



OnTime[®] GROUP CALENDAR

for Microsoft(Ver.4.1-)

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

2021/02/09



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
- Exchange管理センターでの作業 p.06
- Azure Portal(AzureAD)での作業 p.13
- ドメイン設定での作業 p.43
- 保存結果と再起動 p.50
- 補足1) 基本タブと認証タブ p.52
- 補足2) リソースタブ p.55
- 補足3) 認証タブ p.59



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。
 - Exchange管理センターでの作業について
 - EWS接続用に同期するメールボックスへImpersonation（偽装）する同期用アカウントを設定します。
 - 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。

ドメイン設定のページ構成



保存 | キャンセル | 削除

基本

認証

Source

Proxy

高度な設定

↑

ドメイン名やドメインタイプ、テナントの優先順位またはImpersonationユーザーアカウントの登録など P.6

↑

先進(Oauth)認証用のAzure ADのアプリ情報の登録。 P.13

↑

オンプレExchangeの場合は基本(Basic)認証を使用。
Exchange Onlineの場合は2021年後半まで利用可。
P.51

↑

OnTimeを利用するメールボックスアカウントを配布リスト(グループ)で指定。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します。 P.42

↑

LDAP検索による取得についてオンプレExchangeまたはExchange OnlineでもAzure AD Connectを利用してる場合はオンプレADから取得できます。LDAPの場合は拡張属性も利用可能です。 P.54

↑

トレース設定、同期スレッド数の設定 P.48

↑

https接続でProxy経由の接続が必要な場合の設定 P.47



Exchange管理センターでの作業

Exchange側の設定を準備します



- 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

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

アクセス許可

+

Compliance Management

Discovery Management
ExchangeServiceAdmins_...
Help Desk
HelpdeskAdmins_...
Hygiene Management
Organization Management
Recipient Management
Records Management
RIM-MailboxAdmins31b32f8f311742e683481e09fa79474e
Security Administrator
Security Reader
TenantAdmins_1003362474
UM Management
View-Only Organization Management

Compliance Management

この役割グループにより、コンプライアンスを担当する特定のユーザーは、組織のポリシーに従って Exchange 内のコンプライアンス設定を適切に構成して管理できます。

割り当てられている役割

Audit Logs
Compliance Admin
Data Loss Prevention
Information Rights Management
Journaling
Message Tracking
Retention Management
Transport Rules
View-Only Audit Logs
View-Only Configuration
View-Only Recipients

メンバー

所有者

Organization Management

書き込みスコープ

既定

合計 16 件のうち 1 件を選択

- 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



役割グループの新規作成

*名前:
OnTimeImpersonation

書き込みスコープ:
既定

役割:
+ -
名前

この役割グループのメンバーに管理を許可する Exchange の機能とサービスに対応する管理者の役割を選択してください。
[詳細情報](#)

メンバー:
+ -

名前	表示名
----	-----

保存 キャンセル

合計 16 件のうち 1 件を選択

- 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 'Management Role Picker' is open, displaying a list of roles. The 'ApplicationImpersonation' role is highlighted. Below the list, there are fields for '既定の受信者の範囲' (Default Recipient Scope) and '既定の構成スコープ' (Default Configuration Scope). The 'Add' button is highlighted, and the 'OK' button is being clicked. The background shows the 'New Admin Role Group' page with a search bar and a list of roles.

- 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。
- 設定が出来れば「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。



