JANT 한국항행학회논문지
Journal of Advanced Navigation Technology

응용 및 융합 기술

J. Adv. Navig. Technol. 25(5): 415-425, Oct. 2021

블록체인 기반의 디지털 금융보안 아키텍처에 관한 연구

Study on Digital Finance Secure Architecture based on Blockchain

김 경 진[1] · 홍 승 필[2*]
[1]성신여자대학교 융합보안공학과
[2*]㈜한컴위드

Kyoung-jin Kim[1] · Seng-phil Hong[2*]
[1]Department of Convergence Security Engineering, Sungshin Women's University, Seoul 02844, Korea
[2*]HANCOM WITH, InC, BunDangGu, SeongNam Si, Gyoung Ki Do, Korea

[요 약]

금융권은 디지털 전환 흐름에 맞춰 새로운 기술로 금융서비스를 제공하고 있다. 그 중 전세계 금융업계의 관심을 주목받고 있는 오픈뱅킹(Open Banking)은 고객 편의성과 데이터 활용에 극대화된 서비스 환경이다. 빠른 디지털 패러다임의 전환은 데이터 공유로 인한 정보유출, 해킹 등 보안 문제 역시 우려된다는 불안감도 증가시켰다. 이러한 부정적인 시각을 극복하지 못한다면 금융서비스 발전을 저해하는 요인이 될 것이다. 본 연구에서는 디지털 금융 생태계에서 데이터를 안전하고 포괄적 관리할 수 있는 보안 거버넌스 체계를 제시한다. 이는 오픈뱅킹 서비스 환경에 초점을 맞춰 현업 종사자들에게 디지털 금융보안 아키텍처를 제시함으로써 기술적 적용 방안을 마련한다. 금융 IT가 변화하는 환경에서 오픈뱅킹 서비스를 도입하고 활용할 수 있는 종합적 정보보호 체계를 제시함으로써 본 연구의 가치가 있다고 볼 수 있다.

[Abstract]

In line with the trend of the digital transformation, the financial sector is providing financial services with new technologies. Among them, the open banking, which is drawing attention from global financial industry, is a service environment that maximizes customers' convenience and data utilization. In addition, the shift in the digital paradigm has also increased anxiety that security problems such as hacking and information leakage caused by data sharing are also concerned. A failure to overcome the negative view will hinder the development of financial services. This study presents a security governance system that can safely and comprehensively manage data in a digital financial ecosystem. This prepares a technical application plan by presenting a digital financial security architecture to field workers, focusing on the open banking service environment. It can be seen that this study is worthwhile by presenting a comprehensive information protection system that allows financial IT to introduce and utilize open banking services in a changing environment.

Key word : Blockchain, Digital finance secure architecture, Digital finance secure governance, Open banking, Privacy.

https://doi.org/10.12673/jant.2021.25.5.415

Received 15 September 2021; **Revised** 27 September 2021
Accepted (Publication) 22 October 2021 (30 October 2021)

***Corresponding Author ; Seng-phil Hong**

Tel: +82-31-622-6211
E-mail: philhong99@naver.com

Ⅰ. 서 론

코로나19로 인해 2020년 전세계 IT 소비가 +0.3%로 성장 정체를 겪는 가운데, 이러한 위기 극복을 위해 기업들은 클라우드, 빅데이터, AI 등 디지털 기술에 투자를 증가하면서 디지털 전환(Digital Tranformation)을 가속화하고 있다[1]. 디지털 전환 과정은 금융산업에도 영향을 주어 은행의 밸류체인(Value Chain) 전반에 거쳐 혼란을 가져오면서 은행업의 전통적인 산업 구조가 바뀌고 있다. 가트너(Gartner)는 2030년까지 현재 은행의 80%가 폐업하거나 타은행에 흡수될 것이라고 예측한 바 있다[2]. 코로나19가 비대면 금융거래를 더욱 활성화시키는 요인으로 등장하면서 뱅킹은 필요하지만 은행은 사라질 수 있다는 말[3]이 현실화되고 있는 것이다.

디지털 전환 흐름에 맞춰 금융권은 새로운 기술로 편의성이 극대화된 디지털 금융서비스를 제공하여 금융 생태계를 재편하고 있다. 그중에서도 오픈뱅킹(Open Banking)에 대한 전세계 금융업계의 관심이 높다. 여기서 오픈뱅킹이란, 그림 1에서 보여지는 것과 같이 특정 은행이 제공하는 금융서비스를 다른 은행이나 핀테크 기업 등도 API를 통해 이용할 수 있도록 개방하는 것으로 '개방형 금융결제망'이라 할 수 있다[4]. 국내 금융플랫폼의 발전을 보면[5], 1999년 인터넷 뱅킹을 시작으로 2010년에는 스마트폰 뱅킹, 2017년에는 핀테크 뱅킹이였다면, 2019년에는 금융당국 주도로 '금융결제 인프라 혁신방안'정책에 따라 오픈뱅킹을 본격적으로 시작하였다.

하지만 가속화되는 디지털 전환에 대해 보안 문제에 대한 우려도 점점 커지고 있다. 금융보안원에서는 2021년에 금융권의 디지털 금융 및 사이버보안 10대 이슈를 발표하였다[6]. 이 중 보안관점에서 주목할 만한 이슈를 보면, 1) 언택트 및 비대면 금융서비스 확산, 2) 원격근무 등 업무 환경 변화, 3) 고도화되는 사이버 공격 증가 등이 있다. 우선, 코로나 19 장기화로 인해 언택트 및 비대면 금융서비스가 더욱 확대되고 있다. 조사에 따르면[7], 인터넷 뱅킹이나 비대면 결제 이용 규모가 작년 대비 17%가 증가하였다. 더불어 비대면 실명확인 절차의 취약점 악용, 금융 앱 위변조 등 비대면 금융을 타겟으로 한 금융사기가 고도화되고 있다. 둘째, 원격근무나 화상회의가 금융권 기업문화로 자리매김하고 사이버보안 역시 기업 내부에서 외부로 확대되면서 상대적으로 보안통제가 어려워졌다. 화상회의 솔루션도 주요 공격대상으로 부각되어, 회의 중 파일탈취나 악성코드 유포 등 공격 수행이 가능해졌다. 셋째, 고도화되는 사이버 공격 증가는 작년 금융권을 대상으로 활발하던 랜섬웨어(ransomware)와 랜섬디도스(ransom ddos) 공격이 여전히 지속될 것으로[8], 특히 악용 가능한 IoT 기기의 보급 증대 등으로 공격 위험이나 파급력은 더욱 가중될 것으로 보고 있다. 또한 딥페이크(Deepfake) 등 신기술과 보이스피싱이 결합해 정교해지면서 더욱 위협적으로 진화하고 있다.

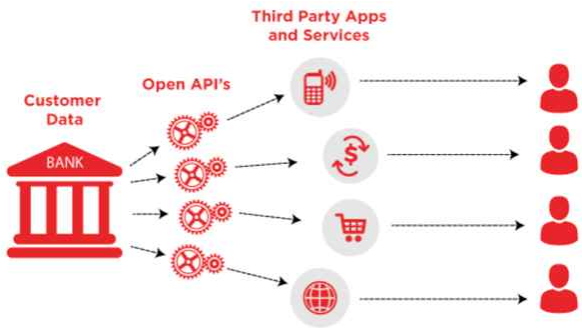

그림 1. WSO2 Open Banking 구조
Fig. 1. WSO2 Open Banking Concept (참고 : Cashdash, https://blockchainhub.net/blockchains-and-distributed-ledgertechnologies-in-general)

금융산업의 디지털 및 데이터 발전을 위해서는 상기 언급된 이슈들을 해결하는 것이 우선이다. 이에 본 논문에서는 금융 분야에서 각종 리스크 및 사이버 위협의 선제적 대응을 하기 위한 거버넌스 체계를 제시하는 것을 목적으로 한다. 이를 위해 다음과 같은 주제에 초점을 두고자 한다. 첫째, 현재 금융플랫폼 변화에 맞춰 사용자들의 보안과 신뢰에 대한 관심이 매우 증가한 최근 상황을 반영하여 오픈 뱅킹을 중심으로 조사 분석하고 연구를 수행한다. 둘째, 보안 문제는 정책이나 기술이라는 부분적 해결책만으로는 한계가 있으므로 거버넌스 차원의 접근이 필요하다. 이에 디지털 금융서비스를 제공하기 위한 거버넌스 체계를 제시한다. 셋째, 제시한 거버넌스를 기반으로 실제 엔지니어 입장에서의 적용 가능한 기술적 방안을 아키텍처로 제시하여 실 적용성을 마련한다.

