「パスワードを忘れた」「アカウントロックがかかった」でもう悩まない

# 注目の“パスワードレス認証”でオンプレ・クラウドにセキュアなアクセスを

Falcon System Consulting

TRUST & INTEGRITY

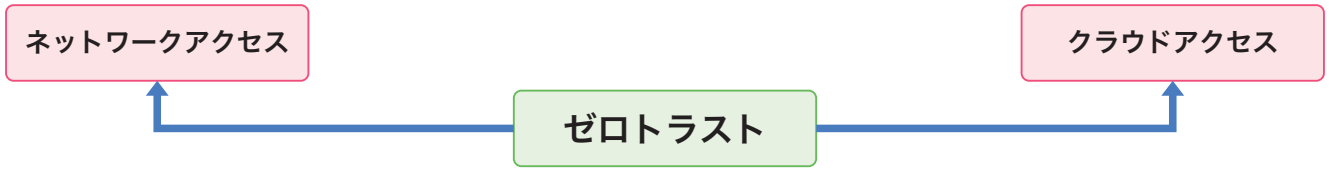
# テレワークの拡大で変化するネットワークセキュリティ

テレワーク利用が拡大する中、企業のネットワークセキュリティは、外部の脅威から社内システムを守るという従来の考え方からの脱却が求められている。ポイントは、すべてを信用しない「ゼロトラスト」という考え方。そのため、アクセス制御の重要性が増大している。さらに、外部クラウドサービス利用の増加に伴い、異なる環境にある複数のシステムのシームレスで安全な利用が、業務生産性に大きく影響するようになっている。

一方で、クラウドサービス活用によって社員が利用するID/パスワードの数は増加傾向にあり、アカウントの個人管理は限界にきている。パスワードが覚えられずアカウントロックがかかって業務がストップしたり、漏えい時に被害拡大につながりかねないパスワードの使いまわしが増加したり、問い合わせ増大やパスワードの発行/失効管理によってシステム部門の負荷が増大するといった問題が起きているのだ。

## ● テレワークによって変化するパスワード管理

### テレワークによってパスワード管理に変化が！




**問題発生・・・パスワードを忘れた。アカウントロックがかかった**

- **利用者のストレス**・・・・・・・・ パスワードが増えた。システム毎に異なるパスワードを覚えるのは面倒。
  定期的変更が面倒。テレワークでの利用が不安。
- **システム管理者への負荷**・・ クラウド増加によるセキュリティ対策の検討。
  パスワードの発行、失効管理の負荷。アカウントロックやパスワード忘れの問合せが増えた。

**利用者にパスワードを意識させないシステムは？でもセキュリティ対策はしっかりと行いたい。**

# 容易に生体やデバイスによる多要素認証を実現するFIDO

前頁のような課題に対し、セキュリティと使い勝手の両立を目指す「FIDO認証モデル」が注目されている。FIDOとはFast IDentity Onlineの略語で、従来のパスワードにとって代わる認証技術。今後業界標準になるとみられている。

FIDO2対応の「認証器」を使えば、指紋・顔認証などの生体認証、スマートフォンやYubiKey等のUSBトークンを使った認証などが利用でき、システム認証からパスワードを無くすことが可能。パスワードを覚える、定期的に変えるといった煩わしさからユーザーを解放する。そもそもパスワードがないので、流出によるハッキングの心配もない。

