

# 2021 Digital Finance & Cyber Security

## 디지털금융 및 사이버보안 이슈 전망



# 2021 Digital Finance & Cyber Security

## 디지털금융 및 사이버보안 이슈 전망

01 언택트 시대, 가속화되는 비대면 금융



02 원격근무 시대의 도래, 필수적인 사이버보안



03 사이버공간 협박범, 랜섬웨어와 랜섬디도스 공격 증가



04 그 누구도 안심할 수 없다, 고도화되는 보이스피싱



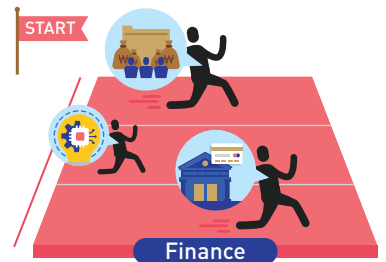
05 새로운 인증시장, 누가 주도할 것인가



06 금융의 신성장 동력, 데이터 산업 경쟁 본격화



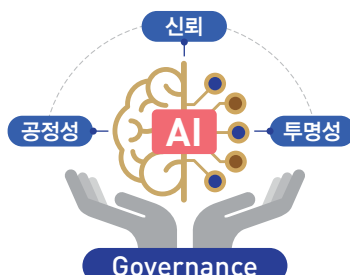
07 금융 산업의 개방, 다양한 플레이어의 등장



08 지갑이 휴대폰 속에? 지갑 없는 사회의 시작



09 책임 있는 AI를 위한 금융권 노력, AI 거버넌스 구축



10 세계로 뻗어나가는 금융, 글로벌 컴플라이언스 강조



# Contents

## 01

연택트 시대, 가속화되는 **비대면 금융** ..... 1

## 02

**원격근무** 시대의 도래, 필수적인 **사이버보안** ..... 3

## 03

사이버공간 협박범, **랜섬웨어**와 **랜섬디도스** 공격 증가 ..... 5

## 04

그 누구도 안심할 수 없다, 고도화되는 **보이스피싱** ..... 7

## 05

**새로운 인증시장**, 누가 주도할 것인가 ..... 9

## 06

금융의 신성장 동력, **데이터 산업 경쟁** 본격화 ..... 11

## 07

금융 산업의 개방, **다양한 플레이어의 등장** ..... 13

## 08

지갑이 휴대폰 속에? **지갑 없는 사회**의 시작 ..... 15

## 09

**책임 있는 AI**를 위한 금융권 노력, **AI 거버넌스** 구축 ..... 17

## 10

세계로 뻗어나가는 금융, **글로벌 컴플라이언스** 강조 ..... 19

# 01. 언택트 시대, 가속화되는 비대면 금융

**키워드 정의** 언택트(Untact) : Un-(부정)과 Contact(접촉)의 합성어로 '비접촉·비대면'을 의미  
 비대면 금융 : PC, 모바일, ARS, CD/ATM 등 대면(face-to-face)하지 않은 채 제공되는 전자금융서비스를 의미

## 1.

### 이슈 분석

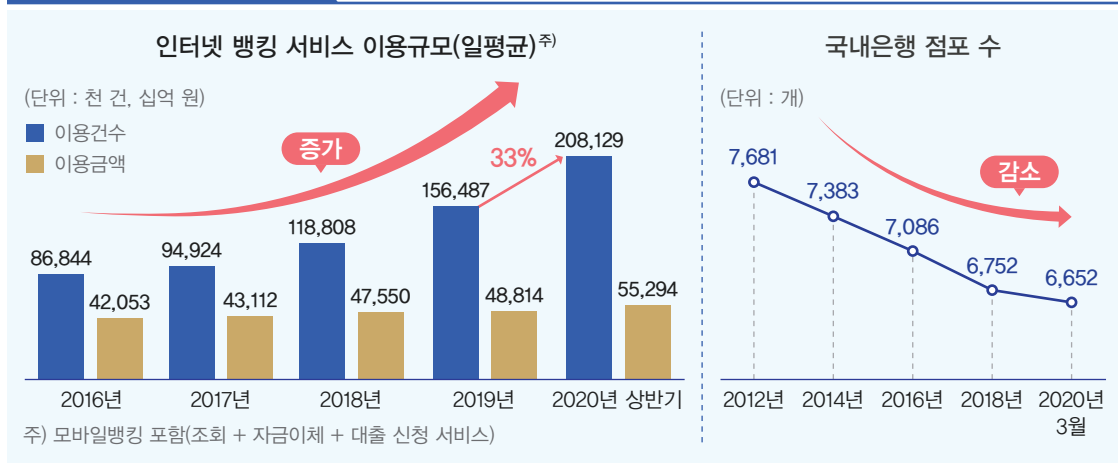
#### 코로나19로 비대면 금융서비스 확산이 가속화

인터넷(모바일) banking 이용 규모는 꾸준히 확대되는 한편 오프라인 점포 수는 지속적으로 감소하는 추세

특히 코로나19로 인한 사회적 거리두기 등으로 인해 인터넷(모바일) banking<sup>1)</sup> 및 비대면 결제\* 이용규모가 큰 폭으로 증가

\* '20.1~9월 기준 비대면결제 이용규모(일평균 0.8조원)는 전년 동기 대비 17% 증가

#### 비대면 금융서비스 현황



[출처] 한국은행, 금융감독원

#### 비대면 금융을 타겟으로 한 금융사기 다양화·고도화

신분증 진위 확인 시 사진 미확인 등 비대면 실명확인 절차\*상의 취약점을 악용한 사고가 발생하는 등 금융사기 기법이 고도화

\* ①신분증 사본 제출, ②영상 통화, ③접근매체 전달 시 확인, ④기존 계좌 활용, ⑤기타 이에 준하는 방법 중 2가지 필수 적용 (추가적으로 ⑥타 기관 확인 결과(휴대폰 본인확인 등) 활용, ⑦다수의 고객 정보 검증 적용을 권고)

1) 인터넷(모바일) banking을 통해 전체 입출금·자금이체 서비스의 64.3%, 조회 서비스의 91.5%를 제공 ('20.6월, 일평균 거래건수 기준) (출처 : 한국은행)

## 비대면 금융을 악용한 사기(예시)



[참고] FISCON 발표자료 중 금융감독원 「디지털금융 혁신과 안정을 위한 IT 감독 방향」

금융 앱을 위·변조하거나 블랙마켓에서 공격 정보를 습득하는 등 공격 방식이 다양화되고 있으며, 신분증 사진의 스마트폰 내 저장 등 사용자 부주의에 의한 보안사고 우려도 존재

## 인터넷(모바일)뱅킹 관련 취약점 사례

- 앱 실행 파일의 일부만 무결성 검증 기능을 적용하여 위·변조 가능
- 블랙마켓 내 위·변조 앱 모니터링 대상에 주요 포털사이트 미 포함
- 중요 정보가 앱 화면에 노출되거나 화면 캡처 방지 등 보호대책 미 적용
- 신분증 사진의 서버 전달 시 보안성이 취약한 암호화 방식을 사용하여 복호화가 우려
- 앱 구동 시 백신 프로그램의 업데이트 상태 미 확인 등

[참고] 금융회사·전자금융업자 행정처분 사례('19~'20)

## 2. 전망 및 시사점

### 비대면 금융의 보안 위협은 지속되고 그 파급력도 확대 전망

전자금융거래법이 개정되면 비대면 금융 방식이나 서비스가 더욱 다양화될 것으로 보여 이를 악용한 공격도 지속될 전망

오픈뱅킹, 마이데이터 산업 활성화 등으로 특정 금융회사 보안사고가 타 금융회사로 쉽게 전파\*될 수 있어 공격에 따른 파급력도 지속 확대

\* (예시) 보안이 취약한 A은행에서 계좌 개설 및 공인인증서 발급 → B은행에서 A은행 공인인증서 등록 및 A은행 계좌를 활용하여 인증 → B은행에서 대출 실행

