

Digital Finance & Cyber Security

# 2023 디지털금융 및 사이버보안 이슈 전망





Digital Finance & Cyber Security

# 2023 디지털금융 및 사이버보안 이슈 전망



01



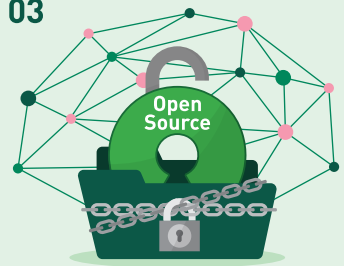
사이버 공격 경로로 악용될 수 있는  
엔데믹 취약점

02



랜섬웨어, 피싱 앱 등  
사이버 위협의 끝없는 진화

03



오픈소스 이용 활성화와  
강조되는 공급망 보안

2023

Digital Finance &  
Cyber Security

디지털금융 및 사이버보안 이슈 전망



금융보안원  
Korea Financial Security Institute

04



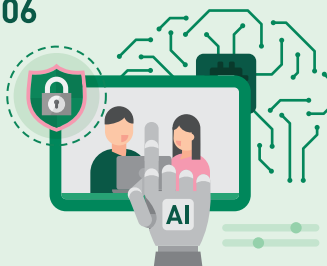
디지털자산의 당면과제,  
리스크 관리체계 마련

05



대세로 자리잡은 클라우드와  
보안 고려사항

06



인공지능 활용, 공정성·보안성  
확보를 통한 이용자 보호 필수

07



디지털 신원증명 활용에 따른  
기대와 우려

08



금융보안 규제 합리화,  
전제되는 자율 보안

09



마이크로플랫폼 시대,  
데이터 확보와 보호

10



금융권 채널 변화의 핵심  
디지털 연결



# Contents

01	사이버 공격 경로로 악용될 수 있는 엔데믹 취약점	01
02	랜섬웨어, 피싱 앱 등 사이버 위협의 끝없는 진화	03
03	오픈소스 이용 활성화와 강조되는 공급망 보안	05
04	디지털자산의 당면과제, 리스크 관리체계 마련	07
05	대세로 자리잡은 클라우드와 보안 고려사항	09
06	인공지능 활용, 공정성·보안성 확보를 통한 이용자 보호 필수	11
07	디지털 신원증명 활용에 따른 기대와 우려	13
08	금융보안 규제 합리화, 전제되는 자율 보안	15
09	마이플랫폼 시대, 데이터 확보와 보호	17
10	금융권 채널 변화의 핵심 디지털 연결	19

---

## 01

# 사이버 공격 경로로 악용될 수 있는 엔데믹 취약점

최근 제로데이 취약점이 사상 최대로 발견된 가운데 일부 취약점은 시스템에 잔존하며 계속 영향을 미치는 '엔데믹 취약점'으로 지목. 취약점 모니터링 및 최신 패치 적용에 유의하고 보다 효과적인 보안 취약점 관리를 위한 제도 수립도 고려해볼 필요

## 1 이슈 분석

### • 제로데이 등 고위험 보안 취약점을 이용한 사이버 공격 우려 심화

제로데이 취약점은 제조사·개발자가 인지하거나 공식적인 패치를 배포하기 전에 발견된 보안 취약점으로, 최근 이를 악용한 공격이 증가

\* 제로데이 취약점 익스플로잇 건수에 대해 구글은 '20년 25개 → '21년 58개로, 미국 보안 회사 맨디언트는 '20년 30개 → '21년 80개로 증가하였음을 각각 발표<sup>1)</sup>

특히 원격코드실행(Remote Code Execution), 권한 상승(Privilege Escalation) 등이 가능한 고위험 보안 취약점을 이용하는 사이버 공격에 대한 우려가 심화

### • 취약점을 선제적으로 식별·방어하기 위해 버그바운티를 적극 활용

구글, MS 등 글로벌 빅테크 기업은 자사 제품 및 서비스의 보안 취약점을 선제적으로 찾아내기 위해 버그바운티(Bug Bounty)<sup>2)</sup>를 활용하고 있으며, 보안기업 및 관련 연구기관에서도 취약점 연구에 적극 투자<sup>3)</sup>

이와 관련하여 국내 금융권도 모바일 애플리케이션, 보안 프로그램 등 사용중인 소프트웨어의 보안 취약점을 신고받는 버그바운티를 운영

\* 금융보안원 「금융권 버그바운티」, 우리은행 「모의해킹 경진대회(WooriCON)」, 토스 「버그바운티 챌린지」 등

#### 금융보안원 「2022년 금융권 버그바운티」



출처 : 금융보안원 보도자료('22.8.3.)

1) 2021년 한 해, 제로데이 취약점 통한 공격이 폭발적으로 증가했다.(보안뉴스, '22.4.22.)

2) 취약점 보상 프로그램(Vulnerability Reward Program)이라고도 하며 기업의 서비스, 소프트웨어 및 IT 인프라의 보안 취약점을 발견하여 신고한 자에게 포상금을 지급하는 제도(버그바운티클럽)

3) 제로데이 취약점, 지난해 사상 최고(데이터넷, '22.5.3.)



## 2 전망 및 대응 전략

### • 보안 취약점 모니터링 및 최신 패치의 신속한 적용 등이 중요

사용하는 소프트웨어와 관련하여 발표되는 보안 취약점 동향을 모니터링하고 최신 보안 업데이트 발표 시 이를 신속하게 패치할 필요

Log4j의 경우와 같이 취약점의 영향을 받는 시스템 수가 많고 광범위한 패치가 필요한 경우, 엔데믹 취약점(Endemic Vulnerability)으로 잔존하며 위협이 될 가능성이 있어 지속적인 주의와 관심 필요

\* 미국 사이버안전심의위원회는 Log4j의 취약한 인스턴스가 앞으로 10년 이상 시스템에 잔존할 것으로 평가하며 '엔데믹 취약점'이라 명명<sup>4)</sup>

### • 보다 효과적인 보안 취약점 관리를 위한 제도 수립도 고려해볼 필요

국내에서도 취약점 관리를 위해 버그바운티를 운영하고 있으나 수집된 취약점 조치 및 공개에 대한 체계화·정형화된 공식 절차는 미비

취약점 제보의 촉진, 공급업체의 취약점 완화 동기 부여 등 효과적인 취약점 관리를 위해 미국, EU 등에서 운영 중인 체계적 취약점 공개(Coordinated Vulnerability Disclosure, CVD<sup>5)</sup>) 제도의 수립도 고려해볼 필요

#### CVD와 버그바운티 비교

CVD	비교	버그바운티
취약점 해결 및 공개 판단이 중심	목적	취약점 제보 방법과 평가에 따른 보상 내용이 중심
취약점 접수, 평가, 처리, 공개(필요시 조정)하는 체계화·정형화된 공식 절차	절차	취약점 접수 후 평가
일반인뿐만 아닌 기업 내부자, 협력업체 직원, 공급업체 개발자 등 제한 없음	제보자	좌동(단, 내부직원 및 가족, 협력업체 직원 등 회사와 이해관계가 있는 경우 포상대상에서 제외)
법, 규정, 가이드에서 의무 또는 권고	의무화	취약점 제보 포상 근거는 있으나 버그바운티를 의무·권고하지 않음
제보자, 공급업체, 중개자 등 CVD 참여자별 역할과 책임을 절차에 명확히 기술	역할·책임	취약점 포상 제외 사항, 주의사항 등 제보자에게 금지된 행위만을 기술
금전적 포상에 국한되지 않음	보상	금전적 포상

출처 : 금융보안원

4) Cyber Safety Review Board, 「Review of the December 2021 Log4j Event」(‘22.7월)

5) 취약점의 접수부터 공개까지 일련의 절차를 제도화한 것으로, 중개자의 개입을 통해 취약점 공개에 대한 의견 조정 등을 수행하고 취약점 발견자와 공급업체에 적절한 권리와 의무를 부여함으로써 취약점 공개제도 참여를 유도

# 02

## 랜섬웨어, 피싱 앱 등 사이버 위협의 끝없는 진화

디지털 환경 또는 기술을 악용하거나 탐지 및 대응을 지연시키기 위한 기법을 적용하는 등 사이버 위협이 고도화, 진화하는 사이버 위협에 대응하기 위해 침해사고 대응훈련 및 정보공유 체계에 대한 적극적인 참여와 함께 제로 트러스트 전략을 검토할 필요

