IBM Security

IBM

シームレスな ID の信頼性で成長とデジタル対応を加速化

IBM Trusteer は、オムニチャネルの顧客体験全体にわたって ID の信頼性をシームレスに確立できるように支援します

では、始めましょう

IBM Security

IBM

目次

はじめに

ほとんどの企業にとって、成長の加速化とデジタル・チャネル増加が最優先事項です。企業が顧客の期待を満たし、新しい市場に参入し、収益を拡大するには、デジタル変革が必要不可欠となりました。

しかし、多くの企業は、デジタル化だけでは不十分であることに気付いています。消費者は、購入するとき、アカウントを登録するとき、ロイヤルティ・プログラムやサービスにサインアップするとき、あるいは単に連絡先情報を更新するときでも、スムーズなオンライン体験を求めています。

消費者が取引実行やサービスの適用、あるいはアカウントのアクセスに余分な認証ステップを実行しなければならない場合、デジタル・チャネルは満足よりも不満足の原因になるおそれがあります。その結果、顧客離れが進み、ユーザーは競合他社サイトやよりコストの高いチャネルに移ってしまいます。また、顧客離れが高くなると、ネット・プロモーター・スコア (NPS) が低くなり、売上の機会を失うかもしれません。

残念ながら、デジタル・チャネルの匿名性のために、適切なツールを持つ個人は自分の ID を隠して、デジタル・チャネルを悪用することができます。

企業が本当の顧客だと信頼できたらどう変わるか想像してみてください。取引がもっとシームレスになり、デジタルの成長とイノベーションが向上し、競争力が増します。

事前の情報または顧客レコードがない場合、公表されている情報しか頼れない場合、サイバー犯罪者が新しいデジタル機能を悪用し、盗んだ ID を使うか、複数のチャネルに作戦を実行する場合、企業はたいてい何とかしてユーザーの ID を確認しようとします。

悪意のあるアクティビティを除外しながら、新規顧客、ゲスト、既存の顧客をシームレスに迎えられるように、顧客体験全体を通じて ID 信頼性を継続的かつ透過的に確立するにはどうしたらいいのでしょうか?

より快適でスムーズな体験を実現するには、リアルタイムな多層構造のオムニチャネル ID の信頼性評価を実施して、ネットワーク、デバイス、環境、挙動、グローバルな情報など多種多様な情報を分析することを検討すべきです。

自分の会社にはどのようなデジタル顧客がいるのかご存知ですか?

IBM® Trusteer® プラットフォームは、デジタル・オムニチャネルのライフサイクルを通じて匿名ユーザーと信頼を素早く透過的に築き、新規顧客との信頼を確立し、既存の顧客との信頼を維持できるように企業を支援するように設計されています。効率性を高めるスケーラブルでアジャイルなクラウド・プラットフォーム、および高度な AI 機能と機械学習機能が組み込まれた情報サービスといった、継続的なデジタル ID 保証を特長としています。

ID 信頼性を複数のチャネルで確立する作業の多くの側面

悪意のある犯罪者は真の ID を簡単に隠すことができます。盗んだ ID を使って新しいアカウントを開いたり、サービスや特別メンバー特典に登録したりすることができます。盗んだ決済データで製品を購入でき、偽の ID や合成 ID (盗んだデータや偽データを本物の ID に加えた ID) を作成して、決済詐欺、新規アカウントの詐欺、第一者詐欺を行うことができます。また、既存の顧客に成りすましてアカウントに侵入し、盗んだ決済情報で製品を買ったり、将来詐欺を働くために個人データを取得したりすることもできます。

悪意のあるアクティビティを暴くには、各ユーザーの ID を 2 つの基本レベル、つまり、デジタル・チャネルへのアクセス方法と接続元を評価する必要があります。デバイスまたは接続が合法に見えても、ユーザーは違うかもしれません。

