디지털산업정보학회 논문지 제15권 제2호-2019년 6월
http://dx.doi.org/10.17662/ksdim.2019.15.2.029

온라인에서 주민등록번호 대체수단 기반의 본인확인서비스의 개선 방안 연구*

김 종 배**

A Study on Improvement of Personal Identity Proofing Service(PIPS) Based on Alternative Methods of Resident Registration Number

Kim Jongbae

〈Abstract〉

As online services become more and more popular due to the development of IT, non-face-to-face transactions are continuously increasing rather than face-to-face transactions. The personal identity proofing service(PIPS) based on the alternative method of the resident registration number is used for the purpose of confirming the identity of the other party on the Internet. However, in the case of the current PIPS, the personal information of the PIPS user is excessively provided to the online service provider. As a result, privacy problems of online users, shortage of choice of information providing options, and lack of differentiation of authentication methods are becoming problems. Therefore, this paper proposes a method to improve the PIPS based on the current resident registration number alternative method and to provide a method to differentiate the provision of excessive personal information. In the proposed method, we analyze trends and current status of overseas online PIPS in order to provide a method of providing differentiation of personal information and proposes an effective improvement method applicable to domestic.

Key Words : Personal Identity Proofing Service, Assurance Level, Alternative Means of Resident Registration Number Service, Connecting Information

Ⅰ. 서론

급속한 IT기술의 발전에 따라 비대면을 통한 상거래의 활성화로 인해 온라인상에서 개인을 식별하기 위한 수단의 필요성이 날로 증가되고 있다. 온라인상에서 상대방의 신원을 확인하기 위해 국내에서는 다양한 본인확인 및 인증 서비스가 등장하고 있다[1-6, 27]. 본인인증에서 인증이란 「전자서명법」에 따르면 "전자서명생성정보가 가입자에게 유일하게 속한다는 사실을 확인하고 이를 증명하는 행위"라고 정의하고 있다[7, 23]. 그리고 본인확인이란 「본인확인기관 지정 등에 관한 기준」에 따르면 "본인확인기관

* 본 논문은 한국인터넷진흥원의 "본인확인기관 지정기준 및 관리체계 개선방안 마련" 연구사업(2018)의 결과를 재정리하였으며 동 연구사업과 "교과부 일반연구자원사업"의 지원을 받아서 수행되었음. (NRF- 2016R1D1A1B03931986)
** 세종사이버대학교 컴퓨터소프트웨어학과 부교수

이 부여한 이용자 본인확인정보(아이핀, 휴대폰, 신용카드, 공인인증서)를 사용하여 해당 이용자가 본인인지 아닌지를 식별하고 제 3자에게 인증해 주는 것"으로 정의하고 있다[8]. 국내에서는 다양한 본인인증서비스가 활용되고 있으며 온라인 서비스 제공 사업자들이 보유한 이용자의 행태정보, 가입 시 수집 받은 정보, 제3자로부터 전달받은 연계정보 등을 활용하여 온라인 서비스 이용자에게 본인인지 증명하도록 요구하고 있다. 온라인 서비스 제공자 사업자들이 서비스 이용자를 가장 명확하게 식별할 수 있는 식별수단으로써는 주민등록번호의 사용으로 명확히 식별할 수 있으나 2012년부터 주민등록번호 저장 및 수집을 원칙적으로 금지하고 있어 새로운 이용자 식별 수단이 필요하게 되었다[9, 10]. 주민등록번호 기반의 서비스 이용자 식별체계를 금지함에 따라 그동안 행정편의성과 신속한 서비스 제공 등 다양한 순기능도 존재하지만 무분별한 이용자의 고유식별정보인 주민등록번호를 오·남용함으로 인해 개인정보 침해사고 발생으로 금전적인 피해, 사생활 침해 등 사회적인 역기능이 확대되고 이는 결국 온라인 서비스 시장의 축소라는 문제점을 개선하는 효과가 있게 되었다[11-13, 28]. 하지만, 여전히 온라인 서비스 제공을 위해 이용자를 식별하는 수단이 필요하게 되었다. 주민등록번호를 대체하여 이용자를 식별하기 위해 주민등록번호를 사용하지 아니하고 이용자가 본인임을 확인하는 서비스인 본인확인서비스를 방송통신위원회가 개발하여 보급하고 있다. 이를 통해 주민등록번호 도용요인을 제거하고 이용자의 개인정보 자기결정권을 보장하며, 개인정보와의 연계 최소화가 될 수 있는 전기가 마련되었다. 현재 본인확인기관으로 지정된 곳은 2009년 아이핀 3개 기관, 2012년 이동통신 3사, 2017-8년에서는 신용카드 8개사까지 주민등록번호를 대체하는 본인확인 수단을 서비스하는 본인확인기관으로 지정하였다. 본인확인기관은 이용자가 자신의 신원정보를 신뢰할 수 있는 기관(본인확인기관)에게 제공하여 본인임을 확인한 뒤 본인확인기관으로부터 발급 받은 본인확인정보를 사용하여 인터넷 사이트 회원가입이나 성인인증 등을 이용할 수 있도록 본인확인서비스를 제공하고 있다[3, 14, 15]. <표 1>은 주민등록번호 대체수단을 통한 본인확인서비스 현황을 나타낸 것이다.

<표 1> 주민번호 대체수단 현황

구분	주민번호 대체수단			
대체수단	I-PIN	범용공인인증서	휴대전화	신용카드
가입자수	430만명	370만명	5,500만명	3,500만명
인증방식	IP+PW	비밀번호	생년월일, 성명,휴대전화 등	신용카드번호+비밀번호, ARS,ID/PW
기관수	3	5	3	8
식별정보	연계정보(Connecting Information: CI), 중복가입확인정보(Duplicated joining verification Information: DI)			
기타	I-PIN 가입자	범용공인인증서 발급자	본인명의 휴대전화 소유자	신용카드 발급자

이처럼 다양한 본인확인서비스 기관의 등장으로 온라인 서비스를 제공하는 사업자들은 주민등록번호 수집 금지에 따라 회원가입, 서비스 제공 등 다양한 목적으로 주민번호 대체수단 기반의 본인확인서비스를 적용하여 이용자들에 서비스 이용을 요구하고 있는 상황이다. 하지만, 현행 본인확인서비스의 경우 서비스 이용자의 개인정보를 이용자 선택권 없이 과도하게 온라인 사업자들에게 제공하고 있으며 불필요한 본인확인서비스 적용으로 온라인 서비스 비용 증가와 개인정보 침해 이슈도 부각되고 있는 상황이다. 따라서 본 논문에서는 현행 본인확인서비스의 동향을 분석하여 대체수단별 사용 현황을 분석하고 국외 온라인 본인확인서비스의 사용 현황에 대해 분석한

다. 그리고 현행 본인확인서비스에서 과도하게 제공하고 있는 서비스 이용자의 개인정보를 차등화하여 제공하는 방안을 제안한다. 제안한 방안은 실제 현행 본인확인서비스 시 사용자 식별에 사용하는 다양한 인증수단의 인증 강도에 따라 본인확인기관에 제공하는 개인정보를 차등화하여 제공하는 방안이다. 또한 온라인 서비스 사업자가 필요로 하는 개인정보만은 선별적으로 본인확인기관이 제공하는 방안, 그리고 본인확인서비스 이용자가 스스로 제공되는 개인정보에 대한 자기 선택권을 보장하여 본인이 직접 제공하는 정보에 대한 선택하게 함으로서 최소화된 개인정보의 제공 방안 등을 본 연구에서 제안하였다. 제안한 방안을 통해 현행 본인확인서비스의 안전성 확보뿐만 아니라 서비스 활성화로 서비스 이용자의 개인정보보호에도 효과적인 방안임을 제시한다.

