OnTime® GROUP CALENDAR

for Microsoft(Ver.5.3-)
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

2023/01/11

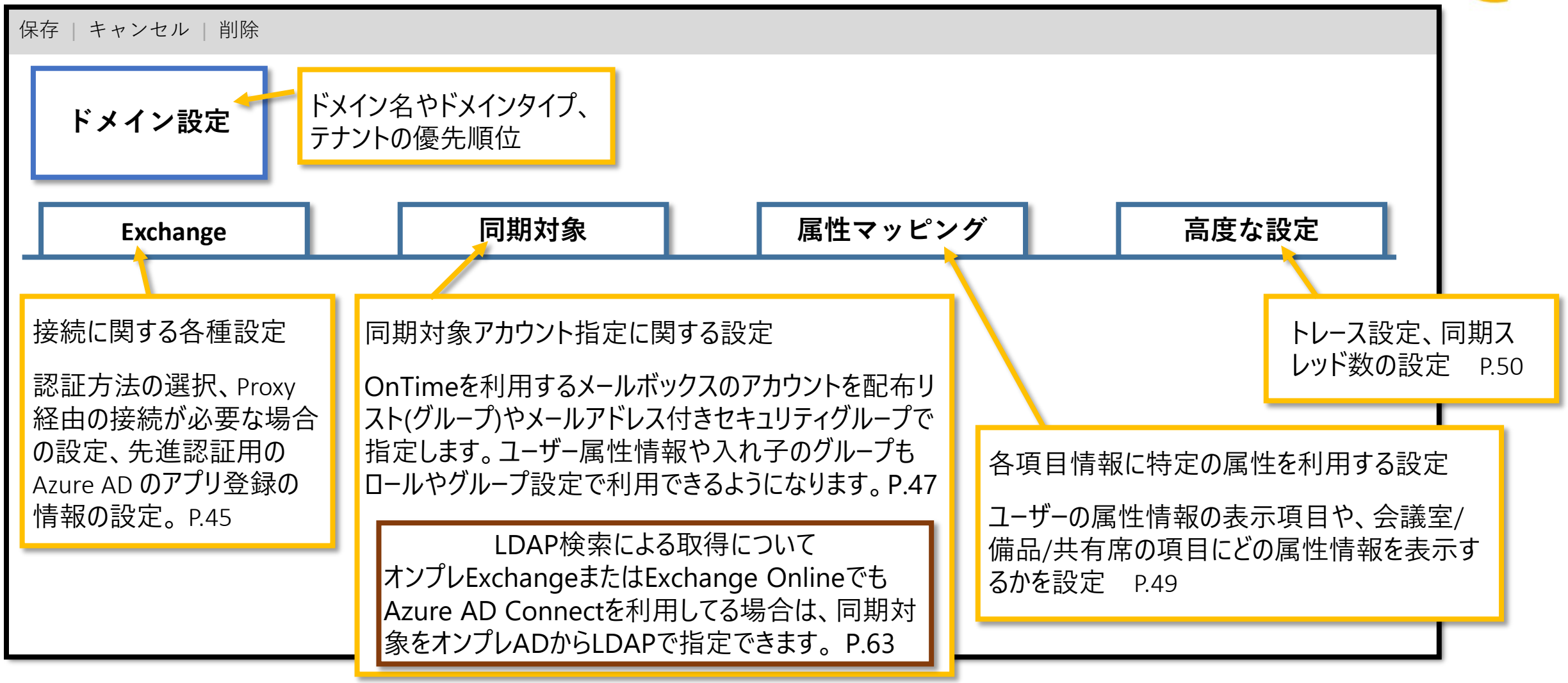
目次　ドメイン設定マニュアル

ドメイン設定について

ドメイン設定ページについて

- 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Microsoft365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等API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イメージを表示します。
  - その他補足事項

ドメイン設定ページの構成



認証方式について

- ドメイン設定の認証タイプで設定する認証方式はOnTimeサーバーがExchangeへ接続する認証方式の設定です。
  ユーザーがOnTimeサーバーへ接続する際の認証方式は別途「フロントエンド」ページで設定します。
- ドメイン設定で指定できる認証方式にはExchange Onlineへの３方式とオンプレExchangeへの1方式の4つがあります。
- 「**先進認証(OAuth - Client資格情報フロー - Client Credentials)**」
  - Azure ADの「アプリの登録」で設定するClient資格情報だけで接続します。
  - アクセスする対象は別途指定する同期対象だけで全テナントユーザーを対象とするわけではありません。
  - **本マニュアルではShop推奨手順として「先進認証(OAuth - Client資格情報フロー - Client Credentials)」をご紹介します。**
- 「先進認証(OAuth - 認可コードフロー - Impersonation User)」
  - 同期を代理で行うユーザーに対象となるメールボックスへのApplication Impersonationの管理者役割の付与が必要となります。
  - 手順参照先・・補足1「先進認証(OAuth - 認可コードフロー - Impersonation User)」　P.53
- 「基本認証(BASIC)」
  - 2023年のExchange Onlineでは特別な理由が無い限り使用しません。
- 接続先Exchangeを「オンプレExchange」にした場合の基本認証方式
  - 手順参照先・・補足2「オンプレExchange の設定」　P.61

Microsoft環境への接続ポート、接続URLについて

- ドメイン設定ではMicrosoft環境の特定URLに接続します。
- Microsoft環境との通信は以下のURLから始まる通信となります。いずれも TCP ポート番号は 443 だけとなります。
  PROXY を経由する通信ももちろん可能です。
  （PROXYの設定はOnTime管理センターのドメイン設定 にて設定）
  （製品の仕様変更により今後変更する可能性はあります）
  - —Microsoft Exchange Online 向け
    - https://outlook.office365.com
  - —Microsoft Graph 及び Microsoft Azure 向け
    - https://login.microsoftonline.com
    - https://graph.microsoft.com
    - https://portal.azure.com

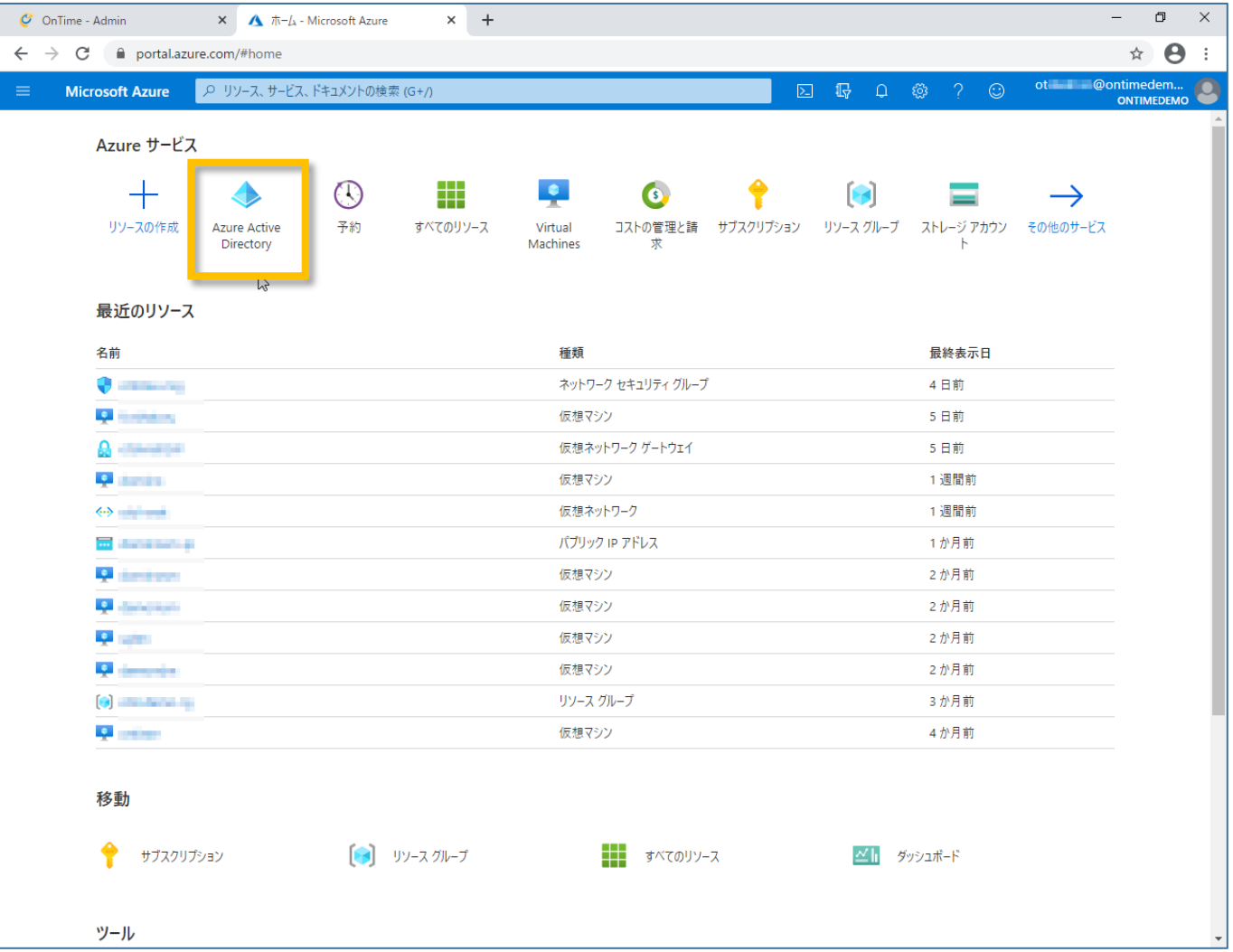
Microsoft Teams連携及びサーバー証明書について

- Teams会議の作成機能は認証方式で先進認証を選択している場合は標準機能です。
  OnTimeサーバーにTLS(SSL)証明書を準備しなくても利用いただけます。
- Teamsアプリへの埋め込み機能はMicrosoftの仕様により組織の実在性と本人性の証明のため、OnTimeサーバーへのパブリックなTLS(SSL)証明書の実装が必須となります。
- OnTimeサーバーへのTLS(SSL)証明書の実装方法はFAQの「OnTimeサーバーにTLS(SSL)証明書を設定する」をご参照ください。
- Teamsアプリへの埋め込み機能の登録方法は「Microsoft Teams アプリ登録マニュアル」をご参照ください。

- OnTimeサーバーへのTLS(SSL)証明書の必要性について
  - Teams会議作成機能の利用のみでTeamsアプリへの埋め込みをしない場合は前述の通り証明書は必要としません。
    例えばトライアルなど操作性の検証目的とした環境の場合も証明書は必要としません。
  - Teamsでタブアプリやレールアプリとして OnTimeを利用する場合は証明書は必須です。
  - ユーザーがOnTimeサーバーに接続する際の通信の暗号化の為にも一般的な手法として証明書を必要とします。
    ユーザーがOnTimeサーバーへ接続する際の認証方式は別途「フロントエンド」ページで設定します。

