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

Intel SGX による安全で高速な DNN 推論の実装方式
Secure and Efficient DNN Inference with Intel SGX

藤原啓成 * 佐藤尚宜 *
Keisei Fujiwara Hisayoshi Sato

キーワード Intel SGX, DNN 推論, TensorFlow, セキュア化

あらまし

産業分野では画像認識 DNN の活用機運が高まっているが，クラウドサーバ上で処理を完結するには機密情報や個人情報などセキュリティの制約があり，機密情報を用いた DNN 利活用の多くはオンプレミス環境に留まっている．一方で，リソース・運用・保守・納期の観点からクラウド環境で行うことも不可欠である. 本研究では，クラウドサーバを利用する DNN 推論を行う際の機密情報の漏洩リスクに対し，Intel SGX により DNN 推論におけるデータ処理部分をセキュア化し，かつ Intel SGX の制約による性能低下を軽減する実装方式の提案および評価を行った。性能評価の結果，提案方式により TensorFlow を用いた DNN 推論のセキュア化を約 2.3 倍の性能オーバヘッドで実現する見通しを得たので報告する.

* 株式会社 日立製作所, 神奈川県横浜市戸塚区吉田町 292 横浜研究所 , Hitachi, Ltd., 292, Yoshida-cho, Totsuka-ku, Yokohama-shi, Kanagawa-ken, 244-0817 Japan