Whitepaper

SecureDoc™ by WinMagic

パスワードレス認証
ウィンマジックの見解

はじめに

長年にわたり、情報漏えいは企業にとってセキュリティ上の1番の懸念事項でした。ベライゾンのデータ漏えい/侵害調査報告書（DBIR）によると、ハッキングに関連する情報漏えいの81%は、パスワードが漏えいした、脆弱であった、あるいは盗まれたことが原因です。個人情報の盗難は、ユーザにとって最大の懸念事項でもありますが、数多くの長いパスワードは面倒で非常に煩わしいものにもかかわらず、パスワードフィッシングなどのサイバー攻撃に対して効果をあまり発揮しませんでした。

また昨今では、働き方改革の推進により、どこにいても業務が遂行できるように、どこからでも業務に必要な情報にアクセスできるためのネットワーク環境を整備する組織が増えてきています。「社内ネットワーク」という概念を撤廃するという考え方です。その様な考え方を推し進めてきた組織だけでなく、新型コロナウィルスの影響によって、否が応でもテレワークを実施せざるを得ない組織も数多くあります。場所を選ばずに必要な時に必要な情報にアクセスすることが求められています。もちろんセキュリティを高く維持した上での情報へのアクセスが必要となります。これまでの情報の置き場所や置き方とは異なるため、これまでと同じアクセス方法では不十分という声も上がってきています。

その様な現在の状況に対して、セキュリティ業界はどのような対策をとっているのでしょうか。

需要の高まりとテクノロジの進歩により、パスワードレス認証が勢いを増しています。

本ホワイトペーパーでは、上記のトピック/主要な調査結果に関するウィンマジックの以下の見解を示していきます。

- セキュリティ業界がパスワードレス認証へ取り組んだことによって、個人情報の盗難が無くなり、その結果、オンライン上の情報漏えいの主な原因は解消されるようになります。
- ユーザは、数多くの長くて複雑なパスワードに悩まされなくなります。
- 今はパスワードレス時代の初期段階にあります。
- 攻撃などを考慮して、パスワードレスソリューションは、例えば、ソフトウェアトークンの展開などによって、クライアント側で簡単に実行されるでしょう。
- 多少時間がかかるとしても、今後はサーバ側でもパスワードレスソリューションが出てくるでしょう。

問題となる認証シナリオ

「パスワードレス」によって変化する認証シナリオのいくつかの工程を検証してみましょう。ユーザがノートパソコンを使用していて、Web サイト（＝サーバが提供する Web ページ）にログインしようとしています。ここでは 2 つの性質の異なる工程が実行されます。

1. **リモート認証：**サーバとデバイス間で発生します。特に検証は、ユーザまたはデバイスが置かれている場所から離れたサーバで実行されます。
2. **ローカルジェスチャ：**ユーザは自身が所有するデバイス上でいくつかの操作を行い、サーバでの認証を実行させます。

