高信賴의 유비쿼터스 사회 구현을 위한 차세대 정보보호

이 홍 섭
한국정보보호진흥원 원장

Ⅰ. 서 론

20세기 후반부터 시작된 IT 혁명은 인터넷을 기반으로 발달한 정보통신서비스가 경제 · 사회 · 문화의 각 영역에 걸쳐 일상생활 속에 깊숙이 스며들어 사람들의 생활방식은 물론 가치관의 변화를 수반하면서 지식사회의 새로운 패러다임을 제시하였다.

이와 같이 생활 곳곳에서 변화와 새로운 가치를 창조하는 정보화는 이제 더욱 진화되어 다양한 종류의 컴퓨터가 사람 · 사물 · 환경 속으로 스며들며, 이들이 네트워크로 연결되어 인간의 삶을 도와주는 새로운 유비쿼터스 IT 환경(이하 '유비쿼터스 환경' 또는 '유비쿼터스 사회')으로 이행하고 있다[1]. BcN, USN 등 인프라의 고도화에 따라 현실과 사이버 공간이 통합된 유비쿼터스 환경의 도래로 인간사회의 커다란 변화가 예상되고 있으며, 특히, IT분야와 타산업과의 컨버전스 가속화에 따라 보편화가 예견되는 u-Health 등 다양한 신규서비스는 우리사회의 발전과 더불어 국가 경쟁력 강화라는 새로운 기회를 제시하고 있다.

유비쿼터스로 대변되는 미래는 광대역화, 융합화, 이동화의 특징을 가진 진화된 망을 통해 지능화, 개인화된 통신서비스가 가능한 사회이다. 과거 어느 시대보다 네트워크에 대한 의존성이 높아진 상황이 도래할 것이다. 그러나 이처럼 생활과 밀접한 정보환경의 도래는 사람들의 삶을 편리하게 만드는 동시에 그 이면에는 심각한 정보보호의 위험을 내재하고 있다. 유비쿼터스 환경에서는 모든 사람들이 컴퓨터가 내제된 지능 공간(Smart Environment)에 놓이게 되어, 지금까지의 인터넷 중심의 보안이나 개인정보보호 환경과는 큰 차이가 발생할 수 있다.

사이버공격은 인터넷망에서 방송 및 음성망으로 확산될 것으로 보이며, RFID, LBS, 스마트카드의 실용화에 따른 새로운 형태의 개인정보의 침해가 예상된다. 인터넷 불법스팸, 자살정보 공유, 폭탄제조 등 불법적이고 반사회적인 활동의 전개로 인한 사회적 문제의 확산도 예측된다. 이에 따라 새로운 위협이 상존하는 유비쿼터스 환경 하에서 안심하고 신뢰할 수 있는 새로운 정보보호 정책방향의 설정이 필요하다.

본고에서는 미래사회 금융, 의료, 교육 등 전 분야에서 IT 서비스를 신뢰하고, 개인정보이용에 안심하며, 건전한 정보이용환경 조성을 위한 차세대 정보보호전략 수립에 대한 청사진을 제시하고자 한다.

Ⅱ. 정보보호 환경 전망

2.1 정보화 사회에서 유비쿼터스 사회로

현재 우리나라는 초고속 인터넷 및 모바일 등 디지털 컨버전스가 이루어지는 단계로 유비쿼터스 사회로 가는 전환기에 위치하고 있다. 우리사회는 광대역 네트워크 인프라(BcN)를 기반으로 사람 · 컴퓨터 · 사물이 안전 · 간편 · 신

01_유비쿼터스(Ubiquitous)란 '도처에 널려있다', '언제 어디서나 존재한다'라는 의미의 라틴어에서 유래한 단어

속하게 연결되는 새로운 정보화 환경으로 급속히 전환하는 중이다. PC, 휴대전화, 디지털 정보가전, 디지털 TV, 자동차, 제조물, 도시시설물 등 사실상 모든 사물과 환경이 정보통신망의 단말이 되는 네트워크 연결시대로 진입함에 따라 정보화의 범위가 지식정보에서 사람, 사물까지 확대되고, 개인생활 및 사회 전반에 확산되어 직접적이고 광범위한 영향을 미치는 사회로 진화하고 있다.

