

# 인터넷상의 본인확인수단인 아이핀의 활성화 방안 연구

장인용\*, 염흥열\*\*

요 약

정보통신기술의 발전은 다양한 인터넷 웹서비스의 개발과 이를 통한 편리한 서비스 환경을 제공한다. 국내 웹서비스 제공자들은 다양한 정보제공과 개인형 맞춤형 서비스를 위해 주민번호를 통한 실명확인서비스를 제공하고 있다. 웹서비스의 특성상 익명성으로 인한 폐단과 서비스 제공자의 부주의 등에 의한 개인주민등록번호 유출 등의 문제점을 해결하기 위하여 정부는 2006년 주민등록번호 대체수단 가이드라인을 마련하고 주민번호를 대체할 가상주민번호 서비스인 아이핀 서비스를 실시하고 있다. 그러나, 아이핀 서비스 정책은 정부의 업계에 대한 지원 미흡과 홍보부족 및 업계의 참여부진 그리고 이용자의 불신에 의하여 활성화 되지 못하고 있는 실정이다. 이에 본 논문은 그간의 아이핀 정책의 추진사항과 문제점 등을 분석하여 아이핀 정책의 활성화 방안 등을 제안하였다.

## I. 서 론

인터넷 정보통신의 발달은 다양한 웹서비스가 개발되고 활성화 되었으며, 웹서비스의 다양화와 편리함으로 인해 많은 사용자들이 일상생활에서 웹서비스를 적극적으로 활용하게 되었고, 그간 수많은 웹서비스들은 제공하는 서비스 범위보다 과도한 사용자 정보를 수집하기 시작하였으며, 특히, 개인 식별 등을 위한 주민등록번호 등과 같은 개인주요정보가 포함되어 개인정보보호 관련 크고 작은 사회적 문제가 발생하기 시작하였다.

정부는 인터넷 웹서비스의 과도한 정보 수집 및 개인 주민등록번호를 보호하기 위한 조치를 위하여 지난 2005년 6월 “인터넷상의 주민등록번호 대체수단 가이드라인”과 대체수단 기술수준을 마련하고, 아이핀 서비스를 통한 대체서비스의 도입을 추진하였다. 아이핀은 사용자 실명인증, 가상주민등록번호와 같은 잇점을 갖고 있으나, 아직 활성화가 미흡한 실정이다. 이에 본 논문은 아이핀의 주요내용을 분석하고 아이핀의 국내 서비스 활성화 측면과 아이핀이 국내 서비스에 국한되지 않고 글로벌화를 향한 가능성을 제시하고자 한다. 본

논문의 구성은 2장에서는 개인주민등록번호 등 개인정보의 유출과 익명성의 피해사례를 살펴보고, 3장에서는 정부의 아이핀 서비스 도입과정 및 아이핀의 동작과정에 대한 분석, 4장에서는 현재 아이핀 서비스의 분석에서 드러난 문제점을 제시하고, 5장에서는 아이핀 서비스의 주요 문제점을 연구조사 분석하여, 아이핀 서비스의 활성화를 위한 방안으로 기술시스템, 비용절감, 정부 정책의 3가지 측면으로 나눠 각각의 해결방안을 제안하며, 마지막 6장에서는 아이핀 서비스의 활성화 방안을 요약 정리하여 결론을 맺는다.

## II. 개인정보유출 및 익명성으로 인한 피해사례

개인정보유출과 익명성으로 인한 피해는 다양하고 광범위하며 커다란 사회적 혼란의 결과를 가져오기도 한다. 실제 개인정보 유출의 피해사례, 유출방식 및 익명성으로 인한 주요 피해사례를 살펴보면 다음과 같다.

가) GS 칼텍스 고객 정보 유출 사건 : 2008년 8월 5일 “GS 칼텍스 고객명단”으로 추정되는 1,125만

\* 순천향대학교 일반대학원 정보보호학과 박사과정(cyberjang@paran.com)

\*\* 순천향대학교 공과대학 정보보호학과 정교수(hyyoum@sch.ac.kr)

명의 개인정보가 CD2장에 담겨 자회사 내부 직원에 의해서 유출된 사례이다<sup>[12]</sup>.

나) 옥션의 고객 정보 유출 사건 : 2008년 2월 4일 중국 해커들의 해킹으로 인해 옥션의 고객 개인정보가 유출 되었으며, 이름, 주민등록번호, 주소, 이메일, 전화번호, 휴대폰번호, 카드번호, 비밀번호 등 옥션 가입 회원 1,081만명의 개인정보가 기술적 해킹에 의해 정보가 유출된 사례이다<sup>[12]</sup>.

다) 국민은행 고객정보 유출 사건 : 2006년 3월 인터넷 복권 구매안내 이메일을 통해 1,024명의 발송 고객정보가 유출되었으며, 고객이름, 주민번호, 이메일 주소 등의 개인정보가 정보보안 담당자의 실수로 유출된 사례이다<sup>[12]</sup>.

라) 하나로 텔레콤의 고객정보 불법 유용사건 : 하나로텔레콤은 2006년 1월부터 2008년 9월까지 자사 고객 600만명의 개인정보 8530만건을 전국 100여개 TM업체에 불법 제공되어 기업의 불법적 개인정보 활용 사례이다.

마) 악성댓글로 인한 피해 : 악성댓글로 인해 2007년 1월 22일 가수 “유니”, 2007년 2월 탈렌트 “정다빈”, 2008년 10월 2일 탈렌트 “최진실”, 2008년 10월 연예인 “장채원”이 자살을 하였다. 그밖에 일반인들도 악성댓글로 인해서 자살을 하거나, 악성댓글 작성혐의로 소송을 당하는 등 일련의 사건들이 아직도 진행 중이다<sup>[13]</sup>.

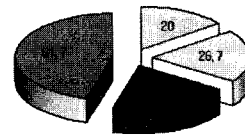
바) 미네르바 사건 : 2008년 7월 30일 외환보유고와 외환 예산 환전 업무에 관한 글을 유포한 혐의로 2009년 1월 7일 필명 미네르바가 체포되었다. 미네르바는 2008년 7월 30일, 12월 29일에 올린 글이 허위사실에 해당한다며, 전기통신기본법 위반으로 구속이 되었으나 법원에서 무죄 판결이 받았다.

이와같이 개인정보가 온라인상에서 다양한 방식으로 유출되고 있으며, 특히 개인주민등록번호 등의 개인식별정보는 정보유출시에 항상 포함이 되어있을 만큼 그 중요도가 매우 높다. 주민등록번호만으로도 개인 핵심 신상정보가 다수 포함되어 있기 때문이다.

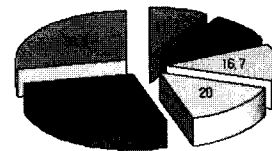
온라인상의 정보유출 이외에도 주민등록번호의 도용은 쉽게 일어나고 있다. 아래 [그림 1]과 같이 주민등록번호는 주변인이나 생생기 등을 통해서 쉽게 얻어질 수 있으며, 자신을 숨기거나 익명성을 구하기 위한 목적 등

으로 사용 된다.

주변 누구 주민등록번호를 도용하나?(%)



주민등록번호를 도용하는 이유는?(%)



[그림 1] 주민등록번호 도용사례

### III. 아이핀 서비스

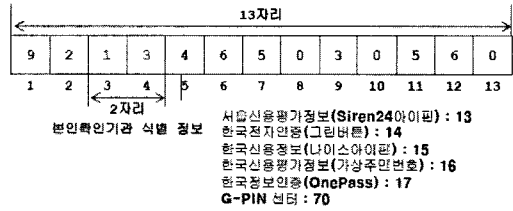
#### 3.1 아이핀

국내 주민등록번호제도는 개개인을 고유하게 식별할 수 있는 기능(생년월일, 출생지, 성별, 내외국인 등)이 있기 때문에 기관이나 관공서 등에서 개인을 인식하는 고유키(Key)의 성격으로 활용 되었으며, 온라인상에서는 고유한 개인을 식별할 수 있는 대표키로서 특성을 갖게 되었다. 주민등록번호는 시스템 상에서 개개인의 연결된 키(Key)와 같은 개념으로 인해서 시스템 간에 상호 연계성과 연동성을 제공함으로써 인터넷상의 다양한 개인화 정보서비스를 발전시킬 수 있는 기반으로도 기여한 바 크다.

