検出から防止へ、ハイテクに精通した犯罪者に対処する

デジタル詐欺とその管理にかかるコストと複雑さは急増しています。消費者がデジタルやモバイルチャネルでのやり取りを増やすにつれて、犯罪者はこれらのチャネルを悪用する新しい戦略を素早く開発しました。リアルタイム決済の登場で、損失はあっという間に発生し、その損失を回復することは難しくなっています。

COVID-19 は、消費者のデジタルチャネル利用をさらに加速させ、犯罪者もそれに追随しています。顧客は、急速に進化するデジタル行動に対応した、シームレスで保護された体験を期待しています。コストの増大により、不正行為による損失と不正行為管理のコストを抑制することが求められています。また、規制当局は、銀行に迅速な対応を求める圧力を強めています。これらの要因により、不正行為の検知と防止が最重要課題となり、金融サービス業界にとって最優先事項となっています。

企業が技術に長けた犯罪者を出し抜き、損失を防止し、優れた顧客体験を提供するには、次のような方法でデジタル詐欺に対処する必要があります。

- **傾聴 :** トランザクションごとに、コンテキストに応じたビューを構築
- **把握 :** 顧客行動が示す詐欺のリスク
- **判断 :** 介入の要否と、介入を要する場合の重大度
- **行動 :** リアルタイムでの介入またはトランザクションの許可

現在の不正防止ソリューションの課題

不正行為の影響とコストが増大しているにもかかわらず、現在のソリューションでは、不正に対抗するには不十分です。これらのソリューションは、犯罪者が検知を逃れるために使用する急速に進化する戦略に追いつくために必要な高度な機能を備えていません。

- **現在の不正防止ソリューションは、生体認証機能が限られています。**ベンダーは、自社のソリューションがデジタル詐欺を防止すると言えるように、急ピッチで不正防止ソリューションに生体認証のサポートを追加しています。しかし、これらの統合は、データ収集機能と分析機能が限定的です。サポートしているといっても、不正を防ぐための処理能力がありません。
- **ほとんどの不正防止ソリューションは閉じたシステムで、データを所有していません。**代わりに、ベンダーは生体認証データを収集して、顧客のトランザクションアクティビティに簡単にリンクできない閉じたまたは匿名化されたクラウドリポジトリに保存します。しかし、不正と戦うには、まずすべてのデータを結合する必要があります。そのため、データを所有する必要があるのです。
- **現在の不正行為対策は十分なスピードで実行されていません。**不正は１つのモデルで止めることはできません。何千ものモデルが必要なのです。そのため、不正行為との戦いは、常に新しい不正手法と新しい不正モデルとの戦いなのです。従来の不正防止ソリューションは、このようなモデルを構築し、稼働させるために必要な量の詳細データを取得、保存、処理する能力を備えていません。

デジタル詐欺の状況

詐欺件数の増加率 **91%**（**2020 年** [1]）

5% アカウント乗っ取り攻撃がデジタルトラフィック全体に占める割合 [2]

2060 億ドル 2021 年～ 2025 年に予測されるオンライン詐欺での損失額 [3]

1 Scam Advisor「The Global State of Scams 2021」

2 Arkose Labs「How Cybercriminals Hack into a Digital Account in a Few Easy Steps」

3 Juniper Research「Online Payment Fraud Losses to Exceed $206 Billion Over the Next Five Years; Driven by Identity Fraud」

celebrus FRAUD DATA PLATFORM | teradata.

テクノロジーに精通した犯罪者と積極的に戦うために、組織は取引や行動を限定的にしか把握できない反応型、検知中心の不正防止ソリューションから脱却しなければなりません。不正防止管理の未来は、コンテキストドリブンで防止中心の、ミリ秒単位で意思決定ができるソリューションにあるのです。

