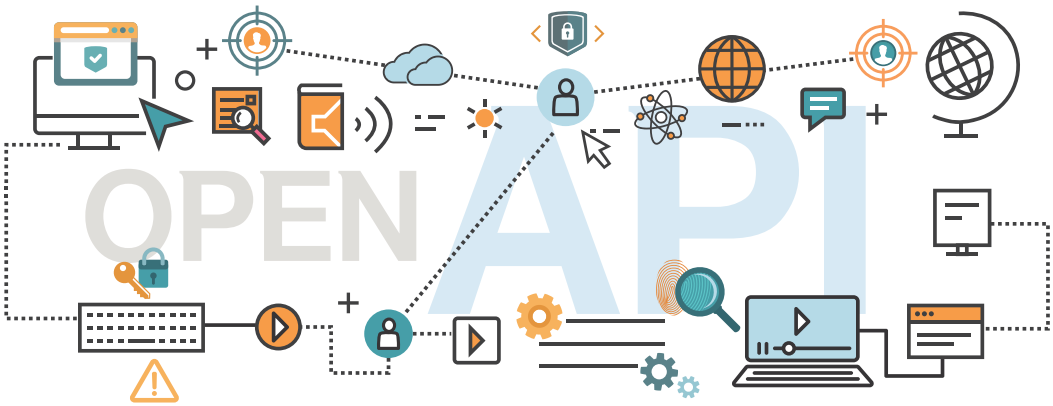
AGR-VI-2018-②-81

금융권 오픈API
이용기관 자체 보안점검 가이드

2018. 12.



금융보안원
FINANCIAL SECURITY INSTITUTE

AGR-VI-2018-②-81

금융권 오픈API
이용기관 자체 보안점검 가이드

2018. 12.

금융보안원
FINANCIAL SECURITY INSTITUTE

【 가이드 제·개정 이력 】

제 · 개정 일자	주요 내용	비고
2018.12.	가이드 최초 제정	

목 차

Ⅰ. 개요

1. 목적

본 가이드는 금융권 오픈API를 이용하여 고객에게 서비스를 제공하는 핀테크기업 등이 오픈API 이용 관련 보안 위험을 이해하고 이를 사전에 제거 또는 최소화 할 수 있도록, 보안점검 시 참고할 수 있는 정보를 제공함을 목적으로 한다.

2. 주요 내용

금융권 오픈API 이용 구조 및 주요 위험, 오픈API 이용기관이 갖추어야 할 보안 요구사항, 자체 보안점검 항목 및 점검보고서 예시를 제공한다.

3. 활용

① 본 가이드는 핀테크기업에 대한 일반적인 모든 위험을 다루기 보다는 오픈API 이용기관의 금융권 오픈API 이용 관련 주요 보안 고려사항을 점검항목으로 구성하였으므로, 이를 유의하여 업무에 활용한다.

② 해외 주요국 모범사례, 국내 유사 제도·규정·가이드 등을 종합 고려하여 가이드를 작성하였으나, 기관별·이용API별·서비스별 특이사항이 존재할 수 있으므로 가이드의 내용을 절대적인 기준으로 활용하지 않도록 유의한다.

③ 오픈API 이용기관은 별도 위험 분석·평가 등을 통해 도출된 추가 보안 요구사항이 존재할 경우, 가이드 점검항목 외 해당 보안 요구사항을 추가 반영하여 점검항목을 구성하고 이에 따라 자체 점검을 수행할 것을 권장한다.

④ 본 가이드는 오픈API 이용기관의 자체 보안 강화를 위해 작성되었으나, 오픈API 운영기관에서 오픈API 이용기관의 보안 적정성 판단 시 참고자료로 활용할 수 있다.(단, 활용 시 ②를 유의)

⑤ 본 가이드에 서술된 내용과 오픈API 이용기관에 적용되는 관련 법·시행령·감독규정 등에 서술된 내용이 상충될 경우 관련 법·시행령·감독규정 등의 서술내용이 우선한다.

4. 용어

본 가이드에서 사용된 용어는 본문에서 정한 바를 따르며 그 외 용어는 「전자금융거래법」, 「전자금융거래법 시행령」, 「전자금융감독규정」, 「전자금융감독규정시행세칙」 등 관련 법·시행령·감독규정에서 정의한 용어 정의를 따른다.

가이드에 기술된 주요 용어에 대한 정의는 다음과 같다.

용 어	정 의
운영기관	오픈API를 제공하는 오픈API시스템 운영기관(금융회사 등)을 의미
이용기관	오픈API를 이용하여 서비스를 개발 및 제공하는 기관(핀테크기업 등)을 의미
오픈API 이용서비스	이용기관이 오픈API를 이용하여 제공하는 서비스(예: 계좌잔액조회, 거래내역분석, 송금 등)
사용자	오픈API 이용서비스를 제공하는 이용기관의 업무 관계자
이용자	이용기관의 오픈API 이용서비스를 이용하는 고객
오픈API 접근서버	오픈API에 접근하는 이용기관 서버
오픈API 이용 애플리케이션	오픈API를 이용하여 이용자에게 서비스를 제공하는 이용기관 애플리케이션(모바일앱/웹애플리케이션 등)
오픈API 인증키	오픈API 이용서비스가 운영기관 오픈API시스템에 등록된 정당한 서비스임을 인증하는데 사용되는 운영기관으로부터 발급받은 특정값 또는 파일

오픈API 접근키	오픈API에 자원을 요청할 수 있는 권한이 부여된 특정값 또는 파일(예를 들어 OAuth 구조의 access token이 이에 해당)
오픈API 관련 중요정보	이용기관이 오픈API 이용서비스를 제공하는데 사용되는 보호가 필요한 중요정보 - 이용자 개인·신용정보 및 인증정보, 오픈API 이용 관련 인증정보 (오픈API 인증키, 오픈API 접근키 등), 암호키 등
오픈API 관련 정보자산	이용기관이 오픈API 이용서비스를 제공하는데 사용되는 이용기관 보유 정보자산 - 서버, 네트워크장비, 정보보호시스템, DBMS, 단말기, 응용프로그램, 소프트웨어, 저장매체, 문서 등

5. 유지관리

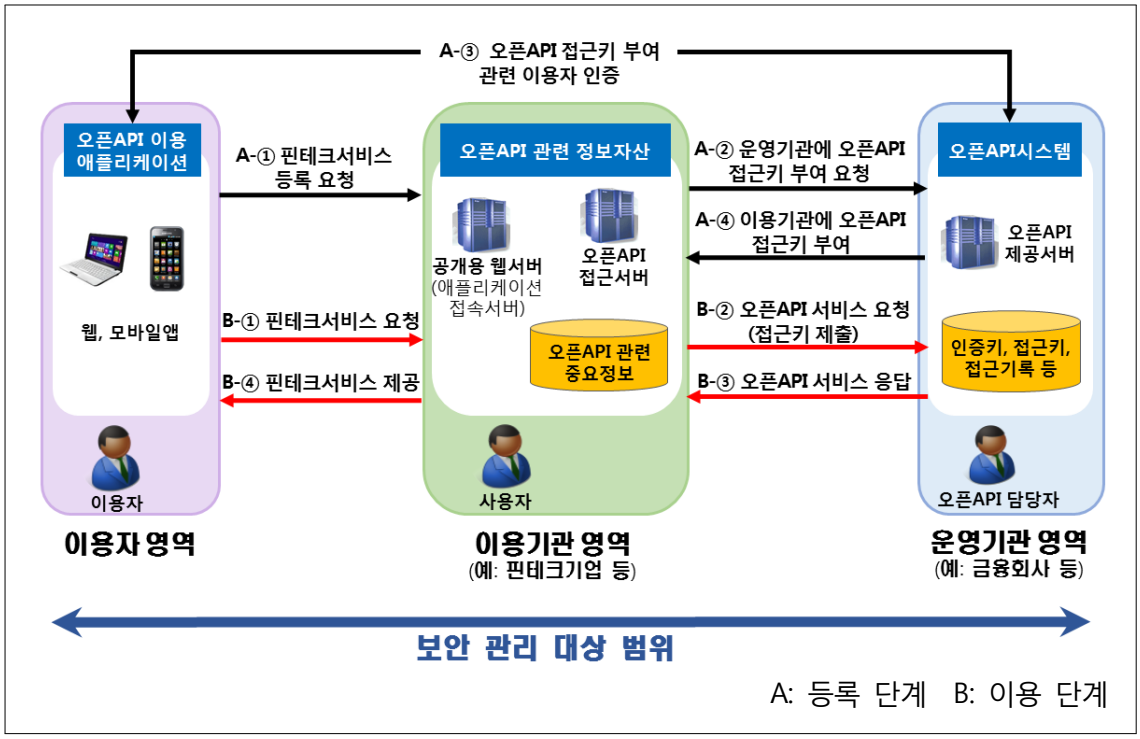
본 가이드는 기술의 변화, 관련 법령 및 감독규정 등의 중요 개정사항, 시장의 요구 등에 따라 개정 필요성이 검토될 경우 개정될 수 있다.

Ⅱ. 오픈API 이용 구조 및 주요 위험

1. 금융권 오픈API 이용 구조

계좌잔액조회, 거래내역조회, 예금주조회, 출금지시, 가상계좌발급 등 이용하는 API의 종류, 오픈API시스템 설계, 비즈니스 특성 등에 따라 금융권 오픈API 이용 구조는 다양할 수 있다. 아래 그림은 국내외에서 일반적으로 활용되고 있는 금융권 오픈API 이용 구조의 예를 보여준다.

<금융권 오픈API 이용 구조의 예>



◆ 등록 단계 (A)

① 이용자는 이용기관에 오픈API 이용 핀테크서비스(예: 계좌잔액조회, 거래내역 조회 등) 등록을 요청한다.
② 이용기관은 운영기관에 해당 이용자에 대한 오픈API 접근키 부여를 요청한다.
③ 운영기관은 오픈API 접근키 부여에 앞서 이용자 인증을 수행한다.
④ 운영기관은 오픈API 접근키를 이용기관에 부여한다.

◆ 이용 단계 (B)

① 이용자가 이용기관에 오픈API 이용 핀테크서비스(예: 계좌잔액조회)를 요청한다.
② 이용기관은 등록 단계에서 부여받은 오픈API 접근키를 운영기관에 제출하고 오픈API 서비스(예: 이용자 계좌잔액정보 제공)를 요청(호출)한다.
③ 운영기관은 해당되는 오픈API 서비스 응답을 이용기관에 제공한다.
④ 이용기관은 ③에서 수신된 이용자 정보를 활용하여 이용자에 서비스를 제공한다.

기존의 전통적인 금융회사 전자금융서비스(예: 인터넷뱅킹)의 이용 구조에서는 거래 주체는 고객과 금융회사만 존재한다. 하지만, 금융회사의 오픈API를 이용하는 구조에서는 고객(이용자)과 금융회사(운영기관) 사이에 이용기관이 추가로 존재한다. 이에 따라 보안 관리 대상 범위가 기존에 비해 확대되며 이를 고려한 종합적인 위험관리가 필요하다.

2. 주요 위험 및 보안 대책 예시

일반적인 금융권 오픈API 이용 구조에서 이용기관의 보안 관리 대상은 운영기관 영역을 제외한 이용자 영역 및 이용기관 영역이다. 해당 영역별로 발생 가능한 주요 위험 및 이를 제거 또는 완화할 수 있는 각 주체별(이용자, 이용기관, 운영기관) 보안 대책 예시는 아래와 같다. 이 외에도 적용 기술(인증, 통신 등), 구조적 특징 등에 따라 다른 위험이 추가로 존재할 수 있다.

가. 이용자 영역

위험	설명/영향	보안 대책(예시)
이용자 단말기의 악성코드 감염	악성코드에 단말기가 감염되어, 이용자 데이터 및 인증정보가 침해되거나 부정행위 발생 가능	**(이용자)** - 악성코드에 감염되지 않도록 단말기를 안전하게 관리
		(이용기관) - 악성코드 감염 예방에 관련된 이용자 교육 - 서비스 애플리케이션 실행 시 안티바이러스 프로그램 실행 및 감염 여부 확인 - 감염된 단말기의 서비스 요청을 거부 - 정상 서비스 애플리케이션임을 이용자에게 증명할 수 있는 대책 마련(개인화된 정보 표시 등) - 이상거래 모니터링
		(운영기관) - 단말기 감염 여부에 대한 정보 수신이 가능한 경우 해당 단말기의 API 요청 거부 - 고위험 요청에 대한 OOB*인증 또는 알림 * OOB(Out-of-band): 정의된 통신 주파수 대역 밖의 활동 또는 메인 네트워크/채널이 아닌 경로를 통한 이용자 인증(멀티팩터 인증에 사용됨)
변조 애플리케이션 유통	악의적으로 변조된 애플리케이션 이용 시 이용자 데이터 및 인증정보가 침해되거나 부정행위 발생 가능	**(이용자)** - 정상적인 유통 경로를 통한 애플리케이션 이용
		(이용기관) - 애플리케이션 위변조 방지 대책 마련 - 정상적인 웹사이트임을 이용자에게 증명할 수 있는 대책 마련(HTTPS를 적용하여 웹서버 정보 제공 등)

위험	설명/영향	보안 대책(예시)
서비스 애플리케이션 취약점을 통한 악의적 행위 시도	공격자가 서비스 애플리케이션 취약점을 악용하여 이용자 데이터 침해, 부정행위, 서비스 이용 불능 공격 시도 가능	**(이용기관)** - 애플리케이션 설계 단계부터 보안 명세를 명확히 하고, 개발 완료 시 해당 보안 요구사항을 만족하는지 검증하며, 알려진 취약점이 존재하지 않도록 보완하여 배포 - 배포 후 개발 변경 발생 시 취약점이 존재하지 않도록 관리 - 이상거래 모니터링
		(운영기관) - 이상거래 모니터링
이용기관 권한부여에 대한 이용자의 인식 부족	이용자가 제3자 권한 부여에 대한 내용을 충분히 숙지하지 않거나 잘못 이해했을 때 발생 가능한 위험 (의도치 않게 과도한 권한 부여, 부정행위 발생 시 이용자가 승인 내용을 이해하지 못했다고 할 경우 책임 문제 등)	**(이용자)** - 제3자 권한 부여를 동의하는 단계에서 동의 내용을 명확히 이해하고 권한 관리
		(이용기관) - 이용자를 대상으로 권한 부여 내용을 적절히 안내하고 상시 확인 가능하도록 홈페이지 등에 공개
		(운영기관) - 권한 부여 내용 및 이용약관 형식에 대해 이용기관에 명확한 표준 등 제시 - 권한 부여를 위한 인증 단계에서 관련 내용을 이해하기 쉽고 명확하게 이용자 화면에 표시 - 핵심 인증정보 변경, 이용자 계좌에 대한 부정 의심 행위 탐지 등의 경우 이용자에게 권한을 검토하도록 요청
정상적으로 획득한 계좌 정보의 침해	API를 통해 정상적인 방법으로 획득한 계좌 정보가 이용자 단말기에 저장된 이후 침해	**(이용자)** - 단말기를 안전하게 관리
		(이용기관) - 단말기에서 구동되는 애플리케이션을 안전하게 구현하고, 단말기 내 저장 정보를 최소화하고 중요 정보는 암호화 적용

