



# OnTime<sup>®</sup> 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                | p.03 |      |
| —ドメイン設定ページ                  | p.04 |      |
| —Microsoft環境への接続ポート、接続URL   | p.06 |      |
| —Teams連携及びサーバー証明書について       | p.07 |      |
| • Azure Portal(AzureAD)での作業 |      |      |
| —アプリの登録                     | p.09 |      |
| —各IDの取得/認証の設定               | p.14 |      |
| —クライアントシークレットの設定            | p.18 |      |
| —APIのアクセス許可                 | p.23 |      |
| • OnTime管理センター ドメイン設定での作業   |      |      |
| —ドメイン設定                     |      | p.43 |
| —Exchangeタブ                 |      | p.45 |
| —同期対象タブ                     |      | p.47 |
| —属性マッピングタブ                  |      | p.49 |
| —高度な設定タブ                    |      | p.50 |
| —保存結果と再起動                   |      | p.51 |
| 補足1) 認可コードフロー認証方式の設定        |      | p.53 |
| 補足2) オンプレExchangeの設定        |      | p.61 |
| 補足3) 同期対象をLDAPで設定           |      | p.63 |
| 補足4) Graphの認証エラーについて        |      | p.67 |



# 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



保存 | キャンセル | 削除

## ドメイン設定

ドメイン名やドメインタイプ、  
テナントの優先順位

## Exchange

接続に関する各種設定

認証方法の選択、Proxy  
経由の接続が必要な場合  
の設定、先進認証用の  
Azure AD のアプリ登録の  
情報の設定。 P.45

## 同期対象

同期対象アカウント指定に関する設定

OnTimeを利用するメールボックスのアカウントを配布リ  
スト(グループ)やメールアドレス付きセキュリティグループで  
指定します。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できるようになります。 P.47

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、同期対  
象をオンプレADからLDAPで指定できます。 P.63

## 属性マッピング

各項目情報に特定の属性を利用する設定

ユーザーの属性情報の表示項目や、会議室/  
備品/共有席の項目にどの属性情報を表示す  
るかを設定 P.49

## 高度な設定

トレース設定、同期ス  
レッド数の設定 P.50

# 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があります)
  - 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

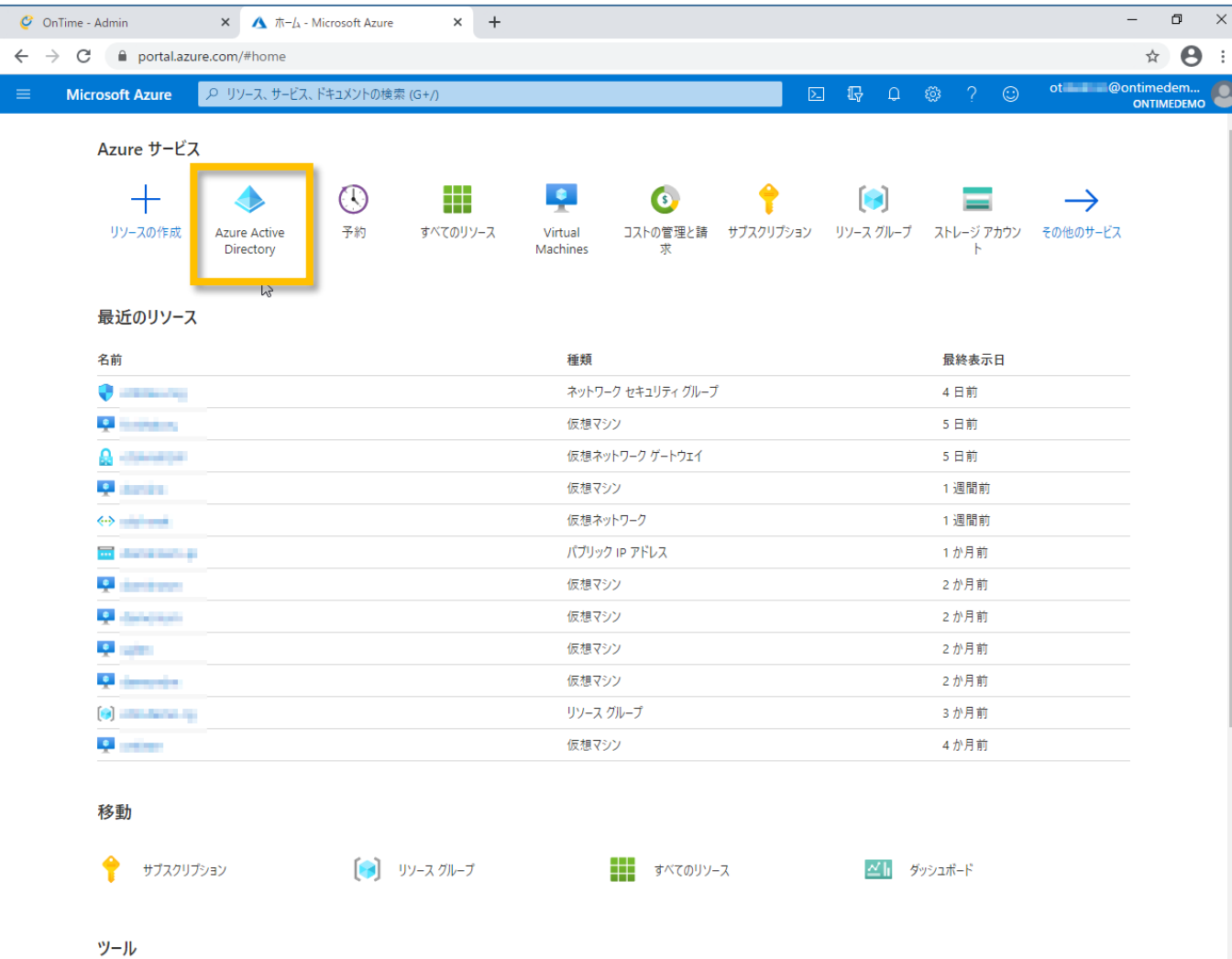
- Teams会議の作成機能は認証方式で先進認証を選択している場合は標準機能です。OnTimeサーバーにTLS(SSL)証明書を準備しなくても利用いただけます。
- Teamsアプリへの埋め込み機能はMicrosoftの仕様により組織の実在性と本人性の証明のため、OnTimeサーバーへのパブリックなTLS(SSL)証明書の実装が必須となります。
- OnTimeサーバーへのTLS(SSL)証明書の実装方法はFAQの「[OnTimeサーバーにTLS\(SSL\)証明書を設定する](#)」をご参照ください。
- Teamsアプリへの埋め込み機能の登録方法は「Microsoft Teams アプリ登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



The screenshot displays the Microsoft Azure portal interface for the 'ontimedemo' tenant. The left-hand navigation pane includes a sidebar with various management options. The 'アプリの登録' (App Registration) option is highlighted with a yellow rectangular box. The main content area shows the 'ontimedemo' tenant overview, including a search bar, tenant information (such as role, license, and tenant ID), and a sign-in graph showing user activity over time. The sign-in graph shows a peak in activity around January 17th.

