WINMAGIC

ホワイトペーパー

パスワードレス認証

安全なリモートアクセスを実現する新たなアプローチ



はじめに

情報漏洩は、企業にとって長年にわたりセキュリティ上の最も大きな懸念事項になっています。Verizon の「情報漏洩調査報告書」（DBIR）によると、ハッキングによる情報漏洩の 81% は、パスワードの侵害や脆弱性、盗難が原因であると報告されています。個人情報の盗難はユーザにとって大きな懸念事項ですが、たとえ長くて複雑なパスワードを設定したとしても、ユーザの負担が大きくなるだけで、フィッシングやパスワードに対する攻撃に対してあまり効果的であるとは言えません。このパスワードの課題に関する、業界の取り組みを紹介します。

パスワードレス認証は、市場のニーズと技術の進歩に伴い、近年普及が進んでいます。

このホワイトペーパーでは、以下のトピックおよび主な調査結果に対するウィンマジックの見解を紹介します。

01

オンライン情報漏洩の主な発生源である個人情報の盗難は、パスワードレス認証による業界の取り組みにより、大半が根絶されます。

02

ユーザは長くて複雑な多数のパスワードに苦労しなくなります。

03

私たちは現在、パスワードレス時代の初期段階にいます。

04

パスワードレスソリューションは攻撃の手法が考慮されており、クライアント側で簡単に導入できます（ソフトウェアトークンの展開を利用するなど）

05

サーバ側は、過去数年の進歩を上回るスピードで迅速に対応できます。

パスワードレスソリューションの認証シナリオ

従来のユーザ名とパスワードを使った認証と、パスワードレス認証の認証プロセスの違いを以下のシナリオで説明します。まず、認証にはノート PC などのエンドポイントデバイスを使用して「サーバ」にログインする場合、次の 2 つの異なる認証を実行する必要があります。

リモート認証

リモート認証は、サーバとエンドポイントデバイス間で発生します。特に、認証情報の検証はサーバ上で行われ、サーバはユーザやエンドポイントデバイスが存在する場所から離れています。

ローカルでの操作

ユーザは、エンドポイントデバイスにログオンし、何らかのローカル操作を行い、サーバ側でリモート認証を実行するようエンドポイントデバイスに指示を出します。

リモート認証

従来のリモート認証方法はユーザ名とパスワードを利用

従来の「ユーザ名とパスワード」による認証を以下に示します。

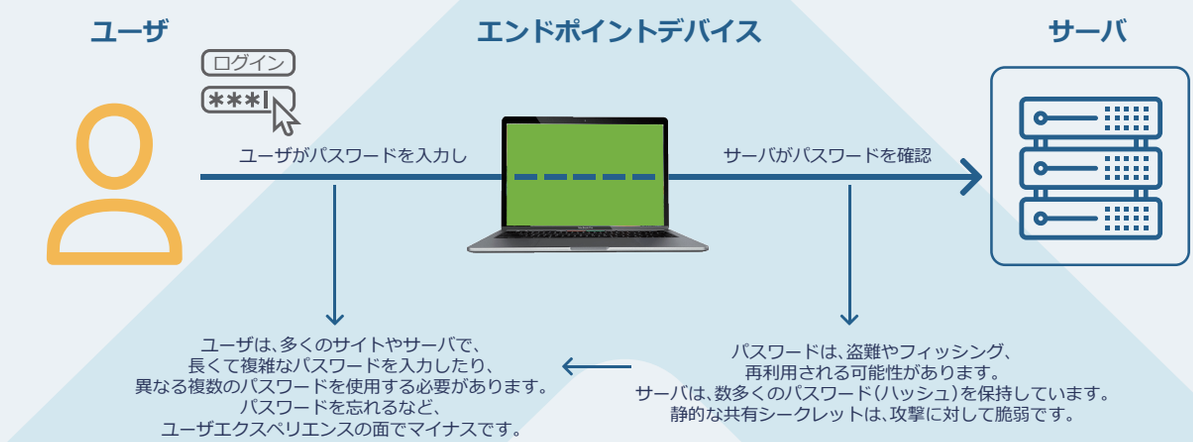
01

パスワードを入力する

02

サーバがパスワードを比較する
例）ハッシュとユーザが入力したパスワードを比較。

「ユーザ名とパスワード」の認証



このシナリオでは、ユーザのパスワードは、フィッシング攻撃などを介して攻撃者に搾取される可能性があります。攻撃者は、ユーザが作成したパスワードの複雑さや強度に関係なく、インターネット上のどこかにあるエンドポイントデバイスからログインして、ユーザになりすまし Web サイトにアクセスできます。長くて複雑なパスワードを使用したり、Web サイトやサーバごとに異なるパスワードを使用した場合、一部の攻撃からは回避できることもありますが、十分ではありません。これは、パスワードを書き留めず、懸命に覚えた場合も同様です。

