금융감독원	**보 도 자 료**	금융은 튼튼하게 소비자는 행복하게

보도	2026.9.9.(수) 14:00	배포	2026.9.9.(수)	
담당부서	디지털금융총괄국 디지털금융총괄팀 디지털리스크분석팀	책임자	국 장	이 석 (02-3145-7120)
		담당자	부국장	손인호 (02-3145-7125)
			팀 장	이정운 (02-3145-7540)
	IT검사국 검사기획팀	책임자	국 장	유희준 (02-3145-7420)
		담당자	부국장	김송범 (02-3145-7416)

프런티어 AI 기반 보안 위협 대비 강화 등을 위한 「全 금융권 정보보호 최고책임자(CISO) 간담회」 개최

Ⅰ 간담회 개요

□ 금융감독원은 **'26.9.9.(수) 이종오 디지털·IT 부문 부원장보 주재**로 **「全 금융권 정보보호 최고 책임자(CISO) 간담회」**를 개최

○ 이번 간담회는 **프런티어 AI 기반**의 **사이버 위협**이 **현실의 문제**로 다가오는 상황에서 **금융회사**의 **대응 상황**을 살펴보고, **경영진 중심**의 **대비 태세 강화**를 독려하기 위해 마련

○ 특히, **근본적**인 **사고 예방·대응**을 위해서는 **대응 체계 고도화**와 함께 금융회사의 **IT 기본 통제 준수**가 **필수**인 점을 강조하면서, 현재 진행 중인 **자율 시정***에 **충실히 참여**하여 **사고 예방·감축**에 힘써달라고 당부

* 금융감독원이 배포한 자가 진단 도구를 기반으로 금융회사 스스로 IT 기본통제 운영실태를 점검·보완

全 금융권 CISO 간담회 개요

☑ **일시/장소** : '26. 9. 9. (수) 14:00 ~ 15:00, 금융감독원 대회의실(9F)

☑ **참 석 자** : **(금융감독원)** 디지털·IT 부문 부원장보, 디지털금융총괄국장, IT검사국장

(금융회사) 업권별 주요 금융회사 CISO (총 16社)

(협회 등) 전국은행연합회, 금융투자협회, 생명보험협회, 손해보험협회, 여신금융협회, 저축은행중앙회, 한국핀테크산업협회 IT 담당 임원 등

Ⅱ 간담회 내용

1 배경 및 경과

□ 지난 4월 앤트로픽社의 **프런티어 AI 미토스**가 등장한 이후 **AI 기반의 보안 위협**이 **고조***되는 가운데, **국내 금융회사** 대상 **사이버 공격**이 **빈발**하고 **공격 방식** 또한 **고도화**되는 모습

* 금년 중 국내외 보안 전문기관의 **신규 취약점 공개 건수**가 **크게 증가**
美 NIST 신규 취약점(건) : ['25.上] 23,664 → ['25.下] 24,497 → ['26.上] 35,872 (↑51.6%, yoy)
KISA 보안 공지(건) : ['25.上] 136 → ['25.下] 141 → ['26.上] 199 (↑46.3%, yoy)

○ 특히, **AI를 해킹에 악용**할 경우 **보안 취약점의 신속한 탐지**뿐만 아니라, 다수의 금융회사를 대상으로 한 **자동화**된 **대량 공격**까지 가능한 만큼, **금융 보안 체계**를 **한층 강화**해야 하는 상황

AI 기반의 사이버 공격 사례

◈ [AI 기반 침투 도구] 방화벽 등 **보안 장비**에 대한 **대규모 스캔·해킹 공격**에 **AI 기반의 해킹 도구** (CyberStrike AI) 사용 ('26.1~2월)

- **AI 기반 자동화**, **여러 AI 모델** 활용, **보안 도구**들을 상황에 맞게 골라서 사용하는 **지능형 오케스트레이터** (orchestrator) 엔진 탑재 등이 특징

  * ① 자연어로 명령하면 AI 에이전트가 100개 이상의 보안 도구를 자동 실행하여 보안 취약 시스템 탐색, ② AI가 침투 계획 수립 및 공격 코드 작성, ③ 클로드, GPT-4, 제미나이, 딥시크 등 15개 이상 AI 활용

