 개별 요소들에 대한 안전성 확보는 어느 것 하나 빠짐없이 중요하지만, 본 고에서 다루는 범위는 상용화 단계에 접어든 3대 인프라 중에서 BcN과 8대 서비스 중 VoIP, DMB, RFID 서비스를 대상으로 한다.

II. 정보보호 환경의 변화

1. 초고속 정보기반의 확산

BcN이 발전하면 유 · 무선, 음성 · 데이터, 방송 · 통신망이 통합되어 정부, 기업, 개인에게 제공되는 다양한 서비스는 삶의 편리성과 윤택함을 더욱 향상시킬 것으로 전망된다. 전자정부 측면에서는 시간 · 장소에 구애받지 않고 각종 민원서비스를 제공받을 수 있고 사이버 의정, 전자국회 등의 서비스로 확대될 전망이며, 기업측면에서는 전자무역, 인터넷 화상회의, ERP · CRM · SCM 등 기업정보화가 확대됨에 따라 기업의 획기적인 효율성 · 생산성 향상이 예상된다.

IT기술의 기반 인프라인 BcN 구축을 위해, 정부에서는 2010년까지 총 3단계로 시범사업을 추진하고 있으며, 1단계 시범사업이 2005년을 기점으로 종료되고, 2006년부터 2007년까지의 2단계로 접어들었다. 1단계 시범사업을 통해 광대역, 유 · 무선 통합, 음성 · 데이터 통합 등이 이루어 졌으며, (그림 2)에서 보여주듯이 품질보장을 위한 기반기술이 구축되어 전국 12개 지역 2076가구에 광대역, 품질보장형 서비스를 제공하고 있다. 2단계에 접어들면서 품질보장 기술고도화 및 타사업자 망간의 연동 고도화를 지속적으로 추진하고, 신규 응용서비스를 중점적으로 발굴하여 BcN 서비스의 대중화를 가속화하는 목표를 가지고 적극 추진하고 있다.



(그림 2) BcN 1단계 시범사업 개요

2. 신규 서비스의 정착

디지털 컨버전스가 빠르게 진행되면서 IT서비스는 개인의 요구를 적극 수용하여 융합화 · 개인화 · 지능화된 서비스로 진화하고 있다. 그 예로, 맞춤형 방송 서비스, 가전 및 산업기기와 IT와의 융합을 통한 신규 서비스, 차세대 로봇 및 센서를 이용한 제3의 서비스 등이 지속적으로 창출될 것으로 전망되며, 우선 상용화 단계에 접어든 대표적인 서비스에 대해서 살펴보면 다음과 같다.

VoIP 서비스는 저렴한 통신비용, 다양한 부가서비스 등의 장점을 가지나 통화품질 보장이라는 문제를 내포하고 있어, 기대와 달리 빠른 속도로 시장이 확대되지 않았다. 하지만, 국내에서는 음성통화품질을 보장할 수 있는 광대역통합망 구축과 맞물려, 대표적인 킬러 애플리케이션 기술로 부상하였으며, 영상전화서비스 제공을 목표로 빠르게 관련 기술 및 장비가 개발되고 있다. 또한, 2004년 10월부터 070 번호체계가 법적 효력을 발휘하게 되었고, 2005년 7월부터는 상용 인터넷전화 서비스가 제공되어 VoIP 기술의 대중화는 더욱 가속화되고 있다.

DMB 서비스는 지상파 DMB와 위성 DMB로 구분되며, 위성 DMB는 2005년 1월부터 제공해온 시범서비스에 이어 2005년 5월부터 본격 상용서비스를 개시하였으며, 지상파 DMB 서비스는 2005년 3월 시범서비스를 시작하여 12월 상용서비스를 개시하였다. DMB 서비스에 발맞추어 DMB용 단말기의 보급이 크게 확대되어 사용자가 지속적으로 증가하고 있으며, 2006년부터 리턴채널로 휴대인터넷망 또는 이동전화망을 이용할 전망이어서 통 · 방 융합 서비스로 거듭날 것으로 전망된다.

RFID 서비스는 정부주도로 2004년부터 다수의 시범사업을 통해 다양한 분야에 적용하고 있으며, 점차 민간부분 주도로 적용 분야가 확대되어 가고 있다. RFID 적용분야를 보면 2004년에 '조달청 물품관리 시스템', '항공 수하물 추적 통제 시스템', 수입쇠고

기 추적 시스템' 등 총 5개 분야에 적용하였으며, 2005년에는 'RFID기반 감염성 폐기물관리 시스템', 'RFID기술 적용 신무기체계 자산관리시스템', '개성공단 통행 및 전략물자관리 시스템' 등 총 5개 분야에 적용하였으며, 점차로 확대 추진하고 있는 추세이다.

