



OnTime[®] GROUP CALENDAR

for Microsoft(Ver.4.0-)

ドメイン設定マニュアル
クイック & ステップ バイ ステップ

OnTime Group Calendar Direct Shop

2020/08/07



目次 ドメイン設定マニュアル

- 各設定の選択について p.03
- 設定画面を開く p.07
- 基本(Basic)認証でEWS接続 p.09
- 先進認証のOAuthでEWS接続 p.12
- Proxy、拡張、同期設定 p.40
- 配布リストでアドレスリスト取得 p.42
- LDAPでアドレスリスト取得 p.45
- 結果と再起動 p.49



ドメイン 各設定の選択について

「2021年後半より先進認証のみ接続予定」の情報

- OnTimeサーバーがExchangeに接続するにあたってどの認証方法を採用すべきか以下を参考にしてください。
- Exchange Online の基本認証が非推奨となります(Microsoft Docs発行元：2019年9月20日)
<https://docs.microsoft.com/ja-jp/lifecycle/announcements/exchange-online-basic-auth-deprecated>
 - --抜粋--
基本認証に代わり、OAuth 2.0 に基づく先進認証が使用されるようになります。2020年10月には基本認証が廃止されるため、それまでに先進認証をサポートするアプリへ移行することをお勧めします。2020年10月以降は、アプリからExchange Online に接続する際に基本認証を使用できなくなります。
- 先進認証に移行するための新しいリソース(Microsoft Docs 発行元：2020年3月2日)
<https://docs.microsoft.com/ja-jp/lifecycle/announcements/new-resources-modern-authentication>
 - --抜粋--
注: Exchange Online での基本認証の無効化日は、2021年後半まで延期されました。
- 準備ができているならぜひ先進認証方式での接続をしましょう。

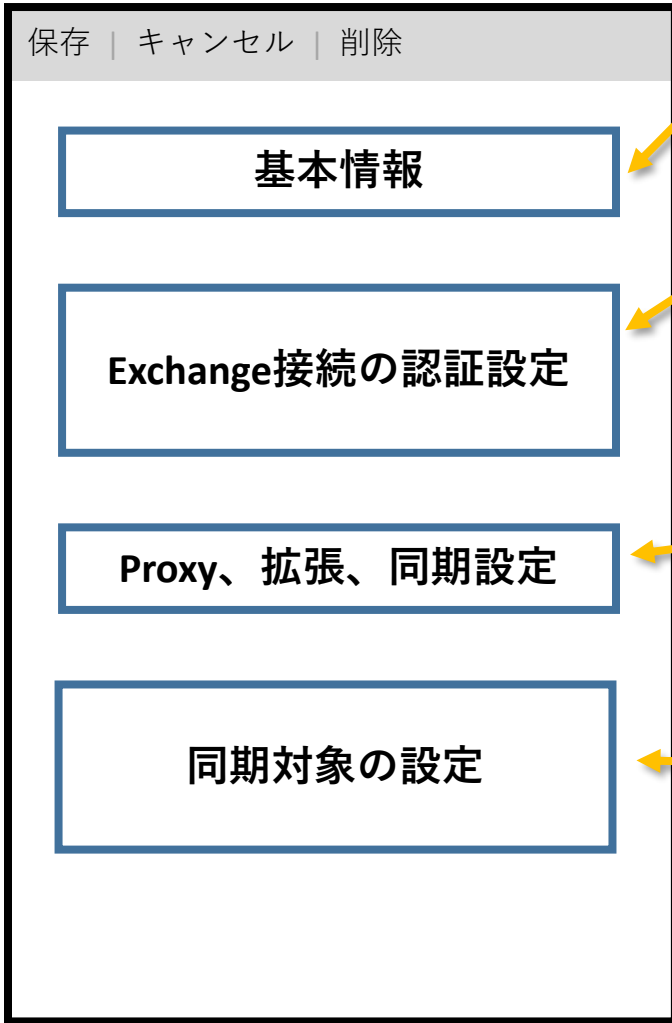
Exchange側の設定準備



- OnTimeはいずれの認証方式を採用するにしてもそのアカウントにはアクセス許可/管理者の役割で偽装ユーザーとしてのロールを付与する必要があります。詳細は以下をご参照ください。
 - 偽装ユーザー(Impersonation User)について
 - OnTime for MicrosoftをExchange OnlineやオンプレのExchangeに接続する際に、全ユーザーをImpersonation(日本語で演技や偽装)してスケジュールデータの入出力を行う1つのアカウントを指します。詳細は以下のURLをご参照ください。
 - Exchange側でのImpersonation Userの設定方法 <https://www3.ontimesuite.jp/impersonation/>
 - 書き込みスコープを制限して特定のメールボックスに制限する方法について
 - 更にテナント運用者とOnTime運用者が違う場合などで厳密に同期対象のメールボックスだけに接続の制限を掛けたい場合は、同期を司るユーザーに割り当てる役割「ApplicationImpersonation」指定時の「書き込みスコープ」を厳密に設定することで明確化が可能です。
 - ドメイン(テナント)の特定のグループのメールボックスだけにOnTimeの利用制限ができますか？ <https://www3.ontimesuite.jp/makescope/>
- 次ページで各ドメインに対しての2つの項目について選択します。
 - 認証方式 準備ができているならOAuthによる先進認証を選択してください。
 - アドレスリスト取得方法 拡張属性などを利用しない場合は配布リストによる取得が簡単です。



