# 보안성 강화를 위한 i-PIN 서비스 적용 사례 연구

## (A Case study f i-PIN Service for Information Security)

김현주‡ 이수종§

(Hyunjoo Kim) (Soojong Lee)

요 약 기존 인터넷 웹 사이트에서는 개인 식별 도구로 주민등록번호를 사용해 왔다. 그러나 인터넷에서의 주민 등록번호 사용은 개인정보 유출 위험을 증가시키는 주 요인이 되고 있다. 현재 정부에서는 인터넷에서의 주민등록번호 수집과 개인정보 유출 최소화를 위해 i-PIN 서비스를 권장하고 있다. i-PIN의 원래 사용 목적은 인터넷 웹 사이트에서 주민등록번호를 사용하지 않고 i-PIN 13자리 가상 번호로 개인을 식별하여 사용된다. 최근에는 i-PIN을 인증서 형태로 사용하는 사례가 늘고 있다. 본 연구에서는 i-PIN을 인증서 형태로 사용하는 소프트웨어 서비스 방법론과 기존 i-PIN 서비스와는 다른 형태의 i-PIN 본인인증서비스 적용 사례를 알아보고자 한다.

키워드 i-PIN, 주민등록번호, 본인 인증

Abstract Personal registration number has been used as a means of personal identification on existing internet. However, its use on internet sites has become a major factor increasing danger of leaking of personal information. Presently, the government recommends i-PIN to minimize the collection of personal registration numbers and leaking of personal information on internet. Original purpose of i-PIN is to recognize persons by its virtual number of 13 digits instead of using personal registration number on internet websites. These days, i-PIN continues to be used increasingly as a form of certification. This study seeks to explore software service methodology of using i-PIN as a form of certification on internet websites and examples in which its other forms of self certification are used than existing i-PIN services.

Key words i-PIN, Registration number, Self Certification

## 1. 서 론

국가 사회 기반의 중추적 역할을 담당하는 정보통신 인프라의 발전은 국가정책 및 정보화 패러다임의 변화와 더불어 사회 전반의 윤택한 도구로 자리 잡고 있다. 다양해지는 정보시스템의 성장

‡ 학생회원 : 단국대학교 전자공학과 정보보안전공
chopin@uhs.ac.krr
§ 일반회원 : 협성대학교 컴퓨터공학과
sjlee@uhs.ac.kr

논문접수 : 2012년 3월 8일
심사완료 : 2012년 3월 24일

못지않게 사이버 공격의 범위가 확대되고 허위 정보의 급증에 따른 개인정보의 훼손은 사회적 문제로 확산되어 정보서비스의 불안이 가중되고 있는 현실이다[1,2]. 특히, 근간의 대형 개인정보(네이트 및 싸이월드) 유출 사고는 우리에게 一觸卽發의 정보 폭발의 위협 속에 진입되었다 해도 과언이 아닐 것이다. 이에 우리나라에서도 개인정보관리에 대한 중요성과 사이버 윤리 정책의 중요성을 법제화 하여 2011년 개인정보보호법의 발효하였다. 현재 인터넷에서의 본인인증 방법으로는 공인인증서, 핸드폰인증, 아이핀 등 다양한 방법이 사용되고 있으나 아직도 가장 많이 사용되는 방법 중의 하나가 주민등록번호를 이용한 본인 식별 방법이라 할 수 있다. 대부분의 인터넷 이용자들은 웹 사이트에 주민등록번호를 등록하여 개인의 신분을 확인하고 ID(identifier)와 암호를 제공받아 다양한 웹 서비스를 이용하고 있다. 왜냐하면, 개인의 구별 할 수 있는 유일한 키로 주민등록번호를 사용하기가 가장 편리하기 때문이다. 그러나, 인터넷 상에서의 개인정보 유출은 ID와 암호, 주민등록번호를 포함하여 웹 사이트에 제공 된  개인 정보를 노출시키는 큰 부작용을 초래하게 된다[3]. 이에 국가에서는 개인정보 유출 및 주민등록번호 사용을 최소화 하기 위해 2005년부터 정보 보안 시책 사업의 하나로 *i*-PIN(internet personal identification number) 개인정보 식별 서비스를 권장 하고 있다[4].