Azure Portal(AzureAD)での作業

「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

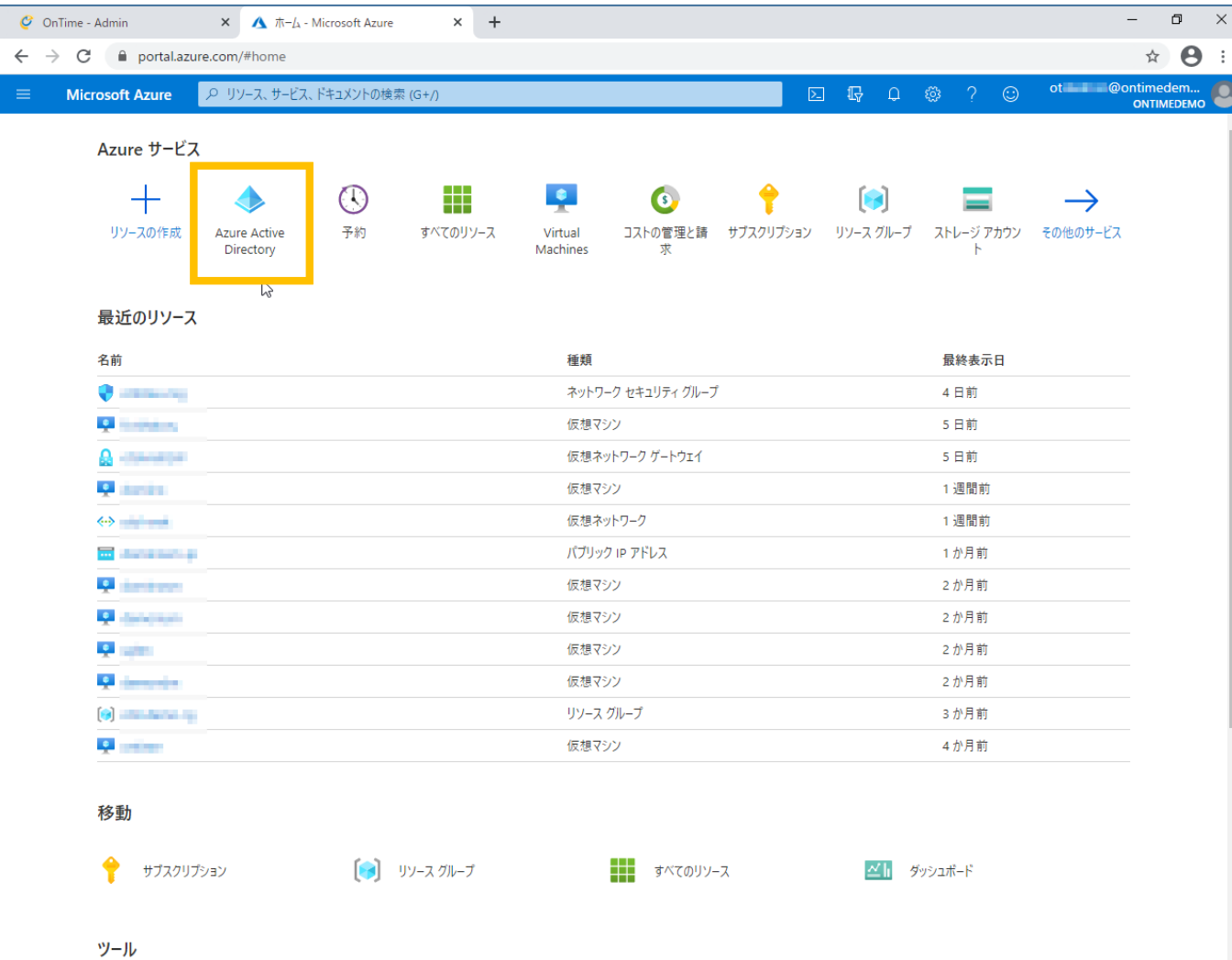
- OnTime が Microsoft365 (Exchange Online) と先進認証(Oauth)で接続する際は Azure Portal で「アプリの登録」を行う必要があります。以下の情報を参考に認証方式は先進認証(Oauth) を採用してください。
- Exchange Online の基本認証が非推奨となります(Microsoft Docs発行元：2019年9月20日)
<https://docs.microsoft.com/ja-jp/lifecycle/announcements/exchange-online-basic-auth-deprecated>
 - --抜粋--
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



- 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出来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。

アプリの登録 1



- 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 displays the Azure Active Directory management interface for the 'ontimedemo' tenant. The left-hand navigation pane is visible, with 'アプリの登録' (App Registrations) highlighted. The main content area shows the 'テナントの情報' (Tenant Information) section, which includes details such as the tenant ID (b943071) and the primary domain (ontimedemo.com). Below this, there is a 'サインイン' (Sign-in) section with a line graph showing activity over time and a current sign-in count of 371.

- 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 ottdemo	5babb6c27-...	2018/...	✓ 現在
ON OnTime-...	f8d17528-...	2020/...	✓ 現在
ON OnTime-...	3b03e46e-...	2020/...	✓ 現在
ON OnTime-...	de25bf72-...	2021/...	✓ 現在
ON ontimedemo-...	0281466a-...	2021/...	✓ 現在
ON OnTimeD-...	ed69bfc2-...	2021/...	✓ 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-410

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したりAPIにアクセスしたり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)

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

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。

アプリの各IDの設定 1



Microsoft Azure portal screenshot showing the configuration page for an application named "OnTimeAuth-from-410". The page displays various identifiers and settings. A yellow box highlights the "Application (Client) ID" field, with a callout bubble containing the text "クリップボードにコピー" (Copy to clipboard). The page also includes sections for "APIの呼び出し" (API calls) and "ドキュメント" (Documents).