ドメイン設定のページ構成



ドメイン名やドメインタイプ、テナントの優先順位など P.7

基本(Basic)認証
ユーザー/パスワードの認証
Exchange Onlineのテスト環境や
オンプレExchange用。 P.9

又は

OAuthによる先進認証
2021年後半にはExchange Online
は先進認証が必須となります。
P.12

Proxy(利用の場合)、拡張設定、同期スレッド数の設定など P.40

配布リスト(グループ)で取得
ExchangeからEWS経由で取得で
きるユーザー属性情報や入れ
子のグループもロールやグ
ループ設定で利用できます。
P.42

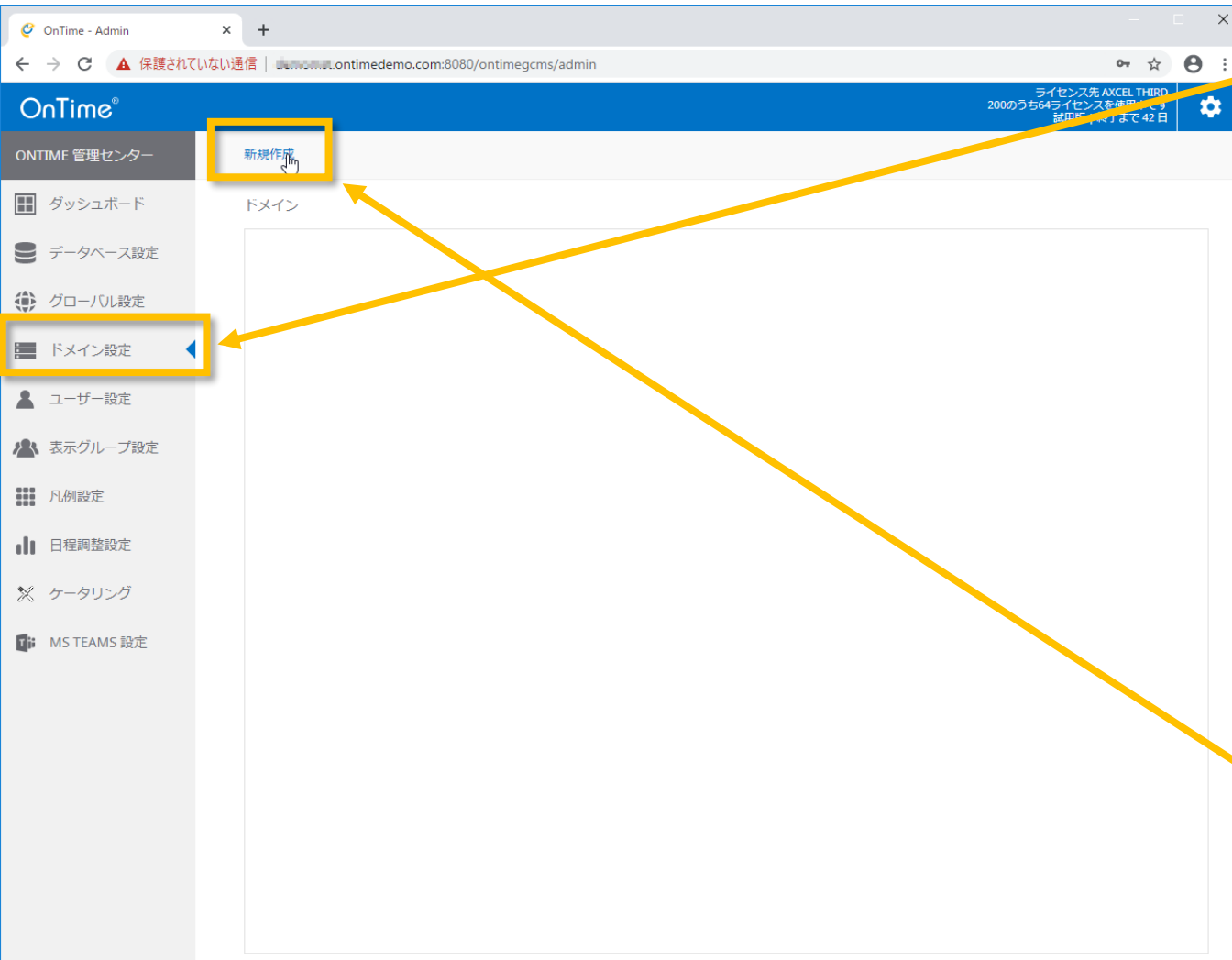
又は

LDAP検索による取得
LDAPで取得する場合は拡張属
性も利用可能です。AzureAD
Connectを利用したExchange
Onlineの環境でもオンプレAD
から取得できます。 P.45



ドメイン 設定画面を開く

ドメイン設定



左サイドメニューで「ドメイン」を選択します。

- ドメインではOnTimeと接続するExchange OnlineまたはオンプレのExchangeサーバーを設定します。
- OnTimeは複数のテナントと接続することも可能です。よってOnTimeサーバーの設置は同じM365のテナントやADメンバー等の必須条件はありません。
- Exchangeドメイン(テナント)に接続するためには必要な条件は、Exchange管理センター/アクセス許可/管理者の役割でOnTimeへの同期対象となるスコープに「ApplicationImpersonation」の役割をもつアカウントを作成し、ネットワーク的に接続できることだけです。

「新規作成」をクリックします。

- 以降のいずれかの認証方法の設定を行います。



ドメイン 基本(Basic)認証でEWS接続

基本認証によるEWS接続 1 (Exchange Online)



OnTime - Admin

保護されていない通信 | ontimedemo.com:8080/ontimegcms/admin

OnTime®

ライセンス先 AXCEL THIRD 200のうち64ライセンスを使用中です 試用版 | 終了まで 42 日

ONTIME 管理センター

保存 | キャンセル | アプリケーションの登録 | 削除

ドメインの編集

ドメイン名: OnTimeDemoCom このドメインを無効

優先順位: 1

ドメインタイプ: クラウド OAuth有効

Impersonation User: [redacted]@ontimedemo.onmicrosoft.com

パスワード: (present)

