AI 시대 침해위협에 대응하기 위한
全금융권 보안체계 혁신방안

2026. 11. 5.

금 융 위 원 회
금 융 감 독 원
금 융 보 안 원

목 차

Ⅰ. 현 황 ····· 1

1. 그간의 대응 ····· 1

2. 최근 해킹사고 특성 및 문제점 ····· 2

Ⅱ. 대응방안 ····· 3

1. 보안취약점에 대한 빈틈없는 점검 ····· 4

2. 2차 피해 방지를 위한 든든한 방어체계 마련 ····· 9

3. AI 기반, Post 망분리 新보안체계 구축 ····· 13

Ⅲ. 향후계획 ····· 16

Ⅰ. 현 황

1 그간의 대응

□ **정부**는 해킹 등 **사이버위협**이 지속 진화함에 따라 **금융권**의 **보안역량 강화**를 위해 **다양한 대책**을 **꾸준히** 추진

① 금융회사의 보안위협에 유연하게 대응할 수 있도록 **규정중심**의 보안규제를 **원칙중심**의 **자율보안 체계***로 **전환**('25.2월)

* 사전적·열거적 형식 지양하고, 원칙·목적을 제시하여 금융회사가 보안조치를 스스로 정할 수 있도록 규정개정(당초 293개 규정에서 166개로 축소)

② AI, SaaS 활용 관련 **망분리 예외 허용**('24.9월~), **SaaS** 이용 관련 **망분리 예외 상시화**('26.4월) 등 **망분리 규제 개선** 실시

③ '25.8월 롯데카드 정보유출 사고 이후, 금융권의 **보안책임성 강화** 등을 위한 「**전자금융거래법**」 **개정*** 추진('25.11월)

* ❶침해사고 발생시 징벌적 과징금(전체 매출액 3%) 도입, ❷취약점 개선 관련 이행강제금 도입 ❸CEO 책임·CISO 권한 강화, ❹정보보호 공시제도 도입 등

□ 한편, '26.4월 AI로 인한 **새로운 보안위협**이 급부상함에 따라 기존 보안체계와 **차별화된 보안대책**도 **신속**하게 **추진**

① 보안목적 AI 활용을 위한 **망분리 규제 긴급 완화 실시, 망분리 규제 전면 해제 추진** 등 망분리 제도 개선방안 마련('26.6월~)

② 금융권이 AI위협에 적극 대응할 수 있도록 **보안패치 관련 임직원 제재면책, AI 보안 가이드라인 배포** 등 실시('26.7월)

③ **금융AI보안연구소·지원센터** 설치, **AI 보안취약점**(블랙박스 테스트) **점검** 등을 통해 **중소형 금융권**의 보안도 지원('26.6월~)

□ 아울러, 정보유출 등으로 인한 **소비자 피해**(보이스피싱 등) **예방**을 위해 **ASAP 구축**('25.10월), 신종피싱 **계좌정지 허용**('26.6월) 등도 추진

2 최근 해킹사고 특성 및 문제점

□ **(해킹위협 확산)** 금융권*에서 **정보유출 등** 침해사고가 **잇따라 발생**하면서 **AI** 활용 공격에 대한 **불안감**과 **공포감**이 확산