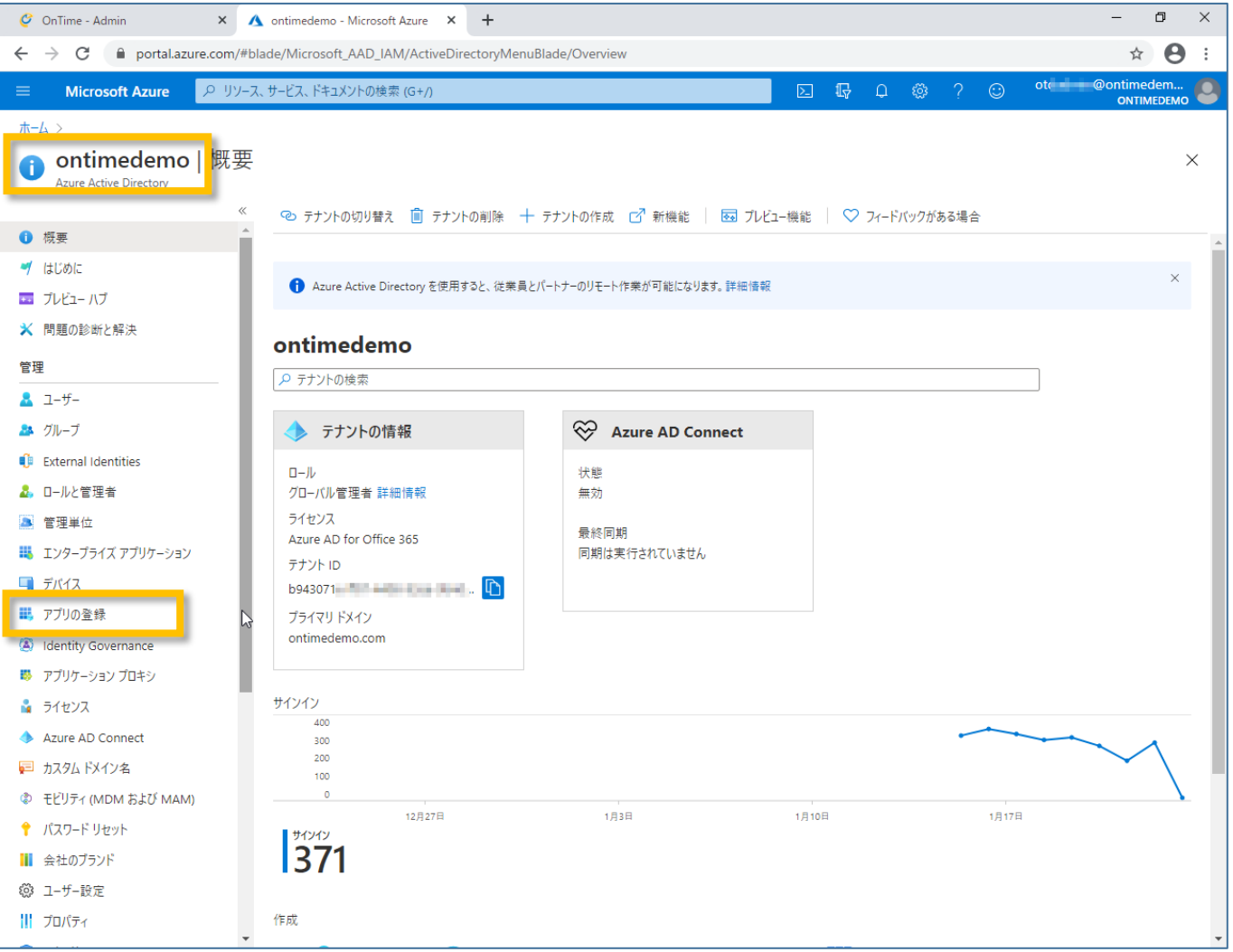
Azure Portal(AzureAD)での作業
アプリの登録

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。

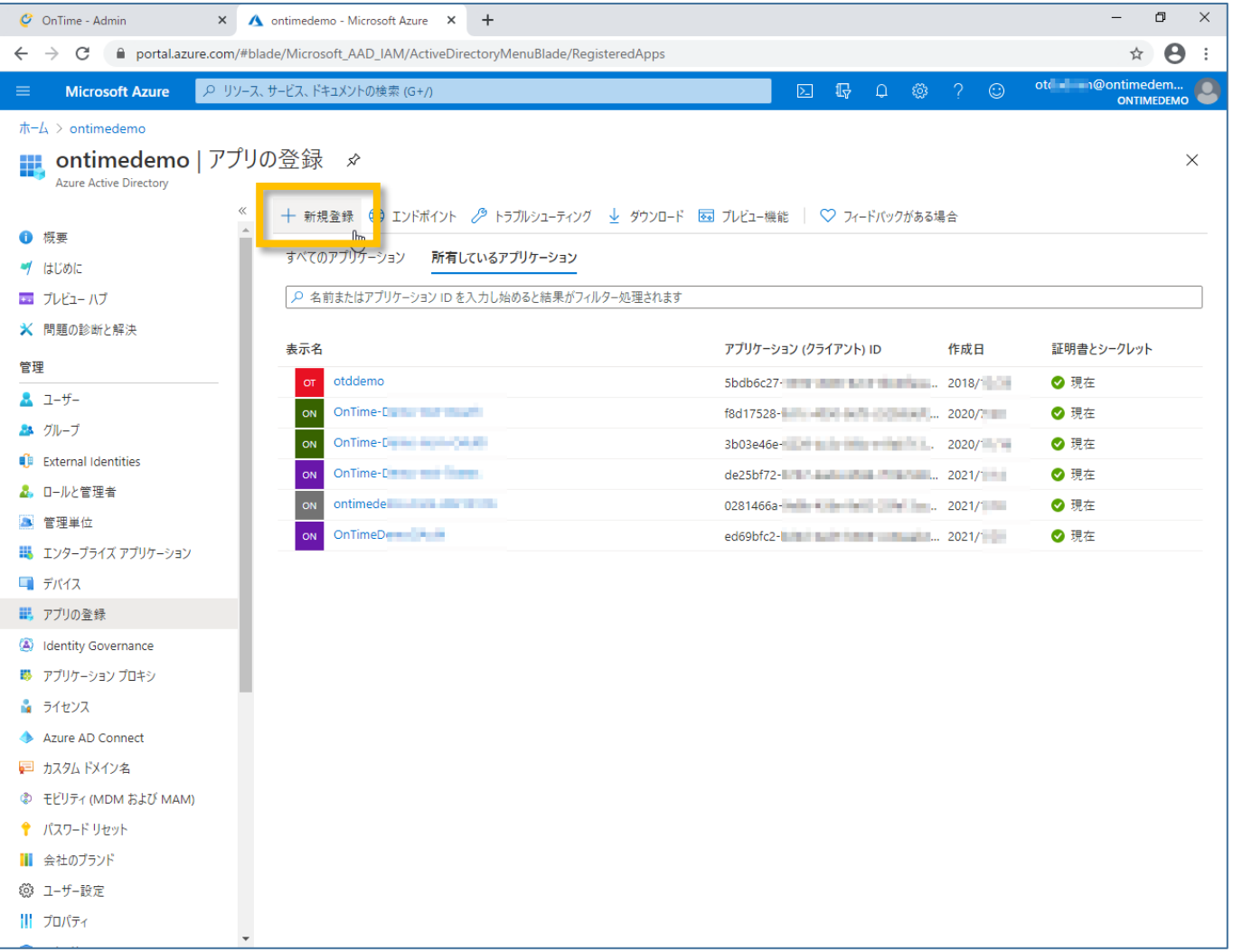
アプリの登録 2



- 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

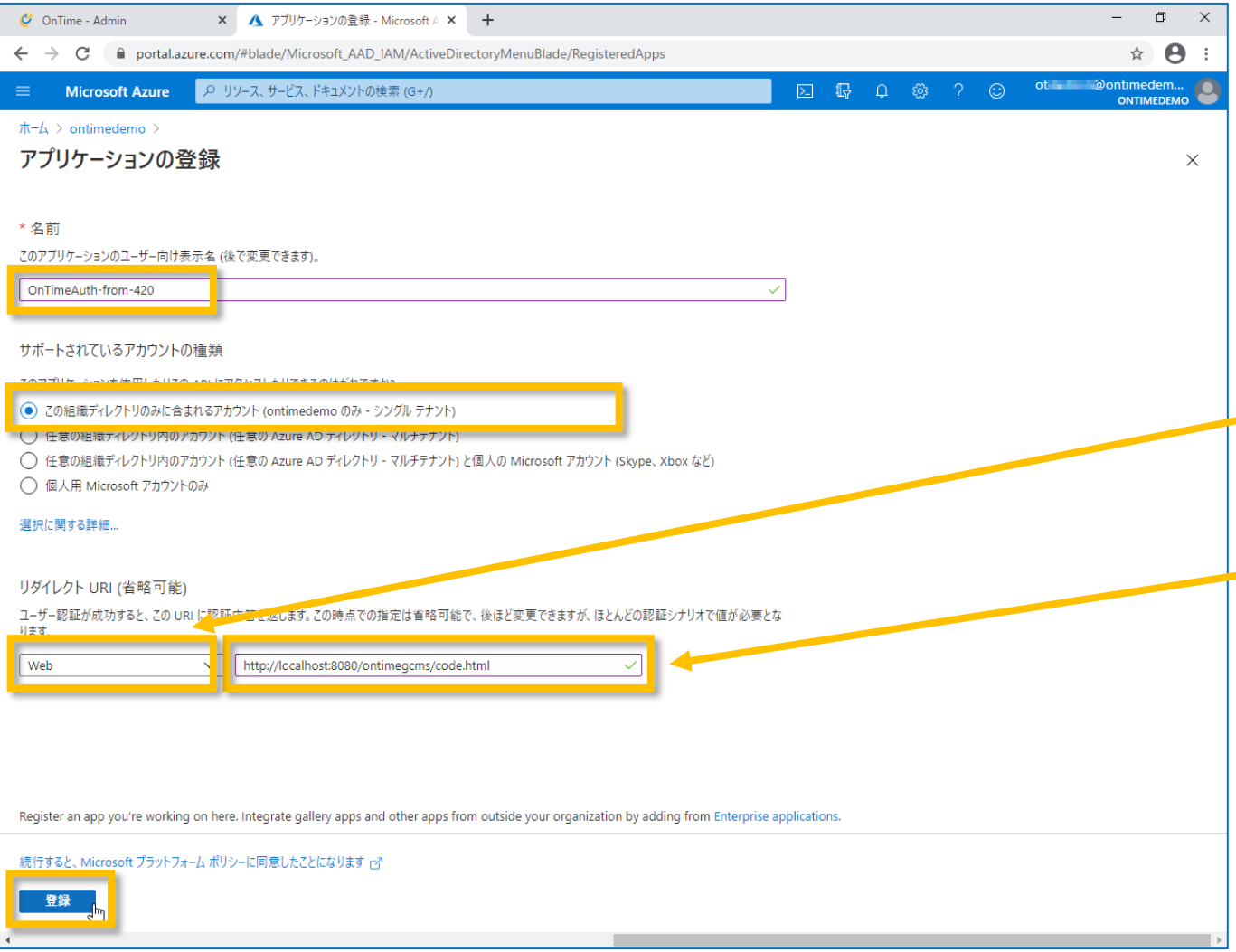


- 「アプリの登録」で「新規登録」をクリックします。

- 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



- 「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。

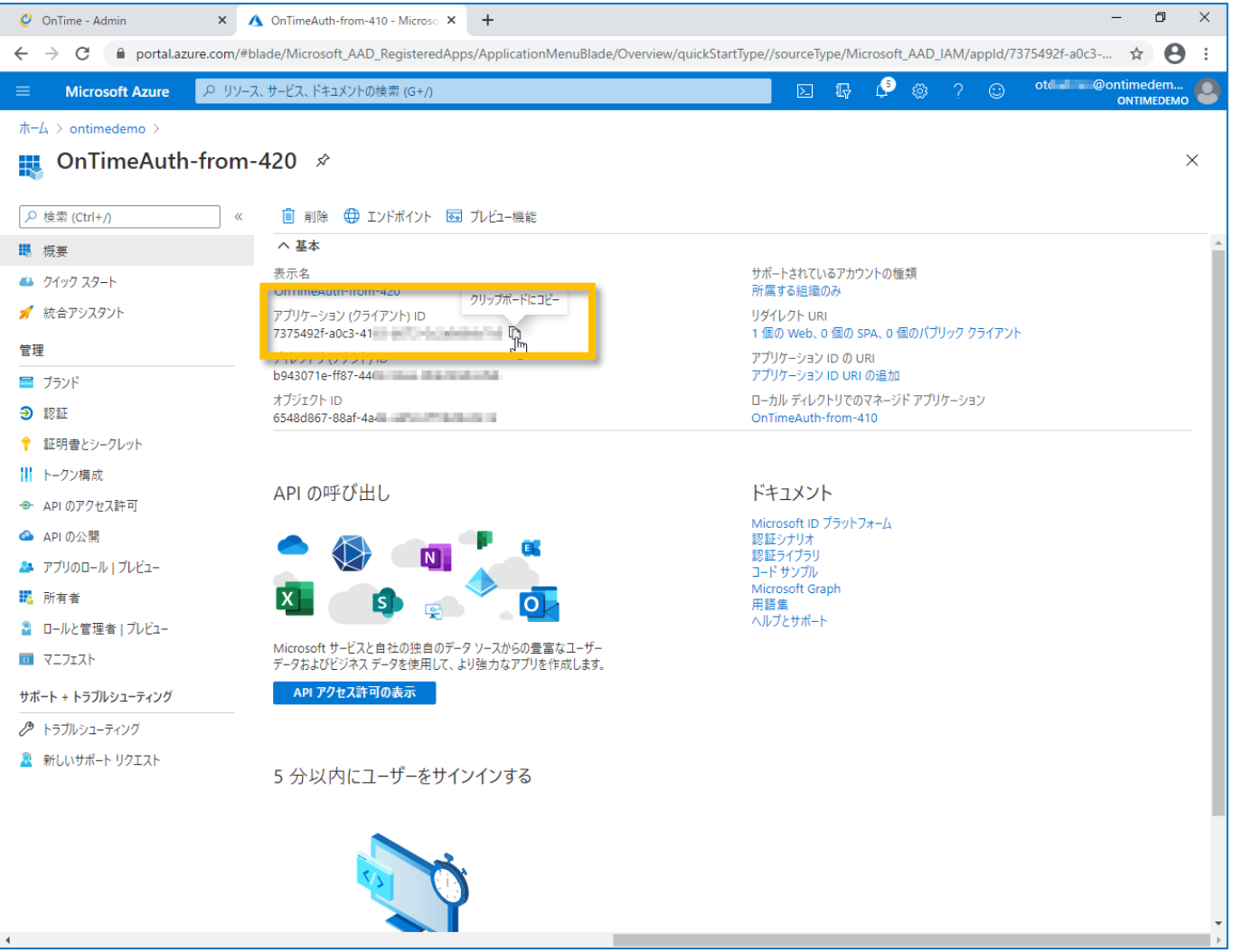
プラットフォームには「Web」を選択してください。

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。

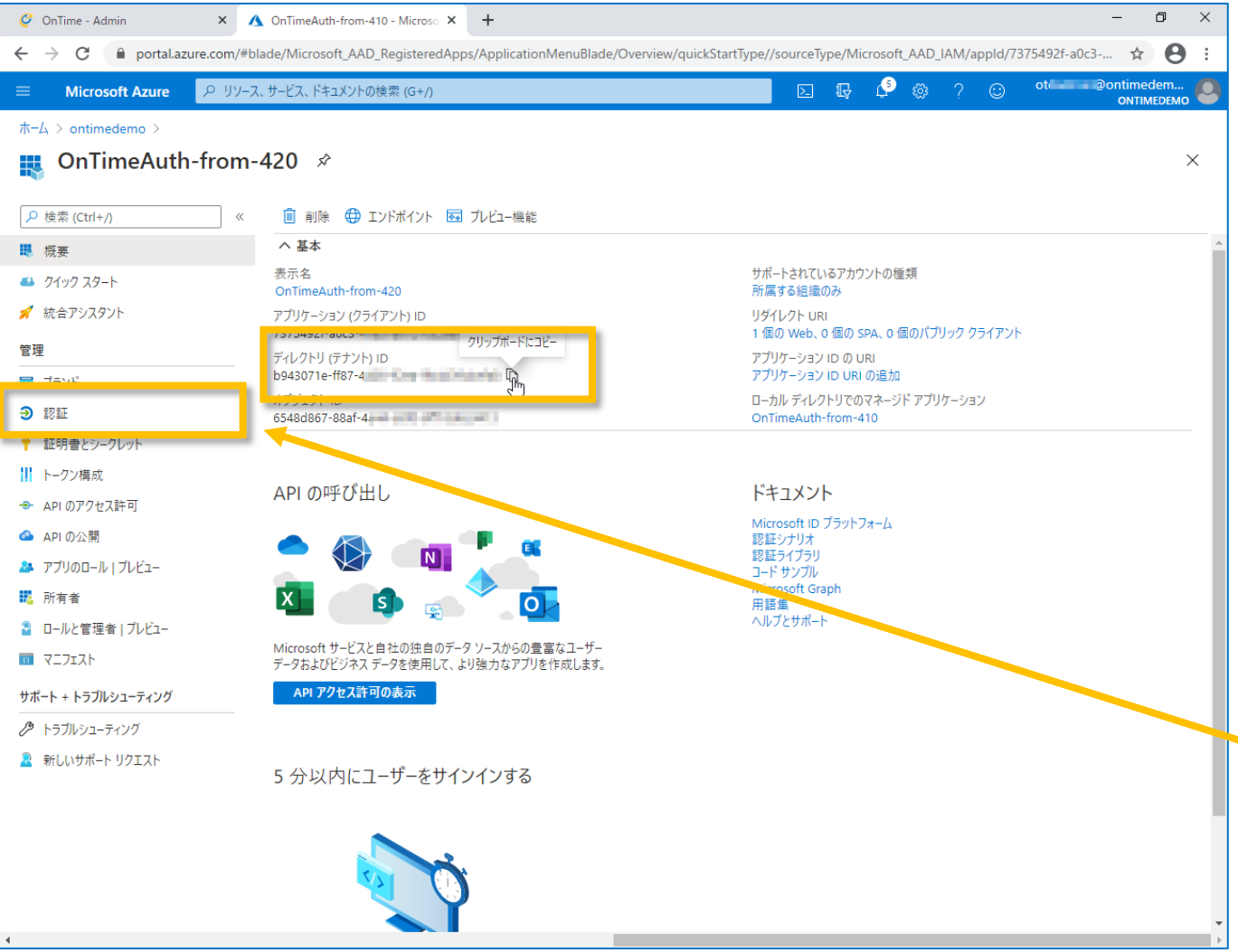
Azure Portal(AzureAD)での作業
各IDの取得/認証の設定

アプリの各IDの取得 1



- 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。

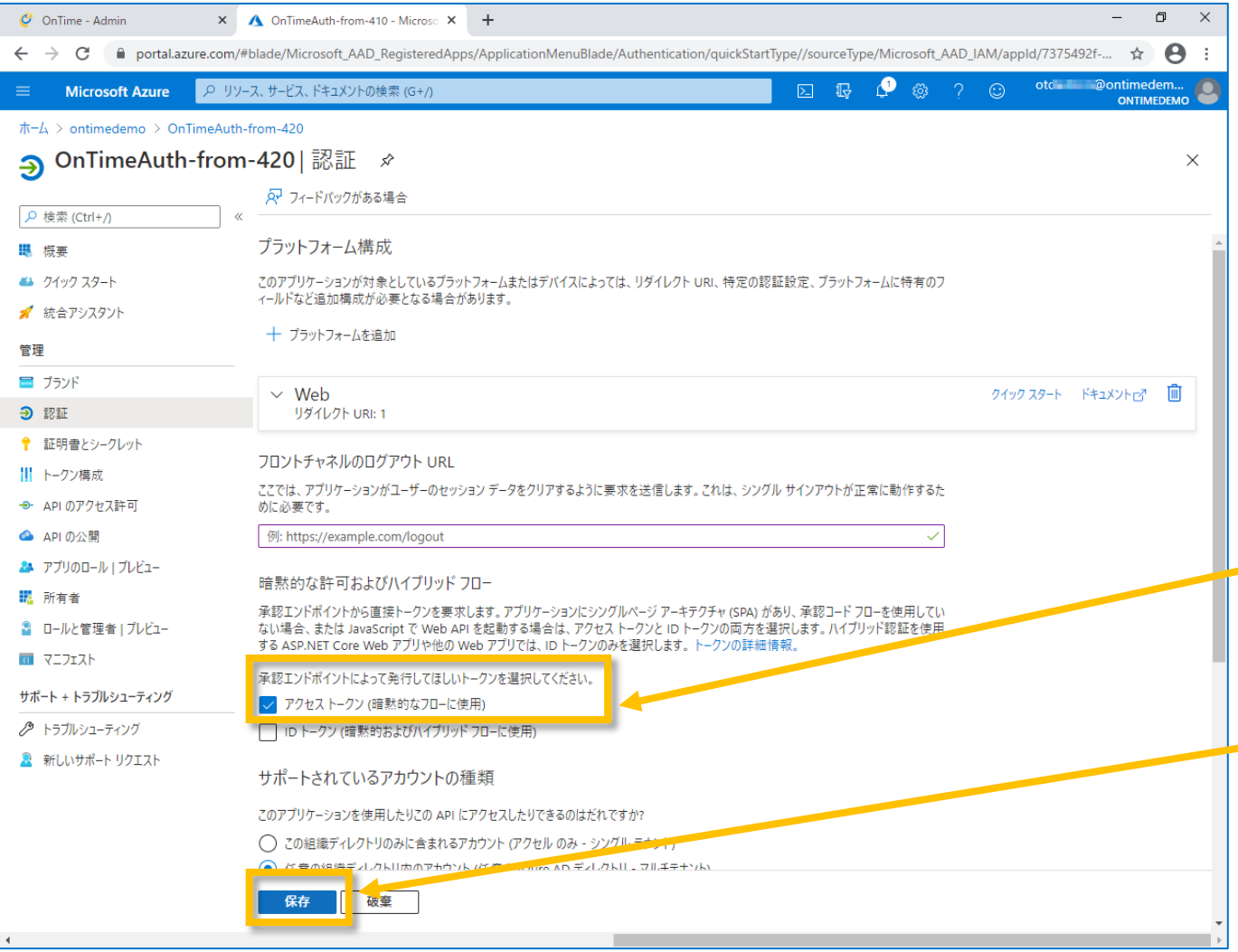
アプリの各IDの取得 2



- 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



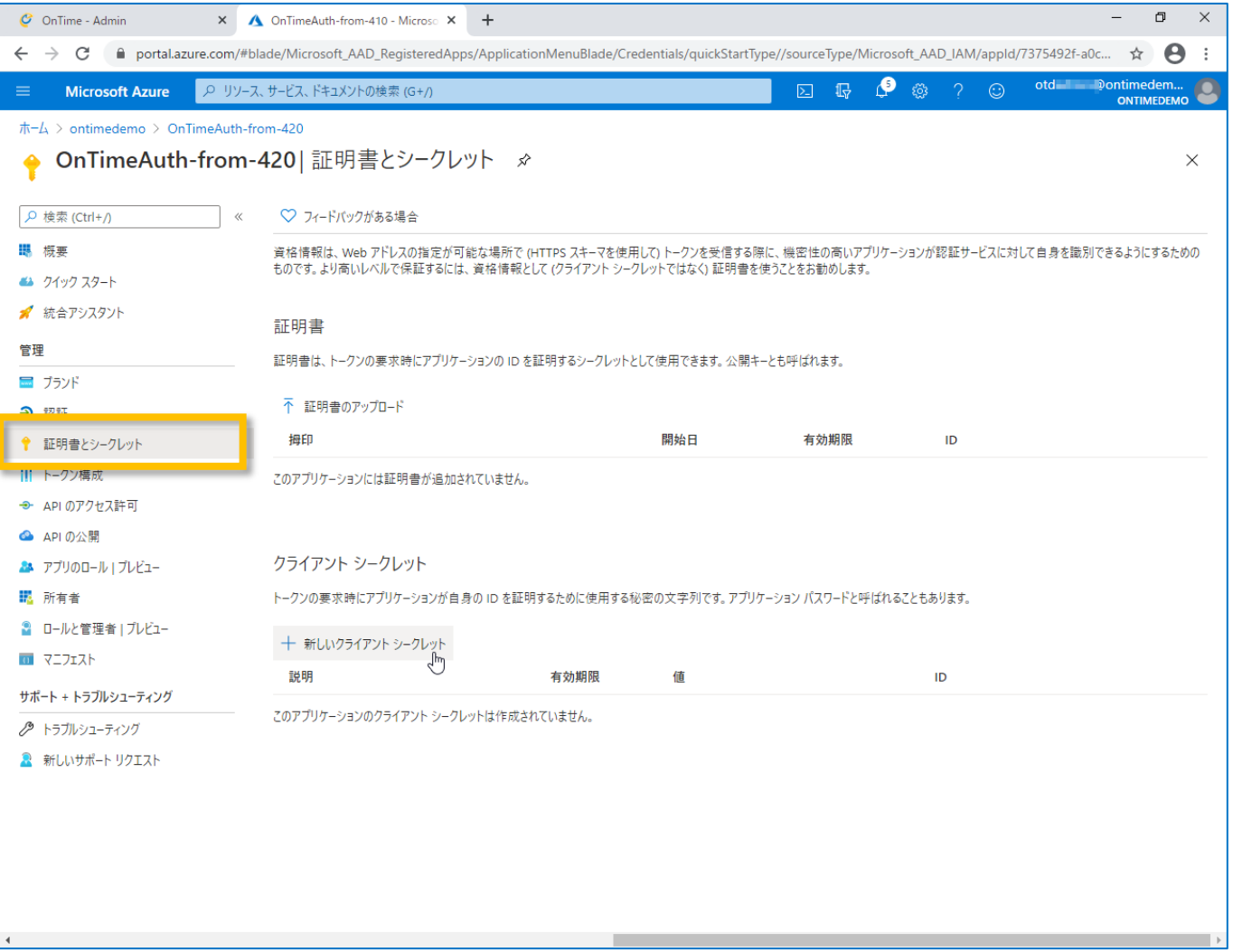
- 発行するトークンを選択します。

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。

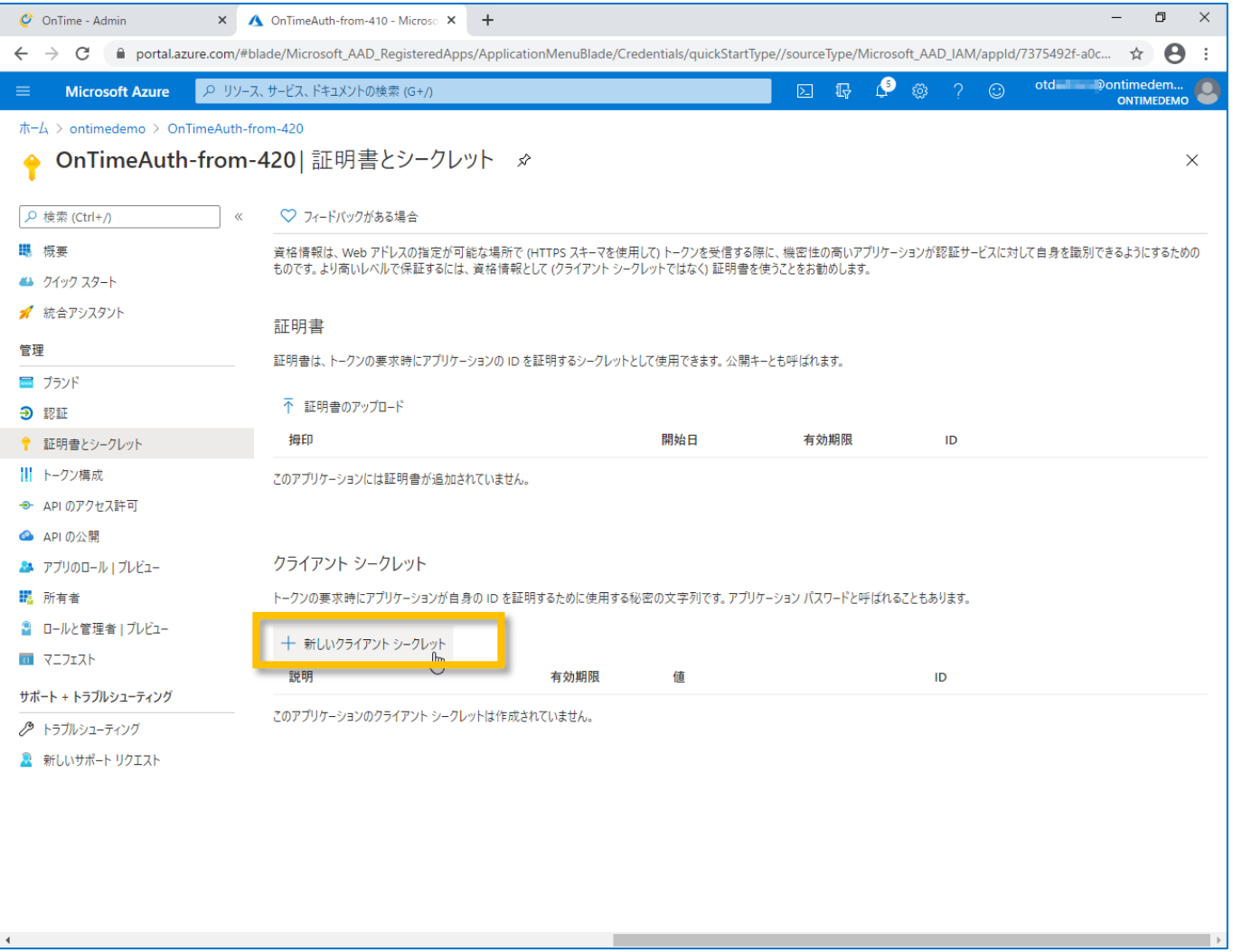
Azure Portal(AzureAD)での作業
クライアントシークレットの設定

クライアントシークレットの設定 1



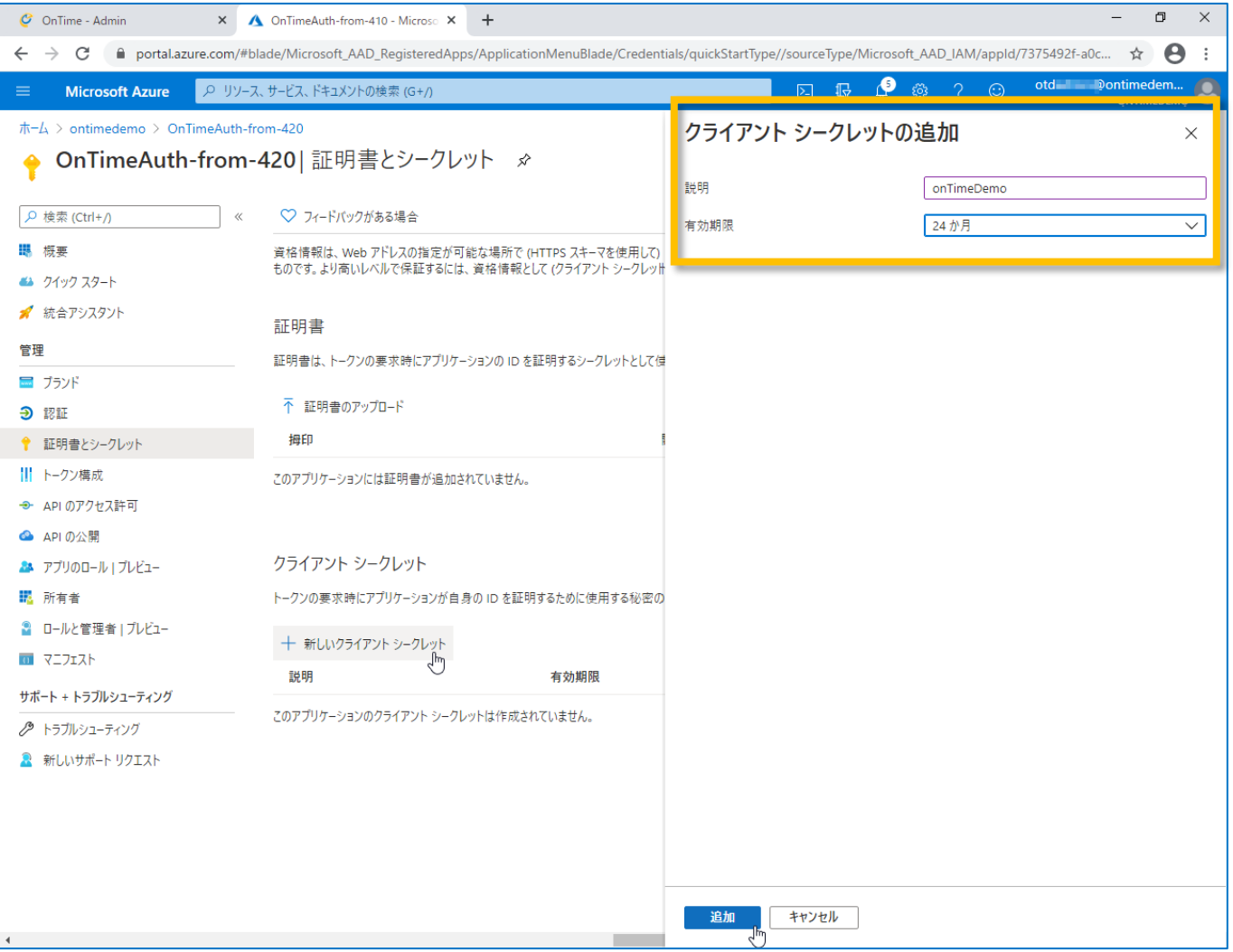
- 「証明書とシークレット」タブに移動します。

クライアントシークレットの設定 2



- こちらでは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。

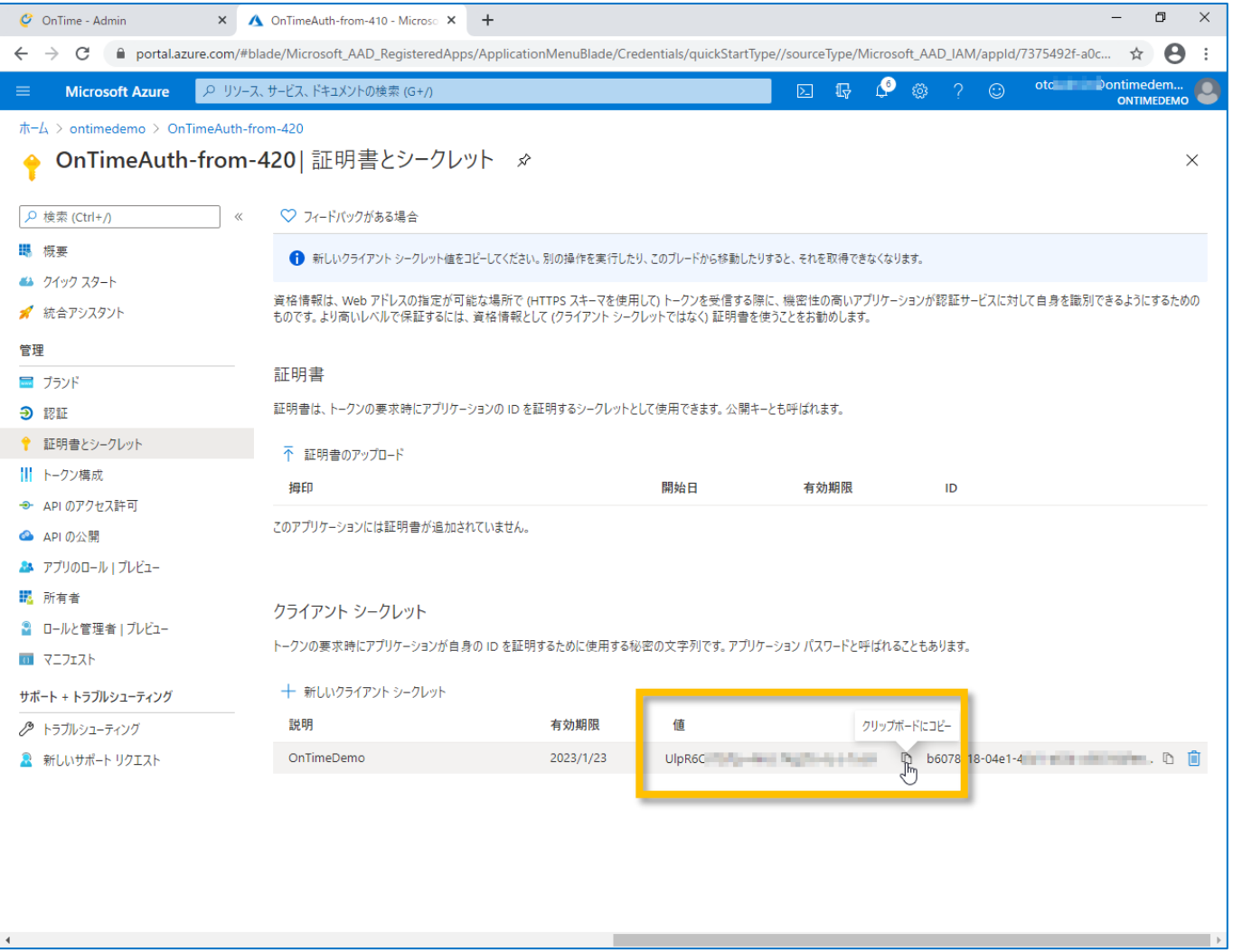
クライアントシークレットの設定 3



- 「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は期限付きの為、自組織の設定に合わせ更新ください

クライアントシークレットの設定 4

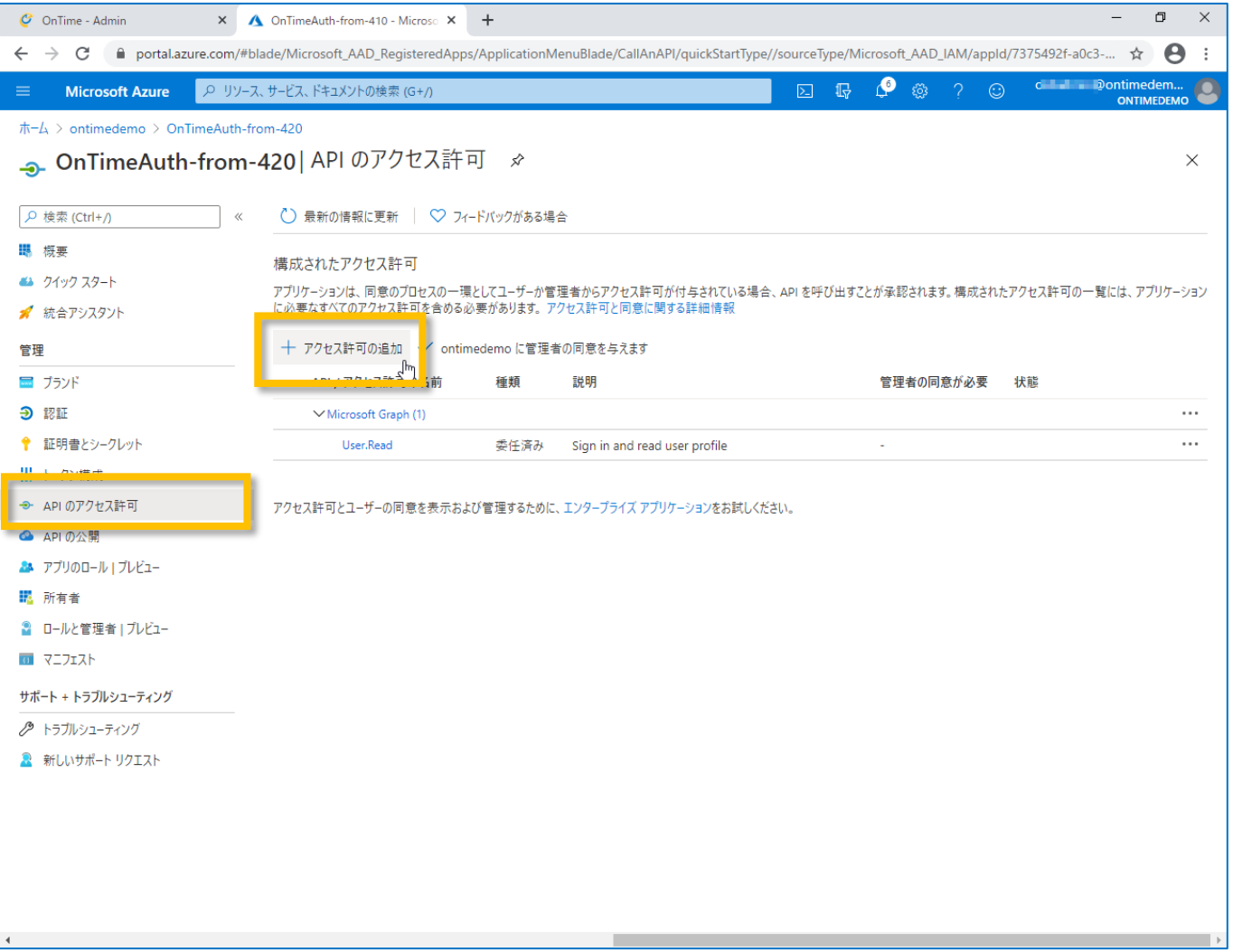


- 先ほどの画面上には作成した「クライアントシークレット」が表示されています。
- 「値」をコピーし、後ほどOnTime管理センターで利用するのでメモ帳などに保持します。