2006년 10월 법률 개정을 통하여 서비스 개시된 아이핀은 인터넷상에서 과도한 주민등록번호 사용에 따른 개인정보보안의 사회적인 문제점을 해소하고, 실명제 도입을 위해 방송통신위원회와 한국정보보호진흥원이

개발한 사이버 신원확인번호로서 일종의 인터넷 가상 주민번호이다.

정부(방송통신위원회)는 2015년까지 온라인상에서 주민등록번호를 전면적으로 사용하지 않는 것을 목표로 하는 “인터넷 상 주민등록번호 대체수단(아이핀) 이용 활성화 기본계획”을 2009년 4월 31일 발표하였으며, 이후 기존 아이핀의 문제점을 해결하기 위한 “아이핀 2.0”을 개발 보급하게 되었다<sup>[11][15]</sup>.



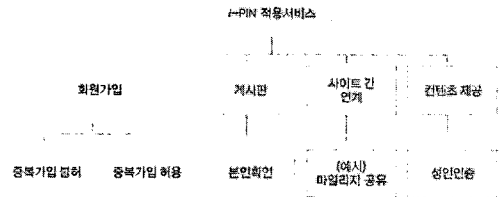
(그림 4) 아이핀 코드의 구성<sup>[10]</sup>

### 3.1.1 아이핀의 동작절차

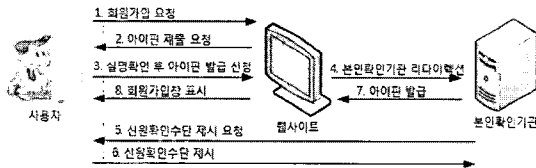
아이핀 서비스의 사용은 아이핀 발급 과정과 아이핀을 이용한 본인인증 과정의 두가지로 구분된다. 사용자는 인터넷 웹사이트에 가입을 할 경우 [그림 2]와 같이 아이핀을 발급받는 과정을 별도로 진행 한 후에 가입을 완료할 수 있으며, 이미 아이핀이 있는 경우 [그림 3]과 같이 별도의 인증 필요시에는 아이핀 식별 아이디와 암호만으로 간편하게 본인인증과정을 진행할 수 있다<sup>[18]</sup>.

### 3.1.3 아이핀 활용 방법

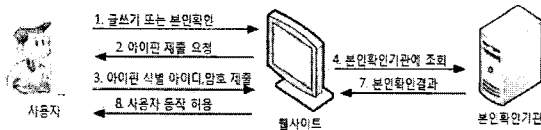
아이핀의 활용 서비스는 회원가입, 게시판, 사이트간 연계, 콘텐츠 제공 연계, 콘텐츠 제공 등으로 구분을 하고 있다.



(그림 5) 아이핀 도입시 적용 서비스의 예<sup>[11]</sup>



(그림 2) 아이핀 발급 과정

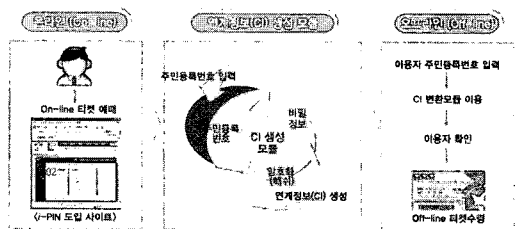


(그림 3) 아이핀을 이용한 본인 확인

아이핀 2.0 서비스에서 도입된 연계정보(Connecting Information)는 사업자간 제휴서비스를 위해 서로 다른 웹사이트 간에도 동일 이용자를 구분할 수 있도록 하였으며, 연계정보가 도입된 아이핀 2.0에서는 주민등록번호를 통해 가입한 경우에도 아이핀과 연계될 수 있도록 지원하고 있으며, 주민등록번호를 연계정보로 변환하는 행위는 사업자 요청 시 본인확인기관에서 제공 한다. 예를들면, 사용자가 A사에서는 아이핀으로, B사에서는 주민등록번호로 가입한 경우, 양 사업자간의 서비스 연계를 위해 사업자가 본인확인기관에 CI를 요청하면 CI 값을 생성해서 전달을 하게 되며 일례로 [그림 6]과 같

### 3.1.2 아이핀 코드 구성

아이핀은 13자리로 구성된 임의의 변수로 개인정보를 포함하지 않는다. 본인확인기관 구별을 위한 2자리를 이용하여 본인확인기관을 구분할 수 있으며, 본인확인기관은 아이핀을 통하여 본인확인기관명, 사용자 이름, 본인확인정보, 중복가입정보, 이용자성별, 이용자나이, 이용자국적, 이용자생일과 등의 정보를 웹서비스에 제공한다.



(그림 6) 연계정보 활용 예<sup>[11]</sup>

이 인터넷을 통해 영화, 항공권등을 예약하고 오프라인에서도 발급이 가능하다<sup>[11]</sup>.

### 3.1.4 본인확인기관 및 웹사이트에서의 사용자 정보 관리 방안

아이핀이 본인확인을 위해 요구하는 기술적 사항들은 다음과 같다<sup>[18]</sup>.

- 실명확인 및 신원확인
- 아이핀 정보의 무결성 및 기밀성
- 중복 가입 방지
- 사용자 편의성

이러한 본인을 확인해 주는 기관들은 국내 총 5개소 각 서비스 기관들과 서비스명은 [그림 7]과 같다.

기관명	서비스명	로고
한국정보인증	Onepass	
한국전자인증	그린버튼	
한국신용정보	나이스아이핀	
한국신용평가정보	가상주민번호	
서울신용평가정보	Siren24 아이핀	

[그림 7] 본인확인기관명 및 서비스 명<sup>[16]</sup>

본인확인기관은 아이핀 서비스를 위해 다음과 같은 개인정보를 보관한다<sup>[16]</sup>.

- 성명
- 주민등록번호
- 본인확인정보
- 전자우편주소

정부는 1년에 1회 이상 본인확인기관에 대하여 개인정보보호를 위한 기술적, 관리적 조치 준수 여부를 점검하고 확인하며, 본인확인기관과 이용자 사이에는 보안 채널(HTTPS)를 이용하여 SSL(Secure Socket Layer) 통신을 통해 보안을 유지한다<sup>[11]</sup>. 웹사이트는 사용자의 주민등록번호를 기존의 사용자 관리 DB에서 삭제하는 대신 본인확인정보(아이핀)와 중복가입확인정보를 추가적으로 삽입하여 사용자 관리 DB를 운용하게 된다.

아이핀을 도입한 사이트는 다음과 같은 정보를 기본적으로 저장하여 관리하게 된다<sup>[16]</sup>.

- 아이핀 인증

- 이용자의 성명
- 생년월일
- 중복가입확인정보
- 성별
- 연령대
- 내외국인 정보

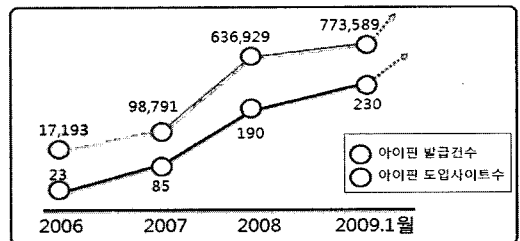
아이핀 서비스에 등록하기 위해서는 신원확인 수단을 제공하여야 하며, 신원확인 수단은 대면확인, 공인인증서, 신용카드, 휴대폰 단문메시지, 법정대리인과 같은 5가지로 구분된다<sup>[16]</sup>.

### 3.1.5 아이핀 도입 방식

아이핀은 게시판에 글을 쓰거나 댓글을 쓸 때 또는 웹사이트에 회원 가입할 때 본인확인용으로 사용 된다. 아이핀을 도입하는 웹사이트는 본인확인기관을 통해서 제공하는 툴킷(Tool Kit)을 설치하고, 현재 사용 중인 DB시스템의 일부 수정만으로 바로 서비스가 적용이 가능하도록 디자인 되었다<sup>[11][19][21]</sup>.

### 3.1.6 아이핀의 적용 현황

아이핀의 적용 현황은 [그림 8]의 그래프를 통해서 확인할 수 있다<sup>[15]</sup>. 2009년 1월까지 아이핀 서비스를 도입한 사이트는 230개, 아이핀 발급 건수는 773,589건으로 향후 2011년까지 도입사이트를 3,000개, 발급건수를 1,000만건을 목표로 진행 되고 있으며, 현재 아이핀 서비스는 2009년 7월 7일부터 2.0으로 업그레이드를 단행하여 서비스를 제공하고 있다<sup>[33]</sup>.



