Whitepaper

SecureDoc™ by WinMagic

注目を集める「パスワードレス認証」、ソリューション選択のポイントとは？さらなるセキュリティ強化の鍵は「デバイスの保護」と「一元管理」

WINMAGIC®

SecureDoc by WinMagic

注目を集める「パスワードレス認証」、ソリューション選択のポイントとは？ さらなるセキュリティ強化の鍵は「デバイスの保護」と「一元管理」

テレワークの普及やSaaSサービスの活用増加、およびデジタルトランスフォーメーション（DX）に向けたIT基盤の急速なクラウド化を背景に、社内外の境界を超えたアプリケーションやサービス、データへのアクセスが頻繁に行われるようになっています。

そうした中、セキュリティのさらなる強化が企業にとって喫緊の課題となっており、特に見直しを迫られているのが、セキュリティ技術が高度化した現在においても、本人認証の核として使われている従来からのパスワードに頼った本人認証の仕組みです。

なぜ、従来のID/パスワードによる本人認証では増大するセキュリティリスクに対処できないのか、また、その課題解決の手段として注目を集めている「パスワードレス認証」とは一体どのようなものなのか？そして、市場では様々なパスワードレス認証ソリューションが存在する中、どのようなポイントを考慮し、選択すればよいのか、本書では詳しく解説していきます。

情報漏洩発生の 6 割はパスワードの流出や脆弱性が原因

すべての企業にとって最も危惧されるセキュリティインシデントが「情報漏洩」であることは、間違いありません。長らく企業は情報漏洩対策にあらゆる手段を講じてきました。

しかし、その脅威は留まることを知らず、今もなお、マルウェア感染やサイバー攻撃による個人情報や機密情報の流出が頻発しています。特に近年では、働き方改革の推進と新型コロナウイルス感染拡大防止に向けたテレワークの利用拡大や、企業のパブリッククラウドサービスの利用増加に伴い、社内外を問わず、どこからでも業務に必要な情報やアプリケーション、サービスにアクセス可能な環境が実現されています。その一方で、情報漏洩のリスクも拡大し、今まで以上にセキュリティ対策の更なる強化が急務となっています。

中でも、喫緊の課題となっているのが、従来のパスワード認証に起因するセキュリティリスクへの対処です。米ベライゾン社が昨年発表した「2021年度ベライゾン データ漏洩／データ侵害調査報告書」（DBIR）によれば、ハッキングに関連する情報漏洩の原因の61%は、ID/パスワードといったユーザ認証に用いられるクレデンシャル情報の盗難や漏洩、および、その脆弱性に起因すると示されています。事実、攻撃者は、フィッシングやネットワーク通信中の情報傍受、サービス提供側のサーバへの攻撃等、様々な経路からユーザが使用しているパスワードを容易に入手し、社内システムや利用しているクラウドサービスに入り込み機密情報を盗み出しています（図1）。

