



# OnTime<sup>®</sup> GROUP CALENDAR

for Microsoft(Ver.5.1-)

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

2022/06/06

# 目次 ドメイン設定マニュアル



- ドメイン設定の概要について p.03
- 各認証方式について p.06
- **Azure Portal(AzureAD)での作業**
  - アプリの登録 p.12
  - 各IDの取得/認証の設定 p.17
  - クライアントシークレットの設定 p.21
  - APIのアクセス許可 p.26
- **OnTime管理センター ドメイン設定での作業**
  - ドメイン設定 p.45
  - Exchangeタブ p.46
  - 同期対象タブ p.48
  - Proxyタブ p.49
  - 属性マッピングタブ p.50
  - 高度な設定タブ p.51
  - 保存結果と再起動 p.52
- 補足1) 認可コードフロー認証方式の設定 p.54
- 補足2) オンプレExchange/基本認証の設定 p.62
- 補足3) 同期対象をLDAPで設定 p.65
- 補足4) Graphの認証エラーについて p.69



# ドメイン設定の概要について

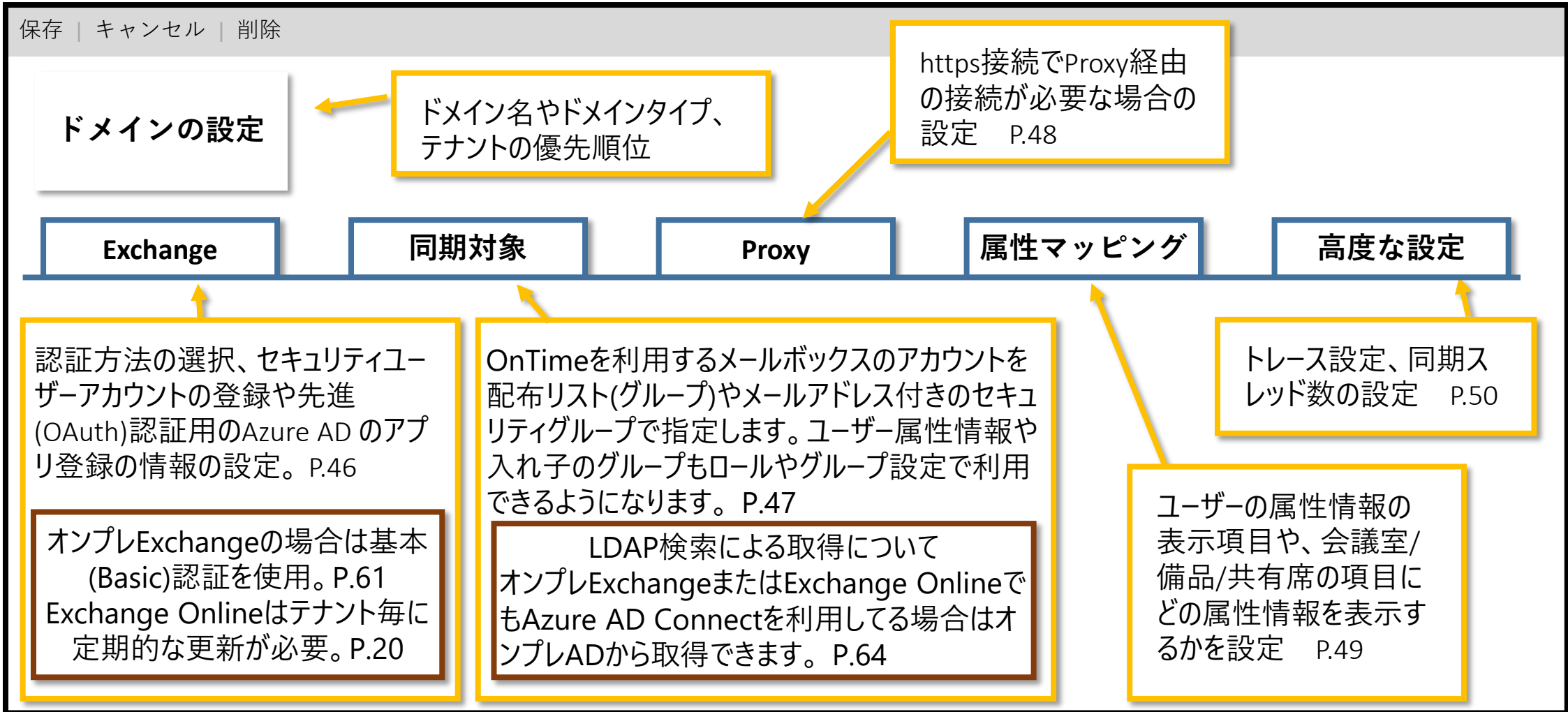


# ドメイン設定について

- ドメイン設定では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（Exchangeドメイン）と接続することも可能です。
- 接続するテナント毎にドメイン設定を行います。
- OnTimeサーバーの設置やドメインは同じM365のテナントやADメンバー等の必須条件はありません。
- 本マニュアルの各手順で設定する内容は以下の通りです。
  - Azure Portal(Azure AD)での作業について
    - Microsoft Graph接続用に「アプリの登録」を設定します。
  - OnTime管理センターでの作業について
    - 接続するテナントへの接続及び認証方法を設定します。
    - 同期するメンバーのソース情報を設定します。
    - 次ページにドメイン設定ページの構成概略図を表示します。
- その他補足事項



# ドメイン設定のページ構成





# 各認証方式について

# 「2021年後半より先進認証のみ接続予定」の情報

2021年2月に情報が追加されています。次頁参照

- OnTime が Microsoft365 (Exchange Online) と先進認証(OAuth)で接続する際は Azure Portal で「アプリの登録」を行う必要があります。以下の情報を参考に認証方式は先進認証(OAuth)を採用してください。
- 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。
- Ver.4.1.0 より Microsoft Teams と連携させるためには OAuth認証は必須となりました。
- Ver.4.1.0 より 会議室のビル階数や定員などを取得できるようになりましたが OAuth認証の場合だけです。

# 「先進認証のみの接続予定」の2021年2月情報



2021年9月に情報が追加されています。次頁参照

- 改めて案内するまで、テナントが基本認証を利用している場合は無効にしない。また無効にするまで遅くとも12ヶ月前には案内する。(Microsoft Exchange Team Blog 2021年02月04日)  
<https://techcommunity.microsoft.com/t5/exchange-team-blog/basic-authentication-and-exchange-online-february-2021-update/ba-p/2111904>
  - --抜粋--
  - 改めて案内するまで、テナントが基本認証を利用している場合は無効にしません。また無効にする際12ヶ月前には案内します。
  - 但し、基本認証を利用していない場合は間違えて使用しないよう無効にします。これはテナントのプロトコル使用状況を調査のうえ30日前にメッセージセンターに通知されます。基本認証の無効化は新規テナントのデフォルト設定にも含まれます。
  - 通知を受けてからも連絡をすれば除外対応が可能で、通知を見逃して基本認証が無効になっても再度有効にできる機能を準備予定です。
- とはいえ、OnTime は Ver.4.1.0 より Microsoft Teams と連携させるためには OAuth認証は必須となりました。
- また、Ver.4.1.0 より 会議室のビル階数や定員などを取得できるようになりましたが OAuth認証の場合だけです。
- OnTime が Microsoft365 (Exchange Online) と先進認証(OAuth)で接続する際は Azure Portal で「アプリの登録」を行う必要があります。可能であれば本マニュアルを参考に認証方式は先進認証(OAuth)を採用してください。