◈ [AI 내장형 악성코드] **악성코드**에 **외부 AI 서비스** (상용 생성형 AI)를 **실시간**으로 **연계**하여, **악성코드 실행 중 AI**를 통해 **탐지 패턴**을 **우회**한 **새로운 공격 코드** 생성

  * ① **레이미 허그 (Lame Hug)** : '25.7월 러시아 해킹그룹 APT28이 우크라이나 국방기관 공격에 사용
  ② **프롬프트 플럭스(PROMPT FLUX)** : '25.11월 구글(GTIG)이 발견한 악성코드로, 외부 AI 서비스 (Gemini)를 사용하여 매시간 새로운 공격 코드를 재작성하고, 보안장비의 탐지 패턴을 우회

◈ [국가 배후 해킹그룹의 AI 기반 공격] **국가 배후 해킹 그룹** (GTG-1002)이 **AI**를 사용하여 **약 30여 개 글로벌 조직**에 **침해 시도** ('25.9월, 일부 성공)

- **사람**의 **개입**을 **최소화***하고, **생성형 AI** (클로드 코드)를 조작하여 **공격**의 **80 ~ 90%**를 **자율적**으로 **수행**

  * 사람은 목표 설정 및 일부 의사 결정만 수행하고, AI가 공격 방법·전략 등을 결정
  ('탐색 → 취약점 발견 → 공격 코드 (Exploit) 작성 → 수평 이동 → 유출' 全 과정을 AI가 수행)

□ 그동안 금융감독원은 금융위원회·금융보안원과 함께 '**AI 공격은 AI로 방어**' 하는 보안 체계 구축 등을 골자로 하는 「**금융권 보안 위협 대응 방안** ('26.5월)」을 마련하고,

○ ‣AI를 보안 목적으로 활용하기 위한 '**망 분리 규제 긴급 완화 조치** (제1차 6월~, 제2차 10월~)', ‣**적극적인 보안 패치** 등을 유도하기 위한 '**면책 방안** (7월)', ‣AI 보안 위협에 효과적으로 대응하기 위한 **금융권 가이드라인** (7월)을 발표

그간의 금융권 프런티어 AI 기반 위협 주요 대응 내용

◈ (프런티어 AI 관련 금융권 보안 위협 대응 방안 '26.5월) ❶ AI 보안 위협의 선제적 파악, ❷ AI는 AI로 방어하는 보안체계 구축, ❸ 금융회사의 AI 보안 위협 체계적 대응 지원 등

・ 보안 목적의 AI 활용을 위한 '망 분리 규제 긴급 완화 조치'(10사 대상 제1차 테스트, 6월~)

◈ (면책 조치 '26.7월) ❶ 보안 목적 AI 활용 테스트, ❷ 보안 취약점 패치 과정에서 경미한 전산 장애가 발생한 경우 신속한 복구와 소비자 보호 조치를 전제로 제재 면책

◈ (가이드라인 '26.7월) ❶ 경영진 책임 강화, ❷ 취약점 및 패치 관리, ❸ 자산 공급망 관리, ❹ AI 기반 방어 자동화, ❺ 금융권 공동 대응 및 복원력 강화, ❻ 침해확산 방지 등

◈ (제2차 망 분리 규제 긴급 완화 '26.9월) 보안 역량 있는 금융회사·전자금융업자 75사로부터 신청을 받아 10월 중 15사를 선정하여 제2차 테스트 예정

2 주요 논의사항

(1) AI 기반 보안 위협 대비 태세 강화

□ 현재 금융회사 대부분이 IT 위험 관리 체계를 마련·운영하는 등 **일정 수준**의 **대응 능력**을 갖추고 있으나, **AI 기반**의 **새로운 보안 위협**이 부상하고 있는 만큼 **전사적인 차원**의 **대응 체계**를 한층 **강화**할 필요

○ 특히, ‣**IT 자산 식별·관리 체계 구축**, ‣**대규모 보안 패치 대비** 등의 핵심 과제는 완비하는 데 **상당한 시간**과 **비용**이 수반되므로 **경영진**의 **적극적인 관심**과 **참여**가 **중요**

