디지털컨버전스에서의 서비스를 위한 개인정보보호 연구

문남미* · 용승림** · 오정민*** · 조태남****

1. 서 론

디지털 컨버전스란 디지털 기술에 의해 기술 간, 기기 간, 서비스 간의 융복합화가 일어나는 것을 말한다. 정보의 3대요소인 음성, 문자, 영상을 송수신하거나 처리하는데 있어서, 과거에는 기술적으로 통일된 방식으로 처리할 수가 없어 다른 방식과 기기를 사용하였다. 그러나, 지금은 디지털 기술의 발달로 이들을 같은 방식으로 통합하여 처리할 수 있게 되었고, 또한 하나의 기기를 사용할 수 있게 되었다. 디지털 컨버전스는 다음 그림1과 같이 4단계의 발전과정을 거치면서 전자 산업에 구조적 변화를 일으키고 있다[7]. 특히, 정보통신기반의 디지털컨버전스는 중요 신규서비스중심으로 사회에 일반화되어가고 있는 것이 현실이다.

이와 같은 디지털컨버전스를 기반으로한 신규서비스전략은 우리 모두에게 매우 편리하고 지능화된 서비스를 제공할 것으로 기대된다. 체계적인 디지털컨버전스 전략이 수립되기 위해서는 생산자와 소비자의 상호관계를 분석하여, 소비자 주체로 가치를 평가하는 것이 필요하다[그림 2참조] [1].

이와 같은 서비스 상호작용 프로세스는 유비쿼

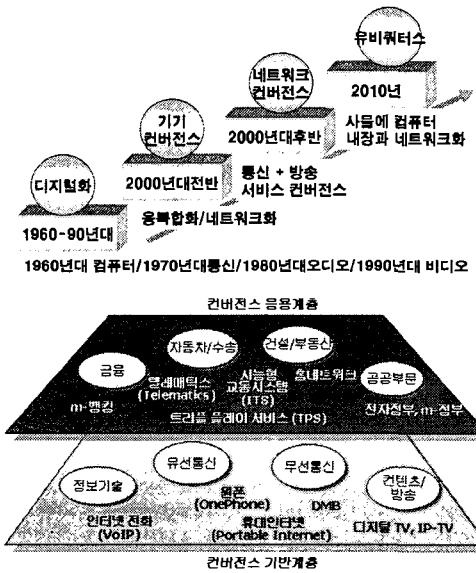

그림 1. 디지털컨버전스의 발전단계와 구도

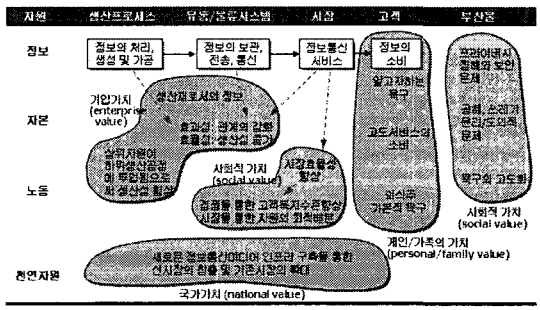

그림 2. 생산자와 소비자의 상호작용프로세스

※ 교신저자(Corresponding Author) : 문남미, 주소 : 서울시 서초동 1603-54(137-070), 전화 : 02)3470-5140, FAX : 02) 523-6767, E-mail : mnm@suv.ac.kr
* (주)종신회원, 서울벤처정보대학원대학교 디지털미디어학과
** 이화여자대학교 컴퓨터공학과 전임교수 (E-mail : dragon@ewhain.net)
*** 서울벤처정보대학원대학교 디지털미디어학과 (E-mail : aliibaba@naver.com)
**** 우석대학교 우석대학교 정보보안학과 조교수 (E-mail : tncho@woosuk.ac.kr)

터스 사회에서 컴퓨팅 기능이 주변에 산재한 정보기기 및 사물에 내재하면서 지능화된 홈 네트워크, 텔레매틱스 서비스를 소비자(이용자)들이 일상생활에서 언제 어디서든지 원하는 정보를 이용할 수 있게 한다. 그러나 모든 기술적 진보와 더불어 유비쿼터스 환경 하에서 발생할 부작용에 대해서도 대비할 필요가 있으며, 그중에서도 가장 우려되는 것은 개인정보의 오남용에 따른 프라이버시 침해 위험에 대한 것이다.

