プライバシを考慮した異業種間データ共同分析手法の検討 ～共通データ構造とガベージクラスを用いた２者間の分析～

染田 拓 [1,*]　長田 繁幸 [2,†]

概要：社会・経済活動のデジタル化が進むにつれて，保有するデータの構造が異なる異業種間のデータを共有し分析することによる新たな価値の創造が期待されている．一方で，データ活用の深化に伴うプライバシ侵害の不安も増加している．プライバシの保護とデータ利活用を両立するために，様々なプライバシ強化技術が提唱されている．本稿では，プライバシ強化技術のうち，複数の組織間でデータを共有することなく共同で深層学習を行う手法である連合学習を対象に，異なるデータ構造を共通のデータ構造に変換した上で学習を行う垂直連合学習を提案する．また，精度向上のためのガベージクラスの導入や，特定の活性化関数を用いた場合に現れる未学習のデータが特定のクラスに偏って予測される性質の考慮を加えることで，高い識別性能を持つ識別器を生成する手法を示す．さらに，提案法の有効性評価にあたって，保有するデータ構造が異なる 2 つの業種の組織が参加するデータ共同分析環境を対象に，2 者を横断する識別器を作成し，その精度と感度から有効性を確認する．

キーワード：プライバシ，垂直連合学習，PSI，ガベージクラス

A Collaborative Data Analysis Method Considering Privacy in Different Industrial Fields

-- A Bilateral Analysis using Common Data Structure and Garbage Class --

Hiroshi Someda[1,*]　Shigeyuki Osada[2,†]

Abstract: Digitalization in social and economic activities brings expectations to create new values by sharing and analyzing data between different industries that have different data structures. On the other hand, there are increasing concerns about privacy violations that accompany the deepening of data utilization. To achieve both privacy protection and data utilization, various privacy enhancing technologies have been proposed. In this paper, we propose a federated transfer learning by transforming different data structures into a common data structure. This paper also shows a method for generating classifications by setting garbage classes and unseen classes to improve their precision and recall. In addition, the paper illustrates several examples to evaluate the effectiveness of the proposed method by creating classifications that cross two organizations in different industries with different data structures and confirm the effectiveness of the method from its precision and recall.

Keywords: Privacy, Vertical federated learning, PSI, Garbage class

1. はじめに

デジタル化によって価値創造をしていくためには，異なる業種の組織間でデータを共有することで新たな知見を得てサービス提供に活かすことが重要である．しかし，プライバシ規制があることから，顧客の同意を得ることなく個人の特定につながる情報を企業間で共有することはできない．そこで，プライバシを保護した状態のまま，データ分析する手法が求められている．

プライバシ強化技術（Privacy Enhancing Technologies: PETs）[1]と呼ばれる技術がある．このなかで，データを共有することなく，深層学習する手法として連合学習[2][3][4]が提案されている．これらは，共同分析する者同士でデータを共有する必要はないが，分析に用いるデータ構造が類似性をもつ必要がある．一般に，異業種間で共同分析することを考えると，各々が持つデータ構造は互いに異なることが想定されるため，この手法を使うためには事前準備にコストがかかる．

また，暗号化された状態のまま集合演算を行う Private Set Intersection（PSI）[5]が提案されている．しかし，個人情報保護法及びそのガイドラインによると，個人を特定しうる情報を暗号化したものについても，個人情報として保護を行うように定めているため，この手法を用いるときには個人の同意を取得しなければならない[6].

本研究では，共同分析したい異業種 2 者が存在する場合を想定して，各々が持つデータ構造のうち，1 つ以上共通する意味を持つものがあれば，それらを連合学習に用いる

1 東京工業大学 環境社会理工学院 イノベーション科学科
School of Environment and Society, Technology and Innovation Management / Department of Innovation Science, Tokyo Institute of Technology.
2 株式会社日本総合研究所 セキュリティ統括部
Security Control Department, The Japan Research Institute, Limited.

