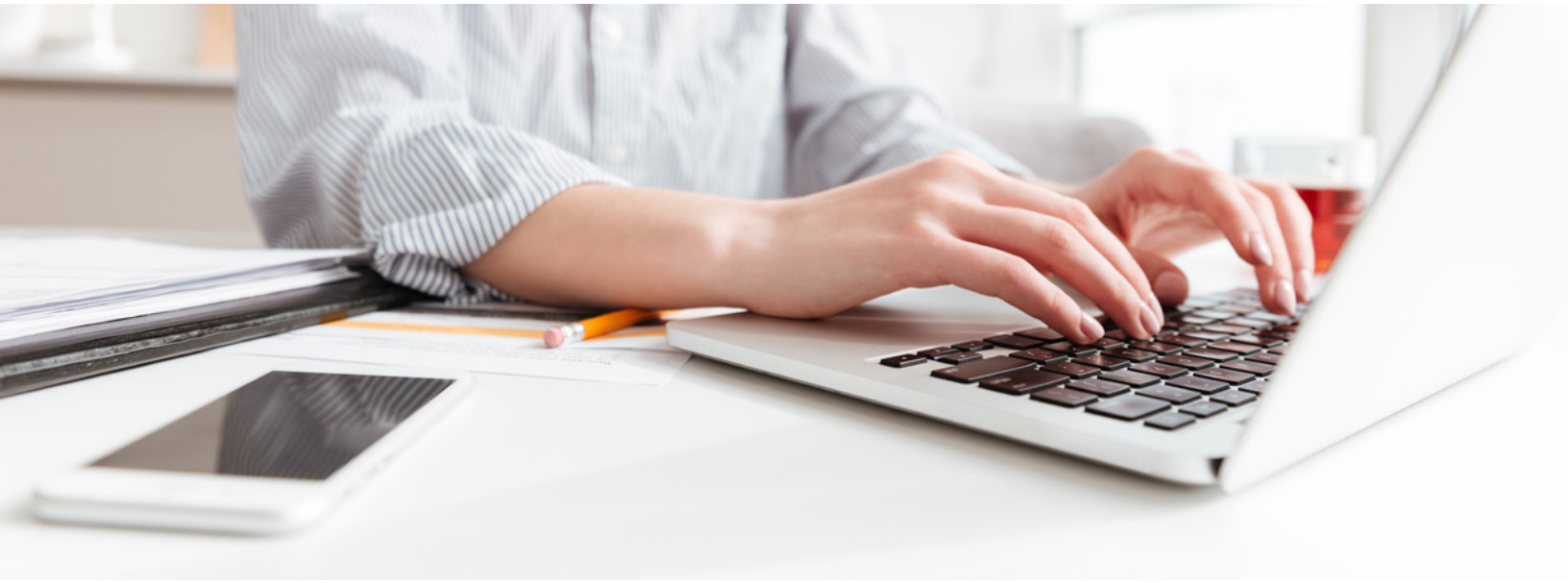
パスワードレス / タッチレス
ソリューション選定ガイド

貴社の組織と従業員を守りましょう

ENTRUST



パスワードが未だに存在する理由

セキュリティの専門家は、長年に渡ってパスワードを無くす必要性について語ってきました。事実、2004年に開かれたRSAセキュリティ会議で、ビル・ゲイツ氏は次のように述べています。「時間の経過とともに、人々がパスワードにますます依存するようになることは間違いありません。人々は異なるシステムで同じパスワードを使い回し、それらを書き留めておくだけで、安全に必要となる本当の挑戦には応えられていません。」

その後、16年もの歳月が経った現在、テクノロジーは進歩を遂げており、我々は今は…パスワードを使用しています！

2019年のVerizonの調査によると、パスワード問題は、あらゆるデータ侵害の80%以上の根本原因であるため、ますます大きくなってきています。それらに対処するには、平均400万ドルから800万ドルのコストがかかると言われています。 従業員がパスワードをリセットするためにヘルプデスクに電話するたびに、企業は平均70ドルを費やしています。

2020年に発生したコロナウイルスのパンデミックは、パスワードの問題をさらに悪化させています。 企業は、疾病の蔓延を和らげるために新たな規則を用意・運用し始めています。 これには、従業員が表面を触れる必要がある、あらゆる作業の徹底的な調査が含まれています。キーボードやタッチスクリーンでパスワードを入力することは、このリスクの中心的な位置付けにあります。これに伴い、企業は単に「パスワードレス」から「パスワードレスでタッチレス」のソリューションに求めるようになりました。 多くの組織では、パスワード以外にも、スマートカードやその他の物理的な認証システムを置き換える「タッチレス」を模索しています。

