IBM Security

パスワードレス顧客体験への道

IBM

パスワードのない安全な世界を想像してみてください

ユーザーが新しくオンライン・アカウントを開設しようとした場合、すでにあるパスワードを再利用する確率が高くなります。これは、次のように説明がつきます。すべてのユーザーは、約 90 個あるアカウントのパスワードを瞬時に思い出す必要があるからです。[1] 顧客はパスワードにうんざりしており、その場しのぎの方法としてパスワードを使い回しますが、これによりセキュリティーが低下します。便利さとセキュリティーのバランスを取ろうとして、セキュリティーを優先するか、便利さを優先するかの二者択一の選択肢の中で揺れることになります。

事実、消費者の 59% が常に、あるいはほとんどの場合同じパスワードを使っており、42% がデバイス上のドキュメントにパスワードを保管しています。[2]1960 年初めにコンピューター・パスワードを使用する技術を発明した Fernando Corbato ですら、パスワード・システムを「ある種の悪夢」と呼んでいました。[3]

ランダムな文字の組み合わせを覚える必要がないデジタル・アイデンティティーの世界を想像してみてください。パスワードの代わりに、指をスワイプしたりボタンをクリックするだけでアカウントにシームレスにアクセスでき、アカウントに安全にログインしているという安心感を持って作業を進められます。これは可能なだけでなく、すでに存在します。ただ、このパスワードレス体験を顧客にどのように提供できるでしょうか？

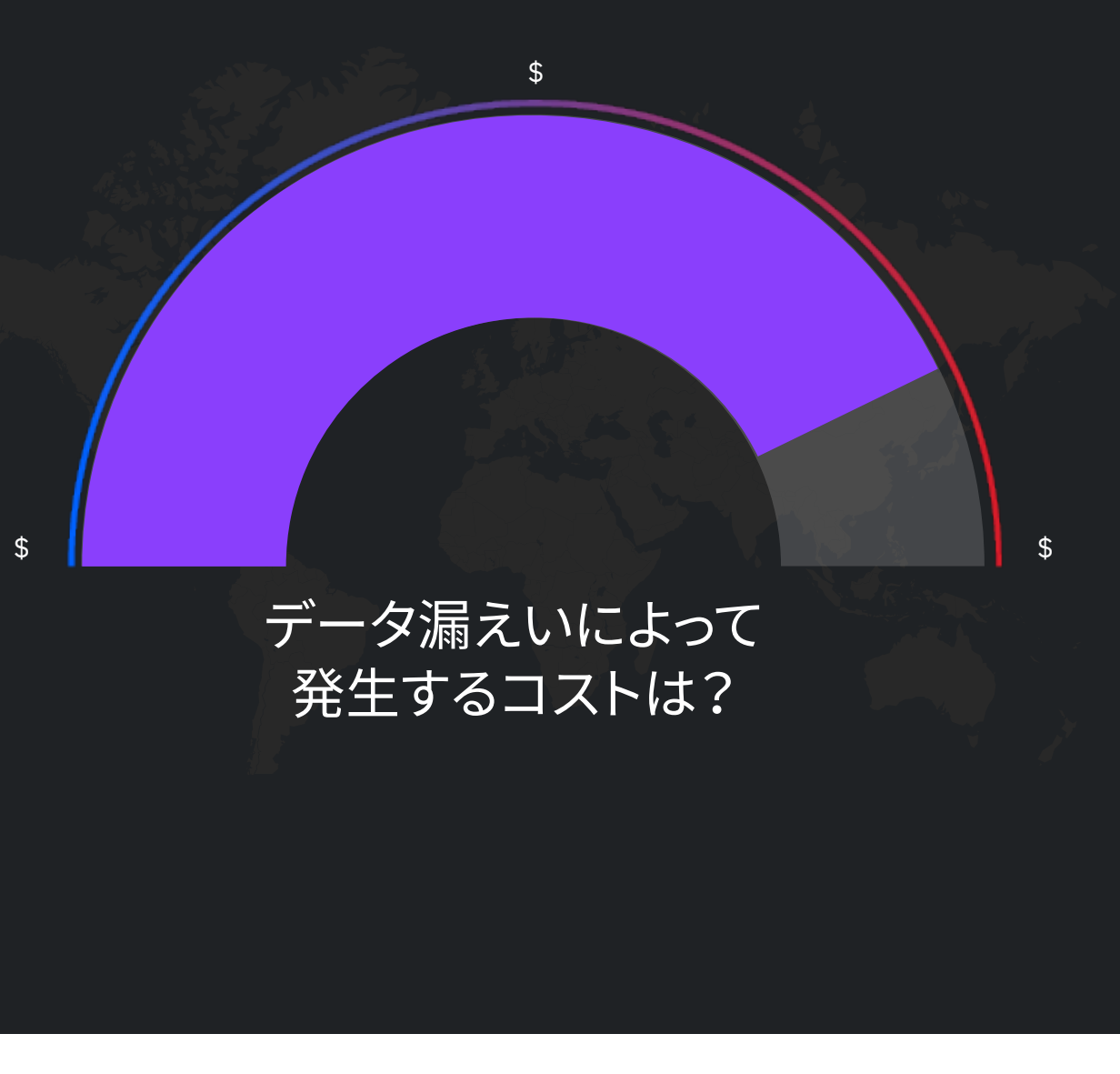
パスワード・システムとは
「ある種の悪夢」である。
cx- Fernando Corbato