위험	설명/영향	보안 대책(예시)
공격자가 이메일 피싱과 가짜 사이트를 통해 이용기관으로 가장	고객 데이터 침해와 부정행위 발생이 가능하며, 신뢰도 저하로 인하여 이용자 확대 제한	**(이용자)** - 사이트 인증서 등을 확인하여 정상 사이트 여부 확인 - 관련 위험에 대한 인식 및 발견 시 신고
		(이용기관, 운영기관) - 이용자 교육 - 피싱사이트가 탐지 및 차단되도록 이용기관 및 운영기관이 조직적으로 협력 대응 - 고위험 금융거래 행위(예: 수취인 등록, 지급 개시) 시 OOB 확인 요구 - 피싱을 방지하기 위한 대책(예: DMARC*)을 고려 * DMARC(Domain-based Message Authentication, Reporting & Conformance) : 이메일 발송지의 도메인 검사
공격자가 가짜 애플리케이션 개발 및 이용기관으로 가장	고객 데이터 침해와 부정행위 발생이 가능하며, 신뢰도 저하로 인하여 이용자 확대 제한	**(이용자)** - 공식 배포처를 이용하여 애플리케이션 설치 및 이용 - 관련 위험에 대한 인식 및 발견 시 신고
		(이용기관, 운영기관) - 이용자 교육 - 피싱 애플리케이션에 대해 조직적으로 협력 대응 - 고위험 금융거래 행위(예: 수취인 등록, 지급 개시) 시 OOB 확인 요구
공격자가 가짜 운영기관으로 가장	운영기관 인증페이지를 위장하여 악의적 애플리케이션 유통 고객 데이터 및 인증정보 침해와 부정행위 발생이 가능하며, 신뢰도 저하로 인하여 이용자 확대 제한	**(이용자)** - 공식 배포처를 이용하여 애플리케이션 설치 및 이용 - 인증을 위한 운영기관 인증페이지에 인증정보 입력 전 정상적인 운영기관 사이트인지 확인(예: 접속 페이지 도메인 확인, 브라우저 내 자물쇠 확인, 인증서 확인 등) - 관련 위험에 대한 인식 및 발견 시 신고
		(이용기관) - 이용자가 정상 운영기관 사이트를 확인할 수 있는 형태로 운영기관 인증 페이지를 호출하도록 애플리케이션 개발 - 피싱 사이트 및 애플리케이션에 대해 운영기관과 협력 대응
		(운영기관) - 이용자 교육 - 이용기관 애플리케이션 개발 시 운영기관 사이트를 안전한 형태로 호출하도록 개발 방식을 안내하고, 위험성이 있는 형태(예. 웹애플리케이션의 frame 내 인증페이지 요청 등)를 최대한 지원하지 않도록 API 구현

위험	설명/영향	보안 대책(예시)
보이스 피싱 위험 증가	이용기관/운영기관의 평판이 하락할 수 있으며, 신뢰도 저하로 인하여 이용자 확대 제한	**(이용자)** - 관련 위험에 대한 인식 및 신고
		(이용기관) - 이용자 교육 - 이용자가 이용기관을 식별할 수 있는 일관된 절차를 적용
		(운영기관) - 이용자 교육 - 이용자가 운영기관을 식별할 수 있는 일관된 절차를 적용
공격자가 계좌 소유주를 사칭하여 이용기관에 등록 (예: 다른 경로로 획득한 개인 식별정보 활용)	공격자가 이용기관을 통해 사칭한 이용자 계좌에 접근하는 경우, 고객 데이터 침해와 부정행위 발생이 가능하며 신뢰도 감소로 인하여 이용자 확대 제한	**(이용기관)** - 이용자 서비스 등록 시 안전한 인증 절차를 적용하여 타인 정보 도용을 통한 서비스 이용 방지
		(운영기관) - 이용기관에 중요 데이터에 접근할 권한을 부여하기 전, 운영기관의 인증 방법을 사용하여 이용자를 인증
이용자 단말기의 도난/분실	공격자가 단말의 불충분한 인증통제 약점을 악용하여 단말기 소유주의 앱/소프트웨어/서비스에 접근할 경우, 고객 데이터 침해와 부정행위 발생이 가능하며, 신뢰도 감소로 인하여 이용자 확대 제한	**(이용자)** - 단말기에 잠금 설정, 앱 사용 후 로그아웃 등 안전조치를 취하고, 도난/분실 시 금융거래 위험이 있을 경우 해당 금융서비스 이용 중지 요청
		(이용기관) - 가급적 이용자 단말기에 데이터를 저장하는 것을 피하고 저장데이터는 민감하지 않은 데이터로 제한 - 단말기를 획득한 공격자가 이용자로 가장하는 것을 방지하기 위해 이용기관은 적절한 인증통제를 적용 - 민감 데이터의 유통을 최소화하기 위하여 별도의 레이블을 사용(예: 계좌번호 대신 계좌별칭)하는 등 사회공학적 공격에 대응

나. 이용기관 영역

위험	설명/영향	보안 대책(예시)
오픈API 관련 정보처리시스템의 악성코드 감염	대량의 이용자 데이터 및 인증정보가 침해되거나 부정행위 발생 가능	**(이용기관)** - 오픈API 관련 정보처리시스템에 대한 악성코드 감염 방지 대책 마련 및 적용 **(운영기관)** - 고위험 금융거래 요청에 대한 OOB인증/인가 시도 - 이상거래 모니터링
정상적으로 획득한 계좌 정보의 침해	API를 통해 정상적인 방법으로 획득한 계좌 정보가 이용기관 시스템에 저장된 이후 침해될 위험	**(이용기관)** - API를 통해 획득한 이용자의 계좌 관련 정보를 안전하게 보호하기 위한 대책 마련 및 적용
API 데이터를 제3자에 제공하는 이용기관에 대한 관리 미흡	이용기관이 보안 수준이 검증되지 않은 제3의 주체에 API 데이터를 제공하는 경우, 고객정보의 침해 위험이 증가하며, 고객정보가 침해되거나 부정행위가 발생 시 책임 소재가 모호할 수 있음	**(이용기관)** - 이용기관으로부터 데이터를 전달받는 제3의 주체에 대해 데이터 보호 역량 확인 및 계약 시 사고에 대한 책임을 계약서에 명시 **(운영기관)** - 제3자에 API 데이터를 전달하는 방법을 관리하는 규칙을 포함하여, 전달 체인에 참여하는 당사자들의 보안 요구사항을 명확히 함 - 보안 점검을 받지 않거나 인가되지 않은 주체가 API를 통해 획득한 데이터를 처리하지 않도록 관리
이용기관 시스템의 침해로 인한 오픈API 접근키의 대규모 도난 발생	오픈API 접근키는 데이터와 서비스에 접근하는 핵심 데이터로, 유출시 고객 데이터의 대규모 침해와 부정사용 발생이 가능	**(이용기관)** - 시스템이 비인가 접근으로부터 보호되도록 보안 표준 적용 - 오픈API 접근키를 보호하기 위한 대책(예: 암호화 저장 등) 적용 **(운영기관)** - 고위험 거래 API에 대해서는 가급적 유효기간이 짧은 접근키를 부여 - 탈취된 접근키의 악용을 막기 위해 기술적 대책을 적용 (예: IP화이트리스트, TLS 상호 인증을 통한 이용기관 오픈API 접근서버 인증)

위험	설명/영향	보안 대책(예시)
이용기관을 사회공학적 공격 대상으로 선택	공격자는 이용자의 계좌정보 등을 얻기 위해 이용기관을 대상으로 사회공학적 공격을 실행할 수 있으며(예: 비밀번호 초기화 요청), 이를 통해 고객 정보의 침해 및 부정행위 발생 가능	**(이용기관)** - 이용기관 고객 서비스 담당 직원을 대상으로 사회공학적 공격 관련 교육 - 고객 서비스 지원 과정에서 견고한 이용자 인증을 요구
오픈API 이용 애플리케이션 침해/오류로 인한 비정상적 API요청	오픈API를 이용하는 애플리케이션이 침해되거나 오류가 발생하여 계획되지 않은 동작을 할 경우 운영기관 시스템에 악영향을 미칠 수 있음	**(이용기관)** - 오픈API 이용 애플리케이션에 대한 위변조 방지, 접근 통제, 변경관리 등 통제 대책 마련 - 이상행위 모니터링 **(운영기관)** - 과도한 API요청 등 이상행위 모니터링

3. 오픈API 이용기관 주요 보안 요구사항

2절에 예시된 오픈API 관련 주요 위험 및 보안 대책을 바탕으로, 이용기관의 오픈API 이용에 따른 주요 보안 요구사항을 아래와 같이 정리해 볼 수 있다.

- ▫ 이용자 단말기 악성코드 감염 방지·대응
- ▫ 이용자 단말기 도난·분실 대응
- ▫ 이용자 단말기 내 오픈API를 통해 수집한 개인·신용정보 유출 및 도용 방지
- ▫ 변조 애플리케이션 유통 및 피싱사이트 방지
- ▫ 오픈API 이용 애플리케이션 취약점 방지
- ▫ 오픈API 접근키와 관련한 이용자 보호 대책
- ▫ 피싱 등 이용자의 사기 피해 예방·탐지·대응
- ▫ 오픈API 관련 정보자산에 대한 보호(악성코드 감염, 시스템 침해사고, 오픈API 관련 중요정보 유출 등에 대한 예방·탐지·대응)
- ▫ 오픈API를 통해 수집한 개인·신용정보에 대한 제3자 제공·위탁 관련 보호 대책 마련
- ▫ 타인의 개인정보 도용을 통한 비인가 서비스 이용 방지
- ▫ 이용기관 내 사용자을 대상으로 한 사회공학적 공격에 대한 대책 마련
- ▫ 이상거래를 포함한 보안사고에 대한 대응(기록, 탐지, 대응, 복구, 정보 공유, 이용자 보상 등)
- ▫ 오픈API 이용 애플리케이션의 침해 또는 오류로 인한 비정상적 오픈API 접근 방지
- ▫ 악의적 행위자(이용기관 내부직원 또는 외부자)에 의한 오픈API 관련 정보자산 접근, 변조, 유출 등의 위협 방지

상기 주요 보안 요구사항은 금융 오픈API 이용과 관련된 사항들로 이용기관 조직 전체에 대한 모든 보안 요구사항을 포함하고 있는 것은 아니다. 이용기관은 오픈API 이용과 별개로 이용자 대상 서비스 제공자로서 이용자의 중요정보(개인·신용정보, 인증정보 등)를 안전하게 처리하고, 금융서비스를 안전하게 제공하기 위한 관리적·물리적·기술적 보호대책 마련이 요구된다. 따라서 이용기관은 서비스에 따라 적용되는 법령을 파악하고 관련 가이드 등을 참고하여, 오픈API 이용서비스에 적합한 보안 요구사항을 종합적으로 도출하고 만족시킬 수 있어야 한다. 이를 위하여

이용기관은 자체적으로 보안점검 항목을 도출하고 이행 여부를 점검하여 보안대책의 적정성을 주기적으로 검토·보완하는 노력이 필요하다.

《 관련 법령 및 가이드 》

☐ **관련 법령**

- 전자금융거래법, 신용정보법, 개인정보 보호법, 정보통신망법, 전자상거래법, 위치정보법, 금융실명법 등

☐ **관련 가이드**

발간처	가이드, 해설서 등	내용
금융위원회	금융분야 개인정보보호 가이드라인	- 개인·신용정보 처리단계별 유의사항
방송통신위원회	개인정보의 기술적·관리적 보호조치 기준 해설서	- 개인정보에 대한 표시제한 보호조치(마스킹) 권고, 개인정보 보호 고려사항 등
방송통신위원회	바이오정보보호 가이드라인	- 바이오정보 수집, 이용시 조치사항
방송통신위원회	스마트폰 앱 접근권한 개인정보보호 안내서	- 스마트폰 앱 접근권한 관련 필요한 구체적인 조치사항 안내
은행연합회	금융실명거래 업무해설	- 비대면거래시 본인확인 방법 규정
금융보안원	금융서비스 바이오정보 인증·관리 가이드라인	- 바이오정보 인증, 관리 시 유의사항
행정안전부	개인정보의 안전성 확보조치 기준 해설서	- 개인정보 안전성 확보조치 기준에 대한 해설
행정안전부	개인정보보호 법령 및 지침·고시 해설	- 개인정보관련 법령에 대한 해설
행정안전부	개인정보 수집 최소화 가이드라인	- 불필요한 개인정보 수집 관행 개선을 위한 권고 내용 등
행정안전부	시스템 개발·운영자를 위한 개인정보보호 가이드라인	- 개발자를 위한 개인정보보호 수칙 등을 수록
…	…	…

※ [출처] 스마트폰 전자금융서비스 보안 가이드 (금융보안원, 2018)

Ⅲ. 보안점검 항목

1. 보안점검 항목 예시

이번 장에서는 Ⅱ장에서 언급한 바와 같이 이용기관에서 자체적으로 보안 요구사항 만족 여부를 점검하는 경우 일반적으로 참고할 수 있는 보안 점검 항목을 예시한다. 오픈API 이용 구조나 서비스 종류·특징 등에 따라 보안 요구사항은 상이할 수 있으므로 자체 보안점검시에는 가이드의 보안 점검 항목은 참고자료로써 활용하고 오픈API 이용서비스에 맞는 보안점검 항목을 개별적으로 구성하여 점검하는 것을 권고한다.

일반적으로 적용할 수 있는 이용기관 보안점검 항목은 아래와 같다.

《 보안점검 항목 예시 》

보안영역	점검분야	보안점검 항목
관리	**1. 정보보호 정책·조직**	1.1 정보보호최고책임자 지정 및 실무조직
		1.2 정보보호정책 수립 및 공표
	2. 외부자 관리	2.1 위탁업체 선정 및 관리
	3. 정보자산 관리	3.1 정보자산 식별 및 등급부여
		3.2 정보자산별 책임자 지정
	4. 정보보호 교육	4.1 정보보호 교육계획 수립 및 이행
		4.2 실무자 정보보호 교육 이수
	5. 인적 보안	5.1 비밀유지서약서
		5.2 직무분리
		5.3 퇴직 및 직무변경 관리
	6. 위험 관리	6.1 취약점 점검 정책 수립 및 점검 수행
	7. 침해사고 대응	7.1 침해사고 대응절차 마련 및 교육 시행
		7.2 침해사고 대응 관련 로그 보존 및 모니터링

	8. 장애 대응	8.1 백업정책 수립 및 복구절차 마련
	9. 이용자 보호	9.1 개인정보 처리 관련 이용자 보호
		9.2 개인·신용정보 접근 및 거래지시 권한 관련 안내
		9.3 이용자 고충 처리방침 마련 및 공개
		9.4 이용자 보안 주의사항 안내
물리	**10. 물리적 보안**	10.1 보호구역 지정 및 출입 통제
		10.2 보호구역 반출입 관리
		10.3 사무실 환경 보안 정책 수립 및 이행
기술	**11. 개발 보안**	11.1 설계 시 보안 요구사항 도출 및 반영
		11.2 시큐어 코딩 적용 및 보안 취약점 점검·보완
		11.3 테스트 시 이용자 개인·신용정보 사용 제한
		11.4 소스 프로그램 및 전산원장 대상 접근·변경 통제
	12. 암호 통제	12.1 중요 정보 암호화 정책 수립 및 이행
	13. 접근 통제	13.1 중요 정보자산 계정 및 접근 권한 관리
		13.2 중요 단말기 지정 및 접근 통제
	14. 시스템 보안	14.1 주요 시스템 등의 악성코드 감염 및 정보유출 방지
		14.2 인터넷망을 통한 원격관리 통제
		14.3 주요 시스템 목적 외 기능·프로그램·포트 등 제거
		14.4 중요 서버 독립 운영 및 정보보호시스템 적용
		14.5 공개용 웹서버 보호대책 마련
		14.6 중요 보안패치 적용 지침 수립 및 이행
	15. 네트워크 보안	15.1 DMZ 구간 구성
		15.2 내부망 사설IP 활용 및 주요 시스템 배치
		15.3 무선 네트워크 이용 최소화 및 보안대책 수립·적용
		15.4 대외기관과 통신 시 보안통신 적용

2. 세부 점검항목

1절에 예시된 보안점검 항목을 기반으로 자체 보안점검을 수행할 경우, 보다 효율적인 점검이 이루어지도록 지원하기 위하여 세부 점검항목과 이에 대한 세부설명을 서술한다.

