

主題

유비쿼터스 환경에서의 정보보호 추진전략

한국정보보호진흥원 원장 이홍섭

차례

- I. 서 론
- II. 정보보호 환경의 변화
- III. 유비쿼터스 환경의 위협요소
- IV. 정보보호 대응전략
- V. 결 론

I. 서 론

정부는 미래 정보기술(IT) 환경을 주도할 IT839전략을 역동적으로 추진하고 있다. IT839전략은 우리 경제의 주요 기반인 IT산업을 경쟁력 높은 미래형으로 끌어 올릴 핵심성장전략으로 '839'는 8대 서비스, 3대 인프라, 9대 신성장동력을 의미한다. 이 전략은 세계 최고 인프라를 바탕으로 국내 경제를 견인하고 있는 IT산업에 날개를 달자는 구상이다. IT839전략의 성공적인 구현은 국가산업 전반에 걸친 글로벌 경쟁력 확보, 고부가가치 창출, 대국민 서비스 질 향상, 기술 선진국 이미지 홍보 등 다양한 분야에서 많은 발전을 가져올 것으로 기대된다. 최근 IT의 발전은 통신망의 광대역화, 통신·방송·정보 등 기술의 융합화를 가속화하고 있으며, 수많은 사물에 전

자태그(RFID)나 컴퓨팅 기능이 부가되고 네트워크화되는 유비쿼터스 시대 진입도 가까이 다가와 있다.

하지만, IT가 발전하고 통신망의 개방성과 상호의존성이 커질수록 사이버공격에 대한 위협도 증가하게 마련이다. 특히, IT839전략으로 유·무선, 통신·방송망이 융합되어 다양한 멀티미디어 서비스가 제공되는 환경에서는 기술발전에 따른 경제적 이익과는 별도로 고도화된 통신·방송 융합망을 통하여 확산되는 침해사고가 현재와는 다른 양상으로 전개될 것으로 예측된다. 즉, 지능화되고 커다란 파괴력을 가지게 된 웜·바이러스가 초고속의 통신·방송 융합망을 통하여 전국적으로 유포되고, 지금까지는 공격대상이 아니었던 부문에까지 공격이 확산될 것으로 예측된다. 그러므로 새로운 환경에 나타날 위협을 미리 분석

하고 적절한 대응책을 마련하지 않는다면, 2003년 국내 인터넷망을 마비시켰던 1.25 침해사고보다 더 치명적인 사고가 발생할 가능성도 배제할 수 없다. 이는 차세대이동통신, 홈네트워크, 텔레메티스 등 현재 우리가 역점을 두어 추구하고 있는 정보화 노력에 커다란 피해를 줄 수 있음을 의미한다.

따라서, 본 고에서는 정보보호 환경의 변화를 분석하여 예상되는 미래의 위협요소를 도출한 후, 유비쿼터스 환경에 대비한 정보보호 추진전략을 제언하고자 한다.

II. 정보보호 환경의 변화

1. 유비쿼터스 사회로의 진입

가. IT인프라의 광대역화, 편재화 진행

통신기술의 발전으로 통신·방송·인터넷이 통합되는 광대역통합망(BcN)을 통해 더 많은 용량의 데이터를 더 빠르고 끊김 없이 안전하게 제

공할 수 있는 환경으로 진화하고 있다. 전달망은 테라급 전송능력과 서비스 품질(QoS) 보장을 제공하는 구조로, 가입자망은 광대역 가입자망으로 발전하고 있으며, 유선망은 물론 무선망의 광대역화를 통해 가입자당 50~100Mbps 대역제공이 가능한 초고속 통합망 서비스를 제공할 전망이다. 또한 유비쿼터스 기술의 진보로 UWB(Ultra WideBand), 스마트센서 기술 등 센서네트워크의 원천기술을 개발하여 BcN과 연동시킴으로써 편재된 컴퓨팅 환경 구현이 가능할 것으로 예상된다.

IT인프라의 발달로 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 민원 서비스를 제공받을 수 있고 사이버 의정, 전자국회 등의 서비스로 확대될 전망이며, 기업측면에서는 전자무역, 인터넷 회상회의, ERP·CRM·SCM 등 기업정보화가 확대됨에 따라 기업의 획기적인 효율성·생산성 향상이 예상된다.



[그림 1] IT인프라의 광대역화 및 편재화에 따른 서비스 확대

신규 IT서비스의 융합화되고, 개인화되고, 지능화되면서 개인의 라이프스타일에도 큰 변화가 예상된다. IT의 발전으로 디지털 컨버전스가 빠르게 진행되면서 IT서비스는 개인의 니즈(Needs)를 적극 수용하여 융합화·개인화·지능화된 서비스로 진화하여 융합형 멀티미디어 서비스, 원스탑 서비스(One-Stop Service) 등 편리한 서비스 이용이 증가할 것이며, 휴대단말의 발전, 고품질의 멀티미디어 VoD 서비스 및 개인 맞춤형 방송의 증가 등 개인화된(Customized) 서비스가 증가할 것이다. 또한 로봇, 차세대 PC, 센서의 발달로 인텔리전트 에이전트 기술이 발달함에 따라 편리하고 지능화된 환경으로 진화되며 정보 가전, 산업기기 등은 IT와 결합하여 지능화된 제3의 새로운 서비스 등이 지속적으로 창출될 것으로 전망된다.

