BKL 디지털금융 전략가이드 시리즈

금융산업의 디지털화와 글로벌화가 빠르게 진행되면서, 기업과 개인은 과거에 경험하지 못한 새로운 법적 리스크에 직면하고 금융 시스템 전반에 대한 까다로운 규제 환경 속에 놓이게 되었습니다.

이에 따라, 법무법인(유한)태평양의 미래금융전략센터는 디지털금융시대에 직면한 여러분이 꼭 알아야 할 법률 이슈들을 통해 현재와 미래를 위한 솔루션을 제시하고자 "BKL 디지털금융 전략가이드" 시리즈를 시작하게 되었습니다. 이 시리즈는 미래금융전략센터의 법률 전문가들이 분석한 디지털금융산업의 최신 동향을 통해, 기업과 개인이 직면할 수 있는 다양한 법적 문제들을 미리 파악하고, 디지털금융산업에 대한 새로운 시각과 선제적인 전략을 제시하는 것을 목표로 합니다.

이 시리즈는 총 9회차에 걸쳐 매주 제공되며, 각 회차별 주요 주제는 다음과 같습니다.

1. 디지털금융과 라이선스
2. **디지털금융시대의 IT 기술 보안 및 정보보호 강화 전략**
3. 디지털금융기업의 글로벌시장 진출전략
4. 혁신금융 서비스 및 샌드박스 활용방안
5. 임베디드뱅킹(Embedded Banking)의 새로운 가능성
6. 자금세탁방지(AML) 트렌드 변화 및 솔루션
7. AI 가 변화시킬 디지털금융의 미래
8. 디지털산업의 규제와 성장
9. 가상자산의 혁신과 기회

미래금융전략센터의 BKL 디지털금융 전략가이드는 매주 새로운 주제를 다루며, 복잡하고 다변화된 디지털금융 시대의 법률 환경에서 독자 여러분이 보다 명확하고 전략적으로 대응할 수 있도록 돕겠습니다.

November 19, 2024

No. 2. 디지털금융시대의 IT 기술 보안 및 정보보호 강화 전략

- 디지털금융 정보보호 강화를 위한 효과적인 방안의 모색

I. 디지털금융보안 現 규율 체계

금융회사 및 전자금융업자가 금융관련 비즈니스를 영위하기 위해서는 은행법 등 해당 업권법에 따라 라이선스를 취득해야 하고, 그 이후의 디지털금융보안 규율은 주로 전자금융거래법 및 감독규정 등을 통해 이루어지고 있습니다. 이와 같은 디지털금융보안의 핵심이 되는 법령인 전자금융거래법 및 감독규정은 그동안 수차례의 해킹 등 보안사고를 거치면서 구체적인 정보보호 수단 및 방법을 열거식으로 나열하는 방향으로 고도화되어 왔습니다. 특히 2013년 3월 금융회사의 대규모 전산망 마비를 계기로 도입된 금융권 망분리는 지금까지의 디지털금융보안 핵심으로 높은 보안성을 유지하는데 큰 역할을 해왔기 때문에 전자금융거래법 등에 따른 주요 의무 및 현재의 규율 체계를 이해하는 것이 핵심입니다.

1. 전자금융거래법 등에 따른 주요 준수 의무

전자금융거래법은 (i) IT 조직 및 시설, (ii) 정보기술, (iii) 내부통제, (iv) 전자금융 등을 각 부문별로 금융회사 등이 준수하여야 하는 다양한 사항을 세부적으로 규정하고 있습니다. 이에 따라 금융회사 등이 디지털금융 보안과 관련하여 준수해야 하는 주요 의무는 다음과 같습니다.

부문	감독규정	주요 규정 사항
IT 조직 및 시설	제3장 제2절, 제3절	• 정보처리시스템 및 전자금융업무 관련 전담 조직 구축 • 정보보호최고책임자 지정, 정보보호위원회 설치·운영 • 전산실 등에 대한 보호대책 수립 운영
정보기술	제3장 제4절	• 단말기, 전산자료, 정보처리시스템에 대한 보호대책 적용 • 해킹, 악성코드 감염 등에 대한 방지대책(물리적·논리적 망분리 등) 수립·운용 • 클라우드컴퓨팅 서비스 이용 절차 준수
내부통제	제3장 제5절	• 정보기술부문 계획 및 정보보호 교육계획 수립·운용 • 정보처리시스템 구축 및 전자금융거래 관련 사업 시 타당성 검토 등

		• 비상대책, 성능관리, 직무분리 등 IT 관련 내부통제 실시
전자금융	제3장 제6절	• 안전한 전자금융거래를 위한 준수사항 적용 및 약관 교부 • 자체 보안성심의 및 취약점 분석 평가 실시 • 정보보안 점검항목 준수 여부 매월 점검