* someda.h.aa@m.titech.ac.jp
† osada.shigeyuki@jri.co.jp

ことで確率的な集合演算を行う手法を提案する．

以降，本稿は次のように構成する．2 章では，解決する問題と連合学習について説明する．3 章では、連合学習を応用して，共通するデータ構造が存在する 2 つの組織間で，データを共有することなく、共通顧客が存在することを確認する方法を提案する．4 章では、提案法を実装により評価する．5 章でまとめと今後の課題を述べる．

2. 背景

2.1 異業種間の連携とプライバシの課題

異業種の組織間でデータを共有し分析する場合は，図 1 に示すように共有する組織に対してデータを送信する必要がある．

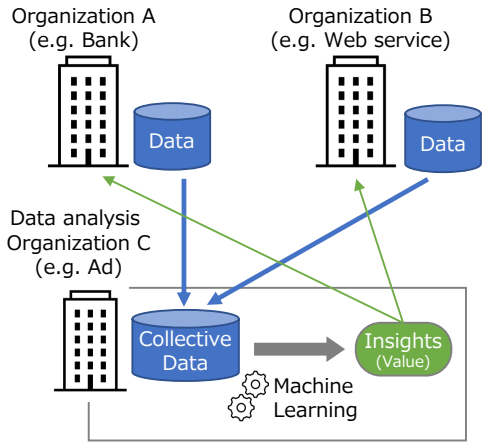


図 1　異業種を横断するデータ分析基盤

Figure 1　A data analysis platform for different industrial fields.

データを提供する組織は，そのデータに個人を特定できる情報が含まれる場合には，個人情報保護法に基づいて，情報の種類や具体的な利用目的を該当する個人に示し，事前に同意を得なければならない．これは，プライバシ強化を確かなものにする観点においては必要な要件である一方で，データを活用するという観点においては手続きの負担が大きく進まないという課題がある．

このような課題を解決する手法として，プライバシ強化技術が提案されている．暗号化した状態のままデータ分析を可能にする準同型暗号やマルチパーティ計算は，個人情報を暗号化した状態を保ったまま異なる組織間でデータ分析を行うことができる．

一方で，個人情報保護法のガイドラインによると，暗号化した状態の個人情報を第三者に提供することについても，平文のときと同様に個人情報保護の対象と位置づけており，個人情報に相当するデータを共有する前には，その個人に同意を取らなければならないとされている．また，個人情報保護法ガイドライン（通則編）によると，匿名化を施した匿名加工情報を暗号化したものであったとしても，匿名化されたデータの作成者において他の情報と容易に照合できる（容易照合性と呼ぶ）状況が作出される可能性がある場合は，引き続き個人情報の保護対象として取り扱わなければならないとされる[6].

したがって，複数の組織間が持つデータを連携して新しい価値を生み出すためには，容易照合性が失われていることを確保する必要性がある．日常的にデータにアクセスし分析するケースにおいては容易照合性がないとされており，データ活用を頻繁に行う場面では適用しにくい．

別のプライバシ強化技術の 1 つに，深層学習のためのプライバシ強化を目的とした連合学習がある．深層学習はデータ分析手法では様々な発展的手法が研究されており，実務化もされているものであることから，利活用の場を広げるためにも，プライバシ強化機能が必要である．連合学習は，図 2 に示すように，連携しようとする組織にデータを送信するのではなく，個人を特定できないように加工されたモデルのパラメータ情報を送信する．モデルのパラメータ情報を統計情報の一種として見なすならば，特定の個人との対応関係が排斥されている限りにおいては，これは個人情報に該当しないと考えられる．

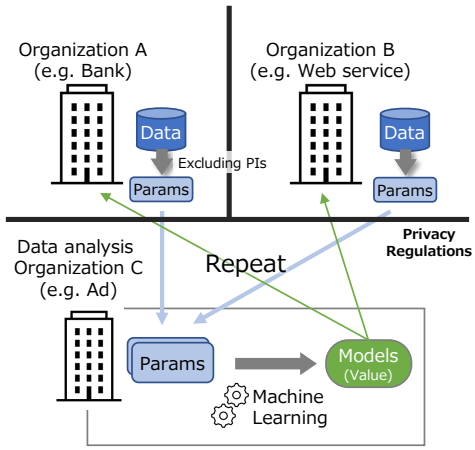


図 2　連合学習を用いたデータ分析基盤

Figure 2　A data analysis platform using federated learning.