コンピューター博物館からの写真

安全地帯から 一歩踏み出す

現実的に、大規模なデータ漏えいの問題は増大しており、その数やコストが減少する兆しはありません。IBM の資金提供を受けて Ponemon Institute が 2019 年に実施したデータ漏えいのコスト調査によると、紛失、または漏えいした機密情報を含む記録当たりの平均コストは 150 ドルです。データ漏えいが起こった各組織の総平均コストは、392 万米ドルです。[4]

2019 年データ漏えいコスト調査報告を読む →



データ漏えいによって
発生するコストは？

企業は、不正行為の増加（およびそれによる信用の失墜）に対し、ユーザーに複雑なパスワードを使用するよう要求することで対処してきました。パスワードレス体験を構築する上で重要になるのは、データ漏えいの脅威によって、ユーザーに厳重なパスワード規制を強いるという安易な方法に戻らないことです。戻ってしまうと、単なるデータ漏えい以上の影響が出る可能性があります。

セキュリティー対策が直観的でないと、ユーザーをいらだたせることが多くなります。これにより、事業の運営コストが増加します。顧客が他のチャネルに移りサイトから離れてしまったり、自分のアカウントにアクセスするためにコール・センターに電話する可能性があります。

コスト節減方法として設置されたコール・センターが、コスト増の原因になりかねません。たとえば、年間コール・センターにかけるコストは 1 兆 3,000 億ドルと見積もられています。[5] コスト増に加え、コール・センターから顧客が悪い印象を受ける可能性があります。