### 비대면 금융의 기반에는 보안성과 포용성이 전제될 필요

금융소비자는 비대면 금융의 편리함에 만족하는 동시에 보안에 대한 우려도 크므로 편리성과 보안성 간 균형성 확보가 중요

스마트폰 사용에 익숙하지 않은 고령층 등 디지털 취약계층이 비대면 금융에서 소외되지 않도록 지속 노력할 필요

## 02. 원격근무 시대의 도래, 필수적인 사이버보안

**키워드 정의**    **원격근무** : 회사 밖에서 근무하는 형태로, 자택에서 근무하는 '재택근무', 출장지에서 근무하는 '모바일근무', 본래 근무지 외의 지역에 설치된 공용사무실을 활용하는 '위성근무' 등으로 다양<sup>2)</sup>

### 1. 이슈 분석

#### 금융권 원격근무 확대<sup>3)</sup>로 공격 범위가 기업 내부 ▶ 외부로 확대

원격근무 장소나 단말기, 네트워크 등의 경우 기업 내부에 비해 상대적으로 보안 통제가 어려워 공격자의 주요 공격 대상으로 부각

#### 원격근무 시 공격 가능 범위



공격자는 원격근무자에 피싱 메일 발송, 크리덴셜 스티핑<sup>4)</sup> 공격 등을 수행하여 악성코드 유포, 내부망 접근, 기업 내부 정보 탈취 등이 가능

#### 원격근무에 따른 주요 보안 위협

구분	주요 보안 위협
원격근무 단말기의 물리적 통제 미흡	· 원격근무 단말기의 분실·도난이나 타인의 훔쳐보기 등으로 단말기 내 데이터가 유·노출되거나 기업 내부망 접근 등이 우려
안전하지 않은 네트워크 사용	· 원격근무자가 사용하는 외부 네트워크(인터넷)는 통제가 어려워 도청이나 중간자 공격(MITM) 등으로 중요 정보가 유출될 우려 · 잘못된 네트워크 장비(VPN 등) 설정이나 네트워크 장비 취약점 존재
악성코드 감염에 따른 내부망 침해	· 악성코드에 감염된 원격근무 단말기로 내부망에 접속 시 시스템의 불법 침해 가능
내부 자원에 대한 원격접근 위협	· 기업 내부에서만 접근 가능했던 내부 자원에 대해 원격근무 단말기도 접근 가능해짐에 따라 비인가 접근 등 보안 위협 존재

[참고] 美 NIST 「Guide to Enterprise Telework, Remote Access, and BYOD Security」 등

2) 참고 : 「With/After COVID-19 시대 금융기관의 과제」 (한국금융연구원, '20.10월)

## 이용자가 급증한 화상회의 솔루션<sup>5)</sup>도 공격 타겟으로 부각

화상회의 솔루션 자체 취약점이나 화상회의 접근통제 미흡\* 등을 악용하여 공격자가 화상회의에 무단 접속하는 사례가 발생

\* 회의방 전체 공개, 회의 참여 접근코드 재사용, 회의 참여자 신원 미확인 등

화상회의 접속에 성공한 공격자는 회의 방해, 회의 중 공유된 정보 또는 파일 탈취, 악성코드 유포\* 등의 공격 수행 가능

\* (예시) 회의 시 업로드하는 GIF 형태의 이미지 파일에 대한 화상회의 솔루션의 검증 기능이 미흡할 경우, 악성코드가 포함된 이미지 파일을 업로드하여 회의 참여자에 유포

## 2. 전망 및 시사점

### 원격근무나 화상회의는 일시적 유행이 아닌 기업 문화로 정착

금융의 디지털 전환 가속화, 일과 삶의 균형(일명 '워라밸') 추구 확대 등으로 원격근무나 화상회의가 기업 문화 중 하나로 자리매김

금융권은 「전자금융감독규정 시행세칙」을 개정(21.1.1 시행)하여 철저한 보안통제 하에 임직원의 상시 재택근무를 허용한 바, 원격근무 등이 빠르게 확대될 전망

### 원격근무나 화상회의의 수행 시 보안통제 강화가 필수

원격근무나 화상회의의 수행에 있어 기존 근무 및 회의 형태에 비해 보안수준이 저하되어서는 안된다는 점이 매우 중요

금융권은 원격근무나 화상회의의 수행 범위를 정하고 재택근무 환경 구축 시부터 종료 시점까지 철저한 보안통제 대책을 마련할 필요

### 원격근무 및 화상회의 시 보안 고려사항

원격근무 시		화상회의 시	
외부 단말기 보안관리	백신 프로그램 설치, 안전한 운영체제 사용 등	1. 화상회의 전	· 화상회의의 보안정책 마련 및 준수 · 화상회의의 참여 접근코드 재사용 제한 등
내부망 접근통제	최소한의 IP 및 Port로만 연결 허용, 미인가 IP 접속 차단 등		
인증	원격접속 시 이중 인증(MFA) 적용 등	2. 화상회의 중 또는 종료 후	· 화면상 민감한 문서 또는 정보 노출 금지 · 회의 참여자 신원확인 등
통신회선	전용회선과 동등한 보안 수준을 갖춘 가상사설망(VPN) 구축 등		

※ 자세한 내용은 금융보안원 보도자료('20.4.10, '20.11.18.) 참고

- 3) 코로나19 이후 원격근무 시행 기업이 4배 이상 증가 (8.3% → 34.3%) (출처 : 대한상공회의소)
- 4) 크리덴셜 스테핑(Credential Stuffing) : 다른 곳에서 탈취한 사용자 계정을 무작위로 대입 및 로그인을 시도하는 공격 방식으로, 이를 통해 기업 메일, 인트라넷 등의 무단접속 시도 가능
- 5) 대표적인 화상회의의 솔루션인 'Zoom' 이용자는 '20.1월 1만여 명(추정)에서 '20.9월 707만 명으로 700여 배 급증 (출처 : 보안뉴스)

# 03. 사이버공간 협박범, 랜섬웨어와 랜섬디도스 공격 증가

**키워드 정의**    **랜섬웨어(Ransomware)** : ‘인질’(Ransom)과 ‘소프트웨어’(Software)의 합성어로, 데이터 암호화, 시스템 가용성 등을 인질로 금전 요구를 목적으로 하는 악성코드

**랜섬디도스(Ransom DDoS)** : ‘인질’(Ransom)과 ‘디도스’(DDoS, 비정상적 대규모 트래픽을 유발하여 서비스를 다운시키는 공격)의 합성어로, 금전 미지불 시 IT 전산 인프라를 마비시켜 서비스 운영에 장애를 일으키겠다고 협박하는 공격 기법

## 1. 이슈 분석

### 랜섬웨어 공격 방식 고도화 및 협박 수위 강화

특정 임직원을 타겟으로 한 스피어피싱<sup>6)</sup> 메일 발송, 보안이 취약한 해외법인 경우 등 랜섬웨어를 사내에 유포하기 위한 방법이 고도화

협박도 데이터 암호화 뿐만 아니라 데이터의 일부(또는 전체) 공개나 데이터 탈취 사실 언론 폭로 등 그 수위가 높아지는 추세<sup>7)</sup>

