

# 詐欺抵抗診断 Web アプリケーションの特微量選択\*

小久保 温†

## Feature Selection of a Fraud Resistance Diagnosis Web Application

Atsushi KOKUBO

### ABSTRACT

The initial version of the web application for fraud resistance diagnosis estimated user resistance to four representative types of fraud using 78 questions and logistic regression. However, its generalization performance was low, with an ROC AUC of 53.3% and a recall of 0.8%, leading to a misclassification where 99.2% of positive cases were predicted as negative. Previous research by the author improved these metrics to an ROC AUC of 82.2% and a recall of 68.9%.

This study compared four feature selection techniques for logistic regression: stepwise forward variable selection, stepwise backward variable elimination, L1 regularization, and L2 regularization, aiming to reduce the number of questions used as features. Stepwise forward variable selection proved effective for question reduction, while L2 regularization proved effective for improving generalization performance. However, the difference in generalization performance was found to be within the margin of error. By combining stepwise forward variable selection with L2 regularization, the study successfully reduced the 78 questions to 9 without sacrificing generalization performance.

**Key Words:** machine learning, feature selection, fraud vulnerability, web application

**キーワード:** 機械学習, 特微量選択, 詐欺脆弱性, Web アプリケーション

### 1. はじめに

この論文では、詐欺抵抗診断 Web アプリ(以降「アプリ」)の特微量選択について論じる。アプリは、URL にブラウザでアクセスすると、一連の択一式の質問(図 1, 2 など)が表示され回答すると、代表的な 4 種類の詐欺「オレオレ詐欺」「架空請求詐欺」「還付金等詐欺」「融資保証金詐欺」に対する抵抗力が機械学習で診断され表示されるものであった(図 3)。抵抗力を推定するための質問への回答が特微量で、説明変数とも呼ばれる。目的変数は回答すると表示される抵抗力である。アプリの初版では、説明変数 66 問と目的変数 12 問の計 78 問の質問に、およそ 20 から 30 分かけて回答する必要があった。これはアプリの主なターゲットと考えていた高齢者が回答するには多すぎた。この論文では推定性能を低下させずに特微量である質問を選択し、質問を 9 問に減らした方法を論じる。

\* 令和 6 年 11 月 29 日 受付

令和 7 年 2 月 13 日 受理 (査読付き論文のみ記載)

† 工学研究科

## 2. アプリ初版の開発と汎化性能の評価と改善

まず、先行研究について論じる。先行研究は、渡部ら<sup>1,2,3,4,5,6)</sup>によるアプリの初版の開発と著者<sup>7)</sup>による汎化性能の評価と改善である。

### 2.1 アプリの開発・運用

アプリは、科学技術振興機構(JST) 社会技術研究開発センター(RISTEX)の「高齢者の詐欺被害を防ぐしなやかな地域連携モデルの研究開発」(研究代表者・渡部諭秋田県立大学教授・当時)で開発・運用<sup>1)</sup>されたものである。このプロジェクトは、「安全な暮らしをつくる新しい公／私空間の構築」領域に採択され、特殊詐欺被害の減少を目指して2017年10月～2021年3月のおよそ3年半実施された<sup>2)</sup>。プロジェクトでは、アプリを活用して詐欺被害防止の啓発活動に取り組んだ。

アプリはWebアプリで、アプリのURLにブラウザでアクセスすると、一連の択一式の質問(図1, 2など)が表示される。回答すると、代表的な4種類の詐欺「オレオレ詐欺」「架空請求詐欺」「還付金等詐欺」「融資保証金詐欺」に対する抵抗力が機械学習で診断され表示された(図3)。アプリは2019年2月21日～2021年3月31日の約2年間運用された。

アプリは初版、2版、3版の計3つバージョンがあり、これら3つで診断結果は計11,564回表示された。このうち、アプリの初版は2019年2月21日から2020年3月23日まで運用された。アプリの初版はプロジェクトでイベントを開催して広報し、TVのニュースにも取り上げられ、診断は9,237件表示され、そのうち有効な診断が8,778件記録された。2版、3版は、新型コロナウイルスの流行によりイベント等で広報ができなくなり、回答が減り陽性の件数も少なく、評価や学習に十分なデータを集めることができなかった。本論文では、アプリ初版までに収集したデータのみを扱う。

図1 質問(説明変数)の回答画面

図2 質問(目的変数)の回答画面

図3 判定結果の画面

## 2.2 アプリ初版の説明変数と目的変数の構成

アプリでは、一見詐欺と関係ない質問への回答から、詐欺の被害に遭いそうな場面で危険な行動を取る傾向を推定しようとしていた<sup>3)</sup>。詐欺と関係があることが明らかな質問だと、回答者はよい診断結果を得ようと、詐欺被害に遭いにくいと思われる選択肢を回答することが予想されるからである。

機械学習には、予測に使う説明変数と予測対象の目的変数がある。学習させるときは説明変数と目的変数からなる学習データを用意し、説明変数から目的変数が予測できるように、機械学習モデルのパラメータを求める。機械学習モデルとはアルゴリズムとパラメータのセットである。たとえば if-else のルールから構成される決定木や、アプリで採用したロジスティック回帰など、さまざまなものがある。機械学習モデルの学習を終えてパラメータが求まったら、パラメータを用いて説明変数から目的変数を予測する。

渡部ら<sup>4)</sup>は、アプリを作る前に質問紙で調査を行って学習データを集め、アプリに採用する説明変数と目的変数を決め、機械学習モデルのパラメータを求めた。アプリ初版のパラメータは先行研究<sup>5)</sup>に掲載されている。調査では、説明変数の候補として性別・年齢・家族などの人口統計学的な属性、渡部らの過去の研究から詐欺被害と関係があると思われる心理特性を聞いた。目的変数としては、詐欺の被害に遭いそうな場面でどう行動するかを聞いた。調査では有効な回答が 667 件得られた。