한편, 프라이버시의 관점에 대한 변화가 있으며, 정보통신기술의 발달로 개인의 신상정보에 관한 수집·분석·검색·복제·유통이 훨씬 용이해지면서 프라이버시의 개념은 '혼자 있을 권리'라는 소극적 개념에서 '자신에 관한 정보를 통제할 수 있는 권리'라는 적극적 개념으로 확대되고 있으며, 대표적인 예로 주거 등 사적인 공간을 포함한 사생활을 침해받지 아니할 권리, 개인 간의 의사소통 내용의 비밀을 보장받을 수 있는 프라이버시권이 있다. 더 나아가, 정보프라이버시권은 적극적 행위권으로 발전된 형태로 자신의 개인 정보에 대한 통제권을 행사할 수 있는 권리를 가리키며, 타인에게 제공된 자신의 개인 정보의 유통과 활용의 전 과정에 관여할 수 있는 권리를 포함한다.

이러한 프라이버시의 개념 변화는 유비쿼터스 환경에서 자신의 다양한 수요를 충족시키기 위해 일정한 목적 범위 내에서 자신을 공개하면서도 다른 한편으로는 자신의 행적을 타인의 권한 없는 관여로부터 보호해야 하는 필요성의 증가에서 출발하고 있다.

2. 프라이버시 개념 및 침해 유형

2.1. 프라이버시 개념 및 중요성

2.1.1 프라이버시 개념

프라이버시(Privacy)라는 용어는 '사람의 눈을 피하다'라는 라틴어에서 유래된 말로 크게 주거의 자유, 신체의 자유, 통신의 자유로 구분되어 왔다. 더 나아가, 정보프라이버시권은 적극적 행위권으로 발전된 형태로 자신의 개인 정보에 대한 통제권을 행사할 수 있는 권리를 가리키며, 타인에게 제공된 자신의 개인 정보의 유통과 활용의 전 과정에 관여할 수 있는 권리를 포함한다.

또한 프라이버시와 유사한 개인정보의 개념을 이해할 필요성이 있는데 생존하는 개인에 관한 정보로서 성명, 주민등록번호 등에 의하여 개인을 식별할 수 있는 부호나 문자, 음성, 음향 및 영상 등의 정보를 모두 개인정보라 일컫는다. 정보 하나만으로는 특정 개인을 알아볼 수 없는 경우라 하더라도 다른 정보와 쉽게 결합하면서 개인 식별이 가능하면 이 범위에 포함된다. 전세계적으로 개인정보에 관한 정의는 다양하게 내려지고 있으나 공통적으로 당사자 식별이 가능한 '개인에 관한 정보(Personal Data)'를 말하는 것으로 이해하면 된다.

이러한 개인정보는 프라이버시 종류 중의 하나인 정보프라이버시의 보호 대상으로, 보호하여야 할 대상을 개인정보 그 자체보다는 개인정보에 관한 '권리'라고 한다면 개인정보보호를 '정보프라이버시 보호'와 같은 의미로 볼 수 있다.

2.1.2 프라이버시 보호의 중요성

유무선을 통합한 유비쿼터스 컴퓨팅 시대에는 많은 정보가 융합되고 컨버전스 되면서 각 개인은 단계별로 ID, 비밀번호, 인증 정보 등을 사용하게 된다. 현재도 이러한 정보를 도용하고 타인 명의를 사용하여 경제적 이득을 취하는 사례가 많은 가운데 유비쿼터스 환경에서는 유무선 상에서 개인 활동이 증가함에 따라 개인정보의 노출이 다각도에서 발생하고 그로 인한 개인정보 불법 취득이 많아질 것으로 예상된다. 또한 현대 정보사회는

모든 경제 주체의 활동이 개인정보를 활용하여 유지, 운영되고 있어 개인정보 없이는 사회적 경제 활동이 어려우며 고객유지관리 등이 기업의 기본적 활동으로 취급되는 상황이다.

따라서 개인정보의 노출은 가벼운 수준에서 일회성으로 일어나더라도 사후구제가 어려운 개인적, 국가적 피해를 야기한다. 특정 개인에 대한 명예훼손 및 사회적 신용의 저하 등 사회 경제적 활동에 치명적 지장을 주는 것이 모두 이러한 개인정보의 노출에서 발생한다.

정보통신 및 디지털미디어 기술의 발전으로 개인정보가 담긴 데이터베이스가 통합, 교류하며 피해의 단위가 대량으로 옮아갈 수 있음은 쉽게 예상되는 일이다. 기업의 개인정보를 활용한 마케팅으로 개인 사생활 침해가 늘어나자 개인의 자기 정보에 대한 권리 요구 수준이 높아졌으며 개인정보에 대한 소홀한 관리는 정부의 유비쿼터스 정보화 활성화 정책 및 신규 서비스에 대한 거부로까지 이어질 수 있는 중차대한 문제로 인식되고 있다.