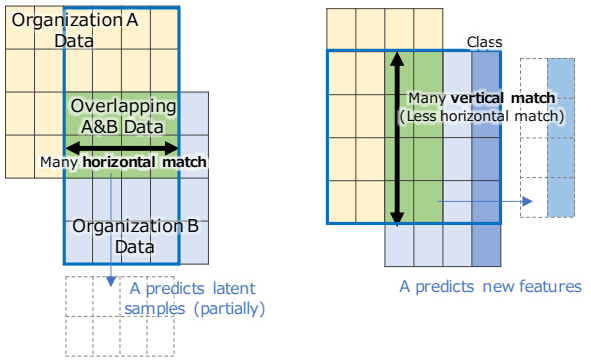
2.2 連合学習

連合学習は，クライアント・サーバ形式の，データ分散状態を維持したまま機械学習を行う方法である．連合学習に参加するクライアント（図 2 の A と B）は，サーバ（図 2 の C）から送信されるモデルと自身の持つデータだけを用いてモデルのパラメータ情報を計算する．計算を終えると，各クライアントはサーバとは異なる第三者（以降，アグリゲータと呼ぶ．ただし，簡略化のために，図 2 の C はサーバとアグリゲータを兼ねて表現している）にモデルのパラメータ情報を送信する．アグリゲータは，各クライアントから受信したパラメータ情報に加えて，各クライアントから送られるデータ量を考慮して，モデルを更新する．

アグリゲータは更新したモデルをすべてのクライアントに再配布し，各クライアントはパラメータを再計算する．アグリゲータは，これらの手順を繰り返すことで生成されたモデルをサーバに送信する．このようにして，連合学習に参加するノードは，個人情報を共有することなく，精度または感度の高いモデルを構築する．

連合学習の実行方法は，連携する組織が持つデータ構造の類似度合いによって異なる．例えば，同種の医療を提供する異なる医療機関同士でデータ共有する場合や，業界規制等により予め定められたデータ構造がある金融や建設などのそれぞれの業種内でデータを共有する場合は，図 3 (a) に示すように同じ意味を持つデータ列が重複する部分が多いことが想定できる．重複部分が水平方向に広がることを前提に分析することを水平連合学習と呼ぶ．

他方，連携する組織が異業種の関係（図 2 の銀行と Web サービスのような関係）にある場合は，データ構造が異なることから，重複部分が水平方向に広がらない．このような性質が予めわかっている場合は，重複部分が垂直方向に重なることを想定して，自組織が保有するデータの各サンプルの未知の属性やクラスなどを予測する．この方式のことを垂直連合学習（図 3 の(b)）と呼ぶ．



(a) Horizontal federated learning　(b) Vertical federated learning

図 3　水平連合学習と垂直連合学習

Figure 3　Horizontal and vertical federated learning.

垂直連合学習を行うためには，連携する組織が持つデータの中から，共起するサンプルを特定する必要がある．これを実現するために，組織間で Private Set Intersection (PSI) というプライバシを保護しながら共通集合や特定条件を満たす部分集合などの集合演算を行う通信プロトコルを用いる方法が提案されている[5]．しかし，この手法は，暗号化をプライバシ保護の手段の一つに用いてるため，個人情報保護法のガイドラインに照らし合わせると，個人情報の第三者提供に該当する可能性がある．

また，水平連合学習と垂直連合学習のどちらの方式においても，データの構造，収集方法，保存形式などのデータ概要情報を予め確認する必要がある．データ概要情報を共有するための記述方法として，データジャケットが提案されている[7]．しかし，異業種間において目的に合わせたデータジャケットを構築するためには，データ構造だけでなく，意味や前提を相互の業界の用語を用いながら何度も対話を通じて理解していく必要がある．それゆえに，データジャケットの草案の作成やデータ収集を何度も繰り返すためのコストが必要になるだけでなく，ビジネスの変化に伴うデータ変更に対するコストが大きいことが考えられる．

また，データを直接共有することなく，あるデータが集合の要素であるかどうかを判定する方法に，確率的データ構造であるブルームフィルタ[8]を応用する方法が提案されている[9]．しかし，データジャケットの課題と同様に，異業種組織間でデータを共有し分析するためには，ブルームフィルタで用いるハッシュ関数や分析対象とする列の意味を理解した状態を作り続けることにコストを要する．

本稿では，2 つの異業種組織からなる連合学習を前提に，データジャケットの構築を簡略化し，同時に，容易照合性がない状態を維持しながら垂直連合学習を行う手法を提案する．

3.　提案法

異業種の組織が持つデータを組み合わせて新たな知見を得るためには，互いの組織で共通となる顧客を特定することが重要である．例えば，銀行と Web サービスに共通の顧客が存在することがわかれば，銀行は Web サービスの利用状況に基づいてライフステージに合った金融商品を推薦したり，逆に Web サービスは銀行の金融資産情報に基づいて広告を最適化したりできる．

本稿で提案する手法は，互いのデータを共有することなく，相手方のデータに自身の顧客が存在するか否かを確率的に判定する．

3.1　基本的な原理

2 つのデータ集合 P と Q を考える．図 4 に示すように，P の所有者は Q を得ることなく共通集合 P∩Q を得たいとする．

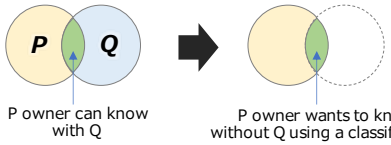


図 4　データ共有制約化における共通集合の導出

Figure 4　Derivation of the intersection without another set.