□ 이에 **금융감독원**은 **AI 보안 위협** 대비 과정에서 우선 보완해야 할 **유의 사항**을 **전달**하면서, **경영진이 앞장** 서서 **급변하는 사이버 환경**에 맞는 **보안 체계 강화 방안**을 **마련·이행**해 달라고 요청

○ 아울러, 대응이 **미흡한 금융회사**에 대해서는 **밀착 감시, 현장 점검, 경영진 면담** 등을 통해 **집중 관리**할 계획임을 안내

프런티어 AI 기반 사이버 위협 대비를 위한「유의 사항」주요 내용

◈ **(전사적 관리체계 마련·운용)** **경영진**을 **중심**으로 **전사적 IT 위험 관리체계**를 **수립**하고, **프런티어 AI** 등 새로운 보안환경에 맞추어 **정기·수시 검토·개선**

◈ **(IT 자산 식별·관리)** **모든 IT 자산**이 **공격 대상**이 될 수 있는 만큼, 이를 **식별·관리**할 수 있도록 **면밀한 IT 자산 식별·관리체계** 마련·운영

> ✔ **(예시)** 시스템, 프로그램, 클라우드, 오픈 소스 등 모든 IT 자산을 파악하고, 전산화 등을 통해 통합 관리하는 한편, 취약점 관리와 연계하여 보호 조치 실행

◈ **(보안 취약점 관리)** 보안 취약점 점검·관리를 **IT자산 식별·관리**와 **유기적**으로 **연계**하고, **단기간 다량**의 **취약점 발견** 시 **보정**(패치) **시간**을 **최소화**할 수 있는 **대비책 마련·운용**

> ✔ **(예시)** 자산·업무 중요도, 위험 노출도 등에 따른 '패치 우선순위'를 수립하고, '취약점·패치 정보 신속 획득 → 패치 테스트 → 패치 적용 등 프로세스를 내재화·자동화

◈ **(정보보안 위협 대응 체계 고도화)** 고도화된 침해행위 대응을 위해 **대응 절차**, **정보보호 모니터링**, **악성코드 감염·확산 방지 대책**, **접근 권한 관리** 등 **대응 체계 지속 점검·개선**

◈ **(침해사고 대비책 마련·소비자 보호 철저)** 침해 사고 발생 시 **서비스 신속 복구 체계** 및 **소비자 보호 방안**(대체 수단 안내, 피해 사실 통지·보상 등)과 함께 **외부 전문기관**과의 **협력·지원체계 수립·운용**

(2) IT 기본 통제 철저 및 금융회사 자율 시정 체계 확립

□ 한편, **고도화·지능화**되는 **사이버 위협**에 대처하기 위해 **AI** 등을 통해 **보안 체계**를 **고도화**하는 것도 중요하지만, **IT 보안**의 **근간**이 되는 **기본 통제**를 **철저히 준수**하는 것이 **필수적**

○ 최근 **주요 IT 사고**의 원인은 대부분 **기본적인 IT 통제 미흡***이었고, AI 공격은 이러한 틈을 **더욱 빠르고 깊게** 파고들 수 있음에 유의할 필요

* ▸중요 보안 패치 미적용, ▸퇴직자 계정 및 불필요한 서비스 포트 방치, ▸이용자 정보 암호화 미흡, ▸프로그램 변경 테스트 미흡 등

□ 이를 위해 금융감독원은 7월부터 **全 금융권**을 대상으로 **IT 기본 통제 준수 여부**를 **스스로 점검·보완**하는 '**자율 시정**'을 진행 중

○ 금융회사에 **적극적인 참여**를 통해 내부 통제 상 미흡 점을 적시에 점검·보완하는 **자율 시정 체계를 확립**하도록 요청하는 한편,

○ 향후 **검사** 시 **IT 기본 통제 운영실태**를 **중점 점검**하고, 기본 통제가 미흡한 **高위험사**에 대해서는 **현장 점검**을 실시할 계획임을 안내

