MagicEndpoint™

パスワードをなくす準備はできていますか？

パスワードレス認証の再定義：
最も安全でユーザがIDやパスワードを入力する必要がない認証

25年以上にわたる経験と絶え間ないイノベーションにより、ウィンマジックは先進の包括的多要素認証(MFA)とフルディスク暗号(FDE)によるエンドポイントセキュリティの最前線に立ち続けています。 NIST AES Certificate #1やNSA認証など、ウィンマジックが取得している数々の認証がそれを物語っています。そして現在もセキュリティを重視する世界中の企業の機密データを保護しています。

オンライン認証に革命をもたらす MagicEndpoint は、エンドポイントを活用することで、ユーザをオンライン認証の負担から解放します。シームレスでセキュア、そしてゼロトラストの原則を満たすMagicEndpointは、 ユーザがIDやパスワードを入力する必要がない次世代の認証を提供します。

WINMAGIC®

MagicEndpoint™

簡単に、バックグラウンドで、安全に認証する

MagicEndpoint では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します。エンドポイントデバイスへのログインが成功すると、このエンドポイントデバイス自体をオンラインサービスへの多要素認証の要素の一つとして使用します。この認証方式は既存のソリューションよりもセキュアで、ユーザが認証操作を一切行うことなく、ユーザが気づかないうちにオンラインサービスへの認証が完了します。このセキュアなオンライン認証では、ユーザがパスワードやPINを覚えたり、トークンやスマホアプリを所有したりする必要がなくなります。またパスワードを使っていないのでパスワードを忘れた際のリセットもなくなり、フィッシングの心配もなくなります。 MagicEndpoint を使えば、オンライン認証はバックグランドで行われ、ユーザはオンライン認証から解放されます。 MagicEndpoint はSaaSなど、殆どのオンラインサービスへの認証に対応しています。

ゼロトラストへのパラダイムシフトをリードする

ホワイトハウスのゼロトラストへの移行を求める覚書(OMB M-22-09)に沿ったMagicEndpointは、セキュリティのパラダイムシフトを象徴しています。パスワードを排除し、エンドポイントベースの認証に焦点を当てることで、フィッシングやクレデンシャル・スタッフィングなどのリスクを大幅に削減します。オンライン認証の標準/最良の方法である公開鍵暗号を利用して、MagicEndpointは以下を提供します：

- **アイデンティティ・ファースト：**公開鍵暗号機能を活用して、“ユーザアカウントをエンドポイントデバイスに紐づけした”ユニークで検証可能なIDを“リアルタイム”に作成します。暗号鍵は、ユーザがログインした後に、認証されたエンドポイントデバイスでのみ生成されます。エンドポイントデバイスはリモート・サーバよりも正確にユーザを認証できるため、エンドポイントデバイスへの認証にMFAを使用します。最新のエンドポイントデバイスはハードウェア暗号チップ（TPM）を搭載しており、暗号鍵をコピー、共有、同期ができないようになっているため解読されることはありません。
- **継続的なモニタリング：**サーバは、ユーザがオンラインサービスにログインを試みるまでは何も検証できません。一方、「エンドポイント・アクセス」 ソリューションは、エンドポイントデバイスにアクセスするすべてのユーザを継続的に監視し、制御することができます。エンドポイントデバイスはパーシステントコネクションで接続されたIdPサーバへリアルタイムに自身の状態をアップデートするため、 IdPサーバはユーザがどのエンドポイントでアクティブになっているか、画面がロックされているか(非アクティブであることを示す)、ユーザがどのサービスプロバイダーにアクセスしようとしているかなどを、すべてリアルタイムで追跡することができます。オンラインサービスのリクエスト前、リクエスト中、リクエスト後のすべての段階で、ユーザとデバイスの両方を継続的に管理および検証することで、強固なセキュリティを提供し、ハッカーによる侵害をはるかに困難にします。常時接続されたパーシステントコネクションはさらに、信頼されたユーザとデバイスだけがIdPにアクセスできることを保証します。