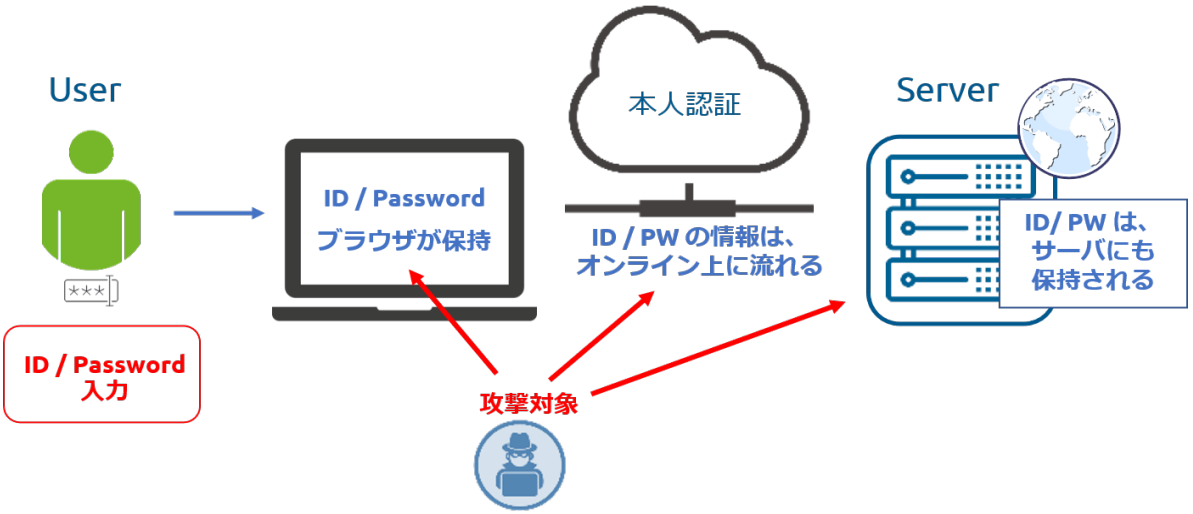


図1　従来型のID /パスワードは簡単に攻撃者に盗まれ、情報漏洩発生の原因となりかねない

このようなパスワードの盗難や漏洩を防ぐため、長くて複雑なパスワードを設定する、有効期限を設定する、といったパスワードポリシーのガイドラインの作成や対策を実施している企業は多いと思われます。しかし、サイバー攻撃の巧妙化・複雑化によって、従来の対策だけでは対応しきれなくなってきています。加えて、これらのパスワードに関するセキュリティ対策は、ユーザやシステム管理者に多大な負担を強いています。ユーザは複雑なパスワードを都度入力するのが面倒なため、Webブラウザー上にID/パスワード情報を保存しているケースが多々見受けられます。また、同様に、利用しているクラウドサービスごとに異なるパスワードを設定することなく、同じパスワードを使い回しているユーザも少なくありません（図2）。

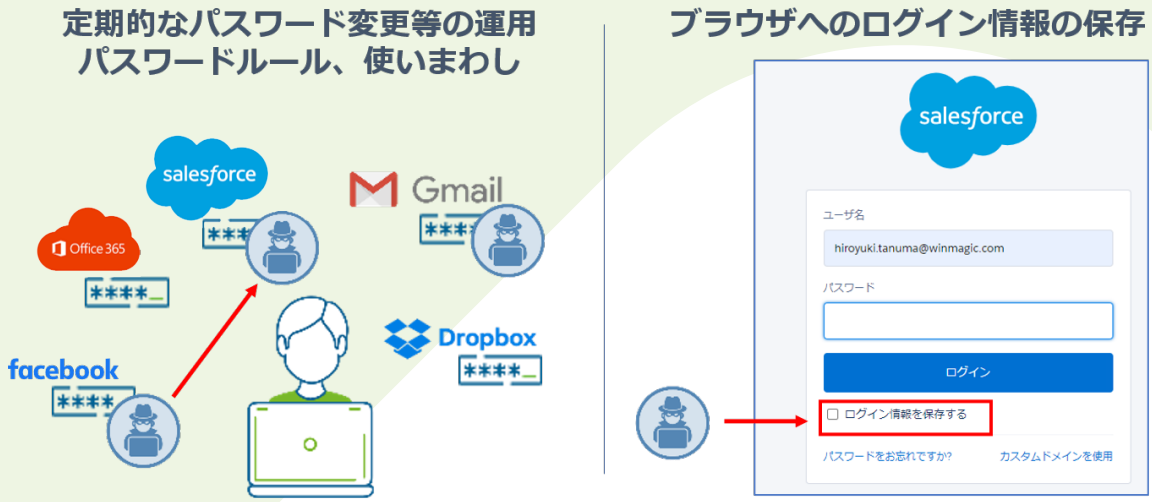


図2　従来型パスワード運用での問題

その一方で、システム管理者も、ユーザのパスワード管理に苦慮しています。
パスワードの使いまわしを防ぐために、サービス毎に異なるパスワードルールを設定・運用することは現実的には難しく、ユーザの意識に委ねられてしまう。パスワードルールを複雑なものに変更すると、ユーザからのパスワード忘れに対する問い合わせが増えてしまうなど、対応に手を煩わされているのではないでしょうか。

