

금융분야 망분리 개선 로드맵

2024. 8.

금 융 위 원 회
금 융 감 독 원

목 차

◆ 금융분야 망분리 개선 방향과 기대효과	i
Ⅰ. 개 요	1
Ⅱ. 금융권 망분리 개선 정책 추진방향	4
Ⅲ. 단계별 규제 개선 방안	5
- 1단계 추진과제	5
- 2단계 추진과제	12
- 3단계 추진과제	14
Ⅳ. 향후 계획	15

"금융권 망분리 10년, 혁신과 보안의 새로운 균형으로의 도약"

- ☞ 급변하는 IT환경 下 금융산업 경쟁력 제고, 금융소비자 효용 증진, 금융보안체계 선진화를 위해 망분리 개선은 선택이 아닌 필수
- ☞ 망분리 개선 과정에서 보안상 허점이 발생하지 않도록 충분한 안전장치 마련

I. 샌드박스를 통하여 규제애로 즉시 해소 + 별도 보안대책

- 샌드박스를 통해 개선이 시급한 과제 즉시 추진
 - ▶ 생성형 AI 허용, 클라우드(SaaS) 활용 범위 대폭 확대
- 선진형 자율보안체계 확립까지는 시간이 소요되므로, 샌드박스 시행 과정에서는 보안상의 문제가 없도록 별도의 보안대책 등 마련
 - ① 예상 리스크에 대한 별도의 보완 방안을 조건으로 부과
 - ② 금감원·보안원이 신청 기업별 보안 점검·컨설팅 실시
 - ③ 내부 보안거버넌스 강화 유도 및 보안사고 발생시 엄중 제재

II. 샌드박스 운영 경험을 토대로 금융보안체계 선진화 추진

- 혁신성·소비자 편익·리스크 관리 등 충분히 검증된 샌드박스 과제 → 제도화
- 「디지털 금융보안법(가칭)」을 마련하여 “규칙(Rule) 중심 → 원칙(Principle) 중심”으로 규제를 전환, “자율보안-결과책임”에 입각한 新 금융보안체계 구축
 - ▶ (자율보안) 법령을 통해 보안 원칙·목표 제시
금융회사는 자체 리스크 평가를 거쳐 세부 보안통제 자율 구성
 - ▶ (결과책임) 실효성 있는 과징금 도입, 배상책임 강화 등 사고 발생시 책임 확대
중요 보안사항 CEO·이사회 보고의무 등 내부 보안거버넌스 강화
 - ▶ (금융당국) 자율보안체계 수립·이행 검증 → 미흡시 시정요구·이행명령 등
국내 금융권도 글로벌 수준으로 IT 보안투자 규모를 확대토록 지속 유도*

* (例) 전체 예산 중 IT예산 및 정보보호 예산 비중 등을 공시 대상으로 추가하는 방안 검토
→ 자발적 보안투자를 유도하고 자율보안체계 下 금융소비자의 선택권도 보장

Ⅲ. 금융산업 경쟁력 제고 + 금융소비자 효용 증진 유도

< 금융 산업 >

- AI·SaaS 기반 업무자동화, ERP(인사·회계 등) 등 도입 → 업무 생산성 향상
- 연구·개발 업무 편의 증가, IT개발 직원 재택근무 허용 등 근무 환경 개선
- AI 기반의 빅데이터 분석, 산업적 연구 및 통계 작성 등 금융데이터 활용 증가
- 금융권 선진 보안기술 도입 활성화에 따른 IT 보안 산업 발전 효과

< 금융소비자 >

- 전에 없던 혁신적인 新상품 개발 → 금융소비자의 기회·편익 확대
 - * (예) AI기반 데이터 분석·예측 및 신용평가 고도화 → 특화 보험, 중금리 대출상품 개발 등 사각지대 해소
- 고객 행동분석, 고객관계관리(CRM) 고도화 → 맞춤형 서비스 제공 및 의사결정 지원
 - * (예) 글로벌 J 투자사 : AI로 자산·투자이력·소비행태 등 분석 → 고객 특성별 포트폴리오 및 투자 결정 추천
- 생성형 AI 기반의 이상금융거래탐지시스템(FDS) 고도화 → 금융소비자 보호 강화
 - * (예) 글로벌 M 카드사 : 생성형 AI로 수십억건의 거래패턴과 피해사례 등을 학습 → 복잡한 사기시도 탐지

