디지털 아이덴티티 및 사용자 중심 IdM 논의의 현황

박 정 현*

1. 개 요

90년대 초반까지만 해도 일부 연구자들의 정보 공유 네트워크에 가까웠던 인터넷은 그래픽 위주의 월드 와이드 웹의 확산과 아마존의 상업적 성공 이후 대중 서비스업의 성격으로 크게 바뀌게 되었다. 이후 각 웹사이트 및 시스템은 아이디(ID)와 비밀번호로 대표되는 닫힌 체계를 지향하였고, 서로 다른 수준의 사용자 정보와 방식으로 설치·관리되는 개인 정보 관리 체제가 각 시스템 수준에서 구성되었다. 최근 들어 인터넷의 행정·사회·경제적 영향력이 급증하면서 여러 곳에 흩어진 개인 정보는 보안 및 편의성의 관점에서 문제점으로 지적되기 시작하였고, 이를 통합적으로 관리할 수 있는 디지털 신원관리(IdM, digital identity management)의 필요성이 제기되어 왔다.

이에 따라 OECD에서는 지난 2년간 정보통신정책위원회(ICCP) 산하 정보보호작업반(WPISP)에서 워크샵 및 자발참여국가(Voluteer Group, VG)의 형태로 IdM논의를 진행해 왔다.[1] 최종 목표는 IdM 국제 규범의 출간이며, 현재까지의 작업은 주로

* 정보통신정책연구원 방송통신협력연구실 연구원, (02)570-4213, nique08@kisdi.re.kr

1) VG에서는 참가 국가 대표단 위주의 메일링 리스트를 통하여 논의를 진행하고 회의 및 문서발간을 진행한다.

정의・필요성・활용 예를 다룬 작업 보고서(working paper)와 1단계 결과물인 입문서(Primer)이다.[2] 향후 발간될 2단계 결과물이 IdM 보안 및 프라이버시 권고안이 될 예정이다. 이에 따라 본고에서는 현 단계에서 이해해 두어야 할 IdM의 주요 개념인 디지털 아이덴티티와 사용자 중심 원칙을 '07~'09년 주요 OECD IdM 문서를 통해 살펴본다.[3]

2. 본 문

(1) 기본 개념

IdM 관련 OECD 문건에서 IdM은 해당 시스템의 서비스나 자원에 접근하기 위해 디지털 아이덴티티를 설정・사용・교환하는 데 관련된 정책의 이행 규정・절차・기술로 정의되고, 논의의 대상은 자연인의 디지털 아이덴티티로 제한하고 있다.[4] 기본 개념 정의 소개를 위해 편의상 어떤 사람이 인터넷 사이트에 접근하는 경우를 가정하면, 사용자(user)는 해당 사이트에 자신을 지시(refer to)하는 정보인 ID・비밀번호 등 식별자(identifier)를 제시한다. 혹은 IP 연동 사이트 접속에서처럼 식별자는 사용자에 의해 제시되지 않을 수도 있으며, 아이덴티티 정보를 대신 관리하는 아이덴티티 제공자(identity provider)에 의해 제시될 수도 있다. 또 다른 주요 개념인 신원 확인(identification)의 주체는 따로 개념화해서 생각하는 일이 적은데, 이는 인터넷을 비롯한 정보통신 맥락에서 신원 확인이란 특정 사람이나 기관이 개입하지 않고 사전에 입력한 절차 및 코딩에 의해 자동적으로 이루어지는 경우가 많기 때문이다. 단, 사용자 신원을 다른 시스템에 위임하여 확인하는 웹사이트 등을 인증위임자(relying party)라고

2) 현재 입문서는 1차 수정안(DSTI/ICCP/REG(2008)10/REV1)이며 4월 3일 경 2차 수정안(REV2)이 발간되고 기밀해제하기로 하였으나 아직 검토 중이다.

3) 해당하는 문서는 '07년 노르웨이 워크샵 발표 문서들, '08년 작업 보고서, '08년 입문서이다(Gross(2007), Pfitzmann(2007), Rundle et. al(2008), OECD(2008)).

4) OECD(2008).

부르는 경우가 있다.[5] 그리고 디지털 정보가 지시하는 특정인을 정보와 구분하여 표현하기 위해 데이터 주체(data subject)라고 한다.

