

국가 개인식별번호체계 개선에 관한 연구 : 독립적 난수기반 개인식별번호체계로 전환*

한 문 정,[†] 장 규 현, 홍 석 희, 임 중 인[‡]
고려대학교

A Study on Reforming the National Personal Identification Number System : The Unconnected Random Personal Identification Number System*

Mun-jung Han,[†] GyeHyun Jang, Seokhie Hong, Jong-in Lim[‡]
Korea University

요 약

주민등록번호 제도가 도입된 이래 주민등록번호는 효과적인 국가 개인식별체계의 역할을 해왔다. 하지만 정보화 사회의 도래로 주민등록번호를 포함한 개인정보가 대규모로 수집됨에 따라 개인정보 유출사고 등의 문제가 발생하고 있다. 주민등록번호는 모든 영역에서 개인과 일대일로 대응되는 강력한 개인식별값이자 본인확인 수단으로 유출될 경우 큰 피해로 이어질 위험이 있으나, 주민등록번호는 변경할 수 없다는 문제가 있어 이러한 피해를 경감할 수 있는 대책이 없는 실정이다.

우리나라의 경우 개인정보가 주민등록번호를 중심으로 하여 기록 및 관리되는 것이 일반이므로, 유출된 주민등록번호와 개인정보의 연결성을 끊음으로써 국민의 개인정보를 보호할 필요가 제기되고 있다. 본 연구에서는 주민등록번호의 종속성을 제거함으로써 주민등록번호 및 개인정보 유출에 대한 피해를 방지할 수 있는 독립적인 난수기반 개인식별번호 체계를 제안하고, 체계의 도입 시 발생할 수 있는 쟁점사항을 식별하고 해소방안을 제시한다.

ABSTRACT

The Resident Registration Number(RRN) system has been effectively acted as a national identification system since it was enforced. On the other hand, there are some problems such as leakages of personal informations including RRNs on a large scale and each RRN makes a pair with each person in all areas of the society. Nevertheless leakages of them might cause a big damage, there is no radical countermeasure for they are never changed in actual fact.

In Republic of Korea, a RRN acts as a primary key of a database, so it has to be protected by severing the connectivity between leaked RRNs and the other personal data. In this paper, the Unconnected Random Personal Identification Number system is proposed for preventing damage of data spills by removing a dependency which the RRN has. Furthermore, this paper suggests the solutions against some potential issues in the system.

Keywords: Personal Identification Number, Resident Registration Number

접수일(2014년 6월 16일), 수정일(2014년 8월 8일), 게재
확정일(2014년 8월 11일)

* 본 연구는 "BK21플러스 사업" 지원으로 수행하였습니다.

[†] 주저자, hanmj@korea.ac.kr

[‡] 교신저자, jilim@korea.ac.kr(Corresponding author)

I. 서론

개인정보의 잇따른 유출사고로 인해 사회적으로 막대한 피해와 우려가 발생하고 있다. 정보화 사회에서 신뢰는 핵심적인 요소로, 개인정보 유출은 이러한 신뢰의 근간을 뒤흔들 우려가 있다. 최근 KB국민·롯데·NH농협 등 카드 3사에서 고객의 개인정보 1억 400만 건이 유출되었고, KT에서는 1200만 건의 고객 정보가 유출되는 사고가 발생하였다[1]. 두 정보유출 사고를 통해 주민등록번호를 포함한 신용카드 정보, 통신회사 가입정보 등 다양한 정보들이 유출되었다. 유출된 정보들은 그 자체로서 피해를 불러올 수 있으며, 타 기업이나 타 기관에서 유출된 정보들이 머징(merging)이 될 경우 특정 개인의 신원 전반이 파악되므로 신원 도용 등 막대한 심리적·재산적 피해가 발생할 수 있다. 한편, 주민등록제도가 시행된 이래, 유출된 주민등록번호는 총 3억 7,400만 건에 달한다[2].

주민등록번호가 개인정보 데이터베이스의 기본키(primary key) 역할을 함에도 불구하고, 현 주민등록법 시행령 8조1)에 따르면 유출된 주민등록번호를 변경할 수 있는 법적 근거는 찾아볼 수 없다. 결국 주민등록번호는 주민등록과 동시에 의무적으로 부여되는 강제성과 한 번 부여되면 실질적으로 변경할 수 없는 종신성의 한계를 갖는다[3][4]. 또한 주민등록번호에는 생년월일, 성별, 출생지역 등의 정보가 표기되어 그 자체로 개인정보가 노출된다는 문제 역시 제기되고 있다.

주민등록번호의 잇따른 유출사고와 본질적인 한계에 따라 제도 개선에 대한 사회적 요구가 발생하고 있으며, 여러 대체 방안들이 논의되고 있다. 논의되고 있는 대체 수단들의 장·단점을 분석하고, 가장 효과적인 해결안이 될 수 있는 대안에 대한 분석과 도입을 위한 현실적인 방안 마련이 필요한 상황이다.

본 논문에서는 주민등록번호의 한계를 파악하고, 대안으로 논의되고 있는 아이핀(I-PIN) 활용 확대방안, 주민등록 발행번호 체계, 현행 주민등록번호를 폐기한 난수기반 개인식별번호(이하 독립적 난수기반 개인식별번호) 체계의 각 특징과 한계점을 비교한다. 주민등록번호의 근본적인 문제를 해소할 수 있는 가장 효과적인 수단으로 독립적 난수기반 개인식별번호 체

계를 제시하고, 도입 시 예상되는 현실적인 쟁점사항과 이를 해소하기 위한 기술적·정책적·법적 해결방안을 강구한다.

본 논문에서는 선행 논문을 기반으로 주민등록번호의 한계와 대체 수단을 조사하였으며, 독립적 난수기반 개인식별번호 체계의 전체적인 구조와 더불어 발급 절차, 비대면상 본인 인증 절차를 흐름 순으로 제시하여 각 절차에서 고려할 수 있는 예상 문제를 파악하고 해소 가능한 방안을 도출하였다.

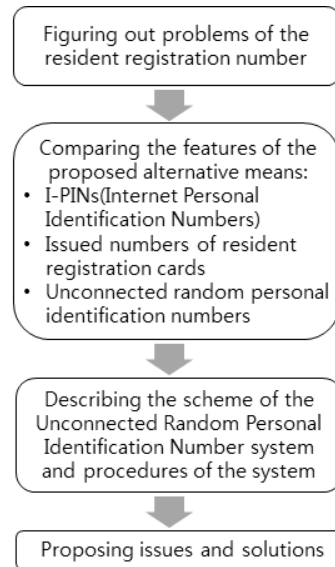


Fig.1. The flow chart of this paper

II. 현행 제도의 문제점과 대안

2.1. 주민등록번호의 한계

현행 주민등록제도에 따라 13자리로 구성된 주민등록번호는 각 자리마다 개인에 대한 정보를 표시한다. 이는 생년월일, 성별, 출생지역(주민등록지) 등에 대한 정보로, 공공기관이나 민간기업 등 신원 인증이 필요한 곳에서 개인을 식별하기 위해 사용된다. 주민등록번호를 수집하는 기관은 일반적으로 주민등록번호를 키 값으로 사용하여 개인의 정보를 처리하므로, 주민등록번호를 연결점으로 하여 여러 기관에서 유출된 개인 정보가 집적될 경우 특정 개인의 신상을 파악할 수 있다는 위험이 있다.

한편, 이러한 유출에 따른 위협 및 위험에도 불구하고

1) 주민등록번호를 정정할 수 있는 경우는 주민등록사항을 정정함으로써 주민등록번호의 정정이 필요하거나, 주민등록번호에 오류가 있는 경우로 한정하고 있다.

고 주민등록번호를 변경할 수 없다는 한계가 있다. 현행법에서는 주민등록번호의 변경이 아닌 정정만을 명시하고 있기 때문이다. 정정은 주민등록번호가 표시하는 정보와 관련된 주민등록사항이 잘못 기재되었거나, 주민등록번호에 오류가 있을 경우에 한하고, 주민등록번호의 오류와 상관없이 개인의 의지나 필요에 따른 변경에 대해서는 명시하고 있지 않다. 이는 유일한 주민등록번호가 한 개인에게 영구히 종속된다는 것을 의미한다.