# 「先進認証のみの接続予定」の2021年9月情報



2022年5月に情報が追加されています。次頁参照

- 2022年10月1日より、SMTP認証を除くすべてのテナントで、使用状況に関係なく、基本認証を恒久的に無効にすることを発表する。(Microsoft Exchange Team Blog 2021年09月23日)  
<https://techcommunity.microsoft.com/t5/exchange-team-blog/basic-authentication-and-exchange-online-september-2021-update/ba-p/2772210>
  - --抜粋--
  - 無効になる範囲も拡張され、Exchange Webサービス(EWS)、Exchange ActiveSync(EAS)、POP、IMAP、リモートPowerShell、MAPI、RPC、SMTP AUTH、およびOABが含まれるようになりました。
  - 2022年の第2四半期中に、テナントを選択的に選択されSMTP AUTHを除くすべての影響を受けるプロトコルの基本認証を12～48時間無効にする検証が行われます。この後、テナント管理者がセルフサービスツールを使用してプロトコルを再度有効にしている場合は、これらのプロトコルの基本認証が再度有効になります。
  - 2022年9月開始まで、各プロトコル（Outlookの場合はプロトコルのセット）ごとにオプトアウトをリクエストすることができます。しかし2022年9月1日からはオプトアウトのオプションを削除し、2022年10月1日からは利用状況にかかわらずすべてのテナントで基本認証がオフになります。
- いずれにせよ、OnTime は Ver.4.1.0 より Microsoft Teams と連携させるためには OAuth認証は必須となりました。
- また、Ver.4.1.0 より 会議室のビル階数や定員などを取得できるようになりましたが OAuth認証の場合だけです。
- OnTime が Microsoft365 (Exchange Online) と先進認証(OAuth)で接続する際は Azure Portal で「アプリの登録」を行う必要があります。可能であれば本マニュアルを参考に認証方式は先進認証(OAuth) を採用してください。

# 「先進認証のみの接続予定」の2022年5月情報



- 2022年10月1日より、世界中のマルチテナントサービスでExchange Onlineでの基本認証をオフにします。  
(Microsoft Exchange Team Blog 2022年05月03日)  
<https://techcommunity.microsoft.com/t5/exchange-team-blog/basic-authentication-deprecation-in-exchange-online-may-2022/ba-p/3301866>
  - --抜粋--
  - 無効になるのはMAPI、RPC、Offline Address Book (OAB)、Exchange Web Services (EWS)、POP、IMAP、Exchange ActiveSync (EAS)、Remote PowerShellです。SMTP AUTHは除外されています。
  - 実際は10月1日から開始されます。但し一斉にではなく、テナントがランダムに選択され、メッセージセンターとサービスヘルスダッシュボードで7日間の警告が行われてから、テナントの基本認証をオフにします。
  - これは今年の終わりまでに完了する予定です。。
- いずれにせよ、OnTime は Ver.4.1.0 より Microsoft Teams と連携させるためには OAuth認証は必須です。
- 同じくOAuth認証の場合だけ会議室のビル階数や定員などを取得できるような機能拡張を行っています。
- OnTime が Microsoft365 (Exchange Online) と先進認証(OAuth)で接続する際は Azure Portal で「アプリの登録」を行う必要があります。10月1日迄に必ずマニュアルを参考に認証方式は先進認証(OAuth) を採用してください。

# 認証方式に「クライアント資格情報フロー」を追加



- Ver.5.0.0よりExchange Onlineとの接続認証方式に「先進認証(OAuth - Client資格情報フロー - Client Credentials)」を追加しました。
- この方式は「先進認証(OAuth - 認可コードフロー - Impersonation User)」と違い同期を司るユーザーに対象となるメールボックスへのApplication Impersonationの管理者役割を必要としない方式となります。
- Microsoftの推奨ともなりますので、既存のお客様も含め今後はこの方式に順次切り替えをお願いいたします。
- Microsoft Graphと接続する場合はOnTimeサーバーもパブリック認証局の証明書取得をお願いいたします。詳細は以下のFAQを参照ください。
  - <https://www3.ontimesuite.jp/using-teams-desktop/>
- 本マニュアルではこの「先進認証(OAuth - Client資格情報フロー - Client Credentials)」を手順としてご紹介し、補足ページとして従来の認証方式についてご案内します。
  - 補足1で「先進認証(OAuth - 認可コードフロー - Impersonation User)」 P.53
  - 補足2でオンプレExchange Serverでも利用する「基本認証(BASIC)」 P.61



# Azure Portal(AzureAD)での作業 アプリの登録

# アプリの登録 1



Microsoft Azure

Azure サービス

- リソースの作成
- Azure Active Directory**
- 予約
- すべてのリソース
- Virtual Machines
- コストの管理と請求
- サブスクリプション
- リソースグループ
- ストレージアカウント
- その他のサービス

最近のリソース

名前	種類	最終表示日
...	ネットワーク セキュリティ グループ	4 日前
...	仮想マシン	5 日前
...	仮想ネットワーク ゲートウェイ	5 日前
...	仮想マシン	1 週間前
...	仮想ネットワーク	1 週間前
...	パブリック IP アドレス	1 か月前
...	仮想マシン	2 か月前
...	仮想マシン	2 か月前
...	仮想マシン	2 か月前
...	仮想マシン	2 か月前
...	リソースグループ	3 か月前
...	仮想マシン	4 か月前

移動

- サブスクリプション
- リソースグループ
- すべてのリソース
- ダッシュボード

ツール

- 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 を開きます。

# アプリの登録 2



The screenshot shows the Azure portal interface for the 'ontimedemo' tenant. The left-hand navigation pane has 'アプリの登録' (App Registrations) highlighted. The main content area shows the 'ontimedemo' tenant overview, including a search bar, tenant information (roles, licenses, tenant ID), and a sign-in graph. The sign-in graph shows a peak in activity around January 17th, with a total of 371 sign-ins.

- 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 3



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
OT otddemo	5bdb6c27-...	2018/7/20	✓ 現在
ON OnTime-Desktop	f8d17528-...	2020/7/20	✓ 現在
ON OnTime-Desktop	3b03e46e-...	2020/7/20	✓ 現在
ON OnTime-Desktop	de25bf72-...	2021/7/20	✓ 現在
ON ontimedemo	0281466a-...	2021/7/20	✓ 現在
ON OnTimeD	ed69bfc2-...	2021/7/20	✓ 現在

- 「アプリの登録」で「新規登録」をクリックします。
- 注意1)  
既に登録しているアプリケーションがある場合は一覧に表示されます。
- 注意2)  
Ver.4.0.8以前で既にOAuth認証を利用されていた場合、またはTeams連携で利用されていた場合は同じアプリケーションを利用できます。  
その場合は新規登録で新たに作成する必要はありません。

# アプリの登録 4



OnTime - Admin | アプリケーションの登録 - Microsoft | 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)。  
OnTimeAuth-from-420 ✓

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は、この組織ディレクトリのみ、または他の組織ディレクトリから追加されたアカウントにのみ使用されます。

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)  
 個人用 Microsoft アカウントのみ

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 | http://localhost:8080/ontimegcms/code.html ✓

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from Enterprise applications.

