금융위원회 보도자료 금융감독원

보도시점 2026.11.5.(목) 9:00 배포 2026.11.5.(목) 7:00

AI시대, 거세지는 침해위협에 맞서 全 금융권이 튼튼한 보안체계로 무장하도록 혁신적인 정책과제를 적극 추진하겠습니다.

-「AI시대 보안체계 혁신을 위한 全금융권 간담회」개최 -

- **全금융권**, 약 **580여개**사 대상 **외부접점·내부통제 전면 전수점검**
- **대형 금융회사**부터 **취약점 분석·평가 연 2회 이상** 의무화
- 다크웹 모니터링, AI를 통한 보이스피싱 차단 등 **2차 피해 적극 방지**
- **"AI 공격은 AI로 방어"** 위해 **망분리 규제 전면해제**, **新보안체계 본격 논의**

[개요]

'26.11.5.(목) **금융위원회**는 **이억원 위원장** 주재로 **금융감독원·금융보안원**과 은행·증권·보험 등 전통적 금융업권 및 가상자산·전자금융·온투업까지 포함한 **全 금융권 협회장**들과 함께 **「AI시대 보안체계 혁신을 위한 全 금융권 간담회」**를 개최하였다. 범정부적 공조 차원에서 **국조실, 과기부, 행안부, 개보위, 방미통위, 경찰청**, KISA도 참석하였다.

금번 회의는 갈수록 거세지는 AI 해킹 등 새로운 침해위협에 맞서 우리 금융권이 튼튼한 보안체계를 확립하기 위한 **다양한 실천과제**와 **제도개선** 사항 등을 논의하기 위해 마련되었다.

·**일시/장소 : '26.11.5.(목) 9:00** / 금융보안원 여의도 분원

· **참석 :** [금융위] **이억원 위원장**(주재), 디지털금융정책관 등
[금감원] 수석부원장, 디지털·IT부원장보 등
[금보원] 금융보안원장, 사이버대응본부장, 금융AI보안연구소장 등
[관계부처·기관] 국조실, 과기부, 행안부, 개보위, 방미통위, 경찰청, KISA
[협회·중앙회] **은행연, 생보협, 손보협, 금투협, 여전협, 저축은행중앙회, 신협·농협·수협·새마을금고 중앙회, 핀산협, DAXA, 온투협회** 협회장
[전문가] 민간 기술자문단

· 논의사항 : AI 시대 보안체계 혁신을 위한 대응방안

[금융권 침해사고 현황]

금융권 침해사고가 확인된 지난 9월 30일 이후 현재(11월 3일 기준)까지 **총 37개사***, **40건**의 침해사고가 신고되었다. 은행·보험·증권 등 전통적인 금융업권뿐 아니라, 가상자산업, 전자금융업, 온투업 등 **全 업권에서 침해사고가 신고**되었으며, 지난 10월 14일 全금융권 체크리스트 점검이 완료된 이후에는 **주로 중소규모 증권·보험사**나 **전자금융업, 온투업, 가상자산거래소 등의 침해사고**가 **많이 보고**되고 있다.

* [은행] 4개사, [금투] 5개사, [보험] 3개사, [저축은행] 5개사, [상호금융] 1개사, [여신] 2개사, [온투] 4개사, [전금] 10개사, [가상자산] 3개사

침해사고에 따른 정보유출 규모는 현재까지 **약 47.3만건**으로 파악되었다. 주로 임직원 정보나 고객 성명, 주민등록번호, 계좌번호 등 금융회사 영업 과정에서 수집한 정보들이 많으며, 계좌 비밀번호 등 **부정결제 우려가 있는 정보유출은 아직 확인되지 않았다.**

정부는 각 금융회사들이 고객 정보유출 사실 통지, 피해 발생시 배상 등 소비자 보호 조치 등에 만전을 기하도록 관리·감독하는 한편, **이상거래 모니터링 강화, 소비자 경보 발령·행동요령 발표(10월 6일) 등 2차 피해 방지**를 위한 대응도 긴밀히 취해 나가고 있다.