* 은행, 제2금융권, 여신, 보험, 금투, 온투, 전자금융, 가상자산 등 대다수 업권

○ 특히, 공격양상이 보안관리가 철저한 **핵심 시스템이 아닌** 인력 등의 한계로 **관리**가 **소홀한 부분***을 집중 공략

* 영업·상담 등 내부직원이 사용하는 웹·모바일 서비스의 외부접점 등

○ AI 활용의 보편화로 인해 금융·공공·IT 등 다양한 분야에서 **광범위한 공격시도***가 발생하고, **고위험 취약점 발견**도 증가

* 금보원은 **매일 10~15만건**의 全금융권 대상 침해공격 의심트래픽 탐지·대응

□ **(소비자 피해 우려)** 해킹으로 인한 정보유출 등 사고 발생시 **소비자 2차 피해**로 이어질 **가능성**도 확대

○ 다크웹·텔레그램 등 **음성적 유통경로**에서 유출정보가 거래되면서 **다양한 금융범죄**(보이스피싱·신종피싱 등)에 **악용**될 우려

○ AI로 인해 금융범죄가 점차 **지능화·정교화***됨에 따라 기존의 **이상거래탐지 체계**만으로는 신속한 탐지·차단이 **역부족**

* (예) 이상거래 탐지기준(임계치) 회피, 정상거래 패턴 모방 등

□ **(보안제도 한계)** 금융권은 **망분리 규제 중심**의 **보안체계로** 인해 **보안체계 강화**에 **AI** 등 다양한 기술 활용이 **어려움**

○ **망분리·인력 중심**의 현행 보안체계에서는 금융회사가 보다 **능동적·적극적 대응체계** 구축에 **한계**가 있다는 지적

➡ 금융분야는 **신뢰와 안정**이 중요한 만큼, **"선제적 보안체계"**와 **"소비자 보호"**를 위한 **대책** 마련이 시급한 시점

Ⅱ. 대응방안

금융권 보안관리 사각지대 해소 및
AI 기반 선제적 대응체계로 전환

보안관리 강화 방안

대응방향	주요과제
1 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 AI해킹대비 지원 강화
2 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
3 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

◆ 全금융권의 보안역량 강화 및 소비자 피해 예방에 총력

ㅇ 대국민 신뢰 확보 및 금융시스템 안전성 제고 등을 위해 빈틈없는 보안체계 구축을 신속하게 추진

1 보안취약점에 대한 빈틈없는 점검

1. 全금융권의 외부접점 · 내부통제 체계 전수점검(11~12월)

◇ 全금융권의 모든 IT자산·서비스에 대해 외부접점·내부통제 체계를 꼼꼼히 점검해 보안 사각지대를 빈틈없이 해소

(1) 현황

□ AI를 활용한 고도화된 해킹이 업무지원·직원관리 등 **주변부 시스템**까지 빠르고 치밀하게 **공격**하는 양상 → **全 외부접점 철저한 관리** 중요

○ 최근 금융사 해킹피해 상당수는 **권한관리 부실·이중인증 우회·부실한 API 관리** 등 그간 소홀히 여겼던 **'약한고리'** 통해 발생

○ 보안 취약점 적시판단, 적극적 보안조치(보안패치 등) 등을 위한 CEO·CISO·CIO 등 **내부통제 장치 작동여부**도 관건

(2) 전수점검 내용

□ 전체 금융회사의 **모든 외부접점**과 **내부통제 운영실태**에 대한 **전수점검** 및 신속 **보완조치** 실시

○ **(점검범위) 全 금융회사**·전자금융업자 + α (**약 580개사**)

* 가상자산사업자 등「전자금융거래법」미적용 업권 포함

○ **(점검대상) 全 IT자산**(API 포함)의 **외부접점** 관리 + **내부통제 실태**

- **(업무)** 홈페이지 등 대고객서비스뿐 아니라, ▲직원관리, ▲내부업무, ▲제휴업무 등 외부에서 접근가능한 **모든 업무영역을 망라**

- **(시스템) 영업·관리목적 API, 인증·접근통제 시스템** 전반*

* 외부접점의 하드웨어, 소프트웨어(오픈소스 포함), API 등 IT자산 전반과 개발·테스트 및 임시운영 시스템을 포함

- **(내부통제)** 외부접점 **생성·운영·폐기** 관련한 **내부통제 전반**

* ①내규 유무, ②내부통제 작동여부(결재, 승인, 보고 등), ③IT자산·서비스 관리대장 운영 여부, ④취약점 분석·평가 및 보안관제 여부, ⑤CEO·CISO·CIO 역할 등

○ **(점검방식)** 우선 금융사가 자체점검*을 실시하되, 점검내용 부실·중요한 취약점 등의 경우에는 **현장점검 실시**(금감원·금보원)

* ▲점검상 문제가 없는 경우라도 조사방법, 판단사유 등을 상세하게 적시하고, ▲관리대장 목록을 철저히 재점검후 목록에 빠졌던 서비스도 등재후 빠짐없이 점검

