The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 20, No. 2, pp.201-208, Apr. 30, 2020. pISSN 2289-0238, eISSN 2289-0246

https://doi.org/10.7236/JIIBC.2020.20.2.201
JIIBC 2020-2-27

온라인 서비스의 본인확인 요구사항 분석 기반의 차등화된 본인확인서비스 적용 방안

A Study on Differentiated Personal Proofing Service Based on Analysis of Personal Identification Requirements in Online Services

김종배*

Jong-Bae Kim*

요 약 최근 온라인 서비스가 확대함에 따라 비대면 거래에서 본인을 확인하기 위한 주민번호 대체수단 기반의 본인확인서비스의 적용이 증가하고 있다. 이에 따라 온라인 서비스 제공 사업자(Internet Service Provider: ISP)들은 대체수단 기반의 본인확인서비스를 무분별하게 적용함으로써 이용자의 개인정보가 과도하게 제공되는 문제점이 발생하고 있다. 따라서 본 연구에서는 온라인 서비스에서 본인확인이 필요한지 여부와 또 필요하다면 어떤 보증수준의 본인확인 인증수단을 적용하는 것이 적정한지에 대한 차등화된 본인확인서비스 적용 방안을 제안한다. 이를 위해 본인확인 관련 요구사항들 분석하여 각각의 요구사항들에 대해 위험을 분석하고, 해당 위험을 최소화하기 위한 보증수준에 따른 차등화된 본인확인서비스 적용 방안을 제시한다. 제안한 방안을 통해 대체수단 기반의 본인확인서비스 적용을 최소화하여 인증비용 감소와 개인정보 제공 최소화를 통해 이용자 개인정보보호에도 도움을 줄 수 있음을 알 수 있다.

Abstract Recently, the application of personal proofing service based on social security number(SSN) replacement means for verifying identity in non-face-to-face transactions is increasing. In this paper, we propose a method of applying differentiated personal proofing service on whether identity verification is necessary in the online service provided by ISP and if it is appropriate to apply a certain level of assurance. By analyzing the requirements related to personal proofing required by current ISPs, we analyze the risks for each of the requirements and propose a method of applying differentiated personal proofing service according to the level of identity assurance guarantee to minimize the risks. In applying the proposed method to online service provision, it is possible to reduce user's unnecessary authentication cost by minimizing the application of personal proofing service based on alternative means, and to help protect user personal information by minimizing excessively collected personal information.

Key Words : Personal identity proofing service, I-Pin, Assurance level, SSN, Digital identity

*정회원, 세종사이버대학교 소프트웨어공학과
접수일자 2019년 10월 16일, 수정완료 2020년 2월 3일
게재확정일자 2020년 4월 3일

Received: 16 October, 2019 / Revised: 3 February, 2020 / Accepted: 3 April, 2020
*Corresponding Author: jb.kim@sjcu.ac.kr
Department of Software Engineering, Sejong Cyber University, Korea

Ⅰ. 서 론

2012년 주민등록번호 수집금지에 따라 국내 온라인 ISP들은 온라인 서비스 이용자를 명확하게 식별하기 위한 방안이 필요하게 되었으며, 이에 따라 이용자를 식별하기 위한 주민등록번호를 대체할 수 있는 본인확인의 필요성이 대두되었다. 주민등록번호를 대체할 수 있는 본인확인 수단으로 2005년부터 시작된 아이핀 기반의 본인확인서비스를 시작으로 현재는 휴대폰 및 신용카드 기반의 서비스까지 본인확인을 이행 할 수 있도록 방송통신위원회(이하 방통위)로부터 본인확인기관으로 지정되었다.[1,2] ISP들은 온라인 서비스를 제공함에 있어 이용자들을 식별 및 확인하기 위해 방통위가 지정한 본인확인기관들로부터 대체수단 기반의 본인확인서비스를 제공받고 있다. 본인확인서비스를 통해 본인확인기관이 ISP들에게 제공하는 개인정보는 이용자의 이름, 생년월일, 성별, 내·외국인정보, 연령대, 휴대폰번호&가입통신사정보, 연계정보(CI), 중복가입확인정보(DI), 그 외 기타 정보(IP, 브라우저 등)들을 제공하고 있다.