이처럼 주민등록번호는 개인과의 일대일로 대응되고 사회 모든 영역에서 활용 가능한 인증수단이며 강제 부여되고 영구히 변경 불가능하게 종속된다는 특성으로 인해, 개인정보 유출에 따른 역기능에 대응하기에 한계가 있다. 이러한 한계는 주민등록번호 제도의 개선이 필요한 이유가 되며, 새로운 대체 수단 도입이 극복해야 할 요소이다. 즉, 주민등록번호의 대체수단은 현행 주민등록번호 제도의 장점인 유일성, 식별가능성을 유지하고 제도의 단점인 불변성, 개인정보 노출여부 등을 보완할 수 있어야 한다.

2.2. 주민등록번호 대체 수단

현재 주민등록번호의 한계를 극복하기 위해 논의되고 있는 대안은 아이핀 활용 확대 방안, 주민등록 발행번호 제도, 독립적 난수기반 본인인증 번호 등이다. 본 절에서는 각 대안의 장·단점 분석하고, 각 대안을 평가한다.

2.2.1 아이핀(I-PIN)의 활용 확대방안

아이핀(Internet Personal Identification Number, I-PIN)은 인터넷에서 주민등록번호 대신 사용하고자 2005년에 도입되었다. 온라인 환경에서 가입과 인증에 아이핀을 사용함으로써 주민등록번호의 수집과 도용 문제를 방지할 수 있다는 것이 큰 특징이다. 아이핀은 온라인상에서 아이핀 인증 모듈을 통한 ID/PW 인증방식으로 구현된다. 아이핀 발급기관은 민간기업인 서울신용평가정보·코리아크레딧뷰로·나이스신용평가정보와 공공기관인 공공아이핀센터로 지정되어 있고, 아이핀을 사용하고자 하는 개인은 아이핀 도입 사이트나 본인확인기관 홈페이지에서 본인을 확인하고 아이핀을 발급받아 사용할 수 있다. 아이핀이 유출되더라도 재발급으로 변경이 가능하며, 폐지하거나 비밀번호를 변경할 수 있는 장점이 있다.

아이핀은 2009년에 2.0 체제로 발전하였으며, 가장 큰 변화는 각 기관 간 연계정보(CI) 값을 추가로 제공하는 것이다. 아이핀 인증 정보가 웹사이트에 전달될 때는 성명·생년월일·성별 등의 개인정보와 함께 중복가입확인정보(DI) 및 연계정보(CI)가 전송된다. 중복가입확인정보는 하나의 웹사이트에서 중복가입여부를 확인하는 값(64 byte)이고, 연계정보는 업자간 제휴서비스 등 연계가 이루어진 웹사이트 간 동일 이용자임을 인증하는 공동 식별자(88 byte)이다.

한편, 악의적 이용자가 주민등록번호를 수집하지 않고도 아이핀 계정의 수집·이용으로 신분위장 등 악의적 행위가 가능하다. 또한, 이미 유출된 주민등록번호를 포함한 개인정보에 대한 문제를 해결할 수 없다는 한계가 있다[5][6].

아이핀의 사용 범위를 오프라인으로까지 확장한 '마이핀(My-PIN)' 제도가 올해 8월 7일부터 시행될 예정이다[7], 사용자는 개인식별정보가 포함되지 않은 13자리의 무작위 번호를 발급받아 사용하게 된다. 또한 마이핀 번호를 외워야 하는 번거로움을 해소하고자 마이핀 번호와 성명 등을 적은 발급증을 신용카드 크기로 제공하거나 마이핀 번호를 수시로 확인할 수 있는 스마트폰 앱 서비스를 제공하는 방안도 제시되고 있다[8].

아이핀과 마이핀은 주민등록번호 수집이 허용되지 않는 온·오프라인 환경에서 주민등록번호를 대체하기 위해 만들어진 본인확인 수단으로서, 유일성과 변경가능성을 제공하며, 기존 주민등록번호는 유지된다.

Table 1. This table shows features of the I-PIN and the My-PIN.

	I-PIN	My-PIN
Uniqueness	O	O
Reissuance	O	O
Personal information	ID of I-PIN may include some personal information.	Not included
Independence against RRNs	RRNs are maintained.	RRNs are maintained.
Social whirl	Social whirl hardly exists for it is optional, but RRNs and My-PINs have to be kept and the form of My-PINs must be distinguished from RRNs' one.	

* RRN: Resident Registration Number

2.2.2 주민등록 발행번호

주민등록 발행번호(이하 발행번호) 체계는 주민등록표 발행 시 일종의 일련번호나 주민등록증 문서번호 등을 추가해 이를 주민등록번호의 대체번호로 사용하는 개념이다(9). 주민등록번호는 행정기관만이 보유하고 제한된 용도로만 사용을 엄격히 제한하며, 민간에서는 주민등록증이나 주민등록번호 대신 발행번호를 이용하는 것이다. 이는 현행 주민등록번호 체계와 발행번호 체계를 병행함으로써 전환에 따른 사회적 혼란을 최소화하며, 발행번호의 변경은 주민등록증 문서를 재발행함으로써 가능하다.

발행번호가 식별번호로 사용되기 위해서는 주민등록번호와 마찬가지로 유일성을 만족해야 한다. 또한 주민등록번호가 가지는 문제를 해결하는 대체 수단인 만큼 개인정보를 포함하지 않는 임의의 값이어야 한다. 아울러, 유일성과 변경 가능성 및 우리나라의 통일 후 인구까지 고려하여 최소 10자리 이상의 임의의 값이 되어야 한다. 주민등록번호처럼 13자리로 설계할 경우 기존 시스템을 변경하는 비용을 줄일 수 있을 것이다. 즉, 주민등록 발행번호 체계는 사회적 혼란과 비용은 최소화 할 수 있으나, 개인은 주민등록번호와 더불어 10자리 이상의 주민등록발행번호 값을 외워야 한다는 심리적 부담감이 있을 수 있다. 또한 기존 주민등록번호를 유지함에 따라 주민등록번호 제도의 근본적인 해소방안이 될 수 없다는 한계가 있다.

Table 2. This table shows features of the issued numbers of resident registration cards.

	Issued Number
Uniqueness	O
Reissuance	O
Personal information	Not included
Independence against RRNs	RRNs are maintained, but the use of RRNs is considerably restricted.
Social whirl	Both RRNs and Issued Numbers have to be kept and the form of Issued Numbers must be distinguished from RRNs' one.

※ RRN: Resident Registration Number

2.2.3 독립적 난수기반 개인식별번호

독립적 난수기반 개인식별번호는 기존의 주민등록번호를 폐기하고 새로운 난수기반의 개인식별값을 부여하는 방안이다. 기존의 주민등록번호 부여 체계에서 난수생성모듈을 도입해 생성한 값을 개인식별값으로 사용하는 것이다. 이는 주민등록번호를 삭제함에 따라 이미 유출된 정보와의 연결을 끊음으로써 현안을 근본적으로 해결할 수 있다. 반면, 개인식별값이자 본인확인수단으로 널리 사용되고 있는 주민등록번호를 완전히 폐기하고 대체한다는 점에서 사회적 혼란과 비용이 예상된다. 하지만 이러한 예상되는 문제점과 쟁점사항 등은 충분한 준비 과정과 과도기를 통한 점진적 추진, 기술적·정책적 조치를 통해 해소할 수 있을 것으로 판단된다.

독립적 난수기반 개인식별번호는 그 값이 난수이므로 개인정보가 노출되지 않으며, 제한된 범위 하에 변경 가능성을 제공하여 유출 시에도 2차적인 피해를 줄일 수 있다. 또한 궁극적으로는 주민등록번호를 완전히 대체한다는 장점이 있다.

한편, 현재 우리나라의 인구와 통일 후의 인구를 포괄하면서 변경 가능성을 고려하여 최소 10자리 이상의 임의의 값이 되어야 하며, 13자리로 설계할 경우 기존 시스템의 변경 비용을 줄일 수 있다.

Table 3. This table shows features of the Unconnected Random Personal Identification Numbers.

	Unconnected Random Personal Identification Number(URPIN)
Uniqueness	O
Reissuance	O
Personal information	Not included
Independence against RRNs	O (RRNs are not maintained.)
Social whirl	RRNs are destroyed after a certain period of time, and the URPINs are used only, which may give people a strain temporarily.

