

DIGITAL

2022 Digital Finance & Cyber Security

디지털금융 및 사이버보안 이슈 전망

6. 디지털자산 확산에 대한 기대와 우려
7. 금융 메타버스, 현실세계와 가상세계의 융합

1. 사이버공격의 대유행, 디지털 팬데믹

2. 디지털 전환 시대, 새로운 금융보안 규제

5. 금융안정을 위협하는 제3자 리스크, 강조되는 운영복원력의 확보

8. 업무 자동화 확산에 따른 리스크 증가

9. 데이터 무한 경쟁 시대 개막과 데이터 양극화

4. 제로 트러스트 전략에 따른 차세대 보안환경 확산

3. 디지털 전환의 필수재로 오픈소스, 그 이면에 감춰진 리스크

10. 멀티플랫폼으로 진화하는 금융서비스와 보안위협

Digital Finance & Cyber Security **2022**

디지털금융 및 사이버보안 이슈 전망



01



사이버공격의 대유행,
디지털 팬데믹

02



디지털 전환 시대,
새로운 금융보안 규제

03



디지털 전환의 필수재료 오픈소스,
그 이면에 감춰진 리스크

04



제로 트러스트 전략에 따른
차세대 보안환경 확산

05



금융안정을 위협하는 제3자 리스크,
강조되는 운영복원력의 확보

06



디지털자산 확산에 대한
기대와 우려

Digital Finance & Cyber Security

2022

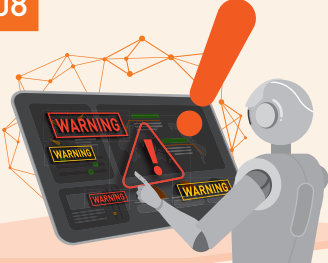
디지털금융 및 사이버보안 이슈 전망

07



금융 메타버스,
현실세계와 가상세계의 융합

08



업무 자동화 확산에 따른
리스크 증가

09



데이터 무한 경쟁 시대 개막과
데이터 양극화

10



멀티플랫폼으로 진화하는
금융서비스와 보안위협

Contents

01	사이버공격의 대유행, 디지털 팬데믹	1
02	디지털 전환 시대, 새로운 금융보안 규제	3
03	디지털 전환의 필수재료 오픈소스 , 그 이면에 감춰진 리스크	5
04	제로 트러스트 전략 에 따른 차세대 보안환경 확산	7
05	금융안정을 위협하는 제3자 리스크 , 강조되는 운영복원력 의 확보	9
06	디지털자산 확산에 대한 기대와 우려	11
07	금융 메타버스 , 현실세계와 가상세계의 융합	13
08	업무 자동화 확산에 따른 리스크 증가	15
09	데이터 무한 경쟁 시대 개막과 데이터 양극화	17
10	멀티플랫폼 으로 진화하는 금융서비스와 보안위협	19

01

사이버공격의 대유행, 디지털 팬데믹

전 세계를 강타한 '코로나19 팬데믹(Pandemic, 세계적 대유행)'에 이어, 랜섬웨어 등 사이버공격에 의한 "디지털 팬데믹(Digital Pandemic)"과 그로 인한 금융위기 발생에 대한 우려가 증가하고 있어 금융업권의 전방위적 준비와 대응이 필요

1 이슈 분석

● 사이버공격의 전 세계적 대유행 '디지털 팬데믹(Digital Pandemic)' 우려

코로나19 유행과 비대면 문화의 확산으로 디지털 전환이 가속화되며, 전 산업 분야에서 IT 의존도가 증가하고 사이버공격 대상도 크게 확대

가상자산의 활성화¹⁾, 공격의 비즈니스화²⁾ 등에 따라 증가하는 랜섬웨어 및 국가 지원 대규모 사이버공격 등에 의한 디지털 팬데믹 우려

● 랜섬웨어의 고도화 및 국가 지원 공격그룹의 활동 지속³⁾

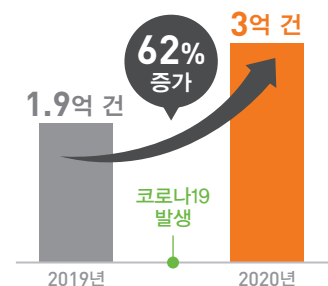
랜섬웨어 공격 대상이 개인에서 주요 인프라 또는 대기업으로 확대되고, 다중협박⁴⁾, APT 또는 공급망 공격과의 결합 등 공격 수법이 고도화

세계 랜섬웨어 공격 동향

최근 공격 사례

피해 업체	발생일자	내용
IT관리용SW 제공업체 'K사'	'21.7월	러시아 랜섬웨어 그룹 Revil은 미국 K사의 VSA 솔루션(원격 모니터링·관리 솔루션)을 랜섬웨어 유포경로로 악용, 대규모 공급망 공격을 수행
송유관 업체 'C사'	'21.5월	랜섬웨어 그룹 Darkside의 공격을 받은 미국 송유관 업체 C사의 유류 공급 중단으로 미 정부는 지역 비상사태를 선언

전 세계 피해 현황



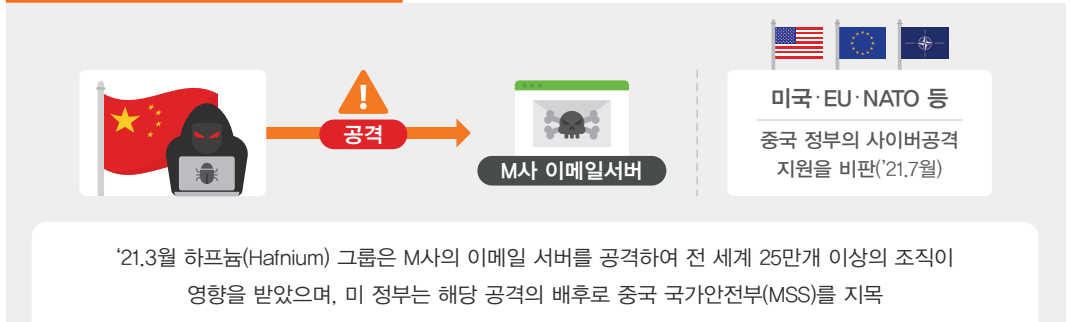
출처 : 관련 언론 보도

출처 : 과학기술정보통신부

국가기밀·핵심기술 등의 탈취, 금전적 이득, 지정학적 힘 행사⁵⁾, 첩보활동 등을 위해 특정 국가의 지원이 의심되는 사이버공격 사례도 일부 존재

- 1) 파이어아이 CEO Kevin Mandia는 랜섬웨어 공격 증가 추이와 가상자산의 상승세가 일치한다고 주장 (CNBC, '21.6월)
- 2) 해커가 제작하여 공격자에게 판매한 후 수익을 배분하는 형태의 '서비스형 랜섬웨어(RaaS)'가 증가하고, 랜섬웨어 공격그룹이 조직화·분업화되는 상황
- 3) 국가정보원은 랜섬웨어 공격, 국가배후 해킹조직의 외교·안보·언론 분야 정보 절취 시도 등을 이유로, 국가공공기관 사이버위기 경보단계를 '21.8월 '관심'으로 상향한 후 유지 중('21.10월 기준)
- 4) 랜섬웨어는 데이터 암호화를 빌미로 금전을 요구하는 악성코드였으나, 최근에는 데이터 유출, 디도스 공격, 고객 또는 이해관계자에 통보 등 위협이 다변화되는 추세
- 5) Forbes는 랜섬웨어가 지정학적 힘을 행사하기 위한 도구로 사용될 수 있으므로, 특정 국가가 일부 랜섬웨어 공격그룹을 지원하는 것으로 파악된다고 보도('21.8월)

국가 지원 사이버공격 의심 사례



출처 : 관련 언론보도

2 전망 및 대응전략

● 파급력이 큰 사이버공격이 새로운 금융위기를 유발할 가능성⁶⁾

사이버공격으로 인한 주요 금융회사 또는 금융 인프라의 장기간 중단 등은 금융시스템 전체에 대한 신뢰 하락 및 리스크 확대로 이어져 금융안정에까지 영향을 줄 우려