이러한 전제 하에 디지털컨버전스 신규 서비스 하에서의 프라이버시 침해 요인을 살펴보기 위한 기본 전제로 사용되는 개인정보는 기존 17개 정도로 구분되던 정보에서 영상 정보, 인증 정보 등을 추가하여 확장된 종류를 갖게 된다. 기존 개인정보 기준에서, 디지털컨버전스 하에 프라이버시 침해요인을 재정리하면 [표1]과 같다.

표 1. 개인정보의 확장 유형

구분	개인정보의 종류
일반정보	이름, 주민등록번호, 운전면허번호, 주소, 전화번호, 생년월일, 출생지, 본적지, 성별, 국적
가족정보	가족 구성원들의 이름, 출생지, 생년월일, 주민등록번호, 직업, 전화번호
교육 및 훈련정보	학적사항, 기술자격증 및 전문면허, 이수한 훈련프로그램, 동아리활동, 상벌활동
병역정보	군번 및 계급, 제대유형, 주특기, 근무부대
부동산 정 보	소유주택, 토지, 자동차, 기타 소유차량, 상점 및 건물 등
동산정보	보유현금, 저축현황, 현금카드, 주식, 채권 및 기타 유가증권, 수집품, 고가의 예술품, 보석
소득정보	현재 봉급, 봉급경력, 보너스 및 수수료, 기타 소득의 원천, 이자소득, 사업소득
기타수익 정 보	보험(건강 생명 등), 가입현황, 회사의 판공비, 투자 프로그램, 퇴직 프로그램
신용정보	대부잔액 및 지불상황, 저당, 신용카드, 지불연기 및 미납의 수, 입금압류통보에 대한 기록
고용정보	현재의 고용주, 회사주소, 상급자의 이름, 직무수행 평가기록, 훈련기록, 출석기록, 상벌기록, 성격, 테스트결과, 직무태도, 휴가, 병가
법적정보	전과기록, 자동차교통위반기록, 파산 및 담보기록, 구속기록, 이혼기록, 납세기록
의료정보	가족병력기록, 과거의료기록, 정신질환기록, 신체장애, 혈액형, IQ, 약물테스트 등 각종 신체테스트정보
조직정보	노조가입, 종교단체가입, 정당가입, 클럽회원
통신정보	전자우편, 전화통화내용, 로그파일, 쿠키
위치정보	GPS나 휴대폰에 의한 개인의 위치정보
신체정보	지문, 홍채, DNA, 신장, 가슴둘레 등
습관 및 취미정보	흡연, 음주량, 선호하는 스포츠 및 오락, 여가활동, 비디오 대여기록, 도박성향 등
영상정보	방문자영상, 통화영상, 회의영상 등 개인 및 가족, 일반인영상, 실시간 및 저장영상
인증정보	ID, 비밀번호, 인증번호, 보안카드번호
구매정보	구매 품목, 구매 시기, 구매처, 구매금액
기타정보	이 외 개인식별이 가능한 정보

2.2. 프라이버시 침해 유형

현재의 디지털미디어 컨버전스 환경에서 유비쿼터스 기술의 발달로 환경이 변화됨에 따른 프라이버시 침해 유형을 큰 관점에서 정리하여 보면 다음 그림3 과 같은 설명이 가능하다. 그림에서 살펴 볼 수있듯이, 유비쿼터스 환경으로 발전하게 되면 현재의 침해 유형에 개방형 네트워크의 융합이 더해져 한 층 치명적인 침해가 발생할 수 있다. 먼저 네트워크를 이용한 개인정보의 공유로 인한 침해, 융합 네트워크망을 통한

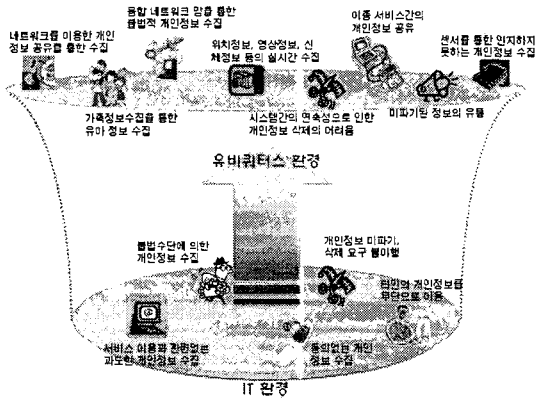

그림 3. 개인정보 침해유형의 변화

불법적 개인정보 수집, 이종 서비스들이 서로 결합함으로 일어나는 개인정보의 공유, 센서와 칩 기술이 발전함으로 인한 개인이 인지하지 못하는 부지불식간의 개인정보 수집이 일어날 것으로 보인다. 서비스의 제공 단위가 개인에서 가족, 사회 전체로 이동하면서 가족정보수집을 통한 유아 정보 수집, 혹은 그 반대의 경우도 가능해진다. 이렇듯 시스템간의 연속성으로 개인정보 삭제가 어려워지고 미파기된 정보가 재유통되는 악순환이 프라이버시 침해의 파급력에 영향을 끼친다.