- 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の設定 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



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

OnTimeAuth-from-410 | 認証

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ルドなど追加構成が必要となる場合があります。

プラットフォームを追加

Web

リダイレクト URI

ユーザーの認証またはサインアウト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 とも呼ばれます。リダイレクト URI と制限の詳細情報

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

URI の追加

フロントチャネルのログアウト 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

暗黙的な許可およびハイブリッド フロー

承認エンドポイントから直接トークンを要求します。アプリケーションにシングルページアーキテクチャ (SPA) があり、承認モード フローを使用していない場合、または JavaScript で Web API を起動する場合は、アクセス トークンと ID トークンの両方を選択します。ハイブリッド認証を使用する ASP.NET Core Web アプリや他の Web アプリでは、ID トークンのみを選択します。詳細情報

アクセス トークン (暗黙的なフローに使用)

ID トークン (暗黙的およびハイブリッド フローに使用)

サポートされているアカウントの種類

- 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。

クライアントシークレットの設定 1



The screenshot shows the Azure portal interface for an application named 'OnTimeAuth-from-410'. The left-hand navigation pane is visible, with the 'Certificates and Secrets' option highlighted in yellow. The main content area is divided into two sections: 'Certificates' and 'Client secrets'. The 'Client secrets' section is currently active, showing a table with columns for 'Description', 'Expiration', 'Value', and 'ID'. A '+ New client secret' button is highlighted with a mouse cursor. The table is currently empty, with a message stating 'This application does not have any client secrets created yet.'

- 「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 an application named 'OnTimeAuth-from-410'. The left sidebar contains navigation options such as '概要', 'クイックスタート', '統合アシスタント', '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', 'アプリのロール | プレビュー', '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', and '新しいサポートリクエスト'. The main content area is titled '証明書とシークレット' and includes sections for '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 contains a table with columns for '説明' (Description), '有効期限' (Expiration), '値' (Value), and 'ID'. A button labeled '+ 新しいクライアント シークレット' (New Client Secret) is highlighted with a yellow box.

- 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」は昨今の傾向から「なし」以外を選択し、更新を心がけましょう。
- 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



Microsoft Azure portal screenshot showing the 'OnTimeAuth-from-410' application configuration page. The page displays the 'クライアント シークレット' (Client Secrets) section. A table lists the secrets, with one entry highlighted. A yellow box highlights the 'クリップボードにコピー' (Copy to clipboard) button next to the secret value.

説明	有効期限	値
OnTimeDemo	2023/1/23	UlpR6C... b6078c1...-04e1-4...

- 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。

APIのアクセス許可 1



Microsoft Azure portal screenshot showing API permissions for an application. The page title is "OnTimeAuth-from-410 | API のアクセス許可". The left navigation pane shows "API のアクセス許可" selected. The main content area displays a table of permissions for Microsoft Graph.

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	-	...

- 「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



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

- 「APIアクセス許可の要求」ページが開きます。
- スクロールして「Microsoft Graph」を見つけます。

APIのアクセス許可 3



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). It displays a grid of various Microsoft APIs, each with a brief description of its capabilities. At the bottom of the grid, a section titled "よく使用される Microsoft API" (Commonly Used Microsoft APIs) is highlighted with a yellow border. Within this section, the "Microsoft Graph" API is prominently displayed, with a mouse cursor hovering over it. The left sidebar shows navigation options, and the top navigation bar includes the Azure logo and search bar.

- 「Microsoft Graph」をクリックします。

APIのアクセス許可 4



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 permission type. Below it, there are two columns of permission options: '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).

- 「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 5



The screenshot shows the 'API アクセス許可の要求' (API permissions) page in the Azure portal. The left sidebar contains navigation options like '概要', 'クイックスタート', and 'API の公開'. The main area lists various API categories such as 'DeviceManagementManagedDevices', 'Directory', and 'EWS'. 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 6

Microsoft Azure portal screenshot showing the 'API アクセス許可の要求' (API Access Permissions) page. The page displays a list of permissions, including 'EWS (1)' with 'EWS.AccessAsUser.All' selected. A yellow box highlights the 'アクセス許可の追加' (Add Access Permission) 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 7



Microsoft Azure

OnTimeAuth-from-410 | API のアクセス許可

概要

クイックスタート

統合アシスタント

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

アプリのロール | プレビュー

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

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

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	-	...