사이버보안 및 금융안정성 간 인과관계



출처 : IMF 「Cyber Risk and Financial Stability」 (’20.12월) 참고 및 재구성

● 사이버리스크의 확산 방지를 위한 금융업권의 전방위적 대응 필요

금융회사는 사이버공격의 예방 역량과 더불어, 공격 발생 시 리스크 확산 방지를 위한 신속한 복구 능력을 확보하는 것이 급선무

아울러, 사이버리스크의 시스템적 확산을 최소화하기 위해서는 정부(금융당국), 금융회사, 관련 기관 간 신속한 정보 공유 등 긴밀한 협력 체계 운영이 중요⁷⁾

6) 금융안정위원회(FSB), 국제통화기금(IMF), 유럽중앙은행(ECB) 등은 '사이버공격이 금융안정성을 위협할 것'이라고 경고하였으며
美 FBI 국장은 '랜섬웨어 공격이 9.11테러와 유사하다'고 언급 (참고 : IMF 「The Global Cyber Threat」(’21.3월), The New York Times (’21.6월) 등)

7) 국가정보원은 국가배후 해킹조직 관련 정보를 국가·공공기관뿐만 아니라 민간 부문에도 지원하고 있다고 밝히며, 정부·민간 협력 및 유사입장국 간의 국제공조를 강조 (아주경제, ’21.10월)

금융의 디지털 전환 가속화에 따라 글로벌 금융보안 규제도 디지털·IT·운영 리스크 관리를 중심으로 변화 중. 국내에서도 금융보안 7대 원칙 등의 내용을 담은 「전자금융거래법」 개정이 추진되고 있어 적극적인 대비가 필요

1 이슈 분석

• 디지털금융에 적합한 규제체계 마련을 위한 각국의 움직임

인공지능·블록체인·클라우드 등 신기술의 적극적 도입, 금융시스템의 개방(오픈뱅킹) 등으로 금융의 디지털 전환이 가속화

EU·영국·싱가포르 등 해외 주요국은 디지털금융에 더욱 적합한 규제체계 마련을 위해 금융보안 등 관련 법·제도 정비⁸⁾를 지속

국가별 디지털금융 규제 제·개정 현황

구분	내용
 EU	<ul style="list-style-type: none"> · 「지급결제산업지침」 (Payment Services Directive2, '19.9월 발효) · 「디지털운영복원법(안)」 (Digital Operational Resilience Act, '20.8월 발표)
 영국	<ul style="list-style-type: none"> · 「운영복원력 및 제3자 리스크 관리 정책*」 ('22.3월 시행 예정) <p>* (원문명) Operational Resilience : Impact Tolerances for Important Business Services, Outsourcing and Third Party Risk Management</p>
 싱가포르	<ul style="list-style-type: none"> · 「사이버위생 규정」 (Notice on Cyber Hygiene, '20.8월 발효) · 「기술위험관리 규정」 (Notice on Technology Risk Management, '21.1월 발효)

• 금융보안 원칙 등이 담긴 국내 「전자금융거래법」 개정 추진

전자금융거래법 개정안(김병욱 의원 발의, '21.11월)은 리스크에 비례한 자율적 보안을 위해 원칙 중심의 규제 (Principles-based regulation)를 선언하고,

금융보안 거버넌스 확립을 위한 이사회의 책무, 금융보안계획 수립·제출 의무, 금융보안 규제 개선·합리화를 위한 금융보안 상시평가제 도입, IT아웃소싱 규제 강화 등의 내용을 포함



8) 각국의 최근 금융보안 규제는 경영진(이사회)의 최종책임, IT 제3자 리스크 관리 및 운영복원력·탄력성 확보를 강조하는 추세

2 전망 및 대응전략

• 금융보안 원칙 중심의 자율적 금융보안 역량 강화 필요

법 개정안이 원칙·리스크를 중심으로 한 자율적인 금융보안 강화를 강조하고 있어 법 개정 시 하위 법규에도 많은 변화가 예상 (현행 금융보안 규제는 사전에 정의된 일률적이고 세세한 통제항목 중심)

금융보안 7대 원칙을 중심으로 금융회사 스스로 리스크를 평가하고 적합한 금융보안 대책을 설계·실행·개선해 나가는 역량을 확보할 필요

금융보안 7대 원칙별 향후 전략

AS IS	TO BE(향후 전략)
원칙 ① 기밀성·무결성·가용성 확보	
규제 준수(컴플라이언스)에 초점	리스크 평가를 기반으로 필요한 통제를 스스로 마련
원칙 ② 업무지속성(회복성) 유지	
IT시스템 장애·사고의 신속한 복구에 중점	주요 업무를 지속할 수 있는 역량 (운영복원력) 확보에 집중
원칙 ③ 조직·임직원의 금융보안 관련 역할 명확화	
정보보호최고책임자·정보보호조직에 금융보안 역할이 집중	금융보안 관련 역할을 이사회·경영진을 포함한 전사 조직으로 확대
원칙 ④ 이사회의 금융보안에 대한 최종 책임성	
금융보안에 대한 최종 책임 소재가 불분명 (또는 CISO가 상응하는 권한은 없이 과도한 책임만 부담)	이사회가 금융보안 관련 주요 사항에 대해 최종 책임성을 가지고 의사결정
원칙 ⑤ 전사적인 금융보안 체계 확립	
IT·정보보호 시스템과 조직 중심의 보안 체계 운영	전사적으로 비즈니스와 연계한 보안 체계 확립·운영
원칙 ⑥ 정보 공유체계 구축	
금융회사 중심의 소극적·제한적 정보공유 체계 운영	금융회사, 전자금융업자 및 시스템운영자 등 이해관계자 전반이 적극적·자발적으로 정보공유체계에 참여
원칙 ⑦ 제3자 리스크 관리	
제3자로 인한 IT·보안 리스크 관리에 집중	제3자 이용에 따른 의존 리스크·집중 리스크 관리로 확대

디지털 전환 등 급변하는 환경에 신속하게 대응하기 위해 금융 분야에서도 오픈소스 활용이 폭넓게 확산 중. 오픈소스 활용 시 취약점을 최소화하는 동시에 라이선스 등의 문제가 발생하지 않도록 체계적으로 관리할 필요

1 이슈 분석

• 다양한 산업 분야에서 오픈소스를 적극적으로 활용

급변하는 산업환경 속 경쟁력 확보를 위해서는 서비스의 혁신을 통해 변화에 신속 대응하고 시장을 선점하는 것이 중요하므로, 새로운 기술의 손쉬운 활용과 신속하고 효율적인 개발을 위해 오픈소스를 활용하는 사례⁹⁾가 확산

Statista의 전망에 따르면 전 세계 오픈소스 시장 규모는 '17년 114억 달러에서 '22년 329억 달러로 5년간 약 3배 성장할 것으로 예상

* Open source services – worldwide revenue 2017–2022('19.9월)

• 누구나 접근·수정이 가능한 오픈소스의 보안 취약점

오픈소스는 누구나 소스 코드에 접근하여 수정할 수 있으므로 공격자가 임의로 악의적 코드를 추가¹⁰⁾하는 것도 이론적으로 가능하며, 공개된 소스 코드에서 취약점¹¹⁾을 찾아내어 악용할 가능성도 있음

오픈소스 라이선스 위반 소송에서 패소, 미국 SW업체에 약 23억 원을 지급한 국내 H사 사례에서 알 수 있듯 소스 코드가 공개된 경우라도 이를 활용·재배포할 때는 반드시 지켜야 할 라이선스 체계가 존재

주요 오픈소스 라이선스 종류 및 특징

라이선스 명	상업적 이용	소스 코드 공개	변경사항 고지	제약조건
MIT	가능	선택	선택	낮음
BSD	가능	선택	선택	낮음
Apache	가능	선택	의무	낮음
MPL	가능	의무(일부 예외)	선택	보통
LGPL	가능	의무(일부 예외)	의무	보통
GPL	가능	의무	의무	높음

9) 국내 모 인터넷은행은 오픈소스 기반의 저렴한 IT 인프라 구축 전략을 통해 약 1천억 원을 절감 (디지털데일리, '21.7월)

