サポート情報記事

Policy Acknowledgementのロールと権限を設定する方法

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

ロールを理解する 4

グループを割り当てる 4

権限の適用による変更を理解する 5

対象者、所有権、権限を区別する 6

代表的なアクセス試験を使う 6

組織変更後もアクセスを維持する 7

アクセスを検証して維持する 8

製品のロールは、Policy Acknowledgementで利用できる操作と表示を制御します。Policy Adminはハブのリストにロールに基づくSharePoint権限も適用します。アクセスを設計する際は両方の層を確認してください。

ロールを理解する

ロール	**Web**パーツでの主な用途
製品管理者	セットアップ、設定、ロール、管理、および管理機能とレポートへのアクセス。
コンプライアンス管理者	製品全体のポリシー、キャンペーン、レポート、免除。
ポリシー作成者	ポリシーの作成と、その作成者が所有するポリシーの管理。
監査役	ポリシー管理操作を伴わないレポートと確認。
従業員	個人の割り当てとポリシーコンテンツ。

チームの上司の対象範囲は報告関係に基づき、直属の部下だけか、その配下全体かを設定できます。ロール一覧に割り当てる六番目のロールではありません。各ポリシーに所有者が保存され、作成者のビューではその所有者でポリシーを絞り込みます。

グループを割り当てる

1 製品管理者としてPolicy Adminを開き、**役割**を選択します。
2 必要なロールに対して、Entra IDセキュリティグループまたはハブサイトのSharePointグループを選択します。
3 **製品管理者**には少なくとも一つのグループを残します。
4 従業員の対象範囲と**上司は直属および間接的に配下に属するすべての従業員を確認できる**を確認します。
5 **保存して権限を適用する**を選択し、同期の完了を待ちます。

厳密なアクセス範囲が必要な場合は、明示的な従業員グループを使用してください。画面には**ライセンスを取得したすべてのユーザー**がありますが、現在のロール判定ではライセンスを確認せず、このオプションを現在のユーザーに一致すると扱います。ライセンスのあるアカウントだけにアクセスが制限される証拠にはできません。



製品のロールと割り当てたグループ

権限の適用による変更を理解する

同期はロールグループにサイトの読み取り権限を付与し、製品のリストの権限継承を解除して、リストの権限マトリックスを適用します。同期を実行するアカウントは、これらのリストのフルコントロールを維持します。既存の共有サイトに適用する前に影響を確認してください。

Directモードでは、従業員は割り当てと確認レコードへの投稿権限を受け取ります。**Service**モードでは、その二つのリストに対するマトリックス上の従業員権限は読み取り専用です。質問への投稿権限は維持されます。複数のロールを持つユー

ザーは、所属グループの権限を組み合わせて受け取る場合があります。

警告

ポリシー所有者や個人の割り当てによる絞り込みは、Webパーツ内に実装されています。権限マトリックスはリスト単位であり、ポリシー単位や従業員単位の分離ではありません。これらのフィルターを、SharePoint経由で他のレコードにアクセスできない保証として説明しないでください。同期が成功しても、既存の権限や昇格された権限がすべて取り消されたことは証明されません。

対象者、所有権、権限を区別する

これらは異なる問いに答える概念です。キャンペーンの対象者は、誰がタスクを受け取るべきかを決めます。ポリシー所有者は責任と作成者で絞り込まれる管理ビューを決めます。ロールは製品操作を有効にし、SharePoint権限は保存レコードへのアクセスを制御します。一つを変更しても、他が自動的に実現するわけではありません。

たとえば、財務部門にポリシーを割り当てても、基になるリストレコードが財務だけの非公開データになるわけではありません。カードを別の所有者に移すと、管理すべき作成者が変わりますが、項目単位の権限移転ではありません。ポータルのナビゲーションで管理ページを隠しても、ユーザーの既存リストアクセスは取り消されません。

責任に合わせてロールグループを設計し、そのグループの有効なデータアクセスを確認します。複数グループに属する人は、組み合わされたメンバーシップをテストします。作成者ロールと管理グループを持つユーザーは、作成者のみのテストアカウントより多くの内容を表示・変更できる場合があります。一つの所属を削除しても、別のグループや高いサイト権限によるアクセスが残る場合があります。

代表的なアクセス試験を使う

テストアカウント	アプリケーションの確認	追加のアクセス確認
管理者	Policy Adminを開き、設定されたロールを確認します。	同期後も期待する管理機能が利用できることを確認します。

テストアカウント	アプリケーションの確認	追加のアクセス確認
作成者	所有するポリシーを開き、目的の管理操作を検証します。	フィルターされたビューから分離を推測せず、実際のリスト権限を調べます。
監査担当者	対象レポートを開き、許可されたエクスポートをダウンロードします。	結果や監査イベントを保存する操作に追加の書き込みアクセスが必要か確認します。
従業員	割り当てられたポリシーを開き、試験用の確認を送信します。	ソースアクセスと設定された証跡書き込み経路を検証します。
マネージャー	想定する報告チームを読み込みます。	有効なデータアクセスと範囲の動作を独立して確認します。

読み取り中心に見える操作でもデータを書き込む場合があります。たとえば、整合性チェックは結果を保存し、レポートエクスポートはファイル生成後に監査イベントを書き込みます。そのため、読み取り専用アカウントが有用な出力を見た後に書き込みエラーになることがあります。ロールを広げる前に、具体的に失敗した操作を調べます。

組織変更後もアクセスを維持する

作成者が異動する場合、グループ所属と、保守していたポリシーの所有権の両方を確認します。マネージャー変更時はディレクトリの関係と割り当てに保存されたマネージャーフィールドを調べます。ページ再読み込みでは過去の割り当ては書き換わりません。記録モードが変わる場合はサービスを確認し、対応する権限マトリックスを再適用します。

誰が権限を適用し、どのグループを意図し、どの代表テストが成功したかを簡潔に記録します。同期するアカウントはフルコントロールを保持するため、サービスモードのラベルがすべての人間のアカウントを読み取り専用にすると思い込まず、そのアカウントを明示的に評価します。配下全体の設定も、現在のTeam

Complianceの選択機能では強制されません。そのレポート上の制限はKB10530. Team Compliance：チームの監視とフォローアップを参照してください。

アクセスを検証して維持する

管理者、作成者、レポート利用者、従業員の別々のアカウントでテストします。意図したページと基になるリスト権限の両方を確認してください。確認の記録モードを変更したら、**保存して権限を適用する**をもう一度実行し、実効権限を確認します。記録モードと制限についてはKB10509. Policy Acknowledgementのデータ保存：DirectモードとServiceモードを参照してください。