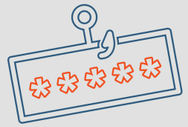
各レベルには、考慮すべき多数のデータ・ポイントがあります。リスク評価に取り込むデータが多いほど、リスク評価は効果的になります。本当のユーザーにとってリスク評価が透明なほど、消費者が期待するスムーズな操作性と信頼性を実現できます。デジタル時代の企業は最終的に、どのユーザーに対して追加のセキュリティー対策を行って ID を確認するのかを見極める必要があります。

幅広いシナリオにわたるリスクの評価

ユーザー

- ゲストのお客様
- 新しいアカウント
- 登録済みのお客様
  - 頻繁なアクセス
- 登録済みのお客様
  - 稀なアクセス

リスク



- 支払い詐欺
- ロイヤルティプログラムの悪用
- ファーストパーティ詐欺
- アカウントの引き継ぎ
  - ポイントの引き出し
  - 保存された支払いデータを使用する
  - 出荷データの変更
- 新規アカウント詐欺
- データ漏洩

主な手がかり

- メールパターンと評判
- 携帯電話番号の情報
- 行動とユーザーの旅のパターン
- 行動バイオメトリクス
- デバイスの信頼性と衛生
- 接続とネットワークの属性
- なりすましの証拠
- アイデンティティ連携
- 悪意のある証拠コンソーシアムのデータ

戦術

- 個人情報の盗難
- 合成アイデンティティ
- 偽のアイデンティティ
- 盗まれた資格情報

オムニチャネル相互作用

- ウェブサイト
- モバイルアプリ
- 携帯電話からコールセンターへ
- 店舗/支店
- ライブチャット/チャットボットインタラクション

新規ユーザー、ゲスト・ユーザー、登録ユーザーの信頼を築く

セキュリティーと操作性の間にある緊張感は、匿名ユーザーと新規顧客と信頼を確立するときに最も鋭く感じられることがよくあります。IBM Trusteer Pinpoint™ Assure ソリューションは、ゲストと新規顧客の悪意ある意図のリスクを理解、検知、予測できるように企業を支援するように設計されています。また、新規アカウントの早期アカウント・モニタリングも実施可能になります。このソリューションは透過的に機能して、独自の豊富な知見とこれらのセグメントに固有のグローバルな情報を相関付けます。

挙動とユーザー行程の分析では、悪意のある BOT 攻撃や既知の悪意のあるアクティビティ使用パターンを検出できます。これらのパターンには、悪意のあるアクティビティに関連付けられたデジタル・フォームの入力手法とパターンの使用、マウスの動き、キーストローク・パターン、Web サイトのナビゲーションがあります。

デバイスの ID、関連付け、信頼性、検疫によって、そのデバイスが信頼できるかどうか、マルウェアで成りすましや侵害が行われているか、あるいは別の悪意のある試みで過去に犯罪者によって使用されていたかどうかを特定できます。また、信頼できるデバイスとしてデバイスをユーザーに関連付けられるかどうかも特定できます。

電話番号情報 は、増加したリスクにフラグを付ける上で役立ちます。たとえば、プリペイド式携帯電話のユーザーは、3 年間アカウント契約しているユーザーよりもハイリスクと見なされる場合があります。

ずさんな対策のため、詐欺犯罪者に利用されることで知られている通信事業者と契約した電話は、大手通信事業者と契約した電話よりもハイリスクと見なされます。アカウント所有者情報を ID 詳細、登録位置情報、ローミング表示と回線ステータスと照合し、グローバルな情報、ユーザー・コンテキストとアクティビティに相関付けることができます。

ID リンク は、同じ ID または ID 属性で新規アカウントが開設されているかどうか、または IBM Trusteer で保護された他の企業での正当なアクティビティと一致しない速度と割合でトランザクションが実行されているかどうかを示すことができます。

世界的なネットワークからの悪意を証明するコンソーシアム・データ を利用して、悪意あるアクティビティを暴くことができます。

小売業におけるデジタル信頼性のメリット

- ロイヤルティー・プログラム登録を透明なセキュリティーを通じて増やす
- 顧客のアカウントを侵害から保護する
- セキュリティー対策の不便さが引き起こす顧客離れを減らす
- エンドユーザーの決済フローを保護する

