jamf

パスワードレスでセキュリティを確保する方法

煩わしく厄介なパスワード

パスワードは、アクセスすべきでない人を排除し、アクセスすべき人を受け入れるためのバリアとして、長いあいだ使われてきました。デバイスとデータの扉を守る用心棒のようなものです。デバイスの入り口に堂々と立ちはだかり、最低文字数と数字や特殊文字が持つすべての力を発揮して、デバイスを守ってきました。

デジタルフットプリントが広がり、デバイスのエコシステムが拡大する中、忙しい日々を送るユーザのニーズも増えており、パスワードの価値や使い勝手は徐々に損なわれつつあります。個々のユーザが1日にデバイスやアプリに接触する時間はかつてないほど増えており、パスワードが漏洩した場合にセキュリティ侵害が起こる可能性もそれに比例して増加しています。

パスワードというものが、デバイスやデータに触れるほぼすべての場面においてエンドユーザのアイデンティティを証明するために使われるものであることを考えれば、IT管理者が「もっともよく使われるパスワード」のリストを非常に恐ろしいものであると考えるのも無理はありません。

もっともよく使われるパスワード（トップ10）[1]

1. 123456	6. qwerty123
2. 123456789	7. 1q2w3e
3. qwerty	8. 12345678
4. password	9. 111111
5. 12345	10.1234567890

1. 出典：Cybernews.com

このホワイトペーパーのトピック:

- セキュリティ向上と使い勝手の良さのバランス
- 「パスワードレス」とは何を意味するのか
- パスワードレスのワークフローが組織にとって重要な理由
- パスワード関連の悩みを解決するソリューション

セキュリティー向上と使い勝手の良さのバランス

今日、組織が抱えるもっとも大きなセキュリティ上の問題は何だと思いますか？**ログイン情報の盗難**です。これを聞いて驚く人はあまりいないかもしれませんが、**データ流出の80%がパスワード盗難や弱いパスワードが原因で発生している**という事実についてはどう思いますか？より強力なパスワードポリシーが施行されていても、サーバへの侵入によりパスワードが流出し、その結果として企業や従業員の情報が漏洩する可能性は十分にあります。さらに、情報セキュリティの敵の手法や攻撃のタイプは、より巧妙になってきています。フィッシング攻撃、プッシュ通知、アカウントの乗っ取りなどは、どれも騙しやすそうなユーザを直接狙い、デバイスや重要なデータに直接アクセスしようとするものばかりです。

セキュリティ強化の必要性から、IT部門は解決策としてパスワードの複雑化や定期的な変更をユーザに求めるようになりました。これらの対策は実際に効果があり、「ベストプラクティス」と呼ぶに値するものですが、同時にユーザエクスペリエンスの面で問題があったことも確かです。負担を軽くするために、多くのユーザは弱いパスワードを作成したり、紙やデバイスにパスワードをメモしたり、時にはキーボードの下に隠しておいたりすることもあります。一方、複雑なパスワードを作成・使用した人は別の問題に悩まされることになりました。文字や数字からなるランダムなパスワードを忘れてしまう人が増え、ヘルプデスクに問い合わせが殺到しました。

パスワードのリセットは手間のかかる作業ではありませんが、もっとやりがいのある仕事を求めて雇われたIT管理者にとって、これほど退屈な作業はありません。さらに言えば、IT管理者の貴重な時間をつまらない問い合わせの対応に費やし続ければ、組織に経済的損害を与えかねません。**1回のパスワードリセットにかかるコストは平均70ドルと言われています。**そして、このような対応に費やされる時間とコストの合計は組織によっては衝撃的なものとなります。エンドユーザにとっても、パスワードを忘れてリセットを待つことは、業務を遅らせ生産性を低下させることになります。しかし、これほどの時間的・金銭的コストを前にしても、パスワードの重要性はセキュリティチームやユーザから十分な注目を受けていません。