기존 연구논문[3]에서 제시한 바와 같이 2018년 한 해 동안 본인확인서비스 인증 건수는 약 14억 건에 이르고 있으며, 이는 사회활동 인구 약 4천 8백만 명으로 기준으로 보아 평균 1인당 연간 30회 이상 이용하고 있음을 의미한다. 또한 ISP들이 본인확인을 어떠한 온라인 서비스에 적용하는 것이 합당한지에 대한 검토 없이 거의 모든 온라인 서비스에 적용하고 있다. 예를 들어, 회원가입, 정보변경, 서비스 거래, 청소년 및 성인 확인, 법정 대리인 확인 등에서 본인확인을 요구하고 있는 상황이다. 하지만, 국외의 경우 우리나라와 같이 주민등록번호 체계가 수립되지 않아 명확하게 식별할 수단이 없어 다른 정보를 요구하지 않는 경향도 있지만 온라인 서비스 계약에 있어서 본인확인을 요구하거나 3자로부터 입증 받은 정보의 요구를 강제화 하지 않는 실정이다[4,5]. 예를 들어 Google이나 e-bay 등과 같은 국외 ISP 사업자들에게 온라인 서비스 제공 받음에 있어 개인정보를 별도로 요구하는 경우는 거의 존재하지 않는다. 대금 결제만 명확하게 이루어진다면 서비스 거래자 당사자의 신원에 대해서는 확인하지 않는 것이 일반적이다.[6,7] 따라서 현행 주민번호 대체수단 기반의 본인확인서비스에서 본인확인기관이 온라인서비스 사업자들에게 개인정보의 제공이 타당한지 재검토하는 것이 요구된다. 물론 본인확인서비스 태동시기부터 주민등록번호에 해당하는 최소한의 개인정보 제공을 합의하여 현재의 서비스에 이르고 있다[8-10].

본 논문에서는 온라인 서비스에 본인확인 요구사항을 조사하고, 각 온라인 서비스의 요구사항들에서 발생 가능한 위험의 정도를 분석한다. 그리고 해당 위험을 감소하거나 최소화하기 위해 온라인 서비스 시 적용해야 하는 본인확인 수단의 보증수준을 선택하는 방안을 제안한다. 그리고 해당 보증수준에 매칭되는 본인확인 인증수단을 적용함으로써 무분별한 주민번호 대체수단 기반의 본인확인서비스 적용이 아닌 다양한 인증수단을 적용할 수 있도록 한다.

Ⅱ. 관련 연구

대체수단 기반 본인확인서비스의 안정성과 신뢰성, 그리고 본인확인서비스 이용자의 개인정보 보호를 위한 다양한 연구가 수행되었다[1-4, 10-13]. 특히 대부분은 현행 대체수단에 대한 안전성 개선 방안 연구가 주류를 이루고 있으며 근본적으로 왜 ISP들이 대체수단 기반의 본인확인서비스를 과도하게 적용하는 문제를 해결하기 위한 연구는 진행되지 못하였다. 온라인 서비스와 같은 비대면 거래에서 상대방의 신원을 식별하고 인증하기 위해서는 현행 대체수단 기반의 본인확인서비스가 필수적이다.[1,2,9,10] 대체수단 기반의 본인확인서비스의 개선을 위한 연구들에서는 기술적인 안전성 개선 방안 연구가 주류를 이루고 있다.[1,2] 다른 연구들에는 본인확인수단의 다양성을 검토하고 새로운 본인확인수단을 제시함으로써 기존 본인확인서비스와의 결합으로 안전성을 높일 수 있는 방안을 제안하였다[3]. 아이핀 서비스 개선에 대한 연구에서는 발급 후 미 사용, 법정 대래인의 동의 문제, 사망자 및 인터넷 취약자의 아이핀 발급 차단 방안, 인터넷 상의 불필요한 본인확인 관행에 대한 차단 방안 등을 제시하였다[2,4]. 연구자의 아이핀 서비스에 개선 방안의 다른 연구에서[1,2]는 기술적인 안전성 강화 방안과 제도적인 안전성 강화 방안에 대해 제안하였다. 제안한 방안에서는 아이핀 서비스의 기관 간 연동 중 개인정보 전송의 기술적인 보호 방안과 아이핀 서비스의 인증 이력, 법정대리인, 허무인(사망자, 국적 포기자 등)에 대한 인증 차단 방안 등을 제안하였다. 현행 본인확인서비스의 부정인증시도 증가에 따른 위험성이 높아짐에 따라 다양한 인증요소와 수단을 이용하여 사용자를 검증할 수 있는 정책과 기술을 제안한 빅데이터 기반의 본인확인 연구가 제안되었다[7,14]. 제안한 연구에서는 온라인상에서 본인확인을 수행할 때 마다 개인정보를 수집하고 검증하는

본인확인정보관리 방안을 적용하는 본인확인 정보공유 모델을 제시하였다. 결국 비대면 거래에서 본인확인 시 사용자와 관련 정보들을 검증하고 온라인 서비스에서 요구하는 본인확인 등급에 따른 검증과 관리하는 시스템 개발을 제안하였다. 하지만, 온라인 서비스 사용자의 행태정보를 수집하고 공유하는 것 역시 비식별화된 빅데이터 수집으로 이용자의 개인정보 침해가 발생할 소지가 있으며 본인확인을 위해서는 온라인 사용자의 식별정보를 함께 저장해야하는 문제점이 여전히 존재하고 있다.

