# 마이데이터 산업의 법률적 의미와 활성화를 위한 과제

**발표자 : 이규림 변호사**

**주식회사 비바리퍼블리카 법무팀 이사**

본 자료에 나타난 견해나 주장은 발표자의 개인적 주장이나 견해를 나타내며, ㈜비바리퍼블리카 법인의 공식적 입장을 나타내는 것은 아닙니다.

# EU 규제 혁신 – 자기 정보 통제권

## PSD2의 핵심 내용

- **소비자 주도의 계좌 접근권 / 정보 접근권의 제도적 보장**
- **기존 정보 보유 기관의 "의무적" 접근 보장**
  - 서비스업체가 일정한 라이선스를 가지고 있을 것 (AISP, PISP)
  - "정보주체"로부터의 수권(동의)이 있을 것
  - 접근 부여에 있어서 기술적, 보안적 요건 충족

## 산업에 미치는 영향

- **상품 및 서비스 경쟁의 본격화**
  - 계좌개설 여부와 상관없이, 더 참신한 서비스를 제공하는 업체의 서비스 이용
  - 기존 금융기관도 동일한 수혜 가능
- **금융서비스의 접근성 증대 및 소비자 편익 증대**
  - 지점망의 수? 서비스의 퀄리티?

# 마이데이터 산업의 도입이 가지는 의미

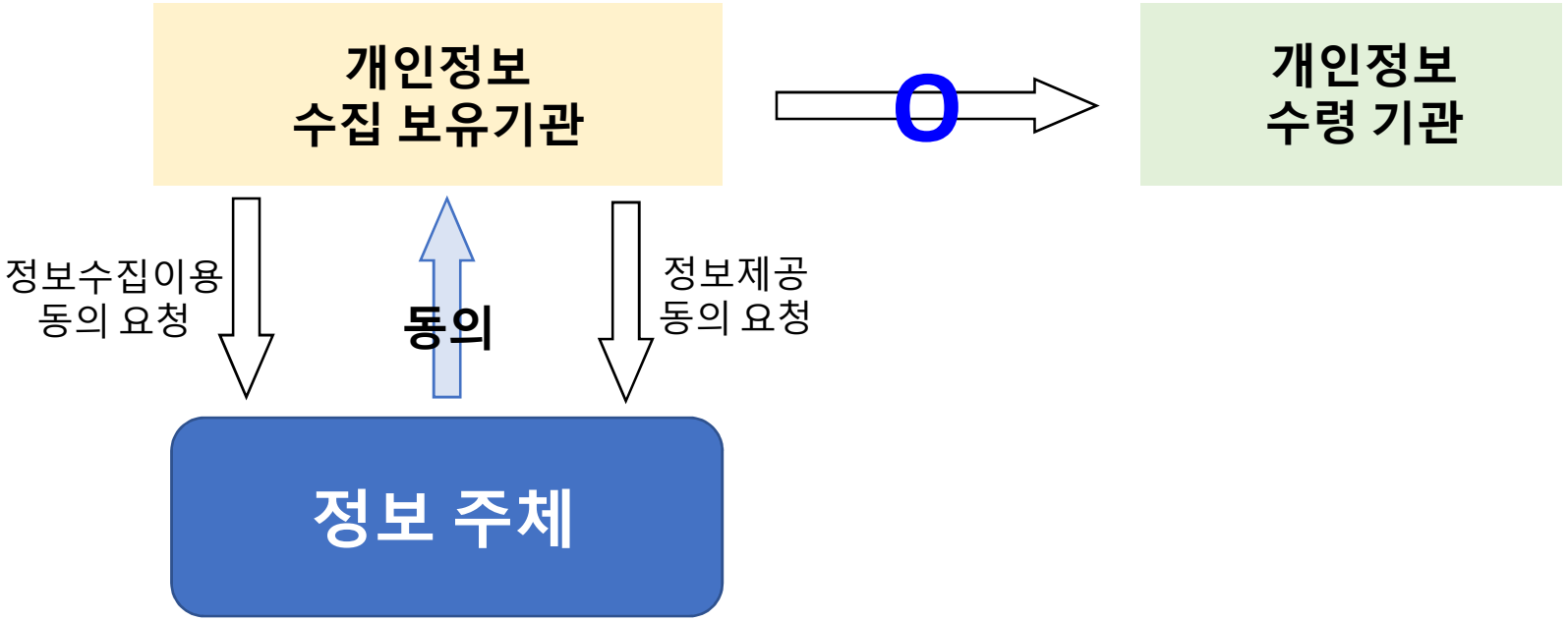
- **"개인정보 주권"의 구성요소**
  - 개인정보의 열람, 정정, 삭제, 통지 요구권 (전통적인 권리)
  - 개인정보의 이용 및 제공 동의권 (전통적인 권리)
  - **개인정보의 제공 요구권 (새로운 권리)**
- **기관이 보유한 개인정보는 누구 소유?**
  - 기관의 소유 ➔ 요구에 대한 거부권 O
  - **개인의 소유 ➔ 요구에 대한 거부권 X**
- **개인 정보의 소유권을 개인에게 환원시키기 위한 장치**
  - 개인의 요구권 및 기관의 거부금지