< 단계별 세부 추진과제 >

1단계('24년 연내 추진)	2단계	3단계												
<div>① 생성형 AI 허용<small>(규제샌드박스)</small> : 생성형 AI를 활용하여, 가명정보*까지 처리할 수 있도록 규제특례 허용 * 추가정보 사용 없이는 특정 신용정보주체를 알아볼 수 없도록 가명처리된 개인신용정보</div>	<div>④ 1단계까지의 규제특례 정규 제도화 : 샌드박스로 성과 검증*된 과제 → 규정 개정 등 제도화 추진 * ~'25.上 : 샌드박스 운영사례 성과검증</div>	<div>⑦ 「디지털 금융보안법」 제정 * 연구용역('24.3Q), 공청회(4Q)를 거쳐 연내 마련 추진</div> <div>- 자율보안-결과책임의 보안체계 구축 : 목표·원칙중심으로 규제 전환</div> <div>- 금융권 책임 강화 : 배상책임 강화, 실효성 있는 과징금 등 : CSO 권한 확대 및 CEO이사회 보고의무</div> <div>- 금융당국의 점검·이행명령 등 금융권 보안수준 제고 뒷받침</div>												
<div>② 클라우드 이용 확대 <small>(규제샌드박스)</small></div> <table><tr><th></th><th>현 행</th><th>개 선</th></tr><tr><td>데이터</td><td>개인신용정보 금지</td><td>가명정보 허용</td></tr><tr><td>프로그램 유형</td><td>협업툴 인사관리 등 비중요업무 허용</td><td>고객관리(CRM), 업무자동화 등 추가 허용</td></tr><tr><td>단말기</td><td>유선 PC만 허용</td><td>모바일단말 허용</td></tr></table>			현 행	개 선	데이터	개인신용정보 금지	가명정보 허용	프로그램 유형	협업툴 인사관리 등 비중요업무 허용	고객관리(CRM), 업무자동화 등 추가 허용	단말기	유선 PC만 허용	모바일단말 허용	<div>⑤ 규제특례 확대·고도화 : 개인신용정보 처리 등 리스크↑ 업무 → 강화된 보안대책 전제로 추가 허용</div>
	현 행		개 선											
데이터	개인신용정보 금지	가명정보 허용												
프로그램 유형	협업툴 인사관리 등 비중요업무 허용	고객관리(CRM), 업무자동화 등 추가 허용												
단말기	유선 PC만 허용	모바일단말 허용												
<div>③ 연구·개발 분야 망분리 개선<small>(감독규정 개정)</small></div> <table><tr><th></th><th>현 행</th><th>개 선</th></tr><tr><td>연구개발망 업무망 간</td><td rowspan="2">물리적 망분리</td><td>논리적 망분리</td></tr><tr><td>연구개발망 전산실 간</td><td>개발 결과물 등 이관을 위한 예외 허용</td></tr><tr><td>데이터</td><td>개인신용정보 금지</td><td>가명정보 허용</td></tr></table>		현 행	개 선	연구개발망 업무망 간	물리적 망분리	논리적 망분리	연구개발망 전산실 간	개발 결과물 등 이관을 위한 예외 허용	데이터	개인신용정보 금지	가명정보 허용	<div>⑥ 제3자 리스크 관리강화 등을 위한 정보처리 위탁제도 정비</div>		
	현 행	개 선												
연구개발망 업무망 간	물리적 망분리	논리적 망분리												
연구개발망 전산실 간		개발 결과물 등 이관을 위한 예외 허용												
데이터	개인신용정보 금지	가명정보 허용												

I. 개 요

□ (검토배경) 금융권 망분리 도입('13.12월) 후 10년 넘게 경과*

* '13.3.20. 금융회사 대규모 전산망 마비를 계기로 '공공부문'의 물리적 망분리를 '금융권' 도입

- ①망분리로 인한 업무 비효율, ②연구·개발 및 신기술(AI 등) 활용 애로, ③해외 규제와의 괴리 등에 따른 규제개선 요청 지속

□ (그간의 경과) 몇 차례 규제개선이 있었으나 시장의 기대에 미흡 → 변화된 IT 환경을 감안하여 규제 적정성 등 종합적 재검토 필요

① ('19.1월) 클라우드 이용시 물리적 망분리 예외 허용, 단 소프트웨어 형태 클라우드(SaaS) 이용 불가

② ('22.11월) "연구·개발 망분리 예외" 허용, 다만 제한조건으로 인해 활용 미흡*

* ①개인신용정보 처리 불가, ②연구·개발망과 내부 업무망간 물리적 분리 등을 충족하는 연구개발 환경 구현 어려움

③ ('23.9월) 규제샌드박스로 업무망 SaaS 이용을 허용했으나, 부가조건*으로 활용 제한

* ①고객 개인신용정보 처리 불가, ②일부 프로그램(보안, 개발, 대고객 프로그램 제외)에 한하여 허용 등

□ (필요성) 현행 망분리 규제를 고수할 경우 ①급격하게 변화하는 IT환경에서 생존하기 어려우며, ②금융보안의 발전을 오히려 저해할 우려

- ① 소프트웨어(S/W) 시장이 자체구축형 → 클라우드 기반의 구독형 SaaS로 빠르게 전환되고*, 특히 AI, 보안 관련 S/W는 대부분 SaaS로 제공

* SaaS(Software as a Service) 시장규모 : 글로벌('19년 187조 → '24년 396.7조), 국내('19년 0.69조 → '24년 1.62조)

- 인터넷 연결을 일괄 차단하는 현행 망분리 규제에 따라 SaaS 이용 제한

- ② 기존 자체구축 환경에서 망분리는 높은 보안성을 보장했으나, 클라우드 환경 下 오히려 보안성 약화* 요인으로도 작용

* 클라우드 보안 솔루션 및 운영체제(OS) 프로그램 등의 보안패치 다수가 SaaS 형태로 배포되는 반면, 망분리 환경은 실시간 업데이트가 어려워 최신 위협에 대응 곤란

- 금융회사는 망분리만을 준수할 뿐 해외 선진 보안체계 도입에 소홀*,

* (예) EU, 미국 등의 경우 제로트러스트(ZeroTrust) 기법에 대한 도입 논의가 활발한 반면, 국내 금융회사 등은 망분리 체계를 전제로 논의 미흡

- 일부 회사는 망분리라는 규제 그늘에 숨어 필요·최소한의 보안 체계도 적절히 갖추지 않는 등 오히려 보안수준이 낮아지는 부작용

➔ 기존 망분리 규제를 개선하고, 장기적으로는 **新 금융보안법·체계 마련**을 통한 **패러다임 전환 추진**

이상 (Ideal)



- 망분리는 손쉬운 보안수단이며, 외부공격 차단 효과가 매우 높음
- 그러나, 외부와의 단절로 AI 시대에 부적합하고 경쟁력이 크게 하락

현실 (Reality)



- 현실적으로 수많은 망분리 예외 설정이 불가피하고 관리소홀 시 문제는 여전
- 갈라파고스적 규제로 보안기술 발전·도입을 저해

국내 금융권 망분리



외딴섬 (인터넷 차단)을 전제로 망보안 설계 * 망분리 예외 통신: 도개교

해외 네트워크 세분화 (Network Segmentation)