본 논문의 구성은 다음과 같다. 2장에서 오픈뱅킹의 정책과 함께 금융보안 거버넌스 및 보안기술에 대한 현황을 살펴본다. 디지털 금융보안 관련하여 수행된 선행연구가 있는지 3장에서 알아보고, 상기 내용을 기반으로 4장에서 문제점을 도출한다. 제안한 거버넌스와 아키텍처는 5장에서 소개하고 이에 대한 당위성을 6장에서 설명한다. 마지막으로 7장에서 결론 및 향후 연구를 제시한다.

Ⅱ. 이론적 배경 및 논의

2-1 오픈뱅킹의 정책과 보안 이슈

오픈뱅킹의 배경은 은행 및 핀테크사업자가 은행계좌에 기반한 금융서비스를 보다 쉽고 합리적인 비용으로 개발할 수 있도록 지원하여 지급결제시장을 개선하고 신규 시장진입자에게 공정경쟁 환경을 제공하기 위한 기반을 마련한 것이다.

오픈뱅킹은 영국이 2018년 최초로 시행한 후, 우리나라를 비롯해 호주, 일본, 싱가포르, 홍콩 등으로 빠르게 확산되었다. 해외 추진현황을 살펴보면, 영국의 오픈뱅킹은 은행 API를 핀테크 기업에 수수료 등 차별없이 제공하도록 의무화하고 고객의 자기결정권을 강화하였다. 또한, 영국의 9대 주요은행은 오픈 API를 통해 타 은행의 고객 정보를 받아, 계좌통합서비스(Account Information Service), 지불개시서비스(Payment

Initiation Service) 등 다양한 서비스를 시행하고 있다. 최근 오픈뱅킹의 확장으로 2021년 3월 오픈 파이낸스를 제시하여 은행뿐 아니라 보험, 증권 등 타업권에서 보유한 고객 정보도 공유하는 개념을 도입하였다[9],[10].

영국 외 다른 국가에서도 오픈뱅킹 정책을 추진하고 있다. 호주는 오픈뱅킹 권고안을 발표하여 4대 주요은행이 신용, 직불카드, 예금 등부터 시작하여 전 은행권이 점진적으로 모든 금융상품에 대한 API(application programming interface)를 공개 예정이다. 일본은 은행법 개정을 통해 은행이 오픈 API 구축에 노력할 의무를 부여하고 있으며, 싱가포르는 정부주도의 금융데이터 개방 정책을 추진 중이다[10].

우리나라의 경우, 오픈뱅킹을 2가지 정책으로 구현하고 있다. 첫째는 은행권과 금융결제원이 공동으로 구축한 '오픈뱅킹 시스템'으로 은행과 핀테크 사업자는 이 시스템을 이용하여 다양한 기능을 편리하게 개발할 수 있게 지원해주고 있고, 둘째, 마이데이터업자(법적 용어는 '본인신용정보관리업')가 고객 동의를 받아 금융회사가 보유한 고객 정보에 접근하는 '오픈뱅킹'업을 수행할 수 있도록 하는 것인데, 일반적으로 '오픈뱅킹 시스템'을 도입하는 첫번째 정책을 '오픈뱅킹'이라 일컫고 있다[13]. 국내에서 오픈뱅킹을 전면 도입한 이후, 가입자 수가 빠르게 증가하며 현재 경제활동인구의 72%가 오픈뱅킹을 이용중으로 조사되었다[12]. 즉, 오픈뱅킹의 빠른 성장과 함께 향후 제2금융권 참여시 더욱 활성화될 것으로 예상하고 있다. 이러한 예측은 설문조사로도 알 수 있는데 조사결과에 따르면[13], 이용자들은 오픈뱅킹 서비스에 대체로 만족하고 있다고 응답하고 있다. 하지만 같은 설문조사에서 오픈뱅킹 서비스에 대해 느끼는 불안 등과 같은 질문에 응답으로 57.9%가 개인정보 유출 등 보안에 대한 불안감이 존재한다고 답변하였다. 이와 유사한 결과로 영국 PwC(price waterhouse coopers)의 오픈뱅킹 설문조사에 따르면[9], 48%가 해킹, 정보누출 등 보안 관련 위협이 이용을 주저하는 주요 요인이라고 답변하였다. 이러한 조사결과에 비추어볼 때 오픈뱅킹 서비스 제공자의 데이터 보안 역량 부족, 데이터 공유로 인한 정보유출 등으로 인한 보안사고 위험을 여전히 우려하고 있다.

오픈뱅킹은 금융소비자와 참여 기업에게 이익을 제공할 수 있지만, 보안사고 및 취약점에 대한 철저한 대비가 갖춰지지 않는다면 이러한 부정적 시각을 극복하기 어려울 것이고 금융서비스 발전을 저해하는 요인이 될 것이다.

2-2 금융보안 거버넌스 현황

국내 금융권 보안 수준은 전자금융거래법, 전자금융감독규정 등에 대한 최소한의 법규 준수 활동만을 하고 있으며, 이러한 활동만으로는 지능화되고 고도화되는 보안위협에 효과적인 대응이 어렵다. 이미 해외에서는 보안 문제를 정보보호 부서나 기술적 관점의 단편적 해결이 아닌, 기업 거버넌스 관점에서 전사적 차원의 보안 강화를 추진하고 있다. FINRA(financial industry regulatory authority)가 발표한 보고서에 따르면[14], 효과적인 사이버보안을 위해서는 기업 내 경영진 주도의 보안 거버넌스가 활성화되어 있어야 한다는 것을 확인할 수 있다. 즉, 미국도 디지털화가 진행됨에 따라 업무 효율화를 지향하면서 백오피스시스템의 디지털화가 진행되고 있다. 이러한 변화가 금융기관의 사이버보안에 영향을 미치게 되면서 본 보고서에 명시된 지침이 미국에서 큰 의미가 있다고 여겨진다[15].

우리나라 경우, 회사 내 각종 기밀정보 및 거래 정보를 보호하기 위하여 보안계획을 수립하고, 정보보호 시스템을 운영하며 정보보호 교육 및 훈련, 취약점 관리, 외부인력 관리, 각종 컴플라이언스 대응, 개인정보보호 등 다양한 정보보호 활동을 수행하고 있다[16]. 하지만 이는 기업의 전반적인 정보보호 활동으로써, 금융정보 및 업무 특성을 반영하여 정보보호 활동을 적용하기는 여전히 어려움이 있다. 더불어 금융회사가 디지털 전환으로 개편된다면 현재 적용 중인 정보보호 활동체계에 많은 변화가 필요할 것이다.

정부에서는 금융보안 거버넌스의 필요성을 인지하고 직면한 문제를 해결하기 위해, 국내 금융회사의 자율보안체계 구축을 지원해주는 '금융보안 거버넌스 가이드'를 발표했다[17]. 국제표준 정보보호 거버넌스(ISO/IEC 27014)를 기반으로 한 국내 기본 지침서로써 금융보안 거버넌스의 7대 기본원칙을 제시하고, 최고경영층 주도로 전사적인 정보보호 체계를 구현하기 위한 전략을 제공하고 있다. 다만 금융보안 거버넌스 체계 도입을 위해 제시하는 지침서로, 금융보안 환경에서 직접 활용할 수 있는 종합적 정보보호 거버넌스를 제시하지는 않는다.

2-3 디지털 금융환경을 위한 보안기술 현황

1) 안전한 데이터 공유를 위한 블록체인 기술

오픈뱅킹은 중앙 집중화가 아닌 네트워크의 개방을 통해 금융데이터를 다른 기관과 안전하게 공유할 수 있게 한다. 즉, 오픈뱅킹을 통해 금융 관련 기업이나 기관에 흩어져 있는 고객 데이터를 확보할 수 있게 되었다. 이러한 인프라는 데이터를 활용하는 측면에서 장점이 될 수 있으나 보안적 이슈 역시 우려된다. 오픈뱅킹은 데이터 공유를 기반한다. 오픈뱅킹을 잘못 사용하며 고객 데이터에 대한 통제력 상실과 더불어 고객 데이터 유출로 이어질 수 있다. 이 문제에 대해서 블록체인 기술의 특성을 이용하여 해결하려는 연구들[18]-[20]이 존재한다. 이러한 연구들의 공통점은 블록체인의 자기주권(self-sovereign) 특성이 고객 또는 이용자가 자신의 데이터를 스스로 통제하고 기업은 고객의 허락하에 적극적으로 고객 데이터를 비즈니스에 이용하는 방안으로 작용하여 이용자의 개인정보 자기결정권을 보장할 수 있다.