○ **(조치사항)** 서비스 및 업무에 **불필요한 외부연결**은 **즉시 차단**

- **고객·금융회사의 금전피해, 개인정보 유출**과 **직결**되는 취약점(他이용자 정보 조회 등)은 **보완 전**까지 **즉시 서비스 중단**

- 즉시 보완이 어렵고 중요한 서비스인 경우에 한해 **CEO승인·책임 하**에 **대체통제 적용후** 서비스 재개(CISO 이사회 보고·승인 병행)

○ **(감독원칙)** 전수점검 과정에서 확인된 관리부실은 즉시보완 전제하에 최대한 유연하게 처리하되, **이후 발생하는 사고**는 **엄정히 책임추궁**

<※참고> 취약점 점검 및 보완 주요내용(예시)

구분	주요 내용
❶ 노출 최소화	▸불필요한 서비스·포트·관리자 페이지 및 내부망 연결 제거
❷ 인증·권한	▸로그인 우회, 他 이용자 정보 조회 여부, 중요 서비스 인증 강화(MFA 등)
❸ 입력값 검증	▸요청 값 조작을 통한 비정상 접근·명령 실행 차단
❹ 보안 패치	▸최신 보안패치 적용, 기술지원 종료 장비 식별·통제
❺ 탐지·차단	▸대량 조회 등 자동화 공격의 탐지·차단

(3) 향후일정

1 관리대장에 등재된 **외부접점 전수조사·보완**(~'26.11월말)

2 전체 **외부접점 점검·보완** 및 **내부통제체계 전수조사**(~'26.12월말)

3 점검결과를 분석하여 **보안 내부통제 가이드라인 마련**('27.1분기)

※ 외부접점 및 내부통제체계 전수조사와 관련한 세부항목, 점검방식 등 구체적인 내용은 별도 안내 예정(금감원)

2. 금융권 공동 해킹 관제시스템 고도화(연내 시범운영)

◇ AI 침해위협에 全금융권이 신속하고 효과적으로 대응하기 위해 **개별 금융사의 위협정보 공유, 사고신고체계 정비** 등 추진

(1) 현황

□ 빠르고 광범위한 AI침해위협에 대응하기 위해서는 공격IP 등 신속한 정보공유가 필수적이나, **개별 금융사 파악정보는 미공유**

※ 통합관제시스템(FIRST, 금감원), 위협정보공유시스템(FCTI, 금보원) 운영중이나, **금감원·금보원 차원에서 파악한 위협정보만 공유** 중

□ 「전자금융거래법」이 적용되지 않는 업권*(가상자산사업자 등)은 침해사고 신고가 KISA에 이루어져 **금융권간 빠른 정보공유에 한계**

* 「정보통신망법」에 따라 조사권한이 인터넷진흥원(KISA)에 있으나, 타 금융권과의 해킹 연관성·연계 금융사와의 정보유출 여부확인 등 차원의 정보공유 필요

(2) 주요내용

① **개별 금융회사가 탐지한 해킹시도·공격 의심정보 全금융권 공유**

○ (대상) 유의미한 공격정보 공유가 가능한 대형 금융사 수집정보

* 대형 금융사(예) : 총 자산 10조원 & 상시 종업원 1천 명 이상 금융회사 + α
** 수집정보(예) : ▲해킹, DDoS 등 공격 방법, ▲공격 대상(내부망, DMZ 구간 등), ▲IP 등 공격 경로, ▲악용된 취약점, ▲악성코드 종류 등

○ (방식) **금감원 통합관제시스템**(FIRST) 통해 **全금융권 공유**

② **「전금법」 미적용 금융사** 등에 대한 **신속한 사고신고체계 마련**

○ (대상) 「전금법」 적용되지 않는 업권(가상자산, 보험GA 등)

○ (내용) **침해사고 인지 즉시** KISA 외에 **금감원·금보원 통보**

* 인지시점, 사고내용, 예상 피해유형·규모 등 포함

(3) 향후 일정

① **(개별금융사 위협정보 공유) '26.12월 시범운영**, '27년부터 전면운영
② **(사고신고체계 정비)** 전금법 미적용사 대상 **가이드라인 마련**('26.11월)

