디지털산업정보학회 논문지 제16권 제3호-2020년 9월
http://dx.doi.org/10.17662/ksdim.2020.16.3.013

주민등록번호 기반의 온라인 본인확인서비스 기관 지정기준 개선방안 연구*

김 종 배**

A Study on Improvement method of designation criteria for Personal Proofing Service Based on Resident Registration Number

Kim Jongbae

〈Abstract〉

Currently, online means of replacing resident registration numbers(RRN) include I-Pin, mobile phone, credit card, MyPin, and general-purpose certificate. In order to issue alternative means based on the RRN, it must be designated through the designation review by the Korea Communications Commission(KCC) through a designation review by personal proofing agency and be subject to annual management. However, the criteria for designation and follow-up of the designation of the personal proofing agency carried out by KCC have been used in 2010 without revision, and there are problems that do not conform to the evaluation standards of various alternative means. Therefore, in this paper, we propose a method for improving the designation criteria and management system of the personal proofing service agency. The proposed method analyzes the characteristics of the alternative identification-based personal proofing service and proposes a follow-up management standard that can appropriately evaluate the analyzed characteristics and improves the designation criteria according to the emergence of new alternatives. Through the proposed method, it can be seen that it is possible to strengthen the safety of the personal proofing service based on the alternative means of RRN provided online and face-to-face and to protect the user's personal information.

Key Words : Personal Proofing Service Agency, Designated Review Criteria, Digital Identity, RRN Alternative Means

Ⅰ. 서론

최근 감염증 확산으로 인해 비접촉 시대로의 진입이 급속하게 진행되고 있다. 이에 따라 온라인서비스 제공 기관(Internet Service Provider: ISP)들은 온라인 상에서 상대방의 신원을 확인하기 위한 본인확인 수단의 적극적인 반영에 이르고 있다[1-7]. 즉, 온라인상에서 사용자를 식별하고 인증하는 것이 필요하다[5]. 온라인 상에서 본인확인은 적법하고 합당한 절차에 따라 합의된 사용자라고 증명하고 인증하는 과정이라고 할 수 있다. 현재 온라인상에서 공신력이 있는,

* 이 논문은 2020년도 산업통상자원부 및 산업기술평가관리원 연구비 지원(20011675)과 과학기술정보통신부와 한국연구재단 보조금에 의해 지원된 연구임(NRF-2020R1F1A106890011)
** 세종사이버대학교 소프트웨어공학과 교수

즉 국가가 보증하는 다양한 본인 식별 수단들에는 방송통신위원회(이하 "방통위")가 지정한 본인확인기관이 제공하는 본인확인서비스이다[8]. 온라인상에서 주민등록번호(이하 "주민번호") 대체수단 기반의 본인확인서비스를 제공하는 기관들은 <표 1>과 같다. <표 1>과 같이 주민번호 대체수단 기반의 본인확인서비스 제공 기관들은 다양하게 있으며 관련 주무 부처의 관리 감독을 받고 있다. 주민번호 대체수단 기반의 본인확인서비스 기관에서는 기존에 주민번호가 제공하였던 정보를 제공하기 위해 <표 2>와 같은 본인확인서비스 이용자 개인정보를 ISP들에게 제공하고 있다. 본인확인서비스 이용자의 다양한 개인정보를 ISP에 제공하고 있어 방통위는 본인확인기관의 지휘를 부여하기 위해 엄격한 기준으로 적합성 진행하고 있다[8]. 그러나 방송통신위원회에서 규정한 본인확인기관 적합성 심사 세부기준은 2012년도에 지정받은 아이핀 3사에 적용하기 위해 마련된 기준으로써, 이후 지정된 이동통신사, 마이핀, 신용카드, 그리고 전자서명 기반의 본인확인서비스 기관에 대한 심사를 위해서는 적합하지 않아 다양한 대체수단을 포괄할 수 있는 기준 개선이 필요한 상황이다. 예를 들어, 이동통신사 및 신용카드는 아이핀의 본인확인 연계정보(CI)와 중복가입정보(DI)를 생성하지도, 저장하지도 않도록 정하고 있으며 본인확인 주체의 정보 가입방식도 달라 2012년에 지정된 심사기준으로는 적합여부 확인이 이루어지지는 않는 문제점이 존재한다[3, 8]. 또한, 각 본인확인기관의 정보시스템 취약점 점검을 이행하기 위한 세부 기준이 존재하지 않아 매년 서로 다른 취약점 점검업체의 선정으로 인해 점검결과가 서로 상이하여 올바른 점검 이해 여부를 확인할 수 없는 문제점이 존재한다. 그리고 「본인확인기관 지정 등에 관한 기준」 고시에서도 신규 본인확인기관 지정 이후 중대한 서비스 변경절차, 기관 간 연계정보의 안전한 보호 및 점검 의무 등에 대한 세부항목이 누락되어 있어 기준 개정으로 안전한 본인확인서비스가 운영될 수 있도록 제도적인 정비가 필요한 상황이다. 마지막으로는 온라인 사업자들은 본인확인기관으로부터 전달받은 서비스 이용자들의 개인정보(이름, 생년월일, 휴대전화번호, 통신사, CI, DI, 내외국인여부 등, <표 3> 참조)에 대한 안전한 관리와 함께 과도한 수집을 금지하고 불필요할 시에는 즉시 파기해야 함에도 이용자로부터 직접 수집하지 않았다는 이유로 적절한 보호조치를 취하지 않는 경우

<표 1> 대체수단별 본인확인서비스 제공 기관 현황

대체수단	서비스 제공기관
아이핀/마이핀	코리아크레딧뷰로, 나이스평가정보, 서울신용평가정보
휴대전화	SKT, KT, LGT
신용카드	하나, 국민, 신한, 농협, 비씨, 현대, 롯데, 삼성카드
범용공인인증서	코스콤, 한국무역정보통신, 금융결제원, 한국정보인증, 한국전자인증