디지털컨버전스가 우리 사회 전 분야에 널리 확대 활용되면서, 우리사회에서 정보통신 의존도가 증가하여 사이버 세상의 중요성 및 역할이 물리적인 현실세계에 버금가게 중요해지는 사회로 진화되고 있다. 디지털 컨버전스는 기기 컨버전스, 네트워크 컨버전스를 넘어 유비쿼터스 컨버전스로 향하고 있다[그림1참조].

유비쿼터스 시대에는 여러 곳에 흩어져 있는 전자 태그·센서와 컴퓨터들이 각종 유·무선통신 네트워크로 서로 연결되어 실시간으로 상황 정보를 인식하고 이러한 정보들이 종합되어 궁극적으로 사람들에게 필요한 여러 가지 서비스를 적시, 적소에 제공하게 된다. 그런데 보다 향상된 맞춤형 서비스를 제공하기 위해서는 보다 많은 정보를 수집·분석해야 하므로 그만큼 프라이버시 침해의 위험도 높아지는 문제가 있다. 유비쿼터스 사회를 준비하며 디지털컨버전스 서비스에서의 위협요인에 대한 파악은 중요하다고 본다. 개인정보가 컨버전스화된 서비스 환경에서 사용될 것이므로 개인의 정보가 침해를 받을 경우 그 문제의 심각성은 현재보다 훨씬 배가될 것으로 예상된다.

디지털서비스의 각 요소들은 정보보호 측면에서 볼 때 여러 가지 위협 요소를 가지고 있다. 따라서 신규서비스별 위협 및 취약점 분석을 통해 안전성과 신뢰성을 보장하기 위하여 각 요소별 위험평가를 수행하고 개인정보의 연계 가능성과 유출 위험 등을 조사하고 분석하여 프라이버시 보호 방안 제정을 위한 기초가 필요하다. 프라이버시의 관점에 대한 변화가 있으며, 정보통신및 디지털미디어 기술의 발달로 개인의 신상정보에 관한 수집·분석·검색·복제·유통이 훨씬 용이해지면서 프라이버시의 개념은 '혼자 있을 권리'라는 소극적 개념에서 '자신에 관한 정보를 통제할 수 있는 권리'라는 적극적 개념으로 확대되고 있으며, 대표적인 예로 주거 등 사적인 공간을 포함한 사생활을 침해받지 아니할 권리, 개인 간의 의사소통 내용의 비밀을 보장받을 수 있는 프라이버시권이 있다. 더 나아가, 정보프라이버시권은 적극적 행위권으로 발전된 형태로 자신의 개인 정보에 대한 통제권을 행사할 수 있는 권리를 가리키며, 타인에게 제공된 자신의 개인 정보의 유통과 활용의 전 과정에 관여할 수 있는 권리를 포함한다.

이러한 프라이버시의 개념 변화는 유비쿼터스 환경에서 자신의 다양한 수요를 충족시키기 위해 일정한 목적 범위 내에서 자신을 공개하면서도

다른 한편으로는 자신의 행적을 타인의 권한 없는 관여로부터 보호해야 하는 필요성의 증가에서 출발하고 있다.

3. 디지털컨버전스 서비스 유형별 개인정보보호를 위한 침해유형별 분석

디지털컨버전스 서비스 유형별로 서비스 공통, 개별 침해요인을 도출하여, 신규서비스 가능성 분석을 시도한다.

3.1. 서비스 공통 · 개별 침해요인

디지털컨버전스 환경으로 접어들면서 사회는 새로운 신규 서비스와 신기술을 파생시키며 산업간, 산업 내의 빠른 융합현상을 보이고 있다. 그러한 가운데 개인정보는 다양한 사업자 간에 여러 목적으로 활용, 공유되게 되고 이는 프라이버시 침해라는 특성에 있어서도 몇 가지 새로운 요인을 낳고 있다. 기본적으로 개인정보 침해 요인은 현재까지의 침해 요인과 일맥상통하며 급격한 차이점을 보이지는 않는다. 그럼에도 불구하고 영상과 위치 정보의 발달, All IP 기반이라는 환경에 따른 개인정보 침해 요소는 눈에 띄는 부분이다. T-Commerce 이용으로 인한 인증, 결제 정보의 중요성은 더욱 커질 것으로 예상된다.