IT 기본 통제 준수를 위한 자율 시정 추진 방안 주요 내용

◈ **(점검 대상)** 「전자금융거래법」 상 안전성 확보 의무가 적용되는 금융회사

◈ **(점검 방법)** 금융감독원이 배포한 자가 진단 도구를 기반으로 IT 감사인(자체) 등이 주관하여 기본 통제 운영 실태를 자체 점검·보완 ('26.7~11월)

◈ **(점검 항목)** 위반 시 사고 발생 개연성이 큰 5개 IT 기본 통제 부문별 점검 항목 및 점검 착안 사항 등을 포함

구 분(5개 부문)	주요 점검 내용
① **정보처리시스템 보호 대책**	☑ 보정작업(Patch) 및 보안 취약점 관리 체계 ☑ 제조사 기술지원 관리체계 등
② **전산 자료 보호 대책**	☑ 백업 및 소산 관리체계 ☑ 전산 자료 이용·유출 관리체계 등
③ **해킹 등 방지 대책**	☑ 업무시스템 및 솔루션 보안정책 관리체계 ☑ 정보보호 시스템(방화벽 등) 관리체계 등
④ **공개용 웹서버 관리 대책**	☑ 공격 표면에 위치한 자산 관리체계 ☑ DMZ 구간에 대한 침해 대응 관리체계 등
⑤ **프로그램 변경 통제**	☑ 프로그램 등록·변경·배포·폐기 관리체계 ☑ 긴급작업 관리체계 등

Ⅲ 주요 당부사항

□ **이종오 부원장보**는 **프런티어 AI 기반**의 **보안 위협**은 막연한 우려가 아니라 금융회사의 **생존**과 **직결**되는 **현실**의 **문제**가 된 만큼 **보다 높은 수준**의 **경각심**을 가져야 한다고 하면서

○ **대표이사**를 비롯한 **경영진**의 진두지휘 아래 **전사적 차원**의 **IT 보안 강화 방안**을 마련하고, **조직·인력·예산**을 **확충**함으로써 **새로운 기술**로 무장한 **사이버 위협**에 **철저히 대비**해달라고 당부

□ 또한, AI 기반의 **사이버 공격**이 **본격화**되는 상황에서 **IT 기본 통제**가 흔들리면 **사고**가 **되풀이** 되어 **금융회사**와 **고객**에게 **막대한 피해**를 초래할 수 있다고 경계하면서, **경영진**에 기본 통제 확립을 위한 **자율 시정**에 **앞장**서 달라고 요청

○ **적극적 자율시정**을 통해 **미흡사항**을 **충실히 보완**한 경우에는 **경미한 사고**가 발생하더라도 **제재 감면**을 **적극 검토**할 **방침**이나,

○ **형식적·소극적 자율시정**에 따라 **IT 기본 통제 미흡**이 원인이 되어 **대규모 IT·침해사고**가 발생할 경우에는 **최대한 엄중 조치**할 예정

Ⅳ 향후 계획

□ 금융감독원은 「**프런티어 AI 관련 금융권 보안 위협 대응 방안**('26.5월)」과 「**사전예방적 디지털 리스크 감독방안** ('26.4월)」 등을 차질 없이 **추진**하여 **금융권** 전반의 **IT·보안역량**을 **한층 강화**해 나갈 예정

○ **(AI 기반 방어 체계 구축 지원)** '**망 분리 규제 긴급 완화 조치**'의 **단계적 확대**를 통해 '**AI는 AI로 방어**'하는 보안체계 구축 지원*

* **제1차·제2차 테스트**를 차질 없이 시행하고, 테스트 결과 확인된 **중요 사항** (AI 보안 위험의 특징, 예상 공격 수법, 효과적 방어 요령 등)을 **全 금융권 적시 공유** 및 **AI 보안 가이드라인**에 반영

○ **(자율 시정 체계 확립)** **중요 위협정보, 진단 도구**(체크 리스트) 등을 **적시 전파**하여 **선제적**으로 **점검·조치***하도록 하는 한편, **불시 현장 점검** 등을 통해 **자율 시정**의 **실효성**을 **확보**

* '26.2월 본격 가동한 '**금융보안 통합관제 시스템 (FIRST)**'을 통해 중요 **보안 위협 요인**을 **금융권에 신속 전파**하여 **자율 점검·시정** 실시 중