Cybersource+ 専門家：
2022年版不正行為の動向編

不正行為の未来

変化する世界の中で、成長を確保するために

cybersource
A Visa Solution

目次

変化する世界では、何にでも対応できることが重要

この数年間は、他では経験したことのないような日々でした。世界中の企業は、eコマースの急増、消費者や不正行為者の行動の絶え間ない変化、政府や規制当局の要求の進化によってもたらされた新しい機会に素早く適応し、驚くべき回復力を見せています。

あとは次の準備です。

私たちは、Merchant Risk Council (MRC)、Aite-Novarica、Cybersourceの専門家チームを集め、不正行為の未来についての洞察を共有し、不正行為を減らすだけでなく、より多くのビジネスをもたらすことができる戦略を策定するお手伝いをしました。

詳細：

1 パンデミックによって不正行為はどう変わったか

2 自動化された不正行為者の台頭

3 気をつけるべき不正行為の傾向とは

4 不正防止戦略をスタートさせるための4つのステップ

専門家の紹介

Tracy Kobeda Brown

マーチャントリスクカウンシル（MRC）プログラム&テクノロジー担当副社長

トレイシーは、スタートアップからフォーチュン500社まで、幅広い分野で活躍する経験豊かな経営者です。彼女は技術戦略、製品設計、エンゲージメント、ゲーム、モバイル、情報セキュリティなど、幅広いスキルを持っています。

余暇にはビデオゲームをしたり、起業のコーチや経営者の相談相手としてボランティア活動をしています。オプラに会ったこともある彼女の夢は、動物保護区の開設、本の執筆、法執行機関のための新しいテクノロジーソリューションの構築です。

David Mattei

戦略アドバイザー、Aite-Novarica Group

デビッドは、決済業界で15年以上の経験を持ち、不正行為や紛争に関するシステムの設計、構築、立ち上げに携わってきました。彼は加盟店や金融機関などを顧客としているため、独自の総合的な視点で課題を把握することができます。

デビッドの夢は、ヨーロッパへの片道切符を買って、すべての観光地を見て回り、やり遂げたと思ったら帰国することです。祖母の生家であるイタリア村の家も買いたいと考えています。

Mari-anne Bayliss

Cybersource 欧州地域ソリューション担当シニアディレクター

マリアンヌはヨーロッパの加盟店と協力して、地域のトレンドを理解し、商品開発に反映させるようにしています。英国の大手小売業で不正防止に携わった20年の経験を生かし、現在の職務に就いています。

仕事以外では、家族や友人のために料理を作ることが、彼女のリラックス方法です。彼女はThe Great British Bake Offに参加することを夢見る、情熱的なパン職人です。

Martin Lee

Cybersource マネージド・リスク・サービス、APAC担当ディレクター

15年以上の不正防止経験を持つマーティンは、アジア太平洋地域の専門家チームを率いています。このチームは、Cybersourceのリスクソリューションを利用するクライアントに代わって、不正防止戦略を管理する役割を担っています。

シンガポール在住、イギリス出身のマーティンは大のサッカー好きで、週末はほとんど深夜の試合を楽しんでいます。

Mark Strachan

Cybersource グローバルサービス担当ディレクター

マークは、決済・銀行業界で12年以上の経験を持つ、不正リスクのプロフェッショナルです。小売、デジタル、チケット販売などの分野の加盟店と連携し、不正行為に関連するリスクを低減するための戦略を策定しています。

仕事以外の時間は、新天地への旅行や山歩き、自宅での料理、演劇に興じています。

1 パンデミックにより不正行為が変化

「eコマースの売上高の伸びには驚かされます。2021年を見ると、eコマースの売上は世界的に大きく伸びています。パンデミックがなければ、世界のeコマース売上が今の水準に達するには何年もかかったはずです」

David Mattei
Aite-Novarica 戦略アドバイザー

パンデミック関連の規制により、ネット通販の売上が急増しました。しかし、これによって必然的に加盟店に対する不正攻撃が世界的に増加することになりました。最近の調査では、約4分の3の加盟店が、パンデミック発生前と比較して、不正行為の試行回数と売上高別の不正行為の割合の両方が増加していると報告しています[1]。

したがって、10社中9社の企業が、eコマースにおける不正行為の管理を、自社の戦略全体にとって非常に重要、あるいは極めて重要であると考えているのは、当然のことでしょう[2]。

消費者心理の変化

eコマースを初めて利用する消費者は、潜在的なリスクについて知らない、あるいは準備できていない可能性があります。デジタル化に伴い、不正行為者は新たな犯罪の手口を発見しました。

ソーシャルメディアは多くの人にとって新たな遊び場となり、わずか12ヶ月で5億人以上のユーザーがソーシャルメディアに参加しました[3]。オンライン詐欺のリスクについての啓蒙活動にも力が注がれていますが、ソーシャルチャネルでは個人情報を簡単に共有できるため、不正行為者はこのような行為に飛びつきました。

不正行為者がソーシャルメディアを利用して個人情報を盗む方法については、第2章を参照してください。

また、消費者主導の詐欺行為、つまりフレンドリー（一人称）詐欺の増加も重要な出来事でした。加盟店が2021年中に経験した最も一般的なタイプの不正攻撃は、2019年[4]は5位だったフレンドリー詐欺でした。受け入れたeコマース注文の約1.2%がフレンドリー詐欺であることが判明したと推定しています[5]。

第3章では、フレンドリー詐欺と、類似のタイプの詐欺であるポリシーの悪用について紹介しています。

1 「2021年版グローバル不正レポート」Cybersource、MRC、2021年、p7
2 「2021年版グローバル不正レポート」Cybersource、MRC、2021年、p6
3 「昨年、5億人のユーザーがソーシャルに参加した（その他の事実）」hootsuite.com、2021年7月
4 「2021年版グローバル不正レポート」Cybersource、MRC、2021年、p17
5 「2021年版グローバル不正レポート」Cybersource、MRC、2021年、p17