不正防止をアクティブ化するための 4 つのステップ

不正をストップさせるためには、次のことができなければなりません。

1. **傾聴：**コンテキストによるビューをトランザクションごとに構築し、ユーザーがどのようにデジタルチャネル内でナビゲーション、移動、インタラクションをするかを記述したトランザクションとデジタルの行動についての情報を結合。
2. **把握：**リアルタイムでハイパーパーソナライズされた AI とマシンラーニングモデルを適用して、不正行為者と各ユーザーの本物の活動のプロファイルを作成し、不正行為者をリアルタイムでブロックしながら本物の活動を認識・許可することにより、不正リスクを把握。
3. **決定：**介入が必要かどうかを判断し、介入が必要な場合は必要な介入の重大度を判断することで、損失の最小化、顧客体験の最大化、不正管理のコスト低減のトレードオフを最適化。
4. **行動：**介入をリアルタイムで実行して不正を防止、真正であると評価された場合はトランザクションの進行を許可。

不正防止のための介入戦略

不正である確率	戦略	介入方法
95%	ハード介入	ユーザーセッションを終了、支払いをブロック、不正防止のための介入を推奨
70 ～ 95%	ソフト介入	二段階認証によるユーザー再検証を要求
50 ～ 70%	手動認証	顧客に警告メッセージを送信し、さらなる調査でフォローアップ

検出からコンテキストに合った防止への切り替え

コンテキストは、不正の検出と防止に重要です。顧客のトランザクションや行動バイオメトリクスの分析は、単独で実行することはできません。不正行為を迅速に検知し、防止するために、取引が行われている環境を理解する必要があります。これには、顧客がどこにいるか、いつ活動しているか、どのようにやりとりしているか、何を見ているか、使用しているデバイスなどが含まれ、過去と現在の取引データを考慮しながら行います。

そのため、不正行為に積極的に対抗するには、データが多ければ良いというものではありません。不正行為を未然に防ぐには、取引データや行動データを含むすべての関連データをリアルタイムで有効化し、不正行為の検出と防止を強化するソリューションが必要です。

将来を見据えた不正防止ソリューションに必要な 5 つの重要な機能：

1. **トランザクションとインタラクションを結合：**従来のトランザクションによる情報と、デジタルインタラクションを記述した新しいデータとを合わせることで、コンテクストによるインテリジェンスが得られ、不正な行動の検出を含め、豊富なインサイトが導出できます。
2. **ID をマッチングして顧客を検出：**顧客はチャネル間を流動的に移動し、顧客データをキャプチャするシステムは多数にわたり形式も異なるので、顧客プロファイルをマッチングしてリンクする能力が要求されます。
3. **何百万ものモデルによるハイパーパーソナライゼーションを実現：**パーソナライズド AI やマシンラーニングモデルを顧客ごとにトレーニングして導入することで、インタラクションが真正なものか、悪者が生成したものか、より正確に検出できるようになります。
4. **リアルタイムのアクションで介入を発動：**応答時間がリアルタイムなら、不正を検出するだけでなく、介入を発動して損失を防止することも可能です。
5. **絶えず学習し進化：**人工知能（AI）とマシンラーニングのメソッドを活用して、ユーザーの行動についてのトレーニングを絶えず行っていれば、新種の不正戦術が出現し次第検出する能力が得られます。

Celebrus と Teradata なら大規模な不正防止が可能

検知を中心とした現在の不正防止ソリューションの限界を超える、新たな不正防止方法があります。Celebrus と Teradata は、企業が真正顧客と悪質業者の両方をプロファイリングできるソリューションを提供します。真正な顧客は認識され、取引を継続することができるため、シームレスで安全な顧客体験を実現し、不正行為者はリアルタイムでブロックされます。

Celebrus と Teradata は次のようなことを可能にします：

- **不正による損失を低減：**不正行為にリアルタイムで介入
- **擬陽性を抑制：**不正行為を阻止し、真正なトランザクションは止めない、これだけでも顧客体験は向上
- **顧客体験を向上：**プロアクティブに介入することで、危険にさらされている顧客を保護
- **オーバーヘッドをなくして効率性を向上：**不正調査の件数を低減して事例管理を軽減するのに加え、調査をシンプル化するインサイトを提供
- **進化する脅威に対処：**新種の詐欺と新しい詐欺手口を先取りし、迅速に対応

このファーストパーティメソッドでのデータ収集に、タグ管理や複雑なデータレイヤーは不要です。1行のコードを使用してデジタルチャネルからのすべてのインタラクションを取得し、このデータを Teradata Vantage™ にプッシュして、事前に構築された不正防止データモデルに格納します。データは企業資産として作成・保存され、多くのユースケースで複数の成果を提供できるようになっているため、データのコピーを取得するための作業は必要ありません。