従来のパスワード運用に大きな変化
政府機関、SaaSベンダーも方針転換

このようなパスワードに関する諸問題に対して、その運用方法に変化が見られ始めています。2017年に米国国立標準技術研究所（NIST）が発表したガイドラインでは、「サービス提供側はパスワードの定期的な変更を要求すべきではない」という内容が示されたほか、米国政府もゼロトラスト戦略として、「特殊文字と定期的なパスワードローテーションは実際の使用においてパスワードを弱体化せるものであり、連邦政府が採用すべきではない」との見解を示しています。

国内でも2018年3月に総務省が「国民のための情報セキュリティサイト」を改訂、「パスワードの定期的な変更は不要であり、その流出時には速やかに変更することが必要」との提言を行っています。

政府機関だけでなく、サービス提供側でも、パスワードの運用に関する方針転換が見られます。その一例が米セールスフォースドットコムで、同社のSaaSソリューションへのアクセスに際して、2022年2月1日から従来のID/パスワード方式ではなく、 MFA （Multi-Factor Authentication：多要素認証）の使用を必須条件とすることに決定しました。

今後は他のSaaSベンダーも追随していくことが予想されます。

MFAの方法には、SMSやワンタイムパスワードを発行するアプリを使った認証などがありますが、昨今ではSMSインターセプトやSIMスワップなど、機器間の通信の内容を傍受するサイバー攻撃である中間者攻撃（Man In The Middle Attack）による被害も発生しており、MFAを導入していれば一概に安全とは言い難くなってきています。

これらのことから、2022年1月26日、米国行政予算管理局（OMB）は、行政命令14028「米国国家サイバーセキュリティ改善」に対応するためのゼロトラスト戦略として、SMSを利用したワンタイムパスワードやスマートフォンの認証アプリケーションへのプッシュ型通知によるMFAでは、フィッシング攻撃を防げず、米国政府の要件に準拠しないことから利用を中止するよう要請しています。

注目されるパスワードレス認証
その実現のための規格「FIDO 2」とは？

こうした背景から、昨今、次世代認証技術として脚光を浴びているのが「パスワードレス認証」です。その名が示すように、パスワードに依存しないユーザ認証を行う方法で、先に述べたパスワードの紛失や盗難、傍受といったインシデントの発生を未然に防ぐことができます。このパスワードレス認証の中でも今後の主流になると目されているのが、認証規格「FIDO（Fast Identity Online）」です。

新しいオンライン認証技術の標準化を目的として発足した非営利団体の「FIDOアライアンス」では、サーバとユーザの認証を切り離して、ユーザのデバイスを「認証器」としてユーザ認証を行い、サーバとの認証を連携する方法を規定しています。認証器を使うことで、サーバ側はパスワードを管理する必要がなくなります。

ユーザはパスワードに頼らず複数のサーバにアクセスできるようになり、サイトごとに複数のパスワードを覚える必要もなくなります。

パスワードを使わずに本人の確認をおこなう仕組みは他にもありますが、サーバからユーザの認証を切り離すFIDOの技術を使うことで、より安全で強固な認証が行えるようになります。

FIDO は前述の米国政府のゼロトラスト戦略において、フィッシング攻撃を防ぐことができる認証方式として認められています。

2013年に最初のFIDO規格が発表され、現在ではFIDO 2が最新規格となっています。

FIDO 2は、W3CのWeb認証仕様（WebAuthn）とFIDOアライアンスのデバイス間連携仕様（CTAP）から成る技術仕様で構成されており、主要なブラウザーがWebAuthnに対応したことで、Webブラウザーを通じたオンラインサービスへの安全なログインが実現できるようになりました。またFIDOでは、ID/パスワードによる認証とPINや生体認証の組み合わせといった、2要素認証も規格化しています。

