주민등록번호 사용현황과 대체수단에 관한 연구

최해랑*, 정정윤, 최성은, 박혜진, 김창수, 안성수
한국인터넷진흥원 정보보호본부 개인정보보호단 주민번호전환지원팀
*e-mail: hlchoi@kisa.or.kr

A Study on the Using Resident Registration Number and Alternatives for RRN

Haelahng Choi, Chung-Yun Chung, Sung-Eun Choi, Hyejin Pak,
Chang-Soo Kim, Sung-Soo Ahn
Identification Conversion Team, Personal Information Protection Division,
Information Security Group, Korea Internet & Security Agency(KISA)

요 약

주민등록번호는 주민생활의 편익 증진과 행정사무의 적정한 처리를 목적으로 도입되었으나 인터넷의 발달과 함께 관행적이고 무분별하게 사용되어 왔다. 수집된 주민등록번호가 해킹 등의 유출사고로 명의도용 등 범죄에 악용될 우려가 커지자 이를 근본적으로 해결하기 위하여 2011년 방송통신위원회는 인터넷상 주민등록번호 수집·이용을 제한하는 법·제도적 정책을 추진하였다. 정보통신망법이 개정되어 주민등록번호의 사용이 제한되면서 사업자에게 본인확인, 연령확인 등 법률의무의 이행이나 고객의 분쟁조정 등 목적을 위해 주민등록번호를 대체할 본인확인수단이 필요하게 되었다. 본 논문에서는 주민등록번호를 이용자가 입력하지 않으며 보편적으로 사용하고 있는 인프라를 이용하고 단순한 입력정보의 변경을 통해 본인확인을 할 수 있는 방안을 제안한다.

1. 서론

주민등록번호는 1962년 주민등록법이 제정된 후 18세 이상인 국민 개개인에게 부여된 고유번호로, 주민의 거주관계 등 인구의 동태를 명확하게 파악하여 주민생활의 편익을 증진과 행정사무의 적정한 처리를 목적으로 도입되었다[1]. 그러나 주민등록번호가 가진 편리함으로 인해 금융, 의료 등 여러 분야에서 광범위하게 사용되고 있으며 인터넷이 발달함에 따라 온라인상의 거래나 회원가입 등에서 주민등록번호를 관행적인 수집·이용하고 있다[2].

또한 개인정보의 가치가 증가하면서 해킹 등을 통한 대규모 개인정보 유출사고가 발생하고 있으며 유출사고 후 스팸, 명의도용, 보이스피싱 등 유출정보를 이용한 2차 피해의 우려가 증가하면서 이에 대한 대책의 연구와 함께 개인정보 최소화 수집정책 등이 수행되었다.

이러한 노력에도 대규모 유출사고가 계속되자 유출사고로 인한 2차 피해의 근본적인 해결을 위하여 방송통신위원회는 인터넷상에서 주민등록번호의 사용을 원칙적으로 제한하는 정책을 추진하고 있다[3].

온라인에서 주민등록번호의 사용을 제한하기 위해서는 본인확인 시 활용되는 주민등록번호의 입력을 없애는 것이 필요하므로, 본 논문에서는 주민등록번호를 사용하지 않는 본인확인수단을 제안한다. 2장에서는 본인확인 등 주민등록번호의 사용현황 및 본인확인수단의 사용목적을 살펴보고 3장에서 기존의 본인확인수단이 어떻게 수행되고 있는지 분석한다. 4장에서는 기존의 본인확인수단을 변형하여 주민등록번호를 사용하지 않는 본인확인수단을 제안한다.

2. 주민등록번호 사용현황

국내 웹사이트 중 2011년 4/4분기 기준으로 일일평균 방문자 수 1만 명 이상[4][5][6]의 웹사이트에서 공공·비영리 등을 제외한 정보통신망법의 대상은 대략 1,200여개이며 해당 웹사이트의 주민등록번호 사용현황을 살펴보니, 회원가입 시 또는 아이디나 비밀번호를 분실하여 확인하고자 할 때 1,200여개 웹사이트 중 72.3%가 주민등록번호를 사용하고 있었다.

이러한 회원가입, 비밀번호 찾기에서 주민등록번호의 사용목적은 중복가입 방지 또는 회원관리가 대부분이며 법령에서 요구하는 연령확인이나 본인확인을 이행하기 위해 입력받거나 이용자의 구매와 관련하여 분쟁의 소지를 명확히 하고자 이용자의 정확한 식별을 위해 입력받고 있었다.