# 현재의 개인정보 활용의 한계 (1)

- **개인정보의 이동의 개시**

  ➔정보 보유 기관의 필요와 의지에 의하여 정보의 이동이 개시

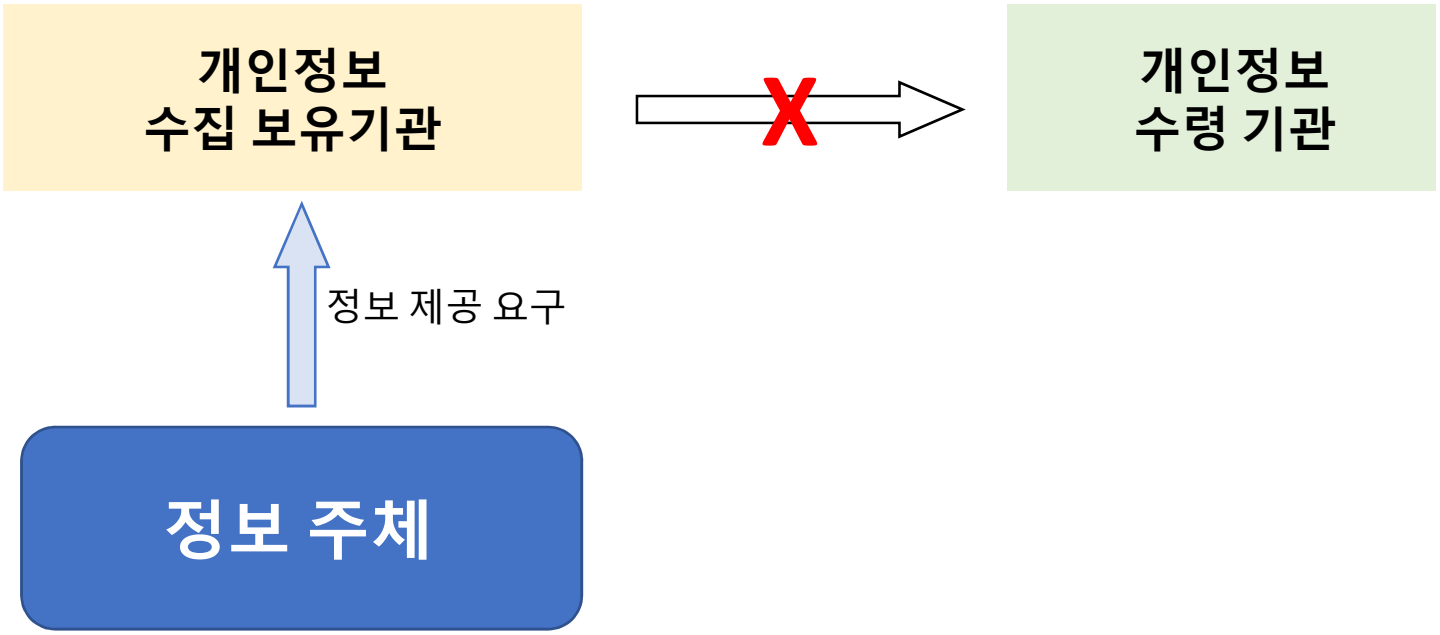
  ➔정보 주체는 수동적으로 “동의”를 제공 해 주는 역할만 수행



# 현재의 개인정보 활용의 한계 (2)

- **개인정보의 이동의 개시**

  ➔정보 주체의 정보 보유기관에 대한 요청으로 말미암아 정보이동이 개시되는 법률적 장치 부재

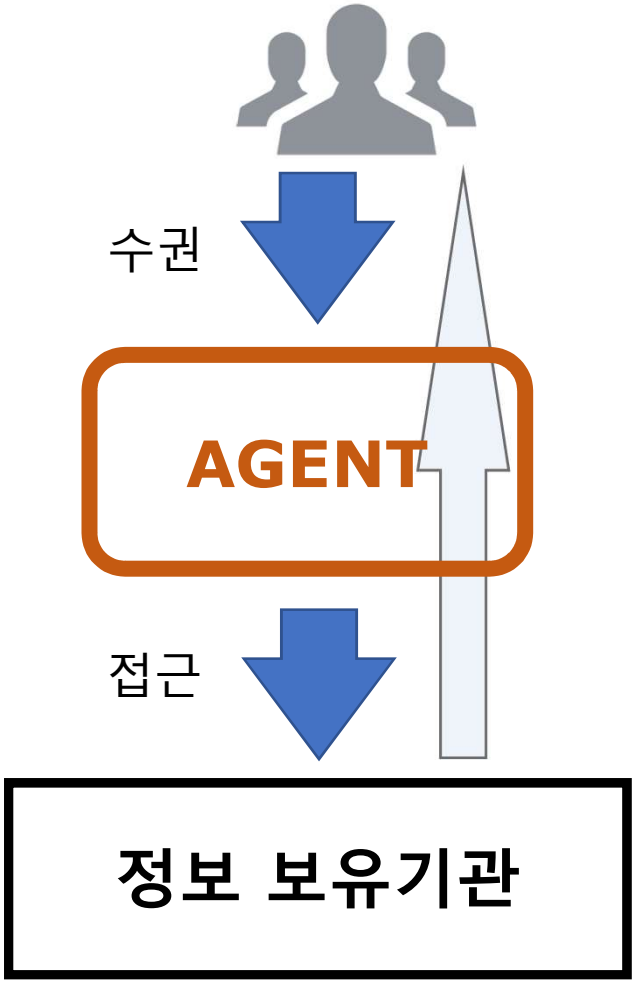


# 개인정보 산업의 현재

- **"본인" 정보 열람 형태의 변형**
  - 대리인 또는 사자(使者) 모델
- **수권의 형태**
  - 정보 주체의 정보 보유기관에 대한 로그인 ID와 PW를 AGENT에게 제공 (수권)
  - AGENT는 **마치 본인이 직접 접속하는 것처럼** 정보보유기관에 접속
  - AGENT는 정보 주체가 원하는 정보를 추출하여 정보 주체에게 제공