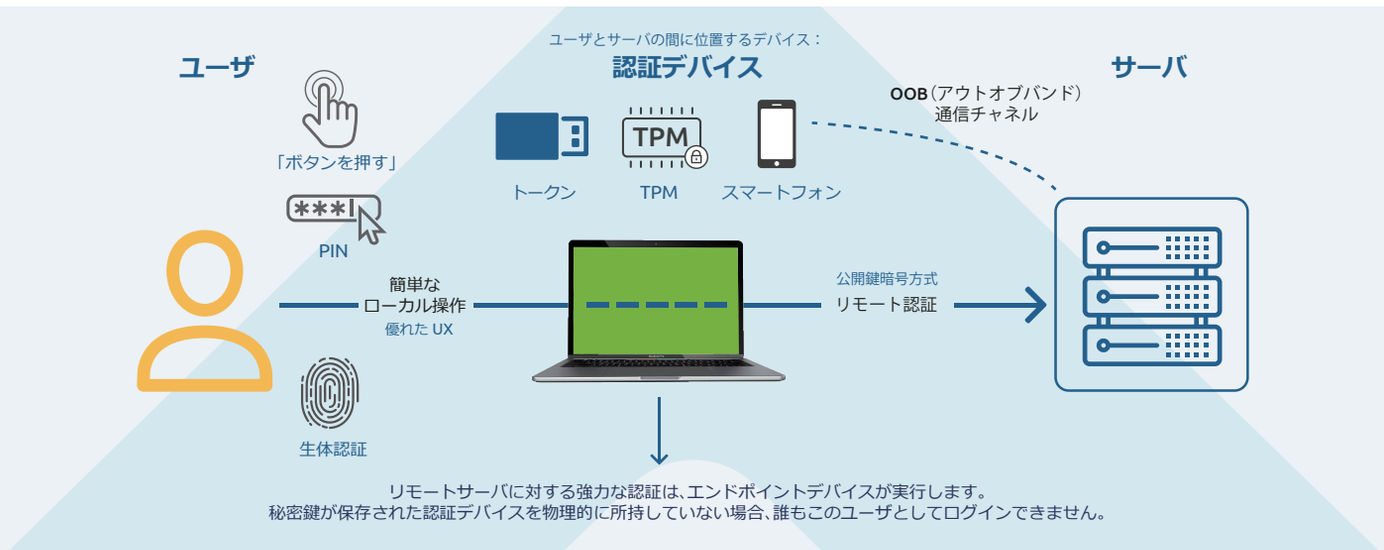
最新のソリューションでは、リモート認証の安全性を強化するために工夫されており、たとえ攻撃者が、世界中のすべてのクラウドやデータセンター、数十億台のコンピュータデバイスを組み合わせた計算能力を使用した場合であっても、認証の偽装に成功するまでに数百年はかかります。

公開鍵暗号方式による認証

公開鍵暗号方式を使用すると、ユーザは自身の秘密鍵を使用してデータに署名することができます。ユーザは秘密鍵を持っている唯一の人物であるため、ユーザの公開鍵を保管するサーバは、署名が当該ユーザのものであることを確認できます。認証や検証の実行は、共有シークレットを使用することはなく、ユーザが秘密鍵自体を共有することもありません。

「パスワードレス」認証

パスワードレス：パスワードは一元管理されていない。



「デバイス」の機能

現時点でのウィンマジックの見解を以下に示します。

01

従来の「ユーザ名とパスワード」の方式では、エンドポイントデバイスは単なる通信チャネルであり、認証は、ユーザとサーバ間で行われます。パスワードは、多要素認証の「知識情報」を意味します。

