Journal of Digital Convergence
Vol. 19. No. 5, pp. 229-239, 2021

ISSN 2713-6434 / eISSN 2713-6442
https://doi.org/10.14400/JDC.2021.19.5.229

국내 전자금융의 환경 변화와 그 과제
-전자금융의 변화 전망과 시사점을 중심으로-

김대현
동국대학교 법학과 박사수료

Changes in the environment of electronic finance and its challenges
-Focusing on the prospects and implications of changes in electronic finance-

Daehyun Kim
Ph. D. Candidate, Department of Law, Dongguk University

요 약 본 연구를 위하여 정부의 금융관련 부서의 발표자료와 각 금융기관 및 전자금융 관련 기관의 자료를 광범위하게 분석한 결과, 우리나라의 전자금융 환경에 있어 첫째) 비대면 금융의 확대, 둘째) 금융권의 원격근무, 셋째) 공인인증의 폐지, 넷째) 고도화되는 보이스피싱, 다섯째) 금융산업의 개방과 형태의 다양화, 여섯째) '지갑 없는 사회'의 도래 등의 실제적 변화가 나타나고 있다. 하지만 이상의 문제 외에도 예를 들어, 4차 산업혁명으로 촉발된 전 세계적 변화는 금융보안 분야에도 전파되어, 인공지능 기술 / 딥러닝 기술 / 사용자 분석 기술 / 딥페이크(deepfake) 기술 등과 같은 문제는 특히 대응하기 어려운 위험요소이다. 전자금융은 사회적으로 점점 그 비중이 확대되고 있는 만큼, 전자금융과 그 환경의 문제 및 그로 인한 범죄와 범죄 수사의 분야까지도 꾸준하게 연구되어야 마땅하다.

주제어 : 전자금융, 금융보안, 비대면 금융, 보이스피싱, 원격근무

Abstract For this study, we have extensively analyzed the presentation data of the government's financial-related departments and the data of each financial institution and electronic financial institution.. As a result, In Korea's electronic financial environment, real changes such as first) expansion of non-face-to-face finance, second) teleworking in the financial sector, third) abolition of accredited certification, fourth) advanced voice phishing, fifth) openness of the financial industry and diversification of forms, sixth) the'walletless society'. In addition to the above, however, global changes triggered by the Fourth Industrial Revolution spread to the financial security sector, making it difficult to respond to problems such as artificial intelligence/ deep learning/ user analysis/ deepfake technology. As the proportion of electronic finance is increasing socially, it should be studied in the fields of electronic finance and its environment, and crime and criminal investigation.

Key Words : Electronic finance, Financial security, Non-face-to-face finance, Voice phishing, Telewor

*Corresponding Author : Daehyun Kim(kim_dhyun@naver.com)
Received March 22, 2021 Revised April 27, 2021
Accepted May 20, 2021 Published May 28, 2021

1. 서론

현재 우리나라의 금융 상황을 한마디로 특징 짓는다면 '컨버전스(convergence) 금융'이라고 할 것이다. 업종 간의 장벽 해제, 겸업화, 대형화, 통합화, 인터넷 은행 등으로 설명할 수 있는 이 상황은 앞으로도 다분히 빠르게 지속될 것은 물론, 사상 초유의 'Covid-19' 팬데믹 사태로 인한 언택트(untact ; noncontact ; zero contact) 상황과 맞물려 전통적인 은행과 함께 전체 금융권은 이과도기적인 경영환경에 슬기롭게 대응하기 위한 방안 마련에 고민하고 있다. 컨버전스 금융을 경쟁, 시장, 규제, 소비자, IT 등의 차원에서 살펴보면 그 변화의 영향과 속도를 더욱 실감할 수 있다.

먼저, 금융규제와 시장의 입장에서는 리스크 관리에 대한 강화·방카슈랑스(Bancassurance)의 정착·은행 간 통합·소비자 및 수요자 위주의 시장 심화·외국계 금융회사의 진출 확대 등과 같은 특징이 확연하게 나타나고 있으며, 업종 간 또는 금융이 아닌 다른 업종과의 경쟁과 협력관계도 빠르게 형성되고 있다[1]. 또한 소비자의 입장에서는 은행·보험·증권 사이에 놓인 상품 장벽의 해소를 강력하게 바라고 있으며, 리스크 요소와 수익 요소에 있어서 보다 자세한 정보의 제공을 요구하고 있다. 그리고 IT 부문에서는 대량 및 고속 데이터 처리·인터넷 환경의 초고도화·무선 네트워크 환경을 넘어선 유비쿼터스(ubiquitous) 금융으로의 진입에 이르렀으며, 한편으로는 정보시스템의 무중단·무재해 요구에 당면해 있다[2]. 그리고 국내외적으로는 경영에서의 투명성 증진을 위한 각종 권고와 규제가 많아지면서 이에 적응하기 위한 IT 컴플라이언스(compliance)가 주목을 받고 있다.

전자금융에는 다양한 요소들이 있다. 이러한 요소들 중에서 특히 중요한 내용들을 살펴보면, 가장 먼저 효율성을 들 수 있다. 훌륭하게 구성되었다고 할 수 있는 IT 시스템은 해당 조직의 경영에 필요한 기능을 충분히 필요한 만큼 효과적으로 제공하여야 한다. 하지만 보다 중요한 것이 있다면 안전성이다. 아무리 효율성이 뛰어난 시스템이라고 해도 잦은 장애는 조직의 기능을 마비시켜 과거의 수작업 시대보다도 못한 결과를 야기한다. 또한 서비스 마비는 동반하지 않더라도 금융기업에서의 IT 시스템 사고는 기업에 대한 신뢰도와 고객에 대한 금전적 피해에 있어 막대한 손실을 발생시킨다[3]. 특히 최근에 빈번히 발생하고 있는 정보 유출 사고나 해킹에 의한 고객의 금전적 피해는 피해 금액의 많고 적음을 떠나 해당 기업에게는 심각한 경영 위험요인이 되고 있다.

