ブロックチェーンを用いた分散機械学習における パラメータ異常検知システムの提案

長友 誠[1]　油田 健太郎[2]　岡崎 直宣[2]　朴 美娘[1]

概要：近年，IoT デバイスやスマートデバイスなどの増加に伴い，生成されるセンサデータなどのデジタルデータが大幅に増加している．深層学習などの機械学習を用いてそれらのデータを学習する際に，1 つのサーバ (クラウド) 上で全てのデータを処理することができないため，サーバの下層に存在するエッジノードが自律的・分散的に学習した後に勾配をサーバに送信することで，クラウド上に統合学習モデルを生成するシステムが考えられる．しかし，勾配から学習データが予測されプライバシーが漏洩する問題や，悪意のあるエッジノードによる異常な勾配の送信などの問題が起こり得る．そこで本論文では，プライバシー漏洩の問題を差分プライバシーで解決し，ブロックチェーン上で敵対的生成ネットワークにより勾配の異常検知を行う分散機械学習システムを提案する．

キーワード：分散機械学習, ブロックチェーン, パラメータ，異常検知，敵対的生成ネットワーク

Proposal of Blockchain System to Detect Anomaly Parameter on Decentralized Machine Learning Model

Makoto Nagatomo[1]　Kentaro Aburada[2]　Naonobu Okazaki[2]　Mirang Park[1]

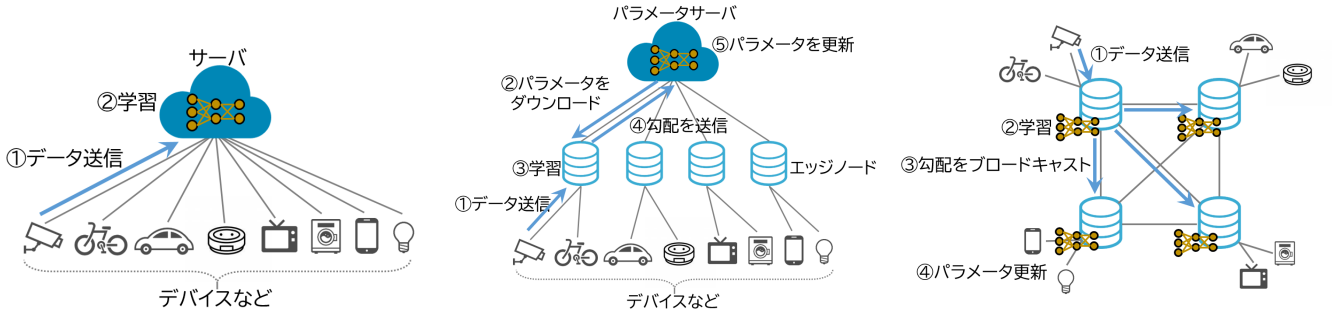
Abstract: Recently, total amount of data generated by IoT devices or smart devices has been increasing. When training the enormous data using machine learning, it is difficult to process it on a cloud. Hence, we can consider the system that edge nodes renew the cloud's parameter of machine learning model each, transmit the local gradient to the cloud, and an integrated model is generated on the cloud. However, this system has two problems of privacy leakage and transmission of the anomaly gradient by malicious edge nodes. Therefore, in this paper, we propose the blockchain system that solves above two problems using differential privacy and anomaly detection by generative adversarial network.

Keywords: decentralized machine learning, blockchain, parameter, anomaly detection, generative adversarial networks

1. はじめに

近年，IoT デバイスやスマートデバイスの増加により，量・種類・変化が大きいビッグデータも増加している．IDC(International Data Corporation Japan) の分析 [1] によると，IoT データと非 IoT データ量が 2025 年までに 163 兆 GB に達すると予測されている．そのようなビッグデータの分析によって予測や知見を得る際に，人によるビッグデータの規則性の把握が困難であるため，機械学習を用いて複雑な規則における予測を行う必要がある．例えば，工場内における設備，センサや気象情報などのデータから機器の故障の原因を予測することが挙げられる [2]．そのような場面において，最近では多層のニューラルネットワークである深層学習が使われており，データの特徴を自動的に抽出することで高い精度で予測が可能である．その際に，一つのサーバ (クラウド) がデータを収集し，学習モデルを生成するシステムを考えることができる (**図 1a**) が，大量

