情 報 保 護 學 會 誌
第 16 卷 第 3 號, 2006. 6

유비쿼터스 환경에서 개인정보보호의 기술동향

송 유 진*, 이 동 혁**, 남 택 용***, 장 종 수****

요 약

최근 유비쿼터스 컴퓨팅이 주목받고 있다. 향후 유비쿼터스 환경으로 기술과 비즈니스의 접목, 그리고 컨버전스에 의한 새로운 패러다임이 형성될 것이며, 사용자에 대한 인비저블(Invisible)형태의 편재된 컴퓨팅 서비스가 제공될 것이다. 그러나 이러한 서비스 제공을 위해서는 필수적으로 사용자의 개인정보가 요구되며, 이에 따른 개인정보 침해에 대한 우려가 점차 부각되고 있다. 본 논문에서는 유비쿼터스 환경에서 개인정보에 대한 국내외 및 시장동향을 살펴보고, 현재 연구개발되고 있는 개인정보보호 기술 및 프로젝트 동향을 살펴본다.

Ⅰ. 서 론

유비쿼터스 환경에서는 모든 사람들이 자신의 의지와는 상관없이 항상 네트워크 공간에 놓이게 된다. 유선과 무선을 통합한 유비쿼터스 컴퓨팅 시대에서는 사용자의 모든 모습들을 계속 감시하고 분석하며 실시간으로 개인정보를 계속 전송할 수 있다. 이러한 유선과 무선사용 환경에서 개인 정보활동이 증가함에 따라 개인정보 노출이 심해지고 불법 취득도 많아질 것이 예상된다. 이와 같이, 개인정보의 부적절한 노출로 인한 개인정보 침해 문제는 유비쿼터스 컴퓨팅의 순기능적 효과를 반감시키는 요인이 될 수 있으며 지금까지의 네트워크에서 생각하는 개인정보보호의 상식을 크게 바꿀 수 있다.

1. 국내외 동향

1.1 국 내

최근 국내에서는 개인정보 침해에 대한 우려가 점차 부각되고 있으며 이에 대한 활발한 논의가 진행되고 있다. 우리나라는 세계 첨단의 정보통신기반을 갖추고 있으나 이에 합당한 개인 프라이버시 보호를 위한 법제도적 인프라와 문화적 환경의 부족으로 개인정보 보호 수준은 매우 뒤떨어져 있는 것이 현실이다.

그러나 2001년 개정한 개인정보보호를 위한 법률 등으로 개인정보의 수집, 이용, 보관에 관한 내용을 규정하고 있으며, 최근 국내를 떠들썩하게 했던 도청사건을 계기로 통신비밀보호법의 공백과 약점을 입법적으로 보완해야 한다는 목소리가 크다. 아울러 국회에 상정된 개인정보보호기본법(안)의 제정을 서두르는 것이 시급하다.

개인정보보호기본법(안)의 입법추진을 통해 일관성 있는 개인정보보호원칙의 확립, 개인정보영향평가의 실시 및 개인정보보호기구의 설립 등을 논의하고 최근의 주민등록번호 오남용에 대한 대책으로써 주민등록번호 대체 인증 수단에 대한 논의도 이루어져야 할 것이다.

이러한 요구에 부응하기 위해 정보통신부는 최근 중장기정보보호로드맵을 발표하였다.[30] 로드맵에서는 향후의 유비쿼터스 환경하에서 발생할 수 있는 여러 가지 프라이버시 침해 문제에 대한 법제도적, 기술적 대책을 프라이버시 보호체계에 대한 가이드라인으로써 제시하고 있다.

ETRI는 중장기정보보호로드맵상의 프라이버시 보호체계를 조기에 구축하기 위해 유비쿼터스 환경에서 필수적인 개인정보보호 기술을 연구중에 있다.

또한, 한국통신(KT)가 최근 사회적인 이슈가 되고 있는 인터넷상의 무분별한 개인정보 노출을 효과적으

* 동국대학교 전자상거래학과 교수(song@dongguk.ac.kr)
** 동국대학교 대학원 전자상거래학과(jazzbop@korea.com)
*** ETRI 개인정보보호연구팀 팀장(tynam@etri.re.kr)
**** ETRI 네트워크보안그룹 그룹장(jsjang@etri.re.kr)

로 막을 수 있는 P3P(Platform for Privacy Preferences)를 도입하여 개인정보 보호 클라이언트용 에이전트 솔루션 개발에 착수해 연내에 이를 시범 적용할 계획이다.[18]

1.2 국 외

OECD는 이미 1980년에 "개인정보의 국제유통과 프라이버시 보호에 관한 가이드라인"을 제정하여 회원국들에게 개인정보의 보호와 유통에 대하여 권고하고 있으며, 유럽연합은 EU 수준의 개인정보 보호를 시행하지 않는 국가와의 교역에서 불이익을 주는 문제를 적극 검토하고 있다.

미국 아리조나 주에서는 2005년 1월 인터넷을 비롯하여 우편물 등에서 SSN (Social Security Number, 사회보장번호) 사용을 제한하는 내용을 골자로 하는 법을 발효하였다.

일본은 2005년 4월부터 5000명 이상의 고객정보를 보유하고 있는 모든 기업은 개인정보에 대한 활용 범위를 고지하고 개인정보관리를 위한 인적, 물리적, 기술적 체계를 갖추어야 하도록 명시하는 개인정보보호법을 제정하고 있다.

