# 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

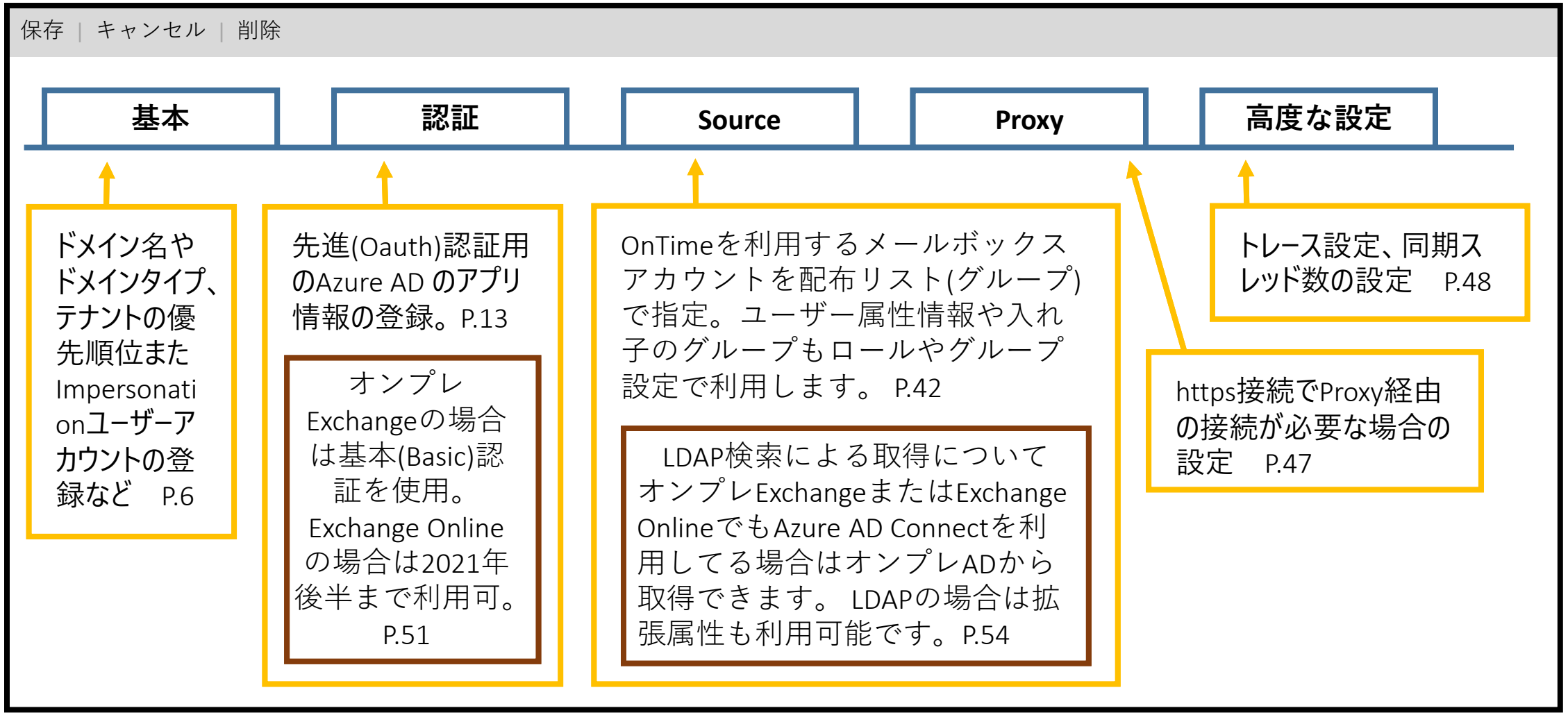
# 目次　ドメイン設定マニュアル

# ドメイン設定の概要について

# 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



# Exchange管理センターでの作業

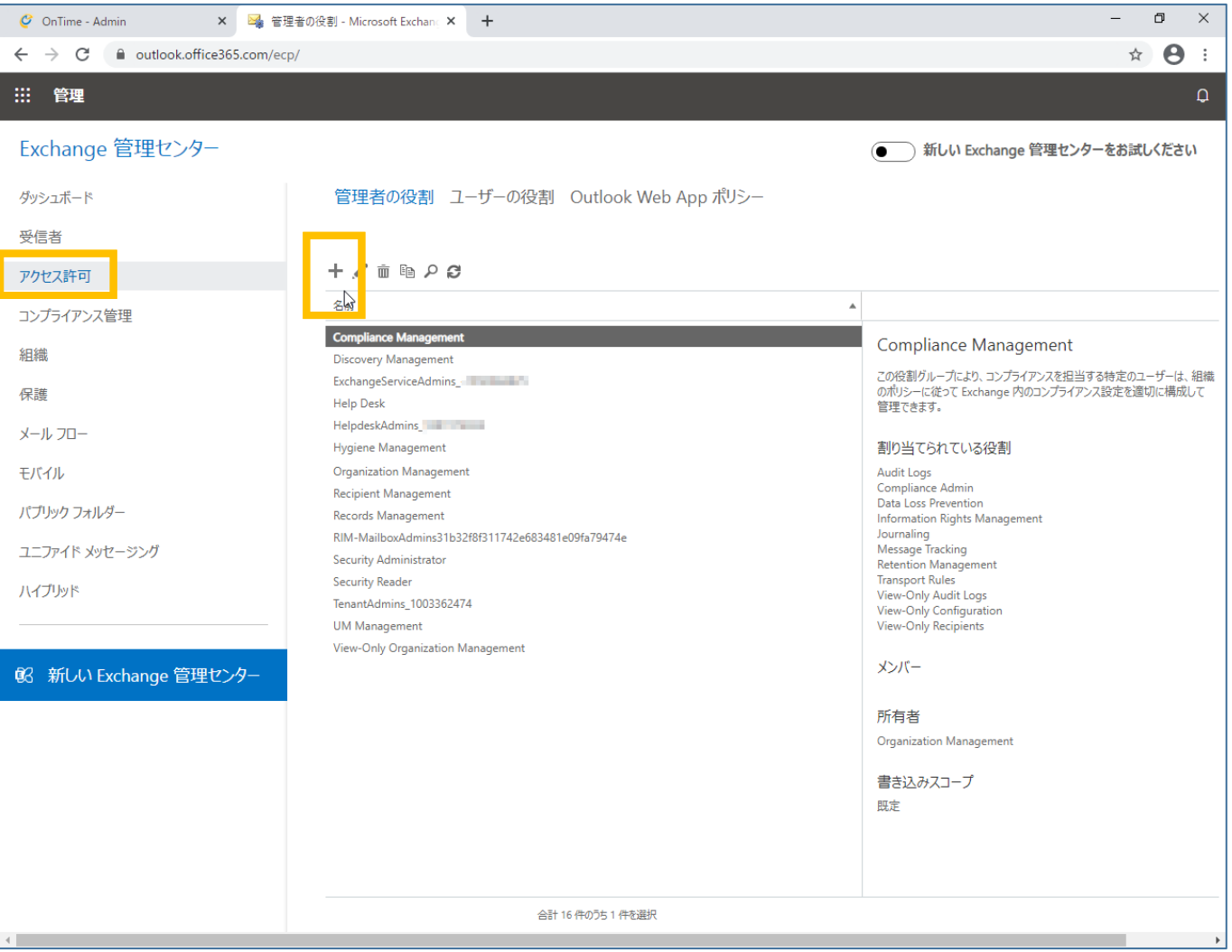
# Exchange側の設定を準備します

- 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/

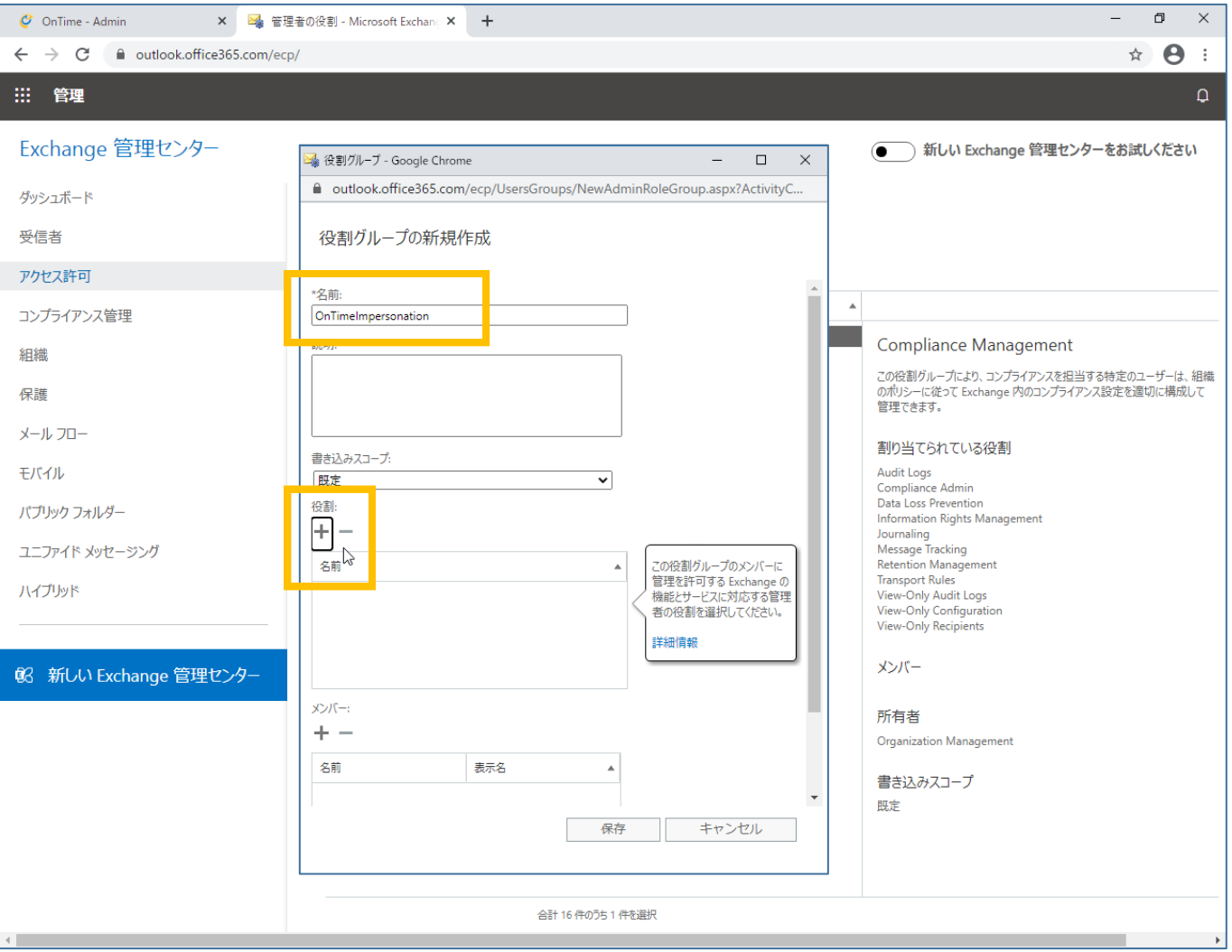
- 書き込みスコープを制限して特定のメールボックスに制限する方法について
  - テナント運用者とOnTime運用者が違う場合などで厳密に同期対象のメールボックスだけに接続の制限を掛けたい場合は、同期を司るユーザーに割り当てる役割「ApplicationImpersonation」指定時の「書き込みスコープ」を厳密に設定することで明確化が可能です。
  - ドメイン(テナント)の特定のグループのメールボックスだけに OnTime の利用制限ができますか？
    https://www3.ontimesuite.jp/makescope/

