2026년
디지털·IT 감독 검사 방향

금융감독 업무설명회
2026. 3. 4.

금융감독원 디지털금융총괄국 · IT검사국

금융은 튼튼하게
소비자는 행복하게

금융감독원

Contents

Ⅰ. 조직 구성 및 소관 업무

✓ 사전예방적 IT리스크 감독을 위한 팀 신설 : '디지털리스크분석팀'

✓ IT검사 기능 일원화 : 은행·금융투자검사국 內 IT검사팀 → IT검사국 이동

✓ AI 혁신 지원 및 감독 강화 : 디지털혁신팀 → AI·디지털혁신팀

디지털·IT 부문
(7개 부서 32개 팀)

디지털금융총괄국
- 디지털금융총괄팀
- 디지털리스크분석팀
- 디지털리스크감독팀
- AI·디지털혁신팀
- 감독데이터팀
- 금융데이터감독팀
- 금융데이터검사팀

IT검사국
- 검사기획팀
- 상시감시팀
- 은행검사팀
- 중소금융검사팀
- 보험검사팀
- 금융투자검사팀

전자금융감독국
- 전자금융총괄팀
- 건전경영팀
- 지급결제제도팀

전자금융검사국
- 검사기획상시팀
- 검사1팀
- 검사2팀
- 검사3팀

가상자산감독국
- 가상자산감독총괄팀
- 가상자산시장감시팀
- 가상자산검사팀
- 디지털자산기본법도입준비TF

가상자산조사국
- 가상자산조사기획팀
- 가상자산조사분석팀
- 가상자산조사팀

정보화전략국
- 정보화기획팀
- 정보화운영팀
- 감독정보시스템1~2팀
- 경영정보시스템팀
- 정보보안팀

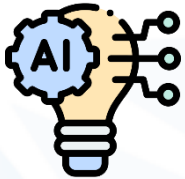
Contents

비대면 전자금융거래 확대

▸ 정보통신기술 발전 및
디지털금융 수요 증가 등
→ 전자금융거래 보편화/다양화
(모바일뱅킹, MTS 등)

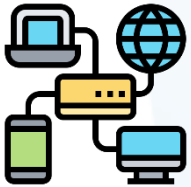
금융회사 디지털 전환 확산

▸ AI 등 디지털 신기술 기반
서비스 출시 및
업무 프로세스 디지털(효율)화



상호 연결성 증대

▸ 오픈뱅킹, 클라우드, 플랫폼사 등
외부 위탁·제휴 확산
→ 금융사·비금융사간
상호 연결성 확대



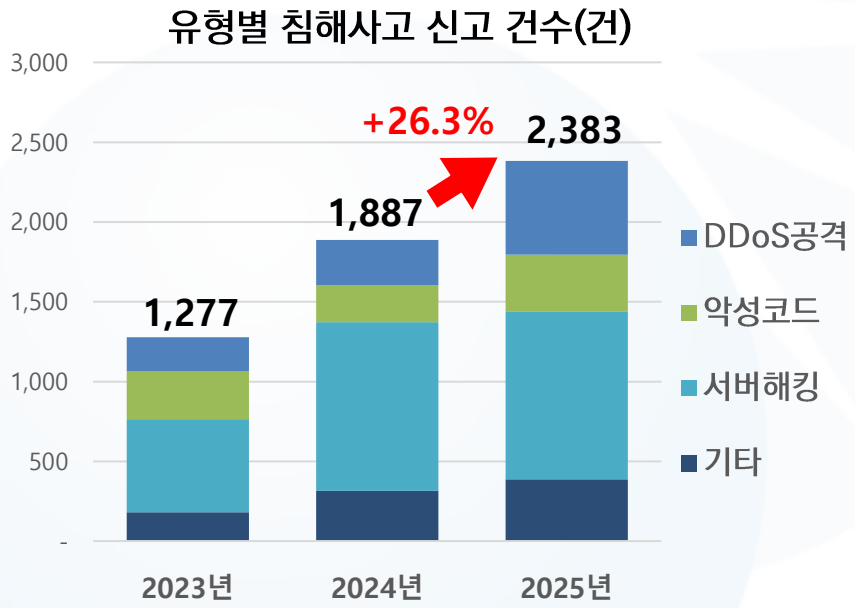
사이버 위협 지속 발생

▸ DDoS, 랜섬웨어,
취약점 악용 등
해킹 공격 지속 확대

✓ 각종 IT·보안 사고 발생

- SKT 유심 정보 유출(4월)
- 서울보증보험 랜섬웨어(7월)
- KT 무단 소액결제 사고(8~9월)
- 롯데카드 해킹(9월)
- 쿠팡 고객정보 유출(11월)