이에 따라 정보보호의 특성도 변화가 요구되고 있다. 첫째, 수많은 이질적(heterogeneous) 디바이스들이 컴퓨팅 기능을 내장하고 상호 네트워크로 연결되면서 정보보호의 대상이 시스템, 네트워크에서 디바이스로 확대된다. 둘째, 사용자들이 다양한 신규 IT 서비스를 연속적으로 불편함 없이 사용하기 위해 정보보호 속성이 기밀성, 무결성, 가용성에 추가하여 신뢰성, 프라이버시 보호 등을 포함하는 안전신뢰성(Dependability)[2]으로 확대되고 있다. 셋째, 불법 · 유해 정보 유통을 방지하고 정보폭력으로부터 사용자를 보호하기 위한 컨텐츠의 건전성이 요구된다. 넷째, 위치기반서비스, CCTV를 활용한 전자감시에 대한 우려가 증가하면서 이용자의 프라이버시 보호의 중요성이 증대하고 있다.

이러한 노력을 보다 체계적이고 정교하게 수행하기 위해 인프라, 서비스, 사용자, 환경적 측면에 따라 정보보호 영역을 계층적으로 분류하고, 4가지 핵심 추진 과제(그림 1)를 제시하고자 한다.

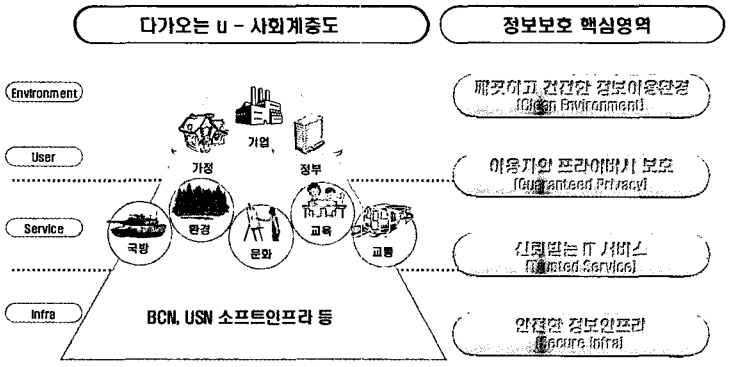
2.2 현재와 미래의 정보보호 핵심 이슈

가. 인프라 위협 고도화 · 글로벌화

이기종 네트워크가 통합된 환경에서 개별 네트워크에서 발생된 위협이 BcN을 통해 통신망, 방송망 및 USN까지 확산될 수 있다. 실제로 인터넷을 이용해 음성통화를 제공하는 VoIP 서비스의 경우 통화내용 도청 및 비정상 패킷의 다량 발송 등이 가능하다. IT기술 발전에 따라 휴대폰 바이러스, 악성 봇(Bot) 등 신종 사이버 위협의 출현 및 공격의 위험 수준도 증가할 것으로 예측된다. 이미 스마트폰 바이러스가 등장하였으며, 향후 다양한 무선 단말에 대한 새로운 공격이 발생할 가능성이 높다. 또한 사이버공격 개발도구의 정교화와 함께 초고속 네트워크의 특성에 따른 초단기 바이러스 전파, 취약점에 대한 즉각적인 공격이 가능한 제로데이 공격도 예상된다.

나. 서비스 신뢰 기반 취약

유비쿼터스 환경에서는 보다 다양한 형태의 인증 수단이 필요하다. 유비쿼터스 환경에서는 센서, 정보가전, RFID 태그 등이 새로운 전자거래 주체로 등장하면서, 이들에 대한 신뢰를 보증할 수 있는 인증수단이 필요하게 될 것이다. 또한 BcN등 첨단 인프라의 발달로 유비쿼터스 서비스가 고속화되고 멀티미디어화됨에 따라 디지털 컨텐츠의 불법유통이 우려된다.