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」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。

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

- 最後に「登録」をクリックします。





# Azure Portal(AzureAD)での作業 各IDの取得/認証の設定

# アプリの各IDの取得 1



The screenshot shows the Azure portal interface for an application named 'OnTimeAuth-from-420'. The 'Application (client) ID' is 7375492f-a0c3-41... and is highlighted with a yellow box. A tooltip 'クリップボードにコピー' (Copy to clipboard) is visible over the ID. The page also displays 'API calls' with various service icons, 'Documents' with links to Microsoft ID Platform, authentication scenarios, and libraries, and a 'Sign in user' prompt.

- 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、後ほどOnTime管理センターで利用するのでメモ帳などに保持します。

# アプリの各IDの取得 2



- 同じく「ディレクトリ(テナント)ID」をコピーし、後ほどOnTime管理センターで利用するのでメモ帳などに保持します。

続いて「認証」をクリックします。

# 認証の設定



- 発行するトークンを選択します。

アクセストークンにチェックをつけます。

「保存」をクリックします。



# Azure Portal(AzureAD)での作業 クライアントシークレットの設定

# クライアントシークレットの設定 1



The screenshot shows the Azure portal interface for configuring an application. The left-hand navigation pane has the 'Credentials' section highlighted in yellow. The main content area is titled 'OnTimeAuth-from-420 | 証明書とシークレット'. It contains two sections: '証明書' (Certificates) and 'クライアント シークレット' (Client secrets). The 'クライアント シークレット' section includes a '+ 新しいクライアント シークレット' button, which is being clicked by a mouse cursor. Below this button is a table with columns for '説明' (Description), '有効期限' (Expiration), '値' (Value), and 'ID'.

- 「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



Microsoft Azure portal screenshot showing the configuration page for 'OnTimeAuth-from-420'. The page is titled '証明書とシークレット' (Certificates and Secrets). The 'クライアント シークレット' (Client secrets) section is highlighted, showing a button to '+ 新しいクライアント シークレット' (Add new client secret). The page also displays sections for '証明書' (Certificates) and 'トークン構成' (Token configuration).

- 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

説明

有効期限

追加 キャンセル

- 「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」は最長「24か月」まで選択できます。
- 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、それを取得できなくなります。

資格情報は、Web アドレスの指定が可能な場所 (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

押印	開始日	有効期限	ID
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	操作
OnTimeDemo	2023/1/23	UlpR6C... b6078	クリップボードにコピー

- 先ほどの画面上には作成した「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、後ほどOnTime管理センターで利用するのでメモ帳などに保持します。
- 注意**  
「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。



# Azure Portal(AzureAD)での作業 APIのアクセス許可

# APIのアクセス許可 1



Microsoft Azure portal screenshot showing API permissions for an application named 'OnTimeAuth-from-420'. The 'APIのアクセス許可' (API permissions) tab is selected and highlighted with a yellow box. A yellow box also highlights the '+ アクセス許可の追加' (Add permissions) button. Below the button, a table lists permissions for Microsoft Graph, including 'User.Read' with a '委任済み' (Delegated) type and 'Sign in and read user profile' description. The 'APIの公開' (API public) tab is also highlighted with a yellow box.

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	-	...

- 「APIのアクセス許可」タブに移動します。
- こちらではOnTimeサーバーが Graph API で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 2



The screenshot shows the Azure portal interface for configuring API access permissions. The main heading is 'API アクセス許可の要求' (API Access Permissions). Below this, there are tabs for 'Microsoft API', '所属する組織で使用する API' (APIs used by the organization), and '自分の API' (My APIs). A list of 'よく使用される Microsoft API' (Commonly used Microsoft APIs) is displayed, with 'Microsoft Graph' highlighted by a yellow box. The description for Microsoft Graph reads: 'Office 365、Enterprise Mobility + Security、Windows 10 の大量のデータを活用しましょう。Azure AD、Excel、Intune、Outlook/Exchange、OneDrive、OneNote、SharePoint、Planner などに単一エンドポイント経由でアクセスできます。' (Use the vast amount of data from Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, and Planner via a single endpoint.)

- 「APIアクセス許可の要求」ページが開きます。
- 「Microsoft Graph」をクリックします。

# APIのアクセス許可 3



The screenshot shows the 'API アクセス許可の要求' (API Access Permissions) page in the Azure portal. The left sidebar contains navigation options like 'API のアクセス許可' (API Permissions) and 'API の公開' (API Public). The main content area shows the 'Microsoft Graph' application with a list of permissions. The '委任されたアクセス許可' (Delegated permissions) option is highlighted with a yellow box, indicating it is the selected option for the application. Below the list, there are buttons for 'アクセス許可の追加' (Add permissions) and '破棄' (Remove).

- 「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 4

The screenshot shows the 'API Access Permissions' page in the Azure portal. The left sidebar contains navigation options like 'Home', 'OnTimeAuth-from-420', and 'API Access Permissions'. The main content area is titled 'API アクセス許可の要求' and lists various API categories. The 'EWS' category is expanded, and the 'EWS.AccessAsUser.All' permission is selected and highlighted with a yellow box. An arrow points from a text box to this permission.

- アクセス許可の選択肢が下に展開されるのでスクロールして「EWS」まで移動します。移動したら「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 5

Microsoft Azure portal screenshot showing API Access Permissions configuration. The page title is "API アクセス許可の要求". The left sidebar shows navigation options like "API の公開", "アプリのロール | プレビュー", and "API のアクセス許可". The main content area lists various permissions, with "EWS (1)" expanded to show "EWS.AccessAsUser.All" (Access mailboxes as the signed-in user via Exchange Web Services) selected. A yellow box highlights the "アクセス許可の追加" button at the bottom.

- 「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 6



Microsoft Azure portal screenshot showing the 'APIのアクセス許可' (API Access Permissions) page for an application. The page displays a list of permissions granted to the application, including 'Microsoft Graph (2)', 'EWS.AccessAsUser.All', and 'User.Read'. A yellow 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 (2)				
EWS.AccessAsUser.All	委任済み	Access mailboxes as the signed-in user via Exchange...	-	...
User.Read	委任済み	Sign in and read user profile	-	...

- 画面が戻ったら再度「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 7



The screenshot shows the Azure portal interface for configuring API access permissions. The main content area is titled 'API アクセス許可の要求' (API Access Permission Requirements) for Microsoft Graph. It lists the required permissions for the application, including '委任されたアクセス許可' (Delegated permissions) and 'アプリケーションの許可' (Application permissions). The 'アプリケーションの許可' section is highlighted with a yellow box, indicating the next step in the process. The interface includes a search bar, navigation menu, and a list of permissions to be added.

- 今度は「アプリケーションの許可」をクリックします。

# APIのアクセス許可 8



The screenshot shows the 'API Access Permissions' page in the Azure portal. The 'Calendars' category is expanded, and the 'Calendars.ReadWrite' permission is checked. A yellow box highlights the checked permission, and a yellow arrow points to it from a text box on the right.