3. 금융권 취약점 분석·평가 내실화('26.11월 규정변경예고)

◇ 全금융권이 상시적으로 보다 철저히 보안관리를 하도록 **취약점 점검·평가 제도**를 **촘촘하고 내실있게 개편**

(1) 현황

□ 금융회사는 외부기관(금보원, 민간 보안기업 등)으로부터 연 1회이상 취약점을 점검받아 결과를 금융당국에 제출(「전금법」 제21조의3)

○ ▲침해위협 강화속도에 비해 **점검주기가 길고, ▲의무점검범위가 명시되지 않아** 주변부 시스템 등 꼼꼼한 점검에 한계 **▲보완조치 미이행시에도 시정수단이 마땅치 않다**는 한계점 지적

(2) 주요내용

1 **(점검주기 단축) 대형 금융사부터 단계적으로 연1회→ 2회** 강화

* [1단계] 대형사(총자산 2조원 & 종업원 3백명 이상) 2회 의무화 (규정변경)
[2단계] 중소형사까지 포함한 全금융권 대상('28년~)

2 **(의무 점검대상)** 전자금융거래와 직·간접적으로 관련된 **모든 외부접점은 취약점 분석·평가 대상에 포함**토록 의무화

3 **(수시점검)** 긴급한 취약점 점검 필요 발생* 시, **금융당국이 수시로 취약점 분석·평가를 요구**할 수 있도록 근거 마련

* (예) 유사한 침해사고의 동시다발적 발생, 심각한 공통 취약점 발견(PHP 사례) 등

4 **(이행력 확보)** 중요한 보안취약점 장기간 방치시 **금융당국이 시정명령**을 내리고, **미이행시 지속적인 이행강제금** 부과

(3) 향후일정

□ **「전자금융감독규정」 개정**(11월 중 규정변경예고)

* ①점검주기 단축, ②의무점검대상 명시 ③수시점검 근거마련 등 포함

□ **이행강제금 부과** 관련 **「전금법」 개정**(법안소위 계류, 연내통과 추진)

4. 중소형 금융회사 AI해킹대비 지원 강화('26.12월~'27.1분기)

◇ 상대적으로 보안역량이 부족해 AI 보안위협 대비가 어려운 **중소형 금융회사를 대상**으로 **다각적인 보안강화 서비스 지원**

(1) 현황

□ 중소형 금융회사는 급변하는 AI 보안위협에 대응하여 보안 전문인력·예산 등 충분한 대응여력을 확보하기 어려운 측면

(2) 주요내용

1 「원스톱 AI방어서비스」 제공

○ 금융보안원에서 중소금융사의 외부접점과 취약요인까지 상시 탐색하고, 위험 우선순위·조치방안까지 원스톱으로 제공

* AI Agent 활용, ▲공격자 관점 모의해킹, ▲맞춤형 취약점 정보 제공 등 실시

2 보안역량별 맞춤형 보안안내서 마련·현장교육 실시

○ 금융회사 보안역량에 맞게 보안조치 내용을 구분·제시하고, 우선순위가 높은 조치부터 이행할 수 있도록 안내

- 외부노출자산 목록화, 패치 적용기한 설정 등 기본적인 내용을 손쉽게 적용할 수 있도록 실행계획(액션툴킷)도 제공

* 프런티어 AI 보안위협 금융분야 대응요령(금보원, '26.6) 개정

○ 보안교육·세미나·자문 등 '찾아가는' 교육 프로그램 마련·시행

3 공격 위험도에 따른 경보체계 및 단계별 행동요령 마련

* (예) ▲AI 능력, ▲금융권 영향, ▲기존 보안통제 대응 가능여부 등을 종합 고려하여, [1단계] 일반, [2단계] 유의, [3단계] 강화, [4단계] 집중 등으로 구분

4 각 업권 협회와 협력하여 「AI기반 공동 보안관제」 구축 지원

(3) 향후일정

□ **「프런티어AI 보안위협 금융분야 대응요령」 개정**('26.12월)