#### 랜섬웨어 공격 방식

원격제어 악성코드 유포 등



최초 감염



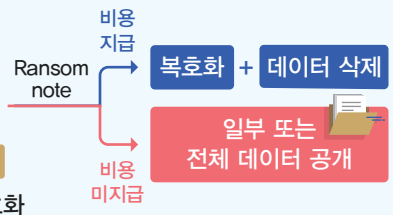
데이터 탈취



랜섬웨어 유포



데이터 암호화



### 국내 금융권을 대상으로 한 랜섬디도스 공격 급증<sup>8)</sup>

공격자는 협박 메일을 통해 가상자산을 입금하지 않으면 대규모 디도스 공격을 수행하겠다고 협박

※ 공격 효과 극대화를 위해 협박 메일 송부 후 소규모 디도스 공격을 우선 수행하는 경우도 존재

디도스 공격은 IP 주소 조작이 가능한 UDP 증폭 반사 공격 기법<sup>9)</sup>을 주로 사용

6) 스피어피싱(Spear-phishing) : 물고기를 작살로 잡는 작살 낚시(Spearfishing)를 빗댄 용어로 불특정 다수가 아닌 특정인을 대상으로 개인정보를 훔치는 피싱 공격을 의미  
 7) 최근 국내 대기업을 대상으로 랜섬웨어 감염 및 기밀 데이터 유출을 빌미로 협박하는 사례 발생  
 8) '20.9월부터 전 세계적으로 랜섬디도스 공격이 증가하였으며, 이는 국내 금융권 대상 랜섬디도스 공격이 본격 발생한 시점('20.8월 중순)과 유사 (출처 : 네트워크 보안업체 'Imperva')  
 9) DNS(Domain Name Service), NTP(Network Time Protocol) 등 UDP(User Datagram Protocol) 기반 서비스를 악용하여 대량의 트래픽을 유발하는 디도스 공격 기법으로, 취약한 서버에 악의적인 요청 패킷을 보내고 응답 패킷을 증폭시켜 공격 효율성을 제고하는 것이 특징



## 랜섬디도스 협박 메일 사례

We are the Fancy Bear and we have chosen [redacted] as target for our next DDoS attack.

Please perform a google search for "Fancy Bear" to have a look at some of our previous work. Also, perform a search for "NZX" or "New Zealand Stock Exchange" in the news. You don't want to be like them, do you?

Your whole network will be subject to a DDoS attack starting in 7 days, Monday next week. (This is not a hoax, and to prove it right now we will start a small attack on your DNS servers that will last for about 60 minutes. It will not be heavy attack, and will not cause you any damage, so don't worry at this moment.) There's no counter measure to this, because we will be attacking your IPs directly [redacted] and our attacks are extremely powerful (peak over 2 Tbps)

This means that your websites and other connected services will be unavailable for everyone. Please also note that this will severely damage your reputation among your customers who use online services.

Worst of all for you, you will lose Internet access in your offices too!

We will refrain from attacking your network a small fee. The current fee is 20 Bitcoin (BTC). It's a small price for what will happen when your whole network goes down. Is it worth it? You decide!

We are giving you time to buy Bitcoin if you don't have it already. And hopefully for this message to reach somebody who can handle it properly.

If you don't pay the attack will start and fee to stop will increase to 30 BTC and will increase by 10 Bitcoin for each day after the deadline that passed without payment.

Please send Bitcoin to the following Bitcoin address: [redacted]

- 유명 공격그룹이라 자칭
- 뉴질랜드 증권거래소 공격 성공사례 언급<sup>10)</sup>
- 스팸메일로 필터링되지 않도록 메일 본문을 이미지 파일로 변환
- 복사·붙여넣기 할 수 있도록 전자지갑 주소는 텍스트 형태로 송부

## 2. 전망 및 시사점

### 랜섬웨어·디도스 공격 수행 환경이 공격자 친화적으로 진화되고 있어 위험이 확대될 전망

(랜섬웨어) 랜섬웨어를 제작·판매하는 서비스형 랜섬웨어(RaaS)<sup>11)</sup> 활용, 다크웹 내 해킹 정보 판매 등 랜섬웨어 공격이 활성화될 수 있는 환경 조성

(랜섬디도스) 봇넷(Botnet)으로 악용 가능한 IoT 기기 보급의 증대\*, 디도스 공격 대행 서비스의 등장 등으로 과거에 비해 공격 수행이 수월

\* IoT 기기 보급 증대 등으로 이를 악용한 테라급 규모의 디도스 공격도 가능한 환경

### 금융권은 랜섬웨어·디도스 공격에 철저히 대비할 필요

금융권은 대량의 개인(신용)정보를 보관하고 있고 서비스 가용성이 중요한 업무로 랜섬웨어나 랜섬디도스 공격의 주요 타겟이 될 전망

국내외 공격 동향 등을 면밀히 모니터링하여 금융권 환경에 맞는 대응 방안을 마련하고 이를 지속 개선할 필요

## 랜섬웨어 및 랜섬디도스 공격 대응 방안

랜섬웨어	<ul style="list-style-type: none"> <li>• e-mail을 통한 악성코드 유입 예방을 위해 스팸메일 차단 및 악성코드 사전 검사</li> <li>• 데이터 유출에 대비하기 위해 DRM 등 문서 암호화 보안솔루션 도입</li> <li>• 다크웹 상에서 이루어지는 랜섬웨어 공모, 데이터 유출 등을 모니터링</li> </ul>
랜섬디도스	<ul style="list-style-type: none"> <li>• 국내외 랜섬디도스 공격 관련 정보 공유 및 모니터링</li> <li>• UDP에 비해 대응이 어려운 TCP 기반 공격 발생 가능성도 있으므로 공격 대응훈련 실시 등 사전 대비 필요</li> </ul>

10) 뉴질랜드 증권거래소의 경우 5영업일('20.8.25.~8.31.) 간 디도스공격이 지속되어 증권거래 업무가 마비

11) 서비스형 랜섬웨어(RaaS : Ransomware as a Service) : 해커가 랜섬웨어를 제작하여 공격자에게 판매하는 형태로, 공격자는 랜섬웨어 공격 후 갈취한 이익금을 제작자(해커)에게 배분

# 04. 그 누구도 안심할 수 없다, 고도화되는 보이스피싱

**키워드 정의** 보이스피싱(Voice Phishing) : 전화, SMS, 웹사이트 등 전기통신을 통해 타인을 속이거나 협박하여 ①자금을 송금·이체하도록 하거나 ②개인정보를 알아내 자금을 송금·이체하도록 함으로써 금전적 이익을 편취하는 사기·공갈 행위<sup>12)</sup>

## 1. 보이스피싱은 갈수록 고도화 및 지능화되는 추세

### 이슈 분석

보이스피싱 범죄조직<sup>13)</sup>은 대출 사기형, 기관 사칭형, 메신저 피싱 및 납치·사고 빙자형 등의 범죄 수법을 사용하여 체계적으로 접근

#### 보이스피싱 범죄 수법 구분

구분	내용
대출 사기형 <sup>14)</sup>	· 저금리 대출 등을 조건으로 수수료, 선이자 등을 요구
기관 사칭형	· 검찰, 금융당국 등을 사칭하여 접근한 후 범죄 수사, 피해자 자금 보호 등의 명목으로 자금을 요구
메신저 피싱 <sup>15)</sup>	· 메신저(또는 문자)를 통해 온라인 결제, 채무 상환 등을 빌미로 자금이체 또는 개인(신용)정보를 요구 · 탈취한 정보로 비대면 계좌개설이나 대출·이체 등을 실행하는 경우도 존재
납치·사고 빙자형	· 자녀의 납치 또는 사고를 빙자하여 금전을 요구

[참고] 금융위원회 보도자료('20.6.24.), 금융감독원 보도자료('20.11.4.), 경찰청 보도자료('19.11.6.)

코로나19 등 사회환경 반영, 서류 위조, 영상통화\* 등 수법이 더욱 치밀해지고 있어 누구든지 보이스피싱 피해자가 될 수 있는 상황

\* (예시) 검사실로 위조한 장소에서 영상통화를 수행하여 피해자로부터 신뢰 획득

#### 최근 보이스피싱 사례

##### 사회환경 반영

코로나19 관련  
정부지원 대출을 사칭

전달: [Web발신] 정부정책 대출 (광고)  
"항상 을 이용해주시는 여러분께 고 계속여 감사 말씀드리며, 언제나 최고의 서비스로 보답하겠습니다."  
금일부터 정부에서 긴급재난지원 대출이 실행이 되어, 전국민 대상으로 담보(보증) 없이 당일기준 추가 한도 승인 진행이되며, 이번 4월 한달간 진행되는 상품으로 경제 및 생계 활동에 부담이 없으시길 바랍니다.