단순한 중복가입 방지의 경우 이메일이나 연락처를 사용하여 확인할 수 있으므로 주민등록번호의 대체가 가능하나, 「청소년보호법」, 「게임산업진흥에 관한 법률」 등 법령에서 요구하는 본인확인의 경우 실제 그 사람이 맞는지 확인이 필요하므로 인터넷상에서 가능한 본인확인수단이 필요하다.

3. 기존의 본인확인수단

본인확인이란 “A라는 사람이 A가 맞다”는 것을 확인하는 것으로 인터넷상에서는 실시간으로 전자적인 정보를 이용해 사용자를 확인하는 과정이다[7].

인터넷상에서의 본인확인은 그 사람이 알고 있는 것(Something you know)을 이용하거나, 그 사람이 가지고 있는 것(Something you possess)을 이용하거나, 그 사람의 물리적인 특성(Something you are)을 이용하는 등의 방법이 있다.

대부분 그 사람만이 알고 있는 것, 즉, 주민등록번호를 입력받거나 이미 입력받아 저장하고 있는 번호를 신용정보회사나 공인인증기관 등 신뢰기관을 통해 확인을 받는데, 이는 신뢰기관을 통해 이용자에 대한 객관성을 확보하는 것이다.

현재 인터넷상에서 보편적으로 활용되고 있는 본인확인수단은 주민등록번호와 성명을 통해 확인하는 실명인증, 아이디와 패스워드 입력을 통해 확인하는 아이핀, 휴대전화번호와 인증번호 전송 및 확인을 통한 휴대폰인증, 공인인증서와 패스워드 입력을 통해 확인하는 공인인증서 인증 등이 있다.

실명인증은 주민등록번호와 성명을 입력하여 신용평가기관 등에서 확인해주는 것으로 그 사람이 아는 정보를 입력하는 방법이며 입력하는 정보가 간단하고 입력 후 확인 버튼만 누르면 완료되므로 편리한 것으로 보일 수 있다. 그러나 이미 대량 유출되었다고 여기고 있는 주민등록번호를 입력하여 확인하는 것으로 본인만이 아는 것을 이용한다고 보기 어려워 명의도용 등에 악용될 위험성이 크다. 따라서 “주민번호 수집·이용 제한정책”에서는 사업자가 실명인증 서비스를 통한 본인확인을 사용할 수 없도록 하고 있다[8].

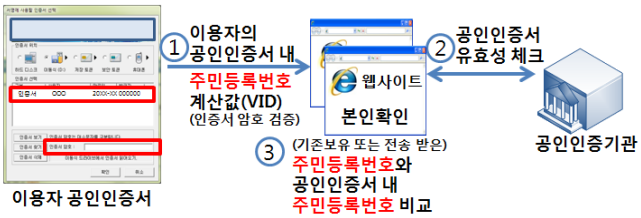
아이핀, 휴대폰인증, 공인인증서 등의 본인확인수단은 오프라인에서의 대면확인이 완료된 것을 전제하여 본인을 확인했다고 할 수 있고 그 사람만이 알고 있는 비밀정보를 활용하고 암호화 전송, 관리·감독을 받는 제3자 신뢰기관이 처리하고 있어 안전성, 객관성을 보장받을 수 있다.

<표 2> 국내 보편적인 본인확인수단

본인확인수단	본인확인 방법
실명확인	신용정보집중기관 및 자체적으로 수집한 실명 DB를 기반으로 **주민등록번호, 성명**을 활용한 인증
아이핀	본인확인기관을 통해 발급된 **아이핀 아이디와 비밀번호**를 활용한 인증
휴대전화	이동통신사를 통한 **통신사, 휴대폰번호, 성명, 주민등록번호, 인증번호** 확인
공인인증서	공인인증기관에서 개인에게 발급된 **범용 공인인증서(주민등록번호) 와 인증서 암호** 확인
신용카드	결제대행업자(신용카드 VAN사, PG사)와 연결되어 있는 신용카드사를 통한 **카드종류, 카드번호, 유효기관, 비밀번호 2자리, 주민등록번호** 확인