□ **원스톱 AI방어서비스, 현장교육 등 마련·시행**('26.12월~'27.1분기)

2 2차 피해 방지를 위한 든든한 방어체계 마련

1. 다크웹 등 개인정보 유통 모니터링 및 차단(상시)

◇ **다크웹·텔레그램 등 음성적 경로**로 개인정보 등이 유통되어 국민의 2차 피해로 이어지지 않도록 **상시 모니터링·피해차단**

(1) 현황

□ 침해사고로 유출된 개인정보 등이 **다크웹 등 경로로 유통될 가능성** 제기되나, 금융사 자체적으로 적시포착·대응 쉽지 않음

* 다크웹은 익명거래·추적회피 등 위하여 특정 방식·기술 통해서만 접근가능

(2) 대응방안

① **다크웹·텔레그램 등 금융권 탈취정보 상시 모니터링·대응**

○ **금융보안원**을 통해 다크웹·텔레그램 등 각종 음성적 채널에서 ▲금융권 탈취정보 유통·거래 여부, ▲금융회사 대상 침해공격 모의정황, ▲신규 악성코드·취약점 출현상황 등 **상시 모니터링**

- 금융사 탈취정보 유통정황 확인시, 해당 금융회사에 즉시 통보하고, **실제 유출·거래사실 확인시 당국신고·고객통보·보상 등 즉각조치**

- 금융사 대상 **침해공격 정황·신규 악성코드 및 취약점 등** 정보는 통합 관제시스템(FIRST) 등을 통해 **즉각 전파, 보안관제에 활용**

② **국내 불법 유통채널 등 폐쇄 검토·추진**

○ 개인정보가 불법 유통되는 **국내 온라인채널 등**이 확인되는 경우 **관계부처 협조**(과기부, 방미통위, 경찰 등)하에 **사이트 폐쇄** 등 검토

(3) 향후일정

□ **금융보안원 다크웹·텔레그램 등 모니터링·대응**(상시)
□ **국내 불법 유통채널에 대한 폐쇄방안 관계부처 협의**(연내)

2. 보이스피싱 탐지·대응체계 고도화(「ASAP」2단계, '26.11월~)

◇ 유출된 정보가 보이스피싱 범죄 등 2차 피해로 이어지지 않도록 AI기반 범죄탐지·정보공유 확대 등 대응시스템 대폭 고도화

(1) 현황

□ AI기술과 유출데이터 등으로 빠르게 진화하는 보이스피싱 범죄를 효과적으로 차단하기 위해 신속한 정보공유·탐지 시스템 필요

□ 「ASAP」 출범후 실질적 성과 거두고 있으나, **▲AI기반 탐지시스템 구축 ▲최신 범죄수법 반영**(신종피싱 등) 등 추가과제 추진 필요

* **ASAP** : 보이스피싱 정보공유·분석 AI 플랫폼(**A**I-based anti-phishing **S**haring & **A**nalysis **P**latform)
↳ 54.5만건 정보공유, 9,045건 지급정지 및 752.6억원 피해예방('25.10월~'26.9월)

(2) 대응방안

① **AI기반 「의심거래 판단지수**("피싱지수")**」 도입**

○ 금융보안원-인터넷은행 3社가 「ASAP」 정보를 바탕으로 개발한 보이스피싱 탐지 **AI 공동모델 결과를 지수화**하여 **全금융권 공유**

- 금융회사가 범죄여부가 의심되는 거래를 「ASAP」에 질의하면, **「ASAP」은 AI 공동모델을 바탕으로 위험도를 판단해 답변**

  * 사기범죄 가능성을 0~100점으로 지수화해 산출·답변

- **금융회사**는 同 답변결과와 자체 FDS 판단내용, 고객확인 등 통해 보다 **효과적으로 범죄계좌 지급정지·자금환수** 가능

※ 특히 보이스피싱 탐지역량이 상대적으로 낮은 **중소형사 역량보완** 기대

<※참고> AI 피싱지수 서비스 개요



2 全금융권 대포계좌·신종피싱 대응시스템 고도화

○ **(공동탐지룰)** 최신수법을 반영해 **대포계좌·신종피싱 FDS 공동탐지룰*** **시나리오를 확대**(51개→66개)하고, **은행권→2금융권까지 공유범위 확대**

