Headline

금융권 망분리 규제 개선 방안

컨설팅사업그룹 금융컨설팅 2 팀 박춘복 수석

■ 개요

2013 년 3 월 20 일 대규모 전산망 마비 사태가 발생해 주요 언론사 및 금융사들이 막대한 피해를 입었다. 정부 발표에 따르면 북한 정찰총국의 소행으로 추정되며, 2012 년 6 월 28 일부터 피해기관에 악성코드를 점차적으로 유포해 온 것으로 분석된다. 해당 사고는 금융거래 중단과 고객 개인정보 유출 등 심각한 피해를 일으켰으며, 이를 계기로 '공공부문'의 물리적 망분리 규제가 도입되면서 현재까지 10 년 이상 운영되고 있다.

■ 금융분야 망분리란

망분리 규제는 외부의 침입으로부터 내부 전산 자원을 보호하기 위한 보안 방식이다. 내부망과 외부망을 물리적으로 분리해 네트워크상의 접속을 제한하는 것이다. 해당 규제는 2014 년 말부터 금융분야에 적용됐다. 금융회사와 전자금융업체들은 내부망에 연결된 전산시스템과 단말기를 외부망과 물리적으로 분리해 해킹 등 외부 공격으로부터 안전을 확보할 수 있었다. 때문에 물리적 망분리는 시스템 간의 연결을 차단하고 특정 환경에서만 접속을 허용함으로써 보안을 강화하는 중요한 조치로 자리잡았다. 이를 통해 전산시스템에 대한 외부의 위협을 차단하고 사고 발생 시 피해를 최소화하는 효과를 기대할 수 있었다.

■ 금융분야 망분리의 문제점

그런데 망분리 규제가 금융회사 및 전자금융업체들이 업무를 수행하는 데 있어 비효율성을 초래하고, 새로운 기술을 적용하거나 연구·개발 활동을 진행하는 데 어려움을 겪게 만든다는 지적 또한 지속적으로 제기되어 왔다. 특히 최근 소프트웨어 시장이 클라우드 기반의 서비스형 소프트웨어(SaaS)로 급변하고 생성형 AI 의 사용이 산업 발전에 중요한 영향을 미치는 상황에서, 망분리가 업무의 불편을 넘어서 국내 금융산업의 경쟁력 저하를 초래할 수 있다는 우려까지 나오고 있다. 더 나아가 일부 금융기관들은 외부 통신과의 완전한 분리는 이루었지만, 선진 보안체계 도입에 소홀하거나 변화하는 IT 환경에 맞는 적절한 보안 대책을 마련하지 않아 오히려 국내 금융권 보안 발전을 저해하는 부정적인 영향을 미치고 있는 상황이다.

* 출처: 금융위원회

그림 1. 망보안 관리의 이상(Ideal)과 현실(Reality)

■ 망분리 규제 개선 방안

2024 년 8 월 13 일 금융위원회에서는 「금융분야 망분리 개선 로드맵」(이하 로드맵)를 발표했다. 금융회사 등의 생성형 AI 활용을 허용하고 클라우드(SaaS) 이용 범위를 대폭 확대하는 것은 물론 연구·개발 환경을 적극 개선한다는 것이 주요 골자다. 중·장기적으로는 금융보안 법·체계를 전면 개편해 자율보안-결과책임 원칙으로 규제 선진화의 방향성을 제시하고, 금융회사 등이 자체적인 역량 강화를 통해 미리 대비할 수 있도록 지원하겠다고 밝혔다. 또한 현행 금융보안체계가 오랜 기간 인터넷 등 외부통신과 분리된 환경을 전제로 구성되어 온 점을 고려해, 급격한 규제 완화보다는 단계적 개선을 추진하겠다고 전했다. IT 환경 변화로 인해 신속한 대응이 필요한 과제는 샌드박스 등을 활용해 규제 애로사항을 즉시 해소하되, 자율보안체계 확립까지는 시간이 소요되므로 보안상의 문제가 없도록 별도의 보안대책 등 충분한 안전장치를 마련하겠다는 것이다.

