サポート情報記事

Employee Directory に必要な Microsoft Graph のアクセス許可

2026 © Vitextra SIA. 無断転載を禁じます。

免責事項

本免責事項の適用上、次のとおり定義します。

- **会社** (本免責事項では「当社」と表記します) とは、Vitextra SIA (Matīsa iela 61-25, Rīga, LV-1009, Latvia) を指します。
- **本ドキュメント**とは、ナレッジベースの記事を指します。
- **お客様**とは、本ドキュメントにアクセスする個人、または該当する場合は、その個人が本ドキュメントにアクセスまたは使用する際に代理となっている会社その他の法人を指します。
- **本 Web サイト**とは、https://vitextra.com からアクセスできる Vitextra を指します。

免責事項

本ドキュメントに記載されている情報は、一般的な情報提供のみを目的としています。

当社は、本ドキュメントの内容における誤りや脱漏について、一切責任を負いません。

いかなる場合も、契約上の訴訟、過失、その他の不法行為上の訴訟であるかを問わず、本ドキュメントの内容の使用に起因または関連して生じる、特別損害、直接損害、間接損害、結果的損害、付随的損害、またはその他一切の損害について、当社は責任を負いません。当社は、事前の通知なく、いつでも本ドキュメントの内容に追加、削除、または変更を行う権利を留保します。

誤りおよび脱漏に関する免責事項

本ドキュメントに記載されている情報は、関心のある事項に関する一般的な指針を示すことのみを目的としています。そのため、本ドキュメントの内容を最新かつ正確に保つために当社があらゆる予防措置を講じている場合でも、誤りが生じる可能性があります。また、法律、規則、規制は変化するため、本ドキュメントに記載されている情報に遅れ、脱漏、または不正確な点が含まれる場合があります。

当社は、誤りや脱漏、またはこの情報の使用によって得られた結果について、責任を負いません。

フェアユースに関する免責事項

当社は、著作権者から明示的な許可を得ていない著作物を使用する場合があります。当社は、批評、論評、ニュース報道、教育、学術研究、または調査の目的で、そのような資料を提供しています。

当社は、これが、米国著作権法第 107 条に規定されている、当該著作物の「フェアユース」にあたると考えています。

お客様が、フェアユースの範囲を超えて、ご自身の目的で本ドキュメントの著作物を使用することを希望される場合は、著作権者から許可を得る必要があります。

「自己責任での使用」に関する免責事項

本ドキュメントのすべての情報は、完全性、正確性、適時性、またはこの情報の使用によって得られる結果について何ら保証することなく、また、性能、商品性、特定目的への適合性に関する保証を含むがこれらに限定されない、明示または黙示を問わずいかなる種類の保証もなく、「現状のまま」提供されます。

当社は、本ドキュメントに記載されている情報に依拠して行われた判断や措置、または結果的損害、特別損害、もしくはこれらに類する損害について、たとえそのような損害の可能性について知らされていた場合でも、お客様またはその他の者に対して責任を負いません。

お問い合わせ

本免責事項についてご不明な点がある場合は、メール (support@vitextra.com) でお問い合わせください。

目次

はじめに 4

アクセス許可 4

アプリケーションのアクセス許可ではなく委任されたアクセス許可 6

ユーザー プロファイル ソースと **SharePoint** 検索 7

アクセス許可がない場合にユーザーに表示される内容 8

アクセス許可の承認 11

アクセス許可の状態の確認 11

セキュリティ レビューのための注意事項 12

用語 13

はじめに

Vitextra Employee Directory ソリューションは、独自の従業員データベースを持ちません。ユーザー、プロファイル属性、写真、上司、Teams のプレゼンス、空き時間情報は、実行時に **Microsoft Graph** API を通じて **Microsoft 365** から読み取られます。そのため、ソリューション パッケージは 5 つの Microsoft Graph アクセス許可を要求し、テナント管理者がこれを一度だけ承認します。

