**머리말**

전세계적으로 4차 산업혁명으로 인한 산업구조 지형의 변화가 예상되는 가운데

빅데이터, 인공지능(AI), 블록체인, 사물인터넷(IoT) 등 디지털 기술발전이 진전되면서 금융은 4차산업 신기술과의 융합이 용이하고 혁신 속도가 빨라 급속한 변화가 한층 가속화될 전망이다.

금융위는 2015년 공인인증서 의무사용 폐지 등**[[1]](#footnote-1)** 전자금융 관련 각종 규제를 폐지 또는 완화하였다. 이에 인터넷 전문은행과 비대면 실명확인을 허용하면서 비대면 채널을 통해 제공되는 금융서비스의 활성화는 더욱 탄력을 받고 있다.

<IT․금융 융합 지원방안(‘15.1.27) 주요내용 >

비대면 실명확인의 허용으로 고객은 금융거래를 위해 지점을 방문하지 않고 스마트폰

등의 모바일기기를 이용하여 원하는 시간에 편리하게 금융서비스를 이용할 수 있게 되었다. 하지만 현재 대부분의 금융회사에서 비대면 실명확인의 추가 방식으로 휴대폰 본인확인을 이용하고 있으나 이러한 방식에 대해서는 안전성에 대한 신뢰가 높지 않다.

금융IT 보안 패러다임이 금융회사 책임하에 자율적 보안체계를 적용 할 수 있도록 변화함에 따라 금융회사는 자체적으로 사용자, 서비스, 접근매체, 보안수준 등 금융거래 특성을 고려하여 강화된 보안체계의 수립이 필요하다. 특히 비대면 계좌개설 서비스를 시작한 해외 이용 현황과 비교·분석하여 향후 비대면 실명확인 방식의 안전성 확보를 위해 필요한 추가 조치사항을 도출하고자 한다.

**1 금융실명제 도입**

금융거래를 위한 실명확인은 실지명의에 의한 금융거래를 실시하고 그 비밀을 보장하여 금융거래의 정상화 및 경제정의를 실현하기 위하여 금융실명법에서 의무화하고 있는 제도이다. 금융실명제가 도입되기 전까지는 국민저축을 늘리기 위해 비실명 거래를 법적으로 허용하였으나, 금융실명제의 시행은 1993년 8월 12일 이후의 모든 금융거래에 전격 도입되었다. 긴급명령의 주요 내용으로는 모든 금융회사와 거래를 할 때 반드시 실명을 사용하여야 하며, 금융회사는 명의자의 동의 없이 다른 사람에게 금융거래 정보를 누출하지 않게 하여 금융거래 정보의 비밀이 철저히 보장되도록 하는 것이 포함되었다. 금융실명제는 대통령 긴급재정경제명령체제로 약 3년 5개월간 실시된 후 1997년 12월 31일 법률로 대체 입법되었다.

**2 비대면 실명확인 허용**

2015년 5월에 열린 제3차 금융개혁 회의에서는 IT와 금융의 융합에 따른 새로운 금융

서비스 창출 방안을 심의 확정하고 동 회의의 결과로 금융회사가 고객을 비대면으로

실명확인 할 수 있는 길을 열어 핀테크 시장 활성화의 기반을 마련하였다. 이후 비대면

실명확인 방법을 구체화한 “비대면 실명확인 관련 구체적 적용방안”8)을 배포하여 금융

회사에서 관련 업무를 대비할 수 있도록 하였다.

**금융위원회의 비대면 실명확인 방식 주요 내용**

|  |  |
| --- | --- |
| 구분 | 설명 |
| 금융거래의 범위 | •금융실명법상 실명확인 의무가 적용되는 모든 거래 |
| 금융거래자의 범위 | •명의자 본인에 한정(대리인 제외)•법인도 가능(대면 확인 권유) |
| 실명확인증표 | •주민등록증, 운전면허증, 여권(예정)•추가 인정대상 증표 확대 검토 |
| 강화된고객확인의무\*준수 | •금융회사는 거래목적, 자금의 원천 등 확인 |
| 실명확인자 | •해당 금융회사 (시스템적으로 자동화되어 업무절차가 진행되는 경우)•날인 또는 서명 불필요(자동화된 실명확인 방식의 경우) |
| 각종 기한 | •절차 완료 기한 : 30일(휴일 포함)•증빙자료 보존 기한 : 계좌 해지 후 5년 |

※ 출처: 전국은행연합회.금융투자협회, 비대면 실명확인 관련 구체적 적용방안, 2015. 10.