나. 사이버공격의 고도화와 피해증가

정보기술의 진전으로 삶의 편리성과 효율성은 크게 향상되었지만, 사이버 공격으로 인한 위협과 피해도 빠르게 증가하고 있다. 최근의 사이버 공격은 이전의 시스템 침입이나 웜·바이러스로 인한 파일 변조, 자료 유출 등 개별시스템과 개인에 대한 공격에서 원격 조정이 가능한 해킹도 구를 사용한 정교한 타겟 공격이나, 웜·바이러스 등을 통해 대량의 트래픽을 발생시킴으로써 인터넷 망 기반구조를 공격하는 형태로 변화되고 있다. 최근 사이버공격의 주요한 특징 및 향후의 전망을 살펴보면 다음과 같다.

o 웜·바이러스와 해킹의 결합으로 지능화, 고도화된 사이버공격 증가

최근의 사이버공격은 웜·바이러스에 취약점 자동스캔, 자체 메일발송엔진, 감염PC 원격제어 등 해킹 기술이 결합되어 능동적으로 확산대상을 탐색하고, 감염시킨 대상을 특정 사이트를 공격

하는 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, 개인의 판단에 따라 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.

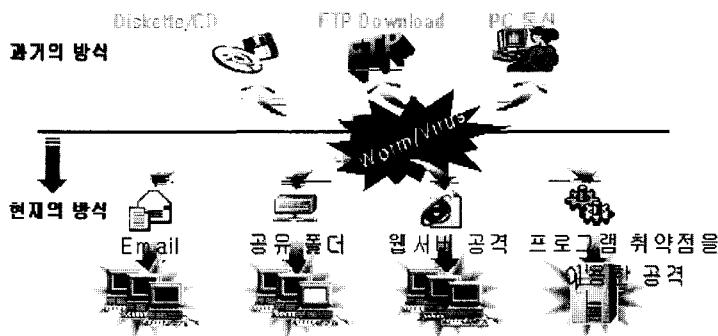
o E-MAIL, 취약점, P2P 등 웜·바이러스 전파경로의 다원화

과거에는 웜·바이러스의 확산 경로가 PC통신 등을 통한 파일 다운로드나 디스크의 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 의한 피해가 급속히 늘어나고 있다.

o 초단기/초고속 사이버공격의 출현

최근의 개인 PC는 불과 몇 년 전 특별한 용도에만 사용되던 고성능 서버의 성능을 능가하는



(그림 2) 공격의 다양성

성능을 가지고 있고, 개인 PC들이 접속된 인터넷의 속도도 매우 빠르게 높아지고 있다. 이러한 고성능 개인 PC의 보급과 보편화된 광대역 네트워크는 초고속으로 공격을 확산시키는 역할을 하고 있다.

또한 소프트웨어가 포함하고 있는 보안취약성에 대한 공격 추이를 보면, 보안취약성의 발표 후 이에 대한 공격이 이루어지는 기간이 점점 짧아져 MS SQL의 취약점을 공격했던 슬래머 웜의 경우 6개월 이상의 시간이 걸렸으나 Sasser와 같은 최근의 웜들은 이 시간이 불과 2주 정도로 단축되었다. 이와 같은 추세로 가까운 시일 내에 취약점에 대한 패치가 발표되기 전에 공격이 이루어지는 Zero-Day 공격이 출현할 것으로 예상된다.

III. 유비쿼터스 환경의 위협요소

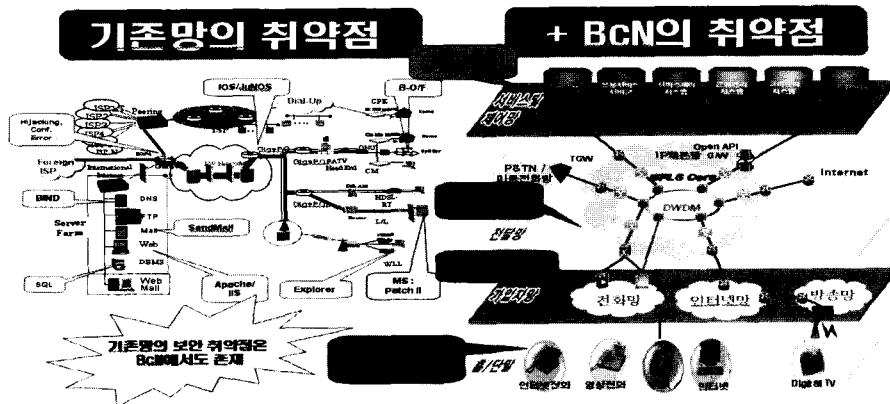
유비쿼터스 환경에서는 BcN, USN, IPv6 등 3대 인프라의 도입 및 통신·방송의 융합으로 사이버 위협의 대상은 IP를 사용한 특정 망에서 통합된 망으로 전이되어 피해 확산 속도가 증가되고, 피해 규모 역시 확대될 것으로 예상된다. 흡네트워크, 텔레매티кс 등 서비스 융합화가 본격

적으로 진행되면서 사이버 위협이 ALL-IP망으로 확대될 것으로 예상된다. 또한 9대 신성장 IT 디바이스의 정보보호 기능이 미흡한 경우에는 기기의 신뢰성 저하, 서비스 장애 등의 위협을 초래할 것으로 예상된다.