この結果、パスワードを主とする安全対策は、顧客体験の質を下げ、収益に直接影響を与える恐れがあります。

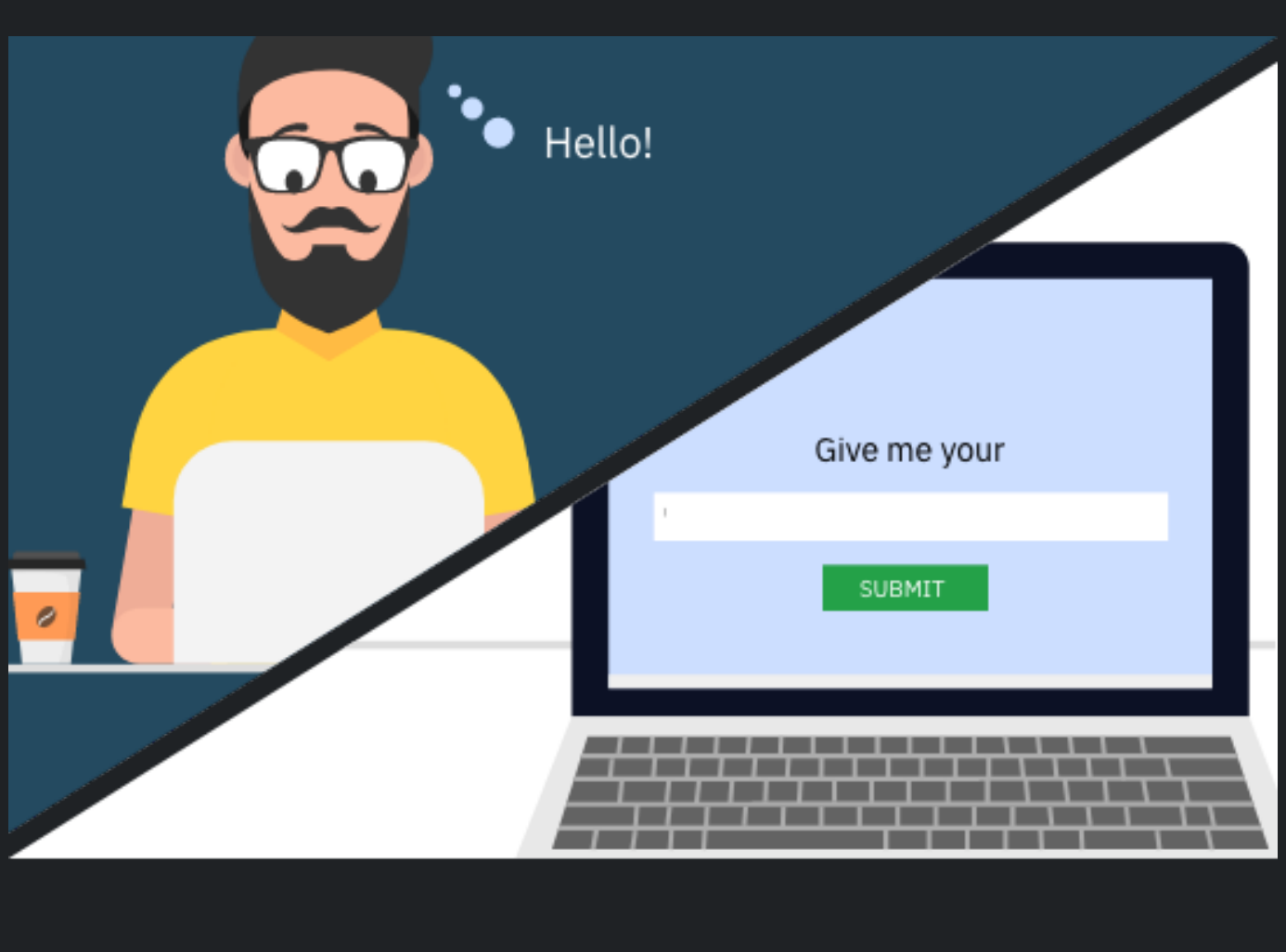
ポイント

年間コール・センターにかかるコストは 1 兆 3,000 億ドルといわれています。

パスワードのデメリットとパスワードのメリット

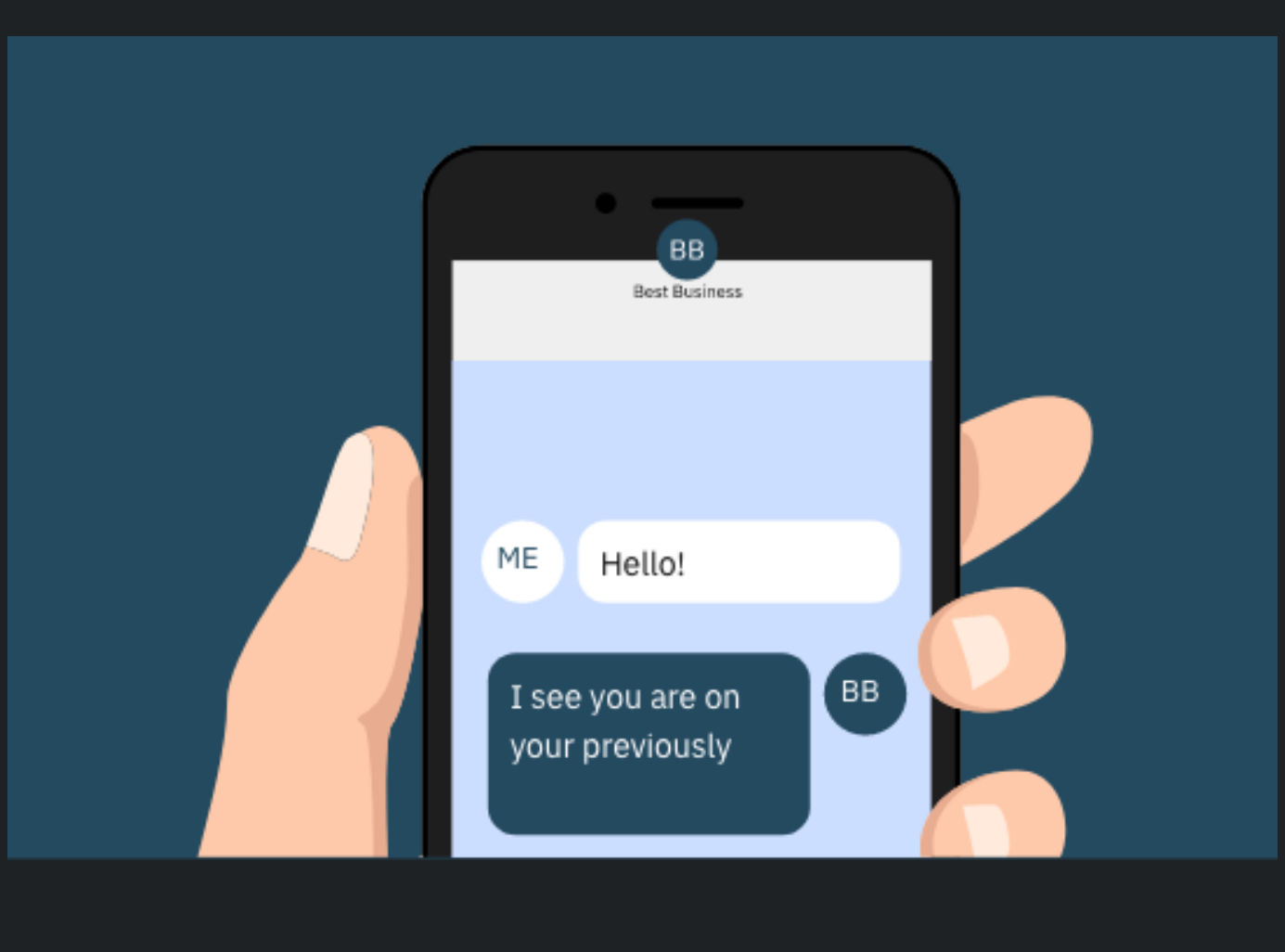
Trusteer について →

従来の方法では、ユーザーに自分の身元を証明することを求めていました。



ユーザー: こんにちは
サイト: パスワードを入力してください。
ユーザー: (数字と記号を含む長いパスワード)
サイト: パスワードが間違っています。
ユーザー: そうだ、パスワードを変更してくださいといわれて変更したはずだ。(数字と記号を含むさらに長いパスワード)
サイト: 認証コードを携帯電話に送信しました。10 分以内に認証コードを入力してください。
ユーザー:「123456!」
サイト: もう一度最初からやりなおしてください。コードの有効期限が切れています。
ユーザー:「36912!」
サイト: ログインできます。

パスワードレス体験は、バランスがとれ、信頼性に基づいています。



ユーザー: こんにちは
サイト: 以前に登録されていた携帯電話です。
サイト: ジェイルブレイクされたり root 化された端末ではないこともわかりました。
サイト: いつもの地域から接続しており、マルウェアがデバイスに入っている形跡はありません。