10) 공격자가 PHP 오픈소스 개발에 참여하여 백도어 공격 코드를 임의로 추가 (IT World, '21.4월)

11) 오픈소스 소프트웨어 취약점 상위 10가지 ① 리소스 누수 ② 초기화되지 않은 변수 ③ Null 포인터 역참조 ④ XSS ⑤ 메모리 손상 ⑥ 호출 시 추가인수 오류 ⑦ 에러처리 문제 ⑧ 안전하지 않은 데이터 처리 ⑨ 제어흐름 문제 ⑩ 고려되지 않은 예외 사항 (Synopsys, 2021 Open Source Security And Risk Analysis Report, '21.5월)

2 전망 및 대응전략

• 오픈소스 취약점을 최소화하기 위한 다각적인 노력 필요

오픈소스 취약점의 악용을 최소화하기 위해서는 우선 오픈소스 활용 정책·절차를 수립하고, 오픈소스 지원 서비스¹²⁾ 활용, 코드 보안성 검사¹³⁾, 주기적인 패치 등의 오픈소스 보안대책을 고려할 필요

주요 오픈소스 보안대책



• 오픈소스 라이선스에 대한 정확한 인식 필요

‘오픈소스 사용에는 제약이 없다’라는 부정확한 인식에서 벗어나, 사용 중인 오픈소스의 라이선스 체계를 정확히 파악할 필요

특히, 소스 코드 공개 의무가 있는 라이선스¹⁴⁾(GPL, LGPL, MPL 등)를 가진 오픈소스 활용 시 특히 유의할 필요가 있으며, 오픈소스 라이선스와 취약점을 일괄 분석하여 조치 사항을 자동 식별해주는 오픈소스 분석·점검 서비스(Software Composition Analysis) 활용 등도 검토해 볼 필요

오픈소스 분석 점검 서비스(예시)

서비스명	서비스 제공자	라이선스 분석	취약점 탐지	의존성 관리	정책 관리	비용
Code Eye	저작권위원회	O	X	X	X	무료
Olive Platform	카카오	O	X	O	X	무료
Sparrow SCA	스패로우	O	O	O	O	유료
Synk OpenSource	Synk	O	O	O	O	유료
Black Duck SCA	Synopsys	O	O	O	O	유료
WhiteSource	WhiteSource	O	O	O	O	유료

12) 특정 오픈소스에 대해 기술지원, 품질보증, 컨설팅 등을 포함하는 서비스 (예 : 레드햇社は 오픈소스 운영체제인 리눅스 개발에 참여 후, 기업용 지원 서비스를 유료로 제공)

13) 주요 보안취약점(XSS, SQL Injection, XXE, DoS, Zip Slip 등)을 다양한 기법(Vulnerability Scanning, Binary Analysis, Fuzzing, Code Review, Penetration Testing 등)을 통해 탐지 및 보안

14) 약 75%의 오픈소스 라이선스 이슈는 GPL 라이선스로 인해 발생(Synopsys, 2021 Open Source Security And Risk Analysis Report, '21.5월)

클라우드 활용의 증가, 원격근무 확산 등으로 인해 제로 트러스트 전략과 차세대 보안환경 구축에 관심이 집중되고 있음. 이러한 환경 변화에 적절히 대응하기 위해 새로운 기술을 활용할 수 있는 성숙한 조직과 절차를 갖출 필요

1 이슈 분석

● 클라우드 등 제3자 활용 증가 및 원격근무 장기화로 보안위협도 심화

코로나19로 비대면 환경이 보편화됨에 따라 원격근무 및 클라우드 도입이 활발해지며 기업의 내부와 외부 사이에 존재하던 보안의 경계가 다소 모호해지는 경향

최근에는 원격근무에 사용되는 SSL VPN 취약점¹⁵⁾을 이용하여 내부 직원 계정을 탈취하고 랜섬웨어를 유포하는 등 공격방식 또한 다변화

● 신뢰할 수 있는 경계가 사라져감에 따라 제로 트러스트 전략에 주목

원격근무, 클라우드 등 금융회사의 디지털 연결이 복잡해지고 보안 경계가 모호해짐에 따라 보안위협은 전통적인 신뢰 경계선을 넘어 금융회사 내부에서도 발생

이에 기업 내부에서 접속한 사용자를 포함하여 모든 사용자를 기본적으로 신뢰하지 않고 검증하는 것을 기본으로 하는 제로 트러스트 전략이 확산 중¹⁶⁾

제로 트러스트의 원칙 (NIST, '20.8월)

- 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



● 제로 트러스트 전략 구현 등을 위한 차세대 보안 솔루션 도입 확산

이러한 제로 트러스트 전략의 구현과 더불어 변화하는 업무 환경, 다양하고 복잡한 보안위협¹⁷⁾의 증가 등에 대응하기 위해 SI 등 신기술을 활용한 차세대 보안 솔루션이 확산 중

15) 국내 기관 원격 근무시스템을 대상으로 SSL VPN Directory Traversal Vulnerability(CVE-2018-13379)를 악용하여 계정정보를 탈취하고 내부 정보를 유출하려는 시도가 발생(연론보도, '21.6월)

16) 미국 백악관은 사이버보안강화 행정명령('21.5월)을 통해 제로 트러스트 아키텍처 도입을 강조

17) 반복적으로 대량의 보안이벤트를 분석함에 따라 중요 이벤트 분석에 집중하기 어려움

포스트 코로나 시대 차세대 보안 솔루션

구분	내용
제로 트러스트 솔루션	소프트웨어 정의 경계, SDP(Software Defined Perimeter) 신원을 기반으로 자원에 대해 접근을 제어하는 방식으로 네트워크 디바이스, 단말상태, 사용자 ID를 확인하여 권한이 있는 사용자 및 디바이스에만 접근권한을 부여하는 솔루션
	제로 트러스트 네트워크 액세스, ZTNA(Zero Trust Network Access) 제로 트러스트를 토대로 기기나 IP 주소를 이용한 전통적 인증방식 대신 사용자 중심으로 강화된 인증을 적용하여 안전한 접속을 제공하는 솔루션
자동화 및 통합 솔루션	보안 통합 자동화 대응, SOAR(Security Orchestration, Automation and Response) 통합된 보안 대응을 위해 대량의 데이터를 자동으로 분석하고, 유입되는 보안위협에 대해 대응 레벨을 자동으로 분류하고 지원하는 등의 역할을 수행하는 솔루션
	엔드포인트 위협 탐지 및 대응, EDR(Endpoint Detection and Response) 제로데이 등 보안위협 대응을 위해 단말(Endpoint)에서 발생하는 악성행위를 실시간으로 탐지하고 이를 분석 및 대응하여 피해를 예방 및 최소화하는 솔루션

2 전망 및 대응전략

● 강력한 인증 기반의 제로 트러스트 전략 검토

원격근무, 클라우드 활용 등에 따른 보안위협 심화에 대응하기 위해 강력한 인증 수단을 기반으로 하는 제로 트러스트 전략과 이를 지원하는 솔루션을 검토할 필요

제로 트러스트 전략의 성공을 위해서는 우선 기존 워크로드를 상세히 분석하고 고위험 업무¹⁸⁾에 필요한 통제를 식별할 필요

기존 인프라 환경과 제로 트러스트 환경이 일정 기간 공존할 필요가 있다면 하이브리드 아키텍처를 고려하는 것도 가능

● 차세대 보안기술이 만능은 아니며 성숙한 조직과 절차가 필수

플레이백¹⁹⁾ 작성이나 시나리오 분석과 같은 사전 준비 없이는 차세대 보안기술의 여러 이점에도 불구하고 오히려 보안 예산이 낭비될 우려

* 대부분의 SI 기반 프로젝트가 사전 준비 부족으로 실패(가트너, '21.4월)

따라서, 차세대 보안기술을 성공적으로 활용하기 위해서는 성숙한 조직과 절차를 갖추고 기술 도입의 이점과 보안 투자의 효용성을 객관적으로 평가할 필요

