Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.32, NO.1, Feb. 2022 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2022.32.1.141

금융데이터거래 정보보호 강화방안: 데이터브로커 보안이슈를 중심으로

김 수 봉,[1†] 권 헌 영[2‡]
[1,2]고려대학교(대학원생, 교수)

Reinforcing Financial Data Exchange Security Policy with Information Security Issues of Data Broker

Su-bong Kim,[1†] Hun-yeong Kwon[2‡]
[1,2]Korea University (Graduate student, Professor)

요 약

데이터 경제시대 속에서 활발한 데이터 유통환경을 조성하고자 다양한 정책들이 시행되고 있다. 국내에서는 공공주도 데이터 거버넌스 아래 금융데이터거래소의 출범을 시작으로 빅데이터 유통 플랫폼 형성과 데이터 거래가 시작되었다. 주요 데이터 선진국들의 경우, 오래전부터 데이터브로커 산업을 바탕으로 데이터 유통환경을 구축해왔고, 그로부터 산출되는 부가가치들을 통해 국가 데이터 경쟁력을 강화해왔다. 그런데 데이터브로커를 통해 이루어지는 활발한 데이터 유통의 이면에는 수많은 정보보호 이슈들이 존재하고, 이로 인해 다양한 프라이버시 문제와 국가 안보적 위협들이 발생하였다. 이러한 문제들은 국내 금융데이터 거래 과정에서도 충분히 발생할 수 있다. 본 연구에서는 데이터브로커로 인해 발생한 데이터 거래의 정보보호 이슈를 살펴보고, 정보보호의 관점에서 데이터 거래 시 고려해야 할 사항들을 도출하였다. 이후, 정보보호 고려사항들이 국내 금융데이터거래소 거래단계별 정보보호 정책에 잘 반영되어 있는지 검증해보았다. 이를 바탕으로 금융데이터거래의 정보보호 강화방안을 제시하였다.

ABSTRACT

In the data economy era, various policies are being implemented to create an active data distribution environment. In South Korea, the formation of a big data distribution platform and data trading began with the launch of the Financial Data Exchange under public data governance. In the case of major advanced countries in the data field, they have built a data distribution environment based on the data broker industry for decades and have strengthened national data competitiveness through added values generated from the industry. However, behind the active data distribution through data brokers, there are numerous information security issues, which have resulted in various privacy issues and national security threats. These problems can occur sufficiently in the process of domestic financial data exchange. In our study, we analyzed various information security issues of data trading caused by data brokers and derived information security requirements to be considered when trading data. We verified whether information security requirements are well reflected in the information security policy for each transaction stage of the domestic financial data exchange. Based on the verification, measurements to strengthen information security for financial data exchange are presented in our paper.

Keywords: Data Trading, Data Brokers, Data Security, Information Security Policy, Personal Information

Received(11. 26. 2021), Accepted(12. 30. 2021)

† 주저자, raspberry315@korea.ac.kr
‡ 교신저자, khy0@korea.ac.kr(Corresponding author)

I. 서 론

1.1 연구 배경 및 목적

디지털 환경은 사람들의 삶의 양상을 데이터 중심으로 전환하였고, 데이터의 활용에 담긴 경제적 가치는 걷잡을 수 없을 정도로 증가했다[1]. 그에 따라 데이터는 4차 산업혁명의 핵심 자원이 되었다. 특히 개인의 데이터는 더 많은 가치와 성장 가능성을 지닌 상품으로 주목받고 있다[2]. 데이터를 활용하여 무궁무진한 가치를 창출할 수 있는 환경을 조성하고, 국가 간 데이터 경쟁력에서 우위를 점하기 위해 디지털 선진국들은 앞다퉈 데이터 정책과 제도를 연구하기 시작했다. 세계 주요국들의 디지털 패권 경쟁 속에서 데이터 자원 확보와 데이터 경제 활성화는 국가 전략을 논하는 데 빼놓을 수 없는 요소가 되었다[3].

미국 정부는 마케팅 서비스회사 혹은 소비자 신용 보고·분석회사를 전신으로 하는 데이터브로커(Data Broker)를 중심으로 활발한 데이터 유통과 거래 정책을 펼치고 있다. 과거 데이터브로커는 소비자의 기호를 분석하여 마케팅 전략을 의뢰한 기업에 제공하는 것을 주된 서비스로 하였다. 그런데 소비자들의 구매패턴이 데이터로 변환되어 인터넷 브라우저 혹은 모바일 애플리케이션에 저장되고, 오프라인 시장에서의 결제데이터가 모바일결제시스템, IoT 장치 등을 통해 판매·유통 기업의 서버로 수집됨에 따라 데이터브로커가 소비자들의 '일상활동'을 얻는 것이 수월해졌으며, 일부 소비자들은 데이터브로커에게 직접 본인의 데이터를 직접 판매하기도 하였다.

데이터 산업의 발전과 함께 데이터브로커는 급속도로 성장하였고, 현재 미국은 데이터브로커를 기반으로 민간주도 데이터 플랫폼을 형성하여 경제적 가치창출과 경제·사회 전 분야의 혁신을 도모하고 있다. 하지만, 이러한 성장의 이면에는 개인정보보호와 국가안보에 관련된 다양한 문제들이 존재한다. 일례로 과거 트럼프 행정부는 2021년 1월 중국의 'ByteDance'와 'WeChat' 애플리케이션을 통해 수집되는 사용자 데이터가 중국에서 국가안보를 위협하는 방식으로 작용한다고 판단했기에 해당 애플리케이션의 사용을 금지했다.

한국 정부는 2020년 8월, '개인정보보호법', '신용정보의 이용 및 보호에 관한 법률' 그리고 '정보통신망 이용촉진 및 정보보호 등에 관한 법률'(이하 '데이터3법')의 개정과 함께 데이터를 활용하여 새로운 가치를 창출하려는 목표를 달성하고자 여러 정책과 제도를 시행하였다. 그중에서도 금융위원회에서는 데이터의 활용을 적극적으로 장려하고, 데이터의 검색·계약·결제·분석 등 유통 전 과정을 원스톱(One-Stop)으로 지원하는 금융데이터거래소를 출범하였다.

금융데이터거래소의 활성화를 통해 활발한 데이터 거래환경을 만드는 것도 중요하지만, 동시에 올바른 정보보호 정책을 설계하여 안전한 데이터 거래환경을 조성해야 한다. 거래되는 데이터는 필연적으로 개인정보를 포함하므로 데이터 거래 과정이 안전하지 않다면 데이터브로커의 사례와 같이 개인의 프라이버시 및 국가안보에 심각한 문제를 일으킬 것이기 때문이다. 따라서, 본 논문은 금융데이터거래소를 통해 이루어지는 금융데이터거래가 개인정보보호와 데이터 안보의 관점에서 안전한지 검증하고, 정보보호 강화방안을 제시하는 것을 목적으로 한다.

1.2 1.2 연구 방법

본 연구의 목적을 달성하기 위해서는 현재 금융데이터거래소를 통해 이루어지는 금융데이터거래 과정이 안전한지 파악해야 한다. 안전성을 파악하기 위해서는 적절한 판단 기준이 필요하다. 제2장에서 판단기준을 마련하기 위해 오랜 기간 데이터 거래 시장을 주도해온 데이터브로커의 정보보호 이슈를 사례 중심으로 분석하였다. 데이터브로커로 인해 발생하는 데이터 거래 과정에서의 정보보호 이슈는 크게 네 가지로 구분된다. 해당 이슈들을 사례 중심으로 살펴보고, 안전한 데이터 거래를 위해 필요한 '데이터 거래 시 요구되는 정보보호 고려사항' 다섯 가지를 도출하였다. 이후 제3장에서 앞서 도출한 고려사항들을 판단 기준으로 하여 국내 금융데이터거래소의 데이터 거래 과정을 분석 및 검증하였다. 이를 통해 국내 금융데이터거래소에서 이루어지는 금융데이터 거래 과정의 문제점을 파악하였고, 제4장에서 금융데이터거래 정보보호 강화방안을 제시하였다.