[1] 神奈川工科大学
Kanagawa Institute of Technology
[2] 宮崎大学
University of Miyazaki



(a) 中央集権型の機械学習システム　(b) 中央集権型の分散機械学習システム　(c) 非中央集権型の分散機械学習システム

図 1: 機械学習システムの種類

の学習計算量がサーバに集中する問題や，サーバがハッキングされるとプライバシーの漏洩が起こる問題，送信経路で学習データが改ざんされる問題 (IoT デバイスから送信されるデータなど，暗号化が行われていないデータが存在する) が考えられる．

そこで，分散的に学習モデルの学習を行うシステムが提案されている [3], [4], [5]．本論文では，**図 1b** のような，サーバの下位に存在するエッジノードが分散的に学習を行い，勾配をサーバへ送信することでサーバ内に統合された学習モデルを生成することを分散機械学習と呼ぶことにする．ここで言う勾配とは，学習モデルのパラメータ (深層学習で言う層の結合の重み) の更新方向を示しているベクトルである．分散機械学習の利点は，学習の計算量が分散しサーバへの負担が減少する点である．しかし，この分散機械学習にも問題があり，勾配が盗聴され，第三者によって改ざんされたり，パラメータと勾配から学習データが予測される問題点がある [6], [7]．

プライバシー漏洩の対策として，勾配の統合を暗号化したまま行うことができる，秘密分散法を用いた手法 [8] や，準同型暗号を用いた手法 [9], [10] が存在する．しかし，エッジノードに対する暗号化・復号するための計算量が多くなってしまう問題がある．また，勾配にランダムなノイズを加えることでプライバシーの漏洩を防ぐ，差分プライバシーを用いた学習方法 [11] も提案されている．

しかし，以上のような分散機械学習においては，悪意のあるエッジノードが故意に他のノードと異なる値を送信し，学習モデルが歪められてしまう問題がある．そこで，異常な値を送信したノードを検出する分散機械学習システム [12] が提案されているが，計算量が多い問題がある．

一方で，サーバがパラメータを管理する中央集権的なシステムではなく，**図 1c** のような，エッジノードがパブリックなブロックチェーンネットワーク [13] を構成し分散機械学習を行う手法が提案されている [14]．ここでは，差分プライバシーを用いてプライバシーを保護し，各エッジノードによってブロードキャストされた勾配の平均に類似していない勾配を排除している．しかし，排除アルゴリズムが単純であるため巧妙に仕掛けられた異常な値を排除できない可能性がある．

そこで本論文では，プライベートなブロックチェーンネットワークを構成し，ブロックの追加を行う計算ノードとブロックチェーン管理者のサーバに異常検知モデルを配置して勾配の異常を検知するシステムを提案する．異常検知モデルについては敵対的生成ネットワーク (GAN: Generative Adversarial Network)[17] の一種である AnoGAN[18] と SGAN[19] を用いて勾配の異常を検知する．ブロックチェーン上に異常を明記することで各エッジノードの信頼度を求め，サーバが各ノードを監視する．以降，2 章で関連研究について述べ，3 章でシステムの提案と評価について述べる．最後に 4 章でまとめとする．

2. 関連研究

2.1 分散機械学習

大量の学習データを用いて分散学習を行う際，学習データを分割して学習を行うことができる確率的勾配降下法 (SGD: Stochastic Gradient Descent) が有効である．SGD では，各エッジノード $P_i (i \in \{1, ..., N\})$ が学習データ D_i を学習したとき，t 回の更新が行われたパラメータ $\mathbf{w}_t$ を更新するための勾配を，損失関数 $E_i(D_i, \mathbf{w}_t)$ によって以下のように定め，パラメータサーバへ送信する．

$$gradient_{P_i} = \frac{\partial E_i}{\partial \mathbf{w}_t} \tag{1}$$

パラメータサーバは，各エッジノードの勾配 $\frac{\partial E_i}{\partial \mathrm{w}_t}$ を平均した値を用いて更新する．よって，分散学習におけるパラメータの更新は以下の式のようになる．

$$\mathbf{w}_{t+1} = \mathbf{w}_t - \eta \frac{1}{N} \sum_{i=1}^{N} \frac{\partial E_i}{\partial \mathrm{w}_t} \tag{2}$$