- アクセス許可の選択肢が下に展開されるのでスクロールして「Calendars」まで移動します。移動したら「Calendars」を更に展開します。

「Calendars.ReadWrite」をチェックします。

# APIのアクセス許可 9



The screenshot shows the 'API Access Permissions' page in the Azure portal. Under the 'Directory (1)' section, the 'Directory.Read.All' permission is selected with a checkmark. A yellow box highlights this permission, and an arrow points from it to a callout box on the right.

- 同様にスクロールして「Directory」まで移動します。移動したら「Directory」を更に展開します。

「Directory.Read.All」をチェックします。

# APIのアクセス許可 10



API アクセス許可の要求

- Member
- Notes
- OnlineMeetings
- OnPremisesPublishingProfiles
- Organization
- OrgContact
- People (1)
  - People.Read.All (Read all users' relevant people lists) はい
- Place
- Policy
- Presence
- Printer
- PrintJob
- PrintSettings

アクセス許可の追加 破壊

- 同様にスクロールして「People」まで移動します。移動したら「People」を更に展開します。

「People.Read.All」をチェックします。

# APIのアクセス許可 1 1



The screenshot shows the 'API Access Permissions' page in the Azure portal. The 'Place (1)' permission is selected and highlighted with a yellow box. A yellow arrow points from a text box to this permission.

API Access Permission	State
People.Read.All (Read all users' relevant people lists)	はい
Place (1)	
Place.Read.All (Read all company places)	はい
Policy	
Presence	
Printer	
PrintJob	

- 同様にスクロールして「Place」まで移動します。移動したら「Place」を更に展開します。

「Place.Read.All」をチェックします。



# APIのアクセス許可 1 2

The screenshot shows the 'API Access Permissions' page in the Azure portal. The 'API Access Permissions' section is expanded, and the 'User (1)' section is selected. The 'User.Read.All' permission is checked. The 'Add' button is highlighted.

API Access Permission	Consent
TermStore	
ThreatAssessment	
ThreatIndicators	
TrustFrameworkKeySet	
UserAuthenticationMethod	
UserNotification	
UserShiftPreferences	
User (1)	
<input type="checkbox"/> User.Export.All Export user's data	はい
<input type="checkbox"/> User.Invite.All Invite guest users to the organization	はい
<input type="checkbox"/> User.ManageIdentities.All Manage all users' identities	はい
<input checked="" type="checkbox"/> User.Read.All Read all users' full profiles	はい
<input type="checkbox"/> User.ReadWrite.All Read and write all users' full profiles	はい

- 同様にスクロールして「User」まで移動します。移動したら「User」を更に展開します。

「User.Read.All」をチェックします。

- 「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 1 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

API を公開するディレクトリ内のアプリは、以下のとおりです

名前	アプリケーション (クライアント) ID
Office 365 Enterprise Insights	f9d02341-e7aa-456d-926d-4a0ca599fbee
Office 365 Exchange Online	00000002-0000-0ff1-ce00-000000000000
Office 365 Information Protection	2f3f02c9-5679-4a5c-a605-0de55b07d135
Office 365 Management APIs	c5393580-f805-4401-95e8-94b7a6ef2fc2
Office 365 Mover	d62121f3-e023-4972-b6b0-794190c0fd98
Office 365 Search Service	66a88757-258c-4c72-893c-3e8bed4d6899
Office 365 SharePoint Online	00000003-0000-0ff1-ce00-000000000000
Office Agent Service	5225545c-3ebd-400f-b668-c8d78550d776
Office Delve	94c63fef-13a3-47bc-8074-75af8c65887a
Office Hive	166f1b03-5b19-416f-a94b-1d7aa2d247dc
Office Scripts Service	62fd1447-0ef3-4ab7-a956-7dd05232ecc1
Office Shredding Service	b97b6bd4-a49f-4a0c-af18-af507d1da76c
Office365 Zoom	0d38933a-0bbd-41ca-9ebd-28c4b5ba7cb7
OfficeServicesManager	9e4a5442-a5c9-4f6f-b03f-5b9fcaaf24b1

- 画面が戻ったら再度「アクセス許可の追加」ボタンをクリックします。

「所属する組織で使用しているAPI」を選択します。

検索欄に office と入力して検索します。

Office 365 Exchange Online を選択します。

# APIのアクセス許可 1 4



API アクセス許可の要求

Office 365 Exchange Online  
https://ps.outlook.com

アプリケーションに必要なアクセス許可の種類

委任されたアクセス許可  
アプリケーションは、サインインしたユーザーとして API にアクセスする必要があります。

アプリケーションの許可  
アプリケーションは、サインインしたユーザーとして、バックグラウンド サービスまたはデーモンとして実行されます。

アクセス許可を選択する

アクセス許可を入力し始めると、これらの結果がフィルター処理されます

アクセス許可	管理者の同意が必要
full_access_as_app Use Exchange Web Services with full access to all mailboxes	はい

アクセス許可の追加

「full\_access\_user\_app」をチェックします。

- 「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 15



APIのアクセス許可の一覧に画面のように8つのAPIが並びます。

「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 / 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 (7)				
Calendars.ReadWrite	アプリケー...	Read and write calendars in all mailboxes	はい	ontimedemo に付与され...
Directory.Read.All	アプリケー...	Read directory data	はい	ontimedemo に付与され...
People.Read.All	アプリケー...	Read all users' relevant people lists	はい	ontimedemo に付与され...
Place.Read.All	アプリケー...	Read all company places	はい	ontimedemo に付与され...
Schedule.Read.All	アプリケー...	Read all schedule items	はい	ontimedemo に付与され...
User.Read	委任済み	Sign in and read user profile	いいえ	ontimedemo に付与され...
User.Read.All	アプリケー...	Read all users' full profiles	はい	ontimedemo に付与され...
▼ Office 365 Exchange Online (1)				
full_access_as_app	アプリケー...	Use Exchange Web Services with full access to all mail...	はい	ontimedemo に付与され...

- アクセス許可の一覧に画面のように8つのAPIが並びます。

「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 16



OnTime - Admin | API アクセス許可の要求 - Microsoft

portal.azure.com/#blade/Microsoft\_AAD\_RegisteredApps/ApplicationMenuBlade/CallAnAPI/quickStartType//sourceType/Microsoft\_AAD\_IAM/appld/7375492f-a0c3-...

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

ホーム > ontimedemo > OnTimeAuth-from-420

OnTimeAuth-from-420 | API のアクセス許可

検索 (Ctrl+/) | 最新の情報に更新 | フィードバックがある場合

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

「管理者の同意が必要」列には、組織の既定値が表示されます。ただし、ユーザーの同意は、アクセス許可、ユーザー、アプリごとにカスタマイズできます。この列には、ご自分の組織や、このアプリが使用される組織の値が反映されていない場合があります。 [詳細情報](#)

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
▼ Microsoft Graph (7)				
Calendars.ReadWrite	アプリケーション...	Read and write calendars in all mailboxes	はい	⚠ ontimedemo に付与され...
Directory.Read.All	アプリケーション...	Read directory data	はい	⚠ ontimedemo に付与され...
People.Read.All	アプリケーション...	Read all users' relevant people lists	はい	⚠ ontimedemo に付与され...
Place.Read.All	アプリケーション...	Read all company places	はい	⚠ ontimedemo に付与され...
Schedule.Read.All	アプリケーション...	Read all schedule items	はい	⚠ ontimedemo に付与され...
User.Read	委任済み	Sign in and read user profile	いいえ	⚠ ontimedemo に付与され...
User.Read.All	アプリケーション...	Read all users' full profiles	はい	⚠ ontimedemo に付与され...
▼ Office 365 Exchange Online (1)				
full_access_as_app	アプリケーション...	Use Exchange Web Services with full access to all mail...	はい	⚠ ontimedemo に付与され...

