금융위원회 **보도자료** 대체불가 대한민국

보도시점 2026. 7. 2.(목) 석간 배포 2026. 7. 1.(수) 16:00

금융회사가 프런티어 AI 보안위협에 적극적으로 대응할 수 있도록 면책 조치와 가이드라인을 마련하였습니다.

✓ AI 보안테스트·보안패치시 발생하는 **전산장애**는 일정범위내 **제재 면책**

✓ AI 보안위협 관련 보안패치 우선순위 등 **금융권 가이드라인 마련·배포**

[개요]

금융위원회는 '26.6.30(화), **면책심의위원회**(위원장 : 김범기 상임위원)를 개최하여 **AI 보안테스트·보안패치 과정**에서 발생하는 **전산장애에 대한 면책조치를 심의·의결**하였다. 아울러, 금융회사들의 AI 보안위협에 효과적으로 대응하기 위한 행동요령을 담은 **가이드라인**(「프런티어 AI 보안위협 금융분야 대응요령」)**도 마련·배포**하였다.

이는 「미토스」 등 프런티어 AI*의 보안위협에 금융권이 적극적으로 대응해 치밀한 보안강화 조치를 취하도록 지원하기 위한 것으로서, 지난 5.22일 개최한 **「고성능 AI 보안위협 대응 간담회**(주재: 권대영 부위원장)**」의 후속조치**이다.

* 프런티어 AI : 현재 가장 높은 수준의 성능과 범용성을 갖춘 AI 모델

동 간담회 이후 금융위원회는 금융감독원·금융보안원 등 유관기관과 함께 면책범위·내용 및 가이드라인에 필요한 세부항목 등에 대해 **금융업계의 의견수렴**을 거쳤고, AI·보안 및 법률 전문가로 구성된 **「민간기술자문단」의 전문적 조언 등을 청취·반영**하여 방안을 확정하였다.

[❶ 면책조치 주요내용]

그간 금융업계는, 프런티어 AI 위협에 대응해 금융회사들이 적극적 조치를 취하도록 하기 위해서는 이 과정에서 발생하는 경미한 전산장애 등 리스크를 지나치게 두려워하지 않도록 일정한 면책조치가 필요하다는 의견을 지속 제기해 왔다. 특히, ▲보안목적 AI 등을 활용한 공격표면 점검이나 취약점 확인, ▲기 확인된 보안 취약점에 대한 보안패치 등 과정에서 전산시스템 오작동 등 우려가 없지 않으며, 금융회사 임직원들이 이러한 리스크를 지나치게 의식해서는 당면한 프런티어 AI 위협에 대응한 적극적 조치를 신속히 취하는데 한계가 있다는 지적이다.

앞으로는 **금융회사들**이 ①**보안목적 AI를 활용해 테스트***를 진행하거나, ②금융위·금감원·금보원 등에서 전파하는 **보안취약점에 대한 보안패치를 실행**하는 과정에서 **경미한 전산장애**가 발생하더라도, **신속한 복구와 소비자 보호조치**가 이루어졌다면 이와 관련한 기관·임직원 신분제재나 과태료 부과 등 **제재조치가 면책**된다.

* '26.5.22일 발표한 보안목적 AI 활용을 위한 망분리 규제 완화 테스트 선정기관과 금융보안원에서 실시하는 AI 취약점 점검(Blackbox 방식) 대상기관 限

첫째, 면책대상은 ①보안목적의 AI를 통해 상시적인 취약점·포트 스캐닝, 자동화된 침투 시도 등 **보안테스트**를 시행하거나, ②금융위·금감원·금보원에서 전파하는 보안 취약점에 대해 **긴급 보안 패치**(OS·SW 등) 또는 **이에 준하는 전산장비 변경 등**을 포괄한다.

둘째, 면책요건은 ①**경미한 전산장애**에 대해 ②**신속한 복구 수단** 및 ③**소비자 보호 조치 마련·이행 여부** 등을 종합적으로 고려할 예정이다.

