JNSA アイデンティティ管理WG主催
「クロスボーダー時代のアイデンティティ管理セミナー」

コンシューマIDの
エンタープライズ領域での活用

伊藤忠テクノソリューションズ株式会社
富士榮　尚寛

自己紹介

- Blog
  - IdM実験室：http://idmlab.eidentity.jp
- 記事 / 書籍
  - @IT/企業のID管理／シングルサインオンの新しい選択肢「IDaaS」の活用 他
  - クラウド時代の認証基盤 Azure Active Directory 完全解説
  - クラウド環境におけるアイデンティティ管理ガイドライン（JNSA）
- その他
  - JNSA アイデンティティ管理WG
  - OpenID Foundation Japan 教育・翻訳WG、エンタープライズ・アイデンティティWG
  - Microsoft MVP for Enterprise Mobility（Jan 2010 -）

アジェンダ

- 組織IT部門への要求事項と対応
  - コミュニケーションのBYOC～BYOIDへ
- BYOIDを組織において実現するためには
  - IDライフサイクル管理
  - ID保証レベル（IAL）
  - 認証保証レベル（AAL）
- Azure AD B2Cで実装した例
- コミュニケーションのBYOCは可能か？
- まとめ

組織IT部門への要求事項

働き方改革
（Any where, Any time, Any device）

- リモートアクセス
- 使い慣れたデバイス
- コミュニケーション基盤

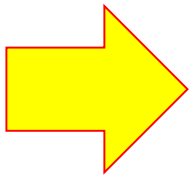
現場（LoB）中心の業務改革
（スピード・利便性＞管理）

- 現場でのクラウド導入
- 使い慣れたツール

組織IT部門の対応

働き方改革
（Any where, Any time, Any device）

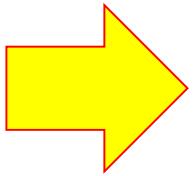
- リモートアクセス
- 使い慣れたデバイス
- コミュニケーション基盤



VPNの整備
BYODの許可とMDM
メール＋α

現場（LoB）中心の業務改革
（スピード・利便性＞管理）

- 現場でのクラウド導入
- 使い慣れたツール



BYOCの許可とIDaaSやCASB

大前提となるのが コミュニケーション強化

メールシステムの課題と限界

増え続ける添付ファイル
→グループウェアで解消？

リアルタイム性の欠如
→ビジネスチャットで解消？

結局ツールが増えるだけ

そもそも見なくなる

ここでもBYOC
→野良LINE、Slackなど

MDMやCASBで対応し続ける？

大前提となるのが コミュニケーション強化

メールシステムの課題と限界

増え続ける添付ファイル
→グ

リア
→ビ

だけ

そも

SB
する

Slackなど

コミュニケーション・ツールのBYOC
に伴う「BYOID」
（Bring Your Own Identity）
について向き合うべき時代の到来

BYOIDの要件

自身で利用 ID を選択できること

よく使う ID が利用できること

組織 ID との紐づけが出来ること

BYOIDへの対応

CIAMのテクノロジーを使って実現

CIAM=Customer Identity and Access Management

CIAMの主要な機能

- コンシューマID（SNSなど）を使ったID登録、ログイン
- 認証強化（多要素認証、リスクベース認証）
- 顧客DBとの紐づけ管理
- アプリケーションやAPIの保護

主なプレイヤー

- Gigya（SAP）
- Janrain
- PingIdentity
- Microsoft

など

Source: Kuppingercole

組織における課題

組織におけるID管理の要件

IDライフサイクル管理
- IDの作成～破棄が組織側によって管理されること
- ID保証が組織のポリシーに則って実行されること

認証
- 組織のポリシーに則って認証されること

認可（アクセス制御）
- IDライフサイクルに連動してコントロールされること

BYOIDを実現する上で必要なこと
- 組織でID作成～破棄ができること
- 組織の要求するレベルのID・認証保証がされること

そのために必要なこと

JNSA

組織でID作成～破棄の管理ができること

- 「顧客DBとの紐づけ機能」を応用し、組織内のID管理システムとコンシューマIDを紐づけることで対応

組織の要求するレベルでID・認証保証がされること

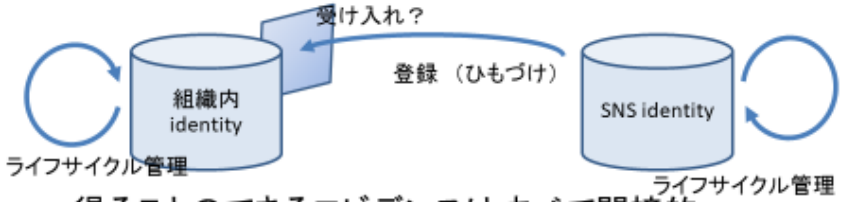
- ID保証（入社・契約時の身元確認）
  - 結局はオーソリティによる第三者保証
    - 住民票
    - 元請け会社
  - マイナンバーや運転免許証を使い対面取得したキャリアIDなどの利用
- 認証レベル
  - そもそもパスワード認証よりは強固
  - 普段から頻繁に使っている＝ID盗難の可能性は低い（気が付ける）