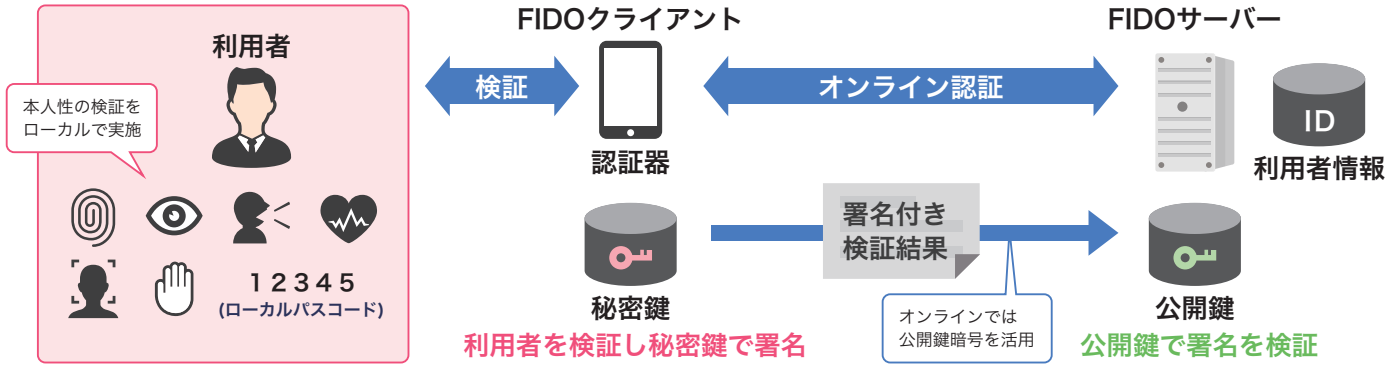
本人確認は認証器が行い、認証サーバーには認証器が生成した公開鍵だけを登録するため、認証サーバーには生体情報などの認証情報が送られることもない。

なお、ファルコンシステムコンサルティングは2021年1月にFIDOアライアンス(※)に加盟し、テレワークにおけるセキュリティ対策への更なる貢献を目指している。

（※）生体認証などを利用した新しいオンライン認証技術の標準化を目指して2012年7月に発足した非営利団体。

## ● 安全性と利便性を兼ね備えたFIDO認証モデル

### FIDO認証モデル（端末とサーバーで秘密を共有しない）




**利用者が「認証器」（Authenticator）に適切な秘密鍵を保有することを確認（検証）することによって認証を実現しており、認証器の簡単な操作だけで多要素認証が可能。**

# 簡単に強固な多要素認証を実現するWisePoint 8

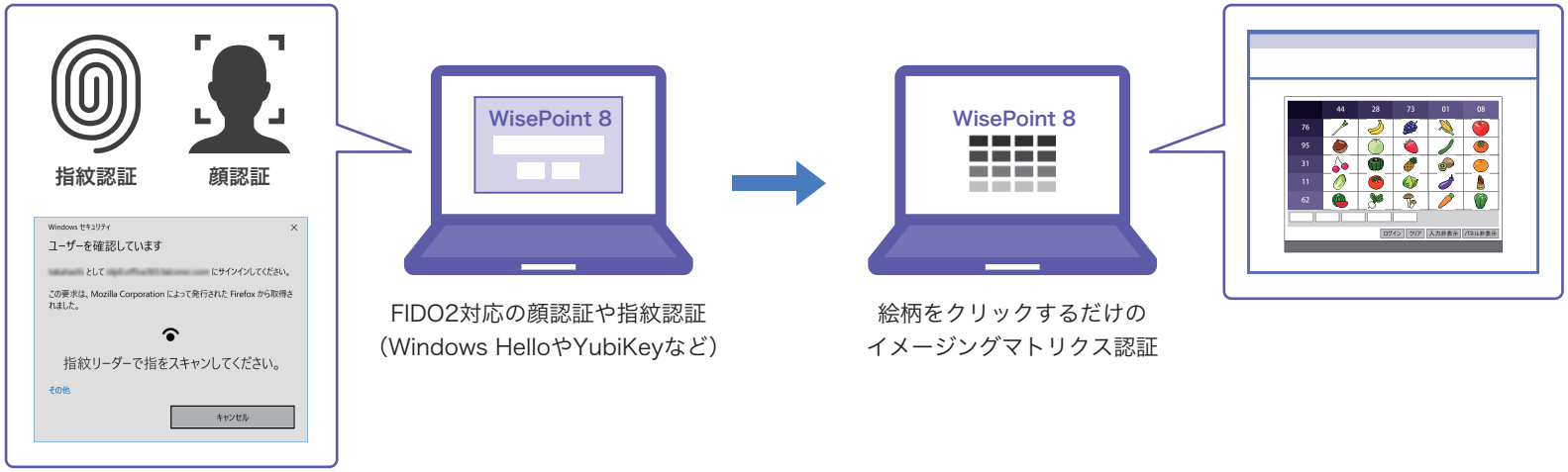
WisePoint 8は、パスワードレスでシングルサインオン（SSO）を実現する認証基盤システムだ。FIDO2対応のWindows HelloやYubiKeyなどの生体認証、スマートデバイス端末認証、パスワードを使用しないイメージや乱数表を用いたWisePointの認証を組み合わせることで、安全に簡単に本人認証ができる。認証方式のバリエーションが多いため、好みの方法を選択可能。サービス単位で認証方式を変えるなど、多段階認証も行うことができる。