### 1 이슈 분석

#### ● 최근 랜섬웨어 공격이 활발, 한국형 랜섬웨어도 지속 탐지

‘22년 상반기 중 가장 활발했던 사이버 위협은 랜섬웨어<sup>6)</sup>로, 최근 다중 갈취(Multi extortion)<sup>7)</sup>로 수법이 진화  
랜섬웨어 공격 증가는 서비스형 랜섬웨어(RaaS)<sup>8)</sup>의 보편화, 국가 배후 공격 그룹의 활동 증가 등에  
기인하는 것으로 보이며, 귀신(Gwisin) 랜섬웨어 등 국내 기업만을 노리는 랜섬웨어도 지속적으로 유포<sup>9)</sup>

#### ● 전화 수신 위장 등으로 기능을 강화한 보이스피싱 악성 앱

보이스피싱에 사용되는 악성 앱의 경우, 전화 발신 가로채기 외에도 전화 수신 위장 등으로 기능을 강화

#### 보이스피싱 악성 앱의 기능적 진화

2018년 하반기(Shadowvoice)		2021년		
기능	전화번호 가로채기	기능	전화번호 가로채기	전화 수신 위장
	문자메시지 탈취		문자메시지 탈취	라이브스트리밍
	전화번호부 탈취		전화번호부 탈취	명령어 실행
	스크린샷 탈취		정보수집(통화정보, 설치된 앱, 기기정보, 위치정보, 음성녹음, 사진, 동영상 탈취 등)	
	기기정보 탈취			
사칭대상	금융사(증권, 은행, 카드 등), 피싱가드	사칭대상	금융사(증권, 은행, 카드 등), 피싱가드, 백신, 공공기관, OTT앱, 메신저, 동영상 플레이어	

출처 : 금융보안원, 「보이스피싱 악성 앱 유포조직 프로파일링」, ('22.1월)

분석을 방해하기 위한 목적으로 파일 포맷의 일부를 의도적으로 정교하게 변조하는 기법을 적용한 경우도 존재<sup>10)</sup>

6) SK윌더스 EQST, 「2022 상반기 보안 트렌드」('22.6월), 트렌드마이크로, 「2022년 상반기 보안 위협 보고서」('22.9월)

7) 파일 암호화 외 데이터 유출, DDoS, 유출 데이터의 소유자와 직접 소통을 통한 불법적인 협상시도 등 다양한 방식으로 금전적 이익을 극대화(이글루코퍼레이션, 「권한상승을 이용한 랜섬웨어 공격 방식」('22.8월))

8) Ransomware as a Service : 해커가 제작해 판매하는 랜섬웨어로 기술 전문성 없이도 랜섬웨어를 배포하거나 사이버 공격에 접근이 가능하도록 함(랜섬웨어 기술 판매 시장 확 커졌다... 갈수록 산업화(디지털투데이, '22.8.25.))

9) 韓 맞춤형 랜섬웨어 '귀신' 5곳 털었다... 과감한 지능범 '경고'(inews24, '22.9.1.)

10) 금융보안원, 「분석 방해를 위해 ZIP 파일 포맷을 변조한 악성 APK 연구」('22.10월)

## 2 전망 및 대응 전략

### ● 디지털 금융의 발전 이면에 사이버 보안 위협도 진화 중

사이버 위협은 오픈뱅킹·간편송금 등 디지털 금융 서비스<sup>11)</sup>, 개방과 연결을 특성으로 하는 디지털 금융 환경<sup>12)</sup>, 디지털 기술<sup>13)</sup> 등을 역이용하며 진화해 나갈 것으로 전망

코드 난독화, 지능화된 우회 기법 적용, 내부 이동(Lateral Movement)<sup>14)</sup> 및 잠복 등 탐지를 무력화하고 대응을 지연시키기 위한 방식도 계속해서 개발

이에 대응하기 위해서는 최신 사이버 위협 트렌드를 반영한 침해사고 대응훈련 실시, 정보공유 체계<sup>15)</sup>에 적극 참여, 관련 시스템 고도화 등 노력 필요

### ● 제로 트러스트로 보안 패러다임 전환 필요

재택·원격근무, 클라우드 도입 등으로 변화하는 업무 환경, 진화하는 사이버 위협 등에 대응하기 위해 최소 권한 접근, 보안 가시성 확보 등에 기반한 제로 트러스트(Zero Trust)<sup>16)</sup>로 보안 패러다임 전환 필요

#### 제로 트러스트 원칙



- 1 모든 데이터 소스와 컴퓨팅 서비스는 리소스로 간주
- 2 네트워크 위치와 관계없이 모든 통신을 안전하게 함
- 3 기업 리소스에 대한 접근은 각 세션에 기반하여 승인됨
- 4 리소스에 대한 접근은 ID, 애플리케이션, 서비스, 자산의 상태 등 동적 정책에 의해 결정
- 5 기업은 소유한 모든 관련 자산의 무결성과 보안 상태를 모니터링하고 측정
- 6 리소스에 대한 모든 인증 및 승인은 동적으로 수행되며 접근을 허용하기 전 엄격히 적용
- 7 기업은 자산, 네트워크, 인프라 통신 상태 정보를 수집하고, 이를 통해 보안을 개선

출처 : 미국 NIST, 「Zero Trust Architecture」('20.8월)

11) 편리할수록 보안에 취약... 보이스피싱에 뺨 맞은 오픈뱅킹(이데일리, '22.5.29.), 간편송금 사기 느는데... 익명에 계좌 요구도 않는 '오픈채팅 송금' (서울경제, '22.8.21.)

12) 서비스 연결, 데이터 전송에 사용되는 API를 타깃으로 하는 사이버 위협이 향후 증가할 전망(API 보안 사고, 2024년까지 2배로 증가 전망... 중간자 공격 등 보안 위협 급증(보안뉴스, '22.6.23.))

13) 마이크로소프트의 에릭 호로위츠는 공격적 AI(Offensive AI)를 통해 사이버 공격이 고조될 수 있다고 밝힘(AI를 활용한 사이버 공격, 증가 불가피해 대책 필요(AI타임즈, '22.5.17.))

14) 지능형 위협(Advanced Persistent Threat) 공격 과정 중 공격자가 조직 내 최초 시스템 해킹에 성공 후 내부망에서 사용되는 계정 정보를 획득하여 내부망의 시스템으로 이동하는 방식(Ahnlab, 「레터럴 무브먼트, 정상과 악성의 경계를 넘어 대응하라」('18.11월))

15) 금융보안원의 '이상금융거래정보 공유시스템' 및 '범금융권 보이스피싱사기정보 공유시스템' 등

16) 정적(Static) 네트워크 기반의 경계선 방어로부터 사용자·자산·자원에 초점을 맞추어 방어를 이행하고 진화하는 사이버 보안 패러다임 (미국 NIST, 「Zero Trust Architecture」('20.8월))

## 03

오픈소스 이용 활성화와  
강조되는 공급망 보안

디지털 전환 가속화로 소프트웨어 사용이 증가함에 따라 소프트웨어 공급망을 대상으로 한 사이버 공격 우려가 심화. 이용 중인 소프트웨어의 구성 요소를 빠짐없이 식별하고 이를 기반으로 체계적인 리스크 관리를 추진할 필요

## 1 이슈 분석

## ● 디지털 전환의 필수 재료인 오픈소스를 노리는 사이버 위협이 우려

오픈소스는 소프트웨어 개발기간 및 비용 단축 등의 이점을 제공함에 따라 디지털 전환의 필수 재료로 주목받고 있으며 애플리케이션에 광범위하게 활용<sup>17)</sup>

오픈소스는 누구나 접근 가능할 뿐 아니라 검증 없이 재사용되는 경우가 많기 때문에, 이를 노린 악성코드 삽입, 정상 패키지와 유사한 이름의 악성 패키지를 등록하는 타이포스쿼팅(Typosquatting) 등 공격이 가능

## 오픈소스 공격 유형 및 사례

유형	사례
악성코드 삽입	유명 오픈소스 라이브러리인 colors.js, faker.js 관리자가 해당 라이브러리에 악성코드를 삽입하여 NPM <sup>18)</sup> 을 통해 배포('22.1월)
	UA-Parser-JS 관리자의 NPM 계정이 탈취되어 해당 라이브러리에 악성코드를 삽입한 오픈소스 배포('21.11월)
타이포스쿼팅	RubyGems 리포지토리에 비트코인을 훔치기 위해 제작된 700여 개의 악성 패키지가 업로드('20.2월)

출처 : 유럽네트워크정보보호원(ENISA), 「Threat Landscape for Supply Chain Attack」('21.7월) 등

## ● 소프트웨어 공급망 공격이 중요 사이버 이슈로 부상

소프트웨어의 개발, 배포, 설치, 유지보수 과정에 개입하여 변조된 소프트웨어가 사용자의 시스템에 전달되도록 하는 소프트웨어 공급망 공격이 디지털 시대를 맞아 중요 사이버 이슈로 부상<sup>19)</sup>