アクセス許可とユーザーの同意を表示および管理するために、エンタープライズ アプリケーションをお試しください。

- 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 8



The screenshot shows the Azure portal interface for configuring API permissions. The main content area is titled 'API アクセス許可の要求' (API Access Permission Requirements). It lists the application 'Microsoft Graph' and shows a table of permissions. The 'アプリケーションの許可' (Application permissions) section is highlighted with a yellow box. Below this section, there is a warning message: '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 application permissions section contains the following text: 'アプリケーションの許可' (Application permissions) and 'アプリケーションは、サインインしたユーザーなしで、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。' (The application runs as a background service or daemon without a signed-in user).

- 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 9



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 'Calendars.ReadWrite' permission, and a yellow arrow points from a text box to it.

API Access Permission	Consent
Calendars.Read	はい
Calendars.ReadWrite	はい

- 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 10



API アクセス許可の要求

- Device
- DeviceManagementApps
- DeviceManagementConfiguration
- DeviceManagementManagedDevices
- DeviceManagementRBAC
- DeviceManagementServiceConfig
- Directory (1)
 - Directory.Read.All (Read directory data) はい
 - Directory.ReadWrite.All (Read and write directory data) はい
- Domain
- EduAdministration
- EduAssignments
- EduRoster
- EntitlementManagement

アクセス許可の追加 破棄

- 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 1 1



API アクセス許可の要求

すべての API

- Mail
- Member
- Notes
- OnlineMeetings
- OnPremisesPublishingProfiles
- Organization
- OrgContact
- People
- Place (1)
 - Place.Read.All (1) Read all company places はい
- Policy
- Printer
- PrintJob

アクセス許可の追加 破棄

- 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 アクセス許可の要求' (API Access Permissions) page in the Azure portal. The left sidebar shows the navigation menu with 'API のアクセス許可' (API Permissions) selected. The main content area shows a list of permissions under the 'User (1)' category. The 'User.Read.All' permission is checked, and a yellow box highlights it. A yellow arrow points from a text box to this permission.

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



APIのアクセス許可 1 3

Microsoft Azure portal screenshot showing API access permissions for 'OnTimeAuth-from-410'. The 'API / アクセス許可' section is expanded, showing a list of permissions under 'User (1)'. The 'User.Read.All' permission is selected with a blue checkmark. A yellow box highlights the 'アクセス許可の追加' button at the bottom left of the permissions list.

権限	説明	状態
<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

- 「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 4



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-410

OnTimeAuth-from-410 | 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

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
▼ Microsoft Graph (6)				
Calendars.ReadWrite	アプリケーシ...	Read and write calendars in all mailboxes	はい	ontimedemo に付与され...
Directory.Read.All	アプリケーシ...	Read directory data	はい	ontimedemo に付与され...
EWS.AccessAsUser.All	委任済み	Access mailboxes as the signed-in user via Exchange...	-	
Place.Read.All	アプリケーシ...	Read all company places	はい	ontimedemo に付与され...
User.Read	委任済み	Sign in and read user profile	-	
User.Read.All	アプリケーシ...	Read all users' full profiles	はい	ontimedemo に付与され...

アクセス許可とユーザーの同意を表示および管理するために、[エンタープライズ アプリケーション](#)をお試しください。

- アクセス許可の一覧に画面のように6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 1 5



OnTimeAuth-from-410 | API のアクセス許可

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。

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 (6)				
Calendars.ReadWrite	アプリケーシ...	Read and write calendars in all mailboxes	はい	⚠ ontimedemo に付与され...
Directory.Read.All	アプリケーシ...	Read directory data	はい	⚠ ontimedemo に付与され...
EWS.AccessAsUser.All	委任済み	Access mailboxes as the signed-in user via Exchange...	-	...
Place.Read.All	アプリケーシ...	Read all company places	はい	⚠ ontimedemo に付与され...
User.Read	委任済み	Sign in and read user profile	-	...
User.Read.All	アプリケーシ...	Read all users' full profiles	はい	⚠ ontimedemo に付与され...