ただし，η は学習の速度を決める係数である．

以上，それぞれのエッジノードが勾配をパラメータサーバへ送信し，それらをサーバ内で統合しているが，サーバが更新を行う際に各ノードの勾配の送信を待つ同期型と各ノードの送信を待たずに更新する非同期型がある [3]．非同期型においてスループット (パラメータ更新の頻度) は高くなるが，最新のパラメータに対してエッジノードから送られた勾配が古い可能性があり，結果的に精度の低下につながる．よって現在の主流は同期型の SGD であり [4], [5]，本論文でも同期型の SGD について考える．一方で，各ノードからサーバへ送信される勾配を盗聴されると学習データが再現できる問題 [6] やパラメータサーバからダウンロードしたパラメータを用いてプライバシーが漏洩する問題 [7] がある．

2.2 プライバシー保護を目的とした分散機械学習

分散機械学習におけるプライバシー保護に関して，暗号化技術を用いた手法が提案されている [8], [9], [10]．文献 [8] では，秘密分散法を用いて送信する更新パラメータを暗号化したまま統合を行うことができる手法を提案している．また，CryptoNets[9] や文献 [10] では，準同型暗号を用いた手法を提案している．しかし，これらの手法は暗号化を行っているため，プライバシー漏洩を防ぐことができるが，各エッジノードが暗号化・復号を行うための計算量が多い問題がある．

そこで，暗号化技術ではなく，学習データにノイズを加える，差分プライバシーを用いた分散機械学習が提案されている [11]．分散機械学習においては，以下の式に示すように，各エッジノード P_i が勾配を計算した後，ガウス分布に従うノイズ $N(0,\sigma^2\mathbf{I})$ を加えることでプライバシー情報の漏洩を防ぐことができる．

$$\mathbf{w}_{t+1} = \mathbf{w}_t - \eta \sum_{i=1}^{N} \left(\frac{\partial E_i}{\partial \mathrm{w}_t} + N(0,\sigma^2\mathbf{I}) \right) \qquad (3)$$

ただし，σ はノイズスケールであり，生成される統合学習モデルの精度とのトレードオフである．

以上より，分散機械学習においてプライバシー漏洩の問題は防ぐことはできるが，1 つの問題点が残っている．それはあるノードが他のノードと送信したデータと異なるデータを送信する，ビザンチン将軍問題である．例えば，あるエッジノードが他のエッジノードの勾配と全く異なる勾配をパラメータサーバへ送信することで，パラメータの更新が正しく行われない問題が生じる．この問題に対して耐性を持つ分散機械学習は研究されている [12] が，計算量が多い問題がある．さらに言えば，中央管理者であるサーバ自体が完全に信用できなく，パラメータを改ざんされる可能性もある．

2.3 ブロックチェーン技術を用いた分散機械学習

2.3.1 ブロックチェーン

ブロックチェーン [13] とは，ブロックチェーンネットワークに参加しているノード全体で合意形成を行うことでデータの保存を行う分散型台帳技術である．保存するデータについては，データを保持するノード全体が同じデータを共有しており，ネットワークに参加しているノードが誰でもデータを見れる，透明性がある．また，追加のデータを保存する際には，データをネットワーク上にブロードキャストし，計算ノードと呼ばれるノードがブロック (ブロードキャストされたデータを集めたもの) を追加するためにある条件を満たす計算を行う．それをチェーンのように前ブロックと関連付けてつなげることによって改ざん困難性を確保している．例えば，ビットコインでは，前ブロックのハッシュ値とランダムな値 (Nonce 値) をブロックに追加し，そのブロックのハッシュ値の先頭 16 桁が 0 になることができればブロックとして認められる．計算ノードはこの条件を満たすような Nonce 値を探すことで報酬が手に入り，同時に改ざんの困難性が確保される．

ブロックチェーンの特徴として，一つのサーバに全てのデータを集約する必要が無く，管理者が必要ない分散型のデータベースである点が挙げられる．これはパブリックブロックチェーンと呼ばれる．しかし，一つの管理者によって管理されるプライベートブロックチェーンや複数の管理者によって管理されるコンソーシアムブロックチェーンも存在する．管理者がいればブロックの追加を迅速に行うことができ，また，ブロックチェーンネットワークに参加しているノードを管理することができる利点があるが，中央集権型のデータベースと同様に，管理者が信用されている必要がある．

