

2024 디지털금융 및 사이버보안 이슈 전망

Key Issue 금융보안 프렌들리
Financial Security Friendly



금융보안원
FINANCIAL SECURITY INSTITUTE

2024 디지털금융 및 사이버보안 이슈 전망

Key Issue 금융보안 프렌들리
Financial Security Friendly

2024 디지털금융 및 사이버보안 이슈 전망

Key Issue 핵심이슈

디지털 경쟁력, 금융보안 프렌들리 전략이 필수

F

Financial Policy 디지털금융 정책

더 이상 거스를 수 없는 패러다임,
자율보안체계 전환



깨지지 않는(anti-fragile) 탄력성,
사이버복원력



클라우드 마이그레이션,
하드웨어 넘어 소프트웨어로



S

Security Threat 보안 위협

공격채널의 다양화, 영역을 넘나드는
하이브리드 위협 고조



S/W 공급망 공격 성행,
SBOM의 중요성이 강조



피싱 범죄, '내 얼굴과 목소리까지도?'
딥페이크 기술 악용



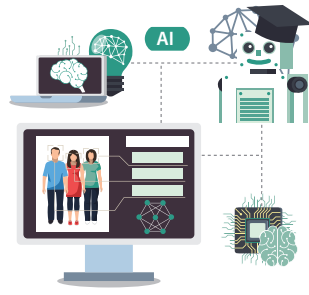
I

IT Innovation IT 혁신

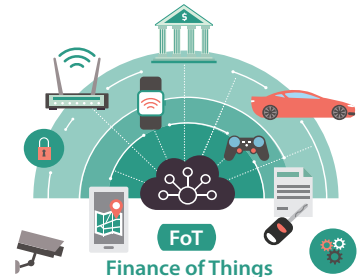
모든 것을 담는다,
디지털지갑 경쟁 가속화



AI의 안전성과 신뢰성 확보,
책임감 있는 AI 구현



사물과 디지털금융의 만남,
금융 사물인터넷(FoT)



FINANCIAL SECURITY FRIENDLY

금융보안원 원장 김철웅

금융보안원은 금융보안 싱크탱크로서의 역할을 충실히 수행하고 디지털금융 환경의 변화와 사이버보안 위협을 금융권이 사전에 인식하고 선제적으로 대응할 수 있도록 다음 해에 발생할 수 있는 디지털금융 및 사이버보안 이슈를 전망하고 발표하고 있습니다.

작년 말, 금융보안원은 올해 부각될 이슈로서 엔데믹 취약점, 랜섬웨어·피싱 등으로 인한 ‘보안의 사각지대’를 짚어내고 마이데이터, 디지털 연결 등 ‘디지털 금융의 개방’을 전망한 바 있습니다. 동시에 디지털자산, 금융보안 규제 합리화 등을 뒷받침할 수 있는 ‘안전한 보안 체계’의 마련과 클라우드·인공지능(AI)·디지털신원인증·오픈소스 등 금융권이 경쟁적으로 도입하고 있는 신기술 이면에 숨어있는 보안 우려도 제기하고자 하였습니다.

어느덧 마무리되고 있는 2023년을 돌아보면, 실제 금융보안원이 전망한 이슈들이 크게 주목받는 한 해였습니다.

그 중 올 해에는 챗GPT 등 생성형 AI가 화두로 떠오르면서 금융권이 AI기술과 데이터의 잠재력에 본격적으로 눈을 뜬 동시에 국가 배후 해킹 조직의 안보위협도 목격하며, 사이버공간에 대한 관심과 신뢰의 중요성에 대해서도 되짚어본 한 해였던 것 같습니다.

이에 금번 발간하는 2024년 디지털금융 및 사이버보안 이슈 전망 보고서에서는 디지털금융 관련 금융정책(Financial Policy), 보안위협(Security Threat), IT혁신(IT Innovation)을 체계적으로 진단하고 전체 이슈를 관통하는 키워드로 ‘금융보안 프렌들리’ 전략을 제시함으로써 핵심가치(Core value)를 전달하고자 하였습니다.

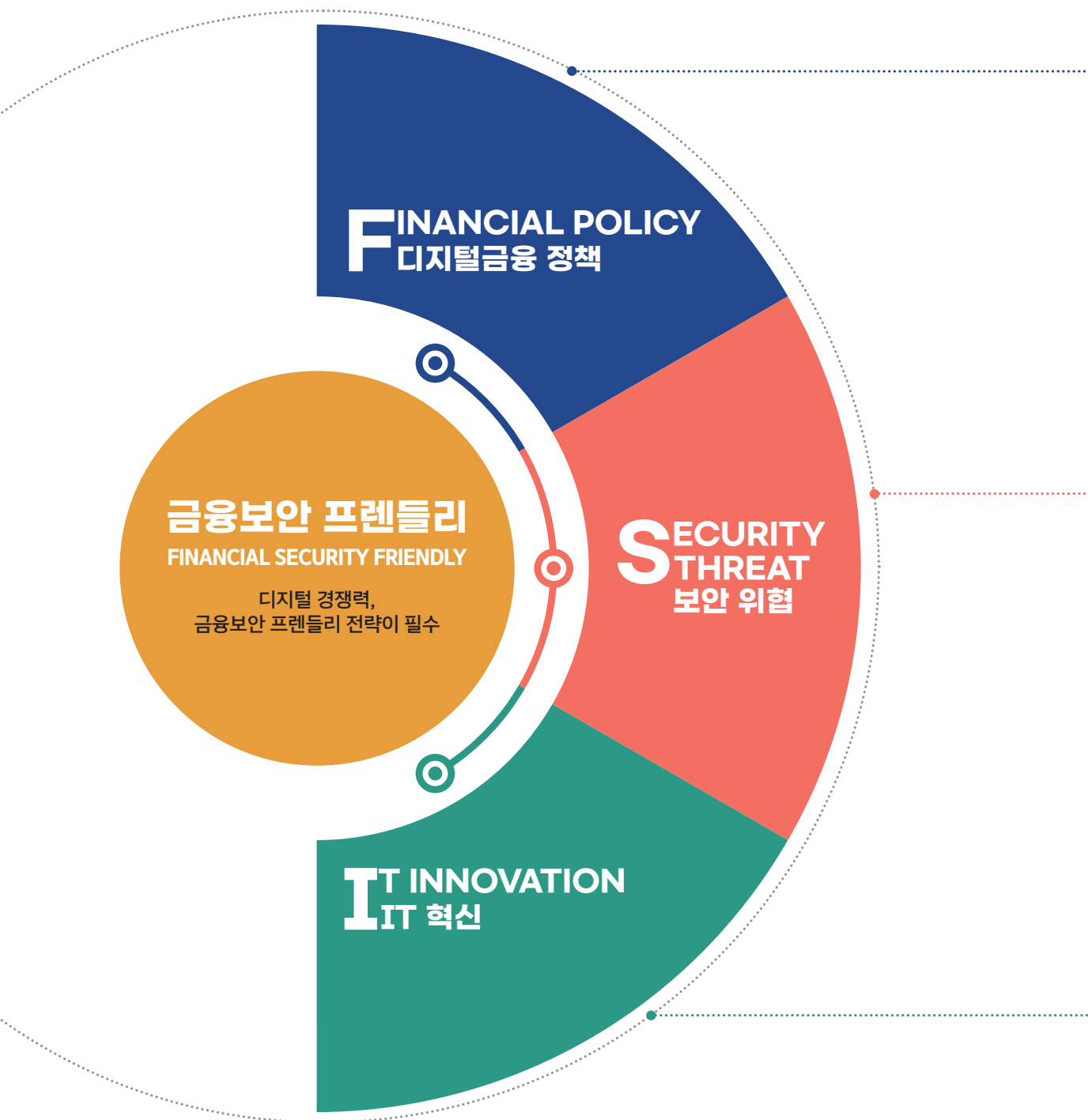
‘금융보안 프렌들리’란 금융회사, 금융소비자 등 금융생태계 전반이 ‘금융보안’을 소수의 전문 영역으로만 한정하지 않고 우리 일상 속에서 신뢰와 떼어낼 수 없는 핵심가치로 여기고 인식하자는 의미입니다.

날로 지능화·고도화되고 있는 금융보안 사고를 원천 차단하는 것이 불가능한 상황에서 지금껏 ‘편의성’을 선두로 외연이 확장된 금융 서비스를 되짚어 본다면, 이제부터 쏠 금융생태계는 편의성의 가치만큼 ‘보안성’의 가치에 주목해야 하는 시점이 되었습니다. 세계경제포럼(WEF)에서도 앞으로 필요한 국제 표준역량에 IQ(지능지수), EQ(감성지수)를 넘어 디지털 안전과 보안을 포괄하는 개념인 DQ(디지털지능) 역량의 중요성을 제시한 바가 있습니다.

모쪼록 이번 이슈 전망 보고서를 통해 앞으로 금융회사, 금융소비자가 금융보안을 특정 기술의 영역으로 한정하지 않고 일상 업무와 생활 속에서 보편적·필수적으로 고려해야 할 가까운 가치로 인식하며 다가올 2024년에 대비하여 금융보안과 한걸음 더 가까워지는데 도움될 수 있기를 기대합니다.

2023년 11월

김 철 웅



2024 디지털금융 및 사이버보안 핵심이슈

디지털 경쟁력, 금융보안 프렌들리 전략이 필수 06

디지털금융 정책

더 이상 거스를 수 없는 패러다임, 자율보안체계 전환 08

깨지지 않는(anti-fragile) 탄력성, 사이버복원력 10

클라우드 마이그레이션, 하드웨어 넘어 소프트웨어로 12

보안 위협

공격채널의 다양화, 영역을 넘나드는 하이브리드 위협 고조 14

S/W 공급망 공격 성행, SBOM의 중요성이 강조 16

피싱 범죄, '내 얼굴과 목소리까지도?' 딥페이크 기술 악용 18

IT 혁신

모든 것을 담는다, 디지털지갑 경쟁 가속화 20

AI의 안전성과 신뢰성 확보, 책임감 있는 AI 구현 22

사물과 디지털금융의 만남, 금융 사물인터넷(FoT) 24

참고문헌 26

디지털 경쟁력, 금융보안 프렌들리 전략이 필수

01

AI 등 新기술 적용으로 디지털금융이 복잡해지고 있고 이에 비례하여 보안 관리영역도 지속 확대되고 있는 상황이므로, 이제 금융보안을 소수의 전문 영역으로만 한정하지 않고 일상 업무와 생활 속에서 당연히 고려해야 할 핵심가치로 인식할 필요.

