

差分プライバシーを適用したクロスサイロ連合学習における インセンティブメカニズムの提案

宮越 奨太[†] 橘 拓至^{††}

[†] 福井大学 工学部 〒910-8057 福井県福井市文京 3-9-1

^{††} 福井大学 大学院工学研究科 〒910-8057 福井県福井市文京 3-9-1

E-mail: [†]shotam@network.fuis.u-fukui.ac.jp, ^{††}takuji-t@u-fukui.ac.jp

あらまし 複数の企業・組織が参加するクロスサイロ連合学習では、多数の企業・組織がローカルモデルの学習に参加することで、訓練データが増加してグローバルモデルの予測精度が向上する。各企業・組織は訓練データを内部でのみ使用し、機械学習パラメータを公開・共有することで、所有データに関するプライバシーを保護している。しかしながら、機械学習パラメータから訓練データを推定される可能性があり、差分プライバシーを用いることで訓練データの推定を回避することができる。一方で、差分プライバシーの利用はグローバルモデルの予測精度を低下させてしまい、他企業・組織の差分プライバシーによって獲得報酬が減少することで参加企業・組織が減少する可能性がある。そこで本稿では、差分プライバシーを用いたクロスサイロ連合学習において社会余剰最大化を達成するインセンティブメカニズムを提案する。提案するメカニズムでは、組織間で金銭移転を行うことでクロスサイロ連合学習への積極的な参加を促す。提案法の性能はシミュレーションで評価し、各組織が協力してプライバシーを保護しながら社会余剰を最大化することを示す。

キーワード 連合学習, 差分プライバシー, インセンティブメカニズム, 分散アルゴリズム

Proposal of Incentive Mechanism for Cross-Silo Federated Learning with Differential Privacy

Shota MIYAGOSHI[†] and Takuji TACHIBANA^{††}

[†] School of Engineering, University of Fukui 3-9-1 Bunkyo, Fukui, Fukui 910-8507, Japan

^{††} Graduate School of Engineering, University of Fukui 3-9-1 Bunkyo, Fukui, Fukui 910-8507, Japan

E-mail: [†]shotam@network.fuis.u-fukui.ac.jp, ^{††}takuji-t@u-fukui.ac.jp

Abstract In cross-silo federated learning, where multiple companies/organizations participate, the prediction accuracy of the global model is improved by increasing the training data when a larger number of companies/organizations participate in the learning of the local model. Each company/organization protects the privacy of its own data by using the training data only internally and disclosing and sharing the machine learning parameters. However, there is a possibility that the training data may be reconstructed from the machine learning parameters. This reconstruction can be avoided by using differential privacy. On the other hand, the prediction accuracy of the global model is reduced by using the differential privacy. The differential privacy of other companies/organizations may reduce the number of participating companies/organizations by decreasing the obtained revenue. Therefore, in this paper, we propose an incentive mechanism to maximize social surplus in cross-silo federated learning with differential privacy. The mechanism encourages active participation in cross-silo federated learning by transferring money between companies/organizations. We evaluate the performance of the proposed method by simulation and show that each company/organization cooperates to maximize the social surplus while protecting privacy.

Key words Federated learning, Differential privacy, Incentive mechanism, Distributed algorithm