※ RRN: Resident Registration Number

2.2.4 소결

주민등록번호는 번호 자체에 개인정보가 노출되며, 사실상 변경이 불가하다는 한계가 있다. 주민등록번호 제도의 한계를 개선하기 위해 논의되고 있는 아이핀의 활용 확대방안, 주민등록 발행번호 및 독립적 난수 기반 개인식별번호 체계의 특징을 살펴보았다. 주민등록번호 체계 및 대체 수단들의 유일성, 재발급 가능성 (또는 변경가능성), 번호의 개인정보 포함여부, 주민등록번호와의 독립성 및 사회적 혼란정도에 대해 Table 4에서 각 특징을 비교하여 파악할 수 있다.

아이핀의 활용 확대방안과 주민등록 발행번호 체계의 경우 변경가능성을 제공하므로 추후 개인정보 유출 사고 발생 시 어느 정도 경감효과는 있을 수 있다. 한편, 기존 주민등록번호와 병행하면서 이들 또한 13자리 값을 유지한다면, 주민등록번호와의 혼동을 피하기 위해 구별되는 형태의 값이 마련되어야 한다. 또한 기존 유출된 정보에 대한 연계 가능성은 여전히 존재하는 한계점이 있다. 따라서 본 논문에서는 사회적 혼란은 클 수 있으나, 기존 주민등록번호로부터 독립성을 가짐으로써 효과적인 대체 방안이 될 수 있는 독립적 난수기반 개인식별번호의 생성, 발급, 이용 및 재발급 절차를 설명하고 예상되는 쟁점사항과 이를 해소하기 위한 방안을 제시한다.

Table 4. This table shows comparisons between the current resident registration number(RRN) system and the alternative systems.

	RRN	I-PIN	Issue Number	URPIN
Uniqueness	Y	Y	Y	Y
Reissuance	N	CI : Y DI : N	Y	Y
Personal information	Y	N	N	N
Independence against RRNs	-	N	N	Y
Social whirl	-	Low	Middle	High

III. 독립적 난수기반 개인식별번호 체계

3.1 독립적 난수기반 개인식별번호의 동작 절차 및 관리체계

3.1.1 발급 과정

본 논문에서 제안하는 독립적 난수기반 개인식별번호 체계는 행정정보보유기관, 주민등록 행정기관, 본인확인기관 및 개인식별번호 수집 허용기관 등으로 구성된다. 현재 국내에서는 주민센터가 본 논문의 주민등록 행정기관에 해당하며, 안전행정부의 행정정보공동이용센터가 행정정보보유기관에 해당한다. 개인식별번호 수집 허용기관이란 현행법에 따른 주민등록번호 등 수집 허용 민간 기관을 의미한다.

- 행정정보보유기관 - 안전행정부 행정정보공동이용센터
- 주민등록 행정기관 - 주민센터
- 본인확인기관 - 수집 허용기관에 본인확인을 위한 정보를 제공하는 기관
- 개인식별번호 수집 허용기관 - 현행법상 주민등록번호 수집이 허용된 기관

독립적 난수기반 개인식별번호 체계에서 개인식별번호는 생성, 사용, 사용 중지 단계를 거친다. 개인식별번호 생성 단계에서는 기존 주민등록 과정에서 주민등록정보시스템에 난수생성모듈이 추가되는 특징을 가지며, 출생신고에 의한 생성 또는 변경신청에 의한 생성이 이뤄진다.

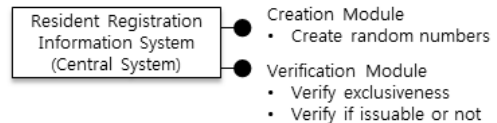


Fig.2. Two-modules that the resident registration information system includes

행정정보보유기관의 주민등록정보시스템(중앙시스템)에서 난수를 생성할 때 Fig.2와 같이 난수생성모듈과 난수검증모듈로 구분되어 두 개의 모듈이 동작한다. 난수생성모듈에서는 개인식별번호로 부여될 난수를 생성하는데, 이때 생성된 난수가 이전에 생성된 값과 충돌하지 않는지 1차적으로 확인하도록 할 수 있

다. 이미 한 번 생성된 값은 개인에게 발급되었을 가능성이 크므로, 생성된 난수 값이 이전에 생성된 값이 아니도록 한다. 여기서 발급되었을 가능성이 크다고 한 것은 생성된 난수 값이 난수검증모듈에 의해 발급이 제한되는 값으로 판단되면 개인에게 발급이 되지 않을 수 있기 때문이다.

난수생성모듈에서 생성한 난수를 난수검증모듈에서 2차적으로 이미 발급된 개인식별번호와 중복되는지 확인하고, 또한 발급이 가능한 값인지 확인한다. 예를 들어, 이미 개인에게 발급된 값 이외에도 1111...1 이나 1717...17 과 같이 단순 반복이 되는 값을 개인식별번호로 발급할 경우 안전하지 않으므로, 이러한 값들은 블랙리스트로 작성하여, 난수검증모듈에서 걸러내도록 한다.

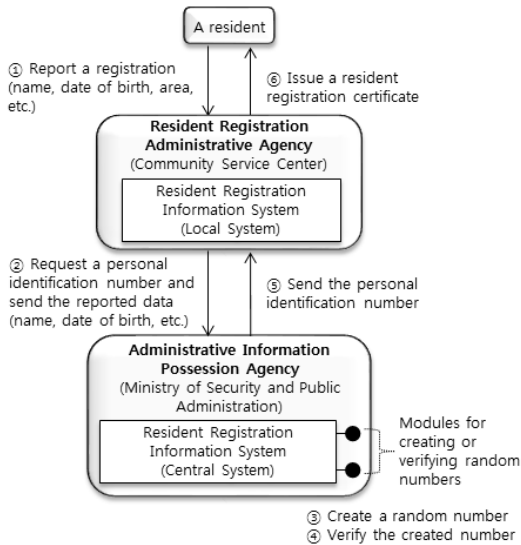


Fig.3. The procedure for issuing a personal identification number

3.1.2 오프라인에서의 사용

개인식별번호 생성 후 사용 단계는 개인정보 수집 허용 기관 및 기업에 의한 수집, 보관, 파기로 구분되며, 개인정보 수집 허용 기관 및 기업의 데이터베이스와 본인확인 기관의 데이터베이스가 연동되어 본인확인 작업이 이루어진다. 개인식별번호의 오류, 유출 등의 사유로 개인식별번호를 변경할 경우 변경 전의 개인식별번호는 사용 중지 단계로 들어간다.

본 논문에서는 민간 기관에서 행정정보보유기관의

주민등록정보시스템에 직접적으로 접근함으로써 발생할 수 있는 보안 사고를 예방하기 위해, 주민등록정보시스템(중앙시스템)과 개인정보확인시스템을 물리적으로 구분하였다. 개인정보확인시스템은 행정정보보유기관에서 직접 관리할 수도 있고 본인확인기관을 별도로 마련하여 운용할 수도 있다. 별도의 본인확인기관을 마련할 경우, 행정정보보유기관의 부속기관이나 그에 준하는 국가기관이 그 역할을 담당한다. 이는 개인정보확인시스템을 민간에서 관리할 경우 발생할 수 있는 유출사고를 차단하기 위함이다. 성명, 개인식별번호를 포함한 개인정보의 최신 값을 유지하기 위해 본인확인기관의 데이터베이스는 주기적으로 행정정보보유기관의 데이터베이스와 동기화된다. 각 데이터베이스의 기본키는 개인식별번호가 될 수 있다.

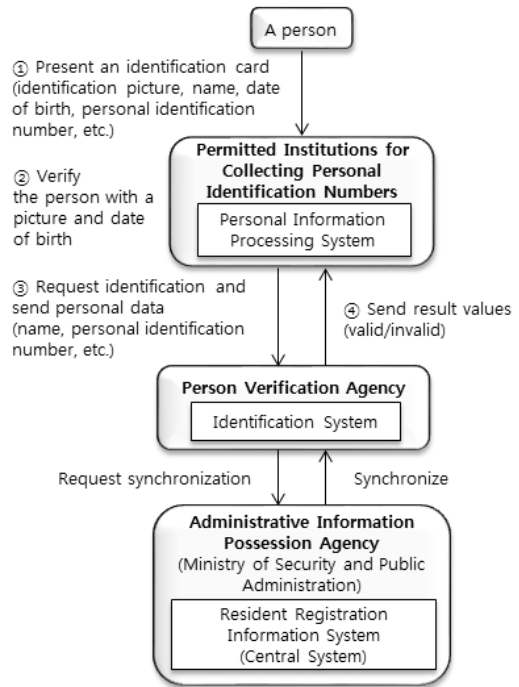


Fig.4. The procedure for the person verification in the real world

독립적 난수기반 개인식별값의 생성 및 처리 절차를 나타내는 Fig.3.와 Fig.4에서 각 기관 시스템의 정보 처리와 시스템 간 데이터의 이동은 Table 5와 같다.