渡部ら<sup>4)</sup>は、目的変数をよく説明する説明変数を選んだ。最終的にアプリの初版に採用されたのは「あなたの性別を教えてください。」などの人口統計学的質問 6 問、「自分は詐欺に遭わない自信がある」(図 1)など詐欺場面における行動特性 9 問、「私の人生は、これから楽しくなると思う」など未来展望 10 問、「何か仕事をするときは、自信をもってできる」など自己効力感 16 問、「普段、自分は健康であると感じる」など生活の質 25 問であった。人口統計学的な質問以外は、「当てはまる」「少し当てはまる」「だいたい当てはまる」「当てはまらない」の 4 択で回答する。

渡部ら<sup>5, 6)</sup>は、目的変数として詐欺の被害に遭いそうな場面を読んでどう行動するかの回答を用いた。取り上げた詐欺の種類は代表的な「オレオレ詐欺」「架空請求詐欺」「還付金等詐欺」「融資補償金詐欺」の 4 種類であった。質問はそれぞれの種類の詐欺について 3 問で、オレオレ詐欺は問 A・F・K、架空請求詐欺は問 B・E・H、還付金等詐欺は問 C・I・L、融資保証金詐欺は問 D・G・J であった。ただし、実際に使ってみたところ、質問 H の日本語がわかりにくくおかしい回答傾向が得られた。そこで、12 問表示されるが、推定には問 H を除いた 11 問が用いられた。回答は「そうしない」「おそらくそうしない」「おそらくそうする」「そうする」の 4 択であった。詐欺のシナリオ問題 12 問全体の概要は渡部らの先行研究<sup>6)</sup>に、具体的な内容は先行研究<sup>3)</sup>に 3 問掲載されている。質問はたとえば次のようなものであった(および図 2)。

警察から自宅に電話があり、「犯人を逮捕したんですが、あなたの口座が犯罪に使われていることがわかりました。直ぐに手続きをしないと口座から引き出しができなくなります。」という連絡だった。この後、自宅に銀行協会の担当者がキャッシュカードを受け取りに来るので、来訪してきた担当者にカードを渡し聞かれた暗証番号を伝えた。

そして、すべて回答すると機械学習による推定をもとに判定画面(図 3)が表示された。

アプリの初版で採用された質問は説明変数 66 問と目的変数 12 問の計 78 問あり、回答するのに 20 から 30 分近くの時間を必要とした。一覧を表 1 に示した。

表1 アプリ初版の質問の構成

種類		個数	備考
説明変数	人口統計学	6	
	行動特性	9	
	未来展望	10	
	自己効力感	16	
	生活の質	25	
	小計	66	
目的変数	オレオレ詐欺	3	
	架空請求詐欺	3	1 問日本語に問題あり
	還付金等詐欺	3	
	融資保証金詐欺	3	
	小計	12	
合計		78	

### 2.3 アプリ初版の性能の評価

渡部らのアプリの初版<sup>2, 3, 4, 5, 6)</sup>は評価されてこなかったので、著者は汎化性能の評価を行った<sup>7)</sup>。これをまとめたのが図4である。

アプリの初版は、質問紙調査で収集した 667 件のデータで学習したロジスティック回帰のモデルであった。渡部らはロジスティック回帰の計算で陽性の個数が少ないことに対応するために陽性・陰性の閾値を修正し、説明変数を選択するために AIC(赤池情報量基準)を参照して stepwise の変数減少法を実行していた。

機械学習では、学習に使っていない未知のデータを予測できる必要があり、これを汎化性能という。アプリの初版の場合、事前に集めた質問紙調査のデータ 667 件を学習に用いていて、アプリの初版で収集されたデータ 8,778 件は学習に使われていないので、アプリの初版で収集したデータ 8,778 件をどれだけうまく推定できたかが汎化性能になる。汎化性能を求めたところ、機械学習の全体的な性能を表す ROC AUC(受信者操作特性の曲線下面積)は 53.3%であった。ROC AUC は、すべて正しく予測できると 100%，ランダムな予測は 50%，すべて逆に予測すると 0%になる。つまり、アプリの初版の性能はランダムな予測に近かった。また、アプリでは、詐欺被害に遭う行動を取る危険な人が陽性で、そうでない人が陰性である。実際に陽性のうち、陽性と診断された割合を再現率というが、アプリの初版の再現率は 0.8%で、陽性(危険)の 99.2%を陰性(安全)と診断していた。

つまり、アプリの初版では、78 問の質問に 20 から 30 分近くかけて回答しても、診断はランダムに近く、危険な人もほぼ安全と診断されていたということである。

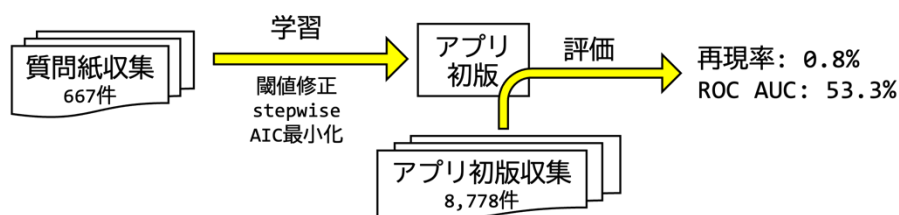


図4 アプリ初版のロジスティック回帰の学習と汎化性能の評価

## 2.4 アプリの汎化性能の改善

著者は汎化性能が低かった原因を調べ、改善を行った<sup>7)</sup>。

まず、渡部ら<sup>2,3,4,5,6)</sup>はアプリ初版の機械学習のモデルの開発の際、学習データが不均衡クラスであることを考慮していなかった。不均衡クラスとは、陽性・陰性の個数が(大きく)異なることを言う。アプリでは、詐欺被害に遭う可能性が高い行動を取る危険な人が陽性で、そうでない人が陰性である。一般に詐欺の被害に遭う人は人口全体から見ると少数である。実際に著者による研究<sup>7)</sup>で、陽性は質問紙調査では2.6%、アプリ収集データでは3.1%と少数で、どちらも不均衡クラスであることがわかった。全体のうち予測が正解した割合を正解率というが、不均衡クラスの場合は多い方だと推定するだけで正解率は向上する。例えばこのアプリの場合、すべて陰性(安全)と推定すると、陽性は3%程度なので正解率は97%程度になるが、陽性はすべて取りこぼされてしまう。著者は、不均衡クラスを考慮し、陽性と陰性の数の逆数の重みをつけて機械学習を行った。これは陽性のものと陰性のものを分けてそれぞれ学習させたものを組み合わせて使うことに相当する。また、学習データには一般に誤差が含まれるが、この影響によりモデルが複雑になりすぎないように正則化も行っている。その結果、再現率は0.8%から68.7%に上昇し、陽性を取りこぼす割合は99.2%から31.3%に減少した。ただし、全般的な性能であるROC AUCについては53.3%が57.0%になり、あまり改善は見られなかった。