サイト: あなたのアクティビティーは低リスクです。
サイト: ようこそ

ユーザーが快適に感じる認証方法

組織では、誰も信用しないことを前提としたプロセスが基本となっており、認証を強制し、できるだけ少ないアクセス権だけを与えるイニシアチブが展開されることが多くなります。この過度に侵襲的な方法では、ユーザーは、次から次へと課せられるセキュリティー条件をクリアして自分のデジタル・アイデンティティーを証明していかなければなりません。

これでは、顧客は自分が犯罪者扱いされていると感じても不思議ではありません。しかし、実際に不正アクセスするユーザーは非常にまれです。

<0.1%

IBM Security Trusteer の調査によると、不正アクセスが疑われるユーザーは 0.1% 未満

目標は、製品やサービスを意図した目的と利益のために使用しようとする顧客を、犯罪者ではなく顧客らしく扱うことです。

信頼性と便利性は両立できるはずです。この 2 つの間でバランスを取ることを考えるよりは、厳重なセキュリティーと、顧客が求める摩擦のないプロセスの両方を提供するソリューションが何かを特定することが先決です。

セキュリティーの網をくぐることを何度もユーザーに強いるのではなく、信頼性と便利性の両方を提供する摩擦のない体験を提供するのです。

パスワードレス・セキュリティーのf基礎を築く

パスワードレス認証 は、適切なユーザー・コンテキストを取得することから始まります。意思決定フレームワークにコンテキスト・データを設定すると、合法ユーザーの大多数にシームレスなエンドユーザー体験を提供できます。

