

# Detection of Credit Card Fraud Records Using Hierarchical Neural Networks

メタデータ	言語: jpn 出版者: 公開日: 2022-03-24 キーワード (Ja): キーワード (En): 作成者: 河合, 真知, 小高, 知宏, 黒岩, 丈介, 諏訪, いずみ, 白井, 治彦, Kawai, Masato, Odaka, Tomohiro, Kuroiwa, Jousuke, Suwa, Izumi, Shirai, Haruhiko メールアドレス: 所属:
URL	<a href="http://hdl.handle.net/10098/00028957">http://hdl.handle.net/10098/00028957</a>

## 階層型ニューラルネットワークによる クレジットカード不正利用履歴の検出

河合真知\* 小高知宏\*\* 黒岩丈介\*\* 諏訪いずみ\*\*\* 白井治彦\*\*\*\*

### Detection of Credit Card Fraud Records Using Hierarchical Neural Networks

Masato KAWAI\* Tomohiro ODAKA\*\* Jousuke KUROIWA\*\*

Izumi SUWA\*\*\* Haruhiko SHIRAI\*\*\*\*

(Received January 24, 2022)

In this paper, the effectiveness of the multilayer perceptron model for detecting credit card fraud records was examined by using real data. Since the original data set had an imbalance between normal and abnormal data, a shaping process was applied. Next, we conducted a preliminary experiment to determine the model structure to be used for the detection of credit card fraud records.

The model was trained by inputting well-formed data to the model structure determined by preliminary experiments. Each model trained with differently processed data sets were validated if the models can discriminate between abnormal and normal transactions with a validation data set. Four evaluation indices were used to evaluate each model that discriminated between abnormal and normal.

For the purpose of this study, the maximum value of recall, which indicates the percentage of fraudulent transactions that were actually judged to be fraudulent, was approximately 98 %.

For practical use, the value of recall should be close to 100 %, so further improvement is needed.

**Key words** : Credit Card Fraud Detection, multilayer perceptron

#### 1. 緒言

近年、現金を使わずに支払いを済ませる方法であるキャッシュレス決済が普及しており、日本国民の3割ほどの国民が何らかのキャッシュレス決済を利用している。キャッシュレス決済の種類には、クレジットカードやデビットカード、プリペイドカードのほか、電子マネーやQR・バーコード決済など多種多様にわたっている。

\*大学院工学研究科 知識社会基礎工学専攻

\*Fundamental Engineering for Knowledge-Based Society, Graduate School of Engineering

\*\*知能システム工学講座

\*\*Department of Human and Artificial Intelligent Systems

\*\*\*仁愛女子短期大学 生活科学学科

\*\*\*Jin-ai Women's College

\*\*\*\*工学部 技術部

\*\*\*\*Technical Division

その中でも、クレジットカード払いが最も多く利用されており、全体の9割以上を占めている。

クレジットカードは、現金の持ち合わせがなくても、与信限度額の範囲内で商品やサービスを購入し、請求に対する時間的余裕を提供する。<sup>[1]</sup> また、カード一枚で決済ができるため、財布の中から小銭や紙幣を探すといった手間が省け精算がスピーディーでスマートに行えたり、支払い履歴が残るため無駄遣い防止にもつながる。そういった利便性からクレジットカードの利用はますます浸透している。

しかし、それと同時に、クレジットカードの不正利用被害も年々増加傾向にある。ここ数年、フィッシング詐欺やなりすまし、ネットショッピング詐欺、スキミングなど、クレジットカードに関する様々な不正利用がニュースで取り上げられており、世界中のほとんどの人々が不正行為を念頭に置いている。不正利用に対する認知は高まっているが、クレジットカードの不正利用は簡単なターゲットであり、何のリスクもなく、所有者の知らな

うちに、短期間で多額の金額が引き出されたり、見知らぬ取引が行われてしまう。不正利用者は不正な取引を正当なものにしようとするため、不正利用の検知は非常に難しく、困難な作業である。

不正利用に対する対策として、例えば銀行では、EMVカードという磁気ストライプではなく集積回路にデータを保存するスマートカードへの移行が進んでいる。これにより、カードによる支払いの一部は安全になったが、カードを使用しない不正行為は依然として高い確率で発生している。

