



# OnTime<sup>®</sup> 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

2021/03/17

# 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

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

認証

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

Source

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

Proxy

https接続でProxy経由の接続が必要な場合の設定 P.47

高度な設定

トレース設定、同期スレッド数の設定 P.48



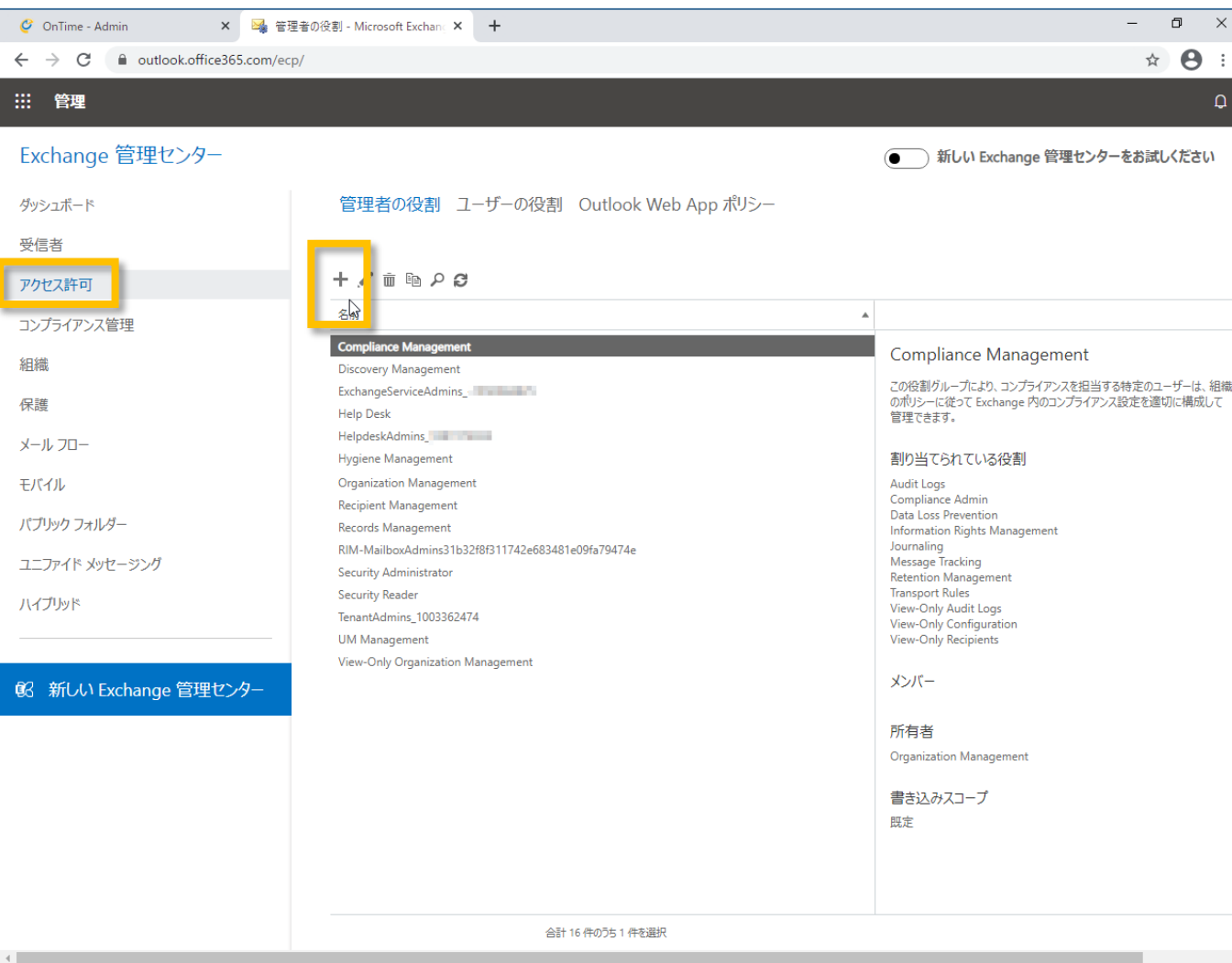
# Exchange管理センターでの作業

# 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Impersonatin(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。