2要素認証を使うことで、より厳密な認証が可能となります。

FIDO 2を用いた具体的な認証の仕組みについて見ていきましょう（図3）。

FIDO 2に対応し認証器として動作するMagic Endpoint をインストールしたパソコンで、ログイン先のSaaS等でFIDO 2による認証の設定を行うと、Magic Endpoint は秘密鍵と公開鍵を作り、公開鍵をサーバ側（サービス提供側）に渡します。一方、秘密鍵は、ユーザ側でのみ保持します。FIDO2の設定が完了したSaaS 等にログインする際、サーバは認証器での認証結果を要求します。ユーザはMagic Endpoint でPIN コードを入力し、本人認証に成功すると、Magic Endpoint は、認証結果に秘密鍵を使って電子署名し送り返します。サーバ側で、秘密鍵とペアの公開鍵で復元できれば、ユーザを特定できるためログインを許可します。

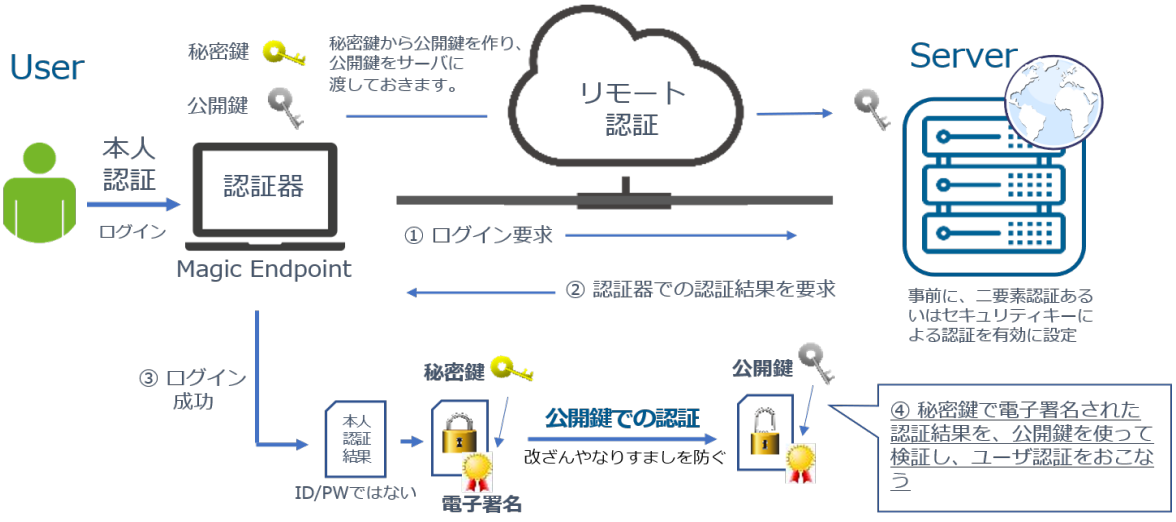


図3　FIDO2を用いたパスワードレス認証の仕組み（Magic Endpointを使用した場合）

一元管理、安全な保護機能により、
更に強固なパスワードレス認証を実現する「Magic Endpoint」

ID/パスワードによる資格情報に頼らない認証の仕組みにより、改竄やなりすましを防ぎ、情報漏洩に繋がる課題を解決することができますが、FIDO 2の実運用において、考慮すべき事項が2つあります。それは「秘密鍵の保護」と「認証器の保護」です。

FIDO 2の認証には「公開鍵」「秘密鍵」の二種類の鍵がセットとして用いられますが、秘密鍵はユーザだけが保持するもので、セキュリティを担保するうえで秘密鍵の保護を完全におこなうことが実運用において重要になります。