본장에서는 네트워크 융합에 따른 위협 및 피해의 확산, 새로운 신규서비스의 취약한 보안기능, 지능형 정보기기의 보안취약성, 등 유비쿼터스 환경의 도래에 따른 주요한 정보보호 위협요소에 대하여 고찰해 보고자 한다.

1. 네트워크 융합에 따른 위협 및 피해 확산

BcN 환경에서는 아래 그림과 같이 기존 인터넷망에 잠재된 취약점에 추가적으로 망 융합에 따른 신규 보안 위협이 나타날 것으로 예측된다. 첫째, 네트워크의 광대역화로 악성코드의 전파 역시 급속하게 진행되어 취약한 네트워크 기반을 마비시킬 수 있다. 둘째, 기존에 별도로 운영되고 있던 방송·통신망 등이 통합되어 구성·운영되므로 공격에서 상대적으로 안전했던 전화망, 방송망으로 공격이 전이되어 피해 범위 확산이 우려된다. 셋째, 휴대폰, PDA등 기능이 융합된 단



[그림 3] BcN 환경에서의 보안위협

말기와 환경을 구성하는 RFID 등 내장형 장치들을 대상으로 한 해킹 및 웜·바이러스가 발생할 것으로 예측되며, 이들이 네트워크 기반을 공격하는 경우 현재의 개인용 PC에 의한 공격보다 공격이 매우 넓은 범위에서 이루어져 현재보다 더욱 위협적일 것으로 예측된다.

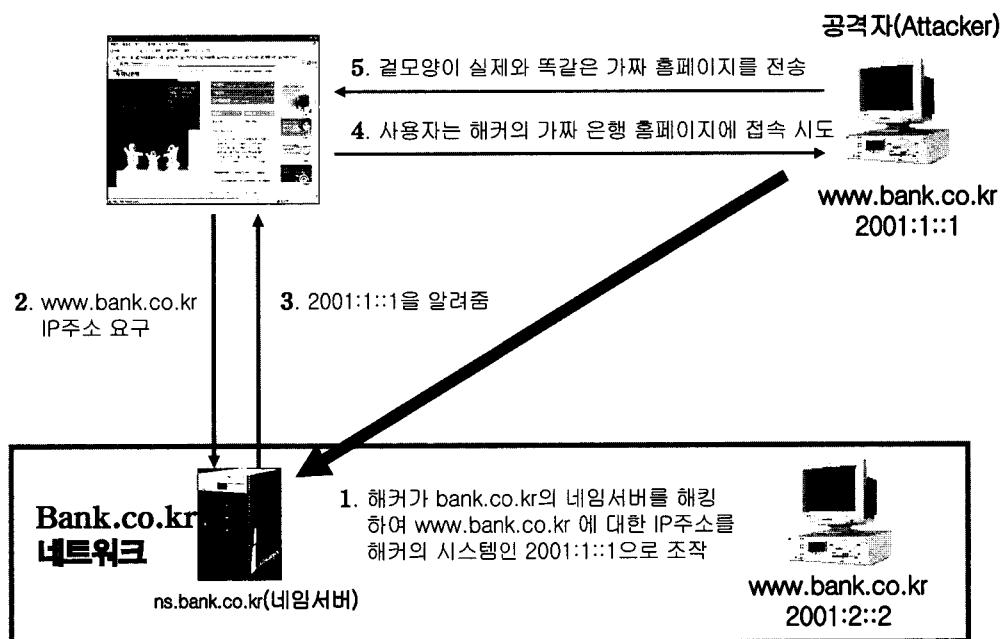
USN 환경에서는 고객 맞춤형 서비스 제공을 위해 도처에 설치된 센서를 통해 고객의 위치정보 등을 수시로 수집하므로 프라이버시 침해 위험이 증가할 것으로 예측된다. 특히 도처에 설치된 센서를 통해 수집된 정보가 오·남용되어 이용자에 대한 24시간 감시시스템의 역할을 수행하게 되면 개인의 프라이버시가 크게 손상될 수 있다. USN 환경에서 사용되는 이동단말, 센서 등은 CPU와 배터리의 용량이 적기 때문에 보유자원을 집중적으로 소모시키는 공격을 받을 경우 전체 서비스의 중단 발생 가능성이 높다. 또한 USN은 보안기능이 상대적으로 취약한 Ad-hoc 네트워크 구조로 구축되어 이동단말기기에 대한 통제가 어려워 사이버 공격에 대한 취약성이 가중될 것으로 예측된다.

