Vol.2015-MPS-102 No.1
2015/3/3

差分プライベート弱学習器の統合

南　賢太郎[†1]　佐藤一誠[†1]
荒井ひろみ[†1]　中川裕志[†1]

データが複数の組織にわたり分散して存在しているとき，それらを互いに共有することで，各組織におけるデータ解析の精度向上が期待できる．しかし，保護すべき個人情報がデータに含まれている場合には，異なる組織間での情報の交換は，プライバシ保護を考慮した上で行われなければならない．本研究では，差分プライバシをみたす弱学習器を互いに交換し，それらを統合する枠組みを提案する．これによって，複数の組織に分散したデータからの学習を，個人情報を保護しつつ効率的に行うことができる．また，特に学習タスクが二値分類である場合について計算機実験を行い，提案手法の性能を評価する．

Aggregating Differentially Private Weak Learners

Kentaro Minami,[†1] Issei Sato,[†1] Hiromi Arai[†1]
and Hiroshi Nakagawa[†1]

When the dataset is distributed over a number of organizations, one can expect the improvement of data analysis by sharing the dataset each other. However, if the dataset consists of personal information, data sharing procedures must be performed under privacy-preserving constraints.

Recently, differentially private algorithms for some statistical learning problems, such as empirical risk minimization, have been considered by several authors. In this work, we introduce a general framework for exponential weighting aggregation (EWA) of differentially private weak learners. This framework allows us to learn effectively from distributed dataset without leakage of personal information. Especially in the case of the binary classification problem, we evaluate the effectiveness of our approach on synthetic and real dataset.

†1 東京大学
The University of Tokyo

1. はじめに

近年，医療データ，移動履歴，購買履歴など，個人情報を含むデータ貯蓄量の増大に伴い，それらの利活用に対する関心が高まっている．例えば，データから得られる要約統計量や，分類や回帰問題など種々の機械学習手法によって得られる知見の利用は重要である．一方，そのような個人情報を含むデータを用いた解析結果を外部に公表する場合には，個人情報漏洩のリスクが発生する．そこで，プライバシを保護しつつデータ解析結果を公開する手法が数多く提案されている．

個人情報を含むデータは複数の組織にわたり分散して存在している場合も多い．その場合，それらを統合してデータ解析を行うことで，ひとつの組織内では得ることの出来なかった知見が得られることが期待される．特に医療データを例にとると，ある特定の症例に関して 1 つの組織 (病院) 内で取得可能なデータ数が少ないという状況が考えられ，精度の良いデータ解析のためには異なる組織のデータを統合して解析することの意義が大きい．しかし，組織間で個人データそのもの，あるいは個人データを元にして得られた解析結果を直接共有することは，個人情報の漏洩につながるため望ましくない．したがって，異なる組織間の情報交換は，何らかのプライバシ保護基準を満たすように加工された形で行われる必要がある．本研究の目的は，そのような情報交換に関するプライバシの制約のもとで，複数の組織に属するデータを効率的に活用して学習を行う手法を考察することである．

考察の対象となるフレームワークは 2 つの要素からなる．ひとつは，組織間での情報交換に際して制約条件として課されるプライバシ保護基準であり，これには Dwork[1)] によって提案された差分プライバシ (differential privacy) を用いる．このプライバシ制約のもとで，各組織は自分のデータを使って学習した学習器を互いに提供しあう．もうひとつの要素は，他組織から提供された多数の学習器を統合してひとつの学習器を作るための方法であり，これには指数型重み付け統合 (exponential weighting aggregation, EWA) と呼ばれる手法群を用いる．

このような統合フレームワークの導入によって期待される学習精度への影響の概念図を**図 1** に示す．もし組織間での情報交換が許されていなければ，ある組織 m_0 で学習された学習器 $\hat{f}^{(0)}$ の性能は，全データ D_n を使って学習された理想的な学習器 $\hat{f}_{D_n}$ の性能に劣る．しかし，差分プライバシ制約を満たした上での学習器交換が許されるならば，それらを統合して作った学習器 $\hat{f}_{\mathrm{agg}}$ の性能はより理想的な学習器の性能に近づけることができると考えられる．一般に，共有できる情報量とプライバシ保護強度との間にはトレードオフの関係が