80% ハッキング関連の犯行の80%は、認証情報の漏えいが原因です。

65% 65%もの人々が、複数のアカウントで同じパスワードを使い回しています。

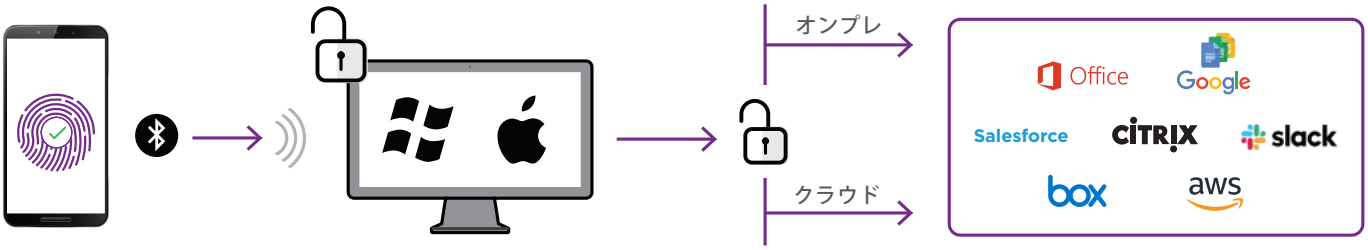
2.7B 27億ものパスワードが、1度の侵害で漏えいしました。

企業は適切なソリューションを模索する中で、乱用される製品用語に遭遇することがあります。 多くの生体認証ソリューションは、ユーザーに「パスワードレスな体験」を提供すると主張しています。 これは、従業員が物理的にパスワードを入力する代わりに生体認証をスキャンするという意味では正しいですが、これらのソリューションは、中央リポジトリに存在するパスワードをアクティブ化するための新しいフロントエンドを提供しているにすぎません。 そして、これらの一元化された認証情報リポジトリは、もちろんハッカーにとってお気に入りのターゲットです。 1度でも侵入が成功すれば、サイバー犯罪者は何千もの認証情報を入手でき、それらを様々な攻撃に利用できます。 多くの生体認証技術も、実は「タッチレス」問題に対処できていません。

では、どうすればいいのでしょうか？パスワードから離れることを検討している場合 ー データと多くのホラーストーリーがそうすべきと訴えていますが ー 一元管理されている認証情報がもつ脆弱性からの解放されることを可能にするソリューションが必要です。 真にセキュアなアプローチとは、新しい分散モデルを展開することです。 このモデルでは、従業員の認証情報がモバイルデバイス内に安全に保存されています。 ユーザーエクスペリエンスの観点から、そして業務効率性の観点から、真のシングルサインオン（SSO）機能を提供するソリューションを選択することが重要です。

真のパスワードレス / タッチレスソリューションの仕組み

市場には「パスワードレス」という銘打ったソリューションが多く存在しますが、それらは従業員を想定したパスワードレスの「エクスペリエンス」のみを提供するものであり、これは真の意味でのパスワードレス セキュリティではありません。 これらのソリューションの多くは、ユーザーが指紋、虹彩、または音声認識を使用して、ワークステーション、アプリ、またはネットワークにアクセスできるようにしています。 このような体験型のソリューションでは、一見パスワードは排除されているように見えますが、「タッチレス」の問題には対処していません。 ほとんどの場合、ユーザーのパスワードは依然として中央リポジトリに存在します。 生体認証をスキャンした後も認証にパスワードは必要であり、ハッカーに対し脆弱性を露呈しています。 つまり、セキュリティの向上ではなく、ユーザーエクスペリエンスがわずかに向上しているだけです。 これらのソリューションは、パスワードレスが可能にするセキュリティの半分しか提供しておらず、ほとんどの場合、問題に意味ある方法で対処することができていません。



分散型認証情報ストレージ

安全なパスワードの代替手段 ー そして、利用がスムーズで、真のSSO機能とタッチレスエクスペリエンスを提供するもの ー は、信頼できるデジタルIDに基づいています。 これらのIDは、ユーザーのモバイルデバイスに安全に保管できるデジタル証明書を発行することで実現されます。 IT部門は、証明書を社内で管理するか、マネージドサービスで管理するかを選択できます。これらの暗号化されたデジタル証明書は、従業員のデバイスに存在する仮想パスポートまたはIDカードと考えてください。これらはユーザーのデバイスに保存されるため、安全性の高い分散型資格情報インフラを構築できます。従業員の認証情報のための中央リポジトリはありません。