加盟店の適応

パンデミック時には、チームメンバーが在宅勤務や一時帰休を余儀なくされ、多くの不正対策チームがプレッシャーにさらされました。同時に、注文量の増加に伴い、不正対策チームのリソースはしばしば制限されることになりました。

加盟店にとっては、まるで繁忙期が延長されたような体験でした。その期間、ピークシーズンのレベルで不正対策チームの人員を確保するのに苦労しました。お客様の満足度を高めるために、従来なら断られていた注文を通すこともあります。つまり、収益が増加しても、不正行為の発生率も同様に増加した可能性があるのです。

フリクションのない流れ

パンデミックでは、フリクションのない体験がこれまで以上に重要になりました。特に、オンラインで購入し、店頭で受け取る（BOPIS）場合や、カーブサイドピックアップでの購入でこれは顕著で、顧客は迅速な対応を期待しています。1～2時間以内に商品を受け取ることができれば、注文を承認するか拒否するかを決定する前に検討する時間がなく、ビジネスにおける不正のリスクを高める可能性があります。

「パンデミックによって、不正行為に関して加盟店が歴史的に知っていたことが覆されました。例えば、フレンドリー詐欺の量は、以前加盟店が受けていた攻撃のやり方ではないので、審査や確認のスタイルを変えなければならなかったのです」

Tracy Kobeda Brown
プログラム＆テクノロジー担当副社長
MRC

パンデミック以前の店舗では、自動審査に加え、IDチェックや決済カードの照合など、受け取り時の物理的なセキュリティ対策が併用されていました。

現在では、機械学習による検出の自動化、グローバルなネガティブリスト、複数の受け取り場所を1つのIDにリンクさせるなどのより高度な多変数速度などを組み合わせて、注文の受け取り段階の前に異常を発見するために不正スクリーニングを使用する加盟店が見られます。

そこで、第4章で紹介する不正管理へのレイヤーアプローチが威力を発揮します。

「一部の小売企業が経験した収益争いは、不正行為を防止することを自らの役割と考える不正管理者と、収益を上げるための責任者との間の「綱引き」を引き起こしました。より多くの収益と引き換えに、どれだけのリスクを受け入れることができるのか？ということです」

