【SharePoint】ドキュメントの権限設定

2025年1月31日

改訂履歴

版数	発行日	改訂内容
第1版	2025年1月31日	初版発行

本資料の内容は 2025/1/31 時点のものです。製品のアップデートにより変更となる場合がございます旨ご了承ください。

Agenda

1. 前提情報
    1. 前提条件
    2. 用語集
2. ドキュメントライブラリの機能
    1. SharePoint Onlineの構造
    2. SharePoint Onlineの権限設定
    3. ドキュメントライブラリの機能
    4. ドキュメントライブラリ アクセス権限の仕組み
    5. シナリオに応じたドキュメントライブラリの推奨構成
3. テストケース検証
    1. テストケース検証とその結果
    2. テストケース① 階層ごとのフォルダ権限設定
    3. テストケース② ファイルのダウンロード制御

1. 前提情報

1.1. 前提条件

- 本書は、クラウドサポートのService Request情報の回答を基に作成しております。
- 本書に記載するサービス仕様、サービス名称などの各情報については、2025年1月時点でのサービス仕様に基づくものとしております。
- 本書は、Microsoft 365のキャプチャを利用しております。

- 本書は過去に発生した顧客質問を元に仕様の確認および検証を行っています。
  質問のカテゴリ、内容詳細を以下に記載します。

Microsoft 365	機能	内容詳細
SharePoint	権限設定	SharePoint Online にて、最上部とその 1 つ下の階層のフォルダに、下記のような制約を設けることは可能か。 <制約> ・フォルダ削除禁止 ・名前の変更禁止 ・フォルダの移動禁止 ・3 階層目以降や、最下層のファイルについては、自由に操作して構わない
SharePoint	権限設定	Excelデータを編集はできてダウンロードはできないように設定することは可能か。

1.2. 用語集

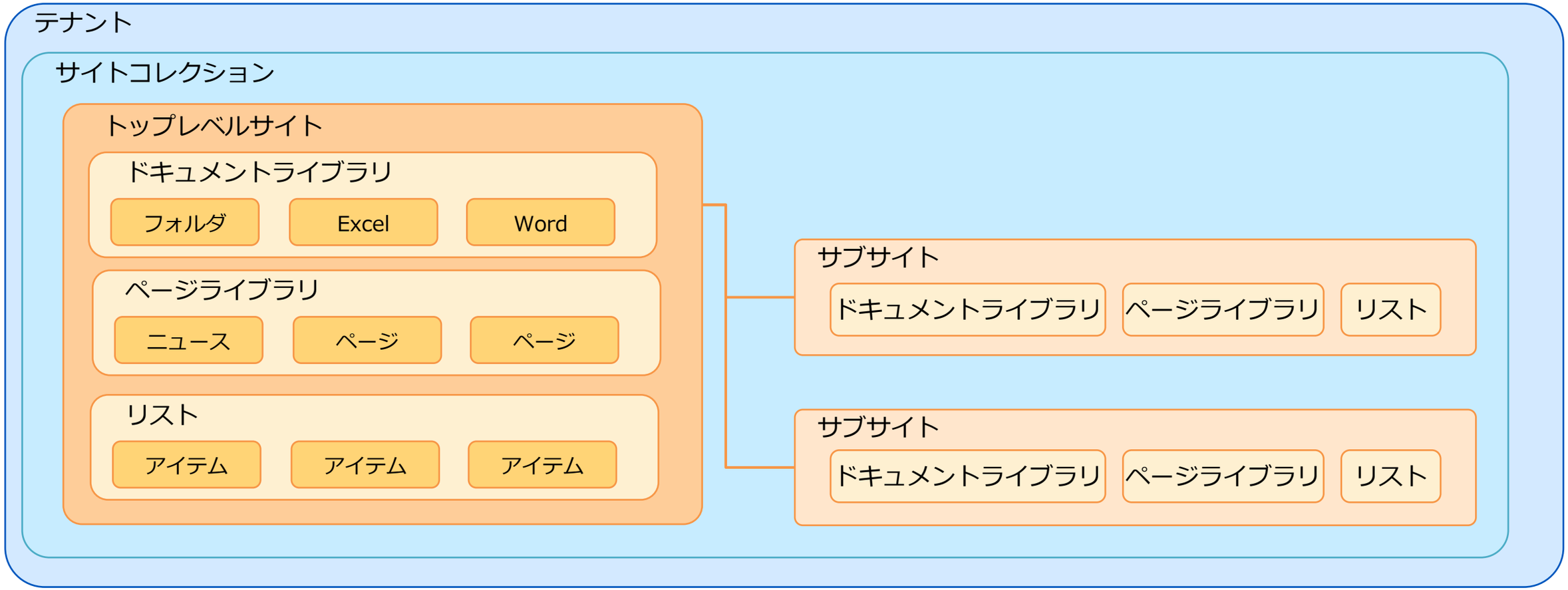
本書で使用する用語及び略称を以下の通り定義します。

No.	用語	説明
1	セキュリティグループ	SharePoint などのMicrosoft 365リソースへのアクセス権を、ユーザーやデバイスにまとめて付与するための仕組み。メールアドレスは持たない。 動的なメンバーシップ設定により、属性に基づいてメンバーを自動管理できる。
2	Microsoft 365グループ	組織内外のユーザー間の共同作業を支援する機能。メールアドレスを持つ。 各グループには、会話、ファイル、予定表などの共有スペースが提供され、TeamsやViva Engageにも接続できる。 動的メンバーシップにより、属性に基づいたメンバーの自動管理も可能。 SharePointのアクセス権限にも利用できる。
3	SharePointグループ	SharePoint独自のグループで、権限制御を目的に利用するサイト毎のグループ。 セキュリティグループやMicrosoft 365グループ、複数のユーザーをまとめて、グループを作成する。 「フルコントロール」の権限を持つユーザーが作成可能。 サイト作成時は、規定の「メンバー」「閲覧者」「所有者」のSharePointグループが作成される。
4	ハブサイト	プロジェクト、部署、部門、地域などの組織属性に基づいて、SharePointの 関連サイトを接続および整理する中央ハブ。 サイトをハブサイトに関連付けると、関連付けられているすべてのサイトで、 コンテンツ、ニュース、サイトアクティビティを簡単に検出可能。 共有ナビゲーションとブランド、コンテンツのロールアップと検索などの機能が提供される。

2. ドキュメントライブラリの機能

2.1. SharePoint Onlineの構造

SharePoint Onlineはテナント、サイトコレクション、サイト、ドキュメント、ページ、リストの要素から構成される、階層的なコンテンツ管理システムです。
各サイトの中にドキュメントやページ、リストが存在します。



2.1. SharePoint Onlineの構造

SharePoint Onlineの各構造は以下の機能を持ちます。
本資料では<**ドキュメントライブラリ**>の機能と操作方法について詳細に解説していきます。

構造	機能
テナント	組織ごとに用意された SharePoint Online の専用スペース、環境全体を管理する最上位の単位
サイトコレクション	テナント内に作成されるサイトやサブサイトをグループ化したコンテナ 特定のプロジェクトや部門、目的ごとにサイトをまとめて管理する
サイト	情報共有、コンテンツ管理、共同作業を行うためのスペース ドキュメントライブラリ、ページライブラリ、リストなどの要素で構成される アクセス権限、ナビゲーション、外観などはサイトごとに設定を行う　(※1)
サブサイト	サイトや他のサブサイトの下に作成される、階層構造を持つサイト 特定のチーム、プロジェクト、部門など、より小さなグループの情報共有に利用 サイトのアクセス権限を、親サイトから引き継ぐか、親サイトとは異なる独自の権限を持つかを選択することが可能
ページライブラリ	サイト内で、Webパーツを組み合わせてページやニュースを作成し、保存・管理する
ドキュメントライブラリ	ファイルを保存、管理、共有するためのストレージ機能、Word、Excel、PDFなど様々な種類のファイルを保存可能 アクセス権限を設定して情報共有や共同作業を行う
リスト	情報を構造化して管理するための機能、Excelの表のようにデータを行と列で整理して共有する タスク管理、イベント管理、連絡先管理など様々な用途に使用される

※1　サイトは「チームサイト」と「コミュニケーションサイト」の2種類に分かれる。大きな機能の差異はないため、使用用途に分けて選択する。
チームサイト：チームやプロジェクトなど小規模での共同作業、情報共有に使用。Microsoft 365グループと接続可能。
コミュニケーションサイト：社内ポータルなど、幅広いユーザーを対象に情報発信する場に使用。

2.2. SharePoint Onlineの権限設定

SharePointでは**アクセス許可レベル**を利用して、ユーザーやグループにSharePointのサイトやドキュメントライブラリ、リスト、アイテムに対する操作権限を設定します。
あらかじめ定義された下記の許可レベルに加えて、独自のアクセス許可レベルを作成することも可能です。

アクセス許可レベル	権限
フルコントロール	サイト内のすべての設定、管理を行う
デザイン	サイトの外観の変更、リスト、ライブラリ、ページの作成・管理、アイテム(※1)の追加、編集、削除を行う
編集	リスト、ライブラリ、ページの作成・管理、アイテムの追加、編集、削除を行う
投稿	ページの作成、アイテムの追加、編集、削除を行う
閲覧	サイト内のページやリスト、ドキュメントを表示する、変更は不可

※1 アイテム：リストのアイテムやライブラリのドキュメントを含む

権限の設定対象

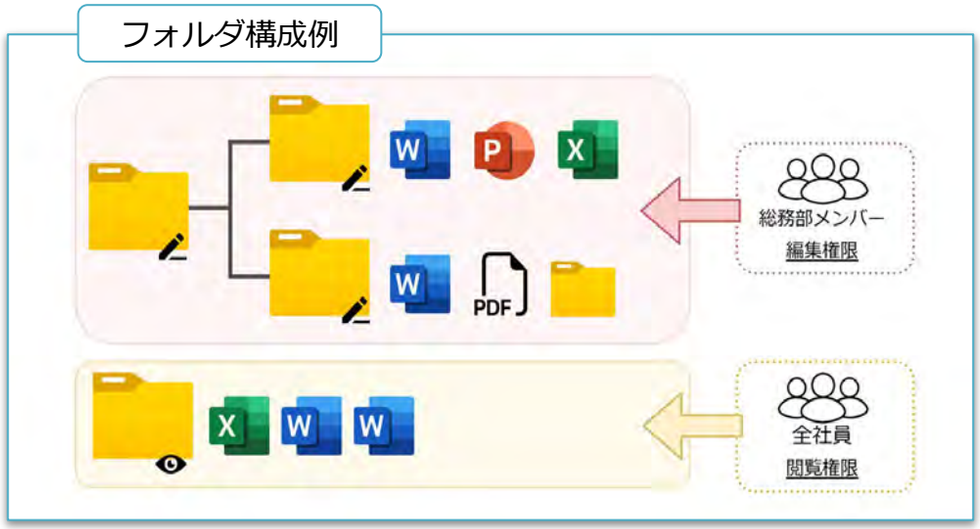
アクセス許可レベルは、ユーザーやグループに対して権限を設定することが可能です。※各グループの説明は用語集をご確認ください。

