

Azure AI Face サービスとは

[アーティクル] • 2024/09/03

Azure AI Face サービスは、画像に含まれている人の顔の検出、認識、分析する AI アルゴリズムを提供します。顔認識ソフトウェアは、本人識別、タッチレス アクセス制御、プライバシーのための自動顔ぼかしなど、さまざまなシナリオで重要となります。

Face サービスは、クライアント ライブラリ SDK を通じて、または REST API を直接呼び出すことで使用できます。使用を開始するには、クイックスタートに従ってください。

クイックスタート

または、Vision Studio を使用して、ブラウザーですばやく簡単に Face サービスの機能を試すことができます。

Vision Studio for Face を試す

⊗ 注意事項

Microsoft の責任ある AI の原則をサポートするために、Face サービスの利用は、適格性と使用基準に基づいて制限されています。Face サービスは、Microsoft が管理する顧客とパートナーのみが利用できます。[顔認識受付フォーム](#) [🔗] を使用して利用申請を行ってください。詳細については、「[Face の制限付きアクセス](#)」ページを参照してください。

このドキュメントには、次のような記事が記載されています。

- [クイックスタート](#)は、サービスの呼び出しと結果の取得を短時間で行えるようにする、ステップバイステップの手順です。
- [攻略ガイド](#)には、より具体的またはカスタマイズした方法でサービスを使用するための手順が記載されています。
- [概念の記事](#)では、サービスの機能と特長について詳しく説明します。
- [チュートリアル](#)はより長文のガイドであり、より広範なビジネス ソリューションの 1 コンポーネントとしてこのサービスを使用する方法を示すものです。

より構造化されたアプローチについては、Face の次のトレーニング モジュールに従ってください。

- [Face サービスを使用した顔の検出と分析](#)

ユース ケースの例

Face サービスの一般的なユース ケースを以下に示します。

ユーザー ID の確認: 信頼できる顔画像と比較してユーザーを検証します。この検証は、銀行口座、建物へのアクセスなど、デジタルまたは物理的な所有物へのアクセスを許可するために使用できます。ほとんどの場合、信頼できる顔画像は、パスポートや運転免許証などの政府発行の ID から取得するか、本人が撮影した登録写真から取得することができます。検証中、ライブネス検出は、画像が印刷された写真やマスクではなく、実際の人物の画像であることを確認する上で重要な役割を果たすことができます。ライブネスでの検証の詳細については、[ライブネスのチュートリアル](#)を参照してください。ライブネスのない ID 検証については、[クイックスタート](#)に従ってください。

ライブネス検出: ライブネス検出は、ユーザーがカメラの前に物理的に存在するかどうかをチェックするスプーフィング対策機能です。これは、印刷写真、録画ビデオ、またはユーザーの顔の 3D マスクを使用するスプーフィング攻撃を防ぐために使用されます。[ライブネス チュートリアル](#)

タッチレス アクセス制御: カードやチケットのような昨今の方法と比較した場合、オプトインの顔認識を使用すると、カードの共有、損失、盗難による衛生上ならびにセキュリティ上のリスクを軽減しながら、アクセス制御エクスペリエンスを向上できます。顔認識は、空港、スタジアム、テーマパーク、建物へのチェックイン時や、オフィス、病院、ジム、クラブ、学校の受付キオスクで、人間のチェックイン プロセスに役立ちます。

顔編集: プライバシーを保護するため、ビデオに記録された人の顔を編集またはぼかします。

⚠ 警告

2020 年 6 月 11 日に、Microsoft は、人権に基づく厳格な法令が制定されない限り、米国内の警察に顔認識テクノロジーを販売しないことを発表しました。このため、顧客は、米国内の警察である場合、または警察による顔認識機能および Azure サービスに含まれる機能 (Face や Video Indexer など) の使用を許可する場合、これらの機能を使用できません。新しい Face リソースを作成する際には、Azure portal で、サービスを米国の警察で、もしくは警察のために使用しないこと、および責任ある AI のドキュメントを確認し、それに従ってこのサービスを使用することに同意する必要があります。

顔検出と分析

顔検出は、他のすべてのシナリオの最初の手順として必要です。Detect API では、画像に含まれている人の顔を検出し、その位置の四角形の座標を返します。また、保存されている顔データを表す一意の ID も返されます。これは、後の操作で顔を識別または検証するために使用されます。