보안영역	관리	점검분야	1. 정보보호 정책·조직
보안점검 항목	1.1 정보보호최고책임자 지정 및 실무조직		
세부 점검항목	1.1.1 정보보호최고책임자를 지정하고, 실무조직을 구성하고 있다.		
세부설명	• 최고경영자는 조직의 정보보호 관련 업무를 총괄 관리할 수 있도록 정보보호최고책임자를 지정하여 조직의 정보보호를 관리하여야 한다. • 책임자의 역할을 지원하고 조직의 정보보호 활동을 체계적으로 이행하기 위한 전문성을 가진 실무조직*을 구성하여야 한다. * 정보보호산업법 시행규칙 <별표 1>에서 서술한 초급 이상 기술인력을 1명 이상 포함 권고 • 종업원 수가 적은 소규모 조직의 경우 법적 요구사항 및 조직 내 업무분장 등을 감안하여 조직에 맞게 정보보호 조직을 구성한다. ※ 예) 정보보호최고책임자 1인으로 실무조직 구성, 최고경영자가 정보보호최고책임자 겸임 등 **【점검 자료의 예】** • 정보보호최고책임자 지정을 확인할 수 있는 문서 - 최고경영자의 결재(또는 서명)가 있는 임명장, 인사발령서 등 • 정보보호 조직 구성 및 역할이 반영된 규정 또는 지침 • 정보보호 실무조직 인력의 정보보호 전문성을 확인할 수 있는 문서 - 학위, 자격증, 경력증명서 등 **【참고 법규】** • 전자금융거래법 제21조의2(정보보호최고책임자 지정) • 전자금융거래법 시행령 제11조의3(정보보호최고책임자 지정대상 금융회사 등) • 전자금융감독규정 제6조의2(정보보호최고책임자의 지정대상) • 개인정보 보호법 제31조(개인정보 보호책임자의 지정) • 정보통신망법 제27조(개인정보 보호책임자의 지정)		

보안영역	관리	점검분야	1. 정보보호 정책・조직
보안점검 항목	1.1 정보보호최고책임자 지정 및 실무조직		
세부 점검항목	1.1.2 정보보호최고책임자 및 실무조직은 정보보안 점검항목을 마련하고 정기적으로 점검하고 있다.		
세부설명	• 정보보호최고책임자는 정보보안 점검항목* 준수여부를 적절한 주기(예: 분기당 1회 이상)로 점검하여야 한다. *「전자금융감독규정」 시행세칙 <별표 3-2> 정보보안 점검항목, 정보통신망법에서 명시한 '정보보호조치에 관한 지침' 등을 참고하여 조직에 맞는 점검항목 수립 • 점검 결과는 정보보호최고책임자의 결재를 득하고, 최고경영자에게 보고되어야 한다. **【점검 자료의 예】** • 정보보안 점검항목 수립 문서 • 정보보안 점검항목에 따른 점검 실시 결과 **【참고 법규】** • 전자금융감독규정 제37조의5(정보보호최고책임자의 업무) • 전자금융감독규정 시행세칙 제7조의3(정보보호최고책임자의 업무) • 정보통신망법 제45조(정보통신망의 안전성 확보 등)		

<table>
<tr><td>보안영역</td><td>관리</td><td>점검분야</td><td>1. 정보보호 정책·조직</td></tr>
<tr><td>보안점검 항목</td><td colspan="3">1.2 정보보호정책 수립 및 공표</td></tr>
<tr><td>세부 점검항목</td><td colspan="3">1.2.1 정보보호정책 및 정책시행 문서를 수립하여 문서화하고, 이를 임직원에게 공표하고 있다.</td></tr>
<tr><td>세부설명</td><td colspan="3">• 조직이 수행하는 모든 정보보호 활동의 근거가 될 수 있도록 다음과 같은 항목이 포함된 최상위 수준의 정보보호정책을 수립하고 최고경영자의 승인을 득하여야 한다.

《 포함 내용의 예 》
- 경영진의 정보보호에 대한 의지 및 방향
- 조직의 정보보호 목적, 범위, 책임
- 조직이 수행하는 정보보호 활동의 근거
- 조직이 준수해야 하는 법령 및 관련조항 등

• 또한 정보보호정책을 시행하기 위한 수행주체, 방법, 절차 등의 세부내용을 포함하는 정책시행 문서*를 수립하고 정보보호최고책임자의 승인을 득하여야 한다.
* 지침, 절차, 매뉴얼 등의 형태
- 임직원의 정보보호에 대한 경각심을 높일 수 있도록 임직원의 역할 및 책임, 정보보호 규정 위반 시 제재 사항 포함을 권고

• 정보보호정책 및 정책시행 문서를 임직원이 알 수 있도록 공표*하고 수시로 최신 문서를 확인할 수 있도록 제공하여야 한다.
* 교육, 메일, 게시판 등 활용

【점검 자료의 예】
• 정보보호정책 및 정책시행 문서
• 임직원 대상 정보보호정책 및 정책시행 문서의 공표 현황을 확인할 수 있는 자료(게시물 화면, 배포 문건 등)

【참고 법규】
• 정보보호 관리체계 인증 등에 관한 고시 제21조(인증심사 방법 및 보완조치)</td></tr>
</table>

<table>
<tr><td>보안영역</td><td>관리</td><td>점검분야</td><td>2. 외부자 관리</td></tr>
<tr><td>보안점검 항목</td><td colspan="3">2.1 위탁업체 선정 및 관리</td></tr>
<tr><td>세부 점검항목</td><td colspan="3">2.1.1 위탁업체 선정 시 보안 요구사항을 정의하여 계약서에 반영하고 있다.</td></tr>
<tr><td>세부설명</td><td colspan="3">• 정보처리 업무를 외부자에게 위탁하거나 정보자산에 대한 접근을 허용할 경우, 또는 업무를 위해 클라우드 서비스 등 외부 서비스를 이용하는 경우에는 보안 요구사항을 식별하고 관련 내용을 계약서 및 협정서 등에 명시해야 한다.

《 위탁업체 보안 요구사항의 예 》
- 관련 법령 및 내규 준수
- 정보보호서약서 제출(비밀유지, 정보보호 책임 등)
- 중요정보 유출 방지 대책
- 접근통제 대책(정보자산 접속제한, 반출입제한, 휴대용 단말보안 등)
- 정보보호 교육 수행
- 재위탁, 인력 변경 제한
- 보안요구사항 준수 여부 점검
- 보안요구사항 위반 시 처벌 및 손해배상 등

《 참고 자료 》
- 클라우드 서비스를 위한 SLA가이드, 방송통신위원회
- 클라우드 표준계약서(B2B, B2C), 과학기술정보통신부

- 외부자 업무형태에 따라 보안 요구사항을 계약서에 충분하게 반영하지 못할 경우 타당한 사유가 존재해야 한다.

• 계약서에 명시된 보안 요구사항의 준수 여부를 정기적으로 점검하여야 한다.

【점검 자료의 예】
• 위탁 관련 정보보호정책 또는 정책시행 문서
• 위탁 계약서 또는 협정서
• 위탁업체 대상 보안 요구사항 준수 여부 점검 결과 문서

【참고 법규】
• 개인정보 보호법 제26조(업무위탁에 따른 개인정보의 처리 제한)</td></tr>
</table>

	• 표준 개인정보 보호지침 제15조(개인정보취급자에 대한 감독) • 전자금융감독규정 제21조(정보처리시스템 구축 및 전자금융거래 관련 계약) 제2호, 제60조(외부주문등에 대한 기준) 제1항 • 개인정보의 기술적·관리적 보호조치 기준 제3조(내부관리계획의 수립·시행) 제1항 제5호

<table>
<tr><td>보안영역</td><td>관리</td><td>점검분야</td><td>2. 외부자 관리</td></tr>
<tr><td>보안점검 항목</td><td colspan="3">2.1 위탁업체 선정 및 관리</td></tr>
<tr><td>세부 점검항목</td><td colspan="3">2.1.2 클라우드 서비스를 이용하는 경우 관련 위험을 파악하고 대응 방안을 수립하고 있다.</td></tr>
<tr><td>세부설명</td><td colspan="3">• 클라우드 서비스 이용에 따른 위험을 식별하고 대응 방안*을 수립하여 관리하여야 한다.
* 사고 발생 시 대응 절차, 책임 범위 및 보상 범위 등을 정리하여 문서화

《 클라우드 컴퓨팅 보안위협의 예 》
• 관리적 보안위협 : 클라우드 컴퓨팅 남용, 악의적인 내부자들, 공개되지 않은 위협, 클라우드 서비스 이해 부족, 불충분한 식별자, 권한 및 접근 관리, APT공격 등
• 기술적 보안위협 : 안전하지 않은 API, 가상화 취약점, 계정, 서비스 및 트래픽 탈취, 데이터 유·손실, 서비스 거부공격(DDoS), 시스템 취약점 등
※ 출처: 클라우드 정보보호 안내서, 한국인터넷진흥원

《 참고 자료 》
- 클라우드 정보보호 안내서, 한국인터넷진흥원
- 클라우드 표준계약서(B2B, B2C), 과학기술정보통신부

• 보안 관련 인증을 획득한 클라우드 서비스를 이용하여 보안 위험을 낮추는 것을 권장한다.

【점검 자료의 예】
• 클라우드 서비스 이용 계약서
• 클라우드 서비스 이용 관련 위험 관리 방안이 포함된 문서

【참고 법규】
• 클라우드컴퓨팅법 제4장 클라우드컴퓨팅서비스의 신뢰성 향상 및 이용자 보호
• 클라우드컴퓨팅서비스 정보보호에 관한 기준</td></tr>
</table>

<table>
<tr><td>보안영역</td><td>관리</td><td>점검분야</td><td colspan="2">3. 정보자산 관리</td></tr>
<tr><td>보안점검 항목</td><td colspan="4">3.1 정보자산 식별 및 등급부여</td></tr>
<tr><td>세부 점검항목</td><td colspan="4">3.1.1 오픈API 관련 정보자산을 식별하여 목록을 관리하고 보안등급을 부여하고 있다.</td></tr>
<tr><td>세부설명</td><td colspan="4">
• 오픈API를 이용한 서비스와 관련하여 정보보호 관리 대상이 되는 모든 정보자산을 식별하여야 한다. 또한 식별된 정보자산을 목록(시스템 또는 문서)으로 정리하여 체계적으로 관리하여야 한다.
- 정기적으로 정보자산 목록을 최신화하는 체계를 갖추고 이행해야 한다.

《 정보자산 목록 항목의 예 》
- 정보자산 분류*, 정보자산명, 자산번호, 모델명, 용도
* (예) 서버, 네트워크 장비, 정보보호시스템, 응용프로그램, DBMS, 단말기, 소프트웨어, 문서 등
- 정보자산별 책임자, 관리부서, 보안등급 등

• 식별된 정보자산에 대한 기밀성, 무결성, 가용성, 법적 요구사항 등을 고려하여 조직에 미치는 중요도를 자체적인 기준*을 마련하여 평가하고 그 중요도에 따라 보안등급을 부여하여야 한다.
* 예를 들어, 정보자산 별로 기밀성, 무결성, 가용성 각 항목에 대하여 점수(1~5)를 부여하고, 기타 요소 등을 가산하여 정보자산의 총 점수를 계산하고 점수별 등급 기준에 따라 보안등급을 부여하는 식으로 조직 자체 기준 마련
- 보안등급이 높은 정보자산에 대한 별도 취급절차를 정의하고 이에 따른 접근통제를 이행하여야 한다.
- 임직원이 보안등급을 쉽게 식별할 수 있도록 표시*하는 것을 권장한다.
* (예) 하드웨어 자산의 경우 자산번호 라벨링, 문서의 경우 대외비/기밀 표시 등

• 네트워크 구성도를 마련하고, 변경사항이 있을 경우 보완·관리하여 비상 시 빠른 대응을 취할 수 있도록 한다.
※ 해당 네트워크와 분리된 곳에 별도 관리(또는 사본 별도 보관) 권고

【점검 자료의 예】
• 정보자산목록 및 네트워크 구성도
• 정보자산목록 갱신 여부를 확인할 수 있는 문서
• 정보자산 보안등급별 취급절차 정의 문서
</td></tr>
</table>

	• 정보자산에 보안등급 표시 여부를 확인할 수 있는 자료 **【참고 법규】** • 전자금융감독규정 제13조(전산자료 보호대책) 제1항

보안영역	관리	점검분야	3. 정보자산 관리
보안점검 항목	3.2 정보자산별 책임자 지정		
세부 점검항목	3.2.1 정보자산 보안등급에 따라 책임자를 지정하고 식별 가능하도록 하여야 한다.		
세부설명	• 정보자산의 도입, 변경, 폐기, 반출입 등의 책임을 질 수 있는 식별된 정보자산에 대한 책임자를 지정하여 책임소재를 명확히 하여야 한다. • 책임자를 쉽게 식별할 수 있도록 정보자산에 표시하는 것을 권고한다. **【점검 자료의 예】** • 정보자산목록 • 정보자산에 책임자를 표시한 경우 해당 표시 확인 가능 자료 **【참고 법규】** • 전자금융감독규정 제13조(전산자료 보호대책) 제1항 제3호, 제14조(정보처리시스템 보호대책) 제6호		

<table>
<tr><td>보안영역</td><td>관리</td><td>점검분야</td><td colspan="2">4. 정보보호 교육</td></tr>
<tr><td>보안점검 항목</td><td colspan="4">4.1 정보보호 교육계획 수립 및 이행</td></tr>
<tr><td>세부 점검항목</td><td colspan="4">4.1.1 내외부 직원을 대상으로 정보보호 교육계획을 수립하고 시행하고 있다.</td></tr>
<tr><td>세부설명</td><td colspan="4">• 정보보호 교육의 시기, 기간, 대상, 내용, 방법 등의 내용이 포함된 연간 정보보호 교육계획을 수립하고 시행하여야 한다.
- 교육 대상으로 임직원 뿐만 아니라 업무를 위탁한 외부자를 포함하여야 한다.
- 가능한 정보자산에 직·간접적으로 접근하는 모든 인력을 대상에 포함하는 것을 권장한다.

《 정보보호 교육 내용의 예 》
- 정보보호 정책, 지침, 절차 등 정보보호 관련 내규
- 정보보호 관련 법률의 이해
- 침해사고 대응 절차
- 정보보호 규정 위반 시 상벌규정, 법적 책임 등

• 정보보호최고책임자(또는 최고경영자)가 정보보호 교육계획을 수립 및 시행하여야 한다.