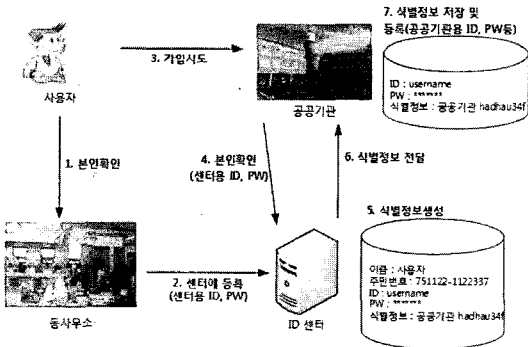
[그림 8] 아이핀 도입 현황 및 발급건수<sup>[15]</sup>

### 3.2 공공 아이핀

공공아이핀 서비스는 행정안전부에서 제공하는 인터넷

넷상의 개인식별번호 서비스이다<sup>[22]</sup>. 행정공공기관에서 인터넷 이용자의 주민등록번호를 대체하는 본인확인 기능으로 행정공공기관과 민간기관간 연계 운영하는 서비스를 일컫는다.

공공아이핀은 행정공공기관에서 별도의 이용요금 없이 이용자를 확인할 수 있는 무료서비스로서 아이핀 서비스를 기본으로 하고 있으나, 본인확인절차시 행정전산서명(GPKI)를 이용할 수 있는 것과 관공서에서 주로 사용되는 차이점이 있다. [그림 9]는 공공아이핀의 일반적인 사용방법을 보여주고 있다. 공공아이핀은 공공기관을 상대로 서비스를 받는다는 것만 제외하면 일반 아이핀과 동일하며, 공공아이핀은 공공기관의 개인정보보호에 관한 법률 제9조의2, 개인정보보호법 제23조, 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제44조의 5, 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제 23조 2에 의해서 시행이 된다<sup>[22]</sup>.



(그림 9) 공공아이핀 서비스의 이용 흐름도<sup>[23]</sup>

#### IV. 아이핀의 문제점

아이핀은 정부의 정책추진 목표와 달리 현재 광범위하게 확산되지 못하고 있다<sup>[34]</sup>. 본장에서는 아이핀 서비스의 문제점에 대한 세부적인 내용들을 분석 및 조사하였다.

##### 4.1 불편한 UI

사용자가 아이핀 사용시 UI상에서 다음과 같은 문제에 직면하게 되며, 사용자의 아이핀 접근시 야기되는 UI 관련 개선되어야 할 관련 사항들은 다음과 같다.

첫째, 사용자 PC보안을 위해서 반드시 키보드 보안 프로그램을 설치해야 하며, 키보드 보안 프로그램을 설

치하지 않거나, ActiveX를 지원하지 않는 브라우저를 사용할 경우 아이핀 서비스의 동작이 보장되지 않는다<sup>[27]</sup>.

둘째, 본인 확인 기관간의 아이디 공유가 되지 않기 때문에 아이핀 확인 아이디, 암호 이외에 자신의 본인확인 기관을 항상 기억하고 있어야 한다. 아이핀 2.0에서 신뢰게이트를 통해 본인확인기관 선택을 자동화 했지만, 아이핀 갱신등과 관련된 작업에서는 아직도 본인이 발급받은 아이핀 기관을 알고 있어야 한다<sup>[17]</sup>.

셋째, 아이핀 서비스는 윈도우 계열의 OS인 인터넷 익스플로어에 최적화된 서비스 형태를 취하고 있어 특정 서비스 플랫폼에 종속적이다. 이외의 OS와 웹브라우저에서는 아이핀의 사용이 아직까지는 불가능하거나 매우 제약적이다<sup>[27]</sup>.

넷째, 본인확인기관별로 서비스의 안정화가 미흡하다. 아이핀은 각 본인확인기관에서 제공하는 툴킷을 이용하여 팝업창을 호출하도록 하고 있는데, 본인확인기관에 따른 기술적 안정화 정도가 다르고, 표준화된 워크플로어가 없어 아이핀 정보관리, 아이핀 신청등의 과정에서 문제를 보여주고 있다.

다섯째, 신원확인시 공인인증기관에서 발급한 유료 공인 인증서만 가능한 점이다. 은행 등에서 발급해주는 무료인증서는 아이핀에서 신원확인수단으로 인정되지 않는 문제점이 있다.

##### 4.2 사용자에 의한 추가 작업 부담

아이핀 서비스를 대부분의 인터넷 웹서비스에서는 기본이 아닌 선택사항으로 분류해 놓고 있다. 아이핀 인증방식이 아직 일반화 되지 않았고, 기존 인증방식과 통합이 불가능한 원인이기도 하지만, 그로 인하여 사용자는 아이핀을 사용하기 위해서 새로운 아이핀 서비스의 가입과 같은 불필요한 행동을 통한 아이핀 발급 과정을 추가적으로 거쳐야 한다. 아이핀으로 단일화 된 아이디 관리 방식에 기존 아이디 관리 방식 기술을 포함하는 새로운 아이디 관리 모델이 필요한 이유가 여기에 있다.

또한, 아이핀 발급 과정에서 본인인증을 위해 별도의 신원확인 수단을 갖고 있어야 한다. 성인이 아닐 경우 대리인이 곁에 있거나 직접 지정된 곳으로 가서 인증을 받아야 하는 번거로움이 있다. 성인이라도 여러 가지 사정으로 공인인증서, 신용카드, 휴대전화와 같은 신원확인 수단이 없을 경우 아이핀 발급이 쉽지 않은 문제점이 있으며, 현재 이와 같은 경우 사용자는 해당 본인확

인기관으로 직접 찾아가서 발급 받는 방법밖에 없다.

#### 4.3 익명성 훼손에 대한 사용자 우려 및 본인확인기관 의 신뢰성 의문

본인 확인기관은 아이핀 서비스의 본인확인 절차를 수행하기 위해 개인의 이름, 주민등록번호, 본인확인정보, 전자우편주소 등을 별도의 DB로 저장한다<sup>[16]</sup>. 기존 웹서비스에서는 각 웹 운영자가 개인정보를 자기 가입자에 한해서 보유하게 되어 있으나, 본인확인기관은 대부분 사용자의 주민등록번호를 보유하게 되는 형태를 취하게 되어 웹상에서 해킹을 통한 유출은 HTTPS와 SSL을 통해서 상당부분 해결될 수 있으나<sup>[1]</sup>, 모든 아이핀 사용자의 주민번호를 5개의 본인확인기관에 분산 저장되어지게 될 경우 외부 유출등에 대한 위험성은 그만큼 커지게 된다.

또한, 본인확인을 하기 위해서 본인확인기관에 항상 사용자 확인절차를 거치는 과정이 필요하기 때문에 아이핀을 적용한 웹사이트에 로그인하거나, 글을 쓸 경우 사용자의 관련 행동에 대한 기록이 본인확인기관에 저장되어 향후 개인의 인터넷 활동에 대한 사생활 침해의 논란을 가져올 수 있다.

#### 4.4 인터넷 사업자의 비용 부담

정부는 아이핀 서비스를 도입하는 기업에게 일정부분 도입비용을 제공하는 방법을 사용하고 있으나, 도입비용은 실제 웹서비스의 규모에 따라서 큰 차이를 갖고 있다. 최문순 민주당 의원은 2008년 9월 방송통신위원회에 대한 국정감사에서 인터넷 사업자들이 아이핀에 적극적으로이지 않은 이유로 비용 문제를 언급했고, 아이핀으로 전환할 경우 업체의 규모에 따라 500만원에서 11억원까지 비용이 들어간다는 분석을 발표하였다<sup>[20][24]</sup>.

방송통신위원회에서는 실제 아이핀을 도입한 포털, 게임등의 업체를 통해서 조사한 결과 기존 시스템 변경을 위한 분석과 개선에 중급기술자 4명이 1개월간 투입되어 약 2천만원 정도 소요되었다고 발표하였다<sup>[11]</sup>. 하지만, 구체적인 근거가 부족하고, 각 회사들마다 처한 환경이 다르기 때문에 단순한 평균값을 통한 비용산출은 근거가 미약하다.