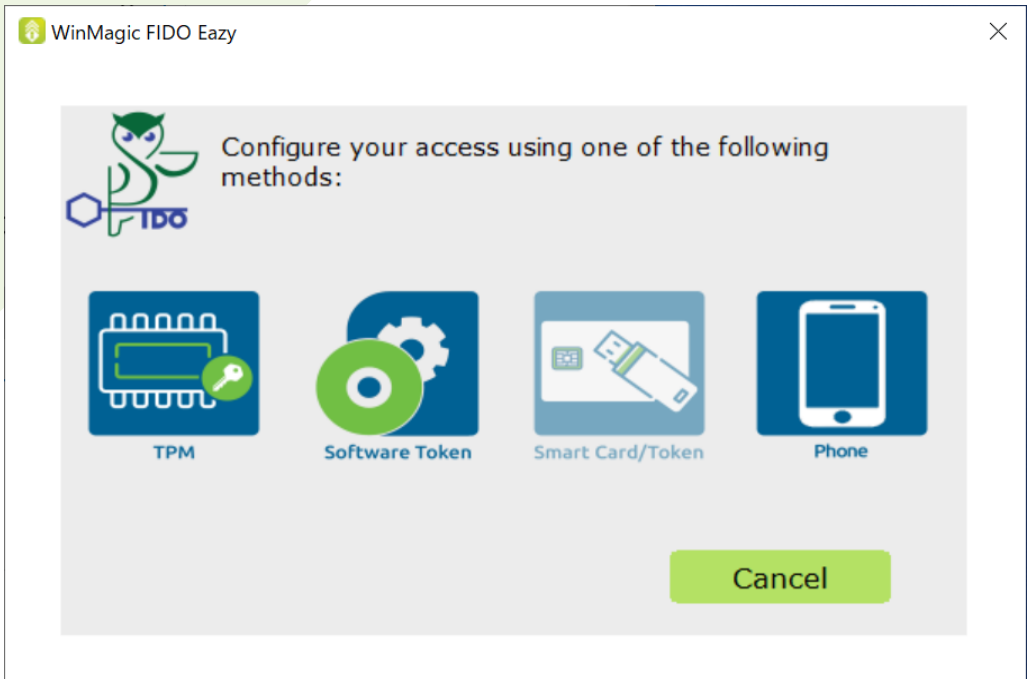
また、認証器がインストールされたパソコンを紛失、或いは盗まれた場合、そのままでは認証器自体は保護されていないため、第三者がPIN入力を行うことで本人認証に成功してしまうリスクも生じます。PINは、パスワードと異なりデバイスと紐づけられることからユーザの利便性を考慮し、多くの場合、PINコードには複雑さを要求しないポリシーとする場合が多く、簡単に認証が行われてしまう可能性があります。

これらの課題を解決するのが、ウィンマジックの「Magic Endpoint」です。

他の方法とは異なり、Magic Endpointでは、Windows10/11のBitLocker でも用いられるセキュリティチップ「TPM(Trusted Platform Module)」内に秘密鍵を保護することができます。

TPMのタンパープロテクション機能により、もしマルウェアに感染した場合でも、マルウェアによって秘密鍵を盗み出すことはできません。FIDO 2による認証が設定されているサイトへのログイン認証には、認証器と秘密鍵が必要なため、攻撃者はその両方がなければサイトに不正アクセスすることは許されず、情報漏洩を防げます。なお、本人認証の方法は、PIN入力の他、生体認証を使用することも可能です。

それ以外の認証方法として、iPhoneアプリの「WinMagic Authenticator」を併用した本人認証も可能です（画面1）。



画面1 TPMで秘密鍵保護の他、スマートフォン（iPhone）も選択可能

Magic Endpointがインストールされたパソコンとスマートフォンアプリの「WinMagic Authenticator」の両方を利用する方法で、これによりPCを複数のユーザで利用する環境にも対応できるので、普段使っているパソコン以外のパソコンから本人認証を行いSaaSやアプリケーションにアクセスすることも可能です。（図4）

