

# デジタルブランドの 信頼度調査から考察する 顧客アイデンティティの重要性

---

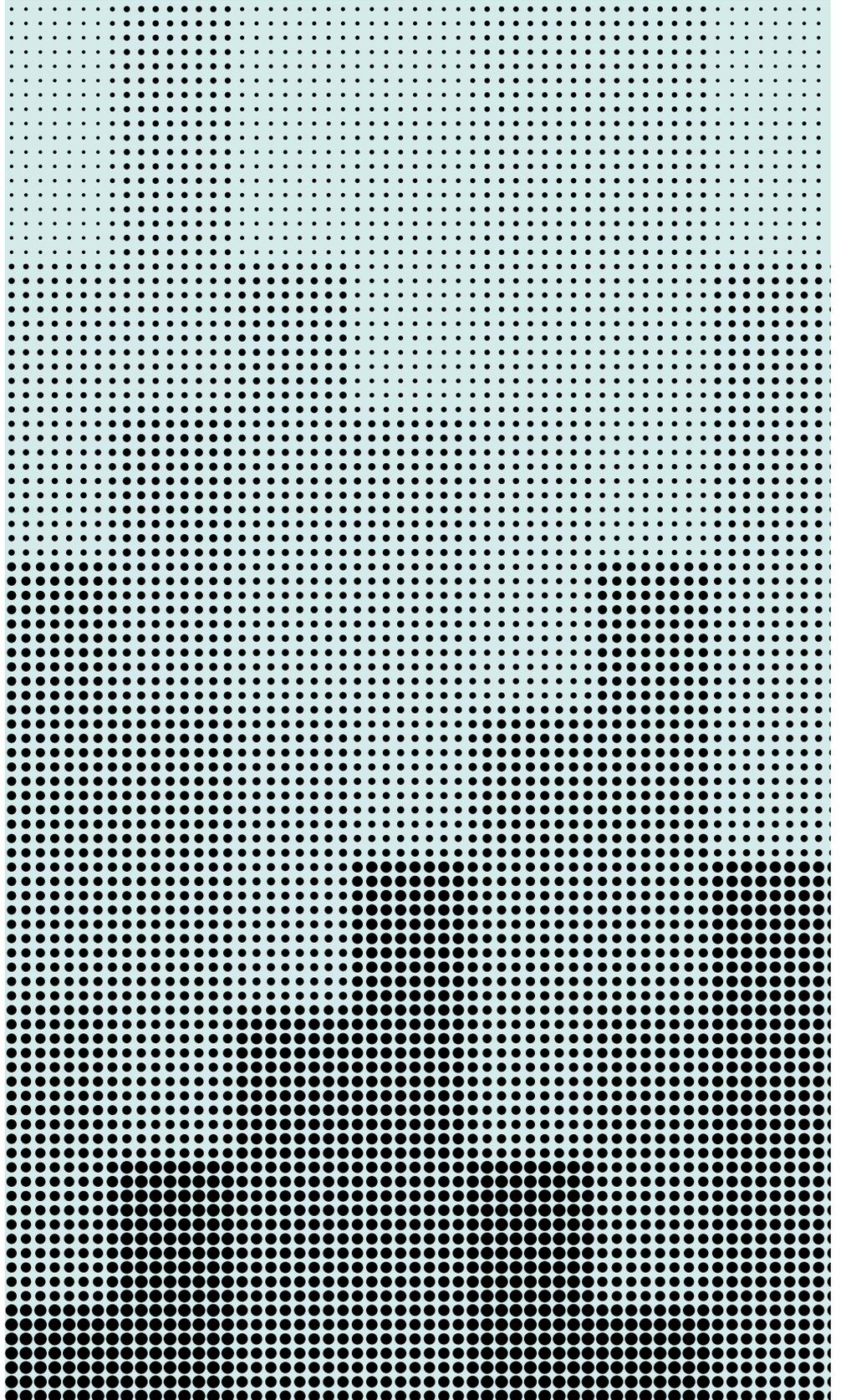
Okta Inc.