특히 업데이트 서버를 공격해 파일을 내려받는 시스템을 감염시키는 등 신뢰관계를 악용하는 방식이 주로 사용<sup>20)</sup>되는데 한 번의 공격으로 대규모 사용자를 감염시킬 수 있어 공격자 입장에서는 매우 효율적

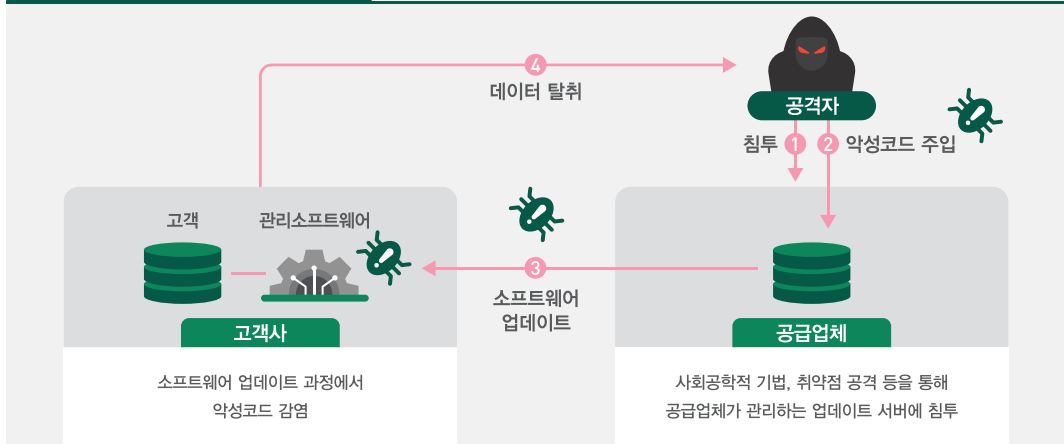
17) 디지털 전환 성공의 키, 오픈소스... 거버넌스 및 커뮤니티 활용 방안은(디지털데일리, '22.9.18.)

18) Node Package Management : 자바스크립트 프로그래밍 언어를 위한 패키지 관리자(CCTV 뉴스)

19) '19년 이후 소프트웨어 공급망 공격이 연평균 742% 증가(Sonatype, 「State of the Software Supply Chain」('22.10월))

20) 대규모 피해 양산하는 공급망 공격(데이터넷, '21.11.1.)

## 신뢰관계를 악용한 공격 흐름도



출처 : 유럽네트워크정보보호원(ENISA), 「Threat Landscape for Supply chain Attack」('21.7.) 참고 및 재구성

## 2 전망 및 대응 전략

## • 복잡해지는 소프트웨어 공급망, 체계적인 보안 관리 필요

디지털 전환이 가속화됨에 따라, 복잡한 소프트웨어 공급망 구조상 약한 고리를 노리는 사이버 위협 또한 심화될 것으로 전망<sup>21)</sup>

소프트웨어 자재명세서(SBOM)<sup>22)</sup> 등을 통해 소프트웨어 구성 요소를 빠짐없이 식별하고 이와 관련된 보안 취약점, 출처 및 이력, 라이선스 의무 등을 체계적으로 관리할 필요

## 소프트웨어 공급망 관리 방안(예시)

구분	관리 방안(예시)
내부 정책 마련	美 NIST 「사이버 공급망 위험관리 지침(C-SCRM)」 <sup>23)</sup> 을 활용하여 내부 위험관리 지침 마련
구성 요소 식별·관리	SBOM 등을 활용하여 소프트웨어 구성 요소를 식별하고 목록화·관리
소프트웨어 종속성·취약점 관리	사용하는 오픈소스 패키지의 종속성 및 취약점을 주기적으로 식별·검증 필요
정보 공유	공급망 구성원 간 보안 취약점 등 위협 정보, 안전한 오픈소스 정보 등 공유
라이선스 관리	오픈소스 라이선스 준수 의무 위반이 발생하지 않도록 관리

출처 : 정보통신기획평가원, 「소프트웨어 기반의 공급망 공격 동향 및 대응방안」('22.6월) 등

21) '25년까지 전 세계 조직의 45%가 소프트웨어 공급망 공격 동향을 경험할 것이라고 전망(가트너, 「2022년 주요 보안 및 리스크 관리 트렌드」('22.3월))

22) Software Bill of Materials : 소프트웨어 구축시 사용되는 다양한 구성요소의 세부 정보와 공급망 관계를 기술하는 공식 기록(NIST)

23) NIST, 「Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations」('22.5월)

## 04

디지털자산의 당면과제,  
리스크 관리체계 마련

디지털자산을 향한 보안 위협이 급증하고 있으며, 국내외 규제당국을 중심으로 디지털자산에 대한 규제 논의가 활성화되는 등 관련 규제 이니셔티브 확보를 위한 경쟁이 활발. 디지털자산에 대한 사이버 위협 관리 방안 수립 및 글로벌 정합성을 고려한 규제 마련 필요

## 1 이슈 분석

## ● 디지털자산의 가치 상승 및 이용 활성화에 따라 사이버 공격이 급증

디지털자산은 랜섬웨어 및 DDoS 공격 중단 대가로 요구될 뿐만 아니라 최근에는 디지털자산을 직접 탈취 대상으로 한 공격 등 산업 전반에 대한 보안 위협도 크게 증가<sup>24)</sup>

디지털자산 관련 보안 위협과 사례

대상	보안 위협	사례
거래소	데이터 유출	거래소 해킹으로 고객 정보 유출 및 삭제('21.4월)
	전자지갑 탈취	거래소 내 전자지갑의 개인키 해킹으로 \$2억 상당 디지털자산 탈취('21.12월)
전자지갑	가짜 하드웨어	하드웨어 전자지갑에 스파이 칩을 부착하여 디지털자산 탈취('21.6월)
	타인 명의도용	전자지갑 개설 시 타인 명의로 신원증명을 수행한 후 지원금 편취('21.10월)
디파이	디지털자산 무단발행	스마트 계약 코드의 보안 취약점을 악용하여 트랜잭션 위조를 통한 디지털자산 무단 발행('22.2월)
	외부 네트워크 공격	BGP 하이재킹으로 정상적인 요청을 공격자가 가로채 악성코드 유포 후 디지털자산 탈취('22.2월)





출처 : 금융보안원, 「디지털자산 보안 위협 및 대응」('22.2월)

## ● 국내외 규제당국을 중심으로 디지털자산에 대한 규제 논의 활성화

정부는 투자자 보호·신사업 지원·산업진흥을 위한 디지털자산 인프라 및 규율체계 구축을 국정과제 중 하나로 선정하였고, 금융위원회 주관의 민·관합동 TF가 출범하여 디지털자산기본법 제정 논의에 착수<sup>25)</sup>

EU·미국 등 국외 주요국에서도 최근 디지털자산의 법적 성격 명확화, 투자자 보호 방안, 사이버 리스크 관리 등 관련 규제 마련을 논의 중이며, 디지털자산 관련 규제 이니셔티브 확보를 위한 경쟁이 활발

디지털자산 관련 국외 규제 논의 동향

국가	내용
 EU	디지털자산의 법적 규제 명확화 및 투자자 보호를 위한 법안(MiCA) 발표('20.9월)
 미국	FBI와 CISA에서 디지털자산에 관한 보안 방침 권고안 발표('22.4월)
 미국	백악관에서 디지털자산의 포괄적 규제 프레임워크 발표('22.9월)
 일본	스테이블 코인의 투자자 보호 및 자금세탁 대응을 위한 자금결제법 개정('22.6월)

출처 : 관련 언론보도

## 2 전망 및 대응 전략

### • MiCA 등 해외 규제와의 정합성을 고려한 디지털자산 관련 규제 마련 추진

국내 디지털자산 관련 규제에는 글로벌 규제 정합성<sup>26)</sup>을 고려하여 시장 안정, 이용자 보호 및 규제 차익 방지<sup>27)</sup> 등이 중점적으로 포함될 전망

또한 디지털자산의 발행·유통 전 과정에서 발생할 수 있는 사이버 리스크 관리 및 내부통제 등 안전성 확보를 포함한 디지털자산 시장 규율체계 마련 방안이 논의될 것으로 예상<sup>28)</sup>

