<별첨2>

자본시장 거래 안전성 제고 방안

2025. 8.

금융감독원

Ⅰ. 금융투자부문 전자금융사고* 현황

* <**전자금융사고 유형분류**(전자금융감독규정 제37조의5 및 시행세칙 제7조의4)>
① 전자금융업무 지연·중단 시간이 30분 이상인 경우
② 전자금융업무 지연·중단 시간이 10분 이상이고 해당 전자금융서비스 가입자가 1만명 이상인 경우
③ 전산자료 또는 프로그램의 조작 및 오류와 관련된 사고가 발생한 경우

□ **(개요) 최근 5년간**('20~'24년) **증권사**에서 **총 429건**의 **사고**가 **발생**하였으며, 매년 **발생건수**도 **증가**하는 추세('20년 66건→'24년 100건)

- 특히, **'25년 상반기**중 **다수**의 **전산사고***(58건)가 **연이어 발생**하여 **투자자** 등의 **불안·불신**이 **높아진 상황**

* 전년동기(40건) 대비 사고가 증가하였고, 주로 **해외주식 브로커 전산장애** 등 **외부요인**에 기인

※ 최근 5년간 **금융권 전자금융사고 피해액**은 **294.6억원**이며, 이중 **금투부문**(증권사)이 **대다수(262.5억원, 89%)**를 **차지** ☞ 사고발생 시 **매매체결 지연·중단**에 따른 **투자자 피해**로 **직결**

금투부문(증권사) 전자금융사고 유형별 발생건수

사고유형	'20	'21	'22	'23	'24	'25 (1~6월)	계
프로그램 오류	**23**	**31**	**27**	**41**	**34**	**32**	**188**
외부요인	**14**	**18**	**24**	**37**	**40**	**18**	**151**
시스템·설비 장애	24	33	21	19	22	8	127
인적 재해	5	3	6	3	4	-	21
계	**66**	**85**	**78**	**100**	**100**	**58**	**487**

□ **(증권사 규모별)** 최근 5년간 **35개 증권사**에서 **총 429건**의 **사고가** 발생하였으며, 연평균 **26개 증권사**에서 **86건**(1사당 연간 3건)이 발생

○ **대형社**(자기자본 상위 10사)에서 **총 202건**(47%, 1사당 연간 4건)이 **발생**, **중소형社**에서는 **총 227건**(53%, 회사당 연간 3건)의 **사고**가 발생

○ 한편, **온라인 기반 증권사**의 **사고발생 건수**가 **상대적**으로 **높은** 가운데 **리테일 부문**(위탁매매) **경쟁 심화**로 **사고발생 가능성**도 더욱 **증대**

□ **(사고유형)** 최근 5년간 **증권사**의 **전자금융사고**(총 429건)는 **주로 프로그램 오류**(156건, 36.4%)로 인해 **발생**, **최근**에는 **외부요인**(133건, 31%)으로 인한 **사고**가 **증가**하는 추세

○ **프로그램 설계·테스트** 및 **제3자 검증 미흡** 등 **프로그램 오류**로 인한 **장애**가 **지속 발생**하는 가운데 **시스템·설비 장애**는 **감소**

○ 최근 **해외주식 거래**가 **대폭 증가**하면서 **해외 브로커·거래소 장애** 등 **외부요인**에 의한 **전자금융사고**도 **증가 추세**

Ⅱ. 주요 리스크 요인

◈ 대규모 전산장애 등 **투자자 피해**로 **직결**될 수 있는 주요 **전자금융거래 리스크 요인**에 대해 **종합적인 대응**이 **필요**

1 **(대규모 전산장애)** **금년중 거래소·증권사**의 **대규모 전산장애** 발생으로 시장의 **불안·불신**이 **확대**됨에 따라, **금투회사**의 **전사적 대응**이 필요

