개인정보 유출 피해 방지를 위한 공인인증서 기반 인터넷 개인인증체계 개선 모델에 관한 연구

이정현* · 권헌영** · 임종인*

요 약

최근 인터넷을 통해 개인정보 유출사례가 빈번히 발생하고 있으며, 한번 유출된 개인정보는 회수·변경이 어렵고, 명의도용·사기 등 제3의 범죄로 까지 이어지고 있어 국가차원의 대책 마련이 요구된다. 현재 각 포털社·쇼핑몰 등 인터넷 사업자는 회원 가입시 개인정보를 무분별하게 수집하고 있으며 제대로 된 보안관리가 이루어지지 않고 있는 실정이다. 이러한 상황은 시간이 지날수록 해커가 공격할 수 있는 취약 요인의 수만 증가 시킬 뿐이며 보안 관리 범위도 통제할 수 없게 된다. 또한 국내·외 해커들은 금전적 이득을 얻기 위해 개인정보를 선호하고 있어 향후에도 개인정보 유출 사고는 지속 증가할 것으로 예상된다. 이에 본 논문에서 인터넷 회원가입을 위해 수집하는 개인정보 보안 관리 실태를 살펴보고 유출된 개인정보를 인터넷에서 재사용할 수 없도록 하는 공인인증서 기반 개인 인증체계 개선 모델을 제안하기로 한다.

A Study on Certificate-based Personal Authentification System for Preventing Private Information Leakage through Internet

Jung Hyun Lee* · Hun Young Kwon** · Jong In Lim*

ABSTRACT

Recently, We have many private information leakage cases through internet which cause social problems and it is impossible to change or update the leaked information, it is also used to the third crime such as identity theft, internet fraud. Hackers are interested in stealing private information for making money, in this point private information leakage problems are constantly increased hereafter. In this paper, I surveyed the authorization model on site registration which is currently used in Korea, and the problem of collecting personal identification number, I proposed policy model of useless method of private information, especially leaked information can not be used anymore in internet.

Key words : Privacy, Personal Identification Number, Internet Authentication, I-Pin, Certificate

접수일 : 2010년 9월 25일; 채택일 : 2010년 12월 2일

* 고려대학교 정보경영공학전문대학원

** 광운대학교 법학과

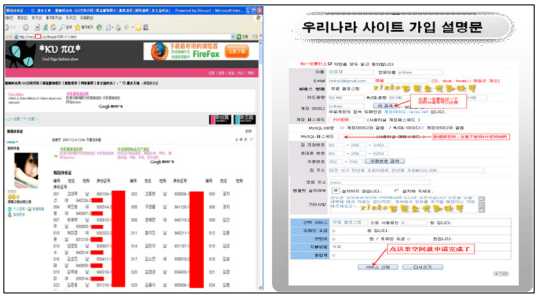
1. 서 론

인터넷의 발달은 전자상거래의 활성화는 물론 전자정부 출현으로까지 이어져 국민생활의 편리함과 동시에 업무처리의 신속함까지 더해 한층 풍요로운 삶을 영위할 수 있는 계기를 마련하였다. 또한, Web2.0의 출현으로 보다 인터렉티브한 사용자와의 의사소통이 가능해지는 등 국민생활에서 보편적인 서비스로까지 자리 잡았다[1]. (그림 1)에서 보는 바와 같이 한국인터넷진흥원(KISA)에 따르면 개인정보 유출사례는 최근 3년 간 2배 이상 증가하고 있으며, 개인정보를 탈취하기 위한 공격들도 교묘하고 지능적으로 발전하고 있다고 지적하고 있다[2].

(그림 1) 최근 개인정보 유출 사례

하지만 2008년도 한 해 동안 유명포털 사이트, 경매 사이트, 정유사, 통신사 등 2천 8백만여건 개인정보 유출사례를 볼 때 인터넷을 통한 개인정보 유출을 더 이상 개인의 문제가 아닌 국가차원에서 보호해야 될 중요한 문제라고 할 수 있다. 또한 중국 등 해외 개인 블로그에는 이미 유출된 우리나라 국민의 이름, 주민번호 등이 수 천 건씩 게재되고, 사이트 가입시 명의도용 등을 유도하는 한편, 보이스피싱 등 각종범죄 사례도 쉽게 발견할 수 있을 정도로 개인정보 악용사례가 지속 발생하고 있다. (그림 2)는 실제 해외사이트에 게재된 우리나라 국민의 주민번호와 그에 대한 활용 방법을 보여주고 있는 사례이다.

이러한 상황에 각 인터넷 사이트별 사용자 개인



(그림 2) 해외사이트에 게재된 개인정보 및 사용법

정보 수집은 일상화 되어 있고, 일반사용자 또한 본인의 개인정보가 향후에 어떻게 활용되는지 여부조차 알지 못한 체 회원 가입시 동의하고, 동의하지 않으면 가입조차 할 수 없게 되어 있다. 2008년도 한 해 동안 개인정보 유출사고의 유형을 보면 다음과 같이 크게 4가지로 나눠볼 수 있다.