✓ 민간기업 침해사고 확대



(자료 : 한국인터넷진흥원)

Ⅱ－❸ 디지털금융 위험 요인

디지털금융 확대 → 공격 표면 확대

- 위탁·연계 확대
  → 제3자 리스크 확대
- 망분리 예외 대상 확대
- IT자산 식별 복잡성 증대

사이버위협 지능화 및 피해 대형화

- AI활용 공격, 해킹세력 조직화 등 사이버 위협 지능화
- 침해사고 및 전산장애 발생시 광범위한 피해 유발

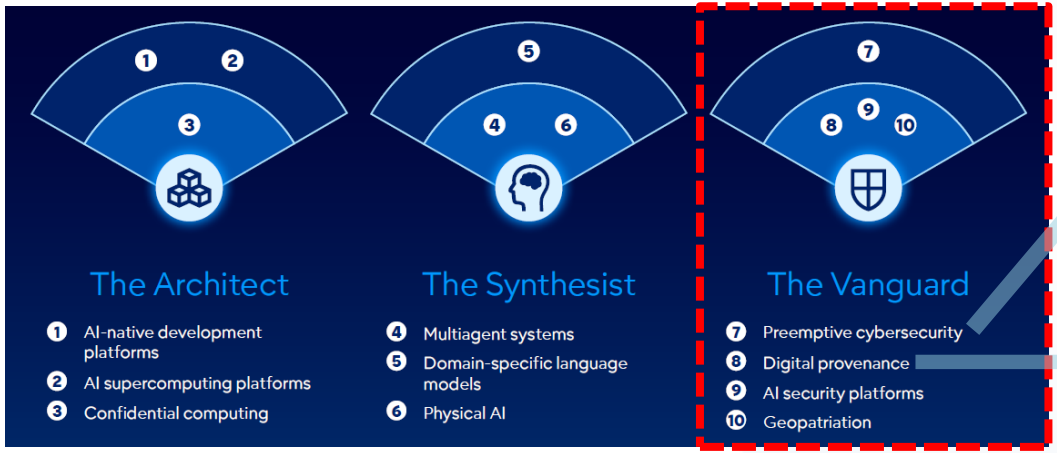
IT보안 관련 회사 경영진 인식 저조

- '정보보안 투자' = '비용' ?
- 투자·인력 최소화
  (규제 준수만 충족)

능동적 사전 예방체계 부족

- 보안 취약점 능동적·사전적 대응(식별·분석·조치) 저조
- 사이버 복원력(Resilience) 확보 부족

가트너(Gartner)「2026년 10대 전략 기술 트렌드」中



⑦ 선제적 사이버보안

- 사후 대응 중심의 방어 전략에서 **사전 예방 중심**의 전략으로 전환

⑧ 디지털 출처

- 오픈소스 코드, AI 생성 콘텐츠 활용 증가에 따라 **디지털 자료출처** 검증 중요성 확대

포브스(Forbes)「사이버보안 2026 : 6가지 전망과 청사진」中

[1] 에이전트 AI, 새로운 공격 및 방어의 최전선

[2] 포스트 양자 암호화로의 전환

[3] 딥페이크, 합성 미디어, 신원 사기 증가

[4] IoT, 엣지, 기기 증가에 따라 공격 표면 확대

[5] 사이버 범죄, 기업형 사업으로 성장

[6] 사이버보안, 전체 비즈니스의 전략적 기둥

◈ 사이버 보안을 단순 IT센터 비용이 아닌 전사적인 주요 전략(a strategic pillar for the whole business)으로 다루는 기업이 성공

◈ CISO를 전략적 비즈니스 파트너로 격상

◈ '위협 방어', '사이버 복원력 측정'을 관리 목록에 추가

Contents

이용자 보호 최우선 → 안전한 디지털금융 생태계

‘안전’한 디지털금융		‘책임’ 있는 금융 혁신
❶ 사전 예방적 감독·검사		❹ 금융 AI 활용의 신뢰성
❷ 디지털 복원력 강화	+	❺ 데이터 활용·결합 활성화
❸ 책임성 강화 제도 개선		❻ 망 분리 등 규제 개선