특히 특정 금융기업이나 일정 기업에서의 개인정보 해킹 및 유출은 단순하게 해당 기업에서의 문제로 국한되지 않고, 유출된 개인정보가 다른 금융기업이나 각종 인터넷 사이트에 사용되어 또 다른 범죄와 피해를 발생시키기 때문에 커다란 사회적 문제를 일으키게 된다. 즉, 현재의 모든 일상이 컴퓨터와 인터넷으로 연결되어 있고 각종 디바이스(device)에서 사용되는 개인정보가 제법 유사한 경우가 많음에 따라 하나의 기업이나 금융회사에서 유출된 정보가 여러 인터넷 사이트에서, 또는 인터넷 사이트에서 유출된 정보가 금융회사에서 교차 사용될 가능성이 매우 높은 것이다[4]. 각 개인정보 보관 주체들은 자신의 사이트에 접근하는 정보가 다른 사이트에서 사용되어 발생하는 문제는 개인의 책임이라고 주장하고 있지만, 이는 개인정보를 수집하고 관리하는 주체로서 무책임한 생각일 수밖에 없다. 모든 정보보호 주체들은 자신이 보관하고 있는 개인정보를 철저하게 보관하여 정보가 유출되지 않도록 하여야 함과 동시에, 특히 금융기업들은 해킹이나 정보 유출 사고가 발생하면 시민들이 갖는 불안감과 실질적 피해가 매우 크다는 점을 인식하고 가장 안전한 금융거래 환경을 구축하여야 할 것이다.

그럼에도 불구하고, 이윤을 추구하는 기업의 입장에서는 항상 안정성보다는 효율성을 우선순위의 높은 곳에 올려놓는 경우가 많다[5]. 따라서 개인의 정보보호를 기업 경영의 최우선으로 여기는 경우를 빼놓고는 소비자들의 이용 편리성을 놓치지 않고 하루에도 수천만 건의 상용 거래를 처리하여야 하는 금융회사 및 기업으로서는 강력한 보안대책을 적용하기에 한계가 있음이 현실이다. 그러므로 고객의 이용 편리성을 유지하면서도 처리 속도를 저하시키지 않도록 하기 위해서 친기능적인 보호 수단을 개발하고 적용하여야 하며, 다수의 금융회사 및 기업과 거래하는 고객들의 편리를 위해 금융기업 간에도 공동으로 사용할 수 있는 보안 대책들이 요구된다.

이에 본 연구는 더욱 확장되고 있는 전자금융, 또는 온라인 금융의 새로운 환경 변화에 대하여 알아보고, 이렇게 빠르게 변화하고 있는 전자금융의 환경에 대한 전망과 그에 대한 시사 및 문제점 등을 알아보고자 한다.

2. 이론적 배경

2.1 전자금융 사고의 변동 추이

전자금융 및 금융IT 관련 사고는 이용수단의 변화에 따라 그 대상과 방법이 변화하고 있다. 1990년대에는 텔

레뱅킹 사고가 집중적으로 발생하였으며, 2000년대 초기에는 PC뱅킹에 대한 사고가 많이 발생하였다[6].

구체적으로는 2003년 말부터 2004년 초에는 신용카드, 현금카드 복제사고가 집중적으로 발생하였으며, 2005년도에는 인터넷 뱅킹 해킹, 피싱 등의 사고가 주를 이루었다. 2007년도는 CD/ATM을 이용한 카드 복제사고와 변형된 피싱, 해킹사고가 복합적으로 발생하였으며, 세금환급·범죄연관·자녀납치 등 이용자의 심리를 이용한 전화금융 사기를 통하여 시민들의 귀중한 금전을 절취해 가고 있다. 또한 2008년부터는 금전적인 목적과 사회 혼란을 노린 DDoS(Distributed Denial of Service) 공격이 일반 인터넷서비스 업체를 대상으로 시작해서 금융회사까지 발생하였다[7].

이와 같은 사고 유형의 변화를 분석해보면, 대부분 금융거래에 필요한 개인정보와 습득이 용이한 대상부터 시작하고 있으며, 사고 이후 보호대책이 강화되면 다른 대상으로 변경되는 것을 알 수 있다. 따라서 전자금융 사고에 대한 대응은 사고 유형을 미리 분석하여 범인들보다 먼저 대응 방안을 개발하는 것이 필요하다고 본다.

또한 초기의 범행은 단독으로 정보를 절취하여 현금화시키는 모든 과정을 수행함으로써 특정 범인을 체포하면 유사한 범죄가 발생되지 않았으나, 2010년대부터 발생되는 내용을 보면 범행 시나리오를 기획하는 팀과 정보수집팀, 대포통장이나 대포폰 구매팀, 자금이체 실행팀, 현금인출팀 등으로 구분되어 있었다[8]. 따라서 핵심이 되는 집단은 해외에서 활동하기 때문에 범인을 체포하기도 어렵고, 체포하여도 각 단계별로 확인이 불가능하여 범인들을 일망타진하기가 어려워 유사한 사고의 재발 비율이 높다.

2.2 최근 전자금융 사고의 특징

2.2.1 해킹·피싱에 의한 금융사고 지속 증가

과거에는 이메일을 통해 위장 사이트로 유인하여 개인정보를 획득하는 단순한 피싱이 주를 이루었으나, 최근에는 악성코드 유포, 파밍 기법과 결합된 피싱, 웹메일 해킹 등 전자금융 관련 사고가 점차 복잡화·지능화를 거듭하고 있다.

이러한 해킹·피싱에 의한 전자금융 사고가 지속되는 원인은 먼저, 해킹·피싱 등 복합적인 공격 기술의 진화에 따른 즉각적인 대응기술의 확보가 부족하고, 보안패치가 적용되지 않은 PC나 개인 휴대폰이 많아 악성코드의 감염 위험에 대부분 노출되어 있으며, 해킹·피싱 등에 대한 이용자의 보안의식 부족 등을 들 수 있다[9].

2.2.2 인증서 절취에 의한 전자금융 사고

「전자금융거래법」 시행에 따라 전자금융 거래 시 「전자서명법」에 따른 인증서 사용이 의무화되어 전자금융 거래의 보안이 한층 강화되었다. 하지만 PC 내부 및 개인 핸드폰에 보관된 인증서의 위치가 노출되기 쉽고 해킹에 의한 인증서의 복제가 가능하며, 여러 부문에서 공동 사용이 가능한 특성으로 인해 전자금융 범죄에 많이 악용되고 있다.

특히, 많은 사용자들이 가정과 사무실, 국내와 해외에서 사용하기 위해 웹메일이나 웹하드에 인증서를 저장하였다가 복제 당하여 피해를 보는 사례가 발생하고 있다[10].