# Exchange管理センターを開く



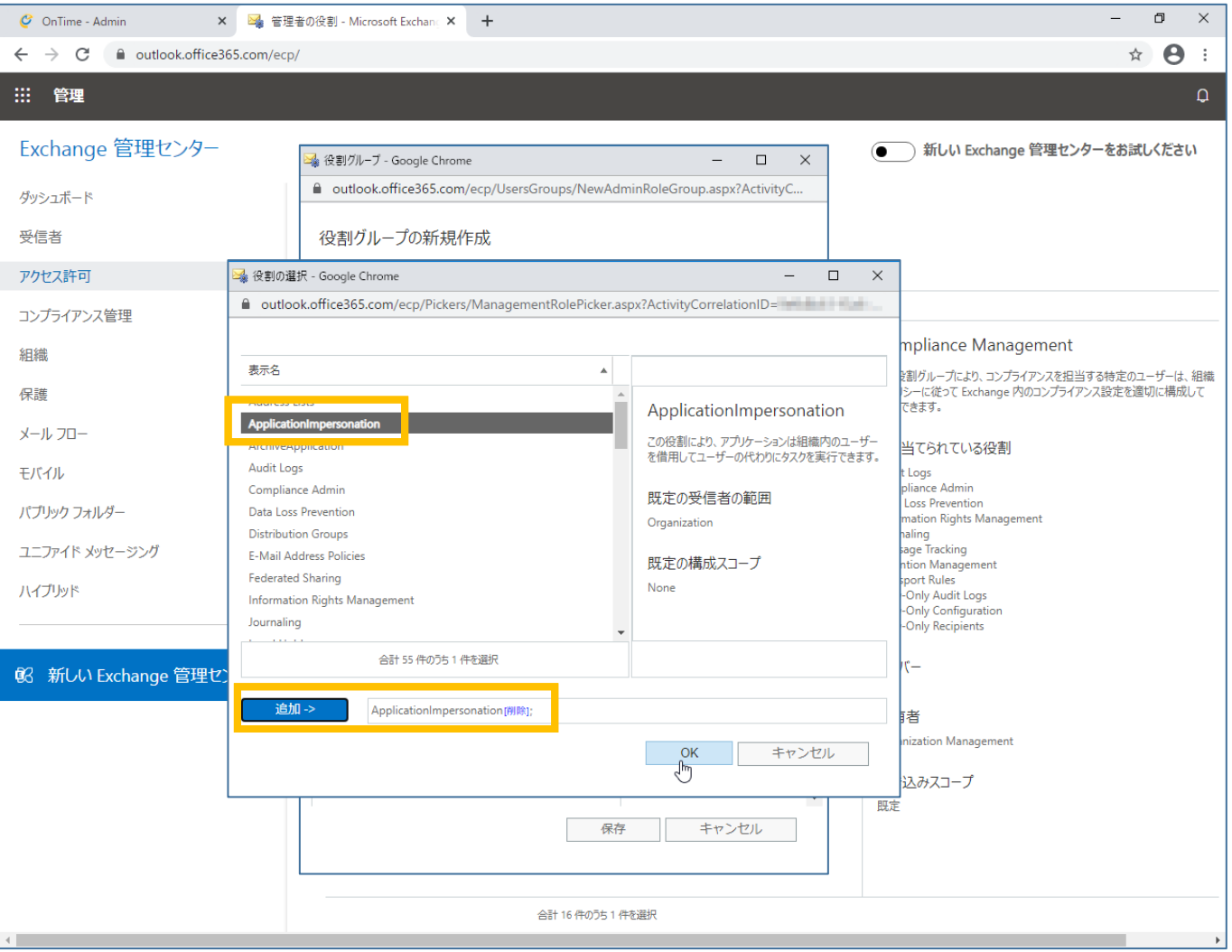

- Exchange管理センターを開きます。
- アクセス許可を開きます。
- 管理者の役割を開きます。
- ＋ボタンを押して管理者の役割を追加します。

# 管理者の役割の追加 1



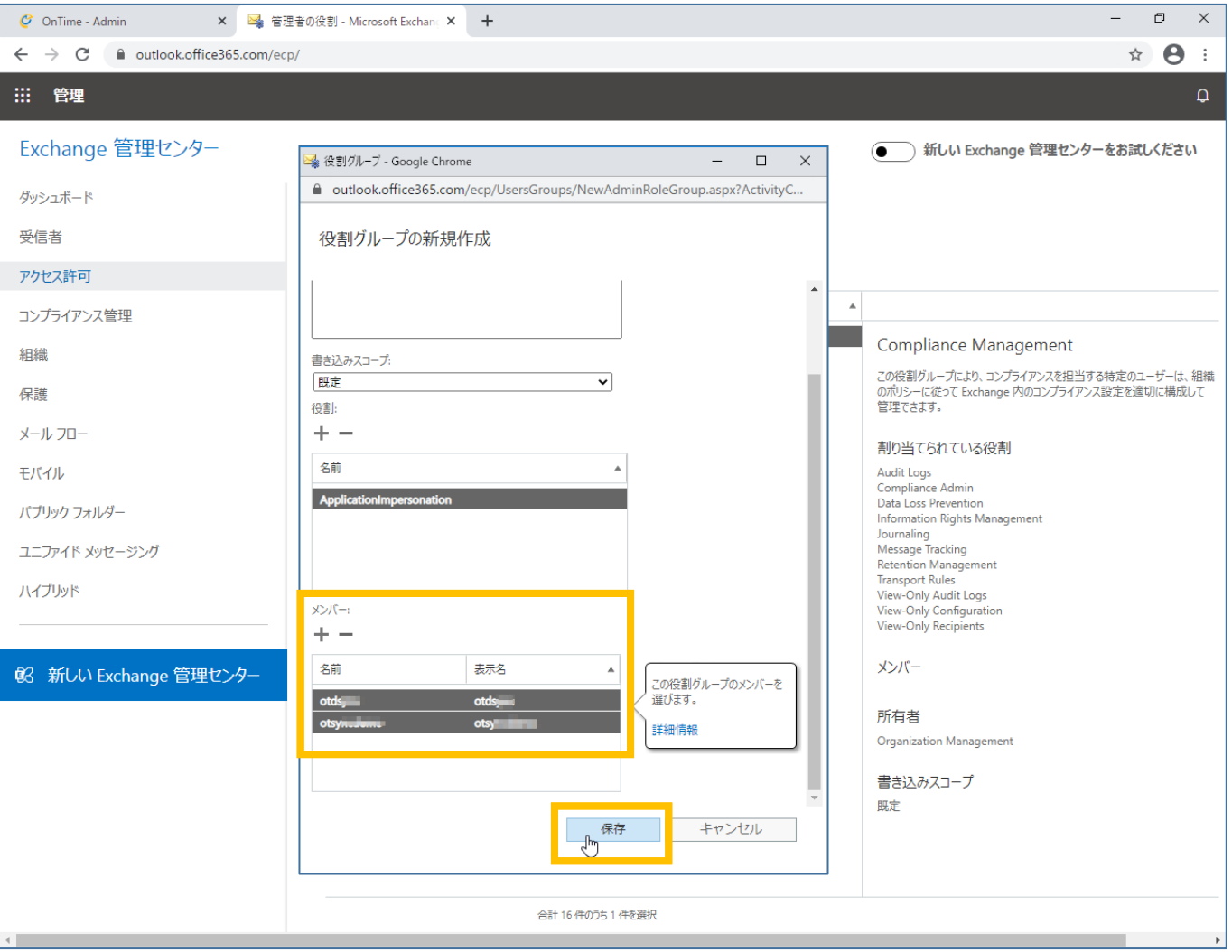

- 新しい役割を作成します。
- 名前には識別しやすい名前を指定してください。
- 役割の＋ボタンを押して役割を選択します。

# 管理者の役割の追加 2



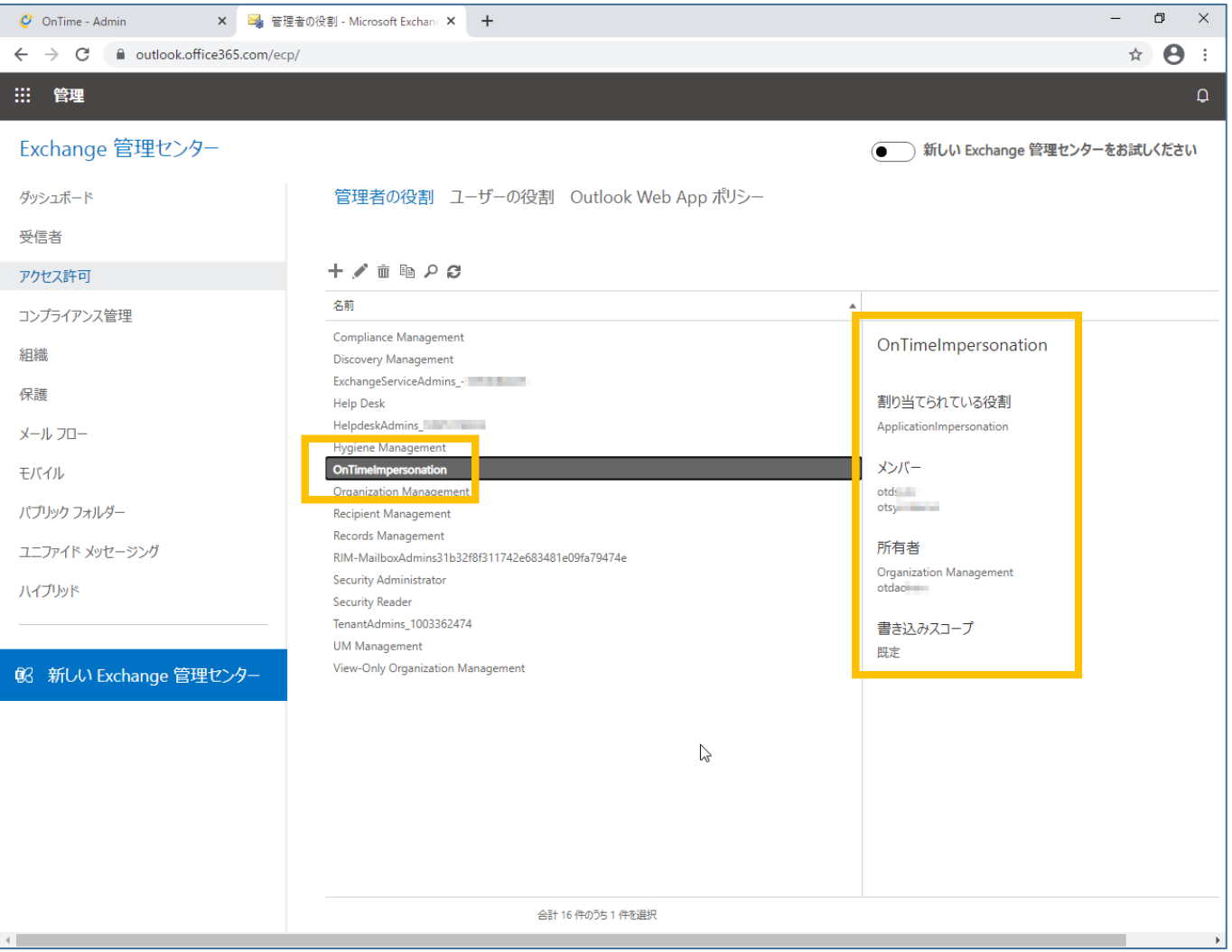

- ApplicationImpersonationを選択します。
- 「追加」を押して追加後に「OK」を押します。

# 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

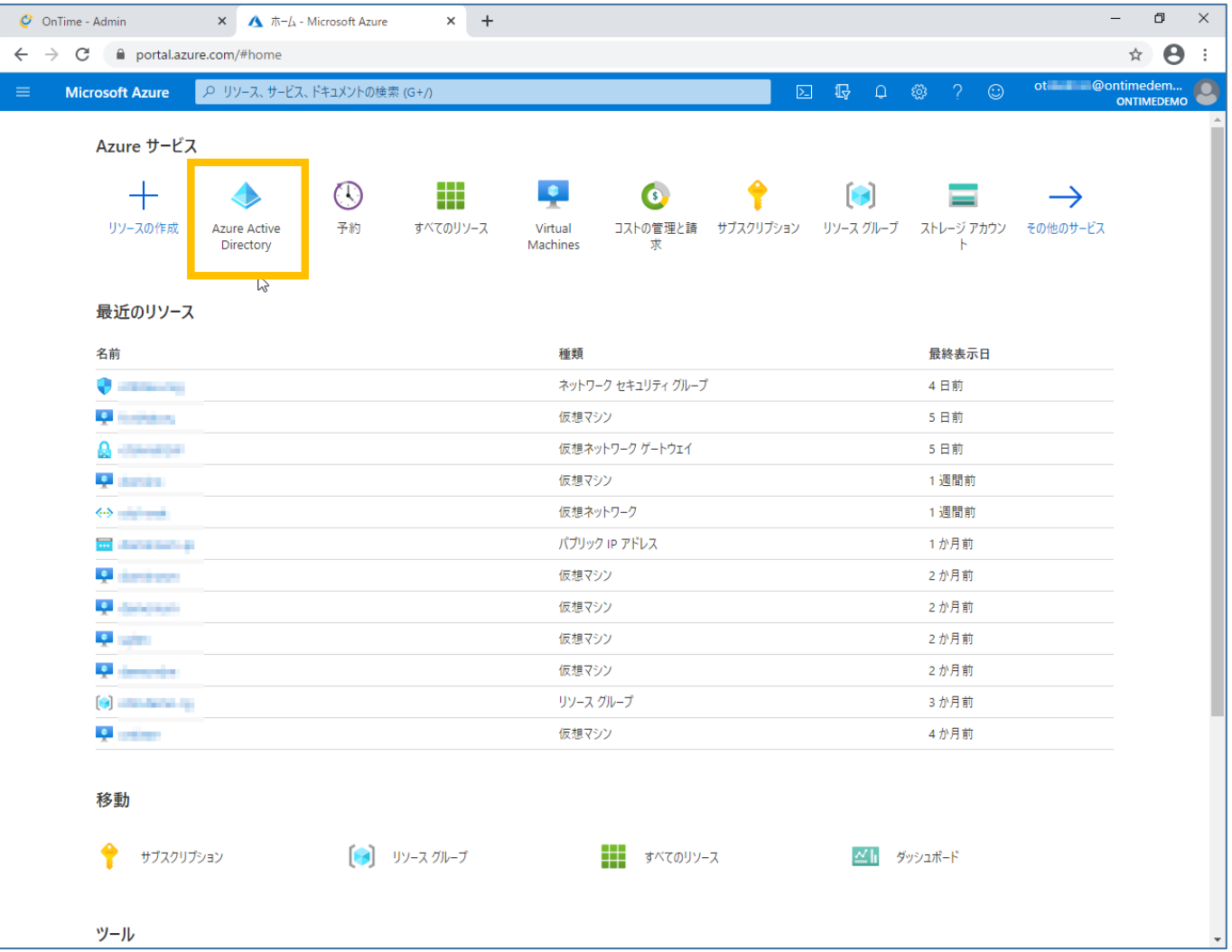
2021年2月に情報が追加されています。次頁参照

- 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

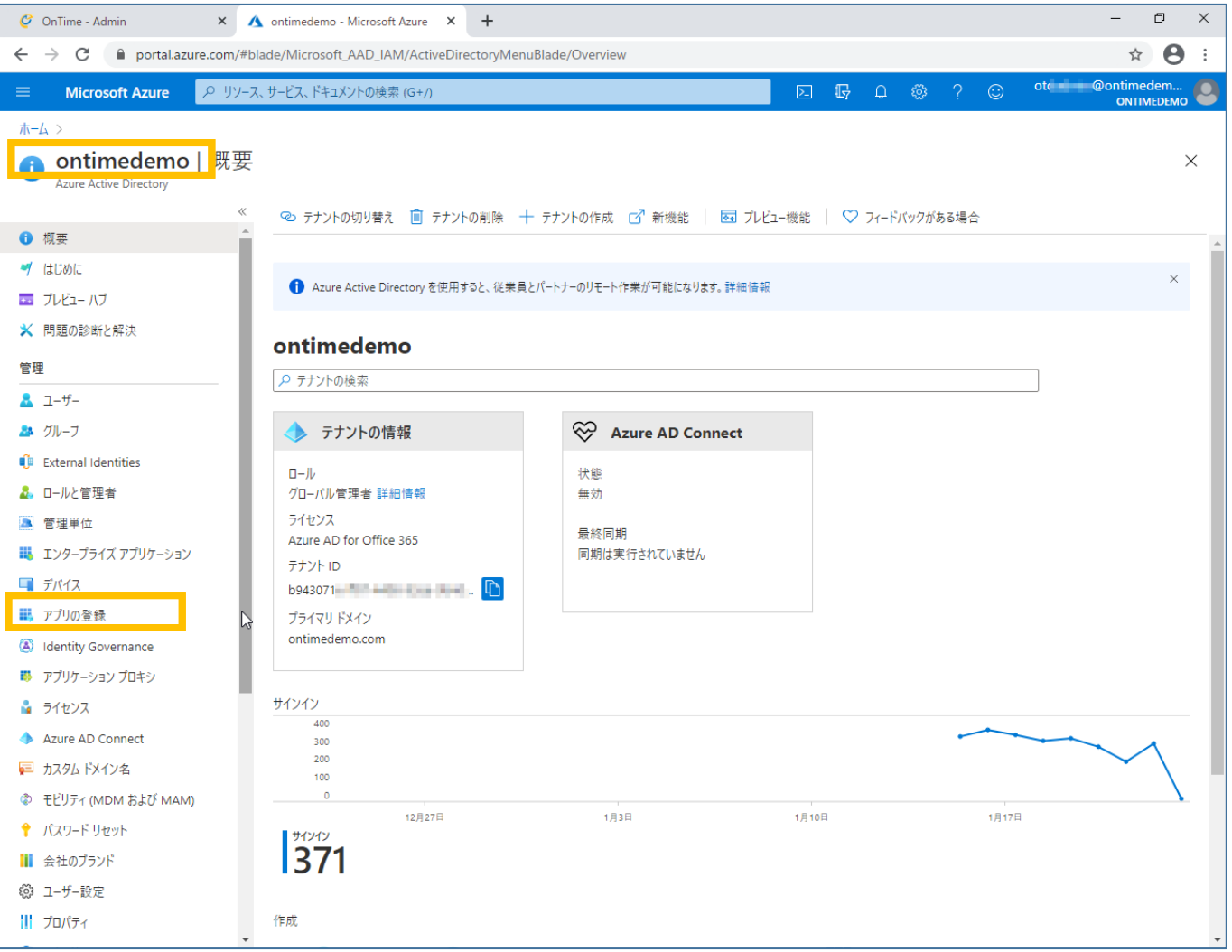
- 改めて案内するまで、テナントが基本認証を利用している場合は無効にしない。また無効にするまで遅くとも12ヶ月前には案内する。(Microsoft Exchange Team Blog 2021年02月04日)
  https://techcommunity.microsoft.com/t5/exchange-team-blog/basic-authentication-and-exchange-online-february-2021-update/ba-p/2111904
  - --抜粋--
  - 改めて案内するまで、テナントが基本認証を利用している場合は無効にしません。また無効にする際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っ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 Direcotry を開きます。

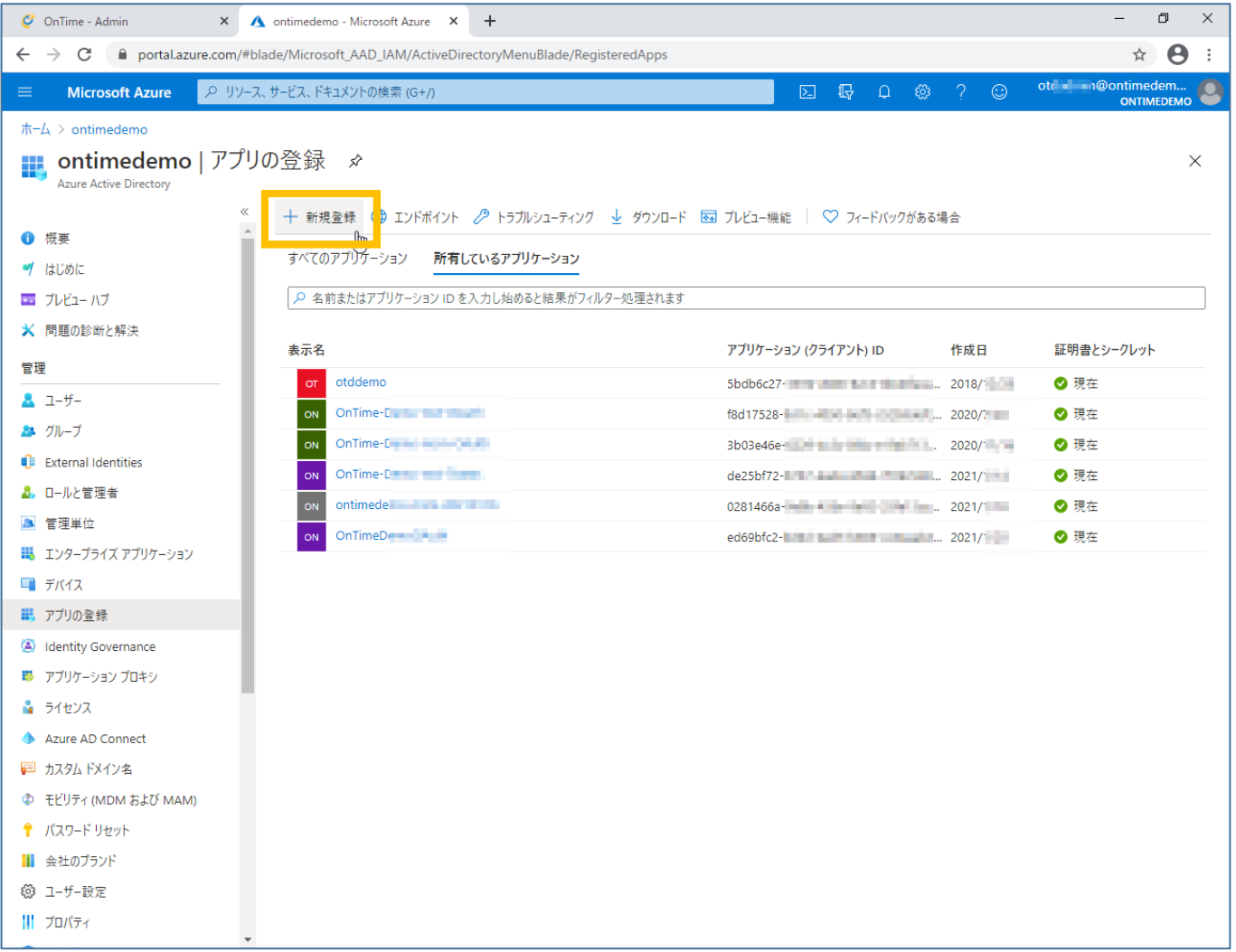
# アプリの登録 2




- 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

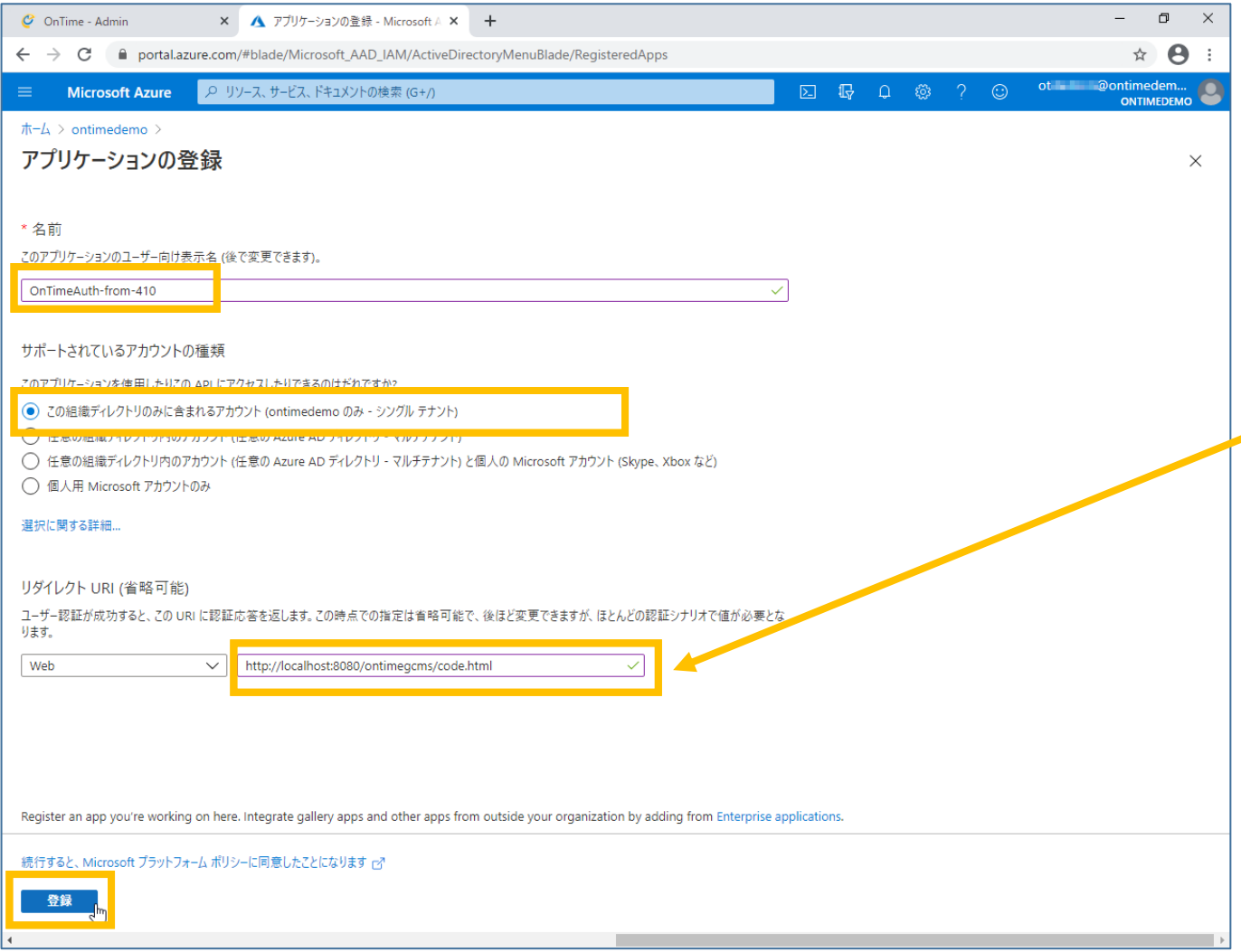



- 「アプリの登録」で「新規登録」をクリックします。

- 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

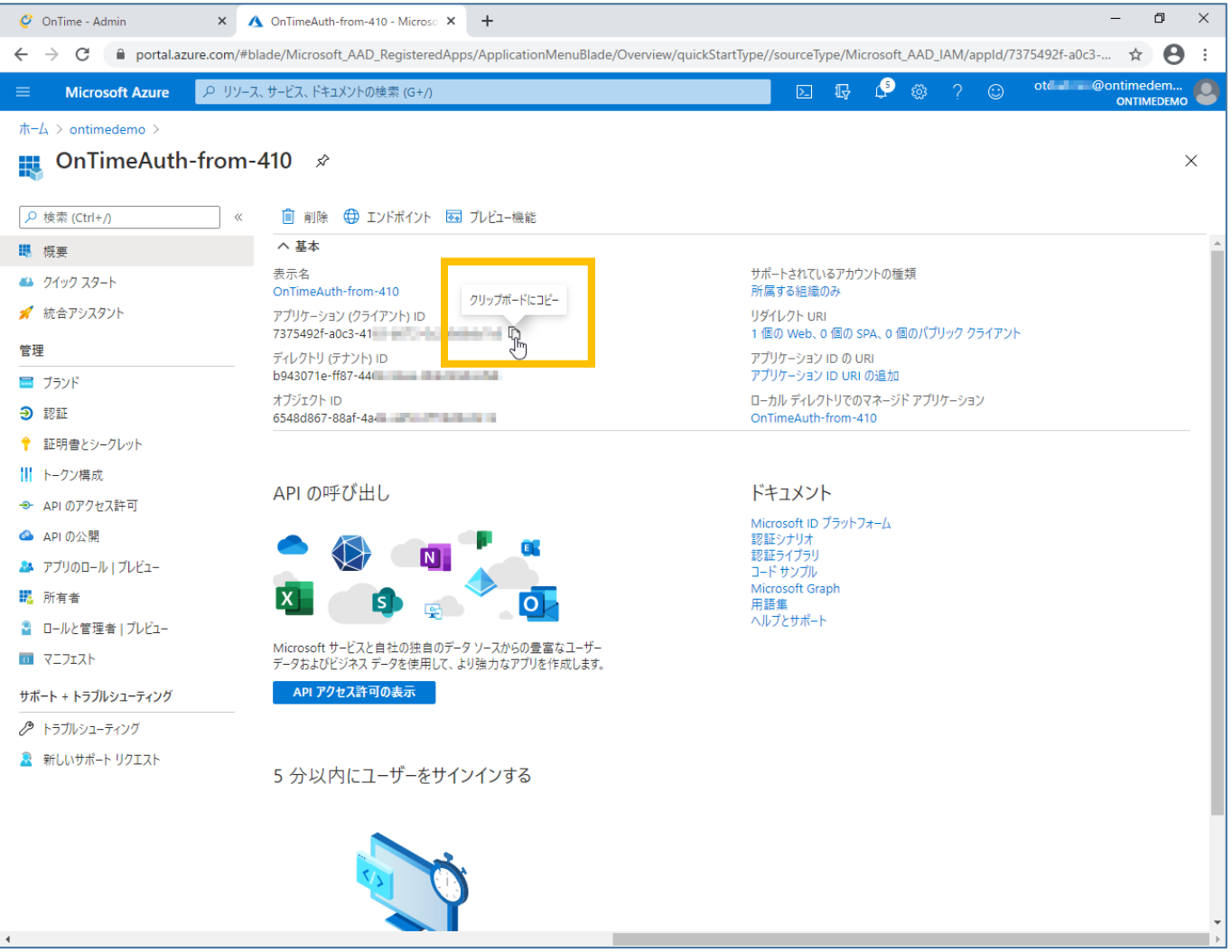



- 「名前」はエンドユーザーには表示されない名前なので管理上識別しやすい名前を入力します。
- 「サポートされているアカウントの種類」は「この組織ディレクトリのみに含まれるアカウント」を選択します。

