# Microsoft ID の実装 (パート 2)

- 認証を実装する
- 承認を実装する

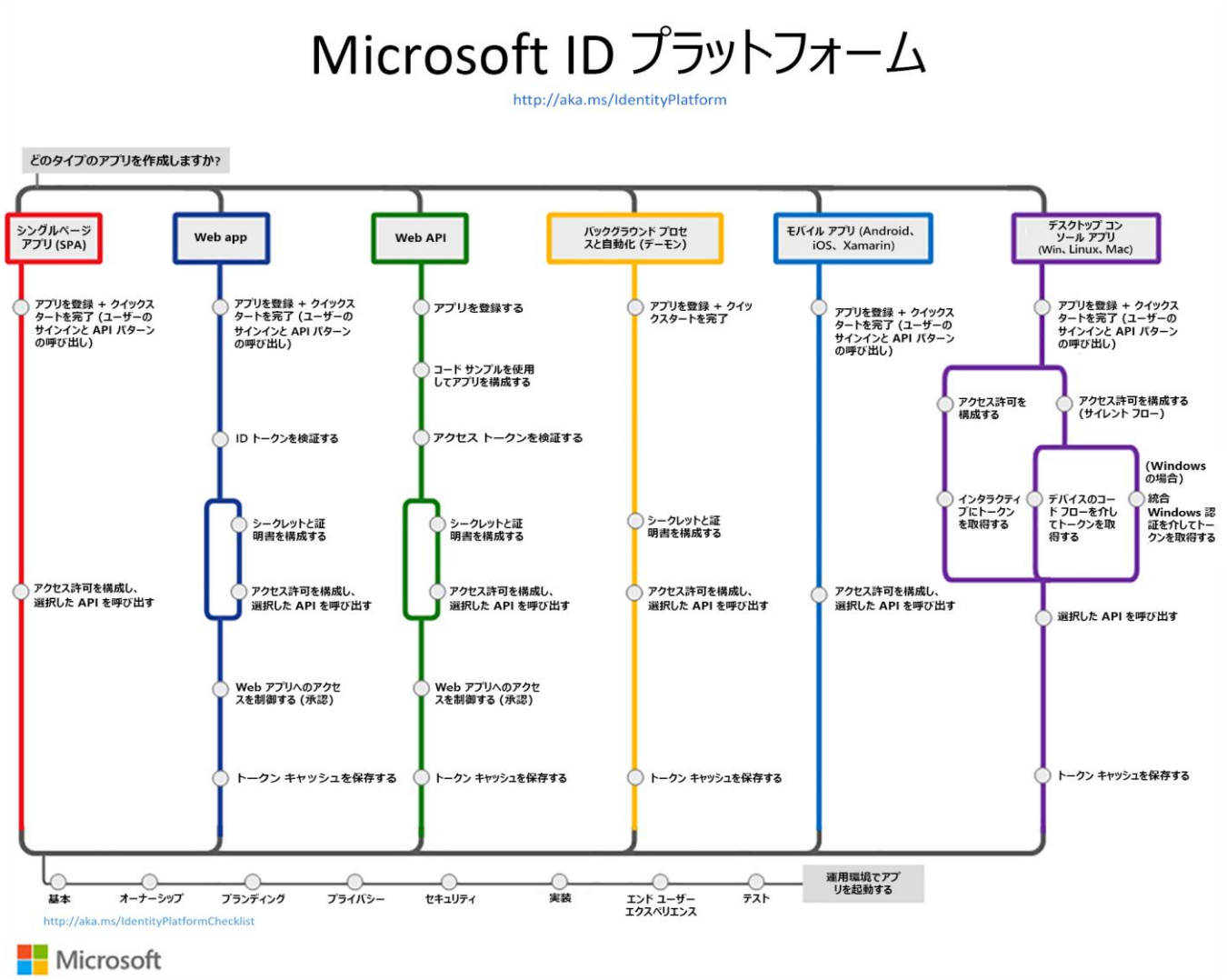
Microsoft

# 認証を実装する

# 認証フローとアプリケーションのシナリオ

## 認証カテゴリ

- 保護されたリソースとクライアント アプリケーション
- ユーザーありまたはユーザーなし
- シングルページ、パブリック クライアント、および機密性の高いクライアント アプリケーション
- サインイン対象者
- サポートされている OAuth 2.0 フロー
- サポート対象のプラットフォーム