본 논문의 구성은 Ⅱ장에서는 관련연구들에 대해 제시하고, Ⅲ장에서 본인확인서비스의 개요와 문제점들에 대해 소개하고, Ⅳ장에서는 국내·외 본인확인서비스 동향에 대해 소개한다. 그리고 Ⅴ과 Ⅵ장에서는 현행 본인확인서비스의 개선방안과 효과를 제시하고, 마지막 Ⅶ장에서는 결론을 맺는다.

Ⅱ. 관련연구

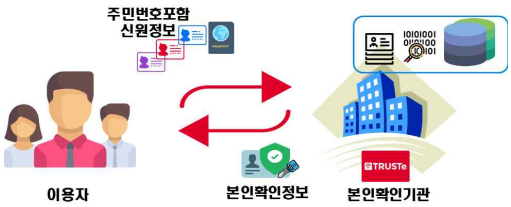
현재 대부분의 온라인 서비스 제공 사업자들은 서비스 이용자들을 식별하거나 관련 법령의 준수를 위해 주민등록번호 대체수단 기반의 본인확인서비스를 이용하고 있는 상황이다[16]. 청소년 여부, 성인 인증, 법정 대리인의 동의 등 관련 법적 구속력을 확보하기 위해 방송통신위원회가 지정한 본인확인서비스를 회원가입, 이용자 식별, 개인정보 변경, 결제, 배송 등에서 적용하고 있다. 이러한 이유는 현행 본인확인서비스를 통해 이용자가 본인임을 본인확인기관으로부터 식별 및 인증을 받으면 본인확인기관은 온라인 서비스 사업자에게 서비스 이용자를 식별할 수 있는 다양한 개인정보들을 제공하고 있다. 제공하는 이용자 개인정보들에는 주민등록번호에 상응하는 정보들로써 이를 활용함으로써 온라인 사업자들은 명확하게 온라인 서비스 이용자들을 식별할 수 있게 되었다. 그러나 현재 주민등록번호 대체수단을 이용한 본인확인서비스 이용자가 2017년에 한 해 동안 약 12억 건 이상 본인확인서비스를 이용하고 있어 1인당 평균 년 20회 이상의 본인확인서비스를 이용하고 있다[14, 17]. 이것은 무분별하게 본인확인서비스를 온라인 서비스 사업자가 적용하고 있는데서 기인한 것으로 볼 수 있다. 결국 본인확인서비스를 통해 서비스 이용자의 개인정보가 과도하게 온라인 사업자들에게 제공되고 있어 과거 주민등록번호 제공으로 발생한 사회적 역기능에 못지않아 서비스 이용자의 사생활 침해 등과 같은 문제가 대두될 수 있다. 또한 제공받은 개인정보의 파기나 오·남용으로 인한 문제, 마케팅 등의 활용으로 개인정보의 수집 목적 이외의 이용 등도 문제점으로 볼 수 있다. 지금까지 이러한 문제점들을 해결하기 위해 다양한 시도가 있었으나 실제 그 노력은 주민등록번호 대체수단 기반의 본인확인서비스의 안전성 확보에만 그치고 있는 상황이다[1, 13, 15, 18]. 그동안 주민등록번호 수집 금지에 따라 온라인 사업자들은 서비스 이용자를 식별하기 위해 본인확인서비스를 통해 이용자의 개인정보 수집으로 이용자를 식별하는데 집중하고 있으며 본인확인서비스의 안전성 확보를 통해 온라인 서비스의 활성화를 꾀하고 있는 상황이다. 이러한 이유는 신용카드사, 이동통신사, 온라인쇼핑몰 등의 개인정보 유출사고, 그리고 공공아이핀의 부정발급 등에 기인하여 안전한 본인확인서비스의 이용에 중점을 맞추어 서비스를 활성화하고 있는 상황이다. 특히 공공아이핀의 부정발급[15]은 아이핀에 대한 신뢰도가 매우 낮아 졌으며 해킹 사고 이후 아이핀 탈퇴자가 일일 평균 1,000여명을 넘는 반응을 보였으며 이로 인해 2018년 10월자 기준으로 더 이상 공공아이

핀의 신규가입은 불가능하며, 온라인에서 발급 받은 공공아이핀은 2019년 10월까지, 주민센터에서 발급받은 아이핀은 2021년 10월까지 사용가능하고, 2021년 이후부터는 공공아이핀의 폐지를 실시하고 기존 가입자와 서비스 제공 기관들은 민간아이핀 기관으로 전환함을 발표하였다[14]. 이처럼 2015년에 발생한 공공아이핀의 대한 부정발급 이후 아이핀 등 현행 주민등록번호 대체수단 기반의 본인확인서비스의 필요성이 감소하는 의견을 피력하였으며, 전반적으로 본인확인서비스의 안전성이 부족하다는 의견을 제시하였다[15]. 하지만, 본인확인서비스의 안전성 확보도 중요하지만 현행 본인확인서비스를 통해 과도한 서비스 이용자의 개인정보 제공으로 인한 사회적 문제도 다시금 살펴볼 필요가 있다.

Ⅲ. 본인확인서비스 개요

3.1 본인확인의 정의

본인확인은 특정한 방법을 사용하여 해당 사람이 본인인지 아닌지를 식별하고 제3자가 해당 사람이 그 사람이 맞는다고 인증해 주는 것을 말한다. 특정한 방법은 본인확인기관에 따라 본인확인을 위한 수단이 상이하다. 즉, 아이핀 기반의 본인확인서비스인 경우는 아이핀 아이디와 패스워드, 휴대폰 기반은 휴대폰과 문자메시지 인증번호, 그리고 신용카드 기반은 신용카드 번호와 결제 비밀번호가 본인임을 식별하는 정보에 해당한다. 각각의 본인확인서비스 방법에 따라서 2차 패스워드, 간편인증(지문, 얼굴, 홍채 등), ARS, 홈페이지 로그인 인증 등으로 구분할 수 있다. 본인확인기관이 서비스 이용자를 식별하고 인증하기 위해 본인확인정보(아이핀 아이디, 휴대폰번호, 신용카드 번호 등)를 부여하게 되고 이것을 활용하여 이용자들이 온라인 서비스에서 본인임을 확인받기 위해 사용하고 있다. <그림 1>과 같이 본인확인을 위해 이용자가 자신의 고유식별정보(주민등록번호, 외국인등록번호 등)와 신원정보(이름, 이메일, 휴대폰 번호 등)를 본인확인기관에게 제공하고 본인확인기관을 제공받은 이용자의 개인정보를 바탕으로 허무인(사망자, 국적 상실자 등) 여부 등을 검증하여 본인확인정보를 발급한다.