Table 5. This table shows a process of personal identification data.

Institution	Institution System	Database Attributes	Main Processes of the System	Transmitted Data	Destination System
Administrative Information Possession Agency	Resident Registration Information system (Central system)	Resident registration database	Creating personal identification numbers, Checking collision of created numbers, Creating·modifying·deleting instances, etc.	Personal identification numbers, Personal identification information*, etc.	Resident Registration Information System (Local system)
		Personal identification numbers, Personal identification information*, Modifying value of personal identification numbers, etc.			Identification System
Resident Registration Administrative Agency (Community Service Center)	Resident Registration Information System (Local system)	Resident administrative database Administrative application number, Personal identification numbers of declarers, Personal identification information of declarers*, etc.	Treating and administering administrative applications, Creating·modifying·deleting instances, etc.	Institution information, Administrative application number, Personal identification information*, Request value issuing personal identification number, etc.	Resident registration information System (Central system)
Person Verification Agency	Identification System	Identification database	Creating·modifying·deleting instances, Accepting/Denying requests for identifications, Checking identifications for requested personal information, etc.	Synchronization request value	Resident Registration Information System (Central system)
		Personal identification numbers, Personal identification information*, Inquiry record, etc.		Identification result value	Personal Information Processing System
Permitted Institutions for Collecting Personal Identification Numbers	Personal Information Processing System	Institution database Personal identification numbers, Personal identification information*, etc.	Creating·modifying·deleting instances, Checking identifications for personal information, etc.	Personal identification numbers, Personal identification information*, Identification request value, etc.	Identification System

* Personal identification information*: Name, Gender, Date of birth, Place of birth, Recent residence address, Telephone number, Family relations, and etc.

3.1.3 온라인에서의 사용

본 논문에서 제안하는 온라인 환경에서의 독립적 난수기반 개인식별번호 체계는 3.1.2의 오프라인 기관이 온라인 공간으로 대체된다. 온라인 공간은 비대면 환경이므로, 주민등록번호 수집 허용 기관의 개인정보처리시스템에 본인인증을 위한 본인확인모듈이 추가된다. 온라인상에서 본인인증을 받고자 하는 사용자는 본인인증정보를 입력하면, 본인확인모듈로 입력값이 전송되어 처리된다. 이때 본인인증은 성인인증도 포함한다.

본인확인을 위한 인증방법으로는 현행과 같이 휴대폰 인증, 아이핀 인증, 공인인증서 인증 등이 사용될 수 있다.

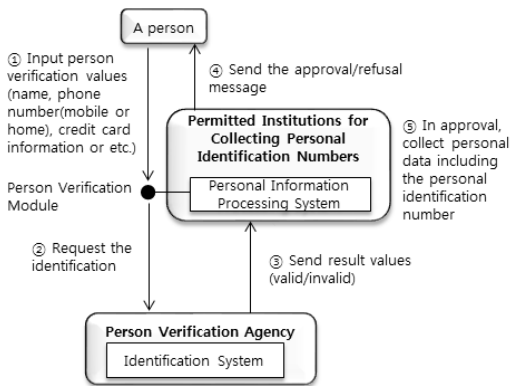


Fig.5. The procedure for person verification and gathering the personal identification data on the Internet

IV. 쟁점사항 및 해소방안

4.1 쟁점사항

4.1.1 도입 전 준비단계

독립적 난수기반 개인식별번호 체계는 기존 주민등록번호를 대체함에 따라 공공기관, 병원, 금융기관 등 주민등록번호 수집이 허용되는 기관의 시스템, 데이터베이스 등의 전환 비용이 발생할 것이다. 또한 기관이나 기업의 데이터베이스에서 주민등록번호를 삭제하고 개인식별번호를 추가하여 일괄적으로 갱신하는 과정에서 고려해야 할 요소들 역시 있다. 법적 측면에서는 개인식별번호의 변경·정정 및 재발행에 대한 법안을 마련하여, 주민등록번호 대체 수단인 개인식별번호

체계가 원활히 발급, 유통 및 사용될 수 있도록 해야 할 것이다. 예컨대, 한 개인이 평생 동안 개인식별번호를 변경할 수 있는 사유와 횟수, 한 번 부여된 개인식별번호에 대한 최소한의 유지기간 등에 대한 설정이 필요하다.

가. 주민등록법 및 관련법 등 검토

독립적 난수기반 개인식별번호 체계의 도입 및 활용을 위해서는 주민등록법시행규칙 제2조와 주민등록법 시행령 제8조의 개정이 선행되어야 한다. 주민등록법시행규칙 제2조는 주민등록번호에 대해 생년월일·성별·지역 등의 개인정보를 포함한 13자리로 작성할 것을 명시하고 있으며, 주민등록법 시행령 8조는 주민등록번호의 오류에 따른 정정만을 명시하고 있다. 독립적 난수기반 개인식별번호 체계로 전환되기 전, 개인식별번호의 변경·정정 가능한 요건 및 변경 횟수에 대한 제한 등의 법 개정이 요구된다.

개인식별번호가 난수기반으로 발급되는 경우에는 외국인에 대한 구분 역시 필요하다. 현재 주민등록번호의 일곱 번째 자리의 값을 통해 외국인등록번호가 구분되어지는 것처럼 외국인등록번호의 구분 등을 위한 방안들이 모색되어야 한다.

나. 개인식별번호 생성 및 회수

개인식별번호가 생성 및 관리되는 행정정보보유기관의 중앙시스템에 도입되는 난수생성모듈 및 난수검증모듈의 신뢰성 검증이 필요하다. 또한 한 개의 개인식별번호 내에서 동일한 숫자가 연속되거나 일련의 번호로 구성되는 등 제3자가 쉽게 추측 또는 추출할 수 있는 번호이거나, 개인식별번호의 첫 자리가 0으로 시작하여 일부 시스템 상에서 정확하게 인식이 안 될 가능성이 있는 번호가 부여되지 않도록 알고리즘 구성 혹은 도입 번호 검증 등의 절차가 필요하다.

주민등록번호가 표기되어 있는 주민등록증, 운전면허증 등의 신분증에 대한 회수와 재발급 절차도 이루어져야 한다. 또한 오프라인 상에서 주민등록증에 표기된 주민등록번호를 통해 쉽게 성인인증이 가능했던 부분도 난수의 개인식별번호 기반의 신분증 체계에서 생년월일을 표기하는 등 구현 방안 역시 고려해야 한다.

다. 데이터베이스 변경

고객정보 또는 수집한 개인정보에서 주민등록번호를 삭제하고 개인식별번호로 갱신하는 작업에 있어, 수정 시기 또는 시점, 데이터베이스의 일괄 수정 또는

개별적 수정 등 데이터베이스 전환 전반에 따른 논의가 필요하다.

4.1.2 주민등록번호와 개인식별번호 혼용 단계

독립적 난수기반 개인식별번호 체계가 도입되는 시점부터는 출생 신고 시 개인식별번호만이 부여되며 주민등록번호는 부여되지 않을 것이다. 반면, 이미 주민등록번호를 부여받은 국민은 새로운 개인식별번호를 부여받게 될 것이며, 기존의 주민등록번호는 전 국가 차원에서 삭제를 강제하게 될 것이다. 공공기관이나 개인식별번호 수집 허용 기관의 경우 본인 확인이 필요한 업무에서 기존 주민등록번호가 새로 부여된 개인식별번호와 동일한 인물이라는 것에 대한 확인이 필요할 수 있기에 이에 대한 대응이 필요하다.

가. 본인확인 및 개인식별번호의 관리

개인식별번호 도입 전에 사용한 주민등록번호에 대한 본인 인증이 필요하다. 즉, 기존 문서·데이터 등에 기록된 주민등록번호가 개인식별번호만을 보유한 개인이 본인과 일치함을 입증할 수 있어야 한다. 또한, 개인식별번호의 경우 주민등록번호와 다르게 법에서 정한 사유에 따라 제한적으로 변경이 가능하므로, 개인식별번호 수집 허용 기관·기업 등에서는 한 개인의 개인식별번호 값을 수정할 때 한 개인의 변경 전·후의 개인식별번호들에 대해 같은 인물임을 확인할 수 있어야 한다.