<표 2> 주민번호 대체수단 기반의 본인확인서비스가 제공하는 정보

대체수단	제공하는 정보
아이핀	아이핀번호, 성명, 생년월일, 성별, 내외국, 연령대, 연계정보(CI), 중복가입확인정보(DI)
휴대전화	휴대폰번호, 통신사, 성명, 생년월일, 성별, 내외국, 연령대, CI, DI
신용카드	성명, 생년월일, 성별, 내외국, 연령대, CI, DI

<표 3> 본인확인기관이 제공하는 연동전문 상의 세부 내용

항목	세부내용
연계정보1	주민등록번호와 1:1일 대응되는 88byte 길의 값
연계정보2	Null
중복가입방지정보	ISP에 중복가입 여부를 확인하기 위한 64byte 길의 값
성명	대체수단 발급자의 성명
생년월일	YYYYMMDD 형식의 8자리 숫자
성별정보	0: 여자, 1: 남자
내외국정보	0: 내국인, 1: 외국인
아이핀 번호	13자리 숫자
휴대폰 번호	휴대폰 번호
가입통신사	가입통신사 정보
기타 부가정보	IP주소, 인증시간 등

가 발생하고 있다.

따라서 본 논문에는 본인확인기관의 지정심사 및 사후관리를 위해 규정한 「본인확인기관 지정 등에 관한 기준」 고시에 대해 세부 심사기준을 다양한 신규 대체수단에 적용할 수 있도록 기준을 개선하여 서비스 이용자의 개인정보에 대한 안전성 강화와 침해 방지를 위한 개선 기준을 제시한다.

II. 관련 연구

본인확인서비스의 안전성을 강화하고 이용자의 개인정보를 보호하고자 하는 방안 연구는 지속적으로 수행되고 있다[1-5, 7]. 특히, 아이핀 기반의 본인확인서비스가 최초 등장으로 아이핀 서비스에 대한 기술적 안전성 강화와 서비스 활성화를 위한 방안 연구가 다양하게 수행되었다[1, 3, 7, 8-13]. 하지만, 아이핀 서비스의 경우 지식 기반의 서비스, 즉 사용자 아이디와 패스워드를 기반으로만 인증하는 서비스로써 고유의 취약점을 해결하지 못해 2차 패스워드, 1년간 미사용 시 휴면화 계정 실시 등으로 인해 서비스 활용도가 다른 대체수단들에 비해 현저히 낮은 상황이다. 휴대전화번호 기반 본인확인서비스에서 본인확인을 위한 이동통신사가 발송한 SMS 문자 메시지를 스미싱(smishing)하는 문제로 인해 이를 해결하기 위한 기술적 방안들이 연구되고 있다[14, 15]. 추가적으로 이동통신사들은 간편인증 서비스를 도입하여 생체정보(지문, 얼굴, 음성 등)을 활용한 본인확인서비스를 제공하고 있다[6]. 신용카드번호 기반의 본인확인서비스의 경우에는 과거 신용카드 번호의 대량 유출로 인해 신용카드 결제 비밀번호와 본인확인 시 입력하는 비밀번호의 분리, 그리고 사용자가 ISP에게 본인확인용 비밀번호를 제공하는 것이 아닌 자동응답시스템(ARS)을 사용한 방법도 제공하고 있다. 본인확인수단에 대한 기준과 관리체계에 대한 개선방안에 대한 연구는 현재까지 미비한 상황이며 대부분 기술적인 안전성 개선에 치중하고 있는 상황이다. 이는 본인확인기관의 신규 지정이 다른 서비스에 비해 요구하는 조건이 상대적으로 높아 시장에 진입하기에 어려운 것이 사실이다. 즉, 자본금 80억 이상 서비스 관련 전담 인력 8인 이상, 관련 설비의 별도 분리 운영 등을 요구하고 있으며, 주민번호 수집 시 법적 실효력을 갖는 환경 하에서 요구 조건과 대면확인에 준하는 수준의 본인식별이 필요하므로 일반 사업자들이 본인확인기관 신규 지정을 신청하지 않는 이유이기도 할 것이다. 이처럼 많은 사업자들이 본인확인기관 지정에 있어 그 관심이 낮아서 본인확인기관 지정기준 및 관리체계의 문제점을 인지하지 못하고 있으며, 이에 따른 개선방안에 대한 연구도 부족한 상황이다.

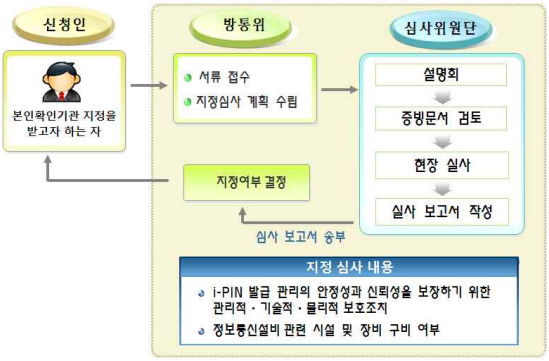
기존 주민번호 대체수단의 인증절차 개선방안 연구[16]에서는 아이핀과 휴대폰 기반의 본인확인서비스에서 주민번호 이외의 다른 식별수단 정보를 활용한 방안을 제시하였다. 현행 본인확인서비스의 주요한 문제는 과도하게 ISP들이 주민번호 대체수단 기반의 본인확인서비스를 적용하는 데 있고, 이로 인해 과도한 이용자의 개인정보, 특히 연계정보를 제공하는 데 있다. 연계정보는 온라인상에서 주민번호를 사용하여 이용자를 유일하게 식별할 수 있는 정보이다. 즉, 주민번호와 일대일 매칭 되는 88byte 크기로 일방향 암호화된 값이다. 일반적으로 사람의 인지능력으로 외울 수는 없지만, 시스템 간의 연동 과정에서 이용자를 고유하게 식별할 수 있는 정보로써 개인정보 침해에 대한 이슈가 발생할 수 있음을 피력하고 있다. 해당 연구에서는 이러한 주민번호 기반의 대체수단이 아닌 다양한 정보에 기반을 둔 대체수단 사용을 제시한 바 있다[4]. 휴대폰 기반의 본인확인서비스에 있어 이용자 인증을 위한 메커니즘을 제시한 연구[17]를 수행한 바 있다. 현행 휴대전화 문자 메시지 기반의 본인확인서비스의 경우 수신된 문자 메시지에 악의적인 행위를 유도하게 하는 링크를 삽입하여

