November 2026

NEWSLETTER

디지털금융팀 | Digital Finance Team

CONTACT



변호사 **권진홍**
T: 02.772.4373
E: jinhong.kwon@leeko.com



변호사 **신상록**
T: 02.772.5947
E: sangrok.shin@leeko.com



변호사 **한서희**
T: 02.6386.6297
E: suhhee.han@leeko.com



변호사 **주성환**
T: 02.6386.6345
E: seonghwan.ju@leeko.com



수석전문위원 **안병남**
T: 02.772.4835
E: byungnam.ahn@leeko.com

AI 대응 全금융권 보안체계 혁신방안의 주요내용과 시사점

금융위원회는 2026. 11. 5. 이억원 위원장 주재로 금융감독원·금융보안원과 은행·증권·보험 등 전통적 금융업권 및 가상자산·전자금융·온투업까지 포함한 全금융권 협회장들과 함께 「AI 시대 보안체계 혁신을 위한 全금융권 간담회」를 개최하고, 「AI 시대 침해위협에 대응하기 위한 全금융권 보안체계 혁신방안」(**혁신방안**)을 발표하였습니다. 위 간담회에는 범정부적 공조 차원에서 국무조정실, 과학기술정보통신부, 행정안전부, 개인정보보호위원회, 방송미디어통신위원회, 경찰청, 인터넷진흥원(KISA)도 참석하였습니다.

금융권 침해사고가 확인된 2026. 9. 30. 이후 2026. 11. 3.까지 총 37개사에서 40건의 침해사고가 신고되었으며, 약 47.3만 건의 정보유출과 약 10억 원 수준의 자금탈취가 신고되는 등 전 업권에서 침해사고가 발생하고 있습니다. 금번 혁신방안은 AI를 활용한 해킹 등 새로운 유형의 침해위협이 심화되는 상황에 대응하여, 1) 금융권의 보안관리상 허술한 점을 꼼꼼히 바로잡고, 2) 소비자 2차 피해가 없도록 방비를 든든히 하며, 3) 나아가 AI시대에 걸맞는 "新 보안체계"를 구축하기 위한 대응방안을 담고 있습니다.

혁신방안의 주요 내용은 다음과 같습니다.

대응방향	주요과제
보안취약점에 대한 빈틈없는 점검	① 全금융권 외부접점 · 내부통제 체계 전수점검 ② 금융권 공동 해킹 관제시스템 고도화 ③ 금융권 취약점 분석 · 평가 내실화 ④ 중소형 금융회사 AI 해킹대비 지원 강화
2차 피해 방지를 위한 든든한 방어체계 마련	① 다크웹 등 개인정보 유통 모니터링 및 차단 ② 보이스피싱 탐지 · 대응체계 고도화 (ASAP 2단계) ③ 보이스피싱 무과실책임 법제화
AI 기반, Post 망분리 新 보안체계 구축	① 망분리 규제 전면해제 TF 구성 ② 보안목적 AI 테스트 상시화 및 혁신금융서비스 활성화 ③ 「디지털금융 안전법」 추진

이하에서는 그 구체적인 내용을 살펴보겠습니다.

1. 최근 해킹사고 특성 및 문제점

혁신방안은 침해사고에서 나타난 공격양상이 보안관리가 철저한 핵심 시스템이 아니라 인력 등의 한계로 관리가 소홀한 부분을 집중 공략하거나, AI 활용의 보편화로 인해 금융 · 공공 · IT 등 다양한 분야에서 광범위한 공격시도가 발생하고, 고위험 취약점 발견도 증가하였다는 점을 그 특성으로 지적하였습니다.

아울러 이와 같은 침해사고에 따라 유출된 정보는 다크웹·텔레그램 등 음성적 유통경로에서 거래되면서 다양한 금융범죄(보이스피싱 · 신종피싱 등)에 악용될 우려가 있으며, AI로 인해 금융범죄가 점차 지능화·정교화됨에 따라 기존의 이상거래 탐지 체계만으로는 신속한 탐지 · 차단이 역부족한 상황으로, 소비자 2차 피해로 이어질 가능성도 확대되고 있음도 강조하였습니다. 반면 금융권은 망분리 규제 중심의 보안체계로 인해 보안체계 강화에 AI 등 다양한 기술 활용이 어려움이 있고, 능동적·적극적 대응체계 구축에 한계가 있다고 지적하였습니다.

