CYBER
THREAT
ANALYSIS

Recorded Future®

Payment Fraud Intelligence

January 21, 2025

年次不正支払いインテリジェンスレポート：2024年

窃取されたデータの数は2024年に急増しました。脅威アクターは、不正に取得されたカード2億6,900万枚と小切手190万枚分のデータを有償販売または無料で投稿し、カードデータを盗む新たなeスキマー感染がこれまで以上に多く見つかりました

脅威アクターがデジタルウォレットを詐欺に使用することが増えています。セキュリティメカニズムを不正実行メカニズムとして活用し、ソーシャルエンジニアリングとワンタイムパスワードの傍受がそれを支援します。

アメリカでは、小切手詐欺が根強く残っています。それでも、不正対策インテリジェンスの新たな改善とビジネスの優先順位の再調整により、金融機関は小切手詐欺への対策を強化することができます。

エグゼクティブサマリー

2024年の不正の脅威の状況と、2025年の課題を示すワードとして「進化」があげられます。Recorded Future® Payment Fraud Intelligenceデータの分析によれば、2億6,900万件のカード記録がダークウェブとクリアウェブのソースに掲載され、2024年以降に190万件のアメリカの銀行小切手が盗難されたことが示されています。一方、Recorded Futureのマーチャントデータセットからは、詐欺を目的とした詐欺マーチャントアカウント、正規の電子商取引ウェブサイトからデータを盗むMagecartのeスキマー感染、不正なカード検証活動に悪用される「テスター」マーチャントの増加が明らかになりました。最も厄介なのは、Recorded Futureによるダークウェブのソースに関する観察において、脅威アクターの間で、最新の決済セキュリティ技術の弱点を受け入れて悪用したり、さらには詐欺に利用したりすることに対する意欲が広く見られることが示されたことです。この調査結果は、多数の不正ワークフロー、詐欺作戦、eスキマーグループの分析によって裏付けられました。これらの要因は、脅威アクターが詐欺を実行するために、詐欺を防止する信頼性確保システムやテクノロジーの悪用にシフトしている姿勢を示している可能性があります。AI（人工知能）の実現と洗練されたソーシャルエンジニアリングによる戦術は、脅威アクターがこうした変化を起こすのに大方役立っています。

これらの傾向などにより、金融機関、マーチャント、決済サービスプロバイダー、電子商取引・銀行業界のその他組織の金融詐欺リスクが高まりました。これらのリスクを軽減できうる緩和策には、まず1つ目に顧客のオンボーディングと検証プロセスの厳格さを高めること、2つ目にサイバーセキュリティ資産と不正防止資産を調和させて不正行為をより効果的に防止するフュージョンインテリジェンスの成果物フィードバックループを組み込むことがあります。これらの成果を達成するための具体的な戦略については、本レポートの軽減策セクションで詳しく説明しています。

今後を見据え、2025年については3つの主要な予測が挙げられます。

- 特に詐欺グループがキャッシュアウトスキームのためにデジタルウォレットを優先する中、デジタルeスキミングと詐欺電子商取引が2025年にデータ侵害事象を引き起こすでしょう。
- Telegramなどのプラットフォームが経験の浅い脅威アクターの主戦場となる中、ダークウェブマーケットプレイスは決済詐欺エコシステムの中心的存在であり続けるでしょう。
- 過去3年間にアメリカで見られた小切手詐欺の爆発的な増加は今後も続くでしょうが、小切手詐欺の防止方法を改善することで、金融機関は小切手詐欺の損失をより効果的に低減することができます。

主な調査結果

- **Magecart**の**e**スキマーは、データ窃取に対して高い有効性を維持しました。2024年には、CVE-2024-34102（以下「CosmicSting」）発見後の感染量の急増、脅威アクターの技術的障壁を下げるeスキマーキット、MagecartのTTP（戦術、技術、手順）の継続的な開発という3つの主要要因がMagecartの脅威の状況を定義しました。全体として、eスキマーに感染した独自のeコマースドメインの数は昨年の約3倍に増加しました。
- **2024**年、詐欺電子商取引ウェブサイトはますます顕著な脅威となっています。本年、詐欺マーチャントアカウントのネットワークにリンクされた約1,200件の詐欺ウェブサイトドメインを特定しました。Recorded Futureが発見した詐欺マーチャントアカウントのほとんどはイギリスと香港で登録されており、詐欺のTTPは年々巧妙かつ高度に進化しています。
- 特定された**CPP**（共通購入地点）の傾向からは、脅威の状況の進化が見られます。侵害元としては飲食店が依然として突出しており、Recorded Futureの調査では、プラットフォームの侵害がeコマース業界に引き続き与える大きな影響が浮き彫りになりました。同時に、アパレル店舗での侵害がますます一般的になっていますが、この傾向は主に詐欺ウェブサイト数の増加によって引き起こされています。
- ダークウェブソース上での盗難カードデータ量の急増は、盗難カードとカード所有者のデータの利用可能性の高まりを広く示しています。2024年、脅威アクターの販売用カード記録投稿数は、2023年と比較して7,000万件増加しました。これが今年の販売用盗難データ急増に大きく影響しているかどうかは不明ですが、この増加は、再投稿頻度の増加とデータ侵害イベントの両方を反映している可能性があります。カードデータの中では、効果的なCP（カード提示）詐欺ワークフローが続く中でも、CNP（カード非提示）データが引き続き優勢です。
- **Telegram**は無料のユニークカードデータのソースとして引き続き活況です。Pavel Durovの逮捕後、Telegram上の一意でないカードデータの量は減少しましたが、Telegramは依然として信頼できる一意データのソースであり、脅威アクターが同プラットフォーム上で活動を続ける可能性が高いことを示唆しています。
- ダークウェブでのカード検証活動は**2024**年に増加し、マーチャントカテゴリーの傾向には、脅威アクターがテスターマーチャント悪用に使用した可能性のあるアクセス方法が反映されています。ダークウェブチェッカーサービスは前年よりも多く観察されました。テスターマーチャント全体の3分の1は5つのマーチャントカテゴリーのいずれかに属しており、これは脅威アクターがテスト活動にマーチャントを悪用するために使用したアクセス方法を反映している可能性があります。一般的に、チェッカーは、検出回避の可能性を低めるため、非連続的な短期間にわたってテスターマーチャントを悪用することを好みました。
- 小切手詐欺の脅威の状況は再投稿の横行と地理的な傾向で定義されました。盗難されたアメリカの銀行小切手190万件がTelegramのソースに売りに出されましたが、このうち約9割は再投稿されたものでした。Recorded Futureは、盗難された小切手の多数がアメリカ東海岸地域に由来するものと特定しています。脅威アクターは支払者からの小切手を特定の州において他州よりも頻繁に再投稿しており、これらの州では盗まれた小切手に対する脅威アクターの需要が高まっている可能性があることを示唆しています。
- **2024**年のダークウェブにおける詐欺の状況は高度化が進み、不正行為防止技術やプロセスの機会と限界を利用しようとする意欲の高まりによって定義されました。脅威アクターの言説では、セキュリティ重視の金融テクノロジーを悪用したワークフロー、微妙な検証のバイパス、複雑なマネーロンダリングサービスや戦術への着実な依存が見られます。

目次

脅威分析

金融機関にとって、詐欺は厄介なものです。Recorded Futureでは、この課題を例えて城のジレンマと称しています。CTI（サイバー脅威インテリジェンス）チームとサイバーセキュリティ資産には直接的な攻撃から組織（城）を保護するための優れた設備がありますが、CTIチームは不正行為防止チームが顧客を保護できるようにする上で課題に直面しています。このジレンマを乗り越えるために、CTIチームと不正行為防止チームは秩序あるインテリジェンスフィードバックループを採用し、経営陣からの支援を受けて、不正行為を効果的に防止し、顧客を保護し、組織のレピュテーションを保護する必要があります。

近年、金融機関は、この城のジレンマを克服し、より効果的な不正防止措置を可能にするために、CTIと不正対応を融合させた取り組みを強化しています。2024年、これらの融合した取り組みの成功による選択的圧力は、詐欺グループの高度化と生産性の向上に最も顕著に現れました。年間を通じ、実証済みの多くの不正対応TTPは、お客様からのフィードバックや本レポートで説明している脅威調査が示すように、効果的であった可能性があります。同時に、2025年の詐欺の脅威の状況を描く2つの明確な新しいパターンが浮かび上がってきました。

- 脅威アクターは、顧客の利便性とセキュリティ向上のためにマーチャントや金融機関が設置したシステムを熱心かつ効果的に悪用しました。脅威活動からは、不正防止メカニズムを不正実行メカニズムへと変換する意欲が高まっていることを示しており、これは城のジレンマを根底から覆すものです。
- 脅威アクターは、ソーシャルエンジニアリングを流動的に活用して、サイバー対応の技術的な詐欺攻撃チェーンのギャップを埋めています。上流のCTIにより、不正対策チームが最新の不正行為の課題に取り組む力が生まれるのと同様に、ソーシャルエンジニアリングは不正攻撃チェーンの弱点を埋め、その中断点を最小限に抑えることができます。

本レポートでは、2025年に起こることをより深く理解するために、2024年に進化をみせた不正行為の脅威の状況をプロファイリングします。本レポートの調査は、金融機関、カードネットワーク、決済サービスプロバイダー、マーチャント、銀行および電子商取引業界のその他の事業体が、タイムリーで実用的なアップストリームインテリジェンスを使用して不正を事前に検出・防止することを可能にする製品データセットの分析に基づいています。また、Recorded Futureの調査には、オープンソースの情報と、ダークウェブソースに関する脅威アクターの言説の分析も組み込まれています。本レポートに掲載されているすべての調査は2024年1月6日時点のものです。

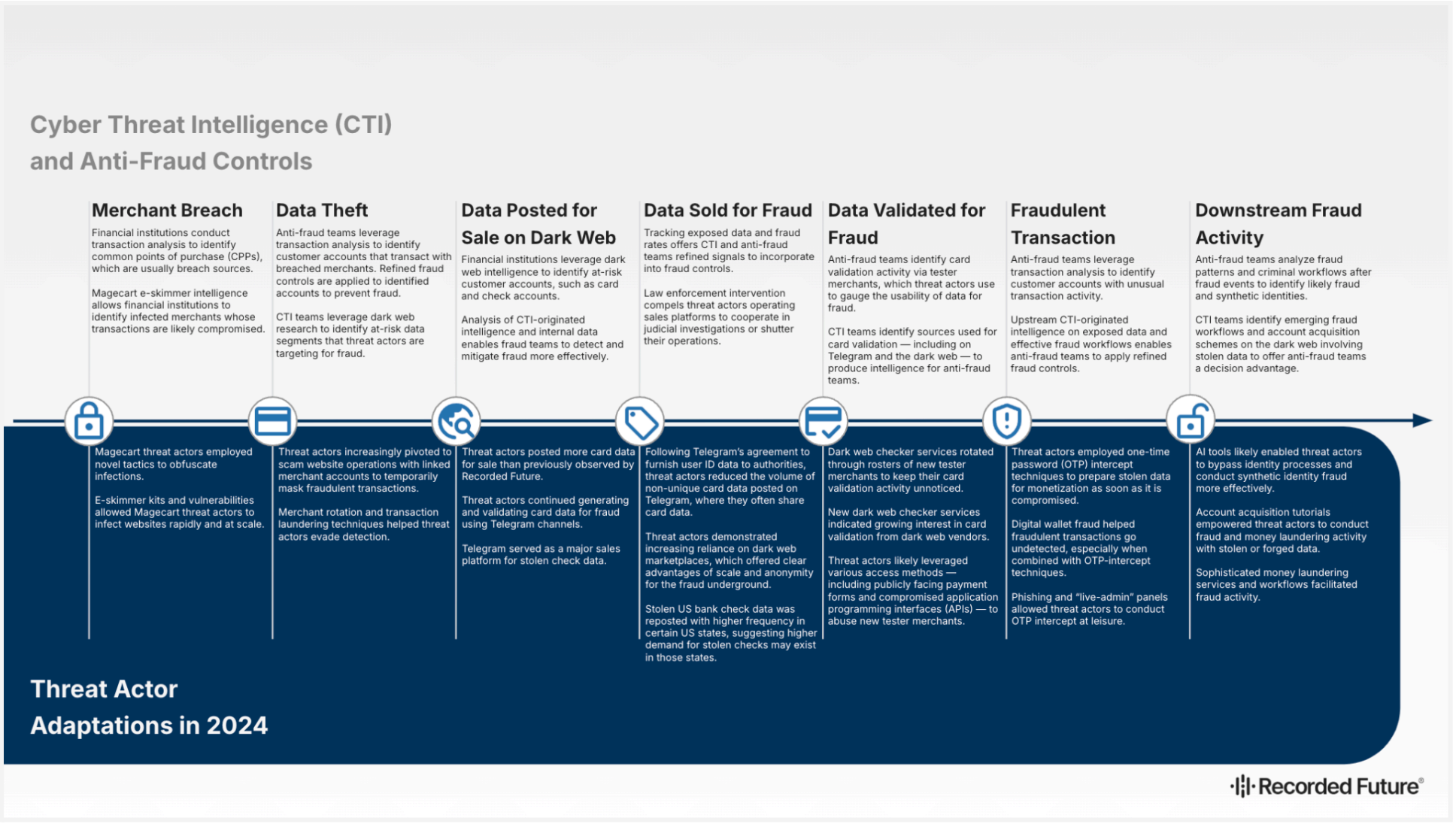


図*1*:*2024年のRecorded Futureの調査では脅威アクターが金融機関の不正対策戦略にどう先んじているかについての洞察が明らかに*(出典:*Recorded Future*)