**스크린 스크래핑**
**Screen Scrapping**

**WHY? ➔ 정식 제휴 설정 어려움**
**개인정보는 누구 소유?**



# 현재 개인정보 산업의 한계 (1)

- **법령 해석상 법적 지위의 불명확성 (인가대상인지 여부)**
  - "신용조회업"의 개념 범위가 매우 넓음
  - 현행 법령상 **"타인정보"**일 것을 요구하지 않음

8. "신용조회업무"란 **신용정보를 수집·처리하는 행위**, 신용정보주체의 신용도·신용거래능력 등을 나타내는 신용정보를 만들어 내는 행위 및 의뢰인의 조회에 따라 신용정보를 제공하는 행위를 말한다.

**제4조(신용정보업의 종류 및 영업의 허가)** ① 신용정보업의 종류 및 그 업무는 다음 각 호와 같다. 이 경우 제2호 및 제3호의 딸린 업무는 대통령령으로 정한다. <개정 2015. 3. 11.>
1. 신용조회업: 신용조회업무 및 다음 각 목의 업무
가. 본인인증 및 신용정보주체의 식별확인업무로서 금융위원회가 승인한 업무
나. 신용평가모형 및 위험관리모형의 개발 및 판매 업무

9. "신용조사업무"란 타인의 의뢰를 받아 신용정보를 조사하고, 그 신용정보를 그 의뢰인에게 제공하는 행위를 말한다.