ユーザーはパスワードを覚える必要がなく、どこからでも安全にシステムを利用できる。いずれの方法も登録は簡単でユーザー本人がセルフサービスで行うため、管理者はパスワードの発行や失効などの管理が不要に。問い合わせ対応も大幅に削減でき、管理負担が軽減する。

## ● WisePoint 8のパスワードレス認証

### パスワードレスでSSO

Windows Helloとイメージングマトリックス認証の組み合わせによる多要素認証とシングルサインオン



# シングルサインオンでシームレスなシステムアクセスを実現

WisePoint 8はシングルサインオンも実現する。

異なるインターネットドメイン間でユーザー認証を行うための標準規格「SAML2.0」に対応するクラウドサービスはもちろん、SAML2.0未対応の社内システムも、シングルサインオンで利用可能。例えばWindowsログオンが成功すれば、その後の認証をスキップすることもできる。

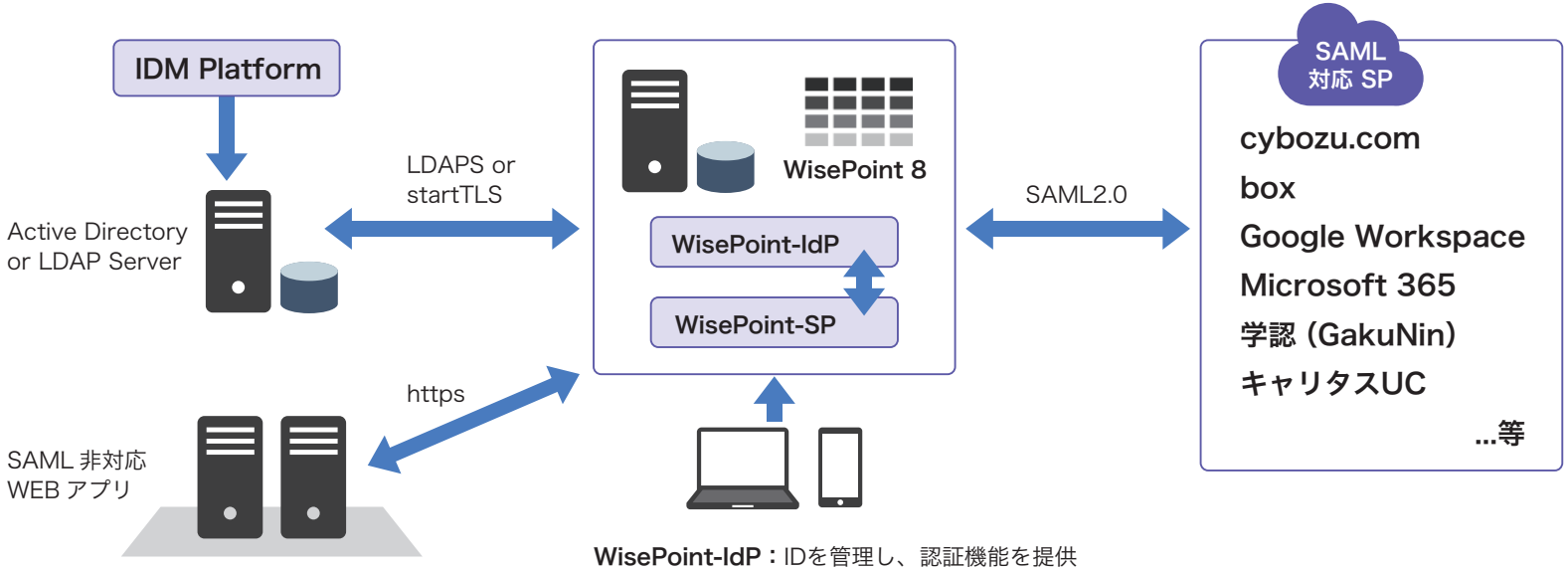
アプリケーションやサービスごとに認証することなくシームレスに利用できるので、ユーザーは複数のシステムをまたがった作業をする場合でも、システムの壁を意識することなく作業ができ、生産性向上にも寄与する。