IPv6는 자동환경 설정(Autoconfig), 이웃노드 탐색(Neighbor Discovery), Mobile IP 등의 기능이 추가되면서 기존 공격을 변형한 새로운 유

형의 헤더조작, 바이러스·웜 등의 공격이 발생할 것으로 예측된다. IPv6망으로 완전히 전환하기 전에 과도기적으로 IPv4와 IPv6의 병행 사용이 요구되어 End-to-End 네트워크 보안이 어려울 수 있다. 홈네트워크 장비 등 IPv6가 장착된 장비가 다양해지면서 사이버공격의 대상 또한 급격히 증가할 위험이 크다. 또한 IPv6환경에서는 DNS에 대한 의존도 증가로 아래 그림과 같은 주소 위·변조 등을 통해 인터넷 사용자를 속이는 피싱(Phishing) 공격이 증가할 것으로 예측된다. 2004년 가트너그룹 조사에 따르면 2003년 미국에서만 피싱으로 23억 달러의 손실이 발생했다.

2. 새로운 신규서비스의 보안기능 취약

IT839전략의 본격적 추진으로 신규 IT 서비스가 지속적으로 출현할 것으로 예상되지만, 신규 IT 서비스의 보안성 강화를 위한 제도적인 장치는 아직 미흡한 상황이다. 신규 서비스의 융합화, 복잡화에 따른 서비스의 보안결합 발견 및 해결 비용의 증가로 보안 서비스 품질에 대한 서비스 사업자의 관심과 투자가 상대적으로 저조한 상황이다. IBM에서 발표한 아래의 보안결합 탐지 비율 비교를 보면 보안의 결함은 서비스의 설계 단

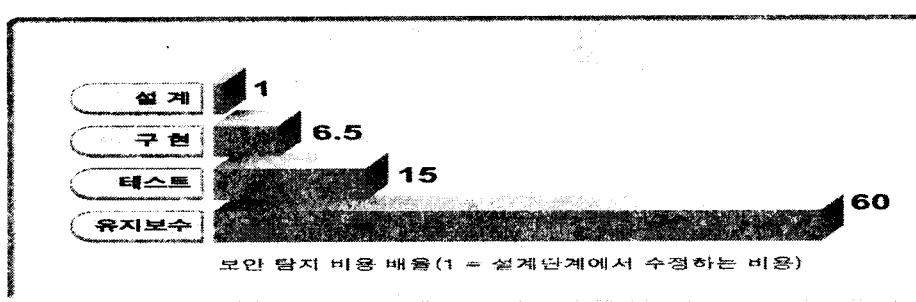


[그림 4] IPv6 DNS 정보 위·변조해킹의 예

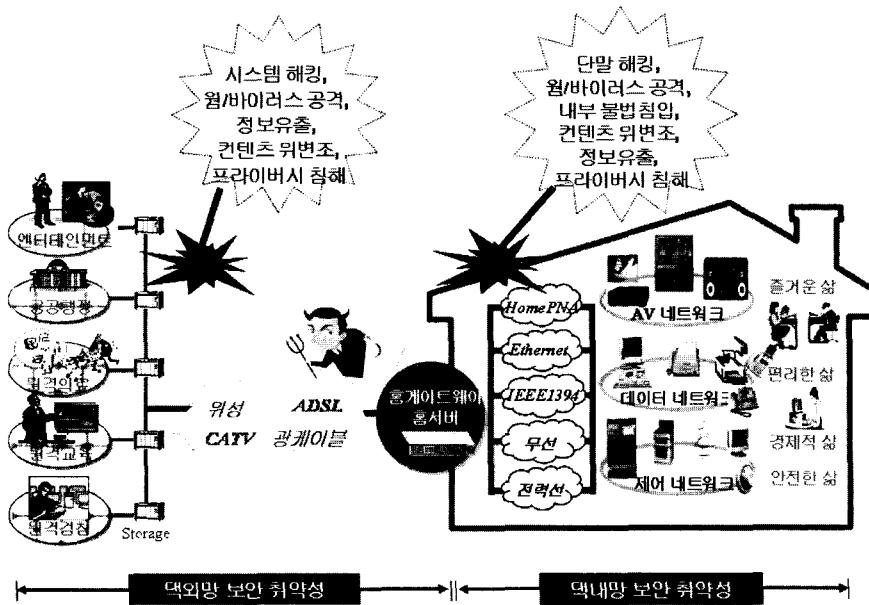
계에서 가장 적고, 보안결함 수정에 소요되는 비용은 생명주기 후반으로 갈수록 커지며 특히, 운영단계에서는 설계단계에 비해 60~100배 증가하고 있는 것을 알 수 있다. 따라서 신규서비스의 설계 단계에서부터 서비스의 신뢰성 및 사용자의 안전을 보장하기 위해 사전영향평가와 같은 제도적인 장치가 요구된다.