2.2.3 On/Off-Line 신용(직불)카드 사고 증가

유럽의 경우, 2005년 이전 카드 스키밍(skimming)에 의한 CD/ATM에서의 카드복제 사고가 325,000건, 440만 유로의 금융 피해가 발생할 정도로 CD/ATM 사기가 가장 많았으며, 그 이후 마그네틱 카드를 EMV 스마트카드로 전환하면서 CD/ATM 사기 건수와 금융 피해가 각각 20%, 43% 감소하였다. 미국에서는 2004년에 약 3백만 건의 CD/ATM을 이용한 카드복제 사고가 발생하여 2.75억 달러의 금융 피해가 발생하였으며, 국내에서도 Tapping 및 가짜 CD/ATM 기기를 이용한 카드복제 사고가 발생한 바 있다[11].

국내 카드사들은 안전한 인터넷 카드결제를 위해 안심클릭 방식과 인터넷안전결제(IPS) 방식을 제공하고 있으나, 이 방식을 이용하는 다수의 사고가 발생하고 있는 것이 현실이다. 과거의 안심결제 방식의 경우 CVV값을 요구하지 않아 카드번호 및 안심클릭 비밀번호가 유출될 경우 불법 거래가 가능하였으나, 최근에는 모든 카드 결제 시 CVV값을 요구하도록 보완하여 동일한 사고는 제거하였지만 여전히 카드를 촬영하여 요구하거나 식구임을 속여 카드 내용을 요구하는 방식 등이 등장하고 있다. 여전히 카드의 불법 복제나 복제는 수익성이 확실한 범죄인 것이다.

3. 전자금융의 새로운 환경과 그 시사점

3.1 비대면 금융의 확대

물론, 인터넷 및 스마트 기기의 급격한 보급으로 인하여 그동안 인터넷(모바일) 뱅킹 이용규모는 꾸준히 확대

되는 한편 오프라인 점포 수는 지속적으로 감소하는 추세가 계속되어왔지만, 특히 '코로나19'로 인한 사회적 거리두기 등으로 인해 2020년에 들어 인터넷(모바일) 뱅킹 및 비대면 결제 이용규모가 큰 폭으로 증가하였다.

unit : thousand matter, a billion Won

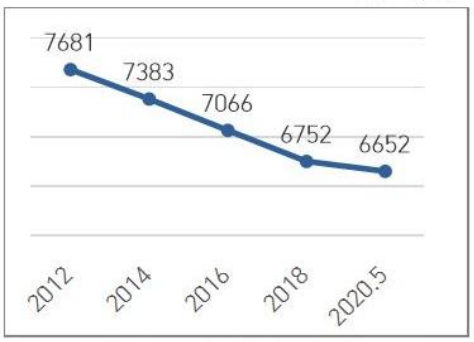
Source : Bank of Korea(2019)[12], Financial Supervisory Service (2020)[13]

Fig. 1. Daily use of internet banking service

즉, 위의 그림과 같이 2020년 상반기 기준 비대면 결제 이용규모는 일평균으로 전년 대비 약 6,500억 원, 5,200만 건이 증가하여 각각 13.2%, 33.0% 등이 증가하였다(Fig. 1).

또한 은행의 오프라인 점포 수는 꾸준하게 줄어들고 있어, 아래 Fig 2의 내용과 같이 2020년 3월 현재 6,652개로 2012년과 비교하면 불과 8년 사이에 1천여 개 이상의 오프라인 점포가 줄어든 것을 알 수 있다.

unit : a place



Source : Bank of Korea(2019)[12], Financial Supervisory Service (2020)[13]

Fig. 2. Number of domestic bank stores

이러한 비대면 금융의 증가 및 확대는 이를 이용한 전자금융 범죄 및 사기의 다양화와 고도화가 야기될 가능성이 높다. 다시 말해, 금융기관에서 신분증의 진위를 확인할 때 사진과 실물의 확인이 어려운 점 등 비대면 금융에서의 실명 확인 절차상의 취약점을 악용하는 전자금융 사기 기법이 발생하기 쉬우며, 또한 금융 앱을 위·변조하거나 블랙마켓(black market)에서 사이버 공격 정보를 습득하는 등 공격 방식을 다양화시킬 수 있는 여건이 커지고 있고, 신분증 사진을 스마트폰 내에 저장 등과 같은 여건 변화에 따라 이용자들의 부주의에 의한 보안사고 우려도 충분히 존재한다.

그리고 비대면 금융의 보안 위협은 지속되고 그 파급력도 확대될 것을 전망할 수 있는데[14], 특히 「전자금융거래법」이 개정되면 비대면 금융 방식이나 서비스가 더욱 다양화될 수 있을 것으로 보여, 이를 악용한 공격도 지속될 것이 분명하다. 왜냐하면, 오픈뱅킹이나 마이데이터 산업 활성화 등으로 특정 금융회사 보안사고가 타 금융회사로 쉽게 전파될 수 있어 공격에 따른 파급력도 비약적으로 확대될 수 있기 때문이다. 즉, 보안이 취약한 특정의 A 은행에서 계좌 개설 및 공인인증서를 발급받아 B 은행에서 A 은행 공인인증서를 등록하고 A 은행 계좌를 활용하여 인증받은 후 B 은행에서 대출을 실행하는 방법 등을 예상할 수 있다.

따라서 비대면 금융의 기반에는 보안성과 포용성이 전제될 필요가 있으며, 그만큼 금융소비자는 비대면 금융의 편리함에 만족하는 동시에 보안에 대한 우려도 크므로 편리성과 보안성 간의 균형을 확보하려는 노력이 중요하고, 특히 스마트폰 등의 전자기기 사용에 익숙하지 않은 고령층 및 디지털 취약계층이 비대면 금융에서 소외되지 않도록 지속적으로 노력할 필요가 있다. 물론 금융기관 및 금융기업의 보다 적극적인 예방 대책이 만들어져야 할 것이다.

3.2 금융권의 원격근무

'코로나19' 상황으로 인하여 국내·외의 많은 기업들이 원격 재택근무를 실시하고 있으며[15], 결국 기존의 근무 형태에 대하여 다소 보수적인 금융권 역시 향후 원격근무의 형태가 보다 확대될 것이 분명하다. 이에 따라, 전자금융 시스템 및 전자금융 사용자에 대한 공격 범위가 기업 내부에서 외부로 확대될 가능성이 크다. 즉, 원격근무 장소나 단말기, 네트워크 등의 경우가 기업 내부에 비해 가정 및 기업의 외부는 상대적으로 철저한 보안 통제가 어려운 만큼 공격자의 주요 공격 대상으로 부각될 것이며, 공격자는 원격근무자에 피싱 메일 발송, 크리덴셜 스터핑(Credential Stuffing) 공격 등을 수행하여 악성코드 유포, 내부망 접근, 기업 내부 정보 탈취 등의 위험성이 커질 수 있다.