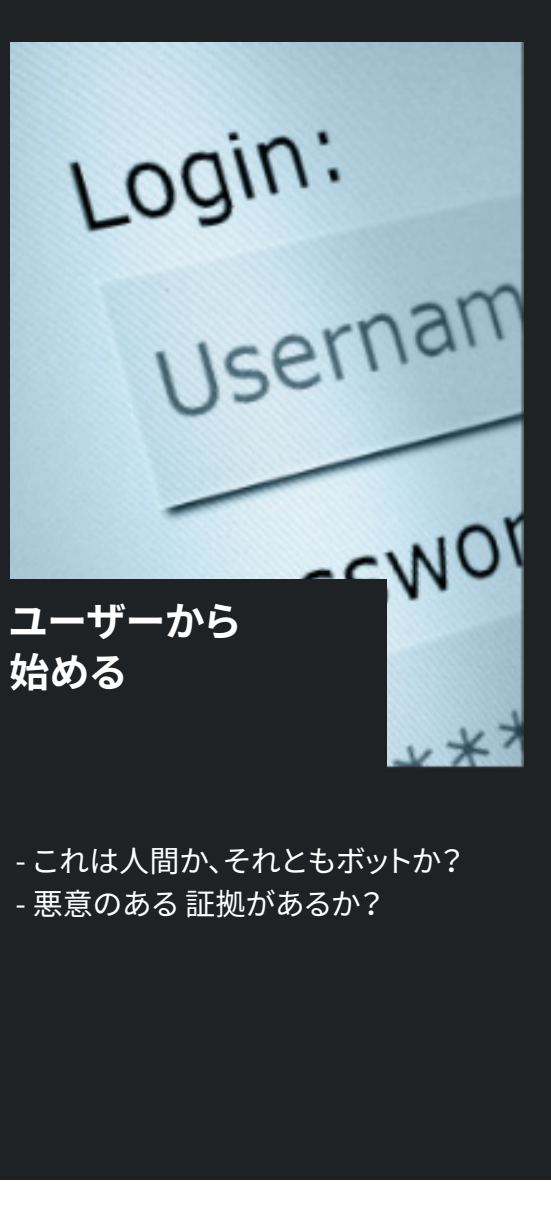
この目標を達成するには、以下の 3 つのことが重要になります。
- 顧客に提供しているサービスから 注意をそらすセキュリティー操作を最小限に抑える
- ユーザーのデジタル操作全体について徹底的に 調査する
- ユーザーの包括的視点をやりとりの中で継続して取得することにより 信用（トラスト）を確立する

パスワードレス体験の基礎を築くには、処理ごとにユーザーの信頼性を透過的に分析する必要があります。

ポイント

目標は、顧客を、犯罪者ではなく顧客らしく扱うことです。

デジタル・アイデンティティーの信頼性はコンテキストから始まる



ユーザーから始める

- これは人間か、それともボットか？
- 悪意のある 証拠があるか？

ユーザーのデバイスをオンボードする

- プリペイド携帯電話か？
- ジェイルブレイクされたり root 化された端末か？
- 正しい電話番号 または電子メールか？

ユーザーのアクティビティーを評価する

- 既知の 悪意のあるパターンか？
- 帯域外認証 (OOB) をすり抜けたか?

ユーザーのネットワークを特定する

- ログオン・プロキシーがあるか？

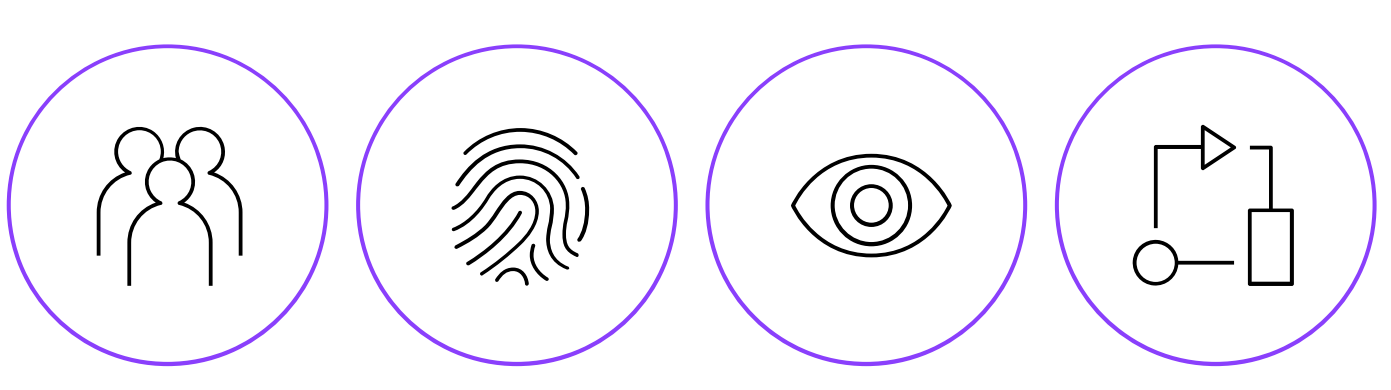
ユーザーの行動を監視する

- これは既知のユーザー行動パターンか？
- 通常と異なる自動化された マウスの動きがあるか？

デジタル・トラストのフレームワークを理解する

コンテキスト・データを使って構築されたパスワードレス・セキュリティーの基礎の効力は、デジタル・トラストのフレームワークにそのコンテキストをどのように適用するかで決まります。結局のところ、フレームワークは動的で柔軟である必要があります。ユーザーにどれだけのコンテキスト情報が紐づけられているかによって、ユーザーがアクセスするセキュリティー・レイヤーは異なる必要があります。