---

Okta.com

---

press@okta.com



## Contents

- 2 はじめに
- 3 今日のデジタルブランドが消費者からの信頼を築くには？
- 7 デジタルブランドへの信頼を失くす要因とその影響
- 9 デジタルブランドが消費者からの「信頼」を得るためには？
- 11 未来の企業のセキュリティをOktaで実現

## はじめに

コロナ禍において、「信頼」という概念が私たちの仕事や生活にとって最優先事項となりました。多くの企業は、従業員を「信頼」して在宅勤務を推進することを余儀なくされました。また、サイバー攻撃やデータ侵害数がかつてないほど高まっている中であっても、消費者は、オンライン上で様々な製品・サービスを提供している企業（以下、デジタルブランド）を「信頼」して商品を購入しています。

昨年1年間で消費者は、ネットスーパーでの買い物をはじめ、オンラインレッスン、バーチャル観光、Zoom懇親会にいたるまで、あらゆる種類のデジタルエクスペリエンスを受け入れるようになったため、この期間で習得したデジタル習慣が今後も進化を遂げながら続いていくことが想定されます。そのため、デジタルブランドは、消費者がオンラインで安心して快適に商品・サービスを購入できる仕組みを構築し、消費者からの「信頼」を得ていくことが最重要の課題となっています。

このような状況でデジタルブランドが消費者からの「信頼」を得るためにはどのような取り組みをしていったら良いのでしょうか。この答えを探すために、Oktaは調査機関のYouGovと協力して、消費者がデジタルブランドを「信頼」するためにどのような要素を重視しているのか、デジタルブランドへの「信頼」を失くしてしまう要因は何なのか、そして、デジタルブランドへの「信頼」を失くした場合に消費者がどのような行動をとるのかについて調査するため、世界10か国（米国、英国、オランダ、イタリア、フランス、スウェーデン、オーストラリア、ドイツ、日本、スペイン）の13,163名のオフィスワーカー（日本では1,005名）を対象に調査「The State of Digital Trust」を実施しました。調査期間は、2020年11月26日から12月10日です。

本レポートでは、消費者でもある世界中のオフィスワーカーからの回答をふまえて、デジタルブランドが消費者からの「信頼」を得るために、今後どのようなことを考慮していくべきか考察します。