本研究では、クレジットカードの利用履歴から不正の取引を検出することを目標とする。不正の取引を検出する手法として、異常検知分野で応用されているニューラルネットワーク、その中でも単純な多層パーセプトロンモデルを用いる。クレジットカード不正利用検出に対する多層パーセプトロンモデルの有効性の検証には、第3章で説明する kaggle で提供されている Credit Card Fraud Detection<sup>[3]</sup>を用いる。また、モデルの評価には第3章で説明する4つの評価指標を用いる。

本論文では、2章にクレジットカード不正利用の原因と手口、不正利用対策に関する過去の研究を述べる。3章で異常検知実験について述べ、4章にその異常検知実験に対する結果を示す。5章で実験結果に対する考察を述べ、6章で本論文に対するまとめを述べる。

## 2. クレジットカード不正利用の手口と対策

最近では、オンラインネットショッピングの普及に伴い、店頭以外でもクレジットカードを利用する機会は増えている。企業間で行われる仕入れや売り上げといった取引では、現金での取引はほとんど発生していない。クレジットカードを使用することで、事業者側にも顧客側にも多くのメリットがあるが、カード決済が持ち合わせているリスクを把握していないと思われぬ被害に巻き込まれる可能性がある。以下にクレジットカード不正利用の原因や手口の例を挙げる。<sup>[2]</sup> また、クレジットカード不正利用の対策に関する過去の研究について述べる。

### 2.1 クレジットカード不正利用の手口

#### 1. フィッシング詐欺

フィッシング詐欺とは銀行等の金融機関やクレジットカード会社を装って、偽の web サイトに誘導するメールを送りつけ、誘導したサイトでクレジットカード番号や暗証番号等の情報を入力させて情報を盗み取る手口のことである。

#### 2. ネットショッピング詐欺

ネットショッピング詐欺とは架空のネットショッピングサイトで商品購入手続きをさせた上で商品を送らず、クレジットカード情報を盗む手口のことである。

#### 3. スキミング

スキミングとは、スキマーと呼ばれるカード情報読み取り装置を用いてカードの磁気ストライプ情報を盗み取り、偽造カードにコピーする手口のことである。

#### 4. 盗難や紛失

スリや置き引き、車上荒らしなどによってクレジットカードが盗難されるケースのほか、飲食店や電車、トイレ等での財布の置き忘れによる紛失によって、クレジットカードが不正利用されるケースである。

#### 5. なりすまし

なりすましは、第3者が不正に入手したクレジットカード情報やカード本体をカード所有者本人になりすまして利用する手口のことである。

#### 6. 出会い系サイト詐欺

出会い系サイト詐欺は、出会い系サイト内で使えるポイントをクレジットカード決済によって購入させ、サクラを使ってポイントを消費させ、カード情報を盗み取る手口のことである。

#### 7. ネットショップからの情報漏洩

ネットショップからの情報漏洩は、ネットショップに不正アクセスすることで、クレジットカード情報を盗み出す手口のことである。

### 2.2 クレジットカード不正利用に対する対策と関連研究

クレジットカードが不正利用される原因や手口は様々なものがあり、カード所有者本人が原因や手口を理解して気を配っていたとしても、悪人は巧妙な手口で不正利用を試みる。また、実際に不正利用が行われたことをカード所有者本人が気づくのは、カードの利用明細を確認してからであるため、発見が遅れることが多い。

そこで、本研究では、クレジットカードを使用した取引履歴において、各取引が持つ個々の特徴を学習し、不正利用を検出することを目的とする。クレジットカード不正利用の検出には、近年、異常検知分野に応用されているニューラルネットワークモデルを使用し、その中でも本研究では多層パーセプトロンモデルを用いる。クレジットカードの不正利用検出に対する多層パーセプトロンモデルの有効性の検証には、kaggle で提供されて