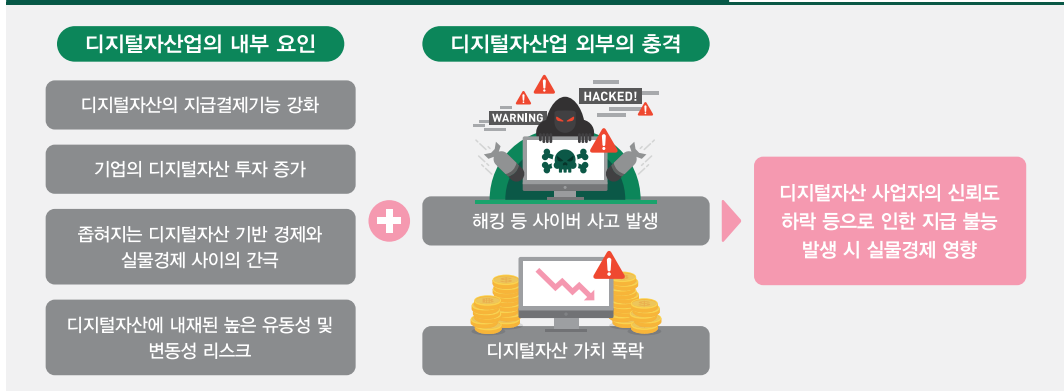
이에, 디지털자산 관련 글로벌 입법 동향을 지속 모니터링하고 새롭게 마련되는 법적 요구 사항에 즉각 대응할 수 있도록 대비할 필요

### • 디지털자산 관련 사업자의 사이버 리스크 관리 필요

FSB 등 국제기구<sup>29)</sup>는 디지털자산의 취약성이 금융안정, 통화정책을 저해하고 전통 금융산업에 시스템릭 리스크<sup>30)</sup>를 유발할 수 있음을 경고

높은 유동성 리스크 및 지급결제기능 강화 등 디지털자산업의 내부적 특성과 해킹과 같은 외부적 충격이 결합될 시 디지털자산 사업자의 신뢰도 하락으로 인한 시스템릭 리스크 발생 가능

#### 디지털자산업이 금융산업에 시스템릭 리스크를 야기할 수 있는 시나리오



출처 : 보험연구원, 「CEO Brief 가상자산 시장의 성장과 향후 주요이슈」(‘22.4월) 및  
국회미래연구원, 「가상화폐의 파급효과와 정책 대안 연구」(‘20.12월) 내용 요약 및 재구성

디지털자산 관련 사업자는 위험평가, 비즈니스 연속성 계획 수립 등을 통해 리스크를 적극적으로 관리할 필요

24) 디지털자산 해킹으로 인해 '22년 상반기 중에만 약 20억 달러 피해가 발생하였으며 이러한 추세가 계속될 경우 지난해 전체 피해금액인 32억 달러를 능가할 것으로 예상(디지털금융의 이면..., 디지털자산 해킹 주의보(아이뉴스, '22.8.20.))

25) 범정부 차원 디지털자산기본법 제정 '속도'(연합뉴스, '22.8.17.)

26) 금융감독원은 향후 디지털자산에 대한 글로벌 공통 기준 마련에 적극 동참할 예정임을 발표(금감원장, 바젤은행감독위 참석... 디지털자산 규제 논의(뉴시스, '22.9.13.))

27) 금융위 "국제 정합성 성립 전 가상자산 국내 단일 규제 어려워"(디지털투데이, '22.9.19.)

28) 「디지털자산 민·관합동 TF」 출범 및 1차 회의 개최(금융위원회, '22.8.17.)

29) 국제결제은행(BIS), 「Investigating the impact of global stablecoins」(‘19.10월), 금융안정위원회(FSB), 「Assessment of risks to financial stability from crypto-assets」(‘22.2월)

30) Systemic Risk : 금융 시스템의 중요 부분에 대한 손상으로 실물 경제에 중대한 부정적 영향을 초래할 수 있는 위험(한국은행, 「금융안정보고서 제15호」 '10.4월))

## 05

대세로 자리잡은 클라우드와  
보안 고려사항

클라우드는 금융권 디지털 전환을 뒷받침하는 핵심 인프라로써 거스를 수 없는 대세로 자리매김 중. 금융권 클라우드 도입 확산과 관련하여 보안 사고, 집중·종속 리스크 확대 등이 우려되므로 철저한 보안 관리 및 중요 업무의 클라우드 의존도 관리 강화 필요

## 1 이슈 분석

## ● 디지털 신기술 활용 증가 등에 따라 클라우드에 대한 관심 고조

금융권은 디지털 전환을 위해 애플리케이션 운영, 자동화, 빅데이터 분석 등 다양한 기술을 활용함에 따라 보다 유연한 인프라 운용이 가능한 클라우드 이용을 적극 검토<sup>31)</sup>

내부 직원 간 협업 강화 및 업무 생산성 증대를 위한 클라우드 기반의 서비스형 소프트웨어(SaaS)<sup>32)</sup> 이용 수요도 증가

## ● 관리 미흡 등으로 인한 클라우드 보안 사고가 지속 발생

클라우드 이용과 관련하여 계정 도난, 설정 오류, 운영 실수 등에 따른 서비스 중단, 데이터 유출 등이 지속 발생하고 있으며 클라우드 보안 사고 대부분이 기술적인 문제보다는 관리 미흡에서 비롯<sup>33)</sup>

최근 클라우드 보안 사고 동향

구분	사고원인 및 피해내역	발생연월
계정 도난	온라인 예약 소프트웨어 제공업자의 클라우드 접근 계정 도난으로 37만 명의 이름, 이메일 주소, 전화번호 등 개인정보 유출	'21.12월
설정 오류	비인가자가 클라우드 데이터에 접근 가능하도록 서버가 설정되어 있어 저장된 백업 파일 및 4만 7천 명의 데이터 등 유출	'21.4월
	비인가자가 클라우드 내 데이터에 접근 가능토록 설정, 클라우드 접속키, 데이터, 결제 내역 등 A사의 내부 문서 및 데이터가 온라인 상에 노출	'21.10월
CSP 운영 실수	가상서버의 인터넷 연결 문제로 서울지역 데이터센터 장애 발생 및 해당 클라우드 서비스 사용자의 접속이 20여 분 마비	'22.2월
	유지보수 작업 중 고객 사이트 삭제로 400여 개의 고객 서비스 중지	'22.4월

출처 : 관련 언론보도

31) 컴퓨터월드에서 '22.2월 실시한 설문조사 결과, 전체 응답자의 62%가 IT시스템 운영 측면에서 가장 고민하고 있는 부분에 대해 클라우드 환경 구축이라고 응답(삼성SDS, 「디지털 전환의 시작, 클라우드 마이그레이션」('22.4월))

32) Software as a Service : 클라우드 기반의 소프트웨어 제공 모델로, 클라우드 제공업체가 클라우드 애플리케이션 소프트웨어를 개발 및 유지 관리하고, 인터넷을 통해 고객에게 소프트웨어를 제공(Oracle)

33) 불충분한 ID, 자격증명, 액세스 및 키 관리, 잘못된 구성 설정과 변경 제어, 안전하지 않은 소프트웨어 개발 등 사용자의 통제 영역과 관련된 보안 위협이 상위 항목을 차지(Cloud Security Alliance, 「Top Threats to Cloud Computing」('22.6월))



## 2 전망 및 대응 전략

### ● 금융권 핵심 인프라로 자리잡는 클라우드

최근 추진 중인 금융권 차세대 시스템 프로젝트 대부분 클라우드 전환을 목표<sup>34)</sup>로 하고 있으며, 또한 관련 규제 개선, 재해복구 전략 강화 필요성 증가 등에 따라 클라우드 이용 수요가 더욱 증가할 것으로 전망<sup>35)</sup> 36)

특히 기업의 비즈니스 니즈 및 가치 우선순위에 따라 최적화된 방식으로 클라우드 마이그레이션 전략을 수립하는 것이 디지털 혁신 추진에 있어 더욱 중요하게 부각될 것으로 예상

### ● 클라우드 보안 및 리스크 관리의 중요성이 더욱 강조될 전망

클라우드 도입이 확대됨과 관련하여 클라우드 보안 역량 확보 또한 중요하게 강조될 것으로 예상되며, 특히 클라우드 관리를 목적으로 MSP<sup>37)</sup>를 이용하는 경우에도 보안 관리의 사각지대가 발생하지 않도록 유의할 필요

클라우드 자원, 애플리케이션, 데이터를 안전하게 관리할 수 있도록 CSPM(Cloud Security Posture Management)<sup>38)</sup> 등 통합 모니터링 및 관리 기능을 적극 사용할 필요

클라우드 이용 수요가 극소수의 서비스 제공자에 집중됨에 따라 집중 리스크, 종속 리스크가 우려<sup>39)</sup> 되는 만큼 멀티 클라우드 이용 등 출구 전략을 마련하고 중요 업무의 클라우드 의존도를 관리할 필요

#### 클라우드 이용에 따라 발생할 수 있는 리스크

구분	설명
집중 리스크	외부 위탁한 서비스 또는 제품이 제한된 수의 서비스 업체에 의해 제공됨에 따라 한 서비스에서 장애 발생시 이용하는 여러 고객이 피해를 입을 수 있는 리스크
종속 리스크	제3자에 의존하는 경우, 제3자의 신뢰성·투명성 등 리스크가 위탁자에게 전이되거나 새로운 정책 수립·전환에 과도한 비용이 들게 되는 리스크

출처 : 금융보안원, 「2022년 디지털금융 및 사이버보안 이슈 전망 보고서」(‘21.11월)



34) 금융권 차세대, 클라우드가 중심(ITdaily, '22.8.18.)