ゼロトラスト：ユーザ、デバイス、トランザクションの継続的な検証を保証します。 MagicEndpointは、” アイデンティティ・ファースト、エンドツーエンド “のアプローチで “常に検証する “というゼロトラストの原則を独自に実現する一方で、ユーザにとっても大きな利点を提供します。

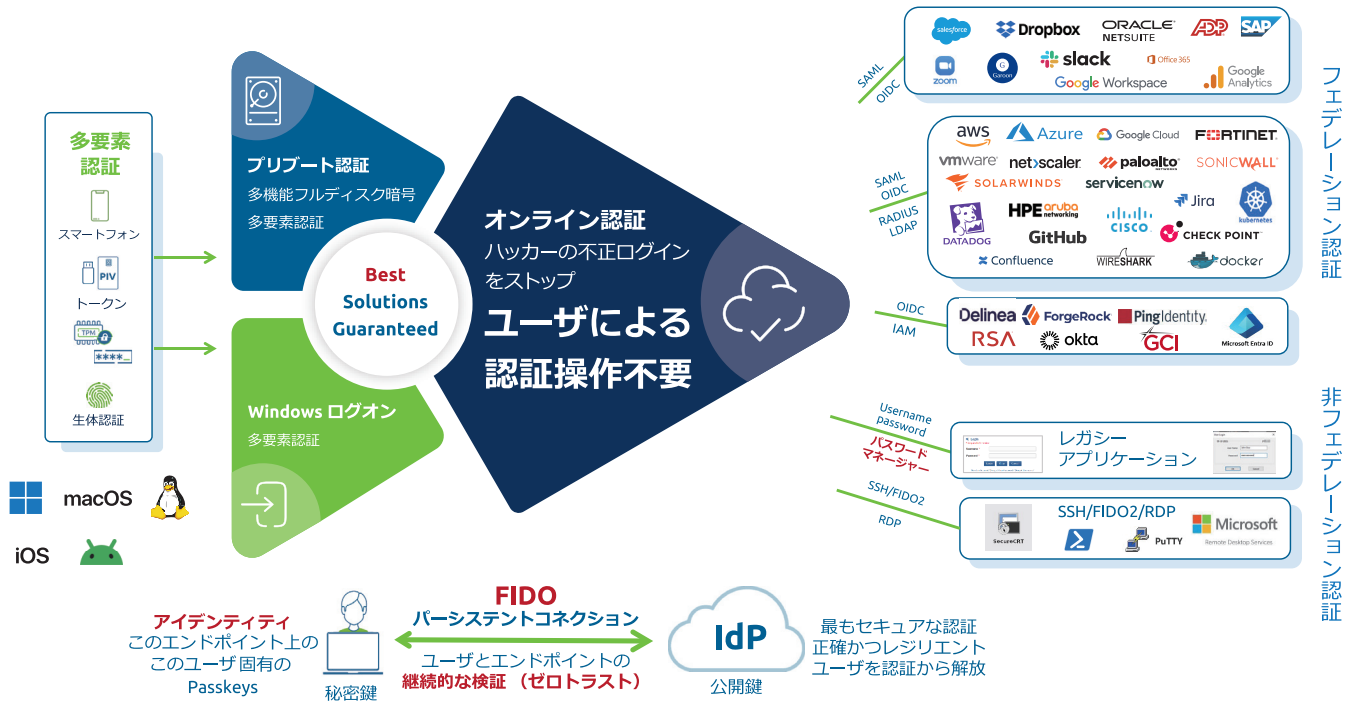
「一度サインオンすれば複数のアプリケーションにアクセスできる」 という、便利ではあるが必ずしも安全とは言えないアプローチを提供する従来のSSOソリューションとは異なり、 MagicEndpointはすべての認証リクエストをエンドポイントで明示的に検証します。

スマートフォンを使った Windowsログインの多要素認証の画面

Windows のログインにおいて、スマートフォンアプリと指紋などの生体認証による多要素認証が行えます。
同時にユーザーの操作なしで IdP サーバにも自動的にログインします。
スマートフォンアプリ・生体認証・IdP を活用すると「パスワードをなくす準備ができます」