■ 망분리 규제 개선 방안의 단계별 세부 추진과제

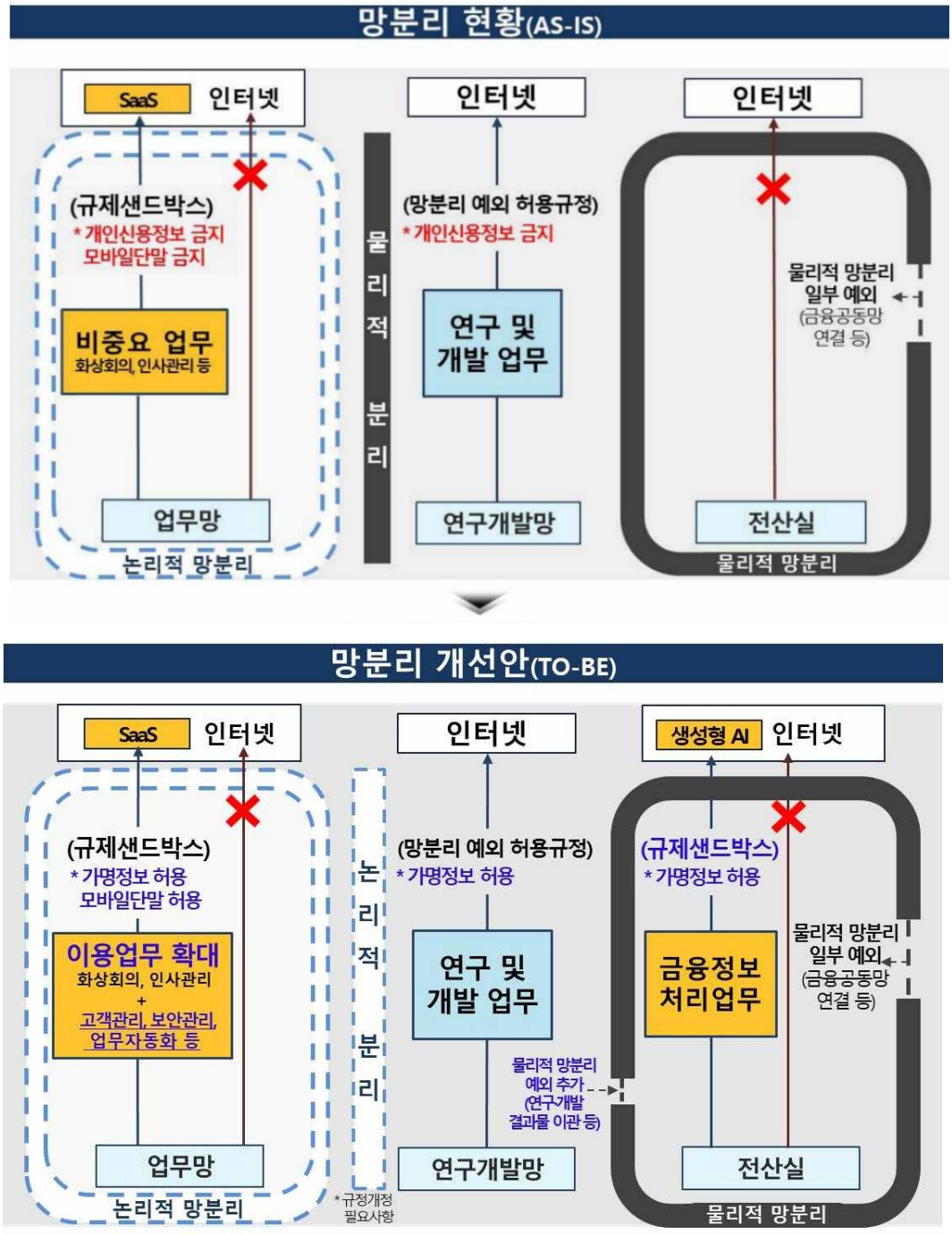
<table>
<tr><th>1단계</th><th>2단계</th><th>3단계</th></tr>
<tr><td>1) 생성형 AI 허용(규제 샌드박스)
: 생성형 AI를 활용해, 가명정보*까지 처리할 수 있도록 규제특례 허용
* 추가정보 사용 없이는 특정 신용정보주체를 알아볼 수 없도록 가명처리된 개인신용정보</td><td>4) 1단계까지의 규제특례 정규 제도화
: 샌드박스로 성과 검증*된 과제
→ 규정 개정 등 제도화 추진
* ~`25.上 : 샌드박스 운영사례 성과 검증</td><td rowspan="3"><b>7) 「디지털 금융보안법(가칭)」 제정</b><br>* 연구용역(`24.3Q), 공청회(4Q)를 거쳐 연내 마련 추진
- 자율보안-결과책임의 보안체계 구축
: 목표·원칙중심으로 규제 전환
- 금융권 책임 강화
: 배상책임 강화, 실효성 있는 과징금 등
: CISO 권한 확대 및 CEO·이사회 보고의무
- 금융당국의 점검·이행명령 등 금융권 보안수준 제고 뒷받침</td></tr>
<tr><td>2) 클라우드 이용 확대(규제 샌드박스)
<table>
<tr><th></th><th>현행</th><th>개선</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></td><td>5) 규제특례 확대·고도화
: 개인신용정보 처리 등 리스크↑ 업무 → 강화된 보안대책 전제로 추가 허용</td></tr>
<tr><td>3) 연구·개발 분야 망분리 개선(감독규정 개정)
<table>
<tr><th></th><th>현행</th><th>개선</th></tr>
<tr><td>연구·개발망 ↕ 업무망 간</td><td rowspan="2">물리적 망분리</td><td>논리적 망분리</td></tr>
<tr><td>연구·개발망 ↕ 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></td><td>6) 제3자 리스크 관리강화 등을 위한 정보처리 위탁제도 정비</td></tr>
</table>

