

IT 資格道場

DP-600 学習用テキスト

予備知識ゼロから合格ラインへ——読んで理解する1冊目

無料サンプル(第1章まで)

DP-600 出題範囲(Skills measured)2026-10-19版 準拠
2026年10月版

ご利用にあたって

- このテキストは「IT資格道場」(www.shikaku-doujou.com)の購入者限定テキストのうち、学習用テキストの第1章までを収録した**無料サンプル**です。どなたでもご覧いただけます。
- 無料サンプルも著作物です。転載・改変しての再配布・二次販売はできません。
- AI モデルの学習データとしてのご利用(学習目的の入力・データセット化を含む)はできません。
- 製品版(学習用テキスト・頻出度別ノート・暗記用ノートの3点)は、ご購入者を識別できる透かし入りのPDFとして提供されます。
- 本PDFはスマートフォン・タブレットでの閲覧に合わせたA5版面・文字サイズで組版しています。

目次

第1章 Maintain a data analytics solution [1.1/1.2]

権限は4つの層で重なる [1.1]

ワークスペース ロール [1.1]

アイテムの共有とアイテム権限 [1.1]

ウェアハウスと SQL 分析エンドポイントの行レベル セキュリティ [1.1]

列レベル セキュリティ、オブジェクト レベル、動的データ マスク [1.1]

セマンティック モデルの行レベル セキュリティ [1.1]

セマンティック モデルのオブジェクト レベル セキュリティ [1.1]

OneLake security [1.1]

絞り方の選び方 [1.1]

秘密度ラベル [1.1]

アイテムの推奨 (endorsement) [1.1]

Git 統合 [1.2]

Power BI プロジェクト (.pbip) [1.2]

デプロイ パイプライン [1.2]

系列ビューと影響分析 [1.2]

XMLA エンドポイント [1.2]

再利用できる資産 (.pbit、.pbids、共有セマンティック モデル) [1.2]

サンプルはここまでです

3冊の使い方は、ダウンロード欄の案内を参照してください。

SAMPLE

第1章 Maintain a data analytics solution

[1.1/1.2]

Fabric のソリューションを維持する仕事は、2 つの問いに分かれます。誰に何を見せるか (1.1) と、作った物をどう安全に変えて運ぶか (1.2) です。どちらも「その操作は誰ができるか」「その設定はどの層に効くか」を取り違えると、選択肢の差が見えなくなり、正解を選べません。出題範囲は、試験ガイドの Maintain a data analytics solution にある 11 項目です。[^c1-34]

日本語で受験するときは、次の語の対応を頭に置きます。

本文の語	日本語版で見かける語
Admin / Member / Contributor / Viewer	管理者 / メンバー / 共同作成者 / ビューアー
アイテム権限	項目レベルのアクセス許可、アイテム共有
秘密度ラベル	機密ラベル、秘密度ラベル
推奨 (endorsement)	推奨、保証、承認
Promoted / Certified / Master data	昇格 (プロモート) / 認定 / マスター データ

権限は 4 つの層で重なる [1.1]

Fabric の権限は、広い順にワークスペース ロール、アイテム権限、コンピュータ権限、OneLake security の 4 層です。データに届くまでの評価は 3 段で、Microsoft Entra の認証、Fabric へのアクセス、データ セキュリティ (テーブルやファイルへの操作の可否) の順に進みます。各段で権限が要ります。1 段でも欠ければ、データには届きません。[^c1-1]

層	効く範囲	使いどころ
ワークスペース ロール	ワークスペース内の全アイテム	Admin / Member / Contributor / Viewer
アイテム権限	共有した 1 アイテムだけ	ロールを持たない人に 1 つだけ見せる
コンピュート権限	各エンジンの内側 (SQL 分析エンドポイント、セマンティック モデル)	テーブル、列、行まで絞る
OneLake security	OneLake のテーブルとフォルダー	ロールごとに読める場所を決める

SQL 側の権限は、SQL 経由のクエリにだけ効きます。DAX 側の制限は、セマンティック モデル経由のクエリにだけ効きます。同じデータでも入口が違えば、片方の制限はもう片方を止めません。ワークスペース ロールは全アイテムに及び、コンピュート権限は 1 つのエンジンの中で細かく絞ります。

ワークスペース ロール [1.1]

ロールは Admin、Member、Contributor、Viewer の 4 種です。割り当てたワークスペースの中だけで有効で、他のワークスペース、容量、テナントには及びません。ロールを持たない人は、ワークスペースに入れません。[1-2]

できること	Admin	Member	Contributor	Viewer
ワークスペースの更新と削除、Admin の追加と削除	○			

できること	Admin	Member	Contributor	Viewer
workspace identity の作成、Git リポジトリへの接続	☐			
Member 以下のロールの追加、再共有 (reshare) の許可	☐	☐		
Lakehouse、Warehouse、パイプライン、ノートブックの作成・変更・削除と実行	☐	☐	☐	
オンプレミス ゲートウェイ経由の更新スケジュール	☐	☐	☐	
OneLake API と Spark での読み取り (ReadAll)、Lakehouse エクスプローラー	☐	☐	☐	
SQL 分析エンドポイントと Warehouse への接続、T-SQL での読み取り (ReadData)	☐	☐	☐	☐

できること	Admin	Member	Contributor	Viewer
パイプラインや ノートブックの 閲覧、実行結果 の確認	○	○	○	○

ロールを割り当てられる相手は、個人、セキュリティ グループ、Microsoft 365 グループ、配布リストです。Entra のサービス プリンシパルにも割り当てられ、Items REST API と Job Scheduler API では、ユーザーと同じ権限を引き継ぎます。複数のグループ経由でロールを持つ人は、その中で最も高い権限になります。低い権限のグループが勝つことはありません。グループを入れ子にしても、含まれる全員に権限が及びます。A さんが Viewer のグループと Contributor のグループの両方に入っていれば、実効のロールは Contributor です。

ノートブックの作成・変更・削除は、REST API でも Admin、Member、Contributor だけが行えます。Viewer は行えません。Job Scheduler API の実行の開始とキャンセルも同じ 3 ロールで、実行状況と出力の確認だけは、Viewer を含む全ロールができます。ゲートウェイの接続設定の変更や更新スケジュールには、ロールに加えて、ゲートウェイ側の権限が別に要ります。

間違えやすい点は 4 つあります。Viewer は T-SQL では読めますが、Spark と OneLake API では読めません。Contributor は、メンバーの追加も再共有の許可もできません。Reshare 権限を持たない限り、Contributor や Viewer はアイテムを共有できません。読ませるだけの目的でロールを上げると、Contributor 以上は書き込みもできるので、権限が過剰になります。

ロールは最小特権で選びます。見るだけなら Viewer、アイテムを作って実行するなら Contributor、メンバーの追加と共有の許可まで要るなら Member、

ワークスペースの設定と削除まで要るなら Admin です。必要以上のロールは付けません。

場面で確かめます。営業部のアナリストに、レイクハウスのデータを Spark ノートブックから読ませたいとします。アイテムの変更と削除は、させたくありません。Viewer では ReadAll が付きません。Contributor では書き込みまで付きます。ロールは Viewer のままにして、レイクハウスの共有で Read all with Apache Spark を付ければ、読み取りだけが加わります。この場面の答えは、ロールの引き上げではなく、アイテム権限の追加です。