- 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



Microsoft Azure | アプリの登録

すべてのアプリケーション | 所有しているアプリケーション

名前またはアプリケーション ID を入力し始めると結果がフィルター処理されます

| 表示名            | アプリケーション (クライアント) ID | 作成日      | 証明書とシークレット |
|----------------|----------------------|----------|------------|
| OT otddemo     | 5bdb6c27-...         | 2018/7/1 | ✓ 現在       |
| ON OnTime-Demo | f8d17528-...         | 2020/7/1 | ✓ 現在       |
| ON OnTime-Demo | 3b03e46e-...         | 2020/7/1 | ✓ 現在       |
| ON OnTime-Demo | de25bf72-...         | 2021/7/1 | ✓ 現在       |
| ON ontimedemo  | 0281466a-...         | 2021/7/1 | ✓ 現在       |
| ON OnTimeD...  | ed69bfc2-...         | 2021/7/1 | ✓ 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

ホーム > ontimedemo >

アプリケーションの登録

\* 名前

このアプリケーションのユーザー向け表示名 (後で変更できます)。

OnTimeAuth-from-420

サポートされているアカウントの種類

この組織ディレクトリのみ (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 にリダイレクトされます。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。

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



Microsoft Azure portal showing the 'OnTimeAuth-from-420' application details. The 'Application (client) ID' is highlighted with a yellow box and a 'Copy to clipboard' tooltip.

Basic information:

- Application (client) ID: 7375492f-a0c3-41...
- Application ID URI: b943071e-ff87-44...
- Object ID: 6548d867-88af-4a...

API calls section shows a list of services and a button to 'API access permissions'.

Documents section lists various resources like Microsoft ID Platform, authentication scenarios, and code samples.

- 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



OnTime - Admin | OnTimeAuth-from-410 - Microsoft

portal.azure.com/#blade/Microsoft\_AAD\_RegisteredApps/ApplicationMenuBlade/Credentials/quickStartType/sourceType/Microsoft\_AAD\_IAM/appld/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-420

### OnTimeAuth-from-420 | 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

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

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



Microsoft Azure portal screenshot showing the 'OnTimeAuth-from-420' application settings. The 'Credentials' section is expanded, showing the 'Client secrets' tab. A button labeled '+ 新しいクライアントシークレット' (Add new client secret) is highlighted with a yellow box. The left sidebar shows the navigation menu with '証明書とシークレット' (Certificates and secrets) selected.

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

# クライアントシークレットの設定 3



クライアント シークレットの追加

説明: onTimeDemo

有効期限: 24 か月

追加 キャンセル

- 「クライアントシークレットの追加」ダイアログが開きます。
- 「説明」には識別しやすい名前を入力します。
- 「有効期限」は最長「24か月」まで選択できます。
- 内容がよろしければ「追加」ボタンをクリックします。

クライアントシークレットは期限付きの  
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



OnTime - Admin

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

Microsoft Azure

ホーム > ontimedemo > OnTimeAuth-from-420

### OnTimeAuth-from-420 | 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、それを取壊すことができます。

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         | 操作                 |
|------------|-----------|-----------|--------------------|
| OnTimeDemo | 2023/1/23 | UlpR6C... | b6078 18-04e1-4... |

- 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。



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

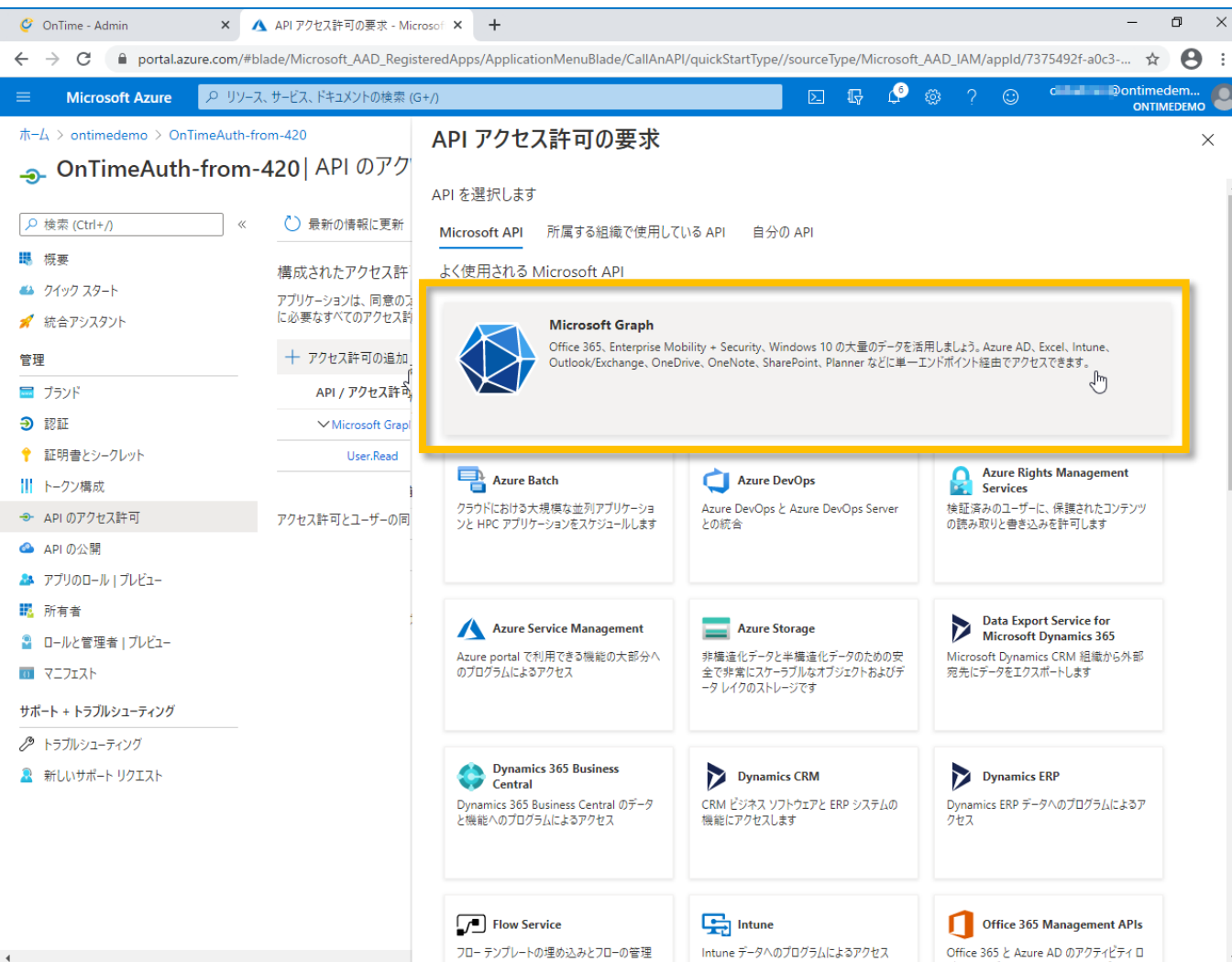
# APIのアクセス許可 1



- 「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



The screenshot shows the 'API アクセス許可の要求' (API permissions) page in the Azure portal. The left sidebar shows the 'API のアクセス許可' (API permissions) section. The main area lists various permissions, with 'EWS' expanded. The 'EWS.AccessAsUser.All' permission is highlighted with a yellow box, and an arrow points to it from a text box on the right.