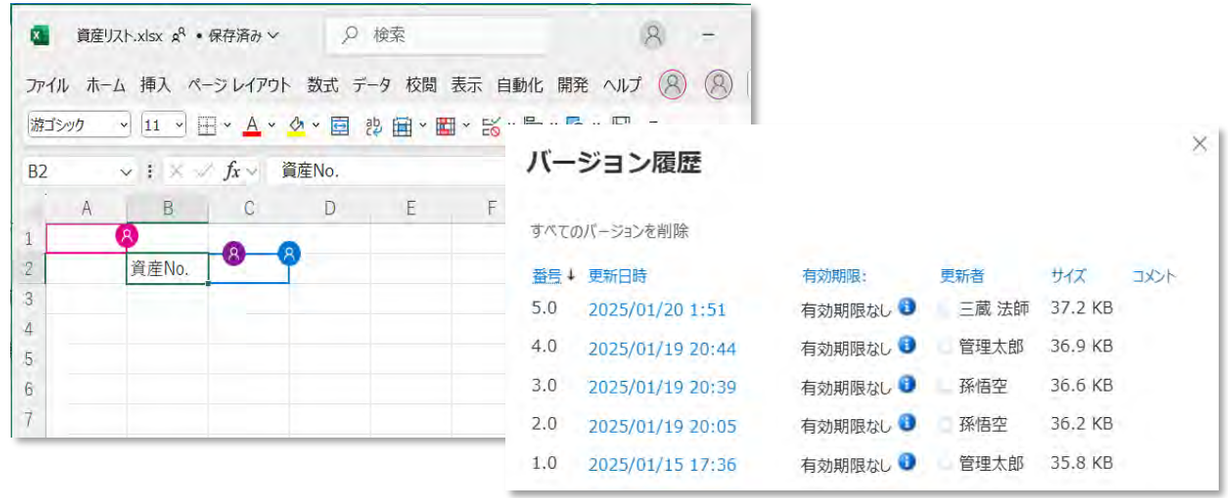
- **個々のユーザー**　（特定のユーザーを指定して権限を付与）
- **セキュリティグループ**　（Microsoft 365管理センターで管理）
- **Microsoft 365グループ**　（Microsoft 365管理センターで管理）
- **SharePointグループ**　（SharePointのサイト毎に管理）

また、組織外のアカウントへ外部共有を行うことも可能です。

2.3. ドキュメントライブラリの機能

SharePointのドキュメントライブラリは、ファイルを保存、管理、共有するためのストレージ機能を提供します。
チームがファイルを一元管理し、アクセス権を設定して共有・共同編集を行います。主な機能は以下の通りです。





ファイルの保存と整理

- Word、Excel、PowerPoint、PDFなど、様々な種類のファイル拡張子に対応
- フォルダやサブフォルダを作成してファイルを階層的に整理

権限設定

- ユーザーやグループごとに、フォルダ・ファイルのアクセス権限を設定
- 特定のユーザーにのみ編集を許可する、などのきめ細かい設定が可能
- 上位フォルダの権限が下位フォルダに継承される。（権限の継承）
  必要に応じて継承を中止して、独自の権限を設定可能

共同編集

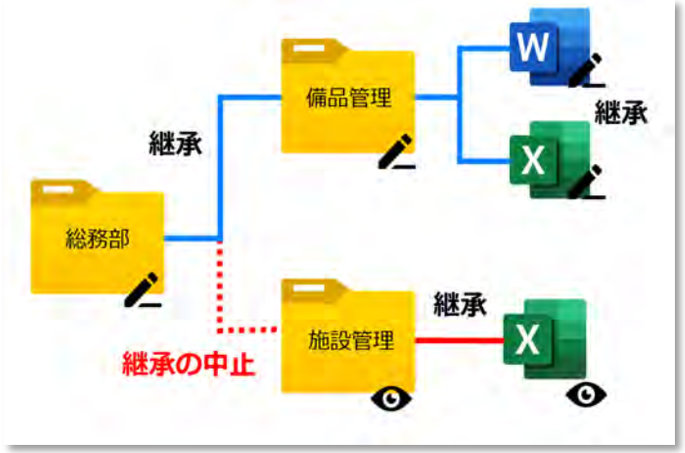
- 複数人が同時に同じファイルを編集可能
  変更内容はリアルタイムに反映される

バージョン管理

- バージョン履歴が自動的に保存され、変更履歴を確認できる
  必要に応じて以前のバージョンに復元可能

2.4. ドキュメントライブラリ アクセス権限の仕組み

SharePointのドキュメントライブラリでは、**誰がどのファイルやフォルダに対してどのような操作をできるか**、
「**アクセス許可レベル**」を用いて制御します。
SharePoint のドキュメントライブラリは階層構造を持つことが出来るため、**上位レベルで設定した権限は下位レベルに自動的に継承される**仕様です。（**権限継承**）
必要に応じて、**特定のフォルダやファイルの権限継承を解除し、独自の権限を設定する**こともできます。（**権限継承を中止**）
なお、ドキュメントライブラリ自体もサイトの権限を継承します。必要に応じて継承を中止することが可能です。



- 「総務部」フォルダには「編集」権限が設定されています。
  - 「備品管理」フォルダと配下のファイルは、「編集」権限を**継承**しています。
- 「施設管理」フォルダは**権限継承を中止**し、「閲覧」権限を設定しています。
  - 配下のファイルは「閲覧」権限を**継承**します。

権限継承のメリット

- **効率的な権限設定**
  上位レベルで一度権限を設定すれば、下位レベルに自動的に適用されるため、権限設定の手間を省くことができます。
- **一貫性の維持**
  すべてのファイルやフォルダに同じ権限が適用されるため、権限設定のミスや漏れを防ぎ、セキュリティレベルを維持することができます。

継承中止の注意点

権限の継承を中止する際は、以下の点に注意をして慎重に操作を行う必要があります。

- 上位レベルの権限設定が適用されなくなるため、意図せずアクセス権限が広がり、**セキュリティリスクが高まる**可能性があります。
- 権限継承を中止すると、**管理が煩雑**となり、「誰がアクセスできるのか」可視化が難しくなります。
- 権限継承を中止することで、ユーザーがアクセスできる範囲が変わってしまう可能性があります。

2.5. シナリオに応じたドキュメントライブラリの推奨構成

SharePointのドキュメントライブラリは、アクセス許可レベルや権限継承の機能を活用して、様々な状況に合わせたフォルダ構成を設定することが可能です。
ただし、前項の”継承中止の注意点”でも記載した通り、複雑な権限設定を行うことでセキュリティリスクや、管理の煩雑化を招いてしまうため、できるだけ**シンプルな構成**にすることを推奨します。
ここでは、ドキュメントライブラリ利用時のシナリオごとの推奨構成を紹介します。

シナリオ1：プロジェクトチームでの利用

目的

・プロジェクトメンバーでファイルを共有し、共同作業を効率的に行う。

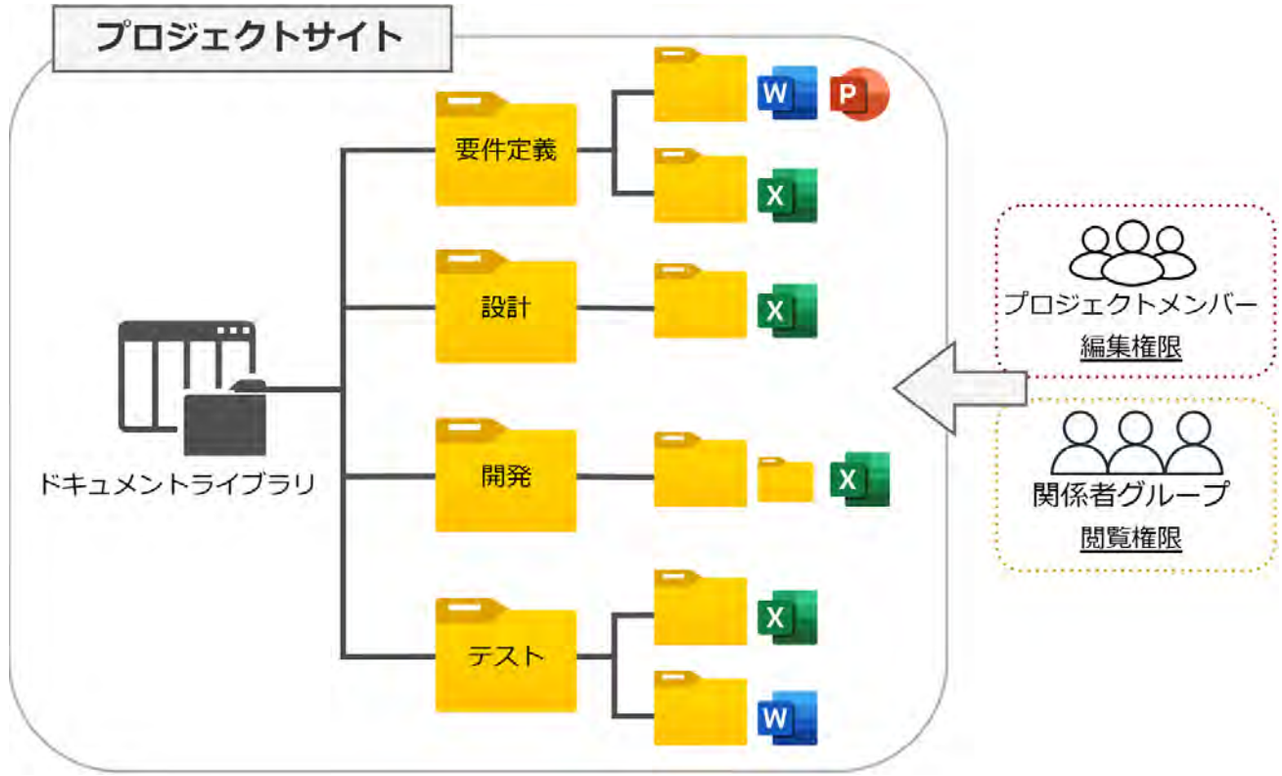
サイト・ドキュメントライブラリ構成

・プロジェクト専用のサイトを作成する。
・ドキュメントライブラリには、プロジェクトのフェーズや作業内容ごとにフォルダを作成し、ファイルを整理する。
例：「要件定義」「設計」「開発」「テスト」

アクセス権限

・プロジェクトの作業者全員にサイト全体の編集権限を付与する。
・実際に作業を行わない関係者（上司など）は、「関係者グループ」をSharePointグループとして作成し、サイト全体の閲覧権限を付与する。
※SharePointグループはサイトの権限内でのみ管理されるため、柔軟にグループを作成・管理出来る。
一時的な権限の場合は個人単位での付与も可能。

・サイトの権限がドキュメントライブラリに継承されるため、同様の権限を持つ。



2.5. シナリオに応じたドキュメントライブラリの推奨構成

シナリオ2：全社ポータル・部門ポータルでの利用

目的

・全社ポータル：全社員に対して企業情報、お知らせ、
規程類などをわかりやすく提供し、情報共有を促進する。
・部門ポータル：部署内での情報共有やコミュニケーション、資料類の共有を行う。

