특집

인터넷 상에서 주민등록번호 대체수단 발전방향

염흥열, 이석래 (순천향대 정보보호학과, 한국정보보호진흥원 인증관리팀)

요약

주민등록번호 도용 문제가 사회적 문제가 되고 있고, 인터넷 사이트 가입시에 현재 가입자에 대한 본인확인이 정확히 수행되고 있지 않다. 대체수단은 성인 인증과 인터넷 사이트 가입시에 적용되며, 기존의 주민등록번호를 대체하여 인터넷 가입시에 활용 가능한 가입자 식별번호를 발급하고 폐지하는 절차와 프레임워크를 정의하고 있다. 본 논문에서는 최근 정보통신부가 추진하고 있는 주민등록번호 대체수단의 개요, 동작원리, 대체수단의 종류, 논쟁거리, 향후 발전 방향을 제시한다. 본 고는 주민등록번호 대체수단의 정책 결정에 유용하게 활용될 수 있을 것이다.[1][3]

I. 서 론

인터넷을 안심하고 편안한 마음으로 사용하기 위해서는 인터넷 사용자의 개인정보가 온라인상에서 적절한 수준으로 보호되어야 한다. 이러한 개인정보 보호는 수집 단계에서부터 필요이상의 개인정보가 수집되는 것을 막는 방법이 가장 효과적인 방법일 것이다. 우리 국민 모두가 소지하고 있는 주민등록번호에는 출생지, 성별, 생년월일 등 많은 개인정보 관련 정보가 포함되어 있다. 주민등록번호는 전자거래업체와 정부의 전자업무의 효율을 향상시키는 긍정적인 측면이 있다. 현재 인터넷 사이트 가입 시에 사이트 중복 가입 방지, 14세 이상여부, 성인 여부를 확인하기 위하여 대부분의 전자거래업체에서 이를 제출하기를 요구하고 있다. 이러한 상황에서 발생하는 가장 큰 문제는 신원확인을 위하여 수집되는 주민등록번호에 너무 많은 개인정보들이 포함되어 있다는 것과, 다른 사람이 타인의 주민등록번호를 도용하는 경우 이를 실효성 있게 확인 및 제어하기 위한 수단이 없다는 점, 그리고 온라인 경우 사용자가 실제 그 주민등록번호에 해당하는 사용자인지를 확인하는 신원 인증 기능이 없다는 점이다. 일반적으로 본인확인은 특정한 주체를 선언하는 신원선언 과정과 그 사용자가 현재 거래를 수행하는지를 확인하는 신원인증 과정을 통하여 이루어진다. 인터넷 거

래에서 본인확인은 인터넷 서비스를 제공하기 이전에 수행되어야 할 매우 중요한 기능이다. 오프라인의 경우 우리나라에서는 주민등록증과 거기에 부착된 사진을 이용하여 본인여부를 확인하고 있으며, 비대면 온라인 거래인 경우 아이디나 패스워드 방법과 생체 인증기법 등을 이용하여 신원확인을 받는다. 그러나, 온라인상에서 주민등록번호를 이용하여 본인확인을 수행하는 경우 전자거래업체는 기술적으로 오직 신원선언만을 확인하고 신원인증은 수행하지 않고 있는 실정이다. 따라서, 온라인상에서 신원 선언은 물론 신원 인증까지를 수행할 수 있는 대체수단이 필요하다. 또한 현재 주민등록번호는 대부분의 전자거래업체에서 특정 사용자를 위한 데이터베이스 관리 및 사용자 속성 관리 등을 위하여 사용되고 있다. 이 경우, 각 사용자의 주민등록번호가 너무 많은 전자거래 업체의 데이터베이스 상에 존재하게 되어, 유출 가능성이 높게 된다. 대표적으로 현재 나타나고 있는 주민등록 정보관련 대표적인 민원은 악의적인 사용자가 다른 사람의 주민등록번호를 도용하여 특정 인터넷 사이트에 가입하여, 주민등록번호를 도용당한 피해자가 그 사이트에 가입하고자 하는 경우 사이트 가입이 거부되는 문제로 나타나고 있다.

이러한 문제를 극복하기 위한 여러 기술적 대안 중의 하나가 주민등록번호 대체수단이다. 이 수단은 기본적으로 기존의 주민등록번호를 대체하기 위한 또 다른 차원의 식별번호를 한시적으로 사용자에게 부여하는 방법이다. 주민등록번호가 평생 동안 고유하게 본인과 연결되며 국가가 부여하는 고유 식별번호인 반면에, 대체 식별번호는 한시적으로 본인과 유일하게 연결되는 제삼의 신뢰기관이 부여하는 사용자의 식별정보이다. 이러한 주민등록번호 대체수단은 현재 전 세계 어느 나라에도 없음을 고려하면, 다른 나라의 사례를 벤치마킹할 수 없음은 자명하다.

