2008

유비쿼터스 사회의 정보보호 방안

Development of Privacy Protection Infrastructure for Ubiquitous Information Society

장 무 경

서울시정개발연구원
Seoul Development Institute

시 정 연
2008-PR-29

유비쿼터스 사회의 정보보호 방안

Development of Privacy Protection Infrastructure
for Ubiquitous Information Society

2008

서울시정개발연구원
Seoul Development Institute

연 구 진

연구책임	장 무 경	• 창의시정연구본부 부연구위원
연 구 원	최 지 원	• 창의시정연구본부 연구원
	이 지 은	• 창의시정연구본부 연구원

요약 및 정책건의

Ⅰ. 연구의 개요

1. 유비쿼터스 정보화 사회에서의 정보보호 중요성

○ 지금은 시민생활과 산업경제에 급진적 변혁을 일으킬 것으로 예측되는 유비쿼터스 도시가 실현될 수 있도록 서울시의 u-City(Ubiquitous City) 구현 목표에 대해 심도있는 논의가 필요한 시점임. 특히 유비쿼터스 사회의 시민 신뢰도와 직접적인 연관이 있는 정보보호 측면의 고려가 필요함.

- 이와 관련된 중앙정부의 사업추진 일정에 비추어 2010년 전후 유비쿼터스 관련 기술 및 제반여건의 변화가 급진적으로 발생할 소지가 있기 때문임.
- 또한, 국내의 u-City 사업은 기술주도형으로 주요 정보기술에 대한 성공적 개발에 의존하고 있는 실정이므로 전략적 측면 및 소프트웨어적 요소, 그리고 관련 정책 개발 측면에 대한 강조가 다소 미흡함.
- 이렇듯 일부 측면만을 강조하는 u-City 비전은 유비쿼터스 도시에 대한 올바른 이해를 저해할 뿐 아니라 유비쿼터스 도시 건설의 목표를 왜곡할 소지가 있음.

○ 유비쿼터스 환경에서는 BcN, USN, IPv6 등 3대 인프라의 도입이나 통신과 방송의 융합으로 사이버 위협의 대상이 IP를 사용한 특정 망에서 통합된 망으로 전이되어 피해 확산속도가 빨라지고, 피해 규모 역시 확대될 것으로 우려됨.

- 홈 네트워크, 텔레매틱스 등 서비스 융합화가 본격적으로 진행되면서 사이버 위협이 ALL-IP 망으로 확대될 것으로 전망됨.
- 또한, 9대 신성장 IT 디바이스의 정보보호 기능이 미흡한 경우 기기의

신뢰성 저하, 서비스 장애 등의 위협을 초래할 것으로 예상됨.

○ 진정한 유비쿼터스 사회를 실현하기 위해서는 시민의 개인정보보호에 대한 사전 준비가 충분히 이루어져야 함. 하지만 정부가 추진 중인 유비쿼터스 관련 정보화 플랜에서의 정보보호 측면은 그 중요성에 비해 상대적으로 고려가 미흡함.

- 유비쿼터스 사회에서는 정보의 주체가 인식하지 못하는 사이에 개인의 신상정보가 저장, 축적되고 노출될 위험성이 높음. 이는 폭넓은 정보공유의 반대급부로서 피할 수 없는 문제이기도 함.

○ 개인정보의 부적절한 수집 및 사용으로 인한 정보침해 문제는 유비쿼터스 컴퓨팅(ubiquitous computing)이 가져다 줄 긍정적인 효과를 반감시키는 데 결정적인 요인으로 작용할 전망임.

- 이러한 경향은 유비쿼터스 네트워크 및 서비스에 대한 시민 신뢰도의 저하로 이어질 수 있음.

2. 유비쿼터스 사회에서의 정보보호의 의의

1) 개인정보의 이해

○ 우리나라의 경우 개인정보를 “생존하는 개인에 관한 정보로서 당해 정보에 포함되어있는 성명·주민등록번호 등의 사항에 의하여 당해 개인을 식별할 수 있는 정보(당해 정보만으로는 특정개인을 식별할 수 없더라도 다른 정보와 용이하게 결합하여 식별할 수 있는 것을 포함한다)”라고 법적으로 정의함(「공공기관의개인정보보호에관한법률」 제2조).

○ 개인정보의 분류는 최근 개인정보보호에 관한 논의가 활발하게 이루어지면서 본격적으로 체계화되기 시작함.

- 개인정보는 관리주체에 따라 공공개인정보와 민간개인정보로 분류하거나, 정보의 민감도에 따라 분류되기도 함. 또한 Weible(1993)의 내용에

따라 분류될 수도 있음.

○ 정보통신기술 등의 발달로 인한 사생활 침해 사례가 빈번하게 발생하여 현대적 의미의 개인정보 보호 문제에 대한 관심이 증대되면서 '정보 프라이버시(information privacy)'라는 용어가 등장함.

- 정보 프라이버시는 기존의 사생활 보호나 전화 등 통신상의 프라이버시 보호의 개념을 전제로 하되, 더 나아가 인터넷 공간에서 이동하는 개인정보에 대한 통제권이라는 적극적인 성격으로 발전되어 도출된 개념임.

○ 유비쿼터스 시티에서 인터넷 공간으로 대표되는 디지털공간의 개인정보에 대한 프라이버시 보호는 결국 물리적 공간까지 확대될 것임.

2) 정보보호 환경 변화

○ 유비쿼터스 컴퓨팅 환경에서는 네트워크를 통해 오가는 정보의 양이 비약적으로 증가하게 됨에 따라 정보보호 환경 역시 제어가 어려운 수준으로 변화할 수 있음.

- 웹 2.0, UCC, RFID 등의 새로운 유비쿼터스 기술의 등장은 유비쿼터스 IT환경에서의 또 다른 위협을 초래하고, 웜 바이러스와 해킹 기능의 결합으로 복합화되고 악성화된 사이버 공격을 증가시키고 있음. 정보보호 환경은 개별 시스템, 네트워크 보호에서 서비스와 이용자 보호로 그 중심이 급격히 옮겨져(개별 디바이스로 확대) 그 범위가 크게 확대됨.

3) 유비쿼터스 사회의 특성과 정보보호의 역할

○ 유비쿼터스 사회에서 정보의 특성

- 상호 연결된 장치들의 편재형 네트워크와 통신으로 인해 개인 정보의 유통량이 급증할 것임.

- 특정 응용 프로그램에 인지적 및 생체인식 인터페이스를 도입함에 따라 유통 중인 개인 정보의 질적 성격이 바뀔 것임.
- 개인 맞춤형 서비스를 제공하기 위해 유비쿼터스 네트워크는 사용자들의 일상활동 중 상당부분을 추적 조회하고 수집해야 할 것임.

○ 유비쿼터스 사회에서의 정보보호는 u서비스 및 거래정보에 대한 이용자의 신뢰도를 향상시켜 신규 IT 서비스에 대한 수용성 및 활용도를 높이는 핵심적인 역할을 수행할 것임. 또한 유비쿼터스 사회에서 예상되는 새로운 유형의 해킹, 바이러스, 사이버 범죄 등 사이버 위협에 대한 사전 예측 및 방지의 역할을 할 것임.

4) 유비쿼터스 환경에서의 개인정보 침해

○ 유비쿼터스 환경에서는 시공간의 제약없이 개인정보가 유출될 가능성이 비일비재하고, 감시수단의 소형화, 편재화가 진행되어 좀더 공개적이고 실시간적인 감시 형태로 진화하고 있음. 또한 개인 맞춤형 서비스를 제공하기 위해 더 많은 개인정보들이 수집되고 개인정보 DB 관련 시스템들의 통합이 활발해짐에 따라 개인정보의 대량 노출 위험이 더욱 증가함. 여기에는 개인정보에 대한 보호인식 부족 및 사업자의 부주의도 한 몫을 하고 있음.

○ 유비쿼터스 컴퓨팅 환경에 있어서 오프라인이 기반인 기존의 환경과 비교하여 개인정보침해 유형 자체는 크게 달라지지 않았으나, 그 침해규모가 광범위해질 수 있음. 이러한 위험은 기존과 달리 사회시스템의 운영초기 단계부터 발생할 수 있음. 유비쿼터스 정보화 사회의 대표적인 개인정보 침해 유형은 <표 1>과 같음.

<표 1> 유비쿼터스 정보화 사회의 개인정보 침해 유형

개인정보 침해유형	현 행	u-City 환경
부적절한 접근과 수집	정보주체의 동의 없이 개인정보를 수집하는 행위	정보주체가 인식할 수 없는 상황 속에서 완전한 개인정보 통제권을 상실할 가능성 존재
부적절한 분석	개인의 동의 없이 사적인 정보를 분석하는 행위	사적인 정보의 분석을 통해 개인의 지배 또는 개인의 생활에 대한 통제가 심화될 가능성 존재
부적절한 모니터링	개인의 인터넷 활동을 동의 없이 조사하는 행위	개인의 사적인 생활 및 취향 등의 전반적 정보가 노출될 가능성 존재
부적절한 개인정보 유통	개인의 동의 없이 개인정보를 제3자에게 넘기는 행위	수집된 개인정보를 정보주체의 동의 없이 제3자에게 양도하는 정보의 종류 증가 및 양도 가능성 존재
원하지 않는 영업행위	동의 없이 스팸메일, 문자 등의 광고성메일을 보내는 행위	개개인의 특성에 정확하게 조응하는 광고성 메일의 동의 없는 무차별 유통 가능성 존재
부적절한 저장	필요에 의해 수집된 정보를 목적달성 후 파괴하지 않은 행위	기존보다 더욱 다양하게 수집된 정보의 파기가 이루어지지 않고 다양한 용도로 재활용될 가능성 존재

출처 : 고웅, 이동범, 곽진, "u-City 서비스 분류에 따른 적용사례와 보안 고려사항", 2008.

3. 정보보호 현황 및 문제점

○ 유비쿼터스 정보화 사회에서 나타날 것으로 전망되는 정보보호 상의 문제점을 기술적 영역, 규제적 영역, 그리고 사회적 영역으로 나누어 설명하면 다음과 같음.

1) 기술적 영역 : 유비쿼터스 컴퓨팅 환경의 정보보안 기술

○ 향후 정보보호기술은 개인정보보호, 지식 및 지적재산권 보호, 침해확산 및 사이버 범죄 방지, 끊김없는 서비스 간 상호인증 등 사용자 중심의 정보보호 정책 및 기술이 전개될 것으로 전망됨.

○ 그러나 유비쿼터스 기술 발전은 정보의 주체가 인식하지 못하는 사이에 개인의 신상정보를 저장, 축적하고, 구매 패턴, 위치정보 등을 노출시킴. 또한 이러한 정보들을 더욱 더 광범위하게 수집하고, 매우 신속하게 그리

고 양과 무관하게 유통하며, 무한정 복제하는 일이 가능하게 함.

○ 현재 정보보호에 대한 축적된 기술력이 부족하고, 관련 지적재산권의 확보와 같은 기술지원적 기반이 취약하다는 한계가 있음.

2) 규제적 영역 : 유비쿼터스 정보보호의 법적 현황

○ 공공부문과 민간부문에 공통으로 적용되는 개인정보보호에 관한 일반법이 없어, 공공부문과 민간부문을 분리해서 규제하는 방식을 취하고 있음. 따라서 법제가 분산되어 일관성 있는 개인정보 보호체계가 정립되지 못하였고, 개인정보의 보호 관련 업무를 수행하는 기관이 담당 부처별로 다르거나 업무가 중첩되는 문제가 발생함.

○ 정부의 개인정보보호를 위한 접근방법이 사전적이기보다는 사후적인 관리에 집중되어 있고, 처벌위주의 방식임.

○ 개별법에 의해 단편적으로 존재하고 있는 개인정보보호기구는 그 체계나 독립성, 혹은 기능이나 역할 등에 있어서 매우 제한적이며 각각의 기구가 영역별로 단편적으로 운영되고 있음.

○ u-City 환경 하에서의 개인정보보호에 대한 법적 공백

- 현행법에 의하여 보호되는 개인정보는 대부분 컴퓨터에 의하여 전산화된 개인정보에 한정되어 있음.
- 최근 국내·외에서 RFID, CCTV, 위치정보, 인터넷감시기술 등을 둘러싸고 많은 논의들이 전개되지만, 그와 같은 기술 또는 서비스들을 내포하는 개인정보 또는 프라이버시 침해 요인들에 대한 적절한 입법적 대응이 아직 이루어지지 않고 있음.

○ 이에 따라 유비쿼터스 환경변화에 따른 법 개정 움직임으로,「위치정보의 보호및이용등에관한법률(안)」추진과「공공기관의 개인정보보호에 관한 법률」에서 공공기관의 CCTV에 한하여 법적 규제 신설을 들 수 있음. 또한

행정안전부는 「개인정보보호법」을 제정함으로써 공공·민간을 포괄하여 개인정보 침해로 인한 개인의 피해 구제 강화와 개인의 권리와 이익을 보장하려고 함(2008년 8월 입법예고).

3) 사회적 영역 : 시민들의 인식과 공공영역의 요구

○ 자신의 개인정보와 프라이버시 침해에 대해 그 어느 시대보다 높은 우려감이나 막연한 불안감과 달리 실생활에서의 정보보호에 관한 의식수준은 비교적 낮은 편임.

- 주민등록번호 등 개인정보 관련 정책에 대해 국민의 인식이 부족하여 타인의 정보도용이 빈발하게 발생하거나 사업자들의 경우 이익에만 급급하여 개인정보의 수집형태 및 이용을 자의적으로 해석함. 불건전 정보 이용환경도 이런 인식의 부재에서 비롯되었다고 볼 수 있음.
- 인터넷 환경을 통제하는 가치규범적 규율이 없기 때문에 윤리적 지체 현상이 발생하는 정보윤리의 부재가 발생하게 됨.
- 또한 새로운 유비쿼터스 정보기술들의 등장은 찬반양론적인 사회갈등 문제를 생성함.

○ 공공영역에 있어서 개인정보에 대한 관리 대책이 시급함.

- 공공기관들은 기관별로 개인정보보호에 관련된 자체교육을 실시하지 않는 경우가 많았고, 안전조치를 확보하지 않은 채 개인정보파일을 다른 기관에 제공하는 경우가 있는 등 세부적인 관리 측면에서 미흡한 점이 발견됨. 또한 실무담당자들에게 개인정보보호에 대한 인식이나 전문성을 키워주는 등의 정보보호인력 양성이 필요함.

○ 개인정보보호에 대한 사회구성원들의 관심 및 권리의식의 부재와 사회적 갈등은 정보사회에 대한 신뢰를 상실시켜 정보사회의 발전에도 악영향을 끼칠 수 있음.

4. 유비쿼터스 정보보호의 요구사항 분석

○ 유비쿼터스 서비스 개발 시 고려해야 하는 개인정보보호 요구사항을 네트워크 정보보안 요구사항, u-Service 정보보호 요구사항으로 나누어 분석함.

1) 네트워크 정보보안 요구사항

○ 현재의 정보보호 요구사항으로 고려되고 있는 데이터의 기밀성, 무결성, 사용자 인증, 부인방지, 익명성, 자기정보 통제 및 제어 등의 문제는 유비쿼터스 서비스가 현실화되는 시점에 더욱 확대될 것으로 보임.

○ 이는 유비쿼터스 서비스의 최대 장점으로 꼽히는 사용자의 상황에 따른 맞춤형 정보제공을 가능하게 하기 위해서 사용자의 상황인식(context awareness)을 위한 다양한 정보수집이 필요하다는 것과 사이버 위협의 대상이 IP를 사용한 특정 망에서 통합된 망으로 전이되어 피해 확산속도가 빨라지고, 피해 규모 역시 확대될 것으로 예상되기 때문임.

○ 따라서, 유비쿼터스 서비스의 기반 망과 서비스 제공 레이어(layer) 사이에 미들웨어로서 프라이버시보호계층(Privacy Protection Infrastructure)을 두고, 개별적 정보침해유형에 대한 종합적이고 일관된 대책 마련이 필요함.

2) u-Service 정보보호 요구사항 분석

○ u-City 내 다양한 서비스의 효율적인 제공을 위해 운영하게 되는 도시통합운영센터는 도시전체 시설물, 시스템 인프라, 시민들의 정보 등 모든 정보를 통합된 데이터베이스에 저장하고 이용하게 함. 이에 따라, 악의를 가진 사용자 또는 관리자의 개인정보침해의 가능성은 더욱 높아질 것으로 예상됨.

○ 이를 예방하기 위해 프라이버시 보호기능의 인프라화, 개인정보 특성에 따른 처리, 프라이버시를 보호하는 접근제어, 개인정보의 분산관리를 통한 개인정보 보호 등의 방안을 제시함.

- 유비쿼터스 인프라 내에 개인정보 보호를 위한 프라이버시 보호 계층의 인프라화가 필요하며, 이를 통해 개인식별 정보의 통합관리, 접근제어, 이용자의 식별과 인증 등의 공통기능을 수행하도록 함.
- 개인과 관련된 정보는 어떤 특정인과 연계되는 순간 개인정보화되는 경향이 있음. 이를 위해, 개인정보가 통합되는 것을 지양하고 개별 정보들이 쉽게 조합되어 개인정보화되는 것을 방지하는 대책 마련이 필요함.
- 개인정보의 사용범위는 서비스 제공자가 사용자에게 제시한 프라이버시 정책에 명시되어 있으며, 허가된 업무 인가자에 한하여 그 사용을 허가하여야 함.

5. 정보보호 대응전략 개발

○ 유비쿼터스 환경에서의 보안 위협에 효과적으로 대응하기 위해서는 IT 환경의 변화에 따른 보안 위협을 사전에 분석하여 신규 IT 서비스의 초기 단계에서부터 정보보호 대책을 적용하는 노력이 필요함.

○ 유비쿼터스 사회에서의 정보보호 대응전략은 안전한 네트워크 인프라 구현, 신규서비스 안전 및 신뢰체계 구축, 정보기기의 정보보호 기능강화, 개인정보보호 개발절차의 확립 등의 측면에서 살펴봄.

○ 특히 안전한 네트워크 인프라를 구축하기 위해서는 사이버 공격 예방전략 수립, 정보보호 요소기술의 확보, 정보기기 간 상호연동성 보장 표준화, 유비쿼터스 통합망 환경에 맞는 정보보호 규제 방안 마련 등이 필요함.

○ 서비스의 안전 및 신뢰체계를 구축하기 위해서는 정보보호 사전 영향평가

제의 도입, 서비스 장애 대응체계, 통합인증 체계의 구축이 필요함.

○ 정보기기의 정보보호 기능을 강화하기 위해서는 홈네트워크/텔레매틱스 등에 활용되는 다양한 이동통신 기기를 노린 정보침해 공격에 대한 대책 마련이 필요함.

Ⅱ. 정책건의

1. 유비쿼터스 정보보호의 중요성에 대한 공감대 형성이 필요함.

○ 개인정보의 집적화 활용은 정보화의 진전과 함께 계속 증가할 수밖에 없고, 정보의 데이터베이스화와 공동 활용은 정보화의 효용을 극대화시키는데 필수적이기 때문에 인터넷 침해사고나 개인정보의 악용이 발생할 가능성은 더욱 커질 수밖에 없음.

○ 정보보호를 위한 인프라는, CCTV의 설치와 관련된 논란에서 알 수 있듯 시민의 안전을 위해 불가피한 측면이 있으나 시민 사생활 보호를 저해한다는 측면에서 일정정도 타협점(trade-off)이 필요한 측면이 많음.

○ 하지만, 이 연구에서 살펴본 바와 같이, 정보보호를 위한 인프라를 체계적으로 구축하고 개인정보보호를 위한 강력한 가이드라인을 갖춤으로써 시민과의 충분한 공감대 형성을 촉진할 수 있는 방안 마련이 강구되어야 함.

2. 네트워크 모니터링을 통해 정보침해 예방체계 구축이 필요함.

○ 유비쿼터스 사회에서의 정보침해는 유비쿼터스 네트워크의 특성상 일단 사고가 발생하면 전체 네트워크로 빠르게 확산될 위험이 매우 높음.

○ 따라서, 개인정보 침해사고에 대한 예방 대응체계를 고도화함으로써 BcN, IPv6등 첨단 네트워크의 이상 징후를 모니터링할 수 있도록 하여 침해사

고 대응 성능을 높이고 차세대 위협에 대한 취약점과 대응방법을 미리 개발하며, 신규 취약점을 분석할 수 있는 능력을 강화하여야 함.

○ 그리고 통합망의 연계성이 점차 국제적으로도 높아지므로 국제 관련기관 간 협력을 강화하여야 하며, 이를 담당할 전문인력의 육성을 체계적으로 지원할 필요가 있음.

3. u-Service 표준화로 정보보호 체계 정립이 필요함.

○ 체계적인 유비쿼터스 정보보호 원칙과 개념을 개발하기 위해서는 u-Service의 기본개념과 기능을 중심으로 관련 시스템 체계와 프로세스를 표준화할 필요가 있음. 현재는 u-Service 개발에 있어 유사한 서비스들이 서로 다른 이름으로 소개되거나 서로 다른 계층적 분류를 가지게 됨에 따라 매우 혼란스러운 실정임.

○ 따라서, u-Service를 특징지을 수 있는 분류기준(classification factor)을 개발하여, 앞으로 추가되거나 현재 개발되어 있는 u-Service들을 쉽고 빠르게 분류할 수 있는 체계의 마련이 필요함.

○ 이러한 체계를 통해 분류별로 어떠한 형태의 개인정보침해 유형이 발생하는지, 그리고 그러한 정보침해를 예방하기 위한 대책은 어떻게 마련되어야 하는지 등에 대한 상세한 가이드라인을 마련하여야 함. 이러한 체계는 공공 또는 민간에서 제안되는 u-Service들의 정보침해 사전영향 평가제를 실시하기 위한 프레임워크 역할도 할 수 있을 것으로 판단됨.

목 차

표 목 차

그림목차

제1장 연구의 개요

제1절 연구의 배경 및 목적

제2절 연구 절차 및 수행방법

제1장 연구의 개요

제1절 연구의 배경 및 목적

1. 연구의 필요성

○ 지금은 시민생활과 산업경제에 급진적 변혁을 일으킬 것으로 예측되는 유비쿼터스 도시가 실현될 수 있도록 서울시의 u-City 구현 목표에 대해 심도있는 논의가 필요한 시점임. 특히 유비쿼터스 사회의 시민 신뢰도와 직접적인 연관이 있는 정보보호 측면의 고려가 필요함.

- 이와 관련된 중앙정부의 사업추진 일정에 비추어 2010년 전후 유비쿼터스 관련 기술 및 제반여건의 변화가 급진적으로 발생할 소지가 있기 때문임.
- 또한, 국내의 u-City 사업은 기술주도형으로 주요 정보기술에 대한 성공적 개발에 의존하고 있는 실정이므로 전략적 측면 및 소프트웨어적 요소, 그리고 관련 정책 개발 측면에 대한 강조가 다소 미흡함.
- 이렇듯 일부 측면만을 강조하는 u-City 비전은 유비쿼터스 도시에 대한 올바른 이해를 저해할 뿐 아니라 유비쿼터스 도시 건설의 목표를 왜곡할 소지가 있음.

○ 유비쿼터스 환경에서는 BcN, USN, IPv6 등 3대 인프라의 도입이나 통신과 방송의 융합으로 사이버 위협의 대상이 IP를 사용한 특정 망에서 통합된 망으로 전이되어 피해 확산속도가 빨라지고, 피해 규모 역시 확대될 것으로 우려됨.

- 홈 네트워크, 텔레매틱스 등 서비스 융합화가 본격적으로 진행되면서 사이버 위협이 ALL-IP 망으로 확대될 것으로 전망됨.

- 또한, 9대 신성장 IT 디바이스의 정보보호 기능이 미흡한 경우 기기의 신뢰성 저하, 서비스 장애 등의 위협을 초래할 것으로 예상됨.

○ 진정한 유비쿼터스 사회를 실현하기 위해서는 시민의 개인정보보호에 대한 사전 준비가 충분히 이루어져야 함. 하지만 정부가 추진 중인 유비쿼터스 관련 정보화 플랜에서의 정보보호 측면은 그 중요성에 비해 상대적으로 고려가 미흡함.

- 유비쿼터스 사회에서는 정보의 주체가 인식하지 못하는 사이에 개인의 신상정보가 저장, 축적되고 노출될 위험성이 높음. 이는 폭넓은 정보공유의 반대급부로서 피할 수 없는 문제이기도 함.

○ 개인정보의 부적절한 수집 및 사용으로 인한 정보침해 문제는 유비쿼터스 컴퓨팅(ubiquitous computing)이 가져다 줄 긍정적인 효과를 반감시키는 데 결정적인 요인으로 작용할 전망임.

- 이러한 경향은 유비쿼터스 네트워크 및 서비스에 대한 시민 신뢰도의 저하로 이어질 수 있음.

2. 연구의 목적, 내용 및 기대효과

1) 연구목적

○ 유비쿼터스 사회에서의 개인정보 침해 요인들을 분석하고 개인정보 보호를 위한 요구사항들을 정립함으로써, 앞으로 유비쿼터스 서비스의 설계 및 개발 시 개인정보보호 측면의 요구사항이 반영될 수 있도록 개념적 가이드라인을 제시하고자 함.

2) 연구내용

○ u-City와 관련된 기본 개념들과 국내 · 외 추진현황을 정리함. 현재의 개

인정보보호 패러다임 및 기반기술들은 유비쿼터스 사회가 도래함에 따라 혁신적인 발전이 필요하므로, u-City의 기본 개념을 일반 시민이 공감할 수 있는 수준에서 국내·외 u-City 추진현황을 살펴봄.

○ 유비쿼터스 사회의 정보보호에 대한 의의를 살펴보고 문제점을 분석함. 개인정보의 의의 및 분류체계를 살펴보고 유비쿼터스 사회의 도래에 의한 정보보호 환경의 변화요인들을 분석함. 이러한 과정을 통해 유비쿼터스 정보보호 현황 및 문제점을 기술적 영역, 규제적 영역, 그리고 사회적 영역 등의 3가지 영역으로 구분하여 정리함.

○ 유비쿼터스 서비스에 정보보호 측면을 반영한 개념설계 가이드라인을 개발함. 유비쿼터스 서비스를 구성하는 정보보호 요인 분석을 통해, 유비쿼터스 서비스를 개발할 때 반드시 고려되어야 하는 측면들인 유비쿼터스 네트워크 보안측면, 개인정보 수집 및 활용측면 등을 분석함. 이 과정을 통해 유비쿼터스 서비스 구현 시 필요한 정보보호 요구사항들을 개발함.

- 체계적인 유비쿼터스 정보보호의 원칙과 개념을 개발하기 위해서는 u-Service의 기본개념과 기능을 중심으로 체계와 프로세스를 표준화할 필요가 있음. 현재는 u-Service 개발에 있어 유사한 서비스들이 서로 다른 이름으로 소개되거나 서로 다른 계층적 분류를 가지게 됨에 따라 매우 혼란스러운 실정임.

- 이 연구에서는 지능제어(Intelligent Control) 모델을 확장하여 u-Service의 패턴을 분류, 체계화하고 패턴별로 앞에서 정의된 정보보호 요구사항을 매핑(mapping)하는 형태로 u-Service 설계 가이드라인을 제시하려고 함.

3) 기대효과

○ 서울시의 u-City 관련 정보화 플랜에 시민들의 개인정보보호 측면을 반영함으로써 보다 현실적인 플랜이 될 수 있으며, 서울시에서 제시하고 있는 u-City 비전에 대한 시민들의 공감대 형성에도 도움을 줄 수 있음.

제2절 연구 절차 및 수행방법

○ 연구보고서의 연구내용 및 절차를 정리하면 <표 1-1>과 같음.

<표 1-1> 보고서 구성 체계

연구 내용		세부 연구 내용
Ⅰ	연구의 개요	• 연구의 배경 및 필요성 • 연구 목적, 내용 및 기대효과 • 연구 절차 및 수행방법
Ⅱ	u-City 추진현황	• u-City(Ubiquitous City) 개요 • 국내외 u-City 구축현황
Ⅲ	정보보호의 이론적 배경	• 정보보호 개요 • 정보보호환경과 패러다임의 변화 • 유비쿼터스 정보보호의 의의
Ⅳ	정보보호 현황 및 문제점	• 유비쿼터스 환경의 개인정보보호 침해 • 기술적 영역의 현황 및 문제점 • 규제적 영역의 현황 및 문제점 • 사회적 영역의 현황 및 문제점
Ⅴ	u-Service의 정보보호 가이드라인	• 개인정보보호 요구사항 • 정보보호 대응전략 • u-Service 표준화를 통한 정보보호 체계 개발
Ⅵ	결론 및 정책제언	• 결 론 • 정책 제언

제2장 u-City 추진 현황

제1절 u-City(Ubiquitous City) 개요

제2절 국내·외 u-City 구축현황

제2장 u-City 추진 현황

제1절 u-City(Ubiquitous City) 개요

1. 개요

1) u-City의 등장 배경

(1) 시민의 삶의 질 향상을 위한 대안 마련이 필요함.

○ 도시라는 공간은 현대인의 삶에 가능성이면서 한계라는 양면성을 가지고 있음.

- 자연의 위협에 대한 방어, 생산력의 제고, 비용의 절감, 세련된 문명 등을 제공한다는 측면에서는 긍정적이나, 인위적으로 특정 장소에 밀집되어 있음으로 해서 다양한 문제들이 발생됨. 예를 들어 일터와 삶터의 공간적 분리에 따른 시공간의 비효율화, 용지부족, 주거공간의 과열 밀집, 난개발, 대형화재의 위험, 교통문제, 도시범죄, 주거불안정, 대중소요의 위험, 지역 간 갈등, 대기공해, 토질 악화, 식수 부족 및 수질 악화, 도시형 재난, 대형 범죄, 도시확장에 따른 자연파괴, 전통 파괴에 따른 아노미 현상, 공공서비스의 대응능력 부족현상 등 수많은 문제들이 해결될 수 없는 상태로 지속되고 있음.

○ 그러나, 산업 생산성이 증가하고 개인소득이 증대됨에 따라 삶의 질에 대한 관심이 높아지고 있고 행정신도시, 혁신도시 건설 등으로 인해 도시마다 그 기능과 역할이 세분화·분산화 되어가고 있음. 이에 따라 도시 간의 기능 연계 및 역할 분담, 그리고 도시 경쟁력의 중요성이 높아지고 있음.

○ 따라서 도시 간 기능의 연계와 함께 도시자체의 설계에 정보통신 기술을 반영하여 주민의 생활을 편리하게 하는 등 다양한 분야에 대한 도시기능

을 효율적이고 체계적으로 구현할 필요성이 커지고 있음.

○ 즉, 기존의 도시와는 달리 도시의 다양한 기능에 정보기술을 접목시켜 주민에게 편리한 생활을 영위하게 하고, 기업에게는 비즈니스 효율 향상의 기회를 제공하며, 지자체에게는 효율적인 도시 관리 등을 이루게 하는 신개념의 도시가 필요한 상황임. 이러한 신개념의 도시가 u-City라고 할 수 있음.

(2) 국가와 지자체의 신 성장동력 마련이 필요함.

○ 국민들이 소득 향상과 함께 편안한 삶을 영유할 수 있는 환경을 조성하기 위해서는 경제의 활성화 및 부흥을 위한 신산업 성장 동력으로 유비쿼터스 기술과 이를 실제로 접목한 u-City의 건설이 절실히 필요한 시점임.

○ 아울러, IT의 메가 트렌드인 디지털 컨버전스(digital convergence)의 등장으로 신규 제품 및 시장이 생성됨에 따라, 승자가 모든 것을 갖는 IT 시장에서 승자가 되기 위한 전략 개발이 요구됨. 또한, 한계이익에 도달한 IT 성과의 재도약을 통해 신고부가가치를 창출하고 신성장의 계기로 삼아 글로벌 시장을 선점할 수 있는 전략을 마련해야 함.

- 유비쿼터스 네트워크에 기반한 u-City를 구축하기 위해서는 정보기술의 고도화가 전제되어야 함. 컨버전스 기술의 일반화 · 광대역화, IT 기기의 가격저하 등이 없이는 모든 기기에 통신 능력을 부여하는 것이 어렵기 때문임. 실제로 유비쿼터스 시대가 열리게 되면 자동차, 가정, 실외 등 다양한 공간에서의 IT 활용이 늘어나고 네트워크에 연결되는 컴퓨터 사용자의 수도 늘어나는 등 IT 산업의 규모와 범위는 더욱 커지게 될 전망임.

(3) u-City의 정의

○ 도시는 그 자체로 다양한 기능 및 역할을 수행하고 있기 때문에 도시의 기능에 유비쿼터스의 개념이 결합되어 있는 형태인 u-City에 대해 명확한 정의를 내리기는 어려우나 다음과 같음.

- u-City는 주거, 산업, 문화, 행정, 환경 등에 대한 도시기능을 효율적이고 체계적으로 구현하기 위해, 도시기획의 초기단계부터 IT 기술과 정보통신 인프라를 반영함으로써, 정보화에 따른 도시생활의 편의 도모, 삶의 질 향상, 체계적인 도시관리에 의한 안전과 주민복지 향상 등 도시의 기능을 획기적으로 향상시킬 수 있는 도시라고 할 수 있음.