II. 데이터 거래의 정보보호 고려사항

본 장에서는 미국의 데이터브로커 산업의 정보보호 이슈를 살펴보고[10], 데이터 거래 과정에서 발생할 수 있는 문제점들을 파악하였다. 해당 문제점을 해결하기 위한 요소들을 정리하며 안전한 데이터 거래를 위해 요구되는 정보보호 고려사항을 도출하였다.

2.1 데이터 거래의 정보보호 이슈

미국 정부는 연방거래위원회(Federal Trade Commission, 이하 "FTC")에서 데이터브로커 산업을 규제한다. FTC는 데이터브로커를 '다양한 출처를 통해 소비자에 대한 개인정보를 수집하고 해당 정보 또는 해당 정보에서 파생된 정보를 결합, 분석 및 공유하여 상품의 마케팅, 개인 신원확인 또는 사기탐지와 같은 영역에 활용하는 회사'로 정의한다[4]. 연구기관 Upturn에서는 '데이터 주체 자신이 아닌 출처에서 수집된 사람들에 대한 데이터 또는 추론을 제공하여 수익을 창출하는 사업'으로 정의한다[5].

데이터브로커는 주로 (1) 정부 기관 제공정보, (2) 공개정보, (3) 상업 정보 등을 수집한다. 수집 과정에서 데이터의 출처에 대한 평가 기준을 마련하고 충분한 테스트를 통해 상품으로서의 가치를 판단한다. 또한, 신뢰성이 확보된 출처는 계약을 통해 지속해서 데이터를 공급받는다. 데이터 제공기관은 계약을 통해 데이터브로커에게 특정한 목적을 위해서만 데이터를 사용할 수 있도록 데이터 사용 범위를 규정할 수 있다. 추가로, 제공기관의 허가 없이는 데이터를 디코딩 및 리버싱하지 못하도록 제한하거나 FCRA, HIPAA[6], COPPA[7]에 저촉되는 데이터 활용 행위를 제한할 수 있다.

데이터브로커는 위와 같은 데이터 출처에서 수집한 데이터를 활용하여 (1) 마케팅 관련 데이터의 판매, (2) 위험 완화 서비스, (3) 인물 검색 등과 같은 서비스를 제공한다. 또한, 클라이언트의 요구사항에 맞게 데이터를 가공하여 판매함으로써 데이터의 활용도를 높이고 자유로운 데이터 거래환경을 조성한다. 데이터브로커 산업의 이익은 2018년에만 210억 달러였고, 2025년 전 세계 데이터 경제 규모가 4000억 달러에 이른다는 예측을 고려할 때, 전 세계 데이터 시장에서 데이터브로커가 차지하는 비율은 더욱 높아질 것이다[8]. 또한, 2025년에 예상되는 데이터 유통량(175 ZetaBytes)을 고려한다면 데이터브로커의 영향력은 앞으로도 더욱 커질 수밖에 없다[9].

하지만, 데이터브로커의 데이터 거래는 정보보호 관점에서 다양한 문제를 일으킨다. NATO의 보고서를 참고하여 정보보호 이슈들을 (1) 프라이버시 침해, (2) 데이터 유출, (3) 개인정보의 악의적 사용, (4) 데이터 안보 이슈로 분류하였다[10]. 아래에서는 각 이슈를 사례 중심으로 살펴보았다.

2.1.1 프라이버시 침해 이슈

데이터브로커의 데이터 거래 과정에서 발생하는 첫 번째 이슈는 프라이버시 침해이다. 데이터브로커는 소비자의 개인정보를 수집할 때, 해당 정보의 유통에 대한 명백한 동의 없이, 수집 이후 개인정보와 관련된 문제가 발생하면 소비자가 개인정보의 유통 금지를 요청하도록 한다(opt-out). 동의 없이 유통된 개인정보는 소비자가 모르는 사이에 여러 데이터브로커의 데이터베이스에 저장되고, 이것이 프라이버시 침해로 이어진 경우가 많다. 일례로, 2014년 미국의 한 유통업체(OfficeMax)가 고객에게 보내는 홍보 메일 내에 "교통사고로 사망한 딸"이라는 문구가 포함되어 있었다. 해당 소비자는 자신의 딸과 관련된 개인정보를 제공한 적이 없음에도 불구하고, OfficeMax는 데이터브로커의 마케팅 서비스를 통해 관련 정보를 얻게 되었다[11]. 데이터브로커는 적절한 익명화를 통해 소비자의 프라이버시를 보호한다고 하지만, 개인정보 침해와 관련된 이슈들에서 익명화가 제대로 이루어지지 않음을 알 수 있다.

2.1.2 2.1.2 데이터 유출 이슈

다음으로, 고객 데이터의 유출문제이다. 화제가 되었던 사건만 종합해보더라도, 2003년 Acxiom, 2011년 Epsilon, 2015년 Experian, 2017년 Equifax 등 주요 데이터브로커들이 보유한 소비자의 개인정보가 유출되었고, 알려지지 않은 개인정보 유출 사례는 훨씬 더 많을 것으로 추정된다. 특히 Equifax 해킹 사건에서는 공격자가 76일 동안 자유롭게 개인정보를 탈취했고, 총 1억 4600만 명의 피해자가 발생했다[12]. 개인정보 보호조치를 취함에 있어 구글, 애플과 같은 일반적인 IT 플랫폼 기반으로 서비스를 제공하는 기업들과 데이터브로커의 가장 큰 차이점은, 데이터브로커의 경우 자신들이 직접 서비스를 제공하는 고객의 개인정보 외에 간접적으로, 혹은 무관한 사람들의 개인정보도 대량 소유하고 있다는 것이다. 그러므로 데이터 거래 과정에서는 적절한 수준의 정보보호 조치를 하였는지 판단하는 것 외에 개인정보 유출문제에 관한 추가적인 규제가 요구된다. 데이터 거래 과정에서 명확한 피해보상 절차와 정도를 마련하고, 유출된 개인정보로 인한 추가 피해 조사 방안 및 추적 기술을 갖도록 하는 것이 필요하다.

2.1.3 개인정보의 악의적 사용 이슈

세 번째는 개인정보의 악의적 사용문제이다. 합법적인 절차를 통해 거래된 개인정보도 활용 주체에 따라 악의적으로 이용되기도 한다. 예를 들어, 'Cambridge Analytica Scandal'이라고 불리는 사건에서 광고 목적으로 수집된 개인 데이터가 정치적인 조작에 사용되었다. 데이터브로커는 8700만 명이 넘는 개인정보를 수집한 뒤, 이를 정치적 목적의 광고(트럼프 대선 캠페인, 브렉시트 등)에 활용하였다. 또한, 이메일 주소 목록 데이터가 피싱에 악용되거나, 개인정보를 도용하여 신용카드 스키밍에 악용된 사례도 있다. 데이터브로커 혹은 데이터브로커에게서 구매한 데이터들을 광고와 정치적 목적에 사용하는 것이 큰 문제가 되지 않는 경우도 많고, 오히려 소비자들에게 유익한 측면도 있다. 하지만, 일부 허위 광고로 인해 발생하는 피해와 정치적 공격 대상의 사생활 문제를 고려한다면, 데이터 거래 시 윤리적인 관점에서 적절한 조치가 필요하다.