Mari-anne Bayliss
欧州地域ソリューション担当シニアディレクター
Cybersource

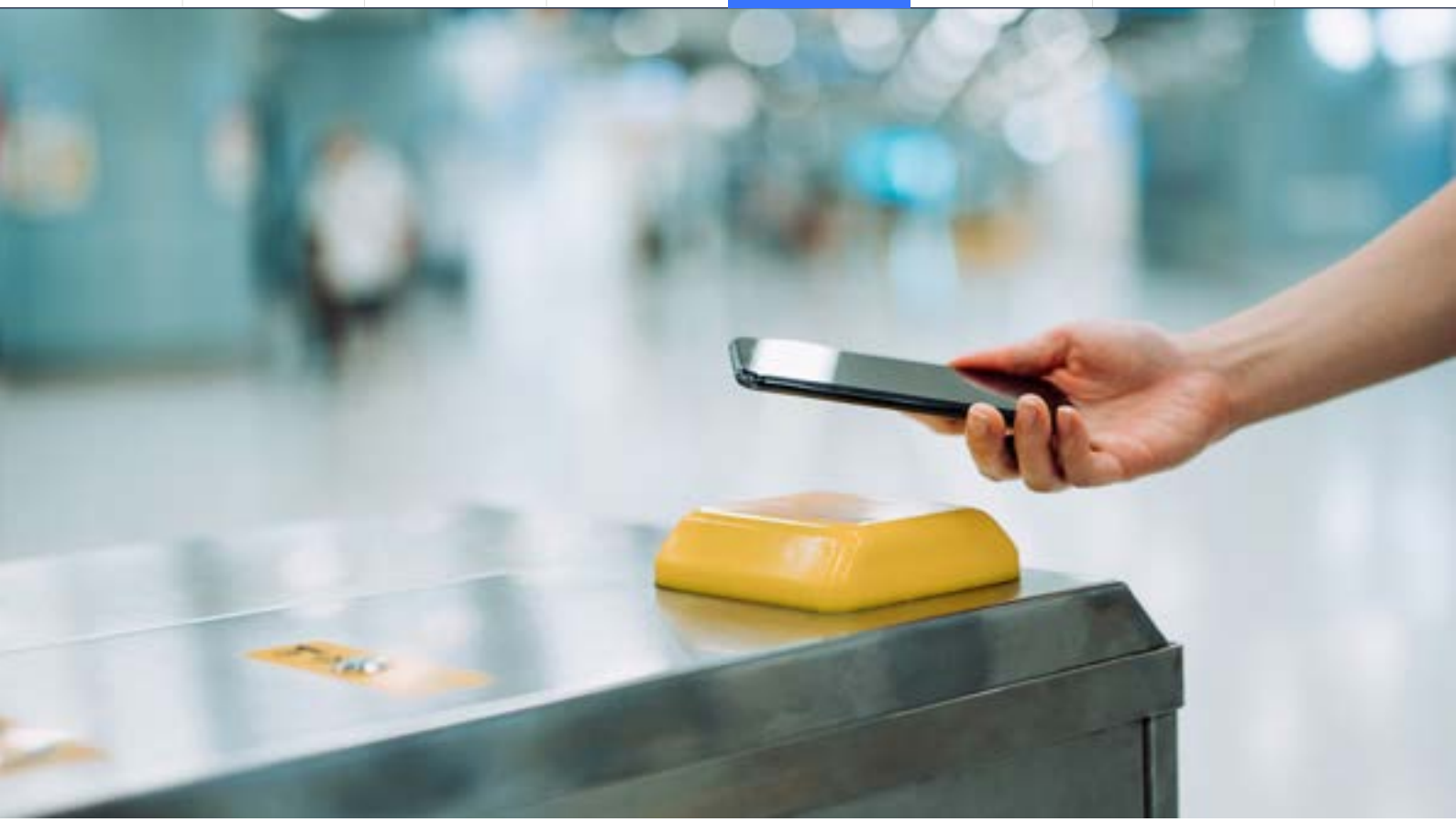
不正行為者が歩調を合わせる

パンデミックが始まる前から、新しいタイプの不正行為者が出現していました。組織化され、自動化され、単独よりもグループや集団の一部として活動する可能性が高いのです。

- **その焦点は、支払い時の詐欺から、個人情報全体を盗むことに移っています。**より多くの消費者がデジタル化する中、不正行為者はその脆弱性を利用し、本物、偽物、または合成のIDを使用して全く新しいアカウントを設定するためのデータを盗むことに成功しています。
- **不正行為者は、進化するフルフィルメントスタイルを利用して、不正対応ツールを回避するために素早く行動しています。**例えば、配送先が把握されていないBOPISや、フレンドリー詐欺に見せかけた不正転売行為などです。

キーメッセージは？

支払い以外のリスクも管理し、アカウントの作成から商品の配送または受領、さらには返品に至るまで、エンドツーエンドのプロセスを検討します。どこにリスクがあるかを検証し、弱点に対処して、最適な顧客体験を維持します。



2 自動化された不正行為者の台頭

個人情報の盗難とデータの漏洩は、サイバー犯罪の最大の原動力の一つとなっています。なぜなら、個人情報を盗むことは、詐欺の攻撃だけよりもはるかに大きな価値があることを不正行為者が知ったからです。不正行為者の従来の手口はもはや十分ではありません。過去には、盗んだ支払情報を何週間も使用できることが一般的でしたが、もはやそのような贅沢は許されないのです。オンラインバンキングやモバイルバンキングのアプリでは、口座は1日に数回チェックされるため、盗まれた情報は数時間しか使えない場合があります。

今日の不正行為者は、数週間使用可能な「クリーン」なアカウントを設定するために、IDデータを盗んでいます。私たちが発見しているのは：

- **個人情報の盗難**や偽のアカウントを作成するための洗練されたアプローチ。
- **自動化の進展：**不正行為者は、ボット、チャットボット、CAPTCHA回避技術、さらには人間のクリックファームなどの最新技術を取り入れ、新たな脆弱性を見つけるとすぐに攻撃するようになりました[6]。
- **見え隠れする不正行為：**また、ダークウェブから離れ、ソーシャルメディアに直接技術や手口を持ち込む不正行為者もいます。