相手	目的	付ける物
ロールを持たない人	1 つの Warehouse を T-SQL で読む	アイテム共有で Read と Read All with SQL analytics endpoint
ロールを持たない人	1 つの Lakehouse を Spark で読む	アイテム共有で Read と Read all with Apache Spark
Viewer	Spark で読む	アイテム共有で Read all with Apache Spark を追加
Viewer	特定のフォルダーに書き込む	OneLake security の ReadWrite ロール
誰か	ワークスペースの全アイテムを作成・変更する	Contributor 以上

アイテムの共有とアイテム権限 [1.1]

アイテム権限は、個別のアイテムだけに及びます。他のアイテムには及びません。ワークスペース ロールを持たない人に、1 つのアイテムだけを見せたいと

きに使います。共有すると、既定で Read が付きます。共有の画面で選べる権限は、アイテムの種類で変わります。[^c1-3]

権限	できること
Read	OneLake catalog (data hub) でアイテムを見つけて開く。Warehouse や Lakehouse の SQL 分析エンドポイントに接続する。共有時に必ず付く
Edit	アイテムとその内容を編集する
Share	自分が持つ権限の範囲までを、次の人に付与する
Read All with SQL analytics endpoint (ReadData)	T-SQL (TDS エンドポイント) でデータを読む
Read all with Apache Spark (ReadAll)	OneLake API と Spark、Lakehouse エクスプローラーで読む。Subscribe to OneLake events も一緒に付く
Build	セマンティック モデルの上に新しいコンテンツを作る
Execute	アイテムの実行とキャンセル

Read だけでは、SQL や OneLake の元データは読めません。Direct Lake のレポートを共有された人は、レポートを開けます。基の Delta テーブルを読むには、OneLake のデータ権限が別に要ります。[^c1-1] 閲覧者にレポートを見せる方法は 2 つで、レイクハウスに ReadData を直接付けるか、データソースの資格情報をシングル サインオン (SSO) から固定 ID に切り替えます。

Share を持つ人が次の人に付けられるのは、自分が持つ権限までです。Share、Edit、Read を持つ人は、その 3 つを超えて渡せません。

共有リンクの種類	使える相手
People in your organization	組織内の人。外部ユーザーとゲストには効かない
People with existing access	リンクを送るだけで、アクセスは付与しない
Specific people	指定した人やグループ。Entra のゲストには共有できるが、ゲストでない外部ユーザーには共有できない

管理者が People in your organization のリンクを無効にしている場合、使えるリンクは 2 種類に減ります。コピーして共有できるのは、People with existing access と Specific people のリンクだけです。サービス アカウントのようにリンクを使えない相手には、Manage permission の Direct access から Add user で直接付与します。

権限管理のページでは、ワークスペース ロールから継承された権限を、変更も削除もできません。アイテム権限を取り消しても、ロールが残っていれば、その人は引き続き見られます。見せたくないなら、ロールの削除が要ります。取り消しの反映には、サインイン中の人で最大 2 時間かかります。サインインしていない人は、次にサインインするまで評価されません。

場面で確かめます。社外のコンサルタントに、1 つの Warehouse だけを T-SQL で読ませます。ワークスペースのロールは付けません。相手は Entra のゲストです。Specific people のリンクで共有し、Read と Read All with SQL analytics endpoint を付けます。People in your organization のリンクは、ゲストに効かないので使えません。

場面で確かめます。Martaさんはワークスペースの Viewer で、Veronicaさんがレポートを共有していました。Veronicaさんがレポートに付けた Martaさんの権限だけを取り消しても、Martaさんはワークスペース経由で見続けま

す。見えなくするには、ワークスペースの Viewer も外します。外した後で改めてレポートを共有すれば、Marta さんは、ワークスペースに入れなくても、リンクで見られます。

セマンティック モデルでは、Build、レポートの共有、アプリでの配布の使い分けが出ます。[^c1-4] Build を付けずにレポートだけを共有された人は、閲覧できますが、基のモデルの上に新しいコンテンツは作れません (Reshare と Build を持つ人は、レポートの共有時に Build も付けられます)。新規コンテンツの作成、基礎データのエクスポート、Analyze in Excel、XMLA エンドポイントでのアクセスには、Build (ビルド) 権限が要ります。Contributor 以上は、ワークスペース内のモデルに Build を自動で持ちます。それ以外の人には、所有者が Manage permissions で Build を付けます。セマンティック モデルを共有するときも、共有の画面で Build を選んで付けられます (Allow recipients to build content...)。

アプリで配布するときは、Admin か Member が公開時に、アプリの権限を持つ人へモデルの Build も付けられます。モデルが別のワークスペースにあるアプリでは、利用者がモデルにもアクセスできないと、レポートが開きません。Build の申請は、既定では所有者へのメールです。独自の案内文に切り替えるときは、プレーン テキストしか使えません。切り替えられるのは Admin、Member、Contributor です。

ウェアハウスと SQL 分析エンドポイントの行レベル セキュリティ

[1.1]

Warehouse の RLS は、行を絞る条件を述語として書きます。述語は、インライン テーブル値関数です。それを CREATE SECURITY POLICY で表に結び付けます。[^c1-5]

```

CREATE FUNCTION Security.tvf_securitypredicate(@SalesRep AS
nvarchar(50))
    RETURNS TABLE
WITH SCHEMABINDING
AS
    RETURN SELECT 1 AS tvf_securitypredicate_result
WHERE @SalesRep = USER_NAME() OR USER_NAME() = 'manager@contoso.com';
GO

CREATE SECURITY POLICY SalesFilter
ADD FILTER PREDICATE Security.tvf_securitypredicate(SalesRep)
ON sales.Orders
WITH (STATE = ON);

```

`WITH (STATE = ON)` は、作ったセキュリティ ポリシーを有効にする指定です。OFF なら、述語は働きません。

Sales1 が 5 行、Sales2 が 5 行の計 10 行の表で試します。Sales1 と Sales2 は、相手の行を見られません。自分の 5 行だけが見えます。manager には 10 行が見え、どちらでもない人は 0 行です。0 行でもエラーにはならず、空の結果が返ります。

Fabric の Warehouse の RLS は、フィルター述語で行を絞ります。SELECT、UPDATE、DELETE では、該当しない行が黙って除外され、アプリはその存在に気づきません。INSERT は、後で見えなくなる行でも拒まれません。

ポリシーは、dbo や db_owner を含む全ユーザーに効きます。Admin、Member、Contributor に全行を見せたいなら、その条件を述語に書きます。

ポリシーは表ごとに別に作り、他の表には及びません。ポリシーのない表は、絞り込まれません。

項目	内容
SCHEMABINDING	セキュリティ ポリシーのオプションで、既定は ON。ON なら、述語が参照する表や関数への追加の権限確認は行われない。OFF なら、述語関数と参照先への SELECT または EXECUTE が利用者に要る
ポリシーの作成・変更・削除	ALTER ANY SECURITY POLICY が要る。作成と削除ではスキーマの ALTER も要る
述語ごとの権限	関数への SELECT と REFERENCES、対象の表と使う列への REFERENCES
関数を直すとき	先にポリシーを削除し、ALTER FUNCTION を実行して、ポリシーを作り直す