(그림 1) u-사회의 4대 핵심 정보보호 영역 및 과제

02_Dependability는 Security의 기본속성(기밀성, 무결성, 가용성)과 신뢰성, 프라이버시보호 등을 포함한 개념

인터넷상에서 전자상거래의 발달과 더불어 무분별하게 전송되는 스팸메일로 인한 국민의 경제적 손실이 심각한 상황이다. 유비쿼터스 환경에서는 스팸메일의 전송대상이 인터넷, 휴대폰에서 DMB 단말기, VoIP 단말기 등 다양한 융복합 단말기로 확대되어 이용자의 불편 및 손실 증가가 더욱 커질 것으로 예측된다.

다. 이용자 프라이버시 침해 위협

현재 범죄예방 목적으로 공공장소에 설치된 CCTV[3]는 기존의 단순모니터링에서 녹화, 저장, 전송이 가능해짐에 따라 프라이버시 침해 가능성이 커지고 있다. 또한 온라인 거래나 무인 출입관리 등에 본인 확인수단으로 부각되고 있는 바이오 인증으로 인한 프라이버시 침해 위협도 예상된다. 바이오 인증을 통해 추출된 정보에서 개인의 신원을 추적하고 유추할 수 있는 경우에는 프라이버시 침해가 발생할 수 있기 때문이다.

그 밖에도 u-건강관리(Healthcare), u-물류(Logistics) 등 다양한 u-서비스를 제공하기 위해 주변 사물에 설치된 RFID 태그 정보를 추적하면 이용자의 행동 및 신원 관련 정보를 다량으로 수집할 수 있으며, RFID 태그와 RFID 리더와의 무선통신에서 보안성이 높지 않은 경우에 도청을 통한 개인정보의 유출 가능성이 높다(그림 2). 정보통신서비스제공자가 인터넷상에서 개인정보를 암호화하지 않고 송 · 수신하는 경우에 해커는 가로채기 프로그램 등을 통해 손쉽게 개인정보의 탈취가 가능하다.

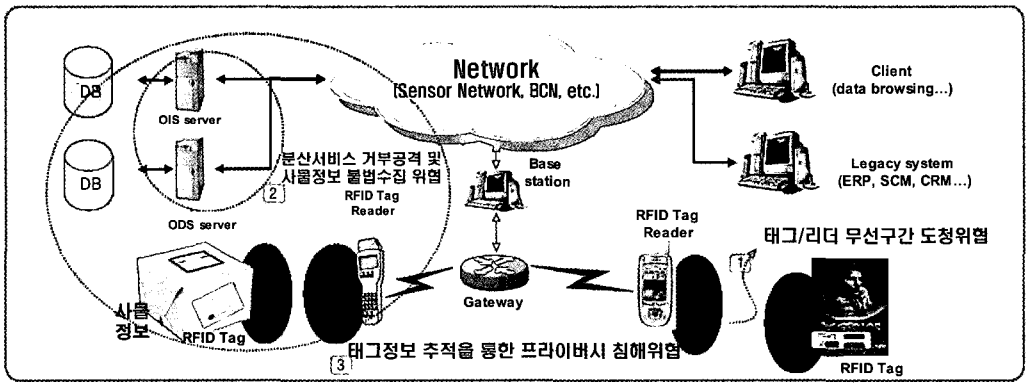
주변에 설치된 센서를 통한 개인에 대한 감시도 우려되고 있다. CCTV, 카메라폰, RFID 등 원격 및 실시간 감시 도구들이 점차 지능화되고 네트워크로 연결되어 수집된 정보를 교환하며, 감시수단의 소형화, 편재화가 진행되어 과거의 은밀한 감시 형태로부터 점차 공개적이고 실시간 감시가 가능한 형태로 변화하고 있다. 과거 감시의 문제가 국가 감시에 초점을 맞추었던 반면, 유비쿼터스 사회에서는 점차적으로 개인 상호간의 감시가 증가하고 네트워크 안에 공존하는 누구라도 감시자이자 피해자가 될 수 있다.[4]

III. 4대 핵심 추진 과제

3.1 안전한 인프라 구축 (Secure Infra)

가. BcN 보안관리 체계 구축

휴대폰, PDA 등 차세대 지능형 휴대 단말기기의 보급 증가와 개인정보 유출을 시도하는 신종 웜 · 바이러스 출현에 따른 피해 방지를 위한 차세대 웜 · 바이러스 예방 대책, BcN 일부 서비스의 장애나 침해사고 시, 피해가 전체 망으로 확산되는 것을 방지하기 위한 네트워크 차원에서의 침해사고