35) 금융위원회가 '22.4월에 발표한 「금융분야 클라우드 및 망분리 규제 개선방안」으로 연구·개발 목적의 망분리 정책이 완화됨에 따라 향후 클라우드 환경을 이용한 연구·개발 시스템 구축이 증가할 것으로 예상

36) '22.10월 국내 데이터센터 화재로 발생한 서비스 장애와 관련하여 향후 클라우드 기반의 서비스형 재해복구(Disaster Recovery as a Service, DRaaS)에 대한 수요 증가 가능성(카카오 먹통에 'IDC·클라우드' 재조명... 조용히 웃는 통신사들(연합인포맥스, '22.10.20.))

37) Managed Service Provider : 클라우드 도입 컨설팅부터 이전, 운영·관리, 보안 등의 서비스를 지원하는 사업자

38) 보안 및 위험 평가, 지속적인 모니터링 및 알림, 자격증명 및 접근관리, DevSecOps 통합, AI/ML 기반 보안 기능 등 제공

39) 영란은행(Bank of England), 「Critical third parties to the finance sector : policy statement」('22.6월), 유럽 증권시장감독청(European Securities and Markets Authority), 「Financial stability risks from cloud outsourcing」('22.5월)

## 06

# 인공지능 활용, 공정성·보안성 확보를 통한 이용자 보호 필수

금융산업 전반의 디지털 혁신을 주도하는 기술로 인공지능에 대한 관심이 고조, 향후 안전한 인공지능 활용을 위한 기반이 마련될 것으로 예상되며, 공정성, 신뢰성 및 보안성 확보를 통한 이용자 보호 노력에 더욱 집중할 필요

## 1 이슈 분석

### ● 금융산업 전반의 디지털 혁신을 주도하는 인공지능(AI) 시대

빅데이터에 기반한 금융시장 분석 및 전망, 금융상품 추천, 담보물 가격 결정, 리스크 측정·관리, 투자전략 수립, 고객 응대 등 금융권 내 다양한 분야에서 AI가 활용

금융보안관제, 금융사기 범죄 탐지 및 예방 등 사이버 보안 및 이상금융거래 탐지에도 AI를 적용하여 고도화

#### 금융분야 AI 활용 사례

구분	사례
업무 자동화	보험금 지급 여부를 AI가 실시간으로 심사하는 AI 자동심사 시스템 도입(한화생명)
고객 응대	AI 상담원이 선결제와 한도 조정, 비밀번호 등록·변경 등을 상담하는 인공지능 자동응답시스템을 고객센터에 도입(현대카드)
신용 평가	담보대출 인공지능 자동화 시스템 도입(하나은행)
투자 및 상담	금융 자연어 처리 인공지능 알고리즘을 기반으로 매일 뉴스를 분석하고, 투자 가치가 있는 정보를 선별하여 전달하는 AI 뉴스 서비스(SK증권)
사이버 보안	AI 기반 방어체계를 지향하는 보안 위협 대응 자동화 시스템 및 프로세스 구축(KB국민은행)

출처 : 한국금융연구원, 「금융업의 인공지능 활용과 정책과제」(‘22.2월) 및 관련 언론보도

### ● 금융위원회, 금융분야 AI 활용 활성화 및 신뢰확보 방안 발표

금융위원회는 유관기관 및 전문가 의견 수렴 등을 토대로 금융권의 AI 활용을 활성화하고 AI에 대한 사회적 신뢰도를 제고하기 위한 방안을 마련<sup>40)</sup>

빅데이터 확보를 위해 금융회사 AI 데이터 라이브러리 구축 등을 수행하는 한편, AI 활용에 따른 다양한 보안 위험 요소를 제거하기 위해 금융분야 AI 보안성 검증체계를 구축·운영할 예정

\* '23년부터 금융분야 챗봇서비스에 적용된 AI 알고리즘에 대한 검증을 실시하고 향후 단계적으로 확대 예정

40) 금융위원회, 「금융권 인공지능 활용 활성화 및 신뢰확보 방안」(‘22.8월)

## 금융권 인공지능 활성화 방안 주요 내용



출처 : 금융위원회, 「금융권 인공지능 활용 활성화 및 신뢰확보 방안」(‘22.8월)

## 2 전망 및 대응 전략

## • 금융권 내 안전한 AI 활용 확대·정착을 위한 기반이 마련될 것으로 전망

데이터 결합 후 재사용 허용, 공동 AI 데이터셋 구축 및 합성 데이터 기술 사용 등에 따라, 그간 AI 활용 활성화의 가장 큰 걸림돌로 지목되어 온 학습 데이터 부족이 다소 해소될 것으로 기대

또한 XAI의 정의, 요건 및 구현 사례 등을 포함한 안내서가 마련될 경우, 현재 전 세계적으로 활발하게 논의되고 있는 AI 의사결정 과정에 대한 신뢰성 확보에 기여할 것으로 예상

## XAI와 합성 데이터

구분	설명가능한 AI(XAI)	합성 데이터(Synthetic data)
정의	AI의 판단 결과에 대한 이유를 인간이 이해할 수 있도록 제공하는 기술	실제 데이터와 통계적 특성이 유사하여 실제 데이터를 분석한 결과와 유사한 결과를 얻을 수 있도록 인공적으로 재현하여 생성한 가상 데이터

출처 : 한국정보통신기술협회

## • 공정성, 신뢰성 및 보안성 확보를 통한 이용자 보호 필요

AI 기술 활용으로 예상되는 개인정보 유출, 학습 데이터 조작 등과 같은 위험을 예방하기 위해 데이터 획득 시점부터 가공되는 모든 단계에 대한 AI 보안성 검증을 통해 신뢰성 및 보안성 확보 필요

또한, 방대한 데이터를 학습·처리하는 과정에서 잘못된 데이터를 학습하여 AI 알고리즘이 편향된 결과를 도출할 우려가 있으므로, AI 알고리즘의 공정성 확보를 통한 이용자 보호 필요<sup>41)</sup>

41) 국외에서는 AI 기술 개발시 또는 이용 주체가 소비자 권리를 침해하거나 AI 기술로 인한 차별이 발생하는 것을 방지하는 내용을 담은 규제를 마련(유럽진행위원회, 「The purpose of the AI Liability Directive」(‘22.9월 발표), 美 백악관 과학기술정책실, 「Blueprint for AI Bill of Rights」(‘22.10월 발표))

## 07

디지털 신원증명 활용에 따른  
기대와 우려

디지털 전환, 코로나 등으로 다양한 비대면 신원증명 방식의 이용이 증가. 최근 금융권 내 디지털 신분증 활용이 허용되었으며 향후 이를 활용한 비대면 서비스가 확대될 전망. 관련 보안 위협에 선제적으로 대응하고 디지털 격차 해소에도 노력할 필요

## 1 이슈 분석

## ● 기존 비대면 신원증명 방식에 안전성·편의성을 더한 새로운 디지털 인증방식 필요성 증대

코로나19 이후 인터넷뱅킹 등 비대면 금융거래 이용이 크게 증가<sup>42)</sup>함에 따라 다양한 비대면 신원증명 방식이 활용

다만, 실명확인증표 사본 제출, 바이오인증, 생체인식 등 기존의 비대면 신원증명 방식에는 개인정보 유출, 해킹, 신원 도용의 위험이 존재<sup>43)</sup>

특히 실명확인증표는 이용자가 신원정보 노출범위를 통제할 수 없으며, 훼손이나 도난 혹은 위·변조를 통해 범죄에 악용될 우려

## 비대면 인증기술 관련 취약점 시나리오

분류	취약점	예시
실명확인증표 사본 제출	주민등록번호 메모리 정보 노출	메모리에 주민등록번호 노출
	네트워크 평문 전송	실명증표 및 관련정보 전송 시 평문 전송
타기관 확인 결과 활용	인증단계 우회	스크립트 및 동적 디버깅 툴을 이용한 인증 단계 우회
	식별정보 재사용	식별정보 및 패킷을 재사용하여 인증 가능
바이오인증	바이오정보의 복제	지문, 홍채 등의 정보를 복제하여 도용
	암호화 미저장	바이오정보의 암호화 저장 미실시