ROC AUCは全体的な性能を表し、これが低いということは学習データの個数が不足している可能性が考えられた。著者が陽性の個数を調べたところ、11種類ある目的変数のうち、最少のものは3件、最多でも71件で、説明変数66個の係数を求めるには不足していたことがわかった。そこで、アプリで収集した8,778件のデータを用いて、学習データを増やすことにした。ただし、汎化性能の評価は、学習には使っていない機械学習モデルには未知のデータで行う必要がある。そこで、8,778件のデータを学習データ80% 7,022件と評価データ20% 1,756件に分割した。そして、学習データでモデルを学習させ、モデルにとって未知の評価データで性能を計算した。

学習と評価の分割は乱数を用いて、目的変数11種類それぞれについて陽性と陰性の割合が学習と評価で等しくなる層化抽出を行った。なお、機械学習の学習結果は分割によって変動する可能性がある。そこで、分割は20種類作り、性能は平均を取って評価した(図5)。このときの改良したモデルを図5では「小久保2023」と記載している。「小久保2023」の汎化性能は全体的な性能であるROC AUCが平均で82.2%、陽性を拾う確率である再現率が平均で68.9%となった。アプリの初版はROC AUCが平均で53.3%、再現率が平均で0.8%だった(図4)ので、大幅に汎化性能が向上した。

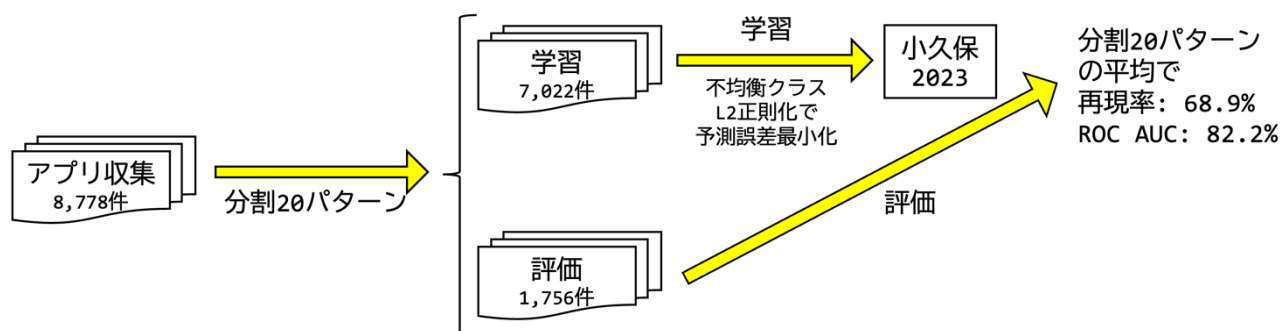


図5 著者が改良したアプリ「小久保 2023」のロジスティック回帰の学習と汎化性能の評価

### 3. アプリの特微量選択

アプリの初版の質問は、説明変数が 66 問、目的変数が 12 問(推定に使用したのは 11 問)の合計 78 問あった。アプリが主なターゲットとしていた詐欺被害者が多い高齢者にとって、20 から 30 分近くかけて 78 問に回答するのは大変だった。

そこで、今回の研究では、機械学習の特微量選択の手法を比較し、アプリの性能を下げずに質問を削減することに取り組んだ。

今回の研究では、性能だけではなく、どの特微量を選び、その特微量が係数いくつなのかを分析する。このため、以降の計算では学習と評価の分割を 100 セットに増やした。

#### 3.1 特微量選択手法の比較

渡部ら<sup>2, 3, 4, 5, 6)</sup>がアプリで採用した機械学習はロジスティック回帰である。ロジスティック回帰の場合、代表的な特微量選択は stepwise と正則化がある。stepwise は特微量(説明変数)を逐次的に追加・削除を行う局所最小解になり、正則化は全体最小解になる。それぞれの方法で、特微量の個数と汎化性能を求めた。

#### 3.2 stepwise 法

一般的に説明変数の数が増えると、機械学習の推定式の次数が上がり複雑な関数になる。複雑な関数を用いれば学習に用いたデータを説明することはできるが、学習データに含まれる誤差の影響を受けやすく、未知のデータを推定する汎化性能が低くなる。そこで、さまざまな説明変数の組を作り、推定式の複雑さと最大尤度からモデルの良さを AIC(赤池情報量規準)で評価して、最良のモデルを求めることが考えられる。AIC は  $-2 \ln L + 2k$  で、 $L$  は最大尤度、 $k$  は自由パラメータの数で、AIC が小さいほど良いモデルとされる。

ただし、説明変数の数が多い場合、組み合わせの数が増えるため、全てを調べることはできない。そこで、モデルに説明変数を逐次的に追加や削除していき、AIC が最小のモデルを見つけようとするのが stepwise 法である。逐次的に特微量選択を行うため、実際に得られるのは局所最小解である。

表 2~5 に stepwise 法で、説明変数の個数を、最多から減らしていく変数減少法(backward elimination)、最少から増やしていく変数増加法(forward selection)の場合の特微量の個数と ROC AUC の平均を示した。平均とは、本研究では学習と評価への分割を 100 セット用意したが、この 100 セットの平均のことである。目的変数は A から J まで(H は日本語に問題があったため除外)の 11 種類である。計算にはアプリ初版で用いられていた R 言語の stats パッケージの GLM を用いた。

減少法では特徴量 12～18 個, ROC AUC 77～85%となった. 増加法では特徴量 6～11 個, ROC AUC 76～86%であった. 増加法と減少法のどちらがいいかは目的変数によって異なることがわかった.

