2024년

(사)디지털금융법포럼 춘계학술대회

금융 AI시대 금융상품·가상자산·마이데이터의 규제 변화

일 시 2024. 4. 18(목). 14:00 ~ 17:30

장 소 **생명보험교육문화센터**
(서울시 종로구 새문안로5길 31,
센터포인트빌딩 3층)

(사)디지털금융법포럼
Digital Financial Law Forum

2세션

디지털금융시대 마이데이터 활용과 정보보호

발제 : 조규민 센터장(금융보안원 데이터혁신센터)
좌장 : 김정혁 감사 (한패스)
토론 : 추승우 차장(한국은행 전자금융팀)
토론 : 유창훈 대표(센스톤)

(사)디지털금융법포럼
Digital Financial Law Forum

금융보안원
FINANCIAL SECURITY INSTITUTE

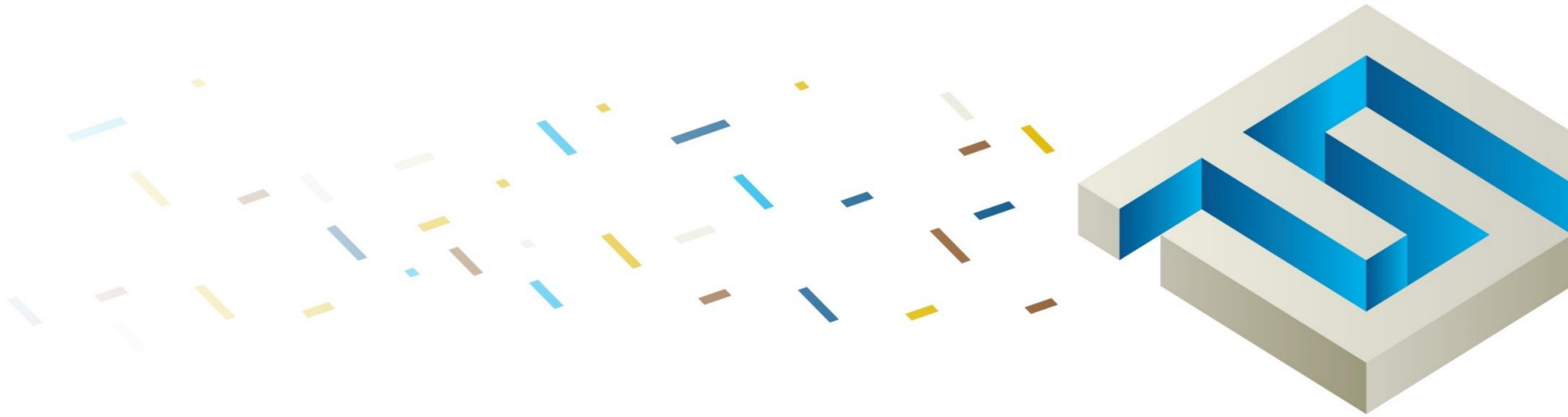
디지털 금융시대
마이데이터 활용과 정보보호

2024. 4. 18.

조 규 민

목차
INDEX

금융분야 마이데이터 1.0



마이데이터(MyData)

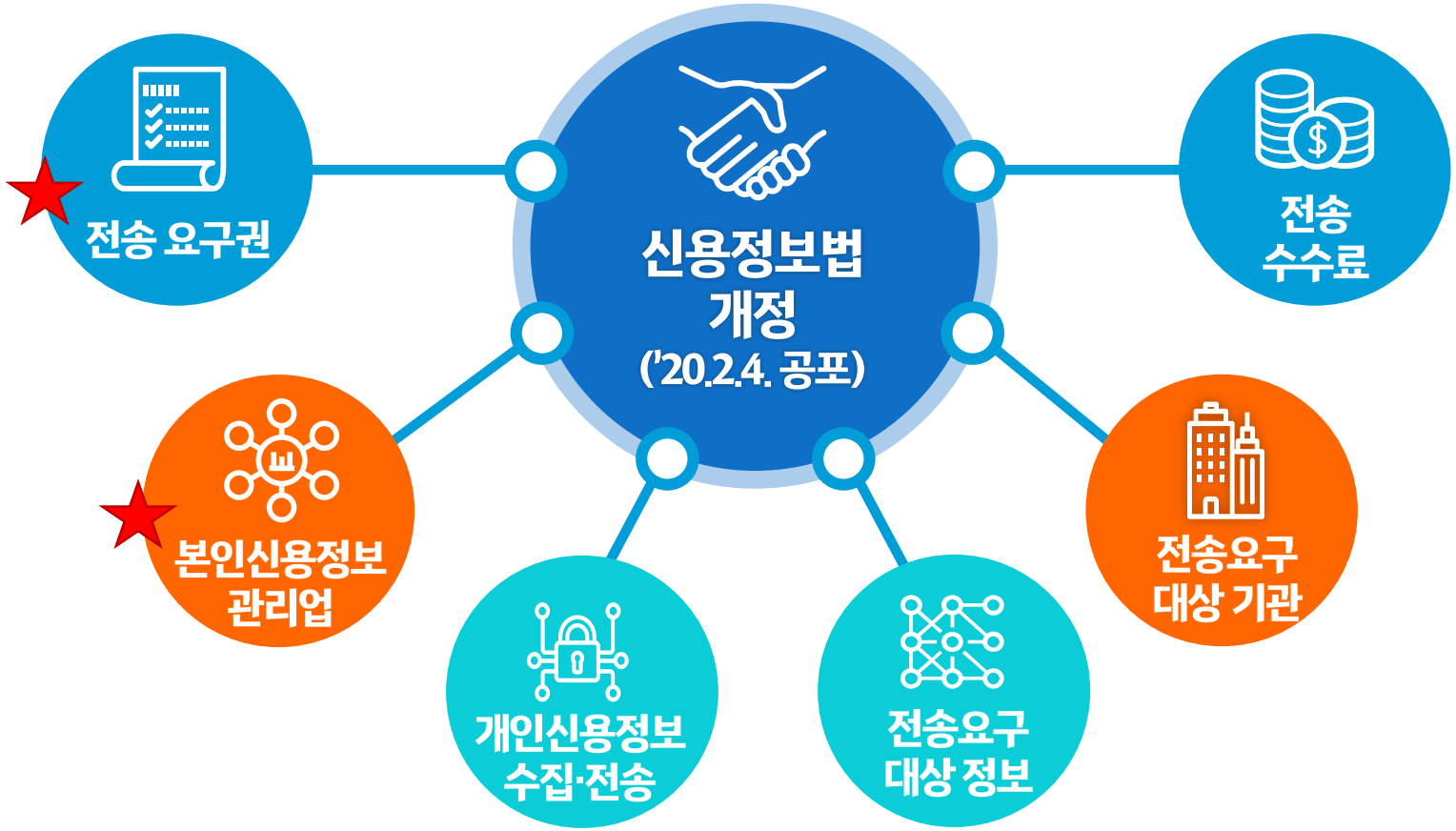
데이터 개방을 통한 경쟁촉진, 정보주체의 권리강화 등의 환경 변화에 따른 개인정보자기결정권*이 실현되는 추세에 따라 개인정보 관리·활용에 대한 패러다임이 기업중심에서 정보주체 중심으로 변화