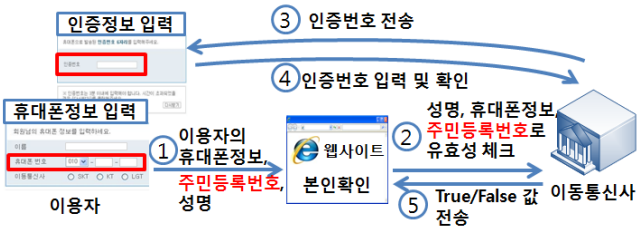
그런데 아이핀의 경우 이용자가 주민등록번호의 입력 없이 본인확인을 할 수 있지만 휴대폰인증, 공인인증서 등은 이용자가 주민등록번호를 함께 입력하거나 이미 웹사이트에서 보유하고 있는 주민등록번호를 활용하는 방식으로 운영되고 있어서 주민등록번호 사용제한 정책의 목적에 맞지 않은 상황이다.

공인인증서의 경우 공인인증서에 저장되는 해시된 주민등록번호 값을 활용한다. 이용자가 본인확인을 받고자 할 때 ①공인인증서 암호(개인키 비밀번호) 입력하여 복호화 된 개인키에서 R(비트열난수) 추출 후 웹사이트에 R과 공인인증서를 암호화하여 전송하면, ②공인인증기관에서 인증서의 유효성을 확인하고, ③웹사이트에서 저장하고 있는 주민등록번호와 전송받은 R값과의 연산을 통해 VID를 생성(R◎주민등록번호 해시 = VID)하여 인증서에서 추출한 주민등록번호 해시 값을 R값과의 연산을 통해 생성한 VID’(R◎주민등록번호 해시 = VID’)와 비교하는 과정을 통해 본인을 확인한다[9]. 본인이 알고 있는 암호와 가지고 있는 인증서를 통해 확인하기 때문에 안전성 및 신뢰성이 높지만 주민등록번호가 요구되는 상황이다.



(그림 1) 주민등록번호를 사용하는 공인인증서 방식

휴대폰 인증의 경우 본인이 알고 있는 휴대폰정보 및 개인정보를 이동통신사를 통해 확인받고 일종의 OTP (One Time Password)처럼 전송받은 인증번호를 통해 휴대폰 소지자에 대한 확인까지 수행하여, 알고 있는 것, 가지고 있는 것을 통한 본인확인이 이루어진다. 그러나 공인인증서와 마찬가지로 웹사이트에서 기존에 보유하고 있는 주민등록번호 또는 이용자에게 입력받은 주민등록번호를 이동통신사의 이용자 DB에서 찾아 유효성을 체크하는 방식으로 본인확인을 수행하여 주민등록번호 사용을 전제하고 있다.



(그림 2) 주민등록번호를 사용하는 휴대폰인증 방식

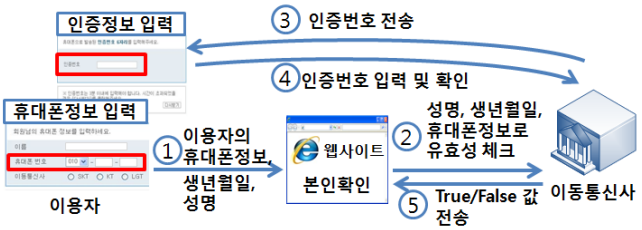
이렇게 안전성이나 신뢰성이 보장되는 국내 보편적인 본인확인수단에서도 주민등록번호의 사용이 요구되고 있어 개선이 필요한 상황이다.

4. 주민등록번호를 사용하지 않는 본인확인수단

본 논문에서는 기본적으로 본인확인에 대한 유일성이나 안전성, 신뢰성을 만족하되, 최대한 기존 인프라가 조성되어 있는 것을 활용하여 단 시간 내에 실제 도입할 수 있는 본인확인수단을 제안한다.

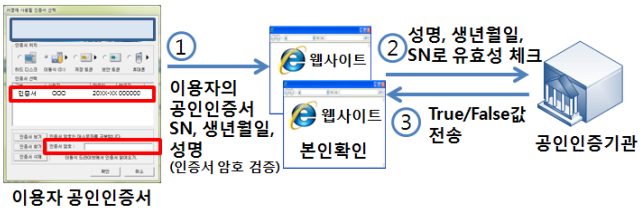
앞서 살펴본 휴대폰인증과 공인인증서 등은 안전성이나 신뢰성을 보장받으며 많은 이용자를 확보하고 있어 방식을 조금만 개선하면 주민등록번호를 사용하지 않을 수 있다.