Table 1. Major security threats from Telework

Division	Major security threat
Insufficient Physical Control of Telework Terminals	· The loss, theft, or the peek of others of the remote working terminal may cause data in the terminal to leak or access the company's internal network.
Unsafe network usage	· External networks (Internet) used by Teleworkers are difficult to control, so there is a concern that important information will be leaked due to wiretapping or mid-person attacks (MITM). · Incorrect network equipment (VPN, etc.) setting or vulnerability exists in network equipment.
Internal Network Infringement due to Malware Infection	· Illegal infringement of system when connecting to internal network with Teleworking terminal infected with malicious code.
Remote access threats to internal resources	· As Telework terminals become accessible to internal resources that were only accessible within the company, there is a security threat such as unauthorized access.

Source : Souppaya & Scarfone(2016)[16]

실례로, 최근에 들어 이용자가 급증한 화상회의 솔루션도 사이버 공격의 타겟으로 부각되고 있는데, 이는 화상회의 솔루션 자체의 취약점이나 화상회의 접근통제 미흡(회의방 전체 공개, 회의 참여 접근코드 재사용, 회의 참여자 신원 미확인 등) 등을 악용하여 공격자가 화상회의에 무단 접속하는 사례가 나타나고 있다. 그리고 화상회의 과정 내 접속에 성공한 공격자는 회의 방해, 회의 중 공유된 정보 또는 파일 탈취, 악성코드 유포(회의 시 업로드하는 GIF 형태의 이미지 파일에 대한 화상회의 솔루션의 검증 기능이 미흡할 경우, 악성코드가 포함된 이미지 파일을 업로드하여 회의 참여자에 유포) 등의 공격 수행 가능해질 수 있다.

또한, 원격근무나 화상회의는 일시적 유행이 아닌 사회와 학교와 기업의 문화로 정착될 것이므로, 그만큼 금융의 디지털 전환이 가속화되고, 일-삶의 균형(Work-life balance, 이른바 '워라밸')을 추구하는 문화 등으로 원격근무나 화상회의가 많은 기업에서 일상적인 근무 형태의 하나로 자리매김하게 될 것이다. 우리나라 금융권 역시 「전자금융감독규정 시행세칙」을 개정(21.1.1 시행)하여 철저한 보안 통제 아래에서 임직원의 상시 재택근무를 허용한 사실이 있으며, 이에 따라 원격근무 등이 빠르게 확대될 전망이다[17].

따라서 원격근무나 화상회의를 수행할 때는 보안 통제를 강화하는 것이 필수적인 상황이 되었으며, 원격근무나 화상회의 수행에 있어 기존 근무 및 회의 형태에 비해 보안 수준이 저하되어서는 안 된다는 점이 매우 중요하고, 금융권은 원격근무나 화상회의 수행 범위를 정하고 재택근무 환경 구축 시부터 종료 시점까지 철저한 보안 통제 대책을 마련할 필요가 있다. 그리고 그만큼 금융기관의 특수한 여건을 고려한 원격근무 매뉴얼이 반드시 필요하다.

3.3 공인인증의 폐지

그동안 일정 환경에서 의무적으로 사용되었던 공인인증서 제도가 폐지되고 다양한 인증수단으로의 인증 정책이 이미 시행되었다. 즉, 「전자서명법」 개정(20.12.10 시행)으로 20여 년 만에 공인인증서의 우월적 지위가 폐지됨에 따라 금융과 공공분야 등에서 여러 가지의 인증수단이 동등한 차원에서 경쟁할 수 있는 시스템이 조성되어, '공인인증서', '공인인증기관' 등의 용어가 '인증서', '전자서명인증사업자'로 통합·변경된 것이다.

Table 2. The change of the accredited certification system in the financial sector

Year	Content
1999	Establishment of Authorized Digital Signature System by the Enactment of the Electronic Signature Act.
2002	Mandatory use of accredited certificates when using Internet banking.
2003	Mandatory use of accredited certificates when trading securities online.
2005	Use of an official certificate when paying more than 300,000 won by credit card.
2006	Mandatory use of accredited certificates in electronic financial transactions.
2015	Repeal of Duty to Use Certificates in Electronic Financial Transactions (Various certifications appear in financial institutions, such as biometric and private certificates.)
2020	The abolition of the accredited certification system (Enforcement Decree of December 10, 2012) by the amendment of the Electronic Signature Act.

이에 따라, 금융위원회는 보안성·편의성을 갖춘 다양한 인증수단이 금융권에 활용될 수 있는 정책 마련을 추진 중으로, 금융거래 위험 수준별 인증수단의 차등화 등을 검토[18] 중인 것으로 알려져 있다. 예를 들어, EU는 계좌에 대한 온라인 접근, 전자지급거래 개시 등의 고위험거래 시에는 2팩터 인증 방식과 같은 보다 강력한 고객인증(SCA) 적용을 의무화한 바 있다.

또한 공인인증서 폐지로 인하여 금융인증 시장의 선점을 위한 경쟁이 본격화되었으며, 각 금융권은 사설인증서, 바이오인증 등 다양한 인증수단을 활용하고 있고, 최

근에는 자체 인증서를 개발하여 그 이용 범위를 확대하려는 움직임도 많이 존재하고 있다. 예를 들어, “KB 국민은행”은 행정안전부의 공공분야 전자서명 확대 도입 시범사업의 후보사업자로 선정되었으며, 네이버·카카오 등 플랫폼 사업자나 이동통신사 등도 넓은 고객 접점을 기반으로 금융권 인증시장 진출을 추진하고 있다.

Table 3. Development of private certificates using financial sector

Division	Name of issuing agency and service	Characteristics
Financial sector joint	Federation of Banks, Bank sign	· Utilization of Banking Consortium Blockchain.
	KFTC, Financial certificate	· Joint participation of KFTC and banking sector (‘2012. Dec. 10. Full implementation). · Keep certificates in the KFTC cloud.
Financial company self-certification	KB Kookmin Bank, KB mobile certificate	· Promoting expansion of use within KB Financial Group (insurance, securities, cards, etc.). · No valid period of certificate (but automatic disposal when not in use for more than one year).
	IBK Industrial Bank, i - Mobile certificate in ONE Bank	· It can be used in its mobile banking service. · A 6-digit password-based certificate for replacing an authorized certificate.
Platform operator	Naver, Naver certificate	· Used for Naver electronic document (notice) service. · Available in mobile and PC (self-browser)-based services.
	Kakao pay, Kakao pay certificate	· Interworking with Messenger 'Kakao Talk'. · Introduced to more than 200 institutions including financial companies (insurance, securities, cards, etc.), financial institutions, governments, and public institutions.
Carrier	Three mobile communication companies, PASS certificate	· Perform real-time telephone number, name, and terminal authentication when issuing and using certificates. · Introduction to financial companies (banks, insurance, securities, etc.), Nice public services, etc.

