Privacy Report 2020.09

SOMANSA

데이터3법. 핵심은 보호와 활용의 균형

개 개인정보 보호법 ⊃ 정 정보통신망법 신 신용정보법

관련법 전 전자금융거래법 온 온라인투자연계금융업법

신 신용정보법 2020년 8월 시행 + 전 전자금융거래법 2020년하반기개정

신용정보이동권으로 New Player 등장 ②
마이페이먼트사업자

모든 입출금계좌에 접근가능하며 실제 입출금을 수행하므로

보안점검수준이 높아야함

점검기관	금융보안원	
점검시기	사업개시 전 (사업개시 후에도 주요항목변경시 재점검)	
점검항목	〈기관보안점검〉	30개항목 서면 및 현장점검
	〈서비스 취약점점검〉	웹 40개, 앱 48개 항목으로 원격테스트

My Payment 사업자
내가 Pay할 수 있도록
하나의 앱으로
입출금계좌 통합조회
은행에 입출금을 지시

My Data 사업자
나의 모든 신용도데이터를
하나의 앱으로 통합조회, 분석,
신용도프로필 관리 및
정보주체의 권리 대리행사

신용정보이동

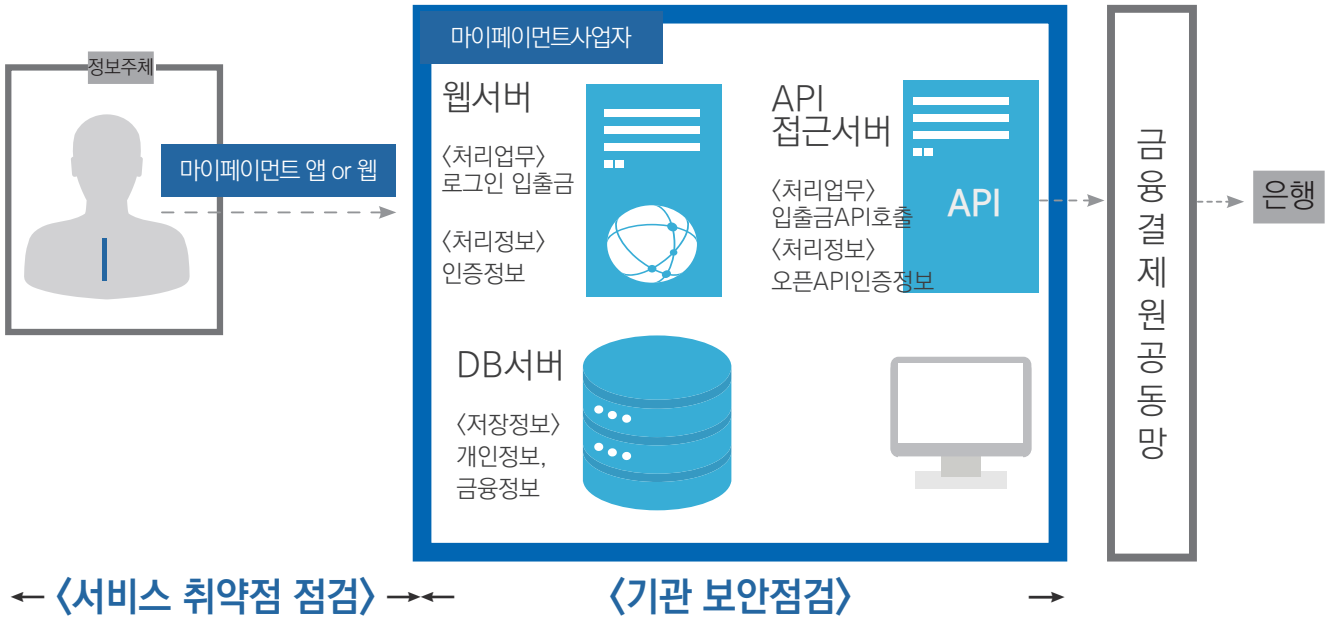
오픈뱅킹표준API
금융결제원 은행망
은행

업종별 중계망
금융권, 비금융권을 망라한
신용정보제공이용자

[My Data VS My Payment 사업자]

