SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

データ流通におけるトラスト管理モデルの技術的課題分析
Analysis of Trustworthiness in Data Trading and Its Technical Issues

磯原 隆将* 中村 徹* 清本 晋作* 田中 俊昭†
Takamasa Isohara Toru Nakamura Shinsaku Kiyomoto Toshiaki Tanaka

キーワード データ流通，トラスト，信頼性評価，社会基盤

あらまし

社会的課題の解決と経済的発展の両立を目指す社会として，フィジカル空間とサイバー空間が緊密に一体化して，双方の空間の間にデータの循環が生じる，データ駆動型社会の構築が進められている．このような社会基盤では，人間が介在せずにマシン同士がデータを処理した結果に基づいて自律的に機能する IoT システムや，多量の学習データから構築されるモデルが各種の判断を行う AI 技術が我々の日常生活に広く深く浸透する．よって，システムが処理するデータが虚偽のものであったり，AI のモデルを構築する学習データが不正なものであったりする場合，フィジカル空間における我々の生活に好ましくない影響が直接的に及びうる[1]．すなわち，データの流通や利活用の場面における安心・安全は，実現すべき最優先課題の一つであり，その要件としては，セキュリティとプライバシの担保のみならず，データが流通するライフサイクルの全体を通じた，継続的な信頼性も確保する必要が指摘されている[2]．

データ自体とその流通における信頼性を対象とする研究開発に，ポリシーやレピュテーションに基づいて信頼性を管理する技術[3]，暗号技術を応用してデータ自体の真正性を確保する技術，統計的な解析やデータの来歴の管理によって信頼性を評価する技術[4]などがある．しかし，いずれの技術もデータ流通のライフサイクル全体を見通した設計や実装とはなっていない．また，多種多様なデータに適用可能な標準的な枠組みも整備されていない．データの流通における継続的な信頼性を確保するためには，複数の異なるユースケースにおいて信頼性が評価可能であること，その評価結果を異なるユースケース間で比較可能な相互運用性を備えることも求められる．

そこで我々は，データの信頼性を確保する手法について，その最新の研究動向をサーベイする．そして，データの信頼性を，流通するデータそのものに起因する要素，データの生成・流通・処理の過程で作成されるメタデータに起因する要素，データとは独立に作成・評価されて存在する要素から定量化され，データが流通するユースケース間において相互に評価可能な概念と定義する．また，データの利用者，仲介者，提供者および信頼できる第三者機関を構成要素とする，データ流通の基本モデルを構築し，これに従って，代表的なユースケースの分類を試みる．これらを通じて，データ駆動型社会に求められる信頼性の確保に向けた現状の課題を整理すると共に，汎用性を備えた統一的なフレームワークの実現に向けて，今後の研究開発に求められる方向性を示す．

参考文献

[1] Mingfu Xue, Chengxiang Yuan, Heyi Wu, Yushu Zhang and Weiqiang Liu, “Machine Learning Security: Threats, Countermeasures, and Evaluations,” IEEE Access, vol. 8, pp. 74720-74742, April 2020.
[2] “System Software to Support Safety, Security, and Trust in the Era of Society 5.0”, CRDS-FY2020-SP-06, 2020.
[3] D. Artz and Y. Gil, “A survey of trust in computer science and the Semantic Web,” Web Semantics, vol. 5, no. 2, pp. 58–71, 2007.
[4] Costa, Felipe Schneider, Silvia Modesto Nassar and Mário Antônio Ribeiro Dantas. “GoAT: A Sensor Ranking Approach for IoT Environments.” CLOSER (2021).

* KDDI 総合研究所, 埼玉県ふじみ野市大原 2-1-15, KDDI Research, 2-1-15 Ohara, Fujimino-shi, Saitama
† 兵庫県立大学大学院，兵庫県神戸市中央区港島南町 7-1-28, Graduate School of Information Science, University of Hyogo, 7-1-28, Minatojima-minamimachi, Chuo-ku, Kobe, Hyogo