公開鍵基盤（PKI）テクノロジー

証明書の発行とライフサイクル管理には、公開キー基盤（PKI）テクノロジーが必要となります。 ユーザーがワークステーション、アプリ、またはネットワークにアクセスしたい場合、デジタルIDには、暗号化された鍵のペアを用いてアクセスできるようになります。 デジタルIDは、これら鍵の安全な交換を通じて確認されます。ハッキングまたは盗むためのパスワードはなく、画面やキーボードに触れる必要もありません。

SSO認証

この暗号化された鍵の交換が行われると、従業員やその他の承認されたユーザーは、セルフサービスのオンボーディングツールを使用して登録作業を行います。その後、インターネットに接続している場所ならどこからでも、クラウドベースのアプリやオンプレミスのアプリなどを、安全にアクセスできるようになります。 適切に設計されたソリューションは、一度のユーザー登録でユーザーとデバイスを認証し、デバイスごとあるいはアプリごとに認証情報を再登録する時間のかかるプロセスを排除できます。 これにより、安全でスムーズなシングルサインオンソリューションを提供します。

パスワードレス/タッチレスソリューションの操作の流れ

1. ユーザーはモバイルデバイスにデジタル証明書（仮想IDカード）をインストールします。
2. 承認されたユーザーは、自動オンボーディングツールを利用して自己登録します ー これは、インターネット接続できる場所ならどこからでも可能です。
3. デバイスロックを外し、指紋や顔認識などの生体認証を通じて、信頼できるIDにアクセスします。
4. ユーザーが認証されると、Bluetooth接続を介し、コンピュータに近接している間は、パスワードレスのログイン、ならびにすべてのクラウドアプリ・オンプレミスアプリに対し、シングルサインオン（SSO）ができるようになります。
5. ユーザーがモバイルデバイスを持ってコンピュータから離れると、コンピュータとアプリから自動的にログアウトされます。 自動ログアウトをトリガーする条件は設定可能であり、組織のポリシーによって異なります。

パスワードレス /タッチレスのメリット

先進ユーザーに見る導入効果

脅威が低減する：パスワードが不要になると、資格情報の詰め込み、フィッシング、中間者攻撃などの、パスワード ハッキングからの脅威を取り除くことができます。

徹底したセキュリティ管理：脆弱なパスワードの使用や、危険なパスワードの管理方法に悩まされることが無くなります。 証明書と暗号化キーは企業の管理化にあります。

拡張は自由自在：分散された認証情報の保存・管理により、新規ユーザーの追加は、自由自在にできるようになります。 必要となるのはスマートフォンなどのモバイルデバイスのみであり、ユーザーは数分でセルフ オンボードできます。

TCOの削減：パスワードには継続的な監視とメンテナンスが必要ですが、パスワードがないということは、リセットに時間を費やしたりしたり、複雑なパスワードポリシーを導入する必要がないことを意味します。

よりハッピーなユーザー：ユーザーは、セキュリテイのために複雑なパスワードを覚えたり、更新したりする必要がなくなります。

接触リスクを低減：パスワードと物理的な認証システムの使用を排除し、共有デバイスへの依存を減らしてBYODを優先することで、職場での物理的表面への接触機会を最小限に抑えることができます。

貴社に適したソリューションを選定する方法

今日、従来のパスワードの必要性を完全に排除し、物理的表面への接触機会を減らし、高保証のセキュリティを提供するソリューションは複存在数存在しています。

では、貴社にとって最善の結果につながるような検討をどのように開始すべきでしょうか？ まずは、切り替えに伴う不必要な中断を予測して排除する方法を検討してください。 大規模な、または広く分散している従業員をオンボーディングするタスクは、パスワードレスでSSO機能を導入しようとする多くの企業にとって深刻な障害になる可能性があります。 安全かつ確実に従業員がどこからでも自己登録できる自動ツールを提供するソリューションを探してください。 面倒なオンボーディングプロセスでIT部門または人事部門に負担をかけることはお勧めできません—それは完全に回避できるものです。

次に重要な検討事項としてスケーラビリティがあります。 有機的または買収を通じて成長することを期待している場合 ー および新しいクラウドアプリを追加し続け、外部のエコシステムとの幅広い接続を継続することを計画している場合 ー 簡単に拡張できるパスワードレス認証ソリューションが必要です