顔検出では、オプションとして、頭部姿勢、年齢、感情、ひげ、眼鏡などの顔関連の属性を抽出できます。これらの属性はおおよその予測であって、実際の分類ではありません。一部の属性は、ユーザーが自身を Face サービスに追加するときに、アプリケーションが高品質の顔データを取得するために役立ちます。たとえば、ユーザーがサングラスをかけている場合、アプリケーションで、サングラスを外すようにユーザーに伝えることができます。

⊗ 注意事項

Microsoft は、感情の状態や ID 属性の推測に使用できる顔認識機能を廃止または制限しています。この機能が誤って使用されると、人々が固定観念的な見方、差別、不当なサービス拒否にさらされる恐れがあります。廃止された機能は、感情と性別です。制限付き機能は、年齢、スマイル、顔ひげ、髪、メイクです。制限付き機能のいずれかの使用によってメリットが得られる責任あるユースケースがある場合は、[Azure Face API](#) をメールで送信してください。この決定について詳しくは、[こちら](#) をご覧ください。

顔検出と分析の詳細については、[顔検出](#)の概念に関する記事を参照してください。また、[Detect API](#) リファレンス ドキュメントも参照してください。

Vision Studio を使用して、ブラウザーですばやく簡単に顔検出を試すことができます。

[Vision Studio for Face を試す](#)

ライブネス検出

① 重要

ライブネス用の Face クライアント SDK は、ゲートされたフィーチャーです。[顔認識の取り込みフォームに](#) を入力して、ライブネスフィーチャーへのアクセスを要求する必要があります。Azure サブスクリプションにアクセス権が付与されたら、Face liveness SDK をダウンロードできます。

Face Liveness 検出を使用して、入力ビデオ ストリーム内の顔が実際の顔 (ライブ) か偽の顔 (スプーフィング) かを判断できます。これは、写真、ビデオ、マスク、またはその他の手段を使用してシステムにアクセスしようとする詐欺師からスプーフィング攻撃を防ぐために、生体認証システムの重要な構成ブロックです。

ライブネス検出の目的は、認証時にシステムが物理的に存在するライブユーザーと対話していることを確認することです。このようなシステムは、デジタル ファイナンス、リモート アクセスの制御、オンライン 本人確認プロセスの増加に伴ってますます重要になっています。




ライブネス検出ソリューションは、紙のプリントアウト、2d/3d マスク、スマートフォンやラップトップ上のスプーフィング プレゼンテーションなど、さまざまな種類のスプーフィングから正常に保護します。ライブネス検出は、時間の経過と共にますます高度なスプーフィング攻撃に対抗するために継続的な改善が行われている研究のアクティブな領域です。クライアントとサービス コンポーネントに継続的な改善がロールアウトされることで、ソリューション全体が新しい種類の攻撃に対してより堅牢になっています。

当社のライブネス検出ソリューションは、iBeta レベル 1 および 2 の ISO/IEC 30107-3 標準に準拠しています。

チュートリアル

- [Face liveness チュートリアル](#)の概念
- [不正使用の監視](#)

Face liveness SDK リファレンス ドキュメント:

- [Java \(Android\)](#) 
- [Swift \(iOS\)](#) 
- [JavaScript \(Web\)](#) 

顔認識操作

最新の企業やアプリでは、Face Verification ("1 対 1" 照合) や Face Identification ("1 対多" 照合) などの顔認識テクノロジーを使用して、ユーザーが主張する本人であることを確認できます。