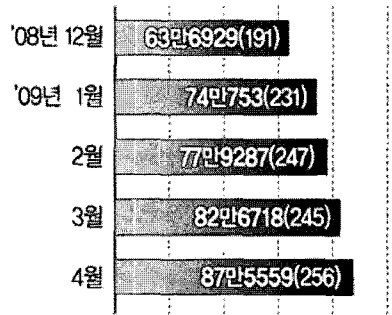
아이핀의 운영 비용은 초기 도입 시에만 투입되는 것이 아니라, 운영하는 동안 지속적으로 발생한다. 본인확

인 인증을 받기 위해서 한국신용평가정보 등 본인확인기관에 건당 16~60원의 수수료가 부가되는 등 본인확인기관에 접속하는 비용 때문이다<sup>[25]</sup>. 이에 방송통신위원회에서는 아이핀을 도입한 사이트들의 경우 이용자수에 따른 인증비용이 연 100만원 이내라고 발표하였다<sup>[11]</sup>. 그러나 아이핀의 사용자가 적은 현재 시점의 소요 비용이기 때문에 아이핀의 적극적인 도입이 이뤄진 후에는 그 이상의 비용소요가 될 것은 쉽게 예측이 가능하다.

#### 4.5 홍보 부재로 인한 사용자 인식 부족

한국정보보호진흥원이 2008년 9월 16일 국회 문화체육관광 방송통신위원회 소속 한나라당 최구식 의원에게 제출한 “아이핀 이용현황 실태조사 보고서”에 따르면 아이핀 서비스를 채택한 Naver와 Daum에서 아이핀의 이용률을 조사한 결과 각각 0.2%에 불과한 것으로 나타나고 있다<sup>[35]</sup>. [그림 10]에서 2009년 1월 이후로 아이핀의 누적 발급건수의 증가가 월 200건밖에 되지 않으며, 2008년 아이핀 발급 캠페인이 끝난 직후로 실질적 증가가 둔화된 것을 알 수 있다<sup>[26]</sup>.

민간기업 아이핀 발급건수 (단위 : 건)



※ ( )안은 사이트수, 개      자료 : 정보보호진흥원

(그림 10) 아이핀 가입자 현황(2008)<sup>[26]</sup>

업체의 아이핀에 대한 이해 및 도입의사는 매우 부정적임을 알 수 있으며, 아직까지는 홍보 및 도입에 따른 장점을 업계조차 제대로 인식하지 못하고 있기 때문으로 추정된다[표 1].

최근 지상파 방송에서 정부의 아이핀 홍보가 시작되었으나, 사용자의 적극적인 참여 의지를 고취시키기

는 광고내용이 너무 포괄적이며, 특히, 사용자가 아이핀을 사용하게 될 인터넷상의 웹서비스 제공자들에 의한 홍보 및 계도가 제대로 이뤄지지 않고 있다.

(표 1) 업계의 아이핀 도입 관련 현황(KISA 2009. 8. 1)<sup>[25]</sup>

(단위: %)

보기	업체구분				회원수	
	포털 (14)	게임 (8)	전자상 거래 (13)	기타 (29)	500만 미만 (39)	500만 이상 (25)
현재로서는 도입계획 없음	64.3	62.5	61.5	72.4	74.4	56.0
도입을 위한 사전 검토중	28.6	25.0	30.8	17.2	15.4	36.0
기타	7.1	12.5	7.7	10.3	10.3	8.0
전체	100.0	100.0	100.0	100.0	100.0	100.0

#### 4.6 정부 지원 재정의 부족

2007년 정부는 아이핀 서비스 관련 500억원의 예산을 책정하였으나, 2008년과 2009년에는 각각 343억원으로 정부 예산지원 금액을 삭감하였다. 실제 이들 예산 중에 아이핀 관련 직접지원 예산은 훨씬 더 적게 배정이 되었다<sup>[24]</sup>.

2009년 아이핀 정책설명회 및 개인정보의 기술적 관리적 보호조치 기준 개정공청회에서도 정부의 예산지원에 대한 부분은 언급이 되지 않고 있다. 2009년도 행정안전부 정보화 예산으로 성립된 350억원중 실제 개인정보보호 대책 강화와 공공기관 웹사이트 개인정보 상시 모니터링, 주민번호 대체 수단(아이핀)보급을 위해 책정된 금액은 31억원으로 상반기에 조기 투입한다는 계획만 수립되어 있었다<sup>[28]</sup>. 지난해 국회 예산 정책처 한나라당 이성원 의원에 따르면 아이핀의 실제 적용사이트는 18개의 사이트에 평균 인증비율은 7.3%에 그쳤다고 한다. 이의원은 정부의 관련 예산을 2008년 51억여원의 10배 이상 늘려야 한다고 주장한 바와 같이 아이핀 도입이 미진한 원인 중 가장 큰 원인은 정부의 아이핀 정책 예산이 실제로 적게 배정되어 효과적인 결과를 도출하지 못하고 있는 것이다<sup>[29]</sup>.

#### 4.7 국제적 활용 방안 정립 필요

아이핀 서비스는 국내에서 2015년을 기점으로 모든

웹사이트가 도입해야 하는 개인 아이디 관리 모델로서 국가에서 정책적으로 아이디 관리 모델을 설정하고 추진하는 것은 세계적으로 찾아보기 힘든 사례이다<sup>[26]</sup>.

이러한 일원적인 아이디 관리 모델의 적용은 다국어 웹서비스 개발시 어떤 아이디 관리 모델을 선택해야 할 것인가와 같은 논란을 일으키고 있다. 즉, 국내에 기반한 웹서비스 제공자의 경우 다국어버전으로의 웹페이지 구성시, 아이핀을 사용하는 국내사용자와 아이핀을 사용하지 않는 해외 사용자들을 위한 가입, 인증서비스에서 각각 다르게 대응해야 하는 문제점이 발생한다. 예를 들면, 국내 사용자가 영어로 만들어진 사이트에서의 로그인을 필요로 할 경우에 사용자가 아이핀 방식과, 해외 사용자를 위한 방식중 하나를 선택하도록 해야 하고 이에 따른 별도의 기술적 관리 프로세스와 추가 시스템 보완 등에 따른 리소스의 소비가 발생한다.

해외 웹서비스 제공자가 국내에 진출할 경우 아이핀 서비스를 도입해야 할지, 기존 자사의 아이디 관리 모델을 그대로 적용해야 할지를 선택해야 하는 문제점이 발생하게 되어 실제 유튜브(www.youtube.com)의 경우 실명제에 대한 국내 법적제약을 회피하기 위해 한국 사용자의 경우에는 댓글쓰기를 원천적으로 막아버렸던 사례가 있었다<sup>[30]</sup>. 즉, 해외 웹서비스의 국내 진출시 적절한 로그인 해결 방법을 찾지 못할 경우 로그인이 필요한 서비스를 막거나, 편법적인 방법을 동원하거나, 아예 국내 진출을 포기하는 경우가 발생할 수도 있다.

아이핀 서비스 형태를 다양한 아이디 관리 모델 들을 포용하는 방향으로 확대 개편하는 인증모델로 확장을 통하여 국제적 활용도를 제고한 위상을 갖추도록 해야 한다<sup>[9]</sup>. 개인주민등록번호 관리에 국한된 아이디 관리 모델이 아닌 국내 아이핀 아이디관리 서비스와 외국의 다양한 아이디 관리 모델을 모두 통합하여 활용 가능한 새롭고 확장된 아이디 관리 모델의 정립을 통해, 정부와 관련업계 등에서 이러한 문제점을 근본적으로 해결 할 수 있는 방안을 제시해야 한다.

#### 4.8 오프라인에서의 주민등록번호의 지속적 활용

아이핀 서비스의 주된 목적은 주민등록번호의 유출을 막는 것이나 주민등록번호의 유출은 온라인상에서만 발생하는 것이 아니라, 실제로 오프라인상에서의 유출이 더욱 심각하다<sup>[12]</sup>. 이렇게 유출된 주민등록번호를 통해서 아이핀 서비스에 가입하려고 할 경우 뚜렷한 제재

방법의 마련이 쉽지 않은 게 사실이다.

결국, 아이핀의 적극적인 도입 이전에 개인주민등록번호 관리 정책 및 관리체계를 개선하지 않으면 아이핀의 도입을 통한 근본적인 문제해결은 이뤄지기 어렵다.

