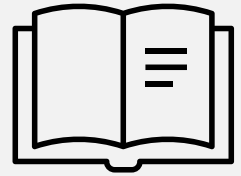
SC-5008

補足資料

エンタイトルメント管理



アクセス権管理の 理想 と 現実

	理想	現実
適切な ユーザーに	必要なユーザーにだけ 付与する	**必要となりそうな** ユーザーに付与する
適切な アクセス権を	必要最小限の権限を 付与する	**必要となりそうな** 権限を付与する
適切な 期間のみ	必要なくなったらすぐに はく奪する	**消すのがこわいから** とりあえず残しておく

アクセス権管理の 理想 と 現実

	理想	現実
適切な ユーザーに	必要のないユーザーにアクセス権が付与されている	
適切な アクセス権を	必要以上のアクセス権が付与されている	
適切な 期間のみ	必要としなくなってもアクセスができている	

Identity Governance とは

- **ID ガバナンスを簡単に表現すると、以下を実現する事**

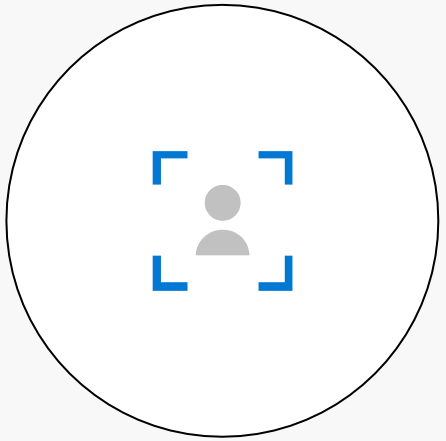
  適切なユーザーに**適切なアクセス権**を**適切な期間**付与する

- **この 1 文を実現するには以下のような運用が必要で非常に大変**
  - 人事イベントにあわせた ID ライフサイクル の実現
  - アクセス権(役割やグループ など)の管理
  - タイムリーなアクセス権の付与と剥奪
  - 重要なアクセス権(特権)に対する保護
  - アクセス権の棚卸
  - アクセス権の利用の監視と監査