온라인상에서 비대면 서비스 이용자들을 식별하기 위해 본인확인서비스의 안전성 강화와 이용자 개인정보 보호를 위한 다양한 정책 및 기술에 대한 개선 방안을 여러 연구자들이 제안하였다.[5,8,11,13] 하지만, 기존 연구들은 주민등록번호 대체수단 기반의 본인확인서비스의 기술적·관리적 개선 방안, 본인확인서비스의 인증 수단 다양화 방안, 본인확인기관의 정책적인 개선 방안 등을 위주로 연구가 진행되었다. 온라인 서비스에서 문제점은 과도하게 본인확인을 요구하는데 있다. ISP사업자들의 입장에서는 안전하고, 활성화된 사업을 영위하기 위한 목적으로 온라인 거래 당사자의 신원을 명확하게 식별하고자 하는 것은 당연한 일이다.

따라서 기존의 연구들에서는 본인확인서비스의 기술적 안전성 확보, 관리적·정책적 개선 방안에 대한 연구를 수행한 바, 본 연구에서는 ISP들 입장에서 최소화된 본인확인을 적용하기 위한 기준과 방법을 제시함으로써 근본적으로 무분별하게 적용하는 본인확인 요구를 최소화하고, 보증수준에 따른 다양한 본인인증 수단을 통해 본인확인을 받을 수 있는 기준을 제시하는 것이 큰 의미가 있을 것이다.

Ⅲ. 본인확인서비스 현황

1. 대체수단 기반의 본인확인서비스 현황

국내 대체수단 기반의 본인확인서비스는 방통위가 지정한 아이핀 3개 기관(2009년), 이동통신 3사(2012년), 8개의 신용카드사(2018년) 가 수행하고 있다. 본인확인서비스를 위해 사용하는 대체수단이란 이용자가 자신의 신원정보를 신뢰할 수 있는 기관에게 제공하여 본인임을 확인한 뒤 한국인터넷진흥원이 인정하는 기술을 이용하여 본인확인정보를 발급받아 인터넷 사이트 회원가입이나 성인인증 등을 위해 주민등록번호 대신 사용하는 것을 말한다.[2] 즉, 아이핀 기관은 이용자의 아이핀 가입 시 입력한 ID와 PW이고 휴대폰 기관은 휴대전화 번호와 인증문자, 그리고 신용카드 기관은 신용카드 번호와 결제용 비밀번호이다. 다양한 수단을 사용한 본인확인서비스의 인증 건수는 매년 급속도로 증가하고 있으며 최근 2018년 한 해 동안 인증 건수는 약 14억 건에 이르고 있다.[3,9] 대부분의 본인확인은 휴대폰이 약 95%이상을 점유하고 있는 상황이다. 결국, 전체 본인확인서비스 시장에서 다양한 신기술들이 등장할지라도 현재의 대체수단 기반의 본인확인서비스가 일반화되어 있어 오히려 본인인증에 관한 신기술의 연구와 개발, 그리고 혁신이 이루어지지 못하고 있다.

2. 온라인 서비스 사업자(ISP) 설문조사

현재 ISP들은 온라인 서비스 제공에 있어 이용자를 명확하게 식별하고 관련 법령 준수와 연계 서비스 제공 등을 위해 대체수단을 활용한 본인확인서비스를 온라인 서비스에 적용하고 있다. 본 논문에서는 ISP들이 온라인 서비스 제공에 있어 이용자의 본인확인을 적용한 사유, 목적, 방안 등에 대해 조사하고, 조사 결과를 바탕으로 현행 본인확인서비스에서 이슈화 되고 있는 무분별한 본인확인서비스의 적용, 과도한 개인정보의 제공, 이용자의 권리보장 등에 대한 개선 방안을 마련하고자 조사를 진행하였다. 설문조사는 2019년 08월 19일부터 30일까지 국내 ISP들 중 금융, 전자상거래, 포털, 게임, 교육, 공공서비스 사업자들의 개인정보보호책임자 및 담당자들에게 이메일을 통해 조사를 진행하였다. 조사사항에는 현행 대체수단 기반의 본인확인서비스 적용을 최소화하고 무분별한 사용을 억제하기 위해 온라인 서비스 제공 시 적용하는 본인확인 수단의 종류, 목적, 사용방법 등에 대해 현황을 조사하였으며, 대체수단을 온라인 서비스 이용자의 본인확인 목적으로 활용하고 있는 사례를 분석하고, 또한 대체수단을 사용하고 있지 않는 사업자의 현황도 분석하였다.

가. 온라인상에서 대체수단 도입 목적

ISP가 대체수단을 도입하여 적용하고 있는 사유를 파악하고자 설문을 진행한 문항으로, 사업자 입장에서는 다양한 목적으로 본인확인서비스를 적용하고 있으나 실제 해당 사유에 관련 법적 문제가 없는지, 혹은 과도하게 본인확인서비스를 적용하고 있는지 확인하는 과정이 필요하다. 설문조사 결과, 회원가입, 정보변경, 이용자 응대 등 법적 요구사항(청소년, 법정대리인 확인 등) 확인 목적인 경우는 88%, 연동서비스 제공 목적이 50%, 그리고

제공서비스의 안전성 확보가 13%로 조사되었다.