2.1.4 데이터 안보 이슈

디지털 패권 경쟁 과정에서 주요국들은 데이터 문제를 국가안보 관점에서 접근하고 이를 '데이터 안보'로 정의한다[13]. 데이터 안보의 관점에서 데이터브로커의 정보보호 이슈는 크게 두 가지이다. 먼저, 데이터브로커에 대한 해킹공격과 국가안보의 연관성이다. Equifax 해킹의 배후도 중국으로 지목되었다. 중국은 공격으로 얻은 정보를 미국의 해외 정보활동 저지에 활용한 것으로 알려져 있다[14].

다음으로 데이터브로커를 통해 합법적으로 거래된 데이터도 국가안보에 영향을 미친다. 데이터브로커가 거래하는 위치 정보, 개인 신원 정보, 장비 정보 등을 혼합하여 국가안보와 관련된 자산에 영향을 주는 데이터를 얻을 수 있다. 국가안보와 관련된 자산이란, 사람, 장비, 정보, 시설, 활동 등을 말한다. 아래 표 Table 1.에 자산 목록, 관련 취약 데이터 그리고 발생 가능한 위협에 대해 정리하였다.

실제 사례를 살펴보면, (1) 개인이 특정되지 않은 데이터의 집합을 이용하여 특정인(Personnel)의 위치나 활동 이력을 추적할 수 있다. 실제로 핸드폰에서 발생하는 약 500억 개의 신호를 활용해서 트럼프 전 대통령의 이동 경로를 추적한 프로젝트가 진행된 적이 있다[15]. 또한, (2) 데이터브로커가 제공하는 데이터를 통해 군사 장비(Equipment)의 위치를 추적하거나 그것의 능력을 파악할 수도 있고, (3) 프로필 데이터와 위치 데이터를 혼합하여 주요 기관의 직원을 식별하고, 이들의 개인 데이터

Table 1. Risk Taxonomy of Military Organization for Data Security [10]

Asset	Vulnerabilities	Threats
Personal	- Personal information including social media data on personal preferences - Geo-location data	- Extortion / black mail - Manipulation of behavior or opinion - Impersonation or identity theft - Intelligence gathering / Surveillance
Equipment	- Device ID - Data on device use - Data on specific equipment such as credit cards	- Exposure of device IDs - Intelligence on equipment - Mapping of communication patterns - Credit card theft
Information	- Information about personnel - Information about system usage and user behavior	- Information theft via for example spear phishing - Exposure of sensitive information such as lists of personnel etc. - Data leaks/hacks
Facilities	- Geo-location data - Personal information - User data	- Localization of sensitive or secret facilities - Identification of personnel working in specific facilities - Access to facilities via impersonation
Activities	- Geo-location data - Personal information including social media data on personal preferences	- Mapping or tracking of personnel movement - Localization of ops or exercises - Disruption of activities

를 활용하여 제한된 시스템에 접근하거나 민감 정보(Information)를 얻기 위한 공격을 설계할 수 있다. (4) 헬스케어 애플리케이션 데이터를 이용하여 군사시설의 위치를 파악한 사례도 있다[16]. (5) 마지막으로, 모바일 데이터를 활용하여 군인들의 활동(activity)을 추적한 사례도 존재한다[17]. 노르웨이의 언론사 NRK가 영국의 데이터브로커로부터 14만 개의 핸드폰 데이터와 위치 정보를 구매하여 업무 시간 외에 핸드폰 신호의 움직임을 추적하고, 군인들이 거주지와 활동 반경을 식별하였다.

2.2 안전한 데이터 거래를 위한 정보보호 고려사항

데이터브로커와 관련된 여러 사례를 통해 데이터 거래 과정에 존재하는 네 가지의 정보보호 관련 이슈들을 살펴보았다. 데이터브로커를 통해 유통되는 데이터들은 소비자에게 다양한 프라이버시 문제를 일으키고, 더 나아가 여러 데이터를 혼합·가공·분석하여 도출되는 부가 정보들은 국가안보에 중대한 영향을 미쳤다. 이는 국내 금융데이터거래소를 통해 이루어지는 금융데이터거래 과정에서도 유사하게 나타날 수 있다.

다양한 정보보호 이슈들을 종합하여 데이터 거래에 요구되는 정보보호 고려사항을 정리해보면, (1) 데이터의 수집 범위와 규모, 사용에 대한 명확한 규제가 필요하다. 데이터브로커와 같이 데이터 거래의 중재자가 과도한 데이터를 소유하고, 해당 데이터로부터 추가로 확보하는 데이터에 특별한 제약이 없다면 프라이버시 침해가 발생할 가능성이 크다. (2) 데이터를 안전하게 저장하는 것과 함께 확실한 피해 구제 대책을 마련해야 한다. 해킹공격을 예상하는 것은 매우 힘들기에 데이터 유출을 완벽하게 방지하는 것은 불가능하다. 그러므로, 안전한 저장 방안과 함께 피해 발생 이후 구제 대책을 명확하게 수립해야 한다. (3) 또한, 개인정보의 악의적 사용을 방지하기 위해 데이터 판매 이후에도 데이터가 어떻게 활용되는지 추적하고, 관리해야 한다. (4) 데이터브로커와 관련된 프라이버시 이슈를 종합적으로 살펴보면, 결국 데이터 유통의 투명성 보장할 수 있는 정책적 고려가 필요하다. 데이터브로커의 수집, 가공 및 분석, 판매 과정을 공개하고, 데이터의 주체가 자신과 관련된 데이터의 유통 경로를 명확히 인식할 수 있어야 한다. (5) 마지막으로, 데이터 안보를 고려한 데이터 관리가 필요하다. 군사정보와 직접적인 관련이 없더라도, 특정 정보와 혼합 혹은 가공되어 군사적 목적으로 활용될 수 있는 정보는 분리하여 관리해야 한다. 안전한 데이터 거래에 요구되는 정보보호 고려사항을 정리하면 다음과 같다.

① 데이터의 수집 범위와 규모, 사용에 대한 규제
② 데이터의 안전한 저장 및 피해구제 대책 마련
③ 데이터 판매 이후 불법적 이용방지
④ 데이터 주체에 대한 유통 투명성 보장
⑤ 데이터 안보를 고려한 데이터 관리

III. 금융데이터거래소 데이터 거래 과정 분석

국내 금융데이터거래는 금융데이터거래소에서 이루어진다. 금융데이터거래소는 데이터 공급자와 수요자를 연결 및 중재하고, 데이터 검색, 계약, 결제, 분석 등 데이터 유통 전 과정을 지원한다.

금융데이터 거래는 거래의 당사자인 1차 이해관계자, 데이터 거래를 중재하는 2차 이해관계자, 데이터 거래와 관련해 직·간접적인 영향을 받거나 기반 서비스를 제공하는 3차 이해관계자로 구성된다[18]. 1차 이해관계자는 다양한 데이터를 직접 생산하거나 수집 및 가공하여 데이터를 상품화하는 데이터 공급자(Producer)와 그러한 데이터를 활용 목적에 따라 구매하는 데이터 수요자(Consumer)를 말한다. 2차 이해관계자는 공급자와 수요자가 데이터를 교환, 거래될 수 있는 환경을 제공하는 금융데이터거래소이다. 마지막으로 3차 이해관계자는 데이터 거래 플랫폼을 원활히 하기 위해 여러 서비스를 제공한다. 공급자의 데이터 분석 및 가공 단계에 관여하는 데이터 분석가, 가명·익명처리를 돕는 데이터 전문기관을 예로들 수 있다.