なお, 表 2～5 には, 一覧性を高め比較しやすくするために「3.3 正則化」で説明する「L1 正則化」と「L2 正則化」, 「3.5 選択された特徴量と予測性能」で説明する「特徴量選択後 L2 70%カバー」と「特徴量選択後 L2 90%カバー」も載せている.

### 3.3 正則化

データの誤差などで過学習が起こり, 機械学習の推定式で特定の特徴量の係数が大きくなりすぎ, 結果として汎化性能が低下することがある. これを防ぐのが正則化で, 機械学習で最適化する損失関数に特徴量の 1 次の L1, 2 次の L2 のペナルティ項を学習時に加える. 正則化は逐次的ではなく全体最適化になる. このとき L2 は特徴量を削減しないが, L1 は削減する効果が得られる. 本研究では, Python の scikit-learn 1.3.2 の LogisticRegression モデルを用い, L1 または L2 正則化を行った. そして 5 分割層化交差検証で PR 曲線下の面積を最大化する L1 や L2 の強さを求めた. stepwise 法同様に表 2～5 に特徴量の個数と ROC AUC の平均を示した. L2 は特徴量削減の効果がなく 66 個すべての説明変数が採用され, ROC AUC 76～88%であった. L1 は特徴量 38～62 個, ROC AUC 76～87%であった.

表 2 オレオレ詐欺の目的変数と変数削減方法, 説明変数(質問)の個数, ROC AUC の比較

目的変数	方法	説明変数の個数	ROC AUC
A	stepwise 変数減少法	12.35 ± 2.13 個	77.11 ± 3.89%
	stepwise 変数増加法	5.41 ± 1.67 個	76.89 ± 3.89%
	L1 正則化	61.91 ± 8.15 個	77.77 ± 3.80%
	L2 正則化	66.00 ± 0.00 個	78.47 ± 4.04%
	特徴量選択後 L2 70%カバー	9.00 ± 0.00 個	80.15 ± 3.43%
	特徴量選択後 L2 90%カバー	19.00 ± 0.00 個	79.85 ± 3.53%
F	stepwise 変数減少法	15.74 ± 1.70 個	81.42 ± 2.29%
	stepwise 変数増加法	10.67 ± 2.18 個	80.92 ± 2.19%
	L1 正則化	51.50 ± 12.63 個	81.19 ± 2.21%
	L2 正則化	66.00 ± 0.00 個	81.13 ± 2.24%
	特徴量選択後 L2 70%カバー	9.00 ± 0.00 個	80.95 ± 2.19%
	特徴量選択後 L2 90%カバー	19.00 ± 0.00 個	81.72 ± 1.98%
K	stepwise 変数減少法	13.39 ± 1.69 個	81.53 ± 3.40%
	stepwise 変数増加法	8.66 ± 1.44 個	82.25 ± 3.25%
	L1 正則化	45.76 ± 10.10 個	82.45 ± 3.33%
	L2 正則化	66.00 ± 0.00 個	82.89 ± 3.53%
	特徴量選択後 L2 70%カバー	9.00 ± 0.00 個	84.28 ± 2.85%
	特徴量選択後 L2 90%カバー	19.00 ± 0.00 個	84.01 ± 2.99%

表 3 架空請求詐欺の目的変数と変数削減方法, 説明変数(質問)の個数, ROC AUC の比較

目的変数	方法	説明変数の個数	ROC AUC
B	stepwise 変数減少法	15.92 ± 2.05 個	80.16 ± 2.58%
	stepwise 変数増加法	7.54 ± 1.79 個	79.08 ± 2.81%
	L1 正則化	55.78 ± 11.62 個	80.67 ± 2.63%
	L2 正則化	66.00 ± 0.00 個	81.53 ± 2.87%
	特徴量選択後 L2 70%カバー	9.00 ± 0.00 個	80.15 ± 3.06%
	特徴量選択後 L2 90%カバー	19.00 ± 0.00 個	82.19 ± 2.46%
E	stepwise 変数減少法	14.82 ± 1.90 個	75.96 ± 2.76%
	stepwise 変数増加法	8.34 ± 1.48 個	76.11 ± 2.83%
	L1 正則化	38.82 ± 7.29 個	76.83 ± 2.80%
	L2 正則化	66.00 ± 0.00 個	76.87 ± 2.67%
	特徴量選択後 L2 70%カバー	9.00 ± 0.00 個	77.28 ± 2.68%
	特徴量選択後 L2 90%カバー	19.00 ± 0.00 個	77.11 ± 2.72%

表 4 還付金等詐欺の目的変数と変数削減方法, 説明変数(質問)の個数, ROC AUC の比較

目的変数	方法	説明変数の個数	ROC AUC
C	stepwise 変数減少法	15.17 ± 2.61 個	84.78 ± 3.34%
	stepwise 変数増加法	7.19 ± 1.47 個	85.86 ± 3.39%
	L1 正則化	44.73 ± 9.97 個	86.19 ± 3.15%
	L2 正則化	66.00 ± 0.00 個	87.78 ± 2.90%
	特徴量選択後 L2 70%カバー	9.00 ± 0.00 個	87.79 ± 3.01%
	特徴量選択後 L2 90%カバー	19.00 ± 0.00 個	87.13 ± 2.86%
I	stepwise 変数減少法	16.48 ± 2.45 個	78.63 ± 3.31%
	stepwise 変数増加法	7.36 ± 1.64 個	79.12 ± 3.35%
	L1 正則化	43.75 ± 11.35 個	81.89 ± 2.74%
	L2 正則化	66.00 ± 0.00 個	83.39 ± 2.59%
	特徴量選択後 L2 70%カバー	9.00 ± 0.00 個	81.37 ± 3.34%
	特徴量選択後 L2 90%カバー	19.00 ± 0.00 個	82.39 ± 2.93%
L	stepwise 変数減少法	14.39 ± 1.92 個	82.02 ± 2.77%
	stepwise 変数増加法	8.21 ± 1.48 個	82.67 ± 2.80%
	L1 正則化	48.63 ± 14.20 個	82.95 ± 2.83%
	L2 正則化	66.00 ± 0.00 個	83.82 ± 2.66%
	特徴量選択後 L2 70%カバー	9.00 ± 0.00 個	83.76 ± 2.70%
	特徴量選択後 L2 90%カバー	19.00 ± 0.00 個	83.86 ± 2.61%