지난 10월에 정보통신부에서 발표된 주민등록번호 수단(안)에 관한 가이드라인을 살펴보면, 주민등록번호 대체수단은 제삼의 신뢰기관인 본인확인정보관리기관(이하 관리기관이라 칭함)을 두고, 여기서 주민등록번호 대체 식별정보를 각 사용자에게 발행하며, 관리기관이 가져야할 기술적, 재정적, 운영적 조건들을 규정하고, 대체 정보를 발급받는 시점에 관리기관에 의하여 수행되어야 하는 신원확인 방법으로 대면확인 방법, 유무선 전화, 신용카드정보, 금융정보를 이용하는 온라인 방법, 그리고 공인인증서를 이용하여 신원확인 방법 등 여섯 가지의 신원확인 방법을 규정하고 있다. 또한 향후에 시범사업 시행, 세부시행방안 마련, 그리고 법제화 추진 등의 로드맵 또한 발표되었다.[1-3]

II. 주민등록번호 대체수단 일반사항

1. 주민등록번호의 특성과 사용 문제점

주민등록번호는 인터넷 사업자에게 가입자에게 적합한 서비스를 제공하고, 성년 여부를 확인할 수 있는 중요한 수단이 되어 왔다. 그러나 주민번호에는 출생지, 성별, 출생년월일 등의 많은 개인정보를 포함하고 있고, 한번 발급되고 나면 변경이 매우 어려우며, 평생 동안 가입자에 대한 유일성을 제공하고, 개인정보를 너무 많이 포함하고 있다.

이에 반하여 주민번호를 대체하기 위한 본인확인정보는 출생년월일, 성별 등의 개인정보를 전혀 포함하지 않고 있으며, 가입자가 언제든지 갱신, 폐지를 할 수 있으며, 본인확인 정보는 가입자와 한정적인 시간동안에만 유일성을 보장하고, 본인확인기관에 의하여 발급되는 난수이다.

현재 가장 심각한 문제는 다른 사람의 주민번호를 이용하여 인터넷 사이트에 회원으로 가입하고, 인터넷 사업자들이 필요 이상의 개인정보를 수집하여 다른 목적으로 이용할 가능성이 있다는 것이다. 물론 인터넷 사업자 측면에서는 정상적인 고객 맞춤형 상거래 행위라고 주장할 수 있지만, 개인정보를 보호해야 한다는 사용자 및 사회적 요구가 매우 큰 현 상태에서는 커다란 문제가 아닐 수 없다. 이는 주민등록번호와 이름이 정확하게 연관되어 있는지 만을 확인하는 신원선언만을 수행하고 실제로 신원인증은 하지 않는 문제에 기인한다. 따라서 인터넷 회원 가입시에 명확한 신원인증 기능이 필요하다고 할 수 있다.

지금 사용자가 각 인터넷 사업자마다 주민번호를 주고 인터넷 회원으로 가입하는 경우, 너무 많은 인터넷 사업자에게 자신의 개인정보를 전달하게 되어서 결과적으로 자신의 개인정보에 대한 자기 통제권을 상실하게 되는 문제점이 있다. 다시 말해, 자신의 주민번호가 너무 많은 인터넷 사이트에 분산되어 관리되어, 자신의 개인정보를 삭제하려면 모든 인터넷 사이트에 연락을 취해야 하고, 이는 많은 시간 및 노력을 요구하게 된다. 따라서, 주민등록번호 등의 개인정보에 대한 자기 통제권이 확보되어야 한다.

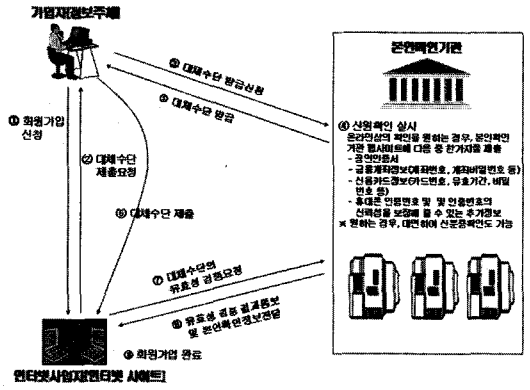
2. 대체수단을 위한 용어 정의

본인확인정보는 인터넷 상에서 본인확인을 위하여 본인확인기관이 각 가입자에게 부여하는 식별정보라고 정의될 수 있다. 본인확인서비스는 본인확인기관이 인터넷 상에서 본인확인정보를 이용하여 가입자를 유일하게 식별 인증하기 하여 필요한 제반 서비스라고 정의될 수 있다. 본인확인기관은 본인확인서비스를 제공하는 주체로서, 시설, 관리, 운영, 개인정보보호 요건을 만족하는 기관이라고 할 수 있다. 인터넷 사업자는 인터넷을 이용하여 정보 또는 서비스를 제공하는 일을 업으로 하는 기관이나 사람을 의미한다. 가입자는 본인확인기관에 자신의 개인정보를 제공하고 신원확인을 받은 후 인터넷 사이트 가입이나 성인 인증을 위하여 본인확인정보를 본인확인기관으로부터 발급받는 자를 의미한다.

3. 대체수단 서비스 모델 및 이용방법

대체수단 서비스 모델은 그림 1과 같다. 크게 가입자, 인터넷 사업자 또는 인터넷 사이트, 그리고 본인확인기관으로 구성된다. 대체수단 서비스 모델에서 가입자가 인터넷 사업자의 인터넷 홈페이지에서 가입을 요구하기 위한 절차는 다음과 같다.[1] [4-5]

- 가입자는 해당 인터넷 사이트의 홈페이지를 통하여 가입을 요청한다.
- 인터넷 사이트는 대체수단 제출을 요청한다.
- 사용자가 특정 대체수단을 선택하면, 인



〈그림 1〉 대체수단 서비스 모델

터넷 사업자는 해당 가입자를 대체수단을 발급하는 본인확인기관으로 연결한다.

