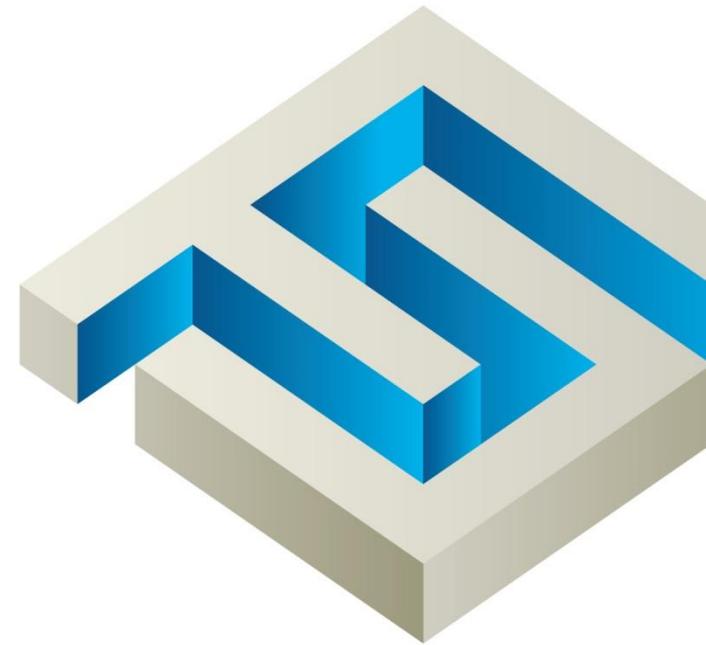


# 오픈뱅킹 관련 보안점검 주요내용

2019. 6. 20.