마케팅 등에 활용

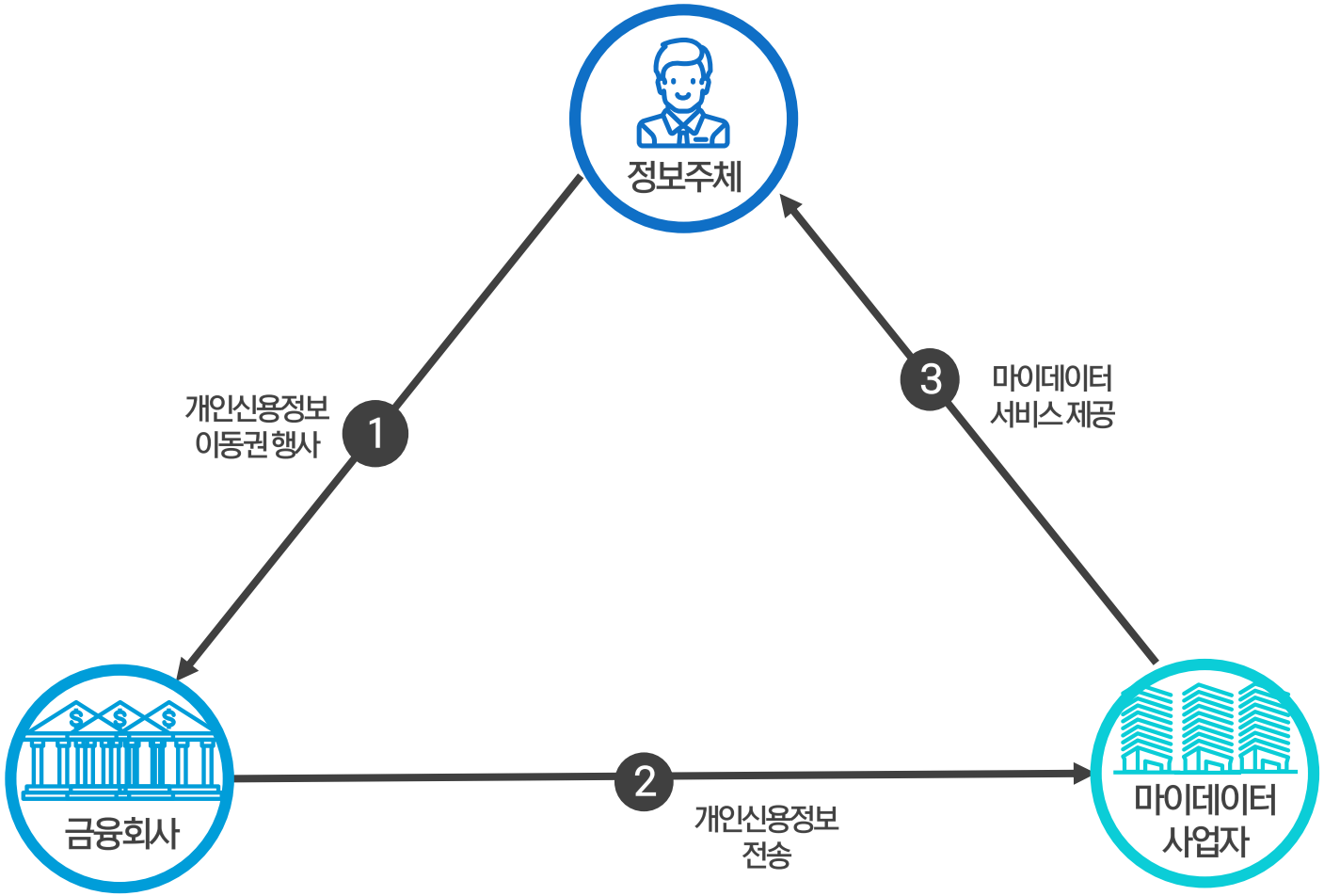
직접 활용 또는 제3자 제공

금융분야 본인신용정보관리업(마이데이터) 도입

[개인신용정보 전송요구권 도입 및 안전한 마이데이터 생태계 조성을 위한 마이데이터 산업 규율체계 마련]



금융분야 마이데이터 개요



개인신용정보 전송 개요

개인신용정보 전송요구권 도입 (제33조의2)

- 신용정보주체가 신용정보제공·이용자등(이하 정보제공자)이 보유하고 있는 본인의 개인신용정보를 본인, 본인신용정보관리회사, 금융회사 등(이하 정보수신자)에게 전송을 요구할 수 있도록 보장

- 정보제공자는 지체 없이 컴퓨터 등 정보처리장치로 처리가 가능한 형태로 전송

전송요구 시 특정 사항

(제33조의2 제5항)

- 전송요구를 받는 자 (정보제공자)
- 개인신용정보를 제공받는 자 (정보수신자)
- 전송을 요구하는 개인신용정보
- 전송 요구의 종료시점
- 전송을 요구하는 목적
- 전송을 요구하는 개인신용정보의 보유기간
- 정기적 전송 요구 여부 및 그 주기

개인신용정보 전송 개요

전송요구 대상 정보 범위 (제33조의2제2항)

- 정보제공자가 신용정보주체로부터 수집한 정보
- 신용정보주체가 정보제공자에게 제공한 정보
- 신용정보주체와 정보제공자 간의 권리·의무 관계에서 생성된 정보

제외 대상

- 민감정보 (개인정보보호법)
- 영업비밀 (부정경쟁방지 및 영업비밀보호에 관한 법률)
- 가공정보 (신용정보보호법)

전송 대상 및 형태 (시행령 제28조의3제4항)

- 거래관계 종료 시점을 기준으로 과거 최대 5년 까지의 정보를 컴퓨터로 처리 가능한 형태로 전송

개인신용정보 전송 개요

즉시 전송 (시행령 제28조의3제4항 및 제5항)

- 개인신용정보 전송요구를 받은 시점에 즉시 전송
- 전산시스템 장애 등으로 전송이 지연되거나 불가한 경우, 사유를 신용정보주체에 통지하고 사유 해소 후 즉시 전송

전송요구 거절 (제33조의2제8항)

- 신용정보주체의 본인 여부가 확인(강력한 본인인증)되지 않는 등 타당한 사유 발생 시 개인신용정보 전송 요구를 거절하거나, 정지·중단 가능

개인신용정보 제공 의무 부여 (제52조)

- 정보주체 전송요구 시 개인신용정보를 전송하지 않을 경우 3천만원 이하의 과태료 부과

개인신용정보 전송 개요

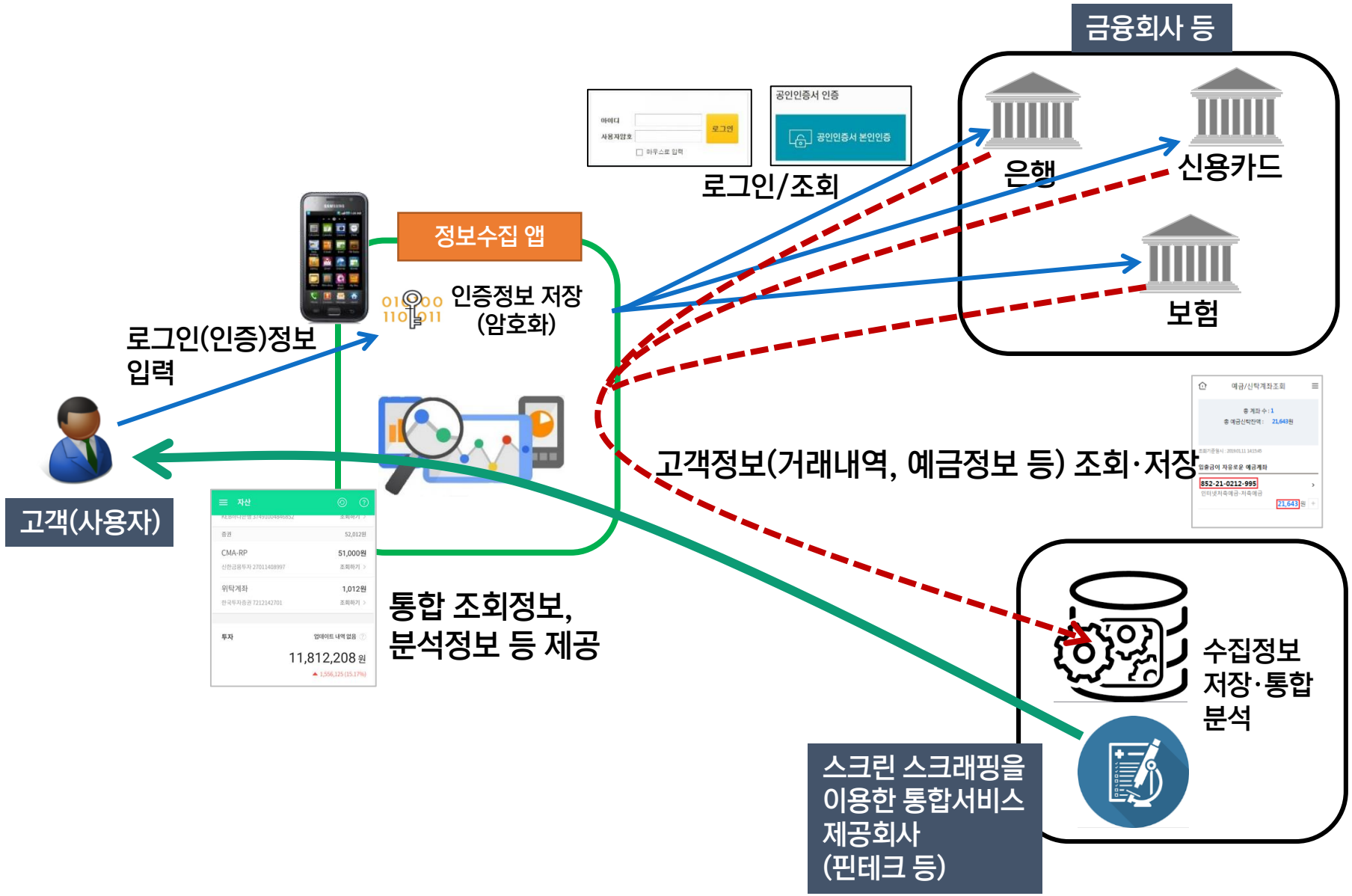
정보주체의 접근매체 사용 제한(스크린 스크래핑 금지) (제22조의9제3항)

- 마이데이터 사업자가 정보주체의 접근매체(ID/패스워드, 인증서, 생체정보 등)를 사용하여 개인신용정보를 수집하는 것을 제한

  ※ 위반 시 6개월 이내 업무정지 가능, 5천만원 이하 과태료 부과 가능

- 마이데이터 사업자가 정보제공자로부터 개인신용정보 수집 시에는 안전성·신뢰성 보장이 가능한 방식(표준 API)으로 직접 전송
  - 개인신용정보 송·수신자 간 미리 정한 방식
  - 개인신용정보 송·수신자 간 상호 식별·인증할 수 있는 방식
  - 정보 전송 시 안전한 알고리즘을 사용하여 암호화 등