SQL 分析エンドポイントでは、CREATE TABLE ができません。CREATE SCHEMA、CREATE FUNCTION、CREATE SECURITY POLICY は実行できます。Warehouse に RLS を付けると、Direct Lake on SQL analytics endpoint のモデルの Power BI クエリは DirectQuery にフォールバックして、制限に従います。CLS の時の動きは、文書によって DirectQuery へのフォールバックともエラーとも書かれています。

列レベル セキュリティ、オブジェクト レベル、動的データ マスク [1.1]

列レベル セキュリティ (CLS) は、GRANT で、読ませる列だけを挙げます。[^c1-6]

```
GRANT SELECT ON Customers(CustomerID, FirstName, LastName, Phone,
Email) TO [Charlie@contoso.com];
```

挙げなかった CreditCard 列を含む SELECT * は、列の SELECT 権限が拒否されたというエラー (Msg 230) になります。列を指定して読めば、拒否されません。対応する認証は Entra だけで、SQL 認証は使えません。管理のしやすさから、個人よりロールへの付与が向いています。

オブジェクトレベルの制御は、GRANT、REVOKE、DENY で行います。ユーザーは、組み込みかカスタムのデータベース ロールに入れます。自分の権限は、sys.fn_my_permissions で確かめます。

CREATE USER は、明示的には実行できません。GRANT か DENY を実行した時点で、ユーザーが自動で作られます。そのユーザーが接続するには、ワークスペース ロールかアイテムの Read が、別に要ります。[^c1-7] 先に SQL で細かい権限を定義してから、ロールや Read を与えれば、接続した瞬間から制限が効いています。

動的データマスク (DDM) は、結果の見せ方だけを変えます。元のデータは変わりません。[^c1-8]

関数	結果
default()	型ごとの全面マスク。文字列は XXXX (短い列はそれ以下)、数値は 0、日付と時刻は 1900-01-01 00:00:00.0000000、バイナリは ASCII 0 の 1 バイト
email()	先頭 1 文字と固定の .com だけを見せる (aXXX@XXX.com)
random(開始, 終了)	数値型を、範囲内の乱数に置き換える

関数	結果
partial(prefix,"padding",suffix)	先頭と末尾の文字数を見せ、間に固定の文字列を入れる。値が短いと、見せる部分が削れる

partial(1,"XXXXXXX",0) は、555.123.1234 を 5XXXXXXX にします。
partial(5,"XXXXXXX",0) なら 555.1XXXXXXX です。

操作	必要な権限
マスクの追加・変更・削除	ALTER ANY MASK とテーブルの ALTER
マスクされた値を見る	SELECT
元の値を見る	列の UNMASK、またはデータベースの CONTROL

Admin、Member、Contributor は CONTROL 相当なので、マスクの影響を受けません。DDM 単独では、守り切れません。Salary > 99999 AND Salary < 100001 のような範囲検索で、値を推測できてしまいます。DDM だけに頼らず、CLS と RLS を併用します。

セマンティック モデルの行レベル セキュリティ [1.1]

セマンティック モデルの RLS は、ロールごとに DAX のフィルター式を書きます。式は行ごとに TRUE か FALSE を返します。FALSE の行は、見えません。
[^c1-9] 流れは、次の 4 手順です。

1. Power BI Desktop で、ロールと式を定義します (Modeling の Manage roles)。
2. セマンティック モデルとレポートを、サービスに発行します。
3. サービスで、ロールにメンバーを割り当てます。

4. Test as role で、絞り込みを確かめます。

メンバーの割り当ては、Desktop ではできません。ロール名にカンマは使えません。

静的な式は、[Region] = "West" のように、固定値で絞ります。動的な式は、[UserEmail] = USERPRINCIPALNAME() のように、ユーザー対応表の列とサインイン中のユーザーを突き合わせます。対応表で絞った結果は、リレーションを通して売上テーブルに伝わります。担当地域が West の [a@x.com](#) には West の行だけが見え、対応表に載っていない人は、どの行も見られません。

関数	Power BI Desktop	Power BI サービス
USERNAME()	DOMAIN\User の形	UPN
USERPRINCIPALNAME()	UPN (user@contoso.com の形)	UPN

CUSTOMDATA() は、埋め込みアプリが渡した文字列で絞る場面で使います。

RLS が効くのは、Viewer だけです。Admin、Member、Contributor は編集権限を持つので、効きません。Viewer が Build 権限を持っても、Analyze in Excel を含めて RLS が適用されます。RLS を効かせたい人に、Viewer 以外のロールを与えてはいけません。開発者が Contributor のまま確かめて全行が見えても、不具合ではなく仕様です。

ロールのメンバーにできるのは、ユーザー、Entra のセキュリティグループ、メール有効グループ、配布グループです。Microsoft 365 グループは追加できません。サービス プリンシパルも追加できず、それを最終的な実効 ID にするアプリでは、RLS は適用されません。外部の B2B ゲストは、グループ経由ではなく、メール アドレスで直接ロールに入れます。

フィルターは、既定では単方向に伝われます。リレーションで Apply security filter in both directions を有効にすると、双方向になりますが、性能に響くことがあります。複数の双方向リレーションに加わるテーブルでは、1 つのリレーションにしか選べません。

Test as role は、SSO を有効にした DirectQuery のモデルでは使えません。その場合は、Viewer ロールの本人でサインインして確かめます。Direct Lake のモデルでも、RLS は使えます。DirectQuery にフォールバックしても、RLS のフィルターは外れません。

セマンティック モデルのオブジェクト レベル セキュリティ [1.1]

オブジェクト レベル セキュリティ (OLS) は、テーブルや列を、特定のビューアーから隠します。権限のない人には、最初から存在しないように見えます。[1-10] RLS と同じく、モデルのロールの中で定義します。設定の道具は、TMDL ビューア、Tabular Editor などの外部ツールです。

```
createOrReplace
  role CategoriesOLS
    modelPermission: read
    tablePermission Customers
      columnPermission Address
        metadataPermission: none
```

metadataPermission が none なら、そのロールからは見えません。read なら見えます。tablePermission だけに none を書くと、テーブル全体が隠れます。権限のない人のビジュアルには、フィールドが見つからないというメッセージが出ます。

OLS も、Viewer だけに効きます。OLS を設定したモデルでは、Quick insights、Smart narrative、Excel Data Types ギャラリーが使いません。

CLS との違いは、隠れ方にあります。Warehouse の CLS は、列の存在を保ったまま、SELECT * を拒否します。OLS は、名前を含めて、存在ごと見えなくします。

OneLake security [1.1]

OneLake security は、Lakehouse 中のテーブルとフォルダー（ファイル）への読み取りを、ロールで決める仕組みです。[^c1-11] 既定では何も許可されません (deny-by-default)。許可を足すロールだけがあり、Deny ロールはありません。

構成要素	内容
Permissions	Read (SELECT と VIEW_DEFINITION 相当) か、ReadWrite (ALTER、DROP、UPDATE、INSERT 相当)
Type	Grant のみ
Data in role	テーブル、フォルダー、スキーマ。テーブルは行と列でも絞れる
Members in role	ユーザー、グループ、非ユーザー ID

ReadWrite は、Viewer のような読み取りだけの人に、特定の場所の書き込みを許すためのものです。Admin、Member、Contributor に付けても、効果はありません。ReadWrite のロールには、RLS も CLS も入れられません。