いる Credit Card Fraud Detection を使用する。このデータセットを用いた従来の研究では、2019 年に Vaishnavi Nath Dornadula や Geetha S によって、<sup>[1]</sup> サポートベクタマシン、ロジスティック回帰、決定木、ランダムフォレストなどの様々な機械学習手法を用いて、不正行為を予測するための最良の手法を開発する研究が行われた。この論文でのクレジットカード不正利用検出精度の最大値は accuracy で 99.98, precision で 99.96 であった。このほかにも、電子商取引をはじめとする多くのオンラインサイトで、オンラインでの決済手段が増え、オンライン詐欺のリスクが高まっているという現状を踏まえ、研究者たちはオンライン取引における詐欺を検出・分析するために様々な機械学習手法を開発している。

### 3. 異常検知実験

本章では、多層パーセプトロンモデルを用いたクレジットカード不正利用履歴の検出実験について述べる。まず、本実験に使用するデータセットと整形処理について述べる。次に、本実験に使用するモデル構造について説明する。

#### 3.1 データセットと整形処理

本実験では、kaggle からダウンロードした 2013 年 9 月の 48 時間に行われたヨーロッパのクレジットカードトランザクションデータセット<sup>[3]</sup>を使用する。このデータセットは非常にアンバランスで、284807 件の取引のうち、492 件が不正の取引である。特徴としては、取引の金額、最初の取引からの経過時間（単位：秒）、主成分分析によって匿名化された 28 の共変量が挙げられ、図 1 に一部を示す。各データポイントには、不正な取引かそうでないかのラベル (0:真正, 1:不正) が付けられている。図 1 中の数値特徴量は、前処理の段階でデータの平均を 0、標準偏差を 1 に正規化した。<sup>[4]</sup>

	Time	V1	V2	V3	V4	V5
0	0.0	-1.359807	-0.072781	2.536347	1.378155	-0.338321
1	0.0	1.191857	0.266151	0.166480	0.448154	0.060018
2	1.0	-1.358354	-1.340163	1.773209	0.379780	-0.503198
3	1.0	-0.966272	-0.185226	1.792993	-0.863291	-0.010309
4	2.0	-1.158233	0.877737	1.548718	0.403034	-0.407193

図 1: データプレビュー

このデータセットには、全 284807 件のトランザクション履歴が入っているが、そのうち不正のトランザクシ

ョンは 492 件と正常のトランザクションに対して非常に少ないアンバランスなものとなっている。このままのデータでモデルを学習すると、正常のトランザクションの特徴をより学習し、階層型ニューラルネットワークでクレジットカードの不正利用を検出するという本研究の目的に沿わない。そこで、元のデータに対して整形処理を行い、以下の [1]~[7] の新たなデータセットを用意した。比較のために、元のデータセットもモデルの学習に使用する。データ整形の方法としては、まず len 関数を用いて不正のトランザクションの件数 (492 件) を取得し、iloc というスライス機能を用いて、不正のトランザクションの k 倍分の正常のトランザクションを切り出す。

表 1: 整形処理後のデータセット

	件数	真正	不正	真正:不正
[1]k=2	1476 件	984	492	2:1
[2]k=3	1968 件	1476	492	3:1
[3]k=4	2460 件	1968	492	4:1
[4]k=6	3444 件	2952	492	6:1
[5]k=12	6396 件	5904	492	12:1
[6]k=24	12300 件	11808	492	24:1
[7]k=48	24108 件	23616	492	48:1
[8]元データ	284807 件	284315	492	

[1]~[8] のそれぞれのデータに対して、訓練用、検証用、テスト用の割合を

- ・訓練用データ：80% (検証用データ：20%)
- ・テスト用データ：20%

として分割した。

#### 3.2 モデルの構築

本研究では、クレジットカードの不正利用を検出するモデルとして多層パーセプトロン (MLP) を用いた。多層パーセプトロンとは、単純パーセプトロンを層状に重ね合わせ多層構造にしたニューラルネットワークである。ここで、単純パーセプトロンは、入力信号とそれに対応する重みを掛け合わせた値を全て足し合わせた値がある閾値を超えた場合に 1 を、そうでない場合に 0 を出力する。<sup>[5]</sup> 多層パーセプトロンは、単純パーセプトロンでは扱うことができなかった線形分離不可能な問題についても扱うことができるため、様々な場面で応用されている。本研究で使用する多層パーセプトロンの構造としては、図 2 に示すように、入力層、中間層 1 層、出力