나. 본인확인서비스 적용 이유

최근 대체수단을 사용하지 않는 다양한 사설 본인인증 서비스가 출현하고 있는 상황에서 이메일 인증, 주소 인증, ARS 인증 등을 적용하고 있는 사업자들이 증가하고 있는 상황이다. 관련 법령에서도 대체수단을 이용한 본인확인서비스를 필히 적용하여 이용자를 식별 및 인증하도록 하는 규정은 존재하지 않는 상황이다. 그럼에도 불구하고 ISP들이 대체수단을 이용자 확인에 적용하고 있는 상황으로 실제 다양한 본인인증 수단을 적용하지 않는 사유를 조사한 문항이다. 설문조사 결과, 대체수단 기반의 본인확인서비스가 타서비스 보다 저렴해서가 81%, 타 서비스보다 편리해서 56%, 그리고 기타가 13%로 조사되었다. 조사 결과, 실제 사업자들은 현재의 본인확인서비스가 이용자의 진성 개인정보를 제공해 주는 서비스이며, 향후 법적 문제 발생 시 법적 대항력을 확보할 수 있는 이점으로 많은 사업자들이 현행 대체수단을 이용자 식별 및 인증에 적용하고 있는 상황이다.

다. 대체수단 미 도입으로 인한 우려 사항

대체수단 기반의 본인확인서비스를 적용하지 않아 사업자가 온라인사업 영위에 있어 불편한 사항에 대한 설문 문항이다. 대체수단을 적용하지 않음으로써 온라인 서비스 이용자의 진성 개인정보를 수집할 수 없는 한계가 있음에도 사설 본인인증을 이용하거나 이용자가 입력한 정보 기반으로만 이용자를 식별함으로써 온라인 사업자가 발생 가능한 위험을 수용하고 실제 서비스 관련 위험이 발생할 지라도 모두 처리하고자 하는 방향으로 사업을 진행함을 알 수 있다. 설문조사 결과, 개인정보 도용 등으로 인해 피해 발생을 억제 할 수 없는 것이 대체수단을 미적용 사업자 25%가 응답하였으며, 법적 구속력 미확보와 개인정보 변경 시 실지명의 여부 미확인의 불편함이 6%로 조사되었다.

라. 대체수단 적용 시 고려 사항

대체수단을 온라인 서비스에 적용하고 있지 않으나 향후 대체수단 기반의 본인확인서비스를 온라인 서비스에 적용할 경우 해당 사업자가 고려해야 하는 사항에 대한 문항이다. 즉, 본인확인서비스 미 도입 사업자가 대체수단 도입에 가장 큰 동기가 부여되는 원인을 파악하고자 함에 있다. 설문 조사 결과. 법적 대항력 및 타당성 확보 여부와 타 사업자 제휴가 13%, 이용자 식별(실지명의 확인)이 6%로 조사 되었다.

Ⅳ. 업종별 본인확인 요구사항 분석

ISP들의 본인확인서비스 적용 목적과 이유 등을 조사한 결과, 본인확인을 적용하는 요구에는 법률 준수, 온라인 서비스의 안전성 제공, 그리고 타 사업자와의 서비스 연동을 본인확인의 요구사항으로 도출할 수 있다. 따라서 업종별 본인확인 요구사항에 대해 다음과 같이 분석하였다.

1. 금융

금융 사업자는 관련 법령에 의해 주민등록번호 수집이 가능하다. 그러나 서비스 이용자가 홈페이지를 통하여 회원가입 단계에서 주민번호 입력 없이도 가입할 수 있는 방법을 제공하도록 하고 있다. 그리고 금융 업종의 특성상 회원가입 및 서비스 제공, 본인확인증 및 식별, 부정이용방지, 법정대리인 동의, 분쟁해결, 민원처리 등의 목적으로 개인정보 처리 시 개인을 식별 및 인증하기 위한 요구사항으로 본인확인 서비스를 이용하였다. 그리고 앱카드, 모바일카드 발급을 통한 금융회사와 통신회사 간 자동이체 및 요금할인 서비스 제공, 복지 포인트, 멤버쉽 포인트 연동을 통한 이용자 편의 증진과 은행, 카드, 보험, 저축은행 등 금융 계열사 간 연동 서비스 제공에 대한 요구사항을 충족하기 위한 본인확인을 적용하고 있다.