2.3.2 LearningChain[14]

中央管理者が存在しない分散機械学習 (図 1c) として，パブリックブロックチェーンを用いた分散機械学習システムである，LearningChain[14] が提案されている．LearningChain では，ブロックチェーンネットワーク上のブロックに，更新されたパラメータが随時記録されていく．各エッジノード $P_i(i \in \{1,...,N\})$ はブロックチェーン上に保存されている最新のパラメータ $\mathbf{w}_t$ を用いて，差分プライバシーを含めた勾配 $\Delta\mathbf{w}_t^i = \frac{\partial E_i}{\partial \mathbf{w}_t} + N(0,\sigma^2\mathbf{I})$ を算出し，ブロックチェーンネットワーク上へブロードキャストする．そして，ブロックの追加を行う計算ノードがそれらの平均を以下の式のように計算する．

$$average = \frac{1}{N}\sum_{i=1}^{N} \Delta\mathbf{w}_t^i \qquad (4)$$

その後に，$average$ とのコサイン類似度が高い勾配を一定個数 (N より小さい個数) 選び，それらの平均を用いてパラメータを更新する．コサイン類似度は以下の式によって

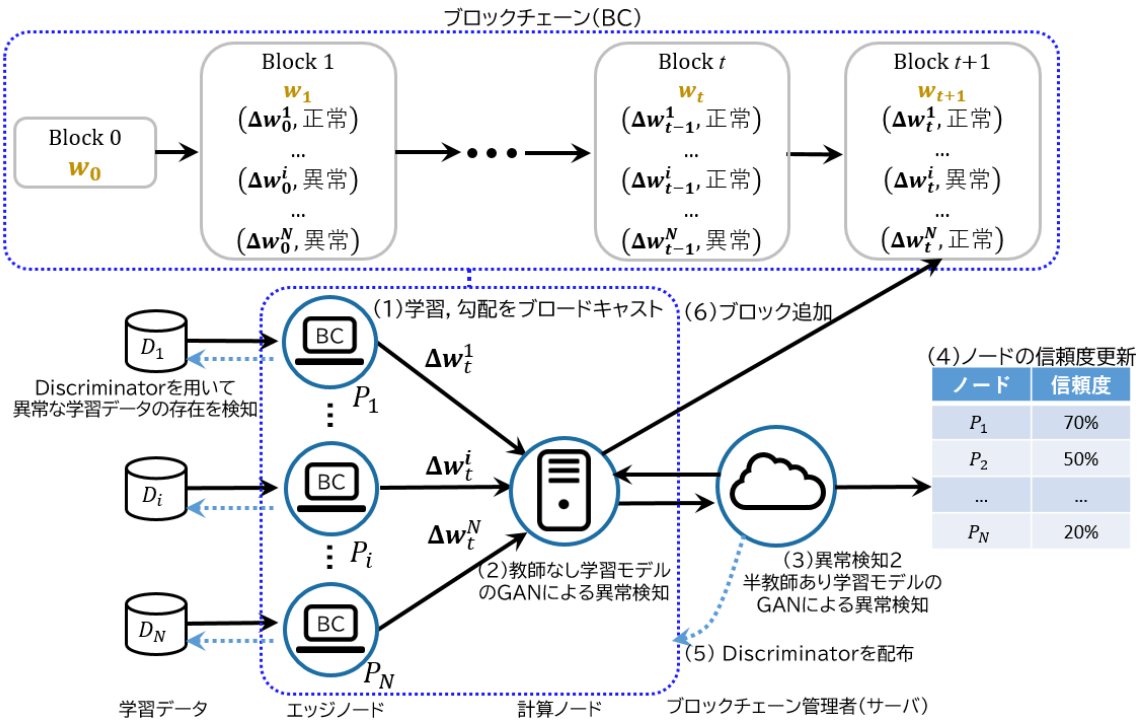


図 2: 提案システムのパラメータ異常検知

計算される．

$$similarity_i = \frac{average \cdot \Delta \mathbf{w}_t^i}{||average|| \cdot ||\Delta \mathbf{w}_t^i||} \qquad (5)$$