**3 전자금융서비스 - 비대면 채널 이용 현황**

국내 인터넷뱅킹서비스 이용현황[[2]](#endnote-1) (하단 표1)을 보면 2015년 12월 이후 대정부 차원에서 비대면 실명확인을 통한 계좌개설을 허용하는 등 변화하는 환경에 적응하고 있다. 2017.9월말 현재 국내 금융기관에 등록된 인터넷뱅킹(스마트폰뱅킹 포함) 고객수 1억 3,246만명으로 전분기말 대비 4.3% 증가하였다. 이후 약 1년간 총 73.4만개의 계좌가 비대면 방식으로 신규 개설되었으며, 로보어드바이저, 인터넷전문은행의 출범, 보험 및 펀드의 온라인 판매와 같이 다양한 비대면 금융 거래가 확대되고 있다.

핀테크시장의 활성화를 통해 온라인 금융시장 진입장벽 완화로 인터넷전문은행이 본격적으로 영업을 개시[[3]](#endnote-2) 하였다. 케이뱅크 (‘17.4월 기준) 고객 73만명, 수신액 1조 587억, 여신액 8,138억원, 카카오뱅크 (’17.7월 기준) 고객 584만명, 수신액 4조 7406억, 여신액 4조 4796억으로 비대면 채널의 효과를 충분히 확인할 수 있다.

**4 비대면 채널의 증가 추세**

스마트폰 보급 확대에 따른 비대면 채널의 비중이 지속적으로 증가하고 현금 입출금을 제외한 대부분의 금융업무를 인터넷 뱅킹에서 수행할 수 있다는 것이 중요한 원인으로 작용한 것으로 보인다. 이러한 비대면 채널의 증가 추세는 비대면 실명확인의 전자금융서비스 활용과 맞물려 앞으로도 지속될 것으로 전망된다.

|  |
| --- |
|  |

**5 국내 비대면 실명확인 방식 및 이용 현황[[4]](#endnote-3)**

금융당국은 비대면 실명확인 방안으로 실명확인증표 사본 제출, 영상통화, 접근매체 전달과정 확인, 기존계좌 활용 및 기타 이에 준하는 방법 등 5개를 선정하였고, 그 중에서 금융회사가 자율적으로 2개 이상을 선택하여 적용하도록 의무화하였다. 또한 금융당국은 타 기관 확인결과 활용, 다수의 개인정보 검증의 2가지 방법 중에서 선택적으로 추가 확인하도록 권고하였다. 따라서 금융회사가 2가지 이상의 실명확인 방식을 적용하고 자체적으로 추가 확인을 실시함으로써 다중의 검증과정으로 확인하였다면 금융실명법상의 실명확인 의무를 준수한 것으로 판단할 수 있다고 해석하였다.



**6 해외 비대면 실명확인 방식 및 규제 현황**

비대면 실명확인 방식에 대한 본격적인 논의와 시행이 이루어진지 1년여 밖에 되지 않는 국내와는 달리 해외에서는 이미 수년 전부터 비대면 계좌개설 서비스를 제공하고 있다. 해외 사례에서는 비대면 실명확인으로 신분증 사본 제출, 우편을 통한 접근매체 전달, 영상통화, 계좌이체, 개인정보 확인 등 다양한 비대면 확인 방식을 제공하고 있으며 안전성확보를 위해 추가 인증방식을 중복 적용하고 있다.

해외 비대면 실명확인 방식[[5]](#endnote-4)

|  |  |
| --- | --- |
| **방 식** | **실명확인 절차** |
| 다수의 개인정보 검증(Charles Schwab Bank, 미국) | ① 인터넷뱅킹 접속 및 계좌개설 신청서 작성(이름, 주소, 사회보장번호,운전면허증, 고용정보 등)② 입력 정보 신원조회(신용평가기관)③ 전화를 통해 고객정보 확인④ 계좌개설 및 요청시 접근매체 우편 송부 |
| 실명확인증표수집(UBank, 호주) | ① 인터넷뱅킹 접속 및 회원가입 후 기본정보 입력(이름, 생년월일, 휴대폰번호,운전면허증 번호, 이메일 등)② 실명확인증표 정보 입력(2개 이상)③ 실명확인증표 발급기관을 통해 진위 여부 확인④ 확인 완료 및 계좌 개설 |
| 접근매체 전달과정에서 확인(Seven Bank, 일본) | ① 인터넷뱅킹 접속 후 계좌개설 신청서 작성(이름, 주소, 휴대폰번호, 이메일 등)② 본인 한정 우편을 통해 접근매체 송부③ 고객은 배달원에게 사진이 부착된 실명확인증표를 제시해 본인확인 후우편물 수취④ 금융회사는 배송 완료 여부를 확인해 거래 허가 |
| 실명확인증표 사본 제출(Jibun Bank, 일본) | ① 인터넷뱅킹 접속 후 계좌개설 신청서 작성(이름, 주소, 휴대폰번호, 이메일 등)② 실명확인증표 사본 제출(스마트폰 앱, 인터넷뱅킹 사이트, 우편 등 이용)③ 실명확인증표 확인 후 접근매체 송부④ 우편 수취 및 거래 개시 |