1. 이슈 분석

● 디지털이 지배하는 금융환경, 전사적인 보안의 가치가 발현되는 시점

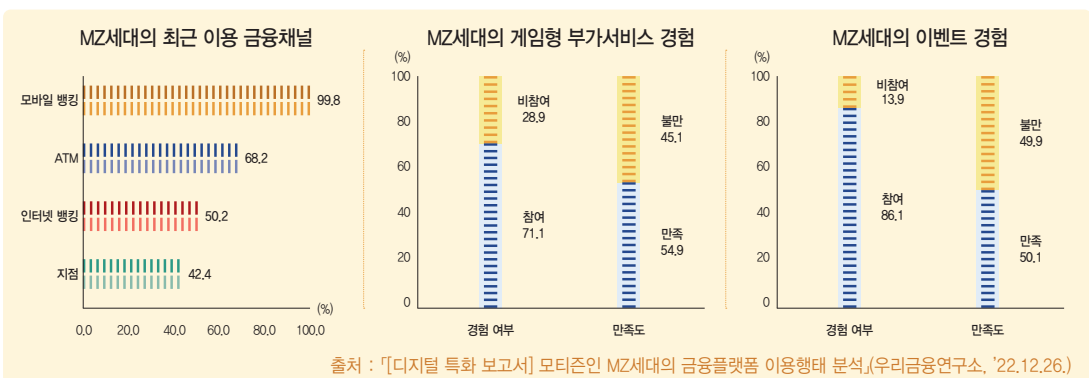
디지털금융 혁신의 일상화로 금융보안은 특정 전문조직이 관리하는 '통제'의 관점에서 누구나 필수로 여기는 '신뢰'의 가치로 진화해야 하며, 편의성과 보안성에 대한 균형적인 접근이 요구

금융권은 능동적 보안문화 형성을 위해 기존 경직적인 보안업무 형태를 쏠 직원이 참여 가능한 Bottom Up(상향식) 방식으로 전환을 시도(모의해킹 경진대회, 버그바운티¹⁾ 개최 등)

● 금융소비자의 능동적 보안 인식을 높일 수 있는 보안문화 형성 필요

'간편함', '실리'를 주요 가치로 추구하는 2030(MZ)세대가 디지털금융의 핵심 소비 주체로 등장²⁾함에 따라, 금융보안도 자발적으로 실천해야 하는 개념으로 접근성을 높일 필요

2030(MZ)의 금융서비스 이용행태



고령층 등 디지털 소외 계층은 피싱과 같은 사회공학적인 기법³⁾에 상대적으로 취약하므로, 금융권은 이들이 디지털 금융을 이해⁴⁾하고 보안의 필요성을 상시 인지할 수 있도록 노력

1) 버그바운티(Bug Bounty) : 보안취약점을 찾아내기 위해 모두에게 공개적으로 공격을 요청하고 유의미한 취약점을 찾아낸 제보자를 포상하는 제도

2) 2030(MZ)세대가 이끌며(Zgeneration drive) 급격한 변화와 합종연횡이 벌어지는(Zig Zag) 새로운 기반의 금융(Zero Base)을 '자이낸스(Z+Finance)'로 명명

3) 기술적인 방법이 아닌 사람 사이의 심리·사회적 관계를 이용해 정보를 캐내는 기법으로 사람의 취약점을 공격

4) 22년도 우리나라 성인의 디지털 금융이해력 점수는 42.9점으로 일반 금융이해력 점수(66.5점)를 크게 하회하며, 세대별로는 30대(45.0점) 등 젊은 세대에 비해 70대(36.0점) 등이 낮은 것으로 조사(출처 : '2022 전국민 금융 이해력 조사(한국은행·금융감독원, '23.3.29.)

2. 전망 및 대응 전략

● [금융회사 등] 금융보안 프렌들리(Friendly) 전략의 이행

금융보안은 더이상 투입되는 전문자원만으로 완벽할 수 있다고 장담하기 어려운 영역으로 보안 사각지대가 발생할 수 밖에 없음을 인정하고 항상 주의깊게 살펴볼 필요

금융회사 등은 정보보호 조직이 통제하는 기술적 영역을 벗어나 임직원 모두가 필수적으로 보안을 체득하고 일상에서 이를 적용할 수 있도록 금융보안 프렌들리(Friendly) 전략을 수립 · 이행할 필요

※ 가트너(Gartner)는 「23년 9가지 주요 사이버 보안 트렌드」에서 27년까지 기업의 절반이 '인간중심' 보안 설계를 채택할 것으로 전망(보안을 인간중심으로 설계하여 편의성과 자율성을 보장하면서도 일정 보안수준을 유지)

인간중심보안(PCS : People Centric Security) 개념 및 원칙

6대 원칙

책임성 Responsibility	보안에 대한 책임은 모든 임직원에게 있음.
자율성 Autonomy	임직원의 행동은 스스로 결정하고 책임의식이 전제되어야 함.
책임추적성 Accountability	정보보호에 대한 책임은 정보 소유자에게 있음을 명확히 해야 함.
비례성 Proportionality	보안 대책은 위험에 비례하여 수립해야 함.
투명성 Transparency	보안 대책은 모두에게 공유되어야 하며 임직원 동의를 기반으로 함.
즉시성 Immediacy	부정 행위에 대해서는 즉각적인 제재 등이 필요함.

출처 : 「인간중심보안 프레임워크 1부」(인간중심보안포럼, '22.1.19.), 「Gartner Top Strategic Cybersecurity Trends 2023」(Gartner, '23.4.19.)

● [금융소비자] 보안을 필수불가결한 생활습관으로 관념화

디지털금융에서의 보안은 서비스 제공자인 금융회사 등의 노력과 더불어 이를 이용하는 금융소비자의 보안인식과 실천의지에 비례해 강화되는 분야

건강을 위해 손 씻기와 같은 위생준칙을 지키듯, 금융소비자는 보안을 안전한 디지털금융을 위한 생활습관으로 인지(사이버위생)하고 일상에서 필수불가결하게 실천할 수 있는 가치로 인식할 필요

사이버위생(Cyber hygiene)의 개념

美 상무부 산하 표준기술연구소(NIST)에서는 '사이버 하이젠(Cyber Hygiene)의 중요성을 권고하고 있으며, 美 카네기멜론대는 건강한 삶의 기본인 '개인위생'의 빔대어 보안을 질서있는 디지털서비스의 근간이 된다는 의미로 '사이버 위생(Cyber Hygiene)'으로 명명



출처 : 「Critical Cybersecurity Hygiene: Patching enterprise」(NIST, '20.3.20.), 「What is Cyber Hygiene?」(Carnegie Mellon University, '19.3.7.)

더 이상 거스를 수 없는 패러다임, 자율보안체계 전환

02

급변하는 금융IT 환경변화에 맞춰 정부는 목표·원칙 중심의 규제, 위험기반 보안을 강조하는 자율보안 체계로의 전환을 추진. 자율보안체계의 성공적 전환을 위해서는 금융회사 등이 자체 보안역량을 제고하는 노력을 병행할 필요.

1. 이슈 분석

● 디지털금융 시대, 사전통제 방식의 금융보안 규제는 한계

클라우드, AI 등 新기술 출현으로 그간 변화에 소극적이던 금융IT 환경이 빠르게 진화하고 있으며, 이에 비례해 보안사고 위험도 커지고 있어 금융보안의 중요성이 더욱 강조

반면, 현행 금융보안 규제는 사전 통제방식의 세세하고 경직적인 규제로 금융IT 환경 변화를 신속하게 반영하지 못하며, 새로운 보안위협에 효과적으로 대응하는데 한계

사전통제 방식의 금융보안 규제 (예시)

구 분	규제 내용
건물 및 전산실	<ul style="list-style-type: none"> • 비상 시에 대비하여 정전대비 유도등 설치 • 전원실 등 주요 설비시설에 자물쇠 등 출입통제장치 설치 • 전산실 공조설비 상태 점검을 위해 압력계, 온도계 등 설치 • 정전에 대비하여 조명설비 및 휴대용손전등 비치 등
정보처리시스템	<ul style="list-style-type: none"> • DB, 운영체제 등은 유지보수관리대장을 작성 및 보관 • 주요 정보처리시스템에 대해 운영매뉴얼을 작성 등
기타	<ul style="list-style-type: none"> • 전산직무를 분리·운영 (프로그래머/오퍼레이터, 응용프로그래머/시스템프로그래머, 시스템 보안관리자/시스템프로그래머 등) • 내부IP 주소는 사설IP 주소로 사용 등

● 정부 주도로 자율보안체계로의 전환을 추진

정부는 금융권의 안전한 디지털 전환을 지원하고 新기술 보안위협에 능동적으로 대응할 수 있도록 「금융보안 규제 선진화」 정책을 마련하고, 자율보안체계로의 전환을 추진

규제 선진화 정책에는 금융회사 등이 규제준수라는 소극적 태도를 벗어나 자율보안체계를 확립할 수 있도록 ①보안 거버넌스 개선, ②보안규제 정비, ③관리·감독 선진화를 기본방향으로 제시

「금융보안 규제 선진화」 기본방향

1 보안 거버넌스 개선

- ① 금융보안을 금융회사 등의 전사적 차원에서 준수하는 **핵심가치**로 제고
- ② 보안체계를 리스크 기반의 **“자율보안체계”** 로의 전환 추진

2 보안규제 정비

- ① **목표·원칙 중심**으로 규제를 전환하고, 세부사항은 가이드 형태로 전환
- ② 자율보안체계 미구축 또는 보안사고 발생 등의 경우 **사후책임**을 강화

3 관리·감독 선진화

- ① 보안규정 위반여부 감독 중심에서 자율보안체계 수립·이행 등에 대한 **검증 중심**으로 전환
- ② 금융회사 등의 보안 거버넌스 개선 및 자율보안체계로의 이행 **컨설팅 기능 강화**




* 출처 : 「급변하는 IT환경에 탄력적으로 대응할 수 있도록 금융보안 규제 선진화를 추진하겠습니다.」(금융위, '22.12.27.)