そのために必要なこと

大学ICT推進協議会（AXIES）年次大会での議論 / NII佐藤先生

基本

- SNSの提供するidentity保証レベルを直接評価することができない
  - 業務委託をしているわけでもない（cf. IDaaS）
  - 監査記録を提出してくれるわけでもない（cf. IDaaS）
  - 勝手格付けするか？



- 得ることのできるエビデンスはすべて間接的

2017/12/13 AXIES 2017@広島 12

問題になること

- SNS Identityを自組織提供サービス利用アカウントとして用いるときに求める要件
  - 前述の通り、基本的に制御不可能。しかし以下について、十分合理的な評価はできるかもしれない
  - IALは十分であるのか
    - 本人の申告のみでOKなのか
  - AALは十分であるのか
    - 多要素認証（スマートフォンという「デバイス」紐づけ）
    - 常に利用しているというアドバンテージ（常時モニタリングの要件をある程度みたしている）

2017/12/13 AXIES 2017@広島 13

SNSなど外部のIDを持ち込む場合の課題
- ID保証レベル（IAL）　⇒　間接的なトラストの捉え方
- 認証保証レベル（AAL）　⇒　スマホ、常時利用の捉え方

そのために必要なこと

大学ICT推進協議会（AXIES）年次大会での議論 / NII佐藤先生

IALは十分か/AALは十分か

- Mobile キャリア　asトラストアンカー
- キャリアの提供するidentity
  - 国による規制（IAL）
  - SIMの堅牢さへの信頼（AAL）

- 残りはこれからの派生identity
  - しかし
  - 一定の留保をつけて高い保証レベルを与えて構わないだろう
- では、キャリアの認証を経ないアカウントはどうなのか？
  - 本人かどうかは自己申告にして、アカウントと自己申告した本人の結びつき（登録）がどのくらい強いのかが問題

2017/12/13　AXIES 2017@広島　14

LINE

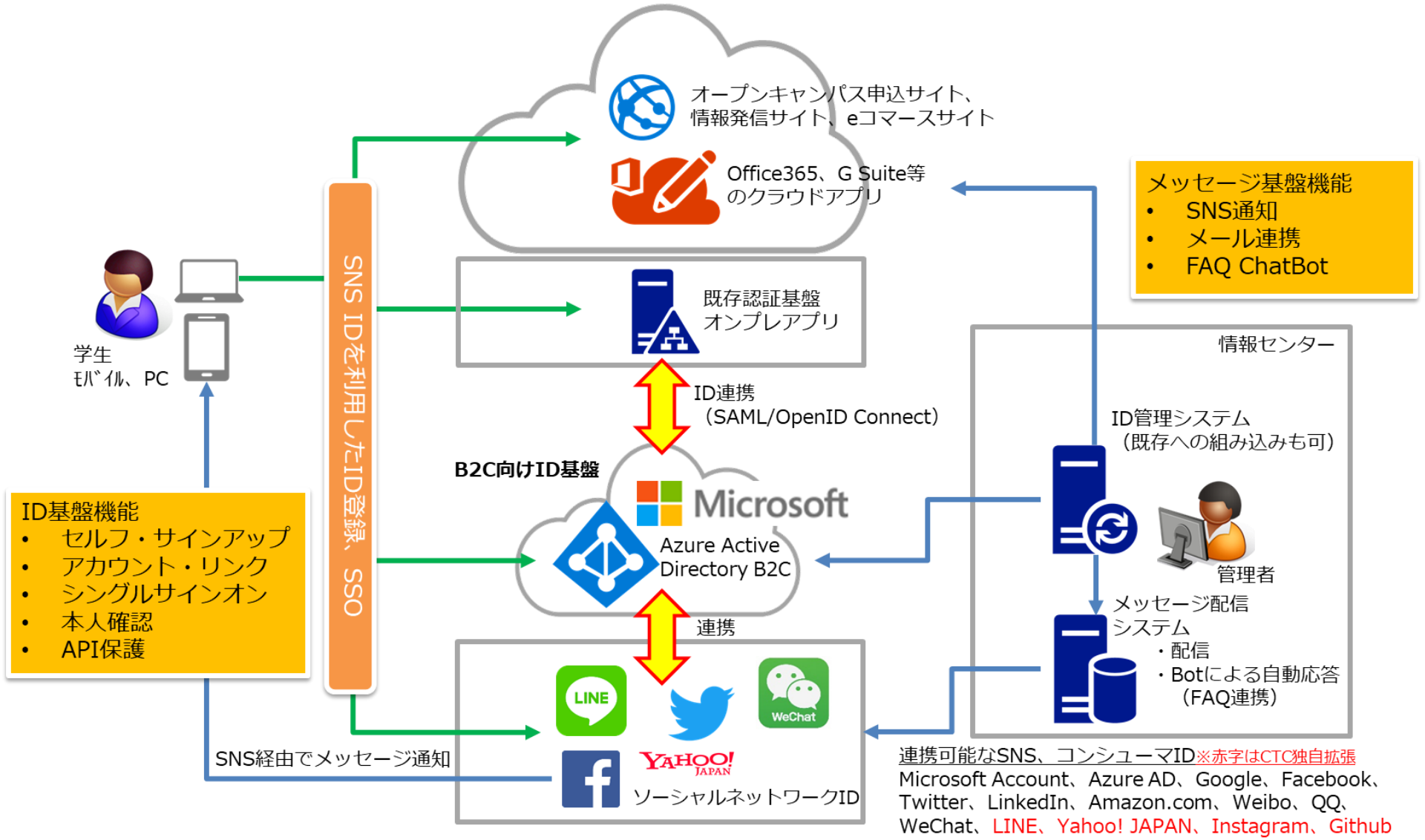
- パスが2つ
  - 電話番号認証 → ID
    - Higher Assurance
  - Facebook認証 → ID
    - 下の理由で高い保証レベルを持つかもしれない
- SNSの強み
  - アカウントは普段使い
    - いろいろ例外はあるにせよ、常時モニタリング状態にある
  - したがってアカウントのbehaviorは常にチェックされている
    - Authenticateの保証レベルとしてプラス要因
  - だいたい、利用はmobile デバイスからの方が多いので、端末との（ゆるい）紐づけも期待できる