Vol.2015-MPS-102 No.1
2015/3/3

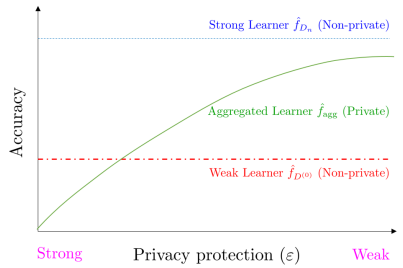

図 1 自組織データのみを使った非プライベート学習器 $\hat{f}^{(0)}$，全データを使った理想的な非プライベート学習器 $\hat{f}_{D_n}$，およびプライベート学習器を統合して作られた学習器 $\hat{f}_{\mathrm{agg}}$ のそれぞれの学習精度と，プライバシ保護強度の関係のイメージ

Fig. 1 An intuitive picture of the relationship between the strength of privacy protection and learning accuracy of estimators. $\hat{f}^{(0)}$ is a non-private local estimator trained over the node m_0's local data set, $\hat{f}_{D_n}$ is a non-private global estimator trained over the whole data set, and $\hat{f}_{\mathrm{agg}}$ is an aggregated estimator made of private weak learners, respectively.

表 1 本研究の位置づけ
Table 1 Our Contribution

		弱学習器のタイプ	
		プライバシ制約なし	プライバシ制約あり
統合手法	ERM	罰則なし (非最適[2])	ロジスティック回帰[3]
		罰則あり: BIC 型[4], LASSO[5], Dantzig selector[6]	
	EWA	Averaging Expert[7], データ分割 + Mixing[8], Mirror Averaging[9]	本研究

あるため，プライバシ保護を強くすると個々の弱学習器の性能は下がる．そのため統合学習器の性能もプライバシ強度の設定に応じて変化するが，もしデータ増加によって見込まれる解析精度の向上が大きければ，比較的プライバシ保護尺度を強めに設定しても，統合学習器は元の学習器より高い精度を達成することが期待できる．

2. 差分プライバシ

2.1 定　　義

本節では差分プライバシの定義といくつかの基本的な性質について説明する．データセット D を入力として，要約統計量や学習器など，何らかのデータに依存する値を出力する状況を考える．差分プライバシとは，1 要素のみで異なるデータセットに対する出力の確率分布があまり変わらないということを定式化したものである．

入力となるデータセットを D で表し，データセットの全体を $\mathcal{D}$ と書く．$\mathcal{D}$ に属するデータセットには対称的な隣接関係 $D \sim D'$ が定義されているとする．例えば $D = (d_1, \ldots, d_n)$ は個人情報を含むデータ d_i $(i = 1, \ldots, n)$ の集まりとし，$\mathcal{D}$ は要素数 n のデータセットの全体とすると，$D \sim D'$ であるとは，1 要素のみで $d_i \neq d'_i$ となり，それ以外の $n-1$ 個の要素では $d_j = d'_j$ $(j \neq i)$ であることと定義する．隣接関係をどのように定義するかは考えている状況によって異なりうる．各 D に対して確率変数 $f_D : \Omega \to \mathcal{X}$ が与えられれているとする．f_D は D から得られる要約統計量，あるいは D から学習された学習器などに対応する．f_D によって値域の空間 $(\mathcal{X}, \mathcal{A})$ に誘導される確率分布を P_D と表す．差分プライバシとは，$D \sim D'$ の場合に分布 P_D 同士の近さを定義したものである．