(그림 2) RFID를 이용한 서비스의 이용자 프라이버시 위협 요소

03_CCTV는 국내 약 200만대 설치되어 있으며, 개인정보에 관한 구체적인 조례나 지침 없이 녹화된 CCTV 자료가 30~60일간 보관되고 있음
04_워싱턴 포스터지는 과거의 국가권력에 의한 빅 브라더가 형태가 아닌 우리의 이웃(예, 지하철의 사람들)과 같은 새로운 감시자 도래를 예견(2005.7)

격리 메커니즘, 사이버 공격이 발생하기 이전에 발생 가능한 주요 위협들을 식별하고 잠재적 위험을 예보하는 기술 등에 대한 연구 개발이 필요하다. 또한 BcN 통합망에서 정보보호 수준이 상이한 이기종 망간 보안성 확보, 사업자간 연동시 보안성 보장을 위한 정보흐름의 통제와 관련된 기술, 정책, 절차 등이 마련되어야 한다.

나. USN 안전보안 관리체계 구축

USN 운영의 안전성 확보를 위한 보안기술에는 센서 노드 내의 정보에 대한 무단 유출과 위 · 변조, 오동작 등과 같은 USN 보안위협을 차단하고 대응할 수 있는 센서노드용 경량 보안 칩, 도청, 위 · 변조 등 인프라 공격을 능동적으로 모니터링, 탐지, 대응할 수 있는 USN 침입탐지 및 대응 기술, 도청, 라우팅 경로 및 메시지 위변조, DoS 공격, 소비전력 공격 등과 같이 USN 인프라에서의 보안 취약성을 방어할 수 있는 보안 라우팅 기술, 메시지 보호 및 인증 기술 등이 있다.

이들 보안 기능이 탑재된 USN 정보통신기기의 안전성은 설계 단계에서부터 확보될 수 있어야 하며 USN 정보통신기기의 안전성 검증 방법론 개발 및 검증체계 구축이 필요하다. 또한 안전한 기기 개발을 위한 정보보호 가이드라인도 마련되어야 할 것이다.

다. 소프트웨어 안전 · 신뢰성 강화

융 · 복합 환경에서 모바일 악성코드에 의한 침해확산 방지, 디지털 콘텐츠 등의 지적재산권 보호 등을 위해서는 소프트웨어의 안전 · 신뢰성이 더욱 강화되어야 한다. 주요 소프트웨어의 보안성을 설계 단계에서부터 검증할 수 있도록 소프트웨어 안전기준 마련 및 검증체계 구축, 소프트웨어 취약점을 감소시킬 수 있는 보안성 점검도구 개발 등이 필요하다. 특히 융 · 복합 디바이스에 내장된 소프트웨어의 취약점에 대한 안전 관리체계를 구축하기 위하여 휴대폰, DMB, Wi-Bro, Telematics, PMP 등에 적용된 내장형(Embedded) 소프트웨어의 취약점 분류 체계 및 DB 구축, 내장형 소프트웨어의 보안성 평가 등이 주요과제로 제시되고 있다.

라. 사이버 침해사고 억제력 확보

기존의 인터넷침해사고 대응체계를 고도화하기 위한 조치들이 필요하다. 사이버 침해사고의 전파를 네트워크 차원에서 봉쇄하기 위해 통신사업자간 연계체계를 강화하고, 모니터링에 의한 네트워크 · 시스템 보호체계에서 침해사고 원인을 사전에 탐지 · 제거할 수 있는 예방체계 중심으로 전환하는 노력이 필요하다. 한편으로는 RFID 미들웨어, 소프트스위치 등 BcN의 주요 구성요소에 대한 보안성 인증 체계 구축을 위해 기술개발, 시험환경, 법제도 등에 대한 검토도 요구된다.