API アクセス許可の要求

すべての API

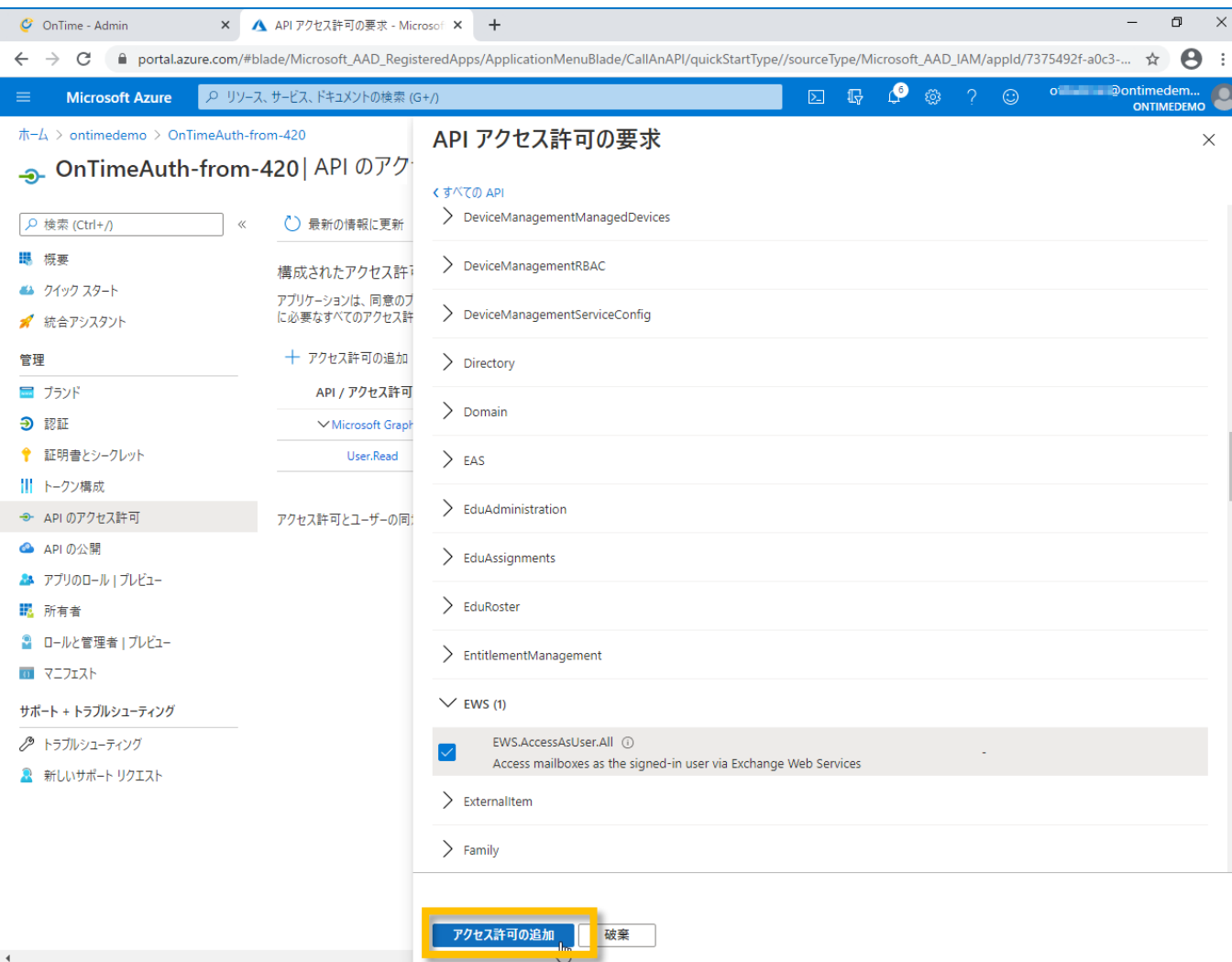
- DeviceManagementManagedDevices
- DeviceManagementRBAC
- DeviceManagementServiceConfig
- Directory
- Domain
- EAS
- EduAdministration
- EduAssignments
- EduRoster
- EntitlementManagement
- ✓ EWS
  - ✓ EWS.AccessAsUser.All (Access mailboxes as the signed-in user via Exchange Web Services)
- ExternalItem
- Family

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「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



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-420

### OnTimeAuth-from-420 | 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

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 (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 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



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 9



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 10



API アクセス許可の要求

- > IdentityUserFlow
- > InformationProtectionContent
- > InformationProtectionPolicy
- > LearningContent
- > LicenseAssignment
- ▼ MailboxSettings (1)
  - ☐ MailboxSettings.Read ⓘ  
Read all user mailbox settings
  - ☒ MailboxSettings.ReadWrite ⓘ  
Read and write all user mailbox settings
- > Mail
- > Member
- > Notes
- > OnlineMeetingArtifact
- > OnlineMeetingRecording
- > OnlineMeetings

アクセス許可の追加 破棄

- 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 1 1



API アクセス許可の要求

すべての API

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

アクセス許可の追加 破壊

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

「People.Read.All」をチェックします。

# APIのアクセス許可 1 2



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

OnTimeAuth-from-420 | API のアクセス許可

API アクセス許可の要求

すべての API

- Member
- Notes
- OnlineMeetings
- OnPremisesPublishingProfiles
- Organization
- OrgContact
- People (1)
  - ☒ People.Read.All (1)  
Read all users' relevant people lists
- Place (1)
  - ☒ Place.Read.All (1)  
Read all company places
- Policy
- Presence
- 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 3



The screenshot shows the 'API Access Permissions' page in the Microsoft Azure portal. The left sidebar contains navigation links for 'OnTimeAuth-from-420 | API のアクセス許可'. The main content area shows a list of permissions under the 'User (1)' section. The 'User.Read.All' permission is selected with a checkmark. The 'Add' button at the bottom is highlighted.

| API Access Permission     | Consent |
|---------------------------|---------|
| TermStore                 |         |
| ThreatAssessment          |         |
| ThreatIndicators          |         |
| TrustFrameworkKeySet      |         |
| UserAuthenticationMethod  |         |
| UserNotification          |         |
| UserShiftPreferences      |         |
| User (1)                  |         |
| User.Export.All           | はい      |
| User.Invite.All           | はい      |
| User.ManageIdentities.All | はい      |
| User.Read.All             | はい      |
| User.ReadWrite.All        | はい      |
| User.ReadWrite.All        | はい      |

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

「User.Read.All」をチェックします。

- 「アクセス許可の追加」をクリックします。

# APIのアクセス許可 1 4



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

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

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

ホーム > ontimedemo > OnTimeAuth-from-420

OnTimeAuth-from-420 | API のアク

検索 (Ctrl+/) 最新の情報に更新

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 ロール

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

API アクセス許可の要求

API を選択します

Microsoft API 所属する組織で使用している API 自分の API

API を公開するディレクトリ内のアプリは、以下のとおりです

office

名前 アプリケーション (クライアント) ID

|                                   |                                      |
|-----------------------------------|--------------------------------------|
| Office 365 Enterprise Insights    | f9d02341-e7aa-456d-926d-4a0ca599fbee |
| Office 365 Exchange Online        | 00000002-0000-0ff1-ce00-000000000000 |
| Office 365 Information Protection | 2f3f02c9-5679-4a5c-a605-0de55b07d135 |
| Office 365 Management APIs        | c5393580-f805-4401-95e8-94b7a6ef2fc2 |
| Office 365 Mover                  | d62121f3-e023-4972-b6b0-794190c0fd98 |
| Office 365 Search Service         | 66a88757-258c-4c72-893c-3e8bed4d6899 |
| Office 365 SharePoint Online      | 00000003-0000-0ff1-ce00-000000000000 |
| Office Agent Service              | 5225545c-3ebd-400f-b668-c8d7850d776  |
| Office Delve                      | 94c63fef-13a3-47bc-8074-75af8c65887a |
| Office Hive                       | 166f1b03-5b19-416f-a94b-1d7aa2d247dc |
| Office Scripts Service            | 62fd1447-0ef3-4ab7-a956-7dd05232ecc1 |
| Office Shredding Service          | b97b6bd4-a49f-4a0c-af18-af507d1da76c |
| Office365 Zoom                    | 0d38933a-0bbd-41ca-9ebd-28c4b5ba7cb7 |
| OfficeServicesManager             | 9e4a5442-a5c9-4f6f-b03f-5b9fcaaf24b1 |