18) 고객 신원확인, 원격 거래 수행, 대량의 개인신용정보 처리, 정보 시스템 관리 등

19) 특정 사고가 발생했을 때를 가정하여 행동 수칙, 절차, 수행 업무 등을 사전에 정리한 가이드

05

금융안정을 위협하는 제3자 리스크, 강조되는 운영복원력의 확보

사이버리스크의 확대가 금융안정에 영향을 미칠 수 있다는 인식의 확산과 함께 제3자 리스크 관리와 운영복원력 확보의 중요성이 더욱 강조되고 있으므로, 관련 규제 변화 등을 살펴 선제적 검토와 대응을 준비할 필요

1 이슈 분석

● 사이버리스크의 확대 및 금융회사 등 간 연결에 따른 금융안정성 저해 우려

금융의 디지털 전환으로 관리해야 할 사이버리스크의 범위가 확대되고 있으며, 사이버공격의 양상도 더욱 체계화·정교화²⁰⁾



특히, 금융회사, 소비자, 핀테크 기업 등 금융시스템 참여자 간 연계가 복잡해짐에 따라 사이버리스크는 금융회사의 운영 리스크 차원을 넘어 금융시스템 전체로 확산되어 금융안정에까지 영향을 미칠 수 있다는 우려²¹⁾도 제기

● 운영복원력 확보와 제3자²²⁾ 리스크 관리를 위한 정책 추진

코로나19의 대유행 등으로 기존 IT시스템과 프로세스 중심의 BCP만으로는 위기상황에 적절히 대응하기 어렵다는 인식이 확산됨에 따라

위기 상황에서도 중요 금융기능이 영향 허용한도²³⁾ 내에서 유지되도록 하는 역량인 운영복원력 강화 중심의 정책이 다수 국가에서 추진되고 있음

제3자 리스크 및 운영복원력에 관한 각국의 정책 현황

국가	기관	정책명
 영국	영란은행(BoE) 금융행위감독청(FCA) 건전성감독청(PRA)	아웃소싱과 운영복원력 (Operational Resilience : Impact tolerances for important business services, Outsourcing and third party risk management)
 EU	EU 위원회	디지털 운영복원력 법안 (Digital Operational Resilience Act, DORA)
 미국	통화감독청(OCC)	운영복원력 강화를 위한 모범관행 (Sound practices to strengthen operational resilience)

20) 세계적으로 인정받아 온 IT 모니터링 솔루션 기업 S사에 악성코드를 삽입한 공급망 공격 발생(보안뉴스, '20.12월)

21) ESRB(Europe Systemic Risk Board)는 「Systemic Cyber Risk」('20.2월) 보고서에서 금융회사에 대한 사이버리스크가 시스템릭 리스크로 발전될 수 있음을 이론적 모델과 시나리오를 통해 설명

22) 서비스나 용역의 아웃소싱, 독립 자문기관 이용, 네트워킹 약정 등 금융회사와 다른 기업 간의 모든 사업약정을 포함(FSB), 파트너십, JV 등 은행과 다른 기업 간 모든 사업 약정으로까지 광범위하게 정의(OCC)

23) 중요서비스 또는 기능이 최대로 중단 가능한 수준을 의미(발생 가능성 등은 배제한 개념)

또한, 금융분야의 클라우드 이용 확대²⁴⁾, 핀테크 기업과의 연계가 증가함에 따라, 그와 관련한 장애 발생, 정보 유출 등의 사고가 증가하고 있어 제3자 리스크에 대한 관리 필요성이 크게 부각

특히, 주요 제3자에 대해서는 보안리스크 뿐만 아니라 집중 리스크 및 종속 리스크²⁵⁾에 대한 관리를 위해 출구전략의 마련 필요성 등이 강조되고 있음

제3자 리스크 관련 사고 사례

구분	시점	내용
클라우드 업체 A사	'18.11월	A사에서 발생한 서버 장애가 84분간 지속되어 국내 전자상거래 서비스 등에서 접속이 불가
미국 금융회사 C사	'19.7월	C사의 방화벽 설정 오류를 악용하여 클라우드 업체 A사에 저장된 1억 600만 명의 고객 개인정보가 유출
독일 핀테크 업체 W사	'20.6월	독일 대형 핀테크 업체인 W사가 분식회계로 파산하여 연계된 업체에 영향
클라우드 업체 F사	'21.6월	CDN 업데이트 과정 중 PoPs 구성 오류로 인해 연결되어 있던 CNN, 백악관, 아마존 등 주요 민·관사이트에 일시적으로 접속 불가

출처 : 관련 언론보도

2 전망 및 대응전략

● 제3자 리스크 관리 강화 및 운영복원력 확보를 위한 노력 필요

계속되는 금융의 디지털 전환은 금융회사의 제3자 의존성을 보다 증가시킬 것이며, 디지털 금융에 있어 운영복원력의 중요성은 더욱 강조될 전망

제3자 관계 목록화를 통한 제3자 의존성 파악, 제3자 리스크 관리 시스템 구축, 계약서 내 운영복원력 확보를 위한 사항 명시 등 제3자 리스크 관리를 강화할 필요

아울러, 중요업무 식별, 업무별 영향 허용한도 설정, 서비스 유지에 필요한 자원 식별 등을 수행하는 한편, 업무 중요도에 비례하는 운영복원력을 확보하기 위한 지속적인 점검 및 개선 활동을 수행할 필요

● 전자금융거래법 개정 등 관련 규제에 대비할 필요

국회 논의 중인 전자금융거래법 개정안에서도 업무 지속성, 수탁자 관리 등에 대한 규제를 강화하려는 움직임 따라서, 금융회사는 이사회 및 고위 경영진을 중심으로 전사적인 제3자 리스크 관리 및 운영복원력 관련 정책을 정비하고, 필요한 조직과 자원을 확보하는 등 규제 변화에 대비할 필요

24) 글로벌 기업 대상 설문 결과, 절반 이상의 기관이 클라우드 상으로 업무를 이관(Flexera, '20.4월)

25) 집중 리스크 : 외부 위탁한 서비스 또는 제품이 제한된 수의 서비스업체에 의해 제공됨에 따라, 한 서비스에서 장애 발생 시 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

비트코인, 이더리움, 스테이블 코인, NFT(대체불가토큰), CBDC(중앙은행 디지털화폐) 등의 '디지털자산'이 확산되며 금융생태계의 변화 가능성도 제기되는바, 그에 앞서 보안위협, 범죄 악용 가능성, 프라이버시 등의 과제 해결이 필수

1 이슈 분석

● 디지털자산²⁶⁾의 형태와 용도는 다양한 양상으로 확대되는 추세

지금·결제²⁷⁾, 투자뿐만 아니라 자산의 소유권 보장 및 거래(예 : NFT²⁸⁾) 등 디지털자산의 용도가 점차 다양화되는 추세

이와 함께 탈중앙화 금융, 즉 중개기관 없이 블록체인상의 스마트 계약을 통해 디지털자산 간 교환, 대출, 파생상품 등의 서비스를 제공하는 디파이(DeFi)²⁹⁾가 등장

* '21.11.8. 기준 약 1,057억 달러가 디파이에 예치되어 있으며, 이는 전년 동기 대비 약 4.9배 증가한 수치 (DEFI PULSE, '21.11월)

한편, 세계 각국의 중앙은행은 디지털 전환의 흐름에 발맞추어 물리적 법정화폐를 대체 또는 보완하기 위한 수단으로 CBDC 도입을 추진³⁰⁾

● 디지털자산 관련 보안위협³¹⁾ 등 해결해야 할 과제 존재

디지털자산 거래소 또는 CBDC 발행·참여기관에 대한 사이버공격, 디파이의 스마트 계약 관련 취약점을 이용한 공격 등 디지털자산과 관련하여 다양한 보안위협이 존재

디지털자산 및 디파이 관련 보안위협(예시)³²⁾

- 디지털자산 거래소 또는 CBDC 발행·참여기관 대상 DDoS, 해킹 등의 사이버 공격
- 거래소 사칭 사기 또는 거래소에 의한 금융사기*
* 시세조작, 거래소 영업 중단 후 이용자의 디지털자산 인출 차단 등
- 이용자의 관리 부실 등으로 인한 디지털자산 전자지갑 개인키 탈취
- 블록체인 기술의 취약점을 악용한 공격(예 : 더스팅 공격³³⁾, 51%공격³⁴⁾ 등)
- 신규 디파이 서비스를 미끼로 디지털자산 발행 및 투자금 모집 후, 의도적으로 스마트계약에 취약점을 심어 디지털자산을 탈취