* 신종 범죄유형·특성 등을 통계적으로 분석해 마련·공유하는 시나리오 (각 금융회사 FDS 탐지의 기본 시나리오로 활용)

○ **(정보공유 확대)** 경찰수사중 획득한 **"신종피싱 의심정보*"**를 「ASAP」을 통해 **全금융권에 공유**하는 방안 협의·추진

* ▲신종피싱 사이트 유형·도메인 정보 ▲해당사이트 접속번호·시간 등

3 「ASAP」 공유정보 확대 및 실시간 연동체계 완비

○ 기존 공유정보 외에 보이스피싱 탐지에 중요한 역할을 하는 **다양한 정보* 추가 공유**([기존] 9종 90항목→[개선] 14종 137개항목)

* ▲카드 명의인 정보 ▲부정결제 가맹점 정보 ▲다크웹 유출카드 정보 등

○ 제2금융권·우체국 등도 **API를 활용한 실시간 연동체계 구축**

* (現)141개 참여기관 중 48개사만 API 활용 → (개선) 全금융사 API 연결

(3) 향후일정

□ **AI기반 「의심거래 판단지수**("피싱지수")**」 도입**('26.11월 시범운영)

□ **대포계좌·신종피싱 공동탐지룰 개편**('26.12월)

□ **「ASAP」 공유정보 확대, 실시간 연동 추진**('26.12월~)

3. 보이스피싱 무과실책임 법제화(연내 법안논의·통과 추진)

◇ 2차피해 발생시 피해자 보호, 금융사의 보이스피싱 방지유인 강화 차원에서 **범죄피해 일정부분 금융사가 보상**토록 **법제화**

(1) 현황

□ 정보유출 등에 따른 보이스피싱 범죄로 2차피해가 발생한 경우, 금융회사가 일정부분 피해금을 보상하는 제도 마련 필요성

*「통신사기 피해환급법」 개정안(강준현·조인철 의원안) 정무위 계류중

① 고도로 발전하는 범죄수법상 **피해자 주의책임으로 범죄예방 곤란**

② ▲의심거래 탐지·계좌 지급정지 등 법적책무 ▲「ASAP」 등 의심정보 분석 인프라 제공받은 **금융사가 스스로 책임다할 유인부여** 필요

(2) 대응방안

1 **우선 금융회사부터** 보이스피싱 피해금을 일정부분 책임지도록 **「통신사기 피해환급법」 개정안*** **신속히 국회 통과** 추진

* ❶송금계좌·수취계좌 금융회사 1:1로 보상금 분담
❷1~5천만원 범위내 보상한도 설정(대통령령으로 위임)
❸피해자에 충분히 범죄위험 알린 경우 등에는 금융사 면책부여 등

2 **통신사 책임성 강화** 등 관련하여 **정부차원 공론화 추진**

※ 금융업권 등은 동 법안 논의 과정에서 ▲보이스피싱 범죄가 통신수단을 매개로 이뤄지며 ▲피해자에 대한 보다 두터운 보호가 필요한 점 등을 근거로 통신사에 대한 책임성 강화 논의도 필요하다는 입장

(3) 향후일정

□ **「통신사기 피해환급법」 개정 추진**(연내 국회논의·통과 목표)

3 AI기반, Post 망분리 新보안체계 구축

1. 망분리 규제 전면해제 TF 구성('26.11월)

◇ AI 보안위협이 현실화된 상황에서 망분리 규제를 뛰어넘어 "AI공격은 AI로 방어하는" 新보안체계 마련 논의 본격화

(1) 현황

□ AI를 활용한 해킹위협이 현실로 다가온 시점에서 "AI공격은 AI로 방어하는" 보안체계를 확립하기 위한 구체적 실천과제 논의 필요성

(2) 주요내용

□ 금융권 망분리 규제 단계적 전면해제와, 이를 대체하기 위한 AI기반 "新보안체계" 논의를 위한 **「망분리 규제 전면해제 TF」 본격 가동**