Source: KFTC press release (Nov. 17, 2020), KB Kookmin Bank press release (Nov. 4, 2020), IIBK Industrial Bank press release (May 21, 2019), Naver press release (May 22, 2020; Sep. 26), Kakao Pay certificate official website, PASS certificate introduction (Sep. 2020).

다만, 기업의 입장에서는 인증수단을 순수하게 보안 목적이 아닌 신규 사업 기회로 인식하는 경향이 있다. 즉, 금융기업은 자사 인증수단 활성화를 통해 고객 잠금 효과(Lock-in effect)를 기대하고, 비금융기업은 금융산업 진출을 위한 초석으로 인증수단을 활용할 가능성이 있는 만큼 금융회사는 자사 인증서의 개발 및 확대에 보다 집중할 것으로 보이며, 통신사 등의 금융권 인증시장 진입 시도는 더욱 활발할 것으로 전망된다.

이렇게 인증수단이 복합적으로 나타남에 따라 보안성이 전제된 인증수단의 다양성에 대한 존중이 필요하고, 공인인증제도 폐지로 민간 중심의 다양한 인증수단이 도입되어 금융소비자의 선택폭이 확대되고 편리성이 제고될 것으로 기대된다. 다만, 금융은 타 산업과는 달리 높은 수준의 신뢰성·안전성이 요구되는 만큼, 보다 높은 수준의 보안성 요구나 거래 리스크별 인증수단 차등화 등 보안성을 확보하기 위한 조치가 요구된다. 더불어, 기존 공인인증서를 계속 사용하고자 하는 수요자에 대한 보완적 방법 역시 필요하다 할 것이다.

3.4 고도화되는 보이스피싱

대표적인 전자금융 범죄인 보이스피싱(Voice Phishing)은 갈수록 고도화 및 지능화되는 추세로 나타나고 있다. 보이스피싱 범죄조직은 대출 사기형, 기관 사칭형, 메신저 피싱 및 납치·사고빙자형 등의 다양한 범죄 수법을 사용하여 체계적으로 접근하고 있다[19].

Table 4. Classification of voice phishing crime methods

Kind	Content
Loan fraud type	· Demanding commissions, pre-interest, etc. on condition of low interest rate loans.
Agency impersonation type	· Request funds in the name of criminal investigation, protection of victims' funds, etc. after impersonating the prosecution, financial authorities, etc.
Messenger Phishing	· Request funds transfer/personal (credit) information through messenger (or text) under the pretext of online payment, debt repayment, etc. · In some cases, non-face-to-face account opening, loans, transfers, etc. are implemented with information taken from the company.
Kidnapping/accidental icebreaker	· Request money under the guise of kidnapping or accident of a child.

Source: Financial Services Commission Press Release (Jun. 24, 2020), Financial Supervisory Service Press Release (Nov. 4, 2020), and National Police Agency Press Release (Nov. 6, 2019)

또한 최근 들어 ‘코로나19’ 등 사회환경이 반영되어 서류 위조, 영상통화 등의 수법이 더욱 치밀해지고 있고,

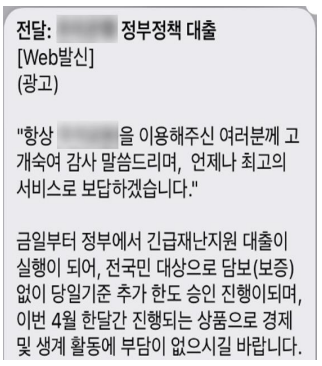
원격수업과 같은 언택트 접촉의 양이 많아지고 영상통화에 대한 거부감이 많이 사라지면서 누구라도 보이스피싱의 피해자가 될 수 있는 상황이다. 또한 스마트폰의 보급에 따라 모바일 앱(App)을 악용한 보이스피싱도 성행하고 있는데, 보이스피싱 범죄조직은 URL(인터넷 웹페이지 주소, Uniform Resource Locator) 등을 보내 악성 모바일 앱 설치를 유도한 후 전화를 가로채거나 휴대폰을 원격제어하여 피해자의 금융 앱을 실행할 수 있게 되는 것이다[20].

최근의 악성 모바일 앱은 정보(SMS, 연락처, 단말기 모델 정보, 통신사 등) 탈취나 전화 가로채기뿐만 아니라 실시간 스트리밍, 로그 수집·삭제, 카메라 전·후면 변경 등 다양한 기능을 탑재하고 있는 등, 보이스피싱은 신기술과 연계하여 더욱 위협적으로 진화하게 될 전망이다.

예를 들어, AI로 음성이나 영상을 실제처럼 조작하는 딥페이크(Deepfake) 기술 등을 악용한 본인 사칭 등 보이스피싱 공격은 더욱 정교해지게 될 것인데, 이미 영국에서는 2019년에 딥페이크 기술을 악용하여 회사 최고경영자의 음성을 모방해 약 22만 유로를 편취하는 사건이 발생하였으며, 이후 유사 사건도 산발적으로 발생하고 있다. 더구나 향후 클라우드 이용 확대에 따라 취약한 클라우드 해킹을 통해 취득한 정보로 보이스피싱을 수행하는 경우도 발생할 것으로 예상된다.

따라서 보이스피싱의 고도화에 대한 체계적이고 전방위적인 대응이 필요하며, 실효성 있는 보이스피싱 대응을 위해서는 일차적으로 정부 부처, 수사기관, 금융회사, 통신사뿐만 아니라 각각의 개인 시민 모두가 경각심을 제고하는 노력 역시 필수적이다.

Government-backed loans impersonating Covid-19.



Forging business cards, official documents, accusations, arrest warrants, etc.