サイト構成

・全社ポータルと部門ポータルは、サイトを分けて作成する。

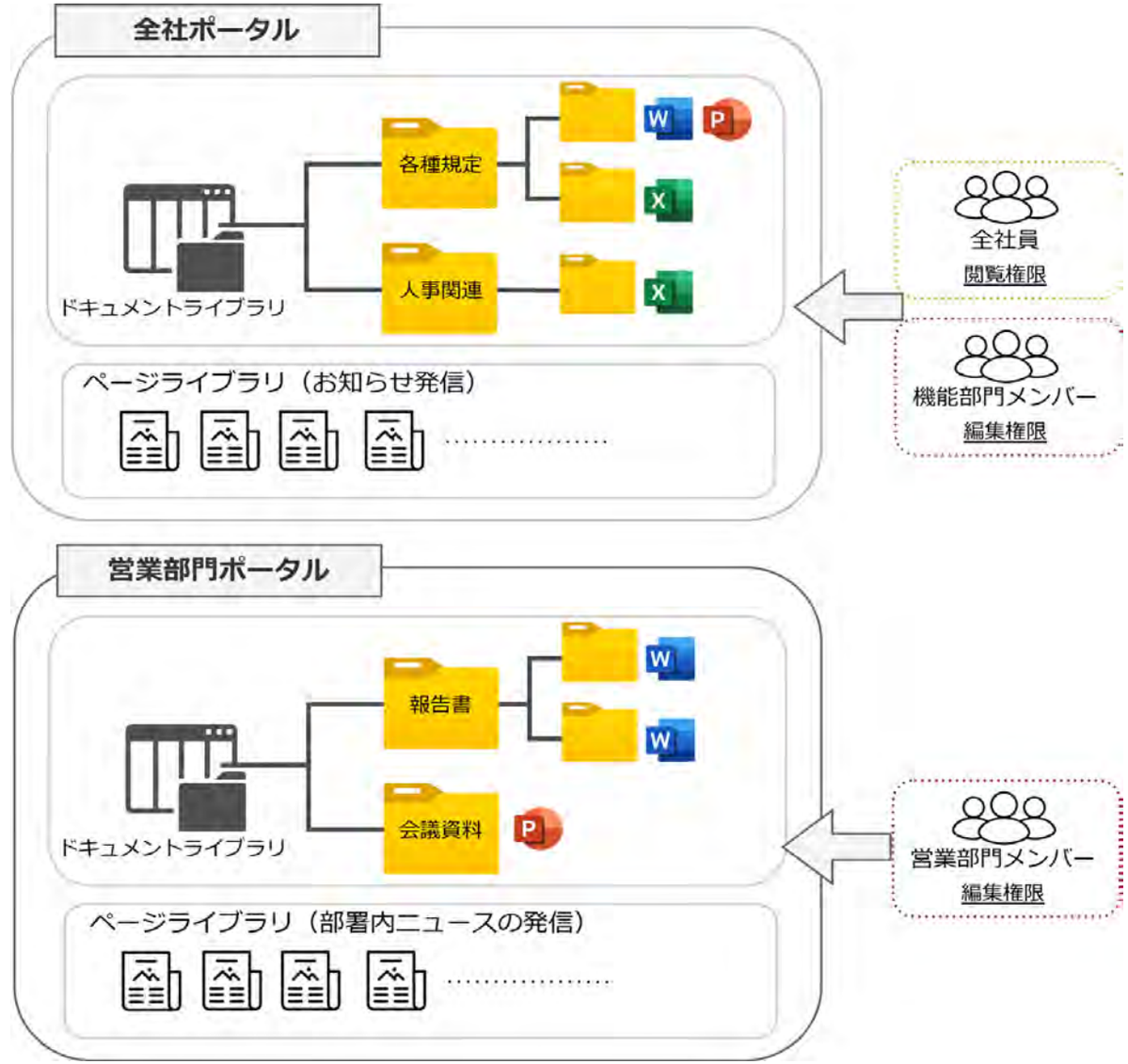
ドキュメントライブラリ構成

・全社ポータル：全社員共通のドキュメント
（例：人事関連、各種規程、マニュアルなど）を格納する。
・部門ポータル：部門固有のドキュメントを格納する。
必要に応じて、ドキュメントライブラリを「会議資料」
「報告書」などのカテゴリ別にフォルダ分けする。

アクセス権限

・全社ポータル：全社員に閲覧権限を付与する。ドキュメントの
作成や更新を行う機能部門にのみ編集権限を付与する。
・部門ポータル：部門メンバーに編集権限を付与する。

目的や利用者が異なる場合は、管理者の負担低減や利用者の利便性向上のために、
サイト単位で分けて運用を行うことを推奨します。
「ハブサイト」機能を用いることで、サイトの関連付けを行うことも可能です。



2.5. シナリオに応じたドキュメントライブラリの推奨構成

シナリオ3：外部共有と内部利用の分離

目的

・外部ユーザーとのファイル共有を安全かつ効率的に行う。
・機密情報を含むファイルへのアクセスを制限し、情報漏洩のリスクを抑制する。
・外部ユーザーと内部ユーザーでアクセス権限を明確に分離し、管理を容易にする。

サイト構成

・部門ポータルのサイトに外部共有用と内部共有用の
ドキュメントライブラリを作成する。

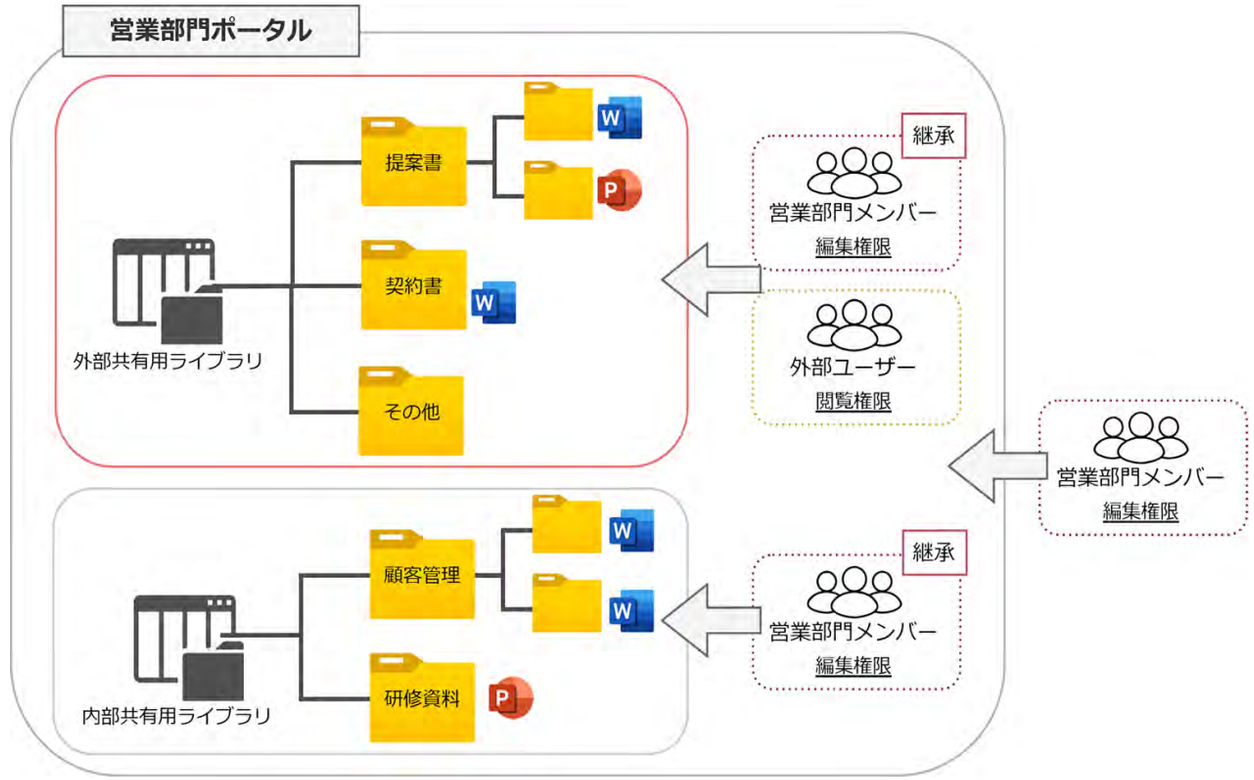
ドキュメントライブラリ構成

・外部共有用ライブラリ：外部ユーザーとの共有専用のライブラリ
・内部共有用ライブラリ：部署内で利用するライブラリ

アクセス権限

・部門ポータル：部門メンバーに編集権限を付与する。
・外部共有用ライブラリ：外部ユーザーに閲覧権限を付与する。
編集や削除は許可しない。必要に応じてダウンロードを制限するなど、
セキュリティ対策を強化する。
ファイルのアップロードや編集は部門メンバーが行う。（権限継承）
・内部共有用ライブラリ：サイトの権限を継承して、部門メンバーが
編集権限を持つ。

サイト内に複数のドキュメントライブラリを作成し、アクセス権限を分けることで、
セキュリティリスクの低減と、利用者の利便性向上が実現します。



3. テストケース検証

3.1. テストケース検証とその結果

本書は以下のテストケースに沿って検証を行います。検証の詳細は、次項のテストケース①②をご確認ください。

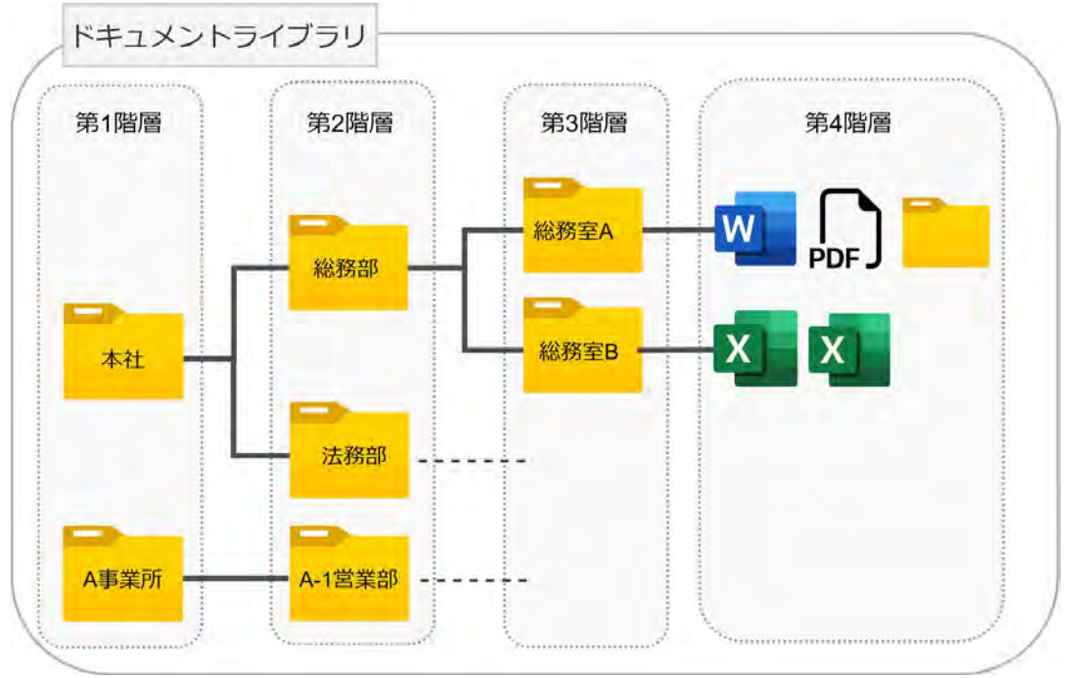
No.	テストケース	内容	検証結果
1	階層ごとのフォルダ権限設定	SharePoint Online にて、最上部とその 1 つ下の階層のフォルダに、下記のような制約を設けることは可能か。 <制約> ・フォルダ削除禁止 ・名前の変更禁止 ・フォルダの移動禁止 ・3 階層目以降や、最下層のファイルについては、自由に操作して構わない	アクセス許可レベルの「閲覧」を1,2階層目に設定し、3階層目に「編集」を付与することで、制御をすることが可能。 上記設定をした場合の留意事項として、3階層目のフォルダの名前変更が出来ない仕様になる。
2	ファイルのダウンロード制御	Excelデータを編集はできてダウンロードはできないように設定することは可能か。	アクセス許可レベルの「編集」から、「アイテムを開く」の権限を剥奪したアクセス許可レベルを該当のファイルに付与することで、ダウンロードの制限が可能。 ただし、完全なダウンロード制限とはならず、ファイルの種類や操作方法によってはダウンロードが行えてしまうことがある。