연구뿐만 아니라 최근 금융권에 블록체인 기술을 상용화한 사례를 보면, 미국의 경우 블록체인을 응용한 지급 결제 시스템을 개발하였으며, 중국은 정보의 포괄적 관리를 위한 블록체인 기반 정보 공유 플랫폼을 개발하였다[21]. 국내 역시 블록체인 기술을 활용한 많은 연구가 추진 중인데 대표적으로 신한은행의 경우 국내 금융권에서 첫 DID(Decentralized identity) 서비스

표 1. 국내 금융산업에서 블록체인 기술을 활용한 최근 사례
Table 1. Recent cases using blockchain technology in domestic financial industry

Organization	System	Feature
Shinhan bank	Blockchain qualification system	Verification of certificate documents necessary for non-face-to-face loan work using blockchain technology.
Nonghyup bank	P2P financial certificate blockchain service	P2P financial investors' "Certificate of Principal and Interest" is stored in blockchain to ensure the integrity of the certificate and inquired through the app.
Kyobo life insurance	Optimum insurance coverage and on-going services	Insurance information and statistics management are convenient by establishing a blockchain-based payment system joint network.
Fintech company[1)]	Overseas remittance service	Safe remittance to other countries using an electronic wallet platform operated by blockchain technology, and track the process.

[1)] MOIN, Coinone Transfer, etc.

Source: [21], [22] 수정

표 2. 프라이버시 보호 기술 요소별 특징 비교
Table 2. Comparative analysis of PETs

Factor	Feature	Pros	Cons
Differential Privacy (DP)	A technology that combines personal data with many other people's data to obtain statistics.	Obtain statistically significant data without infringing on personal information.	Controlled data tends to be relatively less accurate and useful due to noise.
Privacy model	How to define possible forms of inference and quantitative risks to privacy exposure.	As a pseudonym information de-identification technology, typical k-anonymity can respond to connection attacks.	k-anonymity lacks diversity. l-diversity exists according to the protection model, such as being vulnerable to leaning and similarity attacks.
Synthetic Data (SD)	A de-identification method that generates imitation data so that personal information contained in the original data can be protected, analyzed, and utilized.	Increased the number of samples indefinitely	Reduced prediction accuracy due to inconsistency
Privacy Preserving Data Mining (PPDM)	Technology that analyzes data while protecting personal information in big data containing personal information.	Practical use through randomization techniques used for statistical processing and machine learning	Ambiguous effectiveness depending on the computing environment
Homomorphic Encryption	Cryptographic technology that enables data operations while encrypted.	Theoretically, it has quantum-resistant encryption and turing completeness.	Limit of external transmission processing speed by encrypting data.

Source: [23] 수정

도입으로 비대면 실명확인 절차를 통해 인증을 간소화하였다. 그 외 국내 은행, 보험사 등 금융산업에서 블록체인 기술을 활용한 사례는 표 1과 같다. 표 1의 사례를 보면 자기주권신원을 위해 중앙집중기관을 대신하여 개인의 신원 데이터를 관리하거나, 블록체인의 강력한 보안 특성인 무결성을 이용하여 증서 및 증명서류 등을 검증하는 역할로 기술을 활용하였다. 본 연구에서는 오픈뱅킹에서 블록체인 활용 방안을 제시함으로써 기존 연구들과의 차별성을 둔다. 유사한 연구로써 Zhiyu Xu (2020)[19]는 오픈뱅킹의 요구사항을 충족하기 위해 블록체인을 적용한 PPM(Provenance-Provided Data Sharing Model)을 제시하였으며, 스마트 컨트랙트, 데이터 레이어 등을 통해 안전한 방식으로 은행 간 전송 및 교환방안을 제시하였다. 우리는 데이터 전송 및 교환 기술을 포함한 거버넌스 체계를 제시함으로써 디지털 금융 서비스에서 포괄적 관리 방안을 제안한다.

2) 분산된 정보 통제를 위한 개인정보보호 강화 기술

전통적인 은행 시스템은 중앙 집중적인 관리에 용이하도록 설계되어 있다. 은행 시스템의 거래는 돈의 이동을 의미하기에 추가적인 기능은 기존의 시스템 확장을 통해 기능을 구현하려는 경향이 강하다. 이로 인해 디지털 금융플랫폼으로의 변화는 여전히 근본적인 취약점이 존재하고 새로운 위협에 즉각적인 대응이 어렵다. 특히 코로나 19로 비대면 서비스가 더욱 활성화되는 상황에서 사이버 위협 또한 노출되어 있다. 이와 같은 여러가지 요인들로 인해 디지털 금융서비스를 제공하는 오픈뱅킹은 기존 오프라인 형태에 준하는 보안성 확보를 위해 철저한 보안통제 대책이 필요할 것이다.

오픈뱅킹은 데이터를 활용하는 관점에서 정보 유출에 대한 이슈는 계속 언급되어 왔다. 특히 고객의 프라이버시를 보호하는 방안으로써 프라이버시 보호 기술(PETs; Privacy Enhancing Technologies)을 활용하고 있다. 여기서 PETs는 개인정보 활용을 최소화하고 보호를 강조해 개인에게 권한을 부여하는 개인정보보호 원칙을 구현한 기술이다[23]. 이 기술은 기존의 프라이버시를 위한 기술뿐만 아니라 새로운 암호기술을 만들거나 신기술과 결합하면서 꾸준히 발전하고 있다. 표 2는 최근 PETs의 대표적인 기술을 분석한 것으로 하나의 기술을 단독으로 이용하는 것보다는 장점을 극대화할 수 있는 기술들끼리 결합하

여 시스템에 적용하는 것을 권장한다.

Ⅲ. 디지털 금융보안에 관한 선행연구

코로나19와 함께 비대면 거래 환경의 확대로 금융산업은 사용자 편의성에 맞춰진 금융서비스를 제공하는 환경으로 변화하고 있다. 이러한 디지털 전환 패러다임으로 최근에 금융산업이 어떻게 변화하고 어떤 방향성을 가져야 하는지에 대한 연구가 진행되고 있다. 박정국과 김인재(2020)[10]는 오픈뱅킹 시행이 가져올 주요 변화와 활성화를 위해 정책방향을 연구하였으며, 은행권과 금융당국 등의 관점에서 추진과제를 제시하며 오픈뱅킹의 성공적인 안착과 활성화를 위한 연구 방향을 언급하고 있다. 송민택과 이원부(2021)[25]는 통합기술수용이론을 기반으로 여러 요인에 따라 사용자의 오픈뱅킹 수용의도에 어떤 영향을 미치는지 연구하였는데, 분석 결과 기대노력, 성과기대, 인지위험 순으로 영향을 미치는 것으로 보아 기존보다 사용이용이하고 편의성이나 혜택 등의 경제적 효과에 기대하는 것을 확인할 수 있었다. 그 외 기술적으로 접근한 연구에서는 오픈뱅킹 API를 활용하여 애플리케이션, 시스템, 플랫폼 등을 개발함으로써 다른 기술이나 산업과 융합했을 때 정보의 효율성을 보여주었다[18],[26],[27].

