금융위원회

보 도 자 료

다시 도약하는 대한민국
함께 잘사는 국민의 나라

보도 일시	2022. 12. 27.(화) 석간	배포 일시	2022. 12. 26.(월) 15:00
담당 부서 <총괄>	금융혁신기획단 전자금융과	책임자	과 장 김종훈 (02-2100-2970)
		담당자	사무관 안영비 (02-2100-2975)

급변하는 IT 환경에 탄력적으로 대응할 수 있도록 금융보안 규제 선진화를 추진하겠습니다.

※ 「제5차 금융규제혁신회의」 보고 및 회의결과 반영

□ 급변하는 IT환경과 새로운 보안 리스크에 금융회사 등이 탄력적으로 대응할 수 있도록 「금융보안규제 선진화 방안」을 마련하고,

○ 「제5차 금융규제혁신회의」(12.20일)에서 해당 안건을 논의하였습니다.

< 「금융보안규제 선진화 방안」 주요 내용 >

❶ (**보안 거버넌스 개선**) 금융회사 등이 전사적 차원에서 보안을 준수하고, 리스크 기반의 자율보안체계를 구축할 수 있도록 규율체계를 개선

❷ (**보안규제 정비**) 목표·원칙중심, 사후책임 중심으로 규제를 전환

❸ (**관리·감독 선진화**) 금융보안 전문기관이 금융회사 등의 보안체계를 검증하고 컨설팅할 수 있도록 지원 기능을 강화

□ 금융규제혁신회의 논의사항을 바탕으로, `23년 상반기 중 「금융보안 규율체계 정비 TF」를 구성하여 보안규제 선진화 로드맵을 검토할 예정입니다.

---

1. 추진 배경

□ 최근 **금융분야**에서 클라우드·빅데이터·AI 등 **디지털 신기술 활용**이 **확대**됨에 따라 **금융보안**의 **중요성**이 **증가**하고 있습니다.

○ **신기술 도입**에 따른 **보안 취약점**을 이용한 랜섬웨어, DDoS 공격* 등 **사이버 위협**의 **유형**도 **다변화**하고 있으며,

* DDoS(Distributed Denial of Service) : 다수의 기기를 특정 시스템에 일시적으로 접속시켜 시스템을 마비시키는 공격

○ **빅테크**의 **금융업 진출**, **클라우드 등 아웃소싱 확대** 등으로 **제3자 리스크***(3rd Party Risk)가 **심화**되고 있는 **상황**입니다.

* 非금융부문의 장애발생, 정보유출 등의 사고가 금융 부문으로 전이되는 리스크

□ 그러나 **現 금융보안 규제**는 **급변**하는 **IT환경**과 **보안 리스크**에 **효과적**으로 **대응**하기 **어렵다**는 **의견**이 **지속 제기**되고 있습니다.

○ 이에 따라, **디지털 금융혁신**을 **뒷받침**하면서 **리스크**에 **효과적으로 대응**할 수 있는 **금융보안 규제 선진화 방안**을 **마련**하였습니다.

2. 현황 및 문제점

1 (**금융보안 거버넌스의 문제**) **금융회사 등**은 **금융보안**을 **정보보호최고책임자**(CISO) **중심**의 **실무적 문제**로만 **인식**하고 있으며, **사고 발생시 임기응변식**으로 **대응**하고 있는 실정입니다.

* 금융보안을 정보보호 부서에만 맡겨놓고, 현업부서나 내부 감사조직 등을 모두 포함하는 전사적 차원의 금융보안 역할 및 책임 부여는 미흡

❶ **금융보안**을 **기술적 영역**으로 **한정**함에 따라, 기업의 **핵심전략**과 **우선순위 등**을 **반영**한 **종합적**인 **보안전략 수립**이 어려우며,

❷ **자율보안체계 구축**을 위한 **자체 리스크 평가, 전문인력 육성** 등에 대한 **투자**도 **미흡***하여 **보안 리스크 대응**에 **한계**가 있습니다.

* 임직원 의무 교육시간 충족 등 「전자금융감독규정」상 안전성 확보조치의 최소 기준만 준수하려 할 뿐, 전문 보안인력 양성 등 능동적 보안활동에는 소극적

2 (**금융보안 규제의 문제**) 現 **보안 규제**는 **미시적**인 **규정 중심**이며, **사전통제적 성격**이 강하여 **제도개선**의 **필요성**이 **제기**되고 있습니다.