- 궁극적으로 u-City는 유비쿼터스 컴퓨팅(ubiquitous computing)과 정보통신 기술을 기반으로 도시 전반의 영역을 융합(convergence)하여, 통합되고(integrated), 지능적(intelligent)이며, 스스로 혁신(innovative)되는 도시 건설이 목표임.

- 정보통신 인프라와 유비쿼터스 정보 서비스를 도시 공간에 융합하여 도시생활의 편의 증대와 삶의 질 향상, 체계적 도시관리에 의한 안정보장과 시민복지 향상, 신산업 창출 등 도시의 제반 기능을 혁신시킬 수 있는 21세기 한국형 신도시를 의미함.

2) 유비쿼터스 네트워크

○ 유비쿼터스 컴퓨팅이란 용어는 Xerox PARC 사의 마크 와이저가 1988년 “사용하기 쉬운 컴퓨터” 라는 제목의 논문에서 처음으로 제시함.

- 이 논문에서 마크 와이저는 업무 처리 시간보다도 컴퓨터 조작에 더욱 많은 시간을 소비해야 하는 문제점을 지적하고 인간 중심의 유비쿼터스 컴퓨팅 기술을 제안함.

- 마크 와이저는 1991년에 발표한 논문 “The computer for the 21st

Century"에서 유비쿼터스라는 개념을 좀 더 명확히 정리하여 "미래의 컴퓨터는 우리가 그 존재를 의식하지 않는 형태로 우리 생활 속에 점점 파고들면서 확산될 것이다. 한 개의 방에 수백개의 컴퓨터가 설치되고, 그것들은 유무선 네트워크를 통해 상호 연결 될 것이다"라고 함.

- 이후 유비쿼터스 컴퓨팅은 "어디에나 컴퓨터가 존재하며, 자연스럽고 의식하지 않고 사용" 할 수 있는 새로운 컴퓨팅 패러다임으로, 유비쿼터스는 "언제, 어디서나 컴퓨터를 사용하고 네트워크에 접속되어 서비스를 누릴 수 있는 IT 환경" 이란 개념으로 사용되어 왔음.

○ 이는 1999년 일본의 노무라 연구소에 의해서 "인간이 언제 어디서나 네트워크에 연결되어 있는 IT 환경"이란 의미의 유비쿼터스 네트워크란 개념으로 확대됨.

○ 유비쿼터스는 5C5A를 지향하는 공간 환경으로서 IT 뿐만 아니라 BT, NT, ET 등 최신 기술의 융합을 포함하는 유비쿼터스 기술에 의해 기존의 물리적 공간과 전자적 공간이 실질적으로 결합된 공간 개념임.

- 여기서, 전자공간과 유비쿼터스 공간의 근본적 차이는 과거의 전자공간이 현실의 물리적 공간을 컴퓨터에 가상적 상황으로 귀속시키는 것이었다면 유비쿼터스 공간은 물리적 공간에 정보의 수신과 발신, 처리 기능을 갖는 컴퓨터가 이식된 환경임.

- 결론적으로, 유비쿼터스 공간은 물리공간과 전자공간의 한계를 동시에 극복하고, 사람, 컴퓨터, 사물이 하나로 연결된 새롭게 창출된 공간이라고 할 수 있음.

3) 유비쿼터스 도시(u-City)에 대한 이해

○ u-City는 유비쿼터스 기술이 접목된 공간들로 이루어진 도시를 의미함. 즉, 도시를 구성하는 수많은 환경, 구조물 등에 컴퓨터가 이식됨으로써 이

들이 전자공간으로 연결되어 정보를 주고받고, 사람과의 커뮤니케이션도 이루어져 언제, 어디서나 다양한 서비스를 주고받을 수 있게 된 도시를 의미함.

○ 유비쿼터스 도시 사회란 모든 사물들이 지능화되고 네트워크화됨으로써 인간과 인간, 인간과 사물, 더 나아가 사물과 사물 간에 대화가 가능한 사회라고 말할 수 있음.

○ 유비쿼터스 도시는 유비쿼터스 기술을 기반으로 도시의 모든 자원을 지능화시키고 이를 네트워크화하며, 이를 통해 도시의 모든 시스템을 혁신시키고 도시 내 기업의 생산성을 형상시키며 시민들에 대한 서비스 향상을 극대화하여 궁극적으로 도시 안에 사는 시민 각 개인의 삶의 질을 한 단계 향상시키는 미래형 도시를 말함.

(1) 유비쿼터스 사회

○ 유비쿼터스 기술이 중심이 되는 유비쿼터스 사회는 사람들이 언제, 어디서나 도구나 네트워크의 장애 없이 정보와 서비스를 주고받을 수 있는 사회임. 단, 컴퓨터는 모든 사물에 내재되어 있어 보이지 않고, 그러한 컴퓨터들을 통하여 우리가 의식하지 않아도 서비스가 스스로 이루어져야 하며, 모든 컴퓨터들이 서로 연결되어야 함.

○ 유비쿼터스 사회는 시간, 거리의 제약이 소멸되는 사회로, 개인을 위한 정보와 서비스가 맞춤형으로 전개되는 사회를 의미함. “제3의 공간”이라는 유비쿼터스 공간에서는 사물 속에 내재된 컴퓨터들과 무선 네트워크로 연결되어 사람이 인식하지 못하는 상황에서도 의사소통을 할 수 있고, 정보를 주고받아 실시간으로 선도 높은 정보를 제공하거나 필요한 의사결정을 내려줄 수도 있게 됨으로써 물리적 공간과 가상공간이 최적으로 연계·통합된 기능을 형성할 수 있게 됨.

(2) 기존 도시개발과의 차이점

○ u-City와 일반 도시와의 차이점을 크게 개발계획, 디지털 격차, 서비스 제공, 도시 관리 측면에서 분석하면 다음과 같음.

- 개발계획 측면의 경우, 일반도시는 눈에 보이는 공간에 대한 마스터플랜을 구상하는데, u-City는 도시 공간과 눈에 보이지 않는 환경에 대한 구상까지 포함함.
- 디지털 격차 측면의 경우, 일반도시는 행정중심의 키오스크(kiosk)나 AP(Access Point)를 설치하고 수익성 중심으로 유·무선 망을 계획하는데 반해, u-City는 공공주택 뿐 아니라 단독 주택지 등에도 일정수준 이상의 인프라를 구축하여 다양한 공공 공간에서 일반시민들의 인터넷 이용을 용이하게 함.
- 서비스 제공 측면의 경우, 일반도시는 지방자치단체가 계획하고 있는 공공서비스와 연계하고 부가서비스는 민간 사업자 계획에 의해서만 제공하지만, u-City는 다양한 공공서비스를 많은 전달매체를 통해 제공하고 고품질의 부가서비스를 제공함.
- 도시 관리 측면의 경우, u-City는 일반 도시에 비해 기술발전에 대비한 유·무선 망 계획이 가능하여 계획에 소요되는 비용을 절약할 수 있고, 도시시설에 대한 관리 효율성도 큼.

제2절 국내·외 u-City 구축 현황

1. 중앙정부 차원의 u-City 관련 추진 현황

(1) 국가 차원의 추진 현황

○ 유비쿼터스와 관련해서 정부가 추진하고 있는 전략 중 대표적인 것이 'u-Korea'로, 그 핵심은 IT839[1] 전략임.

○ u-Korea 전략의 추진 배경은 다음과 같음.

- IT의 메가 트렌드인 디지털 컨버전스(digital convergence)의 등장으로 신규 제품 및 시장이 생성되게 되었으며, 승자가 모든 것을 갖는 IT 시장에서 승자가 되기 위한 전략이 요구됨. 또한, 한계이익에 도달한 IT 성과의 재도약을 통한 신고부가가치 창출과 이를 통한 신성장의 계기를 마련하여 글로벌 시장을 선점할 수 있는 전략이 요구됨.

- 각 부처 단위 및 특정 영역단위별로 추진되고 있는 관련 정책 간의 시너지 효과 제고 및 유비쿼터스 사회 진전에 따라 발생할 수 있는 문제를 사전에 방지하기 위한 국가차원의 종합적인 전략 마련이 요구됨.

○ 정부차원에서 제시된 u-Korea 전략 가운데 지방자치단체의 u-City 추진에 직접적 동인을 제공한 것으로 볼 수 있는 사업으로 IT839 시범사업인 "1300만 가구에 홈네트워크의 시범구축", "텔레매틱스 시범도시 구축", "u-센서 네트워크의 전국 확대" 등을 들 수 있음.

---

1) IT839는 8대 신규서비스(2.3GHz 휴대인터넷, DMB(위성/지상파), 홈네트워크 서비스, 텔레메틱스 서비스, RFID 활용서비스, W-CDMA 서비스, 지상파 DTV, 인터넷 전화(VoIP), 3대 인프라구축(광대역통합망, u-센서 네트워크, IPv6), 9대 신성장동력(차세대 이동통신, 디지털 TV, 홈네트워크, IT SoC, 차세대 PC, 임베디드 S/W, 디지털 콘텐츠, 텔레메틱스, 지능형 로봇)을 일컬음.

(2) 중앙정부 기관차원의 추진현황

○ (구)과학기술부는 “21세기 프론티어 연구개발사업”으로 유비쿼터스 컴퓨팅, 네트워크 원천기반기술개발사업을 추진 중이며, uT 홈/빌딩, uT 타운, uT 코리아 실현에 필요한 유비쿼터스 핵심기술 개발을 3단계(2002~2013년)로 구분하여 추진하고 있음.

○ (구)산업자원부는 기업물류시스템 혁신 및 물류산업의 고도화 지원을 위한 핵심물류기술 확보를 위해 RFID 기반 유비쿼터스 전자물류시스템 기술, 신속물류망 형성기술, 모바일 기술을 이용한 공급사슬망관리시스템 구축 및 지능형 물류센터 운영시스템 개발 등을 포함하는 “지능형 종합물류시스템 기술개발”을 추진 중이며, “지능형 홈 산업 발전전략”을 수립하여 그 과제의 하나로 유비쿼터스 컴퓨팅 및 네트워크 원천기술 개발을 시도하고 있음.

○ (구)건설교통부는 “국가 GIS 추진 3단계 전략”을 수립하여 추진하고 있음. 1995~2000년에 수행된 1단계는 공간정보 데이터베이스 구축을 중심으로 한 GIS 기반 조성단계이고, 2001~2005년에 수행된 2단계는 1단계에서 구축된 공간정보를 활용한 대 국민 응용서비스를 개발하는 GIS 활용단계이며, 그리고 2006년에서 2010년까지 수행될 3단계는 언제, 어디서나 필요한 공간정보의 편리한 생산, 유통, 이용 등이 가능하게 하는 GIS 정착단계임.

○ 농림부도 농식품안전종합대책의 일환으로 유비쿼터스 사업을 추진하고 있음. 여기에는 농축산 농가 이력정보통계와 농축식품정보체계 및 농축산물 유통체계 구축, 국내 가축방역 지리정보시스템, 국가검역 DB 체계 구현 등이 포함되어 있음.

○ 그 외에도 문화관광부의 “디지털 공공도서관 사업”, 환경부의 “국립공원 관리”, 재경부의 “LBS 시장활성화” 등의 정책이 있으며, 지자체의 경우 UIS(Urban Information System) 구축을 목표로 다양한 사업들이 진행되고 있음.

2. 지방자치단체의 u-City 관련 추진 현황

○ 지방자치단체에서 추진하는 u-City는 u-City가 개발되는 공간적 입지, 기존도시와의 관련성에 따라 기존도시 지역에 적용되는 '기존도시 적응형'과 기존의 도시를 모도시로 하고 이에 인접하여 지구 또는 단지 차원에서 개발하거나 대규모 신도시를 u-City로 개발하는 '신도시 개발형'으로 구분할 수 있음.

- 자치단체의 u-City 추진전략 가운데 기존도시 적응형은 부산, 광주, 전주, 제주가 기존의 도시 공간구조란 전체적 틀에서 u-City 개발을 구상하거나 계획하고 있으며, 신도시 개발형은 송도만이 전체 도시적 차원에서 장기적 계획으로 u-City 개발에 임하고 있음. 나머지 지역들은 100만평 내외의 지구차원에서 u-City를 추진하고 있음.

○ 서울, 부산 등 14개 기존도시, 행복도시, 화성/동탄 등 8개 신도시 등 전국 22개 지역에서 u-City 사업을 적극 추진 중임. 대표적인 경우를 들어 설명하면 다음과 같음.

(1) u-송도(인천광역시)

○ 인천경제자유구역(1단계 773만평, 인구 25만명)에 2020년까지 도시 전체를 총인구 50만의 u-City로 개발하려는 것으로 구체적인 마스터플랜과 첨단 IT도시 구축을 위한 전략을 수립하고 있음. 여기에는 장래(시간대별) 발전 시나리오 및 공간·시설별 정보 인프라의 설계가 포함되어 있음. 비전은 All in One Network, 고도의 정보서비스 제공, 디지털 웰빙 구현, 21세기 첨단 정보화 도시임.

○ 또한, 도시건설 후에도 u-City로서 지속성을 유지할 수 있도록 관리하기 위한 조직구성 및 운영방안의 마련에 노력을 경주하고 있음.

(2) u-상암(서울특별시)

○ 서울시는 2007년까지 상암동에 상암 DMC(Digital Media City), 첨단정보미디어 단지(17만평)를 최첨단 IT 콤플렉스, R&D, 모바일 비즈니스의 테스트베드 역할이 중심인 디지털 콘텐츠 산업의 허브로 조성하기 위한 사업을 수행하고 있으며, 2008년 6월부터 첨단산업센터에 기업들의 입주가 시작됨.

○ 유비쿼터스 서울을 구현하기 위한 서울시의 마스터플랜인 'u-서울 마스터플랜'에 대해서는 항을 바꾸어 설명함.

(3) 디지털 시티(용인시)

○ 한국토지공사는 용인시 기흥읍 영덕리 일원(약 64만 9천평, 수용인구 29,000명)의 흥덕택지개발지구를 2008년까지 5년 동안 '미래형 디지털 시범도시'로 개발하기 위해, 지구 전체의 인프라인 초고속 광통신망 구축과 아파트 단지에 초고속 인터넷망 설치, ITS 설치, 신호등/도로/지하시설물 등에 통신칩 설치 등을 추진함. 이를 통해 도시 전체를 도시정보관제센타(공공정보상황실)의 컴퓨터 시스템으로 관리하는 미래형 도시가 목표임.

(4) u-광주(광주광역시)

○ 광주시는 국내 최고 수준의 디지털 공동체 건설을 목표로, 뉴미디어 콘텐츠 산업 중심의 소프트 타운(유비쿼터스 성장동력 만들기) 조성, 유비쿼터스 기반의 생산시설 구축, 유비쿼터스 기반 첨단 신도시 건설, u-건설 장기 종합계획 수립(2005~2012년) 등 유비쿼터스 광주를 실현하기 위한 10대 전략을 발표함.

(5) u-부산(부산광역시)

○ u-부산의 추진 목적은 도시 교통문제의 해결, 기술과 인프라의 조화를 통한 선도도시 조성으로 이미지를 개선함으로써 후퇴하고 있는 도시경제의 재도약과 시민의 삶의 질 향상에 있음.

○ u-부산을 구현하기 위한 핵심프로젝트들은 센텀 시티 유비쿼터스 클러스터 조성(교통 및 지역 시스템 통제센터, 최상의 유비쿼터스 통신 및 IT 빌딩 구축, 유비쿼터스 컨벤션 및 전시 센터), 유비쿼터스 솔루션을 적용한 신 항만 건설, 도시 행정, 지능형 교통시스템 구축 등임.

(6) u-제주(제주도)

○ 정부의 IT839 전략인 텔레매틱스 시범사업과 연계하여 각종 유비쿼터스 기술의 시험 무대로, 유비쿼터스 시범도시를 지향하며, 국제자유도시 건설과 연계하여 개발하려는 전략을 추진하고 있음.

○ 세부적인 전략은 크게 u-City(도시교통센서네트워크 구축), u-Ecology(생태계 모니터링, 수자원관리, 환경관리정보체계), u-Tour(문화관광자원정보체계, 전시관람 정보체계, 회의산업 정보체계), u-Safe(재난재해정보체계)의 네 부문으로 나누어짐.

(7) 기타

○ 경상북도는 도 차원에서 국내 최대 유비쿼터스 테스트베드 만들기를 목표로 u-경북을 추진하고 있는데, 주요 내용은 u-NT 특구, u-IT 특구, u-관광 특구, u-교육 특구, u-BT 특구 등 분야별 킬러 시스템을 개발하는 것임.

○ u-대전의 경우 유비쿼터스 관련기술의 산업화를 지원하는 핵심기지로 조성과 유비쿼터스 체험공간 조성을 주요 추진 내용으로 하고 있으며, u-창원은 디지털 종합 방송망, 미디어 센터, 자동제어, RFID 기술활용, 지능

형 홈네트워크 시스템 구축 등을 주요내용으로 계획을 추진 중임.

○ 그 외에도 경기도 파주(한국주택공사), 수원 동탄(한국토지공사), 연기공주의 행정복합도시를 u-City로 건설한다거나, 충북의 오송생명과학단지를 u-City로 리모델링하려는 계획 등이 추진 중임.

3. 국외 u-City 추진 현황

(1) 국외의 일반 동향

○ 한국은 물류, 모바일, 도시인프라를 중심으로 유비쿼터스 서비스를 개발하고 있는데 비해, 미국은 국방, 의료, 물류를 중심으로, 일본은 주택(홈네트워크, 가전)과 안전서비스를 중심으로 서비스를 개발 중임.

- 미국은 국방성 산하의 고등연구계획국(DARPA)과 국립표준기술원(NIST)을 중심으로 캘리포니아 대학의 Smart Dust, Pervasive Computing, EasyLiving 등을 통해 다양한 유비쿼터스 컴퓨팅 프로젝트를 추진하고 있음.

- 일본에서는 1984년 이후 도쿄대학을 중심으로 추진되고 있는 TRON (The Realtime Operating System Nucleus) 프로젝트를 비롯하여 지능형 빌딩, 주택, 도시, 자동차망 등 기술개발 프로젝트가 다수 수행되고 있음.

- 유럽은 2001년에 시작된 유럽연합 정보화사회기술계획의 '사라지는 컴퓨팅 계획(Disappearing Computing Initiative)'을 중심으로 다양한 유비쿼터스 실험들을 추진하고 있음. 특히 스위스 연발기술연구소(ETH), 독일의 TecO(Telecooperation Office), 핀란드의 국립기술연구소(VTT) 등이 '스마트 사물' 프로젝트를 공동으로 추진 중임.

○ 해외국가 대부분은 IT 인프라 고도화에 치중하고 있는데, u-IT 기술 및 서비스를 도시 전반에 적용하려는 시도는 아직 미흡한 상태임. 즉, 해외에

서 유비쿼터스 도시의 개념은 아직 보편적으로 자리매김되고 있지 않으며, 인터넷시티, 미디어시티 등의 개념을 통해 도시정보 인프라 관점에서만 사용되고 있음.

- 대부분의 첨단 신도시에는 업무나 상업시설에 유선통신망 중심의 인프라가 구축되어 있으며, 공공시설에 무선망 구축이 증가하고 있는 추세임. 주거건물의 경우 신축 공동주택에 초고속정보통신망이 구축되는 수준으로 홈네트워크 도입 수준은 미미한 실정임.

○ 홍콩의 사이버포트, 말레이시아의 MSC, 두바이의 인터넷시티 등 국외 주요 u-City의 개발목표 및 주요시설을 정리하면 <표 2-1>과 같음.

<표 2-1> 국외 u-City의 개발전략 및 주요시설

도 시	개발목표/전략	주요 시설 및 IT인프라
홍콩 Cyberport	• 미디어산업(DMC)에 집중하여 전문성 높임 • 도시 전체에 첨단 IT 기술/디바이스/하이테크 디자인 구현-첨단이미지 높임 • 고급주거단지 개발을 통한 고급화	• 오피스 : 사이버포트 1/2/3/4 • IT street(DMC, 디지털자원센터, 전시/홍보시설) 중심 • 1-10G 무선랜
말레이시아 MSC	• 국가 전역의 IT 네트워크 구축 • 친환경적 멀티미디어 도시 • 규제완화, 기업에 대한 이력 제공 등 기업환경 제고	• 사이버자야(IT기업, 주거, 상업시설, 멀티미디어 대학), 테크놀로지 파크, 행정도시. • 초고속망 (일부)/ADSL • 방대한 규모에 비해 인프라수준 미약
싱가포르 One north	• 우수한 IT인프라를 바탕으로 미래산업(biomedical) 중심의 IT 복합자족도시 • 다국적 체류자의 라이프스타일에 대응하는 도시개발	• 생물의학도시, IT/미디어산업 중심도시, 지원도시로 구성 • 100Mbps
헬싱키 Arabianranta	• IT/미디어/디자인/문화도시 • 기존 건물의 재활용과 첨단건물 조화로 문화보존 이미지	• 첨단분야 대학 5개, 지역산업 전시장/판매장/공장, 비즈니스센터, 주거시설 • 1G 백본망/WiFi
코펜하겐 Crossroads	• IT & Eco 도시 • IT 기술개발의 테스트베드 • R&D의 테스트베드 역할	• IT대학, 덴마크 방송, 소비자 정보협회, 업무시설, 주거시설 • 100Mbps/무선랜
퀼른 Mediapark	• 미디어/관광도시(업무, 상업, 주거, 엔터테인먼트의 복합적 자족도시) • 미디어산업, 친수환경/녹지, 건축계획, 이벤트의 융합	• 16개 건축물군(병원, 뮤직타워, 문학하우스, 공동주택 등) • 100Mbps 유선망 중심

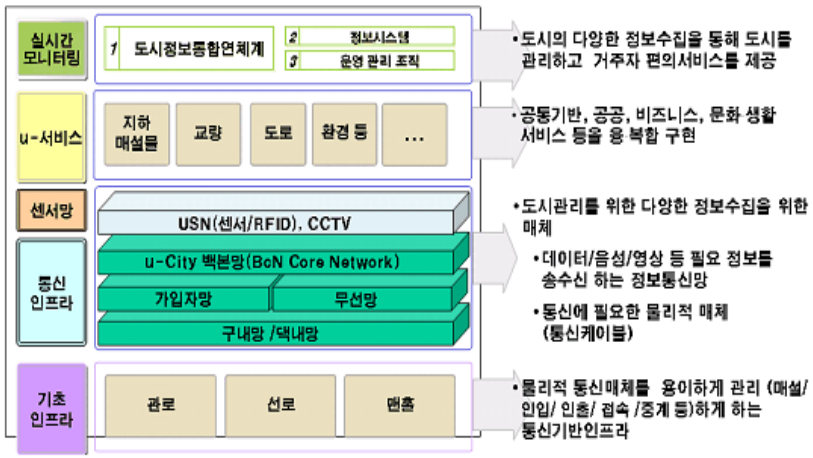
<표 계속> 국외 u-City의 개발전략 및 주요시설

도 시	개발목표/전략	주요 시설 및 IT인프라
두바이 Internetcity	• 정보산업의 세계적 허브 지향 • IT 기업유치를 위한 최적의 비즈니스 여건 제공(물리적환경, 지원제도) • 인터넷/미디어시티/인력공급 집적화	• 데이터 센터 • 100Mbps/무선랜, VoIP

4. 국내 u-City 추진 체계

1) u-City 인프라 구축 : u-City 인프라 아키텍처 표준화

○ u-City 인프라는 도시의 유비쿼터스 환경을 구현하기 위해 계획적으로 사전에 검증 및 표준화되어야 할 기본적인 구성요소임. 이는 u-City 인프라, 기술, 서비스, 도시통합모니터링 체계로 구성되며, 향후 추진 시 필요한 구성요소는 <그림 2-1>과 같이 크게 기초 인프라, 통신 인프라, 센서망, u-서비스 및 실시간 모니터링 체계 등으로 나눌 수 있음.



<그림 2-1> u-City 인프라 아키텍처(NIA)

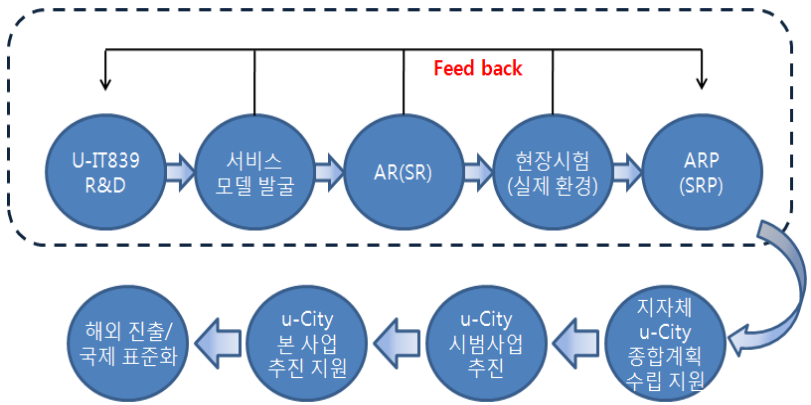
○ (구)정보통신부와 NIA(한국정보사회진흥원)가 2007년부터 버전1.0 수준의 u-City 인프라 가이드라인 마련에 대한 기초상세연구를 수행 중이며, 지속적으로 업그레이드할 예정임.

2) u-City 서비스 추진 방향 : 선 표준 모델 개발, 검증 후 운영, 확산

(1) u-City 서비스 추진 방향

○ u-City의 난개발 방지와 도시 간 상호 운영성 확보 및 연계를 위해서는 표준모델을 먼저 개발하고 이에 대한 경제적, 기술적 타당성을 충분히 검증한 후 확산 및 운영을 해야 함.

○ 이를 위해 <그림 2-2>와 같은 R&D → 테스트베드 구축을 통한 기술 및 서비스 검증 → 시행착오 최소화를 위한 표준화 → 시범사업 추진 → 본사업 추진 등의 단계적 추진이 필요함.



• AR(SR)/ARP(SRP) : 개별 서비스에 대한 사전적/사후적 적용 기술 및 서비스 시나리오
• U-IT839 : 8대서비스(HSDPA, WiBro, RFID 등), 3대 인프라(BcN, USN 등), 9대 신성장동력(IT SoC, 임베디드S/W, DTV 등)

<그림 2-2> u-City 서비스 추진단계

(2) 서비스 표준 모델 개발을 위한 u-City 테스트베드 구축사업 현황

○ u-City 관련 기술의 성숙도 및 지자체 수요 등을 반영하고, 공공성, 시급성, 기술적 구현 가능성이 상대적으로 큰 과제를 중심으로 세계 최초로 u-City 테스트베드 구축과제를 추진한 바 있음(2007. 5.12).

- 테스트베드 과제는 서울, 부산, 광주, 울산, 연기/행복청(행정중심복합도시건설청), 인천 송도 등 4개 기존도시와 2개 신도시에서 진행되고 있으며, 주요 내용은 <표 2-2>와 같음.

<표 2-2> u-City 테스트베드 구축 사업 현황

구 분	과 제 개 요
u-청계천 (생태/문화관리)	• 청계천을 중심으로 USN 기반 실시간 생태정보 관리 및 프리보드 형태의 방문기록, 동영상, 사진 촬영 등 문화 서비스 제공
u-해운대 (관광/안전관리)	• 해운대에 RFID/USN, GPS, CCTV 등의 기술을 적용한 유비쿼터스 관광존(u-Tour zone)을 구축하여 관광정보 제공 및 미아 찾기 서비스 등 시험 구현
u-컨벤션 센터 (지상시설물 관리)	• 3D GIS와 USN 기술을 접목하여 DJ컨벤션 센터 내 전력선, 가스관 등의 실시간 모니터링과 행사정보 및 주차관리 서비스 제공
u-태화강 (환경관리)	• 태화강과 공단 인근에 USN을 활용하여 수질/수위/대기 모니터링과 CCTV 및 대형 LED 전광판을 통한 태화강 인근의 방범 주차관리 서비스
u-세종/연기 (건설현장 및 공정관리)	• 본격 신도시 건설을 대비하여 RFID/USN, CCTV를 활용한 건설현장의 건설자재, 작업지 안전관리, 공사현장의 과적차량 모니터링 및 공사토로 인한 오·폐수관리 서비스 등 제공
u-국제신도시 (지하매설물 관리)	• RFID/USN, CCTV를 활용하여 인천 송도에 위치한 지하공동구(전력, 통신, 상수도관 등)의 화재, 누수 및 출입자 관리 등 구현

○ 2007년 테스트베드 구축 사업의 주요 목적 및 특징은 다음과 같음.

- RFID/USN, 모바일 RFID, 텔레매틱스, N/W CCTV, WCDMA, HSDPA, WiBro, IPv6, GIS/GPS 등 다양한 u-IT 기술을 활용하여 지하매설물, 도시구조물, 도로, 교통, 환경 등 도시기반 공공 및 생활 서비스 중 3개 이상의 단위 서비스를 통합, 연계하는 융/복합 서비스 모델 구현에 초점을 둠. 이는 향후 u-City 서비스가 상호 운영, 연계되고 통합관리될 것으

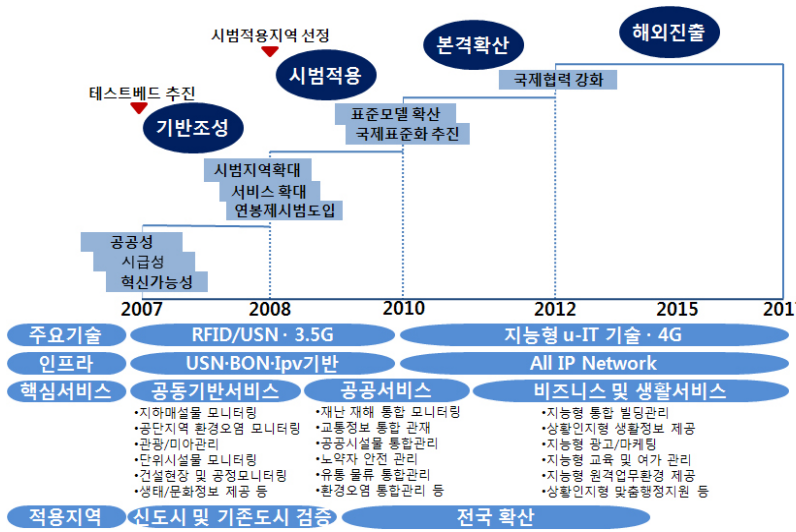
로 예상하고 타당성 분석과 검증을 하였다는 점에 의의가 큼.

- 신도시 뿐만 아니라 기존도시도 중점 고려하여 서비스 모델을 개발하였다는 점임. 이를 통해 도시 유형별로 다양한 서비스 구현 시 고려되어야 할 현장 애로사항에 대한 해결책 마련에 도움을 주고자 함. 또한 과제의 결과를 통해 u-City 서비스 표준모델 마련과 서비스 가이드라인을 제공하고자 함.

- u-City 추진 시 중요한 논의대상인 도시정보의 통합과 연계 체계를 어떻게 정의하고 구체화할 것인지에 대한 현실적인 해결 방안을 모색하고자 함.

3) 중장기 추진 계획(안) : 단계적이고 수요자 중심의 표준모델 개발

○ 앞으로 정부는 u-City를 기반조성, 시범적용, 본격확산 및 해외 진출 등 단계적으로 추진할 예정임. 대상지역은 신도시와 기존도시를 고루 적용하고, 서비스 개발은 공통기반 서비스와 공공서비스를 중심으로 추진하며, 특히 수용자 중심의 u-City 서비스를 지속적으로 발굴할 예정임.



<그림 2-3> u-City 중장기 추진계획(안)

제3장 정보보호의 이론적 배경

제1절 정보보호 개요

제2절 정보보호 환경과 개인정보보호 패러다임의 변화

제3절 유비쿼터스 사회의 정보보호 의의

제3장 정보보호의 이론적 배경

제1절 정보보호 개요

1. 개인정보의 개념정의

○ 개인정보는 법률상 정의를 통해 그 개념을 살펴볼 수 있음. 개인정보의 개념은 국가 혹은 법 집행 주체에 따라 다르게 규정됨.

- 유럽연합(European Union)의 개인정보보호지침에서는 '신체, 정신, 심리, 경제, 문화, 사회적 특성의 요소에 의하여 직접 또는 간접적으로 식별되는 자연인에 관한 정보'로 정의함.
- OECD는 '식별된 또는 식별될 수 있는 개인에 관한 모든 정보'로 정의함.
- 영국의 정보보호법에서는 '생존하는 개인의 신원을 식별할 수 있는 당해 데이터와 데이터 관리자가 보유하거나 장차 관리할 가능성이 있는 데이터로서 당해 개인에 관한 표현까지도 포함'하도록 규정됨.
- 우리나라의 경우 공공부문에서는 '생존하는 개인에 관한 정보로서 당해 정보에 포함되어 있는 성명·주민등록번호 등의 사항에 의하여 당해개인을 식별할 수 있는 정보(당해 정보만으로는 특정개인을 식별할 수 없더라도 다른 정보와 용이하게 결합하여 식별할 수 있는 것을 포함한다)'[2]로 정의함.
- 민간부문에서도 이와 유사하게 '생존하는 개인에 관한 정보로서 성명·주민등록번호 등에 의하여 당해 개인을 알아볼 수 있는 부호·문자·음성·음향 및 영상 등의 정보'[3]로 정의함.