2. 現 규율 체계의 이해

최근 금융IT 환경은 클라우드, 생성형 AI 등 신기술의 출현으로 빠르게 변화하고 있으며 특히, 금융IT의 소프트웨어 시장이 자체 구축형에서 클라우드 기반의 구독형(Software as a Service, 이하 "Saas")으로 빠르게 전환되고, 생성형 AI의 활용이 증가하고 있는 추세입니다. 이에 비례하여 보안사고의 위험도 증가하고 있으나 현행 금융보안 규제는 사전 통제방식의 세세하고 경직적인 규제 체계로 인해 금융IT 환경 변화를 적시에 반영하지 못하여, 새로운 보안 위험에는 효과적으로 대응하지 못하는 한계가 있고, 망분리 규제에 따라 인터넷 연결이 필요한 Saas 등 클라우드 및 생성형 AI를 이용하는데 제약이 있습니다.

이에 따라 규정만 준수하면 면책이라는 인식과 금융회사 및 전자금융업자가 최소한의 규정상 기준만 준수하면 되며, 변화하는 금융IT 환경에 부합하는 보안 조치를 적절히 갖추지 않는 등의 현재의 문제적인 인식의 변화를 통해 금융권 보안 발전이 저해되지 않도록 하는 노력이 필요한 상황입니다.

II. 금융위원회 「금융분야 망분리 개선 로드맵」 발표

이와 같은 상황을 개선하고자, 금융위원회는 디지털금융보안의 現 규율체계를 개선하고 중·장기적으로 금융 보안 법·제도를 전면 개편하는 등 혁신과 보안의 새로운 균형을 찾기 위한 패러다임 전환을 추진할 계획이라고 밝히고 금융분야 망분리 규제 개선을 위한 세부 추진과제와 금융보안체계의 선진화 방향을 담은 『금융분야 망분리 개선 로드맵』(이하 "망분리 로드맵")을 2024.8.13. 발표하였습니다. 망분리 로드맵은 총 3단계로 구성되어 있으며, 각 단계별 추진 과제의 주요 내용은 다음과 같습니다.

1. 1단계 추진 과제

샌드박스를 통해 망분리 규제 특례를 허용하여 금융회사 등의 생성형 AI 활용을 허용하고 Saas 이용 범위를 보안관리, 고객관리 등의 업무까지 대폭 확대하며 금융회사 등의 연구·개발 환경을 개선하기 위해 논리적 망분리를 허용하는 등 규제를 완화하고 있습니다.

개선 대상	변경 전	변경 후
생성형 AI 활용	인터넷 등 외부 통신 활용 제한 등으로 인해 생성형 AI 도입에 제약이 있음	금융회사의 정보처리시스템과 AI 모델 간 연결에 대한 규제특례(샌드박스)를 인정하고, 충분한 안정장치를 마련
SaaS 이용	내부망에서의 SaaS 이용에 대해 규제특례를 부여(2023.9.)하고 있으나, 문서・인사 관리 등 비중요 업무에 대해서만 SaaS 이용이 허용되어 SaaS의 다양한 업무에 대한 활용은 제한됨	보안관리, 고객관리(CRM) 등의 업무까지 SaaS 이용 범위를 확대하고, 가명정보처리 및 모바일 단말기에서의 SaaS 이용까지 허용
연구·개발 환경	연구・개발망에 대한 망분리 예외를 허용(2022.11.)하였으나, 물리적 분리 및 개인신용정보 활용 금지 등 부가조건에 따라 소스코드의 내부망 연계에 불편이 있음	연구·개발망과 업무망 간 논리적 망분리를 허용하고, 향후 가명처리된 개인신용정보의 활용을 허용

2. 2단계 추진 과제

생성형 AI 활용 등 1단계까지의 규제 특례에 대해서는 충분한 성과검증을 거쳐 `25년 말까지 정규 제도화할 예정이며, 가명정보가 아닌 실제 개인신용정보를 직접 처리할 수 있도록 규제특례를 추가 확대하는 한편, 금융회사에게 정보처리를 위탁받은 제3자에 대한 감독·검사권 마련 등 정보처리 업무위탁 제도를 정비할 계획입니다.

3. 3단계 추진 과제

자율보안-결과책임 원칙에 입각한 새로운 금융보안체계 구축을 위해 디지털금융보안법(가칭)을 제정하여, 열거식 행위 규칙(Rule) 중심의 금융보안 규제를 목표·원칙(Principle) 중심으로 전환하고, 금융회사 등은 자체 리스크 평가를 바탕으로 세부 보안 통제를 자율적으로 구성할 수 있도록 할 예정입니다.

