バイヤーズガイド:

パスワードレスの

顧客認証サービスの選び方

顧客に応じて適切なパスワードレスソリューションを特定、評価、選択するためのガイドです。

1

2

パスワードレスの定義

ビジネスにおいてパスワードレス顧客認証サービスが必要な理由

- パスワードに関連するあらゆる形態のリスクや詐欺を排除します
- 顧客が本当にその人であることがより確実となります
- あらゆるアプリ、チャネル、デバイス、ブラウザからアカウントに迅速かつ簡単にアクセスできる方法を顧
  客に提供することで、顧客離れを最小限に抑え、ロイヤリティを構築します
- サポートコール、パスワードのリセット、過度に複雑なIDスタックに関連する運用コストを削減します

パスワードレスエクスペリエンスによる顧客側のメリット

- 脆弱なパスワードや再利用可能なのパスワードを排除し、すべてのアカウントで堅牢なセキュリティを維持します
- すべてのチャネル、デバイス、アプリで、常にストレスのないパスワードレス体験をもたらします
- すべてのアプリとチャネルで、使い慣れた信頼できる方法によってログインを簡素化します
- パスワードを忘れても、面倒な手続きなく簡単にアカウントを復元できます

パスワードレス顧客認証サービスのコア要件

1. パスワードレス＝どこへ行ってもパスワードは不要
2. すべてのデバイスをひとつのIDに統合
3. あらゆるデバイス、アプリ、ドメインでクロスチャネルを実現
4. ワンステップの多要素認証で顧客を即座に認証
5. アプリレスでも、アプリとしてもフレキシブルに使える
6. 既存のIDシステムとの統合が容易

素早く導入

数カ月～数年ではなく、数週間～数カ月で

1.

パスワードレス＝どこへ行ってもパスワードは不要

カスタマーエクスペリエンスの向上とリスク低減のため、顧客認証サービスは**100%**パスワードレスであるべきです。つまり、登録やアカウント復元のプロセスを含む、認証の全行程からパスワードを無くすということです。多くの顧客認証サービスはパスワードレスな体験を提供していますが、それでも基になるアーキテクチャにはパスワードが保存されています。パスワードがどこかに存在するのであれば、パスワードに関するリスクや不満は残り、パスワードベースの攻撃ベクトルが依然として悪用される可能性があります。

り、アカウントの乗っ取りや詐欺のリスクを招きます。サイバー攻撃が巧妙化する中、パスワードは最も悪用されやすいターゲットです。たった一度の顧客情報の漏えいで、信頼が損なわれ、ブランドの評判が台無しになる可能性があります。パスワードとすべての共有情報を排除することで、ビジネスにおけるすべてのリスクとコストを軽減することができます。

1. パスワードを保存しますか？
2. 顧客がアカウントを作成する際に、パスワードを作成する必要がありますか？
3. 顧客に対する代替認証方法は何ですか？
4. 顧客のアカウント復元プロセスはどのようなものですか？

2.
すべてのデバイスをひとつのIDに統合

一度の登録で、所有する他のデバイスでも認証情報を共有できるようにするべきです。このプロセスでは、顧客がどのデバイスを使用していても、顧客に単一のIDを作成します。現在利用可能なパスワードレスサービスのほとんどは、顧客に各デバイスを新しい別のアカウントで個別に登録させ、多くの場合パスワードベースの認証情報を使用させています。つまり、顧客は各アプリごとにアカウントを作成するため、実際に必要な（あるいは作りたい）数よりも多くのIDを作ることになります。

不可欠である理由

ニーズに対応することが不可欠です。カスタマーエクスペリエンスが断片化され、顧客をイライラさせることはよくあります。一人の顧客が同じ企業が提供するサービスに対してモバイルアプリ用、店舗用、サポート用と、いくつものIDを持つ場合もあります。デバイスではなく、ID に基づく認証であれば、再登録を含むすべての複雑性が排除されます。適切なパスワードレスソリューションがあれば、すべてのチャネルでスムーズな行程を実現できます。

確認すべき主な質問

1. のサービスを使用す

2. 顧客は新しいデバイスを購入するたびに新しいデバイスでアカウントを再登録する必要がありますか？

3. 様々なデバイス、アプリ、ドメイン間でパスワードレスエクスペリエンスを実現する方法は？

4. 認証シナリオはデバイスのみに依存していますか？

---

1 https://www.telecompetitor.com/report-connected-devices-have-more-than-doubled-since-2019/

3.