---

2) 「공공기관의개인정보보호에관한법률」 제2조 제2항

3) 「정보통신망이용촉진및정보보호등에관한법률」 제2조 제6항

○ 이러한 법적 규정들을 토대로 기존의 여러 연구들도 개인정보에 대하여 나름의 정의들을 내리고 있음.

- 정영화(2002)는 '생존하는 자연인의 내면적 사실, 신체나 재산상의 특질, 사회적 지위나 속성에 관하여 식별되거나 또는 식별할 수 있는 정보의 총체'로 정의함.

○ 다양한 법적 규정과 개념들을 살펴본 결과, 개인정보는 공통적으로 '개인을 특정할 수 있는 모든 정보'를 의미함. 기존의 연구들도 이러한 보편적 정의를 토대로 개인정보의 중요성과 개인정보보호의 역할을 부각시키는 다양한 연구들을 시도하고 있음.

2. 개인정보의 분류체계

○ 개인정보의 분류체계는 최근 개인정보보호에 관한 논의가 활발하게 이뤄지면서 본격적으로 체계화되기 시작한 것으로 보임. 이러한 분류체계와 기준은 개인정보의 취급과 이를 다루는 제도의 내용에 큰 영향을 미치게 되며, 궁극적으로는 개인정보에 대한 사회적 인식을 반영한다고 볼 수 있음.

1) 주체별 분류

○ 개인정보는 관리주체에 따라 일반적으로 공공개인정보와 민간개인정보로 분류할 수 있는데, 공공개인정보와 민간개인정보는 관리주체나 법적 근거에 있어서 큰 차이를 보이고 있음. 현재 우리나라의 개인정보보호 법률체계는 이러한 분류체계에 기반하고 있음.

- 공공개인정보는 공공기록, 정보주체로부터 직접 수집한 기록, 정보주체 이외의 자로부터 수집한 기록 등으로 구분되며, 수집단계부터 각종 행정법규의 정확한 법적 근거에 따름.

- 민간개인정보는 원칙적으로 당사자 간의 계약에 의하여 수집 및 관리

되는 정보로, 거래관계의 대상에 따라 다양하게 나타나지만 대개 개인정보를 제공하고 반대급부를 받는 정보주체에 대한 보호차원에서 규제가 이루어짐. 대표적인 예로 신용정보, 의료정보, 통신정보, 인터넷거래정보, 고용 및 근로정보 등을 들 수 있음(황인호, 2001).

○ 영국의 정보위원회(Information Commissioner's Office)는 개인정보 항목 및 관리·보호절차에 관하여 고지받을 대상인 정보주체를 구분하고 있음. 이러한 정보주체 분류는 보호대상이 되는 행정객체, 즉 공공이나 민간이나 잠재적인 개인정보 분쟁의 당사자를 명확히 사전에 분류하여 그에 적합한 정보제공 및 정보주체별 권리보장을 실천하기 위한 것임. 따라서 분쟁자체를 미연에 방지하거나 사전적 구제절차로 침해를 최소화하는데 의미가 있음(권헌영, 2004).

2) 내용별 분류

○ Weible(1993)의 연구는 개인정보를 그 내용에 따라 14개의 종류로 분류하면서 그 내역들을 비교적 상세하게 제시하였다는 점이 주목할 만함.

- 2001년 영국의 정보위원회 사무국은 정보보호법(Data Protection Act of 1998)의 실행을 위하여 발간한 개인정보안내지침서에서 개인정보를 14개의 분류항목으로 정리함(Information Commissioner's Office, 2001).

- 2004년 우리나라 정부혁신지방분권위원회는 개인정보관리현황조사를 실시하면서 조사표에 의한 분류를 시도한 바 있음. 이 위원회에서는 영국 정보위원회의 분류체계를 대체로 따르면서도 우리나라 실정에 맞게 분류체계를 보다 포괄적으로 묶고자 한 것이 특징임(권헌영, 2004).

<표 3-1> Weible의 개인정보 분류표

분 류	개인정보의 종류
일반정보	이름, 주민등록번호, 운전면허번호, 주소, 전화번호, 출생지, 본적지, 성별, 국적 등
가족정보	부모의 성명 및 직업, 배우자의 성명 및 직업, 부양가족의 성명, 가족구성원의 출생지 및 생년월일, 가족구성원의 주민등록번호 등
교육 및 훈련정보	학생기록부, 학력, 학교성적, 기술자격증, 전문면허증, 서클활동, 상벌사항, 성격 및 행태보고 등
병역정보	군번, 계급, 제대유형, 주특기, 근무부대 등
부동산정보	소유주택, 소유토지, 소유상점 및 건물 등
동산정보	자동차, 보유현금, 저축현황, 현금카드, 주식, 채권, 유가증권, 수집품, 고가의 예술품, 보석 등
소득정보	연봉, 이자소득, 임대소득, 기타 소득의 원천 등
기타 수익정보	보험가입현황, 보험 수익자, 회사의 판공비, 투자프로그램, 퇴직 프로그램, 휴가, 병가 등
신용정보	대출상황, 저당권설정여부, 신용카드 연체 및 미납의 수담보설정여부 등
고용정보	고용형태, 고용주, 회사주소, 상사의 성명, 직무수행 평가기록, 훈련기록, 상벌기록 등
법적정보	전과기록, 교통위반기록, 파산 미 담보기록, 구속기록, 이혼기록, 납세기록 등
의료정보	본인 및 가족병력, 과거의 의료기록, 정신질환기록, 신체장애, 혈액형 등
조직정보	노조가입, 종교단체 가입, 정당가입, 클럽회원 등
습관 및 취미정보	흡연량, 음주량, 취미의 종류, 여가활동, 도박성향, 비디오 대여기록 등

출처 : 권헌영, “전자정부시대 개인정보보호법제의 쟁점”, 정보화정책 제11권 제3호, 2004

<표 3-2> 영국 정보위원회의 개인정보 분류표

분 류	예 시
개인속성	성명, 주소, 연락처, 연령, 성별, 생일, 신체적 특징, 공공개인식별번호(주민번호 등) 등
가족, 사회 환경	혼인관계, 동거관계, 이혼경력, 가족속성, 세대원 정보, 취미, 주거환경, 여행 및 레저활동, 사회단체 봉사 및 기부활동 등
교육・훈련	학력, 자격, 기능, 직업훈련 기록, 전문성강화 실습기록, 학생기록부 등
고용 및 근로	경력 및 이력, 취업상세정보, 근태기록, 보건기록, 근무평정기록, 직장내 훈련기록, 사회보장기록 등
금융 및 신용	소득 및 수입, 자산 및 투자평가정보, 지출정보, 신용평가기록, 부채, 수익, 보험 상세정보, 연금정보 등
계약활동 등	제공받는 재화 및 용역에 관한 정보, 법적 이용권 확보에 관한 정보, 계약상의 합의나 계약에 관한 정보 등
민감한 정보	인종 및 민족, 정치적 견해, 종교 및 신앙, 노조가입정보, 신체 및 정신적 건강 상태, 성생활정보, 행정처분기록, 범죄 및 수사기록

<표 3-3> 정부혁신지방분권위원회의 개인정보 분류표

분 류		예 시
속성정보		이름, 성별, 나이, 생년월일, 주민등록번호, 주소, 전화번호, 이메일주소, 혈액형, 신장, 체중, 사진, 지문, 장애, 기타 개인을 타인으로부터 식별하고 특성을 규정하는 정보
활동정보	가족, 출신 및 생활환경	결혼・이혼경력, 가족관계, 습관, 주거, 여행, 레저활동, 자선단체 가입 등
	학력 및 교육	학력, 출신학교, 성적, 학교생활, 기능, 자격 등
	고용 및 경력	취업, 사업경력, 구직・채용, 인사, 근태, 근무평정기록 등
	재산・신용・납세	수입, 임금, 투자, 지출, 채무, 보험, 재산, 연금, 보조금, 납세사실 등
	사회보장 및 행정서비스	정부로부터의 급부, 급여, 면허・특허・인가, 행정계약 등
	기타	기타 개인의 일상생활과 관련된 정보
민감한 정보		인종・민족, 국적, 정치적 성향, 종교, 노조・사회단체활동, 보건・의료, 성생활, 행정처분사실, 전과・수형기록, 병역사항, 기타 개인의 기본적 인권을 현저하게 침해할 우려가 있는 개인정보

○ 또한 개인정보는 성격에 따라 민감한 정보와 그렇지 않은 정보로 분류되며, 인격적 정보와 재산적 정보로 구분되기도 함(황인호, 2001).

- 대체로 인격적 정보 중에서 차별적 처우의 기준이 되는 정보는 민감도

가 높은 정보이며, 우리나라의 경우에는 출신지역, 학력 등이 이에 속함. 재산적 정보에서도 신용불량기록 등은 민감도가 높은 정보에 속함.

○ 지금까지 살펴본 개인정보의 개념정의나 분류체계는 개인정보를 명확히 구분하거나 모든 것을 포함하여 나열할 수 없다는 한계를 갖고 있음. 단지 이러한 정의나 유형화의 의미는 개인정보를 둘러싸고 일어나는 각종 사회적 갈등이나 제도에 관한 논쟁에 있어서 얼마나 사회적 합의를 쉽게 이끌어낼 수 있는가라는 측면에서 중요하다고 봄.

3. 개인정보 침해 유형

1) 일반적 침해 유형

○ 개인정보는 일반적으로 수집에서부터 저장 및 관리, 이용 및 제공, 폐기까지 일련의 과정을 거침. 개인정보는 여러 경로를 통해 수집되고 다양한 기기에 저장될 수 있으며, 이렇게 저장·관리된 개인정보는 다양한 용도로 이용됨. 이러한 과정에서 정보보호의 취약점이 나타남.

- 개인정보의 수집단계에서는 부적절한 접근과 수집 또는 모니터링이 일어날 수 있음.
- 저장과 관리단계에서는 수집된 개인정보를 불법적인 유출 위협이 있는 상태로 저장하거나, 개인정보보호정책에 명시된 저장기간 외에도 저장상태를 유지시킬 수 있음. 또한 관리자나 이용자가 제공자의 동의 없이 혹은 실수로 개인정보를 유출할 수 있는 관리적 위협이 나타날 수 있음.
- 이용 및 제공단계에서는 제공자의 동의 없는 개인정보의 분석과 수집된 개인정보의 부적절한 분석, 개인정보보호정책에 명시되지 않은 위탁사업자나 제3서비스 제공자에게 주거나 개인정보를 제3자에게 양도하는 불법적 거래 등의 위협이 우려됨.
- 폐기단계에서는 개인정보보호정책에 명시된 보유기간 이후에 개인정보

를 파기하지 않고 저장하거나, 권한관리의 오류로 권한 없는 이용자가 개인정보를 파기하는 등의 위협이 생길 수 있음.

<표 3-4> 유통단계별 개인정보 침해유형

단계	침해유형	세부내용
수집	부적절한 접근과 수집	개인정보보호정책에 명시되지 않은 개인정보 수집
		사용자 동의 없이 개인정보 수집
	부적절한 모니터링	동의 없이 개인의 인터넷 활동이나 사생활을 모니터링
저장 및 관리	부적절한 저장 (개인정보 저장)	수집된 개인정보를 불법적인 유출 위협이 있는 상태로 저장
		수집된 개인정보를 개인정보보호정책에 명시된 수집 목적 달성 시점이나 저장기간 외에도 저장 상태 유지
	부적절한 저장 (개인정보 관리)	동의 없이 개인정보 노출
		권한관리, 시스템/서비스 오류로 개인정보 노출
		관리자 또는 이용자의 실수로 개인정보 노출
이용 및 제공	부적절한 분석	동의 없는 개인정보의 분석
		수집된 개인정보의 부적절한 분석
	원하지 않은 영업행위	동의 없는 상품광고, 광고성 정보 제공
	부적절 개인정보 제공	개인정보보호정책에 명시되지 않은 위탁사업자나 제3서비스 제공자에 개인정보 제공
		개인정보보호정책에 명시된 위탁사업자가 제3서비스 제공자에게 명시되지 않은 개인정보 항목을 제공
		개인정보를 제3자에게 양도하는 등 불법적 거래
파기	부적절한 저장(보유기간 외 개인정보 저장)	개인정보보호정책에 명시된 보유기간 이후에 개인정보를 파기하지 않고 저장
	부적절한 저장(부적절한 개인정보의 파기)	파기해야 할 개인정보에 대한 비파기
		권한관리의 오류로 권한 없는 이용자가 개인정보 파기

출처 : 김성훈 외, “u-City 프라이버시 보호방안 연구”, 한국정보보호진흥원, 2006

2) 유비쿼터스 환경에서의 침해 유형

○ u-City는 기존의 컴퓨팅 환경에 비해 정보의 저장·분석량이 무수히 많아지고, 민감한 개인정보를 다루는 컴퓨터가 많아짐. u-City 내에서 유비쿼터스 IT 기술을 활용하여 개인이 원하는 서비스를 제공하기 위해서는 개인에 대한 정보가 필요하며, 이를 위해서는 개인의 인증이 필수임. 그로

인해 u-City 네트워크에서는 무수히 많은 개인정보가 떠돌게 되고, 이를 악용할 소지가 생기게 되는 것임.

○ 기존의 유통단계별 정보침해 분류에서는 u-City 서비스 환경에서 발생할 수 있는 프라이버시 침해 유형을 다음과 같이 나눔(고웅 외, 2008).

- u-City 서비스 환경에서는 정보의 수집단계에서 일반적으로 정보주체의 동의나 고지 없이 개인정보가 수집되거나, 명시의무를 지키지 않는 행위들이 정보주체가 인식할 수 없는 상황 속에서 발생할 수 있기 때문에, 개인정보에 대한 통제권 상실을 초래할 수도 있음. 또한 정보주체의 동의 없이 개인의 인터넷 활동을 클릭 스트림 조사 등의 방법으로 모니터링하거나, 개인 몰래 카메라 또는 CCTV를 이용한 행동의 감시로 인해 개인의 사적인 생활 및 취향 등의 전반적인 정보가 노출될 가능성이 있음.

- 이용 및 제공단계에서는 개인에게 고지하지 않고 사적인 정보를 분석해 차별적 서비스를 하거나, 개인의 생활에 대한 지배 및 통제를 더욱 심화시킬 수 있음. 또한 정보주체인 사용자에게 알리지 않고 그들의 정보를 다른 기업이나 제3자에게 넘겨주는 행위, 고지하거나 명시된 내용을 넘어서는 정보를 이용하거나 공급하는 행위가 유비쿼터스 사회에서는 더욱 다양해지고 빈도도 증가할 것으로 보임. 원치 않는 스팸 메일이나 문자 등의 광고성 메일 역시 유비쿼터스 사회에서는 개개인의 특성에 맞춘 무차별 유통으로 더욱 문제화될 수 있음.

- 저장이나 파기 단계에서는 기존보다 더욱 다양하게 수집된 정보의 파기가 이루어지지 않고 다양한 용도로 재활용될 가능성이 증가할 것으로 보임.

○ 물론 이러한 개인정보 침해 유형은 유비쿼터스 환경에서만 발생하는 것이 아니라 기존 컴퓨팅 환경에서도 발생할 수 있음. 유비쿼터스 컴퓨팅 환경은 기존의 오프라인 기반의 환경과 비교하여 개인정보 침해 유형 자체는

크게 달라지지 않았으나, IT기술의 발전을 통한 정보처리기술과 정보수집 기술의 발전으로 그 침해규모가 광범위해질 수 있다는 것이 문제임.

○ 유비쿼터스 컴퓨팅 사회에서는 개인정보가 단순히 개별적으로 수집되는 것에 그치지 않고, 모든 사람이 자신의 의지와 상관없이 상시적으로 네트워크에 의해 정보를 수집당하는 것을 의미하게 되는 것이므로, 오프라인이 기반일 경우 개인정보침해가 발생할 소지가 희박한 사안이라 할지라도 이것이 유비쿼터스 컴퓨팅 기술과 결합하게 되면 개인정보침해의 소지가 급격히 커질 수 있음(윤수진, 2006).

<표 3-5> u-City에서의 개인정보 침해 유형

개인정보 침해유형	현행	u-City 환경
부적절한 접근과 수집	정보주체의 동의 없이 개인정보를 수집하는 행위	정보주체가 인식할 수 없는 상황 속에서 완전한 개인정보 통제권을 상실할 가능성 존재
부적절한 모니터링	개인의 인터넷 활동을 동의 없이 조사하는 행위	개인의 사적인 생활 및 취향 등의 전반적 정보가 노출될 가능성 존재
부적절한 분석	개인의 동의 없이 사적인 정보를 분석하는 행위	사적인 정보의 분석을 통해 개인의 지배 또는 개인의 생활에 대한 통제가 심화될 가능성 존재
원하지 않은 영업행위	동의 없이 스팸메일, 문자 등의 광고성메일을 보내는 행위	개개인의 특성에 정확하게 맞춘 광고성메일의 동의 없는 무차별 유통 가능성 존재
부적절한 개인정보 제공	개인의 동의 없이 개인정보를 제3자에게 넘기는 행위	수집된 개인정보를 정보주체의 동의 없이 제3자에게 양도하는 정보의 종류 증가 및 양도 가능성 존재
부적절한 저장	필요에 의해 수집된 정보를 목적달성 후 파괴하지 않은 행위	기존보다 더욱 다양하게 수집된 정보의 파기가 이루어지지 않고 다양한 용도로 재활용될 가능성 존재

출처 : 고웅・이동범・곽진, “u-City 서비스 분류에 따른 적용사례와 보안 고려사항”, 2008; 조규백, “유비쿼터스 환경에서의 정보보호 기술동향”, 2005; 이성몽, “유비쿼터스 컴퓨팅 환경에서 개인정보보호 방법” 2005

제2절 정보보호 환경과 개인정보보호 패러다임의 변화

1. 정보화 사회의 도래

○ 우리나라는 정보통신 인프라를 기반으로 인터넷의 생활화, 디지털 경제로의 전환, 전자정부 구축 등이 가속화되고 있음. 또한 네트워크의 통합, 정보통신서비스의 융합 등을 통해 제2의 디지털 혁명이 도래하고 있음. 나아가 광대역통합망(BcN), u-센서네트워크(USN) 등의 IT 기술발전으로 주변에 산재한 컴퓨터를 자유롭게 이용하는 공간지능화(Smart Space) 환경, 이른바 유비쿼터스 환경의 구축이 이미 시작됨.

○ 개인화·지능화된 새로운 IT 서비스의 등장으로 편리한 디지털 라이프가 확산되어 개인의 삶이 편안해지고, 전자상거래의 활성화와 전자정부의 효율성이 크게 향상될 것으로 예상됨.

○ 유비쿼터스 컴퓨팅의 시대는 많은 정보기술이 서로 융합되고 컨버전스(Convergence)하게 됨.

- 유비쿼터스 컴퓨팅 환경에서는 주변에 있는 전자기기들의 정보 교환 능력이 증가할 뿐만 아니라 인간친화적인 컴퓨터 환경을 실현하기 위해 음성이나 화상, 영상을 구사한 인터페이스가 주류를 이루고 있어 네트워크를 통해 오가는 정보의 양이 비약적으로 증가할 것임.

○ 인간의 주변에 있는 모든 사물 안에 컴퓨터 기능을 탑재하거나, 인간이 휴대하고 다니는 소형단말기에 컴퓨터 기능을 부착하여 “언제, 어디서나” 삶의 모든 것을 관리하고 감독할 수 있는 시대가 도래함.

○ 이러한 정보사회의 변화에 따라 개인정보 침해위험 역시 높아질 것으로 보임.

2. 정보보호 환경의 변화

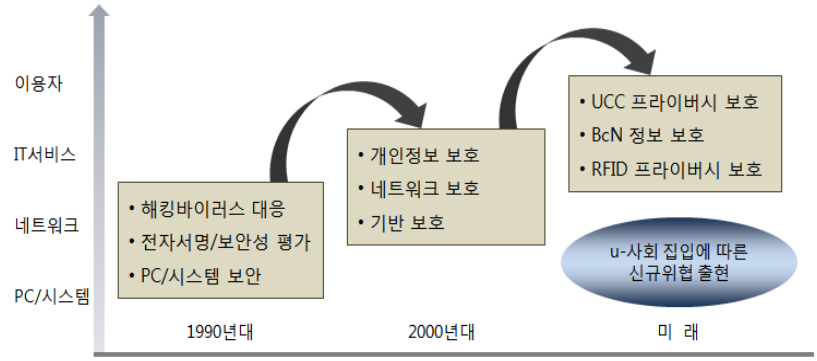
○ 새로운 유비쿼터스 기술의 등장은 유비쿼터스 IT 환경에서의 또 다른 위협을 초래함.

- Web 2.0, UCC, RFID 등이 현재 널리 이용됨에 따라 이미 이를 통한 저작권 침해나 프라이버시 침해와 같은 다양한 역기능이 발생하고 있음. 블로그와 소셜 네트워크 등에서 발생하는 개인정보 침해와 Ajax, RSS 같은 신기술의 다양한 취약점을 이용한 악성코드 유포 등이 예측 불가능한 새로운 정보 위험 요소로 자리잡게 됨.
- 복합화되고 악성화된 사이버 위협은 이메일은 물론 PC의 공유폴더, P2P, 휴대폰 등으로 전파경로가 확대되고 있음. 이기종 네트워크가 통합된 환경은 개별 네트워크에서 발생된 위협을 통신망, 방송망 및 USN으로까지 확산을 가능하게 함(황중연, 2008; 정경호 외, 2006).

○ 이러한 정보환경 속에서 정보보호는 개별 시스템, 네트워크 보호에서 벗어나 서비스와 이용자 보호로 그 중심이 급격히 옮겨져 범위가 크게 확대되고 있음.

- 기존의 정보보호가 시스템과 네트워크 보안을 중심으로 사업자 일방형이었던 데 비해, 점차 일반 이용자의 정보 단말(개별 디바이스로 확대)과 서비스 중심의 정보보호로 변화하고 있음. 즉 기존 유선망 중심의 인터넷 기반의 정보보호에서 컨버전스 네트워크상의 정보보호로 변화가 이루어지고 있음. 이에 따라 속도와 서비스의 품질이 중요시되었던 광대역 망에서 이제는 이동성과 보안, 그리고 프라이버시가 강조되는 유비쿼터스 네트워크로 진화되고 있음.

○ 즉 "u-사회에서 네트워크의 규모 및 복잡도가 환경에 따라 변화하고 이동성이 증가하면서, 'Static' 정보보호에서 주변상황을 인지하여 적합한 서비스를 제공하는 'Conformable' 정보보호로 변화"하고 있음(정경호 외, 2006).



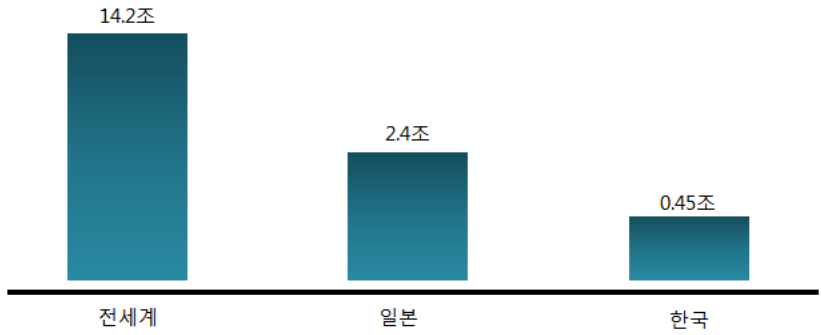
출처 : 황중연, "유비쿼터스 환경변화에 따른 정보보호의 주요 현황과 대응전략", 「정보와 통신」, 한국정보보호진흥원, 2008

<그림 3-1> 정보보호의 범위 확대

○ 개인정보 침해 사건들이 빈번하게 발생하면서 이러한 사건들은 곧바로 개인정보 피해자들의 손해배상 문제로 확대될 수 있기 때문에 경제적 손실과 사회적 영향이 매우 큼.

- 2005년 인터넷 침해사고로 인한 국내 기업의 연간 누적 피해액은 약 4,500억 원인 것으로 조사됨. 개인정보 유출 피해를 막기 위한 연간 지불의사 금액은 개인이 47,000원, 국가 전체로는 1조 3천억 원에 이름. 우리나라의 GDP 대비 인터넷 침해사고 피해액은 전 세계 평균의 1.8배로 매우 높음. 이는 일본보다는 약간 높은 수준으로 향후에는 그 규모가 더욱 확대될 것으로 우려됨.

- 2008년에는 은행전산망에 해커가 침입해 100여개의 금융기관 대출정보가 유출되는 사건이 발생함. 같은 해 온라인 상거래 사이트에서는 1800만 명의 고객정보가 유출되었고, 한 포털 사이트에서는 55만 명의 개인정보가 노출되는 사건이 발생함. 그 외 이동통신사들의 고객정보가 노출되는 등 큰 이슈들이 빈번하게 발생함[4].



출처 : 황중연, "유비쿼터스 환경변화에 따른 정보보호의 주요 현황과 대응전략", 「정보와 통신」, 한국정보보호진흥원, 2008

<그림 3-2> 인터넷 침해사고로 인한 경제적 손실규모(2005)

3. 개인정보보호의 패러다임 변화

○ 현대적 의미의 개인정보보호 문제에 대한 관심이 점차 증대됨.

- 정보통신기술의 발전과 범세계적인 서비스기반이 확대됨에 따라 디지털화된 개인정보는 가공 및 활용이 용이해졌고, 개인정보의 이동과 유통이 활발해짐. 이 과정에서 개인정보의 유출, 남용 및 이를 이용한 불법행위들이 늘어나고 있으며, 이로 인해 사생활이 침해되는 사례가 빈번하게 발생하여 사회문제로 대두됨.

○ 지식정보화 사회에서 프라이버시 침해 문제가 전통적인 의미의 프라이버시 보호에서 개인정보보호의 관점으로 옮겨지고 있음(문송철 외, 2005).

- 과거에는 프라이버시라는 용어가 주로 사용되었지만, 최근에는 프라이버시라는 용어와 개인정보라는 용어가 혼용되거나 오히려 개인정보라는 용어가 더 많이 사용되는 경향임.

---

4) 해커에 뚫린 은행전산망(보안뉴스 2008/05/15), 금융기관 대출정보 무더기 '해킹'(2008/05/27), 옥션 1800만 고객정보 대부분 유출… 정말?(2008/03/07), LG텔레콤 700만 고객정보 노출사건… 논란은 계속(2008/04/25), 하나로텔 사태로 통신사 TM영업 '비상'(아이뉴스24, 2008/04/27), 다음 '한메일' 55만명 개인정보 노출(한국경제 2008/07/22) 참조.

- 과거에는 국가권력이나 매스컴에 의한 개인의 프라이버시 침해가 주된 요소였지만, 오늘날에는 데이터베이스에 축적되어 있는 개인정보의 유출과 인터넷을 이용한 프라이버시 침해 사례가 증가하고 있음.

○ 비슷한 맥락에서 자기정보에 대한 통제권의 개념으로 '정보 프라이버시(information privacy)'라는 개념이 등장함.

- 이는 1995년 미국 행정부의 국가정보화추진위원회(Information Infrastructure Task Force, IITF)에서 제시한 개인정보보호원칙에서 처음 사용한 용어임(강장묵 외, 2006).

- 기존의 전통적인 의미의 프라이버시가 "혼자 있을 권리"에서 시작된 매우 포괄적인 개념이라면, 정보 프라이버시는 자기 자신의 재산에 대한 권리 행사의 관점에서 자신의 개인정보에 대한 배타적 통제권을 가진 권리로 발전함(서계원, 2005). 다른 사람이나 혹은 다른 기관에 제공된 자신에 관한 개인정보의 유통과 활용과정에 관여할 수 있는 권리를 포함하는 것으로 이해됨.

- 개인정보가 이를 수집하고 활용하는 기업에게 경제적인 이익을 향유하게 한다는 측면에서 개인정보에 대한 재산권적 배타적 권리를 부여하여 스스로 자신의 개인정보를 관리할 수 있도록 보호해주어야 한다는 필요성이 강조된 결과임(강장묵 외, 2006).

○ 그러나 정보 프라이버시는 주로 인터넷 공간에서 이동하는 개인정보에 대한 프라이버시 보호라는 측면에서 이해되고 있음. 디지털 시대의 개인정보보호 문제에 대한 관심이나 제도적 변화 역시 오히려 개인정보의 프라이버시 영역만을 강조하여 과거의 물리적 공간에서의 프라이버시 문제를 포함하지 못하고 있다는 한계를 가지고 있음. 이러한 한계는 유비쿼터스 환경에서 또 다른 국면을 갖게 함.

○ 유비쿼터스 사회에서는 물리공간, 가상공간, 그리고 제3의 공간이 모두 중대한 프라이버시 보호 영역이 될 것임.

- u-City가 만들어내는 제3공간, 즉 물리공간과 가상공간이 끊임없이 실시간으로 연결되는 유비쿼터스 환경은 개인 정보가 물리공간으로 침투되고 확대되는 것을 의미함. 따라서 인터넷 공간으로 대표되는 디지털 공간의 개인정보에 대한 프라이버시 보호는 유비쿼터스 환경에서 물리공간까지 연계되는 프라이버시 보호로 그 영역이 확대되어야 함.

<표 3-6> 유비쿼터스 환경에서의 정보 프라이버시 영역

분 류	세 부 내 용
물리공간에서의 정보 프라이버시	• CCTV, 생체인증기술 및 각 침해주체에서 몰래 운영할 수 있는 몰래카메라 ※ 물리공간에서 수집된 정보는 RFID 등 통신기술을 통해 실시간으로 연계된 가상공간에서 새로운 정보로 재생산됨.
유·무선 중심의 정보 프라이버시	• 유선전화기, Fax, 이동전화, 전자우편, MSN 등 ※ 유선전화기의 경우 1990년까지 프라이버시 주요이슈 및 보호영역이었음.
인터넷 중심의 정보 프라이버시	• 사생활침해, 사생활 공표, 허위공표, 성명 및 개인식별 정보의 영리적 이용 (주민등록번호, 신용카드 정보)

출처 : 강장묵·방기천, "유비쿼터스 센싱 네트워크 환경하에서 정보 프라이버시의 보호 기술과 영역에 관한 연구 : 상황인식시스템과 개인정보를 중심으로", 「디지털콘텐츠학회 논문지」 제7권 제4호, 2006.12

제3절 유비쿼터스 사회의 정보보호 의의

1. 유비쿼터스 사회 및 환경의 특징

○ 유비쿼터스 사회란 유비쿼터스 IT 기술을 기반으로 전 사회에 혁신을 가져오고 삶의 질을 향상시키는 사회로 정의할 수 있음(문송철 외, 2005).

- 유비쿼터스 컴퓨팅 환경이 구축되어 모든 사물이 지능화·네트워크화 됨으로써 개인의 삶의 질 향상, 기업의 생산성 증대, 공공 서비스의 혁신이 이루어지고 이를 통해 국가 전반의 경쟁력이 제고됨.

- 그러나 빠르게 발전하고 있는 유비쿼터스 컴퓨팅 기술은 점점 고도화, 분업화되면서 사용자의 편의성을 증대하고 있지만, 그와 관련된 역기능도 우려되고 있음.

○ 유비쿼터스 기본개념인 '어디에서나 컴퓨팅을 이용한다'는 것은 곧 어디에서든지 정보가 누출되고 왜곡될 위험이 있다는 것을 의미함(홍승필외, 2006). u-City에서는 기본적으로 프라이버시의 침해라는 중요한 문제를 내포함.

- 유비쿼터스 컴퓨팅 환경은 개인신상명세, 서비스 사용 종류, 위치정보, 생체정보를 비롯한 사용자에 대한 다양한 개인정보를 수집, 저장하며, 이를 토대로 각 사용자에게 특화된 서비스를 제공할 수 있음. 그 결과 사용자의 편리성은 증대되지만, 도처에 있는 센서들이 정보 수집 및 서비스 제공의 역할을 하기 위해서는 맞춤형 서비스 제공이나, 과금, 권한관리 등의 이유로 서비스 이용자의 인증 과정을 거쳐야 하고, 이러한 인증 과정에서 도시 내의 모든 센서들이 개인 정보에 대한 처리를 수행해야 함. 이 과정에서의 빈번한 정보교환은 자신도 모르는 사이에 정보가 노출될 위험성을 더욱 증대시킬 수 있음.

○ 기존의 정보화 환경이 드러난 컴퓨팅에 의해 한정된 공간에서 일정한 명령행위에 의해 개인 행적을 어느 정도 분산하고 디지털화하였다면, 유비쿼터스 컴퓨팅 환경은 이와 달리 숨겨진 컴퓨팅에 의해 별도의 명령행위 없이 언제 어디서나 개인의 행적을 집약적·전자적 기록으로 남기게 함. 즉 전자적인 측면에서는 일정한 목적 범위 내에서 개인을 완전히 발가벗기기 때문에 개인 프라이버시의 한계와 그 보호가 핵심과제로 대두될 만하다고 봄(정준현, 2003).

