DISCOVERIES INC.

IntelliReport

Microsoft 365(Office 365)監査ログ連携機能

アクティブ化手順書

第八版　2022 年 11 月 25 日

目次

1　はじめに

1.1　本書の目的

本書は、Microsoft 365(Office 365)監査ログをご利用中のお客様について、Office 365 監査ログを弊社インテリレポートと連携し、監査ログ機能をアクティブ化することを目的とします。
そのために必要となる、お客様の Office 365 環境情報*をディスカバリーズ サポートデスクまでご送付頂く手順について説明します。
※インテリレポートの監査ログ連携には、「ディレクトリ ID」「アプリケーション ID」「テナント名」「キーの値」「キーの有効期限」が必要です。

※Office 365 および Microsoft Azure における操作に関する不具合やご不明点等をお問い合わせの場合は、日本マイクロソフト株式会社へご連絡ください。

1.2　作業対象者

Azure Active directory および、SharePoint Online サイトの管理権限、Office 365 のグローバル管理権限を持っている IT 管理者を対象とします。

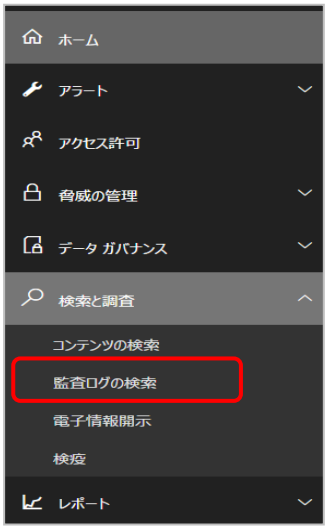
2　作業手順

2.1　Office 365 監査機能のアクティブ化

お客様環境の Office 365 セキュリティセンターにおいて、監査機能をアクティブ化します。

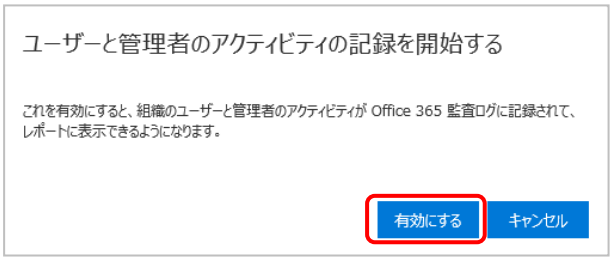
既に Office 365 監査機能がアクティブ化されている場合は、次章に進んでください。

1. https://protection.office.com にアクセスします。
2. Office 365 グローバル管理者を使用し、サインインします。
   ※エラーメッセージが表示される場合、作業アカウントの権限が不足しています。
3. 左側のウィンドウから「検索と調査」をクリックし、「監査ログの検索」をクリックします。
   ※「検索と調査」が表示されない場合、作業アカウントの権限が不足しています。



4. 「監査ログの検索」画面が表示されるので、[ユーザーと管理者のアクティビティの記録を開始する]をクリックします。
※このメッセージが表示されていない場合、組織の監査機能は既に有効になっているため、次章に進んでください。