2. 전망 및 대응 전략

● 위험(리스크)기반 자율보안체계로의 전환 본격화

금융보안 규제가 세세한 열거식 규정(rule) 중심에서 목표·원칙 중심으로 합리화될 것이며 사전통제로 보안사고를 100% 예방할 수 없는 현실이므로, 국내 금융보안 정책도 실패용인접근(non-zero failure approach)의 불가피성을 인정하고 위험(리스크)기반 자율보안체계로의 전환이 본격화

해외 주요국의 위험기반 자율보안체계 정책 사례

국가	담당기관	규제 명칭	주요 내용
 EU	유럽은행 감독청	ICT 위험평가 가이드라인	은행에서 ICT시스템 관련 보안위험을 적절히 다루는지 평가
 미국	FFIEC	비즈니스 연속성 관리 핸드북	규모 및 복잡성에 따라 업무연속성 계획을 수립하고 시나리오 기반으로 평가 수행
	뉴욕주 금융서비스국	23 NYCRR 500 개정안	사업·기술 변화가 보안성에 중대한 영향을 미칠 때마다 위험평가 실시 ※ 대형사는 최소 3년 주기로 위험평가 수행
 캐나다	연방 금융감독원	운영 위험 관리 가이드라인	위험관리를 운영복원력 달성을 위한 핵심으로 규정하고 전사적 위험관리체계 요구

자율보안체계 전환 과정에서 이사회·CEO의 금융보안 책임성을 강조하는 거버넌스 확립, 전사적 위험관리 체계 도입, 사고 시 신속한 대응을 보장하는 사이버복원력 확보 등이 주요 추진과제로 제시될 전망

● 자율보안체계의 성공적 정착을 위해서는 자체 보안역량 강화가 핵심

금융권은 그간 보안을 규제 준수라는 소극적 관점에서 바라왔으나 자율보안체계로 전환 시 보안 세부사항을 스스로 판단하고 대응해야 하므로 자체 보안역량 확보가 중요¹⁾

과거와 달리 보안이 디지털 경쟁력을 좌우하는 핵심 요소로 부각되고 있으므로 금융회사 등은 보안에 대한 인적·물적 투자는 물론 성숙한 사내 보안체계 및 문화 형성을 위해 노력할 필요

건전한 보안 위험관리 12대 원칙

- 원칙1. 이사회는 행동기준과 인센티브 설정 등 위험관리 문화를 구축해야 함
- 원칙2. 은행의 성격, 규모, 복잡성, 리스크 등 여러 요인에 따라 운영리스크 관리 프레임워크는 달라질 수 있음
- 원칙3. 이사회는 운영리스크 관리 프레임워크를 효과적으로 이행할 수 있도록 보장해야 함
- 원칙4. 이사회는 감수하고자 하는 리스크의 선호도 및 성격·유형·수준 등을 명시한 성명서를 주기적으로 승인·검토해야 함
- 원칙5. 고위 경영진의 책임소재는 명확하고 투명하며 일관성 있어야 함
- 원칙6. 고위 경영진은 운영리스크를 포괄적으로 식별·평가하여 내재된 위험과 인센티브가 잘 이해될 수 있도록 보장해야 함
- 원칙7. 고위 경영진은 합의된 객관적인 원칙에 근거해 정책 및 프로세스 등 변화관리가 이루어질 수 있도록 하고, 관련 방어선 간 역할과 책임을 명확히 분배해야 함
- 원칙8. 이사회, 고위경영진, 비즈니스 조직 수준에서 적절한 리스크 모니터링 및 보고 메커니즘이 마련되어야 함
- 원칙9. 은행은 위험 완화 및 통제 환경을 위한 정책, 프로세스, 시스템을 갖춰야 함
- 원칙10. 은행은 운영리스크 관리 프레임워크와 연계된 견고한 ICT위험 관리 프로그램을 구현해야 함
- 원칙11. 은행은 비즈니스 연속성 계획을 수립하고 운영리스크 관리 프레임워크와 연계되어야 함
- 원칙12. 은행은 공개 공시를 통해 운영리스크 관리에 대한 접근방식과 리스크를 이해관계자가 평가할 수 있도록 해야 함

출처 : 'Principles for Sound Management of Operational Risk'(美 BIS, '23.4월)

1) 정부는 금융회사 스스로 임원별(CEO, CISO 등) 내부통제 책임영역을 사전에 구분·확정짓고 위험관리 노력을 이행할 수 있도록 책무 구조도(Responsibility Map) 도입 등 내부통제 제도개선 방안을 발표(「금융사고, 제재보다 예방에 주력」(금융위·감독원, '23.6.22.))

깨지지 않는(anti-fragile) 탄력성, 사이버복원력

03

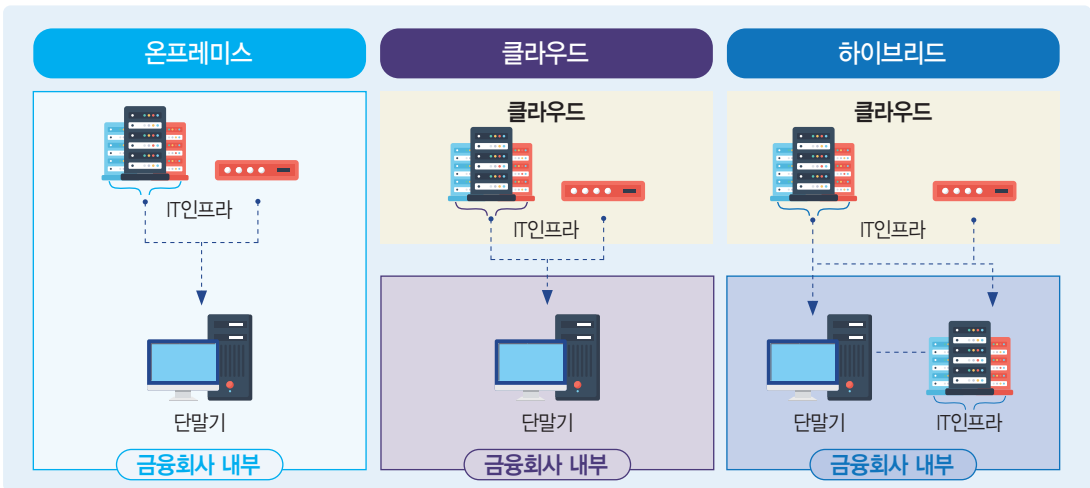
IT 복잡성이 증대되고 있으며, 공격기법도 고도화되고 있는 상황으로 보안위협을 완벽히 대응하고 차단하는데 한계. 이에 금융보안 사고 시 신속한 대응을 강조하는 사이버복원력 개념을 적용할 필요가 있으며 단계적으로 확대·강화할 필요.

1. 이슈 분석

● 금융권 디지털 일상화에 따른 IT 복잡성 증대

금융권은 그간 IT 인프라를 자체 구축·운영(온프레미스, On-Premise)하였으나, 클라우드 기술의 발전으로 온프레미스와 클라우드를 결합한 하이브리드 컴퓨팅 도입 등 IT 인프라 구성이 다양화되는 추세

온프레미스, 클라우드, 하이브리드 컴퓨팅 환경 개념도



AI나 클라우드 등 新기술 접목, 외부 오픈소스 기반 개발의 일상화, 마이데이터·오픈뱅킹·전자서명 등 제3자와의 상호 연결성 확대 등으로 금융IT 환경의 복잡성은 지속 증대되고 있는 상황

● 보안위협 예측가능성의 한계로 사이버복원력에 대한 관심 증대

각종 설정 오류나 하이퍼바이저¹⁾ 취약점 등 클라우드 환경에 특화된 보안위협이 심화되고 있으며, 생성형 AI 등을 악용한 공격도 현실화²⁾되는 등 디지털금융을 노리는 보안 위협이 고도화되는 추세

1) 하이퍼바이저(Hypervisor) : 단일 물리적 서버 환경에서 다양한 가상화 서버(머신)를 실행하는데 사용하는 S/W로 클라우드 기반 가상화 환경 구성에 필수 요소

2) 글로벌 보안기업인 체크포인트(Checkpoint)는 '23년 상반기 사이버위협 리서치 보고서에서 공격자는 피싱 이메일, 키입력 모니터링 멀웨어, 랜섬웨어 코드 생성 등에 생성형 AI기술을 활용하고 있다고 발표

IT 복잡성과 함께 보안위협도 다양화·고도화되고 있는 현실에서 보안위협을 완벽히 예측·대응하는데 한계가 있는 바, 사고 시 신속한 대응을 강조하는 사이버복원력에 대한 관심 증대

사이버복원력(Cyber Resilience) 개념

보안위협이나 공격이 발생되더라도 IT인프라(시스템 등)를 지속적으로 운영할 수 있는 능력을 갖추는 것으로, 기존 침해사고 예방 및 탐지에 더해 보안위협 대응능력을 극대화하는 것을 의미






2. 전망 및 대응 전략

● 금융보안 분야에 사이버복원력 개념 접목

미국, EU 등 해외 주요국은 보안위협을 포함한 사고대응의 한계를 인정하고 금융분야 디지털 운영복원력 도입을 정책적으로 추진

해외 금융권의 디지털 운영복원력 도입 정책 현황

국가명	정책명	정책 내용
 미국 (OCC)	운영복원력 강화를 위한 건전한 관행 지침('20년 제정)	대형 금융회사는 핵심업무에 대해 운영복원력을 갖출 것을 요구
 EU	디지털 운영복원력법 ('25.1.17. 시행 예정)	디지털 운영복원력 확보를 위해 위험관리, 운영복원력 테스트, 제3자 리스크 관리 강화 등을 규정
 싱가포르 (MAS)	기술위험 관리지침 ('21년 개정)	운영복원력 확보를 위해 위험관리 프레임워크 마련, 보안 활동에 대한 IT 감사 등을 규정

국내도 사전 규제방식의 금융보안 정책을 사후규제·책임강화, 원칙중심의 규제에 개선을 진행하고 있는 상황에서 글로벌 규제 환경에 맞게 사이버복원력 개념의 적용 필요

● 금융권 환경에 맞는 단계적인 사이버복원력 설계·운영 중요

사이버복원력은 공격 대응을 위한 기술력 확보뿐만 아니라 보안 정책, 사내 보안문화 등 보안역량 전반의 제고 및 고도화가 요구되므로 단기간에 완벽하게 구축하기는 어려운 개념

금융회사 등은 자사 보안역량의 현주소를 정확히 진단하고, 비즈니스 환경 및 IT·보안 운영여건 등을 종합적으로 고려하여 사이버복원력 기준을 자체 설계하고 단계적으로 이행할 필요가 있으며, 개발(Dev)·보안(Sec)·운영(Ops)이 하나로 동작하는 데브섹옵스(DevSecOps)³⁾ 도입 등도 고려

사이버복원력 구축 시 필요사항(예시)

- ① 이사회 및 C-level에게 직위에 걸맞는 금융보안 역할·권한 및 책무를 부여하도록 거버넌스 체계 마련
- ② 위험의 식별·평가·관리·개선으로 이어지는 일련의 위험관리 체계를 전사적으로 구축 및 운영
- ③ 금융서비스 중단 시 심각한 위험 또는 피해를 발생시킬 수 있는 '주요 전자금융 기반시설'에 대하여 중단 허용한도를 미리 설정
- ④ 가상 사이버공격을 수행하고 운영복원력 관점에서 대응하는 '위협 기반 침투테스트' 실시
- ⑤ 제3자 리스크 전이를 차단하기 위하여 규모가 크거나 집중리스크 등이 우려되는 '주요 제3자'에 대해 감사 강화 등

3) 데브섹옵스(DevSecOps) : 개발팀과 운영팀이 처음부터 보안을 염두에 두고 S/W 개발 프로세스의 모든 단계에서 긴밀하게 협력하는 개념

클라우드 마이그레이션, 하드웨어 넘어 소프트웨어로

04

정부의 규제샌드박스 정책 등에 따라 SaaS형태의 S/W 도입이 금융권에도 지속 확대될 것으로 전망. SaaS 관리 소홀이나 제3자 제공 앱 취약점 등 SaaS 이용에 따른 보안위협도 확산될 것으로 보여 철저한 보안대책 마련이 필요.