3.2. テストケース①
階層ごとのフォルダ権限設定

3.2. テストケース① 階層ごとのフォルダ権限設定

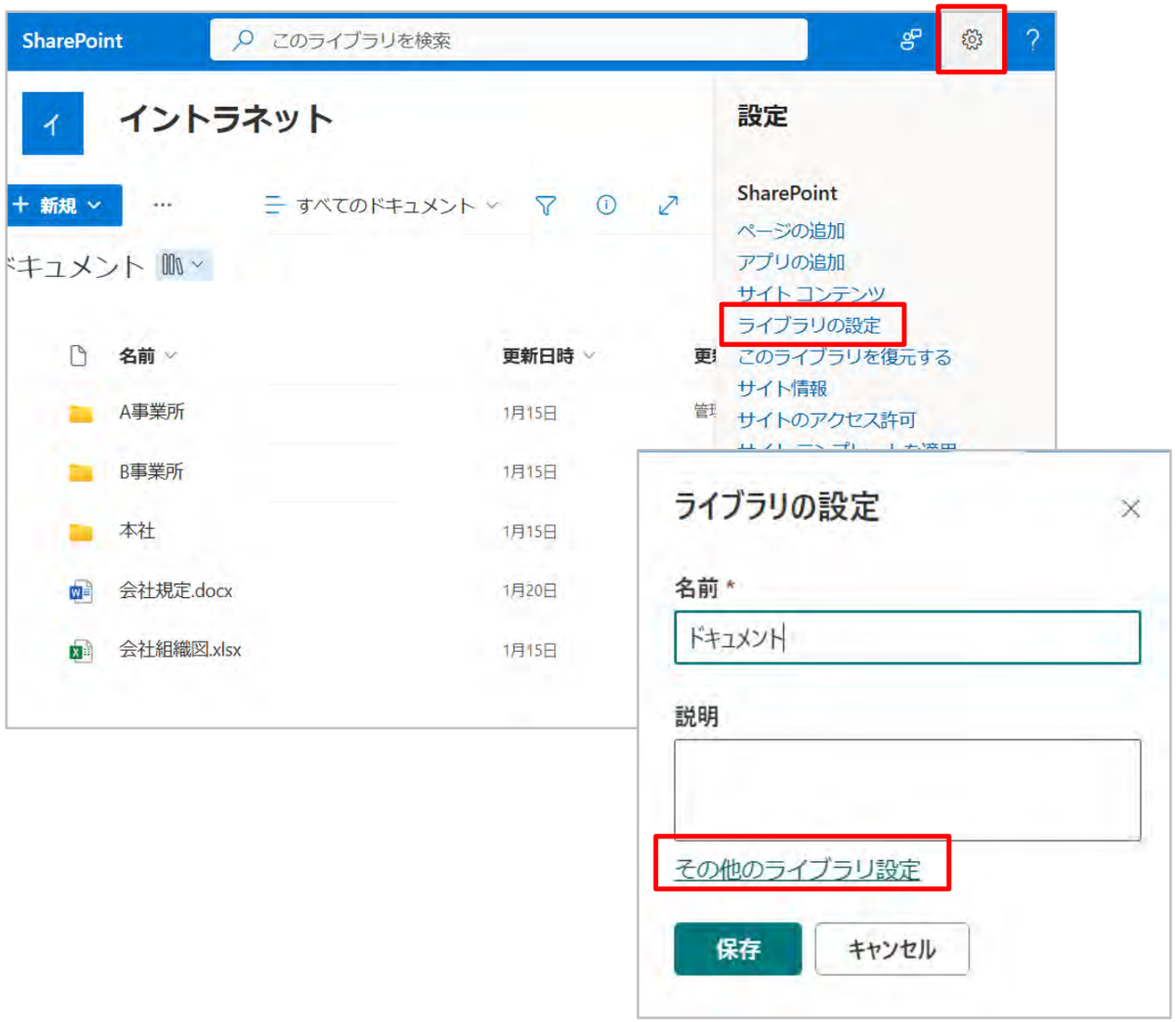
■検証内容
SharePointのドキュメントライブラリで最上部とその一つの階層フォルダに、フォルダの削除、名前の変更、フォルダの移動の制御を設定することが可能かを確認します。

■検証条件
右図のフォルダ構成でドキュメントライブラリを作成し、
1,2階層目の制御をするための設定を行います。
3階層目以降は自由に編集可能、権限を調整する対象のユーザーは、
外部ユーザーを除くテナント内の全メンバーとします。



■検証結果
アクセス許可レベルの「**閲覧**」を1,2階層目に設定し、3階層目に「**編集**」を付与することで、制御をすることが可能です。
上記設定をした場合の留意事項として、3階層目のフォルダの名前変更が出来ない仕様になります。
※削除や移動は可能です

3.2. テストケース① 階層ごとのフォルダ権限設定

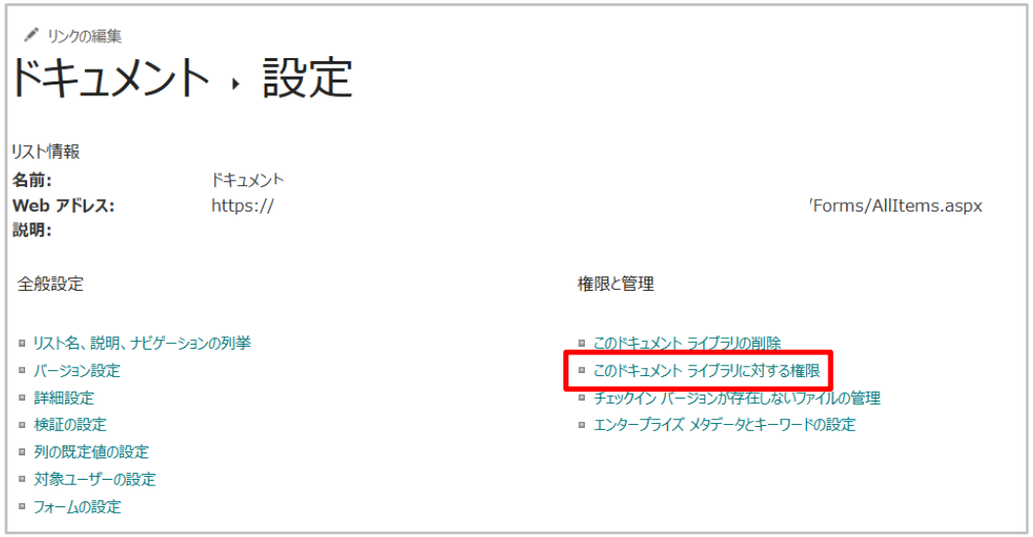


【権限の継承を中止】

1. 権限の設定を行う SharePoint サイトのドキュメントライブラリにアクセスします。

2. 画面右上の歯車アイコンをクリックし、[ライブラリの設定]> [その他のライブラリ設定] をクリックします。

3.2. テストケース① 階層ごとのフォルダ権限設定



【権限の継承を中止】

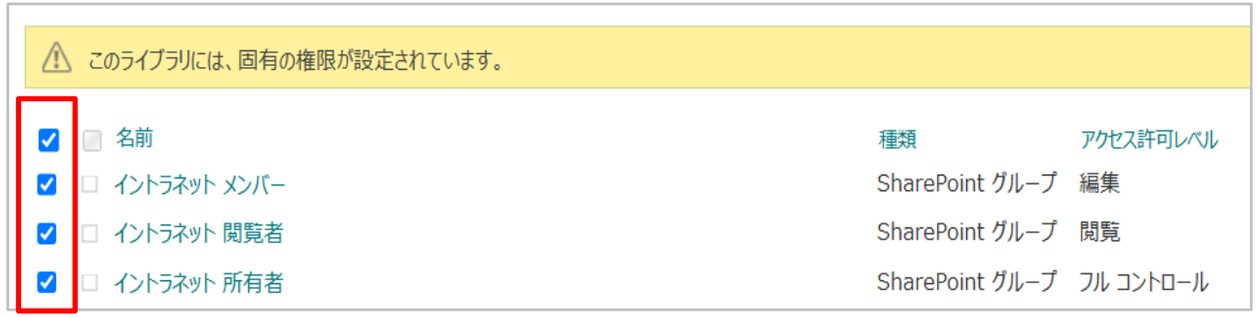
3. [権限と管理] 列の [このドキュメント ライブラリに対する権限] をクリックします。

4. 画面上部 [権限] タブに [権限の継承を中止] アイコンが存在する場合はクリックし、確認画面で [OK] をクリックします。

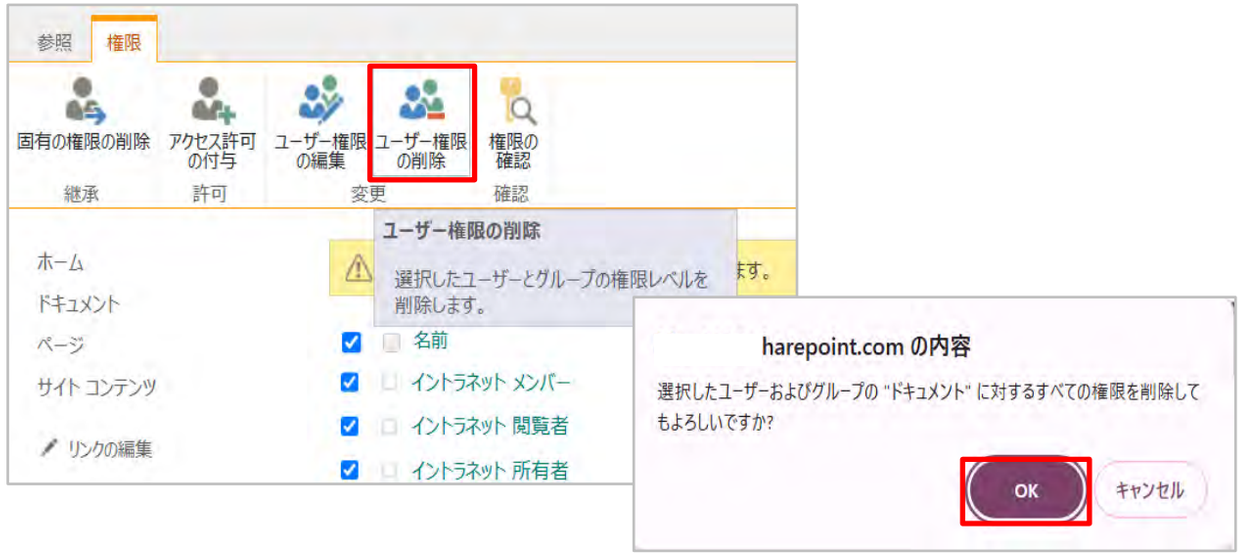
※ [権限の継承を中止] が存在せず、代わりに [固有の権限の削除] が存在する場合は、すでに目的の動作が設定されていますので、そのまま手順 5) へお進みください。