현재 각국에서는 RFID를 비롯한 유비쿼터스 컴퓨팅 환경을 중심으로 개인 프라이버시 침해 방지와 관련된 연구가 진행되고 있다.[3,4,6,7,11-13]

2. 시장 및 산업동향

국내 정보보호 시장규모는 2005년 3,182억 규모로, 연평균 10.7% 성장하여 2009년에는 4,383억원으로 성장할 전망이다. 개인 정보보호 시장은 안티바이러스/안티스팸 시장의 50%, 정보보호 S/W의 약 20% 수준을 차지하는 것을 가정할 때, 2005년에 812억원, 2009년 1,213억원 규모로 성장 예상되며, 향후 유비쿼터스 관련 개인 정보보호의 보급으로 급격한 성장이 전망되고 있다.[31]

정보보호 산업의 수출시장도 2005년 213억원 수준으로, 연평균 17.7% 성장이 예상된다. 개인 정보보호 시장은 안티바이러스/안티스팸 시장의 50%, 정보보호 S/W의 약 20% 수준을 차지하는 것을 가정할 때, 2005년에 57.4억원 규모로 성장이 예상되며, 유비쿼터스 기술의 보급과 개인정보 보호를 위한 안티바이러스/안티스팸 시장의 증가를 고려할 때 급격한 수출 성장이 이루어질 전망이다.[31]

한편, 애버딘그룹(Aberdeen Group)은 ID절도로 인한 경제적 손실이 2003년 한해에만 전세계적으로 약 2,210억 달러에 이를 것으로 전망했으며 그 피해가 연평균 300%로 증가하면서 2005년에는 2조달러에 이를 것으로 전망하고 있다.[15]

II. 개인정보보호 기술 동향

현재, 개인정보를 보호하기 위한 여러 가지 법제도적 대책과 기술이 연구개발되고 있다.[1,2,14,15,20-22,24,26]

본 절에서는 기존의 프라이버시 침해기술과 보호기술에 대해 요약한다.

1. 프라이버시 침해 기술(PIT, Privacy Invading Technology)

1) TCP/IP 주소 : TCP/IP 주소의 분배 및 관리 체계 특성 때문에, 인터넷 이용 시 TCP/IP 주소를 추적하여 이용자 신원을 확인하는 것이 용이함
2) 도메인 네임 : E-mail의 출처를 확인하는 것은 매우 간단하며, 누구나 ISP 정보와 e-mail 이용자의 ID를 알 수 있음. ISP는 이용자의 ID를 이용하여 이용자의 계정을 확인
3) Processor Serial Number (PSN) : Intel사는 자사가 개발하는 Pentium III 칩에 고유의 프로세서 일련 번호(serial number)를 부여하여, 인터넷에 접속하는 특정 컴퓨터의 이용자의 신원 정보와 연결시켜 전자상거래에 있어서 인증 목적으로 이용
4) IPv6 : IPv6의 계획은 인터넷상의 모든 장치에 고정된 주소를 할당 하는 것으로, IPv6의 새로운 주소는 하드웨어 속에 내장될 것이고, 추적 가능한 정보를 포함하게 됨. 이것은 마치 영구적인 쿠키를 심는 것과 동일한 개념임.
5) 쿠키(cookie) : 쿠키 파일을 이용하여 인터넷 이용자의 신원을 쉽게 파악 할 수 있음. 두 가지 방식으로, 첫째, 쿠키는 로그인 정보(예컨대, 이름, 주소, 비밀번호 등)를 불러내는 데에 사용될 수 있다. 둘째, 쿠키에 담긴 정보와 마케팅 데이터베이스에 있는 이용자의 이름, 주소, 이전의 소비정보 등을 상호 비교함으로써 이용자의 신원 확인 가능.
6) 웹 버그(Web bug) : 웹 버그는 온라인 이용자가 모르는 사이에 이용자에 관한 정보를 유출 해가거나 심지어 이용자의 시스템을 파괴 할 수도 있는 기술임. 웹 버그는 Web Page에 심어 놓은 매우

작은 그래픽이미지 파일로, 통상 해당 Web Page의 바탕화면과 같은 색을 지니기 때문에 육안으로는 거의 보이지 않음.

7) 스파이웨어(spyware) : 무료 또는 유료로 배포되는 소프트웨어에 들어 있는 일종의 프로그램 모듈을 통칭하는 것으로, 해당 소프트웨어를 설치한 컴퓨터 이용자가 인터넷을 서핑 할 때 이용자의 개인정보나 온라인 활동 정보를 스파이웨어를 설치한 회사의 서버에 지속적으로 전송하는 것이 주된 기능임.

8) 고성능 스파이웨어(sophisticated spyware) 기술 : 스파이웨어 기법이 한 단계 진보한 기법으로, 스파이웨어를 탐지하기 위해 사용되는 백신이나 안티 스파이웨어 솔루션 등을 우회하기 위해, 스파이웨어를 통해 수집된 정보를 작은 크기로 나누어 컴퓨터의 파일 시스템상에 보이지 않는 틈새 공간(slack space)에 임시 저장한 다음, 특정 시간대에 내외부의 특정인에게 전송하는 방법을 이용함. 이러한 기법은 정부의 수사기관에서 범죄자의 감시 및 경쟁사에 대한 정보수집, 국가간첩 정보 수집에 이용된 사례가 있음.

9) WLAN 환경 : WLAN 사용자가 액세스 포인트에 접속할 때, 해커가 가상의 액세스 포인트를 이용하여 사용자의 중요한 개인정보를 모니터링

10) 웹메일의 첨부 파일 유출 : 웹메일 첨부파일 유출 기법은 기존 e-mail이나 웹메일을 모니터링하여 데이터를 유출하는 방식에서 한 단계 진화하여, 웹메일에 첨부된 파일을 encoding하는 방식으로 주로 기업이 운용하는 메일 모니터링 프로그램을 우회하여 기밀 정보를 유출하는데 사용됨.

11) Steganography : 이미지 및 오디오 파일에 중요한 파일이나 메시지를 첨부할 수 있는 스테가노그래피 기법이 확산 될 전망이다. 이 기법은 오사마빈라덴이 알카에다 조직원과의 연락을 위해 사용된 것으로 보고되면서 널리 알려짐.

12) 접속세탁(connection laundering) : 접속세탁 기법은 해커들이나 해커 그룹간 공간 창조를 통해, 해커 역추적 경로 파악을 어렵게 만드는 것으로, 해커가 여러 국가를 경유하여 해킹을 할 경우, 중간 단계에 해커 그룹이 운용하는 가명경로(anonymizer)를 거쳐 해커에 대한 역추적이 불가능하게 하는 방법임.