3.2 서비스의 신뢰기반 확보

가. 차세대 전자인증 프레임워크 구축

유비쿼터스 컴퓨팅 서비스의 인증과 관련된 위협 및 침해사고 등을 예방 · 대응할 수 있는 위험 평가 방법론이 개발되어야 한다. 여기에는 유비쿼터스 컴퓨팅 전자거래 환경에서 확인가능한 위협에 대한 취약점 평가, 위협에 의해 발생되는 피해와 위협가능성을 평가하여 기업의 자산유형에 따라 위험 수준을 평가하는 방법론, 피해범위를 고려한 응용서비스의 보증 레벨 개발 등의 세부 과제가 포함된다. 또한 주요 응용서비스 인증을 위한 크리덴셜(credential) 서비스를 제공하는 사업자를 평가하고 서비스의 신뢰성을 증명하기 위한 크리덴셜 평가체계 구축도 필요하다.

제도적으로도 현재 전자서명법이 정의하는 공인인증서비스를 유비쿼터스 컴퓨팅 환경에 맞추어 다양한 디지털 증명 기능을 제공할 수 있도록 확대 개선해야 한다. 인증수준에 따라 다르게 적용되는 전자거래 증명 등의 다양한 디지털 증명기능에 대한 법적 효력 부여를 위한 전자서명법 확대 · 개편, 다양한 디지털 증명기능을 제공하는 인증기관의 안전성을 확보하기 위한 인증기관 관리체계 구축, 인증 기반 USN, 홈네트워크, 텔레메틱스 등의 IT 839 인증 서비스 안전성 검토 및 평가체계 마련 등이 주요 과제이다.

나. ID 관리체계 강화

사용자가 제공한 개인정보에 대한 공개여부 및 조건을 개인정보 보호정책에 근거하여 설정할 수 있는 ID 관리기술 개발이 필요하다. 주요 요소기술에는 첫째, 개인정보의 등록, 저장, 조회, 관리, 전송 및 공유, 폐기에 이르는 개인정보 생명주기 관리를 위한 프로토콜 및 기술, 둘째, 사용자가 원치 않는 신원정보를 보호할 수 있는 익명(anonym) 또는 가명(pseudonym) 식별자 제공 기술, 셋째, 정보시스템에 대한 정보의 중요도와 서비스 특성에 따라 다양한 수준의 인증강도 지원 기술 등이 있다. ID 관리 기술과 함께 개인정보를 저

장하고 있는 시스템의 안전신뢰 모델을 구축하고 이를 인증하는 서비스도 필요하다.

유비쿼터스 컴퓨팅 환경에서 확대되는 개인정보의 경제적 가치가 효과적으로 이용될 수 있도록 개인정보의 생명주기에 따른 개인정보 활용 제도를 개선할 필요가 있다.

기업은 마케팅 활동을 위해 개인정보의 경제적 가치를 기반으로 활용하되, 민감한 개인정보는 보호될 수 있도록 개인정보 활용 환경을 조성하고 개인정보 보호 및 경제적 활용을 지원하는 효과적 관리체계와 함께 사용자의 개인정보 관리 편의성을 강화하는 방향으로 제도가 정비되어야 한다. 한편 국가가 발급하는 ID인 주민번호의 유출 및 도용방지를 위해 개발된 주민번호 대체수단(i-PIN)의 사용 확대를 위하여 '주민번호 대체수단 가이드라인' 의 법제화를 추진하여 주민번호대체수단 제도를 정착시키고, i-PIN 사용 사업자에 대한 인센티브를 부여하는 등 이용활성화를 위한 노력이 수반되어야 한다.

다. 건전한 디지털 콘텐츠 유통환경 구축

유·무선 인터넷, 디지털 방송, 디지털 홈 등 콘텐츠 유통 도메인별로 독립적으로 개발된 DRM (Digital Right Management), CAS (Conditional Access System), CP(Cpoy Protection) 기술이 유비쿼터스 컴퓨팅 서비스 환경에서 끊김없이 서비스될 수 있도록 콘텐츠 보호 환경의 구축이 필요한데, 이를 위해서 이동저장장치(MMC, SD Card, USB, DVD) 및 디지털 인터페이스를 통한 복제방지 기술의 개발과 이기종 모바일 디바이스 간 상호 유통(수신, 전송, 저장, 복제)되는 융·복합 지식과 콘텐츠의 저작권한을 보호하는 서비스 체계(그림 3)의 구축 등도 검토할 필요가 있다.