2. 전자상거래

전자상거래 분야 사업자들은 판매하는 물품 중 청소년에게 유해한 상품에 대해 노출, 유통 등으로 피해가 가지 않도록 예방해야할 의무가 있다. 청소년들에게 유해 매체물들을 제공하는 자는 본인의 나이 및 확인하는 과정이 요구된다. 이러한 법률을 준수하기 위한 요구사항으로 본인확인서비스를 적용하고 있으며, 본인여부, 연령 확인, 부정이용 방지, 맞춤 서비스 제공, 성인 인증, 최초 본인인증 시 정보 자동 업데이트를 목적인 안전성 확보를 위한 요구사항으로 본인확인서비스를 적용하고 있다. 그리고 캐시백, 쿠폰제공 서비스업체 등 포인트 조회 및 전환 서비스 제공, 다양한 페이 등 간편 결제서비스 제공(은행, 카드사 등 금융기관 연동)과 계열사 연동을 위한 요구사항으로 활용하고 있다.

3. 온라인 게임

온라인 게임서비스 사업자는 심야시간대에 인터넷 게임 제공시간 제한과 게임과 몰입 및 중독 예방을 위한 청소년 셧다운제를 적용받는다. 이러한 법률을 준수하기 위한 요구사항으로 회원가입 단계에서 본인확인서비스를 이용하고 있으며, 성인게임물에 대해 성인인증을 위해 본인확인서비스를 이용하고, 만약 만 14세 미만 아동의 게임이용을 위해 회원 가입 시에 법정대리인의 동의를 받아야 하며, 이를 준수하기 위해 본인확인서비스를 적용하고 있다. 또한, 회원가입들에게 특화된 서비스 제공, 부정사용자 확인, 민원과 분쟁 조정을 위한 확인 등의 목적에 부합하기 위한 요구사항으로 본인확인서비스를 적용하고 있다.[1-3] 그리고 채널링 서비스를 제공하는 게임사의 경우, 자사의 회원정보를 게임서비스를 제공하는 업체로 제공 시 개인정보를 제공하기 위한 요구사항 등으로 본인확인서비스를 적용하고 있다.

표 1. 본인확인을 명시한 법령 목록
Table 1. List of laws specifying personal proofing service

내용	관련 법령
청소년 셧다운제	-청소년 보호법 제26조(심야시간대의 인터넷게임 제공시간 제한) -게임산업진흥에 관한 법률 제12조의3(게임과몰입 · 중독 예방조치 등)
게시판 이용자의 본인확인	-정보통신망 이용촉진 및 정보보호 등에 관한 법률 제44조의5(게시판 이용자의 본인 확인)
만 14세 미만 아동의 법정 대리인의 동의획득	-정보통신망 이용촉진 및 정보보호 등에 관한 법률 제31조(법정대리인의 권리) -개인정보보호법 제22조(동의를 받는 방법)
실명확인	-공직선거법 제82조의6(인터넷언론사 게시판 · 대화방 등의 실명확인)
청소년 유해매체물 제공 시 성인확인	-청소년 보호법 제16조(판매 금지 등)
주민번호 대체수단 제공	-정보통신망 이용촉진 및 정보보호 등에 관한 법률 제23조의2(주민등록번호의 사용 제한) -개인정보 보호법 제24조의2(주민등록번호 처리의 제한)

V. 본인확인 요구사항 관련 위험분석

ISP의 본인확인서비스 요구사항을 바탕으로 온라인 서비스 제공 시 본인확인 관련 위험을 식별하였다. 위험분석은 온라인 서비스 사업자가 본인확인 서비스를 이용하는 목적인 법률 준수, 온라인 서비스 안정성, 연동 서비스 제공 분야로 나누어 위험을 분석하였다.

1. 법률 위반에 대한 위험분석

온라인 서비스 제공 시 본인확인 관련 준수해야 할 법령을 정리하면 표 1과 같다. ISP는 제공하는 서비스 및 수집하는 개인정보에 따라 법령 준수에 대한 위험평가를 수행하는 것이 필요하다. 온라인 서비스와 관련된 법령 위반 시 과태료 부과, 이용자 평판 저하 등의 위험이 있다. 따라서 본인확인을 적용하는데 있어 발생 가능한 위험도 판별은 법령 해당 유무에 따라 판단할 필요가 있다. 만약 법률 사항에 해당된다면 가장 높은 등급의 본인확인 수단을 적용하는 것이 요구된다. 온라인서비스에 본인확인 적용에 있어 사업자가 제공하는 서비스 중 법령을 준수해야 하는 서비스가 있는 경우와 아닌 경우로 온라인 서비스를 2 level로 분류할 수 있다.