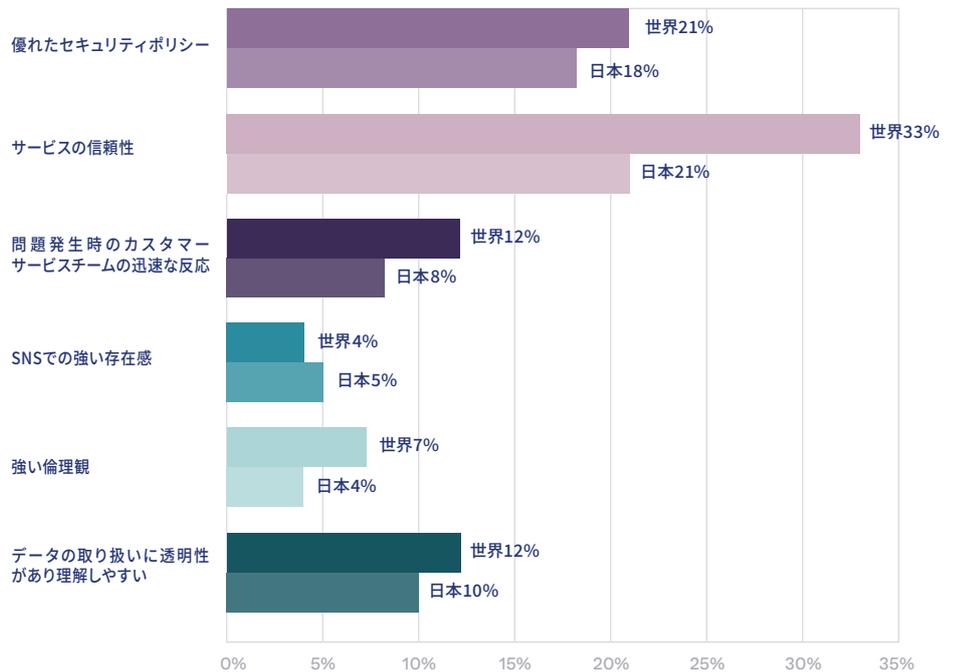
# 今日のデジタル ブランドが消費 者からの信頼を 築くには？

## 消費者の期待に応えるサービスの信頼性

信頼を置くデジタルブランドが備えている最も重要な特性は何かという質問に対して、世界中の回答者が選択したのは、「サービスの信頼性（注文した製品を約束した配達予定日までに届けるなど）」（世界33%、日本21%）でした。日本においてもこの特性が最も重視されていました。実際、優れたデジタルエクスペリエンスを提供しているデジタルブランドは、アクセスのトラフィックが増加しても安定して製品・サービスを提供する「サービスの信頼性」に力を入れています。消費者が安心して個人情報を入力でき、在庫情報に基づいて商品がいつ配達されるのか、発送されたのか、配送状況がどうなのかを随時SMSやメール、アプリなどで消費者に報告しながら、商品を配達予定日までに届け、最後には配達完了通知まで届ける仕組みを構築しています。

### あなたが信頼を置くデジタルブランドが備えている最も重要な特性は？

（該当するもの1つ） Total: 世界13,163名、日本1,005名



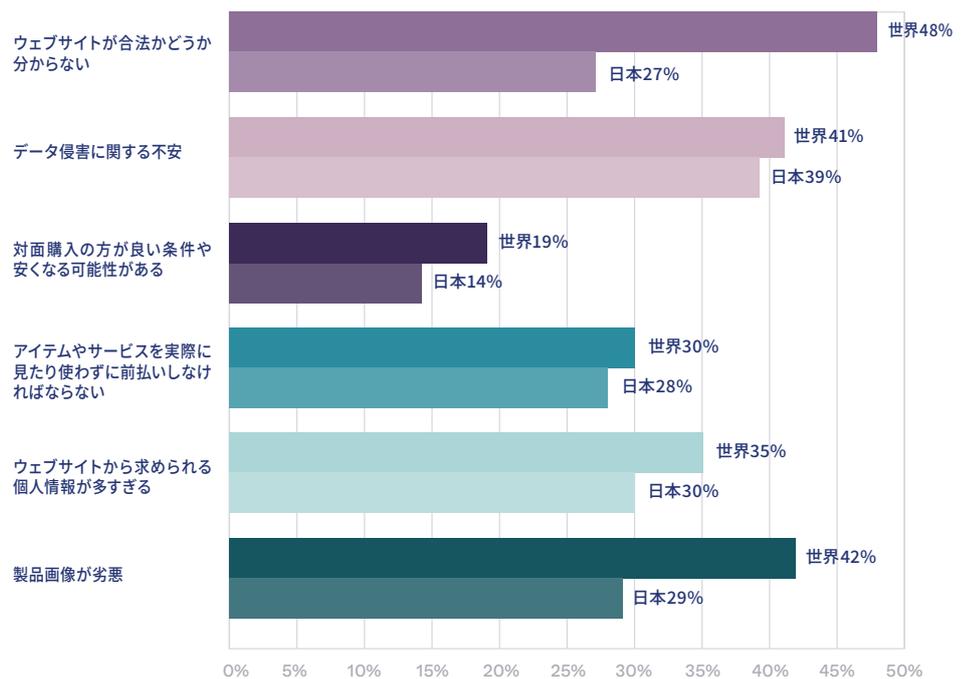
## なりすましやデータ侵害を防ぐ優れたセキュリティポリシー

回答者が重視する特性として2番目に多かったのは、「優れたセキュリティポリシー（多要素認証、安全なログインオプションの提供など）」（世界21%、日本18%）でした。消費者の個人情報が漏洩することがないようにセキュリティ対策を講じていることが「信頼」につながります。今回の調査対象者の中で在宅勤務ができる回答者（世界9,127名、日本445名）に、在宅勤務の際に何を警戒しているか尋ねたところ、「機密データの取り扱いや共有によるデータ侵害」（世界38%、日本48%）や、「フィッシングEメール」（世界37%、日本44%）を最も警戒していることが分かりました。特に日本ではこの2点に対する警戒が高いことが伺えます。