- 画面が戻ったら再度「アクセス許可の追加」ボタンをクリックします。

「所属する組織で使用しているAPI」を選択します。

検索欄に office と入力して検索します。

Office 365 Exchange Online を選択します。

# APIのアクセス許可 1 5



- 「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 1 6



検索 (Ctrl+F) << 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。

「管理者の同意が必要」列には、組織の既定値が表示されます。ただし、ユーザーの同意は、アクセス許可、ユーザー、アプリごとにカスタマイズできます。この列には、ご自分の組織や、このアプリ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](#)

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 (8)            |             |                                                            |           |             |
| Calendars.ReadWrite              | アプリケーション... | Read and write calendars in all mailboxes                  | はい        | に付与されていま... |
| Directory.Read.All               | アプリケーション... | Read directory data                                        | はい        | に付与されていま... |
| EWS.AccessAsUser.All             | 委任済み        | Access mailboxes as the signed-in user via Exchange W...   | いいえ       |             |
| MailboxSettings.ReadWrite        | アプリケーション... | Read and write all user mailbox settings                   | はい        | に付与されていま... |
| People.Read.All                  | アプリケーション... | Read all users' relevant people lists                      | はい        | に付与されていま... |
| Place.Read.All                   | アプリケーション... | Read all company places                                    | はい        | に付与されていま... |
| User.Read                        | 委任済み        | Sign in and read user profile                              | いいえ       |             |
| User.Read.All                    | アプリケーション... | Read all users' full profiles                              | はい        | に付与されていま... |
| ▼ Office 365 Exchange Online (1) |             |                                                            |           |             |
| full_access_as_app               | アプリケーション... | Use Exchange Web Services with full access to all mailb... | はい        | に付与されていま... |

- 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



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

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

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

ホーム > ontimedemo > OnTimeAuth-from-420

OnTimeAuth-from-420 | API のアクセス許可 ✕

検索 (Ctrl+/) << 最新の情報に更新 フィードバックがある場合

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 ロール

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

ontimedemo のすべてのアカウントについて、要求されたアクセス許可に対する同意を付与しますか? この操作により、このアプリケーションが既に持っている既存の管理者の同意レコードが、以下の一覧の内容に一致するよう更新されます。

はい いいえ

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

構成されたアクセス許可

アプリケーションは、同意のプロセスの一環としてユーザーが管理者からアクセス許可が付与されている場合、API を呼び出すことが承認されます。構成されたアクセス許可の一覧には、アプリケーションに必要なすべてのアクセス許可を含める必要があります。 [アクセス許可と同意に関する詳細情報](#)

+ アクセス許可の追加 ✓ ontimedemo に管理者の同意を与えます

| API / アクセス許可の名前                  | 種類          | 説明                                                         | 管理者の同意が必要 | 状態              |
|----------------------------------|-------------|------------------------------------------------------------|-----------|-----------------|
| ▼ Microsoft Graph (8)            |             |                                                            |           |                 |
| Calendars.ReadWrite              | アプリケーション... | Read and write calendars in all mailboxes                  | はい        | に付与されていま... *** |
| Directory.Read.All               | アプリケーション... | Read directory data                                        | はい        | に付与されていま... *** |
| EWS.AccessAsUser.All             | 委任済み        | Access mailboxes as the signed-in user via Exchange W...   | いいえ       | ***             |
| MailboxSettings.ReadWrite        | アプリケーション... | Read and write all user mailbox settings                   | はい        | に付与されていま... *** |
| People.Read.All                  | アプリケーション... | Read all users' relevant people lists                      | はい        | に付与されていま... *** |
| Place.Read.All                   | アプリケーション... | Read all company places                                    | はい        | に付与されていま... *** |
| User.Read                        | 委任済み        | Sign in and read user profile                              | いいえ       | ***             |
| User.Read.All                    | アプリケーション... | Read all users' full profiles                              | はい        | に付与されていま... *** |
| ▼ Office 365 Exchange Online (1) |             |                                                            |           |                 |
| full_access_as_app               | アプリケーション... | Use Exchange Web Services with full access to all mailb... | はい        | に付与されていま... *** |

- 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



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

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

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

ホーム > ontimedemo > OnTimeAuth-from-420

OnTimeAuth-from-420 | API のアクセス許可 ✕

検索 (Ctrl+/) << 最新の情報に更新 フィードバックがある場合

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 ロール

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。

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

構成されたアクセス許可

アプリケーションは、同意のプロセスの一環としてユーザーが管理者からアクセス許可が付与されている場合、API を呼び出すことが承認されます。構成されたアクセス許可の一覧には、アプリケーションに必要なすべてのアクセス許可を含める必要があります。 [アクセス許可と同意に関する詳細情報](#)