【점검 자료의 예】
• 정보보호 교육계획 수립 문서
• 정보보호 교육 실시 결과 문서

【참고 법규】
• 전자금융감독규정 제19조의2(정보보호 교육계획의 수립 시행) 제1항
• 신용정보법 제17조(수집·조사 및 처리의 위탁) 제5항, 제20조(신용정보관리책임의 명확화 및 업무처리기록의 보존) 제4항 제5호
• 신용정보법 시행령 제14조(수집된 신용정보 처리의 위탁) 제5항
• 개인정보 보호법 제26조(업무위탁에 따른 개인정보의 처리 제한) 제4항, 제28조(개인정보취급자에 대한 감독), 제31조(개인정보 보호책임자의 지정) 제2항 제5호
• 정보통신망법 시행령 제15조(개인정보의 보호조치) 제1항
• 개인정보의 기술적·관리적 보호조치 기준 제3조(내부관리계획의 수립·시행) 제2항</td></tr>
</table>

<table>
<tr><td>보안영역</td><td>관리</td><td>점검분야</td><td>4. 정보보호 교육</td></tr>
<tr><td>보안점검 항목</td><td colspan="3">4.2 실무자 정보보호 교육 이수</td></tr>
<tr><td>세부 점검항목</td><td colspan="3">4.2.1 IT직무자(개발, 운영) 및 정보보호 직무자는 직무 수행에 필요한 정보보호 교육을 이수하고 있다.</td></tr>
<tr><td>세부설명</td><td colspan="3">• IT 및 정보보호 조직 내 임직원은 정보보호와 관련하여 직무별 전문성 제고를 위하여 필요한 별도의 교육*을 이수하여야 한다.
* 정보보호 관련 컨퍼런스·세미나·워크샵 참가, 전문기관 교육 수료 등

《 참고 자료 》
- 개인정보보호 교육
※ privacy.go.kr의 교육마당 참고
- 정보보호·개인정보보호 관리체계 교육
※ isms.kisa.or.kr의 온라인학습 참고
- KISA 사이버보안인재센터
※ academy.kisa.or.kr 참고

《 실무자 정보보호교육의 예 》
- IT 개발자 : 시큐어 코딩 교육
- IT 운영자 : 서버 보안 교육
- 정보보호 직무자 : 침해사고 대응 관련 전문 교육

• 특히 오픈API 이용 애플리케이션은 외부에 공개되어 공격에 쉽게 노출될 수 있으므로, IT개발자가 애플리케이션 시큐어 코딩 교육을 이수하는 것을 적극 권장한다.

【점검 자료의 예】
• IT 및 정보보호 직무자를 확인할 수 있는 자료
- 정보보호정책 시행문서, 조직도 등
• 직무자 정보보호 교육 이수 여부를 확인할 수 있는 자료

【참고 법규】
• 전자금융감독규정 제8조(인력, 조직 및 예산) 제1항 제3호</td></tr>
</table>

<table>
<tr><td>보안영역</td><td>관리</td><td>점검분야</td><td>5. 인적 보안</td></tr>
<tr><td>보안점검 항목</td><td colspan="3">5.1 비밀유지서약서</td></tr>
<tr><td>세부 점검항목</td><td colspan="3">5.1.1 내외부 직원 대상으로 비밀유지서약서를 받고 있다.</td></tr>
<tr><td>세부설명</td><td colspan="3">• 임직원 및 오픈API 관련 정보자산에 접근권한을 부여받은 외부자로부터 정보보호에 대한 책임 및 준수사항을 포함한 서명된 정보보호 서약서를 받아야 한다.

• 임직원 퇴직 및 외부자의 업무 종료 시, 직무 상 알게 된 조직의 중요정보에 대한 유출 방지를 위하여 서명된 비밀유지서약서를 받고, 유출 발생 시 그에 따르는 법적 책임이 있음을 상기시켜야 한다.

• 정보보호서약서 및 비밀유지서약서는 법적 분쟁 발생 시 법률적 책임에 대한 증거자료로 사용할 수 있기 때문에 안전하게 보관하고, 필요 시 용이하게 찾아볼 수 있도록 관리하는 것을 권고한다.

《 정보보호·비밀유지서약서 포함 내용의 예 》
- 조직 내 제 규정 준수
- 규정 미준수로 인한 사고 발생 시 처벌 또는 손해배상 책임
- 업무 목적 외 정보자산에 접근 금지
- 업무수행을 위해 제공받은 정보자산 등은 업무수행 후 반납 또는 폐기
- 중요정보 무단 복사 또는 유출 금지
- 퇴직 또는 업무 종료 시 비밀유지 및 비밀 유출에 따른 법적 책임 등

【점검 자료의 예】
• 조직도 및 임직원 정보보호·비밀유지서약서
• 위탁업체 계약서 및 외부자 정보보호·비밀유지서약서

【참고 법규】
• 표준 개인정보 보호지침 제15조(개인정보취급자에 대한 감독)
• 신용정보법 제42조(업무 목적 외 누설금지 등)</td></tr>
</table>

보안영역	관리	점검분야	5. 인적 보안
보안점검 항목	5.2 직무분리		
세부 점검항목	5.2.1 개발, 운영, 정보보호의 직무를 분리하고 있다.		
세부설명	• 직무의 권한 오남용을 예방하기 위하여 정보보호 관련 주요 직무 분리 기준을 수립·이행하고 직무별 역할과 책임을 명확하게 정의해야 한다. • 비인가 수정 등을 감소시키기 위하여 개발, 운영, 정보보호 관리 직무를 분리해야 한다. - 조직의 규모에 따라 가능한 경우 추가적으로 운영 직무 내 전산 시스템(서버, DB, 네트워크 등) 간 직무분리를 권고한다. • 조직 규모 등의 사유로 불가피하게 직무분리가 어려운 경우, 중요 정보자산 변경 등 위험성이 높은 업무 수행 시 직무자간 상호 검토, 상위관리자의 주기적인 직무수행 모니터링 및 변경 검토/승인, 직무자의 책임추적성 확보 등의 보완적인 통제수단을 마련해야 한다. **【점검 자료의 예】** • 직무분리 기준이 명시된 정보보호정책 또는 정책시행 문서 • 직무기술서 또는 업무명령서 **【참고 법규】** • 전자금융감독규정 제26조(직무의 분리)		

보안영역	관리	점검분야	5. 인적 보안
보안점검 항목	5.3 퇴직 및 직무변경 관리		
세부 점검항목	5.3.1 내외부 직원의 퇴직 및 직무변경 시 권한 관리를 적절히 수행하고 있다.		
세부설명	• 내외부 직원의 퇴직 및 직무 변경 시 오픈API 관련 정보자산에 접근권한을 조정 또는 회수하는 절차를 수립 및 운영하고 있다. • 부서 및 직무 변경, 휴직, 퇴직 등 인사 변경 발생 시 오픈API 관련 정보자산 접근권한의 변경·회수 등의 조치가 신속하게 이루어질 수 있도록 인사 부서(또는 담당자)는 변경내용을 정보보호부서 및 정보처리시스템 운영 부서 등에 신속히 공유하여야 한다. - 타당한 사유에 따라 불가피하게 계정을 공유하고 있는 경우, 해당 계정의 인증정보(비밀번호 등)를 변경해야 한다. **【점검 자료의 예】** • 접근권한 관리 기준이 포함된 정보보호정책 또는 정책시행 문서 • 최근 인사 변동(퇴직, 직무변경 등) 내역 • 최근 위탁에 따라 정보자산 접근권한이 허용된 외부자 정보 • 내외부 직원 대상 접근권한의 변경·회수 조치 기록 - 시스템별 계정 목록, 계정 신청·변경·회수 신청서 및 처리기록, 계정관리솔루션 기록 등 **【참고 법규】** • 전자금융감독규정 제13조(전산자료 보호대책) 제1항 제14호 • 표준 개인정보 보호지침 제15조(개인정보취급자에 대한 감독)		

보안영역	관리	점검분야	6. 위험 관리
보안점검 항목	6.1 취약점 점검 정책 수립 및 점검 수행		
세부 점검항목	6.1.1 중요 정보자산에 대해 취약점 점검 정책을 수립하고, 취약점 점검을 수행하고 있다.		
세부설명	• 오픈API 관련 정보처리시스템이 알려진 취약점에 노출되어 있는지 여부를 확인하기 위하여 취약점 점검 정책을 수립하고, 정기적으로(연 1회 이상) 취약점 점검*을 수행하여 위험을 관리하여야 한다. * 점검 대상 : 오픈API 관련 중요정보를 처리하는 서버, 서비스 응용프로그램(모바일앱/웹애플리케이션 포함) 등 - 가급적 오픈API 이용서비스와 관련된 기타 전산시스템(네트워크장비, 정보보호시스템 등)도 점검 대상에 포함하여 다층적 보안 대책이 안전하게 구현될 수 있도록 관리하는 것을 권장한다. • 취약점 점검 결과 발견된 취약점을 제거 또는 상응하는 보완조치를 수행하여야 한다. **《 참고 자료 》** - 주요정보통신기반시설 기술적 취약점 분석 평가 상세 가이드 - 홈페이지 취약점 진단제거 가이드 ※ kisa.or.kr의 자료실 > 관련법령·기술안내서 > 기술안내서가이드 참고 - OWASP Testing Guide - Mobile Security Testing Guide ※ OWASP(www.owasp.org) 참고 - 한국인터넷진흥원 중소기업 지원 서비스 ※ www.boho.or.kr의 보안서비스 참고 **【점검 자료의 예】** • 취약점 점검 정책이 포함된 정보보호정책 또는 정책시행 문서 • 취약점 점검 수행 결과 • 취약점 점검 결과에 따른 보완조치 결과		

	【참고 법규】 • 전자금융거래법 제21조의3(전자금융기반시설의 취약점 분석·평가) • 전자금융감독규정 제37조의2(전자금융기반시설의 취약점 분석·평가 주기, 내용 등) • 개인정보의 안전성 확보조치 기준 제6조(접근통제) 제4항

<table>
<tr><td>보안영역</td><td>관리</td><td>점검분야</td><td>7. 침해사고 대응</td></tr>
<tr><td>보안점검 항목</td><td colspan="3">7.1 침해사고 대응절차 마련 및 교육 시행</td></tr>
<tr><td>세부 점검항목</td><td colspan="3">7.1.1 침해사고 대응절차를 마련하고 있다.</td></tr>
<tr><td>세부설명</td><td colspan="3">• 침해사고 유형별 중요도 분류 및 보고·대응·복구 절차, 비상연락체계 등을 포함한 침해사고 대응 절차를 수립하여야 한다.
- 비상연락체계에 오픈API 운영기관을 포함하여 침해사고 발생시 운영기관이 오픈API에 대한 영향을 검토하고 대응할 수 있도록 한다.

《 침해사고 대응절차 내용의 예 》
- 침해사고의 정의 및 범위 (중요도 및 유형 포함)
- 침해사고 선포 절차 및 방법
- 비상연락체계 (오픈API 운영기관 포함)
- 침해사고 발생 시 기록 및 보고 절차
- 침해사고 신고 및 통지 절차 (관계 기관, 서비스 이용자 등)
- 침해사고 보고서 작성(발생일시,보고자,보고일시,사고내용,대응경과 등)
- 침해사고 대응 및 복구 절차
- 침해사고 복구조직의 구성 및 책임, 역할
- 침해사고 복구장비 및 자원 조달
- 외부 전문가나 전문기관(KISA 등)과의 협조체계
- 침해사고 대응 및 복구 훈련 계획 및 시나리오 등

《 침해사고 관련 참고 자료 》
- 침해사고대응팀(CERT) 구축/운영 안내서
- 침해사고 분석절차 안내서
※ kisa.or.kr의 자료실 > 관련법령·기술안내서 > 기술안내서가이드 참고

【점검 자료의 예】
• 침해사고 대응절차 관련 정책 또는 정책시행 문서

【참고 법규】
• 전자금융거래법 제21조의5(침해사고의 통지 등), 제21조의6(침해사고의 대응)
• 전자금융감독규정 제37조4(침해사고대응기관 지정 및 업무범위 등), 제73조(정보기술부문 및 전자금융 사고보고)
• 신용정보보호법 제39조의2(신용정보의 누설통지 등)
• 개인정보 보호법 제34조(개인정보 유출 통지 등)
• 정보통신망법 제27조의3(개인정보 유출등의 통지·신고), 제48조의3(침해사고의 신고 등), 제48조의4(침해사고의 원인 분석 등)</td></tr>
</table>

보안영역	관리	점검분야	7. 침해사고 대응
보안점검 항목	7.1 침해사고 대응절차 마련 및 교육 시행		
세부 점검항목	7.1.2 침해사고 대응 관련 교육을 실시하고 있다.		
세부설명	• 침해사고 대응절차를 임직원들이 숙지할 수 있도록 관련 교육을 실시하여야 한다. - 또한 침해사고 발생 시 처리가 종결된 후 해당 사고에 대한 정보와 발견된 취약점들을 관련 조직 및 임직원들과 공유하여 재발을 방지할 수 있도록 노력해야 한다. • 대응절차에 대한 임직원의 숙지 및 침해사고 대응절차에 대한 적정성·효과성을 평가하기 위하여 주기적으로 시나리오에 따라 침해사고 대응 모의훈련을 실시하고 대응절차를 보완하는 것을 권고한다. **【점검 자료의 예】** • 침해사고 대응절차 관련 정책 또는 정책시행 문서 • 침해사고 대응절차 관련 임직원 대상 교육 실시 내역 **【참고 법규】** • 전자금융감독규정 제37조4(침해사고대응기관지정 및 업무범위 등) 제5항		

보안영역	관리	점검분야	7. 침해사고 대응
보안점검 항목	7.2 침해사고 대응 관련 로그 보존 및 모니터링		
세부 점검항목	7.2.1 침해사고 대응에 필요한 로그를 일정기간 보존하고 주기적으로 검토하고 있다.		
세부설명	• 침해사고 분석 시 필요한 로그를 일정기간 보존하고 주기적으로 검토하여야 한다. - 법적 요구사항을 고려하여 보존기간 및 검토주기를 정한다. - 로그기록의 정확성을 보장하고 법적인 자료로서 효력을 지니기 위해 전산시스템 시각을 공식 표준시각으로 동기화하여야 한다. **《 침해사고 분석 시 필요 로그의 예 》** - 보안관련 감사로그 : 사용자의 접속기록(식별정보, 접속일시, 접속지, 수행업무 등), 인증 성공/실패 로그, 계정 및 권한 등록/변경/삭제 등 - 시스템 이벤트 로그 : 운영체제 구성요소에 의해 발생되는 로그(시스템 시작, 종료, 상태, 에러 등) - 정보보호시스템 정책(룰셋 등) 등록/변경/삭제 및 이벤트 로그 - 이용자 정보 및 전자금융거래 원장 등 중요정보 접속/조회/변경 로그 - 오픈API 이용 기록 등 • 자체적으로 업무의 중요도나 위험도를 검토하여 높다고 판단할 경우, 침해사고 탐지·대응을 실시간으로 수행하는 것을 권장한다. **【점검 자료의 예】** • 로그 보존 및 검토 기록 **【참고 법규】** • 전자금융감독규정 제12조(단말기 보호대책) 제2호, 제13조(전산자료 보호대책) 제1항~제4항, 제14조(정보처리시스템 보호대책) 제10호, 제15조(해킹 등 방지대책) 제2항~제3항, 제18조(IP 주소 관리대책) 제3호, 제27조(전산원장 통제) 제5항 • 개인정보의 안전성 확보조치 기준 제5조(접근권한의 관리) 제3항, 제8조(접속기록의 보관 및 점검) • 개인정보의 기술적·관리적 보호조치 기준 제5조(접속기록의 위·변조 방지) • 신용정보업감독규정 [별표 3] 기술적·물리적·관리적 보호대책 마련 기준 Ⅱ.기술적·물리적 보호대책 2.접속기록의 위·변조방지		