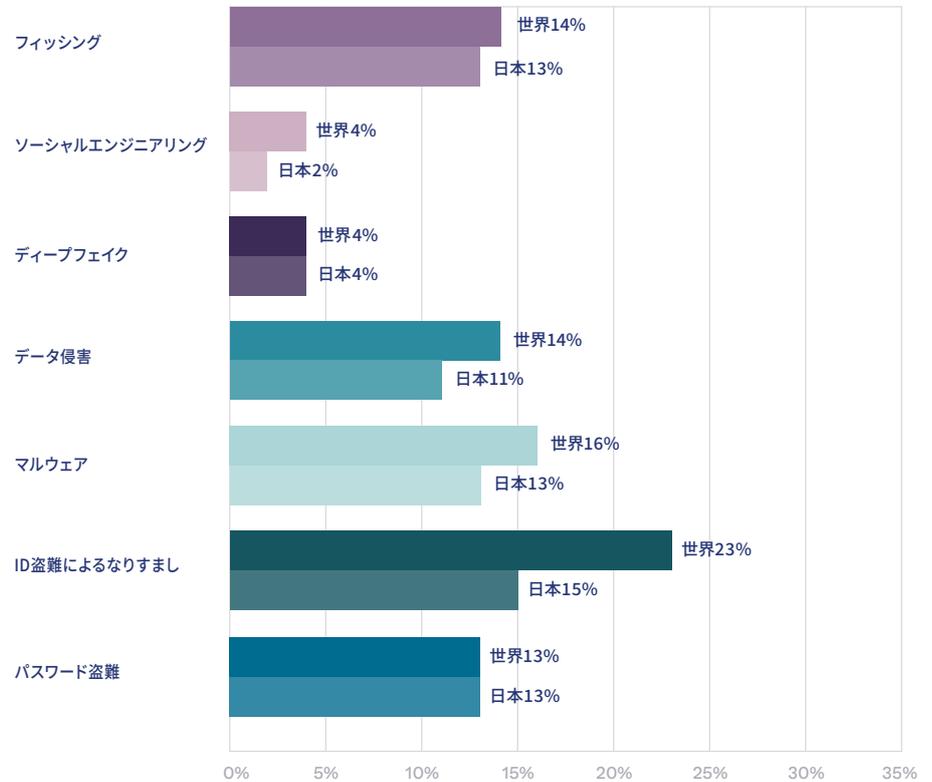
また、デジタルブランドから商品・サービスを購入する時に不安に思っていることを聞いたところ、「データ侵害に関する不安（企業の顧客に関する個人情報や機密情報が、意図的にまたは意図せずに、信頼できない環境に公開されるなど）」（世界41%、日本39%）を多くの方が抱いていました。さらに、今後晒される危険が最も高いと思うデジタルセキュリティの脅威について質問したところ、最も多かった回答が「ID盗難によるなりすまし」（世界23%、日本15%）でした。デジタルブランドは、多要素認証など強力な認証要素を取り入れることによって、ハッカーによるなりすましを防ぐことが求められています。