アクセス許可とユーザーの同意を表示および管理するために、[エンタープライズ アプリケーション](#)をお試しください。

- 確認画面では「はい」をクリックします。

APIのアクセス許可 16



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-410

OnTimeAuth-from-410 | 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

要求されたアクセス許可の管理者の同意が正常に付与されました。

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 (6)				
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...
EWS.AccessAsUser.All	委任済み	Access mailboxes as the signed-in user via Exchange...	-	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...
User.Read	委任済み	Sign in and read user profile	-	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...

アクセス許可とユーザーの同意を表示および管理するために、[エンタープライズ アプリケーション](#)をお試しください。

- 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



The screenshot shows the OnTime Admin interface. The left sidebar contains the following menu items: ONTIME 管理センター, 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, ケータリング設定, 来訪者管理設定. The main content area is titled 'ドメイン' and contains a table with two entries:

ID	Domain Name	Status	Details
1	ontimebiz	RUNNING	レガシー認証が使用されています。2021年夏までに先進認証に変更を検討してください。 最終更新日時: Sat Jan 23 01:03:40 JST 2021
2	axcel	NOT_STARTED	レガシー認証が使用されています。2021年夏までに先進認証に変更を検討してください。 最終更新日時: Sat Jan 23 01:03:39 JST 2021

The '新規作成' button is located at the top left of the domain list. The 'ドメイン設定' menu item in the sidebar is highlighted with a yellow box.

左サイドメニューで「ドメイン」を選択します。

「新規作成」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インフォメーションが表示されますが2021年後半までは利用可能です。

Microsoft365(Exchange Online)への接続



OnTime - Admin | OnTimeAuth-from-410 - Microso... | +

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

ライセンス先 AXCEL 4th environment
500のうち70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 343 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

ドメインの編集

基本 | 認証 | Source | Proxy | 高度な設定

ドメイン名: OnTimeDemo このドメインを無効

優先順位: 1

ドメインタイプ: Exchange Online

Impersonation User: onlinedemo.onmicrosoft.com

パスワード:

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出来ます。

ドメインタイプで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.51 参照

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。

先進認証とGraphによるEWS接続



OnTime - Admin | OnTimeAuth-from-410 - Microso... | +

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

ライセンス先 AXCEL 4th environment
500のうち70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 343 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

ドメインの編集

基本 | 認証 | Source | Proxy | 高度な設定

認証タイプ: 先進認証(OAuth)

アプリケーションID: 7375492f-a...

ディレクトリ(テナント)ID: b943071e-...

クライアントシークレット:

認証タイプは「先進認証(OAuth)」を選択します。
オンプレExchangeもしくはMicrosoft365（但し2021年後半まで）では「基本認証(BASIC)」を選択します。

先進認証(OAuth)に必要な各種IDとパスワードを入力します。メモ帳にコピーした3つのテキストを貼り付けます。

配布リストでアドレスリストを取得



OnTime - Admin

OnTimeAuth-from-410 - Microso...

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

ライセンス先 AXCEL 4th environment
500のうち70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 343 日

ONTIME 管理センター

保存 | キャンセル | 「アプリの登録」を開く | 削除

ドメインの編集

基本 | 認証 | Source | Proxy | 高度な設定

LDAP

LDAPを有効にする

ユーザー

ontimeusers@ontimedemo.com,ontimestaff@ontimedemo.com

会議室

ontimerooms@ontimedemo.com,dynamic@ontimedemo.onmicrosoft.com

備品

ontimeresources@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。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（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、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。

Proxyを利用する場合の設定



The screenshot shows the OnTime Admin interface. The top navigation bar includes the OnTime logo and a license notice: "ライセンス先 AXCEL 4th environment 500のうち70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 343 日". The left sidebar lists various settings: ONTIME 管理センター, 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, ケータリング設定, and 来訪者管理設定. The main content area is titled "ドメインの編集" and has tabs for "基本", "認証", "Source", "Proxy", and "高度な設定". The "Proxy" tab is active, showing two input fields: "ホスト名" (Host Name) and "ポート番号" (Port Number). These two fields are enclosed in a yellow rectangular 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。

高度な設定



OnTime Admin interface showing the '高度な設定' (Advanced Settings) page. The '同期設定' (Synchronization Settings) section is highlighted with a yellow box, showing '起動時の同期スレッド数 (?)' and '連続同期スレッド数 (?)' both set to 5. A yellow arrow points from the '保存' (Save) button in the top navigation bar to the '同期設定' section.