1) 아이덴티티 · 속성 · 주장

OECD 논의에서 디지털 아이덴티티(digital identity)는 식별자로 제한되지 않고, 현실 세계 정체성에 대한 이해에서 출발하되 현실 세계와 인터넷의 차이를 다루기 위해 디지털 아이덴티티의 두 가지 특징으로 속성(attribute)과 주장(claim)을 제시한다. 우선 속성은 특정 개인과 연관된 지시적 정보를 뜻하며, 현실 세계 정체성이 맥락에 근거한 다중 정체성임에 주목한다. 현실 세계에서 한 개인은 누군가에게 한 명의 사람으로 이해된다기보다 상황과 맥락에 따라 서로 다른 정체성으로 상대방에게 인식된다고 할 수 있다. 이 때 각 정체성은 서로 다르거나 일부 겹치는 세부적 속성으로 구성되므로, 특정인이 갖는 속성의 전체 집합 중에서 일부 조합을 통해 상황과 맥락에 맞는 정체성을 구성하여 상대와 소통한다고 할 수 있다. 즉, 한 개인의 아이덴티티 구축은 그 사람이 가진 여러 속성들의 집합에서 일부를 선별하여 이루어지는 것이다. 이와 같은 관점에서 디지털 아이덴티티는 속성의 집합으로 정의되며, 그 세부적 의미는 아래 pID 논의에서 다룬다.[6]

디지털 아이덴티티의 또 다른 특징인 주장은 인터넷 환경의 비대면적 특징과 익명성에 의해 신원 확인이 데이터 주체와 무관하게 제시될 수 있는 주장(claims)에 근거함을 주목한다. 이것은 현실 세계의 정체성이 특정 사물이나 사람이 인지되거나 알려지는 "개별적 특성의 포괄적 집합"임에 반해, 온라인 정체성은 누군가가 특정 데이터 주체에 관해 제기하는 주장의 집합이기 때문이다. 다시 말해, 현실 세계에서는 누군가의 신원을 확인할 때 데이터 주체의 얼굴이나 목소리, 서명 등을 신원 확인자가 인식한 뒤 적절한 결정을 내리지만, 온라인에서는 신원 확인을 위해 제시된 내용이 정말 데이터 주체에게서 기인한 것인지 여부를 판단하기가 더욱 어렵다. 이 같은 차이를

5) 인증위임자는 사용자 인증을 다른 서비스 제공자나 아이덴티티 제공자에 의존하기 때문에 relying party라고 불린다.

6) Pfitzmann(2007); OECD(2008).

부각시키기 위해 작업 보고서는 디지털 아이덴티티를 “주장의 집합... 특정인을 지시하되 그 사람과는 다른 인위적 산물”로 정의하고 있다.[7)]

속성에 관한 논의는 속성의 종류・핵심(core) 속성・생체 정보 등을 다루고 있다. 속성의 종류로는 여러 가지가 제시되고 있으나, 대부분 변화 가능성과 획득 여부에 초점을 맞추어 대립적 개념으로 파악한다.

〈표 1〉 속성의 종류와 핵심 아이덴티티

속성의 종류		핵심 아이덴티티
바꾸기 쉬운가?	바꾸기 어려운가?	바꾸기 어렵다
시간이 지나면 변하는가?	변하지 않는가?	시간이 지나도 변하지 않는다
주어진 것인가?	획득된 것인가?	주어진 것이다
단순 속성인가?	부가적 정보 포함한 속성인가?	부가적 정보를 포함한다
단일 개체의 특성인가?	다른 개체와의 관계에서 보이는 특성인가?	n/a

자료: Pfitzmann(2007)

이 중 바꾸기 어렵고, 시간이 지나도 변하지 않고, 주어진 것이고, 부가적 정보를 포함할 경우 신원 확인에 더욱 효과적으로 사용될 수 있다고 보고 핵심 아이덴티티(core identity)라고 한다. 그 이유로는 이름처럼 자주 식별자로 사용되거나, 혈액이나 DNA처럼 소량으로도 많은 부가적 정보를 알 수 있거나, 키나 눈동자 색(유럽의 경우)과 같이 잘 변하지 않기 때문이다. 특히 이 중 생체 정보는 흔히 강력한 인증 체계에 사용될 수 있는 생물학적 및 행태적 특징으로 본다.[8)] 생체 정보의 장점으로는 디지털화하여 자동 인식에 사용할 수 있으며, 아이덴티티의 DB 복수 등록을 막고, 물리적인 소유나 암기와 무관하기 때문에 강력한 인증이 가능하다는 점이다. 단점으로는 일부 생체 정보는 복사에 취약하며, 민감한 정보이므로 얼마나 자주 사용하는지 논의가