금융데이터거래소는 데이터 유통 생태계의 중추 역할을 하고, 수많은 데이터가 거래소를 통해 유통되므로 데이터 공급자와 수요자, 그리고 데이터의 주체 모두가 안전성을 보장받는 공간이어야 한다. 또한, 거래의 대상이 되는 데이터가 데이터 주체의 민감하고, 사적인 정보를 담고 있으므로 거래가 이루어지는 시장은 안전하고, 신뢰받는 장소여야 한다. 금융데이터거래소는 신뢰성 있는 데이터 거래환경을 제공하기 위해 다양한 정보보호 기술과 정책들을 적용하고 있다. 이번 장에서는 사전준비, 거래 및 계약, 사후관리로 진행되는 데이터 거래단계들을 분석하고[18], 앞 장에서 도출한 '안전한 데이터 거

래를 위한 정보보호 고려사항'이 적절하게 반영되어 있는지 살펴보았다.

3.1 데이터 거래단계별 정보보호 고려사항 반영 여부

3.1.1 사전준비 단계

데이터 사전준비 단계는 공급자와 수요자 각각이 데이터 거래를 준비하는 단계이다. 이때, 데이터 공급자는 i) 데이터 상품기획, ii) 데이터 가격 산정, iii) 데이터 가공을 수행하고, 데이터 수요자는 i) 데이터 활용 요건 검토, ii) 데이터 구매 기획, iii) 데이터 상품 검색을 수행한다.

데이터 가공 시에 데이터 공급자는 개인정보에 대해 가명·익명처리를 수행하고, 적정성 평가까지 완료해야 한다. 가명처리란 추가정보를 사용하지 아니하고는 특정 개인을 알아볼 수 없도록 개인신용정보를 처리하는 것이고[19], 익명처리란 데이터 값 삭제, 가명처리, 총계처리, 범주화 등의 방법으로 개인신용정보의 전부 또는 일부를 삭제하거나 대체함으로써 특정 개인을 알아볼 수 없도록 개인신용정보를 처리하는 것이다[20]. 공급자는 사전준비 단계에서 다음을 고려한다. P는 Producer, C는 Consumer다.

P1.1 불특정 다수에게 가명정보 제공 금지
P1.2 수요자의 구매 목적 확인
P1.3 모든 수요자에게 동일한 가명정보 상품제공 금지
P1.4 가명처리 관련 사항의 공개

위와 같은 고려사항을 통해 공급자는 개인정보보호법에 명시된 통계작성, 연구, 공익적 기록보존 등의 목적 외에 가명정보가 이용되지 않도록 조치하고, 수요자의 요구사항에 따라 적절한 수준의 가명처리를 하게 된다. 수요자 다음 사항들을 고려한다.

C1.1 개인식별금지
C1.2 내부관리계획수립
C1.3 제3자 위탁 시 관련 법령 준수

수요자는 구매한 가명정보 상품을 이용하는 과정에서 특정인을 식별하게 된 경우 즉시 처리를 중지 후, 해당 정보를 삭제해야 하고, 신용정보법 제40조의2에 따라 적절한 내부관리계획을 수립하며 제3자에게 가명정보 처리 위탁이 필요한 경우 관련 법령을 준수해야 한다.

사전준비 단계에서는 앞장에서 제시한 다섯 가지 고려사항 중 첫 번째 고려사항(① 데이터의 수집 범위와 규모, 사용에 대한 규제)과 세 번째 고려사항(데이터 판매 이후 불법적 이용방지)이 반영되어 있다. 가명·익명처리를 통해 해당 데이터의 구매 후 활용에 대한 규제장치를 마련하였기 때문이다. 그리고 공급자가 데이터 상품을 기획할 때, 데이터 상품 요구사항을 정의하는 과정에서 데이터 상품의 범위도 지정한다.

그런데 데이터를 직접 수집 및 구매하여 판매 가능한 형태로 가공하는 데이터브로커와 달리, 금융데이터거래소에서는 공급자가 직접 판매할 데이터를 마련한다. 이때, 데이터 공급자가 수요자의 요구조건을 달성하기 위해 데이터를 과도한 범위와 규모로 수집할 위험이 있다. 따라서, 첫 번째 고려사항을 완벽히 충족하기 위해서는 금융데이터거래소에서 공급자의 수집 범위, 규모, 출처 등을 확인하여 데이터 주체의 프라이버시 침해 요인을 검증하는 과정이 필요하다. 아래 Table 2.는 사전준비 단계에서 공급자와 수요자의 고려사항들이 앞선 5가지 정보보호 고려사항을 만족하는지 정리한 것이다. ○는 공급자 혹은 수요자가 고려하는 사항 중에 정보보호 요구사항이 잘 반영되어 있음을 의미하고, △는 미흡함을, ×는 반영되어 있지 않음을 뜻한다.

Table 2. Whether 5 security requirements are reflected in 'Ready to Trade' step

Requirements	Producer	Consumer
①	△ (P1.1 P1.3 P1.4)	△ (C1.1)
②	X	X
③	○ (P1.2)	○ (C1.2 C1.3)
④	X	X
⑤	X	X

3.1.2 거래 및 계약 단계

데이터 거래 및 계약 단계는 i) 공급자와 수요자가 거래대상 데이터에 대해 협의를 진행하는 것으로 시작된다. 거래당사자 간의 협의가 완료되면 ii) 데이터거래소에서 상호 계약서 작성을 진행하고, iii) 이후 대금결제와 데이터 전송이 이루어진다. 일반적

인 거래에서 물건의 양도와 대금결제 그리고 소유권이 이동된 거래대상이 구매자에 의해 사용될 때 발생하는 여러 가지 문제들을 계약에 명시된 조항에 따라 해결한다. 데이터의 거래에서는 거래당사자와 무관한 수많은 제3자의 개인정보가 포함된 경우가 대부분이므로 올바른 계약의 중요성이 더욱 강조된다. 거래 및 계약 단계에서는 안전한 데이터 거래를 보장하기 위해 공급자와 수요자는 아래 다섯 가지를 고려한다. 계약은 공급자 수요자가 동시에 검토하므로 PC로 표현하였다.

PC2.1 계약대상 데이터 검토
PC2.2 권리 범위 설정
PC2.3 데이터 보증
PC2.4 침해 예방
PC2.5 계약의 해지

공급자와 수요자가 계약대상을 검토할 때 양측은 거래대상 데이터와 거래당사자를 명확히 하고, 데이터나 서비스의 적법성 등을 검토하여 거래 가능 여부를 점검한다. 수요자는 계약하려는 데이터에 포함된 공급자 외 제3자의 권리 포함 여부나 데이터의 공동소유 여부를 확인하고, 공급자가 해당 데이터 주체로부터 거래에 대한 동의를 받았는지 확인하여 데이터 권리가 공급자에게 인가되었는지 검토한다. 또한, 개인신용정보 포함 여부를 판단하여 가명·익명처리의 적정함에 대한 보증을 요구해야 한다. 공급자는 자신이 공급하는 데이터가 수요자의 데이터 이용목적이나 활용 대상 서비스에 적합한지 검토해야 한다.

양측이 계약대상과 그에 관련된 권리들에 대한 검토가 끝나면, 데이터의 이용에 관한 수요자의 권리 범위를 설정한다. 공급자는 수요자의 데이터 이용목적을 고려하여 원 데이터와 거기서 파생되는 데이터의 복제, 배포, 전송 등 이용 한계를 설정하고, 재이용 가능 여부, 독점권리 여부, 권리양도 여부 등을 검토한다. 수요자는 공급자와의 계약 목적 외에 설정된 범위를 넘어선 데이터 활용이 불가능함을 충분히 인지하고, 해당 내용을 계약에 포함하여야 한다.