あらゆるデバイス、アプリ、ドメインでクロスチャネルを実現

顧客はアプリ、チャネル、デバイス間をシームレスに、ほぼストレスなく移動できる必要があります。Web、モバイルアプリ、匿名ブラウザ、コールセンターや実店舗チャネルを問わず、一貫したクロスチャネルエクスペリエンスの実現のためには、顧客は毎回同じIDで迅速に認証されなければなりません。この要件を満たすことはこれまで困難であるとされてきました。これは、デジタルと非デジタルの対話は異なる認証方法を必要とし、異なるテクノロジースタックに支えられているためです。パスワードレス方式は、どのチャネルからも普遍的に利用され、セキュリティとユーザーエクスペリエンスの一貫性を促進する必要があります。

不可欠である理由

利用可能なデバイスやブラウザを使用してログインできない、単にログインできなければ、顧客は逃げてしまいます。パスワードのリセットが恐ろしく面倒だと思うと、顧客は二度と戻ってこなくなり、結果的に顧客離れが進みます。クロスチャネル認証サービスを利用することで、顧客は使いやすさの向上とあわせて高いセキュリティレベルの恩恵を受けることができます。

同じことが、オフラインエクスペリエンスにも当てはまります。コールセンターに電話するなどオフラインでの認証を、オンラインエクスペリエンスと一体化させることは、スムーズで親しみやすい顧客体験のために不可欠です。

確認すべき主な質問

1. デジタルとオフラインのすべてのチャネルで、統一されたパスワードレスエクスペリエンスを提供していますか？
2. ユーザーは、新しいデバイスやチャネルで再登録する必要がありますか？
3. 顧客はブラウザやデバイスを切り替えたときに、再認証が必要ですか？
4. 匿名モードやCookieの削除など、ドメインの状態が変化しても、パスワードレスエクスペリエンスを提供できますか？

4.

ワンステップの多要素認証で顧客を即座に認証

来の方法をパスワードレスサービスに置き換えることで、企業は複雑でコストがかかり、ストレスの多い方法（煩わしいステップアップ過程で実行されるSMS OTPに支えられたパスワードなど）から顧客認証の過程全体を解放することができます。パスワードレスな顧客認証では、従来の方法とは異なり、ワンクリックで**MFA**を有効にできます。デバイスは顧客が「持っているもの」、生体情報は「あなたが誰であるか」を表します。

不可欠である理由

従来の二要素認証（2FA）方式は、ユーザーが

証情報にまで縮小されます。これらの共有認証情報は、パスワードと同様に簡単に盗まれ、危険にさらされます。OTPやナレッジベース認証（KBA）もまた、障害点となります。OTPが届かなかったり、自分の設定した質問に正しく答えられなかったりすると、顧客はログインできず、企業はビジネスチャンスを失うことになります。

パスワードレスサービスを導入することで、より強力なセキュリティと、SMS OTP、KBA といった煩わしくストレスの多いハードルのない、シームレスなカスタマーエクスペリエンスを提供することができます。

確認すべき主な質問

1. 貴社のパスワードレスソリューションは、ワンクリック「ピュアパスワードレス」特性を備えていますか？
2. 顧客が複数の要素でIDを設定し、確認するために必要なステップはいくつですか？
3. MFA方式が傍受される可能性はありますか？
4. MFAのステップはどれほどのストレスをともないますか？

5.

アプリレスでも、アプリとしてもフレキシブルに使える

般に好まれるサービスとは、組織がアプリを使用するかしないかを柔軟に決定できるものです。アプリを使用する場合は、サービスを組織の既存のモバイルアプリと簡単に統合できる必要があります。アプリを使用しない場合は、WebAuthNやFIDOなどのプロトコルがテクノロジースタックの重要な構成要素になります。ユーザーのOSにすでにインストールされている一般的なブラウザを使ってパスワードレス認証を行えるようになったためです。

不可欠である理由

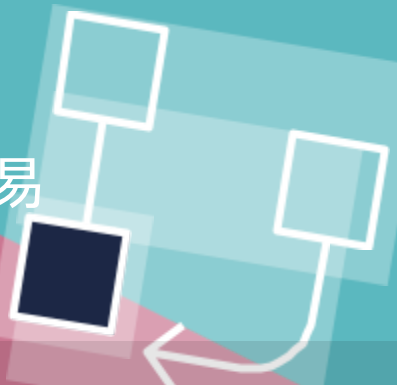
アプリとしてもアプリレスとしても使用できる柔軟性は、パス
あることを保証するために不可欠です。組織は、顧客が求
めるエクスペリエンスと必要なセキュリティレベルを提供す
るための選択肢を持つべきです。顧客に別のアプリをダウ
ンロードさせたくない、あるいはパスワードレスサービスを
既存の顧客向けアプリに統合させたいといった要望があるかもしれません。