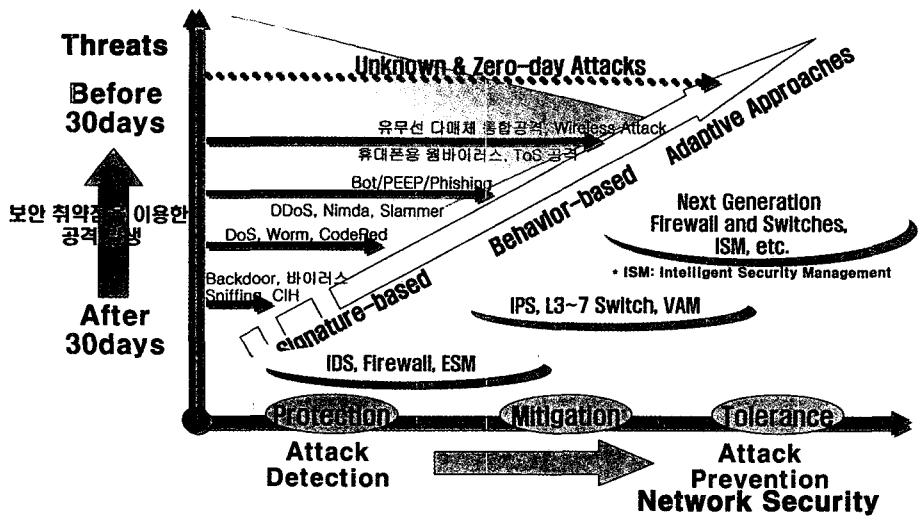
3. 사이버공격의 고도화와 피해증가

최근의 사이버공격은 이전의 시스템 침입이나 웜 · 바이러스로 인한 파일 변조, 자료 유출 등 개별시스템과 개인에 대한 공격에서 원격 조정이 가능한 해킹도구의 사용을 통한 타겟 공격이나, 웜 · 바이러스 등을 통해 대량의 트래픽을 발생시킴으로써 인터넷 망 기반구조를 공격하는 형태로 변화되고 있다. 더욱 심각한 것은 최근의 사이버 공격이 금전적인 피해 유발 등의 사이버 범죄가 차지하는 비중이 크게 증가하고 있다는 점이다. (그림 3)은 최근 사이버 공격의 고도화 추세를 보여주고 있으며, 최근 사이버공격의 주요한 특징 및 향후의 전망은 아래에서 살펴본다.

가. 지능화, 고도화, 고속화

최근의 사이버공격은 웜 · 바이러스에 취약점 자동스캔, 자체 메일발송엔진, 감염PC 원격제어 등 해킹 기술이 결합되어 능동적으로 확산대상을 탐색하고, 감염시킨 대상을 특정 사이트를 공격하는 중간경유지로 악용하는 등 고도화되고 있다. 또한 이러한 해킹 프로그램 및 웜 · 바이러스 소스가 인터넷에 공개되고, 공개된 해킹 프로그램 및 웜 · 바이러스 소스프로그램을 통해 전문지식이 없는 일반인도 쉽게 해킹 기술을 익히고, 누구라도 사이버공격을 감행할 수 있게 되었다. 이러한 경향에 따라 최근의 웜 · 바이러스는 다양한 악성 변종들이 급속하게 확산되고 있고, 광범위하게 확산된 변종들에 의하여 백신 등 방어체계가 무력화되는 등 부작용이 심각해지고 있다.

개인 PC의 성능향상과 개인 PC들이 접속된 인터넷의 속도도 매우 빠르게 높아지고 있으며, 이는 초고속으로 공격을 확산시키는 역할을 하고 있다. 또한 소



(그림 3) 사이버 공격의 고도화 추세

프트웨어가 포함하고 있는 보안취약성에 대한 공격 추이를 보면, 보안취약성의 발표 후 이에 대한 공격이 이루어지는 기간이 점점 짧아져 취약점에 대한 패치가 발표되기 전에 공격이 이루어지는 Zero-Day 공격으로부터의 위협이 증가하고 있다.

나. 전파경로 다양화

과거에는 웜 · 바이러스의 확산 경로가 PC통신 등을 통한 파일 다운로드나 디스켓의 복제 등 사용자의 행위가 반드시 개입되어야 하는 것들이 많았다. 그러나 최근의 확산 방식은 이전과 달리 소프트웨어에 내재된 취약점을 악용하거나, 이메일에 웜 자체를 첨부하여 전송함으로써 불특정 다수에게 전파시키거나, 공유 폴더, P2P 등과 같이 최근 보편화된 네트워크 서비스를 통하여 감염을 시도하는 등 전파경로가 다원화되어 가고 있다.

특히, 메일로 전파되는 웜들은 이전과 같이 감염된 사용자가 사용하는 메일서버를 경유하여 전파하는 것보다 신속하게 자신을 복제하기 위하여 메일전송 프로그램을 내장하고 있고, 메일의 제목이나 본문의 내용을 수신자가 읽어보도록 현혹시키는 사회공학적 수법을 가미하는 등 전파 수법이 매우 지능화되고 있어 이로 인한 피해가 급속히 늘어나고 있다.

다. 사회공학적 역기능 증가

최근의 사이버 공격 추세를 보면, 기존의 과시형 공격 또는 특정 대상에 대한 공격에서 점차로 인터넷 뱅킹 사고 등과 같이 범죄의 수단으로 사용되는 경우가 지속적인 증가 추세를 보이고 있어 그 심각성은 날로 심화되고 있다.

또한, 경제 · 사회활동 등 생활전반에 걸쳐 인터넷 의존도가 점차로 심화됨에 따라 많은 개인정보가 인터넷에 저장되고 있다. 이러한 이유로, 사용자의 프라이버시 침해에 대한 우려가 급속히 증가하고 있는 추세이다.