개인정보 탈취 등을 시도하는 문제점이 존재한다. 이러한 문제점을 극복하기 위해 휴대폰 단말기 내부 보안영역에 저장되는 정보를 활용하여 안전한 사용자 인증 방안을 제시하였다.

그리고 현행 주민번호 기반의 본인확인제도에 대한 문제점들을 제시하고 이러한 문제점들을 해결하기 위해 주민번호의 근본적인 사용을 배제하는 방안을 법적으로 제도화하려는 연구가 수행되었다[18]. 이처럼 다양한 대체수단에 대한 개선 방안에 대해 연구를 진행한 바 있으나 실질적으로 본인확인기관 지정제도, 그리고 관리체계 개선을 위한 방안에 관해서는 연구를 수행한바가 없는 상황이다. 기존 연구들에서도 온라인 서비스에서 차등화된 본인확인서비스 적용 방안 연구[2, 11], 본인확인서비스에서 제공되는 개인정보의 이용자 동의 선택권 부여 연구[1], 본인확인통합인증센터 구축 방안 연구[19], 디지털 사용자 신원 확인 가이드 마련 연구[20], 대체수단의 안전성 강화 방안 연구[16], 본인인증 수단 및 절차 개선 방안 연구[3] 등이 수행되었다. 따라서 이미 수행한 기존 연구들과 달리 주민번호 대체수단 기반의 본인확인서비스의 안전성 강화와 이용자 개인정보에 대한 보안 강화를 위해 본인확인기관에 대한 현행화된 지정심사 기준의 개선이 필요하다. 이를 통해 과도하게 제공되는 이용자 개인정보에 대한 최소화와 법적 근거가 없는 마이핀 서비스를 점검하는 방안, 기준 고시에 대한 개선을 통한 본인확인서비스의 안전성 강화가 가능하다.

Ⅲ. 본인확인기관 지정 제도

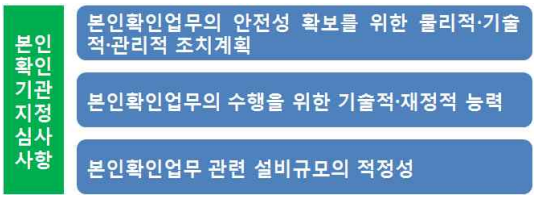
<그림 1>의 본인확인기관 지정 절차와 같이 신청자가 방통위에 신청서를 접수하고 외부평가위원회의 서면과 현장심사를 통해 보고서를 작성 한다. 이를 근거로 방통위가 지정여부에 대한 위원회 의결을 통해 지정서가 교부되는 절차를 수행하고 있다.



<그림 1> 본인확인기관 지정 절차

3.1 제도 현황

「정보통신망법」 제23조의3(본인확인기관의 지정 등), 제23조의4(본인확인업무의 정지 및 지정취소)에서 본인확인기관 지정 시 심사기준, 지정절차 및 휴지· 폐지 절차 등에 관한 사항을 규정하고 있다[21]. 지정 등에 관한 규정은 <그림 2>와 같이 「정보통신망법」 제23조의3(본인확인기관의 지정 등)에서 방통위는 다음 사항을 심사하여 대체수단의 개발 · 제공 · 관리 업무를 안전하고 신뢰성 있게 수행할 능력이 있다고 인정되는 자를 본인확인기관으로 지정할 수 있도록 정하고 있다. 그 사항에는 1. 본인확인업무의 안전성 확보를 위한 물리적 · 기술적 · 관리적 조치계획, 2. 본인확인업무의 수행을 위한 기술적 · 재정적 능력, 그리고 3. 본인확인업무 관련 설비 규모의 적정성을 정하고 있다. 추가적으로 본인확인기관이 본인확인업무의 전부 또는 일부를 휴지하고자 하는 때에는 휴지기간을 정하여 휴지하고자 하는 날의 30일 전까지 이를 이용자에게 통보하고 방통위에 신고함을 규정하고 있으며, 본인확인기관이 본인확인업무를 폐지하고자 하는 때에는 폐지하고자 하는 날의 60일 전까지 이를 이용자에게 통보하고 방통위에 신고하도록 정



<그림 2> 본인확인기관 지정심사 사항

하고 있다. 그 외 심사사항별 세부 심사기준·지정 절차 및 휴지·폐지 등에 관하여 필요한 사항은 대통령령으로 정하고 있다. 또한, 동 법에서는 본인확인업무의 정치 및 지정취소에 관한 규정을 마련하고 있다. 그리고 「본인확인 기관의 지정 및 관리에 관한 고시」에 본인확인기관의 대체수단 발급·관리 업무의 안전성과 신뢰성을 보장하기 위하여 본인확인기관의 지정에 관한 세부 심사기준 및 절차를 마련하고, 본인확인기관의 관리 등에 관한 사항을 규정하고 있다. 본인확인기관 지정심사를 위한 심사 진행을 위한 세부심사기준은 <표 4>와 같다.