나. 수기문서, 종이에 출력된 문서 등의 처리 및 관리
관공서나 기업 등에서 법·정책·내규 등의 명목으로 주민등록번호가 표기된 자료를 종이 등의 형태로 보관하고 있는 경우 주민등록번호를 삭제하고 개인식별번호를 표기하기 위해 문서 일체를 파쇄하고 재작성하는 것은 현실적으로 어려울 수 있다. 이 경우 단계적으로 전자문서로 전환하며 이 과정에서 주민등록번호를 삭제하고 해당되는 개인식별번호로 대체하는 등 정책적인 대안 마련이 필요하다.

다. 사용

새로운 개인식별번호를 사용해야 하는 국민들의 불편도 예상된다. 주민등록번호에 익숙한 개인이 일정 자리 이상의 난수를 새로 부여받아 사용할 경우, 발급받은 개인식별번호를 외워야 한다는 것에 대한 심리적 부담이 따를 수 있다.

개인식별번호를 부여받은 개인이 기존 문서에 기록된 주민등록번호에 있어 본인 인증이 불가피할 때 임시적으로 인증서를 발급받는 등의 절차로 인해 일시적으로 불편함을 느낄 수 있다.

주민등록을 담당하는 행정기관 역시 새로운 개인식별번호를 부여하고 관리함에 있어 어려움이 있을 수 있다. 특히 전환과정에서 두 번호가 임시적으로나마 혼용이 되어 발생하는 혼란과 입증 요청 등을 예상할 수 있다. 또한 개인식별번호의 특성인 변경가능성에 따라 변경 요청 과정 역시 우려할 수 있다. 특히 개인정보 세탁 등의 관점에서 개인식별번호 유지에 따른 충분한 피해가 예상되지 않음에도 재발급을 신청하는 등 남용할 수 있을 것이다.

4.1.3 독립적 난수기반 개인식별번호 단독 사용 단계

본인 인증 등을 위해 주민등록번호를 더 이상 사용할 필요가 없어지는 시점부터 독립적 난수기반 개인식별번호의 단독 사용 단계로 접어든다. 즉 한 개인이 문서상 기록된 주민등록번호가 본인의 것임에 대한 인증이 요구되어지지 않으며, 한 개인에게 부여되었던 주민등록번호와 새로 부여된 개인식별번호의 연결성이 완전히 끊어지게 된다. 또한 기관 및 기업은 보유하고 있는 개인정보에서 주민등록번호 값이 없어도 전혀 업무나 관리 등에 지장이 없는 단계이다.

이 단계는 국가기관을 포함한 국내의 모든 기관 및 기업 등의 데이터베이스에 주민등록번호나 주민등록번호가 표기된 신분증 등이 완전히 삭제·파기된 상태를 기대할 수 있다. 중앙행정기관인 행정정보보유기관만 인증 등의 목적으로 주민등록번호를 보유하고 있을 수는 있으나, 주민등록번호가 유통되지는 않는다.

가. 본 단계의 진입의 시점

독립적 난수기반 개인식별번호의 단독 사용 단계에 이르기까지 오랜 기간이 소요될 수 있다. 현재 주민등록번호를 발급받은, 경제활동이 가능한 연령층이 경제활동인원에서 제외되는 시점이 되어야 이 단계가 도래할 수도 있다.

나. 개인에 대한 개인식별번호 이력의 관리

개인식별번호의 경우 주민등록번호와 다르게 법에서 정한 사유에 따라 제한적으로 변경이 가능하므로 개인식별번호 수집 허용 기관·기업 등에서는 한 개인의 개인식별번호 값을 수정할 때 한 개인의 변경 전·

후의 개인식별번호들에 대해 같은 인물임을 확인할 수 있어야 한다.

개인식별번호 수집 허용 기관·기업 등에서는 한 개인의 변경된 개인식별번호를 수집하여 데이터베이스·관리상 문서 등을 수정한 때는 변경 전 개인식별번호에 대한 기록을 바로 삭제하여 개인식별번호의 이력을 추적 할 수 없어야 한다.

4.2 해소방안

4.2.1 기술적 해소방안

독립적 난수기반 개인식별번호의 도입을 위해서는 앞서 언급한 쟁점사항들을 해소할 필요가 있다. 특히 개인식별번호로 생성되는 난수값의 위상을 생각했을 때 난수의 생성과 검증에 대한 기술적인 연구와 안전성 검토 등이 필요하다. 또한 독립적 난수기반 개인식별번호의 재발급 및 개인정보 변경 절차에도 혼란이 없어야 한다.

가. 난수의 신뢰성

난수를 생성함에 있어 충돌이 없거나 최소화하는 난수생성 알고리즘이 필요하며, 검증하는 단계에서는 생성된 값이 유일한 값인지(유일성), 발급 가능한 값인지(유효성) 등에 있어 신뢰성을 보장할 수 있어야 한다. 따라서 난수생성 알고리즘과 시스템, 난수검증 모듈에 연구와 신뢰성 평가가 필요하다.

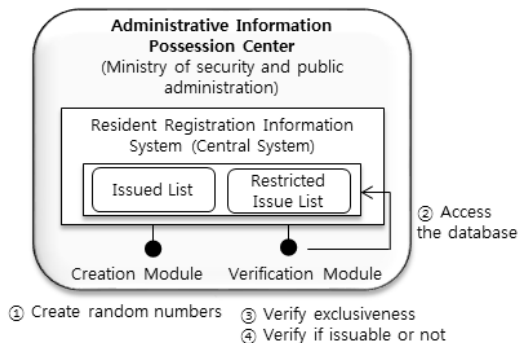


Fig.6. The process of verifying a created random number

난수가 13자리로 구성될 경우 난수 생성 시 생일역설(Birthday Paradox)에 의해 10^{13} 의 루트 개인 약 3백만($10^{6.5}$)개 당 한 개씩 충돌이 50%의 확률로

발생한다. 이를 고려했을 때 충돌 발생은 피하기 어렵다. 그러므로 충돌은 최소화하며, 효과적으로 난수를 생성할 수 있는 알고리즘과 시스템에 대한 연구가 필요하다. 이러한 충돌 발생 가능성과 본인확인정보의 유일성, 유효성 보장을 위해 난수 검증 모듈은 중요하다. 기존 발급 정보와 블랙리스트 등을 보유하며 이 정보들과 생성된 알고리즘과 비교하여 적절성을 효과적으로 검증할 수 있도록 검증 모듈의 설계와 구현이 필요하다.

나. 재발급 및 개인정보 변경 절차

재발급 과정에서도 새 개인식별번호를 발급하는 절차는 '가. 난수의 신뢰성' 과정에 따라, 주민등록정보시스템에서 난수생성모듈과 난수검증모듈에 의해 생성된다. 한편, 재발급 받은 개인식별번호가 활성화됨과 동시에 기존의 개인식별번호는 비활성화 된다.

여러 기관에서 보유한 사용자의 개인정보를 편리하게 갱신하기 위해서는 본인확인기관의 개인정보확인 시스템이 각 기관의 개인정보처리시스템과 실시간으로 동기화되도록 할 수 있다. 다만, 이때는 동기화를 요청하는 개인정보처리시스템이 개인식별번호 수집 허용 기관의 것이며, 동기화를 시도하는 개인식별번호에 대해 본인의 동의하에 수집한 개인정보라는 것을 입증해야 한다. 개인식별번호 수집 허용 기관이라는 것은 인증키로 입증할 수 있으나, 시스템 간의 통신 과정에서 본인의 동의하에 수집한 개인정보라는 것에 대한 입증은 신뢰성을 확보하기 어렵다.

한편, 개인식별번호 수집 허용 기관이 사용자의 재발급 이전 개인식별번호를 수집한 상태더라도 사용자의 동의가 더 이상 유효하지 않거나 사용자가 재발급 된 개인식별번호의 제공을 원하지 않을 수 있다. 개인식별번호의 변경가능성의 목적을 달성하기 위해, 편의보다 개인정보의 보호에 기초한 절차를 구성할 수 있다.

주민센터에서 개인에게 개인식별번호 및 신분증을 재발급 할 때, 별도의 인증 값을 부여한다. 이는 '개인식별번호 변경에 따른 동일 인물 인증서'와 같은 문서에 표기하여 부여될 수 있다. 이 별도의 인증값은 두 가지 목적으로 사용된다. 우선은 개인식별번호 수집 허용 기관이 변경 전 개인식별번호와 변경 후 개인식별번호가 동일인인 것이라는 확인하기 위함이고, 다음은 개인식별번호 수집 허용기관이 본인확인 기관에 개인정보를 요청할 때 개인의 동의하에 진행되는 것임을 확인하기 위함이다.