이에 혁신방안은 금융분야는 신뢰와 안정이 중요한 만큼, "선제적 보안체계"와 "소비자 보호"를 위한 대책 마련이 시급한 시점이라고 보았습니다.

2. 혁신방안의 주요 내용

1) 보안취약점에 대한 빈틈없는 점검

- **全금융권 외부접점 · 내부통제 체계 전수점검**

  금융당국은 전 금융회사와 전자금융업자, 가상자산사업자 등 약 580사를 대상으로 全 IT자산(API 포함)의 외부접점 관리와 내부통제 운영실태에 대한 전수점검 및 신속 보완조치를 실시할 예정입니다. 구체적으로, 업무는 홈페이지 등 대고객서비스뿐 아니라, 직원관리, 내부업무, 제휴업무 등 외부에서 접근가능한 모든 업무영역을 망라하며, 시스템 측면에서는 영업·관리목적 API, 인증 · 접근통제 등 시스템 전반을 점검합니다. 내부통제의 경우 ① 내규 유무, ② 내부통제 작동여부(결재, 승인, 보고 등), ③ IT자산·서비스 관리대장 운영 여부, ④ 취약점 분석 · 평가 및 보안관제 여부, ⑤ CEO · CISO · CIO 역할 등 외부접점 생성·운영·폐기 관련한 내부통제 전반을 점검합니다.

  점검은 우선 대상회사가 자체점검을 실시하되, 점검상 문제가 없는 경우라도 조사방법, 판단사유 등을 상세하게 적시하고, 관리대장 목록을 철저히 재점검후 목록에 빠졌던 서비스도 등재후 빠짐없이 점검하여야 합니다. 점검 내용이 부실하거나 중요한 취약점이 발견되는 경우에는 금융감독원, 금융보안원 등이 직접 현장점검을 실시할 예정입니다.

  대상회사는 서비스 및 업무에 불필요한 외부연결은 즉시 차단하여야 하고, 고객·금융회사의 금전피해, 개인정보 유출과 직결되는 취약점은 보완 전까지 즉시 서비스를 중단하여야 합니다. 다만 즉시 보완이 어렵고 중요한 서비스인 경우에 한해 CEO승인·책임 하에 대체통제 적용후 서비스를 재개할 수 있습니다.

  금융당국은 이와 같은 일련의 전수점검 과정에서 확인된 관리부실은 즉시보완 전제하에 최대한 유연하게 처리할 예정이나, 이후 발생하는 사고는 엄정히 책임을 추궁한다는 입장입니다.

  관리대장에 등재된 외부접점 전수조사 · 보완은 2026년 11월 말까지, 전체 외부접점 점검 · 보완 및 내부통제체계 전수조사는 12월 말까지 진행됩니다. 금융당국은 점검결과를 분석하여 2027년 1분기까지 보안 내부통제 가이드라인을 마련할 방침이며, 외부접점 및 내부통제체계 전수조사와 관련한 세부항목, 점검방식 등 구체적인 내용은 별도로 안내할 예정입니다.

- **금융권 공동 해킹 관제시스템 고도화**

  빠르고 광범위한 AI 침해위협에 대응하기 위해서는 공격IP 등 신속한 정보공유가 필수적입니다. 그런데 현재 통합관제시스템(FIRST, 금융감독원), 위협정보공유시스템(FCTI, 금융보안원)이 운영 중이기는 하나, 금융감독원·금융보안원 차원에서 파악한 위협정보만 공유되고 있을 뿐 개별 금융사가 파악한 정보는 공유되고 있지 않습니다. 이에 혁신방안은 개별 금융회사가 탐지한 해킹시도·공격 의심정보를 全금융권 공유할 방침입니다. 구체적으로, 유의미한 공격정보 공유가 가능한 대형 금융회사(예: 총자산 10조원 & 상시 종업원 1천 명 이상 금융회사)가 수집한

1) 해킹, DDoS 등 공격방법, 2) 공격대상, 3) IP 등 공격 경로, 4) 악용된 취약점, 5) 악성코드 종류 등을 금융감독원 통합관제시스템(FIRST)을 통해 全금융권에 공유할 예정입니다. 이러한 공유체계는 2026년 12월에 시범운영을 거쳐 2027년부터 전면 운영될 예정입니다.