(1)　データジャケット構築

データジャケットの構築を簡易に行うために，データ概要情報を全て理解するのではなく，互いに個人を特定する

1 つ以上のデータ概要情報を特定する. P と Q の所有者は，それらに共通して現れるデータ概要情報のデータに対して，文字列の出現頻度を N-gram を用いて計算する．出現頻度は，図 5 に示すように，文字種数の N 乗個の列を持つマトリクスを準備して，文字列出現の有無を，ブルームフィルタと同様にビットのオンとオフで表現する．例えば，電話番号やクレジットカード番号のように 0 から 9 までの数字で構成されるデータを考えた場合，N-gram の計算結果は，図 6 に示すようになる．

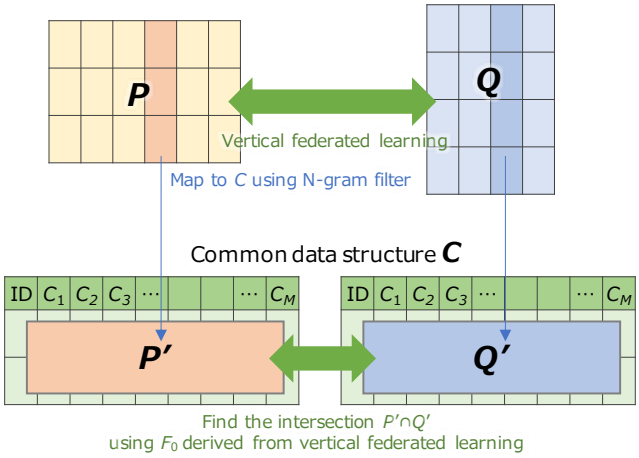
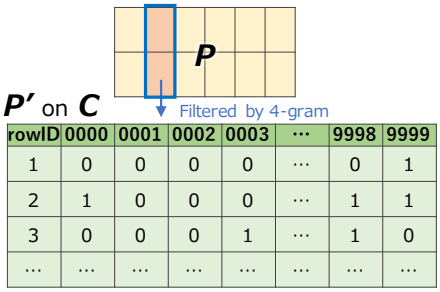


図 5　共通データ構造 C を用いた垂直連合学習

Figure 5　Vertical federated learning using common data structure C.



rowID	0000	0001	0002	0003	···	9998	9999
1	0	0	0	0	···	0	1
2	1	0	0	0	···	1	1
3	0	0	0	1	···	1	0
···	···	···	···	···	···	···	···

図 6　P から P’を生成する例

Figure 6　An example of mapping P’ from P.

共通データ構造 C に変換した P と Q の集合のことを，それぞれ P’と Q’ と呼ぶ．P’と Q’は比較可能な状態になることから，C 上で垂直連合学習を行うことにより共通集合を特定する．

(2) 偽陽性の低減

文字列出現頻度を元にデータ連結を行う提案法は，確率的データ構造であるブルームフィルタと同様に偽陽性の可能性が増加する. そこで, P∩Q の識別精度を高めるために，Q には存在しないランダムな値を持つガベージクラスに属するデータ G を Q に混在することで，P∩$\overline{Q}$についての識別精度を高める．

また，活性化関数に SoftMax を指定したニューラルネットワークで識別器を作る場合，学習データに一様に分布したクラスに属するデータを用いると，その識別器は未学習のクラスに属するデータのクラスを，少数の特定のクラスにバイアスされて予測することが Matan らによって示唆されている[10][11]．この性質を応用して，垂直連合学習によって過学習した識別器を用いてデータの所属クラスを予測したときに，複数のサンプルが，あるクラスに共通して予測されたものについては，識別器の学習データである Q には存在しないデータであると見なすことで，P∩$\overline{Q}$の検出精度を高める．

3.2　手順

P と Q のそれぞれの保有者は，互いのデータ集合を参照できない前提の元で，重なる部分 P∩Q を特定する手順を示す．この手順では，データ集合 P の所有者視点で手順を説明している．すなわち，データ集合 Q のデータを参照することはできない．