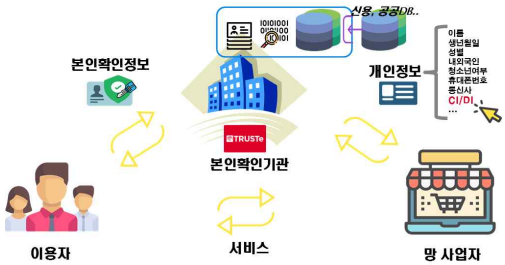


<그림 1> 본인확인 개요도

3.2 본인확인서비스

<그림 1>과 같이 본인확인기관으로부터 본인확인을 위한 식별정보를 부여받은 이용자가 온라인 서비스를 이용하기 위해 온라인 사업자들이 본인확인을 요구하는 경우 이용자가 발급받은 본인확인정보를 사용하여 본인확인기관에게 제공하여 본임임을 식별 및 인증을 받는 과정이 본인확인서비스이다. <그림 2>는 본인확인서비스의 개요도를 나타낸 그림이다. 이용자가 온라인 서비스 사업자로부터 서비스를 제공받기 위해 서비스 요청 시 온라인 사업자는 이용자에게 본인확인을 요구하고 이용자는 본인확인기관으로부터 본인확인을 식별 및 인증 받은 후 본인확인기관은 이용자로부터 가입 시 전달받은 개인정보와 이용자를 식별할 수 있는 특정 개인정보(연계정보, Connecting Information: CI, 중복가입확인정보, Duplicated joining verification Information: DI)를 망사업자에게 제공한다. <그림 2>에서와 같이 본인확인기관은 본인확인서비스를 요청한 망사업자에 본인확인정보를 통해 식별 및 인증한 이용자의 개인정보를 제공하고 있

다. 결국 이용자는 자신의 주민등록번호를 대체하는 대체수단을 본인확인기관으로부터 발급 받아 대체수단을 통해 본인임을 식별하고 인증과정을 통해 본인임을 입증하게 되는 것이 본인확인서비스라고 할 수 있다. 이러한 본인확인서비스를 통해 본인확인기관을 이용자의 개인정보를 망사업자들에게 제공하고 있다. 제공하는 개인정보들은 <표 2>와 같다.

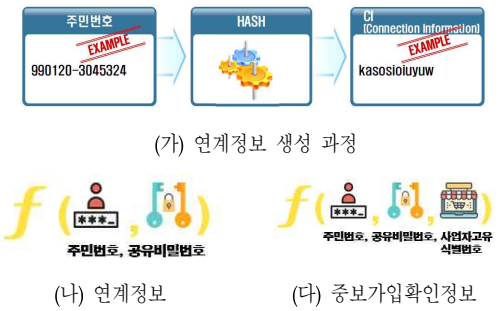


<그림 2> 주민번호 대체수단 기반의 본인확인서비스 개요도

<표 2> 본인확인기관에 의해 제공되는 개인정보의 항목 현황

제공 정보	내용
성 명	신원확인 수단을 이용한 본인확인을 수행하여 검증한 이용자의 실명
휴대폰번호, 이동통신사	휴대폰번호와 소속 이동통신사 정보 ※휴대폰 기반의 서비스인 경우에 한함
중복가입확인정보(DI)	해당 웹사이트 내에서만 유일하게 이용자를 식별할 수 있는 64byte 정보
연계정보(CI)	주민등록번호에 1:1일 매칭 되는 식별자로 88byte 암호화된 정보
생년월일	주민등록번호에서 추출한 8자리정보
성별	주민등록번호에서 추출한 1자리정보
연령대	법적연령대 1자리정보
내·외국인	1자리 정보
기타	IP, OS, App 버전 정보 등

<표 2>에서 CI는 <그림 3>과 같이 주민등록번호를 입력하여 해쉬 함수를 적용한 88Byte 암호화된 값으로써 주민등록번호와 1:1일 매칭 되는 정보로 유일하게 해당 사용자를 식별할 수 있는 식별 값으로 사용하고 있는 정보이다. 즉, CI를 사용하여 유일하게 사용자를 식별할 수 있어 개인 사생활 침해 등과 같은 문제점이 야기될 수 있다. 물론, 암호화된 값으로써 인간의 인지기억으로 외울 수 있는 값은 아니지만 시스템 간 연동을 통해 얼마든지 온라인 서비스 활동을 조회하거나 추적할 수 있는데 사용할 수 있는 유일키에 해당하기 때문에 그 만큼 연계정보의 과도한 제공이나 오·남용을 방지하기 위한 방안 마련이 요구되고 있다. DI는 연계정보 생성과 유사하나 해쉬함수 입력으로 사업자의 고유식별번호를 추가함으로서 온라인 사업자들마다 동일한 이용자일지라도 DI정보는 서로 상이한 차이점을 가지고 있다.



(가) 연계정보 생성 과정

(나) 연계정보 (다) 중보가입확인정보

<그림 3> 연계정보(CI)와 중복가입확인정보(DI) 생성 처리 과정[3]

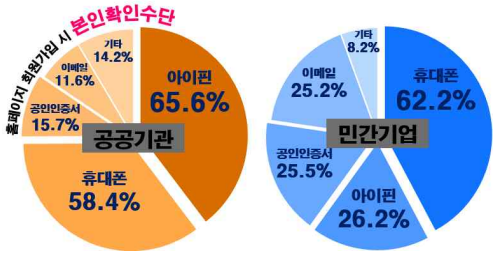
3.3 본인확인서비스 현황

주민등록번호 대체수단 기반의 본인확인서비스를 제공하는 기관은 아이핀, 휴대폰, 신용카드, 공인인증서를 발급하는 기관들로써 방송통신위원회가 지정함으로서 본인확인 업무의 기술적, 관리적, 물리적 적정성에 대한 평가를 수행하고 있다. 홈페이지 회원 가입 시 본인확인수단을 적용하고 있는 현황을 조사한 자료에 따르면 <그림 4>와 같이 조사되었다. 공공 및 민간 기관에서는 사용하는 대체수단이 휴대폰과 아이핀으로 양분되었으나 공공아이핀이 더 이상 신규

발급이 불가능한 상황이 되어 공공기관의 경우는 아이핀 보다는 휴대폰을 활용한 본인확인을 적용할 가능성이 높은 것으로 예측할 수 있다. 또한 민간아이핀과 휴대폰 기반의 본인확인서비스의 인증 건수를 <그림 5>에서 분석한 결과, 2017년까지 약 12억 4천만건의 인증 건수를 제시하였으며 2018년 4월까지 4억 7천만건의 인증 건수를 제시하여 2018년 총 인증 건수는 약 13억 건 이상으로 예측할 수 있다. 본인확인서비스는 이용률을 분석하면 국내 인구 5천백만 명 인구 중 인터넷 사용자 수가 4천7백만 명으로 분석[19, 24]할 때 최근 4년간 본인확인서비스(민간아이핀, 휴대폰)의 평균 인증건수가 약 10억 건으로 추정하면 인터넷 사용자 1인당 년 간 20회 이상의 본인확인서비스를 이용하고 있음을 알 수 있다. 즉, 주민등록번호 대체수단 기반의 본인확인서비스 이용이 광범위하게 우리 일상생활에 사용되고 있으며 온라인 서비스 사업자들 역시 과도하게 본인확인서비스가 적용되어 있지 않는지 살펴볼 필요가 있다.