① 개인정보 DB 해킹
② 내부자에 의한 유출
③ 개인정보 관리소홀
④ 개인정보 무단제공으로 인한 오·남용

위에서와 같이 유출된 개인정보는 명의도용·인터넷 사기·불법스팸 등 온라인상에서의 문제뿐만 아니라 보이스 피싱 및 대포폰(통장) 불법개설 등 오프라인 범죄로 악용될 가능성이 높아 심각한 사회적문제로 대두되고 있는 상황이다. 물론 이러한 사항들에 대한 심각성을 인식해 개인정보 보호를 위한 법·제도 개선 및 i-Pin 등 주민번호 대체수단을 도입하고 있지만 이미 유출된 개인정보에 대한 회수·변경이 불가능해 여전히 개인정보 악용의 여지가 남아있는 실정이다. 이에 본 논문에서는 기술적 방법론에 대한 부분은 연구과제로 남겨두고 인터넷을 통해 유출된 개인정보를 악용한 피해가 발생되지 않도록 하기 위해 인터넷 사이트에 회원 가입시 주민번호를 사용하지 않는 개인 인증체계 개선 방안에 대한 정책 모델을 제

안하고, 향후에는 세부 기술에 대한 연구를 진행하고자 한다.

2. 기반 연구

2.1 국내외 인터넷 개인 인증 현황 및 법·제도적 시사점

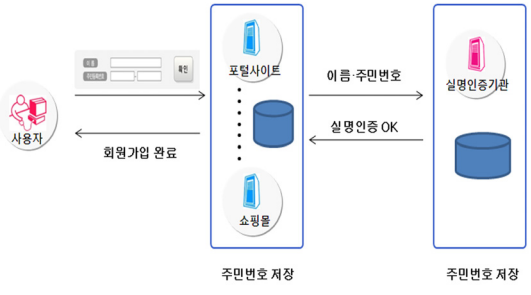
2.1.1 해외 인터넷 개인인증 현황

해외 주요국도 우리나라 주민번호와 유사한 개인 식별번호를 사용하고 있다. 미국은 사회보장번호(social security number), 일본은 주민표 코드번호, 영국은 ID카드, 캐나다는 사회보험번호 등이 그 예이다. 이러한 개인식별 번호는 공공분야에서 의료, 사회복지, 조세 등 행정 서비스에서 활용되는 것이 대부분이며, 민간분야에서는 활용을 엄격히 제한하고 금융, 부동산, 통신 등에서 일부 활용하고 있을 뿐이다. 그 밖의 서비스 분야의 경우 대부분 성명, 생년월일, 연락처, 이메일 등을 이용해서 개인을 식별하고 있다. 특히 인터넷에서 개인인증의 사례를 살펴보면 미국·중국의 금융 분야에서 일부 사용하는 것을 제외하고 영국·일본·캐나다 등 대부분 국가의 인터넷에서 개인 식별번호를 사용하지 않고 있는 상황이다[3]. 여기에서의 시사점은 우리나라의 주민번호와 유사한 개인식별번호는 공공분야에서만 관리되며 사용되어지고 있다는 점이다.

2.1.2 국내 인터넷 개인인증 현황

(1) 주민등록번호를 이용한 인증체계

국내의 경우 주민등록번호는 온·오프라인을 막론하고 개인을 구별하기위한 고유 식별자로 사용되고 있으며 각종 정보시스템에서 개인을 식별하기 위한 Key 값으로 활용되고 있다. 특히 최근에는 포털 등 사이트에 가입시 신용평가회사 등에서 제공하는 실명인증 방식을 사용하므로 각 사이트에서 주민등록번호를 수집할 필요가 적어 졌음에도 관행적으로 회원 가입시 주민번호 입력을 요구하고 있는 실정이다. 주민등록번호는 1인당 1개의 번호를 부여받아 평생을 사용하는 번호이다. 따라서 주민등록번호가 유출되었을 경우 회수는 물론 변경·갱신이 어렵고 인터넷을 통해 쉽게 유출될 수 있어 국민 불안감은 물론 심각한 사회적 문제를 야기할 수 있다. (그림 3)은 현재 시행되고 있는 신용정보社의 실명인증을 이용한 회원가입 체계를 보여준다. 여기서 주민번호가 실명인증기관은 물론 각 인터넷 포털·쇼핑몰 등에도 저장되어 있어 개인정보를 수집하려는 해커들의 공격목표가 되고 있는 실정이다.



(그림 3) 주민번호를 통한 인터넷 회원 인증 체계

이러한 문제를 해결하기 위해 오래전부터 i-PIN과 같이 주민번호를 대체할 수 있는 식별번호에 대한 연구가 활발히 진행되어 왔으며, 더 이상 주민번호 오·남용으로 인한 피해를 고스란히 국민들에게 전가해서는 안 된다는 인식이 확산되고 있는 상황이다[5]. 또한 「정보통신망법」 제28조(개인정보의 보호조치)에서는 '수집된 개인정보는 정보통신서비스제공자 및 개인정보보호 의무 준용사업자는 주민등록번호 및 금융정보를 암호화하여 저장'토록 의무화 하였다[6]. 이에 따라 각 사업자는 DB 구축시 막대한 자금이 소요되게 되고, 저장 서버 및 개인정보를 보호하는 측면에서도 상당한 부

담으로 작용하고 있다. 따라서 주민번호 등 개인정보를 집중관리 할 수 있는 체계가 마련된다면 개인정보보호를 위해 투자되는 경제적 비용과 노력을 줄일 수 있으며, 국가차원의 개인정보보호의 기반이 마련되어질 것으로 기대된다.