パスワードをなくす準備が整った環境

ユーザはエンドポイントに 多要素認証でログイン → **以後オンラインサービスに 自動でログイン** → **対象のサービスは SaaS およびオンプレミス**



アイデンティティ このエンドポイント上のこのユーザ固有の Passkeys

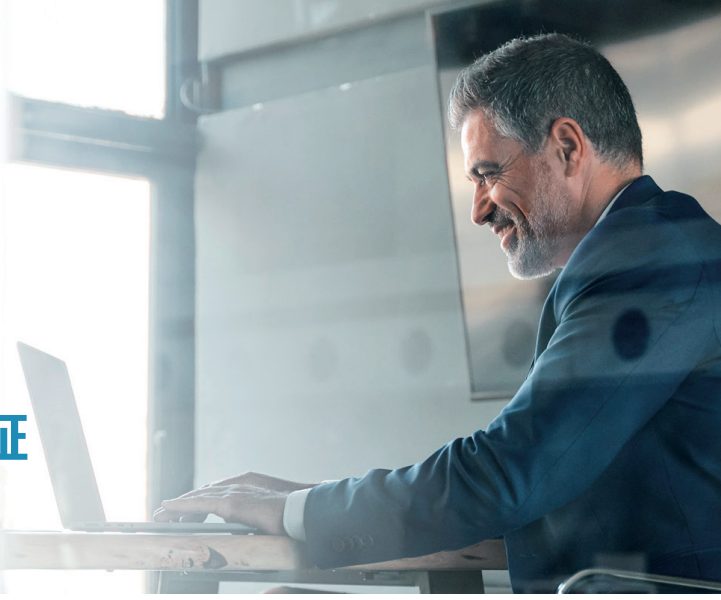
秘密鍵

FIDO パーシステントコネクション
ユーザとエンドポイントの**継続的な検証（ゼロトラスト）**

IdP

公開鍵

最もセキュアな認証
正確かつレジリエント
ユーザを認証から解放



企業のために作られ、ユーザのために最適化された認証

MagicEndpointは、今日の最も差し迫った認証の課題を解決するために設計されています。企業環境にシームレスに統合すると同時に、ユーザエクスペリエンスを改善します。

- **Windowsログオンの多要素認証：**MagicEndpointは、 Windowsログオンの安全な多要素認証およびパスワードレス認証を提供します。
- **プリブート・ログインの多要素認証：**MagicEndpointは、 オペレーティング・システムが起動する前のフルディスク暗号プリブート認証に対しても安全な多要素認証およびパスワードレス認証を提供します。
- **認証サービス - アイデンティティ・ファブリックの統合：**既存の IAM (アイデンティティとアクセス管理)システムとシームレスに統合するように設計されたMagicEndpointは、セキュアな認証のためのアイデンティティファブリックの中で動作することができます。

MagicEndpoint：ユーザの認証操作が不要なシームレスなセキュリティ

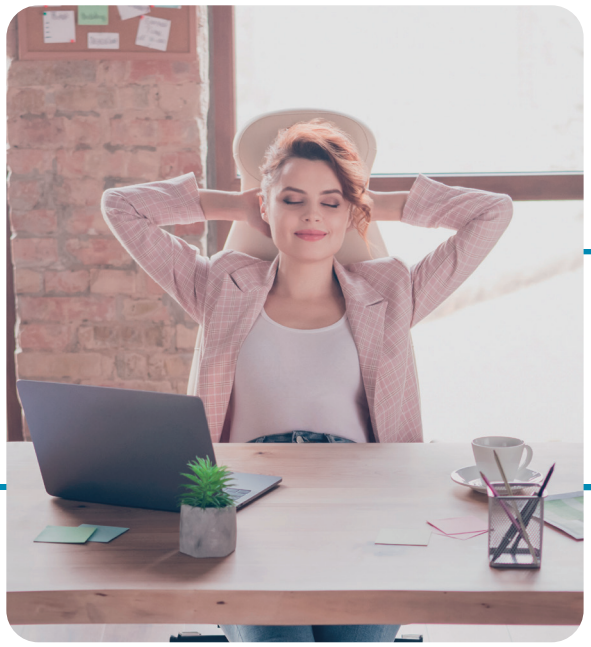
セキュリティが最も重要な世界において、 MagicEndpointはユーザの介入を不要にすることで認証を再定義します。ユーザは認証の操作を一切することなく、オンラインアプリケーションやシステムへのスムーズなアクセスが可能になり、より重要な業務に集中することができます。認証の負担をユーザからエンドポイントデバイスに移行することで、セキュリティを損なう事なく、はるかに正確な認証が可能になります。