상기 언급된 연구들은 오픈뱅킹의 리스크나 보안규제보다는 오픈뱅킹의 발전과 활성화를 위한 방향성에 주력한 것을 알 수 있다. 하지만 보안은 금융 시스템에서 서비스의 완성을 위한 필수 요소이다. 이와 관련된 많은 연구들은 보안과 함께 금융서비스의 신뢰가 중요하다는 것을 인지하고 연구를 추진하고 있다. 예전부터 Kim과 Prabhakar(2004)[28]는 사용자의 신뢰가 인터넷뱅킹을 도입하는 데 있어 중요한 영향을 주고 있다고 언급하였으며, Ha와 Akamavi(2009)[29]는 사용자의 신뢰가 이후 지속적인 거래 의지에 영향을 주고 있다는 것을 보여주었다. 또한 John(2012)[30]은 온라인뱅킹 결정 요인에 관한 연구에서 보안과 신뢰가 중요한 요인으로 제시하고 있다. 현재 금융변화 플랫폼에 맞춰 최근 금융보안 연구들을 살펴보면, 김대현(2021)[31]은 금융권의 디지털 금융 및 사이버보안 10대 이슈에 대한 타당성뿐만 아니라, 전자금융의 환경에 대한 전망과 시사 및 문제점을 구체적으로 설명하고 있다. 전용진(2021)[32]은 모바일뱅킹 보안과 정보 신뢰가 사용자 태도 및 사용 의지에 얼마나 어떻게 영향을 미치는가 연구하였다. 여러 요소 중 안전성, 고객 신용, 정보 신뢰가 사용 만족도에 영향을 준 것을 확인하였다. 편의성 인지는 보안이 영향을 미치고 있는 것을 확인할 수 있었다. 유효선, 김정덕과 김수진(2020)[33]은 모바일 전자금융서비스와 관련한 기존의 보안성 심의 제도와 금융분야 취약점 분석하여 보안점검 항목 개선안을 도출함으로써 변화된 금융서비스의 보안성이 중요한 요인임을 확인할 수 있었다.

상기 연구들에서 알 수 있듯이, 기존 연구들은 변화된 금융보안 관련하여 문헌이나 설문조사로 현황 파악하거나, 대응을 위한 정책 및 부분적 기술적 대안을 제시하는 연구가 주를 이루었다. 하지만 보안 문제는 정책이나 기술과 같이 단편적인 관점으로 해결하기에는 한계가 있다. 특히 금융정보 위협의 경각심과 함께 은행업자, 금융권자 등 이해관계자들의 전방위적인 대응이 필요하기 때문에 거버넌스 차원의 접근이 요구된다. 본 연구에서는 앞에서 검토한 오픈뱅킹 신뢰 이슈를 토대로 한 선행연구를 근거로 디지털 금융 위험의 대응을 위한 거버넌스 체계를 제시하고자 한다. 유사한 관점의 Sushil prakash와 ilaventhan gunalan(2020)[34] 연구는 디지털 거버넌스를 위한 블록체인을 적용하여 새로운 비즈니스 모델을 제시하고 있으나, 금융산업이 아닌 포괄적 디지털 거버넌스를 위해 블록체인을 다루고 있어 금융산업에 직접적으로 적용하기는 한계가 있다.

본 연구는 현재 오픈뱅킹을 포함한 디지털 금융플랫폼에서 사용자들의 우려를 감소시키고 신뢰보장을 위해 어떻게 금융기관이 대응을 해야 하는지에 관한 연구이다. 그러므로 기존의 전통적인 금융산업에서의 보안 체계나 디지털 환경에서의 부분적 대안 연구와는 다른 관점으로 선제적 대응을 하기 위한 연구를 수행한다.

Ⅳ. 문제점 제시

앞서 검토한 오픈뱅킹 현황과 보안 이슈를 살펴보면, 디지털 금융서비스를 사용하는 이용자와 참여 기업에게 이익을 제공할 수 있지만 보안사고에 대한 대비가 철저하게 갖춰지지 않는다면 선행연구에서 분석했듯이 금융서비스 발전을 저해하는 요인이 될 것이다. 보안이 중요하다는 것을 인지한 금융기업과 연구소에서는 디지털 서비스를 제공하는 금융산업에서의 사이버 위협 및 위험에 대한 관심을 갖고 일찍이 연구를 추진하고 있다. 하지만 앞서 2-1절과 2-2절에서 언급한 것과 같이, 변화된 플랫폼에서도 국내 금융권 보안수준은 여전히 최소한의 법규준수 활동만을 유지하고 있으며, 특히 오픈뱅킹 이용기관의 법적 근거가 없으므로 보안수준을 보장하기에는 제한이 있다. 이를 문제로 제기한 논문이나 연구들도 법이나 정책방안으로만 해결안을 제시하고 있다. 최대현 (2019)[35]은 정보유출에 대비하여 오픈뱅킹 중계기관을 거치지 않는 고객과 금융회사 간에 직접 인증하는 방안으로써 정책 및 모델을 제시하였으며, 권남훈과 김인석(2020)[36]은 오픈뱅킹에 대한 규제개선 방안으로 전자금융거래법을 보완하는 방향성을 제시하였다. 기술적 관점 역시 2-3절에 언급한 것처럼 접근제어, 암호화, 이상탐지 등의 부분적 대안으로 연구를 추진하였다. 하지만 이러한 단편적인 해결안으로는 디지털 전환 패러다임에서 지능화되고 고도화되는 사이버보안 위협에 효과적인 대응이 어렵다.

위와 같은 한계로 인해 정책 및 지침 위주의 거버넌스 연구들도 추진되었다. 특히 국내에서는 금융보안 거버넌스 체계 도입을 위해 지침서를 발표하였다. 하지만 이는 금융기업에 거버넌스 체계에 도움을 주기 위한 가이드일 뿐이며, 금융보안 환경에서의 거버넌스 모델을 제시하는 것은 아니여서 실제 엔지니

어 입장에서 기술적으로 적용하기에는 어려움이 있다.

금융산업에서 보안 거버넌스의 필요성은 인지하고 있으나, 거버넌스 자체의 특성상 구현의 어려움 역시 존재한다[24]. 특히, 기존의 조직에서 주로 지시에 의한 긴급업무를 착수하거나 대책을 시행하기 위한 일회성 정책추진, 보안사고 시 사후대응 등이 주를 이루고 있어 시스템화된 기능 구현의 어려움이 존재한다. 이는 디지털 금융 특성상 보안사고 발생 시 빠른 탐지와 함께 교정이 필요한 상황에서 효율적이지 못한 구조 체계가 될 수 있다.

기존 전통적인 금융거래 구조와 달리 오픈뱅킹은 금융기업, 고객, 그리고 핀테크 기업과 같은 정보를 활용하는 이용기관 등의 거래 연계구조가 복잡하다. 금융사고가 발생했을 때 금융 조직 및 시스템의 복잡도로 인해 이해 당사자 간 역할과 책임(R&R, Role&Responsibility) 관계가 불명확하여 해소되지 못한 부분이 아직도 존재하고 있다[35]. 이는 추후 기관 간의 분쟁, 금융소비자의 피해 등 예기치 못한 혼란이 발생할 수 있다. 즉 기존에 적용되던 거버넌스 체계를 통해서 종합적이고 효율적으로 방어하기 위한 디지털 금융환경의 적합한 거버넌스를 도출하기란 쉽지 않은 과제이다.

보안 문제는 정책이나 기술과 같이 단편적인 관점으로 해결하기에는 한계가 있다. 특히 금융정보 위협의 경각심과 함께 은행업자, 금융권자 등 이해관계자들의 전방위적인 대응이 필요하기 때문에 거버넌스 차원의 접근이 요구된다. 하지만 상기 여러 연구에서 우려하듯이 일반적인 거버넌스 체계를 제시한다면 실제 적용할 수 있는 방안과는 차이가 발생할 것이다.

본 연구에서는 오픈뱅킹 서비스의 안전성과 소비자 보호로 범위를 한정하여 실제 접근하기 유용한 방안으로 디지털 금융서비스 환경에 적합한 거버넌스 체계를 제시하며, 현업 종사자들에게 아키텍처로써 기술적 방안을 제시하고자 한다. 금융산업에서는 디지털 금융보안을 위한 거버넌스 체계 연구가 없었으므로 본 연구는 금융 분야에 적합한 새로운 거버넌스 체계를 제시하고 나아가 실제 적용할 수 있는 기술적 방안을 제시하는 것에 의의가 있다고 할 수 있다.

Ⅴ. 디지털 금융보안 아키텍처 제안

5-1 디지털 금융보안 거버넌스 – 오픈뱅킹

금융권은 데이터를 통해 기업이나 기관에 흩어져 있는 고객 데이터를 확보하고 오픈 API에 기반한 인프라를 통해 데이터를 실시간으로 얻을 수 있는 환경이 되었다. 더불어 이러한 금융 IT 환경의 변화는 보안사고가 지속적으로 발생하는 환경이 되면서 금융보안 위험에 효과적인 관리가 필요하게 되었다. 보안사고 발생 시 신속한 사이버 복원력 향상을 위해 전사적인 금융보안 거버넌스 구축이 요구되고 있다. 그림 2는 금융 IT가 변화되는 환경에서 도입할 수 있는 디지털 금융보안 거버넌스 개념도를 나타내고 있다.