또한 신규 IT 서비스에 적합한 인증체계가 현

재 마련되어 있지 못하다. 현재의 공인인증서비스는 센서, RFID 태그 등 수많은 디바이스가 존재하는 IT 서비스 환경에서의 인증서비스를 제공하기에는 부적합하다. 또한 유·무선 통신망 관련 신규 IT 서비스의 인증체계 취약으로 ID 도용 및 오남용 등 피해가 확산될 것으로 예측된다. 현재 사용자들은 다양한 종류의 많은 digital ID를 소유하고 있으며, 향후 그 종류와 수는 더



[그림 5] 보안 결함 탐지 비용 비교



[그림 6] 홈네트워크 보안 취약성

속 증가하게 되어 사용자의 ID 도용 및 오남용으로 인한 피해는 더욱 심화될 것으로 전망된다. 미 연방무역위원회(FTC, 2003.9)는 2002년 미국 내에서 ID 도난 피해자가 1천만 명에 달하며 피해 액수도 530억 달러에 이를 것으로 추정하고 있으며, 애버딘 그룹(Aberdeen Group)은 ID 도용으로 인한 경제적 손실이 2003년 한 해에만 전 세계적으로 약 2,210억 달러에 이르고, 그 피해가 연평균 300% 증가하면서 2005년에는 2조 달러에 이를 것으로 전망하고 있다.

3. 지능형 정보기기의 보안기능 미비

향후 많은 가정의 정보가전이 네트워크로 연결되는 홈네트워크 환경이 구현되면서 홈네트워크에 사용되는 정보기기의 보안 취약성으로 인한 위협이 증가할 것으로 예측된다. 홈네트워크 정보기기에 대한 불법적인 공격은 개인의 프라이버시 침해뿐 아니라 생명 및 재산에까지 직접적인 피해를 줄 수 있어 보안취약성에 대한 대응책 마련이 시급한 상황이다. 아래 그림은 홈네트워크에서 정보기기의 취약성으로 인해 발생할 수 있는 위협요소를 표시하고 있다. 홈네트워크 서비스는 의료·방범 등 고객맞춤형 서비스와 접목되면서 민감한 개인정보를 수시로 수집 및 저장하는 경우에 가정 내 주요 개인정보의 노출 위협이 증대할 것으로 전망된다. 또한 홈네트워크에서 사용하는 홈게이트웨이/홈서버와 다양한 험 기기 간의 보안 프로토콜 및 표준화 기술 미비로 인한 보안 취약성도 증가할 것으로 예측된다.

텔레매틱스에서 사용하는 정보기기의 보안 취약성으로 인한 위협도 새롭게 출현할 것으로 전망된다. 텔레매틱스에서는 이동통신망을 이용한 텔레매틱스 기기에 대한 사이버공격에 의한 서비스 장애가 우려된다. 즉 텔레매틱스 단말과 이동통신망 사이의 불법 사용자로 인한 ToS (Theft of Service) 공격 발생 가능성이 높으며, 텔레매틱스 기기에 대한 웹·바이러스, DoS 공격으로 인한 트래픽 폭주, 서비스 기능 마비 등이 예상

된다. 또한 실시간 인증기능 미비로 불법적인 PDA, 휴대폰 등을 통해 정확하지 않은 도로정보 제공 시 운전자의 불편이 가중될 수 있으며, 자동차 내 단말기를 통한 인터넷 사용, 홈쇼핑, 홈뱅킹, 주식거래 등 개인정보서비스 이용 시 단말기 불법 접근으로 인한 금전적 피해도 예상된다.

향후 다양한 차세대 이동통신 휴대 단말기들이 등장하면서 이들에 대한 웹·바이러스 공격, 불건전 스팸메일 범람이 예상된다. 무선환경에서 스팸은 동영상 형태의 MMS (Multimedia Messaging Service)를 이용한 멀티미디어형으로 변화할 것으로 예상된다. 2004년 9월초 서울과 대전 6개 고교 학생 4313명을 상대로 휴대전화 음란광고수신 여부 등을 설문조사한 결과, 2명 중 1명꼴(52%)로 음란광고 수신경험이 있을 정도로 위협이 크게 증가하고 있다. 이동환경에서 뱅킹, 주식거래 등의 다양한 비즈니스 거래가 늘어남에 따라, 휴대용 기기에 대한 웹의 위험도 증가할 것으로 예상된다. 표준 WIPI 무선 플랫폼의 보급은 단말로의 악성코드 유입과 확산 경로를 다양화할 것이다. 최근 2004년 6월 심비안 OS를 탑재한 노키아, 지멘스, 소니, 에릭슨 휴대폰에 카비르(Cabir)가 발생되었으며, 이는 대량 유포 위험도는 높지 않았지만, 모바일 단말에 대한 악성코드의 발생 가능성성이 더욱 높아졌음을 보여주고 있다.

IV. 정보보호 대응전략

위에서 살펴 본 유비쿼터스 환경에서의 보안 위협에 효과적으로 대응하기 위해서는 IT 환경의 변화에 따른 보안위협을 사전에 분석하여 신규 IT 서비스의 초기 단계에서부터 정보보호 대책을 적용하는 노력이 필요하다. 이 장에서는 안전한 네트워크 인프라 구현, 신규서비스 및 안전

및 신뢰체계 구축, 정보기기의 정보보호 기능강화 등 사이버 위협에 대처하기 위한 정보보호 전략을 고찰해 보고자 한다.