この記事では、これらのアクセス許可の一覧、それぞれの用途と必要とする **Web パーツ**、アクセス許可が承認されていない場合にユーザーに表示される内容を正確に説明し、アクセス許可の承認方法と状態の確認方法を示します。**SharePoint** と Microsoft 365 の管理者、および展開前に製品を評価するセキュリティ レビュー担当者を対象としています。

アクセス許可

Vitextra Employee Directory パッケージには、**Employee Directory**、**Employee Directory (Entra ID)**、**New Employees** の 3 つの Web パーツが含まれており、そのすべてに対して 1 組のアクセス許可を要求します。5 つはいずれも Microsoft Graph の委任されたアクセス許可です。

アクセス許可	用途	必要とする **Web パーツ**	承認されていない場合
`Directory.Read.All`	フィルター エディターの **ユーザー ロール** 条件のために、Microsoft Entra ディレクトリ ロールのメンバーを読み取ります。`User.Read.All` とともに、ユーザー アカウントの読み取りにも使用できます	Employee Directory (Entra ID)、New Employees - フィルターで **ユーザー ロール** 条件を使用する場合のみ	ロール フィルターが設定されている場合、Employee Directory (Entra ID) は警告を表示し、ロールへの所属を確実に判定できません。New Employees はエラーを表示します。

アクセス許可	用途	必要とする **Web** パーツ	承認されていない場合
`User.Read.All`	ユーザー アカウントとそのプロファイル属性の読み取りと検索、ユーザーの上司と直属の部下、サインインしているユーザー自身のチーム、従業員の写真	3 つの Web パーツすべて。**ユーザー プロファイル** ソースを使用する **Employee Directory** Web パーツでは、写真、詳細ウィンドウ、クイック フィルター	ユーザーの一覧を読み込めず、エラーが表示されます (後述を参照)
`Presence.Read.All`	カード上の **Microsoft Teams** プレゼンス インジケーター、**状態** 列、詳細ウィンドウの **不在** メッセージ	3 つの Web パーツすべて	ユーザーはプレゼンスなしで表示され、**状態** 列には **オフライン** と表示されます
`Calendars.Read`	ユーザーとサインインしているユーザーの今日の空き時間情報、およびそのユーザーのタイム ゾーンと勤務時間	Employee Directory、Employee Directory (Entra ID) - 詳細ウィンドウ	**現地時間**、**勤務時間**、**予定の空き状況** のセクションが表示されません
`People.Read`	サインインしているユーザーが最もよく一緒に仕事をしている人の一覧	Employee Directory、Employee Directory (Entra ID) - **一緒に仕事をしている人** クイック フィルター	**一緒に仕事をしている人** タブが表示されません

メモ

`Directory.Read.All` と `User.Read.All` は重複しています。ユーザー アカウントの読み取りには、Microsoft Graph はどちらのアクセス許可も受け付けます。そのため、`User.Read.All` の行に記載したエラーは、どちらも承認されていない場合に発生します。これは展開直後、5 つの要求がすべて保留中のときの通常の状態です。パッケージが要求するとおり、両方を承認してください。

Employee Directory はこれらのアクセス許可を使用して、**Microsoft Entra ID** と Microsoft 365 のディレクトリ、プロファイル、メールボックスのデータを**読み取る**だけです。これらのデータを変更せず、名前に *Write* を含むアクセス許可も要求しません。SharePoint ページへの Web パーツ設定の保存は、これらの Microsoft Graph アクセス許可とは別の処理です。

アプリケーションのアクセス許可ではなく委任されたアクセス許可

5 つのアクセス許可はすべて **委任された** アクセス許可です。Microsoft Graph の呼び出しはすべて、サインインしているユーザーのブラウザーから、そのユーザーに発行されたトークンを使用して行われます。Web パーツには、**アプリケーションのアクセス許可** (アプリのみ)、サービス アカウント、ディレクトリを読み取る独自のバックエンドはありません。

Microsoft Graph は、付与された委任スコープとサインインしているユーザーの権限を組み合わせてアクセスを判定します。そのため、ディレクトリに表示されるユーザーは Outlook や Teams と異なる場合があります。それらのアドレス帳のコピーではありません。