* 출처: 금융위원회

표 1. 단계별 세부 추진과제

1) 금융회사 등의 생성형 AI 활용 허용

- 대부분의 생성형 AI 가 클라우드 기반의 인터넷 환경에서 제공되는데, 국내 금융권의 경우 인터넷 등 외부 통신 활용의 제한 등으로 인해 생성형 AI 도입에 제약이 있는 상황
- 이에 샌드박스를 통해 인터넷 활용 제한 등에 대한 규제 특례를 허용
- 이와 함께, 예상되는 리스크에 대한 보안대책을 조건으로 부과하고 금융감독원·금융보안원이 신청 기업별 보안 점검·컨설팅을 실시하는 등 충분한 안전장치를 마련할 계획



* 출처: 금융위원회

그림 2. 망분리 개선 단기 추진 과제 종합 구성도

2) 클라우드 기반의 응용 프로그램(SaaS) 이용 범위 대폭 확대

- 기존에는 문서관리·인사관리 등 비 중요 업무에 대해서만 SaaS 이용이 허용되고, 고객 개인신용정보는 처리할 수 없는 등 엄격한 샌드박스 부가 조건이 부과돼 SaaS 활용이 제한
- 앞으로는 보안관리, 고객관리(CRM) 등의 업무까지 이용 범위를 확대하고, 가명정보 처리 및 모바일 단말기에서의 SaaS 이용까지 허용하는 등 SaaS 활용도를 제고할 예정
- 마찬가지로 규제 특례 확대에 따른 보안 우려에 대응하기 위해 보안대책을 마련해 샌드박스 지정 조건으로 부과할 계획

3) 금융회사 등의 연구·개발 환경 개선

- 2022 년 11 월 연구·개발 환경에서 인터넷을 자유롭게 활용할 수 있도록 한차례 규제가 개선되기는 했으나, 여전히 연구·개발 환경의 물리적 분리 및 개인신용정보 활용 금지 등 때문에 고객별 특성·수요에 맞는 혁신적인 서비스 연구·개발에 제약이 크다는 지적이 지속적으로 제기
- 이에 따라「전자금융감독규정」을 개정하여 금융회사 등이 연구·개발 결과물을 보다 간편하게 이관할 수 있도록 물리적 제한을 완화하고, 가명정보 활용을 허용하는 등 혁신적인 금융상품을 개발할 수 있는 환경 제공

4) 1 단계까지의 규제특례 제도화

- '생성형 AI' 및 '임직원 업무망에서의 SaaS 활용' 관련 1 단계까지의 규제 특례에 대해 효용성 평가와 보안 검증을 거쳐 2025 년 말까지 정규 제도화 및 샌드박스 추가 확대
- (`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

5) 개인신용정보 처리 허용 등 규제 특례 고도화

- 가명정보가 아닌 실제 개인신용정보를 직접 처리할 수 있도록 규제특례 추가 확대
- 1 단계 과제에 대한 충분한 성과검증과 보안평가 등 추가 보안대책을 전제로 실제 개인신용정보 처리까지 허용할 예정

6) 제 3 자 리스크(3rd-party risk) 관리 강화 등 정보처리 위탁제도 정비

- 최근 클라우드, 데이터센터 등 정보처리 업무 위탁이 증가하고 있음에도 실효성 있는 제 3 자 리스크 관리 규율이 부재함에 따라, 선진 해외사례 연구를 통해 금융사에게 정보처리를 위탁 받은 제 3 자에 대한 감독·검사권 마련 등 정보처리 업무위탁 제도를 정비할 예정
- 新금융보안체계 구축을 위한 연구용역을 통해 해외의 선진사례를 분석하고 국내 환경에 맞는 도입 방향 등을 검토할 예정

