Tech Brief

# VPN サーバへのパスワードレス認証 （RADIUS 連携）

## 課題 / 状況

多くの企業や組織では、 サイバー攻撃の脅威とプライバシー上の理由から、 安全で高度な VPN などのソリューションを利用してデータを継続的に保護しています。 特に現在は、 より柔軟性の高いリモートワークや BYOD （私物端末の業務利用）の導入が求められており、 デジタルセキュリティの一層の強化が不可欠で、 その中でも特に VPN の利用は大幅に増大しています。

そして、 依然として多くの VPN サービスでは RADIUS 認証が利用されています。 しかし、 RADIUS プロトコルは性質上、外部の IdP （ID プロバイダ） や IAM （ID およびアクセス管理） との相互連携が不明瞭なプロトコルとされています。一部の IdP や IAM は RADIUS に対応しておらず、 また、 他の IdP や IAM では、 RADIUS を動作させるため、 多くの複雑な手順を踏んだり、 追加エージェントを利用する必要があります。

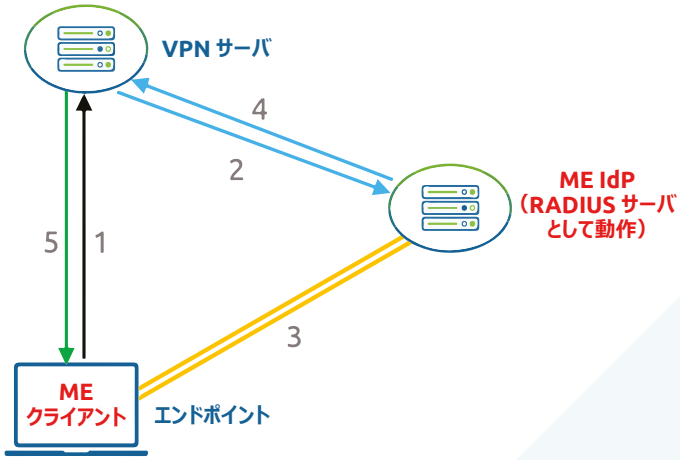
一方で、 企業各社は、 これらの VPN サービスの認証の安全性を確保するため、 通常、 多要素認証ソリューションを利用しています。 多要素認証を利用すると、 脆弱なパスワードの推測や、 データ漏えいを通して取得したパスワードの再利用など、不正アクセスの標準的な攻撃手段から保護できます。 しかし、最近の高度なフィッシング攻撃では、公式のアプリケーションを巧妙に偽装してユーザと動的にやりとりすることが可能なため、 多要素認証の多くのアプローチでは、 保護することはできません。 米国政府はこのような危険性を危惧し、 スマートフォンに搭載されている SMS や OTP、 プッシュ通知、そして一部のパスワードレスソリューションさえも利用を禁止するゼロトラスト戦略 （英語） をこの数年間推進してきました。 このような米国政府が禁止するパスワードレスソリューションは、 ユーザエクスペリエンスの観点では許容されるように見えますが、 エンドポイントの認証が含まれてないため、 認証要求が、 正当かつ意図したエンドポイントから来たものであることを保証できないという 「関連性の問題」 が発生してしまいます。

## 解決策

ウィンマジックの MagicEndpoint は、 耐フィッシングパスワードレスソリューションの 1 つで、 VPN アクセスだけでなく、 RADIUS や他の最新のプロトコルである SAML や OIDC などを利用する他の多くのリモートサービスに適用可能です。 現在のサイバー保険で求められる多要素認証の要件に対応しており、 認証は、 現在の市場で入手可能な最高レベルのユーザエクスペリエンスを備えています。 MagicEndpoint と VPN （RADIUS） サービスを統合することで、 多要素認証によるユーザ認証が可能になり、 ユーザは最小限の操作で、 VPN への認証を実施することができるようになります。

さらに MagicEndpoint はエンドポイントに内蔵された TPM に保存された認証鍵を使い、 RADIUS と連携した VPN サーバと認証を行うため、 他の多要素認証デバイスは必要ありませんし、 ハードウェアレベルのセキュリティ （TPM） で認証鍵を保護するためセキュリティ面でも他の多要素認証よりも強化されます。 また、 MagicEndpoint を使った認証には、 ユーザの知識や本人のみが持ち合わたり、 本人のみが行える固有性は必要ありません。 そして MagicEndpoint が導入されたエンドポイントデバイスは、 ユーザ、 外部の暗号化デバイス、 スマートフォンなどの他の 「要素」 がなくても、 完璧にリモート認証を行うことができます。 MagicEndpoint はさらに、 VPN ログインごとにユーザの意図と、 当該リクエストが確かに正当なデバイスから来たものであることを検証することが可能で、 上記で述べた 「関連性の問題」 を排除することができます。

MagicEndpoint は RADIUS サーバとしても機能するため、 下記の図の通り、 VPN サーバが接続されていれば他のコンポーネントがなくても VPN サービスを構成することが可能です。




1. VPN サーバにリクエストを送信
2. VPN サーバは、 バックチャネルを使用して、MagicEndpoint IdP にリクエストを送信
3. MagicEndpoint IdP は、 エンドポイントをチェックし、 “ユーザ + デバイス” の組み合わせを識別し認証
4. MagicEndpoint IdP は、 バックチャネルを使用して、 VPN サーバに応答
5. VPN サーバは、 “ユーザ + デバイス” に対してアクセス権を付与

**ウィンマジックの MagicEndpoint は、 ユーザのためにエンドポイントを最大限に活用することに焦点を合わせ開発された、非常にセキュアなパスワードレス認証ソリューションです。 ユーザの認証操作や追加の多要素認証デバイス / USB キーが不要なため非常に安全で、 使用にあたってもシームレスで MagicEndpoin が導入されていることを意識する必要がありません。**

2022 年 10 月 26 日

**認証し、 暗号化し、 成し遂げる。**

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、 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。