다만, 금융회사 등의 책임 강화를 위해 중요 보안사항의 CEO·이사회 보고의무 등 금융회사 등의 내부 보안 거버넌스를 강화하고, 전산사고 발생시 배상책임 확대 및 실효성 있는 과징금 도입 등 법적 근거 마련을 통해 금융회사 등의 보안 노력 제고도 함께 유도할 예정입니다.

마지막으로 금융당국은 금융회사 등의 자율보안체계 수립·이행을 검증하여 미흡한 경우 시정요구・이행명령을 부과하고 불이행시 엄중 제재하는 등 금융권 보안 수준 강화를 위해 지속 노력해 나갈 계획입니다.

III. 금융회사 등을 위한 전략가이드

이상 살펴본 디지털금융보안의 핵심이 되는 전자금융거래법과 망분리 로드맵 등을 종합하여 보면, 디지털금융보안을 강화하기 위해서는 관련 법령 준수 여부를 주기적으로 자체 점검하고 급변하는 금융IT 환경에 맞추어 실질적으로 고객의 자산과 데이터를 보호할 수 있도록 보안대응 방안을 고도화하는 한편, 중장기적으로는 자율보안체계로의 전환을 준비할 필요가 있습니다.

첫째로, **디지털금융보안 관련 법령 준수 여부에 대한 주기적인 자체 점검 및 내부통제를 강화**할 필요가 있습니다. 전자금융거래법 등 디지털금융보안 관련 법령 준수 여부에 대해 금융회사 등은 자체적으로 주기적인 점검을 통해 미흡한 부분을 식별하고 개선하는 활동이 필요합니다. 특히 금융감독원은 '23년 및 '24년 IT검사 방향 발표에서 시스템 장애, 접속 지연 등 소비자 피해와 직접 연관이 있는 (i) 전산시스템 성능관리, (ii) 프로그램·전산원장 통제, (iii) IT부문 비상대책 수립·운용의 3개 분야를 적극적 관리 영역으로 선정하고 중점 관리하겠다고 하였으므로 위 분야들에 대해서는 IT사고가 발생하지 않도록 내부통제를 강화하고, 관련 규정을 준수할 필요가 있습니다.

또한 금융감독원이 2023. 12. 마련한 위반행위별 과태료 부과 기준에 따르면[별첨 참조], 전자금융거래법상 안전성 확보의무 위반 시 지적사항을 모아서 과태료를 부과하였던 기존 과태료 부과 방식에서 위반행위별 부과원칙에 따라 2개 이상의 질서위반행위가 경합하는 경우에는 과태료를 각각 부과하도록 과태료 부과 방식이 변경되어 위법 사항이 적발되는 경우에는 기존보다 다액의 과태료가 부과될 수 있으며, IT검사의 특성상 지적을 받게 되면 로그 등의 증적이 명확하여 반론을 제기하기가 어려우므로, 금융회사 등은 위 중점관리 대상을 포함하여 다른 법규 조항들에 대해서도 사전에 법규를 위반하지 않도록 관리할 필요가 있습니다.

둘째로, **급변하는 금융IT환경 및 보안 위협에 대응하기 위해 실효성있는 보안 대응 방안을 마련하고 고도화**할 필요가 있습니다. 최근에도 정부기관 및 금융회사 등을 상대로 한 해킹시도 및 보안 사고가 지속적으로 발생하고 있습니다. 특히 AI가 발전함에 따라 생성형 AI를 악용한 악성코드 개발, 공격 대상에 허위조작 정보를 유통하는 등 보안 위협 기법이 지능화되고 있는 추세이며, 금융회사 등에 비해 상대적으로 보안이 취약한 오픈소스 소프트웨어 공급망을 우회 공격하고, 딥페이크 기술의 발전으로 인증을 우회하는 등 이를 악용한 금융사기 범죄도 증가할 것으로 예상되고 있습니다.

따라서, 법령상 요구하고 있는 보안대책만으로는 대응에 한계가 있으므로 금융회사 등은 디지털금융 서비스에 대한 실질적인 보안 위협을 식별하고 이를 예방하기 위한 보안 대책을 마련하는 등 지능화되는 보안 위협에 적극적으로 대응하여 고객의 자산과 데이터를 보호할 필요가 있습니다.

마지막으로, **중장기적으로는 금융회사 등은 자체 보안역량을 강화하는 등 자율보안체계로의 전환을 준비하고 추진**할 필요가 있습니다. 그동안 규제 준수라는 소극적인 대응이 아닌 자율보안체계로의 전환시에는 보안의 세부사항 및 대응 수준을 금융회사 등이 스스로 판단하고 대응해야 하므로 자체 보안역량 확보가 중요합니다. 금융당국도 중요 보안사항의 CEO·이사회 보고의무 등 금융회사 등의 내부 보안 거버넌스를 강화하고, 전산사고 발생시 배상책임 확대 및 실효성 있는 과징금 도입 등 법적 근거 마련을 통해 금융회사 등의 보안 노력 제고를 유도할 예정입니다.