한편 가상자산사업자 등 「전자금융거래법」이 적용되지 않는 업권은 침해사고 신고가 인터넷진흥원(KISA)에 이루어져 금융권간 빠른 정보공유에 한계가 있는 실정입니다. 이에 「전자금융거래법」이 적용되지 않는 가상자산사업자, 보험GA 등에 대하여도 침해사고 인지 즉시 KISA 외에 금융감독원 · 금융보안원에 인지시점, 사고내용, 예상 피해유형·규모 등을 통보하도록 하는 신속한 사고신고체계를 구축하는 방안이 추진됩니다. 금융당국은 이를 위해 2026년 11월 「전자금융거래법」이 적용되지 않는 금융회사를 대상으로 한 가이드라인을 마련할 예정입니다.

- **금융권 취약점 분석·평가 내실화**

종래 금융회사는 「전자금융거래법」 제21조의3에 따라 외부기관(금융보안원, 민간 보안기업 등)으로부터 연 1회 이상 취약점을 점검받아 결과를 금융당국에 제출하여 왔으나, 이에 대하여 1) 침해위협 강화속도에 비해 점검주기가 길고, 2) 의무점검범위가 명시되지 않아 주변부 시스템 등 꼼꼼한 점검에 한계가 있으며 3) 보완조치 미이행시에도 시정수단이 마땅치 않다는 한계점이 지적되어 왔습니다.

이에 혁신방안은 1) 대형 금융회사(총자산 2조원 & 종업원 3백명 이상)부터 점검주기를 연 1회에서 2회로 단축하고, 2028년 이후에는 중소형사까지 포함한 全금융권을 대상으로 점검주기를 단축하며 2) 전자금융거래와 직·간접적으로 관련된 모든 외부접점은 취약점 분석·평가 대상에 포함토록 의무화하고 3) 긴급한 취약점을 점검할 필요가 있을 때 금융당국이 수시로 취약점 분석·평가를 요구할 수 있도록 「전자금융감독규정」을 개정할 계획입니다. 4) 나아가 중요한 보안취약점을 장기간 방치시 금융당국이 시정명령을 내리고, 미이행시 지속적인 이행강제금을 부과하는 내용의 「전자금융거래법」 개정안이 법안심사소위원회에 계류중이며 연내 통과를 추진하고 있습니다.

- **중소형 금융회사 AI해킹대비 지원 강화**

중소형 금융회사는 급변하는 AI 보안위협에 대응하여 보안 전문인력·예산 등 충분한 대응여력을 확보하기 어려운 측면이 있습니다. 이에 금융보안원에서 중소금융사의 외부접점과 취약요인까지 상시 탐색하고, 위험 우선순위·조치방안까지 원스톱으로 제공하는 원스톱 AI방어서비스를 지원합니다. 또한 보안역량별 맞춤형 보안안내서를 마련하여 금융회사 보안역량에 맞게 보안조치 내용을 구분·제시하고, 우선순위가 높은 조치부터 이행할 수 있도록 안내할 예정입니다. 특히 외부노출자산 목록화, 패치 적용기한 설정 등 기본적인 내용을 손쉽게 적용할 수 있도록 실행계획(액션툴킷)도 제공할 방침입니다.

또한 금융당국은 보안교육·세미나·자문 등 '찾아가는' 교육 프로그램도 마련·시행할 계획이며, 공격 위험도에 따른 경보체계 및 단계별 행동요령을 마련하고, 각 업권 협회와 협력하여 AI 기반 공동 보안관제 구축도 지원할 방침입니다.

