デジタル化 ✚ 成長

ビジネスを不正利用から守る

サイバーセキュリティで先手を打つ方法

PayPal
ペイパル

フラウドエコノミーとは？

これまでオンラインの不正利用は、個人のハッカーや詐欺師が行う単独のインシデントだと考えられていました。しかし近年、このようなサイバー犯罪が、サイバー犯罪者の組織的かつ洗練されたネットワークによって行われることが増えてきました。企業は不正取引の被害を防ぐために、同じように洗練された保護措置を講じる必要があります。

パンデミックはあらゆる面に大きな変化をもたらしましたが、eコマースは特に大きな影響を受けました。新型コロナウイルスの流行により、インターネットによるトラフィックは60%急増し、その結果、オンラインショッピング利用者の支出は約2倍になりました[1]。2021年になると、不正利用の脅威はかつてないほど大きくなりました。eコマース小売業者はオンラインの不正取引により200億ドル以上の損失を被る危険にさらされていました。実際、前年に比べてオンラインの不正取引が18%増加しました[1]。パンデミックの緊迫した状況の中で、不正利用者たちは、チャリティー詐欺、WHO（世界保健機関）やCDC（米国疾病対策センター）を装ったメール、さらには政府機関や困窮した家族、銀行やクレジットカード会社を装ったロボコールなどにより、被害者を食い物にしました[2]。

フラウドエコノミーが拡大すると、サイバー犯罪者は大胆になります。より賢く、より洗練され、そして、オンラインビジネスを不正利用するのに必要なツールをいっそう使用できるようになりました。標的にする企業と同じくらい、あるいはそれ以上に、eコマースの仕組みに精通しています。そのため、セキュリティの脆弱性を正確に把握し、思いもよらないところから攻撃することができるのです[3]。

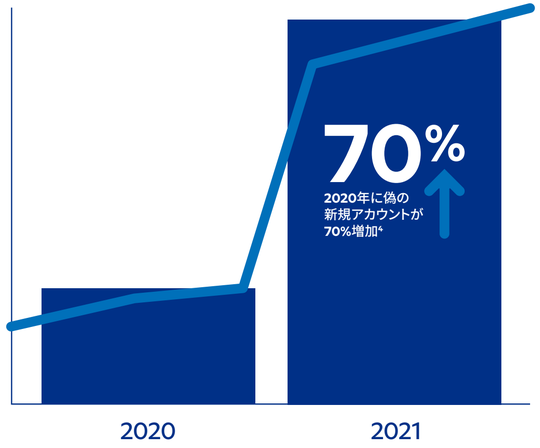
不正利用が横行する中、企業はこれまで以上に対策を講じています。しかし顧客の期待に変化はありません。オンラインショッピング利用者は、厳重なセキュリティに加えて、迅速で無駄のないスムーズな体験を求めています。購入の所要時間が長すぎたり、購入時に必要なデータ量が多すぎたり、購入手続きが複雑すぎたりすると、顧客はカートを放棄して別のサイトに行ってしまいます。このように顧客が期待を持っているため、小売業者にとっての課題は、顧客のニーズを満たしつつ様々なサイバー脅威からビジネスを守ることだと言えます。

1. Payments Dive、E-commerce fraud to surpass $20B in 2021, an 18% jump over last year, report finds、2021年4月30日。 **2.** CyberCrime Support Network、COVID-19 Scam Alerts、2021年4月12日。 **3.** Sift、Exposing the Multi-billion Dollar Fraud Economy、2021年第1四半期。

企業は世界中の不正利用に対して新たな課題に直面している

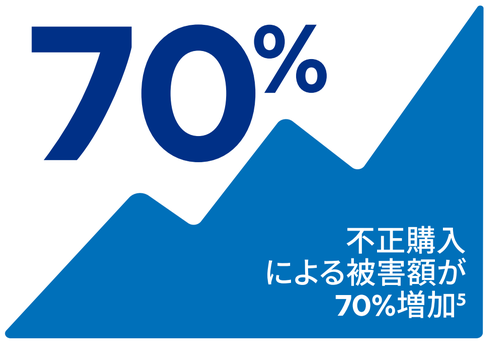
新規アカウント不正の増加

2021年には、偽の新規アカウント登録が**70%**以上増加しました[4]。



より大きな企業を狙う大胆な動き

各種の不正購入の被害額は、パンデミック前にと比較して平均**70%**上昇しました[5]。



モバイルへの攻撃の増加

デジタルトラフィック全体の**50%**がモバイルであり、2021年上半期のモバイルへの攻撃率は**24%**に上りました[6]。

4. Business Wire、70% Increase in Fraudulent Account Registrations Puts Digital Accounts in the Crosshairs, Arkose Labs Reports、2021年8月5日。 **5.** Retail Week、Every day is now Black Friday – and retailers need to prepare、2021年11月4日。 **6.** Security Boulevard、Here's How to Fight Diverse Attacks Across Multiple Touchpoints、2021年10月8日。