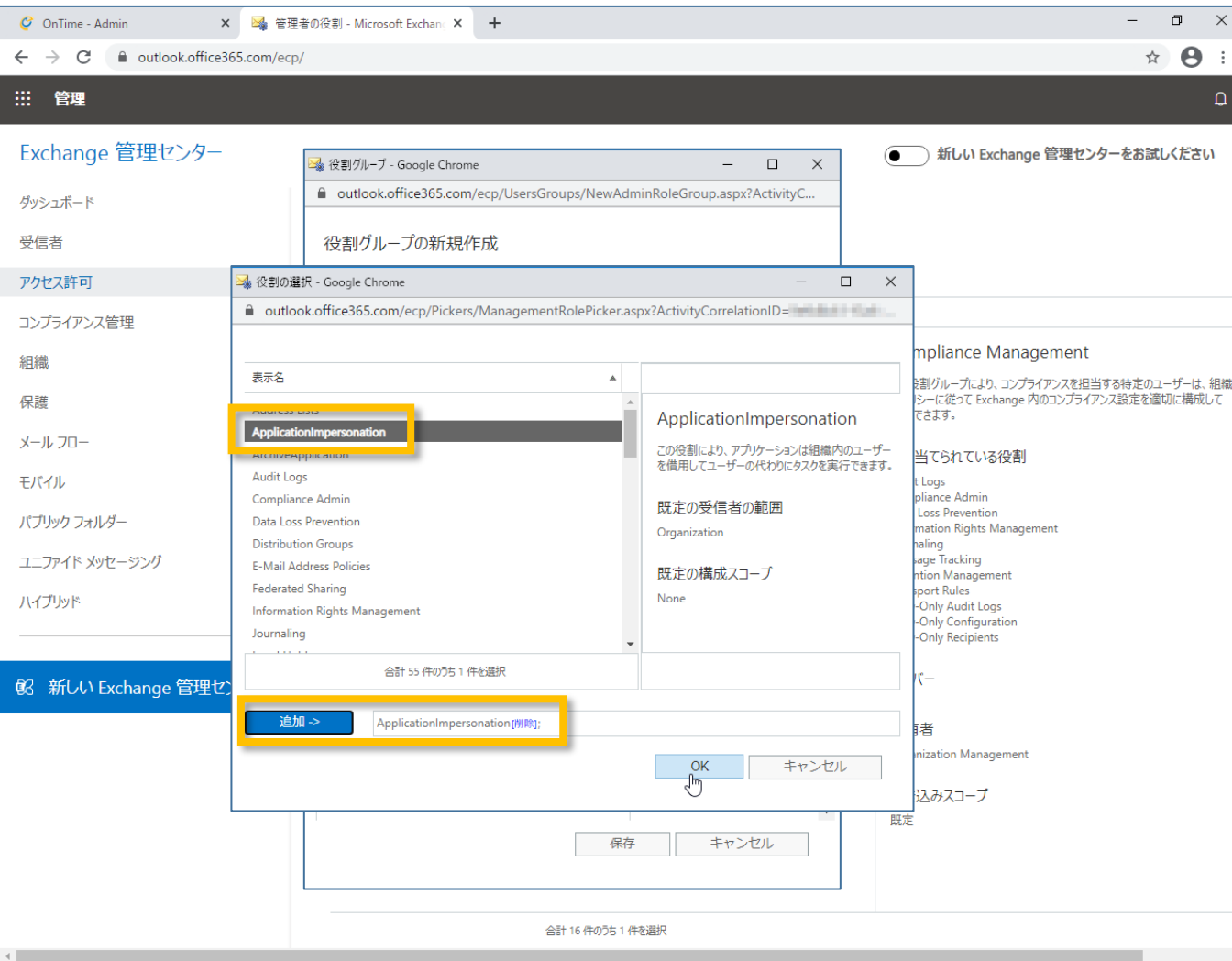


# 管理者の役割の追加 1



- 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



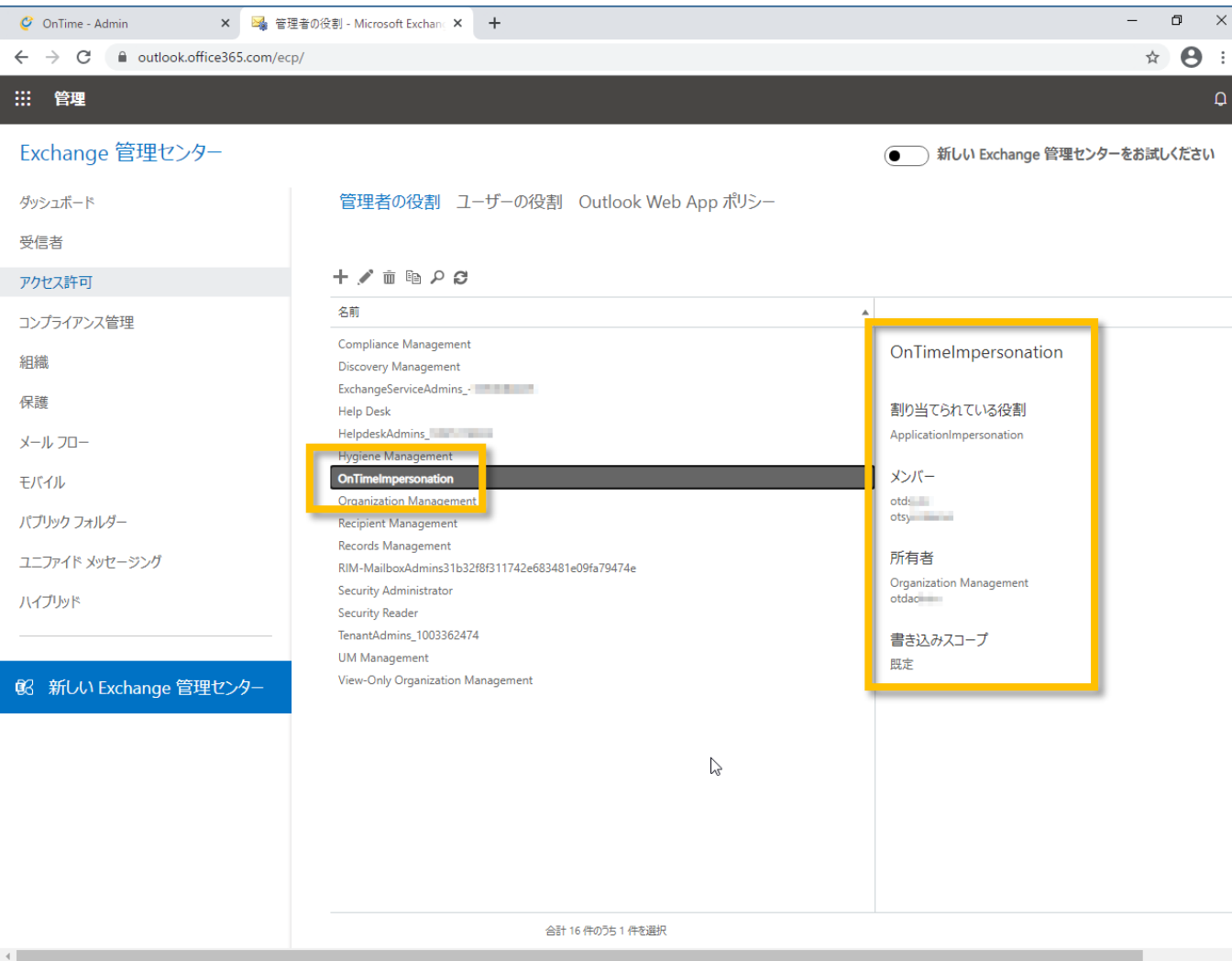
- ApplicationImpersonationを選択します。
- 「追加」を押して追加後に「OK」を押します。

# 管理者の役割の追加 3



- 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



- 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

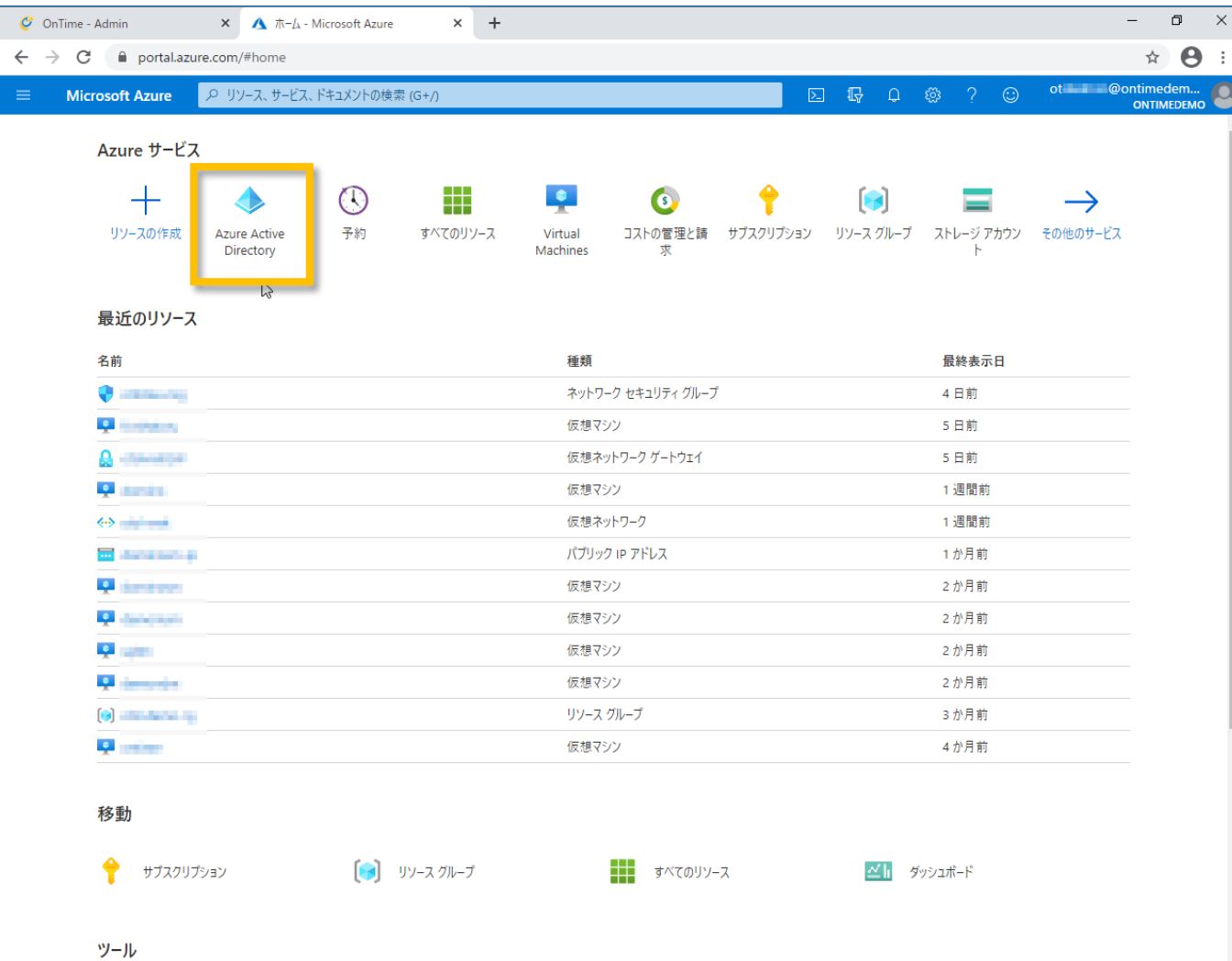
- OnTime が Microsoft365 (Exchange Online) と先進認証(Oauth)で接続する際は Azure Portal で「アプリの登録」を行う必要があります。以下の情報を参考に認証方式は先進認証(Oauth) を採用してください。
- Exchange Online の基本認証が非推奨となります(Microsoft Docs発行元：2019年9月20日)  
<https://docs.microsoft.com/ja-jp/lifecycle/announcements/exchange-online-basic-auth-deprecated>
  - --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