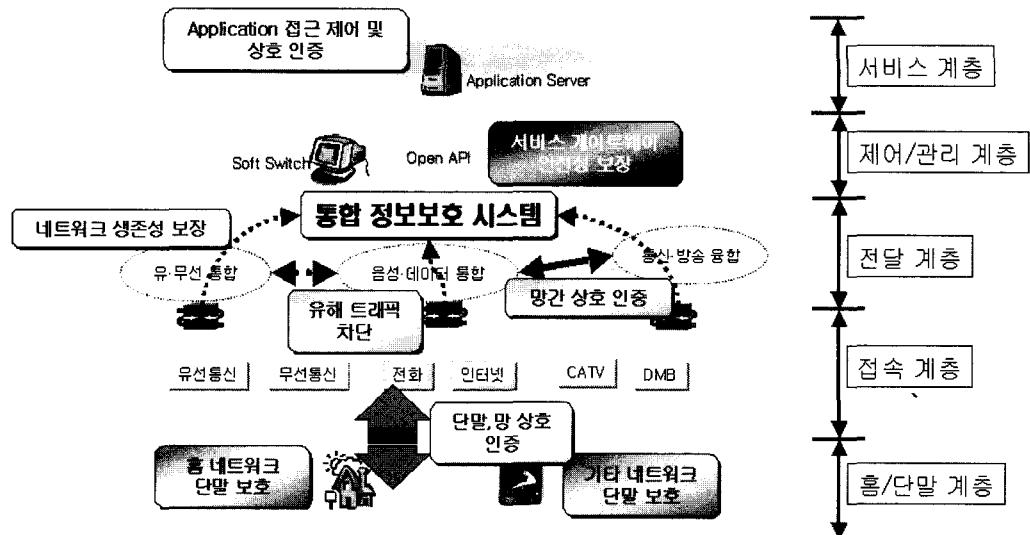
1. 안전한 네트워크 인프라 구현

네트워크 인프라의 보안위협에 대응하기 위한 정보보호 전략을 제시하면 다음과 같다. 첫째, 망융합에 따른 트래픽 모니터링 영역 확대 등 침해사고 발생 시 사전 감지 및 피해를 최소화할 수 있도록 사이버공격 예방 및 고도화 전략이 마련되어야 한다. 즉, 방송망 등에 대한 공격의 발생이나, 지능형 홈을 위한 제어센터 등에 대한 공격은 그 피해가 단순히 개인에 한정되지 않고 불특정 다수에게 미치기 때문에, 이와 같은 피해를 예방하기 위하여 공격을 조기에 탐지하고 피해를 예방하기 위한 대책이 필요하다.

둘째, 3대 침단인프라 환경에 적용 가능한 고성능 정보보호 요소기술 확보가 필요하다. 또한 이러한 정보보호 요소 기술들을 사물에 내장된 초소형 내장형 시스템들과 연계하여 능동적으로 공격에 대응할 수 있는 능동적 통합보안기술과, IPv4환경에서 IPv6로 안전하게 전환하기 위한 기술의 확보도 필요하다.

셋째, IPv6 또는 RFID/USN 등에 적용하기 위한 정보보호제품의 안전성 검증 및 정보보호 제품 간 상호 연동성 보장을 위한 표준 제정 및 표준적합성 인증 등을 위한 제도가 필요하다. IPv6가 적용된 환경에서는 매우 많은 정보기기들이 서로 연동되어 작동하고, 각각이 서로 다른 특성을 가지고 있으므로 각 기기들에 내장된 정보보호 기능들을 연동할 수 있도록 관련된 표준이 필수적으로 마련되어야 한다.

넷째, 방송망에 대한 사이버공격의 발생 등 망융합에 따른 정보보호 환경의 변화를 수용할 수 있고, 온·오프라인 상에서 개인의 프라이버시를 보장할 수 있도록 정보보호 관련 법·제도 정비



(그림 7) 광대역 통합망에서의 정보보호

가 필요하다. 기존의 방송망, 통신망 등이 분리된 환경에서는 각각의 영역에 따라 관련 법규가 존재하여 왔으나, 통합망 환경에서는 각 망의 영역을 특성에 따라 분리하기 어려우므로, 이와 같은 환경에서 발생하는 역기능에 대응할 수 있는 법규가 필요하다. 또한 RFID, 내장시스템 등이 보편화됨에 따라 개인정보가 누출될 수 있는 가능성이 확대되므로, 이러한 환경에서 개인정보를 보호해 줄 수 있는 제도의 확립이 요구된다.