サイバー犯罪に先手を打つ

サイバー脅威がかつてないほど複雑化し流行しているからといって、不正利用をビジネス上の必要なコストだと企業は諦めてはいけません。昨年、オムニチャネル小売分野では、不正利用の発生率が前年比で50%増加し、不正な注文は前年比で9%増加しました[7]。企業は不正利用から身を守るために、適切なインフラを整えることに注力しなければなりません。

お客様のビジネスを守るための5つのヒント：

1. 不審の疑いのある動きがないかサイトを監視する
2. 決済時のサイバー犯罪を防ぐ
3. 安全に決済が行えるようにデータを暗号化する
4. ソフトウェアをアップデートしてセキュリティを高める
5. 盲点を把握してサイバー防御力を高める

7. Sift、Exposing the Multi-billion Dollar Fraud Economy、2021年第1四半期。

1 不正の疑いのある動きがないかサイトを監視する

不正の疑いのある動きはあなたのビジネスの時間と費用の損失になり、発見するのは必ずしも容易ではありません。また用心するに越したことはありません。ここでは、お客様のサイトを監視するための方法をご紹介します。

過剰なチャージバックには注意しましょう。特定できない購入の場合や、忘れられていた購入の場合や、返品ポリシー誤解の場合のチャージバック請求は、チャージバック詐欺（フレンドリー詐欺、第一者詐欺とも呼ばれる）の可能性があります。94%の企業が、フレンドリー詐欺を依然として問題視しています[8]。

馴染みのないマーケットでは、住所に注意したり、請求先と発送先の住所が一致していない場合に注意したりすることで、買い手の不審な活動のサインを特定することができます。また、不審なメールアドレス、未着の電子メール、異常に大量な注文、1つの注文に複数のクレジットカードが使用されている場合も注意が必要です。

自社サイトを監視することも重要ですが、専門家の相談することも大切です。チャージバック管理を外部の専門家に委託することができれば、こうしたパターンを監視する負担が軽減します。また、顧客のIPアドレスを追跡してリスクの高い地域からアクセスが行われている場合に警告してくれるツールもあります。

PayPal Commerce Platformの不正防止および売り手保護機能は、チャージバックを最小限に抑えるためにお客様のビジネスに適応した機械学習を実装し、特定の不正行為が発生した場合にカバーすることで、この問題を解決することができます。

8. Business Wire、8 Out of 10 Merchants Have Seen an Increase in Friendly Fraud, According to the 2021 Chargebacks911 Field Report、2021年6月2日。

2 決済時のサイバー犯罪を防ぐ

59%の企業で不正利用が増加しており、カード未使用の取引の被害に遭っています。決済時の不正防止ソリューションなら、このタイプの攻撃に先手を打つことができます[9]。