## ● ユーザーと管理者の複数パスワード管理に関する負担を軽減

**多彩な認証方式と**
**シングルサインオンでセキュリティ強化**

**WisePoint 8**

WisePoint はセキュリティと利便性を両立した認証基盤システムです。
多彩な認証方式でゼロトラストモデルにおいて重要となる「認証」を強化し、
各種クラウドサービスへの「シングルサインオン」で
ユーザーと管理者の複数パスワード管理の負担を軽減します。




**WisePoint-IdP**：IDを管理し、認証機能を提供
**WisePoint-SP** ：リバースプロキシサーバ。WebアプリのSSO機能を提供

# テレワークのセキュリティ対策と利便性を両立する利用例

テレワークでの安全で便利な利用例を紹介しよう。PC、スマートフォン、タブレットなど様々なOSを利用した各種デバイスから、社内システムやクラウドサービスなど、あらゆるアプリケーションに安全にアクセスできる「VMware Workspace ONE」と、WisePointの認証を連携。自宅や外出先から社内システム（仮想デスクトップ環境）へ接続する際は、社内で行う認証に別のパスワードレス認証を加えることで、よりセキュリティを強化できる。この認証連携は、Citrix Workspaceでも利用可能。テレワークのセキュリティと利便性を両立できる。

## ● VMware Workspace ONEとWisePoint 8の認証連携ソリューション

### 事例　官公庁　テレワーク時のセキュリティ対策と利便性の両立

**課題・問題**

- テレワーク環境から庁内システムにアクセスする際のセキュリティ製品を検討
- VMware社のVDIと連携が取れる認証製品を探してた
- 職員が利用し易い認証方式

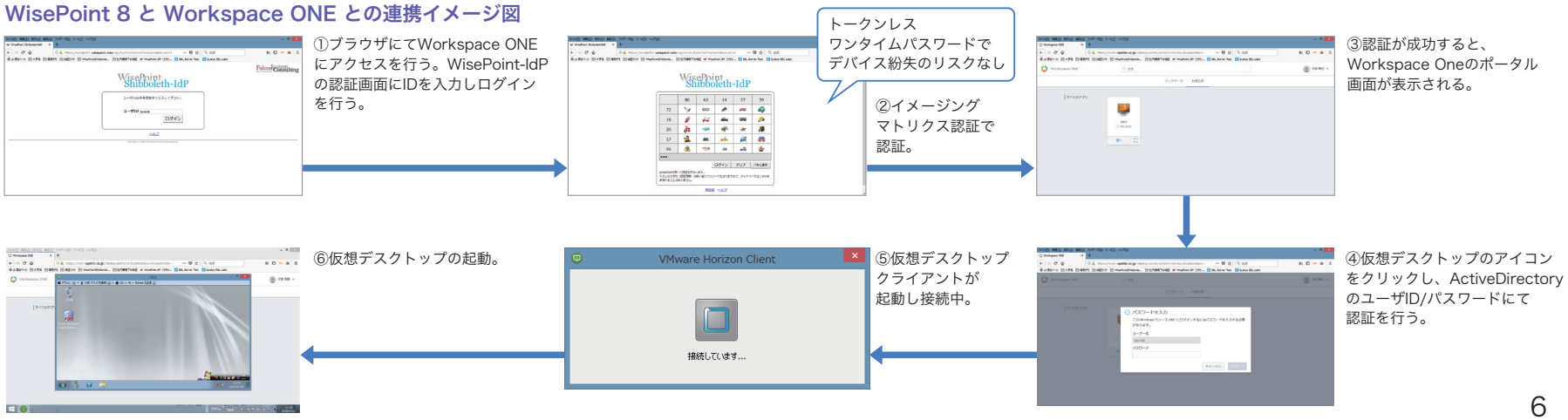
→

**導入の効果**

- 自宅、庁内からも同レベルのセキュリティを実現
- 情報リテラシーのレベルを問わない簡単な認証（イメージングマトリクス認証）

**■VMware社「VMware Workspace ONE」と、WisePoint 8の認証連携ソリューション**
**■自宅や外出先から社内システム（仮想デスクトップ環境）への接続時は認証強化でセキュリティ確保**

### WisePoint 8 と Workspace ONE との連携イメージ図



# モバイルデバイスからの安全で便利なクラウドサービス利用事例

ある運輸業では、現場業務でもシステム活用ができるよう社員にiPadを配布し、Google Workspaceを利用している。その導入にあたって、複数のセキュリティ製品を検討した結果、WisePoint8を導入した。