1. 이슈 분석

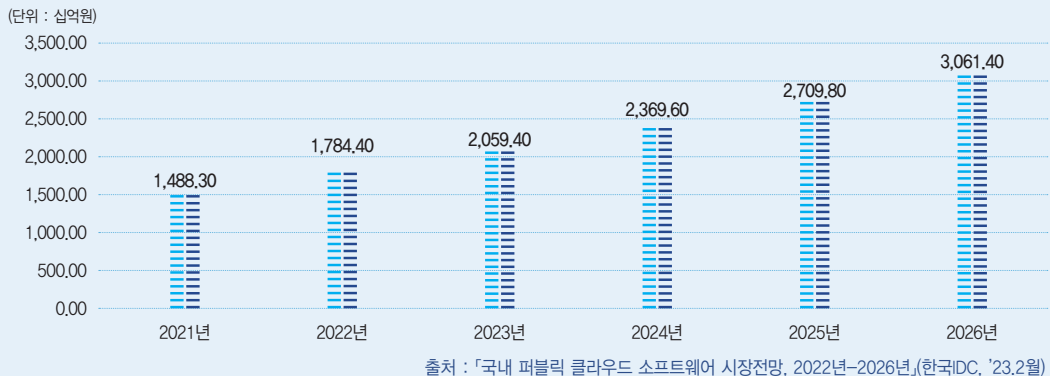
● SaaS(Software as a Service)형태의 S/W 도입이 확대

SaaS는 S/W 뿐만 아니라 이를 운영하는데 필요한 IT 인프라까지 일괄 제공하는 클라우드 컴퓨팅 형태로, 오피스 S/W와 같은 협업도구부터 인사정보나 ERP¹⁾, 보안관리 등 다양한 S/W가 SaaS로 제공되고 있는 상황

SaaS는 구독형태로 비용을 납부하므로 S/W 자체 도입에 비해 초기 소요비용이 적고, S/W 유지·관리에 대한 부담이 완화되는 등 장점이 있어 국내 기업의 SaaS 이용 비율은 지속 확산되는 추세

※ 정부는 '26년까지 국내 SaaS 기업을 1만개 이상으로 확대할 계획임을 발표(과기정통부, 「대통령 직속 디지털플랫폼 정부위원회」, '23.4.14.)

국내 SaaS 시장 규모(2021~2026년)



● 정부는 규제샌드박스를 통해 금융권의 내부망 SaaS 이용을 허용

정부는 금융회사 등이 내부망에서 SaaS를 이용할 수 있도록 규제샌드박스를 통해 망분리 규제 예외를 허용하였고, 일부 금융회사 등이 혁신금융서비스 대상으로 지정

다만, 보안성에 대한 우려가 있어 고객·거래정보를 다루지 않는 비중요 업무에 한해 SaaS 이용을 우선 허용하였고, 부가조건으로 정보보호를 위한 보완장치를 마련

1) ERP(Enterprise Resource Planning) : 기업 내 생산, 물류, 재무, 회계 등 경영활동 프로세스들을 통합적으로 관리·공유해주는 전사적 통합 자원관리시스템을 의미

내부망 SaaS 이용 허용업무 범위(예시)

구 분	대상 S/W
협업도구	오피스S/W, 메신저, 디자인, 화상회의, 이메일, 그룹웨어 등
ERP	인사관리, 성과관리, 계약관리, 재무회계, 지출결의 등
기타	마케팅 분석, 금융지표 분석, 교육 관리, 자료번역, 설문조사 등



2. 전망 및 대응 전략

● 금융권의 SaaS 수요 확대에 대비한 정책적 지원 필요

대부분의 S/W가 비용 대비 효용성이 높은 SaaS로 제공되고 있으며 온·오프라인 하이브리드 형태로 근무환경이 변화되고 있는 현실 등을 감안할 때, 금융권의 SaaS 이용 수요는 빠르게 확대될 전망

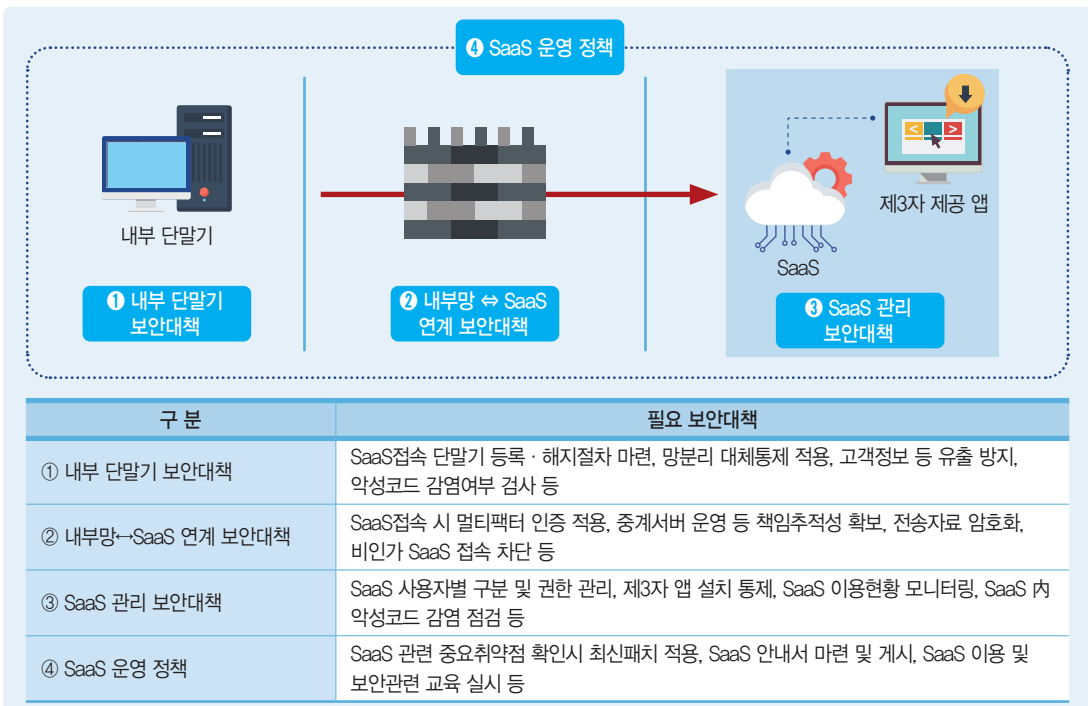
정부는 규제샌드박스를 통해 내부망 SaaS 이용에 따른 문제점 등을 실증하고 있는 상황으로, 금융권 SaaS 수요에 맞춰 SaaS 이용 범위 확대 등 정책 마련을 유연하게 논의할 필요

● SaaS 이용으로 발생될 수 있는 보안위협에 철저히 대응

SaaS 이용으로 업무환경이 효율화되는 동시에 IT·보안 조직이 통제해야 할 영역 또한 크게 확대됨에 따라, 관리 소홀 등에 의한 보안 사각지대가 발생될 가능성이 존재

SaaS 설정 오류나 SaaS 연계된 제3자 제공앱 취약점 등을 통해 비인가자 접근 데이터 유출 등이 발생되지 않도록 SaaS 이용 보안대책을 철저히 수립·이행해야 하며 SaaS 이용 내부 직원에 대한 주기적인 보안 교육 실시 등이 필요

내부망 SaaS 이용 관련 필요 보안대책(예시)



공격채널의 다양화, 영역을 넘나드는 하이브리드 위협 고조

05

온·오프라인을 연계한 하이브리드 위협의 부상과 더불어 공격도구에 AI 적용 등 하이브리드 위협이 더욱 지능화·고도화될 전망이다. 하이브리드 위협 대응을 위해 자체 보안역량 강화, 국가 간 및 민·관 협력의 중요성 등이 강조

1. 이슈 분석

● 온·오프라인 연계 공격 등 하이브리드(Hybrid) 위협의 부상

하이브리드 위협은 사이버 공간뿐만 아니라 물리적 영역까지 다양한 채널이 동시에 이용되어 피해를 초래하는 것으로, 온·오프라인 연계를 바탕으로 공격주체의 노출을 최소화하며 전략적 목적을 달성하는 것이 특징

재택근무, 클라우드 등이 혼재된 업무 형태의 복잡성 증대, 태블릿기기, 스마트폰 등 업무 기기의 다양화 등으로 인해 공격대상 범위가 과거에 비해 방대해진 점도 하이브리드 위협을 가중

하이브리드 위협 사례(예시)



구 분	위협 내용
데이터센터 장애 확산	판교 데이터센터 화재로 의료기관·택시·쇼핑몰 등 실생활과 연계된 서비스가 일시 정지되었으며, 재난이 발생한 해당 사(社)를 사칭한 다양한 피싱공격이 수행
사회적 이슈 악용	코로나19 방역 증명서 발급, 선거 이슈 등 사회적인 관심사를 악용하는 형태로 악성코드 설치 등을 유도
오프라인 침투	공격자가 직접 공격 대상 회사에 고용되어 공격을 시도하거나, 악성코드가 설치된 제품을 납품하는 등 오프라인 연계 공격 시도
원격·재택 근무	원격·재택 근무가 일상화되면서 국내 주요 기관 원격접속 인프라에 대한 공격 시도

출처 : 각종 언론보도

● AI 등 新기술 적용으로 하이브리드 위협이 지능화될 전망

생성형 AI를 악용(웜 GPT, 사기 GPT 등)한 피싱¹⁾이나 악성코드 개발, 공격 대상에 허위조작 정보를 유통하는 등의 고도화된 기법을 통해 하이브리드 위협이 더욱 지능화되는 추세

※ 북대서양 조약기구 NATO는 데이터, AI, 양자기술 등 새로운 파괴적 기술인 EDT²⁾를 선별하고 EDT 기술 및 이용관련 위협에 대비할 것을 당부(NATO Science & Technology Organization, 「Science & Technology Trends 2020-2040」, '20.3.)

1) 영국 사이버 보안 기업인 다크트레이스(DARKTRACE)는 자사 고객사를 기준으로 수천 개의 활성 계정에서 생성형 AI를 이용한 신종 소셜 엔지니어링 공격(novel social engineering attacks)이 '23년 1~2월 동안 135% 증가했다는 분석 결과를 발표(DARKTRACE, 「Generative AI: Impact on Email Cyber-Attacks」, '23.4.3.)