※ 디지털자산 및 디파이 서비스와 관련하여 발생 가능한 보안위협의 예시로, 설계·운영방식 등에 따라 위험이 상이할 수 있음

디지털자산의 익명성 보장 정도에 따른 범죄 악용 가능성, CBDC의 프라이버시 이슈 등도 살펴봐야 할 과제

26) 본 보고서는 '디지털자산'을 비트코인, 이더리움, 스테이블 코인(가격 변동성을 최소화한 토큰), NFT(대체불가토큰), CBDC(중앙은행 디지털화폐) 등을 포괄하는 개념으로 정의

27) '21.1월부터 미국 통화감독청(OCC)은 시중은행이 지금·결제업무를 위해 스테이블 코인을 구매, 판매 및 발행하는 것을 허용하였으며, 비자카드·마스터카드·페이팔 등은 디지털자산을 이용한 결제서비스를 제공

28) 대체불가토큰(Non-Fungible Token) : 토큰에 소유자, 판매이력 등의 정보를 담아 디지털 콘텐츠 등의 소유권을 보장·거래할 수 있는 토큰(예 : 트위터 역사상 첫 번째 트윗은 NFT형태로 한화 약 34억원에 판매)

29) 디파이(DeFi)는 탈중앙화 금융(Decentralized Finance)의 약자로, 블록체인상에서 디지털자산과 스마트계약을 통해 중개기관 없이 자동으로 제공되는 금융서비스를 의미

30) CBDC를 발행(5개국), 파일럿 테스트 실시(14개국), 개발(16개국), 연구(32개국)하는 등 83개국이 세계 GDP의 90%를 차지하는 CBDC 도입을 시도 또는 구축 중(Gartner·Atlantic Council, '21.9월)

2 전망 및 대응전략

● 디지털자산 활성화에 따른 금융생태계 변화에 유의할 필요

일각에서는 디지털자산이 금융의 제2의 디지털전환을 일으키며 금융회사의 역할 및 금융인프라 등을 대대적으로 변화시킬 가능성도 제기되고 있으므로,

금융회사는 비즈니스 모델 다변화 등 이러한 환경 변화에 선제적이고 적극적으로 준비할 필요³⁵⁾

● 디지털자산에 대한 보안성 확보는 선택이 아닌 필수

디지털자산은 금전적 이득을 노리는 해커에게 매력적인 공격 대상이므로, 디지털자산의 특성과 용도 등에 따른 적절한 보안대책이 중요

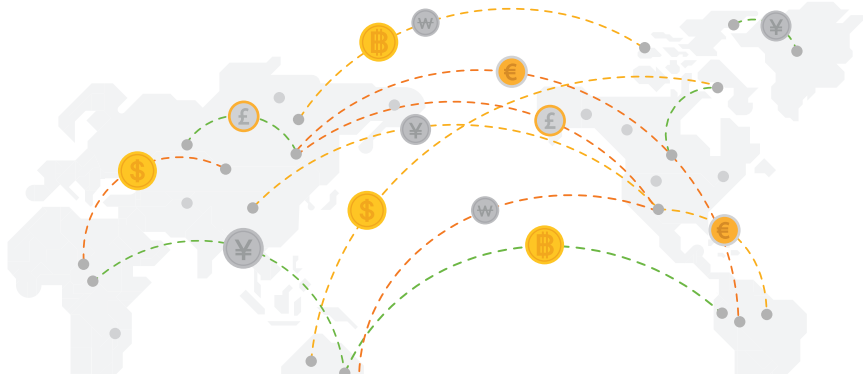
* (예) 블록체인 기술 적용 시 코드 감사 등을 통한 스마트계약의 취약점 최소화, 피해보상체계 구축, 디지털자산 개발자·제공자의 책임소재 명확화, 금융서비스 중단 방지를 위한 운영복원력 확보 등

또한, 범죄 악용 가능성 모니터링 및 차단, 프라이버시 보호, 거래 신뢰성 확보를 위한 인증체계 구축 등 안전한 디지털자산 활용을 위한 엄격한 기준과 원칙을 마련할 필요

주요 7개국(G7)이 제시한 소매용(Retail) CBDC 원칙('21.10월)

- | | |
|--------------------------|-----------------------------------|
| 1 통화·금융안정성 보장 | 8 CBDC 인프라의 효율적인 에너지 사용 |
| 2 적절한 규제 및 거버넌스 체계 구축 | 9 디지털경제의 혁신을 촉진 |
| 3 프라이버시(개인정보보호) | 10 포용적 금융 실현 |
| 4 운영복원력 및 사이버보안 확보 | 11 항상 빠르고 안전하고 저렴한 대중의 지급수단 역할 수행 |
| 5 기존 지급수단과의 공정한 경쟁 | 12 대외지급수단으로의 활용 가능성 제고 |
| 6 범죄에 악용되지 않도록 방지 | 13 국제 발전 지원 |
| 7 국제 통화·금융시스템에 대한 피해 최소화 | |

출처 : Public Policy Principles for Retail Central Bank Digital Currencies('21.10월)



31) 딜로이트의 '2021 글로벌 블록체인 서베이'(10개국 고위경영자·실무자 1280명 대상, 중복투표 가능)에 따르면 디지털자산의 도입·사용을 방해하는 가장 큰 장애물로 '사이버보안(71%)'이 1위를 차지

32) CBDC는 분산원장을 통해 구현하는 것만이 아닌 중앙은행이 직접 발행하고 관리하는 디지털화폐를 총칭하는 개념으로, 분산원장(블록체인) 기술 미 적용 시 블록체인 및 스마트계약 관련 보안위협은 미 해당

33) 아주 적은 양의 토큰을 사용자 지갑에 전송해 사용자의 프라이버시를 침해하는 공격

34) 네트워크의 51%를 초과하는 해시 연산력을 확보하여 거래정보를 조작하는 공격

35) 현재 일부 금융회사는 디지털자산을 안전하게 보관해주는 커스텀 산업에 진출 또는 자체 CBDC 플랫폼 구축을 추진

금융분야 메타버스 활용 증가로 인해 메타버스가 차세대 금융채널로 부상할 가능성과 함께 가상세계 속 신규 경제체계(Meta-nomics)의 등장도 예상. 메타버스 내 해킹·사기 등 범죄예방, 자금세탁방지, 개인정보 관리 등에 유의할 필요

1 이슈 분석

● 금융분야 메타버스 활용 사례 및 범위가 빠르게 증가

국내 금융회사들의 메타버스 기술 활용은 주로 직원교육, 업무회의, 대고객 홍보·마케팅 등에서의 실험적 목적에서 시작하였으나,

최근 국내·외 금융분야의 메타버스 활용 범위는 온·오프라인 업무 연계, 디지털 지점 운영, AI 은행원 배치 등 본격적인 업무 영역까지 확장되고 있음



출처: Citi 유튜브



출처: 신한은행

● 메타버스 세계 속 새로운 형태의 독자적 경제활동이 태동

특히, 금융회사의 메타버스 기술이나 플랫폼 활용을 넘어, 최근에는 메타버스 플랫폼 내 독자적인 경제활동이 나타나면서 신규 금융시장의 형성 가능성이 대두

대표적 메타버스 플랫폼인 로블록스(Roblox)에서는 그 이용자가 직접 게임 및 아이템을 제작해 자체 가상자산인 로벅스(Robux)³⁶로 교환 가능하며, 개발자 환전 프로그램(데벡스, DevEx)을 이용하여 80 로벅스 당 1달러로 현금화 가능

디센트럴랜드(Decentraland)³⁷ 등의 플랫폼에서는 부동산이나 예술작품 등을 NFT(Non-Fungible Token, 대체불가토큰)화하여 거래하는 사례가 계속해서 나타나고 있음