02

最新のパスワードレスソリューションの主な変更点は、認証は、ユーザではなくエンドポイントデバイスが能動的に行います。上記の公開鍵暗号方式の認証で「ユーザ」の言及がある場合、認証デバイスを意味します。エンドポイントデバイスは、公開鍵暗号方式の操作を実行できる必要があり、サーバ上の対応する公開鍵に合う秘密鍵を持っている必要があります。秘密鍵は、エンドポイントデバイスから外部にコピーすることはできないため、エンドポイントデバイスを物理的に所持していない人物は認証できません。

03

したがって、「エンドポイントデバイス」を利用すると、リモート認証を安全に行うことが可能で、非常に長く複雑なパスワードより、数千・数百万倍安全です。また、この「ユーザとサーバの間に位置するデバイス」を利用すると、ユーザはいくつもの長く複雑なパスワードを覚える必要がなくなり、ユーザエクスペリエンスの面でも非常に優れています。

NISTは一部の「パスワードレス」方式や、デバイスを推奨していません

一部のソリューションでは、デバイスと暗号化を使用している場合でも、最新の攻撃に対しては不適切だとみなされています。特に「SMS プッシュ」（スマートフォンにメッセージを送信）やOTP（ワンタイムパスワード）は、近い将来に非推奨になることが予想されます。

このホワイトペーパーでは、公開鍵暗号方式を利用した認証方式のみを検討します。その中でも FIDO は現在非常によく知られていますが、PKI やスマートカード、証明書を使用した方式も普及しており、同様のセキュリティレベルが得られます。

ローカル操作

上記で説明したとおり、ユーザは、エンドポイントデバイス上でローカル操作を行うことで、サーバとの認証を実行するようエンドポイントデバイスに指示することができます。このローカル操作は、エンドポイントデバイスへのログオンを認証するものではありません。ユーザはローカル操作を行う時点ですでにエンドポイントデバイスを利用しています。

一般的にローカル操作はユーザや所属会社のポリシーによって全く異なります。ローカル操作は「ユーザ名とパスワード」の従来のケースとは異なり、エンドポイントデバイスとリモートサーバ間の強力な認証とは一切関係ありません。ユーザとサーバの間のデバイスが強力なリモート認証を行います。ローカル操作は非常にシンプルであっても、リモート認証は非常に強力です。ユーザは該当のデバイスを所持する必要があるだけです。



その他の考慮事項

認証デバイスとして使用可能なデバイス

公開鍵暗号方式を利用した認証のセキュリティは、秘密鍵の保護やセキュアなストレージ、**利用時の安全な実行**に大きく依存しています。鍵をデバイスから外部にコピーできない場合、秘密鍵を取得する唯一の方法は、デバイスを窃取し、ロックを解除する方法を知ることです。

通常、暗号化チップは、鍵の安全な保管、および安全な実行環境の両方を備えており、チップ内で保護されています。「ハードウェアベース」の暗号化を利用すると、秘密鍵が持ち出されることは絶対にありません。

現在、データ保護に役立つ機能を備えたハードウェア（USB）がますます増加しています。一般的に、暗号化トークンやスマートカード、TPM は、暗号化チップを備えており、このようなジョブを適切に実行することができます。スマートフォンやコンピュータは、安全に実行・保管するための機能がますます強化されています。

認証デバイスとサーバ間の通信チャネルについて

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焦点を当てざるをえないと考えています。世界は、パスワードレス認証への移行の初期段階であるため、Gartner 社が推奨する「最小限の移行部分を組み合わせて、主要な用途に対してパスワードレス認証を導入する総合的な戦略を策定する」ことをお勧めします [1]。この通信チャネルは重要な役割を担っており、今後の過程で、変更や修正があると考えられます。

新しいパスワードレス時代への移行には、以下の明確な変化を伴います。

01

ユーザとサーバの間に位置するエンドポイントデバイスがリモート認証を行います。

02

クライアント・サーバアプリケーションの認証は現在分離されていますが、今後は、認証の負担が認証サーバに移管（オフロード）される可能性があります。これにより、セキュリティに影響を与える可能性があります。

03

認証に使用する通信チャネルは、エンドポイントデバイスとサーバ間に限定されなくなります。エンドポイントデバイスの代わりに、異なる通信チャネルを持つスマートフォンを利用する場合、複数の影響が生じる可能性があります。

[1]Gartner "Top Five Midsize Enterprise Security Projects for 2020," Paul Furtado, Brian Reed, 6 May 2020