# Microsoft Authentication Library (MSAL)

Microsoft 認証ライブラリ (MSAL) を使用すると、開発者は Microsoft ID プラットフォーム エンドポイントからトークンを取得して、セキュリティで保護された Web API にアクセスできます。

- アプリケーションのタイプとシナリオ。
- 言語とフレームワーク。

# Microsoft ID のセキュリティ トークン

- ID トークン

ID トークンは、クライアントがユーザーの ID を確認できるようにするセキュリティ トークンです。

- アクセス トークン

アクセス トークンを使用すると、クライアントは Azure AD によって保護された API を安全に呼び出すことができます。アクセス トークンは、「User+App」または「App-Only」と呼ばれることもあります。

# デモ

認証の実装

Microsoft

# 承認を実装する

# 承認モデルの概要

Microsoft ID プラットフォームと統合されたアプリケーションは、ユーザーと管理者がデータへのアクセス方法を制御できる承認モデルに従います。

- OAuth 2.0 承認コード フロー
- スコープとアクセス許可
- 委任とアプリケーションのアクセス許可
  - 効果的なアクセス許可
- テナント全体の同意の要求
- 管理者が制限するアクセス許可

# 管理者の同意

- 一部のアクセス許可をテナント内で付与するには、管理者の同意が必要です。また、管理者の同意エンドポイントを使用すると、テナント全体にアクセス許可を付与できます。
- アプリ登録 UI には、アプリに付与されたアクセス許可と管理者の同意が表示されます。これには以下のセクションがあります。
  - 構成済みのアクセス許可
  - 付与されたその他のアクセス許可
  - [管理者の同意] ボタン
- ディレクトリ管理者にアクセス許可を要求します。
- アプリケーション承認の同意について理解します。

