

# 10년 늦춰진 금융산업, AI·클라우드를 디지털 혁명 시작

## 금융사 망분리 규제 완화

지난 2013년 금융사 대규모 전산망 마비 사태로 금융사에 엄격하게 적용되던 망분리 규제가 완화된다. 망분리 규제는 무려 10년 넘게 금융사의 업무 비효율을 키우면서 금융산업의 발전을 저해시킨 요인으로 꼽힌다. 이번 규제 완화로 금융권은 생성형 AI를 활용한 다양한 혁신 금융 상품 출시를 기대하고 있다.

### ◆ '갈라파고스 규제' 금융사 망분리 풀린다

금융사에 엄격하게 적용되던 망분리는 지난 2013년 금융사 대규모 전산사고를 계기로 인터넷 등 외부 통신과 분리된 환경을 전제로 운영되어 왔다.

다른 산업군에서 누구나 사용할 수 있는 글로벌 클라우드 서비스가 금융권에서만 사용할 수 없었다. 10년간 금융사의 업무 비효율을 키운 것이다.

### 금융위, '망분리 개선 로드맵' 발표 샌드박스 활용 AI·클라우드 규제 완화 SaaS 적용 영역 확대에 혁신 예고 디지털금융보안법, 자율보안 확립

망분리 규제란 금융사가 외부 침입으로부터 내부 전산 자원을 보호하기 위해 내부망과 외부망을 나누는 네트워크 보안 기법 적용을 의무화한 것이다. 내부망과 외부망에 접속하는 단말기를 물리적으로 분리(PC 두 대 사용)하거나, 가상화 기술 등을 사용해 구분한다.

하지만 시대가 변화하면서 디지털 시대가 개막했고 인공지능(AI)과 서비스형 소프트웨어(SaaS) 등 외부 기술과 인프라를 활용하려는 수요가 높아지면서 망분리 체계는 금융권 발전을 저해하는 요소로 꾸준히 지적됐다.

금융위원회는 지난 8월 금융협회, 금융감독원, 금융보안원 등 유관기관이 참여한 가운데 '금융분야 망분리 개선 로드맵'을 발표했다.

망분리 규제완화는 충분한 안전장치를 전제로 단계적으로 진행된다.

1단계로 급격한 IT 환경 변화 때문에 신속한 대응이 필요한 과제의 경우 샌드박스를 통해 인터넷 활용 제한 등에

## PCI-DSS와 국내 망분리 접근방식 비교

	PCI-DSS	한국
망분리 개념	망세분화(network segmentation)	내부망과 외부망 차단
망분리 목적	관리비용 절감 & 기술적 전문화	사고발생 방지
망분리 방식	물리적·논리적 망분리 모두 가능	물리적 망분리
보호대상	핵심정보	내부정보

## 주요국가 망분리 규제방식 비교

	규제원칙	재량권 수준	금융회사의 책임성
한국	망분리의 의무 부과 - 금융회사의 책임인식 저조	낮음(망분리 방식 지정)	- 낮은 수준의 과징금·과태료
미국	- 네트워크 구분·접근통제를 통한 보안 확보 - 금융회사의 책임성	높음(망분리 방식 선택)	- 규제위반의 심각성을 고려한 사후 규제 - 금전적 제재 중심
유럽	- 정보데이터의 기밀성, 무결성, 가용성 보장 - 금융회사에 강한 책임 요구	높음(망분리 방식 선택)	- 엄중한 금전적 제재를 통한 사후규제
호주	- 다층화된 정보보안 통제 장치의 마련 - 금융회사의 책임성 강조	높음(망분리 방식 선택)	- 다양한 사후규제 적용 - 벌금, 시정명령, 면허정지 등의 제재

자료/자본시장연구원



김병환 금융위원장. /뉴스1

대한 규제 특례를 허용하고, 문서관리 등 기존 범위를 넘어 SaaS 적용 영역을 확대하는 내용이 담겼다. 대신 추가적인 보안 대책을 운용하도록 했다.

대표적으로 생성형 AI의 금융권 도입이 가능해졌다. 대부분의 생성형 AI는 클라우드 기반의 인터넷 환경에서 제공되고 있는데 국내 금융권은 망분리 규제 때문에 그동안 생성형 AI 도입에 제약이 있었다.