Magecartのeスキマー感染は新しい脆弱性と新eスキマーキットの登場、新戦術の開発を受けて急増

2024年を通じ、Magecartのeスキマーは明らかにデータ盗難の方法として効果的であり続けました。新たに検出されたeスキマー感染に苦しむ一意のeコマースドメインの合計数は2023年から約3倍に増加し、11,000件に近づき、単年の数値としては過去最高となりました。Magecartのeスキマー感染は、電子商取引ウェブサイトを標的とする脅威アクターがこうしたサイトにマルウェアを埋め込み、チェックアウトページの決済フォームから顧客データを盗む際に発生します。eスキマーの感染は、感染したウェブサイトで取引を行う被害者の金融詐欺のリスクを高めます。

本年にMagecartの脅威の状況を再定義した主要な要因は3つありました。

- 2024年10月以降、Adobe CommerceやMagentoを利用したECサイトに影響を与える新たな脆弱性「CosmicSting」（CVE-2024-34102）により、感染数が急増
- 脅威アクターが「すぐに使える」eスキマーキットの利点を活用することで、技術的な専門知識が不足しているMagecart運営者の参入障壁が低下
- MagecartのTTPは開発を続け、より高度で検出不可能で生産性の高いMagecartのeスキマー感染に貢献

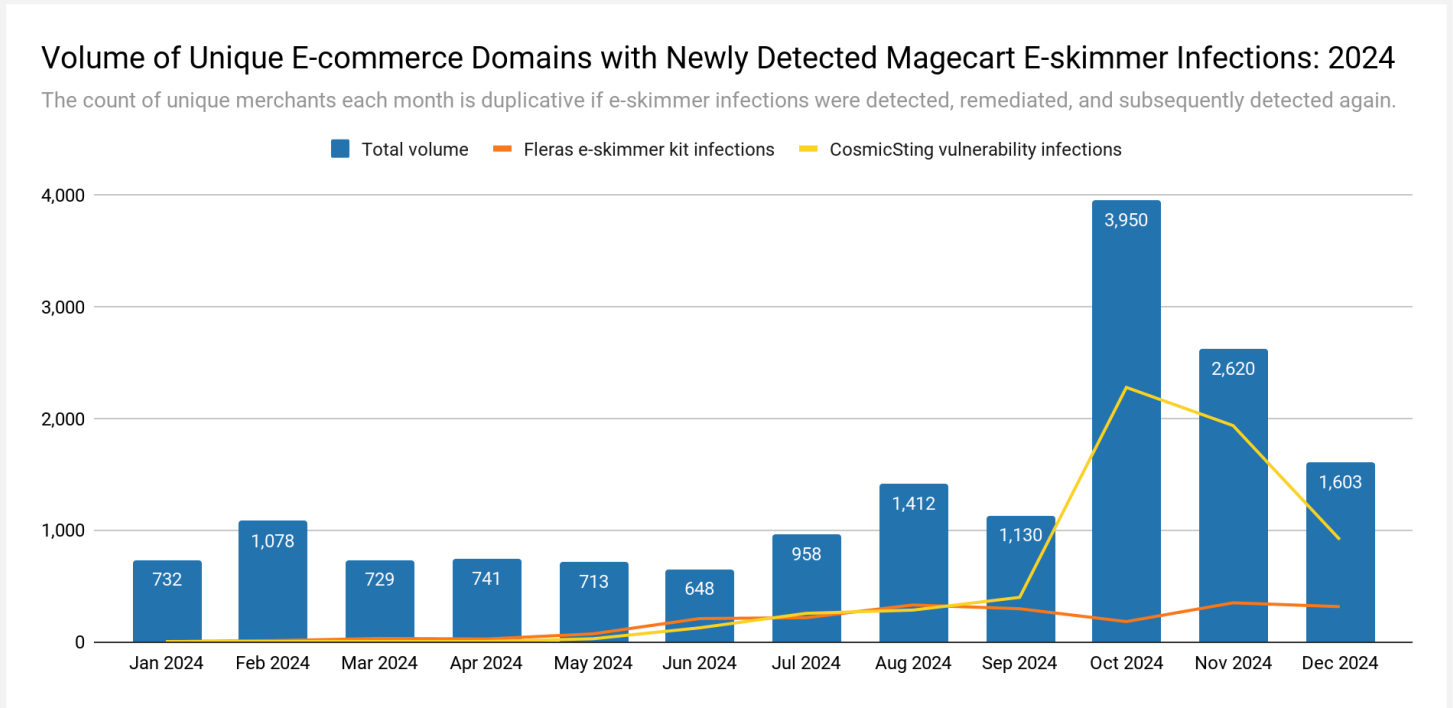


図*2*：eスキマーキット、特に「*Sniffer by Fleras*」に依存した*Magecart*の*e*スキマー感染が合計感染数に占める割合は*CosmicSting*によって合計感染数が急増した*2024*年*10*月まで拡大（出典：*Recorded Future*）

*2024*年後半には*CosmicSting*が*Magecart*の脅威の状況を再定義

2024年後半、Recorded Future独自のMagecart eスキマースキャナーMagecart Overwatchは、脅威アクターが新たに特定された脆弱性であるCVE-2024-34102（別名CosmicSting）を広く悪用した結果、Magecart

の感染数が前例のない水準で増加していることを検出しました。Adobeは、2024年6月にCosmicStingを米国のNational Vulnerability Databaseに提出しました。2024年7月までに、Sansecはこの脆弱性の大規模な悪用を観測しています。

2024年10月以降、CosmicStingにより感染の検出数は大幅に増加しました。これ以降、この脆弱性によって感染したeコマースドメインの侵害の指標（IOC）は急速に変化しており、Magecartのオペレーターが脆弱なウェブサイトで競合するMagecartグループの感染を徐々に排除していることを示唆しています。これは、電子商取引ウェブサイトの管理者がCosmicStingの脆弱性にパッチ適用していないことも示しており、悪意のあるアクターは引き続きこの脆弱性を悪用してウェブサイトにアクセスできます。

主要*e*スキマーキットの採用が広まるにつれ、*Magecart*脅威アクターの技術的障壁が低下

脅威アクター「Fleras」が開発・販売する堅牢なeスキマーキット「Sniffer by Fleras」を使用した新しいMagecart eスキマー感染は、年初の導入以来、2024年9月までに新規感染全体の25%を占めるまでに成長しました。これは、このeスキマーキットが技術的な専門知識を持たないMagecartの脅威アクターに提供するスケールと展開の利点を示しています。Sniffer by Flerasについては、脅威アクターが一斉にCosmicStingを悪用し始めた10月まで、すべての感染に比例してかなりの使用が見られました。

Sniffer by Flerasは今年最も顕著なeスキマーキットとなりましたが、他のキットも広く使用されました。R3ninキットは簡素化されたコマンド&コントロールパネルが評価されており、2023年の作成者失踪にもかかわらず、引き続き使用されました。InterKitはMagecartグループの間で主力であり続け、そのソースコードは多くのeスキマー感染で一般的になっています。

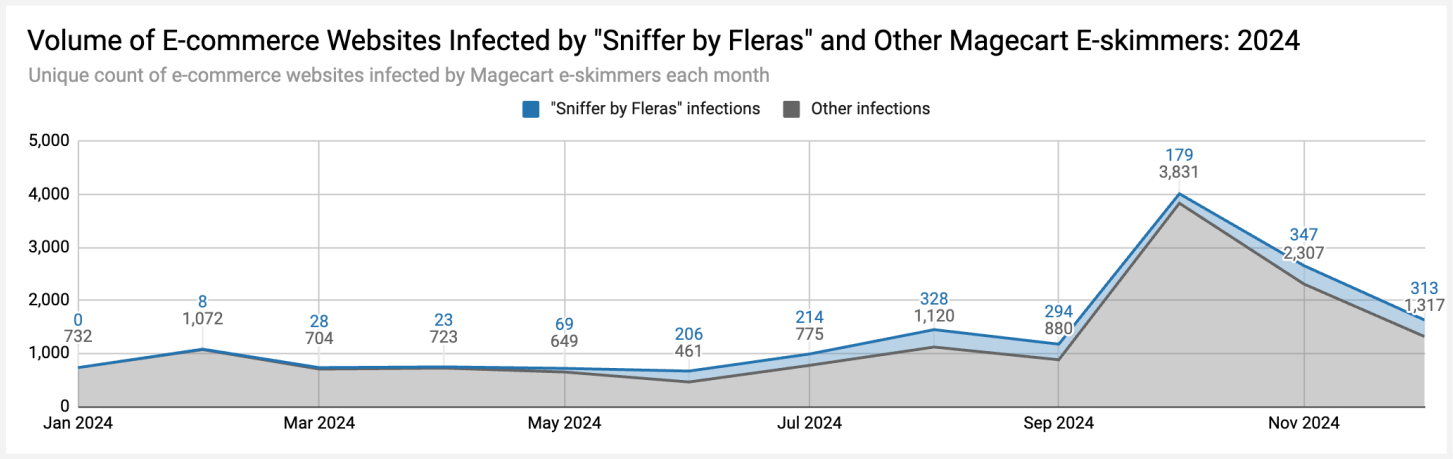


図*3*：今年の「*Sniffer by Fleras*」の感染数は*e*スキマーキットのもたらす利点を反映（出典：*Recorded Future*）

*Magecart*の*TTP*は進化を続け、不正行為の影響を強化

Recorded Futureの分析によれば、2024年にMagecartグループの間で新たに出現したTTPが効果的であった可能性が高いことがわかりました。これらのTTPは、Magecart運営者の巧妙化が進み、その影響が増大していることを示します。最終的には、Magecartのeスキマーが感染した電子商取引ウェブサイトの決済フォームから顧客データをより効果的に窃盗できるようになります。

- **OTP**インターセプト：Magecartグループ「OTPExplorer」は、eスキマー感染において被害者のOTP（ワンタイムパスワード）を傍受する新たな技術を組み込んでおり、モバイルウォレット詐欺を支援します。

Magecartの脅威アクターの間でこのような手法が観察されたのは今回が始めてです。ダークウェブの言説を分析したところ、詐欺やフィッシングサイトの運営者が同様の手法を使用した場合、成功率が高くなることが示されています。