通信チャネルについて、以下で説明します。

異なる通信チャネルのスマートフォンを認証デバイスとして使用する

近年、認証プロセスでスマートフォンを利用することが一般的になっていますが、SMS プッシュや OTP は近い将来、非推奨になると思われます。FIDO の利用者は今後も増え続けると思われます。

同じ通信チャネルのエンドポイントデバイスやトークンを認証デバイスとして使用する

エンドポイントデバイスと認証サーバ間の通信チャネルを使用する認証方法（認証デバイス）には選択肢があります。スマートフォンは、Bluetooth® を介してエンドポイントデバイスとやりとりすることもできるため、スマートフォンも同じ通信チャネルを使用する認証デバイスになることができます。

TPM チップを搭載したエンドポイントデバイス、USB トークン、上述の Bluetooth 接続のスマートフォンは、エンドポントデバイスとサーバ間で、アプリケーションと認証に同じ通信チャネルを使用するため、非常に安全なソリューションである、と考えられます。現時点では、この通信チャネルを使用した認証方式を採用すれば、移行部分を最小限に抑えることができると考えられます。

移行部分を更に最小限に抑えるには

最新のノート PC にはメモリ暗号化やセキュア実行を備えています。一般的に個人情報の盗難は通常、フィッシングやオンライン攻撃、場合によりマルウェアを介して行われます。個人情報を不正に入手するために、ノート PC を窃取しようとする攻撃者も存在します。SecureDoc™によるフルディスク暗号化やファイル暗号化を利用すれば、盗難された場合でもノート PC の安全を確保することができます。

ソフトウェアベースのトークンは、PC に対する攻撃やテクノロジーを考慮すると、秘密鍵をより適切に保護することが可能で、企業各社は移行部分を最小限に抑えながら、パスワードレス時代に簡単に対応することができます。ウィンマジックの「SecureDoc トークン」は、TPM や FIDO トークン、スマートカードや PIV カード、更に非常に柔軟なソフトウェアトークンをサポートしています。ソフトウェアトークンを使えば、ハードウェアを追加するコストや管理・保守のコストは発生しません。

SecureDoc トークンは、小売企業がオンラインビジネスのために顧客に提供するトークンとして利用できるだけでなく、Windows ログインや Web サイト、SaaS や VPN など、さまざまなアプリケーションを使用する企業の従業員が利用することも可能です。SecureDoc トークンを利用すると、将来性のあるパスワードレス環境に簡単に移行することができ、非常にハイエンドで安全性の高いソリューションを導入することが可能になります。

多要素認証に関するいくつかの見解

認証は、しばしば多要素認証がイメージされます。多要素認証には、知識情報（ユーザとユーザのみが知っている何か（パスワードなど））、所持情報（ユーザとユーザのみが持っている何か（ハードウェアトークンなど）、および生体情報（ユーザとユーザに限定されたもの（生体認証、ユーザが入力する速度やリズムなど）が含まれます。

認証に関する現状解析とウィンマジックの見解

サーバが使用可能な唯一のものは、ネットワーク（インターネットなど）を介してエンドポイントデバイスから送信されたデータです。しかし、サーバでは、ユーザの所持情報や生体情報を物理的に確認することはできません。「所持情報」は、物理的な鍵などを指すと考えられますが、正確な定義は、ここでは追及しません。

シナリオで説明した利用方法以外の場面で多要素認証が使われているケースが見受けられます。多要素認証がリモートサーバへのアクセス要件となっていることは理解できます。一方で、ユーザはすでにコンピュータデバイスを使用しており、デバイスの再認証を行う必要がないため、ここで述べているローカル操作は最小限に抑えることができます。

ノート PC などのエンドポイントデバイスへのログインに、（強力な）多要素認証を使用する必要があります。ノート PC 本体には、トークンやスマートカードリーダーに使用する USB ポート、指紋リーダーなどの生体認証センサ、マイクやカメラなどが搭載されています。

ウィンマジックは、自社のフルディスク暗号および Bitlocker のプリブート認証に多要素認証を提供していますが、多くの企業では、PIN を使用していたり、プリブート認証（PBA）を使用していない場合があります。ただし、これは別のトピックになります。留意点として、リモート認証では、帯域外通信チャネルを使用することが可能で、これは、サーバが把握する唯一の情報はエンドポイントからのデータであるということにも適用できます。

パスワードレス認証の「パスワードレス」という用語について

結論として、「パスワードレス」とは、パスワードが一元的に管理・保管されないことを意味すると考えます。パスワードレス認証は、サーバに対する認証を指しており、ローカル操作で、パスワードの使用が不要になるという意味ではありません。

更新情報：2022 年 6 月 WinMagic Corp.