〔표 1〕 프라이버시 침해 기술 요약

침해 기술	방 법
TCP/IP 주소	인터넷 이용시 TCP/IP주소를 추적하여 이용자 신원 확인
도메인 네임	E-mail의 출처를 통하여 ISP 정보와 e-mail 이용자의 ID확인
Processor Serial Number	고유의 프로세서 일련 번호(serial number)를 통하여 인터넷에 접속하는 특정 컴퓨터에 대한 이용자의 신원 정보와 연결
IPv6	IPv6는 고정된 주소가 할당되며 추적 가능한 정보를 포함한다.
쿠 키	쿠키 파일을 이용하여 인터넷 이용자의 신원을 쉽게 파악 가능
웹 버그	온라인 이용자가 모르는 사이에 이용자에 관한 정보를 유출 해가거나 심지어 이용자의 시스템을 파괴 할 수도 있는 기술
스파이웨어	해당 소프트웨어를 설치한 컴퓨터 이용자의 개인정보나 온라인 활동 정보를 스파이웨어를 설치한 회사의 서버에 지속적으로 전송
고성능 스파이웨어 기술	스파이웨어를 통해 수집된 정보를 분할하여 틈새공간(slack space)에 임시 저장한 다음, 특정 시간대에 내외부의 특정인에게 전송
WLAN 환경	WLAN 사용자가 액세스 포인트에 접속할 때, 해커가 가상의 액세스 포인트를 이용하여 사용자의 중요한 개인정보를 모니터링
웹메일의 첨부 파일 유출	웹메일에 첨부된 파일을 encoding하는 방식으로 주로 기업이 운용하는 메일 모니터링 프로그램을 우회하여 기밀 정보를 유출하는데 사용
Steganography	이미지 및 오디오 파일에 중요한 파일이나 메시지를 첨부
접속세탁	접속세탁 기법은 해커들이나 해커 그룹간 공간 창조를 통해 해커에 대한 역추적이 불가능하게 하는 방법
위치측정 정보 침해	GPS 또는 휴대전화기의 위치 측정 내용을 인터넷을 통해 확인 할 수 있게 되어, 개인의 위치 정보 유출 가능

13) 위치측정 정보 침해 : GPS 또는 휴대전화기의 위치 측정 내용을 인터넷을 통해 확인 할 수 있게 되어, 개인의 위치 정보가 유출되어 개인의 신변에 위협이 될 수 있음

2. 프라이버시 보호 기술 (PET, Privacy Enhancing Technology)

1) P3P (Platform for Privacy Preference) : P3P는 W3C(World Wide Web Consortium)에서 개발한 개인정보보호 표준기술 플랫폼으로서 웹사이트에서 이루어지는 데이터 처리에 관한 표준을 제시하고 있음. P3P의 목표는 웹사이트 운영자에게 이용자 자신의 정보를 관리 할 수 있는 권한을 넘겨주는 것이며, 이용자 정보가 잘못된 방법으로 사용되지 않도록 보호하기 위해 만들어졌음.
2) 프라이버시 정책 생성(Privacy Policy Statements Generator) : OECD가 1980년에 발표한 "프라이버시 보호 및 개인 정보의 국가간 유통에 관한 지침"에 따라 개발되었고, 프라이버시 정책 문구를 자동적으로 생성하는 기능을 가지고 있음. 특히, 정보보호 생성 소프트웨어가 요구하는 절차에 따라 실제 운영중인 개인정보 보호방침을 입력하면, 해당 기업이나 조직의 개인정보 보호방침 문구를 HTML 문서로 자동 작성하여 출력하는 기능을 갖고 있음.
3) 쿠키 관리(통제) : 이용자로 하여금 언제 쿠키가 자신의 컴퓨터에 저장되는지를 결정하게 함으로써 쿠키의 수용 여부를 결정하고 관리하도록 하며, 개별적인 쿠키에 저장된 정보가 무엇인지를 판단 할 수 있는 방법으로, 개인에게 자신의 컴퓨터에 저장된 쿠키에 대해 통제권을 주는 방법임.
4) 암호화 소프트웨어(Encryption Software) : 암호화 소프트웨어는 암호화를 통해 자신의 전자메일 메시지, 저장된 파일, 그리고 온라인에서의 커뮤니케이션을 보호할 수 있게 하는 기능을 제공함. 한번 암호화가 이루어지면 오직 그 당사자만 암호화된 정보에 대한 디지털 키를 가지고 그 정보를 열람하며, 디지털 키는 브라우저, 생체인증, 스마트 카드등과 결합하여 생성됨.
5) 익명화(Anonymizers) 기술 : 익명화는 클라이언트와 웹사이트간에 중개자 역할을 수행함으로써 이용자가 익명으로 웹을 서핑하도록 하는 서비스를 제공함. 일반적으로 익명화 서비스는 웹사이트가 방문객의 IP 주소를 식별하거나 쿠키를 개인의 컴퓨터에 저장하는 것을 막아줌으로, 소비자가 웹을 브라우징 하거나 보내는 이가 누구인지 알 수 없도록 익명화된 메일을 보낼 때 유용함. 그러나 이러한 기능은 반대로 개인화된 서비스나 온라인 계정관리, 과거의 구매기록 보관 또는 열람 등에 대한 특정한 기능을 사용할 수 없게 함.

Ⅲ. 개인정보보호 주요 기술 동향

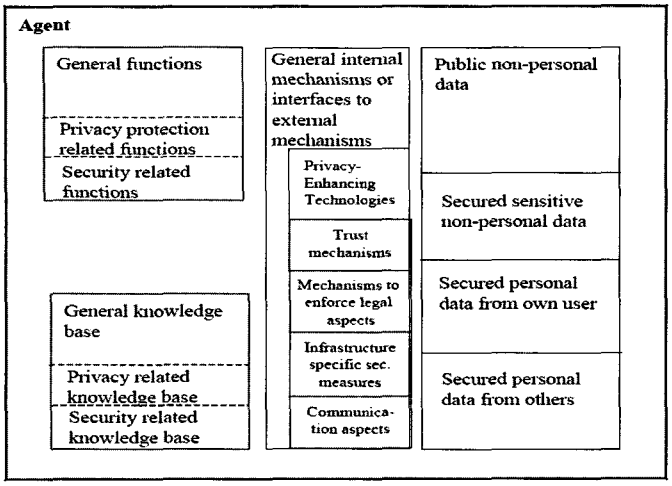
1. PISA

1.1. 개요

2001년에 시작된 PISA(Privacy Incorporated Software Agent) 프로젝트는 네트워크 환경에서 개

〔표 2〕 프라이버시 보호 기술 요약

보호 기술	방 법
P3P	P3P는 W3C(World Wide Web Consortium)에서 개발한 개인정보보호 표준기술 플랫폼으로서 웹사이트에서 이루어지는 데이터 처리에 관한 표준을 제시
프라이버시 정책 생성	OECD가 1980년에 발표한 "프라이버시 보호 및 개인 정보의 국가간 유통에 관한 지침"에 따라 개발되었고, 프라이버시 정책 문구를 자동적으로 생성하는 기능을 가지고 있음.
쿠키 관리(통제)	이용자로 하여금 언제 쿠키가 자신의 컴퓨터에 저장되는지를 결정하게 함으로써 쿠키의 수용 여부를 결정하고 관리하도록 하며, 개별적인 쿠키에 저장된 정보가 무엇인지를 판단하는 방법
암호화 소프트웨어	암호화 기술을 통해 자신의 전자 메일 메시지, 저장된 파일, 그리고 온라인에서의 커뮤니케이션을 보호할 수 있게 하는 기능을 제공함.
익명화 기술	클라이언트와 웹사이트간에 중개자 역할을 수행함으로써 이용자가 익명으로 웹을 서핑하도록 하는 서비스를 제공