**인터넷은 자유롭게 활용 가능하며, 업무의 중요도 등에 따라
자율적으로 보안대책 (울타리, 병사 등) 적용**

* 망분리(인터넷 차단)을 명시적으로 요구하는 규제는 없음

II. 금융권 망분리 개선 정책 추진 방향

◆ ^①단계적 개선, ^②금융권 보안노력 강화, ^③규제 합리화 이익 금융소비자 향유
⇒ “망분리 규제 10년, 혁신과 보안의 새로운 균형 모색”

1 망분리 규제의 단계적 개선 추진

- 현행 금융 보안체계는 모두 망분리 환경을 전제로 구성되어 있으므로, 급격한 규제 완화보다는 “**변화→적응**”을 반복하는 점진적 전환 필요
 - 보안 책임성을 제고하는 법·제도가 마련되기도 전에 금융회사 등의 사전 준비 없이 규제 완화시 금융사고 발생 우려
- ‘자율보안-결과책임’ 원칙 下 ^①「디지털 금융보안법(가칭)」 제정을 추진하는 큰 방향을 제시하여 금융권이 스스로 대비할 수 있도록 함과 동시에,
 - 급격한 IT 환경변화로 인해 신속한 대응이 필요한 부분의 경우 ^②규제특례(샌드박스) 등을 적극 활용하여 금융회사의 애로 즉시 해소

2 보안 거버넌스 강화 및 자율보안 역량 제고를 통한 취약부문 개선

- 금융회사 등은 중요 보안사항의 최고경영자(CEO) 및 이사회 보고의무, 정보보호최고책임자(CISO) 권한 확대 등 내부 보안체계를 강화하고,
 - 금융당국은 금융권의 보안수준을 지속 점검·컨설팅하고, 미흡한 부분에 대한 시정조치 및 엄중 제재 등을 통해 보안 노력 제고 유도
- 금융회사 등은 망분리 규제개선에 따른 IT 관련 연구·개발 활성화 및 新 보안체계 도입 등 보안역량 강화를 위한 자체적인 노력 확대
 - * 클라우드 기반의 보안솔루션 활용 및 최신 취약점이 반영된 실시간 보안 업데이트 등

3 규제 개선의 이익을 금융 소비자도 향유할 수 있도록 구조화

- 망분리 개선에 따른 이익이 기업의 비용 절감, 업무 효율성 제고에 그치지 않고, “금융 소비자”에게 공유
 - 연구·개발 활성화, 신기술 활용 제고 ⇒ 혁신적인 금융상품 출시*
 - * 고객 정보 활용분석 증가 → 맞춤형 상품 개발, 비용 절감 → 對고객 서비스 수수료 절감
 - 샌드박스 지정시 “소비자 편익”과 “서비스 혁신성”을 중점 심사
⇒ 소비자 중심의 혁신적인 금융서비스 출시 유도