5. メッセージが表示されるので、「有効にする」をクリックします。



6. メッセージが表示されるので、「はい」をクリックします。

7. Office 365 監査ログの準備メッセージが表示されます。

※インテリレポートご契約期間中は、Office 365 監査機能を停止しないでください。

※Office 365 監査機能を停止しても、インテリレポートの監査ログ機能は停止しません。

監査ログのデータ取得がご不要になった場合は、弊社サポートデスクまでご連絡ください。

2.2　Azure Active Directory アプリ登録

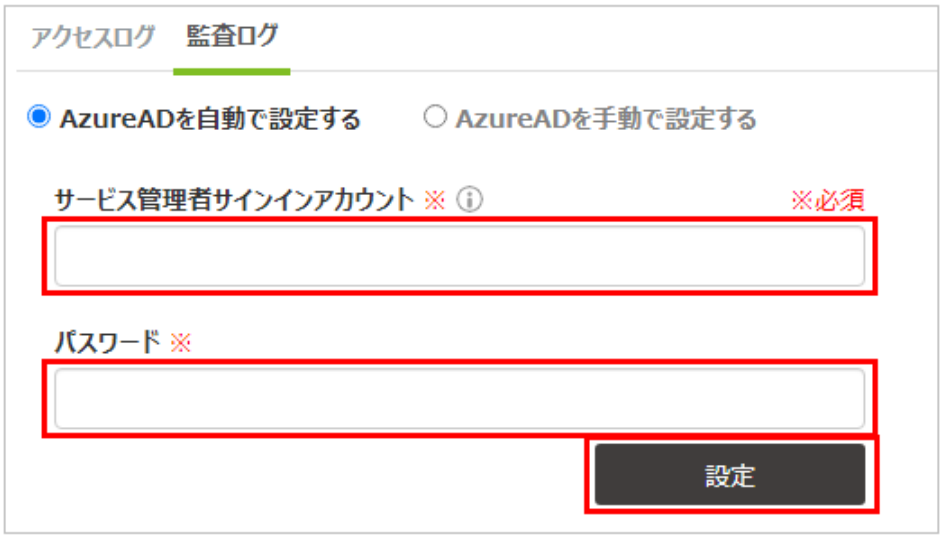
2.2.1　自動設定機能でアプリ登録を行う

本作業はインテリレポートの全体管理者のアカウントを使用して実施します。

1. インテリレポート 管理サイト<https://intelli.report/>にアクセスして、全体管理者アカウントでサインインします。

2. 歯車アイコンの「設定」メニューから、「アクセストークン設定」の「監査ログ」タブを開きます。

3. 「サービス管理者サインインアカウント」「パスワード」にそれぞれグローバル管理者アカウント情報を入力し、「設定」ボタンをクリックします。

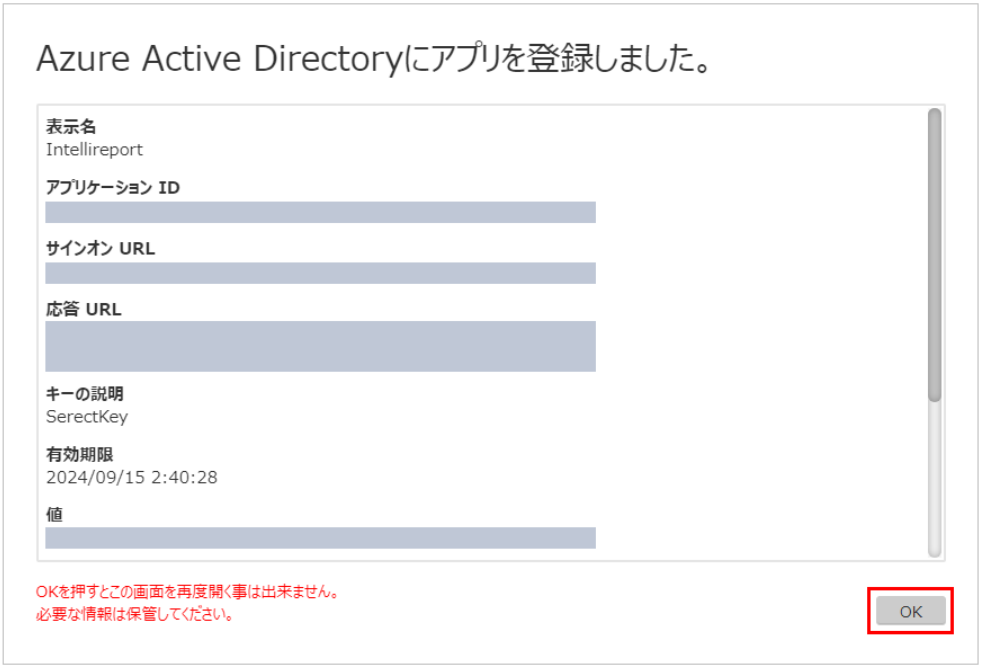


※ Microsoft 365 の多要素認証（MFA）を利用するアカウントでは設定を行うことができません。多要素認証を設定していないアカウントをお使いください。

4. Azure Active Directory アプリの自動登録が成功すると、設定された情報の詳細が表示されますので、内容を確認後に「OK」をクリックして画面を閉じます。

※ 本画面は一度しか表示されないため、必要な情報はコピーして保管してください。

- アプリケーション ID：設定後、アクセストークン設定画面のアプリケーション ID で確認できます。
- サインオン URL：IntelliReport ログイン画面の URL です。
- 応答 URL：SharePoint 管理センターおよび IntelliReport ログイン画面の URL です。
- 値：設定後、アクセストークン設定画面のアプリケーション Key で確認できます。