해외 주요국의 비대면 실명확인은 자금세탁방지 관련법에 법적 근거를 두고 있다. 미국은 일찍이 1970년부터 Bank Secrecy Act에서 비대면으로 계좌를 개설하는 보안요건을 명시하고 있다. 최소한의 보안요건을 만족시키는 가이드라인15)을 제공하고 이를 만족하는 인증기술을 자율적으로 선택할 수 있기 때문에 다른 해외사례와 다르게 특정한 인증방식을 규정하지 않는 점은 주목할 만하다. 반면에 독일은 여느 국가와 다르게 비대면 실명확인을 법으로 금지하고 있으며 타 은행에 실명확인 업무를 위탁하여 확인하는 방식에 한정하여 비대면 계좌개설을 허용하고 있다.

해외 주요국 비대면 실명확인 규제 현황

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **국 가** | **미국** | **일본** | **영국** | **독일** | **호주** |
| 비대면허용여부 | 보안요건충족 시허용 | 고객확인절차 수용시 허용 | 추가인증시 허용 | 법으로 금지(위수탁 가능) | 허용 |
| 근거법령 | BankSecrecy Act(1970) | 범죄수익이전예방법(2007) | MoneyLaunderingRegulations(1994) | GermanAnti-moneyLaundering(1993) | Anti-Money Launderingand CounterTerrorism Financing Act(2006) |
| 내용 | 최소 요구사항 충족,대면 확인대비 보안강화 | 신분증 수신,우편확인,거래목적,직업 등확인 | 전화연락,우편송부,신원보증서수취 등추가 인증의무 | 타은행에실명확인업무 위탁 | 사용가능한신분증목록 명시 |

**7 비대면 서비스분야 위험**

인터넷 전문은행의 경우에도 금융시장의 안정성 확보가 금융소비자 보호측면에서 매우 중요하다. 한편 인터넷전문은행은 일반은행과는 달리 전산시스템으로 운영되는 특성상 자본금 규모 대비 상대적으로 높은 투자비용으로 인해 영업초기 부실화의 가능성이 있다. 인터넷전문은행이 일반은행과 동일한 업무를 영위하면서 모든 금융서비스가 비대면거래를 통해서만 제공되는 경우 오히려 금융소비자 보호가 취약해질 우려가 있다.

인공지능의 잠재적 위험이 있다. 특히 정확성 문제의 경우 인공지능의 정확성은 학습에 사용되는 데이터와 알고리즘의 신뢰성 따라 달라질 수 있어서 부정확한 데이터 및 알고리즘의 오류로 인해 인공지능을 적용한 시스템의 오류발생 가능하다. 비대면이나 인공지능으로 신용평가시 부정확한 신용평가로 인한 부실대출 발생이 가능하다. 결정적으로 정상거래가 이상금융거래로 판단되어 차단되거나 고객응대 서비스 품질의 하락으로 민원 발생여지가 분명히 존재한다.

**8 비대면 거래 보안위험** 비대면 실명 확인과 개인정보 보호

비대면 계좌개설 허용으로 가장 우려되는 보안위험 요소 중 하나는 불법 대포통장 개설이다. 대부분의 금융회사에서 비대면 실명확인 방식으로 실명증표 사본 제출과 기존계좌 활용을 채택하고 있기에 본인명의의 계좌가 하나만 있어도 다수의 대포통장을 개설할 수 있는 위험이 있다.

기술적 보완에도 불구하고 비대면이라는 제약사항으로 인해 비대면 실명확인이 정확하게 이루어지기에는 많은 어려움과 위험요소가 있을 수 있다. 비대면 실명확인시스템을 도입.운영하기 위해서는 은행연합회와 금융투자협회에서 마련한 비대면 실명확인 관련 구체적 적용방안에 따라 시스템을 구축하고 시스템 안전성 및 보안성 테스트를 충분히 수행한 후 서비스를 실시해야 한다.

