



LDAP 認証とクライアント組織について

目次

| | |
|--------------|---|
| 概要 | 3 |
| 構成について | 3 |
| 設定について | 6 |

概要

この資料では、Yellowfin のクライアント組織を LDAP 認証で運用する方法について記載しています。この資料を作成するにあたって使用した製品のバージョンは、Yellowfin 7.1 Build20151026 です。ディレクトリサービスは ActiveDirectory を使用しています。

構成について

1. LDAP の構成について

ここでは、LDAP の構成について説明します。

LDAP の構成を以下のように設定にすることで、Yellowfin のクライアント組織として運用することが可能になります。

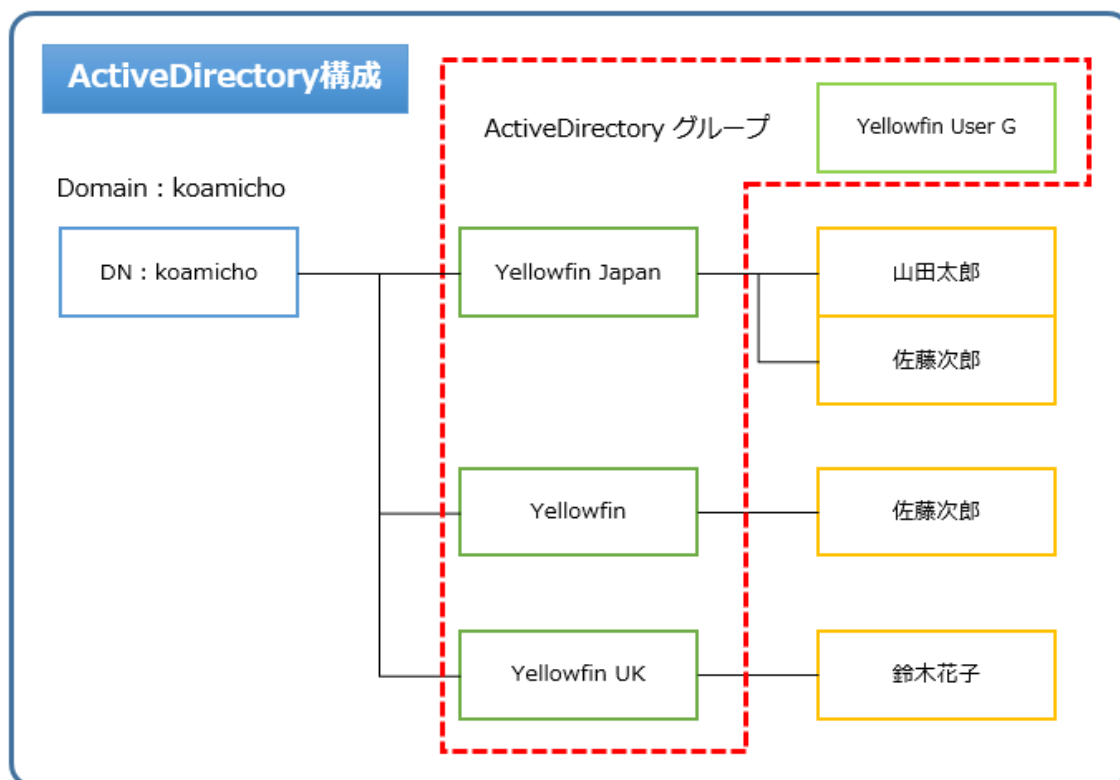


図 1 ActiveDirectory 構成

Yellowfin にログインする必要があるすべてのユーザーは Yellowfin User G に所属しています。この Yellowfin User G は、Yellowfin の LDAP 認証の設定で使用します。各ユーザーは、それぞれ別の ActiveDirectory グループ（Yellowfin, Yellowfin Japan, Yellowfin UK）に所属しています。