+ アクセス許可の追加 ☒ ontimedemo に管理者の同意を与えます

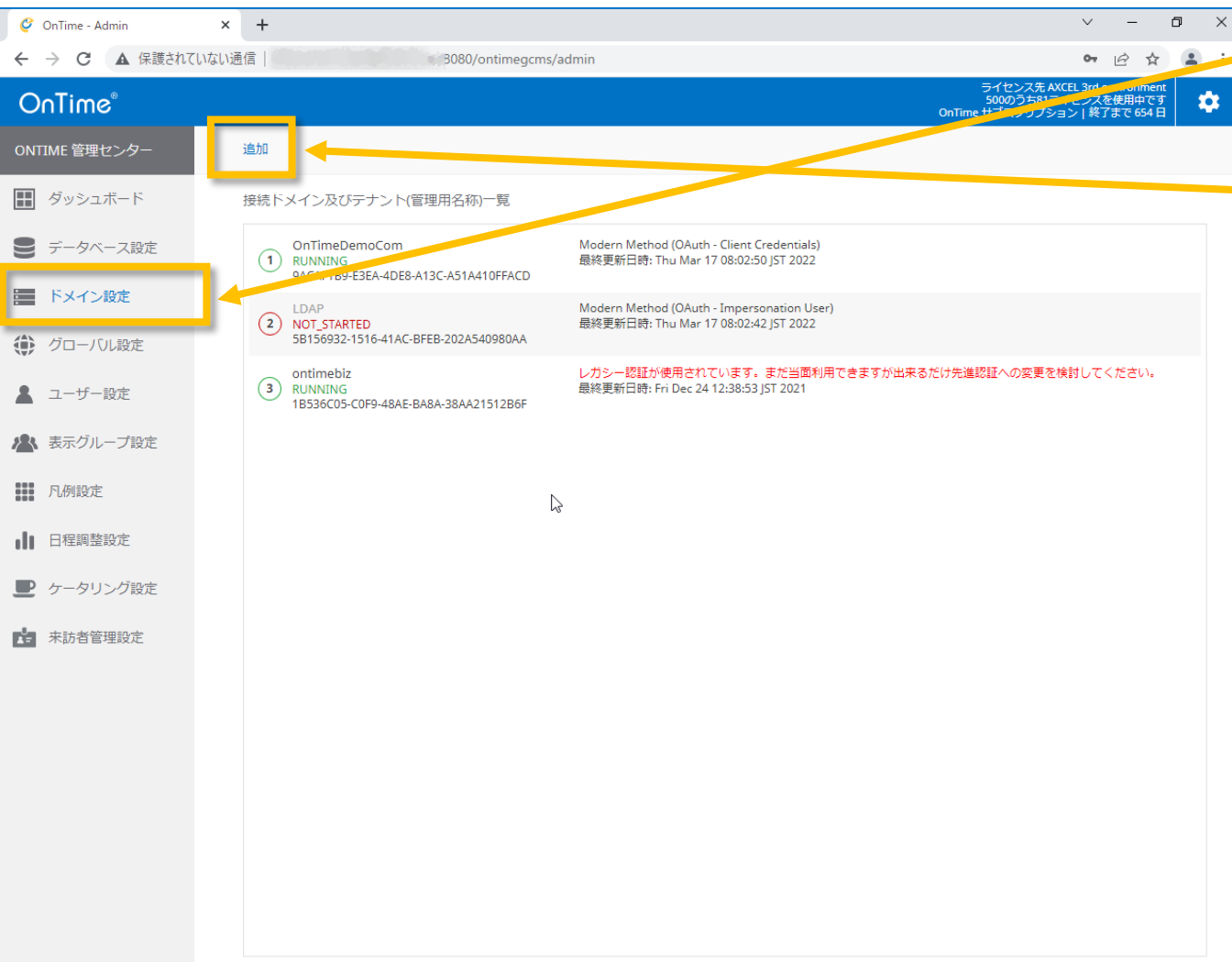
| API / アクセス許可の名前                  | 種類          | 説明                                                         | 管理者の同意が必要 | 状態         |
|----------------------------------|-------------|------------------------------------------------------------|-----------|------------|
| ▼ Microsoft Graph (8)            |             |                                                            |           |            |
| Calendars.ReadWrite              | アプリケーション... | Read and write calendars in all mailboxes                  | はい        | ✓ に付与されました |
| Directory.Read.All               | アプリケーション... | Read directory data                                        | はい        | ✓ に付与されました |
| EWS.AccessAsUser.All             | 委任済み        | Access mailboxes as the signed-in user via Exchange W...   | いいえ       | ✓ に付与されました |
| MailboxSettings.ReadWrite        | アプリケーション... | Read and write all user mailbox settings                   | はい        | ✓ に付与されました |
| People.Read.All                  | アプリケーション... | Read all users' relevant people lists                      | はい        | ✓ に付与されました |
| Place.Read.All                   | アプリケーション... | Read all company places                                    | はい        | ✓ に付与されました |
| User.Read                        | 委任済み        | Sign in and read user profile                              | いいえ       | ✓ に付与されました |
| User.Read.All                    | アプリケーション... | Read all users' full profiles                              | はい        | ✓ に付与されました |
| ▼ Office 365 Exchange Online (1) |             |                                                            |           |            |
| full_access_as_app               | アプリケーション... | Use Exchange Web Services with full access to all mailb... | はい        | ✓ に付与されました |

- 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



OnTime - Admin

com:8080/ontimegcms/admin

ライセンス先 AXCEL 3rd environment  
500のうち68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 380 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 | 削除

ドメイン設定

名前(管理用名称)  ☐ このドメインを無効

優先順位(メールが同じ場合)

接続先Exchange

認証タイプ

セキュリティユーザー

Proxy

ホスト名

ポート番号

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(機)

追加設定が必要なアクセス許可

ドメイン名はOnTime 管理センターで識別しやすい名前をつけます。通常はテナント名です。  
優先順位は複数テナント時に同じメールアドレスが使用されている場合にどのテナントを優先するかを指定します。

一時的に接続しない場合は無効にできます。

接続先ExchangeでExchange OnlineかオンプレExchangeを選択します。Microsoft365(Exchange Online)の場合は「Exchange Online」を選択します。  
オンプレExchangeの設定は補足 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)に必要な各種IDや値を入力します。  
メモ帳にコピーした3つのテキストを貼り付けます。
- 「アプリケーションID」「ディレクトリID」「クライアントシークレット」の3つを入力後、作成したアプリケーションに対して付与された「APIのアクセス許可」に不備があると、赤字で何が足りていないか表示されます。  
赤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タブーProxy Proxyを利用する場合の設定



OnTime - Admin

com:8080/ontimegcm/admin

ライセンス先 AXCEL 3rd environment  
500のうち68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 380 日

保存 | キャンセル | 「アプリの登録」を開く | 削除

ドメイン設定

名前(管理用名称) OnTimeDemoCom ☐ このドメインを無効

優先順位(メールが同じ場合) 1

接続先Exchange Exchange Online

Exchange Online 同期対象 属性マッピング 高度な設定

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

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

**Proxy**

ホスト名

ポート番号

接続テスト

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

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

クライアントシークレット(他) .....