- 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。

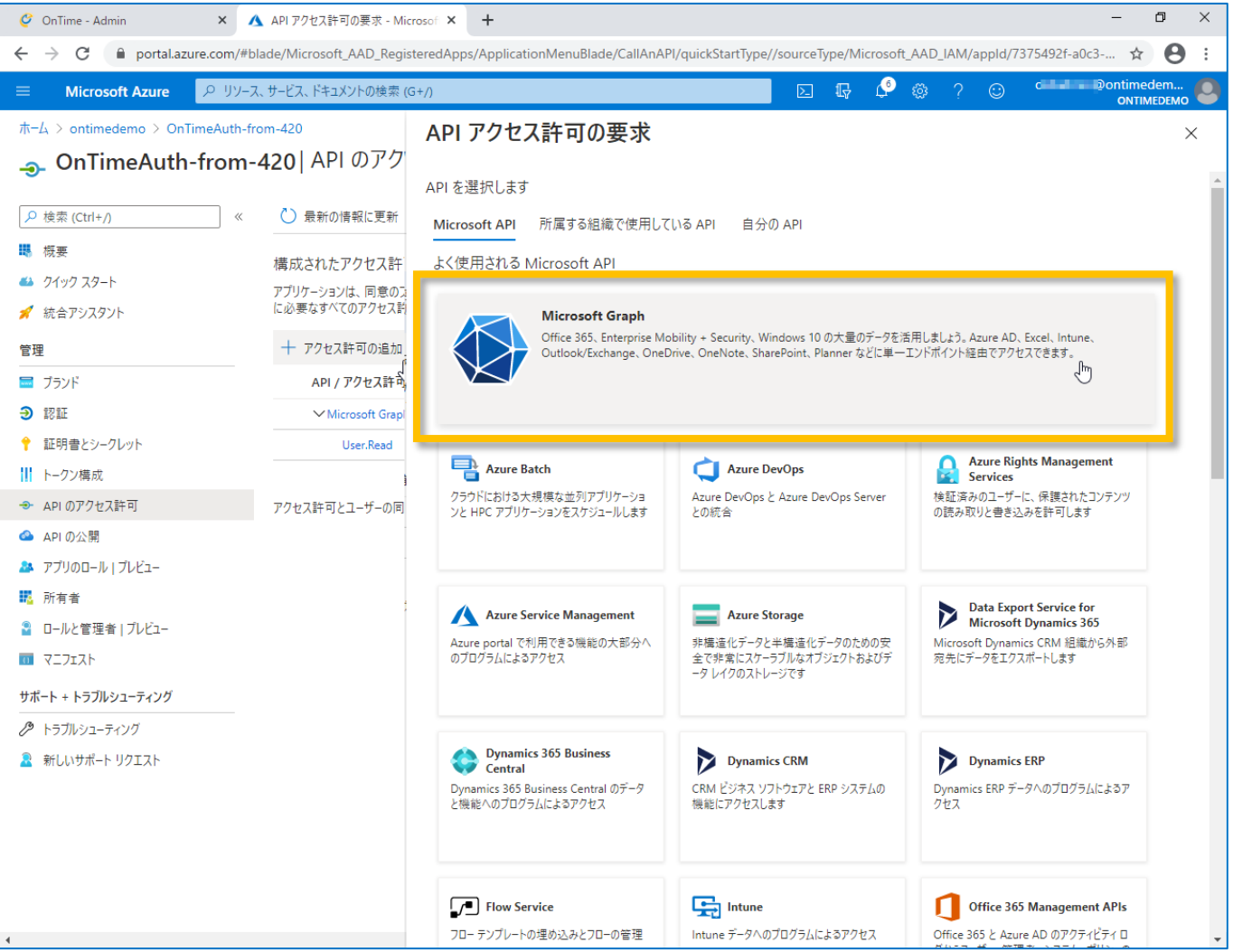
Azure Portal(AzureAD)での作業
APIのアクセス許可

APIのアクセス許可 1



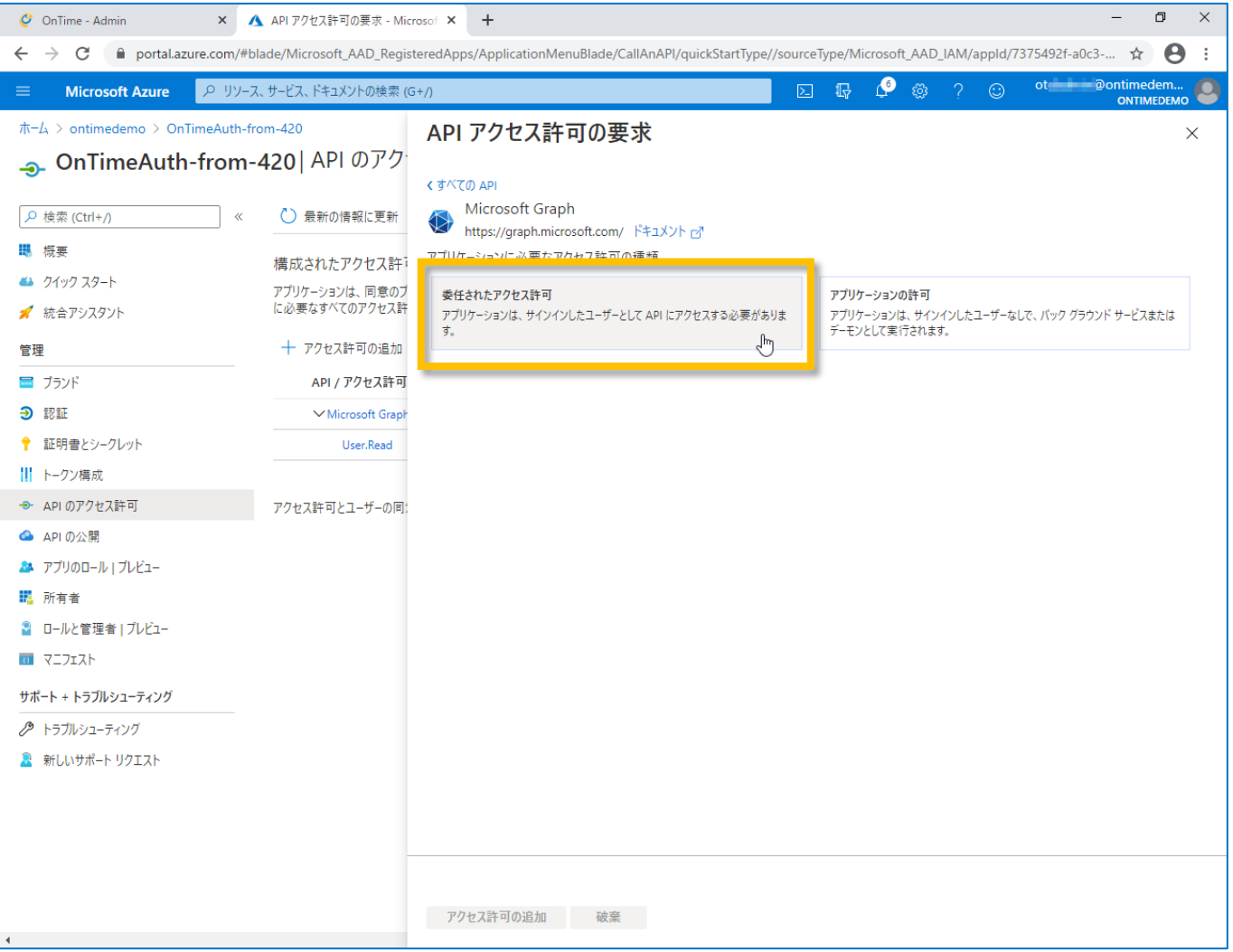
- 「APIのアクセス許可」タブに移動します。
- こちらではOnTimeサーバーが Graph API でアクセスする内容を定義します。
- 「アクセス許可の追加」ボタンをクリックします。

APIのアクセス許可 2



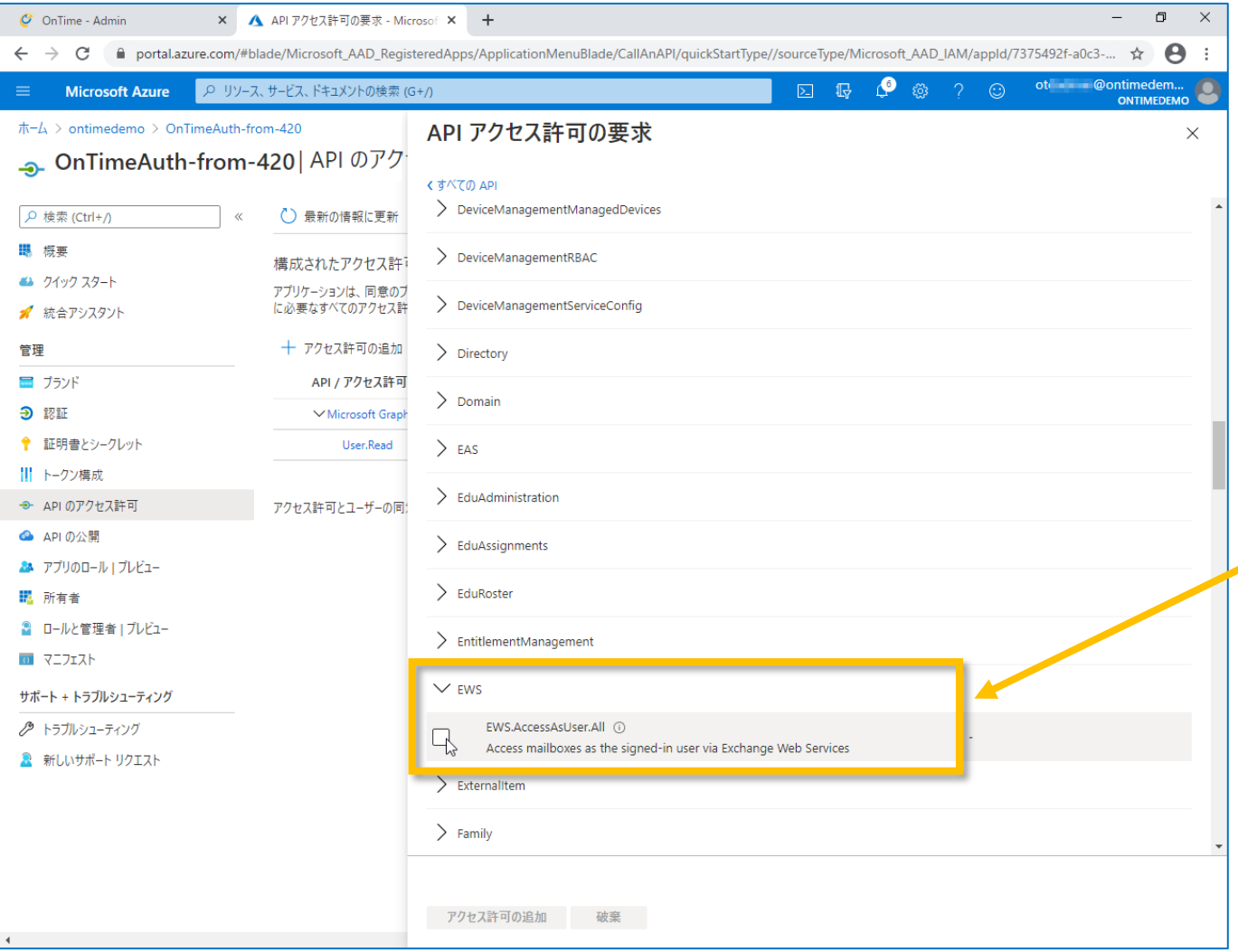
- 「APIアクセス許可の要求」ページが開きます。
- 「Microsoft Graph」をクリックします。