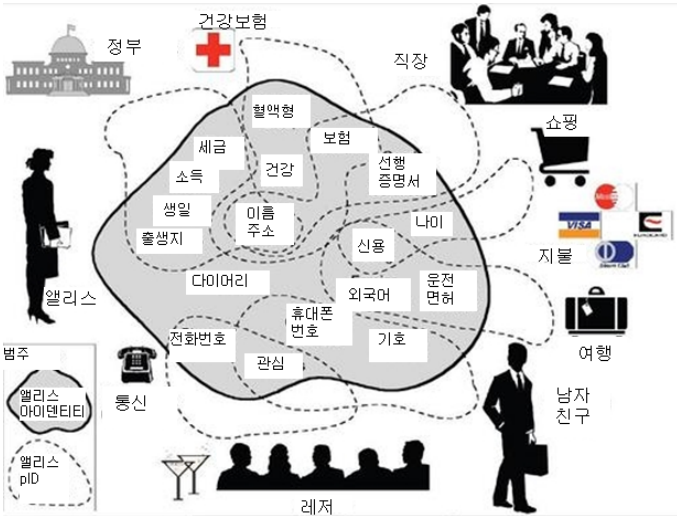
7) Rundle et. al(2008), p.7.
8) OECD(2008).

필요하고, 사용자 동의 없이 주어질 수 있으며, 한 번 신원이 확인되면 되돌리기 어렵다는 것이다.[9)]

2) pID · 크리덴셜

상기한 바와 같이 속성의 관점에서 디지털 아이덴티티를 이해한다면 각 맥락에서 일부 속성만 선별적으로 모아서 아이덴티티가 구성되므로, 각 사용처에 맞는 속성을 모아두고 적합한 명칭(이름・식별자・인증도구)을 붙인 것을 부분 아이덴티티(pID, partial identity)라고 한다. 이에 따라 pID는 특정 영역 내에서 한 개인을 독특한 한 명의 개체로 인식한다.

〔그림 1〕 pID 개념도



자료: Pfitzmann(2007)

예를 들어, 〔그림 1〕에서 Alice의 "남자친구" 영역, "레저" 영역, "쇼핑" 영역을 보면, "관심"만 남자친구와 레저 영역에서 겹치는 것을 알 수 있다. 또한 레저 동호인에

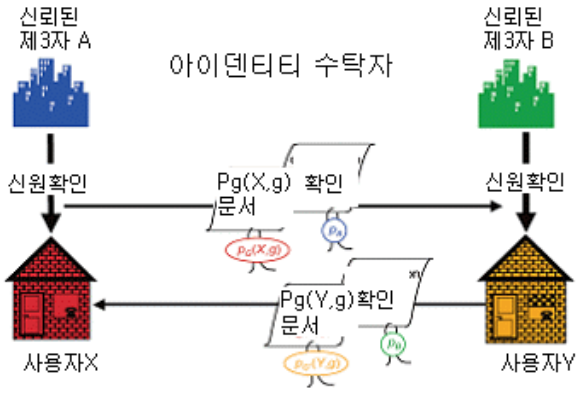
9) Pfizmann(2007).

게 알려주는 전화번호와 남자친구에게 알려주는 전화번호가 다르고, 나이는 쇼핑 영역에서만 알려진다. 즉, 각 영역에 따라 서로 다른 속성을 선별적으로 모은 pID 구성이 가능하다.

또한 각 pID의 목적에 따라 몇 가지 속성만 알아두면 충분하므로 모든 정보를 모든 상황에 활용할 필요가 없기 때문에, 인터넷 환경에서 보안과 프라이버시를 강화하기 위해 사용자의 디지털 아이덴티티로 오직 pID만 이용하는 것이 제안된다. 즉, 〔그림 2〕처럼 각 pID에 대해 식별자로 쓰이는 디지털 가명을 만들고 초기 연결을 사용자가 직접 설정하되, 일종의 아이덴티티 수탁자(trustee for identities)가 각 디지털 가명과 사용자 사이의 관계에 대해 보증을 서는 것이다.