組織を攻撃から守り重要なデータを保護するためのセキュリティニーズが高まったことで、企業のセキュリティ予算も増加傾向にあります。それにもかかわらず、パスワードの流出は増加の一途をたどっており、それを防ぐための予算が問題の大きさと比例していないのが現状です。実際、**セキュリティ侵害の実に80%以上が認証情報の漏洩に起因しているのにも関わらず、この問題に割り当てられる予算は10%以下**となっています。こんな状況下で活躍するのが、パスワードレスのワークフローです。

「パスワードレス」とは何を意味するのか

ガートナー社は、2022年までに大型企業とグローバル企業の60%および中堅企業の90%が、50%以上の使用事例にパスワードレス方式を導入すると予測しています。

これはなぜなのでしょうか？パスワードを使わずにユーザを認証するワークフローは、その性質上、脆弱なパスワードがもたらす問題を排除し、ユーザのパスワード疲れを緩和してくれます。さらに、漏洩または流出する可能性のあるパスワードを組織側が管理する必要がないことを意味しています。つまり、冒頭で述べた物理的なパスワードの問題点をほぼすべて軽減してくれるのです。

パスワードレスのワークフローを確実に導入するためには、IT部門からアクセスや使用を許可されたリソースやデータ、ソフトウェアへのサインイン過程において、ユーザが認証を行う、または身元を証明する方法を提供する必要があります。IAM（アイデンティティおよびアクセス管理）やセキュリティのリーダーは、アイデンティティ管理の核とも言える、認証と認可の概念に精通している必要があります。

認証方法の一例として、スマートカードシステムが挙げられます。スマートカードはクレジットカードに似た物理的なカードです。ユーザに紐づけられた暗号化キーが搭載されており、安全な認証方法として使用されています。しかし、こういったシステムは導入に時間がかかり、非常に高価で、エンドユーザが物理的に管理しなければならないものが増えるという問題があります。高いリスクを抱えた組織でない限り、スマートカードの紛失または破損の可能性やそれにまつわるコストを考えると、このレベルのセキュリティは潜在的な脅威への対策としては過剰であると言えます。

パスワードレスのもっとも身近な例として挙げられるのは、生体認証技術の利用かもしれません。Face IDやTouch IDはAppleユーザなら誰でも知っている例でしょう。生体認証を利用すれば、パスワードを入力したり、盗まれたり推測されたりする可能性のある秘密の質問などを必要とせずに、ユーザを認証することができます。他人の顔や親指を盗むのは、ほぼ不可能だからです。これに定期的に変更される暗証番号を加えれば、セキュリティの効果は倍増します。

パスワードはもはや、ユーザにデバイスやリソースへのアクセスを許可するもっとも安全な方法ではなく、また、1日に何度も入力し直さなければならないという意味でもユーザエクスペリエンスの点で劣るのは確かです。また、リモートワークやハイブリッドワークなどの導入で働く環境が変化する今、組織はエンドユーザエクスペリエンスを考慮に入れたより優れたセキュリティ対策を検討しなければなりません。ここからは、パスワードレスのワークフローを導入する必要性がDXによってどのように高まっているのかを見てみましょう。

多要素認証（MFA）とは？

多要素認証（MFA）は、リソースにアクセスするために、2つ以上の認証要素を提供することをユーザに要求する認証プロセスです。これにはいくつかのオプションがあり、ユーザの端末の暗証番号やFace ID、指紋認証などが含まれます。