2) 2차 피해 방지를 위한 든든한 방어체계 마련

- **다크웹 등 개인정보 유통 모니터링 및 차단**

현재 침해사고로 유출된 개인정보 등이 다크웹 등 경로로 유통될 가능성이 제기되고 있으나, 금융사 자체적으로 적시에 포착하여 대응하기는 쉽지 않은 상황입니다. 이에 금융보안원이 다크웹 · 텔레그램 등 각종 음성적 채널에서 1) 금융권 탈취정보 유통 · 거래 여부, 2) 금융회사 대상 침해공격 모의정황, 3) 신규 악성코드 · 취약점 출현상황 등을 상시 모니터링할 계획입니다. 또한 금융회사 탈취정보 유통정황이 확인되면 해당 금융회사에 즉시 통보하고 실제 유출 · 거래사실 확인시 당국신고 · 고객통보 · 보상 등을 즉각조치하며, 금융사 대상 침해공격 정황 · 신규 악성코드 및 취약점 등 정보는 통합 관제시스템(FIRST) 등을 통해 즉각 전파하고 보안관제에 활용할 방침입니다.

또한 개인정보가 불법 유통되는 국내 온라인채널 등이 확인되는 경우 과학기술정보통신부, 방송미디어통신위원회, 경찰 등 관계부처 협조 하에 사이트 폐쇄 등을 검토할 예정입니다.

- **보이스피싱 탐지·대응체계 고도화(ASAP 2단계)**

AI기술과 유출데이터 등으로 빠르게 진화하는 보이스피싱 범죄를 효과적으로 차단하기 위해서는 신속한 정보공유·탐지 시스템이 필요합니다. 보이스피싱 정보공유·분석 AI 플랫폼(AI-based anti-phishing Sharing & Analysis Platform, **ASAP**)은 출범 후 2026. 9.까지 54.5만 건 정보공유, 9,045건 지급정지 및 752.6억 원 피해예방을 하는 등 실질적 성과를 거두고 있으나, AI 기반 탐지시스템 구축, 최신 범죄수법 반영 등 추가과제를 추진할 필요가 있습니다.

금융당국은 금융회사가 범죄여부가 의심되는 거래를 ASAP에 질의하면, ASAP은 금융보안원-인터넷은행 3社가 개발한 보이스피싱 탐지 AI 공동모델을 바탕으로 위험도를 판단해 답변하는 AI 기반 의심거래 판단지수(**피싱지수**)를 2026. 11.부터 시범 운영합니다. 금융회사는 위 답변결과와 자체 FDS 판단내용, 고객확인 등을 통해 보다 효과적으로 범죄계좌 지급정지·자금환수가 가능하게 되며, 특히 보이스피싱 탐지역량이 상대적으로 낮은 중소형사의 역량보완이 기대됩니다.

또한 최신수법을 반영해 대포계좌·신종피싱 FDS 공동탐지룰 시나리오를 51개에서 66개로 확대하고, 그 공유범위를 은행권에서 제2금융권까지 확대하며, 경찰수사중 획득한 신종피싱 의심정보를 ASAP을 통해 全금융권에 공유하는 방안도 협의·추진됩니다. ASAP 공유정보는 기존 9종 90항목에서 공유정보 외에 보이스피싱 탐지에 중요한 역할을 하는 카드 명의인 정보, 부정결제 가맹점 정보, 다크웹 유출카드 정보 등 다양한 정보를 추가한 14종 137개 항목으로 확대되고, 현재 141개 참여기관 중 48사만 활용하고 있는 API 실시간 연동체계를 제2금융권·우체국 등 전 금융사에 확대할 계획입니다.

- **보이스피싱 무과실책임 법제화**

금융당국은 정보유출 등에 따른 보이스피싱 범죄로 2차피해가 발생한 경우, 금융회사가 일정부분 피해금을 보상하는 보이스피싱 무과실책임 법제화를 추진합니다. 이는 고도로 발전하는 범죄수법상 피해자 주의책임으로 범죄예방이 곤란한 상황에서, 의심거래 탐지·계좌 지급정지 등 법적 책무와 ASAP 등 의심정보 분석 인프라를 제공받은 금융회사가 스스로 책임을 다할 유인을 부여하기 위함입니다.