*i*-PIN이란 주민등록번호를 대체하여 개인의 식별하는 인터넷상의 가상식별번호로 홈페이지에서 회원가입, 글쓰기에 주민등록번호를 사용하지 않고도 본인임을 확인 할 수 있는 개인 정보 보호 서비스이다[2-6]. *i*-PIN 서비스를 이용하기 위해서는 제3의 신뢰기관인 *i*-PIN 등록 기관에서 *i*-PIN 아이디와 암호를 발급 받아야하며, *i*-PIN 등록기관은 이용자의 정보를 저장하고 인증해 주는 역할을 담당한다. 국내 *i*-PIN 서비스 등록 기관으로는 민간기업 5개와 국가에서 운영하는 행정안전부 g-PIN(govement personal identification number)으로 총 6개의 서비스가 지원된다.[7]. *i*-PIN 서비스는 제공기관 간 상호연동 기술과 중복가입확인 코드를 제공하여 1개의 *i*-PIN으로 인터넷에서 개인 식별이 가능하다. *i*-PIN의 원래 사용 목적은 인터넷 웹 사이트에서 주민등록번호를 사용하지 않고 *i*-PIN 13자리 가상번호로 개인을 식별함에 있다. 즉, 개인을 구분하는 유일한 키인 주민등록번호를 *i*-PIN 13자리 가상번호로 대체하여 회원가입, 글쓰기 등의 권한을 주어 정보서비스 사용을 가능하게 한다.

본 논문에서는 기존의 *i*-PIN 서비스 방식에서 벗어나 *i*-PIN을 인증서 형태로 사용하는 *i*-PIN 서비스 방법론과 웹 사이트의 적용 사례를 알아보고자 한다. PKI 공인인증서는 서비스를 제공하는 기관이나 서비스를 제공받는 개인이 일정 비용을 지불하고 발급받아야 한다. 그러나, *i*-PIN는 국가를 중심으로 기관, 개인 모두에게 무상으로 제공된다는 점에서 비용 지불이 꺼리는 사용자 측면에서는 의미가 있다고 할 수 있다.

## 2. 관련 연구

### 2.1 *i*-PIN(internet personal identification number)

#### 2.1.1 i-PIN 개요

*i*-PIN은 인터넷상의 주민등록번호를 대체하는 개인 식별번호이다. 2005년부터 시작된 *i*-PIN 서비스는 *i*-PIN2.0 서비스로 개선되어 중복가입확인정보 및 본인 확인기관 간 상호 연동을 통해 이용자가 1개의 *i*-PIN 아이디와 암호로 다수의 인터넷 웹 사이트와 연계가 가능하도록 구성되어 있다[7-9]. 또한, *i*-PIN은 한번 부여 받으면 변경이 불가능한 주민등록번호와는 달리 자신의 *i*-PIN이 노출되었다고 해도 언제든지 폐기가 가능하여 분실 시 다른 *i*-PIN으로 재발급을 받아

사용하므로 주민등록번호 노출로 인한 개인정보 침해의 피해를 최소화 할 수 있는 특징이 있다[6][10].

### 2.2 *i*-PIN 서비스 기술

i-PIN은 이용자가 인터넷 웹 사이트 회원 가입 시 주민 등록번호를 기입하는 대신 본인확인기관에 이용자의 신원을 확인하고 발급받은 *i*-PIN 13자리 가상번호로 개인을 식별이 가능한 기술이다. *i*-PIN은 기존 인터넷 웹 사이트에서 사용되는 주민 등록번호의 수집 목적을 충족시키며, 그 문제점을 보완할 수 있다[10]. 또, 웹 사이트와 연계한 *i*-PIN 서비스 본인확인기관은 이용자 관리에 필요한 정보를 웹 사이트에 전달하여 준다. *i*-PIN 본인확인기관이 웹 사이트에 전달하는 정보로는 성명, *i*-PIN 13자리, 중복가입확인 정보, 생년월일, 성별, 연령대, 내·외국민 정보를 제공하며 관련 내용 및 활용 가능 분야를 정리하면 [표 1]과 같다[7][10][13][14].

**표 1. *i*-PIN 서비스 제공 정보**

| 구분 | 제공 정보 | 활용 정보 |
|---|---|---|
| 성명 | 신원확인 수단을 이용한 본인확인을 수행하여 검증한 사용자의 실명 | 사용자식별 방법으로 활용 |
| i-PIN (13자리) | 사용자의 본인확인을 수행한 이후에 본인확인기관이 사용자에게 부여하는 13자리 정보 *i*-PIN (13자리)의 3~4번째는 본인확인기관 정보 2자리와 난수 값) | 불량 사용자 추적 시 활용 |
| 중복가입 확인정보 | 회원가입 또는 글쓰기 권한을 얻고자 하는 인터넷 사이트 내에서만 유일하게 사용자를 식별 할 수 있는 64byte 정보 | 중복기관 확인 및 사용자 식별 시 활용 |
| 생년월일 | 신원확인수단을 통한 본인확인을 수행하여 검증한 주민번호에서 추출 한 8자리정보 (YYYYMMDD) | 사용자서비스 제공 시 활용 (예 : 생일축하, 생일쿠폰, 메일 발송 등) |
| 성별 | 신원확인수단을 통한 본인확인을 수행하여 검증한 주민번호에서 추출한 1자리 정보 | 사용자마케팅 시 활용 (예:패션, 미용 정보 등) |
| 연령대 | 신원확인수단을 통한 본인확인을 수행하여 검증한 주민번호에서 추출한 정보를 분류하여 제공하는 8단계의 법적연령대 1자리 정보 | 연령대별, 서비스 식별에 활용(예: 영화관람, 게임이용 등급 등) |
| 내외국인 | 신원확인수단을 통한 본인확인을 수행하여 검증한 주민번호 또는 외국인 등록번호에서 추출한 1자리 정보 | 내·외국인 가능서비스 구분 시 활용 |