3.4 현행 본인확인서비스의 문제점

현재 주민등록번호 대체수단 기반의 본인확인서비스의 경우 <표 2>와 같이 사용자가 한 번의 본인확인으로 다량의 개인정보가 사업자들에게 제공하고 있어 실제 온라인 서비스 사용자가 사업자에게 제공되는 본인의 개인정보에 대한 선택권이 없는 것이 문제점 중에 하나이다. 또한 사업자들 역시 무분별하게 본인확인서비스를 필수적으로 적용하고 있어 온라인 서비스 사용자가 서비스를 받기 위해서는 본인확인을 거쳐야 하는 문제점도 지적되고 있다. 이러한 문제점들을 해결하기 위한 방안을 모색하기 위해 국외 본인확인서비스의 동향을 살펴보고 이를 바탕으로 국내 본인확인서비스에 적용가능한 점을 설펴보고자 한다.



<그림 4> 본인확인서비스 사용현황 분석(개인정보보호 위원회, 2017)

<그림 5> 주민번호 대체수단(I-PIN과 휴대폰) 기반의 본인확인서비스 인증 건 수[24]

<그림 6> 국내 본인확인서비스 적용 현황

IV. 본인확인서비스 관련 국내·외 동향

4.1 국내 동향

국내 본인확인서비스는 본인확인을 위해 각 온라인 사업자들은 <그림 6>과 같이 이용자들에게 요구하

는 식별용 개인정보가 서로 상이한 경우가 대부분이다. 이는 온라인 사업자들이 본인확인의 주요한 목적 달성 보다는 추가적인 이용자의 개인정보 수집으로 마케팅 등의 활용이 더 큰 부분을 차지하고 있는데서 기인한다. 결국 본인확인을 위한 인증 수단이 파편화되고 단일인증 즉, Single-Sign-On(SSO) 기반의 다중 사용이 가능한 문제점이 존재한다. 온라인 사이트 가입 시 SSO 개념을 적용한 공공 기관 사이트로는 <그림 7>과 같이 행정안전부가 제공하고 있는 전자정부 디지털 원패스[20]가 존재하고 있으나 실제 SSO로 연계하는 공공기관의 사이트가 현재 14개로 미비한 실정이며 활성화도 미진한 상황이다.

<그림 7> 디지털 원패스 개요도[20]

4.2 국외 동향

국외 본인확인서비스는 본인확인을 위해 온라인 서비스 이용자의 다양한 정보를 집중하여 관리하고 사용자의 복합인증 방법을 적용한 후 SSO를 통한 다양한 온라인 서비스에 활용할 수 있도록 서비스가 제공되고 있다. <그림 8>과 같이 온라인 서비스 이용자는 SSO를 통한 단일 복합 인증으로 다양한 서비스를 제공받을 수 있으며 복합인증을 통해 온라인 사업자에게 제공되는 개인정보에 대해서도 자기 정보 제공 선택에 따라 제공되도록 서비스가 활성화되고 있는 상황이다. <표 3>에서는 국외 본인확인 관련 서비스 적용 현황을 나타낸 것이다. 표에서와 같이 국내와 같이 국민을 식별하는 유일키를 사용하여 본인확인을 적용하는 것이 대부분으로 조사되었다.

미국은 사이버 신원 확인을 위한 국가전략 발표에 따라 국가표준기술연구소(NIST)에서 개인과 조직을 위한 전자신원확인을 위한 디지털 신원 가이드[21]를 발표하였다. 온라인 서비스를 이용하고자 하는 사용자는 자신이 소지하고 있는 본인확인용 인증수단의 보안강도에 따른 차등화된 수준으로 온라인 서비스를 제공받을 수 있도록 가이드를 마련하고 있다. 따라서 자이 보유하고 있는 신원증명, 인증강도, 연계 보증 수단에 따라 차별화된 온라인 서비스와 개인정보의 제공 방안을 마련하고 있다. 그리고 유럽 내 전자상거래를 위한 전자 본인확인에 관련 규칙(eIDAS)[22] 제정과 이행에 따라 전자신분증(eID)과 지문정보 등으로 EU 국가 간 본인확인서비스를 2018년 9월부터 시행하고 있다. eIDAS에서는 사용자가 제공하는 인증수단의 강도에 따라 차등화된 온라인 서비스를 이용할 수 있도록 방안을 제시하고 있다.

Ⅴ. 본인확인서비스 개선 방안

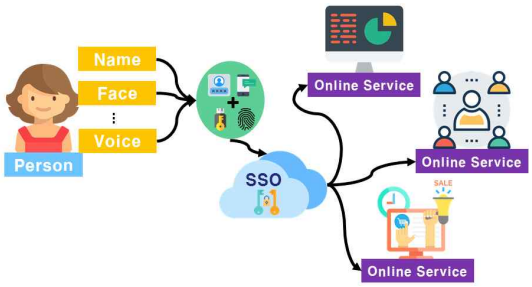
5.1 본인확인기관이 제공하는 이용자의 개인정보 최소화 방안

주민번호 대체수단 기반의 본인확인서비스에서는 온라인 사업자들에게 서비스 이용자의 개인정보를 과도하게 제공하고 있는 문제점을 언급한 바 있다. 제공하는 개인정보들에는 이름, 생년월일, 내·외국인, 연령대, 성별, CI, DI, 휴대폰번호, 가입통신사 정보 등을 제공하고 있다. 국외 동향에서도 살펴본 바와 같이 본인확인서비스의 경우는 온라인상에서 신원확인이 주된 목적으로써 온라인 서비스를 이용하고자하는 이용자의 신원 증명이 참인지 거짓인지를 확인하고 이에 대한 확인정보만을 사업자에게 전달하거나 혹은 서비스 제공에 필요한 최소한의 정보들 예를 들어 주소, 이름, 부모이름 등만 제공하고 있다. 하지만

국내 본인확인서비스의 경우는 2012년 주민등록번호 수집 금지에 따른 주민등록번호에 준하는 진성 개인정보를 사업자들에게 제공하고 있다. 따라서 본인확인서비스의 특성상 실제 신원을 증명하는 이용자가 본인인지 아닌 지만을 확인함으로써 그에 합당한 정보만을 제공하는 것이 필요하다. 만약 온라인 사업자들이 추가적인 이용자의 개인정보가 필요할 경우에는 별도의 수집·동의를 받아 수집하는 과정이 필요할 것이다. 이러한 과정을 거치게 되면 결국 온라인 사업자들이 주민번호 대체수단 기반의 본인확인서비스의 적용보다는 사설인증이나 자체인증(이메일 인증 등) 등으로 서비스를 제공 가능함으로써 온라인 본인확인서비스를 이용하는 사회적인 비용을 줄일 수 있는 이점이 있다.

