

금융권 침해사고 재발방지를 위해 금융보안 관리체계를 전면 강화하겠습니다.

금융위 사무처장 주재, 「제2차 긴급 상황대응 회의」 개최-

- ▶ 신한은행 사고 전후 총 16개사 침해사고 확인, 동일주체 여부 등은 정밀 조사중
- ▶ 총 555개사 체크리스트 점검결과 130개사 일부 미흡사항 확인, 즉시 보완조치 실시
- ▶ ①보안체계·관리시스템 전수점검, ②해킹위협 관제 시스템 고도화, ③취약점 점검평가 강화, ④중소형 금융사 AI 해킹위협 대응 지원 등 제도개선 과제 신속히 검토 추진
- ▶ 보안점검 권고가 실제 현장에서 제대로 이행·작동될 수 있도록 CEO 책임 강화 및 제재 실효성 제고 등을 위한 다양한 제도개선 방안도 조속히 추진할 계획

[개요]

'26.10.14.(수) 금융위원회는 신진창 사무처장 주재로 금감원, 금보원, 과기부, 행안부, 개보위, 경찰청, KISA 등 관계기관과 함께 「제2차 긴급 상황대응 회의」를 개최하였다.

금융위원회와 금융감독원·금융보안원은 신한은행·국민은행 등 주요 금융회사 해킹사고 직후부터 ▲즉각적인 현장 조사인력 파견, ▲정보유출 고객 소비자 보호조치 안내, ▲全금융권에 공격자 IP 공유·체크리스트 배포 등 조치를 긴밀하게 취해나가고 있고, ▲사무처장 주재 「긴급 상황대응 회의(10.2.)」, 금융위원장 주재 「全금융권 긴급점검 회의(10.4.)」 등을 통해 全금융권이 경각심을 갖고 금번 사태에 엄중히 대응해 줄 것을 주문한 바 있다.

금번 회의는 지난 10월 2일 신진창 사무처장 주재 회의를 통해 지시한 체크리스트 점검결과를 확인하고, 향후 이러한 사고가 재발하지 않도록 하기 위한 정책 과제를 논의하기 위해 개최되었다.

·일시/장소 : '26.10.14.(수) 15:00 / 정부서울청사

·참석 : [금융위] 신진창 사무처장(주재), 디지털금융정책관 등
[금감원] 디지털·IT부원장보, 디지털금융총괄국장, IT검사국장 등
[금보원] 금융보안원장, 사이버대응본부장, 금융AI연구소장 등
[관계기관] 과기부, 행안부, 개보위, 경찰청, 한국인터넷진흥원, [보안전문가]

·논의사항 : ①全금융권 체크리스트 점검결과, ②금융권 침해사고 조사경과,
③금융권 보안 관리체계 강화방안 등

[금융권 침해사고 조사경과]

신한은행 침해사고 전후로 사고 발생이 확인된 금융회사는 은행·저축은행·상호금융·여전업·전금업·온투업·가상자산사업자 등 **소업권에 걸쳐 총 16개사***로 파악되었다. 현재도 금융회사들이 공유된 IP 등을 바탕으로 침해발생 여부를 확인중에 있어, 사고발생 금융회사 수는 이보다 더 확대될 수 있다. 현재까지 확인된 금융회사들의 **정보유출 규모는 약 10만건**(성명, 연락처, 주민등록번호, 이메일 등) 수준으로 파악되었으며, 직접적 부정결제 우려가 있는 **정보 유출**(계좌번호, 카드번호 등)은 **확인되지 않았다**.

* [은행] 신한, 국민, 부산, 하나, [저축] 예가람, 웰컴, 디비, 오케이 [여신] 현대캐피탈, 산은캐피탈, [온투] PFCT, 모우다, [전금] 브라이트픽스 [가상자산] 스트리미, 프라뱅, [상호] 새마을금고중앙회

사고 발생이 신고된 금융회사들에 대해서는 ▲신속히 공격IP를 차단하고, 보안패치, 관련 서비스 중단 등 추가 침해사고 방지조치를 취하고, ▲개인 정보 유출사실·대응요령 안내 등 소비자 보호 조치를 취하도록 관리·감독하고 있으며, ▲금감원·금보원 현장 조사 등을 바탕으로 침해경로·공격방식 등을 신속히 파악해 각 사례별 연관성·동일 주체 여부·AI해킹 가능성 등에 대해 심도 있게 확인중에 있다. ▲아울러, 과기부·행안부·개보위·경찰 등 유관기관과 긴밀한 협조를 통해 금융 외 부문에 피해확산을 방지하고 공격자 검거 등 수사가 원활히 이뤄질 수 있도록 만전을 기해 나갈 예정이다.