구체적으로, 2026. 3.부터 국회 정무위원회에 계류중인 「통신사기 피해환급법」 개정안(강준현 · 조인철 의원안)의 신속한 국회 통과를 추진합니다. 동 개정안은 금융회사부터 보이스피싱 피해금을 일정부분 책임지도록 1) 송금계좌·수취계좌 금융회사가 1:1로 보상금을 분담하고, 2)1~5천만원 범위 내 보상한도를 설정하며(대통령령으로 위임) 3) 피해자에 충분히 범죄위험 알린 경우 등에는 금융회사에 면책을 부여하는 등의 내용을 골자로 하고 있습니다.

또한 금융업권 등은 동 법안 논의 과정에서 보이스피싱 범죄가 통신수단을 매개로 이루어지며 피해자에 대한 보다 두터운 보호가 필요한 점 등을 근거로 통신사에 대한 책임성 강화 논의도 필요하다는 입장을 보이고 있는 만큼, 통신사 책임성 강화 등과 관련하여 정부차원 공론화를 추진할 방침입니다.

3) AI 기반, Post 망분리 新보안체계 구축

- **망분리 규제 전면해제 TF 구성**

AI를 활용한 해킹위협이 현실로 다가온 시점에서 "AI공격은 AI로 방어하는" 보안체계를 확립하기 위한 구체적 실천과제를 논의할 필요가 있습니다. 이에 금융당국은 금융권 망분리 규제 단계적 전면해제와, 이를 대체하기 위한 AI 기반 新보안체계 논의를 위한 망분리 규제 전면해제 TF 본격적으로 가동합니다.

TF에는 금융위원회, 과학기술정보통신부, 국가정보원, 개인정보보호위원회 등 정부부처와 금융감독원, 금융보안원, 금융결제원, 신용정보원 등 유관기관, AI·보안·정보보호·법조계 전문가 등 민간 전문가, 全금융권 협회 및 주요 금융회사 담당임원 등이 참가합니다.

TF에서는 1) 고도의 AI·보안역량 갖춘 금융회사를 선정하여 엄격한 대체통제하에 망분리규제를 해제하는 등의 망분리규제 전면해제 추진절차·평가기준과 2) 데이터 관리(N2SF 등), 제로트러스트 원칙, CEO-이사회-CISO-

현업부서의 각 책임성을 포함한 보안 내부통제, 침해사고 발생시 대응체계 등 AI 기반 新보안체계 구체적인 내용·적용방식을 논의할 예정입니다.

- **보안목적 AI 테스트 상시화 및 혁신금융서비스 활성화**

  2026. 6. 실시된 보안목적 AI 망분리 규제 긴급 완화 1차 테스트에서는 AI를 통한 내부 소스코드 점검 결과 상당수 금융회사에서 접근·인증통제 미흡, 공격코드 주입 등의 취약점이 다수 발견되었으며, 이는 최근 금융권 침해사고 주요원인인 인증·접근통제 API 취약점 해결에 상당히 효과적인 것으로 평가되었습니다. 또한 혁신금융서비스를 활용한 업무용 SaaS, 생성형AI 활용 등 망분리규제 완화 정책도 일관되게 이어갈 필요성이 있습니다.

  이에 현재 비조치의견서를 통해 허용되던 보안목적 AI 테스트와 SaaS 서비스 활용에 대한 망분리 규제의 예외를 「전자금융감독규정」 개정을 통해 상시 제도화할 계획이며, 외부접점 관리, 인증·접근통제, 보안사고·장애대응 등 대체통제를 적용할 예정입니다. 다만 긴급한 수요 감안하여 2 · 3차 망분리규제 긴급완화조치는 예정대로 추진되며, 이후의 보안목적 AI 활용 수요는 상시 제도화를 통해 해소할 방침입니다. 아울러 엄격한 대체통제를 전제로 생성형 AI · 블록체인 등 다양한 IT기술을 대상으로 혁신금융서비스를 통한 망분리 규제완화를 일관되게 추진할 예정입니다.