ここに、デジタル・トラスト・フレームワークを適用する上で役立つ 4 つの構成要素を示します。



これらのインターロック・ブロックにより、主に背景で動作する、継続的なセキュリティーが常時提供できます。これにより、状況に応じてポリシーを実装する柔軟性が得られます。常に変化する特定のビジネス・ニーズを基に新しいポリシーを簡単に実装できます。

顧客に自分が守られていると感じさせる

顧客は、個人情報が保護されているとは信じず、保護が目につくと信用を失いかねないため、保護は透明である必要があります。シームレスで柔軟な方法でユーザーのデジタル・アイデンティティーが保護されていると知らせることで信頼性が得られます。これは、以下により達成できます。

- 認証登録を含める
- 認証方法を顧客自身が選択できるようにする
- 必要な場合はステップアップ認証を使用する

パスワードレスは、セキュリティーがないことではありません。
顧客にこれを気付かせることが大切です。

ポイント

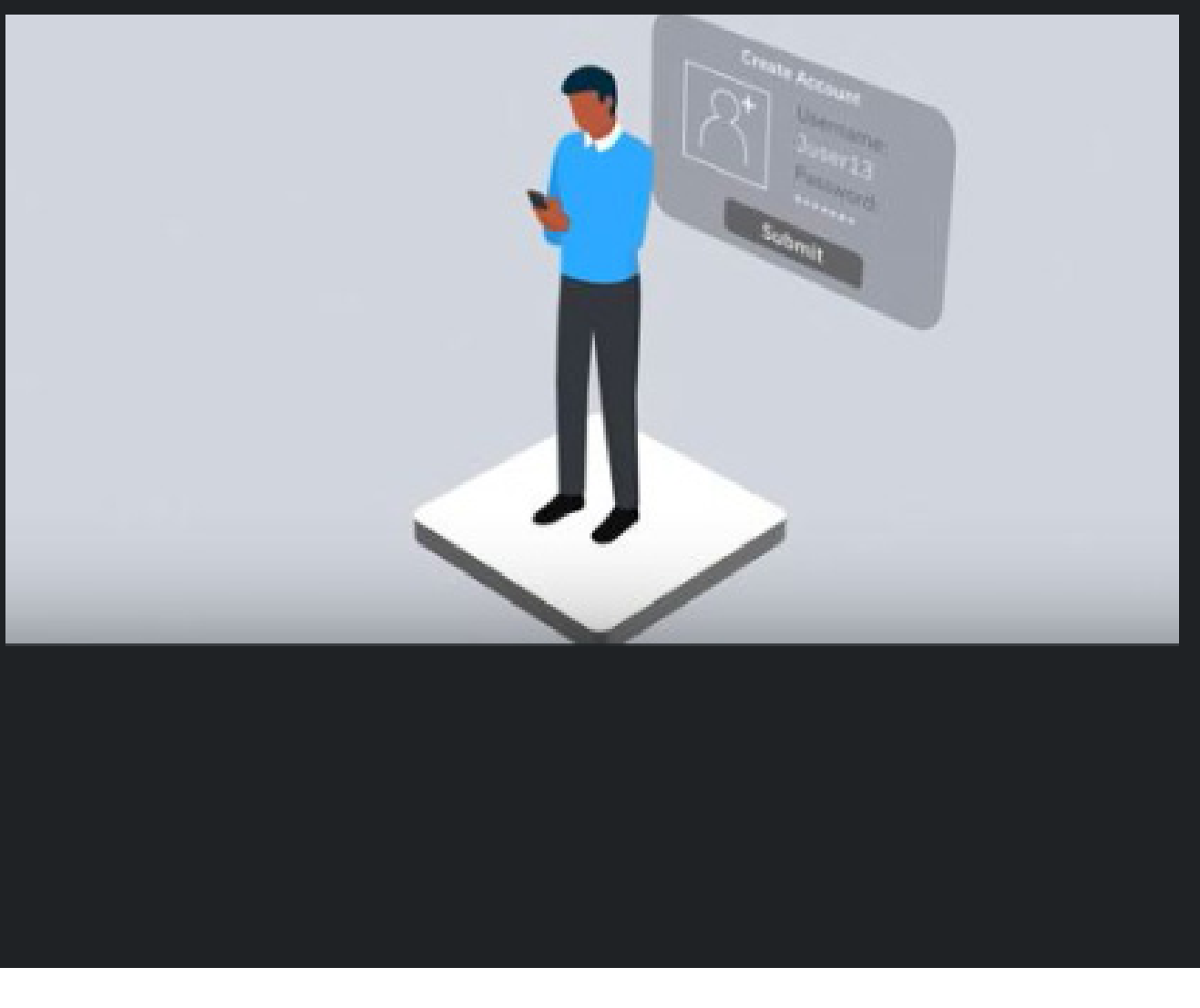
パスワードレスは、セキュリティーがないことではありません。顧客にこれを気付かせることが大切です。