〔그림 1〕 PISA의 Agent 구조

인정보 유출 없이 사용자를 대신하여 복잡한 업무를 수행하는 지능형 소프트웨어 에이전트 모델을 구축하는 프로젝트이다. 즉, 사이버 공간에서 찾고자 하는 데이터의 정확한 수집을 사용자 대신에 지능적으로 수행할 수 있는 에이전트인 지능형 소프트웨어 에이전트(ISA, Intelligent Software Agent)를 개발하는 것이다.

지능형 소프트웨어 에이전트는 복잡한 네트워크 환경하에서 사용자의 편의를 제공하기 위하여 독립적으로 작동하는 소프트웨어/하드웨어를 지칭한다. 여기에는 일반적인 개인 에이전트, 특정 작업을 수행하는 에이전트, 그리고 개인정보의 보호를 고려하는 서비스 에이전트 등 세 가지 종류의 ISA가 있다.

ISA는 자동화된 방식으로 업무를 처리하기 위해서 에이전트는 사용자의 개인정보를 소유하게 된다. 이는 ISA 기술이 프라이버시에 대한 중대한 위협이 된다는 것을 명백히 드러내고 있다. 따라서 ISA 개발 시 개인정보보호가 중요 과제로 간주되고 있다.

1.2. PISA의 구조

프라이버시에 대한 침해 공격으로부터 ISA를 보호하기 위하여 ISA에는 다음과 같은 부분이 필요하다. 〔그림 1〕

- 프라이버시 보호 관련 기능을 내장하고 있어야 하며, 이러한 프라이버시 보호 기능을 갖는 PET와 같은 메커니즘이나 인터페이스를 갖고 있어야 한다.
- 정책상의 노하우를 내장하고 있어야 하며 데이터 보호 지침에 따라 개인정보를 보호하기 위한 정책을 수행할 메커니즘을 갖고 있어야 한다.

ISA는 대상이 데이터 주체(Data Subject), Controller 혹은 Processor의 역할을 하는가에 따라 논리적으로 나뉘어 있다. 데이터 주체(Data Subject)는 Natural Person에 연관되며, Controller와 Process는 Natural Person과 Legal Person 모두 연관된다.

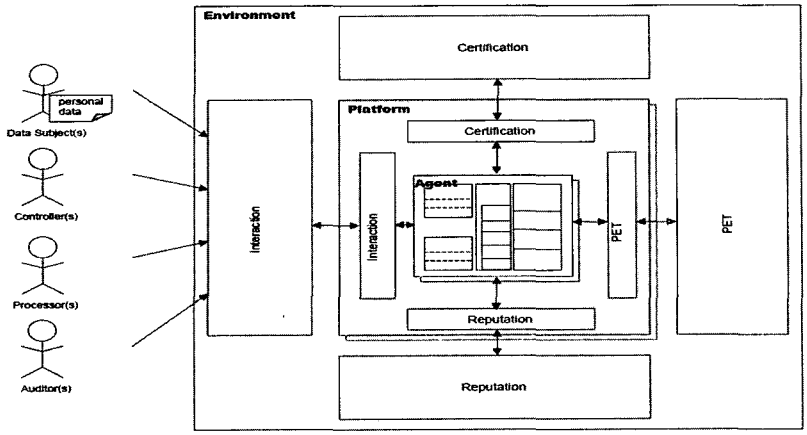
PISA에서 프라이버시 보호는 PET, 증명(Certification), 상호작용(Interaction), 평가(Reputation)의 조합으로 이루어진다. 이러한 내용을 그림으로 나타내면 〔그림 2〕와 같다. (〔그림 2〕의 Platform 내에 〔그림 1〕에서 언급한 Agent가 속해 있다)

1.3. 요소 기술

PISA 프로젝트는 네트워크 환경에서 개인정보 유출 없이 사용자를 대신하여 복잡한 업무를 수행하는 소프트웨어 에이전트 모델을 만들고자 하는 것이 핵심이다. 이를 위해서 PISA 프로젝트의 기본적인 모델은 다음과 같은 여러 발전된 기술을 통합하고 있다.

1) 에이전트 기술

에이전트는 주어진 업무를 수행할 때 실제로 능동적으로 정보를 수집해야 하는 인공지능 정보검색을 위한



〔그림 2〕 PISA 모델

소프트웨어이다. 예를 들어 에이전트는 영화의 장르나 영화에 나온 배우들을 기반으로 사용자가 좋아하는 영화가 무엇인지를 학습할 수 있어야 하며 실제적으로 사용자가 좋아하는 영화가 출시되었을 때 티켓을 구매할 수 있는 판단력을 가져야 할 것이다.

2) 데이터 마이닝

데이터 마이닝은 방대한 데이터베이스에서 이전에는 알려지지 않은 정보를 자동적으로 추출해내는 기술로써 개인정보보호에 반드시 필요한 기술 중의 하나이다. 웹상에서의 데이터 마이닝을 통해서 사람이 수행하기에는 많은 양의 웹 사이트가 분석되어지고 웹 사이트들로부터 노출되는 위험이 평가되어지며 개인정보 침해가 감지되어진다.

3) 암호화

개인정보보호 차원 뿐 아니라 업무내용의 기밀성을 위해서 데이터의 암호화가 필수적이다.

라. 시스템 설계기술

개인정보보호 관련 법률 및 표준을 실제로 구현하기 위해서 기술적 자문 역할을 하고 법적인 조건을 기술적으로 단계로 만드는 시스템 설계기술이 요구된다.