アクセスルに付与されたその他のアクセス許可

- 確認画面では「はい」をクリックします。

# APIのアクセス許可 17



APIのアクセス許可

構成されたアクセス許可

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 (7)				
Calendars.ReadWrite	アプリケーション...	Read and write calendars in all mailboxes	はい	✔ ontimedemo に付与され...
Directory.Read.All	アプリケーション...	Read directory data	はい	✔ ontimedemo に付与され...
People.Read.All	アプリケーション...	Read all users' relevant people lists	はい	✔ ontimedemo に付与され...
Place.Read.All	アプリケーション...	Read all company places	はい	✔ ontimedemo に付与され...
Schedule.Read.All	アプリケーション...	Read all schedule items	はい	✔ ontimedemo に付与され...
User.Read	委任済み	Sign in and read user profile	いいえ	✔ ontimedemo に付与され...
User.Read.All	アプリケーション...	Read all users' full profiles	はい	✔ ontimedemo に付与され...
▼ Office 365 Exchange Online (1)				
full_access_as_app	アプリケーション...	Use Exchange Web Services with full access to all mail...	はい	✔ ontimedemo に付与され...

- 無事に付与されてるか確認します。
- 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。
- 以上で Azure Portal での作業は完了です。



# OnTime管理センター ドメイン設定での作業

# ドメイン設定



接続ドメイン及びテナント(管理用名称)一覧	
1 OnTimeDemoCom RUNNING 9A5C1189-E3EA-4DE8-A13C-A51A410FFACD	Modern Method (OAuth - Client Credentials) 最終更新日時: Thu Mar 17 08:02:50 JST 2022
2 LDAP NOT_STARTED 5B156932-1516-41AC-BFEB-202A540980AA	Modern Method (OAuth - Impersonation User) 最終更新日時: Thu Mar 17 08:02:42 JST 2022
3 ontimebiz RUNNING 1B536C05-C0F9-48AE-BA8A-38AA21512B6F	レガシー認証が使用されています。まだ当面利用できますが出来るだけ先進認証への変更を検討してください。 最終更新日時: Fri Dec 24 12:38:53 JST 2021

左サイドメニューで「ドメイン設定」を選択します。

「追加」をクリックします。

- Ver.4.0.8以前をご利用だった場合は既存のドメイン設定を選択してください。
- BASIC認証をご利用の場合は左図のような赤字のレガシー認証に対するインフォメーションが表示されますがご利用になられているテナントによっては利用可能です。お早めに先進認証に変更をお願いします。

# ドメイン設定画面



OnTime - Admin | 8080/ontimegcms/admin

ライセンス先 AXCEL 3rd environment  
500のうち81ライセンスを使用中です  
OnTime サブスクリプション | 終了まで 694 日

ONTIME 管理センター

保存 | キャンセル | 「アプリの登録」を開く

ドメイン設定

ドメイン名(管理用名称)   このドメインを無効

優先順位(メールが同じ場合)

接続先Exchange

Exchange Online | 同期対象 | Proxy | 属性マッピング | 高度な設定

認証タイプ

セキュリティユーザー

アプリケーションID

ディレクトリ(テナント)ID

クライアントシークレット(値)

追加設定が必要なアクセス許可

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。  
優先順位は複数テナント時に同じメールアドレスが使用されている場合にどのテナントを優先するかを指定します。

一時的に接続しない場合は無効にできます。

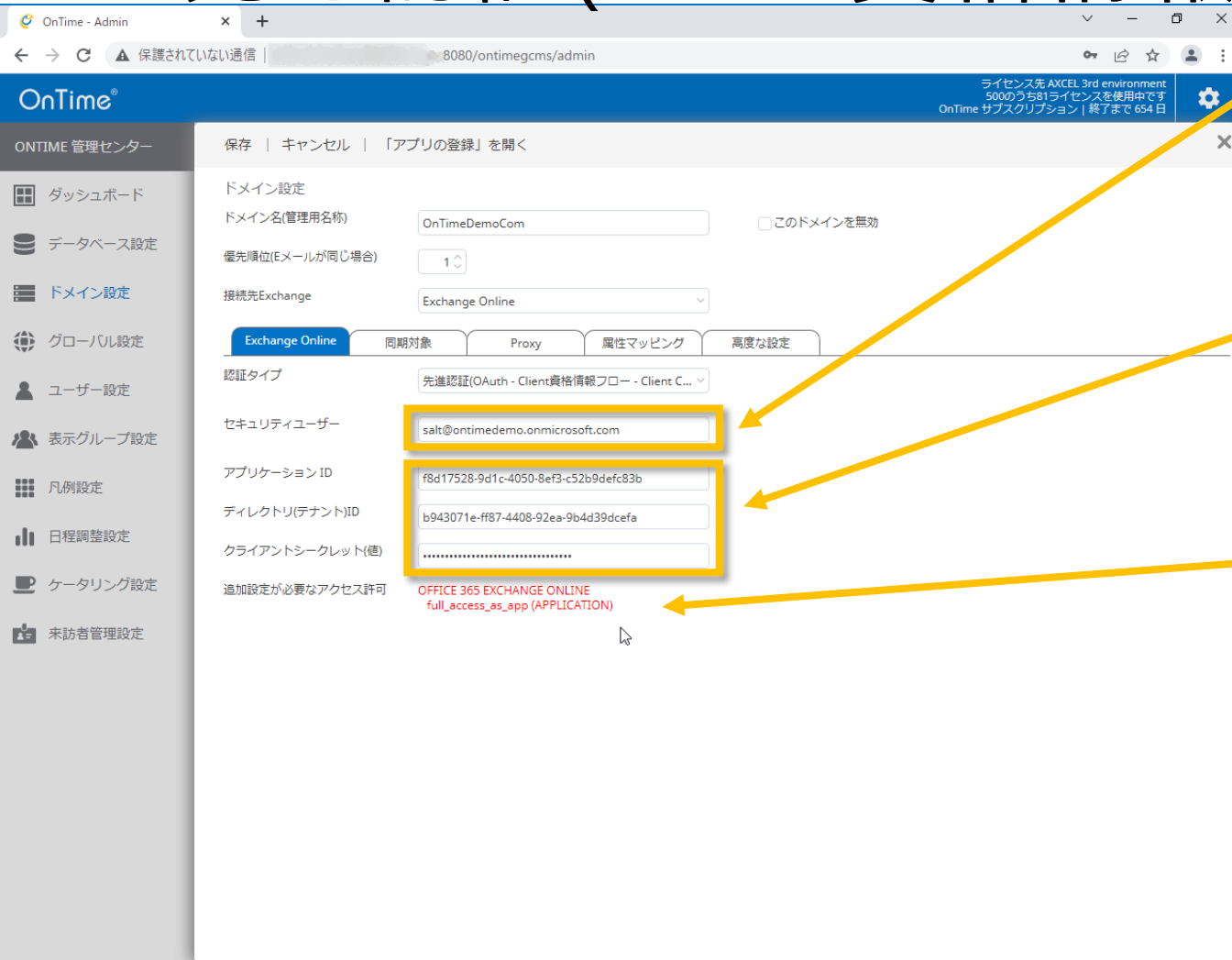
接続先ExchangeでExchange OnlineかオンプレExchangeを選択します。Microsoft365(Exchange Online)の場合は「Exchange Online」を選択します。