(2) i-PIN을 통한 인증

최근 대규모의 개인정보 침해사고가 다수 발생되어 주민등록번호를 통한 계정 도용 등 심각한 피해가 우려됨에 따라 방송통신위원회가 주축이 되어 아이핀(i-PIN:Internet Personal Identification Number)을 개발·보급하고 있다. 그러나, 기능 제약 및 이용상의 불편 등으로 인해 2005년 10월 서비스 개시이후 현재까지의 보급이 저조한 실정이다. 이에 대한 해결책으로 2009년 7월부터 i-PIN 2.0체계를 마련하여 시행 하였으며[7], 이전 버전에서 가장 문제가 되었던 'i-PIN 통합 ID 관리'구현을 통해 본인확인기관 선택을 생략하고, 인터넷 사업자는 i-PIN을 이용해 온라인 제휴서비스 및 온·오프라인 연계서비스를 편리하게 제공할 수 있도록 연계정보(Connecting Information)를 추가하는 등 편의성 및 기능을 개선하였다[8]. 그러나 본래 취지였던 인터넷 상의 주민등록번호 대체를 완벽히 소화해 내지 못하고 있는 것이 사실인데, 그 이유는 「전자상거래 등에서의 소비자보호에 관한 법률」 제6조(거래기록의 보존 등) 2항에 사업자가 보존하여야할 거래의 기록 및 그와 관련된 개인정보(성명·주소·주민등록번호 등)를 규정하고 있기 때문에 전자상거래에서는 반드시 주민번호를 이용한 거래가 이뤄져야만 하고[7], 또한 인터넷 뱅킹 등 전자 금융 거래시 공인인증서를 이용한 인증수단을 사용해야하기 때문이다. 이러한 이유로 인해 i-PIN을 발급받아 사용하더라도 주민번호와 공인인증서를 사용할 수밖에 없는 것이다. 이러한 점은 오히려 사용자가 관리해야 될 개인인증 수단의 개수를 증가시키게 되어 사용자가 느끼는 복잡함과 불편함이 더 가중되고 있는 상황이다. 또한 인터넷 사업자들이 i-PIN 도입에 적극적이지 않는 가장 큰 이유는 비용 문제이다. 기존의 개인인증 방식에서 i-PIN으로 전환할 경우, 업체의 회원규모에 따라 수백만 원에서 수십억 원까지 들어간다고 한다. 인터넷 사업자들은 처음부터 큰 부담을 안게 되고, 가입자를 확인해야하는 인터넷 사업자들은 아이핀 도입 후에도 본인확인 인증을 받기 위해 신용정보업체에 건당 수수료를 지불해야 하는 경제적 문제도 존재한다. 물론, 「정보통신망법」에 의거 일정 수준의 회원을 보유하고 있는 사업자는 주민번호와 병행하여 의무적으로 적용해야하는 상황이다. 또한 i-PIN을 발급해주는 본인확인 기관에서도 개인의 신용정보 및 주민번호 등을 보유하고 있어 국민들의 불안감은 여전히 존재한다. 만일, 본인확인 기관에 취약점이 존재한다면 또 다시 대형 개인정보 유출사고가 발생될 수 있기 때문이다. 이러한 차원에서 본 논문에서는 본인확인 기관을 국가공공기관에서 집중관리 할 수 있는 체계를 제안한다. <표 1>은 i-PIN을 발급해주는 기관이다.

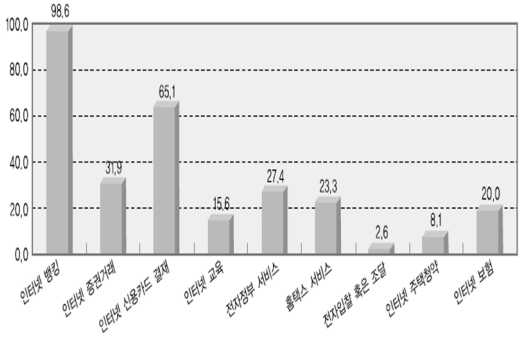
〈표 1〉 I-PIN 발급기관

I-Pin 발급기관	SIREN24	NICE i-PIN	가상주민번호 아이핀	한국정보인증	공공 i-PIN
본인확인 기관	서울신용평가정보	한국신용정보	한국신용평가정보	한국정보인증	공공아이핀센터
홈페이지	siren24.com	nuguya.com	vno.co.kr	sgipin.com	gpin.go.kr
연락처	846-5000	1588-2486	1600-1522	1577-8787	3279-3476

(3) 공인인증서를 통한 인증

공인인증서는 인터넷상의 본인확인 수단으로 5

개 공인인증기관을 통해 동일인에게 여러 개를 발급할 수 있는 체계로 전자정부 민원발급서비스, 인터넷 뱅킹, 전자상거래 분야에서 널리 사용되는 인증체계이며, i-PIN 발급시에도 본인확인을 위해 사용되고 있을 정도로 많이 활용되고 있다. (그림 4)는 공인인증서가 활용되고 있는 분야를 100% 기준으로 분류한 그래프이다[9].