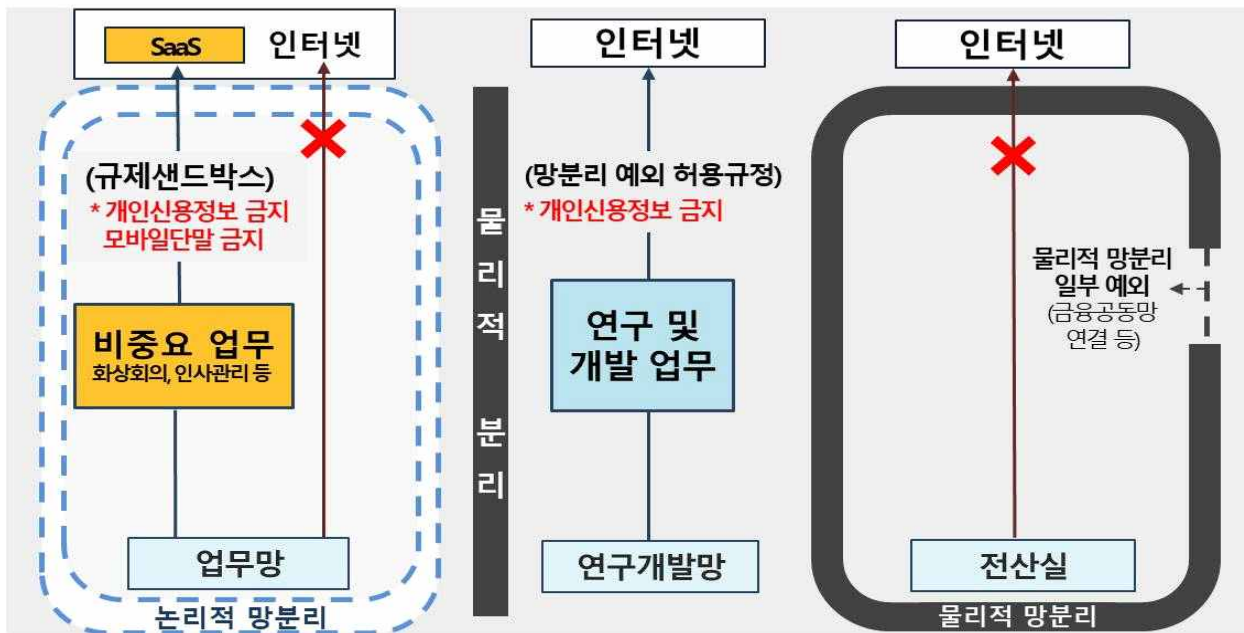
Ⅲ. 단계별 개선 방안

1 단계 추진과제

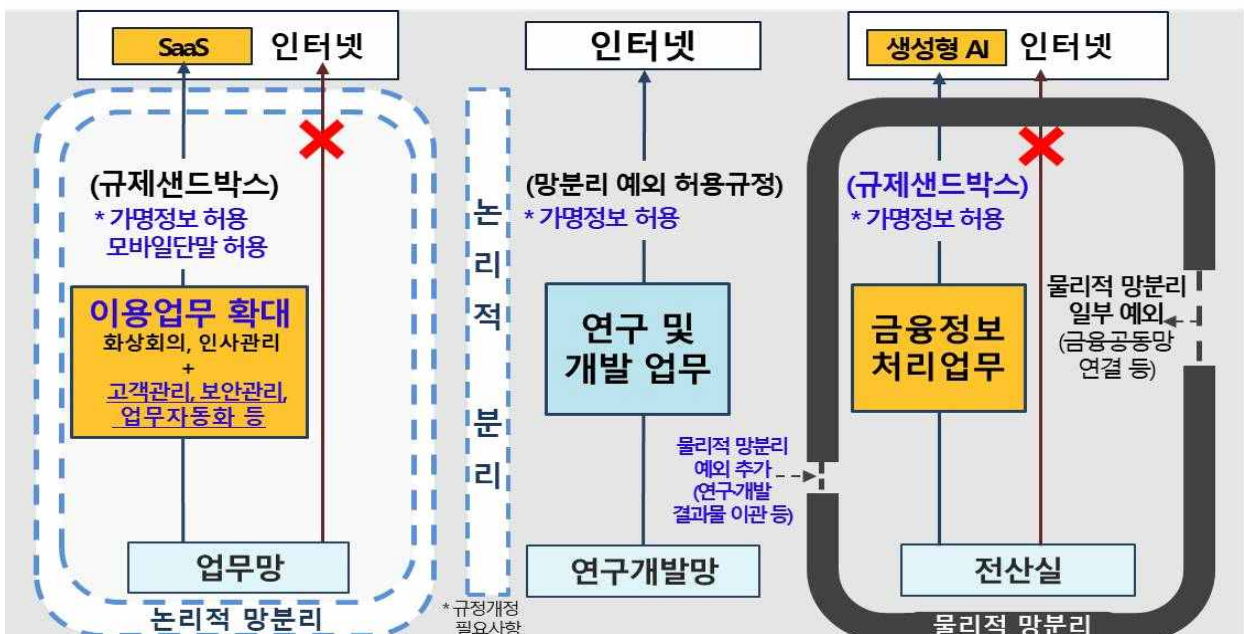
1단계 추진 과제 종합 구성도

(1-1) 생성형 AI 활용 허용, (1-2) 클라우드 기반의 응용 프로그램(SaaS) 활용도 제고,
(1-3) 연구·개발 분야 망분리 규제개선

망분리 현황(AS-IS)



망분리 개선안(TO-BE)



1-1. 생성형 AI 활용 허용

 금융회사의 생성형 AI 활용을 폭넓게 허용하겠습니다

□ (현행) 대부분의 생성형 AI*가 클라우드 기반의 인터넷 환경에서 제공되나, '망분리 규제'로 인해 활용에 제약

* 기존 데이터를 분석하는 것을 넘어, 새로운 콘텐츠를 생성해 내는 AI 유형

○ 또한, 국내에 서버가 없는 해외 소재 AI 모델을 통한 개인신용정보(가명정보 포함) 처리·보관 불가

※ (개인정보보호법) 개인정보는 원칙적으로 국내 처리·보관 등, 일정한 경우* 예외 허용(§28의8)

* ①정보주체 별도 동의 또는 ②이전받는 자가 위원회가 정하는 국내·외 정보보호인증 등 획득 또는 ③이전되는 국가의 개인정보 보호수준 인정 등

(전자금융감독규정) 클라우드로 개인신용정보 처리시 해당 클라우드 정보처리시스템 국내 설치(§1492③)

□ (개선) 금융회사가 생성형 AI를 활용하여 가명처리된 개인신용정보까지 처리할 수 있도록 규제 특례 허용

○ (망분리 특례) 금융회사 정보처리시스템(내부)과 AI 모델(외부)간 연결을 위한 망분리 규제특례 허용

○ (데이터 특례) 해외소재 AI를 통한 가명정보 처리를 위해 관련 법령(「전자금융감독규정」, 「개인정보보호법」)에 대한 관계부처 협업 추진

□ (필요조치) 신청 기업별 AI 사용 목적, 처리 데이터 범위, 보안 수준 등을 종합적으로 고려하여 규제샌드박스 심사·지정

○ 망분리 예외에 따른 강화된 보안대책, 금융회사-해외 AI사업자간 계약시 반영할 필요·최소한의 내용 등을 부가조건으로 부과*(→p.7)

○ 사전 업무설명회(24.3Q)를 통해 지정방식*, 보안 유의사항 등 안내·컨설팅

* 자율보안체계 확립을 위한 자발적 노력 유도 차원에서, 정보보호최고책임자(CISO) 결정 및 이사회 보고 등 보안 거버넌스 작동 기업에 대해 샌드박스 심사시 가점 부여 예정