금융보안원



I

개요

II

이용기관 보안점검

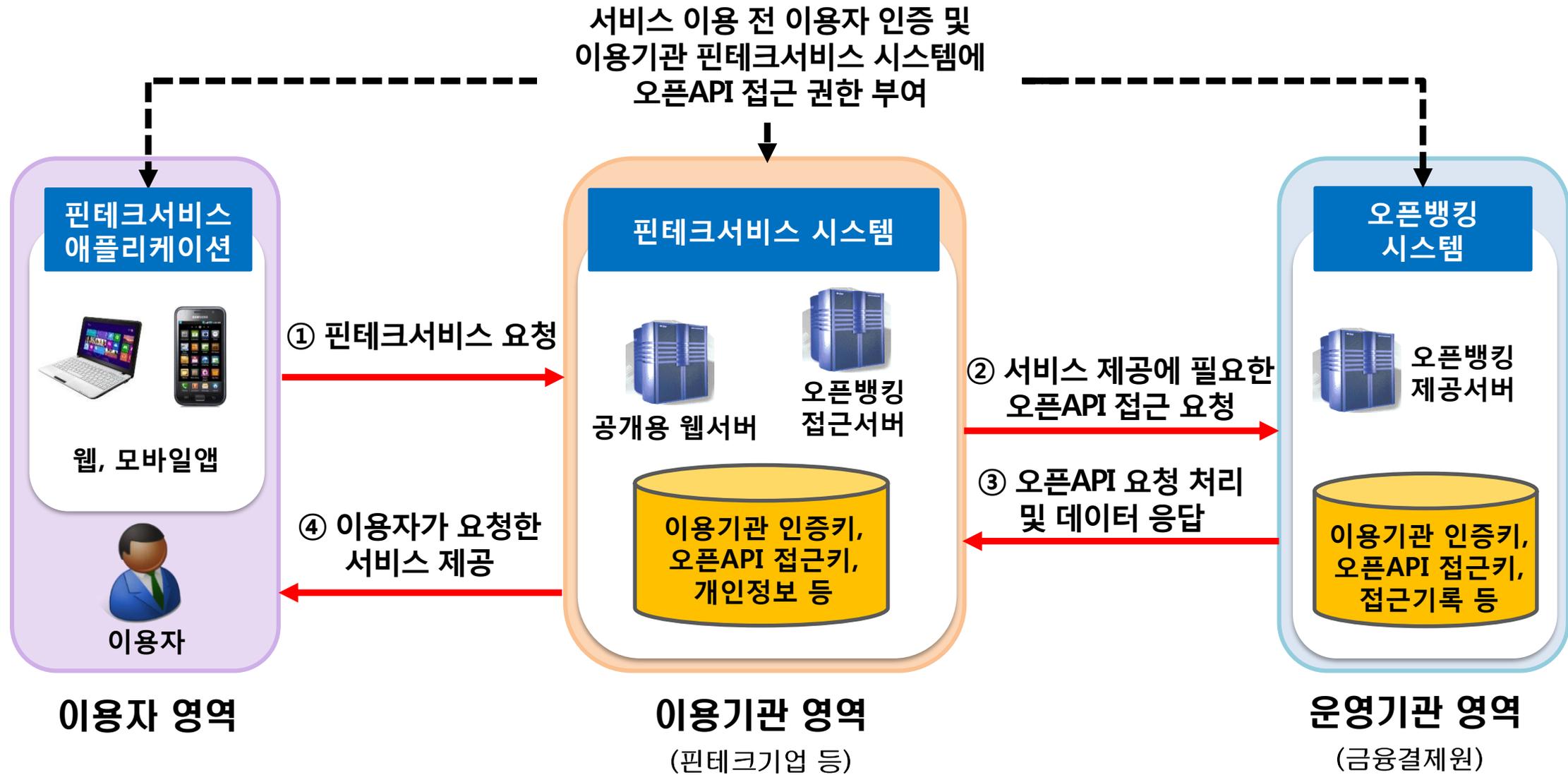
III

핀테크서비스 취약점 점검

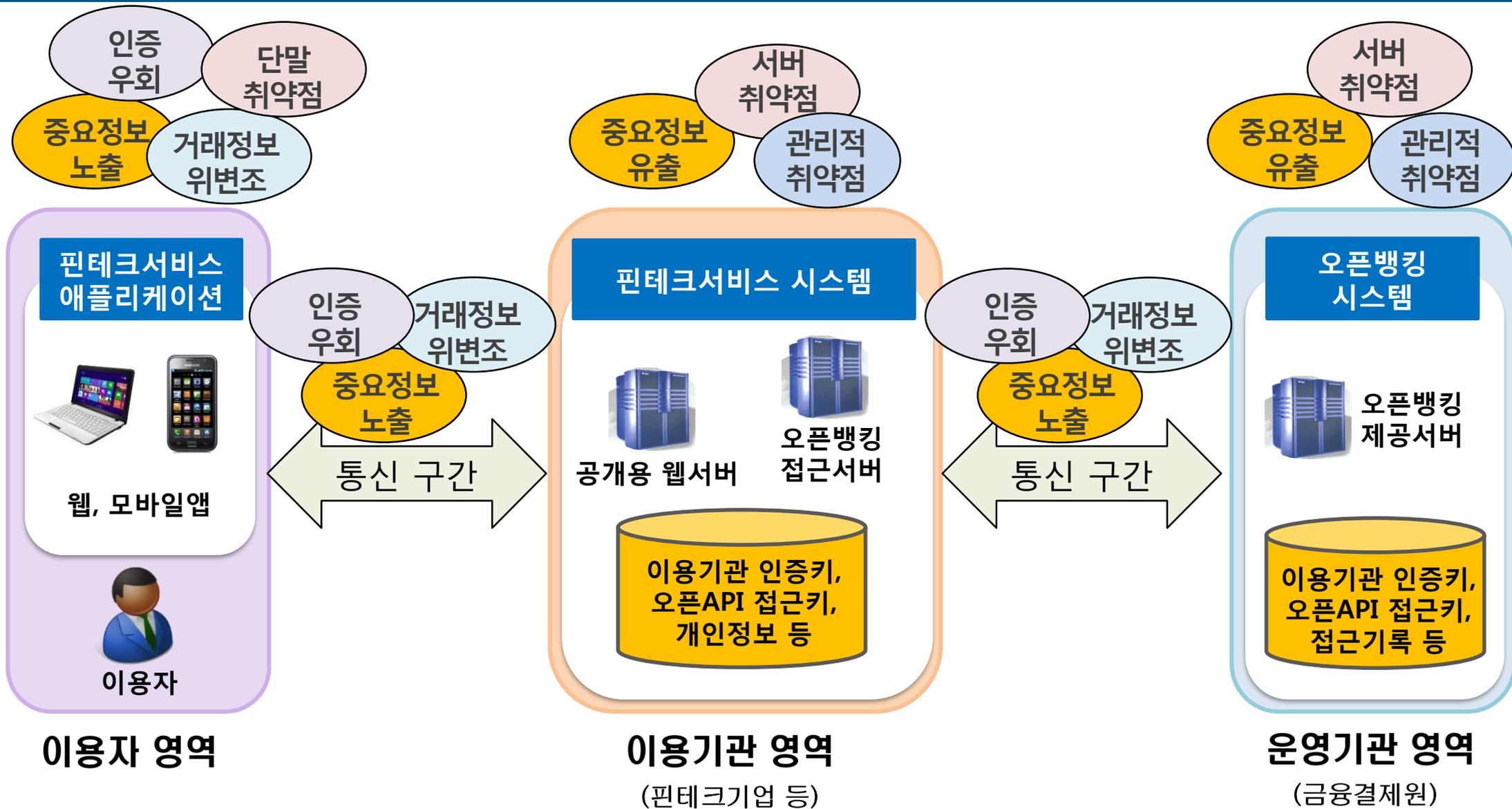
# I. 개요



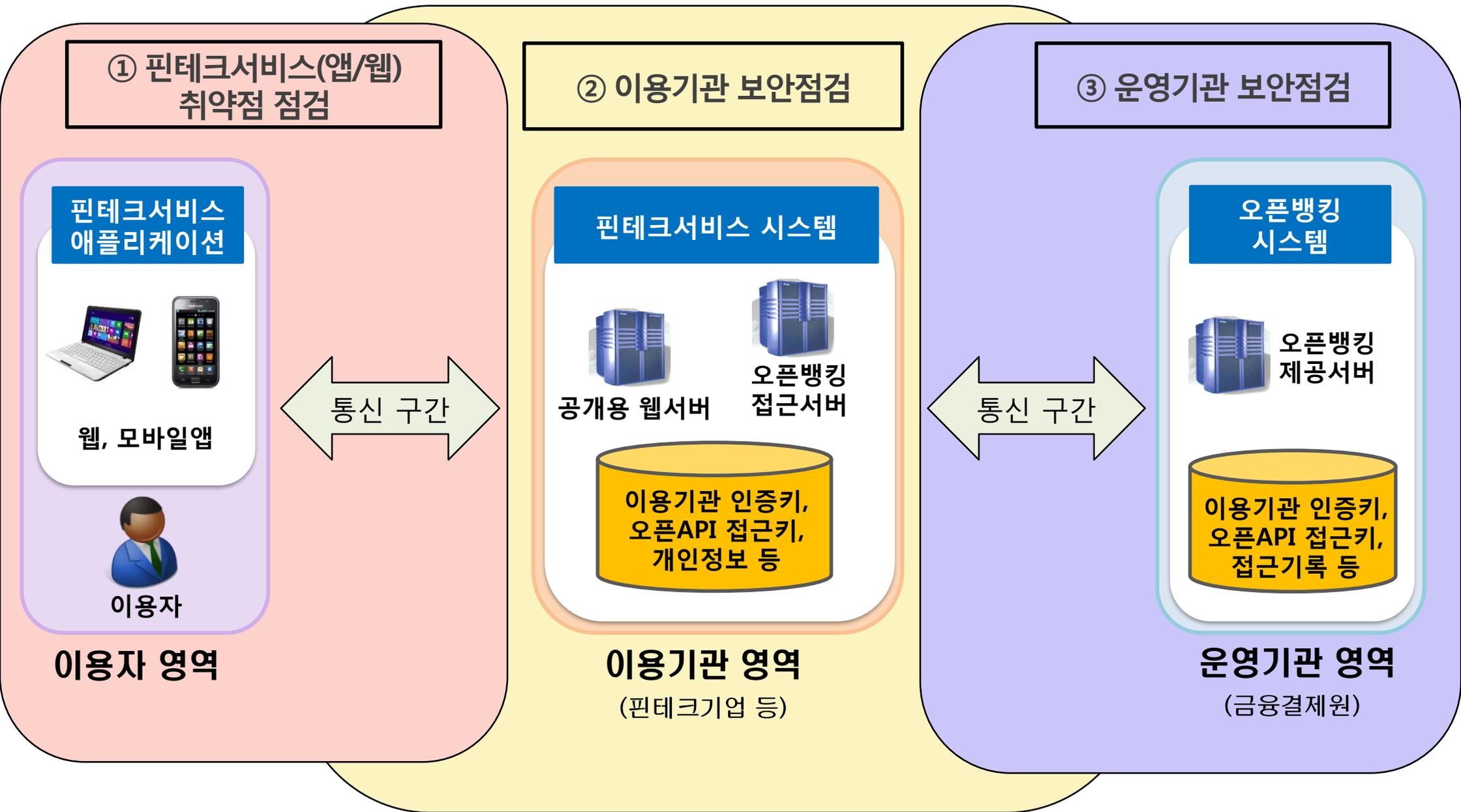
# 1. 오픈뱅킹 운영 구조



## 2. 오픈뱅킹 운영 시 보안 위협/취약점



# 3. 오픈뱅킹 보안성 확보방안



## 4. 오픈뱅킹 보안점검 개요

### □ 목적

⇒ 오픈뱅킹공동업무의 안전한 운영 및 이용을 지원하고  