最後に，計算ノードは更新されたパラメータと各ノードによってブロードキャストされた勾配をブロックに追加する．

しかし，この手法では異常な勾配排除のアルゴリズムが単純であるため，巧妙に計算された異常な勾配を排除できない可能性がある．例えば adversarial example [15], [16] を本来と異なるラベルとして学習された勾配を排除できない可能性がある．adversarial example とは，元データにある微小なノイズを加えたデータの一種であり，学習モデルが adversarial example を元データの分類と異なると予測してしまう，学習モデルが誤認識を起こすデータである (例えば，元データが画像である場合，ある微小なノイズを加えて異なる予測が出力されても，人間の目には同じ画像に見える)．この adversarial example に対して本来の予測と異なるものであると学習した勾配によって，adversarial exmaple による誤認識が生じやすいパラメータの更新が行われる可能性がある．

3. 提案システム

本論文では，プライベートブロックチェーンを用いた分散機械学習において，計算ノードと管理者であるサーバの 2 カ所で，敵対的生成ネットワーク (GAN: Generative Adversarial Network)[17] を用い，上記の LearningChain における巧妙に計算された異常な勾配を検知することができるシステムを提案する．

GAN は Generator と Discriminator の二つ学習モデルで成り立っており，Generator は，Discriminator に対してあるデータが Generator から生成されたデータか否かを判別できないように学習を行い，反対に Discriminator は判別ができるように学習を行う．本論文では，計算ノードが教師なし学習でブロードキャストされた勾配の異常検知を行う AnoGAN[18]，サーバがブロックチェーンの履歴から半教師あり学習で異常検知を行うことができる SGAN[19] を用いて異常の検知を行う．

また，サーバの SGAN から生成された Discriminator を各エッジノードに配布することにより，勾配をブロードキャストする前に各ノードが異常を検知でき，ブロックチェーンネットワーク上にブロードキャストされる異常な勾配を減らすことができる．

3.1 パラメータ異常検知手順

本システムにおける学習手順は以下の通りである (図 **2**)．

(1) 勾配計算フェーズ：
各エッジノード $P_i (i \in \{1, ..., N\})$ はブロックチェーンに保存されている最新のパラメータ $\mathbf{w}_t$ と学習データ D_i を用いて学習を行い，LearningChian と同様に，差分プライバシーを含めた勾配 $\Delta \mathbf{w}_t^i = \frac{\partial E_i}{\partial \mathbf{w}_t} + N(0, \sigma^2 \mathbf{I})$ を計算し，ブロックチェーンネットワーク上へブロードキャストする．

(2) 異常検知フェーズ 1：
計算ノードは最新のパラメータとブロードキャストされた勾配の組み合わせ $\{(\mathbf{w}_t, \Delta \mathbf{w}_t^i) | i \in \{1, ..., N\}\}$ を

AnoGAN を用いて学習する．その後に AnoGAN の Generator へ $\{(\mathbf{w}_t, \Delta\mathbf{w}_t^i)|i \in \{1, ..., N\}\}$ を入力し，閾値以上の近さを持つものが出力されれば正常，そうでなければ異常とみなし，その結果をブロックチェーンの管理者であるサーバへ送信する．
ここで，異常判定結果 R_t は以下のように表すことができる．

$$R_t = \{((\mathbf{w}_t, \Delta\mathbf{w}_t^i), result)\}|result \in \{normal, anomaly\}\} \tag{6}$$

(3) 異常検知フェーズ 2：
サーバは SGAN の Discriminator を用いて $\{(\mathbf{w}_t, \Delta\mathbf{w}_t^i)|i \in \{1, ..., N\}\}$ の正常・異常を判定する．その結果は以下の式で表される．

$$S_t = \{((\mathbf{w}_t, \Delta\mathbf{w}_t^i), result)\}|result \in \{normal, anomaly\}\} \tag{7}$$

ここで，手順 (2) で送信された判定 R_t と S_t の判定結果が同じであれば正しく判別できたとみなす．正しく判定された結果は T_t は以下のように表すことができる．

$$T_t = R_t \cap S_t \tag{8}$$

その後に T_t を学習データセットとして半教師あり学習である SGAN による学習を行う．

(4) 配布フェーズ：
サーバは T_t を計算ノードに送信し，手順 (3) において更新した SGAN の Discriminator をブロックチェーンネットワーク上へブロードキャストする．

(5) 信頼度更新フェーズ：
サーバは，管理している各ノードの信頼度を，T_t を用いて更新する．例えば，正常な勾配をブロードキャストしたノードは信頼度が向上し，異常な勾配であれば減少する．