디지털컨버전스에서의 신규서비스는 서로 다른 프라이버시 침해 요인을 가지고 있기도 하지만, 공통의 침해요인도 찾아볼 수 있다. 정보의 생명주기별로 신규 서비스를 통합 분석하여 본 결과 다음과 같은 공통적인 침해요인이 발생되었다.

• 각 서비스는 정보의 수집 단계에서 사용자가 서비스에 가입할 때 필요이상의 정보를 요구하고, 서비스 제공을 미끼로 과도한 정보를 요구한다. 또한 동의나 충분한 고지 없이 개인의 정보를 제공하도록 강요하기도 한다.

• 개인의 정보를 저장하고 관리할 때에는 내부 직원에 의하여 개인정보가 유출되거나 변경될 수 있다. 또한 악의적인 외부인이 해킹, 악성코드, 스파이웨어등과 같은 불법적인 접근 방법을 이용하여 개인정보를 유출할 수 있다. 그리고 각 개인이 서비스를 이용하는 동안 이용자 자신도 모르는 사이에 이용자의 생활 패턴에 모니터링 되어 프라이버시가 침해되는 경우도 있다.

• 정보가 이용되고 제공되는 단계에서는 사용자가 서비스를 이용하는 사업자에게 동의하여 제공된 개인정보가 동의없이 사업자의 관련 사업자에게 무단으로 제공되거나 공유됨으로서 프라이버시 침해가 발생될 수 있다. 그리고 서비스 사업자별로 가지고 있는 개인정보들이 임의적으로 조합되어 사업자가 통계나 서비스의 질 향상을 위하여 이용되었던 중요하지 않은 개인의 정보들이 실제 개인을 식별할 수 있는 정보와 조합되어 개인의 사생활을 침해하는 정보들로 활용될 수 있다.

표 2. 서비스 공통/개별 침해 요인

서비스 구분	공통 침해 요인	개별 침해 요인
HSDPA/W-CDMA	**정보수집** - 가입시 필요 이상의 정보 요구 - 서비스 제공을 미끼로 한 과도한 정보 수집 - 부가서비스 임의 가입 권유	- 영상 정보에 대한 물리적인 관리 기준 - 영상정보+위치정보를 통한 개인 실시간 활동 모니터링
WiBro		- 쿠키에 의한 개인정보 수집 - 가지국과의 교신으로 인한 개별 정보 자동 생성
광대역 융합 서비스	- 동의 및 충분한 고지 없는 개인정보 수집 - 사용자가 인지하지 못하는 새로운 형태의 개인정보 생성 및 수집 **정보 저장 및 관리** - 내부직원에 의한 개인정보 유출 및 변경 - 외부인의 불법적 접근에 의한 개인정보 유출 - 메핑, 악성코드 등에 의한 개인정보 유출	- 쿠키에 의한 개인정보 수집 - 사용자의 조직 행위 정보가 STB 상에 저장, 기록 - IP망을 통한 광고 안내 및 구매 권유 - 미성년자 보호를 위한 식별의 어려움 - T-Commerce로 인한 인증, 결제정보 노출
DMB/DTV		- 위치정보와 결합된 동의하지 않은 정보 제공 - M/T-Commerce로 인한 인증, 결제정보 노출 - 구매 행위 모니터링으로 생활 패턴 분석
u-Home	- 이용자의 생활 패턴에 대한 모니터링 **정보 이용 및 제공** - 동의 없는 개인정보의 공유 및 무단 제공 - 개별 정보마리의 임의적 조합 및 활용 **정보 파기**	- 관리서버 또는 단지서버에 집중되는 방대한 개인정보 관리 체계 미비 - 원격검침, 홈뱅어 등과 같은 미인자 모니터링 - 다양한 관리 주체가 수집한 정보를 조합과 공유 - 서비스 제공시에 개인정보가 집중됨에 따른 정보 관학와 - T-Commerce로 인한 인증, 결제정보 노출
텔레매틱스	- 개인정보 삭제의 본인 확인 어려움 - 기기상의 개인정보 물리적 삭제 위험 및 복구 가능성	- 위치정보와 결합된 동의하지 않은 정보 제공 - 모니터링으로 개인의 위치 추적 가능 - 실시간 위치 정보 마케팅 수단으로 활용 - M-Commerce로 인한 인증, 결제정보 노출
RFID/USN		- 부적절한 RFID 정보의 접근과 수집 - RFID 정보를 활용한 개인의 행동 모니터링 노출 - RFID 인식 기술을 이용한 위치 정보 노출 - RFID 태그 정보를 활용한 광고 및 구매 권유
IT 서비스		- 존재하지 않음.