[체크리스트 점검결과]

지난 10월 8일까지 진행한 **소 금융권 555개사**에 대한 12개 항목의 **체크리스트** 점검도 마무리 되었다. 점검결과 **총 425개사**는 ‘적정’으로 제출하였고, **130개사**는 **미흡사항**이 있음을 보고하였다. 미흡사항이 발견된 회사들은 대부분 보안패치·관제체계 관련 1~2건의 점검항목에서 보완 필요사항이 확인되었으며, 상대적으로 보안역량이 약한 전금업·온투업 부문에서 비교적 많은 미흡사항이 발견되었다.

체크리스트 점검에 앞서, 공격자로 확인된 IP에 대해서는 우선 즉시 차단토록 조치하였고, 발견된 미흡사항에 대해서는 긴급한 조치부터 신속히 시행토록 지도·감독하고 있다.

구체적으로, 주요한 주요한 미흡사항은 ▲최신 보안패치 미적용, ▲제조사 기술지원 종료(EOS : End of Support) 시스템 관리 미흡, ▲실시간(24시간) 관제 체계 미구축, ▲공격표면 관리 미흡(대외시스템 대상 인증·인가 누락, 중요 서비스에 대한 강화된 인증절차(MFA) 미도입 등) 등이 보고되었고, 각 금융회사들은 ▲신속한 보안패치·노후장비 처분 및 교체, ▲보안관제 인력·설비 등 확충, ▲인증범위 확대·접근통제 강화 등 공격표면 관리 강화 조치 등 신속한 보완조치 실행계획도 함께 보고하고 즉시 조치 시행중이다.

[정책과제]

금일 「제2차 긴급 상황대응 회의」에서는 이번에 체크리스트 점검과정 등에서 발견된 취약요인 발생을 구조적·체계적으로 방지할 수 있는 근본적인 제도개선 과제에 대해서도 심도있게 논의하였다.

첫째, 금융회사 보안체계·관리시스템 전수점검을 추진한다.

금번 침해사고의 특성·공격유형 등을 감안해 시급한 조치가 필요했던 12개 항목의 체크리스트 점검이 마무리된 만큼, AI 해킹위협 등 새로운 보안 위협에 대해 금융권이 충분한 대비태세를 갖추 수 있도록 공격표면 관리·인증체계·내부통제 등 보안관리 전반을 촘촘히 전수점검하고 대응계획을 마련토록 할 계획이다. ▲전산시스템이 외부와 연결되는 모든 접점을 목록화·현행화하고, ▲외부접점의 인증·접근통제 권한을 명확히 설정·엄격히 관리하며, ▲외부접점 관리 등 보안체계 운영·관리와 CEO·CISO·CIO 등의 보고체계·책임범위 등도 명확히 하도록 지도·감독해 나갈 예정이다.

이와 관련한 구체적인 점검범위와 일정을 금융권과 협의를 통해 신속히 확정·추진해 나갈 예정이다.

둘째, 금융권 해킹위협을 조기에 포착하고, 공동 대응하는 체계를 마련한다.

현재, 금감원·금보원이 파악한 해킹위협 정보는 통합관제시스템(FIRST) 등을 통해全军금융권에 신속히 전파되고 있으나, 금융회사가 자체 보안관제 과정에서 파악한 정보는 공유되지 않고 있는 상황이다.