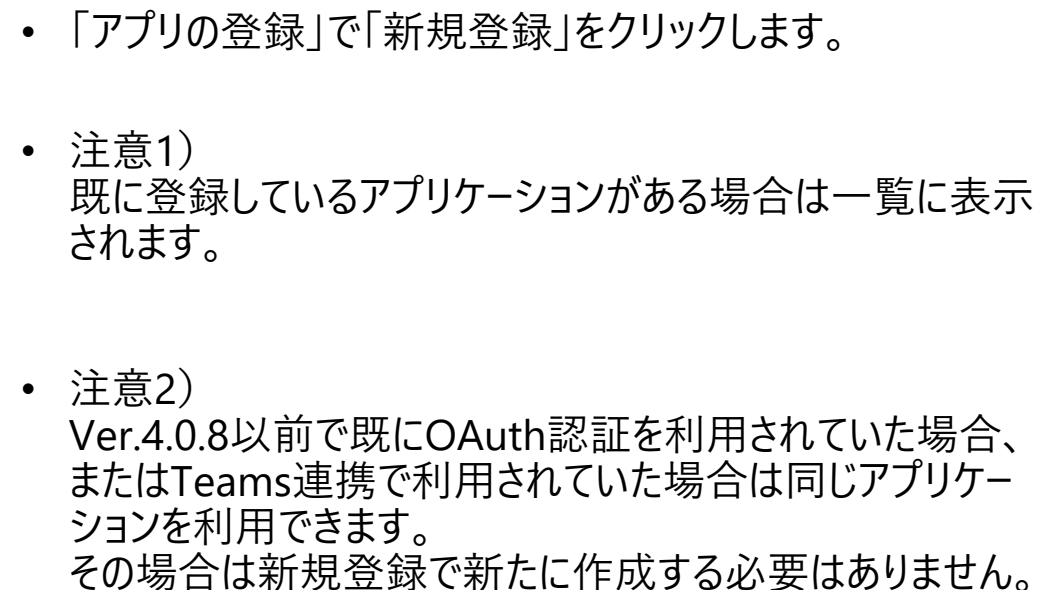


# アプリの登録 2



The screenshot displays the Azure Active Directory (Azure AD) portal for the 'ontimedemo' tenant. The left-hand navigation pane contains various management options, with 'アプリの登録' (App Registrations) highlighted by a yellow rectangular box. The main area of the portal shows the 'ontimedemo' tenant details, including its ID, primary domain, and a sign-in graph. The graph shows a peak in sign-ins around January 17th, with a total of 371 sign-ins recorded.

- 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 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するための API にアクセスし、呼び出せるのはどれですか？

☒ この組織ディレクトリのみ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) または個人の 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。

# アプリの各IDの設定 1



OnTime - Admin

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

Microsoft Azure

ホーム > ontimedemo >

OnTimeAuth-from-410

検索 (Ctrl+/)

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

基本

表示名  
OnTimeAuth-from-410

アプリケーション (クライアント) ID  
7375492f-a0c3-41

ディレクトリ (テナント) ID  
b943071e-ff87-44

オブジェクト ID  
6548d867-88af-4a

クリップボードにコピー

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

リダイレクト URI  
1 個の Web、0 個の SPA、0 個のパブリック クライアント

アプリケーション ID の URI  
アプリケーション ID URI の追加

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  
OnTimeAuth-from-410

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

5 分以内にユーザーをサインインする

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

- 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



- 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



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 | 証明書とシークレット

検索 (Ctrl+/) << フィードバックがある場合

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**  
トークン機能  
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

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 | 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 | ID |
|-------------------------------------|------|---|----|
| 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。 |      |   |    |

