



暗号通貨取引向けの Cybersource収益最適化 ソリューション

→

→

→

→

→

→

--	--	--	--	--	--	--

ビジネスの 課題



ビジネスの課題

暗号通貨取引所は、特に法定通貨を使用して売買しようとするときに不正攻撃の主要な攻撃対象となります。消費者の関心が高まりにつれ、暗号通貨市場の変動性とその拡張性は、不正詐欺行為の市場を増大させる可能性があり、取引所にはその不正検知と防止が求められます。

暗号通貨の価値と採用は急上昇しており、メディア広告や著名人による支持、アクセスしやすいモバイルアプリなどを通じて社会での認識が深まる¹につれて、今後も成長していくでしょう。¹この急速な成長によりさまざまなリスクが発生しており、支払や金融、商取引等広範囲に影響を及ぼしています。²

暗号通貨は、その価値の高さゆえに不正詐欺攻撃にとって理想的な標的となります。また、イシューから疑われやすく、その結果として与信承認率が低くなる可能性があります。

暗号通貨取引所は多くの攻撃の対象となりやすいため、基盤となる不正インフラや認証管理の構築を行う必要があります。購入（法定通貨から暗号通貨への変換）やアカウント間の資金の移動などの個々の取引は、取引所の収益を直接危険にさらします。これは口座情報の盗難やフレンドリー詐欺の両方が原因となる可能性があります。

VisaソリューションであるCybersourceは、こうした課題のソリューションとして、収益の最大化を実現しながら不正詐欺を軽減するエンドツーエンドの不正およびリスク商品やサービスを提供します。Cybersourceの収益最適化ソリューションなら、関連する顧客体験の課題を気にすることなく暗号通貨事業展開を促進できます。

¹ 関心の高まりが示す、暗号通貨が獲得した最新の資産形成手段という地位

² 暗号通貨の現象：暗号通貨に対する顧客の行動と使い方

不正行為の傾向



不正行為の傾向

世界的に混乱を引き起こしているパンデミックにより、革新的な決済ソリューション採用のニーズが加速しています。顧客は新しいテクノロジーを採用し、分散型金融 (DeFi) を導入し始めている一方で、企業は今までとは異なる状況に対するニーズを満たそうと焦っています。しかし、そのときに劇的に戦略を変更する時に必要なプランニングが欠けていることがあります。不正攻撃者はこうした変化に目を付け、独自開発した手段を使って今まで以上に巧妙で精度の高い攻撃を実行します。このような攻撃は大きな犠牲を生みます。例えば、Cybersource³による2020年度の調査によると、企業のうち33%が新たな不正攻撃の特定と対応に苦慮していると答え、さらに、28%は不正防止管理に必要なデータが不足していることが明らかになりました。³

法定通貨を暗号通貨やNFTに換金する機会を提供する暗号通貨取引所は不正攻撃者にとって最も「儲かる」標的であり、2021年には260億米国ドル以上の支出がありました。⁴中でも人気のある暗号通貨は、決済手段の盗難や詐欺から、価値を人工的に膨張させる「パンプ アンド ダンプ」スキーム、「買い手の後悔」というフレンドリー詐欺に至るまで、さまざまな不正関連の課題を誘発しています。

不正行為による支出が増加するため、多くの企業では顧客体験の向上より不正行為を削減する方を優

先せざるを得ず、それに応じたITへの資金や取り組みも不十分でした。³従来の不正防止には、IT面での変更を伴わない手動レビューが多く用いられてきましたが、調査対象の60%の企業が、不正防止に対する手動レビューへの依存を削減または排除したいと考えています。³こうした変化を促進するには、顧客体験を優先する正確で自動化された不正防止が欠かせません。

さらに懸念する事項となっているのは、イシューが対面決済 (CP) の1%と比較して、非対面決済 (CNP) トラフィックの18%を拒否していることです。⁴これは、不正件数の多い企業や取引所では認識されたリスクによりイシューからの承認率が低くなるという点を考えると、暗号通貨取引所により深刻な影響を与えます。イシューの承諾ポリシーに一貫性がないと、顧客の混乱やサービス上の問題、さらにはチャージバックが引き起こされる可能性があります。Cybersourceの収益最適化ソリューションで不正を軽減することで、企業はイシューの承認率と顧客体験を向上させることができます。