Proxy

ホスト名: [empty]

ポート番号: [empty]

拡張設定

接続のトレース トレースを有効にすると同期時間が増大するのでご注意ください

同期設定

起動時の同期スレッド数 (?): 5

連続同期スレッド数 (?): 5

同期対象

LDAP LDAPを有効にする

ユーザー: [empty]

会議室: [empty]

- ドメイン名はOnTime 管理センターで識別しやすい名前をつけます。通常はテナント名です。

例: "OnTimeDemoCom" と入力。優先順位: "1" を入力。

- 優先順位は複数のテナントを接続する際、同じメールアドレスのユーザーがいた場合にどちらのドメインを優先するかを決めます。例えば、オンプレとクラウドのハイブリッド環境の移行時に有効です。

一時的に接続しない場合は無効に出来ます。

ドメインタイプでオンプレかクラウドを選択します。Microsoft365(Exchange Online)の場合はクラウドを選択。基本認証の場合はOAuthのチェックはつけません。

接続するテナントで予め準備した Impersonation User とパスワードを入力します。

基本認証によるEWS接続 2 (オンプレExchange)



- ドメイン名はOnTime 管理センターで識別しやすい名前をつけます。通常はテナント名です。

例: "OnTimeDemoCom" と入力。優先順位: "1" を入力。

ドメインタイプでオンプレかクラウドを選択します。
Exchange Serverの場合はオンプレを選択します。

接続するサーバーで予め準備した Impersonation User とパスワードを入力します。
Exchangeのドメインも入力します。

Exchange Serverの情報を入力します。
主となるメールボックスサーバーのアドレスを指定してください。



ドメイン 先進認証のOAuthでEWS接続

先進認証によるEWS接続



- ドメイン名はOnTime 管理センターで識別しやすい名前をつけます。通常はテナント名です。

例:“OnTimeDemoCom”と入力。優先順位:“1”を入力。

ドメインタイプでオンプレかクラウドを選択します。Microsoft365(Exchange Online)の場合はクラウドを選択。OAuth認証にチェックをつけます。

接続するテナントで予め準備した Impersonation User とパスワードを入力します。

- 引き続きOAuth認証のための各種IDの取得のために OnTime管理センターは開いたまま、Azure Portalを新たに開いて Azure Active Directoryの画面に移動します。

アプリの登録 1



The screenshot displays the Azure Portal interface for the 'ontimedemo' tenant. The left-hand navigation pane is visible, with 'アプリの登録' (App Registration) highlighted. The main content area shows the 'ontimedemo' tenant overview, including a search bar for tenants, a 'テナントの情報' (Tenant Information) card, and an 'Azure AD Connect' card. The 'テナントの情報' card lists the role as 'グローバル管理者', the license as 'Azure AD for Office 365', and the primary domain as 'ontimedemo.com'. The 'Azure AD Connect' card shows the status as '無効' (Disabled) and the last sync as '同期は実行されていません' (Sync has not been performed). Below this, there is a 'サインイン' (Sign-in) graph showing user activity over time, and a '作成' (Create) section with icons for 'ユーザー' (User), 'ゲストユーザー' (Guest User), 'グループ' (Group), 'エンタープライズアプリケーション' (Enterprise Application), and 'アプリの登録' (App Registration).

- 利用するTeamsのテナントの Azure Portal に管理者でログインします。
- Azure Portal から Azure Active Directory の「アプリの登録」を開きます。
- 注意)本マニュアルでの構成
 - OAuthを利用するテナントを「ontimedemo.com」としてご説明しています。
 - OnTimeサーバーのホスト名は「ontime.ontimedemo.com」としてご説明しています。

アプリの登録 2



Microsoft Azure portal showing the 'App Registrations' page for 'ontimedemo'. The 'New Registration' button is highlighted with a yellow box. The page displays a list of registered applications:

表示名	アプリケーション (クライアント) ID	作成日	証明書とシークレット
AA Azure AD Domain Services Sync	a1d68f74-14fb-4128-977a-9daf9e03c...	2018/8/11	現在
OT ottdemo	5bdb6c27-3359-4906-82c3-6b40face...	2018/12/28	現在

- 「アプリの登録」で「新規登録」をクリックします。

アプリの登録 3



OnTime - Admin | アプリケーションの登録 - Microsoft Azure

portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/RegisteredApps

Microsoft Azure | リソース、サービス、ドキュメントの検索 (G+)

ホーム > ontimedemo | アプリの登録 > アプリケーションの登録

* 名前
このアプリケーションのユーザー向け表示名 (後で変更できます)。
OnTime-Demo-mst-OAuth

サポートされているアカウントの種類
このアプリケーションを使用するアプリに接続できるのはどれですか?
 この組織ディレクトリのみに含まれるアカウント (ontimedemo のみ - シングル テナント)
 任意の組織ディレクトリ内のアカウント (任意の Azure AD ディレクトリ - マルチテナント)
 任意の組織ディレクトリ内のアカウント (任意の Azure AD ディレクトリ - マルチテナント) と個人の Microsoft アカウント (Skype、Xbox など)

選択に関する詳細...

リダイレクト URI (省略可能)
ユーザー認証が成功すると、この URI に認証応答を返します。この時点での指定は省略可能で、後ほど変更できますが、ほとんどの認証シナリオで値が必要となります。
Web | 例: https://myapp.com/auth

続行すると、Microsoft プラットフォーム ポリシーに同意したことになります

登録

- 「名前」にはエンドユーザーには表示されない名前なので管理上識別しやすい名前を入力します。
- 「サポートされているアカウントの種類」は「この組織ディレクトリのみに含まれるアカウント」を選択します。
- 最後に「登録」をクリックします。

アプリの各IDの設定 1



Microsoft Azure portal showing the configuration page for an application named "OnTime-Demo-mst-OAuth". The "Application (client) ID" field is highlighted with a yellow box, and a tooltip with the text "クリップボードにコピー" (Copy to clipboard) is visible over it. The page also displays the tenant ID, object ID, and supported account types.