- 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。
 - 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。

設定が完了したら「保存」をクリックします。



OnTime管理センター 保存結果と再起動

設定したドメインリストについて



ドメイン	最終更新日時
1 OnTimeDemo NOT_STARTED 202220CB-ED06-4CC7-B3C1-5346B443D648	最終更新日時: undefined
2 ontimebiz RUNNING 37645AD4-3668-44CC-9A59-F809DC4E581F	レガシー認証が使用されています。2021年夏までに先進認証に変更を検討してください。 最終更新日時: Sat Jan 23 01:03:40 JST 2021
3 axcel NOT_STARTED EA709FCF-A535-4B86-9CEA-5BA9420D708E	レガシー認証が使用されています。2021年夏までに先進認証に変更を検討してください。 最終更新日時: Sat Jan 23 01:03:39 JST 2021

- 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。
- 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) 基本タブと認証タブ オンプレExchangeと基本認証

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。

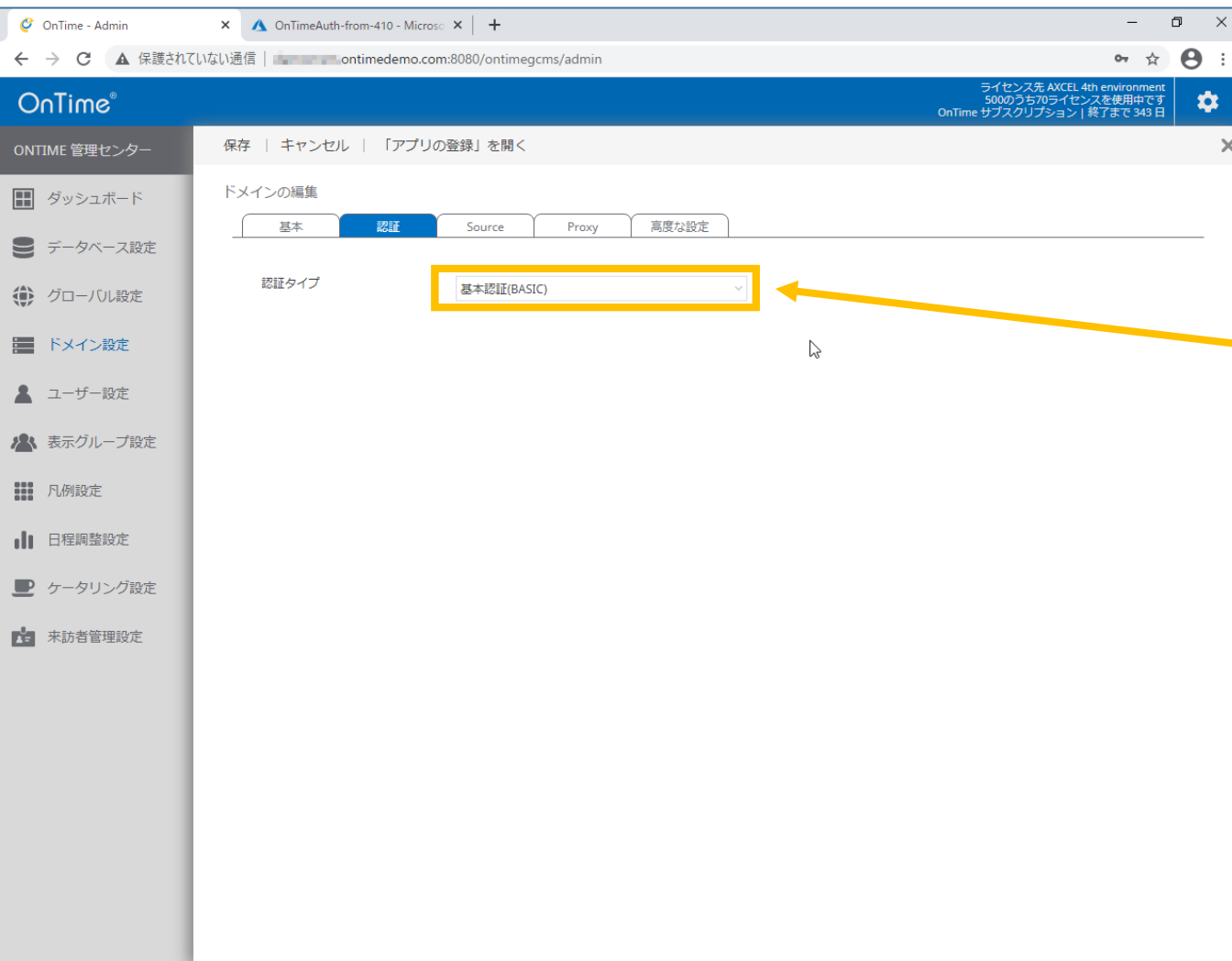
- 優先順位は複数テナント時に同じメールアドレスが使用されている場合にどのテナントを優先するかを指定します。例えばオンプレからクラウドに移行の最中の場合はクラウドを優先したいのでオンプレは大きい数字を指定します。