- 가입자는 본인확인정보 발급을 본인확인기관에 요청한다. 이때 가입자는 본인확인기관이 선택하거나 본인이 원하는 신원확인방법으로 본인확인기관에 의하여 신원확인이 된다. 구체적인 신원확인 방법은 주민등록증을 이용한 면대면 인증방법, 공인 인증서를 이용하는 방법, 은행의 계좌번호와 비밀번호를 이용하는 방법, 신용카드 번호와 비밀번호를 이용하는 방법, 휴대폰을 이용한 인증 코드와 이를 보완하기 위한 추가정보를 통하여 신분확인이 이루어진다.
- 본인확인기관은 특정 가입자에 대하여 신원확인을 한 후 가입자에게 본인확인정보를 발급하게 된다.
- 가입자는 해당 본인확인정보를 가입을 원하는 인터넷 사업자에게 전달한다. 본인확인정보는 특정 가입자와 한시적으로 결합되는 난수라고 볼 수 있다.
- 인터넷 사업자는 본인확인정보의 유효성을 본인확인기관에 요청한다.
- 본인확인기관은 유효성 결과를 인터넷 사업자에게 통보한다.
- 인터넷 사용자는 이 본인확인정보의 무결성 및 인증성을 검사한 후, 해당 사용자에 대한 회원가입을 허락한다.

예를 들어 현재 인터넷 사이트에 가입하려면 해당 홈페이지에 가서 주민등록번호를 입력하고 사이트에 가입하게 된다. 이때 주민등록번호와 실명을 이용하여 신원선언이 이루어진다. 따라서 진정한 의미의 신원확인을 하지 않는데 기인하여 주민등록번호의 도용 문제가 발생하게 된다. 그러나 주민등록번호 대체수단을 이용하면, 본인확인기관으로 먼저 가서 5가지 방법으로 신원확인을 받은 후 본인확인기관으로부터 주민등록번호를 대체할 본인확인정보를 발급받아 그것을 이용하여 인터넷 사이트에 가입하게 된다. 본인확인 기관에서 수행하는 신원확인 방법은 크게 본인확인기관에 직접 출석하는 대면 확인 방법, 공인인증서를 이용하는 방법, 계좌번호와 비밀번호를 이용하는 방법, 신용카드 번호와 비밀번호를 이용하는 방법, 그리고 인증번호와 신원확인증표의 사본확인 등을 이용하는 가입자 휴대폰 유무선 전화기를 이용한 인증 방법 등이 제시되고 있다. 가입자는 이중 한 가지 방법을 이용하여 신원확인을 받은 후 본인확인기관으로부터 본인확인 정보를 발급받아서 해당 인터넷 사이트에 가입하게 된다. 이 과정은 인터넷 사이트를 처음으로 가입할 때 단 한번만 수행되며, 추후 가입 시에는 본인확인기관으로부터 발급받은 본인확인 정보로 바로 인터넷 사이트에 가입하게 되는 것이다.

4. 본인확인정보의 구성 및 발급 조건

본인확인정보는 생년월일, 출생지, 성별 등의 개인정보를 포함하지 않는 13자리 이상의 숫자나 영문자로 구성되며, 본인확인정보에 본인확인기관을 식별할 수 있는 정보가 포함되어야 하며, 본인확인기관은 가입자에게 부여하는 본인확인정보에 대한 유일성을 보장하도록 발행해야 한다.

본인확인정보는 정당한 사유가 있어 대리인을 통해 발급 받는 경우를 제외하고는 타인 명의로 본인확인정보를 발급 받아서는 안 되고, 본인확인기관은 가입자가 본인확인정보의 유효기간을 관리하거나 선택 할 수 있는 기능을 제공하여야 하며, 본인확인기관은 본인확인정보를 인터넷을 통해 전송하는 경우 당해 전송정보의 위조 및 변조를 방지하는 기능을 제공하여야 한다. 본인확인기관은 다음의 경우 본인확인정보를 폐지하여야 한다.

① 가입자가 본인확인정보의 폐지를 신청한 경우
② 본인확인정보를 사위 기타 부정한 방법으로 발급받은 사실을 인지한 경우
③ 본인확인정보가 분실훼손 또는 도난 유출된 사실을 인지한 경우

또한, ②,③의 경우에는 본인확인기관은 가입자 및 자신의 인터넷 서비스를 이용하는 인터넷 사업자에게 본인확인정보의 폐지사실을 통지하여야 한다.

본인확인기관은 본인확인 서비스를 위하여 수집된 개인정보를 보호하기 위하여 법령에 특별한 규정이 있는 경우를 제외하고, 본인확인정보의 본인확인을 위한 목적 외 이용 및 제3자에게 제공해서는 안된다. 본인확인기관 및 인터넷사업자가 보유중인 본인확인정보의 보호에 관하여서는 「정보통신망이용촉진및정보보호등에관한법률」의 개인정보에 관한 규정을 준용한다.

본인확인기관은 본인확인정보의 유효성 확인 서비스, 이용자의 동의를 얻은 경우 연령 성별 확인 서비스를 제공 가능하다. 또한 본인확인기관은 가입자에게 본인확인정보 발급 갱신 폐지 등의 내역을 확인할 수 있는 방법을 제공할 수 있다. 정보통신망을 통하여 인터넷사업자와 유효성 확인서비스 내용 등을 송수신하는 경우에는 해당 내용에 대한 위변조 검출 기능을 제공해야 한다.