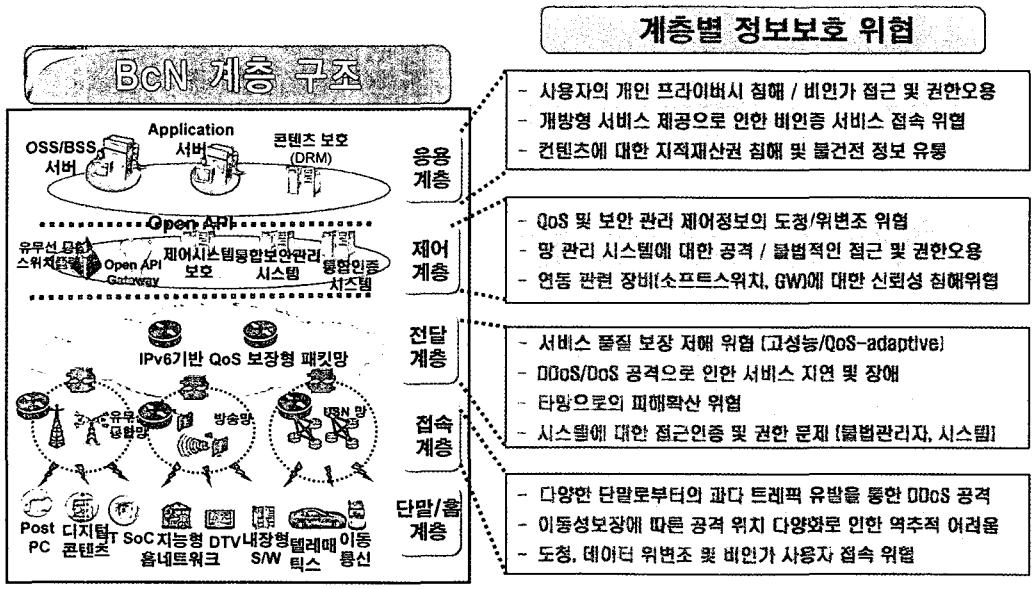
마지막으로, 불특정 다수에 대한 무작위적인 스팸메일 또는 메시지가 증가함에 따라 인터넷 사용자에게 불편함과 거부감을 유발시키고 있으며, 각 개인의 피해를 떠나 점차 사회문제화 되고 있다. 하지만, 점차로 스팸이 단순 광고 수준에서 벗어나, 사회공학적 수법을 통한 개인정보의 불법적 취득, 악성코드 삽입을 통한 공격 경유지화 등, 제 2의 사이버 공격 혹은 범죄의 수단으로 사용되고 있다는데 더 큰 문제가 있겠다.

III. 초고속 정보기반 환경의 위협요소

본 장에서는 전국 12개 지역에 서비스를 개통한 BcN 인프라와 8대 서비스 중 상용화 단계에 있는 VoIP, DMB, RFID 서비스에서 예상되는 정보보호 위협요소에 대해 살펴본다.

1. BcN 인프라의 정보보호 위협

BcN 환경에서는 기존 인터넷망에 잠재된 취약점 외에 망융합과 신규 구성요소 및 기술의 적용으로 인한 새로운 보안위협이 나타날 것으로 예측된다. 첫째, 네트워크의 광대역화로 악성코드의 전파 역시 급속하게 진행되어 취약한 네트워크 기반을 마비시킬 수 있다. 둘째, 기존에 별도로 운영되어 왔던 방송 · 통신망 등이 통합되므로 공격에서 상대적으로 안전했던 전화망, 방송망으로의 피해 범위확산이 우려된다. 셋째, 휴대폰, PDA, RFID 내장, WiBro, DMB 등 기능이 융합된 복합 단말기를 대상으로 하는 해킹 및 웜 · 바이러스가 발생할 것으로 예측되며, 이들이 네트워크 기반을 공격하는 경우 현재의 개인용 PC에 의한 공격보다 더욱 위협적일 것으로 예측된다.



(그림 4) BcN 계층별 정보보호 위협

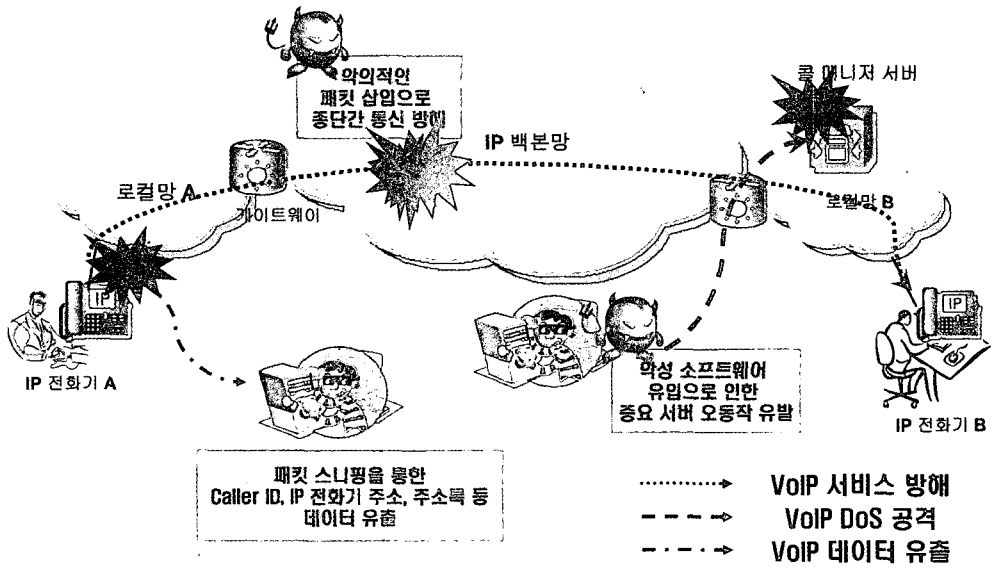
BcN을 통신망에서의 기능에 따라 계층별로 구분하면 (그림 4)에서와 같이 서비스 및 제어계층, 전달계층, 접속 계층, 단말 및 홈네트워크 계층으로 구분되며 네트워크 인프라가 아닌 단말 및 홈네트워크 계층을 제외한 각 계층별 특성에 따른 정보보호 위협들은 다음과 같다.