3.2 제도의 문제점

본인확인기관 지정에 대한 사항은 「정보통신망법」에 규정하고 있는데 본인확인 업무의 특성 상 본인확인기관으로 지정 받을 수 있는 기관의 요건이 상당히 높은 수준에 해당한다. 하지만, 본인확인기관으로 지정받은 이후 관련 서비스의 변경이 발생할 경우 이를 신고하여 재검토 받을 수 있는 근거가 마련되어 있지 않다. 또한, 본인확인기관으로 지정받은 이후 해당 기관이 다른 본인확인기관과 양수 또는 합병 시 어떠한 절차를 거쳐야 하는지도 명확하지 않은 상황이다. 마지막으로 본인확인기관이 될 수 있는 기관의 범위가 불명확하다. 현행 규정에서는 본인확인기관 신규 지정을 위해서는 서류심사와 더불어 현장심사를 통해 본인확인서비스 이용자의 개인정보에 대한 기술적, 관리적, 물리적 보호조치 마련 여부를 심사하도록 정

<표 4> 본인확인기관 지정 세부 심사기준

구분	심사기준
물리적·기술적·관리적 조치계획	가. 본인확인업무 관련 설비의 관리 및 운영에 관한 사항
	나. 정보통신망 침해행위의 방지에 관한 사항
	다. 시스템 및 네트워크의 운영·보안 및 관리에 관한 사항
	라. 이용자 보호 및 불만처리에 관한 사항
	마. 긴급상황 및 비상상태의 대응에 관한 사항
	바. 본인확인업무를 위한 내부 규정의 수립 및 시행에 관한 사항
	사. 대체수단의 안전성 확보에 관한 사항
	아. 접속정보의 위조·변조 방지에 관한 사항
	자. 본인확인업무와 다른 인터넷 서비스와의 분리
기술적 능력	가. 기술인력 : 8명 이상 보유 나. 기술인력 요건 - 정보통신기사·정보처리기사 및 전자계산기조직응용기사 이상의 국가기술자격 또는 이와 동등 이상의 자격이 있다고 방송통신위원회가 인정하는 자격 - 정보보호 또는 정보통신운영·관리 분야에서 2년 이상 근무한 경력
재정적 능력	가. 자본금 : 80억원 이상 (국가기관 및 지방자치단체 제외)
설비규모의 적정성	가. 이용자의 개인정보를 검증·관리 및 보호하기 위한 설비 나. 대체수단을 생성·발급 및 관리하기 위한 설비 다. 출입통제 및 접근제한을 위한 보안설비 라. 시스템 및 네트워크의 보호설비 마. 화재·수해 및 정전 등 재난 방지를 위한 설비

하고 있다. 하지만, 신규 지정기관의 입장에서는 지정 여부와 관계없이 사전에 정보시스템을 구축하여 평가를 받은 것이 필요한 상황이다. 물론 사전에 관련 부처와 협의를 거쳐 사업 진행 여부를 타진한 뒤 지정신청을 요구하겠지만 법적인 사항을 본다면 지정신청 기관이 준비해야 할 사항을 명확히 제시하는 것이 요구된다. 그리고 본인확인기관 지정심사 기준 및 관련 고시 사항은 2012년 제정되어 현재까지도 개정이 이루어지고 있지 않는 상황이다. 지금까지 수차례 「정보통신망법」, 「개인정보보호법」 등의 관련 법령들이 개정됨에도 이를 고시 기준에 반영하지 못하고 있

다. 이로 인해 최신 법령들과의 준거성 여부 확인이 필요하고 이후 고시 기준에 누락되어 있는 사항들의 추가와 삭제, 그리고 심사사항별 세부 심사기준의 평가기준의 중복, 축소, 삽입 등의 과정을 통해 심사기준의 현행화, 최신화, 체계화를 꾀할 필요가 있다. 더구나 마이핀 서비스의 경우는「정보통신망법」상에 법적인 근거가 없다. 마이핀 서비스는 <표 5>와 같이 주민번호와 달리 마이핀은 나이, 성별 등 개인식별 정보가 포함되지 않은 발행년도, 발행기관코드 및 무작위 등의 13자리의 번호이며, 유·노출 등 특정한 경우 변경이 가능한 특징이 있다. 그러나 마이핀 서비스는 인지도가 낮아 활성화되지 않고 있으나 아직은 시장에서 미미하게 사용하고 있어 마이핀 서비스의 폐지 여부에 대한 검토가 요구된다.

<표 5> 주민등록번호, 아이핀 및 마이핀 비교

구분	주민번호	아이핀	마이핀
번호체계	생년월일, 성별 13숫자	기관코드, 난수	발행년도/기관, 검증코드
변경여부	매우 곤란	폐기 후 신규가입	변경가능
발급방법	주민센터	홈페이지, 주민센터	
이용영역	온/오프라인	온라인	오프라인
이용방법	주민번호	ID,비밀번호	마이핀
의무발급	의무	선택	선택

Ⅳ. 본인확인기관 제도 개선방안

현행「정보통신망법」및 동법 시행령,「본인확인기관 지정 등에 관한 기준」(방통위 고시)는 "본인확인서비스" 및 "본인확인기관 지정 심사기준" 등이 아이핀 서비스에만 한정하여 규정되어 있어 휴대전화, 신용카드, 그리고 전자서명 등 신규 대체수단을 포괄할 수 있는 지정심사 기준 마련이 필요하다. 이에 따라 관련 법률 및 시행령, 고시 내용을 검토하여 본인확인 업무가 아이핀 외 주민번호 대체수단들을 포함할 수 있도록 개선 방안 제시가 요구된다.