본인확인기관은 가입자의 요구가 있는 때에는 지체 없이 본인확인을 위해 수집,이용중인 주민등록번호를 파기하여야 한다.

5. 본인확인기관에 의한 신원확인 방법

가입자에 대한 신원확인 기준은 내국인의 경우 주민등록표에 기재된 성명 및 주민등록번호, 재외국인의 경우 여권에 기재된 성명 및 여권번호, 그리고 외국인의 경우 등록외국인기록표에 기재된 성명 및 등록번호 등이다.

가입자에 대한 신원확인방법은 대면확인방법과 비대면 확인 또는 온라인 확인방법으로 구분된다. 대면확인방법은 신원확인증표를 이용한 대면확인 방법으로 주민등록증 발급 대상자의 경우 주민등록증을 이용하고, 주민등록 발급대상자가 아닌 사람은 국가 기관, 지방자치단체 또는 학교의 장이 발급한 증표

와 본인의 주민등록표등본과 법정대리인의 주민등록증을 이용하며, 재외국인 경우 여권 또는 재외국민등록증, 그리고 외국인의 경우 출입국관리법에 의한 외국인 등록증을 이용한다. 온라인 인증방법은 가입자의 공인인증서와 비밀번호를 이용한 전자서명 방법, 계좌번호와 비밀번호를 이용하는 가입자의 금융거래 계좌 인증, 신용카드 번호와 유효기간, 그리고 비밀번호를 이용한 가입자의 신용카드 인증, 그리고 가입자의 이동전화번호 및 신원확인표의 사본 확인 등을 이용한 인증번호 및 추가 정보를 이용하는 인증 방법 등이 있다.

6. 본인확인기관의 자격요건

본인확인기관이 가져야 할 요건은 크게 기술능력, 재정능력, 시설 및 장비 능력이 있어야 한다. 기술능력의 경우, 본인확인 서비스의 안전성과 신뢰성을 확보하기 위하여 필요한 시설 및 방비 운영인력으로 요건을 갖춘 8인 이상으로 구성되어야 하며, 재정능력의 경우 자본금 50억 이상으로 했으며, 시설 및 장비의 경우, 가입자의 등록정보를 관리하기 위한 설비, 본인확인정보를 생성 및 관리하기 위한 설비, 그리고 시설 및 장비를 안전하게 운영하기 위한 보호 설비로 구성된다. 또한 본인확인기관은 전자적 침해행위로부터 보호조치를 취해야 하고, 외부인의 출입통제 등 방호조치, 화재 및 수해 등 재해에 대비한 조치, 그리고 기타 안전성을 확보하기 위한 관리적 조치를 취해야 한다.

7. 본인확인기관에 대한 적합성 평가와 환경영향평가

한국정보보호진흥원은 본인확인기관의 신청이 있는 경우 본인확인기관의 요건, 보호조치, 그리고 기관의 공정성에서 규정된 요건의 충족여부에 대한 적합성평가를 실시할 수 있다. 그리고 본인확인기관은 개인정보를 취급하는 새로운 서비스를 제공하거나 대량의 개인정보를 축적하는 데이터베이스 등의 전산시스템을 구축하는 경우 당해 서비스 또는 전산시스템이 고객의 개인정보보호에 미칠 영향 을 평가하는 등 개인정보 침해 예방을 위한 최선의 조치를 강구하여야 한다.

8. 대체수단의 활용방안

본인확인 수단이 안전성과 편의성을 모두 만족하기는 어려우므로 인터넷 사업자는 안전성, 편의성, 법적 요구 정도 등을 종합적으로 고려하여 용도에 맞는 대체수단을 선택 활용해야 한다. 대체수단의 종류 및 발급 시 신원확인 방법에 따라 안전성이 다르므로 서비스의 성격과 안전성의 요구 정도 등을 고려하여 적합한 대체수단을 선택한다.

공인인증서를 이용하는 방법은 안전성이 가장 높으나 편리성이 떨어지며, 문제가 발생한 경우 배상책임은 전자서명법에 의거하여 공인인증기관에게 지워지게 된다. 그 외 방법은 안전성은 공인인증서 방식보다는 낮으나, 사용자 편리성이 좋은 특성이 있다. 그러나, 문제가 발생한 경우, 손해배상은 과실책임주의 원칙에 의하여 결정된다. 즉, 과실 책임의 소재를 가려서 배상이 이루어지게 된다.

〈표 1〉 대체수단의 비교

구분	공인인증서(대체수단)	공인인증서 이외의 대체수단	주민번호 실명확인 서비스
안전성	높음	중간	낮음
편의성	낮음	중간	높음
배상책임	전자서명법에 의해 공인인증기관에게 배상책임 규정	손해배상에 대해 과실책임주의(민법 제750조) 원칙에 따라 해결	손해배상에 대해 과실책임주의(민법 제750조) 원칙에 따라 해결

9. 중복가입 여부 확인

인터넷 사업자가 특정 가입자의 중복가입을 확인할 수 있어야 한다. 중복가입의 확인이 필요한 대표적인 인터넷 사업자는 인터넷 복권 및 경매 등과 연관된 사업자로 알려지고 있다. 본인확인기관은 인터넷 사업자에게 중복가입 여부를 확인해야 한다. 만약 인터넷 사업자가 1개의 대체수단을 수용하는 경우, 1개의 본인확인기관으로부터 1개의 대체수단만 발급 가능하므로 기본적으로 중복가입 여부는 확인 가능하다. 그러나, 가입자가 사이트 회원탈퇴 없이 대체수단을 폐지한 경우, 가입자가 새로운 대체수단을 발급받아 동일 사이트에 중복가입이 가능하다. 이 경우 인터넷 사업자가 식별번호 검증 시에 중복가입 여부 확인을 위해 필요한 자료를 요청하면 본인확인기관은 본인여부 확인결과와 함께 중복가입 확인 위한 자료를 제공해야 한다.