• 정보를 파기하는 단계에서는 서비스 이용 종료에 따라 개인정보 삭제를 요구하거나 개인정보를 삭제하였음에도 실제로 사업자의 데이터베이스에서 자신의 개인정보가 삭제되었는지 확인하기 어려운 문제가 있고, 개인이 이용하였던 단말기에 있는 개인정보를 삭제하였다 하더라도 단말기가 다시 유통되었을 때 개인정보를 복원하거나, 사용자가 알아차리지 못한 부분에서의 정보가 불완전하게 삭제되었을 위험이 있다.

각 서비스들은 위와 같은 공통적인 침해요인 이외에 서비스의 특성에 따라 개별적으로 개인의 프라이버시를 침해할 수 있는 요인들을 분석하면 다음과 같다.

• HSDPA/W-CDMA는 영상 서비스를 강조하면서도 영상정보에 대한 관리 기준이 아직 확실치 않다. 현재는 영상의 용량이 크다는 문제점으로 인해 저장의 비율이 높지 않지만 향후 영상 압축 기술이 발달하게 되면 영상정보에 대한 침해 문제가 이슈가 될 것이다. 따라서 이에 대한 관리 기준을 사전에 점검해야 할 필요성이 있으며 더불어 영상정보에 위치정보가 결합하여 개인 실시간 활동 모니터링이 가능해질 것이다.

• 와이브로는 그 특성상 쿠키에 의한 개인정보 수집이 가능하며 사용자가 이동하면서 와이브로를 사용할 경우, 가장 가까운 기지국과 계속적으로 교신이 발생함으로 이를 시간대별로 추적하면 경로 정보가 자동으로 생성되게 된다.

• 광대역 융합 서비스, 즉 IPTV는 IP가 기반이므로 쿠키에 의한 개인정보 수집이 가능하며 사용자가 리모콘을 사용하여 채널을 돌리거나 물건을 구매하는 등의 조작 행위 정보가 STB 상에 저장, 기록되어 개인의 취향 및 취미 정보가 수집 가능하다. 인터넷에서 팝업창으로 광고를 보여주듯 TV 상에서도 IP망을 통한 광고 안내 및 구매 권유가 발생할 수 있으며 이런 경우 미성년자에게도 무차별적으로 광고가 노출되거나 성인 인증이 필요한 화면이 보여질 수 있어 이에 대한 식별 기술과 보호 정책이 필요하다. TV를 통해 즉각적인 구매 행위가 발생하는 T-Commerce를 하는 과정에서는 인증 정보와 결제 정보가 노출되는 위험성이 여전히 존재한다.

• DMB/DTV 서비스는 이동 중 위치 정보에 의한 개인이 인지하지 못하거나 혹은 동의하지 않은 정보가 제공될 수 있으며 서비스 이용 과정에서 물건을 구매하는 등의 행위가 가능함으로 인증, 결제 정보에 대한 노출 위험성이 있다. 이러한 구매 행위를 일정 기간 이상 모니터링 할 경우 생활 패턴이 분석된다.

• u-Home은 침해 요인이 다양하게 발생할 수 있는데 무엇보다 관리서버 혹은 단지서버에 집중되는 방대한 양의 개인정보를 관리하는 체계가 미흡하여 통일된 기준을 갖고 있지 못하다. 원격검침, 홈뷰어 등과 같이 외부와 통신하는 서비스 사용시 모니터링되는 부분에 대한 사용자의 인식이 적으며 이를 다양한 관리 주체가 각각의 이해관계 하에 정보를 수집, 조합, 공유하는 문제가 발생한다. 특히나 u-Home 서비스 제공사(통신사)에 개인의 정보가 집중되어 정보 권력 현상이 일어날 수 있다. 서비스를 이용하기 위해서는 인증과정이 필수적이라 이에 대한 정보 노출시 크나큰 파급효과가 일어날 수 있으므로 철저한 사전 보안이 필요하다.

• 텔레매틱스는 위치 정보로 인한 침해가 가장 큰 부분을 차지한다. 이를 마케팅 수단으로 활용시 시와 때를 가리지 않는 광고가 발생하고 위치정보를 누적적으로 저장시 개인의 사생활 이동 경로가 노출된다.