2017/12/13　AXIES 2017@広島　15

ID保証レベル（IAL）
アンカーとしてキャリアIDは一つの選択肢となりうる

認証保証レベル（AAL）
デバイス＝多要素、常時利用状態は強みと考えられる

Azure AD B2Cでの実装例



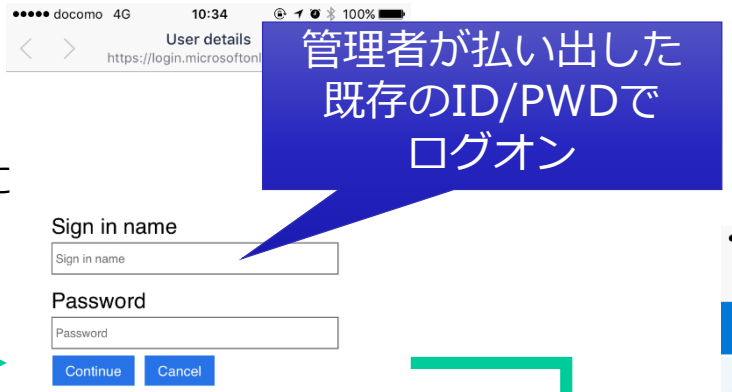
IDライフサイクル管理に関する要求に対する対応

①QRコード等でLINE@を友達登録

②友達登録をすると
トークルームを利用可能に

LINEアプリ

④LINE ID紐付けを実施



管理者が払い出した
既存のID/PWDで
ログオン

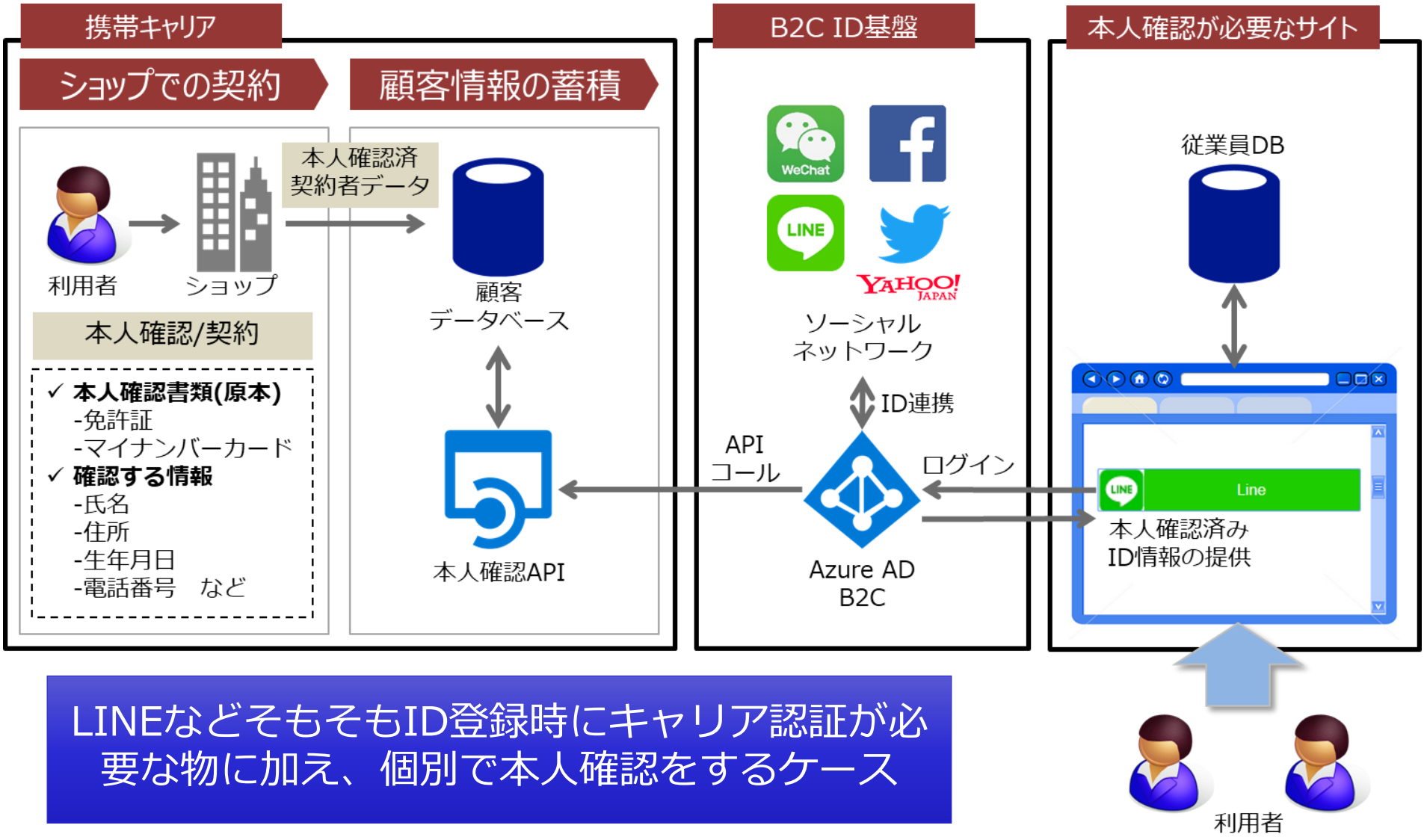
③LINE ID紐づけをしないと
従来のメールアドレス/
パスワードでログイン

⑤LINE ID紐づけを実施後
はシングルサインオン

自身で紐付けた
SNS IDでログイン

※Graph APIによる
ID管理が可能

ID保証要求に対する対応



LINEなどそもそもID登録時にキャリア認証が必要な物に加え、個別で本人確認をするケース

認証保証要求に対する対応

コミュニケーションの改善（LINEの例）

LINEトークルームのメニューより各種機能を呼び出すことが可能

- メールを見る
- ポータル
- 組織IDとLINEアカウントを紐づける
- 重要度の高いメールをLINEへも通知する

SNSはあくまで入り口。個々のやり取りをSNS上で行う訳ではない

重要なメールが届くとタイムラインに通知される

Office365へのアクセス（Exchange Online、SharePoint Online）