定義 2.1 (Differential Privacy)．確率変数の集合 $\{f_D : D \in \mathcal{D}\}$ が (ε, δ)-差分プライバシを満たすとは，任意の $D \sim D' \in \mathcal{D}$ と $A \in \mathcal{A}$ に対して

$$P_D(A) \leq e^{\varepsilon} P_{D'}(A) + \delta \tag{1}$$

が成り立つことをいう．ここで，$\varepsilon, \delta \geq 0$ は非負のパラメータである．$\delta = 0$ のときは特に ε-差分プライバシを満たすという．

2.2 差分プライバシを考慮した学習

2.2.1 経験リスク最小化としての二値分類問題

データ (x_i, y_i) $(i = 1, \ldots, n)$ は $\mathcal{X} \times \{-1, 1\}$ 上の未知の確率分布 P からの独立な n 個のサンプルとする．データセット $D = \{(x_1, y_1), \ldots, (x_n, y_n)\}$ が与えられたとき，誤分類リスク $\mathbb{E}_P\left[1_{\{f(x) \neq y\}}\right]$ を最小化するように学習器 (分類器) $f : \mathcal{X} \to \{-1, 1\}$ を構成したい．

分類器の構成は，しばしば次のような凸関数損失に対する経験リスク最小化として定式化される．すなわち，有限次元のパラメータ $\theta \in \mathbb{R}^p$ をもつ学習器 $f_\theta : \mathcal{X} \to \{-1, 1\}$ を，次の経験リスク

$$\mathcal{L}(\theta; D) = \frac{1}{n}\sum_{i=1}^{n} \ell(\theta; d_i) \tag{2}$$

を最小化するような θ を求めることで構成する．ここで，d_i はデータの組 (x_i, y_i) であり，$\ell(\cdot; d)$ は損失関数である．損失関数は θ に関する凸関数とする．

線形分類器 $f_\theta(x) = \mathrm{sgn}(\langle\theta, x\rangle)$ を ϕ-risk $\ell_\phi(\theta; d) = \phi(-y\langle\theta, x\rangle)$ に関して最適化する問題は経験リスク最小化問題である．例えば，ロジスティック回帰は $\ell(\theta; d_i) = \log(1 + \exp(-y\langle\theta, x\rangle))$ の場合に相当する．

2.2.2 差分プライベート経験リスク最小化

前節の経験リスク最小化問題は凸最適化問題である．いま，「差分プライバシを満たすように経験リスク最小化問題の解を公開する」とは，差分プライバシを満たし，かつ目的関数の期待値 $\mathbb{E}[\mathcal{L}(\tilde{\theta}; D_n)]$ をなるべく小さくするような確率変数 $\tilde{\theta}$ をサンプルすることとして定式化できる．この問題を差分プライベート経験リスク最小化ということにする．

差分プライベート経験リスク最小化に対するアプローチのうち代表的なものとして，出力摂動法[1),10)] および目的関数摂動法[10),11)] がある．出力摂動法は経験リスク最小化問題の解にノイズを加える手法，目的関数摂動法は経験リスクそのものに一次関数のノイズを加えてから最適化問題を解く手法である．双方のアルゴリズムの出力 θ_{priv} は実際に (ε, δ)-差分プライバシを満たすことが示されている．[10),11)] また，出力摂動法と比較すると，目的関数摂動法は経験リスクの幾何を反映している分，得られる学習器の精度も良くなるということが知られている．

3. 学習器統合

3.1 指数型重み付けによる統合

本節では指数型重み付け統合 (Exponential Weighted Aggregate, EWA) の原理について説明する．有限個の学習器 $\hat{f}^{(m)}$ $(m = 1, \ldots, M)$ を凸結合して学習器 $\hat{f}$ を作ることを考える．つまり，$\Lambda = \{\lambda \in \mathbb{R}^M_{\geq 0}; \sum_{i=1}^M \lambda_i = 1\}$ を確率単体として，学習器の混合率 $\lambda \in \Lambda$ を適切に選ぶことで，$\hat{f}_\lambda(x) = \mathrm{sgn}\left(\sum_{m=1}^M \lambda_m \hat{f}^{(m)}(x)\right)$ として新たに学習器 $\hat{f} = \hat{f}_\lambda$ を作る．