既存客の信頼を維持

毎回、比類ない顧客体験を実現できるように、登録済みの顧客との信頼をどのように維持していますか?IBM Trusteer Pinpoint Detect は、既存の顧客のユーザーおよびデバイス・プロファイルを透過的に作成し、オンライン ID を継続的に確認することで、アカウントの乗っ取りや不正なログイン/アクティビティの検出を支援するように設計されています。デバイス、セッション、ユーザー、オムニチャネル・ビューといった複数の視点から、ユーザーとアカウントのアクティビティーを包括的に表示します。

デバイスの ID、信頼性、検疫、成りすましのエビデンス。デバイス ID は役に立ちますが、成りすましやマルウェアに感染しやすい弱点があります。より強固な戦略としては、デバイスの信頼性、検疫と成りすましのエビデンス、およびデバイス ID を調べる複数のセキュリティー層があります。

セッションとネットワークの属性 は、ユーザーの接続元と接続時間、使用されている接続の種類、リスクを高める可能性のある疑わしいセッションの特定に役立ちます。

ユーザーの行動、行動認証、ユーザー行程の分析と知見 はユーザー・パターンを確立して、異常なマウスの動き、タイピング・パターン、またはアプリケーション内のユーザー・ナビゲーション・パターンなどの異常を特定します。

悪意のあるパターン情報 は、認証方法を操作または回避使用とする動きを検出し、Remote Access Trojan (RAT) やマルウェアなどの既知の攻撃ツールがあると検知します。デジタル・インタラクションで非常に小さい足跡しか残さないソーシャル・エンジニアリング攻撃の特定にもこの知見が役立ちます。

世界的なネットワークからの悪意のある犯罪者コンソーシアム・データ によって、他の組織を攻撃している既知の悪意のある犯罪者を検出することができます。

オムニチャネルとクロスチャネル・ビュー により、Web サイト、モバイル・アプリ、コール・センターへの携帯電話からの通話、店舗/支店、ライブ・チャット、またはチャットボットのやり取りでのユーザーのアクティビティを表示します。

IBM Trusteer Platform

- 継続的なデジタル ID 保証
- スケーラブルでアジャイルなクラウド・プラットフォーム
- 高度な AI と機械学習が組み込まれた情報サービス

IBM Trusteer が選ばれる理由

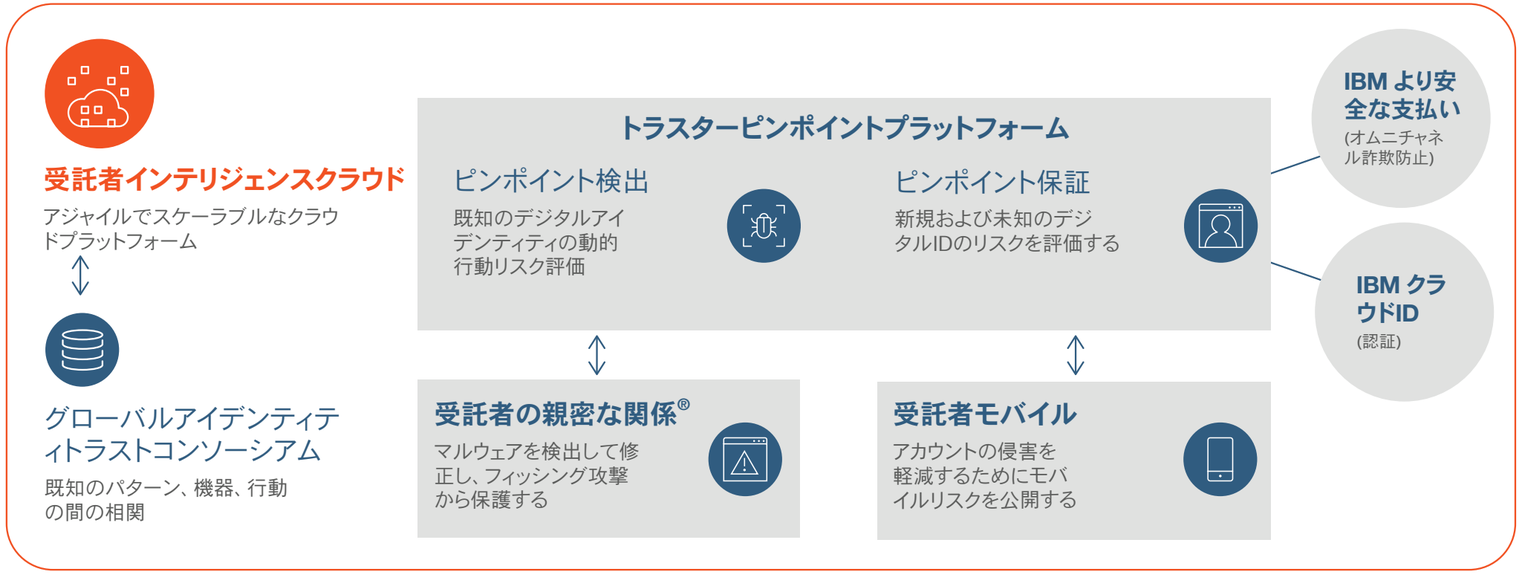
IBM Trusteer は多層型の包括的なユーザー・ビューとモジュール式アプローチにより、幅広いユーザーの ID 信頼性を透過的に築いて、シームレスなデジタル顧客体験を実現できるように企業を支援します。

