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

ビザンチンロバストな連合学習における学習モデル保護の基礎検討
Towards Trained Model Protection for Byzantine-Robust Federated Learning

中井 綱人 *† 鈴木 大輔 * 藤野 毅 †
Tsunato Nakai Daisuke Suzuki Takeshi Fujino

キーワード 連合学習，Trusted Execution Environment，Intel SGX，準同型暗号，Microsoft SEAL

あらまし

連合学習 (Federated Learning) は，サーバやクライアント間と学習データを共有することなく，共同でモデルを学習することができる技術である．連合学習は，学習データの代わりに，各クライアントで学習したモデル情報 (クライアントモデル) を共有する．クライアントは，自身が保有するプライバシー情報や機密情報を含むデータを学習データとしてサーバへ提供する必要がないため，学習データのプライバシーや機密性に配慮した技術として注目されている．

連合学習におけるクライアントモデルの共有には，主に，モデル情報保護とビザンチン耐性に関する 2 つのセキュリティ課題が指摘されている．近年の研究によると，連合学習において，サーバに集約されるクライアントモデルから，クライアントの学習データに関する情報が推測できると報告されている．また，大量の学習データにより生成したモデル情報自体は，知的財産として保護することも考えられる．したがって，モデル情報の保護が必要とされている．一方で，近年の研究では，連合学習システムにおいて，学習モデルの性能や学習の収束を損なうような異常や悪意あるクライアントの脅威も指摘されている．これは，ビザンチン攻撃と呼ばれ，ビザンチン耐性のある連合学習が必要とされている．

先行研究では，モデル情報保護とビザンチン耐性の両立に着目した研究は少ない．モデル情報保護に関する先行研究では，準同型暗号やマルチパーティ計算，Trusted Execution Environment(TEE) を用いた方式がいくつか提案されている．ビザンチンロバストな連合学習に関する先行研究では，サーバがクライアントモデルを直接観測できる前提で，いくつか方式が提案されている．したがって，モデル情報を保護した状態で，ビザンチンロバストな連合学習を考える必要がある．Zhao ら [1] は，TEE として Intel SGX を活用し，ビザンチン耐性を実現しつつ，クライアントモデルを保護する方式を提案している．Zhao らの方式は，Intel SGX の限られたセキュアなメモリ空間の中で，クライアントモデルの集約とビザンチン攻撃の検出を，効率と性能のバランスを考慮して実装している．

本論文では，モデル情報保護とビザンチン耐性の両立を目指した方式について，基礎検討した結果を報告する．Zhao らの方式と同様に，モデル情報保護に TEE を活用することに加え，準同型暗号の活用も検討した．更に，クライアントモデルの保護に加え，サーバからクライアントへ配布するモデル (グローバルモデル) の保護も考慮した．検討した方式の簡易実装を行い，クライアント数やモデルサイズによる効率や性能について考察した．

本論文の寄与は，ビザンチンロバストな連合学習における学習モデル保護に向けて，基礎検討を踏まえた，TEE や準同型暗号を用いた方式の実現性や課題についての考察にある．

参考文献

[1] Zhao, Lingchen, et al.,“SEAR: Secure and Efficient Aggregation for Byzantine-Robust Federated Learning,” IEEE Transactions on Dependable and Secure Computing (2021)

* 三菱電機株式会社 情報技術総合研究所, 〒 247-8501 神奈川県鎌倉市大船 5-1-1 Mitsubishi Electric Corporation, 5-1-1, Ofuna, Kamakura, Kanagawa, 247-8501, Japan Nakai.Tsunato@dy.MitsubishiElectric.co.jp
† 立命館大学, 〒 525-8577 滋賀県草津市野路東 1-1-1 Ritsumeikan University, 1-1-1, Nojihigashi, Kusatsu, Shiga, 525-8577, Japan fujino@se.ritsumei.ac.jp