4.1「정보통신망법」의 개선방안

① 본인확인서비스 및 업무의 변경에 대한 개선: 방통위로부터 지정받은 본인확인기관이 새로운 주민번호 대체수단을 개발 혹은 도입하여 본인확인업무가 확대되거나 기존 본인확인 업무에 관련된 정보시스템, 설비 등에 변경이 생긴 경우에는 현행 본인확인서비스에 대한 적합성 여부 확인을 위한 재지정심사를 받거나 본인확인업무에 관한 변경 신고를 하는 등의 절차가 이행되어야 한다. 그러나 현행법에서는 이에 대한 관련 규정이 마련되어 있지 않아 향후 변경 발생 시 본인확인서비스에 대한 안전성을 확보하기 어려운 문제가 있다. 이에 대한 개선방안으로 본인확인기관 협의체와 전문가 의견 검토를 통해 서비스 변경에 따른 절차를 개정하도록 한다. 유사한 사례로「위치정보의 보호 및 이용 등에 관한 법률」[22] 제5조 제5조(위치정보사업의 허가 등) 제1항에 따라 위치정보사업의 허가를 받은 자(이하 "위치정보사업자"라 한다)가 허가를 받은 사항 중 위치정보시스템을 변경(그 변경으로 개인위치정보 보호를 위한 기술적 수준이 허가받은 때보다 저하되는 경우에 한한다)하려는 경우에는 대통령령으로 정하는 바에 따라 방송통신위원회의 변경허가를 받아야 하고, 상호 또는 주된 사무소의 소재지를 변경하려는 경우에는 방송통신위원회에 변경신고를 하도록 정하고 있다.

② 연계정보(CI)의 최초 저장 기준 마련: 본인확인기관이 아닌 자가 본인확인업무(대체수단의 개발·제공·관리 업무)를 수행하지 못하도록 규정하고 있으나 실제 ISP들은 본인확인 업무의 명확한 정의가 없어 다른 기관들에게 자신들이 보유하고 있는 본인확인에 필요한 식별정보인 CI를 제공하고 있는 상황이다. CI는 식 (1)과 같이 생성된다.

$$CI = HMAC_{sk}((RN \| Padding) \oplus S_A) \quad (1)$$

여기서, $H()$는 암호화 함수, RN은 주민번호, $Padding$은 정해진 자리 수를 만들기 위한 과정, S_A는 본인확인기관과 한국인터넷진흥원(KISA)이 공유하는 비밀정보, sk는 본인확인기관과 KISA가 공유하는 비밀키, 그리고 ||는 앞뒤를 연접하는 기호이다 [5]. 이처럼 CI 생성을 위해서는 주민번호를 보유하고 있는 본인확인기관이 생성하고 제공할 수 있으나 CI를 수신 받은 ISP가 다른 사업자들에게 연계목적으로 제공하는 경우가 발생한다. 이후 제공받은 CI를 정보를 제공받은 기관이 저장하여 이용자 식별 값으로 활용하고 있는 경우가 존재한다. 따라서 최초로 CI를 저장할 때는 본인확인기관으로부터 수집 받은 경우에 한함을 명시하고, 그 외 사항으로는 관련 법령에 따라 정당하게 수집한 경우로 한정시킬 필요가 있다.

③ 본인확인 업무의 양수 또는 합병 시 개선: 본인확인기관이 다른 본인확인기관의 본인확인 업무를 양수하거나 다른 본인확인기관인 법인을 합병하고자 하는 경우에 대한 관련 절차가 마련되어 있지 않다. 물론 본인확인기관의 지정받은 법인이 더 이상 서비스 유지가 어려울 경우는 휴지·폐지 절차에 따라 서비스를 중단할 수 있다. 그러나 그 중단에 따른 피해는 고스란히 이용자들에게 전가되는 문제가 있다. 예를 들어 특정 아이핀 기관이 본인확인 업무의 중단 시 서비스에 가입 이용자는 더 이상 해당 기관의 서비스를 받지 못하고 다른 아이핀 기관에 새롭게 가입해야 하는 문제가 있다. 사실 현재도 아이핀 기관 간의 정보 연동을 통해 아이핀 ID만으로 어떤 본인확인기관 가입자인지 식별할 수 있으며 다른 아이핀 기관의 인증모듈을 통해 전달받은 아이핀 이용자의 정보를 전달받아 본인확인 처리 후 해당 결과를 전달해주는 구조로 서비스를 연계하고 있어 실질적으로 특정 아이핀 기관이 폐지 시 이용자의 정보도 함께 폐지하는 것이 옳은 것인가는 다시금 생각해 볼 필요가 있다. 만약 이용자의 개인정보 제공 동의 등을 통해 해당 서비스에 차질이 없이 연계될 수 있다면 이용자의 불편을 최소화 할 수 있을 것이다. 휴대폰 기반 본인확인서비스 역시도 해당 이동통신사가 본인확인 업무의 중단을 결정하였을 경우 해당 이용자는 더 이상 휴대폰을 통한 본인확인서비스를 받지 못하는 문제가 있다. 따라서 본인확인기관이 아닌 사업자가 본인확인 업무를 양수하거나 법인인 본인확인기관을 합병하고자 하는 경우 이를 관리·감독하고 해당 본인확인기관의 법적 지위를 승계하도록 하는 규정 마련이 필요하다. 이처럼 본인확인기관의 지위를 승계한 경우 재지정심사를 진행할 것인지 혹은 기술적·물리적·관리적 조치는 변동 없이 법인만 변경될 경우 이를 어떻게 처리할 것인가에 관한 규정 마련이 요구된다.

④ 마이핀 서비스에 대한 법적 근거 마련: 마이핀 서비스가 비록 활성화되지는 못하였으나 현재는 주무 부처인 행정안전부의 관리가 전무한 상황이다. 마이핀 서비스는 주민번호와 1:1로 매칭 되는 테이블을 관리하고 있어야 하여 관리 과정에서의 엄격한 기준 제시가 필요하다. 하지만, 현재 방통위 역시 마이핀 발급기관인 아이핀 기관 점검 시에 마이핀 서비스에 대한 법적 근거가 없어 사후관리 시 점검을 이행하고 있지 않는 상황이다. 따라서, 법적 기준을 마련하여 심사를 진행하는 것보다는 서비스의 활용도가 낮아 마이핀 서비스의 폐지를 검토하는 것이 타당할 것이다.