- 高度な難読化：Magecartグループ「Shablon」は、検出回避のための新しい難読化技術を採用しました。この手法では、ランダムに順序付けられたアルファベットを変数に解凍し、それらを組み合わせてキーワードやその他のスクリプト要素を再構築します。
- 標的のカスタムペイロード：Magecartグループ「Dispatcher」は、リレーと通信するローダースクリプトを使用して、別々の攻撃者ドメインでホストされているeスキマーペイロードを取得し、リレーが標的となる電子商取引ウェブサイト用に特別に構築されたeスキマーを急送できるようにしました。これらのリレーはリファラーヘッダーを使用して被害ウェブサイトを特定し、送信するeスキマーを決定した可能性があります。

新しいMagecartのTTPも出現していますが、確立されたTTPも引き続き有効であるようです。

- 正規サービスの悪用：Magecartグループ「ADSWG」は、公開されている2つのWebサービス（Google Tag Manager（GTM）とAmazon CloudFront）を攻撃インフラストラクチャとして悪用しました。このグループのeスキマーは、ローダースクリプトを収容するGTMコンテナを使用して、Amazon CloudFrontディストリビューションサブドメインでホストされているeスキマーURLを感染したeコマースウェブサイトに注入しました。この正当なインフラストラクチャの悪用により、ADSWGはオンラインジュエリー小売業者向けの電子商取引プラットフォームを標的としたプラットフォーム侵害を達成できた可能性があります。ADSWGと同様に、Magecartグループ「FakejQuery」は、標的となったマーチャントの感染した電子商取引ウェブサイトのメインページにトロイの木馬化されたGTMコンテナへのリンクを埋め込みました。
- 正当な電子商取引ドメインの悪用：Magecartグループ「Megaebun」は2024年も活動を続けました。多くの場合、Megaebunの感染は、正規の電子商取引ウェブサイトに属する侵害された「攻撃キャリア」ドメインでホストされているeスキマーURLを使用していました。

マーチャントアカウントがリンクされた詐欺ウェブサイトは脅威として急成長

2024年には、特定された詐欺ウェブサイトの膨大な数、リンクされたマーチャントアカウント、詐欺ウェブサイトのTTPの巧妙化と高度化の進展が示すように、詐欺の脅威としての詐欺ウェブサイトの地位がより顕著になりました。この傾向は、詐欺サイトの運営者が被害者を騙すことに成功していることからも明らかです。Better Business Bureauの報告によると、2024年6月現在、被害者がオンラインショッピング詐欺に引っかかる傾向が強まり、詐欺による金銭的損失が増えていることが報告されています。マーチャントアカウントがリンクされ、決済ベースのキャッシュアウトメカニズムを持つ詐欺ウェブサイトの脅威が増大していることは、ソーシャルエンジニアリングとセキュアな決済技術により、詐欺防止の防御を回避できるという脅威アクターの認識が高まっていることを示しています。

自社の顧客が詐欺電子商取引ウェブサイトの被害を受けている金融機関の場合、詐欺ウェブサイトにリンクされたマーチャントアカウントを検出してブロックリストに登録するだけでは、解決策としては不十分でしょう。詐欺マーチャントアカウントを組み込んだ詐欺電子商取引ウェブサイトは、脅威アクターが、最初は詐欺ウェブサイトでの即時の不正取引を通じ、次に下流の詐欺取引やダークウェブソースでの取引データの販売を通じた「二重の収益化」を達成できるようにします。

*2024*年の詐欺マーチャント登録はイギリスと香港で最多

今年特定された詐欺ウェブサイトの半数以上はイギリスに拠点を置くマーチャントアカウントを使用しており、詐欺マーチャントのおよそ2割は香港に拠点を置いていました。一意のマーチャント名767件と、一意のMID（マーチャント識別番号）474件を使用してマーチャントアカウントにリンクされた詐欺ウェブサイトの合計1,191件を特定しました。

脅威アクターは、多くの場合、詐欺マーチャントアカウントを詐欺ウェブサイトのクラスターにリンクします。2024年、そのような詐欺マーチャントアカウントの 1つは、マーチャント名に「JUYUE」を組み込み、MID「3792972NCoYlu50」を使用していました。Recorded Futureでは、2024年9月にダークウェブマーケットプレイスに売り出された4,000件以上のCNP（カード非提示）記録にJUYUEを関連付けました。当社の調査では、MalwareTipsがこの詐欺ネットワークを独自に報告する3日前の2024年8月27日までに、複数の詐欺電子商取引ドメインにJUYUEに紐づけました。

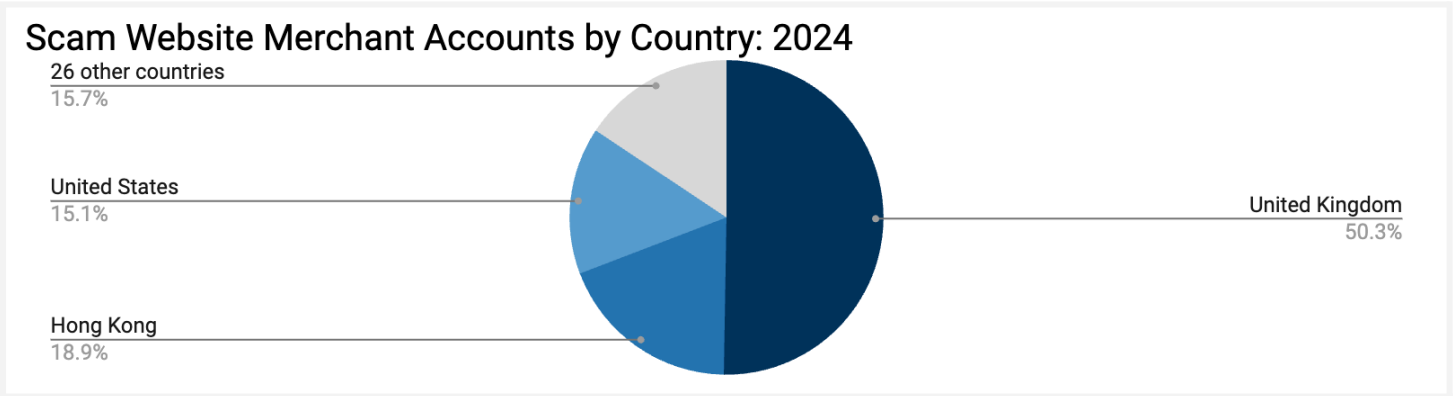


図*4*：*2024*年に特定された詐欺業者の約*4*分の*3*がイギリスまたは香港で登録（出典：*Recorded Future*）

巧妙化と高度化の進む詐欺サイトの*TTP*

今年、主要な詐欺ウェブサイトの運用では、加盟店にリンクされた詐欺ウェブサイトの運用がますます巧妙化していることを象徴する戦術が使用されました。

- 検出を回避するための被害者スクリーニング：「ERIAKOS」は、モバイルデバイスを使用しているかどうか、ソーシャルメディア広告ルアーを介してウェブサイトにアクセスしたかどうかに基づき、詐欺ウェブサイトへの訪問者をスクリーニングしました。これは、オンライン広告サービスの静的検出ルールによる検出を回避することを狙ったものと考えられます。詐欺ウェブサイトの運営によくあることですが、ERIAKOS詐欺ウェブサイトにリンクされた広告ルアーは、ブランドのなりすましやマルバタイジングを使用してソーシャルメディアネットワーク上で被害者を誘引していました。
- **OTP**インターセプト：OTPExplorerと同様に、脅威アクター「Chenlun」が運営する詐欺ウェブサイトキャンペーンに関連する脅威アクターは、OTPインターセプト手法を使用して、リアルタイムの不正なデジタルウォレットプロビジョニングの試行を促進することに成功しました。このグループに関連する攻撃は多段階であり、スミッシング通信と詐欺ウェブサイトを組み合わせて被害者のデータを盗み、被害者を騙すというもので、以前のChenlunに関連する作戦では、郵便局のウェブサイトをモデルにした詐欺ウェブサイトを使った戦術が成功しています。
- 2024年後半、MailTzz詐欺ウェブサイトネットワークは、リンクされたマーチャントアカウントの使用からフィッシングベースの**OTP**インターセプト技術に移行し、詐欺運営者による盗難カードデータのデジタルウォレットへの不正プロビジョニングも可能にしました。この戦術的な転換は、デジタルウォレットを中核的なキャッシュアウトメカニズムとして戦略的に方向転換する中で発生しました。
- トランザクションロンダリングとマーチャントローテーション：2024年には、詐欺運営者の間で、検出を回避するためにトランザクションロンダリングとマーチャントローテーションへの依存度が高まっていることが判明しました。トランザクションロンダリングとマーチャントローテーションにより、こうした運営者は、無関係なウェブサイトを通じて取引をリダイレクトすることで不正トランザクションを不明瞭にし、リスクの高い取引を隠蔽できます。

詐欺ウェブサイトの脅威の状況の進化にもかかわらず、詐欺ウェブサイトの運営者は2024年、作戦の準備と実行において、季節的な機会に対する並外れた感度を示し続けています。詐欺電子商取引ウェブサイトは、多くの場合、季節的な機会を利用して被害者の感受性の増加を利用し、通常は架空のプロモーションオファーを通じて緊急性を煽ります。2024年11月、Visa Payment Ecosystem Risk and Controlは、詐欺ウェブサイトの数が前の4か月と比較して284%に増加したことを特定しました。2024年12月、TransUnionは、サンクスギビングとサイバーマンデーの間に行われた取引の4%以上に詐欺の疑いがあることを示しました。これは、詐欺活動とより一般的な不正行為の両方によって引き起こされた可能性が高いです。

CPP分析により強調される確立された侵害と新たな侵害の傾向

金融機関による取引分析を通じ、被害者の金融データや個人データの流出源となることが多いCPP（共通購入地点）を特定し、分析することができます。2024年、Recorded Futureは提携金融機関と協業し、788件の一意のCPPを特定しました。

2024年を通じてCPPの傾向を分析した結果、脅威の状況が進化していることが判明しました。データからは、侵害されたマーチャントとしては飲食店が多数であることや、小規模な侵害と比較してプラットフォームの侵害によってもたらされる脅威が高まっていることなど、長年見られる傾向が依然として顕著です。同時に、CPPの中でアパレル店舗が目立つようになった点は、特定された詐欺マーチャントのCPPの増加によるところが大きく、年間を通じた脅威アクターの詐欺ウェブサイトへのシフトを浮き彫りにしています。

CPPマーチャントのカテゴリーとして飲食店が占める割合は、主にアメリカにおける不正行為の傾向を反映したもので、レストランやバーは依然としてカード提示型の侵害に対して脆弱です。こうした脆弱性は、サーバーが顧客の目の届かないところで顧客のカードを取引するために使用する、レストランやバーの集中型POS（販売時点情報管理）システムから発生します。こうした仕組みから、悪意のあるスタッフがポケットスキマーを使用してカードデータを盗む機会が生まれます。今年目立った点としては、2024年のCPPの中でアパレル店舗が優勢となったことが挙げられますが、これは詐欺電子商取引の傾向に牽引されたものです。詐欺ウェブサイトは、多くの場合、割引価格で衣料品を販売していると主張しています。2024年には、MCC（マーチャントカテゴリーコード）5621で特定されたすべてのCPPの38%と、MCC 5691で確認されたすべてのCPPの39%のマーチャントで詐欺行為が確認されています。