인터넷 사업자가 2개 이상의 대체수단을 수용 할 경우, 1개의 대체수단 수용시 중복가입 문제와 복수 대체수단의 발급가능으로 인한 중복가입 문제가 동시 발생한다. 이 경우 본인확인기관이 중복가입 확인을 위해 필요한 최소한의 정보를 다른 본인확인기관에게 제공하여 복수 대체수단 발급으로 인한 중복 문제를 해결해야 한다.

10. 본인확인기관의 부가서비스

본인확인기관은 연령확인 서비스와 성별확인 서비스를 인터넷 사업자에게 제공할 수 있다. 연령 확인 서비스 제공이 필요한 경우, 이는 14세 미만의 경우 아동의 개인정보 수집 시 법정대리인의 동의획득(정통망법)을 해야 하며, 12세, 15세, 18세의 경우 게임 등에 이용 가능한 연령(등급) 표시의무(음반 비디오물 및 게임물에 관한 법률)와 연관되며, 19세의 경우 청소년유해매체물의 경우 유해매체물 표시 및 연령확인(청소년보호법)과 연관된다. 인터넷 사업자가 식별번호 검증 시에 "19세 이상 여부를 알려달라"는 식으로 연령에 대한 정보를 요청하면 본인확인기관은 본인여부 확인 결과와 함께 그 여부를 알려줄 수 있다. 성별확인의 경우에도 서비스의 특성상 성별정보가 반드시 필요하다면 인터넷 사업자가 식별번호 검증 시에 성별에 대한 정보를 요청하면 본인확인기관은 본인여부 확인결과와 함께 성별을 알려줄 수 있다.

11. 향후 추진로드맵

현재 시범사업이 시행중에 있으며, 로드맵이 발표되었는데, 큰 방향은 두 가지이다. 하나는 법제화하여 대체수단을 의무화하는 방안이고, 다른 하나는 현재대로 자율 운영 방안이다. 법제도화 하는 경우 2005년 내에 대체수단을 마련하고 시범사업을 실시하며, 2006년도부터 공공기관을 중심으로 일부 시행하고, 2007년도에 의무적으로 전면시행하게 되어 있다. 이렇게 되면 주민번호기입 없

이 대체수단을 이용하여 인터넷 사이트에 가입할 수 있게 된다. 자율 운영방안인 경우도, 금년 내에 대체수단을 마련하고 시범사업을 실시하고, 2006년 상반기에 일부 시행하며, 2006년도 하반기부터 전면 시행하도록 되어 있다.

III. 주민번호 대체수단의 종류 및 특성

현재 그린버튼 서비스(이니텍과 전자인증), 공인인증서를 이용한 주민번호 대체 서비스(한국정보인증), 가상주민번호 서비스(한국신용평가정보), 개인 ID 인증 서비스(서울신용정보), 개인 인증키(한국신용정보) 등의 5가지 대체수단이 제시되고 있다. 기본적으로 이름은 다르지만 동작원리는 비슷하고, 본인확인기관을 두어 여기서 현재 주민번호를 대신할 본인확인정보를 발행하는 방식으로써 인증서 사용 여부에 따라서 두 가지로 구분될 수 있다. 그린버튼 서비스와 공인인증서를 이용한 주민번호 대체 서비스 등 인증서를 이용한 방식과 가상주민번호 서비스, 개인 ID 인증서비스, 그리고 개인 인증키를 이용한 서비스는 기존의 주민번호와 비슷하나, 여기에서 개인정보를 제거한 방식이라고 볼 수 있다. 기본적으로 무료로 발급되며 대체수단의 명칭은 서로 다르지만 이용자가 금융계좌, 공인인증서, 신용카드번호, 휴대폰 인증번호 등의 신원 정보를 인터넷으로 해당 발급기관에 제공하고 13자리 난수를 발급 받는 방식은 동일하다. 각 방식은 각각 독창성이 있으며, 안전성, 편리성 등에 있어서 약간 차이가 있다. 가입자는 이 5가지 방법 중 인터넷 사업자가 제시하거나, 가입자 자신이 선택한 한 가지 이상의 대체수단을 선택하면 된다.