→ 다양한 AI 수요를 가진 금융회사 등이 차질 없이 신청하고, 혁신금융서비스가 신속히 개시될 수 있도록 지원

< 생성형 AI 허용 방안 (1) : IaaS를 통한 AI 연결 >



< 생성형 AI 허용 방안 (2) : DMZ를 통한 AI 연결 >



* 허용 방안 (1), (2)는 구성 가능한 대표적인 사례로 금융회사별 세부 구성 방식은 달라질 수 있음

< ※ 생성형 AI 활용을 위한 “강화된 보안대책 (예시)” >

- 이용자 프롬프트에서 신뢰할 수 없는 콘텐츠 차단
- 클라우드 내 금융회사 테넌트(IaaS)에서 불필요한 인터넷 등 외부 통신망 접속 차단
- 금융회사 영역(DMZ 또는 금융회사 클라우드 테넌트)과 AI 모델 영역간 접속시 **안전한 연결방식** (가상사설망 또는 이에 준하는 보안수준을 갖출 것 등) **사용**
- 학습, 추론, 상용 생성형 AI 응용 서비스에 필요한 자원은 금융회사의 독점적·배타적 영역에 할당
- 이용자 입력 및 생성형 AI 개발·활용 시 신뢰할 수 있는 개인정보 보호조치 마련
(※ 예시: 출력 모니터링·검증, 개인정보 노출 시 사후 신고·처리 절차 마련 등)
- 가명정보 처리 목적 적합성, 가명처리 적정성 등에 대해 심의 수행
- 가명정보를 원래의 상태로 복원하기 위한 추가정보는 분리하여 암호화 및 별도 보관

< ※ 생성형 AI 활용을 위한 “계약시 반영 필수사항* (예시)” >

- 서비스 제공 위치(지역 또는 국가), 데이터 처리·저장 위치 및 이를 변경시 금융회사에 대한 사전통지 등
- 데이터 보호와 관련하여 가용성 · 신뢰성 · 무결성 · 기밀성 관련 사항
- 가명정보 수탁 목적 외 활용(SaaS AI모델 고도화, 제3자 제공 등) 금지
- IT사고 발생 시 사전에 합의된 비용으로 금융회사를 지원할 제3자의 의무
- 제3자가 관할당국 등에 협조해야 할 의무
- * 금융회사당국의 접근·검사·감사 권한 중요문서 사본을 현장에서 가져갈 수 있는 권한 권한 행사가 다른 계약내용 등에 의해 제한되지 않을 것 등
- 계약 해지 권한 및 최소 통지 기간

1-2. 클라우드 기반의 응용 프로그램(SaaS) 활용도 제고

- ☞ (1) 임직원 업무망에서의 SaaS 활용 범위를 대폭 확대하고,
(2) 금융회사의 SaaS 이용절차를 보다 간소화하겠습니다

[1] 임직원 업무망에서의 SaaS 활용 범위 확대

- (현행) '23.9월, 규제샌드박스로 업무망에서의 SaaS 사용을 허용하였으나, 엄격한 부가조건*으로 활용 제약

* ①고객의 개인신용정보 처리 불가, ②업무협업 도구, 인사관리 프로그램 등(보안, 개발, CRM 등 제외)에 한하여 허용, ③모바일 단말 금지

- (개선) 규제샌드박스를 통해 업무망에서의 SaaS 활용 범위 대폭 확대*

* ①데이터 범위 : 개인신용정보 불가 → 가명처리된 개인신용정보 허용

※ 단, 관련 법령(「전자금융감독규정」, 「개인정보보호법」)에 따른 국외 이전 제한 이슈 상존

②프로그램 유형 : 협업도구, ERP 등만 허용 → 보안, 고객관리, 업무자동화 등 추가 허용

③단말기 유형 : 유선 PC만 허용 → 모바일 단말기도 허용

- (필요조치) 신청 기업별 SaaS 활용 범위, 이용업무, 보안수준 등을 종합적으로 고려하여 규제샌드박스 심사·지정

- 활용범위 확대에 따른 강화된 보안대책* 등 부가조건 부과
- 사전 업무설명회를 통해 지정방식*, 보안 유의사항 등 안내·컨설팅

* 내부 보안 거버넌스 작동 기업에 대해 샌드박스 심사시 가점 부여 예정

< ※ 임직원 업무망에서의 SaaS 활용을 위한 “강화된 보안대책 (예시)” >

- 가명정보를 원래의 상태로 복원하기 위한 추가정보는 분리하여 암호화 및 별도 보관
- 모바일 단말의 장치 추적성 확보 및 데이터 저장 및 반출 제한 등
- 보안대책을 적용한 별도 지정된 모바일 단말 사용, 개인 용도의 사용 금지 등

[2] SaaS 이용 절차 간소화

- (현행) 협업·디자인 도구 등 단순 업무용 SaaS임에도 불구하고, SaaS 도입시 업무 대비 과도하고 관련성이 낮은 클라우드 이용 절차까지 획일적으로 준수할 필요*

* (예) 고객정보를 미처리하는 SaaS임에도 불구하고 계약시 금융회사 등의 비상 대응훈련 협조, 비밀유지 의무 등을 반영

- 특히, SaaS 이용 전 ③업무연속성 계획, ④안전성 확보조치 방안, ⑤위수탁계약 주요 기재사항을 모두 갖추어야 하는 부담이 큰 상황

< ※ “클라우드 이용절차(전자금융감독규정 §14의2⑧)” >

- ① (이용업무 중요도 평가) 클라우드로 처리하는 업무 특성, 서비스 중단시 영향 등 고려
- ② (CSP 평가) 클라우드서비스제공자(CSP)의 건전성 및 안정성을 평가[별표 2의2]
- ③ (업무연속성 계획) 백업, 재해복구, 침해사고 대응훈련, 출구전략 등 계획 수립[별표 2의3]
- ④ (안전성 확보조치) 계정관리, 접근통제 등 클라우드 이용 안전성 확보방안 수립[별표 2의4]
- ⑤ (계약 주요 기재사항) 비상대응훈련 협조, 고객정보보호, 비밀유지 등 필수 포함[별표 2의5]

- (개선) 업무연속성 계획 필수사항 : 21개 → 18개,
안전성 확보조치 필수사항 : 47개 → 33개로 간소화*

* `24.2.1. 「전자금융감독규정」 개정안 입법예고 → 연내 개정 완료 예정

- 추가로, 전자금융거래와 무관하고 고객 개인신용정보를 처리하지 않는 SaaS의 경우 “위수탁계약 주요 기재사항” 차등화

- (필요조치) 「전자금융감독규정」 개정

1-3. 연구·개발 분야 망분리 개선

☞ IT 개발 환경 개선을 통해 혁신적인 금융상품 개발 활성화 등 소비자 효용이 증진될 수 있도록 하겠습니다.