オンプレExchangeの設定は P.61 参照

認証タイプは「基本認証(Basic)」「先進認証(OAuth - 認可コードフロー - Impersonation User)」「先進認証(OAuth - Client資格情報フロー - Client Credentials)」の3つが選択可能です。

- Microsoftは基本認証を非推奨とし、廃止予定です。先進認証を御利用ください。

# Exchange Onlineタブ 先進認証(Client資格情報フロー)



セキュリティユーザーはどのユーザーを指定してもかまいません。

- セキュリティユーザー名は操作ログ情報に残ります。

Azureで作成したアプリケーションの情報を指定します。

- 先進認証(OAuth)に必要な各種IDや値を入力します。メモ帳にコピーした3つのテキストを貼り付けます。
- 「アプリケーションID」「ディレクトリID」「クライアントシークレット」の3つを入力後、作成したアプリケーションに対して付与された「APIのアクセス許可」に不備があると、赤文字で何が足りていないか表示されます。赤文字が表示された場合は補足4を参照してください。

※先進認証(OAuth - 認可コードフロー - Impersonation User)での設定方法は補足1を参照してください。オンプレExchange、基本認証の設定方法は補足2を参照してください。

# 同期対象タブ 配布リストでアドレスリストを取得



OnTime - Admin | 8080/ontimegcms/admin

ライセンス先 AXCEL 3rd environment  
500のうち81ライセンスを使用中です  
OnTime サブスクリプション | 終了まで 654 日

ONTIME 管理センター

保存 | キャンセル | 「アプリの登録」を開く

ドメイン設定  
ドメイン名(管理用名称) OnTimeDemoCom  このドメインを無効  
優先順位(メールが同じ場合) 1  
接続先Exchange Exchange Online

Exchange Online **同期対象** Proxy 属性マッピング 高度な設定

LDAP  LDAPを有効にする

ユーザー  
ontimeusers@ontimedemo.com,ontimestaff@ontimedemo.com,testdeleteuser@ontimedemo.com

会議室  
ontimerooms@ontimedemo.com,osaka1@ontimedemo.com,osaka2@ontimedemo.com

共有席  
workspace1@ontimedemo.com,workspace2@ontimedemo.com,demoyama3@ontimedemo.com

備品  
ontimeresources@ontimedemo.com

例) Exchange側で事前に以下の様なグループを作成しておくことで運用のメンテナンスが容易です。

ユーザーグループ : OnTimeUsers@ontimedemo.com

会議室グループ : OnTimeRooms@ontimedemo.com

共有席グループ : OnTimeFreeAddress@ontimedemo.com

備品グループ : OnTimeEquipment@ontimedemo.com

- 今回はグループのメールアドレスのリストで指定します。

“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。
- グループアドレスにはOnTimeで表示する、または操作できるいずれの場合のアカウントでも含まれている必要があります。
- 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。入れ子になっているグループを指定するとOnTime管理センターのその他の設定(ロール設定や静的グループ設定)などで利用できます。
- ドメインのユーザー、会議室、共有席、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)のメールアドレスが複数の場合はカンマで区切ってください。

※LDAP利用の設定方法は補足3を参照してください。



# Proxyタブ Proxyを利用する場合の設定



The screenshot shows the OnTime Admin interface. The browser address bar displays '8080/ontimegcms/admin'. The page title is 'OnTime®'. The left sidebar contains navigation items: ONTIME 管理センター, ダッシュボード, データベース設定, ドメイン設定, グローバル設定, ユーザー設定, 表示グループ設定, 凡例設定, 日程調整設定, ケータリング設定, and 来訪者管理設定. The main content area is titled '保存 | キャンセル | 「アプリの登録」を開く'. Under 'ドメイン設定', the 'ドメイン名(管理用名称)' is 'OnTimeDemoCom', '優先順位(Eメールが同じ場合)' is '1', and '接続先Exchange' is 'Exchange Online'. Below this, there are tabs for 'Exchange Online', '同期対象', 'Proxy', '属性マッピング', and '高度な設定'. The 'Proxy' tab is active. Underneath, the 'ホスト名' and 'ポート番号' fields are visible and highlighted with a yellow box.

- Proxyをご利用の場合はProxy設定を行います。
- もしProxyをキャッシュ目的で利用されている場合でダイレクト通信も可能であればOnTimeはダイレクト通信させていただきます。OnTimeが行うデータはあまり副次利用されません。

# 属性マッピングタブ 各属性情報に特定の項目を利用する場合の設定



OnTime - Admin

8080/ontimegcms/admin

ライセンス先 AXCEL 3rd environment  
500のうち81ライセンスを使用中です  
OnTime サブスクリプション | 終了まで 654 日

ONTIME 管理センター

保存 | キャンセル | 「アプリの登録」を開く

ドメイン設定

ドメイン名(管理用名称) OnTimeDemoCom  このドメインを無効

優先順位(メールが同じ場合) 1

接続先Exchange Exchange Online

Exchange Online 同期対象 Proxy **属性マッピング** 高度な設定

ユーザー

部署 -デフォルト-

事業所 -デフォルト-

勤務先電話 -デフォルト-

携帯電話 -デフォルト-

役職 -デフォルト-

会議室/備品/共有席

事業所 -デフォルト-

勤務先電話 -デフォルト-

建物 -デフォルト-

デフォルト-  
-デフォルト-  
Department  
OfficeLocation  
BusinessPhone  
MobilePhone  
JobTitle  
ExtensionAttribute1  
ExtensionAttribute2  
ExtensionAttribute3  
ExtensionAttribute4  
ExtensionAttribute5  
ExtensionAttribute6  
ExtensionAttribute7  
ExtensionAttribute8  
ExtensionAttribute9  
ExtensionAttribute10  
ExtensionAttribute11  
ExtensionAttribute12  
ExtensionAttribute13  
ExtensionAttribute14

閉じる | 個人ビュー

ココア 二郎

部署 営業部  
勤務先電話 03-  
事業所 東京本社  
携帯電話 090-  
電子メール cocoa@ontimedemo.com

- OnTimeメインビューでユーザープロフィール情報を表示した際に表示される項目の情報の設定を行います。プロフィール情報に表示させる項目や順番はOnTime管理センターの「フロントエンド」にある「属性表示設定」タブで変更できます。  
※詳細は別紙「[設定マニュアル](#)」を参照してください

# 高度な設定タブ



- 接続のトレースはチェックをつけません。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。**起動時設定は5を推奨します。**
  - 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20程度に設定します。  
**注意）一つのExchangeテナントに20以上のスレッドは設定しないでください。**

