サポート情報記事

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

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

概要 4

何が、なぜ要求されるのか 4

要求はどこから来るのか 6

前提条件 7

要求を承認する 8

アクセス許可の一部のみを承認する 9

アクセス許可がないときにユーザーに表示されるもの 9

更新と新しいアクセス許可 10

アクセス許可の確認と取り消し 10

審査担当者向けのセキュリティに関する注意事項 11

用語 12

概要

いくつかの Vitextra Web パーツは、**SharePoint** サイトの外部にあるデータを読み取ります。**Microsoft Entra ID** のユーザー プロファイルと上司の階層、**Microsoft Teams** のプレゼンス、予定表、Planner と To Do のタスク、OneDrive のファイルなどです。**SharePoint Framework (SPFx)** ソリューションは **Microsoft Graph** を通じてこれらのデータにアクセスし、テナント管理者はそれを一度だけ許可する必要があります。

この仕組みはすべての SPFx ソリューションで共通です。ソリューション パッケージは必要なアクセス許可を宣言し、パッケージが アプリ カタログに展開されると、SharePoint はその宣言を*アクセス許可の要求*に変換します。要求は、管理者が承認または拒否するまで、SharePoint 管理センターの **API アクセス** ページで待機します。

この記事では、どの Vitextra 製品がどのような理由でアクセス許可を要求するのか、要求を承認する方法、後で要求を確認して取り消す方法、アクセス許可が不足しているときに Web パーツに何が表示されるかを説明します。Vitextra 製品をインストールする SharePoint 管理者とグローバル管理者、およびこのような要求を審査するセキュリティ担当者を対象としています。

> **メモ**
>
> この記事で扱うのは、SPFx ソリューションの API アクセス要求のみです。パッケージ自体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で説明しています。

何が、なぜ要求されるのか

以下のアクセス許可は**委任された**アクセス許可です。Web パーツはサインインしているユーザーの代理で Microsoft Graph を呼び出します。実効アクセス権は、付与されたスコープとユーザー自身のアクセス許可の両方によって決まります。Graph の結果が Outlook や Teams の表示と完全に一致するという意味ではありません。 Microsoft Graph

次の表は、Microsoft Graph を使用する製品の現在のバージョンが宣言しているア

クセス許可の一覧です。

製品	API	アクセス許可	用途
Employee Directory	Microsoft Graph	User.Read.All, Directory.Read.All, People.Read, Presence.Read.All, Calendars.Read	ユーザー プロファイル、部署、上司の読み取り、関連するユーザー、Teams のプレゼンス、空き時間インジケーターのための空き時間情報
Employee Details	Microsoft Graph	User.Read.All, User.ReadWrite, People.Read.All, Presence.Read.All, Files.Read.All, Sites.Read.All, Calendars.Read.Shared	プロファイルの読み取り、ユーザー自身によるプロファイル フィールドの編集、関連するユーザー、プレゼンス、本人が最近作業したドキュメントとサイト (Microsoft Graph インサイト)、勤務時間と空き状況のための同僚の空き時間情報
Organizational Chart	Microsoft Graph	User.Read.All, Directory.Read.All, Presence.Read.All	上司属性からの指揮命令系統の構築、部署と役職、Teams のプレゼンス
Absence & Coverage	Microsoft Graph	User.Read.All	申請、承認、代理のための従業員、その上司、直属の

製品	API	アクセス許可	用途
			部下の特定
My Tasks	Microsoft Graph	User.Read, User.ReadBasic.All, Tasks.ReadWrite	Planner、To Do、フラグ付きメールからのタスク、タスク作成者の名前
My Tasks	**Azure DevOps**	user_impersonation	**Azure DevOps** ソースと **Azure DevOps Query Web** パーツ
Password Vault	Microsoft Graph	Files.ReadWrite.AppFolder	ユーザーの OneDrive のアプリケーション フォルダーへの暗号化された保管庫の保存

現在のサイトのみを対象とする製品 (Announcements Carousel、List Filter Online、QR Code Generator、Questions & Answers、Quick Poll、**RSS** Reader、Smart Search、Smart Tiles) は、API アクセス許可を**要求しません**。これらの製品については、**API アクセス** ページに何も表示されません。

メモ

Tasks.ReadWrite や *User.ReadWrite* などのアクセス許可名は Microsoft Graph のスコープの名前であり、製品が実際に行う操作よりも広い範囲を表す場合があります。My Tasks はタスクを読み取るだけであり、Employee Details はサインインしているユーザーのプロファイル　フィールドのみを書き込みます。各アクセス許可の詳細は、製品ごとの記事で説明しています: KB10235. Organizational Chart に必要な Microsoft Graph のアクセス許可、KB10303. My Tasks: 必要なアクセス許可、プライバシー、セキュリティ。