# 현재 개인정보 산업의 한계 (2)

- **지속적 서비스 제공의 안정성 측면**
  - 스크래핑 서비스는 정보 보유기관이 제공하는 웹페이지에 접속하여 컨텐츠를 분석하여 필요한 정보를 찾아서 추출해 내는 서비스
    - ✓ 정보 보유기관이 웹페이지의 구성을 바꿀 때마다, 스크래핑 엔진 수정 필요
    - ✓ 정보 보유기관이 ID/PW 또는 공인인증서 외의 추가 인증 수단을 요구하는 경우 사실상 스크래핑 서비스 어려움
    - ✓ 정보 보유기관이 Web service를 제공하지 않고 App service만 제공하는 경우 스크래핑 자체 불가능

- **중요 개인 정보에 관리의 안전성 우려**
  - 스크래핑 서비스는 스크래핑 대상 기관이 많으면 많을 수록, 개인의 다양한 ID/PW를 활용
  - ID/PW의 보관 형태에 관한 안전성 문제

➔ **단, 서버에서 보관하지 않는 방법(단말기상 암호화 하여 보관)으로 안전성 확보 가능**

# 개인정보 산업의 미래 – 마이데이터

- **자기정보 접근권 방식의 다양화**
  - 본인 직접 접근뿐만 아니라,
  - 제3자(대리인 또는 사자)를 통한 접근의 제도적 허용

- **자기정보 접근성의 보장**
  - 제3자를 통한 접근에 대하여도 정보 보유 기관의 접근 거부 금지
  - 단, 정보주체의 수권 기반
  - **정보 주체의 필요와 의지에 의한 정보 이동 개시**

- **정보 접근 방식의 안전성 강화**
  - 개인의 정보보유기관별 ID/PW의 수집 불필요

# 마이데이터 산업의 구체적 구현 요건

- **본인신용정보관리업 라이선스의 보유**
  - 자본금 요건, 인적 요건, 물적 요건
  - 금융위원회의 라이선스 부여

- **정보주체로부터의 수권**
  - 정보주체에 의한, 정보보유기관의 제3자에 대한 정보 지시 동의권
  - 정보주체에 의한, 제3자에 대한 정보 접근 수권

- **의무적, 비차별적 정보 접근권**
  - 정보보유기관은 정당한 이유 없이 정보 제공 거부 금지
  - 정보보유기관은 접근자별 비차별적 정보 접근 허용

# 구현 요건의 실무적 쟁점 (1)

- **진입 장벽의 정도**
  - 허가제 – 개인정보의 강력한 보호 필요성 관점
  - 등록제 – 정보주체의 다양한 접근 채널 확보 및 다양한 사업의 출현과 경쟁 촉진

- **개별 계약의 필요 여부**
  - 마이데이터 사업자와 정보 보유기관간의 개별 계약 (EU는 불필요)