³ 2022年グローバル不正対応および決済レポート
⁴ Cybersource収益最適化ホワイトペーパー

収益最適化のための戦略

承認を最大化するための新しい方法



Cybersourceの戦略は、不正詐欺リスクを軽減し、承認率を引き上げることで収益の最適化を推進します。それによって与信コンバージョン率を最適化して失われた収益を取り戻すことができます。決済業界のパイオニアとして、Cybersourceの最適化ソリューションは、承認率の引き上げやリスクを最小限に抑えることで収益増加をサポートします。多様なVisaチームやイシューとの緊密なパートナーシップにより、当社の不正防止管理ツールの強化、承認可視性の改善、そして顧客の摩擦削減を実現します。

Cybersourceの5つの主要なイニシアチブ

Cybersource収益最適化ソリューションは、不正防止、可視性の改善、不正の事前スクリーニング、ツールの最適化、そして自動化による顧客体験の強化という5つの主要イニシアチブに特化しています。

- **不正防止:** 不正行為は顧客や企業に多額の損失をもたらし、企業に風評被害をもたらします。チャージバックを減らすことは、eコマースビジネスにおける優先事項ですが、直接承認率への影響の方がより差し迫った事項になります。⁴ 高いチャージバック率は、ペナルティや風評被害につながる可能性があります。収益最適化ソリューションを使用することで、チャージバック率を低下させ、イシューの信頼を高め、与信承認率を改善させることが可能です。
- **承認率の可視性の向上:** シームレスな承認は顧客体験にとって必要不可欠ですが、承認率を把握できている企業は30%にすぎません。⁴ これにより、改善のためのベースラインの確立や改善する機会を特定することが難しくなっています。こうした事情を踏まえ、Cybersourceのソリューションは詳細な与信率レポートを通じて高い可視性を提供し、積極的に変更することを可能にします。
- **不正の事前スクリーニング:** 不正攻撃の中には、企業に多数の取引を仕掛けて成功したものは何なのか、その結果をうかがう量特化型のタイプもあります。こうした大量型のランザクション試行により、与信率が低下します。Cybersourceのソリューションは、不正防止を上流に移動させ、承認前に事前スクリーニングすることで、イシューに送信されるリスクのあるランザクションを減らし、結果的に拒否率を低下させることができます。
- **ツールの最適化:** 不正防止ソリューションの多くは静的モデルと手動処理に依存しています。Cybersourceは、不正の動的な性質を認識し、Visa全体のネットワークから得る洞察を活用して進化し続ける機械学習モデルを提供します。

このネットワークにはVisaNetからの1,410億件のトランザクション、⁵ 加盟店全体からのデータ、そしてほかの暗号通貨取引所からのデータが含まれます。これにより、不正詐欺の状況に応じて進化するイベントのポジティブな面とネガティブな面を判定できるソリューションが可能になります。当社の革新的なReplay機能を使用することで、計画された戦略変更による潜在的な結果を確認できるため、さらなるスクリーニングを必要とするリスクの高いトランザクションの数を減らすことができます。

- **自動化による顧客体験の強化:**今日の顧客は自動でシームレスなデジタル体験を求めています。そして、手動によるトランザクション審査はコンバージョン率を劇的に低下させ、顧客からのエスカレーションを発生させます。CybersourceはDecision Managerと支払人認証ツールに3-Dセキュア機能を完全統合しているため、エンドツーエンドの承認フローと透明性の高いトランザクション審査が可能です。ポジティブおよびネガティブなトランザクションの大部分を前もってフィルタリングすることで、手動レビューへ送られるトランザクション数を大幅に減らせます。これらの

原則はCybersource収益最適化ソリューションの根幹となるものです。組み合わせて使うことで、顧客体験に集中しながら企業や 이슈が自信をもって意思決定できるデータや洞察を提供します。どのようにして実現するのでしょうか？業界トップレベルの機械学習と人工知能を活用し、経験豊富なグローバルチームからの洞察をまとめ、自動化と承認率を向上して、お客様はビジネス成長に集中することができるのです。