5.2 온라인 사업자의 본인확인서비스 적용 최소화 방안

온라인상에서 서비스 이용자의 본인을 확인하도록 하는 관련법들에는 「전자서명법」, 「전기통신사업법」, 「정당법」, 「자동차관리법」, 「청소년보호법」, 「게임산업 진흥에 관한 법률」, 「전자금융거래법」, 「전자상거래 등에서 소비자보호에 관한 법률」 등이 있다. 그러나 실제 주민등록번호 대체수단 기반의 본인확인서비스 즉, 「정보통신망법」 제23조에 따라 본인확인기관으로 지정된 본인확인서비스를 이용하여 본인확인을 이행하도록 강제하는 조항은 존재하지 않는다. 그러나 현재 온라인 사업자들은 회원가입, 정보변경, 게시글 작성 등에서 주민번호 대체수단 기반의 본인확인서비스를 필수적으로 적용하고 있는 상황이다. 사업자들이 서비스 이용자의 신원을 명확하게 확인하고 또한 추가적으로 국가가 보증하는 이용자의 진성 개인정보를 제공해 주는 현행 대체수단 기반의 본인확인서비스를 적용하고 있는 상황이다. 결국, 향후 발생 가능한 법적 대항력 확보, 저렴한 서비스 비용으로 이용자의 진성 개인정보 수집, 명확한 이용자 식별, 다른 서비스 연계 목적 등의 이유로 본인확인서비스를 필수로 적용하고 있다. 기존 연구[17]에서 수행한 온라인 사업자들의 본인확인서비스 적용 목적을 설문한 결과, 약 54%가 회원가입, 정보 변경, 응대 등 이용자 식별 목적, 41%가 법적 요구사항(청소년 인증, 법정대리인 확인 등)의 목적, 25%가 다른 사업와의 이용자 정보 연계 목적, 20%가 이용자 불만제기 등 법적 대항력 확보를 위한 목적, 그리고 8%가 향후 서비스 확대를 대비하기 위한 개인정보 수집 목적으로 조사되었다. 이처럼 온라인 사업자들은 불필요하게 본인확인서비스를 필수적으로 적용하고 있어 서비스 이용자들이 서비스를 제공받기



<그림 8> 국외 본인확인서비스 적용 현황

<표 3> 국가별 본인확인서비스 적용 현황

국가	내용
미국	- NIST 800-63 디지털 신원지침 마련 - Login.gov를 통해 공공 온라인 서비스 이용을 위한 SSO 본인확인 제공
캐나다	- 사회보험번호로 신원확인 - SecureKey Concierge Service 정부 본인확인 사이트 운영
독일	- 온라인에서 전자신분증(eID)와 지문으로 본인확인
영국	- 국가 보험 번호로 본인확인 - GOV.UK 정부 사이트 운영
인도	- Aadhaar 법에 따른 고유 식별정보 부여로 본인확인
호주	- 세금파일번호로 본인확인 - myGov 정보 사이트 운영
일본	- MyNumber 도입으로 온라인 본인확인 사용

위해 필수적으로 본인확인서비스를 이용할 수밖에 없도록 구성되어 져 있다. 따라서 온라인 사업자들이 서비스 제공에 있어 필수적으로 본인확인서비스의 적용 유무를 판단할 수 있게 하는 가이드 마련이 필요하다. 미국 NIST의 Digital Identity 가이드라인[21]과 같이 온라인 사업자가 본인확인서비스 적용에 있어 본인확인서비스를 적용하지 않음으로써 발생 가능한 위험을 분석하여 해당 위험분석 결과에 따라 도입하도록 하는 과정이 요구된다. 즉, 온라인 서비스 이용자의 본인확인 실패로 인해 발생할 수 있는 결과로 조직과 서비스에 미치는 잠재적인 영향을 점검할 수 있는 기준을 마련하여 이를 온라인 사업자들이 자체적으로 위험을 분석하는 것이 필요하다.

발생 가능한 위험에는 <표 4>와 같이 나열한다. 각각의 위험분석 항목들은 다시금 3단계(높음, 중간, 낮음)로 구분하고 본인확인서비스의 인증실패로 인한 잠재적인 영향을 평가하는 프로세스를 <그림 9>와 같이 제시한다. 평가 프로세스에 따라 온라인 사업자들인 ID 식별, 자제 식별, 본인확인서비스 이용에 따른 구분으로 본인확인서비스 적용 여부를 판단하도록 하는 기준을 마련하는 것이 필요하다. ID 식별은 본인확인이 없이 서비스 이용자가 제공하는 ID 기반의 인증으로만 이용자를 식별하여 서비스를 제공하는 것으로 볼 수 있으며, 자체 식별은 회원가입 등 이용자가 제공한 개인정보 등으로 자체적인 사용자 식별로 가능함을 의미한다. 그 외 경우는 본인확인서비스의 이용이 필요한 경우로 구분할 수 있다.

<표 4> 본인확인서비스 도입 시 평가하는 위험분석 리스트

위험분석 항목
- 불편, 곤란, 명성 또는 평판의 훼손
- 금전적 손실 또는 배상 책임
- 조직, 사업 또는 공공 이익에 해를 끼치는 정도
- 민감 정보의 비인가 배포
- 개인의 안전
- 법령 위반