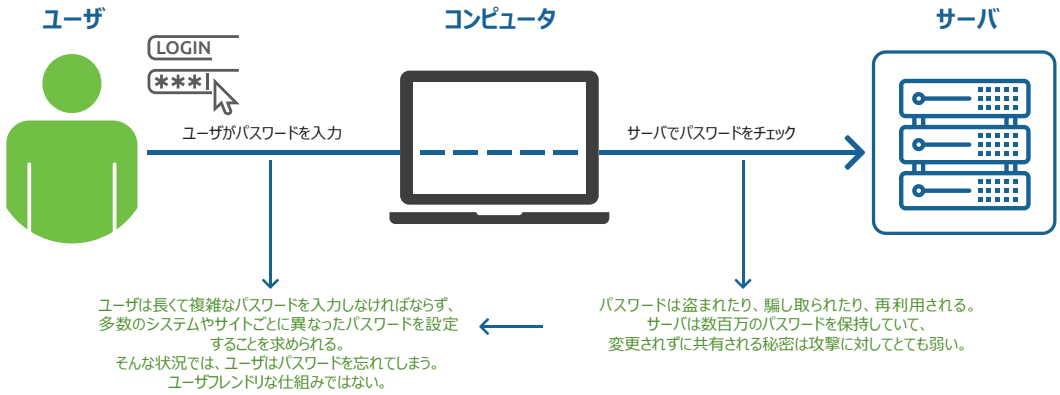
リモート認証

ユーザ名とパスワードを使用する現在のリモート認証

現在の「ユーザ名とパスワード」認証の仕組みは次のとおりです。

1. パスワードに同意します。
2. サーバにそのバージョン（ハッシュなど）とユーザが入力したバージョンを比較させます。

“ユーザ名とパスワード”認証

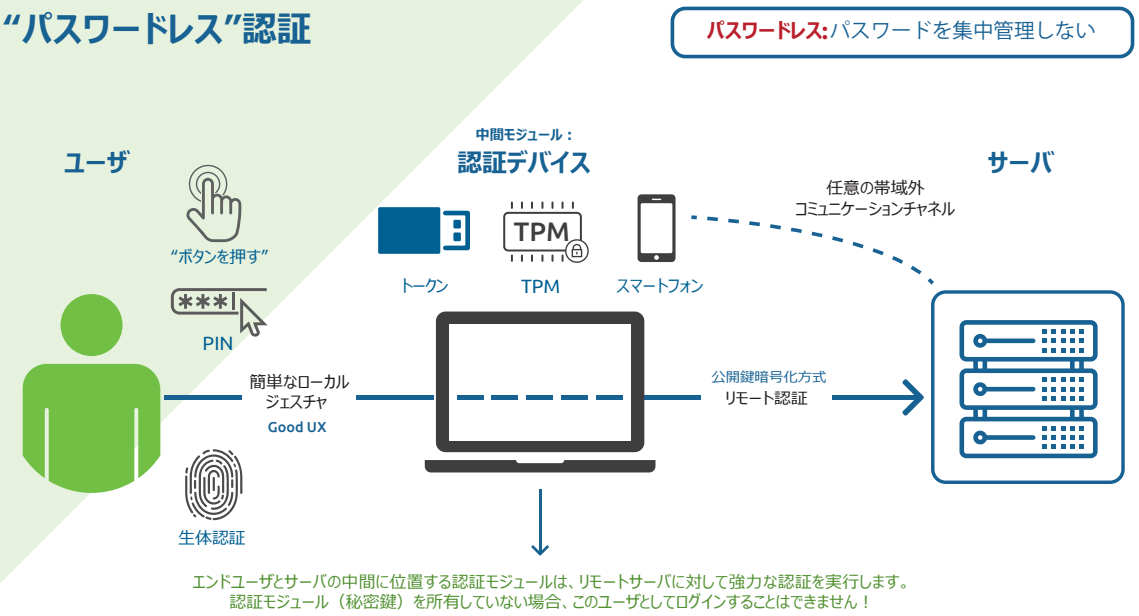


攻撃者は、フィッシングなどの攻撃を介して、ユーザが現在使用しているパスワードを入手できます。そして、あたかも正規のユーザであるかのように、インターネット上のどこかにあるデバイスからログインし、Webサイトにアクセスできます。多くの場合、ユーザがどれだけ強力で推測しにくいパスワードを作成したかは関係ありません。長くて複雑なパスワードを選択したり、Webサイトやサーバごとに異なるパスワードを設定したりすれば、攻撃の有効性はいくらか低下しますが、それ以上の効果はありません。ユーザが多くのパスワードを書き留めずに覚えようと努力しても、関係ありません。

一方、セキュアなリモート認証であるこの新しいソリューションは、たとえ攻撃者が世界中の（すべてのクラウド、データセンター、そして数十億台のコンピューティングデバイスを連動させた）処理能力を利用できたとしても、認証に成功するまでに数百万年を要するように構築されています。

公開鍵暗号化を使用した認証

公開鍵暗号化方式を使用することで、ユーザは秘密鍵を使用してデータに署名できます。ユーザの公開鍵を持つサーバは、その署名がユーザ、つまり秘密鍵を持つ唯一の人物からのものであることを確認できます。検証を含む認証は、ユーザが秘密鍵を共有することなく実行が可能です。



