디지털 금융 정책 동향

전자금융감독규정 개정안의 주요내용 및 시사점

금융위원회는 2024년 2월 1일 보안 규제의 선진화를 위한 전자금융감독규정 개정안(이하 "**개정안**")을 발표하였습니다.

기존 전자금융감독규정(이하 "**감독규정**")은 전자금융거래의 안전성을 확보하기 위한 보안 수단, 방법을 열거식으로 규정하여 금융회사의 효과적인 보안 수단 및 방법의 도입을 억제한다는 지적이 지적이 있었습니다. 특히, AI, 클라우드 등 기술변화 및 고도화되는 사이버 위협 등에 효과적으로 대응하기 위해 금융보안체계의 유연성 제고와 회복력 강화에 중점을 둔 제도개선의 필요성이 지속적으로 제기되어 왔습니다. 이에, 이번 개정안은 금융보안 규제를 "규칙(Rule) 중심에서 원칙(principle) 중심"으로 개선하여 금융회사의 자율 보안의 기초 토대를 마련하였고, 지나치게 미시적이고 세부적인 수범사항을 삭제하여 규제의 효율화를 도모하였습니다.

한편, 최근 타사의 데이터센터 화재 사례로 데이터 관리 및 복원의 중요성이 커짐에 따라 "재해복구센터 확충", "사고 시 이용자 보호 체계 강화" 및 "보안거버넌스 개선" 등 금융 전산의 복원력을 요구하는 규제가 일부 강화되었습니다.

주목할 필요가 있는 이번 개정안의 주요 내용을 정리하면 아래와 같습니다.

1. 개정안의 주요 규제 강화 내용

가. 재해복구센터 설치의무 확대

기존에는 재해복구센터 구축 의무가 없었던 아래 회사들까지 재해복구센터 구축 의무가 확대되었습니다(개정안 제23조 제8항 제6의2호, 제8호 및 제11호). 재해복구센터 설치의무의 경우 개정안 시행 후 최소 6개월 이상의 유예기간이 부여될 예정이나, 재해복구센터를 구축하는데 다소 긴 시간이 소요된다는 점을 고려하였을 때 새롭게 의무가 부여된 회사의 경우에는 사전 준비가 필요할 것입니다.

- "연간 총거래액 2조 원 이상의 전자금융업자(36개사)"

- “총자산 2조 원 이상의 시설대여업자·할부금융업자·신기술사업금융업자(10개사)”
- “자체 전산시스템을 구축하여 운영하는 상호저축은행(12개사)”

현행	개정안
제23조(비상대책 등의 수립·운용) ⑧ 다음 각 호의 금융회사는 시스템 오류, 자연재해 등으로 인한 전산센터 마비에 대비하여 업무지속성을 확보할 수 있도록 적정 규모·인력을 구비한 재해복구센터를 주전산센터와 일정 거리 이상 떨어진 안전한 장소에 구축·운용하여야 한다.	**제23조(비상대책 등의 수립·운용)** ⑧ <좌동>.
<신설>	6의2. 「여신전문금융업법」에 의한 시설대여업자, 할부금융업자, 신기술사업금융업자(다만, 시행령 제11조의3제1항에 해당하는 회사에 한한다.)
8. 「상호저축은행법」에 의한 상호저축은행중앙회	8. ---------- 상호저축은행중앙회 및 자체 전산시스템을 구축하여 운영 하는 상호저축은행
<신설>	11. 「전자금융거래법」에 의한 전자금융업자(다만, 연간 전자금융거래 총액이 2조 원 이상인 회사에 한한다.)

나. 전자금융사고 책임이행보험 한도 상향

전자금융사고에 대한 최저보상한도가 낮은 수준에 머물러 있어 피해자에 대한 실질적인 피해보상에 한계가 있다는 지적에 따라 전자금융사고 관련 책임 이행을 위한 보험 또는 공제에 가입할 시 설정해야 하는 보상한도가 아래와 같이 일부 상향되었습니다(개정안 제5조 제1항).

- 자산 2조 원 이상이 금융투자업자: 5억 원 → 10억 원
- 여신전문금융회사·보험회사·저축은행: 1억 원 → 2억 원
- 선불업자·PG업자 등: 1억 원 → 2억 원

전자금융거래 규모 등을 반영하여 보상한도가 현실화된 것이며, 금융회사 및 전자금융업자는 위 각 내용을 고려하여 보험 또는 공제 조건을 수정할 필요가 있겠습니다.