- **Microsoft の Identity Governance は生産性を落とさずにこれらを助ける事を目的とする**

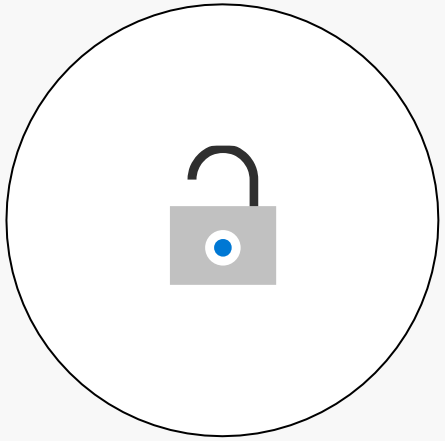
Microsoft Identity Governance とは

「適切なユーザーに」「適切なアクセス権を」「適切な期間のみ」を実現する



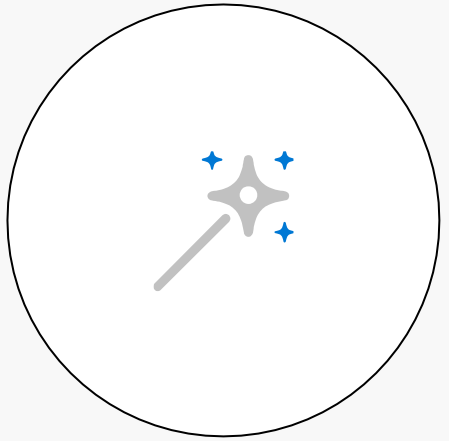
ID ライフサイクル

- Entra Connect
- Cloud Sync



アクセス ライフサイクル

- エンタイトルメント管理
- アクセス レビュー



特権アクセス

- Privilege Identity Management

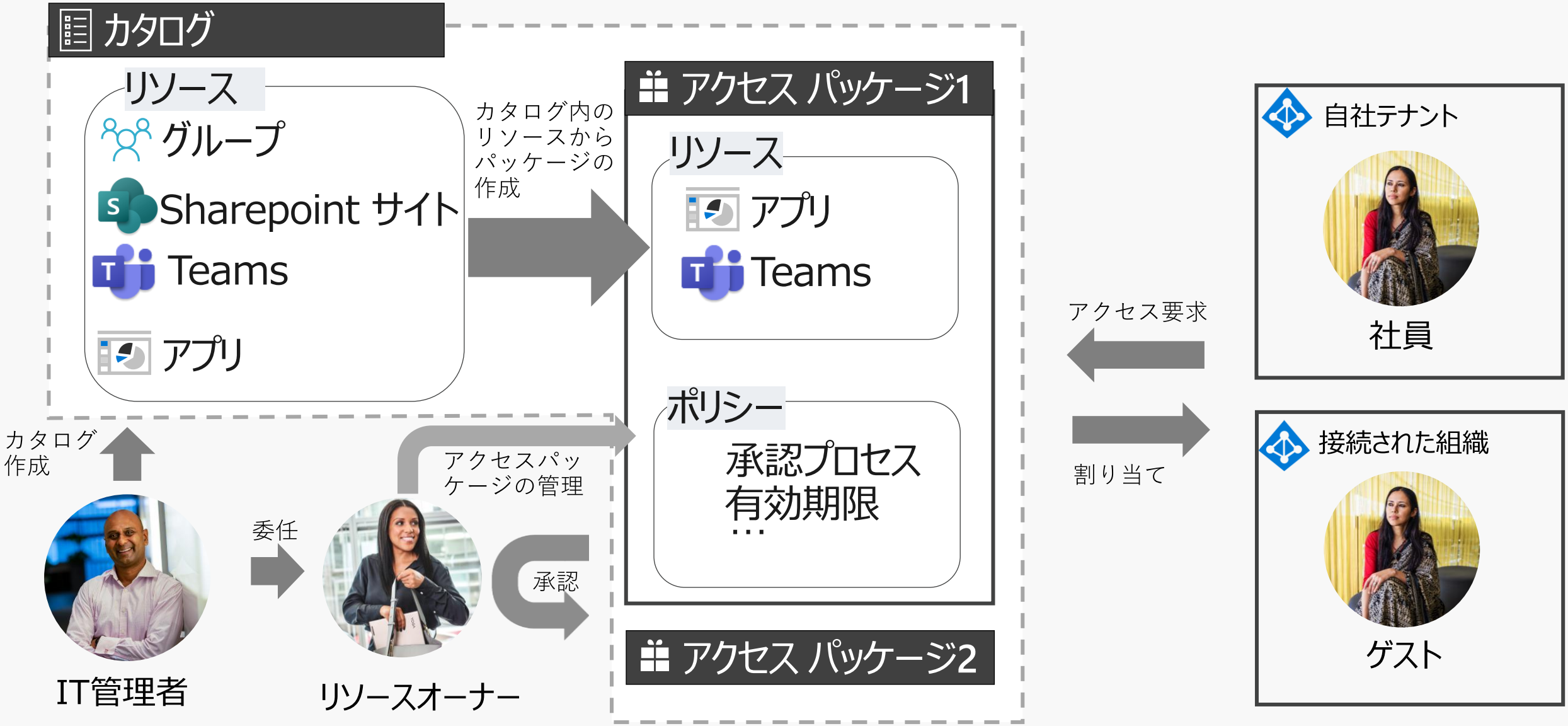
エンタイトルメント管理とは

- **エンタイトルメント(entitlement) = 資格 / 権利の付与する事**
- **アクセス権をユーザーの要求をベースに管理するための機能**
- **エンタイトルメント管理は以下のような機能を元にアクセス権管理を効率化する**
  - アクセス要求のワークフロー化
  - 管理の委任
  - アクセス権のレビュー
  - 失効処理
- **管理できるリソース**
  - グループ / Team
  - SharePoint サイト
  - アプリケーション