「デバイス」の機能 ：

ここまでのウィンマジックの見解は、次のとおりです。

- 従来の「ユーザ名とパスワード」認証では、デバイスは通信装置にすぎず、認証はユーザとサーバ間で行われています。パスワードは、多要素認証における「知識情報」です。
- 新しいパスワードレスソリューションの大きな変更点は、ユーザではなくデバイスによって積極的に認証が行われる点です。前述した公開鍵暗号化方式の工程における「ユーザ」とは、認証モジュールとしてのデバイスを意味します。デバイスは、公開鍵暗号化方式の操作を実行でき、サーバ上の公開鍵に対応する秘密鍵を持っている必要があります。また、秘密鍵をデバイスからコピーできなければ、そのデバイスなしでの認証は一切不可能です。
- 従って、デバイスがリモート認証を非常にセキュアにします。その堅牢さはとても長くて複雑なパスワードの数千～数百万倍を超えるものです。何らかの方法で、この「認証モジュール」が、長くて複雑な数多くのパスワードをユーザが覚えなくていいようにすることもできれば完璧です。

NISTは、「パスワードレス」であるにもかかわらず、一部の方法やデバイスに反対を唱えています。

今日のいくつかのソリューションではデバイスと暗号化が使用されていますが、それらは最新の攻撃には対抗できないと考えられています。「SMSプッシュ」（電話へのメッセージ送信）やワンタイムパスワード（OTP）は今後廃止されると予想しています。

本ホワイトペーパーでは、公開鍵暗号化方式のみを検討します。現在、FIDOが注目されていますが、PKI、スマートカード、証明書を使用する他の方法も普及しており、同様のセキュリティレベルを提供しています。

ローカルジェスチャ

前述したように、ユーザは自身が所有するデバイス上でいくつかの操作を行い、サーバでの認証を実行させます。このローカルジェスチャは、ユーザのデバイスに対する認証ではなく、そうである必要もありません。なぜなら、ユーザは既にそのデバイスを使用しているからです。

そして、一般的には、ユーザがデバイス上で実行する必要のある操作は、ユーザまたは会社のポリシーに完全に依存します。従来の「ユーザ名とパスワード」の場合とは異なり、ローカルジェスチャは、デバイスとリモートサーバ間の強力な認証には関与しません。認証モジュールがユーザに代わって強力な認証という素晴らしい仕事をしてくれます。これによってリモート認証が非常に強力になると同時に、ローカルジェスチャはシンプルになります。ユーザは単にそのデバイスを持っているだけでよいのです。

考慮すべきその他の事項

認証デバイスとして使用できるものは何か？

公開鍵暗号方式の認証のセキュリティは、秘密鍵やセキュアストレージの保護と操作時（セキュアな実行）に大きく依存しています。鍵をデバイスからコピーできない場合、秘密鍵を入手するにはデバイスを盗み、ロック解除の方法を入手するしか方法はありません。

通常、暗号化チップは、セキュアな鍵の格納場所および、チップ内で保護されたセキュアな実行環境を提供します。この「ハードウェアベース」の暗号化を使用すると、いかなる状況でも秘密鍵が露呈することはありません。

今日、データの保護に役立つ機能が搭載されたハードウェアは増え続けています。（USB）暗号トークン、スマートカード、およびTPMには通常、暗号チップが搭載されており、それらがデータの保護に役立ちます。電話とコンピュータには、セキュアな実行と保存のための機能が以前よりも多くなっています。

認証デバイスとサーバ間の通信チャネルは何か？

現時点では、認証デバイスと認証サーバ間の通信チャネルに重点を置く必要があります。世界がパスワードレス認証に移行し始めたばかりのこの段階においては、「企業内の様々な利用形態にわたりパスワードレス認証を導入するには既存のシステムに対する変更を最小限に抑えた統一性のある戦略を策定することが重要」というガートナーの推奨事項にウィンマジックは同意します。この通信チャネルは重要な役割を果たしており、今後も変化や適応が見られるとウィンマジックは考えます。