パスワードレス認証とは？

パスワードレス認証は、ユーザがパスワードを入力したり秘密の質問に答えたりすることなくコンピュータにログインできる認証方式です。

証明書ベース認証とは？

証明書ベース認証は、リソースやネットワーク、アプリケーションなどへのアクセスを許可する前に、デジタル証明書を使用してユーザやマシン、デバイスを識別する方法です。

パスワードレスのワークフローが組織にとって重要な理由

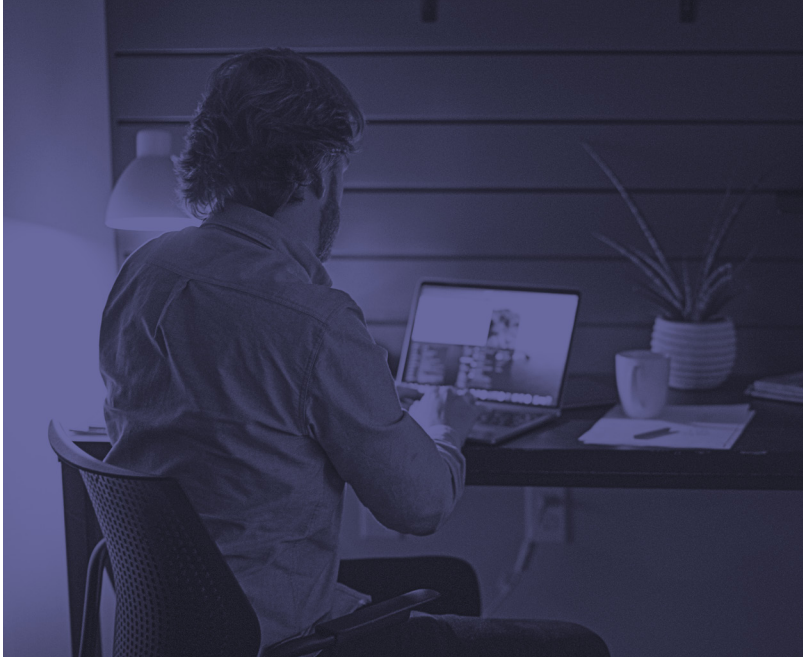
冒頭で触れたパスワードにまつわるセキュリティの脆弱性だけでは、パスワードレスのワークフローを目指すきっかけとしては十分でないと考える人もいるかもしれません。ここからは、DXとそれがパスワードにもたらす影響についてもう少し掘り下げて考えてみましょう。

リモートワーカー

リモートワークやハイブリッドワークへの移行により、優れたユーザエクスペリエンスとリモートセキュリティを提供することが特に重要視され、パスワードレス認証の必要性は加速の一途を辿っています。その大きな要因は、エンドユーザがリモートでログインするということです。ユーザは、自宅やオフィス、カフェ、公園など、どこにいても自分のデバイスやリソースにアクセスできます。これは柔軟性が高く便利ですが、組織の手が届かない場所にいることに伴うリスクが発生します。ユーザが安全でないネットワークを利用すれば、セキュリティに穴が開き、攻撃の可能性が高くなります。このようなリスクを軽減する簡単な方法のひとつが、ユーザが必要とするすべてのものにアクセスするための、シンプルで信頼性の高いパスワードレスのワークフローです。これにより、流出のリスクを伴うパスワードを入力する必要がなくなり、ヘルプデスクへの問い合わせも減ります。また、セキュリティを確保しつつ、パスワード疲れまで解消してくれるというメリットもあります。

クラウドに移行した業務

クラウドコンピューティングが世界を変えた今、その活用が現代のITインフラ全般において重要な要素であることは間違いありません。オンプレミスの壁が崩壊し、組織がクラウドに移行しつつある中、アイデンティティ管理の戦略もそれに追随する必要があります。クラウド上にはさまざまなアプリやリソースが散らばっています。それらへのアクセスを従業員に与え、生産性を維持するための安全な方法を見つけることはIT部門の課題ですが、パスワードレスのワークフローがあれば、クラウドやそこにあるすべてのアプリへの安全でシームレスなアクセスを提供する上で役に立ちます。



パスワード管理のコストダウン

世界経済フォーラムによると、世界中の従業員たちは毎年平均11時間をパスワードの入力や再設定に費やしているそうです。これに組織内の従業員数を掛け合わせれば、いかに莫大な時間がパスワード管理のために無駄にされているかがわかります。新しいソリューションの導入にはコストがかかりますが、面倒なパスワードの再設定にかかる時間や、従業員が業務に集中できない時間が生み出す無駄と比較すれば大したことはありません。

生産性の向上を促進

パスワードの管理に費やす時間を減らすことにより、従業員はより多くの時間を自分のタスクに費やすことができます。また、使用権限のあるリソースに自由にアクセスできるため、より生産的な1日を過ごせるようになります。パスワード管理の手間が省けたりパスワードのリスクに伴うセキュリティ関連の懸念が減ったりすることでコストが削減できるだけでなく、従業員の生産性の向上は収益の増加にもつながります。