○ **(구성) 정부, 유관기관, 민간 AI·보안 전문가, 全금융권 담당임원 등**

* [정부] 금융위, 과기부, 국정원, 개보위 등
[유관기관] 금감원, 보안원, 금결원, 신정원 등
[민간 전문가] AI·보안 전문가, 정보보호·법조계 전문가 등
[금융권] 全 금융권 협회 및 주요 금융사 담당임원 등

○ **(논의사항) ❶ 망분리규제 전면해제① 추진절차·평가기준 등**
❷ AI기반 "新보안체계②" 구체적인 내용·적용방식 등

* ① 고도의 AI·보안역량 갖춘 금융사 선정, 엄격한 대체통제하 규제 해제
② ▲데이터 관리(N2SF 등) ▲제로트러스트 원칙 ▲보안 내부통제(CEO-이사회-CISO-현업부서 책임성) ▲침해사고 발생시 대응체계 등

○ **(운영)** 전체회의 - 실무회의 등 종합적인 논의를 거쳐
망분리규제 전면해제 + AI기반 新보안체계 방안마련('27.1분기내)

(3) 향후일정

□ **「망분리규제 전면해제 TF」 발족·운영**('26.11월)

2. 보안목적 AI 테스트 상시화 및 혁신금융서비스 활성화('26.11월~)

◇ 보안강화 목적의 AI활용을 안정적·상시적으로 지원하고, 혁신금융서비스 통한 망분리 규제 완화도 일관되게 추진

(1) 현황

□ 보안목적 AI활용시 망분리규제 긴급완화조치(1차, '26.6월) 경험 등 바탕으로 **보안강화 용도 AI 활용을 안정적·상시적 지원 필요**

<※ 참고> 보안목적 AI 망분리 규제 긴급 완화 1차 테스트 주요 시사점

· AI를 통한 **내부 소스코드 점검 결과**, 상당수 금융회사에서 **▲접근·인증통제 미흡, ▲공격코드 주입**(인젝션) 등의 **취약점**을 **다수 발견**

→ 최근 금융권 침해사고 주요원인인 **인증·접근통제 API 취약점 해결**에 상당히 **효과적**

□ 혁신금융서비스를 활용한 **업무용 SaaS, 생성형AI 활용** 등 **망분리규제 완화 정책도 일관되게 이어갈 필요성**

* 업무용 SaaS('26.4월 상시제도화), 생성형 AI(혁신금융서비스 활용)

(2) 주요내용

1 **보안목적 AI 활용 상시 제도화**(전금업 감독규정 개정)

○ (대상) **보안목적 AI 테스트 + SaaS 서비스**
○ (내용) 망분리 규제 예외 허용
○ (대체통제) 외부접점 관리, 인증·접근통제, 보안사고·장애대응 등
○ (절차) 비조치의견서 → **전금업 감독규정 개정**

* 긴급한 수요 감안하여 **2·3차 망분리규제 긴급완화조치는 예정대로 추진**하되, **이후의 보안목적 AI 활용 수요**는 **"상시 제도화" 통해 해소**

2 **혁신금융서비스 지정을 통한 망분리 규제완화 지속 확대**

○ 엄격한 대체통제 전제로, **생성형AI·블록체인 등 다양한 IT기술 대상**으로 혁신금융서비스를 통한 **망분리 규제완화 일관되게 추진**

(3) 향후일정

□ **전자금융감독규정 개정**('26.11월 규정변경예고)
□ **혁신금융서비스 지정을 통한 망분리 규제완화**(지속)

3. 「디지털금융 안전법」 추진(연내 방안 마련)

