

보도	2025.5.15.(목) 10:30	배포	2025.5.14.(수)	
담당부서	디지털금융총괄국	책임자	국 장	위충기 (02-3145-7120)
	디지털금융총괄팀	담당자	팀 장	이수인 (02-3145-7125)

## 금융감독원, 금융권 CISO 간담회 개최 - SKT 해킹사고 등 사이버 위협에 대응한 보안 강화를 당부 -

### I. 개 요

- 최근 SKT 유심정보 해킹 여파로 사이버 위협이 고조된 가운데 금융IT 안전성 확보를 위한 금융권의 체계적인 대응이 필요
- 이에 금융감독원은 '25.5.15.(목) 이세훈 수석부원장 주재로 주요 금융업권 CISO(정보보호최고책임자) 간담회를 개최하여,
  - 금융회사의 사이버 위협 대응 현황을 점검하는 한편, 금융권 보안 강화를 위한 당부사항을 전달하고 애로·건의사항을 청취하였음

#### 금융권 CISO 간담회 개요

■ 일시 · 장소 : '25. 5. 15.(목) 10:30~11:30, 금융감독원 본원 9층 중회의실

■ 참석자 : 금융감독원, 금융보안원, 금융협회 및 주요 금융회사 CISO

- (금 감 원) 수석부원장, 디지털·IT 부원장보, 디지털금융총괄국장
- (유관기관) 금융보안원, 은행연합회, 금융투자협회, 생명보험협회, 손해보험협회, 저축은행중앙회, 여신금융협회
- (은 행) 농협은행, 우리은행, 하나은행, 카카오뱅크 - (증 권) 미래에셋증권 토스증권
- (보 험) 삼성생명, KB손해보험 - (여 전) 신한카드, 현대캐피탈

## II. 최근 사이버 위협 동향 및 대응 현황

- **(국내 동향)** AI 등 IT 신기술을 활용한 디지털 금융 확산으로 금융거래 편의성이 제고되고 있으나, 이에 따른 잠재적 사이버 위협도 증가 추세
  - 최근 금융권에서 침해사고\*가 잇따르고 있으며, 이동통신사 해킹에 따른 부정거래 등 2차 피해도 우려되는 상황
    - \* ① 아이디/패스워드 무차별 대입 공격에 따른 개인정보 유출('25.3월)
    - ② 악성코드 감염에 따른 사내 그룹웨어 중단('25.4월)
    - ③ IT외주업체를 통한 고객정보 유출('25.4월)
  - 특히, 클라우드 이용 등으로 외부와의 연계성이 높아짐에 따라 공격표면\*(Attack Surface)이 확대되는 등 보안 위협이 복잡·다양화
    - \* 사이버 공격을 수행하는데 사용할 수 있는 모든 장치, 네트워크 경로 및 취약점
- **(해외 동향)** 사이버 공격으로 인한 정보유출 사고\* 등이 빈번히 발생하고 있으며, 이에 따라 국제감독기구도 IT 안전성 감독을 강화하는 추세
  - \* ① 대출기관(미국, LoanDepot) 랜섬웨어 공격으로 1,600만명 고객정보 유출('24.1월)
  - ② 은행(스페인, Santander) 해커 공격으로 최대 3,000만명 고객정보 유출('24.6월)
  - ③ 연금기금(호주, AustralianSuper) 해커 공격으로 고객자금 50만달러 손실('25.4월)
  - IMF·FSB 등은 사이버 보안 위협의 시스템리스크 전이 우려에 따라 사이버 사고에 대한 효과적 대응지침 등을 제시한 바 있으며,
  - EU는 ①IT 사고관리·보고체계 구축, ②운영복원력 테스트 의무화, ③사이버 위협정보 공유 강화 등을 위한 DORA법 시행 중
- **(대응 현황)** 금융감독원은 비상대응본부 운영, 유관기관과의 공조 등을 통해 금융권 대응상황을 모니터링\*하고, 금융사고 및 소비자 피해 예방에 역량을 집중하고 있으며,
  - \* SKT 유심정보 유출사고에 따른 부정거래 등 2차 피해 발생 여부 일일 모니터링
  - 사이버 공격의 복잡·다양화에 대응한 정보공유체계 구축 및 IT 감독 강화 등 근본적인 보안 위협 대응방안을 마련할 예정

### Ⅲ. 보안 강화를 위한 당부사항

---

- 이세훈 수석부원장은 사이버 위협에 대응하여 금융보안에 만전을 기해줄 것을 강조하면서 아래와 같이 주요 사항을 당부하였음

#### ① CEO 책임 하에 철저한 보안체계 구축

- 보안사고는 회사의 중대한 피해로 직결될 수 있으며, 이에 대한 최종 책임은 CEO 등 경영진에게 있다는 점을 명심하여, 사이버 위협에 대비한 보안체계 구축에 각별한 관심을 기울일 필요
- 이를 위해 CISO는 이사회에 중요사항을 충실히 보고\*하는 등 최고 경영진의 보안 리더십이 원활하게 발휘될 수 있도록 적극 지원

\* CISO로 하여금 전자금융거래의 안전성 및 신뢰성에 중대한 영향을 미치는 사항을 이사회에 보고하도록 '25.2월 「전자금융감독규정」 개정('25.8월 시행)

#### ② 외형 성장에 걸맞는 내부 보안역량 구비

- 금융회사 업무범위 및 영업 확장 등 외형성장에 따라 내부 IT 보안 역량도 이에 걸맞는 수준으로 갖추도록 노력할 필요
- 특히, 기본적인 보안 역량이 미흡함에도 업무 확장에만 치중하는 회사에 대해서는 영위할 수 있는 업무의 범위 및 규모에 제약이 따를 수밖에 없음에 유의

#### ③ 대선 등 정치적 상황에 따른 사이버 공격에 각별히 유의

- 대선 등 정치적 상황을 틈탄 사이버 공격 가능성에 대비하여 평소보다 긴장감을 가지고 보안과 안전에 각별히 유의할 필요
- 이를 위해 IT정보자산에 대한 악성코드 탐지·방어체계의 보안 사각지대를 전사적으로 재점검하고, 미흡사항은 즉시 보완

## IV. 향후 계획

---

□ 금융감독원은 현재 가동중인 비상대응본부를 중심으로 SKT 해킹 사고 여파로 인해 금융소비자 2차 피해가 발생하지 않도록 집중 모니터링을 지속할 예정이며,

- 금융권이 신속하고 효율적으로 사이버 보안 위협에 대응할 수 있도록 유관기관과의 통합관제체계\*를 구축할 계획

\* 5월 중 금융보안원과 정보공유 및 협력강화를 위해 MOU를 체결하고, 하반기 까지 금융권 실시간 쌍방향 비상연락체계 구축을 완료할 예정

□ 또한, 변화하는 디지털 금융 환경에 맞추어 금융회사 자율보안 역량과 IT 안전성 강화를 위한 감독대책을 마련할 예정

- 금융권의 IT 안전성 및 복원력을 강화하고 사이버 위협의 복잡·다양화에 효과적으로 대응하기 위해 해외 감독기구 사례 등을 참고하여 종합적인 대응방안을 수립하고,
- 금융권의 IT 인프라 운영 및 통제에 사각지대가 발생하지 않도록 소규모 금융회사\* 또는 제3자에 대한 감독 강화도 추진할 계획

\* 영세한 규모를 감안하여 규제수준을 높이기 보다는 자체점검, 컨설팅 등을 통해 보안수준 개선을 유도하는 맞춤형 대책 마련