- 「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

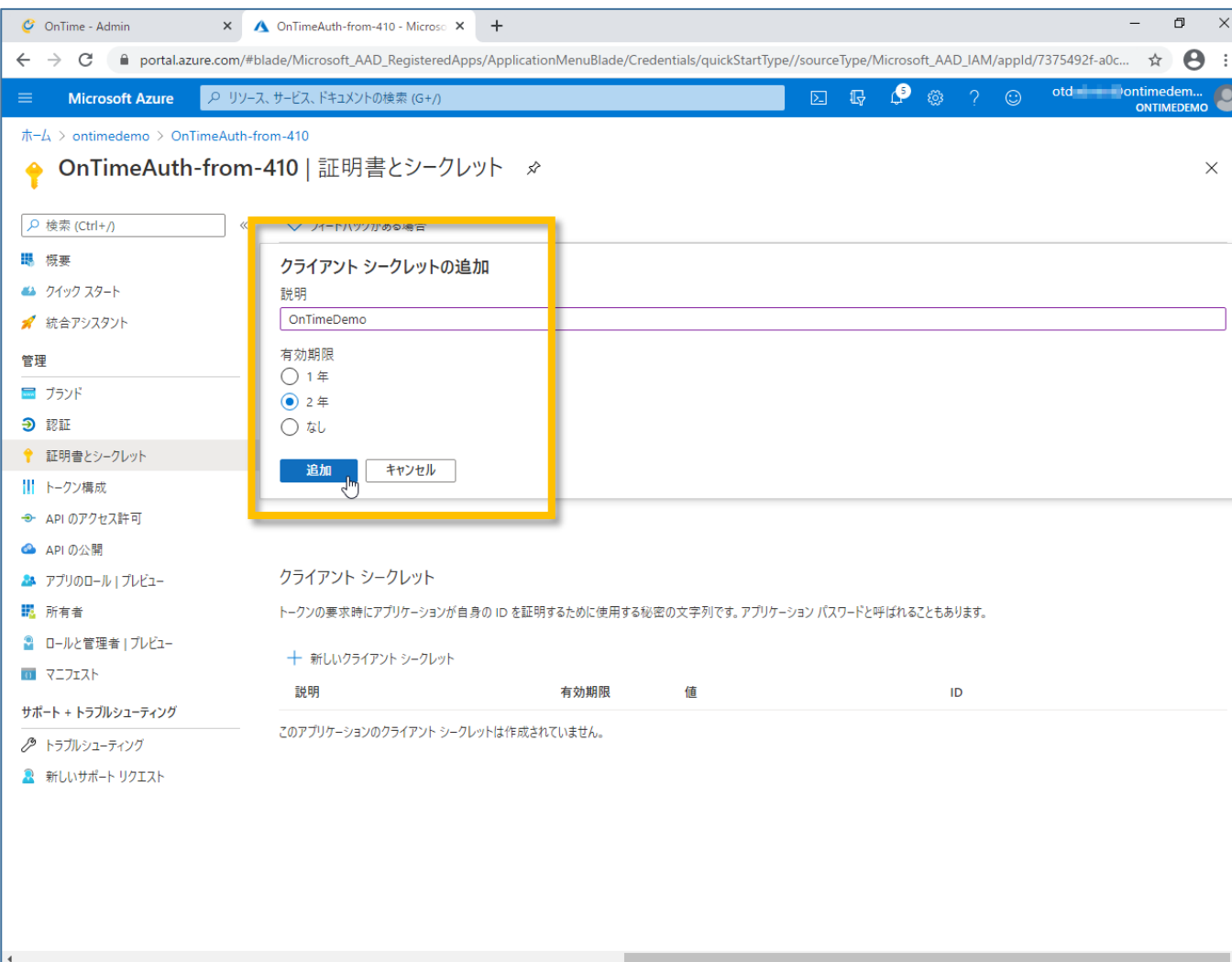


The screenshot shows the OnTime Admin console for the application 'OnTimeAuth-from-410'. The left sidebar contains navigation links: Home, Overview, Quick Start, Integration Assistant, Management, Certificates and Secrets (selected), Token Configuration, API Access Permissions, API Public, App Roles | Preview, Owners, Roles and Administrators | Preview, Manifests, Support + Troubleshooting, Troubleshooting, and New Support Request. The main content area is titled 'OnTimeAuth-from-410 | 証明書とシークレット'. It includes a search bar, a feedback link, and sections for 'Certificates' and 'Client Secrets'. The 'Client Secrets' section has a table with columns '説明' (Description), '有効期限' (Expiration), '値' (Value), and 'ID'. A '+ 新しいクライアント シークレット' (New Client Secret) button 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



OnTime - Admin | OnTimeAuth-from-410 - Microsoft

portal.azure.com/#blade/Microsoft\_AAD\_RegisteredApps/ApplicationMenuBlade/Credentials/quickStartType//sourceType/Microsoft\_AAD\_IAM/applid/7375492f-a0c...

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 | 証明書とシークレット

検索 (Ctrl+/) | フィードバックがある場合

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、それを取扱できなくなります。

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

| 拇印                         | 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                             |
|------------|-----------|-------------------------------|
| OnTimeDemo | 2023/1/23 | UlpR6C... b6078c1...04e1-4... |

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。

# APIのアクセス許可 1



- 「APIのアクセス許可」タブに移動します。
- こちらは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: データ資産を登録、注釈、検索するための Data Catalog リソースへのプログラムによるアクセス
- Azure Data Explorer: ほぼリアルタイムの複雑な分析ソリューションを構築するため、TB 単位のデータに対してアドホッククエリを実行する
- Azure Data Explorer (with Multifactor Authentication): ほぼリアルタイムの複雑な分析ソリューションを構築するため、TB 単位のデータに対してアドホッククエリを実行する
- Azure Data Lake: ビッグ データ分析シナリオのストレージとコンピューティングへのアクセス
- Azure DevOps: Azure DevOps と Azure DevOps Server との統合
- Azure Import/Export: インポート/エクスポート ジョブのプログラムによる制御
- Azure Key Vault: ご利用のキー コンテナーに加え、そのキー コンテナー内のキー、シークレット、証明書を管理します
- Azure Maps: Azure のシンプルで安全な地理空間サービス、API、SDK を利用して、位置情報認識の Web およびモバイル アプリケーションを作成します
- Azure Purview: オンプレミス、マルチクラウド、サービスとしてのソフトウェア (SaaS) のデータの管理と制御に役立つ統合データガバナンス サービス
- Azure Rights Management Services: 検証済みのユーザーに、保護されたコンテンツの読み取りと書き込みを許可します
- Customer Insights: 製品のプロファイルと対話のモデルを作成します
- Dynamics ERP: Dynamics ERP データへのプログラムによるアクセス
- Speech: 音声テキスト変換とテキスト読み上げを使用して、音声対応の強力な機能を作成します
- Universal Print: プリンターと印刷ジョブ リソースを作成および管理するためのプログラムによるアクセス