アプリケーションの一部としての認証 - 次のステップ

パスワードレス時代に移行する中、業界では、パスワードレス認証が、VPN などのアプリケーションやレガシーアプリケーションにも追加されると思われます。一部の Web サイトでは、FIDO 認証がサポートされています。私たちは、強力な認証が普及していることをうれしく思います。将来、個人情報の盗難が過去の話になると信じています。ウィンマジックの見解および説明が、お客様に役立つこと、また本書をお楽しみいただけたら幸いです。

まとめ

01

オンライン情報漏洩の主な発生源である個人情報の盗難は、パスワードレス認証による業界の取り組みにより、大半が根絶されます。また、ユーザはいくつもの長くて複雑なパスワードに苦労しなくなります。

02

認証に使用する通信チャネルは、スマートフォンなどを利用した帯域外チャネルより、エンドポイントデバイスの方が安全です。スマートフォンを使用するよりも、簡単な方法があります。

03

私たちは現在、パスワードレス時代の初期段階にいます。たとえば、大手のプレイヤーは現在、Web サイトや SaaS 上で FIDO を一部サポートしていますが、すべてではありません。一般的なアプリケーション（サーバ）のベンダーは、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予定していますが、エンドポイント上での（各サーバへの）パスワードレス認証登録手続きの簡略化が課題になると思われます。

04

ウィンマジックは、ローエンドからハイエンドまでサポートする包括的なマルチプラットフォームのクライアントソフトウェアにより、率先して貢献できると考えています。エンドポイントデバイス（主にノート PC）は、TPM に暗号化チップが組み込まれていたり、セキュア実行を備えており、企業各社は、移行部分を最小限に抑えながら、パスワードレス時代に簡単に対応することができます。

注：SecureDoc では、既存の PIV カードを FIDO 認証に使用することが可能です。追加のトークンは不要です。

05

ウィンマジックの SecureDoc Endpoint Encryption は暗号化ソフトウェアとして多くのお客様に実績があります。すべてのデータと認証は暗号化され、パスワードレス認証により最高のユーザエクスペリエンスを提供します。SecureDoc では、起動時のプリブート認証（多要素認証）を行うだけで、お使いになるすべてのリモートサーバへのシングルサインオンを可能にします。

ウィンマジック
認証し、暗号化し、成し遂げる。

詳細は、ウィンマジックにお問い合わせください

ウィンマジックは、サイバーセキュリティソリューションを開発してきた業界を代表する企業であり、25 年以上にわたってエンドポイント暗号化を進化させてきました。エンドポイントセキュリティに関する豊富な経験と、継続的なイノベーションへのコミットメントにより、世界中の 2,500 以上の企業や政府機関がウィンマジックの製品を信頼して使用しており、全世界で 300 万以上のアクティブライセンスが利用されています。ウィンマジックの認証および暗号化製品は、ノートパソコン、物理データセンター、仮想データセンター、オンプレミス、クラウドなどのあらゆる環境にあるデータを保護します。ウィンマジックのソリューションは、プラットフォームに依存せず、Windows、Linux、Mac デバイスのデータを保護できます。ウィンマジックは、サイバー攻撃の脅威やデータの損失から企業を保護し、プライバシーや法規制のコンプライアンス要件を満たすことができるように支援しており、幅広い評価を得ています。ウィンマジックは、セキュアでシームレスな認証と暗号化を実現します。お客様が、従業員とデータが確実に保護されていることを実感しながら、自由に活動できるようになり、アイデアを共有し、目標を達成できるようなソリューションを提供しています。詳細については、winmagic.com/ja/home-jp/ を参照してください。



WINMAGIC

米国 / カナダ
+1 888 879 5879

欧州 / 中近東 / アフリカ
+49 69 175 370 530

日本
+03 5403 6950

詳細は、こちらをクリックするか、
ウィンマジックまでお問い合わせください。