#### 2.2.1 구성요소

*i*-PIN 서비스 구성은 인터넷 이용자, 인터넷 사업자, 인터넷 사용자의 신원 확인과 인터넷 웹 사이트에 사용자의 개인 정보를 제공하는 본인확인기관으로 구성된다[15]. [그림 1]은 이용자와 본인확인기관, 웹 사이트에서의 *i*-PIN 정보서비스 관계를 설명한 것으로 *i*-PIN 서비스 프레임워크 구성이다. 이용자 본인은 여러 개의 본인확인기관으로부터 *i*-PIN을 발급 받을 수 있고, 자신이 이용하는 본인확인기관으로부터 *i*-PIN 발급받아 회원가입 또는 글쓰기 권한 획득에 사용할 수 있다[15]. 웹 사이트는 이용자에게 *i*-PIN 서비스 제공을 위해 본인확인기관 중 하나의 기관에서 *i*-PIN 연계서비스를 제공받아야 한다. *i*-PIN 연계서비스 제공 기술은 이용자가 발급받은 *i*-PIN의 본인확인기관과 웹 사이트가 연계한 본인확인기관이 서로 다르더라도 웹 사이트에 *i*-PIN 정보가 안전하게 전송되도록 상호호환성을 제공하는 본인확인기관 간 연동 기술이다[16][17].

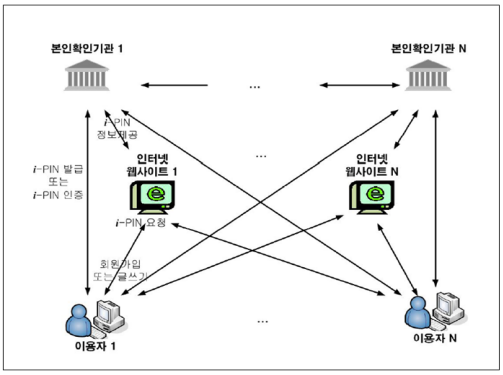


**그림 1. *i*-PIN 서비스 프레임워크 구성**

2.2.2 *i*-PIN 서비스 형식

2.2.2.1 *i*-PIN 본인확인기관 간 상호 연동

6개 *i*-PIN 본인확인기관은 *i*-PIN 하나로 모든 인터넷 웹 사이트에서 이용이 가능케 하는 상호연동 기술을 제공한다. *i*-PIN 상호연동 기술 적용을 위해서는 송수신 메시지에 대한 전달 형식 표준이 필요하다. *i*-PIN 서비스 규약은 하이퍼텍스트 통신 규약을 기본 통신 프로토콜로 사용하며 전달메세지 표준에는 WebsiteInfo(본인확인기관 정보 전달 메세지), PersonalInfo(개인정보 전달메세지) 구조체를 사용한다[10][17].

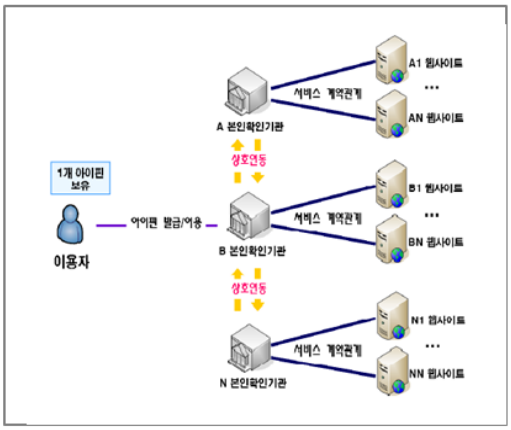


**그림 2. 본인확인기관 간 상호연동 서비스 구성**

2.2.2.2 웹 사이트에 전달되는 개인정보 형식

이용자의 *i*-PIN 발급 본인확인기관과 웹 사이트에서 연동 한 본인확인기관이 같은 경우 해당 본인확인기관은 개인정보를 암호화하여 웹 사이트에 전달한다. 이용자의 *i*-PIN 발급 본인확인기관과 웹 사이트 연계 본인확인기관이 다른 경우는 *i*-PIN 발급 본인확인기관은 이용자의 개인정보에 전자서명을 수행하여 본인확인기관들이 공유 하는 비밀키 또는 임의의 비밀키로 암호화하여 개인정보를 전달한다. *i*-PIN 발급 본인확인기관은 이용자의 주민 등록번호를 이용하여 PublicInfo 구조체를 만들어 해쉬함수를 입력하여 해쉬값을 획득하고, 해쉬값에 자신의 전자 서명용 인증서의 개인키를 이용하여 전자서명을 수행한다[10][15].