□ (현행) '22.11월 연구·개발망 망분리 예외가 허용되었으나, 연구·개발망과 내부망간 물리적 분리 등의 제한으로 실효성 저하*

* 구축 비용의 문제로 도입이 어렵고, 연구개발망에서 개발된 결과물의 내부망 전송 곤란

- 또한, 연구·개발망에서의 개인신용정보 활용이 금지됨에 따라, 고객별 특성·수요에 맞는 혁신적인 서비스 연구·개발에 제한
- he업종은 IT개발자 등의 재택근무가 보편적이나 금융권은 IT 개발자 재택근무가 불가하여 우수인력의 유출 등 문제

□ (개선) 연구·개발망과 업무망간 논리적 망분리를 허용하고, 소스코드 등 연구·개발 결과물의 망간 이동 편의 확대

- 망분리 예외 허용에 따른 강화된 보안대책* 마련

< ※ 연구·개발 망분리 예외에 따른 “강화된 보안대책 (예시)” >

- 연구개발망-전산실간 소스코드 전송 등 제한적 통신 허용, 인가된 서버·단말만 전산실 접속통제 등
- 데이터 전송시 악성코드 감염 여부, 인가된 파일 여부(확장자 등) 등 사전 검사
- 데이터 이동 내역, 망분리 예외 정책 설정(신규, 삭제, 변경) 등에 대한 주기적 감사 실시
- 가명정보를 원래의 상태로 복원하기 위한 추가정보는 분리하여 암호화 및 별도 보관