출처 : 금융보안원, 「금융회사의 안전한 비대면 인증을 위한 연구」('16.4월)

● DID<sup>44)</sup> 기반 모바일 운전면허증을 통한 새로운 신원증명 체계 도입

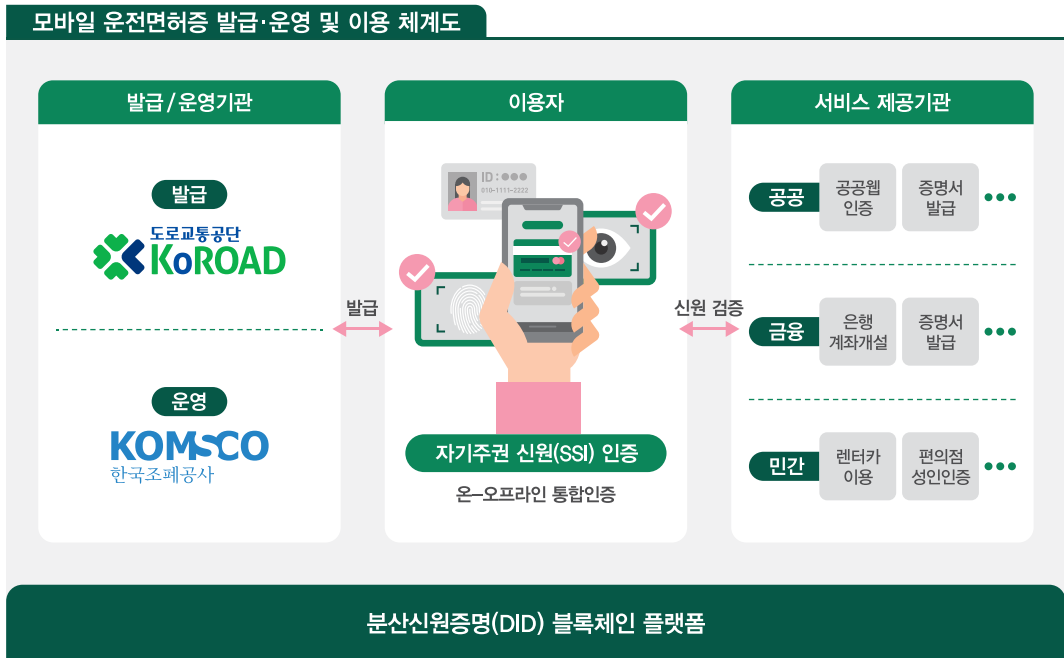
기존 실명확인증표가 가진 개인정보 유출, 신원 도용, 위·변조 및 분실·도난의 위험으로부터 비교적 자유로운 DID 기반 모바일 신분증이 등장

42) '21년 모바일뱅킹 이용 건수가 1436만 건으로 전년 대비 23% 증가(한국은행, 「2021년 국내은행 인터넷뱅킹 서비스 이용현황」('22.3월))

43) 기존의 인증 서비스 제공기관에서는 정보를 서버에 저장하기 때문에 중앙서버 공격을 통해 데이터 위·변조 가능(이광형, 「블록체인 기반 안전한 마이데이터 서비스 모델」('20.12월))

44) Decentralized Identifier : 분산원장기술 또는 그 밖의 다른 분산 네트워크 기술을 활용하여 분산된 저장소에 등록함으로써 중앙집중화된 서버와 같은 등록기관이 필요하지 않은 전역 고유 식별자(한국정보통신기술협회)

금융권의 경우 '22.7월부터 13개 은행 영업점 창구와 4개 은행 스마트폰 앱을 통해 모바일 운전면허증으로 계좌개설 등 금융거래가 가능



출처 : 라온시큐어, 「대한민국 최초의 디지털 신분증」(‘21.11월)

## 2 전망 및 대응 전략

### • 금융권 내 디지털 신분증 이용 영역이 확대되고 관련 연구도 활발해질 전망

현재 은행을 중심으로 활용되고 있는 모바일 운전면허증은 향후 증권, 보험 등 다른 금융권으로도 사용 범위가 확대될 수 있을 것으로 전망<sup>45)</sup>

한편 전 세계적으로 디지털 신분증 개발이 추진되고 디지털 신원증명 기술의 상호운용성 확보를 위한 표준화 논의, 디지털 ID의 국제표준 개발 등이 진행됨에 따라 향후 디지털 신분증 시대가 본격화될 가능성

### • 디지털 신원증명 기술 활용에 따른 새로운 위협에 대비할 필요

모바일 신분증 유형에 따라 다양한 인증 방법이 사용되고 있으므로 각 인증 방법별<sup>46)</sup> 특성으로 인한 보안 위협이 발생할 수 있음에 유의할 필요

새로운 디지털 신원증명 체계를 수용할 수 있는 거래환경을 조성하고, 낮은 디지털 접근성을 가지고 있는 소외된 이용자에게도 평등한 금융 서비스를 제공할 수 있도록 금융포용을 고려할 필요<sup>47)</sup>

45) 7.28.(목)부터 13개 은행 영업점 창구에서 모바일 운전면허증으로 계좌를 개설할 수 있습니다.(금융위원회, '22.7.28.)

46) 모바일 운전면허증은 PIN 또는 안면인식, 모바일 주민등록증은 ID/PW 또는 간편인증, 인증서 등으로 인증

47) 모바일 운전면허증 만들려 돈 내고도 1/3은 미설치... 절차 복잡(연합뉴스, '22.10.19.)

## 08

금융보안 규제 합리화,  
전제되는 자율 보안

금융위원회가 디지털 신기술 도입·활용을 안정적으로 지원하기 위해 클라우드 및 망분리 규제 개선방안을 발표. 이러한 규제 합리화는 금융회사 등의 자율적인 보안 노력 강화를 전제하므로 내부통제 강화 및 추가 보안대책 마련 등을 적극 추진할 필요

## 1 이슈 분석

## ● 금융권의 디지털 전환에 따른 금융혁신이 가속화

금융권은 핀테크 산업의 성장, 빅블러 현상, 재택·원격근무 일상화 등의 환경 변화로 ICT 기술을 활용한 디지털 전환을 적극 추진

특히 빅데이터, 인공지능(AI)/머신러닝(ML), 오픈 API 등을 기반으로 하는 다양한 혁신금융서비스를 창출함으로써 소비자의 편익을 증진

## 신기술을 활용한 혁신금융서비스 주요 사례

구분	주요 사례
안면인식기술을 활용한 비대면 실명확인 서비스	비대면 금융거래 또는 접근매체 발급 시 실명확인증표 사진과 고객이 촬영한 얼굴 사진을 대조하는 안면인식기술을 활용하여 실명확인 절차를 간소화
디지털 신원증명 플랫폼	블록체인 기술을 기반으로 하는 정보보관업을 통해 비대면 계좌개설 시 소비자의 신원증명 절차를 간소화하는 서비스
안면인식 결제	실물카드 또는 스마트폰 없이도 얼굴만으로 간편하게 결제(Face pay)할 수 있도록 하는 서비스
동형암호 기반 데이터 결합·분석 서비스	서로 다른 기관이 보유한 개인신용정보를 동형암호로 암호화하고, 암호화된 정보를 결합 및 분석하여 맞춤형 모형을 개발하는 서비스
빅데이터 기반 부동산 시세 자동평가 서비스	국가 공공데이터 등 빅데이터, AI 알고리즘을 이용해 아파트, 빌라 등 부동산 시세·담보가치를 산정하는 서비스

출처 : 금융감독원, 「금융규제 샌드박스 관련 혁신성 심사 사례집」 ('21.6월)

## ● 금융위원회, 「금융분야 클라우드 및 망분리 규제 개선방안」 발표

그간 엄격한 망분리 규제와 클라우드 이용 절차로 디지털 신기술을 도입·활용하는데 어려움이 있다는 의견이 지속 제기

이에 금융위원회는 클라우드 이용 절차의 불분명한 기준을 정비하고 개발·테스트 분야의 물리적 망분리 규제를 예외적으로 완화하는 내용을 골자로 하는 클라우드 및 망분리 규제 개선 방안을 발표<sup>48)</sup>

48) 금융위원회, 「금융분야 클라우드 및 망분리 규제 개선방안」('22.4월)

