EQST insight

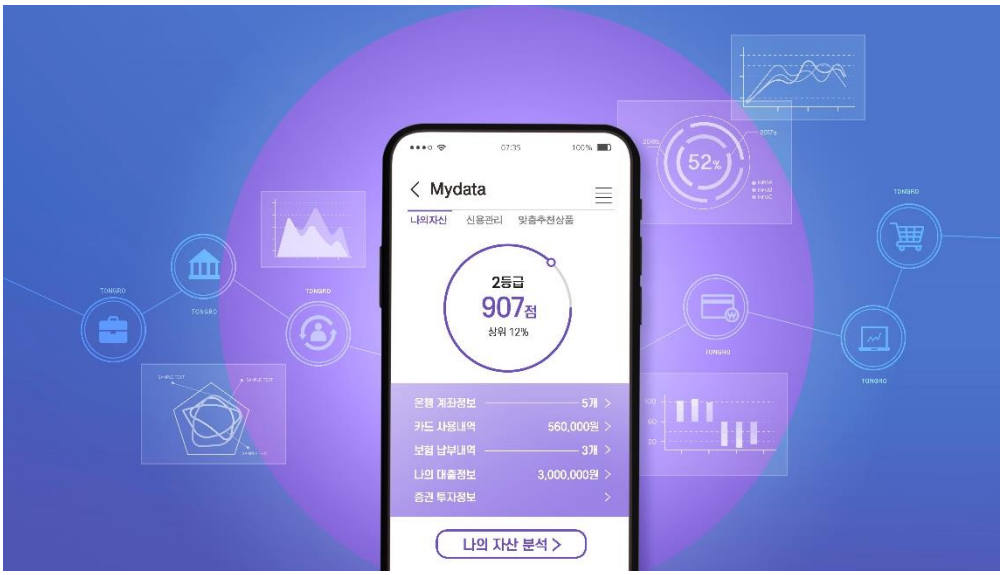
마이데이터 서비스 본격화에 따른 마이데이터 사업자 보안 위협 분석 및 보안 대응 전략

1. 마이데이터 서비스, 개인신용정보 활용 본격화

2021년에 “신용정보의 이용 및 보호에 관한 법률”(이하 “신용정보법”) 개정으로 올해부터 다양한 마이데이터 서비스가 출현하며 정보주체인 소비자의 개인신용정보 활용이 본격적으로 시작되었다.

마이데이터 서비스는 기존 금융 서비스와 달리 컴플라이언스 및 규제 기관의 가이드라인 요건에 맞게 구축되어야 하는 특성을 가지고 있기 때문에 다양한 업권의 금융회사들은 서비스를 출시하며 수많은 시행착오를 겪었다. 막상 힘겹게 서비스를 오픈했지만 시장 초기 마이데이터 사업자 간의 가입자 유치 경쟁으로 인해 커피 쿠폰을 제공하는 기업의 매출이 증가하고 있다는 일부 언론 기사가 간혹 눈에 띄기도 했다. 이와 같이 2021년에는 서비스 오픈을 위해 분주했다면, 올해는 개인신용정보 활용을 통해 이윤을 창출하는 방안을 모색하기 위한 각 금융회사의 다양한 마케팅 연구가 지속될 것으로 보인다.

다만 안정적인 서비스 운영 및 고도화를 위해서는 최신 컴플라이언스를 준수하고, 개인신용정보 유출 등 각종 사이버 침해 공격을 예방하기 위한 강화된 보안 체계와 대응 전략 수립이 필요할 것으로 보인다. 이러한 상황에 발맞춰 SK쉴더스는 보안 관점에서 마이데이터 서비스의 현재 상황과 보안 위협 및 강화된 법령 등을 살펴보고, 서비스 보안 체계 고도화를 위한 방안을 모색해보고자 한다.



2. 금융회사 마이데이터 사업자 현황

`22년 1월 현재 마이데이터 사업자로 본허가를 받은 기업은 55개사, 예비허가 7개사, 허가신청 19개사이며 허가를 받기 위한 기업들은 지속적으로 늘어날 전망이다.