⁵ 2020会計年度に基づくVisaNetトランザクション量。トランザクション量には国内ルートのもが含まれていない場合があります。



暗号通貨向け Cybersource収益最適 化ソリューション

承認を最大化するための
新しい方法



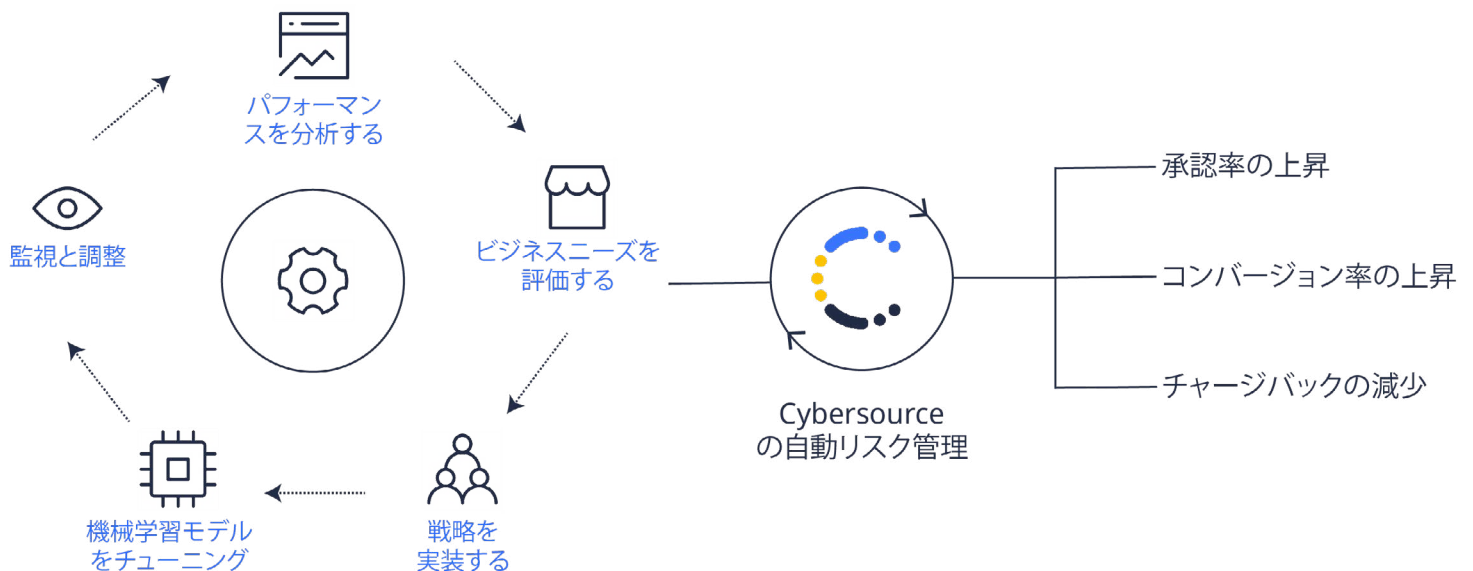
暗号通貨向けCybersource収益最適化ソリューションは、包括的で完全なアウトソーシング型ソリューションであり、高度な自動化と世界最大級のネットワークを活用し、あらゆる形式のお金の流れをリアルタイムで最適化します。この機能と卓越した専門知識を組み合わせることで、企業は、個々の不正防止ソリューションを維持するために必要な諸経費なしで、新しいテクノロジーの革新を推進することができます。

階層化アプローチ

従来、不正詐欺の防止には階層化アプローチが必要とされてきました。例えば、ビジネスでは平均で最低4つの不正防止商品が使用されています。3こうした階層の実装にはコストや時間がかかるだけでなく、貴重なITのキャパシティも浪費してしまいます。その代わりとして、複数の決済プロバイダとプラットフォームを管理することを避けるために、Cybersourceは機械学習やAIの活用によってリスク管理を自動化する単一でシンプルなエンドツーエンドのプラットフォームを提供します。これで、デバイスプロファイリング、3DS承認能力、サードパーティーデータサービスとの完全統合により実装が容易になります。当社のソリューションは、フレキシブルでスケーラブル、そして

自動です。さらに、たった1つの接続やプロバイダを通じてツール間で学習結果を共有できます。

不正詐欺攻撃は常に変化しており、また新しい変数も加わるため、パフォーマンス分析は継続的なプロセスとなります。Cybersourceのソリューションは、お客様独自のユースケースの理解、収益を最大化するための戦略の実装、業界トップレベルの機械学習によるリスクモデル調整、そして最適化に到達するために必要な調整を行うことで、承認率の引き上げと不正詐欺の減少に特化しています。