ポイントは、タップするだけの簡単な認証でクラウドに安全にアクセスできること、数十社のグループ会社を含めたマルチドメイン環境で、各社ごとに異なる認証ポリシー管理ができることだ。WisePointの忘れにくく簡単なイメージマトリクス認証を採用することで、ユーザーの負担を軽減し、管理者へのパスワード問い合わせが激減。管理部門の負担軽減にもつながった。

## ● マルチドメインでの認証管理システム事例

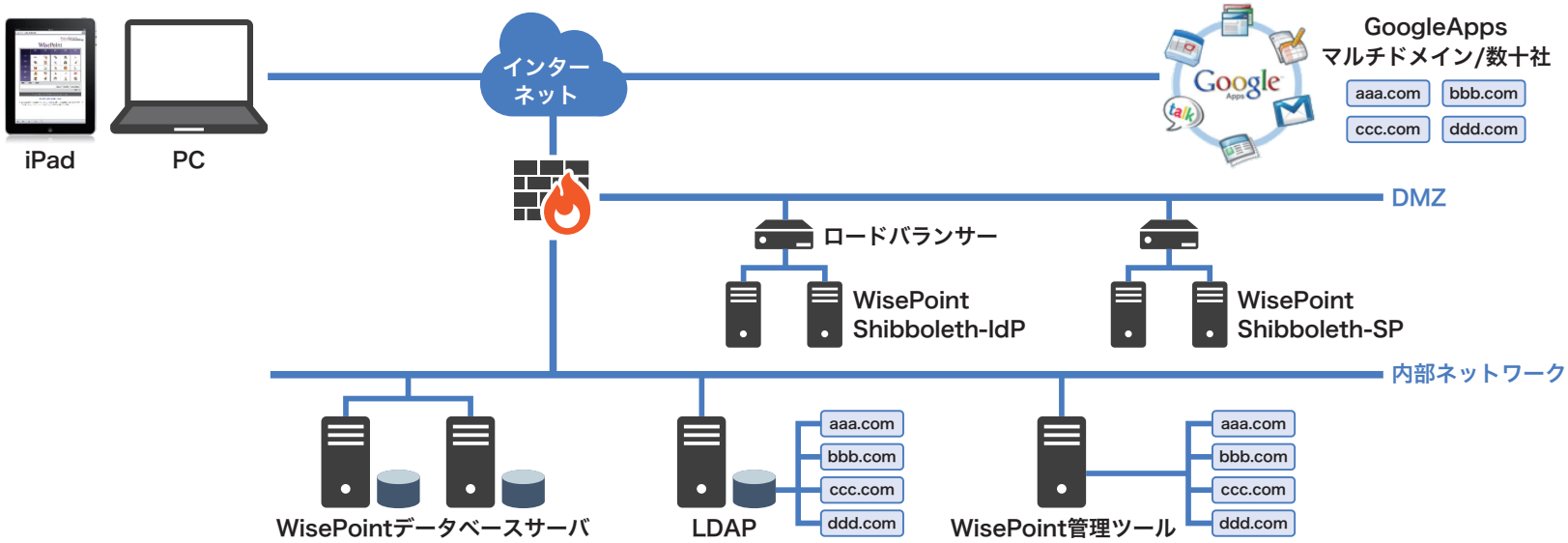
### 事例　某運輸業　モバイル/クラウドサービス

**課題・問題**

- GoogleAppsとiPadの導入に際して、セキュリティ製品を検討
- 数十社のグループ会社全体での利用

**導入の効果**

- モバイルからクラウドへ安全にアクセス
- タブレットでタップするだけの簡単な認証（イメージングマトリクス認証）
- ユーザからのパスワード問い合わせが減少
- グループ会社単位で認証ポリシーの個別管理を実現



## お問い合わせ

**ファルコンシステムコンサルティング株式会社**

〒104-0033

東京都中央区新川 1-16-3　住友不動産茅場町ビル

TEL:03-6228-3220　FAX:03-6222-8597

https://www.falconsc.com/

**WisePoint8**

https://wisepoint.jp/