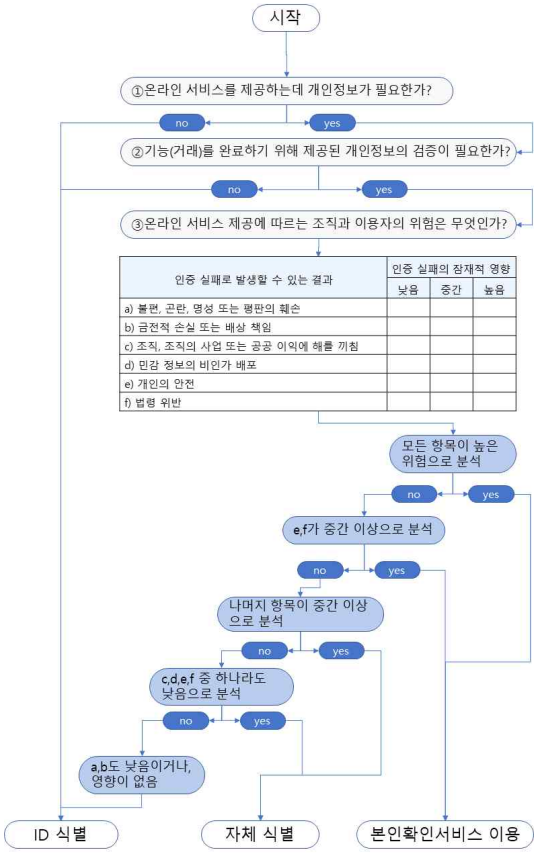
5.3 본인확인서비스 차등화 제공 방안

주민번호 대체수단 기반의 본인확인서비스를 통해 이용자의 개인정보가 과도하게 온라인 사업자에게 제공되는 문제점이 있다. 즉, 온라인 사업자가 온라인 서비스 이행에 불필요한 이용자의 개인정보까지도 본인확인기관이 함께 시스템 연동전문을 통해 제공하고 있어 온라인 사업자가 선별적으로 필요한 개인정보를 저장하고 나머지는 파기하고 있는 상황이다. 하지만, 정보시스템 연계과정에서 본인확인기관과의 연계 서버나 미들웨어의 연동전문 로그 상에 이용자의 개인정보가 저장될 수 있으며 불필요한 개인정보를 본인확인기관이 선별적으로 전송하는데도 한계가 있다. 따라서 이를 해결하기 위해서는 온라인 사업자가 본인확인서비스를 통해 필요한 개인정보를 본인확인기관에 질의를 하고 이에 대응하는 본인확인서비스 이용자의 개인정보만을 제공해 주는 방안 마련이 필요하다. 이를 통해 본인확인기관은 과도한 이용자의 개인정보를 전송하는 것이 아니라 온라인 사업자가 요구하는 개인정보만을 전송하게 되고 온라인 사업자는 서비스에 필요한 개인정보만을 요구함으로써 최소 개인정보 수집의 원칙에도 부합하는 방안일 것이다. 이러한 방안을 실현하기 위해서는 온라인 사업자가 서비스에 필요한 타당한 개인정보를 요구하고 있는가를 검증하는 것이 필요하다. 현실적으로 본인확인기관이 모든 온라인 사업자들이 요구하는 정보가 타당한지 검증하는 것은 불가능한 일일 것이다. 따라서 온라인 사업자들이 서비스 이용에 필요한 이용자 개인정보 수준에 따른 서비스 제공의 차등화 방안을 제시하는 것이 필요하다. 이를 위해 온라인 사업자들이 서비스에 필요한 이용자 개인정보의 수준을 3단계로 구분하고 1단계는 본인 및 청소년 여부, 2단계는 본인 및 청소년 여부, 이름, 생년월일, 내·외국인, 3단계는 2단계를 포함한 개인정보와 CI

및 DI정보까지 제공하는 것으로 차등화할 수 있다. 온라인 사업자들이 각 단계별 수준을 결정하는 것은 <그림 9>의 본인확인서비스 적용 프로세스에 따라 본인확인이 필요한지를 결정하고 이후 본인확인서비스에서 최소의 개인정보 수집원칙에 따라 최소한의 개인정보 수집을 이행하기 위한 단계를 결정함으로써 차등화된 개인정보 제공이 가능하다.

5.4 연계정보(CI) 제공 최소화 방안

CI는 주민등록번호와 1:1로 매칭되는 정보로서 실제 CI만으로도 사용자를 식별할 수 있는 고유식별정보에 해당한다. 실제 「정보통신망법」 상에서는 고유식별정보에는 포함되어 있지 않으나 CI만으로도 사용자 식별이 가능하고 자체적으로 변경이 불가능한 개인정보이기 때문이다. 이러한 CI는 88byte로 암호화된 값으로써 실제 인간의 인지능력으로 기억할 수는 없으나 시스템간의 연계를 통해 사용자 식별이 가능하여 온라인 사업자들은 과거 주민등록번호로 이용자를 식별하는 대신에 근래에서는 CI를 사용하여 이용자를 식별하고 다른 사업자들과의 서비스 연계에 활용하고 있는 상황이다. 그러나 무분별하게 본인확인서비스를 적용하여 과도한 이용자의 CI가 활용되고 있어 이용자에 대한 사생활침해 등이 문제를 야기하고 있다. 따라서 CI의 무분별한 오·남용 문제를 해결하기 위해 근본적인 방법은 현재의 CI값을 변경하고 더 이상 불필요한 CI의 제공을 근절하는 것이다. 하지만, 국내 온라인 사업자뿐만 아니라 오프라인 다양한 사업자들도 보유하고 있는 국민의 CI의 변경 시간 및 비용에서 상당한 소모가 발생하는 것은 자명한 일이다. 또한 수천만 명에 해당하는 주민등록번호를 입력으로 새로운 CI를 생성하는 것은 본인확인기관의 시스템 부하에도 영향을 줄 것이고 서비스 이용자인 국민입장에서는 연계서비스의 일시 단절로 인해 금전적·시간적인 피해를 보게 되는 문제점이 있다.



<그림 9> 본인확인서비스 차등 적용을 위한 온라인 서비스의 위험평가 프로세스

결국 현재의 CI를 유지하되 과도한 CI의 제공을 근절함으로서 점차적으로 CI의 노출을 최소화하는 것이 필요하다. 그러나 온라인 사업자들 간의 서비스 연계를 위해서는 CI가 필요하나 CI 제공을 차단하게 됨으로서 본래의 서비스 간 연계가 불가능하게 되는 또 다른 문제점이 발생한다. 따라서 이에 대한 해결방안으로 CI 달리 DI를 온라인 사업자들에게 제공하고 있으며 이를 각 온라인 사업자들이 본인확인기관에게 다시금 질의하여 동일인인지를 확인함으로써 서비스 간 연계가 가능할 것이다. 즉, CI는 주민등록번호와 1:1로 매칭된 정보이자만 DI는 동일한 이용자일지라도 각 사업자마다 서로 다른 64byte 값을 가지고 있어

온라인 사업자간의 직접적인 연계는 불가능하지만 본인확인기관은 해당 정보를 보유하고 있어 DI가 동일 이용자의 정보인지를 확인할 수 있다. 이를 이용함으로써 CI의 제공을 최소화하고 DI는 모든 사업자들마다 다른 정보로써 온라인 서비스 이용자가 온라인상에서 사생활이 침해되는 등의 문제점 야기는 최소화될 수 있을 것이다.

VI. 본인확인서비스 개선방안 효과

6.1 최소한의 개인정보 제공

현행 주민번호 대체수단 기반의 본인확인기관에서 온라인 사업자들에게 제공하는 본인확인서비스 이용자의 개인정보를 최소로 제공함으로써 온라인 사업자들의 수집 받은 개인정보의 암호화 등의 적절한 보호조치를 취함에 있어 비용적인 면에서 경감이 가능할 것이며, 본인확인기관에서는 본인확인용 개인정보의 암호화 전송을 위해 매년마다 실시하는 인증모듈에 대한 취약점 분석, 인증모듈의 암호화 키 갱신 등의 비용 절감효과가 발생할 것이다. 본인확인기관에서는 보유하고 있는 개인정보를 본인인지에 대한 정합여부만을 검증함으로써 타 기관과의 연동, 서비스 연동 모듈에 대한 HMAC 코드 검증, 본인확인서비스 대행사의 위탁사 관리감독 비용 감소 등의 본인확인기관의 서비스 제공 비용의 감소를 귀결되어 시장에서 요구하는 본인확인서비스 인증 수수료의 경감효과도 발생할 것이다.