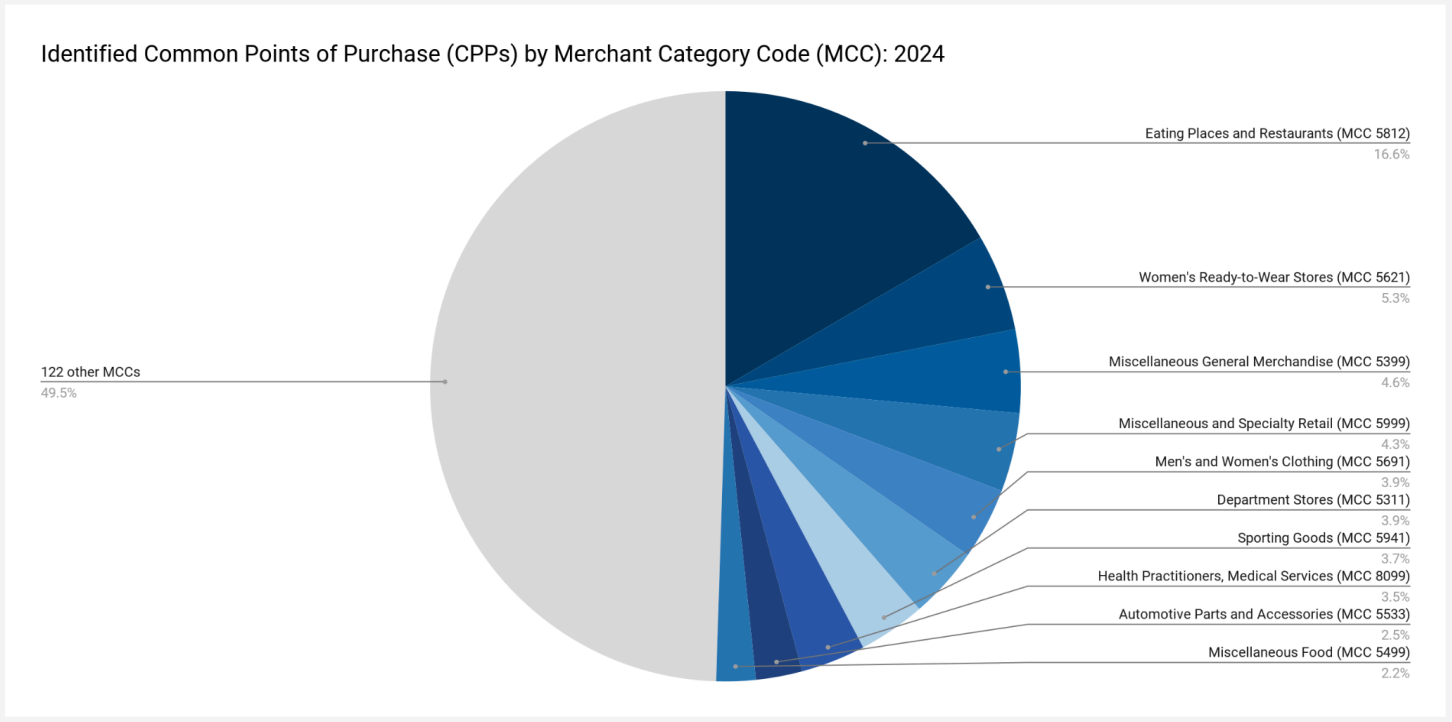


図*5*：今年の*CPP*は飲食店が多数も、詐欺の傾向によりアパレル店舗が*CPP*件数で*MCC*の上位*10*位入り（出典：*Recorded Future*）

CPPの中では、プラットフォーム侵害が2024年も引き続き電子商取引に大きな脅威をもたらしました。プラットフォームの侵害は、複数のマーチャントが使用する電子商取引プラットフォームの侵害により、そのプラットフォームを使用するマーチャントとのすべての顧客取引が危険にさらされる可能性があるため、非常に影響が大きくなります。

MagecartのeスキマーデータとCPPデータの分析により、2024年に発生する可能性のある2つの主要なプラットフォーム侵害を特定することができました。

- **2024**年**7**月現在、アメリカを拠点とするジュエリー販売業者向けの電子商取引プラットフォームを使用している電子商取引ウェブサイト**67**件が**Magecart**の**e**スキマーに感染しています。ADSWG Magecartの運営者は、中央集権的なコードリポジトリに感染するか、侵害された管理者の資格情報を使用して手動でマーチャントに感染することで、これらのマーチャントを侵害した可能性があります。
- アメリカを拠点とする飲食店向けの電子商取引プラットフォームが**2024**年後半に侵害された可能性があります。Magecartの脅威アクターは同プラットフォームのコンテンツ配信ネットワークでホストされているファイルにeスキマー感染を注入し、同プラットフォームを使用しているすべての飲食店が侵害の影響を受けた可能性が高いことが示されています。Recorded Futureが金融パートナーと共同で取引分析を行ったところ、本書の執筆時点で、同プラットフォームを使用しているマーチャント約50件がダークウェブ上の販売カード記録にリンクされています。何百ものマーチャントがこのプラットフォームを使用しているように見えることは注目すべきでしょう。

2024年を通じ、無料カードデータと販売用カードデータの投稿件数が急増

被害者のカードとカード所有者のデータの利用可能性は2024年に急増し、2億6,900万件のカード記録がダークウェブとクリアウェブソースに掲載されました。これは特にダークウェブマーケットプレイスで販売されているカードデータに顕著で、2023年と比較して販売されたカード記録の数は7,000万件以上増加しています。2023年から2024年にかけてダークウェブのソース数はほとんど変わらず、売り出された記録の月次件数は一貫して多く、ソース間で分散していることから、ダークウェブのベンダーが盗難されたカードをより多く取得したためにデータ件数が増加した可能性が高いことが示唆されています。

盗難に遭った販売用カードデータの利用可能性が高まった点はこの年の特色と言えますが、急増の影響は依然として不明です。例えば、販売用カードデータの実際の不正行為リスクが、その年の件数急増に見合って増加していない可能性があります。それにもかかわらず、販売用カードデータの利用可能性が高まったのは、カード侵害事象の増加と、カードエコシステム内での再投稿の頻度の増加の両方によるものと思われます。分析によると、他のソースから再投稿または再利用された可能性が高い販売用カードデータの割合は、2023年の19%から2024年には36%に増加し、新規かつ一意と思われるデータの割合は同期間にほぼ倍増しました。

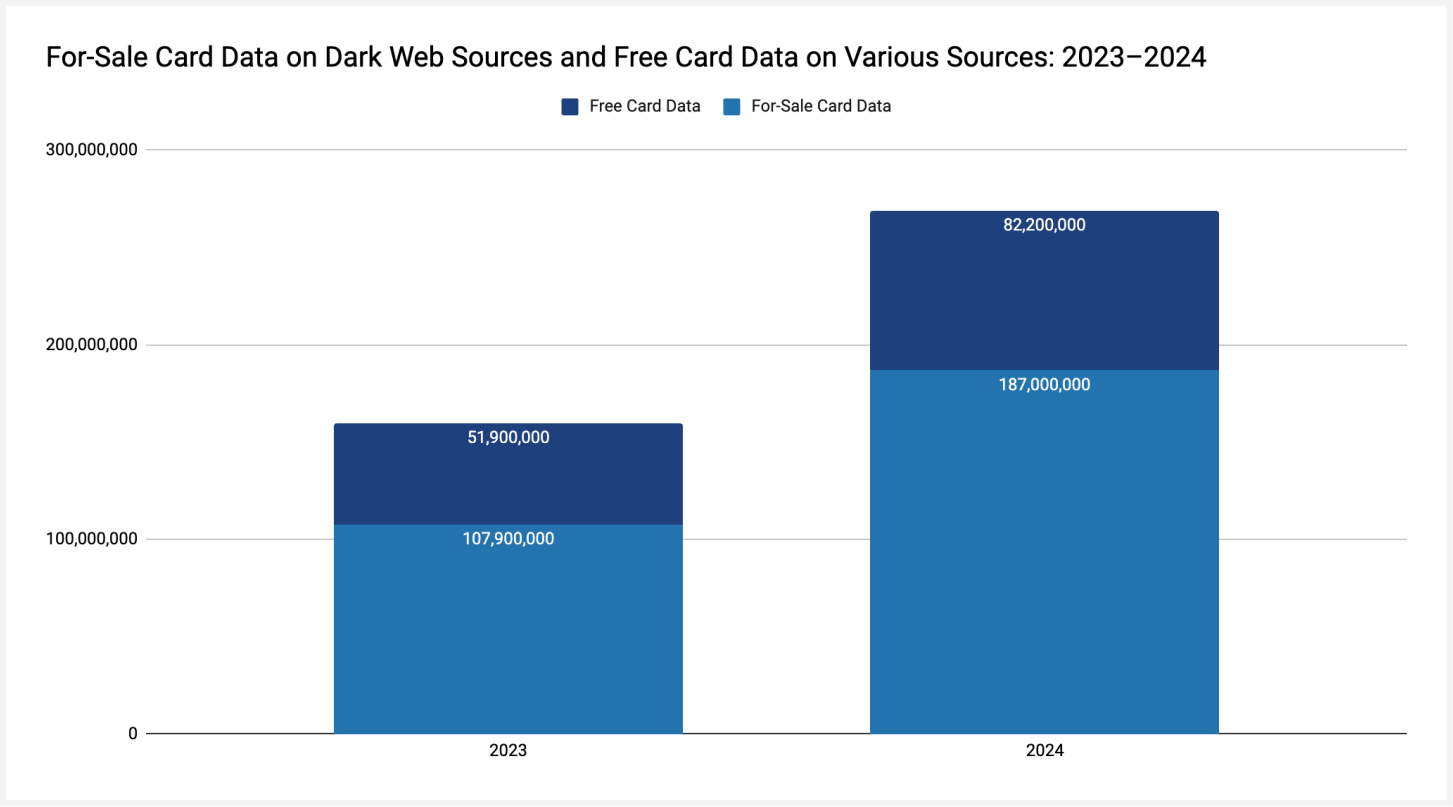


図*6*: *2024*年には無料カードデータと販売カードデータの数量が急増、*Recorded Future*の分析によれば販売カードデータの増加はカード侵害の増加とダークウェブソースへの再投稿の両方による可能性が高いことが示唆（出典：*Recorded Future*）

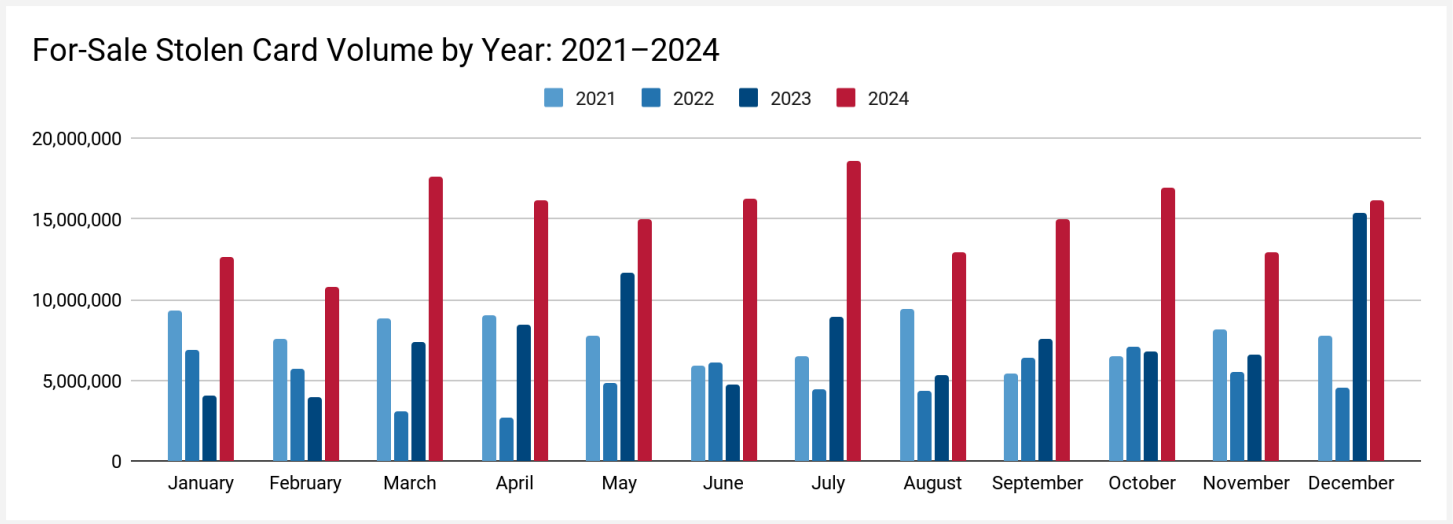


図**7**：ダークウェブソースで売り出されたデータの月次件数は一貫して多く、この年の増加が単にベンダーがより多くのカード記録を盗んだ結果であることを示唆（出典：*Recorded Future*）