서비스 계층은 Open API 기반의 다양한 응용서비스가 제공되는 계층으로써, 다양한 서비스가 쉽게 탑재되어 제공될 수 있는 구조를 가진다. 이러한 개방형 구조를 가짐으로써, 비인가 서비스의 접속 위협, 다양한 콘텐츠에 대한 지적재산권 침해 위협 및 불건전 정보의 유통위협들이 존재한다. 기존인터넷에서와 마찬가지로 응용서비스에 대한 비인가 접근 및 권한오용 위협과 서비스 사용자의 프라이버시 침해 위협이 존재한다.

제어계층은 망장비, 인증, QoS 제어 등을 관리하는 역할을 담당하는 계층으로써 여러 제어/관리정보에 대한 도청 및 위변조 위협이 존재한다. 또한, 인증서버, 과금서버 등과 같은 중요 관리/제어 시스템에 대한 공격 위협이 존재하며, 이로 인한 피해는 2003년 발생한 1.25인터넷 침해사고와 같이 네트워크 전체에 파급효과를 미칠 수 있다.

전달계층은 높은 대역폭을 제공하고 품질을 보장한다는 점이 가장 큰 특징으로써, 서비스 품질을 저해하거나 악의적인 제어 메시지 전송을 통한 임의의 대역폭 할당 및 타인의 대역폭 축소 등의 공격위협이 존재한다. 또한 광대역 환경에서 악의적인 대량트래픽 발생을 통한 DDoS 공격위협은 기존보다 큰 파급효과를 미칠 것으로 예상된다.

접속계층은 유선망, 무선망, 방송망으로 구분되며 광대역과 이동성을 보장하는 접속기술로 구성된다. 다양한 단말로부터의 과다 트래픽이 네트워크로 유입될 수 있으며, 이동성 보장에 따른 공격위치의 다양화로 역추적이 어려울 수 있다. 또한, 기존과 마찬가



(그림 5) VoIP 서비스 정보보호 위협

지로 사용자 데이터에 대한 도청위협이 존재하며, 특히 전송매체를 공유하는 무선망에서 보다 취약할 것으로 예상된다.

2. 신규서비스의 정보보호 위협

상용화 단계에 있는 VoIP, DMB, RFID서비스에 대한 정보보호 위협을 살펴보면 다음과 같다.

가. VoIP 서비스의 정보보호 위협

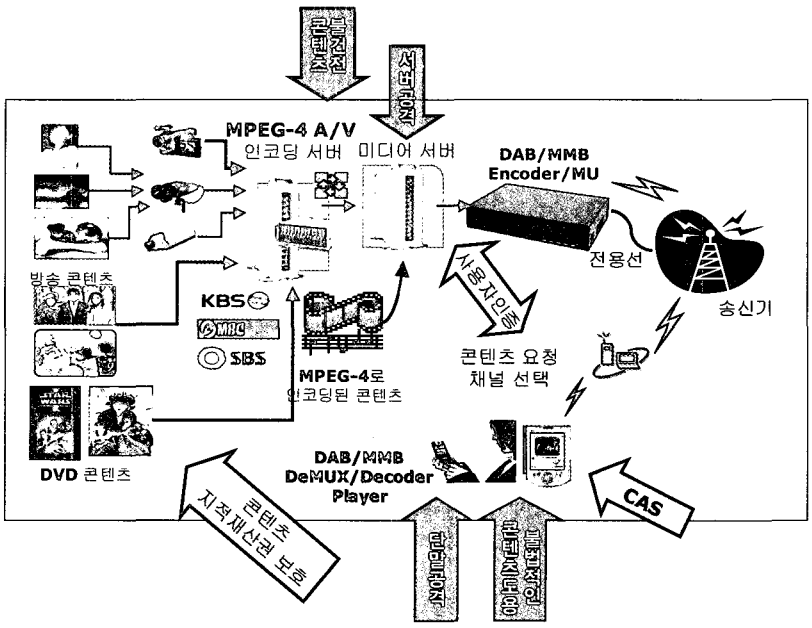
VoIP 서비스 환경은 IP 기반 망에서 발생할 수 있는 위협을 모두 고려할 수 있지만, 여러 위협 중에서도 가장 문제가 될 수 있는 주요 보안위협들은 (그림 5)에서와 같이 요약할 수 있으며, 각 요소에 대한 설명은 다음과 같다.

음성 트래픽을 불법으로 스니핑하여 재생 또는 특정 정보를 수집할 수 있으며, TCP/IP 프로토콜의 취약점을 악용하여 발신주소를 조작하고, 이를 통해 정상적인 사용자로 위장할 수 있다.

시스템의 정상적인 보호수단을 우회하여 합법적 이용자로 가장하려는 재사용 공격위협이 존재하며, 불법적인 제 3자가 양단간 통신에 개입할 수 있는 권한을 획득하여 정당한 통신주체로 참여하는 중간자 공격위협이 존재한다.

VoIP 스팸 및 음성메일 폭탄 공격을 통해 불특정 다수에게 음성광고 메시지로 대량으로 보냄으로써 음성사서함을 무용화시키는 현상 등은 외국의 사례에서도 보고된 바가 있다.

마지막으로, 인증 받지 않은 불법 VoIP 단말이나 시스템이 망에 접속하여 정상적인 시스템으로 위장할 수 있으며, SIP 서버와 같은 주요 시스템에 대한 자원을 고갈시키거나 독점 · 파괴하여 해당 시스템이 서비스를 제공하지 못하도록 무력화할 수 있는 DoS 공격위협이 존재한다.