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



- 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。
2021年後半には利用が禁止される予定です。

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2) リソースタブ LDAPでアドレスリスト取得

LDAPでアドレスリスト取得 1



OnTime Admin interface showing the LDAP configuration page. The 'Source' tab is selected, and the 'LDAPを有効にする' checkbox is checked. A yellow arrow points from the checkbox to a text box on the right.

- 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。

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	
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=*)

<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。



補足3) 認証タブ 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



ライセンス先 AXCEL 4th environment
500のうち10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 342 日

ONTIME 管理センター

ライセンスの編集 更新

タッシュボード

システム状況

アプリケーション:	RUNNING	実行	停止	最終実行日時: Sat Jan 23 13:58:12 JST 2021
有効なライセンスの確認:	RUNNING	実行	停止	最終実行日時: Sat Jan 23 13:58:13 JST 2021

接続状況

SQL DB 接続状況:	RUNNING			最終実行日時: Sat Jan 23 13:58:11 JST 2021
Exchange ドメイン:	1 / 2 RUNNING			

同期スケジュール

Directory Synchronisation:	SCHEDULED TO RUN 02:00	実行		最終実行日時: Sat Jan 23 13:56:06 JST 2021
User & Group Synchronisation:	SCHEDULED TO RUN 02:00	実行		最終実行日時: Sat Jan 23 13:56:07 JST 2021
Photo Synchronisation:	SCHEDULED TO RUN 02:00	実行		最終実行日時: Sat Jan 23 02:00:53 JST 2021
Permission Synchronisation:	SCHEDULED TO RUN 02:00	実行		最終実行日時: Sat Jan 23 02:00:47 JST 2021
Event Synchronisation:	SCHEDULED TO RUN TOMORROW 02:00	実行		最終実行日時: Sat Jan 23 02:00:54 JST 2021

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出来ていない状態です。
- 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 console showing domain settings. The 'OnTimeDemo' domain is highlighted with a red box and an error message: 'エラー: com.ontimesuite.ontime.ms.v2.web.api.v2.Api2ErrorException: Error: Authentication Tokens is expired. Refresh ...'.

ドメイン	ステータス	最終更新日時	エラーメッセージ
OnTimeDemo 202220CB-ED06-4CC7-B3C1-5346B443D648	STOPPED	Sat Jan 23 13:58:12 JST 2021	エラー: com.ontimesuite.ontime.ms.v2.web.api.v2.Api2ErrorException: Error: Authentication Tokens is expired. Refresh ...
ontimebiz 37645AD4-3668-44CC-9A59-F809DC4E581F	RUNNING	Sat Jan 23 13:58:12 JST 2021	レガシー認証が使用されています。2021年夏までに先進認証に変更を検討してください。
axcel EA709FCF-A535-4B86-9CEA-5BA9420D708E	NOT_STARTED	Sat Jan 23 13:58:12 JST 2021	レガシー認証が使用されています。2021年夏までに先進認証に変更を検討してください。

- 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 | OnTimeAuth-from-410 - Microso... | ontimedemo.com:8080/ontimegcms/admin

ライセンス先 AXCEL 4th environment
500のうち70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 343 日

ONTIME 管理センター

保存 | キャンセル | 「アプリの登録」を開く | 削除

ドメインの編集

基本 | 認証 | Source | Proxy | 高度な設定

認証タイプ: 先進認証(OAuth)

アプリケーションID: 7375492f-...

ディレクトリ(テナント)ID: b943071e-...

クライアントシークレット:

追加設定が必要なアクセス許可

- MICROSOFT GRAPH
- Calendars.ReadWrite (APPLICATION)
- Directory.Read.All (APPLICATION)
- EWS.AccessAsUser.All (DELEGATED)
- Place.Read.All (APPLICATION)
- User.Read.All (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。