6 「サイバーセキュリティへの警告：ハッカーが自動化を利用して攻撃を強化する10の方法」ZDNet、2020年3月

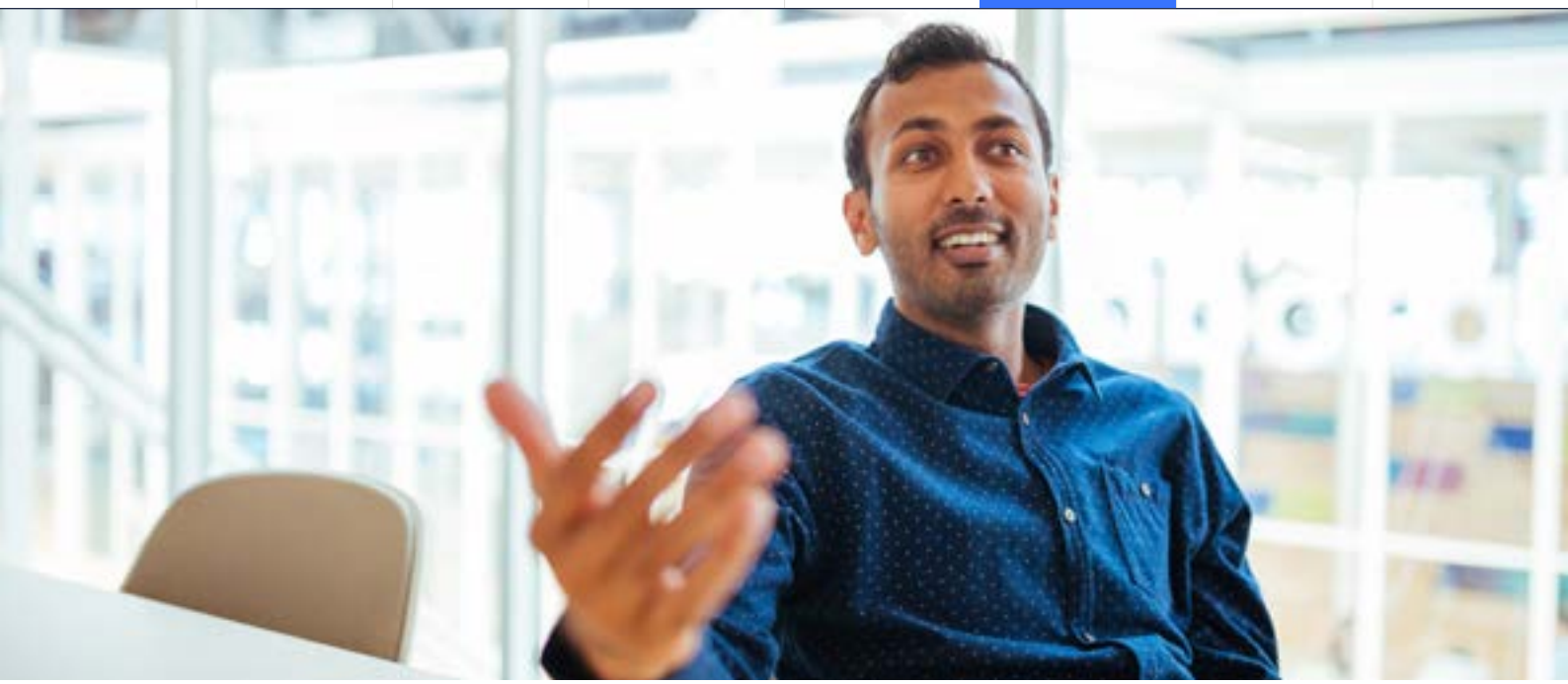
スポットライト：**ソーシャルメディアを使用したIDの盗難**

不正行為者は、ハッキングやソーシャルエンジニアリング、大規模なデータ侵害など、さまざまな手段で個人情報を盗み出そうとします。パンデミック発生以降、ソーシャルメディアは新たなユーザーを次々と獲得し、肥沃な土壌となりました。

ソーシャルメディアユーザーの行為：

- **情報をアカウントに掲載する**（氏名、生年月日、居住地や勤務先の写真など）
- **不正行為者が友人や家族をトロールして**母親の旧姓を簡単に収集できるようにする
- **一見無害に見えるが、**実はそうでないポップアップクイズに答える。例えば、「あなたが生まれたときに1位だった曲はどれですか」と尋ねれば、生まれた年や月が判明します。生年月日と組み合わせることで、このフィッシング詐欺はあなたの生年月日を明らかにしたのです
- **新しい連絡先を装って、**好きなスポーツや初めて飼ったペットの名前などの個人的な質問をする不正行為者に対応する（パスワードを忘れたときのヒントとしてよく使われる）

不正行為者がわずかな労力で取得することができるこれらの情報があれば、顧客のオンラインアカウントにアクセスしたり、他のウェブサイトで不正に使用するための完全な顧客IDを構築したりすることが可能です。



3 注目ポイント

来年は不正行為者が特に活動しそうな分野がいくつもあり、警戒が必要です。

アカウント乗っ取りとロイヤルティ詐欺が懸念される理由

新規アカウント開設詐欺、偽装IDを使った新規アカウント詐欺、アカウント乗っ取り詐欺（不正行為者が顧客のアカウントデータに不正にアクセスし、操作すること）は、いずれも依然として重要な問題です。個人を特定できる情報（PII）を含む数百万件の記録が漏洩するデータ漏洩は、不正行為者がデジタルアカウントを攻撃するための餌となります。

アカウント乗っ取りを防止することは、モニタリングの重要な部分を形成し、次の理解を深めるのに役立ちます。

- 新規にオンラインアカウントを作成しているのは誰か
- 既存のアカウントにログインしているのは誰か
- パスワードや配送先住所など、重要なアカウント情報を改ざんしようとしているのは誰か

情報漏えいやその他のなりすましは、不正行為者が既存のアカウントにアクセスするための正しいユーザー名とパスワード、または新しいアカウントを設定するための説得力のあるデータの組み合わせを入手できることを意味します。不正防止ソリューションがアカウントイベントを調査し、本物のアカウントへのアクセスや作成の可能性を判断できるようにしましょう。

「最近見受けられる攻撃経路の中には、古いものに新しい工夫を加えたものもあります。例えば、新しいアカウント不正では、特定の人物に関係しない偽のアカウントを作成し、将来的に使用できるように仕込まれています」

David Mattei
Aite-Novarica 戦略アドバイザー

ロイヤルティ詐欺は増加傾向にあり、特に旅行業や接客業で問題になっています。最近、旅行に行く機会が少なくなっている人が多いと思います。不正行為者は、私たちが旅行をしていなければ、航空会社やホテルのポイントプログラムを以前ほど頻繁にチェックしていないという事実を当てにしています。不正行為者がこれらのアカウントに侵入すると、ポイントをすぐにお金に換えることができます。

不正なアカウント作成や乗っ取りからビジネスや顧客を守るツールは、ロイヤルティプログラムの不正使用からも守る必要があります。

「最近まで、旅行規制があったため、不正行為者はポイントを盗んで利用することにほとんどメリットを感じていませんでした。しかし、旅行ができるようになると、それを利用しようとします。アカウント乗っ取りを防ぐための技術を駆使するだけでなく、アカウントを監視することの重要性をお客様に伝えることが重要です」

Mark Strachan
Cybersource グローバルサービス担当ディレクター

決済詐欺に利用される3種類のデータ盗難

私たちは、このようなデータ盗難に優先的に対処することをお勧めします。いずれも、最近のアカウント乗っ取り攻撃の特徴であるカードテストやクレデンシャルスタッフィングにオンラインで利用することが可能です。

1 悪意のあるアクセス権を利用してデータを盗み出す

不正行為者は、ブルートフォース攻撃からフィッシング、スミッシング、マルウェアに至るまで、データへの悪意あるアクセスを得るための手法を長年にわたって使用してきました。

このような攻撃の増加だけでなく[7]、在宅勤務者の増加を利用した詐欺も発生しています。メールアドレスを偽装して管理職や役員になりすまし、従業員からネットワークにアクセスするための認証情報を聞き出し、データを盗み出そうとする手口です。

2 休眠アカウント：長い目で見る

2020年初めに発生した情報漏えい事件では、パンデミックの発生と同時に不正行為者が新しいオンラインアカウントを設定することができました。彼らは、初めてネットショッピングをする本物の顧客が設定した大量の新規アカウントの中に紛れ込んでいたのです。

多くの場合、不正行為者は、古いアカウントで行われた取引は詐欺のスクリーニングを受ける可能性が低いという前提で、ずっと後までそれらのアカウントを使用しなかったのです。高度な不正対応ツールは、このようなアカウントを特定し、ブロックすることができます。