V. 아이핀의 주요문제 해결방안

위에서 살펴본 문제점들에 대한 개별적인 대응방안들은 [표 2]와 같다.

아울러, 본 논문은 아이핀 활성화 방안을 3가지 측면

[표 2] 아이핀의 문제점과 대응방안

문 제 점	대 응 방 안
불편한 UI	<ul style="list-style-type: none"> <li>○ 본인확인기관 인증코드를 이용한 SSO 서비스 구현</li> <li>○ 본인확인기관별 인증 페이지 콜이 아닌 동일한 인증페이지 제공 또는 웹사이트 특색에 맞는 인증페이지 개발을 위한 API 제공</li> <li>○ 정형화된 작업 플로어 개발 및 서비스 안정화</li> <li>○ 서비스 환경 최적화를 통한 속도 향상</li> </ul>
사용자의 추가작업 부담	<ul style="list-style-type: none"> <li>○ 사용자 인증 방식을 아이핀으로 단일화하여 별도의 아이디 관리 모델유지를 위한 비용 절감 및 연계정보(CI)를 활용한 온오프라인 연계 방안 제시</li> <li>○ 본인인증절차의 간편화 필요</li> </ul>
개인정보 유출 부담	<ul style="list-style-type: none"> <li>○ 본인인증기관의 개인 기록 보관 금지 범안 모색</li> <li>○ 주민등록번호를 보안인증기관이 아닌 정부관할 DB에 저장하고 본인인증기관에 서비스 조회를 통한 열람방식으로의 변경검토 필요</li> <li>○ 실명인증 이외에 로그메타저장 금지</li> <li>○ 개인정보에 대한 본인인증기관의 활용범위 제한</li> </ul>
아이핀 비용 부담	<ul style="list-style-type: none"> <li>○ 정부의 아이핀 도입비용 적극적인 예산지원 필요</li> <li>○ 아이핀 사용비용에 대한 한시적 지원 필요</li> <li>○ 아이핀 사용비용의 최소화 필요</li> </ul>
홍보 부족	<ul style="list-style-type: none"> <li>○ 정부의 아이핀 홍보 지원</li> <li>○ 서비스업체의 아이핀 채용시 인센티브 제공</li> </ul>
정부의 재정지원	<ul style="list-style-type: none"> <li>○ 아이핀 관련 예산 증액 필요(관련 연구개발비)</li> <li>○ 아이핀 전담 부서 확충 및 전담 연구기관 설정을 통한 지속관리체계 확보</li> </ul>
글로벌 표준화 필요성	<ul style="list-style-type: none"> <li>○ 아이핀 서비스에 대한 일반사업자의 참여 활성화</li> <li>○ 아이핀 서비스에 대한 정부의 참여 최소화</li> <li>○ 아이핀 포럼등의 구상을 통한 외부 기업들의 참여 활성화 및 제안등 적극 수렴</li> <li>○ 주민등록번호가 아닌 아이디 관리 모델로 확장을 도모 할 표준화 제정 필요</li> </ul>
주민번호 정책 제고	<ul style="list-style-type: none"> <li>○ 주민번호 정책의 개선이 필요</li> <li>○ 일반 민간기업의 주민번호 사용을 금지, 또는 최소화 하는 법적 체계 마련 시급</li> </ul>

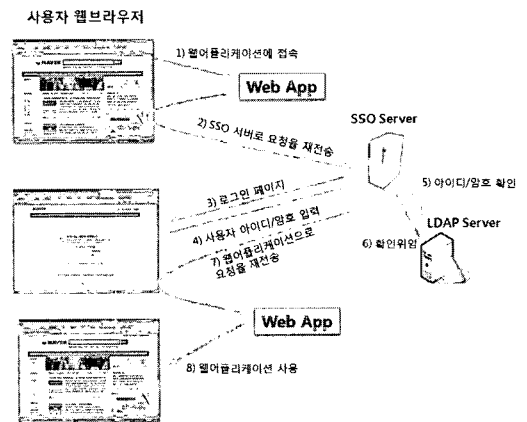
에서 연구하여 분석 정리하고 아이핀의 활성화에 필요한 사항을 아래와 같이 시스템적인 측면, 비용절감의 측면, 정부정책적인 측면에서의 제안내용을 기술하고자 한다.

[표 3] 아이핀의 문제점과 대응방안(요약)

관점	해결방안
시스템 측면	<ul style="list-style-type: none"> <li>○ SAML<sup>[6]</sup>을 이용한 SSO 구현 및 SAML assertion을 이용한 이기종간 아이디 변환 서비스 관리 모델 제안</li> <li>○ ActiveX의 능동적 적용으로 다양한 플랫폼 지원</li> </ul>
비용절감 측면	<ul style="list-style-type: none"> <li>○ 아이핀의 적극적 도입을 위한 운영 재정 지원</li> <li>○ 웹서비스 사업자의 아이핀 운영 비용 최소화</li> <li>○ 아이핀 의무도입 웹서비스 분류를 통한 아이핀 활성화 및 사회적 비용 최소화</li> </ul>
정부정책 지원방안	<ul style="list-style-type: none"> <li>○ 아이핀의 적극적인 홍보와 교육 지원</li> <li>○ 관련 정책 목표 달성을 위한 산학연 구심체로서의 역할</li> <li>○ 정부주도형에서 민간주도형으로의 변화 필요</li> </ul>

5.1 시스템 측면에서의 해결방안

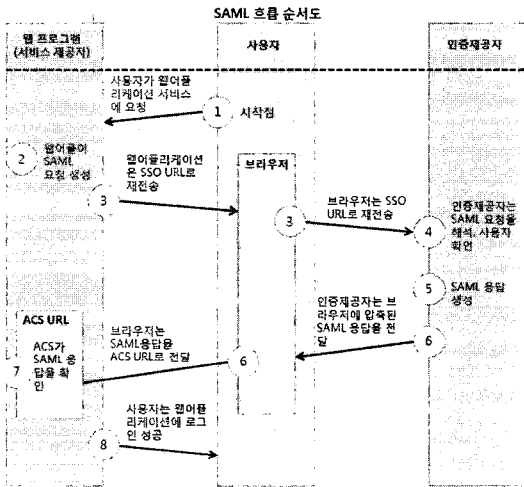
아이핀 서비스 이용 방식을 본인확인기관이 아닌 규격화된 표준화 정책을 추진하여 기술적인 통일성을 찾으려 하기 위해 국제 표준인 SAML(Security Asserting Markup Language)을 이용한 아이핀 아이디 관리 모델을 제안한다. [그림 11]처럼 웹서비스에 로그인 할 경우 다른 서비스에서 별도의 로그인 없이도 서비스를 사용할 수 있는 SSO(Single Sign On) 서비스가 구현되어야 한다<sup>[20]</sup>.



[그림 11] SSO 서비스 시퀀스<sup>[31]</sup>



SSO<sup>[8]</sup>는 SSO Server를 배치함으로써 이러한 시스템적 문제를 해결할 수 있다. SAML(Security Asserting Markup Language)은 웹브라우저 상에서의 SSO의 구현을 위해 고안된 언어로 시스템 구축으로 구현이 가능하다<sup>[32]</sup>.



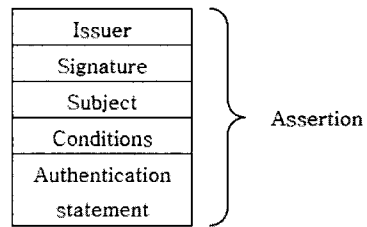
(그림 12) SAML을 이용한 SSO의 시퀀스 다이어그램<sup>[5]</sup>

위 [그림 12]의 전개 과정은 다음과 같다

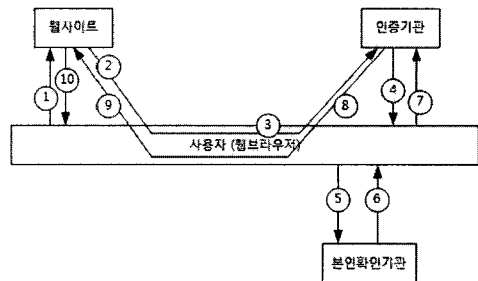
- 1단계 : 유저는 서비스 제공자(Service Provider)에게 서비스 이용을 위하여 접근한다.
- 2단계 : 서비스 제공자는 SAML Request를 생성하며, SAML Request는 XML format 텍스트로 구성된다.
- 3단계 : 유저의 브라우저를 이용하여 인증 제공자(Identity Provider)로 Redirect 한다.
- 4단계 : 인증 제공자(Identity Provider)는 SAML Request를 파싱하고 유저인증을 진행한다.
- 5단계 : 인증제공자(Identity Provider)는 SAML Response를 생성한다.
- 6단계 : 인증제공자(Identity Provider)는 유저 브라우저를 이용하여 SAMLResponse data를 ACS로 전달한다.
- 7단계 : ACS는 Service Provider가 운영하게 되는데 SAMLResponse를 확인하고 실제 서비스 사이트로 유저를 Forwarding한다.
- 8단계 : 유저는 로그인에 성공하고 서비스를 제공

받는다.