① **경미한 전산장애**란 「금융회사의 검사 및 제재에 관한 규정 시행세칙」 [별표3]의 제재대상·기준에 해당하지 않는 IT사고로서, **▲고의성이 없고 ▲금전피해**(1억원 미만), **▲시스템 장애 시간**(최대 4시간 이내), **고객정보 유출**(개인신용정보 제외, 1만건 미만) 등이 **일정기준 이내에 해당**하는 경우를 의미한다.

② **신속한 복구 수단**이란 **사전테스트***, **피해확산 방지**** 및 **서비스 연속성 확보***** 를 위한 작업계획서(경영진 보고)를 **마련하여 실시**한 경우이다.

* [예시] 검증환경에서 패치 적용 후 정상 작동 여부 확인, 영향도 분석 등
** [예시] 롤백(Rollback), 킬스위치(Kill Switch), 서비스 모듈 격리(Isolation) 등
*** [예시] 페일오버(Failover), 수동 처리 등 임시 대체 프로세스 등

③ **소비자 보호조치**란 대고객 사전 안내 및 피해 구제 방안을 마련하고 이행하는 경우로서, 홈페이지, 문자(SMS) 등을 통해 **보안테스트 또는 패치 일시·대상·내용·대체 서비스 경로 등**을 고객에게 **사전에 안내**하고 소비자 피해 발생 시 **구제조치를 마련·실행**한 경우이다.

셋째, 면책범위는 **▲기관·임직원에 대한 제재·신분제재와 ▲과태료를 포괄**한다. 다만, 「신용정보법」에 따른 **개인신용정보 유출사고** 발생시에는 금번 면책 조치와 관계없이 동 법에 따른 **제재조치가 그대로 적용**된다.

[❷ 가이드라인 주요내용]

「미토스」 등 프런티어 AI는 그 실체와 능력 범위가 충분히 규명되지 않아 위협의 강도나 예상되는 공격기법을 사전에 가늠하기 어렵다. 아울러 새로운 유형의 보안위협에 대해 구체적으로 어떤 방식으로 대응해야 하는지 명확한 방법이 제시되지 않은 상황이다.

금융권에서는 보안 현장실무에서 적용할 수 있는 구체적인 행동요령 등을 마련해서 배포해 줄 것을 요청하고 있다. 특히, 국내외 동향을 빠르게 확인하기 어렵고 자체 보안인력·예산·자원이 한정적인 중소형 금융회사들은 빠르게 변화하는 보안위협에 대응해 실무적으로 참고할 구체적 가이드라인이 절실하다는 입장이다.

이에, 금융위는 금감원·금보원 등 관계기관 협의를 거쳐 금융회사들이 프런티어 AI 보안위협에 보다 적극적으로 대응할 수 있도록 지원하기 위해 ①**경영진 책임 강화**, ②**취약점 및 패치관리**, ③**자산·공급망 관리**, ④**AI 기반 방어 자동화**, ⑤**금융권 공동대응 및 복원력 강화**, ⑥**침해확산 방지 체계** 등 **6개 분야의 대응요령**을 담은 **가이드라인을 배포**하였다.

동 가이드라인은 금융회사가 프런티어AI 보안위협에 효과적으로 대응할 수 있도록 기준으로 활용할 **행동요령이나 모범사례를 제시**하기 위함이며, 이를 준수하지 않더라도 제재 등 불이익이 부과되지 않는다.

① 경영진 책임 강화

금융회사의 이사회와 CEO는 AI 보안위협에 적극 대응할 필요가 있다. 이사회 내 정보보호위원회 등에서 보안위협을 핵심 안건으로 다루고, **최종 책임자**인 **이사회**와 **CEO**는 **CISO**에게 **실질적인 예산 편성권**과 **인력 운영의 권한을 부여**하는 것이 바람직하다.