infosec

업권	본허가(55개사)	예비허가(7개사)	허가신청(19개사)
은행	국민은행, 농협은행, 신한은행, 우리은행, SC제일은행, 하나은행, 광주은행, 전북은행, 중소기업은행, 대구은행 (10개사)	-	카카오뱅크 (1개사)
보험	교보생명, KB손해보험 (2개사)	신한생명, 미래에셋생명 (2개사)	메리츠화재, 흥국화재해상보험 (2개사)
금융투자	미래에셋대우, 하나금융투자, 한국투자증권, 키움증권, NH투자증권, KB증권, 현대차증권 (7개사)	교보증권, 신한금융투자 (2개사)	하이투자증권, 대신증권, 한화투자증권 (3개사)
여신 전문금융	국민카드, 우리카드, 신한카드, 현대카드, BC카드, 현대캐피탈, 하나카드, KB캐피탈, 롯데카드 (9개사)	-	-
상호금융	농협중앙회 (1개사)	-	-
저축은행	웰컴저축은행 (1개사)	-	동양저축은행 (1개사)
CB사	나이스평가정보, 코리아크레딧뷰로 (2개사)	-	SCI평가정보 (1개사)
핀테크	네이버 파이낸셜, ㈜핀테크, 카카오페이, 토스, 핀크, NHN페이코, SK플래닛, 민앤지, 뱅크샐러드, 뱅큐, 보맵, 쿠콘, 팀윙크, 핀다, 한국금융솔루션, 해빗팩토리, 아이지넷, 디셈버앤컴퍼니자산운용, 유비벨록스, 애프앤가이드, 코드에프, 한국신용데이터 (22개사)	HN핀코어, 기웅정보통신 (2개사)	오라인포, 웰스가이드, 인공지능연구원(AIRI), 코나아이 SCI평가정보, 차이코퍼레이션, 패스트포워드, 다날 (7개사)
기타	LG CNS (1개사)	피플펀드컴퍼니 (1개사)	SK텔레콤 11번가, KT, LGU+ (4개사)

< 마이데이터 허가 현황(`22년 1월 기준, 신용정보협회 홈페이지) >

마이데이터 업권 별 사업자들의 비즈니스 모델을 살펴보면 아래와 같다.

(1) 은행권 : 개인 자산관리 고도화에 중점을 둔 다양한 생활편의성을 제공하는 등의 종합 금융 플랫폼 지향

(2) 금융투자권 : 금융투자권은 맞춤형 자산관리 컨설팅과 빅데이터 분석, 인공지능(AI) 기술을 활용한 투자 진단 서비스 등 차별화된 서비스를 제공

(3) 카드권 : 새로운 비즈니스 기회 창출을 위해 소비패턴 분석에 기반하여 생활 서비스&금융 플랫폼으로 영역네 확대를 모색하는 등 현재의 결제 및 카드 금융 중심의 사업에서 벗어나 새로운 데이터 기반의 종합 생활금융 플랫폼 기반 구축

(4) 보험권 : 보험권은 인허가 자격 이슈, 비즈니스 모델 검토 중으로 아직 2개 사업자만이 본허가를 받았다. 사업모델은 보험 통합조회, 보장 분석, 일상생활 보험 판매, 건강 분석 등 다양한 서비스로 영역을 확장할 예정

(5) 핀테크 : 기존의 스크린 스크레이핑 기술 기반 서비스의 제공 등 기업간편결제업의 영역을 넘어 종합 플랫폼 비즈니스 선점을 위해 타 사업자들과 경쟁

※ 스크린 스크레이핑 : 공인인증서 등 본인 확인 수단을 정보주체로부터 위탁받아 정보를 수집하는 방식

3. 마이데이터 서비스 보안 위협

개인맞춤형 금융서비스인 마이데이터 서비스는 양질의 개인정보를 다량 보유하고 있어 불특정 다수의 공격 대상이 되기 쉬우므로 마이데이터 플랫폼 또는 API 연계 지점 등을 노리는 공격이 증가할 것으로 보인다.

마이데이터 사업자는 마이데이터 플랫폼의 관문이 되는 API의 보안 강화(지속적 인증 도입, 보안성 갖춘 API 중개자 선정, API Gateway 접근통제 강화 등)와 함께 공격자 관점의 플랫폼 공격 시나리오와 TTP(전술·기술·절차) 분석 등 고도의 인텔리전스 역량을 갖출 필요가 있다.