(그림 4) 공인인증서 활용 분야

공인인증서는 이용범위에 제한이 없는 '범용 공인인증서'와 이용 범위에 제한이 있는 '용도제한용 공인인증서'로 구분되며 현재 공인인증서는 2009년 5월 현재 2,063만 명이 사용하고 있을 정도로 보급률 측면에서 많은 사용자를 보유하고 있는 인증 체계이다. 하지만 현재 공인인증서에는 가입자의 나이 및 성별을 구분할 수 있는 정보가 포함되어 있지 않아 성인인증·성별 확인 등의 부가 인증서비스 제공이 어려우며, 개인별 다수의 공인인증서 소유가 가능함에 따라 중복 가입 방지 등을 위한 개인 식별자로 이용 또한 어려운 것이 사실이다. 공인인증서에 성인인증·성별 확인 등이 가능한 고유키를 삽입하는 방안을 검토하기만 한다면 통합적인 개인인증체계를 제공할 수 있는 대안이 되기에 충분한 조건을 갖추고 있다고 할 수 있다. 이러한 사항에 대한 기술적인 논의는 본 논문에서 다루지는 않는다. <표 2>는 공인인증서 발급 기관 리스트 이다.

〈표 2〉 공인인증서 발급 기관

인증기관	등록기관	홈페이지 주소
(주)코스콤	대행기관	http://www.signkorea.com
한국전자인증	대행기관	http://www.crosscert.com
	국민은행	http://www.kbstar.com
	하나은행	http://www.hanabank.com
	산업은행	http://www.kdb.co.kr
한국정보인증	대행기관	http://www.signgate.com
	우체국	http://www.epostbank.go.kr
	SC제일은행	http://www.scfirstbank.com
	기업은행	http://www.mybank.co.kr
	우리은행	http://www.wooribank.com
	외환은행	http://www.keb.co.kr
한국무역정보통신	한국무역정보통신	http://www.tradesign.net
한국전산원	한국전산원	http://sign.nca.or.kr

2.1.3 법 · 제도적 시사점

우리나라는 IT강국으로서 포탈·쇼핑몰 등 부가서비스 사업이 다른 나라에 비해 활성화 되어 있다고 할 수 있다. 그러나 각 사업자들은 마케팅 및 새로운 비즈니스 모델을 개발하기 위해 개인정보 수집에 열중하고 있는 상황 이다. 「정보통신망법」 제28조(개인정보의 보호조치)에 의거 "수집된 개인정보는 정보통신서비스제공자 및 개인정보보호 의무준용사업자는 주민등록번호 및 금융정보를 암호화하여 저장"토록 의무화 하고 있으나 영세사업자의 경우 제대로 된 보안관리가 이루어지지 않고 있으며, 데이터베이스에서 마스터키가 되는 주민등록번호를 암호화하기 위한 기술적 제반사항도 성능 및 추가 발생 비용 등의 이유로 제대로 된 관리가 이루어지지 않고 있는 것이 현실이다. 또한 「전자상거래 등에서의 소비자보호에 관한 법률」

제6조(거래기록의 보존 등) 2항에 의거 “사업자가 보존하여야할 거래의 기록 및 그와 관련된 개인정보(성명, 주소, 주민등록번호 등)를 규정하고 있어 인터넷 사업자는 전자상거래를 위해 회원 가입시 주민번호를 요구하고 있다. 이렇듯 인터넷 각 사이트별 사용자의 개인정보 수집이 일상화 되어 있으며, 회원 가입시 개인정보 활용에 동의해야만 하고, 동의하지 않으면 가입조차 할 수 없는 문제를 가지고 있다. 이에 법·제도적 보완이 필요하다고 할 수 있다.

3. 인증체계 개선을 통한 주민등록번호 관리 모델

3.1 인터넷상 인증체계 방식 비교

특히 문제가 되는 것은 익명성이 보장되는 인터넷에서 이다. 한번 유출된 주민등록번호는 회수·변경·갱신이 어렵다. 이러한 이유로 명의를 도용하게 되면, 회원가입은 물론 소액결제 등 금전적 피해를 발생할 수 있게 된다. 이러한 문제를 해결하기 위한 방안으로 인터넷에서 주민번호 사용을 금지토록 하면 주민번호가 유출되었다 하더라도 인터넷에서는 사용할 수 없게 된다. 물론 오프라인에서는 본인의 신분증을 확인하는 절차가 있기 때문에 도용될 가능성은 더욱 줄어들게 될 것이다. 유출된 주민번호를 도용하지 못하도록 하는 방안에는 I-PIN과 유사한 방식의 번호를 가지고 대체하는 방식을 생각해 볼 수 있다. <표 3>은 인증체계로서 대체수단이 갖추어야 될 조건을 파악한 것으로 현재 사용 중인 인증체계인 공인인증서와 i-PIN의 장단점을 비교 분석한 것이다. 먼저 주민번호 대체 수단은 유일하게 개인을 식별할 수 있어야 하며, 중복가입 여부를 확인할 수 있어야 하며, 연령·성별 등이 확인 가능해야 된다. 또한 기존 주민번호와 호환성을 제공해야하며 유출되었을 경우 도용이 불가능하도록 새로운 것으로 재발급 받을 수 있어야 한다. 또한 주민번호와 같이 13자리 숫자로 되어 있어서는 안 된다. 이는 직관적으로 생년월일·성별 등을 알아 낼 수 있기 때문이다. 따라서 주민번호 대체 수단은 복잡성을 가져야만 한다. 마지막으로 이용자들에게 쉽게 보급할 수 있어야 하며, 국민들로 하여금 안전성에 대한 신뢰도를 인정받아야 한다는 것이다[4].

