

競合他社の不正検知技術比較

国内の主要な後払い・BNPLサービス（Paidy/あと払いペイディ、NP後払い、メルペイ など）における不正検知・AI活用状況を表にまとめると以下ようになる。Paidy は事前登録不要の後払いサービスだが、2020年に発生した二重請求問題を受け、AI顔認証によるeKYCと機械学習を用いた不正検知強化策を導入した^①^②。NP後払い（ネットプロテクションズ）は国内最大手で、2019年にAWS上でSageMakerを活用した機械学習基盤を構築し、与信審査・不正検知モデルを導入して精度向上を図っている^③。メルペイ（メルカリ）も機械学習によるリスクスコアリングやグラフ分析を研究しており、取引属性データをリアルタイムで評価して不正検知を行う仕組みなどを開発している^④。

サービス	不正検知・AI活用の特徴
NP後払い（ネットプロテクションズ）	AWS上でAmazon SageMakerを利用した与信・不正検知モデルを構築。大量の取引データをAIが処理し、学習モデルの推論結果を与信審査・不正判定に反映 ^③ 。
Paidy（あと払いペイディ）	免許証＋顔認証によるeKYCで本人確認を実施 ^① 。さらに不正取引データをAIに反復学習させて検知モデルを継続的にレベルアップし、事前検知の実現を図っている ^② 。
メルペイ（メルカリ）	取引毎の属性データを用いたリアルタイム不正リスク評価システムを開発。Vertex Pipelinesやグラフ分析を活用し、取引属性が更新されるたびにリスク再計算し、事前検知を可能にしている ^④ 。

GMOグループ内での影響

GMOペイメントゲートウェイ（GMO-PG）の決算資料によれば、2024年9月期（FY2024）の連結売上収益は737億円、当期利益は187億円と好調だった^⑤。その中で「金融関連事業」（GMOペイメントサービスが提供する後払い・掛け払いなど）は売上164億円、営業利益41億円と、特に利益面で前年から大幅に伸長している^⑥。同社広報や決算説明会では、GMO-PS（子会社）の後払い事業が計画を上回り増収に寄与したことが報告されている^⑦。また2024年第2四半期時点でGMO-PGグループの累計決済処理件数は約17.7億件、処理高4.6兆円に達しており^⑧、後払いサービスもこの大規模な取引に含まれる（GMO-PSは大手ECサイトで導入が進む）ため、取扱件数・件高の増加に貢献している。以上から、GMO-PSの後払い決済ビジネスはグループ全体の約2割程度の売上規模（164/737億円）を占め、未回収リスク低減によるコスト削減で利益拡大にも貢献しているものと考えられる^⑥^⑦。

AI観点：課題と活用技術

後払い決済データを用いた不正検知モデルの主な課題は、「与信（与信審査）と不正検知の両立」である。具体的には、①**実際に支払いが行われるか**や②**不正な申し込み・利用**を早期に見つける必要がある^⑨。AI技術では、まず**教師あり学習**で大量の取引データを学習し、不正か正常かを判定するモデル（分類器）を構築する。GMOではRandomForestやLightGBMなど決定木系モデルで不正判定モデルを学習させ、高い精度で危険度の高い取引を絞り込んでいる^⑩。さらに、通常とは異なるパターンを検出する**異常検知（アンラベールドモデル）**も併用し、新たな不正パターン発生時にも反応できる仕組みを構築している^⑩。近年では、**ネットワーク分析**（グラフアルゴリズム）も活発に研究されており、メルペイなどではアカウント間の関連性や取引フローをグラフ化して集合的・組織的な不正を検知する手法が示されている^④。また、GMO-PGでは支

払遅延リスク予測のために時系列データをXGBoostに学習させる取り組みも進められており、類似取引検索にLLMを活用する研究など多方面でAI技術を活用している ¹⁰ ⁴。

代表的なモデルと手法

後払い決済不正検知で使われる機械学習モデルには、大きく**教師あり学習モデル**と**異常検知モデル**がある。表に代表例を示す。

モデル名	種類	特徴・用途
Random Forest	教師あり（木）	複数の決定木を組み合わせで予測。欠損値やスケール変換に強い。GMOでも不正判定モデルに活用 ¹⁰ 。
XGBoost / LightGBM / CatBoost	教師あり（勾配ブースティング木）	競合優勝ソリューションで多用される高速・高精度な手法 ¹¹ 。大量データに対するスケーラビリティに優れ、特徴量エンジニアリング後の学習に強い。
AutoEncoder (NN)	教師なし（深層学習）	正常データの自己再構成を学習し再構成誤差で異常を検出。不正パターンが稀な場合に活用。
グラフニューラルネットワーク (GNN)	グラフベース（深層学習）	ユーザ・アカウント間のネットワーク構造を学習。不正グループや組織的手法の検出に有効。