유비쿼터스 환경의 특징(Gordon A. Gow, 2005)

- 상호 연결된 장치들의 편재형 네트워크와 통신은 개인 정보의 유통량이 급증할 것이라는 점을 의미한다.
- 특정 응용 프로그램에 인지적 및 생체인식 인터페이스를 도입함에 따라 유통 중인 개인 정보의 질적 성격이 바뀔 것이다.
- 개인 맞춤형 서비스를 제공하기 위해 유비쿼터스 네트워크는 사용자들의 일상활동 중 상당부분을 추적 조회하고 수집해야 할 것이다.

2. 유비쿼터스 사회의 정보보호 역할

○ 개인정보보호는 유비쿼터스 컴퓨팅 환경에서 초기부터 핵심이슈로 인식되어 왔음. 유비쿼터스 환경이 가져다주는 편리하고 안전하며 윤택한 삶을 누릴 수 있는 이면에는 주변의 모든 사물 안에 부착된 컴퓨터 기능으로 인하여 언제 어디서나 인간의 모든 것이 관리·감독될 수 있기 때문에 개인정보 권리침해의 위험성이 상존하게 됨.

○ 자기 자신을 상호 연결된 컴퓨터들의 보이지 않는 네트워크상에 노출하는 것이 유비쿼터스 환경을 구성하는 기본 전제라고 볼 수 있음.

- 유비쿼터스 환경에서는 가정, 회사, 정부, 교통 등 모든 사물과 역무에 있어서 센싱(sensing)과 태그(Tag), 리더(Reader)가 역동적으로 상호작용하면서 정보를 수집·처리함. 사람들은 이러한 도구를 통해 연속적·입체적으로 정보를 노출시키면서 실시간 정보를 제공하게 되고, 그에 따른 맞춤형 서비스를 제공받을 수 있음.

○ 향후 유비쿼터스 사회의 본격 대두로 새로운 기술을 통한 개인정보 유출과 침해로 인한 피해 및 손실은 정보화 사회에서 한층 심화되고, 피해복구도 이전보다 더 어려울 수 있음.

- 유비쿼터스 사회의 위협은 두려움, 불안, 짜증 등 심리적 위협 및 ID 오남용, 침해사고, 사이버폭력 등 실제적 피해 모두를 포함함.

- 유비쿼터스 인프라는 정치, 경제, 교통, 의료, 개인생활 등 국가 사회의 모든 영역과 밀접하게 관련되어 있으므로, 위협으로 인한 피해가 한층 높아질 것임.

○ 개인정보의 부적절한 사용으로 인한 개인 정보 침해 문제는 유비쿼터스 컴퓨팅이 가져다줄 긍정적인 효과를 반감시키는데 결정적인 요인이 될 수 있음. 명확히 기술된 프라이버시 보호정책과 체제가 확실한 검증장치가 함께 마련되지 않는다면, 이용자들은 자신들에 관한 정보보호 인프라를 마음놓고 신뢰할 수 없게 되고, 그로 인해 해당 시스템들의 수용성 및 유용성이 손상되는 결과가 초래될 수 있음.

- 즉 사용자들에게 유비쿼터스 네트워크를 사용하라고 설득하려면 그들이 자신들의 개인정보가 항상 보호를 받고 있다고 믿을 만한 이유를 제공해야 함. 따라서 유비쿼터스 환경의 안전성과 신뢰성을 보장할 수 있는 사회적 여건이 마련되어야 할 것임.

○ 이러한 사실은 개인의 프라이버시, 정보보호관련 법과 기술, 이해당사자들의 상호연관에 관하여 매우 중요한 시사점을 던져주고 있음(홍준현, 2004). 즉 정보보호의 법적규제와 규제수준이 정보보호기술의 발전에 영향을 미치고, 정보보호기술의 발전과 기술채택의 확산은 다시 정보시스템의 성능, 안전성, 수용성을 향상시키고 이해관계인들의 저항 등 갈등비용을 감소시킴으로써 정보화의 전체적 효율성 확보에 기여함. 반면 이해당사자들의 프라이버시 또는 개인정보 보호에 대한 요구가 정보보호관련 기술수준과 더불어 정보보호의 법적 규제와 규제수준에 결정적 영향을 미치게 됨.

유비쿼터스 사회에서의 정보보호의 역할(정경호 외, 2006)

• 역기능 방지 : 유비쿼터스 사회에서 예상되는 새로운 유형의 해킹, 바이러스, 사이버 범죄 등 사이버 위협에 대한 사전 예측 및 방지
  - IPTV, VoIP 등 인터넷 기반의 신규 IT 융복합 서비스에서 유·무선 인터넷을 이용한 사이버공격으로 인한 서비스 장애 예방
  - 첨단기술을 악용한 새로운 사이버 범죄와 생활 속으로 침투하는 불건전 정보 등 인간의 삶을 위협하는 역기능 방지
  - 위치정보, 의료정보보호 등 정보보호 법제도(원격진료 등) 등 유비쿼터스 사회의 역기능 방지를 위한 사회적·제도적 기반 제공

• 신뢰성 향상 : u서비스 및 거래정보에 대한 이용자의 신뢰도를 향상시켜 신규 IT 서비스에 대한 수용성 및 활용도를 높이는 핵심적인 역할을 수행
  - 정보화 추진의 역기능을 해소하는 부수적인 역할 수행에서 벗어나 신규 IT 서비스에 대한 불안을 해소하여 새로운 IT시장 창출 및 진흥에 기여
  - u-IT 기반 감시수단 다양화, 보편화에 따른 감시사회에 대한 국민의 불안감 해소

제4장 정보보호 현황 및 문제점

제1절 기술적 영역 : 유비쿼터스 컴퓨팅 환경의 정보보호 기술

제2절 규제적 영역 : 유비쿼터스 정보보호의 법적 현황

제3절 사회적 영역 : 시민들의 인식과 공공영역의 요구

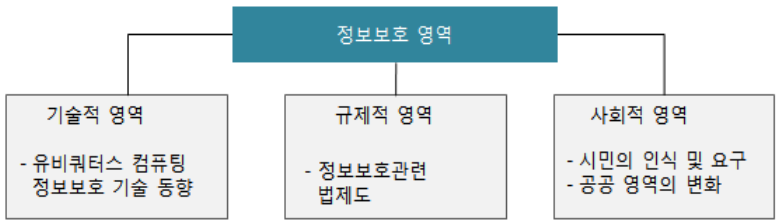
제4장 정보보호 현황 및 문제점

○ 지금까지 개인의 프라이버시 보호 문제는 주로 개인의 기본적 권리에 관한 것으로 법에 명문화되어 있었으며, 정보사회 이전까지는 개인의 사생활에 관한 법률적 보장이 주를 이룸. 그러나 정보사회가 심화되면서 정보기술사회에서의 프라이버시 보호는 다양한 관점에서 새로운 방식으로 부각되고 있음.

○ Gordon A. Gow(2005)는 개인정보 보호 문제를 3가지 영역으로 나누어 접근함.

- 기술적 영역에서 개인정보 보호는 네트워크 보안이나 사용자 인터페이스 설계 등의 기술 환경과 관련한 이슈임. 정보보안 기술이 어떻게 사회적으로 구성되거나 적용되는지 하는 관점에서 접근할 수 있음.
- 규제적 영역에서 개인정보 보호는 데이터 보호에 대한 법규정과 관련한 이슈임.
- 사회적 영역에서 개인정보 보호는 문화적 관행, 윤리, 제도 등과 관련된 사회적 이슈임. 정보보호에 대한 인식의 문제와 더불어 오늘날 공공영역에서 구현되고 있는 정책적 모습에서 접근할 수 있음.

○ 이 연구는 유비쿼터스 환경에서의 개인정보보호를 다루는 데 있어서 이와 같은 3개 영역을 통해 현황과 문제점을 살펴보고자 함.



<그림 4-1> 정보보호 문제의 세 가지 접근영역

제1절 기술적 영역 : 유비쿼터스 컴퓨팅 환경의 정보보호 기술

1. u-City 서비스 구현과 정보침해

1) u-City 서비스

○ 현재 u-City의 건설은 중앙정부와 지방자치단체 주도로 전국에 걸쳐 활발히 이루어지고 있음. 전국 각 지방자치단체에서 u-City건설을 목표로 하고 있으며, 서울 상암, 서울 강남, 부산 송도, 대전, 광주, 대구, 제주 등에서 그 구현이 추진되고 있음[5].

출처 : 정보통신부, 2006

<그림 4-2> u-City 개념도

5) 정보통신부 미래정보전략본부 미래전략기획팀, 'U-Korea 기본계획' 참조, 2006. 9

○ u-City의 구현을 위해서는 필수적으로 도시 거주민과 도시네트워크의 상시 접속성이 이루어져야 함.

- 이를 위해 각종 무선단말기를 이용한 위치정보확인기술, RFID를 통한 전파식별기술, 데이터의 처리와 관리를 위한 통합관제기술 등 유비쿼터스 컴퓨팅과 관련한 첨단 정보통신기술이 u-City의 건설에 사용되고 있음. 각종 상품이나 서비스에는 고유식별장치가 붙어 그 이동이 추적되며, 개인의 이동정보, 의료정보, 교육정보, 자동차의 운행정보 등이 수집되어 관리됨.

- u-City 건설의 핵심기능인 통합관제센터는 위에서 언급한 각종 장치 등을 통해 수집된 데이터를 처리하고 관리하여 새로운 유비쿼터스 도시의 필수기반시설로 자리잡게 될 전망임.

○ u-City 서비스란 'u-City 추진목적에 따라 유비쿼터스 기술(상황인지/정보처리) 및 정보통신 인프라(센싱/태그)를 활용하여 도시 구성요소(도시 인프라, 사람, 자연환경)의 관리 및 효용성을 극대화하기 위한 통합 및 지능화된 정보/콘텐츠의 집합'임.

○ u-City 서비스는 유·무선 서비스(예 : xDSL, FTTH, RFID, 와이브로, 이동통신, HSDPA 등)의 통신 인프라와 첨단 인텔리전트 빌딩과 지능형 도로 등의 도시 인프라, 홈 네트워킹, 건물관리 시스템 등의 솔루션, e-Learning, IP-미디어 등의 콘텐츠가 결합되어 구현됨.

○ u-City가 제공하는 서비스는 그 적용범위에 따라 크게 u-Home, u-Work, u-Traffic, u-Health, u-Environment, u-Public service, u-Education으로 구분할 수 있음.

<표 4-1> u-City 서비스 유형

구 분	주요내용
u-Home	• 원격검침, 원격제어, 원격수리, 출입문제어, 홈네트워킹, IP-미디어
u-Work	• 재택근무, 원격회의, 무선상거래
u-Traffic	• 교통상황, 교통사고처리, 도로통합관리, 텔레매틱스
u-Health	• 헬스케어 서비스, 원격검진, 원격의료/치료, 응급조치
u-Environment	• 환경관리, 위생관리
u-Public	• 전자정부, 방범, 재난관리
u-Education	• E-Learning, 학교관리 시스템, 학원 등 • 하교 관리 시스템

출처 : 전호인, "u-City 공공/민간 서비스 구현을 위한 핵심기술", TTA 저널 112호, 한국정보통신기술협회, 2007.7

○ u-City 서비스유형은 크게 공공서비스와 민간서비스로 구분함.

- 공공서비스는 u-Public service, u-Environment Management, u-Traffic 등으로, u-Environment, u-Public service, 통합운영센터의 도움 없이는 구현될 수 없는 서비스들임.
- 민간서비스로 가장 각광을 받을 것으로 기대되는 u-Healthcare, u-Home, u-Work, u-Education 서비스는 u-City 통합운영센터의 지원 없이 자체적으로 서비스가 가능하지만 u-City통합운영센터와 연계될 때 제대로 시너지 효과를 얻을 수 있음(전호인, 2007).

2) 유비쿼터스 기술의 정보침해 가능성

○ 유비쿼터스 기술은 다음과 같은 특성을 지니기 때문에 기본적으로 프라이버시를 침해할 가능성이 높음(임영덕, 2005).

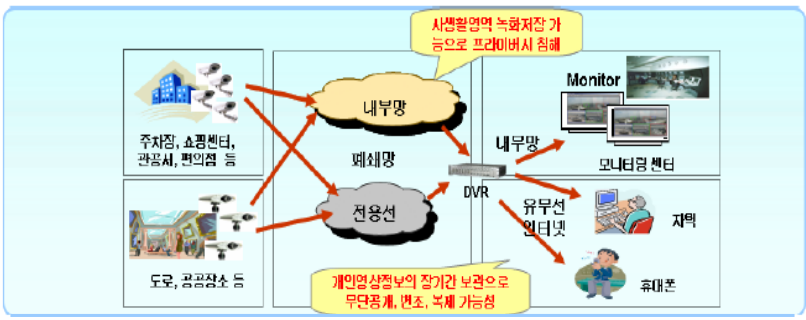
- 유비쿼터스 기술은 사물 속에 존재하기 때문에 정보주체가 인식하지 못하는 사이에 개인의 신상정보를 저장, 축적하거나 노출시킬 수 있는 은밀성과 용이성을 지니고 있음.

- 기술 발달에 의해 정보는 더욱 더 광범위하게 수집되고, 매우 신속하게 유통되며 무한정 복제될 수 있음. 이는 프라이버시 침해가 발생하면 구제는 사실상 불가능함을 의미함.

- 유비쿼터스 환경에서는 개별적으로 수집된 개인정보가 다른 방식으로 처리된 정보와 결합하여 한 개인에 대한 전반적인 정보를 파악할 수 있게 됨. 즉 수집된 개인정보의 확대 및 재생산이 용이함.

○ 이러한 기술적 특성을 기반으로 개인정보가 유출될 수 있는 공간과 그 가능성은 비일비재함.

- 범죄예방을 목적으로 공공장소로 확대 설치된 CCTV[6]는 기존의 단순 모니터링에서 녹화, 저장, 전송이 가능하게 되어 프라이버시 침해 가능성을 증대시킴. 가령 CCTV를 이용하여 실시간으로 사생활 영역에 대한 녹화 및 저장이 가능하고, 장기간 저장된 개인정보의 무단공개, 변조, 복제 등이 가능함. 온라인 거래나 무인 출입관리 시 본인 확인수단으로 부각되고 있는 바이오 인증도 개인의 신원을 추적 및 유추할 수 있으므로 프라이버시가 침해될 수 있음(정경호 외, 2006).



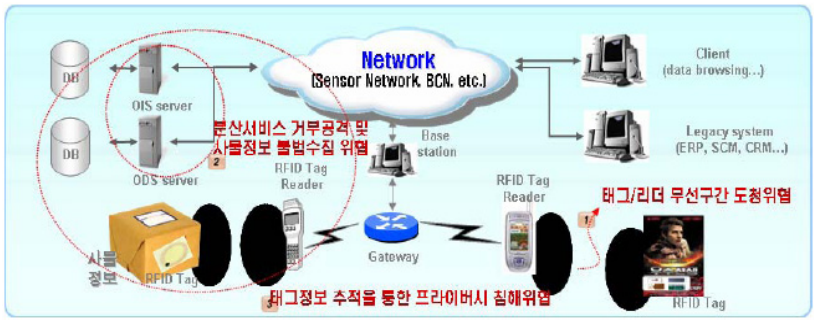
출처 : 정경호 외, 『유비쿼터스 정보보호 기본전략 연구』, 한국정보보호진흥원, 2006

<그림 4-3> CCTV 관련 프라이버시 침해 위협

6) CCTV는 국내 약 200만대가 설치되어 있으며, 개인정보에 관한 구체적인 조례나 지침 없이 녹화된 자료가 30~60일간 보관됨(정경호 외, 2006).

○ 다양한 u-서비스를 제공하기 위해 설치된 RFID[7] 태그 시스템은 오히려 정보 추적을 통한 프라이버시 침해 위협을 발생시킬 수 있음.

- RFID 태그를 이용하여 이용자의 행동 및 신원 관련 정보의 다량 수집 및 네트워크를 통한 유통이 가능하다는 이점은 오히려 RFID 태그와 RFID 리더와의 무선통신에서 보안성이 높지 않은 경우에 도청을 통해 개인정보가 유출될 수 있고, RFID 태그로 수집된 정보를 이용해 개인의 신원을 추적하거나 개인의 행동유형을 분석할 수 있음.



출처 : 정경호 외, 『유비쿼터스 정보보호 기본전략 연구』, 한국정보보호진흥원, 2006

<그림 4-4> RFID 관련 프라이버시 위협요소

○ CCTV, 카메라폰, RFID 등 원격 및 실시간 감시 도구들이 점차 지능화되고 네트워크로 연결됨에 따라 수집된 정보를 서로 교환할 수 있음. 이로 인해 감시수단의 소형화, 편재화가 진행되어 과거의 은밀한 감시 형태에

7) 유비쿼터스 환경에서 근거리 무선기술을 이용하여 사물(Objects)을 원격으로 인식하여 정보교환을 가능하게 하는 기술임. 수동 스마트카드(Smart Tag), 전자제품코드(Electronic Product Code : EPC), 객체이름서비스(Object Name Service : ONS), PML(Physical Markup Language) 등의 기술들을 이용하여 제품이나 물건 등에 전 세계적으로 통용되는 고유식별부호(ID)를 붙이고 필요에 따라 무선신호로 읽을 수 있게 함으로써 제품의 종류, 제조일자, 시간적 유통경로 및 관련소유자에 관한 데이터 등과 같은 식별된 물건에 대한 정보를 읽거나 저장할 수 있도록 해주며, 식료품부터 축산물관리, 폐기물관리, 환경관리, 물류·유통, 보안 등 우리 생활의 다양한 분야에 적용될 것으로 예상되고 있음. RFID는 이미 20여 년 전부터 사용되어 왔지만, 비용과 기술 등의 문제로 확산되지 못하다가 최근 관련 기술의 발달로 보편적 상용화 단계에 접어들고 있음.

서 좀더 공개적이고 실시간적인 감시 형태로 진화되고 있음.

- 기존의 감시문제가 국가에 의한 감시에 초점을 맞추었던 반면, u-사회에서는 점차적으로 개인 상호 간의 감시가 증가하고 네트워크 안에 공존하는 누구라도 감시자가 될 수 있음.

2. 유비쿼터스 환경의 정보보호 기술 동향

1) 정보보호 기술 동향

○ 유비쿼터스 컴퓨팅 환경은 정보보호에 취약하고, 사용자 정보에의 접근이 용이한 문제 등 역기능이 적지 않음. 이는 '유비쿼터스 기술이 제공하는 편리성에 도취되어 정보보호 문제의 심각성이 제대로 인식되지 못하고 있다'는 우려를 경청해야 하는 이유임(임종인, 2003).

○ 그러나 기술은 반드시 프라이버시에 대한 위협만은 아니며 그 보호수단을 제공하는 경우도 많음(Daniel J. Solove 외, 2003).

- 암호화(Encryption), 익명화 기술(Anonymizing Technologies)은 웹사이트 방문자의 추적을 봉쇄함으로써 그 프라이버시를 보호해줄 수 있음.

○ 정보보호 기술은 정보통신망의 마비, 개인정보 유출, 불건전 정보의 유통 등 정보통신 환경을 저해하는 위협과 부작용에 대응할 수 있도록 정보통신 시스템 및 데이터의 기밀성(정보유출 방지), 무결성(데이터 위조 및 변조 방지)을 유지하고 시스템의 가용성을 보장 및 활성화하기 위한 기술을 말함(홍도원, 2006).

- 이 기술은 핵심 및 기반이 되는 정보보호기반기술, 정보통신시스템 및 네트워크 보안성을 확보하기 위한 정보통신 인프라 보호기술, 정보통신 시스템을 활용하여 서비스에 정보보호를 적용하는 디바이스 및 서비스 보호기술로 분류함[8].

- 또한 이 기술은 IT 환경 변화에 따라 사용자 측면에서 개인정보 및 프

라이버시 제공기술, 서비스 및 디바이스 측면에서 안전한 신뢰서비스 제공기술, 인프라 환경 측면에서 끊김없고 이동성이 지원되는 안전한 인프라 제공 기술을 의미함.

<표 4-2> 정보보호기술의 분류

분류	기술분야	기술내용
정보보호 기반기술	암호기술	• 기밀성 유지, 전자서명 등에 사용되는 대칭키와 공개키에 대한 알고리즘, 서명 알고리즘에 대한 설계·분석과 암호모듈의 하드웨어적인 고속 구현 기술 • 부인방지, 동시성(전자계약 등), 익명성, 콘텐츠 보호 등에 사용되는 프로토콜 구현 기술 • 암호키의 분배, 전송, 동의, 복구를 위해 사용되는 키의 관리
	인증기술	• 인증서 전달을 위한 CA, RA, 인증서 관리기술 등 공개키 기반 구조(PKI) 구축에 사용되는 기술 • 다양한 전자거래에서 ID 서비스를 위한 단일 ID관리/분산인가/ID중개/위임 기능을 제공하는 Identity 보호용 기술 • 사용자 신분 확인을 위한 바이오인식, 다중인식 등의 기술 －유비쿼터스 환경에서 개인인증이 가능한 실시간 다중 바이오 인식 알고리즘, 칩셋 및 응용기술
	개인정보보호 기술	• PET(Privacy Enhancing Technology) • 자기정보 통제권, 익명화 에이전트 등의 기술 • 개인정보의 이용범위에 따라 해당되는 정보 외에 다른 정보를 읽거나 해독할 수 없게 하는 개인정보의 안전한 분산 저장 및 추출 기술
정보통신 인프라 보호기술	BcN 보호기술	• BcN 환경에서 네트워크 위협을 능동적으로 탐지/분석/차단하여 고속 침입방지 기능을 수행할 수 있는 네트워크 종합 위협 대응 기술 • BcN 통합 정보보호시스템 구축 • 알려지지 않은 공격으로부터 네트워크 인프라를 보호하기 위해 공격 패킷들만이 가지는 signature를 생성하여 대응할 수 있는 실시간 공격 signature 생성 및 관리기술 • 유·무선 IPv6 환경에서 발생되는 새로운 보안 취약성에 대응하기 위한 정보보호기술 및 멀티캐스트 보안기술

8) 정보보호기반기술은 안전한 정보통신 환경을 구축하기 위해 필수적으로 요구되는 기술로 차세대 IT 및 BT 환경에 적용 가능한 원천기술이며, 정보보호제품 전반에 적용되는 암호기술, 인증기술 및 개인정보보호기술 등을 포함함. 정보통신 인프라 보호기술은 유비쿼터스 환경을 지원하는 핵심 인프라인 BcN, IPv6, USN(Ubiquitous Sensor network) 네트워크의 안전성, 신뢰성을 보장하는 인프라 보호기술로 BcN, IPv6, USN 등 시스템 구성요소 부분과 정보통신 시스템을 구성하는 서버, 네트워크에 대한 보호기술을 포함함. IT 디바이스 및 서비스 보호기술은 다양한 서비스의 연동 및 융복합화의 진행이 본격화되는 유비쿼터스 환경에서 IT디바이스 및 서비스 안전성을 제공하기 위한 기술로 전자상거래 보호, 시스템 및 PC 등 유·무선 단말시스템에서의 IT서비스보호, 유해정보 차단 및 콘텐츠 보호기술 등을 포함함(홍도원, 2006).

<표 계속> 정보보호기술의 분류

분류	기술분야	기술내용
정보통신 인프라 보호기술	RFID/USN 보호기술	• RFID/USN 환경에서 개인 프라이버시를 적극적으로 보호하고, 사물의 자동식별・이력추적 등 RFID/USN 서비스를 안전하게 제공하기 위한 보안기술 • RFID 네트워크용 ODS 위・변조 방지기술 • 초경량 보안칩, 센서노드 기술
디바이스 및 서비스 보호기술	IT 서비스 보호기술	• 전자지불, 전자화폐, 전자입찰, 전자공증, 콘텐츠 보호 등 전자상거래의 안전・신뢰성 확보기술 • 행정, 보건, 교육, 금융 등 각종 서비스에 대한 보안 • 서버 보안기술, 해킹 및 바이러스 방지기술 • XML기반 전자거래 보호기술 • 웹서비스 해킹 방지기술 • IPv6 기반 환경에서 VoIP(Voice over Internet Protocol) 불법 스팸메일 예방, 피해 최소화를 위한 능동형 대응기술 및 VoIP 사용자 프라이버시 보호를 위한 사용자 위치정보 보호기술
	유해정보차단 및 콘텐츠 보호관리 기술	• 스팸메일에 대한 제도, 기술적 정책 • 콘텐츠 유해 정도별 관리기술 • DRM(Digital Right Management) 기술 • CAS(Condition Access System) 기술
	홈네트워크 보안	• 신뢰성 있는 홈네트워크 인프라 구축을 위해 유효한 사용자를 구별하여 서비스 로봇, 차세대 PC 등 다양한 정보기기 간 안전한 통신 및 제어기술
	모바일 단말용 공통보안 플랫폼	• 모듈(STPM, Secure & Trusted Platform Module) 장착을 통한 공동보안 및 신뢰서비스 제공기술

출처 : 홍도원, “정보보호기술의 현재와 미래”, 『지역정보화』, 2006.9

<표 4-3> 정보보호 기술개발 전망

구 분	정보보호 위협	관련 기술 개발
User 측면	개인정보 유출 및 금전적 피해 발생	u-개인정보보호
	ID 위장 및 도용을 통한 ID 인증 체계 위협(리니지 등)	u-Universal 인증
Service & Device 측면	전자문서 위・변조, 디지털 콘텐츠 불법 유통 등	u-지식 및 지적재산권 보호
	개방형 플랫폼으로 인해 서비스 간 침해 전파/확산	u-침해확산 방지
Infra 측면	네트워크 인프라에 대한 위협 및 소프트인프라웨어의 보안 취약성	u-IT 인프라 보호
	상이한 무선망 간 접속/이동 보안 호환성 부재	u-무선 보안

출처 : 홍도원, “정보보호기술의 현재와 미래”, 『지역정보화』, 2006.9 재구성

○ 현재까지의 정보보호기술을 살펴보면, 1990년때 중반까지는 PSTN & Narrowband 네트워크를 중심으로 Bandwidth & Speed가 중요하였으며, 2000년대 중반까지는 브로드밴드 네트워크를 기반으로 QoS가 중요시되는 환경에서 시스템 및 네트워크 중심의 개별보안 및 통합보안에 중점을 둠.

○ 향후 정보보호기술은 유비쿼터스 네트워크를 기반으로 'Mobility', 'Security', 'Privacy'가 중심이 되는 u-사회가 될 것임. 따라서 u-사회에서는 개인정보 보호, 지식 및 지적재산권 보호, 침해확산 및 사이버 범죄 방지, 끊김없는 서비스 간 상호인증 등 사용자 중심의 정보보호 정책 및 기술이 전개될 것으로 전망됨.

3. 기술적 영역의 문제점

○ 유비쿼터스 기술은 정보주체가 인식하지 못하는 사이에 개인정보를 저장·축적하고, 이렇게 축적된 정보는 노출 및 확대와 재생산이 용이하다는 특성을 지님. 이와 같은 유비쿼터스 기술의 특성은 유비쿼터스 사회의 프라이버시 문제의 한 축을 형성함.

○ 정보기술 발전에 따른 인프라 위협의 고도화·글로벌화는 사이버위협의 고도화 및 신종 사이버위협의 출현을 가져옴. 휴대폰 바이러스와 같이 IT 기술 발전에 따른 신종 사이버 위협의 출현 및 공격의 위험수준이 높아지고 있음.

○ 네트워크 인프라 통합 역시 대량의 정보를 유통시킴으로써 프라이버시 침해 위협을 증대시킴. 특히 u-센서 네트워크의 구축으로 주변 환경에 설치된 센서를 이용해 사람과 사물의 위치정보 및 이용정보의 유통이 증가하게 되면, USN 대상의 공격을 통한 정보 유출은 사회 전반에 연쇄적 위험을 초래할 것임.

○ 현재의 전자서명 인증체계에서는 개인·법인에 대한 신원을 확인하는 인

증서비스만을 제공하고 있음. 즉, 유비쿼터스 환경에서 새로운 전자거래 주체들이 등장하면서 사람, 사물 등 모든 주체와 객체 간 신뢰할 수 있는 인증체계가 미흡함. 따라서 u-City에 적용되는 모든 주체와 객체에 적용할 수 있는 통합 인증체계가 필요함. 국내에서 실명확인 수단으로 사용되는 주민등록번호도 온·오프라인을 통해 유출되어, 이를 이용한 명의도용 사고가 빈번하게 발생하고 있음.

○ 마지막으로 CCTV, RFID 등 개인정보 유출 공간의 다변화로 프라이버시 침해 위협이 증가하고 있음. 이에 따라 서비스마다 각기 다른 개인 프라이버시 정보의 접근에 대해 적응적이고 동적으로 정보 이용 범위를 제공하는 지능형 개인정보보호 에이전트와 접근제어 기술[9](송유진 외, 2006) 등 정보보호 핵심응용기술의 개발이 시급함.

○ 정부차원에서는 정보보호 기술 개발에 대한 예산지원의 불충분, 정보보호에 대한 축적된 기술력의 부족, 관련 지적재산권의 확보와 같은 기술지원적 기반의 취약 등이 한계로 나타나고 있음(서동일, 2005).

제2절 규제적 영역 : 유비쿼터스 정보보호의 법적 현황

1. 개인정보보호와 관련한 현행법제도

1) 개인정보보호와 관련된 현행법제도 및 문제점

○ 우리나라는 개인정보보호와 관련하여 종합적인 일반법을 두지 않고 분야별 입법으로 대처하면서, 공공부문과 민간부문으로 나누어 각기 그 법적

9) 개인정보의 접근/사용 시 상황정보를 토대로 User Preference의 동적인 적용과 개인정보 특성에 따른 정보공개의 판정 메커니즘 제공, 클라이언트-서버 통합 지능형 에이전트 기반 프라이버시 보호 기술 개발, 프라이버시 정책에 의한 접근 판단 및 동적 상황에 근거한 접근제한, 개인 신상정보와 분리된 상황인식 데이터 관리를 통한 적응적 개인정보 이용 등의 대책에 대한 논의가 진행 중임.

근거 및 추진체계를 달리하여 보장하고 있음. 이러한 이원적 법체계에 따라 공공부문과 민간부문에 각각 적용되는 기본적인 법률이 다르게 제정됨.

- 공공부문의 경우 공공기관이 보유한 개인정보보호에 대한 일반법의 성격을 가진 「공공기관의개인정보보호에관한법률」이 일반법으로 개인정보를 보호하고 있음. 그 밖에 「전자정부구현을위한행정업무등의전자화촉진에관한법률」 및 「주민등록법」 등의 개별법에 개인정보보호에 관한 규정을 둠.
- 민간부문의 경우 「정보통신망이용촉진및정보보호등에관한법률」이 일반법의 기능을 담당함. 신용정보의 경우 「신용정보의이용및보호에관한법률」이 기본법의 기능을 담당하고 있으며 「통신비밀보호법」, 「정보통신기반보호법」, 「금융실명거래및비밀보장에관한법률」 등의 개별법에서 개인정보보호에 관한 사항을 개별적으로 규정함.

<표 4-4> 개인정보보호 관련 현행법제도 현황

적용분야		법률명	비고
공공부문		공공기관의개인정보보호에관한법률	일반법
민간부문	온라인사업자	정보통신망이용촉진및정보보호등에관한법률	일반법
	신용정보	신용정보의이용및보호에관한법률	
기타 개별법	공공부문	국가공무원법, 주민등록법, 통계법, 통신비밀보호법, 독점규제및공정거래에관한법률	
	민간부문	전기통신사업법, 전자서명법, 전자거래기본법, 국민건강보험법, 의료법, 응급의료에관한법률, 의료기사등에관한법률, 후천성면역결핍증예방법, 전염병예방법, 금융실명거래및비밀보장에관한법률, 증권거래법, 공증인법, 법무사법, 변호사법	

(1) 공공부문 개인정보보호 체계

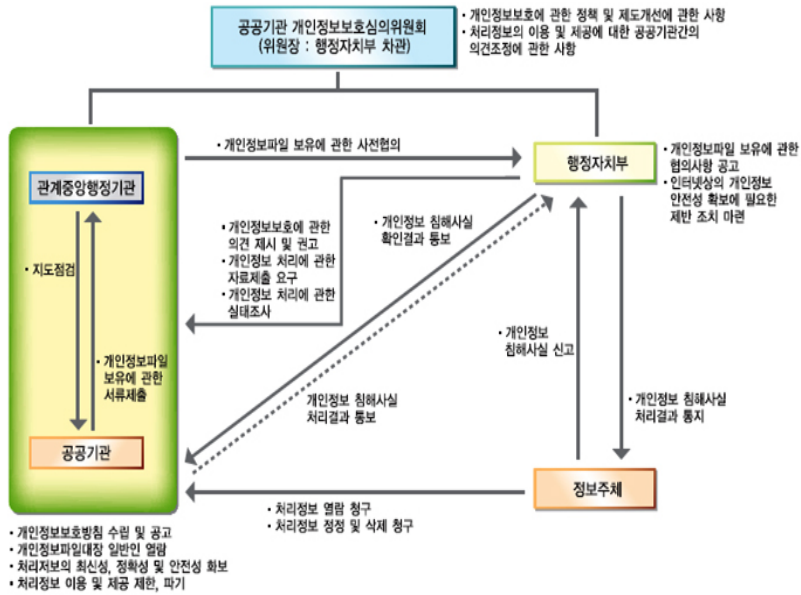
○ 공공기관에서 수집 · 처리되는 개인정보를 보호하기 위해 「공공기관의개인정보에관한법률」에 공공부문의 개인정보보호 체계를 규정함.