◇ AI 해킹위협 현실화, 디지털 혁신 가속화 등 **급변하는 보안 환경**에 맞춰 **全금융권과 유관업종 등에 치밀한 보안규율 확립**

(1) 현황

□ AI 해킹위협 현실화, 가상자산 등 새로운 업종 활성화, 디지털금융·클라우드 환경 보편화 등에 맞춰 **보안규제 전반 재정비 필요성**

(2) 주요내용

□ 全 금융권과 유관업종 등에 걸쳐 치밀한 전산보안 규율이 확립되도록 **「디지털금융 안전법」 마련 추진**

○ **가상자산 사업자, 보험GA, 대부업 등** 직접 전자금융거래를 수행하지는 않으나 ▲많은 금융·고객정보를 보유하고 ▲침해사고시 고객의 직접적 자산손실 가능성 있는 업종 등에 대해서는 **현 「전자금융거래법」에 준하는 수준의 보안규율** 등 적용

○ **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 적용** 검토

○ **금융회사 스스로·상시적으로·철저히 보안관리**에 임할 수 있도록 CEO 책임성·이사회 구성·현업부서 역할 등 **보안 거버넌스·내부통제 차원의 규율도 검토·반영**

(3) 향후일정

□ **관계기관 의견수렴 등 거쳐 방안 마련**(연내)
□ **「디지털금융 안전법」 법안 마련·발의 추진**('27.1분기)

Ⅲ. 향후계획

추진과제	추진일정
1. 보안취약점에 대한 빈틈없는 점검	
1 全금융권의 외부접점·내부통제 체계 전수점검	
· 관리대장에 등재된 외부접점 전수조사·보완	~'26.11월
· 전체 외부점검 점검·보완 및 내부통제체계 전수조사	~'26.12월
· 점검결과를 분석하여 보안 내부통제 가이드라인 마련	'27.1분기
2 금융권 공동 해킹 관제시스템 고도화	
· 각 금융사가 탐지한 해킹시도·공격 의심정보 全금융권 공유	'27.초
· 전금법 미적용사 대상 가이드라인 마련	~'26.11월
3 금융권 취약점 분석·평가 내실화	
· 점검주기를 대형 금융사부터 단계적으로 연1회→2회 강화	~'26.11월
· 전자금융거래 관련 모든 외부접점을 분석·평가 대상 포함	~'26.11월
· 긴급 취약점 점검 필요 발생 시, 수시점검 근거마련	~'26.11월
· 보안취약점 방치시 시정명령, 미이행시 지속적인 이행강제금 부과	연내 통과 추진
4 중소형 금융회사 AI해킹대비 지원 강화	
· 중소형 금융사 대상 「원스톱AI 방어서비스」 제공	~'26.12월
· 보안역량별 맞춤형 보안안내서 마련·현장교육 실시	~'26.12월
· 공격 위험도에 따른 경보체계 및 단계별 행동요령 마련	~'27.2월
· 각 업권 협회와 협력하여 「AI기반 공동 보안관제」 구축 지원	'27.1분기

추진과제	추진일정
2. 2차 피해 방지를 위한 든든한 방어체계 마련	
1 다크웹 등 개인정보 유통 모니터링 및 차단	
· 다크웹·텔레그램 등 금융권 탈취정보 상시 모니터링·대응	즉시
· 국내 불법 유통채널 등 폐쇄 검토·추진	즉시
2 보이스피싱 탐지·대응체계 고도화(ASAP 2단계)	
· AI기반 「의심거래 판단지수(“피싱지수”)」 도입	~’26.11월
· 대포계좌·신종피싱 공동탐지룰 개편	~’26.12월
·「ASAP」 공유정보 확대, 실시간 연동 추진	’26.12월~
3 보이스피싱 무과실책임 법제화	
·「통신사기피해환급법」 개정 추진	~’26.12월
3. AI기반, Post 망분리 新보안체계 구축	
1 망분리 규제 전면해제 TF 구성	
·「망분리규제 전면해제 TF」 발족·운영	’26.11월
2 보안목적 AI 테스트 상시화 및 혁신금융서비스 활성화	
· 보안목적 AI 활용 상시 제도화를 위한 전자금융감독규정 개정	’26.11월
· 혁신금융서비스 지정을 통한 망분리 규제완화 지속 확대	지속
3 「디지털금융 안전법」 추진	
·「디지털금융 안전법」 법안 마련·발의 추진	’27.1분기