代表的な不正取引のリスクを特定し、回避するには。

事業と顧客の双方を
不正取引から守る方法。

PayPal
ペイパル

目次

世界の不正取引の最新動向を追う . . . 3
サイバーセキュリティを最優先するべき理由 . . . 4
代表的な不正決済の種類 . . . 5
オンライン小売業/eコマースにおける不正取引の概要 . . . 6
オンラインゲームにおける不正取引の概要 . . . 7
SaaSおよびサービス産業における不正取引の概要 . . . 8
不正取引対策 . . . 9
ペイパルによる不正取引対策の支援 . . . 11
参考文献 . . . 12

世界の不正取引の最新動向を追う

サイバー犯罪はあらゆる場所で発生しています。この類の犯罪の被害額は、年間で1兆米ドル近くに達し[1]、誰もが被害に遭う恐れがあります。ハッカーは全世界のありとあらゆる産業をターゲットにしています。また、世界にビジネスを展開する多国籍企業だけでなく、地域の中小企業なども狙われる可能性があります。

あらゆる状況において、どのようなタイプの攻撃が行われる可能性が高いかを学ぶことで、企業は不正の予測と対策をより効果的に進められるようになります。

1兆米ドル

サイバー犯罪による世界の年間の被害額[2]。

82%

2021年に不正取引の試みが増加したと報告した大企業の割合[3]。

18%

不正取引によるeコマースの損失の前年比増加率[4]。

3.3倍

不正取引から派生する時間などのコストは実際の被害額の約3.3倍に達する[5]。

5回に1回

アカウントの乗っ取りを試みるログインの頻度[6]。

8倍

日本で2019年から2021年の間にフィッシング詐欺の試みが8倍に増加[7]。

1, 2. Center for Strategic & International Studies (2020), *The Hidden Costs of Cybercrime* **3.** Cybersource (2021), 2021 Global Fraud Report **4.** Payments Dive (2021), *E-commerce fraud to surpass $20B in 2021, an 18% jump over last year, report finds*
5. LexisNexis (2020), *2020 True Cost of Fraud Study – E-Commerce/Retail Report* **6.** Arkose Labs (2022), *2022 State of Fraud & Account Security Report* **7.** Nikkei Asia (2021), *Japan's Line, NTT share smartphone payment fraud data*

サイバーセキュリティを最優先するべき理由

不正取引とサイバー犯罪は企業に損害をもたらします。当然ですが、収益や商品が騙し取られる恐れがあります。しかし、不正取引対策には多額のコストも費やされ、被害額の3倍以上のコストが投じられているのです[8]。

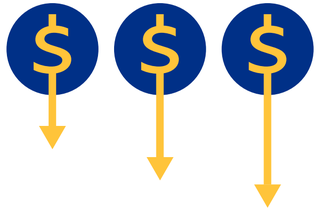
不正決済の損害には、3つの種類があります。

- まず、提供する商品やサービスが盗まれる、直接的な損害が挙げられます。この場合、在庫の商品を置き換えるためにコストが生じます。
- 本来のカード所有者から返金を、決済処理業者からはチャージバック手数料を要求されます。つまり、売上が消え、さらに追加の運用コストを支払う必要があるのです。
- 不正取引への対応に加え、アカウントを乗っ取られた本当の顧客からのクレームに時間とリソースを投じる必要もあります。その結果、運用コストが増加します。

その上、大規模な攻撃を受けたことが大々的に報じられ、評判の面で被害を受ける恐れもあります。また、不正取引が注目を浴びなかったとしても、チャージバックをはじめとする不正取引の試みが多数行われると、決済プロバイダからリスクの高い企業と見なされて、より厳しい条件を課されたり、処理コストが増加したりするデメリットが発生します[9]。

データ漏洩や不正取引の不適切な処理は、アンチマネーロンダリング(AML)機関などの規制機関からの制裁や罰金の対象となります。

本ガイドは複数の産業を取り上げ、その産業で多発する不正取引の種類を紹介し、また対策についてご説明します。



失われる収益と比べて —
3倍以上
の資金が不正取引対策に費やされています[8]。

8. LexisNexis (2020), *2020 True Cost of Fraud Study – E-Commerce/Retail Report* **9.** Forbes (2021), *High-Risk Merchant Account: What It Is And How It Works*