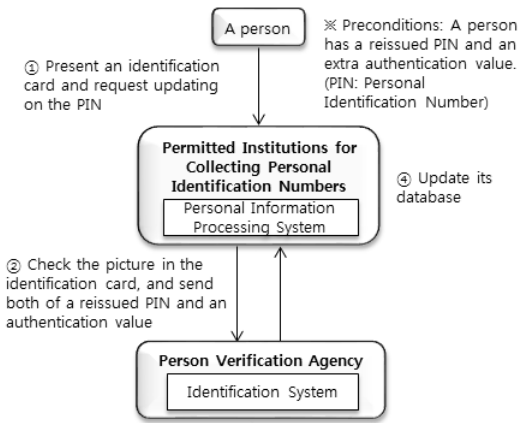


Fig.7. The process of identifying and updating the database in the real world when a personal identification number is reissued.

오프라인에서 개인식별번호 수집 허용 기관은 개인의 요청에 따라 재발급 된 개인식별번호를 수집한다. 이 과정에서 신분증의 증명사진을 통해 동일인임을 확인할 수 있으며, 별도의 인증값 입력을 통해 본인확인 기관으로부터 관련 개인정보를 확인할 수 있다.

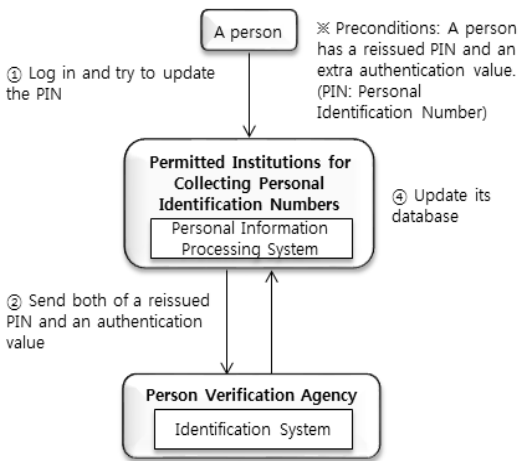


Fig.8. The process of updating the database in the Internet when a personal identification number is reissued.

개인식별번호 수집 허용 기관의 온라인상에서는 기존의 개인의 계정으로 로그인을 함으로써 동일 사용자임을 알 수 있으며, 개인정보 변경 시 재발급 된 개인식별번호와 함께 별도의 인증값을 입력함으로써 본인

임을 확인할 수 있다.

Table 6. This table presents a summary of predicted issues and technical solutions.

Issue	Solution
Creation and destruction of PINs	This paper proposes effective technical processes concerning creation, destruction and reissuance.
Managing a record of each individual PIN	<ul style="list-style-type: none"> • A reliability of random number through a verification module • Effective process of reissuance and updating a personal information using a certificate value

※ PIN: Personal Identification Number

4.2.2 정책적 해소방안

앞 절에서 난수의 생성 및 검증 단계에서의 신뢰성을 기술적으로 해소하였다면, 동일한 숫자의 연속이거나 일련의 번호의 형태인 개인식별번호를 사용하지 않도록 제한하는 정책과 기존의 주민등록번호와 패턴이 비슷하게 생성되어 사용 시 혼란을 야기할 값은 아닌지, 내국인과 외국인의 구분이 가능한지 등 발급과 관리방안을 정책으로 해소할 필요가 있다. 또한 개인식별번호 체계 도입 시 최초의 발급 과정, 변경된 개인식별번호에 대해 동일 인물임을 입증하는 방법 등 행정적인 해결수단이 동반되어야 할 것이다. 한편, 개인식별번호를 수집하는 기관 역시 내부 관리 정책 등을 수립해 발생할 수 있는 문제를 해소해야 할 것이다.

가. 발급 가능한 개인식별번호의 한정

독립적 난수기반 개인식별번호 생성 시 특정 값은 사용 시 불편을 초래할 우려가 있어 제한할 수 있다. 대표적으로 제한할 수 있는 값은 '111...1'과 같이 처음부터 끝까지 같은 숫자로 이루어진 번호, '12345...'과 같이 일정 자릿수 이상의 값, 그리고 '091...' 등 0으로 시작하는 값 등이다. 이는 임의로 입력할 수 있거나 시스템에서 입력에 혼동이 있을 수 있는 값이므로 이와 같은 특정 값들은 발급되지 않도록 하여 개인식별번호의 임의성을 높일 수 있다.

만약 독립적 난수기반 개인식별번호 역시 13자리의 값으로 구성된다면 난수기반 개인식별번호와 기존 주민등록번호와의 중복성 문제와 구별 역시 필요하다. 이는 난수번호의 설계를 통해 해소할 수 있다. 예를

들어, 주민등록번호의 세 번째 자리 값은 0 또는 1로만 구성되므로 주민등록번호와 개인식별번호의 혼용 기간 동안 개인식별번호의 세 번째 자리 값은 0과 1을 피하여 생성되도록 할 수 있다.

나. 외국인등록번호의 마련

개인식별번호의 특정 자리의 값은 난수생성모듈에 의해 생성되지 않고 최소한의 개인정보를 갖게 한다. 즉, 개인식별번호의 첫 번째 자리에 내·외국인 여부에 따라 다른 값을 정하여 구분할 수 있다.

다. 최초 개인식별번호의 발급 및 신분증의 재발급

개인은 개인식별번호를 부여받기 위해 본인의 주민등록증을 지참하여 주민센터 또는 이에 준하는 기관에 방문하여 주민등록증 반납과 동시에 개인식별번호 발급 신청을 할 수 있다. 기 주민등록번호 보유자의 개인식별번호는 행정정보보유기관에 의해 일괄적으로 생성되어진 상태이며, 전환 요청 시 해당 번호가 부여된다. 이때 담당행정기관은 개인의 개인식별번호 발급 신청을 수리하는 동시에 주민등록번호가 기재된 주민등록증을 회수하게 된다. 개인식별번호를 발급받은 개인은 발급 완료 시점부터 주민등록번호 수집 허용기관에 주민등록번호가 아닌 개인식별번호를 제공하게 된다. 개인식별번호가 기재된 신분증은 현행처럼 수일 내에 등기우편 또는 방문으로 받게 된다. 주민센터에서 주민등록번호 회수 및 개인식별번호 발급이 완료되면, 운전면허증 발급 기관과 같이 주민등록번호가 기재된 신분증 또는 자격증 등을 발급하는 기관은 주민등록번호가 표기된 신분증·자격증을 회수하고, 개인식별번호를 기재하여 재발급 한다.

라. '주민등록번호 변경에 따른 동일 인물 인증서'의 임시적 발급

주민등록번호와 개인식별번호의 혼용 기간 중 공공기관이나 개인식별번호 수집 허용 기관에 의해 기 사용 주민등록번호와 개인식별번호가 동일한 인물의 것임을 확인해야 할 상황을 위해 임시 인증서 발급 제도를 도입할 수 있다. 즉, 개인이 행정기관 및 무인민원발급창구 등을 통해 위·변조 및 복사 방지 처리가 되어있는 '주민등록번호 변경에 따른 동일 인물 인증서' 등을 발급받아 활용할 수 있으며, 이때 발급된 인증서는 유효 기간을 엄격히 한정하여 해당 용도로만 사용하며 남용을 방지할 수 있다.

개인식별번호가 변경되었을 경우에도 유사한 형태

의 동일 인물 인증서를 발급받아 본인인증 업무에 대해 본인임을 입증하고, 기존 개인식별번호가 기록된 서류 혹은 디지털 매체에 저장되어 있는 데이터 일체를 변경하도록 한다.

마. 개인식별번호가 기록된 데이터베이스의 관리

개인식별번호 수집 허용 기관·기업 등은 개인정보 수집에 있어 특정인에 대한 개인식별번호는 한 개만 보관할 수 있도록 해야 한다. 즉, 개인의 변경된 개인식별번호를 수집하여 데이터베이스·문서 등을 수정함에 있어 변경 전 개인식별번호는 바로 삭제하여야 한다. 이는 개인식별번호의 이력을 관리·보존할 수 없도록 하기 위한 것으로, 기 유출된 주민등록번호 혹은 개인식별번호와의 연결성을 끊어내 2차, 3차 피해를 예방하기 위한 목적이다.