続いて、ライブラリに付与されているすべての権限をいったん削除します。

3.2. テストケース① 階層ごとのフォルダ権限設定

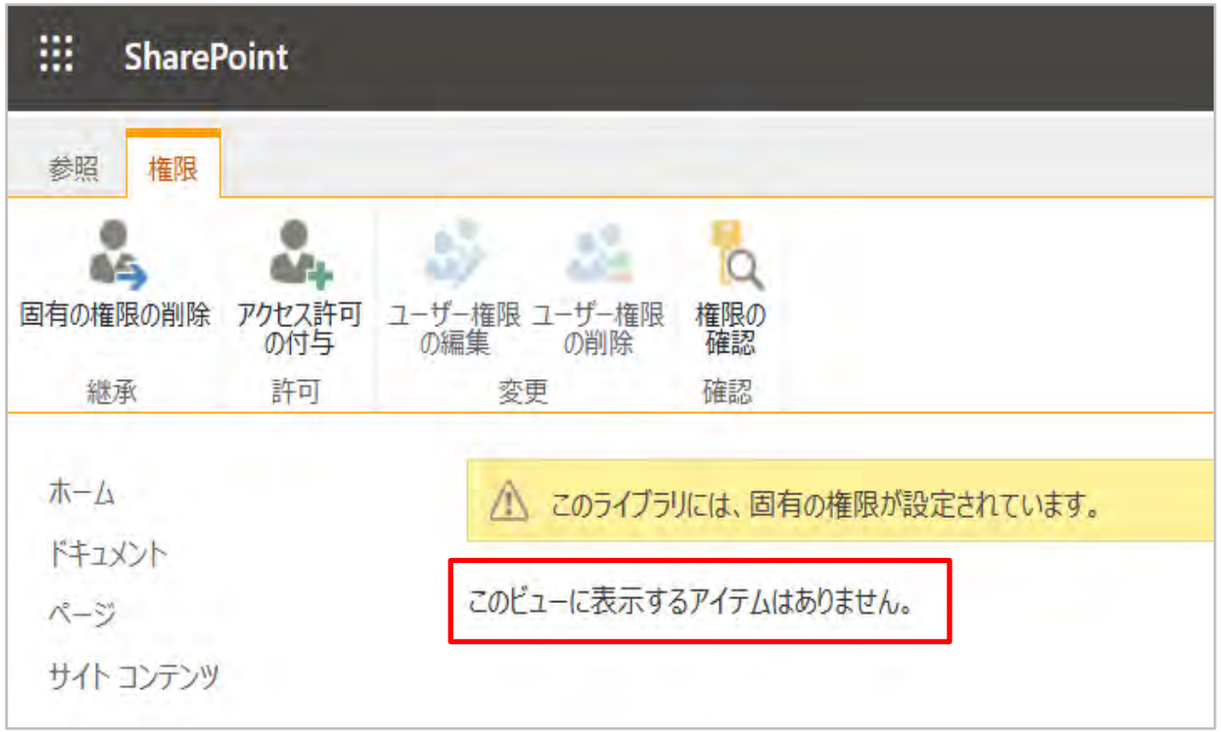


【ライブラリの権限削除】
5. 画面上の [名前] 見出し左横端に表示されているチェック ボックスをクリックし、画面内のすべてのアイテムを選択します。



6. [権限] タブの [ユーザー権限の削除] をクリックし、確認画面で [OK] をクリックします。

3.2. テストケース① 階層ごとのフォルダ権限設定



【ライブラリの権限削除】
7. 画面上部にベージュの帯が表示されていて、
[このサイトへのアクセスが制限されているユーザーがいます。(中略) ユーザーを表示します。]
と言いう記述がある場合は、[ユーザーを表示します] リンクをクリックします。

8. 再度画面上にユーザーまたはグループが表示されたら、手順 5) と同様の方法ですべてのユーザーを選択し、[ユーザー権限の削除] をクリックします。

9. 確認画面で [OK] をクリックし、画面上からすべてのユーザーおよびグループが削除されたことを確認します。

ここまでの手順で、該当のドキュメント ライブラリに付与されているアクセス許可を、一旦すべて削除いたしました。
続いてこのライブラリに [閲覧] 権限を付与する手順を実施します。

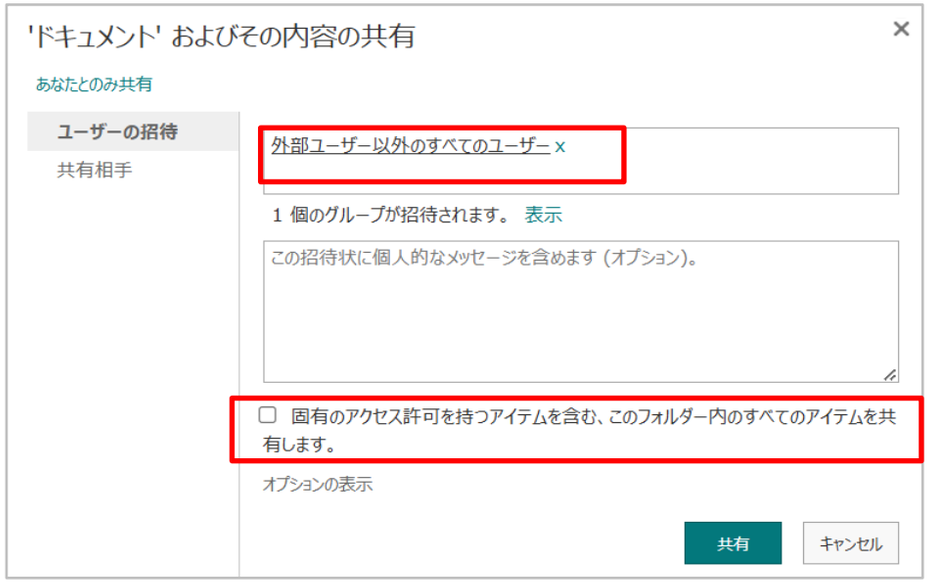
3.2. テストケース① 階層ごとのフォルダ権限設定

【ライブラリへ閲覧権限の付与】

10. 画面上部の [権限] タブにある [アクセス許可の付与] をクリックします。

11. ['ドキュメント' およびその内容の共有] 画面で、左上部にあるテキスト ボックスに "外部ユーザー" と入力します。

3.2. テストケース① 階層ごとのフォルダ権限設定



【ライブラリへ閲覧権限の付与】

12. ボックス下部に表示される “外部ユーザー以外のすべてのユーザー” をクリックして選択します。

13. [固有のアクセス許可を持つアイテムを含む、このフォルダ内のすべてのアイテムを共有します] チェック ボックスをオフにします。

14. [オプションの表示] をクリックし、[アクセス許可レベルの選択] を展開して [閲覧] をクリックします。

※ [電子メール招待状を送信する] オプションは、今回はオン・オフどちらでも構いません

15. [共有] をクリックします。

ここまでの手順で、このドキュメント ライブラリに対し、テナント内の全メンバーに [閲覧] 権限を付与いたしました。

続いて、自由な操作を許可するフォルダに対し、同じくテナント内の全メンバーに [編集] 権限を付与する手順を実施します。

3.2. テストケース① 階層ごとのフォルダ権限設定

【第3階層に編集権限を付与】

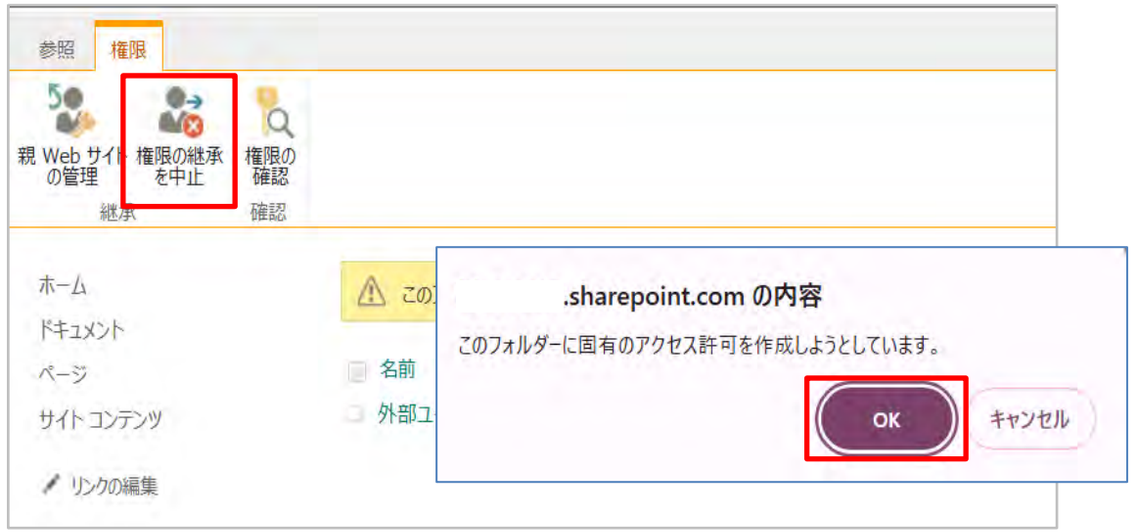
16. 自由な操作を許可するフォルダを含むフォルダ（2階層目のフォルダ）を開きます。

17. 自由な操作を許可するフォルダ（3階層目のフォルダ）が表示されたら、右クリックし [アクセス許可の管理] をクリックします。

3.2. テストケース① 階層ごとのフォルダ権限設定

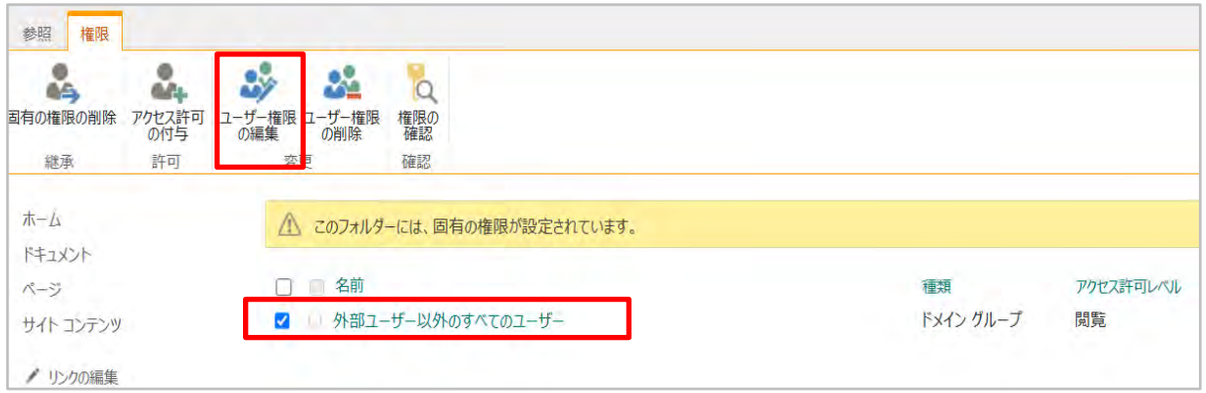
【第3階層に編集権限を付与】

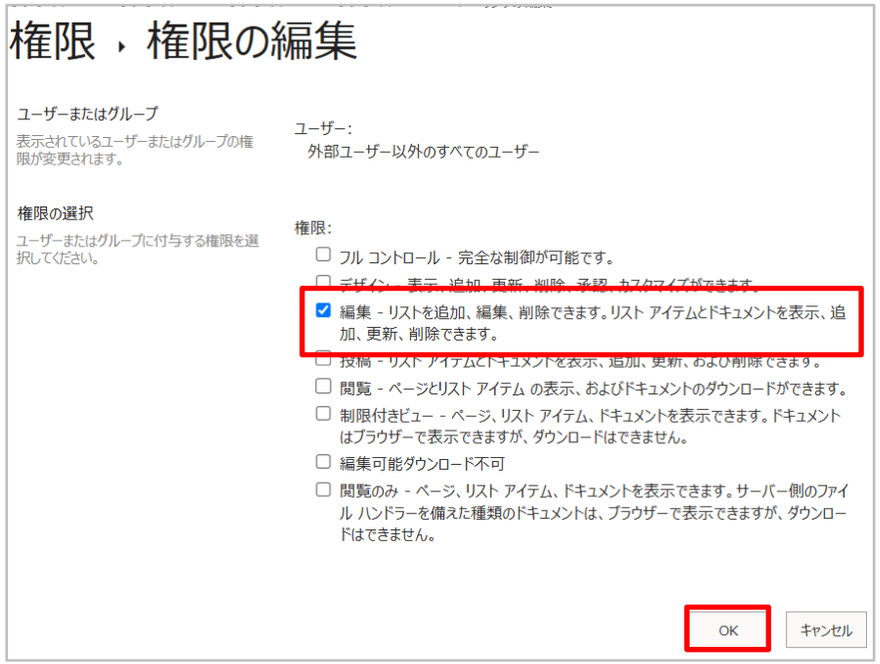
18. [アクセス許可を管理] 画面最下部右の [詳細設定] リンクをクリックします。