• RFID/USN은 부적절한 방식으로 RFID 정

보의 접근과 수집이 발생하거나 RFID 정보로 인해 개인이 어떠한 물품을 소유하고 있는지 실시간으로 파악이 가능하다. 태그 인식을 통해 위치 정보가 노출됨은 물론, 개인이 소유한 물품과 비슷한 성격의 물품을 광고하거나 구매를 권유하는 등의 사생활 침해가 발생될 수 있다.

지금까지 설명한 디지털컨버전스 상에서의 신규 서비스에 대한 프라이버시 침해 요인을 토대로 공통 침해 요인을 제거하고 개별 침해 요인을 각기 서비스별로 제어하는 과정이 필요하다.

3.2. 디지털컨버전스 신규 서비스 가능성 분석 및 우선순위 도출

디지털컨버전스 신규 서비스는 각 서비스를 독립적인 관점으로 발전시켜왔다. 이용자 측면에서 신규 서비스는 일상생활과 함께 존재하는 서비스이다. 따라서 신규 서비스는 이들 서비스 각각에 이용자의 상황을 맞추기 보다는 이용자의 상황에 따라 신규 서비스가 적절히 융·복합되어 통합서비스 형태로 제공된다. 디지털컨버전스 신규 서비스는 각각의 독립적인 서비스들 사이에서 각각 다른 신규 서비스와의 연계 및 통합을 통해 부가적인 기능의 생산과 가치를 높이고 있다. 다음의 [표3]은 현재 제공되고 있는 서비스들 중에서 각각의 신규 서비스가 융합되어 있는 현황을 보여주고 있다.

표 3. 서비스 융합 현황

	HSDPA	와이브로	IPTV	DMB	u-Home	텔레매틱스
RFID	×	×	×	×	○	○
텔레매틱스	○	○	×	○	×	
u-Home	○	○	○	×		
DMB	○	○	×			
IPTV	×	×				
와이브로	○					

현재 서로 융합되어 서비스되고 있거나 앞으로 서비스될 예정인 서비스들 이외에 신규 서비스의 통합 가능성을 분석하고 새로운 통합 서비스 대안을 끌어내기 위해 표 4와 같이 신규서비스들을 정보수집기능, 정보전달 매체기능, 응용서비스 기능으로 분류하였다. 정보수집기능을 가진 서비스는 RFID/USN 서비스, 텔레매틱스 서비스, 와이브로 서비스, W-CDMA 서비스가 있다. 정보전달 매체기능에 해당되는 서비스는 와이브로 서비스, W-CDMA 서비스, DMB/DTV 서비스, IPTV 서비스가 있다. 응용서비스로는 홈네트워크 서비스, 텔레매틱스 서비스, DMB/DTV 서비스, IPTV 서비스가 있다.

실제로 신규 서비스를 이용하는 사용자 입장에서는 응용서비스를 사용할 때 정보수집기능이나 정보전달 매체 기능이 필수로 요구되기 때문에 두 기능에 해당되는 서비스들은 응용서비스를 사용하기 위한 수단의 역할을 하게 된다. 따라서 홈네트워크나 텔레매틱스 서비스와 같은 응용서비스에 속한 서비스들은 상황에 따라 정보수집기능에서 속한 서비스와 정보전달 매체기능에 속한 서비스와 적절히 융합될 수 있다. 융합 가능한 서비스들은 다음과 같다. 그리고 이중에서 융합도가 높은 서비스들은 앞 내용에 근거하여 홈네트워크와 텔레매틱스가 되고, 침해우선순위가 높은 것들도 앞의 내용에 근거하여 홈네트워크와 텔레매틱스가 된다.

표 4. 신규 서비스 기능별 분류

기능	신규 서비스
정보 수집 기능	RFID/USN, 텔레매틱스, W-CDMA/HSDPA 와이브로,
정보전달 매체기능	와이브로, W-CDMA/HSDPA, DMB/DTV, IPTV
응용서비스 기능	홈네트워크, 텔레매틱스, DMB/DTV, IPTV

4. 결 론

위에서 언급되어진 신규서비스는 현재 시점활용하거나 혹은 예견할 수 있는 서비스이기 때문에, 디지털컨버전스가 발전해 나가면서, 새로운 융복합화에 의하여 더 많은 서비스가 제공되어질 것이다. 디지털컨버전스 시대는 유비쿼터스 단계가 되면서 한 차원 진일보한 서비스가 가능할 것인데, 유비쿼터스의 궁극적인 목적인 언제 어디서나 이용자에게 맞추어진 컨버전스 서비스를 제공하는 상호작용 프로세스에서, 가장 중요하게 언급되어지는 정보보호는 흔히 생각하는 것처럼 기술만으로 해결될 수 있는 문제가 아니다.