3 強力な顧客認証の導入でSIMスワップが増加

SIMスワップは、SIMハイジャックまたはSIMジャッキングとも呼ばれ、不正行為者が個人の携帯電話のアカウントを制御することができます。ソーシャルメディアから得た情報や情報漏えい事件で盗んだ情報をもとに、不正行為者はアカウントの所有者を装い、携帯電話会社を説得してアカウントを所有者のSIMから不正行為者が管理するSIMに移行させます。

そして、オンラインショッピングの際の強力な顧客認証（SCA）に使用されるワンタイムパスワード（OTP）やPINを含むSMSメッセージを不正行為者が傍受することができるのです。欧州でPSD2 SCAが導入されると、OTPやPINへの依存度が高まり、SIMスワップ攻撃が増加する可能性があります。

7 「新型コロナウイルス期間中のサイバー攻撃の驚くべき割合を示すINTERPOLの報告書」INTERPOL、2020年4月

スポットライト：**フレンドリー詐欺やポリシーの悪用の増加**

フレンドリー詐欺（第一当事者詐欺）とは、顧客がオンライン決済カードで商品やサービスを購入した後、カード発行会社に連絡して、商品が届かなかった、破損していたなどの理由で請求に異議を唱えることで、発生します。

また、顧客が返品や返金の手続きに手間取ったり、返金に時間がかかったりしたときに発生することもあります。

「フレンドリー詐欺への対応や係争は、加盟店にとって多くのオペレーション業務を発生させます。これは収益の損失や予測にも影響を与える、歓迎されない課題です。フレンドリー詐欺は、実際にはまったくフレンドリーではありません」

Martin Lee
アジア太平洋地域 マネージド・リスク・サービス担当ディレクター
Cybersource

専門家の指摘によると、かつてフレンドリー詐欺は、加盟店のプロセスの弱点につけこむような、日和見主義的なものが一般的でした。

加盟店がフレンドリー詐欺の事例を特定し、顧客に異議を唱えると、通常、そのようなことは二度と行われませんでした。しかし、フレンドリー詐欺は増加し、進化しています。おそらく、パンデミックの経済効果が消費者の起業家精神を高めたためでしょう。また、荷物が届かなかったと偽っても罰則があまりありません。世界の加盟店によると、フレンドリー詐欺は現在、最も一般的な詐欺行為であり、カードテスト、フィッシング、個人情報盗難がそれに次いでいます。

企業規模別に見た、経験した不正攻撃のトップ5

SMB

1. フレンドリー詐欺
2. カードテスト
3. フィッシング/ファーミング/ホエーリング
4. なりすまし
5. クーポン/割引/返金不正

中規模事業者

1. フレンドリー詐欺
2. カードテスト
3. なりすまし
4. フィッシング/ファーミング/ホエーリング
5. クーポン/割引/返金不正

大企業

1. フレンドリー詐欺
2. カードテスト
3. フィッシング/ファーミング/ホエーリング
4. ロイヤルティ詐欺
5. クーポン/割引/返金不正

情報元：世界の不正調査結果2021年、Cybersource、MRC

フレンドリー詐欺に見られる主な変化について見てみましょう。

- **ファミリー詐欺**とは、家族間でデバイスを共有することで発生するフレンドリー詐欺の一種で、カード所有者の許可なくアプリ内課金を行う可能性があります。カード所有者は、資金を取り戻すために紛争/チャージバックのルートを取ることができます。
- **デジタル商品に関するフレンドリー詐欺は、**署名などの配達証明がないため、証明するのが難しい場合があります。加盟店は、顧客が注文したことを銀行に証明するために、追加のデータを収集する必要があります。デバイス指紋認証、位置情報、行動バイオメトリクスは、ここで役立つツールです。
- **フレンドリー詐欺は、不正転売に関連するものが増えている可能性があります。**組織的な詐欺集団がフレンドリー詐欺を十分に行った場合、事実上盗品である商品をオンラインで転売することになる可能性があります。
- 各国が再開したことで、消費者は通常よりも大きな支出に走りました。このような消費衝動はリベンジ支出として知られています[8]。これは、**買い手の後悔を助長**し、顧客が取引に異議を唱える可能性を高める可能性があります。

8 「リベンジエコノミーの台頭」インターネット・オブ・ビジネス、2021年8月

フレンドリー詐欺とポリシーの悪用には密接な関係があり、クーポン、割引、返金などの悪用は、世界で5番目に多いタイプの詐欺行為となっています[9]。

ポリシーの不正行為は、以下の通りです。

- **購入した商品と異なる商品を返品する顧客**。例えば、本物のハンドバッグの代わりに偽物のハンドバッグを送り返すなど、かなり悪質な場合もあります。
- **BOPISで購入した商品を返品し、**別のカードに返金を依頼する顧客。
- SNSで**堂々と宣伝しているプロの返金業者**。彼らは、返金を確実に承認するための戦略を持つ、返品ポリシーの専門家であると自称しています。返金処理後、プロの返金業者はそのサービスに対して手数料を請求し、その額は商品価値の20%になることもあります。

過去2年間の増加を受けて、世界の**80%の加盟店がフレンドリー詐欺に対抗するための正式なアプローチを持っています**[10]。その多くは、顧客への通知、明確な支払い・返品規定、顧客の身元を確認するさまざまな検証手段など、さまざまな戦術を駆使した多角的な戦略を選択しています。

フレンドリー詐欺の増加により、ネガティブリストの神聖さが損なわれているため、定期的な見直しとクリーニングが必要になっています。グローバルなネガティブリストを活用したCybersource Decision Managerのアイデンティティ行動分析など、**追加のスクリーニング技術を使用する**ことで、適切な承認/拒否の判断ができるようになります。