- 「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



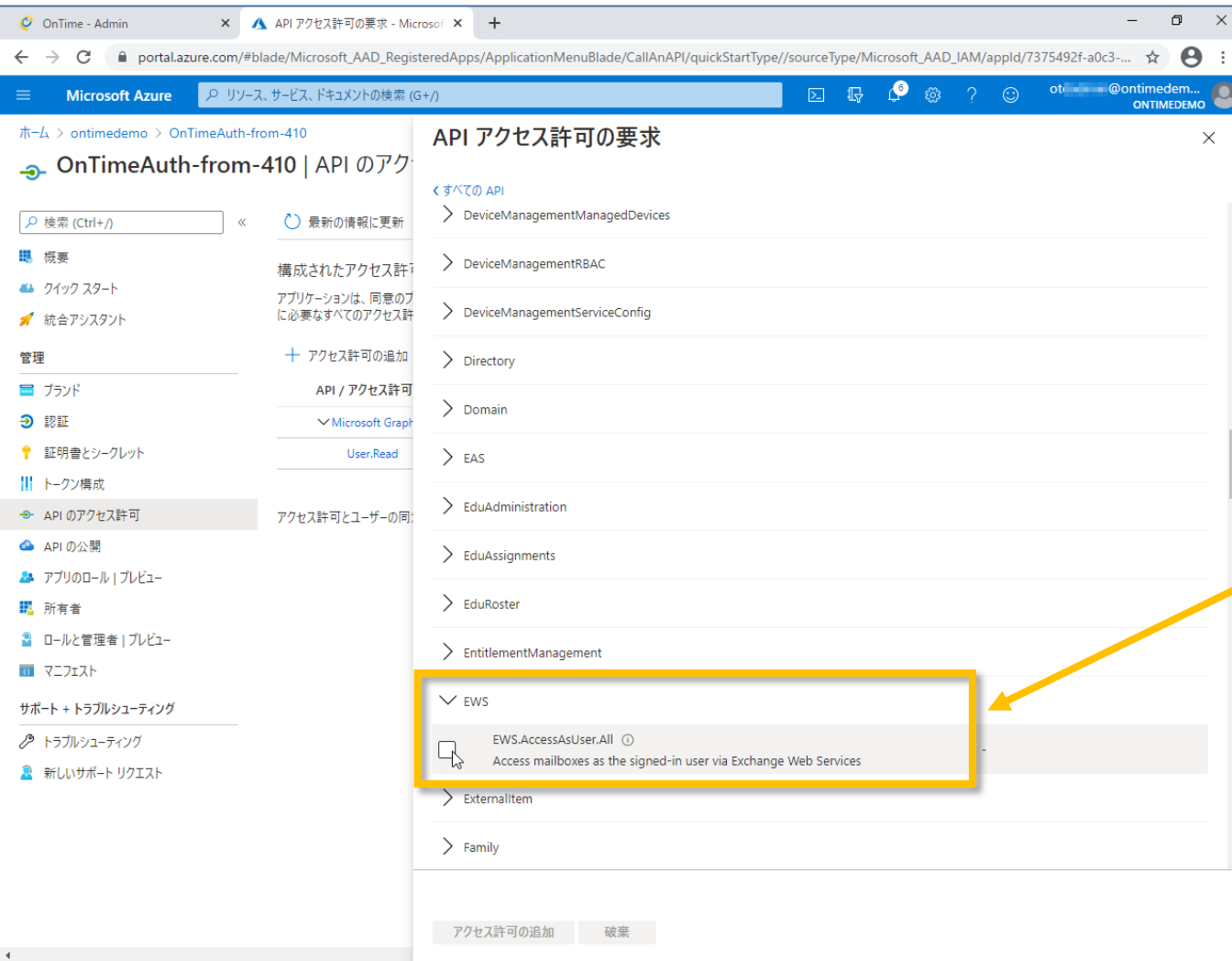
- 「Microsoft Graph」をクリックします。

# APIのアクセス許可 4



- 「委任されたアクセス許可」をクリックします。

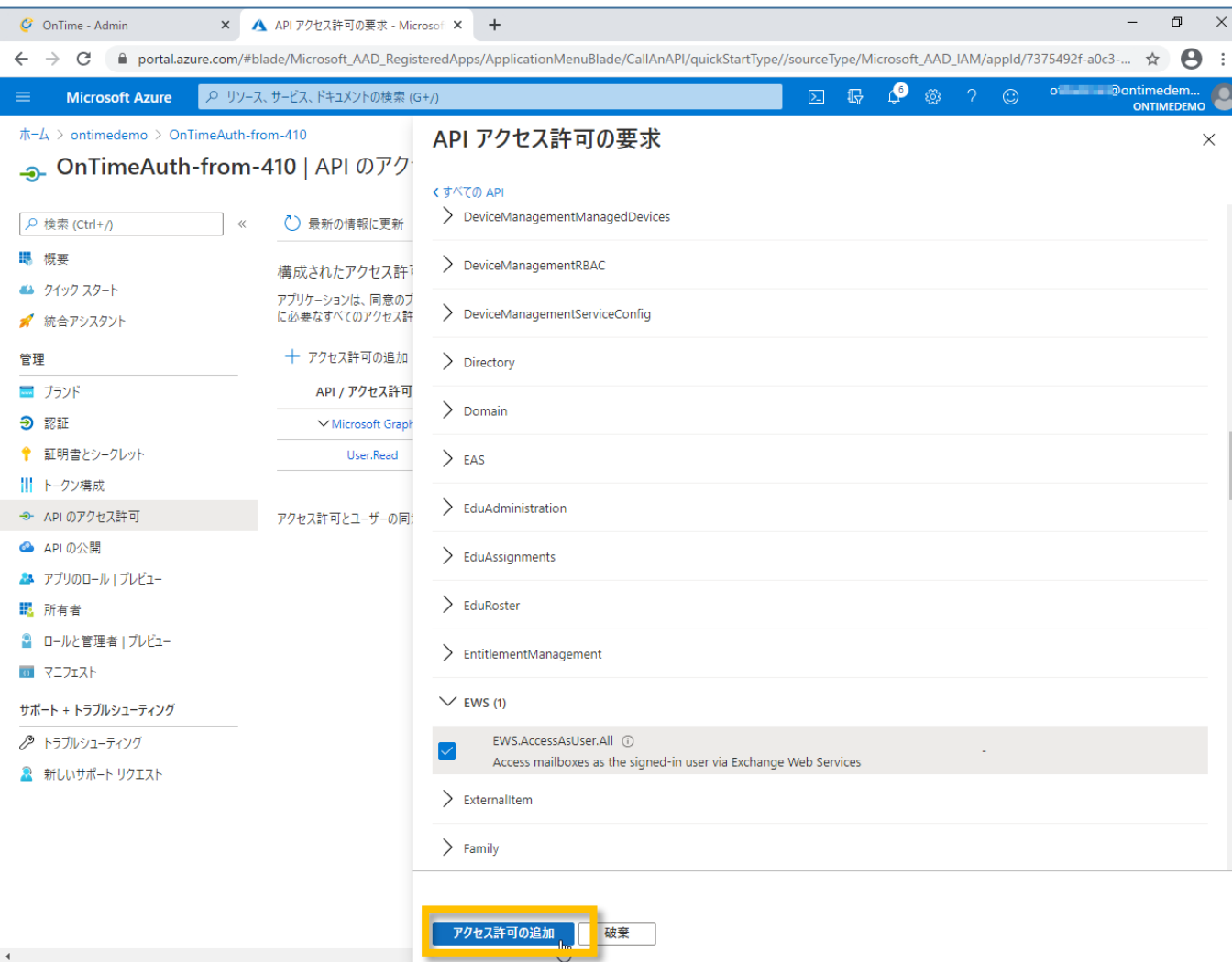
# APIのアクセス許可 5



- 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



- 「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



OnTime - Admin | OnTimeAuth-from-410 - 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-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

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 | 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 (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



API アクセス許可の要求

Microsoft Graph  
https://graph.microsoft.com/ ドキュメント

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 API にアクセスする必要があります。 | 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。 |

アクセス許可の追加 破棄

- 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



API アクセス許可の要求

- AppRoleAssignment
- ApprovalRequest
- AuditLog
- BitlockerKey
- Calendars (1)
  - Calendars.Read
  - ☒ Calendars.ReadWrite
- CallRecord-PstnCalls
- CallRecords
- Calls
- Channel
- ChannelMember
- ChannelMessage
- ChannelSettings

アクセス許可の追加 破棄

- 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

すべての API

- Device
- DeviceManagementApps
- DeviceManagementConfiguration
- DeviceManagementManagedDevices
- DeviceManagementRBAC
- DeviceManagementServiceConfig

Directory (1)

- ☒ Directory.Read.All (1)  
Read directory data
- ☐ Directory.ReadWrite.All (1)  
Read and write directory data

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



Microsoft Azure portal showing the 'API Access Permissions' page for an application named 'OnTimeAuth-from-410'. The page lists various permissions under the heading 'API アクセス許可の要求'. A yellow box highlights the 'Place (1)' section, which contains the permission 'Place.Read.All' with a checked checkbox. An arrow points from a text box to this checkbox.

- 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 'API のアクセス許可' (API Permissions) section. The main content area shows a list of permissions under the 'User (1)' category. The 'User.Read.All' permission is selected, and its description 'Read all users' full profiles' is visible. A yellow box highlights the 'User.Read.All' permission, and a yellow arrow points from the text box on the right to this permission.

| API                      | 権限                                                | 権限の説明                                                | 権限の範囲 |
|--------------------------|---------------------------------------------------|------------------------------------------------------|-------|
| TermStore                | TermStore.Read                                    | Read all terms                                       | はい    |
|                          | TermStore.Read.All                                | Read all terms in the organization                   | はい    |
|                          | TermStore.Write                                   | Write terms                                          | はい    |
|                          | TermStore.Write.All                               | Write terms in the organization                      | はい    |
|                          | TermStore.Delete                                  | Delete terms                                         | はい    |
| ThreatAssessment         | ThreatAssessment.Read                             | Read threat assessment results                       | はい    |
|                          | ThreatAssessment.Read.All                         | Read threat assessment results in the organization   | はい    |
| ThreatIndicators         | ThreatIndicators.Read                             | Read threat indicators                               | はい    |
|                          | ThreatIndicators.Read.All                         | Read threat indicators in the organization           | はい    |
| TrustFrameworkKeySet     | TrustFrameworkKeySet.Read                         | Read trust framework key sets                        | はい    |
|                          | TrustFrameworkKeySet.Read.All                     | Read trust framework key sets in the organization    | はい    |
| UserAuthenticationMethod | UserAuthenticationMethod.Read                     | Read user authentication methods                     | はい    |
|                          | UserAuthenticationMethod.Read.All                 | Read user authentication methods in the organization | はい    |
| UserNotification         | UserNotification.Read                             | Read user notifications                              | はい    |
|                          | UserNotification.Read.All                         | Read user notifications in the organization          | はい    |
| UserShiftPreferences     | UserShiftPreferences.Read                         | Read user shift preferences                          | はい    |
|                          | UserShiftPreferences.Read.All                     | Read user shift preferences in the organization      | はい    |
| 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



API アクセス許可の要求

すべての API

- TermStore
- ThreatAssessment
- ThreatIndicators
- TrustFrameworkKeySet
- UserAuthenticationMethod
- UserNotification
- UserShiftPreferences

User (1)

|                                     |                                                                 |    |
|-------------------------------------|-----------------------------------------------------------------|----|
| <input type="checkbox"/>            | User.Export.All ⓘ<br>Export user's data                         | はい |
| <input type="checkbox"/>            | User.Invite.All ⓘ<br>Invite guest users to the organization     | はい |
| <input type="checkbox"/>            | User.ManageIdentities.All ⓘ<br>Manage all users' identities     | はい |
| <input checked="" type="checkbox"/> | User.Read.All ⓘ<br>Read all users' full profiles                | はい |
| <input type="checkbox"/>            | User.ReadWrite.All ⓘ<br>Read and write all users' full profiles | はい |