そして、最後の重要な検討事項は、暗号化ニーズです。 従業員が機密性の高い情報にアクセスまたは共有したり、高価値のトランザクションを実行したりする場合は、エンタープライズクラスの暗号化機能を提供するシステムが必要になります。 最高のパスワードレス認証プラットフォームは、トランザクションのセキュリティと継続的なセッション監視のための明確なロードマップを提供します。

パスワードレス / タッチレスソリューションを評価する際に考慮すべき5つの追加要素を次に示します：

1. デバイスのロックインを回避する

これはリストの最上位にあるべきです。 従業員のモバイル化とリモート化が進む中、従業員がどこにいても必要なアプリケーションやシステムに確実にログインできるようにするには、デバイスの柔軟性が不可欠です。 デバイスの持ち込み（BYOD）の台頭、特にパンデミック後の世界では、企業が労働者が使用するデバイスを制御できなくなっています。 選択するパスワードレスのソリューションがテクノロジーにとらわれないことを確認してください。Mac、PC、クラウドアプリ、オンプレミスソフトウェアと完全な互換性が必要です。 これにより、採用時の従業員の混乱を最小限に抑えるだけでなく、将来的にハードウェアまたはソフトウェアを導入する際の柔軟性を企業に提供します。

2. SSOと真のモビリティを実現

特にリモートワークの時代には、モバイルを新しいデスクトップとして採用し、幅広い認証オプションを提供するソリューションを探すことが重要です。 従業員が使用するデバイス数が増え続けるにつれ、SSO機能はログインプロセスを大幅に合理化し、オムニチャネルワークフローを簡素化します。 これは従業員にとってはスムーズな操作を意味し、企業にとっては最適な生産性を意味します。 さらに、近接性に基づきコンピュータとアプリケーションをロックおよびロック解除するためにNFCまたはBluetoothを使用することで、特にホームオフィス環境では、いつでもどこからでもシステムにアクセスしても予期しないセキュリティの問題が発生しなくなります。 従業員がコンピュータから離れるとき、デバイスがこの動きを検知でき、ユーザーが戻るまでログアウトし続ける必要があります。

3. 証明書ベースのIDを選択する

スマートフォンを仮想スマートカードに転換し、認証、暗号化、およびエンタープライズモビリティ管理（EMM）を行うことのできるソリューションを探してください。 PKIを使用してスマートフォン、タブレット、その他のユーザーデバイスにデジタル証明書が配置されると、認証情報の詰め込みや再利用された認証情報の悪用など、主要なハッカー攻撃を緩和することができます。 認証情報の保存箇所を分散化すれば、これらの不正な行為を実行することができなくなります。

4. デジタルロードマップに対応する

直近の用途には、ファイルの暗号化、デジタルドキュメントの署名、ホットデスクが含まれることでしょう。従業員のモビリティが拡大するにつれて、パスワードレスのソリューションが必要不可欠になります。ニーズの変化に応じて拡張できるソリューションを選択することが重要です。スケーラブルなソリューションがなければ、最終的にはメール用の認証ソリューション、システムログイン用の認証ソリューション、ドキュメントの署名用の認証ソリューションなど、多数が乱立する可能性にがあります。これは不要な複雑さを作り出し、ユーザーを苛立たせ、企業ワークフローに大きなの負担を追加します。

5. 実績豊富なベンダーを採用する

クラス最高のソリューションは、政府当局による使用が承認されており、FIDO2に準拠しているベンダーによって提供されます。 FIDOプロトコルは、PKIのパワーと高度なデータ暗号化技術に依存して、ワーカーの認証を簡素化し、企業のセキュリティを向上させます。 最も熟練したベンダーは、これらのサービスを国の政府やグローバル銀行に提供してきた実績があります。

選定に役立つリソース

パスワードレス認証技術の評価に役立つ情報やインサイトを探している場合 ー もしくは当社のプラットフォームのデモを見たい場合 ー は、www.entrust.com/passwordlessをご覧ください。

ENTRUST について

Entrust は信頼できる認証、支払い、データ保護を実現することで、動き続ける世界をセキュアにしています。今日、支払いや国際取引、電子政府サービスへのアクセス、そして企業ネットワークへの認証において世界中でより安全で円滑なユーザ体験が求められています。Entrust はこれらの要となる部分において、他に類を見ない幅広いデジタル セキュリティとID発行ソリューションを提供しています。2,500人を超える従業員、グローバルパートナーネットワーク、そして150カ国以上におよぶ顧客に支えられ、世界で最も信頼されている組織から信頼されています。

エントラストジャパン株式会社
Tel：03-6738-6710(代表)
Fax：03-6738-6711
https://japan.entrust.com