

NIIオープンフォーラム2021

認証トラック2

AXIES認証基盤部会・学認合同企画セッション：認証技術の最新動向



Shibboleth IdP v4対応 **WisePoint 8**と パスワードレス認証

2021年7月

ファルコンシステムコンサルティング株式会社
営業本部 山下 克美

WisePoint v8製品仕様



SAML2.0対応

IdP機能、SP機能（Shibboleth Identity Provider ver4 / Shibboleth Service Provider ver3 対応）

認証

- ・ イメージングマトリクス認証
- ・ マトリクスコード認証
- ・ Jパスワード認証
- ・ ハードウェアトークン認証（OneSpan社DIGIPASS）
- ・ TOTP認証（GoogleAuthenticator等）
- ・ Cookie認証
- ・ スマートデバイスID認証
- ・ クライアント証明書対応
- ・ Kerberos認証（Windowsログイン）
- ・ ID/パスワード認証（LDAP/ActiveDirectory連携）
- ・ FIDO2対応認証



シングルサインオン

- ・ SAML2.0
 - ・ G Suite
 - ・ Office365
 - ・ Salesforce
 - ・ Cybozu.com
 - ・ Desknet's NEO
 - ・ box
 - ・ 学認対応SP 他
-
- ・ 非SAML対応のWEBシステム（ベーシック認証/フォーム認証）

その他の特長

- ・ マルチテナント機能
- ・ アカウントロック機能
- ・ LDAP/ActiveDirectory連携

アクセスコントロール

- ・ 場所（学内、学外等のIPアドレス制御による認証方式変更）
- ・ 時間
- ・ OSやブラウザ（ユーザエージェント）
- ・ SP単位による認証方式
- ・ ロール単位でのアクセス制御

WisePoint 8

認証／シングルサインオン デモンストレーション

デモの流れ

PCからのアクセス

- ①IDの入力
- ②Windows HelloをつかったFIDO認証
- ③目的のサイト（サイボウズ）にアクセス

スマートフォンからのアクセス

- ①IDの入力
- ②Touch IDを使用したFIDO認証
- ③目的のサイト（サイボウズ）にアクセス

FIDO認証の登録

- ①登録サイトにログイン
- ②FIDO資格情報（生体情報など）の登録

デモの流れ

順序	項 目
①	SPのCybozu.comにアクセス
②	IdPにリダイレクト
③	利用者の画面にてID入力（ユーザの判別）
④	FIDO認証（Windows Hello）
⑤	Cybozu.comにログイン完了
⑥	他Webシステムにもシングルサインオンでアクセス
	登録（PC、iPhone）
	PCはWindows Hello iPhoneはTouchID

[PCデモ](#)

[FIDO登録](#)