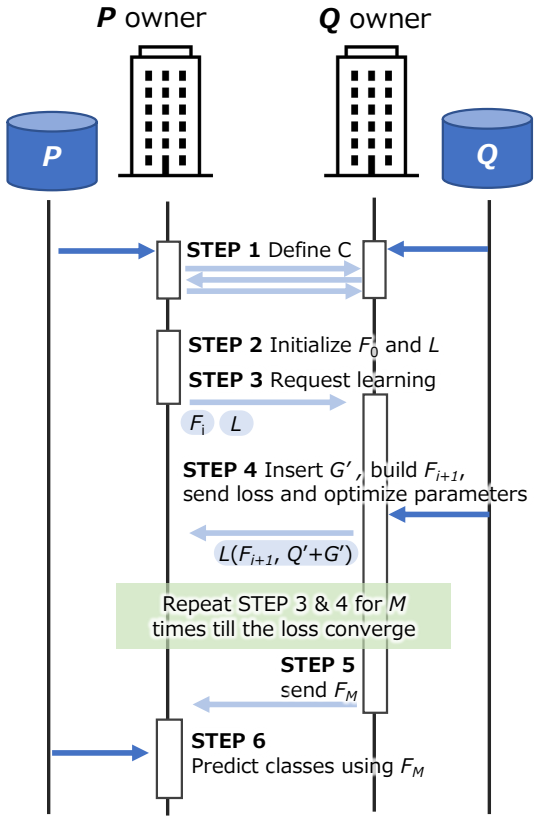


図 7　STEP 1 から 6 までの手順

Figure 7　Procedure of STEP 1 to 6.

STEP 1 共通データ構造の定義

P と Q の所有者は，それぞれ P と Q のデータ構造とサンプル数，列数，各列の名称，意味，入力規則などのデー

タ概要情報を可能な範囲で公開する．P と Q の各所有者は，互いのデータ概要情報を確認して，重複する可能性が高いと合意した列を P と Q のそれぞれから 1 つまたは複数指定し，共通データ構造 C とそれに変換する方法を定義する．

STEP 2 初期化

P の所有者は，Q の所有者に識別器の学習を要求するときに送信する識別器の原型 F_0 と Q の所有者が行う識別器のパラメータ最適化を評価するための損失関数 L を作成する．F_0 は，C の列数のノードを入力層，P のサンプル数に offset を加えた数のノードを出力層とし，隠れ層と活性化関数を持つ未学習状態のニューラルネットワークである．

STEP 3 識別器の作成要求

P の所有者は, Q の所有者に対して STEP 2 で作成した F_0 と L を送信し, Q'を用いて深層学習するように要求する．

STEP 4 識別器の最適化

Q の所有者は，Q に存在しないランダムな値を持つガベージクラスに属するデータ集合 G を生成する．Q の所有者は，G を C 上に変換した G'と Q'，及び F_i を用いて深層学習を行い，識別器 F_{i+1} を得る．また，L を用いて F_{i+1} の評価値を算出し，その評価値のみを P の所有者に送信する．P の所有者は，Q の所有者から受け取る評価値が収束するまでの間，Q の所有者に深層学習と評価値算出の要求を M 回繰り返す．

STEP 5 識別器の完成

P の所有者は，評価値が収束したと判断すると，Q の所有者に対して識別器 F_M を送信するように要求する. Q の所有者は要求に従い，F_M を P の所有者に送信する．

STEP 6 データ連結

P の所有者は，F_M を用いて P の全てのサンプルのクラスを予測する．このときに，1 つのクラスに 1 つのサンプルのみが対応する関係が現れたら，そのサンプルは P と Q の両方に存在しているとみなす．他方，1 つのクラスに複数のサンプルが対応する関係が現れたら，そのクラスはガベージクラスか，あるいは未学習のクラスに属するサンプルが集中して予測される特定クラスと考える．したがって，このクラスに対応したサンプルは，P には存在するが Q には存在しないサンプルであると見なす．

このようにして， P の所有者は，Q の所有者から直接データを提供されることなく，共通集合 P∩Q を得ることができる．

4. 評価

4.1 評価環境

提案法の評価にあたって，無償利用が可能で安定性のあるバージョンを提供している OpenMined の PySyft [12] を用いた評価環境を構築する．評価環境で用いる F_0 は，図 8 に示すように，層数が 4，入力層のノードが 10^4 個，隠れ層が 2 層，各隠れ層のノードが 1,000 個，各隠れ層の活性化関数は ReLU，また，出力層の活性化関数は Log SoftMax を指定する．損失関数は負の対数尤度を指定する．最適化は Adam を用いて学習率 0.01 とし，エポック数を 30 とする．なお，評価環境で用いるその他の諸元を表 1 に示す.