그렇지만 앞에서 살펴본 것처럼 인터넷 환경의 아이덴티티 설정은 주장에 의지하는 측면이 강하다. 주장하는 내용만으로는 인터넷 환경에서 신원 확인을 요청하는 주체가 데이터 주체와 동일인인지 확인하기 어렵기 때문에, 주장하는 내용이 데이터 주체에 관련된 것이 맞는지 확증해 주는 크리덴셜(credential)이 종종 발급된다. 크리덴셜의 예로는 은행카드 번호·디지털 증명서(certificate)·생체 정보 템플릿(template) 등이 있다.

〔그림 2〕 아이덴티티 수탁자



자료: Pfitzmann(2007)

3) IdM 절차

IdM의 절차는 크게 두 단계, 등록과 승인으로 나뉜다. 소개되는 개념 자체는 간단하지만 현재는 용어 간 구분이 명확하지 않아 각 단계별로 살펴본다.

〈표 2〉 IdM 절차

등 록		승 인		철 회
조회	크리덴셜 발급	승인-확증 수준	권한 부여	크리덴셜 무효화

자료: OECD(2008)

IdM 절차는 등록(enrolment)에서 시작한다. 등록이란 해당 기관의 DB에 데이터 주체의 정보를 저장하는 것으로 생각할 수도 있겠으나, OECD 문서에서는 등록을 2단계로 이해하여 기관이 개인의 아이덴티티 주장의 신뢰도를 조회(verification)한 뒤 적절한 크리덴셜을 발급하는 것을 의미한다. 조회는 온라인 혹은 오프라인으로 이루어질 수 있으며, 보다 엄격한 조회일 경우 다른 기관에서 발급한 크리덴셜의 제출을 요구할 수 있다. 조회를 통과한 개인에게 기관은 크리덴셜을 발급하며, 향후 개인은 주로 해당 기관의 자원 접근을 위해 크리덴셜을 사용하게 된다.

개인이 특정 기관의 시스템에 접근하고자 할 때, 해당 기관 혹은 다른 기관에서 발급한 크리덴셜을 제출하여 자신이 크리덴셜에서 보증하는 인물과 동일인임을 주장하는 것에 대해 기관이 확인하는 것을 승인(authentication)이라 한다. 승인에는 크리덴셜의 신뢰도와 승인 과정 자체의 신뢰도 등 몇 가지 위험요소가 들어있어 일정 정도의 확증 수준(a level of assurance)을 갖는다. 승인을 통과한 개인에게 기관이 시스템에 대한 접근 허가를 부여하는 과정은 권한 부여(authorisation)라고 한다. 또한 개인이 기관을 떠날 때 크리덴셜을 무효화하는 과정을 철회(revocation)라고 한다.[10]

10) OECD(2008).

(2) IdM 설계의 사용자 중심 원칙

1) 사용자 중심 원칙의 배경

OECD 아이덴티티 논의는 IdM 설계에 책임성과 신뢰성 제고를 위하여 사용자 중심(user centric) 원칙을 제시한다. 업계나 정부 등 서비스 제공자의 입장에서 효율성을 높이기 위해 전 시스템 차원의 IdM을 제시하는 것이 아니라, 사용자의 입장에서 프라이버시를 최대화하기 위해 익명성이 보장된 개인화된 IdM을 제공하여 개인의 선택을 존중하고자 한다. 작업 보고서는 사용자 중심 원칙의 사상적 배경을 헤겔(Hegel)과 로크(Locke)에게서 찾고 있다. 유럽의 개인 정보법은 헤겔 사상의 영향을 받아 데이터 주체가 자신에 관한 개인 정보를 소유물처럼 통제할 수 있어야 하고 이에 관한 자유가 공동체 안에서 보장되어야 한다고 생각하며, 영미 법체계는 로크의 영향을 받아 개인 정보는 개인에게 머무르며 국가의 간섭에서 분리되어야 한다고 보는 것이다.