	My Data 사업자	My Payment 사업자
사업허가	금융위로부터 마이데이터사업자 허가취득	금융위로부터 마이페이먼트사업자 허가취득
적용법	(신용정보 통합이므로) 신용정보법 적용	(온라인 입출금거래이므로) 전자금융거래법 적용 오픈뱅킹과 〈마이페이먼트사업자〉의 법적근거를 제공하는 방향으로 〈전자금융거래법〉 개정예정 (2020년 3분기에 국회제출) 출처: 금융위원회.2020.7. 〈4차 산업혁명시대의 디지털금융종합혁신방안〉
사용망	미정 (금융결제원 은행공동망 사용가능성 있음) (신용정보제공이용자들이 업종별로 중계기관을 두고 중계망을 구축할 가능성 있음)	금융결제원 은행공동망 사용
사업의 경쟁력	정보주체의 모든 신용, 재산정보를 통합분석하여 개인에게 맞춘 금융컨설팅 가능	기존에는 은행각각과 펌뱅킹(사업자와 은행간의 온라인뱅킹)계약을 해야 했음 이제는 은행각각과의 계약없이도 은행계좌를 기반으로 한 서비스 가능
조회정보	모든 신용정보 (입출금계좌+공공요금+증권+보험+SNS+보유부동산시세+대출...)	입출금계좌 관련정보만 조회 + 입출금 등의 실제 거래 가능
정보주체의 혜택	하나의 앱으로 모든 신용정보조회, 분석, 종합적인 자금관리 및 신용도관리가능	하나의 앱으로 모든 은행 계좌현황을 한곳에서 집중관리. 타행간 거래수수료 하락, 간편송금

전 마이페이먼트사업자 〈보안점검〉



전 〈서비스 취약점 점검_웹〉

플랫폼	분야	점검항목		
		대상정보	점검항목 설명	
웹	중요정보보호	기밀성이 요구되는 이용자 중요정보	① 메모리내 노출방지수준	평문노출 여부 점검
		기밀성이 요구되는 중요정보	② DOM영역내 노출방지 수준	
			③ 네트워크구간내 노출방지수준	평문노출여부 및 네트워크보안설정
			④ 파일저장수준	이용자구간 내 파일저장여부
			⑤ 화면표시 및 보호수준	화면표시 및 화면캡처를 통한 탈취가능여부
		이용자입력중요정보	⑥ 입력정보 보호 적용수준	노출방지를 위해 구현된 보호기능 적용
	거래정보위변조	전자금융거래 중 무결성이 요구되는 계좌정보	① 계좌정보 변조방지수준	메모리 및 네트워크 구간에서 위·변조시 부정이체 가능 여부
		전자금융거래 중 무결성이 요구되는 금액정보	② 금액정보 변조방지수준	
		전자금융거래에 이용되는 거래정보	③ 거래정보 재사용방지수준	재사용 가능 여부
	서버보안		① 서버보안 적용수준	잘 알려진 웹서비스 취약점에 대한 보안대책 적용 등 서버보안대책의 적용여부
	인증		① 멀티로그인 탐지 적용수준	서로 다른 단말에서 동일 계정으로 로그인시 탐지 및 대응 여부
			② 인증 우회방지수준	이용자인증 및 세션 관리와 관련된 기능 구현의 적정성