エンタイトルメント管理で出てくる重要な用語

用語	説明
アクセス パッケージ	**チームまたはプロジェクトが必要とし、ポリシーに準拠しているリソースをまとめた物。** アクセス パッケージは常にカタログに含まれているリソースから選択され作成されます。
アクセス要求(リクエスト)	**アクセス パッケージのリソースへのアクセス要求。** 要求は通常、承認ワークフローを通じて処理されます。 承認されると、要求元のユーザーにアクセス パッケージが割り当てられます。
割り当て	**アクセス パッケージ内のリソースへのアクセス権をユーザーに付与する事。** 通常、アクセス パッケージの割り当てには有効期限があり、期限が切れると失効します。
カタログ	**関連リソースとアクセス パッケージをまとめた物。** カタログは主に管理の委任に使用されます。これにより、管理者以外のユーザーが独自のアクセス パッケージを作成できるようにすることができます。 カタログ所有者は、自分が所有するリソースをカタログに追加できます。
接続されている組織	**自組織が関係を持っている、外部の Entra ID ディレクトリ/テナント。** 接続された組織のユーザーは、アクセス権の要求を許可されたユーザーとして、ポリシーで指定できます。
ポリシー	**アクセス権のライフサイクルを定義する一連のルール (どのようなユーザーが要求できるか、誰が承認を実行できるか、割り当てによって付与されたアクセス権がいつ失効するかなど)。** ポリシーはアクセス パッケージにリンクされます。 たとえば、アクセス パッケージに 2 つのポリシーを含めて、1 つは従業員によるアクセス要求、もう 1 つは外部ユーザーによるアクセス要求に使用することもできます。
リソース	**Office グループ、セキュリティ グループ、アプリケーション、SharePoint Online サイトなどのアセット/資産。**アクセス許可は、ロールによってユーザーに付与します。
リソース ロール	**リソースに関連付けられ、リソースによって定義されている一連のアクセス許可の種類。** 主に、リソースに対して、どのような立場でアクセスするかを定義します。グループには 2 つのロールがあります (メンバーと所有者)。 SharePoint サイトには通常 3 つのロールがありますが、追加のカスタム ロールを使用することもできます。 アプリケーションにはカスタム ロールを設定できます。