○ 국무총리 소속하에 설치된 '공공기관 개인정보보호심의위원회'는 개인정보

보호에 관한 정책 및 제도개선과 처리정보의 이용 및 제공에 대한 공공기관 간의 의견조정 등 공공기관의 개인정보보호에 관한 전반적인 사항을 심의함.

○ 행정안전부(구 행정자치부)는 개인정보보호에 관한 의견 제시 및 권고와 개인정보 처리에 관한 자료제출 요구 및 필요 시 개인정보 처리에 관한 실태조사 등을 수행함. 또한, 개인정보파일 보유와 관련하여 공공기관과 사전 협의한 내용을 공고하고 인터넷상에서의 개인정보보호를 위해 관련 법령 정비, 계획 수립, 시설 및 시스템 구축 등 제반 조치를 취함.

○ 공공기관은 관계 중앙행정기관을 통해 행정안전부와 사전협의한 후 개인정보파일을 보유할 수 있으며, 이럴 경우 개인정보보호 방침을 수립·공고하고 개인정보파일의 보유 목적 외의 목적으로 처리정보가 이용되거나 제공되지 않도록 제한함. 정보주체는 처리정보에 대한 열람, 정정, 삭제를 청구할 수 있으며, 개인정보에 관한 권리 또는 이익의 침해를 받은 자는



주 : 2008년 정부조직법 개정에 따라 행정자치부는 행정안전부로 변경됨.

<그림 4-5> 공공부문의 개인정보보호 체계

행정안전부에 침해사실을 신고할 수 있음. 공공기관은 침해사실에 대한 처리결과를 행정안전부를 통해 신고인에게 통지해야 함.

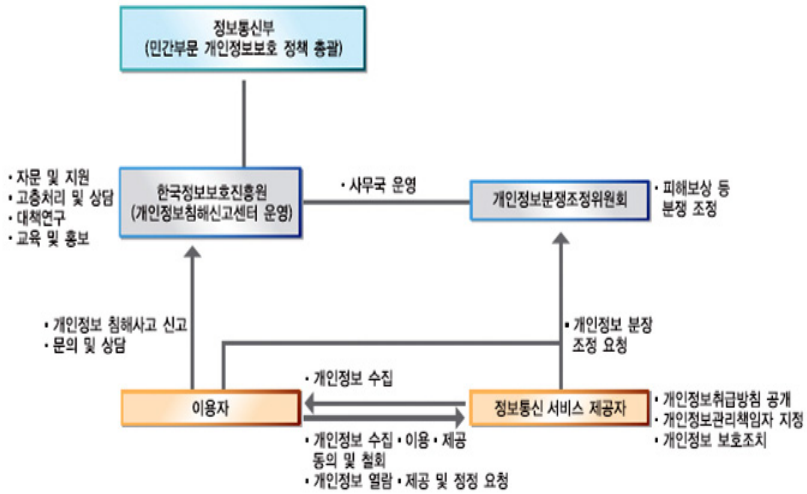
(2) 민간부문 개인정보보호 체계

○ 민간부문의 개인정보보호에 관한 일반법으로 「정보통신망이용촉진및 정보보호등에관한법률」이 있음. 또한 「신용정보의이용및보호에관한법률」, 「통신비밀보호법」, 「정보통신기반보호법」, 「금융실명거래및비밀보장에관한 법률」 등에도 개인정보보호에 관한 규정이 있음.

○ 민간부문의 개인정보보호는 방송통신위원회(구 정보통신부)에서 종합적으로 수행하고 있으나 신용정보보호 등은 기획재정부(구 재정경제부)에서 담당하고 있음.

○ 방송통신위원회 산하의 한국정보보호진흥원에 설치된 개인정보침해신고센터가 개인정보 고충처리 및 피해상담 등을 실시하고 있고 개인 정보보호에 관한 피해보상 등 분쟁조정 업무를 수행하기 위해 '개인정보분쟁 조정위원회'를 설치·운영하고 있음.

○ 정보통신 서비스 제공자는 수집한 개인정보를 이용자에게 동의 받은 목적과 다른 목적으로 이용할 수 없으며, 이용자의 개인정보를 보호하고 개인정보와 관련한 이용자의 고충을 처리하기 위해 개인정보 관리책임자를 지정하고 개인정보취급방침을 정하여 공개해야 함. 이용자는 정보통신 서비스 제공자 등에 대하여 언제든지 개인정보 수집·이용·제공 등의 동의를 철회할 수 있고 본인에 관한 개인정보, 제3자 제공내역 및 동의내역에 대한 열람 또는 제공을 요구할 수 있으며 오류가 있는 경우 정정을 요구할 수 있음.



주 : 2008년 정부조직법 개정에 따라 정보통신부는 방송위원회와 통합하여 방송통신위원회로 변경됨.

<그림 4-6> 민간부문 개인정보보호 체계

(3) 개인정보보호 관련 법률 개정 현황

○ 정부는 정보환경 변화에 능동적으로 대처하고 사업자의 개인정보보호 관리·감독 책임을 강화하기 위해 개인정보 취급·위탁 시 사업자의 관리·감독 책임강화, 이용자의 동의권·동의 철회권의 확대 등을 골자로 한 「정보통신망이용촉진및정보보호등에관한법률」을 개정함.

- 이 법률은 1999년 제정된 「정보통신망이용촉진등에관한법률」에 정보통신서비스이용자의 개인정보 보호제도에 관한 사항이 대폭 추가됨에 따라 2001년 1월 법 개정과 함께 명칭을 변경한 것임.
- 이 법률은 OECD에서 제시한 개인정보보호 8가지 원칙을 수용하고, 유럽연합의 개인정보보호지침을 고려해 국민의 프라이버시 보호를 위한 개인정보의 수집·이용·제공에 따른 제반 사항을 규정함.
- 「정보통신망이용촉진및정보보호등에관한법률」의 개인정보와 관련한 조

항은 현재까지 총 7회 제·개정됨. 그동안의 법률 개정 방향은 이용자의 권리를 보장하고 사업자의 의무부과를 강화하는 방향으로 진행됨. 가장 최근에 개정된 법령 또한 개인정보의 수집·이용·제공에 대한 고지·동의제도 및 취급위탁에 따른 사업자의 관리·감독을 강화하도록 개정됨.

○ 한편 행정안전부는 공공기관이 보유하고 있는 개인정보를 더 안전하고 체계적으로 관리하기 위해 2007년 5월「공공기관의개인정보보호에관한법률」을 개정 공표함.

- 이 법률은 개인정보의 안전하고 체계적인 관리체계 마련[10]과 개인정보 관리의 투명성 제고[11], 정보주체의 자기정보통제권 강화[12]등을 골자로 하고 있음.

(4) 개인정보보호 관련 법률의 특성과 문제점

○ 이와 같이 살펴본 현행 개인정보보호 법제도는 공·사 구분의 이원적 규율체계로 이루어져 있고, 개별법주의적 특성을 지님.

- 우리나라 개인정보보호 법률체계는 공·사 부문에 적용되는 법률이 각각 규율된 이원적 시스템으로 이루어짐. 또한 각 부문을 규율하는 기본법에 원칙이 규정되고, 개별법에 특수한 부분이 규율되는 시스템이 아

10) 개인정보파일의 '사전통보제'를 '사전협의제'로 변경하여 개인정보의 보유요건을 보다 엄격히 하였고, 보유목적의 달성 등으로 인해 불필요하게 된 경우에는 이를 지체 없이 파기하도록 함. 또한, 기관별로 개인정보관리책임관을 지정하여 개인정보보호 관련 계획의 수립, 실태조사 및 감독, 민원의 처리 등 그 기관의 개인정보의 보호 및 관리에 관한 사무를 총괄하고 책임지도록 함.

11) 개인정보의 수집, 위탁 관리, 목적외 이용 및 제공, 폐기 등 모든 처리과정에 걸쳐 관련 사실을 투명하게 인터넷을 통해 공시하도록 함.

12) 현행 정보주체의 본인정보의 열람·정정청구권 외에 삭제청구권을 신설하여 본인이 원치 않을 경우 본인의 정보에 대해 삭제할 수 있도록 하였으며, '개인정보침해사실신고제도'를 도입하여 공공기관으로부터 개인정보에 관한 권리 또는 이익을 침해받은 자는 행정안전부장관에게 그 침해사실을 신고할 수 있도록 함.

니라 개별법에 개인정보보호관련 조항이 있어 이를 토대로 개인정보가 보호되고 있음.

○ 이처럼 공·사 부문의 이원적 규율체계로 인해 민간부문과 공공부문이 보유한 개인정보보호의 정합성에 문제가 발생함.

- 공공부문의 경우 개인정보를 보유하고 관리하는 전 행정기관에 적용되어 일단 보유기관에게 일반적인 개인정보 관리상의 의무가 부여되어 있는 반면, 민간부문의 경우 전 민간부문에 적용되는 일반법이 제정되지 않고, 특정분야별로 적용되는 법률과 관련된 조항이 산재하기 때문에 개인정보관리상의 기본적 보호조치가 마련되지 않고, 주로 사후 처방적인 보호가 중심이 되고 있다는 것을 알 수 있음.

○ 또한 개별법주의와 맞물려 개인정보보호의 사각지대 발생을 방치하고 있음.

- 법률마다 관련 조항에 따라 개인정보가 보호되는 경우 개인정보를 관리하는 기본지침이 보호대상 정보에 따라 다르게 규율되고, 그 관리상의 차이는 혼돈을 일으킬 소지가 있음. 따라서 개인정보보호에 대한 법제도의 공백이 발생할 수밖에 없고 규제도 중구난방식으로 이루어지고 있다는데 문제가 있음.

2) 유비쿼터스 환경의 개인정보 보호를 위한 법제도

○ 유비쿼터스 환경에서는 종래 '보안(Security)'의 개념이 지니는 기밀성, 무결성, 가용성의 요소 외에 신뢰성과 프라이버시 보호 등을 포괄하는 개념인 '보호(Dependability)'라고 하는 정보보호 법제도가 요구됨.

- 유비쿼터스 사회에서의 정보보호 법제도는 정보보호에 대한 위협으로 인한 피해 및 손실이 한층 커진 상황에 대응할 수 있어야 함.

- u-IT 기반 감시수단의 다양화, 보편화에 따라 이용자의 개인정보 유출,

해킹, 바이러스 사고, 사생활 침해 등에 대한 불안감이 해소될 수 있으며, 여기에는 금전적 목적의 최근 사이버공격으로부터의 보호도 포함되어야 함.

○ 그럼에도 불구하고 유비쿼터스 환경에 대한 법제도 수준에서의 대응은 대단히 미흡한 수준에 머물러 있음.

- 최근 국내·외에서 RFID, P2P서비스, IPv6, CCTV, 위치정보, 전자우편감시기술, 인터넷감시기술, 몰래카메라, 카메라폰 등을 둘러싸고 많은 논의들이 전개되고 있음. 특히 향후 위치기반서비스, CCTV를 활용한 전자감시에 대한 우려가 증가하면서 이와 관련한 이용자 프라이버시 보호의 중요성이 증대될 것임. 그러나 그와 같은 기술 또는 서비스들을 내포하는 개인정보 또는 프라이버시 침해 요인들에 대한 적절한 입법적 대응이 아직 이루어지지 않고 있음. 이에 따른 법제도의 변화가 필요함.

○ 따라서 RFID 기술과 위치정보서비스(Location-Based Service)[13]를 둘러싸고 제기되는 문제점들을 해소하기 위해 정부는 「위치정보의보호및이용등에관한법률」을 제정[14]하여 이와 같은 기술 또는 서비스들에서의 개인정보 침해요인에 대한 적절한 입법적 대응을 만들고자 노력하고 있음.

○ 2007년 11월 시행한 「공공기관의 개인정보보호에 관한 법률」에서는 공공기관의 CCTV에 한하여 법적 규제를 신설함.

---

13) 유·무선 통신망을 통해 획득된 위치정보를 기반으로 이용자에게 다양한 컨텐츠 및 온라인·오프라인 통합서비스를 제공하는 기술임.

14) 위치정보의 이용을 통하여 국민생활의 향상과 공공복리의 증진을 도모하면서, 위치정보의 이용환경을 조성한다는 목적 아래, 사업의 진·퇴출과 서비스 제공 등에 관한 사항을 규정(안 제2조 내지 제8조 및 제11조)하였고, 사업자[1]가 위치정보의 수집 및 이용 시 확보한 위치정보의 관리 또는 이용범위 등에 대해 반드시 지켜야 할 사항 등을 규정하고 있음(안 제12조 내지 제22조). 이 법률안은 관련 기술개발·표준화의 지원 및 위치기반서비스의 신뢰성을 제고하기 위하여 위치정보의 등급을 정하여 고시할 수 있도록 하는 한편(안 제26조 내지 제29조), 사업추진 체계, 위치정보의 오·남용 방지의무 등 법 위반정도에 따라 사업허가 취소, 과징금 및 벌금 등을 차등적으로 부과토록 함(안 제9조 및 제10조, 제30조 내지 제34조).

- CCTV는 개인의 화상정보를 무작위적으로(본인의 동의 없이) 수집한다는 측면에서 프라이버시 및 인권침해 논란이 끊임없이 있음. 이에 따라 공공기관의 CCTV에 대한 설치 및 운영에 대한 본격적인 법적 규제의 토대가 마련되기 시작함.

○ 또한, 행정안전부는 개인정보의 유출과 오·남용을 막기 위해서 공공과 민간을 포괄하는 「개인정보보호법」 제정안을 2008년 8월 입법예고함.

○ 「개인정보보호법」의 제정취지는 다음과 같음.

- 정보사회의 고도화와 개인정보의 경제적 가치 증대로 사회 모든 영역에 걸쳐 개인정보의 수집과 이용이 보편화되고 있음. 그러나 공공행정, 정보통신, 신용 등 분야별 개별법에 따라 개인정보 처리행위가 규율되고 있어 국가사회 전반을 규율하는 개인정보보호원칙과 개인정보 처리기준이 부재함. 이로 인해 개인정보보호와 관련된 법 적용을 받지 않는 개인정보보호의 사각지대가 발생할 뿐만 아니라 개별법률 간 처리기준이 상이하여 혼란을 야기하고 있는 실정임.

- 특히, 최근 개인정보의 유출, 오·남용 등 개인정보 침해사례가 지속적으로 발생함에 따라 개인의 프라이버시 침해는 물론 명의도용, 전화사기 등 정신적·금전적 피해를 초래하고 있음.

- 따라서 공공·민간을 망라하여 국제 수준에 부합하는 개인정보 처리원칙을 규정하고, 개인정보 침해로 인한 개인의 피해 구제를 강화하여 개인정보의 안전한 이용 환경을 조성하고 개인의 권리와 이익을 보장하고자 함.

- 주요내용을 살펴보면, CCTV나 네트워크 카메라 같은 영상정보처리기기의 설치 규제가 민간에까지 확대됨으로써 범죄나 화재 예방 등 공익적인 목적을 위해서만 설치, 운영할 수 있음. 법적용의 대상도 현행 공공기관이나 정보통신분야 사업자에서 비디오, 대여점 등 오프라인 사업자와 비영리단체까지 확대됨.

- 공공기관의 개인정보침해에 대한 처벌기준도 민간수준인 5년 이하의 징역 또는 5천만원 이하의 벌금으로 강화함.
- 인터넷상에서 회원에 가입하거나 본인 실명을 확인할 때 주민등록번호 외에 전자서명이나 아이핀, 휴대전화 인증 등을 병행하도록 의무화함.
- 주민등록번호와 은행계좌번호, ID와 비밀번호와 같은 주요 정보는 반드시 암호화하도록 해 유출과 오·남용 해결책을 마련하고자 노력함.
- 정부는 실질적인 법 집행을 위해서 국무총리실 산하에 기본계획과 제도 개선 등 주요사안을 심의하는 개인정보보호위원회를 신설하기로 함.

<표 4-5> 공공기관의 개인정보보호에 관한 법률과 개인정보보호법 비교

구 분	공공기관의 개인정보보호에 관한 법률	개인정보보호법(제정안)
개인정보 파일	개인정보파일에 대한 정의 중 '컴퓨터 등에 의하여' 조항으로 인해 수기화된 의무기록은 보호대상이 안됨	'컴퓨터 등에 의하여' 라는 말이 삭제됨으로서 수기화된 의무기록도 보호대상이 됨
개인정보 보호 기구	개인정보보호기관의 독립성 부족(개인정보보호심의위원회 위원장은 행정자치부차관이 맡고 위원의 선출도 위원장이 추천)	위원장은 공무원이 아닌 자로 개인정보보호에 관하여 학식과 경험이 풍부한 자(제7조 3항)로 규정해 독립성 확보
영상정보 처리기기	민간부문에 설치 제한이 없어 사생활 침해 가능성 높음	민간부문을 포함하여 설치 및 규제 강화(범죄나 화재예방 등 공익적인 목적을 위해서만 설치 운영할 수 있음)

2. 해외의 정보보호 관련 규제 동향

○ 안전한 유비쿼터스 사회를 구현하기 위해 해외에서도 정보보호와 관련하여 다양한 정책들을 추진하고 있음. 국제기구와 주요국가들의 정보보호정책을 통해 국제적 정보보호 트렌드를 살펴보고자 함(신영진, 2008; 이창범 외, 2003; 정보통신부, 2006).

1) 국제기구의 개인정보 보호원칙 및 규제 동향

(1) OECD

○ OECD는 1980년 9월 23일에 「프라이버시 보호와 개인정보의 국제적 유통에 관한 가이드라인(Guidelines on the Protection of Privacy and Transborder Flows of Personal Data)」을 이사회 권고 안으로 채택함.

- 이 가이드라인은 정보의 국제적 흐름을 원활하게 하면서 프라이버시 보호와 조화를 이루고자 하는 데 그 목적을 두고 있음. 또한 다국적 기업의 데이터의 유통관리를 위하여 회원국의 일치된 의견을 정리하여, 개인정보 보호를 위하여 회원국이 준수해야 할 일반적인 사항을 규정한 것임.

- 이 가이드라인은 자동 처리되는 개인정보에 한정하지 않고 모든 개인정보를 대상으로 삼고 있음. 개인정보가 다루어지는 방법이나 수단에 관계없이 프라이버시와 개인의 자유에 위협을 가할 수 있는 모든 개인정보의 처리에 적용됨. 가이드라인은 8가지 개인정보보호 기본원칙을 정리하고 있으며, 이러한 개인정보보호원칙은 UN 가이드라인이나 EU 지침을 비롯하여 각국의 개인정보보호법에 큰 영향을 미침(정찬모, 1998).

○ 1998년 10월에 캐나다에서 열린 OECD 각료회의는 1980년의 가이드라인에서 제시되었던 8가지 원칙을 재확인하는 「범세계 네트워크상의 개인정보 보호를 위한 각료선언(Ministerial Declaration on the Protection of Privacy on Global Network)」을 채택하고, 각국 정부에 대하여 온라인 환경에서 신뢰를 구축하고 데이터의 국제적인 자유로운 유통을 촉진하기 위해 범세계적 네트워크에서의 개인정보 보호에 관한 관심을 새롭게 가져줄 것을 촉구함(박인수, 2008).

<표 4-6> OECD의 개인정보 보호원칙

원 칙	내 용
수집제한	개인데이터의 수집에는 제한을 두어야 한다. 모든 개인 정보의 수집은 합법적이고 공정한 절차에 의하고 가능한 경우에는 데이터주체에게 알리거나 동의를 얻은 연후에 하여야 한다.
정확성확보	개인데이터는 그 이용목적에 부합되는 것이어야 하며 이용 목적에 필요한 범위 안에서 정확하고 완전하며 최신의 것이어야 한다.
목적명시	개인정보는 수집 시 그 수집목적이 명확히 제시하고, 그 후의 이용은 수집목적의 실현 또는 수집목적과 양립되어 목적이 변경될 때마다 명확화될 수 있는 것으로 제한되어야 한다.
이용제한	개인정보는 목적명확화의 원칙에 의하여 확인된 목적 이외의 다른 목적을 위해 개시, 이용, 그 밖의 사용에 제공되어서는 안 된다 다만 정보주체의 동의가 있거나 법률의 규정에 의한 경우에는 예외로 한다.
안전성확보	개인데이터는 그 분실 또는 불법적인 엑세스, 파괴, 사용, 수정, 개시 등의 위험에 대하여 합리적인 안전조치를 함으로써 보호하여야 한다.
공개	개인데이터와 관련된 개발, 실시, 정책에 대하여는 일반적인 공개정책을 취하여야 한다. 개인데이터의 존재, 성질 및 그 주요 이용 목적과 함께 데이터관리자의 식별, 주소를 명확하게 하기 위한 수단은 용이하게 이용할 수 있어야 한다.
개인참여	개인은 자신에 관한 정보를 합리적인 기간 내에 합리적인 비용과 방법에 의해 알기 쉬운 형태로 통지 받을 권리를 갖는다. 이러한 권리가 거부된 경우에 개인은 그 이유를 구하고 거부에 대하여 이의를 제기하거나 데이터의 폐기, 정정 및 보완을 청구할 권리를 갖는다.
책임	데이터관리자는 위의 제 원칙을 실시하기 위한 조치에 따를 책임이 있다.

(2) UN(국제연합)

○ 국제연합은 1990년 12월 4일 총회 결의로 「컴퓨터화된 개인정보 파일의 규율에 관한 가이드라인(Guideline for the regulation of computerized personal data file)」을 채택함.

- UN 가이드라인은 모든 공공부문과 민간부문에 적용되며 컴퓨터 파일뿐 아니라 구조화된 수작업 파일에도 적용됨. 회원국들이 이와 같은 개인정보 파일에 대하여 입법 등을 통해 규율하고자 할 때 참고하여 각국의 실정에 맞는 이행방안과 절차를 채택하도록 하고 있음.
- 이 가이드라인은 강제력이나 구속력은 없으며, 1980년의 OECD 가이드라인과 비슷한 내용의 6가지 원칙들을 제시함.

(3) EU(유럽연합)

○ EU는 세계 개인정보보호 정책의 방향을 주도하고 있으며, EU의 개인정보보호 기준은 사실상의 시장경제적인 기준으로 자리를 잡아가고 있음.

○ EU 회원국 간의 원활한 정보유통과 역외에서 EU 시민의 개인정보를 적절하게 보호하기 위해 산하단체인 '각료회의이사회'에서 유럽협약인 각료회의의 내용을 기초로 개인의 권리와 자유 및 프라이버시권의 보호 원칙을 포함하는 「개인정보처리에 대한 개인의 보호 및 개인정보의 자유로운 이용에 관한 지침(1995)」을 제정함.

- EU 회원국 내 프라이버시의 보호와 정보의 자유로운 흐름을 지향하고 있으며, 온라인 네트워크상의 개인정보보호만을 위해 제정된 것이 아니라, 정치, 경제, 행정 등 개인정보가 수집·처리되는 모든 영역을 규정하기 위해 제정됨(이창범 외, 2003).

○ EU는 회원국으로 하여금 이 지침에 따른 국내법 제정 및 법률준수 여부를 감찰할 수 있는 독립적인 감독기관 설치를 강력히 촉구함.

- 감독기관은 개인정보에 대한 접근권, 수사권을 가지고 감독의무를 이행함. 법률을 위반한 경우 법적 절차를 전개할 권한 및 상급 사법기관에 소송할 수 있는 권한도 소유하고 있음. 또한 개인정보의 유출로 손해를 입은 경우, 이 기관을 통하여 일차적인 책임이 있는 정보 관리자에게 배상을 청구함으로써 사법기관에 심사를 청구하기 전에 행정 구제를 받을 수 있도록 하고 있음.

- 이 기관은 대외적으로 각 국의 개인정보보호 대책의 적정성을 심사하는 기능도 담당하고 있음.

○ 2002년에 「전자통신부문에서의 개인정보처리 및 프라이버시 보호에 관한 지침」을 마련함.

- 이 지침은 지난 1995년 정보통신부문의 개인정보 처리와 프라이버시

보호에 관한 지침을 폐기하고 대체하는 새로운 지침으로, 기술발달의 영향을 가장 빨리 그리고 가장 밀접하게 받고 있는 전자통신 분야에서 이용·전송되고 있는 개인정보를 어떻게 보호할 것인가에 대한 문제를 다루고 있음.

- 또한 위치정보와 발신자번호표시, 스팸메일과 같이 최근 급격히 문제가 되고 있는 사안들에 대해 구체적으로 규율하고 있다는 점에 의미가 있음(정보통신부, 2006).

<표 4-7> EU 개인정보보호지침(95/46/EC)의 주요내용

구 분	내 용
적용범위	• 물적범위 : 자동처리되는 개인정보 및 구조화된 파일링 시스템에 포함되는 개인정보 • 인적범위 : 자연인의 개인정보
적용제외영역	• 국가안보, 공공의 안전 및 방위를 위한 개인정보 처리 • 형사법 영역에서의 개인정보 처리 • 서신왕래와 같은 지극히 개인적이고 사적인 목적의 개인정보 처리 • 언론보도, 문학, 예술적 표현을 위한 개인정보 처리
정보처리자의 의무	• 공정하고 적법한 개인정보의 처리 • 정보처리목적의 명시 • 정보처리목적과의 적절성과 관련성, 비례성 유지 • 개인정보의 정확성과 최신성 확보 • 기술적, 조직적 보안조치 확보 • 감독기구에 정보처리에 대하여 고지
정보주체의 권리	• 정보처리에 전반적인 사항에 대하여 통지받을 권리 • 정보처리에 대하여 협의할 권리 • 자신의 개인정보에 대해 수정을 요구할 권리 • 특정상황에서의 개인정보 처리에 대하여 반대할 권리
제3국으로의 정보이전 금지	• 적절한 보호수준을 갖추지 않은 제3국으로의 개인정보 이전 금지
독립기구의 설치	• 회원국 내 독립적인 개인정보보호기구의 설치

출처 : 이창범, 윤주연, "각국의 개인정보피해구제제도 비교연구", 2003.

2) 주요국의 개인정보 보호원칙 및 규제 동향

(1) 미국의 입법 및 정책

○ 미국에서 개인정보보호를 위해 가장 중요한 역할을 하는 것은 「세이프 하버 원칙(Safe Harbor Principles)[15]」임. 지난 1998년 10월 25일부터 발효된 EU지침은 적절한 수준의 개인정보보호체계를 갖추지 못한 제3국으로의 개인정보 이전을 엄격히 제한하도록 하였는데 이와 관련하여 미국은 자국의 항공사, 은행, 여행사 및 다국적 기업의 피해를 방지하기 위하여 이 원칙을 마련하고 EU와 협상 끝에 2000년 7월 합의하여 시행하고 있음.

- 세이프 하버 원칙에 참가할 것인지 여부는 전적으로 미국 기업의 자발적 의사에 달려 있으며, 실질적으로 이 원칙에 참가할 경우 EU 집행위원회가 개인정보취급의 적정성을 확인하여 주는 효과를 가지게 됨. 따라서 EU 회원국과는 개별적으로 협의와 논의를 할 필요 없이 적정성이 추정되기 때문에 특별한 사안이 없는 한 계속해서 개인정보를 교류할 수 있음.

(2) 영국의 입법 및 정책

○ 영국은 「1984년 정보보호법(The Data Protection Act 1984)」을 제정함으로써 개인정보보호를 위한 첫 번째의 발판을 마련함. 그러나 이 법은 개인정보보호를 위한 일반원칙을 모두 규정하고 있다기보다는 개인정보를 처리하는 공공기관이나 사업자 등을 등록하여 '정보처리자 등록부'를 유지·관리하는 것에 더 큰 초점이 맞추어져 있음.

○ 1995년 EU지침이 제정됨에 따라 영국도 이 지침의 내용에 맞추어 국내법

---

15) 'Safe Harbor' 란 면책특권이라는 의미로, 기본적으로 유럽연합 회원국과의 국제교류와 관련하여 유럽 시민들의 개인정보를 전달받아 처리하는 미국 기업이 EU지침에서 규정한 '적정성(adequacy)'을 갖추고 있는지 여부를 판단하기 위한 기준임. 이 원칙은 고지, 선택, 제공, 접근, 안전성, 정보 무결성, 이행의 총 7가지 원칙으로 구성되어 있음.

을 전면 수정하여 「1998년 정보보호법(The Data Protection Act 1998)」을 제정함. 이 법은 공공과 민간부문의 구분 없이 영국에서 이루어지는 모든 개인정보 처리에 적용되는 개인정보보호 기본법의 역할을 하고 있음.

○ 개인정보의 수집·처리 등을 규율하기 위한 정보보호 8가지 원칙을 규정하고 있음. 이 원칙은 기본적으로 OECD 프라이버시 8가지 원칙과 유사하나, EU 개인정보보호지침의 내용을 흡수하여 개인정보의 국외이전 제한 원칙을 규정하고 있다는 점과 민감한 개인정보에 대하여는 특별히 처리할 것을 포함시키고 있다는 점에서 특색이 있음.

○ 또한 2000년 3월 1일부터 시행된 정보보호법은 개인정보보호 기본원칙 등 정보주체의 권리와 정보처리자의 의무, 개인정보보호기구의 설립 및 운영, 정보법원(Information Tribunal)의 설치, 개인정보의 국외이전 등에 관한 사항을 포괄적으로 규정함.

- 적용범위는 더욱 확대되어 에 있어서 공공과 민간의 구분이 없음. 특히 전자적인 형태로 처리되는 개인정보뿐만 아니라 특정한 구조화된 수기파일링시스템(manual filing systems)은 물론, 의료기록이나 교육기록에 대해서는 순수하게 수기로 처리되는 개인정보까지도 이 법의 규율을 받는 것으로 포함시킴.

(3) 일본의 입법 및 정책

○ 일본 정부는 정보화전략인 총무성의 “e-Japan 전략 중점계획”에서 고도정보통신네트워크의 안전성·신뢰성 확보를 목표로 전자정부의 정보보호 확보와 주요 기반시설의 사이버 공격에 대한 대비책을 정보보호 시책으로 강구함(2002).

○ “e-Japan 중점계획 2003”을 통해 e-Japan Ⅱ 전략에 대한 보다 구체적인 정책방향과 추진계획을 제시함(2003. 8).

- 정보보호 분야로 ① 기간통신망 사업자의 정보보호 시책, ② 정보보호

를 위한 지속적인 대응기술 개발 촉진, ③ 정보보호 전문인력 육성, ④ 이용자 보호를 위한 시책 추진, ⑤ 정보보호 관련법 정비, ⑥ 해커대책 등 기반정비에 관한 행동계획 중심의 민·관 협력 추진 등이 제시됨.

○ 한편, 2003년 10월 경제산업성 자문기관인 산업구조심의회의 정보보안부회에서 일본의 첫 종합 정보보호 전략이라고 할 수 있는 "정보보호종합전략"을 수립함.

○ 2005년 4월 정보보호에 대한 정부의 역할 및 기능제고를 위해 정보보호대책추진실을 개편하여 내각관 내 '국가정보보호센터(Natinal Information Security Center)'를 설치함.

○ 이어 5월에는 내각부 IT전략본부 산하에 '정보보호정책회의'를 설치함. 정보보호정책회의는 2006년 2월 정보보호문제에 대한 중장기계획인 "제1차 정보보호 기본계획(2006~2008년)"을 확정, 발표함.

3. 규제적 영역의 문제점

○ 기존의 정보통신 환경을 중심으로 한 현행법제도에서는 유비쿼터스 환경에서 발생할 새로운 개인정보 침해에 대한 규제의 사각지대가 존재할 수밖에 없음. 유비쿼터스 컴퓨팅 환경에서 개인정보보호를 위한 법제도를 마련함에 있어서는 먼저 이러한 환경에 대한 충분한 이해가 전제되어야 함.

- 유비쿼터스 컴퓨팅 환경에서 공급되는 서비스는 직접적이고 강제적인 특성을 가지게 됨. 따라서 사후적으로 개인정보의 보호를 위한 방안을 마련하는 것은 실효적이지 못함. 결국 유비쿼터스 컴퓨팅 환경에 있어서는 사후대책 못지않게 사전적 개입논의가 중요함.

- 유비쿼터스 환경에서의 개인정보는 정보수집 방법이나 경로가 이전 환경에 비해 매우 다름. 대부분의 정보주체는 자신의 정보가 누군가로부터 수집되고 있다는 사실을 인식하지 못함. 즉 유비쿼터스 기술에 의해 개인의 정보가 동시에 그리고 자동적으로 입력되는 환경에서는 기존의

정보통신환경과 같이 고지하거나 동의를 얻는 것이 어려움.