다음으로, 제공된 데이터의 품질 및 보증에 관한 사항을 사전에 협의하여 향후 발생 가능한 분쟁을 사전에 방지한다. 수요자와 공급자는 샘플 데이터를 통해 데이터의 접근성, 활용성, 준거성 등을 검토하고, 제공 데이터에 오류가 발생하거나 품질이 저하될 경우 어느 범위까지 수정·보완이 가능한지 사전에 협의한다. 갱신에 대해서도 주기, 기간, 방법 등을 미리 확인한다.

추가로 수요자가 거래된 데이터를 활용하면서 발생할 수 있는 개인정보 침해사고를 예방하기 위해 수요자가 데이터 이용 권리를 벗어나서 이용하거나 제3자가 불법으로 공급자의 권리를 침해하지 않도록 필요한 조치들을 협의한다. 데이터 수요자의 제3자 복제·배포·전송을 금지하는 원칙을 명확히 제시하고, 데이터 이용 시 출처를 명확히 하며 필요한 기술적·관리적 보호조치를 계약서에 명시해야 한다. 마지막으로 계약의 해지 사유 및 방법 그리고 종료 효과에 대해 검토한다.

데이터 거래 및 계약 단계에서 일어나는 공급자와 수요자의 행위를 분석해본 결과, 정보보호 고려사항 ②(데이터의 안전한 저장 및 피해구제 대책 마련), ③(데이터 판매 이후 불법적 이용방지), ④(데이터 유통의 투명성 보장)이 거래 및 계약 과정에 반영되어 있다. 계약에 이러한 고려사항들이 잘 반영되고 위반사항 발생 시 계약에 정한 절차에 따라 해결된다면 데이터거래소를 통한 데이터 유통은 안전성이 보장된다.

하지만, 계약이 완벽하지 않을 가능성이 존재하고, 계약의 당사자는 데이터 공급자와 수요자이므로 데이터 주체의 권리를 안전하게 보장하기 어려운 문제가 발생한다. 특히, 데이터 유통의 투명성을 완벽히 보장하기 위해서는 데이터 주체에게 데이터 공급자가 누구인지, 데이터 수요자는 해당 데이터를 어떻게 활용할 것인지 등에 관한 정보를 알려줄 필요가 있다. 또한, 데이터 거래 이후 수요자의 불법적인 행위 혹은 불가피한 상황으로 데이터 주체에게 개인정보 침해가 발생한 경우, 어떻게 피해를 구제

Table 3. Whether 5 security requirements are reflected in 'Trade & Contract' step

Requirements	Producer & Consumber
①	X
②	○ (PC2.4)
③	○ (PC2.2 PC2.3 PC2.5)
④	△ (PC2.1 ~ PC2.5)
⑤	X

할 것이며 불법적 이용에 대해 조치할 것인지 대한 규정도 필요하다. Table 3.은 거래 및 계약 단계에서 공급자와 수요자의 고려사항들이(PC2.1 ~ PC2.5,) 앞선 5가지 정보보호 고려사항을 만족하는지 정리한 것이다.

3.1.3 사후관리 단계

데이터 거래의 마지막 단계인 사후관리는 i) 당사자 간 계약에 따른 사후관리, ii) 신용정보법 제40조의2(가명처리에 관한 행위규칙)에 따른 사후관리, iii) 신용정보업감독규정(가명정보 및 추가정보에 관한 보호조치 기준)에 따른 사후관리로 구분된다.

당사자 간 계약에 따른 사후관리는 공급자와 수요자가 계약의 범위 내에서 데이터를 관리하는 것을 말한다. 신용정보법 제40조의2는 신용정보회사 등의 가명처리에 관한 행위규칙을 규정한다('신용정보회사 등은 가명처리에 사용한 추가정보를 분리하여 보관하거나 삭제하여야 한다. 이때 금융위원회가 정하여 고시하는 기술적·물리적·관리적 보호조치를 통해 추가정보의 접근을 통제하는 방법을 준수하여야 한다'). 신용정보감독규정에서도 신용정보법과 마찬가지로 가명정보에 대한 신용정보회사의 조치사항을 규정하고 있고, 공급자와 수요자는 이에 따라 적절한 조치를 이행해야 한다. 이에 따라, 데이터 공급자와 수요자는 아래의 사항을 준수해야 한다.

P3.1 데이터 현황 관리 및 모니터링 결과 확인
P3.2 데이터 품질 보증(가용성, 정확성, 완전성 유지)
P3.3 가명처리에 사용한 추가정보를 분리 또는 삭제
P3.4 기술적·물리적·관리적 보안대책 수립 및 시행
P3.5 가명처리 시 영리 또는 부정한 목적으로 특정 개인을 식별할 수 있도록 처리금지
C3.1 계약에 따른 데이터 현황 관리 및 모니터링
C3.2 데이터 활용 및 보호 활동 점검
C3.3 구매한 데이터의 유출 및 위·변조 방지를 위한 기술적·관리적·물리적 보호조치
C3.4 데이터 구매 후 활용 시 특정 개인이 재식별되면 해당 정보 공급자에게 전송 및 삭제

사후관리 단계에서는 정보보호 고려사항 ②(데이터의 안전한 저장 및 피해구제 대책 마련), ③(데이터 판매 이후 불법적 이용방지), ④(데이터 유통의 투명성 보장)이 반영되어 있음을 알 수 있다. 데이터의 안전한 저장을 위해 공급자와 수요자에게 적절한 보호조치 의무를 부여함으로써 데이터가 안전하게 저장될 수 있도록 하고, 데이터 판매 이후 불법적 이용을 방지하는 것도 관리적 보호조치에 포함된다. 하지만, 사후관리 단계에서도 데이터 주체에 대한 투명성이 보장되지 않는다. 사후관리 단계에서 데이터 수요자가 생성하는 데이터 활용현황, 혹은 데이터 공급자의 모니터링 결과들을 데이터 주체에게 주기적으로 알리는 과정이 필요하다. 또한, 정보보호 조치사항과 결과를 공개함으로써 안전한 거래가 이루어지고 있음을 보장하는 규정들도 필요하다. Table 4.는 사후관리 단계에서 공급자와 수요자의 고려사항들이(P3.1 ~ P3.5, C3.1 ~ C3.4) 5가지 정보보호 고려사항을 만족하는지 정리한 것이다.

Table 4. Whether 5 security requirements are reflected in 'Management' step

Requirements	Producer	Consumer
①	X	X
②	○ (P3.2 P3.4)	○ (C3.3)
③	○ (P3.1 P3.5)	○ (C3.1 C3.2)
④	△ (P3.3)	△ (C3.4)
⑤	X	X

3.2 금융데이터 거래 과정 분석 결과

국내 금융데이터거래소는 민간주도로 이루어지는 데이터브로커와 달리 공공에서 주도하는 정책이다. 또한, 기능을 기준으로 비교한다면 금융데이터거래소와 공급자의 역할을 합친 것이 데이터브로커의 역할과 비슷하므로 운영방식에 차이점이 존재한다. 그러나, 두 정책 모두 데이터 유통을 위해 거래라는 수단을 활용하고, 데이터의 안전한 유통을 위해 법적, 제도적 장치가 마련되어야 하는 공통점이 있다. 즉, 세부적인 유통 방식에는 차이가 있으나 데이터브로커와 금융데이터거래소 모두 데이터를 안전하게 보호하면서 활용가치를 높이려는 정책이다.