表 5 融資保証金詐欺の目的変数と変数削減方法, 説明変数(質問)の個数, ROC AUC の比較

目的変数	方法	説明変数の個数	ROC AUC
D	stepwise 変数減少法	16.30 ± 2.20 個	84.34 ± 2.85%
	stepwise 変数増加法	7.39 ± 1.90 個	83.74 ± 2.85%
	L1 正則化	47.00 ± 8.52 個	85.15 ± 2.72%
	L2 正則化	66.00 ± 0.00 個	86.00 ± 2.67%
	特微量選択後 L2 70%カバー	9.00 ± 0.00 個	85.09 ± 2.83%
	特微量選択後 L2 90%カバー	19.00 ± 0.00 個	85.57 ± 2.52%
G	stepwise 変数減少法	17.84 ± 2.11 個	80.17 ± 2.68%
	stepwise 変数増加法	7.75 ± 1.63 個	80.51 ± 2.55%
	L1 正則化	53.91 ± 11.29 個	81.56 ± 2.72%
	L2 正則化	66.00 ± 0.00 個	81.98 ± 2.75%
	特微量選択後 L2 70%カバー	9.00 ± 0.00 個	82.17 ± 2.46%
	特微量選択後 L2 90%カバー	19.00 ± 0.00 個	82.39 ± 2.52%
J	stepwise 変数減少法	15.65 ± 2.31 個	81.73 ± 3.15%
	stepwise 変数増加法	8.73 ± 2.31 個	81.44 ± 3.12%
	L1 正則化	52.09 ± 10.64 個	82.94 ± 3.07%
	L2 正則化	66.00 ± 0.00 個	84.02 ± 2.96%
	特微量選択後 L2 70%カバー	9.00 ± 0.00 個	83.31 ± 2.89%
	特微量選択後 L2 90%カバー	19.00 ± 0.00 個	83.33 ± 2.96%

### 3.4 ROC AUC の箱ひげ図による詳細な比較

表 2~5 に示すように, 目的変数にもよるが ROC AUC は L2 正則化が最良である場合が多い. 特微量の個数は変数増加法が最も少なくなることがわかった. この場合, どのくらい差があるのかを, 標準偏差を含めて比較することにした. それぞれの詐欺の種類, 特微量(質問)ごとに, 図 6~16 に箱ひげ図を示した. それぞれの箱ひげ図は上から「stepwise 変数減少法」「stepwise 変数増加法」「L1 正則化」「L2 正則化」「特微量選択後 L2 正則化 70%カバー」「特微量選択後 L2 正則化 90%カバー」での ROC AUC である. 特微量選択後 L2 正則化の 2 つについては, 「4 アプリのパラメータの導出」で説明するが, 改めて示すには図の要素の重複が多くなるため, ここで示している.

目的変数 I 除くと, 「stepwise 変数増加法」「stepwise 変数減少法」「L1 正則化」「L2 正則化」は, 25%の位置である第 1 四分位点から, 75%の位置である第 3 四分位点の範囲(長方形)がオーバーラップしており, 特微量選択の方法の違いは誤差の範囲内であった. そこで, 特微量選択には変数増加法を採用することにした.

なお, オレオレ詐欺は問 A・F・K で問 K の ROC AUC が平均で最良だった. 架空請求詐欺は問 B・E で問 B が平均で最良だった. 還付金等詐欺は問 C・I・L で問 C が平均で最良だった. 融資保証金詐欺は問 D・G・J で問 D が平均で最良だった.