2.2.3 *i*-PIN 중복가입확인 정보

*i*-PIN 사용하는 인터넷 웹 사이트는 사용자의 주민등록번호를 수집할 수 없기 때문에 사용자를 유일하게 식별할 수 있는 정보를 필요로 한다. 중복가입확인 정보는 사용자의 중복가입확인 정보를 본인확인기관으로부터 전달받아 보관하고 이후 사용자의 중복가입확인 정보와 비교하여 중복가입 여부를 확인 할 수 있다. 또, 1인당 n개의 계정을 허용하는 인터넷 웹 사이트에서도 중복가입정보 개수를 저장해 n개의 계정보다 작으면 계정 생성을 허용하고 회원가입을 거절 할 수 있다[12]. 중복가입정보는 주민등록번호(RN:Resident Number)와 웹 사이트 식별 번호(SI:webSite Identification information)를 해시함수 SHA2로 압축하여 1차 결과 값을 생성하고 다시 1차 결과 값에 *i*-PIN 본인확인기관 공유 식별 번호를 더해 2차 해시 함수 SHA2로 압축한 결과 값이다[2][10][15][18].

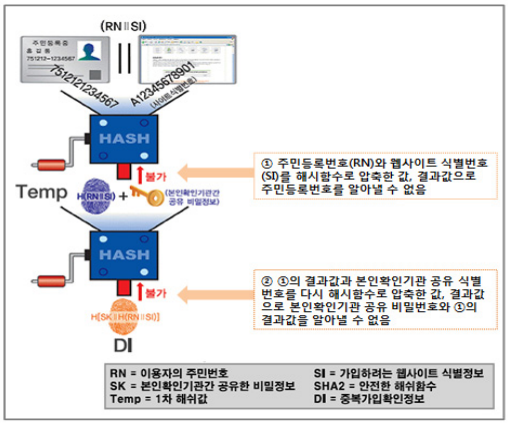


**그림 3. i-PIN 서비스 중복가입확인정보 생성 과정**

<그림 3>은 *i*-PIN 서비스 중복가입확인과정 생성 과정으로 주민등록번호(RN)과 해쉬함수(SI)를 이용해 중복 가입확인 정보(DI)를 생성하는 과정을 그림으로 도식화했다.

## 3. *i*-PIN 서비스 활용

### 3.1 *i*-PIN 서비스 이용

*i*-PIN 정보서비스의 사용은 크게 *i*-PIN 발급, *i*-PIN 본인인증, *i*-PIN 제공·사용으로 구분되어 나누어진다. 다음은 *i*-PIN 발급에서 사용까지의 정보제공 과정에 대한 설명이다. *i*-PIN을 이용한 본인확인 과정과 *i*-PIN 아이디에 대한 유효성 검사 과정을 자세히 설명하면 <그림 4>와 같다.

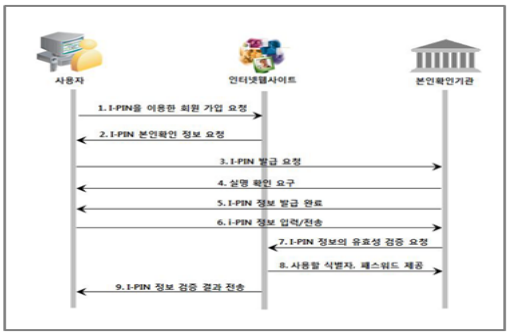


**그림 4. i-PIN 본인확인 절차**

### 3.2 국내외 본인확인 동향

#### 3.2.1 국내 *i*-PIN 서비스 동향

2009년 정보보호 실태조사 기업부문 결과에 의하면 웹 사이트에서 *i*-PIN 서비스를 도입한 기업은 8.5%, 2008년도와 비교해 3배가량 증가되었다. *i*-PIN을 아는 사용자도 58.1%, 이 중 *i*-PIN 서비스의 인지에 대해 전년 대비 19.7% 상승되어 *i*-PIN에 대한 인지도가 꾸준히 성장하고 있는 것으로 나타났다[11][12].