##### 서류 위조

명함, 공문, 고소장, 구속영장 등을 위조



[출처] (원)금융감독원 보도자료('20.4.8.), (오)서울중앙지방법경찰청 보도자료('20.11.13.)

## 모바일 앱(App)을 악용한 보이스피싱도 성행

보이스피싱 범죄조직은 URL 등을 보내 악성 모바일 앱 설치를 유도한 후 전화를 가로채거나 휴대폰을 원격제어하여 피해자의 금융 앱을 실행

### 모바일 앱(app)을 악용한 보이스피싱 수법

전화 가로채기	· 피해자가 금융회사 대표번호로 발신하는 확인 전화를 가로채어 범죄조직이 수신
휴대폰 원격제어	· 피해자의 휴대폰에 원격제어 앱을 설치하여 개인정보 탈취 또는 이체·대출 등을 실행

최근 악성 모바일 앱은 정보(SMS, 연락처, 단말기 모델 정보, 통신사 등) 탈취나 전화 가로채기 뿐만 아니라 실시간 스트리밍, 로그 수집·삭제, 카메라 전·후면 변경 등 다양한 기능을 탑재

## 2. 전망 및 시사점

### 보이스피싱은 신기술과 연계하여 더욱 위협적으로 진화할 전망

AI로 음성이나 영상을 실제처럼 조작하는 딥페이크(Deepfake) 기술 등을 악용한 본인 사칭 등 보이스피싱 공격은 더욱 정교해질 전망

※ 영국에서는 딥페이크 기술을 악용하여 회사 최고경영자의 음성을 모방해 약 22만 유로를 편취하는 사건이 발생('19년)하였으며, 이후 유사 사건도 발생

클라우드 이용 확대에 따라 취약한 클라우드 해킹을 통해 취득한 정보로 보이스피싱을 수행하는 경우도 발생할 것으로 예상

### 보이스피싱에 대한 전방위적 대응이 필요

실효성 있는 보이스피싱 대응을 위해서는 정부부처, 수사기관, 금융회사, 통신사 뿐만 아니라 국민 모두가 경각심을 제고하는 노력도 필수

### 보이스피싱 대응 방안

#### 정부부처 등

- 대국민 홍보 등 경각심 강화
- 보이스피싱 수사 단속
- 피해 구제 대책 마련
- 범죄 악용 우려 업체 점검 등

#### 금융회사

- 피해 의심 계좌에 대한 이체 지연 등 피해 방지 조치
- 금융 앱에 보이스피싱 방지 기능 탑재 등

#### 통신사

- 휴대폰 명의도용 등 부정 사용 방지 체계 구축
- 보이스피싱 블랙리스트 등록 번호 수신 시 정보 표시 등

#### 국민

- 출처가 불분명한 링크나 앱은 클릭 금지
- 모바일 백신 업데이트
- 지인 사칭 의심 시 사실 확인 등

[참고] 금융위원회 보도자료('20.6.24.) 등

보이스피싱 예방·대응 방안도 시 등을 기반으로 고도화할 필요가 있으며, 범금융권 정보 공유체계 구축 등도 적극 추진할 필요

- 12) 통상 '보이스피싱'은 본 정의와 같이 「통신사기피해환급법」 상 '전기통신금융사기'를 의미하나, 법률상 전기통신금융사기에 포함되지 않는 대면 편취형 사기 등을 포괄하여 넓은 의미로 사용되기도 함.
- 13) 범죄조직은 주로 중국 내 총책 및 콜센터(시나리오팀·마케팅팀·전산팀), 국내 계좌개설팀, 현금인출팀, 환전송금팀 등으로 구성 (출처 : 이기수(2018), 최근 보이스피싱의 범죄 수법 동향과 법적 대응 방안, 범죄수사학 연구)
- 14) 건당 피해액(약 802만 원)은 상대적으로 적은 편이나 전체 피해건수의 약 78%를 차지('19년 기준)
- 15) 보이스피싱 대응 강화, 코로나19 등의 영향으로 '20. 1~9월 보이스피싱 총 피해액은 전년 동기 대비 감소하였으나 메신저 피싱 피해액은 25.3% 증가

## 05. 새로운 인증시장, 누가 주도할 것인가

**키워드 정의** 인증(Authentication) : 금융거래 시 안전성 및 신뢰성을 확보하기 위해 본인 여부, 금융거래 지시·내용 등을 전자적으로 확인 또는 증명하는 방법

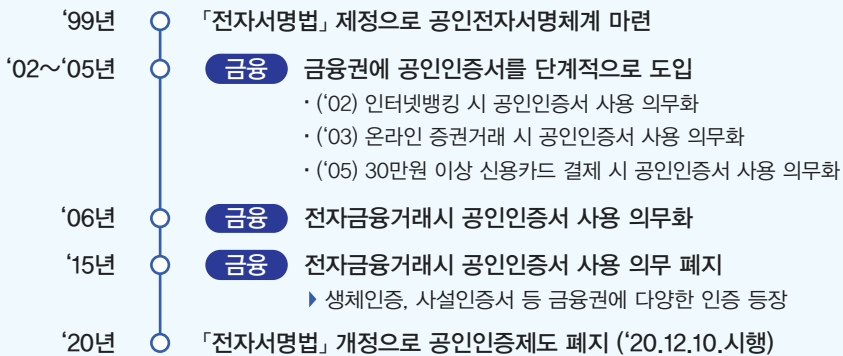
### 1. 이슈 분석

#### 공인인증서 ▶ 다양한 인증수단으로 인증 정책이 전환

전자서명법 개정(20.12.10 시행)으로 20여 년 만에 공인인증서의 우월적 지위가 폐지\*됨에 따라 금융, 공공분야 등에서 다양한 인증수단이 동등하게 경쟁할 수 있는 환경이 조성

\* '공인인증서', '공인인증기관' 등의 용어를 '인증서', '전자서명인증사업자'로 통합·변경

#### 공인인증제도의 변천



금융위는 보안성·편의성을 갖춘 다양한 인증수단이 금융권에 활용될 수 있도록 정책 마련을 추진 중으로, 금융거래 위험 수준별 인증수단 차등화 등을 검토 중<sup>16)</sup>

※ EU는 계좌 온라인 접근, 전자지급거래 개시 등의 고위험거래 시 2팩터 인증과 같은 강력한 고객인증(SCA)<sup>17)</sup> 적용을 의무화

#### 공인인증서 폐지 이후 금융 인증시장 선점을 위한 경쟁 본격화

금융권은 사설인증서, 바이오인증 등 다양한 인증수단을 활용하고 있으며, 최근에는 자체 인증서를 개발하여 이용 범위를 확대하려는 움직임도 존재\*

\* (예시) KB국민은행은 행정안전부 공공분야 전자서명 확대 도입 시범사업의 후보사업자로 선정

네이버, 카카오 등 플랫폼 사업자나 이동통신사 등도 넓은 고객 접점을 기반으로 금융권 인증시장 진출을 추진

16) 출처 : 금융위원회 「디지털금융 종합혁신방안」 (보도자료 '20.7.24.)