### オンラインでアイテムやサービスを購入する際にあなたが抱く不安は？

(該当するもの全て) Total: 世界13,163名、日本1,005名



今後ある時点で晒される危険が最も高いと思うデジタルセキュリティの脅威は？  
(該当するもの1つ) Total: 世界13,163名、日本1,005名

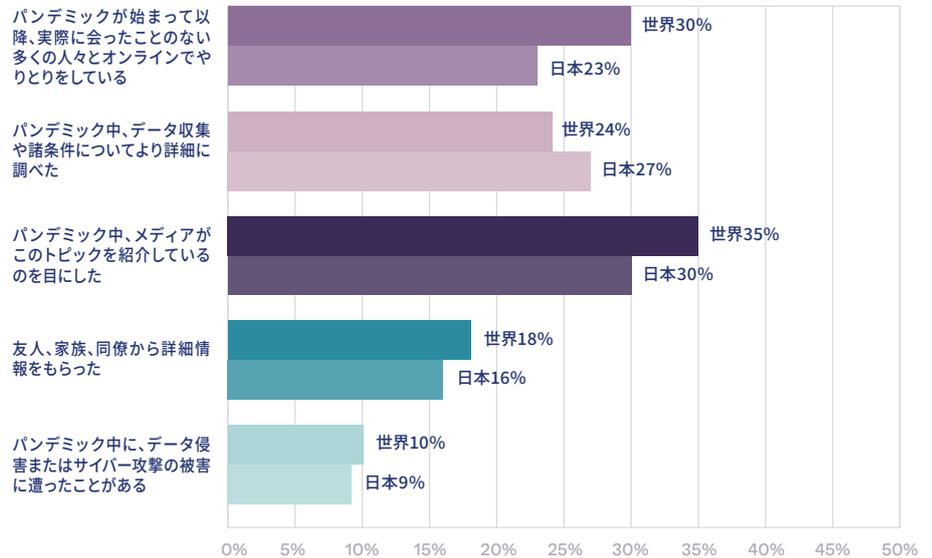


## 透明性のある個人データの扱い

回答者が重視する特性で3番目に多かったのが、「データの取り扱いに透明性があり理解しやすい(個人データがどのように使用されるかが明確に説明されているなど)」(世界12%、日本10%)でした。このコロナ禍で消費者は年代を問わず、個人データの扱いに対して慎重になっています。実際、コロナ禍になってから、デジタルデータをオンラインで他者に渡すことに以前よりも慎重になったと回答しています(世界41%、日本39%)。以前よりも慎重になった回答者(世界5,408名、日本393名)にその理由を聞いたところ、「パンデミックが始まって以降、実際に会ったことのない多くの人々とオンラインでやりとりをしている。」(世界30%、日本23%)、「パンデミック中、データ収集や諸条件についてより詳細に調べた」(世界24%、日本27%)という回答が多く見られました。実際に「パンデミック中にデータ侵害またはサイバー攻撃の被害に遭った」(世界10%、日本9%)方々もいました。デジタルブランドは、個人データをどのように扱っているのか、透明性を持って消費者に開示することで消費者の信頼を得ることが必要です。

## デジタルデータをオンラインで他者に渡すことに以前よりも慎重になっている理由は？

(該当するもの全て) Total: 世界5,408名、日本393名



## デジタルブランドの倫理観とSNSでの存在感

消費者が重視する特性としてあげる割合が比較的少なかったのは、デジタルブランドの「強い倫理観（環境への取り組みや社会問題に関する運動への支持など）」（世界で7%、日本4%）でした。「強い倫理観」については、国ごとに見ると米国で重視する消費者が多く（10%）、日本では最も低い（4%）結果が出ていました。また、デジタルブランドを信頼しないことになる要素を質問した際にも、「事業活動や商品調達が倫理的に行われていない」（世界8%、日本6%）、「社会問題や運動に対する企業の立場や姿勢を示していない」（世界3%、日本3%）を選択した回答者の割合が低く出ていました。