確認すべき主な質問：

1. 貴社の顧客認証サービスは、モバイル導入戦略
   か？
2. 貴社の顧客認証サービスは、アプリレスまたはアプリとしても使用できる柔軟性を備えていますか？
3. 既存のアプリとの統合は容易ですか？
4. 貴社の認証サービスでは、顧客のデバイスにソフトウェアをダウンロードする必要がありますか？

6.

既存のIDシステムとの統合が容易



織には通常、現行のCIAMシステムを導入済みであるため、顧客向けのパスワードレスログインエクスペリエンスを追加するには、それが既存のテクノロジーと連携できなければなりません。既存の認証システムを維持し、導入リスクを低減し、サービスの継続性を確保するには、柔軟性、俊敏性、およびパスワードレスサービスを容易に統合する能力が極めて重要です。パスワードレスによる増強は、複雑であったり、コストがかかったり、過度な労力を必要とするものであってはなりません。

不可欠である理由

ンスの戦略にすぐに適応できるソリューションを必要としています。どのようなビジネスにとっても、IDシステムを統合して管理を簡素化し、IDスタック全体を見渡せるようにすることも重要です。

確認すべき主な質問

1. プロバイダーと統合

2. 統合はどれほど柔軟に行えますか？

3. 自社のブランディングに合わせてサービスをカスタマイズできますか？

4. 既存業務へのリスクを抑えてサービスを組み込むにはどうすればよいですか？

7.

素早く導入
数カ月～数年ではなく、数週間～数カ月で

一般的な顧客のID管理改革プログラムでは、多くの開発者を必要とし、導入に何年もかかることがあります。これは、各種多様なアプリケーション技術、多様なセキュリティニーズ、レガシーシステムと自社製システムの混在が原因です。パスワードレスを活用することですべてをゼロから構築せずにすみ、統合の一貫性、顧客のID処理、統合の手段を確保できます。パスワードレスは書き換えではなく、拡張であるため、サービスは数年単位ではなく、数週間から数カ月単位で迅速に展開できなければなりません。

ここで重要なのは時間です。サービスの導入が早ければ早いほど、早くそのメリットを享受し、競争上の優位性を実現し、KPIを達成することができます。その逆もまたしかりです。導入が困難なパスワードレスソリューションは、リソースを浪費し、予算、時間、開発者をより多く費やすことになります。

確認すべきこと

1. くらいの時間がかかりますか？
2. サービスの導入に必要なリソースはどれくらいですか？
3. サービス導入後の保守や管理はどの程度必要ですか？
4. オープンスタンダードを活用することで、統合を簡素化、迅速化できますか？

顧客認証の未来

BindIDは、顧客がどこからでもすべてのチャネルにパスワードレスで簡単にアクセスできるようにする唯一のパスワードレス認証サービスです。

業界初となるBindIDは、単一の顧客IDを作成し、そのIDをチャネルやデバイス間でバインドすることで、アカウント乗っ取り詐欺のリスクなしに、顧客がワンクリックでパスワードレスアクセスできるようにします。

BindIDは、ユーザーのプライバシーを保護しながら、すべてのチャネル間を自由に行き来できる完全なパスワードレスエクスペリエンスを提供します。アプリを使わない初の顧客認証サービスとして、BindIDはWebやアプリレベルでの複雑な変更を必要としない、スムーズなID エクスペリエンスを実現します。

BindIDの最も魅力的な点の1つは、わずか数日で既存のすべてのチャネルに統合できることです。オープンスタンダードによる超高速の実装により、数週間以内に、わずか1人の開発者で提供を開始することができます。

オープンスタンダードとデバイス生体認証の組み合わせにより、パスワードはフロントエンドでもバックエンドエクスペリエンスでも、登録やデバイス復元プロセスでも、どこにも作成、使用、保存されることはありません。これにより、簡単、安全、かつポータブルな顧客認証が可能になります。これこそが本来のパスワードレスです。

transmit security

未来の認証を導入する準備はできていますか？

BindIDの詳細については、今すぐこちらをご覧ください。