2. IBM Tivoli Privacy Manager〔5〕〔11〕

2.1. 개요

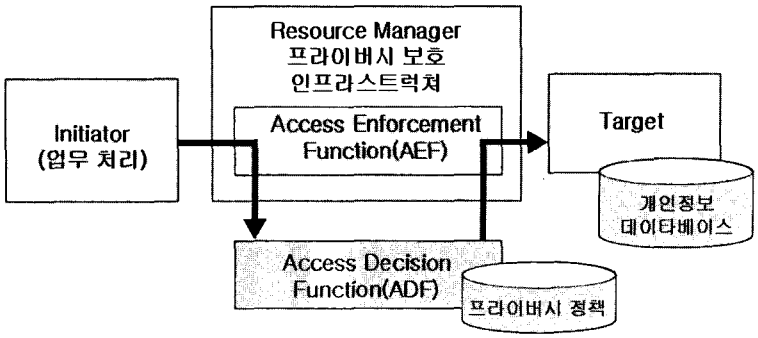
개인정보가 저장된 데이타베이스에의 접근제어를 미들웨어 등에 맡겨 접근제어 정책에 따라 검사하고 부정한 요구를 배제하는 예로서 ISO/IEC 10181-3에 의한 접근제어 모델을 검토한다〔그림 3〕.

개인정보에 대한 접근제어는 프라이버시 정책에 의한 동적인 판단을 필요로 한다. 동적인 접근제어 룰은 프라이버시·정책으로서 표현할 수 있고 이러한 정책을 적용시켜 접근의 가부를 판단한다.

* 프라이버시 정책: 개인정보보호 방침을 의미하는 것으로서, 개인정보 취득이나 보호에 관해 기업이 준수해야 할 체제나 각 기업 프로세스
* 프라이버시 스테이트먼트: 사용자에 대해 사이트상에서 개인정보의 수집, 처리 및 보존 방법에 대해 통지하기 위한 웹사이트상에서 기술된 성명문으로서 프라이버시 정책과 일치해야 한다.

국제 표준인 ISO 인가 모델의 「ISO/IEC 10181-3」에서는 이러한 접근제어 방식을 규정하고 있다〔그림 3〕. 이러한 접근제어 방식의 일례로서 「IBM Tivoli Privacy Manager for e-business」(이하, TPM)를 들 수 있다.

IBM TPM은 애플리케이션과 IT 시스템의 개인정보 보호 규칙과 데이터 처리 규칙을 추출하는 미들웨어를 제공함으로써, 이들 과제에 대처하도록 설계된 엔터프라이즈 개인정보 보호관리 솔루션이다. 이러한 방식에서 개인 정보 보호 관련 데이터는 수집하는 시점부터 정책과 연결되며, 이 데이터에 대한 사용 요청은 정책과 데이터 소유자의 설정에 따라 필터링 되어 허용되거나 거부된다.



〔그림 3〕 ISO/IEC 10181-3에 의한 접근제어 모델

데이터 사용에 대한 감사, 추적 기록을 자동으로 작성할 수도 있다. TPM을 이용해 기업은 자동화된 방식으로 개인정보를 관리할 수 있으며 개인 정보 관리 비용을 줄이고 권한 없는 사용자에게 정보가 노출될 위험을 완화시킬 수 있다.

이와 같이 TPM은 개개의 프라이버시 우선권에 따라 민감한 데이터에 접근하는 것을 제어하고 개인정보보호 정책을 어플리케이션에 결부하기 위한 혁신적인 프라이버시 미들웨어 솔루션이다. 이는 기업이 모든 IT 인프라 구조에 따라 개인정보보호 정책을 생성, 편집, 실시 그리고 중앙 관리하는 것을 가능케 하는 기업 전반적인 개인정보보호 정책의 뷰를 제공한다.

이러한 기술은 기업의 프라이버시 정책을 IT시스템에 구현하는 것으로 복잡한 프라이버시 관리 작업을 자동화해서 개인정보를 효율적으로 관리하고 프라이버시 준수에 수반하는 작업의 효율화를 지원하기 위한 것이다. 개인정보를 요구하는 프로그램이 개인정보 데이타베이스에 접근하는 경로상에 접근제어 기능을 삽입해서 프라이버시 정책과 결합시킴으로써 개인정보에 대한 부정접근을 감시 및 제어한다.

2.2. 시스템 구성

TPM은 〔그림 4〕과 같이 크게 두개의 컴포넌트인 Privacy Manager Server와 Privacy Manager Monitor로 나눌 수 있다.

Privacy Manager Server는 다음과 같은 기능을 제공한다.

- 프라이버시 정책을 정의
- 정책으로부터 IT자원을 맵핑
- 감사 추적을 생성
- 레포팅 툴을 제공

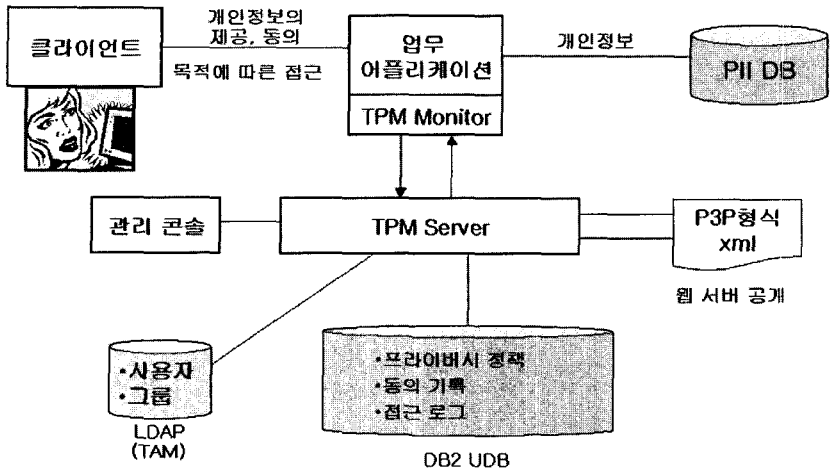
그리고, Privacy Manager Monitor는 프라이버시 매니저 서버와 어플리케이션 환경 사이에서 작용하며 다음과 같은 기능을 제공한다.