SAML을 이용할 경우 아이핀을 좀 더 일반화된 아이디 관리 모델로 확장을 할 수 있으며, 본 논문에서는 SAML의 assertion<sup>[4]</sup>을 활용한 통합 아이디 관리 모델을 제안한다. SAML assertion은 SAML authority(예: Identity provider)에 의해서 만들어진 하나 이상의 statement를 제공하는 정보패키지로서 인증, 속성, 권한부여 결정 또는 사용자가 정의한 statement를 나타내며 Assertion의 구조는 다음과 같다.



(그림 13) SAML 구조



(그림 14) 기본 아이디 정보 관리 모델

[그림 14]와 같이 SAML을 활용한 아이핀의 기본 정보관리모델 유형은 다음과 같다<sup>[2][3]</sup>.

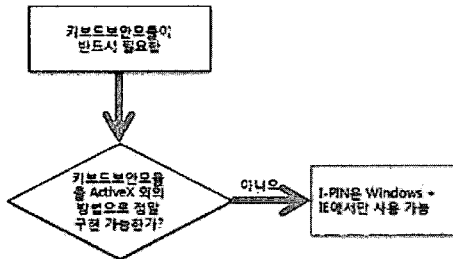
- 1단계 : 사용자가 웹사이트에 접속 요청을 한다.
- 2-3단계 : 웹사이트는 자신이 신뢰하는 인증기관으로 사용자를 재접속 시킨다.
- 4단계 : 사용자가 해당 인증기관에서 제공하는 인증서가 없을 경우, 인증기관은 자신이 보유하고 있는 신뢰하는 인증기관 목록을 사용자에게 전송한다.
- 5단계 : 사용자는 인증기관의 목록에서 자신의 프로파일을 저장하고 있는 본인확인기관에 요청을 해서 username/password로 인증을 받는다.
- 6단계 : 본인확인기관은 인증 결과를 SAML

assertion 형태로 변환하여 사용자에게 전달한다.

- 7단계 : 사용자는 인증서/SAML assertion을 처음에 목록을 준 인증기관에 전달한다.
- 8단계 : 인증기관은 인증서/SAML assertion을 검토하고 문제가 없다면 웹사이트로 전달을 한다.
- 9단계 : 사용자는 인증기관으로부터 받은 token을 갖고 웹사이트로 이동을 한다.
- 10단계 : 웹사이트는 인증서를 검토하고 사용자가 요청한 리소스를 제공한다.

이상의 서비스 모델은 본인확인기관이 직접적인 인증기관이 되거나, 다른 기술을 사용하는 인증기관과 웹사이트의 경우에는 username/password값을 이용하여 인증을 받고, 그 결과를 SAML assertion을 통해서 전달받음으로써, 기존의 아이디 관리 모델과 아이핀의 아이디 관리 모델이 동시에 연동될 수 있는 방법을 제공할 수 있게 된다.

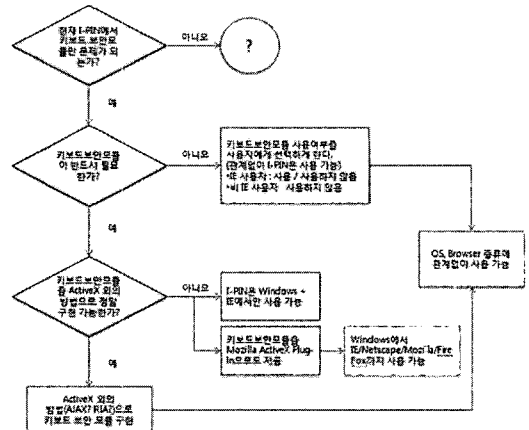
그리고 아이핀은 해킹 등의 문제점을 극복하기 위해 [그림 15]과 같은 흐름으로 키보드 보안을 위한 ActiveX의 기술을 사용하고 있다.



(그림 15) 현재의 ActiveX를 이용한 아이핀 서비스

ActiveX기술이 해킹을 차단시키는데 매우 효율적이라 하여도 웹서비스가 특정 플랫폼에 종속되는 결과를 가져오게 된다. ActiveX가 아닌 범용적인 기술을 적용하거나, 다른 플랫폼 사용자도 삼용이 원활하도록 하는 방법이 필요하여 본 논문에서는 다양한 서비스 플랫폼에 대응할 수 있는 키보드 보안 서비스 모델을 다음과 같이 제안한다. [그림 16]에서는 사용자의 서비스 환경에 맞게 ActiveX나 Ajax나 RIA와 같은 기술을 동적으로 결정하여 실행하도록 하는 서비스 모델이다.

또한, 아이핀을 발급받기 위해서는 실명 인증이 필요하다. 하지만, 청소년이나, 특정한 서비스(휴대전화 등)



(그림 16) 비ActiveX 환경을 고려한 ActiveX 사용방법

를 사용하지 않는 사용자의 경우에는 아이핀을 발급 받는 행위 자체가 불편할 수 있다. 17세 미만의 청소년의 경우 인증서, 휴대전화와 같이 인증을 쉽게 할 수 있는 환경을 갖고 있지 못할 수도 있는 경우, 아이핀을 발급받기 위하여 직접 방문하여 발급신청을 하는 수 밖에 없다. 일반인의 경우에도 인증을 위한 방법을 갖추고 있지 않은 경우가 있기 때문에 현실적으로 쉽게 발급받을 수 있도록 하는 방안이 필요하여, 현재 실명인증이 가장 쉽게 이뤄질 수 있는 동사무소나 금융기관 등을 통해서 이러한 아이핀 발급을 쉽게 받을 수 있도록 각 관련 기관과의 협력이 필요하다.

### 5.2 비용 절감 측면에서의 해결방안

기존 주민등록번호를 이용한 방식을 아이핀으로 변경은 웹서비스를 운영하는 운영자 입장에서는 추가적인 큰 비용이 발생할 수도 있는 부분이다. 정부는 이러한 부분에 대한 적극적인 지원을 통해서 가급적 많은 웹서비스 사업자가 아이핀을 도입할 수 있도록 도입 문턱을 낮추는 재정적인 지원이 시급하다.

사업자의 초기 아이핀 도입시 뿐만 아니라 아이핀을 운용 중에도 지속적인 비용이 발생하게 된다. 아이핀 정책은 사용자 정보의 유효성을 로그인이나 댓글을 쓸 때 마다 항상 확인되어야 하고, 이러한 확인을 위하여 본인확인기관과의 상호간 트래픽(Traffic)을 필요로 한다. 이러한 트래픽에 대해서 본인확인기관에 지불하는 비용과 네트워크 구성 비용은 웹서비스의 규모가 커질수록 비례적으로 커지게 된다. 하지만, 아이핀 서비스의 도입

목적을 고려할 때 이러한 비용을 정부에서 지원하거나 정부에서 본인확인기관에 직접 지원함으로써 웹서비스 제공자의 비용부담을 줄여주어야 많은 웹서비스 사업자의 아이핀 정책에 참여를 유도할 수 있다.

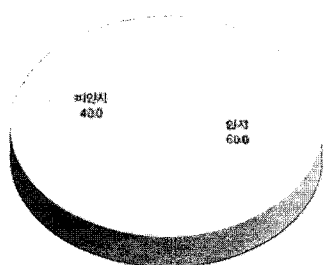
아이핀 서비스가 필요한 웹서비스, 권장하는 서비스, 필요로 하지 않는 서비스를 각각 구분하여 모든 웹서비스 사업자들이 초기 사업을 시작할 때 투입되는 불필요한 비용을 지불하지 않도록 할 필요성도 있다. 현재 추진되는 정책의 기준은 단순히 10만 사용자의 경우 아이핀의 도입을 의무화하려고 하지만, 예를들면 블로그의 경우 접속인원이 10만 이상이라는 이유로 아이핀을 도입하려 한다면 정책 추진시 현실적으로 곤란한 문제에 직면 하게 된다.