APIのアクセス許可 3



- 「委任されたアクセス許可」をクリックします。

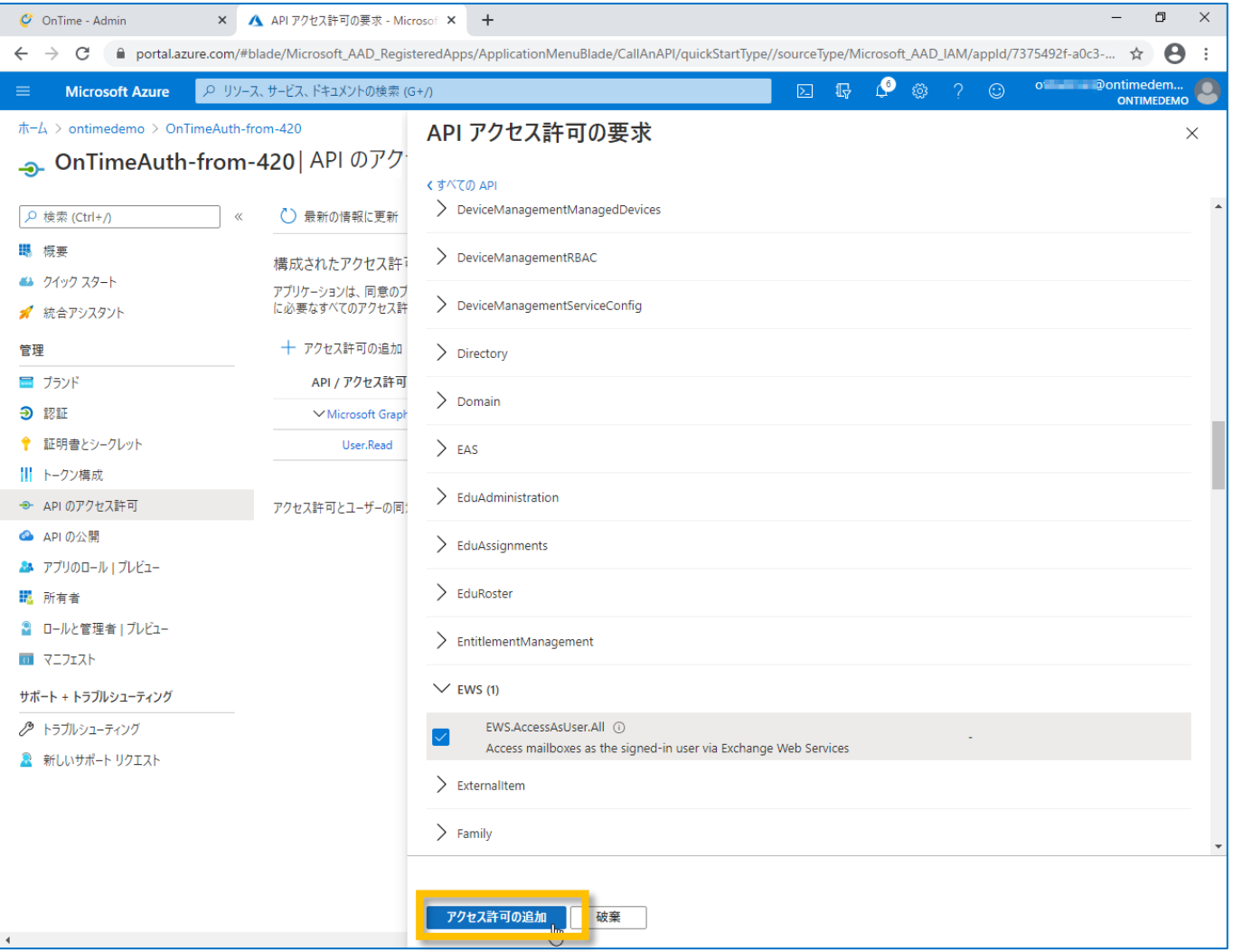
APIのアクセス許可 4



- 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。

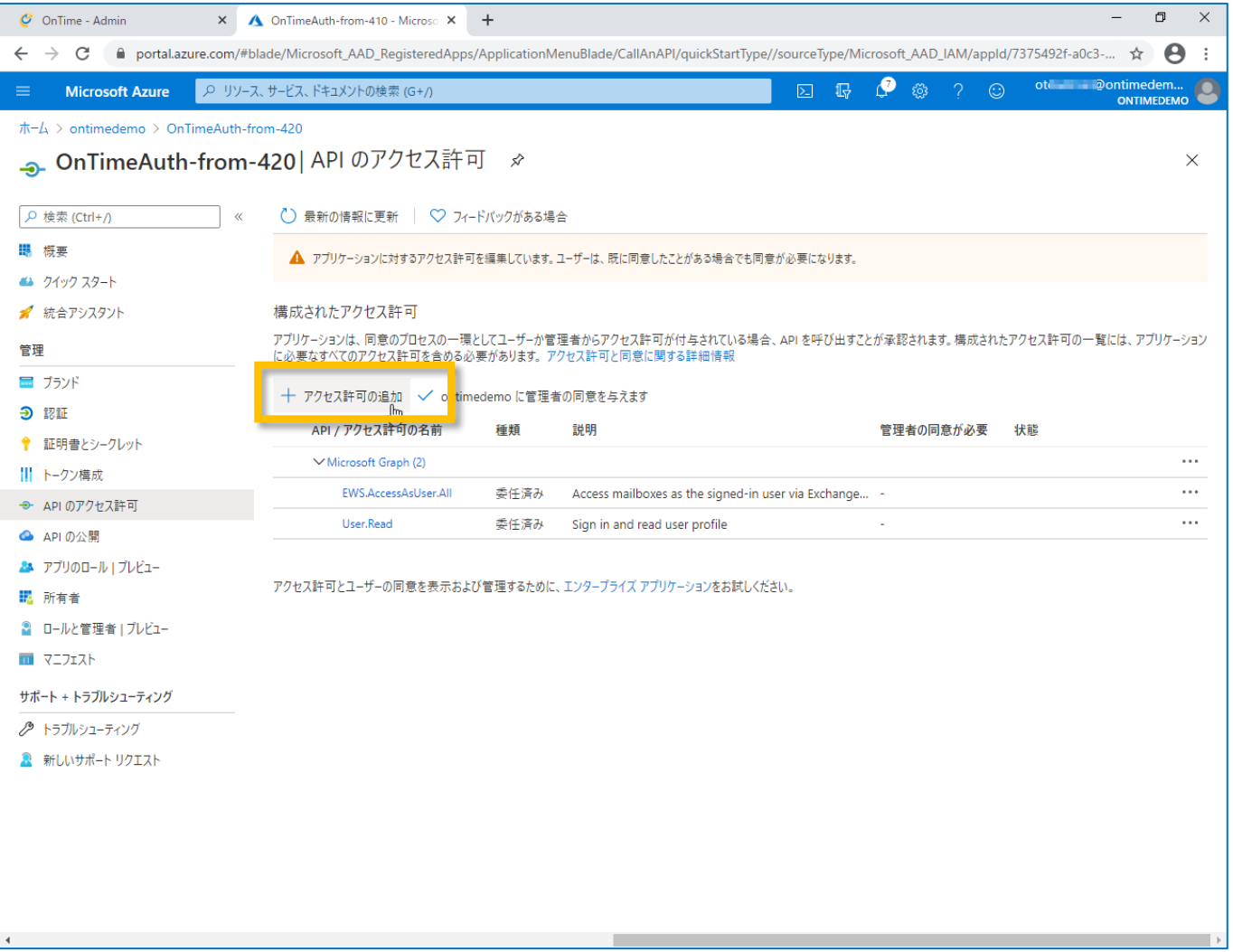
「EWS.AccessAsUser.All」をチェックします。

APIのアクセス許可 5



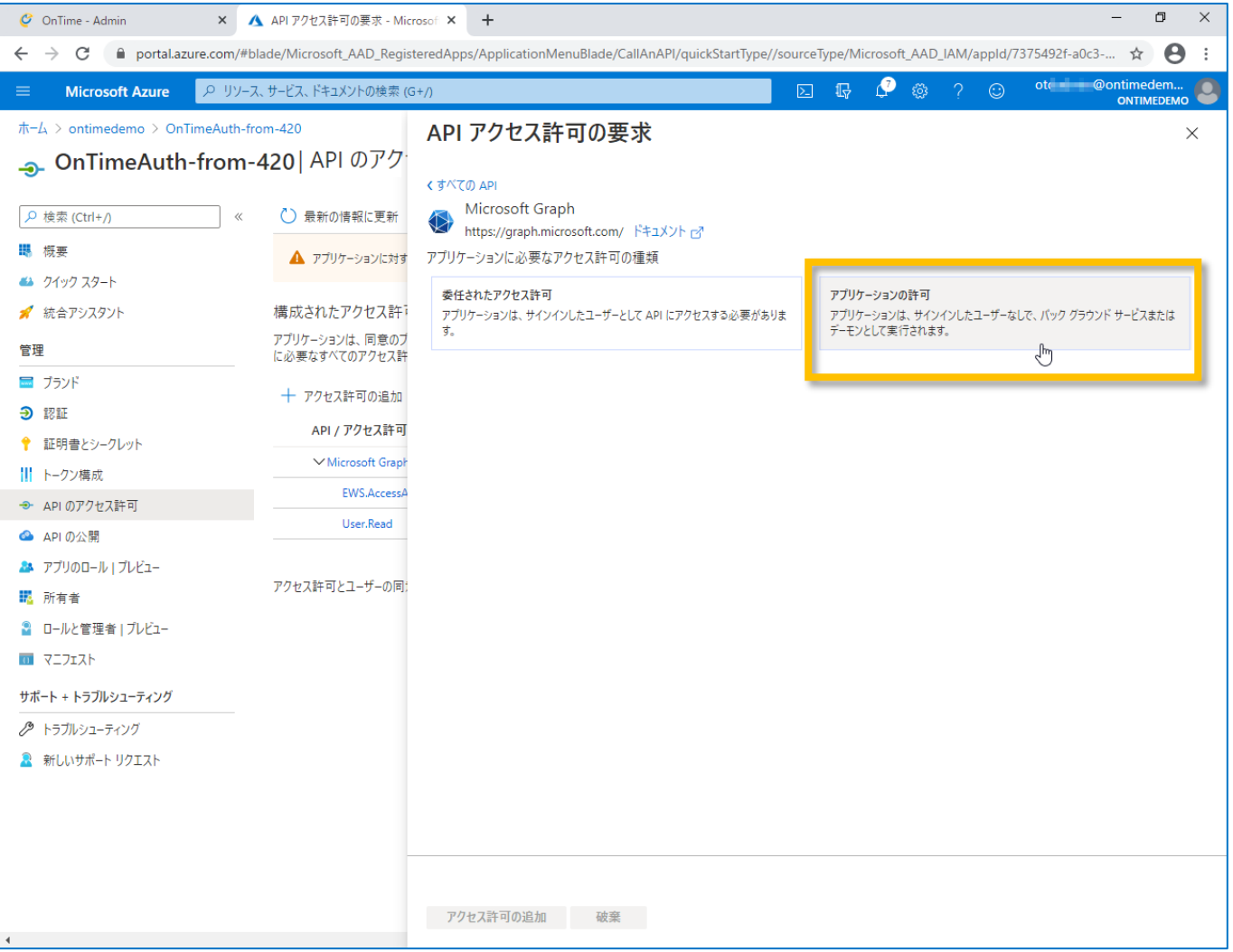
- 「アクセス許可の追加」をクリックします。

APIのアクセス許可 6



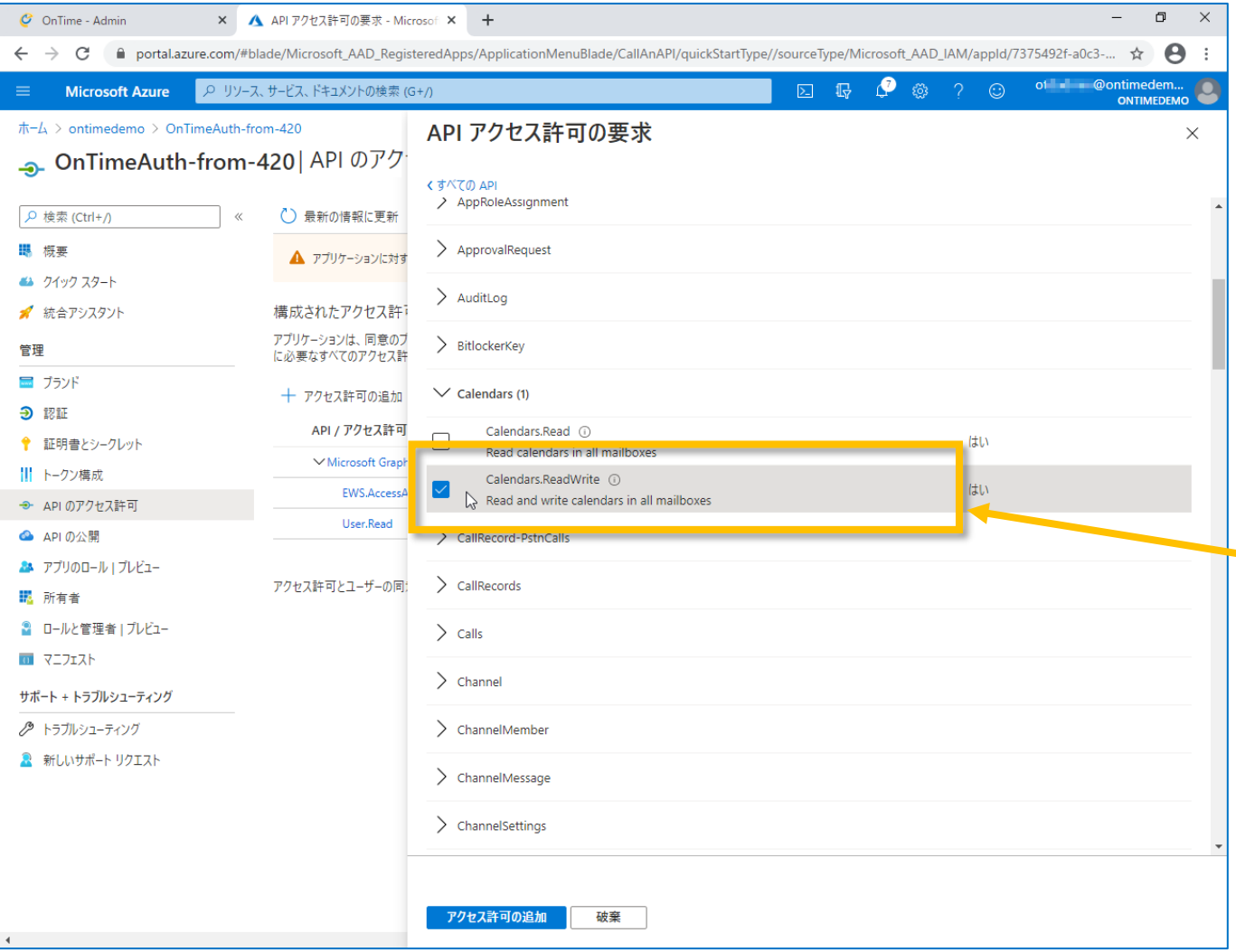
- 画面が戻ったら再度「アクセス許可の追加」ボタンをクリックします。

APIのアクセス許可 7



- 「Microsoft Graph」をクリックします。
- 「アプリケーションの許可」をクリックします。

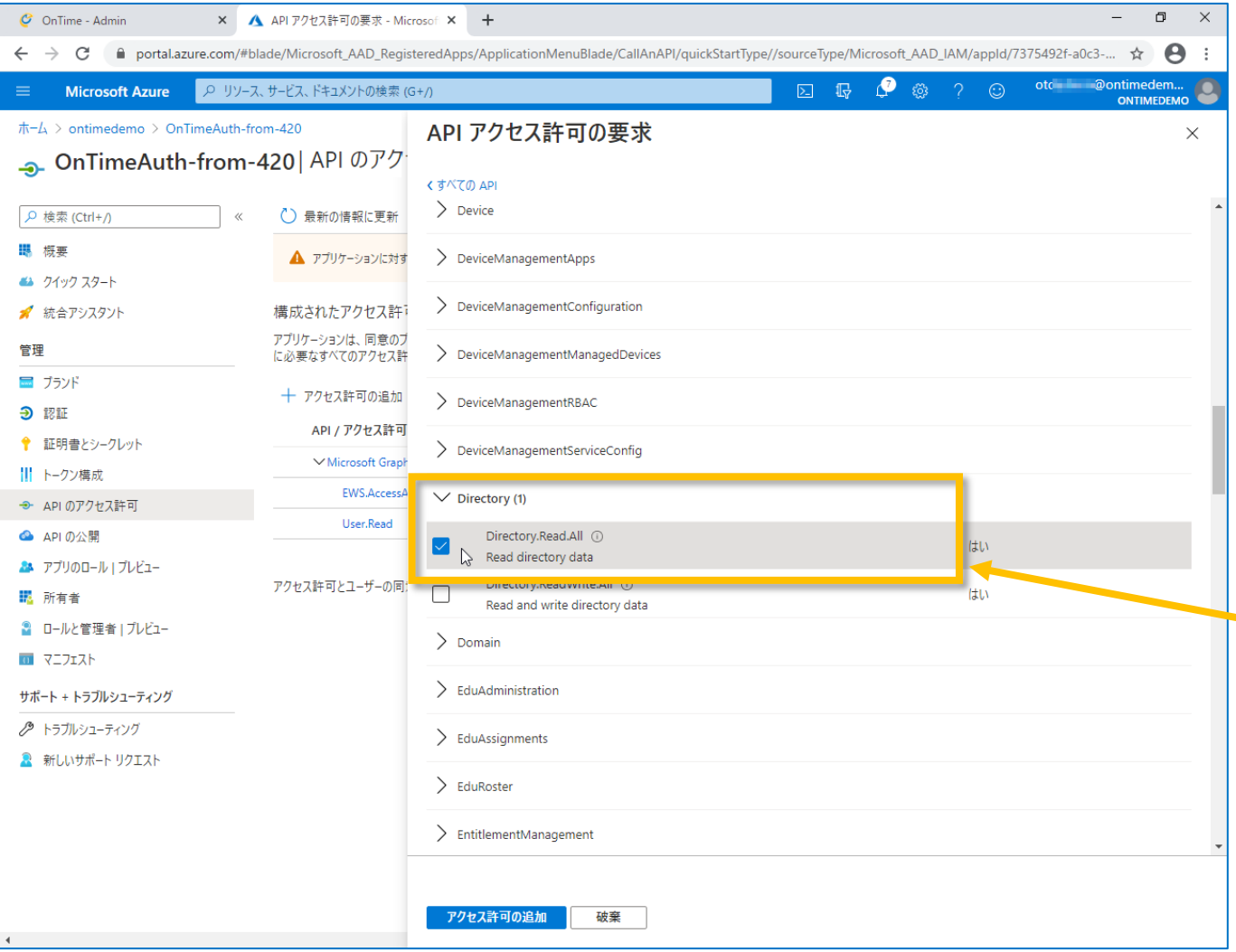
APIのアクセス許可 8



- 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。

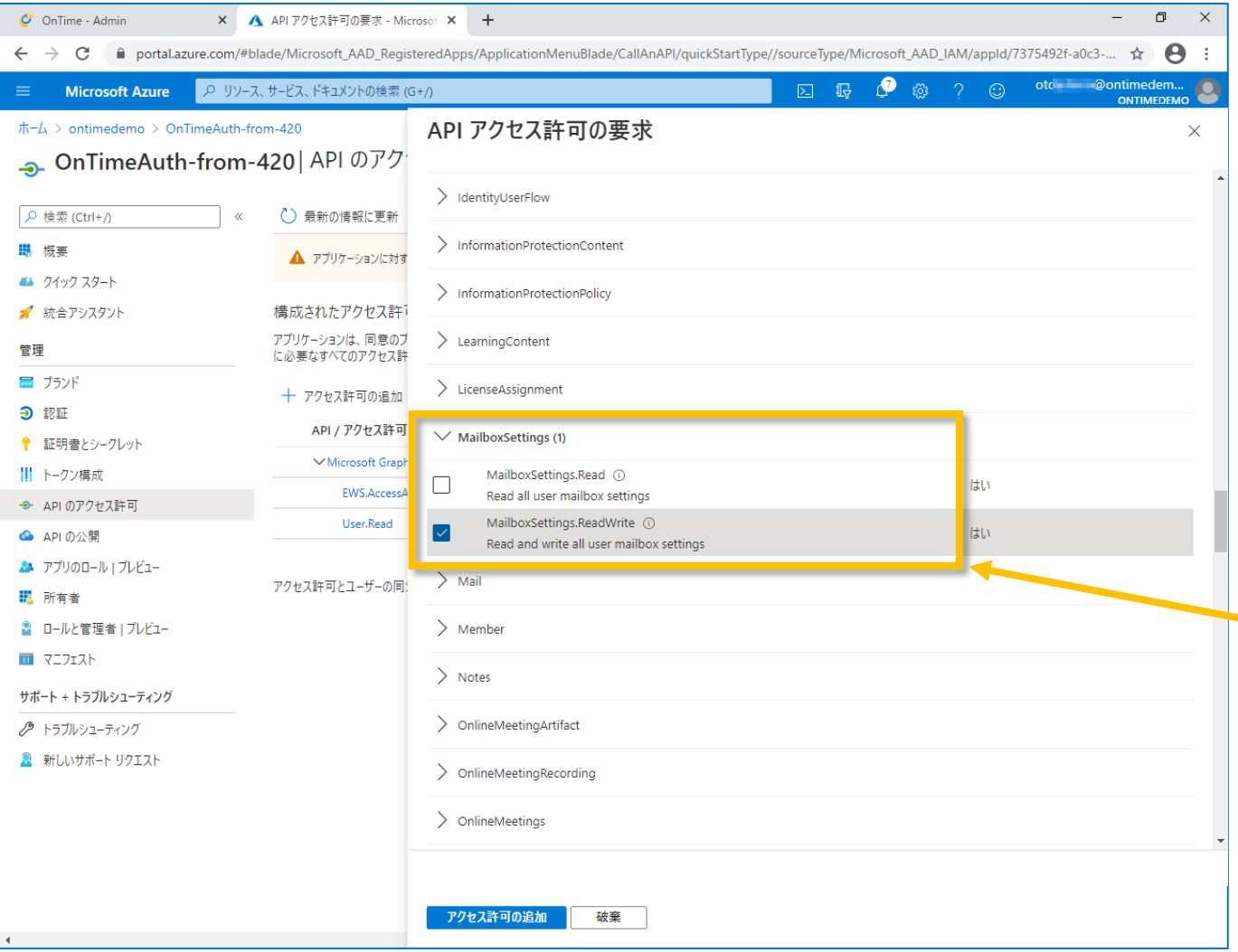
APIのアクセス許可 9



- 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。

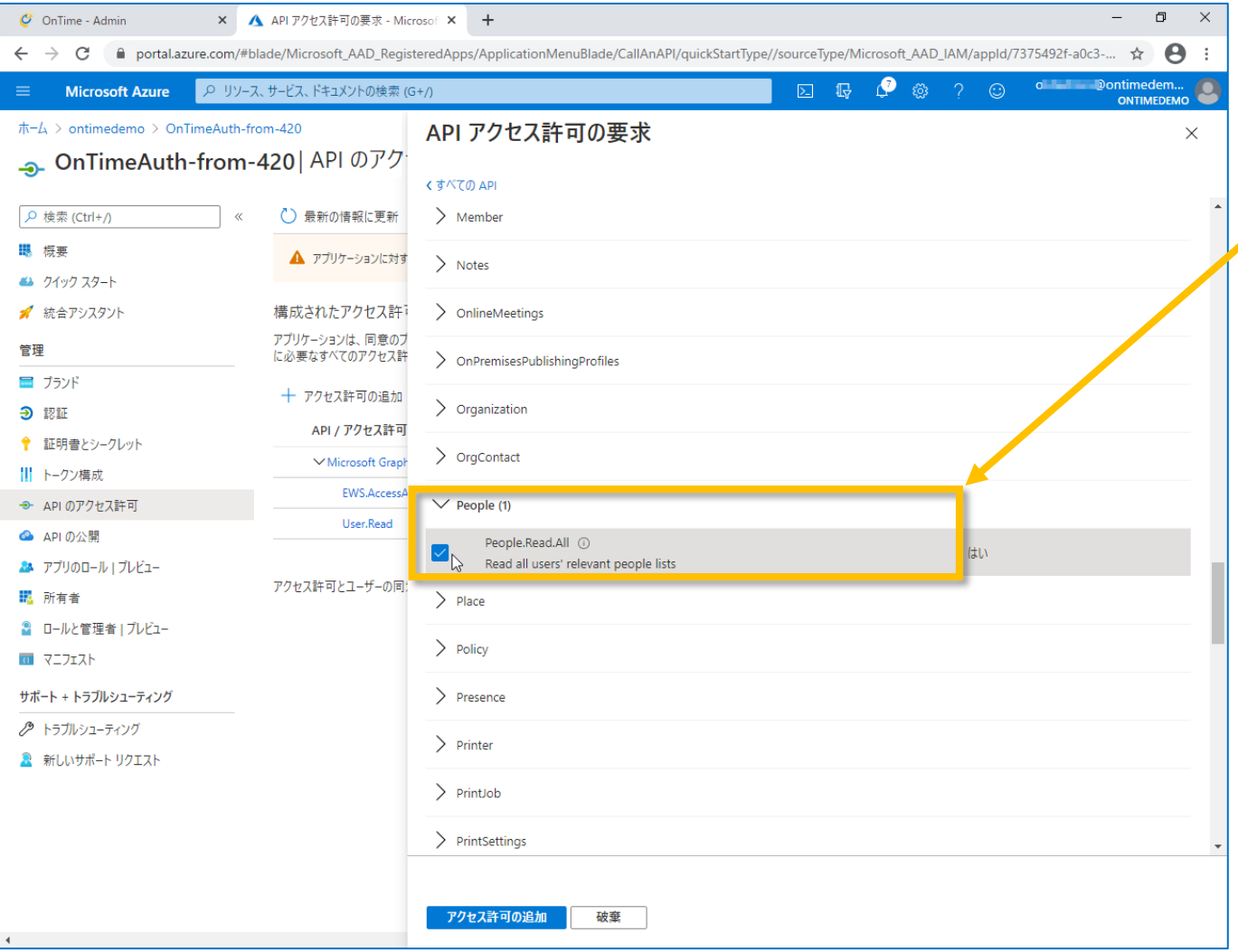
APIのアクセス許可１０



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

「MailboxSettings.ReadWrite」をチェックします。

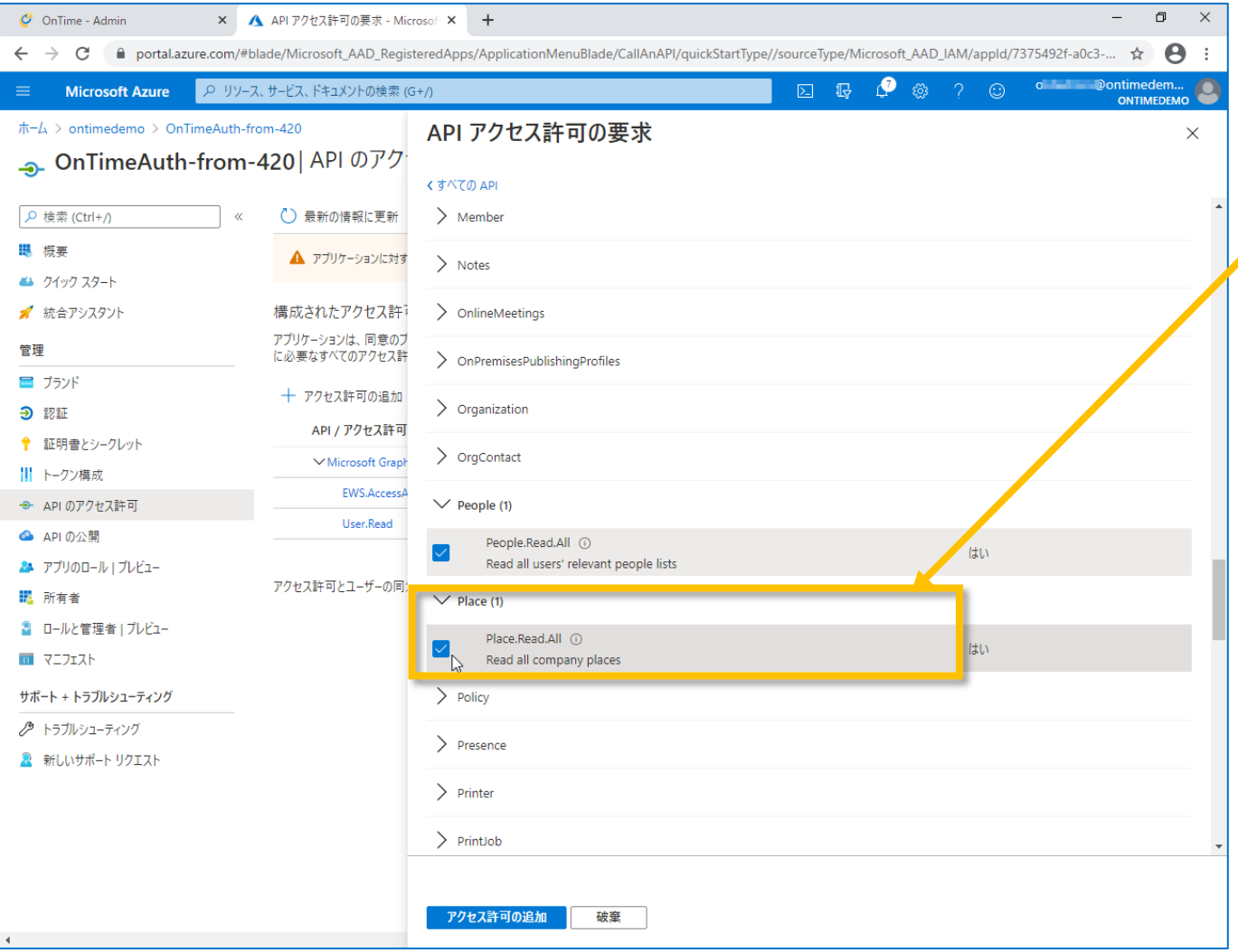
APIのアクセス許可１１



- 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。

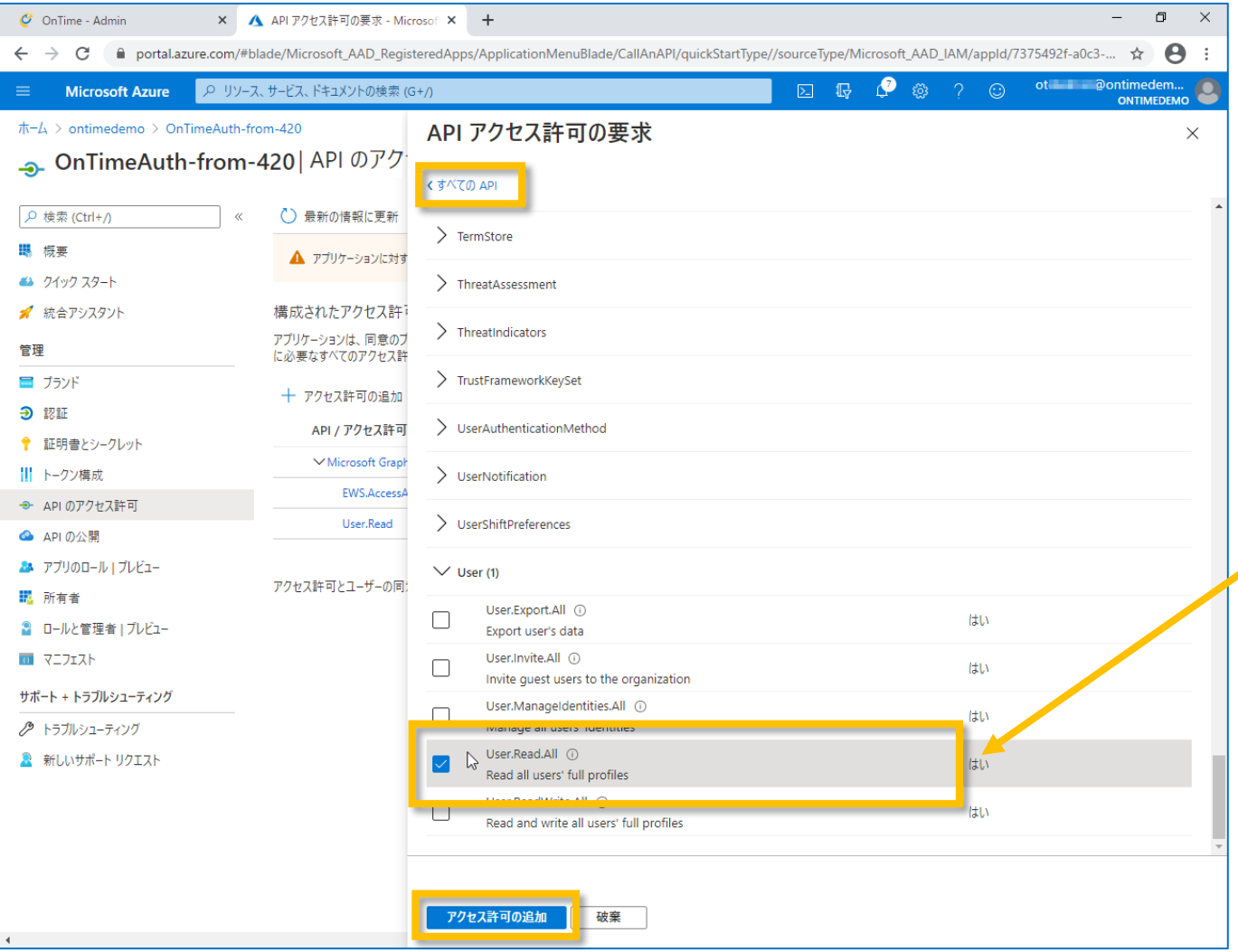
APIのアクセス許可１２



- 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１３

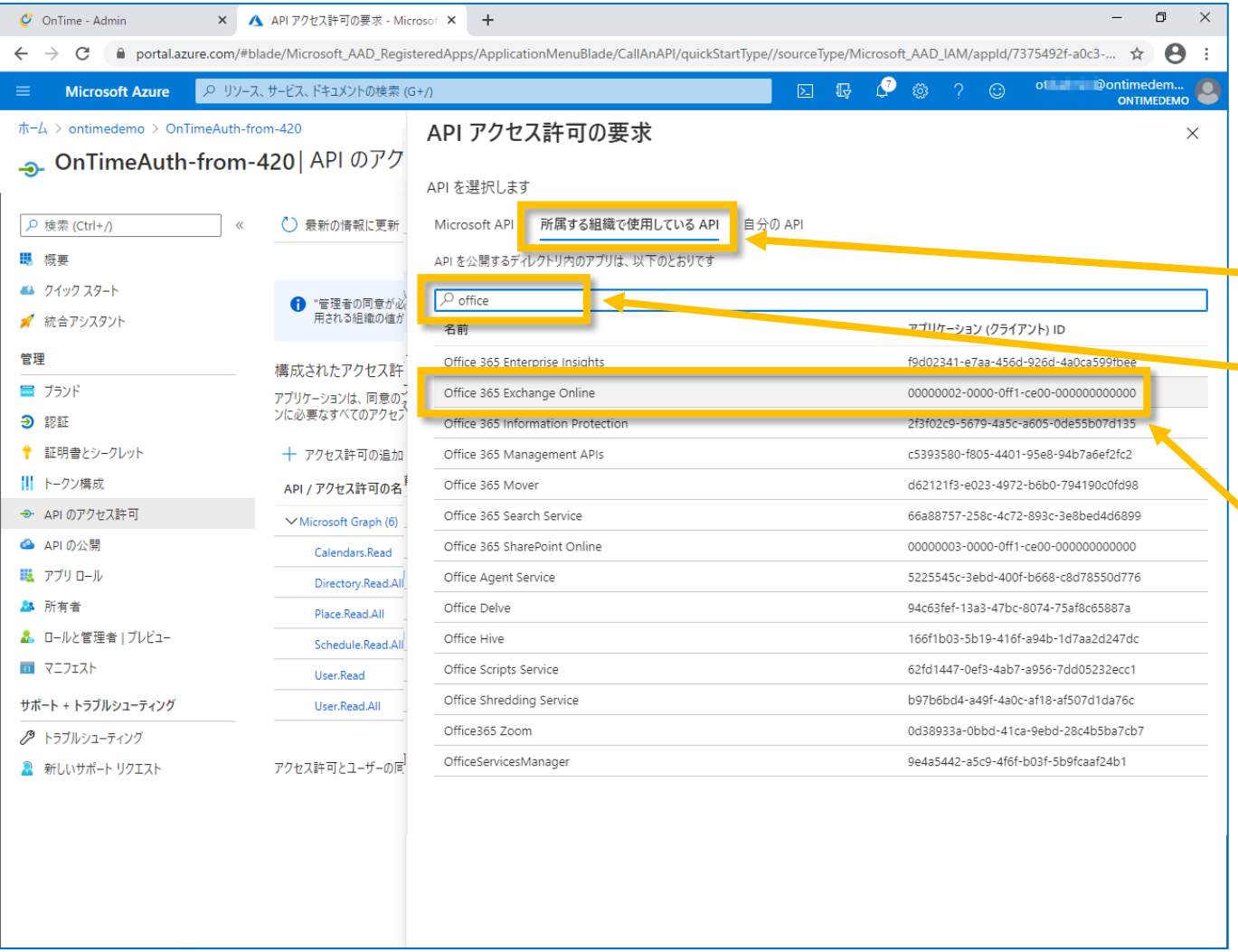


- 同様にスクロールして「User」まで移動します。移動したら「User」を更に展開します。