한편, 개인식별번호 발급 기관인 행정정보보유기관은 한 개인에 대한 개인식별번호의 이력을 관리할 책

Table 7. This table presents a summary of predicted issues and legal solutions.

Issue	Solution
Processes to create and reissue random PINs	This paper considers related law revisions as follows. <ul style="list-style-type: none"> • Concealment of personal information Amendment : Article 2, the Enforcement Regulations of the Residents Registration Law • Modifiability of PINs : Article 8, the Enforcement Regulations of the Residents Registration Law
Restrictions of reissuance for preventing abuse and misuse	This paper considers related law revisions as follows. <ul style="list-style-type: none"> • Reasons and the number of times reissuing PIN : Modifiability of PINs : Article 8, the Enforcement Regulations of the Residents Registration Law
Processing PINs by permitted institutions for collecting PINs	This paper considers related law revisions as follows. <ul style="list-style-type: none"> • Process of reissued PINs : Article 2, the Personal Information Protection Law • Process of PINs before reissuance : Article 16, the Personal Information Protection Law

※ PIN: Personal Identification Number

임이 있다. 이는 앞서 개인식별번호 변경에 따른 확인 절차에서 설명한 것과 같이 서로 다른 개인식별번호를 가진 개인이 동일인임을 증명하기 위한 목적이다. 이때 행정정보유기관은 개인식별번호 이력에 대한 데이터가 외부로 유출되지 않도록 강력한 보안조치를 취해야 한다.

4.2.3 법적 해소방안

본 논문에서 제시한 기술과 정책적으로 해소방안에 선행하여 독립적 난수기반 개인식별번호 체계가 국가의 개인식별값으로 인정받기 위한 법제 개선이 필요하다. 이를 위해 현행법에서 규정하고 있는 주민등록번호 발급, 주민등록번호 구성, 정정 및 변경 금지 등 관련 조항의 개정과 관련 정책 이행을 위한 제·개정이 필요하다.

독립적 난수기반 개인식별번호 체계 도입을 제안함에 있어 발생할 수 있는 논점에 대한 법적 해소방안은 다음과 같다.

가. 주민등록법 시행규칙 제2조의 개정

본 논문에서 제시하는 독립적 난수기반 개인식별번호의 특징 중 개인정보 비(非)노출성을 만족하기 위해서는 대체 수단으로서의 도입 시 주민등록법시행규칙 제2조의 개정이 선행되어야 한다.

주민등록법시행규칙 제2조는 주민등록번호가 생년월일·성별·지역 등의 개인정보를 포함한 13자리로 작성될 것을 명시하고 있다. 독립적 난수기반 개인식별번호 체계로 전환되기 전, 개인정보를 포함하지 않는 임의의 수로 개인식별번호가 작성되기 위한 개정이 필요하다.

나. 주민등록법 시행규칙 제8조의 개정

새로운 개인식별번호의 특징인 변경가능성을 만족하기 위해서는 주민등록법 시행령 제8조의 개정이 필요하다.

주민등록법 시행령 8조는 주민등록번호의 오류에 따른 정정만을 명시하고 있다. 독립적 난수기반 개인식별번호 체계로 전환되기 전, 개인식별번호의 변경·정정 가능한 요건 등이 개정되어야 한다. 또한 개인식별번호의 변경·정정 시, 변경·정정 가능한 요건에 제한을 두어 개인식별번호의 재발급에 대한 남용 또는 악용을 방지할 수 있다. 미국의 사회보장번호 제도와 같이 일 년에 3회, 평생 10회 등 횟수 제한을 두는 방

안이 가능하다. 또한 해킹사고 등으로 개인정보 대량 유출로 인해 피해가 예상될 경우 국가에서 개인식별번호의 변경을 권고·강제한 경우에는 예외적으로 횟수에 적용받지 않고 변경할 수 있으며, 이 경우 변경에 따른 비용을 개인정보 유출 기관이 부담하도록 하는 방안이 가능하다.

다. 개인정보 보호법 상 개인식별번호 관련 조항의 개정

본 연구에서 제안하는 새로운 국가 개인식별번호의 효과성을 위해서는 개인이 정당한 사유가 있을 경우 개인식별번호를 변경할 수 있으며, 이에 따른 처리가 이루어져야 한다. 이를 위해서는 개인정보 보호법 등 관련법에서 개인식별번호 처리 등과 관련된 조항의 개정이 필요하다. 대표적인 관련 조항은 개인정보 보호법 제15조와 제16조 등이다.

개인정보 보호법 제15조제1항은 개인정보처리자가

Table 8. This table presents a summary of predicted issues and legal solutions.

Issue	Solution
Processes to create and reissue random PINs	This paper considers related law revisions as follows. <ul style="list-style-type: none"> • Concealment of personal information Amendment : Article 2, the Enforcement Regulations of the Residents Registration Law • Modifiability of PINs : Article 8, the Enforcement Regulations of the Residents Registration Law
Restrictions of reissuance for preventing abuse and misuse	This paper considers related law revisions as follows. <ul style="list-style-type: none"> • Reasons and the number of times reissuing PIN : Modifiability of PINs : Article 8, the Enforcement Regulations of the Residents Registration Law
Processing PINs by permitted institutions for collecting PINs	This paper considers related law revisions as follows. <ul style="list-style-type: none"> • Process of reissued PINs : Article 2, the Personal Information Protection Law • Process of PINs before reissuance : Article 16, the Personal Information Protection Law

※ PIN: Personal Identification Number

개인정보를 수집할 수 있는 경우를 명시함에 있어 각 호와 더불어 개인의 개인식별번호가 변경된 경우를 추가할 수 있다. 이와 더불어 제16조에서는 개인정보 수집 제한을 명시하고 있는데, 개인식별번호를 재발급 받은 경우, 변경 전의 개인식별번호를 수집할 수 없도록 항이 추가되어야 한다.

한편, 2012년 8월부터 정보통신망법에 의해 온라인상에서 법령상 근거 없는 주민번호 수집이 금지되고 있으며, 개인정보보호법에 의해 올해 8월 7일부터는 오프라인으로 확장된다.

4.2.4 소결

김민호 외 연구(2009)에 따르면, 주민등록번호는 특정인을 지시할 수 있게 하는 식별기능, 본인 여부를 특정 문서나 기관에 인용하여 증명하게 하는 인증기능, 개인이 지니고 있는 속성을 알려주는 묘사기능, 행위자를 특정하기 위해 본인확인 또는 실명확인 기능 등이 있다[10]. 식별기능은 주민등록번호의 유일성·종속성을 기반으로 한다.

독립적 난수기반 개인식별값은 재발급과 동시에 이전 값은 비활성화 되어 사회적으로 유효하지 않은 값이 되므로, 한 시점에 한 사람은 하나의 개인식별번호만을 가지며 이는 식별기능을 만족한다. 이 식별기능으로 인해, 개인식별번호 수집 허용기관에서 본인 확인 시 개인식별번호를 사용하여 본인확인기관에 본인 확인을 요청하므로 인증기능 역시 만족한다.

개인식별번호는 난수기반이므로 번호 자체에 묘사 기능을 가지지 않는다. 다만, 특정 자리의 값이 내·외국인 구분을 위해 할당될 수 있다. 성인인증 등 나이 확인이 필요한 경우에는 오프라인에서는 신분증에 생년월일을 표기하여 확인할 수 있으며, 온라인에서는 현재 시행되는 바와 같이 휴대폰 인증 등의 인증 수단을 사용하여 성인인증이 가능하다.

아울러, 독립적 난수기반 개인식별번호 제도에서 오프라인 본인확인 절차는 신분증의 증명사진과의 대조를 통해 본인확인이 가능하며, 온라인 본인확인 절차는 본인확인기관과 연동하여 휴대폰 인증 또는 공인인증서 인증이 유지될 수 있다. 실명확인 절차 역시 본인확인기관과의 연동을 통해 가능하다.

Table 9는 기존의 주민등록번호가 국가 개인식별번호로서 가지는 기능 및 용도를 독립적 난수기반 개인식별번호 제도에서도 만족함을 설명한다. 이는 본 논문의 4.2에서 제시하는 방안들을 고려하여 적용함

으로써 가능한 것이며, 현재 주민등록번호가 사용되는 영역에서 대체 가능하다는 것을 의미한다.