「フレンドリー詐欺は（オンラインゲームなどの）デジタル商品販売業者にとって現実的な問題であり、Aite-Novaricaによれば、チャージバックの最大75%[11]がこの詐欺によるもので、これは驚異的な数字です」

David Mattei
Aite-Novarica 戦略アドバイザー

9 「2021年版グローバル不正レポート」Cybersource、MRC、2021年、p16
10 「2021年版グローバル不正レポート」Cybersource、MRC、2021年、p18
11 「紛争体験の改善：透明性は力なり」Aite-Novarica Group、2020年5月

スポットライト：**規制の影響拡大**

世界中の加盟店が経験する不正管理の課題として、規制や業界ルールの変更に対応することが第一に挙げられ、次いで新たな不正攻撃への対応が挙げられています[12]。

PSD2 SCAの導入はその好例で、欧州内外の販売企業に影響を与えています。強力な顧客認証（SCA）要件は、二要素認証で電子決済取引を保護するために設計されていますが、不正行為者は規制を回避する方法を見つけようとします。増加するSIMハイジャックは、不正行為者がSCAに使用するワンタイムパスワードや暗証番号へのアクセスを試みる、多数のルートの1つです。

PSD2 SCAでは、SCA要件に対応する方法としてEMV® 3-D Secure[13]（3DS）の採用が進みました。不正防止ソリューションプロバイダーと密接に連携している加盟店は、顧客の決済体験の中でEMV® 3DSをいつ起動または抑制するか、また免除の対象となる取引やSCAの対象外となる取引をどう処理するかを選択できるようになりました。

PSD2 SCAの影響を直接受けない人々は、ある地域でうまく機能した規制が最終的に他の地域でも採用される可能性があるため、EMV® 3DSが電子商取引の決済詐欺を軽減するために果たす役割と**何が起こるのかを注視しています。**

12 「2021年版グローバル不正レポート」Cybersource、MRC、2021年、p19
13 EMV® は、米国およびその他の国における登録商標であり、それ以外の地域では未登録の商標です。EMV の商標は EMVCo, LLC. が所有しています。

4

より多くのビジネスを獲得する不正防止戦略の構築

自動化された不正行為者に対処し、不正防止戦略を将来にわたって維持し、犯罪者を阻止するだけでなく、より多くのビジネスを獲得するための段階的な変更を行うために、できることはたくさんあります。

アクションプラン：不正防止戦略をスタートさせるための4つのステップ 〉

ステップ1：不正行為に対抗するための重層的なアプローチをとる

不正行為に対抗するために必要なことをすべて1つのツールで実現できるわけではありません。レイヤーアプローチでは、カスタマーエクスペリエンス全体で複数のツールを使用します。不正防止ソリューションの組み合わせを確認する：

アカウントレベルのツール。**アカウント開設時に不正のスクリーニングを開始します。**アカウント乗っ取りを特定し、防止するためには、本物のイベントとリスクの高いイベントの違いを見極める必要があります。これには、アカウントの作成、ログイン、更新、アカウント乗っ取り詐欺が含まれます。

Cybersourceのアカウントの乗っ取り防止のようなソリューションには、デバイス指紋認証、行動バイオメトリクス、物理バイオメトリクス、ワンタイムパスワード（OTP）などの機能が含まれています。

プリスクリーントランザクションツール。**個人情報の盗難、カードテスト、クレデンシャルスタッフィングに関連する注文を、**認証拒否に至る前にキャッチすることができます。プリスクリーニングツールは、処理中の上流で使用され、承認前に不正を検出することができます。

機械学習とお客様独自のポリシーを組み合わせて不正をブロックし、カードテストの試行を事前に阻止して、認証手数料が発生する前に阻止することができます。

決済トランザクションレベルのツール。Aite-Novarica Groupが最近行った調査では、半数以上[14]の加盟店がオンライン決済の不正行為を管理するために、いまだにルールベースのアプローチに依存しています。

今日の自動化された不正行為者に対処するには、グローバルなデータと業界の洞察にアクセスし、過去の取引データを評価してパターンを発見し、新しい不正防止戦略を知らせる**高度な機械学習モデルを使用します。**

ツール設定のためのオーケストレーション層。**機械学習を利用してリスクキャリブレーションを自動化し、**不正防止チームの負担を軽減し、レビューを削減します。洗練された分析とレポート機能により、これらのツールを最適化し、セルフチューニングを可能にすることで、不正行為ではなく、ビジネスに集中することができます。

「不正行為の進化速度が速いということは、従来の不正行為スクリーニングのルールが固定的で、それだけでは十分でないということです。ルール、AI、機械学習、手動レビューの間で適切なバランスを見つける必要があります」