アクセス許可の追加 破棄

- 「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

⚠️ 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... | -         |                        |
| 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                          | -         |                        |
| 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。

- 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



OnTime - Admin | OnTimeAuth-from-410 - 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+J)

ホーム > ontimedemo > OnTimeAuth-from-410

OnTimeAuth-from-410 | API のアクセス許可 ✕

検索 (Ctrl+J) | 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に更新されます。

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 1 6



OnTime - Admin | OnTimeAuth-from-410 - 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-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

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

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... |

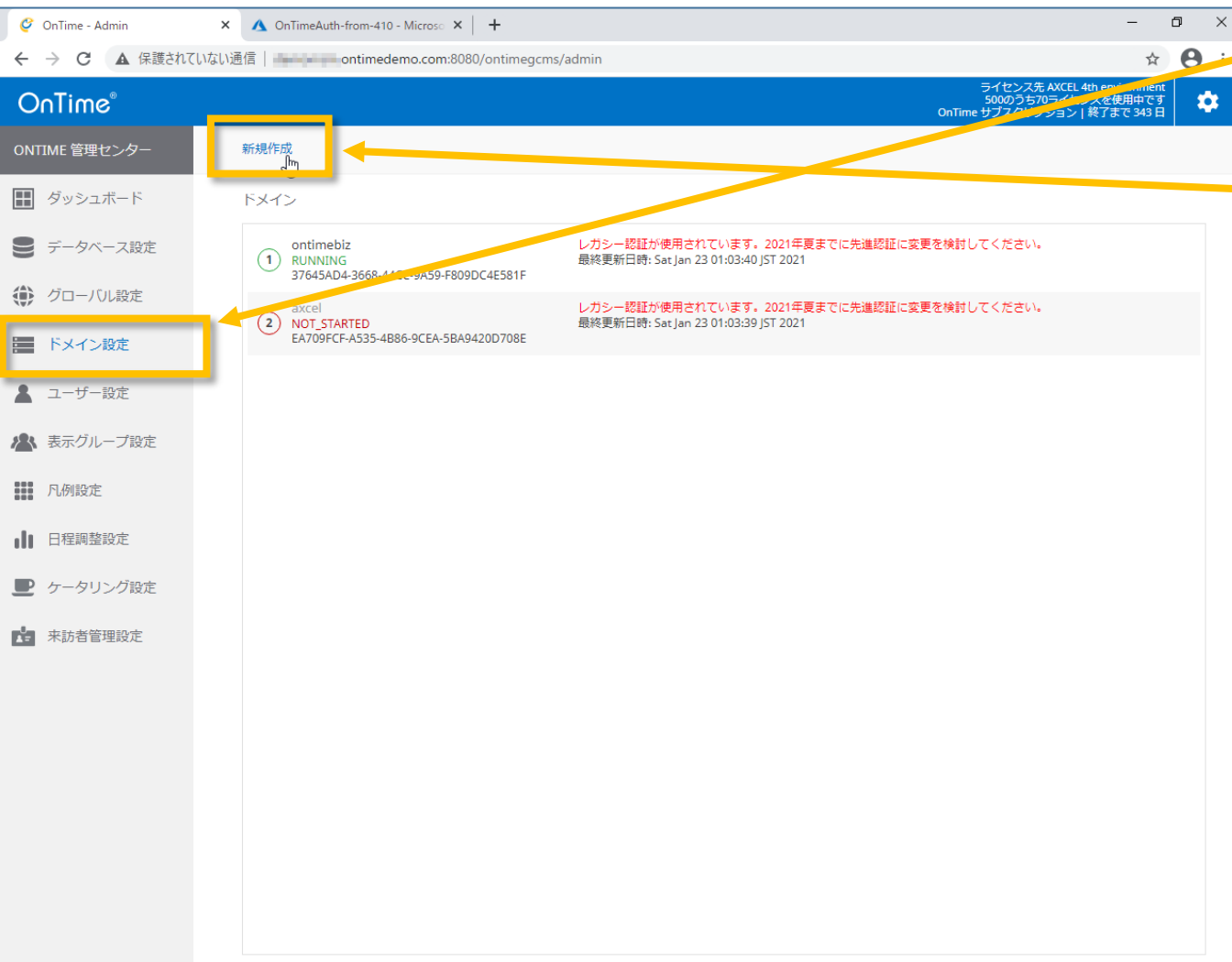
アクセス許可とユーザーの同意を表示および管理するために、[エンタープライズ アプリケーション](#)をお試しください。