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

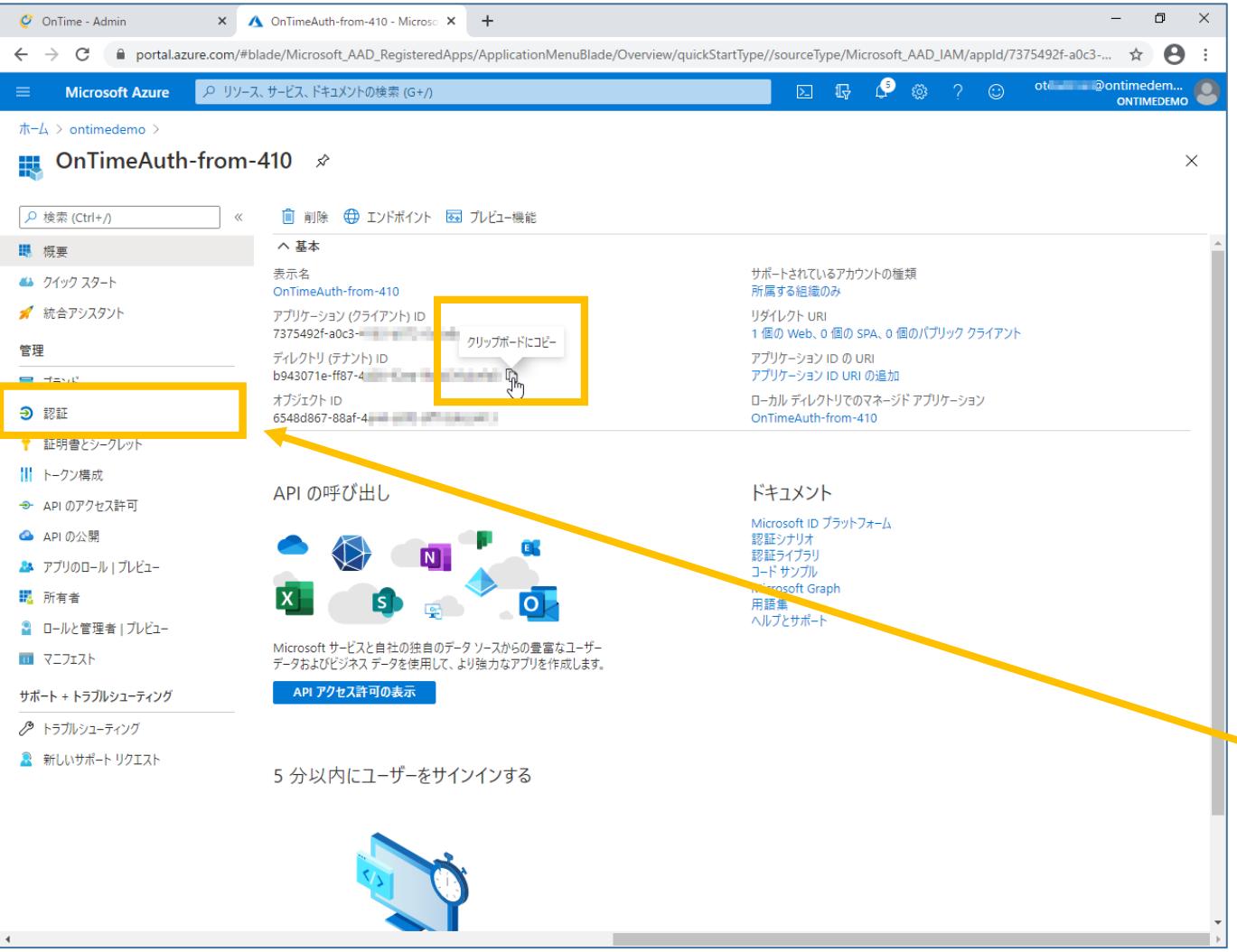
- 最後に「登録」をクリックします。

# アプリの各IDの設定 1




- 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。

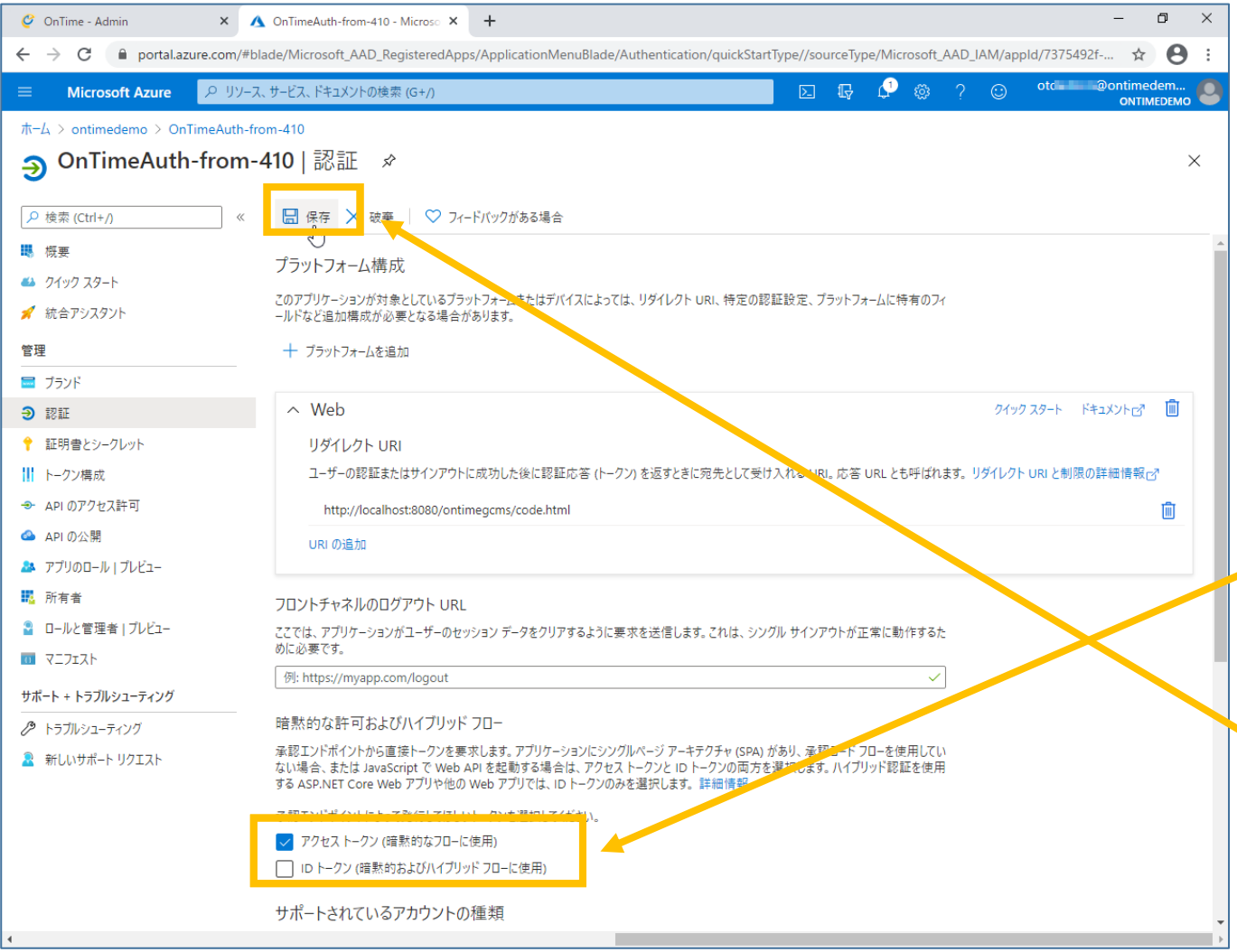
# アプリの各IDの設定 2




- 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

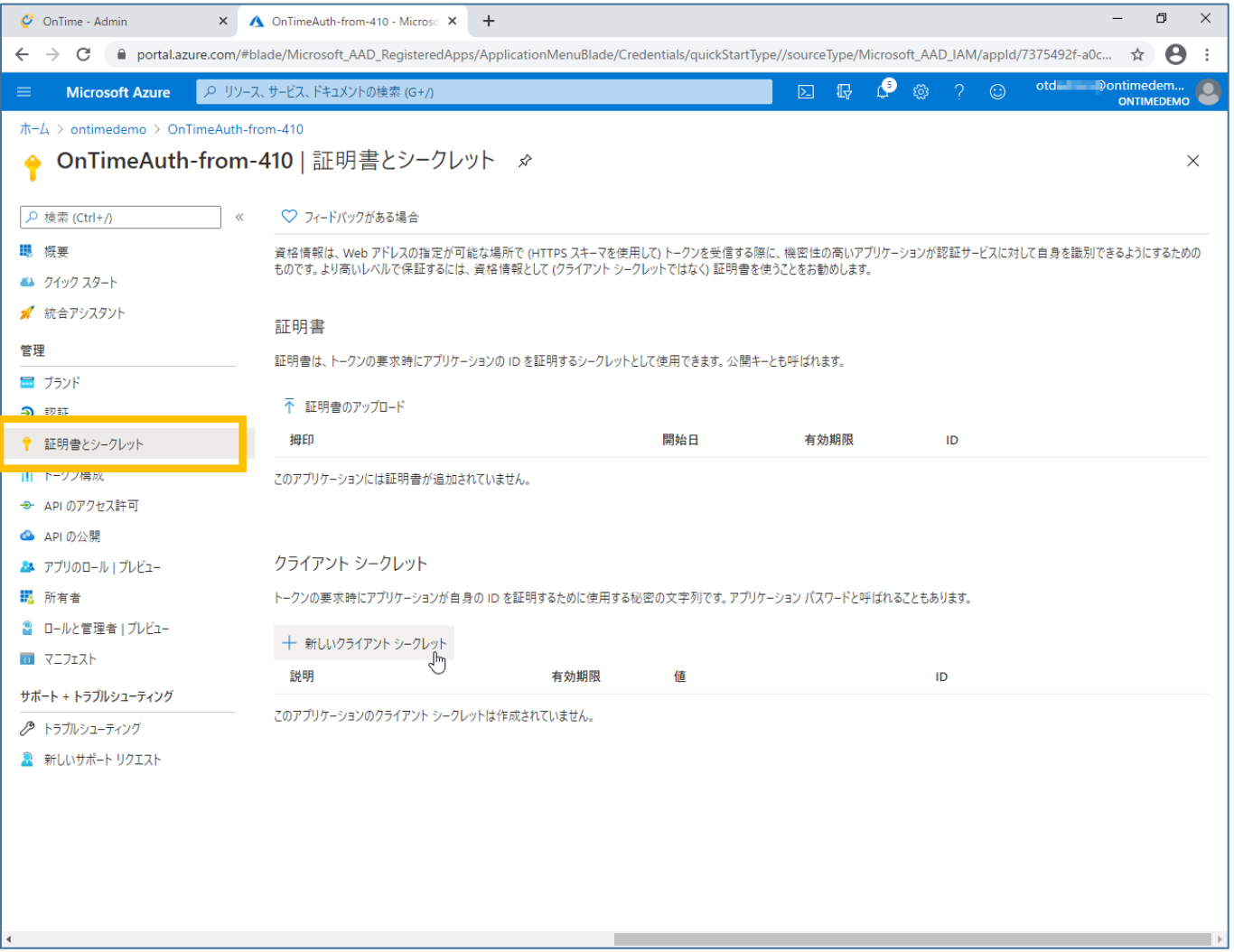



- 発行するトークンを選択します。

アクセストークンにチェックをつけます。

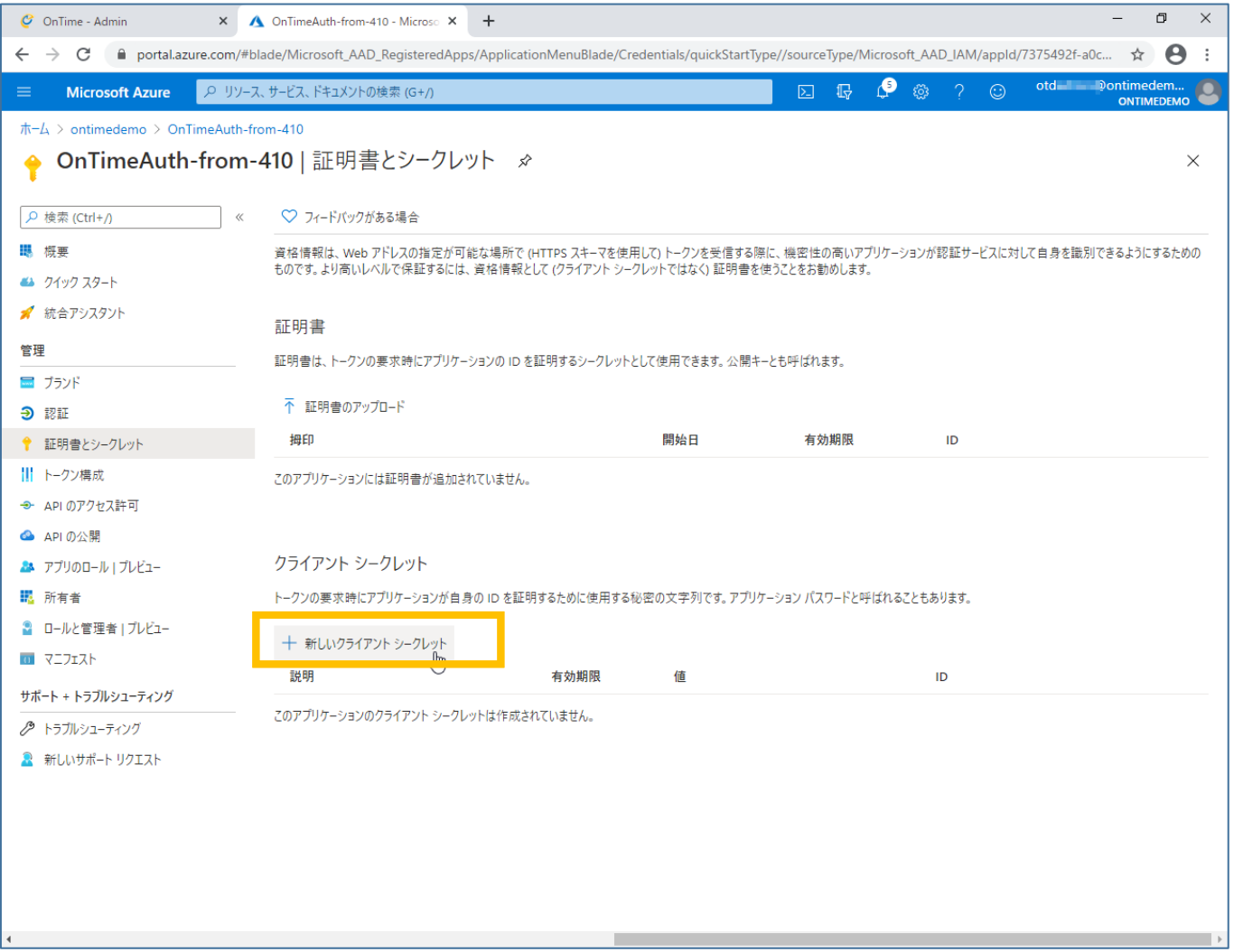
「保存」をクリックします。

# クライアントシークレットの設定 1



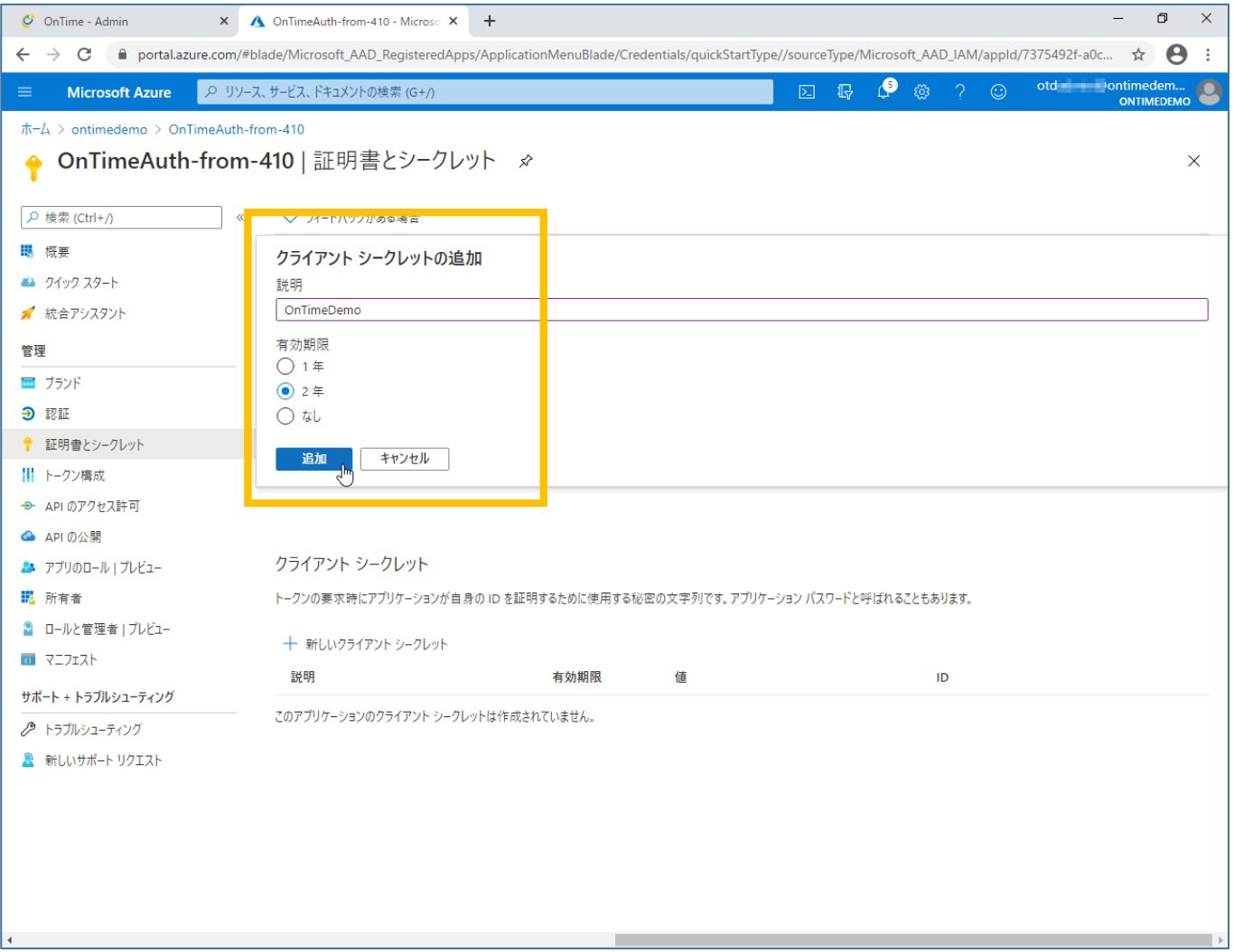

- 「証明書とシークレット」タブに移動します。

# クライアントシークレットの設定 2



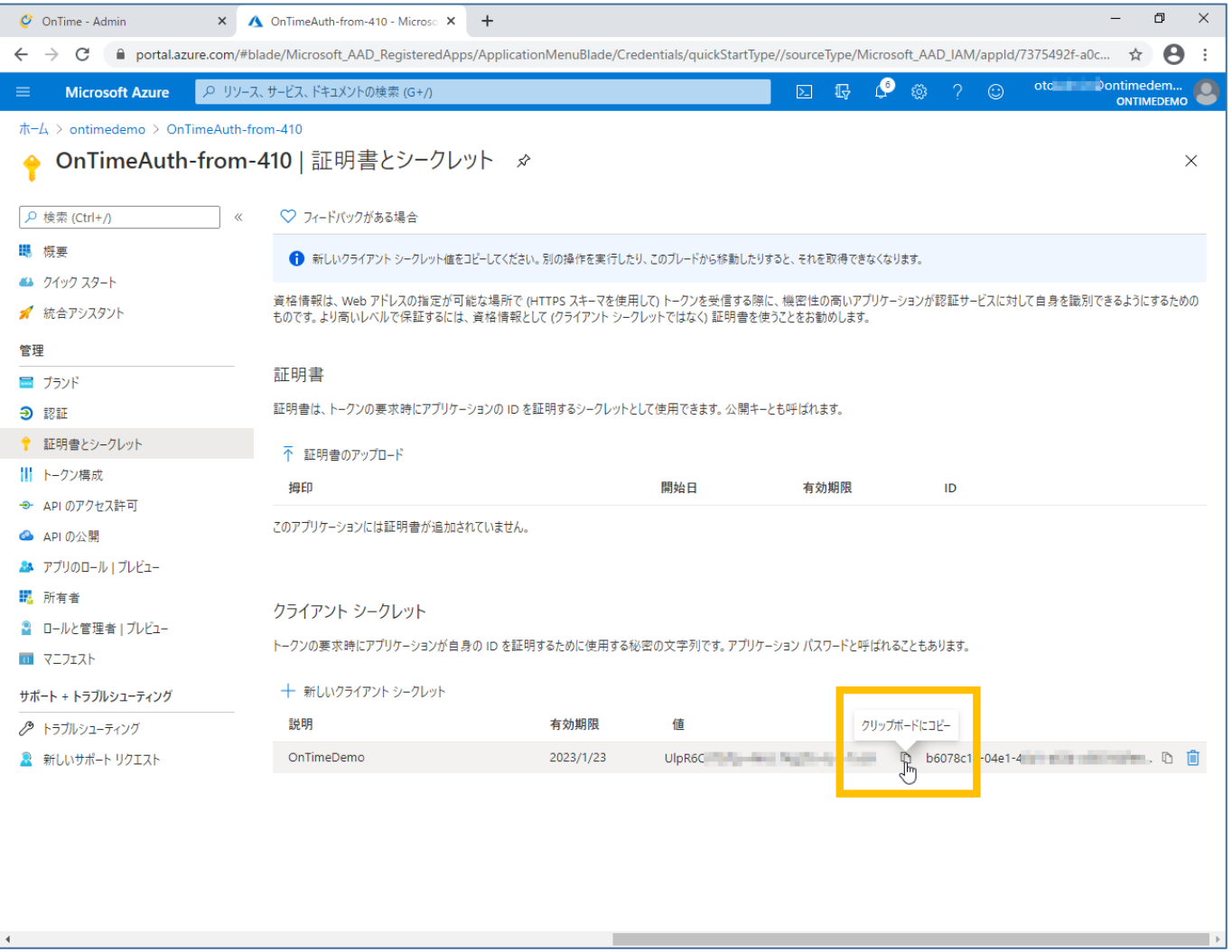

- こちらではOnTimeサーバーがアクセスする際に自身のIDを証明する為の「クライアントシークレット」を作成します。
- 「クライアントシークレット」は「アプリケーションパスワード」と呼ばれることもあります。
- 「新しいクライアントシークレット」をクリックします。