## オレオレ詐欺の ROC AUC の比較

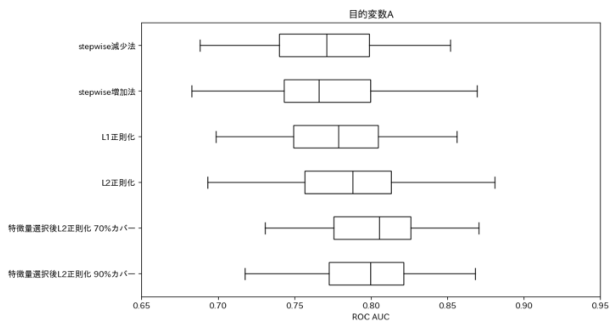


図 6 目的変数 A

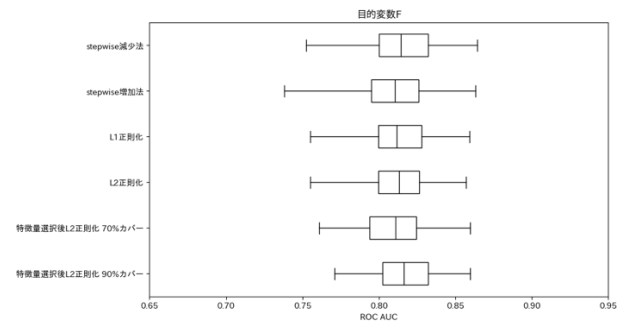


図 7 目的変数 F

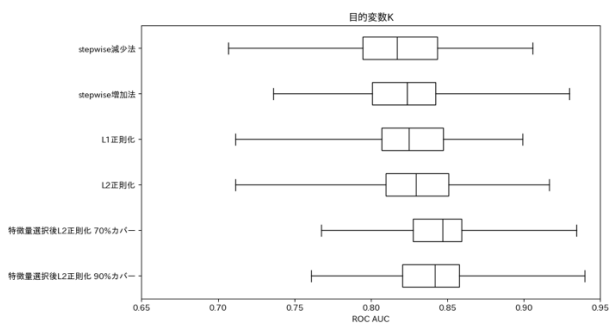


図 8 目的変数 K

## 架空請求詐欺の ROC AUC の比較

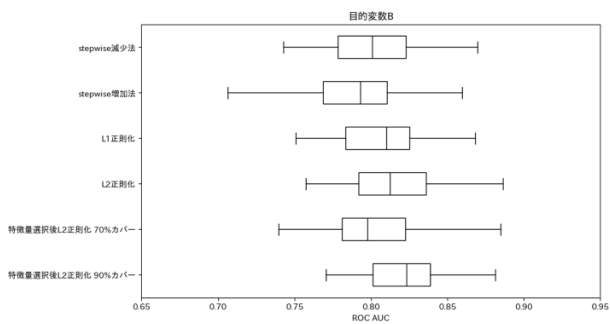


図 9 目的変数 B

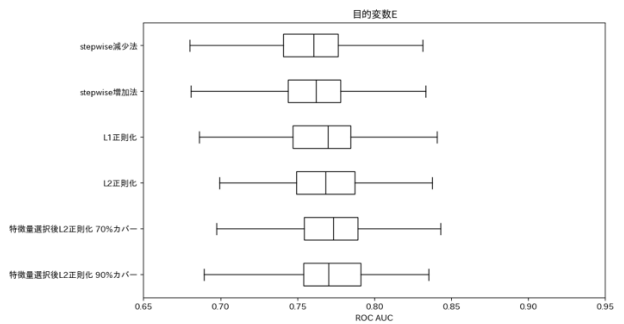


図 10 目的変数 E

## 還付金等詐欺の ROC AUC の比較

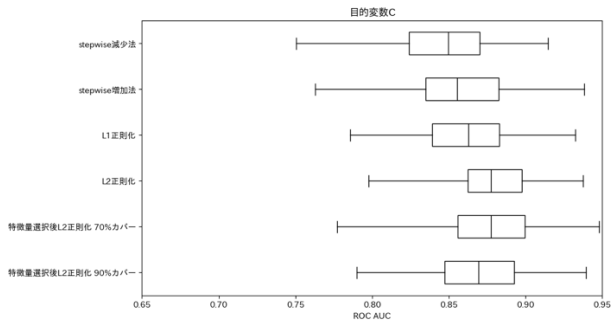


図 11 目的変数 C

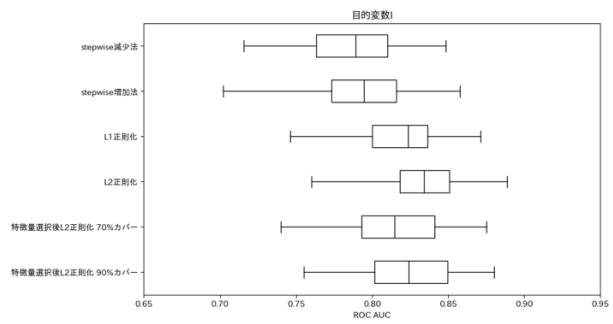


図 12 目的変数 I

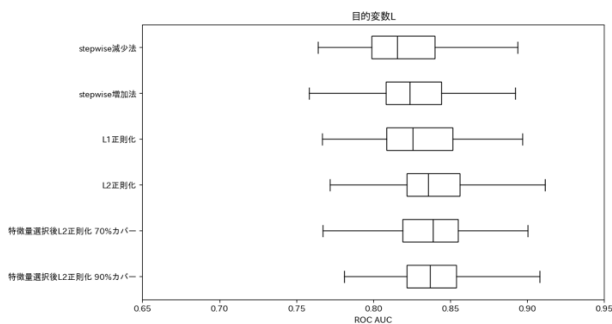


図 13 目的変数 L

## 融資補償金詐欺の ROC AUC の比較

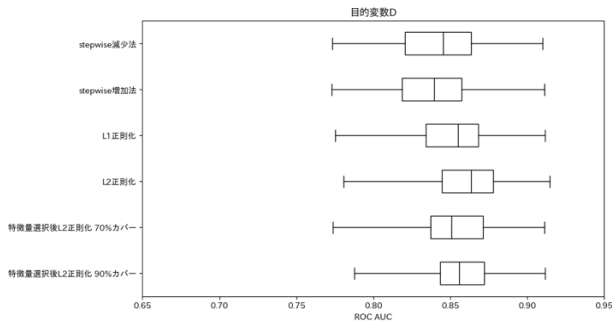


図 14 目的変数 D

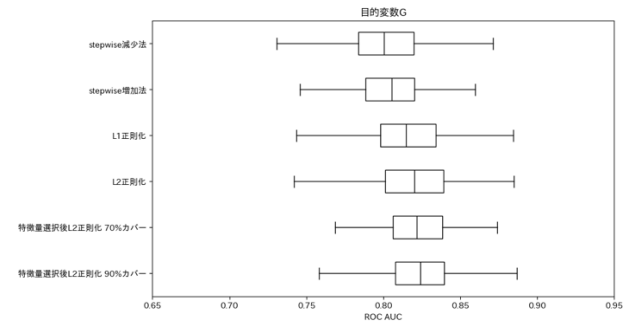


図 15 目的変数 G

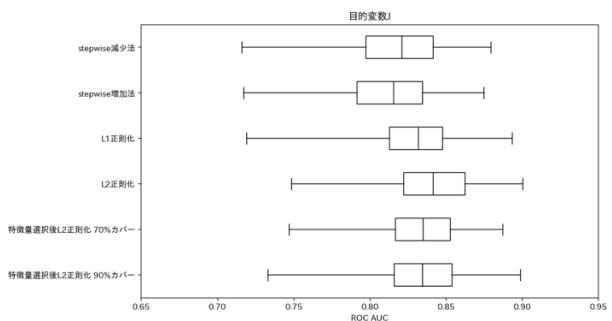


図 16 目的変数 J

### 3.5 選択された特徴量と予測性能

目的変数 11 個で選択された特徴量を調べた。データは学習 80%と評価 20%に分割した。学習・評価の分割は、目的変数それぞれごとに陽性・陰性の割合が等しくなるように層化抽出したものを 100 セット作った。それぞれのセットで採用される特徴量は確率的に決まるため、それぞれ異なってくる。そこで、特徴量(質問)が採用された割合を調べ、特徴量の種類と選択された割合を調べた。表 6 に示した。