일부 소규모 가상자산거래소·전자금융업자·온투업자의 경우에는 회사가 관리하는 자금이 탈취되는 사고도 발생했다.

자금탈취 규모는 현재까지 **약 10억원 수준**으로 신고되었으며, 주로 가상자산 핫월렛, 소비성 포인트, 온투업 예치금 등 회사에서 고객자금을 통합 관리하는 계정 등에서 자금이체가 발생한 것으로, **개별 이용자의 자금손실이 아직 현실화되지는 않은 것으로 파악**되고 있다.

「전자금융거래법」에는 침해사고 등으로 고객 손해 발생시 **무과실 배상책임이 규정**되어 있고,「가상자산 이용자 보호법」에는 **보험가입·적립금 마련** 등 소비자 보호 조치가 규정되어 있는 만큼, 금융위원회·금융감독원은 이러한 제도적 장치 등을 바탕으로 **소비자 보호 조치가 면밀히 이루어지도록 지도·감독**하는 한편, 추가적인 자금탈취 사고가 발생하지 않도록 가상자산업권 등에 철저한 관리 조치를 주문*한 바 있다.

* '26.11.2.(월) 금융위·금감원·금보원, DAXA, 주요 가상자산사업자 등과 긴급점검 회의

[추진방안]

금일 회의에서는 금융권의 ①**보안관리상 허술한 점을 꼼꼼히 바로잡고**, ②**소비자 2차 피해가 없도록 방비를 든든**히 하며, ③**나아가 AI시대에 걸맞는 "新 보안체계"를 구축**하기 **대응방안**을 심도 있게 논의하였다.

첫째, 보안취약점에 대한 빈틈없는 점검과 제도개선에 즉시 착수한다.

① 全금융권 외부접점·내부통제 체계 전면 전수점검

은행·보험·증권 등 전통적 금융업 뿐 아니라, 전금업, 온투업 및「전자금융거래법」적용대상이 아닌 가상자산업권까지 포함한 全 금융업권 대상으로, 全 **IT자산**의 **외부접점**(API 등 포함)·**내부통제체계 운영실태**를 **신속하고 면밀히 전수 점검한다.**

구체적으로, **全 금융업권 약 580여개사** 금융회사·전금업자·가상자산사업자 등이 **전수점검 대상에 포함**되며, ▲홈페이지 등 대고객 서비스뿐 아니라, ▲직원관리, ▲내부업무, ▲제휴업무 등 **외부에서 접근가능한 모든 업무영역**에 대하여, ①인증·접근통제 시스템 전반, ②영업·관리목적 API, ③개발·테스트 및 임시운영 시스템 등 **최근 침해사고가 주로 발생한 시스템**과 그간 관리가 소홀했을 것으로 여겨지는 **주변부 시스템까지 포함해 폭넓고 빠짐없이 전수점검을 추진할 계획**이다.

금융회사 보안관리 전반의 내부통제 운영실태도 **점검**한다.
CEO·CISO·CIO 등 보고체계·역할분담·의사조율 등에 따라 상시적 보안관제, 중요한 보안인력·시설 투자 의사결정, 침해사고 발생시 신속·면밀한 대응 여부 등이 크게 영향받을 수 있는 만큼, ▲**각 주요 임원**(CEO·CISO·CIO 등)**의 역할·책임 전반**, ▲**외부접점 생성·운영·폐기** 과정에서의 **의사결정 절차**, ▲**IT자산 관리대장 운영 여부** 등에 대해 **촘촘히 점검**하고 **필요시 즉각적 보완을 요청할 방침**이다.

금융회사는 **외부접점 전수점검 과정**에서 고객·금융회사의 금전피해로 이어질 수 있거나 개인정보 유출이 우려되는 **중요한 취약점이 확인**되는 경우 **즉시 서비스를 중단하고 외부접근을 차단**하여야 한다.