Lakehouse には、DefaultReader というロールが自動で作られ、ReadAll を持つ全員が Read になります。DefaultReader を消すと、ReadAll だけではデ

ータに届きません。Admin、Member、Contributor は、書き込み権限があるので届きます。配布リストをロールに入れると、SQL 分析エンドポイントはメンバーを解決できず、利用者はロールのメンバーに見えません。

上限と遅延	値
1 アイテムのロール数	250 (申請で 1,000 まで)
1 ロールのメンバー数と権限数	どちらも 500
ロール定義の変更の反映	約 5 分
グループのメンバー変更の反映	約 1 時間 (エンジンのキャッシュで、さらに約 1 時間)

フォルダーの権限は、下へ継承されます。子に権限があれば、親は辿れますが、兄弟は見えません。

```
Files/  
  folder1/  
    file11.txt          <- 見えない (subfolder11 の兄弟)  
    subfolder11/  
      file111.txt  
      subfolder111/  
        file1111.txt  
  folder2/  
    file21.txt          <- Role1 では見えない
```

Role1 のメンバーは、file111.txt と subfolder111 の中を読めます。folder1 は辿れますが、file11.txt と Tables は見えません。

テーブルとして扱われるのは、Tables/ の下にあり、_delta_log を持ち、子のショートカットを含まないフォルダーです。この条件を満たさないフォルダーに RLS や CLS を付けると、OneLake はアクセスを許可しません。

複数のロールの解決は、2 段で進みます。1 つのロールの中では、OLS、RLS、CLS の共通部分 (積) だけが残り、どれか 1 つを満たさない行や列は見えません。ロールをまたぐと、和 (最も緩い側) になります。同じ表に 2 つのロールの行条件があれば、OR で結合されます。city = 'Redmond' と city = 'New York' なら、両方の行が見えます。

列も和ですが、SQL 分析エンドポイントだけは和になりません。積の扱いで、1 つでも隠すロールがあれば、その列は隠れます。c1 と c2 を許すロールと、c2 と c3 を許すロールの両方に入った人は、Lakehouse では c1 から c3 の 3 列が見えます。SQL 分析エンドポイントでは c2 だけです。2 つのロールが異なる列を許し、かつ片方が行も絞る組み合わせは、使えません。一緒に効かせたい RLS と CLS は、同じロールに入れます。

ショートカットは、OneLake 同士なら、既定で呼び出した人の ID を使います (passthrough)。外部のストレージへのショートカットは、設定した接続の資格情報を使います (delegated)。OneLake 同士のショートカット自体には、OneLake security の権限を直接定義できません。

絞り方の選び方 [1.1]

要件	使う仕組み	効く入口
SQL で読む人に、表の行を見せない	Warehouse と SQL 分析エンドポイントの RLS	Warehouse と SQL 分析エンドポイントへのクエリ。 Direct Lake のレポートは DirectQuery に切り替わる

要件	使う仕組み	効く入口
レポートを見る人に、自分の担当の行だけ見せる	セマンティック モデルの RLS (動的なら USERPRINCIPALNAME)	セマンティック モデル経由のクエリ。Viewer にだけ効く
特定の列やテーブルを、存在ごと隠す	セマンティック モデルの OLS	セマンティック モデル経由のクエリ。Viewer にだけ効く
SQL の結果で、列の値を伏せて見せる	動的データ マスク	Warehouse と SQL 分析エンドポイントのクエリ結果。CONTROL を持つ人には効かない
Spark やファイルのフォルダーの範囲を絞る	OneLake security	OneLake のテーブルとフォルダー。ロールの Read と ReadWrite で決まる

Direct Lake のレポートで、SQL 分析エンドポイントにセキュリティを定めると、クエリは DirectQuery にフォールバックします。フォールバックを避けたいなら、元の Lakehouse のテーブルへのショートカットで、新しい Lakehouse を作ります。そこには、SQL の RLS と OLS を定めません。[^c1-1]

秘密度ラベル [1.1]

ラベルとポリシーは、Microsoft Purview Information Protection の物です。Azure Information Protection のラベルは、統合ラベル プラットフォームへ移行しないと、Fabric で使えません。[^c1-12] 付け方には、手動、既定 (default)、必須 (mandatory)、REST API によるプログラムの 4 通りがあります。

場面	要件
ラベルを付けられる人	テナント設定で指定したユーザーで、かつ、ラベルが Purview のポリシーでその人に公開されていること
サービスで付ける	Power BI Pro か PPU のライセンスと、コンテンツへの Edit 権限。Free は自分の My workspace のアイテムだけ
Desktop で使う	Pro か PPU、サインイン、テナントでの有効化。2020 年 12 月版より前の Desktop は、保護された .pbix を開けない
設定画面でラベルを選べない	使用権限が足りない。付けた人に変更を頼むか、管理者に使用権限を頼む

既定のラベルは、作成や編集のときに、利用者が自分で選ばなかった場合に付きます。Power BI 以外の Fabric アイテムでは、作成のダイアログがはっきりある場合にだけ付き、そうでない作成方法では付きません。ラベルの付与状況は、OneLake catalog で、ラベル付きとラベルなしの資産に分けて確認できます。

下流(ダウンストリーム)への継承(downstream inheritance)は、既定で ON です。[^c1-13] 対応する向きは、Power BI から Power BI、Fabric から Fabric、Fabric から Power BI です。Power BI のアイテムから Fabric のアイテムへは、伝わりません。

Lakehouse や Warehouse から自動生成されるアイテムは、親のラベルを取ります。さらに上流のラベルは継承しません。作成時にも継承が働き、次の組み合わせが親のラベルを引き継ぎます。

- Lakehouse から作ったパイプライン、ノートブック、ショートカット

- ノートブックから作ったパイプライン
- KQL Database から作った KQL Queryset とパイプライン

データソースのラベルを取り込んで適用できるのは、セマンティックモデルだけです。作成後に関係が変わったときも、ラベルは再評価されます。きっかけは、アイテムの内容や接続の変更、ラベル付きの新しいデータソースへの接続、新しい系列関係の追加（ノートブックを UI で Lakehouse につなぐ操作など）です。

場面で確かめます。Confidential のラベルを付けた Lakehouse から、ノートブックとセマンティックモデルを作り、そのモデルでレポートを作りました。ノートブックは作成時の継承で Confidential です。モデルは Fabric から Power BI への下流継承で、レポートは Power BI 同士の継承で、Confidential を取ります。逆に、Power BI のレポートに付けたラベルは、Fabric のアイテムには伝わりません。

必須ラベルが完全に効くのは、Power BI のアイテムだけです。Lakehouse、パイプライン、Warehouse では、ラベルを選んでも強制されず、ラベルなしで保存できます。

ラベルは、Excel、PDF、PowerPoint へのエクスポート、Analyze in Excel、.pbix のダウンロードに付いていきます。公開ポリシー付きのラベルなら、暗号化などのアクセス制御も保たれます。.csv と .txt のエクスポート、クロステナントのデータ共有では、アクセス制御は働きません。Git 統合では、秘密度ラベル付きのアイテムの書き出しが無効になることがあります。Power BI プロジェクト(.pbip)は、ラベルに対応していません。

アイテムの推奨 (endorsement) [1.1]

推奨は、信頼できるコンテンツを見つけやすくする印です。バッジが付き、一部の一覧では先頭に並びます。[^c1-14]