19. [権限] タブ上の [権限の継承を中止] をクリックし、確認画面で [OK] をクリックします。

3.2. テストケース① 階層ごとのフォルダ権限設定





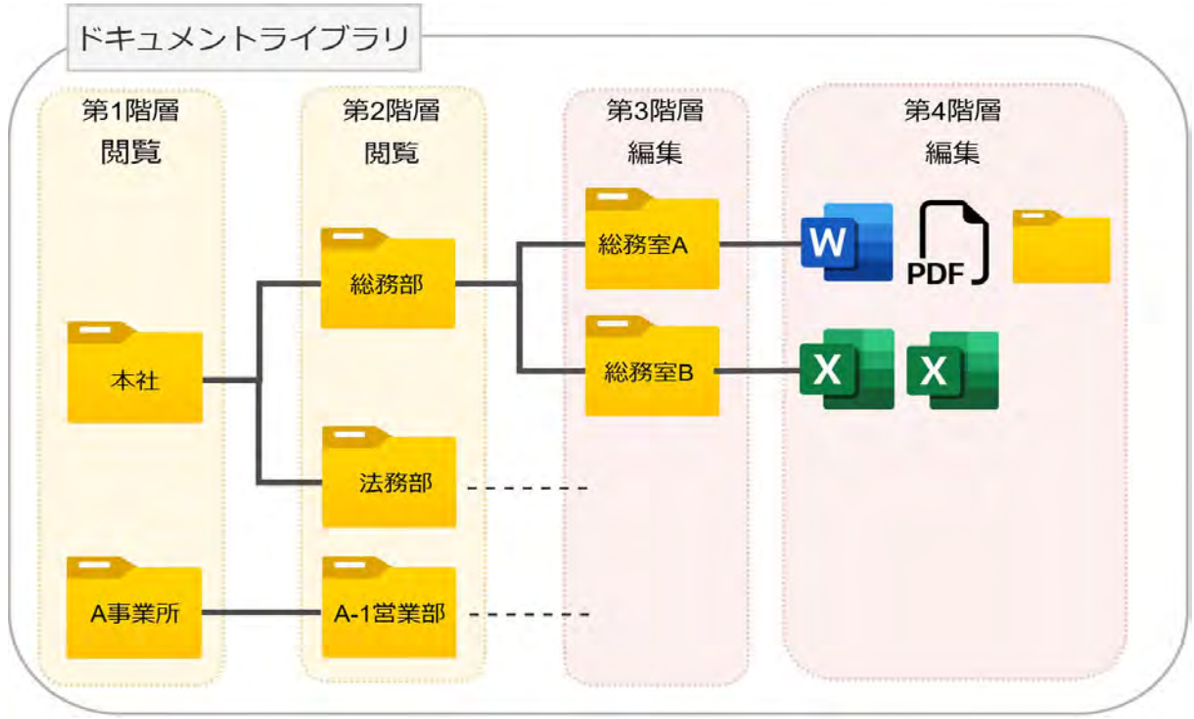
【第3階層に編集権限を付与】

20. 画面内に [外部ユーザー以外のすべてのユーザー] が表示されていることを確認しチェックを付け、[権限] タブの [ユーザー権限の編集] をクリックします。

21. 表示された画面の [閲覧] のチェックを外し、[編集] をクリックしてチェックします。
[OK] をクリックします。

3.2. テストケース① 階層ごとのフォルダ権限設定

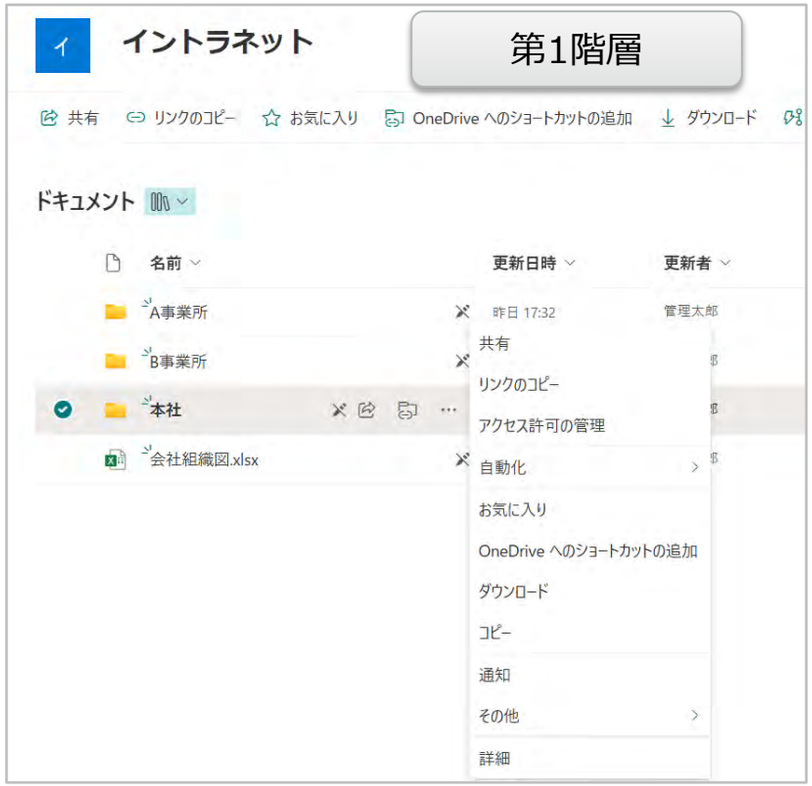
以上の操作で、1,2階層目に該当するフォルダに対してすべてのユーザーが「**閲覧**」の状態、
3 階層目に該当するフォルダに対して、すべてのユーザーが「**編集**」の状態にするための権限設定が完了しました。
以後、自由に編集などを許可するコンテンツはすべて3階層目以降のフォルダに格納します。
また、第3階層のフォルダに作成したサブフォルダについても、既定では「親の権限を継承」するので
自由に編集などを行うことができるフォルダ階層となります。
次スライド以降で1,2階層目に**フォルダの削除、名前の変更、フォルダ移動の制御**がされているか、設定後の画面を確認していきます。



3.2. テストケース① 階層ごとのフォルダ権限設定

設定後の画面（第1階層、第2階層）

第1階層、第2階層は「閲覧」権限を付与しているため、フォルダの削除、名前の変更、フォルダの移動は出来ません。
ファイルは読み取り専用で開かれます。



3.2. テストケース① 階層ごとのフォルダ権限設定

設定後の画面（第3階層）

第3階層のフォルダは「編集」権限が設定されています。以下の操作が可能です。

・フォルダの削除…可能

・フォルダの移動…編集権限が付与されている範囲で可能

・フォルダ名の変更…不可

※フォルダ名の変更が不可の理由

名前の変更を行う場合は、上位階層（第2階層）に対して

投稿以上の権限を持っている必要があるためです。

3.2. テストケース① 階層ごとのフォルダ権限設定

設定後の画面（第4階層）

4階層目以降のフォルダ・ファイルは移動、削除、名前の変更が可能です。※移動は編集権限を持つ範囲内

また、ファイル自体の編集を行うことも可能です。それ以降は権限が継承されます。

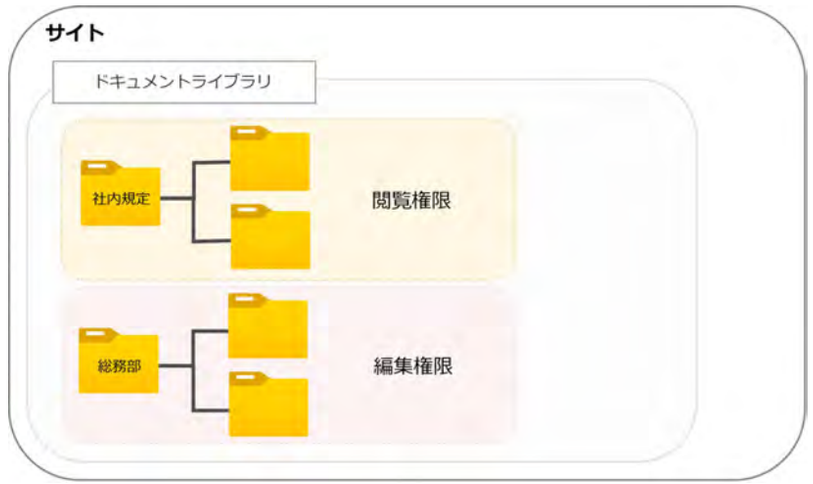
3.2. テストケース① 階層ごとのフォルダ権限設定

第3階層でフォルダ名の変更が出来ない仕様など、本設定は一部機能に制限が出てしまうこと、
第3階層のフォルダやファイルそれぞれに権限を設定する必要があるため、**権限の管理が煩雑**になってしまいます。
そのためドキュメントによって権限を分けたい場合は、以下のフォルダ構成にすることで、要望の権限設定が実現出来ます。

①1階層目からフォルダを分ける運用
閲覧権限を付与するフォルダと編集権限を付与するフォルダを作成

- ドキュメントライブラリ
  - ・第1階層（社内規定）：閲覧権限を付与
  - ・第2階層：閲覧権限を継承
    ※フォルダの削除、名前変更、移動が不可

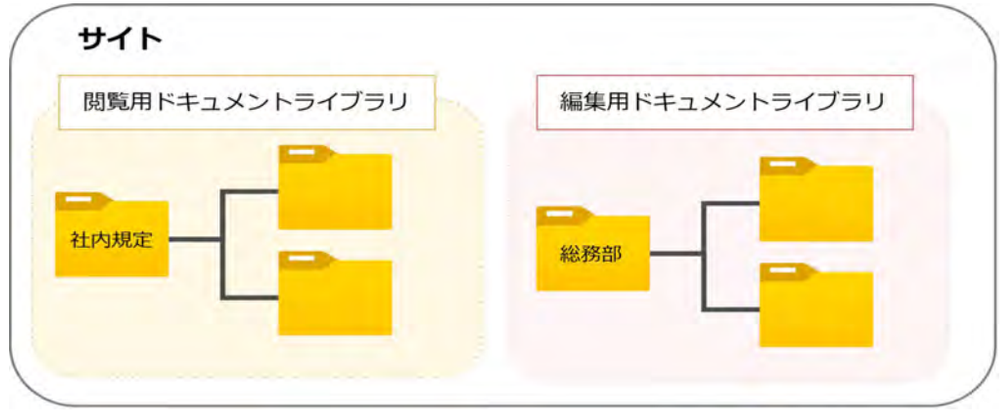
  - ・第1階層（総務部）：編集権限を付与
  - ・第2階層：編集権限を継承
    ※フォルダの削除、名前変更、移動が可能



②ドキュメントライブラリ自体を分ける運用
閲覧権限を付与するライブラリと編集権限を付与するライブラリを作成

- 閲覧用のドキュメント ライブラリ (閲覧権限)
  - ・第1階層（社内規定）：閲覧権限を継承
  - ・第2階層：閲覧権限を継承
    ※フォルダの削除、名前変更、移動が不可

- 編集用のドキュメント ライブラリ (編集権限)
  - ・第1階層（総務部）：編集権限を継承
  - ・第2階層：編集権限を継承
    ※フォルダの削除、名前変更、移動が可能



3.3. テストケース②
ファイルのダウンロード制御

3.3. テストケース② ファイルのダウンロード制御

■検証内容
SharePointのファイルに対して、編集可能な状態でダウンロード機能を制御することが可能か確認します。

■検証条件
権限を調整する対象のユーザーは、外部ユーザーを除くテナント内の全メンバーとします。
ライブラリ全体に「編集」権限が付与されていることを前提とします。

■検証結果
アクセス許可レベルの「**編集**」から、「**アイテムを開く**」の権限を剥奪したアクセス許可レベルを、
該当のファイルに付与することで、ダウンロードの制御が可能になります。
ただし、完全なダウンロード制御とはならず、ファイルの種類や操作方法によってはダウンロードが行えてしまうことがあります。