① **안전성 확보의무**를 **포괄 규정**(전금법 §21)하고, 감독규정(§8~37)에서 인력·시설, 정보기술 등의 **세부사항을** 열거*

* (예) 경비원이 출입구를 통제 / 휴대용 손전등 비치 / 압력계, 온도계 등을 갖출 것 등

② 금융회사 등의 **사전 의무사항**을 **나열**하고, 이를 **준수**했다면 **보안 책임**을 **면제**하고 **사고 발생시**에도 **경미한 과태료** 및 **임직원 신분제재**만을 **부과**

❶ **급변**하는 **IT환경**을 **신속**하게 **반영**하지 **못하는 경직적 규정**으로 인해 **새로운 리스크**에 **효과적**으로 **대응**하기 **곤란***한 상황입니다.

* (예시) ①빅테크 등 전금업자의 규모·영향력이 증가했음에도 불구하고 재해복구센터 설치 의무가 면제되어 있고, ②전자금융사고의 파급력이 확대됐음에도, 사고시 책임이행을 위한 보험 가입기준은 과거에 머물러 있음(금투업 : 5억원, 저축은행·보험·선불업 : 1억원 등)

→ **금번 데이터센터 화재 사태로 現 감독규정의 개정 필요성이 제기된 상황**

❷ **보안규정 준수**가 **금융회사 등**의 **보안 목표**로 **인식**되어, **수동적인 보안 활동**에 머무르는 **한계**가 있습니다.

* ①규정상의 보안 의무만 준수하면 모든 보안 책임을 다하는 것이라는 인식이 만연하고, ②감독규정상 보안방법 등을 특정함에 따라 자율적으로 동일 목적을 달성하거나 보안을 강화할 수 있는 他 방법에 대한 가능성을 차단

❸ 금융회사 등의 **규모, 성격** 등에 따른 **리스크 경중**을 고려하지 않고 **평균 수준의 금융회사**를 **상정**하여 **통일된 의무**를 **부과**함에 따라, **영세**한 **전금업자**의 경우 **규제 준수**가 **어려운 실정**입니다.

* (예시) 프로그램 등록·변경시 제3자 검증을 받아야 하는데, 금융회사는 아웃소싱 또는 조직 내 전담팀을 통해 이를 수행하는 반면 소규모 전금업자의 경우 매번 제3자 검증을 받기 곤란

3. 개선방안

[기본 방향]

1 보안 거버넌스 개선	① 금융보안을 금융회사 등의 전사적 차원에서 준수하는 **핵심가치**로 제고 ② 보안체계를 리스크 기반의 "**자율보안체계**"로의 전환 추진
2 보안규제 정비	① **목표·원칙 중심**으로 규제를 전환하고, 세부사항은 가이드 형태로 전환 ② 자율보안체계 미구축 또는 보안사고 발생 등의 경우 **사후책임**을 강화
3 관리·감독 선진화	① 보안규정 위반여부 감독 중심에서 자율보안체계 수립·이행 등에 대한 **검증 중심**으로 전환 ② 금융회사 등의 보안 거버넌스 개선 및 자율보안체계로의 이행 **컨설팅 기능 강화**

□1 (보안 거버넌스) 금융회사 등이 전사적 차원에서 금융보안을 준수하고, 자율보안체계를 구축할 수 있도록 규율체계를 개선하겠습니다.

❶ 정보보호최고책임자(CISO)의 권한을 확대하고, 중요 보안사항의 이사회 보고 의무화 등을 통해 금융보안을 기업의 핵심가치로 제고하겠습니다.

* CISO는 리스크 관련 주요 회의에 참석, CEO에게 직접 보고 등(美 FFIEC)
CISO는 사이버보안 프로그램과 중요 보안리스크를 이사회에 보고(美「23 NYCRR 500」)

❷ 금융회사 등이 보안리스크를 스스로 분석·평가하고, 리스크에 비례하여 보안방안을 수립할 수 있는 리스크 기반의 "자율보안체계"로의 전환을 추진하겠습니다.

* NIST(美표준기술연구소)는 新금융리스크 대응 방식으로, 기업 스스로 리스크를 식별하고 비즈니스 환경에 맞는 보안 통제를 선택하는 RMF(Risk Management Framework) 방식 제시

□2 (보안규제 정비) 목표·원칙중심*, 사후책임 중심으로 규제를 전환하겠습니다.

* 금융당국은 원칙·상위기준을 제시, 목표 달성과정은 금융회사 등의 자율적인 판단을 존중

❶ 現 **안전성 확보의무**(「전금법」§21)를 인력·조직·예산, 내부통제, 시스템 보안, 데이터 보호 등으로 **구분**하여 **금융보안**의 주요 **원칙과 목표**를 **법에 명시**하고 세부사항은 폐지하겠습니다.

- **이를 위해** 「전자금융감독규정」(§8~37) 중 **필수사항**만을 **남기고, 세부적**으로 **규율**할 **사항**은 **가이드라인** 또는 **해설서** 등으로 **전환**하겠습니다.