〈표 3〉 인증체계로서 공인인증서와 i-PIN과의 비교

주민번호 대체 요건	공인 인증서	i-PIN
대국민 신뢰성	▲	▽
본인확인정보(유일성)	▲	▲
연령, 성별확인	▽	▲
호환성	▲	▽
도용 방지	▲	▲
복잡성	▲	▲
중복가입 확인	▽	▲
범용성	▲	▽

이러한 요건들을 만족하는 개인 인증체계로서 연령·성별확인 및 중복가입 확인이 가능토록 기능을 개선한 ‘공인인증서’ 방식을 사용하는 것이 <표 3>, <표 4>의 내용 등으로 볼 때 적절하다고

〈표 4〉 대체수단의 비교

구 분	공인인증서	i-PIN	주민번호
안전성	높음	중간	낮음
편의성	낮음	중간	높음
배상 책임	전자서명법에 의해 공인인증기관에게 배상책임 규정	손해배상에 대해 과실책임주의(민법 제750조)원칙에 따라 해결	손해배상에 대해 과실책임주의(민법 제750조)원칙에 따라 해결

판단된다[11]. 이러한 개선된 공인인증서는 최초 사용자가 회원가입시 ID/PW를 생성하기 위한 인증체계로서 사용되는 것이다. 결국, 최초 회원가입 이후에는 ID/PW만을 가지고 현행대로 해당 사이트에 로그인 하면 된다.

3.2 주민등록번호 대체수단인 '전자주민번호' 생성 요건

<표 5>에서 보듯이 유출된 주민등록번호를 대체 할 수 있는 방안을 논하기 전에 주민등록번호를 대체하기 위한 수단인 전자주민번호의 요건에는 어떤 것이 있는지 파악해야 될 필요가 있다. 물론 이러한 사항들이 반영된 전자주민번호의 한 형태가 i-PIN이라 할 수 있다. 그러나 전자주민번호의 생성에 관한 기술적 부분은 논하지 않는다. 중요한 것은 <표 5>에서 볼 수 있듯이 어떤 종류의 형태이든 주민등록번호를 대체할 수 있는 수단이기만 하면 된다는 것이다. 그런데 여기서 해외사례에서 볼 수 있듯이 전자주민번호에 연령 및 성별확인 정보가 반드시 제공되어야 하는지에 대한 의문이 있을 수 있다. 하지만 우리나라의 경우 「청소년보호법」 제17조(판매금지 등)에 의거 청소년 유해매체물을 판매·대여·배포하거나 시청·관람·이용에 제공하고자 하는 자는 그 상대방의 연령을 확인하여야 하고, 청소년에게 이를 판매·대여·배포하거나 시청·관람·이용에 제공하여서는 아니 된다고 규정하고 있어 연령 및 성별확인 내용이 필요하다 할 수 있다.

〈표 5〉 전자주민번호의 요건

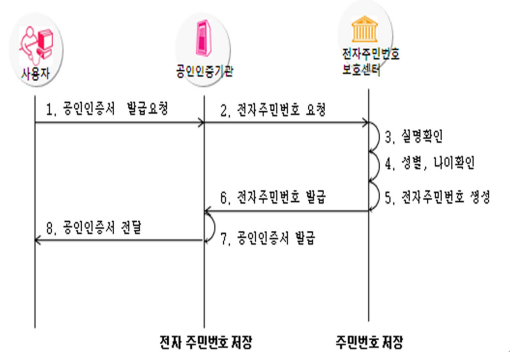
주민번호 대체 요건	내 용
대국민 신뢰성	국민들이 믿고 신뢰할 수 있어야 함
본인확인정보 (유일성)	개인 식별을 위한 유일한 개인식별코드
중복가입 확인	인터넷 사이트에 중복가입 여부확인
연령, 성별확인	성인인증 및 정보제공 지정을 위한 정보
호환성	인터넷 모든 서비스와의 연계 가능
도용 방지	유출되더라도 도용할 수 없어야함
복잡성	대체수단을 직관적으로 알 수 없어야함
범용성	다양한 분야에 적용할 수 있어야함

이렇게 전자주민번호를 발급하기 위해서는 실제 주민등록번호를 총괄 관리하는 기관이 필요한데 공공성이 있어야 하며, 우리 국민의 주민등록번호를 안전하게 관리할 수 있는 기관이면 된다. 여기서 공공성을 강조하는 이유는 주민등록번호를 보호하는 곳의 신뢰도를 높이기 위해서 이다. 이와 관련 본 논문에서는 '전자주민번호 보호센터' 설립을 제안한다.