보안영역	관리	점검분야	8. 장애 대응
보안점검 항목	8.1 백업정책 수립 및 복구절차 마련		
세부 점검항목	8.1.1 IT 재해에 대비하여 복구 가능하도록 백업정책 및 복구절차를 수립하여 운영하고 있다.		
세부설명	• IT 재해 위험요인들(해킹, 시스템 결함, 화재 등)에 따른 장애에 대비하여 복구 가능하도록 주요 정보에 대한 복구절차를 수립하여야 한다. - 복구가 필요한 주요 정보는 오픈API 관련 중요정보, 침해사고 분석 시 필요 로그(7.2.1 참고), 고객DB, 복구에 필요한 기타 시스템 관련 정보(OS, DBMS 백업 등)를 포함한다. **《 IT 재해복구 체계 내용의 예 》** - 재해 시 복구조직/담당자 및 역할 정의 - 비상연락체계(담당자, 유지보수 업체 등) - 복구 대상 업무, 서비스, 시스템 식별 - 복구 순서 및 절차 등 • 복구 대상 데이터에 대해서 법적 요구사항*을 고려하여 백업정책을 수립하고, 백업기록 및 백업데이터를 일정기간 유지하여야 한다. * 예) 개인신용정보처리시스템 접속기록(1년 이상), 개인정보처리시스템 접속기록(6개월 이상) 등 • 중요 업무에 대해서는 업무지속성 확보를 위하여 복구목표시간을 정하고, 정보 뿐만 아니라 시스템 및 서비스 복구까지 가능한 수준으로 백업 및 복구 절차를 수립하여 운영하는 것을 권고한다. **【점검 자료의 예】** • IT 재해복구 체계 및 복구절차 문서 **【참고 법규】** • 전자금융감독규정 제13조(전산자료 보호대책) 제1항 제8호, 제14조(정보처시스템 보호대책) 제8호, 제15조(해킹 등 방지대책) 제2항 제6호, 제23조(비상대책 등의 수립·운용), 제24조(비상대응훈련 실시) 제1항		

<table>
<tr><td>보안영역</td><td>관리</td><td>점검분야</td><td>9. 이용자 보호</td></tr>
<tr><td>보안점검 항목</td><td colspan="3">9.1 개인정보 처리 관련 이용자 보호</td></tr>
<tr><td>세부 점검항목</td><td colspan="3">9.1.1 개인정보 처리방침을 이용자가 확인하기 쉽게 공개하고, 법적 절차에 따라 이용자로부터 개인정보 처리 동의를 받고 있다.</td></tr>
<tr><td>세부설명</td><td colspan="3">• 오픈API 이용서비스에서 회원을 가입받거나 개인정보를 입력받는 경우, 개인정보 처리방침을 작성하여 이용자가 쉽게 확인할 수 있는 위치(예:홈페이지 메인화면 등)에 공개하여야 한다.
- 수집하려는 개인정보 항목, 수집방법 및 이용목적, 보유 및 이용기간, 동의 거부 권리 및 거부에 따른 불이익 내용 등 법적으로 요구되는 필수 사항이 기재되도록 작성하여야 한다.

• 수집하려는 개인정보가 목적을 위한 최소한의 정보가 되도록 필수/선택을 적절히 구분하고 동의를 받아야 한다.

《 참고 자료 》
- 개인정보처리방침 작성예시
- 금융분야 개인정보보호 가이드라인
※ privacy.go.kr의 자료마당 > 지침자료 참고

- 개인정보처리방침 만들기
- 개인정보 보호조치 진단(소상공인)
- 개인정보보호 자가진단
※ privacy.go.kr의 사업자 > 개인정보도우미 참고

【점검 자료의 예】
• 개인정보 처리방침 공개 화면 및 처리방침 전문
• 이용자 개인정보 수집·이용 동의 획득 화면

【참고 법규】
• 정보통신망법 제27조의2(개인정보 처리방침의 공개)
• 개인정보 보호법 제3조(개인정보 보호 원칙), 제15조(개인정보의 수집·이용), 제30조(개인정보 처리방침의 수립 및 공개)</td></tr>
</table>

보안영역	관리	점검분야	9. 이용자 보호
보안점검 항목	9.2 개인·신용정보 접근 및 거래지시 권한 관련 안내		
세부 점검항목	9.2.1 오픈API를 통한 개인·신용정보 접근 및 전자금융거래 지시 가능 사실에 대해 이용자에게 안내하고 있다.		
세부설명	• 오픈API를 통하여 이용자의 금융회사 계좌에 대한 개인·신용정보 접근 및 전자금융거래 지시가 필요한 경우, 이용기관은 해당 내용을 충분히 설명하고 이용자의 동의를 획득하여야 한다. • 안내가 필요한 주요 사항은 다음과 같다. - 오픈API를 통한 이용자 정보 접근 및 전자금융거래 지시 목적 - 이용자를 대신하여 오픈API를 통해 접근 가능한 이용자 관련 정보 및 지시 가능한 전자금융거래 종류 - 동의 유효기간 및 철회 방법 - 오픈API 이용 불가 상황 발생 시 서비스 영향 등 • 이용기관은 이용자가 동의 시점 외에도 관련 내용을 수시로 용이하게 확인할 수 있는 수단*을 제공해야 한다. * 예) 웹사이트 등에 정보 조회 기능 제공, 정보 요청 가능한 연락처 게시 등 **【점검 자료의 예】** • 오픈API 접근에 관한 이용자 동의 및 설명 화면 **【참고 법규】** • 개인정보 보호법 제3조(개인정보 보호 원칙) • 신용정보법 제32조(개인신용정보의 제공·활용에 대한 동의)		

보안영역	관리	점검분야	9. 이용자 보호
보안점검 항목	9.3 이용자 고충 처리방침 마련 및 공개		
세부 점검항목	9.3.1 이용자 문의에 대응하는 처리방침을 마련하고 이용자가 확인하기 쉽게 공개하고 있다.		
세부설명	• 상담, 조회, 불만, 사고 신고 등 이용자의 각종 문의에 대응하기 위한 처리방침*을 마련하고, 홈페이지 등에 이용자가 확인하기 쉽게 공개하여야 한다. * 연락처, 대응절차, 손해배상 시 범위 및 처리 절차, 사고 신고 절차 등 • 특히 개인정보 관련 이용자 고충 처리에 관한 사항은 관련 법적 요구사항을 반영하여야 한다. **【점검 자료의 예】** • 이용자 고충 처리방침 안내 화면 및 처리방침 전문 **【참고 법규】** • 정보통신망법 제27조의2(개인정보 처리방침의 공개) 제2항 제7호 • 표준 개인정보 보호지침 제22조(개인정보 보호책임자의 공개) 제2항		

<table>
<tr><td>보안영역</td><td>관리</td><td>점검분야</td><td>9. 이용자 보호</td></tr>
<tr><td>보안점검 항목</td><td colspan="3">9.4 이용자 보안 주의사항 안내</td></tr>
<tr><td>세부 점검항목</td><td colspan="3">9.4.1 서비스 이용 시 이용자의 보안 관련 주의사항을 안내 및 개발에 반영하고 있다.</td></tr>
<tr><td>세부설명</td><td colspan="3">• 이용자가 서비스 이용 시 보안 위험성에 대해 이해하고 주의를 기울일 수 있도록 이용자 측면의 주의사항을 안내하고, 해당 위험을 낮출 수 있도록 서비스 개발에도 반영하여야 한다.

《 이용자 측면 보안 고려사항 》
- 비밀번호 유출위험 및 관리에 관한 사항(단순 비밀번호 사용 금지 등)
- 제한된 횟수를 초과하여 연속 인증 실패 시 계정 잠금 또는 중지(잠금 및 중지 해제는 안전한 절차로 수행)
- 미사용 시 자동 로그아웃
- 안전한 장소 및 기기에서 접속(루팅·탈옥 기기에서 접속 금지, 공용이 아닌 안전한 단말기·네트워크에서 접속 권장 등)
- 서비스에 접속하는 이용자 단말기(휴대용 기기 등)의 잠금 설정 등

【점검 자료의 예】
• 이용자 대상 보안 주의사항 안내 화면
• 개발 시 정보보호 기능명세 산출물
• 애플리케이션 취약점 점검 결과

【참고 법규】
• 전자금융감독규정 제33조(이용자 비밀번호 관리), 제35조(이용자 유의사항 공지)
• 개인정보의 안전성 확보조치 기준 제7조(개인정보의 암호화)</td></tr>
</table>

<table>
<tr><td>보안영역</td><td>물리</td><td>점검분야</td><td>10. 물리적 보안</td></tr>
<tr><td>보안점검 항목</td><td colspan="3">10.1 보호구역 지정 및 출입 통제</td></tr>
<tr><td>세부 점검항목</td><td colspan="3">10.1.1 중요 시스템이 운영되는 장소에 대해 보호구역을 별도로 지정하고 출입을 통제하고 있다.</td></tr>
<tr><td>세부설명</td><td colspan="3">
• 비인가자의 물리적 접근 및 각종 물리적·환경적 재난으로부터 주요 설비 및 시스템을 보호하기 위하여, 물리적 보호구역을 지정하고 각 구역별 보호대책을 수립·이행하여야 한다.

《 보호구역 구분의 예 》
- 접견구역 : 외부인이 별다른 출입증 없이 출입 가능한 구역 (예: 접견실)
- 제한구역 : 비인가된 접근 방지를 위하여 별도의 출입통제 장치 및 감시 시스템이 설치된 장소로 직원 카드 등의 출입증이 필요한 장소 (예: 사무실 등)
- 통제구역 : 제한구역의 통제항목을 모두 포함하고, 출입자격이 최소인원으로 유지되며 출입을 위하여 추가적인 절차*가 필요한 곳 (예: 전산실, 통신장비실, 관제실, 전원실 등)
* 인가자만이 출입 가능한 통제시스템(지문인식, 출입카드 등)

• 오픈API 관련 중요시스템이 운영되는 장소는 통제구역으로 지정하여 출입을 통제해야 한다.
- 외부 IDC에 위탁운영하는 경우 상응하는 물리적 보안 요구사항을 계약서에 반영하고 운영 상태를 주기적으로 검토해야 한다.

《 출입 통제의 예 》
- 공식적인 출입절차(신청,승인,부여,회수,기록,정기 검토) 마련
- 출입가능 직원 식별 및 출입권한 부여, 출입 기록 검토
- 외부자에 대한 별도 출입절차(담당자 동행, 출입관리대장 등) 마련
- 비인가자 출입 시도 확인 등

• 통제구역 등에 대한 출입기록은 일정기간(1개월 이상) 보존하고 주기적으로 검토할 수 있어야 한다.

【점검 자료의 예】
• 보호구역 지정 및 출입통제 관련 정책 또는 정책시행 문서
• 출입권한 처리 기록, 출입통제시스템 사진 및 접근 기록
</td></tr>
</table>

	• 외부 IDC 위탁 운영 계약서 • 출입관리대장 **【참고 법규】** • 전자금융감독규정 제11조(전산실 등에 관한 사항) • 정보통신망법 제46조(집적된 정보통신시설의 보호)

<table>
<tr><td>보안영역</td><td>물리</td><td>점검분야</td><td>10. 물리적 보안</td></tr>
<tr><td>보안점검 항목</td><td colspan="3">10.2 보호구역 반출입 관리</td></tr>
<tr><td>세부 점검항목</td><td colspan="3">10.2.1 휴대장치의 통제구역 반출입을 통제하고, 중요 단말기 및 휴대장치 등의 사무실 반출입을 통제하고 있다.</td></tr>
<tr><td>세부설명</td><td colspan="3">• 미승인 장치의 반출입을 통한 중요정보 유출, 내부망 악성코드 감염 등의 보안사고 예방을 위하여 보호구역 별로 휴대용 장치 등의 반출입 통제절차를 수립하여 통제하여야 한다.

《 반출입 통제절차의 예 》
- 보호구역 출입통제 책임자 사전 승인
- 반출입 관리대장 기록
- 휴대용 기기 보안점검 수행
- 휴대용 기기 반출입내역의 주기적 사후 점검

• 오픈API 관련 중요시스템이 위치한 통제구역 내 휴대용 기기(노트북, 태블릿PC 등) 및 저장매체의 반출입은 원칙적으로 금지하여야 한다.
- 불가피하게 사용하여야 할 경우 반출입 통제절차에 따라 사전 책임자의 승인을 받고, 보안사고 예방절차를 이행한 후 사용하여야 한다.

《 휴대용 기기/저장매체 관련 보안사고 예방절차의 예 》
- 안티바이러스 S/W를 통한 악성코드 감염여부 점검
- USB 포트 차단 및 USB 반입 금지
- 휴대용 기기 카메라 렌즈 봉인
- 반출 시 중요정보 저장 여부 확인 등

• 제한구역(예: 사무실)에 대한 중요 단말기, 휴대용 기기 및 저장매체의 반출입을 통제하여야 한다.

【점검 자료의 예】
• 보호구역에 대한 반출입 통제절차 포함 정책 또는 정책시행 문서
• 반출입 관리대장

【참고 법규】
• 전자감독규정 제13조(전산자료 보호대책) 제1항 제5호
• 개인정보 안전성 확보조치 기준 제11조(물리적 안전조치)</td></tr>
</table>

<table>
<tr><td>보안영역</td><td>물리</td><td>점검분야</td><td>10. 물리적 보안</td></tr>
<tr><td>보안점검 항목</td><td colspan="3">10.3 사무실 환경 보안 정책 수립 및 이행</td></tr>
<tr><td>세부 점검항목</td><td colspan="3">10.3.1 비인가자 접근을 막기 위한 보호대책을 수립 및 이행하고 있다.</td></tr>
<tr><td>세부설명</td><td colspan="3">• 단말기에 대한 비인가자 접근을 막기 위한 단말기 보호대책을 수립 및 이행하여야 한다.

《 단말기 보호대책의 예 》
- 화면보호기 설정 및 일정시간 미사용 시 비밀번호 재확인
- 비밀번호(부팅, 로그인) 설정
- 복잡한 비밀번호 사용 및 주기적 변경
- 비인가·불법 S/W 설치 제한
- 퇴근 시 전원끄기
- 악성코드 감염 방지(악성코드 검사 등)

• 중요 정보의 보호를 위하여 일정시간 이상 이석, 퇴근 시 책상 위에 중요문서 또는 저장매체를 방치하는 것을 금지하여야 한다.

• 중요 문서가 보관된 서랍장이나 캐비넷은 잠금장치를 사용하여야 한다.