전 〈서비스 취약점 점검_앱〉

플랫폼	분야	점검항목		
		대상정보	점검항목 설명	
모바일 (안드로이드, iOS)	중요 정보 보호	기밀성이 요구되는 이용자 중요정보	① 메모리내 노출방지수준	평문노출 여부
		기밀성이 요구되는 중요정보	② 네트워크구간내 노출방지수준	평문노출여부 및 네트워크보안설정
			③ 디버그로그내 노출방지수준	디버그로그내 평문노출여부
			④ 중요정보 파일저장수준	단말 내 파일 저장 여부를 점검
			⑤ 중요정보화면표시및 보호수준	화면 표시 및 화면캡처를 통한 탈취 가능 여부
		이용자 입력 중요정보	⑥ 입력정보 보호 적용 수준	노출 방지를 위해 구현된 보호기능 적용여부
	거래 정보 위변조	전자금융거래 이용 중 무결성이 요구되는 계좌정보	① 계좌정보 변조방지수준	메모리 및 네트워크 구간에서 위·변조 시 부정이체 가능 여부를 점검
		전자금융거래 이용 중 무결성이 요구되는 금액정보	② 금액변조 방지수준	메모리 및 네트워크 구간에서 위·변조 시 부정 이체 가능 여부를 점검
		전자금융거래에 이용되는 거래정보	③ 거래정보 재사용방지수준	재사용 가능 여부를 점검
	클라이언트보안		① 앱 위·변조 탐지 적용 수준	점검대상 앱의 중요파일에 대한 위·변조 수행 후 서비스 정상 실행 가능 여부
			② 해킹OS 탐지 적용 수준	루팅/탈옥된 단말에서 점검대상 앱 실행 시 정상 실행 가능 여부
			③ 안티디버깅 적용 수준	디버거를 이용한 동적 디버깅 시도 시 정상 실행 가능 여부
	서버보안		① 서버보안 적용수준	잘 알려진 웹서비스 취약점에 대한 보안대책 적용 등 서버보안대책의 적용 여부
	인증		① 멀티로그인 탐지 적용수준	서로 다른 단말에서 동일 계정으로 로그인 시 탐지 및 대응 여부
			② 인증 우회방지수준	이용자 인증 및 세션 관리와 관련된 기능 구현의 적정성

전 〈기관 보안점검_기술적보호조치가 필요한 항목〉

조	보안점검항목	세부점검사항		기술적 보호조치
3 정보 자산 관리	3.1 〈오픈API 관련 보호대상인 정보자산〉식별	〈오픈API 정보자산〉을 식별, 목록화		
		〈오픈API 정보자산〉의 도입, 변경, 폐기, 반출입 등의 책임자 지정		
		네트워크구성도를 작성, 변경시 보완		
5 인적 보안	**5.2 퇴직 & 직무변경**	내외부직원의 퇴직 &직무변경시 〈오픈API 정보자산〉에 접근권한을 조정 or 회수	인사이동정보를 인사부서가 정보보호/정보처리시스템 운영부서 등에 신속히 공유	
			불가피하게 계정공유시 해당 계정의 인증정보 변경	
6 위험 관리	6.1 취약점 점검정책 수립 &점검	취약점 점검 정책수립 연1회 이상 점검	점검대상 : 〈오픈API 관련 중요정보〉 처리서버 &응용프로그램	
		발견된 취약점을 제거, 보완	서버(웹서버, DB서버, 오픈API 접근서버 등), 응용프로그램(모바일앱/웹애플리케이션 포함) 등	
7 침해 사고 대응	7.2 침해사고대응 로그보존, 모니터링	〈침해사고분석시 필요한 로그 보존 &검토정책〉 수립 로그별로 보존기간, 검토주기를 지정		Mail-i DB-i WebKeeper WAS-i
		침해사고 분석 시 필요한 로그를 일정기간 보존 잠재적인 위협요소 식별을 위해 주기적으로 검토		
		전산시스템(서버, 네트워크 장비, 정보보호시스템 등) 시각을 공식 표준시간으로 동기화		
		침해사고 분석시 필요한 로그	· 시스템 이벤트로그 : OS에 의해 발생되는 로그 (시스템 시작, 종료, 상태, 에러 등), 계정별 접근 기록 · 이용자정보 &전자금융거래 원장 등 중요정보 접속/조회/변경 로그 · 오픈API 이용기록 : 일반이용자접근기록 등	
10 개발 보안	10.1 설계 보안대책을 설계에 반영	법	정보보호 관련법 반영	
		보안 취약점	· 웹서비스 : 주요정보통신기반시설 기술적 취약점 분석평가 방법 상세가이드(한국인터넷진흥원, 2017) 內 Web 분야, OWASP TOP10 · 모바일앱 : OWASP Mobile Top10 등 주요 취약점	
		보안 기본요소	기밀성 무결성 가용성 반영	
		〈오픈API 중요정보 보호대책〉	인증키(client_secret), 접근키(access_token) 등 오픈API 관련 중요정보가 노출되지 않도록 개발	
			인증과정에서 발급한 state 변수값과 이용자에게 반환받은 state 변수값이 불일치할 경우 인증 종료	
	10.2 테스트서비스 이용자의 개인·신용정보 사용 않음	테스트데이터는 임의생성 or 운영데이터가공으로 이용자비식별화		
		운영데이터 사용시 관리대책 (책임자의 승인, 목적달성 후 즉시 폐기 등의 절차) 수립 &이행		
11 암호 통제	11.1 중요정보 암호화정책 수립및이행	공개적으로 보안성이 검증된 안전한 암호 알고리즘을 사용		DB-i Privacy-i
		저장 &전송시 암호화		
		암호키의 안전한 생성, 이용, 보관, 배포 &파기 등에 관한 절차 포함		