「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１４



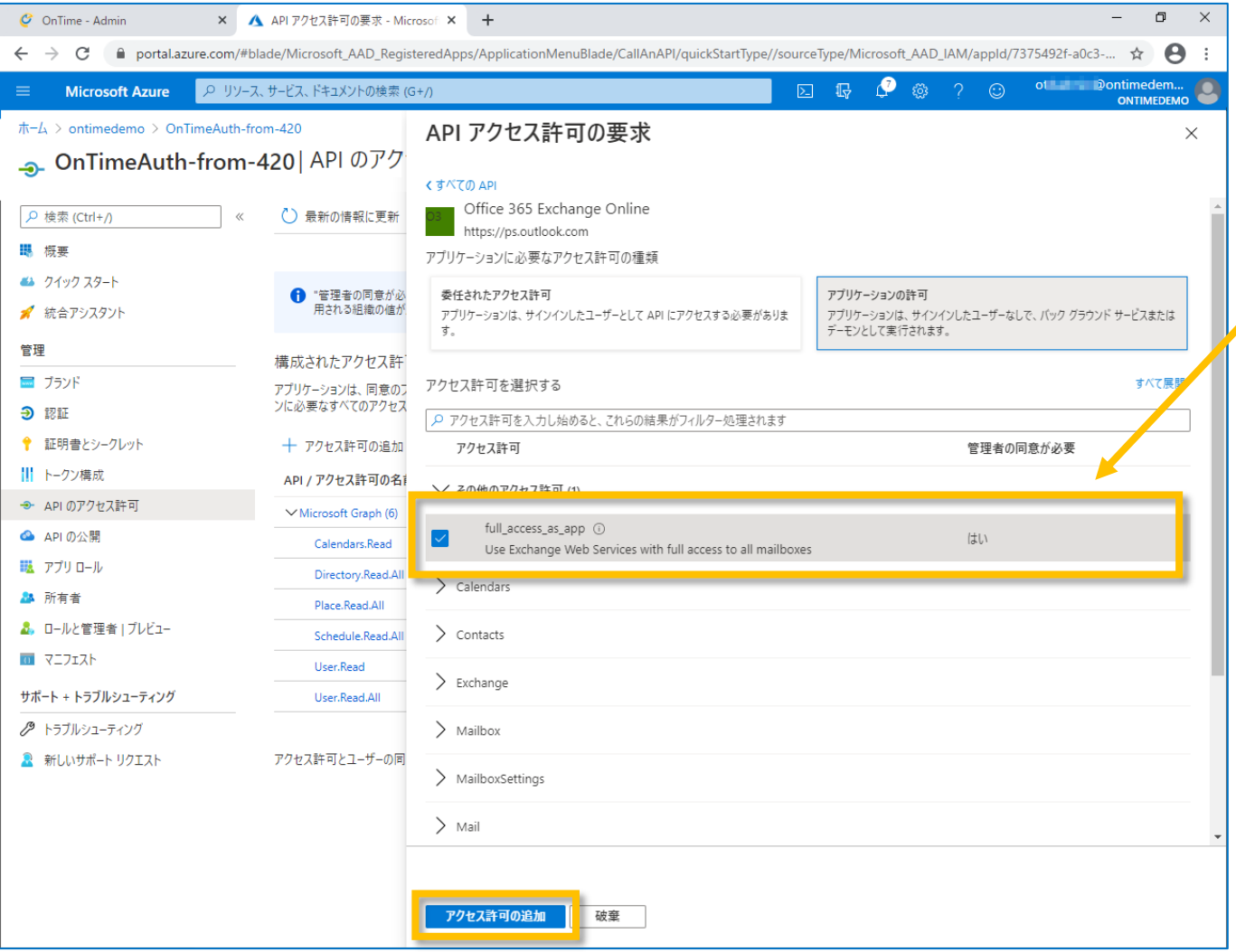
- 画面が戻ったら再度「アクセス許可の追加」ボタンをクリックします。

「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１５

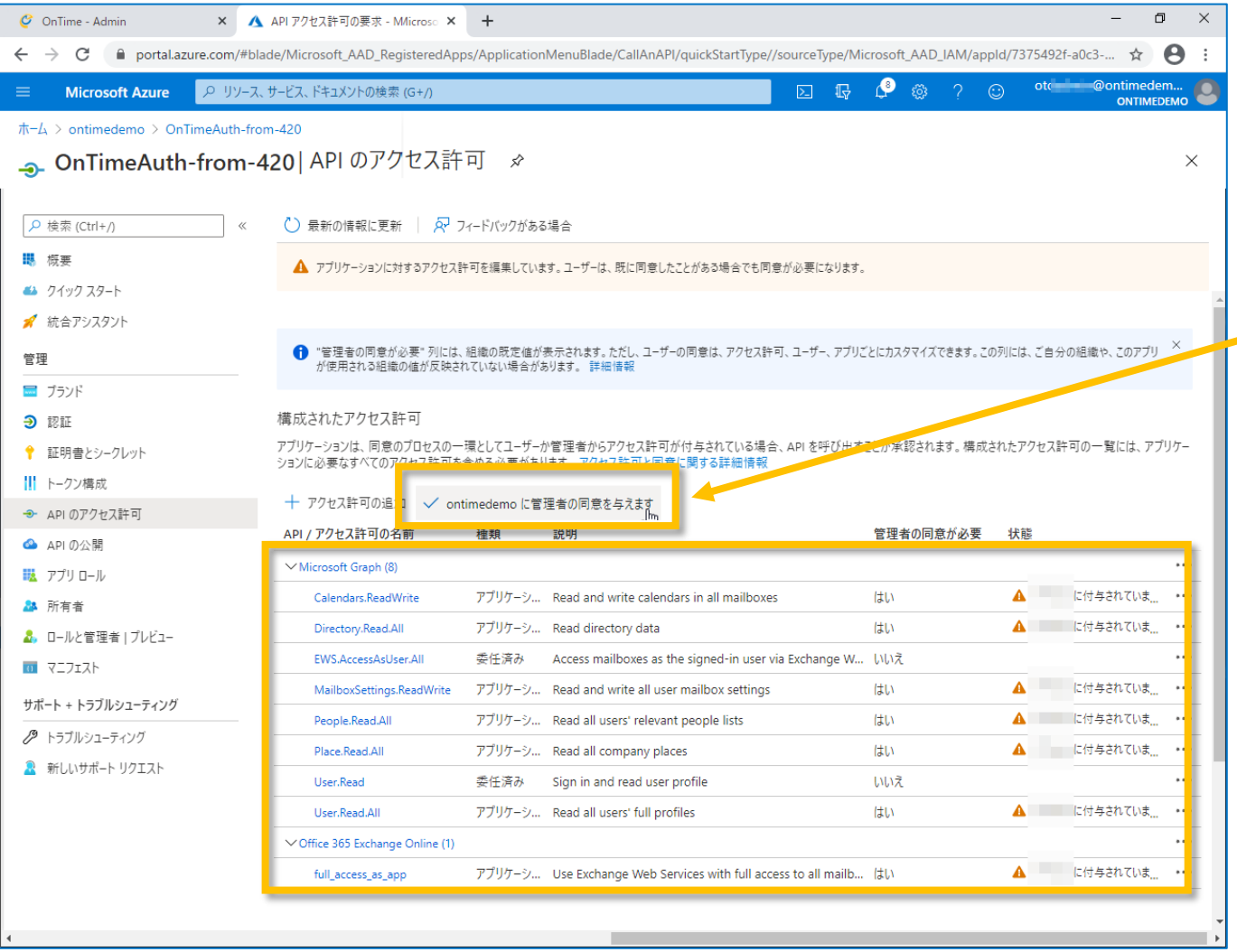


- 「アプリケーションの許可」をクリックします。

「full_access_as_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。

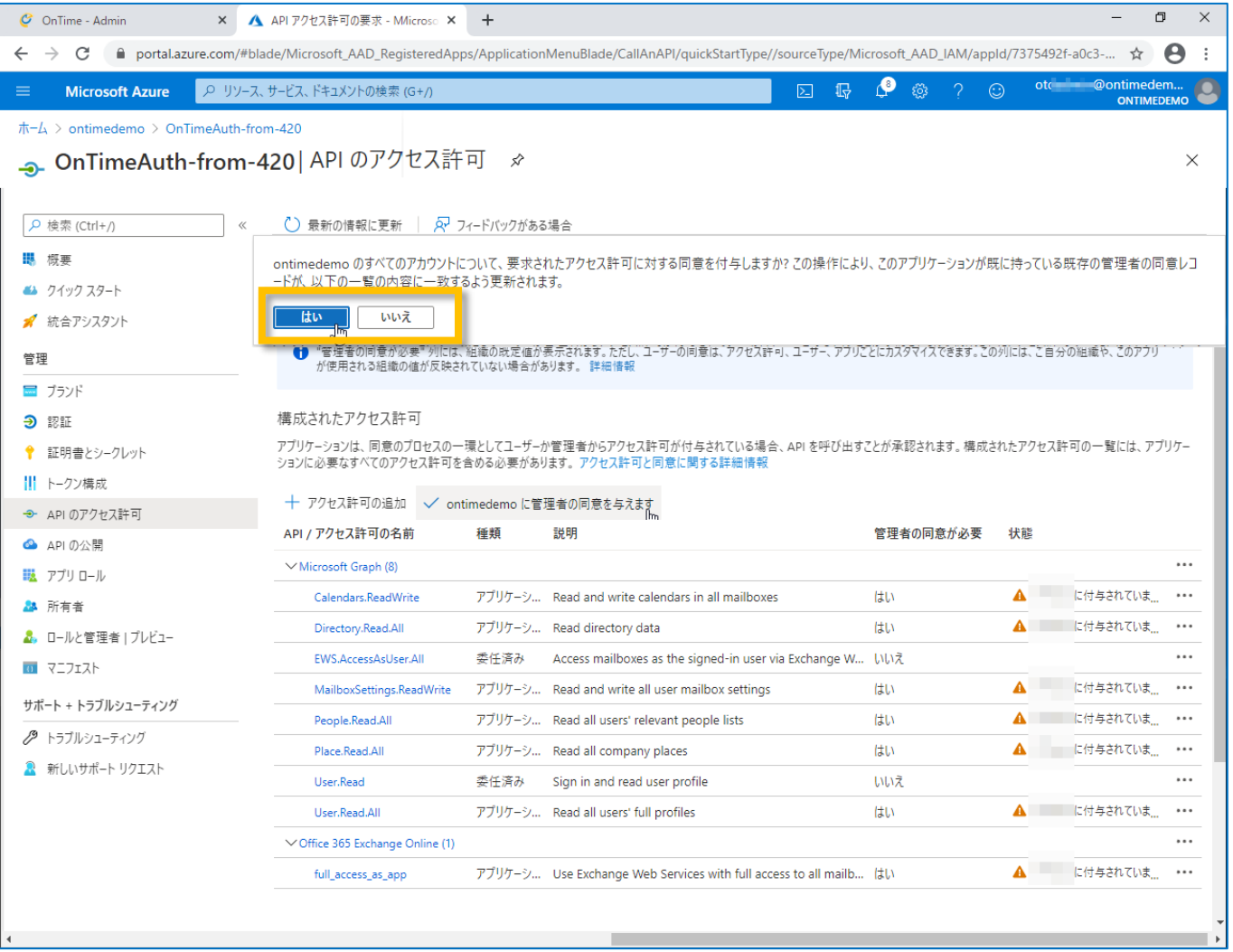
APIのアクセス許可１６



- アクセス許可の一覧に画面のようにAPIが並びます。

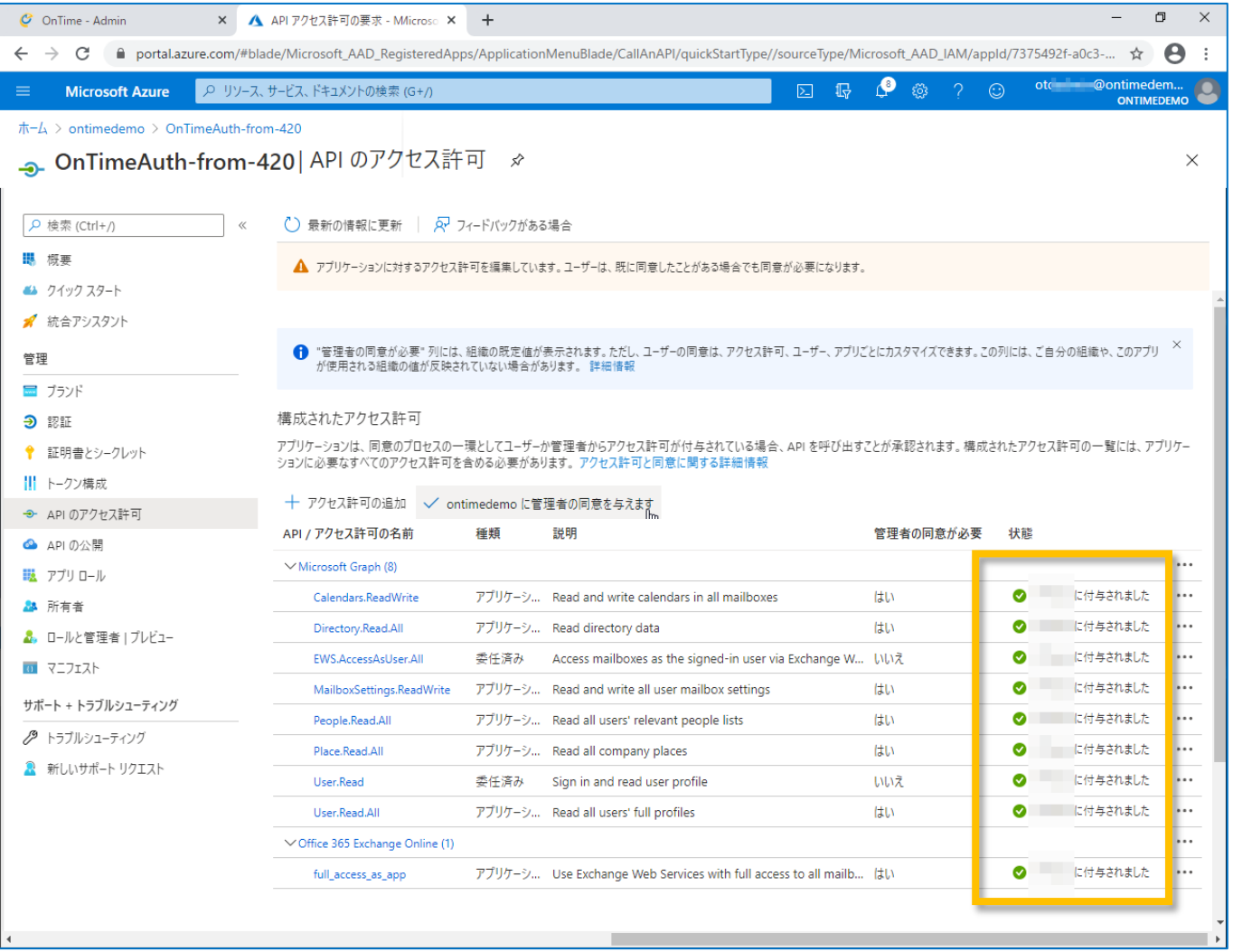
「“ドメイン名”に管理者の同意を与えます」ボタンをクリックします。

APIのアクセス許可１７



- 確認画面では「はい」をクリックします。

APIのアクセス許可１８

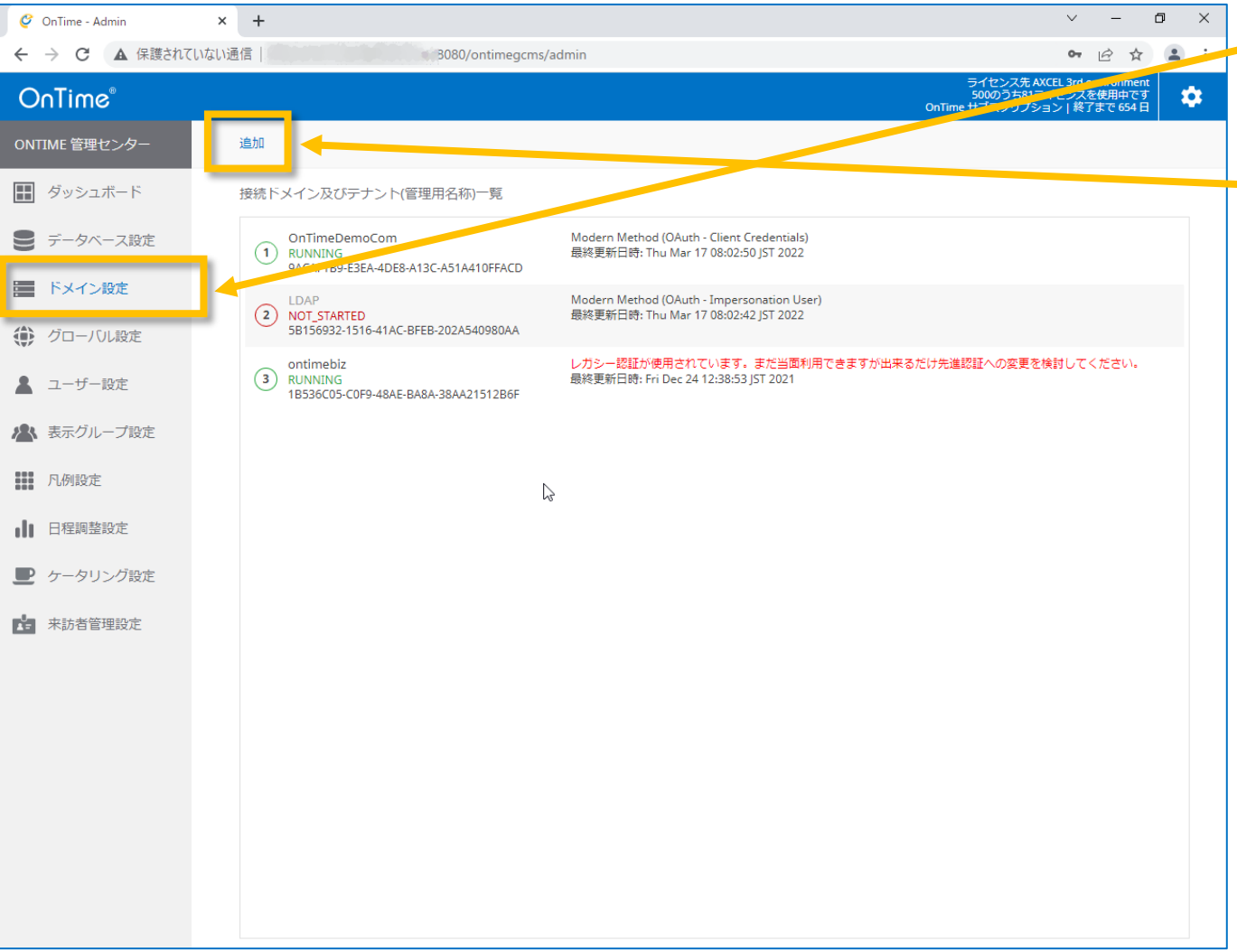


- 無事に付与されてるか確認します。
- もし付与されない場合はAzureグローバル管理者に連絡してご確認ください。

- 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

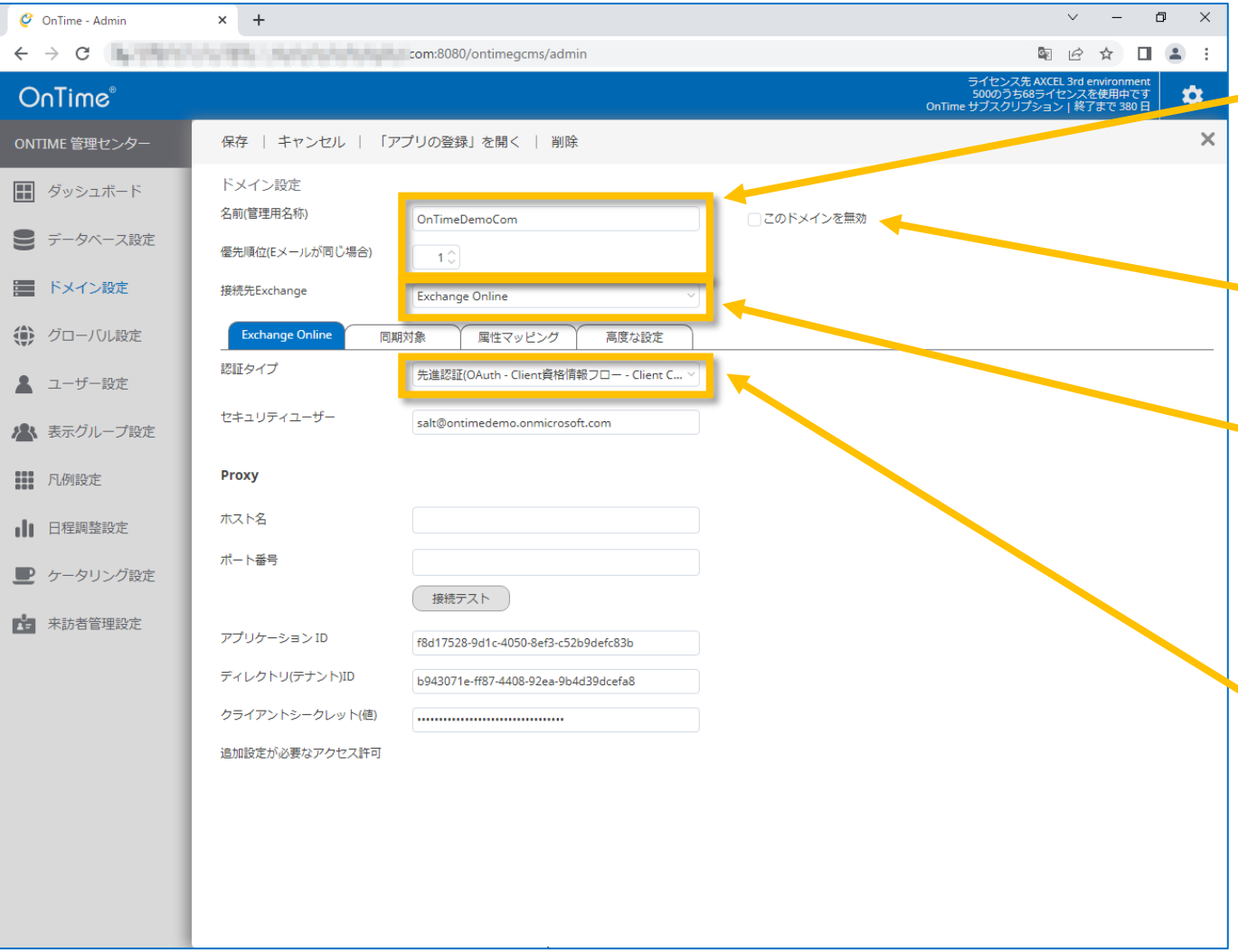


左サイドメニューで「ドメイン設定」を選択します。

「追加」をクリックします。

- Exchange Onlineへの接続で未だ「基本認証(BASIC)」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ーメーションが表示されます。先進認証への変更をお願いします。
- オンプレExchangeサーバーへは基本認証で接続します。

ドメイン設定画面



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。

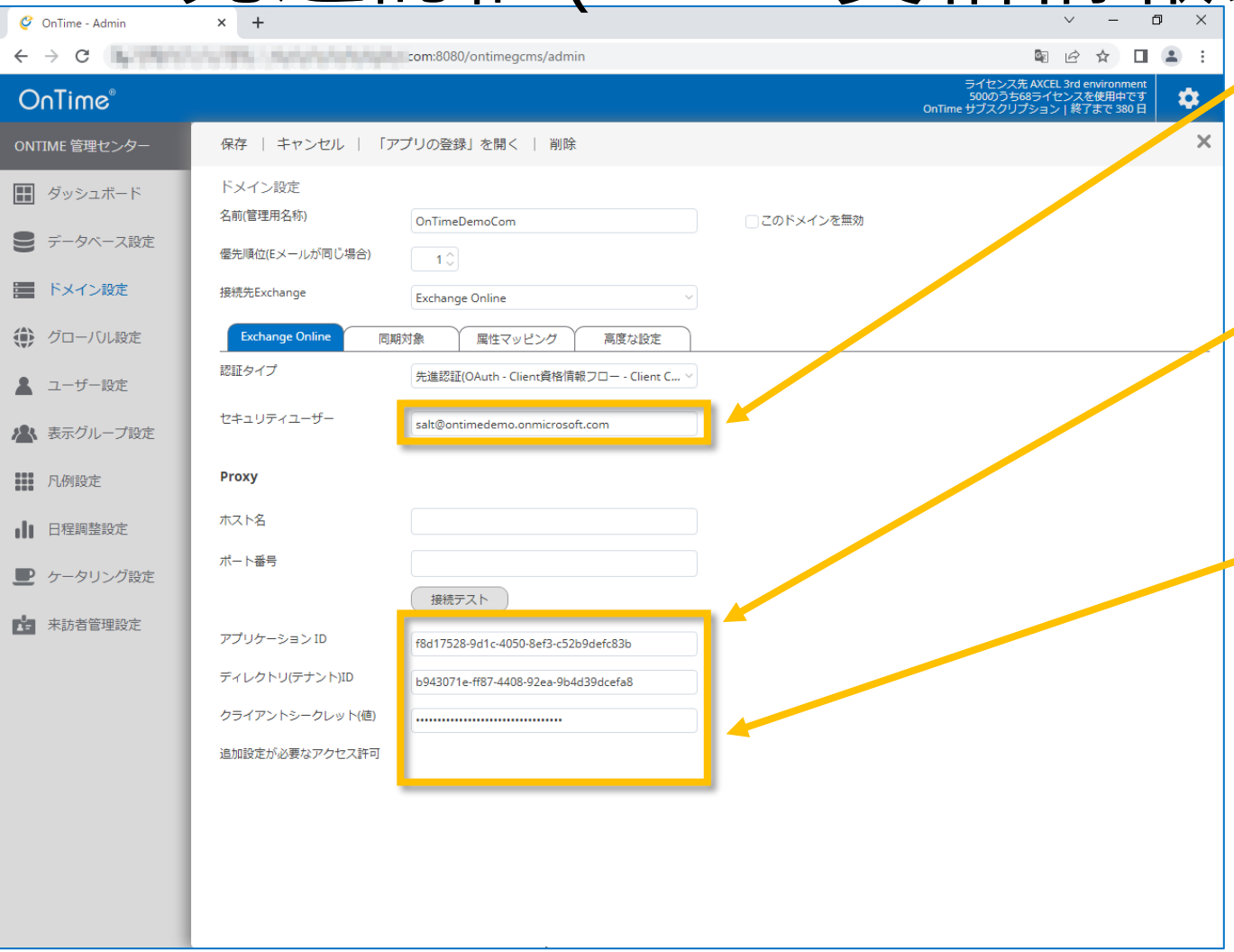
接続先ExchangeでExchange Onlineかオンプレ Exchangeを選択します。Microsoft365(Exchange Online)の場合は「Exchange Online」を選択します。