この他に、ユーザーは、**Domain Users** に属しています。

2. Yellowfin の構成について

ここでは、Yellowfin のクライアント組織の構成について説明します。

上記の ActiveDirectory の構成をベースにした、Yellowfin のクライアント組織の構成は図 2 のとおりです。

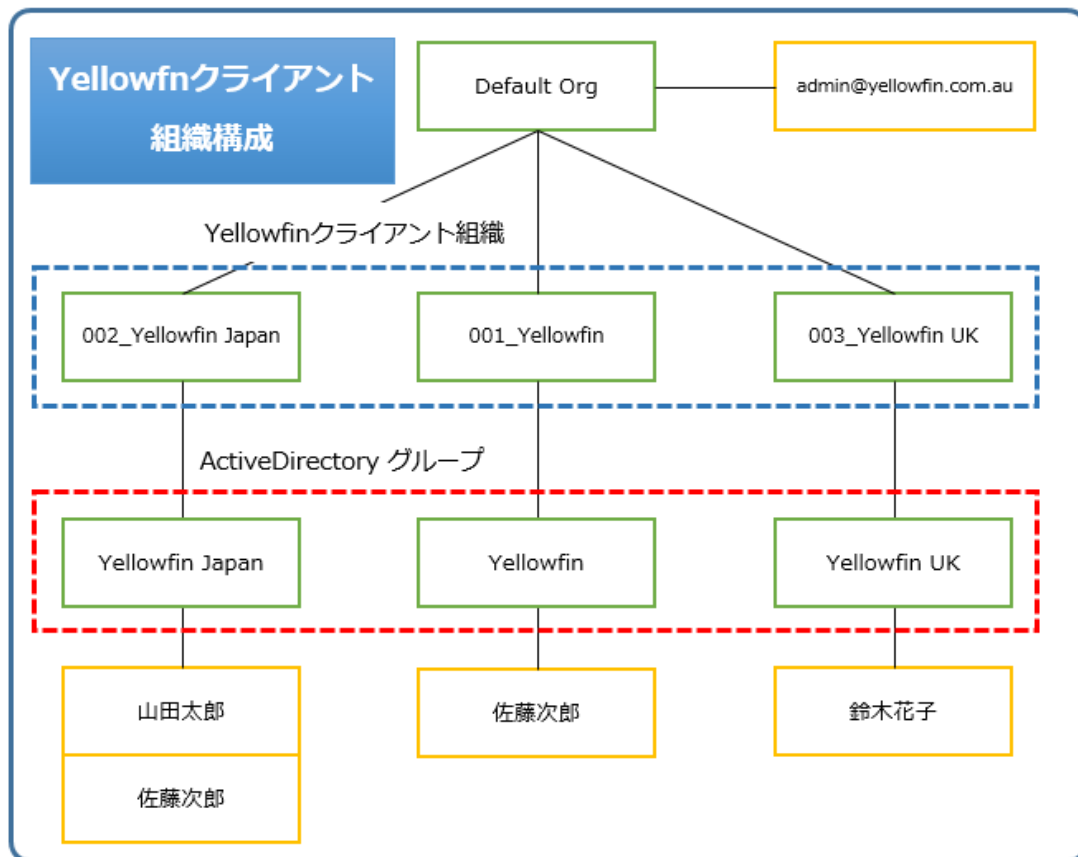


図 2 Yellowfin クライアント組織構成

各ユーザーは、ActiveDirectory グループに紐づくそれぞれのクライアント組織へログインします。

※Default 組織へログイン可能なユーザーは、admin@yellowfin.com.au のみとしています。

| AD グループ | Yellowfin クライアント組織 | ログインユーザー |
|------------------------|---------------------|------------------------|
| <i>Yellowfin</i> | 001_Yellowfin | 佐藤次郎 |
| <i>Yellowfin Japan</i> | 002_Yellowfin Japan | 山田太郎 佐藤次郎 |
| <i>Yellowfin UK</i> | 003_Yellowfin UK | 鈴木花子 |
| - | Default | admin@yellowfin.com.au |

※ admin@yellowfin.com.au 以外の各ログインユーザーは上記 AD グループ以外に、
Domain Users および Yellowfin User G に属しています。