ワークフロー例: 取引履歴・ユーザ情報など多様な特徴量を収集・前処理し（特徴量エンジニアリング）、訓練データ（過去の正常取引・不正取引）でモデル学習。クロスバリデーションで性能評価（ROC-AUCなど）し、実運用では新規取引データにモデルを適用してスコアリングし、閾値超でアラート化。定期的にモデル再学習・検証を行い、不正の変化に対応する。近年のコンペティションや実装では、これらのモデルをアンサンブルして高精度化する例が多い ¹¹。

不正検知に使われるデータタイプ

後払い決済不正検知では多岐にわたるデータが利用される。主なデータタイプを整理すると、例えば以下が挙げられる。

- ・**取引データ:** 購入金額、商品カテゴリ、支払い方法、利用時刻・日付など。過去取引の履歴や累計利用額も含む。
- ・**ユーザ属性:** 会員登録日、年齢・居住地などの基本情報、過去の信用情報（未払い履歴や与信スコア）、会員の利用頻度や傾向。
- ・**デバイス情報:** 使用デバイスID・IPアドレス・ブラウザやOS情報、端末登録情報など。不正者が使うデバイスと正常利用者の違いを検知するのに重要。
- ・**時間情報:** 取引の日時、頻度、一定期間内の取引間隔など。通常と異なる時間帯やペースは異常指標となる。
- ・**ネットワーク情報:** 同一住所・電話番号・ログイン情報などでつながる複数アカウントの関係性、取引相関ネットワーク。共通要素を持つ複数の取引で不正グループを検出できる。

これらを組み合わせて特徴量化し、不正検知モデルは学習・予測に活用する。

代表的なKaggleコンペ事例

類似課題としてKaggleの不正検知コンペが参考になる。代表例の「IEEE-CIS Fraud Detection」では、実際のEC取引データの各レコードに対し、二値変数 `isFraud`（不正かどうか）の予測を行うタスクであった ¹²。

評価指標は**ROC-AUC**であり¹³、これは適合率・再現率に依存せずモデルの識別力を測る指標である。上位チームのソリューションではXGBoost/LightGBM/CatBoostなどの勾配ブースティングモデルを組み合わせ、特徴量エンジニアリングを徹底的に行ったアンサンブルが多く使われていた¹¹。たとえば優勝チームはXGBoostを基幹に、CatBoostやLightGBMとアンサンブルして最終的に高いAUCスコアを達成している¹¹。この他にも、別のデータセットを用いたクレジットカード不正検知コンペなどで、同様に決定木系モデルや異常検知アルゴリズムが用いられており、手法や評価方法の議論が行われている。これら事例では**教師あり学習の分類**アプローチが主流である点も参考になる。

参考文献: GMO-PG／GMO-PS各種資料・決算説明会資料⁹¹⁰⁸⁷、各社プレスリリース・技術ブログ³¹²⁴¹²¹³¹¹。

¹ ² PaidyがAI顔認証導入による不正利用防止の取り組みを発表 | 家電Biz

<https://kadenbiz.com/2020/03/13/paidy-introduces-ai-face-recognition/>

³ ネットプロテクションズの後払い決済と信審査システム、ISIDがシステム・データ分析基盤をAWS上に構築支援 - New Retail Navi

<https://newretailnavi.com/archives/90883>

⁴ Accelerating Fraud Detection Using Data on Fraud Risk of Potential Transactions / 発生可能な取引の属性データを用いた素早い不正検知 - Speaker Deck

<https://speakerdeck.com/mercari/fa-sheng-ke-neng-naqu-yin-noshu-xing-detawoyong-itasu-zao-ibu-zheng-jian-zhi>

⁵ ⁶ GMOペイメントゲートウェイの決算内容を3分で解説！ | マサキタカオ

<https://note.com/ohbos/n/n3a0146f99aa0>

⁷ ⁸ GMO-PG、対面、非対面などグループ総合力発揮で計画上回る進捗 | ペイメントナビ

<https://paymentnavi.com/paymentnews/145333.html>

⁹ ¹⁰ AIを活用し審査精度を飛躍的に向上一データアナリストが明かす「決済業界」のおもしろさ | あなたのとなりに、決済を

<https://www.gmo-pg.com/blog/articles/article-0151/>

¹¹ ¹² ¹³ Leveraging Machine Learning to Detect Fraud: Tips to Developing a Winning Kaggle Solution | NVIDIA Technical Blog

<https://developer.nvidia.com/blog/leveraging-machine-learning-to-detect-fraud-tips-to-developing-a-winning-kaggle-solution/>