指数型重み付け統合の基本的なアイデアは，凸結合の重み $\lambda = (\lambda_1, \ldots, \lambda_M)$ を

$$\lambda_m \propto \exp\left(-\frac{1}{\beta}\sum_{i=1}^{n} \ell(\hat{f}^{(m)}(x_i), y_i)\right) \tag{3}$$

に比例するようにとることである．言い換えると，学習器の集合 $\{\hat{f}^{(m)}\}$ を，温度パラメータ $\beta > 0$, エネルギーが経験リスク $n \times \mathcal{L}(\hat{f}^{(m)}; D_n)$ であるような Gibbs 分布で平均化して新たな学習器 $\hat{f}$ を作る．

統合手法の学習理論的な評価指標を与えるために，オラクル不等式の概念について説明しておく．いま，M 個の弱学習器 $\{\hat{f}^{(m)}\}_{m=1}^M$ が与えられたとして，リスク $\mathcal{R}(\hat{f}_{\mathrm{agg}}, f) = \mathbb{E}[\ell(\hat{f}_{\mathrm{agg}}(x), y)]$ によって統合された学習器 $\hat{f}_{\mathrm{agg}}$ の性能を評価する．このとき，$\{\hat{f}^{(m)}\}$ の中で最良のものに対する $\hat{f}_{\mathrm{agg}}$ のリスクを評価する不等式

$$\mathcal{R}(\hat{f}_{\mathrm{agg}}, f) \leq \min_{1\leq m\leq M} \mathcal{R}(\hat{f}^{(m)}, f) + \Delta_{n_0, M} \tag{4}$$

をモデル選択型オラクル不等式という．12) では，回帰問題において達成可能な $\Delta_{n_0,M}$ のオーダーの下界として $\Delta_{n_0,M} = O(\log M/n_0)$ が与えられた．次節で紹介する mirror averaging と呼ばれるアルゴリズムは，この最適な下界を達成することが知られている．

3.2 Mirror averaging による統合

指数型重み付けに区分されるアルゴリズムの具体例として，mirror averaging[9)] によって二値分類の学習器を統合する手法について説明する．まず $t = 1, \ldots, n_0$ について，t 個のデータ $\{d_1, \ldots, d_t\}$ を用いた混合率 $\lambda^{(t)} = (\lambda_1^{(t)}, \ldots, \lambda_M^{(t)})^\top$ を $\lambda_m^{(t)} \propto \exp\left(-\beta^{-1}\sum_{i=1}^t \ell(\hat{f}^{(m)}(x_i), y_i)\right)$ として計算する．ただし $\beta > 0$ は温度パラメータであり，ℓ に応じて十分大きく定める．次に，学習器の混合率 $\lambda = (\lambda_1, \ldots, \lambda_M)^\top$ を $\lambda^{(t)}$ の平均 $\lambda_m = \frac{1}{n_0}\sum_{t=1}^{n_0} \lambda_m^{(t)}$ で求める．したがって，統合された学習器 $\hat{f}_{\mathrm{agg}}$ は次のように表される．

$$\hat{f}_{\mathrm{agg}}(x) = \mathrm{sgn}\left(\sum_{m=1}^{M} \lambda_m \hat{f}^{(m)}(x)\right) = \mathrm{sgn}\left(\sum_{m=1}^{M}\sum_{t=1}^{n_0} \lambda_m^{(t)} \hat{f}^{(m)}(x)\right). \tag{5}$$

Mirror averaging 推定量は，比較的多くのクラスの問題において，前節のオラクル不等式の意味での理論最適性を達成することが示されている．[9)]