iPhoneのTouchIDを利用したSSO

①TouchIDの登録

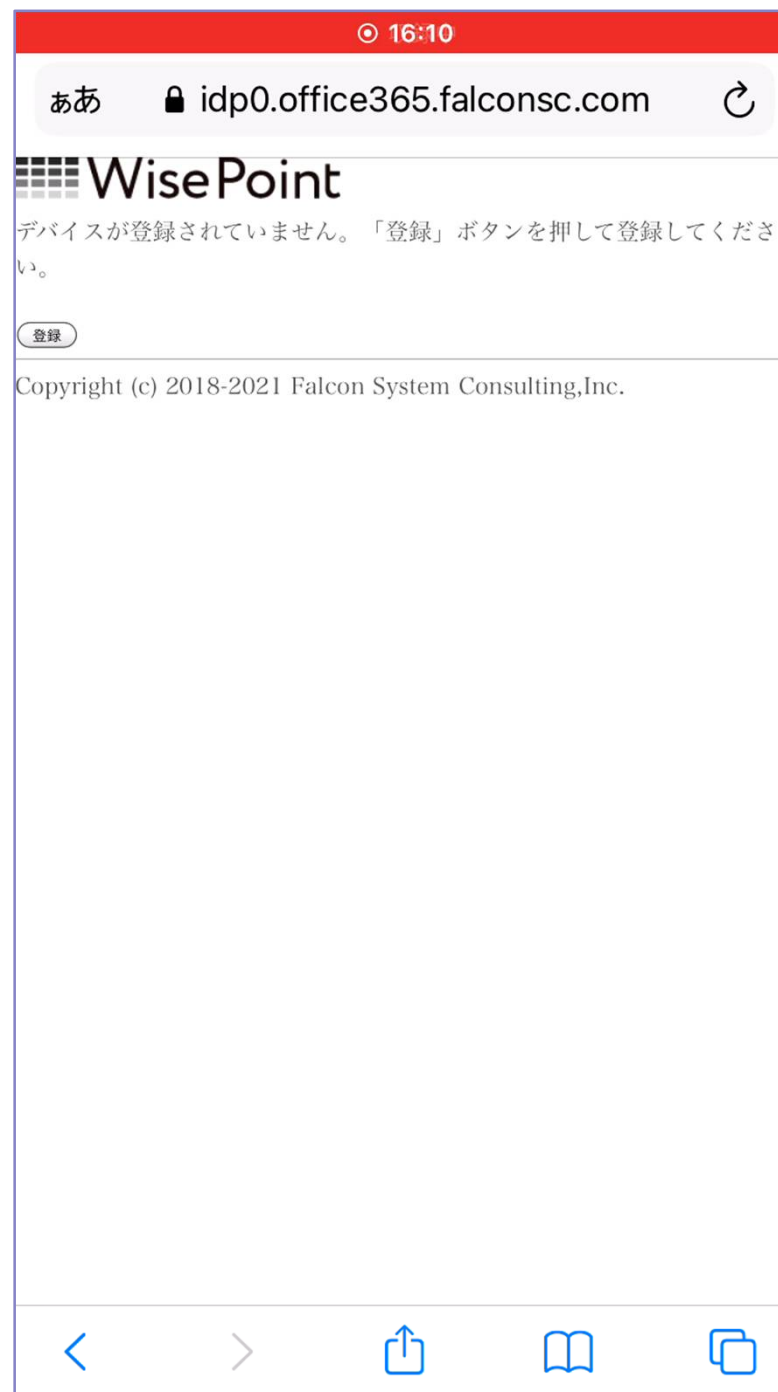
- (1) FIDO認証登録サイトからTouchIDを登録
- (2) 登録完了
- (3) 登録サイトからログアウト

②TouchIDで認証

- (1) ブックマークからデモ用cybozu.comにアクセス
- (2) ID入力
- (3) FIDO認証 (TouchID)
- (4) cybozu.comにアクセス成功