3.3 '전자주민번호 보호센터'를 통한 인증체계 개선 방안

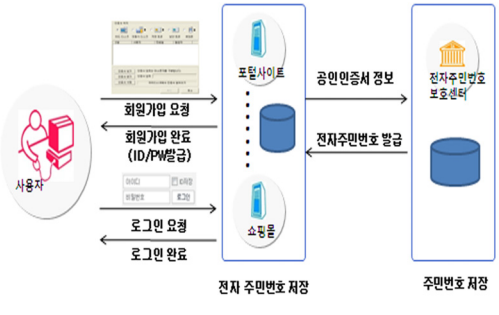
'전자주민번호 보호센터'는 우리나라 모든 국민의 주민등록번호에 대한 정보를 공유하고 있으며, 민간기관이 아닌 공공분야의 기관이어야만이 신뢰성을 향상 시킬 수 있다. '전자주민번호 보호센터'는 기존 주민번호를 통해 '전자주민번호'를 생성·발급·갱신·삭제하는 기능을 하며, 전자주민번호는 일반사용자가 기억해두지 않아도 된다. 단지 인터넷 사업자와 상호 정보교환을 통해 가입회원의 전자주민번호가 어떤 것인지 인증을 해주기만 하면 된다. 이렇게 될 경우 기존 수많은 사이트에서 회원 가입시 수집했던 개인정보는 모두 삭제될 수 있으며 대신 '전자주민번호 보호센터'에서 제공하는 전자주민번호를 저장토록 한다. 사용자는 최초 오프라인 인증을 통해 공인인증서 발급 권한을 획득하고, (그림 5)에서 보면 알 수 있듯이 온라인상에서 공인인증 기관을 통해 공인인증서를 발급 받게 된다. 이에 따라 실제 주민등록번호는

전자주민번호 보호센터에만 저장되어 있고, 공인인증기관 및 포탈 등 서비스 사업자는 주민번호 대체키인 전자주민번호만을 저장하는 방식이다. 만일 전자주민번호가 유출됐거나 공인인증서가 외부에 유출 되었을 경우 공인인증서 재발급만으로 신규 전자주민번호를 발급 받을 수 있게 된다.



(그림 5) '개선된 공인인증서' 발급 방안

이 전자주민번호의 생성·배포 등 기술적인 부분에 대해서는 본 논문에서 논의하지 않고 새로운 연구과제로 남겨두기로 한다. 물론 이 전자주민번호의 기술적인 부분들은 i-PIN이 가지고 있는 특성을 고려해서 연구를 진행해도 무방할 것이다. 다만 여기서 논하는 방향은 i-PIN 번호(주민번호 대체 수단) 자체를 얘기하는 것이지 i-PIN 운영에 관한 부분과는 많은 차이가 있다. 가장 큰 차이점이라고 한다면, i-PIN의 경우 일반 사용자가 관리하게 되지만, 본 논문에서 제시한 '전자주민번호'는 공인인증기관 및 포털사이트·쇼핑몰 등 사업자가 관리하게 된다는 것이다. 결국 '전자주민번호 보호센터'는 우리나라 국민들의 주민등록번호 정보를 공유하며, 전자주민번호를 필요로 하는 인터넷 사이트 등에 전자주민번호를 생성·저장·배포·삭제하는 역할을 수행하게 된다. 이렇게 되면 주민번호가 유출될 수 있는 취약 포인트가 현재는 수십만 곳에 달하지만 전자주민번호 보호센터를 통해 중앙 집중적인 보안관리가 이루어 질 수 있고 유출된 주민등록번호에 대해서 전자주민번호를 포함한 공인인증서를 사용함으로서, 인터넷에서 더 이상 주민등록번호를 사용한 회원가입은 사라질 것으로 전망된다. 한편 각 인터넷 사이트에서도 주민등록번호에 대한 개별적인 저장 및 집중 보안관리가 사라져 그린IT 정책에도 상당한 효과를 발휘할 수 있게 된다. '전자주민번호 보호센터'는 각 사이트가 보유하고 있는 개인정보를 기반으로 회원 가입시 개인 인증하는 방식에서 중앙 집중화 방식으로의 획기적인 방안을 마련하게 되는데, 우선 개인 사용자는 '개선된 공인인증' 방식을 통해 회원 가입하도록 한다. 사용자는 인터넷 사이트에 회원가입시 공인인증서를 통해 생성한 ID/PW를 발급받게 되고 공인 인증서 내에 정보와 전자주민번호 보호센터의 전자주민번호와 일치 여부를 확인한 후 각 사이트별 인증을 하게 된다. 이때 포털사이트·쇼핑몰 등에는 전자주민번호가 저장된다. 한편, 사이트에 저장된 개인정보는 이름, 전자주민번호, 주소, 이메일, 전화번호 등이 되며 포털사이트나 쇼핑몰 등 마케팅에 사용될 최소한의 정보만을 수집하는 것을 원칙으로 하게 된다. 만일 공인인증서가 유출될 경우에도 새로운 전자 주민번호를 발급받게 됨으로 문제없이 해결할 수 있게 된다. 또한 각 사이트에 저장된 전자주민번호는



(그림 6) 논문이 제안한 개선된 인증 체계

전자주민번호 보호센터와의 연동으로 지속 업데이트 될 수 있다. (그림 6)은 본 논문에서 제안하고 있는 주민번호를 사용하지 않고 인터넷에서 공인인증서와 전자주민번호 보호센터를 통한 개인 인증 체계를 도식화한 것이다. 결국 사용자는 회원가입시 공인인증서를 가지고 ID/PW를 발급 받아 인터넷을 사용할 수 있게 되어 현재와 같이 사용자는 공인인증서와 ID/PW만을 관리하면 된다.