IBM Trusteer ソリューションは、その強力な情報サービスを利用します。このサービスは AI と高度な分析テクノロジーを組み合わせて、毎日数十億ものセッションを人的情報リサーチャーおよび経験豊富な脅威リサーチャーと共に分析します。クロスオーガニゼーション、グローバル・コンソーシアム、新しい脅威の知見をすべて組み合わせて、新しいパターン、進化する脅威を特定し、保護を素早く適用します。

また、スケーラブルでアジャイルなクラウド・プラットフォームによって、導入を簡素化し、最新情報に基づくリアルタイムのリスク評価を実現することで、効率性を高め、コストを軽減します。

IBM Trusteer の透明性の高い ID 信頼性の詳細については、日本 IBM の担当者または IBM ビジネス・パートナーにお問い合わせいただくか、次の Web サイトをご覧ください。
ibm.com/security/fraud-protection/trusteer

IBM Trusteer: アイデンティティーを発見してください。信頼を築きましょう。



IBM Security

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in Japan
June 2018

本資料は最初の発行日の時点において最新の内容であり、IBM によって予告なしに変更される場合があります。掲載されている製品・サービスは IBM がビジネスを行っているすべての国・地域でご提供できるとは限りません。

本資料の情報は「現状のまま」提供され、商品性、特定目的への適合性に対する保証、および非侵害の保証または条件を含め、いかなる明示的または黙示的な保証も行いません。IBM 製品は、IBM 所定の契約書の条項に基づき保証されます。

適用されるすべての法令と規則の順守は、お客様の責任範囲とします。IBMは法律上の助言を提供することはいたしません。また、IBMのサービスまたは製品が、お客様がいかなる法規も遵守されていることの裏づけとなると表明するものでも、保証するものでもありません。

確実なセキュリティー体制への取り組みについて: IT システムのセキュリティーでは、社内外の不適切なアクセスの防止策、検出、対応に取り組むことで、システムと情報を保護しています。不適切なアクセスにより、情報が改ざん、破壊、不正流用、または悪用される可能性があり、システムへのダメージが生じたり、他者への攻撃のための使用など、システムの悪用が生じることがあります。IT システムまたは製品によってセキュリティー対策が万全になると考えることは危険であり、1 つの製品、サービスまたはセキュリティー対策で不正使用や不正アクセスを完全に有効に防ぐことはできません。IBM のシステム、製品、およびサービスは、合法的で包括的なセキュリティー・アプローチの一部として設計されています。そのため、運用手順を追加することがどうしても必要となり、効果を最大限に高めるには、他のシステム、製品、サービスが必要になることがあります。IBM は、システム、製品、またはサービス、あるいは貴社が、他者による悪意のある行為または不法行為を受けないことを保証するものではありません。

29016929-JPJA-00