- **「디지털금융 안전법」 추진**

  금융당국은 AI 해킹위협 현실화, 가상자산 등 새로운 업종 활성화, 디지털금융·클라우드 환경 보편화 등에 맞춰 보안규제 전반을 재정비하고, 全금융권과 유관업종 등에 걸쳐 치밀한 전산보안 규율이 확립되도록 「디지털금융 안전법」 마련을 추진합니다. 「디지털금융 안전법」에서는 1) 가상자산사업자, 보험GA, 대부업 등 직접 전자금융거래를 수행하지는 않으나 많은 금융·고객정보를 보유하고 침해사고시 고객의 직접적 자산손실 가능성 있는 업종 등에 대해서 현 전자금융거래법에 준하는 수준의 보안규율 등을 적용할 예정입니다. 2) 또한 클라우드 사업자, 플랫폼 등 금융회사는 아니나 다수 금융회사와 연계되고 다양한 업무 위수탁 관계를 통해 다량의 정보처리, 침해사고시 파급영향 등 있는 경우에는 침해사고 예방·신속한 피해복구 등 차원의 다양한 규율 적용을 검토할 방침입니다. 3) 나아가 금융회사 스스로·상시적으로·철저히 보안관리에 임할 수 있도록 CEO 책임성·이사회 구성·현업부서 역할 등 보안 거버넌스·내부통제 차원의 규율도 검토·반영할 예정입니다.

3. 시사점

이번 혁신방안은 1) 보안취약점에 대한 전방위적 점검체계 확립, 2) 2차 피해 예방을 위한 대응체계 강화, 3) AI 기반 Post 망분리 보안체계로의 전환이라는 세 가지 기본방향에 따라 총 10개의 세부 주요과제를 제시하였습니다. 단기적으로는 금융권 전반에 걸친 보안관리의 사각지대를 해소하고 금융소비자의 피해를 예방하는 데 중점을 두는 한편, 중장기적으로는 기존 망분리 규제를 전면적으로 해제하고 AI 기반의 새로운 보안 패러다임을 구축하겠다는 정책적 방향을 구체화하였다는 점에서 주목할 필요가 있습니다.

먼저, 보안취약점 점검과 관련하여 금융회사는 2026년 11월 말까지 관리대장에 등재된 외부접점을, 같은 해 12월 말까지는 전체 외부접점 및 내부통제체계에 대한 전수점검을 완료하여야 합니다. 이와 별도로 취약점 분석·평가 주기가 연 2회로 단축되는 한편 수시점검과 함께 이행강제금 제도가 추진되고 있으므로, 향후 보안점검은 상시적인 관리의무로 정착할 것으로 예상됩니다. 이에 금융회사는 IT자산 및 외부접점 관리 현황을 전반적으로 재점검하고, 자체점검 과정에서 적용한 점검방법과 취약점에 대한 판단 근거 및 후속 조치 내역을 구체적으로 기록·보존할 필요가 있습니다. 또한 대형 금융회사는 자체적으로 탐지한 공격정보를 공동 관제시스템에 공유할 수 있는 체계를 마련하여야 하며, 가상자산사업자 등 「전자금융거래법」의 적용을 받지 않는 업권은 금융감독원 및 금융보안원에 대한 침해사고 신고·통보 절차를 정비할 필요가 있습니다. 아울러 중소형 금융회사의 경우 금융보안원이 제공하는 원스톱 AI방어서비스 등 외부 지원체계를 적극 활용하여 보안 대응역량을 보완하는 방안도 고려할 수 있습니다.

다음으로, 소비자 2차 피해 방지를 위해서는 개인정보 등 탈취정보의 유통에 따른 후속 피해에 대응할 수 있는 체계적인 절차를 마련하는 것이 중요합니다. 금융회사는 금융보안원으로부터 탈취정보의 유통 정황을 통보받는 상황에 대비하여 고객 통지, 피해 확산 방지 및 보상 등 단계별 대응절차를 사전에 정비할 필요가 있습니다. 또한 피싱지수 도입, 공동탐지룰

확대, 공유정보 범위 확대 및 전 금융회사 API 실시간 연동 등 ASAP 고도화에 대응하여 자체 이상거래탐지시스템(FDS)과의 연계 및 활용방안을 마련하여야 합니다. 특히 보이스피싱 피해에 대한 무과실책임 제도가 법제화될 경우 금융회사는 과실이나 귀책사유의 유무와 관계없이 피해금의 일정 부분을 부담하게 될 수 있으므로, 범죄위험 사전고지 등 향후 면책요건으로 규정될 가능성이 있는 절차를 미리 정비하는 것이 바람직합니다. 아울러 향후 하위법령을 통해 구체화될 보상대상과 보상 한도, 면책 범위 및 적용 요건 등에 관한 제도개선 동향도 지속적으로 확인할 필요가 있습니다.