- 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



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



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 - Microsoft

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

アプリケーションID

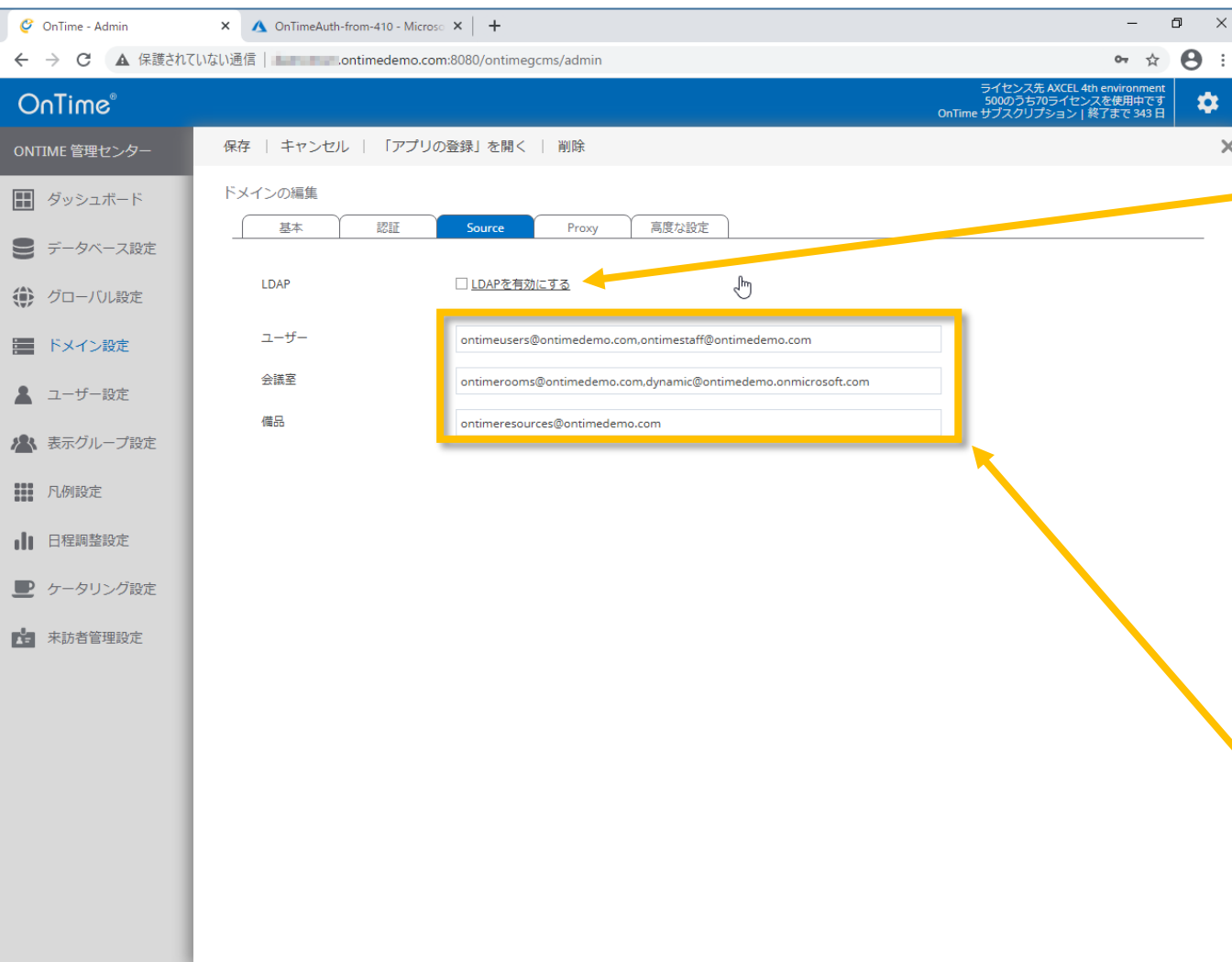
ディレクトリ(テナント)ID

クライアントシークレット

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



- 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

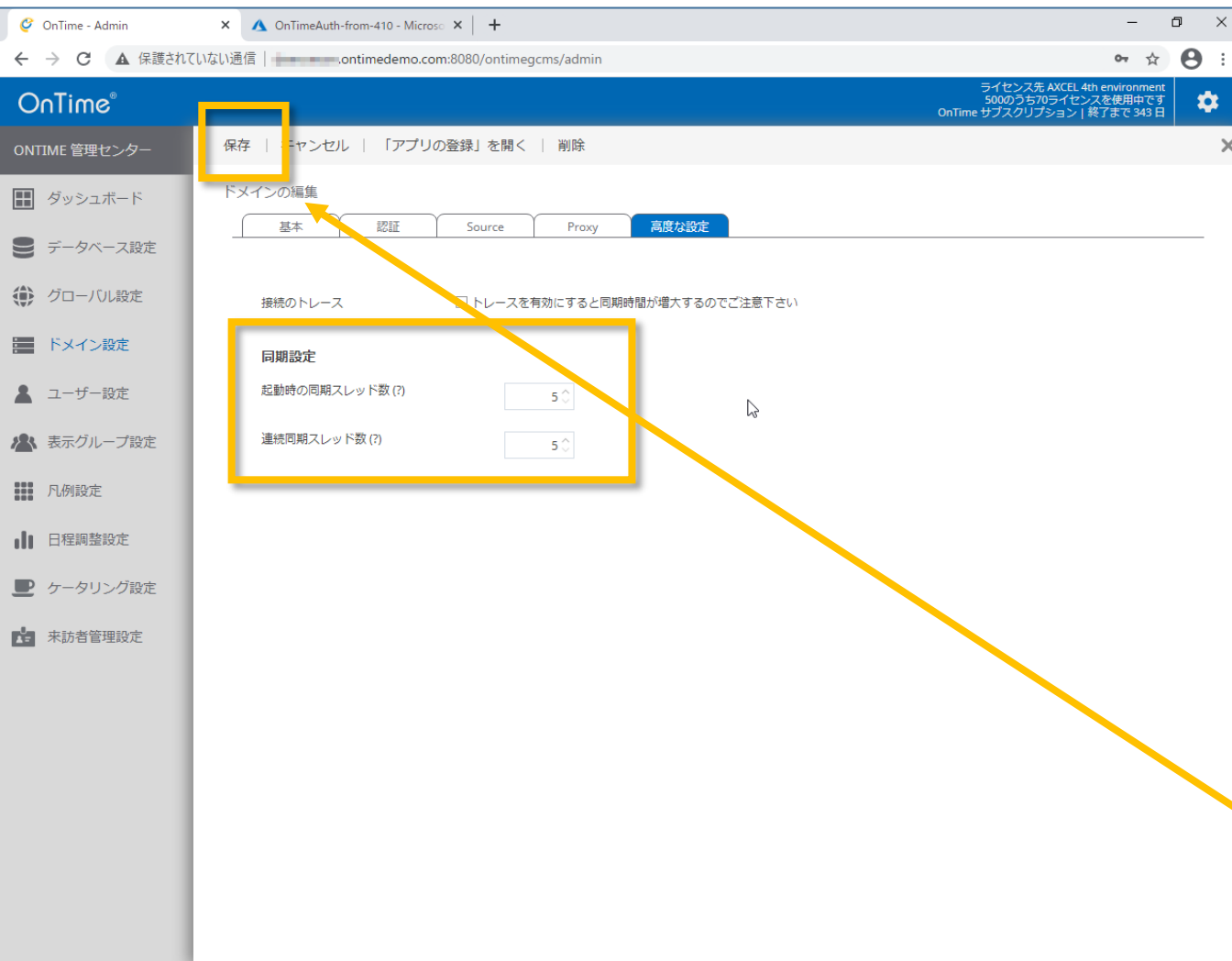


The screenshot shows the OnTime Admin interface. The top navigation bar includes the OnTime logo, a user profile, and a settings gear. The main content area is titled 'ドメインの編集' (Edit Domain) and has tabs for '基本' (Basic), '認証' (Authentication), 'Source', 'Proxy', and '高度な設定' (Advanced Settings). The 'Proxy' tab is active. Below the tabs, there are two input fields: 'ホスト名' (Host Name) and 'ポート番号' (Port Number). These fields are highlighted with a yellow rectangular box. The left sidebar contains various management options like 'ダッシュボード' (Dashboard), 'データベース設定' (Database Settings), 'グローバル設定' (Global Settings), 'ドメイン設定' (Domain Settings), 'ユーザー設定' (User Settings), '表示グループ設定' (Display Group Settings), '凡例設定' (Legend Settings), '日程調整設定' (Schedule Adjustment Settings), 'ケータリング設定' (Catering Settings), and '来訪者管理設定' (Visitor Management Settings).