2) EDT(Emerging and Disruptive Technologies) : 데이터, 인공지능, 자율성(Autonomy), 우주기술, 초음속기술, 양자기술, 생명공학 및 인간증강(Human Enhancement), 신재료(Materials) 등

AI 악용 공격도구(예시)



웜 GPT(Worm GPT)	사기 GPT(Fraud GPT)
채팅 기반의 생성형 AI로 피싱메일을 자동 생성하고 배포를 지원	스피어피싱(신뢰할 수 있는 발신자가 보낸 것으로 가장하는 이메일 공격)이나 악성코드 작성 등을 지원

국가 단위 해킹조직은 군사 공격에 앞서 사이버 공간을 공략하는 경향이 있어, 하드 킬(Kill) 뿐만 아니라 AI 등을 이용한 소프트 킬 방식의 능동방어체계(APS, Active Protection System)³⁾도 강조

※ 2022년~2027년까지 글로벌 APS 시장은 연평균 5.5% 성장을 성장할 것으로 예측되며 소프트 킬 시스템 부문이 시장을 주도할 것으로 예상(Research and Markets, 「Global Active Protection System(Soft Kill System, Hard Kill System, Reactive Armor) Markets, 2022-2027」, '22.8월)

하드 킬 VS 소프트 킬 개념

하드 킬(Hard Kill)	소프트 킬(Soft Kill)
물리적인 대응으로 목표물을 직접적으로 교란·파괴	물리적인 파괴 없이 해킹 등을 통한 전자적인 대응으로 목표물을 간접적으로 교란·무력화 ※ (예) 획득한 정보를 AI로 분석하여 위협에 대한 대응체계를 자동으로 생성

출처 : 각종 언론보도 등

2. 전망 및 대응 전략

● 하이브리드 위협에 대비한 공격 대응역량 강화가 더욱 중요

하이브리드 공격에 선제적으로 대응할 수 있도록 금융권에 위협이 되는 최신 공격사례를 사전에 선별·분석하고 신기술 분야 지식 획득과 주기적인 리스크 평가 수행 등 대응 역량을 자체 보유하도록 노력

AI나 빅데이터를 공격대응 기술에 활용하거나, 각종 이벤트를 연관분석하는 상관역량(Correlation Capability) 기법⁴⁾을 공격탐지에 적용하는 등 공격대응 기법도 고도화할 필요

AI 및 빅데이터를 활용한 공격대응 기술 사례

- (사례 1) 금융분야 통합보안관제센터에 AI, 빅데이터 등 최신 보안기술을 적용한 차세대 관제시스템을 구축
- (사례 2) 다크웹 상에서 각종 범죄데이터를 효과적으로 추출할 수 있는 다크웹 전용 AI 언어 모델 개발

● 하이브리드 위협 대응을 위한 국가 간, 민·관 협력이 요구

복잡·다양화되는 하이브리드 위협을 특정 분야 또는 영역만의 역량으로 완벽하게 대응하기에는 한계가 있으므로 정부, 전문기관, 민간 금융회사 등 간 긴밀한 협력이 요구

클라우드 사업자와 같은 글로벌 ICT 업체의 활용이나 국제적 해킹그룹의 공격 형태 등을 고려할 때 하이브리드 위협 대응을 위한 국가간 협력의 중요성도 강조

※ 미국, 독일, 프랑스, 영국 등 34개국은 Hybrid CoE(The European Centre of Excellence for Countering Hybrid Threats)에 참가하여 하이브리드 위협에 공동 대응(Hybrid CoE, 「Establishment」, '23.10.5.)

3) 능동방어체계(APS, Active Protection System) : 공격을 받기 전에 능동적으로 위협체를 무력화해 공격을 막는 방어 체계로 방어 방식에 따라 하드 킬과 소프트 킬로 구분

4) 상관역량(Correlation Capability) 기법 : 더욱 복잡해지고 서로 결합하는 형태를 지닐 것으로 보이는 지능형 하이브리드 위협에 대비하여 각 공격을 개별로 탐지하지 않고 공격 탐지 이벤트를 서로 연관시켜 분석하는 상관 역량(「Identifying Emerging Cyber Security Threats and Challenges for 2030」, ENISA, '23.3월)

S/W 공급망 공격 성행, SBOM의 중요성이 강조

06

금융권에 오픈소스를 활용한 S/W 개발이 일상화되면서, S/W 内 구성요소의 보안취약점을 공격하는 S/W 공급망 공격이 주된 보안 위협으로 부상. S/W 공급망 공격 예방을 위해 SBOM(Software Bill of Materials)에 대한 관심 및 활용이 금융권에 본격화될 전망.

1. 이슈 분석

● S/W 공급망이 금융권의 주요 공격대상으로 부각

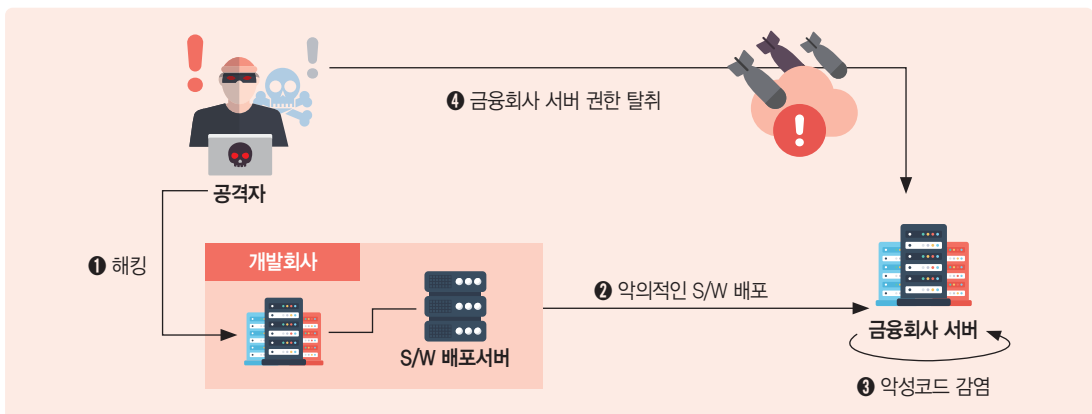
금융권에 오픈소스 등을 활용한 S/W 개발이 일반화되면서, 금융회사 등에 비해 상대적으로 보안이 취약한 S/W 공급망을 대상으로 한 공격이 성행

공격자는 오픈소스 저장소 内 악성코드 유입이나 S/W 개발회사를 해킹하여 정상적인 S/W를 변조하는 등의 다양한 형태로 S/W 공급망 공격을 시도

S/W 공급망 공격 최근 사례

- (사례 1) NPM (S/W 개발용 패키지 관리자) 대상 공격('23.4~5월)
 - NPM¹⁾에 금융회사 업무와 관련된 악성 패키지를 업로드(등록) → 악성패키지를 다운로드 받아 실행한 금융회사 등의 업무 권한을 탈취
- (사례 2) 3CX(화상회의 S/W 공급사) 대상 공격('23.3월)
 - 공격자가 3CX를 해킹하여 화상회의 S/W 설치파일에 악성코드를 주입 → 화상회의 이용을 위해 S/W를 설치하는 경우 악성코드에 감염

S/W 공급망 공격 개념도



1) NPM(Node Package Manager) : 자바스크립트 프로그래밍 언어를 위한 패키지 관리자로 공개용 패키지 및 개인패키지 DB로 구성

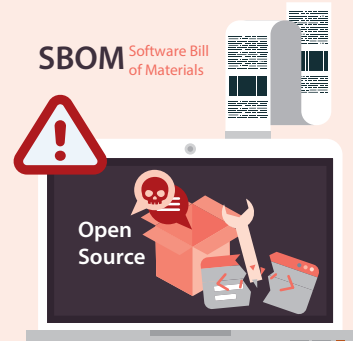
● S/W 공급망 공격 예방대책으로 SBOM에 대한 관심 증대

S/W 공급망 공격은 정상적인 S/W 전달 경로(S/W 개발회사 ↔ 금융회사)를 이용하므로, 금융회사 등이 이를 사전에 파악하고 대응하는데 어려움이 존재

이에, S/W 內 구성요소 및 패키지 정보 등을 목록화한 명세서인 SBOM이 S/W 공급망 보안성 강화를 위한 방안으로 대두

SBOM 데이터 기본 구조

구분	내용
작성자 이름	SBOM 데이터를 만든 주체의 이름
작성일시	SBOM의 최근 업데이트 일시
공급자 이름	SBOM 구성요소의 공급자 이름
구성요소 명	구성요소의 이름
버전	구성요소 버전
구성요소 해시(Hash)	구성요소의 해시값 목록
고유 식별자	구성요소 식별 및 DB 조회 키
종속성 관계	SBOM 구성요소 간 관계



출처 : 美 전기통신정보청(NTIA : National Telecommunications and Information Administration)

SBOM과 취약점 정보(DB)를 상호 연계할 경우 S/W 內 취약요인 등을 신속하게 파악할 수 있어 미국, EU 등 해외 주요국은 국가안보 관점에서 SBOM 활용을 정책적으로 추진 중

해외 주요국의 SBOM 관련 정책

국가	법령 명칭	주요 내용
미국	행정명령 14028	S/W 공급망 보안 개선을 위해 연방기관이 S/W 조달 시 SBOM 제출을 의무화하고 SBOM 최소 구성요소를 공표('21.5.)
EU	사이버 복원력법	S/W 취약점 분석을 용이하게 하기 위해 S/W 제조업체의 SBOM을 포함한 S/W 구성요소 식별 및 문서화를 명문화('22.9.)

2. 전망 및 대응 전략

● S/W 공급망 공격 예방을 위해 SBOM 활용이 본격화될 전망

금융권에 대한 S/W 공급망 위협이 현실화되고 있어 모바일뱅킹 앱(App) 등 주요 금융 S/W에 대한 SBOM 활용이 본격화될 것으로 예상

S/W 개발 전 과정(개발→테스트→배포→유지보수)에서 SBOM을 통해 오픈소스 취약점을 확인하거나, 제3자가 개발한 S/W 도입 시 SBOM을 제출받아 S/W 취약 요인을 상시 관리할 필요

● 금융권 환경에 맞는 SBOM 정책 및 관리체계 마련 필요

SBOM을 통해 S/W 공급망 공격을 예방하기 위해서는 SBOM과 보안취약점 정보(CVE²⁾ 등 간 상호 연계가 필수 요소
금융권의 체계화된 SBOM 활용을 위해서는 금융 S/W에 대한 구성요소 등을 SBOM을 활용하여 목록화하고, 이와 연계된 보안취약점 정보를 분석·제공(Finance VEX³⁾)하는 SBOM 프레임워크 마련 필요

2) CVE(Common Vulnerabilities & Exposures) : 공개적으로 알려진 보안취약점 및 기타 정보보안 결함요인에 대한 목록으로 美 MITRE Corporation(사이버보안 비영리법인)에서 관리

3) VEX(Vulnerability Exploitability eXchange) : S/W 구성요소별 보안취약점에 대한 상세 분석정보(VEX)를 의미하며, 美 NTIA에서는 VEX를 SBOM 정보와 연계하여 활용 중

피싱 범죄, ‘내 얼굴과 목소리까지도?’ 딥페이크 기술 악용

07

개인의 목소리, 얼굴 등을 진짜인 것처럼 제작하는 딥페이크(Deepfake) 기술의 발전과 더불어 이를 악용한 금융사기 범죄도 증가할 것으로 예상. 금융권은 딥페이크 악용에 선제적으로 대응하여야 하며, 관련 정책 마련도 검토 필요.