(참고) 스크린 스크래핑


금융회사 등
은행
신용카드
보험
로그인/조회
정보수집 앱
인증정보 저장
(암호화)
로그인(인증)정보
입력
고객(사용자)
고객정보(거래내역, 예금정보 등) 조회·저장
통합 조회정보,
분석정보 등 제공
수집정보
저장·통합
분석
스크린 스크래핑을
이용한 통합서비스
제공회사
(핀테크 등)

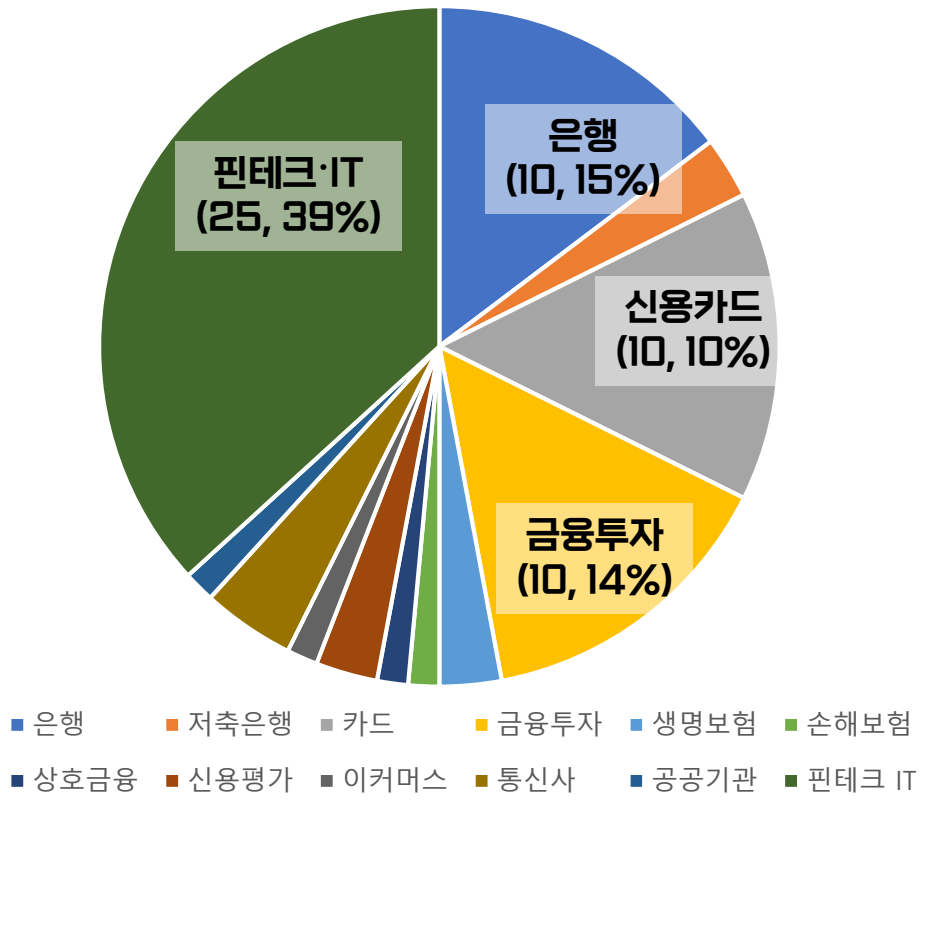
(참고) 스크린 스크래핑

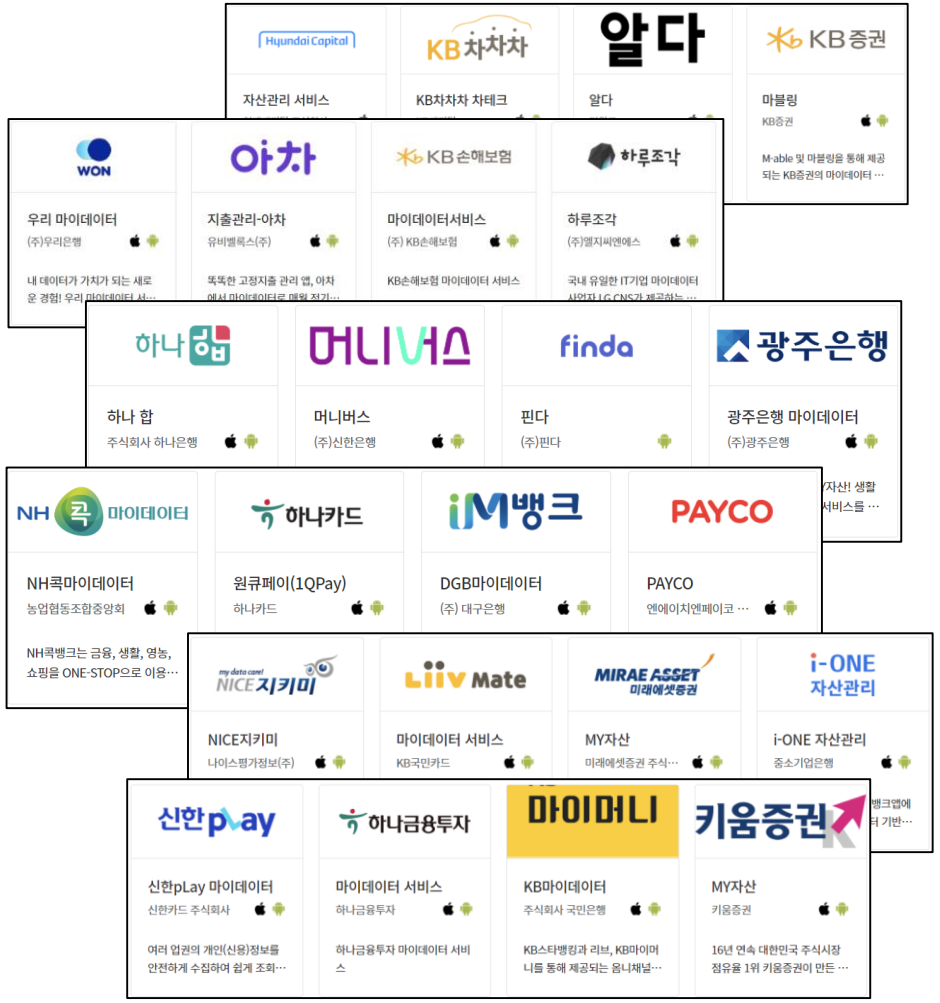
- 다수 웹 사이트에서 사용자의 개입 없이 자체적으로 정보수집 가능
  * 각 사이트마다 사용자 로그인 과정을 별도 수행
- 정보수집을 위한 투자 비용이 상대적으로 저렴(정보제공 협의 불필요 등)

- 사용자의 인증정보(아이디/패스워드, 공인인증서 비밀번호 등)를 프로그램에 저장
  * 인증정보 유출/노출 위험
- 웹 화면에 표시되지 않는 정보는 수집 불가능
- 카카오뱅크 등 앱(App) 기반 화면 데이터는 수집이 어려움
- 스크린 스크래핑 프로그램을 통한 접속시 오류 발생(정보 송수신의 낮은 신뢰성)
- 웹 페이지가 변경되면, 스크린 스크래핑 프로그램 수정 필요
- 스크린 스크래핑 업체가 무슨 정보를 수집하는 지/어떤 활동을 하는지 통제·관리 어려움
  (필요이상 과다 수집?)
- 사고발생시 책임 소재

금융분야 마이데이터 서비스 현황(24년2월)

총 68개사가 본인신용정보관리업자(마이데이터 서비스 사업자)로 지정, 65개사가 서비스 제공 중





금융분야 마이데이터 서비스 현황(24년2월)

서비스 가입자 1억2천만명 (누적)

정보 전송 건수 월간 전송 건수 : 325억건

정보 제공 기관 650여개사 743종 정보 제공(서비스 참여 기준)