【점검 자료의 예】
• 단말기 보호대책을 포함한 사무실 환경 보안 관련 정책 또는 정책 시행 문서
• 서랍장 및 캐비넷 잠금장치 확인 가능 자료

【참고 법규】
• 전자금융감독규정 제12조(단말기 보호대책), 제32조(내부사용자 비밀번호 관리)
• 개인정보 안전성 확보조치 기준 제11조(물리적 안전조치)
• 신용정보업감독규정 제22의4(개인신용정보가 포함된 문서 등의 관리 방법)</td></tr>
</table>

보안영역	기술	점검분야	11. 개발 보안
보안점검 항목	11.1 설계 시 보안 요구사항 도출 및 반영		
세부 점검항목	11.1.1 신규개발 및 변경 시 보안 요구사항을 도출하고 이에 대한 대책을 설계에 반영하고 있다.		
세부설명	• 신규개발 및 변경 시 정보보호 관련법, 최신보안취약점*, 정보보호 기본요소**를 고려하여 보안 요구사항을 도출하고 이에 대한 대책을 설계에 반영해야 한다. * 웹서비스의 경우 OWASP TOP10 등 주요 취약점 포함 ** 기밀성, 무결성, 가용성 ※ 보안성을 고려한 설계 절차는 정보통신망법 시행령 제36조의2(정보보호 사전점검기준)에 따른 '정보보호 사전점검에 관한 고시' [별표 3]의 사전점검 절차를 참고할 수 있음 • 운영기관의 약관, API개발가이드 등을 숙지하여 오픈API 이용서비스를 안전하게 개발한다. - 특히 오픈API 인증키, 오픈API 접근키 등 오픈API 관련 중요정보를 운영기관의 API개발가이드 등에 따라 안전하게 관리할 수 있도록 개발하여야 한다. - 또한 오픈API 관련 알려진 보안 위협*에 적절히 대응하도록 안전하게 개발하여야 한다. * 예) CSRF(Cross-Site Request Forgery) 공격, 접근키 부여를 위한 이용자 인증페이지를 위장한 피싱사이트 공격 등 • 전자금융거래 서비스의 경우 금융정보 위변조 방지, 중요정보(비밀번호, 고유식별번호 등) 노출방지, 인증 우회 방지 등을 위한 대책을 설계에 반영해야 한다. - 전자금융거래 서비스 별 위험 수준을 파악하여 위험 관리대책*을 마련해야 한다. * 예) 추가 인증 적용, 이상 금융거래 모니터링 등 - 모바일 애플리케이션 서비스 제공 시 무결성 검증 등을 통해 불법 위조 프로그램이 유통되는 것을 방지해야 한다.		

《 개발 보안 관련 참고 자료 》

- 정보보호 사전점검 안내서
- 정보보호 사전점검 해설서
- 홈페이지 SW(웹) 개발보안 가이드
- 웹서버구축 보안점검 안내서
- 홈페이지 취약점 진단제거 가이드
- 웹어플리케이션 보안 안내서
- 모바일 대민서비스 보안취약점 점검 가이드
- 홈페이지 개발보안 안내서
- 소프트웨어 개발 보안(JAVA, C, Android-JAVA 시큐어 코딩) 가이드 등

※ kisa.or.kr의 자료실 > 관련법령·기술안내서 > 기술안내서가이드 참고

- The Secure Coding Practices Quick Reference Guide
- OWASP Code Review Guide

※ OWASP(www.owasp.org)의 참고

- The OAuth 2.0 Authorization Framework (RFC 6749)
- The OAuth 2.0 Threat Model and Security Considerations (RFC 6819)
- OAuth 2.0 for Native Apps (RFC 8252)

※ Internet Engineering Task Force (tools.ietf.org) 참고

【점검 자료의 예】

• 서비스 개발 산출물 중 정보보호 기능명세 관련 문서

【참고 법규】

• 전자금융감독규정 제34조(전자금융거래 시 준수사항) 제5호
• 정보통신망법 제45조의2(정보보호 사전점검)

보안영역	기술	점검분야	11. 개발 보안
보안점검 항목	11.2 시큐어 코딩 적용 및 보안 취약점 점검·보완		
세부 점검항목	11.2.1 개발 시 시큐어 코딩을 적용하고 문제 발견 즉시 수정하고 있다.		
세부설명	• 시큐어 코딩 방법에 따라 정보처리시스템을 구현하고, 분석 및 설계 과정에서 도출한 보안요구사항이 정보처리시스템에 적용되었는지 시나리오, 체크리스트 등을 작성하고 시험을 수행하여 확인하여야 한다. • 코딩 완료 후 시큐어 코딩 표준에 따라 구현되었는지 소스코드를 검증*하고, 운영환경과 동일한 환경에서 기술적 보안 취약점 점검(또는 모의해킹)을 수행하여 취약점 발견 즉시 소스코드를 수정하여야 한다. * 소스코드 검증도구 활용 가능 **【점검 자료의 예】** • 정보보호 기능명세 확인 시험 계획서(또는 결과서) • 시큐어 코딩 검증 수행 기록 • 보안 취약점 점검(또는 모의해킹) 결과 보고서 및 조치 보고 문서 **【참고 법규】** • 전자금융감독규정 제29조(프로그램 통제) 제6호		

보안영역	기술	점검분야	11. 개발 보안
보안점검 항목	11.3 테스트 시 이용자 개인·신용정보 사용 제한		
세부 점검항목	11.3.1 개발 및 테스트 시 서비스 이용자의 개인·신용정보를 사용하지 않고 있다.		
세부설명	• 개발 및 테스트 과정에서 개인·신용정보를 포함한 중요 정보가 유출되는 것을 방지하기 위하여 테스트데이터는 운영데이터를 사용하지 않아야 한다. - 테스트데이터는 임의의 데이터를 생성하거나 운영데이터를 가공하여 이용자를 식별할 수 없도록 처리한 후 사용하여야 한다. - 불가피하게 운영데이터의 사용이 필요한 경우, 책임자의 승인 절차를 거쳐 사용하고, 목적 달성 후 즉시 폐기하는 등의 관리 대책을 수립하고 이행하여야 한다. **【점검 자료의 예】** • 개발 산출물 중 테스트데이터 화면 캡처 • 테스트데이터 생성 작업 계획서(또는 결과서) • 테스트데이터 생성을 확인할 수 있는 문서(생성시스템 이용 시 관련 계약서·이용기록 등) **【참고 법규】** • 전자금융감독규정 제13조(전산자료 보호대책) 제1항 제10호 • 신용정보업감독규정 [별표 3] 기술적·물리적·관리적 보호대책 마련 기준 Ⅲ.관리적 보안대책 3.개인신용정보의 이용제한 등		

보안영역	기술	점검분야	11. 개발 보안
보안점검 항목	11.4 소스 프로그램 및 전산원장 대상 접근·변경 통제		
세부 점검항목	11.4.1 소스 프로그램 및 전자금융 전산원장에 대한 접근·변경 통제를 적용하고 있다.		
세부설명	• 소스 프로그램 및 전자금융 전산원장에 대한 변경 관리를 수행하고, 인가된 사용자만이 접근할 수 있도록 통제절차를 수립하여 이행하여야 한다. - 소스 프로그램은 운영환경이 아닌 별도의 환경에 보관하며, 운영환경에 이관 후 운영환경에서 삭제하여야 한다. **《 프로그램 등록/변경/폐기 절차 내용의 예 》** - 프로그램 등록/변경/폐기 방법 - 프로그램 변경 기록 관리 - 변경 관련 책임자 확인 및 승인 관련 사항 등 • 전자금융 전산원장 접근 및 변경 내역을 기록해 일정기간 보존해 책임추적성을 확보할 수 있어야 한다. **【점검 자료의 예】** • 변경 관리 및 접근 통제 관련 정책 또는 정책시행 문서 - 프로그램 등록/변경/폐기 절차 문서 등 • 전자금융 전산원장 접근 및 변경 이력 **【참고 법규】** • 전자금융감독규정 제29조(프로그램 통제)		

<table>
<tr><td>보안영역</td><td>기술</td><td>점검분야</td><td>12. 암호 통제</td></tr>
<tr><td>보안점검 항목</td><td colspan="3">12.1 중요 정보 암호화 정책 수립 및 이행</td></tr>
<tr><td>세부 점검항목</td><td colspan="3">12.1.1 오픈API 관련 중요정보 보호를 위해 암호화 정책을 수립 및 이행하고 있다.</td></tr>
<tr><td>세부설명</td><td colspan="3">• 오픈API 관련 중요정보 보호를 위하여 암호화 관련 정책을 수립하고 이행하여야 한다. 또한 정책에 중요 정보의 저장 및 전송시 암호화 적용 등 암호화 관련 법적 요구사항을 반영하여야 한다.
- 공개적으로 보안성이 검증된 안전한 암호 알고리즘 사용

《 안전한 암호 알고리즘의 예 》
- 대칭키 암호 알고리즘: SEED, LEA, HIGHT, ARIA-128/192/256 등
- 공개키 암호 알고리즘: RSAES-OAEP 등
- 일방향 암호 알고리즘: SHA-224/256/384/512 등
※ 2016년 9월 기준
※ 출처: 개인정보의 암호화 조치 안내서(행자부·한국인터넷진흥원, 2017.1.)

• 암호화에 사용되는 암호키는 용도에 따라 적합한 암호키를 생성하여 이용하고, 유·노출 되지 않도록 안전하게 관리하여야 하며, 개인정보처리시스템에 평문으로 저장하여 이용하거나 프로그램 내부에 하드코딩(Hard-coding)하여 사용하지 않아야 한다.
- 암호키의 안전한 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립하여 시행할 것을 적극 권장

《 안전한 암호 키 유효기간의 예 》
ㅇ 대칭 암호 키
- 사용 환경: 저장된 정보, 메시지 또는 통신 세션 보호에 사용
- 유효기간: (발신자 사용기간) 2년 이하, (수신자 사용기간) 발신자 사용기간+3년 이하 권장
ㅇ 개인 서명 키
- 유효기간: 1~3년 권장
※ 출처: 암호 키 관리 안내서(과기정통부·한국인터넷진흥원, 2014.12.)</td></tr>
</table>

《 암호화 관련 정책 내용의 예 》

- 암호화 대상 식별
- 암호화 대상별 안전한 암호화 방식과 알고리즘 정의
- 암호키 관리 대책
- 정보 전송 및 저장 시 암호화 방안
- 암호화 관련 시스템 운영 담당자 역할 및 책임 정의
- 암호화 관련 법적 요구사항(개인정보 보호 관련 법률 등)

《 암호화 관련 참고 자료 》

- 개인정보의 암호화 조치 안내서
- 암호 키 관리 안내서
- 암호 알고리즘 및 키 길이 이용 안내서
- 개인정보의 안전성 확보조치 기준 해설서 등

※ kisa.or.kr의 자료실 > 관련법령·기술안내서 > 기술안내서가이드 참고
※ seed.kisa.or.kr 참고
※ privacy.go.kr의 자료마당 > 지침자료 참고

【점검 자료의 예】

- 암호화 관련 정책 및 정책시행 문서
- 암호화 대상 정보처리시스템의 개발 산출물(정보보호 기능명세, 소스코드 등)
- 암호화 대상 저장 및 전송 구간의 암호화 적용 여부를 확인할 수 있는 자료(화면 캡쳐 등)

【참고 법규】

- 전자금융감독규정 제33조(이용자 비밀번호 관리) 제1항
- 신용정보업감독규정 [별표 3] 기술적·물리적·관리적 보호대책 마련 기준 Ⅱ.기술적·물리적 보호대책 3.개인신용정보의 암호화
- 개인정보 보호법 제24조의2(주민등록번호 처리의 제한) 제2항
- 개인정보 보호법 시행령 제21조의2(주민등록번호 암호화 적용 대상 등)
- 개인정보의 안전성 확보조치 기준 제7조(개인정보의 암호화)
- 정보통신망법 시행령 제15조(개인정보의 보호조치) 제4항

보안영역	기술	점검분야	13. 접근 통제
보안점검 항목	13.1 중요 정보자산 계정 및 접근 권한 관리		
세부 점검항목	13.1.1 오픈API 관련 정보처리시스템에 대한 접근 권한을 안전하게 통제하고 있다.		
세부설명	• 오픈API 관련 정보처리시스템에 대한 접근 권한은 책임자 통제 하에 최소화하고, 안전한 방식으로 시스템에 접근하도록 해야 한다. - 시스템 별로 접근 가능한 관리자 및 중요 단말기를 지정, 시스템에 접근 시 암호화 연결(SSH, VPN 등) 적용, 시스템 별로 다른 안전한 비밀번호 설정* 및 갱신, 1인 1계정 원칙** * 유추하기 어려운 비밀번호 설정(호스트명, 연속 숫자 등 이용 금지) ** 책임추적성 확보를 위하여 1인 1계정이 원칙이나, 그렇지 않은 경우 타당한 근거가 존재해야 함 • 주요 정보처리시스템에 대한 연결시간을 제한하여야 한다. - 서버 사용자 접속 후 일정시간 사용이 없으면 연결을 종료(세션 타임아웃 시간 설정 등)하여 비인가자 접근을 방지해야 한다. ※ 업무상 필요로 세션 타임아웃 예외 처리 필요시 책임자 승인 • 오픈API 관련 정보처리시스템 중 서버의 운영체제 계정 접근 시 비밀번호 이외에 추가인증을 적용하는 것을 적극 권장한다. **【점검 자료의 예】** • 접근통제 관련 정책 또는 정책시행 문서 • 시스템 별 접근 가능 관리자 지정 관련 문서(정보자산목록 등) • 시스템 별 계정 목록 • 시스템 접근 시 비암호화 연결(TELNET, HTTP 등) 불가 설정 • 특정 관리자 및 단말기만 접근 허용된 설정 등 **【참고 법규】** • 정보통신망법 제28조(개인정보의 보호조치) • 개인정보의 안전성 확보조치 기준 제5조 제4항, 제6조 제5항 • 전자금융감독규정 제13조(전산자료 보호대책) 제2항		

<table>
<tr><td>보안영역</td><td>기술</td><td>점검분야</td><td>13. 접근 통제</td></tr>
<tr><td>보안점검 항목</td><td colspan="3">13.1 중요 정보자산 계정 및 접근 권한 관리</td></tr>
<tr><td>세부 점검항목</td><td colspan="3">13.1.2 중요정보를 처리 및 관리하는 관리자 권한 프로그램에 대해 접근을 통제하고 있다.</td></tr>
<tr><td>세부설명</td><td colspan="3">• 이용자의 개인·신용정보나 전자금융거래 등을 관리하는 관리자 전용 프로그램에 대해 접근통제를 해야 한다.
- 관리자 전용 프로그램(관리자 웹페이지, 관리콘솔, 클라우드 서비스 관리콘솔 등)은 외부 공개를 차단하고 특정 위치의 단말에서만 접근 가능하도록 통제하고 접근 내역 기록
- 관리자 전용 프로그램에 대한 접근 권한을 분류하여 관리 권한은 업무 목적에 맞게 최소화하여 부여
- 관리자 전용 프로그램 접근 시 인증수단*을 적용하여 권한 없는 자의 접근 차단
* 중요도에 따라 추가 인증 적용 권고
- 사용자 권한 및 법적 요구사항에 따라 중요정보의 필요 부분만 표시하여 화면 노출 최소화
- 세션 타임아웃 설정을 통해 일정 시간 동안 입력이 없을 경우 자동으로 연결 차단*
* 업무상 필요로 세션 타임아웃 예외 처리 필요시 책임자 승인

《 서비스 관리 프로그램에 대한 접근통제의 예 》
- 공개망에서의 접근 차단
- 허용된 IP 주소 외 접근 제한
- 관리자에 대해 1인 1계정 원칙 적용
- 동일 계정 동시 접속 제한
- 안전한 인증 방식 적용(안전한 비밀번호 설정, OTP 적용 등) 등

【점검 자료의 예】
• 권한 변경 승인 내역서, 업무별 권한 리스트 등
• 관리자 전용 프로그램 관련 침입차단시스템 차단·허용 정책
• 관리자 전용 프로그램

【참고 법규】
• 개인정보의 기술적·관리적 보호조치 기준 제10조(개인정보 표시제한 보호조치)</td></tr>
</table>

<table>
<tr><td>보안영역</td><td>기술</td><td>점검분야</td><td>13. 접근 통제</td></tr>
<tr><td>보안점검 항목</td><td colspan="3">13.2 중요 단말기 지정 및 접근 통제</td></tr>
<tr><td>세부 점검항목</td><td colspan="3">13.2.1 오픈API 이용서비스 관련 중요 단말기를 지정하고, 접근을 통제하고 있다.</td></tr>
<tr><td>세부설명</td><td colspan="3">• 오픈API 이용서비스 관련 중요 단말기를 지정하여 관리하고 강화된 보호대책을 적용해야 한다.
- 중요 단말기에는 백신 프로그램 설치 등을 통하여 악성코드 감염을 방지하여야 한다.
※ 기타 단말기의 경우도 경유를 통한 악성코드 감염을 방지하기 위한 유사 보호대책 적용을 권장
- 휴대용 저장매체의 사용을 원칙적으로 금지하되, 휴대용 저장매체 연결 및 정보 저장 필요 시 책임자 승인 하에 이용하고 목적 달성 후 정보 삭제 확인 등의 별도 통제 대책을 마련하여야 한다.