追加設定が必要なアクセス許可

- 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。

# 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で運用のメンテナンスが容易です。

ユーザーグループ: OnTimeUsers@ontimedemo.com

会議室グループ: OnTimeRooms@ontimedemo.com

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

備品グループ: OnTimeEquipment@ontimedemo.com

- 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。





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

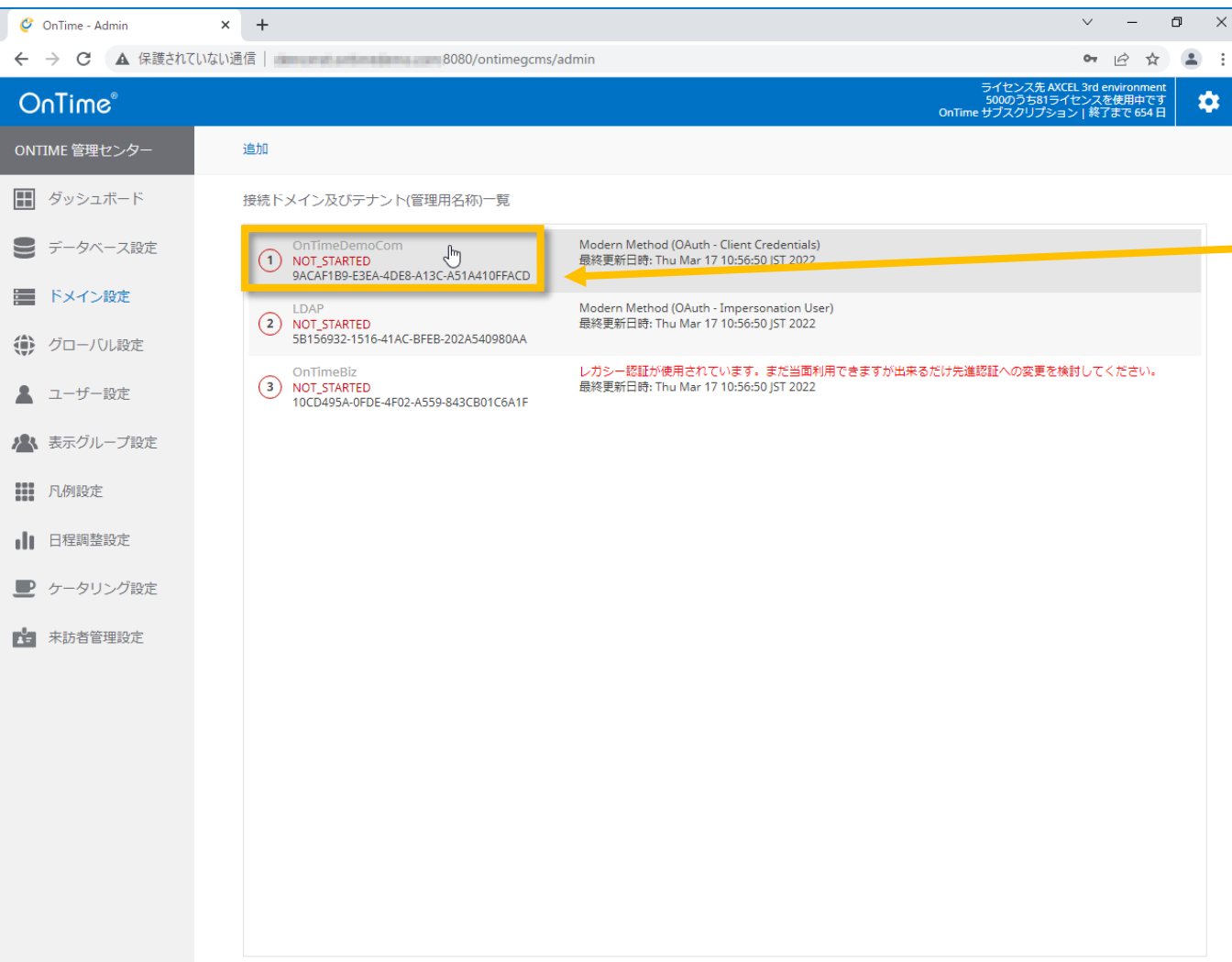
# 高度な設定タブ



- 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。

# 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きます。

アプリケーションを再起動するまで“NOT\_STARTED”と表示されます。  
修正する場合はクリックすることで編集画面が表示されます。修正した場合はOnTimeアプリケーションの再起動が必要です。