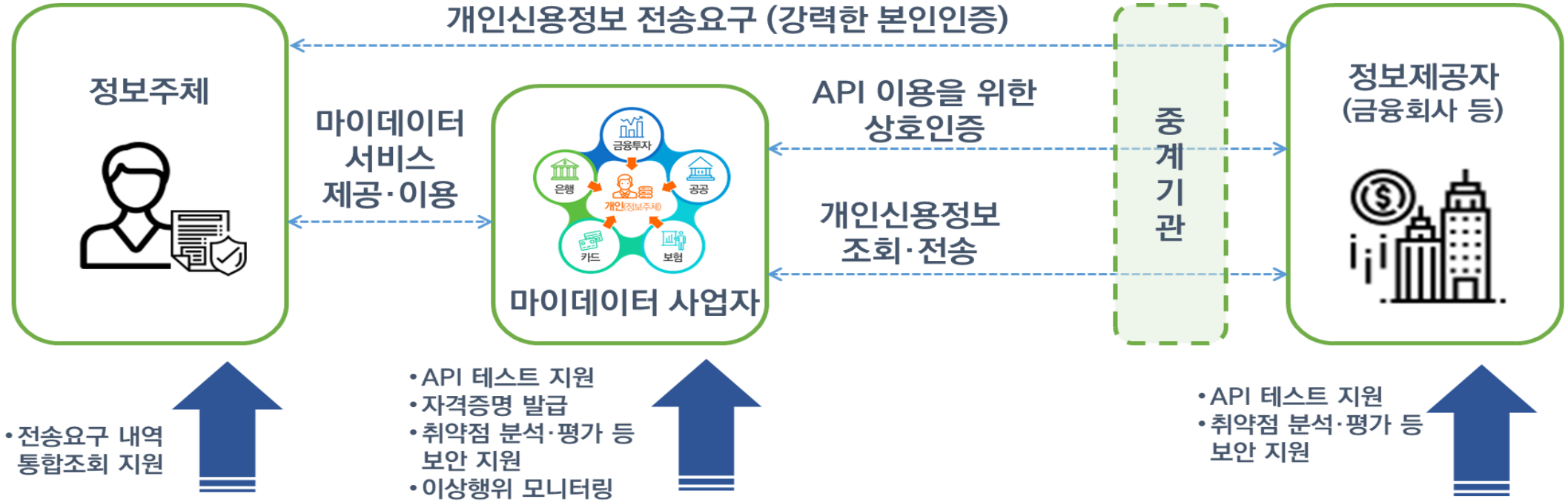
업 권	제공 정보
은행	예·적금 계좌잔액 및 거래내역, 대출잔액·금리 및 상환정보 등
보험	주계약·특약사항, 보험료납입내역, 약관대출 잔액·금리 등
금투	주식 매입금액·보유수량·평가금액 편드 투자원금·잔액 등
여전	카드결제내역, 청구금액, 포인트 현황, 현금서비스 및 카드론 내역
전금	선불충전금 잔액·결제내역, 주문내역(13개 범주화) 등
통신	통신료 납부·청구내역, 소액결제 이용내역 등
공공	국세·관세·지방세 납세증명, 국민·공무원 연금보험료 납부내역 등

금융분야 마이데이터 전송체계 구성

금융분야 마이데이터 전송체계는 정보주체(고객), 정보제공자, 마이데이터 사업자, 통합인증기관, 중계기관 및 지원기관으로 구성

참여자	대상	역할
정보주체(고객)	하나 이상의 정보제공자에 개인신용정보를 보유한 자	▪ 개인신용정보 전송 요구 ▪ 마이데이터서비스 이용
정보제공자 (금융회사 등)	고객의 개인신용정보를 보유하고 있는 자로 신용정보법상 신용정보제공·이용자등	▪ 개인신용정보 제공(전송) ▪ 개별인증수단 발급·관리 ▪ 고객 본인인증
마이데이터 사업자	금융위원회로부터 본인신용정보관리업 허가를 받은 자	▪ 개인신용정보 전송 요구 전달 ▪ 개인신용정보 수신 ▪ 마이데이터 서비스 제공 등
통합인증기관	CI활용이 가능한 인증수단 제공기관 (정통망법 상 본인확인기관 등)	▪ 통합인증 수단 발급·관리
중계기관	금융결제원, 코스콤, 신용정보원 등	▪ 개인신용정보 전송 중계 ▪ 고객 본인인증
지원기관(종합포털)	**금융보안원**, 신용정보원	▪ 마이데이터 활성화 지원

금융분야 마이데이터 전송체계 구성



마이데이터 지원기관

금융분야 마이데이터 전송체계 구성

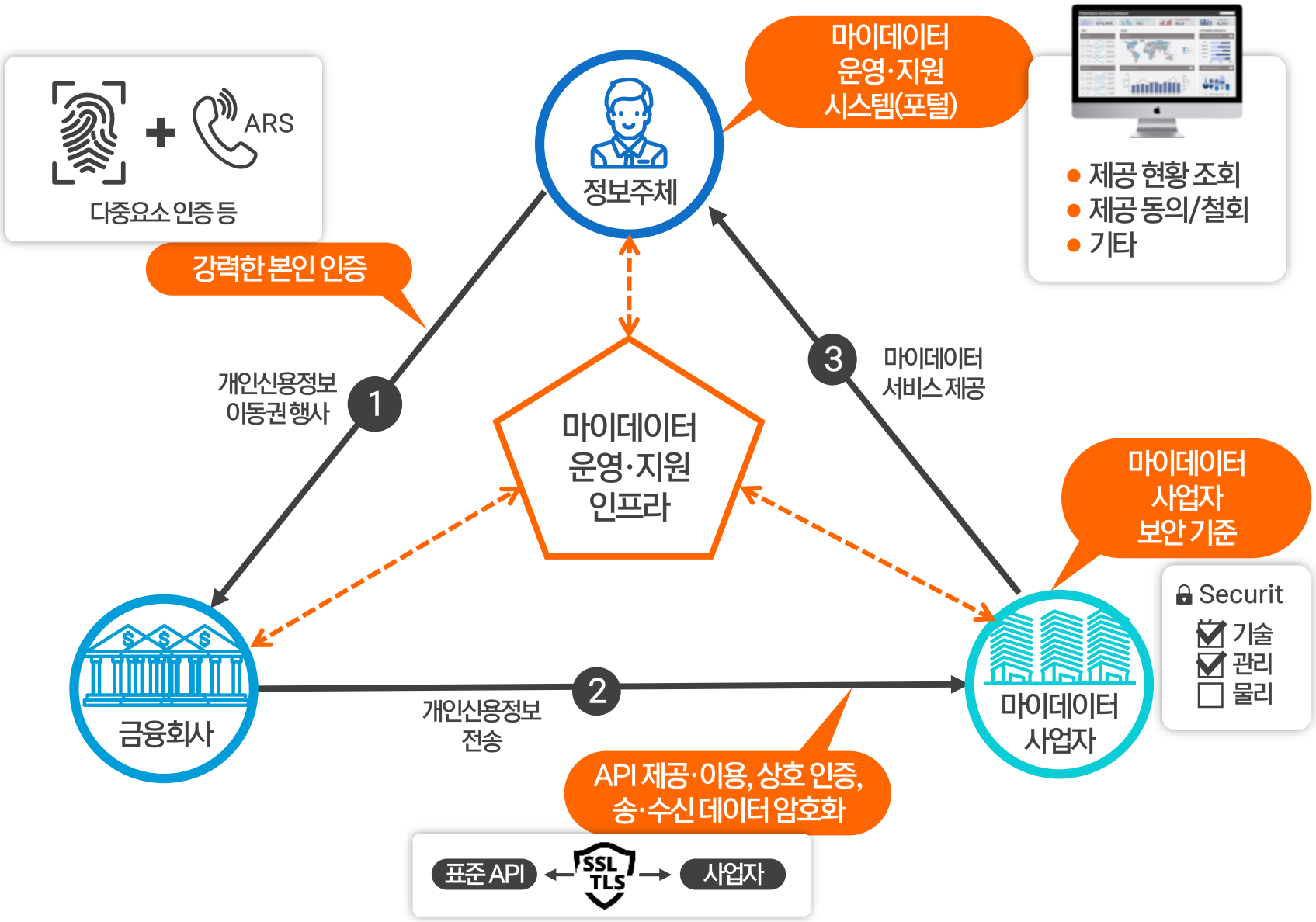
중계기관 (제22조의9제5항)

- 일부 정보제공자(규모, 상거래의 빈도 등을 고려)는 중계기관을 통하여 마이데이터 사업자에게 개인신용정보 전송이 가능
  ※ 금융결제원, 코스콤, 한국신용정보원, KAIT, 저축은행중앙회 등 각 업권 중앙회

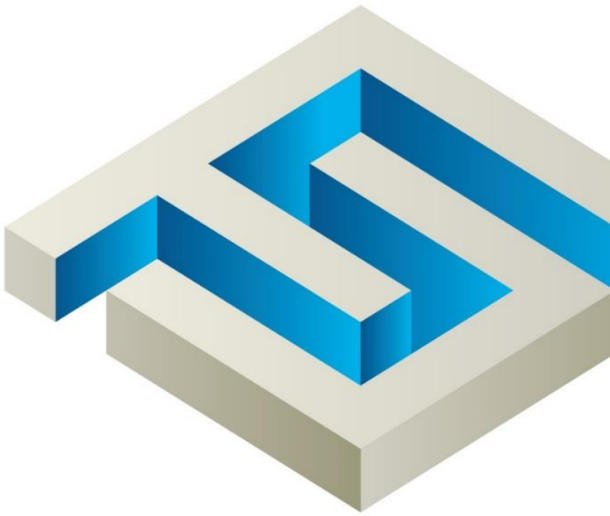
지원기관 (시행령 제28조의4)

- 개인신용정보 전송에 관한 업무를 지원하는 기관
  - 전송요구 가능한 개인신용정보 범위, 데이터 표준화 및 API 규격 관리
  - 전송요구에 따른 비용산정
  - 금융소비자 권리 보장
  - 정보주체 등의 인증기준
  - 안전한 개인신용정보 전송·관리를 위한 정보보호 및 보안 등

금융분야 마이데이터 개요



금융분야 마이데이터 2.0



금융분야 마이데이터 1.0의 한계

- 오프라인에서는 사용 불가?
- 구매 정보는 어디에?
- 접속도 없는데 계속 사용?
- 개인 맞춤형 서비스는?