新しいパスワードレス時代への移行では、次のような特徴的な変化が起きます。

- 認証モジュールの使用
- クライアント/サーバ型プリケーションの認証に関して、認証は認証サーバにオフロードされる事があります。認証をアプリケーションサーバから認証サーバに分散するとセキュリティ上予期しない影響が生じる事があります。
- 認証用の通信チャネルは、もはやクライアントとサーバの間のみではありません。別の通信チャネルを介してパソコンの代わりにスマートフォンを使用すると、いくつかの予期しない影響が生じることがあります。

通信チャネルについて以下に説明します。

別の通信チャネルでのスマートフォンの使用

最近はスマートフォンの使用が一般的になっています。SMSプッシュとOTPはいずれ廃止されますが、FIDOは普及することが予想されます。

認証デバイスとしてのトークンまたはパソコンの使用

ここでは、パソコンと認証サーバの間の通信チャネルを使用する全ての方法を一括して扱います。スマートフォンはBluetoothなどを介してパソコンとの通信も可能です。そのため、スマートフォンはパソコンと認証サーバ間の通信チャネルを使う認証デバイスにもなり得る点に注意が必要です。

TPMチップを搭載したノートパソコンと、USBトークンとBluetooth接続の電話の使用により、非常にセキュアなソリューションが提供されます。また、ノートパソコンがこれまでと同じ通信チャネルを使うことが可能になり、アプリケーションと認証の良好な接続を維持できます。現時点では、この通信チャネルはこれまでの認証から変更となる箇所を最小限に抑えられると考えます。

これまでの認証から変更となる箇所をさらに少なくするには

最新のノートパソコンには、メモリ暗号化やセキュアな実行の機能が搭載されています。個人情報の窃取は通常、フィッシング、オンライン攻撃、あるいはマルウェアを介して行われます。通常の個人情報の窃取でノートパソコンを盗む攻撃者はほとんどいません。ノートパソコンが盗まれたとしても、SecureDocのフルディスク暗号化とファイル暗号化によって、ノートパソコンのセキュリティは確保されます。

パソコンに対する攻撃とテクノロジを踏まえると、ソフトウェアベースのトークンは、秘密鍵の保護において十二分な機能を果たすことができるうえ、これまでの認証から変更となる箇所がほとんどないため、企業はパスワードレス時代に容易に移行できると思われます。ウィンマジックの「SecureDocトークン」は、TPM、FIDOトークン、スマートカード/PIVカード（独自）などの非FIDOトークン、および最も柔軟性の高いソフトウェアトークンをサポートします。ハードウェアコストもかからず、管理コストも保守コストもかかりません。

SecureDocトークンは、小売業者がオンラインビジネスを行うために顧客に提供する数多くのトークンの1つとして使用できるだけでなく、Windowsログオン、Webサイト、SaaS、VPNなどのさまざまなアプリケーションを利用するユーザも使用できます。今すぐ簡単に導入でき、将来的にも対応可能な最上位かつ最もセキュアなソリューションです。

アプリケーションの一部としての認証 – 次のステップ

本書では認証についてご説明しました。パスワードレスの時代が進むにつれ、セキュリティ業界はこれらの認証をVPNやレガシーアプリケーションを含むその他のアプリケーションに追加するようになるでしょう。一部のWebサイトは既にFIDOをサポートしています。強固な認証が普及しつつあるのを目の当たりにして、大変嬉しく思います。個人情報の盗難は過去のものになるでしょう。本書で示したウィンマジックの見解および説明が、皆様のお役に立つことを願っています。