1. 이슈 분석

● 딥페이크(Deepfake) 기술의 발전에 따른 부작용 우려 증대

딥페이크 기술의 발전으로 AI에 대한 전문적인 지식이 없는 사람도 쉽게 가짜 음성(Deepvoice)*이나 영상 등을 제작할 수 있어 다양한 범죄에 악용될 우려

* 음성 AI 기술 중 음성합성¹⁾ 또는 변조기술²⁾을 사용해 가짜 목소리를 진짜인 것처럼 제작하는 딥보이스는 딥러닝(Deep Learning)과 가짜 음성(Fake Voice)의 합성어로 실제 목소리와 유사한 목소리 구현이 가능

딥페이크 기술이 정교화될수록 사람의 합리적인 주의만으로는 진위 파악이 어려워 신원 사기, 인증 우회 등 딥페이크를 악용한 사회공학(social engineering) 공격 등이 발생될 가능성 존재

딥페이크 악용 사례



● 딥보이스(Deepvoice)를 통한 금융사기 확산에 주의 필요

딥보이스를 악용한 피싱범죄 검거 사례는 아직 확인되지 않았지만, 딥보이스를 통해 타인의 목소리를 범죄자가 쉽게 사칭할 수 있어 보이스피싱 등 금융사기에 악용될 위험이 큰 상황

1) 음성합성 : 특정 음성의 일부(호흡, 속도, 억양 등)만 추출하여 Text 전체를 해당 음성으로 제작하는 기술 → TTS(Text-to-Speech)로 명명

2) 음성변조 : 화자의 음성(source speaker)을 원하는 다른 화자(target speaker)의 음성으로 변환하는 기술(음성 A → 음성 B로 변조)

답보이스 악용 금융사기 시나리오(예시)

구 분	주요 내용
보이스피싱	<ul style="list-style-type: none"> • (악성앱 설치) 악성앱으로 개인의 음성 및 통화내역 파일을 획득하고, 목소리를 분석하여 보이스피싱에 악용 • (SNS 접근) SNS에 있는 개인의 음성 및 영상을 통해 목소리를 복제 • (금융·공공기관 사칭) 금융·공공기관의 안내음성을 녹음하고 이를 복제하여 기관을 사칭
화자인증 우회	<ul style="list-style-type: none"> • 답보이스 기술로 가짜 음성을 제작하여 화자인증(개인의 음성정보 특징을 활용한 인증) 우회 시도
생성형AI 기술과 연계	<ul style="list-style-type: none"> • 챗GPT 등 생성형 AI와 답보이스간 연계를 통해 타인 모방이 가능하며, 공격자는 챗GPT를 통해 피싱 메시지 등을 생성

답보이스 피해 예방을 위해 정부는 대국민 주의를 지속 당부하고 있으며, 정상 목소리와 답보이스를 통해 생성한 가상의 목소리를 탐지·대응할 수 있는 기술개발이 진행* 중(초기 단계)인 상황





* 대검 과학수사부는 답보이스 탐지기술 개발을 국책과제로 추진('24년~'27년) 등

2. 전망 및 대응 전략

● 딥페이크 보안성 확보를 위한 정책 마련 검토

미국, EU 등 해외 주요국은 딥보이스를 포함한 딥페이크 악용에 대비해 보안성 평가, 투명성 확보 등 다양한 정책을 마련하여 시행

딥페이크 관련 해외 정책 동향

국가명	주요 내용
 미국	딥페이크 관련 연방법안 입법이 다수 진행되었으며, 각 주(州) 별로 딥페이크 범죄에 대한 자체 규정을 마련
 EU	딥페이크 규제를 자율 → 강제력 있는 입법으로 강화하는 추세이며, 플랫폼 기업에 딥페이크에 대한 책임을 부여 ※ (예) 「디지털서비스법」('24.1월 시행), 「허위정보 행동규약」('22.6월 개정) 등
 영국	디지털문화미디어포츠부(DCMS)는 딥페이크 포르노 등 유해한 콘텐츠에 대해 온라인서비스 제공자가 이용자 보호조치를 취하도록 의무 부과 ※ (예) 「온라인 안전법」('22.11월 발의)
 중국	세계 최초로 딥페이크에 대한 포괄적인 규제를 시행하는 등 딥페이크를 강력하게 규제 ※ (예) 「딥페이크 규정」('23.1월 시행), 「온라인 음성 및 영상 정보 서비스 관리 규정」('20.1월 시행)

국내는 선거, 음란물 외 딥페이크 악용에 대한 구체적인 정책이 없는 상황*으로 금융권은 딥페이크를 통한 금융사기 예방을 위해 콘텐츠 제작·활용 시 보안기준 마련 등을 검토할 필요

* 음란물 및 선거 관련 법령·기준이 마련되어 있으며, 딥페이크 피해자 권리보장 등을 위한 법안이 발의 중(「딥페이크 처벌법」('20.6월 시행), 「딥페이크 영상 관련 법규운용기준」('22.1월 발표))

● 딥보이스 악용에 대한 금융권의 선제적 대응 필요

딥보이스를 악용한 보이스피싱 등 금융사기 범죄가 본격화될 것으로 보이므로 금융소비자 홍보 강화를 비롯한 금융사기 피해 예방 대책을 선제적으로 마련하고 추진

AI 기술의 발전과 더불어 금융분야에 딥보이스 기반 서비스(AI 행원, AI 음성봇 기반 고객상담서비스 등) 도입도 확대될 것으로 예상되므로 서비스 설계 단계부터 발생할 수 있는 보안위험 등을 사전 파악하고 대응하는 것이 중요

모든 것을 담는다, 디지털지갑 경쟁 가속화

08

금융권은 생활밀착형 모바일플랫폼 전환의 구심점으로 인증서, 결제, 전자문서 등 다양한 서비스를 제공하는 디지털지갑을 전략적으로 확대·강화. 디지털지갑 이용 확대에 따라 보안위협도 증대될 것이므로 철저한 보안대책 마련이 요구.

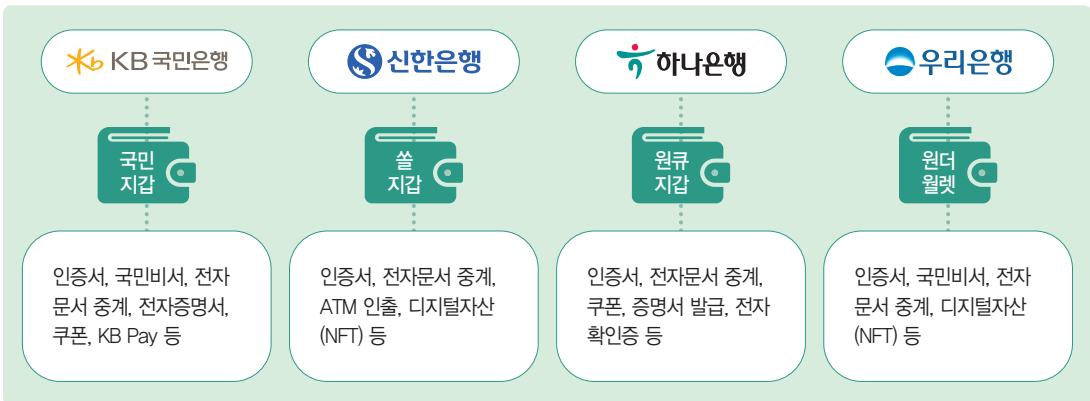
1. 이슈 분석

● 금융권 디지털지갑 사업영역 확대 추진

금융회사 등은 자체 인증서¹⁾ 확보 노력과 더불어 이를 기반으로 본인확인, 결제, 전자문서 중계²⁾ 등 금융·비금융 서비스를 모바일 앱에서 통합·제공하는 디지털지갑 사업을 활발하게 추진 중

디지털지갑은 고객을 묶어두는 잠금효과³⁾는 물론 고객 이용 데이터를 기반으로 맞춤형 금융서비스 제공도 기대할 수 있어 금융회사의 생활밀착형 모바일플랫폼 전환 전략에 구심적 역할을 수행

은행권의 디지털지갑 추진 사례



● 디지털지갑 대상 공격을 통한 2차 피해 발생 우려

디지털지갑은 인증서 등 신원확인 매체뿐만 아니라 정부 증명서(주민등록등본 등)와 같은 민감 정보도 보관하므로 전자적 침해 발생 시 개인정보 유출은 물론 신원도용, 사기 등 광범위한 2차 피해도 유발

향후, 모바일 신분증⁴⁾ 등 디지털지갑에 담기는 정보나 서비스가 지속 확대될 것으로 예상되므로 디지털지갑이 주된 공격대상이 될 우려

1) 금융권 전자서명인증사업자 지정현황 : 은행(6개사), 전자금융업자(4개사), 금융공동(2개사)(출처 : 한국인터넷진흥원(23.9월 기준))

2) 금융권 공인전자문서중계자 지정현황 : 은행(3개사), 카드사(1개사), 전자금융업자(4개사)(출처 : 전자문서통합지원센터(23.9월 기준))

3) 잠금효과(lock-in effect) : 어떤 상품 또는 서비스를 한번 이용하면 전환비용으로 인해 기존의 것을 계속 이용하게 되는 효과

4) 정부는 모바일 신분증을 국민이 자주 이용하는 민간 플랫폼에서도 사용할 수 있도록 민간 개방 계획을 발표(행정안전부, 「민관이 모여 모바일 신분증을 활용한 혁신 서비스 발굴 나선다」, '22.12.26)

디지털지갑 공격 목적

구 분	설 명
개인신원 사칭	<ul style="list-style-type: none"> 인증서 등 개인의 신원을 증명하는 매체를 탈취하거나 위·변조하여 금융거래, 공공·의료 서비스, 온라인 계약 등에서 개인을 사칭
개인정보 획득	<ul style="list-style-type: none"> 개인의 정부증명서(주민등록등본, 납세증명서 등)나 금융거래 증명서, 자격증 등을 탈취하여 타인 명의로 대출신청, 휴대폰 개통, 신용카드 발급 등을 진행 이름, 생년월일, 연락처, 주소, 가족 정보 등 디지털지갑에 저장된 개인정보를 획득하여 피싱 등 금융사기 범죄에 악용



2. 전망 및 대응 전략

● '24년은 금융권 디지털지갑 경쟁의 원년이 될 전망

기존 디지털지갑 제공 금융회사 등은 이용 고객 확대를 위해 서비스를 고도화할 것이며, 여타 금융회사 등도 자체 인증서 도입, 공인전자문서중계자 자격 취득 등 디지털지갑 사업을 단계적으로 추진할 전망

빅테크 기업이 이미 디지털지갑 시장을 선점하고 있는 상황에서 금융회사는 결제 등 자신만의 강점을 앞세워 점유율을 확대하는 등 디지털지갑 시장에서 금융과 빅테크 간 경쟁이 심화될 전망

빅테크 기업 디지털지갑 제공 서비스 내용

구 분	NAVER	kakao
서비스 명	네이버 NA	카카오톡 지갑
서비스 내용	인증서, 출입증, 전자증명서, 자격증, 학생·동문증, 결제(간편결제, 오프라인 결제, QR결제), 전자문서 중계, 멤버십, 송금 등	인증서, 학생증, 성인 인증, 자격증, 디지털자산(NFT), 전자문서 중계, 간편결제, 송금, 신용관리, 디지털 ID, 예약 관리 등

● 디지털지갑 보안성 강화를 통해 안전성 및 신뢰성 확보 필요

오프라인 지갑 분실 시처럼 디지털지갑에 침해가 발생될 경우 금전적 피해는 물론 신원도용 등 각종 사기에 악용될 수 있으므로 금융권은 금융거래에 준하는 철저한 보안대책 마련·이행이 요구

특히, 정부증명서 등 민감한 개인정보가 디지털지갑에서 처리되는 만큼 데이터 보호에 만전을 기하여야 하며 금융분야 특성에 맞는 디지털지갑 보안성 검토 및 검증체계 마련도 고려 필요

AI의 안전성과 신뢰성 확보, 책임감 있는 AI 구현

09

AI 기반 초개인화 금융서비스가 금융산업 전반으로 확산되는 추세로 AI의 안전성 및 신뢰성 확보 요구가 강조될 전망. 이에, 금융권은 책임감 있는 AI 구현을 위한 노력을 확대할 것이며, AI 수명주기 전반에 대한 보안성 강화도 병행할 필요.

