



1) Office365を導入するには どのようなID管理が必要か？ ～オンプレミス及びクラウド上のID管理方法～

Soliton

平成27年11月18日
株式会社 ソリトンシステムズ
ID Manager担当
倉田和人

- ① 2種類のID
- ② アカウント管理
- ③ 利用目的別グループ
- ④ 階層型アドレス帳
- ⑤ ライセンス管理
- ⑥ パターン別ID管理推奨モデル

■ アカウントを登録するIDシステムは2種類

– 組織アカウント

- クラウドID

- クラウド上に設定したID/パスワードで認証

– フェデレーションアカウント

- フェデレーションID

- オンプレミスAD上で認証した情報を利用

- Azure AD管理ポータル上でディレクトリ統合設定（シングルサインオン設定）する事でフェデレーションIDシステムとして設定される

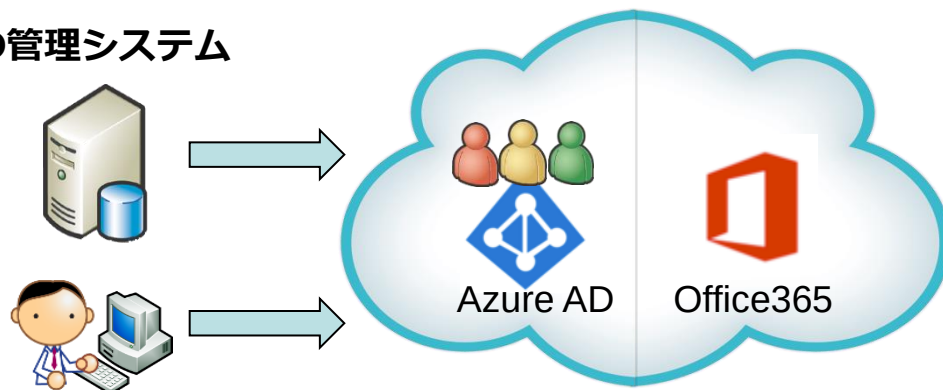
■ IDシステムはドメイン単位で選択

- 1つのドメインで複数のIDシステムは利用できない
- (サブ)ドメインを分ければ複数のIDシステムを利用可能
 - 一般社員用ドメイン : domain1.soliton.co.jp
 - オンプレミスのADドメインにログオンする
 - ディレクトリ統合しフェデレーションIDとして利用
 - メール専用ユーザードメイン : domain2.soliton.co.jp
 - オンプレミスのADドメインにはログオンしない
 - 組織アカウント（クラウドID）をAzure AD上に登録

■ クラウド上にIDを登録

- GUIベース
 - Office365管理センター
 - Azure ADポータル上作成
- 一括処理
 - PowerShell
 - ID管理システム

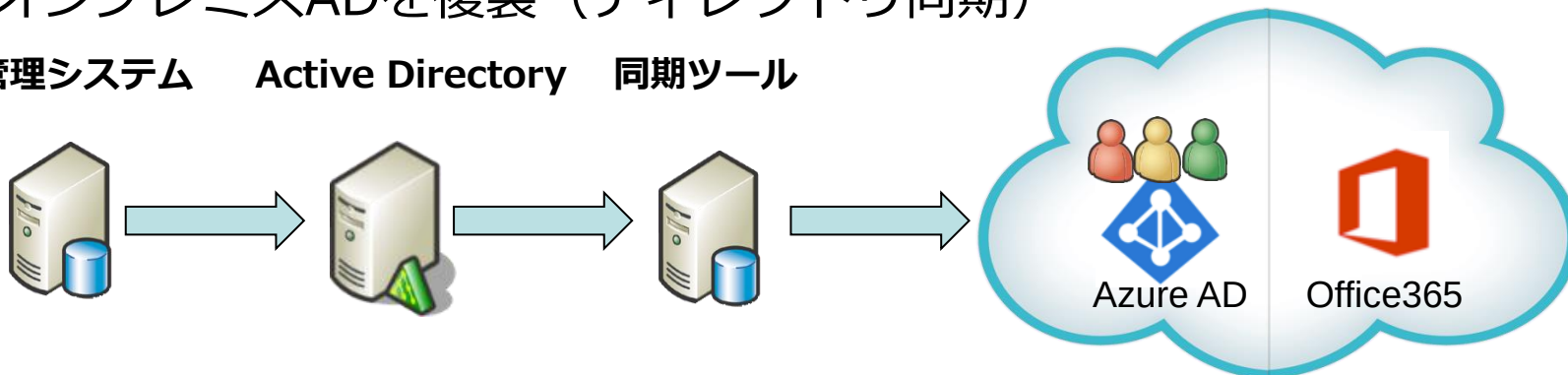
ID管理システム



■ ディレクトリ同期

- オンプレミスADを複製（ディレクトリ同期）

ID管理システム Active Directory 同期ツール



■ Microsoft社から提供される仕組み

- DirSync（当初） or AAD Sync（ちょっと前）
 - マルチフォレスト対応：AAD Sync
 - DirSyncの場合は、複製用ドメインを別途作成など
 - 逆同期（書き戻し）
 - パスワードの逆同期に対応：AADSync
 - デバイスの書き戻し：Dir Sync
- 今は、Azure AD Connect
 - 上記2ツール、ADFSも含めて統合されたディレクトリ統合支援ツールの的な位置づけ
 - ディレクトリ同期やIDフェデレーション環境をウィザード形式で簡単セットアップ

Azure AD Connectに関する情報

<https://msdn.microsoft.com/ja-jp/library/azure/dn757582.aspx>

https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnect/?WT.mc_id=A0618AD15

<http://azuread.net/2015/06/29/azure-ad-connectを利用したoffice-365-x-adfs設定/>