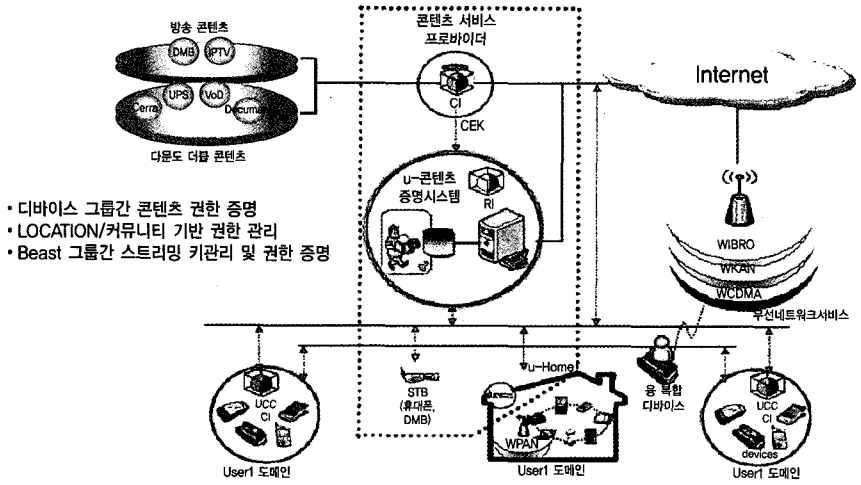
라. 디바이스 신뢰성 확보

다양한 유비쿼터스 컴퓨팅 서비스 환경에 적합한 디바이스 인증모델을 개발하고 이를 위한 인증관리 위험관리 체계의 구축이 필요하다. 디바이스 인증모델에는 서비스 가입자 디바이스 인증, 네트워크 접속 디바이스 인증, 홈네트워크 디바이스 인증 등이 있지만, 인증 시나리오별 인증 위협분석을 통해 안전성에 대한 연구와 서비스 시나리오별 디바이스 인증환경에서 인증서의 발급, 관리, 폐기에 이르는 생명주기에 따른 관리체계 모델 개발, 관리모델별 인증관리 및 보호체계 등에 대한 가이드라인이 개발되어야 한다.

디바이스에서의 안전한 암호처리환경 실현을 위한 TPM(Trusted Platform Module) 기술, 클라이언트 및 어플리케이션의 진위 여부를 판별하기 위한 인증기술도 필요하다. 또한, 물리적인 해킹 방지 기능, 안전한 스토리지 기능 및 신뢰·보안 서비스용 미들웨어 기술의 개발과 관련 정책도 시의 적절하게 마련되어야 한다.

마. 신뢰할 수 있는 서비스 이용기반 마련

VoIP, WiBro 등 융·복합 신규 IT서비스 침해발생 시, 예



(그림 3) 디지털콘텐츠 유통권한 증명 서비스 사례

상되는 사회적 손실을 최소화하기 위해, 서비스 개발단계에서의 정보보호 사전점검이 필요하다. 이를 위해 IT 서비스의 개발단계부터 정보보호 취약점을 분석하고 대책을 마련할 수 있는 절차 및 방법과 정보보호 대책 도출시 참조할 수 있는 보호대책 DB, 영향평가 기준 등이 마련되어야 한다.

유비쿼터스 컴퓨팅 서비스의 기밀성 확보를 위해 암호 이용과 관련한 환경의 정비가 필요하다. 현재 모호하게 되어 있는 '자율적인 암호사용 영역'과 '규제가 필요한 암호사용 영역'을 명확히 규정함으로써, 투명한 암호사용 환경이 조성되어야 한다. 여기에는 인터넷 등 개방형 정보통신망을 이용하여 처리되는 정보의 기밀성 및 신뢰성을 확보하기 위한 수단의 하나인 암호키분배인증서의 안전한 생성 · 발급 · 관리 체계, 암호제품의 안전성을 보증하기 위한 평가 및 인증 체계 등의 이슈가 포함된다.