図 3 ActiveDirectory グループと Yellowfin クライアント組織

設定について

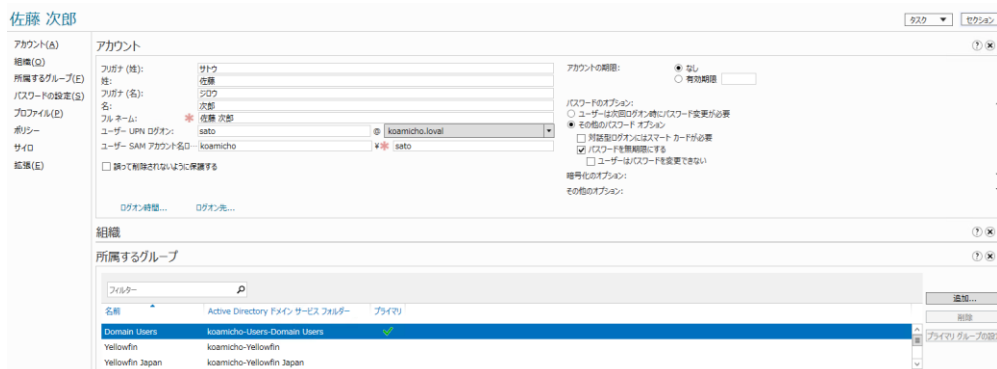
1. ActiveDirectory の設定

ここでは、ActiveDirectory 上のユーザー、グループの設定について、記載します。

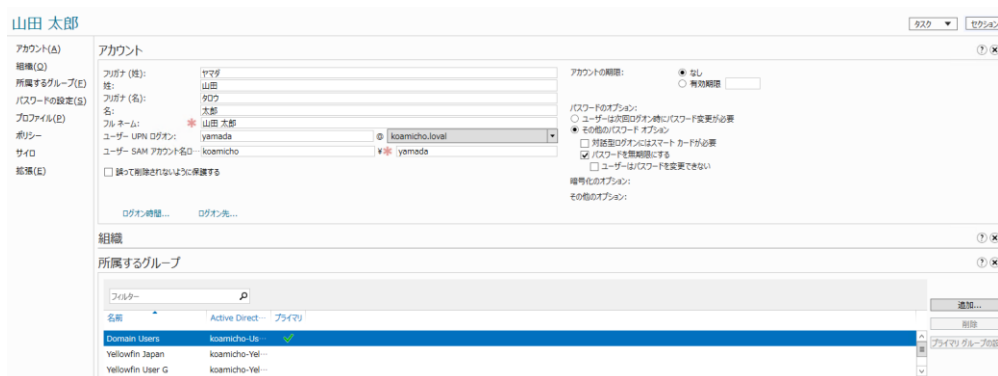
ActiveDirectory のユーザー設定



各ユーザーは、**Domain Users** をプライマリグループに設定してください。



※ Yellowfin User G にも所属しています。



鈴木 花子

アカウント(A)

組織(O)
所属するグループ(F)
パスワードの設定(S)
プロファイル(P)
ポスター
サイト
拡張(E)

アカウントの期間:
なし
有効期限

パスワードのオプション:
ユーザーは次回ログイン時にパスワード変更が必要
その他のパスワード オプション
対応型ログインにはスマート カードが必要
パスワードを強制にする
ユーザーはパスワードを変更できない

電子メールのオプション:
その他のオプション:

組織

所属するグループ

フィルター

| 名前 | Active Directory | タイプ |
|------------------|-----------------------------|------|
| Domain Users | koamicho-Users-Domain Users | グループ |
| Yellowfin UK | koamicho-Yellowfin UK | グループ |
| Yellowfin User G | koamicho-Yellowfin User G | グループ |

ActiveDirectory のグループ設定

Active Directory 管理センター - koamicho (ローカル)

Active Directory (16)

| 名前 | 種類 | 説明 |
|---------------------------|------|--|
| Builtin | コンテナ | builtinDom |
| Computers | コンテナ | Default container for upgraded computer accounts |
| Domain Controllers | 組織単位 | Default container for domain controllers |
| ForeignSecurityPrincipals | コンテナ | Default container for security identifiers (SIDs) associated with objects from external, trusted domains |
| Infrastructure | コンテナ | Default container for infrastructure |
| LostAndFound | コンテナ | Default container for orphaned objects |
| Managed Service Accounts | コンテナ | Default container for managed service accounts |
| NTDS Quotas | コンテナ | Quota specifications container |
| Program Data | コンテナ | Default location for storage of application data. |
| System | コンテナ | Builtin system settings |
| TPM Devices | コンテナ | msTPM-Inf |
| Users | コンテナ | Default container for upgraded user accounts |
| Yellowfin | グループ | Yellowfin クライアント組織: 001_Yellowfin |
| Yellowfin Japan | グループ | Yellowfin クライアント組織: 002_Yellowfin japan |
| Yellowfin UK | グループ | Yellowfin クライアント組織: 003_Yellowfin UK |
| Yellowfin User G | グループ | Yellowfinにてユーザー検索対象のグループ |

【Yellowfin】所属メンバー：佐藤次郎

Yellowfin

グループ(G)
管理者(B)
所属するグループ(F)
メンバー(M)
パスワードの設定(P)
拡張(E)

グループ名: Yellowfin
グループ名 (SAM アカウント): Yellowfin
グループの権限:
セレクト
配布
グループのスコップ:
ドメイン ローカル
グローバル
ユニバーサル