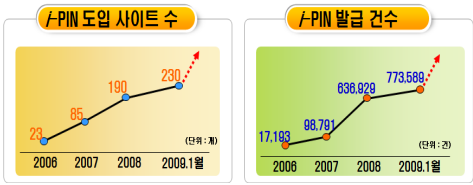


**그림 5. i-PIN 서비스 도입 현황**

실제 i-PIN 서비스 운용 현황을 보면 국가에서 운영하는 공공기관은 별도의 회원가입 없이 *i*-PIN을 인증하여 접속하는 방법과 회원가입 전에 실명인증을 *i*-PIN을 통해 승인 받아 처리하는 방식을 사용하고 있었다. 전자의 경우 실명 확인만 가능하며 정보시스템 접속 후에는 정보서비스의 열람만 가능했다. 후자의 경우 기존 회원가입의 형태를 준수하며 실명확인을 *i*-PIN으로 대체함으로 실제적으로 인터넷상에 주민등록번호를 수집하지는 아니했다.

#### 3.2.2 국외 본인확인 동향

프랑스, 독일, 벨기에은 우리와 동일하게 개인 신분증이 발급되면 일련번호를 부여하는 방법을 사용하고 있다. 발급된 일련번호를 등록하여 사용하고 분실이 발생하면 기존 일련번호는 폐기, 기존 일련번호는 재사용이 불가능하다. 또, 미국의 경우는 주마다 다른 번호를 부여하여 사용하는 사회보장번호(Social Security Number)가 있으며 개인 식별이 가능하다. 카나다는 아직까지 온라인상에서 계좌 개설 등의 금융 서비스를 제공하지 않으므로 온라인에서의 신원 확인 절차는 사용하지 않고 있다

[20]. 대부분의 국가에서는 온라인에서 회원 가입 시 또는 본인 식별 시에는 주로 이메일을 개인 식별로 사용하는 경우가 많았다.[21][22].

## 4. *i*-PIN 서비스 모델을 이용한 본인 인증

기존 웹 사이트에서는 *i*-PIN을 회원 가입 시 주민등록번호 대신 사용하여 왔다. 본 논문에서는 웹 사이트 접속 시 *i*-PIN을 인증서로 활용하여 내부 시스템과 접속하는 인증도구로 사용한다. *i*-PIN 인증 과정을 기존 웹 사이트에서 사용되는 개인의 ID와 암호로 대체하여 사용하고 주민등록번호를 수집하지 않으면서 조직의 내부 시스템과의 인증 과정을 *i*-PIN 서비스 하나로 연계하여 사용할 수 있다. 무엇보다 *i*-PIN은 한번 부여받으면 평생 바꿀 수 없는 주민등록번호와 달리 자신의 *i*-PIN이 노출되어도 언제든지 폐기가 가능하고 언제든지 새로운 *i*-PIN으로 발급 받아 사용 할 수 있다. 사용하던 i-PIN이 인터넷 상에 노출되어도 해독이 불가능해 개인정보 침해로 인한 피해를 최소화 할 수 있다.

### 4.1 *i*-PIN 본인 인증 서비스 모델

본 논문에서 제안하는 *i*-PIN을 인증서로 활용하여 내부 시스템과 접속하는 서비스 flow는 다음의 <그림 6>과 같다.

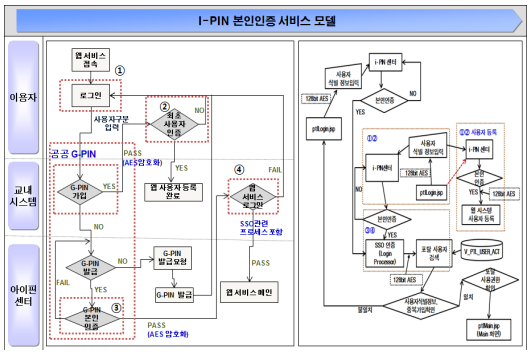


그림 6. i-PIN 본인확인 서비스 Flow

<그림 6>의 *i*-PIN 본인 인증 서비스 플로우를 기반으로 i-PIN 본인 인증 서비스 과정을 <그림 7>로 설명한다.

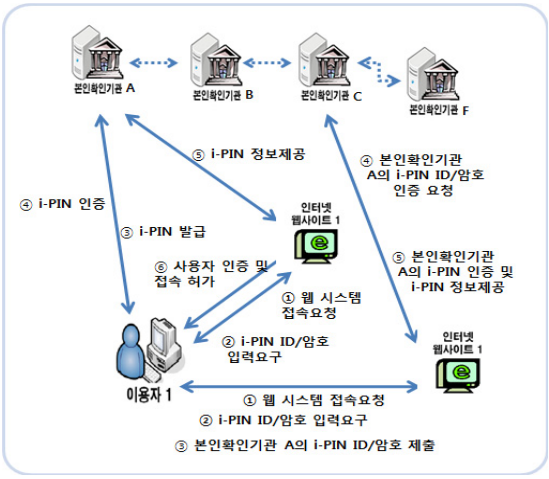


그림 7. i-PIN 본인확인 웹 서비스 시스템 구성도

### 4.2 본인인증 i-PIN 서비스 사례

*i*-PIN 서비스는 2005년부터 정보통신부를 중심으로 시작되었다. 2011년 9월 개인정보보호법 발효 이 후, 개인정보에 대한 중요도가 의무화되어 그 관리의 중요성을 강조하고 있다. 현재 웹 사이트 중 인터넷 회원 5000명이상의 가입자를 보유하고 있는 인터넷 사이트는 반드시 *i*-PIN 적용을 하여 웹 서비스를 지원하도록 하고 있다. 이에 민간 포털 사이트 및 공공기관 사이트 등 대부분의 웹 사이트에서는 *i*-PIN을 사용하고 있으며 회원에게 선택권을 주어 *i*-PIN 또는 주민등록번호를 선택하여 사용하게 하고 있다.