조	보안점검항목	세부점검사항			기술적 보호조치
12 접근 통제	12.1 〈중요정보 자산〉 계정& 접근권한 관리	오픈API 관련 정보처리 시스템 접근권한	root 계정은 원격접속을 제한		DB-i Privacy-i
			시스템별로 접근가능한 관리자를 지정, 최소한의 권한부여(1인1계정)		
			시스템에 접근 가능한 중요단말기를 지정		
			시스템에 접근 시 암호화 연결(SSH, VPN 등)		
			세션 타임아웃 설정		
			시스템 별로 다른 안전한 비밀번호 설정 &갱신 *ID, 호스트명, 연속숫자 이용 금지, 영문자, 특수문자, 숫자를 혼합한 8자리 이상, 갱신주기설정(90일 이하),오류횟수제한(5회) 등		
		관리자 전용프로그램 접근권한	(이용자의 개인/신용 정보나 전자금융거래 등을 관리하는 관리자페이지, 네트워크장비 관리자 페이지, 관리콘솔, 클라우드 서비스 관리콘솔 등)	외부공개 차단, 알려진 계정명 (root, admin, manager 등)접속 제한	
				프로그램별로 접근 가능한 관리자를 지정 최소한의 권한 부여(1인 1계정)	
				프로그램에 접근 가능한 중요 단말기 지정	
				프로그램에 접근시 암호화 연결	
				세션 타임아웃 설정	
				프로그램 별로 다른 안전한 비밀번호 설정 &갱신	
				외부에서 접근가능한 관리자 전용프로그램 (예: 클라우드 관리 페이지)의 경우 접근시 추가 인증	
				중요정보는 마스킹하여 화면노출 최소화	
	12.2 중요단말기 지정 & 접근 통제 오픈API 이용 서비스 관련 중요 단말기 지정 &보호	망분리	외부통신망과 격리		
			외부통신망접속이 필요시 접근통제정책하에서 접속		
		비밀번호	유추하기 어려운 비밀번호 (영문, 숫자, 특수문자를 포함하여 8자리 이상)를 설정		
			분기별 1회 이상 변경		
		악성코드	악성코드탐지프로그램을 정기업데이트, 실시간검사 &매일 점검		
		보안패치	최신 보안패치 적용(Hot Fix 등)		
			설치된 응용프로그램은 정기적으로 패치 적용		
		매체	휴대용저장매체는 원칙적으로 사용금지		
			매체연결 &정보저장시 별도의 통제 대책 (책임자 승인하에 이용, 목적달성 후 정보 삭제 확인 등)		
		삭제	중요 단말기는 외부로 반출하지 않도록 통제 외부반출시 중요 데이터 삭제 등의 조치		
		넷앱스	비업무프로그램(메신저, 웹서버 등) 사용 통제		