(그림 6) DMB 서비스 정보보호 위협

나. DMB 서비스의 정보보호 위협

현재의 DMB 서비스 구축 상황은 이동 DMB 단말기에서 방송서비스만 수신할 수 있는 단방향 통신만이 가능하며, 금년에 리턴채널이 구축되어 전자상거래 등 다양한 부가서비스가 제공될 예정이다. 양방향 서비스가 제공되는 상황을 고려한다면, IP 기반 망에서 발생할 수 있는 위협을 모두 고려할 수 있으며, 리턴채널로 WiBro가 대표적인 접속기술로 대두되고 있으므로, WiBro환경이 가질 수 있는 정보보호 위협을 분석하고 그에 대한 대책을 마련하는 노력이 병행되어야 할 것이다.

현재의 단방향 서비스 환경을 중점적으로 고려하여, 문제가 될 수 있는 주요 보안위협들은 (그림 6)에서 간략하게 보여주고 있으며, 이를 보다 자세하게 살펴보면 다음과 같다.

첫째는, 허가받은 사용자만 적법하게 사용할 수 있도록 제어하는 CAS에 대한 불법적인 해독을 통해 불법적으로 콘텐츠를 도용할 수 있는 위협이 존재한다.

둘째, 프로그램 공급자의 미디어 서버 등 서비스 제공관련 서버들에 대한 공격으로 컨텐츠 유출 및 DMB 서비스 가용성 침해위협이 존재한다.

셋째는 리턴채널로써 휴대인터넷 및 이동통신 기술이 사용될 경우, 리턴접속 망의 취약성을 이용한 통신 데이터 도청 및 비인가 접속 등의 공격위협이 존재한다.

마지막으로, 위성 DMB 서비스에서 음영지역에 대한 방송신호 중계역할을 담당하는 갭필러를 효과적으로 관리하기 위한 갭필러관리시스템에 대하여 가용성을 침해하는 공격 위협이 존재한다. 갭필러관리시스템은 원격 상태 모니터, 고장감시, 제어 및 각종 통계 등의 중요한 역할을 수행하므로, 악의적인 공격에 노출될 경우 위성 DMB 서비스에 커다란 장애를 유발할 수 있다.

다. RFID 서비스의 정보보호 위협

RFID 서비스를 제공하는데 있어서 가능한 공격은 (그림 7)에서 보여주고 있으며, 각 위협요소에 대해서는 RFID 서비스 구성요소가 가지는 정보보호 위협과 통신구간에서의 위협으로 구분하여 살펴본다.

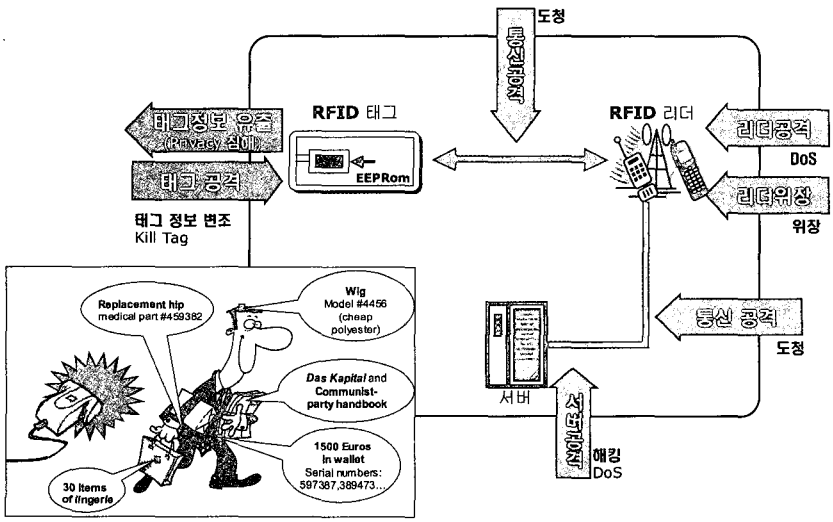
RFID 태그는 가장 기본적인 구성요소로써, 태그를 부착하는 물품의 정보를 담고 있기 때문에 가장 중요하게 보호해야 할 구성요소이다. 저장되는 정보에는 물품에 대한 식별코드 값과 그 외의 부가정보가 입력된다. 이때, 저장되어져 있는 식별코드 값을 변경함으로써, 다른 물품으로 인식되도록 할 수 있다. 현재 EU에서는 새로 발행하는 지폐에 RFID 태그를 부착하려고 한다. 만약 이러한 상황에서 100유로화에 부착된 태그 정보를 읽은 다음, 10유로화에 부착된 태그에 삽입한다고 하면, 10유로화는 RFID 리더기에서는 100유로로 인식 될 것이다.

(그림 7)에서 보듯이 RFID 태그와 RFID 리더기 사이의 무선 통신상에서 전송되는 데이터를 공격자가 도청할 수 있는 취약점이 존재한다. 또한 RFID 태그에 통신요청을 무한적으로 발생시킴으로써 RFID 태그가 필요한 시기에 적합한 RFID 리더기와의 통신을 수행하기 어렵게 만들 수 있으며, 악의적인 가짜 RFID 리더기가 RFID 태그와 통신하여 RFID 태그가 부착된 사용자에 대한 모든 정보를 얻을 수 있는 위협이 존재한다. 앞에서 언급한 부분은 개인의 프라이버시와 관련된 부분으로, 현재 가장 중요한 취약성으로 부각되고 있다.