#### 4.2.1 *i*-PIN 본인인증 적용 사례(1)

국가에서 운영하는 공공기관 웹 사이트에서는 주민등록 번호를 수집하지 않고 *i*-PIN 본인 인증 후 서비스 사용권을 주는 웹 서비스 모델을 사용한다. <그림 8>은 공공기관에서 *i*-PIN을 이용하여 본인 인증이 완료되면 서비스 사용이 부여되는 모델이다. <그림 8>과 같이 공공 *i*-PIN 서비스 인증을

선택하면 <그림 9>와 같이 공공 *i*-PIN 접속 화면으로 변경된다. <그림 10>은 이미 발급받은 *i*-PIN 아이디와 암호를 입력하면 i-PIN 유효성 검사 후 본인 인증이 완료되면 사용자에게 웹 서비스 권한이 부여된다.

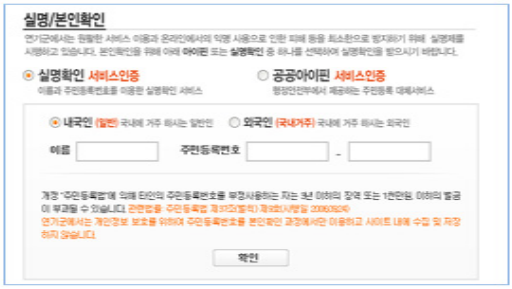


**그림 8. 본인확인을 위한 웹 서비스 화면**


**그림 9. i-PIN 본인확인 웹 서비스 화면**

**그림 10. i-PIN 본인확인 완료 후 서비스 부여 화면**

4.2.2 *i*-PIN 본인인증 적용 사례(2)

다음은 대학의 웹 포탈 사이트에서 회원가입 절차 없이 *i*-PIN 본인 인증으로 대학 내 포탈 시스템에 접속하여 사용자 권한에 맞는 서비스를 부여하는 모델이다. 그러나, 이 모델은 *i*-PIN 본인확인기관의 장애가 발생되면 *i*-PIN 본인 인증이 불가능하게 된다. 즉, *i*-PIN 본인확인기관의 장애가 발생되면 본인 인증이 불가능하므로 대학 내 전체 시스템의 마비를 초래 시킨다. <그림-11>은 i-PIN 웹 포탈 시스템에 최초 접속 화면이다. 이미 부여되어 본인만 알고 있는 내부시스템 아이디와 인증 암호를 입력 후 최초 사용자 등록을 처리 한다. 이 때 내부 시스템과의 인증 확인 서비스 승인이 거부되면 웹 포탈 시스템에 접근이 불가능하게 된다. 서비스 승인이 완료되면 *i*-PIN 서비스 모듈은 입력받은 이용자의 *i*-PIN을 본인확인기관에 전송하고 본인확인기관은 이용자를 관리한다.

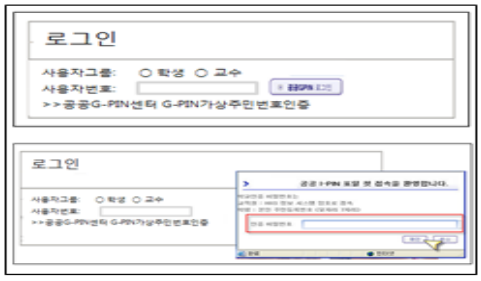


**그림 11. *i*-PIN 웹 포탈 시스템 접속**

<그림 12>는 <그림 11>의 최초 사용자 등록이 완료 후 *i*-PIN 서비스 모듈이 연동되어 이용자의 본인인증과 유효성 검사를 수행하여 이용자의 본인 인증 값이 본인 확인 기관으로부터 웹 포탈에 전송되면 <그림 13>의 웹포탈 서비스 권한을 부여받게 된다.


**그림 12. *i*-PIN 본인인증 확인 서비스**

**그림 13. *i*-PIN 본인 인증 웹 포탈 시스템 Main**

4.2.3 *i*-PIN 본인인증 적용 사례(3)

*i*-PIN 본인인증 적용 사례(2)의 시스템 마비 현상을 개선하고자 웹 사이트와 본인확인기관 간의 서비스 구성을 다중으로 구성한 서비스 모델로 공공 g-PIN과 민간 *i*-PIN 서비스를 병렬로 구성한 서비스 모델이다.