2. 온라인 서비스 제공 안전성에 대한 위험분석

ISP의 본인확인 이용현황 분석을 통해 온라인 서비스 제공의 안전성에 영향을 주는 위협은 회원제 서비스 제공, 개인 식별, 불량회원의 부정 이용 방지, 비인가 사용 방지, 가입 의사 확인, 연령확인, 불만처리 및 고객상담 등 민원처리, 분쟁 조정을 위한 기록보존, 고지사항 전달 등 업종별 다양한 위협이 조사되었다. 이러한 서비스 제공 시 발생 가능한 위협을 범주화하면 다음과 같다. ① 이용자의 불편함, 이미지에 대한 손상, ② 이용자의 금전적 손실 또는 온라인 서비스 사업자의 배상 책임, ③ 온라인 서비스 사업자의 서비스 제공에 대한 손상, ④ 이용자의 개인정보 노·유출, ⑤ 이용자의 안전에 대한 손상으로 범주화 할 수 있으며, 이렇게 범주화 된 위협의 예시와 영향도를 정의하면 표 2와 같다.

표 2. 본인확인 안정성에 대한 위험의 예시 및 영향도
Table 2. Examples of risks and their impact on personal proofing

① 이용자의 불편함, 이미지에 대한 손상	
낮음	일부 이용자에 영향, 제공 서비스 중 제한적 기능에 단기간의 불편함 초래, 미비한 이용자 이미지 손상
보통	모든 이용자에 영향, 제공 서비스 중 중요 기능에 단기간 또는 장기간 불편함 초래, 이용자 이미지 손상
높음	모든 이용자에 영향, 제공 서비스 중 중요 기능에 장기간 불편함 초래, 심각한 이용자 이미지 손상

② 이용자의 금전적 손실 또는 ISP의 배상 책임	
낮음	이용자에게 중요하지 않은 금전적 손실 또는 ISP의 책임
보통	일부 이용자에게 심각한 금전적 손실 또는 심각한 ISP의 책임
높음	모든 이용자에게 심각한 금전적 손실 또는 치명적인 책임
③ ISP의 서비스 제공에 대한 손상	
낮음	온라인 서비스 사업자의 주 기능을 현저하게 감소시켜 주요 기능을 수행할 수 있는 기간 및 지속 기간에 경미한 손상, ISP의 자산 또는 이용자 전체 이익에 대한 경미한 손상
보통	ISP의 운영, 자산 및 이용자의 이익에 제한된 심각한 악영향
높음	ISP의 운영, 자산 및 이용자의 이익에 심각한 악영향
④ 이용자의 개인정보 노·유출	
낮음	3등급의 개인정보(자동생성정보, 가공된 개인정보, 제한적 본인식별 정보)가 승인되지 않은 이용자에게 제한적으로 공개되어 낮은 영향으로 개인정보 정보가 손실
보통	2등급의 개인정보(개인 식별 정보, 개인 관련 정보)가 승인되지 않은 이용자에게 제한적으로 공개되어 중간 정도의 영향으로 개인정보가 손실
높음	1등급의 개인정보(고유식별정보, 민감정보, 인증정보, 신용정보, 의료정보, 위치정보)가 승인되지 않은 이용자에게 제한적으로 공개되어 높은 영향으로 기밀 정보가 손실
⑤ 이용자의 안전에 대한 손상	
낮음	치료가 필요하지 않은 가벼운 부상
보통	경미한 부상 위험 또는 중증 부상 위험
높음	심각한 부상 또는 사망의 위험

3. 연동 서비스 제공에 대한 위험분석

온라인 서비스 제공 시 타 서비스와 제휴 및 연동하여 이용자의 편의를 증진하거나, On-Off line 매장을 운영 중인 사업자가 각 매장의 회원의 정보를 연동할 때 본인확인이 필요하다. 표 3은 연동 서비스 제공 시 위협과 영향도를 나타낸다.

표 3. 연동 서비스 제공 위협의 예시 및 영향도
Table 3. Examples and impact of connecting service provision threats

① 온라인 서비스 간 연동	
② On-Off line 연동	
낮음	연동 시 3등급 개인정보 제공
보통	연동 시 2등급(이메일 등 개인식별 정보) 개인정보 제공
높음	`연동 시 1등급(고유식별정보) 개인정보 제공

Ⅵ. 차등화된 본인확인서비스 도입방안

온라인 서비스에서 본인확인을 적합하게 적용하기 위해 ISP들은 온라인 서비스에 존재하는 본인확인 관련 법률, 서비스 안전성, 연계 서비스, 그리고 개인정보 측면에서 위험 평가를 수행한다. 위험평가 결과를 토대로 식별된 위험을 감소시키기 위한 본인확인의 보증수준을 매핑한다. 그리고 매핑된 보증수준에 대항하는 본인확인을 위한 인증수단 중 온라인 서비스에 적합한 인증수단을 선택 및 적용한다. 이후 시간이 지남에 따라 신규 위험이 존재하는 지 주기적으로 확인하고, 기존 인증수단보다 발전된 인증수단이 신규로 개발되었는지 확인하고 적용을 검토하는 것이 요구된다. 결국 ISP가 제공하는 서비스의 주요 트랜잭션을 식별하고 각 트랜잭션 별 위험평가 체크리스트를 적용하여 등급을 산정한다. 법률 위반, 온라인 서비스 안전성, 연동 서비스 안전성, 개인정보 처리 위험에 대해 각각 등급을 부여하고 가장 높은 등급을 해당 트랜잭션의 최종 등급으로 부여한다.