層の3層からなるモデルである。入力層のユニット数は入力データの次元数と同じ28、出力層のユニット数を2(正常と異常を判別する2値分類より)としてモデルの構築を行った。中間層のユニット数については、後述する事前実験で決定する。中間層と出力層の活性化関数は、ほかのモデルを参考に、中間層をReLU関数、出力層をソフトマックス関数と設定した。重みの更新には、確率的勾配降下法(SGD)を採用した。

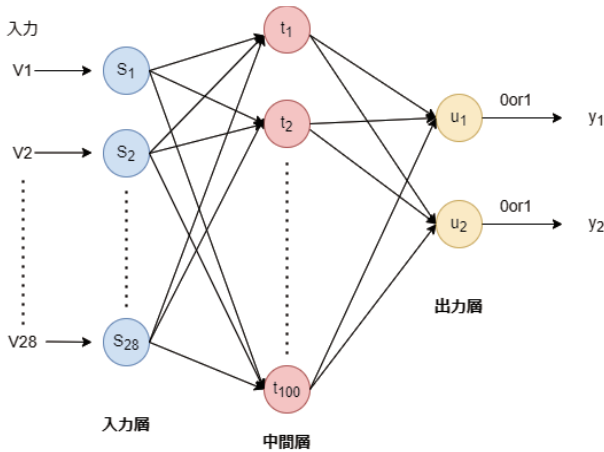


図2: 階層型ニューラルネットワーク(多層パーセプトロン)

ここで、中間層のユニット数を決定するための事前実験を行う。[4]k=6, 3444件, 真正:2952, 不正:492, 真正:不正=6:1のデータセットに対して、入力層のユニット数28と出力層のユニット数2は固定し、中間層のユニット数 $t_{1\sim n}$ 数のみを変化させ、最適な結果を示した時のモデル構造を採用する。そのモデルに対して、[1]~[8]それぞれのデータセットで学習し、結果を比較する。中間層のユニット数のみを変化させて学習させ、異常検知を行った結果を比較する指標を次の3.3節で述べる。

### 3.3 評価指標

[1]~[8]それぞれのデータセットで学習したモデルでクレジットカードの不正利用を検出した結果を比較するための評価指標として、accuracy(正解率), precision(適合率), recall(再現率), F-measure(F値)の4つを用いた。accuracy(正解率)は、全てのサンプルのうち正解したサンプルの割合、precision(適合率)は、不正と予測されたサンプルのうち正解したサンプルの割合、再現率(recall)は、実際に不正のサンプルのうち正解したサンプルの割合、F-measure(F値)は、precision(適合率)とrecall(再現率)の調和平均である。真陽性、真陰性、偽陽性、偽陰性をそれぞれTP: True Positive, TN: True Negative, FP: False Positive, FN: False Negativeとすると、4つの評価指標は以下の式で表される。<sup>[5]</sup>

$$accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

$$precision = \frac{TP}{TP + FP}$$

$$recall = \frac{TP}{TP + FN}$$

$$F\text{-measure} = \frac{2 * recall * precision}{recall + precision}$$

ここで、真陽性(TP: True Positive)は実際のクラスが不正:1で予測も不正:1、真陰性(TN: True Negative)は実際のクラスが正常:0で予測も正常:0、偽陽性(FP: False Positive)は実際のクラスは正常:0で予測が不正:1、偽陰性(FN: False Negative)は実際のクラスは不正:1で予測が正常:0を表す。

### 3.4 モデル構造の決定

中間層のユニット数を決定するためにn=1, 10, 20, 30, ..., 170, 180, 190, 200と変化させたときの4つの評価指標の値を表2に示す。