- 모니터할 저장 시스템의 데이터 스키마에 대한 습득과 이해
- 저장 시스템의 세부 항목 기록
- 감사를 위한 접근의 기록
- 정책을 기반한 접근에 대한 적합성 체크

이와 같이, TPM은 프라이버시 정책에 근거해서 개인정보 취급 목적별로 정의된 접근제어를 수행하도록 Privacy Manager Server(〔그림 3〕의 ADF)와 Privacy Manager Monitor(〔그림 3〕의 AEF)의 기능에 의해 접근을 감시, 제어한다.

Privacy Manager Server는 Privacy Manager Monitor로부터 받은 개인정보에의 접근 제어 정보에 의해 프라이버시 정책에 적합한지를 판단하여 접근 가부를 결정한다.

Privacy Manager Monitor는 개인정보에 접근하는 어플리케이션 프로그램에 내장되어 개인정보 접근이 발생했을 때 Privacy Manager 서버에의 접근 가부 판단을 문의해서, 판단 결과를 어플리케이션 프로그램에 응답한다. 이러한 접근 기록에 의해 종래의 DBMS(Database Management System : 데이타베이스관리시스템)의 기능만으로는 곤란함, 읽기를 포함한 데이타베이스에의 문의 결과를 본인의 동의의 유무, 접근제어 정책의 검사 결과, 데이터의 이용자 정보와 함께 취득할 수 있다.



〔그림 4〕 TPM 구성

2.3 주요 기능

Tivoli 소프트웨어의 주요 기능은 다음과 같다.

- IT 인프라 전반에 대해 개인정보보호 정책을 적용한다.
- 개인정보보호 정책을 일반적인 문장으로부터 P3P (Platform for Privacy Preferences) 형식으로 변환한다.
- 정책을 작성하고 관리할 수 있는 사용하기 쉬운 자연 언어 인터페이스를 제공한다.
- 개인 정보 접근을 모니터링하고 상세한 감사 로그 기록을 작성한다.
- 전사적으로 정보를 공유할 수 있도록 통지 및 동의 개인 설정을 관리한다.
- 기업 정책 준수를 상세하게 설명하는 보고서를 자동으로 작성한다.

3. NTTCom〔12〕

개인정보를 저장하고 있는 시스템에 누군가의 침입이 있을 때 개인정보가 파괴되고 개인의 프라이버시 침해로 이어지며 또 파괴된 개인정보 DB를 복원하기에는 많은 비용과 시간이 필요하다.

NTTCom의 기밀정보 보관서비스는 비밀정보 분산 기술에 의해 기밀성을 유지함으로써 안전한 개인 기밀정보의 저장이 가능하고 암호화, 전자서명의 약점(시간이 흐르면 해독될 우려) 을 극복하고 안전하게 장기간의 보관을 낮은 비용으로 구현하고 있다.

주요 기능은 다음과 같다.

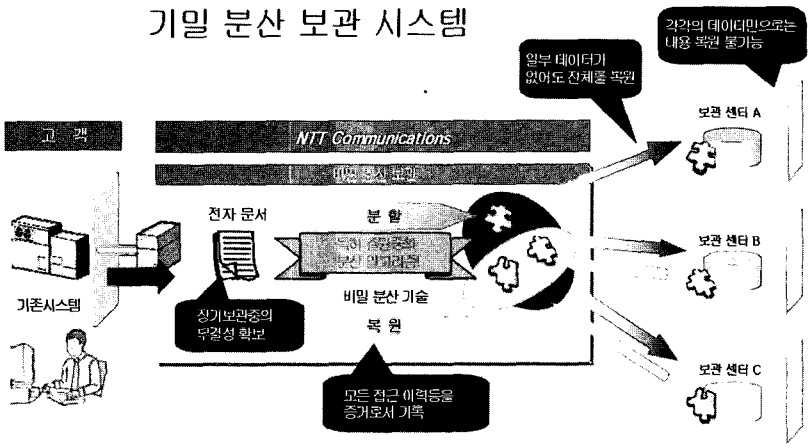
- 오퍼레이터도 내용을 모르는 은닉 저장으로 정보 누설을 방지
- 장기간에 걸쳐 데이터의 원본성(무결성)을 확보하여 안전하게 저장하는 것이 가능
- 데이터를 분산 보관함으로써 재난에 대한 복구 가능
- 모든 접근이력을 감사 증적으로서 기록하고 있어 일련의 처리의 정당성을 장기간에 걸쳐 검증 및 설명이 가능
- 분산된 개인정보 3개의 데이터 가운데 2개를 결합하지 않으면 원래의 정보의 복원은 불가능. 하나를 분실해도 정보 누설은 되지 않으므로 안심하고 유통할 수 있음. 그리고 전용 사이트로부터 분실한 데이터를 무효화하는 것도 가능

NTT Com.의 기밀정보 보관서비스 구성도는 〔그림 5〕와 같다.

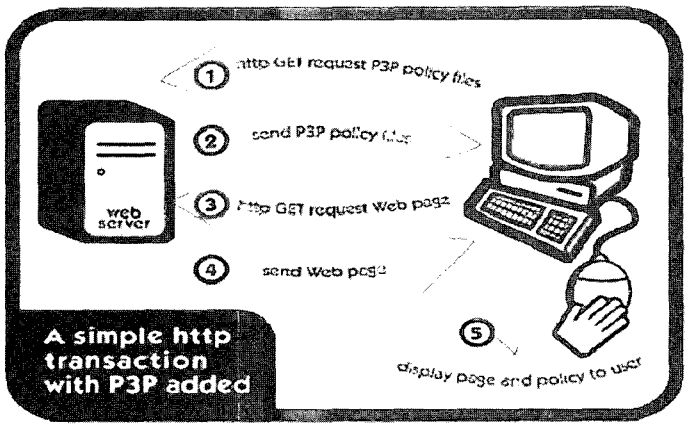
4. P3P〔7,14〕

4.1. 개요

P3P는 국제 웹 표준화 기구인 W3C가 웹사이트 이용 시 프라이버시를 보호하기 위해 정한 표준 기술 플랫폼으로, 사용자 PC의 웹 브라우저에 설치된 에이전트가 자동으로 사용자의 개인정보 보호정책과 서비스 제공업체의 개인정보 사용정책을 비교해 약관 동의 여부 등을 결정하는 방식이다. 이에 따라 사용자가 이용하는 서비스 종류에 따라 개인정보 노출 수위를 조절하는 것은 물론, 자신의 정보가 서비스 제공자나 제



〔그림 5〕 기밀정보 보관 서비스 구성도



〔그림 6〕 P3P 구현 과정

3자에게 어떤 목적으로 사용되는지를 쉽게 알아볼 수 있는 것이 장점이다.