즉시 보완이 어렵고 중요한 서비스 제공에 직접 관련된 경우에 한해, 면밀한 대체통제 시스템을 갖추고 **CEO의 승인**을 받은 **엄격한 조건 하**에 **서비스**를 **재개**할 수 있으며, 이 경우에도 취약점 보완, 장비 교체 등 근본적인 개선조치를 최대한 신속히 취해야 한다.

우선 금융회사가 자체점검을 실시하되, 점검상 문제 없는 경우라도 **점검내용, 방식, 판단사유 등**을 **상세히 적시**해야 하며, **점검내용이 부실**하다고 판단되거나, **중대한 취약점**이 발견된 경우에는 **금융감독원·금융보안원에서 직접 현장 점검**을 **실시**할 계획이다.

금융회사들이 금번 전수점검에 성실하게 임하도록 **전수점검 과정에서 발견**되는 **취약점**이나 **그간의 관리 부실사항**에 대해서는 즉각적·면밀한 보완조치를 전제로 **최대한 유연하게 처리**해 나갈 계획이다.

다만, **전수점검 이후에 침해사고**가 발생하는 경우에는 **그간의 점검이 제대로 이루어졌는지까지 꼼꼼히 따져 엄정히 책임을 묻도록 할 방침**이다.

관리대장에 등재되어 있는 시스템상 **외부접점 전수점검**은 최대한 신속히 추진하여 **11월 30일까지 마무리** 지을 계획이며, 관리대장에 등재되지 않은 **미등재 시스템**에 대한 **전수점검**과 CEO·CISO 등 **내부통제체계 전반에 대한 전수조사**도 조속히 추진하여 **12월 31일까지 마무리** 지을 방침이다.

아울러, 금번에 추진하는 전수점검 결과를 바탕으로 全금융권이 효과적인 보안 내부통제 시스템을 갖출 수 있도록 「**보안 내부통제 가이드라인**」을 **’27.1분기 중 마련·시행**할 계획이다.

② 금융권 공동 해킹 관제시스템 고도화

AI를 통한 침해시도가 빠르고 광범위하게 全금융권을 위협할 가능성이 제기되는 만큼, 각 **개별 금융회사**들이 각자 파악한 **침해시도 정황·내용** 등을 **최대한 신속**하게 全금융업권에 **전파**하는 시스템도 신속하게 구축한다.

※ 현재 금감원(FIRST)·금보원(FCTI) 관제시스템이 운영중이나, 금감원·금보원 차원에서 파악한 위협정보만 공유중

구체적으로, 유의미한 공격정보 탐지·공유능력을 갖춘 **대형 금융회사**는 자체 관제 관점에서 탐지한 ▲공격방식, ▲공격자 IP, ▲악용된 취약점, ▲악성코드 정보 등을 선제적으로 대응할 수 있도록 **통합관제시스템**(FIRST)을 **활용**해 **全 금융권에 신속히 전파**하고, 이를 공유받은 금융회사들은 자체적인 침해사고 대응, 취약점 보안 등 업무에 이를 적극 활용할 수 있다.

동 시스템 고도화 작업은 12월 중 시범운영을 거쳐, **'27.1분기 중에는 全 금융권이 전면적**으로 **활용**할 수 있도록 추진할 계획이다.

가상자산거래소 등 **「전자금융거래법」 미적용 업권**에 대한 **신속한 사고신고·상황전파 대응체계**도 정비한다.

현재 가상자산거래소 등 **일부 업권**은 **「전자금융거래법」이 적용되지 않아** 침해사고 발생시 「정보통신망법」에 따라 KISA에 사고신고를 하고 있으나, 최근의 해킹사고가 금융권 전반에 걸쳐 이루어지고 있으며, 가상자산사업자가 他업권 등과 밀접한 관계를 가지고 있는 만큼, 효과적 사고조사, 사례전파, 소비자 보호 조치 등을 위해서는 **금융감독원·금융보안원** 등**이 사고상황을 신속히 전파**받는 것이 **필수적**이다.