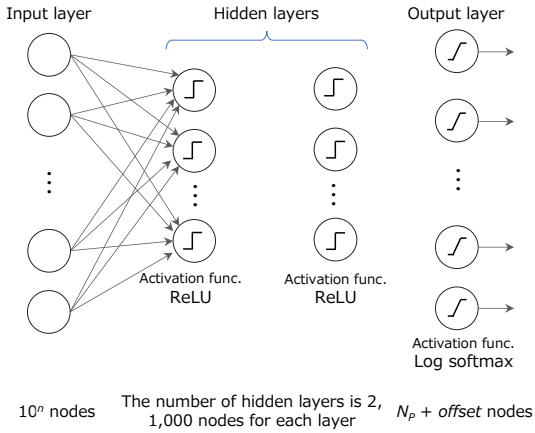


図 8 P の所有者が作成する識別器の原型 F_0

Figure 8 Prototype of classification F_0 initialized by P owner.

表 1 評価環境の諸元

Table 1 Parameters of evaluation environment.

Parameter	Explanation	Values
N_P	The number of samples in P	2000
N_Q	The number of samples in Q	3000
N_G	The number of dummy samples belonging to the garbage classes which are added to Q	0, 200, 1000, 2000, 3000
$N_{P\cap(Q+G)}$	The number of samples in P∩(Q+G)	10, 100, 200, 400, 600, 800, 1000
N_C	The number of columns in C	10000

また，P と Q にはそれぞれ電話番号の意味を持つ列が存在することし，評価環境で用いる電話番号は、メルセンヌツイスター・アルゴリズム（MT19937）を用いて、090 から始まる 11 桁の数字からなる文字列をランダムに作成する。

STEP 1 において P と Q の各所有者は，データ概要情報を互いに開示することで，電話番号の意味を持つ列を用いて共通データ構造を構築することを合意できるものとする．共通データ構造は，電話番号を 1 桁ごとに長さ 1 の文字列とし，N=4 の N-gram を用いて作成されるものとする．すなわち，共通データ構造は，N=4 の N-gram を実行して得られる，電話番号に現れる長さ 4 の文字列（0000 から 9999 の文字列）の共起の有無を示すマトリクスとなる．

4.2 結果と考察

前節で述べた評価環境を用いて，識別器の F 値について，P と Q の重複数，ガベージクラスのデータ量，3 章で述べた Matan らのバイアス有無が及ぼす影響を図 9 に示す．図中の凡例の G は，ガベージクラスのデータ量を示す．また，凡例の“w/ B”は Matan らのバイアスの存在を考慮せずにバイアスを含めた状態で識別する場合を示し，他方，“w/o B”はバイアスを取り除くことで $P \cap \overline{Q}$ の検出精度を向上させたものを示す．

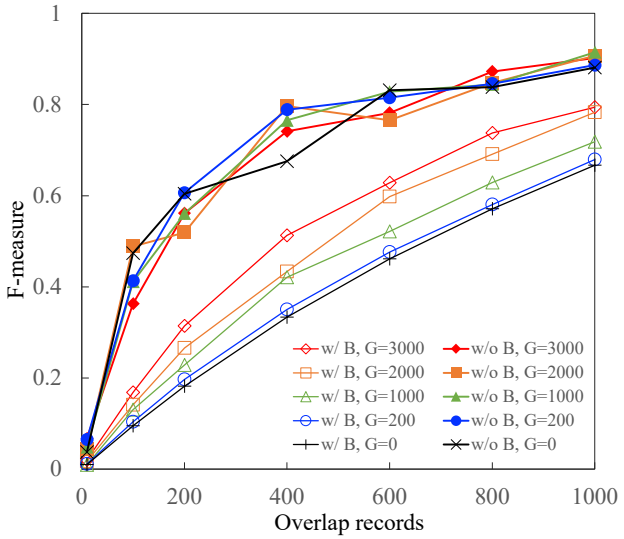


図 9　識別器の F 値

Figure 9　F-measure of classifications.