代表的な不正決済の種類

アカウント乗っ取り(ATO)詐欺

アカウントの乗っ取りは、なりすまし詐欺の形態の一つです。アカウントの乗っ取りとは、顧客のアカウントにアクセスして、勝手に購入を行ったり、アカウントに保存されている個人情報や決済情報を盗む犯罪行為を指します。アカウント乗っ取り詐欺は基本的に次の方法で行われます。

- **クレデンシャル・スタッフィング** – ダークウェブで購入した無数のユーザー名/パスワードの組み合わせを使って、ボットが大量にログインを試みます。
- **フィッシング詐欺およびソーシャルエンジニアリング** – 偽のメールや電話を通して、顧客を騙して個人情報を提供させます。

カードテスティング

カードテスティングとは、盗まれた大量のカードの情報が有効かどうかを確認する不正行為です。通常はボットやコンピュータスクリプトを使って、少額の取引を大量に実行します。その後、有効なカードを使って高額の商品を購入したり、別のハッカーにカード情報を売却したりします。

カード不介在(CNP)詐欺

CNP詐欺とは、カードを提示することなく、カードを使って購入を行う不正行為を指します。元々は、電話販売や通信販売に用いられていた手法ですが、現在ではさまざまなeコマースの購入にも採用されています。CNP詐欺は、盗んだカード情報を使う従来の手法と、フレンドリー詐欺(下記を参照)の2つの形式に分類されます。どちらの種類のCNP詐欺においても、結果的に本当のカード所有者がチャージバックを求めます。

フレンドリー詐欺

フレンドリー詐欺は、カード所有者本人が正当な取引に対して異議を提起することで発生します。購入したことを忘れた、または家族がカードを使って購入したことを知らなかったことが原因で発生する場合もあります。また、購入者が衝動買いを後悔したり、サブスクリプションのキャンセルを忘れたものの、ミスを認めるのではなく、チャージバックを申請するケースも見受けられます。さらに、顧客が「未着品」を偽るフレンドリー詐欺も存在します。

不正なチャージバック

カード所有者が支払の取り消しを求めると、銀行やカード会社は支払をキャンセルした上で、販売した企業にチャージバック手数料を要求します。チャージバックは取引時の問題が原因で発生する可能性があります(商品が届かなかった、またはカード決済時にエラーが発生したなど)。また、カード所有者本人が詐欺に気づいた際にチャージバックを要請することもあります。正当なチャージバックが大半を占めますが、不正なチャージバックの要求が増加傾向にあります。

合成アイデンティティ詐欺

合成アイデンティティ詐欺は、金銭に関わる詐欺の中で、急激に増加している詐欺の一つに挙げられます。盗んだ個人情報を基に、または完全に架空の個人情報を基に偽の身元を作り上げ、徐々にクレジットヒストリーを構築するものです。一見有効なIDを用いてクレジットカードや融資を申請し、限度額ぎりぎりまで使ってから姿を消します。このタイプの詐欺は手遅れの状態になるまで、見つけ出すことが困難です。

オンライン小売業 / eコマースにおける不正取引の概要

eコマースはここ数年の間に世界で急成長を遂げましたが、さまざまな種類の不正決済も激増しています。

その中でもとりわけ多いのがフレンドリー詐欺とカードテスティングです[10]。オンライン小売企業はチャージバックやフレンドリー詐欺を含むあらゆる種類の攻撃が増加していると報告しています[11]。

アンケート調査に参加した販売企業のうちの半数以上が、アイデンティティ詐欺やアカウントの乗っ取り、なりすまし、新規アカウント開設詐欺などのアイデンティティ(身元)やアカウントに関連する不正取引が増加していると回答しています[12]。また、カード不介在詐欺の増加を報告する販売企業は59%にのぼります[13]。

不正取引を専門とするArkose Labsは、4回の取引のうち1回は不正取引の試みであると指摘しています[14]。

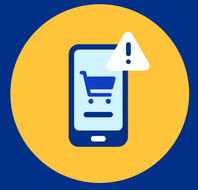
規模や場所に関係なく、すべてのeコマース企業が不正取引を重大な問題と見なしています。