1. 온라인서비스 별 등급 산정

등급 부여 방법은 우선, 법률 위반 위험은 해당 여부로 나눌 수 있으며, 해당 항목이 하나 이상이면 가장 높은 3등급 인증 보증수준을 부여한다. 온라인서비스 제공 안전성 위험은 낮음, 중간, 높음으로 영향도를 나누고 가장 높은 등급으로 전체 등급을 부여한다. 연동서비스 제공 서비스가 있으면 3등급 보증수준을 부여한다. 그리고 개인정보 처리 위험은 처리하는 개인정보의 등급에 따라 인증 보증 수준을 결정한다. 1등급을 처리하면 3등급 보증수준을 부여한다. 표 4는 온라인 서비스에 본인확인을 적용하는 위험평가 항목을 나타낸다.

표 4. 본인확인 이용 시 적용하는 위험평가 항목
Table 4. Risk assessment items that apply when using personal proofing

위험평가 항목			
① 법률 위반 위험	영향도		
	미 해당		해당
가. 청소년 셧다운제			
나. 게시판 이용자의 본인확인			
다. 만 14세 미만 아동의 법정 대리인의 동의 획득			
라. 실명확인			
마. 청소년 유해매체물 제공 시 성인 확인			
바. 주민등록번호 대체 수단 제공			
② 온라인 서비스 제공 안전성 위험	영향도		
	낮음	중간	높음
가. 회원제 서비스 이용에 따른 본인확인			
나. 불량 이용자의 재가입 방지			
다. 가입의사 확인			
라. 연령 확인			
마. 불만처리 및 고객 상담 등 민원처리			
바. 포인트 적립/사용 등 멤버십 필수 서비스 제공			
사. 모든 당사자에게 심각한 경제적 손실			
③ 연동 서비스 제공 안전성 위험	영향도		
	미 제공		제공
가. On-Off 연동 서비스			
나. 멤버십 포인트 등 연동 서비스 제공			
④ 인증 완료 후 처리하는 개인정보	영향도		
	미 처리		처리
가. 1등급 개인정보 처리			
나. 2등급 개인정보 처리			
다. 3등급 개인정보 처리			

표 5. 보증수준 별 본인확인 인증수단의 유형
Table 5. Types of personal proofing methods for each level of assurance

요구 사항	1등급	2등급	3등급
허용된 인증수단 유형	암기된 비밀 룩업 비밀 대역 외 장치 단일 요소 OTP 장치 다중 요소 OTP 장치 단일 요소 암호화 소프트웨어 단일 요소 암호화 장치 다중 요소 암호화 소프트웨어 다중 요소 암호화 장치	다중 요소 OTP 장치 다중 요소 암호화 소프트웨어 다중 요소 암호화 장치 암기된 비밀에 다음 인증수단 추가 - 룩업 비밀 - 대역 외 장치 - 단일 요소 OTP 장치 - 단일 요소 암호화 소프트웨어 - 단일 요소 암호화 장치	다중 요소 암호화 장치 단일 요소 암호화 장치 + 암기된 비밀 단일 요소 OTP 장치 + 다중 요소 암호화 장치 또는 소프트웨어 다중 요소 OTP 장치 + 단일 요소 암호화 소프트웨어 + 암기된 비밀

2. 인증수단 선택 및 적용

온라인 서비스 트랜잭션의 인증 보증수준이 결정되면 해당 보증 수준에 허용된 인증수단 중 이용자 접근성, 구현 편의성 등을 고려하여 적용한다. 온라인 서비스 사업자가 직접 인증수단을 등록 및 배포하거나, 본인확인서비스 사업자의 서비스를 이용하여 적용한다. 표 5는 표 4를 통해 도출된 위험등급에 따른 보증수준별 본인확인 인증강도를 충족하는 인증수단을 제시한 것이다. 사업자들은 본인확인 적용 유무와 더불어 본인확인 적용 시 보증수준에 따른 인증강도 수준을 선택할 수 있고 이러한 단계를 통해 획일적인 대체수단 기반의 본인확인서비스 적용이 아닌 다양한 인증수단들을 복합적으로 적용할 수 있게 된다. 이를 위해 차등화된 본인확인서비스 적용을 위한 제도적인 방안이 마련되어야 하고, 본인확인 적용 가이드라인 등을 배포함으로써 본인확인서비스 적용을 최소화하며, 온라인 사업자의 사업 영위에 발생 가능한 위험들을 최소화하는 방안을 제시할 수 있다.