마지막으로, RFID 리더기는 RFID 태그에서 읽은 물품 식별번호를 이용하여 관련정보를 저장하고 있는 서버에 추가정보를 묻거나, 정보를 전달한다. 이러한 과정에서 정보에 대한 도청 및 위변조 위협과 관련 서버에 대한 DoS 공격 위협이 존재한다.

IV. 정보보호 대응전략

이제까지 BcN과 VoIP, DMB, RFID 서비스에 대한 정보보호 위협을 살펴보았다. 본 장에서는 안전한



(그림 7) RFID 서비스 정보보호 위협

BcN 인프라 환경을 구축하기 위한 대응전략과 VoIP, DMB, RFID 서비스 각각에 대한 정보보호 대응전략을 살펴보고, 안전한 유비쿼터스 환경 구현을 위한 정책적 대응전략에 대해 살펴본다.

1. 안전한 네트워크 인프라 구현을 위한 대응전략

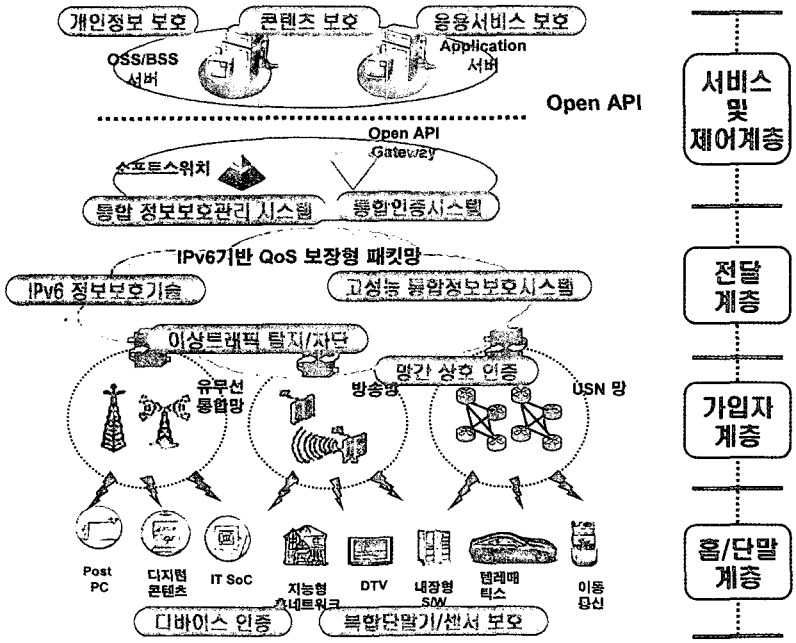
BcN 정보보호 위협에 대비하여 BcN에 적용되어야할 주요 정보보호 요소들을 (그림 8)에서 보여주고 있으며, 각 계층별 기술적 대응방안 다음과 같다.

서비스계층에서는 응용서비스에 대한 불법접근 및 권한오용을 방지하기 위해 접근제어 및 인증기술이 적용되어야 하며, 프라이버시 침해방지를 위해 사용자 개인정보보호 기술이 적용되어야 하고, 다양한 컨텐츠에 대한 콘텐츠 지적재산권 보호(DRM) 기술이 적용되어야할 것이다.

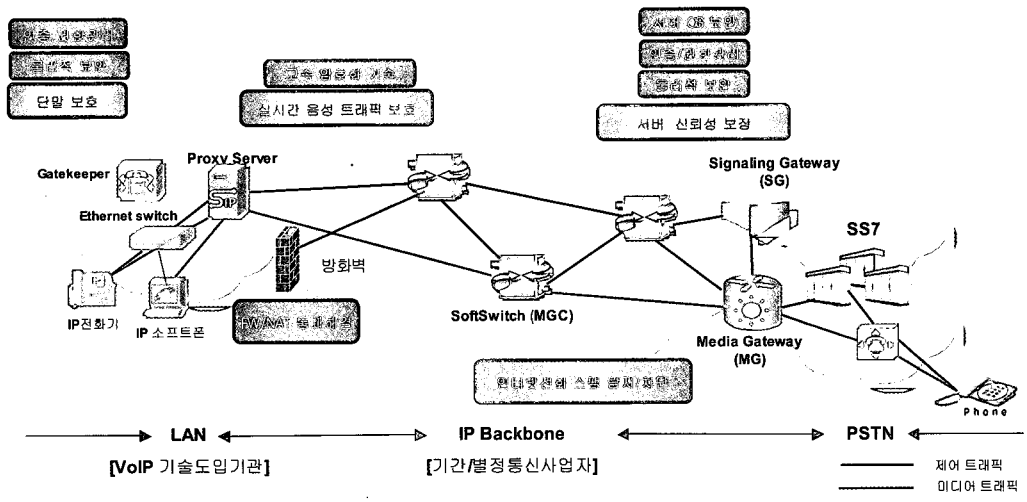
제어계층에는 개별 정보보호 장비간 연동 및 제어를 통해 전체 네트워크를 보호할 수 있는 통합정보보호관리 기술이 적용되어야 하며, 보안관리, 과금, QoS 관리 등 중요 제어 시스템의 신뢰성을 보장할 수 있는 기술이 적용되어야 하며 관련정보의 유출 및 위변조를 방지하여야 한다.

전달계층에서는 백본 네트워크의 처리능력에 따른 능동 고성능 네트워크 보안기술이 필요하며 사이버 공격이 지능화, 고속화, 다양화됨에 따라 DDoS 공격에 대응할 수 있는 지능형 이상트래픽 탐지/차단 기술이 마련되어야 한다.