Source: Financial Supervisory Service press release (Apr. 8, 2020), Seoul Central District Prosecutors' Office press release (Nov. 13, 2020)

Fig. 3. Recent Voice Phishing Cases

3.5 금융산업의 개방과 형태의 다양화

오픈뱅킹 등 지급결제망의 개방, 간편결제를 중심으로 한 빅테크(big tech)의 금융산업에의 진출 및 확대 등과 같이 금융산업에 진출하고자 하는 플레이어가 확대되는

Table 5. Status of Financial Industry Opening Promotion

Division	Content
Open banking	· Open financial settlement network that opens the services of a particular financial company through the application programming interface (API) so that other financial companies can develop services using it → All bank accounts can be inquired and transferred through one app.
MyData	· A project to develop new additional services by delivering personal information to a third party company based on the right to send personal credit information → New services such as collective inquiry and management of personal information or recommendation of customized financial products can be provided.
Payment instruction delivery business (MyPayment)	· A project that delivers financial consumer's payment order (payment, remittance, etc.) to financial companies and helps them implement it → Payment and remittance services can be provided even small businesses without having financial consumer funds.
Comprehensive payment settlement business	· It is a platform project that can provide all electronic financial services such as fund transfer, payment, and payment agency based on the account. → It is possible to open an account, but it is expected to participate mainly in big tech companies.

Source: Financial Services Commission press release (Jul. 24, 2020; Oct. 21), The Electronic Financial Transactions Act (Nov. 27, 2020)

추세에 있는 것처럼 금융산업의 개방에 따른 내부 체계의 확대 및 다변화가 나타나고 있다. 이에 따라, 금융당국은 「전자금융거래법」 개정(20.11.27 법안 발의)을 통해 소규모 기업도 진입 가능한 지급지시전달업(MyPayment) 및 모든 전자금융업을 영위할 수 있는 종합지급결제업의 신설도 추진중에 있다.

이러한 현황과 현상에 따라, 금융산업에의 각 플레이어는 협력 등의 방식으로 경쟁력 확보를 위해 노력하고 있다.

Table 6. Measures to secure competitiveness of financial companies and big and fintech companies

Division	Content	Case
Financial companies (traditional financial companies such as banks, credit card companies, securities firms, and insurance companies)	· Strengthening cooperation within group companies, such as establishing a group company integration platform	Shinhan Financial 'Shinhan Plus' - It is possible to use services such as banks, cards, financial investment, and life insurance without a separate mobile app.
	· Collaborating with big and fintech companies or other industries	Woori Bank - Convenience Store 'Seven-Eleven' signed a business agreement to support low-interest loans to franchise owners, develop customized financial products, and promote co-marketing based on big data.
Big Tech (provides financial services based on non-financial platforms such as portals and SNS, which are the main businesses)	· Partnership with existing financial companies	Naver - Mirae Asset Capital to lend to Naver Smart Store operators.
	· Direct entry into the financial business	Kakao - Internet bank 'Kakao Bank' and securities company 'Kakao Pay Securities'.
FinTech Companies (Providing Innovation Financial Services Using IT Technology)	· Provide various financial services based on innovative ideas	NHN Payco - Provides financial services such as payment, remittance, account and card inquiry, credit management, exchange, shopping accumulation, and transportation card.
	· Comparing, recommending, or providing brokerage services for financial products	PINK - Provides financial companies with loan product comparison services and customized insurance recommendation services.

Source: Shinhan Financial Group Press release (Aug. 13, 2018), Kakao Pay press release (Feb. 6, 2020).

즉, 위 Table 6의 내용처럼, 금융회사는 금융그룹사 통합 플랫폼 구축, 빅·핀테크 기업 또는 타 산업(유통·통신 등)과의 협력 등을 통해 자사 금융상품 및 서비스 고도화를 추구하고 있으며, 빅테크 기업의 입장에서는 수많은 고객과 접근성을 갖춘 비금융 플랫폼(포털, SNS 등)을 기반으로 기존 금융회사와 전략적으로 제휴하거나 금융업에 직접 진출하고자 할 것이 분명하다. 또한 핀테크 기업은 혁신적 아이디어를 바탕으로 새로운 금융 서비스를 제공하거나, 타 금융회사의 상품을 비교·추천하는 서비스 등을 개발하고 있다.

이처럼, 향후 금융기업과 데이터 산업계는 무한경쟁의 시대로 진입할 것을 쉽게 전망할 수 있으며[21], 그에 따라 금융권은 유통·통신 등 이종 산업과의 데이터 협업, 데이터 전담 조직 신설 등 데이터 산업 경쟁에서 살아남기 위해 역량을 집중하게 될 것이고, 그에 더해 금융회사 및 빅·핀테크 기업은 대량의 데이터 보유, 우수한 개발 역량 등 자사의 여건과 장점에 맞는 다양한 금융 데이터 산업을 추진할 것이 분명하다.

또한 개방형 금융체계 안에서 금융권 혁신과 상호 경쟁은 가속화될 것이 극명한데, 금융산업의 대외 개방 본격화로 오픈뱅킹, 마이데이터, 지급지시전달업 등의 활성화뿐만 아니라 각 서비스 간 연계를 통한 혁신적이고 다양한 금융 서비스가 다수 등장할 것이 예상된다.

따라서 금융회사와 빅·핀테크 기업 간 경쟁이 가속화되는 상황 속에서 모두가 공정하게 경쟁하고 시너지 효과를 발휘할 수 있는 법적·제도적 환경 마련이 선행될 필요가 있고, 금융권 보안 리스크의 상호연계성 확대를 경계할 필요도 분명하다. 즉, 타 기업과의 경쟁을 위한 금융회사 등의 전략적 협력이 확대됨에 따라 협력기업의 보안 취약점이 금융회사의 취약점으로 전이될 수 있는 위험이 존재하고, 협력기업에 보안사고 발생 시 연계된 금융회사도 책임으로부터 완전히 자유로울 수 없고 평판 리스크 등도 야기될 수 있으므로 협력기업의 보안 리스크를 면밀히 고려하여야 한다. 사용자 및 소비자 역시 급격하게 다양해지는 금융전문 및 금융복합 기업에 대한 선별의 능력을 증진시켜야 한다.

3.6 '지갑 없는 사회'의 도래

세계 각국에서 중앙은행 디지털 화폐(CBDC, Central Bank Digital Currency)를 발행하고자 하는 논의를 시작하고 있다. 기업의 측면에서는 "페이스북"이 디지털 화폐의 발행을 추진하고 있고, 많은 선진국에서 현금 이용

이 감소하는 현상 등을 계기로 각 중앙은행이 발행하는 전자적 형태의 디지털 화폐(CBDC)에 대한 논의가 본격화되고 있다. 현재로서는 중국이 CBDC 도입에 가장 적극적이며, 국내의 경우 한국은행에서 CBDC 관련 기술·법률 검토 및 파일럿 테스트를 추진 중으로 알려져 있다.