5社のうち3社

のオンライン販売企業が決済詐欺がもたらす収益の減少が事業に実害、または重大な影響をもたらしていると回答[15]。

5社のうち3社

のオンライン販売企業が決済詐欺がもたらす生産性の低下が事業に実害、または重大な影響をもたらしていると回答[16]。



10社のうち9社

のオンライン販売企業がeコマースの不正取引への対策は、全体的な事業戦略において「とても重要、または非常に重要」と回答[17]。

5社のうち1社

のオンライン販売企業が、顧客のデータを保護する取り組みは困難を極めると回答[18]。

10, 17. Cybersource (2021), *2021 Global Fraud Report* **11, 12, 13, 15, 16, 18.** FIS Worldpay (2021), *Global Payment Risk Mitigation* **14.** Arkose Labs (2022), *2022 State of Fraud & Account Security Report*

オンラインゲームにおける不正取引の概要

オンラインゲームやeスポーツは取引量が多く、また、早く、スムーズな取引が求められます。さらに、ゲーム内アセットの価値は世界で合計500億米ドルに達することから[19]、以前からオンライン不正取引のターゲットにされてきました。

盗んだFortniteのアカウントを販売することで、ハッカーは年間10億米ドルの収益を得ていると推測されています[20]。

ゲーム会社にとって厄介なことは、不正攻撃の実行がサイバー犯罪者に多額の利益をもたらすことです。Arkose Labsが指摘しているように、たった15米ドル/日でボット攻撃を仕掛けることが可能であり、盗んだアカウントは最高で3,000米ドルで売却できます[21]。

また、同社によると、オンラインゲームは2020年中に最も多くの攻撃を受けた産業[22]であり、2021年には横ばいの状態に落ち着いたものの、攻撃の種類は多様化が進んでいると言われています[23]。

オンラインゲーム産業における代表的な不正行為の種類を挙げていきます。

- **アカウントの乗っ取り攻撃** – 2021年においては、3回の攻撃のうち2回はユーザーのログイン情報に狙いを定める攻撃でした[24]。攻撃方法には、ボットを配備してユーザーネームとパスワードのさまざまな組み合わせを試すクレデンシャル・スタッフィングが含まれます。アカウントを乗っ取られると、ゲーム内アセットに加えて、決済情報や個人情報などがすべて盗まれ、売却されます。
- **フィッシング詐欺およびソーシャルエンジニアリング**は通常アカウントの乗っ取りや決済情報、個人情報の盗難をもたらします。
- **フレンドリー詐欺**はオンラインゲーム産業を代表する詐欺の一つです。顧客が正当な取引に対して異議を申し立てることで発生します。この不正行為は、取引を行ったことを忘れてしまったり、家族による購入を勘違いしたり、あるいは衝動買いを後悔したりすることが原因で起きます。
- **カードテスティング詐欺**もゲーム産業では多く見受けられます。大量の取引が行われるものの、少額の取引が大部分を占めるため、カードテスティング行為を隠蔽する上で理想的な環境が整っているためです。

アジア太平洋(APAC)地区は世界のゲーム産業で最も多くの収益を生み出しており、2021年にはモバイルゲームのプレーヤーが2億5,000万人に到達する勢いで増加しました[25]。全世界を対象としたモバイルゲームの収益ランキングでは、中国、日本、韓国、インドネシア、オーストラリアのすべてがトップ10入りしています[26]。その結果、APAC地域全体でテクノロジー企業とゲーム企業が、主要なターゲットとして不正取引攻撃の被害に遭っています[27]。

19. Intellicheck (2021), *How companies can prevent fraud in online gaming* **20.** Business Insider (2020), *Stolen Fortnite accounts are being sold on the black market...* **21, 22.** Arkose Labs (2021), *How to Level Up in the Fight Against Online Gaming Fraud*
23. Arkose Labs (2021), *Fraud in Online Gaming: A Midyear Snapshot of 2021 Attack Trends* **24, 27.** Arkose Labs (2022), *2022 State of Fraud & Account Security Report* **25.** Transperfect (2021), *What Does Global Gaming Industry Growth Look Like in 2021?* **26.** Newzoo (2021), *Global Mobile Market Report 2021*