마이데이터 접근성 확대

오프라인 지점에서 가입·조회·활용 가능

- 현재 오프라인 지점에서는 마이데이터 서비스 가입 불가
- 디지털 소외계층(고령층 등) 지원 강화
- 오프라인 지점에서 마이데이터 서비스 제공
  - 은행·증권사 등 지점 방문
  - 지점 담당자가 정보조회
  - 금융상품에 대한 상담 진행

마이데이터 전송요구 동의 절차 간소화

- 현행 : 1단계(상품목록 조회), 2단계(상세정보 요구)별 동의서 작성 및 인증
  - 모든 동의서를 한번에 확인 후 1회 인증만으로 정보전송 간소화

마이데이터 서비스 수준 제고

마이데이터 물품구매 정보내역 구체화

- 현재 결제 정보는 판매자 정보를 PG사로 제공
- 실제 판매자 정보, 거래품목, 결제 금액 정보 제공
  - 현행 : 2024년4월18일 OOPG사, 5만원
  - 개선 : 2024년4월18일 OO쇼핑몰, 운동화, 5만원

마이데이터를 통한 미사용 계좌 해지·잔고 이전 서비스 확대

- 현재 사용하지 않는 계좌 조회만 가능
- 계좌조회 후, 해지 및 잔고 이전 서비스 제공(금결원 어카운트인포 연계)
  - 현행 : 마이데이터 서비스에서 미사용계좌 조회만 가능
  - 개선 : 어카운트인포와 연계하여 마이데이터에서 계좌해지 및 잔고이전 가능

마이데이터 보안 강화

미접속 마이데이터에 대한 정보 삭제

- 현재 서비스 가입 후 장기간 미접속하는 경우도 정기적전송을 통한 데이터 누적 가능
- 6개월 미접속 시 정기적 전송 중단
  - 현행 : 1년간 미접속시 전송 중단
  - 개선 : 6개월 미접속 시 정기적 전송 중단, 1년 미접속 시 데이터 전체 삭제

제3자 정보제공을 위한 안전장치 마련

- 현재 마이데이터 사업자가 개별적으로 정보주체의 데이터를 제3자에게 제공
- 마이데이터 안심 제공 시스템을 통해 제3자 정보제공
  - 현행 : 정보제공 후 관리가 어려움
  - 개선 : 제3자 정보제공 내역 조회 및 삭제 가능

맞춤형 마이데이터 서비스 확대

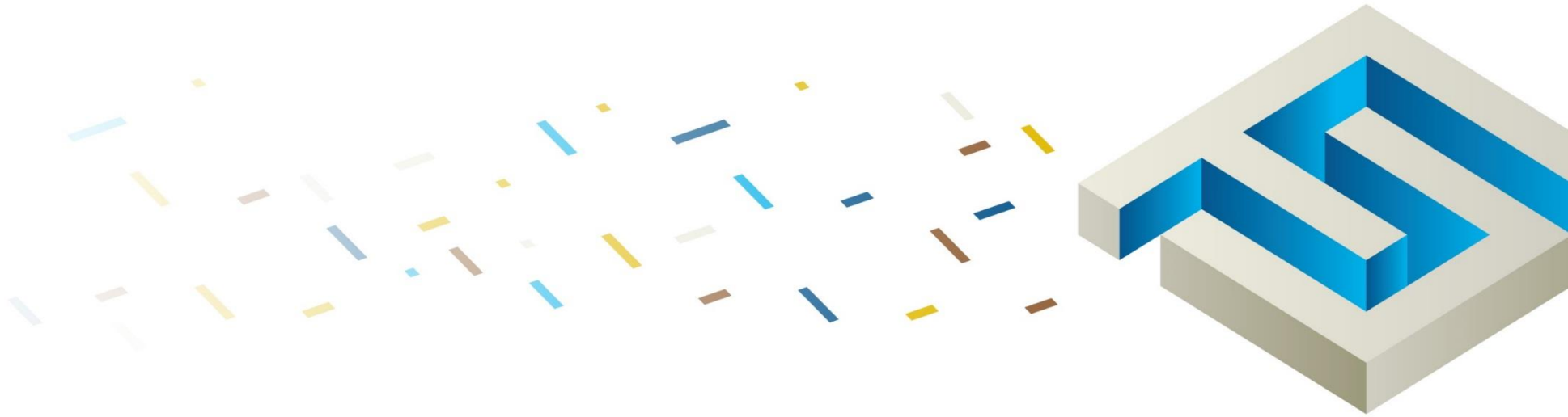
마이데이터 정보 결합 활용 방안 마련

- 현재 명확한 결합 기준이 없어 결합 및 분석을 통한 활용이 사실상 제한
- 정보주체의 동의 범위 및 제3자 제공의 일반원칙을 고려하여 결합 기준 마련
  - 정보주체 동의 시 : 실명으로 이용 또는 제3자 제공
  - 정보주체 미동의 시 : 가명처리하여 활용 또는 제3자 제공

정기적 전송 중심의 마이데이터 서비스 제공

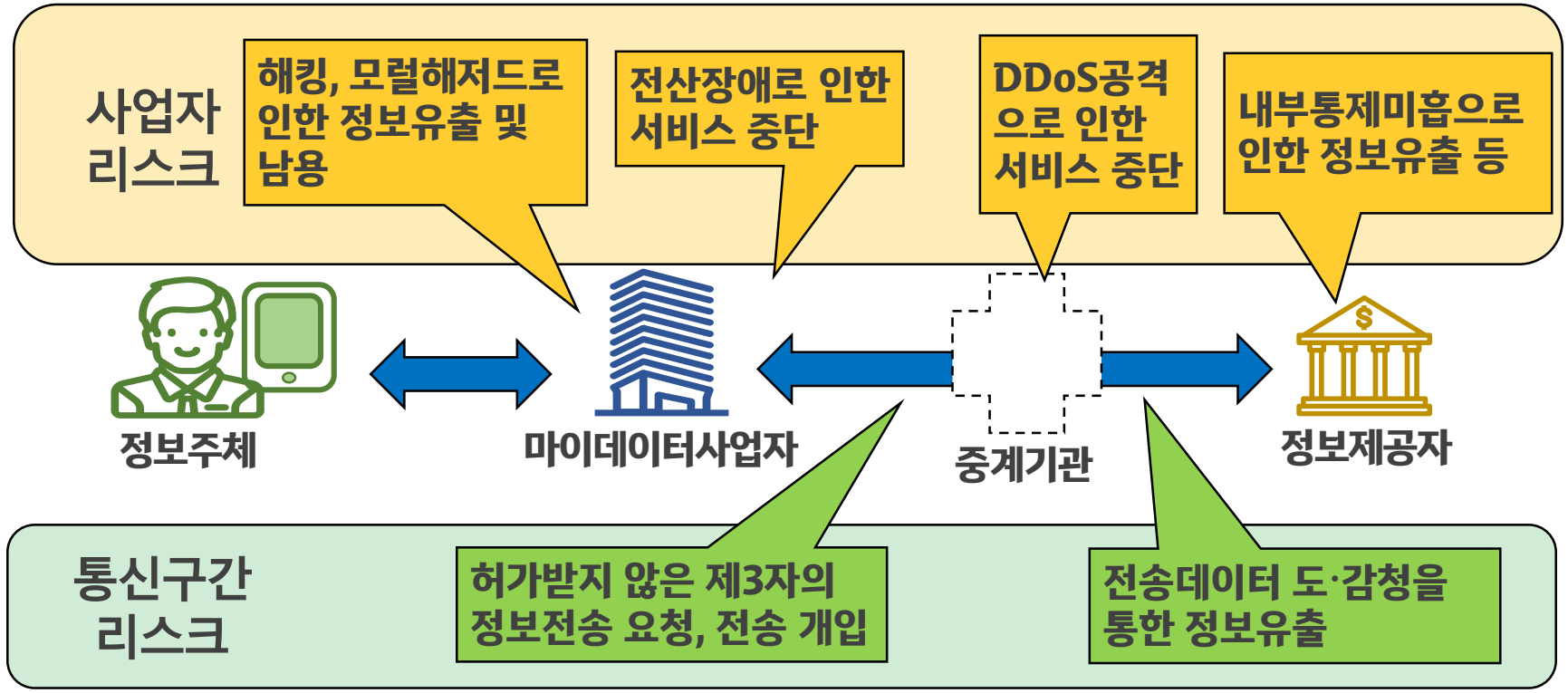
- 현재 비정기적 전송 중심의 마이데이터 사업 운영(과금대상 아님)
  - 과도한 정보 전송 트리픽 발생, 건전한 과금 구조 왜곡
- 비정기적 전송 허용 범위를 제한하여 정기적 전송 중심으로 전환