17) SCA(Strong Customer Authentication) : 지식, 소유, 특징 중 두 가지 이상의 요소를 기반으로 한 인증

금융권 활용 사설인증서(예시)<sup>18)</sup>

구분	발행기관	서비스명	특징
금융권 공동	은행연합회	뱅크사인	• 은행권 컨소시엄 블록체인 활용
	금융결제원	금융인증서	• 금융결제원 및 은행권 공동 참여 ('20.12.10.본격실시) • 금융결제원 클라우드에 인증서를 보관
금융회사 자체 인증	KB국민은행	KB모바일인증서	• KB금융그룹(보험·증권·카드 등) 내 이용 확대 추진 • 인증서 유효기간 없음 (단, 1년 이상 미사용 시 자동 폐기)
	IBK기업은행	i-ONE뱅크 내 모바일 인증서	• 자사 모바일뱅킹 서비스에서 활용 가능 • 공인인증서 대체를 위한 6자리 비밀번호 기반의 인증서
플랫폼 사업자	네이버	네이버 인증서	• 네이버 전자문서(고지서) 서비스 등에 활용 • 모바일 및 PC(자사 브라우저) 기반 서비스에서 이용 가능
	카카오페이	카카오페이 인증서	• 메신저 '카카오톡'과 연동 • 금융회사(보험·증권·카드 등), 금융유관기관, 정부, 공공기관 등 200개 이상 기관에 도입
통신사	이동통신 3사	PASS 인증서	• 인증서 발급 및 이용 시 실시간 전화번호·명의자·단말 인증 수행 • 금융회사(은행·보험·증권 등), 나이스 대국민서비스 등에 도입

2. 전망 및 시사점

금융권은 인증수단을 단순 보안 목적이 아닌 신규 사업 기회로 인식

금융회사는 자사 인증수단 활성화를 통해 고객 잠금 효과(Lock-in effect)<sup>19)</sup>를 기대하며, 비금융회사는 금융산업 진출을 위한 초석으로 인증수단 활용 가능 이에, 금융회사는 자사 인증서의 개발 및 확대에 보다 집중할 것으로 보이며, 통신사 등의 금융권 인증시장 진입 시도는 더욱 활발할 전망

보안성이 전제된 인증수단의 다양성 존중 필요

공인인증제도 폐지로 민간 중심의 다양한 인증수단이 도입되어 금융소비자의 선택폭이 확대되고 편리성이 제고될 것으로 기대

다만, 금융은 타 산업과는 달리 높은 수준의 신뢰성·안전성이 요구되는 바, 보다 높은 수준의 보안성 요구나 거래 리스크별 인증수단 차등화 등 보안성 확보 조치가 요구

18) 참고 : 금융결제원 보도자료('20.11.17.), KB국민은행 보도자료('20.11.4.), IBK기업은행 보도자료('19.5.21.), 네이버 보도자료 ('20.5.22., 9.26.), 카카오페이 인증서 공식 홈페이지, PASS인증서 소개서('20.9월)

19) 잠금 효과(Lock-in effect) : 특정 상품·서비스 사용 시 전환비용이 매우 커서 다른 상품·서비스로 쉽게 갈아타기 어려운 현상을 의미

## 06. 금융의 신성장 동력, 데이터 산업 경쟁 본격화

**키워드 정의** **데이터(Data)** : 디지털 금융에서 새로운 가치 창출 등을 위한 핵심 자원으로, 다수의 참여자가 동시에 사용 가능한 '비경합성(non-rival)' 특징과 사용해도 양이나 가치가 감소되지 않는 '비소모성(non-depletable)' 특징<sup>20)</sup>을 보유

### 1. 금융권 데이터 산업 활성화를 위한 제도 및 인프라 구축 이슈 분석

신용정보법 개정('20.8.5.시행)으로 개인신용정보의 가명·익명처리나 데이터 간 결합이 가능해지는 등 데이터 활용의 제도적 기반이 마련

#### 가명·익명처리 및 데이터 결합 내용

구분	내용
가명처리	· 추가 정보 없이는 특정 개인을 알아볼 수 없도록 처리하는 것으로, 통계 작성·연구 등의 목적에 한하여 정보주체 동의 없이 활용 가능
익명처리	· 특정 개인을 알아볼 수 없도록 처리하는 것으로, 익명 처리 시 개인정보가 아니므로 목적 제한 없이 자유롭게 활용 가능
데이터 결합	· 데이터전문기관(금융보안원·신용정보원)을 통해 금융, 통신 등의 데이터 간 결합 가능 * (예) 카드사의 카드 이용 정보(온·오프라인 이용업종·장소·시점 등) + 택배사의 배송 정보(온라인 소비 품목 등) 간 결합 → 온·오프라인 소비행태 분석 가능

[참고] 금융위원회 보도자료('20.8.7.) 등

금융 빅데이터 개방시스템(CreDB)\* 등을 통해 금융데이터를 개방하고, 금융데이터거래소를 출범(20.5월)하여 데이터 거래의 활성화를 지원

\* 한국신용정보원에 축적되는 금융거래(대출, 연체 등) 정보를 비식별 조치하여 제공

### 마이데이터 등 금융권 데이터 산업 주도권 확보를 위한 경쟁이 시작

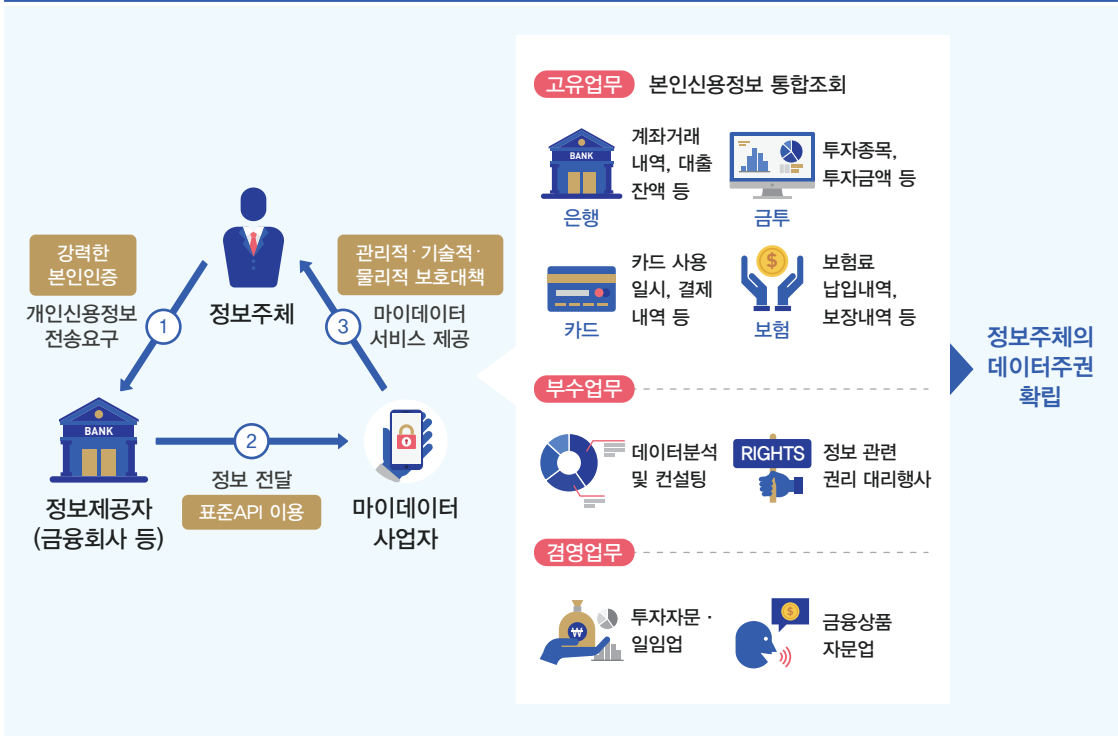
개인신용정보 전송요구권\*을 기반으로 신용정보 통합조회 등을 제공하는 본인신용정보관리업(마이데이터) 도입이 금융당국 주도로 추진

\* 본인의 개인신용정보를 본인 또는 특정 기관으로 전송하도록 요구할 수 있는 권리

마이데이터는 데이터를 통한 부가가치 창출이 용이하고 고객 잠금 효과(Lock-in effect)<sup>21)</sup>도 있어 금융회사·빅테크·핀테크 기업 등의 초기 시장 선점 경쟁이 활발\*

\* 금융분야 마이데이터 허가 수요조사 결과 116개 회사(금융회사 55개사, IT 회사 등 비금융회사 41개사, 핀테크 20개사)가 참여를 희망 (출처 : 금융위원회)