バッジ	付けられる人	付けられるアイテム
Promoted	アイテムの書き込み権限を持つ人なら誰でも	Power BI ダッシュボードを除く全アイテム
Certified	Fabric 管理者が認可したレビューアー（書き込み権限も要る）	Power BI ダッシュボードを除く全アイテム
Master data	Fabric 管理者が認可したレビューアー（書き込み権限も要る）	データを持つアイテム（Lakehouse、セマンティックモデルなど）だけ

Certified と Master data は、Fabric 管理者がテナントで有効にするまで使えません。認定の有効化は、ドメイン管理者に委任できます。ドメインごとに、別のレビューアーを置けます。

設定は、ワークスペースでアイテムの設定を開き、endorsement のセクションでバッジを選び、Apply を押します。権限がないと、Certified と Master data のボタンはグレーアウトされ、押せません。案内リンクの先で、認定や Master data の申請手順を確かめます。[^c1-15] リンクを押しても元の画面に戻るだけなら、管理者が案内を公開していません。その場合は、Fabric 管理者に直接連絡します。

Promoted か Certified のセマンティック モデルでは、Make discoverable をオンにできます。アクセス権のない人にも、モデルを発見させる設定です。セマンティック モデルを Promote か Certify するには、Pro か PPU のライセンス

が要ります。デプロイ パイプラインは、セマンティック モデルの推奨の設定を次のステージへコピーしません。

場面で確かめます。部門の売上モデルを、全社の基準にしたいとします。作成者は、書き込み権限があれば、Promoted を付けられます。Certified は、作成者が認可されたレビュアーでない限り、自分では付けられません。依頼は、組織の手順に従って出します。

Git 統合 [1.2]

Git 統合は、ワークスペース単位でバージョン管理します。サブフォルダーを含むワークスペースの構造が、リポジトリに保たれます。[^c1-16] 対応するプロバイダーは、Azure DevOps、GitHub、GitHub Enterprise のクラウド版です。オンプレミス版と主権クラウドには、対応していません。

接続の手順は、次のとおりです。[^c1-18]

1. ワークスペースの設定で Git integration を開き、プロバイダーを選びます。
2. 組織、プロジェクト、リポジトリ、ブランチ、フォルダーを指定します。接続できるのは 1 ブランチ、1 フォルダーだけで、複数は選べません。
3. Connect and sync を押します。

Azure DevOps の URL は、https://dev.azure.com/{organization}/{project}/_git/{repository} の形です。認証は OAuth2 かサービス プリンシパルです。GitHub は個人用アクセストークンを使い、fine-grained トークンの Contents の読み書き、または classic トークンの repo スコープが要ります。接続は利用者ごとの設定で、他の人の接続は引き継げません。自分のアカウントを設定します。

最初の同期は、片側が空なら、中身のある側から空の側へコピーされます。両方に中身があるときは、向きは自動では決まりません（自分で選びます）。ワークスペースを Git へコミットすると、Git の内容が上書きされます。Git からワークスペースを更新すると、ワークスペースの内容が上書きされます。Git は前の状態に戻せますが、ワークスペースは戻せません。後者を選ぶときだけ、確認が出ます。

操作	向き	選べる単位
Commit	ワークスペースから Git	変更したアイテムを選べる
Update	Git からワークスペース	選べない。常にブランチ全体を、最新のコミットまで同期する

Git のブランチに更新があると、ワークスペースを更新するまで、コミットは無効です。同じアイテムが両側で変わった競合では、解決するまで更新が無効です。コミットと更新を、同時には行えません。

Git の状態	意味
Synced	ワークスペースと Git で同じ
Uncommitted changes	ワークスペースに、コミットしていない変更がある
Update required	Git に、取り込んでいない更新がある
Conflict	同じアイテムが、両側で変更された
Unsupported item	Git が扱わないアイテム

競合の解決には、3 つの方法があります。[^c1-19] 1 つ目は UI で、Resolve Conflicts を選び、アイテムごとに Accept incoming changes (Git 側で上書

き)か Keep current content (ワークスペース側を残す) を選びます。2 つ目は、Undo か git revert で、最後に同期した状態へ戻す方法です。3 つ目は、新しいブランチを作り、Git 側で競合を解いてマージする方法です。切断して再接続する手もありますが、競合したアイテムだけを直す方法ではありません。全アイテムが上書きされます。

場面で確かめます。A さんがワークスペースでレポートを編集し、同じレポートを B さんが Git のブランチで更新しました。A さんがコミットしようとしても、ブランチに更新があるので無効です。Update を押すと、同じアイテムが両側で変わっているため競合になり、Resolve Conflicts が出ます。A さんの変更を残すなら Keep current content を選び、状態が Uncommitted changes に変わってから、改めてコミットします。

操作	必要なロール
Git への接続、切断、同期	Admin だけ
Checkout new branch	Admin。Switch branch と同じ設定が有効なら、Member と Contributor も可
Switch branch	Admin。ワークスペース設定 Allow users with at least Contributor role to change Git branch が有効なら、全アイテムに書き込める Member と Contributor も可
Commit、Update	Contributor 以上 (全アイテムへの書き込み権限が要る)。テナントの切り替えで所有者以外の更新を止めているときはアイテムの所有者であること、外部の依存先があればその Build も要る
Branch out to another workspace	Contributor 以上

Viewer には、Git に関する情報が見えません。[^c1-17] Branch out は、開発者が自分専用のワークスペースを別ブランチに結び付けて作業する操作です。共有のワークスペースを直接変えて、他の人に影響する事態を避けられます。[^c1-35] ファイル単位でコミットする機能は、まだプレビューで、正式な機能ではありません。

コミットの先を変えたいときは、Commit to new branch を使います。現在のブランチから離れずに、最後に同期した状態を基にした新しいブランチへコミットします。新しいブランチは、現在のワークスペースには接続されません。

上限と制約	値
対応するアイテム	一部だけ（一部はプレビュー）。非対応のアイテムは無視され、保存も同期も削除もされない
フォルダーの深さ	10 階層。空フォルダーは Git にコピーされない
ワークスペースのアイテム数	1,000
ブランチ名、パス全体、ファイル	244 文字、250 文字、25 MB
コミットの大きさ	Azure DevOps は、サービス プリンシパルで 25 MB、既定の SSO (Entra) ユーザーで 125 MB。GitHub は、一度に 50 MB
非対応の構成	サブモジュール。Azure DevOps で IP 条件付きアクセス検証が有効な場合

ワークスペースとリポジトリが別リージョンにある Azure DevOps では、テナント管理者が cross-geo export を有効にします。GitHub では、有効にする必要がありません。Analysis Services へのライブ接続のレポートやモデルと、プッシュ データセットは、対象外です。

2026 年 12 月 1 日以降は、ワークスペースのアイテムへの読み書き権限を持たない人は、Git 統合を使えません。デプロイ パイプラインの展開も、同じ日から全アイテムへの読み書き権限が要ります。この制限が当たる範囲は、文書によって書き方が違います (デプロイ パイプラインの文書は「保護ポリシー付きの秘密度ラベルで守られたアイテムを含むワークスペース」だけに当たると書き、Git 統合の文書は、ラベルと保護ポリシーの付いたアイテムに触れなくなることがあると書きます)。

Power BI プロジェクト (.pbip) [1.2]