휴대폰인증의 경우 이용자의 휴대폰정보, 주민등록번호, 성명을 이동통신사 DB에서 확인하는 방식이라 오프라인 및 신분증을 통한 본인확인을 끝낸 이동통신사 DB를 활용하되 온라인에서는 주민등록번호가 아닌 생년월일로 바꾸어 비교한다고 하더라도 충분히 본인확인의 목적을 달성할 수 있을 것이다. 즉, ① 이용자의 휴대폰정보, 생년월일, 성명을 입력받아 ② 이동통신사에서 DB정보와 비교한 뒤 ③ 해당 정보가 맞는다면 인증번호를 이용자 휴대폰에 전송하여 ④ 정확한 인증번호를 입력하는지 확인하고 본인이 맞는지 아닌지를 웹사이트에 알려주는 방식이다.



(그림 3) 생년월일을 사용하는 휴대폰인증 방식

이렇게 바꾼 휴대폰인증 방식은 이용자의 성명, 생년월일만으로는 동명이인이 발생할 수 있으나 휴대폰정보, 즉, 이동통신사와 휴대폰번호도 같이 비교하므로 한 사람을 지칭할 수 있을 것이고 인증번호 전송 및 확인을 통해 휴대폰 소지자에 대한 확인을 같이하여 휴대폰을 실제로 가지고 있는 휴대폰 명의자에 대한 본인확인이 가능하다.



(그림 4) 생년월일을 사용하는 공인인증서 방식

공인인증서의 경우 기존의 보편적인 방식으로는 웹사이트에서 별도의 검증된 개인의 정보를 알아야 하므로 공인인증기관을 통해 확인하는 방식으로 개선할 수 있다. 즉, ① 이용자의 인증서 암호를 입력받아 비밀 값을 알고 있는지 확인한 뒤 공인인증서를 안전하게 전송하여 ② 공인인증서에 있는 SN(Serial Number)와 이용자의 생년월일, 성명을 공인인증기관 DB와 비교하고 ③ 본인이 맞는지에 대한 결과 값을 전송하는 방식이다.

이 방식 역시 기존의 공인인증서에 있는 정보를 이용하되 인증서 암호를 알고 있어야 공인인증기관으로 정보가 전송되고 신뢰기관에서 정보를 검증하므로 안전성이나 신뢰성이 확보된다. 또한 공인인증서의 SN가 유일하므로 한 사람에 대한 확인이 가능하다. 공인인증서 방식은 공인인증서 내에 있는 다른 정보를 이용하거나 공인인증서의 정보를 변경하여 다른 방식으로도 개선할 수 있을 것이다.

5. 결론

위 제안을 통해 기존의 인프라를 많이 변형하지 않고 주민등록번호를 사용하지 않는 본인확인이 가능할 것으로 기대된다. 즉, 주민등록번호와 같은 민감한 정보를 이용자가 입력하지 않아도 될 것이다.

다만, 원칙적으로는 본인확인이 꼭 필요한 것인지 검토하여 본인확인의 요구를 최소한으로 줄이는 것이 더 중요할 것이며 주민등록번호를 사용하지 않는 본인확인수단에 대한 실제 서비스로의 실현을 위해 관련 기관들의 협조와 수행이 필요할 것이다. 또한 사업자가 부담하게 되는 인증비용을 절감하는 형태의 또 다른 본인확인수단 및 오프라인에서의 본인확인을 위한 주민등록번호 대체수단의 연구가 필요할 것이다.

참고문헌

[1] “주민등록법”, 1962.5
[2] “주민등록번호 수집·이용 최소화 방안 연구”, 한국정보화진흥원, 2009.3
[3] “개인정보보호체계 강화를 위한 정보통신망법 개정”, 방송통신위원회, 2012.2.17
[4] 랭키닷컴, http://www.rankey.com/
[5] 메트릭스, http://www.internetindex.co.kr/
[6] 코리안클릭, http://www.koreanclick.com/
[7] Ant Allan, "A Taxonomy of Authentication Methods, Update", Gartner, 2011.5
[8] “인터넷상 주민번호 사용 제한정책 시행 계획”, 방송통신위원회, 2012.6
[9] “식별번호를 이용한 본인확인 기술규격[v1.21]”, 한국인터넷진흥원, 2009.9