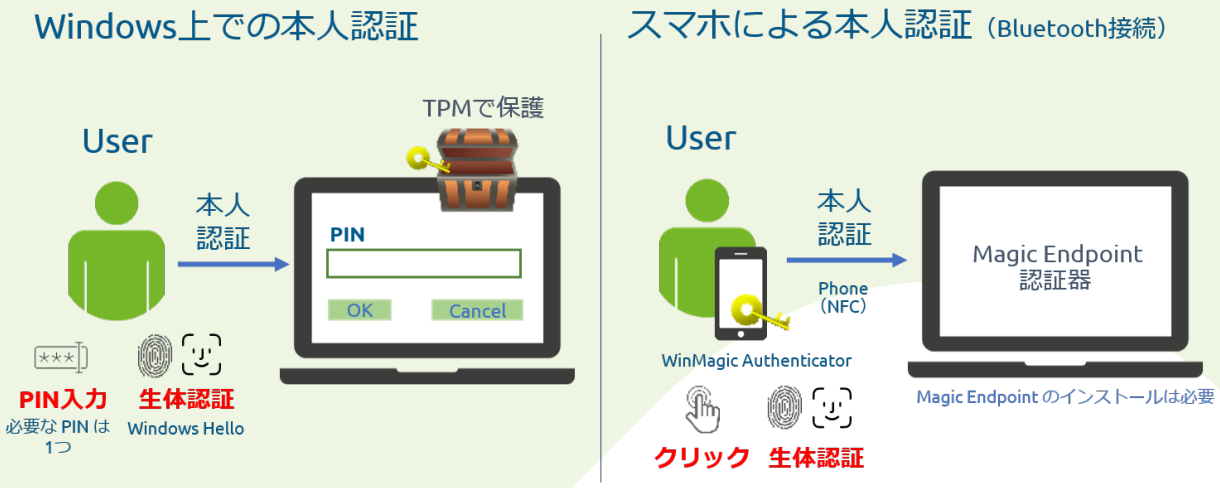


図4　PIN入力や生体認証のほか、スマートフォンアプリを用いた本人認証も可能

もう一つの大きな優位性は、ウィンマジックがセキュリティ市場で高い実績を培ってきたディスク暗号化ソリューション「SecureDoc Disk Encryption」との連携により、より強固なデバイス保護を実現できることです。上述したように、紛失や盗難に遭ったパソコンは、第三者がPINチャレンジをした場合、簡単に本人認証を成功してしまう恐れがあります。

そうしたリスクを回避するために有効となるのが、ディスク暗号化です。

SecureDoc Disk Encryptionは、SecureDocによるソフトウェア暗号の他、BitLockerもサポートしており、パソコン電源投入後のWindows OS が起動する前に、ユーザ認証を求めるプログラム（プリブート認証）が起動します。

プリブート認証でのユーザ認証に成功しなければWindowsが起動しないため、Magic Endpointによる本人認証のためのPIN入力そのものが不可能となります。プリブート認証ではデバイスの保護のために、パスワードの誤入力回数に基づいてアカウントをロックさせることも可能です。

一元管理によって運用負荷を抑制
エンドポイントセキュリティの強化に向けさらなる進化を目指す

FIDO認証の運用を効率化する機能が用意されていることも、Magic Endpointのポイントです（図5）。
SecureDoc Enterprise Serverにより、PIN ポリシー設定やリカバリ、秘密鍵のバックアップ、レポート機能の提供等、Magic Endpointを集中管理できます。