풀어서 말하면, IdM은 여러 시스템을 아울러 제공하는 개념이므로 부차적인 프로파일링과 잘못된 신용 평가서 등의 파급효과로 인해 개인의 명성과 활동에 큰 영향을 입힐 수 있다. 즉, 사람 자체가 아닌 과거의 행동에 근거하여 작성된 프로파일이 디지털 아이덴티티의 명성과 활동에 영향을 줄 수 있는 인터넷 환경에서는, 자신에 관한 정보 통제 능력이 더욱 중요해지는 것이다. “자신의 아이덴티티 데이터 활용을 통제할 수 있는 능력은 다른 사람들에게 데이터 이면에 사람이 있음을 일깨워주고 그 사람이 타인과의 관계에서 완전한 지위를 가질 수 있게 하는데 결정적인 역할을 한다.” 따라서 디지털 아이덴티티는 사용자 중심으로 설계되어 데이터 주체의 자율성을 촉진하여야 한다고 주장한다.[11)]

2) 사용자 중심 IdM 설계

사용자 중심 IdM은 사용자들에게 자신의 개인 정보에 대한 높은 수준의 통제를 가능하게 하는 것으로, 서비스 제공자와 무관한 아이덴티티 제공자(identity provider)를

11) Rundle et. al(2008), pp.9~10.

별도로 제시한다.[12] 즉, 사용자가 특정 시스템에 접근할 때, 서비스 제공자에게 자신의 개인 정보를 제시하지 않고 공인된 제3자인 아이덴티티 제공자에게 개인 정보를 저장시킨 뒤 필요 시 승인하게 하는 것이다. 이를 통해 사용자 중심 IdM은 사업자가 아닌 사용자의 이익을 위해 일하는 아이덴티티 제공자를 설정하며, 구성 요소로 다음의 세 가지가 제시된다.

〈표 3〉 사용자 중심 IdM의 구성 요소

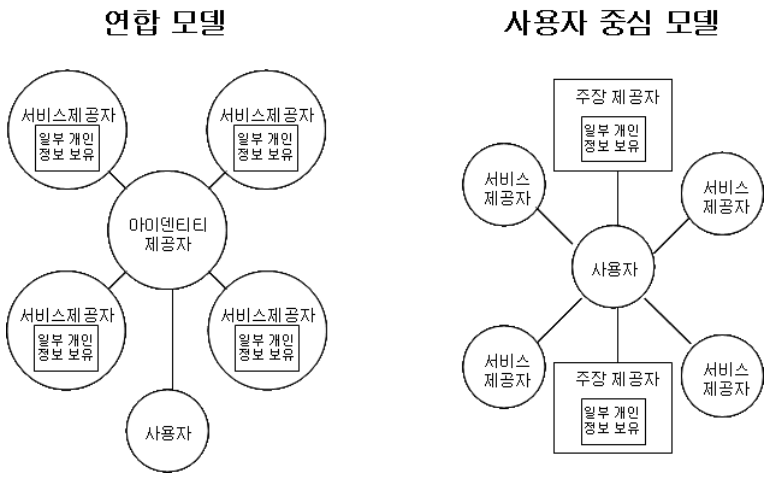
구성 요소	역 할
아이덴티티 제공자	사용자 계정과 정보를 저장하고 사용자를 승인한다.
인증위임자	사용자 아이덴티티 승인 여부에 대해 아이덴티티 제공자에 의존하는 당사자로서, 사용자 중심 IdM에서는 서비스 제공자 중 일부가 된다.
서비스 제공자	아이덴티티 제공자에게서 사용자 승인 여부를 확인받아 사용자에게 서비스를 제공한다.

자료: Rundle et. al(2008)

연관된 개념인 연합 IdM은 “연합된 사이트들 간에 ID 정보를 필요에 따라 공유하는 모델”이다.[13] 연합된 사이트 중 하나가 아이덴티티 제공자가 되고 다른 서비스 제공자들은 해당 사이트에 의존하는 의존자가 된다. 그렇지만 여전히 각 서비스 제공자는 사용자에 관한 서로 다른 정보 집합을 가지고 있으며 필요시 서로 협의할 수 있다. 연합 IdM에서 사용자가 갖는 장점으로는 주요 계정 승인을 통해 복수의 서비스 제공자에 접속할 수 있다는 것이다. 단, 연합의 범위를 사용자가 알 수 없으며, 아이덴티티 제공자가 특정 사용자의 식별자 및 정보를 사용자의 동의 없이 모두 수합할 수 있다는 단점이 있다.[14]

12) Rundle et. al(2008).
13) 한국전자통신연구원(2008), p.7.
14) OECD(2008).