4.2 「본인확인기관 지정 등에 관한 기준」의 개선방안

ISP들이 온라인상에서 이용자를 식별하기 위해 주민번호 대신에 CI를 과도하게 이용하고 있으나, CI에 대한 안전한 제공에 대한 기준이 미비한 실정이다. 따라서 본인확인기관 지정 고시 상에 본인확인기관

의 의무에 있어 CI 제공에 신중을 기할 수 있는 방안 마련이 필요하다. 우선 CI 정의를 명확히 하고 이를 근거로 최소 제공 원칙을 수립하는 것이 필요하다. 그리고 본인확인기관 운영업무에 대한 원칙을 명확히 하는 것이 필요하다. 안전하고 신뢰성 있는 본인확인 업무 이행을 고시 상에 규정하고 이를 준수하기 위한 일련의 보호조치 과정을 본인확인기관에게 요구하는 것이 필요할 것이다. <표 6>에서는 고시 상의 현행 심사기준과 개선안을 비교한 것이다.

① 심사 범위 설정: 본인확인기관으로 지정을 받고자 하는 기관은 일정 이상의 정보시스템을 보유하고 있는 기관이며 일정 규모(자본금 80억 이상) 이어야 가능하다. 따라서 본인확인기관 지정신청을 위해서는 사전에 본인확인서비스가 가능함을 제시하기 위해 서면뿐만 아니라 현장 확인을 통해 정보시스템 운영 현황도 확인할 필요가 있다. 고시상의 심사 방법 역시도 서면 심사와 현장 심사를 이행할 수 있도록 정하고 있다. 다만, 신청기관의 규모나 서면 신청서에 대한 사실 확인 등을 위해 사전에 점검을 통해 심사 진행 여부를 파악할 필요가 있으나 현행 고시 상에서는 사전심사에 대한 조항이 포함되어 있지 않아 제출한 서류만으로 사실 여부를 확인하는데 그치고 있다. 특히, 본인확인기관으로 지정받고자 할 시에는 본인확인 업무 관련 시설과 장비의 보유를 명기하고 실제 해당 장비의 보유 여부를 확인하기 위해서는 심사 이전에 사실 여부를 확인하는 과정을 거침으로써 지정심사에 있어 불필요한 행정력, 예산 낭비 등을 줄이는 과정이 요구된다. 추가적으로 제8조(심사방법)에는 서류심사와 현장실사로 구분하여 실시하도록 정하고 있다. 이처럼 서류심사와 현장실사에 대한 일정을 지정심사 계획수립에 반영될 수 있도록 구분하는 것이 필요하다. 고시 제2절에 존재하는 지정심사 기준 및 방법에 있어 제6조(심사기준)에는 본인확인서비스의 안전성과 신뢰성을 보장을 위한 보호조치와 정보통신설비 관련 시설 및 장비를 대상으로 정하고 있다. 기존의 아이핀 기관의 경우는 아이핀 자체가 대체수단으로 활용되고 다른 용도로는 사용되지 않기 때문에 아이핀 서비스에 관련된 전체 정보시스템 및 설비가 지정심사 범위에 포함시킬 수 있다. 그러나 휴대폰, 신용카드 등 그 자체만으로 본인확인 대체수단이면서 고유의 용도를 가지고 있어 이 고유 용도에 해당하는 설비까지 지정심사에 포함 할 것인가를 검토해야 한다. 심사사항별 세부심사기준의 평가기준 상에서도 본인확인업무 관련 설비의 관리 및 운영에 관한 사항을 점검하도록 정하고 있어 실제 본인

<표 6> 고시 상의 심사기준 개선안

현 행	개선안
제6조(심사기준) ①지정심사는 본인확인서비스의 안전성과 신뢰성을 보장하기 위한 물리적·기술적·관리적 보호조치와 정보통신설비 관련 시설 및 장비를 대상으로 한다. ②영 제9조의3제2항에 따른 심사사항별 세부심사기준의 평가기준은 별표 2와 같다.	제6조(심사기준) ①지정심사는 본인확인서비스의 안전성과 신뢰성을 보장하기 위한 물리적·기술적·관리적 보호조치와 정보통신설비 관련 시설 및 장비를 대상으로 한다. ②영 제9조의3제2항에 따른 심사사항별 세부심사기준의 평가기준은 별표 2와 같다. ③영 제9조의3제2항에 따른 심사사항별 세부심사기준의 평가기준을 적용하는 대상은 별표 3과 같다.
	[별표 3] 심사사항별 세부심사기준의 평가기준 적용 대상 -본인확인 정보시스템 : 서버, DB, PC 등 단말기, 개발장비, 모바일장비, 상담처리장비, 보조저장매체, 네트워크 장비, 응용 프로그램 등 정보의 수집, 가공, 저장, 검색, 송수신에 필요한 하드웨어 및 소프트웨어 -본인확인 정보보호시스템 : 정보의 훼손, 변조, 유출 등을 방지하기 위하여 구축된 시스템으로 침입차단시스템, 침입탐지시스템, 침입방지시스템, 개인정보유출방지시스템 등을 포함 -정보 : 문서적 정보와 전자적 정보 모두를 포함 -인력: 해당 업무를 수행하는 인력 등

확인업무의 범위 설정이 모호하여 매년 이행하는 사후관리심사에서 심사자 및 기관 담당자들의 혼선을 발생하고 있다. 가장 효율적인 방안은 대체수단별 협의체를 통해 각 대체수단별 본인확인설비의 범위를 선정하는 것이 필요하다. 선정 후 이에 대한 타당성 검토를 외부 전문가들의 검토를 거쳐 확정하고 이를 본인확인기관에게 안내함으로써 향후 발생할 수 있는 범위 설정의 오해로 인한 불필요한 낭비를 줄일 수 있을 것이다.