- 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



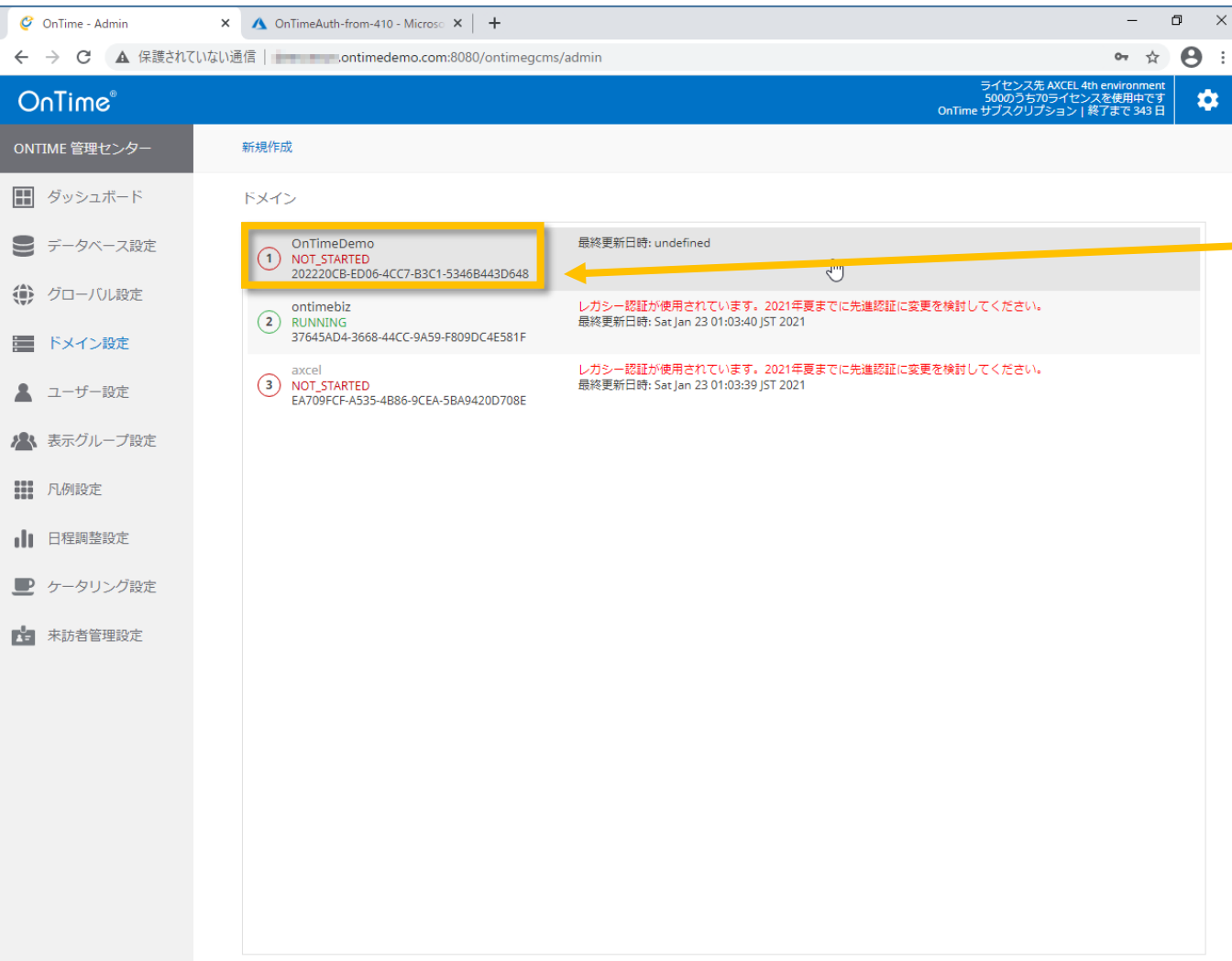
- 接続のトレースはチェックをつけません。サポートから依頼があった場合のみ設定してください。
- 同期設定では「起動時」「通常運用時」それぞれのスレッド数を指定できます。
  - Exchange上のイベント更新情報がOnTimeに反映されるのが遅い場合はOnTimeの同期処理がExchange上のイベント更新頻度に追いついていない可能性があります。そのような場合にスレッド数を増やすことで改善する場合があります。
  - 最小数は5です。**起動時設定は5を推薦します。**
  - OnTimeサーバーのCPUやメモリに十分なパワーがある場合はCPUやメモリの使用率を見ながら徐々に数値を変更してみてください。
  - 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。



# 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



- 画面が閉じると先ほど設定したドメインが増えています。

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。

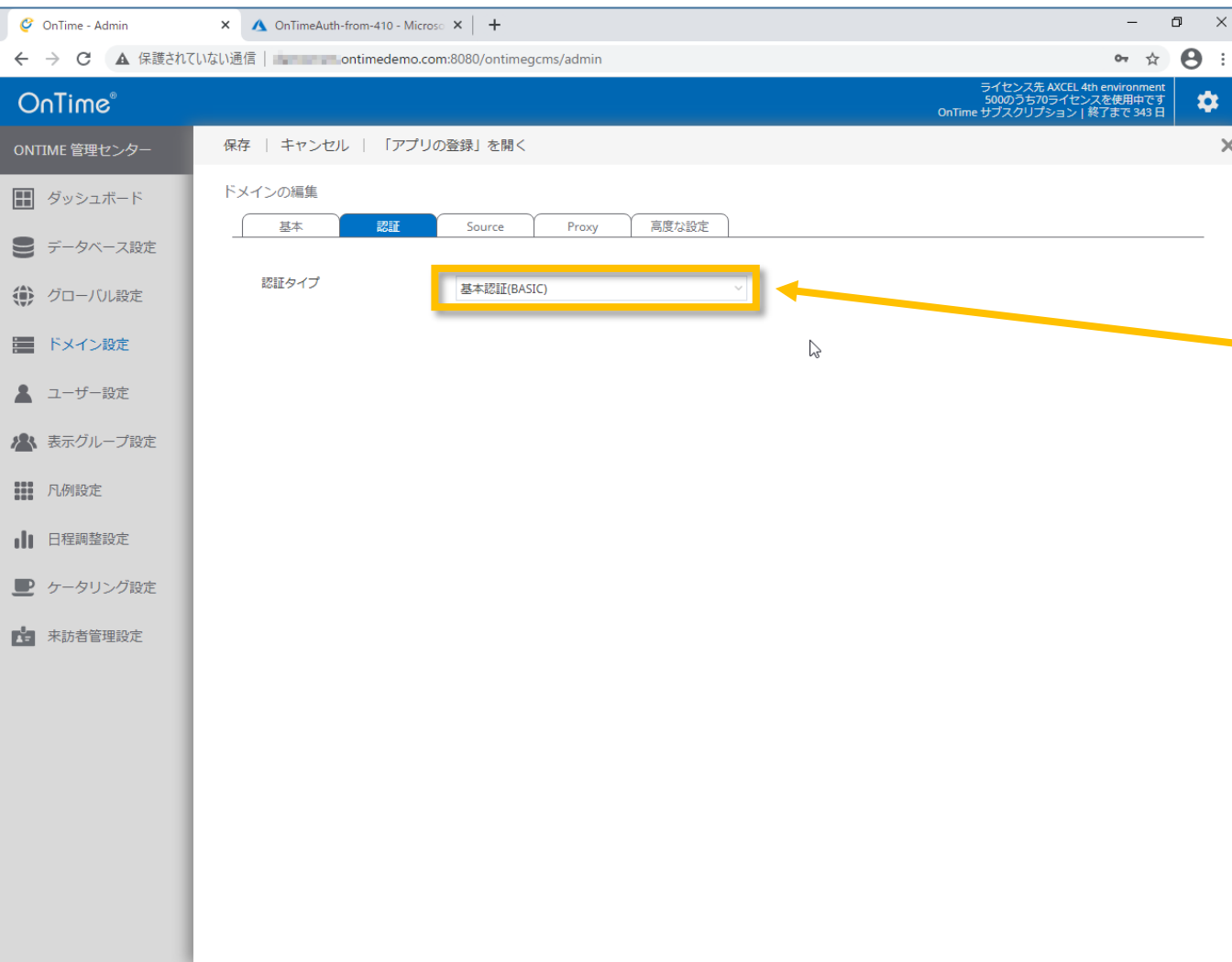
- 優先順位は複数テナント時に同じメールアドレスが使用されている場合にどのテナントを優先するかを指定します。例えばオンプレからクラウドに移行の最中の場合はクラウドを優先したいのでオンプレは大きい数字を指定します。

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 ☒ 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 .....

テスト

ベース OU=o365, DC=ontime, DC=otbz

スコープ SUB\_TREE

フィルター (cn=\*)

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 .....

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)

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



OnTime Admin interface showing system status. The 'Exchange ドメイン' (Exchange Domain) 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 | Sat Jan 23 13:58:12 JST 2021 |
| 有効なライセンスの確認:                  | RUNNING                         | 実行 | 停止 | Sat Jan 23 13:58:13 JST 2021 |
| 接続状況                          |                                 |    |    |                              |
| SQL DB 接続状況:                  | RUNNING                         |    |    | 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 |    | Sat Jan 23 13:56:06 JST 2021 |
| User & Group Synchronisation: | SCHEDULED TO RUN 02:00          | 実行 |    | Sat Jan 23 13:56:07 JST 2021 |
| Photo Synchronisation:        | SCHEDULED TO RUN 02:00          | 実行 |    | Sat Jan 23 02:00:53 JST 2021 |
| Permission Synchronisation:   | SCHEDULED TO RUN 02:00          | 実行 |    | Sat Jan 23 02:00:47 JST 2021 |
| Event Synchronisation:        | SCHEDULED TO RUN TOMORROW 02:00 | 実行 |    | 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                        |                                 |    |    |                              |

- インジケター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



- 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 - Microsoft

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。