〔그림 3〕 연합 IdM과 사용자 중심 IdM



자료: OECD(2008)

사용자 중심 IdM의 세부 설계 내용으로 정보의 내용・노출 기간・범위를 사용자가 결정하거나 사용자에게 고지하여야 한다는 것이 제안되었다. 여기서는 IdM 디자인 세부 사항에 관해 좀 더 명확하게 제시한 작업 보고서의 네 가지 사항을 살펴본다.[15]

① 타인에 의한 아이덴티티 정보 취급(treatment) 통보

사용자는 인증위임자가 어떤 정보를 요청하였으며 데이터 보유(data retention) 및 처리 방침(handling policy)의 내용을 알고 고지에 입각한 선택(informed choice)을 내릴 수 있어야 한다. 단, 현 포털 가입 혹은 소프트웨어 사용 동의 시 제공되는 장문의 법적 문서는 현실적이지 않으므로 서비스 제공자 신뢰도 제고를 위한 시스템을 만들고 국제적 협력을 이룰 수 있는 체계가 필요하다.

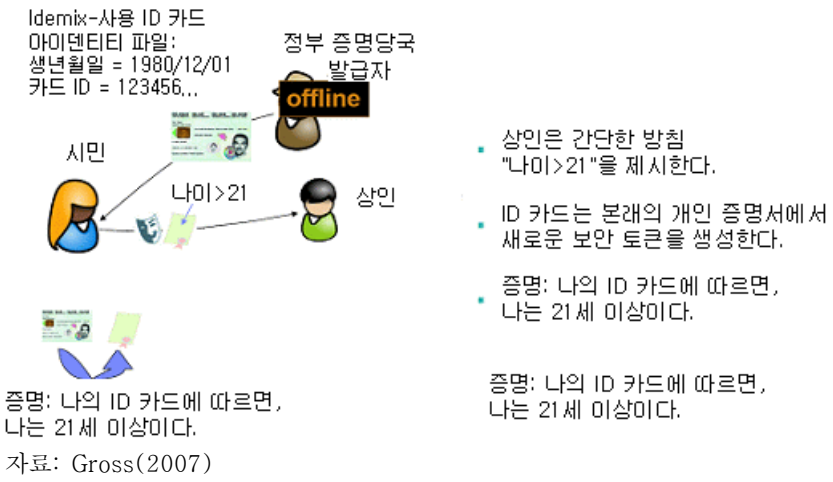
② ①과 같은 정보 취급에 대한 사용자의 동의 혹은 거부 기회

사용자는 상기한 사항에 대해 언제라도 동의 및 거부 의사를 밝힐 수 있어야 한다. 더욱 바람직한 것은 사용자 스스로 매 상황마다 자신의 아이덴티티 정보 활용을 위한 조건과 의무를 설정하는 것이다. 일견 어려워 보이지만, 적절한 암호학 기술을 활용하

15) Rundle et. al(2008).

면 기술적 구현이 가능할 수 있다. PRIME에서 제안하는 “Identity Mixer(Idemix)”에서, 사용자 ID 카드는 정부 승인을 얻은 것으로 해당 개인의 개인정보와 개인 증명서를 담고 있다. 사용자가 자원 접근을 요구하면, 서비스 제공자는 개인 정보의 일부만 이용하여 답할 수 있는 질문을 제기한다. 사용자의 ID 카드는 답변을 구성하여 개인 증명서와 함께 제시하고, 서비스 제공자는 내용을 확인하면서 (정부에서 사전에 제공한) 공개 키를 이용하여 사용자가 데이터 주체임을 확인한다. pID 개념으로 설명하면, 각 정보 처리마다 각기 다른 가명과 속성을 담은 서로 다른 pID가 구성되고, 또한 해당 pID가 나의 것이라는 것을 공개 키－개인 증명서로 확인하기 때문에, 사용자 중심 원칙 외에도 책임성과 익명성이 보장되는 것이다.[16)]

〔그림 4〕 PRIME의 Idemix 개념도



자료: Gross(2007)

③ 보안 및 프라이버시 보장

IdM은 설계 상 표준화된 IdM 컴포넌트 연동을 통해 아이덴티티 정보 자체는 아니더라도 아이덴티티 정보의 흐름을 집중화시키는 만큼, 해커 등의 관심을 특정 요소로

16) Gross(2007).

집중시켜 보안 및 프라이버시 위험을 오히려 증가시킬 수 있다. 이를 상쇄하기 위해, 사용자 중심 IdM은 다음을 포함하여야 한다.