금융 소비자를 보호하기 위하여 보안점검 업무 수행

### □ 점검 종류

- ① 이용기관 보안점검
- ② 핀테크서비스 취약점 점검

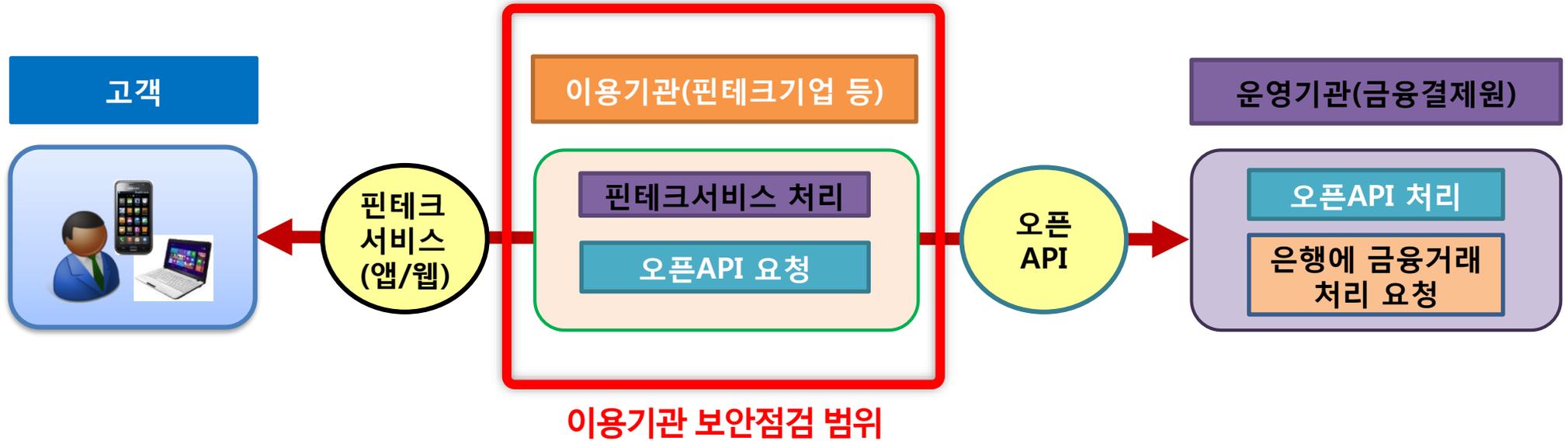
# Ⅱ. 이용기관 보안점검



# 1. 이용기관 보안점검 개요 (1)

이용기관이 오픈API 이용 핀테크서비스 운영 시 중요정보 보호 등 적절한 보안관리체계를 마련하고 있는지 점검

## <이용기관 보안점검 범위>



# 1. 이용기관 보안점검 개요 (2)

□ 점검 방법 : 서면 및 현장 점검

□ 점검 시기 : 오픈뱅킹 이용 서비스 실시 전

□ 소요 기간 : 약 4주(서면점검, 현장점검, 보완조치, 결과정리 등)

□ 점검 항목 : 금융보안원에서 개발한 보안점검 항목

⇒ 3개 영역, 14개 분야, 30개 점검항목으로 구성 예정

※ 「금융권 오픈API 이용기관 자체 보안점검 가이드」(금융보안원, '18.12월)와 「로보어드바이저 시스템 보안성 심사기준」 등을 참고하여 점검항목을 개발