이에 동 업권에서 침해사고가 발생할 경우, KISA뿐 아니라 금융감독원·금융보안원에도 즉시 신고토록 **신고대응 가이드라인**을 **11월 중 마련**할 계획이다.

③ 금융권 취약점 분석·평가 제도 내실화

全금융권이 상시적으로, 보다 철저히, 빈틈없이 보안관리에 임하도록 **취약점 분석·평가 제도**를 촘촘하고 내실있게 **개편**한다.

현재 금융회사는 「전자금융거래법」 및 「전자금융감독규정」에 따라 외부기관(금보원, 민간 보안기업 등)으로부터 **연 1회 이상 전산시스템**의 **취약점**을 **점검**받아 금융당국에 제출하도록 의무화되어 있다.

다만, ▲최근 빠르게 변화하는 보안환경·침해위협 등을 고려할 때 **점검주기가 너무 길고**, ▲외부 점검범위가 명시되지 않아 **주변부 시스템까지 꼼꼼한 점검이 이루어지지 않으며**, ▲점검결과 **보완사항이 발견되더라도 이행할 수단이 마땅치 않은** 등 한계점이 지적되어 왔다.

앞으로는, ▲**대형 금융회사**부터 단계적으로 취약점 분석·평가 **점검주기**를 **연 1회 → 2회로 단축**하고, ▲전자금융거래와 직·간접적으로 관련된 **모든 외부접점**은 **취약점 분석·평가 대상**에 **포함**하도록 의무화할 계획이다. 아울러, ▲긴급한 취약점 점검 필요성이 있을 경우 **금융당국이 수시**로 **취약점 분석·평가를 요구**할 수 있도록 근거를 마련하고, ▲중요한 취약점을 장기간 방치한 경우 **금융당국이 시정명령**을 내리고, **미이행시 지속적인 이행강제금**을 부과하는 방안(「전자금융거래법」 개정안 旣발의)도 적극 추진할 계획이다.

금융회사의 상시적 보안관리 강화가 시급한 만큼 제도개선을 최대한 신속히 추진한다. ▲점검주기 단축, ▲全외부접점을 점검대상 포함, ▲수시평가 등 사항은 「**전자금융감독규정**」 **개정안**에 포함하여 **11월 중 규정변경 예고**를 **실시**할 계획이며, ▲이행강제금 제도는 旣 발의된 「전자금융거래법」 개정안이 연내 국회를 통과할 수 있도록 입법 지원에 만전을 기할 방침이다.

④ **중소형 금융회사 AI해킹 대비 지원 강화**

상대적으로 보안 전문인력과 예산이 부족해 급변하는 보안환경과 AI 침해위협에 충분히 대비하기 어려운 **중소형 금융회사**를 대상으로 **다각적인 보안강화 서비스를 지원**한다.

▲금융보안원에서 AI 등을 활용해 중소 금융회사의 **외부접점**과 **취약요인**을 **상시 탐색하**고 위험 **우선순위·조치방안**까지 원스톱으로 제공하는 「**원스톱 AI 방어서비스**」 **지원**, ▲금융회사의 보안역량에 맞게 **보안조치 내용을 구분·제시**하고, 외부노출자산 목록화·패치 적용기간 선정 등 **기본적인 내용을 손쉽게 적용**할 수 있도록 안내하는 「**맞춤형 보안 안내서**」 등을 지원한다. 아울러, 금융회사가 침해공격의 위험도를 직관적으로 알 수 있도록 **단계별 경보체계·행동요령** 등도 지원한다.

중소형 금융회사의 **보안 수요가** 많은 만큼, 금융보안원의 역량을 최대한 활용하여 **12월**부터 **순차적**으로 신속히 **추진**해 나갈 것이다.

둘째, 2차 피해 방지를 위한 든든한 방어체계를 마련한다.

① **다크웹 등 개인정보 유통 모니터링 및 차단**

금융권 침해사고로 유출된 소비자 정보가 **보이스피싱·명의도용** 등 각종 범죄로 **이어지지 않도록**, **불법유통 감시**부터 **피해차단**까지 대응체계를 강화한다.