オンプレExchangeの設定は補足 2 をご参照ください。

認証タイプは以下の 3 つから選択します。

・先進認証(OAuth - Client資格情報フロー - Client Credentials)
・先進認証(OAuth - 認可コードフロー - Impersonation User)
・基本認証(BASIC)

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。

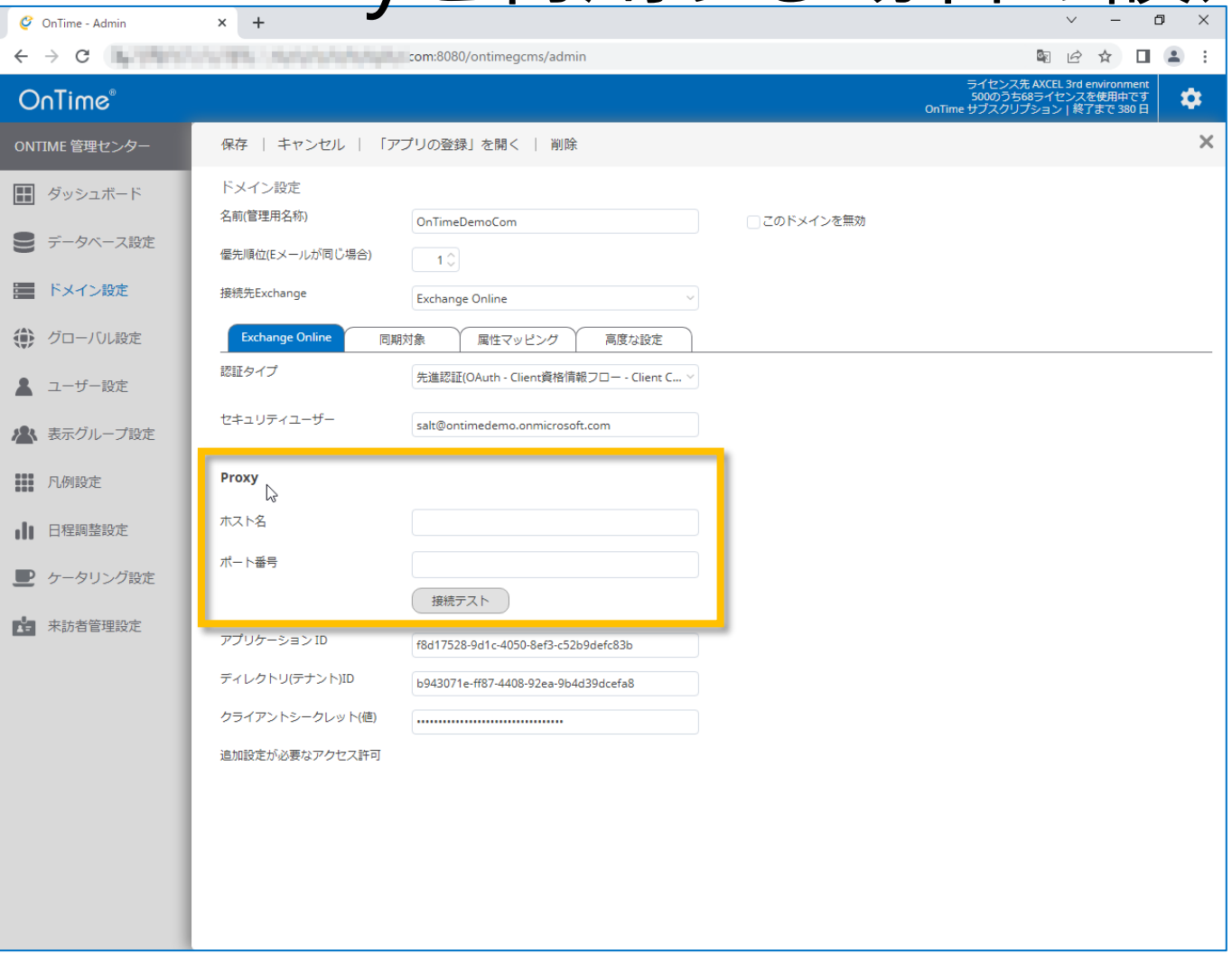
- セキュリティユーザー名は操作ログ情報に残ります。

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)に必要となる各種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。

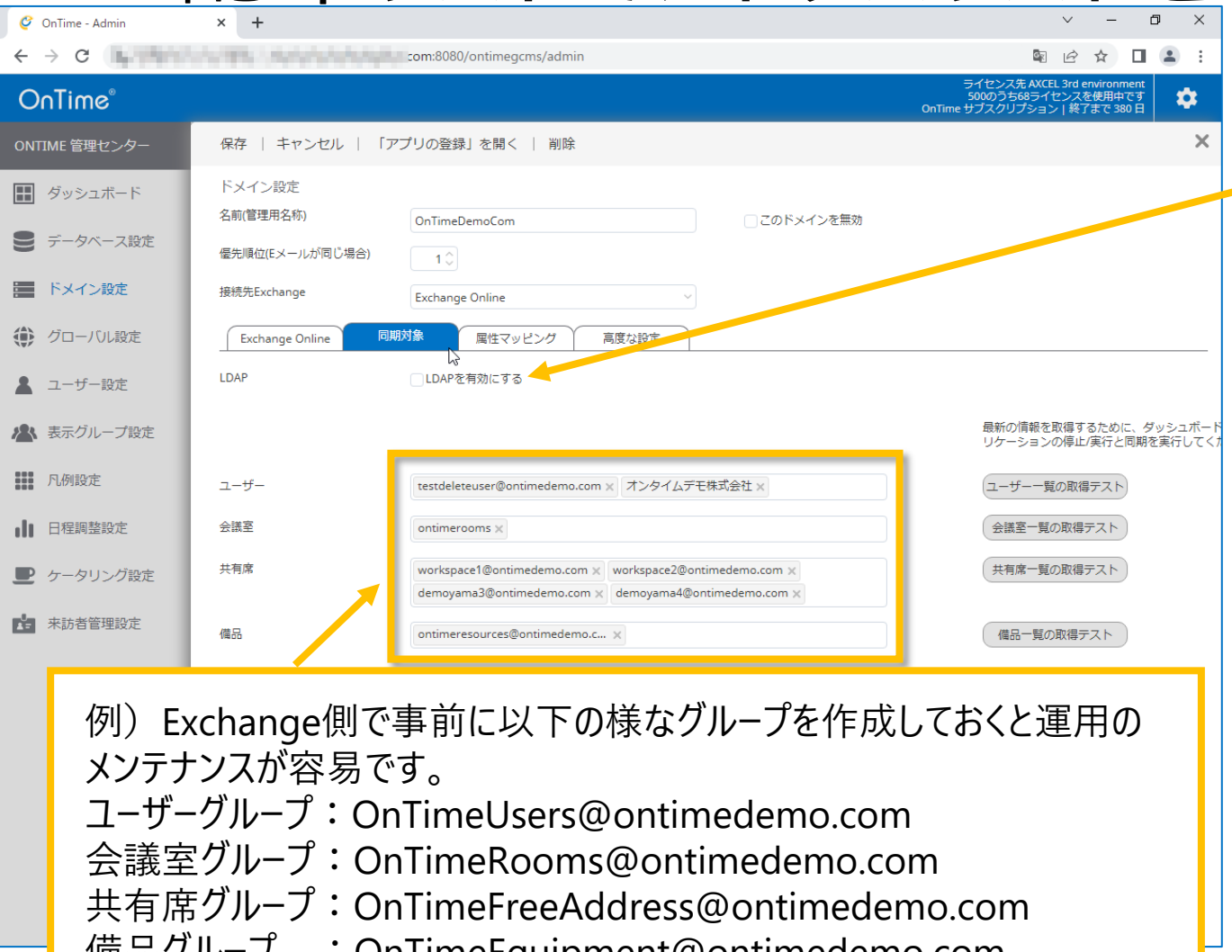
クライアントシークレットは期限付きの為、自組織の設定に合わせ更新ください

Exchange Onlineタブ−Proxy
Proxyを利用する場合の設定



- 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ください。OnTimeが行うデータはあまり副次利用されません。

同期対象タブ
配布リストでアドレスリストを取得



例）Exchange側で事前に以下の様なグループを作成しておくと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

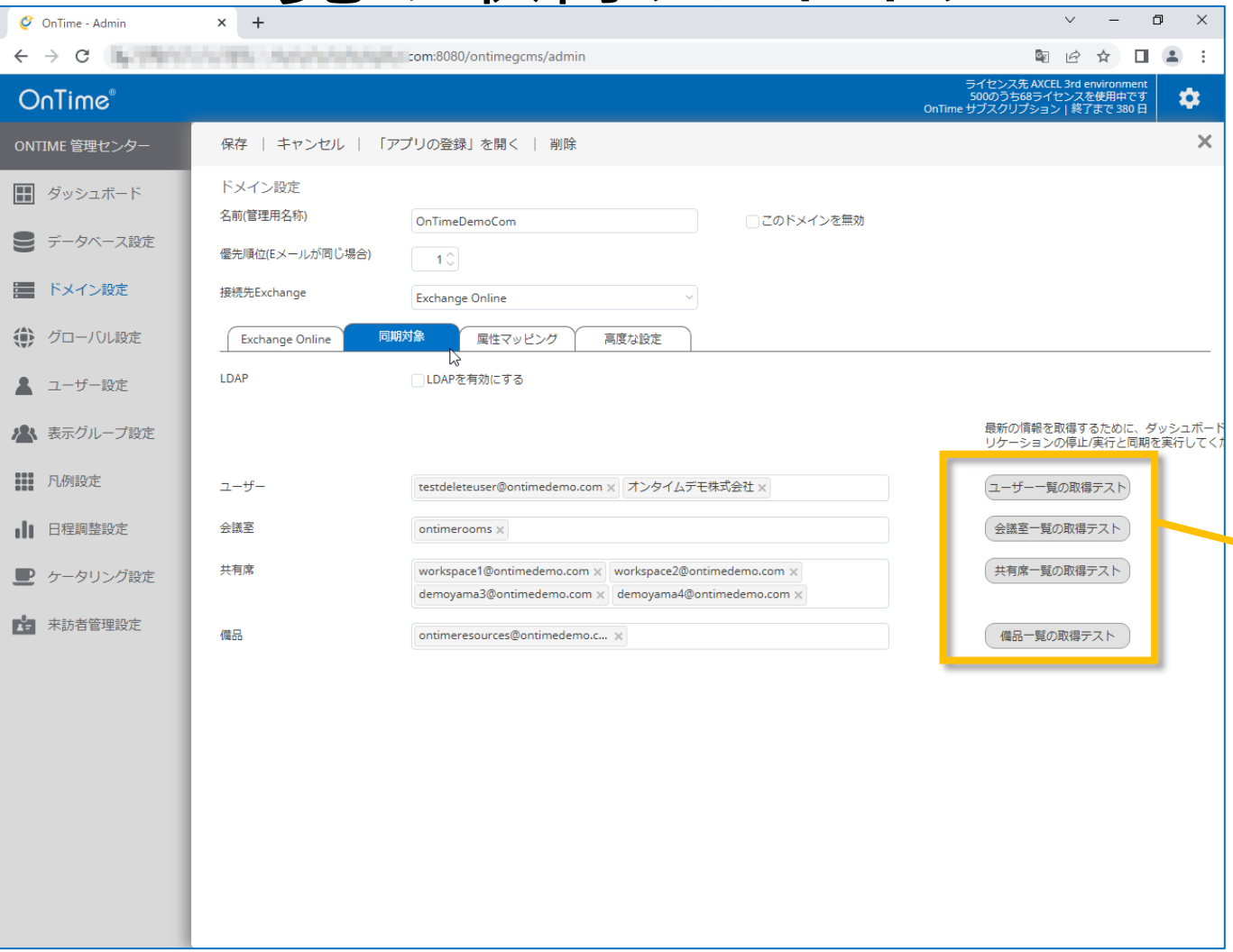
- グループのメールアドレスのリスト指定を推奨します。

"LDAPを有効にする"のチェックはLDAP利用の際にチェックします。

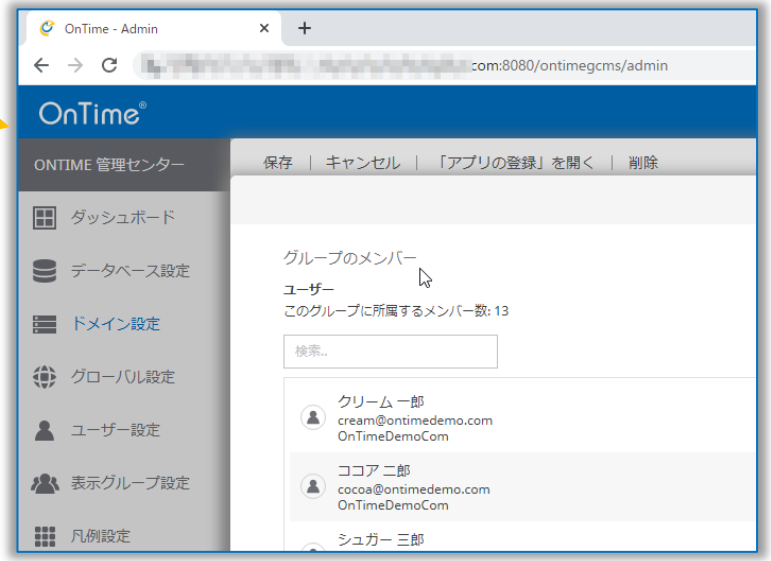
- 次にOnTimeと同期するリストをグループ化した配布グループ(配布リスト)のメールアドレスを指定します。
- グループアドレスにはOnTimeで表示する、または操作できるいずれの場合のアカウントでも含まれている必要があります。
- 設定した配布グループが入れ子になっていても問題ありません。入れ子になっているグループを指定するとOnTime管理センターのその他の設定（ロール設定や静的グループ設定）などで利用できます。
- ドメインの ユーザー、会議室、共有席、備品のそれぞれに指定されている配布グループ(配布リスト)のメールアドレスが複数の場合はカンマやエンターキーで区切ってください。

※LDAP利用の設定方法は補足 3 をご参照ください。

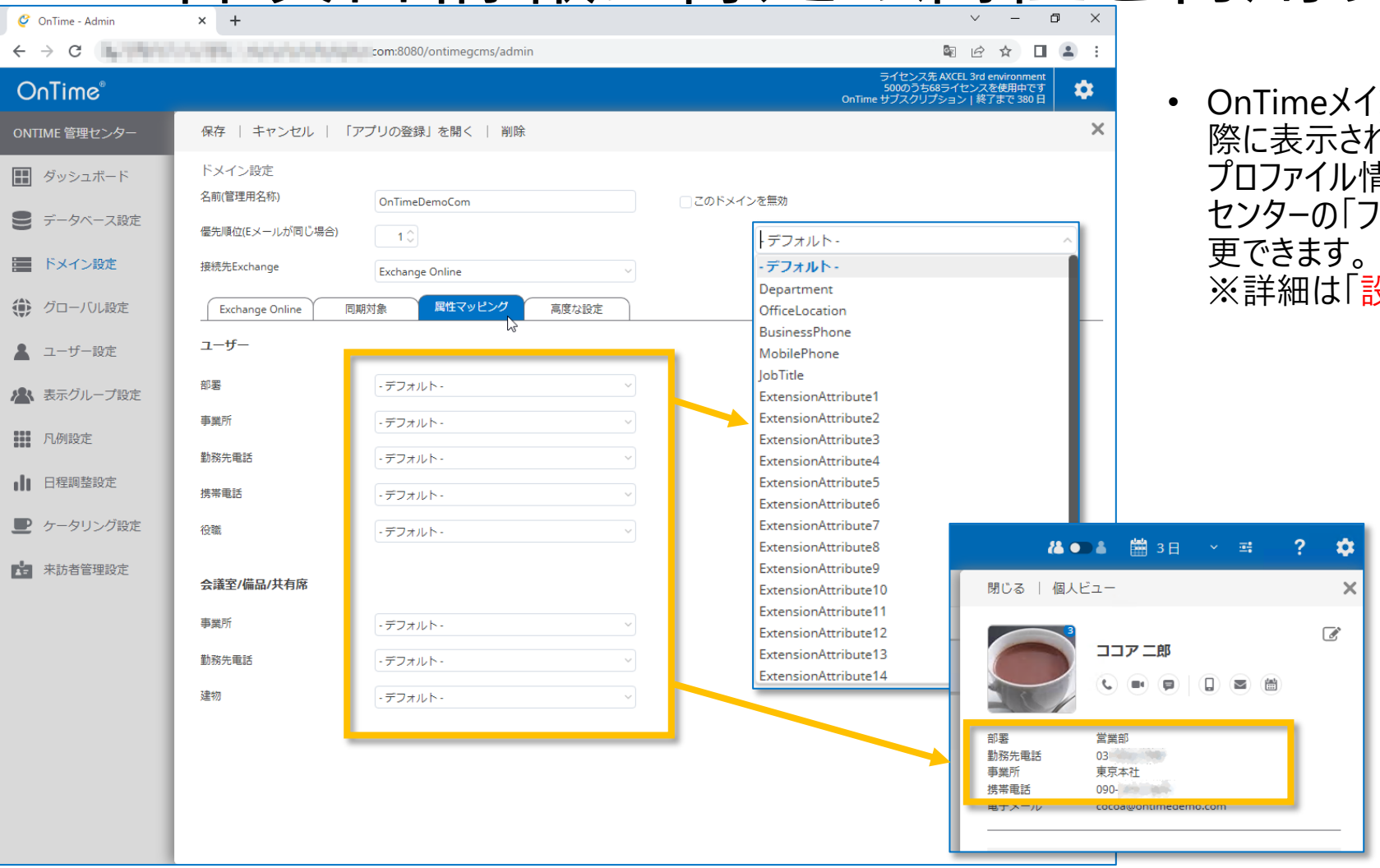
同期対象タブ
一覧の取得テストボタン



- 指定欄の右側にある各ボタンを押すと、その欄に指定したユーザーやグループの指定結果の一覧を確認できます。

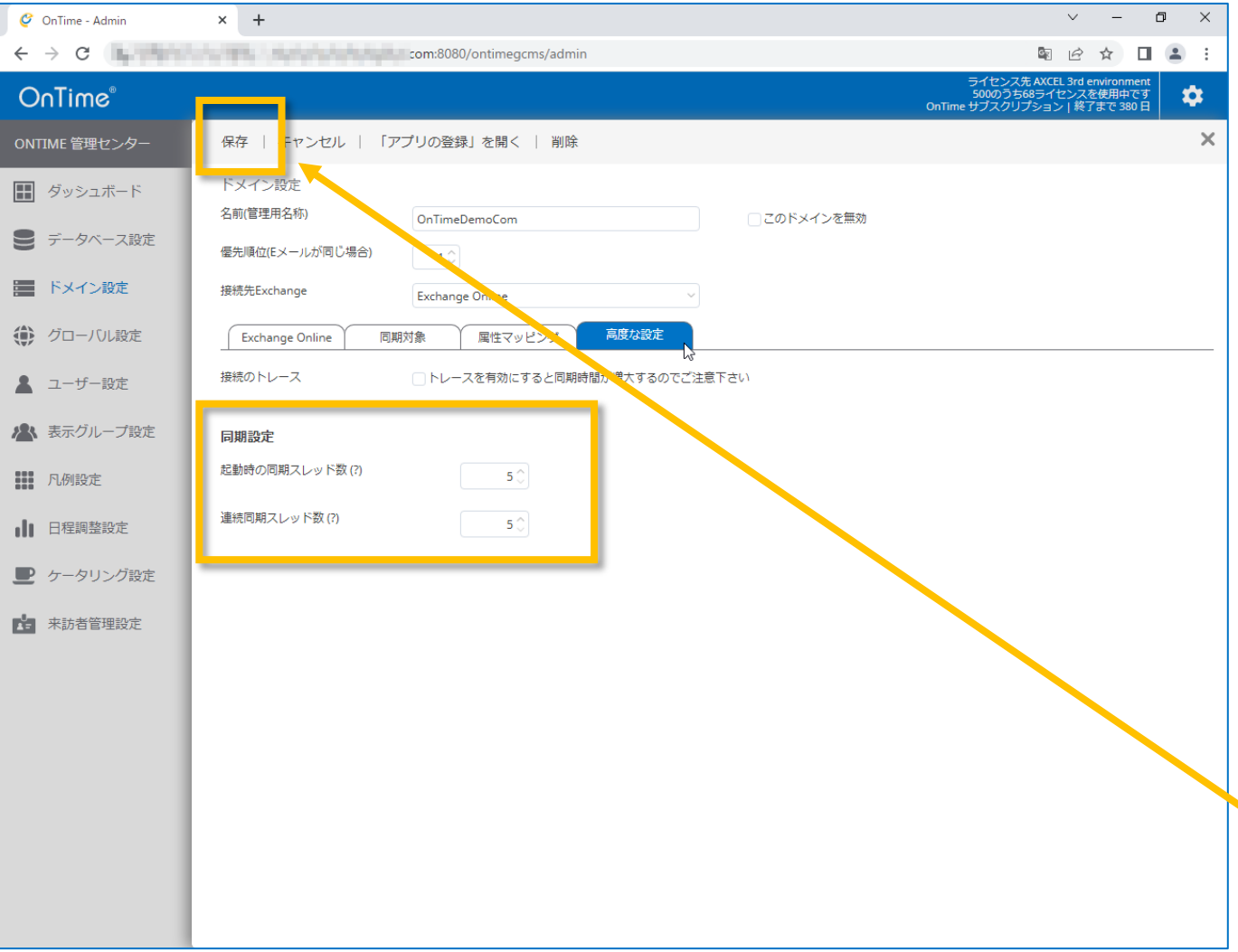


属性マッピングタブ
各項目情報に特定の属性を利用する場合の設定



- OnTimeメインビューでユーザープロファイ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。
プロファイ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「設定マニュアル」をご参照ください

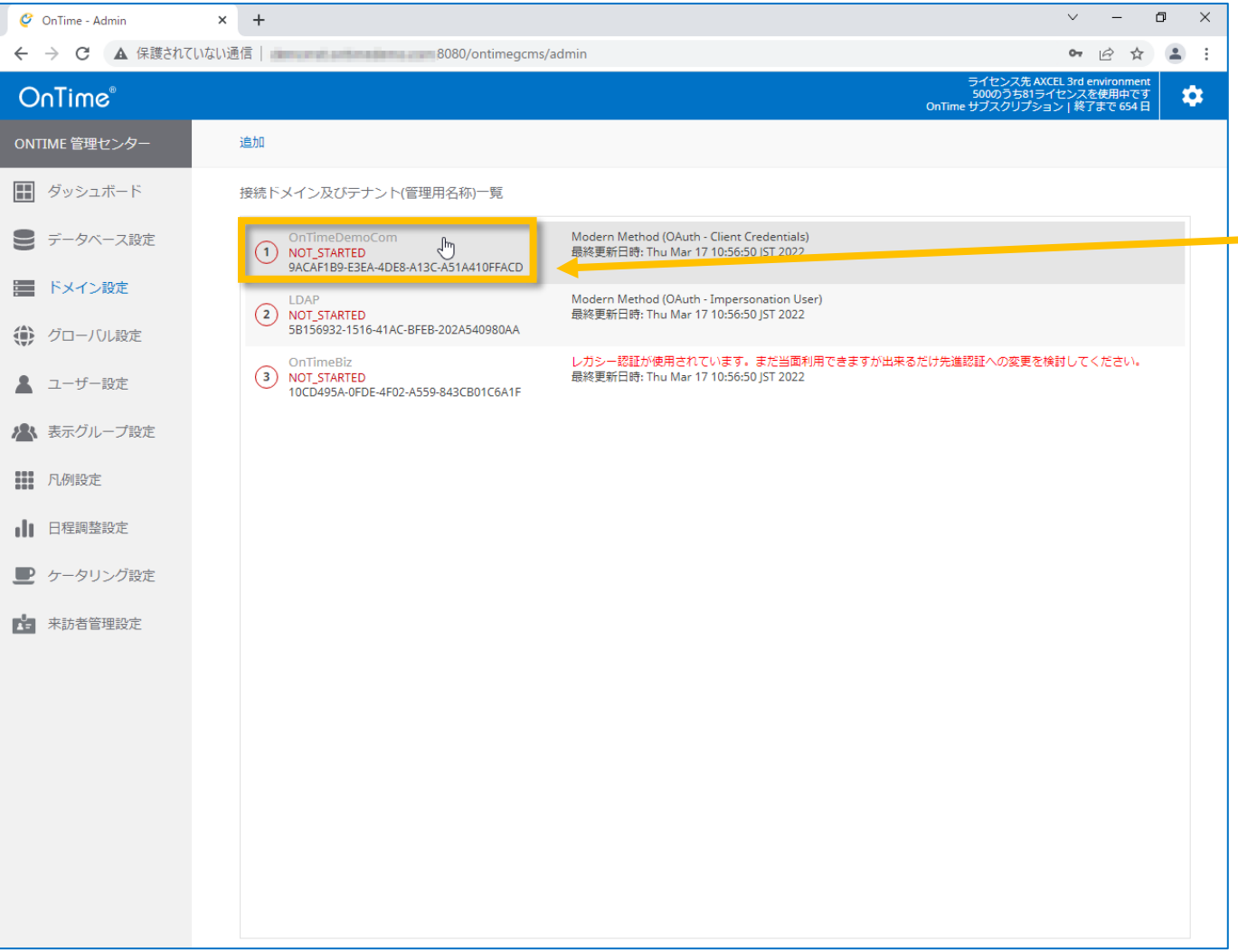
高度な設定タブ



- 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もあります。
  - 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やメモリに充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