# 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。

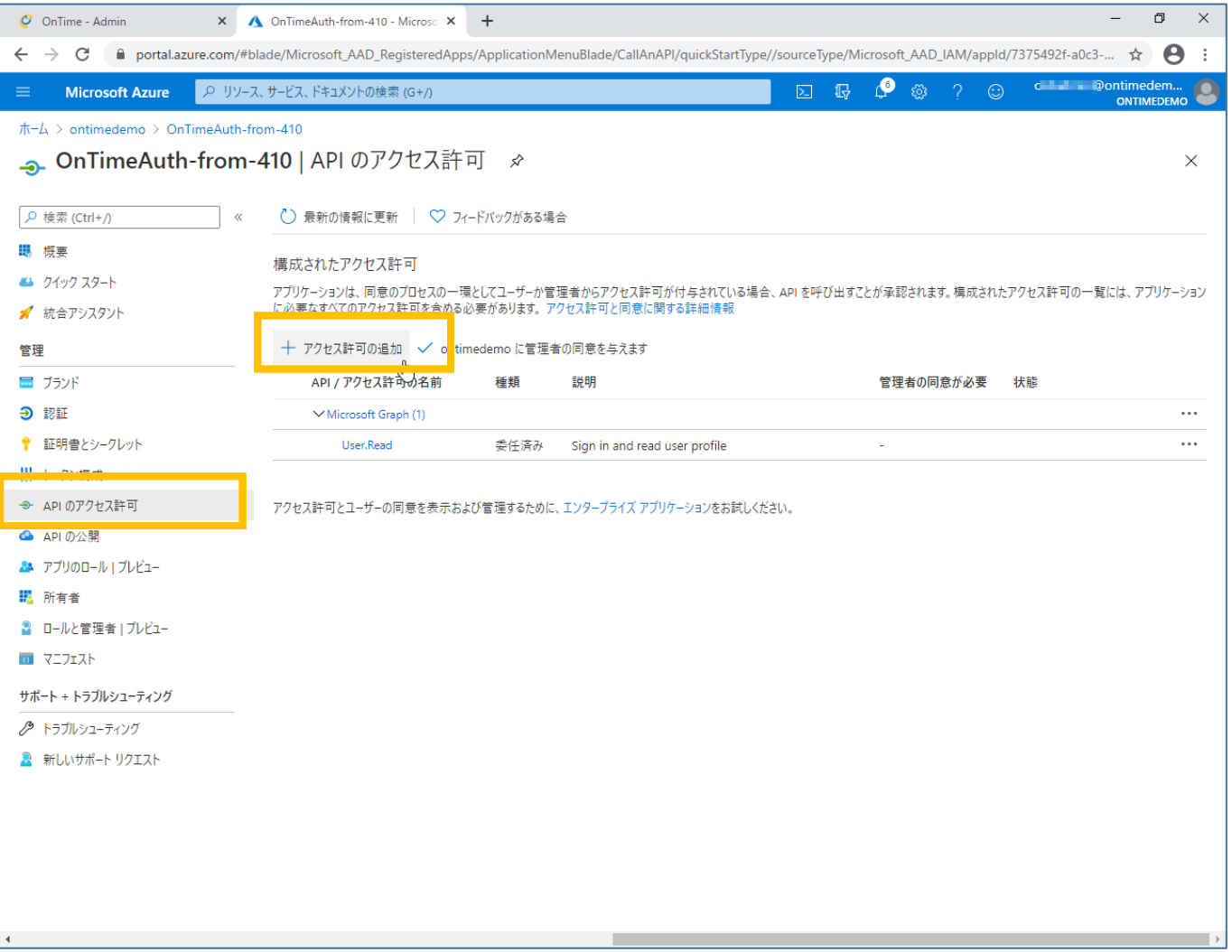
# クライアントシークレットの設定 4




- 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。

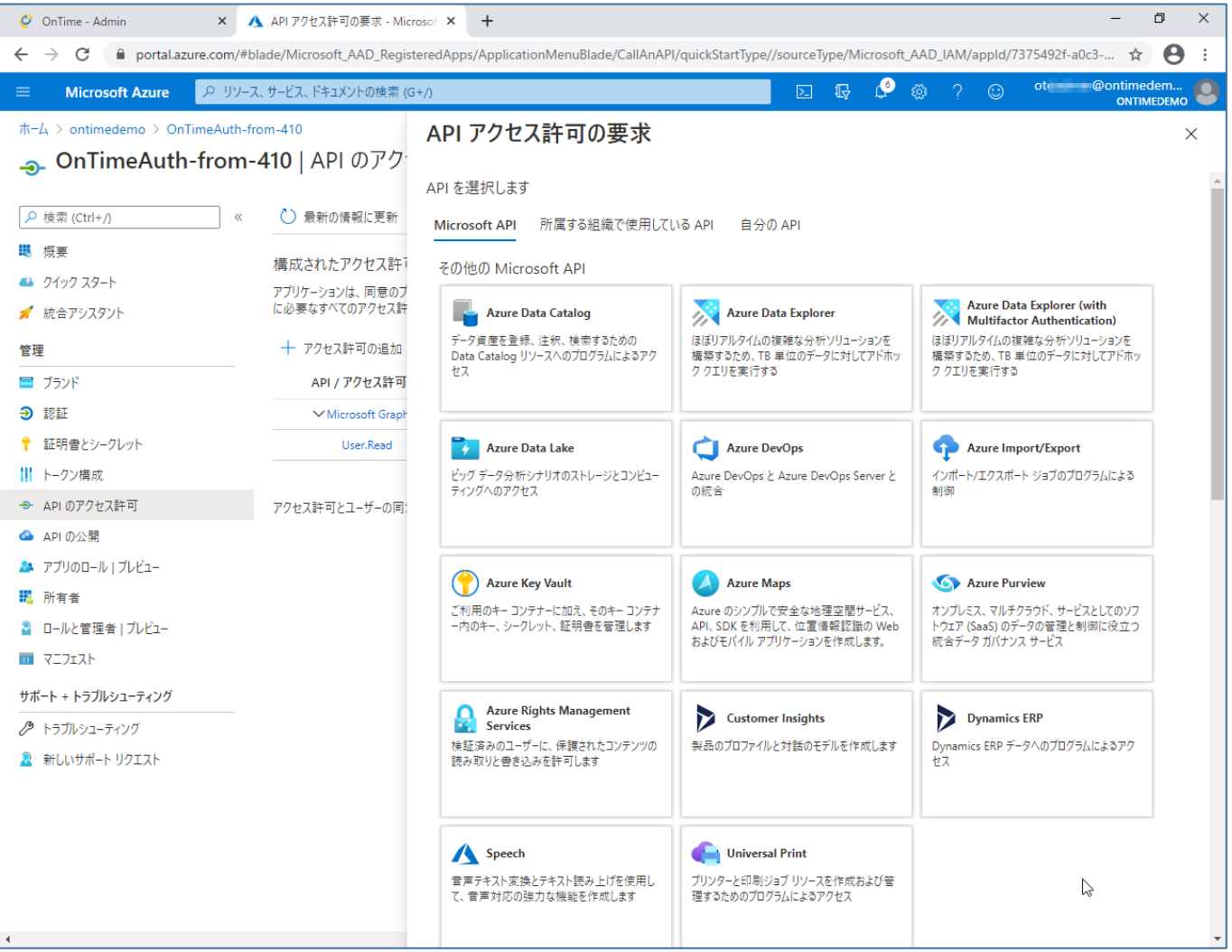
- 注意
「値」はこのタイミングでコピーしないと二度と取得できないのでご注意ください。

# APIのアクセス許可 1



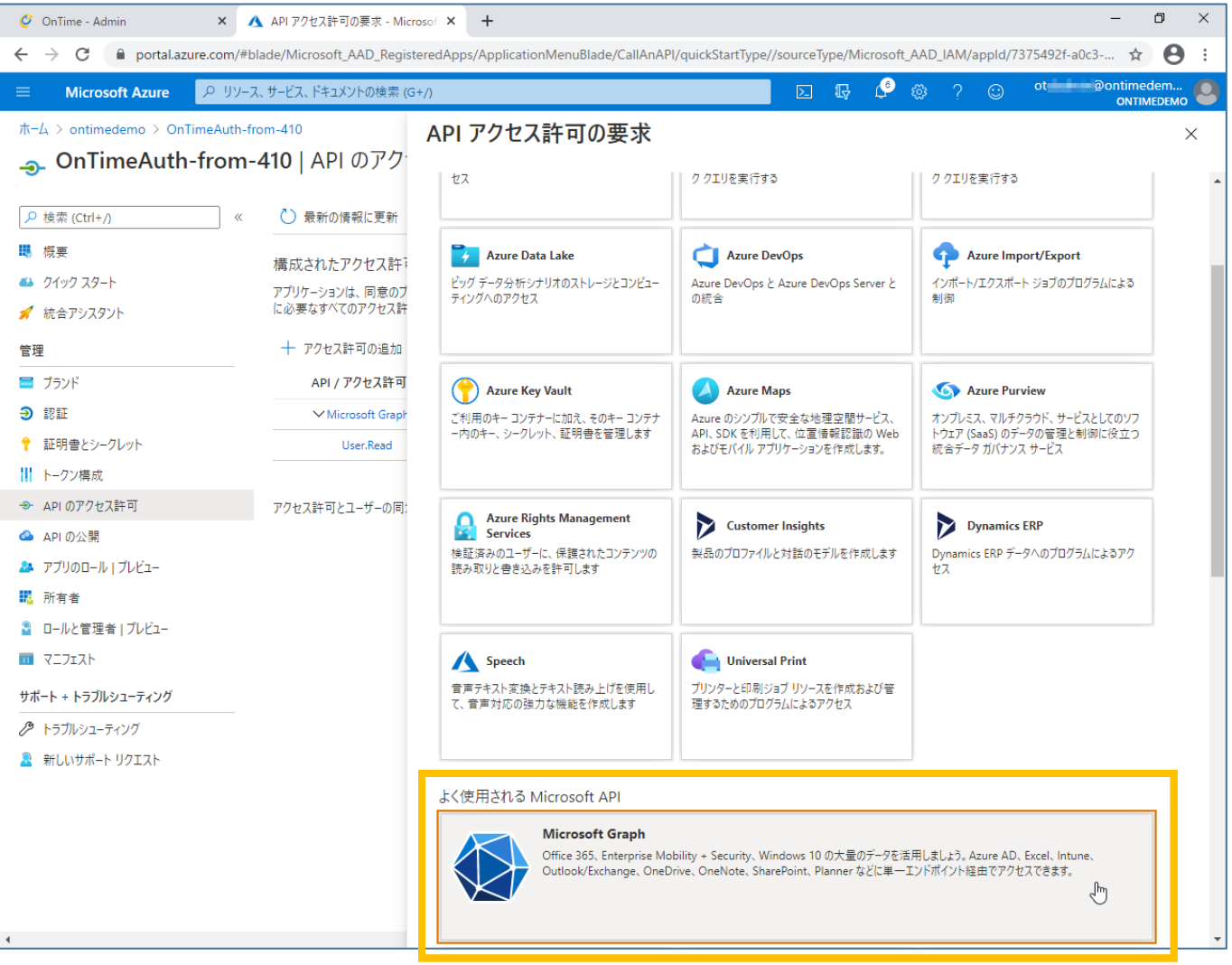

- 「APIのアクセス許可」タブに移動します。
- こちらではOnTimeサーバーが Graph API でアクセスする内容を定義します。
- 「アクセス許可の追加」ボタンをクリックします。