AI 보안 위협 모니터링 및 신속한 대응을 위해 **CISO 직속 대응반을 구성·운영**할 수 있다. CISO 직속 대응반은 ▲위협 상황 모니터링, ▲취약점 인지·패치·개발 등 조치기간을 단축할 수 있도록 회사 내 다양한 IT직군*으로 구성하는 것이 바람직하다.

* 보안 담당자를 포함하여 ▲네트워크·시스템 인프라, ▲개발·배포 파이프라인, ▲데이터 엔지니어링 등 IT 全 분야 담당자로 구성하여 운영

② 취약점 및 패치 관리

국내외에서 AI를 활용한 보안테스트가 활발히 이뤄지면서 취약점 발견이 빠르게 늘어날 수 있는 만큼, **보안 패치 관리의 중심**을 취약점 제거에서 **공격 성공가능성을 감소시키는 것**으로 전환하는 것이 필요하다.

많은 보안패치 작업을 한정된 시한내 이뤄내야 할 수 있기 때문에 **정교하고 세심한 패치 우선순위 설정**이 필요하며, 고위험 취약점을 일단위로 관리하거나, 패치가 불가피하게 지연되는 시스템을 적절히 조치(예 : 네트워크 임시격리, 서비스 제한 등)하는 방법도 강구할 필요가 있다.

패치 우선순위는 각 금융회사 시스템의 특성이 상이한 만큼 일률적으로 제시할 수는 없으나, **▲취약점의 심각도·악용 가능성, ▲금융회사 핵심 비즈니스·자산 영향도, ▲대외 노출도,** ▲전금법·신정법·개보법 등 **주요 법령 준수 여부** 등을 감안해 **체계적으로 설정·관리**하는 것이 필수적이다.

나아가, 취약점 점검부터 패치까지 신속하게 이루어질 수 있도록 **취약점 점검·보안 패치 업무 체계**와 **프로그램 개발·배포 체계를 연계**하는 노력도 기울일 필요가 있다.

③ 자산·공급망 관리 강화

AI는 금융회사의 공격 표면을 빠르게 탐색할 수 있으므로, 금융회사는 보유한 **전산자원·공급망을 정확히 식별·관리**하는 것이 무엇보다 중요하다.

시스템·애플리케이션·API·클라우드·오픈소스·위탁업체 등 모든 자산을 명확히 파악하고 통합적으로 관리하는 것이 중요하며, 이러한 전산자원을 ▲인터넷 노출여부, ▲업무 중요도, ▲데이터 민감도, ▲패치 상태 등을 기준으로 구분하여 종합적으로 관리해야 유사시 즉시 대응이 가능하다.

아울러, 자체적으로 활용 중인 오픈소스 SW에 대해서는 SW 구성명세서(SBOM) 작성도 고려할 필요가 있으며, 취약점이 포함된 오픈소스 사용이 차단될 수 있도록 소프트웨어 분석 도구(SCA)도 활용할 수 있다.

④ AI 기반 방어 자동화

AI 기반 공격에 대비해 **보안시스템 자동화 체계**를 마련할 수 있다. 다만, 이 경우 보안 자동화 과정의 오탐지, 과잉대응, 서비스 장애 가능성에 대비하기 위해 **업무 위험도** 등을 고려하여 **자동화 수준**을 **차등화**할 필요가 있다.

<※참고> 보안시스템 자동화 시 인적개입 차등화 예시

위험수준	대응 자산 및 시나리오	자동화 조치 수준	인적 개입 여부
저위험	대내 직원 포털, 단순 로그 분석, 피싱 메일 수신 등	완전 자동화 (예시) 악성 이메일 즉시 격리, IP 주소 자동 차단	조치 결과 로그만 모니터링
중위험	일반 웹서버, 내부 정보 자산 권한 상승 시도 탐지 등	조건부 자동화 (예시) 의심 단말의 네트워크 격리	보안관제요원 확인 후 5분 내 미승인 시 자동 격리
고위험	코어 계정계, 실시간 결제·이체, 인증 DB 등	권고 및 대안 제시 (예시) 차단 규칙 추천	보안담당자/CISO 최종 승인 후 차단 실행