다크웹·텔레그램 등 추적이 어려운 **온라인 채널**을 상시 모니터링하여, ▲**금융권 탈취정보 유통·거래 여부**, ▲금융회사 대상 **침해공격 모의정황**, ▲새로운 **악성코드와 보안 취약점 출현 여부** 등을 면밀히 모니터링한다. 탈취정보의 유통 정황이 포착되면 해당 금융회사에 즉시 통보하고, 실제 개인정보 유출·거래가 확인되면 해당 금융회사를 통해 **고객통지, 추가 피해 예방 안내, 피해 보상** 등 **필요한 조치**가 신속히 이루어지도록 할 계획이다.

개인정보가 불법 유통되는 국내 온라인 채널에 대해서는 관계부처와 긴밀히 협력하여 **사이트 차단·폐쇄, 범죄자 검거** 등 가용한 모든 수단을 동원해 강력히 대응할 계획이다.

② 보이스피싱 탐지·대응체계 고도화(ASAP 2단계)

AI를 활용해 범죄계좌와 의심거래를 조기에 포착내고, 금융회사 간 정보 공유를 확대하는 등 **보이스피싱 공동 대응체계**를 한층 강화한다.

유출된 개인정보가 범죄에 악용되면 실제 금융거래나 기관의 안내로 오인하기 쉬운 정교한 사기가 늘어날 수 있다. 이에 지난해 10월 출범한 금융권 공동 보이스피싱 정보공유·분석 플랫폼인「ASAP*」의 AI의 분석기능을 강화하여 **범죄계좌**를 **보다 신속하게 탐지·동결**하는 체계를 구축할 계획이다.

* ASAP : AI-based anti-phishing Sharing & Analysis Platform

구체적으로, 금융회사가 범죄여부가 의심되는 거래를 ASAP에 질의하면, AI를 활용해 **해당 거래가 보이스피싱에 연루되었을 가능성**을 분석해 점수(0~100점)로 제시하는 **AI 기반 「의심거래 판단지수**("피싱지수")」를 **11월부터 시범 도입**한다.

금융회사는 이를 통해 범죄가 의심되는 **거래의 위험도를 보다 빠르고 정확하게 판단**하여 지급정지 조치 등을 취함으로써, **효과적인 범죄 차단과 소비자 보호**를 해 나갈 수 있을 것으로 기대된다. 특히 그간 인력·자원 등의 한계로 자체 보이스피싱 탐지모델을 적극적으로 개발하기 어려웠던 상호금융, 저축은행 등 **중소형 금융사의 탐지역량이 제고**되어 효과적인 소비자 보호가 가능할 것으로 기대된다.

또한 **대포계좌와 신종스캠 등 새로운 범죄수법**까지 신속하게 탐지·차단할 수 있도록 다양한 시나리오를 반영해 공동 탐지룰도 추가해 나간다. 지난 6월 **자금 흐름과정의 이상징후, 피해과정에서 보이는 특징 등을 중심**으로 **공동탐지룰 추가안**을 마련하였고, 업권별 시뮬레이션 이후 최종안을 확정하였다. 이를 **은행권 및 제2금융권까지 적용**하는 동시에 **12월까지 ASAP에 편입**함으로써 **진화하는 범죄에 보다 실효적으로 대응**해나갈 예정이다.

③ 보이스피싱 무과실책임 법제화

보이스피싱 피해자를 두텁게 보호하고, 금융회사의 예방 노력을 높이기 위해 범죄 피해 일정 부분을 금융회사가 배상토록 **무과실책임 법제화**도 추진한다.

정보유출 등에 따른 보이스피싱 등 2차 피해 우려가 커지고 있는 상황에서 **보이스피싱 피해금의 일정부분**을 **금융회사가 보상**하는 무과실책임 제도 도입의 목소리가 커지고 있다. 이는 고도로 발전하는 범죄수법으로 **피해자 개인의 주의만으로는 범죄예방이 곤란**한 상황에서, **의심거래 탐지·계좌 지급정지** 등 금융사들에 **법·제도적으로 부여된 다양한 법적조치**를 통해 **금융사 스스로가 책임을 다할 유인구조**를 마련하기 위한 목적이다.