# APIのアクセス許可 2



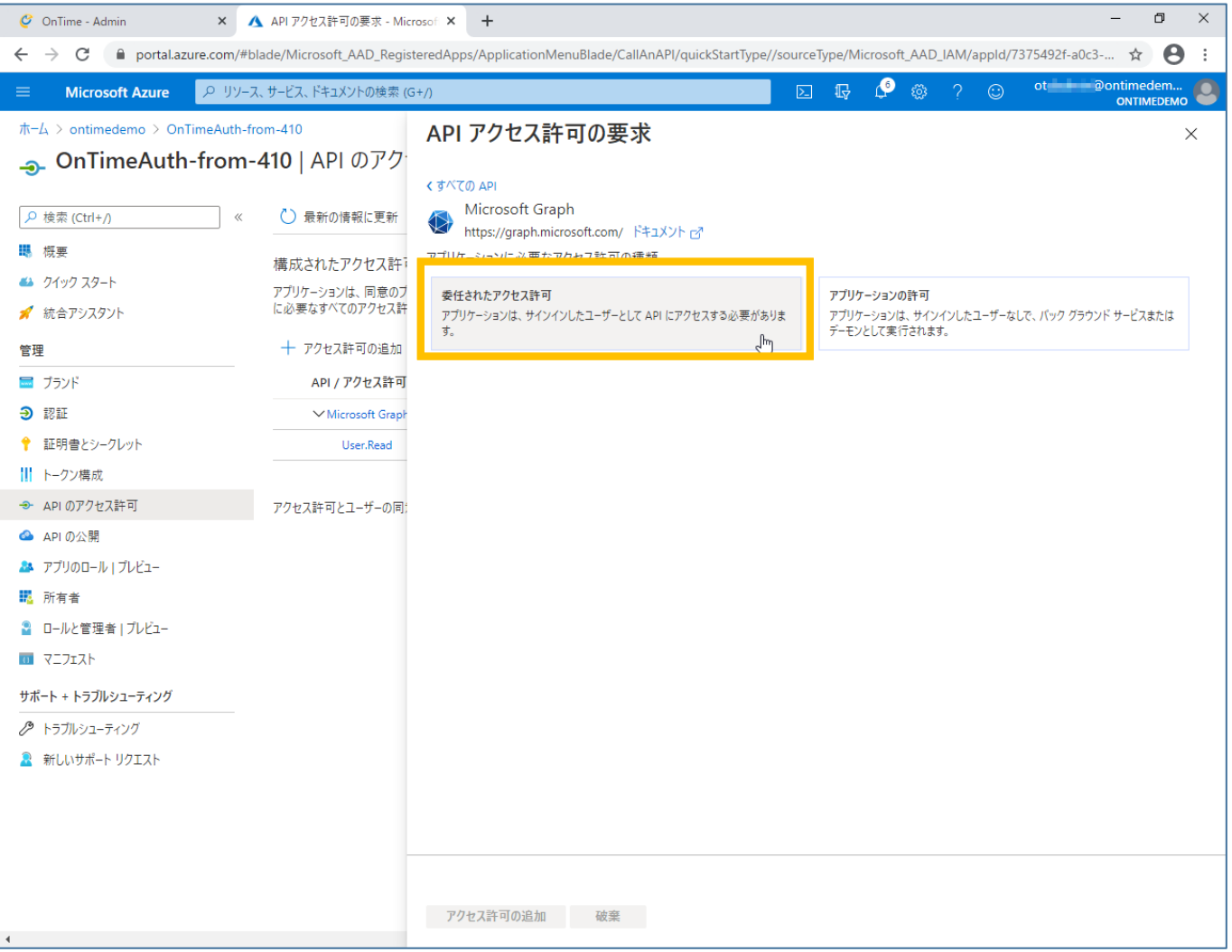

- 「APIアクセス許可の要求」ページが開きます。
- スクロールして「Microsoft Graph」を見つけます。

# APIのアクセス許可 3



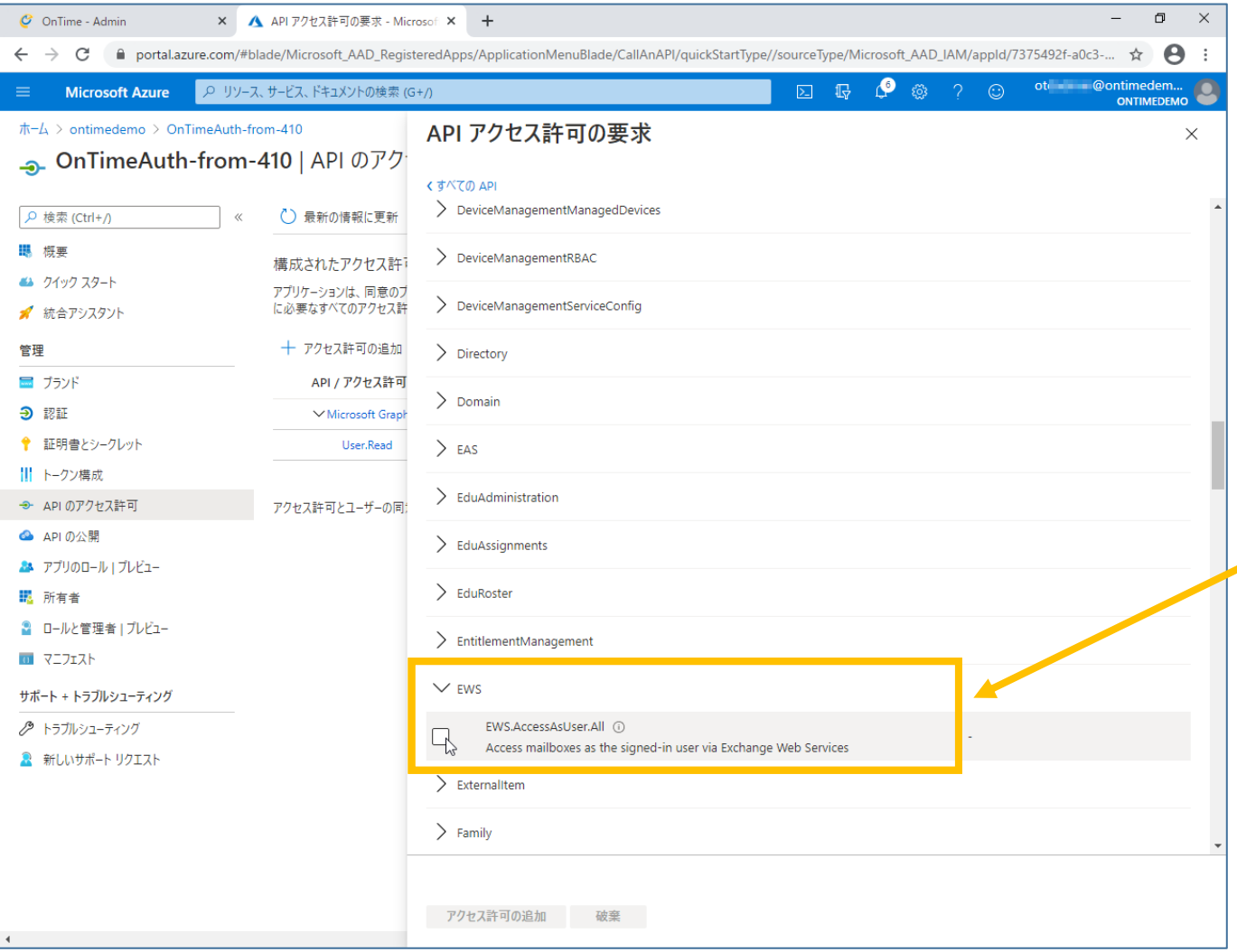

- 「Microsoft Graph」をクリックします。

# 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。

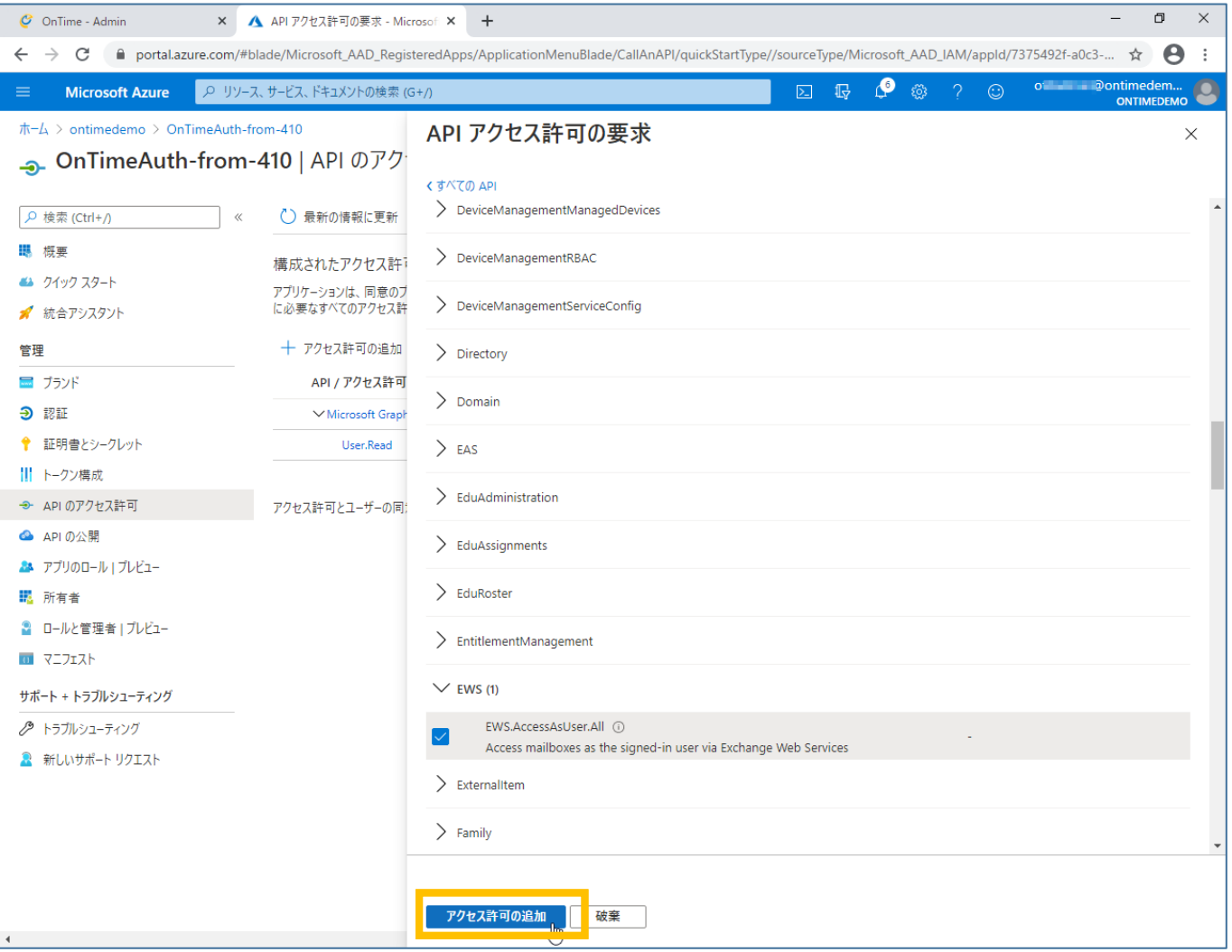
# APIのアクセス許可 5




- 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。

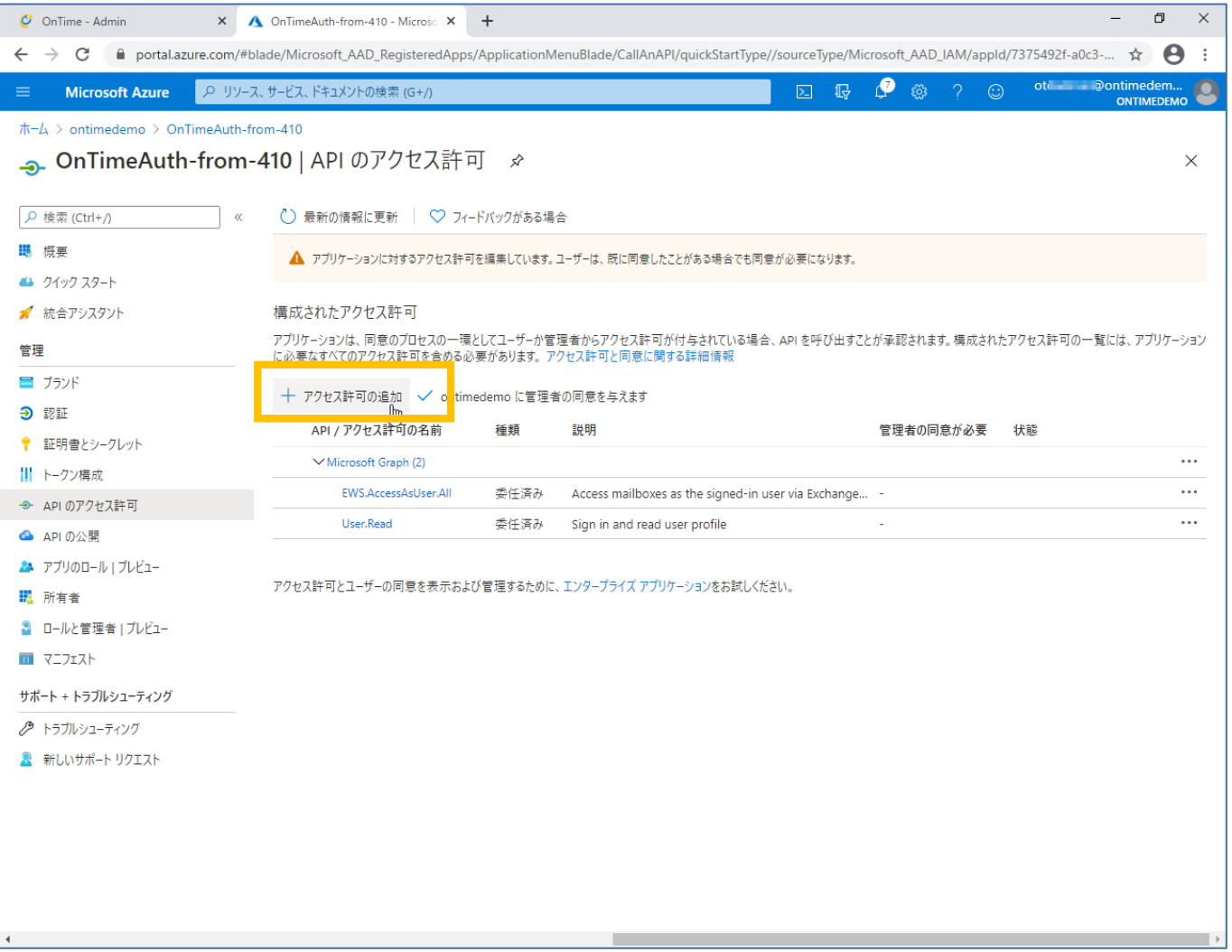
「EWS.AccessAsUser.All」をチェックします。

# APIのアクセス許可 6



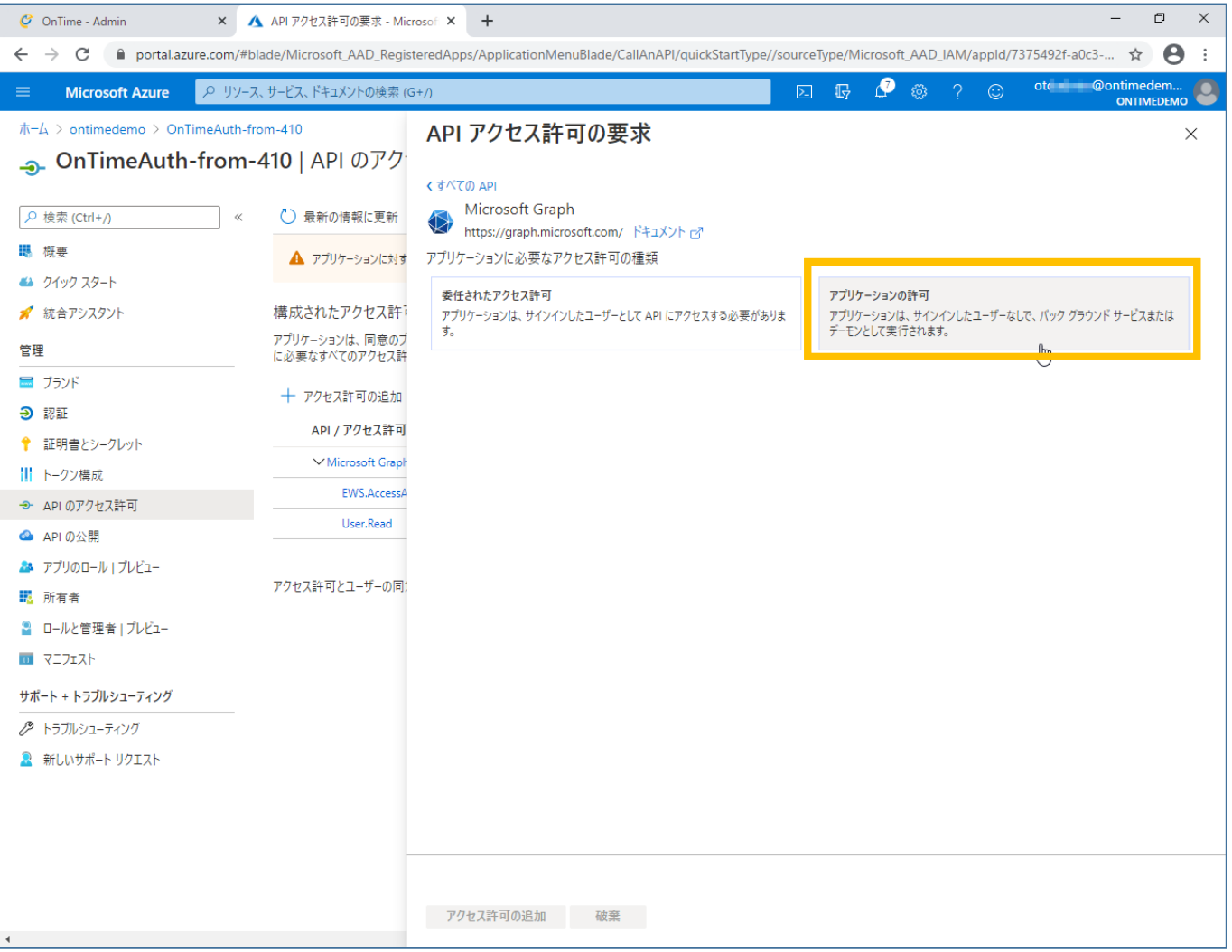

- 「アクセス許可の追加」をクリックします。

# APIのアクセス許可 7



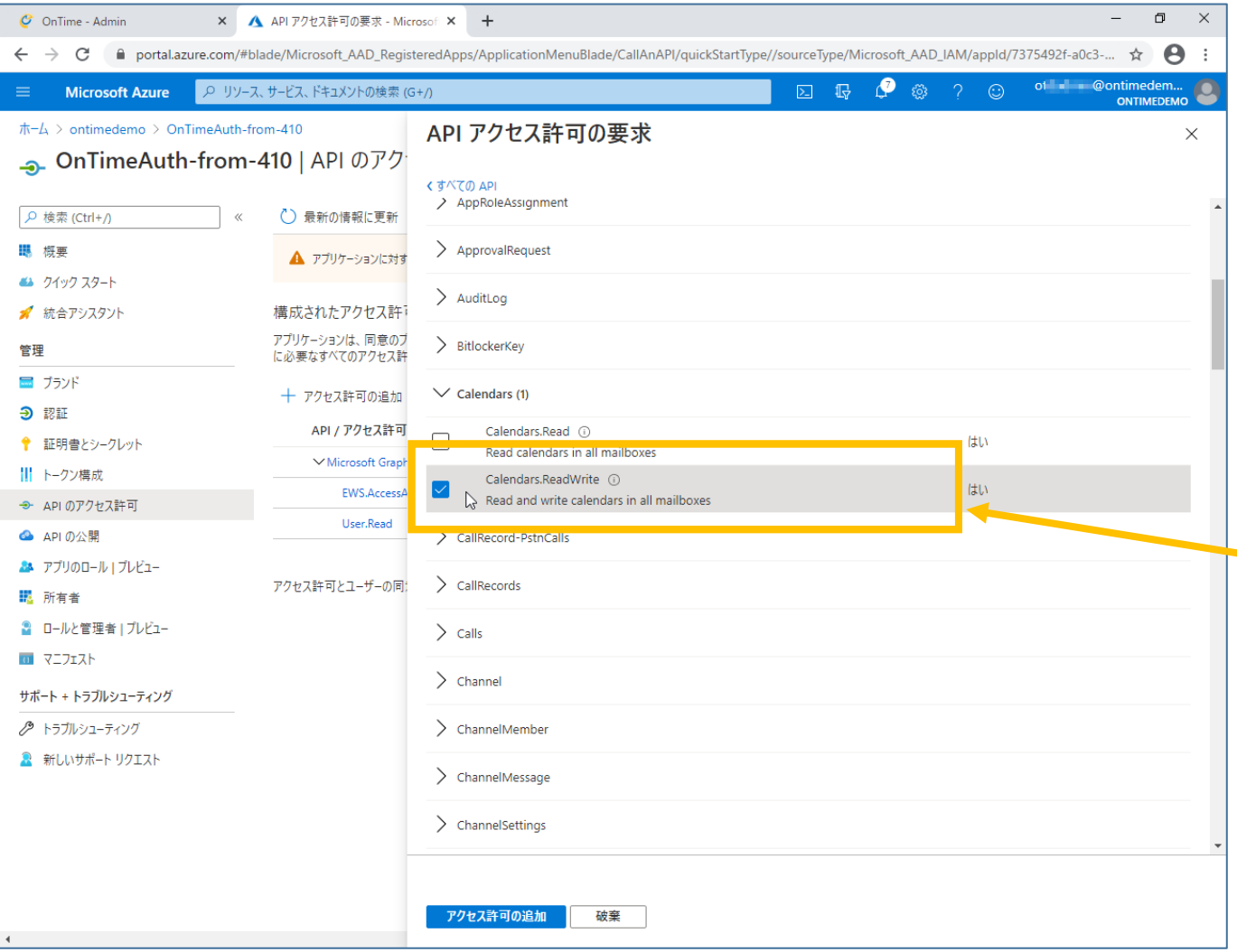

- 画面が戻ったら再度「アクセス許可の追加」ボタンをクリックします。

# APIのアクセス許可 8




- 今度は「アプリケーションの許可」をクリックします。

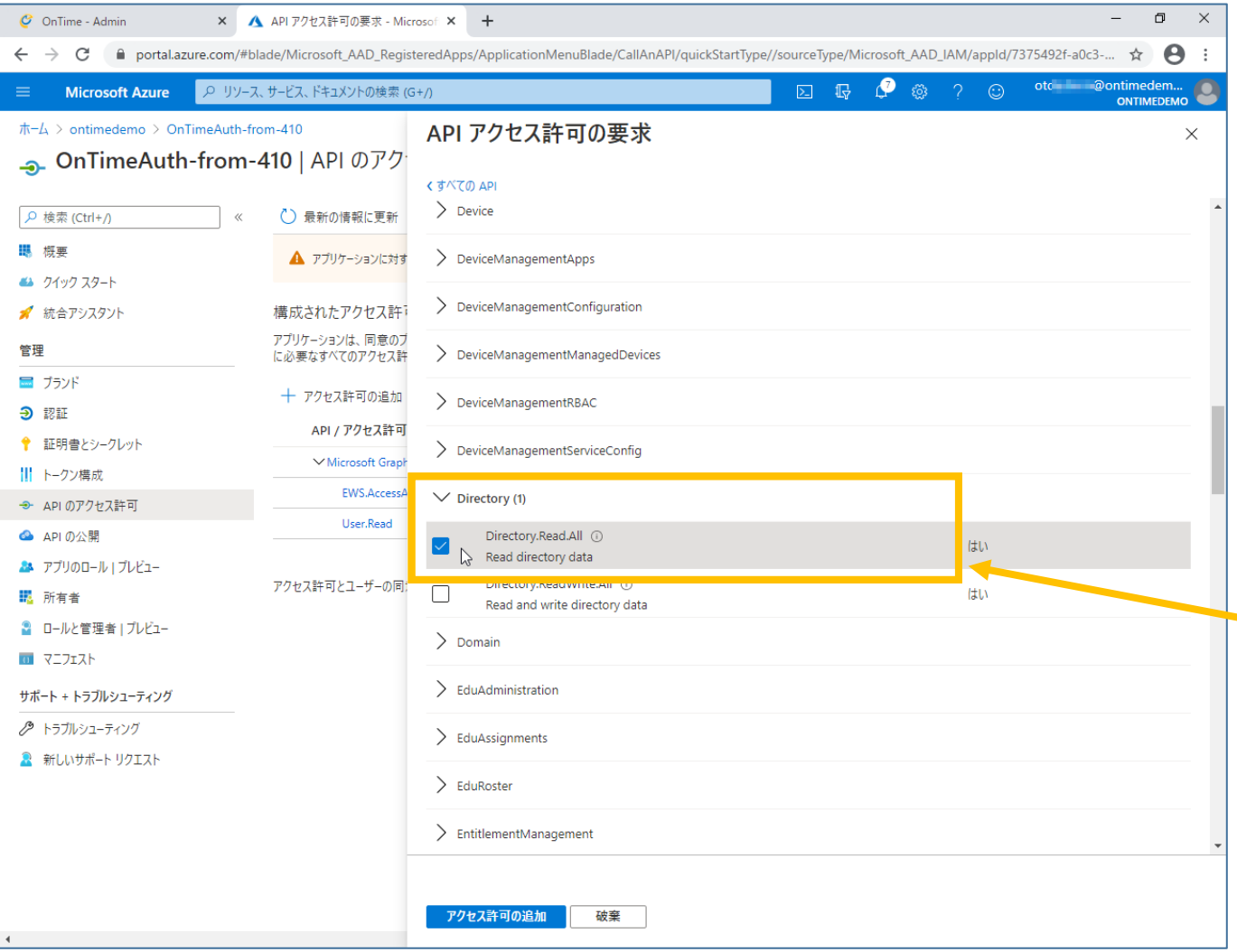
# APIのアクセス許可 9




- 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。

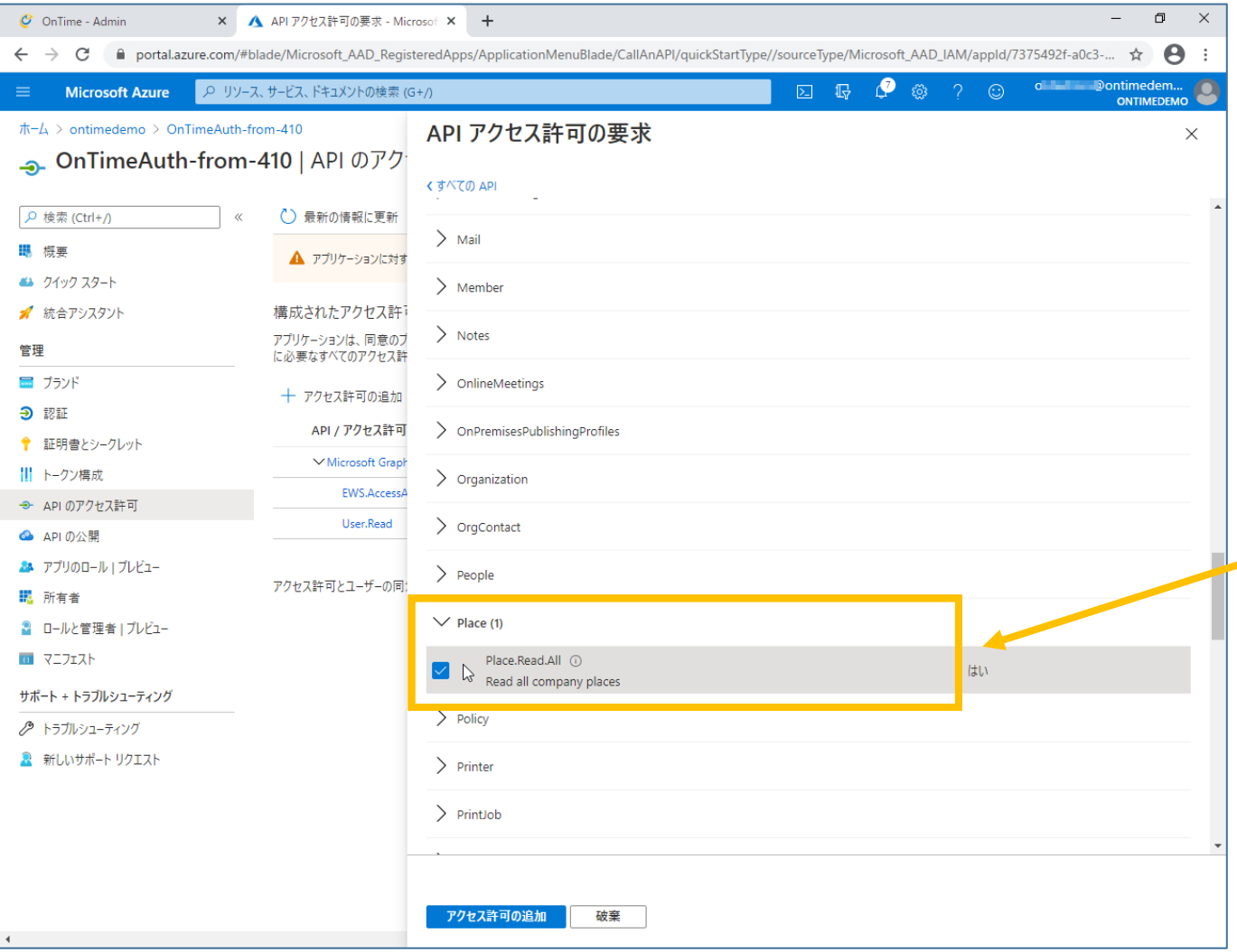
# APIのアクセス許可１０




- 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。

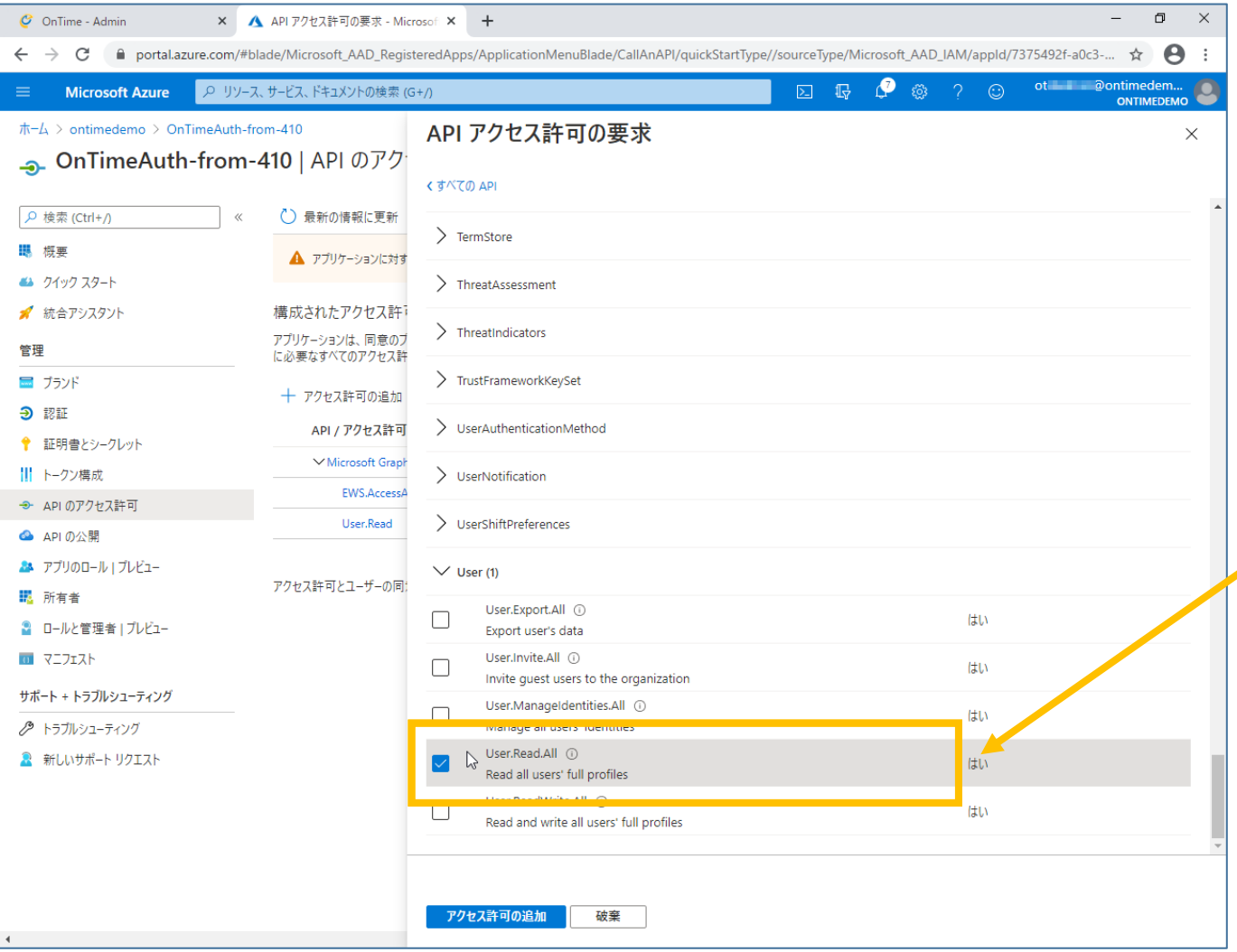
# APIのアクセス許可１１




- 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。

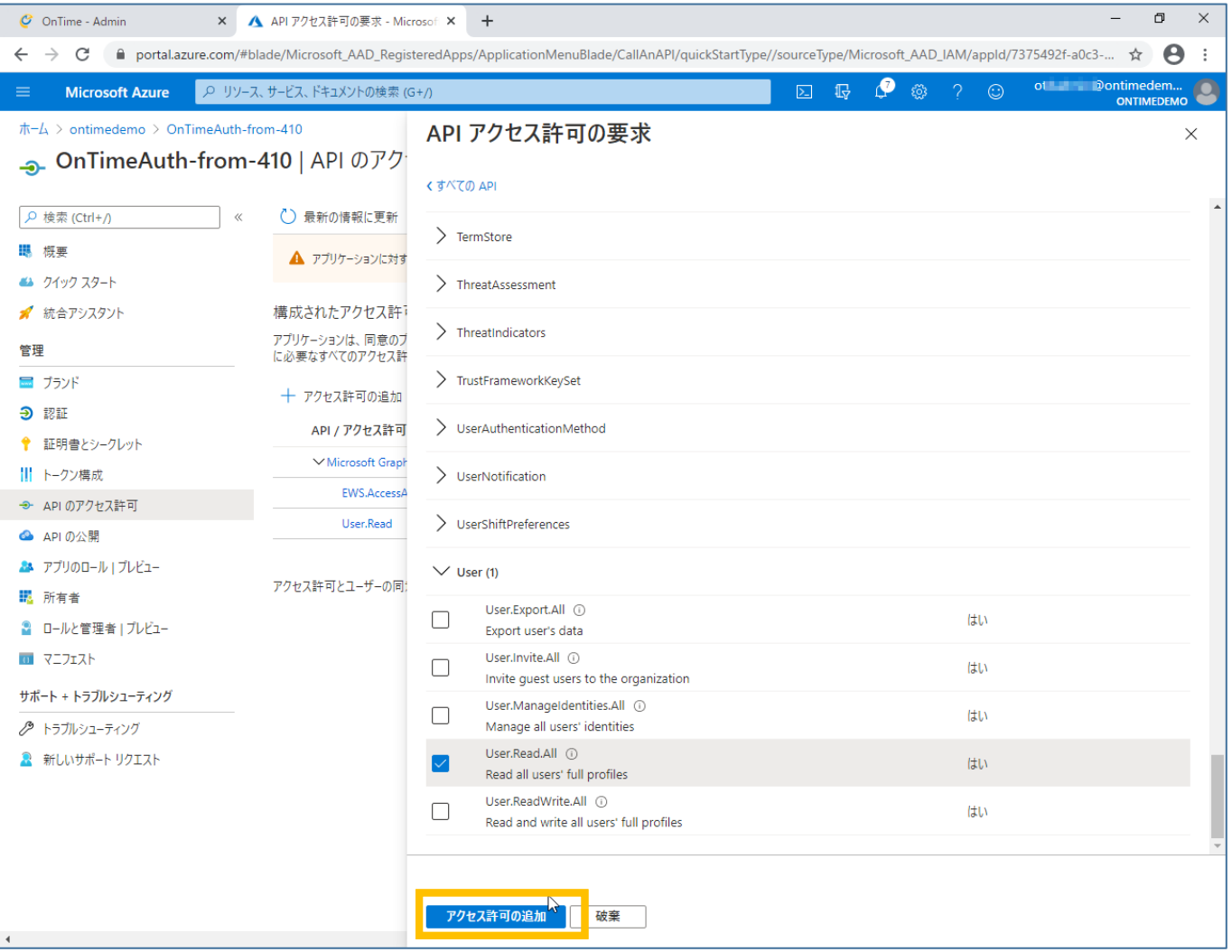
# APIのアクセス許可１２




- 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。