メモ

アクセス許可は Employee Directory パッケージ自体に付与されるわけではありません。SharePoint は、テナント内のすべての SPFx ソリューションに使用する単一の Microsoft Entra ID アプリケーション、 *Web Client Extensibility* (以前の名称: *SharePoint Online Client Extensibility Web Application Principal*) にアクセス許可を付与します。アクセス許可が別のソリューション (たとえば Vitextra Organizational Chart) のためにすでに承認されている場合は同じ付与が再利用され、要求が再び保留中として表示されることはありません。Web パーツを Microsoft Teams で実行する場合も、同じ承認が適用されます。

ユーザー プロファイル ソースと SharePoint 検索

Employee Directory Web パーツは、設定で選択する 2 つのソースからユーザーを読み取ることができます。

- **Entra ID (Azure AD)** - 一覧、検索、ページングは Microsoft Graph を通じて行われ、上記のアクセス許可に依存します。
- **ユーザー プロファイル** - 一覧、検索、**絞り込み**、並べ替えは、Microsoft Graph ではなく **SharePoint 検索** (SharePoint 検索サービスのユーザー結果) から取得されます。これらはユーザー自身の SharePoint 検索の権限で、通常のセキュリティトリミングを伴って動作し、Microsoft Graph のアクセス許可を必要としません。詳細ウィンドウの **最近使ったドキュメント** セクションも SharePoint 検索を使用します。

ユーザー プロファイル ソースを使用している場合でも、Web パーツの一部は引き続き Microsoft Graph を呼び出します。写真、プレゼンスと **不在** メッセージ、詳細ウィンドウの **上司** と **部下** のセクション、**現地時間**、**勤務時間**、**予定の空き状況** のセクション、および **自分のチーム** と **一緒に仕事をしている人** のクイック フィルターです。これらは **Entra ID (Azure AD)** モードと同じアクセス許可に依存します。

Employee Directory (Entra ID) Web パーツと **New Employees** Web パーツは、常に Microsoft Graph を使用します。

ヒント

2 つのディレクトリ Web パーツとそのソースの違いについては、KB10310. Employee Directory と Employee Directory (Entra ID) の比較: どちらの Web パーツを選ぶべきか の記事を参照してください。

アクセス許可がない場合にユーザーに表示される内容

Web パーツは、省略可能なアクセス許可が不足している場合に、それに依存する機能だけが無効になるように設計されています。現在のバージョンでの正確な動作は次のとおりです。

Web パーツ / モード	不足しているアクセス許可	ユーザーに表示される内容
Employee Directory (Entra ID)	`User.Read.All` (および `Directory.Read.All`)	以前に読み込まれた空でない一覧がない状態での初回読み込み時：一覧の代わりに、エラー アイコンと Microsoft Graph が返したエラー テキストが表示されます。テキストがない場合は *申し訳ございません。問題が発生しました。ページを更新してやり直してください。* というメッセージが表示されます
Employee Directory、**Entra ID (Azure AD)** ソース	`User.Read.All` (および `Directory.Read.All`)	検索結果の代わりに同じエラーが表示されます
Employee Directory、ユーザー プロファイル ソース	`User.Read.All` (および `Directory.Read.All`)	一覧、検索、絞り込みは引き続き動作します。詳細ウィンドウには 上司 と 部下 のセクションが

Web パーツ / モード	不足しているアクセス許可	ユーザーに表示される内容
		表示されず、写真は Microsoft Graph ではなく SharePoint から取得されます
New Employees	`User.Read.All` (および `Directory.Read.All`)	エラー アイコンと *申し訳ございません。問題が発生しました。ページを更新してやり直してください。* というメッセージに続いて、Microsoft Graph が返したエラー テキストが表示されます
Employee Directory (Entra ID)、New Employees	`Directory.Read.All`	ロール フィルターが設定されている場合、Employee Directory (Entra ID) は警告を表示し、ロールへの所属を確実に判定できません。New Employees はエラーを表示します。
すべての Web パーツ	`Presence.Read.All`	カードにプレゼンス インジケーターが表示されず、**状態** 列には全員 **オフライン** と表示され、詳細ウィンドウに **不在** メッセージは表示されません
Employee Directory、Employee Directory (Entra ID)	`Calendars.Read`	詳細ウィンドウの **現地時間**、**勤務時間**、**予定の空き状況** のセクションが表示されません。エラーは