CNP取引や悪意のあるオンライン活動（侵害された電子商取引、フィッシング、情報窃取型マルウェア感染など）によって窃取された被害者データは、2024年も引き続き侵害されたカードおよびカード所有者データの大部分を占めています。今年、ダークウェブ上の販売カード記録の約87%はCNPであり、実質的に無料で入手できるカードデータはすべてCNPでした。

物理的なトランザクションセキュリティ技術の向上と近年の小売部門における電子商取引のシェア増加の結果としてCPデータのエクスポージャーは減少していますが、Recorded Futureの分析では、CP詐欺スキームが少ないながらも引き続き機能している可能性が高いことが確認されました。今年、ダークウェブのソースを調査したところ、カードスキミング、カードシミング、POSマルウェア、カードクローニングに関連する複数のCP詐欺ワークフローとサービスが明らかになりましたが、これらは引き続き有効である可能性が高いです。

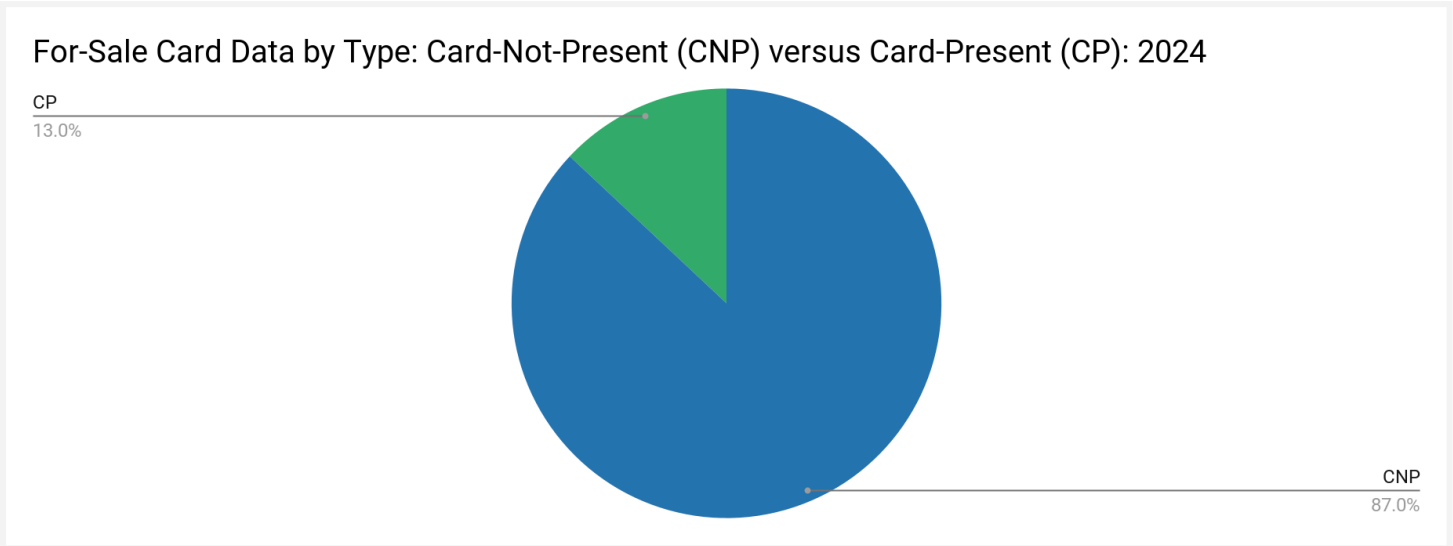
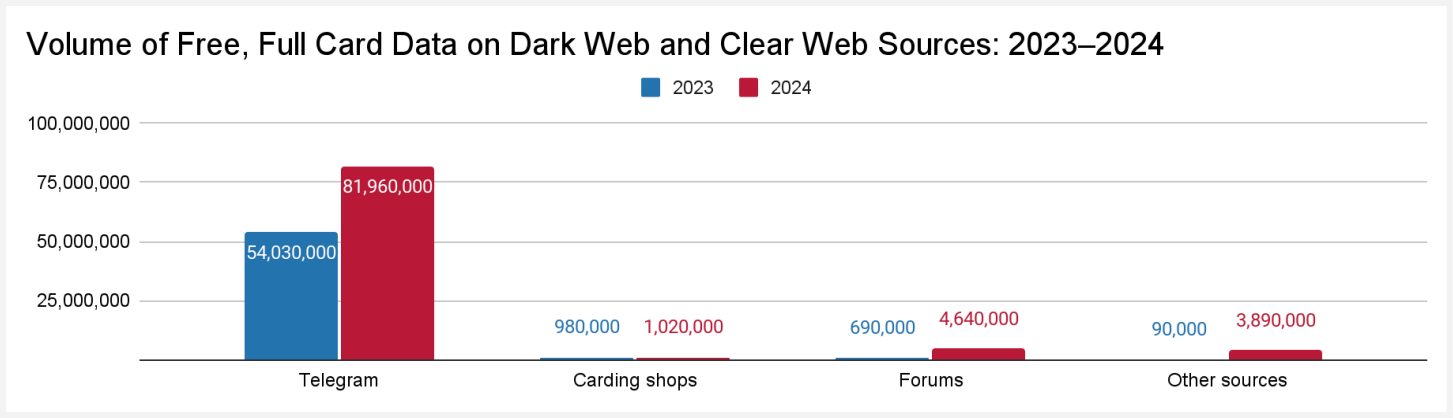


図**8**：*2024*年にダークウェブマーケットプレイスで売り出された盗難カード*8*枚のうち*7*枚は*CNP*取引と悪意のあるオンライン活動によるもの（出典：*Recorded Future*）

今年、法執行機関による犯罪決済インフラの中断に続くダークウェブの瓦解を受け、ダークウェブのカード分野の運営は一時的に混乱に陥りましたが、その回復力も示されました。こうしたインフラの中断は、現在は廃止さ

れたかつて悪名を馳せたダークウェブマーケットプレイスJoker's Stashの運営者であるTimur Shakhmametovの起訴とともに発表されました。その結果、Joker's Stashの閉鎖後、販売用カードデータの主要なソースであったBriansClubは新しいインフラに軸足を移し、その運営を保護するため、オフライン移行を余儀なくされました。BriansClubは1か月の休止期間を経て再開しました。

長年にわたり詐欺を中心とした活動の温床となっているTelegramでは、2024年、無料カードデータのソースの増加が主に見られました。Telegramのソースあたりのデータ量は減少しました。Telegramの創業者であるPavel Durovが逮捕され、その後TelegramがユーザーIDデータを当局に提供することに同意したことが、2024年9月からTelegramのソースに投稿されるカード記録の総数が減少する前兆となりました。Telegramの譲歩を受けて全体的に数量が減少したにもかかわらず、Telegramに投稿された新規かつ一意の記録の総数は安定しており、近い将来もこのソースが詐欺に使用され続ける可能性が高いことを示しています。



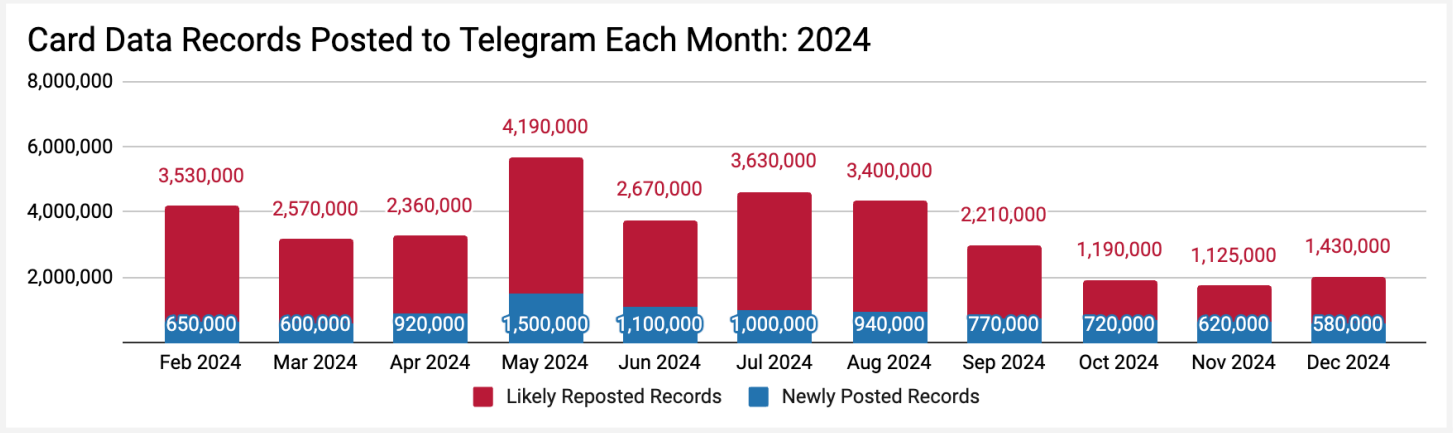


図**9**および図**10**：*Pavel Durov*の逮捕にもかかわらず*Telegram*は*2024*年も引き続きカードデータのソースの地位を維持（上）。*Telegram*の元の無料カードデータ数量は*Pavel Durov*逮捕後の*2024*年9月から減少も、分析によると新規かつ一意のカードデータの量は安定している可能性が高いことが示唆（下）。（出典：*Recorded Future*）

Telegram上の新規かつ一意のカードデータは、脅威アクターがカードデータを生成して検証しようとした結果として作成されることが多くなっています。Telegramソースのカード検証および生成機能は、BIN攻撃とも呼ばれるアカウント列挙攻撃をサポートしています。2024年を通じ、BIN攻撃によると思われる、生成された記録のインスタンスが複数観測されました。ある大規模な例はTelegramチャンネル「Free Worldwide Data」で発生し、2,000万件の完全なカードデータ記録を含むデータベースを公開しました。パートナーとの分析により、このデータにはアクティブで有効なレコードがほとんど含まれておらず、有効期限の分布が異常に均一であることが明らかになりました。さらに、どの記録にもカード所有者の個人を特定できる情報（PII）は含まれていませんでした。これらの要因から、これらの記録は生成された可能性が高く、少なくともこの場合は脅威度が低いことを示しています。

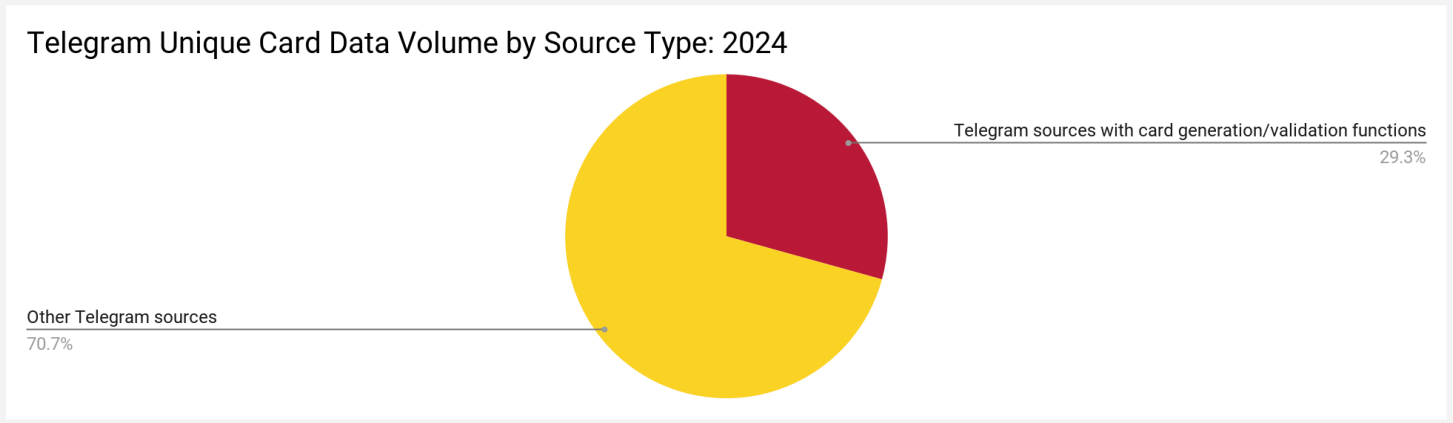


図*11*：*2024*年の*Telegram*由来の一意のカードデータの大部分を占めるカード生成機能と検証機能を備えたソース（出典：*Recorded Future*）