要求はどこから来るのか

アクセス許可の要求は、`.sppkg` パッケージがテナントのアプリ カタログに展開されたときに作成されます。要求は個々の Web パーツではなくパッケージに属するため、2 つの Web パーツを含むソリューションでも要求は 1 セットだけ表示され、オプション機能 (たとえば My Tasks の Azure DevOps ソース) でのみ必要なアクセス許可も、他のアクセス許可と一緒に要求されます。

ガバナンスの観点から重要な点が 2 つあります。

- **承認はテナント全体に適用されます。** SharePoint は、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*) に対してアクセス許可を付与します。Employee Directory のために *User.Read.All* が承認されると、同じ付与が Organizational Chart と、それを要求するテナント内の他のすべての SPFx ソリューションで使用されます。これは SharePoint Framework の仕組みであり、Vitextra の設計上の判断ではありません。
- **展開は承認に依存しません。** Vitextra 製品は、要求が保留中、あるいは拒否された状態でも、展開してサイトに追加し、ページに配置できます。不足しているアクセス許可に依存する機能だけが動作しません。

前提条件

- Vitextra パッケージがテナントのアプリ カタログにアップロードされ、展開されていること (**アプリを有効にする**)。
- Microsoft Graph およびその他の Microsoft API のアクセス許可を承認するには、**グローバル管理者**としてサインインします。テナントに登録されたサードパーティ API には**アプリケーション管理者**ロールで十分です。SharePoint 管理者ロールだけでは Microsoft Graph のアクセス許可を承認できません。 Microsoft

警告

API アクセス ページに表示されるのは、**テナント**のアプリ カタログに展開されたパッケージの要求です。Vitextra 製品をサイト コレクションのアプリ カタログから展開する場合は、先にパッケージをテナントのアプリ カタログに展開し、そこで要求を承認してください。承認されたアクセス許可はテナント全体に適用され、サイト コレクションのアプリ カタログにあるコピーでも使用できるようになります。

要求を承認する

1. Microsoft 365 管理センターを開き、**SharePoint 管理センター**に移動します。

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、Vitextra パッケージの要求を見つけます。各行には、パッケージ名 (たとえば *Vitextra Employee Directory*)、API (*Microsoft Graph* または *Azure DevOps*)、アクセス許可が表示されます。

4. 要求を選択し、**承認**をクリックします。パネルの説明を読み、**承認**で確定します。

5. パッケージのすべての要求について繰り返します。別のソリューションのために既に承認されているアクセス許可は再び表示されません。SharePoint は既存の付与を再利用します。

6. **承認済みの要求**タブに切り替え、パッケージのすべてのアクセス許可が一覧に含まれていることを確認します。

ユーザーに同意のプロンプトは表示されません。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。付与は通常、数分以内に有効になります。Web パーツがアクセス許可の不足を報告し続ける場合は、ページを再読み込みするか、サインアウトして再度サインインし、新しいトークンを取得してください。

ヒント

SharePoint Online 管理シェルを使用すると、要求をまとめて承認できます。`Get-SPOTenantServicePrincipalPermissionRequests` は保留中の要求を一覧表示し、`Approve-SPOTenantServicePrincipalPermissionRequest -RequestId <id>` はそのうちの 1 つを承認します。複数の Vitextra 製品を一度に展開するときに便利です。

アクセス許可の一部のみを承認する

一部の要求を承認し、他の要求を拒否することもできます。Web パーツは動作し続け、依存する機能だけが影響を受けます。

- *Presence.Read.All* を拒否した場合: Employee Directory、Employee Details、Organizational Chart は、Teams のプレゼンス インジケーターなしでユーザーを表示します。
- *Calendars.Read / Calendars.Read.Shared* を拒否した場合: 空き状況と勤務時間の情報は表示されません。
- *Files.Read.All / Sites.Read.All* を拒否した場合: Employee Details に最近のファイルとサイトは表示されません。
- *user_impersonation* (Azure DevOps) を拒否した場合: My Tasks の Azure DevOps ソースと Azure DevOps Query Web パーツは Azure DevOps にサインインできません。

製品の中核となるアクセス許可 (ユーザー中心の製品では *User.Read.All*、My Tasks では *Tasks.ReadWrite*、Password Vault では *Files.ReadWrite.AppFolder*) を拒否すると、Web パーツにデータが表示されなくなります。

アクセス許可がないときにユーザーに表示されるもの

症状	考えられる原因
Web パーツに、アクセスが拒否された、権限が不足している、同意がないといったエラーが表示される	中核となるアクセス許可が保留中または拒否されている
従業員は一覧表示されるが、色付きの	*Presence.Read.All* が承認されていない