まとめ

- セキュリティ業界がパスワードレス認証へ取り組んだことによって、個人情報の盗難は無くなり、その結果オンライン上の情報漏えいの主な原因は解消されるようになります。ユーザもまた、数多くの長くて複雑なパスワードに悩まされなくなります。
- 業界で使用されている「パスワードレス」という用語に、最初は少し混乱するかもしれません。これはリモート認証に用いられるものであり、デバイスに対する認証とは関係ありません。具体的には、ユーザがパスワードを使用できなくなるわけではありません。
- 今はパスワードレス時代の初期段階にあります。たとえば、すでにWebサイトやSaaSでのFIDO認証については、複数の大手企業がサポートしていますが、どこにでも導入されているわけではありません。一般的なアプリケーションサーバのベンダは、今後数年以内にパスワードレスソリューションの提供を開始するでしょう。また、標準化に伴って、主にアプリケーションと認証/サーバ/クライアント間でのプラグアンドプレイになると予想されます。
- ウィンマジックはまず、包括的なマルチプラットフォームクライアントソフトウェアを提供し、最も単純なものから最上位のものまであらゆるニーズに対応できると考えています。コンピューティングデバイス（主にノートパソコン）では、TPMに暗号化チップが組み込まれています。TPMがない場合でも、企業はセキュアな実行を通じて、これまでの認証から変更となる箇所を最小限に抑えつつ、パスワードレス時代に簡単に移行することができます。なお、SecureDocトークンは、FIDO認証用の既存の（PIV）スマートカードもサポートしています。
- ウィンマジックのSecureDocエンドポイント暗号化、そして新たなパスワードレス認証により、エンドポイントのすべての暗号化と認証で最高のユーザエクスペリエンスを提供できます。数あるベンダの中で、MFAプリブート認証からパスワードレス認証サーバにシングルサインオンを提供できるベンダはウィンマジックだけです。

多要素認証（MFA）に関連する見解

多くの場合、認証は以下の要素を1つ以上使用する多要素認証（MFA）を伴います。要素とは、知識情報（パスワードなど、ユーザのみが知っていること）、所持情報（ハードウェアトークンなど、ユーザのみが持っているもの）、そして生体情報（バイオメトリクスや、ユーザの入力スピード/リズムなど、ユーザ自身の特徴）です。

上記の認証についてのウィンマジックの見解は、 次のとおりです。

サーバが使用できる唯一のものは、ネットワーク（インターネットを含む）経由でデバイスから送信されるデータです。サーバは所持情報や生体情報を物理的に検証できません。「ユーザが持っているもの」とは、物理的な鍵のようなものを指すと考えることができます。しかし、具体的に定義することはここではしません。

いずれにしても、前述のシナリオで求められる強力なMFAからは逸脱しています。一方、MFAが一部のリモートサーバにアクセスするための要件になり得ることは理解できます。しかし実際には、ローカルジェスチャを最小限にしてユーザエクスペリエンスを向上させることができます。これは主に、ユーザがすでにそのパソコンを使用中であり、デバイスへの再認証が不要であるためです。

（強力な）多要素認証は、ローカルデバイス（ノートパソコンなど）への認証に関しても同様に適用されるべきです。ノートパソコン自体には、トークン、スマートカードリーダー、または指紋リーダー、マイク、カメラなどの生体認証センサーに使用されるUSBポートが装備されています。ウィンマジックはフルディスク暗号化ベンダとして、プリブート認証（PBA）でのMFAを推進していますが、ほとんどのユーザはPBAを使用しないことに甘んじているようです。ウィンマジック製品を使用することで、どれだけ簡単にPBAでMFAを実行できるのかが広く認識される日が訪れるはずです。

さらに、リモート認証の場合には、帯域外認証が可能です。MFAではありませんが、これはまた別の要素です。帯域外認証の場合、別の通信チャネルを使用していれば、サーバが認識するのはデータだけであるという同じ考え方が適用されます。

パスワードレス認証の「パスワードレス」とは

「パスワードレス」とは、パスワードが一元的に管理されることも、一元的に保存されることもない、という意味だとウィンマジックは結論付けました。パスワードレス認証とは、サーバへの認証を指します。ローカルデバイスでのローカルジェスチャにパスワードが含まれていないという意味ではありません。

「パスワードレス」とは、フルディスク暗号状態のプリブート認証の様なデバイスへの認証や、OS へのログインについてのことでは断じてありません。

2020年7月、ウィンマジック

暗号化および認証ソリューションの詳細については、ウィンマジックにお問い合わせください。
sales.jp@winmagic.com

ウィンマジック・ジャパン株式会社
〒 105-0022 東京都港区海岸 1-2-3 汐留芝離宮ビルディング 21 階
TEL.03-5403-6950 FAX.03-5403-6953