따라서, 사용자(가입자)의 수, 실명제 추진정도, 로그인 수 등에 따라서 웹서비스 제공사업자의 자율정책에 의한 아이핀 적용 선택을 일정수준의 아이핀 정책 확산 시 까지 유예 등으로 배려해 줄 필요가 있다.

### 5.3 정부의 정책적 지원 측면

아이핀의 홍보는 아이핀의 실제 사용에 커다란 영향을 주게 된다. 한국정보보호진흥원(KISA)의 2008년 실태조사 개인편에서 조사한 결과에 따르면, 아이핀이나 공인인증서등과 같은 주민번호대체수단의 인식률은 60%정도로 나타났다<sup>[14]</sup>.

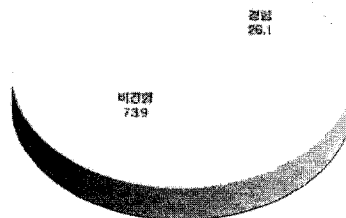
인터넷 서비스 회원가입 시 주민번호 이외 수단 인지도



(그림 17) 주민번호대체수단 인식률<sup>[14]</sup>

또한, 개인정보유출에 대한 예방수단과 유출 후 사후 조치에 대해서는 아래와 같이 73.9%만이 대응에 대한 경험이 있는 것으로 나타났다.

개인정보/프라이버시 침해에 대한 관련기관 문의여부



(그림 18) 개인정보침해에 대한 대응 경험<sup>[14]</sup>

아울러 정부는 인터넷 환경에서 사용자들이 아이핀 서비스를 적극적으로 사용할 수 있게 하기 위해서는 개인정보의 보호에 대한 인식제고와 함께 개인정보보호를 위한 방법 등에 대한 홍보와 교육을 통하여 아이핀에 대한 실질적인 사용자 증대를 가져올 수 있음을 인지해야 한다<sup>[15]</sup>.

또한, 주민등록번호의 대체수단인 아이핀에 대해서는 76.2%, 명의도용방지 서비스에 대해서는 50%가 모르고 있으며 유출된 개인정보에 대한 삭제요청 및 침해 신고 방법을 모르는 비율도 73.9%에 이르고 있다<sup>[15]</sup>.

이러한 결과는 정부가 아이핀과 기타 관련된 사업들에 대해서 적절한 정책 홍보를 하고 있지 않기 때문이며, 아이핀을 도입한 웹서비스 업체들도 아이핀의 사용을 적극적으로 홍보하기보다 정부의 시책에 동참하는 수준에 머무르고 있기 때문으로 해석된다.

따라서 정부는 아이핀의 홍보를 위해서 다음과 같은 방법으로 사용자들의 자발적인 참여를 이끌어 내야 한다.

- 홍보를 위한 국가 예산 배정 및 집행
- 일반 네티즌들의 참여 유도
- 방송, 대중교통수단, 신문등을 통한 지속적인 홍보
- 아이핀의 기술에 대한 접근 및 적용을 쉽게 하기 위한 기술자/연구자들을 위한 커뮤니티 마련
- 다양한 이벤트와 세미나를 통한 아이핀의 지속적 관심 유발

마지막으로 정부는 아이핀 서비스를 확대 보급하기 위해서 산업체, 학계, 연구계 등에 대한 정책 연대와 지속적인 관련 예산의 지원 등을 통한 관계관리 강화를

통하여 아이핀 서비스 보급 정책이 성공리에 운영되어 모든 국민이 안전하게 인터넷을 활용하고, 관련 산업이 발전 될 수 있도록 정책 추진이 필요하다. 또한 국가산업 전반의 정부주도형 개인인증체계를 민간 주도의 인증체계로 전환을 모색하여 정부는 관련 규제 정책 목표를 설정 운영하면서 핵심 정보를 제공하는 인터페이스를 제공하고, 실제 사업의 주체와 방향을 민간에서 주도하여 연구개발의 확대를 통한 아이핀 서비스의 고도화와 확산을 도모할 수 있으며, 정부주도로 인해서 인터넷에서 개인사생활 등을 정부가 관리한다는 비판 등을 피해나갈 수 있다.

## VI. 결 론

아이핀 서비스 정책은 사용자에게는 제5장에서 제시된 SSO(Single Sign On)의 실현 및 안전한 인터넷 웹 서비스 이용 환경을 제공할 수 있으며, 웹서비스 제공자 입장에서는 다양한 사용자 중심의 서비스 도입을 통해 많은 사용자들을 손쉽게 유입하여 폭 넓은 서비스를 제공할 수 있는 환경을 부여받을 수 있는 개인정보보안 및 실명인증 솔루션이다.

정부의 정책 목표 달성을 위한 아이핀 서비스의 확산과 안정된 정착을 위해서 본 논문에서는 아이핀 서비스 정책의 발전과 확대 배포 및 고도화 등을 위한 연구개발, 관련 홍보 등을 위한 정부 정책 재정의 확보가 긴요하며, 주민등록번호 등 개인의 실명 정보 집중에 따른 다양한 법적 제도를 완비해서 사용자들이 아이핀 서비스 정책을 믿고 사용할 수 있도록 주변 환경을 개선해야 함을 지적하였다. 또한, 정부주도 형태에서 민간주도 형태로의 전환을 모색하여 더 많은 사용자들이 참여해서 정부의 정책 목표에 부합하는 인터넷 환경의 변화가 이뤄지도록 기반을 조성해야 하며, 웹서비스 제공사업자들의 적극적인 동참을 위한 정책 환경을 조성하여 자발적인 참여를 유도하고, 그간 익명성과 개인정보유출로 인해 발생하는 사회적 문제점 해소를 통하여 인터넷 이용자들의 안전성을 확보하게 하여 IT산업 전반에 건전한 발전을 도모하기 위하여 아이핀 서비스 도입 정책은 적극적으로 추진 되어야 한다.

그리고 웹서비스 제공사업자들은 아이핀이 좀 더 쉽게 발급되고 사용될 수 있는 기술개발 및 연구 활동을 통하여 다양한 플랫폼에 맞는 관련 기술이 인터넷 환경에 적용 되도록 정부와 협력하고 적극 노력해야 한다.

아울러, 사용자들은 정부의 정책에 대한 신뢰감을 갖고 아이핀 서비스 도입에 주도적으로 참여해야 하며, 이를 통하여 개인 정보의 유출과 불법사용 등을 통한 많은 개인과 사회적 피해를 사전에 예방할 수 있다는 신뢰를 가져야 한다.

마지막으로 아이핀을 단순히 국내 환경에 국한된 단편화된 기술이 아닌 전 세계적으로 사용이 가능할 수 있도록 아이핀의 목적성을 단순화하고, 국내의 제삼의 상이한 ID관리 시스템 등과의 호환성을 고려한 기술 연구가 추진되고, 개발 지원 되어 많은 국내외 인터넷 상의 웹서비스 플랫폼에서 아이핀 서비스를 활용할 수 있도록 아이핀의 국제화 등을 위한 지속적인 노력이 필요하다.