제2장에서 상대적으로 오랜 기간 데이터 유통의 핵심 역할을 했던 데이터브로커를 분석하여 데이터브로커 산업이 지닌 데이터 거래 과정의 보안이슈들을 살펴보았다. 이러한 이슈들은 금융데이터거래소에서도 충분히 발생할 수 있으므로 이러한 문제점을

Table 5. Whether 5 security requirements are reflected in each trading steps at financial data exchange

Step & Subject / Requirements	Ready To Trade		Trade & Contract	Management		Result
	Producer	Consumer	Producer & Consumer	Producer	Consumer	
① Restrictions on the scope, scale and use of data	△	△	X	X	X	△
② Safe storage of data and preparation of damage relief measures	X	X	○	○	○	○
③ Prevention of illegal use after data sale	○	○	○	○	○	○
④ Ensuring distribution transparency for data subjects	X	X	△	△	△	△
⑤ Data management considering national data security	X	X	X	X	X	X

예방할 수 있는 정보보호 정책 설계가 필요하다. 이를 위해 데이터브로커 산업의 정보보호 이슈들을 통해 안전한 데이터 거래를 위한 정보보호 고려사항 다섯 가지를 도출하였으며, 국내 금융데이터거래소의 금융권 데이터 유통 가이드를 분석하며 데이터 거래단계마다 다섯 가지 고려사항들이 어떻게 녹아들어 있는지 확인하였다.

결과를 종합하여 Table 5.에 나타내었다. 각 단계에서 두 번째(② 데이터의 안전한 저장 및 피해구제 대책 마련), 세 번째(③ 데이터 판매 이후 불법적 이용방지) 고려사항은 잘 반영되어 있었다. 이는 공공주도를 기반으로 금융데이터거래소가 운영되어 법적, 제도적인 검토가 잘 이루어진 것으로 판단된다.

그런데 첫 번째(① 데이터의 수집 범위와 규모, 사용에 대한 규제), 네 번째(④ 데이터 주체에 대한 유통 투명성 보장) 고려사항, 즉 데이터 주체 대한 정보보호 정책은 미흡했다. 국내에서 개인정보의 활용은 정보 주체의 동의로 시작한다(opt-in). 그래서 정보 주체의 동의만 있으면 개인정보를 소유하고 있는 자(데이터 공급자)가 정해진 권리 내에서 자유롭게 이용할 수 있다. 하지만, 데이터가 거래되기 시작하면 그 활용처가 동의를 얻은 자가 예상한 범위와는 비교할 수 없을 정도로 넓어진다. 그러므로, 유통단계에서 데이터 주체에게 데이터 활용의 투명성을 보장해줄 수 있는 제도적 장치가 필요하다.

또한, 다섯 번째 고려사항(⑤ 데이터 안보를 고려한 데이터 관리)은 데이터 거래에서 고려하지 않은 것으로 판단된다. 거래 및 계약 단계에서 국외 이전에 대한 특약을 넣거나, 사후 관리단계에서 관리적 보호 대책을 통해 유통된 데이터가 국외로 이전되는 것은 방지할 수 있고, 개인정보보호법 제39조12(국외 이전 개인정보의 보호)에서는 국외 이전에 관한 의무사항들을 규정하고 있다. 하지만, 유통과정에서 원 데이터로부터 파생된 데이터나, 가공된 데이터가 국외로 이전되는 것을 규제하는 것은 현실적으로 쉽지 않다. 그리고 데이터브로커의 사례에서 알 수 있듯, 국가안보에 영향을 미치는 이슈들은 국외 이전 이슈보다는 데이터 자체가 군사적으로 가공되고 활용되기 때문에 발생하는 경우가 대부분이었다. 따라서, 안보적 관점의 문제점은 계약과 사후 관리단계에서 데이터 활용을 규제하는 방향으로 해결해야 한다.

IV. 금융데이터거래 정보보호 강화방안

앞 장에서 국내 금융데이터거래소의 거래단계를 분석하며 각 단계에 데이터 거래에 필요한 정보보호 고려사항이 어떻게 반영되어 있는지 살펴보았다. 전반적인 정보보호 고려사항은 잘 반영되어 있으나, 미흡한 점을 발견하였다. 이번 장에서는 해당 문제의 해결을 위해 금융데이터거래의 정보보호 강화방안을 제시하였다.

4.1 공공주도 데이터 거래 거버넌스 강화

국내에선 정부의 주도 아래 금융데이터거래소를 설립하고, 금융데이터거래소에 데이터 유통 생태계의 선도적 역할을 부여함으로써 금융데이터거래에 대한 적절한 수준의 규제가 가능했다. 민간주도의 데이터브로커는 데이터의 유통과 활용이 상대적으로 자유롭다. 하지만, 데이터브로커로 인해 발생하는 사건들을 살펴보면 데이터 주체의 권리가 법적으로 보호받기 어려운 경우가 많고, 데이터브로커로 인해 발생하는 데이터 유출 사고는 매해 증가하고 있다[21]. 그러므로 현재의 공공 중심으로 이루어지는 금융데이터거래 환경은 정보보호와 프라이버시 보호의 측면을 고려했을 때 데이터브로커의 거래보다 우위에 있다. 특히, 두 번째(② 데이터의 안전한 저장 및 피해구제 대책 마련)와 세 번째(③ 데이터 판매 이후 불법적 이용방지) 고려사항이 금융데이터 거래 단계에 적절히 반영된 것도 공공주도 데이터 거버넌스 하에서 데이터3법의 개정을 통해 가명정보의 개념을 법제화하고, Opt-In 중심의 규제를 거래단계에 잘 적용하였기 때문이다.

그런데 데이터 유통으로 인해 더 많은 경제적 효과를 얻기 위해선 데이터 시장 자체의 활성화도 중요하다. 그러므로 현재의 공공주도 거버넌스는 강화하되 이것을 바탕으로 민간데이터거래소를 활성화하고, 관련 부처가 해당 민간데이터거래소의 운영을 관리·감독하는 확장적 움직임도 필요하다. 금융데이터거래소 출범 이전에도 국내에는 다양한 데이터거래소가 존재했다. LG CNS의 빅데이터 공유 플랫폼 'ODPIA', KTH의 'API Store', SKT의 'Data Hub' 등을 꼽을 수 있다[22]. 앞으로 더욱 다양한 데이터거래소 및 플랫폼이 탄생할 것이고, 금융데이터거래소의 정보보호 정책은 이러한 데이터거래소의 본보기가 되어야 한다.

이를 위해서는 데이터 거래 과정에서 개인정보보호와 관련된 문제가 공급자, 수요자, 데이터 주체 등에게 발생하지 않도록 좋은 가이드에 대해 끊임없이 고민하고 개선하며, 관련 부처가 해당 가이드의 이행 여부를 관리·감독하는 구조가 구축되어야 한다. 이는 안전한 민간데이터거래소가 출범할 수 있는 기반이 될 것이다. 안전한 유통 생태계가 형성된다면 여러 기업은 자사의 데이터를 직접 판매하는 비즈니스, 데이터브로커와 같이 데이터를 직접 수집 및 가공하여 클라이언트에게 적절한 데이터를 판매하는 비즈니스도 활성화될 것이다.