□ 점검 수행 주체 : 금융보안원 등

# 1. 이용기관 보안점검 개요 (3)

## □ 점검 대체

① (기관유형) 은행 또는 전자금융업자

② (관련 인증 보유) ISMS 인증을 보유

⇒ ① 또는 ② 충족 시, 이용기관 자체 점검으로 대체 가능

※ 이용기관은 보안점검 항목별 충족 여부를 자체적으로 점검하여 운영기관에 제출

## □ 점검 시기 조정

⇒ 은행 또는 전자금융업자는 서비스 실시 전 점검을 유예 하되, 서비스 실시 후 1년 내 점검

## 2. 이용기관 보안점검 절차



### 3. 이용기관 보안점검 항목 (1)

보안영역	점검분야	보안점검 항목
관리	정보보호 정책·조직	① (정보보호최고책임자 지정 및 실무조직 구성) 정보보호최고책임자를 지정하고 실무조직을 구성하고 있는지와, 동조직이 정보보안 점검항목을 마련하여 정기적으로 점검을 수행하고 있는지 점검
		② (정보보호정책 수립 및 공표) 정보보호정책 및 정책시행 문서를 수립하여 문서화하고, 이를 임직원에게 공표하고 있는지 점검
	외부자 관리	① (위탁업체 선정 및 관리) 위탁업체 선정 시 보안 요구사항을 정의하여 계약서에 반영하고 있는지 점검
	정보자산 관리	① (정보자산 식별) 오픈API 관련 정보자산을 식별하여 목록을 관리하고 있는지 점검
	정보보호 교육	① (실무자 정보보호 교육 이수) IT직무자(개발, 운영) 및 정보보호 직무자는 직무 수행에 필요한 정보보호 교육을 이수하고 있는지 점검
	인적 보안	① (비밀유지서약서) 내외부 직원 대상으로 비밀유지서약서를 받고 있는지 점검
		② (퇴직 및 직무변경 관리) 내외부 직원의 퇴직 및 직무변경 시 권한 관리를 적절히 수행하고 있는지 점검
위험 관리	① (취약점 점검 정책 수립 및 점검 수행) 중요 정보자산에 대해 취약점 점검 정책을 수립하고, 취약점 점검을 수행하고 있는지 점검	

### 3. 이용기관 보안점검 항목 (2)

보안영역	점검분야	보안점검 항목
관리	침해사고 대응	① (침해사고 대응절차 마련 및 임직원 대상 공표) 침해사고 대응절차를 마련하고 임직원 대상으로 공표하고 있는지 점검
		② (침해사고 대응 관련 로그 보존 및 모니터링) 침해사고 대응에 필요한 로그를 일정기간 보존하고 주기적으로 검토하고 있는지 점검
	이용자 보호	① (개인정보 처리 관련 이용자 보호) 개인정보 처리방침을 이용자가 확인하기 쉽게 공개하고 이용자로부터 개인정보 처리 동의를 받고 있는지 점검
		② (개인·신용정보 접근 및 거래지시 권한 관련 안내) 오픈API를 통한 개인·신용정보 접근 및 전자금융거래 지시 가능 사실에 대해 이용자에게 안내하고 있는지 점검
		③ (이용자 고충 처리방침 마련 및 공개) 이용자 문의에 대응하는 처리방침을 마련하고 이용자가 확인하기 쉽게 공개하고 있는지 점검
	물리	물리적 보안
② (보호구역 반출입 관리) 휴대장치의 통제구역 반출입을 통제하고, 중요 단말기 및 휴대장치 등의 사무실 반출입을 통제하고 있는지 점검		

### 3. 이용기관 보안점검 항목 (3)

보안영역	점검분야	보안점검 항목
기술	개발 보안	① (설계 시 보안 요구사항 도출 및 반영) 신규개발 및 변경 시 보안 요구사항을 도출하고 이에 대한 대책을 설계에 반영하고 있는지 점검
		② (테스트 시 이용자 개인·신용정보 사용 제한) 개발 및 테스트 시 서비스 이용자의 개인·신용정보를 사용하지 않고 있는지 점검
	암호 통제	① (중요 정보 암호화 정책 수립 및 이행) 오픈API 관련 중요정보 보호를 위해 암호화 정책을 수립 및 이행하고 있는지 점검
	접근 통제	① (중요 정보자산 계정 및 접근 권한 관리) 오픈API 관련 정보처리시스템 및 관리자 권한 프로그램에 대해 접근 권한을 안전하게 통제하고 있는지 점검
		② (중요 단말기 지정 및 접근 통제) 오픈API 이용서비스 관련 중요 단말기를 지정하고, 접근을 통제하고 있는지 점검
	시스템 보안	① (주요 시스템 등의 악성코드 감염 및 정보유출 방지) 오픈API 관련 정보처리시스템의 악성코드 감염 및 정보유출 방지 대책을 마련하고 있는지 점검
		② (인터넷망을 통한 원격관리 통제) 오픈API 관련 정보처리시스템에 대해 인터넷망을 통한 원격 관리를 통제하고 있는지 점검
		③ (주요 시스템 목적 외 기능·프로그램·포트 등 제거) 오픈API 관련 정보처리시스템 내 서비스 목적 외의 기능·프로그램·포트 등을 제거하고 있는지 점검