② 심사결과 통보일 변경에 대한 개선: <표 7?과 같이 지정심사 결과에 대한 통보 일정도 지정신청일이 아니 심사종료 일정으로 기준을 정하는 것이 필요하다. 심사결과일 통보를 지정서 접수 일정이 아닌 지정심사일 혹은 지정심사 종료일 혹은 보완사항 공식 통보일로부터 90일 이내로 개선하는 것이 필요하다.

<표 7> 고시 상의 심사결과 통보일 개선안

현 행	개선안
제10조(심사결과 통보) ②방송통신위원회는 지정신청일로부터 90일 이내에 심사결과를 지정신청기관에게 통지하여야 한다. 다만, 부득이한 사유가 있을 때에는 그 사유를 알리고 30일의 범위 내에서 그 기한을 연기할 수 있다.	제10조(심사결과 통보) ②방송통신위원회는 지정심사 시작일 혹은 적합성 심사 시작일로부터 90일 이내에 심사결과를 지정신청기관에게 통지하여야 한다. 다만, 부득이한 사유가 있을 때에는 그 사유를 알리고 30일의 범위 내에서 그 기한을 연기할 수 있다.

③ 사후관리에 대한 기준 설정 개선: <표 8>과 같이 본인확인기관 지정 이후 사후관리 주기를 명기하고 있지 않아 사후관리 이행에 대한 명확한 주기 설정이 필요하다. 정보보호 관리체계와 개인정보보호 관리체계 인증과 같이 「정보통신망법」 제47조(정보보호 관리체계의 인증)에서 정보보호 관리체계의 실효성 제고를 위하여 연 1회 이상 사후관리를 실시하고 그 결과를 통보하도록 정하고 있다[8]. 고시 상에서도 제12조(사후관리)의 조항을 통해 근거를 마련하고 있으나 시행 주기를 명기하고 있지 않아 명확한 주기 설정이 요구된다. 또한, 해당 조항이 강제조항이 아니라 선택조항으로 규정되어 있어 본인확인서비스 이용자의 신뢰도 확보와 본인확인기관의 심사사항별 평가기준의 적합성 확인과 관리체계의 실효성 제고를 위해 강제화 할 필요가 있다. 추가적으로 심사기준에 있어 현재 아이핀과 휴대폰번호 기반의 본인확인기관의 경우는 과학기술정보통신부로부터 본인확인설비에 대해 국가기반시설로 지정되어 매년 취약성 진단 및 보안조치 이행 여부를 점검 받고 있는 상황이다. 또한 본인확인기관의 평가기준 사항에도 본인확인설비에 대한 취약점 진단 이행여부가 존재하여 이중으로 취약점을 진단하는 결과를 초래하고 있다. 따라서 만약 기반시설로 지정된 본인확인설비에 대한 취약점 진단 이행을 기반시설 점검으로 갈음할 수 있는 조항의 신설이 필요하다. 다만, 지정심사 시에는 전체 본인확인 설비에 대한 점검 진행이 필요하고 사후관리 시 이를 갈음할 수 있는 방안 제시가 요구된다.

<표 8> 고시 상의 사후관리기준 개선안

현 행	개선안
제12조(사후관리) 방송통신위원회는 본인확인업무의 적정한 추진과 영 제9조의3의 심사사항별 세부 심사기준에 적합한지 여부를 확인하기 위하여 지정을 받은 기관에 대해 관련 자료의 제출을 요구하거나 현장실사를 할 수 있다.	제12조(적합성 심사) ①방송통신위원회는 본인확인업무의 적정한 추진과 영 제9조의3의 심사사항별 세부 심사기준에 적합한지 여부를 확인하기 위하여 지정을 받은 기관에 대해 연 1회 이상 관련 자료의 제출을 요구하거나 현장실사를 진행한다. ②지정받은 기관의 본인확인업무 시스템이 국가기반시설로 지정되어 별도의 보안점검을 받은 경우는 영 제9조의3의 심사사항별 세부 심사기준 상의 일부 평가기준에 대한 적합성 심사하지 않을 수 있다.

④ 본인확인 업무의 안전성 및 신뢰성 확보를 위한

방안 마련: 본인확인기관 지정 등에 관한 기준의 목적에 본인확인 업무의 안전성과 신뢰성을 확보를 위한 목적이 추가됨에 따라 이해 대한 조항의 삽입이 필요하다. 또한 현행 본인확인기관이 지정심사 이후 설비의 변경이 발생하더라도 별도의 신고 절차가 존재하지 않아 사후관리심사까지 현장을 방문하지 않고서는 설비의 변경 등을 확인할 방안이 존재하지 않는다. 따라서 설비 등의 변경 발생 시 방송통신위원회에 신고하여 검사할 수 있는 방안의 마련이 필요하다. 추가적으로 본인확인 업무의 안전성과 신뢰성 확보를 위해 배상책임 보험에 가입하도록 제도화하는 것이 필요하다. 본인확인서비스의 다양한 활용으로 인해 본인확인 업무의 오류로 인해 그 피해를 이용자에게 돌아갈 수 있어 이에 대한 물질적 보상 방안을 본인확인기관들에게 강구하도록 하는 방안 마련이 필요하다. 본인확인설비의 장애 발생 시 신속한 대처와 방송통신위원회에 적절한 대응을 위해 신고하는 절차 마련이 요구된다.

