

최근 침해위협 대응
금융권 긴급 점검회의

모두 말씀

2026. 10. 4. (일) 14:00

금융위원회 위원장
이 역 원

1

인사 말씀

안녕하십니까.

금융위원회 이익원 위원장입니다.

먼저, 사안의 엄중함을 감안하여
주말임에도 불구하고
이찬진 금융감독원장님,
박상원 금융보안원장님,
그리고 쏘금융권업권의 협회장님들과
금융회사 CEO 여러분들을 모셨습니다.

아울러, 이 자리에는 과기부, 개보위, 경찰청 등
관계부처에서도 함께해 주셨습니다.

2

최근 금융권 침해위협 상황

여러분, 최근 며칠간 잇따라 발생한
금융권 침해사고로 인해
국민들의 우려가 커지고 있습니다.

우리 금융권에서 가장 높은 신뢰를 갖춘
주요 시중은행뿐 아니라,
저축은행, 캐피탈 등 여러 금융업권에서
침해사고가 단기간에 다수 발견되고 있는 만큼,

금융권 전체가 지금의 상황을 엄중하게 인식하고
최고 수준의 경각심을 가져야 할 시점입니다.

현재 개별 사고의 정확한 원인과 공격수법에 대해서는
보다 면밀한 조사와 분석이 필요합니다.

다만, 현재까지 파악된 사고들을 살펴보면
대출모집인, 임직원 등이 업무상 편의를 위해 사용하는
외부 웹사이트, 서버 등
상대적으로 관리의 관심이 덜했던 영역이
공격 대상으로 활용된 사례가 확인되고 있습니다.

일각에서는 인증 등 기본적인 보안조치가 미흡하거나,
업무상 필요 이상의 정보가 보관·조회되는 등
보안관리의 사각지대가 있다는 점도 제기되고 있습니다.

이는 아무리 견고한 보안체계를 갖추고 있더라도
관리되지 않는 하나의 빈틈이
전체 보안체계의 취약점이 될 수 있다는 점을
다시 한번 보여주고 있습니다.

현재까지 부정결제 등에 직접 활용될 수 있는
민감한 정보가 유출된 정황이 확인되지 않았지만,
유출된 정보를 악용한
보이스피싱·스미싱 등 2차 피해로
이어질 가능성도 배제할 수 없는 만큼,
긴장의 끈을 놓지 않고 선제적으로 대응해야 합니다.

확정적으로 말씀드리기는 어렵지만,
AI를 활용한 해킹공격의 가능성도
배제할 수 없습니다.

새로운 유형의, 빈도 높은 사이버 공격이
앞으로도 이어질 수 있는 만큼
“AI공격은 AI로 방어하는”
보안체계 마련도 서둘러 나가야 합니다.

3 당부사항

이러한 상황에서, 비상한 각오로
금융권에 다음과 같은 사항을 당부드리고자 합니다.

첫째, 쏘금융권은 신속하고 철저한 보안점검을 해주시기 바랍니다.

무엇보다 중요한 것은
추가적인 침해사고가 발생하지 않도록
사전에 철저히 대비하는 것입니다.

소비자들이 안심하고 금융서비스를 이용할 수 있도록
외부에 노출된 IT자산과 서비스는 물론,
인증·접근통제, 침해활동 탐지체계 등
보안체계 전반을 공백과 빈틈이 없도록
빠짐없이 점검해 주시기 바랍니다.

특히, 공격 IP, 공격수법 등
이미 금융권에 공유된 위협정보가
실제 탐지·차단체계에 제대로 반영되었는지,

필요한 보안패치와 대응조치가
신속하게 이루어졌는지를
재차, 삼차 확인해 주시기 바랍니다.

이미 공유된 공격정보와 사고사례가 있음에도
필요한 점검과 대응을 소홀히 하여
유사한 사고가 발생하는 경우에는
관련 법령에 따라 엄정히 책임을 묻겠습니다.

둘째, 외부접점 등 잠재적 위험요인을 최소화해 주시기 바랍니다.

보안은 가장 기본적인 외부접점에 의해
무너질 수 있으므로,
대고객 서비스뿐만 아니라
임직원, 대출모집인, 위탁업체 등이 사용하는
외부접점과 접근경로까지 빠짐없이 살펴야 합니다.

일단 긴급대응 차원에서
소비자 서비스 제공이나 업무수행에
반드시 필요한 경우가 아니라면
외부접근은 모두 차단하는 것을 기본 원칙으로 하고,

업무상 불가피하게 외부접근이 필요한 경우에도
접근권한과 조회 가능한 정보는
필요 최소한으로 제한해 주시기 바랍니다.

특히, 개인신용정보 등 고객정보가
업무상 필요한 범위를 넘어
불필요하게 보관되거나 조회되고 있지는 않은지,
인증절차가 누락되거나 우회될 수 있는
접근경로는 없는지 철저히 점검해 주시기 바랍니다.

셋째, 소비자 보호와 피해구제에 빈틈이 없도록 해주시기 바랍니다.