- 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。

ダッシュボードで再起動

- 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

- 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

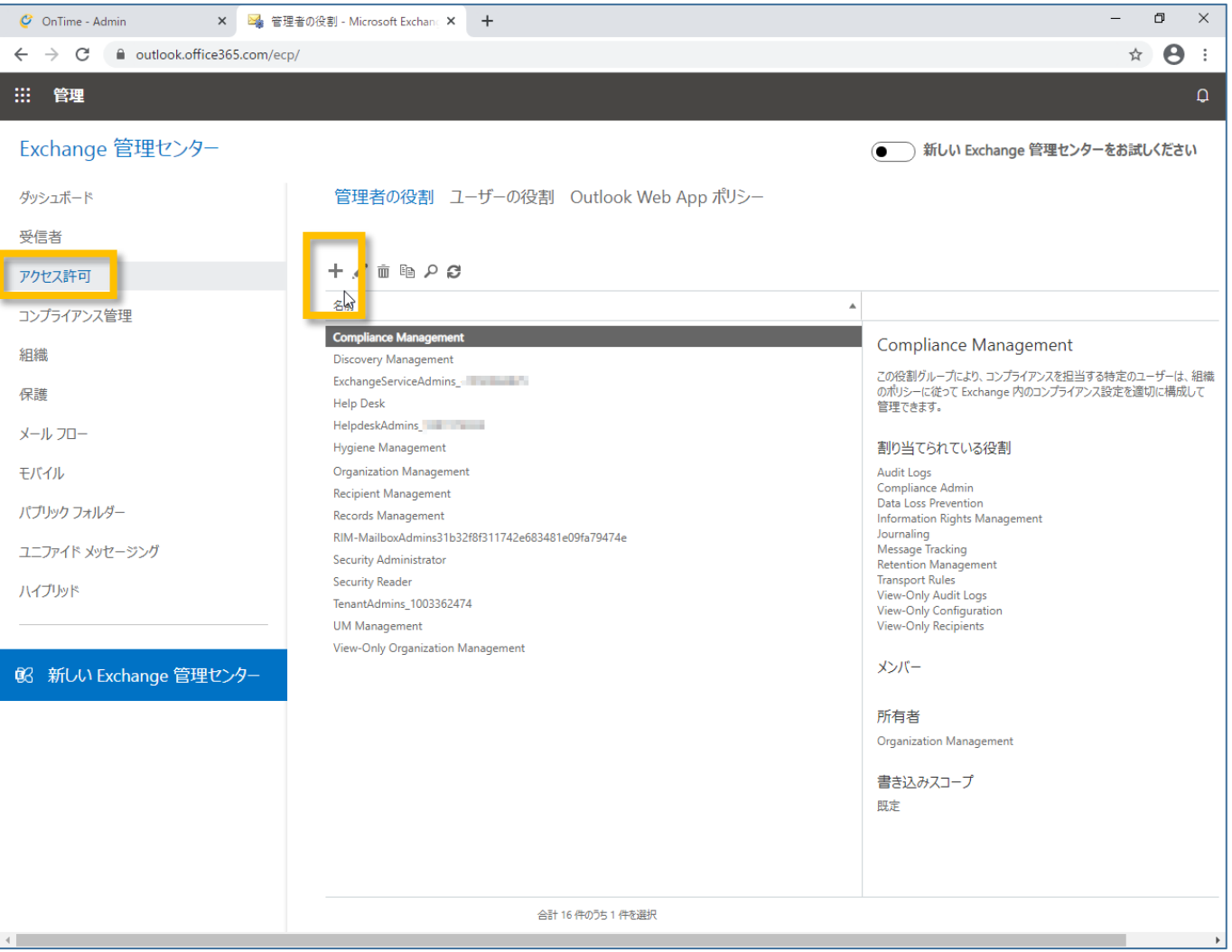
Exchange側の設定準備

- 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/

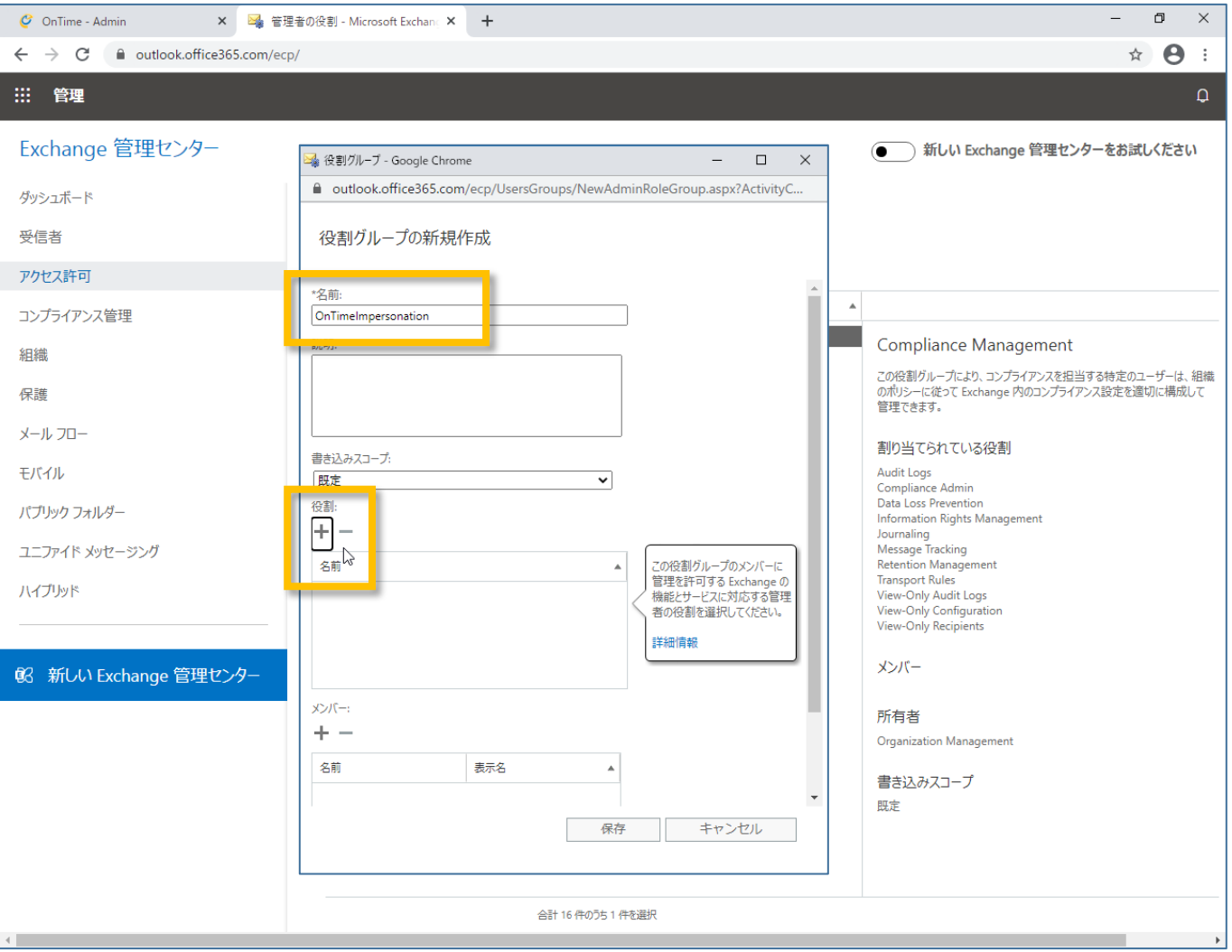
- 書き込みスコープを制限して特定のメールボックスに制限する方法について
  - テナント運用者とOnTime運用者が違う場合などで厳密に同期対象のメールボックスだけに接続の制限を掛けたい場合は、同期を司るユーザーに割り当てる役割「ApplicationImpersonation」指定時の「書き込みスコープ」を厳密に設定することで明確化が可能です。
  - ドメイン(テナント)の特定のグループのメールボックスだけに OnTime の利用制限ができますか？
    https://www3.ontimesuite.jp/makescope/

Exchange管理センターを開く



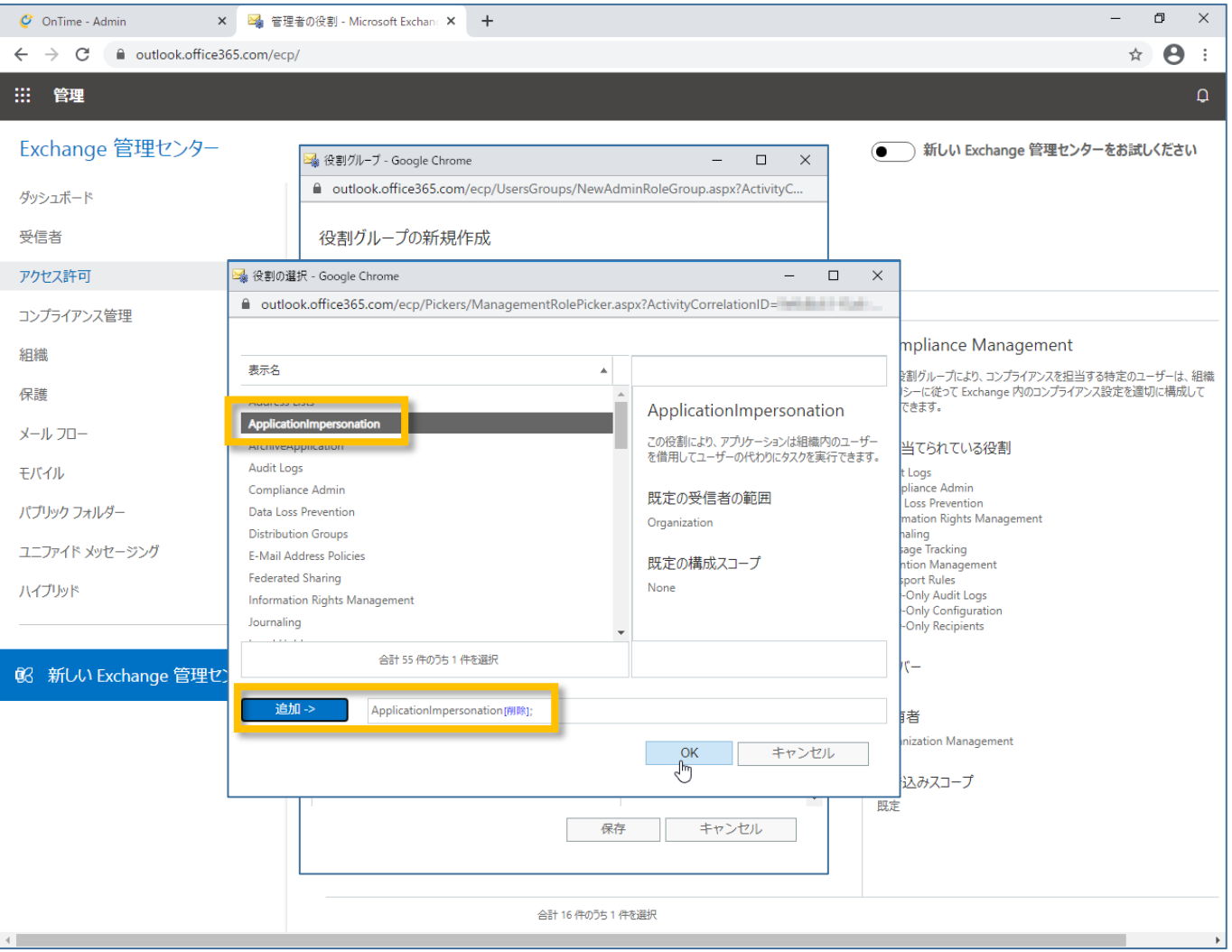
- Exchange管理センターを開きます。
- アクセス許可を開きます。
- 管理者の役割を開きます。
- ＋ボタンを押して管理者の役割を追加します。

管理者の役割の追加 1



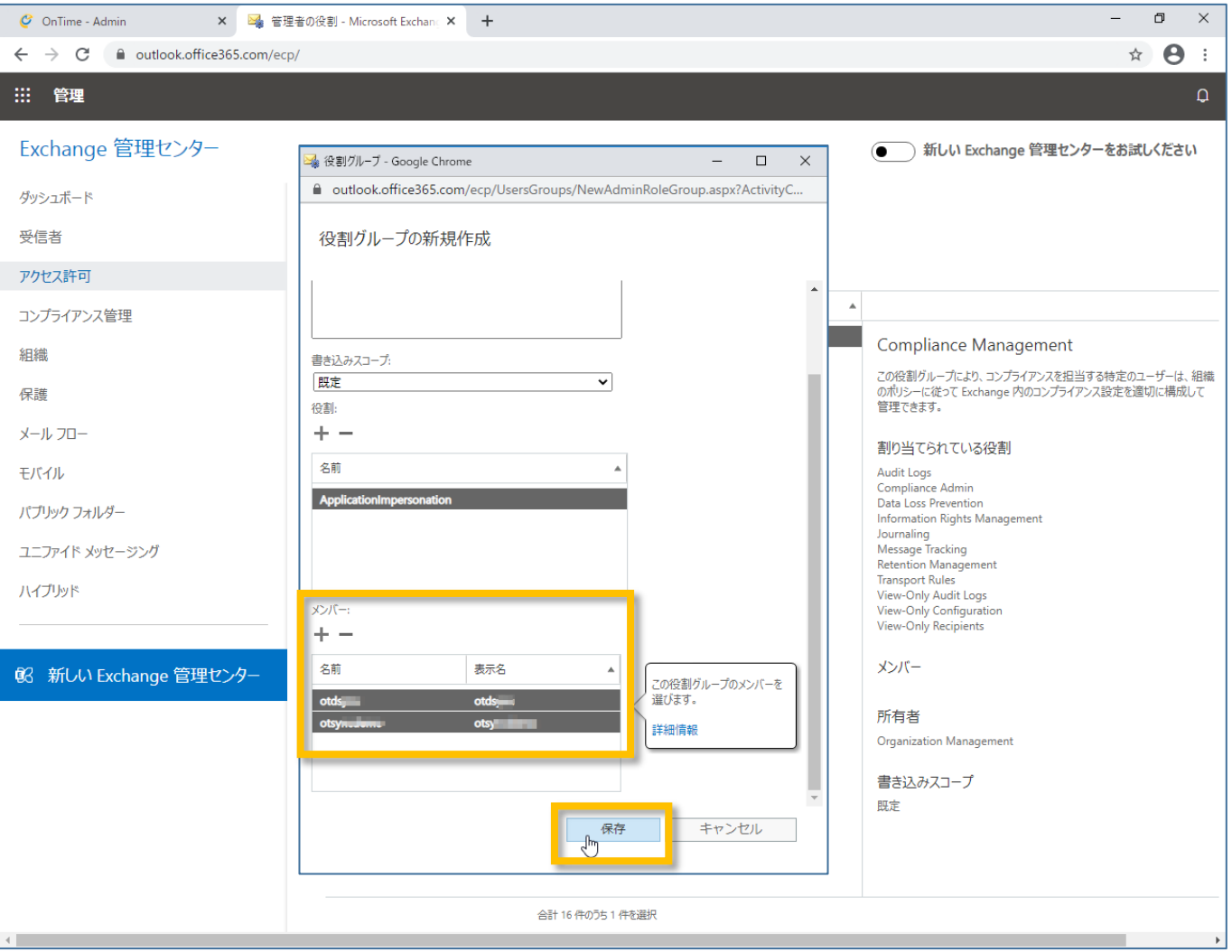
- 新しい役割を作成します。
- 名前には識別しやすい名前を指定してください。
- 役割の＋ボタンを押して役割を選択します。

管理者の役割の追加２



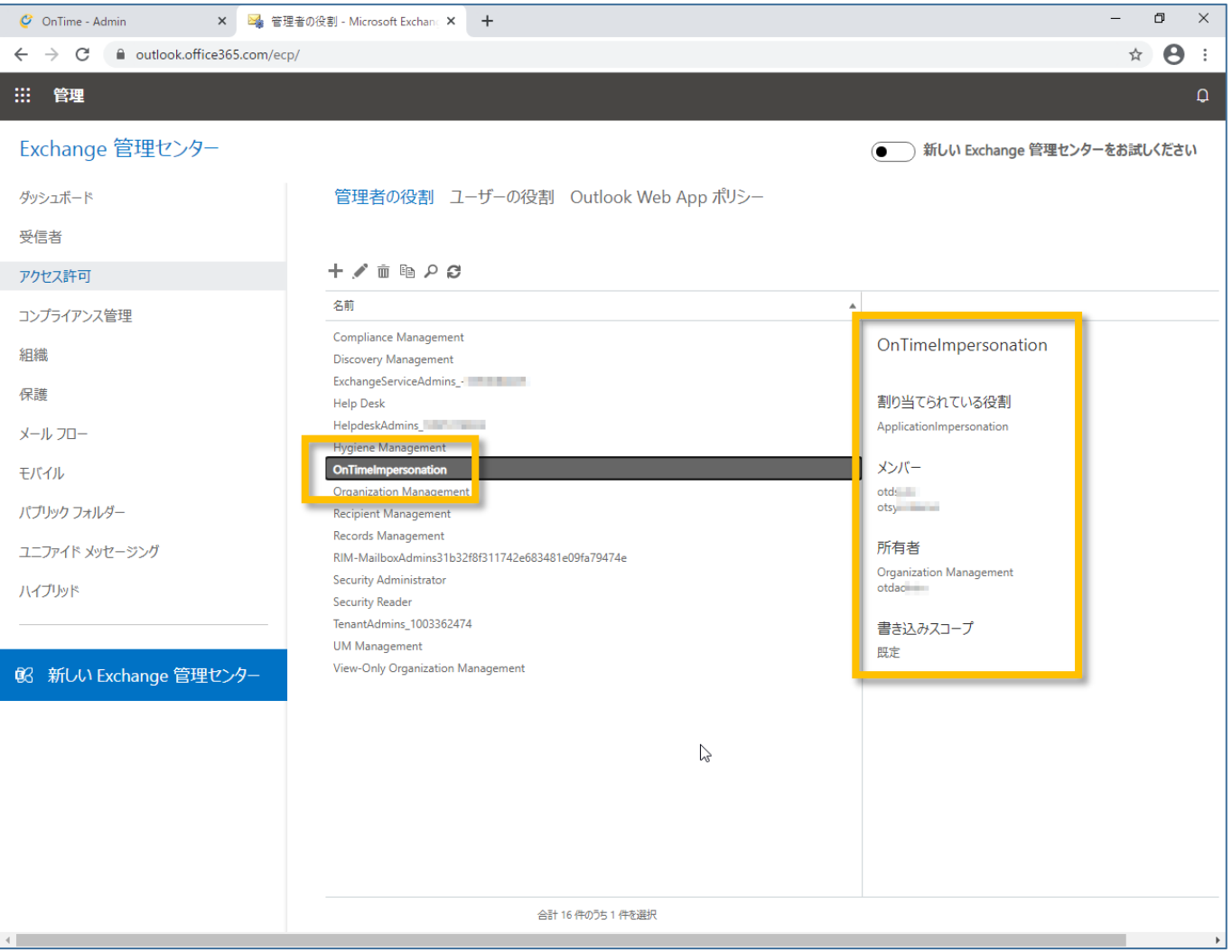
- ApplicationImpersonationを選択します。
- 「追加」を押して追加後に「OK」を押します。

管理者の役割の追加 3



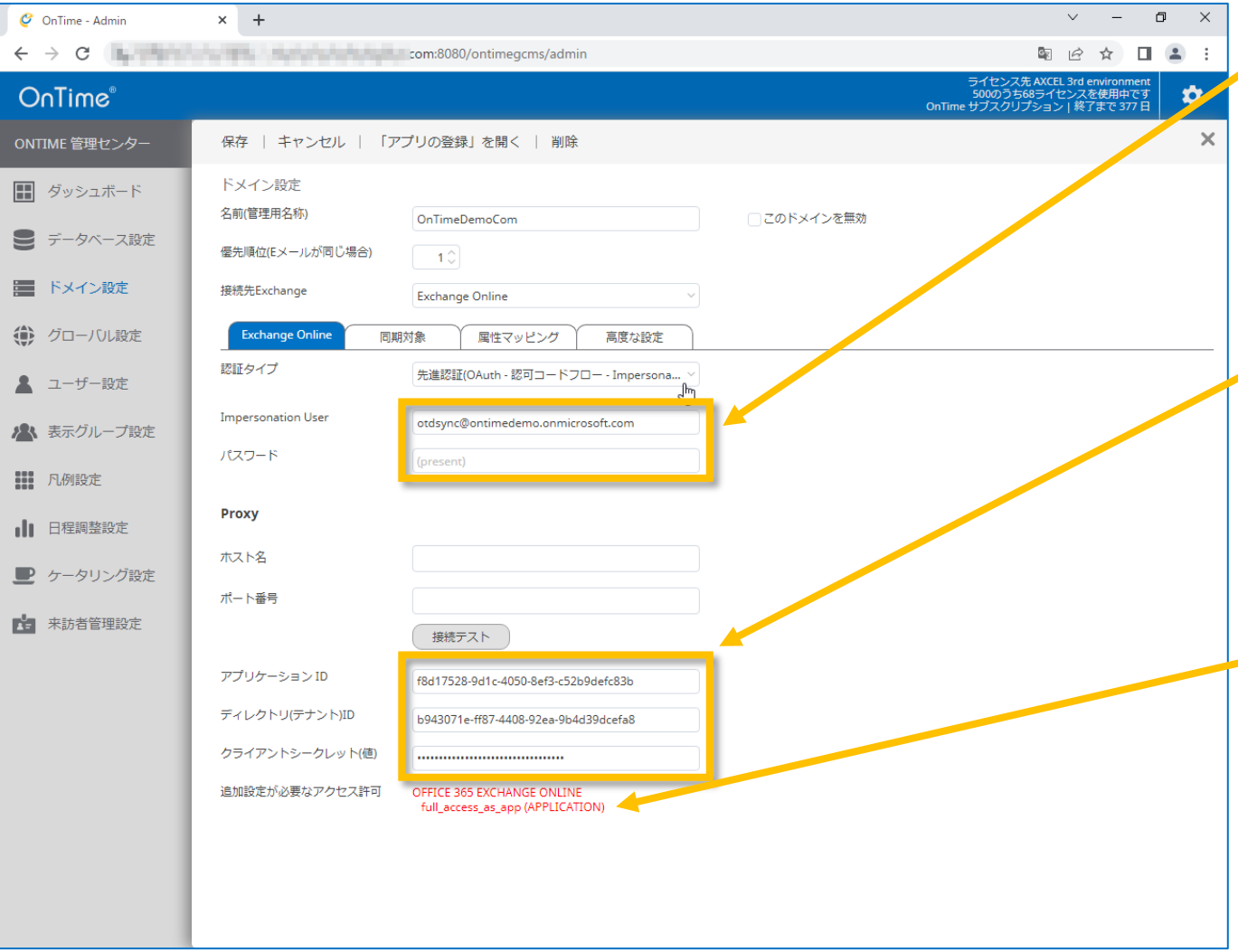
- 同じくOnTimeから同期を行うアカウントを追加します。
- 設定ができたら「保存」を押します。