1. 이슈 분석

● AI 발전으로 초개인화(Hyper-Personalization) 금융서비스 확산

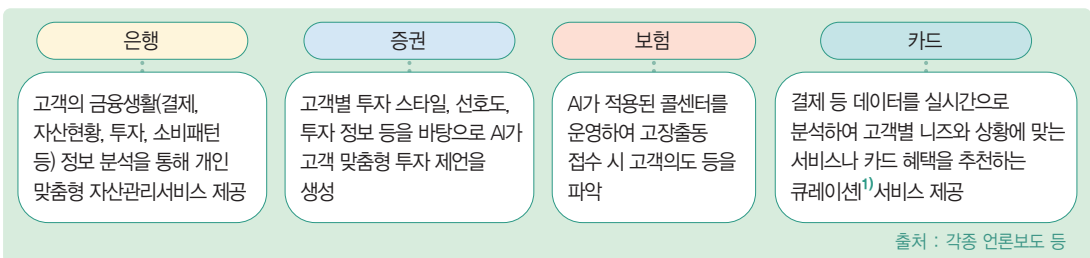
AI가 데이터 분석에서 개인의 미래 행동을 예측하는 단계로 진화함에 따라, 고객별 상황이나 맥락을 분석해 최적의 방안을 제시하는 초개인화 금융서비스가 새로운 비즈니스 형태로 부상

개인화 vs 초개인화 개념 비교

개인화(Personalization)	초개인화(Hyper-Personalization)
축적된 데이터를 토대로 고객의 니즈를 파악하고 제안 (비슷한 유형의 사람들을 타겟팅)	고객의 상황과 미래 행동까지 예측하여 고객의 잠재적 니즈를 파악하고 제안 (특정 개인을 타겟팅)

금융권은 마이데이터 등 개인의 다양한 정보를 수집·이용하고 있어 AI와의 접목을 통해 초개인화 금융서비스 개발을 추진 중

국내 금융권의 AI 기반 초개인화 서비스 개발 사례



● 금융권 AI 활성화를 위해서는 AI에 대한 신뢰성 확보가 전제

금융권 AI 활용이 아직 초기 단계로 AI가 내린 의사결정에 대한 고객의 신뢰가 아직 부족하므로, 의사결정 사유를 고객이 이해할 수 있도록 설명하는 XAI²⁾(설명가능한 인공지능) 기술의 필요성이 부각

AI가 정확한 의사결정을 하기 위해서는 양질의 학습데이터 확보가 필요하지만, 정보유출 등의 우려로 학습데이터 확보가 용이하지 않은 만큼 원본과 유사한 통계적 특성을 가진 합성데이터에 대한 관심도 증대

1) 큐레이션 : 미술관 등에서 전시되는 작품을 기획하고 설명해주는 큐레이터에서 파생한 신조어로 인터넷에서 원하는 콘텐츠를 수집·분석하여 새로운 가치를 부여하고 전파하는 것을 의미

2) XAI(eXplainable AI, 설명가능한 인공지능) : AI가 머신러닝 알고리즘으로 생성한 결과와 출력물을 대중이 이해하고 신뢰할 수 있게 만드는 일련의 프로세스 및 방법

XAI 및 합성데이터 개념 및 사례

구분	개념	사례
XAI (설명가능한 인공지능)	AI가 어떤 근거로 의사결정을 내렸는지 알 수 있게 설명가능성을 추가하는 기술	XAI로 AI기반 부정결제 카드거래 감지시스템의 감지 사례에 대한 설명을 제공
합성데이터 (Synthetic Data)	실 데이터를 기반으로 통계적 방법 등을 이용해 새롭게 생성한 모의데이터(개인정보 비식별 조치기법 中 하나)	(미국) 자금세탁방지 분야에 합성데이터를 활용 (한국) AI 교육(실습)용 학습데이터 모의DB 제공

출처 : 각종 언론보도 등

2. 전망 및 대응 전략

● 금융권의 책임감 있는 AI(Responsible AI) 구현 노력 확대

AI 기반 초개인화 금융서비스 확산으로 AI 활용에 대한 윤리적·법적 이슈 등이 제기될 것으로 보여, AI의 신뢰성 및 투명성 확보를 위한 책임감 있는 AI 구현 움직임이 금융권에 확산될 것으로 전망

책임감 있는 AI(Responsible AI) 개념

AI 시스템 및 서비스를 개발·운영·배포하는 과정이 윤리적이고 투명하며, 개인정보와 사회적 가치를 존중하는 방식으로 이뤄지는 것



책임감 있는 AI에 대한 각국 정부의 정책 마련³⁾도 속도감 있게 진행될 것으로 보여, 국내 금융권도 XAI 등 글로벌 기준에 맞는 책임감 있는 AI 구현 정책을 선제적으로 추진할 필요

● AI 수명주기 전반에 대한 보안성 확보 노력도 병행

적대적 공격⁴⁾ 등 AI의 신뢰성을 저해하는 보안위험은 학습데이터 수집부터 파기까지 전반에 걸쳐 발생할 수 있으므로 AI 수명주기 각 단계별로 위험을 통제하고 효율적으로 관리할 필요

AI 활용에 따른 보안위험 사례

구분	사례 및 내용
개인정보 유출	AI 챗봇 서비스 학습에 사용된 대화 메시지 유출
윤리적 문제	AI가 성별, 인종 등에 대해 차별적 행태를 발현
제3자 리스크	특정 거대기업의 AI를 다수 금융회사가 활용함에 따라 해당 기업의 AI 취약점이 다수에게 영향
고위험 거래 확대	AI 주식 매매 알고리즘의 오류·오작동에 따른 증시 폭락
알고리즘 오작동	AI 학습데이터 오염에 따른 AI 모델의 오작동 발생으로 금융사고 초래

출처 : 「금융산업의 인공지능 활용과 정책과제」(한국금융연구원, '23.5월) 등

책임감 있는 AI 구현을 위해 XAI, 합성데이터 등 활용 시 개인정보 보호는 물론 데이터의 편향성 및 부정확성 등을 사전 검증해야 하며, AI위험 등에 공동 대응할 수 있도록 금융권 AI 거버넌스 체계 및 로드맵 마련, 금융회사 자체 대고객 AI 운영원칙⁵⁾ 제정 등도 고려

3) 미국 바이든 정부는 책임감 있는 AI 혁신 촉진을 위한 신규 조치를 발표(「FACT SHEET: Biden-Harris Administration Announces New Actions to Promote Responsible AI Innovation that Protects Americans' Rights and Safety」, 美 백악관, 23.5월)

4) 적대적 공격(Adversarial Attack) : 머신러닝의 알고리즘 취약점에 의해 적대적 환경에서 발생할 수 있는 보안 위험(학습 데이터 교란, 역공학, 학습데이터 추출 등)

5) 구글·마이크로소프트·네이버·카카오 등 빅테크 기업과 우리금융그룹, KB금융그룹 등 금융권에서는 AI 운영 또는 윤리 원칙 등을 제정

사물과 디지털금융의 만남, 금융 사물인터넷(FoT)

10

사물과 디지털금융을 연결하는 “금융 사물인터넷(FoT, Finance of Things)”이 금융권에 새롭게 시도되고 보다 폭넓게 활용될 것으로 전망. 사물인터넷 보안위협이 금융과 연계해 고도화될 것으로 보여 사물인터넷 위험 대응역량 확보 필요.

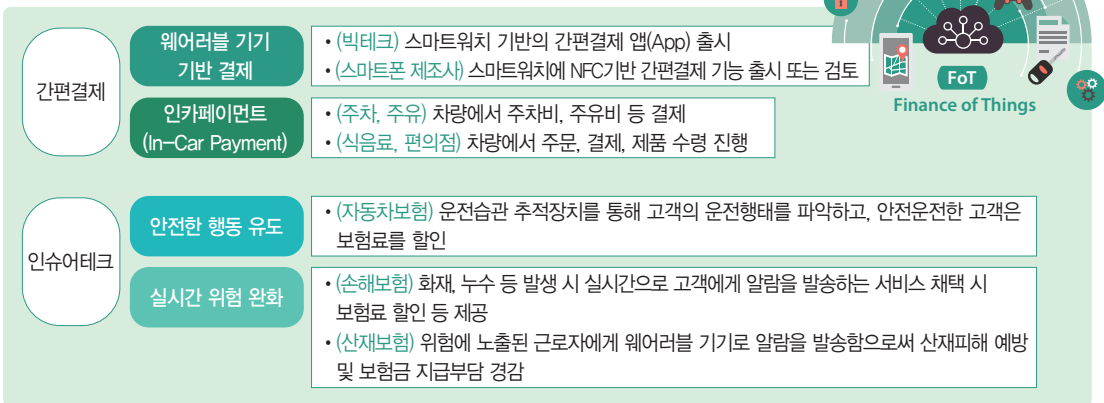
1. 이슈 분석

● 결제, 보험 중심으로 금융 사물인터넷(FoT)이 확산

근거리 무선통신(NFC) 결제에 대한 관심 증대로, 그간 다소 정체되었던 웨어러블 기기 기반 결제가 스마트워치를 중심으로 빠르게 확산될 전망¹⁾

인슈어테크(보험)²⁾ 분야에서도 운전습관에 따라 보험료를 할인하는 등 사물인터넷 기반의 다양한 보험상품·서비스를 개발하여 고객의 안전한 행동을 유도하고 실시간으로 위험을 완화

금융 사물인터넷(FoT) 적용 현황



● 사물인터넷의 보안위협이 금융영역으로 전이 및 고도화

사물인터넷 기기는 제한된 컴퓨팅 자원이나 메모리공간 등으로 PC나 스마트폰 수준의 보안성 확보가 어려워 공격자에게는 매력적인 공격 대상

기존 사물인터넷의 보안취약점³⁾을 악용하여 금융 데이터 유출, 비인가 결제 등 전자금융사고를 유발할 수 있으며, 취약한 사물인터넷 기기를 내부망 침투 경로나 악성코드 유포지 등으로 악용 가능