마이데이터(MyData) 산업



2. 전망 및 시사점

21년은 금융권 데이터 산업 무한 경쟁의 원년이 될 전망

금융권은 유통·통신 등 이종 산업과의 데이터 협업, 데이터 전담조직 신설 등 데이터 산업 경쟁에서 살아남기 위해 역량을 집중<sup>20)</sup>

금융회사, 빅·핀테크 기업은 대량의 데이터 보유, 우수한 개발 역량 등 자사의 여건과 장점에 맞는 다양한 금융데이터 산업을 추진할 전망

데이터 산업의 성공을 위해서는 보안성 확보가 필수

데이터의 활용 확대로 다양한 부가가치 창출이 가능한 반면 이를 타겟으로 한 보안 위협도 지속 확대될 전망

※ 특히, 마이데이터 사업자는 개인의 금융데이터가 집중되므로 주요 공격 대상이 될 우려

안전하지 않은 인증이나 취약점 등으로 금융데이터 유출 사고가 발생할 경우 금융소비자 피해는 물론 금융데이터 산업 전반의 신뢰성 저하가 우려되므로 철저한 보안 관리 및 프라이버시 강화 조치가 선행될 필요

20) 참고 : 「Data Economy: Radical transformation or dystopia?」 (UN DESA, '19.1월)

21) 잠금 효과(Lock-in effect) : 특정 상품·서비스 사용 시 전환 비용이 커져 다른 상품·서비스로 쉽게 갈아타기 어려운 현상을 의미

22) (예시) 온라인 쇼핑물과의 제휴를 통한 데이터 기반 서비스 개발, 통신사와 협업하여 금융·통신을 결합한 마이데이터 사업 추진, 마이데이터 산업 전담조직 신설 등

## 07. 금융 산업의 개방, 다양한 플레이어의 등장

**키워드 정의** **플레이어(Player)** : 본 보고서에서는 '금융산업에 진출한 경제주체'를 의미하며, 은행 등 기존 금융회사뿐만 아니라 빅테크 기업, 핀테크 기업 등을 포괄

### 1. 이슈 분석

#### 금융 산업 개방에 따른 플레이어 확대 및 다변화

오픈뱅킹 등 지급결제망 개방, 간편결제를 중심으로 한 빅테크의 금융 산업 진출 확대 등으로 금융 산업 플레이어가 확대되는 추세

금융당국은 「전자금융거래법」 개정(20.11.27 법안 발의)을 통해 소규모 기업도 진입 가능한 지급지시전달업(MyPayment) 및 모든 전자금융업을 영위할 수 있는 종합지급결제업 신설도 추진 중

#### 금융 산업 개방 추진 현황<sup>23)</sup>

구분	내용
오픈뱅킹	· 특정 금융회사의 서비스를 응용프로그래밍인터페이스(API)를 통해 개방하여 타 금융회사 등도 이를 활용한 서비스를 개발할 수 있는 개방형 금융결제망 → 하나의 앱으로 모든 은행 계좌 조회·이체 가능
마이데이터(MyData)	· 개인신용정보 전송요구권을 기반으로 본인의 정보를 제3의 업체에 전달하여 새로운 부가 서비스를 개발하는 사업 → 본인 정보의 일괄 조회·관리나 맞춤형 금융상품 추천 등 신규 서비스 제공이 가능
지급지시전달업(MyPayment)	· 금융소비자의 지급 지시(결제·송금 등)를 금융회사 등에 전달하여 이를 이행하도록 지원하는 사업(추진 중) → 금융소비자 자금을 보유하지 않아도 결제·송금 서비스 등을 제공할 수 있어 소규모 기업도 진입 가능
종합지급결제업	· 계좌를 기반으로 자금이체, 대금결제, 결제대행 등 모든 전자금융 서비스를 제공할 수 있는 플랫폼 사업으로 여·수신 업무는 제한(추진 중) → 계좌 개설이 가능한 대신 자기자본 등 지정 요건이 강하므로 빅테크 기업 중심으로 참여가 예상

#### 각 플레이어는 협력 등의 방식으로 경쟁력 확보를 위해 노력

**(금융회사)** 금융그룹사 통합 플랫폼 구축, 빅·핀테크 기업 또는 타 산업(유통·통신 등)과의 협력 등을 통해 자사 금융상품 및 서비스를 고도화

**(빅테크 기업)** 수많은 고객과 접근성을 갖춘 비금융 플랫폼(포털, SNS 등)을 기반으로 기존 금융회사와 제휴하거나 금융업에 직접 진출

**(핀테크 기업)** 혁신적 아이디어를 바탕으로 새로운 금융 서비스를 제공하거나, 타 금융회사의 상품을 비교·추천하는 서비스 등을 개발



**금융회사, 빅·핀테크 기업의 경쟁력 확보 방안(예시)<sup>24)</sup>**

구분	내용
<p><b>금융회사</b></p> <p>은행, 카드사, 증권사, 보험사 등 전통적 금융회사</p>	<ul style="list-style-type: none"> <li>그룹사 통합 플랫폼 구축 등 그룹사 내 협력 강화 (예) 신한금융 '신한플러스' - 별도의 모바일 앱 없이 은행, 카드, 금투, 생명 등의 서비스 이용 가능</li> <li>빅·핀테크 기업 또는 타 산업과 협력 (예) 우리은행 - 편의점 '세븐일레븐'과 업무협약을 체결하여 가맹 경영주에게 저금리 대출을 지원하고 맞춤형 금융상품 개발 및 빅데이터 기반 공동 마케팅 등을 추진</li> </ul>
<p><b>빅테크</b></p> <p>주력 사업인 포털, SNS 등 비금융 플랫폼을 기반으로 금융서비스를 제공</p>	<ul style="list-style-type: none"> <li>기존 금융회사와 제휴 (예) 네이버 - 미래에셋캐피탈과 함께 네이버 스마트스토어 사업자 대상 대출 실시</li> <li>금융업에 직접 진출 (예) 카카오 - 인터넷전문은행 '카카오뱅크' 및 증권사 '카카오페이증권' 설립</li> </ul>
<p><b>핀테크 기업</b></p> <p>IT 기술을 활용하여 혁신적 금융서비스를 제공</p>	<ul style="list-style-type: none"> <li>혁신적 아이디어 기반의 다양한 금융 서비스 제공 (예) NHN페이코 - 결제, 송금, 계좌·카드 조회, 신용 관리, 환전, 쇼핑 적립, 교통카드 등 금융서비스 제공</li> <li>금융상품 비교·추천 또는 중개 서비스 제공 (예) 핑크 - 금융회사의 대출상품 비교 서비스 및 맞춤형 보험 추천 서비스 등 제공</li> </ul>

**2. 전망 및 시사점**

**Open Finance 속 금융권 혁신과 상호 경쟁은 가속화될 전망**

금융 산업 개방 본격화로 오픈뱅킹, 마이데이터, 지급지시전달업 등의 활성화 뿐만 아니라 각 서비스 간 연계를 통한 혁신적 금융 서비스가 다수 등장할 전망

금융회사와 빅·핀테크 기업 간 경쟁이 가속화되는 상황 속에서 모두가 공정하게 경쟁할 수 있는 법적·제도적 환경 마련이 선행될 필요

**금융권 보안 리스크의 상호연계성 확대를 경계할 필요**

타 기업과의 경쟁을 위한 금융회사 등의 전략적 협력이 확대됨에 따라 협력기업의 보안 취약점이 금융회사의 취약점으로 전이될 수 있는 위험이 존재

협력기업에 보안사고 발생 시 연계된 금융회사도 책임으로부터 완전히 자유로울 수 없고 평판리스크 등도 야기될 수 있으므로 협력기업의 보안 리스크를 면밀히 고려할 필요