以下のユーザの認証操作が不要になります

- ✖ パスワードの入力
- ✖ SMS、ワンタイムパスワードの入力
- ✖ スマートフォンでの操作
- ✖ タイムアウト後の再認証
- ✖ パスワードリセット
- ✖ クレデンシャル盗難への対策
- ✖ MFAバイパスへの対策

MagicEndpoint：
パスワードレス・セキュリティへの鍵

MagicEndpointで次世代のエンタープライズセキュリティを体験してください。ウィンマジックのソリューションは、**ゼロトラスト**のような業界のベスト・セキュリティ・プラクティスに準拠しながら、ユーザ・ファーストのアプローチで究極のパスワードレス認証を提供します。



セキュリティを強固にする

バックグラウンドで、
簡単かつ安全に認証する

今すぐデモをご予約ください！

ユーザ事例

コンシューマ・サポート・サービス社

企業プロフィール

コンシューマ・サポート・サービス社（CSS）は、約 2,500 人の従業員を擁し、米国オハイオ州全域で発達障害や身体障害を持つ人々にデイ・ハビリテーション、送迎、フルタイムの住み込み住宅サービスを提供する医療機関です。

業種

医療

所在地

米国オハイオ州

主なサービス

CSS は、以下のような重要なサービスを提供しています：

- デイ・ハビリテーションとデイケア施設
- 受診を予約している患者の送迎
- 条件を満たした患者のためのフルタイムの住み込み住宅

課題：分散型デジタル・エコシステムの保護

2023 年、 CSS はその業務を支えるデジタルシステムとサービスに関連する重大なセキュリティ上の課題に直面しました。 VDI （仮想デスクトップインフラ）、 Microsoft Azure と Office 365 のクラウドサービス、発券システム、リモートサポートシステムなどの主要サービスは、Active Directory と統合され、インターネット経由でアクセスできるようになり、遠隔地のスタッフにも対応できるようになりました。

便利になった一方で、特にパスワード・ハッシュの同期と認証のためのクレデンシャルの使用により、攻撃の対象になってしまいました。攻撃者は、セキュリティレベルの低いシステムを標的にし、特にパスワードベースの認証を悪用し、クレデンシャル・スタッフィング、ブルート・フォース、またはフィッシング攻撃によってユーザ・クレデンシャルを侵害する可能性があります。

さらに、 Microsoft Azure などのプラットフォームでは、条件付きアクセス、ジオロケーション・フィルタリング（アクセスするユーザの地域を限定）、デバイスヘルスなどの高度なセキュリティ機能が提供されていますが、 CSS の他のシステムの多くにはこれらの機能がありませんでした。システム全体で**統一されたセキュリティ管理が行われていない**ため、攻撃者は最もセキュリティレベルの低いシステムを攻撃し、侵害された認証情報を使って攻撃を他のシステムに拡大することが可能になりました。

もう一つの大きな問題は、**パスワードに対する疲労**です。スタッフは、セッションのタイムアウトの度に、また異なる複数のシステムにそれぞれのパスワードを入力してログインする必要があります。この一貫性のなさは、フィッシング攻撃のリスクを高めるだけでなく、パスワード管理の非効率性やスタッフ全体のフラストレーションにもつながっていました。

解決：ウィンマジックの MagicEndpoint の導入

Okta、Duo、Azure MFA （多要素認証）など、さまざまな IdP （アイデンティティ・プロバイダ）を評価した結果、 CSS は、ほとんどの主流製品は、自分たちの懸念に完全に対応していないか、パスワードレス認証ソリューションを実装するために高価な追加のライセンスが必要であることがわかりました。

ウィンマジックの **MagicEndpoint** は、 CSS の全システムでパスワードベースの認証を完全に排除できる数少ないソリューションの一つとして際立っていました。ウィンマジックのチームは CSS と緊密に連携し、トライアル環境を構築し、CSS の既存インフラにシームレスに統合できることを実証しました。