《 중요 단말기 보호대책의 예》
- 외부 반출 금지
- 전용 또는 인터넷과 격리된 환경(필요시 접근통제 정책을 수립하고 제한적 접속 허용)에서 인가된 이용자만 이용할 수 있도록 통제
- 사전 지정용도 외 사용 금지
- 노트북 등 휴대용 전산장비 사용 금지
- 그룹웨어 접속, 메일 송수신 금지
- 운영체제 방화벽 활성화 및 필요 포트만 허용
- 불필요 서비스 비활성화, 업무 목적 외 프로그램 설치 금지
- 악성코드 매일 점검 실시 등

【점검 자료의 예】
• 중요 단말기 관리대장
• 중요 단말기 보호대책 포함 정책 또는 정책시행 문서
• 휴대용 저장매체 이용·관리 내역(관련 대장, 책임자 결재 내역 등)
• 중요 단말기 관련 침입차단시스템의 차단·허용 정책

【참고 법규】
• 전자금융감독규정 제12조(단말기 보호대책) 제3항
• 정보통신망법 제28조(개인정보의 보호조치)</td></tr>
</table>

	• 개인정보 보호법 제29조(안전조치의무) • 개인정보의 안전성 확보조치 기준 제6조(접근통제), 제9조(악성 프로그램 등 방지), 제10조(관리용 단말기의 안전조치) • 개인정보의 기술적·관리적 보호조치 기준 제9조(출력·복사시 보호조치) • 신용정보업감독규정 [별표 3] 기술적·물리적·관리적 보호대책 마련 기준 Ⅱ.기술적·물리적 보호대책 1.접근통제 4.컴퓨터바이러스 방지

보안영역	기술	점검분야	14. 시스템 보안
보안점검 항목	14.1 주요 시스템 등의 악성코드 감염 및 정보유출 방지		
세부 점검항목	14.1.1 오픈API 관련 정보처리시스템의 악성코드 감염 및 정보유출 방지 대책을 마련하고 있다.		
세부설명	• 오픈API 관련 정보처리시스템의 악성코드 감염을 방지하기 위해 악성코드 예방, 탐지, 대응 등의 보호대책을 수립·이행하여야 한다. **《 악성코드 감염 방지 대책의 예 》** - 사용자 PC 사용지침(출처가 불분명한 이메일 및 파일 열람 금지, 허가 받지 않은 프로그램 다운로드 및 설치 금지 등) - 백신 프로그램 등을 통한 주기적인 악성코드 감염여부 모니터링 정책 - 악성코드 감염 대비 복구절차 - 사용자 교육 및 정보제공 등 **《 악성코드 예방 및 탐지 활동의 예 》** - 정기적·비정기적 업데이트를 통해 최신 악성코드 정보를 반영하여 악성코드 감시 및 치료 - 주기적인 악성코드 점검 : 자동 악성코드 점검 일정 설정 등 - 전자메일, 전자게시판 등에서 받은 첨부파일에 대한 악성코드 감염 여부 검사 - 부팅 시 악성코드 검사 및 치료 프로그램 실행 - 하드디스크 전체에 대한 정기적(예. 월 1회 이상) 검사 수행 - 보조기억매체 연결 시 자동 또는 수동 검사 수행 등 • 인터넷을 통한 악성코드 반입, 정보유출을 방지하기 위하여 정보처리시스템에서 인터넷 및 그룹웨어 등에 대한 접속을 통제해야 한다. - 업무상 인터넷 접속 허용이 필요한 경우, 관련 위험을 분석하고 정보보호 책임자의 승인 하에 허용하고 주기적으로 필요성을 재검토하여 필요가 없는 경우 차단해야 한다. - 접속 통제를 위해 망분리, 침입차단시스템(방화벽) 적용, 인터넷 공유기나 라우터 등의 침입차단 기능 활용 등의 방식을 사용할 수 있다. • 중요서버에 백신 프로그램을 설치하고 정기적으로 업데이트하고, 실시간 검사가 이뤄질 수 있도록 설정해야 한다.		

- 설치가 구조적으로 어렵거나 성능 이슈 등으로 백신 프로그램을 설치하지 않은 서버가 존재할 경우, 주기적으로 서버 내 악성코드 존재 여부를 확인하는 등의 별도 보완대책을 수립·이행하여야 한다.

《 참고 자료 》

- 백신프로그램 이용 안내서
  ※ kisa.or.kr의 자료실 > 관련법령·기술안내서 > 기술안내서가이드 참고

【점검 자료의 예】

- 악성코드 감염 방지 관련 정책 또는 정책시행 문서
- 백신 프로그램 정책을 확인할 수 있는 자료(화면 캡쳐 등)
- 백신 프로그램을 통한 악성코드 검사 기록
- 네트워크 구성도, 침입차단시스템 정책

【참고 법규】

- 전자금융감독규정 제15조(해킹 등 방지대책) 제1항, 제16조(악성코드 감염 방지대책)
- 신용정보업감독규정 [별표 3] 기술적·물리적·관리적 보호대책 마련 기준 Ⅱ.기술적·물리적 보호대책 1.접근통제 4.컴퓨터바이러스 방지
- 개인정보의 안전성 확보조치 기준 제6조(접근통제) 제9조(악성프로그램 등 방지)
- 정보통신망법 시행령 제15조(개인정보의 보호조치) 제5항
- 개인정보의 기술적·관리적 보호조치 기준 제7조(악성프로그램 방지)

보안영역	기술	점검분야	14. 시스템 보안
보안점검 항목	14.2 인터넷망을 통한 원격관리 통제		
세부 점검항목	14.2.1 오픈API 관련 정보처리시스템에 대해 인터넷망을 통한 원격관리를 통제하고 있다.		
세부설명	• 원격지에서 인터넷 등 외부 네트워크를 통하여 오픈API 관련 정보처리시스템을 관리하는 것은 원칙적으로 금지하는 것을 권고한다. - 불가피하게 원격관리가 필요한 경우 책임자 승인, 접속 단말·사용자 인증 및 추가 인증 적용, 구간 암호화 등 안전한 접속수단 적용(VPN 등), 접속단말 보안강화(백신 프로그램 설치, 패치 적용 등) 등의 보호대책을 수립하고 보호대책을 적용하여야 한다. **【점검 자료의 예】** • 원격관리 통제 관련 정책 또는 정책시행 문서 • 오픈API 관련 정보처리시스템 원격 접근 이력 • 네트워크 구성도 • 침입차단시스템 정책 **【참고 법규】** • 전자금융감독규정 제15조(해킹 등 방지대책) 제1항 제5호 • 전자금융감독규정 시행세칙 제2조의2(망분리 적용 예외) 제2항 제3호, 제3항 • 개인정보의 안전성 확보기준 제6조(접근통제) 제2항		

보안영역	기술	점검분야	14. 시스템 보안
보안점검 항목	14.3 주요 시스템 목적 외 기능·프로그램·포트 등 제거		
세부 점검항목	14.3.1 오픈API 관련 전산시스템 내 서비스 목적 외의 기능·프로그램·포트 등을 제거하고 있다.		
세부설명	• 오픈API 관련 전산시스템 및 중요 단말기에 최소한의 서비스 포트와 기능만 적용하고 업무목적 외의 기능 및 프로그램 등을 제거하여야 한다. - 정보보호시스템의 경우 인바운드 정책은 기본 전부 차단(All Deny)로 설정하고, 인바운드와 아웃바운드 정책에는 업무에 필요한 포트만 허용하도록 정책 구성 - 네트워크 장비의 경우 필요한 통신만 가능하도록 접근통제목록(ACL)을 설정하고 불필요 서비스 비활성화 - 서버의 경우 사용목적과 관계없는 서비스 사용 및 프로그램 설치를 제한하여야 한다. ▸ 서버의 사용목적과 관련이 없거나 침해사고를 유발할 수 있는 서비스(포트), 프로토콜, 데몬 등을 확인하여 제거 또는 차단 ▸ 안전하지 않은 것으로 판단되는 서비스, 프로토콜, 데몬에 대해서는 추가적인 보안 기능 구현 * 예) NetBIOS, File-Sharing, Telnet, FTP 등과 같은 안전하지 않은 서비스를 보호하기 위하여 SSH, SFTP, TLS, IPSec VPN 등과 같은 안전한 기술 사용 - 중요 단말기의 경우 운영체제 제공 방화벽 활성화 및 필요 포트만 허용, 불필요 서비스(메신저, 웹서버 등) 비활성화 **【점검 자료의 예】** • 서비스 목적 외 사용 통제 관련 정책 또는 정책시행 문서 • 오픈API 관련 전산시스템 및 중요 단말기의 정책 적용여부를 확인할 수 있는 자료(허용 서비스/포트, 설치 프로그램 목록 등) • 오픈API 관련 전산시스템 취약점 점검 결과 및 보완조치 문서 **【참고 법규】** • 전자금융감독규정 제15조(해킹 등 방지대책) 제2항 제2호, 제17조(홈페이지 등 공개용 웹서버 관리대책) 제1항 제3호		

보안영역	기술	점검분야	14. 시스템 보안
보안점검 항목	14.4 중요 서버 독립 운영 및 정보보호시스템 적용		
세부 점검항목	14.4.1 오픈API 관련 서버는 독립서버로 운영하고, 정보보호시스템을 적용하여 보호하고 있다.		
세부설명	• 오픈API이용 관련 서버는 독립된 서버로 운영되어야 한다. - 외부에 서비스를 제공하는 공개용 웹서버, 민감한 정보를 보관·처리하고 있는 데이터베이스 서버 등은 공용 장비로 사용하지 않고 독립된 서버를 사용하여야 한다. • 클라우드나 서버 가상화을 이용하는 경우 공개용 웹서버, 데이터베이스 서버 등을 공용 가상머신으로 사용하지 않고 독립된 가상머신을 사용해야 하며, 서버 가상화로 인해 발생할 수 있는 위협에 대한 별도의 보호대책*이 수립되어 있어야 한다. * 예) 가상머신 별 접근관리, 데이터 분리 및 보호, 하이퍼바이저와 가상머신 사이의 인터페이스 취약점 등에 대한 패치, 표준 이미지 이용 등 **《 참고 자료 》** - 클라우드 정보보호 안내서 ※ kisa.or.kr의 자료실 > 관련법령·기술안내서 > 기술안내서가이드 참고 • 적절한 정보보호시스템을 운영하여 중요서버를 보호하고, 정보보호시스템에 이상징후 탐지를 가급적 빨리 담당자에게 알리도록 경고 기능을 설정하며, 보안기능 정상 작동 여부를 주기적으로(월 1회 이상) 점검하는 것을 권장한다. **【점검 자료의 예】** • 네트워크 구성도 • 시스템 구성도 및 중요 서버 정보(호스트명, IP주소 등) • 정보보호시스템 적용 현황 **【참고 법규】** • 전자금융감독규정 제15조(해킹 등 방지대책) 제1항 제1호, 제2항 제5호		

보안영역	기술	점검분야	14. 시스템 보안
보안점검 항목	14.5 공개용 웹서버 보호대책 마련		
세부 점검항목	14.5.1 공개용 웹서버에 대한 별도 보호대책을 마련하여 적용하고 있다.		
세부설명	• 공개용 웹서버를 운영하는 경우 별도의 보호대책을 마련하여 적용하여야 한다. **《 공개용 웹서버 보호대책의 예 》** - 공개용 서버 목적의 독립된 장비로 운영 - 개인정보 송·수신 시 암호화 통신(HTTPS 등) 적용 - 불필요한 서비스 제거 및 포트 차단 - 불필요한 소프트웨어·스크립트·실행파일 등 설치 금지 등 - 불필요한 페이지(테스트 페이지) 및 에러 처리 미흡에 따른 시스템 정보 노출 방지 - 제공하는 서비스 이외의 다른 서비스가 함께 제공되지 않도록 조치 - 인터넷 접점에 정보보호시스템(침입차단시스템 등) 설치 및 서버 보호 - 주기적인 취약점 점검 등 • 공개용 웹서버에 개인정보 및 신용정보 등 중요정보의 저장·관리를 금지하여야 한다. - 거래로그를 관리하는 경우는 예외로 하되, 이 경우 중요정보를 반드시 암호화 하여 저장·관리하고 업무목적이 종료된 경우에는 중요정보를 포함한 거래로그의 폐기하는 등의 보호대책을 수립 및 이행하여야 한다. **【점검 자료의 예】** • 공개용 웹서버 보호대책이 포함된 정책 또는 정책시행 문서 • 네트워크 구성도 • 침입차단시스템 정책 • 모바일앱/웹애플리케이션 포함 공개용 웹서버 취약점 점검 결과 및 보완조치 문서 • 웹서버 접속로그, 거래로그 **【참고 법규】** • 전자금융감독규정 제17조(홈페이지 등 공개용 웹서버 관리대책) • 개인정보보호법 제24조(고유식별정보의 처리 제한) • 개인정보의 안전성 확보조치 기준 제7조(개인정보의 암호화)		

보안영역	기술	점검분야	14. 시스템 보안
보안점검 항목	14.6 중요 보안패치 적용 지침 수립 및 이행		
세부 점검항목	14.6.1 회사에 적합한 보안패치 적용 지침을 수립하고, 주기적으로 검토 및 적용하고 있다.		
세부설명	• 자산 중요도 또는 특성에 따라 운영체제, 소프트웨어 패치관리 정책 및 절차를 수립·이행하여야 한다. - 서버, 네트워크 장비, PC 등의 운영체제 및 소프트웨어(오피스 프로그램, 백신, DBMS, WEB/WAS 등)의 경우 지속적으로 취약점이 발견되며 이를 해결하기 위한 패치(patch) 파일도 지속적으로 공개된다. 따라서 운영체제 및 소프트웨어 패치 적용을 위한 정책 및 절차를 수립하여 이행하여야 한다. **《 패치적용을 위한 정책 및 절차의 예 》** - 서버, 네트워크장비, 정보보호시스템, 단말기 등 대상별 패치정책 및 절차 (패치정보 입수 및 적용방법 등) - 패치 담당자 및 책임자 지정 - 패치 관련 업체(제조사) 연락처 등 • 보안전문 기관(KISA, NIST 등)의 위협 정보, 시스템 제조사의 보안 패치 정보 등의 수집·검토 체계를 갖추고 패치를 이행하여야 한다. • 긴급 패치가 필요한 경우 업무 영향을 최소화하는 선에서 지체 없이 조치하여야 한다. - 시스템 가용성에 미치는 영향 등의 이유로 운영환경에 따라 즉시 패치 적용이 어려운 경우 그 사유와 추가 보완대책을 마련하여 책임자에게 보고하고 그 현황을 관리하여야 한다. • 오픈API 관련 정보처리시스템 및 중요 단말기는 인터넷 실시간 접속을 통한 패치를 제한하여야 한다. - 인터넷 실시간 접속을 통한 패치가 불가피한 경우, 사전 위험분석을 통해 보호대책을 마련한 후 책임자 승인을 거쳐 적용하여야 한다.		