電子メール:
説明:
Yellowfin クライアント組織: 001_Yellowfin

管理者

所属するグループ

メンバー

| 名前 | Active Directory |
|-------|------------------|
| 佐藤 次郎 | koamicho-Us |

【Yellowfin Japan】所属メンバー：山田太郎、佐藤次郎

Yellowfin Japan

グループ(G)
管理者(B)
所属するグループ(F)
メンバー(M)
パスワードの設定(P)
拡張(E)

グループ名: Yellowfin Japan
グループ名 (SAM アカウント): Yellowfin Japan
グループの権限:
セレクト
配布
グループのスコップ:
ドメイン ローカル
グローバル
ユニバーサル

電子メール:
説明:
Yellowfin クライアント組織: 002_Yellowfin japan

管理者

所属するグループ

メンバー

| 名前 | Active Directory |
|-------|------------------|
| 佐藤 次郎 | koamicho-Us |
| 山田 太郎 | koamicho-Us |

【Yellowfin UK】 所属メンバー：鈴木花子

Yellowfin UK タスク ▼ 🔍

グループ(c) グループ

管理者(B) グループ名: * Yellowfin UK

所属するグループ(F) グループ名 (SAM アカウント...): * Yellowfin UK

メンバー(M) グループの種類:

パスワードの設定(P) グループの範囲:

拡張(E) 電子メール:

セキュリティ 配布 ドメイン ローカル グローバル ユーバーサル

誤って削除されないように保護する

管理者

所属するグループ

メンバー

フィルター

| 名前 | Active Direct... |
|-------|------------------|
| 鈴木 花子 | koamicho-Us... |

【Yellowfin User G】 所属メンバー：山田太郎、佐藤次郎、鈴木花子

Yellowfin User G タスク ▼ 🔍

グループ(c) グループ

管理者(B) グループ名: * Yellowfin User G

所属するグループ(F) グループ名 (SAM アカウント...): * Yellowfin User G

メンバー(M) グループの種類:

パスワードの設定(P) グループの範囲:

拡張(E) 電子メール:

セキュリティ 配布 ドメイン ローカル グローバル ユーバーサル

誤って削除されないように保護する

管理者

所属するグループ

メンバー

フィルター

| 名前 | Active Directory フォ... |
|-------|------------------------|
| 佐藤 次郎 | koamicho-Users-佐藤 次郎 |
| 山田 次郎 | koamicho-Users-山田 次郎 |
| 鈴木 花子 | koamicho-Users-鈴木 花子 |

2. Yellowfin の設定

ここでは、Yellowfin の LDAP 認証の設定について記載しています。

認証方法の設定

管理-システム構成-認証-認証方法にある、ユーザー認証を「LDAP 認証」に設定します。

ダッシュボード 作成 閲覧 管理 デスクトップ ログアウト System Administrator

認証

この画面で設定できることは？
LDAP認証、クライアントの組織、パスワードの桁数など、ここではすべての認証関連の設定を行うことができます。
認証設定から移動する前に、変更内容を保存するのを忘れないでください。

ヘルプが必要ですか？
あなたが探している答えを見つけたら、Yellowfinのフォーラムやwikiをご覧ください。

一般設定 保存 キャンセル

認証方法

ユーザー認証 Yellowfin 認証

ログインするときに、ユーザーは指定されたLDAPディレクトリに対して認証されます。 LDAP 認証

LDAP設定

クライアント組織

パスワードの設定

LDAP 設定

管理-システム構成-認証-LDAP 設定に、ActiveDirectory の構成情報を設定します。

この画面で設定できることは？
LDAP 認証、クライアントの組織、パスワードの制御など、ここではすべての認証関連の設定を行うことができます。
認証設定から移動する前に、変更内容を保存するのを忘れないでください。

ヘルプが必要ですか？
あなたが探している答えを見つけるために、Yellowfin のフォーラムや Wiki をご覧ください。

ヘルプが必要ですか？
あなたが探している答えを見つけるために、Yellowfin のフォーラムや Wiki をご覧ください。

認証設定から移動する前に、変更内容を保存するのを忘れないでください。

ヘルプが必要ですか？
あなたが探している答えを見つけるために、Yellowfin のフォーラムや Wiki をご覧ください。

LDAP 設定

LDAP Host
LDAP サーバのホスト名または IP アドレス。
XXXX.XX.XX.XX

LDAP Port
LDAP サーバがリスニングしている TCP ポート。
389

暗号化(Encryption)
LDAP サーバによって実装される暗号化方法。
なし TLS SSL

LDAP Base DN
すべてのユーザーとグループを含んでいる LDAP ノード。
DC=koamicho,DC=local

LDAP Group
このグループのメンバーだけが Yellowfin にログインすることができます。
CN=Yellowfin User G,DC=koamicho,DC=lo