23) 참고 : 금융위원회 보도자료('20.7.24., 10.21.), 전자금융거래법 일부개정법률안('20.11.27.) 등

24) 참고 : 신한금융지주회사 보도자료('18.8.13.), 카카오페이 보도자료('20.2.6.), 해당 기관 홈페이지 및 언론 기사 등

## 08. 지갑이 휴대폰 속에? 지갑 없는 사회의 시작

**키워드 정의**    **지갑 없는 사회** : 지급수단(현금, 신용카드 등)이나 신분증 등을 실물 지갑에 가지고 다닐 필요 없이 스마트폰만으로 결제나 신분증명이 가능한 사회를 의미

### 1. 이슈 분석

#### 세계 각국에서 중앙은행 디지털 화폐(CBDC) 발행 논의를 시작

페이스북의 디지털 화폐 발행 추진<sup>25)</sup>, 현금 이용 감소 등을 계기로 중앙은행이 발행하는 전자적 형태의 디지털 화폐(CBDC, Central Bank Digital Currency)에 대한 논의가 본격화\*

\* 66개국 중앙은행 중 CBDC 관련 업무를 수행 중인 곳은 19년 기준 전체의 약 80% 수준  
(출처 : 국제결제은행)

중국이 CBDC 도입에 가장 적극적\*이며, 국내의 경우 한국은행에서 CBDC 관련 기술·법률 검토 및 파일럿 테스트를 추진 중

\* 중국은 민간 지급결제사업자(위챗·알리페이)에 대한 의존 완화, 위안화의 국제화 등을 목표로 일부 도시 대상의 '디지털 위안화(CBDC)' 시범 테스트를 진행 중

#### CBDC 분류<sup>26)</sup>

기준	분류	특징
이용 목적 (이용 주체)	소액 결제용 (general-purpose)	· 모든 경제 주체의 일반적인 거래에 사용
	거액 결제용 (wholesale only)	· 은행 등 금융회사 간 거래에 사용
구현 방식	단일원장 방식 (계좌기반)	· 중앙관리자(예 : 중앙은행)가 CBDC 계좌 및 관련 거래 정보를 보관·관리
	분산원장 방식 (토큰기반)	· 다수의 참가자가 상호 동기화된 원장을 가지고 동일한 거래 기록을 관리

#### 간편결제의 대중화 및 모바일 신분증 도입 추진

온라인 간편결제의 활용이 일상화되었으며, 오프라인 매장에서 실물 카드 없이 스마트폰으로 결제하는 오프라인 간편결제도 활성화 추세

25) 페이스북은 디지털 화폐 '리브라(Libra)'(현 '디엠') 출시 계획을 발표('19.6월)하였으나, 각국 정부 및 중앙은행의 반대와 주요 참여사의 탈퇴로 현재 달러화에 가치를 고정한 스테이블 코인 출시를 추진 중

26) 참고 : 한국은행 「중앙은행 디지털 화폐」('19.1월)

### 오프라인 간편결제 서비스 현황(예시)

서비스 제공자	서비스 특징
모바일기기 제조회사	· 자사 모바일 기기에 제휴된 금융회사의 신용카드나 계좌 등을 등록하여 실물 카드 없이 결제 (예) 삼성페이, LG페이 등
카드사	· 자사의 신용(체크)카드 정보를 모바일 앱에 등록하여 실물 카드 없이 모바일 기기로 결제할 수 있는 '앱카드 결제' 서비스 제공
빅테크	· 자사 플랫폼(포털, SNS 등)에 지급수단을 등록하거나 선불금을 충전하고, 바코드 또는 QR코드 등을 활용하여 오프라인 결제 (예) 네이버페이, 카카오페이 등

행정안전부는 모바일 신분증 도입을 추진 중\*이며, 경찰청·이동통신 3사 등은 모바일 운전면허 확인 서비스\*\*를 출시('20.7월)

\* 21년 모바일 공무원증 도입을 시작으로 운전면허증, 장애인등록증 등으로 확대할 계획

\*\* 이동통신3사의 본인인증 앱 '패스(PASS)'에 실물 운전면허증을 등록한 후 사용  
(국제운전면허증 발급 시 신원확인, 편의점에서 성인 여부 확인 등에 활용)

## 2. 전망 및 시사점

### '지갑 없는 사회'로의 전환이 가속화될 전망

국내 CBDC의 도입까지는 장기간의 검토가 필요할 것으로 보이나, 디지털 화폐에 대한 관심은 지속될 것으로 예상<sup>27)</sup>

신분증, 자격증, 각종 증명서 등을 전자적으로 발급·저장하는 서비스가 출시되어 비대면 실명확인이나 각종 증빙서류 제출 작업 등이 간소화될 전망

※ (예시) 계좌개설 시 모바일 신분증을 통한 신원확인, 대출 시 모바일 기기에 저장한 재직증명서 등 서류를 전자적으로 제출 등

### 보안 등 각종 리스크에 철저히 대비할 필요

CBDC 등 디지털 화폐와 관련된 프라이버시 이슈나 분산원장기술 활용에 따른 운영리스크\* 등도 발생할 수 있으므로 사전에 철저한 검증 및 대비가 요구

\* 분산원장 처리 속도 한계 등에 의한 가용성 저하, 이중 지불과 같은 비정상 거래 발생 등

실물 지갑을 대체하는 모바일 기기의 물리적 도난이나 악성 모바일 앱(app) 유포 등과 같은 사이버 공격에도 주의할 필요

27) (예시) 글로벌 간편결제 업체 '페이팔(Paypal)'은 가상통화의 구매·보유·판매 서비스를 출시('20.10월)하였으며, 비자(Visa)는 미국 달러화와 연동된 스테이블 코인(USDC) 결제 지원을 추진 중

# 09. 책임 있는 AI를 위한 금융권 노력, AI 거버넌스 구축

**키워드 정의**    **책임 있는 AI(Responsible AI)** : 윤리, 신뢰, 공정성, 투명성, 설명 가능성, 안전성, 프라이버시 및 컴플라이언스 등의 측면에서 옳바르다고 판단되는 AI

**AI 거버넌스(AI Governance)** : AI 위험 통제를 위한 기업 내부 관리 체계로, AI 전담 조직 및 의사결정 체계, AI 기준 및 내규·절차, AI 알고리즘 및 데이터 관리, AI 위험관리, AI 감사 및 평가 등을 포괄

## 1.

### 이슈 분석

#### AI 활용 확대에 따른 AI 위험(부작용) 우려가 제기

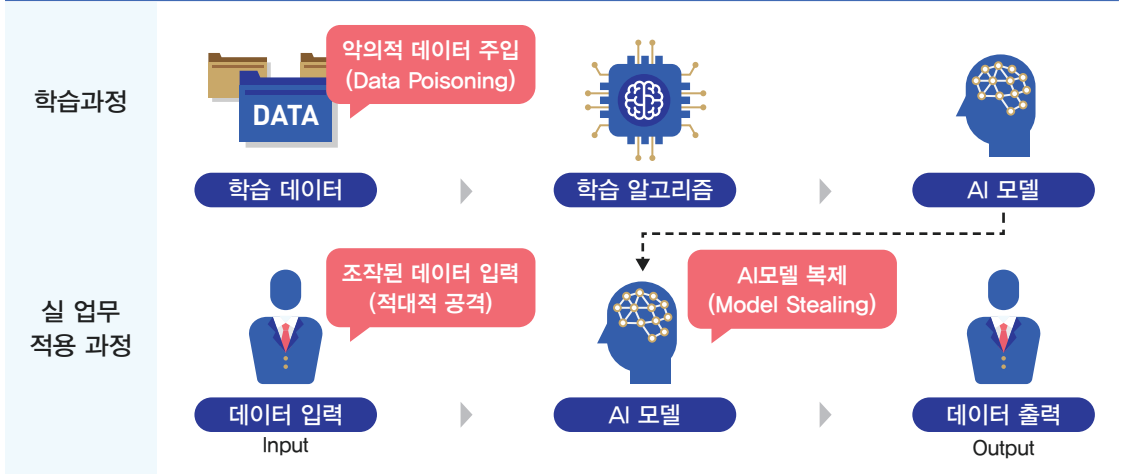
**(AI 편향)** AI가 특정 집단에 불리한 의사결정을 내리는 등 사회적·윤리적 가치에 반한 차별적 결과를 도출하여 금융소비자 피해를 유발