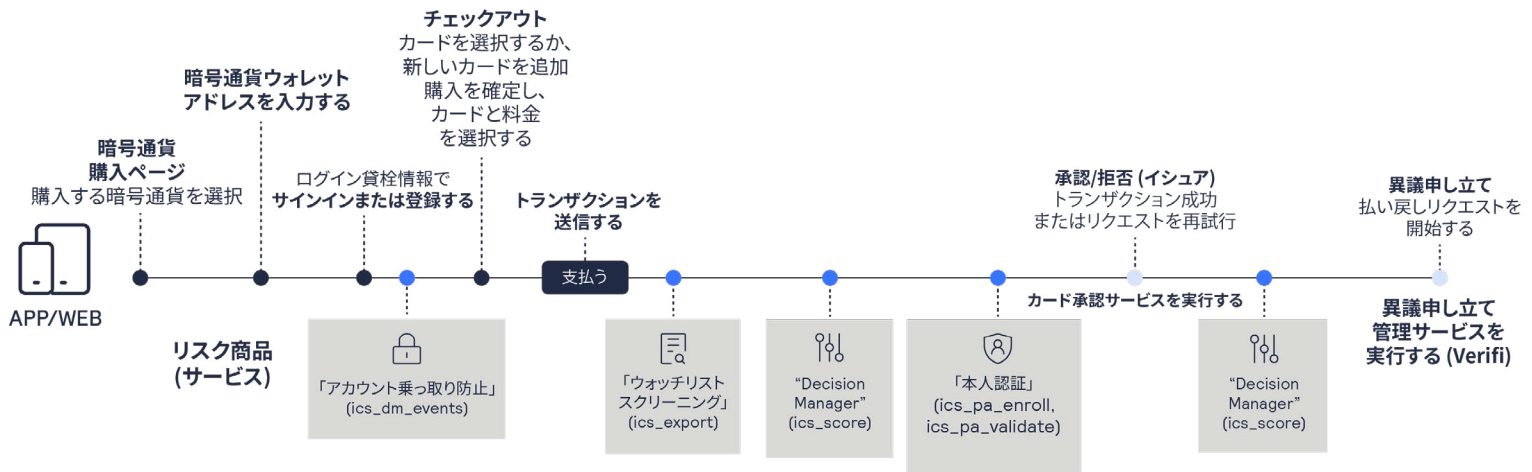
暗号通貨向け Cybersource収益最適化 ソリューション

承認を最大化するための
新しい方法



エンドツーエンドのソリューション

お客様のビジネスには独自性があり、それはお客様の不正詐欺リスクにも独自性があるということです。当社のソリューションの階層はお客様のニーズに合わせてカスタマイズが可能です。これにより、パフォーマンスを密接に監視する完全カスタマイズ型で動的な不正防止戦略が実現されます。このソリューションはお客様の目標を反映したレポートと分析により、継続的で完全な可視性を提供します。



また、リスクコンサルタントの専門知識も活用できます。リスクコンサルタントは多様なクライアントベースとの連携から得た幅広い知識に基づいて、エンドツーエンドのプランを確実に計画できます。これらの要素はすべてリンクして、お客様の特定のリスクに適合し、一部の不正攻撃よりも迅速に適応できる不正防止フレームワークを作成します。

収益最適化ソリューションツール

アカウントの乗っ取り防止



アカウント乗っ取り防止

不正攻撃はいまだかつてないほど巧妙化しており、詐欺師も上流に移動しています。

Cybersourceのアカウント乗っ取り防止ソリューションは、すでに発生した攻撃に反応するのではなく、不正行為をアカウントレベルで早期に検知できます。弊社の収益最適化ソリューションと合わせて使用することで、お客様の戦略を補完し、アカウント設定からチェックアウトまでの保護を提供します。

アカウント乗っ取り防止ソリューションでは、行動、Eメールアドレス、デバイス、通信、その他の予測的属性に基づいて疑わしいアクティビティの指標を識別する柔軟なルールエンジンを利用できます。こうした行動指標では、従来のアカウント乗っ取り不正だけでなく、偽アカウント作成やロイヤルティ詐欺、その他取引前の攻撃の特定やブロックも可能です。例えば、アカウントの作成時に使用されたデバイスの詳細とチャージバックに使用された詳細を比較すると、取引所は異議申し立て、フレンドリー詐欺、法定通貨チャージバックと既存顧客を正常に区別できます。