### 3. 이용기관 보안점검 항목 (4)

보안영역	점검분야	보안점검 항목
기술	시스템 보안	④ (중요서버 독립 운영 및 정보보호시스템 적용) 오픈API 관련 서버는 독립서버로 운영하고, 정보보호 시스템을 적용하여 보호하고 있는지 점검
		⑤ (공개용 웹서버 보호대책 마련) 공개용 웹서버에 대한 보호대책을 마련하여 적용하고 있는지 점검
		⑥ (중요 보안패치 적용 지침 수립 및 이행) 회사에 적합한 보안패치 적용 지침을 수립하고, 주기적으로 검토 및 적용하고 있는지 점검
	네트워크 보안	① (DMZ 구간 구성) DMZ 구간을 구성하여 내부 네트워크를 보호하고 있는지 점검
		② (내부망 사설IP 활용 및 주요 시스템 배치) 내부망은 사설IP 주소를 활용하고 업무영역에 따라 핵심 시스템은 내부망에 배치하고 있는지 점검
		③ (무선 네트워크 이용 최소화 및 보안대책 수립·적용) 무선 네트워크는 통제 하에 이용을 최소화하며, 책임자 승인 하에 이용 시 보호 대책을 적용하고 있는지 점검
		④ (대외기관과 통신 시 보안통신 적용) 대외기관과 통신 시 보안통신이 적용되어 있는지 점검