금융분야 마이데이터 정보보호 체계



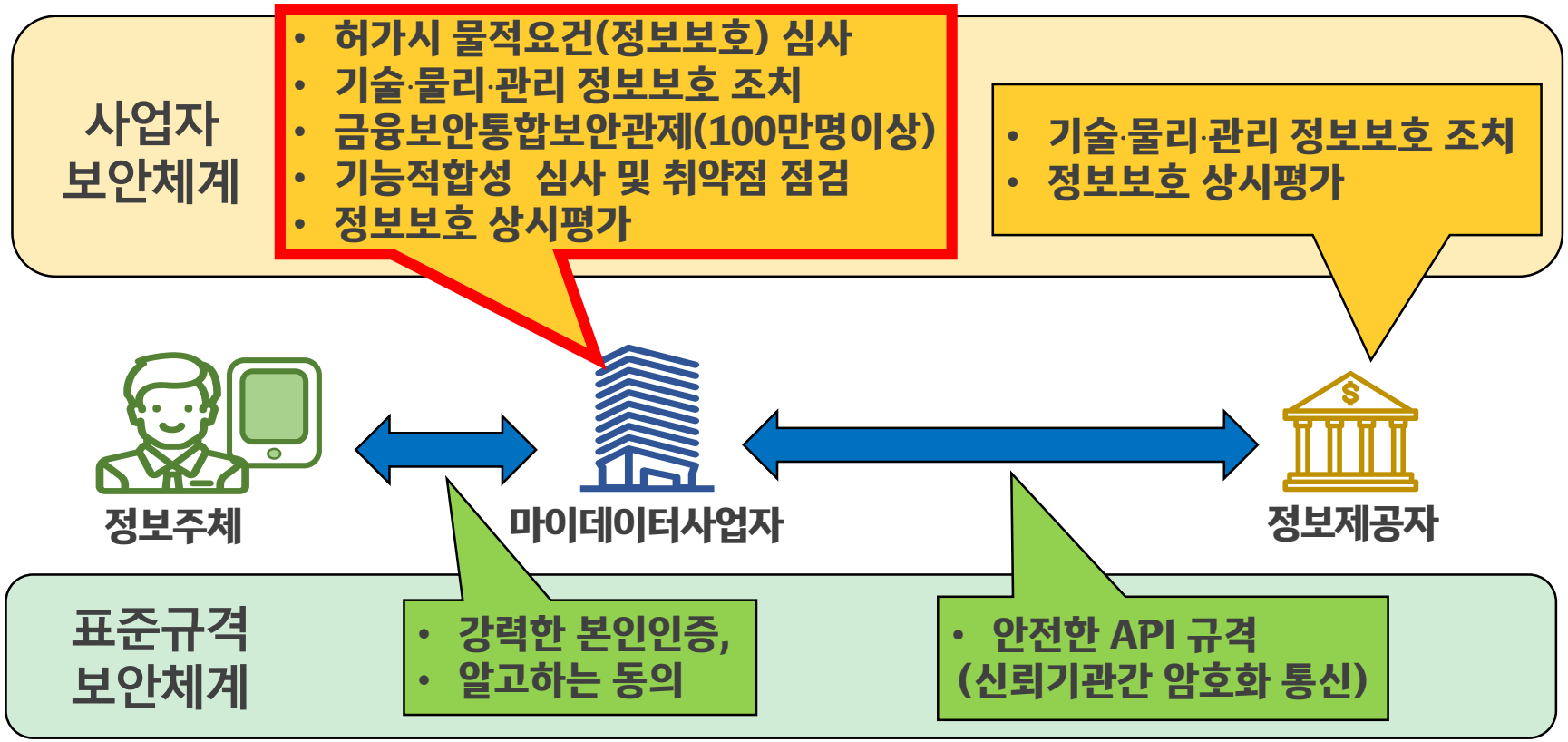
금융분야 마이데이터 주요 보안리스크

마이데이터 사업자 대상 보안리스크와 정보전송 구간 보안리스크로 구분하여 각 구간별 보안대책 마련



금융분야 마이데이터 보안체계 개요

식별된 보안리스크를 해소하고자 수집된 개인신용정보의 안전한 보호와 안정된 서비스 제공과 전송구간에 인증 및 API규격을 통한 신뢰통신 방안을 마련



마이데이터 사업자 보호대책(1)

[금융분야 마이데이터 사업자 허가시 시스템 및 정보보호 대책의 적절성을 심사]

신용정보업 감독규정 별표2의 2

- **관리적 보호대책**
  - 비상계획, 재해복구 훈련 실시 체계, 안전한 백업대책 마련 등
- **기술적 보호대책**
  - 망분리 (전자금융감독규정 제15조제1항제3호 및 제5호)
  - 클라우드 컴퓨팅 이용 시 보호대책 (전자금융감독규정 제14조의2 제1항, 제2항, 제8항) 등
- **물리적 보호대책**
  - 전산실 등에 대한 출입통제 절차, 안전한 물리적 보안설비(통신회선 이중화, CCTV 등) 등

마이데이터 사업자 보호대책(2)

마이데이터사업자는 연1회 이상 취약점 점검을 실시하여야 하며 대형사업자는 금융보안원 보안관제 가입 의무가 부여

- 모든 마이데이터사업자는 점검전문기관을 통해 전자금융기반시설 점검기준에 따라 연 1회 취약점 점검을 실시 (신용정보업감독규정 23조의 3)
- 이용자수 100만명 이상의 마이데이터 사업자는 금융보안원 금융보안관제센터에 가입

개인신용정보 활용관리 실태에 대한 정보보호 상시평가 수행

- 마이데이터 사업자는 연 1회 이상 신용정보법 준수 현황을 자체적으로 점검하고 그 결과를 자율규제기구(금융보안원)에 제출 (신용정보법 제45조의5)

데이터 보유자 정보보호 대책

정보제공자 및 마이데이터 사업자는 관계 법령에 따라 기술적, 물리적, 관리적 보호대책을 수립 이행하고 정보유출시 금융당국에 지체없이 신고

신용정보법 제19조 등

- **관리적 보호대책**
  - 신용정보관리·보호인 지정, 개인신용정보보호 교육 수행, 개인신용정보 관리 정책 마련, 시스템 접근 권한 관리, 직무분리, 접속기록 보관 등
- **기술적 보호대책**
  - 비밀번호 관리, 암호통제, 시스템 보안(접근통제, 침입차단·침입탐지 시스템 운영 등), 컴퓨터 바이러스 방지, 출력·복사 시 보호조치 등
- **물리적 보호대책**
  - 전산설비 분리 설치·운영 등

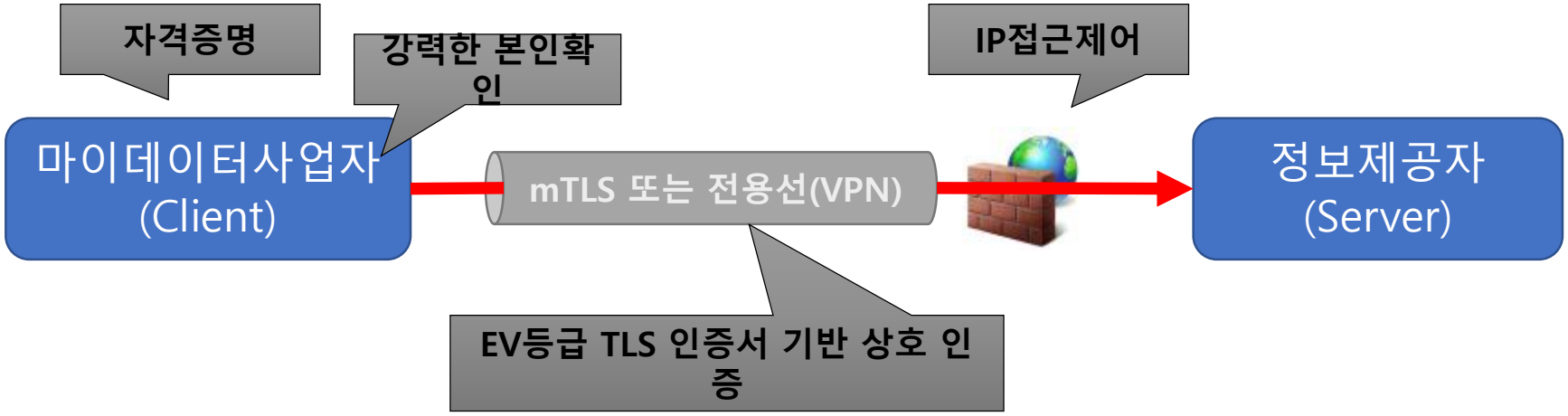
인증 및 전송구간 보호대책

사전에 신뢰성이 확인된 기관만 통신을 허용하고 정보전송은 암호화하여 전송하고 강력한 본인인증을 수행 하여 제3자의 불법적인 접근 및 도감청을 차단