(6) ブロック追加フェーズ：
計算ノードは，サーバから T_t を受け取り，以下の式のように T_t 内の勾配の平均を用いてパラメータを更新する．

$$\mathbf{w}_{t+1} = \mathbf{w}_t - \eta \frac{1}{|T_t|} \sum_{((\mathbf{w}_t, \Delta\mathbf{w}_t^k), result) \in T_t} \Delta\mathbf{w}_t^k \tag{9}$$

ただし，η は学習の速度を決める係数である．

以上のように，AnoGAN と SGAN の 2 つを用いることで勾配の異常を検知する．また，各エッジノードは手順 (5) で配布された SGAN の Discriminator を用いることで，勾配を計算した際に学習データに異常があるかを検知できる．

3.2 評価と応用例

本提案システムではプライベートブロックチェーンを用いており，管理者であるサーバが各エッジノードを管理できる利点がある．例えば，各ノードに信頼度が閾値以下となれば管理者がそのノードを除外することができる．また，信頼度でパラメータ更新における勾配へ重みを付けることで正しいパラメータ更新が期待できる．加えて，異常な勾配がブロックチェーンに記録された後に異常が発見された場合，サーバが異常な勾配を学習する前に巻き戻すことが可能であり，学習のやり直しができる．しかし，ネットワークに参加するノードを限定するため，パブリックブロックチェーンを用いた場合に比べて学習データ量が少なくなる可能性や管理者が不正な信頼度の操作を行う問題も考えられる．

本提案システムによって生成された学習モデルの評価に関して，本システムにおいて異常な勾配を検知することで，adversarial example のような，データに微小なノイズが加えられ，データの識別を変更する攻撃に対しても同じ予測を行えるような学習モデルが生成されると期待できる．よって評価項目としては，実世界から取得したテストデータの精度 ($accuracy_{\text{test}}$) と，テストデータにノイズを加え，それを異常なデータとして考えたときの精度 ($accuracy_{\text{noise}}$) の，2 つの項目を算出できる．また，この 2 つの項目はトレードオフであると考えらえるため，以下の式のように上記 2 項目の調和平均によって信頼性 ($reliability$) の評価を行うことができる．

$$reliability = \frac{2accuracy_{\text{test}} \cdot accuracy_{\text{noise}}}{accuraty_{\text{test}} + accuracy_{\text{noise}}} \tag{10}$$

提案システムは，関連システムに比べてこの $reliability$ が向上すると期待できる．

また，提案システムのユースケースとして，機械学習モデルの誤認識を起こすことによるリスクが高いシーンで有効である．例えば自動車の自動運転が挙げられ，攻撃者によって自動車に搭載されたカメラやセンサにノイズが加えられることによる，標識の誤認識や車と人の距離の誤認識を防ぐことができる．その他にも誤診断が人の命にかかわる医療診断の分野において本提案システムを用いることができる．

4. おわりに

本論文では，ブロックチェーン技術を用いた分散機械学習において，エッジノードから送信される巧妙に計算された異常な勾配を検知するシステムの提案を行った．提案システムでは，プライベートブロックチェーンを用いており，計算ノードとブロックチェーンの管理者が異なる種類の GAN を用いて異常な勾配を検知し，統合機械学習モデルの信頼性の向上が期待できる．また，各ノードの信頼度を求めることによって各エッジノードを管理することがで

きる．よって本提案システムは，モデルの誤認識によるリスクが大きい識別・予測をする学習モデルを生成する際に有効である．

今後の課題として，信頼度の算出方法・利用方法の検討と，提案システムの理論的な安全性の評価や提案システムのプロトタイプの実装と評価が挙げられる．

参考文献

[1] IDC,「2018 年 国内 IoT 市場 データエコシステム / Data as a Service に関わるプレイヤー分析」，2018.

[2] SAS,「IoT データへの機械学習の適用」，<https://www.sas.com/ja_jp/insights/articles/big-data/machine-learning-brings-concrete-aspect-to-iot.html>(参照 2019-08-19).

[3] J. Dean, G. S. Corrado, R. Monga, K. Chen, M. Devin, Q. V. Le, M. Z. Mao, M. A. Ranzato, A.Senior, P. Tucher, K. Yang, An. Y. Ng, “Large Scale Distributed Deep Networks,” Proc. of the 25th International Conference on Neural Information Processing Systems (NIPS 2012), vol. 1, pp. 1223-1231, 2012.