主な利点



顧客の信頼とブランドロイヤリティを保護する。

顧客情報が盗まれると、たとえその情報漏洩がほかの場所で発生したとしても、顧客のブランドに対する評判は低下してしまいます。アカウント乗っ取り防止ソリューションは、こうした攻撃を防止することで、顧客とブランドの評判を安全に保ちます。



不正な取引が発生する前に防止する。

アカウント乗っ取りに起因する不正取引は、チャージバックや在庫の損失、異議申し立て解決費用といった問題を発生させます。アカウント不正を特定することで下流の関連コストを削減できます。



顧客の減少を避ける。

アカウント関連の不正行為が1件起こるだけで、顧客からの信用は失われ、多額の損失につながる可能性があります。

収益最適化ソリューションツール

ウォッチリストスクリーニングと チャージバック管理



ウォッチリストスクリーニング

Cybersourceのウォッチリストスクリーニングでは、企業はウォッチリストスクリーニング認証サービスを通じ、経済制裁や対テロ戦略、マネーロンダリング、取引禁止業者リストをリアルタイムで組み込むことができます。これにより、購入者情報の規制リストとの比較が容易になり、コンプライアンスに配慮した意思決定や取引におけるマネーロンダリングの防止を行えます。

ウォッチリストスクリーニングツールは定期的に更新される23件の制裁リストが含まれており、複数の規制機関全体におよぶスクリーニングやマッチングを1つのステップで実行できます。このマッチングアルゴリズムはビジネス情報をリストと比較するだけでなく、審査の精度を高めるコンフィギャラブルロジックも含み、エラーや誤検知を最低限に抑えます。



チャージバック管理

VisaソリューションであるVerifi提供のチャージバック管理は、不正防止や完全制御において重要なステップの1つです。どのチャージバックに異議を申し立てるのかを把握し、異議を申し立てるには、専門知識やスキルが必要です。その他のツールと連動することで、Verifiのチャージバック管理は、多額のコストを要するチャージバック紛争での勝率を高めます。