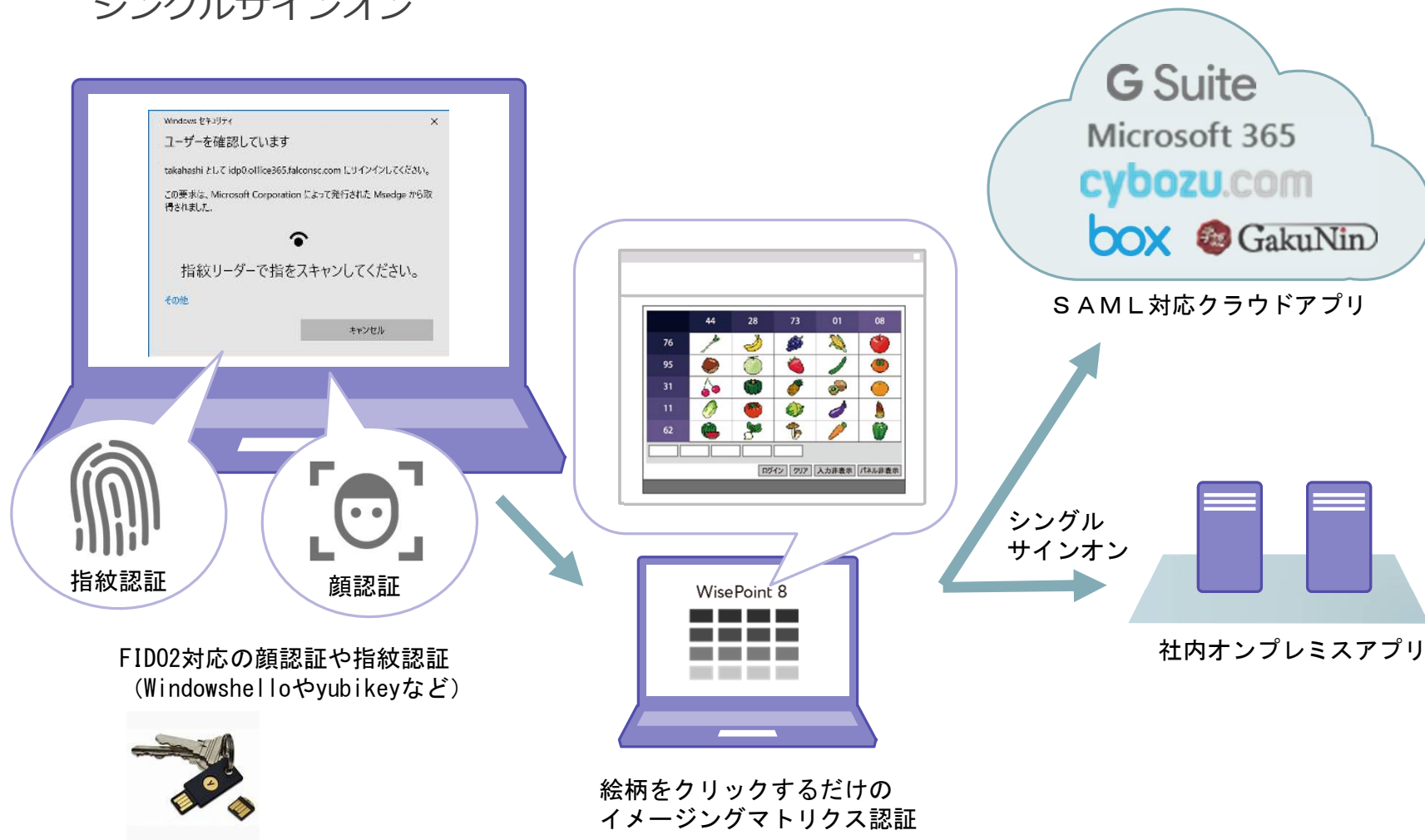
③SSO

- (1) ブックマークよりWisePointポータルにアクセス
- (2) SSOで再度認証をすることなくアクセス成功

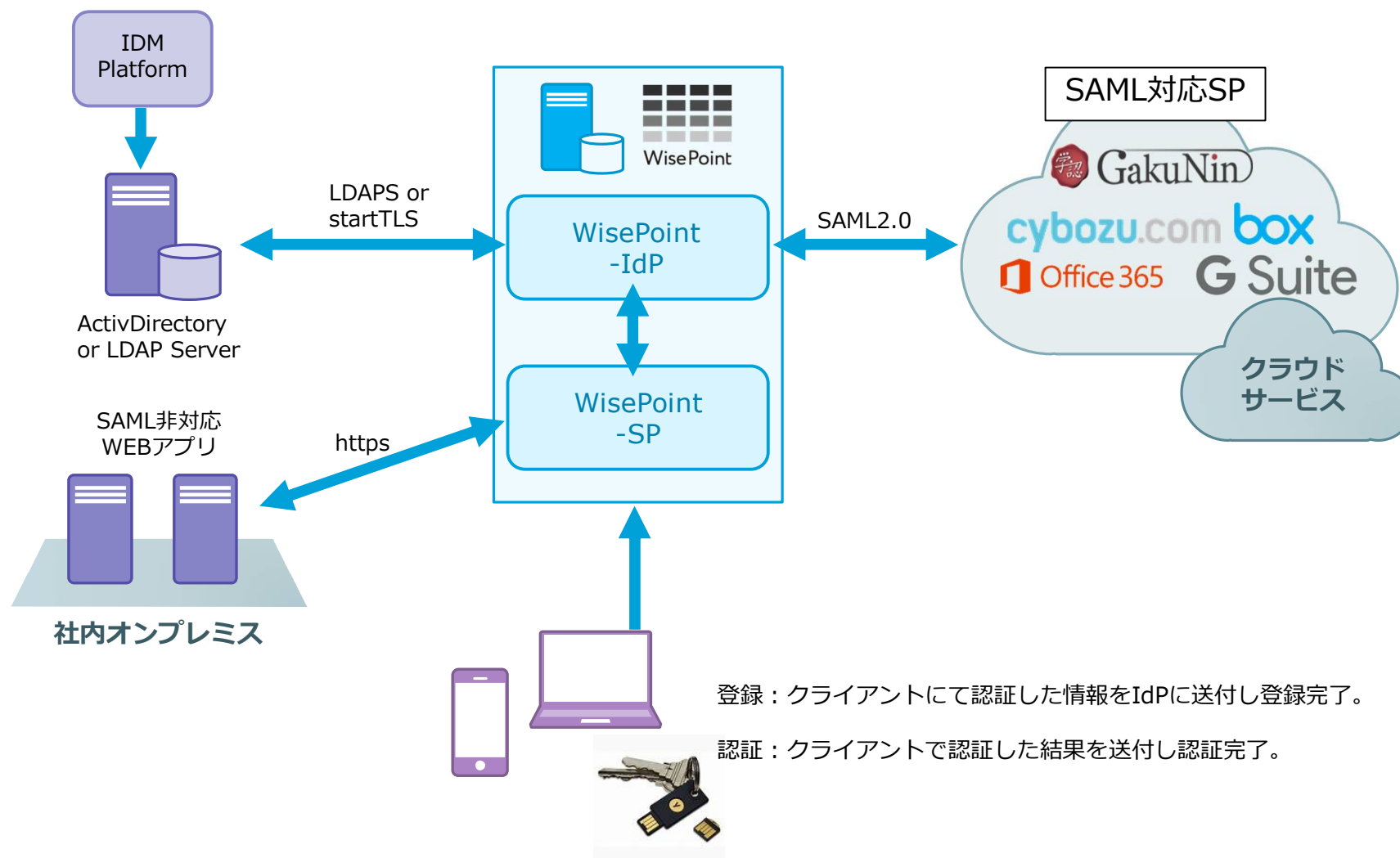


パスワードレスでSSOが可能です！

本人所有の端末と本人そのもの、本人の記憶の組み合わせによる多要素認証とシングルサインオン



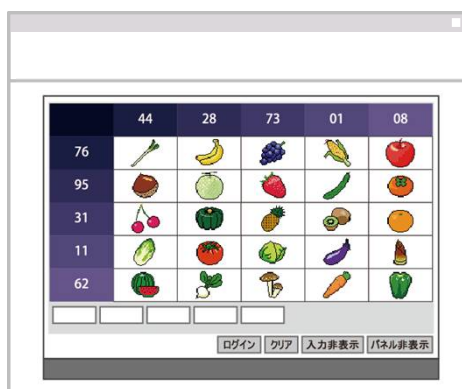
WisePoint 8利用イメージ



認証方式①

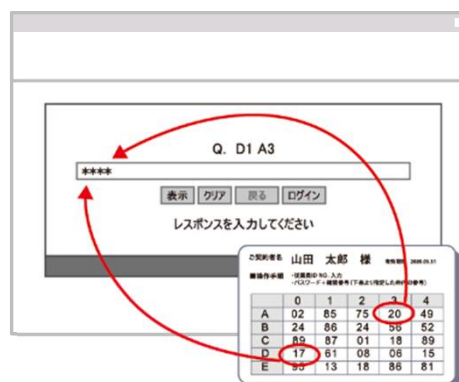
■ ブラウザベースのトークンレスワンタイムパスワード

イメージングマトリクス認証



- ▶ 憶えやすく忘れにくい絵柄・図柄で認証
- ▶ ユーザが思い出すのは自分で事前に決めた画像とその順番
- ▶ クリック方式でスマートフォンなどでも簡単に入力
- ▶ ログイン毎にイメージの位置情報が変化することで、ワンタイムパスワード認証を実現

