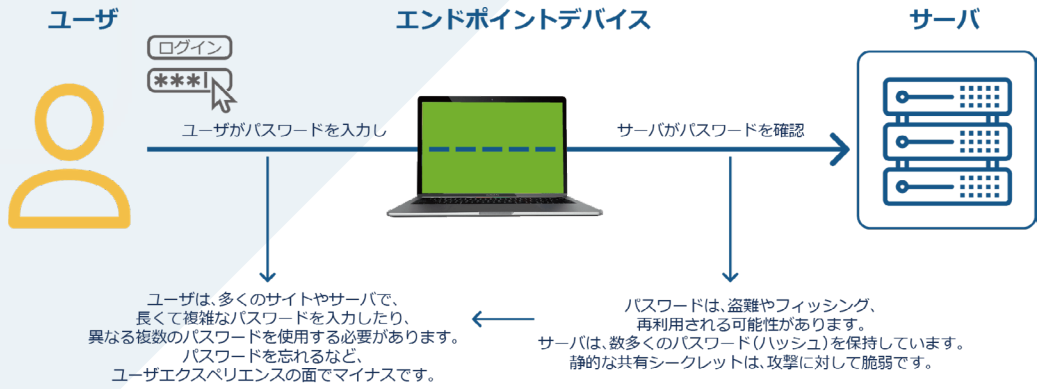
Product Brief

MagicEndpoint FIDO Eazy

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、パスワード侵害や脆弱性、盗難が原因であると報告されています。たとえ長くて複雑なパスワードを設定してもフィッシングやパスワードに対する攻撃に対して効果的であるとは言えません。また米国政府は、 政府機関に対して 2023 年 1 月までに従来の多要素認証の使用を中止し、フィッシング耐性のある多要素認証の使用を開始するよう義務付けています。MagicEndpoint FIDO Eazy はこれらの問題を解決する FIDO アライアンスの認定を受けたパスワードレス認証ソフトウェアです。

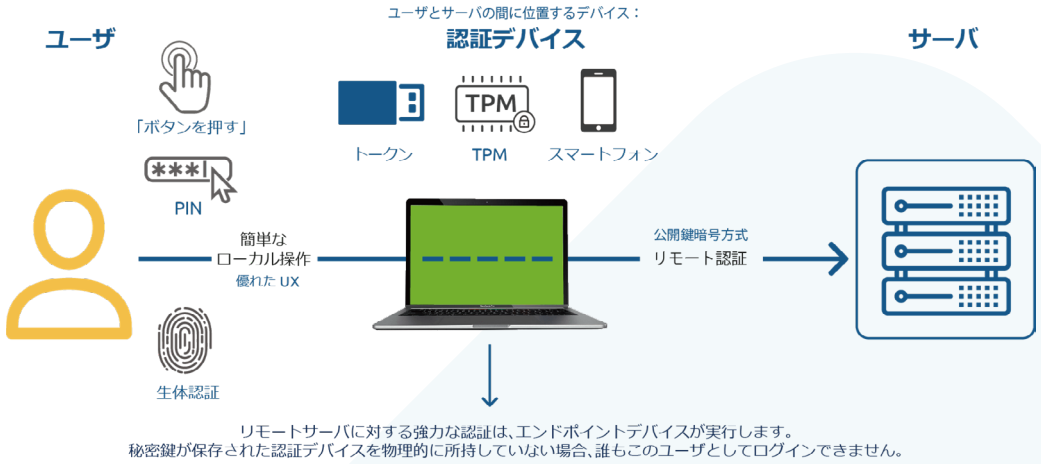
従来のユーザ名とパスワードを使った認証

ユーザがパスワードを入力し、サーバがパスワードを確認します。認証はユーザとサーバ間で行われます。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長さや複雑さに関係なく、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ユーザになりすましサーバにアクセスできます。



MagicEndpoint FIDO Eazy によるパスワードレス認証

ユーザはエンドポイントデバイスにログインするだけです。リモート認証はユーザの代わりにエンドポイントデバイス上の MagicEndpoint FIDO Eazy とサーバ間で行われます。MagicEndpoint FIDO Eazy は公開鍵暗号方式を用いてサーバとの間でリモート認証を実行します。公開鍵暗号方式で使用する秘密鍵は、エンドポイントデバイスの TPM、ソフトウェアトークン、スマートカードやハードウェアトークン、Bluetooth 接続したスマートフォンに保存することが可能です。攻撃者は秘密鍵が保存された認証デバイスを物理的に保持しければサーバにアクセスできません。

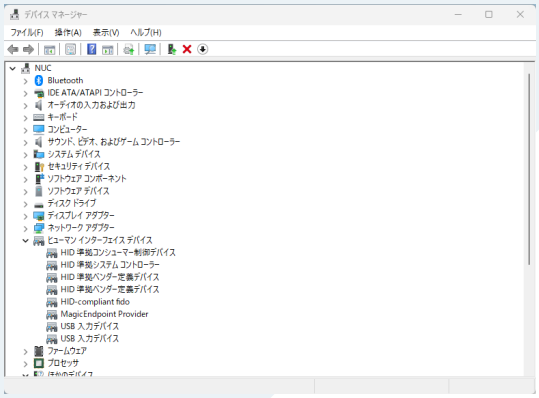


認証し、暗号化し、成し遂げる。

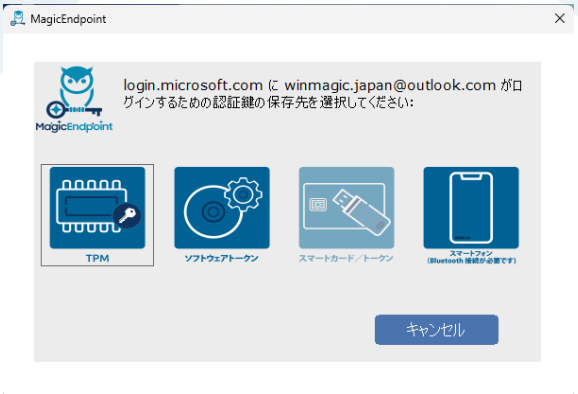
MagicEndpoint FIDO Eazy の特徴

特徴 1 MagicEndpoint FIDO Eazy は FIDO2 準拠のソフトウェアトークンです。MagicEndpoint FIDO Eazy をインストールすると、MagicEndpoint Provider がヒューマンインターフェースデバイスとして登録されます。(図 1)

特徴 2 MagicEndpoint FIDO Eazy は 公開鍵暗号方式を用いてサーバ認証を実行します。公開鍵暗号方式で使用する秘密鍵は、エンドポイントデバイスの TPM、ソフトウェアトークン、スマートカードやハードウェアトークン、Bluetooth 接続したスマートフォンに保存することが可能です。(図 2) ＊セキュリティを最重視する場合、TPM に保存することを推奨します。



(図 1)



(図 2)

特徴 3 ユーザは MagicEndpoint FIDO Eazy へのログインやサーバ認証に PIN を使用できます。(図 3)

特徴 4 MagicEndpoint FIDO Eazy へのログイン方法やサーバ認証時に生体認証を実行するなど、様々な設定が可能です。また、ソフトウェアトークンのインポートやエクスポートが可能です。(図 4)

(図 3)

(図 4)

特徴 5 Web サイトや SaaS 上で MagicEndpoint FIDO Eazy を使用した認証を登録する際の自動登録機能を備えています。(現時点でメジャーな Web サイトや SaaS 約 100 サイトに対応)

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 MagicEndpoint が導入されていることを意識する必要がありません。

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。