- 画面が切り替わったら「アプリケーション(クライアント)ID」をコピーします。

アプリの各IDの設定 2



The screenshot shows the OnTime Admin console interface. The left sidebar contains navigation options: ダッシュボード, データベース設定, グローバリ設定, ドメイン設定 (selected), ユーザー設定, 表示グループ設定, 凡例設定, 日程調整設定, ケータリング, and MS TEAMS 設定. The main content area is titled 'ドメインの編集' and contains the following settings:

- ドメイン名: OnTimeDemoCom
- 優先順位: 1
- ドメインタイプ: クラウド
- Impersonation User: [redacted]@ontimedemo.onmicrosoft.com
- パスワード: [redacted]
- OAuth: OAuth有効
- アプリケーション ID: [redacted] (highlighted with a yellow box)
- ディレクトリ(テナント)ID: [redacted]
- クライアントシークレット: [redacted]
- Proxy: Hostname and Port fields are empty.
- 拡張設定: トレースを有効にすると同期時間が増大するのでご注意ください
- 同期設定: 起動時の同期スレッド数 (?) is 5, 連続同期スレッド数 (?) is 5.

- コピーした「アプリケーション(クライアント)ID」をOnTime管理センターの該当箇所に貼り付けます。

アプリの各IDの設定 3



The screenshot shows the Azure portal interface for an application named "OnTime-Demo-mst-OAuth". The "ディレクトリ (テナント) ID" field is highlighted with a yellow box, and a tooltip "クリップボードにコピー" is visible over it. The page includes sections for "API の呼び出し" and "ドキュメント".

- 同じく「ディレクトリ(テナント)ID」をコピーします。

アプリの各IDの設定 4



The screenshot shows the OnTime Admin console interface. The left sidebar contains navigation options: ダッシュボード, データベース設定, グローバリシ設定, ドメイン設定 (selected), ユーザー設定, 表示グループ設定, 凡例設定, 日程調整設定, ケータリング, MS TEAMS 設定. The main content area is titled 'ドメインの編集' and includes fields for: ドメイン名 (OnTimeDemoCom), 優先順位 (1), ドメインタイプ (クラウド), Impersonation User, パスワード, OAuth (Application ID, Directory (tenant) ID, Client secret), Proxy (Host name, Port number), 拡張設定 (Tracing), and 同期設定 (Startup sync thread count, Continuous sync thread count). The 'Directory (tenant) ID' field is highlighted with a yellow box.

- コピーした「ディレクトリ(テナント)ID」をOnTime管理センターの該当箇所に貼り付けます。

認証の設定 1



OnTime - Admin | OnTime-Demo-mst-OAuth - Mic

portal.azure.com/#blade/Microsoft_AAD_RegisteredApps/ApplicationMenuBlade/Overview/quickStartType//sourceType/Microsoft_AAD_IAM/applid/...

Microsoft Azure | リソース、サービス、ドキュメントの検索 (G+)

ホーム > ontimedemo | アプリの登録 >

OnTime-Demo-mst-OAuth

検索 (Ctrl+/) | 削除 | エンドポイント

表示名 OnTime-Demo-mst-OAuth	サポートされているアカウントの種類 所属する組織のみ
アプリケーション (クライアント) ID f8d...	リダイレクト URI リダイレクト URI を追加する
ディレクトリ (テナント) ID b9d...	アプリケーション ID の URI アプリケーション ID URI の追加
オブジェクト ID d4d...	ローカル ディレクトリでのマネージド アプリケーション OnTime-Demo-mst-OAuth

新しく強化されたアプリの登録へようこそ。アプリの登録 (レガシ) からの変更点を確認することをご希望ですか? [詳細情報](#)

APIの呼び出し

Microsoft サービスと自社の独自のデータ ソースからの豊富なユーザーデータおよびビジネス データを使用して、より強力なアプリを作成します。

[API アクセス許可の表示](#)

ドキュメント

- Microsoft ID プラットフォーム
- 認証シナリオ
- 認証ライブラリ
- コードサンプル
- Microsoft Graph 用語集
- ヘルプとサポート

5 分以内にユーザーをサインインする

- 「認証」タブに移動します。

認証の設定 2



The screenshot shows the Azure portal interface for configuring authentication. The page title is 'OnTime-Demo-mst-OAuth | 認証'. The main content area is titled 'プラットフォーム構成' (Platform Configuration). A yellow box highlights the '+ プラットフォームを追加' (Add Platform) button. Below this, there are sections for 'サポートされているアカウントの種類' (Supported account types) and '既定のクライアントの種類' (Default client types). The 'Supported account types' section has two radio buttons: 'この組織ディレクトリのみに含まれるアカウント (ontimedemo のみ - シングルテナント)' (Selected) and '任意の組織ディレクトリ内のアカウント (任意の Azure AD ディレクトリ - マルチテナント)'. The 'Default client types' section has a dropdown menu set to '既定のクライアントの種類' and a 'はい' (Yes) button. At the bottom, there are three links: 'リソース所有者のパスワード資格情報 (ROPC) 詳細情報' (ROPC), 'デバイスコードフロー 詳細情報' (Device Code Flow), and '統合 Windows 認証 (IWA) 詳細情報' (IWA).