3.4 개인정보보호를 위한 법 체계 개선

앞서 설명한 바와 같이 주민등록번호 수집・이용 제한을 위한 법제 정비가 이루어져야 하는데 현재 공공기관의 개인정보보호를 강화하기위해 2010년 3월 「공공기관의 개인정보보호에 관한 법률」을 개정하는 등 지속적인 정비를 하고 있다. 그러나 개인정보보호에 관한 일반법의 부재로 법적용의 사각지대가 발생되게 되고, 이러한 사각지대를 제거할 목적으로 행정안전부는 「개인정보보호법」 제정을 추진하여 2008년 11월 28일 국회에 제출한 상태이며, 현재 국회 법제사법위원회에 계류되어 있으며 곧 통과될 전망이다. 또한 「전자상거래 등에서의 소비자보호에 관한 법률」에 명시된 '사업자가 보존하여야할 거래의 기록 및 그와 관련된 개인정보'에서 주민번호 대신 전자주민번호와 최소한의 개인정보만 기록하도록 하는 법안 개정이 필요하다. 이러한 법체계를 기반으로 주민번호 저장은 허가된 기관을 제외하고 모두 삭제토록 하고 각 포털・쇼핑몰 등 각 사이트는 전자주민번호를 포함한 최소한의 개인정보만을 수집할 수 있도록 해야 한다. 한편, 미국과 영국, 캐나다, 호주 등 해외 주요국의 경우도 민간사업자가 개인정보를 수집 하는 것 자체를 엄격히 제한하고 있으면서도 개인정보 유・노출 등과 같은 침해사실이 발생할 경우, 이러한 사실을 즉각 통지하도록 법에서 의무화하거나 지침 등으로 적극 권장하고 있다. 특히, 해당 정보주체에게 심각한 피해가 갈 것이라 판단되는 침해 사건에 대해서는 거의 의무적이라 할 수 있다. 그만큼 개인정보 유・노출 사건이 발생하였을 경우 정보주체에게 발생할 수 있는 피해를 미연에 방지하는 절차는 매우 중요한 것일 것이기 때문이다. 우리나라도 현재 제정 추진 중인 「개인정보보호법」에 포함되어 있는 것처럼 인터넷 서비스 제공자가 최소한의 개인정보만을 보유하고 있다고 하더라도 개인정보 침해하고가 발생되면 이러한 사실을 사용자들에게 통지하여 피해를 최소화 하는 노력이 필요하다[12]. 그러나 기업의 입장에서는 이러한 유・노출 사건이 발생하였을 경우, 자발적으로 공개하기가 쉽지 않은데 이러한 사건이 알려질 경우, 기업 이미지에 큰 타격을 줄 수 있기 때문이다. 따라서 강제적인 규정에 의해 공개하도록 하되, 무조건 비판의 대상으로 생각하기보다는 실제 피해의 정도와 가능성 등에 대한 보다 철저한 조사와 판단에 기반하여 필요한 절차를 이행할 수 있도록 하는 체계적인 시스템 마련이 필요할 것이다[12]. 본 논문에서 제안하는 공인인증서 사용과 전자주민번호보호센터를 통한 개인인증체계를 인터넷 사업자 입장에서 또는 마케팅의 관점에서 반대할 수 도 있으나 기업에서 개인정보가 유출되었을 경우 사용자 집단소송으로 이어지는 사회 분위기가 점차 확산되고 있는 상황이고, 기업 Risk관리 차원에서도 바람직하다고 할 수 있으며, 각 인터넷 사업자의 개인정보 저장 및 보호를 위한 노력이 줄어들게 됨으로 인한 그린IT 정책 실현에도 현실적인 대안이 될 수 있다.

4. 논문제안 방식 분석

본 논문에서 제안한 방식은 많은 장점을 얻을 수 있다. <표 6>은 인터넷을 통해 유출된 주민번호를 재사용할 수 없도록 하기 위한 논문 제안내

용을 각 단계별로 분석한 내용이다.