- アプリケーションを再起動するためには“ダッシュボード”に移動します。

# ダッシュボードで再起動



- 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。



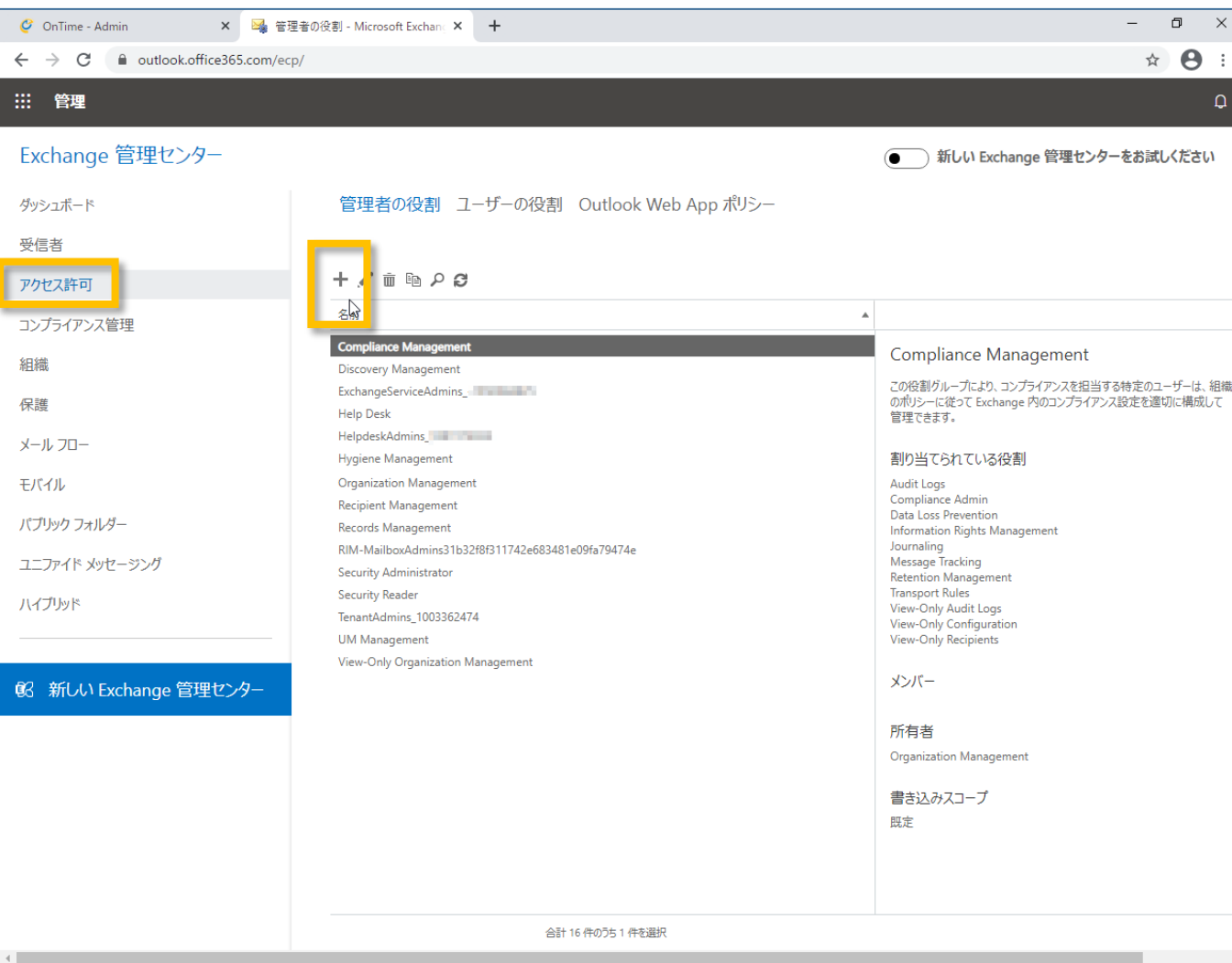
# 補足1) 認可コードフロー認証方式の設定

# 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。

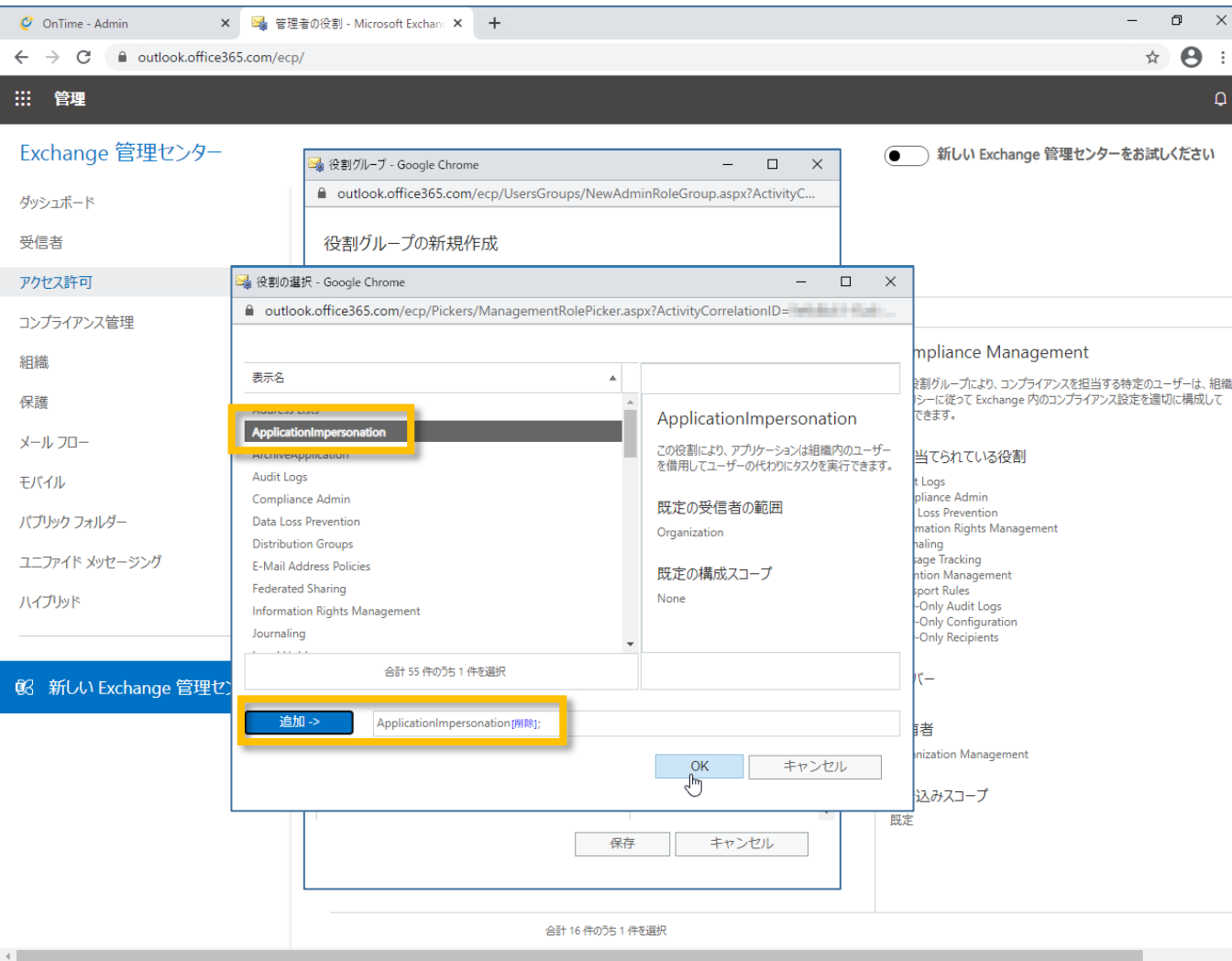
# 管理者の役割の追加 1



- 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



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   |
| otsync | otsync |

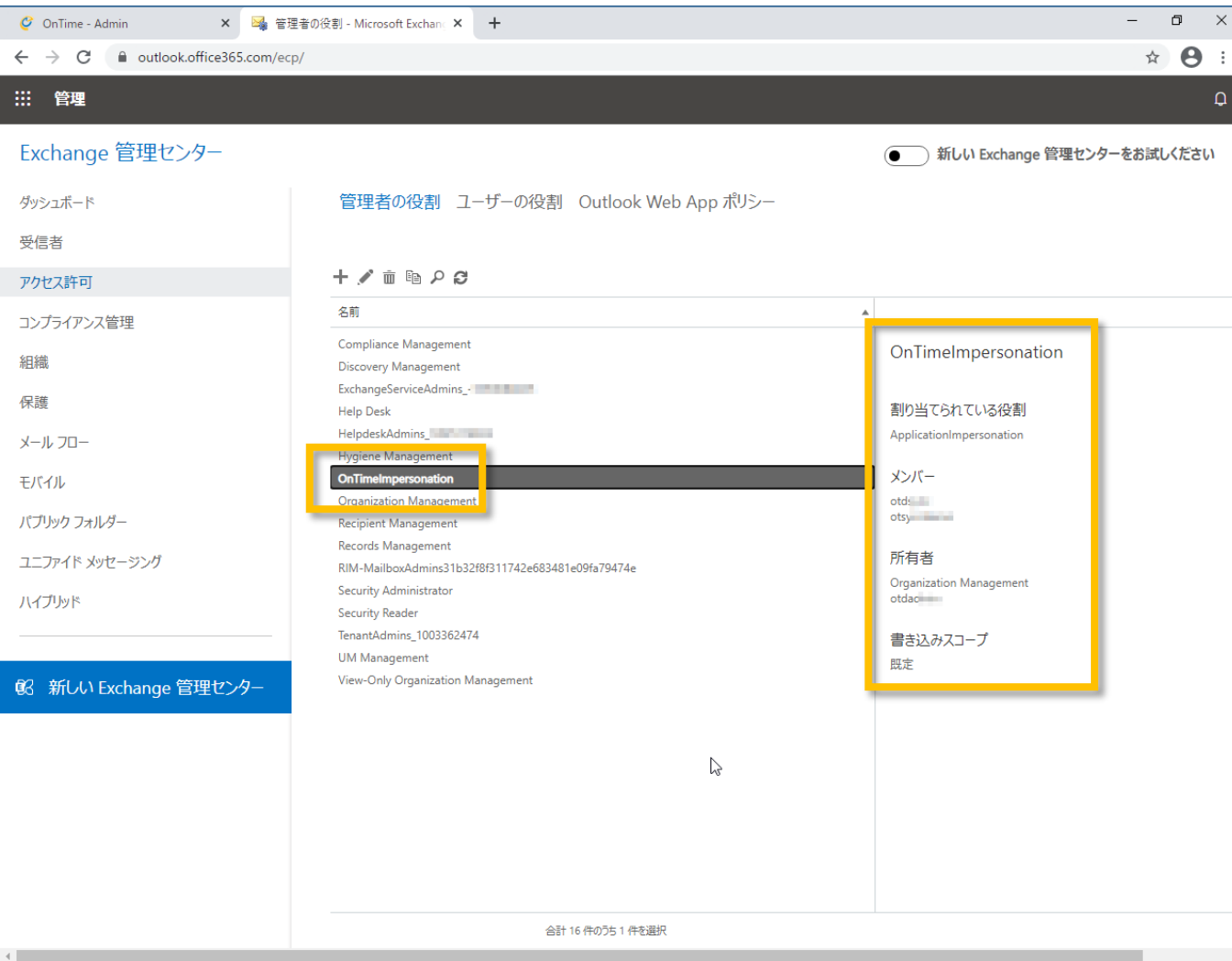
この役割グループのメンバーを選びます。  
[詳細情報](#)

保存 キャンセル

合計 16 件のうち 1 件を選択

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

# 管理者の役割の追加 4



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



# 補足2) オンプレExchangeの設定

# オンプレExchange へのEWS接続



OnTime - Admin

com:8080/ontimegcmcs/admin

ライセンス先 AXCEL 3rd environment  
500のうち68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 380 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

ドメイン設定

名前(管理用名称)  ☐ このドメインを無効

優先順位(メールが同じ場合)

