顔検証または識別に Cognitive Services Face API を使用するには、**LargePersonGroup** または類似のデータ構造に顔を登録する必要があります。 この詳細情報では、ユーザーから有意義な同意を収集するためのベスト プラクティスと、認識精度を最適化する高品質の登録を作成するためのロジックの例を紹介します。

有意義な同意

顔認識用の登録アプリケーションの主な目的の 1 つは、仕事用サイトへのアクセスなどの特定の目的で自分の顔の画像を使用することに同意する機会をユーザーに提供することです。 顔認識テクノロジは、機密性の高い個人データを収集していると認識される可能性があるため、透明性が高く、相手を尊重する方法で同意を求めることが特に重要です。 同意は、ユーザーが自分にとって最適であると思える決断を下すことができる場合に、ユーザーにとって有意義なものとなります。

Microsoft ユーザー リサーチ、Microsoft の責任ある AI の原則、および外部調査を基に、ユーザーがテクノロジに登録するときに次のものが提供される場合に同意が有意義であることが判明しました。

- 認識: 自分の顔のテンプレートや登録写真を提供するよう求められているときに、ユーザーが何の疑いも持っていない。
- 理解: 誰によって、何のために、どのような保証によって、何を求められたかを、ユーザーが自分自身の言葉で正確に述べられる。
- 選択の自由: 顔認識に同意して登録するかどうかを選択するときに、強制されたり操作されているとユーザーが感じない。
- 制御: ユーザーは、いつでも同意を取り消してデータを削除できる。

このセクションでは、顔認識用の登録アプリケーションを開発するためのガイダンスを提供します。 このガイダンスは、建物に入るための顔認識に個人を登録するというコンテキストで、Microsoft ユーザー リサーチに基づいて開発されました。 したがって、これらの推奨事項は、すべての顔認識ソリューションに適用されるとは限りません。 Face API の責任ある使用は、それが統合されている特定のコンテキストに強く依存します。そのため、これらの推奨事項の優先順位付けと適用は、お客様のシナリオに合わせて調整してください。

[!NOTE] お客様の管轄区域で適用される法的要件に合わせて登録アプリケーションを調整し、データの収集および処理に関するすべてのプラクティスを正確に反映することは、お客様の責任となります。

アプリケーション開発

登録フローを設計する前に、データの保護方法についてユーザーに対して行う約束を、作成中のアプリケーションでどのように守れるかを検討してください。 次の推奨事項は、個人データの保護、ユーザーのプライバシー管理、すべてのユーザーがアプリケーションにアクセスできることの保証に対する責任ある取り組みが含まれた登録エクスペリエンスを構築するうえで役立ちます。

カテゴリ	**Recommendations**
ハードウェア	登録デバイスのカメラの品質を考慮します。
推奨される登	多要素認証を使用したログオン手順を含めます。

カテゴリ	Recommendations
登録機能	エイリアスや識別番号などのユーザー情報を Face API の顔テンプレート ID とリンクします (人物 ID と呼ばれます)。 このマッピングは、ユーザーの登録を取得して管理するために必要です。 注: 人物 ID は、アプリケーションでシークレットとして扱う必要があります。 顔認識テクノロジのユーザーではなくなった人物 (たとえば、元従業員) の顔テンプレートや登録写真など、すべての登録データを削除する自動プロセスを設定します。 自動登録は、同意を得るために推奨されている認識、理解、選択の自由、または制御がユーザーに提供されないため、避けてください。 登録に使用される画像の保存を許可するようユーザーにお願いします。 モデルの更新がある場合は、約 10 か月ごとに新しいモデルに再登録するために新しい登録写真が必要になるので、これが役立ちます。 元の画像が保存されていない場合、ユーザーは登録プロセスを最初から実行する必要があります。 ユーザーがシステムに写真を保存しないことを選択できるようにします。 選択をより明確にするために、登録写真の保存に関する 2 番目の同意要求画面を追加できます。 写真が保存されている場合は、モデルの更新があった場合にすべてのユーザーを再登録する自動プロセスを作成します。登録写真を保存したユーザーは、自身を再度登録する必要はありません。 ユーザーの登録がうまくいかない場合に、指定された管理者が特定の品質フィルターをオーバーライドできるようにするアプリ機能を作成します。
セキュリティ	Cognitive Services は、保存中および転送中のユーザー データの暗号化に関してベスト プラクティスに従います。 次に示すのは、登録エクスペリエンス中にユーザーに対して行うセキュリティの約束を守るうえで役立つその他のプラクティスです。 登録中のいかなる時点でも誰も人物 ID にアクセスできないようにするためのセキュリティ対策を講じます。 注:PersonID は、登録システムでシークレットとして扱う必要があります。 Cognitive Services でロールベースのアクセス制御を使用します。 データベースなどのリソースにアクセスするには、キーとシークレットに加えて、トークンベースの認証または Shared Access Signature (SAS) あるいはその両方を使用します。 要求または SAS のトークンを使用すると、アカウント キーを侵害せずに、データへの制限付きアクセスを許可できます。また、トークンの有効期限を指定することもできます。 シークレット、キー、またはパスワードは、決してアプリに保存しないでください。
ユーザーのプライバシー	さまざまなレベルのプライバシーに対する懸念に対処するために、幅広い登録オプションを提供します。 顔認識システムに登録するために、ユーザーが自分の個人用デバイスを使用することを義務付けないでください。 理由の如何にかかわらずいつでも、ユーザーが再登録、同意の取り消し、および登録アプリケーションからのデータの削

カテゴリ	Recommendations
	除をできるようにします。
アクセシビリティ	アクセシビリティの標準 (たとえば、ADA または W3C) に従って、運動または視覚に障碍があるユーザーがアプリケーションを使用できるようにします。

次のステップ

登録アプリの構築に関するガイドに従って、サンプル登録アプリを開始します。 その後、お使いの製品のニーズに合わせてそれをカスタマイズしたり、独自のアプリを作成したりします。