※ API(Application Programming Interface) : 마이데이터 사업자와 정보제공자 간 개인신용정보를 송수신하기 위한 미리 정의된 표준화된 전송규격 및 절차

infosec

보안 위협	취약점 발생 요인	보안 대책
마이데이터 사업자의 IT인프라의 취약점을 이용한 사이버 공격	개인의 금융자산, 거래내역 등 중요한 개인신용정보가 집중되어 있는 마이데이터 인프라의 취약점 개선노력 미흡	- 서비스 출시 전 사전보안성 검토 - 시스템 취약점 진단 및 조치 - 접근통제 시스템 구축 및 고도화
암호화되지 않은 개인정보의 대량 유출로 인한 사회 경제적 막대한 피해 발생	개인정보 암호화 등의 개인정보 유출 대책 미흡	- 본인인증 절차 강화 - 개인정보 처리(출력, 전송, 저장 등)시 안전한 암호화 알고리즘 적용
마이데이터 사칭(피싱, 스미싱 등) 웹/앱에 의한 인증 정보 탈취로 고객의 금전적 피해 발생 및 각종 사이버범죄 악용 가능성	서비스 이용자의 보안수칙 준수 미흡	- 서비스 이용자에 대한 보안 인식 제고 활동 - 이용자의 보안수칙 준수

< 마이데이터 서비스의 보안 위협과 대응 방안 >

위에서 열거한 다양한 보안 위협의 대응을 위해 마이데이터 사업자는 보안성 검토, 취약점 진단 등 기본적인 보안 대책을 통해 전자금융기반시설에 준하는 보안 수준을 확보해야 한다.

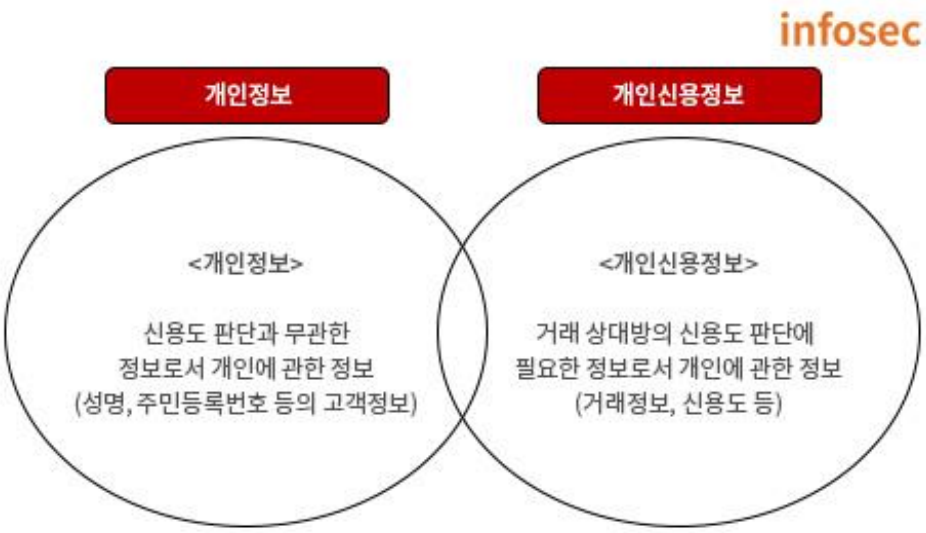
infosec

보안 대책 종류	세부 내용
보안성 검토	자체 보안성심의 평가항목 기반 현황 점검 - 관리·물리·기술 영역 진단 - 취약점에 대한 이행조치 확인 등
취약점 진단	마이데이터 인프라 대상 취약점 진단 - 서버, DB, 네트워크, 미들웨어, 정보보호시스템 - 웹·앱 어플리케이션 등
서비스 수준 평가	마이데이터 관련 법령 및 가이드 준수 현황 점검 - 마이데이터 관련 법령 - 마이데이터 서비스 가이드라인 - 마이데이터 기술 가이드라인 등

< 마이데이터 서비스 기본 보안 대책 >

4. 개인정보보호법 과징금 부과, 마이데이터 사업자도 예외일 수 없어

국내의 개인정보 이동권은 신용정보법에 국한된 개인신용정보에 한해서 이동권을 적용하여 금융 서비스 산업의 데이터유통 활성화 측면을 강조하는 반면, GDPR(유럽연합 개인정보보호규정)의 개인정보이동권은 정보주체의 권리 보장 측면에서 개인정보 전체(개인신용정보 포함)를 대상으로 하고 있다.