Power BI Desktop で「名前を付けて保存」から .pbip を選びます。レポートとセマンティック モデルが、テキスト ファイルのフォルダーとして保存されます。Git に載せやすく、VS Code などで編集できます。[^c1-20]

```
Project/  
  AdventureWorks.Report/  
  AdventureWorks.SemanticModel/  
  .gitignore  
  AdventureWorks.pbip
```

.pbip ファイルは、レポート フォルダーを指すポインターにすぎません。開くと、対象のレポートとモデルが編集用に開きます。Fabric の Git 統合は、.pbip を作りません。レポート フォルダーの definition.pbir を開いても、同じ編集ができます。同じフォルダーに複数のレポートを置いても、.pbip を毎回作る必要はありません。

ファイル	役割
definition.pbir (Report 側)	レポートの定義と、使うセマンティック モデルへの参照。byPath は相対パス、byConnection は接続文字列
definition.pbism (SemanticModel 側)	セマンティック モデルの定義の入口
definition フォルダの TMDL	モデルの内容を、読みやすいテキストで持つ
.gitignore	既定で <code>**/.pbi/localSettings.json</code> と <code>**/.pbi/cache.abf</code> の 2 行

.gitignore は、保存先に存在しないときだけ作られます。localSettings.json は利用者と PC ごとの設定で、cache.abf はデータのキャッシュです。どちらもリポジトリに載せません。

場面で確かめます。既存のリポジトリに .pbip のフォルダーを入れたところ、cache.abf が毎回差分に出ました。リポジトリにはすでに .gitignore があったので、Desktop は新しい .gitignore を作りませんでした。

`**/.pbi/cache.abf` と `**/.pbi/localSettings.json` の 2 行は、自分で足します。

レポートの保存形式は 2 種類あります。PBIR-Legacy は report.json の 1 ファイルで、外部での編集に対応しません。PBIR は definition フォルダ内の複数の JSON で、公開スキーマがあります。変更の追跡とマージ競合の解決が楽になります。[^{c1-21}] version が 1.0 の definition.pbir では、PBIR-Legacy しか使えません。4.0 以上なら、どちらの形式も使えます。

Fabric の Git 統合では、モデルとレポートが同じワークスペースにあれば、byPath で書き出されます。ライブ接続で開きたいときは、byConnection を書いた別の .pbir ファイルを置けます。Git 統合は、definition.pbir 以外の

.pbir を処理しません。REST API でレポートを展開するときは、byConnection を使います。

モデルの外部編集には、2 つの道があります。外部ツールで Desktop の Analysis Services インスタンスに接続する方法と、definition フォルダの TMDL を直接編集する方法です。外で保存した変更は、Desktop が検出して適用を促します。report.json 、 mobileState.json 、 semanticModelDiagramLayout.json 、 SemanticModel の diagramLayout.json は、スキーマが公開されていません。外部での変更は、サポート対象外です。Desktop が作る自動の日付テーブルは、外部ツールで変更してはいけません。Fabric の REST API では、RLS ロールのメンバーと、増分更新のパーティションを、取得も設定もできません。

Desktop の Publish は、一時的な PBIX を発行し、メタデータに加えて、ローカルデータ キャッシュも展開します。Git 統合と Fabric API が展開するのは、メタデータだけです。Report Server 向けに最適化された Desktop では、Power BI プロジェクトは使えません。

リポジトリのこのフォルダーを Fabric の Git 統合につなぐと、Report と SemanticModel のフォルダーが、ワークスペースのレポートとセマンティックモデルとして同期されます。

差分の見方にも癖があります。たとえばメジャーの DAX 式を Desktop で変えて保存すると、モデルの定義ファイルに差分が出ます。Desktop は改行に CRLF を使うので、Git の autocrlf を有効にすると、不要な差分が出ません。外部のエディターで編集するときは、UTF-8 (BOM なし) で保存します。保存先のパスは Windows の既定で 260 文字に制限されるため、短いフォルダーを選びます。OneDrive や SharePoint へは、直接は保存できません。

デプロイ パイプライン [1.2]

デプロイ パイプラインは、ステージごとにワークスペースを 1 つ割り当て、内容をステージ間でコピーする仕組みです。ステージは 2 から 10 で、既定は Development、Test、Production の 3 つです。ステージの数と名前は、作成後に変更できません。[^c1-22] 公開 (public) にするかどうかは、いつでも変えられます。最後のステージは既定で public で、パイプラインの権限を持たない閲覧者には、通常のワークスペースに見えます。[^c1-25]

隣り合うステージの同じアイテムを結び付ける仕組みを、ペアリングと呼びます。ペアのアイテムは、展開で上書きされます。ペアでないアイテムは、名前と種類が同じでも上書きされず、重複したコピーが作られます。ペアは、名前を変えても保たれます。ワークスペースを割り当てた後に足したアイテムは、自動ではペアになりません。[^c1-26]

Development		Test		Production	
Sales(Report)	->	Sales(Report)	->	Sales(Report)	<- ペア。展開で上書き
Sales(Model)	->	Sales(Model)	->	Sales(Model)	
		Sales(Report)			<- 手で作った同名。ペアでない

展開で移るのは、メタデータだけです。データは移らないので、展開後にセマンティック モデルの更新が要ります。[^c1-23] 小さな変更 (テーブルの追加や削除など) では、ターゲットのデータが消えません。スキーマを壊す変更やデータソース接続の変更では、完全な更新が要ります。

区分	中身
コピーされる	データソース、パラメーター、レポートのビジュアルとページ、ダッシュボードのタイル、モデルのメタデータ、アイテムの関係
コピーされない	データ、URL、ID、ワークスペースとアイテムの権限、ワークスペースの設定、アプリのコンテンツ、個人用ブックマーク
セマンティック モデルでコピーされない	ロールの割り当て、更新スケジュール、データソースの資格情報、クエリ キャッシュの設定、推奨の設定

展開したユーザーが、複製されたセマンティック モデルの所有者になり、新しいワークスペースの唯一の Admin になります。

場面で確かめます。RLS のあるモデルを Test から Production へ展開しました。ロールの割り当ては移らないので、Production のサービスで、メンバーを割り当て直します。更新スケジュールとデータソースの資格情報も、同じように設定し直します。

初めて空のステージへ展開すると、容量上に新しいワークスペースが作られます。容量への割り当て権限がなければ、ワークスペースだけが作られ、内容はコピーされません。初回の展開の後、ターゲットのアイテムのゲートウェイは自動では割り当てられません。アイテムの設定で手動で対応づけ、更新が通ることを確かめます。

展開の方法	内容
Full	全アイテムを、ターゲットのステージへ
Selective (選択的なデプロイ)	選んだアイテムだけ

展開の方法	内容
Backward	後ろのステージから前のステージへ。ターゲットのステージが空(ワークスペース未割り当て)のときだけ可能

依存するアイテムがターゲットのステージにないと、展開は通りません。たとえばレポートは、セマンティック モデルに依存します。Select related を使うと、依存するアイテムをまとめて選べます。別のパイプラインにまたがる接続も、同じステージ位置にあれば自動で結び付きます (autobinding)。位置とは、ステージの名前ではなく、先頭から数えた番号です。両方のパイプラインのステージ数が、同じである必要があります。