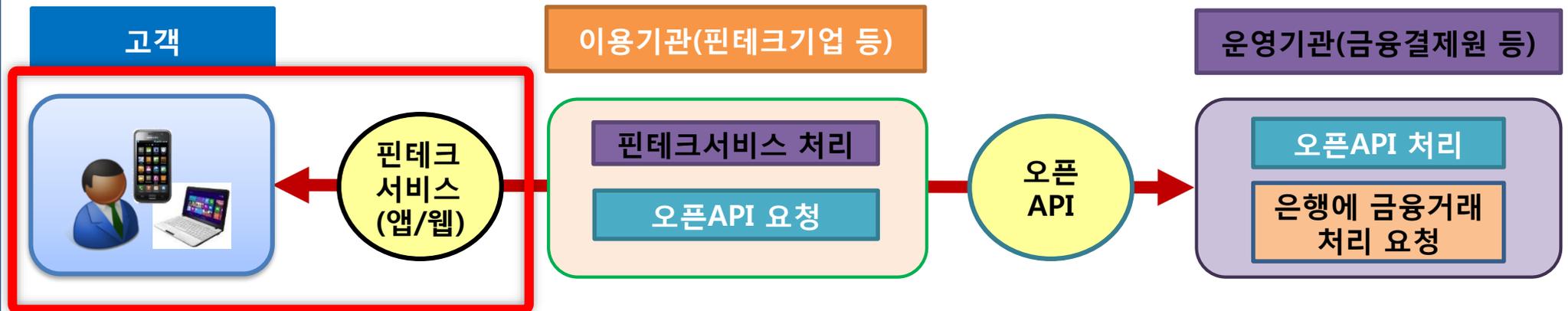
# Ⅲ. 핀테크서비스 취약점 점검



# 1. 핀테크서비스 취약점 점검 개요 (1)

## 오픈API를 이용하는 핀테크서비스 애플리케이션(앱/웹)에 대한 취약점을 점검

### <핀테크서비스 취약점 점검 범위>



핀테크서비스 취약점 점검 범위

# 1. 핀테크서비스 취약점 점검 개요 (2)

## □ 점검 방법 : 실점검 (테스트)

※ 점검도구 등을 이용하여 원격으로 자동 및 수동 점검

## □ 점검 시기 : 오픈뱅킹 환경에서 개발 및 테스트 완료 후 서비스 실시 전

## □ 소요 기간 : 플랫폼 별 5영업일 내외 소요 예정

## □ 점검 항목 : 금융보안원에서 개발한 취약점 점검 항목

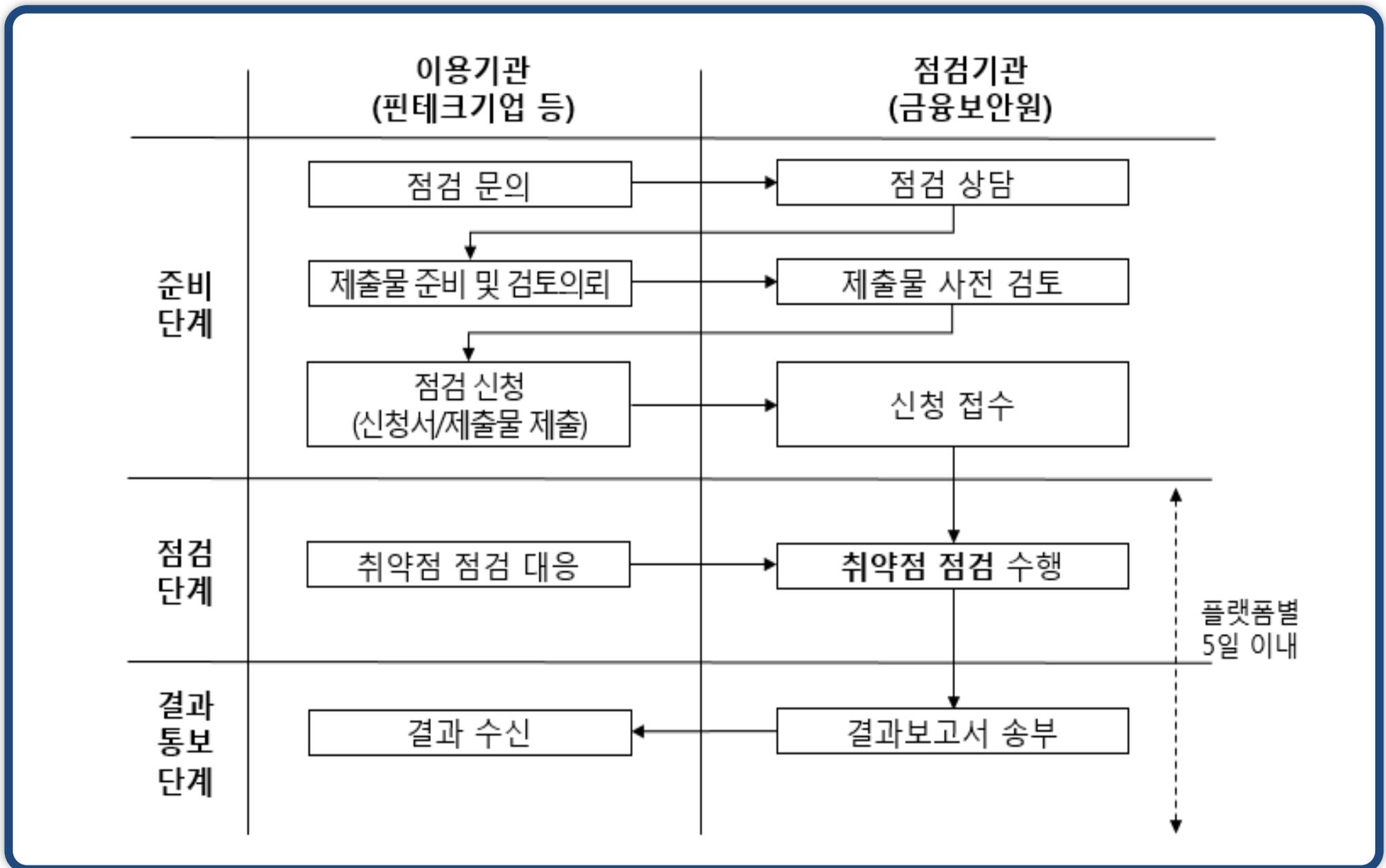
⇒ (웹) 4개 분야, 12개 항목, (모바일) 5개 분야, 17개 항목

## □ 점검 수행 주체 : 평가전문기관\* 또는 이용기관 자체전담반\*\* 등

\* 「전자금융감독규정」 제37조의3제1항에 따라 지정된 평가전문기관(금융보안원 정보보호전문서비스기업)

\*\* 「전자금융감독규정」 제37조의2제2항 요건(총자산 2조원 이상 & 상시 종업원 수 300명 이상)을 충족하는 금융회사 및 전자금융업자의 자체전담반(정보보호최고책임자 포함 5인 이상)

## 2. 핀테크서비스 취약점 점검 절차



### 3. 핀테크서비스 취약점 점검 항목 (1)

플랫폼	분야	점검항목
웹	중요정보 보호	① (메모리 내 노출 방지 수준) 기밀성이 요구되는 이용자 중요정보의 메모리 내 평문 노출 여부를 점검
		② (DOM 영역 내 노출 방지 수준) 기밀성이 요구되는 중요정보의 DOM 영역 내 평문 노출 여부를 점검
		③ (네트워크 구간 내 노출 방지 수준) 기밀성이 요구되는 중요정보의 네트워크 구간 내 평문 노출 여부 및 네트워크 보안 설정등을 점검
		④ (중요정보 파일 저장 수준) 기밀성이 요구되는 중요정보의 이용자구간 내 파일 저장 여부를 점검
		⑤ (중요정보 화면 표시 및 보호 수준) 기밀성이 요구되는 중요정보의 화면 표시 및 화면캡처를 통한 탈취 가능 여부를 점검
		⑥ (입력정보 보호 적용 수준) 이용자 입력 중요정보의 노출 방지를 위해 구현된 보호기능 적용 여부를 점검