조	보안점검항목	세부점검사항		기술적 보호조치
13 시스템 보안	13.1 〈오픈 API 관련 정보처리 시스템〉의 악성코드감염& 정보유출 방지 대책	악성코드 예방, 탐지, 대응 등의 보호대책 수립이행		WebKeeper
		중요서버에 백신설치, 주기적 업데이트 &악성코드 점검, 실시간검사 설정 (UNIX 계열의 서버는 제외)		
		인터넷 &그룹웨어 접속통제 (필요시 정보보호책임자의 승인 하에 허용)		WebKeeper
	13.2 인터넷을 통한 원격관리통제	원격관리가 불가피할 경우 책임자승인, 접속단말과 사용자인증, 구간암호화를 사용하는 접속수단(전용회선 or VPN 등) 적용		DB-i
		IDC, 클라우드 등에 위치한 중요서버와의 원격통신시 지정관리자 &단말기에 한하여 전용회선 or VPN(SSH 등 포함)으로 접속		
	13.3 주요시스템의 목적외 기능·프로그램·포트 제거	오픈API 관련 전산시스템 &중요 단말기에 최소한의 포트와 기능만 적용		Mail-i Privacy-i
		업무상 필요하나 취약한 서비스는 안전한 서비스로 대체 · 취약한 서비스 (NetBIOS, File-Sharing, Telnet, FTP)를 · 안전한 서비스 (SSH, SFTP, TLS, IPSec VPN)로 대체		
	13.4 중요서버 독립운영& 정보보호 시스템적용	오픈API 관련서버는 독립서버로 운영	공개용 웹서버, DB서버 등은 독립서버로 운영	
			클라우드나 서버가상화 이용시 독립가상머신 사용	
		〈중요서버 보호정책〉 하에서 정보보호시스템 운영	· 정보보호시스템정책의 기본은 전부차단(All Deny) · 인바운드, 아웃바운드 정책은 업무에 필요한 포트만 허용	SWG
			· 주기적으로 취약한 정책 존재여부 검토 · 취약한 정책 : 네트워크 IP주소 단위로 허용된 정책, 출발지 포트기반의 정책, 양방향으로 설정된 정책 등	
	13.5 공개용 웹서버 보호대책	공개용웹서버에 개인정보, 신용정보 등 중요정보 저장관리금지		Server-i
		주기적(연1회 이상) 공개용 웹서버(모바일앱/웹애플리케이션 등) 취약점 점검 &보완조치 이행		
	13.6 중요보안패치 적용지침 수립 &이행	자산중요도 or 특성에 따라 서버, 네트워크장비 등의 OS &SW(백신, DBMS, WEB/WAS 등) 보안패치지침 수립 &이행		
		오픈API 관련 정보처리시스템 &중요 단말기는 인터넷 직접 접속을 통한 패치제한		

조	보안점검항목	세부점검사항		기술적 보호조치
14 네트워크 보안	14.1 DMZ를 구성 내부 네트워크를 보호	침입차단시스템을 이용해 외부와 내부 사이에 DMZ를 구성		
		공개서버(웹서버, 메일서버 등)는 DMZ 구간에 배치		
		DMZ상의 공개용서버가 내부네트워크의 DB서버, 응용서버 등에 접속시 엄격한 접근통제		
	14.2 내부망사설IP 활용 & 주요시스템 배치	네트워크 접근통제리스트, IP 관리절차를 수립 서비스, 사용자그룹, 정보자산의 중요도에 따라 내외부 네트워크를 분리	네트워크영역을 넘어설 때는 업무상 접근만 허용 (침입차단시스템, ACL이 설정된 네트워크장비 활용)	
			외부에서 내부네트워크로의 (비정상적 라우팅을 통한) 우회경로가 없도록 구성	
			내부네트워크에 접근가능한 장비 (스위치, 라우터, VPN 등)에 비인가자 접근차단	
		내부네트워크 구성대상	오픈API 관련 중요정보를 저장하고 있는 DB서버, 응용 서버	
			오픈API관련 중요단말기	
		내부 네트워크는 사설IP 사용		
	14.3 무선네트워크 이용최소화 & 보안대책 수립	AP 보안	AP 접속 단말 인증 (MAC 인증 등)	
			SSID 숨김설정 &추측 어려운 SSID 사용	
			기본 설정값 변경 (계정, 패스워드 등)	
			정보 송수신 시 암호화(WPA2 이상) 설정 등	
		무선으로는 내부네트워크에 접근할 수 없도록 분리		
		외부인은 무선으로 내부네트워크에 접속불가 임직원만 무선네트워크를 사용할 수 있도록 인가절차 마련		
	14.4 대외기관과 통신시 보안통신	전용회선(VPN 포함) or 전송계층 이상에서의 보안통신(TLS, SFTP 등) 적용		SWG

(주)소만사 서울특별시 영등포구 영신로220 knk디지털타워 9층
Tel: 02 2636 8300 | Fax: 02 2636 8181 | Email: privacy@somansa.com