2 **(IT내부통제)** **지속적·반복적** 전산사고는 주로 **프로그램 오류** 등 **IT내부통제 미흡**에 **기인**하고 있어 **통제체계 개선**이 필요

3 **(온라인·리테일 확대)** **전자금융거래 증가, 리테일 부문**(위탁매매) **경쟁심화** 등으로 **온라인·리테일** 중심 **증권사**의 **리스크**가 더욱 **가중**

4 **(사고예방·비상대응)** **전산사고 빈발요인**에 대한 **예방대책*** **수립·이행** 및 사고시 적시 대응을 위한 **비상대응계획(BCP)**** **고도화** 필요

* 프로그램 변경 통제, 해외주식 거래 관련 대체수단 확보 및 관리인력 확충 등
** 자본시장(통합) 및 금투회사(개별)의 비상대응계획(BCP)

5 **(신용정보 보호대책)** **신용정보 유출·오남용 위험***이 **가중**되는 점을 감안하여 **기술적·물리적·관리적 보호대책 강화 필요**

* 신용정보의 이동·집적·결합·활용 증가, 침해사고 빈발 등

6 **(전금법 미적용社)** 안전성 관리수준이 상대적으로 낮은 **전자금융거래법 미적용 금투사**는 **정보보호 측면**에서의 보호대책 마련·준수 필요

Ⅲ. 거래 안전성 강화 방안(주요내용)

◈ 금감원은 **그룹별·상황별 맞춤형 대응수단**(Policy Mix)을 **적용**하여 **전자금융사고** 등의 **리스크 예방 및 적시 대응체계를 즉시 시행 예정**

※ (대형사 예시) 평상시 **❸,❹,❼ 방안을 적용**하고, **필요시 추가 수단(❺,❻)** 조치

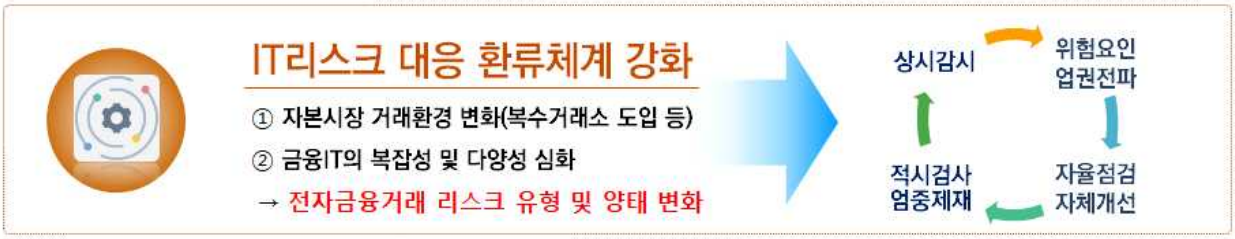
자본시장 거래 안전성 제고 종합방안

【목표】 거래 안전성 강화를 통한 자본시장 신뢰도 제고

1 리스크 그룹	2 리스크 요인	3 대응방안
1) 대형사	1) 대규모 전산장애	1) 상시감시 강화
2) 고위험사	2) IT 내부통제	2) 신속 정보 수집 및 공유
3) 중소형사	3) 온라인·리테일 중심 증권사	3) IT감사 가이드라인 안착
4) 전금법 미적용 회사	4) 사고예방 및 비상대응 미흡	4) 자율시정체계 활성화
	5) 신용정보 보호대책 미흡	5) 고위험社 집중관리
	6) 전금법 미적용 회사	6) 적시검사 및 엄중제재
		7) 소통 및 교육 강화

1 **(상시감시 강화)** **금투회사**의 **IT·정보보안 리스크**를 **정기·수시**로 **정밀분석**하여 **선제적 위험요인 식별, 유관부서·업권 전파, 자율시정, 현장검사 연계** 등 **리스크 대응 환류체계** 기반 구축