2단계 샌드박스로 금융회사가 활용 가능한 데이터 범위를 가명정보가 아닌 개인신용정보로 넓히는 규제 특례의 고도화도 추진한다. 중장기적으로는 샌드

박스 운영 경험을 토대로 한 금융보안 체계의 선진화도 추진한다. 가칭 '디지털금융보안법'을 제정해 '자율보안-결과책임' 원칙에 입각한 새로운 금융보안체계를 구축한다는 구상이다.

김병환 금융위원장은 "이제는 디지털 기술 없이는 금융을 생각하기 어렵다"며 "언제 어디서나 스마트폰 하나로 모든 금융거래를 처리할 수 있는 수준까지 발전했고, AI 시대에 접어들면서 금융 분야도 경쟁력을 유지하기 위해 새로운 기술을 빠르게 받아들여야 하는 상황"이라고 전했다.

### ◆ 해외사례 참고해 보안강화 필수

금융전산과 관련된 보안확보는 해외에서도 중요한 이슈이다. 미국과 유럽의 망분리 규제는 우리나라와 같이 명문화된 의무규정의 형태가 아니라 가이드라인과 같은 연성규제의 방식을 따른다.

금융회사의 재량권을 인정하는 배경에는 자율규제에 대한 기본적인 신뢰와 사고발생 시 높은 수준의 처벌이 이뤄지는 사후규제가 자리 잡고 있기 때문이다.

실제 미국의 연방거래위원회(Federal Trade Commission·FTC)는 지난 2016년 발생한 데이터 유출사고에 대한 책임을 묻기 위해 지난 2019년 페이스

북(Facebook)에 50억달러에 이르는 벌금을 부과한 바 있다. 50억달러는 페이스북의 이전 회계연도 매출의 약 9%에 해당하는 금액이다.

또한 지난 2019년 7월 대규모 해킹 사고가 발생한 캐피털원은 징벌적 손해배상과 피해 처리 비용 등을 모두 합쳐 1억5000만달러(약 2089억원)를 지불했다. 미국의 전산보안에 대한 사후규제가 얼마나 강한 수준인지를 알 수 있는 부분이다.

유럽의 망분리 규제 역시 미국과 유사하다. 금융회사가 정보통신기술(ICT) 및 보안 리스크 관리 시 필요한 사항을 명시한 가이드라인을 제시하되, 구체적인 실행방안은 금융회사가 판단해 선택하도록 재량권을 부여하고 있다.

사후규제는 기업이 정보보안을 적절히 수행하지 못해서 개인정보를 유출하거나 다른 유형의 소비자 피해가 발생할 경우 2000만유로와 기업 전체 매출의 4%중에서 높은 금액을 과징금으로 부과한다.

### 미국과 유럽, 금융사 자율규제 강화 韓, 해외사례 참고 보안 규제 개선 보안 대책 강화 등으로 안전성 확보 단계적 규제 완화 통해 경쟁력 제고

해외의 금융당국과 금융회사는 망분리 규제에 대해 포괄적인 관점에서 유연하게 접근하지만 보안책임은 무겁게 묻고 있다.

이처럼 국내 금융당국 역시 해외 망분리 사례와 국제기구의 권고사항을 비교 분석해 '데이터 금융 보안법'(가칭) 제정 후 '원칙' 중심의 규제를 신속히 만들어야 한다.

황세운 자본시장 연구원은 5일 "금융회사는 대규모 보안사고의 위험성이 높아질 수 있음을 감안해 비용증가가 수반되더라도 높은 수준의 보안리스크 통제체계를 확립해야 한다"며 "금융당국은 금융회사의 자율적인 금융전산보안 체계에 대해 정기적인 검사를 진행하고, 보안상의 문제점이 발견될 경우 이에 대한 시정조치를 요구해 사고발생 시에는 금융회사에 엄격한 제재를 부과해야 한다"고 말했다.

/이승용 기자 lsy2665@metroseoul.co.kr



Chat GPT에 의해 생성된 금융 산업의 디지털 변화를 시각적으로 표현한 이미지.