- **정보 관리 책임소재의 명확화**
  - 마이데이터 사업자에 제공된 정보 유출 사고시의 책임
  - 정보보유기관의 책임 제한

# 구현 요건의 실무적 쟁점 (2)

- **정보 주체의 동의 (수권) 구조에 관한 검토**

**"지시권"으로 구성하는 방안**

정보 제공 지시권으로 구성하고, 정보주체의 개인정보 보유기관에 대한 지시로 구성

**핵심 쟁점**

마이데이터사업자가 개인정보 보유기관에게 전달하는 정보주체의 **"지시문서"**가, **정보주체에 의하여 작성된 것인지 증명하는 방법**

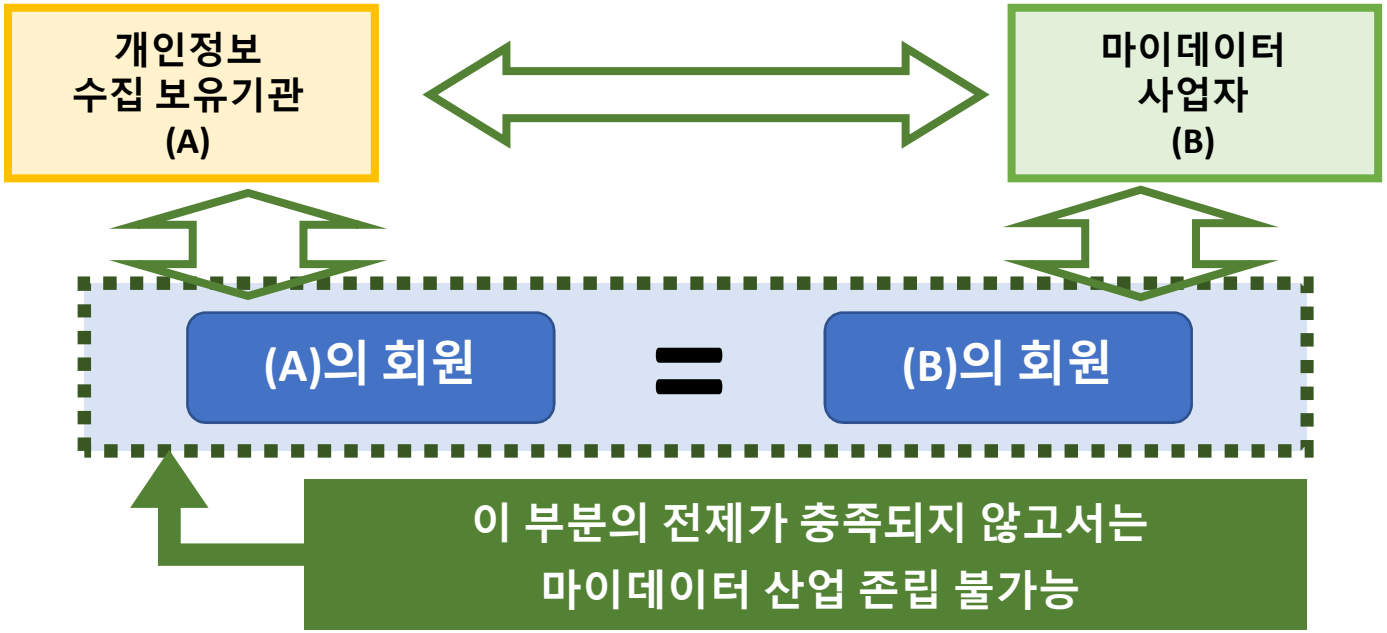
**"대리권"으로 구성하는 방안**

정보주체가 마이데이터사업자를 대리인으로 지정하고, 대리인이 개인정보 보유기관에 접근하는 구성

**핵심 쟁점**

마이데이터사업자가 제시하는 **"위임장"**이 **정보주체에 의하여 작성된 것인지 증명하는 방법**

# 구현 요건의 실무적 쟁점 (3)



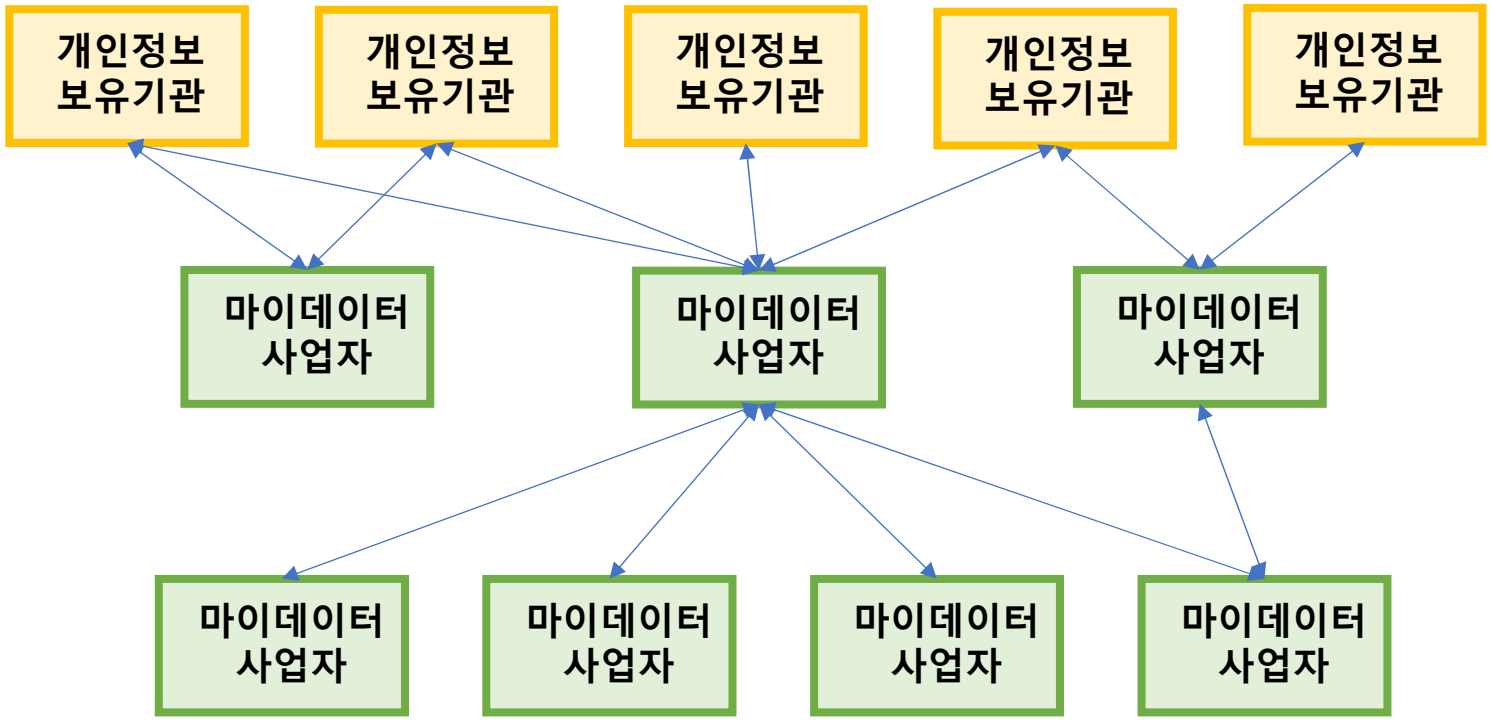

**본인 동일성 확인 요건에 관한 유연한 기준 마련 필요**

- 위험도 기준 = 단순 정보 조회 < 자산의 처분 행위
- 현재 인터넷 뱅킹도 정보 조회는 단순 로그인으로 가능
- 마이데이터 사업자에게 정보를 제공하는 정보 보유기관의 면책 기준 마련 필요

  ➔ 마이데이터 사업 활성화 필수 요소

# 구현 요건의 실무적 쟁점 (4)

- **2중 수권 방식 (API Aggregator)**



# 구현 요건의 실무적 쟁점 (5)

- **정보 보유 기관의 의무적 정보 접근 허용**

**"의무적" 접근 허용 "범위"의 문제**

**정보주체의 정보 주권의 관점 vs. 정보보유기관의 경제적 이익 관점**

- 정보 주권관점에서, 최소한 정보주체에 관한, 정보주체가 생성한 정보는 의무 접근 허용 대상에 포함되어야 할 것
- 정보보유기관이 추가적인 노력 및 가공을 더하여 결합하거나 생성한 정보는 의무 접근 대상에서 배제