表 6 を見ると、9 問が 30%以上の分割で選択されている。逆に言えば、この 9 問を採用すると 70% 近くの分割をカバーできる。9 問の内訳は行動特性 5 問、人口統計学 2 問、未来展望と生活の質が 1 問ずつで、自己効力感含まれていない。更に 10 問採用し、19 問にすれば 90%の分割がカバーできる。分割を広くカバーしているのは行動特性であった。

いずれの分割でも選択されなかったのは、人口統計学 1 問、未来展望 3 問、自己効力感 1 問、生活の質 8 問であった。特に未来展望と生活の質はそれぞれ 1/3 程度の質問がいずれの分割でも採用されなかった。

表 6 選択された質問(説明変数)の種類と数

種類	質問総数	30%以上の 分割で選択	30%未満 10%以上の 分割で選択	10%未満 1%以上の 分割で選択	1%未満の 分割で選択	いずれの 分割でも 選択され なかった
人口統計学	6	2	1	1	0	2
行動特性	9	5	3	0	1	0
未来展望	10	1	0	3	1	5
自己効力感	16	0	1	5	1	9
生活の質	25	1	5	6	3	10
合計	66	9	10	15	6	26

## 4. アプリのパラメータの導出

アプリの説明変数を stepwise の変数増加法で選択した。選択された上位 9 問を使用すると、学習・評価の分割の 70%以上をカバーできることがわかった。9 問に回答するのはアプリの主なターゲットとする高齢者にも容易であり、9 問で診断する機械学習のモデルを作ることにした。

モデルの開発は、アプリで用いているロジスティック回帰のパラメータを求めることである。ロジスティック回帰は、特徴量空間で平面を描き、その表裏で陽性・陰性を分類する。ロジスティック回帰の具体的な推定確率の式は以下である。

$$P_{\text{目的変数}} = \frac{1}{1 + e^{-\lambda}}$$

$$\lambda = \beta_0 + \beta \cdot \text{説明変数}$$

確率 P は変数  $\lambda$  のロジスティック関数で、これを  $\lambda$  について解くと P のロジット関数  $\log(P) - \log(1 - P)$  になる。ロジスティック関数は  $\lambda$  の単調増加関数で、S 字カーブを描くのでシグモイド関数とも呼ばれる。 $\lambda$  が 0 のとき確率 P は 1/2 になり、一般にこれを閾値として陽性・陰性に分類する。 $\lambda$  は説明変数の一次式なので、ロジスティック回帰の分類は、結果として質問ごとにポイント

を割り振って、質問の回答とポイントの線形和が 0 以上か否かで判定しているのと同様である。そのとき用いるポイントはデータを予測し説明するようにフィッティングして決める。ロジスティック回帰ではさらに、分類の決定境界(説明変数の高次元空間での分類の境界の平面)からの距離  $\lambda$  に応じてロジスティック関数で分類の予測確率が得られる。

3 章に示したように L2 正則化を行った場合、ROC AUC が最も大きくなる。そこで、L2 正則化を行って、パラメータを求めた。これは特徴量選択には stepwise 変数増加法を使い、特徴量選択が行われた後の計算には L2 正則化を使うというハイブリッドなものである。求めたパラメータで性能を評価した結果は、既に図 6 から図 16 に示した「特徴量選択後 L2」である。いずれも他の方法とオーバーラップしており、違いは誤差の範囲内であった。

求めたパラメータを表 6 に示した。ここでは各詐欺で最も ROC AUC が高かった問 K, B, C, D のみを示した。また、表 7 で問 1, 問 2, ... と記されている質問の種類と内容を表 8 に示した。問 1 など番号が小さい方が強く効き、番号が大きい方が弱い質問である。また、表 6 の切片が  $\beta_0$ , 問 1, 問 2, ... などが  $\beta$  である。

表 7 のうち、パラメータが正の値を取るものは肯定的な回答を選択すると危険で、負の値は否定的な回答をすると危険なことを示している。つまり、危険なのは相手の話をいい方向に考え、知らない人が訪ねて来ても話を聞き、耳が聞こえにくい、... といった傾向である。

最終的に得られたパラメータでの汎化性能を表 9 に示した。全体的な性能である ROC AUC が平均で 83.5%, 陽性を拾う確率である再現率が平均で 70.5% となった。これは「2.4 アプリの汎化性能の改善」で示した著者による先行研究の「小久保 2023」の ROC AUC が平均で 82.2%, 再現率が平均で 68.9% と分割の誤差の範囲内である。なお、アプリの初版は ROC AUC が平均で 53.3%, 再現率が平均で 0.8% だったので、これに比べると大幅に汎化性能が向上している。

表 7 ロジスティック回帰のパラメータ

詐欺の種類	目的変数	切片	問 1	問 2	問 3	問 4	問 5	問 6	問 7	問 8	問 9
オレオレ詐欺	K	-1.22	0.67	-0.41	-0.19	0.83	0.51	0.38	-0.42	0.33	-0.28
架空請求詐欺	B	-1.02	0.83	-0.41	-0.03	0.67	0.29	0.08	-0.16	0.26	-0.29
還付金等詐欺	C	-1.14	1.03	-0.39	-0.46	1.00	0.52	0.17	-0.39	0.18	-0.14
融資保証金詐欺	D	-0.51	0.79	-0.46	-0.39	0.77	0.32	0.27	-0.31	0.31	-0.21