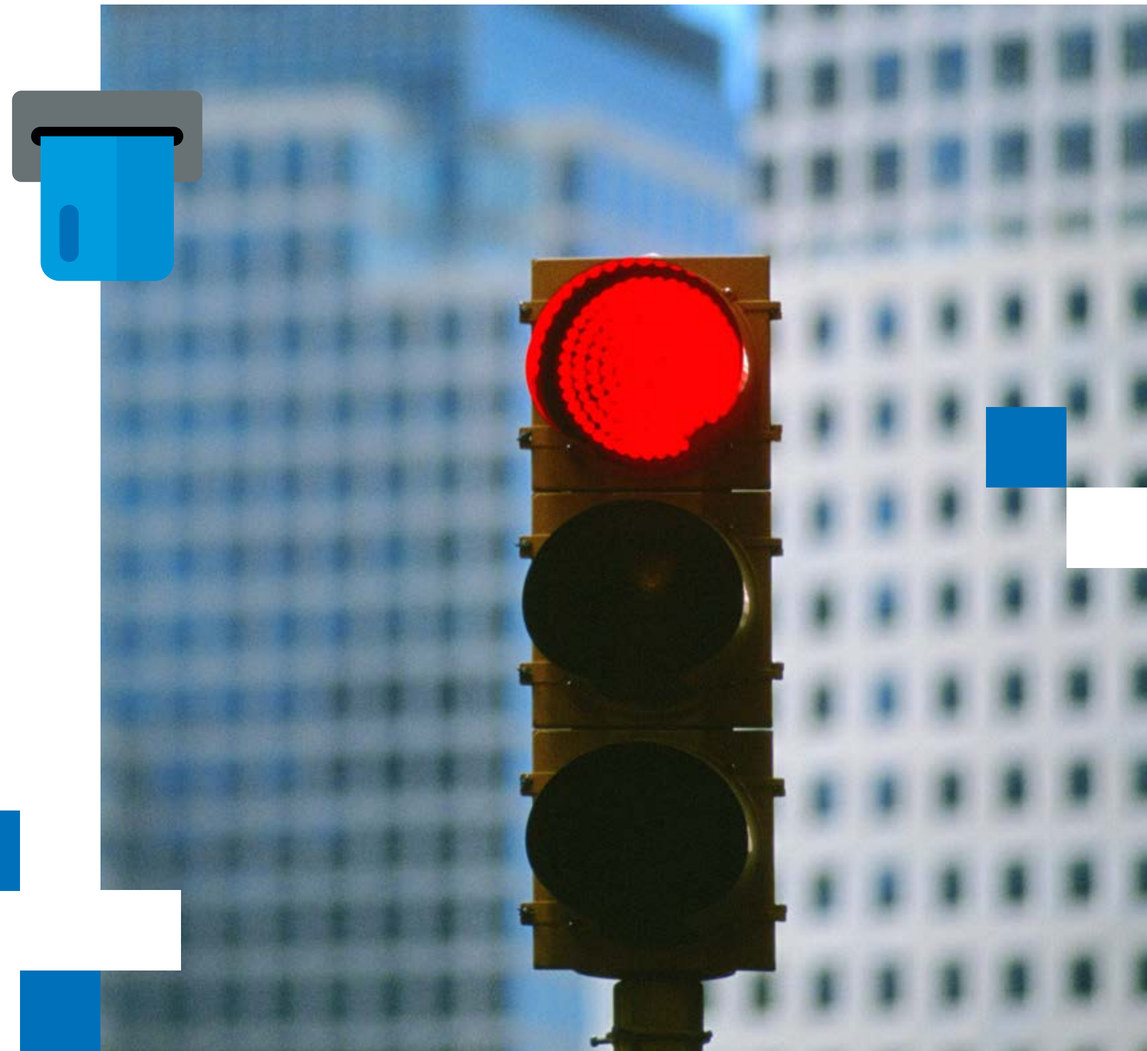
4社のうち1社は、決済セキュリティソリューションの導入に苦戦していますが、こうした手順を踏むことはeコマースの可能性を探る上で不可欠です[9]。

PCI規則では、売り手はクレジットカード番号と一緒にセキュリティーコード(CVV)を保存することができないため、セキュリティーコードを要求すれば、サイバー犯罪者がカード不使用の不正を行うことができなくなります。これにより、顧客が購入に必要な実物のカードを所持していることが確認できます[10]。

住所認証システム(AVS)は、クレジットカードに関連付けられた請求先住所の数字部分を、クレジットカード会社に登録されている住所と比較することで、不正の疑いのある動きを特定できます。

AVSはほとんどの決済システムにも搭載されていますが、サポートされているかどうかを決済会社に確認するのが良いでしょう。

最後に、ベロシティチェックとは、1日に1人の顧客から来る資金や取引の量を制限することができる不正防止の仕組みです。お客様のビジネスに適したしきい値を設定し、そのしきい値を超えた場合には通知を受信したり、取引を自動的にキャンセルすることもできます。これは一般的に、盗難にあったクレジットカードの被害を最小限にするために行われます。



9. Payments Dive、Merchants say they're losing revenue to online fraud, FIS report finds、2021年7月12日。 **10.** Big Commerce、Ecommerce Fraud Protection for Online Merchants: The Ultimate Guide。