Mari-anne Bayliss
欧州地域ソリューション担当シニアディレクター
Cybersource

14 Aite-Novarica Groupによる、北米、欧州、アジア太平洋地域の中堅・大手EC事業者756社への定量調査（2021年）。

ステップ2：不正とフリクションのバランスを正しく保つ

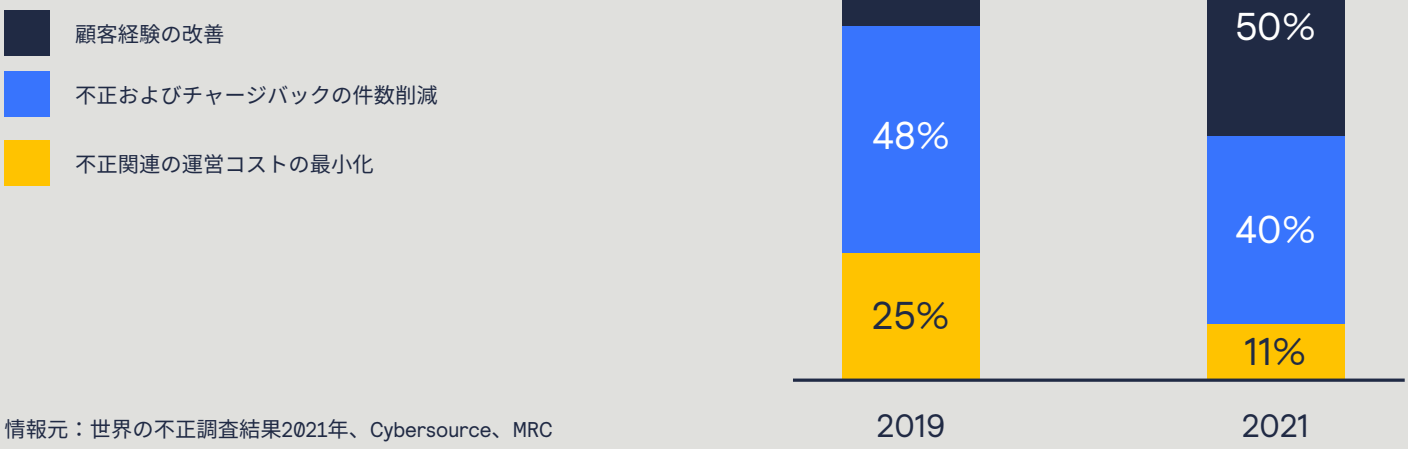
攻撃や収益の損失が増加しているにもかかわらず、半数の加盟店は、不正行為を管理する上で顧客体験の向上が最優先事項であると回答しています[15]。

消費者の体験を注意深くモニターし、フリクションが大きくなりすぎないようにします。一方、適切なフリクションを維持します。まず、バックグラウンドで動作する低フリクションまたは無フリクションのツール（デバイス指紋認証や行動バイオメトリクスなど）を適用することから始めましょう。

怪しいと思ったら、機械学習やAIを使った別の識別方法にステップアップして、取引の相手方を識別したり、OTP入力などのタスクにその人物を巻き込んだりします。

そうすれば、承認率を最大化し、不正損失を最小限に抑えながら、素晴らしい顧客体験を提供することができます。

最も優先すべき重要な不正抑止として選択した割合



情報元：世界の不正調査結果2021年、Cybersource、MRC

「加盟店は、フリクションとカート放棄を何としても避けたいため、顧客体験に懸念を抱いています。しかし、顧客体験に直接影響を与えるのは不正防止戦略と導入されたツールであるため、不正組織を会話に入れない限り、体験について語ることはできないのです」