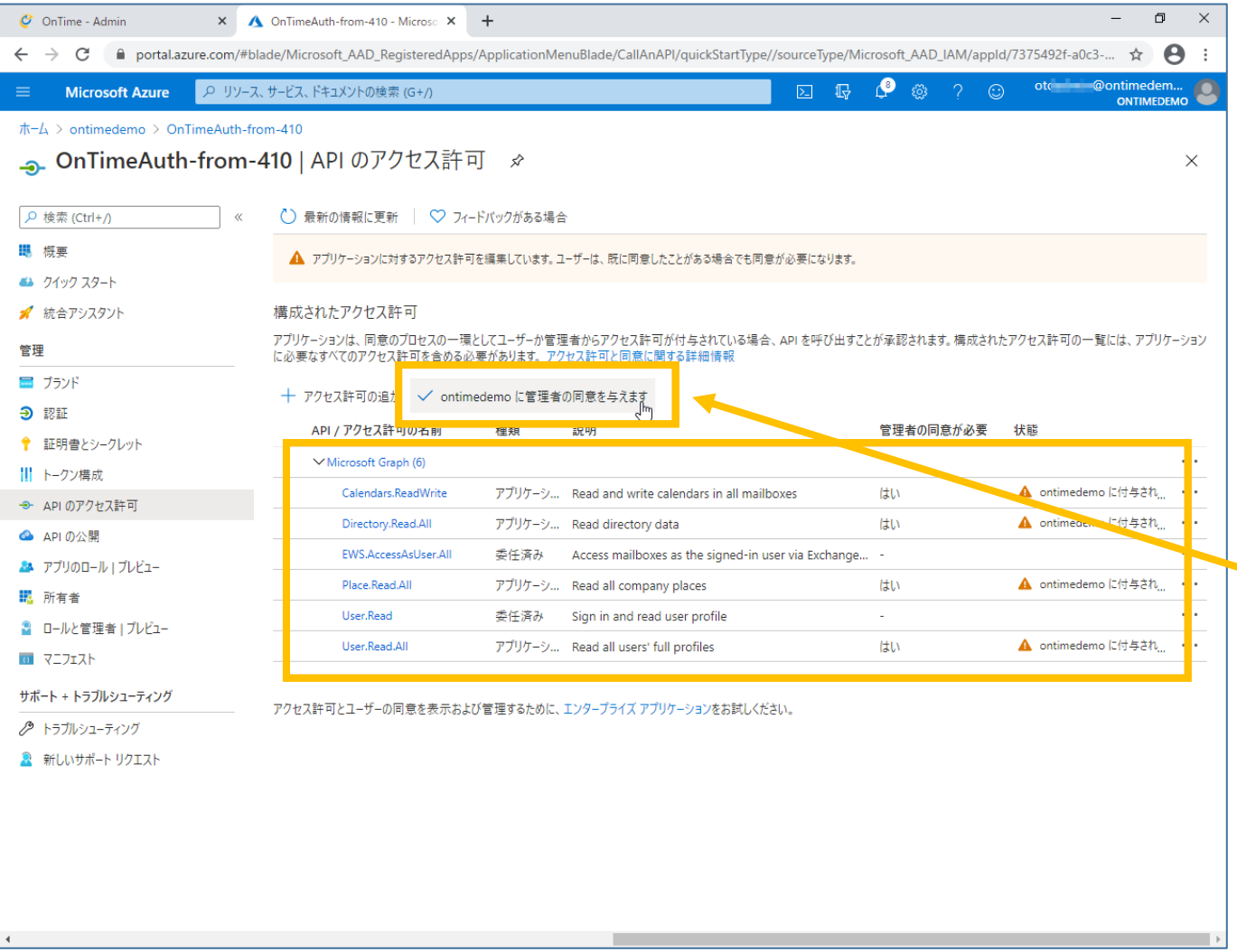
「User.Read.All」をチェックします。

# APIのアクセス許可１３




- 「アクセス許可の追加」をクリックします。

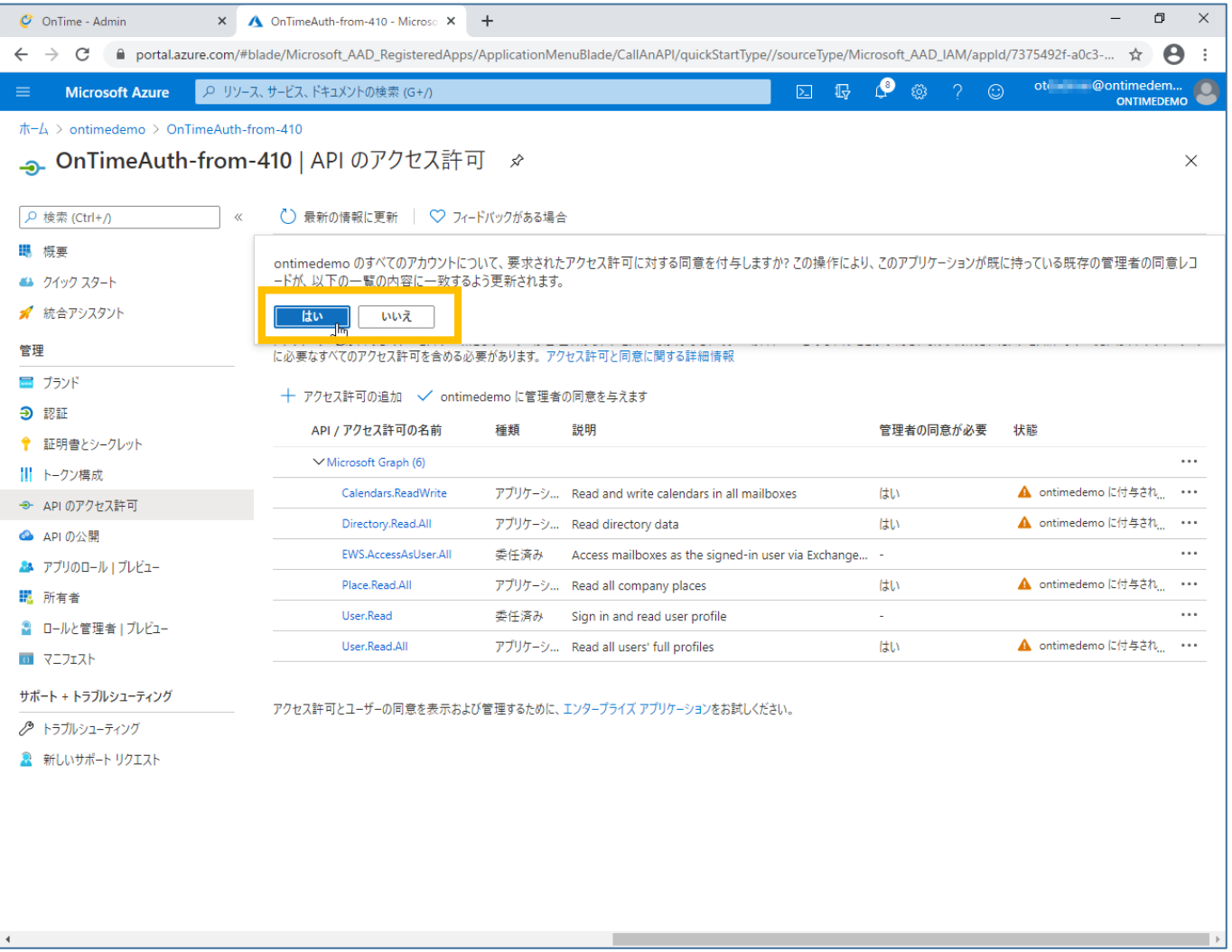
# APIのアクセス許可１４




- 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。

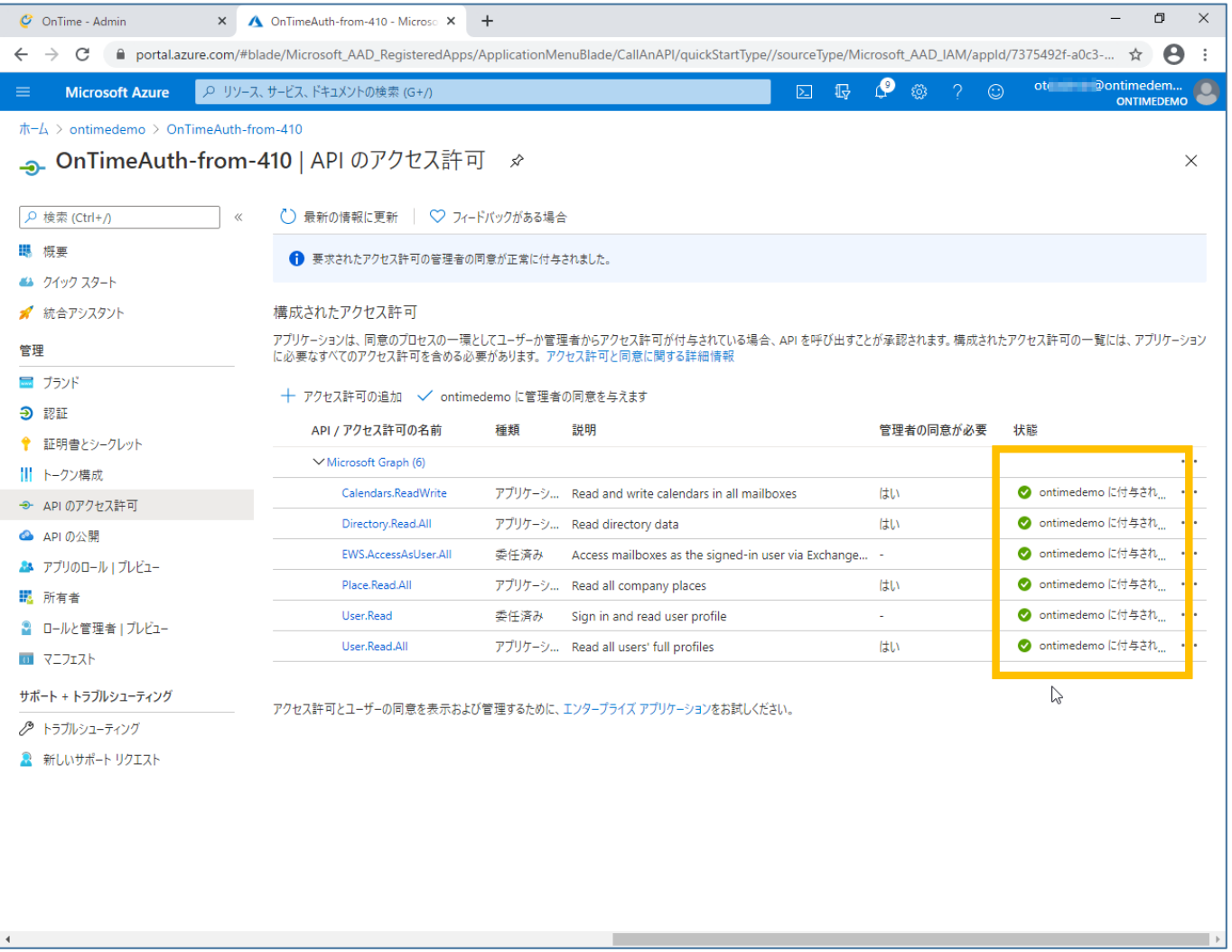
「“ドメイン名”に管理者の同意を与えます」ボタンをクリックします。

# APIのアクセス許可１５




- 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

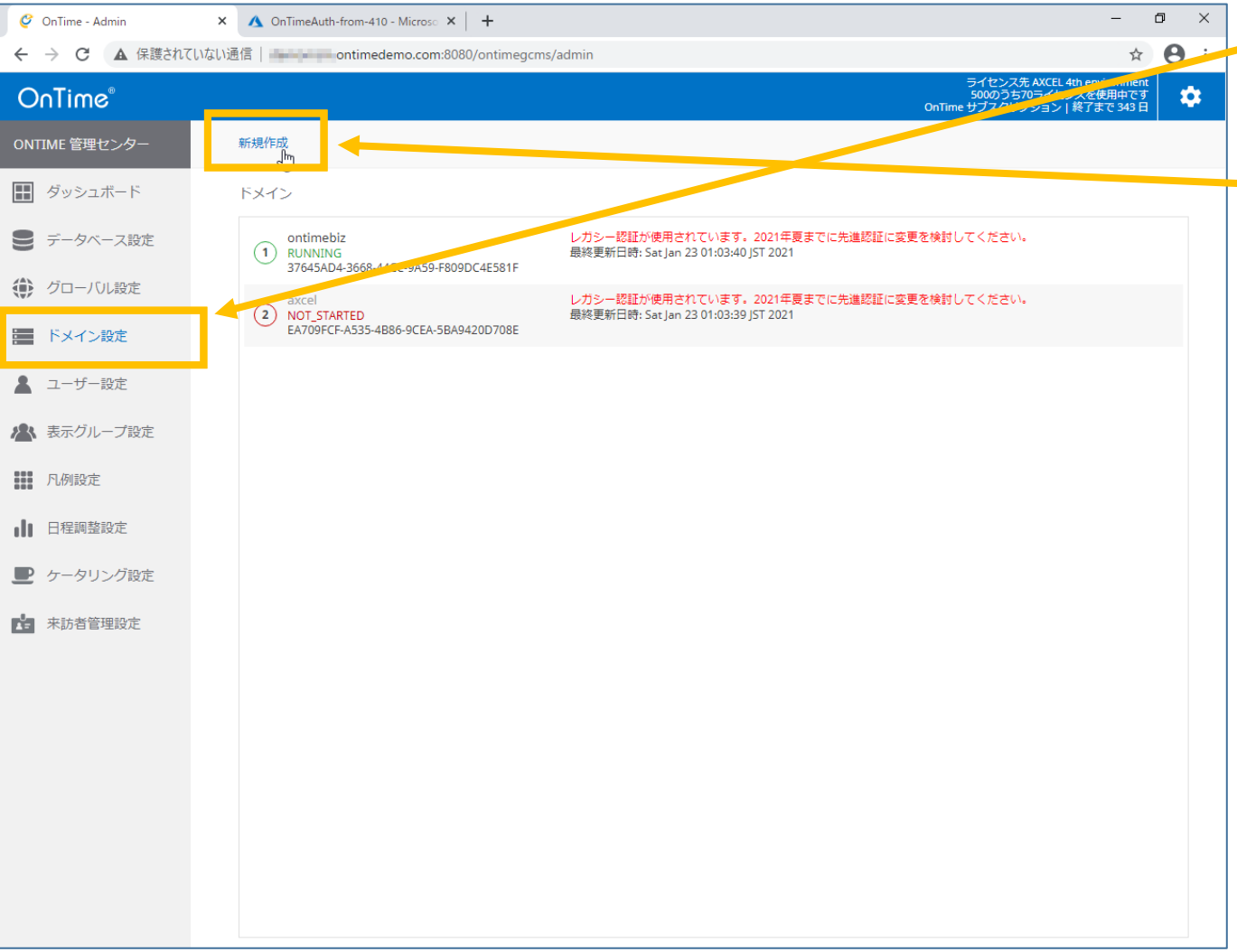



- 無事に付与されてるか確認します。
- もし付与されない場合はAzureグローバル管理者に連絡してご確認ください。

- 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

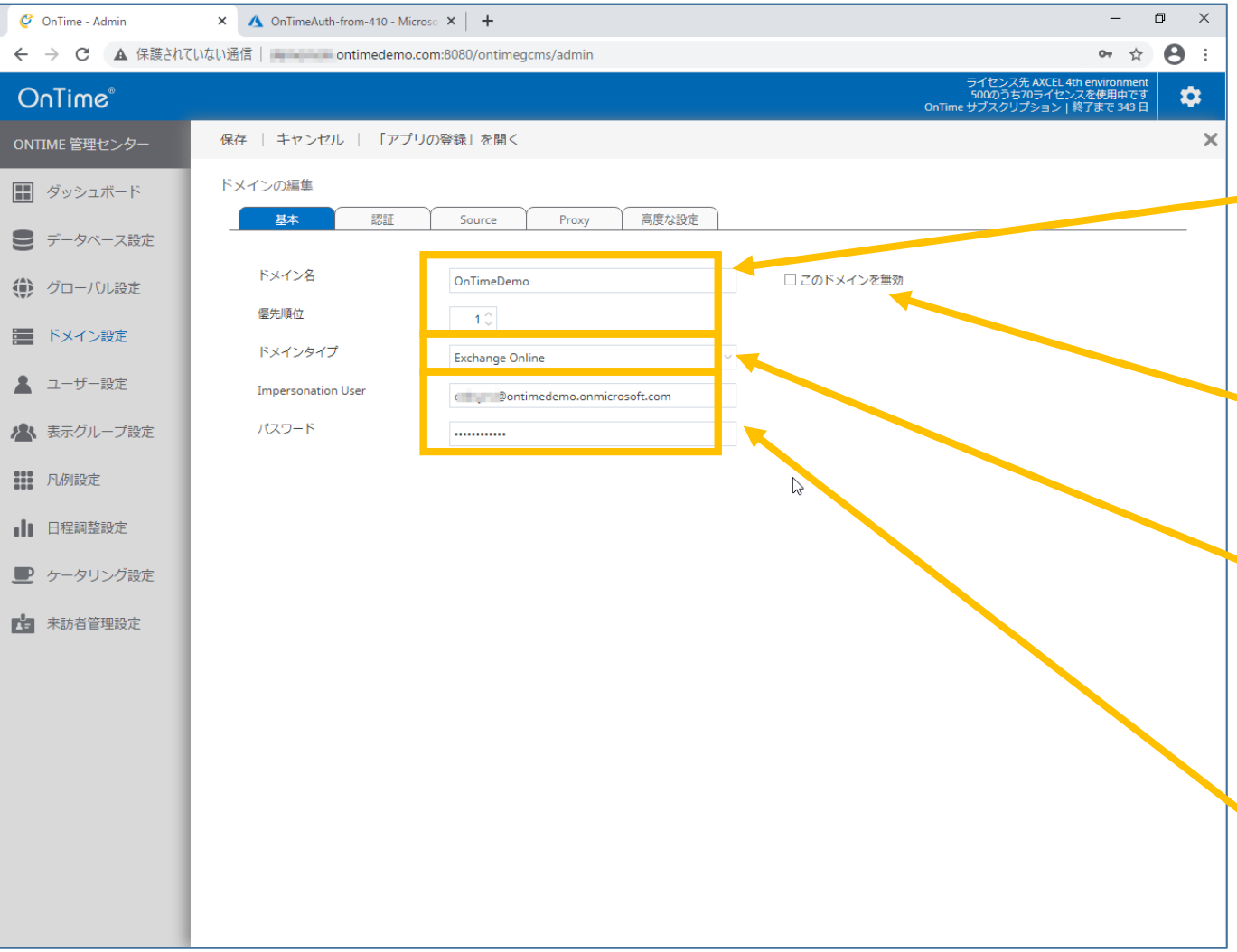



左サイドメニューで「ドメイン」を選択します。

「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ー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(Echange 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。

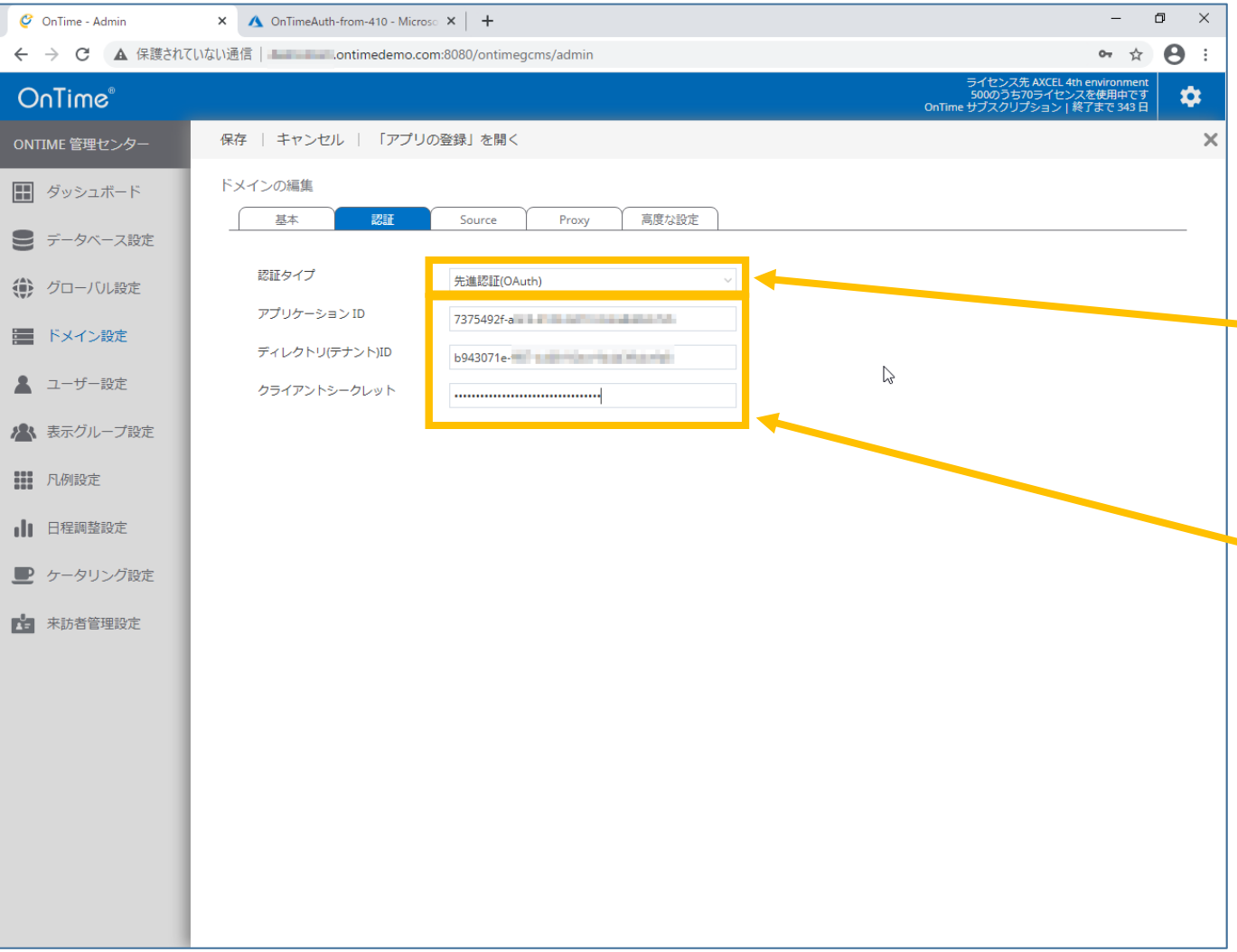
一時的に接続しない場合は無効に出来ます。

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。

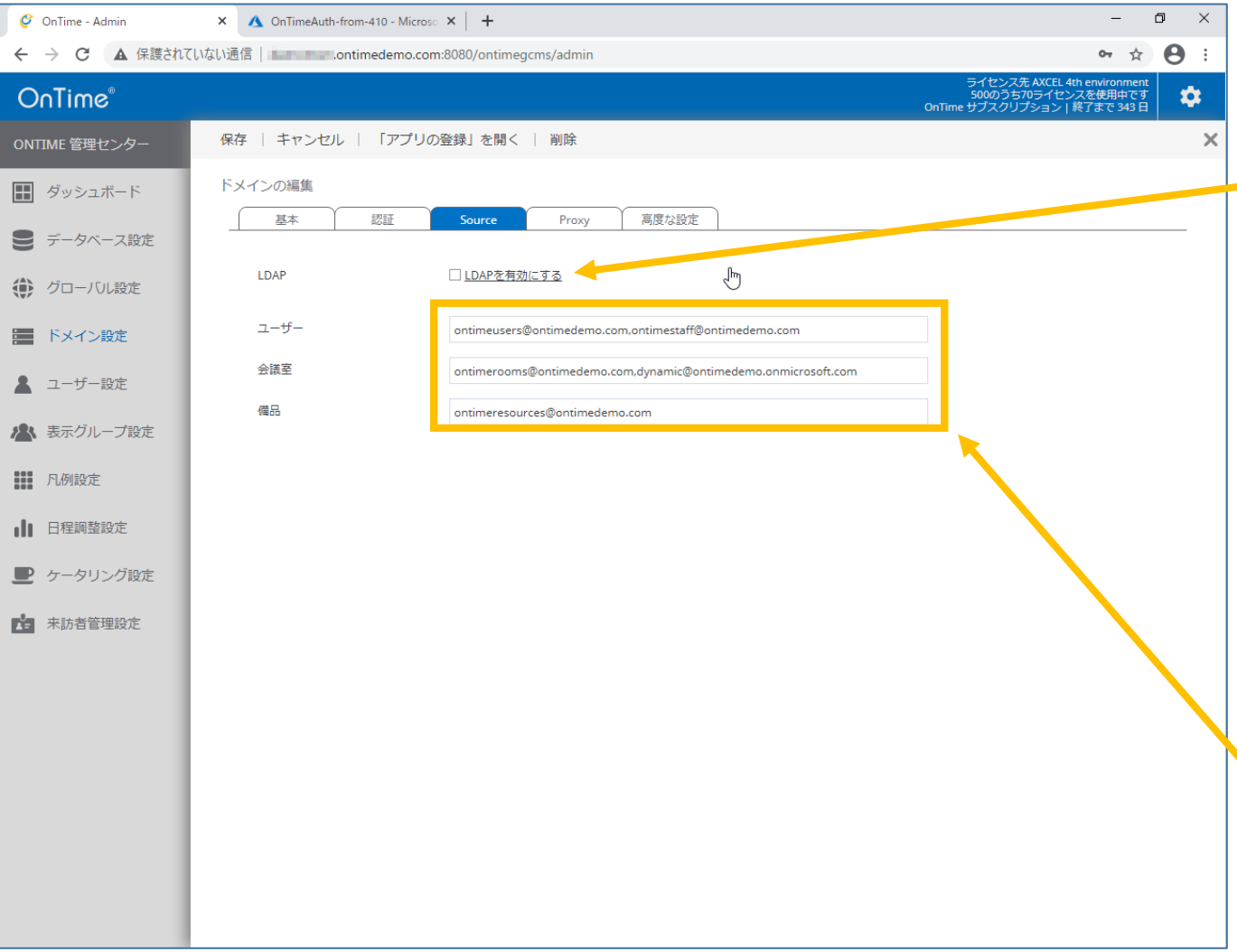
# 先進認証とGraghによるEWS接続




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)に必要となる各種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