① 重要

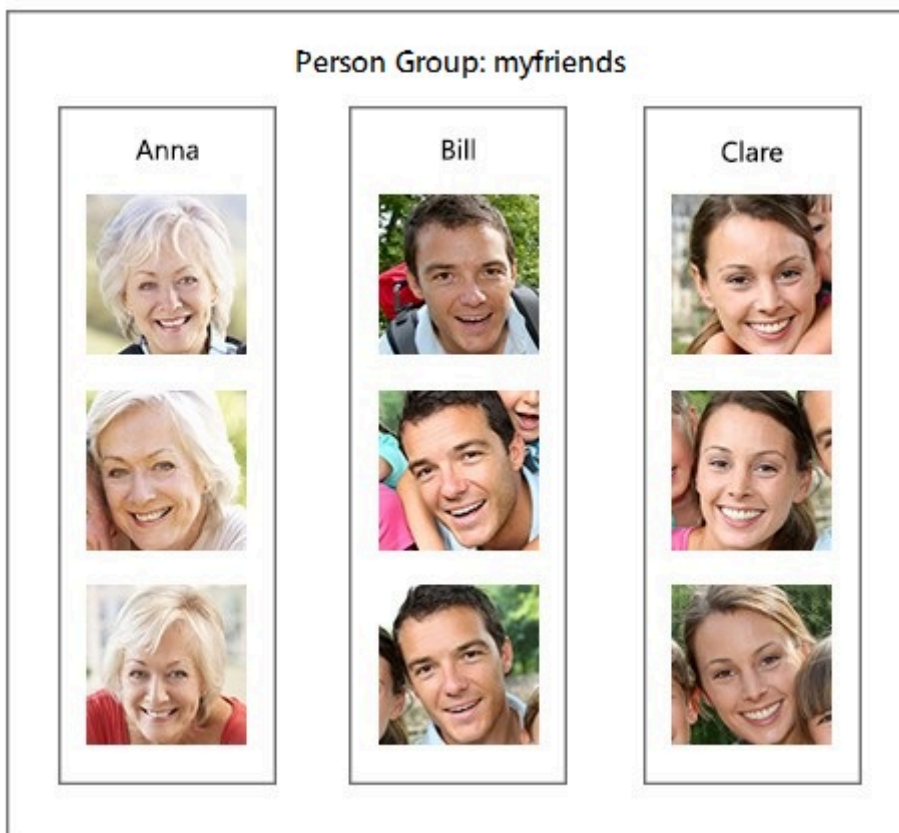
Microsoft 製品またはサービスを使用して生体認証データを処理する場合は、お客様の責任において、次のことを行っていただく必要があります: (i) 保有期間や破棄に関するものを含め、データ主体に通知する、(ii) データ主体から同意を得る、(iii)

生体認証データを削除する (該当するデータ保護要件に基づき、必要に応じてすべて)。"生体認証データ" は、GDPR の第 4 条に規定されている意味を持ち、該当する場合は、他のデータ保護要件における同義語となります。 関連情報については、「[Face のデータとプライバシー](#)」を参照してください。

識別

顔識別では、画像内の 1 つの顔を、安全なリポジトリ内の一連の顔と "一对多" で照合できます。一致候補は、顔データがクエリの顔とどれだけ一致しているかに基づいて返されます。このシナリオは、特定のユーザー グループに建物や空港へのアクセス権を付与したり、デバイスのユーザーを検証したりするために使用されます。

次の画像は、`"myfriends"` という名前のデータベースの例を示しています。各グループは、最大で 100 万個の異なる person オブジェクトを含むことができます。各 person オブジェクトには最大で 248 個の顔を登録できます。



グループを作成してトレーニングした後、新しく検出された顔のグループに対して識別を実行できます。顔がグループ内の person として識別された場合、その person オブジェクトが返されます。

検証

検証操作は、"これら 2 つの顔は同じ人物のものでしょうか?" という質問に答えます。

また、検証では、画像内の顔をセキュリティで保護されたリポジトリや写真からの 1 つの顔と "1 対 1" で照合して、それらが同じ個人であることが確認されます。検証はアクセス制御に使用できます。たとえば、銀行アプリで、ユーザーが自撮りした新しい写真を自分の写真付き ID の写真と共に送信すると、リモートでクレジット口座を開設できます。また、Identification API 呼び出しの結果に関する最終チェックとして使用することもできます。

顔認識の詳細については、[顔認識](#)の概念ガイドまたは [Identify](#) および [Verify](#) の API リファレンス ドキュメントを参照してください。