大規模なデータ漏洩はメディアで話題となる傾向がありますが、当社の観察では、2024年最大のカードデータダンプが最も低い不正行為リスクをもたらす傾向があることが示されています。

- **1**月に脅威グループ「**KibOrg**」は同名の**Telegram**チャンネルで**4,000**万件以上のカード記録を公開しました。このデータベースは、ロシアの金融機関Alfa-Bankから盗まれたとされています。
- **4**月には、ソース「**b1ack's Stash**」が、合計**100**万件以上の**CNP**記録を収録した**2**つのデータベースを公開しました。このリリースのデータのほとんどにカード所有者の住所情報が含まれなかったため、カード情報を収益化する際の脅威アクターの期待成功率は低いものとなりました。
- **5**月、ソース「**BidenCash**」は、継続的なプロモーション戦略の一環として、**400**万件の完全なカード記録が含まれるデータベースをリリースしました。これらの記録は、以前に販売または無料で投稿された可能性が高く、詐欺の脅威度は低い可能性があります。
- **7**月、脅威アクター「**ShinyHunters**」は、約**1,300**万件の取引記録を含むデータベースをリリースしました。これには、**200**万件以上の一意の部分的カードデータ記録が含まれていました。これらの記録は部分的にトークン化されているようで、詐欺の攻撃対象領域を大幅に減らしました。
- **8**月、脅威アクター「**Fenice**」は、**National Public Data**の侵害から得られた**20**億行以上のデータを共有しました。このデータは、不正行為をサポートするルックアップテーブルとして機能する可能性がありますが、直接的な不正行為の脅威は低い可能性が高いです。

テスターマーチャント分析の示唆するチェッカー増加と短期的な悪用

ダークウェブチェッカーは、アプリケーションプログラミングインターフェース（API）、専用ウェブサイト、Telegramボットを通じて、カードショップや脅威アクターにカード検証サービスを提供します。Recorded Futureは、提携金融機関とともに、チェッカーが盗難決済カードの検証に利用するテスターマーチャントを特定し、分析しています。このテスターマーチャントデータは、金融機関がリスクのあるカード口座を特定するために使用できる有用なシグナルも提供します。

チェッカー起源のカード検証活動は2024年に増加しましたが、2025年も増加すると思われます。これは、年間を通じてチェッカーサービスの量が増加していることからも明らかです。調査を通じて浮かび上がったテスターマーチャントの数は2023年に比べて減少しています。これは、2023年5月にTry2Checkが閉鎖された結果であることはほぼ確実で、同組織は同じマーチャントアカウントのテスターマーチャント名を迅速に変更する手段を考案していました。一方、特定されたテスターのMIDの数は48%増加し、カード検証の悪用に対するマーチャントアカウントの利用可能性が高まっていることを浮き彫りにしています。

年	特定されたテスターマーチャント名	特定されたテスターMID	チェッカー
2022	2,953	660	20
2023	1,618	684	27
2024	914	1,010	42

表*1*:*2024*年にはダークウェブチェッカーとテスターマーチャントの*MID*の総数が増加、カード検証活動の活発化を示唆（出典:*Recorded Future)*

ダークウェブのチェッカーは、長期にわたる連続した不正使用よりも、非連続的な短期間にわたるテスターマーチャントの不正使用を好みますが、この意図は金融機関による検出回避にあると考えられます。カード検証のために悪用されたすべてのMIDのうち、1か月以上連続して悪用されたMIDは少数であり、3か月以上連続して悪用されたMIDは52件に過ぎませんでした。まれに、チェッカーが「クールダウン」期間後に以前に悪用されたテスターマーチャントに戻ることもありました。

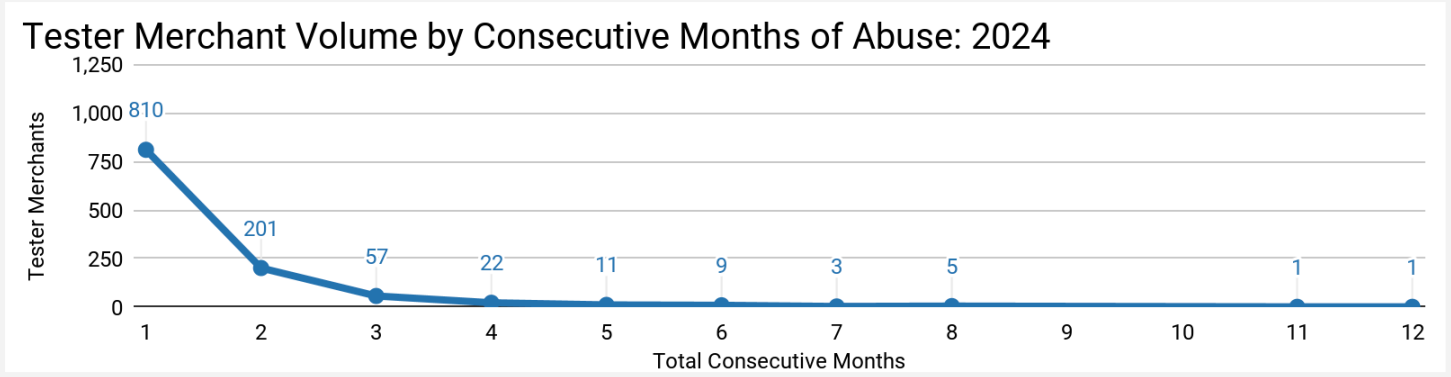


図*12*:チェッカーが*MID*を乱用する頻度が最も高いのは*1*か月で、*2*か月以上連続して乱用を行うケースははるかに少ない傾向（出典:*Recorded Future*）

2024年のテスターマーチャントのほとんどは、複数のマーチャントカテゴリーに集中していました。2024年に悪用されたテスターマーチャントに関連する150件以上のMCCのうち、上位5つのMCCが全テスターマーチャントの3分の1以上を占めていました。Recorded Futureの分析によると、これらのMCCの傾向は、脅威アクターが一般に、正当なマーチャントアカウントを悪用してカード検証活動に使用する方法を反映している可能性が高い

ことを示しています。例えば、多くの飲食店（MCC 5812）ではサイバー衛生状態が悪く、マーチャントアカウントがカードテストに悪用される可能性があります。その他のアクセス方法には、公開されている決済フォームの悪用や、ダークウェブで取引されるAPIキーを介したAPIへの不正アクセスなどがあります。今年のダークウェブに関する議論からは、APIキーの違法取引の増加により、2025年を通じてテスト活動の規模が増加する可能性が高いことが示されています。

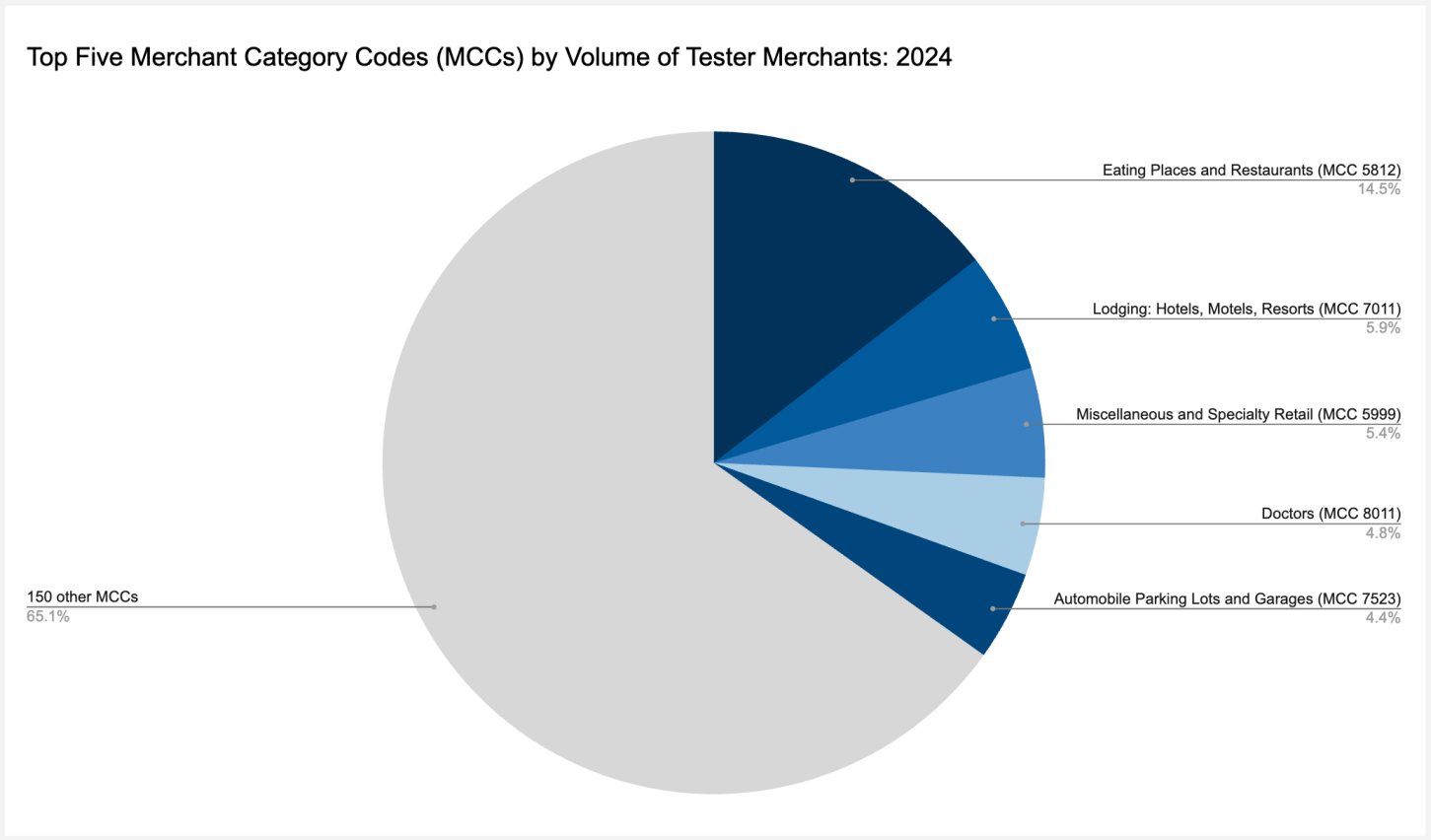


図**13**：*2024*年に不正使用されたテスターマーチャントの上位*5*つの*MCC*がテスターマーチャント全体の*3*分の*1*に相当（出典：*Recorded Future*）