4. 差分プライベート学習器の統合

4.1 統合フレームワークの概略

本節では，複数組織に分散したデータからの学習の問題を定式化し，それを扱うための差分プライベート学習器統合の一般的なフレームワークを提案する．全データ $D_n = \{(x_1, y_1), \ldots, (x_n, y_n)\}$ が，実際には $M+1$ の異なる組織に分散しているとする．各組織 m

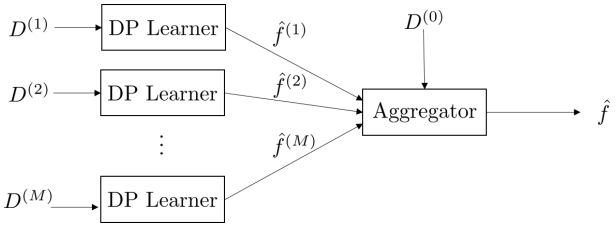

図 2 プライベート学習器統合フレームワーク．各組織 m は学習器 $\hat{f}^{(m)}$ を差分プライバシを満たすように構成し，互いに共有する．組織 m_0 は，他組織 m $(m = 1, \ldots, M)$ から提供された学習器を自組織のデータ $D^{(0)}$ を用いて統合し，学習器 $\hat{f}_{\mathrm{agg}}$ を構成する．

Fig. 2 Framework for aggregation of private weak learners. Each organization m train a differentially private learner $\hat{f}^{(m)}$ on its local data $D^{(m)}$, and disclose them each other. Then an organization m_0 combines the weak learners using its local data $D^{(0)}$ and obtains an aggregated learner $\hat{f}_{\mathrm{agg}}$.

はそれぞれデータセット $D^{(m)}$ $(m = 0, 1, \ldots, m)$ をもち，全データ D_n は $D_n = \coprod_{m=0}^{M} D^{(m)}$ のように $D^{(m)}$ の非交和となっている．ただし，$\coprod$ は非交和をあらわす記号である．

各組織 m は，データセット D_n の情報を用いて学習の問題を解きたい．しかし，他組織のデータ $D^{(l)}$ $(l \neq m)$ を閲覧することはできず，統合されたデータセット D_n の情報を直接利用して学習することはできないものとする．一方，他組織 l $(l \neq m)$ から，$D^{(l)}$ に関して (ε, δ)-差分プライバシを満たすように公開された情報を譲り受けることは許されているとする．以上のような状況で，各組織 m が全データ D_n の情報をなるべく効率的に利用して学習器を作る問題を考える．この問題に対する一般的なアプローチとして，各組織 l から (ε, δ)-差分プライバシを満たすような学習器 $\hat{f}^{(l)}$ を受け取り，それらを弱学習器として統合することが考えられる．

以下では，$m = m_0 = 0$ は自組織を表す添字とし，$D^{(0)}$ はプライバシを考慮せずに使える自組織内のデータとする．**図 2** は差分プライベート弱学習器統合のフレームワークの概念図である．

組織 m_0 は，自分以外の各組織から弱学習器 $\hat{f}^{(m)}$, $(m = 1, \ldots, M)$ を受け取る．このとき，各 $\hat{f}^{(m)}$ はデータセット $D^{(m)}$ に関して (ε, δ)-差分プライバシを満たすように作られる．

次に，組織 m_0 は，自組織で自由に使えるデータ $D^{(0)}$ に基づき，提供された M 個の弱学習器 $\{\hat{f}^{(m)}\}_{m=1}^{M}$ を指数型重み付けによって統合する．これによって，組織 m_0 は統合された学習器 $\hat{f}_{\mathrm{agg}}$ を得る．

上記のフレームワークの効果の直感的な説明は次のとおりである．組織 m_0 が受け取る弱学習器の集合 $\hat{f}^{(m)}$ は，理想的には他組織のデータセット $\{D^{(m)}\}$ がもつ情報のうち，個人情報に起因する成分を取り除いて学習器の汎化能力に影響する部分だけを抽出したものと考えられる．したがって，差分プライバシのノイズによる性能の劣化よりもデータ数増加による学習器の性能の向上が大きく見込めるならば，統合した学習器 $\hat{f}_{\mathrm{agg}}$ は組織 m_0 で独自に学習した学習器よりも良くなることが期待できる．