- 또한 정보주체의 동의라는 형식으로 모든 정보수집 및 처리행위에 당위성을 부여하는 것 역시 유비쿼터스 컴퓨팅 환경에서는 자제되어야 할 것임. 즉 u-City와 같은 집단적 유비쿼터스 컴퓨팅 환경에 있어서는 기존의 계약법원칙에 따른 일반논의가 아니라 사회법원리가 개입하여 수정 적용될 필요성도 대두되어야 함.
- 개인의 일상생활이 선별적이 아닌 전반적으로 노출되는 유비쿼터스 환경에서는 개인의 정보보호 및 사생활보호를 위해 종합적인 수준에서의 개인정보보호대책이 마련되어야 함.

○ 그러나 유비쿼터스 컴퓨팅 환경에서의 개인정보보호와 관련한 제도정비가 시급함에도 불구하고, 현재 입법자나 집행부의 태도는 발생한 현상에 대한 결과론적 대처에만 머물고 있는 실정임. 어떠한 정보통신기술이 존재하는 경우, 그에 따른 프라이버시 침해우려와 그에 대한 대응방안을 그때 그때 논의하는 식으로 운영하고 있으며, u-City 등과 같이 복합적인 사회인프라에 대한 종합적 수준에서의 논의는 아직 하고 있지 않음.

○ 지금까지 논의한 규제적 영역에 있어서의 정보보호의 문제점은 다음과 같이 정리해 볼 수 있음.

- 첫 번째, 공공부문과 민간부문에 공통으로 적용되는 개인정보보호에 관한 일반법이 없으며, 공공부문과 민간부문을 분리해서 규제하는 방식을 취하고 있음. 따라서 법제도가 분산되어 일관성 있는 개인정보 보호체계가 정립되지 못하였고, 개인정보보호 관련 업무를 수행하는 기관이 담당 부처별로 다르거나 업무가 중첩되는 문제가 발생함.
- 두 번째, 정부의 개인정보보호를 위한 접근방법이 사전적이기보다는 사후적인 관리의 문제에 집중되어 있음. 또한 정부는 개인의 정보를 보호하는 제도적인 틀을 마련하는데 있어서 개인정보의 '집적' 단계에서 접근하기보다는 정보의 '유출'을 방지하기 위한 해결책을 모색해 왔음.

- 세 번째, 정부의 개인정보보호 방식이 처벌위주로 되어 있음. 정부가 개인정보를 보호하기 위한 접근방법은 적극적으로 정보주체의 참여를 유도하는 개인정보의 보호라기보다는 불법적으로 개인정보를 유출한 자에 대한 처벌위주가 대부분임.
- 네 번째, 개인정보보호기구의 체계가 비포괄적임. 개별법에 의해 단편적으로 존재하고 있는 개인정보보호기구는 그 체계나 독립성, 혹은 기능이나 역할 등이 매우 제한적이며 각각의 기구가 영역별로 단편적으로 운영되고 있음.
- 다섯 번째, 개인정보보호기구의 독립성이 매우 취약한 상황임. 개인정보심의위원회는 행정안전부와의 관계에서, 개인정보 분쟁조정위원회는 방송통신위원회와의 관계에서 독립적이지 못함.
- 여섯 번째, 개인정보보호기구의 기능과 역할이 매우 한정적임. 보호기구는 감독하고 집행하는 기구가 아니라 단순히 심의기관에 불과한 실정임.
- 마지막으로, u-City 환경하에서의 개인정보보호가 법적으로 공백상태임. 현행법에 의하여 보호되는 개인정보는 대부분 컴퓨터에 의하여 전산화된 개인정보에 한정되어 있음(김태헌, 2006). 최근 이루어지고 있는 법개정 및 제정은 이러한 필요성에 의해 시도되는 것으로 볼 수 있음.

○ 유비쿼터스 IT 환경에서 정보보호 법률의 집행력을 강화하고 투명성과 명확성을 확보하기 위해서는 기존의 정보환경에서의 정보보호 법제도의 한계가 극복되어야 함.

○ 온라인 공간과 오프라인 공간이 통합되는 유비쿼터스 환경의 특성상 사이버 보안 중심의 정보보호 정책에 물리적 보안을 융합시키는 새로운 u-정보보호법제, 공급자 규제중심에서 이용자 보호, IT서비스 신뢰의 제고 등으로 u-사회 전체의 촉진제 역할을 하는 법제도 등이 고려되어야 함(강경근, 2007).

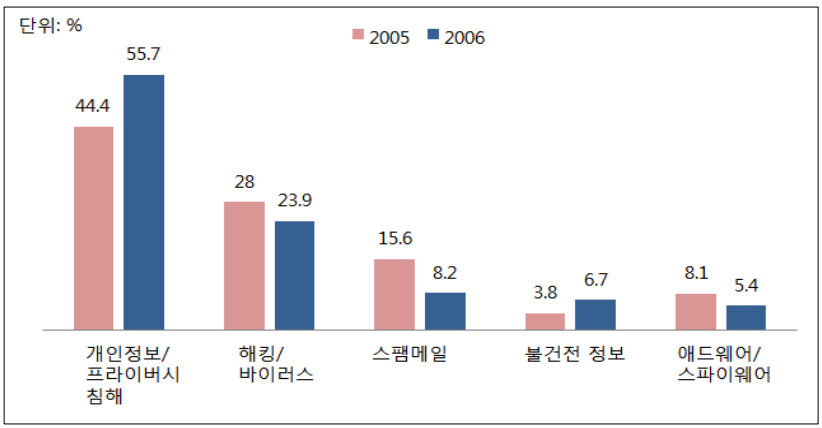
제3절 사회적 영역 : 시민들의 인식과 공공영역의 요구

1. 개인정보보호에 대한 시민들의 인식과 경험

1) 개인정보 보호에 대한 인식

○ 개인정보를 수집하고 이용하는 기관이 개인정보보호에 대한 책임과 의무를 갖도록 하는 데에 중요한 영향을 미치는 것은 사회구성원의 관심 및 권리의식이라고 할 수 있음. 자신의 정보가 어떤 목적으로 어디서 어떻게 사용되고 있는지에 대한 정보주체의 지속적인 관심이야말로 관련법의 엄격한 집행이나 기술적 보호조치보다도 근본적인 보호 효과를 나타낼 수 있음.

○ 유비쿼터스 사회에서의 불안요소를 살펴보면, 일반 사람들은 개인정보 유출로 인한 프라이버시 침해에 대해 막연한 불안감을 느끼고 있는 것으로 조사됨.



출처 : 국가정보원, 국가정보보호백서 2007

<그림 4-7> 정보화 역기능 피해 분야별 우려 정도

- 이러한 경향은 2005년에 비해 2006년에 더욱 증대됨. 이것은 곧 개인정보의 안전성과 투명성을 보장하여 사회전반적인 신뢰감을 형성해야 한다는 점을 시사함.

○ 유비쿼터스 사회의 정보보호에 대한 시민들의 막연한 인식이나 불안감과 달리 실생활에서의 정보보호에 관한 의식수준은 비교적 낮은 편이라고 볼 수 있음.

- 많은 소비자들이 무절제하게 회원으로 가입하고, 사업자의 개인정보보호정책이나 약관을 확인하지 않은 채 부주의하게 자신의 개인정보를 사업자에게 제공하는 경우가 많음. 일부 소비자의 경우 자신의 주민등록번호, 비밀번호 등의 관리를 소홀히 하여 타인에게 도용의 기회를 제공하는 경우도 적지 않음. 이로 인해 개인의 사생활 침해에 따른 정신적·물질적 피해가 심각하여 사회문제로 대두되고 있음.

○ 우리 사회에는 분야마다 여러 가지의 사회통념적 윤리 규범과 사회적 예의범절이 있음. 그러나 정보통신 분야의 활용은 급속히 확대되는데, 윤리관은 아직 정립되어 있지 못한 실정임. 이에 따라 인터넷 환경을 통제하는 가치규범적 규율이 없어 윤리적 지체현상이 발생하는 정보윤리의 부재가 발생함(김재정, 2007).

- 컴퓨터에 의한 디지털 정보통신은 삽시간에 실행될 뿐만 아니라 순간적으로 실행된 종적을 소멸시킬 수 있음. 이런 취약성을 악용하여 새로운 형태의 비윤리적 범죄행위가 발생함.

- 개인정보의 유출과 해킹 사례가 적지 않으며, 심지어 내부직원이 고객의 개인정보를 빼내 개인적으로 이용하거나 거래하는 경우가 있는가 하면, 사업자가 계획적으로 고객의 개인정보를 수집하여 제3자에게 판매하거나 공유하는 사례가 증가함.

○ 또한 새로운 유비쿼터스 정보기술들의 등장은 사회적 갈등문제를 생성함.

- 최근 법무부와 경찰이 강력한 범죄예방 대책으로 감시카메라 설치 확

대와 휴대전화 위치추적 권한 확대, 아동대상 성범죄자에 전자장치 부착 등을 추진 중임. 그러나 이러한 대책의 이면에는 개인의 사생활 침해와 인권 침해 및 권한 남용 우려 등이 있음.

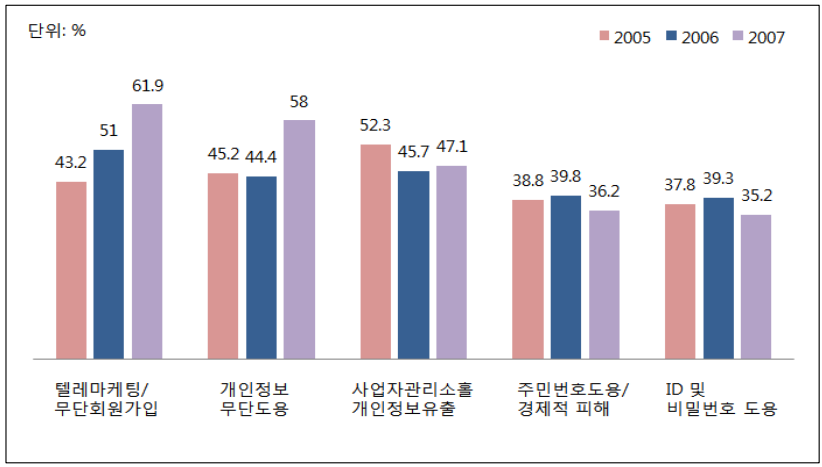
- 주민등록번호 남용 및 도용 문제를 방지하기 위해 추진 중인 '아이핀' 등의 인터넷 개인식별번호 역시 온라인상에서 개인정보가 불필요하게 대규모로 집적되는 위험을 초래한다는 비판을 야기함.
- 전자여권과 같은 전자신분증에 대한 논란 역시 찬반이 팽팽히 맞서고 있는 상황임.

○ 이러한 유비쿼터스 환경 변화 속에서 시민들의 정보보호 문제의 중요성에 대한 인식 및 윤리의 부재와 사회적 갈등 현상은 정보사회에 대한 신뢰를 상실시켜 정보사회의 발전에도 악영향을 끼칠 수 있음.

2) 개인정보보호에 대한 시민의 경험

○ 2007년 정부가 개인 인터넷 이용자를 대상으로 실시한 설문조사 결과에 의하면, 전체 응답자의 16.4%가 개인정보 또는 프라이버시 침해로 인한 피해 경험이 있는 것으로 나타남.

- 대표적인 피해 경험으로는 '개인정보 무단 수집 후 텔레마케팅에 이용하거나 무단회원 가입'이 61.9%로 가장 많음. 그 다음으로 '동의 없이 개인정보를 본래 목적 이외의 용도로 이용'(58.0%),' 사업자 관리 소홀로 개인정보 유출'(47.1%),' 주민번호 도용, 경제적 피해'(36.2%), 'ID 및 비밀번호 도용'(35.2%)의 순으로 나타남.



출처 : 한국정보보호진흥원, "2007년 정보보호 실태조사"; 국가정보원, 2008

<그림 4-8> 유형별 개인정보/프라이버시 침해 피해 경험률

○ 2007년 한 해 동안 총 25,965건의 개인정보 피해에 대한 상담·신고가 접수됨.

- 이는 2006년에 접수된 23,333건에 비해 약 11%가 증가한 수치임. 개인정보 피해에 대한 상담 및 신고 접수 유형을 분석해 보면 신용정보 침해 등의 정보통신망정보법 적용대상 이외의 개인정보침해 관련 건수가 전체의 48.1%(12,497건), 주민등록번호 등 타인 정보의 훼손·침해·도용이 35%(9,086건)로 전체 접수 유형의 83.1%를 차지함.

- 특히 2006년과 비교하여「정보통신망이용촉진및정보보호등에관한법률」적용대상 이외의 개인정보침해 관련 접수 건수가 12,497건을 차지하여 전년 대비 96% 증가함. 이는 2006년 하반기부터 발생한 공공기관 또는 금융기관을 사칭한 전화사기(Voice Phishing)가 2007년에 기승을 부렸기 때문임.

- 또한 고지·명시한 범위를 넘어선 이용이나 제3자에게 제공 관련 접수 건수가 전년보다 9% 증가한 1,001건으로 나타남.

- 반면, 이용자의 동의없는 개인정보 수집, 기술적·관리적 보호조치 미비로 인한 개인정보 누출 등과 주민등록번호 등 타인 정보의 훼손·침해 도용 관련 접수 건수는 감소함. 이는 개인정보 관련 법제도 강화 및 주민번호 노출 점검 활동 등이 주요한 원인임(2008 국가정보보호백서).

<표 4-8> 유형별 개인정보/프라이버시 침해 건수

침해유형	2006년		2007년		증감률 (%)
	건수	비율(%)	건수	비율(%)	
이용자 동의 없는 개인정보 수집	2,565	10.9	1,166	4.4	▼55
개인정보 수집시 고지 또는 명시의무 불이행	27	0.1	7	-	▼74
과도한 개인정보 수집	61	0.3	51	0.2	▼16
고지·명시한 범위를 초과한 목적외 이용 또는 제3자 제공	917	3.9	1,001	3.9	▲9
개인정보 취급자에 의한 훼손·침해 또는 누설	206	0.91	23	0.5	▼40
개인정보 처리 위탁 시 고지의무 불이행	5	0.1	2	-	▼60
영업의 양수 등의 통지의무 불이행	11	0.1	14	0.1	▲27
개인정보관리책임자 미지정	23	0.1	10	-	▼57
기술적·관리적 조치 미비로 인한 개인정보 누출 등	632	2.7	522	2.0	▼17
수집 또는 제공받은 목적달성 후 개인정보 미파기	266	1.1	146	0.6	▼45
동의철회·열람 또는 정정 요구 등 불응	923	4.0	865	3.3	▼6
동의철회·열람·정정을 수집방법보다 쉽게 해야할 조치 미이행	484	2.14	61	1.8	▼5
법정대리인의 동의 없는 아동의 개인정보 수집	23	0.1	14	0.1	▼39
주민등록번호 등 타인 정보의 훼손·침해·도용	10,835	46.4	9,086	35.0	▼16
정보통신망법 적용대상 이외의 개인정보침해 (신용정보침해 등)	6,355	27.2	12,497	48.1	▲96
소계	23,333	100	25,965	100	▲11

출처 : 한국정보보호진흥원, "2007년 정보보호 실태조사"; 국가정보원, 2008

○ 언론에 나타난 개인정보보호 관련 주요 이슈들을 살펴보면, 2008년 은행 전산망에 해커가 침입해 100여개의 금융기관 대출정보가 유출되거나 온라

인사이트들의 회원정보가 노출되는 대형사건들이 발생하여 사회적인 문제가 된 바 있음. 또한 전자상거래 등의 온라인 활동이나 CCTV 설치 등이 증가함에 따라 현행 인증 체계나 정부태도에 대한 비판, 사생활 침해 혹은 보호에 대한 찬반 양론 등의 논란과 이에 따른 사회적 갈등도 야기됨.

- 이와 같이 눈에 띄게 빈번히 발생하는 정보침해 이슈들을 통해서, 유비쿼터스 사회로의 급속한 변화와 달리 현행 개인정보보호체계의 한계를 시민들이 인식하기 시작함.

<표 4-9> 개인정보보호 관련 주요 이슈(2008년 3월~7월 주요기사 검색)

기사명
• 옥션 1800만 고객정보 대부분 유출… 정말? (2008/03/07)
• 피해갈 수 없는 CCTV, 사생활 침해vs범죄 예방 (스포츠서울 2008/03/12)
• 회사 CCTV설치로 적응장애 '업무상 재해' (보안뉴스 2008/04/08)
• 건강보험공단의 개인정보 72만건 유출 (보안뉴스 2008/04/11)
• '민증'보자는 대한민국… 프라이버시가 없다 (중앙일보 2008/04/22)
• 전자여권도 안심 못해… 인권단체들 "유출 가능성 매우 커" (쿠키뉴스 2008/04/23)
• 공공기관 개인정보 과다 요구 여전하다 (보안뉴스 2008/04/24)
• LG텔레콤 700만 고객정보 노출사건… 논란은 계속 (2008/04/25)
• 하나로텔 사태로 통신사 TM영업 '비상' (아이뉴스24, 2008/04/27)
• 낱낱이 드러나는 디지털 발자국… 디지털 빅브라더의 시대 (매일신문 2008/05/03)
• 해커에 뚫린 은행전산망 (보안뉴스 2008/05/15)
• 구글에 공공기관 문서 및 개인정보 그대로 노출! (보안뉴스 2008/05/16)
• 인터넷 개인정보 유출, 주민번호→아이핀으로 대체해야 (중앙일보 2008/05/20)
• 병원 CCTV설치, '인권 v s범죄예방'골머리 (뉴시스 2008/06/17)
• 다음'한메일' 55만명 개인정보 노출 (한국경제 2008/07/22)
• 보안 책임지는 CCTV가 해킹위협에 무방비? (보안뉴스 2008/07/24)
• 금융위, 건보가입자질병정보 열람허용 추진 '파장' (노컷뉴스 2008/07/30)

2. 공공기관의 개인정보보호 실태 및 정책적 추진 현황

○ 정부는 공공기관의 컴퓨터에 의하여 처리되는 개인정보가 적법하고 안전하게 관리되는지 매년 상·하반기 2회에 걸쳐 50여개 기관에 대해 실태조사를 실시하고 있음.

- 시민단체 및 언론을 통해 개인정보 노출 등이 자주 문제로 지적됨에 따라 개인정보보호의 중요성에 대한 일반적인 인식은 점차 높아지고 있음.

- 그러나 개인정보 유출 등 법률 위반사례는 2004년 5건에서 2005년 13건, 2006년 15건으로 점차 증가하는 추세임. 주된 유출 원인으로 개인정보를 취급하고 있는 담당자들의 인식부족과 관리소홀을 들 수 있음. 따라서 개인정보의 불법적인 유출을 방지하기 위해 정부는 공공기관에서 개인정보를 취급하고 있는 직원을 대상으로 한 교육을 강화하여 개인정보보호에 대한 인식을 제고해 나가야 함.

- 또한 기관별로 개인정보보호 관련 자체교육을 실시하지 않는 경우가 많았고, 안전조치를 확보하지 않은 채 개인정보파일을 다른 기관에 제공하는 등 세부적인 관리 측면에서 미흡한 점이 발견됨. 정부는 앞으로도 개인정보의 적법하고 안전한 관리 등을 지속적으로 점검하는 한편, 공공기관 자체적으로도 개인정보관리 역량을 강화할 수 있도록 지원을 계속할 계획임.

○ 법률 개정에 따라 기관별로 지정된 '개인정보관리책임관'을 중심으로 내부점검 및 감사 등을 통해 지속적으로 개인정보에 대한 관리를 강화할 계획임.

- 정부는 2006년부터 공공기관 홈페이지 및 구글 DB를 대상으로 개인정보 노출을 모니터링하여, 약 17만 건의 노출된 개인정보를 발견하여 해당기관에 통보하고 삭제 조치함.

- 정부는 공공기관 홈페이지상에 개인정보 노출에 대한 점검을 지속적으로 사업화하고 취약기관을 추가하여 직접점검 대상범위를 점차 확대할 계획이며, 담당자 위법사항에 대해서는 처벌을 강화할 계획임.

<표 4-10> 연도별 개인정보 노출 점검 및 삭제 현황

연 도	2006년 상반기	2006년 하반기	2007년 상반기	2007년 하반기	합 계
건수	11,973	72,927	25,423	67,159	177,482
기관 수	73	428	325	721	

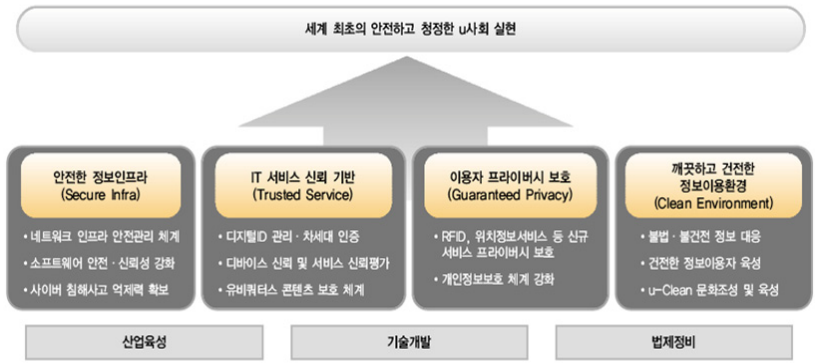
주 : 2007년 하반기는 5차계 반복점검・삭제 조치한 누적수치임.

○ 개인정보보호에 있어서 무엇보다 중요한 것은 개인정보의 처리를 실제로 담당하고 있는 실무담당자의 개인정보보호에 대한 인식과 전문성임. 따라서 개인정보보호를 직접 담당하는 업무담당자들에 대한 교육을 강화하여 전문성을 향상시키고, 이들이 기관별로 전파교육을 실시할 수 있도록 지원하는 것이 필요함.

○ 이를 위해서 정부는 전문교육기관 지정, 구체적인 업무매뉴얼 제공 등 공공기관의 개인정보보호 전문인력 육성을 지원해야 함.

- 2007년의 경우 공공기관 홈페이지 담당자들을 대상으로 학습토론회를 실시하였고, 민·관·학 공동으로 '공공기관 개인정보보호 콘퍼런스'를 개최하여 업무수행과 관련한 정보 제공, 최신기술 소개 등 개인정보보호 업무담당자들의 인식 및 역량제고를 도모함. 또한 매월 1일을'공공기관 개인정보보호의 날'로 지정, 공공기관 업무관리시스템에 개인정보보호 수칙을 게시하여 개인정보보호에 대한 인식이 제고될 수 있도록 노력하고 있음.

○ 이외에도 행정안전부는 전자정부의 핵심적 사업으로 개인정보보호 업무를 강화하여 국민이 공공기관에 믿고 맡긴 소중한 개인정보를 보다 안전하고 투명하게 관리함으로써 "전자정부에 대한 국민적 신뢰기반을 강화"해 나갈 것임.



<그림 4-9> 유비쿼터스 정보보호 기본전략(정보통신부, 2006.12)

○ 정부는 IT839 전략 추진에 따라 8대 신규서비스를 지속적으로 개발·상용화하고 있으며, 신규 IT서비스의 상용화 과정에서 발생할 수 있는 개인정보 침해 요인을 사전에 분석하여 프라이버시보호 대책 수립에 노력을 기울이고 있음.

○ 정부는 안전하고 신뢰받는 전자정부를 구현하고 개인정보 침해의 근원적 예방을 위해 공공기관 개인정보보호 종합대책을 마련 중임.

- 행정안전부는 개인정보의 유출 및 오·남용을 근절시켜 안전한 정보사회를 구현하기 위해 종합적이고 강력한 개인정보보호 종합대책을 발표함(2008년 3월).
- 이 종합대책은 기존의 개인정보 침해사례와 원인분석을 토대로 관리·기술·인식·제도 차원을 망라한 4대 분야, 15개 추진과제를 담고 있음.
- 그 주요내용으로 웹사이트상 개인정보 노출에 대한 상시점검 강화 및 위반사항에 대한 실효성 있는 대응조치 방안 마련과 개인정보보호 수준측정을 위한 진단지표의 적용·확산, 온라인상 주민번호를 대체할 '인터넷본인확인서비스(G-PIN)' 도입 등이 있음.

3. 사회적 영역의 문제점

○ 개인정보는 과거부터 다양한 형태로 존재했으나 최근 세상의 이목이 집중되고 있음. 이는 현대 자본주의의 발전, 시민사회의 성장, IT 기술의 눈부신 진보에 원인이 있음.

- 기업들은 고객 정보가 기업 활동의 중요 요소라는 것을 인식하고, 마케팅 등을 위해 개인 정보에 많은 관심을 기울이게 됨. 이에 따라 기업들의 개인정보 수집 및 이용이 증가하고 있으나, 기업의 개인정보 보호 수단에 대한 신뢰가 부족한 상황임. 인터넷 회원가입 시 대부분의 사이트가 주민번호를 필수적으로 요구하는 것도 주민번호 도용 위험과 프라이버시 침해에 대한 우려를 증가시킴.

- 시민들은 국가와 기업에 의해 자신들의 사생활이 쉽게 감시당할 수 있다는 사실을 알게 됨. 이러한 침해 위험성으로 인해 자신들의 개인정보와 프라이버시의 침해에 대해 그 어느 시대보다 우려가 높음.

○ 유비쿼터스 사회에서의 개인정보 보호 문제는 무엇보다도 개인정보에 대한 사회문화적 인식 및 윤리가 부족한데서 비롯된다고 볼 수 있음. 개인정보보호에 대한 인식의 부족 및 사업자 부주의 등은 대량의 정보침해를 가져올 수 있음.

- 통신·대출·보험 시장에서 고객 유치 경쟁이 심화되면서 내부 직원, 위탁영업점에 의한 개인정보 유출이 증가하는 실정임. 유출된 개인정보는 개인 홈페이지, 블로그, P2P를 통해 반복 거래되고 있으며, 오프라인에서 CD 형태로 유통되기도 함. 가령 2006년 4월 초고속인터넷서비스 가입자 771만명의 개인정보가 유출된 사건이 발생함.

- 주민등록번호 등 개인정보 관련 정책에 대해 국민의 인식이 부족하여 타인의 정보도용이 빈발하고 있음. 특히 사업자들의 경우 개인정보보호의 세부기준을 이행하지 않고 이익에만 급급하여 개인정보의 수집형태 및 이용을 자의적으로 해석하여 개인정보의 침해가 발생하고 있음.

- 이러한 침해 사례들은 서비스 신뢰 기반이 취약하다는 사실을 보여줌.

- 불법·불건전 정보 유통 증가와 이용자의 미디어 중독·의존 심화 등 불건전 정보 이용환경도 개인정보보호에 대한 인식의 부재에서 비롯되었다고 볼 수 있음.

○ 공공기관의 관점에서는 개인정보보호의 중요성 인식과 개인정보에 대한 관리 대책이 시급하다는 것을 알 수 있음.

- 대표적인 사례로 정보보호인력의 부족 문제를 들 수 있음. 2000년부터 정보보호 정규 교육기관이 개설되면서 양적인 인력공급은 늘어났으나, 산업현장 수요를 만족시킬 수 있는 전문성 있는 인력 양성은 미흡함. 그리고 산업현장에서 요구하는 인력요건을 제대로 파악하지 못하여 교

육 및 훈련과정이 산업체 요구대로 특성화되지 못하고, 이로 인해 인력 공급체계의 악순환이 지속되고 있음.

<표 4-11> 정보보호의 영역별 문제점

구 분	문 제 점
기술적 영역	• 인프라 위협의 고도화 · 글로벌화로 인한 사이버위협의 고도화 및 신종 사이버위협의 출현 • 네트워크 인프라 통합으로 인한 침해 위협 증대 • u-서비스에 적합한 인증체계 부재 • 명의도용 사고의 빈번한 발생 • 개인정보 유출 공간의 다변화로 인한 이용자 프라이버시 침해위협 증가 • 정보보호핵심응용기술의 개발에 대한 지원 필요 • 정보보호에 대한 축적된 기술력이 부족함. • 관련 지적재산권의 확보와 같은 기술지원적 기반이 취약함.
규제적 영역	• 공공부문과 민간부문에 공통으로 적용되는 개인정보보호에 관한 일반법이 없으며, 공공부문과 민간부문을 분리해서 규제하는 방식을 취하고 있음. 따라서 법제도가 분산되어 일관성 있는 개인정보 보호체계가 정립되지 못하였고, 개인정보보호 관련 업무를 수행하는 기관이 담당 부처별로 상이하거나 업무가 중첩되는 문제가 발생함. • 정부의 개인정보보호를 위한 접근방법이 사전적이기보다는 사후적인 관리의 문제에 집중되어 있음. • 처벌위주의 개인정보보호 방식 • 개별법에 의해 단편적으로 존재하고 있는 개인정보보호기구는 그 체계나 독립성, 혹은 기능이나 역할 등에 있어서 매우 제한적이며 각각의 기구가 영역별로 단편적으로 운영되고 있음. 보호기구는 감독하고 집행하는 기구가 아니라 단순히 심의기관에 불과한 실정임. • u-City 환경하에서의 개인정보보호의 법적 공백 －현행법에 의하여 보호되는 개인정보는 대부분 컴퓨터에 의하여 전산화된 개인정보에 한정
사회적 영역	• 유비쿼터스 사회에서의 개인정보보호 문제는 무엇보다도 개인정보에 대한 사회문화적 인식 및 윤리가 부족한데서 비롯된다고 볼 수 있음. －주민등록번호 등 개인정보 관련 정책에 대해 국민의 인식이 부족하여 타인의 정보도용이 빈발함. －사업자들의 경우 개인정보보호의 세부기준을 이행하지 않고, 개인정보의 수집형태 및 이용을 자의적으로 해석함. －불법 · 불건전 정보 유통 증가와 이용자의 미디어 중독 · 의존 심화 등 불건전 정보 이용환경도 개인정보보호에 대한 인식의 부재에서 비롯됨. • 공공기관의 관점에서는 개인정보보호의 중요성 인식과 개인정보에 대한 관리차원의 대책이 시급함. －정보보호인력의 부족 등

제5장 u-Service의 정보보호 가이드라인

제1절 개인정보보호 요구사항

제2절 정보보호 대응전략

제3절 u-Service 표준화를 통한 정보보호 체계 개발

제5장 u-Service의 정보보호 가이드라인

제1절 개인정보보호 요구사항

1. 네트워크 정보 보안 요구사항

○ 유비쿼터스 네트워크를 구성하는 다양한 요소 시스템들 간에는 일반적으로 유·무선, 인터넷을 통한 메시지 전송(커뮤니케이션)이 일어나게 되며, 이러한 과정에서 외부의 정보침해가 발생할 소지가 있음.

1) 일반적인 보안 고려사항

(1) 데이터 기밀성(Confidentiality)

○ 기밀성은 권한이 없는 사용자에게는 알려지지 않도록 하는 특성으로 이러한 특성에 대한 위협요인은 정보의 노출(disclosure)임.

○ 어떠한 데이터에 권한이 없는 사용자가 접근을 못하도록 하는 서비스로 개인 프라이버시 보장, 비밀 정보 보안 유지 등에 꼭 필요한 서비스임.

(2) 데이터 무결성(Integrity)

○ 데이터의 전송 또는 저장 시에 인가하지 않은 방법으로 제3자가 변경할 수 없도록 하는 보안 서비스임. 유비쿼터스 환경하에서는 어느 곳에서나 필요한 데이터의 전송이 이루어지게 되는데 이것의 안전을 보장하기 위한 요건이 됨.

○ 송신자와 수신자 간의 데이터 무결성을 보장하는 조건은 두 당사자 외에는 아무도 송신자와 수신자 간에 전송되는 메시지의 내용을 열어 볼 수 없음을 보장하는 것임.

(3) 인증(Authentication)

○ 인증은 기본적으로 정보 전송의 상대방의 ID(identity)를 검증하는 과정으로 정보주체가 되는 송신자와 수신자 간에 교류되는 정보의 내용이 변조 또는 삭제 되지 않았는지를 확인하는 보안 서비스임. 유비쿼터스 서비스를 통해 접하게 되는 상대방(사용자, 시스템, 또는 네트워크)의 진위 여부를 확인하기 위해 필요한 과정임.

(4) 부인 방지(Non-repudiation)

○ 송신자가 자신이 보낸 정보를 부인하는 것을 방지하기 위한 보안 서비스로 불법적인 정보 전송을 막기 위해 필요한 과정임.

(5) 익명성(Anonymity)

○ 사용자 정보는 불법적 또는 악의적 목적으로서의 인용 측면에서 보호하고자 필요 시 사용자 정보에 대한 책임 추적성(accoutability)이 보장되어야 하며, 적용되는 목적에 따라 다른 등급차원에서의 익명성이 보장되어야 함.

○ 익명성이 특히 의의를 가지는 이유는 송신자와 수신자 간에 교환되는 메시지의 암호화로 기밀성을 유지할 수 있다 할지라도, 송신자와 수신자의 통신 사실 및 위치 등을 완전히 보호하기 힘들기 때문임. 경우에 따라 선택적 적용이 필요함.