### 3. 핀테크서비스 취약점 점검 항목 (2)

플랫폼	분야	점검항목
웹	거래정보 위·변조	① (계좌정보 변조 방지 수준) 전자금융거래 이용 중 무결성이 요구되는 계좌정보를 메모리 및 네트워크 구간에서 위·변조 시 부정이체 가능 여부를 점검
		② (금액변조 방지 수준) 전자금융거래 이용 중 무결성이 요구되는 금액정보를 메모리 및 네트워크 구간에서 위·변조 시 부정이체 가능 여부를 점검
		③ (거래정보 재사용 방지 수준) 전자금융거래에 이용되는 거래정보의 재사용 가능 여부를 점검
	서버 보안	① (서버 보안 적용 수준) 잘 알려진 웹서비스 취약점에 대한 보안대책 적용 등 서버 보안대책의 적용 여부를 점검
	인증	① (멀티로그인 탐지 적용 수준) 서로 다른 단말에서 동일 계정으로 로그인 시 탐지 및 대응 여부를 점검
② (인증 우회 방지 수준) 이용자 인증 및 세션 관리와 관련된 기능 구현의 적정성을 점검		

### 3. 핀테크서비스 취약점 점검 항목 (3)

플랫폼	분야	점검항목
모바일 (안드로이드 iOS)	중요정보 보호	① (메모리 내 노출 방지 수준) 기밀성이 요구되는 이용자 중요정보의 메모리 내 평문 노출 여부를 점검
		② (네트워크 구간 내 노출 방지 수준) 기밀성이 요구되는 중요정보의 네트워크 구간 내 평문 노출 여부 및 네트워크 보안 설정 등을 점검
		③ (디버그 로그 내 노출 방지 수준) 기밀성이 요구되는 중요정보의 디버그 로그 내 평문 노출 여부를 점검
		④ (중요정보 파일 저장 수준) 기밀성이 요구되는 중요정보의 단말 내 파일 저장 여부를 점검
		⑤ (중요정보 화면 표시 및 보호 수준) 기밀성이 요구되는 중요정보의 화면 표시 및 화면캡처를 통한 탈취 가능 여부를 점검
		⑥ (입력정보 보호 적용 수준) 이용자 입력 중요정보의 노출 방지를 위해 구현된 보호기능 적용 여부를 점검
	거래정보 위·변조	① (계좌정보 변조 방지 수준) 전자금융거래 이용 중 무결성이 요구되는 계좌정보를 메모리 및 네트워크 구간에서 위·변조 시 부정이체 가능 여부를 점검
		② (금액변조 방지 수준) 전자금융거래 이용 중 무결성이 요구되는 금액정보를 메모리 및 네트워크 구간에서 위·변조 시 부정 이체 가능 여부를 점검
		③ (거래정보 재사용 방지 수준) 전자금융거래에 이용되는 거래정보의 재사용 가능 여부를 점검

### 3. 핀테크서비스 취약점 점검 항목 (4)

플랫폼	분야	점검항목
모바일 (안드로이드 iOS)	클라이언트 보안	① (앱 위·변조 탐지 적용 수준) 점검대상 앱의 중요파일에 대한 위·변조 수행 후 서비스 정상 실행 가능 여부를 점검
		② (해킹OS 탐지 적용 수준) 루팅/탈옥된 단말에서 점검대상 앱 실행 시 정상 실행 가능 여부를 점검
		③ (안티디버깅 적용 수준) 디버거를 이용한 동적 디버깅 시도 시 정상 실행 가능 여부를 점검
		④ (코드 난독화 적용 수준) 점검대상 앱의 디컴파일 가능 여부 및 복구된 소스코드의 난독화 적용 여부를 점검
		⑤ (안티바이러스 적용 수준) 점검대상 앱 실행 시 악성코드 방지 대책을 점검
	서버 보안	① (서버 보안 적용 수준) 잘 알려진 웹서비스 취약점에 대한 보안대책 적용 등 서버 보안대책의 적용 여부를 점검
	인증	① (멀티로그인 탐지 적용 수준) 서로 다른 단말에서 동일 계정으로 로그인 시 탐지 및 대응 여부를 점검
		② (인증 우회 방지 적용 수준) 이용자 인증 및 세션 관리와 관련된 기능 구현의 적정성을 점검



금융보안원  
FINANCIAL SECURITY INSTITUTE

감사합니다.