P3P의 목표는 웹사이트 운영자에게 이용자 자신의 정보를 관리할 수 있는 권한을 넘겨주는 것이며 이용자 정보가 잘못된 방법으로 사용되지 않도록 보호하기 위해 만들어 진 것이다. 따라서 P3P의 기능은 웹 브라우저나 다른 사용자 도구로 하여금 자동적으로 해당 웹사이트의 프라이버시에 관한 정보를 읽고 사용자가 이미 설정해 놓은 정보공개 수준과 비교하여 정보를 선별적으로 제공함으로써 어떠한 때에 개인정보를 제공해야 하는지 이용자가 선택과 결정을 하는데 도움을 주는 것이다.

4.2. 시스템 구성

P3P의 구체적인 메커니즘은 XML을 사용하여 P3P 프라이버시 방침(P3P Policies, XML로 이루어져 기계적으로 읽을 수 있는 웹사이트 프라이버시 보호정책)에 대한 어휘와 구체적 표현(예를 들어 데이터를 수집하는 주체에 대한 어휘, 수집되는 데이터의 종류, 목적, 데이터 수신자, 분쟁해결 등에 대한 것 등)을 비교하여 프라이버시 방침에 대한 개인과 웹사이트간의 협상을 이끌어내는 것이다.

P3P는 또한 사용자가 제공할 수 있는 정보를 표준화할 수 있는 표준언어를 포함하고 있는데, 이를 P3P 선호교환언어(P3P Preference Exchange Language, APPEL)라고 한다. APPEL은 웹사이트에서 요구하는 정보에 따라 사용자가 어떠한 행위를 할 것인가에 대한 도움을 준다.〔7〕 P3P의 구현과정은 〔그림 6〕과 같다. P3P시스템에서 이용자가 사이트를 검색할 때, 사용자 측의 에이전트는 방문 사이트의

〔표 3〕 국외 주요 프로젝트

프로젝트명	주요 연구내용
RAPID ('02.7~'03.6)	프라이버시와 신원 관리 분야에서의 연구 주제를 발굴
PRIME ('04.3~'08.2)	정보사회에서 개인의 자신의 개인공간을 제어하고 신원을 관리할 수 있는 프라이버시 강화형 신원관리 솔루션 구축 환경을 제공
FIDIS ('04.4~'09.3)	적절한 신원확인 및 ID관리를 위한 ID관리의 상호연동, 포렌식, 프로파일링, 고기술의 ID 및 이동성 등의 7가지 분야에 대해 연구

〔표 4〕 국외 주요 연구대학

연구대학	주요 연구내용
UC Irvine	조직이 자신의 데이터베이스를 외부의 서비스 제공자에게 위탁하는 모델에서 외부의 서비스 제공자로부터 조직의 주요 정보의 유출 및 위·변조를 방지하기 위한 기술을 연구하는 "Privacy and Security in Database-as-a-Service Model" 프로젝트 수행
Johns Hopkins	"MIPA(Medical Information Privacy Assurance)" 프로젝트에서는 미국의 건강보험 편이성 및 책임법(HIPPA, Health Insurance Portability and Accountability Act)을 지원하기 위해 의료정보시스템에서의 프라이버시를 보호하기 위한 기술 개발 및 인프라 구조를 개발·연구

P3P 정책 파일을 요구한다. 그리고 이에 대응하여 해당 사이트에서는 프라이버시 정책 파일을 보내게 된다. 이러한 과정에서 이용자가 설정한 프라이버시의 선호수준과 방문한 웹사이트간 트랜잭션이 발생하게 되고 사용자의 설정 기준에 맞는 경우 요청된 웹 페이지가 전송된다.

Ⅲ. 국외 관련 프로젝트

국제 웹 표준화 기구인 W3C(World Wide Web Consortium)는 2002년에 웹사이트 이용시 프라이버시를 보호하기 위해 정한 표준 기술 플랫폼인 P3P를 개발하였다. 한편, 유럽에서는 4년 단위의 IST(Information Society Technologies) 연구 프로젝트를 진행하면서 그 산하에 개인정보보호와 관련된 다양한 프로젝트를 수행 중에 있다.

그 외 유럽연합에서는 PISA(Privacy Incorporated Software Agent) 프로젝트를 통해 네트워크 환경에서 개인정보 유출 없이 사용자를 대신하여 복잡한 업무를 수행하는 지능형 소프트웨어 에이전트 모델 구축을 위한 연구를 수행하고 있다. 한편, 미국은 대학 중심의 프로젝트를 위주로 연구 및 기술 개발이 진행되고 있는데, 주로 개인정보보호 정책을 시행하기 위한 도구, 신원 절도와 신원보호에 대한 이론 위주의 연구가 진행되고 있다.

Ⅳ. 결 론

향후 유비쿼터스 환경이 도래함에 따라 사용자에 대한 인비저블(Invisible)형태의 편재된 서비스 제공을 위해서는, 필수적으로 사용자의 개인정보가 요구된다. 그러나 개인정보의 부적절한 노출로 인한 개인정보 침해 문제는 유비쿼터스 컴퓨팅의 순기능적 효과를 반감시키는 요인이 될 수 있으며 지금까지의 네트워크에서 생각하는 개인정보보호의 상식을 크게 바꿀 수 있다.

본 논문에서는 유비쿼터스 환경에서 개인정보에 대한 국내외 및 시장동향을 살펴보았고 현재 연구개발되고 있는 개인정보보호 기술동향을 조사하였다.

향후에는 개인정보보호 기술을 체계적으로 구체화해서 유비쿼터스 IT 환경에 적합한 개인정보보호기술 개발에 착수해야 할 것이다. 또한, 개인정보가 갖는 특성을 고려해서 기존의 정보보호시스템이 갖는 한계점을 분석한 후 이를 해결할 수 있는 새로운 프라이버시 보호 인프라 및 프라이버시를 고려한 개인정보보호 체계 분석이 필요할 것이다.