なお，学習タスクが二値分類問題である場合には，枠組みとして同等のものが 3) によって提案されている．3) では，統合フェーズにおける差分プライベート線形分類器の混合率を，L_2-正則化ロジスティック回帰で決定する方法がとられており，経験リスク最小化による混合の一種であるとみなせる．

4.2 ロジスティック回帰の例

4.1 節で導入したフレームワークに従い，目的関数摂動法 (アルゴリズム**??**) によって学習された ε-差分プライベートなロジスティック回帰推定量を mirror averaging によって統合し，新たな線形分類器 $\hat{\theta}_{\mathrm{agg}}$ を作ることを考える．統合学習器の性能について，次の評価が得られる．

定理 4.1. 上記のように構成した $\hat{\theta}_{\mathrm{agg}}$ について，確率 $1 - \alpha$ $(0 < \alpha < 1)$ で，次の不等式が成り立つ．

$$\begin{aligned}
&\mathbb{E}_{(X,Y)}^{n_0} \mathbb{E}_{\theta}^{M} [\mathcal{R}(\hat{\theta}_{\mathrm{agg}})] - \inf_{\theta \in \Theta} \mathcal{R}(\theta) \\
&\leq A_2(\lambda_{\mathrm{reg}}) + \frac{1}{\lambda_{\mathrm{reg}}} \left(\sqrt{\frac{M \log(2M/\alpha)}{n - n_0}} + \sqrt{\frac{4M}{n - n_0}} + \frac{C_1 M \log(2M/\alpha)}{n - n_0} \right) \\
&\quad + \frac{C_2 M}{\varepsilon(n - n_0)} + \frac{\beta \log M}{n_0} \qquad (6)
\end{aligned}$$

λ_{reg} は L_2-正則化のパラメータである．$A_2(\lambda_{\mathrm{reg}}), C_1, C_2$ はいずれも，データ数 n_0, n，組織数 M，プライバシパラメータ ε には依らない値である．

5. 計算機実験

提案手法の性能を評価するため，人工データおよび実データに対して計算機実験を行った．

各実験に共通する設定を以下で説明する．まず，各組織に対応する $M + 1$ 個のノードに対して $n/(M + 1)$ 個ずつのデータが均等に配置されるようにする．各ノードは自分のデータを用いて，ε-差分プライベートなロジスティック回帰分類器を学習する．差分プライベー

トロジスティック回帰の学習アルゴリズムとしては 10) の目的関数摂動法を採用した．

次に，各ノードは自分以外の M ノードから受け取った弱学習器を mirror averaging (5) によって統合する．統合時の損失関数としてはロジスティック回帰の損失関数を用いる．

5.1 人工データ

10 次元の単位球面上の一様分布をもとに線形分離可能なデータを 6,000 点生成した．そのうち $n = 5,000$ 点を訓練データ，残りの 1,000 点をテストデータとして用いた．なお，テストデータには二値のラベルが均等に 500 点ずつ含まれるようにした．全 5,000 データを利用してロジスティック回帰を行った場合の正答率を計算すると 0.999 であり，これは最も理想的な場合の学習器の性能に相当する．

統合学習器の性能に対するプライバシ保護の尺度 ε の寄与について考察する．ノードの数は 100 とし，各ノードに 5,000 個の訓練データを 50 個ずつランダムに割り当てた．各ノードは公開用の ε-差分プライベートなロジスティック回帰分類器と，比較用の通常のロジスティック回帰分類器をそれぞれ学習した．差分プライベートな学習器を互いに交換したのち，mirror averaging によってそれらを統合した．