接続先Exchange

**オンプレ Exchange** | 同期対象 | 属性マッピング | 高度な設定

Impersonation User

パスワード

ドメイン

Exchangeサーバー

EWS URL

Autodiscover URL

接続先Exchange

Proxy

ホスト名

ポート番号

Teamsを利用

- 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 - Admin

com:8080/ontimegcms/admin

ライセンス先 AXCEL 3rd environment  
500のうち68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 380 日

保存 | キャンセル | 「アプリの登録」を開く | 削除

ドメイン設定

名前(管理用名称) LDAP ☒ このドメインを無効

優先順位(メールが同じ場合) 2

接続先Exchange Exchange Online

Exchange Online 同期対象 属性マッピング 高度な設定

LDAP ☒ LDAPを有効にする

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

ユーザー CN=Users, DC=ontime, DC=otbz

パスワード \*\*\*\*\* テスト

ベース OU=o365, DC=ontime, DC=otbz

スコープ SUB\_TREE

フィルター (cn=OnTimeRooms)

共有席 ☐ はい テスト

ベース OU=o365, DC=ontime, DC=otbz

スコープ SUB\_TREE

フィルター (mail=OnTimePersons)

- OnTimeはExchangeと連携しているActive DirectoryからLDAP(S)により同期対象を指定することもできます。
- LDAP(S)を使用することで例えばフリガナ属性やカスタム属性1～15なども取得してOnTimeで活用できます。
- Microsoft365のExchange Online接続であってもAzureAD Connectを使用してAD連携しているのであれば利用可能です。
- ちなみにOnTimeは複数のテナントと接続することも可能です。よってActive DirectoryはOnTimeが稼働するテナントである必要はありません。LDAP(S)で接続できればいずれのテナントも利用可能です。

“LDAPを有効にする”のチェックをします。



# 同期対象をLDAPで取得 2



OnTime - Admin

com:8080/ontimegcms/admin

ライセンス先 AXCEL 3rd environment  
500のうち68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 380 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

ドメイン設定

名前(管理用名称) LDAP ☐ このドメインを無効

優先順位(メールが同じ場合) 2

接続先Exchange Exchange Online

Exchange Online 同期対象 属性マッピング 高度な設定

LDAP ☒ LDAPを有効にする

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

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

パスワード \*\*\*\*\*

テスト

ベース OU=o365, DC=ontime, DC=otbz

スコープ SUB\_TREE

フィルター (cn=OnTimeRooms)

共有席 ☐ はい

テスト

ベース OU=o365, DC=ontime, DC=otbz

スコープ SUB\_TREE

フィルター (mail=OnTimePersons)

- 同期対象の設定を行います。

Active DirectoryへのLDAP接続用アカウントの設定です。  
事前にldp.exe等で接続確認を行ってください。

接続先ドメインの ユーザー、会議室、備品のそれぞれを検  
索するフィルター条件を指定してください。  
次ページにサンプルがあります。

設定後は「保存」をクリックします。

# 同期対象をLDAPで取得 3



同期対象

LDAP ☒ LDAPを有効にする

URL

ユーザー

パスワード

ベース

スコープ

フィルター

ベース

スコープ

フィルター

☒ LDAPを有効にする

URL

ユーザー

パスワード

ベース

スコープ

フィルター

ベース

スコープ

フィルター

- 左図を参考に組織に応じたフィルター条件で取得してください。
- 左上 特定の属性に値があるアカウントを全て取得
- 右下 特定のグループに属しているアカウントを全て取得
- 取得したリストにグループが含まれている場合はそのグループをロール設定などで利用できます。



# 補足4) Graphで認証エラーが出る

# ドメイン接続がエラーで接続できない



OnTime - Admin

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

ONTime 管理センター

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: Thu Mar 17 11:02:02 JST 2022 |
| 有効なライセンスの確認: | RUNNING | 実行 | 停止 | 最終実行日時: Thu Mar 17 11:02:03 JST 2022 |

接続状況

|              |               |  |  |                                      |
|--------------|---------------|--|--|--------------------------------------|
| SQL DB 接続状況: | RUNNING       |  |  | 最終実行日時: Thu Mar 17 11:02:02 JST 2022 |
| ドメイン 接続状況:   | 1 / 2 RUNNING |  |  |                                      |

同期スケジュール

|               |                                 |    |  |                                      |
|---------------|---------------------------------|----|--|--------------------------------------|
| ディレクトリ 同期:    | SCHEDULED TO RUN 09:00          | 実行 |  | 最終実行日時: Thu Mar 17 09:00:17 JST 2022 |
| ユーザーとグループ 同期: | SCHEDULED TO RUN 09:00          | 実行 |  | 最終実行日時: Thu Mar 17 09:00:24 JST 2022 |
| 写真 同期:        | SCHEDULED TO RUN 09:00          | 実行 |  | 最終実行日時: Thu Mar 17 09:01:05 JST 2022 |
| アクセス権 同期:     | SCHEDULED TO RUN 09:00          | 実行 |  | 最終実行日時: Thu Mar 17 09:00:58 JST 2022 |
| カレンダー 同期:     | SCHEDULED TO RUN TOMORROW 09:00 | 実行 |  | 最終実行日時: Thu Mar 17 09:01:07 JST 2022 |

日程調整

|              |         |  |  |  |
|--------------|---------|--|--|--|
| アプリケーション:    | RUNNING |  |  |  |
| SQL DB 接続状況: | OK      |  |  |  |

ケータリング

- インジケ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



OnTime - Admin

3080/ontimegcms/admin

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

OnTime®

ONTIME 管理センター

追加

接続ドメイン及びテナント(管理用名称)一覧

|   |                                                                  |                                                                                                                                                                 |
|---|------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | OnTimeDemoCom<br>STOPPED<br>9ACAF1B9-E3EA-4DE8-A13C-A51A410FFACD | エラー:<br>com.ontimesuite.ontime.ms.v2.web.api.v2.Api2ErrorException: Error: ClientCredentials fetch access token failed!<br>最終更新日時: Thu Mar 17 11:02:02 JST 2022 |
| 2 | LDAP<br>NOT_STARTED<br>5B156932-1516-41AC-BFEB-202A540980AA      | Modern Method (OAuth - Impersonation User)<br>最終更新日時: Thu Mar 17 11:02:02 JST 2022                                                                              |
| 3 | OnTimeBiz<br>RUNNING<br>10CD495A-0FDE-4F02-A559-843CB01C6A1F     | レガシー認証が使用されています。まだ当面利用できますが出来るだけ先進認証への変更を検討してください。<br>最終更新日時: Thu Mar 17 11:02:02 JST 2022                                                                      |

ダッシュボード

データベース設定

ドメイン設定

グローバル設定

ユーザー設定

表示グループ設定

凡例設定

日程調整設定

ケータリング設定

来訪者管理設定

- 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

com:8080/ontimegcms/admin

ライセンス先 AXCEL 3rd environment  
500のうち68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 377 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 | 削除

ドメイン設定

名前(管理用名称) OnTimeDemoCom ☐ このドメインを無効

優先順位(メールが同じ場合) 1

接続先Exchange Exchange Online

Exchange Online 同期対象 属性マッピング 高度な設定

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

Impersonation User otdsync@ontimedemo.onmicrosoft.com

パスワード (present)

Proxy

ホスト名

ポート番号

接続テスト

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

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

クライアントシークレット(値) .....

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

- 追加で必要となるアプリのアクセス許可が表示されています。
- AzureADの「アプリの追加」に戻り、必要となるアクセス許可を追加した後、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。