3.3 이용자의 프라이버시 보장(Guaranteed Privacy)

가. 개인정보보호 기반 구축

유비쿼터스 컴퓨팅 환경변화에 따라 개인정보보호를 위한 기술을 체계적이고 구체화해서 적절한 개인정보보호 기술이 개발되어야 한다. 수집, 저장 · 관리, 이용 · 제고, 파기로 이어지는 개인정보의 생명주기별로 발생할 수 있는 침해에 대응하는 프라이버시 보호 관리 프레임워크 기술, 고속 DB 보안기술, 개인정보의 안전한 저장기술 등이 포함된다.

개인정보 침해 기술은 지속적으로 발전 · 등장하고 있으나 이에 대비한 체계적이고 표준화된 개인정보 침해방지 기술 개발이 미흡하여 개인정보 침해를 방치하는 결과를 초래하고 있다.

이에 대하여 기술력이 취약한 SOHO 사업자 등에 대해 고객의 개인정보 보호를 위한 기술조치 사항을 지원하고, 개인정보 침해에 대한 기술적 분석 및 대책 수립을 위한 '개인정보보호기술지원센터'의 설립 · 운영이 필요하다.

나. 개인정보보호 법제도 정비

유비쿼터스 사회에서 개인정보보호를 위한 법제도적 장치는 무엇보다 중요하며, 다양한 제도적 접근이 요구된다. 먼저 개인정보를 다루는 사업자들을 대상으로 하는 것들에는 개인정보 감사(Audit), 개인정보침해 사업자에 대한 제재, 개인정보보호방침 공개의무 및 등록, 개인정보관리책임자, 개인정보 영향평가 등이 고려될 수 있다. 특히, RFID, 위치정보, 홈네트워크 사업 등 프라이버시 침해 논란이 예상되는 사업에 대해서는 개인정보 영향평가를 통하여 적정 수준의 사용자 프라이버시 보호 대책을 강구하도록 제도화 할 필요가 있다.

다. 위치정보, 바이오정보, 의료정보, 영상정보 보호

개인의 위치정보로 인한 프라이버시 침해 방지를 위해서 위치정보 주체인 이용자의 자기정보 통제권 및 편의성을 보장을 위해 개인 스스로 설정한 위치정보 제공기준에 따라 자동적으로 위치기반서비스가 제공될 수 있도록 기술규격을 개발하고, 텔레매틱스, GPS를 활용한 위치정보 등의 정보제공에 대한 감독 · 관리 체계를 구축해야 한다.

바이오 정보의 성격에 따라 프라이버시 보호기준을 차별화하고 바이오인식기술의 안전한 이용환경 조성을 위한 감독 및 지원 체계, 기술개발, 표준, 시험 · 평가, 교육 · 훈련 등 인프라의 정비가 필요하다.

의료정보는 사생활 보호와 동시에 의료과실 발생 시 중요정보로 이용되므로 의료정보의 안전한 보관, 전송을 위한 체계를 마련해야 한다.

웹 카메라 또는 CCTV에 의해 수집된 영상정보에 의해 미치는 프라이버시 보호를 위해서 CCTV의 설치 · 운영과 관련한 프라이버시 규정, 전송 · 저장된 영상정보의 노출 및 변조 방지를 위한 가이드라인 및 법령의 관련 규정 등이 더욱 체계적으로 정비되어야 한다.

라. 서비스 이용정보 보호

신규 서비스의 이용정보는 개인의 취향이나 행위의 유추를 가능하게 하여 프라이버시 침해를 발생시키므로 본인의 동의하에 개인정보를 공개하며, 공개정보는 동의목적 범위 내에서 사용토록 하고 목적 외 사용에 대하여는 엄격한 법적 규제 장치를 마련해야 한다.

특히 댁내 정보 유출 방지를 위해 개인정보유출방지를 위한 기술적 능력요건을 사업자의 시장진입요건으로 법제화(허가제 또는 신고제)하는 것도 검토해 볼 수 있다. 특히 RFID를 이용한 서비스를 개발함에 있어 RFID시스템이 프라이버시에 미칠 영향을 평가하고, 이용자가 언제든지 RFID의 추적으로부터 벗어날 수 있도록 이용자의 RFID 추적 배제권을 보장하는 관련기술 개발도 필요하다.