Table 7. Classification of Central Bank Digital Currency (CBDC)

Criteria	Classification	Characteristics
Use Purpose (Use Subject)	For small amount payment (General-purpose)	· Use for general transactions of all economic entities.
	For large amount payment (Wholesale only)	· Use for transactions between financial companies, such as banks.
Implementation method	Single ledger method (account-based)	· Central managers (e.g., central banks) keep and manage CBDC accounts and related transaction information.
	Distributed ledger method (token-based)	· Manage the same transaction record with multiple participants having mutually synchronized ledgers.

Source : Bank of Korea(2019)[22]

또한 간편결제의 대중화 및 모바일 신분증의 도입 추진 등으로 온라인 간편결제의 활용이 일상화되었으며, 오프라인 매장에서도 실물 카드 없이 스마트폰으로 결제하는 오프라인 간편결제도 활성화되는 추세에 있다. 예를 들어, 행정안전부는 모바일 신분증 도입을 추진 중이며, 또한 경찰청·이동통신 3사 등은 모바일 운전면허 확인 서비스를 2020년 7월에 출시한 바 있다.

Table 8. Status of Offline Simple Payment Service

Service Provider	Service Features
Mobile Device Manufacturer	· Register a credit card or account of a financial company affiliated with its mobile devices and pay without a physical card (Samsung Pay, LG Pay, etc.
Card company	· Provide 'app card payment' service that allows users to register their credit card information in a mobile app and pay with a mobile device rather than a physical card.
Big Tech Company	· Register payment method on our platform (portal, SNS, etc.) or charge advance payment, and use barcode or QR code to make offline payment (Naver Pay, Kakao Pay, etc.)

기술의 발달과 사회의 발전과 함께 '지갑 없는 사회'로의 전환은 가속화될 수밖에 없는 현실이며, 물론 국내에 CBDC의 도입까지는 장기간의 검토가 필요할 것으로 보이지만, 디지털 화폐에 대한 관심은 지속될 것으로 예상된다. 또한 신분증, 자격증, 각종 증명서 등을 전자적으로 발급·저장하는 서비스가 출시되어 비대면 실명확인이나 각종 증빙서류 제출 작업 등이 간소화될 전망이다. 즉, 은행에서 계좌 개설을 할 때 모바일 신분증을 통한 신원확인을 하고, 대출 신청 시 모바일 기기에 저장한 재직증명서 등의 서류를 전자적으로 제출하는 등의 환경이 가능해질 수 있다.

하지만 '지갑 없는 사회'의 도래를 위해서는 온라인 보안 등 각종 리스크에 철저히 대비할 필요가 있다. CBDC 등 디지털 화폐와 관련된 프라이버시 이슈나 분산원장기술 활용에 따른 운영리스크(분산원장 처리 속도 한계 등에 의한 가용성 저하, 이중지불과 같은 비정상 거래 발생 등) 등도 발생할 수 있으므로 사전에 철저한 검증 및 대비가 요구되며, 실물 지갑을 대체하는 모바일 기기의 물리적 도난이나 악성 모바일 앱(app) 유포 등과 같은 사이버 공격에 특히 주의할 필요가 있다.

4. 결론

주요 사회적 이슈는 금융산업은 물론, 전자금융범죄의 하나인 해킹 기법에 빠르게 반영된다. 단순 스패머(spamer)뿐만 아니라, 고도화된 위협그룹들도 공격의 성공률을 높이기 위해 'Covid-19'를 이용함에 따라 'Covid-19'를 이용했다는 사실만으로 공격의 배후를 추적하는 것은 어려워졌다.

글로벌 보안업체인 "RiskIQ"에 따르면, 'Covid-19' 이후 스팸 메일이 세계적으로 하루에 10만 개가량 수집되고 있다고 한다. 이와 같이 'Covid-19'를 이용한 악성코드와 피싱 URL 개수가 급증하면서 기관 보안담당자는 오히려 위험도 높은 위협을 식별하기가 어려워졌다.

그러나 금융기관 및 기업은 'Covid-19'와 관계없이 여전히 현재의 보안 환경에서도 스팸 메일과 악성코드를 효과적으로 차단하여야 하며, 피싱사이트 역시 사용자 보안 의식 제고를 통해 소비자의 피해를 예방할 수 있도록 하여야 한다[23]. 금융기업에 있어 보안의 문제는 일상적인 업무라는 것이다. 다만, 'Covid-19' 이슈로 인하여 금융기업의 내부로 한정되어 있던 보안의 영역이 기업의 외부로까지 확장되었다는 특성이 나타났다고 할 수 있다. 또한 'Covid-19' 상황은 미래의 언택트 사회를 10년 이상 앞당겼다는 주장도 있다. 즉, 금융 및 전자금융

의 환경이 급격하게 변화하고 있으며, 그 속도 역시 기존의 상상력을 훨씬 초월하고 있다는 사실을 부정하기가 힘들어졌다.

본 연구에서는 이제 우리나라의 금융과 전자금융 환경에 있어 급박하게 대처하여야 하는 실제적 변화로 ① 비대면 금융의 확대, ② 금융권의 원격근무, ③ 공인인증의 폐지, ④ 고도화되는 보이스피싱, ⑤ 금융산업의 개방과 형태의 다양화, ⑥ '지갑 없는 사회'의 도래 등에 대하여 제시하였고, 그로 인한 내용과 시사점을 파악하였다. 하지만 연구에서 제시한 문제 외에도 현재 전자금융 환경이 처한 문제는 각종 IT 기술의 개발 및 발달과 함께 더욱 심각해지고 있다. 예를 들어, 4차 산업혁명으로 촉발된 전 세계적 변화는 금융 보안 분야에도 전파되어, 인공지능 기술 / 딥러닝 기술 / 사용자 분석 기술 / 딥페이크(deepfake) 기술 등과 같은 문제는 특히 전자금융 체계에 있어 급박하고도 대응하기 어려운 위험요소로 나타나고 있다.