6.2 본인확인서비스 적용 최소화

온라인사업자들은 주민번호 대체수단 기반의 본인확인서비스를 적용함에 있어 초기 도입 시 인증모듈의 설치를 통해 서비스 이용 건수에 대한 수수료를 지불하고 있는 구조이다. 결국, 본인확인서비스 적용을 최소화함으로써 인증 서비스 비용을 줄일 수 있다. <표 5>와 같이 2018년까지 방송통신위원회 소관 본인확인기관인 이동통신 3사와 아이핀 3사의 본인확인서비스 인증 성공 건수[24]를 본인확인서비스 건당 30원[25]으로 계상하면 2018년 본인확인서비스 인증건수 추정치가 13억건이 발생하게 되어 2018년에만 390억 원 이상의 비용이 발생하게 된다. 결국 이러한 비용은 온라인 사업자들이 본인확인기관에게 제공하고 있으며 이 비용은 실제 서비스를 제공받은 이용자에게 전가 될 수 밖에 없는 상황이다. 따라서 온라인 사업자들이 현행 주민번호 대체수단의 본인확인서비스 적용을 최소화함으로써 서비스 비용을 줄일 수 있으며 결국 온라인 서비스 이용자에게 더 많은 혜택을 부여할 수 있는 효과가 발생한다. 또한, KISA의 I-Pin 2.0 안내서[26]에 제시한 바와 같이 아이핀 인증모듈의 도입 시 기존 시스템 변경을 위한 분석과 개선에 중급기술자 4명이 1개월간 투입되어 약 2천만의 비용발생과 인증모듈 도입 이후 인증비용이 연 100만원으로 제시하고 있다. 따라서 온라인 사업자들이 본인확인서비스의 적용을 최소화함으로써 인증모듈 도입에 따른 비용도 줄일 수 있는 효과가 발생한다.

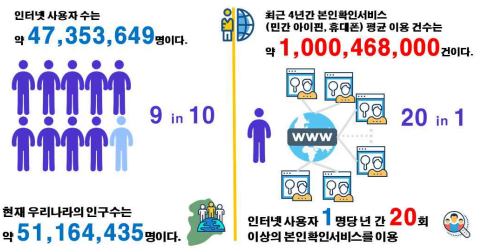
<표 5> 국가별 본인확인서비스 적용 현황 (억건) [24]

년도	2013	2014	2015	2016	2017	2018
인증건수	5.4	7.2	9.1	10.6	12.4	13

6.3 본인확인서비스의 차등화 제공

현행 본인확인서비스의 경우 온라인 사업자가 본인확인서비스를 요청 시 본인확인기관에 사전에 정의된 서비스 연동 규격에 따라 서비스 이용자의 개인정보를 제공하고 있는 상황에서 만약 온라인서비스 사업자가 필요한 정보만을 요청하고 이에 대한 응답

에 해당하는 개인정보만을 제공함으로써 과도한 이용자의 개인정보 제공을 차단할 수 있는 효과가 발생한다. <그림 10>과 같이 인터넷 이용자 당 평균 20회 이상의 본인확인서비스 이용한다고 추정할 경우 인터넷 이용자의 진성 개인정보를 20회 이상 온라인 사업자들에 제공하고 있음을 의미한다. 따라서 본인확인서비스 이용 시 온라인 사업자가 필요로 하는 이용자의 개인정보만을 본인확인기관에게 요청하도록 서비스 연동 전문을 수정함으로서 과도한 이용자의 개인정보가 온라인 사업자들에게 제공되는 것을 차단할 수 효과가 발생한다.



<그림 10> 인터넷 사용자 당 본인확인서비스 평균 이용 건수

6.4 연계정보(CI) 제공 최소화

CI정보는 주민등록번호와 일대일 매칭되는 정보로써 사용자를 고유하게 식별할 수 있는 개인정보이다. 따라서 CI정보의 무분별한 오남용을 방지하고 억제하기 위한 수단으로 온라인사업자들이 본인확인서비스 적용 시 실제 CI정보가 필요한지를 선택적으로 판단하는 기준의 제시가 요구된다. <그림 9>와 같이 온라인 서비스 이용 시 관련 위험분석을 통해 위험평가를 토대로 본인확인서비스의 적용이 필요한지를 판단할 수 있는 근거를 제시함으로써 본인확인서비스의 적용을 최소화 할 수 있고 이는 결국 CI정보의 제공 최소화로 귀결될 수 있다. 결국 제안한 본인확인서비스 개선, 적용 방안과 효과는 <표 6>과 같이 요약할 수 있다.

Ⅶ. 결론

본 연구를 통해 주민등록번호 대체수단 기반의 본인확인서비스의 과도한 적용으로 온라인 서비스 이용자의 개인정보를 안전하게 보호하고 온라인 서비스의 안전성을 확보하는데 필요한 방안을 제안하였다. 현행 본인확인서비스에서는 이용자를 식별하기 위해 온라인 서비스 이용자의 이름, 생년월일, 그리고 주민등록번호에 준하는 연계정보(CI)와 중복가입확인정보(DI) 등을 온라인 사업자들에게 제공하고 있어 제공하는 개인정보에 대한 차등화 방안을 제시하였다. 무엇보다는 근본적으로 온라인 서비스 제공 사업자가 과도하게 본인확인서비스를 필수로 적용하고 있는데서 기안한 문제점들로 확인할 수 있었다. 하지만, 온

<표 6> 본인확인서비스 개선 방안 적용 효과

제안 방안	적용 방안	효과
최소한의 개인정보 제공	▪ 본인확인 연동 모듈의 수정 ▪ 서비스 이용자의 개인정보 제공 선택권 부여	▪ 본인확인기관의 안전성 확보 증가 ▪ 이용자의 개인정보 최소 제공 효과
본인확인서비스 적용 최소화	▪ 지식 기반 및 사설 인증 수단 확대 적용	▪ 온라인 서비스 사업자의 본인확인서비스 비용 감소 ▪ 인증건수에 따른 년간 100만원 이상의 인증 비용 감소
본인확인서비스의 차등화 제공 효과	▪ 본인확인 연동 모듈 상의 정보 요청 질의문 쿼리 추가 ▪ 요청 정보에 따른 차등화된 서비스 비용 부과	▪ 온라인사업자의 본인확인서비스 비용 감소
연계정보(CI) 제공 최소화	▪ 위험분석을 통한 위험도 평가 실시 ▪ 위험도에 따른 차별적인 본인확인서비스 적용	▪ 개인정보 침해 피해 감소 ▪ 본인확인서비스 비용 감소