リスクの高い行動にも対応

パスワードのない環境は、セキュリティー・レベルを下げることにはつながりません。リスクの高い行動が検知され、ユーザーとのやりとりに認証が適切な場合に、対処が必要です。

IBM Security Trusteer Pinpoint の製品は、ゲスト・ユーザーから新しいアカウントのセットアップにいたるまで、バックグラウンドで継続的にユーザーのデジタル操作を認証します。顧客がサービスを使用しているセッション中ずっと動作し続け、ユーザー体験に影響を与えることなくユーザーを守り、必要な場合は不正なユーザーに対処します。

IBM Security Trusteer は、クラウドベースのインテリジェンスや、人工知能、機械学習を使用して悪意のあるユーザーから新規顧客と既存顧客の両方を守りながら、高品質の体験を提供します。



何もしないことがコストにつながる

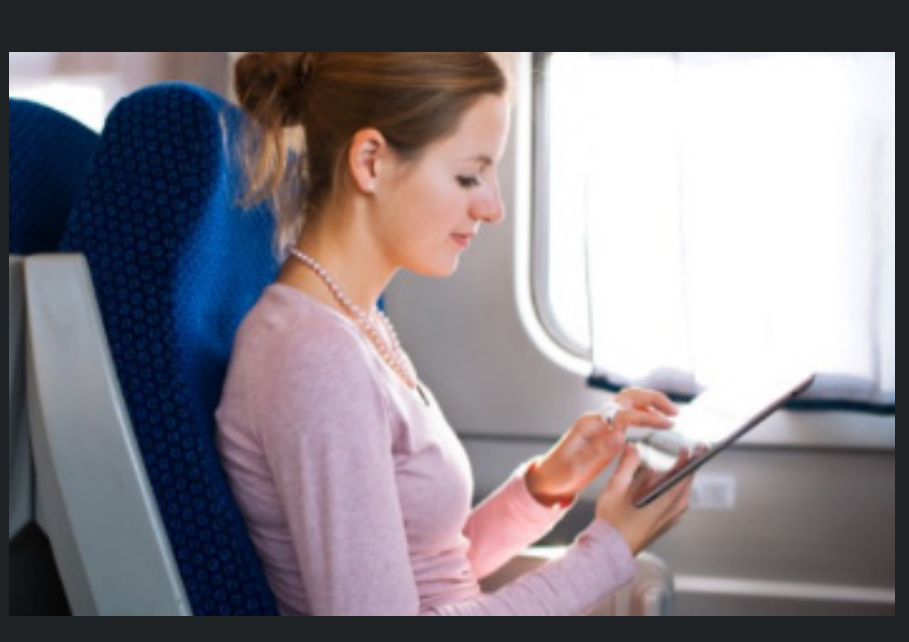
何もしないことは、競争上の価値の減少というコストにつながります。Gartner 社によると、2022 年までに大規模およびグローバル企業の 60% と、中規模企業の 90% における 50% 以上のユース・ケース（現在は 5% 以下）でパスワードレス方法が実装されると考えられます。[6] 顧客が求める保証を他の企業は提供しているのに、ユーザー認証に機械学習機能を使用できない企業は市場シェアを失います。