図 9 をみると，Matan らのバイアスを含めた場合は，G が増加するにつれて F 値が向上することがわかる．これは，Q の所有者が挿入するガベージクラスのデータ量が識別器の精度向上に寄与することを示す．仮に，C 上に現れるビット列の組み合わせを，ガベージクラスのデータを挿入することで全て網羅できたとすると，P は Q+G の部分集合とすることができるため，過学習された識別器を用いると，F 値は限りなく 1 に近づくと考えられる．しかし，これを実現するためには，Q の所有者は自身の計算機資源を大量に使ってガベージクラスを生成し，識別器を作成する必要に迫られるため，Q の所有者に対するインセンティブの設計が必要になる．

また，Matan らのバイアスを取り除くことで，G の数に関わらず F 値は改善することが確認できる．一方で，バイアスを含む場合の F 値を，含まない場合の F 値で除算した値を改善率と定義すると，図 10 に示すように，G が増加するにつれて，改善率は減少する傾向にあることが確認できる．これは，G が増加するにつれて，F_M の識別境界が細かく設定されることで，予測されるクラスにバイアスが発生しにくくなり，その結果，バイアスを取り除くことの効果が弱まるためと考えられる．

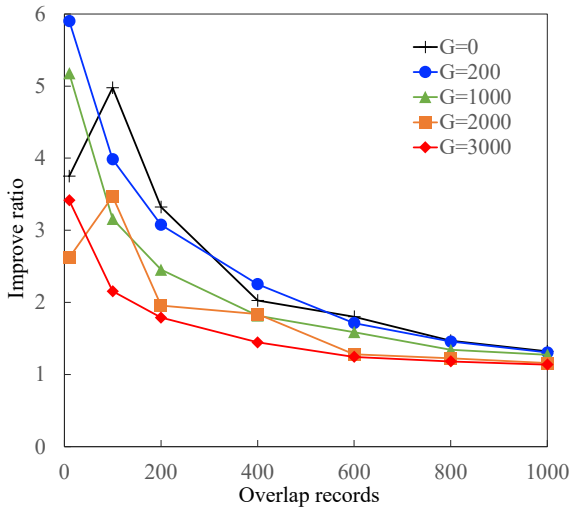


図 10　バイアスを取り除くことによる改善率

Figure 10　Improve ratio of removing bias.

また，図 10 をみると，P∩Q の数が多いほど F 値の改善率は減少することがわかる．これは，P と Q に重複して現れるサンプル数が増加することで，Q の所有者が識別器作成のために用いる学習データに含まれる P のデータが増加し，その結果，バイアスとして取り除く集合 P∩$\overline{Q}$が減少するためであると考えられる．更なる識別性能向上に向けて，P∩Q と Q の要素数の関係については，今後詳細な検討が必要である．

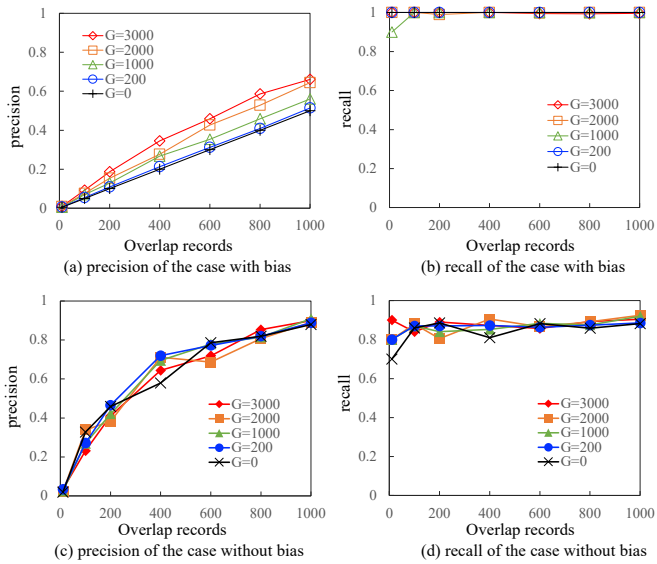


図 11　偽陽性と偽陰性の傾向を見るための精度と感度

Figure 11　Precision and recall for evaluations of false positives and false negatives.

データ共同分析の実用化検討あたって，偽陽性と偽陰性の各傾向を見るために，F 値を構成する精度と感度のそれぞれを図 11 に示す．図 11 の(a)と(b)は，バイアスを含めた状態で識別器を作成したときの精度と感度である．図 11 (a)

を見ると，P∩Q の要素数が増加するにつれて精度が向上することがわかるが，P∩Q の要素数が最大の 1000 であったとしても，その精度は 0.5〜0.6 程度である．そのため，この識別器を用いてクラスを予測した場合に，半数程度は偽陽性となる．また，P∩Q の要素数が小さいときには，精度が極端に低い値になることから，共通集合を正確に特定することができない. 一方, 図 11 (b) で示す感度を見ると，G および P∩Q の要素数によらず常に 1 に近い値になることがわかる．これは，偽陰性による取りこぼしがないことを示しており，医療や金融などのデータの見逃しが許容しにくい業務に適性があるといえる．