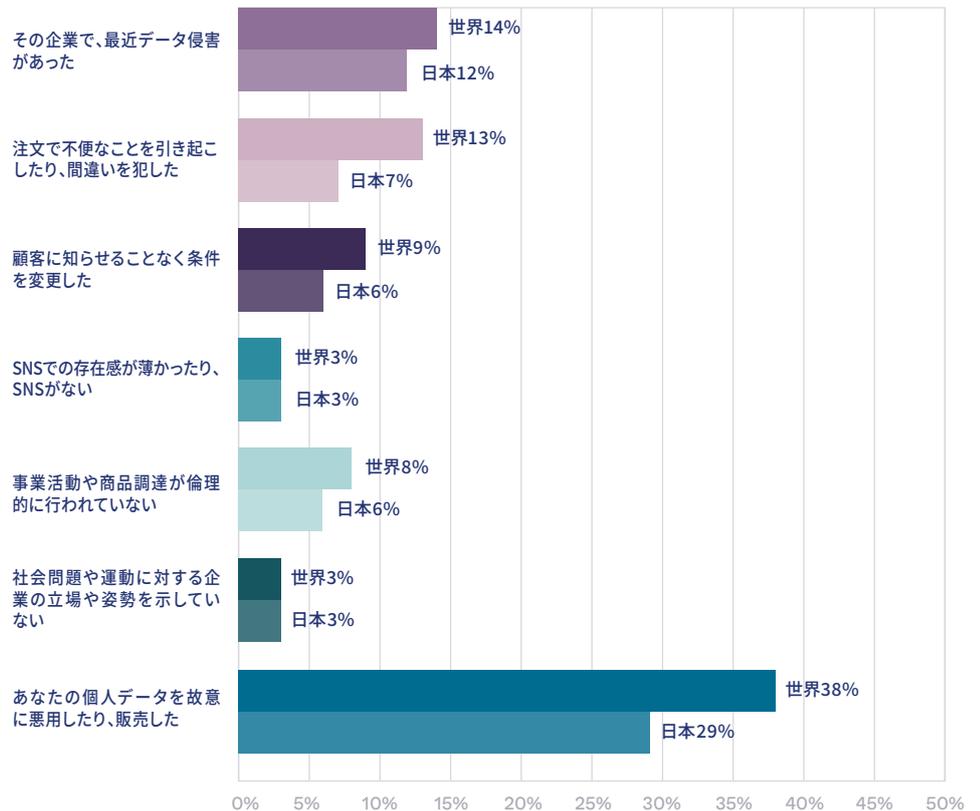
同様に重視する特性として低かったのは、「SNSでの強い存在感（頻繁なSNS投稿など）」（世界4%、日本5%）でした。「SNSでの強い存在感」については、日本（5%）、イギリス（2%）、ドイツ（3%）、米国（4%）など各国での割合が低く出ていました。デジタルブランドを信頼しないことになる要素の質問においても、「SNSでの存在感が薄かったり、SNSがない」（世界3%、日本3%）を選択した割合が低い傾向にありました。

## デジタルブランドへの信頼を失くす要因とその影響

デジタルブランドへの信頼を失くす要因として多く挙げられたのは、「個人データを故意に悪用したり、販売した」（世界38%、日本29%）、「その企業でデータ侵害があった（顧客に関する個人情報／機密情報が意図せずに信頼されない環境に公開されたなど）」（世界14%、日本12%）でした。特にアメリカ（42%）と英国（47%）で、データの取り扱いや販売を誤るとデジタルブランドへの信頼が失われると回答している割合が多い事がわかりました。これは、イタリア（29%）、フランス（23%）、スペイン（28%）、日本（29%）の回答者よりも多い割合です。