ポイント

ユーザー認証に機械学習機能を使用できない企業は市場シェアを失います。

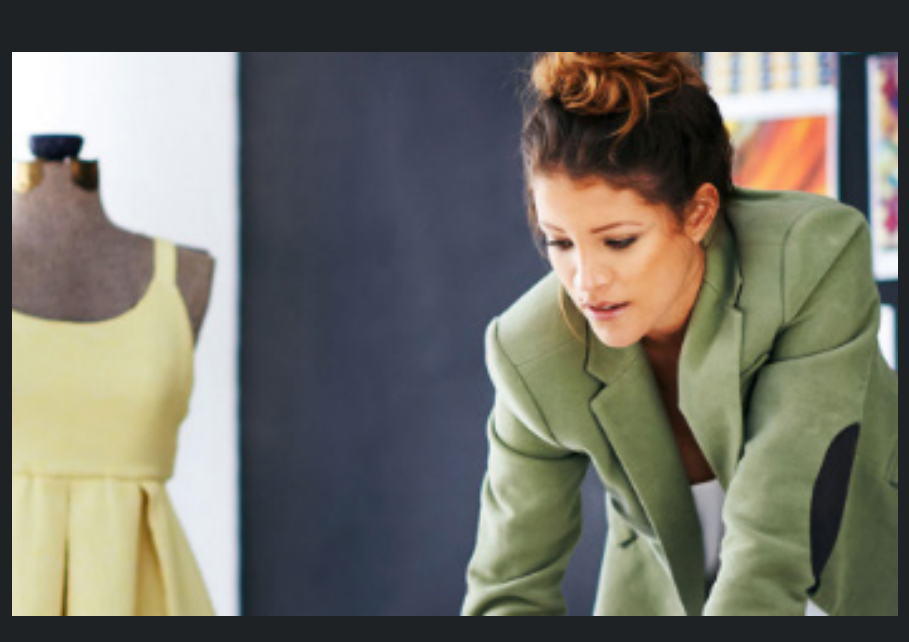
信用はビジネスの基本であり、セキュリティーは信用にとって非常に重要です。

次のステップ



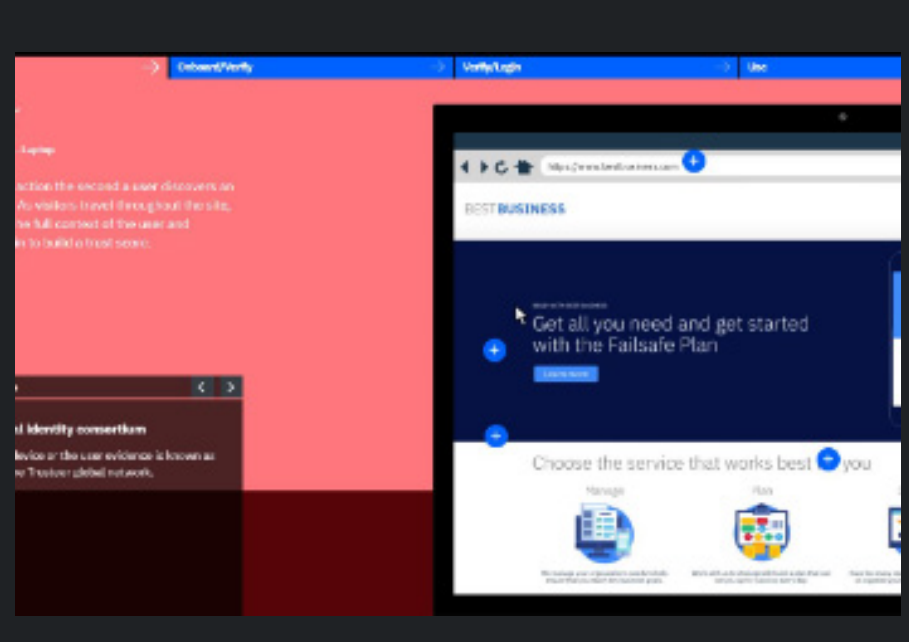
IBM Trusteer ソリューションの概要
シームレスなデジタル顧客体験の構築

ソリューションの概要を見る



オンデマンドWebセミナー
ユーザーの振る舞い分析で防ぐ！不正（なりすまし）ログイン対策

ソリューションの概要を見る



Trusteer について
IBM Trusteer によるデジタル・アイデンティティーの信頼性を構築

ソリューションの概要を見る

出典

1. Phys.org, When Customers Forget Their Passwords, Business Suffers, Tim Johnson, June 20, 2017
2. LastPass, New Research: Psychology of Passwords, Neglect is Helping Hackers Win, Katie Petrillo, May 1, 2018
3. Wall Street Journal, Man Behind the First Computer Password: It's Become a Nightmare, Danny Yadron, May 21, 2014
4. IBM and Ponemon Institute, Cost of a Data Breach Study, July 2019
5. IBM, How Chatbots Can Help Reduce Customer Service Costs by 30 Percent, Trips Reddy, October 17, 2017
6. Gartner, Market Guide for User Authentication, Ant Allan and David Mahdi, November 26, 2018