따라서 자율보안체계로의 전환을 준비하기 위해서는 관련 규제 환경의 변화를 지속적으로 모니터링하고 보안을 전사적인 가치 및 디지털금융시대의 필수적인 요소로 인식하여 인적·물적 투자는 물론 필요시 외부기관과의 협력을 통하여 보안수준을 향상시켜 금융회사 등에 부여된 자율에 따른 책임을 강화하고 신뢰할 수 있는 디지털금융서비스를 지속적으로 제공할 수 있도록 노력할 필요가 있습니다.

[별첨] 위반행위별 과태료 부과 선례

분류	과태료 수위	공시된 제재 사실
약관 게시·통지 (전자금융거래법 제24조)	1천만원 이하[1]	• 전자금융거래약관을 변경하는 때에 그 시행일 1월 전에 변경되는 약관을 전자적 장치에 게시하고 이용자에게 통지하여야 하는데, 이를 이행하지 않음
전자금융기반시설 취약점 분석· 평가 (전자금융거래법 제21조의3)	2천만원 이하[2]	• **(분석·평가 미실시)** 금융회사는 전자금융거래의 안전성과 신뢰성을 확보하기 위하여 사업연도마다 전자금융기반시설에 대한 취약점 분석·평가를 연 1회 이상(홈페이지는 6개월에 1회 이상) 실시하여야 하는데, 이를 누락함 • **(이행계획 미시행)** 전자금융기반시설 취약점 분석·평가 후 그 결과에 따른 이행계획을 수립·시행해야 하는데도, 동 이행계획에 따른 보완조치를 시행하지 않음
	1천만원 이하[3]	• **(결과 미보고)** 전자금융기반시설 취약점 분석·평가 종료 후 30일 이내 금융위원회에 보고하여야 하는데도, 이를 보고하지 않음
안전성 확보의무 (전자금융거래법 제21조)	5천만원 이하[4]	• **(내부 업무용시스템 망분리 미이행)** 내부통신망과 연결된 내부 업무용시스템을 인터넷 등 외부통신망과 분리·차단 및 접속을 금지하여야 하는데, 본사 임직원의 업무단말기 또는 업무시스템을 외부통신망과 분리·차단하지 않고 연결한 상태로 운영함 • **(프로그램 관리통제 위반)** 금융회사는 정보처리시스템에 대한 중요작업 수행 시 책임자가 이중확인을 하고, 일괄작업 수행 시 책임자가 모니터링 해야 하나 이를 각 이행하지 않고, 프로그램 개발자가 프로그램 반출 및 운영시스템 등록을 직접 수행함 • **(클라우드 이용절차 미이행)** 클라우드 이용절차를 수행하지 않고 클라우드 환경에서 시스템을 사용함

1 전자금융거래법 제51조 제3항 제8호
2 분석·평가 미실시에 대해서는 전자금융거래법 제51조 제2항 제4호, 이행계획 미시행에 대해서는 전자금융거래법 제51조 제2항 제5호
3 전자금융거래법 제51조 제3항 제5호
4 전자금융거래법 제51조 제1항 제1호

*　　*　　*

법무법인(유한) 태평양의 『미래금융전략센터』는 금융 시장의 급격한 변화와 기술의 발전에 발맞춰 고객의 신규 사업모델과 금융기법, 정보통신 기술 분야에서의 다양한 법률자문을 제공하고 있습니다. 특히, 해당 센터의 구성원들은 금융위원회, 금융감독원, 과학기술정보통신부, 행정안전부, 개인정보보호위원회 등 다양한 유관기관 출신 전문가들로 구성하고 있어, 금융, ICT, 데이터, AI 등에 관한 규제 자문부터 대안 모델의 제시, 입법적 해법 등을 아우르는 종합적인 대응 전략을 제시하고 있습니다. 본건 가이드라인 관련 전문가들도 구성원의 일부이니, 토큰증권・가상자산 및 디지털금융분야에서 발생하는 법적 이슈에 대한 자문이 필요하신 경우 언제든지 연락주시기 바랍니다.

관련 구성원

김호진
변호사
T 02.3404.0695
E hojin.kim@bkl.co.kr

임세영
변호사
T 02.3404.7640
E seyeong.im@bkl.co.kr

김현정
변호사
T 02.3404.7657
E hyunjung.kim@bkl.co.kr