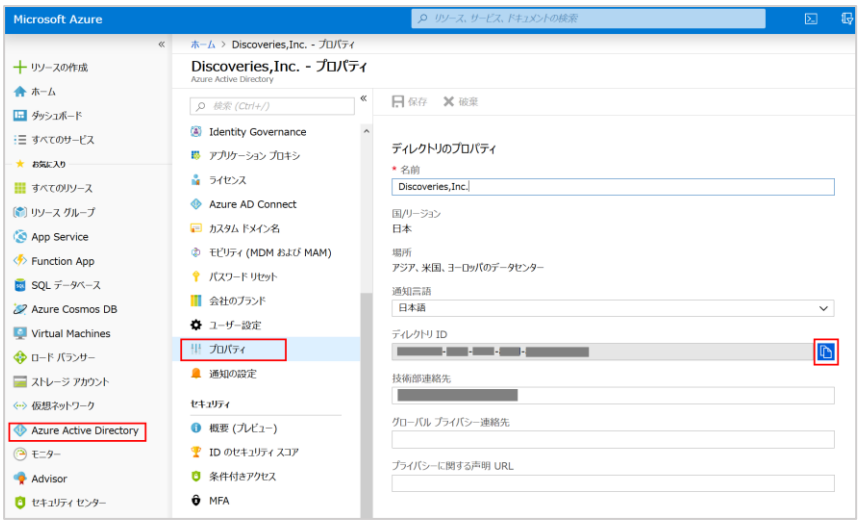
2.2.2　手動でアプリ登録を行う

グローバル管理者の管理者ロールを利用出来ないなどの理由で、自動設定が行えない場合にはこちらの手順を実施し、手動で登録を行ってください。
お客様環境の Microsoft Azure において、インテリレポート認証用のアプリケーションを追加します。
ここでは、「現在のディレクトリ」「ディレクトリ ID」「アプリケーション ID」を取得します。(取得データ①②③)

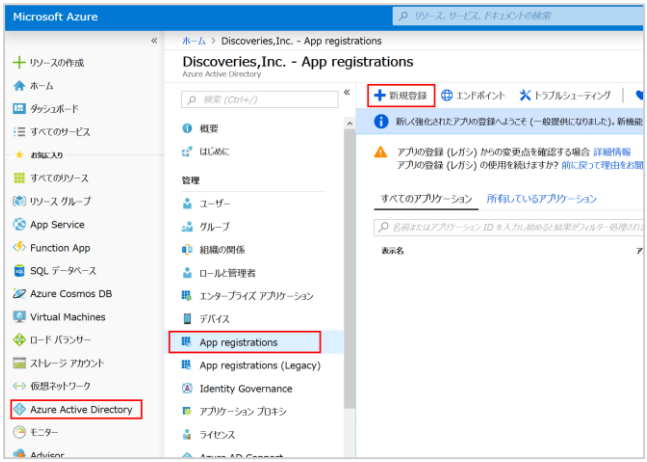
1. Azure ポータルサイトに、Azure 管理者アカウント(Office 365 の管理者アカウント)を使用し、サインインします。
   お客様の既存サブスクリプションをご利用ください。
   https://portal.azure.com/

2. 「Azure Active Directory」-「プロパティ」を開きます。

3. 「ディレクトリ ID」欄の「クリップボードにコピー」をクリックし、テキストなどに保存します。
   ※このディレクトリ ID は、以降の手順で使用します。(取得データ①)