- 가명처리된 개인신용정보 활용을 허용*하여 고객 행동 특성 등 데이터 분석 기반의 혁신적인 금융상품 개발 환경 제공

* 단, 관련 법령(「전자금융감독규정」, 「개인정보보호법」)에 따른 국외 이전 제한 이슈 상존

- 연구·개발망을 통한 IT개발자 등의 재택근무 가능

□ (필요조치) 「전자금융감독규정」 및 「전자금융감독규정 시행세칙」 개정

* 연구개발망 활용범위 등에 대한 상세 지침*은 추후 가이드라인 등을 통해 별도 안내

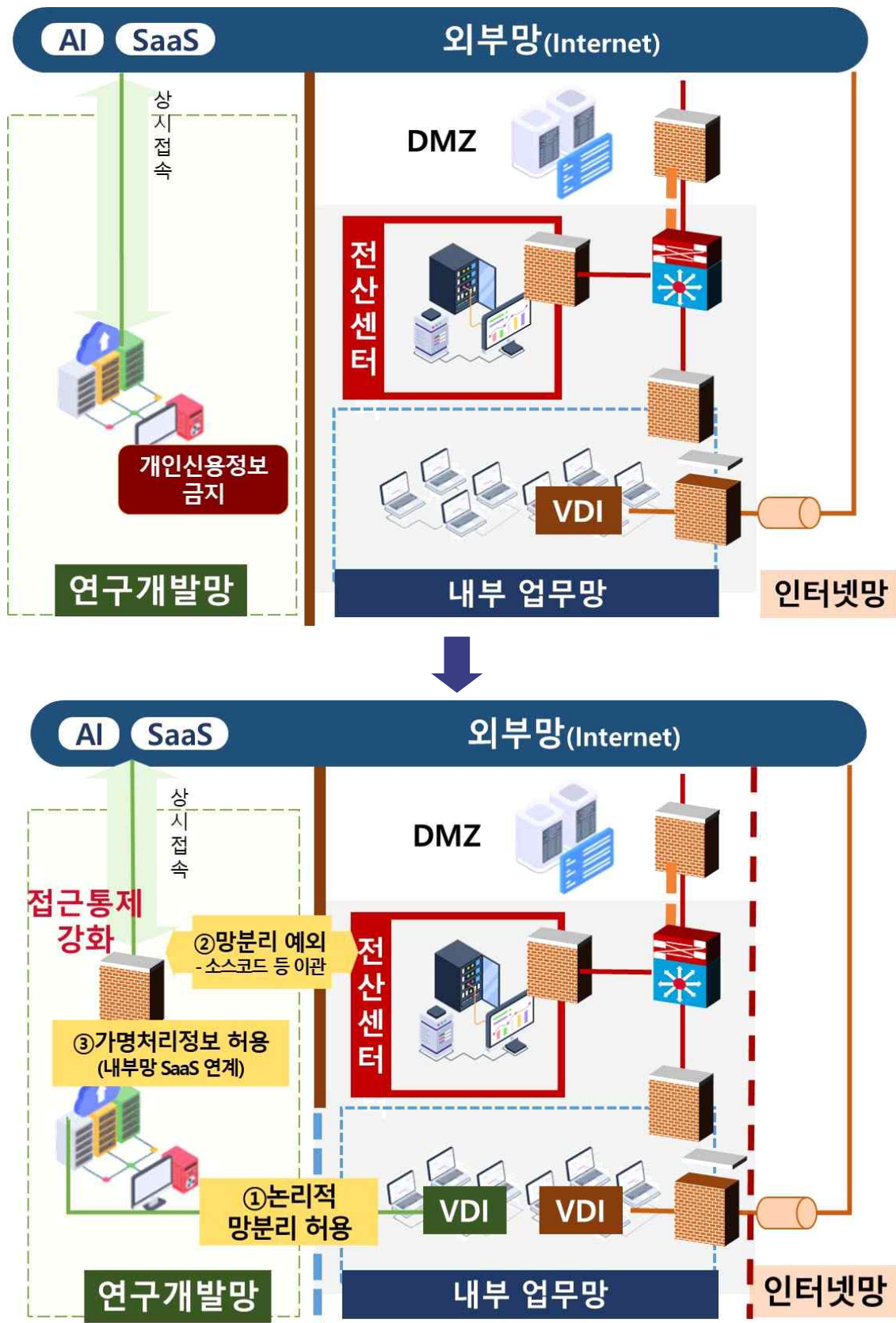
< ※ “연구·개발망 활용범위 등 상세지침 (예시)” >

✓ 스테이징(staging) 단계*부터는 내부망에서 수행

* 운영과 거의 동일한 환경에서 실제 데이터로 최종 확인을 하는 단계

✓ 충분한 보안대책을 갖추지 못한 경우 최소단위 시스템 테스트만 연구개발망 內 수행 등

< 연구·개발 분야 망분리 개선안 구성도 (예시) >



※ 상기 구성도는 대표적 사례로 금융회사 등의 환경에 따라 세부 구성 방식이 다를 수 있음

2-1. 기존 규제 특례의 정규 제도화

☞ '생성형 AI' 및 '임직원 업무망에서의 SaaS 활용' 관련 1단계까지의 규제 특례에 대해서는 충분한 성과검증을 거쳐 '25년 말까지 정규 제도화 하겠습니다

□ (개선방향) '샌드박스 사례누적 및 성과검증 → 정규 제도화 및 샌드박스 추가 확대'를 통해 '변화→적응'을 반복하는 점진적 규제개선

- 생성형 AI 및 임직원 업무망에서의 SaaS 관련 규제특례의 경우 효용성 평가와 보안 검증을 거쳐 상시 제도화 추진

※ ('24.3Q) 샌드박스 접수 및 허용* → ('25.上) 서비스 활용 개시 →
(~'25.3Q) 효용성 평가 및 보안검증 → ('25.4Q) 감독규정 개정 등 제도화 추진

* 기존에 허용되었던 M365, ERP 등의 규제특례도 제도화 추진과제에 함께 포함

□ (필요조치) 「전자금융감독규정」 개정

2-2. 개인신용정보 처리 허용 등 규제 특례 고도화

☞ 가명정보가 아닌 실제 개인신용정보를 직접 처리할 수 있도록 규제특례를 추가 확대해 나가겠습니다

□ (개선방향) 1단계 과제에 대한 충분한 성과검증과 보안평가 등을 거친 후, 추가 보안대책을 전제로 실제 개인신용정보 처리까지 허용

- 실데이터 기반의 금융상품 개발 및 고객관계관리(CRM) 고도화 가능

□ (필요조치) 규제샌드박스 조건 수정

- 더불어, 개인신용정보를 클라우드로 처리할 경우 해당 정보처리 시스템을 국내 설치토록 하는 「전자금융감독규정(§14의2⑧)」 정비 검토

※ 단, 「개인정보보호법」에 따른 개인정보 국내 처리·보관 등의 이슈는 여전히 존재

2-3. 제3자 리스크(3rd-party risk) 관리 강화 등 정보처리 위탁제도 정비

☞ 선진 해외사례 연구를 통해, 금융社에게 정보처리를 위탁받은 제3자에 대한 감독·검사권 마련 등 정보처리 업무위탁 제도를 정비하겠습니다

□ (현행) 최근 클라우드, 데이터센터 등 정보처리 업무 위탁이 증가하고 있음에도 불구하고 실효성 있는 제3자 리스크* 관리 규율 부재**

* 非금융부문의 장애 발생, 정보유출 등의 사고가 금융 부문으로 전이되는 리스크

** 금감원 행정지도, 「금융분야 클라우드 이용 가이드라인」 등을 통해서만 제한적으로 관리 중

○ 정보처리 위탁 업무의 중요도·위험성 등 다양한 특성을 고려하지 않은 일률적 통제와 보고체계로 인해 금융회사 등의 부담 존재

□ (개선방향) 망분리 규제 개선에 따른 SaaS, 생성형 AI 등 활용 확대에 대응하여 제3자 리스크 관리 강화 등을 위한 제도 정비 (「전자금융거래법」 또는 「정보처리 위탁규정」 개정)

○ 新 금융보안체계 구축을 위한 연구용역을 통해 해외의 선진 사례를 분석하고, 국내 환경에 맞는 도입 방향 등을 검토

- 수탁자(제3자)에 대한 금융당국의 검사·감독 권한 등의 법적 근거 마련 및 권한 행사에 따른 실효성 확보 방안 논의

- 제3자 위탁업무의 중요도·위험성 등에 따른 차등화된 보호 조치와 보고 체계 구축

< EU, 영국의 제3자 규제 사례 >

◆ (EU) 주요 제3자에 대한 직접(현장) 조사·감독 권한 및 감독기관 권한행사 미준수시 금전제재 부과* 등을 법에 명시(DORA : Digital Operational Resilience Act)

* 법령 준수 달성시까지 6개월의 범위 내에서 매일 일 평균 매출액의 1% 이내 부과 가능

- 벌금액 결정시 주무감독관과의 협력수준 등 반영 → 조사감독시 협조의무 추가 확보

◆ (영국) 주요 제3자가 금융시장법(FSMA 2023)상 요구사항 위반시, 금융기관에게 해당 제3자와의 서비스 제공 중단 및 계약체결 금지 등 요구 가능