LDAP Bind User
LDAP デレトリリーを検索する権限を持つ LDAP ユーザー。
administrator@koamicho.local

LDAP Bind Password
上記で定義された LDAP Bind User のパスワード。
パスワードを更新

LDAP Search Attribute
ユーザーの Yellowfin のユーザー名 (Yellowfin にログインするための LDAP ユーザー名) が含まれている LDAP 属性。
userPrincipalName

LDAP First Name Attribute
ユーザーの名を含む LDAP 属性。
sn

LDAP Surname Attribute
ユーザーの姓 (surname) が含まれている LDAP 属性。
givenName

LDAP Email Attribute
ユーザーの電子メールアドレスが含まれている LDAP 属性。
userPrincipalName

LDAP Role Attribute
ユーザーの Yellowfin のロールが含まれている LDAP 属性。
title

LDAP グループ条件
LDAP Group の一覧のフィルター条件を使用します。グループのみがフィルタリングされた一覧が表示され、Yellowfin に渡されます。

順序
内部認証が行われる順序。
LDAP 認証を優先

テスト接続
上記で定義した設定で、LDAP 接続を試みます。
テスト

保存 キャンセル

LDAP Group には *Yellowfin User G* を設定します。

クライアント組織の設定

管理-システム構成-認証-クライアント組織にある、マルチテナント機能を「ON」にします。

この画面で設定できることは？
LDAP 認証、クライアントの組織、パスワードの制御など、ここではすべての認証関連の設定を行うことができます。
認証設定から移動する前に、変更内容を保存するのを忘れないでください。

ヘルプが必要ですか？
あなたが探している答えを見つけるために、Yellowfin のフォーラムや Wiki をご覧ください。

クライアント組織

マルチテナント機能
Yellowfin のシステム内に複数の仮想インスタンスを作成できるようにします。
 On

グローバル注釈 (Global Annotations)
プライマリ組織で作成された注釈は、任意のクライアント組織を介してアクセスすることはできません。
 Off

パスワードの設定

保存 キャンセル

クライアント組織の登録

管理-管理コンソール-クライアント組織から、Yellowfin で使用するクライアント組織を登録します。クライアント組織に所属するユーザーとして、ActiveDirectory のグループを登録することで、ActiveDirectory グループに所属するユーザーは、ここで登録したクライアント組織にログインすることができるようになります。

クライアント組織

名前: 001_Yellowfin ⓘ

クライアント参照ID(Client Reference Id): 001 ⓘ

タイムゾーン: アジア (Asia) ▼

東京 (Tokyo) (+9:00) ⓘ

ユーザー

この一覧に追加されたユーザーはこのクライアント組織へのログインが許可されます。

追加

検索

- Schema Admins
- Server Operators
- Terminal Server License Servers
- Users
- Windows Authorization Access Group
- WinRMRemoteWMIUsers__
- Yellowfin
- Yellowfin Japan
- Yellowfin UK
- Yellowfin User G
- ユーザー
- LDAP

保存 キャンセル

※図 4 に記載した AD グループ、Yellowfin クライアント組織のとおり設定しています。

クライアント組織

| 名前 | クライアント参照ID(Client Reference Id) |
|--|---------------------------------|
| <input type="checkbox"/> 001_Yellowfin | 001 |
| <input type="checkbox"/> 002_Yellowfin Japan | 002 |
| <input type="checkbox"/> 003_Yellowfin UK | 003 |
| <input type="checkbox"/> Default | |

追加 編集 削除

ユーザーログインアクセス

アクセス可能なクライアント組織の一覧を表示するユーザーを選択してください。

検索

例) クライアント組織「003_Yellowfin UK」の登録内容

| クライアント組織 | | |
|----------------------------------|--|--|
| 名前: | <input type="text" value="003_Yellowfin UK"/> | |
| クライアント参照ID(Client Reference Id): | <input type="text" value="003"/> | |
| タイムゾーン: | <input type="text" value="アジア(Asia)"/> | |
| | <input type="text" value="東京(Tokyo) (+9:00)"/> | |

| ユーザー | |
|---|------|
| この一覧に追加されたユーザーはこのクライアント組織へのログインが許可されます。 | |
| <input type="button" value="追加"/> | |
| 名前 | ロール |
| <input type="checkbox"/> Yellowfin UK | LDAP |
| <input type="button" value="外す"/> | |