참 고 문 헌

〔1〕 한국전산원, 개인정보보호를 위한 기술개발 및 기술정책에 관한 보고서, 2004.9

〔2〕 서동일, 개인정보보호기술의 개발과 산업육성, ETRI. 2005

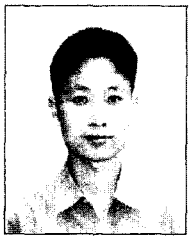
[3] PORTIA Project, http://crypto.stanford.edu/portia
[4] MIPA Project, http://www.cs.jhu.edu/~ateniese/mipa.html
[5] IBM, http://www-6.ibm.com/jp/services/security/features/
[6] PISA Project, http://pet-pisa.openspace.nl/pisa_org/pisa/index.html
[7] P3P, 「The Platform for Privacy Preferences 1.0(P3P 1.0) Specification」, http://www.w3.org/p3p
[8] JJ.Borking, "M. van Eck, P.Siepel, Intelligent Software Agents and Privacy"
[9] www.pet-pisa.nl, "Privacy Incorporated Software Agent System Architecture (PSA)"
[10] Handbook of Privacy and PET (Privacy Enhancing Technology), PISA Project
[11] IBM TPM, Tivoli Privacy Manager, http://www-6.ibm.com/jp/software/tivoli/products/privacy.html
[12] NTT, Secure USB 메모리, http://www.ntt.co.jp/
[13] NEC, http://www.nec.co.jp
[14] 윤재석, 국외 프라이버시보호기술의 개발 동향과 발전 전망, 한국정보보호진흥원, 2001.3
[15] 조동기, 김성우, 인터넷의 일상화와 개인정보보호, KISDI 이슈리포트, 2003.8.25
[16] 지승훈, 개인정보보호 동향 및 서비스 제공자의 책임, 전자신문, 2005.8.2
[17] 홍준형, 도청·해킹 기술 갈수록 정교-개인정보보호법 제정 시급, 한국일보, 2005.8.17
[18] KT, 인터넷 개인정보노출 막는다, 디지털타임스, 2005.8.19
[19] 윤재석, P3P의 논의 현황과 문제점 및 국내정책방향, 전자신문, 2005.3.28
[20] 이성몽, 유비쿼터스 컴퓨팅 환경에서 개인정보보호방법, 국민은행 전산정보그룹, 정보통신연구진흥원 (www.iita.re.kr), 주간기술동향, 2005.5.4
[21] 윤용근, 정병주, "유비쿼터스 컴퓨팅 환경하의 개인정보 침해 유형분석," 한국전산원 정보화정책 이슈, 2004.
[22] 박승창, "유비쿼터스 IT의 2030년 사용자 시나리오(I, II, III, IV, V, VI, VII)," 전자부품연구원 전자정보센터(www.eic.re.kr)
[23] 개인정보 보호백서, 2002.
[24] 강달천, "유비쿼터스 컴퓨팅 환경에서의 개인정보보호," 한국인터넷 법학회, Mobile·Ubiguitous와 법제, 12, 2004, pp.19-45
[25] 강달천, "정보통신환경의 변화와 개인정보보호," 개인정보보호 정책 Forum, 2005. 5. 19.
[26] 개인정보보호를 위한 IT 솔루션, IBM Japan http://www-6.ibm.com/
[27] Misa Aoki, IT 시스템에 의한 프라이버시 대책, PROVISION No.42 Summer 2004
[28] Yoshiaki Watanabe, 정보개시 관리솔루션, PROVISION No.42 Summer 2004
[29] IBM, http://www-6.ibm.com, 프라이버시: 개인존중을 바탕으로 한 서비스: Steven Adler와의 인터뷰
[30] 정보통신부, 중장기정보보호로드맵, 2005.5
[31] 한국정보보호산업협회, 2004.11
[32] 정보통신부, 개인정보보호를 위한 종합대책(안), 2005.9
[33] Takuya Iwamoto, 정보관리 방식 「임계치 비밀 분산법」, 2004/11/27

〈著 者 紹 介〉

송 유 진 (You Jin Song)

1982년 2월 : 한국항공대학교 전자공학과 졸업
1987년 8월 : 경북대학교 대학원 정보시스템학과 석사
1995년 3월 : 일본 Tokyo Institute of Technology 정보보호학과 박사
1988년 3월~1996년 2월 한국전자통신연구원 선임연구원
2003년 12월~2005년 2월 : 미국 Universty of North Carolina at Charlotte 연구교수
1996년 3월~현재 : 동국대학교 전자상거래학과/대학원 교수
2005년 현재 동국대학교 부설 전자상거래연구소 소장
1998년~현재 한국정보보호학회 이사
1997년~현재 한국정보시스템학회 이사
2001년 ICISC2001 운영위원장 역임
2003년 하계CISC2003 프로그램 위원장

관심분야 : 전자상거래응용 보안 (Ubiquitous/Web Service Privacy, Location Privacy, 디지털컨텐츠 보호, XML보안, SCM/CRM 보안 등), Context Aware Application Security

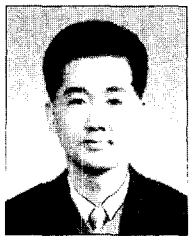


이 동 혁 (Dong Hyeok Lee)
학생회원

2004년 8월 : 동국대학교 전자상거래학과 졸업
2005년 3월~현재 : 동국대학교 대학원 전자상거래학과 석사과정
관심분야 : 유비쿼터스/웹서비스 프라이버시 보호, 전자상거래 보안

남 택 용 (Nam Taek Yong)

1987년 충남대학교 계산통계학과 이학사
1990년 충남대학교 계산통계학과 이학석사
2005년 한국외국어대학교 전자정보공학과 공학박사
1987년 ~ 현재 : 한국전자통신연구원 정보보호연구단, 개인정보보호연구팀 팀장(책임연구원)
관심분야 : 정보보호, 인터넷, 이미지마이닝 등



장 종 수 (Jang Jong Soo)

1984년 경북대학교 전자공학과 공학사
1986년 경북대학교 전자공학과 공학석사
2000년 충북대학교 컴퓨터공학과 공학박사
1989년 - 현재 한국전자통신연구원 네트워크보안그룹 그룹장(책임연구원)
한국정보보호학회 이사
학회지 편집위원장
한국정보처리학회 논문지 편집위원
한국정보과학회 논문지 편집위원
한국통신학회 회원