Web パーツ / モード	不足しているアクセス許可	ユーザーに表示される内容
		表示されません
Employee Directory、Employee Directory (Entra ID)	`People.Read`	クイック フィルター バーで **一緒に仕事をしている人** タブが非表示になります。その他のタブは引き続き動作します

警告

Employee Directory (Entra ID) Web パーツは、読み込んだ一覧のコピーをブラウザーに保存し、次回のアクセス時に表示します。コピーが 24 時間より古くなるとバックグラウンドで更新され、**更新** を選択した場合も新しい要求が送信されます。アクセス許可の取り消し後にこの要求が失敗しても、以前に読み込まれた空でない一覧がすでに表示されている場合は、一覧と元の更新日時が保持されます。警告 *一覧を更新できませんでした。保存済みのコピーを表示しています。* が表示され、エラー テキストがある場合はその後に表示されます。一覧がエラー画面に置き換わることはありません。以前に読み込まれた空でない一覧がない状態で読み込みに失敗した場合は、エラー画面が表示されます。アクセス許可の変更をテストするときは、ブラウザーでサイトのデータを消去するか、プライベート ウィンドウを使用してください。

メモ

プレゼンスと空き時間情報には、アクセス許可だけでは不十分です。プレゼンスの状態を持つには Microsoft Teams を使用している必要があり、空き時間情報を持つには Exchange Online メールボックスが必要です。空き時間情報のセクションの詳細については KB10317. Employee Directory: 現地時間、勤務時間、空き時間情報 を、クイック フィルターについては KB10214. Employee Directory のクイック フィルター: 自分の部署、自分のチーム、一緒に仕事をしている人、お気に入り を参照してください。

アクセス許可の承認

Employee Directory パッケージをテナントのアプリ カタログに展開すると、アクセス許可の要求が自動的に作成されます。**グローバル管理者** が次の手順で承認します。

1 **SharePoint 管理センター** を開きます。
2 左側のナビゲーションで **詳細設定** を展開し、**API アクセス** を選択します。
3 **保留中の要求** タブで、**Microsoft Graph** に対する **Vitextra Employee Directory** パッケージの要求 (`Directory.Read.All`、`User.Read.All`、`Presence.Read.All`、`Calendars.Read`、`People.Read`) を見つけます。
4 各要求を選択し、**承認** をクリックして確定します。

ユーザーに同意を求めるメッセージは表示されません。承認後は、テナント内のすべてのユーザーに対して Web パーツが動作します。承認から数分たっても Web パーツにエラーが表示される場合は、ページを再読み込みしてください。

> **ヒント**
>
> PowerShell による承認、一部のみの承認、アクセス許可の取り消しを含む手順全体については、KB10360. SharePoint 管理センターで Vitextra ソリューションの Microsoft Graph API アクセス許可を承認する方法 の記事を参照してください。

アクセス許可の状態の確認

どのアクセス許可が有効になっているかを確認するには、SharePoint 管理センターで **詳細設定 › API アクセス** を開きます。

- **承認済みの要求** タブに、5 つの Microsoft Graph アクセス許可がすべて表示されている必要があります。付与はテナント全体に適用されるため、アクセス許可が最初に要求した別のパッケージの下に表示されている場合もあります。それで問題ありません。
- **保留中の要求** タブにまだ表示されているアクセス許可は、まだ有効になっていません。それに依存する機能は、「**アクセス許可がない場合にユーザーに表示される内容**」に記載したとおりに動作します。