〈표 2〉 대체수단의 비교

기관	대체수단(안)	비고
한국신용평가정보	o 가상주민번호 : 난수화된 가상번호를 인터넷, 휴대폰 등으로 발급받아 이용자가 웹사이트 회원가입 시 이를 입력	주민번호 실명확인 서비스를 제공하는 신용평가기관
한국신용정보	o 개인인증키 : 사이트 회원가입 시 이용자는 개인인증키를 사용할 수 있는 비밀번호를 입력하여 본인확인, 본인확인 후 13자리 난수로 구성된 개인 인증키를 해당 웹사이트에 전송	
서울신용평가정보	o 개인ID인증서비스 : 인터넷으로 ID/PW를 발급받아 이용자가 웹사이트 회원가입시 이를 입력하여 본인확인, 본인확인 후 난수화된 13자리의 가상식별코드를 해당 웹사이트에 전송	
한국정보인증	o 공인인증서 : 웹사이트 회원가입시 공인인증서 검증을 통해 본인확인, 공인인증서 검증 후 해당 이용자에게 13자리의 식별번호를 부여하고 이를 해당 웹사이트에 전송	전자서명법에 의한 공인인증기관
한국전자인증	o 그린버튼 서비스 : 이용자는 인터넷으로 온라인 신원확인용 인증서를 발급받아 웹사이트 회원가입시 인증서 검증을 통해 본인확인, 인증서 검증 후 해당 이용자에게 13자리의 식별번호를 부여하고 이를 해당 웹사이트에 전송	

Ⅳ. 쟁점사항

지금까지 제기되고 있는 쟁점은 다음과 같다. 여기서는 각 쟁점을 분석하고, 쟁점에 대한 대안을 제시한다.

1. 중복가입 검사 프로토콜

특정한 인터넷 사이트에서 요구되는 중복가입을 검사하기 위하여 요구되는 중복 가입을 검사하기 위하여 본인확인기관 간에 주민등록번호의 제공도 문제가 될 수 있다. 만약 본인확인기관이 여러 개가 발생할 경우, 여러 가입자의 주민등록번호의 공유를 요구하게 되며, 제도 자체의 근본 도입 목적을 훼손할 수 있다. 따라서 주민등록번호를 직접적으로 공유하는 방법이 아니라, 주민등록번호를 공유하지 않고 수행되는 방법으로 중복가입을 검사할 수 있는 보안 프로토콜의 개발이 요구되며, 이에 대한 기술 표준화가 필요하다.

2. 국내외 표준화 추진

현재의 주민등록번호 대체수단을 위한 기본 프레임워크 등이 표준화되어 있지 않아 상호연동성과 개발 비용의 증가 등의 문제를 초래할 수 도 있다. 현재 가능한 주민등록번호 대체수단의 구현 방법은 크게 5가지 정도로 분류될 수 있다. 그러므로, 현재 구현되는 모든 방법을 수용하면서 시스템 및 구성요소 간의 상호호환성을 보장하는 대체수단에 대한 프로토콜의 개발과 이에 대한 국내외 표준화가 필요하다고 할 수 있다.

3. 보안성 논란

주민번호 대체수단의 보안성은 최소의 보안성을 요구하고 있다. 그러나, 보안에 있어서 편리성과 보안성은 타협의 관계로 볼 수 있다. 이는 보안성을 강화하면 편리성이 손상됨을 의미한다. 요새 문제가 되고 있는 인터넷 금융에서의 보안성 문제와 전자정부에서의 보안성 문제는 모두 보안성보다는 편리성에 무게를 두어 발생한 문제라고 볼 수 있다. 따라서, 주민등록번호 대체수단도 보안성의 향상이 무엇보다도 중요하다고 할 수 있다. 따라서, 대체수단을 위한 향상된 보안 요구사항이 필요하며 이에 따라 보안성 평가가 이루어져야 한다. 특히, 본인확인기관과 인터넷 사업자간에 부인방지 서비스 등의 기능도 추가되어야 할 보안 요구사항이라고 할 수 있다.

4. 인터넷 실명제 연관

주민등록번호 대체수단은 인터넷 실명제를 보완하는 수단이 될 수 있다. 일반적으로 가입자들은 사이버 상에서 익명성을 제공받고 싶어 한다. 이는 사용자의 당연한 권한이기도 하다. 그러나, 이는 어디까지나 불법 행위를 하지 않았을 때 보장되어야 한다. 만약 가입자가 사이버 상에서 명예 훼손 등의 불법 행위를 했을 때에는 적절한 법절차에 따라서 익명성을 취소할 수 있는 절차가 필요하다. 이를 조건적 익명성을 제공하는 인터넷 실명제라고 할 수 있다. 다시 말해, 불법 행위 이전까지는 익명성을 보장해주고 불법 행위가 이루어지면 익명성을 취소 가능케 하는 제도

가 현재 도입코자 하는 주민등록번호 대체수단이라고 할 수 있다. 따라서, 제도의 적절한 활용을 통하여 이를 인터넷 실명제와 연계하면, 인터넷 실명제에 대한 사용자의 저항도 최소화 할 수 있다고 볼 수 있다. 따라서, 주민등록번호 대체수단은 인터넷 실명제를 보완할 수 있는 좋은 대안이라고 할 수 있다.

5. 법제화 필요성

주민등록번호 대체수단이 법 · 제도 하에서 시행되는 것이 아니라, 가이드라인의 권고형식으로 도입되고 있다는 것이다. 이는 제도 도입 초기에 관련 이해 당사자의 저항을 최소화할 수 있는 효과적인 방법일 수 있다는 것을 인정함에도 불구하고, 가이드라인 형태의 제도이므로 강제성이 없어서 결국 제도 도입 목적 자체를 훼손시킬 소지가 있다. 또한 가인드라인 형태로 운영하면, 여러 개의 본인확인기관이 존재할 가능성이 있다는 문제점도 있다. 따라서 이러한 제반 사항들의 해결이 요구되며, 법 · 제도로의 수용이 요구되고 있다고 할 수 있다.