大規模な再投稿と地理的条件が小切手詐欺の脅威の状況を形成

小切手詐欺はアメリカ独自の現象です。Recorded Futureの分析によれば、再投稿の横行と地理的な傾向が小切手詐欺の脅威の状況を定義していることが示されました。2024年に盗まれた小切手画像の約9割は、他のソースの一意のデータの再投稿に該当しました。2024年の日付で合計19万枚の一意の盗難小切手が売りに出され、合計190万枚の小切手画像（再投稿を含む）が売りに出されました。こうした再投稿が頻繁であることを考慮すれば、盗まれた元の小切手の数量からは小切手詐欺の脅威の規模を正確に測れないことが示唆されますが、それでも再投稿により、露出した小切手の詐欺に対するアタックサーフェス（攻撃対象領域）が拡大します。

今年、盗難小切手について利用可能な支払者の地理データを分析したところ、次の2つの主要な傾向が示されました。

- 小切手詐欺の影響はアメリカ東海岸地域で目に見えて大きくなっています。アメリカ東海岸地域の人口はアメリカ総人口の35%に相当しますが、同年に盗まれた小切手の60%がこの地域で発行されています。

- アメリカの特定の州からの小切手は他州からの小切手よりも頻繁に再投稿されるため、特定の州では小切手データの需要が増加する可能性があることが示唆されています。アメリカのすべての州での再投稿率は77%（ワイオミング州）から93%（ウェストバージニア州）の範囲でした。

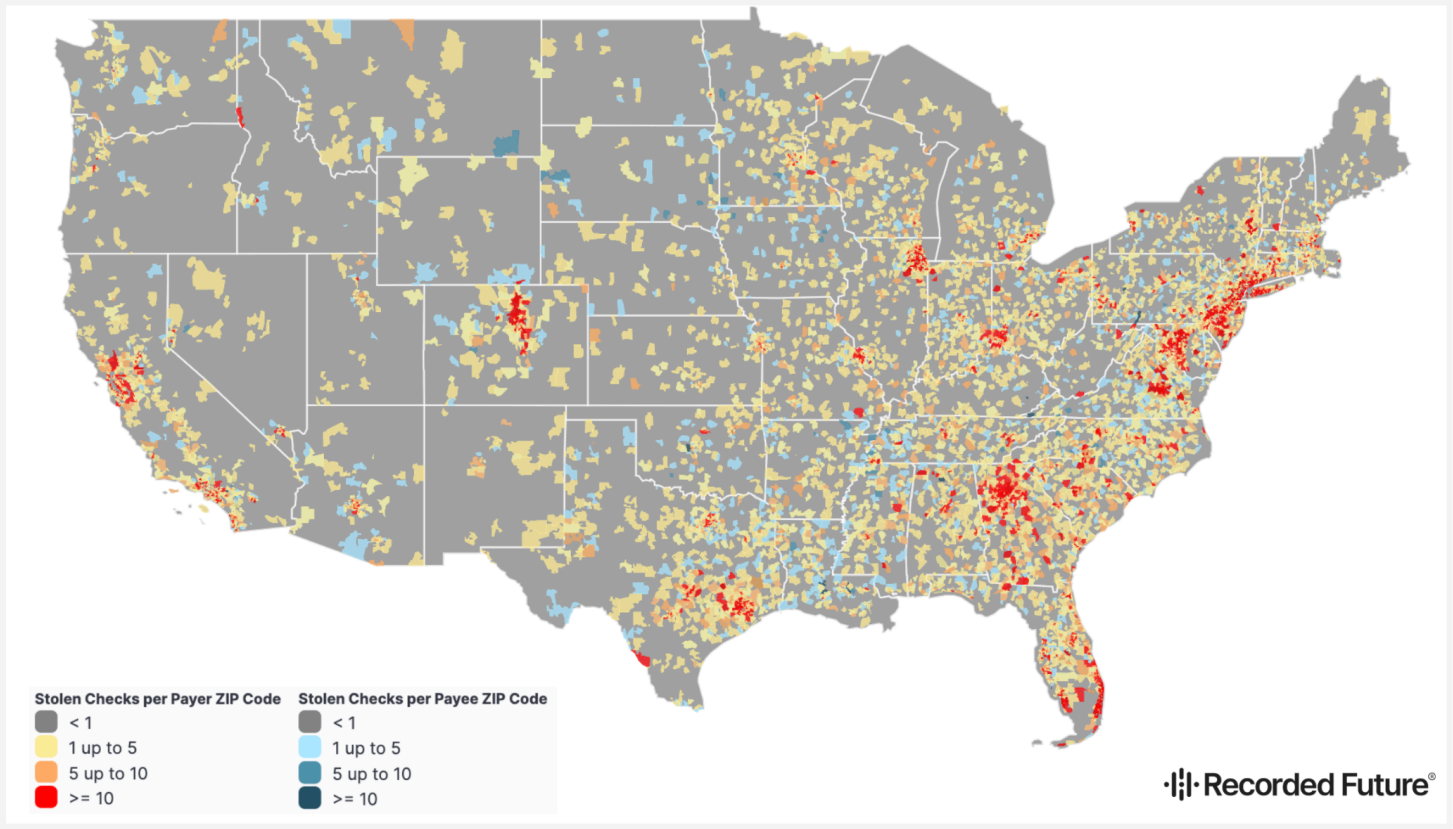


図*14*：アメリカ東海岸地域では小切手詐欺の影響が目に見えて大きい傾向（出典：*Recorded Future)*

巧妙化による詐欺TTPの促進をダークウェブの言説が裏付け

2024年にダークウェブの詐欺に焦点を当てた議論で浮かび上がった主要なテーマは、脅威アクターが詐欺を行うために、利便性とセキュリティに重点を置いた「信頼のためのシステム」を破壊し、克服する意欲を高めていることでした。顧客向けの不正行為は、常に脅威アクターがビジネスルールをナビゲートする能力によって実現されてされてきましたが、今年観測された不正行為のワークフローは、特定のセキュリティ指向テクノロジーの限界を受け入れ、さらにはそれらを有利に利用するという脅威アクターの願望を示すと考えられます。こうした進化の大部分は、効果的な不正防止対応による選択的な圧力とAIの支援により推進された可能性があります。

これらの展開の多くについては、上記のセクションで詳しく説明しています。より広範に見れば、ダークウェブの言説は、不正行為の次の3つのカテゴリーでこの進化を証明しています。

- 被害者を騙すための金融テクノロジーの破壊と敗北
- 新規口座の不正使用、金融口座の不正取得、合成ID詐欺に対する微妙な検証バイパスワークフロー
- 複雑なマネーロンダリングサービスと戦術への依存の継続

顧客のセキュリティを目的とした金融テクノロジーの破壊と敗北

年間を通じて特定された不正行為のワークフローからは、脅威アクターがセキュリティメカニズムを不正行為メカニズムとして採用し始めていることが示されました。今年、脅威アクターは、顧客のセキュリティと利便性を向上させるために設計されたテクノロジーを詐欺のキャッシュアウトツールとして適応させる意欲とノウハウを示しました。

- デジタルウォレット：脅威アクターは主にOTP傍受技術を通じてデジタルウォレット詐欺を行いますが、その方法は異なる場合があります。フィッシングやマルウェアは従来からある手法ですが、2024年にはリアルタイムのパネルベースのプロビジョニングが人気を博しました。それにもかかわらず、不正なプロビジョニングの試行と不正なトランザクションという成功の2つのポイントは不変です。
- オープンバンキングアプリケーション：高度な脅威のワークフローにより、脅威アクターは、顧客の利便性を高めることを目的とした金融テクノロジー（フィンテック）アプリを通じて、侵害された銀行口座を現金化することができ、被害者の口座の資金回収のための複数の経路を入手しています。Recorded Futureの以前の調査によると、脅威アクターによるオープンバンキングの悪用は目新しいものではありません。ただ今年は、その攻撃手法の洗練が進んでいることが明らかになりました。
- フィッシングパネル：フィッシング管理パネルはセキュリティ技術ではありませんが、3DS（3Dセキュア）プロトコルなどのセキュリティ対策によって提供される保護に対する脅威アクターからの回答です。2024年を通じ、「Simba_Service」のような脅威アクターは、3DSで保護されたトランザクションを回避し、MailTzzに関連するものを含む本レポートの他セクションで説明した攻撃を可能にする中間者OTP傍受攻撃を促進できるライブ管理パネルを確立しました。

図*15*：ある詐欺ワークフローでは、オープンバンキングアプリケーションの悪用が脅威アクターが被害者の口座の資金を奪うための複数の収益化経路を提供することが確認されています（出典：*Recorded Future*）

口座取得と不正使用のための微妙な検証バイパスワークフロー

脅威アクターは、金融口座の不正取得や被害者を騙すことを目的とした、ダークウェブソース上で微妙な検証回避ワークフローを実証しました。検証のバイパスは、多くの場合、不正ワークフローにとって避けられない要件です。それにもかかわらず、今年、脅威アクターは、IDプロセスのバイパスフローを考案する際に、AIの支援と複雑さへの嗜好を活用しました。

- ダウンストリーム詐欺のための不正な口座取得：IDプロセスの改善にもかかわらず、新規口座詐欺により依然としてダウンストリーム詐欺が可能となっています。ある口座取得チュートリアルでは、PayPalの検証プロセスをバイパスし、不正なPayPal Mastercardデビットカード口座を取得し、不正な口座をダウ

ンストリームの詐欺やマネーロンダリングに使用するための効果的なガイダンスの概要を説明していました。

- 即時収益化のための事業用カード口座の取得：脅威アクターは、金融商品を綿密に監視し、利益を得る機会を感知すると即座にワークフローを作成します。脅威アクターは、1つのワークフローを使用して、事業用カード商品でアクセス可能なクレジットや、口座開設に関連付けられたプロモーションギフトカードを直ちに収益化できる可能性があります。
- **AI**を活用した合成**ID**：AI技術の採用が進む中、脅威アクターは、特に盗難されたデータと組み合わせることで、ダウンストリーム詐欺やマネーロンダリングのための合成IDをより効果的に偽造する機会を獲得できる可能性があります。Recorded Futureが分析した合成ID詐欺のチュートリアルもAI技術を使用して強化できる可能性があります。AIを使用して合成IDを偽造する行為は、すでに発生している可能性が高いことに注意してください。
- **AI**を活用した検証回避：脅威のエコシステムでは、AI技術を使用してAIが強化する検証プロセスを回避し、「目には目を」で潰し合うことへの欲求が高まっています。微妙なニュアンスのある税金還付詐欺のチュートリアルが登場し、脅威アクターはディープフェイクやAIツールを使用して ID.me ビデオの自撮り写真の検証を回避できるようになりました。このワークフローの有効性は確認できていませんが、AIを活用した検証プロセスが攻撃の防止に有効かどうかもまた確認できませんでした。

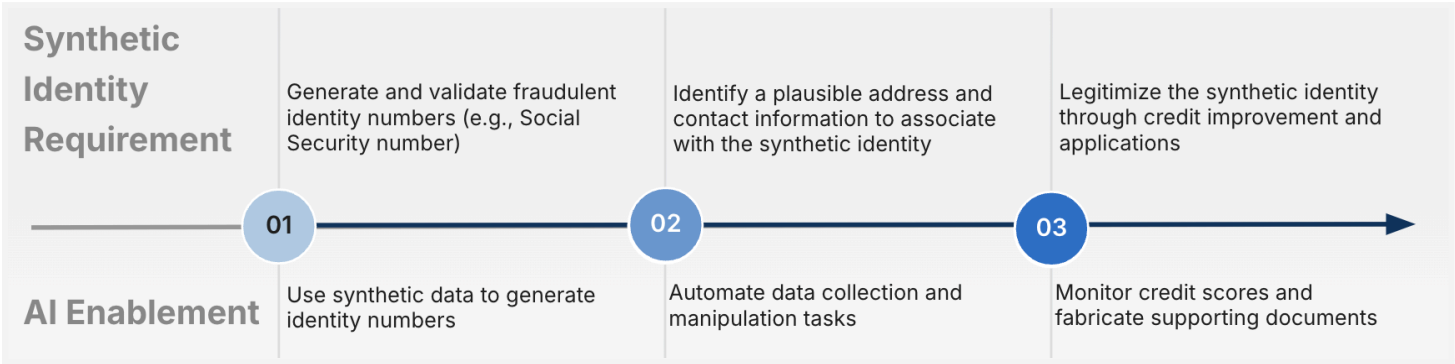


図***16***：*AI*による支援は、特に盗まれたデータとの組み合わせにおいて、合成*ID*詐欺ワークフローの有効性を向上させる可能性があります（出典：*Recorded Future*）