マトリクスコード認証



- ▶ ユーザ毎にユニークな乱数表を用いた認証
- ▶ ユーザはサーバから指定された行列の数値を入力するだけ
- ▶ ログイン毎にチャレンジコードが変化することで、ワンタイムパスワード認証を実現
- ▶ 記憶と所有物による二要素認証
- ▶ ゲストユーザー用に一時貸し出しなどの対応も可能

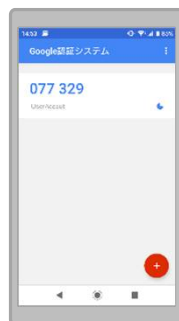
Jパスワード認証



- ▶ 本人しか知らない既知情報を「質問(チャレンジ)」と「答え(レスポンス)」として登録利用できるので、覚えやすく忘れにくい認証方式
- ▶ 日本語(全角文字:漢字やひらがな)と英数字を利用できます
- ▶ パスワードに利用可能な文字数が英数字のみの認証と比べ増加するため、総当たり攻撃に強い耐性を発揮

認証方式②

TOTP認証



- ▶ 「Google Authenticator」や「Microsoft Authenticator」を利用可能
- ▶ モバイルアプリで表示された確認コードを入力
- ▶ 事前に端末側に読み込ませるQRコード(秘密鍵)を社外では表示させない等の安全を保つ設定も有り
- ▶ TOTP方式のソフトウェアトークン認証

OneSpan DIGIPASS認証



*VASCOはOneSpanに社名変更しました

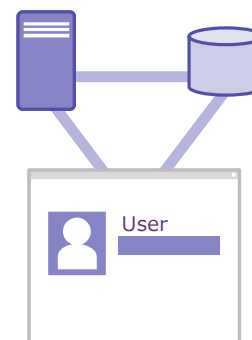
- ▶ 表示されたワンタイムパスワードを入力するだけ
- ▶ 一定時間ごとにパスワードが変わるハードウェアトークンを使ったワンタイムパスワード認証
- ▶ ネットバンキングレベルの高いセキュリティ強度
- ▶ 記憶と所有による二要素認証

スマートデバイスID認証



- ▶ スマートデバイス端末ごとに固有に持たせたIDで端末を特定
- ▶ ユーザID入力の手間を省略
- ▶ 専用アプリ「WisePoint Brower」または「WisePoint Client」からアクセス
- ▶ iOS/Androidに対応

Kerberos認証 (Windowsログオン)



- ▶ Windowsログオンが成功するとWisePointの認証サーバが自動で認証をスキップします。
- ▶ Windowsにログオンすると、Webシステムのログインを省略できます。

動作環境



対応プラットフォーム	Red Hat Enterprise Linux ver8
クライアントOS	Windows／MacOS／iOS／Android
ブラウザ	GoogleChrome／FireFox／Safari／Edge／(Internet Explorerは対象外予定)
対応DB	PowerGres ver11(バンドル)
HW推奨スペック	CPU : 2.2GHzクラス以上
	Memory : 8GB以上