이에 금융위원회는 **우선 금융회사부터** 보이스피싱 피해자의 **피해금의 일정부분을 보상**해줄 수 있도록 **旣발의된 「통신사기피해환급법」 개정안***의 신속한 입법을 **적극 지원**할 계획이다. 아울러 금융회사의 과도한 부담으로 이어지지 않도록 하위규정 등을 통해 **보상대상, 한도, 면책범위 등 구체적인 적용요건**을 정교하게 설계해 나갈 예정이다.

*「통신사기피해환급법」 개정안(강준현·조인철 의원안) 정무위 계류중('26.3월~)

또한 통신수단을 매개로 이뤄지는 보이스피싱 범죄 특성, 피해자에 대한 보다 두터운 보호가 필요하다는 점 등을 고려할 때 **금융회사 뿐만 아니라 통신사 등에 대한 책임 부여**도 필요하다는 의견이 있는만큼, 이에 대해서도 국조실·과기부 등 **관계부처**와 **정부 내** 공론화를 신속히 추진해 나갈 계획이다.

셋째, “AI 공격은 AI로 방어하는” AI기반 新보안체계를 조속히 구축한다.

① 망분리 규제 전면해제 TF 구성

AI 보안위협이 현실화된 상황에서 망분리 규제를 뛰어넘어 “**AI공격은 AI로 방어하는 新보안체계**” 마련 논의를 본격화한다.

AI를 활용한 해킹 위협에 대응하려면 내부망과 외부망을 분리하는 기존 방식에서 나아가, AI로 공격을 탐지하고 차단하는 보안역량을 갖춰야 한다. 이에 「**망분리 규제 전면해제 TF**」를 본격 가동하여 금융권의 AI 활용을 뒷받침하면서도 보안 수준을 높일 수 있는 방안을 마련할 계획이다.

TF에는 정부, 유관기관, 민간전문가, 全금융권 담당임원 등 각계 전문가·이해관계자 등으로 구성할 계획이며, ▲**데이터의 중요도**에 따른 **관리·보호 체계**, ▲모든 접근을 지속적으로 확인·검증하는 **'제로트러스트' 등 대체 보안수단**, ▲**CEO·이사회·CISO의 역할과 책임**, ▲침해사고 발생 시에도 핵심 서비스를 유지하기 위한 **업무연속성 확보방안** 등을 심도 있게 논의하여 **구체적인 방안을 조속히 마련**할 계획이다.

② 보안목적 AI 테스트 상시화 및 혁신금융서비스 확대

금융회사가 보안강화에 **AI**를 상시 활용할 수 있도록 **제도를 정비**하고, **혁신금융서비스** 통한 망분리 규제 완화도 **일관**되게 **추진**한다.

현재, 비조치의견서를 통한 긴급조치 차원에서 진행 중인 **보안목적 AI·SaaS 활용**을 위한 망분리 규제 완화 조치를 **상시 제도화**한다. 이를 통해 보다 많은 금융회사들이 상시적으로 AI를 적극적으로 활용해 보안 취약점 탐색·보완과 새로운 보안서비스를 적극 활용할 수 있을 것으로 기대된다. 다만, 망분리 규제 예외 허용이 또 다른 보안 취약요인으로 작용하지 않도록 외부접점 관리, 인증·접근통제 관리, 보안사고·장애대응 등 **대체통제 수단을 철저히 마련**하도록 할 계획이다.

아울러, 다양하고 새로운 IT서비스에 대한 **망분리 규제 완화**도 **혁신금융서비스 등**을 통해 **일관되게 추진**한다. 이미 **제도화된 업무용** SaaS나 **생성형 AI 서비스** 이외에도 **블록체인** 등 **다양한 IT서비스**가 혁신금융서비스 심사를 통해 **망분리 규제 예외**로 **인정**될 수 있도록 해 나갈 계획이다.