정보보호는 관리와 정책, 그리고 기술이 결합하여 있는 유기체라고 할 수 있다. 아무리 완벽한 기술적 대책을 운영하고 있는 조직이라도 구성원이 정보를 누출하면 기술적 정보보호 대책은 아무런 의미가 없게 된다. 정보보호의 구현 링크 중에서 사람으로 구성된 링크가 가장 약한 링크라는 말은 이를 두고 하는 말이다. 이러한 취약점 사례가 관리적 차원의 정보보호 대책이 필요한 이유이기도 하다.

조직에 대한 상시 정보보호 대책 중 대표적인 제도는 한국정보보호진흥원이 시행하고 있는 '정보보호관리체계 인증'이다. 이는 정보보호 정책 및 조직, 취약성 분석, 대책 마련, 사후 관리 조치 등이 객관적인 기준에 만족하는지 제삼자가 보증해주는 제도다. 이를 위한 기준은 ISO/IEC JTC1 국제표준화기구에 의하여 국제 표준이 개발되었고, 주요 선진국이 이 제도를 적극적으로 도입, 적용하고 있다.

흔히들 정보보호는 사후의 문제라고 주장하는 사람이 있다. 우선 새로운 신규 서비스의 제공이 중요하고 그 다음에 서비스가 어느 정도 성숙하고 나면 정보보호 대책을 세워도 늦지 않다고 주장한다. 이러한 주장은 분명히 문제가 있다. 대부분의 정보통신 및 디지털컨버전스 관련 기술을 표준화하고 있는 IETF나 ITU-T 등의 주요 표준화 기구에서는 앞으로 정보보호 문제가 고려되지 않은 어떤 기술 표준도 절대로 표준이 될 수 없다고 분명히 선언하고 있다. 이것은 디지털컨버전스의 진화를 거듭하고 있는 현 시점에서, 소비 생태계라고도 불리워지는 이용자와 생산자 간의 상호작용 프로세스에서의 개인정보보호의 중요성을 강조하고 있는 것이다.

이를 위해서는 다양한 대응책이 논의 되어져야 하며, 생체정보인증시스템, Security Framework 구축등 안전한 인증체계에 관한 연구가 병행되어져야 할것이다.

참 고 문 헌

[1] 디지털융합연구원, 디지털컨버전스전략, 2005.
[2] e-러닝 백서, 산업자원부,한국사이버교육학회, 2003.
[3] LG 경제연구원, "디지털 컨버전스에 따른 뉴 트렌드," 2004.
[4] 이승욱 외, "e-learning 기술동향:시장에서 필요한 기술을 중심으로," 전자정보센터, 2004.
[5] 조성윤외, "통신.방송융합에 따른 디지털콘텐츠 산업활성화 전략연구," 한국소프트웨어진흥원, 2004.
[6] 이경남, "디지털TV, 정보통신산업동향 II," KISDI, 2003.
[7] 윤종룡. "초일류로 가는 생각," 삼성전자, 2004.

문 남 미

- 1998년 이화여자대학교 컴퓨터공학 박사
- 1999년~2000년 아주대학교 디지털미디어학과 조교수대우
- 2000년~2003년 이화여자대학교 인터넷멀티미디어연구센터장/연구교수
- 2003년~현재 서울벤처정보대학원대학교 부교수
- 2000년~2005년 멀티미디어학회 이사
- 2000년~현재 디지털콘텐츠학회 이사
- 2000년~현재 방송공학회 이사
- 현 재 한국이러닝학회 명예회장
- 관심분야 : u-learning, MPEG, 디지털방송, IPTV, CT, 개인정보보호, T-Commerce

용 승 림

- 2006년 이화여자대학교 과학기술대학원 박사졸업 공학박사
- 2006년 현재 이화여자대학교 컴퓨터공학과 전임교수
- 관심분야 : 정보보호, 디지털 콘텐츠 보호, 암호 이론, 생체정보 보안

오 정 민

- 2002년 숙명여자대학교 경영학과 졸업
- 2006년 현재 서울벤처정보대학원대학교 디지털미디어 석사과정
- 관심 분야 : u-city, CT, 디지털비즈니스모델링, 정보보호

조 태 남

- 1988년-1996년 한국전자통신연구원 선임연구원
- 2004년 이화여자대학교 컴퓨터학과(박사)
- 2004년-2005년 이화여자대학교 컴퓨터학과 전임강사
- 2005년-현재 우석대학교 정보보안학과 조교수