3.3. テストケース② ファイルのダウンロード制御

【アクセス許可レベルの作成】

1. サイトの管理者アカウントにて、対象のサイトにアクセスします。

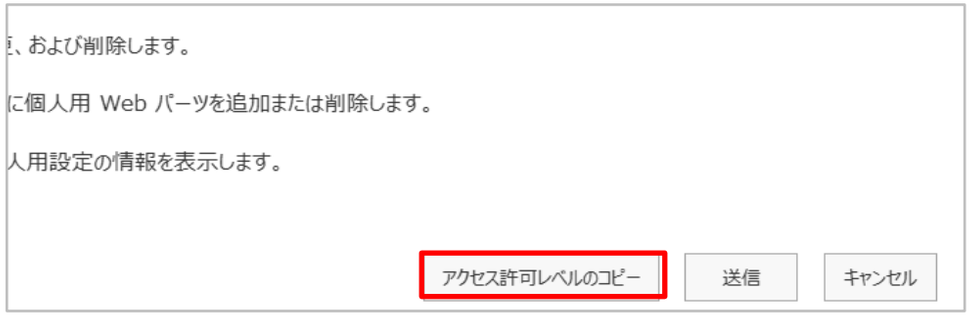
2. 右上の [歯車] - [サイトのアクセス許可] - [高度なアクセス許可の設定] の順にクリックします。

3.3. テストケース② ファイルのダウンロード制御

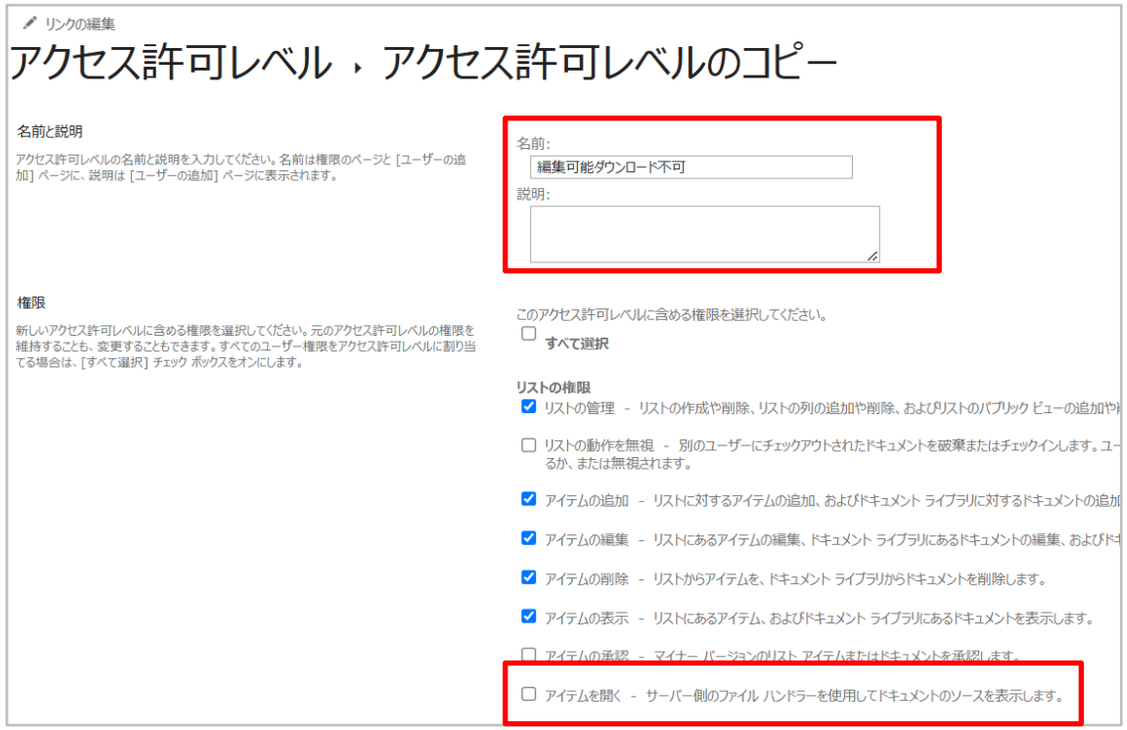
【アクセス許可レベルの作成】
3. 画面上部の [アクセス許可レベル] をクリックします。

4. 既定で存在しているアクセス許可レベルのうち、[編集] をクリックします。

3.3. テストケース② ファイルのダウンロード制御



【アクセス許可レベルの作成】
5. 画面最下部の [アクセス許可レベルのコピー] をクリックします。



6. "名前" 欄に任意の名称を入力します。
(編集可能ダウンロード不可、など)
7. "説明" 欄に権限に対する任意の説明文を入力します。(空白でも問題ございません)
8. "権限" 項目の [アイテムを開く] のチェックを外します。

3.3. テストケース② ファイルのダウンロード制御

【アクセス許可レベルの作成】
9. 画面下部の [作成] をクリックします。

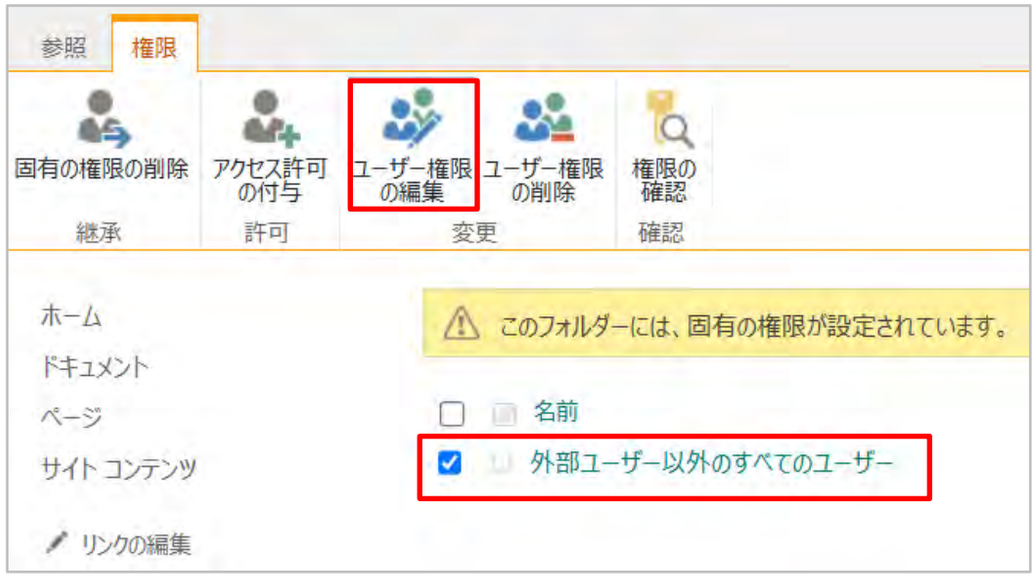
上記でアクセス許可レベルの設定が完了です。
作成されたアクセス許可レベルを対象のユーザーや、
対象のファイルごとに付与します。

【制限するフォルダへ権限の付与】
10. ダウンロードを制御するファイルが含まれる
フォルダ、またはファイルを選択します。
今回は“A-1営業部”と、その配下のフォルダ・ファイルに対して権限を制御します。
11. 権限を制御するフォルダが表示されたら、右クリックし [アクセス許可の管理] をクリックします。
12. [アクセス許可を管理] 画面最下部右の [詳細設定] リンクをクリックします。

3.3. テストケース② ファイルのダウンロード制御

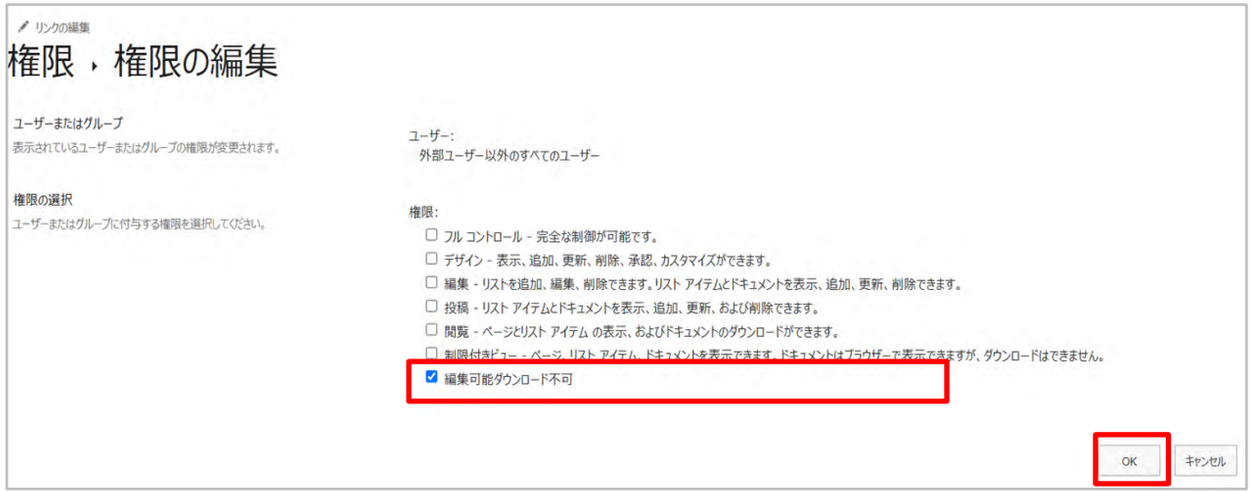
【制限するフォルダへ権限の付与】

13. [権限] タブ上の [権限の継承を中止] をクリックし、確認画面で [OK] をクリックします。



14. 画面内に [外部ユーザー以外のすべてのユーザー] が表示されていることを確認しチェックを付け、
[権限] タブ上の [ユーザー権限の編集] をクリックします。

3.3. テストケース② ファイルのダウンロード制御



【制限するフォルダへ権限の付与】

15. 表示された画面の [閲覧] のチェックを外し、作成した[編集可能ダウンロード不可] をクリックしてチェックします。 [OK] をクリックします。

以上の操作で、ファイルに対して、編集可能な状態でダウンロード機能を制御することが可能になります。

また、設定したアクセス許可レベルをフォルダに設定することで、フォルダに格納されたファイル全てに対してダウンロードが制御されます。

次スライド以降でダウンロードが制御がされているか、設定後の画面を確認していきます。

3.3. テストケース② ファイルのダウンロード制御

設定後の画面

権限を設定したファイルやフォルダは、[ダウンロード]の項目が非表示になります。
編集権限はあるため、フォルダ内にアイテムの追加をしたり、ファイルの編集・削除は可能です。

3.3. テストケース② ファイルのダウンロード制御

< [編集] の権限から [アイテムを開く] 権限をはく奪したアクセス許可レベルを作成する際の留意点 >

ファイルの編集は可能ですが、ファイルの [名前の変更] が行えなくなります。

3.3. テストケース② ファイルのダウンロード制御

< [編集] の権限から [アイテムを開く] 権限をはく奪したアクセス許可レベルを作成する際の留意点 >

本設定はサーバー側のファイル ハンドラーを備えたドキュメント (Office ファイル) のみ制御可能のため、ライブラリの表示を「クラシックUI」にしている場合、テキスト ファイルや動画ファイル、画像ファイルなどはダウンロードが出来てしまう仕様です。