현행	개정안
제5조(전자금융사고 책임이행을 위한 보험 등의 가입에 관한 기준) ① 금융회사 또는 전자금융업자가 법 제9조 제4항에 따라 전자금융사고 책임이행을 위한 보험 또는 공제에 가입하는 경우 보상한도는 다음 각 호에서 정하는 금액 이상이어야 한다.	**제5조(전자금융사고 책임이행을 위한 보험 등의 가입에 관한 기준)** ① ---------- ---------- ---------- 전자금융거래 규모, 전자금융사고 발생 건수 등을 고려하여 다음 ---------- 이상으로 설정해야 --.
2. 「금융위원회의 설치 등에 관한 법률」 제38조 제8호의 회사, 「전자금융거래법」 제2조 제3호 나목(신용카드업자에 한한다) 및 다목의 회사, 「전자금융거래법 시행령」 제2조 제1호의 회사, 「은행법」에 따른 지방금융회사 및 같은 법 제58조에 의해 인가를 받은 외국금융회사의 국내지점: 10억 원	2. 「금융위원회의 설치 등에 관한 법률」 제38조 제2호(다만, 명의개서대행업무를 수행하는 회사는 제외)의 회사 중 자산이 2조 원 이상인 회사, 같은 법 제38조 제8호 ---------- ---------- ---------- ----------.)
4. 제1호 부터 제3호 이외의 금융회사: 1억 원	4. 제1호부터 제3호 이외의 금융회사: 2억 원
5. 법 제28조 제2항 제1호 및 제2호의 전자금융업자: 2억 원	5. 법 제28조 제2항 제1호 ---
<신설>	6. 법 제28조 제2항 제2호의 전자금융업자: 2억 원
6. 법 제28조 제2항 제4호의 전자금융업자 중 제1호 또는 제2호에 속하는 금융회사가 발급한 신용카드, 직불카드 등 거래지시에 사용되는 접근매체의 정보를 저장하는 전자금융업자: 10억 원	8. 법 제28조 제2항 제4호의 전자금융업자: 2억 원 (단, 제1호 또는 제2호에 속하는 금융회사가 발급한 신용카드, 직불카드 등 거래지시에 사용되는 접근매체의 정보를 저장하는 전자금융업자는 10억 원)
7. 제5호, 제6호 이외의 전자금융업자: 1억 원	7. 법 제28조 제2항 제3호의 전자금융업자: 2억 원
<신설>	9. 시행령 제15조 제3항 제1호의 전자금융업자: 2억 원
<신설>	10. 시행령 제15조 제3항 제2호의 전자금융업자: 2억 원
<신설>	11. 법 제28조 제1항의 전자금융업자: 2억 원

현행	개정안
<신설>	12. 제1호부터 제11호에 2개 이상 해당하는 회사는 각 호의 금액의 합계액으로 한다. 다만 제5호부터 제11호의 합계액이 15억 원을 초과하는 경우에는 제5호부터 제11호의 합계액을 15억 원으로 한다.

다. 거버넌스 관련 CISO에 의한 이사회 보고규정 마련

금융보안 거버넌스를 강화하기 위하여, 정보보호최고책임자(CISO)에게 정보보호위원회 주요 심의·의결 사항 등을 이사회에 보고할 의무를 부여하였습니다(개정안 제8조의2 제4항).

정보보호위원회에서 전자금융거래의 안전성 및 신뢰성에 중대한 영향을 미치는 심의·의결사항이 있는 경우 이를 이사회에 보고할 필요가 있고, 이를 증빙하기 위한 의사록 등의 근거자료를 적절히 구비해 둘 필요가 있겠습니다.

현행	개정안
제8조의2(정보보호위원회 운영) ④ 정보보호최고책임자는 정보보호위원회 심의·의결사항을 최고경영자에게 보고하여야 한다.	**제8조의2(정보보호위원회 운영)** ④ ---------- ---------- ---------- 하며, 전자금융거래의 안전성 및 신뢰성에 중대한 영향을 미치는 심의·의결사항에 대해서는 이사회에 보고하여야 한다.

2. 개정안의 주요 삭제 규정 내용

가. 악성코드 및 공개형 웹서버 관리대책 규정 효율화

악성코드 감염 방지대책 및 홈페이지 등 공개용 웹서버 관리대책에 관한 규정의 내용 중 "다른 규정과 중복되는 내용"과 "지나치게 구체적인 규정"이 삭제되었고 주요 내용은 아래와 같습니다.