〈표 6〉 인터넷 회원가입 절차별 논문제안 방식 분석

분석 항목	내 용
공인인증서 회원가입	- 개인 인증체계로서 공인인증서 旣 검증 및 활용분야 많음 - 회원가입시 공인인증서를 통한 전자주민번호 발급(대체효과) - 사용자가 알기 쉬운 ID/PW 방식으로 유출시 재발급 가능
주민등록번호 중앙집중관리 (전자주민번호보호센터)	- 주민등록번호를 인터넷에서 사용하지 않고, '전자주민번호 보호센터'를 통한 전자주민번호 발급·갱신·폐기 가능 - 중앙 집중형 관리로 보안강화
전자주민번호 사용	- 사용자는 전자주민번호를 관리할 필요가 없음(인터넷 사업자 관리) - 전자주민번호의 사용으로 유출된 주민번호 인터넷 재사용 방지 - 인터넷 사업자의 개인정보보호에 대한 부담 감소
그린IT 실현	- 인터넷 사업자의 개인정보보호 투자 절감으로 그린IT 실현에 기여

5. 결 론

본 논문에서 제안한 인터넷을 통해 유출된 개인정보 특히, 주민등록번호를 인터넷에서 더 이상 사용하지 않게 하는 개인 인증체계 개선 방안의 목적은 각 사이트별로 제 각각 수집·관리되어 오던 주민등록번호를 전면 삭제토록하고, 중앙 집중화 되어있는 체계로의 전환을 의미한다. 이렇게 추진될 경우 각 사이트에는 주민등록번호가 아닌 전자주민번호가 저장되게 되고, 이 전자주민번호가 유출될 경우에도 공인인증서를 통해 재발급이 이루어지게 되어 사용자는 공인인증서 재발급을 통해서 쉽게 전자주민번호의 변경·재발급이 가능하게 된다. 또한 사용자는 직접적으로 전자주민번호에 재발급에는 관여하지 않아도 된다. 한편 '전자주민번호 보호센터'는 국민들의 신뢰성을 향상시킬 수 있으며, 각 인터넷 사업자 또한 개인정보보호를 위해 과도한 재정낭비 및 개인정보 유출시 따르는 집단소송 등 위험관리가 필요 없게 된다. 결국 개인정보보호를 위한 저장 공간, 보호 매커니즘 적용 등을 최소화 할 수 있게 되어 그린 IT실현에도 기여할 것이다. 본 논문이 제안하고 있는 정책 모델을 실현하기 위해서는 '전자주민번호 보호센터' 임무 기능에 관한 정책적 연구 및 공인인증서 개선, 전자주민번호 생성·발급에 관한 기술적 세부 사항도 향후 연구가 진행되어야 한다.

참 고 문 헌

[1] ETRI 정보보호연구단 디지털ID 보안연구팀, "웹2.0 환경에서 '전자ID 지갑'을 통한 개인정보보호와 IT서비스 활성화", 국가사이버안전센터, Monthly 사이버 시큐리티, pp. 2-12, 2007.

[2] "2008년 인터넷 이용실태조사", 방송통신위원회, 한국인터넷진흥원, p. 11, 2008.

[3] "해외 주요 국가의 개인정보보호 관련 법제도 연구", 한국정보보호진흥원, 방송통신위원회 정보보호 강화사업 일환, pp. 15-130, 2008.

[4] 정찬주, 김윤정, 김진원, 박광진, "주민번호 대체수단(i-PIN) 개발을 위한 기술표준과 서비스 프레임워크", 정보보호학회지 제18권, 제6호, pp. 20-27, 2008.

[5] 2005 국가정보보호백서, 국가정보원, 방송통신위원회, pp. 68-71, 2005.

[6] 정보통신망 이용촉진 및 정보보호등에 관한 법률.

[7] 이기정, "인터넷상 주민번호 대체수단(아이핀 : i-PIN) 본격 도입", 국가사이버안전센터, Monthly

사이버 시큐리티, pp. 2-14, 2006.
[8] “i-PIN2.0 도입 매뉴얼”, 방송통신위원회, 한국정보보호진흥원, pp. 6-10, 2009.
[9] 전자상거래 등에서의 소비자보호에 관한 법률
[10] 이해춘, 민경식, 이상준, “공인인증서 이용의 경제적 효과에 관한 연구”, 한국정보화진흥원, 정보화정책 제15권, 제2호, pp. 77-90, 2008.
[11] 염홍렬, 이석계, “인터넷상에서 주민등록번호 대체수단 발전방향”, 전자공학회지 제32권 제11호, pp. 1831-1393, 2005.
[12] 변순정, 이강신, 박광진, “개인정보 유·노출 등의 통지 관련 국내외 법제 현황”, 한국정보보호학회지 제18권, 제6호, pp. 35-42, 2008.

이 정 현

現 고려대학교
정보경영공학전문대학원
박사 수료
관심분야 : 정보보호법·제도 및 정책, 개인정보보호, 정보보호기술, 디지털 포렌식

권 헌 영

前 정보통신정책연구원
주임연구원
한국정보화진흥원 책임연구원
대통령자문 전자정부특별위원회
연구위원
現 행정안전부 개인정보수준
진단 위원회 위원
국방부 CIO자문위원
서울시 강남구 정보화추진위원
광운대학교 법과대학 교수

임 종 인

1986년 고려대학교 대학원
수학과 박사(암호학)
現 고려대학교
정보경영공학전문대학원
원장
(정보보호연구원 원장 겸임)
대검찰청
디지털수사자문위원회
위원장
금융보안연구원 보안전문기술
위원회 위원장
행정안전부 정책자문위원회 위원
한국저작권위원회 위원 등