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。

OnTime管理センターでドメイン設定



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。

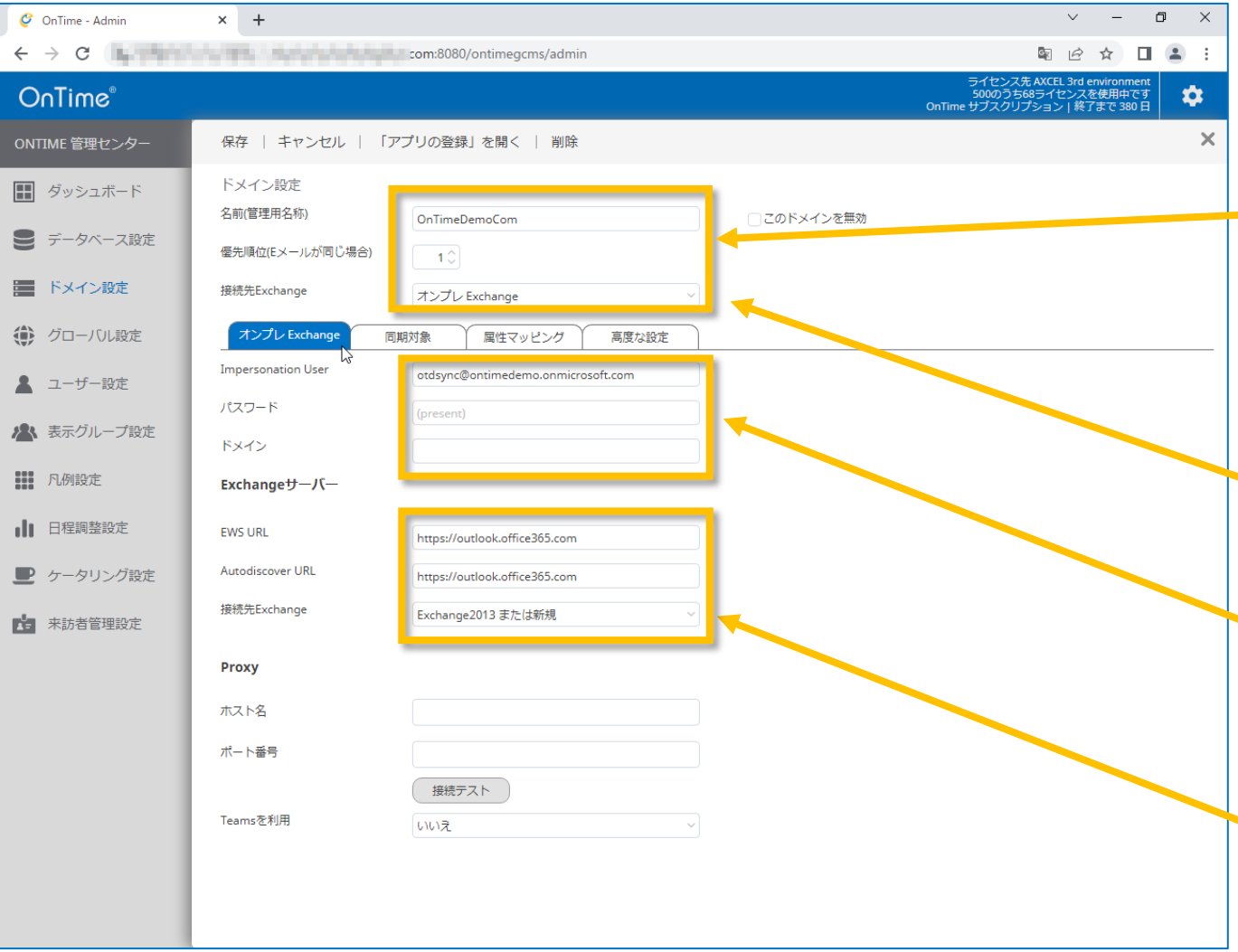
Azureで作成したアプリケーションの情報を指定します。

- 先進認証(OAuth)に必要となる各種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。

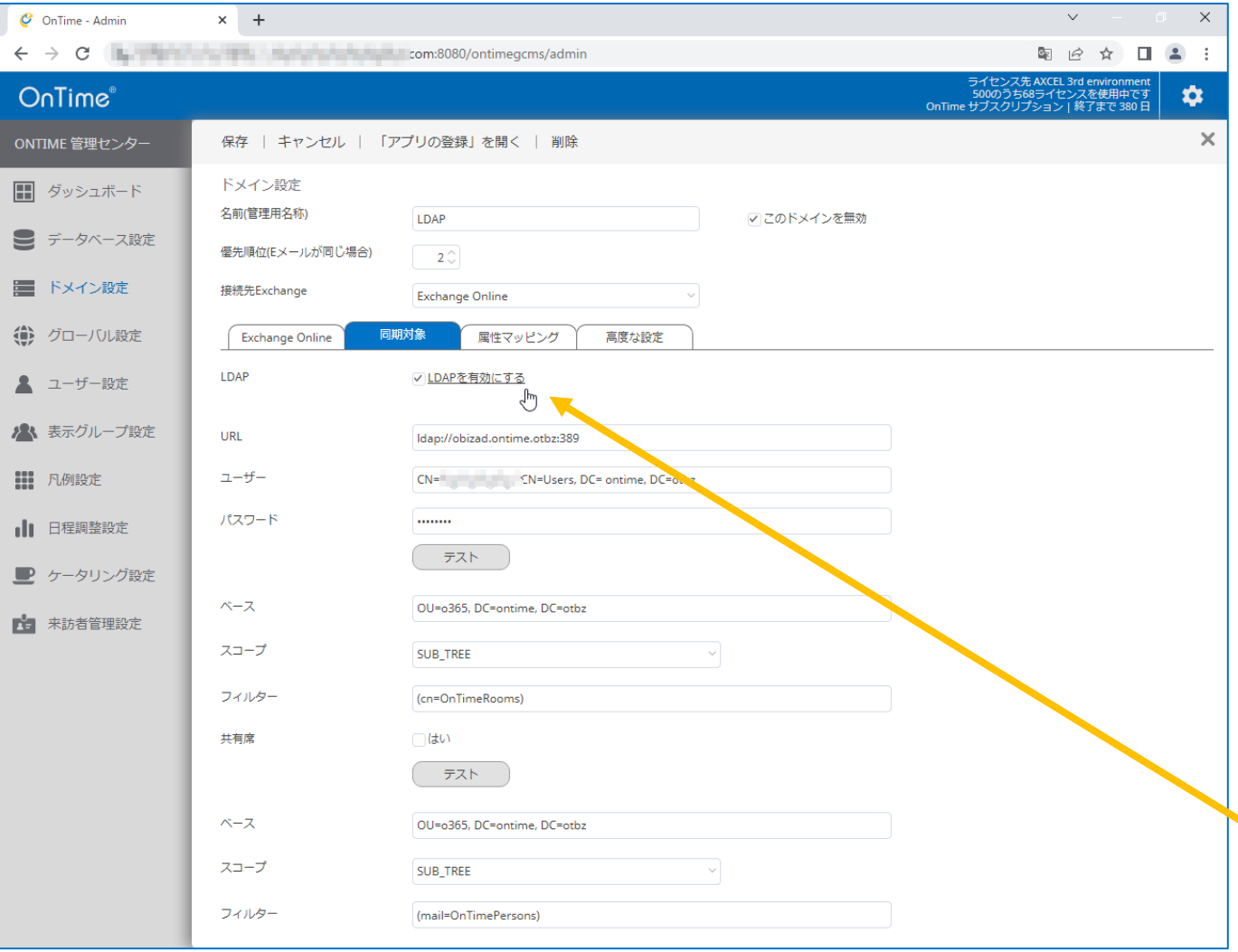
ドメインタイプで「オンプレExchange」を選択します。

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。

補足3）
同期対象をLDAPで取得

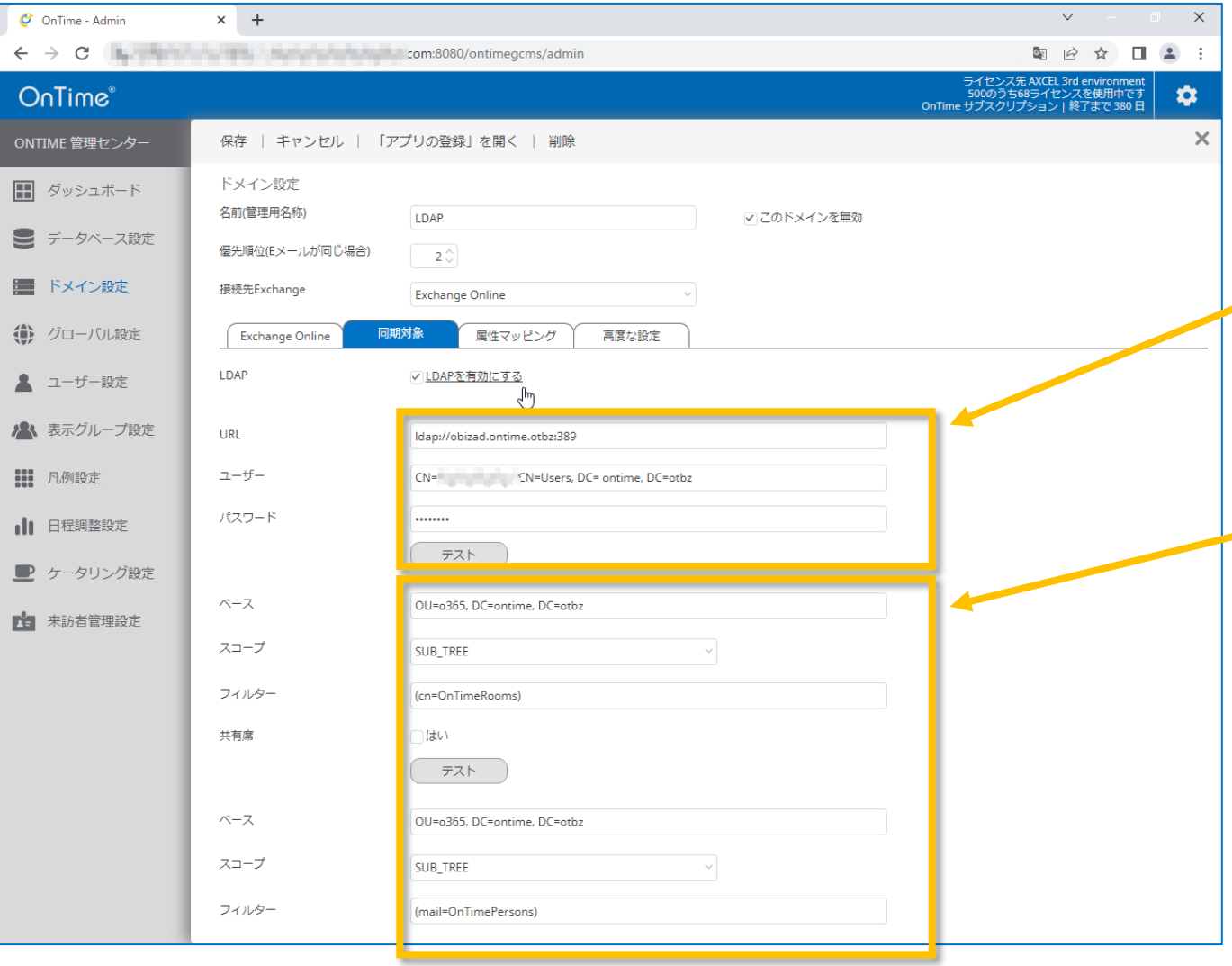
同期対象をLDAPで取得 1



- 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。

同期対象をLDAPで取得 2



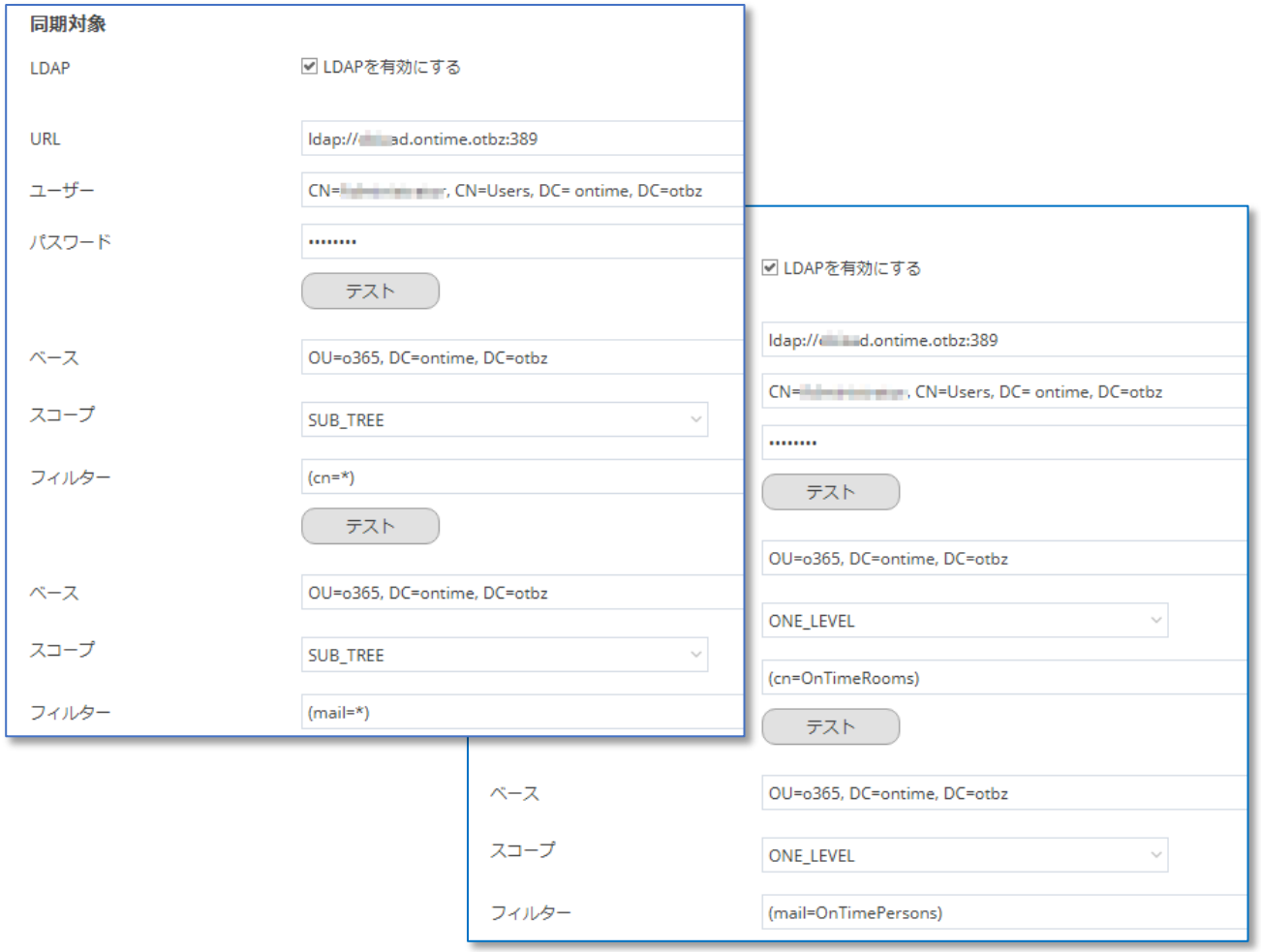
- 同期対象の設定を行います。

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。

同期対象をLDAPで取得 3

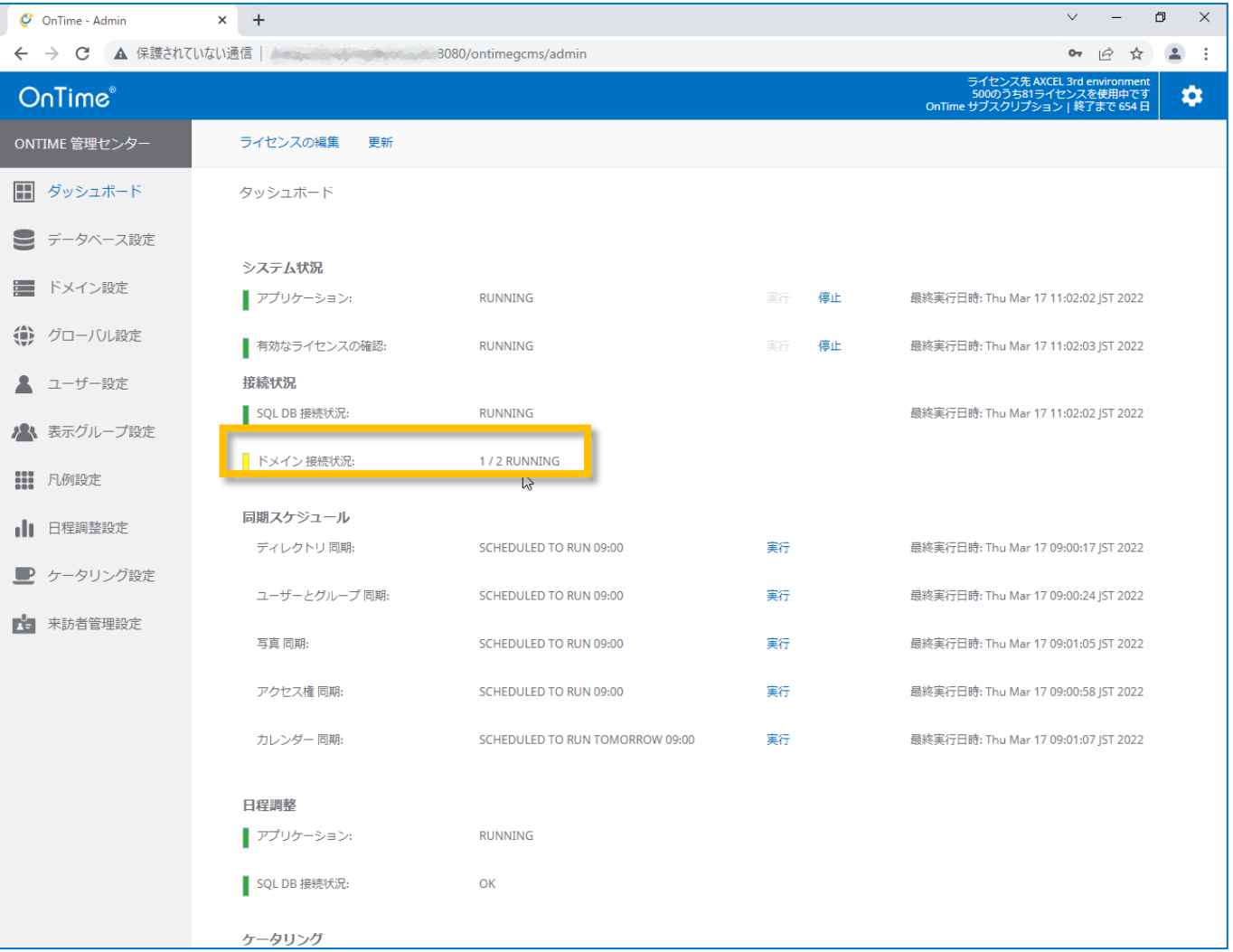


- 左図を参考に組織に応じたフィルター条件で取得してください。
- 左上　特定の属性に値があるアカウントを全て取得
- 右下　特定のグループに属しているアカウントを全て取得

- 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。

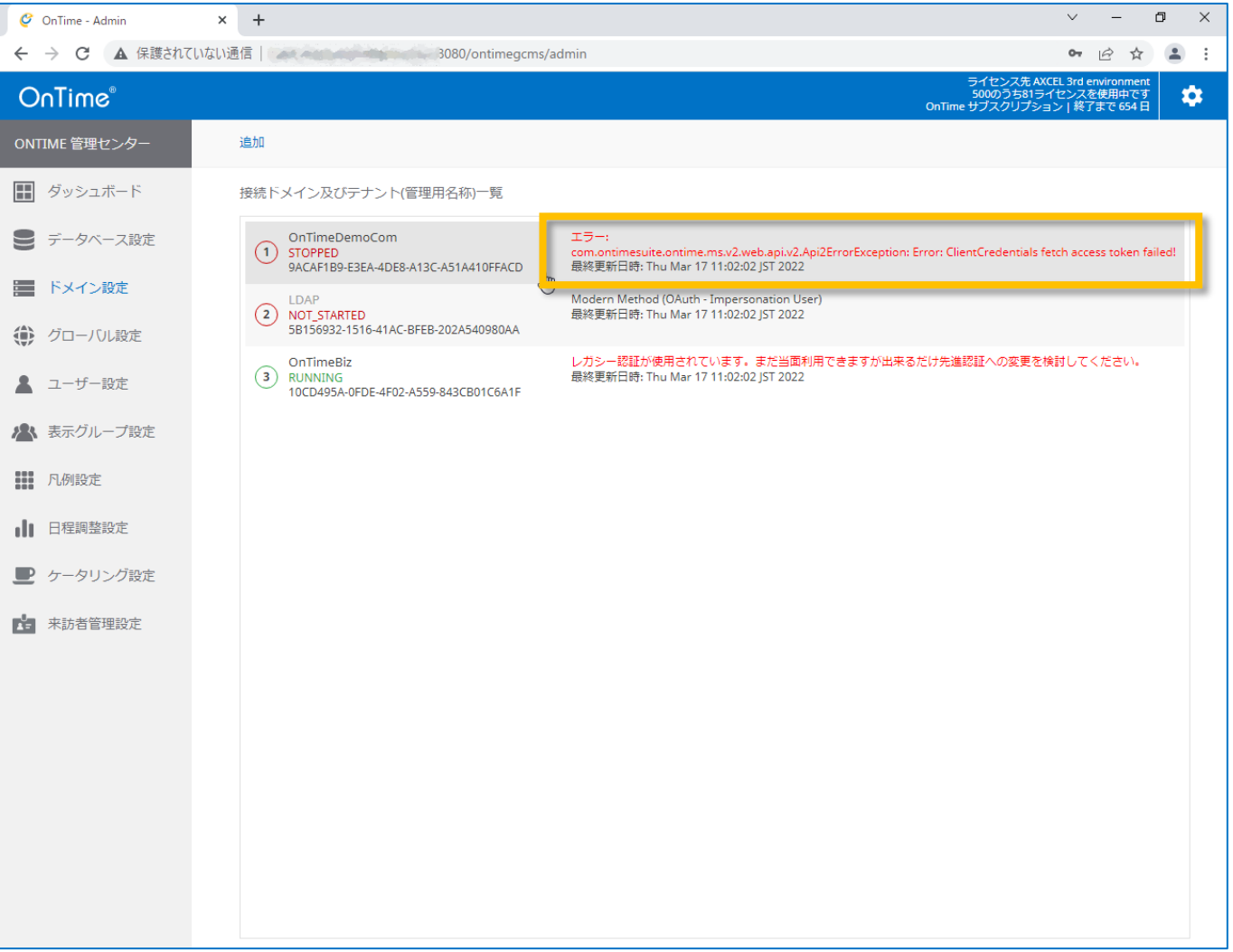
補足4）
Graphで認証エラーが出る

ドメイン接続がエラーで接続できない



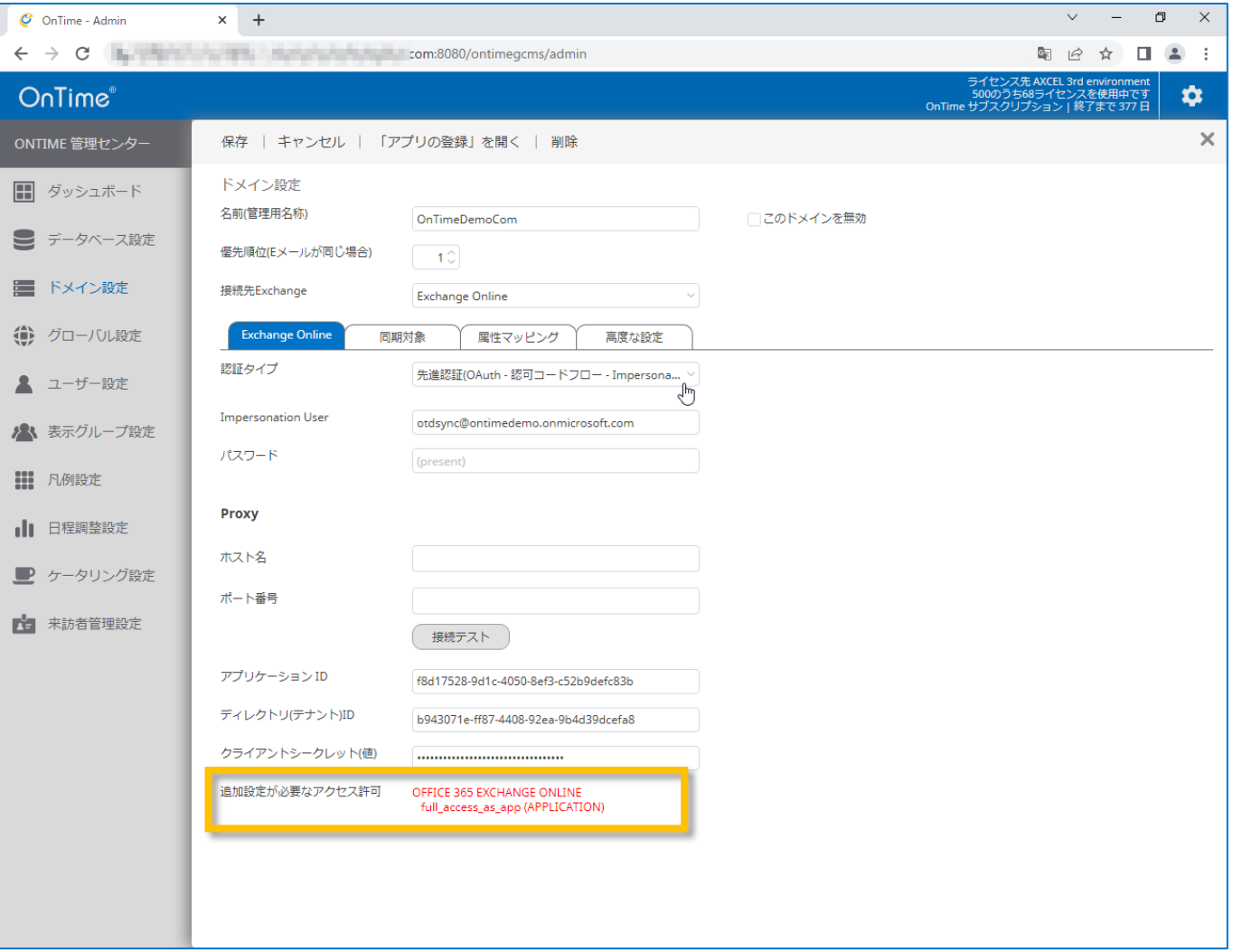
- インジケーターが赤色や黄色の場合はドメイン接続ができていない状態です。
- OnTimeをバージョンアップしたなどの場合はほとんどが先進認証(OAuth)が正しく設定されていないときです。

ドメイン設定で該当ドメインを確認



- 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



- 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た後、このドメイン設定を再保存し、再度OnTimeを起動してください。