전자금융은 사회적으로 점점 그 비중이 확대되고 있으며, 그만큼 전자금융을 위협하는 여러 문제 역시 확대되고 있다. 따라서 전자금융과 그 환경의 문제 및 그로 인한 범죄와 범죄 수사의 분야까지도 꾸준하게 관심을 갖고 연구되어야 마땅하다. 본 연구가 작은 밑거름이 되어 향후 전자금융과 그를 둘러싼 여러 환경에 대한 더 많은 연구가 진행되어주기를 기대해본다.

REFERENCES

[1] M. S. Kim. (2009). A Study on the Importance of Quality for E-Commerce Banking Service in Korea. *Financial Knowledge Research, 7(2)*, 93-111.
UCI(KEPA) : I410-ECN-0102-2012-320-000966747

[2] S. H. Lee. (2010). Enhancing the safety of e-commerce payment and settlement and strengthening consumer protection. *Weekly Financial Brief, 19(22)*, 10-11.
URL : http://www.kif.re.kr

[3] J. Y. Lee & I. S. Kim. (2018). Detecting Abnormalities in Fraud Detection System through the Analysis of Insider Security Threats. *The Journal of Society for e-Business Studies, 23(4)*, 153-169.
DOI : https://doi.org/10.7838/jsebs.2018.23.4.153

[4] J. E. Lee. (2017). Liability for damages for electronic financial transaction accidents. *Weekly Financial Brief, 26(14)*, 3-7.
UCI(KEPA) : I410-ECN-0102-2018-300-000548192

[5] H. S. Kim & S. B. Choi. (2010). The Effects of Electronic-based Banking Service on Efficiency and Effectiveness of Bank. *Journal of Business Research, 25(2)*, 279-306.
DOI : 10.22903/jbr.2010.25.2.279

[6] Y. J. Kim. (2019). Accidents on Electronic Financial Transactions and the Liability of Financial Institutions. *COMMERCIAL CASES REVIEW, 32(4)*, 289-344
DOI : http://doi.org/10.36894/kcca.2019.32.4.289

[7] D. M. Kim. (2020). A Study on the Scope of the Elecronic Financial Fraud by means of Access Device. *Chungnam Law Review 31(2)*, 45-99.
DOI : https://doi.org/10.33982/clr.2020.05.31.2.45

[8] W. Chung. (2020). Trend of Voice Phishing Crime and Development Direction of Investigation Response System. *korean Journal of Public Safety and Criminal Justice , 29(4)*, 461-484.
DOI : http://dx.doi.org/10.21181/KJPC.2020.29.4.461

[9] D. Y. Jeong., K. B. Lee. & T. H. Park. (2014). A Study on Improving the Electronic Financial Fraud Prevention Service - Focusing on an Analysis of Electronic Financial Fraud Cases in 2013 -. *Journal of the Korea Institute of Information Security & Cryptology, 24(6)*, 1243-1261.
DOI : http://dx.doi.org/10.13089/JKIISC.2014.24.6.1243

[10] Y. J. Kim. (2019). Accidents on Electronic Financial Transactions and the Liability of Financial Institutions. *COMMERCIAL CASES REVIEW, 32(4)*, 289-344
DOI : http://doi.org/10.36894/kcca.2019.32.4.289

[11] D. Y. Jeong., G. B. Kim. & S. J. Lee. (2017). A Study on Risk Analysis and Countermeasures of Electronic Financial Fraud. *Journal of The Korea Institute of Information Security & Cryptology, 27(1)*, 115-128.
DOI : https://doi.org/10.13089/JKIISC.2017.27.1.115

[12] Bank of Korea. (2019). *Central Bank Digital Currency.* Seoul : Bank of Korea.
ISBN : 9791155384558 93320

[13] 「Financial Supervisory Service」 www.fss.or.kr

[14] G. W. Kim. (2020). A Study on the Security Guard Model for MICE Events Corresponding to Pandemic - Focusing on the Case of Security Guard in KOREA 2020 METAL WEEK -. *Korean Security Journal, 2020(-)*, 55-78.
DOI : https://doi.org/10.36623/KSSR.2020.pandemic.55

[15] Korea Institute of Finance. (2020). With / After Challenges of financial institutions in the era of COVID-19. *Weekly Financial Brief, 29(19)*, 28-29.
URL : http://www.kif.re.kr/

[16] Souppaya, M. P., & Scarfone, K.(2016). (NIST Special Publication 800-46 Revision 2) *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security*. Gaithersburg, MD : National Institute of Standards and Technology(NIST).

[17] Y. H. Chol, D. H. Kim, & Y. J. Sin. (2020). Teleworking in Covid-19 : A Pandemic Perspective.

The Journal of Public Policy and Governance, 14(2), 33-74.
DOI : http://dx.doi.org/10.37582/CSPP.2020.14.2.33

[18] Financial Services Commission. (2020). *Comprehensive digital finance innovation plan in the era of the 4th industrial revolution(amendment direction of the Electronic Financial Transactions Act, etc.)*. Seoul : Financial Services Commission.

[19] K. S. Lee. (2018). Recent Trends in Crime Methods and Legal Measures of Voice-Phishing. *Crime Investigation Research, 4(2)*, 3-19.
UCI(KEPA) : I410-ECN-0101-2019-360-000346069

[20] S. Y. Lee & . L. Lee. (2020). A Study on the Prediction Method of Voice Phishing Damage Using Big Data and FDS. *Korean Security Journal, 2020(62)*, 185-204.
DOI : https://doi.org/10.36623/KSSR.2020.62.8

[21] Y. R. Choi & J. H. Jung. (2017). A Study on How to Grow the InsurTech during the Fourth Industrial Revolution. Asian Trade Risk Management, 2(1), 25-46.
DOI : https://doi.org/10.22142/atrm.2017.2.1.23

[22] Bank of Korea. (2019). *Central Bank Digital Currency*. Seoul : Bank of Korea.
ISBN : 9791155384558 93320

[23] D. C. Kim & I. S. Kim. (2018). A Study on Cybersecurity Regulation for Financial Sector - Policy Suggestion based on New York's Cybersecurity Regulation (23 NYCRR 500) -. *The Journal of Society for e-Business Studies, 23(4)*, 87-107.
DOI : http://dx.doi.org/10.7838/jsebs.2018.23.4.087

김 대 현(Dae-Hyun Kim) [정회원]

· 2011년 8월 : 서울시립대학교 경영대학원(경영학석사)
· 2018년 2월 : 동국대학교 법학과(법학박사 수료)
· 2018년 2월 ~ 현재 : (주)파인울 감사
· 관심분야 : 전자금융, 금융보안, 자금세탁방지

· E-Mail : kim_dhyun@naver.com