* (예시) ①필요·최소한의 보안 인력, 예산, 조직 등은 진입요건으로 전환하고, ②침해사고 대응, 재해복구, 자율보안체계 구축 등의 필수요소만을 규율, ③기술적이고 세세한 보안규정은 가이드라인이나 해설서 등으로 전환

< 뉴욕주 금융 사이버보안 규정(23 NYCRR 500) >

◈ **정보보호의 3요소**인 **'기밀성', '무결성', '가용성'**을 **원칙**으로 **제시**하고, **금융회사 등**이 **보안체계**를 **수립**토록 **최소한**의 **의무**만을 **부여**

◈ **프로그램 보안, 다중 인증, 암호화 등**의 **구체적 수단**을 **특정하지 않고 금융회사 등**이 **내부 위험평가 등**을 통해 **보안기술 등**을 **자율 채택**하도록 규정

❷ **금융회사 등**이 **자율보안체계**를 **구축**하지 **않거나, 보안사고**가 **발생**한 **경우** 그에 따른 **사후책임**을 **강화하겠습니다.**

- **국제기준 등**을 **고려**하여, **고의·중과실**에 의한 **사고 발생**시 **과징금** 등의 **제도 신설**을 **검토**할 **예정**입니다.

3 (**관리·감독 선진화**) 금융당국의 **관리·감독방식**을 **자율·책임 원칙**으로 **전환**하고, **금융보안 전문기관**(예: 금융보안원)을 **통해 금융회사 등**의 **자율보안체계 검증 및 이행 컨설팅 기능을 강화하겠습니다.**

❶ **보안규정 위반여부 감독 중심**에서 **자율보안체계 수립·이행 등**에 대한 **검증 중심***으로 **전환하겠습니다.**

* 금융회사 등이 업무 성격, 복잡성 등에 비례하여 내부 보안리스크를 평가·관리하는지, 이를 바탕으로 자율보안체계를 구축하였는지·적정한지 등을 주기적으로 검증

※ **유럽은행감독청(EBA) 내부 거버넌스 가이드라인**(Guidelines on internal governance) : 제3자(민간 보안전문기관 등 독립적 감사인)가 금융회사 등의 리스크 관리 체계, 자율보안체계 등을 검증하고, 감독당국은 제3자의 자격과 활동이 적정한지를 관리·감독

❷ **금융회사 등**의 **보안 거버넌스 구축**을 위한 **보안성 검토 지원, 기술 공유, 인력 양성 교육** 등 **지원·컨설팅 기능**을 **강화**하겠습니다.

4. 향후 계획

〈 금융보안 규제 선진화 로드맵 〉

◈ **`23년 상반기 중 「금융보안 규율체계 정비 TF*」를 구성**하여 **장기적 로드맵**에 대한 **검토**를 **시작**하겠습니다.

* 금융감독원, 금융보안원, IT 보안 전문가 등 참여

○ **아래에 제시된 방향**으로 **로드맵**을 **검토**하되, **구체적인 시행 일정**도 **함께 마련**할 **예정**입니다.

□ (1단계) 現 보안규정의 우선순위, 규제 타당성, 금융회사 등의 보안 역량 등을 종합적으로 평가하여 규정을 정비 (감독규정 개정사항)

* (예시) 최근 **데이터센터 화재 후속조치**로서, ①일정규모 이상 전금업자 등의 재해복구 센터 설치의무 신설 검토, ②전자금융사고시 책임이행을 위한 보험금 가입기준을 상향하는 방안 검토 (유럽연합 PSD2의 전문인배상책임보험 최저보상한도 산출기준 등 참고)

□ (2단계) 금융보안의 목표·원칙을 제시하고, 금융회사 등의 자율보안 체계 구축 및 사후책임 중심으로 규제를 정비 (법률 개정사항)

* (예시) ①금융회사 등의 리스크관리체계 및 보안역량에 따른 표준지침 등을 제시, ②제3의 전문기관(금융보안원 등)을 통한 금융회사 등의 자율보안체계 검증 및 지원, ③과징금, 손해배상 책임 등 엄격한 사후책임 규제 도입 등

□ (3단계) 포지티브 규제체계에서 네거티브 방식으로 전환하여 금융회사 등에 보안 자율성을 부여

* (예시) 금융회사 등의 물리적/논리적 망분리의 선택가능성을 부여

담당 부서 <총괄>	금융위원회 전자금융과	책임자	과 장 김종훈 (02-2100-2970)
		담당자	사무관 안영비 (02-2100-2975)
<공동>	금융감독원 디지털금융혁신국	책임자	국 장 김부곤 (02-3145-7120)
		담당자	팀 장 이수인 (02-3145-7135)
<공동>	금융보안원 보안연구부	책임자	부 장 이상록 (02-3495-9700)
		담당자	팀 장 김성웅 (02-3495-9740)