Direct Lake のセマンティック モデルは、自動では結び付きません。Lakehouse とモデルを両方展開しても、ターゲットのモデルは、元のステージの Lakehouse を向いたままです。データソースルールで、向き先を直します。ステージごとに接続先が違うときは、デプロイルールを使います。[^c1-24]

ルール	対象
Data source rule	Dataflow gen1、セマンティック モデル、ページ分割されたレポート、ミラーリング データベース
Parameter rule	Dataflow gen1、セマンティック モデル
Default lakehouse rule	ノートブック

ルールは、変更先 (ターゲット) のステージで、そのアイテムの所有者が作ります。たとえば本番の DB を指す設定は、Production ステージのモデルに作り、Test から展開して初めて効きます。Development ステージには、ルールを作れません。

データソースルールは、同じ種類のデータソースにしか変えられません。同じデータソースを、複数のルールに使うこともできません。ルールを作れるデータソースは、次の表のとおりです。これ以外のデータソースでは、パラメーターで接続先を切り替えます。ただし、Direct Lake のセマンティックモデルが向く Lakehouse は、展開しても次のステージの Lakehouse へ自動では付け替わりません。Data source rule で、次のステージの Lakehouse に付け替えます。

ルールを作れるデータソース

Azure Analysis Services / Azure Synapse / SQL Server Analysis Services / Azure SQL Server / SQL Server / OData フィード / Oracle / SAP HANA (Import モードだけ) / SharePoint / Teradata

ルールが指すデータソースやパラメーターが、ソース側で変わったり消えたりすると、ルールは無効になって展開が通りません。ワークスペースを割り当て直すと、そのルールと展開の履歴は失われます。ステージの比較に、展開は必要ありません。ルールを作った後に比較すると、まだ展開していなくても、ルールを反映した差が出ます。ページ分割されたレポートに Data source rule を使うと、展開後は Power BI Report Builder で開けません。パラメータールールでアイテムを結び付け直す (rebind) ときは、そのパラメーターが Text 型である必要があります。

場面で確かめます。Test から Production へセマンティックモデルを展開したところ、モデルが Test のデータベースを向いたままでした。ルールは、変更先の Production のステージで作ります。モデルの所有者が Data source rule か Parameter rule を作り、もう一度 Test から展開します。展開するまでは、ルールは効きません。

権限は、パイプラインとワークスペースで別に管理します。パイプラインの権限は Admin だけで、共有、編集、削除に要ります。展開するには、パイプラインの

Admin であり、かつ関係するステージのワークスペースで Contributor 以上であることが要ります。Microsoft 365 グループは、パイプラインの Admin にできません。

ワークスペースを割り当てる条件は、次のとおりです。

1. そのワークスペースの Admin であること。
2. 他のパイプラインに割り当て済みでないこと。
3. Fabric の容量上にあること。
4. 隣のステージのワークスペースで、Contributor 以上であること。
5. Power BI のサンプルを含まず、割り当て先のステージが空であること。

増分更新は、Desktop で設定して発行すると、ポリシーが展開時にコピーされます。増分更新のモデルを、増分更新のないモデルで置き換える再発行は、通りません。増分更新のテーブル名や、計算列でない列の名前を変える再発行も、データを失うおそれがあるため通りません。

デプロイ パイプラインが対応するアイテムの一部は、プレビューです。新しい画面と、展開の順序や動作を決めるデプロイ プランも、プレビューの機能です。2026 年 2 月 12 日から、拡張メタデータに上げていないセマンティック モデルは、対象外になりました。

典型的な構成は、Git とデプロイ パイプラインの組み合わせです。[^c1-35] ワークスペースは 1 つのブランチにしか結び付かないので、複数のブランチを同時には扱えません。開発者は専用のワークスペースを自分のブランチに結び付けて作業し、プル リクエストで Development 側のブランチへ統合します。リリースは、デプロイ パイプラインでステージを進めます。展開は、Power BI または Fabric の REST API でも自動化できます。

系列ビューと影響分析 [1.2]

系列ビュー (lineage view) は、ワークスペース内の全アイテムの関係を表示します。ワークスペース外の上流は、1 段より先は見えません。全ワークスペースに、自動で備わります。[^c1-27]

ワークスペースにロールがあれば、誰でも開けます。ただし Viewer には、データソースが表示されません。別のワークスペースにある下流のアイテムは出ません。その調査には、影響分析 (impact analysis) を使います。データソースのカードには、識別に役立つ情報が出ます。Azure SQL サーバーなら、データベース名も出ます。セマンティック モデルとデータフローの系列が正しく出るのは、Get Data の画面と Dataflows コネクタで接続したときです。手書きの Mashup クエリでつないだ場合は、正しい表示が保証されません。

影響分析は、変更が影響するワークスペースとアイテムを示します。直接の子 (Child items) か、全下流 (All downstream items) かを切り替えられます。データソースでは、直接の子より先は出ません。実行するには、そのアイテムへの書き込み権限が要ります。

Notify contacts に変更内容を書いて送ると、影響を受ける全ワークスペースの連絡先リストにメールが届きます。送信者の名前が表示され、返信もできます。[^c1-28] 権限のない項目は、Limited access と表示されます。名前は見えません。それでも、集計と通知には含まれます。

セマンティック モデルの影響分析には、利用状況も出ます。[^c1-29] 影響を受けるワークスペース、レポート、ダッシュボードの数に加えて、閲覧者数 (Viewers) と閲覧数 (Views) です。どちらも過去 30 日間 (当日を除く) の値で、個人用ワークスペースは対象外です。

classic ワークスペースのモデルでは、Notify contacts が使えません。系列ビューに出る別ワークスペースの外部モデルには、影響分析を実行できません。

元のワークスペースへ移って実行します。Desktop から再発行すると、影響を受けるワークスペースとレポートの数が出て、置き換えの確認を求められます。この数は、影響の可能性を示すだけで、実際に壊れるとは限りません。

場面で確かめます。共有セマンティック モデルの列名を変えようとしています。まず、系列ビューでモデルの下流を見ます。別のワークスペースのレポートは、系列ビューには出ません。影響分析を開きます。All downstream items で全体を数え、Notify contacts で連絡先に知らせます。

XMLA エンドポイント [1.2]

XMLA エンドポイントは、Premium、PPU、Embedded のワークスペースへ、Analysis Services と同じプロトコルで接続する入口です。[^c1-30] 既定のモードは公式の文書の間で書き方が分かれ、XMLA エンドポイントの説明では読み取り専用 (read-only)、Fabric の公式ブログでは 2025 年 6 月 9 日から読み書き (read-write) です (今のモードは、容量の設定の XMLA Endpoint で確かめます)。Read Only の容量では、書き込みができません。書き込むには、容量の設定で XMLA Endpoint を Read Write にします。

管理ポータルテナント設定 Allow XMLA endpoints and Analyze in Excel with on-premises semantic models が無効だと、接続できません。この設定は Integration にあり、既定では有効です。

道具	必要な XMLA のモード
Excel、Power BI Report Builder、DAX Studio、SSMS でのクエリ	read-only
SSMS でのメタデータの TMSL スクリプト、Tabular Editor や ALM Toolkit の変更	read-write

道具	必要な XMLA のモード
Analysis Services Deployment Wizard、PowerShell (SqlServer モジュール) での管理	read-write

クライアントのツールは、XMLA と直接は通信しません。Analysis Services 共通のクライアント ライブラリ (MSOLAP、ADOMD) を介して接続します。