*i*-PIN 웹 포탈 시스템을 Active, Standby 형태로 구성하여 만약, Active *i*-PIN 서비스 제공기관에 장애가 발생되면 대기하던 Standby 민간 *i*-PIN 서비스로 자동 전환되는 웹 서비스 모델이다. Active, Standby 형태의 *i*-PIN 웹 포탈 시스템의 장애 발생 시 자동 연동 과정은 <그림 14>로 도식화 하였다. 이 때 사용자는 서비스 시스템이 변경되었는지를 전혀 알 수는 없다. <그림-14>의 *i*-PIN 본인인증기관 장애를 대비한 *i*-PIN 서비스 모델 연동 과정은 다음과 같다. <그림 14>의 ①Active, Standby *i*-PIN 웹 포탈 시스템은 항상 RS232 Asynchronous Adaptor Heartbeat 구성으로 *i*-PIN 웹 포탈 시스템과 *i*-PIN 본인확인기관의 서비스 지원 여부를 상시 확인 한다. <그림 14>의 ②웹 포탈 시스템 연계 i-PIN 본인확인기관에 장애가 발생하면 사전에 미리 구성되어 있는 HACMP (High Availability Cluster Multi Processing)에 의해 <그림 14>의 ③④Standby i-PIN 웹 시스템으로 IP 전환이 이루어진다. <그림 14>의 ⑤민간 *i*-PIN Standby 웹 포탈 시스템은 Active 공공 *i*-PIN 웹 포탈 시스템으로 전환되며 웹 서비스를 시작한다. <그림 14>의 ⑥⑦⑧*i*-PIN 메인 시스템의 장애 조치가 완료되면 현재의 Active 시스템은 Standby 상태로 자동 전환된다.

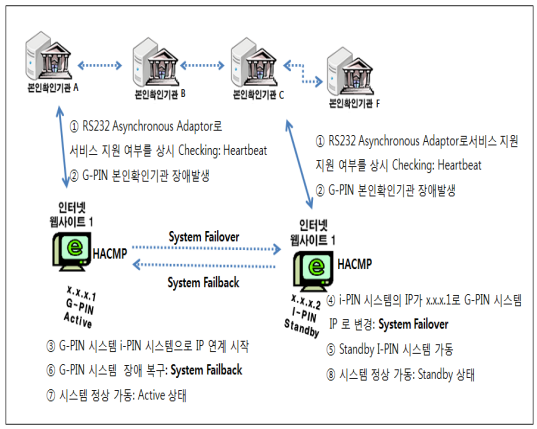


**그림 14. *i*-PIN 본인인증기관 장애 시 서비스 모델**

## 5. 결 론

인터넷상에서 주민등록번호 유출은 심각한 사회적 문제로 대두되고 있다. 또한, 2009년도에 발생한 개인 정보 침해건수에 대한 유형별 분석에 따르면, '신용정보 침해 등 정보통신망법 적용대상 이외의 개인정보침해' 사례가 23,893건으로 가장 많았으며, 정보통신망법을 적용하는 범위 내에서는 '주민번호 등 타인정보 훼손, 침해, 도용 사례'가 6,303건(45%)으로 가장 많이 발생한 것으로 나타났다. 이처럼 IT 기술의 발달로 다양해지는 정보서비스의 홍수 속에 개인정보의 안전한 관리는 없어서는 안 될 소중한 정보 기술로 한자리를 잡고 있다.

본 논문에서는 *i*-PIN 서비스 적용 사례를 기준으로 서비스 방법론과 활용에 대해 조사하였다. 조사 결과 기존 *i*-PIN 서비스는 인터넷 회원가입 시 주민등록번호를 대체하는 서비스 모형을 사용되었으나, 최근에는 *i*-PIN의 본인인증 기술을 웹 시스템에 적용해 본인 인증을 위한 인증서

형태로 사용하는 웹 사이트가 있어 좋은 사례를 찾을 수 있었다. *i*-PIN을 이용한 본인 인증은 그간 인터넷에서 사용되어 온 주민등록번호 사용을 대체하고 인터넷에서 남용되는 웹 사이트별 회원의 ID와 암호를 *i*-PIN 하나로 연계하여 사용 할 수 있다. 또, 한번 부여받으면 평생 바꿀 수 없는 주민등록번호와 달리 자신의 *i*-PIN이 노출되었다고 해도 언제든지 폐기가 가능하다. *i*-PIN 폐기 후에도 새로운 *i*-PIN으로 발급이 용이하고, 이미 노출된 *i*-PIN은 사용자 식별 정보 해독이 불가능하므로 개인정보 침해로 인한 피해를 최소화 할 수 있다. 특히, PKI 공인인증서에서 제공되지 않는 개인의 생년월일, 성별 등의 정보를 *i*-PIN에서는 제공되므로 성인 인증을 필요로 하는 웹 시스템에서 더 유용하다 할 수 있다. 그러나, 아직까지 제도적 개선에 대한 문제와 본인확인기관 장애 시 대처 방안에 대해서도 개선이 되어야 할 것이다. 이러한 합리적인 서비스 정책과 IT 정보 기술의 융합은 보다 더 효율적인 *i*-PIN 서비스 모델 개발과 *i*-PIN 활용, 경제성 등 개인정보보호에 기여 할 것으로 기대된다.