SaaSおよびサービス産業における不正取引の概要

Arkose Labsは、テクノロジー企業が不正取引攻撃の被害に遭う件数は2020年から2021年の間に5倍増加したと指摘しています[28]。

とりわけSaaS、およびサブスクリプションビジネスを展開する企業が不正取引の攻撃を受けやすいことが明らかになっています。これは、すべてのアカウントに決済情報が紐づけられていることが原因です。

2021年、テクノロジー企業は前年の**5倍**に相当する不正取引の被害に遭ったと推測されています[29]。

- **アカウントの乗っ取り(ATO)詐欺**は日常的にSaaS産業に脅威を与えています。アカウントを乗っ取られてしまうと、サービスや商品の購入に使われる、もしくは別のハッカーに売却されます。
- また、盗んだカード情報を用いて、偽のアカウントを開設した後、購入を行う詐欺**(CNP fraud)**や偽造したアカウントを介して無料トライアルを悪用する手法もSaaS産業を苦しめています。
- **チャージバック**もまたSaaS事業にとって大きな課題を突き付けています。実際に、ソフトウェア産業はチャージバックと取引の比率が他の産業の平均値よりも高く、0.66%に達します[29]。サブスクリプションを購入したことを忘れていたユーザーによる、悪意のないチャージバックも中にはありますが、大半は詐欺行為が占めます。

28. Arkose Labs (2022), *2022 State of Fraud & Account Security Report* **29.** Expert Market (2021), *Chargeback Fraud Statistics 2022*

不正取引対策

アカウント乗っ取り攻撃に有効な対応

ペイパルをはじめとする一部の決済サービスプロバイダは多要素認証(MFA)や2段階認証(2FA)を提供しています。これらのシステムは、クレデンシャル・スタッフィングやフィッシング詐欺で盗んだ認証情報の利用を阻止する上で大きな効果が見込めます。実際に、ほぼ半数の販売企業が2段階認証を「とても重要」であると指摘しています[30]。

MFA/2FAを有効にすると、顧客に別の認証(1度のみ有効な数字のコードなど)の提供を要請し、その情報を事前に登録した携帯電話やメールアカウントに送信します。こうすることで、盗んだ認証情報の利用を防止することができます。なぜなら、認証情報の本当の持ち主のモバイルデバイスやメールにアクセスしなければならなくなるためです。

アカウントの乗っ取りでは、最初のステップが自動化されていることが多いため(ボットを使って、クレデンシャル・スタッフィング攻撃を仕掛ける)、人間とのやり取りが必要なCAPTHAテクノロジーなどのシンプルな手順を導入することで、効果が期待できます。

カードテスティングの検出と対処方法

カードテスティングでは、短時間に少額の取引が大量に実施されます。eコマースやオンラインゲームなどの取引量の多い産業では、カードテスティング取引を発見するのは困難であり、防御の術がない状態では、瞬く間に大量のチャージバックに晒されてしまいます。さらに、カードテスティング攻撃は何度も認証に失敗するため、販売企業のインフラの稼働率にも悪影響を及ぼす恐れがあります。

ペイパルは機械学習アルゴリズムとリアルタイムで判断を行うシステムを採用し、正当な取引と不正取引の違いを見極め、カードテスティングなどの不正パターンを素早く特定するためのサポートを行っています。また、ペイパルは過去の傾向とIPアドレスやデバイスの種類、ID、メールアドレスなどの取引情報を比較します。

機械学習の良し悪しは、学習するデータの質に左右されます。ペイパルは買い手と売り手の両方を顧客に抱えており、データの質には確固たる自信を持っています。4億名を超える購入者と、さまざまな産業に属する3,000万の販売会社がペイパルを利用しており、消費者およびリスク特性に関するデータには事欠きません。取引の売り手と買い手の双方に関するインサイトは、非常に高度な不正行為に対処する場合であっても、正当な取引と悪意のある取引を判定する際に役立ちます[31]。