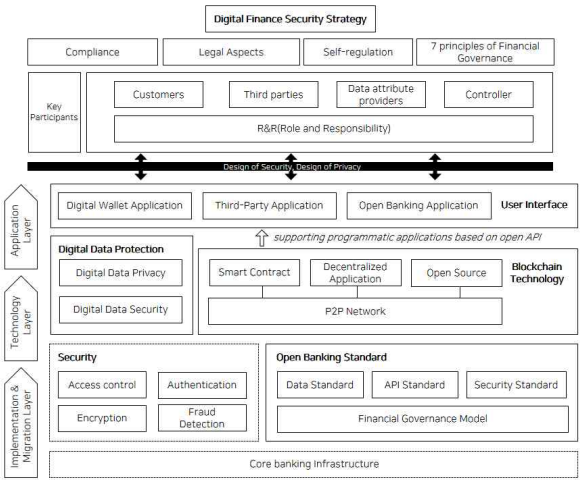

그림 2. 디지털 금융보안 거버넌스 개념도 – 오픈뱅킹 중심
Fig. 2. Concept of DFSG(Digital Finance Security Governance) – Open banking

최상위에 있는 디지털 금융보안 전략(Digital Finance Security Strategy)은 사이버 환경에서 금융권의 업무 특성을 반영한 보안 전략으로써 자연스럽게 정보보호 활동을 할 수 있게 하는 것이 목표이다. 거버넌스의 주요 조건으로는 금융 관련 법률 및 규제(Compliance / Legal Aspects)를 이해하는 것이 중요하며, 특히 스스로 보안을 책임지는 자율적 보안 체계(Self-regulation)를 확립하도록 규정한다. 또한, 금융보안 거버넌스의 7대 기본원칙에 적합하게 거버넌스 체계를 확립한다.

거버넌스는 서비스를 이용하는 금융소비자(Customers), 핀테크 기업 등 데이터를 활용하는 이용기관(Third parties), 은행 등 데이터와 API를 제공하는 제공기관(Data attribute providers)으로 금융 관련 이해관계자들의 이해를 조정하여 의사결정을 하는 것이다. 특히 디지털 금융확대로 이해관계자들의 역할과 책임을 명확히 하고 이에 따른 합당한 권한 부여(R&R)가 필요하다. 금융 관련 이해관계자들에게 정보보호의 비즈니스 가치를 보장할 수 있도록 한다.

여기까지가 관리적 거버넌스 체계를 이루고 있다면 하단에는 실무 및 현업조직이 갖춰야 하는 기술적 대안 체계이다. 단계는 크게 3단계로 구분하며, 본 연구의 범위는 디지털 금융서비스의 핵심인 오픈뱅킹을 중점으로 기술적 방안을 제시한다.

Implementation & Migration Layer는 기존 은행 인프라를 기반으로 디지털 금융보안을 구현할 수 있는 통합 환경을 제공한다. Open Banking Standard[11]는 오픈뱅킹에서 데이터 공유를 용이하게 해주는 지원으로 데이터, 기술, 그리고 보안을 다루는 일련의 규격과 규칙을 제공한다. 또한, 금융 시스템에 정보보호 및 개인정보보호 관련하여 접근제어(Access control), 인증(Authentication), 암호화(Encryption), 이상탐지(FDS Detection) 등 구현된 기본적인 보안기술을 포함한다.

Technology Layer는 디지털 금융서비스에 맞춰 IT 보안기술이 운영될 수 있는 단계이다. 디지털 금융, 특히 오픈뱅킹에서 가장 우려되는 데이터 보안 관련하여 Digital Data Protection에

서는 사이버상의 공격과 위협에 대응할 수 있는 Data Security와 Data Privacy 기술을 적용한다. 그리고 디지털 금융보안에 결합할 수 있는 신기술로는 P2P Network 기반의 블록체인 기술을 도입한다. 블록체인은 앞서 이론적 배경 및 선행연구에서 살펴봤듯이, 무결성 보장과 자기주권을 강화할 수 있는 보안 특성이 있다. 이러한 보안 기능과 함께 Smart Contract, Decentralized Application 등 블록체인에서 제공해주는 다양한 서비스 활용한다면 오픈뱅킹을 블록체인 기반의 안전한 서비스로 제공해 줄 수 있다. 기술 개발이 이뤄지는 단계에서는 Design by Security & Privacy를 원칙으로 개발을 권장한다.

Application Layer는 정의된 기술 표준에 따라 응용프로그램이나 애플리케이션, 앱 등 이해관계자들이 직접적으로 사용할 수 있고 활용할 수 있는 단계이다. 금융 소비자가 접근할 수 있는 애플리케이션뿐만 아니라 이용기관 및 제공기관에서 접근할 수 있는 애플리케이션으로 디지털 금융서비스를 이용할 수 있다. 금융소비자 관점에서는 금융서비스를 이용할 수 있으며, 이용기관 및 제공기관 관점에서는 맞춤형 API 및 애플리케이션을 개발하고 오픈뱅킹 시스템과 연결하여 새로운 수익 채널을 구축할 수도 있다.

5-2 블록체인 기반의 디지털 금융보안 아키텍처 - 오픈뱅킹

본 절은 오픈뱅킹 서비스 중심으로 어떠한 기술들을 적용하여 설계되고 구현될 수 있는지를 설명한다. 그림 3은 블록체인 기반의 디지털 금융보안 아키텍처를 보여주고 있다. 앞서 5-1절 개념도의 기술적 방안을 토대로 단계별 설명을 한다.

성공적인 오픈뱅킹 구현은 기존의 IT 인프라와 새로 도입되는 금융 및 보안기술이 얼마나 잘 융합되는가이다. 그래서 Implementation & Migration Layer는 기존의 은행 시스템인 Core Banking System과 핀테크 기업 등의 Third-Party System, 그리고 Legacy Systems을 비롯한 필수 타사 시스템을 통합할 수 있는 지점(point)을 제공한다. 정보보호를 위한 Security Management는 핵심 라이브러리로 암호화, 접근제어, 인증 등을 보유하고 있다. 이는 기존의 라이브러리를 참고하거나, 이미 자사 기업에서 고유의 보안기술이 있다면 활용할 수 있다.

Technical Layer는 신기술인 블록체인뿐만 아니라, 정보보호 및 프라이버시 보호를 위한 기술을 적용한다. 블록체인 기술은 Blockchain based P2P Network Platform으로 금융권에 실적용이 가능한 허가형 블록체인(permissioned blockahin)을 기반으로 인프라를 제공한다. 본 아키텍처 설계방안은 하이퍼레저 패브릭(hyperledger fabric)을 활용하고 있어 소비자, 금융기관, 핀테크 기업 등 허가된 참여자를 멤버쉽(membership)으로 관리한다. 참여자 수만큼 peer가 발생하며, 각 peer는 Smart Contract를 이용할 수 있으며, 특히 금융소비자의 경우 Digital Wallet Application을 Smart Contract로 배포하여 사용할 수 있도록 지원한다. 블록체인 네트워크에 보관되는 데이터를 누가, 어떻게 사용하였는지 스스로 확인할 수 있고 원한다면 자신의 데이터를 통제할 수 있도록 블록체인 기술을 통해 확장할 수 있다. 물