침해사고가 발생하면
무엇보다 소비자 피해를 최소화하는 것이 중요합니다.

사고 발생 즉시
유출정보의 범위와 소비자 피해 가능성을
신속하고 정확하게 파악하고,

추가적인 정보유출이나 금전피해가
발생하지 않도록 필요한 보호조치를
즉시 시행해 주시기 바랍니다.

만일, 소비자 피해가 확인되는 경우에는
관련 사실을 상세하고 신속하게 안내하고,

피해구제와 보상이

차질 없이 이루어질 수 있도록

최선을 다해 주시기 바랍니다.

아울러, 정보유출을 악용한

보이스피싱·스미싱 등 2차 피해 가능성에도 대비하여,

이상금융거래 탐지를 강화하고

필요한 소비자 안내와 보호조치가

적시에 이루어질 수 있도록 해주시기 바랍니다.

넷째, 금융권 공동대응을 강화해 주시기 바랍니다.

사이버 위협은

어느 한 금융회사만의 문제가 아닙니다.

금융권은 금융회사 간 업무와 서비스가 상호 연계되어 있고,

유사한 시스템과 외부접점을 활용하는 경우도 많은 만큼,

한 금융회사에서 확인된 공격수법이나 취약점이

다른 금융회사에 대한 공격에도

활용될 가능성이 있습니다.

따라서 개별 금융회사의 침해사고를

해당 회사만의 문제로만 보지 않고,

금융권 전체가 선제적으로

공동 탐지하고 차단할 수 있도록
보다 긴밀하게 협력해 주시기 바랍니다.

사이버보안에서는 한 회사의 사고가
곧 금융권 전체의 경고가 되어야 합니다.

금융위원회, 금융감독원, 금융보안원 등
금융당국과 기관들도 금융권과 “원팀”으로
침해활동을 면밀히 모니터링하고,

새로운 공격징후가 포착되는 즉시
관련 정보를 신속하게 공유하는 등
추가적인 피해의 선제적 차단 등을 위해
민관합동 공동대응 체계를 더욱 공고히 하겠습니다.

나아가, 사이버 위협에는
금융과 비금융의 경계가 없는 만큼,
정부도 금융권뿐만 아니라
다양한 산업분야와 위협정보의 공유와 공조를 확대하고
과기부, 개보위, 경찰청 등 관계부처 간
공조체계를 한층 더 강화하여
침해위협에 범정부적으로 대응해 나가겠습니다.

다섯째, “AI공격은 AI로 방어하는” 보안체계 마련도 서둘러 주시기 바랍니다.

숨가쁘게 변화하는 AI 발전속도에 비추어,
새로운 패턴으로, 예상치 못한 취약점을 파고드는
해킹수법이 앞으로 빠르게 확산되고 있는 등
전세계적으로 보안전쟁의 패러다임이 전환되고 있습니다.

이에 AI 시대에는
더 치밀하고, 정교한 보안체계 구축이
절실한 상황입니다.

정부는 AI 보안체계 전환을 위해
망분리 규제 긴급 완화 시행 및 전면해제 검토 등
근본적인 제도개선을 추진중에 있습니다.

금융권에서도
“AI보안테스트” 등 정책에 적극 참여하는 한편,
제로트러스트 원칙에 기반한 보안체계 고도화 등
“AI 기반 보안체계” 전환에도 박차를 가해 주시기 바랍니다.

4 마무리 말씀

여러분, 금융은 무엇보다
‘신뢰’를 기반으로 하는 산업입니다.

오랜 시간 쌓아온 신뢰도
한 번의 보안사고로 흔들릴 수 있습니다.

이제 금융보안은
단순히 전산시스템을 안전하게 관리하는 것을 넘어,
국민의 금융정보와 자산을 보호하고
국민이 금융서비스를 안심하고 이용할 수 있도록 하는
금융산업의 신뢰와 안정성을 지탱하는 핵심 기반입니다.

보안은 비용이 아니라 투자입니다.
금융회사와 시스템의 근간인
‘신뢰’를 지키기 위한 기본 투자라는
근본적인 인식전환이 필요합니다.

디지털 금융이 발전하고
금융서비스 간 연결이 확대될수록
보안의 중요성은 더욱 커질 수밖에 없습니다.
이번 일련의 사고를
단순히 개별 사고를 수습하는 데 그치지 않고,

우리 금융권의 정보보안 체계를
한 단계 더 높이는 계기로 삼아야 합니다.

쏠금융권은 비상한 각오와
최고 수준의 경각심을 갖고,
정보보안 체계 전반을 원점에서 다시 살펴
보안의 기본부터 철저히 다져주시기 바랍니다.

아울러, 정부도

침해사고의 유형과 피해양상 등을 면밀히 분석하여

필요한 제도개선 과제를 적극 발굴하는 등

침해사고로 인한 국민 피해가 발생되지 않도록

금융권과 금융당국이 원팀이 되어

총력 대응해 나가겠습니다.

감사합니다.