パスワードのように、何年も見過ごされ、「こんなものだ」と受け入れられてきたものを微調整し、改善することで、組織全体のセキュリティ戦略や収益、財務の健全性を向上させることができるのです。多くの企業が、パスワードレスのワークフローをDX計画における重要な要素として捉えているのは、ある意味当然のことと言えるでしょう。

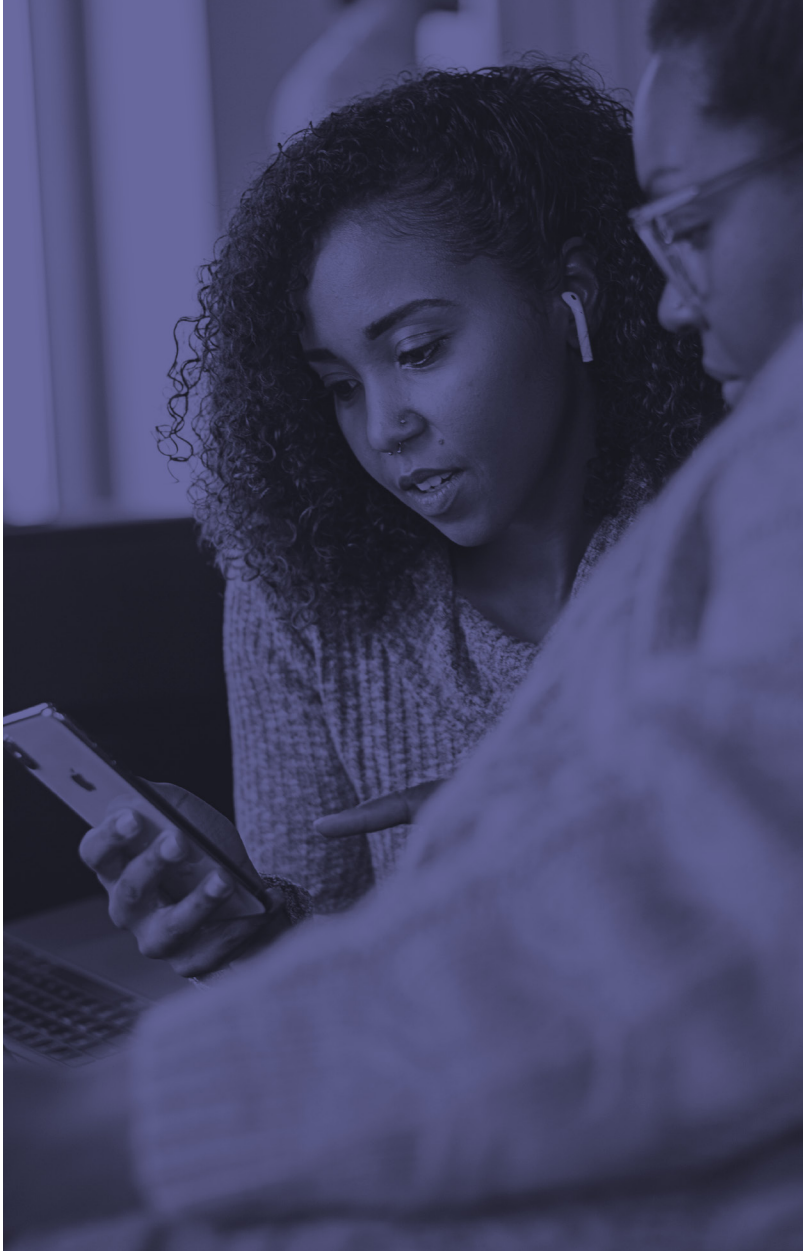
パスワード関連の悩みを解決するソリューション：Jamf Unlock

Jamf Connectに内蔵されたJamf Unlockがあれば、スマートカードなどの管理されない高価なハードウェアに頼る必要はありません。ユーザが常に持っているデバイス、つまりiPhoneでパスワードなしのワークフローを実現するJamf Unlockは、Macのロックを安全に解除し、より安全なログインと認証プロセスをシームレスなエンドユーザエクスペリエンスとともに提供します。Jamf Unlockのワークフローでは、ユーザがMac上でパスワードを入力する代わりに、iOSデバイスに搭載された認証ツールでMacの認証ニーズを満たします。