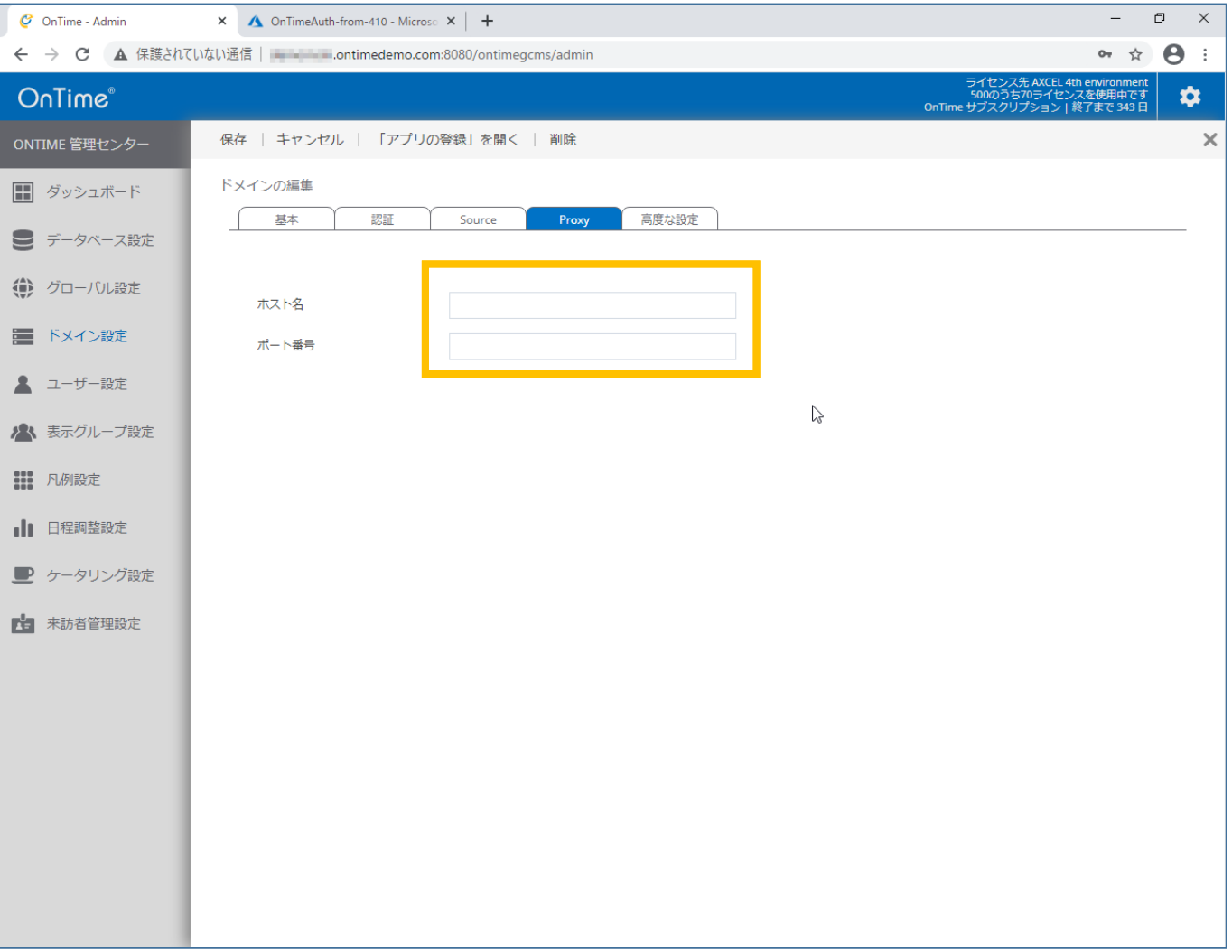

- 今回はグループのメールアドレスのリストで指定します。

"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。

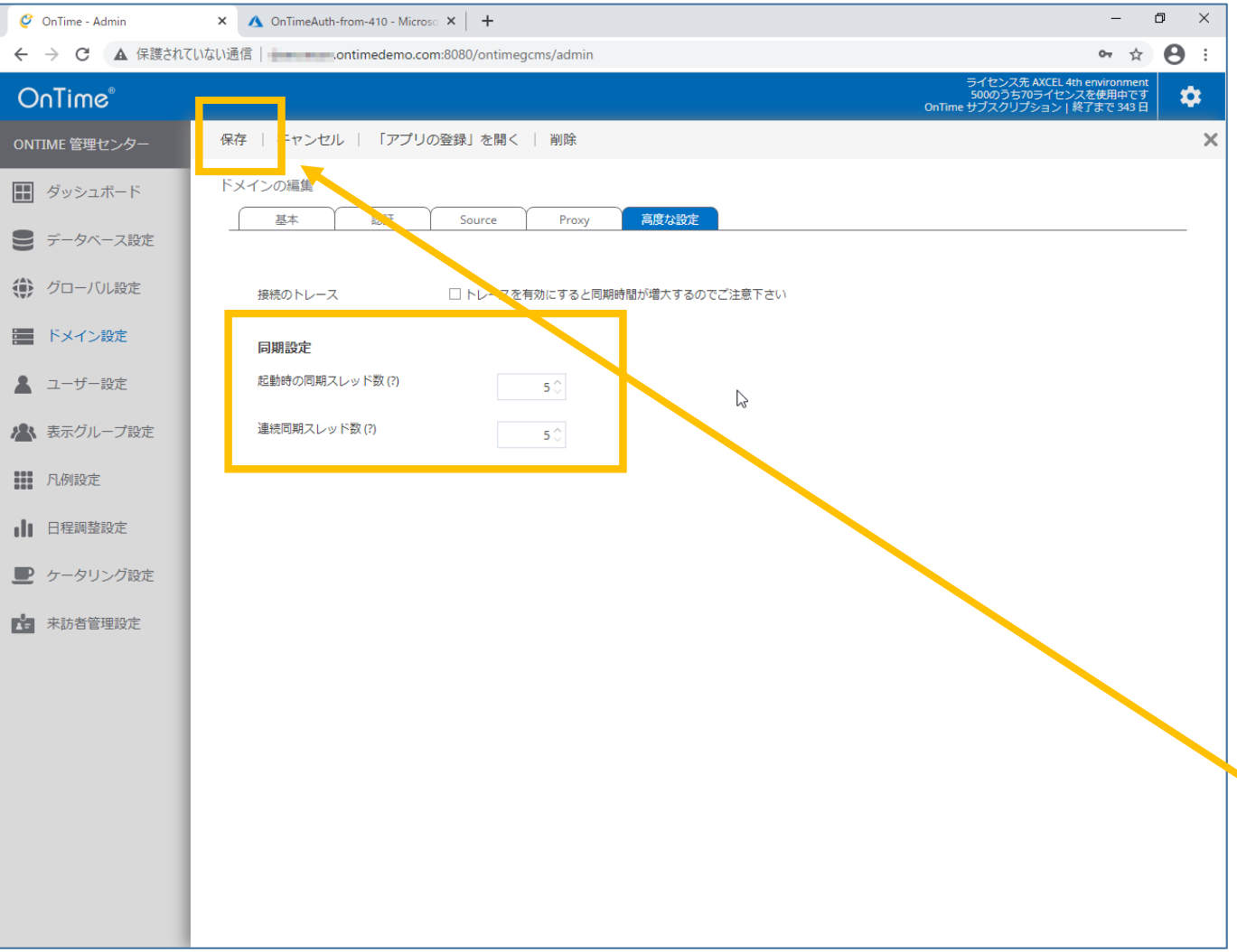
ドメインの ユーザー、会議室、備品のそれぞれに指定されている配布グループ(配布リスト)のメールアドレスを指定します。
複数の場合はカンマで区切ってください。

# Proxyを利用する場合の設定




- 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。

# 高度な設定

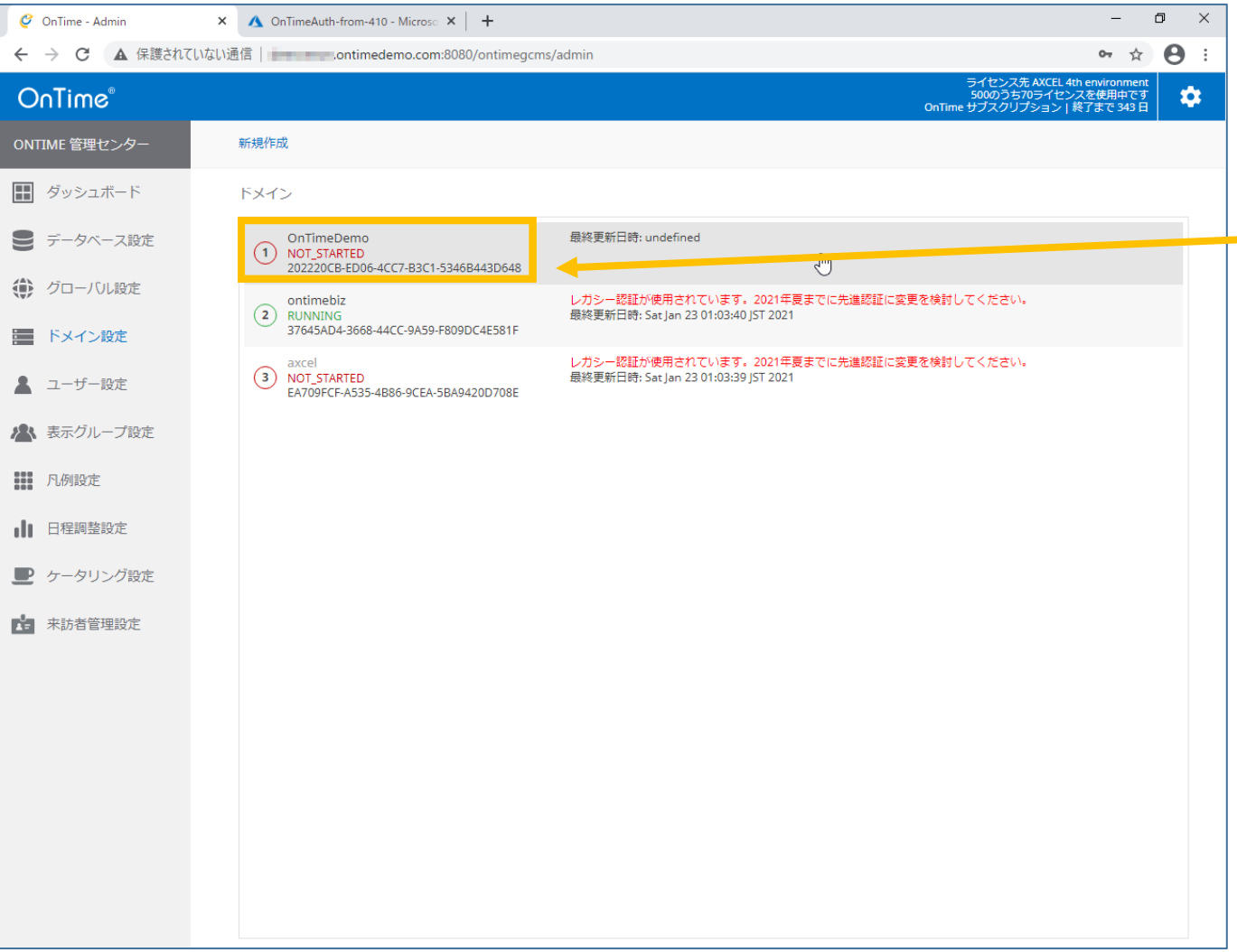



- 接続のトレースはチェックをつけません。サポートから依頼があった場合のみ設定してください。
- 同期設定では「起動時」「通常運用時」それぞれのスレッド数を指定できます。
  - Exchange上のイベント更新情報がOnTimeに反映されるのが遅い場合はOnTimeの同期処理がExchange上のイベント更新頻度に追いついていない可能性があります。そのような場合にスレッド数を増やすことで改善する場合もあります。
  - 最小数は 5 です。
  - OnTimeサーバーのCPUやメモリに充分なパワーがある場合はCPUやメモリの使用率を見ながら徐々に数値を変更してみてください。
  - 1000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



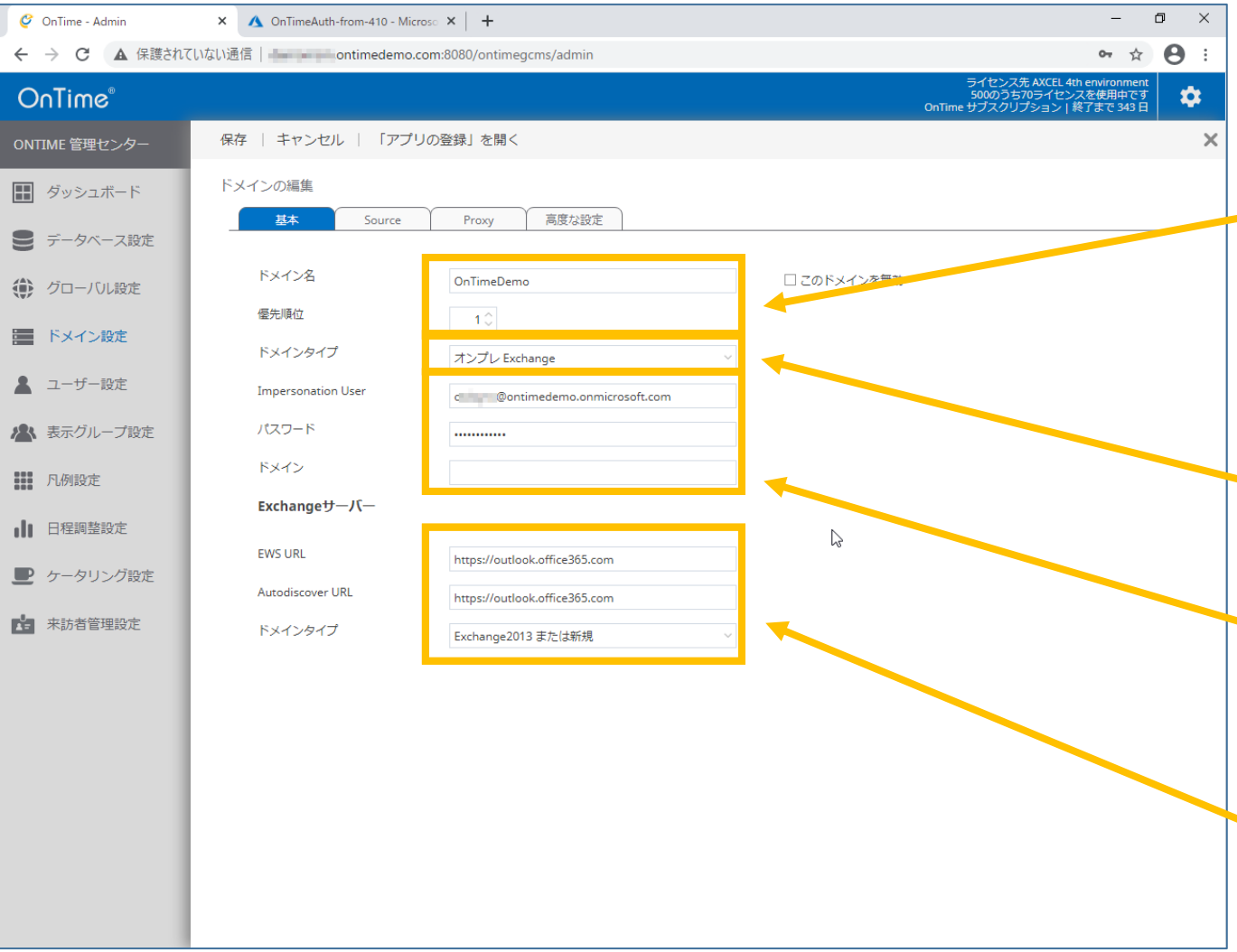

- 画面が閉じると先ほど設定したドメインが増えています。

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。

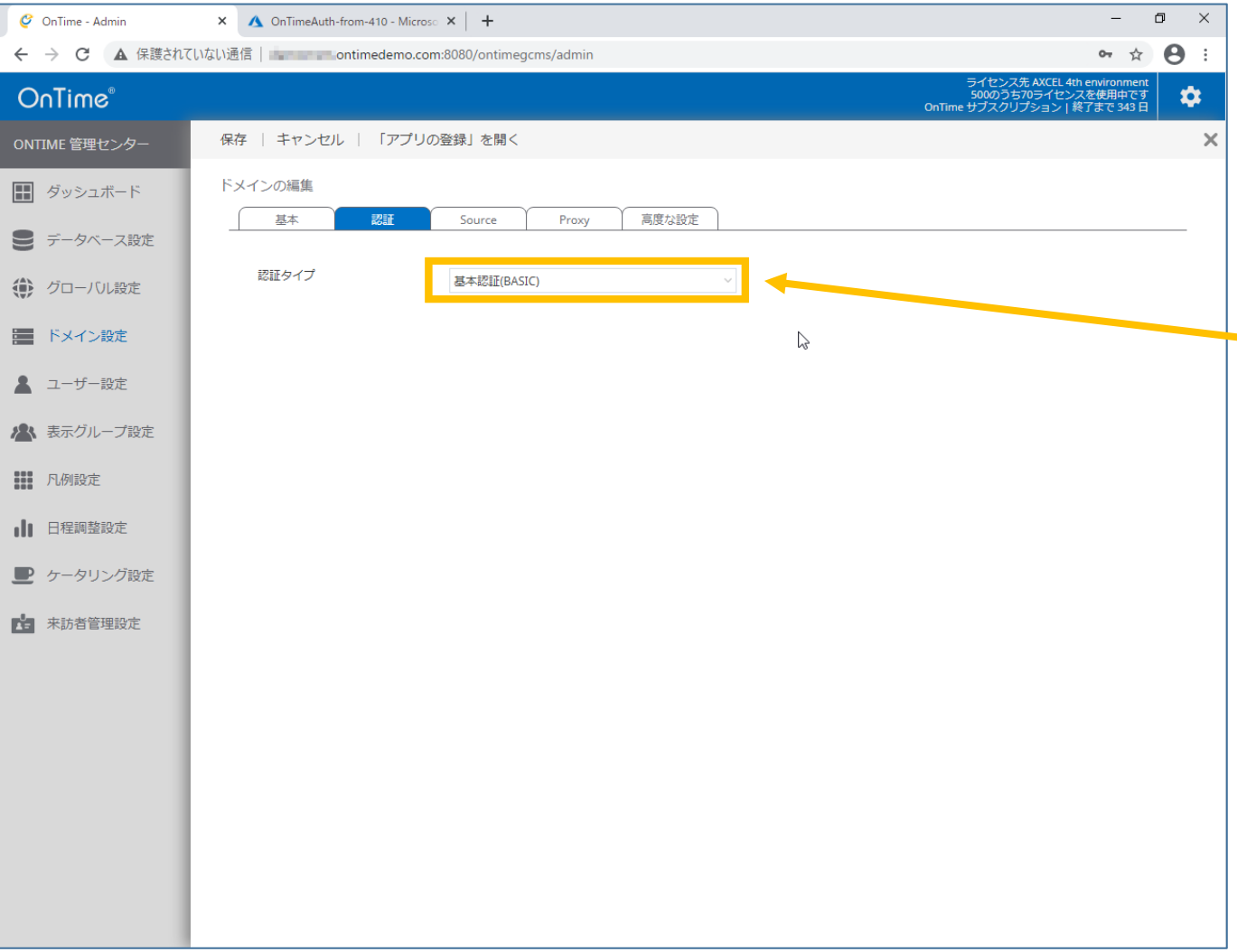
- 優先順位は複数テナント時に同じメールアドレスが使用されている場合にどのテナントを優先するかを指定します。例えばオンプレからクラウドに移行の最中の場合はクラウドを優先したいのでオンプレは大きい数字を指定します。