- 「プラットフォームを追加」ボタンをクリックします。

認証の設定 3



プラットフォームの構成

Web

Web サーバー アプリケーションをビルド、ホスト、デプロイします。 .NET、Java、Python

シングルページ アプリケーション

ブラウザ クライアント アプリケーションとプロGRESSIVE Web アプリケーションを構成します。 JavaScript。

モバイル アプリケーションとデスクトップ アプリケーション

iOS または macOS

Objective-C、Swift、Xamarin

Android

Java、Kotlin、Xamarin

モバイル アプリケーションとデスクトップ アプリケーション

Windows、UWP、コンソール、IoT & 入力制限デバイス、クラシック iOS と Android

- 「Web」をクリックします。

認証の設定 4



- Webの構成が開きます。

リダイレクトURIには
http://localhost:8080/ontimegcms/redirect.html
と入力してください。

アクセストークン
IDトークン
の両方にチェックをつけます。

「構成」をクリックします。

クライアントシークレットの設定 1



OnTime - Admin | OnTime-Demo-mst-OAuth | 認証

portal.azure.com/#blade/Microsoft_AAD_RegisteredApps/ApplicationMenuBlade/Authentication/quickStartType//sourceType/Microsoft_AAD_IAM/applid/fe... 3-...

Microsoft Azure | リソース、サービス、ドキュメントの検索 (G+)

ホーム > ontimedemo | アプリの登録 >

OnTime-Demo-mst-OAuth | 認証

検索 (Ctrl+/) | 保存 | 破棄 | フィードバックがある場合

概要

プラットフォーム構成

このアプリケーションが対象としているプラットフォームまたはデバイスによっては、リダイレクト URI、特定の認証設定、プラットフォームに特有のフィードバックなど追加構成が必要となる場合があります。

管理

+プラットフォームを追加

プラットフォーム

Web

リダイレクト URI

ユーザー認証に成功した後に認証応答 (トークン) を返すときに宛先として受け入れる URI。応答 URL と呼ばれます。リダイレクト URI と制限の詳細情報

このアプリでは、暗黙的な許可の設定が有効になっています。MSAL.js 2.0 を使用した SPA にこれらの URI を使用している場合は、URI を移行する必要があります。→

http://localhost:8080/ontimegcms/redirect.html

URI の追加

ログアウト URL

ここでは、アプリケーションがユーザーのセッション データをクリアするように要求を送信します。これは、シングル サインアウトが正常に動作するために必要です。

例: https://myapp.com/logout

暗黙の付与

アプリケーションが承認エンドポイントから直接トークンを要求することを許可します。アクセストークンと ID トークンの確認が推奨されるのは、アプリケーションがシングルページ アプリケーション (SPA) を備えている場合、バックエンド コンポーネントがなく認証コード フローで MSAL.js の最新バージョンを使用していない場合、JavaScript を使用して Web API を呼び出す場合だけです。ASP.NET Core Web アプリには ID トークンが必要です。暗黙的な許可フローの詳細

- 「証明書とシークレット」タブに移動します。

クライアントシークレットの設定 2



The screenshot shows the Azure portal interface for 'OnTime-Demo-mst-OAuth'. The left sidebar contains navigation options like 'Home', 'OnTime-Demo | App registration', 'Certificates and secrets', 'Tokens', 'API access', 'API public', 'Owners', 'Roles and administrators', and 'Manifests'. The main content area is titled 'Certificates and secrets' and includes sections for 'Certificates' and 'Client secrets'. The 'Client secrets' section has a yellow box around the '+ New client secret' button. Below it is a table with columns for 'Name', 'Expiration date', and 'Value'. The text below the table states: 'このアプリケーションのクライアント シークレットは作成されていません。'

- こちらはOnTimeサーバーがアクセスする際に自身のIDを証明する為の「クライアントシークレット」を作成します。
- 「クライアントシークレット」は「アプリケーションパスワード」と呼ばれることもあります。
- 「新しいクライアントシークレット」をクリックします。

クライアントシークレットの設定 3



- 「クライアントシークレットの追加」ダイアログが開きます。
- 「説明」には識別しやすい名前を入力します。
- 「有効期限」は「なし」を選択します。
- 内容がよろしければ「追加」ボタンをクリックします。

クライアントシークレットの設定 4



新しいクライアント シークレット値をコピーしてください。別の操作を実行したり、このブレードから移動したりすると、それを取ることができなくなります。

資格情報は、Web アドレスの指定が可能な場所で (HTTPS スキーマを使用して) トークンを受信する際に、機密性の高いアプリケーションが認証サービスに対して自身を識別できるようにするためのものです。より高いレベルで保証するには、資格情報として (クライアント シークレットではなく) 証明書を使うことをお勧めします。

証明書
証明書は、トークンの要求時にアプリケーションの ID を証明するシークレットとして使用できます。公開キーとも呼ばれます。

↑ 証明書のアップロード

拇印	開始日	有効期限
このアプリケーションには証明書が追加されていません。		

クライアント シークレット
トークンの要求時にアプリケーションが自身の ID を証明するために使用する秘密の文字列です。アプリケーション パスワードと呼ばれることもあります。

+ 新しいクライアント シークレット

説明	有効期限	値
OnTimeOAuth	2299/12/31	4... [クリップボードにコピー]

- 先ほどの画面上に作成した「クライアントシークレット」が表示されています。
- 「値」をコピーします。
- 「値」はこのタイミングでコピーしないと二度と取得できないのでご注意ください。

クライアントシークレットの設定 5



The screenshot shows the OnTime Admin console interface. The left sidebar contains navigation options: ダッシュボード, データベース設定, グローバリ設定, ドメイン設定 (selected), ユーザー設定, 表示グループ設定, 凡例設定, 日程調整設定, ケータリング, and MS TEAMS 設定. The main content area is titled 'ドメインの編集' and contains the following fields:

- ドメイン名: OnTimeDemoCom
- 優先順位: 1
- ドメインタイプ: クラウド
- Impersonation User: [redacted]@ontimedemo.onmicrosoft.com
- パスワード: [redacted]
- OAuth: OAuth有効
- アプリケーション ID: [redacted]
- ディレクトリ(テナント)ID: [redacted]
- クライアントシークレット: 46A... (highlighted with a yellow box)
- Proxy: Hostname and Port fields.
- 拡張設定: トレースを有効にすると同期時間が増大するのでご注意ください
- 同期設定: 起動時の同期スレッド数 (?) 5, 連続同期スレッド数 (?) 5

- コピーした「クライアントシークレット」をOnTime管理センターの該当箇所に貼り付けます。

APIのアクセス許可 1



Microsoft Azure | リソース、サービス、ドキュメントの検索 (G+/)

ホーム > ontimedemo | アプリの登録 >

OnTime-Demo-mst-OAuth | 証明書とシークレット

資格情報は、Web アドレスの指定が可能な場所で (HTTPS スキーマを使用して) トークンを受信する際に、機密性の高いアプリケーションが認証サービスに対して自身を識別できるようにするためのものです。より高いレベルで保証するには、資格情報として (クライアント シークレットではなく) 証明書を使うことをお勧めします。

証明書

証明書は、トークンの要求時にアプリケーションの ID を証明するシークレットとして使用できます。公開キーとも呼ばれます。

[証明書のアップロード](#)

拇印	開始日	有効期限
このアプリケーションには証明書が追加されていません。		

クライアント シークレット

トークンの要求時にアプリケーションが自身の ID を証明するために使用する秘密の文字列です。アプリケーション パスワードと呼ばれることもあります。

[新しいクライアント シークレット](#)

説明	有効期限	値
OnTimeOAuth	2299/12/31	4d...

APIのアクセス許可

- 「APIのアクセス許可」タブに移動します。

APIのアクセス許可 2



Microsoft Azure portal screenshot showing the 'APIのアクセス許可' (API Access Permissions) page for 'OnTime-Demo-mst-OAuth'. The page displays a table of permissions for 'Microsoft Graph (1)'. A red box highlights the '+ アクセス許可の追加' (Add access permission) button.

API / アクセス許可の名前	種類	説明	管理者の同意が必要	状態
Microsoft Graph (1)				
User.Read	委任済み	Sign in and read user profile	-	...

- こちらはOnTimeサーバーがAzureADにアクセスする内容を定義します。
- 「アクセス許可の追加」ボタンをクリックします。

APIのアクセス許可 3



API アクセス許可の要求

API を選択します

Microsoft API 所属する組織で使用している API 自分の API

その他の Microsoft API

- Azure Batch
- Azure Data Catalog
- Azure Data Explorer
- Azure Data Explorer (with Multifactor Authentication)
- Azure Data Lake
- Azure DevOps
- Azure Import/Export
- Azure Key Vault
- Azure Rights Management Services
- Customer Insights
- Dynamics ERP
- Speech
- Universal Print

- 「APIアクセス許可の要求」ページが開くので一番下までスクロールします。

APIのアクセス許可 4



The screenshot shows the Microsoft Azure portal interface. The main content area is titled "API アクセス許可の要求" (API Access Permissions). It features a grid of service tiles, each with an icon and a brief description of the permissions it provides. The services listed include Dynamics 365 Business Central, Dynamics CRM, Flow Service, Intune, Office 365 Management APIs, OneNote, Power BI Service, PowerApps Runtime Service, SharePoint, Skype for Business, and Yammer. Below this grid, there is a section titled "サポートされているレガシ API" (Supported legacy APIs). In this section, the "Exchange" service tile is highlighted with a yellow border. The Exchange tile includes the text: "Exchange データにアクセスして操作するための強力な使いやすい方法" (Powerful and easy way to access and operate Exchange data).

- 「Exchange」をクリックします。

APIのアクセス許可 5



The screenshot shows the 'API Access Requirements' page in the Azure portal. The left sidebar contains navigation options like 'API の公開', '所有者', and 'API のアクセス許可'. The main content area shows a list of permissions for the 'Exchange' application. The 'Delegated permissions' section is highlighted with a yellow box, and a mouse cursor is pointing at the 'Delegated permissions' link.

- 「委任されたアクセス許可」をクリックします。

APIのアクセス許可 6



- アクセス許可の選択肢が下に展開されるので「EWS」を更に展開します。

「EWS.AccessAsUser.All」をチェックします。

APIのアクセス許可 7



- 「アクセス許可の追加」をクリックします。

APIのアクセス許可 8



OnTime - Admin | OnTime-Demo-mst-OAuth | API

portal.azure.com/#blade/Microsoft_AAD_RegisteredApps/ApplicationMenuBlade/CallAnAPI/quickStartType//sourceType/Microsoft_AAD_IAM/appld/f...

Microsoft Azure | リソース、サービス、ドキュメントの検索 (G+/)

ホーム > ontimedemo | アプリの登録 >

OnTime-Demo-mst-OAuth | API のアクセス許可

検索 (Ctrl+/) | 最新の情報に更新

概要

▲ アプリケーションに対するアクセス許可を編集しています。ユーザーは、既に同意したことがある場合でも同意が必要になります。

構成されたアクセス許可

アプリケーションは、同意のプロセスの一環としてユーザーが管理者からアクセス許可が付与されている場合、API を呼び出すことが承認されます。構成されたアクセス許可の一覧には、アプリケーションに必要なすべてのアクセス許可を含める必要があります。 [アクセス許可と同意に関する詳細情報](#)

+ アクセス許可の追加 | **ontimedemo に管理者の同意を与えます**

API / アクセス許可の名前	種類	説明	管理者の同意が必要	状態
▼ Exchange (1)				
EWS.AccessAsUser.All	委任済み	Access mailboxes as the signed-in user via Exchange...	-	...
▼ Microsoft Graph (1)				
User.Read	委任済み	Sign in and read user profile	-	...