## 「금융분야 클라우드 및 망분리 규제 개선방안」의 주요 내용

구분	현황	개선
 클라우드	중복·유사한 CSP 평가 항목	중복·유사한 평가항목 정비 (평가항목을 141개에서 54개로 축소)
	비중요업무도 모든 이용규제 준수 필요	중요·비중요 업무간 클라우드 이용 절차 차등화
 망분리	금융회사 등이 각각 CSP 평가 수행	금융보안원 대표평가제 도입
	획일적·일률적·물리적 망분리 규제	개발·테스트 분야 망분리 예외
		비전자금융업무 및 SaaS에 대한 망분리 예외 추진 (규제 샌드박스)
		(중장기) 단계적 망분리 완화 추진

## 2 전망 및 대응 전략

## ● 소스코드 유출 등 보안 위험에 대비하여 보안 통제 및 대책 마련 필요

연구·개발 목적의 망분리 예외가 인정될 경우 혁신의 기회가 확대되는 한편 소스코드 및 중요 정보 유출, 취약한 소스코드 사용으로 인한 보안 침해, 내부망 악성코드 감염 등 보안 위험의 우려도 증가

따라서 보안성을 고려한 안전한 네트워크 인프라 구성, 소스코드 보안 관리를 위한 내부 정책 수립·운용, 소스코드 유출에 대비한 침해사고 대응절차 마련 등 내부통제 강화 및 추가 보안대책 마련 필요

\* 정보보호심의위원회 구성·운영 현황 등 내부통제시스템 점검이 예정되어 있으므로 이에 대비할 필요

## ● 디지털 전환을 안정적으로 뒷받침하기 위한 단계적 규제 개선 추진 전망

「금융분야 클라우드 및 망분리 규제 개선방안」을 반영하여 입법예고된 「전자금융감독규정」은 '23년에 시행될 예정이며, 비전자금융업무 및 SaaS에 대한 망분리 예외도 금융규제 샌드박스를 통해서 허용될 예정

이러한 규제 합리화는 금융회사 등의 자율적인 보안 노력 강화를 전제함을 인지할 필요가 있으며, 금융규제 샌드박스 운영 성과에 따라 향후 SaaS 이용 관련 망분리 규제 개선으로 이어질 가능성에도 주목할 필요

마이데이터 산업의 발전, 종합금융플랫폼 지원을 위한 금융규제 완화 등에 기반하여 초개인화 서비스를 제공하는 '마이플랫폼'이 가능해질 전망이다. 개인에 대한 양질의 데이터 확보가 중요해짐에 따라 과도한 데이터 경쟁에 유의하고 정보보호 노력을 강화할 필요

## 1 이슈 분석

### ● 빅블러 시대, 금융권은 플랫폼 구축에 주목

ICT 기술과 대형 플랫폼을 기반으로 한 빅테크·핀테크 기업이 디지털 기반의 종합금융서비스 구축을 주도하는 등 빅블러<sup>49)</sup> 시대가 도래

최근 금융권은 이업종 기업과의 제휴 또는 금융위원회의 혁신금융서비스 제도<sup>50)</sup>를 통해 생활금융플랫폼 구축을 추진하며 시장 경쟁력 확보에 집중

#### 국내 금융회사의 플랫폼화 전략 현황

기업	제공 서비스	플랫폼 형태	서비스 내용
신한은행	땡겨요	직접 제공	고객과 가맹점 등 플랫폼 참여자 모두에게 혜택을 제공하는 상생 배달업
	발란	제휴	온라인 셀러를 위한 특화 금융상품 제공 및 플랫폼 활용 공동 마케팅 추진
우리은행	택배 서비스	제휴	택배 플랫폼 전문업체와 제휴하여 은행앱에서 택배 서비스 제공
NH농협은행	꽃 배달 서비스	제휴	한국화훼농협의 화훼상품을 은행앱에서 주문 배송
국민은행	알뜰폰 상품 결합	직접 제공	기존 금융 고객을 유지하거나 신규 고객 유치를 위해 알뜰폰 서비스 제공 및 통신비 할인 혜택 제공
하나은행	편의점 서비스	제휴	편의점 내부에 금융 서비스 제공을 위한 공간 마련

출처 : 관련 언론보도

### ● 다양한 금융 서비스를 통합하는 금융권 슈퍼 원앱 전략

슈퍼 원앱 전략은 하나의 통합 애플리케이션(원앱)에서 다양한 금융 서비스를 제공하는 것으로, 금융권에서는 플랫폼 전략의 일환으로 추진<sup>51)</sup>

은행을 중심으로 송금·결제·대출·보험 등 계열사 서비스로의 접근성을 강화하는 한편 고객 행동 분석을 통해 초개인화<sup>52)</sup>된 금융 서비스 제공을 지향

49) 생산자-소비자, 소기업-대기업, 온라인-오프라인, 제품 서비스 간 경계융화를 중심으로 산업·업종 간 경계가 급속히 사라지는 현상 (조용호 저, 「당신이 알던 모든 경계가 사라진다」('13.2월))

50) 기존 금융 서비스의 제공 내용, 방식, 형태 등 차별성이 인정되는 금융업 또는 이와 관련된 업무 수행 과정에서 제공되는 서비스에 대해 규제 적용 특례를 인정하는 제도(「금융혁신지원특별법」 제2조제4호)

51) 한국금융연구원, 「국내은행의 플랫폼 전략 : 현황과 전망」('22.7월)



## 2 전망 및 대응 전략

### ● 마이플랫폼 도입 추진에 따라 데이터 확보 경쟁이 더욱 격화될 가능성

향후 오픈 파이낸스<sup>53)</sup>로의 전환, 마이데이터 발전, 규제 혁신·완화<sup>54)</sup> 등에 기반하여 개인별 맞춤형 금융·생활 서비스를 제공하는 마이플랫폼(My Platform)으로 발전 예상<sup>55)</sup>

마이플랫폼은 양질의 개인정보가 대량으로 집중·융합됨을 전제하는 바 데이터 확보 경쟁 과열 및 소수 플랫폼의 정보 독과점 등과 관련된 이슈 발생 가능

### ● 데이터 처리 관련 금융소비자 권리 보장 및 데이터 보호 노력 필수

데이터 보호에 관한 법령 위반 시 강력한 처벌이 예상<sup>56)</sup>되므로 이에 유의하고, 무분별한 데이터 수집·이용 등 처리가 발생하지 않도록 개인정보 이용 원칙 등에 기반한 정보보호 활동<sup>57)</sup>에 집중할 필요

#### 개인정보 처리 원칙

EU 「GDPR」 개인정보 처리원칙(제5조)	「개인정보보호법」 개인정보 보호 원칙(제3조)
적법성·공정성·투명성	적법성 정당성 명확성(제1항), 처리방침 공개(제5항)
목적 제한	목적 제한(제2항 후단)
데이터 최소화	필요 최소 범위 내 수집(제2항 전단)
정확성	정확성(제3항)
보유기간 제한	
무결성·기밀성	안전한 관리(제4항)
책임성	책임성(제8항)

출처 : KISA GDPR 대응지원센터

또한 보유하고 있는 개인정보의 노출 및 유출 위험성이 상존하므로 해킹 등 보안 위협에 선제적으로 대비하고 보호조치 등을 마련할 필요

전 세계적으로 초개인화 서비스에 필수적인 프로파일링<sup>58)</sup> 기술이 발전함에 따라 소비자의 개인정보 통제권 강화를 위한 규율이 마련되는 추세<sup>59)</sup>로, 마이플랫폼 서비스 제공 시 공정성과 투명성을 고려할 필요

52) 소비자의 상황과 맥락을 실시간으로 파악한 뒤 니즈를 예측해서 상품이나 서비스를 제공하는 것을 통칭(삼성 SDS, 「초개인화 시대의 고객 경험 전략-Z세대의 특성을 중심으로」(‘22.5월))

53) 은행의 계좌정보 및 결제기능의 개방에 초점을 둔 오픈뱅킹 개념을 여타업권 상품 추가, 기능 확대 등을 통해 포괄적으로 확장(금융위원회)

54) 금융규제혁신회의에서는 규제 혁신의 최우선 과제로 금산분리 완화를 선정하고, 은행이 디자인 회사·생활서비스 업체·소프트웨어 개발 회사 등을 인수할 수 있는 길을 열어줄 것이라 발표(「금융규제혁신회의」 출범식 개최(금융위원회 보도자료, ‘22.7.19.))

55) 금융위원회는 마이데이터에서 더 나아가 개인화된 금융·생활 서비스를 제공하는 나만의 공간 개념으로 '마이플랫폼' 도입을 추진하겠다고 밝힘(개인화된 금융 서비스 제공받는 '마이플랫폼' 도입 추진(아주경제, '21.12.15.))

56) 최근 이용자 동의 없이 개인정보를 수집하여 온라인 맞춤형 광고에 활용하는 등 개인정보 보호법을 위반한 구글과 메타에 대하여 개인정보보호위원회가 시정명령과 함께 약 1,000억 원의 과징금을 부과(「개인정보 불법수집」 구글, 메타에 1000억 과징금(한국경제, '22.9.14.))