図 3 は横軸に ε, 縦軸に正答率をプロットしたものである．ただし，正答率は 100 個のノード間で平均をとり，差分プライバシを考慮した手法の場合はさらに標準偏差をプロットしている．まず，自分のデータのみで通常のロジスティック回帰を学習した場合の平均正答率 (一点鎖線) は 0.559 であった．これは，情報を一切共有することができず，各ノードが孤立している場合に達成可能な精度に相当する．次に，本稿の枠組みにしたがい，ε-差分プライバシをみたす学習器を統合したものの平均正答率が丸いマーカで示したプロットである．平均正答率は，ε が大きくなり，差分プライバシの保護強度が弱まるにつれて増加することが見てとれる．

5.2 医療関連データ

次に，より実用的な例において提案手法の性能を評価するため，実データに対する実験を行った．実験には UCI Machine Learning Repository[13] で公開されている Pima Indians Diabetes および Breast Cancer Wisconsin (Diagnostic) データセットを用いた．Breast Cancer のタスクは，細胞核の画像特徴量から，がん細胞の良性 (B) あるいは悪性 (M) の二値ラベルを判定するものである．Diabetes のタスクは，患者の年齢，血糖値，血圧，妊娠回数などのデータから糖尿病の診断結果を推定するものである．

図 4，**図 5** はそれぞれ Breast Cancer および Diabetes データセットに対する実験結果である．Breast Cancer のデータセットでは個々のノードにおける平均正答率が，理想的に全

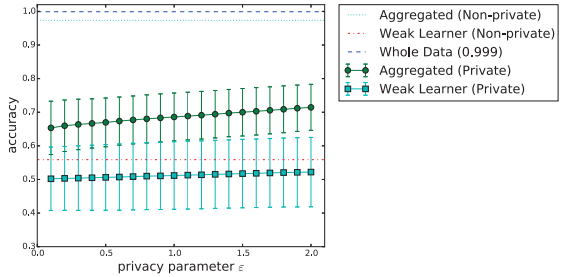

図 3 プライバシパラメータを変化させた場合の正答率．データ数 $n = 5,000$, ノード数 $M + 1 = 100$
Fig. 3 Average accuracies on synthetic data with $n = 5,000$ and $M + 1 = 100$.

データを使った場合の正答率 (0.9231) に近い．そのため，統合学習器を用いたことによる改善はほぼ見られないが，個々の学習器に対して大幅に悪化することもないことがわかる．Diabetes データセットでは，全 600 データを使った場合の正答率が 0.6488 であり，個々のノードが自分で所持しているデータのみを使った場合の平均正答率に対して 20%程度の開きが存在する．そのため潜在的にはデータ増加による精度改善の余地が存在するが，統合学習器の平均正答率はそれらの中間付近に位置しており，情報共有の効果が現れていると考えられる．

6. まとめと考察

本稿では，差分プライベート学習の手法と弱学習器統合の手法を組み合わせることにより，差分プライバシ制約のもとで複数組織に分散したデータを効率的に利用して学習を行うフレームワークを提案した．また，二値分類問題における具体的なアルゴリズムとして，差分プライベート経験リスク最小化によって得られた弱学習器を mirror averaging によって統合する手法を提案した．さらに具体的な場合として，弱学習器がロジスティック回帰である場合の理論的な性能について議論し，計算機実験によって提案手法の有用性を確認した．

本稿の枠組みそのものは，二値分類以外にもより広いクラスの統計的学習の問題に適用可能である．例えば，線形回帰の問題に対しては，本稿と同様にして差分プライベート経験リスク最小化および mirror averaging が適用できると考えられ，その性能の検証は本研究の今後の課題である．5 章の計算機実験の結果は，比較的厳しいプライバシ制約のもとでも統合によって学習器の精度向上が見込めることを示した．このことは，14) で指摘されている

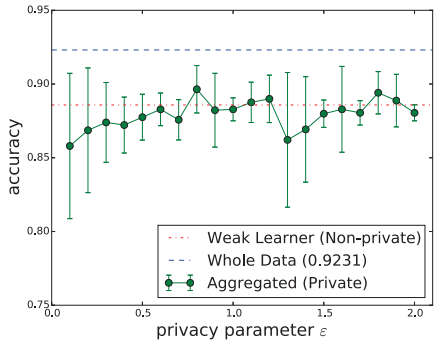

図 4 Breast Cancer における平均正答率
Fig. 4 Average accuracy on Breast Cancer data set.