4.2 데이터 주체에 대한 데이터 거래의 투명성 확보

4.2.1 데이터 주체의 정보이동권 보호

앞장에서 살펴본 금융데이터거래소의 거래단계에서는 거래 간에 데이터 공급자와 데이터 수요자가 거래 전후로 지켜야 하는 규정들을 중심으로 정보보호 대책이 구성되어 있었다. 물론, 데이터 공급자가 판매할 데이터를 준비할 때, 데이터 수요자가 데이터 구매 이후 데이터를 활용할 때는 개인정보보호법, 신용정보법 등 법률에 따른 규제를 받는다. 그런데 데이터의 소유권 이전이 완료된 상태에서 데이터 주체의 권리를 지키기 위해 사용 이력을 지속 추적하며 데이터 주체의 정보이동권을 보호하기 위한 제도적 장치가 부족하다.

데이터 주체의 권리와 관련하여 마이데이터 사업의 규제방안 마련 단계에서 논의된 바 있다. (i) 마이데이터 사업자에 대해서 강력한 본인인증 절차를 이행토록 하고, (ii) 정보 수집과정의 안전성·보안성을 강화하며, (iii) 정보 유출사태에 대비한 배상책임보험 가입을 의무화하는 한편, (iv) 마이데이터 사업자의 개인신용정보 활용·관리실태에 대한 상시적 평가체계를 구축하는 것이 논의되었다[23]. 개인정보가 다양한 데이터의 분석에 사용되고 있다는 사실과 그 사용처를 인지하고, 활용 여부를 결정할 수 있는 것이 데이터 주체에게 보장된 정보이동권이다. 금융데이터거래소 또한 넓은 범위에서 마이데이터 산업과 연계되어 있고, 데이터의 거래 과정에서 마이데이터에 대한 데이터 주체의 권리를 보장할 수 있는 금융데이터거래소의 감독 기능이 강화되어야 한다. 이는 데이터 주체에 대한 데이터 거래의 투명성을 보장하는 밑거름이 될 것이다.

금융데이터거래소에서 일어나는 행위들은 공급자와 수요자 간의 데이터 거래라는 의미도 있지만, 데이터 주체의 마이데이터가 제3자를 통해 소유권이 이전되는 과정으로 볼 수도 있다. 따라서, 금융데이터거래소는 데이터 주체의 정보이동권을 보호하기 위해 사전준비부터 사후관리에 이르기까지 각 개인정보가 어떻게 가공 및 거래되며, 활용되는지 데이터 주체에게 명확히 알려야 한다. 이를 통해 데이터 주체도 자신의 데이터가 안전하게 거래되는 것을 확인하고, 데이터 거래의 가치를 알게 된다. 궁극적으

Table 6. Examples of Data Broker Registration File in California Government

Data Broker Name	Date Added	Website URL	Email Address	Physical Address
Epsilon Data Management	2020-01-31	us.epsilon.com	privacy_EPS [at] lionresources.com	11030 Circle Point Road, ... ,United States

로 많은 데이터 주체들이 데이터 유통에 참여하도록 유도할 수 있다.

4.2.2 데이터 공급자 등록제 시행

데이터브로커를 규제하고 있는 버몬트와 캘리포니아에서는 데이터브로커 등록제를 시행한다. 데이터브로커로 등록된 회사는 지방 정부의 웹사이트에 엑셀 파일로 공개된다[24]. Table 6.과 같이 해당 파일에는 회사의 이름, 등록일, 웹사이트 주소, 물리적 주소 등의 정보가 포함된다. 또한, 데이터브로커가 중개하는 데이터의 주체가 자신들의 권리를 얻는 방법도 명시되어 있다. (1) 법률에 따라 옵트아웃 권리를 행사하는 방법과 요청 방법, (2) 정보의 삭제 요구 방법, (3) 데이터의 수집 방법에 관한 정보 등이 포함된다. 이를 통해 데이터 주체는 자신에게 보장된 정보이동권을 적극적으로 행사한다.

미국은 데이터브로커 등록제를 통해 데이터 주체의 옵트아웃 권리를 보장하고, 정보이동권을 강화한다. 금융데이터거래소도 데이터 공급자에 대한 등록제를 시행하여 데이터 주체의 권리를 보호할 필요가 있다. 데이터 공급자 등록제를 통해 주요 공급자들의 정보를 공개하면 데이터 주체는 자신들의 개인정보의 사용처를 확인하고, 개인정보 침해 확인 시 해당 개인정보의 삭제를 요구할 수 있다.

4.3 국가안보 이슈를 고려한 정보보호 정책 마련

데이터브로커는 초국가적 행위자로서 데이터 선진국들의 데이터 경쟁력 강화에 앞장서고 있다[25]. 데이터브로커가 생산하는 데이터가 국가안보에 중대한 영향을 미친 사례들을 앞 장에서 살펴보았다. 직접 군사자료 혹은 첩보를 중개하진 않더라도, 데이터브로커에게서 구매한 데이터를 혼합·가공하여 안보관점에서 유의미한 데이터를 생산해내었다.

금융데이터거래소를 통해서도 다양한 소비자 데이터나 위치 데이터 등이 유통될 수 있고, 유통되는 데이터가 혼합·가공되어 국가안보에 영향을 미칠 가능성을 배제해서는 안 된다. 그러므로 데이터 거래 과정에서 데이터 안보에 대한 위협을 고려해야 한다. i) 먼저 데이터 거래 프로세스에서 안보위협을 모델링할 수 있는 위협 모델링 프레임워크를 개발해야 한다. 이를 통해, 데이터 유통 시 발생 가능한 모든 안보위협과 그것을 방지하는데 필요한 요구사항들을 목록화해야 한다. ii) 이후, 거래단계의 정보보호 정책을 설계할 때 요구사항들을 반영한다.

예를 들어, 사전준비 단계에서는 공급자가 준비한 데이터의 내용과 품질에 안보적 위협이 될 요소는 없는지, 수요자의 데이터 활용 이력이 국가안보에 영향을 미치지 않았는지 검증할 수 있다. 또한, 거래 및 계약 단계에서는 거래대상 데이터의 활용가능성, 판매 및 이전 가능성 등을 고려하여 안보적 위협 가능성을 판단한다. 마지막으로 사후 관리단계에서는 해킹위협과 데이터 유출 발생에 대해서 안보적 위협 여부를 판단할 수 있다.

국가안보 이슈를 고려하는 것이 데이터 거래 과정을 특별히 개선해야 한다는 것은 아니다. 데이터 유통이 이미 경제적, 군사적으로 유의미해졌고, 국가 데이터 경쟁력의 바탕이 되는 산업이므로 그 속에서 발생하는 보안 문제들이 국가안보 이슈로 확장될 수 있음을 인식해야 한다.

V. 결 론

본 논문에서는 데이터브로커의 보안이슈를 분석하여 안전한 데이터 거래를 위한 정보보호 고려사항을 도출하였다. 이후, 국내 금융데이터거래소의 금융데이터 거래 과정을 분석하며 앞서 도출한 고려사항들이 잘 반영되어 있는지 검증하였다. 그 결과, 전반적인 거래단계에서 일부 고려사항은 반영되어 있지만, 데이터 주체의 정보이동권에 대한 고려와 데이터 안보에 관한 정보보호 대책이 미흡하였다.