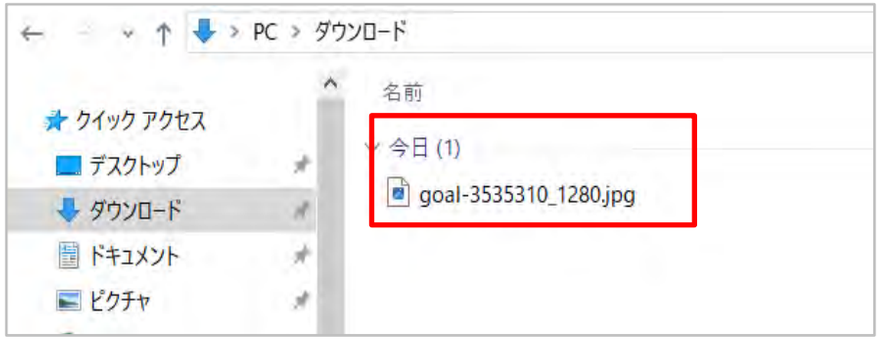
※モダンUIであれば、SharePoint上から画像やテキストファイルのダウンロードはできないため、UIの固定化を実施しておくことを推奨します。

リストとライブラリの既定のエクスペリエンスを新規またはクラシックから切り替える

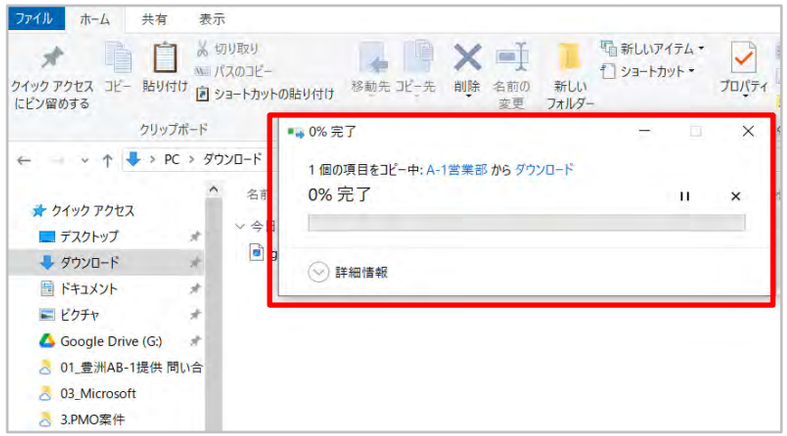
3.3. テストケース② ファイルのダウンロード制御

< [編集] の権限から [アイテムを開く] 権限をはく奪したアクセス許可レベルを作成する際の留意点 >

ただし、エクスプローラー上での画像やテキストファイルのコピーの作成（SharePoint → ローカルフォルダ）は、
制御不可のため、ダウンロードができる仕様です。



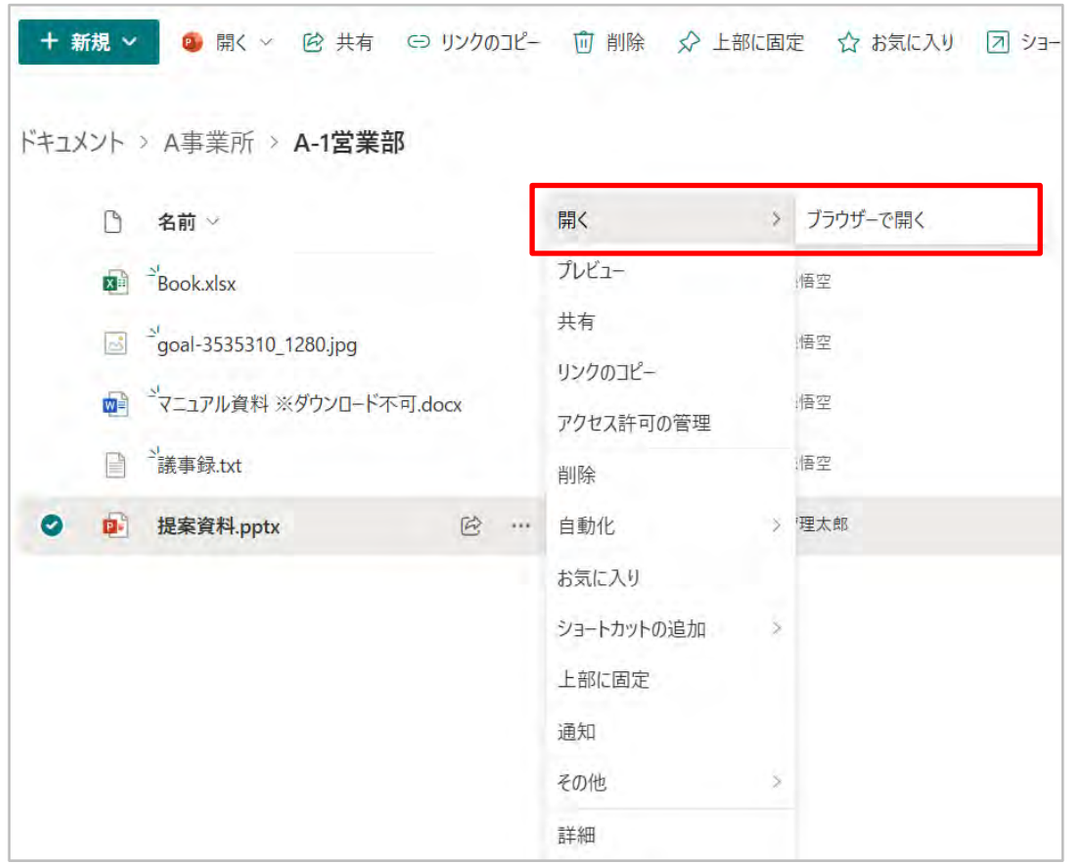
※Officeファイルはエラーが表示され、コピーは出来ません。



3.3. テストケース② ファイルのダウンロード制御

< [編集] の権限から [アイテムを開く] 権限をはく奪したアクセス許可レベルを作成する際の留意点 >

ファイルの編集はブラウザからのみ可能です。アプリでファイルを開くことは不可能になります。

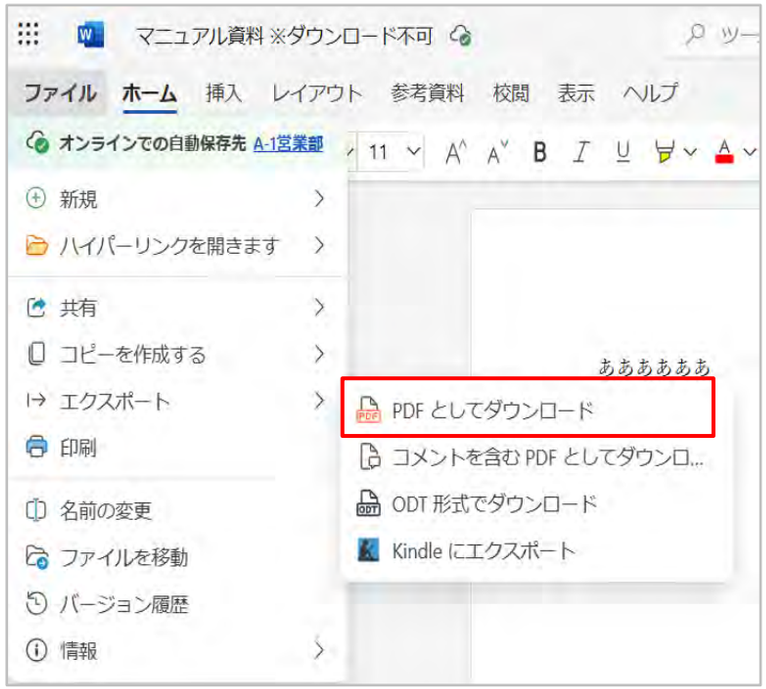


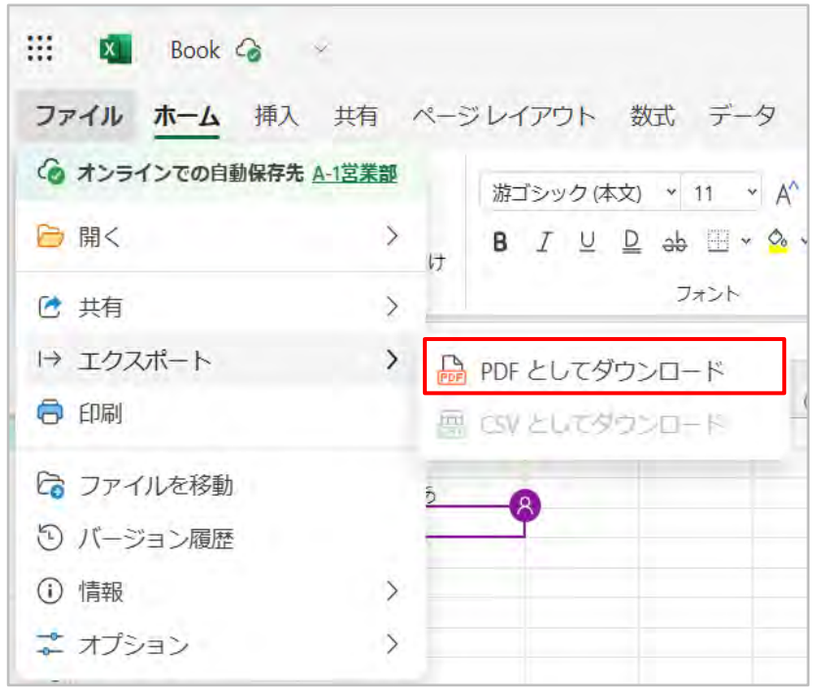
3.3. テストケース② ファイルのダウンロード制御

< [編集] の権限から [アイテムを開く] 権限をはく奪したアクセス許可レベルを作成する際の留意点 >

PDF化によるダウンロード制御は不可のため、Officeファイルの場合、「PDFとしてダウンロード」のオプションがブラウザから利用できてしまいます。

また、ブラウザからの「コピーの作成」は制御不可です。
PowerPointファイルの場合、「コピーをオンラインで作成」「コピーのダウンロード」がブラウザから出来てしまいます。





3.3. テストケース② ファイルのダウンロード制御

前項の設定を行った場合も**完全なダウンロード制限とはならず、ファイルの種類や操作方法によってはダウンロードが行えてしまう**ことがあります。
ダウンロード制御は、前項の設定以外にもいくつかの方法で実現できます。※ 一部制限事項あり

1. 「制限付きビュー」のアクセス許可レベルをライブラリやフォルダ・ファイルに設定する

「制限付きビュー」のアクセス許可レベルを設定することで、ドキュメントを閲覧可能な状態で、ダウンロードを禁止にすることが可能です。
この場合、コピーの作成やPDFによるエクスポートも制御されますが、ファイルの「編集」が出来なくなります。

2. ブロック ダウンロード ポリシーの設定を行う

SharePoint管理センターから「SharePointとOneDriveのダウンロードポリシーをブロック」の設定を行うことが可能です。
PowerShellを用いて、個々のサイトレベルでファイルのダウンロードを制御する機能です。
※ご利用にはSharePoint PremiumライセンスのSharePoint Advanced Management のアドオンが必要となります。　参考情報

3 . Information Rights Management (IRM) 機能の利用

直接的なダウンロード制限機能とは異なりますが、IRM機能を利用することで、以下の操作をライブラリ単位で制限することが可能です。

- IRM 機能をサポートしないドキュメント (Office ファイル以外のファイル) のアップロード
- ドキュメント ライブラリ内のアイテムを Office Online で閲覧
- 編集
- 閲覧者による印刷
- ダウンロード後のドキュメント上でのスクリプトの実行・スクリーン リーダーの使用
- ダウンロード後のドキュメントへのアクセス権の保持 (権限消失までの日数設定が可能です。)

※ご利用には RMS（Azure Information Protection）が含まれたMicrosoft 365プランの契約が必要になります。　参考情報