症状	考えられる原因
プレゼンス ドットが表示されない	
組織図が空、または現在のユーザーだけが表示される	*User.Read.All* または *Directory.Read.All* が承認されていない
My Tasks に Planner、To Do、Outlook のタスクが表示されないが、SharePoint ソースは動作する	*Tasks.ReadWrite* が承認されていない
すべて動作していたが、更新後に 1 つの機能が動作しなくなった	新しいバージョンが追加のアクセス許可を要求しており、まだ保留中である

API アクセス ページを開き、**保留中の要求**タブと**承認済みの要求**タブを、この記事の冒頭の表と比較してください。

更新と新しいアクセス許可

パッケージの新しいバージョンをアップロードしても (KB10050. SharePoint Online で Vitextra SPFx ソリューションを更新する方法を参照)、以前に承認され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以前のバージョンにはなかったアクセス許可を宣言している場合、新しい要求が**保留中の要求**タブに表示されるため、同じ方法で承認する必要があります。Vitextra は、このような変更を製品のリリース ノートに記載しています。

アクセス許可の確認と取り消し

付与はすべての SPFx ソリューションで共有されるため、Vitextra 製品を削除しても、その製品が要求したアクセス許可は取り消され**ません**。アクセス許可を取り消すには:

1 **API アクセス**を開き、**承認済みの要求**タブに切り替えます。
2 アクセス許可を選択し、**アクセスの削除** (Remove access) をクリックします。
3 確定します。

警告

アクセス許可を削除する前に、テナント内の別のソリューションがそれに依存していないか確認してください。自社開発の SPFx Web パーツ、他のベンダーの製品、Microsoft 自身の事前承認済みのアクセス許可が同じタブに表示されます。別のソリューションが使用しているアクセス許可を削除すると、そのソリューションは直ちに動作しなくなります。

拒否された要求は API アクセス ページから削除され、**保留中の要求**には残りません。アクセス許可を再度要求するには、開発者が同じリソースとスコープに対する新しい要求を送信する必要があります。 Microsoft

審査担当者向けのセキュリティに関する注意事項

- Microsoft Graph へのすべての呼び出しは、サインインしているユーザーのブラウザーから、そのユーザーに対して発行されたトークンを使用して行われます。Vitextra Web パーツには、アプリケーション (アプリ専用) のアクセス許可もサービス アカウントもありません。
- Microsoft Graph は、付与された委任スコープとユーザーのアクセス許可を確認します。アドレス帳での表示設定と各アプリケーションのフィルターは別の仕組みです。Outlook で非表示にしたユーザーが Graph クエリでも非表示になるとは限りません。
- 製品ごとのデータフロー、ライセンス要求、テレメトリ、保存については、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。

用語

Azure DevOps
Azure DevOps Services (旧称 Visual Studio Team Services) は、バージョン管理、要件管理、ビルドとリリースの自動化パイプライン、テスト機能を提供するクラウドベースの製品です。

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。

RSS
RSS (Really Simple Syndication) は、Web サイトの更新情報をユーザーやアプリケーションに標準化された機械可読形式で配信するために使用される、一般的な Web フィード形式です。この形式は、ニュース記事、ブログ投稿、その他の頻繁に更新されるコンテンツの配信に広く使用されています。

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、

用語

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。

SharePoint Framework (SPFx)

SharePoint Framework (SPFx) は、SharePoint Online、SharePoint Server (オンプレミス)、Microsoft Teams 向けのクライアント側 Web パーツ、コンポーネント、拡張機能を構築するためのモデルです。SPFx のカスタマイズは JavaScript に基づいており、モダン ユーザー インターフェースをネイティブでサポートします。

SharePoint 管理センター

SharePoint 管理センターは、SharePoint 管理者が、テナントのサイト、共有とアクセスの設定、アプリ カタログ、ストレージ、その他の SharePoint Online の設定を管理するための Web ポータルです。

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。

テナント

Microsoft 365 テナントは、Microsoft 365 サービスの専用インスタンスです。テナントには、ユーザーやドメイン (Microsoft Entra ID)、構成、サブスクリプション、サービスなど、組織の情報が保持されます。組織は、Microsoft 365 サービスにサインアップすることでテナントを受け取ります。

ユーザー プロファイル

ユーザー プロファイルは、ユーザーを説明するプロパティのセットです。プロパティには、ユーザーに関する基本情報、連絡先の詳細、その他のデータが含まれます。ユーザー プロファイルは、Delve、マイ サイトなどのサービスで使用されます。