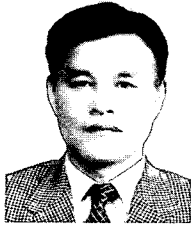
## 참고문헌

- [1] 손태식, 서정우, 문중섭, 서정택, 임을규, 이철원, “안전한 보안패치 분배 구조의 설계 및 구현”, 정보보호학회논문지, pp. 47-62, 2003. 8.
- [2] Ouri Wolfson, Sushil Jajodia, and Yixiu Huang, “An adaptive data replication algorithm”, *ACM Transactions on Database Systems*, 22(2), pp. 255-314, 1997.
- [3] Thanasis Loukopoulos and Ishfaq Ahmad, “Static and adaptive distributed data replication using genetic algorithms”, *Journal of Parallel and Distributed Computing*, 64(11), pp. 1270-1285, 2004.
- [4] Gross, T, “Security analysis of the SAML single signon browser/artifact profile”, *Computer Security Applications Conference 2003, Proceedings. 19th Annual*, pp. 298-307, 2003.
- [5] Michael Fleming Grubb and Rob Carter, “Single Sign-On and the System Administrator”, *Proceedings of the Twelfth Systems Administration Conference(LISA'98)*, 1998.
- [6] OpenSAML, “Open Source SAML Implementation”, <http://www.opensaml.org>.
- [7] SAML V2.0 Executive Overview, Committee Draft 01, 12 2005.4
- [8] Jan De Clercq, “Single Sign-On Architectures”, *Proceedings of the International Conference on*

*Infrastructure Security table of contents, pp. 40-58, 2002.*

- [9] Hristo Koshutanski, Mihaela Icon, Luigi Telesca, "Distributed Identity Management Model for Digital Ecosystems", *Emerging Security Information, Systems, and Technologies, 2007. SecureWare 2007. The International Conference on, 2007.* 8.
- [10] 진승현, "Digital Identity Management for Privacy Protection", *한국전자통신연구원, 2008.* 6.
- [11] 방송통신위원회, 한국정보보호진흥원, "i-PIN 2.0 도입 매뉴얼", 2009. 7.
- [12] 서종표, "가상공간에서의 개인정보보호", *전남대학교 법학과, 2005.*
- [13] 이강신, "개인정보 피해사례, 대책, 그리고 KISA 역할소개", *한국정보보호진흥원 기업정보보호 우수사례 벤치마킹 워크샵, 2008.* 4.
- [14] 한국정보보호진흥원, "2008 정보보호 실태조사", *한국정보보호진흥원, 2009.*
- [15] 방송통신위원회, "i-PIN 정책 설명회 및 [개인정보의 기술적·관리적 보호조치 기준] 개안(안) 공청회" 자료집, *한국정보보호진흥원, 2009.*
- [16] 한국정보보호진흥원, "개인정보보호와 i-PIN", *개인정보보호 시리즈, 8, 2007.*
- [17] 한국정보보호진흥원, "사례를 통해 알아보는 I-PIN", 2007.
- [18] 이재진, 손병록, 구자현, "전자 ID지갑 시스템 기반의 i-PIN 고도화 기술 개발 및 구현", *한국정보보호진흥원 최종보고서, 55, 2007.*
- [19] 한국정보보호진흥원, "i-PIN 도입매뉴얼", 2007.
- [20] 방송통신위원회 개인정보보호과, "인터넷상 주민등록번호 대체수단(i-PIN)활성화 종합대책(안)", *방송통신위원회, 21, 2009.* 3.
- [21] 한국정보보호진흥원, "인터넷상의 주민번호 대체수단 가이드라인", *한국정보보호진흥원 i-PIN 자료실, 2007.*
- [22] 공공 I-PIN센터, <http://www.g-pin.go.kr>.
- [23] 디지털데일리, "공공기관 홈페이지, 주민번호 없이도 회원가입 가능", [http://www.ddaily.co.kr/news/news\\_view.php?uid=43954](http://www.ddaily.co.kr/news/news_view.php?uid=43954), 2008.
- [24] 보안뉴스, "인터넷사 아이핀 전환비용 대책 마련해야", <http://www.boannews.com/media/view.asp?idx=11796&kind=1>, 2008. 10.
- [25] 보안뉴스, "아이핀 의무화강화, 사업자의 부담만 키워", <http://www.boannews.com/media/view.asp?idx=11873&kind=1>, 2008. 10.
- [26] 파이낸셜뉴스, "주민번호 대체 아이핀을 아시나요?", [http://www.fnnews.com/view?ra=Sent0701m\\_View&corp=fnnews&arcid=090531220442&cDateYear=2009&cDateMonth=06&cDateDay=01](http://www.fnnews.com/view?ra=Sent0701m_View&corp=fnnews&arcid=090531220442&cDateYear=2009&cDateMonth=06&cDateDay=01), 2009. 06.
- [27] 디지털타임스, "업계 외면 아이핀 활성화 난항", [http://www.dt.co.kr/contents.html?article\\_no=2008010102011760713002](http://www.dt.co.kr/contents.html?article_no=2008010102011760713002), 2008. 01.
- [28] 디지털데일리, "내년 정보보호사업예산 350억원 조기 집행", [http://www.ddaily.co.kr/news/news\\_view.php?uid=45435](http://www.ddaily.co.kr/news/news_view.php?uid=45435), 2008. 12.
- [29] 보안뉴스 "개인정보보호 예산, 연평균 40.6% 증가해왔지만", <http://www.boannews.com/media/view.asp?idx=10385&kind=1>, 2008. 06.
- [30] 오마이뉴스, "실명제 전투, 구글과 방통위 가운데 승자는?", [http://www.ohmynews.com/NWS\\_Web/view\\_at\\_pg.aspx?CNTN\\_CD=A0001126545](http://www.ohmynews.com/NWS_Web/view_at_pg.aspx?CNTN_CD=A0001126545), 2009. 05.
- [31] Isrus, [http://www.isrus.com/so\\_it\\_solution\\_googleapps\\_sso.php](http://www.isrus.com/so_it_solution_googleapps_sso.php).
- [32] Sun Developer Network 공식 블로그, <http://blog.sdnkorea.com/blog/501>.
- [33] 디지털데일리, "주민번호 대체수단 '아이핀(i-PIN)', 편의성 대폭 개선", [http://www.ddaily.co.kr/news/news\\_view.php?uid=51718](http://www.ddaily.co.kr/news/news_view.php?uid=51718), 2009. 7. 6.
- [34] 이투데이, "실패한 정책 '아이핀'에 정부가 집착하는 이유?", <http://www.e-today.co.kr/news/section/newsview.php?TM=news&SM=0502&idxno=239710>, 2009. 7. 7.
- [35] 동아닷컴, "네이버-다음, 아이핀 이용률 0.2%", <http://news.donga.com/fbin/output?n=200809170044>, 2008. 9. 17.

## 〈著者紹介〉

**장인용 (In-Yong Jang)**

## 정회원

1985년 2월: 명지대학교 공과대학  
전자공학과 졸업(학사)

1995년 2월: 명지대학교 정보산업  
대학원 정보통신공학과(석사)

2009년 2월: 순천향대학교 일반대  
학원 정보보호학과 박사과정 수료

1982년~1990년 2월: 한국통신 전  
자교환운용연구단

1990년 2월~1994년 3월: 한국통신  
중앙연수원 교수실 교수

1994년 3월~1997년 3월: 한국통신  
경영전략실, 공정대책실 과장

1997년 3월~1999년 5월: KT 해외  
법인 MTM사 파견근무 부장

1999년 5월~2001년 2월: KT 기획  
조정실 IMT-2000 사업추진본부  
과장

2001년 3월~2008년 12월: 한국디  
지털위성방송 팀장, 지사장

2003년 2월~2003년 10월: (구)정  
보통신부 위성DMB 무선설비기술  
기준 위원

2009년 1월~현재: 한국디지털위성  
방송 고객센터 팀장

<관심분야> 인터넷 보안, 개인정보  
보호, CAS(방송수신제한시스템),  
컨텐츠 보안

**염홍열 (Heung-Youl Youm)**

## 증신회원

1981년 2월: 한양대학교 전자공학  
과 졸업

1983년 9월: 한양대학교 전자공학  
과 석사

1990년 2월: 한양대학교 전자공학  
과 박사

1982년 12월~1990년 9월: 한국전  
자통신연구소 선임연구원

1990년 9월~현재: 순천향대학교  
공과대학 정보보호학과 정교수

1997년 3월~2000년 3월: 순천향대  
학교 산업기술연구소 소장

2000년 4월~2006년 2월: 순천향대  
학교 산학연컨소시엄센터 소장

1997년 3월~현재: 한국통신정보  
보호학회 총무이사, 학술이사, 교육이  
사, 총무이사(역), 논문지편집위원  
회 위원장(현), 상임부회장(현)

2005년~2008년: ITU-T SG17/Q.9  
Rapporteur

2006년 11월~2009년 2월: 정보통  
신연구진흥원 정보보호전문위원

2008년 8월~현재: 디지털아이디관  
리포럼 의장

2009년~현재: ITU-T SG17 부의장/  
SG17 WP2 의장

<관심분야> 인터넷 보안, USN 보  
안, IPTV 보안, 홈네트워크 보안,  
암호프로토콜