### あなたがデジタルブランドを信用しないことになる要因は？

（該当するもの1つ） Total: 世界13,163名、日本1,005名

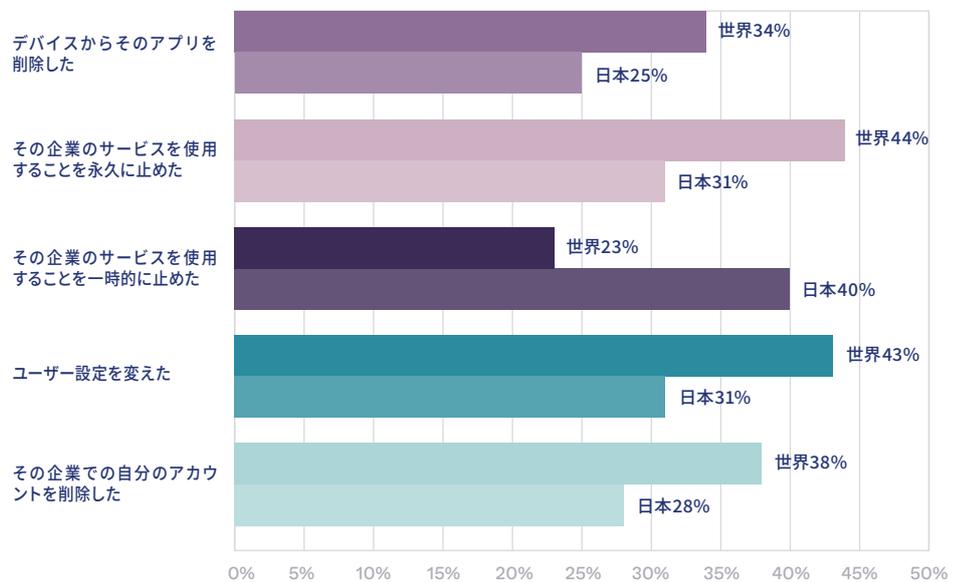


しかし、消費者の個人データを安全に取り扱うデジタルブランドの能力に関する不確実性は世界的な傾向です。ドイツ人の23%、日本人の22%、アメリカ人の19%がこれを懸念事項として挙げています。また、世界の平均で見ると、消費者の年齢層が高くなるほど、データ取り扱いの不備に対する許容度が低くなっています（「個人データを故意に悪用したり、販売した」を選択した回答者のうち、18～24歳が23%に対し、55歳以上は44%）。

信頼を失くしてしまった場合、世界の回答者の76%（日本では62%）が、あらゆるタイプの商品であってもデジタルブランドから購入する可能性がないと回答しています。また、実際にデータ侵害やデータの悪用によって、デジタルブランドへの信頼を失くした回答者（世界4,940名、日本264名）がとった行動で多かったのは、「永久にその企業のサービス使用を止めた」（世界44%、日本31%）、「その企業での自分のアカウントを削除した」（世界38%、日本28%）でした。データ侵害による信頼喪失の影響は世界各国で大きいと言えます。

### 信頼を失った結果としてあなたがとった行動は？

(該当するものを全て) Total: 世界4,940名、日本264名



# デジタルブランドが消費者からの「信頼」を得るためには？

今回の調査結果をふまえると、デジタルブランドが消費者から「信頼」を得るには、今後オンラインでのアクセスが急激に増加したとしても安定して安全に商品・サービスを提供する「サービスの信頼性」、なりすましやデータ侵害を防ぐための多要素認証を用いた「優れたセキュリティポリシー」、そして、消費者の個人データをどのように扱っているのか分かりやすく開示する「透明性のある個人データの扱い」が最優先事項であることを示唆しています。

デジタルブランドがこれらの最優先事項に取り組むためには、具体的にどのようなテクノロジーに投資すべきでしょうか。Oktaでは、顧客のアイデンティティとアクセス管理 (Customer Identity and Access Management = CIAM) の導入が重要な鍵を握ると確信しています。なぜなら、CIAMを導入して、適切なユーザーのみが適切なリソースに適切な時間アクセスできるようにすることで、ユーザーのアイデンティティを保護し、データ侵害を防ぐことができる信頼性のあるサービスを迅速に市場に投入できるからです。また、ユーザーの個人データを統合して管理することで、厳格なセキュリティポリシーを展開できます。

デジタルブランドは、CIAMソリューションを導入することで以下の3つを実現できます。

## 1) 新しいアプリケーションの市場投入までの時間を短縮させる

最新のCIAMプラットフォーム導入により、開発者は、新しいアプリケーションを迅速かつ安全に構築し、迅速に市場投入できます。カスタマイズ可能なアイデンティティのビルディングブロックを使用することで、複雑なアイデンティティ機能でよくエラーが発生しがちなカスタムコードや、数少ない専門の開発者への依存を回避できます。開発者がすでに知っている言語のソフトウェア開発ツールキットを備えたCIAMプラットフォームを活用することで、開発者は効率的に作業できます。