エンタイトルメント管理の仕組みの理解



アクセス レビューの仕組み （概要）

- アクセス権のはく奪をプロセス化

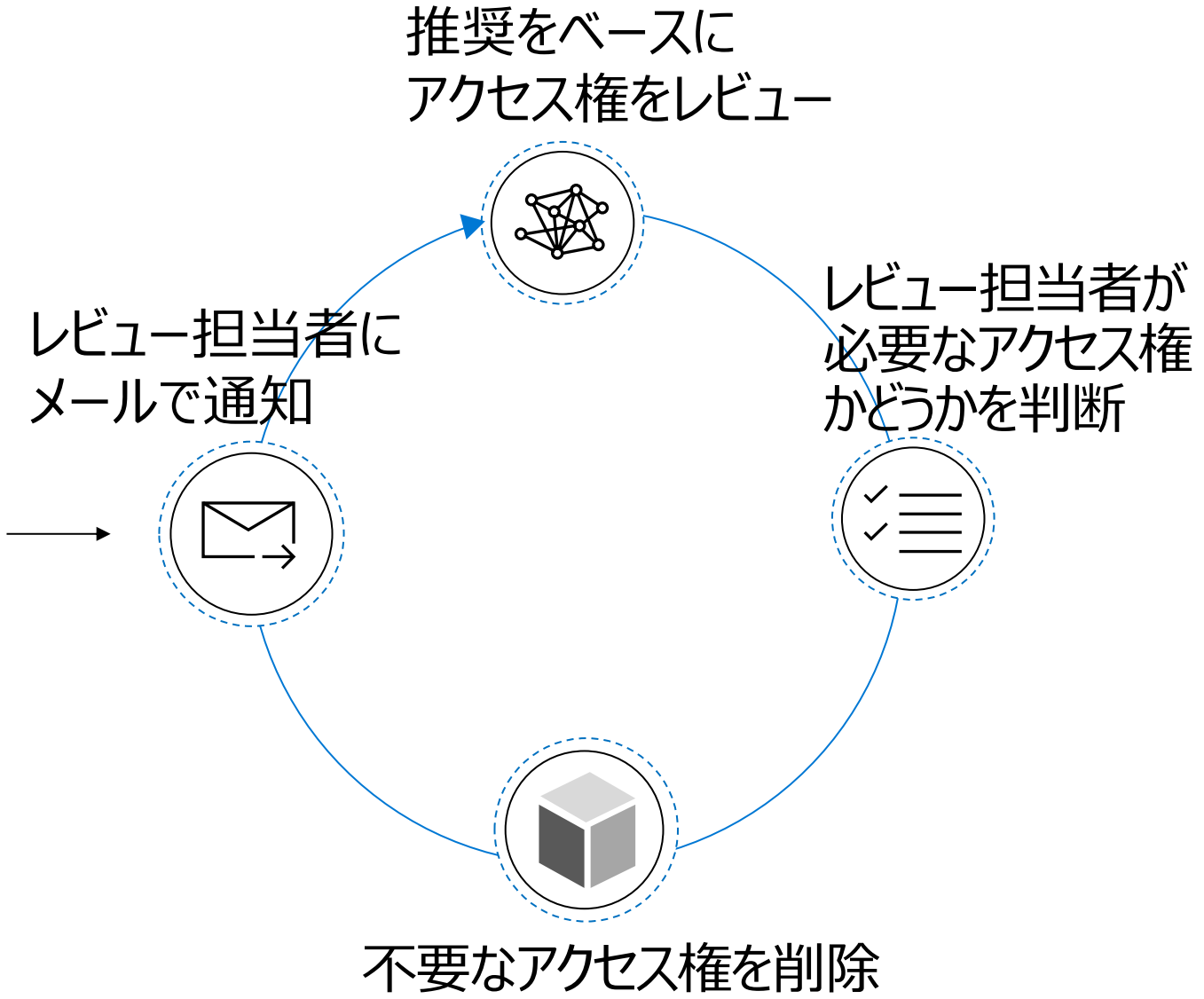
IT 管理者がアクセスレビューを作成

1. レビュー対象を指定
   グループ
   アプリ

2. スコープを指定
   全員
   ゲストのみ

3. レビュー担当者を指定

4. 周期を指定
   Weekly
   Monthly
   Quarterly
   Yearly

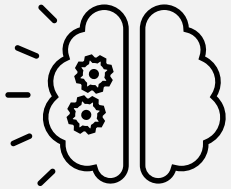


まとめ：アクセス権管理の 理想 と 現実 GAP を無くす

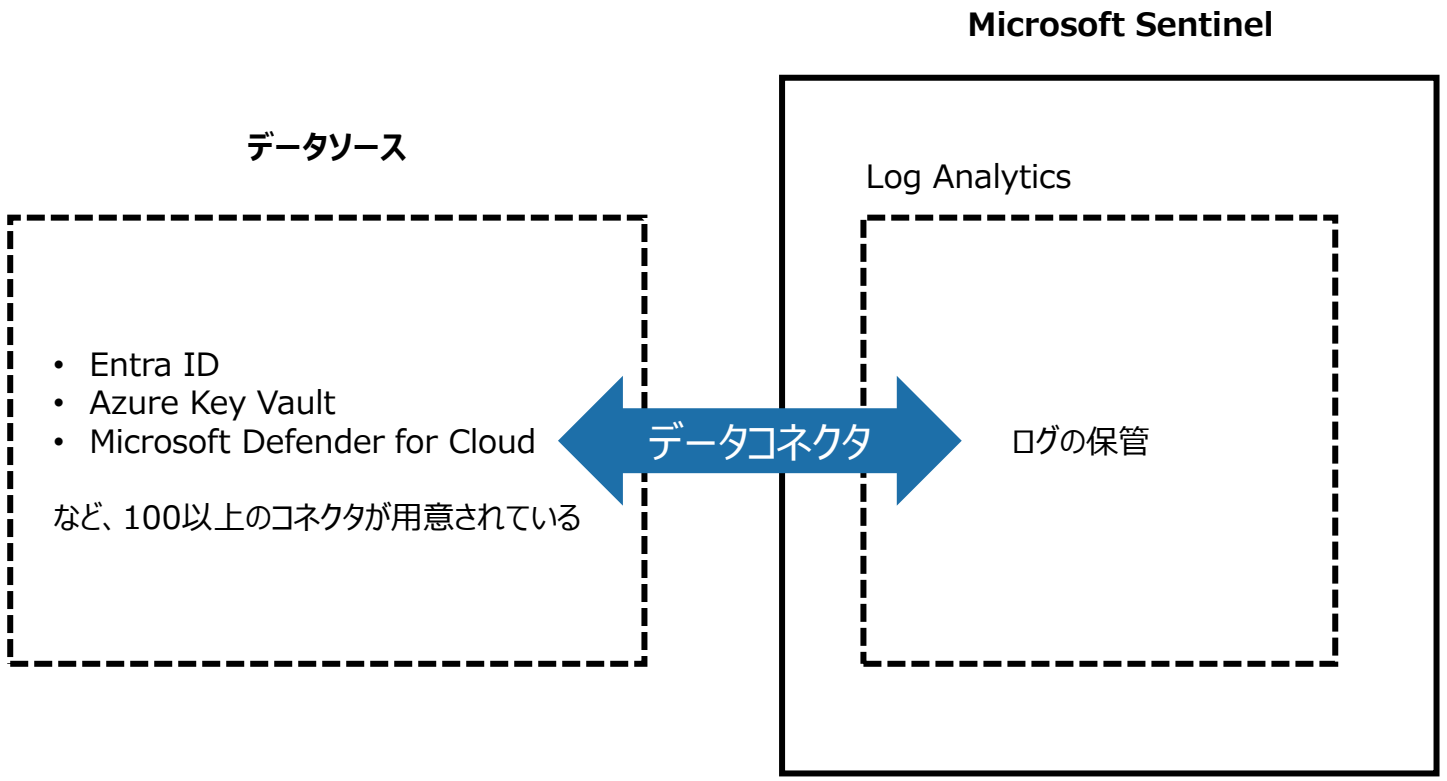
「適切なユーザーに」「適切なアクセス権を」「適切な期間のみ」を実現する

	理想	現実
適切な ユーザーに	【エンタイトルメント管理】 ユーザー自身が必要な時にリクエストする運用をプロセス化。	
適切な アクセス権を	【エンタイトルメント管理】 アクセス パッケージに必要なリソースだけを含める 各リソースの適切なアクセス権 (ロール) の付与をプロセス化	
適切な 期間のみ	【エンタイトルメント管理】 有効期限ではく奪を自動化	【アクセス レビュー】 定期的なレビューをプロセス化

Entra ID 診断ログを有効にし、Log Analytics/Microsoft Sentinel と統合する



Microsoft Sentinel の整理



- **データ収集**
  - メニューとしてはデータコネクタ
  - Entra IDやアクティビティログなどAzureだけではなく、イベントログなどOSのログからPalo等のNW機器など様々なデータソースからLog Analyticsにデータ収集する
- **検知**
  - メニューとしては分析
  - 収集データに対してクエリ(デフォルトで準備されているのもあります。)を実行し合致するイベントがあった時にアラートを作成する
- **調査**
  - メニューとしてはインシデント
  - 影響範囲を特定する
- **対処**
  - メニューとしてはオートメーション(プレイブック)
  - Logic Appで構成され検知したアラートに対しての処理を行う