表2: 中間層のユニット数の変化による評価指標の比較

	accuracy	precision	recall	F-measure
[1]n=1	0.9753	0.9506	0.8556	0.9006
[2]n=10	0.9826	0.9425	0.9213	0.9318
[3]n=20	0.9840	0.9651	0.9121	0.9379
[4]n=30	0.9797	0.9348	0.9149	0.9247
[5]n=40	0.9724	0.9263	0.88	0.9026
[6]n=50	0.9768	0.9524	0.8696	0.9091
[7]n=60	0.9768	0.9462	0.8889	0.9167
[8]n=70	0.9826	0.9529	0.9101	0.9310
[9]n=80	0.9840	0.9697	0.9231	0.9458
[10]n=90	0.9782	0.9101	0.9205	0.9153
[11]n=100	0.9840	0.9787	0.9109	0.9436
[12]n=110	0.9898	0.9667	0.9560	0.9613
[13]n=120	0.9797	0.9314	0.9314	0.9314
[14]n=130	0.9826	0.9451	0.9247	0.9348
[15]n=140	0.9797	0.9080	0.9294	0.9186
[16]n=150	0.9884	0.9429	0.9802	0.9612
[17]n=160	0.9811	0.96	0.9143	0.9366
[18]n=170	0.9826	0.9639	0.8989	0.9302
[19]n=180	0.9840	0.9576	0.9496	0.9536
[20]n=190	0.9797	0.9271	0.9271	0.9271
[21]n=200	0.9797	0.9792	0.8868	0.9307

表2より、中間層のユニット数が150のときのrecall値が最大をとるため、最適であることがわかる。また、ユニット数の増減によるrecall値の推移に目立った傾向は見られないため、ユニット数n=200までで比較を終



了した. 次に recall 値が最適であったユニット数  $n=150$  付近で比較を行った結果を表 3 に示す.

表 3: 中間層のユニット数の変化による評価指標の比較 ( $n=150$  付近)

	accuracy	precision	recall	F-measure
[1] $n=147$	0.9840	0.9792	0.9126	0.9447
[2] $n=148$	0.9884	0.9659	0.9444	0.9551
[3] $n=149$	0.9855	0.9556	0.9348	0.9451
[4] $n=150$	0.9884	0.9429	0.9802	0.9612
[5] $n=151$	0.9811	0.9565	0.9072	0.9312
[6] $n=152$	0.9913	0.9806	0.9619	0.9712
[7] $n=153$	0.9826	0.9419	0.9205	0.9310

表 3 より, ユニット数 150 付近で比較を行ったところ, F-measure の値が最大を取ったのは, ユニット数  $n=152$  のときであったが, 本研究の目的である recall(再現率: 実際に不正のサンプルのうち正解したサンプルの割合) の値が最大をとったのは, ユニット数  $n=150$  のときであった. 以上より, 中間層のユニット数を 150 に決定した.

#### 4. 分類結果

3.4 節により決定した入力層のユニット数 28, 中間層のユニット数 150, 出力層のユニット数 2 の 3 層構造の多層パーセプトロンをそれぞれ [1]~[8] のデータセットで学習させ, 学習した各モデルでクレジットカードの不正利用を検出した時の結果を表 4 に示す.

表 4 実験結果

	accuracy	precision	recall	F-measure
[1] $k=2, 1476$ 件	0.9696	0.977	0.9239	0.9497
[2] $k=3, 1968$ 件	0.9746	0.9775	0.9158	0.9457
[3] $k=4, 2460$ 件	0.9695	0.9712	0.8938	0.9309
[4] $k=6, 3444$ 件	0.9884	0.9429	0.9802	0.9612
[5] $k=12, 6396$ 件	0.9923	0.9681	0.9381	0.9529
[6] $k=24, 12300$ 件	0.9939	0.9512	0.8764	0.9123
[7] $k=48, 24108$ 件	0.9956	0.8889	0.8791	0.884
[8]284807 件	0.9995	0.8837	0.8261	0.8539

本研究の目的である不正利用検出の観点から recall(再現率: 実際に不正のサンプルのうち正解したサンプルの割合) の値が一番良い [4] $k=6$  の時が最適であるという結論に至る. 表 5 に  $k=6$  の時の混同行列を可視化する.