○ 특히, 관련 통계(사고현황, 전자금융거래·고객규모 변화 추이 등), 유관기관 분석자료(금보원, KISA 등), 언론동향 등 **내·외부 정보**를 활용한 **연계분석**을 통해 **위험요인** 및 **고위험군 식별 역량 강화**



2 **(신속 정보수집 · 공유)** **상시감시, 핫라인**(금투회사·유관기관), **언론** 등을 통해 정보사항을 적시 **수집·분석**

○ **중요 사항**(위험요인, 사고·모범사례 등)은 **신속히 업권**에 **전파**(CPC, 간담회 등)하여 **자율시정** 및 **유사사고 재발방지** 유도

3 **(IT감사 가이드라인 안착)** 전자금융사고 빈발요인에 대한 **선제적 예방대책 수립·이행** 및 **비상대응계획 개선** 등을 위해 **IT감사 가이드라인**이 조속히 금투회사의 **내부통제체계**에 **내재화**될 수 있도록 지도

○ **서면점검, 현장검사** 등을 통해 가이드라인 이행 여부를 확인하고 **우수사례**를 **발굴·공유**하는 한편, **미흡사항**에 대해서는 **시정 등 요구**

4 **(자율시정체계 활성화)** **상시감시** 등을 통해 **수집·분석**된 **리스크 요인** 및 **주요 현안사항**에 대해 **금투회사**가 적시에 **자율점검·자체개선**을 실시하는 등 **자율시정체계 활성화**

○ **제도도입 등 환경변화**에 따른 **리스크 요인** 관련 **점검항목**을 **마련·배포**(금감원, 수시)하여 **금투회사**의 **자율적인 점검·시정** 유도

○ 리스크 규모 및 파급력이 상대적으로 낮은 **전금법 미적용 금투회사**(운용사 등)에 대해서는 「**자가진단 체크리스트**」를 **배포**하여 **필수 준수사항**을 **연1회** 이상 **주기적 점검·시정** 지도

5 **(고위험社 집중관리)** **상시감시** 등을 통해 **선별**된 **고위험사**(전산사고 빈발 등)를 대상으로 **경영진 면담**, 전사 차원의 **IT내부통제 개선**, **적정자원**(인력, 예산 등) **투입** 등 **리스크 감축**을 위한 **개선조치** 실시

○ **전담 검사역**의 **집중감시**와 함께 **리스크 수준**(전산사고 빈도·정보유출 발생 등)에 따라 **단계별 조치**(**자율시정**, **경영진 면담**, **현장검사**) 예정

6 **(적시검사 · 엄정제재)** **리스크 대응수준 미흡** 또는 **중대사고 발생 금투회사**에 대해 **적시검사**(검사주기 단축) 실시 및 **엄정한 제재** 실시

○ 또한, 검사를 통해 파악된 **모범·취약사례**는 **간담회·워크숍** 등을 통해 **업권**에 **전파**하고, **제도상 미흡사항**에 대해서는 **유관기관**과 **협업**하여 **신속한 개선**도 추진

7 **(소통 및 교육 강화)** **경영진**(CEO, CIO 등)과의 **소통강화**(간담회 등)를 통해 **전사차원**의 **거래 안전성 강화**와 관련된 **공감대 형성** 및 **주의 환기** 유도

○ **반복적 위규사항, 중대 사고요인, 모범사례** 등 **중요사항**에 대해서는 **다양한 소통채널**(CEO레터, 워크숍 등)을 통해 업권에 **적시 공유·전파**

○ 아울러, **유관기관**과의 **협업**을 통해 **금투부문 임직원** 대상 **IT·정보보안 내부통제 교육**을 실시하여 **업권 전반**적인 **역량 강화** 지원

○ 그간 **규제 사각지대**(Gray Zone)로 여겨졌던 **전금법 미적용社**에 대해서는 **자본시장법**상 **물적설비 유지요건** 등 **필수 준수사항 위주**로 별도 **교육**(필요시 온라인 교육 활용) **실시** 예정