1) 최근 6개월간 간편결제를 이용한 경험이 있는 스마트워치 보유자 중 70%는 웨어러블 기반의 간편결제 서비스 이용 의향이 있다고 밝힘 (하나금융연구소, 「2023년 금융소비 트렌드의 금융 기회 보고서」 '23.2월)

2) 인슈어테크(InsurTech) : 보험(Insurance)과 기술(Technology)의 합성어로 기술을 이용하여 기존 보험산업을 혁신하는 서비스 기술

3) 보안패치 관리 미흡, 취약한 인증 메커니즘, 펌웨어 업데이트 취약점, 잘못된 환경설정 등

사물인터넷(IoT) 관련 보안위협(예시)

구 분	내 용
사물인터넷 기기 대상 보안위협	<ul style="list-style-type: none"> 사물인터넷 기기의 특성 상 컴퓨팅 자원(CPU, 메모리 등)이 제한적으로, 금융거래 정보 등을 암호화하지 않거나 취약한 경량 암호알고리즘을 사용하여 암호화 ➔ 중요 금융정보 등 데이터의 송수신 및 저장 과정에서 데이터가 유출, 변조되거나 탈취
사물인터넷 기기 악용 보안위협	<ul style="list-style-type: none"> 최신 운영체제 미사용, 취약한 비밀번호 사용 등 취약점을 지닌 사물인터넷 기기를 악성코드에 감염시키고 기기를 점유 ➔ 악성코드에 감염된 사물인터넷 기기를 DDoS 공격을 위한 봇넷⁴⁾ 또는 암호화폐 채굴용 악성코드 유포를 위한 경유지로 악용

2. 전망 및 대응 전략

● 금융 사물인터넷(FoT)을 통한 디지털금융 다양화 전망

결제, 인슈어테크 등에서 사물인터넷 기기 활용이 더욱 활성화될 것이며, 사물인터넷 기기를 통해 수집된 데이터를 기반으로 개인 맞춤형 금융상품·서비스*도 등장

* (예) 스마트 ATM으로 현금카드 거부 횟수, 거래 소요시간, 서비스 제공 속도 등의 데이터를 분석하여 고객 편의성 및 보안 수준을 제고할 수 있는 운영방법을 제안

스마트반지⁵⁾ 등 결제에 활용되는 웨어러블 기기도 다양화될 것이며, 사물인터넷과 시가 결합된 지능형 사물인터넷(AIoT⁶⁾)도 금융분야에 도입 시도

● 금융 사물인터넷(FoT) 확산 대비한 선제적 보안대책 마련 필수

금융 사물인터넷이 활성화되면 기존 금융권 대상 보안위협의 전이나 금융 사물인터넷에 특화된 새로운 보안위협이 등장할 수 있으므로 서비스 설계 단계부터 보안성을 고려(Security by Design)할 필요

사물인터넷 기기의 컴퓨팅 자원 한계 등이 존재하지만 해당 기술이 금융분야에 적용되는 만큼 전자금융사고가 발생되지 않도록 금융권 특성에 맞는 보안 기준을 마련하고 준수할 필요

금융 사물인터넷(FoT) 보안대책(예시)

보호대상	내 용
사물인터넷 기기 (Device)	<ul style="list-style-type: none"> · (자산 관리) 금융서비스에 적용되는 모든 사물인터넷 기기의 현황 및 특성을 파악·관리 · (취약성 관리) 사물인터넷 기기의 S/W 등에 알려진 취약점을 확인하고 이를 제거하기 위한 패치, 업그레이드, 환경 설정 등을 진행 · (접근관리) 적절한 인증 사용, 필요 최소한의 접근권한 제한 등을 통해 인가되지 않은 사물인터넷 사용자 및 기기의 접근을 방지 · (침해사고 탐지) 보안 관련 이벤트 로그를 기록하고 IPS⁷⁾, 안티 바이러스 도구 등을 활용하여 잠재적 침해사고를 탐지·대응
데이터 (Data)	<ul style="list-style-type: none"> · 사물인터넷 기기에 저장 또는 송수신되는 모든 중요 데이터에 대해 비인가 접근을 차단 · 사물인터넷 기기 내 보안영역인 TEE(Trusted Execution Environment)를 활용하여 데이터의 기밀성을 보장

출처 : 「Considerations for Managing IoT Cybersecurity and Privacy Risks」(美 NIST, '19.6월), 「지능형 IoT 사회의 보안이슈 분석」(KISA, '22.9월) 등

4) 봇넷(botnet) : 악성 소프트웨어에 감염되어 악성 활동을 수행하는데 사용되는 컴퓨터 또는 기타 인터넷 기반 디바이스의 네트워크

5) 스마트 반지(smart ring) : 삼성전자는 '갤럭시 서클'이라는 스마트반지 상표를 출원하였고, 애플은 애플링에 대한 특허를 공개

6) AIoT(Artificial Intelligence of Things) : 인공지능(AI)과 사물인터넷(IoT)의 융합으로, 사물이 센싱 후 전송한 데이터를 지능적으로 '분석-진단-의사결정'을 수행하는 기술 (출처 : KISA)

7) IPS(침입 차단 시스템, Intrusion Prevention System) : 악성 트래픽을 식별하고 그러한 트래픽이 네트워크에 유입되는 것을 사전에 차단할 수 있도록 도와주는 시스템

참고문헌

- 「[디지털 특화 보고서] 모티즌인 MZ세대의 금융플랫폼 이용행태 분석」(우리금융연구소, '22.12.26.)
- 「Gartner Top Strategic Cybersecurity Trends 2023」(Gartner, '23.4.19.)
- 「2022 전국민 금융 이해력 조사」(한국은행 · 금융감독원, '23.3.29.)
- 「인간중심보안 프레임워크 1부」(인간중심보안포럼, '22.1.19.)
- 「Critical Cybersecurity Hygiene: Patching enterprise」(NIST, '20.3.20.)
- 「What is Cyber Hygiene?」(Carnegie Mellon University, '19.3.7.)
- 「2023 gartner top strategic technology trends」(Gartner, '23.10월)
- 「우리은행, 금융보안원과 모의해킹 경진대회 'WooriCON' 개최」(우리은행, '23.7.5.)
- 「제2회 '토스 버그바운티 챌린지' 개최」(토스, '23.7.12.)
- 「급변하는 IT환경에 탄력적으로 대응할 수 있도록 금융보안 규제 선진화를 추진하겠습니다.」(금융위원회, '22.12.27.)
- 「자본시장법에서의 상장회사 적용 법규 및 개선 과제」(정순섭, '10.6월)
- 「금융사고, 제재보다 예방에 주력」(금융위원회 · 금융감독원, '23.6.22.)
- 「Principles for Sound Management of Operational Risk」(美 BIS, '23.4월)
- 「국내 금융분야 운영복원력 강화 방안 연구」(금융보안원, '22.2월)
- 「Cool Vendors in Platform Engineering for Scaling Application Security Process」(Gartner, '23.6.6.)
- 「그것이 알고 싶다! X옴스란 무엇인가」(안랩, '23.2.8.)
- 「국내 퍼블릭 클라우드 소프트웨어 시장전망, 2022년-2026년」(한국IDC, '23.2월)
- 「Framework_for_Developing_SaaS_Security_Policy」(Gartner, '22.5월)
- 「2022 SaaS Security Survey Report」(Cloud Security Alliance, '22.4월)
- 「Global Active Protection System(Soft Kill System, Hard Kill System, Reactive Armor) Markets, 2022-2027」(Research and Markets, '22.8월)
- 「Establishment」(Hybrid CoE, '23.10.5.)
- 「Identifying Emerging Cyber Security Threats and Challenges for 2030」(ENISA, '23.3월)

- 「카카오 대란, 끝이 안 보인다.. 태시 ‘길빵’ 영업에 쇼핑몰도 ‘휴업」 (머니투데이, '22.10.16.)
- 「카카오 화재로 특 등 ‘먹통’… 의료기관도 ‘혼선」 (데일리메디, '22.10.17.)
- 「3CX Software Supply Chain Compromise Initiated by a Prior Software Supply Chain Compromise; Suspected North Korean Actor Repsonsible」 (MANDIANT, '23.4월)
- 「오픈소스 리포지터리 통한 공급망 공격, 특정 은행 및 몇 군데 피해 입혀」 (보안뉴스, '23.7.24.)
- 「SBOM 활용 관련 동향 검토 및 시사점 보고」 (금융보안원, '23.4월)
- 「AI deepfakes are getting better at spoofing KYC verification」 (Cointelegraph, '23.5월)
- 「‘I’ve got your daughter’ : Mom warns of terrifying AI voice cloning scam that faked kidnapping」 (美 Arizona News, '23.4월)
- 「국내외 음성AI(딥보이스) 활용 및 정책 동향 검토」 (금융보안원, '23.4월)
- 「민관이 모여 모바일 신분증을 활용한 혁신 서비스 발굴 나선다」 (행정안전부, '22.12.26.)
- 「4대 시중은행의 디지털 지갑 서비스 특징과 보안기능 전격 비교」 (보안뉴스, '23.8.16.)
- 「FACT SHEET: Biden–Harris Administration Announces New Actions to Promote Responsible AI Innovation that Protects Americans’ Rights and Safety」 (美 백악관, '23.5월)
- 「책임감 있는 AI와 금융 서비스 산업」 (코스콤, '23.8월)
- 「AI 신뢰성 확보를 위한 위험관리 방안에 관한 연구」 (금융보안원, '23.6월)
- 「2023년 금융소비 트렌드의 금융 기회 보고서」 (하나금융연구소, '23.2월)
- 「Considerations for Managing IoT Cybersecurity and Privacy Risks」 (美 NIST, '19.6월)
- 「지능형 IoT 사회의 보안이슈 분석」 (KISA, '22.9월)
- 「보험회사 사업모형 전환 : IoT 기반 위험예방서비스」 (보험연구원, '21.8.17.)
- 「경영환경 변화와 보험업 비즈니스 전환」 (KB금융지주경영연구소, '23.8월)
- 「국정원, 국내외 IoT 장비 약 1만 2천 대 악성코드 감염 대응 조치 중」 (국가사이버안보센터, '22.1월)
- 「Artificial Intelligence of Things(AIoT) & the role it plays in banking」, (Global Banking & Finance Review, '21.5월)

2024 디지털금융 및 사이버보안 이슈 전망

Key Issue 금융보안 프렌들리
Financial Security Friendly

발 행 일 2023년 11월

발 행 처 금융보안원

발간 총괄 보안연구부장 이상록

발간 협조 연구기획팀 김성규 노민지
금융혁신지원팀 이준호 이대규 이명영 이태희
미래기술보안팀 황송이

발간 실무 금융혁신지원팀 서호진, 황영란

디 자 인 (주)스텐리큐브릭

인 쇄 (주)한영문화사

본 보고서에 수록된 내용에 대한 무단전재를 금합니다.

2024 디지털금융 및 사이버보안 이슈 전망

Key Issue 금융보안 프레임틀리
Financial Security Friendly