ワークスペース接続 URL は、`powerbi://api.powerbi.com/v1.0/[テナント名]/[ワークスペース名]` の形です。名前の空白は、そのままでは書けません。パーセント エンコードして、Sales Workspace は `Sales%20Workspace` にします。ワークスペース設定の Premium にある Workspace Connection からコピーすれば、綴りを間違えません。SSMS の接続の画面では、サーバーの種類に Analysis Services を選び、サーバー名にコピーした URL を入れて、Active Directory - Universal with MFA の認証で接続します。

権限は、Analysis Services の役割に対応します。ワークスペースの Contributor 以上が持つ Write 権限は、データベース管理者に相当し、モデルのデプロイと TMSL の実行ができます。サーバー管理者の権限が要る操作は、サポートされません。Build 権限は、データベース リーダーに相当し、RLS が適用されます。読み取りだけの接続でも、Build は必要です。

データソースの資格情報は、XMLA では設定できません。サービスのセマンティック モデルの設定ページで設定します。Visual Studio からのデプロイ直後は、メタデータが入っても、データの処理が資格情報不足で止まります。

XMLA 経由の更新には、サービスの 1 日 48 回の上限がありません。スケジュール更新のタイムアウトも、かかりません。増分更新の履歴のパーティションだけを更新するような、細かい処理ができます。大きなモデルへの書き込みは、大規模ストレージ形式を有効にすると、オーバーヘッドが減ります。

Desktop で作ってサービスに発行したモデルに、XMLA で書き込むと、PBIX として再ダウンロードできません。元の PBIX は、手元に保管します。書き込みには、拡張メタデータが要ります。

XMLA から見えないものがあります。Analysis Services へのライブ接続のモデル、別ワークスペースのモデルへのライブ接続、REST API のプッシュデータセット、Excel ブックのモデルです。サービス プリンシパルは、RLS と OLS のロールのメンバーにできません。

症状	原因
SSMS で TMSL を実行するとエラーになる	容量の XMLA Endpoint が Read Only に設定されている
どの XMLA 接続も通らない	テナント設定 Allow XMLA endpoints and Analyze in Excel with on-premises semantic models が無効
Viewer がクエリできない	モデルの Build 権限がない
デプロイは通ったが、データが空	データソースの資格情報が未設定で、処理が止まった
発行したモデルを PBIX でダウンロードできない	Desktop で作ったモデルに XMLA で書き込んだ

複数の利用者が使うアプリでは、PPU のワークスペースなら利用者ごとにサインインさせる必要があり、サービス アカウントやアプリ ID で代わりに接続することはできません。Premium の容量では、サービス アカウントやアプリ ID を使えます。接続文字列の EffectiveUserName で別のユーザーとして試すこともできます。その場合、指定した Entra のアカウントが、モデルの Read と Build の両方を持っている必要があります。

再利用できる資産 (.pbbit、.pbids、共有セマンティック モデル) [1.2]

3 つの資産は、運ぶ物が同じではありません。

資産	入っている物	入っていない物
.pbbit (テンプレート)	レポートのページとビジュアル、モデル定義 (スキーマ、リレーション、メジャー)、クエリ定義	データ
.pbids (データ ソース)	1 つのデータ ソースへの接続情報	認証情報、テーブルやスキーマの情報
共有セマンティック モデル	標準化したモデルそのもの (レポートは別ワークスペースからライブ接続)	レポートの定義

.pbbit は、File > Export > Power BI template で作ります。書き出すときは、テンプレートの説明文を入力します。[^c1-31] 開くと、パラメーターの値の入力、データの場所の指定の順に進みます。データを含みません。そのため、.pbix より小さくなります。ビジュアルのフィルター値 (Company = Contoso など) は、メタデータとして残ることがあります。

.pbids は、File > Options and settings > Data source settings で対象を選び、Export PBIDS で作ります。自動生成が勧められますが、手書きもできます。[^c1-32]

```
{
  "version": "0.1",
  "connections": [
    { "details": { "protocol": "analysis-services", "address": {
      "server": "server-here" } } }
  ]
}
```

ファイルに認証情報は入っていません。開くと、Desktop が認証を求め、Navigator が出ます。1 ファイルに入れられるデータソースは1つで、複数指定するとエラーになります。Wiki URL、Live Connect、Blank Query は対象外です。接続モード (DirectQuery か Import) を書かなくても、エラーにはなりません。その場合は、利用者が選びます。

共有セマンティック モデルは、標準化したモデルを、複数のワークスペースで再利用する形です。[^c1-33] 他のワークスペースの作成者は、ライブ接続のレポートを作ります。ライブ接続のレポートは、モデルのデータを持ちません。作成者のアクセスは Build 権限で制御し、Promote か Certify で見つけやすくします。Desktop からは、Get Data の Analysis Services ではなく、Power BI semantic models から接続するのが勧められます。モデルの推奨の段階が一覧に出るので、ワークスペースの URL を覚える必要がありません。

Build 権限を得る道は、4 つあります。

道	内容
ルール	Contributor 以上は、ワークスペース内のモデルに自動で持つ

道	内容
所有者の付与	所有者が Manage permissions で、ユーザーやセキュリティグループに付ける
アプリの公開	Admin か Member が、アプリの権限を持つ人にも、モデルの Build を付ける
レポートの共有	Reshare と Build を持つ人が、レポートの共有時に Build も付ける

Build を外すと、その人はレポートを編集できず、基礎データもエクスポートできません。レポートは見られます。Read だけの人も、集計済みのデータはエクスポートできます。

他のワークスペースのレポートが使っているモデルは、削除できません。共有モデルのレポートでは、Publish to web が動きません。アプリの利用者にも、モデルへのアクセスが要ります。

ライセンスの面では、Free のユーザーも、Build があればレポートを作れます。ただし、モデルが Premium か Fabric F64 以上の容量にある場合です。保存は My workspace に限られ、共有や別ワークスペースへの保存は、Pro か PPU でないとできません。

目的	使う資産
同じページ構成とモデルで、新しいレポートを始めたい。データは別の環境の物を使う	.pbit
決まったデータソースに、迷わず接続させたい	.pbids
複数のチームが、同じ指標の定義でレポートを作りたい	共有セマンティック モデル (Build で制御し、Certified で目印を付ける)

サンプルはここまでです

続き(第2章～巻末)は、DP-600 問題集のご購入で、頻出度別ノート・暗記用ノートと合わせて3点すべてダウンロードできます。

SAMPLE

DP-600 学習用テキスト(無料サンプル)

版

2026年10月版(DP-600 出題範囲(Skills measured)2026-10-19版 準拠)

発行

IT資格道場(<https://www.shikaku-doujou.com>)

お問い合わせ

info@shikaku-doujou.com

Microsoft、Microsoft Fabric、Power BI および Microsoft の製品名・サービス名は、Microsoft Corporation の米国およびその他の国における商標または登録商標です。記載されているその他の会社名・製品名・サービス名は、各社の商標または登録商標です。

本教材は公式シラバスの内容を基に作成したもので、Microsoft Corporation との提携・承認関係はありません。

本文・図表・設問はすべてオリジナルの著作物です。無断での転載・複製・再配布・二次販売はできません。お気づきの点は info@shikaku-doujou.com までご連絡ください。