- 「"ドメイン名"に管理者の同意を与えます」ボタンをクリックします。

APIのアクセス許可 9



portal.azure.com/#blade/Microsoft_AAD_RegisteredApps/ApplicationMenuBlade/CallAnAPI/quickStartType//sourceType/Microsoft_AAD_IAM/applid/f...

Microsoft Azure リソース、サービス、ドキュメントの検索 (G+)

ホーム > ontimedemo | アプリの登録 >

OnTime-Demo-mst-OAuth | API のアクセス許可

検索 (Ctrl+/) << 最新の情報に更新

概要

クイック スタート

統合アシスタント (プレビュー)

管理

ブランド

認証

証明書とシークレット

トークン構成

API のアクセス許可

API の公開

所有者

ロールと管理者 (プレビュー)

マニフェスト

サポート + トラブルシューティング

トラブルシューティング

新しいサポート リクエスト

ontimedemo のすべてのアカウントについて、要求されたアクセス許可に対する同意を付与しますか? この操作により、このアプリケーションが既に持っている既存の管理者の同意レコードが、以下の一覧の内容に一致するよう更新されます。

はい いいえ

+ アクセス許可の追加 ontimedemo に管理者の同意を与えます

API / アクセス許可の名前	種類	説明	管理者の同意が必要	状態
Exchange (1)				
EWS.AccessAsUser.All	委任済み	Access mailboxes as the signed-in user via Exchange...	-	...
Microsoft Graph (1)				
User.Read	委任済み	Sign in and read user profile	-	...

- 確認画面では「はい」をクリックします。

APIのアクセス許可 1 0



Microsoft Azure portal showing API access permissions for 'OnTime-Demo-mst-OAuth'. A notification at the top states 'Required access permissions have been granted by the administrator.' The table below shows permissions for 'Exchange (1)' and 'Microsoft Graph (1)'. The 'User.Read' permission is highlighted with a yellow box, and its status is 'Granted to ontimedemo'.

API / アクセス許可の名前	種類	説明	管理者の同意が必要	状態
Exchange (1)				
EWS.AccessAsUser.All	委任済み	Access mailboxes as the signed-in user via Exchange...	-	ontimedemo に付与され...
Microsoft Graph (1)				
User.Read	委任済み	Sign in and read user profile	-	ontimedemo に付与され...

- 無事に付与されます。
- もし付与されない場合はAzureグローバル管理者に連絡してご確認ください。



ドメイン Proxy、拡張、同期設定

ドメイン設定（共通部分）



OnTime - Admin

OnTime-Demo-mst-OAuth | 証明 | +

保護されていない通信 | ontimedemo.com:8080/ontimegcms/admin

ライセンス先 AXCEL THIRD
200のうち64ライセンスを使用中です
試用版 | 終了まで 42日

ONTIME 管理センター

保存 | キャンセル | アプリケーションの登録 | 削除

ドメインの編集

ドメイン名: OnTimeDemoCom このドメインを無効

優先順位: 1

ドメインタイプ: クラウド OAuth有効

Impersonation User: [redacted]@ontimedemo.onmicrosoft.com

パスワード: [redacted]

OAuth

アプリケーション ID: [redacted]

ディレクトリ(テナント)ID: [redacted]

クライアントシークレット: [redacted]

Proxy

ホスト名: [redacted]

ポート番号: [redacted]

拡張設定

接続のトレース トレースを有効にすると同期時間が増大するのでご注意ください

同期設定

起動時の同期スレッド数 (?) 5

連続同期スレッド数 (?) 5

- Proxyをご利用の場合はProxy設定を行います。
- 拡張設定は変更しません。サポートから依頼があった場合のみ設定してください。
- 同期設定では「起動時」「通常運用時」それぞれのスレッド数を指定できます。
 - Exchange上のイベント更新情報がOnTimeに反映されるのが遅い場合はOnTimeの同期処理がExchange上のイベント更新頻度に追いついていない可能性があります。そのような場合にスレッド数を増やすことで改善する場合があります。
 - 最小数は5です。
 - OnTimeサーバーのCPUやメモリに十分なパワーがある場合はCPUやメモリの使用率を見ながら徐々に数値を変更してみてください。
 - 1000人規模のユーザー数の場合は5程度、8000人規模で25程度に設定します。



ドメイン 配布リストでアドレスリスト取得

配布リストでアドレスリストを取得 1



- 同期対象は「LDAP」か「グループメールアドレス」のどちらかで指定します。
- 本章ではグループのメールアドレスで指定します。

“LDAPを有効にする”のチェックを外します。

- 次にOnTimeと同期するリストをグループ化した配布グループ(配布リスト)のメールアドレスを指定します。
- OnTimeで表示する、または操作できるいずれの場合でも含まれている必要があります。

ドメインのユーザー、会議室、備品のそれぞれに指定されている配布グループ(配布リスト)のメールアドレスを指定します。複数の場合はカンマで区切ってください。

配布リストでアドレスリストを取得 2



OnTime - Admin | ontimedemo | アプリの登録 - Micr... | +

保護されていない通信 | ontimedemo.com:8080/ontimegcms/admin

OnTime® | ライセンス先 AXCEL THIRD | 200のうち64ライセンスを使用中です | 試用版 | 終了まで 42日

ONTIME 管理センター | 保存 | キャンセル | アプリケーションの登録 | 削除

ドメインの編集

ドメイン名: OnTimeDemoCom このドメインを無効

優先順位: 1

ドメインタイプ: クラウド OAuth有効

Impersonation User: [redacted]@ontimedemo.onmicrosoft.com

パスワード: [redacted]