Martin Lee
アジア太平洋地域 マネージド・リスク・サービス担当ディレクター
Cybersource

15 「2021年版グローバル不正レポート」Cybersource、MRC、2021年、p21

ステップ3：不正防止部門をビジネス上の意思決定のキープレーヤーにする

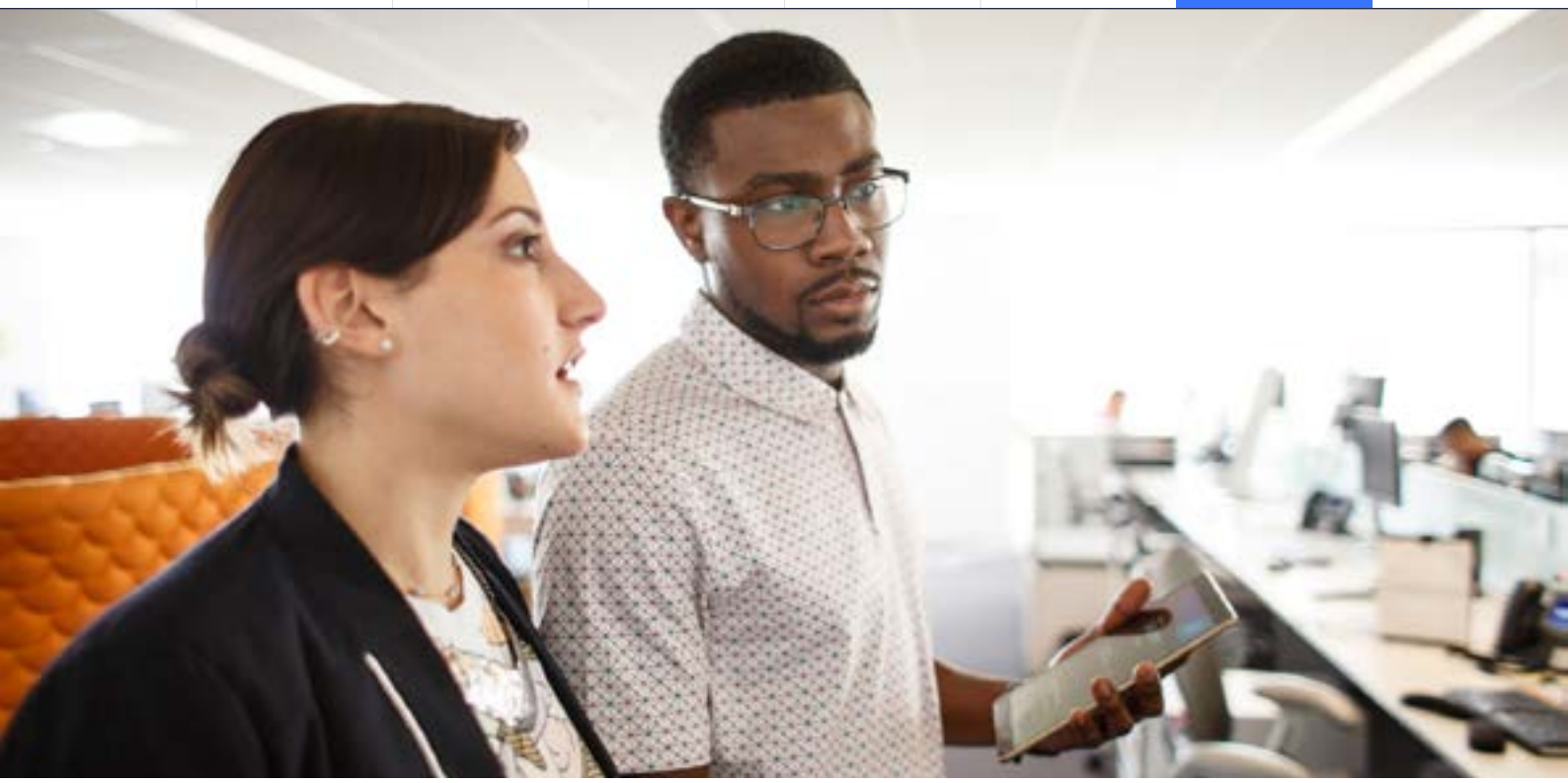
不正の管理は、もはや不正率を削減するための運用機能とは見なされません。

今日の不正管理者は、取引承認率、運用コストの削減、自動化の推進、認証の動的適用をますます重要視しています。

顧客の行動変化を把握し、販売戦略を再構築する重要な役割を担っています。そのため、不正防止チームをビジネスプランの後ではなく、最初の段階で参加させることが重要なのです。

「不正防止部門を強化し、ビジネス全体の共同パートナーにします。最近成功している組織を見ると、ビジネスライン、マーケティング機能、財務、オペレーション、不正防止の各チームが一体となって、協調して仕事をしています」

David Mattei
Aite-Novarica 戦略アドバイザー



ステップ4：適切な評価指標を導入する

適切な指標を適用し、データを活用して不正防止戦略を継続的に改善することで、収益の向上につなげることができます。

不正行為による損失だけでなく、以下のような他の指標にも目を向ける必要があります。

- 真正顧客排除率（オペレーションやコールセンターチームから聞くような、優良顧客を否定するようなもの）
- 承認率（事業部門やオペレーションチームから出ることもある）

そうすれば、過去の事例から学び、その情報を不正対策にフィードバックすることで、売上と承認率を最大化し、不正による損失を削減することができます。

同時に、不正防止チームの全体的なパフォーマンスをより適切に測定することができるようになります。

「不正/売上の比率が高い加盟店には、カード発行会社が厳しく対応することができます。このような立場にある加盟店は、全体的な不正率についてより戦略的になる必要があります。例えば、不正スクリーニングを承認より先に行うことで、承認率に強い影響を与えることを検討します」

Mark Strachan
Cybersource グローバルサービス担当ディレクター

変化に向けたチームの準備

不正防止チームは、パンデミックを通じてサポートとアドバイスを行うために迅速に対応する必要がありました。彼らの役割は進化し続け、新たなKPIも生まれています。

パンデミックに関係なく、**不正行為者は**これまでと同じように、**新しい脆弱性を積極的に探していくでしょう**。例：

- ハイブリッドワーキングモデルへの移行は、戸別訪問による不正行為の増加を促進する可能性があります。
- ワクチンパスポートは、IDのレイヤーが増えるだけでなく、不正行為を誘発する可能性もあります。すでにダークウェブ上では、12ドルという低価格でワクチンパスポートの販売が横行しています[16]。

次への備え

パンデミックの影響を受けた時期の再ベースラインデータ。受注量を見て、どの程度の割合でパンデミックの影響に分類されるかを検討します。

- 承認に伴うフリクションを減らすために、チャージバック率だけでなく、リスク分析対象も見直します。安全に購入障壁を取り除くために、許容範囲の不正を通過させる場合もあります。
- mPOS、デジタルチェックイン、非接触型配送など、顧客体験を向上させる新しいデジタル機能の導入を計画している場合、それらがもたらす可能性のある不正リスクを評価するために十分な時間を確保することが必要です。

「新しいテクノロジーに注目し、収益に影響を及ぼしている不正行為の構成要素に対処するための適性を評価します。ROIと不正行為に追加した場合のTCOに基づき、プロジェクトの優先順位を決定します。そして、もしまだそうしていないのであれば、顧客体験を向上させ、収益を守るための適切な資金を得るために、経営幹部と話し合います」

Tracy Kobeda Brown
プログラム＆テクノロジー担当副社長
MRC

16 「新型コロナウイルスワクチンパスポートの偽造市場の活況が警鐘を鳴らす」ロイター通信、2021年4月

Cybersourceの対応

当社の不正行為およびリスク管理ソリューションは、不正行為の阻止と同様に真正な顧客の受け入れに重点を置いているため、お客様はビジネスに集中することができます。

機械学習とリスクベースの戦略を組み合わせることで、より良い結果を得る

機械学習は、初日から当社の不正防止ソリューションの中核を成しており、その後もバージョンアップを続けています。現在ではVisaのソリューションとなり、私たちの強さ、サイズ、規模を合わせるとかなりの利点があります。

- **リアルタイムの自動化は、数百のデータポイント**をVisaとCybersourceのデータからのインテリジェンスと照らし合わせて分析し、強力なリスクスコアを生成して自動的に取引の承認または拒否を行い、不正行為者をブロックして攻撃の先を行くことができます。
- **アカウントログインから決済受入れまで、リスク検知**を自動化することで、フルフィルメントのスピードアップと収益増加を支援し、フリクションを低く抑えて顧客満足度を高く保ちます。

ビジネスをさらに発展させる

不正率の低減、承認率の向上、コスト削減の適切なバランスを見つけるために必要な洞察と制御を得ることができます。

- **1つの措置では対応しきれない場合があるため、**アカウントの乗っ取り防止からCybersource Decision Managerまで、機械学習の力で多層的な防御を行い、お客様のビジネスを保護します。

準備はできていますか？

変化する世界の中で、成長を確保するためのお手伝いをします。今すぐお問い合わせください。

cybersource.com

>> お問い合わせは**こちら**

cybersource
A Visa Solution