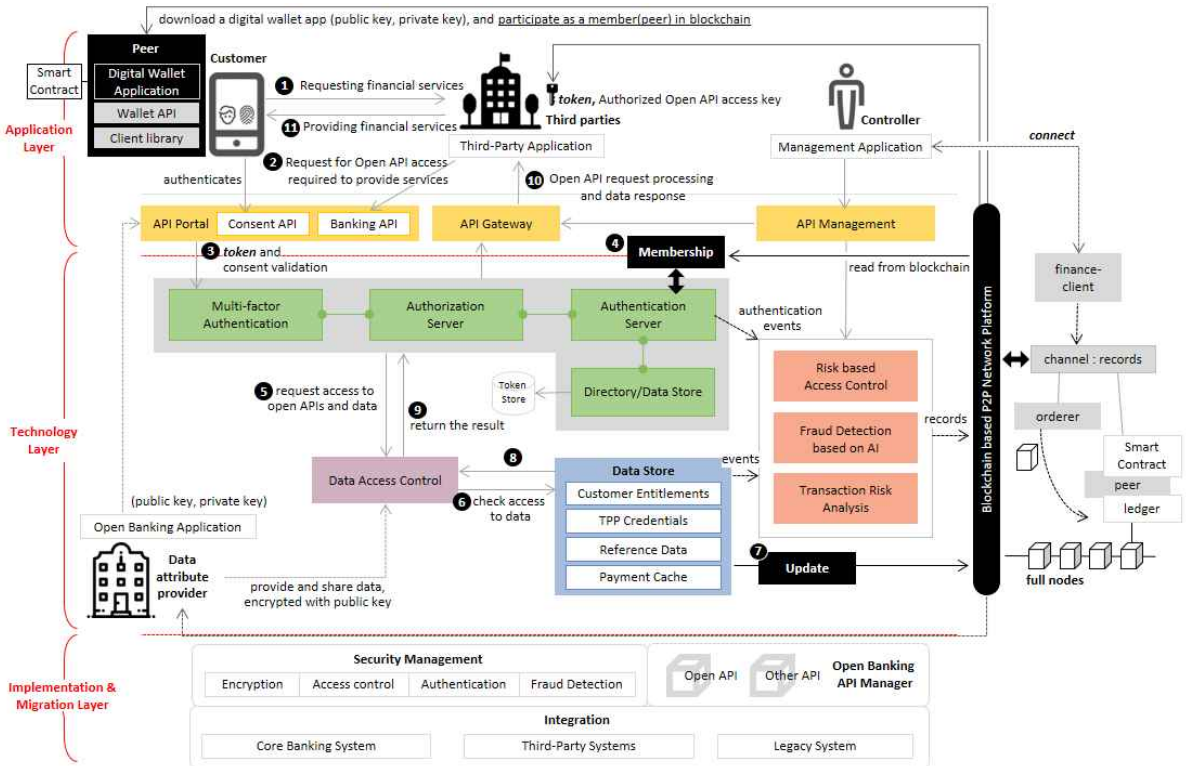

그림 3. 디지털 금융보안 거버넌스 아키텍처 - 오픈뱅킹 중심
Fig. 3. Design of DFSA(Digital Finance Security Architecture) - Open banking

론 이러한 정보는 암호화되어 업로드되기에 기밀성이 유지된다.

오픈뱅킹 서비스를 안전하게 제공하기 위해서 강력한 인증 모듈과 접근제어, 암호화된 데이터, AI(artificial intelligence)를 기반으로 한 이상 탐지까지 디지털 금융정보를 위한 보안기술을 제공한다. 오픈뱅킹을 구현하는 모든 금융권에는 인증 메커니즘이 필요하다. 여기에서는 기본 사용자 아이디 및 암호 인증 외에도 SMS(short message service), OTP(one time password), FIDO(fast identity online), PIN(personal identity number) 등 여러 인증요소를 결합하여 사용할 수 있는 Multi-factor Authentication을 지원한다. 이러한 인증요소는 Authorization Server와 Authentication Server를 거쳐 인증을 한다. 인증은 하이퍼레저 패브리에서 제공되는 멤버쉽을 통해 검증한다.

저장되는 데이터는 Data Store에서 관리된다. 오픈뱅킹의 공유 데이터는 금융고객 정보, TPP(third-party certification) Credential(신뢰된 타사 제공업체 정보), Reference data(참고 데이터), Payment cache(결제 기록) 등으로 본 정보에 접근하는 자는 권한이 있어야 한다. 이에 제공기관, 이용기관, 금융소비자 등은 Data Access Control 모듈에서 권한 검증을 거쳐 Open API 및 보안 데이터에 대한 무단 접근을 방지한다.

그리고 발생되는 모든 이벤트에서 부정행위를 방지 및 탐지, 차단하기 위해 Transaction Risk Analysis를 관리한다. 즉, 실시간으로 발생하는 트랜잭션의 위험 분석 및 부정행위를 탐지하여 조치할 수 있는 모듈이다. Fraud Detection based on AI는 최근 트렌드인 AI를 접목시켜 계정 및 결제 관련하여 지속적인 모니터링을 하고 알려진 이상 징후 및 알려지지 않은 이상 징후, 비정상적인 이벤트 시퀀스 등을 감지할 수 있도록 한다. 무단의 접근이 발생했을 때는 Risk based Access Control로 통제할 수 있도록 한다.

그리고 이러한 보안사고는 블록체인 네트워크를 통해 기록하여 다른 금융기관이나 기업에서 유사한 사고가 발생했을 때 빠른 조치 및 대응할 수 있도록 공유한다.

Application Layer는 금융소비자가 사용하는 Digital Wallet Application, 고객의 데이터에 접근하고자 하는 이용기관은 Third-Party Application, 고객 및 금융, 결제 등의 데이터를 보유하고 제공하는 기관은 Open Banking Application으로 오픈뱅킹 시스템에 접근할 수 있는 인터페이스를 제공한다. 그리고 필요하다면 허가형 블록체인 플랫폼을 관리할 수 있는 중재자(Controller)를 두어 오픈뱅킹 시스템의 보안사고를 확인할 수 있도록 한다.

은행 등 제공기관은 이용기관과 같은 제3자에게 API를 통해 데이터를 안전하게 공유할 수 있다. 여기서 제공되는 API는 Open Banking Standard를 준수하여 API를 설계하고 포괄적으로 관리할 수 있는 기능을 지원하기 때문에 Application은 API를 통해 호출(call)되고 피드백(feedback)을 제공해준다. 즉, API Portal를 활용하여 Application을 사용할 수 있다. 유효성 검사 및 접근 제어, 인증되지 않은 API 호출 방지 등 API의 보안 및 관리 역시 API Management에서 보장된다.

기술적 방안 3단계를 기반으로 금융서비스를 요청하고 제공받는 간략한 시나리오를 그림 3과 함께 설명한다. 그림 3의 아키텍처는 보안에 중점을 두기 위해 오픈뱅킹 서비스를 제공하는 구체적인 시나리오는 범위에서 제외하였다.

우선 오픈뱅킹 서비스를 사용하기 위해 사전준비가 필요하다. 금융소비자가 사용하는 Digital Wallet Application은 핀테크 기업 등 이용기관에게 금융서비스를 요청하고 결제를 지원하기 위해 필요하다. 스마트폰 같은 디바이스는 Digital Wallet Application을 소유하기 위해 블록체인 네트워크의 Peer로써 구성된다. 즉, 블록체인 멤버 구성원으로써 참여한다. 이용기관과 제공기관 역시 블록체인 구성원으로 참여하여 오픈뱅킹 데이터의 접근권한을 부여받는다. 이때 Open API 접근키로 블록체인 네트워크에서 발행해주는 Token으로 오픈뱅킹 시스템에서 본인을 인증할 수 있다. 사전준비가 완료되면, 블록체인 기반의 오픈뱅킹 서비스를 이용할 수 있다. 시나리오상의 주체를 금융소비자 C (Customers), 이용기관 T (Third parties), 제공기관 DP (Data attribute providers)라고 할 때 시나리오 순서는 다음과 같다.

① C는 원하는 금융서비스를 이용기관에 요청한다.

② T는 Open API 접근을 요청하기 위해 자신의 접근키(token)와 함께 오픈뱅킹 시스템에 요청한다.

③ 요청을 받은 시스템은 T의 접근키(token)와 C의 데이터 이용 관련된 동의(consent) 사항을 확인한다.

④ Multi-factor 인증을 통해 T의 유효성을 검사하고, 블록체인에 기록된 Membership을 이용하여 T를 검증한다.

⑤ 인증이 완료되면, Data Access Control을 통해 T의 권한과 함께 요청한 Open API 및 데이터가 가능한지 확인한다. 여기서 DP는 공유되는 데이터를 제공 및 검증에 관여할 수 있다.

⑥ 이용하고자 하는 C의 데이터가 있다면 데이터에 접근가능 여부를 확인한다.

⑦ Data Store의 데이터가 추가, 수정 및 삭제되는 변화가 발생하면 블록체인 네트워크 기록에 업데이트하고 데이터 접근 이벤트도 기록한다.

⑧ 필요한 데이터에 대해 접근이 가능하다면 결과를 전송한다. 필요하다면 DP 의 검증을 진행한다.

⑨ ⑧과 함께 Open API의 이용 가능에 관한 결과를 전송한다.