7) 디지털금융보안법(가칭) 제정

- 현재 세세한 보안수단 규정에 열거, "규정만 지키면 면책"이란 인식이 만연해 최소 기준만을 준수할 뿐 적극적 보안투자에 소홀하고 일률적·경직적 규정으로 인해 IT 리스크에 유연한 대응이 어려움
- 이에 따라 자율보안-결과책임 원칙에 입각한 新금융보안체계 구축을 위해 디지털금융보안법(가칭)을 제정해 주요 보안 원칙·목표를 제시하고, 구체적·기술적 보안 통제사항은 가이드로 모법사례 제시할 예정
- 또한 전산사고 등에 대한 배상책임 강화, 실효성 있는 과징금 도입 등 금융회사의 책임 강화를 위한 법적 근거 마련

■ 금융분야 망분리 개선 추진현황

생성형 AI 활용 등 관련 규제 샌드박스는 각 협회 및 금융규제 샌드박스 웹페이지(sandbox.fintech.or.kr)를 통해 안내했으며, 금융위원회는 2024 년 11 월 27 일 정례회의를 통해 생성형 AI 를 활용한 9 개 금융회사의 10 개 혁신금융서비스를 처음으로 지정했다. 이번 혁신서비스 지정과 관련해 김병환 금융위원장은 "생성형 AI 활용을 위한 혁신금융서비스 지정 신청이 141 건이나 될 정도로 많이 접수됐다. 이를 통해 금융회사들의 망분리 규제개선에 대한 열망과 혁신에 대한 강한 의지를 느낄 수 있었다"고 밝혔다. 그리고 "금융소비자들이 규제개선 혜택을 빠르게 체감할 수 있도록 금융회사들이 지정된 혁신서비스를 신속하게 시장에 출시하고, 혁신과 보안의 균형을 위해 탄탄한 보안체계 하에서 서비스를 제공할 필요가 있다"고 당부했다. 한편, 지난 2024 년 8 월 발표한 「금융분야 망분리 개선 로드맵」에 따라 금융회사의 생성형 AI 및 서비스형 소프트웨어(SaaS) 활용이 폭넓게 허용됐다. 이에 따라 '24.9.16~27 일 혁신서비스 신청 기간 중에 74 개사의 141 개 혁신서비스가 망분리 규제 특례를 요청하는 내용으로 신청·접수됐다고 발표했다.

구분	신청 서비스명	주요 서비스 내용
신한은행	생성형 AI 기반 AI 은행원	자연어 기반 금융 상담 제공, 외국어 변역 제공 등
	생성형 AI 투자 및 금융지식 Q&A 서비스	자연어 기반 각종 뉴스요약, 과거수익률 정보, 시장흐름 정보 등 제공
KB은행	생성형 AI 금융상담 Agent	고객 질의 시 고객 친화적 대화·상담 제공 등
NH은행	생성형 AI 플랫폼 기반 금융서비스	외국인 고객을 위한 AI은행원, 고령층을 위한 상담 서비스 제공 등
카카오뱅크	대화형 금융 계산기	자연어 기반 금융상품 관련 이자·환율 등 계산
NH증권	생성형 AI 대고객 시황정보 서비스	맞춤형 시황 정보 실시간 요약 제공
KB증권	AI 통합금융플랫폼 캐비	환전, 자산관리 등 대화형 서비스 제공
교보생명	보장분석 AI 서포터	설계사에게 고객의 보장분석보고서에 기반한 맞춤형 설명 스크립트 제공 등
한화생명	생성형 AI 활용 고객 맞춤형 화법 생성 및 가상 대화 훈련 솔루션	설계사에게 최신 뉴스 등을 통한 세일즈 화법 제공
KB카드	생성형 AI 활용 모두의 카드생활 메이트	고객 상황에 맞는 카드상품 비교, 발급 등 대화형 금융서비스 제공

*출처: 한국핀테크지원센터 금융규제 샌드박스

표 2. 혁신금융서비스 지정 주요내용

■ 맺음말

금융권 망분리 규제 완화는 디지털 금융 혁신을 촉진하고 효율적인 업무 환경을 조성하는 중요한 전환점을 의미한다. 다만 규제 완화가 가져올 수 있는 보안 위험에 대한 충분한 대비가 필요하며, 이에 따른 정책적 안정성도 동시에 고려되어야 한다. 3 단계(세부 7 단계)의 로드맵을 원활하게 진행하고, 향후 규제 완화가 금융시스템의 안전성과 효율성을 동시에 높이는 방향으로 발전하기 위해서는 지속적인 모니터링과 신속한 대응체계 구축이 필수적이다. 이를 통해 금융산업의 성장과 보안이 조화를 이루는 환경을 만들어 나가야 할 시점이다.