〈표 4〉 사용자 중심 IdM의 보안 및 프라이버시 보장 원칙

탈집중화	가능한 많은 데이터 맥락으로 아이덴티티 정보를 분리
데이터 최소화	처리에 필요한 최소한의 아이덴티티 정보만 저장
지역 식별자	흩어진 개인 정보의 연결을 막기 위해, 각 맥락에 고유한 명명 체계를 사용(주민등록 번호와 같은 전체 식별자 사용 회피)
검증가능성	인증위임자들을 위하여 사용자 관련 주장이 사용자에게서 기인한 것인지 여부를 검증하는 체계 지원
선별적 공개	각 정보 처리에 필요한 만큼만 아이덴티티 정보를 공개(예: 주류 구매 시 나이를 명확히 밝히지 않고 18세 이상 혹은 이하만 검증)
조합가능성	사용자가 자신의 기존 pID를 조합하여 디지털 페르소나를 구성[17]
심사가능성	감사 및 심사를 통해 확인 및 교정 기회 제공

자료: Rundle et. al(2008)

④ 데이터에 영향을 미치는 실질적 실천에 관한 정보 접근 및 교정 기회

자신의 정보가 어떻게 쓰이는지 알고 싶어 하는 것은 사용자의 기본적인 예상이므로, 이미 여러 국제적 데이터 보호 원칙에서 접근성 보장이 지속적으로 제기되어 왔다. 문제는 누가 자신의 정보를 갖고 있는지 사용자에게 스스로 찾도록 하고 있다는 것이다. IdM은 개인정보 활용 현황에 대한 접근성을 제고할 수 있다. 물론 공적인 개인 정보 활용의 경우 초기 동의한 내용과 다른 목적으로 쓰이는 것이 인정되지만, 이 경우 확인을 위한 접근 요청은 각 개인이 하는 것보다 옴부즈맨 역할을 하는 정부 담당자 지정이 더욱 효율적일 것이다.

17) 페르소나(persona)란 "자신의 내적 자아와 구분되는 공적인 이미지 혹은 개성으로, 사회에서 맡겨지거나 드러나는 역할"이라고 정의된다(Rundle et. al(2008), p.8). 아이덴티티와 페르소나를 명확히 구분하기는 어렵지만, 자신이 타인과의 관계에서 만들어나가고 타인에게 보여지는 동태적인 측면을 페르소나라고 한다면, 좀 더 일시적이고 신원 확인에 초점을 맞춘 정태적인 측면을 아이덴티티라고 할 수 있다.

3. 결 어

지금까지 '07~'09년 OECD IdM 주요 문서를 통해 IdM 논의의 가장 기본적인 개념인 아이덴티티와 사용자 중심 IdM 원칙을 살펴보았다. 여타 선진국과는 다르게 보편적 식별자(universal identifier)인 주민등록번호를 다양한 인터넷 사용 환경에서 사용해온 우리나라의 입장에서는 OECD IdM 논의의 기본 방향인 pID・크리덴셜의 사용과 사용자 중심 IdM 원칙이 일견 불편하게 느껴질 수 있을 것이다. 그러나 최근 옥션 소송, 다음 소송, 하나로텔레콤 소송 등에서 보이듯, 웹사이트 보안문제가 점점 심각한 사회문제로 제기되고 있다. 이를 보완하기 위해 지난 몇 년간 우리나라에서는 한국정보보호진흥원(KISA)과 한국전자통신연구원(ETRI)을 중심으로 공인인증서나 iPIN과 같은 사용자 중심 IdM이 개발되어 점점 널리 쓰이고 있으므로, 이와 같은 경험을 교훈으로 삼으면 우리나라가 OECD IdM 정책적 권고안 형성에서 주도적인 역할을 할 수 있을 것이다.

참고자료

한국전자통신연구원(2008), 『Digital Identity Management 2008년 기술 백서』, 한국전자통신연구원.

Gross, Thomas(2007), "Privacy and Identity Management in Europe(PRIME)." http://www.oecd.org/dataoecd/44/3/38590523.pdf.

OECD(2008), "The Role of Digital Identity Management in the Internet Economy: A Primer for Policymakers." DSTI/ICCP/REG(2008)10/REV1.

Pfitzmann, Andreas(2007), "An Introduction to Digital Identity." http://www.oecd.org/dataoecd/6/63/38540119.pdf

Rundle, Mary, et. al(2008), "At a Crossroads: 'Personhood' and Digital Identity in the Information Society." http://www.oecd.org/dataoecd/31/6/40204773.doc.