1. 종합포털을 통해 통신기관의 적격여부 확인(서류검토)
2. 적격기관도 통신시 상호인증을 수행하고 암호화를 진행
3. 허가받지 않은 외부접속을 차단하기 위해 사전 등록된 IP만 허용
4. 전송요구시 기관인증을 한번 더 수행하고 강력한 본인인증을 통해 전송요구 수행

인증 및 전송구간 보호대책 개요

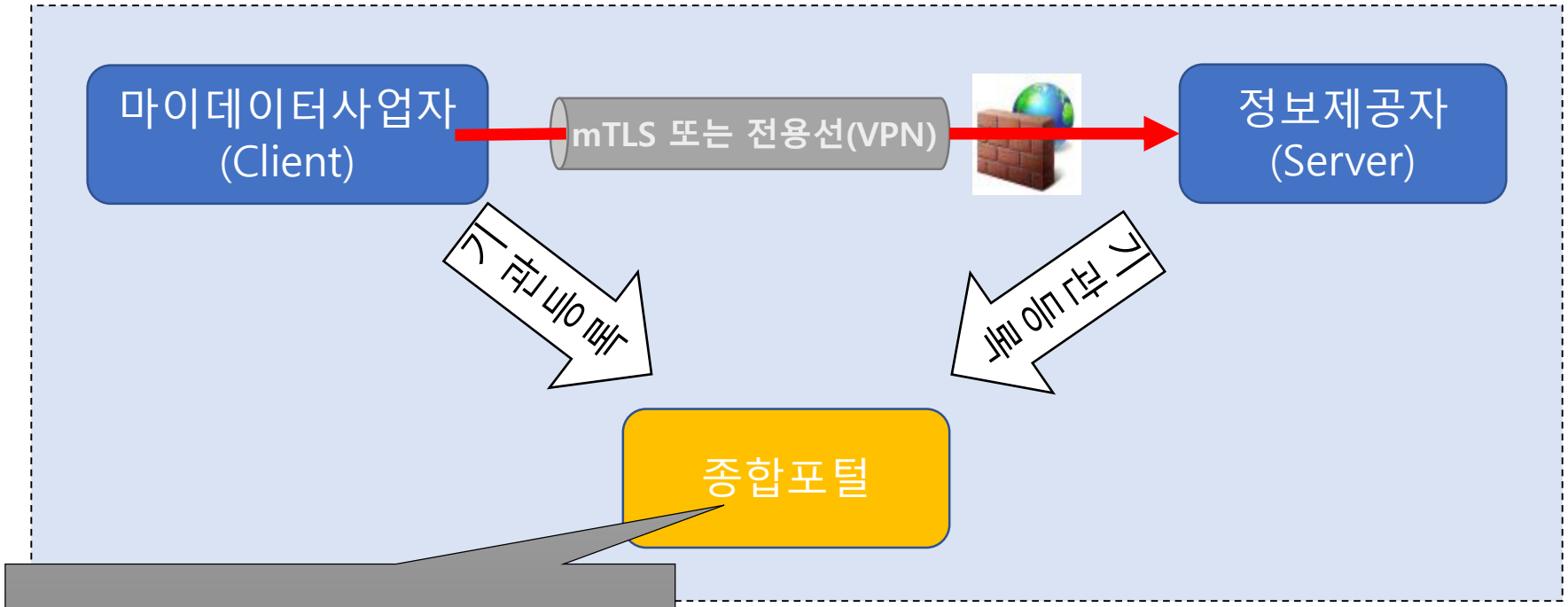
신뢰성이 검증된 기관만 참여하고, 통신구간은 암호화



- 자격증명을 이용한 OAuth 2.0 기반 클라이언트 인증 (신뢰된 지원기관 발급)
- IP 접근제어 (종합포털에 기관정보 등록시 IP 정보도 함께 등록)
- mTLS 또는 전용선(VPN)을 이용한 기관 간 상호인증 및 전송구간 암호화
- 강력한 본인확인(multi-factor) 을 통한 전송요구

전송구간(API) 보호대책(1)

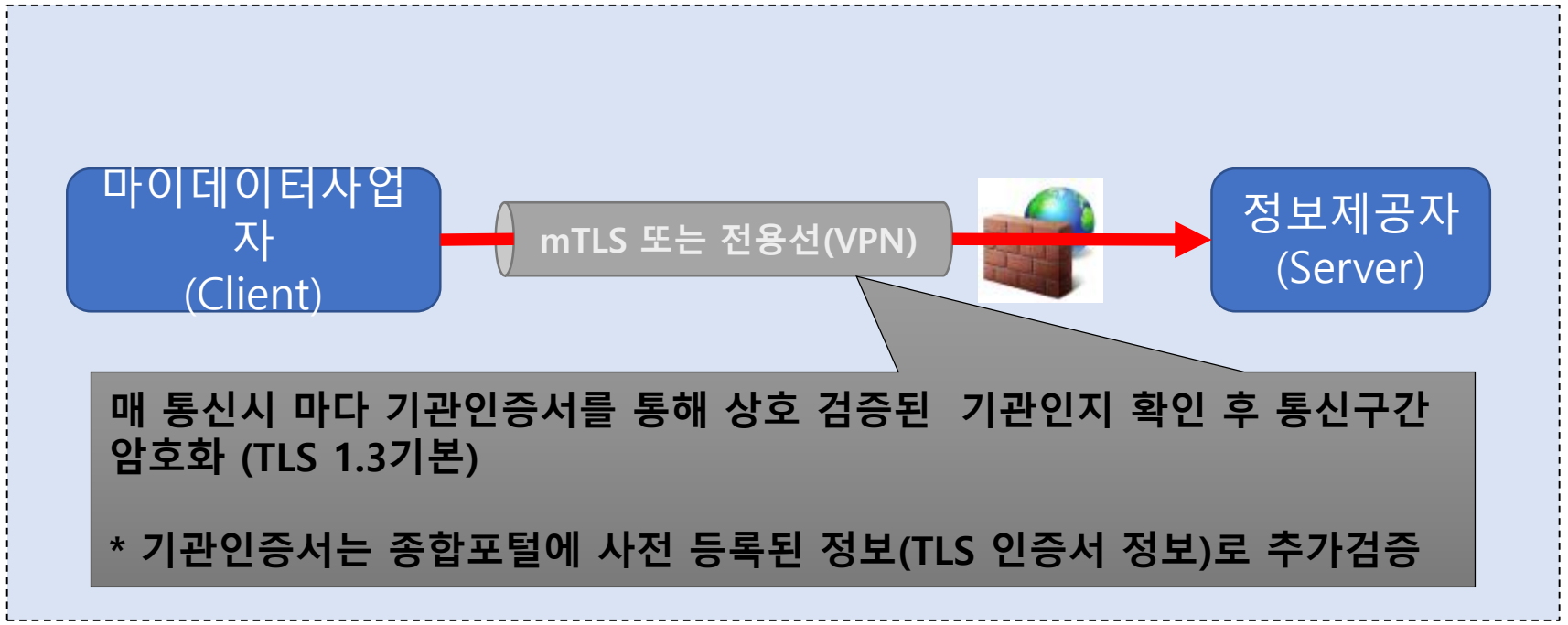
1 종합포털을 통해 통신기관의 적격여부 확인(기관 등록)