- 위탁계약 중요성·위험별로 차등화된 통제 적용(PRA Outsourcing & Third party risk management)

☞ 자율보안-결과책임 원칙에 입각한 新 금융보안체계를 구축하겠습니다

- (현행) 세세한 보안수단 규정에 열거, "규정만 지키면 면책"이란 인식 만연
- 금융회사는 최소 기준만을 준수할 뿐 적극적 보안투자에 소홀하고, 일률적·경직적 규정으로 인해 IT 리스크에 유연한 대응이 어려움
- (개선방향) 자율보안-결과책임 원칙에 입각한 新금융보안체계 구축을 위해 「디지털금융보안법(가칭)」을 제정, "규칙(Rule) → 원칙(Principle)중심"으로 규제 전환
- ① 금융당국은 법령을 통해 주요 보안 원칙·목표를 제시하고, 구체적·기술적 보안 통제사항은 가이드로 모범사례 제시(준수 의무사항은 아님)
- 금융회사는 업무환경, 인프라, 보안역량 등에 대한 자체 리스크 평가를 통해 자율적으로 세부 보안통제를 구성하고 당국에 보고

< 뉴욕주 금융 사이버보안 규정(23 NYCRR 500) >

- ◆ 정보보호의 3요소인 '기밀성', '무결성', '가용성'을 원칙으로 제시하고, 금융회사 등이 보안체계를 수립하도록 최소한의 의무만을 부여
- ◆ 프로그램 보안, 다중 인증, 암호화 등의 구체적 수단을 특정하지 않고 금융회사 등이 내부 위험평가 등을 통해 보안기술 등을 자율 채택하도록 규정

- ② 전산사고 등에 대한 배상책임 강화, 실효성 있는 과징금 도입 등 금융회사의 책임 강화를 위한 법적 근거 마련
- 중요 보안사항의 최고경영자(CEO) 및 이사회 보고의무, 정보보호 최고책임자(CISO) 역할 확대 등 금융회사의 내부 보안체계를 강화

< EU, 미국(뉴욕주) 과징금 사례 >

- ◆ 위반의 경중에 따라 매출액의 일정 비율을 과징금으로 부과하도록 규정
 - * (EU) Digital Operational Resilience Act, (미국 뉴욕주) 뉴욕 은행법, 뉴욕 금융서비스법
 - ** 유출 사고 등 발생 여부, 고의 또는 과실에 의한 위반, 과거 위반 또는 제재 횟수 등
- ◆ 실제 보안규정 위반에 대한 과징금도 집행되고 있는 상황
 - * (뉴욕주) 대출 중개사 A사에 보안관리 미흡 접근통제 부실 등을 이유로 425만 달러(약 57억원) 벌금 부과(23.5월)

- ③ 금융당국은 금융회사의 자율보안체계 수립·이행 등을 검증하고,
- 점검 결과 일정 수준 이하의 금융회사의 경우 보안수준 제고를 위한 시정요구·이행명령을 부과, 불이행시 엄중제재 및 영업정지 등 조치
- ※ 영국은 금융회사 보안 수준이 적정치 않은 경우 문제점, 개선 요구사항, 이행기간 등을 통지하고 미이행에 대한 제재조치 부과 등을 통해 보안 수준을 지속 관리(FSMA : 금융시장법)

IV. 향후 계획

- ('24.8월) 「금융권 망분리 TF」 논의 결과를 바탕으로,
「금융분야 망분리 개선 로드맵*」 발표

* 1.2.3단계 규제개선 내용 및 추진일정



- ('24.3분기) ①사전설명회 및 업권별 보안컨설팅 등 진행
②규제샌드박스 신청 접수 및 허용(계속)
③SaaS 이용절차 개선 관련 「전자금융감독규정」 개정(계속)
④연구·개발 망분리 개선 관련 「전자금융감독규정」 개정(계속)
⑤新 금융보안체계 구축을 위한 연구용역



- ('24.4분기) ①제3자 리스크 관리 강화 등을 위한 정보처리
업무위탁 제도 정비방안 마련
②「디지털 금융보안법(안)」 마련



- ('25.상반기) ①규제샌드박스 성과 검증
②규제샌드박스 추가 확대방안 마련
③「디지털 금융보안법(안)」 발의



- ('25.하반기) ①규제샌드박스 내용의 정규 제도화
②규제샌드박스 추가 확대방안 신청 접수 및 허용
③「디지털 금융보안법(안)」 입법 추진*

* 금융회사 등의 보안역량 확충을 위한 충분한 유예기간 부여 예정



- ('26.이후) ①규제샌드박스 추가 확대방안 성과 검증
②「디지털 금융보안법(안)」 시행을 위한 준비작업

구 분	~`24.3Q	~`24.4Q	~`25.上	~`25.下
① 생성형 AI 활용	규제샌드박스 접수 및 허용		규제샌드박스 성과 검증	규제샌드박스 정규 제도화
			규제샌드박스 추가 확대 방안 마련	규제샌드박스 추가 확대 접수 및 허용
② 업무망에서의 SaaS 이용	규제샌드박스 접수 및 허용		규제샌드박스 성과 검증	규제샌드박스 정규 제도화
			규제샌드박스 추가 확대 방안 마련	규제샌드박스 추가 확대 접수 및 허용
③ SaaS 이용절차 개선	클라우드 이용절차 관련 「전자금융 감독규정」 개정			
④ 연구개발 분야 망분리 개선	연구개발 관련 「전자금융 감독규정」 개정			
⑤ 제3자 리스크 관리 강화	1단계 2단계	정보처리 업무위탁제도 정비방안 마련		
⑥ 新 금융보안 체계 구축	연구용역 발주	「디지털 금융보안법(안)」 마련	「디지털 금융보안법(안)」 발의	입법 추진(계속)

3단계