AI 해킹 위협에 대한 대응은 신속한 위협상황 인지와 조속한 공동대응이 중요한(“속도가 생명”) 만큼, ▲금융회사가 자체 파악한 위협정보도 통합관계 시스템 등을 통해 공유할 수 있도록 시스템을 개선하고, ▲금융회사가 침해위협 정도를 직관적으로 확인·대응할 수 있는 AI 위협수준 정보체계도 조속히 마련해 나갈 계획이다. 또한, ▲공격자 관점에서 외부 노출자산, 내부 소스코드, 모바일 앱 등의 취약점을 탐지할 수 있도록 AI 기반 취약점 점검 인프라 구축도 추진한다.

셋째, 금융회사가 상시적으로 면밀한 보안관리를 하도록 제도기반을 마련한다.

금융회사·전자금융업자는 「전자금융거래법」과 「전자금융감독규정」에 따라 연 1회(외부 홈페이지는 연 2회) 취약점 점검·평가를 하도록 의무화되어 있으나, 빠르게 진화하는 AI 보안위협에 비추어, 보다 치밀하고 정교한 점검이 이루어져야 한다는 지적이 제기되는 상황이다.

▲공격표면·외부접점이 넓고 고객수가 많은 대형 금융회사부터 취약점 점검·평가 주기를 연 2회 이상으로 확대하고, ▲중요한 외부접점 등은 필수 점검대상에 포함하는 방안을 추진한다. ▲아울러, 긴급한 필요가 있을 경우 수시점검 할 수 있는 근거를 마련하는 방안도 검토·추진할 예정이다.

넷째, 중소형 금융회사에 대한 보안관리 지원도 강화한다.

AI보안위협에 대해 충분한 대응여력을 갖추기 어려운 중소형 금융회사 등에 대한 지원방안도 조속히 검토·추진할 예정이다.

▲금융보안원이 각 업권 협회·중앙회와 함께 AI 기반 공동 보안관계 시스템 구축을 검토하고, ▲AI 침해위협에 대비한 공격표면 점검(블랙박스 테스트), ▲중소형 금융회사 맞춤형 보안안내서 마련 등 다양한 방안도 추진할 계획이다.

아울러, 대부업, 보험GA 등 「전자금융거래법」 적용대상에서 빠져있어 그간 면밀한 관리가 어려웠던 부문에 대해서도 AI 보안위협에 대한 대응요령을 신속히 전파하는 등 보안 강화방안도 조속히 검토·추진할 예정이다.

신진창 사무처장은 “금융분야는 그 무엇보다 신뢰와 안전이 중요한 만큼, 보안사고 예방을 위한 철저한 보안관리가 필수적이다.”고 언급하며,

“그간 롯데카드 정보유출, 미토스 쇼크 등 다양한 계기로 수차례에 걸쳐 전수점검과 관리 강화를 주문했음에도, 금융회사에서 기본적인 부분이 잘 지켜지지 않는 사례가 발견된 것은 매우 뼈아픈 부분”이라고 지적하였다.

아울러, “금번 사고를 계기로 금융회사 외부접점·인증관리 등 공격표면 관리뿐 아니라 쏜금융권의 보안관제 체계, CEO·이사회 등 책임성 확보 등 보안체계 전반에 대한 철저한 재점검과 근본적 제도개선이 이뤄지도록 최선을 다할 것”이라고 강조하였다.

또한, “AI 보안위협 확대에 대비해 ‘AI공격은 AI로 방어’하는 보안체계를 확립하기 위한 망분리 규제 완화 등 제도개선도 보다 면밀하고 속도감 있게 추진해 나가겠다”고 언급하였다.

담당 부서 <총괄>	금융위원회 금융안전과	책임자	과 장	김태훈	(02-2100-2970)
		담당자	사무관	김영준	(02-2100-2573)
담당 부서 <공동>	금융감독원 디지털금융총괄국	책임자	국 장	이 석	(02-3145-7420)
		담당자	팀 장	이정운	(02-3145-7540)
			팀 장	노경록	(02-3145-7130)
	금융감독원 IT검사국	책임자	국 장	유희준	(02-3145-7420)
		담당자	팀 장	이우람	(02-3145-7425)
	금융보안원 금융AI보안연구소	책임자	부 장	서호진	(02-3495-9900)
		담당자	팀 장	성인제	(02-3495-9910)
	금융보안원 사이버대응본부	책임자	부 장	김기철	(02-3495-9400)
		담당자	팀 장	장운영	(02-3495-9420)