비대면 실명확인 방식의 위험요소[[6]](#endnote-5)

|  |  |
| --- | --- |
| **실명확인 방식** | **도입사례** |
| 실명증표사본 제출 | •주민등록번호 입력이나 실명증표 촬영후 저장된 메모리에서 정보 노출 위험•실명증표 촬영을 위한 카메라 구동시 악성앱 호출 위험•캡처 및 백그라운드 스크린샷을 통해 화면정보 유출 위험•실명증표 및 관련정보 전송시 평문 전송 위험•실명증표 전송시 악성파일 전송 위험과 대용량 파일을 전송하여 서비스거부 공격 위험 |
| 영상통화 | •피싱 공격에 의해 연결된 공격자에게 인증정보 전달 위험•영상통화 화면 외부에서 공격자의 위협에 의한 사용자 위험 |
| 접근매체전달시 확인 | •접근매체 전달 위탁업체의 부정행위 위험•공격자가 위탁업체 직원으로 위장한 개인정보(신분증 사본, 서명 등) 유출 위험 |
| 기존계좌 활용 | •고객이 본인의 계좌에서 타인의 계좌로 이체하도록 하는 피싱 위험 |
| 기타 이에준하는 방법 | •저장된 바이오정보의 유출 위험•신규 실명확인 방식 도입에 따른 위험 |
| 타 기관확인결과 활용 | •타 사용자의 식별정보를 입력하여 인증정보 획득 위험•식별정보의 평문 전송과 재사용 위험 |
| 다수의개인정보 검증 | •중요 개인정보의 평문 전송 위험•타 사용자의 개인정보를 이용한 인증 위험 |

**9 안정적 비대면 실명확인 확보를 위한 조건**

바이오정보의 안전한 저장 및 다중 인증기술 도입

스마트폰의 사용권한을 획득하기 위해 지정된 패턴이나 비밀번호를 입력해오던 과거와

달리 최근에는 지문인식 센서를 탑재하여 본인의 지문을 이용하여 보다 쉽고 편리하게

접근할 수 있게 되면서 바이오정보가 일반 사용자에게 친숙하고 안전한 인증기술로 인식

되고 있다.

전자금융서비스를 보다 편리하게 이용하고자 하는 고객의 욕구와 안전한 비대면 금융거래 환경을 제공하고자 하는 금융회사의 의지가 서로 맞물려 전자금융서비스에 바이오정보를 활용하는 계획이 적극적으로 추진되고 있다.

바이오인증 수단 특징 및 적용 사례[[7]](#endnote-6)

|  |  |  |
| --- | --- | --- |
| **구분** | **특징** | **도입사례** |
| 지문 | •대중적인 바이오인증 기술•간편결제 업체들 채택 활발•시스템 구축비용이 상대적으로 저렴 | •삼성페이•애플페이•우리은행 ATM•농협은행인 |
| 정맥 | •일본, 유럽 등 금융사 채택 활발•손가락, 손등, 손바닥 등 취득부위 다양•비접촉식으로 사용자 거부감이 적음 | •신한은행 디지털키오스크•일본 교토, 미즈호,미츠이스미토모은행 |
| 홍채 | •비접촉식이지만 다른 신체부위보다비교적 민감한 부위라 거부감 존재•IBK기업은행 등 은행권 검토 가시화 | •IBK기업은행 ATM•스위스 UBS은행•카타르 QAB•시티은행 출입통제 |
| 얼굴 | •비접촉식으로 사용자 거부감이 적음•행자부 등 기준 정보 비교 가능•고객 소유 디바이스 활용 가능•중국 알리바바 결제 | •프랑스 헬로뱅크•미국 찰스 슈어브뱅크 |
| 음성 | •타 바이오인증과의 결합이 용이•편의성 높음•고객 소유 디바이스 활용 가능렴 | •미국 US뱅크•캐나다 TD뱅크 |

금융회사에서는 모바일뱅킹, ATM, 결제 등 다양한 금융서비스에 바이오정보를 도입하여

고객에게 제공하기도 한다. 단일의 바이오정보를 이용한 인증기술의 경우 시각장애, 지문손실 등 선.후천적 장애로 인하여 서비스를 이용하지 못하거나 정보 유출시 재사용이 불가능하다는 단점이 있다. 이러한 단점을 극복하고 범용성과 안전성을 보장하기 위하여 바이오정보를 다중으로 사용하거나, 다수의 개체를 추출하여 인식정보로 가공하거나, 데이터를 추출하는 알고리즘 및 인식 장치를 다중으로 사용하는 등 바이오정보를 활용한 인증기술의 도입 시 다양하게 활용할 수 있는 복합인식 모델의 적용을 고려해 볼만 하다.