  ➔ 정보 보유기관의 재량에 따른 임의 접근 허용
- 법령에 의하여 수집이 제한되는 정보에 대하여는 접근 허용 대상에서 제외

**연계 쟁점**

**API 사용 수수료** : 정보주권 확보 관점에서, 의무 접근 대상 정보에 관한 API 사용료는 무료에 가깝도록 설정하는 것이 타당

# 구현 요건의 실무적 쟁점 (6)

- **정보 보유 기관의 의무적 정보 접근 허용**

**"의무적" 접근 허용 "방식"의 문제**

**API를 이용한 접근 허용 ➔ API의 다양성 확보 방안이 주요 문제**

- ➢ 의무 접근 허용 범위의 정보 제공을 위한 API의 개발 "의무"
  - ✓ API 개발 요청권?
  - ✓ API 개발 이행 의무?
  - ✓ 의무 접근 허용 대상 정보에 관한 API를 제공하지 않는 경우의 처리?
- ➢ 정보보유기관별 API의 표준화 필요성
  - ✓ API의 다양한 출현, 기능적 경쟁 등 시장 경쟁적 관점, 신속한 API의 출시 등 관점에서 표준화가 반드시 바람직하지는 않음
  - ✓ 표준화 되지 않은 API에 따른 효율성은 API Aggregator의 역할로 보완 가능

# 보론: 스크래핑은 나쁜 것?

- **스크래핑 서비스의 장점**
  - 정보 보유기관에서 특정 API를 개발해 주지 않더라도 정보주체가 원하는 정보의 대리 취득 가능
  - 정보 보유기관의 웹을 통하여 입수 가능한 정보는 모두 스크래핑이 가능하므로, 다양한 새로운 서비스의 유연한 개발에 용이
  - 스크래핑은 정보주체에 의한 대리 접근이라는 관점에서 무료

- **스크래핑 서비스 보안 우려에 관한 반론**
  - 정보주체의 인증정보 유출 위험에 관한 우려는, 스크래핑이라는 기술 자체에 내재한 위험이 아니며, 그 서비스를 운영하는 정책과 방식에 내재한 위험
  - 정보주체의 인증정보를 단말기상(Key chain 등)에 암호화 등 보관하고, 스크래핑을 단말기에서(업체의 서버가 아닌) 구동하는 방법으로 정보 보호, 정보 보안에 관한 우려를 상당부분 해소할 수 있음