접속계층을 살펴보면, 사용자로부터의 유해트래픽을 사전에 차단하여 전달계층에 피해가 미치지 않



(그림 8) BcN 정보보호 서비스



(그림 9) VoIP 정보보호 서비스

도록 해야 하며, 이기종 망간의 연동에 있어서 망간 상호인증이 필요하다. 또한, 이동 단말에 대한 로그정보 등 역추적을 위한 정보를 통합보안관리 시스템에 제공하여야 한다.

2. 신규서비스의 안전 및 신뢰체계 구축을 위한 대응전략

앞서 살펴본 VoIP, DMB, RFID 서비스에 대한 안전 및 신뢰체계 구축 방안에 대해 살펴보면 다음과 같다.

가. VoIP 서비스의 안전 및 신뢰체계 구축

VoIP 정보보호 요구사항은 VoIP 프로토콜의 보안 특성과 IP 기반 환경에서 현재 알려진 취약점 및 잠재적인 보안위협 유형을 이해하여 서비스 제공에 앞서 고려해야 하는 정보보호 목표라 할 수 있다. 안전한 망 설계방안과 장비 및 트래픽 보호, IP 보안위협에 대한 대책마련, 방화벽/NAT 통과문제 해결, 관리적 대책등이 세부내용이다. 더불어 본격적인 서비스 상용화를 대비하여 예상할 수 있는 역기능을 최소화하기 위한 노력이 강구되어야 한다. 실시간 멀티미디어 서비스에 적합한 암호화 기술개발과 안전한 VoIP 응용서비스 제공 방안, 보안 기술간 상호 운용성 확보 방안 및 QoS 상충 문제 해결 등은 머지않은 시점에 해결되어야할 이슈들이다. (그림 9)는 안전한 VoIP 서비스 제공을 위해 VoIP 서비스를 구성하는 구성요소와 통신구간상에서 적용되어야할 세부 정보보호 기술들을 보여주고 있다.

나. DMB 서비스의 안전 및 신뢰체계 구축

DMB 사용자 단말에는 방송서비스와 향후 리턴채널을 이용한 다양한 서비스를 제공하기 위한 운영체제와 미들웨어 시스템이 탑재된다. 따라서 단말기 플랫폼을 보호하기 위한 보호대책이 마련되어야 하며, 특히 수신제한 기능을 담당하는 CAS 기능에 대한 신뢰성 보장과 접근통제 및 권한 오용 방지기능이 제공되어야 한다.

멀티미디어 콘텐츠를 제공하는 미디어 서버에 대한 공격으로부터 보호하기 위해 접근통제 및 권한, 플랫폼 보호 기능이 적용되어야 하며, 악의적인 유해 콘텐츠의 배포를 막기 위한 불건전 유해 콘텐츠 필터링 기능이 탑재되어야 한다.

불법적인 디지털 콘텐츠 도용 및 분배 등을 방지하기 위한 디지털콘텐츠 보호 기술이 적용되어야 한다. 특히 유료 방송 서비스를 제공하기 위한 CAS의 무단 복제를 통해 비인가자에 의한 유료방송 청취에 대한 대책을 마련하여야 한다.

마지막으로, 위성파 방송신호를 음영지역에 고르게 중계해주는 역할을 담당하는 갭필러를 관리하기 위한 갭필러관리시스템의 가용성을 침해하는 공격에 대한 대책을 마련해야 할 것이다.

다. RFID 서비스의 안전 및 신뢰체계 구축

RFID 태그에 저장된 정보를 보호하기 위해 강력한 암호 알고리즘으로 RFID 태그에 저장되는 데이터를 암호화할 필요가 있다. 또한 RFID 태그에 존재하는 특수한 정보를 이용하여 물품정보를 암호화 하여 RFID 태그에 저장되어져 있는 물품정보를 다른 RFID 태그에 쉽게 적용할 수 없게 하여야 한다.

RFID 태그와 RFID 리더간의 통신을 보호하기 위해 RFID 태그와 RFID 리더기 사이의 통신은 반드시 암호화가 이루어져야 한다. 하지만, RFID 구성요소 취약점에서 언급 했듯이 RFID 태그의 특징으로 인해 강력한 암호화 알고리즘을 사용하지 못한다는 점에서 많은 취약점이 존재 할 것으로 보이며, 많은 공격 행위가 이와 같은 취약점을 이용 할 것으로 보인다. 또한 불법 RFID 리더가 태그 정보를 유출하는 것을 방지하기 위해 RFID 태그와 RFID 리더기 사이에 적합한 인증과정이 필요하며, RFID 서비스에서 물품정보 및 기타 부가정보를 저장하고 있는 OIS, ODS 시스템 보호 및 저장 정보의 위변조를 방지하기 위한 정보보호 기술이 적용되어야 한다.

3. 안전한 유비쿼터스 환경 구현을 위한 정책적 대응전략

BcN 망은 이기종망간, 타사업자간 연동되는 통합망이다. 따라서 특정 망에서의 침해사고는 타 망에 전파될 수 있으며, 특정 취약망으로 인해 대다수 사용자에게 안전한 서비스를 제공하지 못할 수 있다. 따라서 침해사고에 효과적으로 대응하기 위한 이기종망 및 타사업자와의 협조체계가 필요하다. 서로 정보보호 위협 및 침해사고 정보를 공유하고, 대응전략을 수립하는 등의 이종망 및 타사업자간의 통합보안관리 체계가 구축되어야 할 것이다.

BcN은 서비스 품질을 보장하는 네트워크이다. 하지만, 다양한 접속기술을 가지는 복합단말기의 등장에 따른 접속망 변경과 단말기의 이동성에 따른 핸드오프로 인하여 빈번한 인증절차를 요구하게 되며, 이로 인해 서비스 품질저해와 사용자불편을 유발할 수 있다. 따라서, 서비스 품질에 영향을 최소화하고 사용자의 편리성을 도모하기 위해 통합인증 기술이 마련되어야 한다.