表 5 混同行列の可視化

	予測が正常	予測が不正
実際に正常	582	6
実際に不正	2	99

表 5 を見ると, 実際のクラスは不正で予測が正常を表す偽陰性 (FN: False Negative) の件数が 2 件存在する. この 2 件の中に深刻な被害をもたらす取引が存在している可能性があるため, ニューラルネットワークの構造やモデルの学習方法の見直しを行い, 偽陰性の件数を 0 にすることが今後の課題である. また, 実際のクラスは正常で予測が不正を表す偽陽性 (FP: False Positive) の件数も 6 件あり, 正常なクレジットカード利用者の取引が停止されてしまうことも問題であるため, 偽陽性の件数を減らす工夫も考える必要がある.

#### 5. 考察

本章では, 多層パーセプトロンによるクレジットカード不正利用履歴の検出実験の考察を述べる.

本実験では, クレジットカード不正利用履歴の検出実験に多層パーセプトロンモデルを使用した. モデル構造として, 入力層 1 層, 中間層 1 層, 出力層 1 層の 3 層構造で, 各層のユニット数として, 入力層がデータの特徴量数の 28, 出力層が真正と不正の 2 値分類より 2 と設定した. 次に, クレジットカード不正利用履歴の検出に最適な中間層のユニット数を決定するために事前実験を行った. 真正と不正の割合が 6:1 のデータに対して中間層のユニット数のみを変化させ, 不正利用履歴の検出を行い, 3.3 節の評価指標を用いて, 各モデルの評価を行った. 表 2 と表 3 より, 本研究の目的である recall(再現率: 実際に不正のサンプルのうち正解したサンプルの割合) の値が最適であったユニット数  $n=150$  を本研究で使用するモデル構造として採用した. 事前実験により決定した入力層のユニット数 28, 中間層のユニット数 150, 出力層のユニット数 2 の 3 層構造の多層パーセプトロンに対して, [1]~[8] それぞれのデータセットで学習させ, 学習したモデルでクレジットカードの不正利用履歴を検出した結果を表 4 に示した.

表 4 より, 全体のデータ件数のうち正解した割合を示す accuracy(正解率) の値は, データ件数が多くなるほど大きくなる傾向がある. [1]~[8] のデータセットに含まれる不正のデータ件数は元のデータセットの 492 件のままで, 正常のデータ件数のみを変えることによって全

体のデータ件数を増やしている。データ件数を増やすと、accuracy の値は大きくなるが、これは、モデルが正常のトランザクションの特徴を学習し、真陰性の件数が大きくなっていることが関係する。accuracy はデータ件数を増やすことで大きくなるが、この場合、真陽性の件数が低くても全体としての accuracy が高くなるケースも存在する。本研究の目的は不正を不正と判断できるようになることであるため、accuracy のみで判断することはできない。

一方、不正と予測されたデータのうち正解した割合を示す precision(適合率) の値は、表 4 よりデータ件数が多くなるほど小さくなる傾向がある。これは、データ件数が増加するにつれて正常のトランザクションを不正であると判断する割合が増えることに起因するが、実際の現場に応用しようとした際に、正規のユーザーの利用を妨害することは望ましくないため、不正の件数に対して正常の件数が多すぎるアンバランスなデータでモデルを学習させるのはよくない。

本研究では、不正利用を不正であると判断できることを目的としているため、実際に不正のデータのうち正解した割合を示す recall(再現率) の値が 4 つの評価指標の中で最も重要であると考え。今回の実験で用意した [1]~[8] のデータセットのうち、最も recall の値が高かったのは、[4](k=6, 3444 件) のデータで学習させたときであった。また、precision(適合率) と recall(再現率) の調和平均である F-measure(F 値) の値に関しても [4] のデータで学習させた時が最適であったことから、本実験では入力層のユニット数 28、中間層のユニット数 150、出力層のユニット数 2 の 3 層構造の多層パーセプトロンモデル構造に対して [4] のデータセットで学習させることが最適であると結論づける。一方で、偽陰性の観点から問題点も存在する。表 5 の混同行列に示すように、偽陰性の件数が 2 件存在する。この 2 件の中に深刻な被害をもたらす取引が存在している可能性があるため、ニューラルネットワークの構造やモデルの学習方法の見直しを行い、偽陰性の件数を 0 にすることが今後の課題である。また、偽陽性の件数も 6 件あり、正常なクレジットカード利用者の取引が停止されてしまうことも問題であるため、偽陽性の件数を減らす工夫を考え、正常なクレジットカード利用者が快適に利用できるモデルを構築していきたい。