LINE IDを紐づけ、SSOするための設定

Office365へ重要なメールが届いた場合、LINEへ通知する設定

コミュニケーションのBYOCは可能か？

利用者の視点	管理者の視点
• 普段使っているツール（SNS）を利用 • ストレスのないコミュニケーションの実現（SNSによるBYOC）	• IDの管理は組織側で実施できる（ID紐づけ） • SNSは入り口なので、勝手にSNS上でやり取りをされるわけではない

ただし、

利用にあたっては、啓蒙活動が必要
- 利用者：SNSの持ち込みの気持ち悪さの解消
- 管理者：組織外の個人情報の管理

実際、どこまで持ち込んでいるか？

SNS提供者にもよるが、コンテキストが混ざることを一番気にしているのはSNS提供者（歴史が違う）
例）

- LINE（LINE@）
  - 接続するLINE@（組織）ごとにユニークな個人識別子を払い出し、組織側からは利用者のいわゆるLINE ID（個人同士で使うID）はわからない
- Facebook（Facebook Page）
  - ページ単位、クライアントアプリケーション（Oauthクライアント）の単位でユニークな個人識別子を払い出している

→つまり、**組織側に連携される識別子が仮に漏洩したとしても使いようがない状態**にはなっている

まとめ

コミュニケーション手段の変化（BYOC）によるBYOID の時代へ

ユーザが自分で、よく使うIDを選択することが大切（コミュニケーション手段としての意義、常時利用によるAAL向上）

組織IDとの紐づけによるIDライフサイクル管理、キャリア等との連携によるIALの向上が組織へのBYOID導入におけるキーポイント