36) 로벅스의 전체 거래 규모는 '21년 2분기 약 6억7천만 달러로 전년 동기 대비 35% 증가하였으며, '20년까지 34만 명에 달하는 개발자들의 누적 수익은 약 2억5천만 달러를 상회

37) 가상세계 토지를 거래할 수 있는 메타버스 플랫폼으로, 토지는 NFT로 구성된 랜드(Land)라는 단위로 거래되는데 초기의 비어있는 랜드는 모두 균일한 가격으로 거래되지만 그 대체 불가능한 특성으로 인해 위치나 개발 정도 등에 따라 가격이 다양하게 변화

2 전망 및 대응전략

• 금융분야 메타버스 활용에 따른 금융사기 등 범죄 예방 노력 필요

비대면·가상세계에 익숙한 Z세대 중심으로 인터넷뱅킹, 모바일뱅킹을 잇는 차세대 디지털금융 채널로서 메타버스는 앞으로도 더욱 주목받을 전망

가상화된 디지털 시청각 정보에 바탕한 메타버스 금융채널에서는 금융사기 위험이 더욱 확대되고, 특히 몰입형 기술³⁸⁾을 이용한 고도화된 사기 수법의 등장이 예상되므로 이에 면밀하게 대비하는 것이 중요

그 밖에도 AI, 클라우드, AR/VR 기기 등 메타버스 기반 기술 취약점에 유의해야 하며, 특히 외부 플랫폼과의 연계를 통해 금융채널을 구축할 경우 복잡하고 예측하기 어려운 위험 발생에 대비할 필요

AR/VR 기기 관련 취약점 등 보안 고려사항(예시)



- 사용자의 생체정보 등 민감정보를 다루므로 공격자의 공격 타깃이 되기에 용이
- 패치되지 않은 펌웨어, 취약한 서드파티 앱 등 사용 시 수집정보의 유출 위험성
- 경량화·저전력 OS에 따른 최소한의 기능 수행으로 외부 공격에 보다 취약
- 무선통신을 이용하는 특성상 패킷 캡처가 용이하여 공격자에 의한 복호화에 취약

• 새로운 경제체계 내 자금세탁 방지, 안전한 개인정보 관리 필요

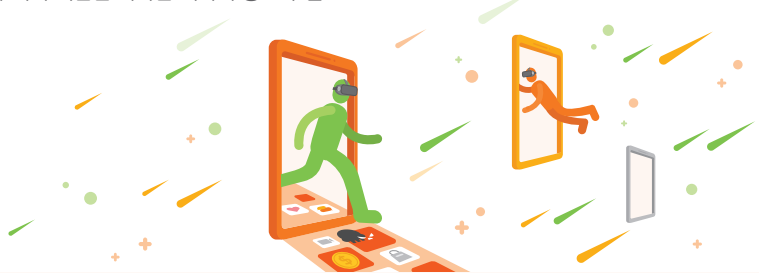
앞으로 메타버스는 일상생활 전반에까지 그 영향력이 확대될 전망

- * 최근 Facebook의 CEO 마크 저커버그는, 향후 10년 이내 10억 명 이상의 메타버스 사용과 수조 달러 이상의 관련 생태계 구축을 예상하면서, 그 시장 선점을 위해 사명을 "Meta"로 변경('21.10월)

아울러, 메타버스 속 가상자산의 지속적 성장 및 NFT 영향력 확대는 메타버스 내 신규 경제체계인 메타노믹스³⁹⁾의 등장을 현실화할 가능성

이에 따라 새로운 체계 내에서의 자금세탁 방지, 과도한 변동성 완화를 위한 방안을 마련하여야 하며, 개인 생체·민감정보의 안전한 관리⁴⁰⁾에도 각별히 유의할 필요

- * 다만, 메타노믹스는 현재의 국가 단위 경제체계가 아닌 초국가적으로 형성되는 글로벌 생태계이므로 이러한 메타버스의 탈국경적 특성에 대한 올바른 이해와 이에 기반한 국가간 적극적 공조가 필요



38) 몰입형 기술(Immersive Technology)이란, 현실과 가상의 경계를 허물어 사용자의 몰입감을 유도하는 기술로, 시청각 효과를 위한 3D 렌더링 및 디지털 휴먼 기술, 사용자 시각 정보 등을 실시간으로 추적하는 트래킹 기술 및 AR/VR 기기, 음성·동작을 통한 조작을 가능하게 하는 NUI(Natural User Interface) 기술 등을 포함

39) 메타노믹스(Metanomics)는 Metaverse와 Economics의 합성어로 메타버스를 통해 일반화된 가상경제(Virtual Economy), 증강경제(Augmented Economy) 및 그를 혼합한 혼합경제(Mixed Economy)를 함께 이르는 용어로서, 구체적으로 금융분야와 관련해서는 메타버스 내 독자적인 자금·결제체계, 여·수신, 보험, 투자 등 새로운 금융서비스에 대한 수요 및 시장 형성으로 이어질 것이라는 전망

40) 메타버스 내 지급·결제 등 금융수요가 증가하면 이용자의 아바타가 상시 무자각 지속 인증(Implicit Continuous Authentication) 상태를 유지할 필요가 있을 것이고, 이 경우 홍채정보, 시각정보 등 개인 생체·민감정보가 지속적으로 수집·활용될 가능성

인간과 로봇이 함께 일하는 시대. 기술의 발전은 금융회사의 많은 업무들의 자동화를 가능하게 하고 있음. 성공적인 업무 자동화는 업무 범위의 명확화, 통제 수단의 확보, 지속적인 관리 등을 통해 위험을 최소화하는 것에서부터 출발

1 이슈 분석

• 단순 업무 자동화를 넘어 진화하는 초자동화⁴¹⁾ 기술

AI 등의 발전으로 금융회사 내 고차원적 업무(신용평가, 비대면인증, 주식투자 등)까지 자동화가 진행되면서 업무 효율성과 정확성⁴²⁾이 극대화

* 전 세계 자동화(RPA) 소프트웨어 예상 매출 : \$8.6억('18년) → \$18.8억('21년) (가트너, '20.9월)

초자동화에 적용되는 신기술(예시)

기술	설명	적용 예시
Low(No) Code	복잡한 코딩을 단순화하여, 간단한 UI 등을 통해 쉽고 빠르게 개발·배포하는 기술	전반적인 개발 업무
SOAR	다양한 보안 솔루션을 일괄 지휘하는 자동화된 컨트롤타워 시스템	보안관제 등을 포함한 전반적인 정보보안 업무
iPaaS	애플리케이션 통합을 위한 플랫폼으로, 여러 환경에서 구축된 프로그램을 상호 연동	비대면 계좌 개설, 프로젝트 관리
Cloud RPA	어디서나 어떤 기기로도 접근할 수 있는 클라우드 기반의 업무 자동화 시스템	재택근무 중 업무처리, 프로젝트 관리
iBPMS	AI 기반의 의사결정을 통해 빠르고 효율적인 업무 자동화 시스템	신용평가, 대출심사, 보험료 산출, 챗봇
RegTech	다양한 법, 시행령, 가이드라인 등을 종합적으로 분석하여 사내 업무 시 컴플라이언스 지원	컴플라이언스 지원, 사내 정책 반영

• 업무 자동화의 확대에 따라 새롭게 발생하는 문제점

업무 자동화를 통해 업무 효율성과 정확성을 제고할 수 있는 반면, ①자동화 오류, ②취약점 증가, ③관리 실패, ④대안 부재 등의 문제 발생 시 오히려 업무 지연 또는 중단이 발생할 우려

41) 기존에 사람이 수행하던 업무, 의사결정 등을 인공지능, 로봇 프로세스 자동화(Robotic Process Automation, RPA) 등의 기술을 통해 자동화함으로써, 업무의 효율과 정확도를 극대화하는 기술

42) 자동화된 업무를 통해 정확성 증가(67%), 생산성 증가(64%), 비용 감소(60%), 운영리스크 감소(54%) (CCR, RPA : An Executive Primer)