✓ (소 비 자) 디지털 금융을 보다 안전하고 편리하게 이용
✓ (금융회사) 불필요한 보안사고 예방, 미래 성장 잠재력 확보

✓ IT 리스크를 조기 식별하여 신속 대응하는 사전 예방적 감독·검사 체계로 전환

금융보안 통합관제시스템(FIRST) → 보안위협에 체계적 대응

* Financial-IT Incident Response Surveillance control-Tower

- 보안정보 상시 수집 DB화 → 중요정보 · 요조치 사항 신속 전달 및 결과 회신
- 유사시 비상연락망 기능 (실시간 쌍방향 소통 채널)

전자금융기반시설 취약점 분석·평가 실효성 확보

- IT자산 목록 체계적 분석·관리 (관리방식 표준화 및 전산화 방안 등 마련)
- 취약점 보고서 분석, 보완 조치 계획 수립·이행 여부 점검 → 실효성 제고

✓ IT 리스크를 조기 식별하여 신속 대응하는 사전 예방적 감독·검사 체계로 전환

IT리스크 상시점검, 高위험사 선별·집중 관리

- IT리스크 계량항목에 사고 개연성이 높은 지표 * 보강 → 위험 상시 점검
  * (예시) [실태평가] 이사회·경영진 금융IT 역할 등, [계량평가] 기술지원 종료서버 비율, UPS노후화 비율 등
- 보안통제 현황 점검 → 고위험사 선별 및 핀포인트·테마검사

전 금융권 IT내부통제 체계 확립

① 자체점검 : 최근 IT사고유발 5대 IT기본통제 실태 점검·보완

② 수시검사 : 전 금융권 고위험사 대상 5대 IT기본통제 집중 점검

③ 정기검사 : IT환경변화에 따른 핵심 리스크* 등 IT업무 운영실태 점검

* 해킹방지, 비상대책, 제3자 서비스, 성능관리, 클라우드, 가이드라인 이행 등 10대 리스크

✓ 사고 대응체계 정비, 비상대응 훈련 등을 통해 금융의 디지털 복원력 강화

금융회사의 IT 사고 대응 체계 정비

- IT 사고에 따른 소비자 피해 확산 방지를 위해
  ‘금융권 중대 전자금융사고 대응 가이드라인’ 마련

  * 사고발생시, 소비자 피해 확산 방지 절차, 신속 복구 체계, 재발방지대책 수립 절차 등 포함

비상대응 훈련 내실화

- 합동 재해복구 전환훈련 확대 실시
  (상호금융 등 중소금융권 금융회사, 대체거래소, 클라우드 서비스 제공자 등 포함)
- 블라인드 모의 해킹, 버그바운티 지속 확대 → 보안 취약점 사전 발굴 조치

✓ IT 안정성 확보 및 사고 예방을 위한 금융회사의 책임성 강화

전자금융거래법 개정 지원

- (경영진 책임) 거래 안정성 확보 의무의 최종 책임자를 대표이사로 명시, CISO 권한·신분 보장, 독립성 규정 법률 명시
- (징벌적 과징금) 대형 전자금융사고 발생시 부과 (예 : 최대 총 매출액의 3%)
- (이행강제금) 취약점 분석·평가 결과 보완조치 미이행 시 부과 (예 : 5천만원 이하)
- (정보보호 공시) 자발적 정보 보호 투자 촉진, 국민의 알 권리 보장 (예 : IT 조직, 인력, 예산, 침해사고 발생 현황, 대응조치 결과 등)

✓ 신뢰성 있는 AI 활용 유도, 데이터 품질 및 활용 제고

혁신과 책임이 균형을 이루는 금융 AI 생태계 조성

- AI 활용 全주기의 위험을 관리하는 AI 위험관리 프레임워크(AI RMF) 도입
- AI활용의 공정성·투명성·책임성 제고를 위한 「금융AI 윤리지침」 제정

데이터의 안전한 활용·결합 지원 등

- 데이터 결합품질 제고, 결합데이터 재사용 및 결합 활성화를 위한 개선방안 마련
- 대규모 데이터를 처리하는 신용정보 집중기관 등의 데이터 보안 ·통제 실태 점검

✓ 신뢰성 있는 AI 활용 유도, 데이터 품질 및 활용 제고

망 분리 예외 확대 등 금융혁신 지원 지속

- 생성형 AI 규제특례 신청 신속 처리 및 변경 절차 간소화 추진
- SaaS 활용 정규화 추진 (시행세칙 개정 중)
- 내실있는 샌드박스 운영을 위한 제도 개선 검토


감사합니다
FINANCIAL SUPERVISORY SERVICE