似た顔の検索

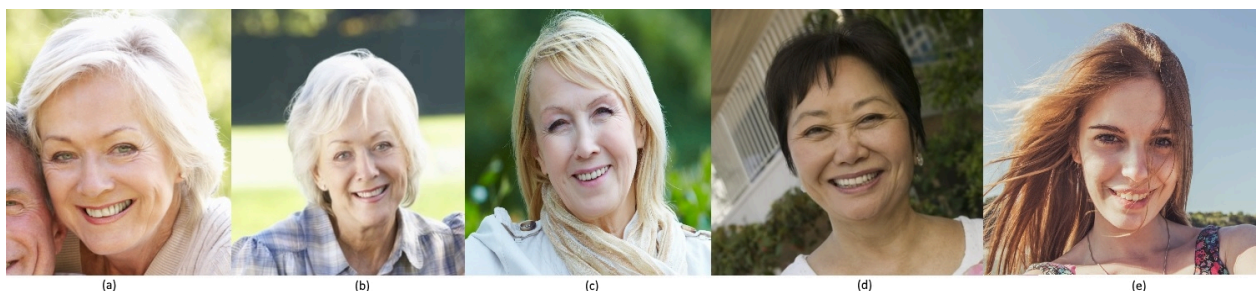
Find Similar 操作では、ターゲットの顔と候補となる一連の顔との間で顔照合を行い、ターゲットの顔によく似ている一連の顔が検索されます。これは、画像による顔検索を行う場合に便利です。

このサービスでは、**matchPerson** と **matchFace** の 2 つの動作モードがサポートされています。**matchPerson** モードでは、[Verify API](#) を使用して同一人物についてフィルター処理が行われた後、似た顔が返されます。**matchFace** モードでは、同一人物フィルターは無視されます。同一人物のものであるかどうかに関係なく、似ている顔の候補のリストが返されます。

ターゲットの顔の例を次に示します。



そして候補となる顔の画像は次のとおりです。



4 つの似た顔を検索する場合、**matchPerson** モードではターゲットの顔と同じ人を表す A と B が返されます。**matchFace** モードでは、ターゲットと同一人物ではない場合や類似性が低い場合でも、厳密に 4 つの候補が返されるので、A、B、C、D が返されます。詳細については、[Find Similar API](#) リファレンス ドキュメントを参照してください。

顔をグループ化する

Group 操作では、未知の顔の集合が、類似性に基づいて複数のグループに分けられます。それぞれのグループは、元の顔の集合から得られる、互いに素な真部分集合です。また、類似点が見つからなかった顔の ID を含む、単一の "messyGroup" 配列も返されます。

返されたグループに含まれるすべての顔は同一人物のものである可能性が高いものの、1 人の人物について、いくつかの異なるグループが存在することがあります。これらのグループは、たとえば表情など、別の要因によって区別されます。詳細については、[Group API](#) リファレンス ドキュメントを参照してください。

入力の要件

一般的な画像入力の要件:

- サポートされている入力画像形式は、JPEG、PNG、GIF (最初のフレーム)、BMP です。
- 画像ファイル サイズは 6 MB 以内である必要があります。

顔検出の入力要件:

- 検出可能な最小の顔のサイズは、1920 x 1080 ピクセル以下の画像では 36 x 36 ピクセルです。1920 x 1080 ピクセルより大きい画像では、最小の顔のサイズも比例して大きくなります。顔のサイズを小さくすると、検出可能な最小の顔のサイズより大きい場合でも、一部の顔が検出されない可能性があります。
- 検出可能な最大の顔のサイズは、4096 x 4096 ピクセルです。
- 36 x 36 から 4096 x 4096 ピクセルのサイズ範囲外の顔は検出されません。

顔認識の入力要件:

- 次のような写真の構成のために、一部の顔を認識できない場合があります。
 - 強すぎる照明を含む画像 (強烈な逆光照明など)
 - 一方または両方の目を遮っている障害物
 - 髪質や顔の毛の違い
 - 年齢による顔立ちの変化

- 極端な表情

データのプライバシーとセキュリティ

Azure AI サービス リソース全般に言えることですが、Face サービスを使用する開発者は、顧客データに関する Microsoft のポリシーに留意する必要があります。詳細については、Microsoft セキュリティ センターの [Azure AI サービスのページ](#) を参照してください。

次のステップ

クイックスタートに従って、顔認識アプリの基本コンポーネントを任意の言語でコーディングします。

クイックスタート

フィードバック

このページはお役に立ちましたか?

👍 Yes

👎 いいえ

[製品フィードバックの提供](#) | [Microsoft Q&A でヘルプを表示する](#)