※ AI 편향 발생 원인 : ①학습 데이터에 사회적 편견이 반영, ②특정 집단의 학습 데이터가 불충분, ③학습 데이터가 악의적으로 조작 등

**(AI 불투명성)** 내부 처리 과정을 알 수 없는 AI 특성상 도출된 결과의 원인 등을 설명하기 어려워 AI 공정성<sup>28)</sup>에 대한 금융소비자 불신이 가중

**(AI 보안 위협)** 적대적 공격<sup>29)</sup> 등 AI의 취약점을 악용한 보안 위협 우려

#### AI 보안 위협



[참고] ISO 24028 : 2020




28) 기업 간 동일한 AI 알고리즘 사용 등을 통해 가격을 담합하는 '디지털 카르텔'은 AI의 공정성을 저해

29) 적대적 공격(Adversarial attacks) : AI가 정확한 판단을 할 수 없도록 조작된 입력데이터를 주입하여 오작동을 유발하는 공격

## 해외 각국은 AI 위험 최소화를 위한 각종 정책을 마련하여 시행

미국, EU 등 해외 주요국은 AI 활용 원칙뿐만 아니라 가이드 등 구체적인 AI 정책도 지속적으로 발표

### 해외 주요국의 최신 AI 정책 내역

국가명	AI 정책명
 미국	• 백악관 「AI 규제원칙」 (20.1월), 뉴욕시 「의사결정 시스템 규정」 (19.11월), 연방거래위원회 「AI 이용 지침」 (20.4월), 미국 의회 「알고리즘 책임법」 (19.4월 발의) 등
 EU	• EU 집행위 「디지털시대 AI 전략」 (20.2월), EU 집행위 「신뢰할 수 있는 AI 자체평가」 (20.7월), EU 의회 「자동화된 의사결정 결의안」 (20.1월 승인), EU 은행청 「빅데이터 고급분석 보고서」 (20.1월) 등
 영국	• 정보위원회 「AI 및 데이터보호 가이드」 (20.8월), 정보위원회 「AI 의사결정 규제지침」 (20.5월), 정보위원회 「AI 감사 프레임워크」 (20.2월) 등

국내는 한국판 뉴딜의 일환으로 AI 활용·융합을 가속화하는 디지털 뉴딜을 추진하고 있으며, 금융권도 AI 활성화 정책 마련을 추진 중<sup>30)</sup>

## 2. 전망 및 시사점

### 금융권의 AI 서비스 도입 확대 및 AI 위험 현실화

로보어드바이저, 챗봇 위주였던 금융권의 AI 도입이 빅데이터와 연계하여 신용평가, 지급 결제, 정보 보안 등으로 점차 확대될 전망<sup>31)</sup>

금융권의 AI 서비스 확대에 따라 AI 편향이나 금융소비자의 설명 요구권 행사<sup>32)</sup>, AI 취약점 등 AI 위험 이슈가 현실화될 것으로 예상

### AI 위험 최소화 및 책임 있는 AI를 위해 AI 거버넌스 구축이 선결

AI 편향 완화나 설명 가능한 AI(XAI : eXplainable AI) 기술에 대한 연구가 국내외에서 진행되고 있으나, 아직 초기 단계로 가시적 성과가 미비

해외 주요국도 이러한 어려움을 인지하고 기업 내 AI 위험통제 체계인 AI 거버넌스 확립을 최우선 정책 과제로 강조

국내 금융권도 책임 있는 AI 구축을 위해 AI 전담 조직 구성, AI 내규 및 사내 감사 절차 마련 등 AI 거버넌스 확립에 주력할 필요

30) 금융위원회는 금융분야 AI 활성화를 위한 워킹그룹을 구성(20.7월)하여 운영 중

31) '20.11월 금융회사 대상 자체 조사 결과(금융보안원 주관, 복수 응답, 194개 기관 대상). AI 도입(또는 예정) 업무 분야는 ①고객데이터 분석(21%), ②정보보안(15%), ③이상금융거래탐지시스템(12%) 등으로 파악

32) 금융권은 신용정보법 제36조의2(자동화평가 결과에 대한 설명 및 이의제기 등)에 의거 금융소비자가 금융회사에 AI 도출 결과에 대한 설명을 요구할 수 있는 권리를 보장





## 해외 금융보안 규제 강화로 국내 금융회사가 규제 리스크에 직면

해외 주요국도 디지털금융으로의 전환이 빠르게 진행되고 있어 금융보안에 대한 규제가 점차 강화되는 추세

각 국가별 준수해야 할 금융보안 규제가 다양하고 규제 변화도 빠르게 진행되고 있어 국내 금융회사도 규제 미 준수 리스크에 노출

※ 국가별로 규제 당국(국가·지역), 규제 범위(전체 업권·개별 업권), 규제 성격(의무·자율)이 다양

### 중국 및 베트남의 주요 금융보안 규제 현황

국가	구분	내용
 중국	개인정보 보호법(안)	· 중국 국민의 개인정보 처리 시 의무사항 및 개인 프라이버시 관련 권리를 규정하고 위반 시 강력한 처벌*을 부과 * 전년도 매출액의 5% 또는 한화 약 84억 원의 벌금 부과 등
	금융소비자 권익 보호방안	· 금융 상품 및 서비스 제공 시 금융소비자 권리를 보장하고 정보보호 대책을 준수하도록 규정
	앱 개인정보 불법 수집 규제	· 모바일 앱(App) 서비스에서 개인정보 수집·활용 시 필요한 요건 및 앱을 통한 푸시(Push) 거부권 보장 등을 명시
 베트남	사이버보안법 2018	· 인터넷 서비스 제공 기업이나 이를 이용하는 개인의 사이버 보안 관련 의무사항을 명시
	은행 업무에 대한 정보시스템 보안규정	· 금융회사 등의 사이버보안 관련 구체적인 준수 사항을 규정(우리나라의 「전자금융감독규정」과 유사) · 정보시스템 중요도에 따라 보안 수준을 차등 적용한 것이 특징
	금융기관의 고객 정보 제공에 관한 시행령	· 금융회사 등이 보관하고 있는 고객 정보에 관한 사항을 규정 · 고객 정보의 외부 제공 금지, 고객 정보 보호 및 정보제공에 관한 내부 규정 수립·시행 등이 명시

## 2. 전망 및 시사점

### 디지털 금융시장을 중심으로 국내 금융회사의 해외 진출 확대

코로나19로 국가·지역 간 이동이 어려운 상황과 맞물려 해외 금융권의 비대면, 디지털 전환은 더욱 가속화될 것으로 예상

※ 일부 신흥국은 전통적인 금융산업 발전 단계를 건너뛰고 디지털금융을 적극 도입

국내 금융회사는 디지털금융에 대한 다양한 노하우 및 기술을 보유하고 있어 해외 디지털금융 시장 공략에 보다 적극적으로 나설 필요

### 해외 진출 시 금융보안 컴플라이언스에 대한 이해 및 준수가 필수

해외에 진출한(또는 진출을 계획 중인) 국내 금융회사가 점차 강화되는 해외 금융보안 규제에 대응하기 위해서는 글로벌 정보보호 관리체계 수립, 전담조직 신설, 전문 인력 양성 등이 중요

금융보안원은 국내 금융회사 등이 준수해야 할 해외 금융보안 규제를 조사·분석 하여 시의성 있게 제공하는 등 금융권의 글로벌 컴플라이언스 업무를 적극 지원할 계획

# 2021 디지털금융 및 사이버보안 이슈 전망