3 安全に決済が行えるように データを暗号化する

暗号化されていないデータは、サイバー犯罪者の格好の獲物です。クレジットカード番号やパスワードなどに簡単にアクセスできてしまうためです。より価値の高い標的への移行が進んでいるものの、多くのサイバー犯罪者は今なおこうした隙を狙っています。

日々、大量の機密データがインターネット上で送信されているため、悪用される可能性は少なくありません。しかし、お客様のビジネスや顧客を護るためにできることはあります。

エンドツーエンドの暗号化技術は、インターネットでデータを送信する前に秘密のコードに変換するので、このような状況に備えることができます。個人情報保護法や地域のデータ保護法の観点からも、データを保存したり共有したりする企業にとっては欠かせません[11]。

さらに、強力なトランスポート・レイヤー・セキュリティ(TLS)設定を使用して、安全なHTTPS接続を確保しましょう。TLS設定は現在の業界標準であり、情報がインターネット上で安全に移動できるようになります。

決済パートナーが、お客様のデータのセキュリティをお客様と同じくらい真剣に捉え、厳しいデータ保護要件を遵守していることを確認しましょう。

ペイパルの決済プラットフォームは、最高のエンドツーエンドの暗号化によって支えられています。TLSおよびHTTPS接続から鍵のピニングまで、これらの慣行は、転送中および保管中のデータを保護する厳しい要件に準拠しています。

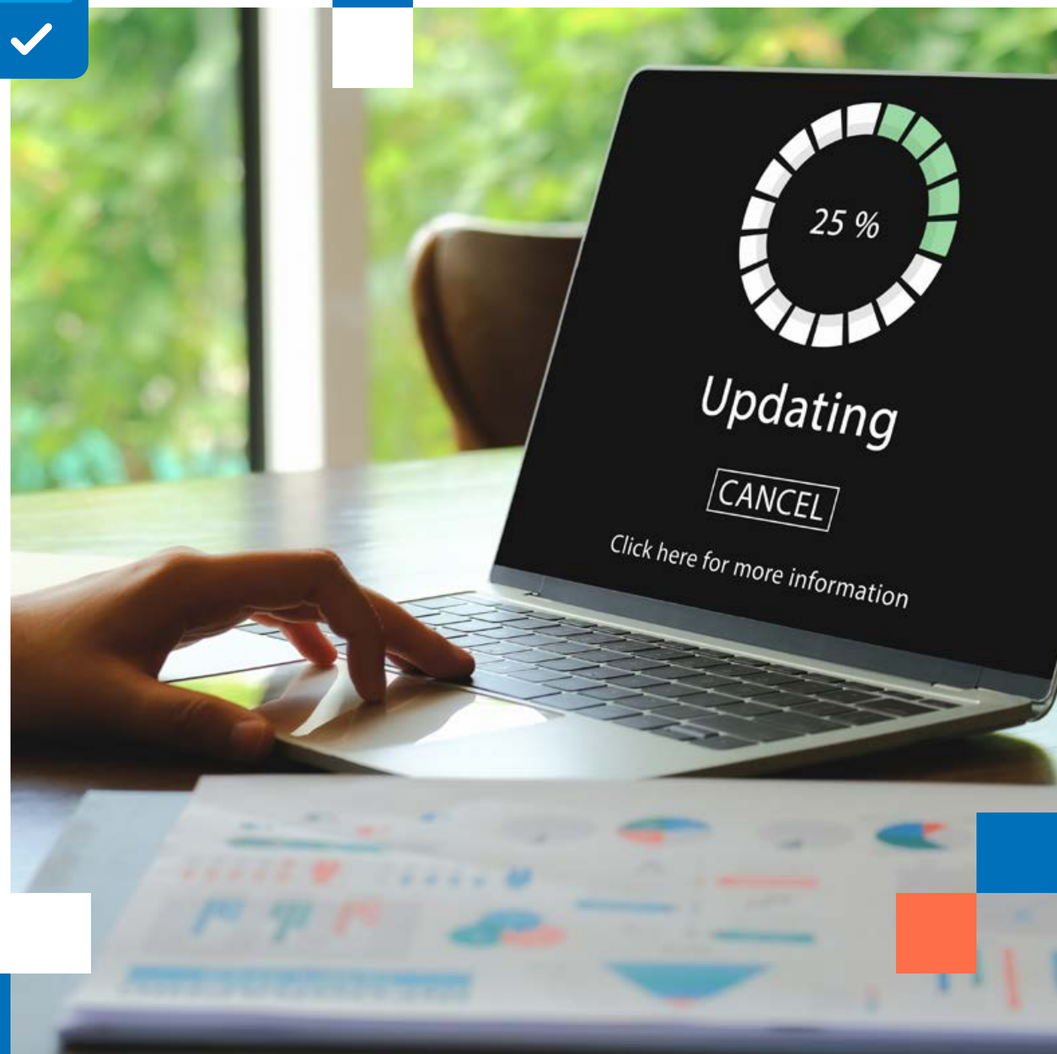
11. Insurance Business Magazine、Ten ways to protect your business from cyber attacks、2021年3月20日。