[4] T. Akiba, K. Fukuda, S. Suzuki, “ChainerMN: Scalable Distributed Deep Learning Framework,” Proc. of the 31th Internationl conference on Neural Information Processing Systems (NIPS 2017), 2017.

[5] P. Goyal, P. Dollar, R. Girshick, P. Noordhuis, L. Wesolowski, A. Kyrola, A. Tulloch, Y. Jia, K, He, “Accurete, Large Minibatch SGD: Training ImageNet in 1 Hour,” arXiv preprint arXiv:1706.02677, 2018.

[6] M. Fredrikson, S. Jha, T. Ristenpart, “Model Inversion Attacks that Exploit Confidence Information and Basic Countermeasurements,” Proc. of the 22nd ACM SIGSAC Conference on Computer and Communications Security (CCS 2015), pp. 1322-1333, 2015.

[7] B. Hitaj, G. Ateniese, F. Perez-Cruz, “Deep Models Under the GAN Information Leakage from Collaborative Deep Learning,” Proc. of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS 2017), pp. 603-618, 2017.

[8] K. Bonawitz, V. Ivanov, B. Kreuter, A. Marcedone, H. B. McMahan, S. Patel, D. Ramage, A. Segal, K. Seth, “Practical Secure Aggregation for Privacy-Preserving Machine Learning,” Proc. of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS 2017), pp. 1175-1191, 2017.

[9] N. Dowlin, R. Gilad-Bachrach, K. Laine, K. Lauter, M. Naehrig, J. Wernsing, “CryptoNets: Applying Neural Networks to Encrypted Data with High Throughput and Accuracy,” Proc. of the 33rd International Conference on Machine Learning (ICML 2016), vol. 48, pp. 201-210, 2016.

[10] L. T. Phong, Y. Aono, T. Hayashi, L. Wang, S. Moriai, “Privacy-Preserving Deep Learning via Additively Homomorphic Encryption,” IEEE Transaction on Information Forensics and Security, vol. 13, no. 5, pp. 1333-1345, 2018.

[11] M. Abadi, A. Chu, I. J. Goodfellow, H. B. McMahan, I. Mironov, K. Talwar, L. Zhang,“Deep Learning with Differential Privacy,” Proc. of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS 2016), pp. 308-318, 2016.

[12] P. Blanchard, E. M. E. Mhamdi, R. Guerraoui, J. Stainer, “Machine Learning with Adversaries: Byzantine Tolerant Gradient Descent,” Proc. of the 31st International Conference on Neural Information Processing Systems (NIPS 2017), pp. 118-128, 2017.

[13] 岸上純一，藤村滋，渡邊大喜，大橋盛徳，中平篤，「ブロックチェーン技術入門」，森北出版株式会社，2017.

[14] X. Chen, J. Ji, C. Luo, W. Liao, P. Li, “When Machine Learning Meets Blockchain - A Decentralized, Privacy-preserving and Secure Design,” Proc. of 2018 IEEE International Conference on Big Data, pp. 1178-1187, 2018.”

[15] I. J. Goodfellow, J. Shlens, C. Szegedy, “Explaining and Harnessing Adversarial Examples,” Proc. of International Conference on Learning Representations (ICLR 2015), 2015.

[16] N. Papernot, P. McDaniel, I. Goodfellow, S. Jha, Z. B. Celik, A. Swami, “Practical Black-Box Attacks against Machine Learning,” Proc. of the 2017 ACM on Asia Conference on Computer and Communications Security (ASIA CCS 2017), pp. 506-519, 2017.

[17] I. J. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, Y. Bengio, “Generative Adversarial Nets,” Proc. of the 27th International Conference on Neural Information Processing Systems (NIPS 2014), vol. 2, pp. 2672-2680, 2014.

[18] T. Schegl, P. Seebock, S. M. Waldstein, U. Schmidt-Erfurth, G. Langs, “Unsupervised Anomaly Detection with Generative Adversarial Networks to Guide Marker Discovery,” Proc. of the International conference on Infomration Processing in Medical Imaging 2017 (IPMI 2017), 2017.

[19] A. Odena, “Semi-Surpervised Learning with Generative Adversarial Networks,” arXiv preprint arXiv:1606.01583, 2016.