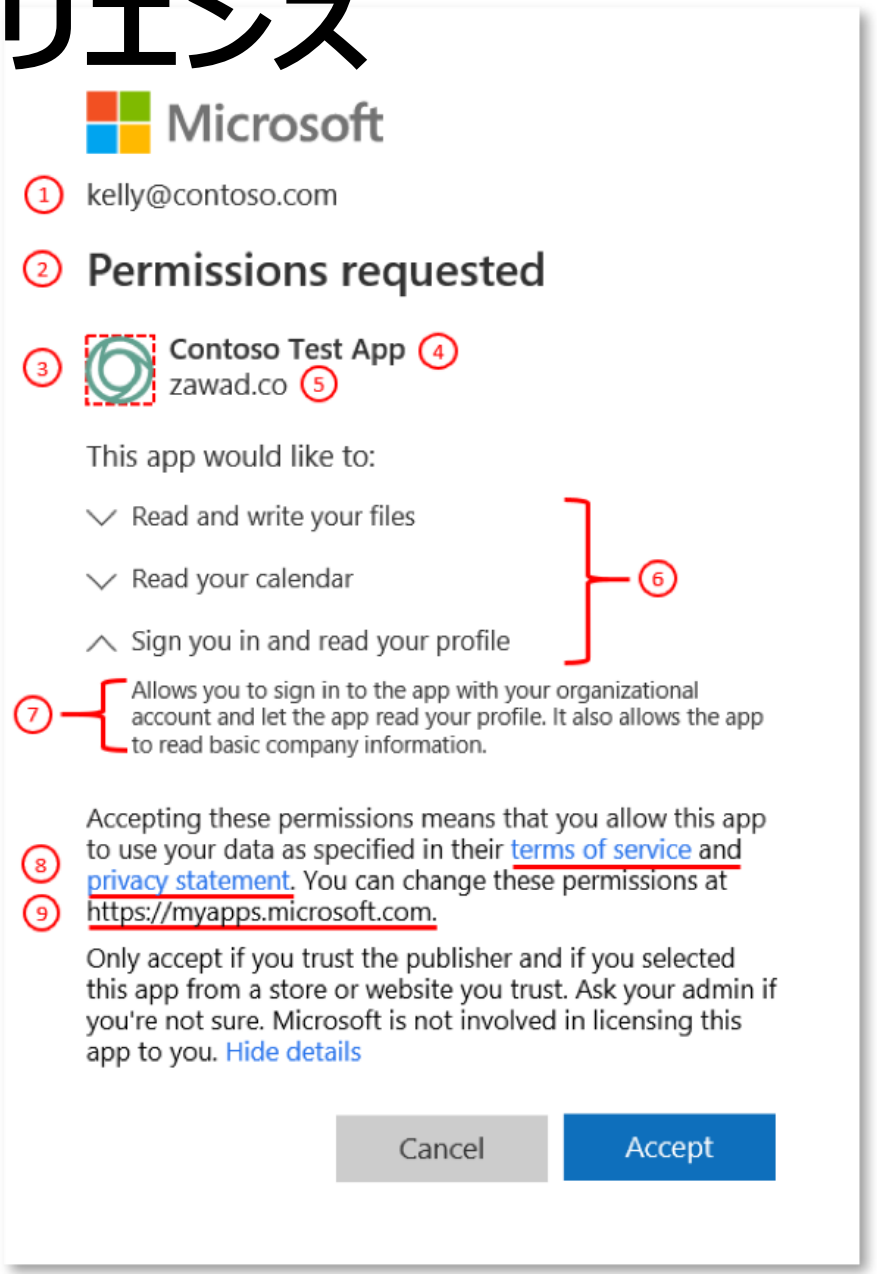
# アプリケーションの同意のエクスペリエンス

・ユーザーの同意の流れ

アプリケーション開発者が、現在のユーザーのみの同意を記録する目的でユーザーを承認エンドポイントに誘導する場合。

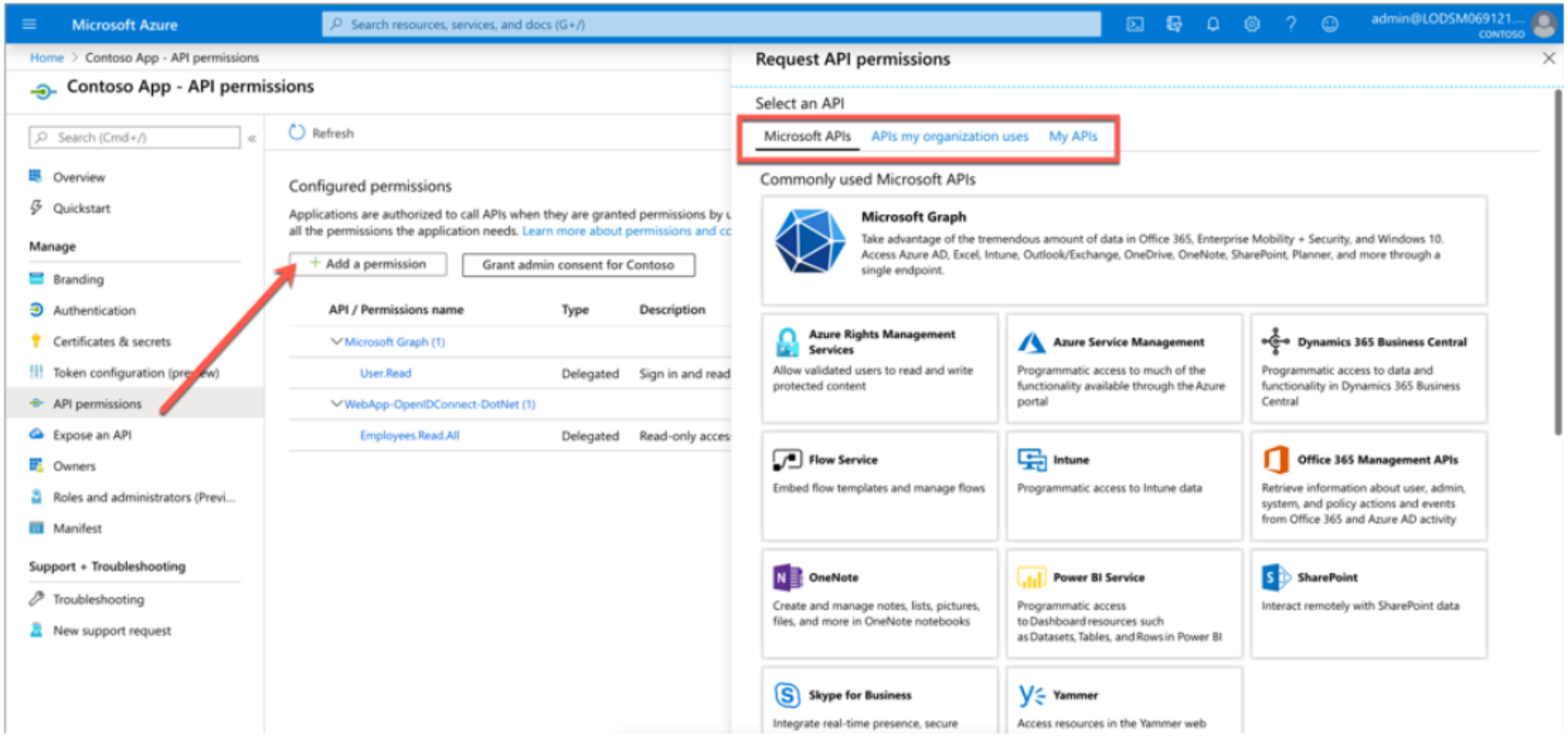
・管理者の同意の流れ

アプリケーション開発者が、テナント全体の同意を記録する目的でユーザーを管理者同意エンドポイントに誘導する場合。管理者の同意フローが適切に機能するよう保証するには、アプリケーション開発者がアプリケーション マニフェストの RequiredResourceAccess プロパティにすべてのアクセス許可をリストする必要があります。



# Web API にアクセスするためのアクセス許可を追加する

- Microsoft API
- 組織で使用する API
- 自分の API



# Microsoft ID でカスタム API を保護する

他のアプリケーションから呼び出すことができる Microsoft ID を使用して Web API を保護するには、主に次の 2 つのタスクを実行する必要があります。

- Azure AD アプリケーションを登録して構成する
  - スコープを定義する
- Microsoft ID をサポートするように構成された Web API プロジェクトをコーディングする
  - 現在の要求に必要なスコープが含まれていることを検証するサポートを追加する

# Microsoft Graph API を呼び出す

Microsoft Graph API は、REST API エンドポイントを介して Azure AD へのプログラムによるアクセスを提供します。アプリケーションは、Microsoft Graph API を使用して、ディレクトリ データおよびオブジェクトに対して作成、読み取り、更新、および削除 (CRUD) 操作を実行できます。

- 以下の機能を提供します。
  - REST API エンドポイント
  - Azure AD による認証
  - ロールベースの承認 (RBAC)
  - 差分クエリ
  - ディレクトリ拡張
  - アクセス許可スコープによる保護
- 以下のようなアプリケーション シナリオを可能にします。
  - 基幹業務 (シングル テナント) アプリケーション
  - サービスとしてのソフトウェア (マルチテナント) アプリケーション

# デモ

API を使用するための承認の実装