Table 9. This table shows the core analysis that the Unconnected Random Personal Identification Number(URPIN) has functions as a national personal identification number.

Function	Analysis
Identification function	<p>The URPIN satisfies an identification function including uniqueness.</p> <ul style="list-style-type: none"> Only one personal identification value which is valid is allowed per person. The verification module at the resident registration information system prevents collision(equal) results.
Certification function	<p>The URPIN satisfies a certification function.</p> <ul style="list-style-type: none"> URPIN has identification and uniqueness, which makes a Person Verification Agency perform personal verification.
Description function	<p>The URPIN system satisfies a description function.</p> <ul style="list-style-type: none"> It has an adult certification function as follows. It provides foreigner registration numbers as follows. It is not indispensable to mark a place of birth to an identification card, and copy of resident registration can be used as needed.
Adult certification function	<ul style="list-style-type: none"> Personal information such as date of birth and gender is marked in an identification card, and it can be an adult certification means in the real world(off-line). On the Internet, institutions can require adult certification by using an identification by a mobile phone or a certificate.
Foreigner registration number function	<ul style="list-style-type: none"> The particular place value of URPIN is allocated for foreigner certification in the real world and on the Internet both.
Personal verification function	<p>The URPIN satisfies a personal verification function.</p> <ul style="list-style-type: none"> A picture of an identification card makes personal

	verification in the real world. • An identification by a mobile phone or a certificate is still maintained on the Internet.
Real name verification function	• Real names can be verified with the URPIN by requesting the person verification agency.

V. 결 론

주민등록번호를 포함한 국가 개인식별체계는 특정 개인을 확인할 수 있는 효과적인 식별값이며 동시에 본인임을 확인할 수 있는 수단이다. 이러한 강력한 효과는 유출사고 시 심각한 피해로 다가올 수 있다. 따라서 본연의 기능인 개인식별, 본인확인 기능을 보장 하면서 피해를 최소화하기 위한 새로운 방안의 마련이 필요하다.

주민등록번호 대체 수단으로 논의되고 있는 아이핀 (I-PIN)의 활용 확대, 또는 주민등록 발행번호 체계, 독립적 난수기반 개인식별번호는 각각 장·단점이 있는 대안이다. 하지만 사실상 현존 경제활동인구 전체의 주민등록번호가 유출된 상황에서 새로운 수단은 주민등록번호와의 연결성이 없어야만 근본적인 해결이 될 수 있다.

올해 7월 31일에 안전행정부 및 관계부처에서 합동으로 발표된 '개인정보보호 정상화 대책'에 따르면, '생명·신체를 해치거나 재산상 중대한 피해를 입을 것이 확실한 사람에 한하여 주민등록번호 변경을 허용하기로 했으나, 이는 극히 제한적이므로 이미 유출된 모든 주민등록번호에 대한 해결책이 될 수 없으며, 주민등록번호는 여전히 개인정보를 포함하고 있게 된다. 또한 아이핀을 오프라인에서도 본인인증 수단으로 사용할 수 있는 것을 제시하고 있으나, 역시 지금까지 유출된 주민등록번호를 보완하는 수단이 아니며, 주민등록번호를 수집할 수 없는 기관에 필요한 대체 수단으로 작용할 뿐이다[11].

이러한 측면에서 독립적 난수기반 개인식별번호는 가장 효과적인 대안임에 분명하다. 기존 주민등록번호를 완전히 삭제하는 근본적인 변화로 사회적 우려와 반발 등이 예상되더라도 불구하고, 개인정보보호 차원에서 근본적인 해결이 되지 않으면 우리는 정보화 사회의 필수요소인 신뢰를 잃게 될 수 있다.

본 연구에서는 이러한 예상되는 쟁점사항, 우려사

항 등을 폭넓게 정리했으며, 기술적, 정책적, 법적 대응방안 마련을 통해 이를 충분히 해소할 수 있음을 보였다. 따라서 본 연구를 통해 향후 주민등록번호 제도 개선에 있어 논의의 폭을 넓힐 수 있을 것으로 기대한다.

하지만 본 연구는 아직까지 구체화되지 않은 체계를 개념적으로 연구한 것이며, 많은 부분 가정을 통한 연구여서 실제 구현되는 환경과는 다를 수 있다. 향후 주민등록번호 전면 개선에 따른 사회적 비용에 대한 연구와 더불어, 구체적인 발급 체계와 절차, 시스템 구성, 난수 생성 알고리즘 연구, 신분증 변화 등 각 세부요인에 대해 연구와 정책 결정이 필요할 것이다.

References

- [1] Financial Services Commission Press release: "The Present Condition and Plan For the Action Against Financial Information Leakage of the Credit Card Companies," Financial Services Commission, Jan. 19, 2014.
- [2] Yeong-hong Kim, "The necessity need of the improvement on the resident registration number system," Resident Registration Number System Reform Forum, Feb. 2014.
- [3] Gi-jung Kim, "The nation administration system and human right - focusing on the family register and the resident registration system," The Golden Jubilee Academic Event of the Universal Declaration of Human Rights, Feb. 1999.
- [4] Hyung-hyo Lee, "Requirements of an alternative resident registration number," 2010 Korean Institute of Information Technology Summer Regular Conference, pp.398-401, May. 2010.
- [5] Min-ho Kim, "A study on the reform of the resident registration number system," 23(3), Sungkyunkwan Jurisprudence Academic Journal, pp. 445-468, Dec. 2011.
- [6] Seung-Hyun Kim et al., "A Study on an alternation of RNN and access control for

- offline environments by using I-PIN," Korea Information Processing Society Spring Meeting Journal, 18(1), May. 2011.
- [7] Interagency Press release: "Personal information security normalization countermeasures," Ministry concerned, Jul. 31. 2014.
- [8] Gi-ho Park, "Offline stores would accept the 'i-PIN' instead of resident registration numbers." The Korea Economic Daily, Jun. 10. 2014.
- [9] Min-ho Kim, "A Study on the reform of the resident registration number system," Sungkyunkwan jurisprudence academic journal, pp. 445-468, Dec. 2011.
- [10] Min-ho Kim, "A study on the reform of the resident registration number system," Sungkyunkwan University Research&Business Foundation, Nov. 2009.
- [11] Interagency Press release: "Personal information security normalization countermeasures," Ministry concerned, Jul. 31. 2014.

〈 저자 소개 〉



한 문 정 (Mun-jung Han) 학생회원
 2013년 2월: 서울여자대학교 정보보호학과 졸업
 2013년 9월~현재: 고려대학교 정보보호학과 석사과정
 <관심분야> 개인정보보호, 시스템보안, 네트워크보안



장 규 현 (Gye Hyun Jang) 학생회원
 2009년 8월 : 고려대학교 산업시스템정보공학과 학사
 2009년 9월 ~ 현재 : 고려대학교 정보보호대학원 석·박사통합과정
 <관심분야> 국가사이버보안정책, 사이버국방, 국제안보, 개인정보보호 등



홍 석 희 (Seokhie Hong) 종신회원
 1995년 2월: 고려대학교 수학과 학사 졸업
 1997년 2월: 고려대학교 수학과 석사 졸업
 2001년 8월: 고려대학교 수학과 박사 졸업
 1999년 8월~2004년 2월: (주)시큐리티 테크놀로지스 선임연구원
 2003년 8월~2004년 2월: 고려대학교 정보보호기술연구센터 선임연구원
 2004년 4월~2005년 2월: K.U.Leuven. ESAT/SCD-COSIC 박사후연구원
 2005년 3월~2013년 8월: 고려대학교 정보보호대학원 부교수
 2013년 9월~현재: 고려대학교 정보보호대학원 정교수
 <관심분야> 대칭키·공개키 암호 분석 및 설계, 컴퓨터 포렌식



임 종 인 (Jong In Im) 종신회원
 1980년 2월: 고려대학교 수학과 졸업
 1982년 2월: 고려대학교 수학과 석사
 1986년 2월: 고려대학교 수학과 박사
 現 고려대학교 정보보호대학원 원장, 고려대학교 사이버국방학과 교수, 개인정보보호위원회
 위원, 대검찰청 디지털수사자문위원회 위원장, 금융보안 연구원 보안전문기술위원회 위원장,
 행정안전부 정책자문위원회 위원, 국방부 정보화책임관 자문위원, 한국저작권위원회 위원 등
 <관심분야> 사이버국방, 정보법학, 디지털포렌식, 개인정보보호, 융합기술보안 등