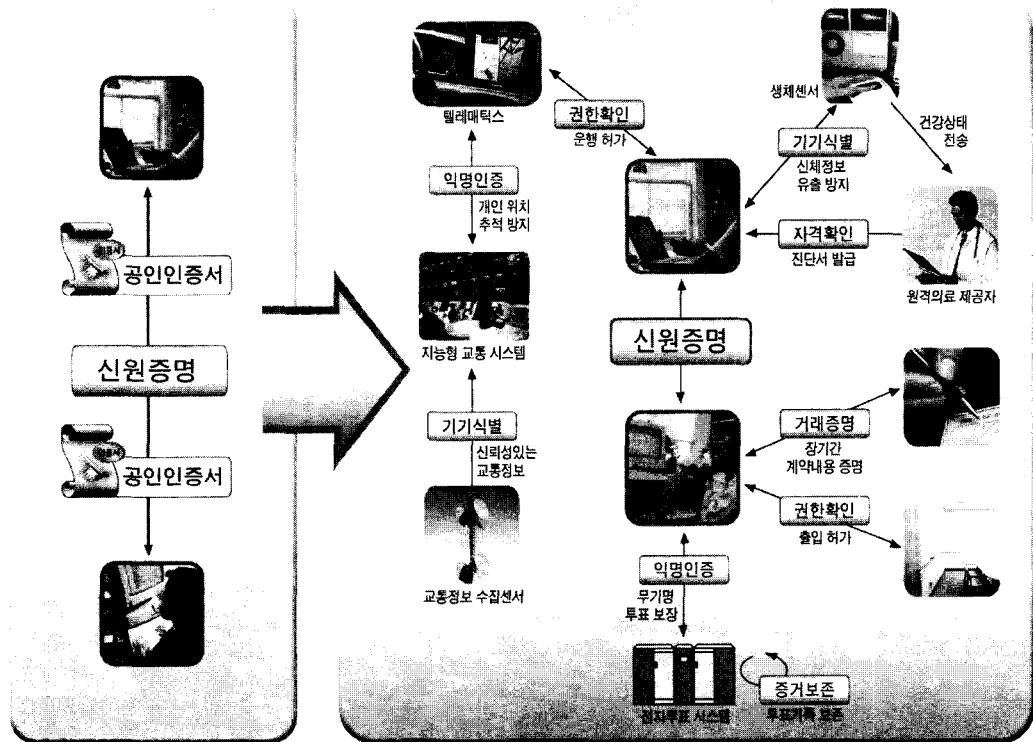
2. 신규서비스의 안전 및 신뢰체계 구축

새로운 신규 IT 서비스에 대한 위협에 대처하기 위한 정보보호 추진전략은 다음과 같다. 첫째, 신규 IT 서비스의 안전 및 프라이버시 위협을 사전에 분석하여 예방하고 능동적으로 대응하기 위해 정보보호 사전 영향평가 체계 마련이 필요하다. 이를 위해서는 침해위협 분석 모형 연구, 정보보호 경제성 분석 등 정보보호 사전영향 평가 수행을 위한 기초 연구 수행이 필요하고, 사

전분석, 평가 대상 및 범위확정, 위협요소 분석 등 사전영향평가 수행을 위한 주요 업무절차 개발이 요구된다. 사전영향 평가체는 계획수립, 분석, 설계, 구축 등 정보시스템 구축 단계별 평가 요소를 분석하여 평가하는 방안이 효과적일 것이다.

둘째, 서비스 장애 대응체계 구축이 필요하다. WiBro, DMB, 홈네트워크 등 IT서비스를 안정적으로 제공하고, 서비스 장애 발생시 피해를 최소화하기 위해 IT839전략의 핵심구성요소와 인프라를 대상으로 서비스 연속성 체계(BCP) 구축이 필요하다. BCP의 도입기에는 조사·분석이 쉽고 사고가 자주 일어나는 디바이스 중심으로 서비스 연속성 체계를 수립하고, 확산기에는 서비스 분야를 대상으로 서비스 연속성 체계를 확대하는 것이 효과적일 것이다. BCP 체계의 효과적인 추진을 위해 공공 및 민간의 백업시스템의 개선이 요구된다.

셋째, 차세대 IT 서비스 환경에서 사람·기기의 신원, 권한·자격, 거래사실·내용 인증이 가



(그림 8) 사람과 사물 모두. 언제. 어디서나 대량의 다양한 정보를 유통

능한 통합인증 체계 구축이 필요하다. 유무선이 통합된 서비스의 신뢰성 제고를 위해 사람의 신원 인증만을 수행하는 현 전자서명법을 확대 및 개편하여 사용자 프라이버시 보호를 강화하기 위해 가명인증서, 익명인증서 사용방안을 마련하고, 불법행위 발견 시 사용자 추적이 가능한 인증체계 마련이 필요하다. 또한 생체인증 등 신기술을 적용한 전자서명기술과 유비쿼터스 환경의 특성을 고려한 인증체계 마련도 필요하다.

3. 정보기기의 정보보호 기능강화

정보기기의 보안취약성에 대한 정보보호 기능을 강화하기 위해서는 정보보호 핵심요소기술 개발 및 표준화 등이 필요하다. 핵심 원천기술은 정부 주도로 개발 후, 민간으로 기술이전하고, 상

용화 기술은 산업체 주도로 개발하는 것이 바람직할 것이다. 이 장에서는 다양한 정보기기에 대한 정보보호 기능강화 방안에 대하여 고찰하고자 한다.

