

# 금융보안원 업무보고



## 1. '빈틈없는' 공격탐지 체계 구축

### 사전에방적 보안관제 개시



취약 요인을 '선제적' 탐지·대응  
(ASM\* 서비스 개시)

\* Attack Surface Management

### 공격탐지에 AI 기술 적용

대량의 공격정보\*를  
AI로 신속·정확하게 분석

\* 금융권 대상 공격탐지 건수(일간, '25년) : 약 12만건



금융 보안관제용  
AI 에이전트 개발 추진

## 3. 사고 예방 및 대응 강화

### 모의해킹 서비스 확대



화이트해커

모의 해킹



금융회사

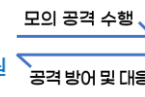
금융보안원 모의해킹(RED-IRIS)  
조직 확대 (팀 → 부서)

※ 금융위 업무계획(모의해킹 의무화) 연관 사항

### 사고대응 훈련 강화



금융  
보안원



금융  
회사

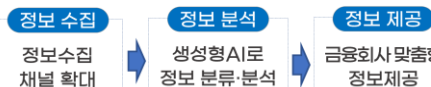
훈련 내용  
랜섬웨어 등  
최신 공격 반영

훈련 방법  
훈련 인프라 확대  
(상시 훈련 가능)

## 2. 사이버위협 정보·수집 분석 강화

### AI 기반 맞춤형 정보 제공

생성형 AI 기반  
사이버위협 정보 분석 고도화  
금융회사 맞춤형 위협정보 제공



### S/W 취약점 관리 강화

S/W 취약점 신속히 파악 → 보안 패치를 빠짐없이 적용

※ 롯데카드 해킹사고 주요 원인 : 보안패치 미 적용

S/W 취약점 종합관리 인프라 구축

취약점 통합 관리    S/W 부품\* 관리

\* SBOM(S/W Bill of Material) : S/W 자재 명세서

## 4. 보이스피싱 정보 공유·분석 고도화

### 보이스피싱 AI 플랫폼 강화



참여대상 확대(은행 → 제2금융권 등)

유관기관 연동 및 상호 연계 강화

※ 금융위 업무계획(보이스피싱 AI 플랫폼 정보공유 및 활용도 확대 추진) 연관 사항

### 은행권 AI 탐지모델 개발

은행권 공동 보이스피싱 탐지  
AI 모델을 개발하여 제공

은행권 보이스피싱 탐지 역량 제고

## 1. 안전·신뢰 기반 AX(AI 전환) 지원

### AI 보안 지침서 제공



AI 보안 안내서  
(안전한 AI 개발·운영)



AI 모델 평가 기준  
(AI모델 신뢰성 제고)

### AI 학습데이터 보호



익명성(개인 식별 X) 평가 대상 확대  
(텍스트 중심 → 새로운 유형 데이터)

### AI 보안 모의점검 실시 및 보안 모범사례 제공

공격자의 시각에서 AI 서비스를 모의 공격 하는  
AI 레드티밍 (AI Red-Teaming) 본격 실시



금융보안원  
AI 전문가

다양한 수단으로 AI 서비스의  
결함이나 취약점 확인



금융회사  
AI 서비스

중소금융회사 지원을 위해 생성형 AI 보안도구 활용 모범사례 제시

✓ AI 보안 조직을 실 → 부서 단위(4개팀)로 확장

## 2. 디지털자산 보안 기반 마련

### 가상자산사업자 보안 강화



블록체인 특화 보안서비스 제공  
(예 : 가상자산사업자 맞춤형 위협정보 제공 등)

### 디지털자산 보안 기준 마련

#### 보안 프레임워크 개발

#### 디지털자산 주요 보안 고려사항

- 토큰 관리(스마트컨트랙트 취약점 점검 등)
- 지갑 및 개인키 관리
- 이용자 보호(강력한 인증, 이상거래 모니터링 등)

#### 디지털자산 입법\* 보안 지원

\* 가상자산 2단계 입법, 토큰증권(STO) 법제화 등

## 3. 철저한 제3자 보안 리스크 관리

### 클라우드 평가 강화

금융권 클라우드 활용 동향을  
반영한 보안 평가 강화

클라우드 S/W  
(SaaS)이용 확대

SaaS  
평가항목 정비

클라우드 관리대행  
업체(MSP)이용 급증

MSP\*  
평가 강화

### 수탁자 보안관리 강화

GA 등 개인정보 수탁자  
위험 확대에 따른 통제 강화

현장점검  
확대

GA 특화  
보안서비스

위수탁  
관계 공유

개인정보 수탁자 보안수준 제고

\* MSP : Managed Service Provider

## 1. 선진화된 보안문화 형성

### 금융보안 거버넌스 강화



경영진 보안 전문성 함양  
(사외이사 교육 강화)



성숙한 보안문화 정착  
(거버넌스 가이드 개정 등)

### 디지털금융안전법 제정 지원

금융위 디지털금융 종합 법제  
정책 지원 (해외정책 조사 연구 등)

규율범위 확대

거버넌스 확립

내부통제 강화

운영복원력

### 금융보안 수준진단 서비스 개시

금융회사가 자사 보안수준(4단계)을 정밀하게 진단·개선하도록  
금융보안 수준 진단 서비스 실시

#### 금융보안 수준진단 프레임워크(Self-regulated Security Framework) v.1.0

거버넌스  
(8개 항목)

식별  
(5개 항목)

보호  
(20개 항목)

탐지  
(5개 항목)

대응  
(4개 항목)

복구  
(1개 항목)

공급망  
(3개 항목)

성숙도  
등급

Initial(초기)

보안 활동이 비체계적 또는 임시로 이루어지는 단계

Defined(기반)

보안체계를 구축하여 안정적으로 운영하는 단계

Managed(발전)

보안이 정교화되어, 대내외 환경변화에 효과적으로 대응하는 단계

Advanced(고도화)

보안이 전사에 내재화되어, 고도화된 역량을 확보한 단계



## 2. 금융보안 인력 양성 지원

### 新기술 특화 교육 확대

금융권의 AI 등 활용 확대  
→ 新기술 분야 교육 강화

교육과정 신설  
AI 보안전문가  
양성 과정

교육 확대  
다양한 교육  
프로그램 개발

### 전문가 및 미래인재 양성



금융권 해킹대회\* 확대  
(AI 해킹 분야 추가 등)

\* FIESTA: Financial Institute' Event on  
Security Threat Analysis



보안 아카데미 내실화  
(우수 대학생과 금융회사 매칭 등)

## 3. 개인신용정보 보호 및 내부통제 강화

### 상시평가 실효성 강화

#### 정보보호 상시평가

신용정보법령에 따라 금융회사의 개인신용정보  
관리실태를 평가 (점수 및 등급 부여)

평가항목에  
모의해킹 추가

현장점검  
병행(필요시)

평가의 실질적 보안 강화 효과 제고

### 내부통제 수준 제고

금융권 내부통제 업무  
전문성 및 역량 강화 추진



핸드북 발간 및 세미나 개최  
(신용정보관리보호인 대상)



개인신용정보 전문가 양성  
과정 신설(이론, 실무 융합형)

금융보안 경쟁력 강화를 통해 금융보안 사고 예방에 최선을 다하겠습니다.