意思決定をサポートするためのデータの収集、処理、配信はすべてリアルタイムで行われ、迅速な不正介入対応と最適な顧客体験が形成されます。また、コネクターと API により、必要に応じてデータのサブセットを送信し、安全かつコンプライアンスに準拠した方法で介入や承認を行うことができます。

導入事例：犯罪者に一歩先んじて顧客を保護

課題

世界のトップ5に入るある銀行は、COVID により15%増加した遠隔操作ウィルス（RAT）詐欺に頭を悩ませていました。1か月あたりの詐欺件数は 2,000 件超、1件あたりの損失額は約 2,700 ドルになっていました。

損失が膨らみ、規制当局からの圧力も強まっていたため、その銀行は行動を急ぐ必要がありました。その銀行では、不正を検出して損失を発生前に防止するリアルタイムのソリューションを必要としていました。

ソリューション

Celebrus と Teradata Vantage の導入後、銀行は、不正行為の防止、顧客体験の向上、損失の削減、業務効率の改善を実現する、超パーソナライズされた行動不正ソリューションを確立することができました。

- デジタルインタラクションをリアルタイムで取得
- トランザクションパターンと行動パターンのデータを分析
- 何百万ものマイクロモデルを実行して行動を評価
- インサイトを応答時間1秒以内で展開

結果

25 万件
1時間あたりの一意のカスタマージャーニー（ピーク時）

70%
詐欺の事例で検出して防止できるようになった割合

1 億ドル
防止できる詐欺で検出された分の金額

celebrus FRAUD DATA PLATFORM | teradata.

Celebrus とテラデータで不正防止の可能性を最大限に引き出す

テラデータは、エンタープライズアナリティクスのためのコネクテッド・マルチクラウド・データプラットフォームを提供するクラウドリーダーとして、毎年、業界の専門家に評価されています。テラデータは Celebrus とのパートナーシップで、組織が不正防止を大規模にリアルタイムで行えるようにしています。

- Celebrus では、インタラクションからのきめ細かいデータを収集し、すべてのデジタルチャネルにわたってユーザーを特定します。
- あらかじめ構築された広範な Teradata Vantage 顧客体験データモデルは、Celebrus からほぼリアルタイムでデータを取得し整理します。
- 強力な Teradata Vantage 分析エンジンは、何百万ものハイパーパーソナライズされた AI およびマシンラーニングモデルを顧客レベルでトレーニングし、これらのモデルをリアルタイムで適用してデジタルジャーニーをリスクスコア化します。
- Teradata Vantage のリアルタイム機能では、ユーザーがデジタルチャネルにつながっている間、不正を防止するためのコンテキストによる意思決定とアクションが可能になります。
- このソリューションは、規制要件を満たせるよう、完全なデータ系統とモデルの説明可能性をサポートします。

デジタル詐欺は進化する一方です。Celebrus とテラデータが、企業はテクノロジーに精通した犯罪者の数歩先を行き、詐欺の損失を減らし、詐欺の管理コストを削減しながら、顧客体験を向上させることができるのです。

Celebrus について

Celebrus は、世界で唯一のファーストパーティ、リアルタイム、エンタープライズクラスのデータキャプチャ / コンテキスト化ソリューションであり、どのオンライン顧客でも、世界トップクラスのデジタル体験を創出して、大幅な節約とオンライン収益の増加を実現します。詳しくは、**Celebrus.com** をご覧ください。

テラデータについて

テラデータは、コネクテッド・マルチクラウド・データプラットフォームを提供する企業です。テラデータの企業向けアナリティクスはあらゆるビジネスの課題を解決します。将来の大規模かつ混在するデータワークロードを今日から扱える柔軟性を提供するのはテラデータのみです。Teradata Vantage のアーキテクチャは、クラウドネイティブで、As-a-Service で提供され、オープンなエコシステム上に構築されています。これらの設計上の特徴により、Vantage は、マルチクラウド環境における価格パフォーマンスを最適化するための理想的なプラットフォームとなっています。詳しくは、**Teradata.jp** をご覧ください。

17095 Via Del Campo, San Diego, CA 92127 Teradata.jp

celebrus FRAUD DATA PLATFORM | teradata.