1. iPhoneでJamf UnlockのiOSアプリを開き、クラウドベースのアイデンティティ認証情報でサインインします
2. QRコードを使ってiPhoneとMacをペアリングします
3. Mac上でローカルパスワードを入力し、ペアリングを許可します
4. ペアリングが完了したら、次回からはアプリを使ってIT部門が指定した方法（生体認証のみ、または暗証番号と合わせて）で安全にMacをロック解除できます

Jamf Unlockは、Appleのマルチピア接続、CryptoTokenKit、およびCore Bluetoothフレームワークを活用し、ユーザのモバイルデバイスとMacの間で証明書ベースのワイヤレス認証を行います。

パスワードレスのワークフローが今後も進化を続けるのは間違いありませんが、あくまでも最新のアイデンティティおよびセキュリティ戦略のひとつの要素でしかありません。Jamf Connectの構成要素のひとつであるJamf Unlockは、ジャストインタイムのアカウントプロビジョニング、アイデンティティ管理機能、Macやリソースにアクセスするためのシングルクラウドを提供します。Jamf ConnectとクラウドIDプロバイダとの連携により、IT部門は各エンドユーザのアイデンティティに紐づくデータや、ユーザアカウントがアクセスを許可されたソフトウェアやリソースをリモートで管理することができます。これにより、セキュリティが向上するだけでなく、アカウントプロビジョニングが効率化され、ユーザは新しいMacを開封して電源を入れるだけで、必要なものに安全にアクセスできるようになります。



Jamf Private Accessで一段階上のセキュリティを目指しましょう。Jamf Unlockは、データやリソースを保護するソリューションの一部分に過ぎません。真のゼロトラストネットワークアクセスのプラットフォームであるJamf Private Accessなら、ユーザ認証を経てデバイスにアクセスした瞬間から安全な接続が保証されます。

Jamf Private Accessの詳細はこちらから

今日から始まるセキュリティ強化

仕事環境が常に進化していることは言うまでもありませんが、その進化には課題とチャンスが伴います。モバイルワークやリモートワークといった進歩は、悪質な行為を企む攻撃者やハッカーにチャンスを与えるものなのかもしれません。しかしそれと同時に、IT管理者や情報セキュリティ、エンドユーザにとって有益な、創造的なワークフローやソリューションをもたらす結果にもなっています。

情報セキュリティというのは常に「セキュリティ第一」の考え方を持っているものですが、毎日デバイスを使用する自らの体験にはるかに重点を置いているエンドユーザの要望やニーズとのバランスという課題を常に抱えています。エンドユーザは、手間のかかるワークフローやセキュリティ対策に多くの時間を奪われることを望んでおらず、データセキュリティの重要性に関する理解にも限界があります。

既存のワークフローと簡単に統合できるJamf Unlockなら、この点においてエンドユーザや情報セキュリティ、IT部門のすべてにメリットがあります。データを盗もうとする悪質な攻撃者がいなくなることはありませんが、Jamf UnlockとJamf Connectを使用したパスワードレスのワークフローを導入することで、優れたエンドユーザエクスペリエンスを保ちながらセキュリティの強化を図ることができます。

パスワードレス環境の導入は、ほとんどのセキュリティ戦略がそうであるように、プロセスをよく考えた上で実行されなければなりません。しかし、それはどの組織にとっても前進と成長の機会をもたらす強力な武器となります。不要なハードウェアを導入して余分なコストをかけるのではなく、プロセスを合理化して諸経費を削減することに重点を置くべきです。それこそがJamf Unlockが実現してくれるものであり、だからこそ、組織のMacを保護するための最良の方法であると言えるのです。

Jamf Connectのアイデンティティ管理機能とパスワードレスのワークフローを組織で活用する方法を知るには、当社のスペシャリストまで**ご連絡**いただくか、お近くのApple販売代理店までお問い合わせください。