設定が完了したら「保存」をクリックします。

# 保存結果



接続ドメイン及びテナント(管理用名称)一覧	接続ドメイン	接続方法	最終更新日時
1	OnTimeDemoCom NOT_STARTED 9ACAF1B9-E3EA-4DE8-A13C-A51A410FFACD	Modern Method (OAuth - Client Credentials)	最終更新日時: Thu Mar 17 10:56:50 JST 2022
2	LDAP NOT_STARTED 5B156932-1516-41AC-BFEB-202A540980AA	Modern Method (OAuth - Impersonation User)	最終更新日時: Thu Mar 17 10:56:50 JST 2022
3	OnTimeBiz NOT_STARTED 10CD495A-0FDE-4F02-A559-843CB01C6A1F	レガシー認証が使用されています。まだ当面利用できますが出来るだけ先進認証への変更を検討してください。	最終更新日時: Thu Mar 17 10:56:50 JST 2022

- 画面が閉じる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。

# ダッシュボードで再起動



ONTIME 管理センター

ライセンスの編集 更新

ダッシュボード

データベース設定

ドメイン設定

グローバル設定

ユーザー設定

表示グループ設定

凡例設定

システム状況

アプリケーション:	RUNNING	実行	停止
有効なライセンスの確認:	RUNNING	実行	停止

接続状況

SQL DB 接続状況:	RUNNING
ドメイン 接続状況:	0 / 0 RUNNING

- ドメイン情報を作成/変更した場合はOnTimeサービスの再起動が必要になります。

左サイドメニューでダッシュボードに移動します

「OnTimeアプリケーション」で停止をクリック

「OnTimeアプリケーション」で実行をクリック

ONTIME 管理センター

ライセンスの編集 更新

ダッシュボード

データベース設定

システム状況

アプリケーション:	STOPPED	実行	停止
有効なライセンスの確認:	STOPPED	実行	停止

接続状況

SQL DB 接続状況:	STOPPED
ドメイン 接続状況:	0 / 0 RUNNING

- 続いてOnTime設定マニュアルでそのほかの設定をします。



# 補足1) 認可コードフロー認証方式の設定

# Exchange側の設定準備



- OnTimeの認証方法で「認可コードフロー(ImpersonationUser)」を利用する場合、OnTimeは同期対象のメールボックスと接続するアカウントにはImpersonation(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
  - 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/>

# Exchange管理センターを開く



- Exchange管理センターを開きます。
- アクセス許可を開きます。
- 管理者の役割を開きます。
- + ボタンを押して管理者の役割を追加します。



# 管理者の役割の追加 1



- 新しい役割を作成します。
- 名前には識別しやすい名前を指定してください。
- 役割の + ボタンを押して役割を選択します。

# 管理者の役割の追加 2



The screenshot shows the Exchange Admin Center interface. A dialog box titled '役割の選択' (Role Selection) is open, displaying a list of roles. The 'ApplicationImpersonation' role is highlighted. Below the list, the '追加 ->' (Add) button is highlighted. The 'OK' button is also highlighted, indicating the next step in the process.

- ApplicationImpersonationを選択します。
- 「追加」を押して追加後に「OK」を押します。

# 管理者の役割の追加 3



役割グループの新規作成

書き込みスコープ: 既定

役割:

名前

ApplicationImpersonation

メンバー:

名前	表示名
otds...	otds...
otsy...	otsy...

この役割グループのメンバーを選びます。  
[詳細情報](#)

保存 キャンセル

合計 16 件のうち 1 件を選択

- 同じくOnTimeから同期を行うアカウントを追加します。
- 設定ができれば「保存」を押します。

# 管理者の役割の追加 4



Exchange 管理センター

管理 管理センター

新しい Exchange 管理センターをお試しください

管理者の役割 ユーザーの役割 Outlook Web App ポリシー

名前

- Compliance Management
- Discovery Management
- ExchangeServiceAdmins\_
- Help Desk
- HelpdeskAdmins\_
- Hygiene Management
- OnTimeImpersonation**
- Organization Management
- Recipient Management
- Records Management
- RIM-MailboxAdmins31b32f8f311742e683481e09fa79474e
- Security Administrator
- Security Reader
- TenantAdmins\_1003362474
- UM Management
- View-Only Organization Management

OnTimeImpersonation

割り当てられている役割  
ApplicationImpersonation

メンバー  
otdc  
otsy

所有者  
Organization Management  
otdac

書き込みスコープ  
既定

合計 16 件のうち 1 件を選択

- 先ほど作成した役割が追加されています。

# OnTime管理センターでドメイン設定



OnTime - Admin

8080/ontimegcms/admin

ライセンス先 AXCEL 3rd environment  
500のうち81ライセンスを使用中です  
OnTime サブスクリプション | 終了まで 694 日

OnTime®

ONTIME 管理センター

保存 | キャンセル | 「アプリの登録」を開く

ドメイン設定

ドメイン名(管理用名称) OnTimeDemoCom  このドメインを無効

優先順位(メールが同じ場合) 1

接続先Exchange Exchange Online

Exchange Online 同期対象 Proxy 属性マッピング 高度な設定

認証タイプ 先進認証(OAuth - 認可コードフロー - Impersona...

Impersonation User otdsync@ontimedemo.onmicrosoft.com

パスワード (present)

アプリケーションID f8d17528-9d1c-4050-8ef3-c52b9dffc83b

ディレクトリ(テナント)ID b943071e-ff87-4408-92ea-9b4d39dcefa8

クライアントシークレット(値) .....

追加設定が必要なアクセス許可

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。

- OnTimeとして各ユーザーの情報を取得する権限を持ったユーザーを指定します。

Azureで作成したアプリケーションの情報を指定します。

- 先進認証(OAuth)に必要な各種IDや値を入力します。メモ帳にコピーした3つのテキストを貼り付けます。
- 「アプリケーションID」「ディレクトリID」「クライアントシークレット」の3つを入力後、作成したアプリケーションに対して付与された「APIのアクセス許可」に不備があると、赤文字で何が足りていないか表示されます。



# 補足2) オンプレExchange/基本認証の設定

# オンプレExchange へのEWS接続



- オンプレExchangeに接続する際はこのページの設定をご参照ください。

例:“OnTimeDemoCom”と入力。優先順位:“1”を入力。

- 優先順位は複数テナント時に同じメールアドレスが使用されている場合にどのテナントを優先するかを指定します。例えばオンプレからクラウドに移行の最中の場合はクラウドを優先したいのでオンプレは大きい数字を指定します。

ドメインタイプで「オンプレExchange」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。

# 基本認証によるEWS接続



OnTime - Admin | 8080/ontimegcms/admin

ライセンス先 AXCEL 3rd environment  
500のうち81ライセンスを使用中です  
OnTime サブスクリプション | 終了まで 694 日

保存 | キャンセル | 「アプリの登録」を開く

ドメイン設定

ドメイン名(管理用名称) LDAP  このドメインを無効

優先順位(メールが同じ場合) 2

接続先Exchange Exchange Online

Exchange Online | 同期対象 | Proxy | 属性マッピング | 高度な設定

認証タイプ **基本認証(BASIC)**

Impersonation User impersonationusertest@ontimedemo.com

パスワード (present)