#	삭제 내용	비고
1.	악성코드 감염 시 복구 절차에 관한 내용(제16조 제1항 제3호)	개정안 제15조 제4항에 통합
2.	악성코드 감염여부 정기 점검에 관한 내용(제16조 제1항 제4호)	개정안 제12조 제3호에 통합

#	삭제 내용	비고
3.	악성코드 감염 시 후속 조치에 관한 내용(제16조 제2항)	개정안 제15조 제4항에 통합
4.	공개용 웹서버가 해킹공격에 노출되지 않도록 대응 조치하여야 한다는 내용(제17조 제4항)	
5.	단말기에서 음란, 도박 등 업무와 무관한 프로그램 또는 인터넷 사이트에 접근하는 것에 대한 통제 대책을 마련해야 한다는 내용(제17조 제5항)	개정안 제15조 제7항 신설
6.	악성코드 감염·확산 방지, 피해 최소화 및 복구를 위한 대책을 수립·준수해야 한다는 원칙만 유지하고, 구체적 대책에 관한 규정 삭제(개정안 제16조)	
7.	공개용 웹서버에 자료 게시 절차· 내용에 관한 내부통제 방안과 개인정보 유출 및 위·변조를 방지하기 위한 보안조치 방안을 수립·운용하여야 한다는 원칙만 유지하고, 구체적 방안에 관한 규정 삭제(개정안 제17조)	

나. 직무분리에 관한 세부 규정 삭제

현행 감독규정은 직무분리 영역을 세분화하여, 개별 업무에 대해 직무를 분리할 의무를 부여하고 있었습니다. 그러나 이러한 규정은 분리된 직무의 내용이 명확하지 않아 업무에 혼선이 생길 수 있다는 지적이 있던 바 개정안에서는 직무 분리의 추상적인 원칙만을 남기고(개정안 제8조의3) 직무 분리가 요구되는 다음의 구체적인 열거 조항을 모두 삭제하였습니다.

- 프로그래머와 오퍼레이터 간 직무 분리
- 응용프로그래머와 시스템프로그래머 간 직무 분리
- 시스템보안관리자와 시스템프로그래머 간 직무 분리
- 전산자료관리자(librarian)와 그 밖의 업무 담당자 간 직무 분리
- 업무운영자와 내부감사자 간 직무 분리
- 내부인력과 전자금융보조업자 및 유지보수업자 등을 포함한 외부인력 간 직무 분리
- 정보기술부문인력과 정보보호인력 간 직무 분리
- 그 밖에 내부통제와 관련하여 직무의 분리가 요구되는 경우 해당 직무 분리

다. 비밀번호 설정방식 관련 획일적 규율 삭제

현행 감독규정은 "주민등록번호, 동일숫자, 연속숫자 등 제3자가 쉽게 유추할 수 있는 비밀번호의 등록 불가" 등과 같은 비밀번호 설정의 세부 규칙을 두고 있었습니다. 그러나, 비밀번호 방식을 구체적으로 특정하는 것이 오히려 보안에 뛰어난 다른 비밀번호 정책의 채택을 제한할 수 있다는 우려가 있던 바 개정안에서는 아래와 같은 규정상의 원칙만 존치되고 그 외 비밀번호 설정의 세부 규칙은 모두 삭제되었습니다.

- 제3자가 쉽게 유추할 수 없는 비밀번호 작성규칙 및 등록·변경 절차 수립·운영할 것(개정안 제34조의3 제2항 제1호).

이 외에도 건물·설비·전산실의 관리·보호를 위한 현행 규정에서 세부 내용을 삭제하고 원칙만 유지하였으며(개정안 제9조 내지 제11조), 임직원별로 정보보호 교육시간을 특정하던 규정을 삭제하는(제19조의2) 등 지엽적인 세부규정의 상당 부분을 삭제하였습니다.

개정안은 위 내용을 포함하여 총 134건의 수범사항을 삭제하여, 형식적인 규제를 완화하였습니다. 따라서 개정안이 시행될 경우 금융회사 및 전자금융업자의 금융보안 관련 의무가 일부 완화될 것으로 보입니다. 다만, 금융감독당국이 위와 같이 감독규정을 정비한 이유는 단순히 수범자의 규제 부담을 완화시키기 위함이 아닌, "형식적 규제 및 감독 체계"에서 "자율 보안 수립 및 이행 점검 체계"로 규제의 패러다임을 변경하기 위함이라는 점을 고려하였을 때 금융회사 및 전자금융업자는 향후 더욱 효과적이고 안전한 보안 수단 등을 고안 및 마련하여야 할 것입니다.

이번 개정안은 규정변경 예고 절차를 거친 후('24.2.1. ~ '24.3.12.), 의견 수렴 및 금융위원회 의결 등을 거쳐 2024년 상반기 중에 시행될 것으로 예상됩니다. 따라서, 금융회사 및 전자금융업자는 이번 개정안의 진행과정을 지속적으로 모니터링 할 필요가 있겠습니다.