초자동화 활용에 따른 새로운 문제점⁴³⁾

문제점	설명
① 예상하지 못한 자동화 오류	<ul style="list-style-type: none"> · 빈번한 오류·장애 발생으로 오히려 업무비용과 시간이 증가 · 특정 상황에서 예상치 못한 결과가 도출 (예) 챗봇 서비스가 사회적 악자 혐오 발언 및 개인정보 유출
② 시스템 복잡도 상승에 따른 취약점 증가	<ul style="list-style-type: none"> · 여러 서비스의 상호 연동으로 시스템 복잡도, 취약점 증가 · 보안보다 기능에 초점이 맞춰진 자동화로 인한 취약점 (예) M사 Low Code 플랫폼의 설계 결함으로 인해 최소 47개 기업에서 개인정보 3,800만 건 유출
③ 지속적인 관리 실패	<ul style="list-style-type: none"> · 자동화 시스템 관리·운동을 위한 예산 및 전문인력 부족 · 변화하는 시장, 규제 등 환경변화에 대한 대응 미흡 (예) 글로벌 RPA 업체 U사에서 환경 변화에 따른 추가 업데이트를 수행하지 않아 자동화 시스템 기능 마비
④ 대인 부재	<ul style="list-style-type: none"> · 자동화 추세에 따라 조직 내 업무 수행 가능 인력이 감소하여 자동화에 대한 의존성이 과도하게 증가하는 문제 (예) 기업 내 보안업무를 자동화 시스템에 의존하거나, 전문인력 없이 혹은 소수 인력으로만 운영할 경우 보안사고 발생 가능성이 오히려 증가 가능

2 전망 및 대응전략

● 초자동화를 활용한 업무 자동화 흐름은 전사적으로 확대될 것

구독형 서비스 형태의 자동화 솔루션⁴⁴⁾ 활용 시 큰 초기 비용 없이 자동화 추진이 가능함에 따라 업무 자동화 도입을 통해 비용, 오류, 기술 복잡성 등을 최소화하려는 기업들이 지속적으로 늘어날 전망
특히, 인력 소비가 크거나(보안관제 등) 인적 실수가 자주 발생하는 분야(버전 관리 등)에서의 업무 자동화가 확대될 것으로 예상

● 위험 요소를 사전에 차단하고 안전하게 활용하는 것이 중요

시스템 설계 시 업무 담당자의 참여를 통해 구체적이면서도 단순한 업무 로직을 마련하고, 시스템 구현 과정에서는 발생 가능한 모든 상황을 최대한 분석하고 필요한 안전장치⁴⁵⁾를 구축해야 함
자동화 구축 이후에는 업무 처리 과정을 지속적으로 모니터링하면서 장애 발생 시에도 사전에 마련된 안전장치와 대체 방안 등을 통해 업무 공백 등의 피해를 최소화할 필요



43) UiPath : Incident History('21.7월), TechTarget : Top 10 causes of RPA failures and how to avoid them('20.8월) 등 참고 및 재구성

44) 미국 Accelrate사의 RPA365의 경우 90일 이내에 고객사 업무에 특화된 자동화 시스템을 구축한 뒤, 월 단위 구독형 자동화 서비스를 통해 비용 청구

45) 장애를 최소화하기 위한 최적화 작업, 장애 발생 시 빠르게 탐지하여 알리는 시스템 구축, 대인 알고리즘으로 전환 등

데이터 수집·활용에 대한 기업들의 니즈가 크게 증가함에 따라 데이터 독점 등에 대한 우려도 증가. 향후 고품질 데이터 확보, 데이터 거래·유통 플랫폼 활용 등을 포함한 균형 있는 데이터 전략을 마련할 필요

1 이슈 분석

• 데이터 활용을 통한 경쟁력 확보 및 수익 창출 추구

적극적인 데이터의 활용을 통해 보다 혁신적인 서비스를 발굴하고, 이를 통해 더 높은 경쟁력과 수익을 창출하려는 기업이 크게 증가

국내·외 기업들의 데이터 활용 사례

구분	내용
국외 C사	소셜 데이터 분석 서비스를 이용하여 SNS에 자사 상품이 언급되는 글을 모니터링하여 비 우호적 정보가 증가하는 경우 홍보를 강화
국내 K사	1톤 이상 화물차 운전자들의 안전운행, 하이패스 납부 기록에 자사가 가지고 있는 신용정보를 결합한 데이터를 분석하여 신용점수를 평가
국외 A사	시장 정보, 원자재 수급, 고객 지불 용의 등의 데이터를 활용하여 가변적 가격 책정 알고리즘을 설계
국내 H사	운전자의 운전 습관을 점수화하고, 사고 정보와의 상관관계를 파악한 후 그 결과에 따라 보험료를 차등화

• 데이터 독점, 개인정보 통제, 소외계층 등 양극화 이슈

데이터 양극화의 다양한 양상

구분	내용
기업-기업	보유 데이터가 충분한 빅테크 기업의 경우 금융회사 등 다른 기업과 데이터를 공유할 유인이 적으며 오히려 데이터를 독점하려는 경향
기업-개인	개인정보를 플랫폼 기업이 수집·가공·활용하면서 개인이 자신의 데이터를 온전히 통제하지 못하는 Data Control Divide ⁴⁶⁾ 현상 발생 가능
개인-개인	디지털 매체에 접근하기 어려운 소외 계층은 적극적으로 데이터 생성 활동에 참여하기 어려운 상황 등이 발생할 우려

출처 : 김미경 「플랫폼 데이터 생태계에서 데이터 격차 : 디지털 불평등을 넘어」(‘20.12월) 등 참고 및 재구성

데이터 활용 증가에 따라 다양한 양극화 이슈가 발생 가능하나, 그 중에서도 기업 간 데이터 양극화는 가장 많은 데이터를 보유한 기업의 시장지배력 강화⁴⁷⁾로 이어져 공정 경쟁을 저해하고 소비자의 부담을 증가시킬 우려

46) 개인정보의 생성·이동·가공 등에 대해 정보주체가 권한을 제대로 행사하지 못하고 플랫폼 기업이 주도권을 갖는 현상

47) 페이스북 등이 아이폰 사용자의 앱 사용을 추적하지 못하게 되면서 애플의 광고시장 점유율이 6개월간 3배 증가 (Financial Times, '21.10월)

이러한 문제를 해결하기 위해 우리나라, 미국, EU, 일본 등에서는 빅테크 기업의 데이터 독점 방지 등 공정한 디지털 경쟁을 유도하기 위한 법안 마련을 추진

국가별 데이터 양극화 등 방지 법률·정책 현황

국가	법률/정책	주요내용
대한민국	온라인 플랫폼 분야 단독행위 심사지침(검토 중)	빅테크 기업의 킬러 인수 ⁴⁸⁾ 를 규정
	개인정보보호법 개정안 ('21.9월 발의)	본인의 정보를 적극적으로 관리·통제하고 능동적으로 활용할 수 있도록 함
	데이터 산업진흥 및 이용촉진에 관한 기본법('21.10월 제정)	민간 데이터의 생산, 거래 및 활용을 통해 다양한 경제적 가치 창출을 도모
미국	서비스 전환 허용에 따른 호환성 및 경쟁 증진법(안) ('21.6월 발의)	플랫폼 기업이 데이터를 독점하지 못하도록 하고 플랫폼 간 정보 이동을 유인
EU	디지털 시장법(안) ('20.12월 발의)	플랫폼 기업이 알고리즘으로 소비자에게 가하는 부당 행위를 금지하고 위반 시 기업 강제 분할
	디지털 서비스법(안) ('20.12월 발의)	게이트키퍼 플랫폼 사업자가 디지털 시장의 공정한 경쟁을 저해할 시 플랫폼 폐쇄까지 가능
일본	특정 디지털 플랫폼 거래 투명화법 ('21.2월 시행)	이용자로부터 수집하는 데이터 이용 범위 공개, 플랫폼 독점 금지

2 전망 및 대응전략

● 고품질 데이터 중심의 데이터 거버넌스 수립을 검토할 필요

적극적인 데이터 수집·분석·활용에 있어 데이터 독점 등의 이슈를 최소화하기 위해서는 공정하고 균형 있는 지속 가능한 데이터 전략을 수립하여 추진할 필요