4億名を超える買い手と3,000万社の売り手がペイパルを利用[31]。

30. FIS Worldpay (2021), *Global Payment Risk Mitigation* **31.** PayPal (2020), *How Data Science, Machine Learning and Artificial Intelligence Lead to Higher Authorization Rates*

カード不介在(CNP)詐欺を削減

CNP詐欺に対しては、購入者に出来る限り多くの情報提供を求めるアプローチが最も効果的です。たとえば、CVVコードの入力や3Dセキュア(3DS)、多要素認証(MFA)などの不正防止対策の導入をおすすめします。

やはり、リアルタイムのデータをベースに機械学習を用いる決済システムプロバイダなら、CNP詐欺の削減に貢献することができます。その代表格がペイパルです。ペイパルが先陣を切って使用するネットワークのトークン化[32]は、盗んだカード情報を不正取引に利用する試みを難しくします。

フレンドリー詐欺への対応

フレンドリー詐欺(ファーストパーティー(当事者)詐欺と呼ばれることもあります)はeコマースとオンラインゲーム産業で多く用いられる不正取引の手法です。この詐欺の特徴は、検出と証明が難しいことです。しかし、正当に商品やサービスの注文が行われたこと、配送したこと、受け取りが行われたことを証明するために記録を取り、そのためのポリシーを定めることで、誤った請求に対して堂々と反論できるようになります。たとえば、商品の受け取りに署名を求めるアプローチなどです。

多くのフレンドリー詐欺の請求は、元をたどれば有効な取引に行き着きます。そのため、明確で、寛大な返品ポリシーを用意し、カスタマーサービスとコミュニケーションに力を入れることで、事実を偽ってチャージバックを請求する行為を防止する効果が期待できます。

また、常にカードのCVVコードを要求し、3Dセキュアの導入を介して、フレンドリー詐欺を実行しにくい環境を作りましょう。

なお、販売事業者はPayPalの売り手保護制度によるメリットを得られる可能性があります[33]。

不正なチャージバックを減らすには

不正な取引の半数近くが最終的にチャージバックをもたらすため、総合的な不正対策を改善することが、不正なチャージバックの削減につながります。

不正なチャージバックを削減する最良の手法の一つとして、ペイパルをはじめとする、高度な不正対策テクノロジーを持つ決済処理プロバイダと協力して対処するアプローチが挙げられます。不正行為の技術は常に進化しているため、その脅威に対抗するためには、リアルタイムのデータを基に常時進化する不正防止ソリューションが欠かせません。

合成アイデンティティ詐欺への対応

合成アイデンティティ詐欺が暗躍している原因は、多くの金融機関がクレジットを提供する上で、単純で、自動化した評価システムを用いているためです。第三者のデータを含む大量のデータを活用することで、偽のIDの特徴ともいえるデータの不一致を検出できることがあります。

ペイパルが誇る、売り手と買い手の巨大なネットワークは、不正検出を行う機械学習モデルに多大な情報を与えます。

32. PayPal (2020), *How Network Tokenization Leads to Higher Authorization Rates and a Better Customer Experience* **33.** 規約適用

ペイパルによる不正取引対策の支援

ペイパルの決済技術の開発には20年以上の歳月が費やされています。この技術は不正行為のリスクを減らし、顧客の消費意欲を高めるように設計されています。

世界中でペイパルブランドは認められ、信頼を得ています。個人情報が絶対に共有されない事実が高く評価されています。ペイパルのユーザーは、現代の消費者が求める簡単で、安全で、便利な支払いを考慮した決済体験の恩恵を得ることができます。

ペイパルを利用することで、販売企業は各種の決済方法(地域で人気の高い決済方法を含む)を1度の導入で提供できるようになります。ペイパルでは1度の導入で、さまざまな決済方法を購入者に提供できる他、支払いを簡単に一元管理できるメリットがあります。

また、適用条件を満たしている取引はペイパルの売り手保護制度[34]の対象となり、本人認証(3Dセキュア)などの不正防止対策もご利用いただけます。

ペイパルは高度な不正防止機能を提供しています。ペイパルでは、4億人以上のアクティブユーザーが購入や販売を行っています。そのため、ペイパルの機械学習モデルはこれらの情報を基に、精度が高く、適応性に優れ、なおかつリアルタイムで不正取引を検出しています。その結果、誤拒否の件数は減り、また、正当な顧客をハッカーのように扱ってしまう可能性は低下します。