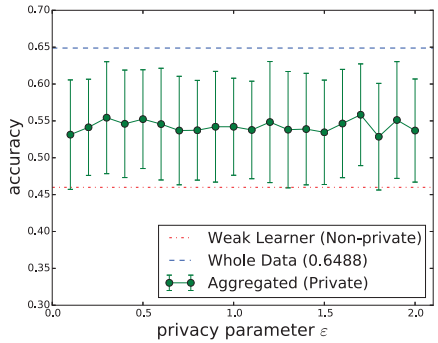

図 5 Diabetes における平均正答率
Fig. 5 Average accuracy on Diabetes data set.

ような，差分プライバシを保証すると医療データ解析で要請される精度が得られないというジレンマ的問題が部分的に解決できる可能性を示唆している．

参 考 文 献

1) Dwork, C.: Differential privacy, *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming (ICALP)*, pp.1–12 (2006).
2) Lecué, G. and Mendelson, S.: Aggregation via empirical risk minimization, *Probability Theory and Related Field*, Vol.145, No.3-4, pp.591–613 (2009).
3) Sarwate, A.D., Plis, S.M., Turner, J.A., Arbabshirani, M.R. and Calhoun, V.D.: Sharing privacy-sensitive access to neuroimaging and genetics data: a review and preliminary validation, *Frontiers in Neuroinformatics*, Vol.8 (2014).
4) Bunea, F., Tsybakov, A.B. and Wegkamp, M.H.: Aggregation for Gaussian regression, *The Annals of Statistics*, Vol.35, No.4, pp.1674–1697 (2007).
5) Tibshirani, R.: Regression shrinkage and selection via the Lasso, *Journal of the Royal Statistical Society: Series B*, Vol.58, No.1, pp.267–288 (1996).
6) Candes, E. and Tao, T.: The Dantzig selector: Statistical estimation when p is much larger than n, *The Annals of Statistics*, Vol.35, No.6, p.23132351 (2007).
7) Vovk, V.: Aggregating strategies, *Proceedings of the 3rd Annual Conference on Learning Theory (COLT)*, pp.371–386 (1990).
8) Yang, Y.: Adaptive regression by mixing, *Journal of the American Statistical Association*, Vol.96, pp.574–588 (2001).
9) Juditsky, A., Rigollet, P. and Tsybakov, A.B.: Learning by mirror averaging, *The Annals of Statistics*, Vol.36, No.5, pp.2183–2206 (2008).
10) Chaudhuri, K., Monteleoni, C. and Sarwate, A.: Differentially private empirical risk minimization, *Journal of Machine Learning Research*, Vol. 12, pp. 1069–1109 (2011).
11) Kifer, D., Smith, A. and Thakurta, A.: Private convex empirical risk minimization and high-dimensional regression, *Proceedings of the 25th Annual Conference on Learning Theory (COLT)*, pp.25.1–25.40 (2012).
12) Tsybakov, A.B.: *Optimal rates of aggregation*, pp.303–313 (2003).
13) Asuncion, A. and Newman, D. J.: UCI Machine Learning Repository. `http://www.ics.uci.edu/~mlearn/MLRepository.html`.
14) Fredrikson, M., Lantz, E., Jha, S., Lin, S., Page, D. and Rintenpart, T.: Privacy in Pharmocogenetics: An End-to-End Case Study of Personalized Warfalin Dosing, *23rd USENIX Security Symposium* (2014).