また，図 11 の(c)と(d)は，バイアスを取り除いた状態で識別器を作成したときの精度と感度である．バイアスを含めた場合の識別器と比較して，精度は全体的に改善する．一方で，感度は G および P∩Q の要素数によらず 0.8 から 0.9 の値を取ることから，偽陰性がわずかに増加する．P∩Q の要素数が小さいときには，バイアスを取り除いた状態で識別器を作成するほうが，偽陰性は増加するが，特定できる共通集合は増える．

図 11 から確認できる傾向は，Open Set Recognition における課題と一致する[13]. すなわち，この課題に対して，出力層の活性化関数 Log SoftMax の代わりに，OpenMax を使用することで精度と感度の両方を改善することが期待できる．

5. おわりに

本稿では，異なるデータ構造を持つ 2 者間で，互いにデータを持ち出すことなく，2 者が持つデータに基づく 1 つの共同分析用モデルを垂直連合学習により構築する手法を提案した．また，評価環境を用いて提案法によって得られたモデルの F 値を評価した．その結果，互いにデータを共有しない制約があった場合においても，共通集合及びその集合に含まれるサンプルの対応関係の有無を確率的に予測できることを確認した．

今後は，提案法に対して，3 者以上が存在する場合に適用できるように拡張すること，共通データ構造の構築手法に一般性を加えること，容易照合性を更に低減するための k 匿名性を取り入れることを検討する予定である．

参考文献

[1] Qiang Yang, Yang Liu, Tianjian Chen, and Yongxin Tong, “Federated Machine Learning: Concept and Applications,” ACM Trans. Intell. Syst. Technol. Vol. 10, No. 2, Article 12, February 2019.

[2] Jiang Jichu, Kantarci Burak, Oktug Sema and Soyata Tolga, “Federated Learning in Smart City Sensing: Challenges and Opportunities,” Sensors 2020; 20. 6230. 10.3390/s20216230, October 2020.

[3] Kholod I, Yanaki E, Fomichev D, Shalugin E, Novikova E, Filippov E and Nordlund M., “Open-Source Federated Learning Frameworks for IoT: A Comparative Review and Analysis,” Sensors 2021, 21(1):167. December 2020.

[4] P. Kairouz, H.B. McMahan, B. Avent, A. Bellet, M. Bennis, A.N. ABhagoji, R.G. d'Oliveira, “Advances and open problems in federated learning”, arXiv:1912.04977, 2019.

[5] 長尾 佳高，宮地 充子，“プライバシを保護したデータ突合プロトコル”，情報処理学会コンピュータセキュリティシンポジウム 2020，2020 年 10 月．

[6] 渡邉 雅之，“匿名化された個人情報はどのように取り扱うべきか”，Business Lawyers，IT・情報セキュリティ，https://www.businesslawyers.jp/practices/613，2017 年 8 月（参照 2021-08-08）．

[7] 早矢仕 晃章，大澤 幸生，“Data Jacket Store: データ利活用知識構造化と検索システム”，人工知能学会論文誌, 2016, 31 巻, 5 号, p. A-G15_1-9，2016 年 8 月．

[8] Burton H. Bloom, “Space/time trade-offs in hash coding with allowable errors,” Communications of the ACM, Vol. 13, Issue 7, pp 422–426, July 1970.

[9] 菅 孝徳，西出 隆，櫻井 幸一，“ブルームフィルタを用いた検索自由度の高い検索可能暗号の設計と実装評価”，情報処理学会研究報告，Vol. 2011-CSEC-53, No.20，2021 年．

[10] O. Matan, Richard Kiang, C.E. Stenard, Bernhard Boser, John Denker, Don Henderson, R.E. Howard, W. Hubbard, Larry Jackel, Y. Cur, “Handwritten Character Recognition Using Neural Network Architectures,” In Proceedings of the 4th USPS advanced Technology Conference, pp 1003-1011, November 1990.

[11] Akshay Raj Dhamija, Manuel Günther and Terrance E. Boult, “Reducing Network Agnostophobia,” 32th Neural Information Processing Systems (NeurIPS), December 2018.

[12] Open Miend, https://www.openmined.org/，(参照 2021-08-13）．

[13] Abhijit Bendale and Terrance E. Boult, “Towards Open Set Deep Networks,” 2016 IEEE Conference on Computer Vision and Pattern Recognition (SVPR), pp. 1563-1572, June 2016.