4 ソフトウェアをアップデートして セキュリティを高める

最新版ではないソフトウェアの場合、サイバー犯罪者がシステムに侵入しやすくなります[12]。ここでは、サイバー犯罪に対して知らないうちに侵入経路を作ってしまわないようにする対策をご紹介します。

オペレーティングシステム(OS)を最新の状態に保つことは、ビジネスを保護を高めるシンプルで効果的な方法ですが、95%のウェブサイトはいまだに既知の脆弱性を持つ最新でないOSを使用しています[13]。OSプロバイダーは、最新の脅威、ウイルス、マルウェアに対応するために、継続的にセキュリティパッチのアップデートを行っています。多少OSをアップデートするだけでも、企業のセキュリティを高める大きな効果があります[12]。

最新のソフトウェアの脆弱性を狙った攻撃を防ぐには、ビジネスグレードのマルウェア対策ソフトウェアやスパイウェア対策ソフトウェアを導入することも有効です。これらのソフトウェアは定期的にアップデートしておく必要があります[14]。無料のソフトウェアや限定的なソフトウェア、消費者向けのソフトウェアでは、機能やビジネスニーズへの対応が不十分であり、長期的にはそのツケを払うことになる可能性があることにも注意が必要です。



12. Business 2 Community、Top 5 Risks of Using Outdated Software in Your Company、2021年6月14日。 **13.** Cybernews、95% of websites run on outdated software with known vulnerabilities、2021年3月18日。
14. Business 2 Community、6 Ways to Keep Your Business Data Safe、2021年10月26日。

5 盲点を把握して サイバー防御力を高める

サイバー犯罪者は新時代の泥棒であり、テクノロジーとイノベーションを活用する方法を知っていますが、従来のスリのように標的の盲点を突きます。例えば、ゲームや暗号の空間でインターネットトラフィックが急増したとき、リスクチームがトラフィックの急増に圧倒されて、すべての不正行為を捕捉できないことを理解しています[15]。

サイバー犯罪者は高度な戦略を駆使して巨額の利益を生む攻撃を行うため、情報を集めて備えることが重要です。自らの脆弱性を知り、サイバー犯罪を過小評価しないようにしましょう。

ブラックフライデー、サイバーマンデー、シングルズデーなど、トラフィックが増加するシーズンのショッピングイベントは、多くの企業の弱点です。売上は急増しますが、注意力も散漫になっており、サイバー犯罪者はそのことが自分たちに有利に働くことを理解しています。

一方で、トラフィックが異常に少ない場合も盲点を突かれやすくなります。新型コロナウイルスの影響で運輸部門のトラフィックが大幅に減少した際、サイバー犯罪者は休眠中の顧客アカウントを狙ってポイントや支払いデータを盗みました[15]。

繁忙期には適切に保護を行えば安心して利益が得られます。事業が停滞している時期は、詐欺に対するガードを固めることで、不正利用者への対策を整える機会になります。

15. Sift、Exposing the Multi-billion Dollar Fraud Economy、2021年第1四半期。

ペイパルで
サイバーセキュリティを強化

eコマースやサイバー犯罪の増加に伴い、サイバーセキュリティは世界中で注目を集めています。不正利用がますます巧妙化し、流行する中で、信頼できる決済パートナーの存在は、もはや「あればいい」ではなく「なくてはならない」ものになりました。ペイパルの強力なネットワークは、1日に1,000万件以上の決済を安全に処理しており、取引を重ねるごとに強化されています。
世界中で安全に自信を持って販売するために必要なツールを手に入れましょう。

今すぐ始める →