表 8 表 7 の問 1～9 に対応した質問と危険な方向

番号	種類	質問	危険な方向
問 1	行動特性	相手の話を怪しいと思っても、良い方向に考える	肯定
問 2	行動特性	知らない人が訪ねてきたら、彼らの話を聞かないようにしている	否定
問 3	人口統計学	あなたの年齢を教えてください	若い
問 4	人口統計学	あなたはどの程度耳が聞こえますか	聞こえない
問 5	生活の質	自分は、「不幸な運命に生まれた人間だ」と感じることもある	肯定
問 6	行動特性	知らない人に強い口調で言われると、怯えてしまう	肯定
問 7	未来展望	自分で、「自分の将来の限界が見えている」と思う	否定
問 8	行動特性	自分だけ褒められたり、特別な待遇を受けると嬉しくなる	肯定
問 9	生活の質	自宅には、自分が自由に使える部屋がある	否定

表 9 最終的に得られた推定結果

種類	目的変数	正解率	再現率	ROC AUC
オレオレ詐欺	K	79.5±1.0%	72.2±6.7%	84.4±2.9%
架空請求詐欺	B	78.3±1.2%	67.8±5.9%	80.4±2.9%
還付金等詐欺	C	82.2±1.3%	74.1±7.4%	87.3±3.1%
融資保証金詐欺	D	79.8±1.0%	74.8±5.7%	84.5±2.9%
総合		79.9±1.1%	72.2±6.4%	84.2±2.9%

## 5. まとめ

アプリの初版では、説明変数 66 個、目的変数 12 個の計 78 問の質問に回答する必要があった。アプリが主なターゲットとしていた高齢者にとって 78 問に回答するのは 20 分程度時間がかかり大変であった。目的変数は学習データを収集するためのもので、アプリの初版の予測には説明変数 66 個を使用していた。本研究では、予測性能を落とさずに説明変数を 9 個に減らし、高齢者にも回答しやすいアプリを作ることができるようになった。

説明変数を削減するために、アプリで採用している機械学習の一種のロジスティック回帰で、stepwise の変数増加法・変数減少法、L1・L2 正則化の 4 種類の方法を比較した。説明変数の削減で最も効果的なのは stepwise の変数増加法で、予測性能が最も高いのは L2 正則化であることがわかった。ただし、予測性能の差を評価したところ、機械学習で学習・評価へデータを分割したときの誤差の範囲内であることがわかった。そこで、説明変数の削減に stepwise の変数増加法を用いることにした。学習・評価に分割したデータを 100 パターン作り、パターンの 70%で説明変数に採用された説明変数は 9 問となり、3 分程度で回答できる問題数となった。その場合の予測性能も学習・評価の分割の誤差の範囲内であった。

## 参考文献

- 1) 科学技術振興機構 社会技術研究開発センター. 高齢者の詐欺被害を防ぐしなやかな地域連携モデルの研究開発.  
[https://www.jst.go.jp/ristex/pp/project/h29\\_5.html](https://www.jst.go.jp/ristex/pp/project/h29_5.html) <2024 年 11 月 29 日アクセス>
- 2) 渡部 諭, 岩田 美奈子, 上野 大介, 江口 洋子, 小久保 温, 澁谷 泰秀, 大工 泰裕, & 藤田 卓仙. (2018). 高齢者の詐欺被害を防ぐしなやかな地域連携モデルの研究開発. 秋田県立大学ウェブジャーナル A (地域貢献部門), 5, 64-72.  
<http://id.nii.ac.jp/1180/00000765/>
- 3) 渡部 諭. (2020). 高齢者の特殊詐欺抵抗判定ルールの修正の試み. 国民生活研究, 60(1), 5-28.
- 4) 澁谷 泰秀, 吉野 諒三, 渡部 諭, 角谷 快彦, 藤田 卓仙, 小出 哲彰, 田中 康裕, & 大工 泰裕. (2019). 社会調査データに基づく特殊詐欺脆弱性判定の試み. 日本世論調査協会報 「よろん」, 123, 40-49.  
[https://doi.org/10.18969/yoron.123.0\\_40](https://doi.org/10.18969/yoron.123.0_40)
- 5) 渡部 諭, & 澁谷 泰秀. (2021). 特殊詐欺抵抗判定式改良の試み. 秋田県立大学総合科学研究彙報, (22), 1-6.  
<http://id.nii.ac.jp/1180/00001192/>
- 6) 渡部 諭, & 澁谷 泰秀. (2021). 高速俊約決定木による特殊詐欺抵抗力の判定. データ分析の理論と応用, 10(1), 29-44.  
<https://doi.org/10.32146/bdajcs.10.28>
- 7) 小久保 温. (2023). 詐欺抵抗判定アプリの推定性能の改善. 八戸工業大学紀要, (42), 27-40.  
<https://doi.org/10.32127/0000004114>

## 要 旨

詐欺抵抗診断 Web アプリケーションの初版では 78 問の質問に回答すると、代表的な 4 種類の詐欺に対する抵抗力が機械学習の一種であるロジスティック回帰を用いて推定され表示された。しかし、汎化性能が低く ROC AUC が 53.3%, また再現率が 0.8%で陽性の 99.2%を陰性と予測していた。著者による先行研究で、ROC AUC は 82.2%, 再現率は 68.9%に改善された。

本研究では、特徴量である質問の数を削減するために、ロジスティック回帰の特徴量を選択する stepwise の変数増加法と変数減少法、正則化の L1 と L2 を比較した。質問を削減するには stepwise 変数増加法が有効で、汎化性能を高めるには L2 正則化が有効だった。しかし、汎化性能の違いは誤差の範囲内であることがわかった。stepwise 変数増加法と L2 正則化を組み合わせ、汎化性能を落とさずに 78 問の質問を 9 問に削減することに成功した。

**キーワード:** 機械学習, 特徴量選択, 詐欺脆弱性, Web アプリケーション