収益最適化ソリューションツール

Decision Manager



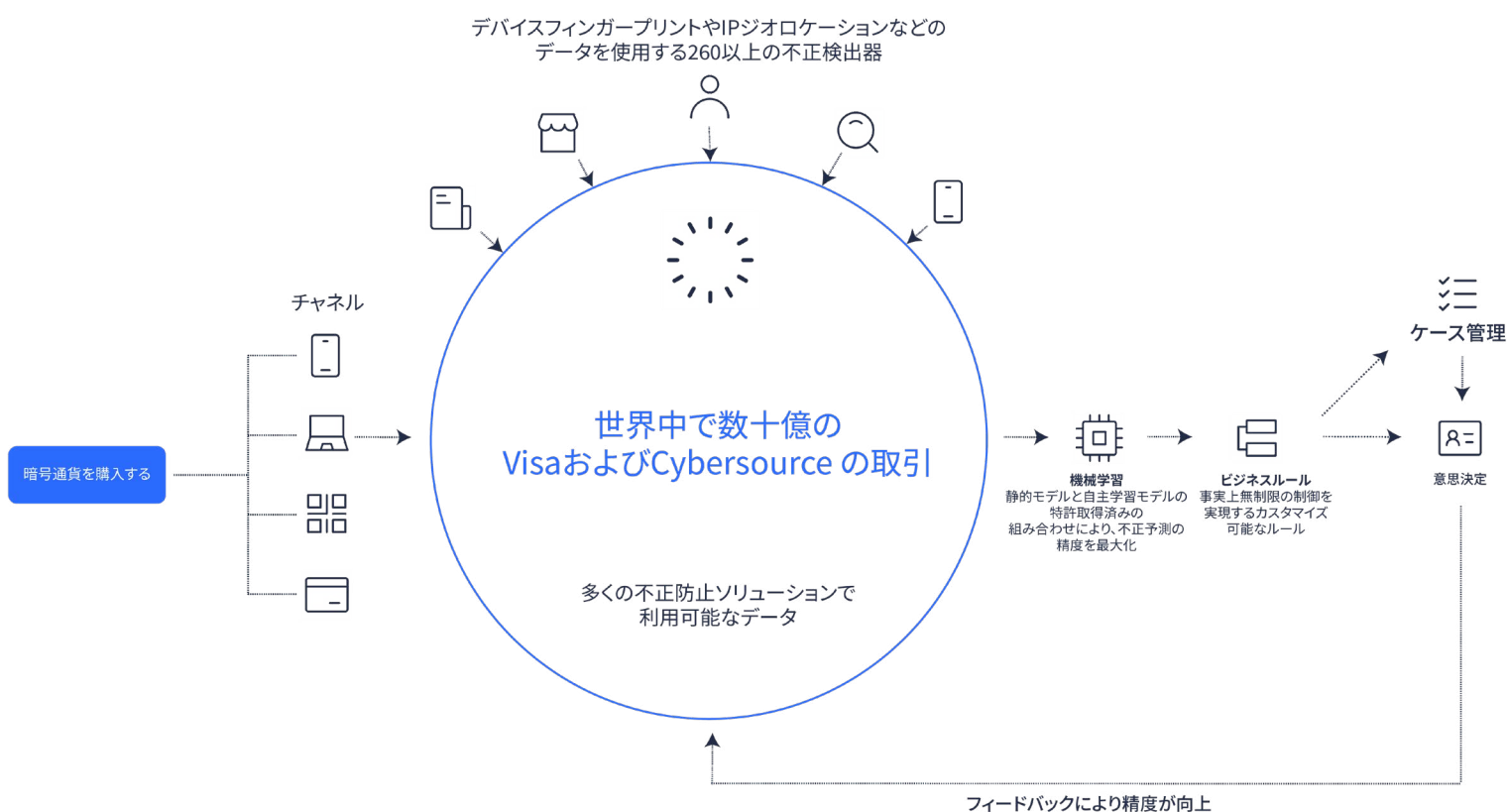
Decision Manager は不正およびリスク管理ソリューションのCybersourceの主力製品であり、グローバルな不正行動モデリングや数十年に渡る決済・リスク知識、そしてVisaネットワークの統合性を組み合わせたものです。その堅牢な性能により、企業は幅広く洗練された機械学習モデルを使用して、トランザクションの判定を行えます。**AIを活用した不正防止に加え、Decision Managerは完全にカスタマイズ可能なルールエンジン、ケース管理システム、分析ツール、そしてリアルタイムのレポートポータルを搭載しています。スタンドアロンサービスとして利用できますが、Cybersourceの決済管理プラットフォームと完全に統合することでさらに強力な結果を得られます。**

Decision Managerは複数の機械学習モデルを使用して、カスタマイズされた不正ルールと併用することで、より優れた柔軟性と精度を提供します。その幅広いデータを取り込み、取り込んだデータを人間行動に関する理解

しやすい知見へと変換する機能によって、 이슈アが送信する前にリスクの高いトランザクションを入念にフィルタリングすることができます。暗号通貨は詐欺の主要な標的であり、従来の多くのソリューションはこれら独自の暗号通貨への攻撃に対する手段を備えていません。

Decision Managerの実装によってコンバージョン率が上がると、承認前・承認後両方での 이슈アからの承認率も高められます。不正チェックを与信呼び出しと切り離すことで、暗号通貨取引所は的確なタイミングで最も収益率の高い取引を注意深く行う柔軟性を得られます。すべての取引でこうした明確な結果を得られれば、売上の増加や顧客体験の改善が期待できます。

また、Decision Managerの複数モデルではポジティブな行動が特定され、その高度な機械学習モデルは取引履歴データを分析して不正なトランザクションと正常な取引を解析します。顧客が暗号通貨市場に参入するのは



初めてかもしれませんが、その顧客のデジタルIDはVisaの広範なネットワークにすでに確認されている可能性が非常に高いです。Decision Managerでは、精度の高い自動化と正確なカスタムルールセットのバランスを制御します。Decision Managerは不正防止レイヤーの完全スイートの中心的役割を果たすことにより、単一の統合を通じて不正詐欺行為の割合を減らし、流動性を促進し、販売の革新や成長の増進を実現します。

主な特徴



アイデンティティ行動分析

より広範なグローバルのビジネスコンソーシアムからの洞察を活用することで、企業は優良なビジネスとリスクをすばやく区別し、正当なトランザクションや定期的なトランザクションの承認に関する不正防止や信頼性向上を促進できます。