また、ペイパルが持つ膨大な売り手データセット、高度な機械学習技術、データ科学の専門知識により、新たにトレンドとなった不正行為を特定し、ネットワーク上の他のすべての売り手に対して迅速に対策を講じることができるようになりました。

その上、銀行やカード受容者、規制当局とのグローバルな関係により、不正行為を未然に防ぐことができます。

ペイパルの不正対策は法人企業のニーズを考慮しています。ペイパルはPayPal Commerce Platformで実践的なツールキットを提供しています。
これは、売り手が取引上の意思決定プロセスにおいて取引上の意思決定プロセスをより明確に理解し、より簡単に管理できるように設計されています。

ペイパルが法人企業のリスク管理やコンプライアンス維持にどのように貢献しているかについて詳しく説明しています。

詳しくはこちら

ペイパルの高度なリスク管理により、以下の恩恵を得られます。

- チャージバックの減少
- 誤拒否率の低下
- 顧客のストレスの低下
- 不正行為による被害の減少
- 運用効率の向上
- 効率化されたカスタマーエクスペリエンス

34. 規約適用

参考文献

1. Center for Strategic & International Studies (2020), *The Hidden Costs of Cybercrime*
2. Center for Strategic & International Studies (2020), *The Hidden Costs of Cybercrime*
3. Cybersource (2021), *2021 Global Fraud Report*
4. Payments Dive (2021), *E-commerce fraud to surpass $20B in 2021, an 18% jump over last year, report finds*
5. LexisNexis (2020), *2020 True Cost of Fraud Study – E-Commerce/ Retail Report*
6. Arkose Labs (2022), *2022 State of Fraud & Account Security Report*
7. Nikkei Asia (2021), *Japan's Line, NTT share smartphone payment fraud data*
8. LexisNexis (2020), *2020 True Cost of Fraud Study – E-Commerce/ Retail Report*
9. Forbes (2021), *High-Risk Merchant Account: What It Is And How It Works*
10. Cybersource (2021), *2021 Global Fraud Report*
11. FIS Worldpay (2021), *Global Payment Risk Mitigation*
12. FIS Worldpay (2021), *Global Payment Risk Mitigation*
13. FIS Worldpay (2021), *Global Payment Risk Mitigation*
14. Arkose Labs (2022), *2022 State of Fraud & Account Security Report*
15. FIS Worldpay (2021), *Global Payment Risk Mitigation*
16. FIS Worldpay (2021), *Global Payment Risk Mitigation*
17. Cybersource (2021), *2021 Global Fraud Report*
18. FIS Worldpay (2021), *Global Payment Risk Mitigation*
19. Intellicheck (2021), *How companies can prevent fraud in online gaming*
20. Business Insider (2020), *Stolen Fortnite accounts are being sold on the black market...*
21. Arkose Labs (2021), *How to Level Up in the Fight Against Online Gaming Fraud*
22. Arkose Labs (2021), *How to Level Up in the Fight Against Online Gaming Fraud*
23. Arkose Labs (2021), *Fraud in Online Gaming: A Midyear Snapshot of 2021 Attack Trends*
24. Arkose Labs (2022), *2022 State of Fraud & Account Security Report*
25. Transperfect (2021), *What Does Global Gaming Industry Growth Look Like in 2021?*
26. Newzoo (2021), *Global Mobile Market Report 2021*
27. Arkose Labs (2022), *2022 State of Fraud & Account Security Report*
28. Arkose Labs (2022), *2022 State of Fraud & Account Security Report*
29. Expert Market (2021), *Chargeback Fraud Statistics 2022*
30. FIS Worldpay (2021), *Global Payment Risk Mitigation*
31. PayPal (2020), *How Data Science, Machine Learning and Artificial Intelligence Lead to Higher Authorization Rates*
32. PayPal (2020), *How Network Tokenization Leads to Higher Authorization Rates and a Better Customer Experience*
33. 規約適用
34. 規約適用