57) Gartner는 개인정보보호 등 디지털 윤리가 2021년 Hype Cycle의 정점에 있으며 2023년 말까지 전 세계 기업 중 80% 이상이 최소한 하나 이상의 데이터 보호 규정을 마련하게 될 것으로 예측(Gartner press release, '21.9.30.)

58) 개인의 관심, 개인적 선호, 건강, 경제 상황, 근무 성과 등을 분석하여 예측하는 등 개인적인 특성을 평가하기 위해 행해지는 모든 형태의 자동화된 개인정보 처리(예 : 이용자 맞춤형 광고, 소비패턴 기반 최적 카드 추천)

59) EU 「GDPR」(‘18.5월 발효), EU 「Digital Services Act」(‘20.12월 발의), 국내 「온라인 플랫폼 중개거래의 공정화에 관한 법률안」(‘21.1월 발의)

## 10

금융권 채널 변화의 핵심  
디지털 연결

최근 금융권은 점포, 웹·앱 등 채널을 유기적으로 연결하는 옴니채널 전략과 은행, 증권 등 다양한 금융 서비스를 하나의 앱을 통해 제공하는 디지털 유니버설 뱅크를 추진 중. 이러한 채널 혁신이 기존 법체계 및 제도 개편에 대한 요구로 이어질 가능성에 주목할 필요

## 1 이슈 분석

## ● 혁신 점포·디지털 공동 점포 등 오프라인 점포에도 디지털을 접목

비대면 금융 서비스 확산으로 이용률이 낮은 오프라인 점포 축소가 가속화<sup>60)</sup> 되고 있으며 그 대안으로 혁신 점포, 디지털 공동 점포가 등장

고객 스스로 업무를 볼 수 있도록 AI 행원·로봇 컨시어지·키오스크·종합금융기기(STM)<sup>61)</sup> 등 디지털 기기를 이용한 무인 형태로 운영

## 혁신 점포 및 디지털 공동 점포 사례

구분	사례
신한은행 - GS리테일	GS편의점 내 신한은행 혁신 점포 설치(숍인숍 형태)
	디지털 데스크, 스마트키오스크, 로봇 컨시어지 등 적용
국민은행 - 이마트	KB디지털뱅크 NB 강남터미널점(디지털 점포) 설치
	종합금융기기(STM)를 통한 체크카드 및 보안매체 발급, 현금 및 수표 입출금, 화상상담 전용 창구를 통한 통장개설 등 가능
미래에셋증권 - 인터넷은행	케이뱅크, 카카오�뱅크 계좌 보유 고객이 주식 계좌를 개설할 수 있는 디지털 공동 점포 추진

출처 : 관련 언론보도

## ● 온-오프라인 및 타 업권 등과의 연결을 시도하는 금융권 채널 전략

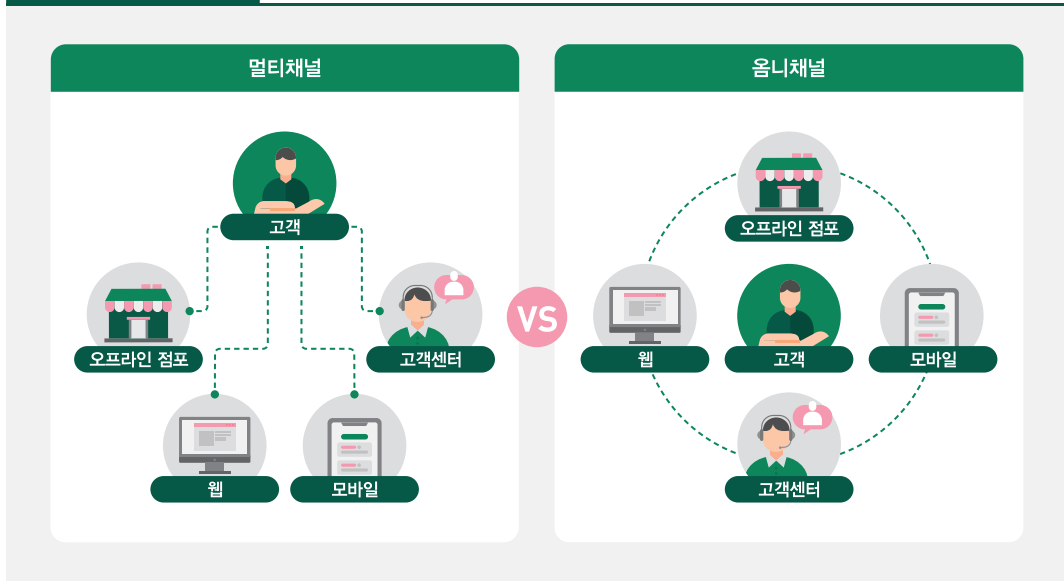
디지털 기반의 대면 채널 혁신과 함께 점포, 웹·앱, 고객센터 등 멀티 채널에서의 고객 경험을 통합함으로써 온·오프라인에서 일관된 서비스를 제공하고 고객 중심 서비스를 강화하는 옴니채널(Omni channel) 전략이 대두<sup>62)</sup>

60) '22.6월 말 기준 4대 은행(KB국민·신한·하나·우리)의 점포(지점+영업소) 수는 총 2,943곳으로 지난해 말 3,079곳 대비 136곳이 축소 ("나이트 우린 어떡하랴구"... 은행원 AI 대체되고 인근점포 사라져(매경, '22.9.12.))

61) Smart Teller Machine : 신분증 스캔, 화상 인증, 얼굴사진 촬영, 바이오인증을 통해 영업점 창구업무를 고객이 직접 처리 가능한 디지털 무인 채널(신한·우리 이어 국민은행도 '디지털 무인채널' 도입(뉴스토마토, '18.7.8.))

62) 오프라인 점포에 디지털 경험을 녹이는 등 대면 채널의 고도화를 통해 대면-비대면에서 일관된 서비스를 제공할 뿐만 아니라 점포, 웹·앱, 고객센터 등 다양한 채널 간 상호 연계를 구축하는 전략(은행 점포의 재발견... '옴니채널'로 변신해 고객과 소통하다.(인사이트코리아, '22.1.20.))

## 멀티채널과 옴니채널



출처 : Freshworks

또한 금융그룹이 하나의 앱을 통해 은행, 증권, 보험, 카드 등 다양한 금융 서비스를 제공하는 디지털 유니버설 뱅크도 추진

## 2 전망 및 대응 전략

- 변화하는 채널 환경에 따른 운영·보안 리스크 관리 방안 마련 필요

디지털 혁신 점포 내 설치된 기기 고장 등 돌발 상황에 따른 서비스 지연<sup>63)</sup>, 키오스크와 같은 셀프 서비스 기기를 노린 사이버 위협<sup>64)</sup> 등 다양한 운영·보안 리스크에 대한 대응 방안 마련 필요

또한, 채널 간 또는 타 업권과의 디지털 연결에 따른 리스크 전이 등 발생 가능한 보안 위협을 검토하고 대응방안을 마련할 필요

- 디지털 채널 혁신의 안착이 기존 법 체계 및 제도 개편 요구로 이어질 가능성

현재 은행권을 중심으로 추진 중인 디지털 유니버설 뱅크는 플랫폼을 활용한 종합금융서비스 체계의 점진적인 전환과 업종간 경계가 확대되는 디지털 유니버설 금융화를 촉진할 것으로 평가<sup>65)</sup>

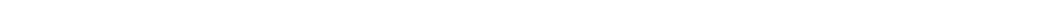
디지털 유니버설 금융화가 가속되는 등 디지털 연결에 기반한 금융 서비스의 안착이 금융회사 업무 범위 확대 등 기존 법체계 및 제도 개편에 대한 요구로 이어질 가능성에도 주목할 필요

63) 편의점 들어간 무인 은행점포... 카드 신청했지만 '30분 허탕'(한겨레, '22.8.28.)

64) 키오스크 등 무인화기기는 Windows Embedded POSready 7, Windows 10 IoT 등 무인화기기에 맞는 윈도우 운영체제가 보급되고 있어 윈도우즈 관련 취약점이 무인화기에도 적용([테크칼럼] 무인화기기 시대 본격화 ①무방비로 노출된 무인화기기 보안 (보안뉴스, '21.1.21.))

65) 한국금융연구원, 「국내은행의 플랫폼 전략 : 현황과 전망」('22.7월)

금융보안원  
FINANCIAL SECURITY INSTITUTE



금융보안원  
FINANCIAL SECURITY INSTITUTE







Digital Finance & Cyber Security

## 2023 디지털금융 및 사이버보안 이슈 전망