⑩ 요청한 Open API 처리 및 데이터에 관한 응답을 하고 이에 따라 T는 C가 요청한 금융서비스를 수행한다.

⑪ C는 결과에 따라 요청한 금융서비스를 제공받는다.

위와 같은 간략한 시나리오를 통해 오픈뱅킹 서비스를 제공하는 디지털 금융 보안 아키텍처의 흐름을 확인할 수 있다.

Ⅵ. 제안한 거버넌스와 아키텍처의 상관관계 분석

안전한 디지털 금융서비스를 위해 정보보호의 대책을 도입한다 하더라도 시스템에 대한 완전한 안전을 보장하기는 어렵

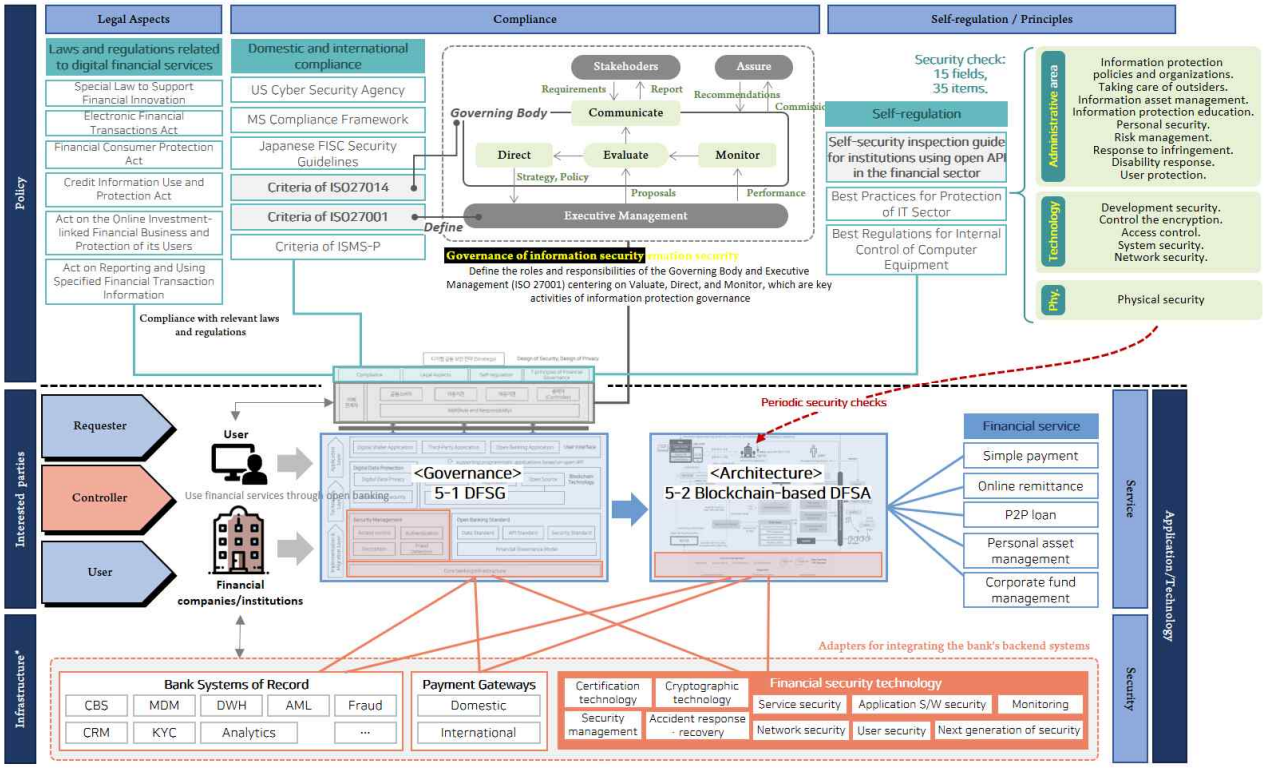

그림 4. 디지털 금융 보안 거버넌스와 아키텍처의 당위성
Fig. 4. Justification of DFSA and DFSG

고, 확실한 보안이더라도 효과가 가시적이지 않다. 이러한 제약사항에도 불구하고 지속적으로 발생하는 금융사고에 대해 정부에서는 다양한 법제 활동 및 개정을 촉구하고 있고, 금융 관련 기업에서는 다각적 측면에서 지원을 마련하고 있다. 본 연구 역시 대책수립의 일환으로 디지털 금융보안 거버넌스 체계를 제시하였으며 기술적 구현의 효과성을 보이기 위해 금융서비스 중 오픈뱅킹을 중점으로 한 블록체인 기반의 디지털 금융보안 아키텍처를 제시하였다.

본 장에서는 제시한 거버넌스와 아키텍처의 당위성을 설명한다. 거버넌스의 당위성을 설명하기 위해 국내 디지털 금융과 관련된 법률, 미국 사이버 보안청 및 일본 FISC 등 해외 금융보안 관련 가이드라인, 그리고 ISO 27014, ISO 27001과 같은 국제 보안 표준화 등을 참고하였다. 자율규제로써는 대표적으로 국내 금융권 Open API 이용기관 자체 보안점검 가이드를 기준으로 설명될 수 있다. 레퍼런스들을 토대로 해당 당위성의 설명은 그림 4와 같다.

디지털 금융서비스에서는 크게 요청자와 이용자로 구분하며, 이들은 이해관계자로써 금융소비자, 이용기관, 제공기관에 해당한다. 중재자(Controller)는 금융서비스에서 필요로 하는 제3의 신뢰자 및 신뢰기관에 해당하며 금융 인프라를 이루는 구성원이다. 요청자와 이용자가 이용할 수 있는 금융서비스는 기존 은행에서 제공해주는 기술 인프라를 통합하여 이미 안전성을 갖춘 금융보안기술을 적용한다. 그뿐만 아니라 오픈뱅킹 서비스를 위한 블록체인 기술을 적용하여 새로운 환경에서 보안을 강화할 수 있으며, 이에 대해서는 오픈 API 보안점검을 통해 주기적으로 안전성을 검토한다.

Ⅶ. 결 론

코로나19로 가속화된 디지털 전환 흐름은 금융권에도 영향을 미치고 있다. 그중에서 오픈뱅킹은 개방형 금융결제망으로 전세계 금융업계의 관심이 높아지면서 보안 문제에 대한 우려 역시 커지고 있다. 즉, 보안사고에 대한 철저한 대비가 갖춰지지 않는다면 오픈뱅킹 서비스를 사용하는 이용자 및 고객 입장에서 부정적 시각을 극복하기 어려울 것이고 이는 금융서비스 발전을 저해하는 요인이 될 것이다.

본 연구는 디지털 금융서비스를 제공하는 사이버 환경에서 연일 발생하는 위협의 선제적 대응을 하기 위한 오픈뱅킹 중심의 보안 거버넌스 체계를 제시하였다. 이를 기반으로 실제 엔지니어 입장에서 적용 가능한 블록체인 기반의 디지털 금융 보안 아키텍처를 제시하여 실 적용성을 제안하였다. 마지막으로 제안한 거버넌스와 아키텍처에 대한 상관관계 분석을 통해 유기적인 관계임을 보여줌으로써 타당성을 제시하고, 참고자료에 대한 설명을 뒷받침함으로써 당위성을 부여하였다.

본 논문은 디지털 금융 보안을 위해 블록체인 기술을 도입하

고자 하는 금융기관 및 핀테크 기업에서 참고할만한 자료로 활용할 수 있을 것이다.

References

[1] IBM, IBM Industry Insight: Finance [Internet]. Available: https://www.ibm.com/downloads/cas/MZAYZGPY.

[2] Samjong KPMG, The digital revolution in banks and the future of bank hegemony [Internet]. Available: https://assets.kpmg/content/dam/kpmg/kr/pdf/2021/kr-insight-digital-banking-20210105.pdf.

[3] The Banker, Is it the end of the bank or the extinction of the banking? [Internet]. Available: http://banker.kfb.or.kr/webzine/web/section.php?idx=76&PublishDate=201807&sub_idx=1512.

[4] Financial Security Institute, 2020 Prospects for digital finance issues [Internet]. Available: https://www.fsec.or.kr/common/proc/fsec/bbs/42/fileDownLoad/2248.do.

[5] Samjong KPMG, Open banking, the beginning of the landscape change in the financial industry [Internet]. Available: https://assets.kpmg/content/dam/kpmg/kr/pdf/2019/kr-issuemonitor-open-banking-20190524.pdf.