종합포털은 해당기관의 적법성,통신 준비상황을 고려하여 기관을 등록

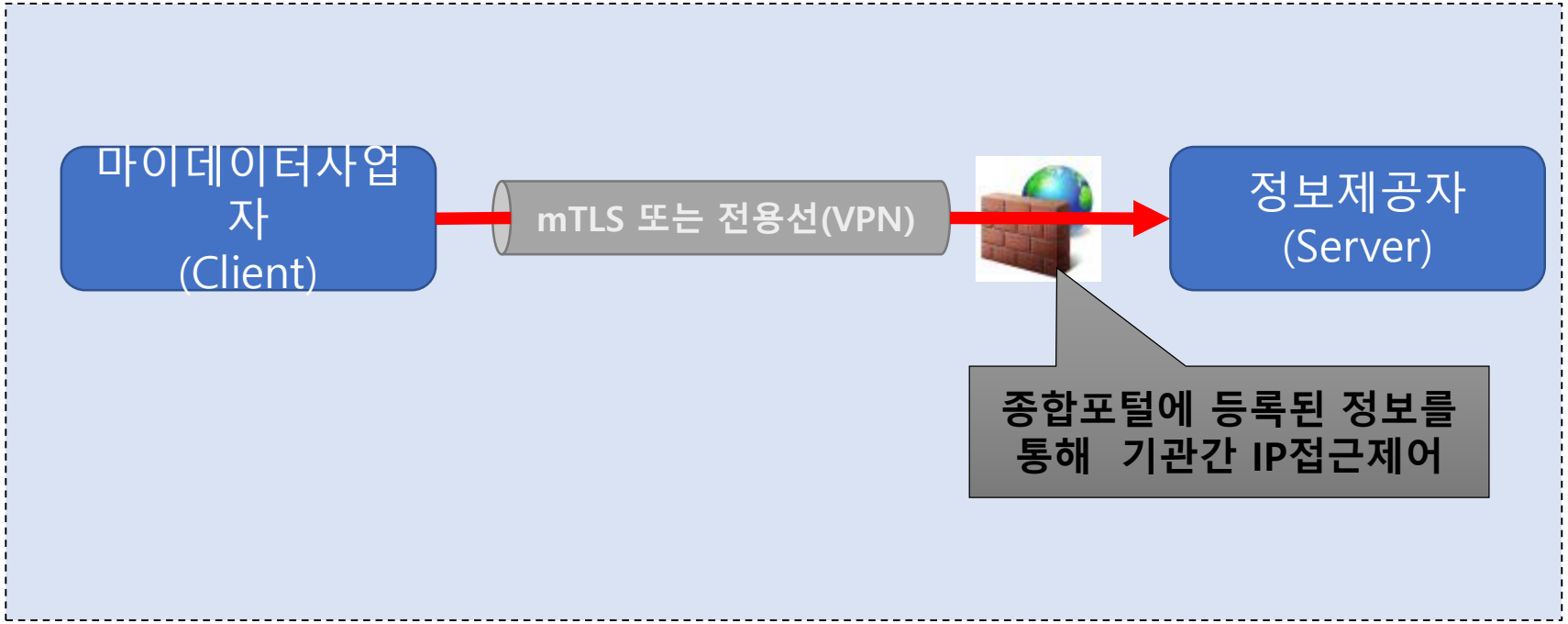
전송구간(API) 보호대책(2)

2 정보제공자와 마이데이터 사업자간 상호인증 수행 및 채널 암호화 적용



전송구간(API) 보호대책(3)

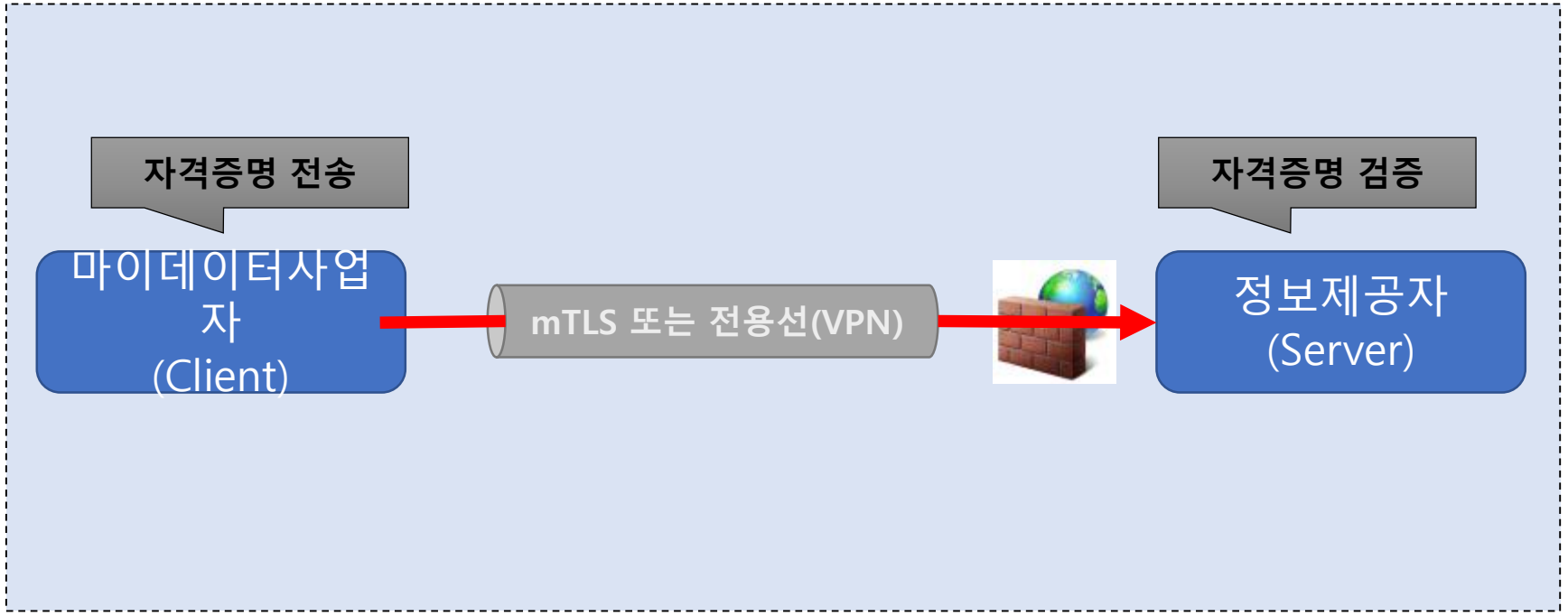
3 화이트리스트(기관 IP)를 적용하여 불법 접속시도 차단



전송구간(API) 보호 대책(4)

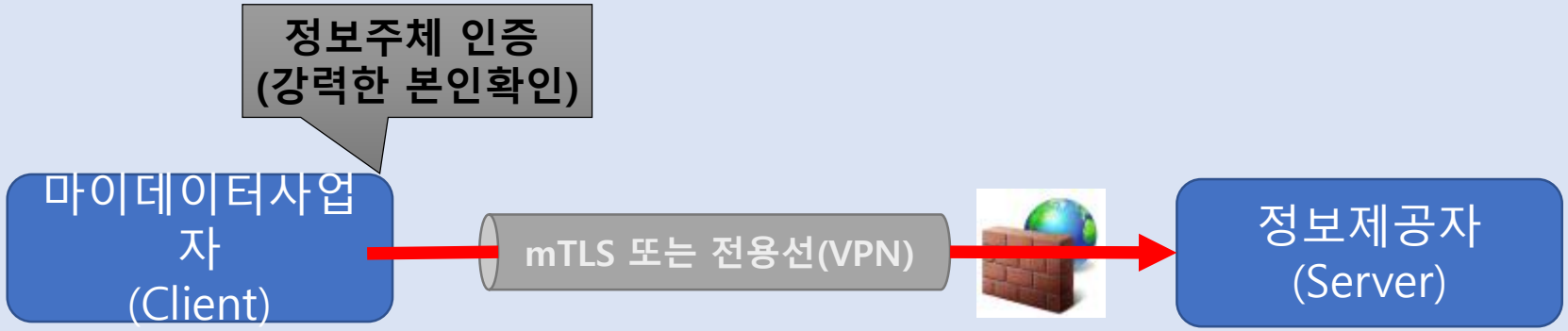
4 정보전송 요청시 사전 발급한 자격증명*을 통해 정당한 마이데이터사업자 여부를 확인

*** 적격 마이데이터 사업자에게 API호출을 위한 ID/패스워드를 사전 발급**



전송구간(API) 보호대책(5)

5 정보주체(고객)가 정보전송 요청시 강력한 본인인증을 수행하고 접근토큰을 발급하여 고객식별 및 마이데이터 사업자의 접근권한을 확인



- **(다중인증)** 2가지 이상의 인증 수단을 중복적용(소유 필수)
- **(공개키 인증서)** 안전하게 생성·보호된 개인키 및 공개키 인증
- **(비대면 실명확인 방식)** 비대면 실명확인 방식 중 2가지 이상 중첩확인

마이데이터 서비스 보안 취약점 점검

마이데이터 서비스 보안성 강화를 위해 연 1회 이상 보안 취약점 점검을 수행하고 결과를 금보원에 제출 (최초에는 서비스 실시전에 수행)

점검 대상·범위	마이데이터 서비스 프로그램(S/W) 및 전산 설비(H/W) 일체
점검 기관	금융위원회 지정 점검 전문기관 또는 마이데이터사업자 자체전담반
점검 주기·시기	연 1회 의무 실시, 마이데이터 서비스 출시 전 점검 완료
점검 기준·방법	전자금융기반시설 취약점 분석·평가 기준 활용 원칙 (5개 분야 375개 항목)
업무 처리 절차	①점검 준비 → ②점검 신청 → ③점검 실시 → ④결과 제출 → ⑤결과 확인 → ⑥결과 보고

감사합니다.

2세션 토론문

(사)디지털금융법포럼
Digital Financial Law Forum

토 론 문

한국은행 추승우 차장

1. 신용정보업감독규정 45조의2조 1항에 따라 신용정보회사, 본인신용정보관리회사, 신용정보집중기관 등은 개인신용정보 활용·관리 실태에 대한 상시평가 수행 후 자율규제기구인 금융보안원에게 결과를 제출할 경우 이에 대한 사후관리(문제점 조치 지원, 조치 결과에 대한 검토등) 방안에 대해 논의

2. 현재 신용정보법 관련 규제 및 제도에서는 명확한 기준이 없는 것으로 판단되는데 마이데이터사업자의 전산장애 또는 보안사고 발생시 효과적으로 대응하기 위한 사고 대응 절차에 대해 논의