(6) 정보의 수집 및 제어

○ 사용자는 필요 시 자기 정보에 대하여 접근 및 변경이 용이하여야 함. 사용자의 동의 없이 개인정보에 접근하고 수집하려 할 때를 고려하여 제도적, 기술적 측면에서 개인정보를 보호하기 위한 접근제어(access control)가 반드시 필요함.

(7) 정보보안(Security)

○ 개인정보의 활용(수집 및 관리, 운영) 시 기술적, 제도적, 관리적 측면에서 혹시 발생할 수 있는 위험 요소에 대하여 그 피해를 최소화하기 위한 대책이 필요하며, 효과적인 모니터링을 위한 정보보안 기술 및 정책, 절차 및 지침 등을 개발, 준수할 수 있도록 해야 함.

2) 상황인식(context awareness) 정보의 보호

(1) 개요

○ 유비쿼터스 서비스의 최대 장점은 사용자의 상황에 따른 맞춤형 정보제공이 가능하다는 점임. 이러한 상황인식 서비스의 원할한 보급을 위해서는 사용자의 선호 및 취미, 일상 생활 등에 관한 폭넓은 개인정보의 수집이 요구되기 때문에, 이는 개인정보보호에 대한 매우 큰 위협요인이 됨.

○ 상황인식의 이해를 위해 다음과 같은 시나리오를 상정해 볼 수 있음.

- "오후 7시 퇴근 무렵, 김 대리는 비가 오는 테헤란로를 걷고 있다. 그가 휴대폰을 열자, 화면에는 3가지 라벨이 달린 버튼이 강조되어 표시된다 : <레스토랑>, <택시>, <지하철>, <레스토랑>을 클릭하자 그가 비오는 날 주로 좋아하는 스파게티 전문점들의 리스트가 나열되고, 각 레스토랑의 버튼을 클릭하면 당일의 스페셜 메뉴들이 나타난다. 비가 오는 날 차를 운전하지 않는 김 대리의 성향을 알고 있는 시스템은 귀가를 위해 주변의 콜택시 정보와 지하철역의 정보를 안내한다"

○ 특히 최근에 서울시를 포함한 지자체에서 제안하고 있는 대부분의 u-Service들은 해당 서비스를 이용하고자 하는 사용자의 위치 정보(위치 및 시간은 대표적인 문맥정보로 활용됨)를 기반으로 하는 LBS(Location Based Service) 들로 효과적인 개인정보 보호 방책의 수립이 더욱 시급한 실정임.

- 무선 환경에서 이동하는 사용자에게 서비스를 지속적으로 제공하기 위해서는 사용자의 위치가 추적되어야 함. 특히 유비쿼터스 컴퓨팅 환경은 도처에 존재하는 유비쿼터스 디바이스와 수시로 정보교환이 이루어지기 때문에 사용자의 위치 정보 노출은 더욱 심각한 문제로 나타날 수 있는데, 개인의 정보통제 수단 확보가 여의치 않아 더욱 어려운 문제임.

2. u-Service 정보보호 요구사항 분석

1) 개요

○ 도시의 핵심적인 기능을 담당하면서 동시에 모든 정보를 제공하는 도시통합운영센터의 보안은 u-City가 안전하게 유지, 활성화되는 데 꼭 필요한 요소임.

- u-City 내의 다양한 서비스를 효율적으로 제공하기 위해 운영하게 되는 도시통합운영센터는 도시전체 시설물, 시스템 인프라, 시민들의 정보 등 모든 정보를 통합된 데이터베이스에 저장하고 이용하게 됨.

○ u-City 서비스와 관련된 모든 정보들이 도시통합운영센터로 통합되는 경우 그로 인한 개인정보의 침해 위험성은 더욱 커질 수 있음.

○ 따라서 개인정보의 수집 및 활용에 대해 프라이버시를 최대한 보장하면서, 서비스마다 각기 다른(Service-specific) 개인 프라이버시 정보의 접근에 대해 적응적이고 동적으로 정보 이용범위를 제공하는 지능형 개인정보보호 에이전트 및 접근제어 기술 개발이 요구됨. 이를 위해서는 다음과 같은 사항이 고려되어야 함.

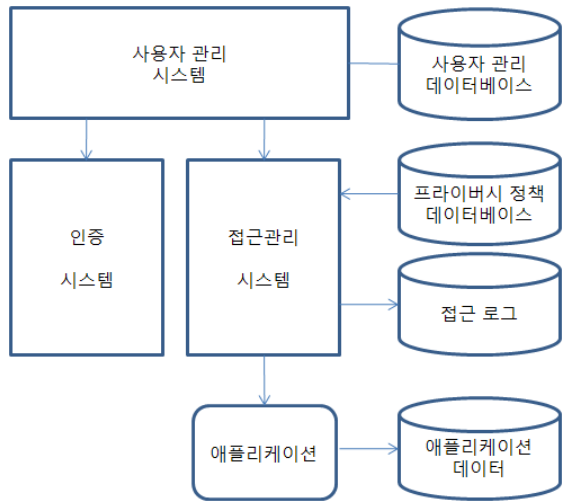
- 개인정보의 접근/이용 시 상황정보를 토대로 user preference의 동적인 적용에 따라 프라이버시 정책(privacy policy)을 시행하여 개인정보 특성에 따른 정보공개의 판정 메커니즘을 제공

- 클라이언트-서버 통합 지능형 에이전트를 기반으로 한 프라이버시 보호기술의 개발
- 프라이버시 정책에 의한 접근 판단 및 동적 상황에 근거한(context aware) 접근 제어를 통해 개인정보에 대한 수집 에이전트(agent)로부터 불법 접근 제한과 동적 개인정보의 이용
- 개인 신상정보와 분리된 상황인식 데이터의 관리로 적응적 개인정보를 이용

2) 요구사항 1 : 프라이버시 보호기능의 인프라화

○ 인프라 기능 내에 개인정보보호를 위한 개인식별 정보의 통합관리, 접근제어, 이용자의 식별과 인증 등 새로운 IT 기능을 개발하고 프라이버시 보호계층(Privacy Protection Infrastructure)을 인프라화할 필요가 있음.

○ 프라이버시 보호계층의 개념은 <그림 5-1>과 같음.



<그림 5-1> 프라이버시 보호계층의 개념도

○ 이를 위해서는, 프라이버시 보호기능을 비즈니스 프로세스로부터 분리하여 프라이버시 보호계층(Privacy Protection Infrastructure)을 업무처리 기능으로부터 분리하는 것이 요구됨.

- 예를 들어, 종래의 접근 보호를 위해서 여러 가지의 조건을 붙여 복수의 쿼리 문(query statement)을 생성하는 업무도 필요성에 따라 단일의 쿼리 문을 만드는 것만으로 끝나게 됨.
- 이 쿼리 문에 대해서 그 업무가 실행된 상황, 조작자, 입수 정보와 관련에 의한 필터링(filtering)을 프라이버시 보호계층이 수행해서 적절한 정보만을 업무 처리에 전달하도록 하는 것임.

○ 프라이버시 보호계층을 업무처리 기능으로부터 분리함으로써 업무처리 기능은 본래의 업무 처리에만 전념할 수 있으므로 결과적으로 프로그램 작성의 생산성도 향상될 수 있음.

3) 요구사항 2 : 개인정보 특성에 따른 처리

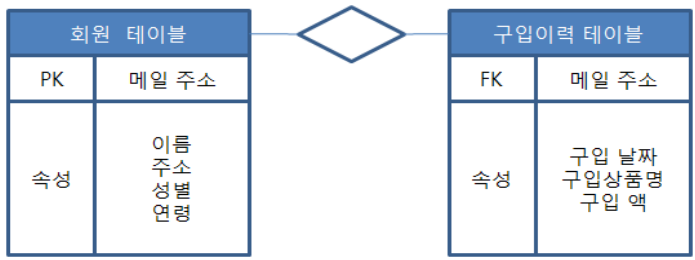
○ 기업의 애플리케이션 서비스는 최근 온디맨드(on demand) 형태로 일반화하고 있음. 이는 기업이 보유한 중요한 개인 정보의 유효한 활용이 요청되고 있는 경향으로 판단됨.

○ 즉, 보유한 개인정보를 유효하게 활용하면서 동시에 개인정보의 부정 사용을 방지하고 정보 노출을 막아야 하는 모순된 2가지 요건을 만족시켜야 함.

○ 이를 위해 개인의 프라이버시를 적정 수준으로 유지할 수 있도록 개인정보 특성에 따라 처리함으로써 서비스 중에 개인이 프라이버시 수준을 선택할 수 있도록 개인화되어야 함.

- 예를 들어, <그림 5-2>에 나타난 것처럼, 회원 정보와 그 구입 이력을 보관 유지하기 위해서 개인 신상정보(개인을 특정할 수 있는 정보)인

메일 주소를 키(key)에 관련지을 경우, 구입이력 테이블도 개인정보로 신중하게 취급되어야 함.



<그림 5-2> 참조키(FK)를 통한 개인정보의 확장

- 하지만, 위의 2개 테이블을 관련짓는 키(key)를 개인과는 직접 관계없는 속성(예를 들어, 회원넘버)으로 하는 경우, 회원번호는 개인신상정보가 아니기 때문에 구입이력 테이블은 개인정보로 취급되지 않아도 됨.

○ 개인 프라이버시 보호의 관점에서 개인정보를 포함한 데이터는 가능한 한 다른 데이터와 분리하여 프라이버시 보호계층만을 포함하는 데이터베이스나 테이블을 구축하는 것이 필요함.

- 프라이버시 보호계층이 필요한 경우에만 데이터베이스나 테이블에 접근함으로써 이용범위 및 이용자의 제한, 애플리케이션으로부터의 개인정보 이용 제어가 용이하게 됨.

4) 요구사항 3 : 프라이버시를 보호하는 접근제어

○ 개인정보의 사용범위는 기업 등이 사용자에게 제시한 프라이버시 정책에 의해 명시된 범위로 허가된 업무인가에 따라 결정됨. 즉, 프라이버시 정책에 적합한 개인정보 요구자에게만 개인정보 사용이 허가되어야 함.

○ 개인정보는 소유자의 동의 유무에 의해 사용범위가 변화되는 특징이 있고

"누가, 무슨 목적으로, 누구의 정보를 취급할까?"에 의해 접근 가부가 결정됨. 즉, 개인정보의 접근 판단은 누가, 누구의 정보를, 무슨 목적으로 접근하고 있는가 하는 동적인 상황에 의해 변화함.

- 예를 들어, 어느 쇼핑 사이트의 고객인 A는 자신의 개인정보를 쇼핑에 필요한 배송 등의 업무 이외에는 이용되지 않기를 바라고 있음. 한편, B씨는 개인화된 세일정보 등을 이메일을 통해 시기적절하게 받기를 희망하고 있음.
- 이 쇼핑 사이트의 데이터베이스를 이용해서 마케팅 매니저가 구입동향을 분석하기 위해 구입이력, 연령, 성별 등을 이용하는 경우, 데이터베이스상의 데이터 항목마다 개인정보 사용자(배송이나 마케팅 부문의 담당자) 각각에 대해 이용목적에 따른 접근제어가 요구됨.

○ 이와 같이 개인정보를 사용할 경우, 식별정보, 처리시간, 환경, 목적 등의 동적인 요소, 즉 개인정보 접근을 위한 문맥(context) 요소도 고려할 필요가 있음.

5) 요구사항 4 : 개인정보의 안전한 분산 관리 및 추출

○ 인터넷을 통한 온라인 상거래가 늘어나면서 민간 사업자에 의한 개인정보의 수집이 늘어나고 있으나, 개인정보보호 의식이 낮아 저장된 개인의 정보가 악의적인 해킹에 노출되는 경우가 많음. 공공기관의 경우도 개인 정보보호를 위한 보안 관리가 허술하고 과도한 개인정보 열람 등으로 프라이버시를 침해하고 있음.

○ 이에 대한 대책으로 개인정보의 안전한 분산 저장관리 및 추출 기능의 개발이 요구됨.

(1) 개인정보의 안전한 분산 저장관리

○ 개인정보의 안전한 저장관리를 위한 기술적 대책인 비밀정보 분산 기술에 의해 기밀성을 유지함으로써 개인정보의 안전한 저장이 가능하고, 시간이 흐르면 해독될 우려가 있는 암호화, 전자서명의 약점을 극복하며 적은 비용으로 안전하게 장기간 저장할 수 있는 분산 저장기능이 요구됨.

○ 정보에 대한 접근 권한을 한곳에 집중시키면 관리는 쉬운 반면, 위험(개인정보 침해)은 커지게 됨.

- 최근의 개인정보 노출의 가장 큰 원인은 정당한 개인정보 관리자에 의한 부정이용임. 관리자는 사용자의 기밀 데이터를 몰래 복사하거나 고쳐 쓰는 것이 가능하며 사용자 키가 로그인 패스워드라면 사용자로 위장하는 것도 가능함.

○ 리스크 분산을 개인정보 관리에 적용할 경우, 예를 들면, 중요한 개인정보를 3개의 분할된 정보로 나누어 관리자 3명에게 각각 맡기는 시스템을 가정할 수 있음.

- 이 경우, 개인정보를 복원하고 싶으면, 관리자 3명이 자신이 가지고 있는 분할 정보를 모아야 하며 이 과정에 3명 모두의 동의가 필요함. 이러한 시스템을 통해 일개 개인의 무단 개인정보 침해를 줄일 수 있음.

(2) 개인정보의 안전한 추출

○ 정보기술의 발달로 기술적이고 교묘한 방법으로 개인정보를 추출하거나 자동적으로 추론하여 개인의 디지털 정체성을 새롭게 생성해 냄으로써 개인 프라이버시를 침해하는 경우가 늘어나고 있음.

○ 최근 활용되고 있는 데이터 마이닝(Data Mining)의 목적은 구매 정보 등의 개인정보를 대량으로 모아 관련 상품 구매 분석 등 일반적으로 성립되는 규칙을 찾아내는 것임.

○ 일반적으로 규칙 자체를 공개하는 것은 프라이버시상 문제는 없지만 데이터 마이닝의 과정에서 개인정보가 마이닝 엔진에 보내짐으로써 프라이버시 침해 우려가 발생할 수 있음.

○ 이를 방지하기 위해 구매이력 등 개인정보를 열람하고자 하는 목적과 대상 및 서비스의 목적에 따라 차등적으로 개인정보의 범위를 선택적으로 추출해 주는 기술의 도입이 필요함.

6) 요구사항 5 : 장소(place) 정보의 보안

(1) 사용자의 위치를 문맥정보로 활용하는 u-Service

○ 유비쿼터스 서비스는 사용자가 위치하고 있는 장소(place)를 문맥(context) 정보로 활용하는 서비스가 주류임.

- u-Service는 광역이든 지역이든 포인트(point)든 서비스 대상지역이 정해져 있으며, 어떤 형태이든 서비스 사용자의 위치나 그 위치를 중심으로 한 일정 영역(area)을 상정하게 됨.
- 예를 들어, 소장 미술품의 소개를 u-Service로 제공하는 미술관인 경우, 그 미술관에 입장한 고객에게 어떤 콘텐츠를 제공할 것인지 여부는 그 고객이 어떤 미술품을 관람 중인지, 즉, 그 고객의 위치가 어디인지에 따라 결정됨.

○ 사용자의 위치를 문맥정보로 활용하는 대표적인 서비스로 텔레매틱스와 같은 위치기반 서비스(Location Based Service; LBS)가 있음.

- LBS는 휴대폰 속의 칩을 이용해 가입자들의 위치를 반경 수십 cm부터 수백 m 내에서 언제든지 확인할 수 있도록 해주는 서비스를 말하며, 이를 기반으로 사용자가 원하는 각종 정보를 개인화된 환경에서 서비스할 수 있음.
- LBS의 중요성은 공공안전 서비스를 통해 확연히 드러남. 예컨대 휴대

폰 사용자가 산속, 사막 등 오지에서 길을 잃었거나 집안에서 위험에 처했을 때 응급버튼 하나로 구조기관과 연결이 가능하게 됨. 또 특정 위치에 있는 가입자 전원에게 응급상황을 통지할 수도 있음. 최근 지자체에서 서비스 개발 중인 '미아찾기 서비스'가 이러한 범주에 들어감.

- u-City 추진 사업에서 LBS가 주목받는 또 다른 이유는 지자체의 행정업무의 80% 이상이 지리정보 기반의 업무라는 사실이며, 향후 급성장이 예상되는 텔레매틱스 시장의 핵심기술이기도 함.

(2) 유비쿼터스 스마트 스페이스

○ 사용자의 위치를 기반으로 한 서비스를 개념화한 모델로 유비쿼터스 스마트 스페이스(Ubiquitous Smart Space, USS)가 있음.

- USS는 u-Service와 사용자 간의 상호작용을 수행하는 물리적인 최소공간을 의미하며, 사용자가 USS에 들어오는 순간 사용자의 ID가 확인되어 자동으로 시스템에 사용자 등록이 이루어지는 공간임.

○ 이 때 특히 문제가 되는 것은 인증(authentication) 과정에 사용자의 개입을 허용할 것인지의 여부임.

- 사용자가 서비스를 받기 위해서는 서비스 공간에 진입할 때 마다 자신을 인증해야 함. 그러나, USS에서 사용자의 진퇴가 매우 빈번하게 그리고 동적으로 이루어짐에 따라 기존의 인증기술을 활용하기 힘듬.

(3) USS에서의 프라이버시 보호 요구사항

○ USS는 사용자의 위치를 감지하여 서비스를 제공하게 됨. 이러한 과정을 통해 수집된 사용자의 위치정보는 사용자가 어떤 장소를 방문했는지, 또는 그 장소에서 어떠한 행위를 했는지 등에 관한 개인정보를 생성하게 됨.

○ 이러한 정보는 개인의 취미, 건강, 생활패턴 등에 관한 유추를 가능하게 함. 이렇게 수집된 정보의 오·남용은 사용자 개인정보에 대한 중대한 침해를 가져올 수 있음.

○ 결국, 사용자의 위치 정보 수집에 대한 사용자의 명확한 동의를 얻는 과정이 필요하게 되나, 이러한 부수적인 보안 절차는 u-Service가 지향하는 보이지 않고(invisible) 자동화된(automated) 서비스의 제공을 어렵게 하는 요소가 됨.

제2절 정보보호 대응전략

1. 개 요

○ 유비쿼터스 환경에서의 보안 위협에 효과적으로 대응하기 위해서는 IT 환경의 변화에 따른 보안 위협을 사전에 분석하여 신규 IT 서비스의 초기 단계에서부터 정보보호 대책을 적용하는 노력이 필요함.

○ 유비쿼터스 사회에서의 정보보호 대응전략을 안전한 네트워크 인프라 구현, 신규서비스 안전 및 신뢰체계 구축, 정보기기의 정보보호 기능강화, 개인정보보호 개발절차의 확립 등의 측면에서 분석하면 다음과 같음.

2. 안전한 네트워크 인프라

(1) 사이버 공격 예방전략 수립

○ 망 융합에 따른 트래픽 모니터링 영역 확대 등 침해 사고 발생 시 사전 감지 및 피해를 최소화할 수 있도록 사이버 공격 예방 및 고도화 전략이 마련되어야 함.

○ 즉, 방송망이나 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 예방하기 위한 대책이 필요함.

(2) 정보보호 요소기술의 확보

○ 3대 첨단 인프라 환경에 적용할 수 있는 고성능 정보보호 요소기술의 확보가 필요함. 또한, 이러한 기술들을 사물에 내장된 초소형 내장형 시스템들과 연계하여 능동적으로 공격에 대응할 수 있는 통합보안기술과 IPv4 환경에서 IPv6로 안전하게 전환화기 위한 기술의 확보가 필요함.

(3) 정보기기 간 상호연동성 보장 표준

○ IPv6 또는 RFID/USN 등에 적용하기 위한 정보보호 제품의 안전성 검증 및 정보보호 제품 간 상호 연동성 보장을 위한 표준 제정 및 표준 적합성 인증 등을 위한 제도의 마련이 필요함.

○ IPv6가 적용된 환경에서 매우 많은 정보기기들이 서로 연동되어 작동하고, 각각 서로 다른 특성을 가지고 있으므로 각 기기에 내장된 정보보호 기능들을 연동할 수 있도록 이에 대한 표준화가 필수적임.

(4) 정보기기 간 상호연동성 보장 표준

○ 방송망에 대한 사이버 공격의 발생 등 망 융합에 따른 정보보호 환경의 변화를 수용할 수 있고, 온·오프라인상에서 개인의 프라이버시를 보장할 수 있도록 정보보호 관련 법제도의 정비가 필요함.

○ 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 요구됨.

○ 또한, RFID, 내장시스템(Embedded System) 등이 보편화됨에 따라 개인정보가 노출될 수 있는 가능성이 증가되므로, 이러한 환경에서 개인정보를 보호해 줄 수 있는 제도의 확립이 바람직함.

3. 신규 서비스의 안전 및 신뢰체계 구축

(1) 정보보호 사전 영향평가

○ 신규 IT 서비스의 안전 및 프라이버시 위협을 사전에 분석하여 예방하고 능동적으로 대응하기 위해 정보보호 관련 사전 영향평가 체계가 마련되어야 함.

○ 이를 위해서 침해위협 분석모형 연구, 정보보호 경제성 분석 등 정보보호 사전영향 평가 수행을 위한 기초 연구수행이 필요하고, 사전분석, 평가 대상 및 범위확정, 위험요소 분석 등 사전영향평가 수행을 위한 주요 업무 절차 개발도 요구됨.

○ 사전영향 평가제는 계획수립, 분석, 설계, 구축 등 정보시스템 구축 단계별 평가요소를 분석하여 평가하는 방안이 보다 효과적일 것임.

(2) 서비스 장애 대응체계

○ 와이브로, DMB, 홈네트워크 등 IT 서비스를 안정적으로 제공하고, 서비스 장애 발생 시 피해를 최소화하기 위하여 IT839 전략의 핵심구성요소와 인프라를 대상으로 서비스 연속성 체계(BCP) 구축이 필요함.

○ BCP의 도입기에는 조사, 분석이 쉽고 사고가 자주 일어나는 디바이스 중심으로 서비스 연속성 체계를 수립하고, 확산기에는 서비스 분야를 대상으로 서비스 연속성 체계를 확대하는 것이 효과적인 방안이 될 수 있음.

(3) 통합인증 체계의 구축

○ 효과적인 u-Service를 제공하기 위해서는 사람/기기의 신원, 권한/자격, 거래사실/내용 인증이 가능한 통합인증 체계의 구축이 필요함. 유·무선이 통합된 서비스의 신뢰성을 제고하기 위해 신원 인증만을 수행하는 현 전자서명법을 확대 및 개편하고 사용자 프라이버시 보호를 강화하기 위해 가명인증서, 익명인증서 사용방안을 마련하며, 불법행위 발견 시 사용자 추적이 가능한 인증체계를 마련해야 함.

4. 정보기기의 정보보호 기능 강화

(1) 홈네트워크 정보기기 보안

○ 홈네트워크 정보기기에 대한 안전성 확보를 위해서는 홈네트워크용 보안 요소기술의 개발 및 보안관리 체계구축이 필요함. 홈네트워크에서 유효한 사용자를 구별하며, 다양한 정보기기 간 안전한 통신 및 제어를 가능하게 하는 홈네트워크 환경에 적합한 인증기술 및 접근권한 제어기술 확보가 필요함.

○ 또한 이종의 유·무선 네트워크와 프로토콜의 혼재로 다양한 보안취약성이 발생하므로 홈네트워크 전체차원에서 안전성 확보를 위한 통합 보안인프라 구축이 요구됨.

○ 이를 위해 네트워크 수준의 다양한 사이버 공격으로부터 홈네트워크를 보호하기 위해 홈네트워크 보안관리기술의 개발 및 외부 응용서비스와 홈네트워크 서비스 간의 안전한 연동을 위한 웹서비스 정보보호 기술의 개발이 시급함.

(2) 텔레매틱스 정보기기 보안

○ 텔레매틱스 정보기기에 대한 안전성을 확보하기 위해서는 단말 식별기술

및 침해방지 기술 확보가 필요함. 텔레매틱스 기기를 구동하기 위한 사용자와 기기 간 인증기술 및 인증되지 않은 휴대단말기의 불법접근을 방지하기 위한 단말기 식별기술이 확보되어야 함.

○ 또한, 악의적인 공격자가 유포한 대량의 유해 트래픽으로 정상 서비스 제공이 불가능해지는 네트워크 자원 소모형 DoS 공격을 사전에 탐지하고 방어할 수 있는 공격탐지 및 방어기술의 개발이 시급함.

(3) 기타 이동통신 기기의 보안

○ 이동통신 단말기의 불법 복제 방지기술 확보 및 기기 인증 대책 마련이 필요함. 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(federated) 신뢰보안기술 등의 개발이 필요함.

5. 개인정보 보호 개발절차의 확립

○ 개인정보를 수집 및 저장, 분석 및 활용하는 응용서비스(application)를 개발하는 경우, 응용서비스의 개발절차에 개인정보의 보호를 보장하기 위한 절차 및 가이드라인을 개발하여 표준화하는 것이 바람직함.

○ 일반적으로 활용되고 있는 애플리케이션에 개인정보 보호 측면의 요구사항을 반영한 개발 절차의 예시를 보여주면 다음과 같음.

(1) 단계 1 : 개인정보보호 정책 수립

○ 개인정보보호 정책은 정보보호의 중요도에 따라 몇 개의 등급으로 분류하여 가이드라인을 개발함으로써 이후 서비스 개발 시 정보보호 측면의 가

장 기초적인 규제 기준이 될 수 있도록 함.

○ 개인정보보호 정책의 수립 예시

- 1등급 : 개인정보 관련 기밀정보로 외부 노출이 절대 불가한 정보 등급
- 2등급 : 개인정보 관련 취급 시 주의를 요하는 정보로 특히 주민등록번호 등 개인의 키(key)와 연관됨으로써 개인의 기밀정보 노출이 염려되는 정보 등급.
- 3등급 : 공개가능 여부를 결정할 때 사용자 동의 등 적절한 통제가 반드시 필요한 정보 등급
- 4등급 : 일부 공개가 가능한 정보 등급
- 5등급 : 대외 공개가 가능한 정보 등급

(2) 단계 2 : 개인정보 관리 가이드라인 수립

○ 개인정보보호 정책 설정이 완료된 후, 이 정책에 준한 세부 준수 사항인 절차, 가이드라인을 구성하고, 사용자, 운영자, 관리자 측면에서 개인정보를 다루는 역할별(role-based) 주요 업무 수행 분야를 지정하며, 향후 개인정보 활용 시 접근제어 측면에서, 실제 활용가능한 가이드라인이 될 수 있도록 정보의 제한(constraints) 및 허가(permissions) 부분을 개발하는 단계임.

(3) 단계 3 : 개인정보시스템 설계

○ 개인정보시스템, 서비스를 대상으로 환경분석을 통한 적절한 개인정보보호 정책, 절차, 가이드라인 설정 후 사용자 측면, 운영자 측면, 관리자 측면에서 적절한 개인정보 접근통제 기준이 마련되면, 실제 다양한 정보의 흐름 분석을 토대로 논리적 기반의 접근제어 체제를 수립할 수 있음.

○ 접근제어 체제 확립에는 개인정보의 입·출력 및 수정사항에 대하여 효과적이고 안전한 접근통제 기능을 수립하는 것을 포함함.

○ 최근 접근제어(access control) 분야에서 역할기반의 접근제어(role-based access control), 장소기반의 접근제어 등의 기술 개념들이 제안되고 있음.

(4) 단계 4 : 보장성 확보

○ 앞의 3단계를 통해 개발된 개인정보보호 가이드라인을 활용하여 개발된 u-Service 또는 애플리케이션의 안정성을 보장하는 단계로, 관련 운영자, 관리자에 대한 교육, 시스템 수정 및 변경 후의 형상관리(CM, Configuration Management), 수집된 개인정보에 대한 접근제어 및 주기적인 백업 등이 이루어지는 단계임.

제3절 u-Service 표준화를 통한 정보보호 체계 개발

1. u-Service의 서비스 분류

○ u-City 서비스는 추진 목적에 따라 유비쿼터스 기술(상황인지/정보처리) 및 정보통신 인프라(센싱/태그)를 활용하여 도시 구성요소(도시 인프라, 사람, 환경)의 관리 및 효용성을 극대화하기 위한 통합 및 지능화된 정보/콘텐츠의 집합이라고 말할 수 있음.

○ 이 서비스는 기관 및 연구자의 견해에 따라 다양한 분류를 제시하고 있으나, 공공성이 강해 필수적으로 제공해야 하는 기반서비스와 지자체 고유의 특성화 목적에 따라 선택이 가능한 특화서비스로 크게 분류할 수 있음. 일반적으로 서비스 표준분류는 공공, 생활, 비즈니스로 나눌 수 있음.

<표 5-1> u-City 서비스 분류체계

구분	기반서비스	특화서비스
특징	• 도시기능의 유지를 위해 적용해야만 하는 서비스 • 모든 도시에 일반적으로 적용가능한 서비스 • 기존의 지자체가 담당하던 업무를 확장	• 도시의 기능 및 특화목적에 따라 필요한 서비스 • 도시의 환경 및 특성에 따라 서비스가 존재할 수 있으며, 도시의 경쟁력 측면에서의 특화된 서비스
적용 공간	• 도시 내의 전 지역 • 주로 광역서비스에 기인	• 도시지역의 특정목적 및 지역범위에 기인
적용 목적	• 공공성 · 효율성 · 안전성	• 편의성 · 수익성 · 자족성
서비스 운영	• 서비스 주체는 지자체에 있음 • 지자체가 직접 서비스 제공 및 운영	• 서비스 주체는 서비스 제공자에게 있음 • 서비스 운영 및 제공이 지자체일 수도 있으며, 위탁 또는 제3의 서비스 제공업체가 될 수 있음.

출처 : 전호인, "u-City 공공/민간 서비스 구현을 위한 핵심기술", TTA 저널 112호, 한국정보통신기술협회, 2007.7

(1) 개인생활부문

○ 개인생활 부문은 문화/오락과 보건/복지 부분으로 다시 나눌 수 있음.

○ 문화/오락 소분류는 실제 생활 속에서 누리는 관광, 스포츠, 예술 등을 IT 기술을 통하여 사용자에게 편리하고 쉽게 제공할 수 있는 서비스로 구성됨.

○ 보건/복지 소분류에서는 병원에 직접 방문하지 않고도 치료를 받을 수 있는 원격진료 서비스와 RFID를 이용한 치매노인/미아 찾기 등 개인 생활 건강에 필요한 서비스를 제공하게 됨.

(2) 산업경제부문

○ 산업경제부문은 비즈니스/상거래, 통신/방송/출판, 금융/보험, 물류/교통, 건설, 정보관련 서비스의 총 6개의 소분류로 나뉘어 짐.

○ 비즈니스/상거래 소분류에서는 u-City 사회의 인프라를 이용한 u-Commerce, u-Business를 통해 사업에 필요한 생산관리, 마케팅, 광역계측 산업 등 비즈

니스와 상거래 전반에 필요한 서비스를 제공하게 됨.

○ 통신/방송/출판 소분류는 인터넷을 통한 e-book 서비스와 와이브로(Wibro)와 DMB를 활용해 통신 및 방송을 어디서든지 이용할 수 있게 하는 서비스들로 구성됨.

○ 금융/보험 소분류에서는 RFID를 활용한 지폐를 이용하고, 상표권 등의 위조방지, u-Payment 전자결재시스템, u-Banking 등을 통해 u-City에서의 금융/보험을 서비스하게 됨.

○ 물류/교통 소분류에는 RFID를 이용하여 유통 현황 및 위치를 알 수 있게 하는 u-유통시스템과 이동하면서 정보를 받을 수 있는 텔레매틱스 서비스, ITS를 이용한 u-교통, 지능형 도로 서비스 등이 포함됨.

○ 건설 소분류에서는 u-Apartment, u-Building으로 건물에 IT 기술을 접목하여 다양한 인프라를 쉽게 접하고 이용하기 편한 서비스를 제공하게 됨.

○ 정보관련 서비스에서는 인터넷을 활용하여 다양한 지식 정보를 제공하고, 원격으로 컴퓨터를 수리하는 등의 컴퓨터 관련 서비스를 제공함.

(3) 공공행정부문

○ 공공행정부문은 일반행정과 사회안전관리 부분으로 나눌 수 있음.

○ 일반행정 소분류에서는 차세대 전자정부, 국가전자조달시스템, u-민원처리 시스템 등을 통해 직접 찾아가지 않고도 u-City 인프라를 통해 어디서든지 민원 처리를 이용할 수 있는 서비스를 제공함.

○ 사회안전관리 소분류에서는 재난안전관리 시스템을 통해 폭우, 지진, 이상기온 등의 천재지변에 대한 대책과 각종 안전관리에 필요한 정보를 실시간으로 제공하는 서비스를 하게 됨.

2. 도시의 기능 및 개발 목적에 따른 분류

○ 한국정보사회진흥원에서 2005년에 제시한 '한국형 u-City 모델제안'에 따르면 u-City 서비스를 도시기능에 따라 다음과 같이 7개로 분류하고 있음.