[6] Financial Security Institute, 2021 Prospects for digital finance issues [Internet]. Available: https://www.fsec.or.kr/common/proc/fsec/bbs/42/fileDownLoad/2755.do.

[7] Yonhapnews, Last year's non-face-to-face payment 17% ↑…It accounted for 4 out of 10 cases in the 4th quarter of last year. [Internet]. Available: https://www.yna.co.kr/view/AKR20210316076200002.

[8] K. S. Min, Y. J. KIm, J. S. Park, and H. N. Jang, Ransomware's latest trend analysis and implications [Internet]. Available: https://www.kisa.or.kr/public/library/insight_View.jsp?mode=view&p_No=291&b_No=291&d_No=4&cPage=&ST=TC&SV=.

[9] J. I. Choi, Current status and implications of open banking in the UK [Internet] Available: https://www.fss.or.kr/download.bbs?bbsid=1537404631244&fidx=1625105119416.

[10] J. K. Park, and I. J. Kim, "A study on the current status and policy direction of open banking," Journal of Service Research and Studies, Vol.10, No.1, pp.17-31, Mar. 2020.

[11] Open Banking Working Group, The Open Banking Standard [Internet]. Available: http://theodi.org/wp-content/uploads/2020/03/298569302-The-Open-Banking-Standard-1.pdf.

[12] Newsis, Open banking, used by 72% of the economically active population in Korea...'Expanding the financial sector' [Internet]. Available: https://newsis.com/view/?id=NISX20200706_0001084715&cid=10404.

[13] H. J. Kwon, Introduction of open banking and direction of development, Korea Institute of Finance, Financial Brief, Technical Report Vol.29, No.17, Sep. 2020.

[14] FINRA, Report on cybersecurity practices [Internet]. Available: https://www.finra.org/sites/default/files/2020-07/2015-report-on-cybersecurity-practices.pdf.

[15] H. K. Lee, "A study on regulations, current status and implications of electronic finance and financial security in the U.S.," Korean Journal of Banking and Financial Law, Vol.10, No.2, pp.141-184, Nov. 2017.

[16] D. H. Kim, "Design and implementation of enterprise information security portal system for financial companies," Journal of convergence security, Vol.21, No.1, pp.101-106, Mar. 2021.

[17] Financial Security Institute, Financial Security Governance Guide (2019) [Internet]. Available: https://www.fsec.or.kr/common/proc/fsec/bbs/147/fileDownLoad/2243.do

[18] M. S. Son, and H. Y. Kim, "A real estate lease transaction system using blockchain and open banking API," Journal of Korean Institute of Information Technology, Vol.18, No.5, May. 2020.

[19] Z. Xu, Q. Wang, Z. Wang, D. Liu, Y. Xiang, and S. Wen, "PPM: a provenance-provided data sharing model for open banking via blockchain," in Proceedings of the Australasian Computer Science Week Multiconference, Melbourne, pp.1-8, Feb. 2020.

[20] H. Wang, S. Ma, H. N. Dai, M. Imran, and T. Wang, "Blockchain-based data privacy management with Nudge theory in open banking," Future generations computer systems, Vol.110, pp.812-823, Sep. 2020.

[21] Financial Security Institute, Blockchain Trend Information for the second half of 2020 [Internet]. Available: https://www.fsec.or.kr/common/proc/fsec/bbs/42/fileDownLoad/2756.do.

[22] Korea Developement Institute, Current status of the introduction of blockchain technology in the financial industry and implications for post office finance [Internet]. Available: https://eiec.kdi.re.kr/policy/domesticView.do?ac=0000152992&issus=S&pp=20&datecount=&pg=.

[23] Security Operation Center, Security enhancement measures for data activation: privacy enhancement technologies (PETs) [Internet]. Available: http://www.igloosec.co.kr/BLOG_데이터%20활성화를%20위한%20보안%20강화방안%20:%20프라이버시%20보존기술(PETs,%20Privacy%20Enhancing%20Technologies)?searchItem=&searchWord=&bbsCateId=1&gotoPage=1.

[24] K. C. Bang, "A building method of designing national cyber xecurity governance model through diagnosis of operation

al experience," Jounal of Digital Convergence, Vol.16, No. 6, pp.205-212, Jun. 2018.
[25] M. T. Song, and W. B. Lee, "A Study on Influencing Factor s on Users' Intention to Accept Open Banking," Informatio n Systems Review, Vol.23, No.2, pp. 135-154, May. 2021.
[26] H. S. Lee, J. H. Lee, T. Lee, K. S. Jang, J. H. Lee, and C. J. Ryu, "An Mobile Application For Integrated Account Bala nce Notification Service Using Financial Technology API," in Proceedings of Korean Institute of Information Technolo gy Conference, Vol.18, No.5, pp.200-203, Aug. 2020.
[27] B. B. Pena, B. Kursar, R. E. Clarke, K. Alpin, M. Holkar, J. Vines, "'Pick Someone Who Can Kick Your Ass' - Money work in Financial Third Party Access," in Proceedings of th e ACM on Human-Computer Interaction, Vol. 4, pp.1–28, Dec. 2020.
[28] K. K. Kim, and B. Prabhakar, "Initial trust and the adoption of B2C e-commerce," ACM SIGMIS Database: the DATA BASE for Advances in Information Systems, Vol.35, No.2, pp.50-64, Jun. 2004.
[29] H. Y. Ha, and R. K. Akamavi, "Does Trust Really Matter in Electronic Shopping?," Seoul Journal of Business, Vol.15, No.1, pp.91-120, Jun. 2009.
[30] Y. J John, "A Determination of the Factors Contributing to Internet Banking," The Journal of Digital Policy & Manage ment, Vol.10, No.11, pp.137-144, Dec. 2012.
[31] D. H. Kim, "Changes in the environment of electronic finan ce and its challenges -Focusing on the prospects and implic ations of changes in electronic finance-," Journal of Digital Covergence, Vol.19, No.5, pp.229-239, May. 2021.
[32] J. Y. John, "Security and Trust on Non-Contact Financial T ransaction," Journal of Digital Covergence, Vol.19, No.7, p p.147-154, Jul. 2021
[33] H. S. Yoo, J. D. Kim, and S. J. Kim, "A Study on Improve ment for Analyzing the Security Check Items in Security R eview of Mobile Financial Services," Korean Journal of Ind ustrial Security, Vol.7, No.1, pp. 129-158, 2017.
[34] S. prakash, I. gunalan, "A new business model for digital g overnance of public records using blockchain," in Proceedi ng of the International Conference on Theory and Practice of Electronic Governance, Athens, 23-25 Sep. 2020.
[35] D. H. Choi, and I. S. Kim, "A Study on the Policy Proposal and Model B2B2C for Safe Open Banking," Journal of The Korea Institute of Information Security and Cryptology, Vo l. 29, No.6, pp.1271-1283, Dec. 2019.
[36] N. H. Kwon, and I. S. Kim, "Improvement of regulations to strengthen the safety and protect users of domestic Open B anking", Journal of convergence security, Vol.20, No.2, pp. 38-52, Jun. 2020.

김 경 진 (Kyoung-Jin Kim)
2007년 성신여자대학교 컴퓨터정보학부 졸업 (공학사)
2009년 성신여자대학교 대학원 전산학과 (이학석사)
2013년 성신여자대학교 대학원 컴퓨터학과 (이학박사)
2013년 3월 ~ 2015년 8월 성신여자대학교 컴퓨터학과 박사후연구원
2015년 9월 ~ 2017년 2월 서강대학교 스마트 핀테크 연구센터 박사후연구원
2017년 3월 ~ 현재 성신여자대학교 융합보안공학과 교수
※관심분야 : 블록체인, 접근제어, 프라이버시 보호 등

홍 승 필 (Seng-Phil Hong)
1993 BS. In Computer Science Indiana State University,USA
1994 M.S. in Computer Science Ball State University, USA.
1997 Ph.D. CS, Illinois Institute of Technology USA.
2003 Ph.D. in Computer Science KAIST, Korea.
1997 ~ 2005 LG-CNS, Inc Korea
2005 ~ 2019 Professor. Sungshin University, Korea
2019 ~ Present CEO / Senior Adviser of HANCOM WITH, Korea
※관심분야 Digital Finance, Blockchain, Security, Privacy Act