ルール提案エンジン

機械学習をお客様独自の取引履歴に基づいた不正分析に活用し、既存の戦略の拡張や改善につながるルールを提案します。各提案はすべてパフォーマンス予測に利用できる詳細なメトリクスが付随しています。



DM Replay

Replayを利用すると、ライブ環境へ移行する前に潜在的な変化による影響をリアルタイムで査定できます。その革新的なテクノロジーは迅速に変更を行い、新しい戦略を実装するために必要な信頼を与えてくれます。



サードパーティーの統合

内蔵のパートナーシップ機能によりグローバル不正対応サービスをすばやく簡単に追加統合できるため、関連するIT開発のコストの節約につながります。潜在的なパートナーには今後もデジタルIDや行動バイオメトリクス、メールやID認証データリソースを含みます。



収益最適化ソリューションツール

支払人認証



支払人認証 は、不正な支払いカードの使用を抑制し、不正なチャージバックから保護します。この連携サービスはEMV® 3-D セキュアプロトコル (3DS)を使用して認証を行い、3DSサーバーを活用して複数ステップの認証を提供し、イシューがトランザクションを確認する前にリスクの最も高い暗号通貨の購入の試みを回避します。

支払人認証をDecision Managerと併用することで、3DS認証に対してより合理的アプローチを行えます。Decision Managerはトランザクションを認証へと自動的にルーティングでき、イシューからのステップアップチャレンジを必要とする高リスクのトランザクションを一時停止できます。このステップアップチャレンジが正常に完了されると、追加の呼び出しを必要とせずに、認証結果をキャプチャし、与信を開始することで取引が再開されます。

Decision Manager と支払人認証を併用することで、保護レイヤーが一層強化されると同時に認証の洞察によって意思決定の質を高め、そして3DSをサポートするより合理的なアプローチをとることができます。