## 6. 結言

本研究では、クレジットカード不正利用検出における多層パーセプトロンモデルの有効性を実際のデータを用いて検証した。データには、kaggle からダウンロード

した 2013 年 9 月の 48 時間に行われたヨーロッパのクレジットカードトランザクションデータセットを用いた。このデータセットには、全 284807 件のトランザクション履歴が入っているが、そのうち不正のトランザクションは 492 件と正常のトランザクションに対して非常に少ないアンバランスなものとなっている。このままのデータでモデルを学習すると、正常のトランザクションの特徴をより学習し、階層型ニューラルネットワークでクレジットカードの不正利用を検出するという本研究の目的に沿わない。そこで、元のデータに対して整形処理を行い、いくつかのデータパターンを用意した。様々なデータパターンによる実験の結果から以下のことが結論付けられる。

まず、全体のデータ件数のうち正解した割合を示す accuracy(正解率) の値は、データ件数が多くなるほど大きくなる傾向がある。本研究では、データセットに含まれる不正のデータ件数は元のデータセットの 492 件のままで、正常のデータ件数のみを変えることによって全体のデータ件数を増やしている。データ件数を増やすと、accuracy の値は大きくなるが、これは、モデルが正常のトランザクションの特徴を学習し、真陰性の件数が大きくなっていることが関係する。単純な正解率はデータ件数を増やすことで大きくなるが、本研究の目的は不正を不正と判断できるようになることであるため、accuracy のみで判断することはできないと考えた。

一方、不正と予測されたデータのうち正解した割合を示す precision(適合率) の値は、データ件数が多くなるほど小さくなる傾向がある。これは、データ件数が増加するにつれて正常のトランザクションを不正であると判断する割合が増えることに起因するが、実際の現場に応用しようとした際に、正規のユーザーの利用を妨害することはよくないため、不正の件数に対して正常の件数が多すぎるアンバランスなデータでモデルを学習させるのはよくないと考える。

本研究の目的である不正利用検出の観点から、実際に不正のデータのうち正解した割合を示す recall(再現率) の値が 4 つの評価指標の中で最も重要であると考え。今回の実験で用意した [1]~[8] のデータセットのうち、最も recall の値が高かったのは、[4](k=6, 3444 件) のデータで学習させたときであったが、実際の現場で導入すると考えたときに、この値は 100% に近い値であることが望ましいため、さらなる改善が求められる。また、予測に失敗したトランザクションデータに特徴の傾向はないのかという検討も必要であろう。

最後に、不正利用検出に対する多層パーセプトロン (MLP) の有効性を判断するためにも、さらにデータ件数の多いデータセットでの検証や CNN をはじめとする、

他の手法との比較実験が必要である.

#### 参考文献

- [1] Vaishnavi Nath Dornadula, Geetha S : Credit Card Fraud Detection using Machine Learning Algorithms, *Procedia Computer Science*,165, 631–641(2019).
- [2] クレジットカード不正利用のパターンとは?予防と対策方法とは?, [https://www.orico.co.jp/service/knowledge/abuse/\(2021/12/11\)](https://www.orico.co.jp/service/knowledge/abuse/(2021/12/11))
- [3] Credit Card Fraud Detection, [https://kaggle.com/mlgulb/creditcardfraud\(2021/11/28\)](https://kaggle.com/mlgulb/creditcardfraud(2021/11/28))
- [4] Ankur A. Patel 著, 中田 秀基 訳: Python ではじめる教師なし学習, 株式会社オライリー・ジャパン, 30-34(2020)
- [5] 平野 誠, 八槇 博史: 機械学習を用いた攻撃検知に関する学習手法の精度評価, 情報処理学会, 第 81 回全国大会, 461-462(2019)