- ドメインタイプで Exchange Online を選択された場合で OAuth 認証を選択できない場合、また旧バージョンからご利用でまだ先進認証の準備が整っていない場合は「基本認証(BASIC)」を選択してください。

基本認証(BASIC)を選択します。

- オンプレExchangeは基本認証のみを受け付けますのでこの画面は表示されません。





# 補足3) 同期対象をLDAPで取得

# 同期対象をLDAPで取得 1



OnTime - Admin | 8080/ontimegcms/admin

ライセンス先 AXCEL 3rd environment  
500のうち81ライセンスを使用中です  
OnTime サブスクリプション | 終了まで 694 日

保存 | キャンセル | 「アプリの登録」を開く

ドメイン設定  
ドメイン名(管理用名称) LDAP  このドメインを無効  
優先順位(メールが同じ場合) 2  
接続先Exchange Exchange Online

Exchange Online | **同期対象** | Proxy | 属性マッピング | 高度な設定

LDAP  LDAPを有効にする

URL ldap://obizad.ontime.otbz:389

ユーザー CN=Administrator, CN=Users, DC=ontime, DC=otbz

パスワード ..... テスト

ベース OU=o365, DC=ontime, DC=otbz

スコープ SUB\_TREE

フィルター (cn=OnTimeRooms)

共有席  はい テスト

ベース OU=o365, DC=ontime, DC=otbz

スコープ SUB\_TREE

フィルター (mail=OnTimePersons)

- 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。

# 同期対象をLDAPで取得 2



The screenshot shows the OnTime Admin interface with the '同期対象' (Synchronization Targets) tab selected. The 'LDAP' section is active, and the 'LDAPを有効にする' (Enable LDAP) checkbox is checked. Two LDAP entries are visible, each with a 'テスト' (Test) button. The first entry has the following fields: URL (ldap://obizad.ontime.otbz:389), User (CN=Administrator, CN=Users, DC=ontime, DC=otbz), and Password (masked). The second entry has: Base (OU=o365, DC=ontime, DC=otbz), Scope (SUB\_TREE), Filter ((cn=OnTimeRooms)), and a checkbox for '共有席' (Shared Seats) which is unchecked. A third entry is partially visible at the bottom with Base (OU=o365, DC=ontime, DC=otbz), Scope (SUB\_TREE), and Filter ((mail=OnTimePersons)).

- 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。



# 同期対象をLDAPで取得 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://ad.ontime.otbz:389
ユーザー	CN=ad.ontime.otbz, 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=*)

LDAP	<input checked="" type="checkbox"/> LDAPを有効にする
URL	ldap://ad.ontime.otbz:389
ユーザー	CN=ad.ontime.otbz, 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。



# 補足4) Graphで認証エラーが出る

# ドメイン接続がエラーで接続できない



OnTime Admin console screenshot showing system status. The 'ドメイン接続状況' (Domain Connection Status) is highlighted with a yellow box and shows '1 / 2 RUNNING'.

システム状況	ステータス	実行	停止	最終実行日時
アプリケーション:	RUNNING	実行	停止	最終実行日時: Thu Mar 17 11:02:02 JST 2022
有効なライセンスの確認:	RUNNING	実行	停止	最終実行日時: Thu Mar 17 11:02:03 JST 2022
接続状況				
SQL DB 接続状況:	RUNNING			最終実行日時: Thu Mar 17 11:02:02 JST 2022
<b>ドメイン 接続状況:</b>	<b>1 / 2 RUNNING</b>			
同期スケジュール				
ディレクトリ 同期:	SCHEDULED TO RUN 09:00	実行		最終実行日時: Thu Mar 17 09:00:17 JST 2022
ユーザーとグループ 同期:	SCHEDULED TO RUN 09:00	実行		最終実行日時: Thu Mar 17 09:00:24 JST 2022
写真 同期:	SCHEDULED TO RUN 09:00	実行		最終実行日時: Thu Mar 17 09:01:05 JST 2022
アクセス権 同期:	SCHEDULED TO RUN 09:00	実行		最終実行日時: Thu Mar 17 09:00:58 JST 2022
カレンダー 同期:	SCHEDULED TO RUN TOMORROW 09:00	実行		最終実行日時: Thu Mar 17 09:01:07 JST 2022
日程調整				
アプリケーション:	RUNNING			
SQL DB 接続状況:	OK			
ケータリング				

- インジケータが赤色や黄色の場合はドメイン接続ができていない状態です。
- OnTimeをバージョンアップしたなどの場合はほとんどが先進認証 (OAuth)が正しく設定されていないときです。

# ドメイン設定で該当ドメインを確認



OnTime - Admin

3080/ontimegcms/admin

ライセンス先 AXCEL 3rd environment  
500のうち81ライセンスを使用中です  
OnTime サブスクリプション | 終了まで 694 日

ONTIME 管理センター

追加

接続ドメイン及びテナント(管理用名称)一覧

1	OnTimeDemoCom STOPPED 9ACAF1B9-E3EA-4DE8-A13C-A51A410FFACD	エラー: com.ontimesuite.ontime.ms.v2.web.api.v2.ApiErrorException: Error: ClientCredentials fetch access token failed! 最終更新日時: Thu Mar 17 11:02:02 JST 2022
2	LDAP NOT_STARTED 5B156932-1516-41AC-BFEB-202A540980AA	Modern Method (OAuth - Impersonation User) 最終更新日時: Thu Mar 17 11:02:02 JST 2022
3	OnTimeBiz RUNNING 10CD495A-0FDE-4F02-A559-843CB01C6A1F	レガシー認証が使用されています。まだ当面利用できますが出来るだけ先進認証への変更を検討してください。 最終更新日時: Thu Mar 17 11:02:02 JST 2022

- 該当ドメインが「STOPPED」でエラーメッセージが表示されています。
- クリックして設定を確認します。

# 認証タブに追加で必要な「アクセス許可」が表示



OnTime - Admin | 8080/ontimegcms/admin

ライセンス先 AXCEL 3rd environment  
500のうち81ライセンスを使用中です  
OnTime サブスクリプション | 終了まで 694 日

ONTIME 管理センター

保存 | キャンセル | 「アプリの登録」を開く

ドメイン設定

ドメイン名(管理用名称) OnTimeDemoCom  このドメインを無効

優先順位(メールが同じ場合) 1

接続先Exchange Exchange Online

Exchange Online | 同期対象 | Proxy | 属性マッピング | 高度な設定

認証タイプ 先進認証(OAuth - Client資格情報フロー - Client C...

セキュリティユーザー salt@ontimedemo.onmicrosoft.com

アプリケーションID f8d17528-9d1c-4050-8ef3-c52b9defc83b

ディレクトリ(テナント)ID b943071e-ff87-4408-92ea-9b4d39dcefa

クライアントシークレット(値) .....

追加設定が必要なアクセス許可 OFFICE 365 EXCHANGE ONLINE full\_access\_as\_app (APPLICATION)

- 追加で必要となるアプリのアクセス許可が表示されています。
- AzureADの「アプリの追加」に戻り、必要となるアクセス許可を追加して再度OnTimeを起動してください。