## 참 고 문 헌


[1] 황중연, “유비쿼터스 환경 변화에 따른 정보 보호의 주요 현황과 대응 전략”, 한국 정보보호진흥원, 2008.

[2] “인터넷 상의 주민번호 보호 수단으로 공인인증서 이용 기술 개발”, 한국정보인증, pp.13-14, 40-42, 2010.9

[3] 조영섭, 진승헌, “인터넷 ID 관리 시스템 개요 및 비교”, 전자통신동향분석 22(3), pp.137, 2007. 6.

[4] 민경식, “주민번호 대체수단으로 아이핀 보급 확산 필요”, 신문과방송, pp.168, 2008,05..

[5] 공공 *i*-PIN 센터, http://www.g-pin.go.kr/

[6] 윤덕중 “주민등록 대체 공공 i-PIN 서비스”, 한국지역 경제개발원, pp.46-49, 2008, 11.

[7] 장인용, “*i*-PIN 서비스 활성화를 위한 문제점 분석 및 대안 제시에 관한 연구”, 순천향대학교, pp.34-36 42-46, 2009.

[8] “*i*-PIN 2.0 도입 메뉴얼”, 방송통신위원회, 한국인터넷 진흥원, 2009, 7.

[9] “*i*-PIN 정책설명회 및 [개인정보 기술적·관리적 보호조치 기준] 개혁안 공청회” 자료집, 한국인터넷진흥원, 2009.

[10] 정찬주, 김윤정, 김진원, 박광진, “주민번호 (*i*-PIN) 개발을 위한 기술표준과 서비스 프레임 워크”, 정보보호학회, pp.20-26, 2008.

[11] “2009년 정보보호 실태 결과보고서”, 정보보호진흥원, pp.122-125, 2010

[12] “아이핀 이용 현황 실태 조사 보고서”, 연구보고서 2007, 정보보호진흥원, 2007.

[13] 최윤성, 이윤호, 김승주, 원동호, “주민등록번호 대체수단에 대한 구현 취약점 분석”, 정보보호학회, pp.148-149, 40, 2007.4.

[14] “*i*-PIN 서비스 프레임워크”, TTAS.KO-12.0054, 정보통신단체표준, pp.4-7, 2007.

[15] 정찬주, 인터넷상의 개인식별번호 서비스 및 표준, 한국정보보호진흥원, pp.75-78, TTA Journal 2008.

[16] 박상환, “인터넷상의 주민번호 대체수단 안전성 확보 기술 연구”, 고려대학교 2010.

[17] “*i*-PIN 서비스 전달메시지 형식”, DidM-2008-001, DidM, pp.3-12, 2008.

[18] “i-PIN 서비스 중복가입확인정보”, TTAK.KO-12.0038/R1, 정보통신표준단체, pp.7-9, 2008.

[19] 성균관대학교(2007) 주민번호 대체수단 서비스 개선 방안 연구. 한국정보보호진흥원.

[20] 이영현, “개인정보유출방지를 위한 개인식별 방법 연구”, 서울산업대학교, pp.19-20, 2009.

[21] Young-Ho Seo:Jong-Hyeon Kim:Young-Jin Jung:Dong-wook Kim, “ITC-CSCC 2000 PROCEEDINGS V.1 - VLSI Design & Applications 1”, ITFIND, 2007.07.

[22] Shuo Bai, “IWAP2001: First International Workshop for Asian PKI-PKI in China”, ITFIND, 2001.10.

## 저 자 소 개

**김 현 주**

2010년 단국대학교 정보통신대학원 정보통신학과 졸업(공학석사)
2012년 현재 단국대학교 대학원 전자・전기공학과 컴퓨터응용 및 정보보안 전공 박사과정.

<주관심분야> 정보보안, i-PIN, 디지털포렌식, 역추적, 인터넷 보안, IT융합

**이 수 종**

1989년 국민대학교 공과대학 전자공학과졸업(공학사)
1992년 연세대학교 대학원 전자공학과 졸업(공학석사)
2000년 연세대학교 전기컴퓨터 공학과 졸업(공학박사)
2002년 현재 협성대학교 컴퓨터공학과 부교수

<주관심분야> IT융합, 생체인식, 영상처리, 신호처리, 영상통신