< 개인정보와 개인신용정보 >

다만 금융회사의 데이터활성화 측면과는 별개로 과징금 부과 기준을 GDPR(유럽연합 개인정보보호 규정) 수준에 맞춰 '전체 매출액의 3%'로 상향하는 개인정보보호법 전면 개정안이 21년 9월 30일 국회에 제출되어 현재 법안 통과를 위해 대기 중이다. 개정안이 발효될 경우 각 사업자들은 개인신용정보를 포함하여 개인정보의 안정성 확보 조치 미흡으로 인한 과징금 제재를 받지 않기 위해 개인정보 관련 서비스의 보안 대책 마련이 시급해 보인다. 특히, 마이데이터 서비스는 다량의 개인정보를 전송 및 제공하는 만큼 더욱 철저한 대비가 필요하다.

infosec

No	개정 내용	비고
1	과징금 전체 매출의 3%로 일원화 과징금 3% 부과되는 경우 1개에서 11개로 10개 내용 신설	신설
	과실에 대한 형사처벌 폐지	폐지
2	기존 정보통신사업자에서 모든 처리자 대상 정보유출 등의 침해사고 발생 시 손해배상책임이행보험 의무화	개정
3	과징금 부과 근거가 되는 중대한 침해사고 판단기준 8가지 제시	신설

< 개인정보보호법 개정안 주요 내용 >

개인정보보호위원회는 다음 각 호의 어느 하나에 해당하는 행위가 있는 경우 해당 개인정보처리자에게 전체 매출액의 3% 이하에 해당하는 금액으로 과징금을 부과한다는 내용을 개정안에 명시하였다.

마이데이터 사업자는 개정안의 내용 중 제29조(안전조치의무) 항목의 안전성 확보에 필요한 기술적·관리적 및 물리적 조치에 관한 사항 등 사전에 대비할 수 있는 항목에 대한 안전 조치를 강화할 필요가 있다.

infosec

No	조항	과징금 부과 사유
1	제15조(개인정보의 수집·이용) 제1항	해당 조항을 위반하여 개인정보를 처리한 경우
⋮	⋮	⋮
9	제29조(안전조치의무)	안전성 확보에 필요한 조치가 미흡한 경우
⋮	⋮	⋮
11	제37조(개인정보의 처리정지 등) 제2항	개인정보를 계속 이용하거나 이를 제3자에게 제공한 경우

< 전체 매출의 3% 과징금이 부과 주요 내용 >

개정안에는 과징금 부과 시 고려사항을 명시하여 위반행위에 상응하는 비례성과 침해 예방에 대한 효과성이 확보될 수 있도록 하였다. 즉, 위반행위의 정도와 안전성 확보 조치 노력 등에 따라 과징금을 차등 부과할 수 있도록 한 것이다.

infosec

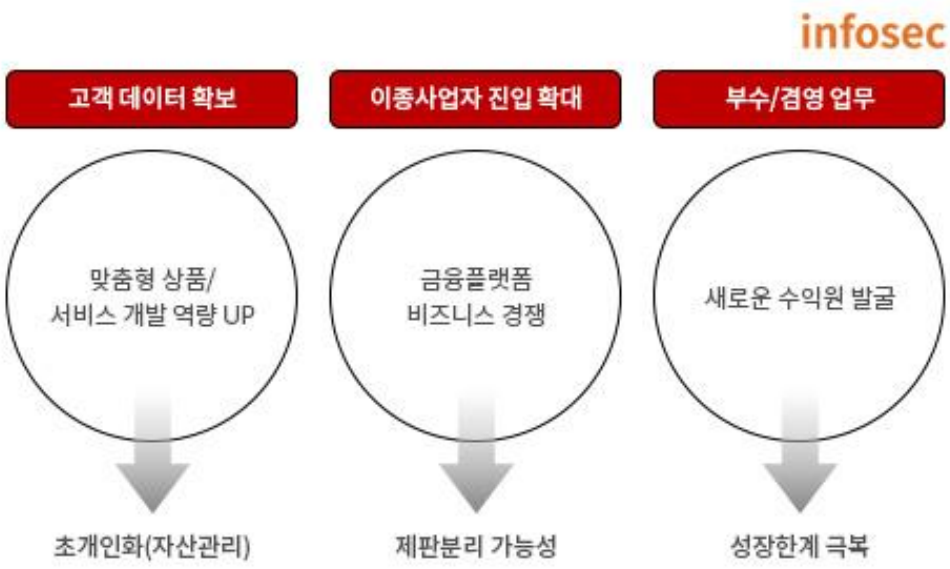
No	조항	세부내용
1	64조의2 제3항	암호화등 안전성 확보에 필요한 조치 이행 노력 정도
2		개인정보가 분실·도난·유출·위조·변조 또는 훼손된 정도 및 안전성 확보 조치 등 의무 위반행위와의 인과관계
3		개인정보처리자의 업무 형태 및 규모
4		처리하는 개인정보의 민감도
⋮		⋮

< 개인정보보호법 개정안 과징금 부과 시 주요 고려사항 >

5. 마이데이터 서비스 보안 대응 전략

마이데이터 서비스의 본격 도입에 따른 긍정적인 측면으로는 정보주체인 고객이 개인신용정보 전송요구권을 바탕으로 다양한 데이터를 활용하여 개인화·맞춤화된 새로운 금융서비스를 마이데이터 사업자로부터 제공받을 수 있게 된다.