6. 실효성 문제

가이드라인으로 시행되고 있으니, 실행하지 않으면 그만이 아니냐 하는 실효성 문제이다. 현재 주민등록번호 대체수단은 가이드라인 형식이다. 이는 법적인 강제 사항은 없음을 의미한다. 그러나, 법제화될 경우 사회적 합의가 전제되어야 하며, 사회적 합의가 법 · 제도일 경우, 의무적인 대체수단의 시행이 이루어 질 수 있다. 현재 정통부에서는 법제화 방안과 자율 운영방안을 모두 고려하고 있고, 내년도에 추가 연구를 통하여 구체적인 방향을 결정하려고 하고 있다.

7. 대체수단 간의 호환성

현재 5가지 수단 간의 상호 호환성은 제공하지 않는다. 따라서, 가입자가 한 가지를 선택하여 특정의 인터넷 사이트에서 사용해야 한다. 즉, 가입자는 원하면 여러 개의 대체수단을 자유롭게 사용할 수 있다. 가입자가 여러 본인확인 기관의 서비스를 중복적으로 받을 수 있음을 의미합니다. 그러나 인터넷 사이트에 대한 중복 가입 문제는 인터넷 사이트가 중복 가입을 방지하고자 할 경우, 기술적으로 여러 대체수단을 가입자가 이용하더라도 중복가입을 막을 수 있도록 구성되어 있다.

8. 시민단체와 인터넷 사업자의 의견

기본적으로 현재의 주민등록번호를 대체해야 한다는 기본 입장에는 동의하고 있다. 그러나, 각론에 있어서, 인터넷 업체에서 복잡성, 속도 저하의 원인 제공, 본인확인기관의 신뢰성에 대한 문제점을 지적하고 있다. 시민단체의 경우 법제화와 자율화에 대한 사회적 합의의 필요성이 주장되고 있고, 인터넷 실명제와 연계성 등의 문제가 지적되고 있으며, 부가 서비스에 대한 개인정보침해 가능성, 그리고 안전성, 편리성, 경제성에 균형유지에 대한 문제가 제기되고 있다. 이 문제는 장기적으로 사회적 합의가 전제되는 문제이다.

9. 인터넷 사업자의 부담

인터넷 업체가 시스템 및 데이터베이스를 변경해야 하는 부담이 있는 것은 확실하다. 따라서 시행 일시를 조정하여 인터넷 사업자가 이에 대비할 시간을 주어야 한다. 그리고 비용은 이용자에게는 떠넘기지 않을 것으로 예측된다. 현재도 실명확인 서비스를 인터넷 사이트들이 한 후 사이트 가입을 받기 때문에, 이에 대한 비용이 인터넷 업체에서 부담하고 있는 것으로 알고 있다. 가이드라인에 가입자에게 비용이 전가되지 않도록 구성되어 있다.

V. 결론

현재 정보통신부에서 추진 중인 주민등록번호 대체수단이 실질적 효과를 가지기 위해서는 다음과 같은 정책적 고려가 필요하다. 첫째, 새로운 정책의 도입은 인터넷 사이트 가입을 위하여 새로운 활동을 요구하게 되어 기존 정보격차를 심화시킬 수 있는 요인이 될 수 있다. 따라서, 정보격차를 심화시키는 것을 방지하기 위한 사용자에 대한 적극적인 교육과 홍보가 요구되며, 보호 수단이 사용자의 편리성과 최소한의 안전성을 동시에 만족하도록 해야 하는 숙제를 안고 있다. 현재 특정한 기술적인 대체수단을 결정하지 않고, 시장에게 우월한 대체수단을 결정하게 하는 방법은 바람직한 방법이라고 볼 수 있으나, 시장에서 사용될 수 있는 대체수단이 가져야 할 최소한의 안전성 기준과 이에 대한 평가 기준 수립도 정부차원에서 마련되어야 할 것으로 보여 진다. 둘째, 현재 주민등록번호 대체수단이 실효적으로 성공하기 위해서는 먼저 법적 체계의 정비가 요구되고 있다. 현재의 주민등록번호 대체수단이 가이드라인 성격이어서 구속력이 없고, 이를 강제하기 위한 실효적인 제어 방법을 찾기가 매우 어렵다는 점이 있다. 따라서, 현재 제정을 고려하고 있는 개인정보보호법에 전자거래업체에 의한 필요이상의 주민등록번호 수집을 제한하게 하고, 이를 구체적으로 담보할 수 있는 식별확인정보관리 기관의 법적인 지위의 확보가 요구되고 있다. 이러한 노력은 국회와 정부를 포함한 범국가 차원에서 이루어져야 한다고 판단된다. 셋째, 현재까지 제안되고 있는 대체기술이 여러 가지 보호 수단들이 존재하며, 각 기술 수단 별로 안전성 수준의 차이가 존재하므로, 따라서 최소 안전성 수준과 안전성 평가 방법의 개발이 요구되며, 이 평가 기준에 의한 관리기관에 대한 점검 또는 만족 여부를 평가가 요구되며, 사용자에게 평가를 통과한 관리기관을 알리는 적절한 방안 마련이 요구되고 있다. 이는 평가 통과 마크를 부여하는 방법도 고려해볼 만하다. 넷째, 관리기관의 난립을 막는 대책이 요구되고 있다. 현재와 같이 가이드라인 성격으로 이러한 정책을 집행한다면, 관리기관의 난립이라는 새로운 문제가 발생하게 될 수 있다. 많은 전자거래업체가 별도의 유령 회사를 설립하여 관리기관의 역할을 수행한다면, 이전과 동일한 상황을 초래하게 되어 인터넷상의 본인확인 식별번호 정책 자체를 무력화할 수 있다. 따라서 관리기관의 난립을 방지하는 대책인 평가와 심사를 통한 일정개수 이하의 관리기관의 지정 또는 인정이 필요하다고 생각된다. 다섯째, 무슨 정책이든