V. 결 론

본 논문에서는 ISP들이 온라인서비스 제공 시 본인확인서비스를 적용함에 있어 적절한 본인확인 인증수단을 적용할 수 있는 방안을 제시하였다. 본 연구에서는 본인확인서비스 적용 시 본인확인 필요한 서비스인지를 평가하고 발생 가능한 위험을 최소화하기 위한 보증수준별 본인확인 인증수단을 적용하는 방안을 제안한다. 제안한 방안을 통해 과도하게 대체수단 기반의 본인확인서비스의 적용이 타당한지 검토함으로써 다양한 인증수단을 활성화 시킬 수 있으며, 보증수준별 요구하는 본인확인 수단의 인증강도에 따라 개인정보도 차등하여 제공받을 수 있어 과도한 개인정보 수집 이슈도 해결할 수 있을 것이다.

References

[1] Young-Jin Shin, Seung-Ho Shin, Ja-Seung Lee, Wong-Ki-Han, "A Study on Improvement of Identification Means in R.O.K", J. of Korean association for regional information society, Vol. 18, No. 4, pp. 59-88, 2015.

[2] Jong-Bae Kim, "Safety Improvement Methods of Personal Identification Services using the i-Pin", J. of Information Technology Service, Vol. 16, No. 2, pp. 97-110, 2017.
DOI: https://doi.org/10.9716/KITS.2017.16.2.097

[3] Jong-Bae Kim, "A Study on Improvement of Personal Identity Proofing Service(PIPS) Based on Alternative Methods of Resident Registration Number", J. of the Korea Society of Digital Industry and Information Management, Vol. 15, No. 2, pp. 29-42, 2019.

[4] Suk-Jin Kang, A study on problem analysis and improvement of identity verification on internet using I-PIN, PhD. thesis, Korea University, 2017.

[5] Young-Do Joo, Young-Hwa An, "Security Improvement of Remote User Authentication Scheme based on Smart Cards", J. of Institute of Internet, Broadcasting and Com., Vol. 11, No. 5, pp. 131-1375, 2011.
DOI: https://doi.org/G704-001948.2011.11.5.015

[6] Seungchul Park, "Evolution of PKI internet Banking in Korea", Int. J. of Advanced Smart Convergence, Vol. 8, No. 1, pp. 44-57, 2019.
DOI: https://doi.org/10.7236/IJASC.2019.8.1.44

[7] Jung-Oh Park, Byung-Wook Jin, "A Study on Authentication Method for Secure Payment in Fintech Environment," J. of Institute of Internet, Broadcasting and Com., Vol. 15, No. 4, pp. 25-31, 2015.
DOI: https://doi.org/10.7236/JIIBC.2015.15.4.25

[8] Woo-Min Shim, "Articles : Issues and Alternatives on Internet Identification: Analysis on the Basis of Architectural Regulation Theory", Korean journal of law & society, Vol. 47, No. 1, 2014.

[9] Jong-Bae Kim, "Online personal proofing trends and implications", 2018, Privacy Fair, Track B, 2018.

[10] Jong-Bae Kim, "Suggestion from Trends of Digital Identity Proofing ", Proc. of korean academic society

of business administration, pp. 376-385, 2018.

[11] Nam-Yun Kim, "Automatic Client Authentication Method in All-In-One Services", J. of the Institute of Internet, Broadcasting and Com., Vol. 16, No. 1, pp. 1-5, 2016.
DOI: https://doi.org/10.7236/JIIBC.2016.16.1.1

[12] Jong-Youel Park, "A Study on the Automated Design of Business Card for Personal Information Leakage Prevention Using IT-based Convergent Service", Int. J. of Internet, Broadcasting and Com., Vol. 10, No. 4, pp. 25-30, 2018.
DOI: https://doi.org/10.7236/IJIBC.2018.10.4.25

[13] Hyungkuy Yang, "An Improved Smart Card-based User Authentication Scheme with Session Key Agreement for Telecare Medicine Information System", Int. J. of Internet, Broadcasting and Com., Vol. 9, No. 3, pp. 35-43, 2017.
DOI: https://doi.org/10.7236/IJIBC.2017.9.3.35

[14] Seung-Jae Kim, "Study on Detection and Recognition of Facial Area using Linear Discriminate Analysis", Int. J. of Advanced Smart Convergence Vol, 7, No. 4, pp. 40-49, 2018.
DOI: https://doi.org/10.7236/IJASC.2018.7.4.40

저 자 소 개

김 종 배(정회원)

- 2000년 : 부산대학교 컴퓨터공학과 학사(공학사)
- 2002년 : 경북대학교 컴퓨터공학과 (공학석사)
- 2004년 : 경북대학교 컴퓨터공학과 (공학박사)
- 2006년 ~ 2019년 : 서울디지털대학교 컴퓨터공학과 교수
- 2019년 ~ 현재 : 세종사이버대학교 부교수
- 주관심분야 : 온라인서비스, 정보보호, 인공지능