이 결과를 바탕으로 '공공주도 거버넌스 강화', '데이터 주체에 대한 거래의 투명성 확보', '데이터 거

Table 7. Predicting the results of reflecting the three reinforcement measures

Requirements	Present	Result
①	△	○ (4.2)
②	○	◎ (4.1)
③	○	◎ (4.1)
④	△	○ (4.2)
⑤	X	○ (4.3)

래 과정에서 국가안보 이슈 고려'를 금융데이터거래 정보보호 강화방안으로 제시하였다. 이를 통해 Table 7.에 정리한 것처럼 현재의 요구사항 달성 수준을 높일 수 있다. 안전한 데이터 거래를 위한 다섯 가지 고려사항 중 '공공주도 거버넌스 강화(4.1)'를 통해 두 번째(②), 세 번째 고려사항(③)을 더욱 강화한다. '데이터 주체에 대한 거래의 투명성 확보'의 두 가지 방안을 통해 첫 번째(①), 네 번째(④) 고려사항의 미흡한 점을 보완한다. 그리고 '데이터 거래 과정에서 국가안보 이슈 고려(4.3)'를 통해 다섯 번째(⑤) 고려사항까지 금융데이터 거래 과정에 포함할 수 있다. ◎은 정보보호 수준이 강화됨을 의미한다.

빅데이터 시대에 데이터 수집·분석 활용 능력, 데이터 유통환경의 규모 등은 국가의 능력을 평가하는 기준이 되었다. 미국을 비롯한 주요 데이터 선진국들은 이미 데이터브로커를 통해 활발한 데이터 유통 시장을 형성하였고, 그 속에서 얻은 데이터를 국력 경쟁에 활용하고 있다. 데이터 거래는 데이터 유통 환경 조성의 촉매 역할을 하고[26], 국내에서는 금융데이터거래소의 역할이 더욱 중요해졌다. 금융데이터거래소에 대한 정책이 앞으로 생길 여러 데이터 거래소의 본보기가 될 것이기 때문이다.

첫발을 잘 내딛기 위해서는 안전하고, 신뢰받는 데이터 거래환경을 조성하는 것이 무엇보다 중요하다. 안전하고, 신뢰받는 금융데이터거래 프로세스를 구축하고 이를 바탕으로 다양한 분야의 데이터 유통 및 거래 정책을 설계해야 한다. 안전성이 확보된 데이터 거래는 데이터 유통시장의 활성화를 이끌 것이고, 이는 필연적으로 국가 데이터 경쟁력 강화로 이어진다. 결과적으로, 전 세계 데이터 패권 경쟁에서의 우위를 점하게 될 것이다.

References

[1] Tuukka Lethiniemi, "Imaging the Data Economy," 978-951-29-8002-4, University of TURKU, Apr. 2020.

[2] Minna M.Rantanen and Jani Koskinen, "Humans of the European data economy ecosystem - What do they demand from a fair data economy?," HCC 2020: Human-Centric Computing in a Data-Driven Society, vol. 590, no. 1, pp. 1, Nov. 2020.

[3] Kim Sangbae, "Data Security and Digital Hegemony Competition:From the Perspectives of Emerging Security and Complex Geopolitics," National Strategy, 26(2), pp. 5-34, 2020.

[4] Edith Ramirez, Julie Brill, Maureen K. Ohlhausen, Joshua and Terrell McSweeny, "Data Brokers: A Call for Transparency and Accountability," Federal Trade Commission, 2014.

[5] Aaron Rieke, Harlan Yu, Robinson and Joris, Data Brokers in an Open Society, Open Society Foundations, London, pp. 3-4, Nov. 2016.

[6] "Health Insurance Portability and Accountability Act," Pub. L. 104 - 191, 110 Stat. 1936.

[7] "Children's Online Privacy Protection Act," 15 U.S.C. 6501 - 6505.

[8] Strategy+business, "data heroes" https://www.strategy-business.com/article/Tomorrows-Data-Heroes Accessed: Nov. 2021. [Online]

[9] Military Embedded System, "The Big Data Battlefield" https://militaryembedded.com/ai/big-data/the-big-data-battlefield Accessed: Nov. 2021. [Online]

[10] Henrik Twetman and Gundars Bergmanis Korats, "Data Brokers and Security: Risks and Vulnerabilities related to Commercially Available Data," 978-9934-564-31-4, NATO

Strategic Communicaitons Centre of Excellence, Jan. 2020.
〔11〕 NBC Chicago, “OfficeMax Sends Letter to ‘Daughter Killed in Car Crash’,” https://www.nbcchicago.com/news/national-international/officemax-sends-letter-to-daughter-killed-in-car-crash/1986493/ Accessed: Nov. 2021. 〔Online〕
〔12〕 Nick Marinos and Michael Clements, “DATA PROTECTION, Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach,” GAO-18-559, GAO(United States Government Accountability Office), Aug. 2018.
〔13〕 Joonkoo Yoo, “Hybrid Nature of the Data Sovereignty in the Context of Global Security: Perspectives, Trends, and Implications”, National Strategy, 27(2), pp. 115-136, 2021.
〔14〕 LAWFARE, “Data Brokers and National Security” https://www.lawfareblog.com/data-brokers-and-national-security Accessed: Nov. 2021. 〔Online〕
〔15〕 “Opinion|How to Track President Trump”, The New York Times, Dec. 2019.
〔16〕 “Fitness Tracking App Strava Gives Away Location of Secret US Army Bases”, The Guardian, Jan. 2018.
〔17〕 NRK, “NRK Data Disclosing” https://www.nrk.no/norge/mobilsporing_-britisk-dataselger-varsler-intern-gransking-etter-nrk-avsloring-1.15031158 Accessed: Nov. 2021. 〔Online〕
〔18〕 Kim Young Ki, “Guidelines for Financial Data Trading,” AGR-IX-2020-2-191, Financial Security Institute, Oct, 2020.
〔19〕 Credit Information Use And Protection Act, Article 2, 15.
〔20〕 Credit Information Use And Protection Act, Article 2, 17.
〔21〕 Guilherme, Moisés Lima Dutra, Douglas D. J. de Macedo and Angel Freddy Godoy Viera, “Personal Data Protection and Its Reflexes on the Data Broker Industry,” DIONE, vol. 319, no. 1, pp. 103-117. June. 2020.
〔22〕 Daehong Min, “Measures to revitalize data transaction for the development of new ICT-based industries,” KISDI, 18(2), pp. 1-155. Oct. 2018.
〔23〕 Hwangyeong Go, Gyeongmin Son and Seonghwan Ju, ″Information mobility and my data industry″. Business finance law, 93(1), pp. 22-39, 2019.
〔24〕 State of California Department Justice, “data brokers in California” https://oag.ca.gov/data-brokers Accessed: Nov. 2021. 〔Online〕
〔25〕 Kim Sangbae, “National Strategy of BigData”, National Strategy, 21(3), pp. 5-37, 2015.
〔26〕 Yiquan Gu, Leonardo Madio, Carlo Reggiani “Data brokers co-opetition,” Oxford Economic Papers, vol. 1, no. 1, pp. 1-20, Sep. 2021

〈저자소개〉

김 수 봉 (Su-bong Kim) 정회원
2019년 2월: 고려대학교 사이버국방학과 졸업
2020년 3월~현재: 고려대학교 일반대학원 정보보안학과 석사과정
〈관심분야〉 정보보호, 금융보안, 데이터보안, 데이터거래, ICT 관련 법 및 정책

권 헌 영 (Hun-yeong Kwon) 종신회원
1992년 2월: 연세대학교 법학과 학사
1998년 2월: 연세대학교 법학과 석사
2005년 2월: 연세대학교 법학과 박사
2008년 3월~2015년 8월: 광운대학교 법과대학 교수
2015년 9월~현재: 고려대학교 정보보호대학원 교수/사이버보안정책센터 센터장
〈관심분야〉 정보보호, 사이버보안, 사이버안보, 정보화, 전자정부, ICT 관련 법 및 정책, 개인정보보호법 및 정책, 데이터법과 정책