(1) 도시통합관제센터

○ 도시통합관제센터 서비스는 핵심 플랫폼을 기반으로 외부의 모든 시스템과 통합연계하여, u-Transport, u-Learning, u-Health, u-Work, u-Government 등 다양한 도시서비스가 융복합된 서비스들로 구성됨.

○ 도시통합관제센터 서비스의 특징은 융복합 서비스로 센터에서 여러 u-City 서비스들을 통합 운영하기 위해 GIS 엔진 기반의 메타정보를 관리하여, 사용자가 기존의 사이트별로 접속하여 정보를 얻는 불편함을 없애고 통합포털을 통해 각종 정보를 한 눈에 조회가 가능하도록 하는 것임.

(2) u-Home

○ u-Home 서비스는 가정에서 편리한 생활을 할 수 있도록 여러 기술들을 이용하여 제공하는 서비스를 말하며, 가정 내의 기기가 홈 네트워크로 연결되어 기기, 장소, 시간 등 다양한 조건에 구애받지 않고 홈 서비스를 제공할 수 있는 디지털 홈 형식으로 구축됨.

(3) u-Work

○ u-Work 서비스로는 개인고객을 대상으로 하는 Personal Storage를 포함한 PIM(Personal Information Management Service) 형태로 개인사업정보를 관리해 주는 개인정보지원 서비스와 SOHO(Small Office Home Office), ASP, Hosting 등이 있음.

○ 그리고 기업고객을 대상으로 하는 서비스로는 재택근무자가 회사에 있을 때와 같은 환경에서 업무를 할 수 있도록 지원하는 원격근무 지원 서비스와 이동 중인 근무자의 업무 수행을 지원하는 이동 근무자 지원 서비스가 있음.

○ 그 외에 특수목적으로 이용할 수 있게 지원하는 사무공간 IT 서비스와 데이터 센터 서비스 등이 있음.

(4) u-Health

○ u-Health 서비스로는 간편화된 의료장비를 휴대용으로 활용하는 소형진단장비활용 서비스와 의료기관을 직접 방문하지 않고 다양한 형태의 진료를 받을 수 있는 원격의료서비스, 병원 간 네트워크 공유를 지원하는 의료정보 공유 네트워크, 의료포털 서비스 등이 있음.

(5) u-Learning

○ u-Learning 서비스는 첨단 멀티미디어 설비를 갖추고 수업을 진행할 수 있도록 첨단 학습장 환경을 제공하는 멀티미디어 학습장 서비스와 인터넷을 활용하여 온라인 학습 환경을 제공하는 원격교육 서비스가 있음.

○ 그리고 다양한 학습자료를 디지털화하여 제공하는 교육용 콘텐츠 공급 서비스와 교육 포털 서비스가 제공됨.

(6) u-Transport

○ u-Transport 서비스는 교통 이용자에게 교통 정보를 제공하는 기본 교통정보제공 서비스와 교통상황, 최적경로, 주차 등 여행에 필요한 정보를 출발 전 또는 주행 중에 제공하는 차량 여행자 부가정보제공 서비스가 있

음. 그리고, 차량을 이용하지 않는 여행자에게 정보를 제공하는 비차량 여행자 부가정보제공 서비스도 있음.

○ 그리고 교통정보를 수집, 관리, 제공하고 자동 제어함으로써 교통흐름을 최적화하는 교통류관리 서비스와 교통사고와 같은 비정상적 교통상황에 관한 정보를 수집하여 대응하는 돌발상황 관리서비스가 있음.

○ 이외에도, 자동교통 단속서비스, 대중교통정보 서비스, 교통공해 관리지원 서비스 등 다양한 서비스들이 포함됨.

(7) u-Government

○ u-Government 서비스로는 원스톱 행정서비스, 유비쿼터스 민원발급 서비스, 자녀안심서비스, 위치기반 모바일 관광정보서비스, 스마트 ID 카드 서비스, 시각장애인 길안내 서비스 등 다양한 서비스가 제공됨.

- 원스톱 행정서비스는 지역주민에게 민원행정의 편의를 위한 온라인 서비스가 제공되며 휴대폰을 활용하는 방향으로 나아가고 있음.
- 유비쿼터스 민원발급 서비스는 직접 방문하지 않고도 휴대폰, PDA 등을 이용하여 무인 키오스크(kiosk)를 통해 해당 서류를 인쇄할 수 있게 하는 서비스를 말함.
- 시각 장애인 길안내 서비스는 시각장애인들에게 위치인식 센서를 부착하고 곳곳에 리더기를 설치하여 이들이 근접 시에 음성메시지로 길안내를 제공하는 서비스를 말함.

3. 지능제어 측면에서의 u-Service 조망

1) 지능제어(Intelligent Control)

(1) 지능제어 시스템

○ 지능제어 시스템에 대한 정의는 다양하지만 “타협이 가능한 목표(goal)를 갖는 시스템으로서 학습기능(learning capability)을 갖고 감지 - 추론 - 행동(perception - reasoning-action)의 형태를 갖춘 시스템”이라는 정의가 가장 일반적임(M. Kokar).

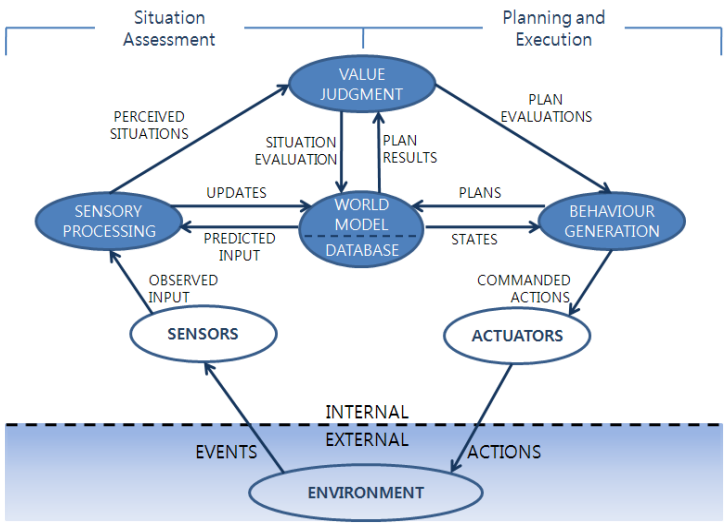
○ 관련 논문에서 논의되고 있는 지능제어시스템의 요건으로는 불확실성에 대한 대처기능, 학습 및 적응 기능, 그리고 목표달성을 위한 최적지향성 등을 들 수 있음. 이를 위한 세부 기능으로 다음과 같은 항목들이 일반적으로 고려되고 있음.

- 학습(learning) 기능 : 과거 경험을 토대로 성능이 향상되도록 지식기반을 변경하는 기능
- 추론(reasoning) 기능 : 결정기능(decision-function)의 일반화 기능
- 자율성(autonomy) : 목표(goal) 설정 및 달성 기능
- 재구성기능(reconfigurability) 또는 확장기능(extensibility) : 제어 시스템의 구조변경 기능
- 문제해결 능력(problem solving)
- 계획 및 결정 능력(planning and decsion making)
- 고장진단(fault diagnosis) 및 대처기능 또는 고장감내기능
- 신뢰성(reliability)
- 내부기능 변화에 대처하는 기능(homeostasis)
- 강인성(robustness)

- 반응성(reactivity) : 외부 자극에 즉각적으로 반응하는 능력
- 정확성(correctness) 또는 에러율 최적화(error-rate optimality) : 정해진 동작요건을 정확하게 잘 수행할 수 있는 능력
- 최적지향성 자기개선능력(optimality oriented self-improvement)
- 불확실성/복잡성 대처능력(uncertainty/complexity handling capability)
- 일반화성(generalizedness) 또는 호환성(compatibility)
- 적응성(adaptivity)
- 빠른 계산 속도(high computational speed)

(2) 일반적인 지능제어 아키텍처

○ 지능제어(intelligent control)는 외부 환경의 변화를 탐색하여, 이에 대한 능동적인 액션을 계획하고 실행할 수 있는 운영체계를 의미하며, 일반적인 아키텍처는 <그림 5-3>과 같음.



<그림 5-3> 지능제어 시스템의 일반적인 아키텍처

○ 모든 지능제어 시스템들은 외부환경에 대한, 즉 외부환경을 현 상황으로 표현하기 위한, 내부 모형(world model)을 포함하고 있음.

- 효과적인 지능제어 시스템을 구축하기 위해서는 실시간(real time) 제어가 가능한 아키텍처의 개발이 필요하며, 이를 위해서는 내부모형과 외부환경 간에 일관성(consistency)을 유지할 수 있는 체계 정립이 매우 중요함.

○ 또한, 지능제어시스템은 내부의 월드모델을 유지(즉, 외부환경과 일관성이 유지되도록)하기 위하여, 센서(sensors)를 통해 입력되는 정보들을 처리하기 위한 시스템으로 감각처리시스템(sensory processing system)을 포함함.

○ 감각처리시스템을 통해 입력된 환경의 속성(또는 속성 변화)과 지능제어시스템의 월드모델을 고려하여 시스템의 행위(behaviour)를 결정하고, 그에 따라 액츄에이터(actuator)를 제어하게 됨.

2) 지능제어 관점에서의 u-Service 해석

○ 서울시의 u-Seoul 마스터 플랜상의 서비스 중 하나인 '환경정보 통합 관제' 시스템의 예를 이용하여 지능제어의 아키텍처를 설명하면 <그림 5-4>와 같음.

<그림 5-4> 서울시 환경정보 통합관제 시스템

- 환경정보 통합관제 시스템에서 대기질, 수질, 위해폐기물 감시를 위한 센서(유·무선 CCTV 등)가 지능제어의 Sensors에 해당됨.

- 그림의 중앙에 위치한 u-Green 센터는 지능제어 아키텍처의 월드모델, 밸류 판단(value judgement), 행위 플래닝(behaviour generation)을 포함하는 의미로 해석될 수 있음. 감시 장비를 통해 들어온 신호나 영상을 처리하여 특정한 현상(예를 들어 수질오염)이 발생하였는지를 확인하는 과정이 됨. 현재 센서로부터 입력된 신호의 수준에 따른 오염 여부의 결정은 일반적으로 월드모델에 의해 결정되나 시스템의 예에서는 사람이 수행하는 것으로 파악할 수 있음.

- 특이한 징후가 발생한 것으로 생각되는 경우, CCTV를 제어하여 좀 더 세밀하게 관찰할 필요가 있음. 이렇게 CCTV의 LOS의 swing이나 tilt 각을 조절하거나 줌인/줌아웃 등의 오퍼레이션을 플래닝하는 과정이 Behaviour Generation에 해당함. 또는 수질오염 등의 비상사태가 발생한 것으로 판단되는 경우 경보신호를 울리는 행위도 해당된다고 볼 수 있음.

제6장 결론 및 정책건의

제1절 결 론

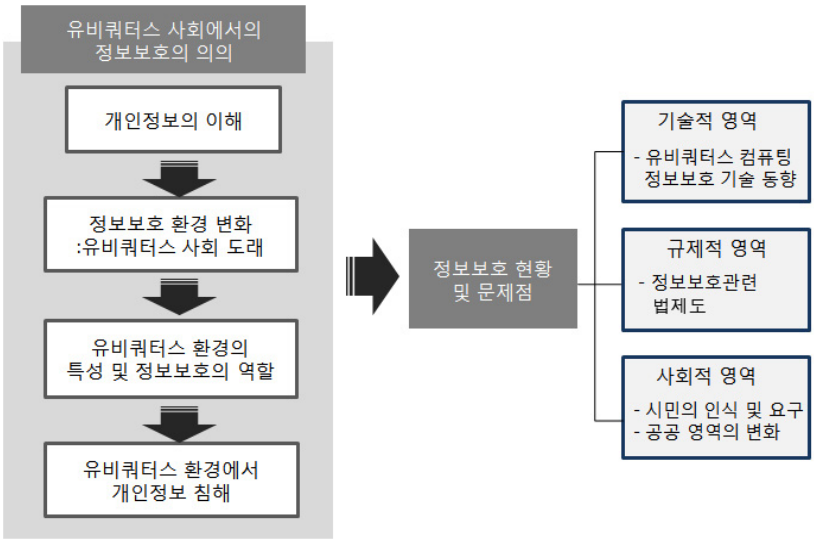
제2절 정책건의

제6장 결론 및 정책건의

제1절 결 론

1. 유비쿼터스 정보보호의 의의 및 문제점 분석

○ 정보보호 문제점을 분석하기 위해 <그림 6-1>과 같은 프레임워크를 통해 3가지 영역—기술적 영역, 규제적 영역, 사회적 영역—에 대한 현황을 살펴보고 문제점을 도출함.



<그림 6-1> 정보보호 문제점 분석을 위한 프레임워크

(1) 기술적 영역 : 유비쿼터스 컴퓨팅 환경의 정보보안 기술

○ 향후 정보보호기술은 개인정보보호, 지식 및 지적재산권 보호, 정보침해 확산 및 사이버 범죄의 방지, 끊김없는 서비스 간 상호인증 등 사용자 중심의 정보보호 정책 및 기술이 전개될 것으로 전망됨.

○ 그러나 유비쿼터스 기술의 발전은 정보주체가 인식하지 못하는 사이에 개인의 신상정보를 저장 및 축적하고, 구매 패턴, 위치정보 등을 노출시킴. 또한 이러한 정보들을 더욱더 광범위하게 수집하고, 매우 신속하게 그리고 양과 무관하게 유통하며, 무한정 복제하는 일이 가능하게 함.

○ 현재 정보보호에 대한 기술력의 축적이 부족하고, 관련 지적재산권의 확보와 같은 기술지원적 기반도 취약함.

(2) 규제적 영역 : 유비쿼터스 정보보호의 법적 현황

○ 공공부문과 민간부문에 공통으로 적용되는 개인정보보호에 관한 일반법이 없으며, 공공부문과 민간부문을 분리해서 규제하는 방식을 취하고 있음. 따라서 법제도가 분산되어 일관성 있는 개인정보 보호체계가 정립되지 못하였고, 개인정보보호 관련 업무를 수행하는 기관이 담당 부처별로 상이하거나 업무가 중첩되는 문제가 발생함.

○ 개인정보보호를 위한 정부의 접근방법이 사전적이기보다는 사후적인 관리에 집중되어 있고, 처벌위주로 되어 있음.

○ 개별법에 의해 존재하고 있는 개인정보보호기구는 그 체계나 독립성, 혹은 기능이나 역할 등에 있어서 매우 제한적이며 각각의 기구가 영역별로 단편적으로 운영되고 있음.

○ u-City 환경하에서의 개인정보보호에 대한 법적 공백

- 현행법에 의하여 보호되는 개인정보는 대부분 컴퓨터에 의하여 전산화된 개인정보에 한정되어 있음.
- 최근 국내·외에서 RFID, CCTV, 위치정보, 인터넷감시기술 등을 둘러싸고 많은 논의들이 전개되고 있지만, 그와 같은 기술 또는 서비스들을 내포하는 개인정보 또는 프라이버시 침해 요인들에 대한 적절한 입법적 대응은 아직 이루어지지 않고 있음.

○ 이에 따라 유비쿼터스 환경변화에 따른 법 개정 움직임으로, 「위치정보의 보호및이용등에관한법률(안)」을 추진하고 있으며, 「공공기관의 개인정보보호에 관한 법률」에서 공공기관의 CCTV에 한하여 법적 규제를 신설함. 또한 행정안전부는 「개인정보보호법」의 제정으로 공공·민간을 포괄하여 개인정보 침해로 인한 개인의 피해 구제 강화와 개인의 권리와 이익을 보장하고자 함(2008년 8월 입법예고).

(3) 사회적 영역 : 시민들의 인식과 공공영역의 요구

○ 자신의 개인정보와 프라이버시 침해에 대한 우려감이나 막연한 불안감이 그 어느 시대보다 높은 것과는 달리 실생활에서의 정보보호에 관한 의식 수준은 비교적 낮은 실정임.

- 주민등록번호 등 개인정보에 관련된 정책에 대한 국민의 인식이 부족하여 타인의 정보도용이 빈발하고 있으며, 사업자들의 경우 이익에만 급급하여 개인정보의 수집형태 및 이용을 자의적으로 해석함. 불건전 정보 이용환경도 개인정보에 대한 인식의 부재에서 비롯되었다고 볼 수 있음.
- 인터넷 환경을 통제하는 가치규범적 규율이 없어 윤리적 지체현상이 발생하는 정보윤리의 부재가 발생함.
- 또한 새로운 유비쿼터스 정보기술들의 등장은 찬반 양론적인 사회갈등 문제를 생성함.

○ 공공영역에 있어 개인정보에 대한 관리차원의 대책이 시급함.

- 공공기관들은 기관별로 개인정보보호에 대한 자체교육을 실시하지 않는 경우가 많았고, 안전조치를 확보하지 않은 채 개인정보파일을 다른 기관에 제공하는 경우가 있는 등 세부적인 관리 측면에서 미흡한 점이 발견됨. 또한 실무담당자들이 개인정보보호에 대한 인식이나 전문성을

키울 수 있도록 도와주는 등의 정보보호 전문인력 양성이 필요함.

○ 개인정보보호에 대한 사회구성원들의 관심 및 권리의식의 부재와 사회적 갈등은 정보사회에 대한 신뢰 상실로 이어져 정보사회의 발전에도 악영향을 끼칠 수 있음.

2. 유비쿼터스 정보보호의 요구사항 분석

○ 유비쿼터스 서비스 개발 시 고려해야 하는 개인정보보호 요구사항을 네트워크 정보보안 요구사항, u-Service 정보보호 요구사항으로 나누어 분석함.

(1) 네트워크 정보보안 요구사항

○ 현재 정보보호 요구사항으로 고려되고 있는 데이터의 기밀성, 무결성, 사용자 인증, 부인방지, 익명성, 자기정보 통제 및 제어 등의 문제는 유비쿼터스 서비스가 현실화되는 시점에 더욱 확대될 것으로 보임.

○ 이는 유비쿼터스 서비스의 최대 장점으로 꼽히는 사용자의 상황에 따른 맞춤형 정보제공이 가능하도록 사용자의 상황인식(context awareness)을 위한 다양한 정보수집이 필요하다는 점과 사이버 위협의 대상이 IP를 사용한 특정 망에서 통합된 망으로 전이되어 피해 확산속도가 증가되고, 피해 규모 역시 확대될 것으로 예상되기 때문임.

○ 따라서 유비쿼터스 서비스의 기반 망과 서비스 제공 레이어(layer) 사이에 미들웨어로서 프라이버시 보호 계층(Privacy Protection Infrastructure)을 두고, 개별적 정보침해유형에 대한 종합적이고 일관된 대응책이 마련되어야 할 것으로 판단됨.

(2) u-Service 정보보호 요구사항 분석

○ u-City 내의 다양한 서비스를 효율적으로 제공하기 위해 운영되는 도시통합운영센터는 도시전체 시설물, 시스템 인프라, 시민들의 정보 등 모든 정보를 통합된 데이터베이스에 저장하고 이용하게 됨에 따라, 악의를 가진 사용자 또는 관리자에 의한 개인정보침해의 가능성은 더욱 높아질 것으로 예상됨.

○ 이를 예방하기 위해, 프라이버시 보호기능의 인프라화, 개인정보 특성에 따른 처리, 프라이버시를 보호하는 접근제어, 개인정보의 분산관리를 통한 개인정보 보호 등의 방안을 제시함.

- 유비쿼터스 인프라 내에 개인정보보호를 위한 프라이버시 보호 계층의 인프라화가 필요하며, 이를 통해 개인식별 정보의 통합관리, 접근제어, 이용자의 식별과 인증 등의 공통기능을 수행하도록 함.
- 개인과 관련된 정보는 어떤 특정인과 연계되는 순간 개인정보화 되는 경향이 있음. 이에 따라, 개인정보가 통합되는 것을 지양하고 개별 정보들이 쉽게 조합되어 개인정보화되는 것을 방지하는 대책 마련이 필요함.
- 개인정보의 사용범위는 서비스 제공자가 사용자에게 제시한 프라이버시 정책에 명시되어 있으며, 허가된 업무 인가자에 한하여 그 사용을 허가하여야 함.

3. 정보보호 대응전략 개발

○ 유비쿼터스 환경에서의 보안 위협에 효과적으로 대응하기 위해서는 IT 환경의 변화에 따른 보안 위협을 사전에 분석하여 신규 IT 서비스의 초기 단계에서부터 정보보호 대책을 적용하는 노력이 필요함.

○ 유비쿼터스 사회에서의 정보보호 대응전략을 안전한 네트워크 인프라 구

현, 신규서비스 안전 및 신뢰체계 구축, 정보기기의 정보보호 기능강화, 개인정보보호 개발절차의 확립 등의 측면에서 살펴봄.

○ 안전한 네트워크 인프라를 구축하기 위해서는 특히 사이버 공격 예방전략 수립, 정보보호 요소기술의 확보, 정보기기 간 상호연동성 보장 표준화, 유비쿼터스 통합망 환경에 맞는 정보보호 규제 방안 마련 등이 필요함.

○ 서비스의 안전 및 신뢰체계를 구축하기 위해서는 정보보호 사전 영향평가제의 도입, 서비스 장애 대응체계, 통합인증 체계의 구축이 요구됨.

○ 정보기기의 정보보호 기능을 강화하기 위해서는 홈네트워크/텔레매틱스 등에 활용되는 다양한 이동통신 기기에 대한 정보침해 공격에 대해 대응책을 마련하는 것이 바람직함.

제2절 정책건의

1. 유비쿼터스 정보보호의 중요성에 대한 공감대 형성이 필요함.

○ 개인정보의 집적화 활용은 정보화의 진전과 함께 계속 증가할 수밖에 없고, 정보의 데이터베이스화와 공동 활용은 정보화의 효용을 극대화시키는데 필수적이나 인터넷 침해사고 및 개인정보의 악용이 발생할 가능성은 더욱 커질 수밖에 없음.

○ 개인정보보호를 위한 인프라는, CCTV의 설치와 관련된 논란에서 알 수 있듯, 시민의 안전을 위해 불가피하지만, 시민의 사생활 보호를 저해한다는 측면에서 일정정도 타협점(trade-off)이 필요함.

○ 하지만, 이 연구에서 살펴본 바와 같이, 개인정보보호를 위한 체계적인 인프라와 강력한 가이드라인의 구축으로 시민과의 충분한 공감대 형성을 촉진할 수 있는 방안 마련이 강구되어야 함.

2. 네트워크 모니터링을 통한 정보침해 예방체계 구축이 필요함.

○ 유비쿼터스 사회에서의 개인정보침해는 유비쿼터스 네트워크의 특성상 일단 사고가 발생하면 전체 네트워크로 빠르게 확산될 위험이 매우 높음.

○ 따라서, 개인정보 침해사고를 예방하는 대응체계를 고도화함으로써 BcN, IPv6등 첨단 네트워크의 이상 징후를 모니터링할 수 있도록 하여 침해사고 대응력을 높이고, 차세대 위협에 대한 취약점과 대응방법을 미리 개발하며, 신규 취약점을 분석할 수 있는 능력을 강화하여야 함.

○ 그리고 통합망의 연계성이 점차 국제적으로도 높아지므로 국제 관련기관간 협력을 강화하여야 하는데, 이를 위해서는 전문인력의 육성을 체계적으로 지원할 필요가 있음.

3. u-Service 표준화를 통한 정보보호 체계 정립이 필요함.

○ 체계적인 유비쿼터스 정보보호 원칙과 개념을 개발하기 위해서는 u-Service의 기본개념과 기능을 중심으로 관련 시스템 체계와 프로세스를 표준화할 필요가 있음. 현재는 u-Service 개발에 있어 유사한 서비스들이 서로 다른 이름으로 소개되거나 서로 다른 계층적 분류를 가지게 되는 등 매우 혼란스러운 실정임.

○ 따라서 u-Service를 특징지을 수 있는 분류기준(classification factor)을 개발하여, 앞으로 추가되거나 현재 개발된 u-Service들을 쉽고 빠르게 분류할 수 있는 체계가 마련되어야 함.

○ 이러한 체계를 통해 분류별로 어떠한 형태의 개인정보침해 유형이 발생하는지, 그리고 그러한 정보침해를 예방하기 위한 대책은 어떻게 마련되어야 하는지 등에 대한 상세한 가이드라인을 마련하여야 함. 이러한 체계는 공공 또는 민간에서 제안되는 u-Service들의 정보침해 사전영향 평가제를 실시하기 위한 프레임워크의 역할도 할 수 있을 것으로 판단됨.

참 고 문 헌

참고문헌

강경근, “정보보호 법률체계 개편 및 발전방향”, 정보통신부, 정보보호법 발전방안 마련을 위한 공청회, 2007.

강달천, “유비쿼터스 시대의 개인정보보호법제”, 「중앙법학」 중앙대학교 법학연구소, 제6집 제2호, 2004.

강장묵 · 방기천, “유비쿼터스 센싱 네트워크 환경 하에서 정보 프라이버시의 보호 기술과 영역에 관한 연구 : 상황인식시스템과 개인정보를 중심으로”, 「디지털콘텐츠학회 논문지」, 제7권 제4호, 2006.

강홍렬 외, 「유비쿼터스 사회의 역기능에 대한 법제도적 기초연구」, 정보통신정책연구원, 2004.

고웅 · 이동범 · 곽진, “u-City 서비스 분류에 따른 적용사례와 보안 고려사항”, 「정보보호학회지」, 한국정보보호학회, 제18권 제2호, 2008.

국가정보원, 「국가정보보호백서 2008」, 2008.

권헌영, “전자정부시대 개인정보보호법제의 쟁점”, 「정보화정책」, 제11권 제3호, 2004.

김기수, “유비쿼터스 네트워크에서 안전한 개인정보보호를 위한 프라이버시 보호 방안”, 「한국정보과학회 학술발표논문집」, 한국정보과학회, 제34권 제2호, 2007.

김성훈 · 이종화 · 정재호 · 김창화 · 조주은 · 남기효, “u-City 프라이버시 보호방안 연구”, 한국정보보호진흥원, 2006.

김재정, “유비쿼터스 환경에서의 개인정보보호 발전방안에 관한 연구”, 한양대학교 석사학위논문, 2007.

김태헌, “정보화시대의 개인정보 보호에 관한 연구”, 한남대학교 석사학위논문, 2006.

남택용 · 장종수 · 손승원, “유비쿼터스 환경에서의 개인정보보호 기술”, 「전자통신동향분석」, 제20권제1호, 2005.

문송철 · 강장묵, “유비쿼터스 컴퓨팅 환경의 프라이버시에 관한 연구”, 「남서울대학교 논문집」, 11-2, 2005.

박인수, “유비쿼터스 환경에서 개인정보 보호에 관한 비교연구”, 「헌법학연구」, 제14권 제2호 한국헌법학회, 2008.

변미리, “서울시 전자정부의 개인정보보호에 관한 연구”, 서울시정개발연구원, 2004.

서계원, “정보 프라이버시와 개인정보의 보호－개인정보보호기본법안을 중심으로”, 「세계헌법연구」, 제11권 제1호, 2005.

서동일, “IT839전략 추진을 위한 정보보호 기술”, 2005.

송유진 · 이동혁 · 남택용 · 장종수, “유비쿼터스 환경에서 개인정보보호의 기술동향”, 「정보보호학회지」, 제16권 제3호, 2006.

송유진 · 이동혁 · 남택용 · 장종수, “유비쿼터스 환경에서 프라이버시보호의 기술적 요구사항과 프레임워크”, 「정보보호학회지」, 제16권 제2호, 2006.

신영진, “미래사회에서의 정보보호 발전방안에 관한 연구”, 「한국행정학회 학술대회 발표논문집 4」, 한국행정학회, 2008.

윤수진, “u-City 구현에 있어서의 개인정보보호”, 「공법연구」, 제35집 제1호, 2006.

이민영, “차세대 전자정부의 개인정보보호 정책방향”, 「정보통신정책」, 제18권 3호, 2006.

이성몽, “유비쿼터스 컴퓨팅 환경에서 개인정보보호 방법” 2005.

이익섭 · 김호성 · 이완석, “u-City 서비스 정보보호 위협 및 보호대책”, 「정보보호학회지」, 한국정보보호학회, 제18권 제2호, 2008.

이창범 · 윤주연, “각국의 개인정보피해구제제도 비교연구”, 개인정보분쟁조정위원회, 2003.

임영덕, 「유비쿼터스 컴퓨팅에서의 개인정보보호」, 성균관대학교 석사학위논문, 2005.

임종인, “유비쿼터스 시대의 정보보호 기술”, 2003.

전호인, “u-City 공공/민간 서비스 구현을 위한 핵심기술”, 「TTA Journal」, 한국정보통신기술협회, No. 112, 2007.

전호인 · 정성훈 · 김용배 · 김범주 · 백준선, “u-City 구현을 위한 핵심 기술 연구”, 한국통신학회지 「정보와 통신」, 한국통신학회, 제22권 7호, 2005.

정경호 · 민경식 · 김윤정 · 이응용 · 최광희 · 김여라 · 임희준, 「유비쿼터스 정보보호 기본전략 연구」, 한국정보보호진흥원, 2006.

정영일, “전후세대의 경제의식”, 「사회과학과 정책연구」, 서울대 사회과학연구소, 제9권 제1호, 1987, 11.

정준현, “유비쿼터스 컴퓨팅과 프라이버시 보호”, 「성균관법학」, 성균관대학교 비교법연구소, 제16권 제1호, 2004.

정찬모, “개인정보 보호 관련 주요국동향 및 국제적 입법의 필요성”, 「통상법률」, 법무부, 제20호, 1998.

조규백, “유비쿼터스 환경에서의 정보보호 기술동향”, 2005.

최명길 · 김세헌, “정보보호 패러다임 변화 및 정보보호 동향에 대한 고찰”, 「정보보호학회지」, 한국정보보호학회, 제17권 제4호, 2007.

한국전산원, “u-City로 바라보는 미래도시의 모습과 전망,” 「유비쿼터스사회연구시리즈」, 제8호, 2005.

한국정보보호진흥원, “2007년 정보보호 실태조사”, 2007.

한국정보보호진흥원, 「2003 개인정보보호백서」, 2004.

한국정보사회진흥원, “u-City 인프라 · 기술 · 서비스 모델의 표준화 방안”, 2006.

홍도원, “정보보호기술의 현재와 미래”, 「지역정보화」, 40, 2006.

홍승필 · 이철수, “유비쿼터스 컴퓨팅 환경내 개인정보보호 프레임워크 적용방안”, 2006.

홍승필 · 장현미, “개인정보 이슈 및 메커니즘”, 2007.

홍준현, “유비쿼터스 환경에서의 개인정보 보호－법정책적 고찰”, 「공법연구」, 사단법인 한국공법학회, 제32집 제5호, 2004.

황인호, “개인정보보호제도에서의 규제에 관한 연구”, 건국대학교 박사학위논문, 2001.

황중연, “유비쿼터스 환경변화에 따른 정보보호의 주요 현황과 대응전략”, 한국통신학회지 「정보와통신」, 한국통신학회, 제25권 제1호, 2008.

Gordon A. Gow, “개인정보보호와 유비쿼터스 네트워크 사회”, 「유비쿼터스 네트워크 사회에 관한 ITU 워크숍 자료집」, 국제전기통신연합(ITU), 2005.

영문요약(Abstract)

Development of Privacy Protection Infrastructure for Ubiquitous Information Society

Mookyung Jang · Ji-Won Choi · Jieun Lee

For recent several years, much effort has taken to develop technological infrastructure of ubiquitous information society in South Korea. Local governments including Metropolitan Seoul are interested specially in finding opportunities to bring the technological investment to one-step upgrade in terms of citizen's life style as well as their living standards. While safety and reliability are important characteristics to successfully deploy the services within the boundary of a city, socio-legal issues such as protection of privacy information have not received the attention that they deserve. These issues should be dealt with sufficiently from an initial stage of the implementation of ubiquitous services because illegal gathering and use of privacy information may reduce the affirmative results of ubiquitous computing. In this report, we try to classify the security problems to be faced in ubiquitous information society and prescribe privacy guidelines that ubiquitous information services should meet.

The threat to privacy in the ubiquitous information society is caused by a fact that privacy information may be collected, analysed, and duplicated without information owner's approval. Moreover, it is nearly impossible for an individual to have a complete understanding about what information is collected and why it is collected. In this study, to analyse present state of privacy protection, security problems are classified according to a framework consisting of the following three categories : technical, legal, and social perspectives.

When developing privacy protection guidelines, two important aspects should be considered : (a) most ubiquitous services are designed to provide personalized information to each individual (context-awareness), and to do this, (b) all the information collected should be stored at an integrated information center. To reveal the effects of these aspects, this study also tackles an issue of how the privacy protection guidelines are developed. Though this study fails to present complete answer about the question, we found that intelligent control theory can be used as an analysis viewpoint to extract behavioral patterns of ubiquitous services in terms of privacy information flow.

Table of Contents

시정연 2008-PR-29

유비쿼터스 사회의 정보보호 방안

발 행 인 정 문 건

발 행 일 2008년 10월 31일

발 행 처 서울시정개발연구원

137-071 서울시 서초구 서초동 391번지

전화 (02)2149-1234 팩스 (02)2149-1025

값 5,000원 ISBN 978-89-8052-641-3 93330