Employee Directory を更新しても、以前に承認したアクセス許可は承認されたまま

です。新しいバージョンが追加のアクセス許可を要求する場合、そのアクセス許可は **保留中の要求** タブに表示され、同じ方法で承認する必要があります。

セキュリティ レビューのための注意事項

セキュリティ レビューでは、通常、次の点が重要になります。

- 5 つの Microsoft Graph アクセス許可はすべて委任された読み取り専用のアクセス許可であり、ディレクトリ、プロファイル、メールボックスのデータの変更は許可しません。
- ディレクトリ　データ、写真、プレゼンス、予定表の情報は、ユーザーのブラウザーが Microsoft Graph と SharePoint から直接取得し、Vitextra や第三者に送信されることはありません。
- **ユーザー プロファイル** ソースは、ユーザー自身の権限で SharePoint 検索を通じてユーザーを読み取り、一覧そのものには Microsoft Graph のアクセス許可を必要としません。
- お気に入り、キャッシュされた従業員の一覧、Teams 個人用アプリの既定の構成は、Microsoft Graph の外部に保存されます。具体的な保存場所と Web パーツが読み取るデータについては、KB10469. Employee Directory: 読み取るデータと、お気に入りと設定の保存場所 の記事で説明しています。
- Vitextra サービスへの要求には、ライセンス確認、技術的な識別子を含む使用状況テレメトリ、および利用する場合は Teams 個人用アプリの既定の構成の保存が含まれます。詳細は KB10363. Vitextra 製品がデータを保存する場所: プライバシー、データ所在地、GDPR を参照してください。

ヒント

ソリューションのインストールについては KB10035. SharePoint Online に Vitextra 製品をインストールする方法 を、ページへの Web パーツの追加については KB10309. Employee Directory Web パーツの追加と構成方法 を参照してください。

製品の詳細: *https://vitextra.com/ja/products/employee-directory*

用語

Microsoft 365
Microsoft 365 は、Word、Excel、PowerPoint、Outlook などの生産性アプリと、SharePoint、OneDrive、Teams、Exchange Online などのクラウド サービスを、高度なセキュリティおよびデバイス管理と組み合わせた、クラウドベースのサブスクリプション サービスです。

Microsoft Entra ID
Microsoft Entra ID (旧称 Azure Active Directory) は、Microsoft が提供するクラウドベースの ID およびアクセス管理サービスです。組織は、ユーザーの ID と、社内外のさまざまなリソースへのアクセスを効率的に管理し、保護できます。これらのリソースには、Microsoft 365、Azure プラットフォーム、その他数千もの Software as a Service (SaaS) アプリケーションが含まれます。

Microsoft Graph
Microsoft Graph は、Microsoft Entra ID (旧称 Azure Active Directory) と OAuth 2.0 で保護された REST API です。SharePoint、Outlook、OneDrive、Teams など、Microsoft 365 のデータやサービスにアクセスするための単一のエンドポイントを提供します。

Microsoft Teams
Microsoft Teams は、オンライン会議、ライブ イベント、ドキュメント共有の機能を備えた、ビジネス コミュニケーション向けのチャット ベースのコラボレーション プラットフォームです。

SharePoint
SharePoint は、コンテンツ管理、ドキュメント管理、ワークフロー アプリケーション、検索、その他のツールを提供する Web ベースのコラボレーション プラットフォームで、従業員やチームが共同で作業できるようにします。SharePoint は、共有情報を保存、整理、アクセスするための安全な場所でもあります。

Web パーツ
Web パーツは、SharePoint ページに配置される機能やコンテンツの主要な構成要

素です。Web パーツの中には、Web パーツの構成や外観の変更など、カスタマイズをサポートするものがあります。

アプリケーションのアクセス許可

アプリケーションのアクセス許可により、アプリケーションは、バックグラウンド サービスやデーモンなどとして、サインインしているユーザーなしで実行できます。常に管理者の同意が必要であり、アプリケーションは、そのアクセス許可の対象となるすべてのデータにアクセスできます。

絞り込み

絞り込みは、検索結果ページのフィルターで、ファイルの種類、作成者、更新日などの管理プロパティの値で結果を絞り込むことができます。