복합인식 모델 특징

|  |  |  |
| --- | --- | --- |
| **분류** | **특성** | **비고** |
| 다중 바이오정보 | 적어도 2개 이상의 다른 바이오정보 데이터를 인식(예: 얼굴 + 지문) |  |
| 다중 개체 | 같은 바이오정보로부터 다수의 개체를 획득(예: 오른쪽홍채 + 왼쪽 홍채, 오른쪽 엄지 지문 + 왼쪽 엄지 지문) |  |
| 다중 알고리즘 | 단일 개체 바이오정보에 다른 인식 알고리즘을 적용 | S/W 기반 |
| 다중 센서 | 단일 개체 바이오정보에 여러 개의 센서들을 사용 | H/W 기반 |
| 다중 샘플 | 단일 개체의 바이오정보 데이터에 대해서 몇 개의대표적인 것과 함께 추출된 정보 | 사용자 입력기반 |

**10 결론**

사이버보안역량 강화

과거의 금융서비스플랫폼은 ‘영업점에 방문해 직원과 상담하는 모습’이었기 때문에, 상대적으로 물리적 보안이 중요했다고 할 수 있다. 즉, ‘문 잘 잠그기’가 중요한 보안역량 이었다. 그러나 비대면 금융플랫폼으로 변화된 환경하에서는 물리적인 보안보다 사이버보안이 더욱 중요해졌다. 특히, 사물인터넷으로 연결성이 강화되고, 클라우드 기반의 금융서비스를 제공하며, 빅데이터에 기초해 맞춤형서비스를 제공하는 과정에서 다양한 금융정보나 개인정보의 유출 우려가 있다. 물리적 보안위협은 단순히 영업점의 업무를 마비시킬 수 있지만, 사이버 보안위협은 금융사의 전체업무를 마비시킬 수 있다.

각 금융사별로 노출될 수 있는 바이러스, 외부해킹, 보안패치 미적용, 무단외부접속, 내부직원의 규정위반 등의 사이버위협의 유형들을 조사하고, 이를 예방하거나 문제 발생시 조기에 대응할 수 있는 사이버 보안시스템을 확충할 필요가 있다. 특히, 모바일 보안기능으로, 백신, 플랫폼 해킹탐지, 앱 위 변조 방지, 생체인증, 보안 키보드 등이 도입되고 있는바, 비대면 플랫폼 구축노력과 함께 사이버 보안기술을 확보하는 노력이 병행될 필요가 있다.

1. <금융위원회 IT․금융 융합 지원방안(‘15.1.27) 주요내용 >

❶ (규제 패러다임 전환) IT‧금융 융합을 활성화하도록 규제의 틀을 전환

**❷ (오프라인 위주 금융제도 개편) 온라인‧모바일 환경에 맞게 금융제도 개선**

❸ (핀테크 산업 육성) 자금조달 지원 및 전자금융업 진입장벽을 완화

**❹ (소비자 보호) 선진형 규제방식(사후점검 + 책임 명확화)으로 보안 강화** [↑](#footnote-ref-1)
2. 기획재정부 한국은행 2017. 3/4분기 국내 인터넷뱅킹서비스 이용현황 [↑](#endnote-ref-1)
3. 기획재정부 범부처 합동 「2018 대한민국 혁신성장 보고대회」 2018.05.24. [↑](#endnote-ref-2)
4. 전국은연합회ㆍ금융투자협회, 비대면 실명확인 관련 구체적 적용방안, 2015. 10.

“[‘대면’부르는 비대면 계좌 개설 서비스①]10명 중 4명은‘헛발질’”, 헤럴드경제(2016.5.30자 기사), [↑](#endnote-ref-3)
5. 금융연구원, 한국형 인터넷전문은행 도입방안, 2015. 4. [↑](#endnote-ref-4)
6. 김현민 . 이진호, 카드사 대체 인증기술 보안성 비교 분석, 전자금융과 금융보안 제4호(금융보안원 2016. 4), [↑](#endnote-ref-5)
7. ‘생체인증’, 금융 차세대 보안수단으로 뜬다, 2016 Annual Report(디지털데일리, 2016. 6.), [↑](#endnote-ref-6)