主な利点

3DSの活用でリスク保護に新たな階層を追加

- トランザクションの認証を自動的にルーティング。
- 高リスクのトランザクションはイシューから追加のチャレンジを受ける可能性がある。

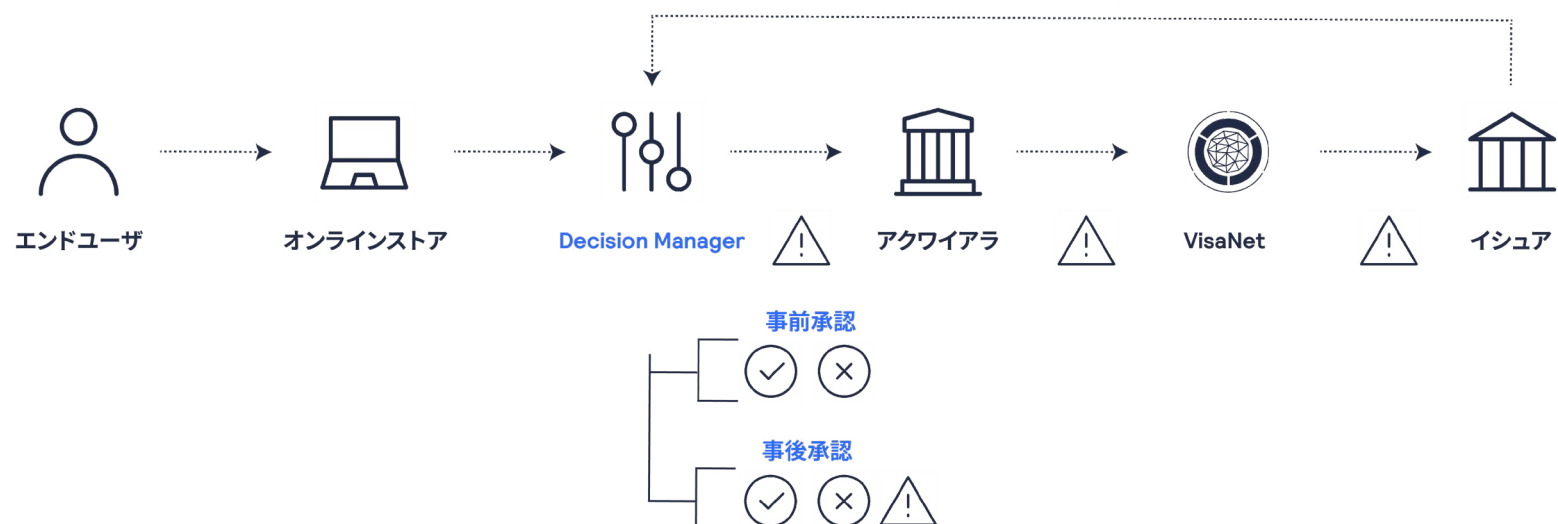
責任のシフト

支払人認証で承認された不正チャージバックについて、発行銀行が責任を負います。

与信率の向上

認証されたトランザクションを与信に送信することで、イシューは承認に対してより信頼を高めることができます。

承認応答



収益最適化ソリューションツール

リスク抑止サービス

不正詐欺の専門家の見識のもとに収益最適化ソリューションのすべての要素をまとめたCybersourceのマネージドリスクサービス。

Cybersourceのマネージドリスクアナリストは、暗号通貨のリスクの最先端にしながら、さまざまな取引に関するビジネスモデルを研究し、お客様独自のニーズをすばやく把握します。

今日の不正管理者は、オペレーション、マーケティング、ロジスティクス、決済、異議申し立て、そして顧客サービスなどさまざまな役割りをこなすことを期待されており、将来的な成長のための「ゲートキーパー」と見なされることが多くなっています。そのため、新たな不正詐欺のトレンドへの対応や日々の業務が難しくなってきたと感じる企業は少なくありません。お客様がビジネスニーズに集中して対応している間に、Cybersourceのマネージドリスクアナリストが不正詐欺に対応します。



主な利点

- パフォーマンス監視を提供する
- 分析によって洞察を生み出す
- 不正詐欺戦略を進化させる
- 専門の不正対策製品を活用する
- IDやメールアドレスに洞察を応用する
- 不正詐欺市場の変化を把握
- 信頼できる不正リソースとして機能する

信頼できるパートナー による実証結果



不正詐欺防止の先駆者として、CybersourceとVisaは経験豊富なパートナーであり、企業独自の不正防止ニーズに合わせながらビジネスのイノベーションを実現します。Visaのインフラと広範なデータコンソーシアムという強みは、安定性と幅広く知識豊富なバックボーンをこの柔軟でパワフルなソリューションにもたらしめます。暗号通貨向けのCybersource収益最適化ソリューションはパートナーシップを可能にし、不正詐欺防止パフォーマンスの改善や、DeFiの普及を安全に促進します。

暗号通貨向けのCybersource収益最適化ソリューションなら、優れた結果をもたらします。例えば、Cybersourceで承認戦略を最適化した企業は次のような成果を得ています。☑

- 手動レビューにかかっていたコスト400万米ドル相当を節約
- 3,680万米ドルの承認額の増加
- 市場が不安定でも安定したパフォーマンスを維持
- 99.997%という異例の稼働時間を達成
- 与信率が1%向上
- 承認率が8%上昇



免責事項:本ドキュメントに登場する結果は、2020年1月から2021年11月までの北米のDecision Managerクライアントに基づく内部データを使用して算出した結果です。結果はクライアントがCyberSourceのマネージドリスクサービスと連携した場合やクライアントのDecision Manager使用方法といった要素によって変動することがあります。トランザクション審査の平均コストは3米ドルです。

定義

暗号通貨(仮想通貨)

保管された価値または商品やサービスとの交換媒体として使用されるデジタル資産です。トランザクションは、銀行や政府機関など中央当局ではなく、参加者の分散ネットワークによる暗号化を用いて検証や記録が行われます。

DeFi

分散型金融(decentralized finance)の略語です。金融は信頼できる仲介者に依存しているため、伝統的に中央集権化が行われています。例えば、お金を友人や家族に送金したい場合、銀行経由で振込先の銀行へと送金します。一方、DeFiは仲介を必要とせず、参加者は資産の送金や受け取りを直接行えます。これによって理論的にはより高速かつ廉価での取引が可能になります。

取引所

ユーザーが暗号通貨の購入や売却を行うウェブサイトやアプリです。

法定通貨

伝統的な通貨には国家による十分な信頼と信用という裏付けがあります。米国ドル、ユーロ、英国ポンドなどが法定通貨に該当します。

NFT

非代替性トークン(non-fungible token)の頭文字を取った言葉で、暗号通貨と同じ基盤技術を使用するデジタルコレクションです。

私たちがお手伝いいたします。