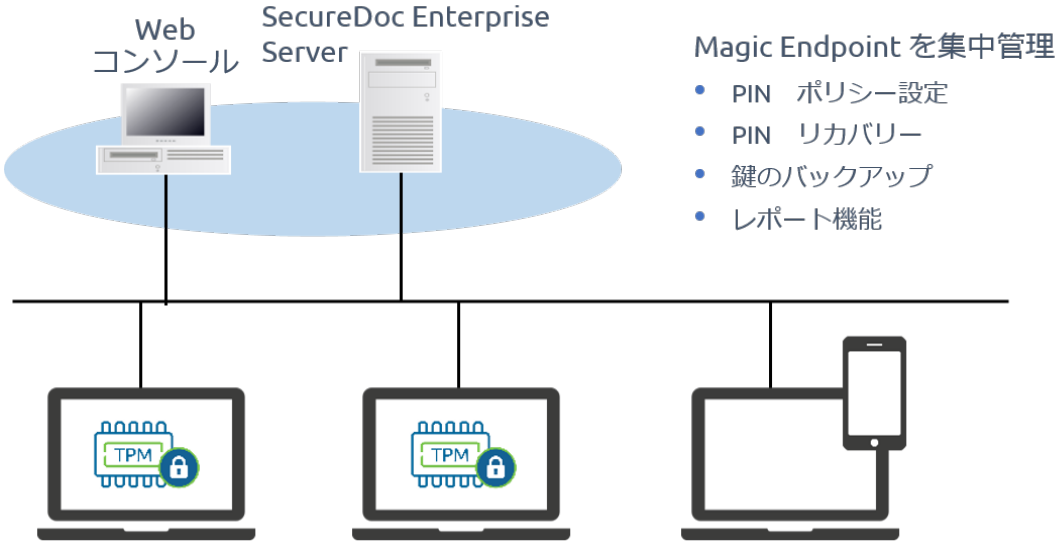


図5　SecureDoc Enterprise ServerによりSPAの統合管理を実現

更に、先に述べたディスク暗号化機能のSecureDoc Disk EncryptionとMagic Endpointを併用すると、プリブート認証からMagic Endpointまでの認証をシームレスに実現することが可能です。

プリブート認証、Windowsサインイン、Magic Endpointへのログインを SSOに設定することができるので、ユーザはプリブート認証でログインに成功すると、SSOの機能によりWindowsへのサインイン、Magic Endpointへのログイン操作を省略できます。(図6)

図6 シングルサインオン (SSO) 機能

更に、SecureDoc Disk Encryptionがインストールされたデバイスのユーザは、SecureDoc Enterprise Serverの機能の1つであるWinMagic IdPを使用することができ、SAML認証をサポートしているサイトへのログインを簡略化できます (図7) 。

SaaSなど、サービス提供側のポリシーで2要素認証 (U2F) を必要とする場合でも、ユーザは、認証のアクションを一切起こすことなく (ID、パスワード、2要素認証情報の入力なしに) ログインでき、エンドユーザに利便性の高いシステムを提供できます。また、ユーザが認証のアクションを一切起こさないことにより、ユーザのアクションが脆弱性の原因になってしまうリスクを防ぐことができます。

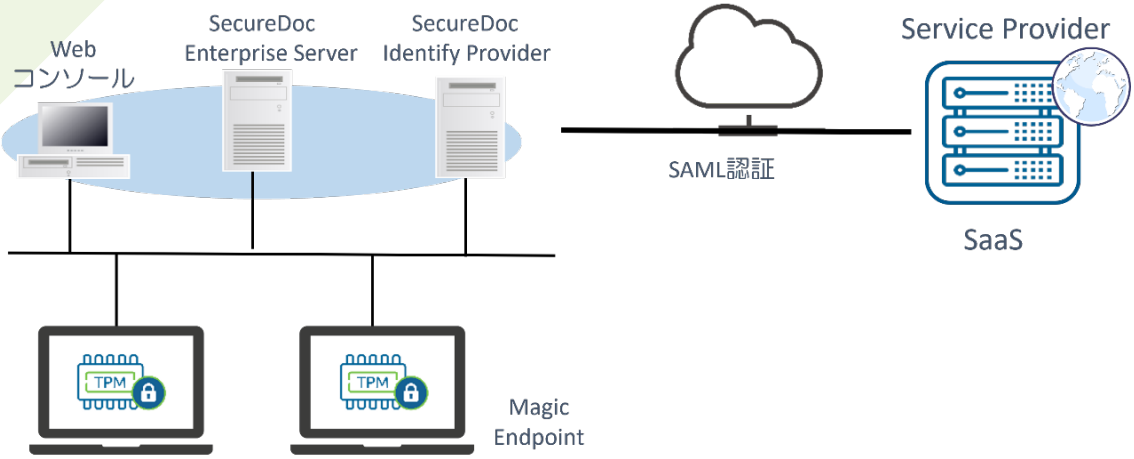


図7 WinMagic IDP

SecureDoc Disk EncryptionについてもSecureDoc Enterprise Serveで一元管理が行えるため、統一されたポリシーでの管理が実現可能です。これにより、パスワードレス認証とデバイスの暗号化に関する運用負荷を軽減できます。

これまで説明してきたように、セキュリティの強化によって機密情報の漏洩を防ぐとともに、ユーザの利便性とシステム管理者の運用性向上を実現するため、パスワードレス認証(Magic Endpoint)は最有力手段となるものです。その導入を検討しているのであれば、ぜひ一度、ウィンマジックにお声がけください。

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
sales.jp@winmagic.com | www.winmagic.com/jp