実施プロセス：

導入の際、ウィンマジックのチームは、 DNS の設定、 Firebase や Apple API へのプッシュ通知フローなど、 CSS の設定に関する問題の特定と解決を支援しました。導入直後から認証は非常に合理化されエンドユーザはシステムを使いやすいと感じました。追加で IdP アカウントを作成する必要はなく、ユーザは MagicEndpoint 経由で携帯電話を登録するだけで、シームレスな認証が可能になりました。

影響：セキュリティ強化と IT 管理者の負担軽減

MagicEndpoint の導入によりすぐに改善をもたらしました：

- **パスワードリセット要求が 76% 減少**（一部のアプリケーションはまだ MagicEndpoint に移行前）
- **ユーザアカウントのロックアウトが前年比で 94% 減**
- ユーザアカウント管理が一元化され、より効率的になったため、 **IT 管理者の負担が軽減**
- ユーザ・クレデンシャルやパスワードリセットを必要としないため、 **IT 管理者による認証の問題解決性が向上**

統一されたログインエクスペリエンスにより、アプリケーション間でパスワードが再利用される可能性も大幅に減少しました。パスワードを使用しなければならないレガシー・アプリケーションでは、強力なランダム生成パスワードに置き換えることで（MagicEndpoint のパスワードマネージャー機能）、セキュリティ体制をさらに強化することができます。

効果：セキュリティと効率の向上

MagicEndpoint により、 CSS はクレデンシャルベースの攻撃を防ぐことができ、 IT チームは他のセキュリティ強化に集中できるようになりました。ログインプロセスを合理化し、プラットフォーム間で一貫した認証ワークフローを実現したことで、スタッフのフラストレーションが大幅に軽減され、業務効率が向上しました。スタッフは、オンライン・アクセスにパスワードを入力したり、 MFA を使用したりする必要がなくなったことに驚きました。MagicEndpoint とその “no user action”機能を使い始めてわずか数日後、この新しい自由さに慣れるのに少し時間がかかりましたが、ほとんどのスタッフは、以前の面倒な認証プロセスに戻ることを想像できませんでした。

今後の展望

CSS はウィンマジックの開発者と密接に協力し、迅速な製品改良の恩恵を受けています。MagicEndpoint ソリューションは、 CSS の長期的なセキュリティ戦略の重要な要素であることに変わりはなく、同社は将来の機能拡張と、さらなるセキュリティの強化に期待しています。

推奨：MagicEndpoint による安全な未来

ウィンマジックの MagicEndpoint は、 Microsoft Windows のクレデンシャルベースの認証から脱却を模索している組織に強くお勧めします。パスワードレス認証がクレデンシャル関連の攻撃を防ぐための重要なソリューションであることが業界のトレンドになっていますが、 MagicEndpoint は業界リーダーとして、現代のセキュリティの課題に対処し、継続的に進化するソリューションとなっています。

> “MagicEndpoint はまさに認証の未来を開拓している。 SMS やプッシュ通知のような時代遅れの方法が完全に廃止されるのは時間の問題です。フィッシングや sim スワッピング、その他広く使われている悪質な手法に対して脆弱であることが知られているからです。 MagicEndpoint のテクノロジーは、その「no user action」アプローチと、主要な認証要素としてのクレデンシャルを排除することで、数マイル先を走っている。市場全体が移行していく技術です。”
>
> **- Ian Armstrong - CSS、システム・エンジニア**

ウィンマジックが保護します

ユーザエクスペリエンスを妨げることなくデータを保護するウィンマジックの詳細については、 sales.jp@winmagic.com までお問い合わせください。または www.winmagic.co.jp をご覧ください。

弊社のデータシート、ホワイトペーパー他各種資料は
以下よりダウンロードいただけます

www.winmagic.co.jp/marketing-assets

米国/カナダ：
+1 888 879 5879

欧州/中近東/アフリカ(EMEA)：
+49 69 175 370 530

日本：
03 5403 6950

詳細は、ウィンマジックまでお問い合わせください。