Default 組織へ登録したユーザーは、SystemAdministrator(admin@yellowfin.com.au)のみです。

| クライアント組織 | | |
|----------------------------------|--|--|
| これはデフォルト組織です。 | | |
| 名前: | <input type="text" value="Default"/> | |
| クライアント参照ID(Client Reference Id): | <input type="text"/> | |
| タイムゾーン: | <input type="text" value="アジア(Asia)"/> | |
| | <input type="text" value="東京(Tokyo) (+9:00)"/> | |

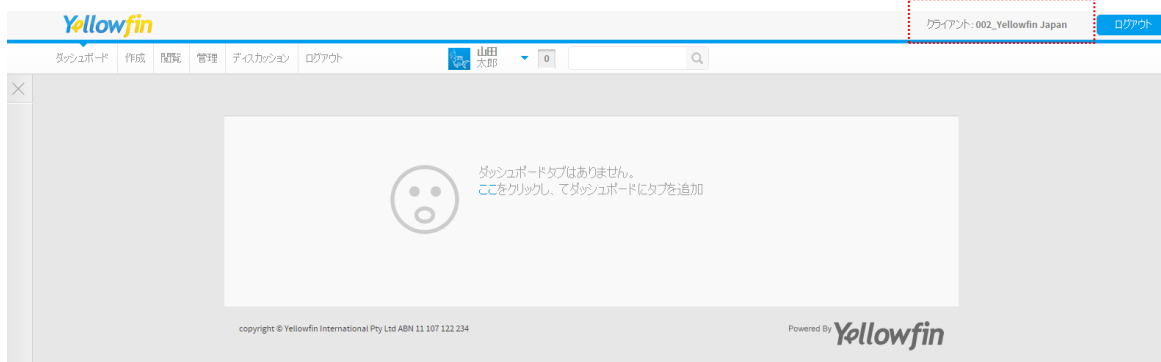
| ユーザー | |
|---|-------|
| この一覧に追加されたユーザーはこのクライアント組織へのログインが許可されます。 | |
| <input type="button" value="追加"/> | |
| 名前 | ロール |
| <input type="checkbox"/> System Administrator | Admin |
| <input type="button" value="外す"/> | |

以上で、ActiveDirectory および Yellowfin への設定は完了です。

ActiveDirectory に登録されているユーザーで Yellowfin にログインして動作確認をおこなってください。

ユーザー：山田太郎でログインした場合

(所属している ActiveDirectory グループが 1 つのユーザー)



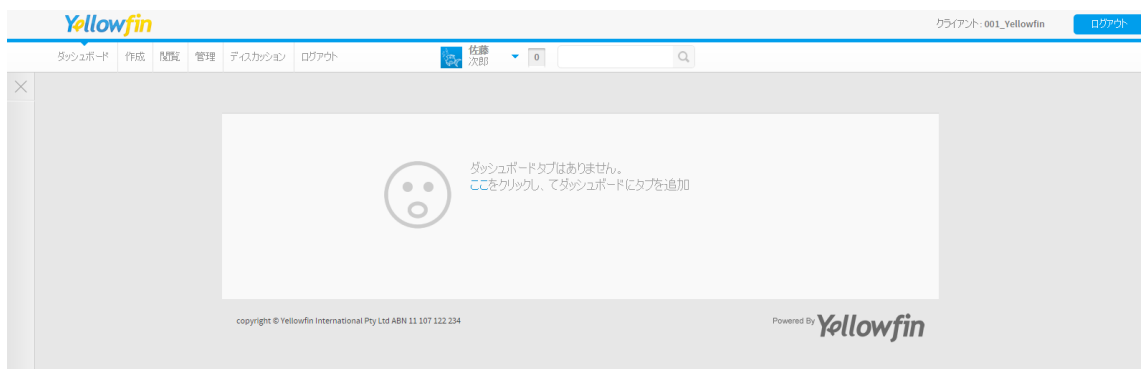
ユーザー：佐藤次郎でログインした場合

(所属している ActiveDirectory グループが 2 つ以上あるユーザー)

複数の ActiveDirectory グループに所属しているユーザーの場合、ログインするクライアント組織を選択する画面が表示されます。



ログインするクライアント組織を選択して、ログインしてください。



以上