V. 결 론

본 논문에서는 본인확인기관 지정제도의 개선방안을 제안하였다. 온라인상에서 주민번호 대체수단 기반의 본인확인서비스의 적용으로 이용자 개인정보가 과도하게 ISP들에게 제공되고 있는 상황이다. 최근에는 다양한 본인인증서비스들이 출현하고 있으며 이들이 본인확인기관으로 지정신청 시 적절하게 검증하기 위한 심사기준 현행화가 필요하다. 더구나 본인확인기관은 명확하게 온라인 이용자를 식별하고 인증하는 과정이 요구된다. 또한, ISP들이 요구하는 본인확인서비스가 정당한 요구인지도 검증하는 과정이 요구된다. 이를 위해 본인확인기관 지정에 대한 명확한 기준 개선과 본인확인서비스 수행 시 보다 안전하고 책임감 있는 업무 수행이 요구된다. 따라서 본 논문에서는 본인확인기관 지정심사 기준에 대한 문제점을 파악하고 해당 문제점을 개선하기 위한 방안들을 제시함으로써 보다 신뢰성 있으며 안전한 본인확인서비스가 수행될 수 있다.

참고문헌

[1] 김종배, “온라인에서 주민등록번호 대체수단 기반의 본인확인서비스의 개선 방안 연구,” 디지털산업정보학회논문지, 제15권, 제2호, 2019, pp.29-42.

[2] 김종배, “온라인 서비스의 본인확인 요구사항 분석 기반의 차등화된 본인확인서비스 적용 방안,” 인터넷방송통신학회, 제20권, 제2호, 2020. pp.201-208.

[3] 김종배, “아이핀 기반 본인확인서비스의 안전성 강화 방안,” 한국IT서비스학회논문지, 제16권, 제2호, 2017, pp.97-110.

[4] 신영진, “우리나라 본인확인수단의 개선방안 연구: 전문가의 진단과 개선방향 제언을 중심으로,” 한국지역정보화학회지, 제20권, 제4호, 2017, pp.145-179.

[5] 김종배 · 전동호 · 박기홍 · 이재호 · 최중석, 주민번호 대체수단 정책 개발을 위한 현황 조사 및 개선방안, 한국인터넷진흥원 연구보고서, 2017.

[6] 유미영 · 이재형 · 강민구, “One ID 본인인증과 FIDO2.0 거래인증 활용,” 한국인터넷정보학회논문지, 제 20권, 제1호, 2019, pp.23-29.

[7] 신영진, “본인확인수단의 개선에 따른 개인정보보호에 관한 연구: 이용자 대상의 주민번호 대체수단을 중심으로,” 한국지역정보화학회지, 제20권, 제2호, 2017, pp.1-24.

[8] 방송통신위원회, 본인확인기관 지정 등에 관한 기준 고시, http://www.law.go.kr/행정규칙/본인확인기관지정등에관한기준

[9] 장인용 · 염흥열, “인터넷상의 본인확인수단인 아

이핀의 활성화 방안 연구," 정보보호학회논문지, 제19권, 제5호, 2009, pp.81-94.

[10[최광희 · 정승욱 · 이강신 · 안승호, "국가 IDM을 위한 아이핀 발전 전략," 정보보호학회논문지, 제21권, 제4호, 2011, pp.40-46.

[11] 염흥렬, "아이핀 보증 등급에 기반한 보증모델," 한국디지털정책학회, 제14권, 제9호, 2016, pp.287-299.

[12] 이영교 · 안정희, "아이핀 대량 부정발급 사고에 대한 개선방안 연구," 디지털산업정보학회, 제11권, 제2호, 2015, pp.11-22.

[13] 이형효, "개인정보보호를 위한 주민등록번호 대체수단 및 관리체계," 한국정보기술학회논문지, 제8권, 제 6호, 2010, pp.49-58.

[14] 최학규 · 김황래, "스미싱 예방을 위한 악성문자훈련시스템 설계 및 구현," 한국정보기술학회논문지, 제 17권, 제10호, 2019, pp.93-99.

[15] 박효민 · 김완석 · 강소정 · 신상욱, "스미싱 공격 방지를 위한 클라우드 메시징 서비스," 디지털융복합연구, 제15권, 제4호, 2017, pp.285-293.

[16] 신영진, 주민번호 대체수단 연구 및 인증절차개선방안 조사, 한국인터넷진흥원 용역과제, 2015.

[17] 정필성, "스마트폰을 이용한 사용자 인증 메커니즘," 한국정보통신학회논문지, 제21권, 제2호, 2017, pp.301-308.

[18] 성준호, "주민등록번호에 의존한 본인확인제도의 문제점," 한국사회학회, 제6권, 제2호, 2016, pp.208-246.

[19] J. B. Kim, "A method to establish a personal identification and authentication integrated center based on the alternative means of resident registration number," Proceedings of Conference on information and Control Systems IEEK., 2019, pp.212-213.

[20] J. B. Kim, "A Study on Digital Identity Guidelines of NIST," Proceedings of Korea Information Processing Society, 2019, pp.160-163.

[21] http://www.law.go.kr/r/법령/정보통신망 이용촉진 및 정보보호 등에 관한 법률

[22] http://www.law.go.kr/r/법령/위치정보의 보호 및 이용 등에 관한 법률

■ 저자소개 ■

김 종 배
(Kim Jong Bae)

2019년 3월~현재
세종사이버대학교
소프트웨어공학과 부교수
2006년 6월~2019년 2월
서울디지털대학교 컴퓨터공학과
교수
2004년 8월 경북대학교 컴퓨터공학과
(공학박사)
2002년 2월 경북대학교 컴퓨터공학과
(공학석사)
2000년 2월 부산대학교 컴퓨터공학과 (공학사)

관심분야 : 온라인서비스, 개인정보보호,
인공지능
E-mail : kjblove@hotmail.com

논문접수일 : 2020년 7월 27일
수 정 일 : 2020년 8월 5일
게재확정일 : 2020년 8월 20일