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



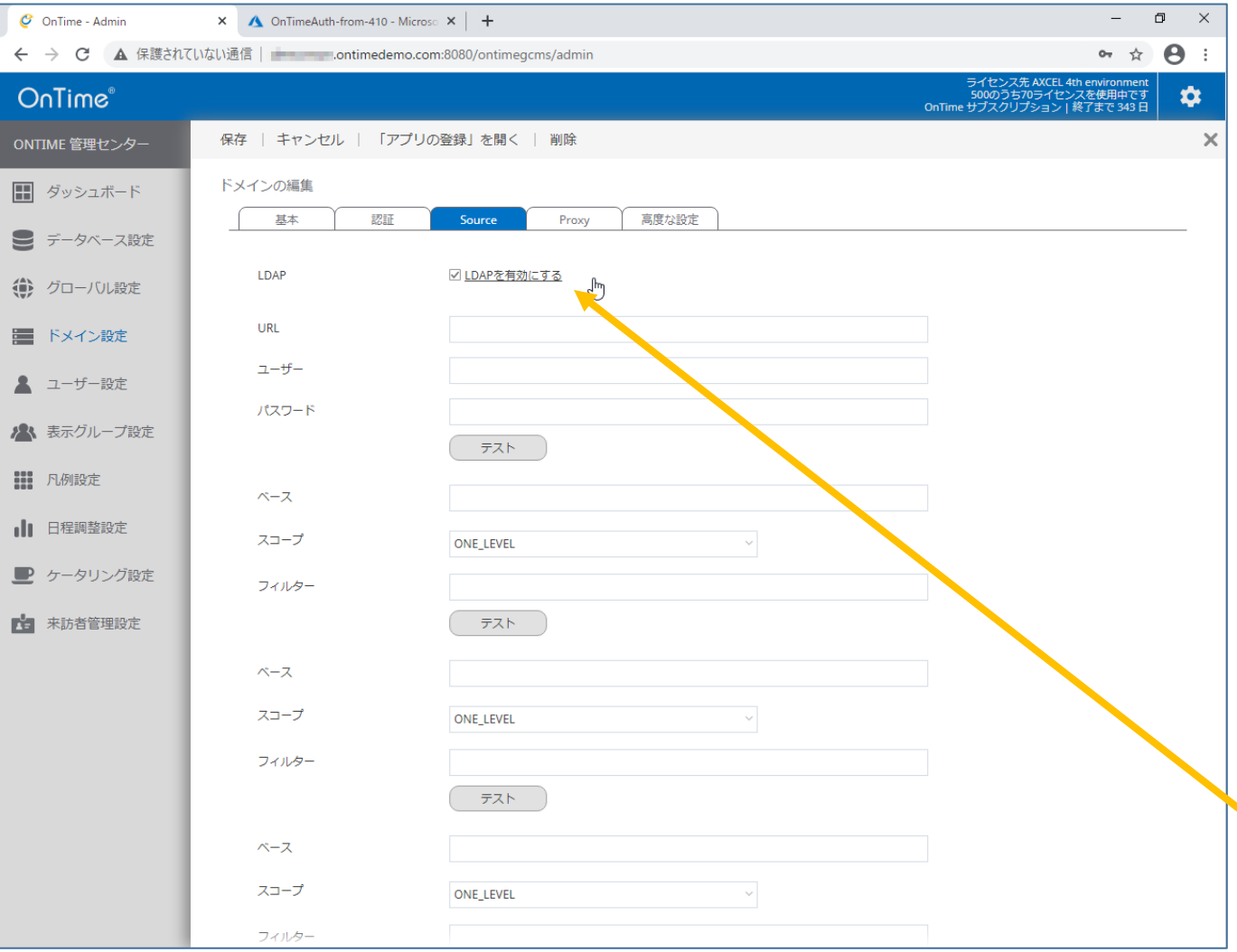

- ドメインタイプで Exchange Online を選択された場合でOauth認証を選択できない場合、また旧バージョンからご利用でまだ先進認証の準備が整っていない場合は「基本認証(BASIC)」を選択してください。
2021年後半には利用が禁止される予定です。

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

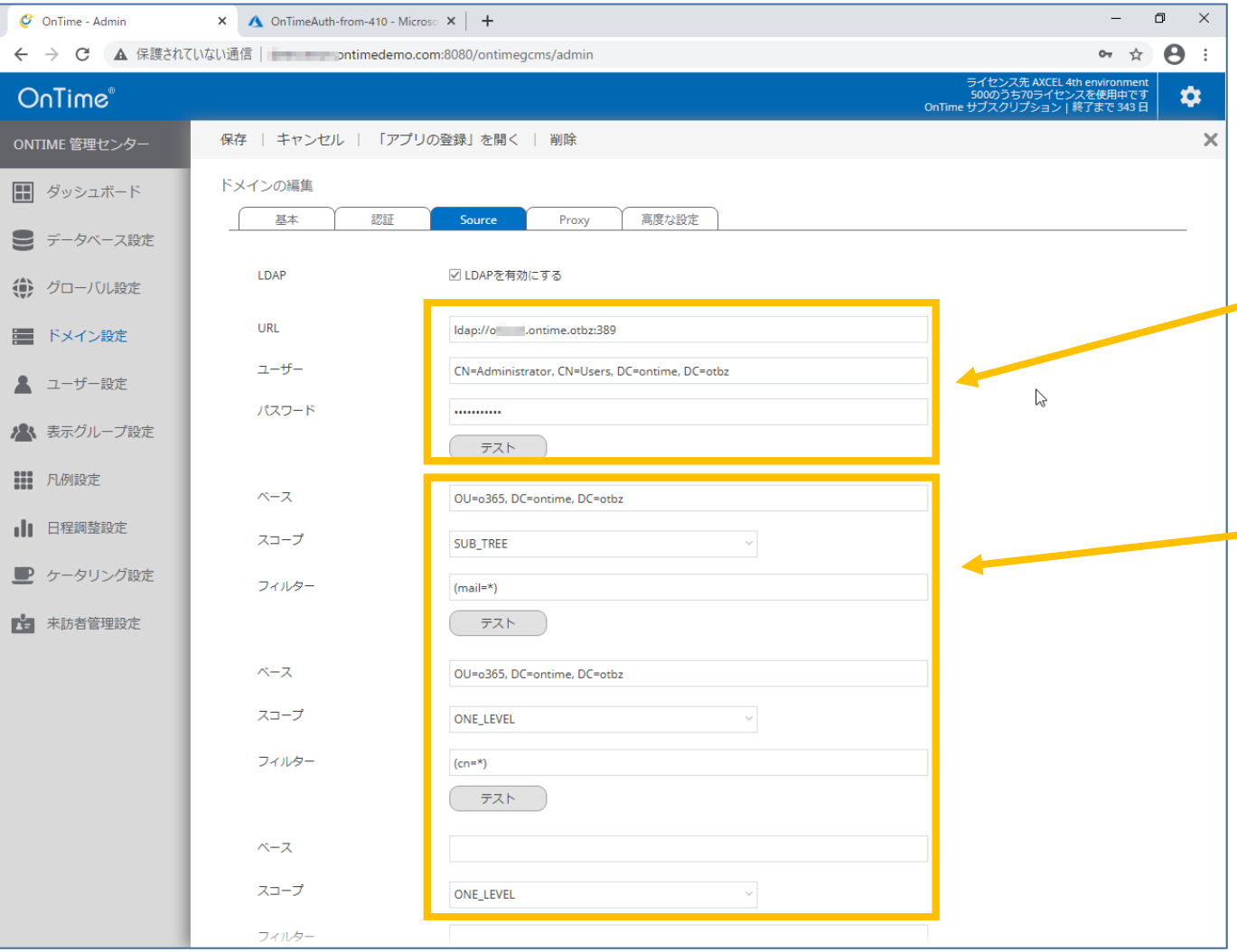
# LDAPでアドレスリスト取得 1




- 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



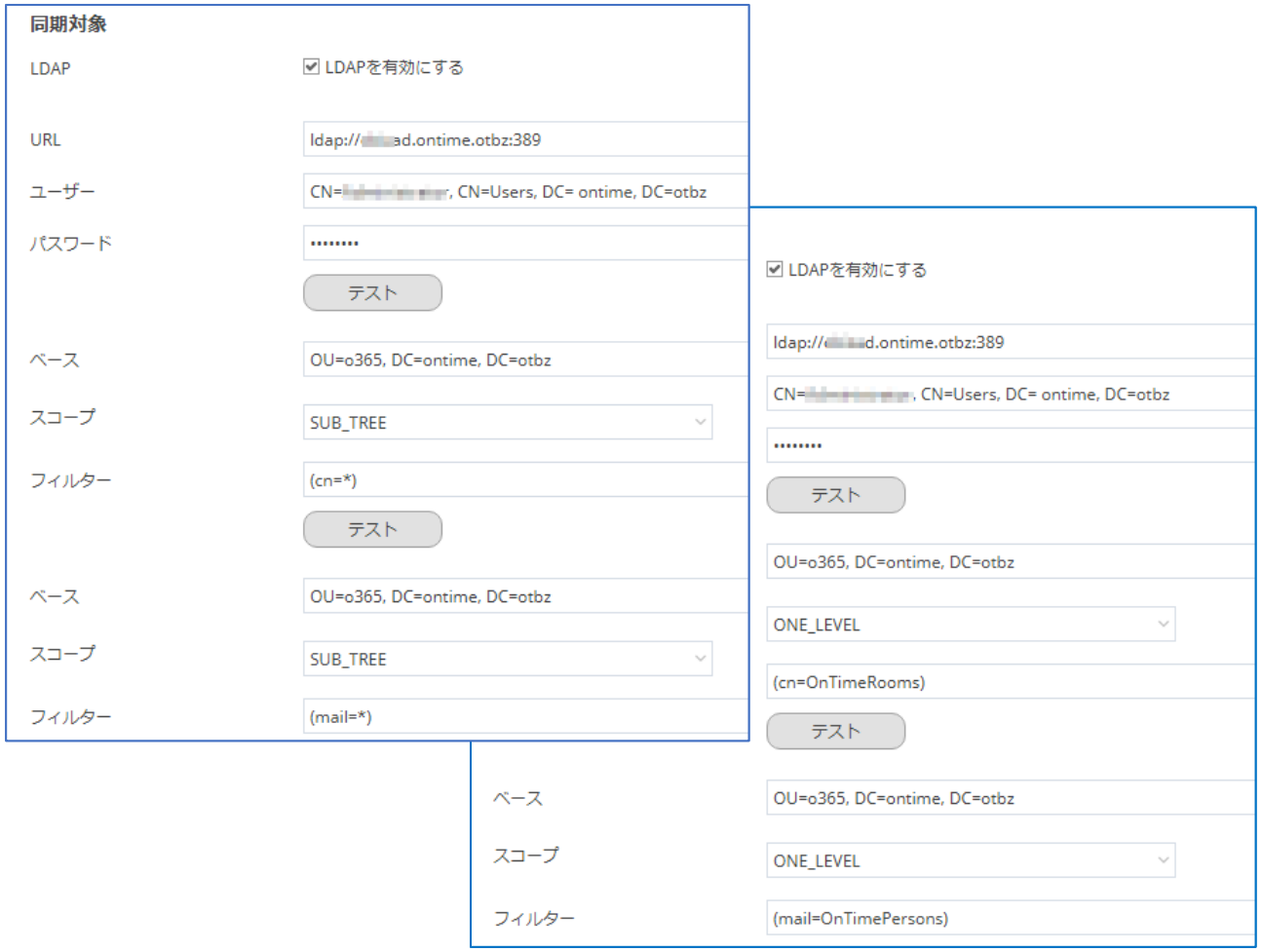

- 同期対象の設定を行います。

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

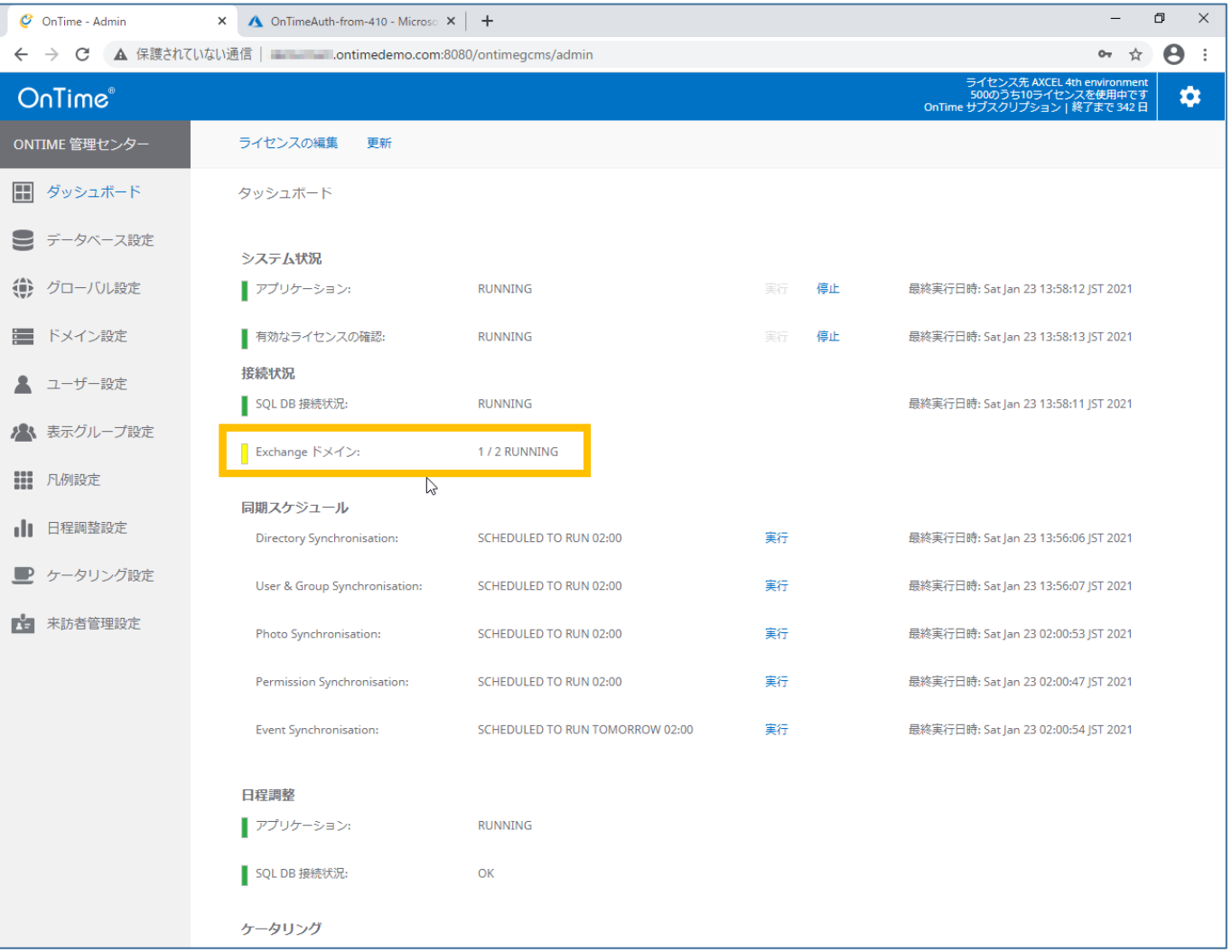



- 左図を参考に組織に応じたフィルター条件で取得してください。
- 左上　特定の属性に値があるアカウントを全て取得
- 右下　特定のグループに属しているアカウントを全て取得

- 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。

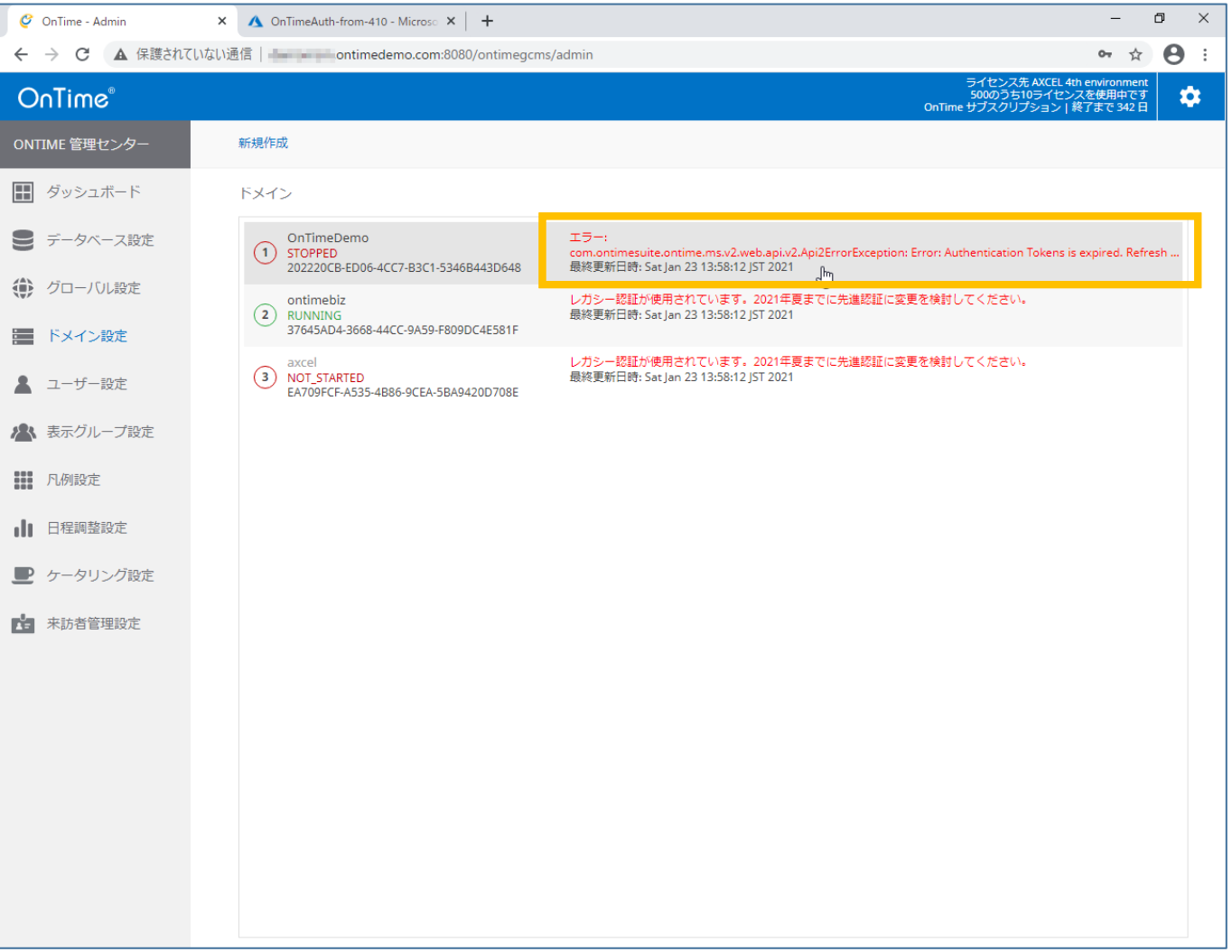
# 補足3）認証タブ
# Graphで認証エラーが出る

# ドメイン接続がエラーで接続できない



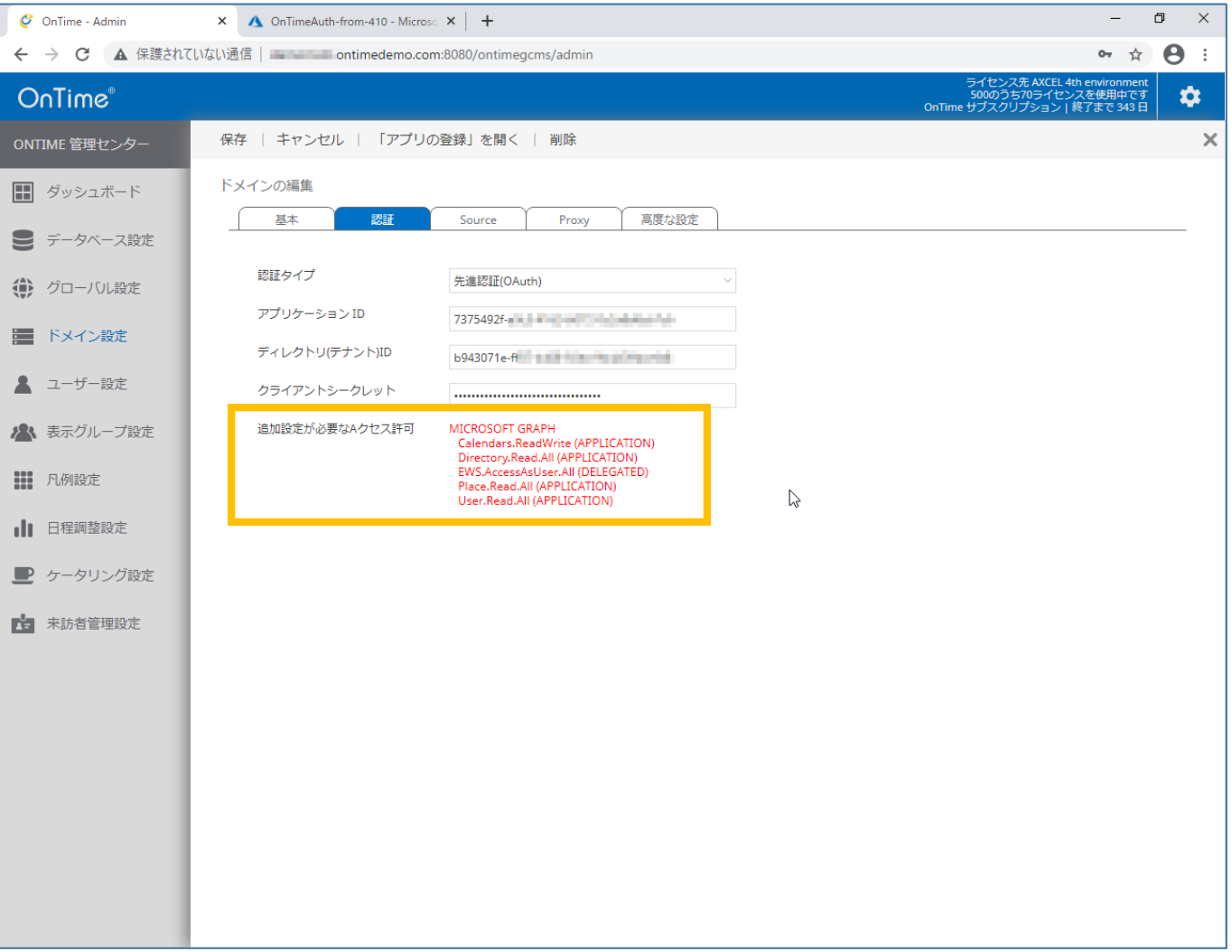

- インジケーターが赤色や黄色の場合はドメイン接続が出来ていない状態です。
- OnTimeをバージョンアップしたなどの場合はほとんどが先進認証(Oauth)が正しく設定されていないときです。

# 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




- 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。