각 참여 주체의 적극적이고 자발적인 참여가 있어야 성공할 수 있다. 각 주체들의 다양한 의견을 수렴하기 위한 의견 수렴을 통하여 다양한 주체들의 의견을 반영한 최선의 수단 마련과 이를 유인하기 위한 정책적 배려도 필요하다. 다행히 정보통신부의 로드맵에 설문조사가 마련되어 있고, 이를 통하여 참여 주체에 대한 배려 방안을 마련하기 위한 기초 자료를 획득해야 한다. 또한 각 주체를 적절하게 유도할 수 있는 인센티브의 도입도 고려할 만하다. 정책적 차원에서 현재 주민등록번호 대체수단이 마련된 만큼 전자거래 업체의 데이터베이스 변경이나 기타 애로점을 자발적으로 극복하게 하는 유인책의 마련도 이 정책을 성공적으로 완수할 수 있는 요인이라고 할 수 있다. 결론적으로 정부의 이 정책에 대한 장기적인 로드맵을 포함하는 분명한 의지 표명이 요구되는 시점이다. 또한 주민등록번호 대체수단이 성공하기 위해서는 사전에 전제되어야 할 법적, 제도적, 교육 홍보 등의 기반이 먼저 조성되어야 한다고 생각한다. 단기적으로는 관리기관의 인증 마크 부여 하는 등 자발적으로 대체수단으로 유인하는 정책의 집행과 함께, 중장기적으로 주민등록번호 수집을 용도이외 목적으로 수집 및 이용하게 못하게 하는 개인정보보호법 등의 법적 대응 마련이 필요하며, 이러한 법체계 하에서 관리기관을 지정하고, 관리기관의 난립을 방지하며, 보호 수단의 안전성 평가와 평가된 수단의 사용을 권유하는 정책적 집행 환경 조성이 요구되고 있는 시점이다.

본 고에서는 주민등록번호를 대체할 수 있는 주민등록번호 대체기술을 살펴보고, 여기서 발생하는 다양한 논쟁거리를 분석했으며 향후 발전 방향을 제시하였다.

Ack: 본 연구의 일부는 정보통신부 및 정보통신연구진흥원에서 지원하는 ITRC 사업에 의하여 수행되었습니다.

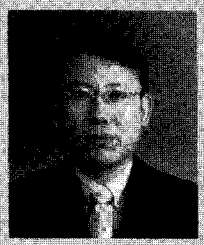
참고 문헌

1. 정보통신부, 인터넷상의 주민등록번호 대체수단 가이드라인, 2005.11.
2. 전성배, 인터넷상의 주민번호 대체수단 가이드라인 및 향후 추진 로드맵, 2005.10. 공청회 발표자료
3. 염흥열, 인터넷 상에서의 주민등록번호 보호수단 기준(안), 2005.5. 공청회 발표자료
4. 염흥열, 주민등록번호 보호 수단, 2005.6.9. 디지털타임즈 전망대
5. 이석래, 주민번호대체수단으로 공인인증서 활용방안, 2005. 8. 31. PKI-KR2005

저자소개

염 흥 열

1981년 2월 한양대학교 전자공학과 졸업(학사)
1983년 2월 한양대학교 대학원 전자공학과 졸업(석사)
1990년 2월 한양대학교 대학원 전자공학과 졸업(박사)
1982년 12월 – 1990년 9월 한국전자통신연구소 선임연구원
1990년 9월 – 현재 순천향대학교 공과대학 정보보호학과 교수
1997년 3월 – 2000년 3월 순천향대학교 산업기술연구소 소장
2000년 4월 – 현재 순천향대학교 산학연컨소시엄센터 소장
1997년 3월 – 현재 한국정보보호학회 총무이사, 학술이사, 교육이사
2004년 1월 – 현재 한국인터넷정보학회 이사, 논문지 편집위원
2003년 9월 – 2004년 3월 ITU-T SG17/Q10, Associate Rapporteur
2004년 3월 – 현재 : ITU-T SG17/Q9 Rapporteur
주관심 분야 네트워크보안, 전자상거래보안, 공개키 기반구조, 부호이론, 이동통신보안



이 석 래

1992년 2월 한양대학교 전자통신공학과 졸업(학사)
1994년 2월 한양대학교 대학원 전자통신공학과 졸업(석사)
1994년 1월 – 1999년 6월 LG전자 멀티미디어연구소 주임연구원
1999년 7월 – 현재 한국정보보호진흥원 인증관리팀 팀장
주관심 분야 전자상거래보안, 네트워크보안