OAuth

アプリケーション ID: [redacted]

ディレクトリ(テナント)ID: [redacted]

クライアントシークレット: [redacted]

Proxy

ホスト名: [redacted]

ポート番号: [redacted]

拡張設定

接続のトレース トレースを有効にすると同期時間が増大するのでご注意ください

同期設定

起動時の同期スレッド数 (?): 5

連続同期スレッド数 (?): 5

- 設定した配布グループが入れ子になっていても問題ありません。また入れ子になっているグループもOnTime管理センターのその他の設定（ルール設定や静的グループ設定）などで利用できます。

設定後は「保存」をクリックします。

- ちなみにOnTimeは複数のテナントと接続することも可能です。よってOnTimeサーバーはいずれのテナントに所属してなくても問題ございません。



ドメイン LDAPでアドレスリスト取得

LDAPでアドレスリスト取得 1



The screenshot shows the OnTime Admin console interface. The left sidebar contains navigation options: ダッシュボード, データベース設定, グローバル設定, ドメイン設定, ユーザー設定, 表示グループ設定, 凡例設定, 日程調整設定, ケータリング, and MS TEAMS 設定. The main content area is titled 'ドメインの編集' (Edit Domain) and contains the following fields and options:

- ドメイン名: LDAP
- 優先順位: 2
- ドメインタイプ: クラウド
- Impersonation User: [redacted]@ontimedemo.com
- パスワード: (present)
- Proxy: Hostname and Port fields.
- 拡張設定: トレースの有効にする (checkbox, unchecked).
- 同期設定: 起動時の同期スレッド数 (5), 連続同期スレッド数 (5).
- 同期対象: LDAP (checkbox, checked) - A yellow arrow points to this checkbox from a text box on the right.
- URL: ldap://obizad.ontime.otbz:389
- ユーザー: CN=Administrator, CN=Users, DC=ontime, DC=otbz

- OnTimeはExchangeと連携しているActive DirectoryからLDAP(S)により同期対象を指定することもできます。
- LDAP(S)を使用することでExchangeのEWS接続では取得できない情報、例えばフリガナ属性やカスタム属性1～15なども取得してOnTimeで活用できます。
- Microsoft365のExchange Online接続であってもAzureAD Connectを使用してAD連携しているのであれば利用可能です。
- ちなみにOnTimeは複数のテナントと接続することも可能です。よってActive DirectoryはOnTimeが稼働するテナントである必要はありません。LDAP(S)で接続できればいずれのテナントも利用可能です。

“LDAPを有効にする”のチェックをします。

LDAPでアドレスリスト取得 2



- 同期対象の設定を行います。

Active DirectoryへのLDAP接続用アカウントの設定です。
事前にldp.exe等で接続確認を行ってください。

接続先ドメインのユーザー、会議室、備品のそれぞれを検索するフィルター条件を指定してください。
次ページにサンプルがあります。

設定後は「保存」をクリックします。

LDAPでアドレスリスト取得 3



同期対象	<input checked="" type="checkbox"/> LDAPを有効にする
LDAP	<input checked="" type="checkbox"/> LDAPを有効にする
URL	ldap://[redacted].ontime.otbz:389
ユーザー	CN=[redacted], CN=Users, DC=ontime, DC=otbz
パスワード
	<input type="button" value="テスト"/>
ベース	OU=o365, DC=ontime, DC=otbz
スコープ	SUB_TREE
フィルター	(cn=*)
	<input type="button" value="テスト"/>
ベース	OU=o365, DC=ontime, DC=otbz
スコープ	SUB_TREE
フィルター	(mail=*)

同期対象	<input checked="" type="checkbox"/> LDAPを有効にする
LDAP	<input checked="" type="checkbox"/> LDAPを有効にする
URL	ldap://[redacted].ontime.otbz:389
ユーザー	CN=[redacted], CN=Users, DC=ontime, DC=otbz
パスワード
	<input type="button" value="テスト"/>
ベース	OU=o365, DC=ontime, DC=otbz
スコープ	ONE_LEVEL
フィルター	(cn=OnTimeRooms)
	<input type="button" value="テスト"/>
ベース	OU=o365, DC=ontime, DC=otbz
スコープ	ONE_LEVEL
フィルター	(mail=OnTimePersons)

- 左図を参考に組織に応じたフィルター条件で取得してください。
- 左上 特定の属性に値があるアカウントを全て取得
- 右下 特定のグループに属しているアカウントを全て取得
- 取得したリストにグループが含まれている場合はそのグループをロール設定などで利用できます。



ドメイン 結果と再起動

設定したドメインリストについて



The screenshot shows the OnTime Admin interface. The left sidebar contains navigation options: ダッシュボード, データベース設定, グローバル設定, ドメイン設定, ユーザー設定, 表示グループ設定, 凡例設定, 日程調整設定, ケータリング, and MS TEAMS 設定. The main content area is titled '新規作成' (New Creation) and 'ドメイン' (Domain). It displays a table of domains:

Domain Name	Status	Last Updated
OnTimeDemoCom	RUNNING	2024/07/20 10:00:00
LDAP	NOT_STARTED	2024/07/20 10:00:00

A yellow box highlights the 'LDAP' row, and a yellow arrow points to the 'NOT_STARTED' status.

- 保存を押すと先ほど設定したドメインが増えていきます。

アプリケーションを再起動するまで“NOT_STARTED”と表示されます。
修正する場合はクリックすることで編集画面が表示されます。修正した場合はOnTimeアプリケーションの再起動が必要です。

- アプリケーションを再起動するためには“ダッシュボード”に移動します。
- 続いて設定マニュアルでそのほかの設定をします。