3.4 깨끗하고 건전한 환경 조성

현재 공공기관을 포함한 조직의 개인정보보호 인식과 정보통신 보안수준이 매우 낮은 실정으로 개인정보관리책임자 및 일반 네티즌의 개인정보 보호에 대한 인식을 제고하기 위한 조치들이 필요하다. 유비쿼터스 환경 도래에 따른 청소년, 학부모, 교사, 사업자 등 기초 정보보호 교육 실시를 위한 대상별 정보보호 프로그램을 개발하고, 기업 대상 정보보호 교육의 실시와 개인정보 관리 책임자 교육의무화의 법제화를 비롯한 사업자의 인식제고 활동을 추진하는 등의 정보보호 교육을 강화할 필요가 있다.

위치정보, CCTV 영상정보, RFID 정보 등을 다루는 기관, 유전자 및 신체정보를 다루는 병원, 건강관리기관 등에 적합한 개인정보보호 모델을 개발하고, 개인정보관리 책임자 교육훈련 의무화 및 추진체계를 정비하는 등의 관리적 제도적 대책의 정비와 함께 인터넷, 이동통신, u-서비스 이용자를 대상으로 개인정보보호의 중요성과 신기술 환경에서의 위험성에 대한 인식교육을 실시하여야 한다. 개인정보보호 취약계층 파악을 위한 프라이버시지수를 개발하여 프라이버시에 대한 의식이 낮은 계층의 인식을 제고하는 노력과 함께 기업내 근무환경에서의 프라이버시 보호 대책도 마련해야 한다.

Ⅳ. 결 론

유비쿼터스 컴퓨팅 기술을 통해 만들어가는 정보환경은 자연적으로 존재하는 환경이 아닌, 인간이 인간의 편의를 위해 만들어낸 환경이다. 그러나 인류의 역사를 돌이켜 볼 때 이러한 기술적 진보는 오히려 인류를 구속할 수 있는 가능성도 내포하고 있다. 따라서 예견되는 유비쿼터스 사회는 단지 장밋빛 미래만을 우리에게 안겨주는 것이 아니라는 점을 명심하고, 그 역기능을 최소화 하는 사회적 노력이 반드시 수반되어야 한다.

특히, 유비쿼터스 사회는 '사용자가 네트워크나 컴퓨터를 의식하지 않고 장소에 상관없이 자유롭게 네트워크에 접속할 수 있는 정보통신 환경' 이 제공되는 만큼 보안 취약점이나 침해행위에 의해 야기되는 피해 및 손실은 더욱 심화될 것으로 예상된다. 또한 그 형태도 두려움, 불안, 짜증 등 심리적 위협부터 ID 오남용, 침해사고, 사이버폭력 등 실제적 피해까지 광범위한 분포를 갖게 될 것이다.

따라서 유비쿼터스 사회에서의 정보보호는 과거 네트워크, 서버 등 인프라 중심적인 형태와 더불어 사용자 중심적인 접근방식이 추가되고 강조되는 형태로 변모할 필요가 있다. 즉, 서비스에 있어서 믿음을 제공하는 '신뢰관계' , 사용자의 권한과 관련된 '프라이버시' 등이 더욱 중요한 이슈가 될 것이다. 이제는 정보보호가 정보화 추진의 역기능을 해소하는 부수적인 역할에서, 다양하고 새로운 IT 서비스에 대한 불안을 해소하여 새로운 IT 시장 창출과 진흥에 기여하는 역할로 변모할 시점이다.

약 력

이 홍 섭

한양대학교 전자공학과 학사, 석사
대전대학교 컴퓨터공학 박사
한국전자통신연구원 실장
한국정보보호진흥원 단장/본부장
아시아PKI포럼 의장
국가정보통신표준 심의위원
TTA 정보보호표준위원회 위원장
서울지방검찰청 사이버수사 자문위원
정부통합전산센터추진위원회 위원
현재 한국PKI포럼 의장
현재 금융분쟁조정위원회 조정위원
현재 정보처리학회 부회장
현재 정보보호학회 수석부회장
현재 한국정보보호진흥원 원장