현재, BcN 시범사업이 개통되어 상용화를 앞두고 있다. 이러한 시점에서 BcN 시범사업에 대한 정보보호 안전성 점검을 통해 세부대책을 마련하도록 하고, 연구소 및 정보보호 업체에서는 BcN에 필요한 기술 및 제품을 개발하도록 유도하는 노력이 필요하다.

또한, 새로이 창출되는 신규 서비스에 대해서도 사전 보안성 평가를 수행하여 안전한 서비스환경을 구축하도록 유도하고, 이를 통해 사용자 신뢰를 확보하도록 함으로써 원활하게 서비스가 제공되도록 하여야 할 것이다.

많은 인터넷 침해사고 등을 살펴보면, 오염된 단말기가 트래픽의 진원지로 파악되고 있다. 이에 따라 가

입자 단말기에 대한 정보보호의 필요성이 크게 중요시되고 있으며, 가입자 망에서 유해트래픽에 대한 사전 탐지 및 차단기능에 대한 요구가 증가하고 있다. 따라서 가입자 단까지 보안기능을 확대하여, 유해트래픽을 사전에 차단할 수 있는 체계 구축이 필요하다고 하겠다.

마지막으로, 정보보호는 어느 한부분에서 대비한다고 이루어지는 것이 아니라, 사업자, 정부, 기업, 개인 등 모두가 역할을 수행하여야 한다. 일반적으로, 가입자들은 정보보호 측면에서 인식이 부족하며, 정보보호를 위해 투자하기에 여력이 없는 중소기업이 많이 존재한다. 또한, 사업자 측면에서는 다양한 정보보호 서비스를 기획하고 있다. 따라서, 인식이 낮은 가입자에 대하여 안전하게 통신할 수 있도록 하고, 중소기업에서는 저렴한 가격으로 원하는 수준의 정보보호 서비스를 제공받도록 하며, 정보보호 서비스를 준비하고 있는 사업자는 서비스에 대한 검증을 수행할 수 있도록 하는 정보보호 시범서비스를 고려할 수 있다. 결국, 정보보호 서비스가 보편화 된다면, 전체 통신환경도 보다 안전한 환경으로 정착될 것이다.

V. 결 론

최근의 사이버공격은 시스템 및 네트워크의 취약점을 악용하여 고속으로 전파되는 양상을 띠고 있다. 또한, 웜 · 바이러스 및 해킹 기술이 결합되어 공격의 확산속도와 파괴력은 점점 커지고 있다. 또, 최근에는 위장 사이트와 이메일을 이용하여 개인 정보를 수집하는 피싱(Phishing) 기법을 사용하여 타인의 은행예금을 불법 인출하는 사고가 증가 추세에 있으며, 다양한 공격도구에 의하여 중요한 정보가 유출되는 사고가 발생하기도 하였다. 이런 사례에서 볼 수 있듯이 미래 IT 환경에서는 경제, 사회, 국방 등 국가사회 전체에 치명적인 피해를 끼칠 수 있는 지능화된 사이버공격이 지속적으로 증가할 것으로 예상된다.

지금 우리는 세계 IT 산업의 발전을 선도하는 IT839전략을 수립하고 그 성공적인 구현을 위한 방안을 마련하고 추진하고 있다. IT839전략은 고도화된 네트워크 인프라를 기반으로 유 · 무선망과 방송망을 통합망으로 개편하고 일상생활의 각 부문을 유비쿼터스 컴퓨팅 환경으로 구성하여 인류 역사를 전환할 디지털 혁명을 가져올 것으로 기대된다. 2005년을 기점으로 BcN 및 몇몇 서비스는 상용화 단계에 접어들고 있다. 그러나 이러한 IT839전략으로 구현된 정보통신 환경에서 사이버공격이 발생할 경우, 사회의 거의 모든 부문에서 커다란 위험에 처하게 될 것이고, 그 피해의 범위 또한 통신 두절, 화재, 자동화된 농장의 동식물 폐사 등에까지 미칠 수 있을 것이라 예상된다.

본 고에서는 이러한 통합 IT환경에서 우리가 직면할 정보보호 문제를 해결하기 위하여 현재 상용화 단계에 접어들어 시급히 정보보호 대책이 마련되어야 하는 BcN과 VoIP, DMB, RFID 서비스에 대한 주요 위협을 분석하고 이에 대한 정보보호 추진전략을 제안하였다. 본고의 정보보호 추진전략은 사이버 위협에 대한 국제 협력 및 공조의 강화, 정부, 기업, 개인의 정보보호 책임과 의무에 대한 인식, 그리고 그 실천이 병행될 때, 더욱 효과적으로 추진되어 안전한 u-Korea 구현을 위한 초석이 될 것으로 기대된다.

이홍섭

1974년 ~ 1979년 한양대학교 전자공학과 학사
1982년 ~ 1985년 한양대학교 전자공학과 석사
1996년 ~ 1999년 대전대학교 컴퓨터공학 박사
1980년 ~ 1996년 한국전자통신연구원 실장
책임연구원
1996년 ~ 2004년 한국정보보호진흥원 기반시설 보호 단장, 평가인증사업단 단장, 기술본부장
2004년 ~ 2005년 아시아 PKI포럼 의장
2004년 ~ 현재 한국 PKI포럼 의장
2004년 ~ 현재 한국정보보호진흥원 원장
2005년 ~ 현재 아시아 PKI포럼 부의장