첫째 홈네트워크 정보기기에 대한 안전성 확보를 위해서는 홈네트워크용 보안요소기술개발 및 보안관리 체계 구축이 필요하다. 홈네트워크에서 유효한 사용자를 구별하며, 다양한 정보기기 간에 안전한 통신 및 제어를 가능하게 하는 홈네트워크 환경에 적합한 인증기술 및 접근권한 제어기술 확보가 필요하다. 또한 이종의 유무선 네트워크와 프로토콜의 혼재로 다양한 보안취약성이 존재하므로 홈네트워크 전체차원에서 안전성 확보를 위한 통합 보안인프라 구축이 필요하다. 이를 위해 네트워크 수준의 다양한 사이버공

격으로부터 홈네트워크를 보호하기 위해 홈네트워크 보안관리기술 개발 및 외부 응용서비스와 홈네트워크 서비스 간의 안전한 연동을 위한 웹서비스 정보보호 기술개발이 필요하다.

둘째, 텔레매틱스 정보기기에 대한 안전성 확보를 위해서는 단말식별기술 및 침해방지 기술 확보가 필요하다. 텔레매틱스 기기 구동을 위한 사용자와 기기 간 인증기술 및 인증되지 않은 휴대단말기(PDA, 노트북, 캠코더, 디지털카메라 등)의 불법접근을 방지하기 위한 단말기 식별기술이 확보되어야 한다. 또한 악의적인 공격자가 유포한 대량의 유해 트래픽으로 정상 서비스 제공이 불가능해지는 네트워크 자원 소모형 DoS 공격을 사전에 탐지하고 방어할 수 있는 공격탐지 및 방어기술이 필요하다.

셋째 다양한 차세대 이동통신 기기 보호를 위한 핵심기술 확보가 필요하다. 이동통신 단말기 기기의 불법 복제 방지기술 확보 및 기기 인증 대책 마련이 필요하다. 이를 위해서는 휴대폰 인증 센터를 구축하고 신규 복합 단말기에 대해 체계적이고 안전한 불법복제 방지기술, 휴대인터넷, W-CDMA, VoIP 등에 사용되는 악성 코드 방지 및 스팸메일 방지기술, 무선 Ad-hoc 네트워크에서, 비인가된 디바이스에 의한 접근 및 공격을 막을 수 있는 협업형 신뢰보안기술 등의 기술개발이 필요하다.

V. 결 론

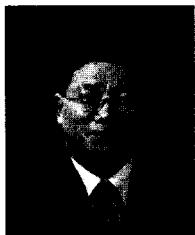
최근의 사이버공격은 시스템 및 네트워크의 취약점을 악용하여 고속으로 전파되는 양상을 띠고 있다. 또한, 웹·바이러스 및 해킹 기술이 결합되어 사이버공격의 확산속도와 파괴력은 점점 커지고 있다. 또, 최근에는 위장 사이트와 이메일을 이용하여 개인 정보를 수집하는 피싱

(Phishing) 기법을 사용하여 타인의 은행 예금을 불법 인출하는 사고가 빈번하게 발생하고 있고, PEEP 등 공격도구에 의하여 중요한 정보가 유출되기도 하였다. 이런 사례에서 볼 수 있는 것처럼 미래 IT 환경에서는 경제, 사회, 국방 등 국가사회 전체에 치명적인 피해를 끼칠 수 있는 지능화된 사이버공격이 더욱 빈번하게 발생할 것으로 예상된다.

지금 우리는 IT산업의 경쟁력을 지속적으로 강화하여 세계 IT 산업의 발전을 선도하는 IT839전략을 수립하고 그 성공적인 구현을 위한 방안을 마련하는 시점에 와 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. 그러나 이러한 IT839전략으로 구현된 정보통신 환경에서 사이버공격이 발생할 경우, 사회의 거의 모든 부문, 즉, 유무선 통신기기, 가전제품, 가스안전시설, 자동화된 동식물 관리 시스템 등에서 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 유비쿼터스 환경의 주요위협을 심층적으로 분석하고 이에 대한 정보보호 추진전략을 제안하였다. 즉 안전한 네트워크 인프라 구현, 신규서비스의 안전 및 신뢰체계 구축, 정보기기의 정보보호 기능강화 등 향후 유비쿼터스 환경의 안전성을 확보하기 위한 정보보호 추진전략을 제안하였다. 본고의 정보보호 추진전략은 향후 예상되는 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.



이홍석

1974년 3월~1979년 2월 : 한양대

학교 전자공학과 학사

1982년 3월~1985년 8월 : 한양대

학교 전자공학과 석사

1996년 3월~1999년 8월 : 대전대

학교 컴퓨터공학 박사

2004년 4월~ : 한국정보보호진흥원 원장

1996년 5월~2004년 4월 : 한국정보보호진흥원 기반

시설보호 단장, 평가인증사업단 단장, 기술본부장

1980년 2월~1996년 5월 : 한국전자통신연구원 실장

책임연구원

2004년 4월 ~ 현재 : 아시아PKI포럼 의장

2004년 4월 ~ 현재 : 한국PKI포럼 의장