⑤ 금융권 공동대응 및 시스템 복원력 강화

프런티어 AI 기반 침해 공격은 기존에 비해 월등히 빈번히·집요하게 이뤄질 것으로 예상되는 바, **사고 발생 가능성**을 **전제**로 하여 **신속한 사후관리 대책**을 수립하는 것이 바람직하다. 공격 IP, 보안위험이 식별된 부분 등에 대한 **실시간 격리 체계**를 마련하고 **업무연속성계획**(BCP)이 **차질 없이 이행**될 수 있도록 실시간 대응체계를 마련하는 것이 좋다.

AI로 인한 고도화된 보안 위협에는 **개별 금융회사 차원의 대응**에 **한계**가 있으므로, **금융AI보안연구소**과 함께 ▲위험정보 공유, ▲공동 탐지룰 마련, ▲공급망 공동 점검 등 **공동 대응체계**를 마련한다.

⑥ 침해확산 방지

AI 기반 공격은 **초기 침투** 이후 금융회사 **내부 시스템 전체**로 **빠르게 확산**될 수 있으므로, **제로트러스트** 기반 **보안체계** 구축에 노력을 기울이는 것이 바람직하다.

공격자가 항상 **내부에 침입**했을 수 있다고 가정하여 ▲다중 인증 체계, ▲최소 권한 부여, ▲휴면계정 제거, ▲중요 데이터 접근시 검증 등 **접근통제 체계**를 **강화**하고, **침해 발생**시 **내부 이동을 제한**하기 위해 네트워크 세분화 등 **시스템 간 격리 체계**를 마련해 나갈 필요가 있다.

동 가이드라인은 1~3차에 걸친 **보안목적 AI 테스트 결과 등**을 반영하여 **지속적으로 업데이트**해 나갈 계획이며, 업데이트 내용 등은 **금융보안원 홈페이지***에서 확인할 수 있다.

* 금융보안원 홈페이지(www.fsec.or.kr) : 홈 > 자료마당 > 가이드

금융위원회는 "프런티어 AI 보안위협 관련 국내외 상황이 빠르게 변화하고 있는 만큼, **금융회사의 불안감을 낮추고 적극적인 보안강화 조치를 유도하는데 방점**을 두고 금번 방안을 마련하였다."고 설명하면서,
"금번 면책 방안과 가이드라인 배포를 통해 **금융업계가 보다 적극적이고 신속하게** 전산자원 관리·취약점 탐지·보안 패치 적용 등 **관리강화 조치에 나서줄 것을 기대**한다."고 언급하였다.

아울러, "앞으로도 프런티어 AI 관련 국내외 상황변화, 망분리규제 완화 등을 통한 AI 보안테스트 결과 등을 반영하여 **가이드라인 등을 유연하고 신속하게 보완**해 나갈 계획"이며, "**망분리규제 전면해제 등을 포함**해 **금융권의 AI 대전환을 지원**할 다양한 정책과제를 **적극적으로 추진**해 나갈 예정"이라고 언급하였다.

담당 부서	금융위원회 금융안전과	책임자	과 장	김 태 훈 (02-2100-2970)
		담당자	사무관	김 영 준 (02-2100-2573)
	금융위원회 금융정책과	책임자	과 장	권 유 이 (02-2100-2830)
		담당자	사무관	김 재 민 (02-2100-2833)
	금융감독원 디지털금융총괄국	책임자	국 장	이 석 (02-3145-7120)
		담당자	팀 장	노 경 록 (02-3145-7130)
	금융감독원 IT검사국	책임자	국 장	유 희 준 (02-3145-7420)
		담당자	부국장	김 송 범 (02-3145-7415)
	금융보안원 금융AI연구소	책임자	소 장	김 성 웅 (02-3495-9040)
		담당자	부 장	이 혁 준 (02-3495-9930)