③「디지털금융 안전법」 추진

AI 해킹위협 현실화, 디지털 혁신 가속화 등 급변하는 보안환경에 맞춰 **全금융권과 유관업종** 등에 **치밀한 전산보안 규율**이 확립될 수 있도록 **「디지털금융 안전법」** 마련도 추진한다.

AI 해킹위협과 디지털 혁신으로 금융서비스의 연결구조가 복잡해지는 만큼, 금융회사뿐 아니라 **고객정보와 금융거래**에 영향을 미치는 관련 **업종**까지 **보안관리 체계**를 촘촘히 갖출 필요가 있다.

이에, **가상자산사업자, 보험대리점(GA)** 등 **대량의 고객정보**를 보유하거나, 침해사고 발생 시 고객의 **직접적 자산손실 우려**가 큰 업종 등에 대해 현 **「전자금융거래법」 수준의 보안규율**을 **적용**하는 방안을 추진한다. 또한, **클라우드 사업자, 플랫폼** 등 금융회사는 아니나, **▲다수 금융회사와 연계**되고, ▲다양한 업무 위수탁 관계를 통해 다량의 정보를 처리하거나, ▲침해사고 시 파급영향 등이 있는 **제3자**에 대한 규율체계 마련을 검토한다.

아울러, 금융회사 스스로 상시적으로 철저히 보안관리에 임할 수 있도록 CEO 책임성·이사회 구성·현업부서 역할 등 보안 거버넌스와 내부통제 차원의 규율도 검토해 나갈 계획이다.

「디지털금융 안전법」은 금융업권, 관계기관 등 여러 의견수렴 등을 거쳐 방안을 마련하고 '27.1분기 중으로 법안 마련을 추진한다.

이억원 금융위원장은 "고객의 정보와 재산을 지키지 못하는 금융회사는 이미 그 **존재가치를 잃은 것**"이라고 강조하며, "하루가 다르게 진화하는 보안위협에 맞서 금융의 생명과도 같은 **국민의 정보와 재산을 지켜내는데 그 어떠한 인적·물적 투자도 아껴서는 안 된다**."고 하였다.

나아가, "**全 금융권 CEO분**들은 절체절명의 위기상황임을 명확히 인식하고 전사적인 **비상대응반을 즉시 구성**하여 정부에서 준비한 전수점검 계획과 제도개선 과제에 맞추어 **긴밀한 상황대응**과 **튼튼한 보안체계 마련**에 **사력을 다해주길** 바란다."며 당부하였다.

아울러, “최근 금융권에서 잇따라 발생한 침해사고는 우리 **금융시스템의 보안체계 전반**을 **근본적으로 전환**해야 한다는 **엄중한 경고**”라고 강조하며, “**작은 보안 취약점 하나**가 **금융회사 전체**는 물론, **금융시스템의 신뢰를 훼손할** 수 있는 상황”이라고 하였다. 마지막으로, “기존의 보안관리 방식과 관행에서 벗어나 **보안체계를 전면적으로 쇄신**해야 할 때”라고 하며, “全 금융권 CEO와 관계자분들은 국민 여러분이 맡겨주신 **정보와 재산**을 **목숨 걸고 지켜낸다는 각오**로 우리 금융권의 신뢰를 회복해야 한다”고 당부하였다.

※ [별첨] 1. 금융위원장 모두말씀
2. 全금융권 보안체계 혁신방안

담당 부서 <총괄>	금융위원회 금융안전과	책임자	과 장	김태훈	(02-2100-2970)
		담당자	사무관	김영준	(02-2100-2573)
			사무관	이다행	(02-2100-2975)
			사무관	김해은	(02-2100-2979)
			사무관	최서린	(02-2100-2974)
			주무관	김민균	(02-2100-2976)
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)

대한민국 정책브리핑
대체불가 대한민국
OPEN 출처표시 공공누리 공공저작물 자유이용허락