특히, 무조건적인 대량 데이터의 수집에서 한 발 나아가 고품질 데이터 확보를 위한 데이터 품질 점검·관리 등 데이터 거버넌스⁴⁹⁾의 수립을 검토할 필요

* 저품질의 데이터는 매년 미국에서 3.1조 달러 규모의 비용을 초래(IBM Watson, '20.1월)

● 데이터 거래·유통 플랫폼의 적극적인 활용 등 종합적인 데이터 전략 검토 필요

향후 데이터 양극화 문제 해소, 데이터 관리 비용 절감 등을 위해 데이터 표준화 및 가치평가의 중요성이 부각될 전망

이러한 환경 변화에 유연하게 대응하기 위해서는 금융 데이터 거래소 등 관련 플랫폼을 적극 활용하는 방안을 포함한 종합적인 데이터 전략을 검토할 필요

48) 자본력을 가진 대기업이 잠재력이 크다고 판단되는 스타트업을 인수해 공정한 경쟁을 방해하는 행위

49) 데이터의 수집·생성·가공·유통 등 전 과정을 통제하고 컴플라이언스 등을 관리하는 개념

금융의 플랫폼화가 가속화되고 이를 선점하기 위한 경쟁이 심화되고 있으며, 다양한 플랫폼을 공격하는 악성코드도 증가. 플랫폼을 둘러싼 혁신의 기회와 위협 요인이 증가하고 있음에 유의할 필요

1 이슈 분석

● 금융의 플랫폼화와 다양한 금융서비스의 등장

오픈뱅킹의 확산 이후 금융서비스의 세분화(unbundling)가 확대되며 금융회사는 서비스형 은행(BaaS)⁵⁰⁾ 등 임베디드 금융⁵¹⁾ 시장 진출에 적극적

특히, 당국의 정책⁵²⁾에 따라 은행도 쇼핑, 음식 주문과 같은 비금융서비스를 함께 제공하는 금융·생활 플랫폼으로의 변화를 추구할 수 있는 길이 열림

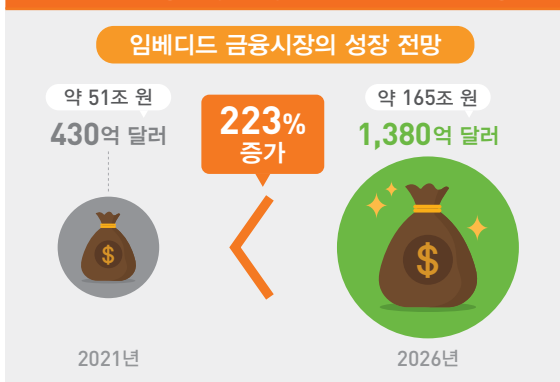
* (예) 싱가포르의 DBS 은행은 자사 플랫폼에서 부동산, 차량 구매, 쇼핑 등 서비스를 제공

아울러, 기존에 많은 고객을 보유한 비금융회사는 여러 금융회사가 제공하는 다수의 금융 플랫폼을 복합적으로 활용한 초개인화⁵³⁾ 서비스를 출시

● 금융서비스 이용 환경과 보안 위협의 멀티플랫폼⁵⁴⁾ 진화

많은 IT 기업들이 금융 플랫폼을 활용하여 자사 서비스에 결제, 송금과 같은 금융서비스 결합을 시도함에 따라 금융서비스 이용환경은 더욱 다양하게 진화

임베디드 금융시장 전망 및 멀티플랫폼 금융서비스 사례



출처 : 주니퍼리서치



출처 : 현대자동차

50) 은행의 여러 금융서비스를 기능 단위로 분해하여 핀테크 기업 등이 활용할 수 있도록 하는 것으로, 임베디드 금융 하나의 형태로 이해

51) 비금융회사가 금융회사의 금융상품을 중개하는 것을 넘어서 자사 플랫폼에 핀테크 기능을 내장하는 것

52) 「디지털금융 규제 제도 개선방안」 (금융위원회, '20.12월) 중 은행의 플랫폼 비즈니스 진출 허용 확대

53) 실시간으로 소비자의 상황과 맥락을 파악하고 이해해 소비자가 가장 원하는 경험을 금융서비스와 상품을 통해 적시에 제공하는 기술 (hyper-personalization)

54) 하나 이상의 플랫폼에서 실행 가능한 소프트웨어를 뜻하는 용어로서 동일한 형태의 실행을 보장

한편, 금융서비스 이용 환경이 다양해짐에 따라 기존의 윈도우즈 운영체제 뿐만 아니라 차량, IoT 등 다양한 환경을 공격하는 멀티플랫폼 악성코드도 증가⁵⁵⁾

특히, 공격자들은 금융정보 및 금전 탈취 목적의 악성코드를 개발함에 있어 다양한 개발언어를 활용하는 등 기존에 알려진 악성코드 탐지를 우회⁵⁶⁾하기 위한 시도를 지속

최근 멀티플랫폼 악성코드 사례

악성코드명	작성언어	설명
Mata	C++, C#	윈도우, 리눅스, 맥 등 다양한 OS를 감염시킬 수 있으며, IoT 기기, 방화벽, 라우터 등을 스캔하는 것도 가능
Milum	Python	파이썬 스크립트인 Guard를 활용하여 키입력 및 화면정보 탈취
GuardMiner	Go	클라우드 호스트를 공격해 가상자산을 채굴하도록 명령 전달
Pysa	Go	도난당한 자격증명을 통해 다양한 환경에서 동작하는 랜섬웨어

2 전망 및 대응전략

● 자동으로 구성되는 금융서비스와 사람이 아닌 고객도 등장할 전망

금융 플랫폼 내 연계를 통해 고객 요구사항을 자동으로 파악하고 필요한 금융서비스를 자동으로 구성하여 제공하는 금융서비스가 확대⁵⁷⁾될 전망

* (예) 금융거래 내역을 기반으로 주택담보 대출상품 안내, 이사 날짜에 주택 보험상품 추천 등

또한, 초개인화가 극대화되며 AI, IoT 등이 사람을 대신하여 서비스를 요청·처리하는 기계고객(Machine Customer)⁵⁸⁾이 금융분야로 확장될 전망

● 플랫폼의 다변화에 따른 체계적 대응이 필요

초개인화 금융서비스는 양질의 개인정보를 다량 보유하고 있어 공격 대상이 되기 쉬우므로, 마이데이터 플랫폼 또는 API 연계 지점 등을 노리는 공격이 증가할 것

금융회사는 금융 플랫폼의 관문이 되는 API의 보안 강화⁵⁹⁾와 함께 공격자 관점의 플랫폼 공격 시나리오와 TTP(전술·기술·절차) 분석 등 고도의 인텔리전스 역량을 갖추 필요



55) 美연방수사국(FBI)의 조사에 따르면 '20.2월부터 1년간 애플사의 운영체제 맥(Mac)을 대상으로 하는 악성코드를 통해 가상자산 거래소에 대한 공격이 있었던 것으로 알려졌다('21.2월)

56) 최근 공격자들은 낮은 보안 탐지율과 다양한 운영체제를 공략할 수 있다는 이점에 따라 고(Go), 러스트(Rust) 등 비주류 언어를 악성코드 개발에 선호하는 추세(보안뉴스, '21.8월)

57) 가트너는 임베디드 금융 확산과 변화하는 고객 요구사항에 따라 제품 중심에서 서비스 중심으로 금융서비스의 관점이 변화하며, 환경에 기반하여 자동 구성되는 금융서비스가 등장할 것이라 전망('21.9월)

58) AI를 통해 뉴스 등 다양한 데이터를 분석하여 주식을 자동으로 매매하는 프로그램 등

59) 지속적 인증 도입, 보안성을 갖춘 API 중개자 선정, API Gateway 접근통제 강화 등

금융보안원

FINANCIAL SECURITY INSTITUTE

금융보안원

FINANCIAL SECURITY INSTITUTE

발간번호 ARR-VII-2021-②-258

발간일자 2021-11-23

DIGITAL FINANCIAL & CYBER SECURITY

2022
디지털금융 및 사이버보안
이슈 전망