	• 조직 내 패치관리시스템(PMS)을 활용하는 등 내부통신망에서의 파일 배포 기능을 통합·최소화하여 운영하고, 패치 배포 전 무결성 검증 수행, 접근통제 등 충분한 보호대책을 마련하여야 한다. - 패치관리시스템(PMS)의 경우 내부망 서버 또는 단말기에 악성코드 유포에 활용될 수 있으므로 패치관리시스템(PMS) 서버, 관리 콘솔에 대한 충분한 보호대책*을 마련하여야 한다. * 관리자 외 비인가자 접근 차단, 패스워드 주기적 변경, 임시계정 삭제 등 • 주요 서버, 네트워크 장비, 정보보호시스템 등에 설치된 운영체제 버전, 소프트웨어 버전, 최종 패치 버전 등을 확인할 수 있도록 목록으로 관리하여 패치 정보 수집 시 원활한 검토가 가능하도록 하는 것을 권장한다. **【점검 자료의 예】** • 패치관리 정책이 포함된 정책 또는 정책시행 문서 • 패치 수행 기록 **【참고 법규】** • 전자금융감독규정 제14조(정보처리시스템 보호대책) 제7호, 제15조(해킹 등 방지대책) 제1항 제2호, 제1항 제4호

보안영역	기술	점검분야	15. 네트워크 보안
보안점검 항목	15.1 DMZ 구간 구성		
세부 점검항목	15.1.1 DMZ 구간을 구성하여 내부 네트워크를 보호하고 있다.		
세부설명	• 침입차단시스템을 이용해 외부 네트워크와 내부 네트워크 사이에 DMZ(Demilitarized Zone) 영역을 구성하고 내부 네트워크를 보호하여야 한다. - 공개서버(웹서버, 메일서버 등)는 DMZ 영역에 설치하여 공개서버가 침해당하더라도 공개서버를 통한 내부 네트워크 침입이 불가능하도록 침입차단시스템 등을 통한 접근통제 정책을 적용하여야 한다. - DMZ에 위치한 공개용 서버가 내부 네트워크에 위치한 DB서버, 응용 서버 등의 정보처리시스템과 접속이 필요한 경우 엄격하게 접근통제 정책을 적용하여야 한다. - 비정상적 라우팅을 통한 외부 네트워크에서 내부 네트워크로의 별도 우회 경로가 존재하지 않도록 하여야 한다. **【점검 자료의 예】** • 네트워크 구성도 및 DMZ 영역 구성 설정 • 라우팅 테이블 정보 • DMZ 영역 및 내부 네트워크 간 침입차단시스템 정책 **【참고 법규】** • 전자금융감독규정 제17조(홈페이지 등 공개용 웹서버 관리대책) 제1항 제4호		

보안영역	기술	점검분야	15. 네트워크 보안
보안점검 항목	15.2 내부망 사설IP 활용 및 주요 시스템 배치		
세부 점검항목	15.2.1 내부망은 사설IP 주소를 활용하고 업무영역에 따라 핵심 시스템은 내부망에 배치하고 있다.		
세부설명	• 네트워크에 대한 비인가 접근을 통제하기 위해 필요한 네트워크 접근통제 리스트, 네트워크 식별자(IP) 등에 대한 관리절차를 수립하고 서비스, 사용자그룹, 정보자산의 중요도에 따라 내·외부 네트워크를 분리하여야 한다. - 침입차단시스템, ACL(Access Control List) 설정이 가능한 네트워크 장비 등을 활용하여 네트워크 영역 간 업무수행에 필요한 서비스의 접근만 허용하도록 통제하여야 한다. • 내부망에서의 주소 체계는 사설IP 주소 체계를 사용하고 내부 주소체계를 외부에 유출되지 않도록 하여야 하며 외부 네트워크와의 연결지점에 NAT(Network Address Translation) 기능을 적용하여야 한다. **《 사설IP 주소 대역 》** - 10.0.0.0 ~ 10.255.255.255 - 172.16.0.0 ~ 172.31.255.255 - 192.168.0.0 ~ 192.168.255.255 • 오픈API 관련 중요정보를 저장하고 있는 DB서버는 외부에 서비스를 제공하는 DMZ 구간에 위치해서는 안되며, 침입차단시스템 등의 정보보호시스템으로 보호된 내부 네트워크 영역에 위치하여야 한다. **【점검 자료의 예】** • 네트워크 구성도 • 침입차단시스템 정책 **【참고 법규】** • 전자금융감독규정 제18조(IP 주소 관리대책) 제1호 • 전자금융감독규정 제15조(해킹 등 방지대책) 제1항 제3호		

<table>
<tr><td>보안영역</td><td>기술</td><td>점검분야</td><td>15. 네트워크 보안</td></tr>
<tr><td>보안점검 항목</td><td colspan="3">15.3 무선 네트워크 이용 최소화 및 보안대책 수립・적용</td></tr>
<tr><td>세부 점검항목</td><td colspan="3">15.3.1 무선 네트워크는 통제 하에 이용을 최소화하며, 책임자 승인 하에 이용 시 보호대책을 적용하고 있다.</td></tr>
<tr><td>세부설명</td><td colspan="3">• 조직 내부 네트워크에 연결이 가능한 무선 네트워크 환경 구축 시에는 내부 승인절차를 마련하여 비인가된 무선 네트워크 장비를 운영하지 않도록 하여야 하며, 사전 보안성 검토를 수행하여 다음과 같은 보호 대책을 적용하여야 한다.

《 보호 대책 》
- 무선 네트워크 장비(AP) 접속 단말 인증 (MAC 인증 등)
- 무선 네트워크 장비 SSID 숨김 기능 설정 및 추측 어려운 SSID 사용
- 무선 네트워크 장비 기본 설정값 변경 (계정, 패스워드, SNMP Community String 등)
- 무선 네트워크 장비에 정보 송수신 시 암호화(WPA2 이상) 설정 등

• 외부인이 무선 네트워크를 통해 내부 네트워크에 접속할 수 없도록 하고 임직원만 무선 네트워크를 사용할 수 있도록 필요한 인가 절차를 마련하여야 한다.

• 내부 네트워크와 무선 네트워크를 분리하여 무선 네트워크를 통한 내부 네트워크 침투 및 내부 정보유출을 방지하여야 한다.

《 참고 자료 》
- 알기쉬운 무선랜 보안 안내서
※ kisa.or.kr의 자료실 > 관련법령·기술안내서 > 기술안내서가이드 참고

【점검 자료의 예】
• 무선 네트워크 통제 관련 정책 또는 정책시행 문서
• 네트워크 구성도
• 무선 네트워크 이용 절차에 따른 산출물(책임자 승인, 이용자 신청, 이용자 목록 등)

【참고 법규】
• 전자금융감독규정 제15조(해킹 등 방지대책) 제6항</td></tr>
</table>

보안영역	기술	점검분야	15. 네트워크 보안
보안점검 항목	**15.4 대외기관과 통신 시 보안통신 적용**		
세부 점검항목	15.4.1 대외기관과 통신 시 보안통신이 적용되어 있다.		
세부설명	• 물리적으로 떨어진 대외기관(오픈API 운영기관 포함)과 통신 시 전송되는 데이터의 기밀성·무결성 등이 보호될 수 있도록 보안통신을 적용하여 연결하여야 한다. - 전용회선 또는 가상사설망(VPN) 적용 - 전송계층 이상의 네트워크 계층에서의 보안통신(TLS, SFTP 등) 방식 등 별도의 프로토콜을 사용하는 경우 이에 맞는 별도의 보호대책* 마련 필요 * 예) 안전한 TLS 프로토콜 사용, 안전한 암호알고리즘 및 강도 적용, 정기적 취약성 제거, 상호 인증, 안전한 인증정보(개인키, 비밀번호 등) 관리, 접근통제 등 **【점검 자료의 예】** • 대외기관 연결 구성이 포함된 네트워크 구성도 • 보안통신 적용 여부 확인 가능한 자료 **【참고 법규】** • 전자금융감독규정 제60조(외부주문등에 대한 기준) 제5호		

Ⅳ. 보안점검 결과보고서 예시

이용기관은 본 가이드에서 예시한 점검항목을 활용하여 자체 보안점검 항목을 구성하고 점검할 수 있다. 아래는 각 항목에 대한 보안점검 결과 보고서의 예를 보여준다.

<table>
<tr><td>보안영역</td><td>관리</td><td>점검분야</td><td colspan="4">1. 정보보호 정책·조직</td></tr>
<tr><td>보안점검 항목</td><td colspan="5">1.1 정보보호최고책임자 지정 및 실무조직</td></tr>
<tr><td>세부 점검항목</td><td colspan="5">1.1.1 정보보호최고책임자를 지정하고, 실무조직을 구성하고 있다.</td></tr>
<tr><td>점검기준 (A)</td><td colspan="5">• 최고경영자는 조직의 정보보호 관련 업무를 총괄 관리할 수 있도록 정보보호최고책임자를 지정하여 조직의 정보보호를 관리한다.
• 책임자의 역할을 지원하고 조직의 정보보호 활동을 체계적으로 이행하기 위한 전문성을 가진 실무조직*을 구성하여야 한다.
* 정보보호산업법 시행규칙 <별표 1>에서 서술한 초급 이상 기술인력을 1명 이상 포함</td></tr>
<tr><td>증빙자료 (B)</td><td colspan="5">자료1.1.1-1 정보보호최고책임자 인사발령서
자료1.1.1-2 정보보호 조직 구성도
자료1.1.1-3 정보보호 실무자 이력서</td></tr>
<tr><td>점검결과 (C)</td><td>이행</td><td></td><td>부분이행</td><td>O</td><td>미이행</td><td></td></tr>
<tr><td>점검결과 요약 (D)</td><td colspan="5">• (정보보호최고책임자 지정) 자료1.1.1-1에 따라 OO.OO.OO일자로 정보보호 관련 업무를 총괄하는 정보호호최고책임자로 △△△를 임명하여 조직의 정보보호를 관리하고 있음
• (정보보호 실무조직 구성)
- 자료1.1.1-2에 따라 정보보호를 위한 실무조직은 정보보호최고책임자를 포함하여 총 3명으로 구성되어 있음
- 직원 '□□□'는 관리적 보안 및 물리적 보안(정보보호 정책 및 관련 문서 관리, 인적 보안, 시설 보안, 외부 계약 등)을 담당하고 있으며, 직원 '◇◇◇'는 기술적 보안(정보보호시스템 정책, 개발 보안, 시스템 보안, 네트워크 보안 등)을 담당하도록 업무 분장이 되어 있음
• (정보보호 실무조직 전문성 미흡)
- 자료1.1.1-3에 따라 현재 조직 내 전문성 기준을 충족하는 인력은 없는 상태임</td></tr>
<tr><td rowspan="2">향후 이행계획 (E)</td><td>목표시기</td><td colspan="4">20XX. X.</td></tr>
<tr><td>세부 이행계획</td><td colspan="4">• □□□는 20XX. X. 시점에 경력 요건을 만족할 예정
• ◇◇◇는 해당 목표 시기 내에 정보보호 관련 자격증을 취득할 예정</td></tr>
</table>

- 점검기준(A) - 세부 점검항목 내 세부설명을 참고하여 조직에 필요한 보안 요구사항을 도출하고 점검기준으로 설정

- 증빙자료(B) - 점검기준 충족 여부를 객관적으로 증명할 수 있는 증빙자료를 의미. 자료 식별 및 지속적인 관리를 위하여 각 증빙자료에 세부 점검항목 번호 및 일련번호로 구성된 파일명을 부여하는 것을 권장

- 점검결과(C) - 보안 요구사항을 모두 만족하는 경우 이행, 부분적으로 만족하는 경우 부분이행, 모두 만족하지 않은 경우 미이행으로 표시

- 점검결과 요약(D) - 점검기준별 충족/미충족 근거를 요약 기술

- 향후 이행계획(E) - 부분이행/미이행 사항에 대한 이행계획이 존재할 경우 목표 시기 및 이행방법을 기술

[참고자료 1] FAQ(Frequently Asked Questions)

1. 「금융권 오픈API 이용기관 자체 보안점검 가이드」의 목적 및 활용용도는?

○ 혁신적인 핀테크서비스의 안전한 이용을 지원하기 위하여 작성되었으며, 금융권 오픈API를 이용하여 고객에게 서비스를 제공하는 핀테크기업 등이 오픈API 이용 관련 보안 위험을 이해하고 이를 사전에 제거 또는 최소화할 수 있도록 지원함

○ 오픈API 이용을 계획하는 핀테크기업이나 오픈API를 이용하는 핀테크기업과의 제휴를 검토 중인 금융회사등이 참고자료로 활용할 수 있음

○ 다만, 오픈API를 제공하는 금융회사 별로 업권 특성, 오픈API시스템 설계, 보안 요구수준 등이 상이할 수 있고, 이용기관 측면에서 오픈API의 이용 구조, 특성, 위험 정도 등에 따라 보안 요구사항이 다양할 수 있으므로

- 본 가이드의 내용을 일률적으로 적용하는 것은 부적절하며, 참고자료로 한정하여 활용하는 것이 바람직(회사별/API별 특성을 반영한 응용 활용 권고)

○ 또한, 본래 목적에 역행하는 타용도(감사 시 기준자료 등) 활용은 부적절

2. '금융권 공동 오픈API'와 금융회사의 '개별 오픈API'의 차이점은?

○ 현재 금융권에서 제공되고 있는 오픈API는 제공 주체에 따라 크게 '금융권 공동 오픈API'와 '금융회사 개별 오픈API'로 구분할 수 있음

- '금융권 공동 오픈API'는 금융회사에서 제공하는 금융서비스를 핀테크기업 등이 편리하게 이용할 수 있도록, 은행업권에서 공동으로 구축한 금융결제원의 '은행권 공동 오픈플랫폼(금융결제원 운영)'과 금융투자업권에서 공동으로 구축한 '자본시장 공동 핀테크 오픈플랫폼(코스콤 운영)'이 있음
- '금융회사 개별 오픈API'는 금융회사 개별적으로 오픈API를 직접 제공하는 형태로 핀테크기업 등이 금융회사의 금융서비스를 이용할 수 있음

[참고자료 2] 참고 문헌 및 자료

- EBA(European Banking Authority), "Regulatory technical standards for strong customer authentication and common and secure open standards of communication", 2018.3.13.
- Review Committee on Open APIs, "Report of Review Committee on Open APIs: Promoting Open Innovation", 2017.7.13.
- FISC, "API 연결 체크리스트", 2018.10.
- OBWG(Open Banking Working Group), "The Open Banking Standard", 2016.2.
- EBA, "Guidelines on authorisation and registration under PSD2", 2017.7.11.
- EBA, "Guidelines on the security measures for operational and security risks of payment services under Directive (EU) 2015/2366 (PSD2)", 2018.1.12.
- IETF, "The OAuth 2.0 Authorization Framework (RFC 6749)", 2012.1.
- https://www.openbanking.org.uk
- 금융보안원, "스마트폰 전자금융서비스 보안 가이드", 2018.6.
- 금융보안원, "금융권에 적합한 정보보호 관리체계 인증기준 점검항목", 2017.2.
- 금융보안원, "중소형 금융회사 보안수준 진단 가이드", 2014.8.

AGR-VI-2018-②-81

금융권 오픈API
이용기관 자체 보안점검 가이드

2018. 12.

금융보안원
FINANCIAL SECURITY INSTITUTE