新しいカスタムアプリを構築するときは、アイデンティティ認証やアカウント検証機能など、消費者が期待する安全で最新のエクスペリエンスを提供するために必要な基盤が整っていることを確認することが重要です。また、OpenID Connect、OAuth、SAMLなどの最新の認証標準をサポートして、最新のセキュリティとアイデンティティの仕様を最新の状態に保つことが必要です。さらに、より最適なユーザーエクスペリエンスを実現するために、適切なタイミングで適切なセキュリティを適用するログイン機能も重要です。

## 2) 新規と既存のアプリケーションの拡張性を向上させる

消費者のニーズは、コロナ禍において変動し続け、それに応じてオンライントラフィックも変動しています。アプリのパフォーマンスを妨げ、ピーク時にユーザーがログインできないようにするレガシーのアイデンティティコンポーネントに依存しているとしたら、最新のCIAMプラットフォームを実装する必要があります。より多くの人々がデジタルインタラクションに依存するにつれて、大量のユーザーとトラフィックの急増を安全に処理する機能があることを確認してください。具体的には、CIAMソリューションは、1分あたり500,000認証の範囲でピークワークロードに達した場合でも、ユーザーエクスペリエンスに影響を与えることなく動的に拡張できる必要があります。

アプリケーションの拡張性に加えて、増加したユーザー数をサポートするための組織の能力の拡張性についても考慮する必要があります。ユーザーが増えると、ユーザー管理タスクも増えます。可能な場合はユーザー管理プロセスを自動化して、すべてのアプリがサポートチームに負担をかけずにユーザーの成長を効率的に処理できるようにしてください。これには、セルフサービスのパスワードのリセット、登録、多要素認証 (MFA) の登録などの機能が含まれます。特にビジネスが成長し、ハッカーの標的になるにつれて、セキュリティを損なうことなくアプリを拡張することが重要です。

### 3) 顧客体験を長期的に最適化する

適応型のアイデンティティレイヤーを導入すると、顧客が期待するレベルのデジタル上での利便性を提供し、長期的に進化するニーズに対応できるようになります。プログレッシブプロファイリングや、電子メールのマジックリンクまたはWebAuthnを使用するパスワードレスのオプションなど、拡張可能でコンテキストに応じてカスタマイズされたアクセスエクスペリエンスを構築します。次に、さまざまなブランド、地域、タッチポイントにまたがるアイデンティティストアを統合して、顧客を360度見渡せるようにすることで、カスタマーエクスペリエンスを段階的に向上できます。このアプローチにより、デジタルブランドは、競合他社と差別化するシームレスなオムニチャネルエクスペリエンスを提供できるようになります。

また、ユーザー管理を改善することで、関連するパーソナライズされたエクスペリエンスの提供に必要な貴重な顧客データを収集できます。たとえば、ユーザープロフィールを大規模に収集、保存、管理するための適切なプラットフォームを使用すると、異なるユーザーストア間でプロフィールを統合し、新しいユーザーが安心して個人情報を共有できるようにし、大量のアイデンティティのデータを必要に応じて簡単に移行できます。その結果、すべてのユーザー属性、グループメンバーシップ、特権、セキュリティポリシーを一元管理でき、ユーザー管理の管理コストを大幅に削減できます。

# 未来の企業の セキュリティを Oktaで実現

アイデンティティは、「信頼」に基づく優れたセキュリティを構築するうえで絶対に欠かせない基盤となります。Oktaは、急速に変化するデジタル世界においてお客様が消費者や従業員の間で「信頼」を高めるのに役立つ、幅広いアイデンティティ管理ソリューションを提供しています。

## **Okta Identity Cloud:**

適切な人に適切なテクノロジーを適切なタイミングで提供する、中立かつ独立したプラットフォームです。

## **Workforce Identity:**

場所を問わず、いかなるデバイスでも従業員、請負業者、パートナーのアクセスを常に保護します。

## **Customer Identity:**

顧客のシームレスで安全なログインを実現します。