아울러, AI 기반 Post 망분리 보안체계로의 전환과 관련하여 금융회사는 망분리 규제 완화에 수반되는 대체통제 요건의 강화에도 대비하여야 합니다. 망분리 규제의 전면해제는 금융회사의 AI 및 디지털 기술 활용 범위를 확대하는 조치이지만, 동시에 기존 망분리 체계를 대체할 수 있는 실효성 있는 보안통제체계의 구축을 전제로 한다는 점에서 유의할 필요가 있습니다. 현재 TF는 AI 및 보안 역량이 우수한 금융회사를 선정하여 엄격한 대체통제 조건하에 망분리 규제를 완화하는 방안과 함께 데이터 관리, 제로트러스트 원칙 및 보안 내부통제 체계 구축 등을 논의하고 있으며, 2027년 1분기까지 구체적인 방안을 마련할 예정입니다. 이에 금융회사는 상시 제도화될 예정인 보안 목적의 AI 및 SaaS 활용 관련 규제 예외와 혁신금융서비스 제도를 적극적으로 검토하는 한편, 향후 망분리 규제 전면해제의 적용 대상 선정기준과 대체통제 요건을 사전에 분석하고 이에 필요한 기술적·관리적 기반을 마련할 필요가 있습니다. 한편, 향후 「디지털금융 안전법」 제정에 따라 가상자산사업자, 보험대리점(GA), 대부업 등에도 「전자금융거래법」에 준하는 수준의 보안규율이 적용될 수 있으며, 클라우드 및 플랫폼 사업자 등 금융회사와 연계된 제3자에 대한 규율도 검토되고 있습니다. 따라서 해당 사업자들 역시 향후 규제 적용 범위와 구체적인 의무사항을 면밀히 살펴보고, 관련 법령 및 정책 동향에 맞추어 내부 보안관리체계를 선제적으로 정비할 필요가 있겠습니다.

그리고 무엇보다 이번 방안은 기술적 취약점 점검뿐 아니라 보안 관련 의사결정과 내부통제의 실효성을 함께 점검한다는 점에도 주목할 필요가 있습니다. 금융회사는 중요 취약점 발견 시 서비스 중단, 대체통제 적용 및 예외적 서비스 재개에 관한 판단·승인 절차를 정비하고, CEO·CISO·CIO 및 이사회의 역할을 구체화할 필요가 있습니다. 특히 예외적 서비스 재개와 관련하여 제시된 CISO의 이사회 보고·승인 요건을 반영하고, 취약점의 내용, 대체통제의 적정성, 보완 일정 및 후속 조치 결과를 기록·관리할 필요가 있습니다. 전수점검 과정에서 확인된 관리 부실을 유연하게 처리하겠다는 방침 역시 신속하고 충실한 보완조치를 전제로 한다는 점에 유의하여야 합니다.

법무법인(유) 광장의 디지털금융팀은 금융IT · 정보보안, 「전자금융거래법」 및 개인정보 보호 관련 다양한 법률 이슈 및 쟁점에 대해 풍부한 자문 경험을 보유하고 있습니다. 위 내용과 관련하여 전문적 검토나 지원이 필요하신 경우, 언제든지 법무법인(유) 광장의 디지털금융팀으로 문의하여 주시기 바랍니다.

이 뉴스레터는 일반적인 정보 제공만을 목적으로 발행된 것으로서, 법무법인(유) 광장의 공식적인 견해나 법률의견이 아님을 알려드립니다. 법무법인(유) 광장에서 발송하는 뉴스레터를 원하지 않으시면 **[수신거부]**를 클릭해 주십시오.

뉴스레터 더 보기

Lee & Ko 법무법인(유) 광장

서울 | 서초, 서울 | 판교 | 북경 | 호치민시티 | 하노이 | 자카르타

02.772.4000 | mail@leeko.com | www.leeko.com