高度に洗練されたマネーロンダリングサービスと戦術

2024年に法執行機関が犯罪関連の決済インフラを混乱させた事実からも、詐欺師にとってのマネーロンダリングインフラの重要性が読み取れます。脅威アクターは今年も、高度な暗号通貨サービスと複雑なマネーロンダリングワークフローを引き続き利用して、詐欺を助長しました。

- 暗号通貨ミキサーとアフィリエイトミキサー：Jambler.ioは、暗号通貨取引を不明瞭にするために洗練されたアフィリエイトスキームを使用しています。ミキサーは、金融機関や暗号通貨取引所にマネーロンダリング防止のリスクをもたらす可能性が非常に高いです。
- 有効性の確認：Exploit Forumに関連する3つの暗号通貨ウォレットは、2018年以降3,850BTC（ビットコイン）以上を受け取っており、サイバー犯罪エコシステム内の金融集団としてのソースの役割を強調しています。
- トランザクションロンダリング：脅威アクターは、詐欺ウェブサイトやその他の高リスクソースからマーチャントベースのトランザクションをリダイレクトすることで、高リスクまたは不正なトランザクションを隠蔽できる可能性があります（上記のトランザクションロンダリングとマーチャントローテーションを参照）。

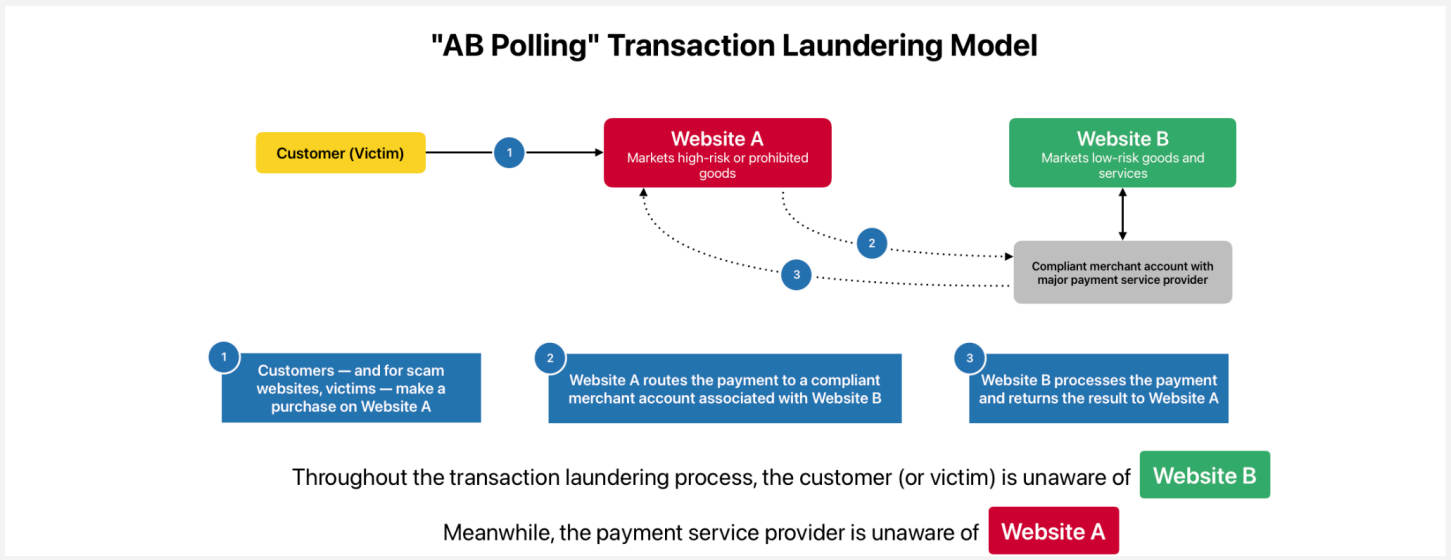


図**17**：中国語の情報源ではトランザクションロンダリングの手法を「*AB Polling*」と呼称（出典：*Recorded Future*）

軽減策

- 買収した販売者に、脅威アクターがMagecartのeスキマー感染を仕掛けるために悪用する可能性のあるeコマースWebサイトの脆弱性を特定し、解決するよう奨励してください。
- マーチャントのオンボーディングプロセスの厳格化を強化して、マーチャントアカウントを不正に取得しようとする脅威アクターを阻止します。
- デジタルウォレットのプロビジョニング試行の検証要件を強化します。プロビジョニングが成功したら、カード所有者に通知します。
- オンラインバンキングアプリケーションを通じてプッシュプロビジョニングを実装します。不正シグナルのトークン化リクエストのデバイスインジケーターを監視します。
- CTIと不正防止の融合ワークフローを、特にインテリジェンス成果物フィードバックループを通じて実装し、CTIチームと不正防止チームが不正をより効果的に検出・防止できるようにします。
    - Recorded Future Payment Fraudカードデータインテリジェンスを使用してポートフォリオ内のリスクのある顧客口座に適切な不正防止策をプロアクティブに特定し、適用します。
    - Recorded Future Payment Fraud Magecarteスキマーインテリジェンスを使用して、感染したeコマースウェブサイトと取引した顧客口座を特定します。
    - 取引分析とRecorded Future Payment Fraud CPPインテリジェンスを活用して、侵害された可能性のあるマーチャントを特定します。
    - Recorded Future Payment Fraudテスターマーチャントインテリジェンスを使用して、カード検証活動に悪用されているマーチャントを特定します。
    - Recorded Future Payment Fraud銀行小切手インテリジェンスを使用して、不正の可能性が高い顧客の小切手または預金を特定します。可能な場合は、構造化された小切手データを活用して、自動化された小切手詐欺防止ワークフローを実行します。
    - Recorded Future Payment Fraud不正マーチャントインテリジェンスを使用して、リスクの高いマーチャントを特定してブロックリストに登録し、リスクのある口座を特定します。
    - ダークウェブソースでの効果的な不正ワークフローを特定し、これらの不正の試みを繰り返し緩和するための方法論を組み込みます。

    - すべてのインテリジェンス成果物について、脅威の状況の指標と内部入力を組み合わせて、不正行為戦略を微調整します。
    - フィードバックをインテリジェンス資産に伝達し、インテリジェンスの優先事項を特定して推進します。

- 不正による損失により追加の不正防止措置が正当化される製品またはポートフォリオセグメントの不正防止手法を継続的に再評価します。インテリジェンスが提供する外部からのインプットがなければ、リアクティブ取引監視は、長期的に金融機関の不正リスクを最小限に抑えるには不十分である可能性が高いことに注意してください。

今後の展望

あらゆる犯罪の脅威の状況で進化が予測されますが、不正行為も例外ではありません。新しいテクノロジーと調査の流れにより不正防止システムの改善が進む中、脅威アクターは金融機関の防御策を探り、被害者を騙すために悪用できる可能性のある弱点を探します。したがって、金融機関やその他の組織が「城のジレンマ」を克服するために協力的なCTIと不正の融合戦略を採用するにつれて、脅威アクターが不正行為を行うために独自の「ダークサイド」融合戦略に着目する方向性が強まることは驚くにあたりません。サイバー対応型の詐欺の状況が絶えず変化し、それ自体が絶えず変化する技術、経済、規制の要因に影響されるという背景に鑑みれば今年の傾向はやや表面的と言えますが、それでも、脅威アクターが2024年に見せたセキュリティと利便性のメカニズムを詐欺メカニズムとして採用する能力は、今後の課題の前兆となるでしょう。

今後を見据え、このレポートの傾向を分析した結果、2025年については3つの主要な予測が挙げられます。

- 特に詐欺グループがキャッシュアウトスキームのためにデジタルウォレットと不正なカードプロビジョニングを優先する中、デジタル**e**スキミングと詐欺電子商取引が**2025**年に**CNP**データ侵害事象を引き起こすでしょう。脅威アクターは3DSやデジタルウォレットなどの決済テクノロジーが効果的であることを認識していますが、OTPや一貫性のないマーチャントのオンボーディングも悪用すべき弱点として特定しています。これにより、脅威アクターは、特に実績のあるソーシャルエンジニアリング戦術と組み合わせることで、詐欺対応決済メカニズムを完全に回避するのではなく、これに適応することができるようになると思われます。eスキマーキットの改善と新たな脆弱性により、eスキマーベースの詐欺が加速する可能性があります。今後予定されているPCI DSS v.4.0の要件実装はほぼ確実にMagecartの脅威の状況を変えるでしょうが、これらの要件の有効性は、中小規模の電子商取引事業者の間での不適切な採用により低下する可能性があります。
- **Telegram**などのプラットフォームが経験の浅い脅威アクターの主戦場となる中、ダークウェブマーケットプレイスは決済詐欺エコシステムの中心的存在であり続けるでしょう。不正防止エコシステムは、データを漏洩するサプライヤー、盗難されたデータを購入して収益化する購入者、サプライヤーと購入者をつなぐ犯罪者のオンラインマーケットプレイスが関与する、セミプロレベルのグローバル市場です。ダークウェブのソースは、規模、永続性、市場の安全性、匿名性という利点があります。中でも匿名性は、特にTelegramがユーザーデータを当局に提供することに同意したことを考えると重要です。
- 過去**3**年間にアメリカで見られた小切手詐欺の爆発的な増加は今後も続くでしょうが、小切手詐欺の最終的な損失を減少させるための準備が金融機関で整うでしょう。小切手詐欺が減少する兆候はありません。コロナ禍における景気刺激策の配布に際して考案された小切手詐欺の手法は、今や広く利用可能です。また、多くのサイバー対応詐欺スキームと異なり、小切手詐欺には高度な技術的専門知識は必要ありません。それにもかかわらず、金融機関では、2025年に向けて小切手詐欺による実際の損失を低減するための準備が整っています。この面で金融機関の施策を推進する主な要因となるのは、盗難された銀行小切手に対する脅威インテリジェンスの採用、以前は設備が整っていなかった小切手詐欺防止資産への組織的なコミットメント、法人顧客がポジティブペイなどのリスク軽減ソリューションを採用するように促すことです。

*Recorded Future*のレポートには、米国インテリジェンスコミュニティー（*ICD*）*203*：分析基準（*2015*年*1*月*2*日発行）と一致する可能性のある表現が含まれています。また*Recorded Future*のレポートでは、米国インテリジェンスコミュニティーが採用する信頼レベル基準を使用して、分析的判断の裏付けとなる情報源の質と量を評価しています。

Insikt Group®について

Recorded Future の脅威リサーチ部門である *Insikt Group* は、政府、法執行機関、軍、諜報機関に深い経験を持つアナリストとセキュリティ研究者で構成されています。彼らの使命は、お客様のリスクを軽減し、具体的な成果を実現し、ビジネスの中断を防ぐインテリジェンスを生み出すことです。

Recorded Future®について

*Recorded Future*は世界最大規模のインテリジェンス企業です。当社のインテリジェンスクラウドは、攻撃者、インフラストラクチャ、標的に関する包括的なインテリジェンスを提供します。オープンウェブ、ダークウェブ、技術ソースにわたるインターネットをインデックス化して、拡大傾向にあるアタックサーフェスと脅威状況をリアルタイムに可視化し、お客様が迅速かつ確信を持ってリスクの軽減と安全なビジネス遂行に取り組めるように支援します。ボストン本社および世界各国のオフィスに従業員を擁し、*75*か国以上で*1,800*社を超える企業と政府組織と連携して、バイアスのかかっていない実用的なインテリジェンスをリアルタイムで提供しています。

詳細については、*recordedfuture.com*をご覧ください。