라인 사업자들 입장에서는 온라인 서비스 이용자의 명확한 식별과 청소년 여부, 법정 대리인 여부를 확인하고 관련 법령들의 대항력을 확보하기 위해서는 국가가 신뢰하고 지정하는 현행 본인확인서비스를 이용하여 이용자를 식별하고 관련 개인정보를 수집할 수밖에 없는 상황이다. 이러한 상황에서 최소한 주민등록번호 대체수단 기반의 본인확인서비스의 도입과 활용을 최소화하기 위해 온라인 사업자가 수행하고 있는 서비스에 대해서 개인정보 수집으로 인한 위험 평가하여 분석한 후 관련 위험 정도에 따라 본인확인서비스 적용 여부를 선택하는 것이 필요하다. 그리고 국외 사례와 같이 다양한 본인확인 인증강도에 따른 차등화된 개인정보 제공방안을 국내 본인확인서비스에도 적용하고 추가적으로 현행 본인확인기관이 온라인 서비스 이용자의 개인정보를 모두 제공하는 것이 아니라 온라인 사업자가 서비스에 필요로 하는 즉, 요구하는 개인정보만을 제공함으로서 불필요한 개인정보의 제공을 근본적으로 차단할 수 있다. 따라서 본 연구에서 제시한 현행 본인확인서비스의 개선을 위한 방안을 적용함으로써 본인확인기관과 온라인 사업자들의 큰 서비스 변경 없이 바로 적용이 가능함을 알 수 있다. 변경이 필요한 사항은 본인확인서비스 연동전문 상에서 온라인 사업자가 질의하여 요청한 정보만을 본인확인기관이 제공하는 형태로 서비스 변경이 필요하고, 온라인 사업자가 DI정보를 사용하여 이용자를 다른 사업자들과의 식별하는 방안을 마련함으로써 CI정보 등이 무분별하게 제공되어 사생활 침해와 같은 문제점들을 해결할 수 있다. 향후 연구에서는 본인확인서비스에서 CI와 DI정보 생성과정의 안정성에 대해 검증하고 보다 안전한 방안을 CI정보의 생성과 활용에 대해서 연구를 수행하고자 한다.

참고문헌

[1] 최중석·김종배, "주민번호 대체 수단의 안전성 강화 방안 연구", 대한전자공학회 학술대회, 2015, pp. 298-301.

[2] 강석진, "아이핀(I-PIN)을 이용한 인터넷상 본인확인의 문제점 분석 및 개선방안 연구", 고려대학교 석사논문, 2017.

[3] 김종배, "아이핀 기반 본인확인서비스의 안전성 강화 방안", 한국IT서비스학회 논문지, 제16권, 제2호, 2017, pp. 97-110.

[4] 신영진·신승호·이자성·한웅기, “한국에서의 본인확인수단 개선방안에 관한 연구”, 한국지역정보화학회지, 제18권, 제4호, 2015, pp. 59-88.

[5] 안정희, “인터넷상의 주민등록번호 대체수단의 문제점들과 해결방법”, 디지털산업정보학회 논문지, 제4권, 제3호, 2008, pp. 1-9.

[6] 이영교·안정희, “공인인증서를 이용한 주민등록번호 대체수단에 관한 연구” 디지털산업정보학회 논문지, 제10권, 제3호, 2014, pp. 107-117.

[7[전자서명법(2017.07.26.), http://www.law.go.kr/법령/전자서명법, 2019.

[8] 본인확인기관 지정 등에 관한 기준(2015.07.31.), http://www.law.go.kr/행정규칙/본인확인기관지정등에관한기준, 2019.

[9] 장원창·신일순, "아이핀의 가치창출효과 추정", 한국IT서비스학회 논문지, 제12권, 제2호, 2013, pp. 185-193.

[10] 이영교·안정희, “주민등록번호 변경 방법에 대한 연구”, 디지털산업정보학회 논문지, 제12권, 제3호, 2016, pp. 65-74.

[11] 장인용·염흥렬, “인터넷상의 본인확인수단인 아이핀의 활성화 방안 연구”, 한국정보보학회지, 제19권, 제5호, 2009, pp. 81-94.

[12] 신영진, "주민등록번호의 수집 금지 및 본인확인

수단의 적용을 통한 개인정보보호방안 연구 : 민간분야의 온·오프라인 개인정보 수집서식을 중심으로", 한국지역정보화학회지, 제17권, 2호, 2014, pp. 173-203.
[13] 신영진·김종배 외 8명, "주민번호 대체수단 연구 및 인증절차 개선 방안 조사", 한국인터넷진흥원 연구보고서, KISA-WP-2015-0028, 2015.
[14] 김종배, "온라인 본인확인 관련 동향 및 시사점", 한국경영학회 통합학술대회, 2018, pp. 3-11.
[15] 이영교·안정희, "아이핀 대량 부정발급 사고에 대한 개선방법 연구", 디지털산업정보학회 논문지, 제 1권, 제2호, 2015, pp. 11-22.
[16] 김승주, "주민번호 대체수단 서비스 개선 방안 연구", 박사학위논문, 성균관대학교, 2007.
[17] 김종배·최중석·전동호·이재호·박기홍, "본인확인기관 지정기준 및 관리체계 개선방안 마련", 한국인터넷진흥원 연구보고서, KISA-WP-0138, 2018.
[18] 김종배·김지연·한흥렬·전동호·전진환·최중석, "주민번호 대체수단 안전성 강화 방안 조사," 한국인터넷진흥원 연구보고서, KISA-WP-0027, 2015.
[19] Internet World Stats, https://www.internetworldstats.com/, 2019.02
[20] 전자정부 디지털 원패스, https://www.onepass.go.kr/, 2019.
[21] NIST 디지털 신원 가이드라인, https://pages.nist.gov/800-63-3/, 2019.
[22] eIDAS, https://www.eid.as/home, 2019.
[23] 조성인, "전자금융거래에서 생체인증 특성이 금융소비자의 사용의도에 미치는 영향에 대한 연구," 한국IT정책경영학회 논문지, 제10권, 제2호, 2018, pp. 1033-1039.
[24] 김종배, "온라인 본인확인 관련 동향 및 시사점", 2018년 개인정보보호페어 Track B, 2018.
[25] 경향비즈, "휴대전화 본인확인서비스로 이통사, 작년 260억 벌어들여", http://biz.khan.co.kr/khan_rt_view.html?artid=201609190100005, 2016.
[26] i-PIN 2.0 도입 안내서, 한국인터넷진흥원, 2010.
[27] 이지엽·권두순, "온라인 게임 중독 특성이 자아통제를 통해 충동성 범죄에 미치는 영향," 디지털산업정보학회 논문지, 제13권, 제1호, 2017, pp. 135-145.
[28] 최희식·김현규, "사회적 이슈 관점에서 바라 본 사이버 테러 유형에 대한 위험 대응방안," 디지털산업정보학회 논문지, 제13권, 제1호, 2017, pp. 59-67.

■ 저자소개 ■

김종배
(Kim, Jong Bae)

2019년 3월~현재 세종사이버대학교 컴퓨터소프트웨어학과 부교수
2006년 6월~2019년 2월 서울디지털대학교 컴퓨터공학과 교수
2000년 4월 경북대학교 컴퓨터공학과 (공학박사)
2002년 2월 경북대학교 컴퓨터공학과 (공학석사)
2000년 2월 부산대학교 컴퓨터공학과 (공학사)

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

논문접수일 : 2019년 3월 12일
수 정 일 : 2019년 3월 21일
게재확정일 : 2019년 4월 19일