※最小構成は2台構成となります。クラスタ構成をとる場合は、H/Wは各2倍となります。

※仮想化環境に対応

※クラウドサービス（AWS、さくらのクラウド等）上での構築も可能

※サーバにはSSLサーバ証明書が必要となります。

WisePoint Shibboleth

ソリューションと導入事例

事例 株式会社ディスコ様 提供サービスの認証連携



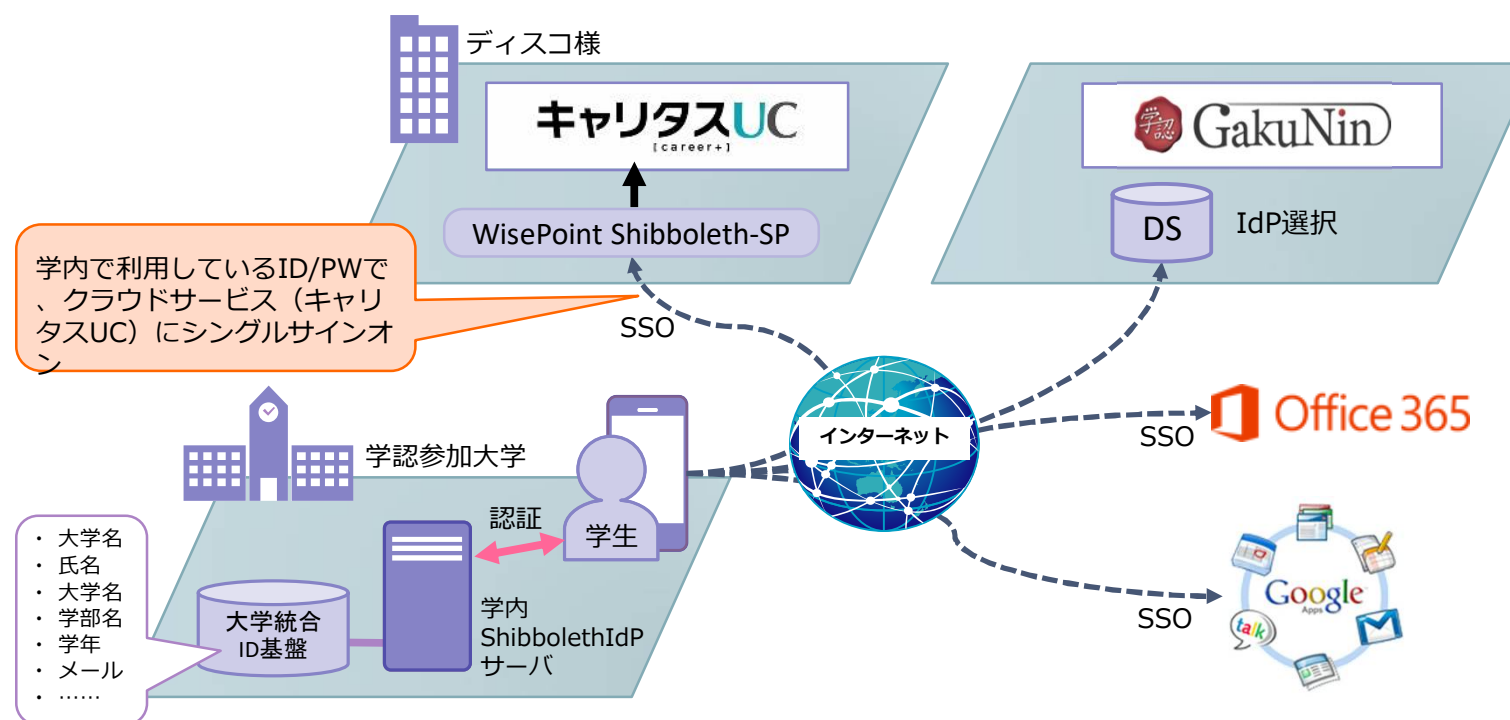
課題・問題

- ・学生から学内IDとキャリアスUC*のIDが別々で使い勝手が悪いと不評
- ・大学側からも学内IDで利用したいという要望

導入の効果

- ・学生が普段から利用している学内IDとサービスのIDを連携して、利用者の利便性とセキュリティ向上
- ・使い勝手の良いサービスとして改善

*キャリアスUC：ディスコ様が運営している大学生の就活管理クラウドサービス。
企業・学校・学生をオンラインで繋ぐ就活メディア。

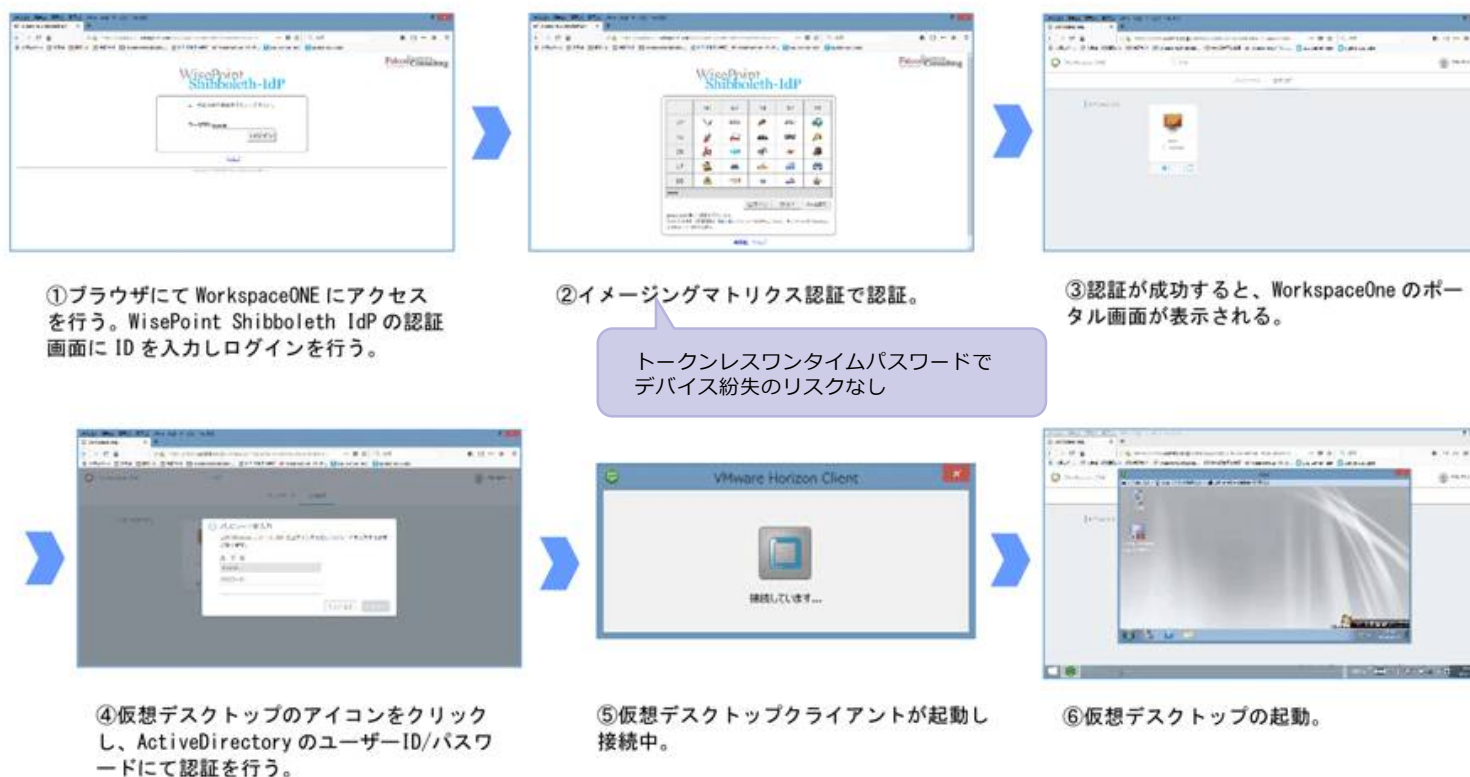


ソリューション テレワーク時のセキュリティ対策と利便性の両立

- VMware社「VMware Workspace ONE」と、WisePoint Shibboleth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

VMware Workspace ONEは、新たな「働き方」の実現を支援するデジタルワークスペースです。アクセスコントロール、アプリケーション管理、マルチプラットフォームに対応するエンドポイント管理を統合し、PCはもちろんiOS、Android、Windows 10など異なるOSを搭載した多様なモバイルデバイスから、社内システムに安全にアクセスすることが可能となります。

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

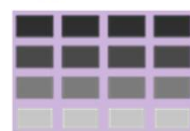


※ Citrix Workspaceにも対応可能

速い パスワードレス

簡単

イメージングマトリクス

 WisePoint 8

シングルサインオン

多要素認証

ゼロトラストセキュリティ

お気軽にお問い合わせください



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
電話番号：03-6228-3220
電子メール：sales@falconsco.com
製品紹介サイト：<https://wisepoint.jp/>
企業サイト：<https://www.falconsco.com/>

ファルコンシステムコンサルティング株式会社は証券コード3968セグエグループの子会社です。

WisePoint、ImagingMatrixはファルコンシステムコンサルティング株式会社の登録商標です。