금융산업의 측면에서는 기존 주요 금융회사의 고객 데이터 독점이 해소되면서 시장 지배력이 약화되고, 시장 경쟁이 치열해짐에 따라 금융분야의 개방형 혁신이 본격적으로 추진될 것으로 예상된다.



< 마이데이터 사업의 영향 및 시사점 – (보험연구원 2021) >

부정적인 측면으로는 마이데이터 서비스가 새로운 금융 플랫폼의 안정적인 수익원으로 자리잡으려면 신용정보법, 개인정보보호법 등 강화된 컴플라이언스를 준수하고 금융회사에 내재되어 있는 보안 취약점을 지속적으로 개선할 수 있도록 보안 체계 고도화 등의 보안 대책이 동반되어야만 할 것이다.

SK쉴더스에서는 마이데이터 사업자들이 보안체계 수립을 통한 서비스 경쟁력 및 신뢰도를 확보할 수 있도록 사업 준비, 구축 및 운영 단계에서 필요한 보안 컨설팅과 관제 서비스 및 적합한 솔루션을 제안한다.

서비스 종류		세부 내용
보안 컨설팅	인허가 준비 컨설팅	서비스 준비 및 허가 단계에서 시스템 및 보안체계 구성 등에 대한 물적요건 대응
	기능적합성 심사 사전 대응 및 보안성검토 컨설팅	서비스 구축 단계에서 관련 컴플라이언스, 가이드 기준 충족 및 서비스 오픈 전 취약점 개선
	보안취약점 점검 컨설팅	서비스 운영과정에서 발생 가능한 취약점 도출 및 개선
	정보보호 및 개인정보보호 관리체계(ISMS-P) 인증 컨설팅	데이터 종류 및 보유량에 따른 개인정보 흐름 파악, 취약점 도출 및 개선대책 수립
	마스터플랜수립 컨설팅	개인신용정보 안전성 확보조치에 대한 중·장기 보호대책 마련
보안 관제	모니터링	마이데이터서비스 인프라 접속이력 모니터링 등
	유해 트래픽 탐지	개인정보 처리 이상징후 관련 탐지 등
보안 솔루션	금융 컴플라이언스 준수	서버보안, 접근통제, 계정관리솔루션 등
	개인정보보호 특화	내부통제강화 솔루션, 개인정보 Life-Cycle 관리 솔루션, 고객(정보주체) 권리보장을 위한 솔루션 등

< SK쉴더스 마이데이터 관련 서비스 >

2022년 개인정보보호법 개정으로 신용정보법 기반의 금융회사뿐만 아니라 정보주체의 개인정보 이동권이 금융권 이외의 전체 업종으로 확대될 예정이다. 마이데이터 서비스의 종류에 따라 이동되는 개인정보의 양이 상당해지는 만큼 대규모 개인정보 침해 사고의 발생 위험 또한 커질 것으로 보인다.

SK쉴더스는 마이데이터 서비스가 본격화되고 있는 시점에서 보안 전문가의 다양한 노하우와 기술력을 바탕으로 마이데이터 사업자의 고객 정보 지킴이이자 든든한 버팀목이 되고자 한다

6. 참고문헌

- 개인정보 보호법 일부 개정안(2021. 9. 28, 의안번호 12723)
- 2022년 디지털금융 및 사이버보안 이슈전망(2022. 01. 금융보안원)
- 금융 마이데이터 도입 현황과 시사점(2021. 04. 보험연구원)
- 본인신용정보관리업(마이데이터) 신규허가 현황(2021. 10. 금융보안원)
- 마이데이터 국내외 현황 및 주요 해외 사례(2021. 03. KDB산업은행)
- 신용정보의 이용 및 보호에 관한 법률
- 금융분야 마이데이터 기술 가이드라인
- 금융분야 마이데이터 서비스 가이드라인
- 금융분야 마이데이터 표준API 규격 등