4. 「Azure Active Directory」-「App registrations」(アプリの登録)を開き、「新規登録」をクリックします。



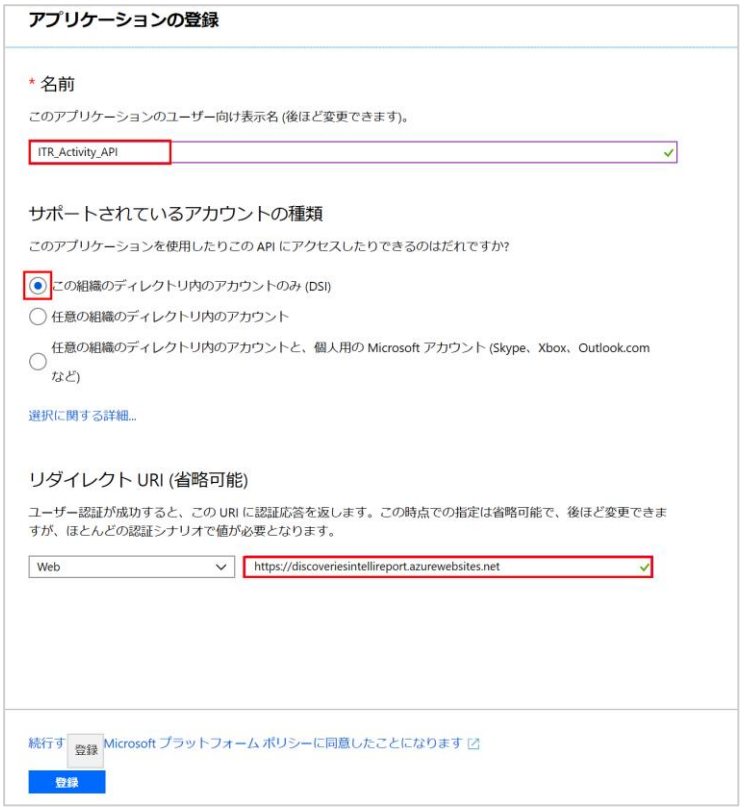
5. 必要な情報を入力し、「登録」をクリックします。

<入力例>

名前：ITR_Activity_API

種類：この組織のディレクトリ内のアカウントのみ

リダイレクト URL：“Web” https://discoveriesintellireport.azurewebsites.net

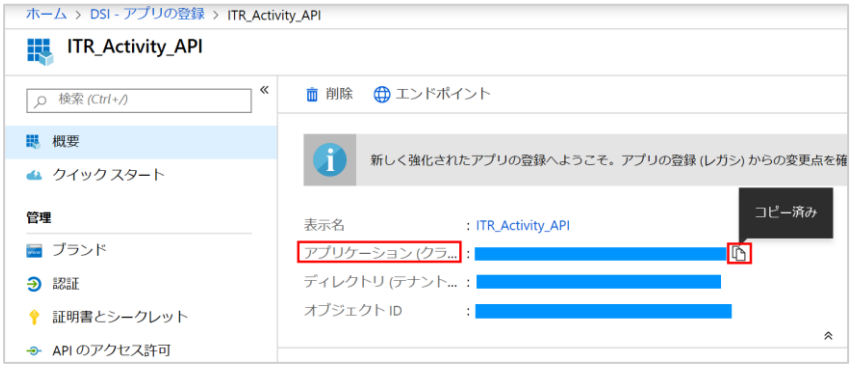


6. 成功メッセージが表示されることを確認します。

7. 作成したアプリケーションの詳細画面が開きます。

8. アプリケーション(クライアント)ID 欄の「クリップボードにコピー」アイコンをクリックし、テキストなどに保存します。

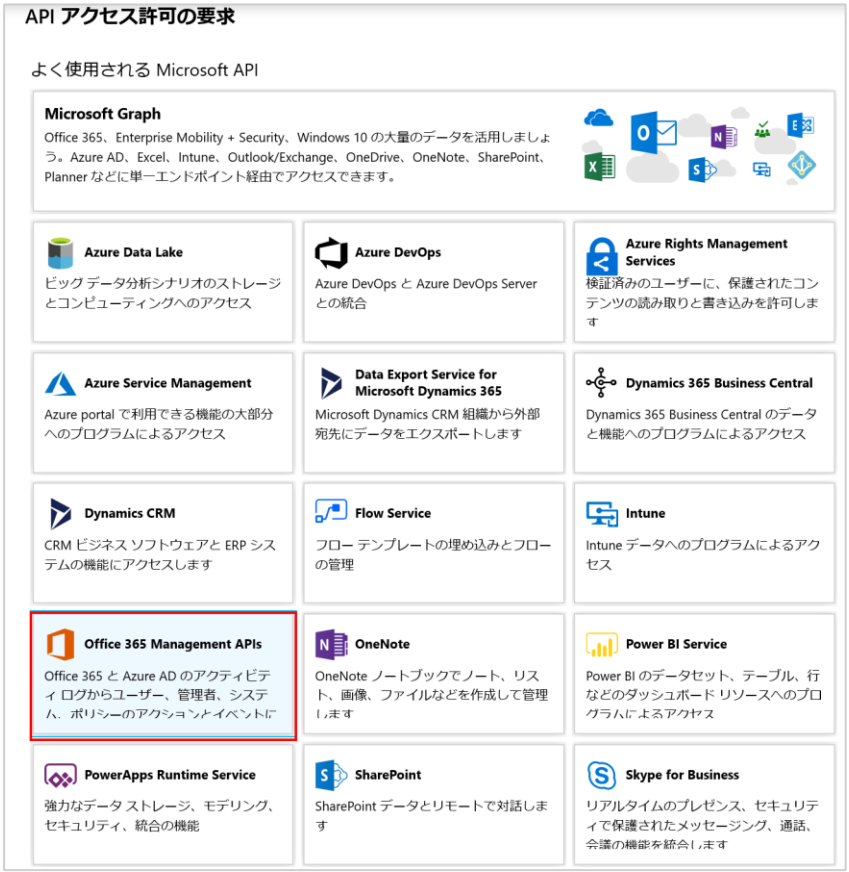
※このアプリケーション ID は、以降の手順で使用します。(取得データ②)



9. 次に作成したアプリに対して、アクセス許可を設定します。
このアクセス許可設定が不十分な場合、アプリケーションが正しく動作しません。

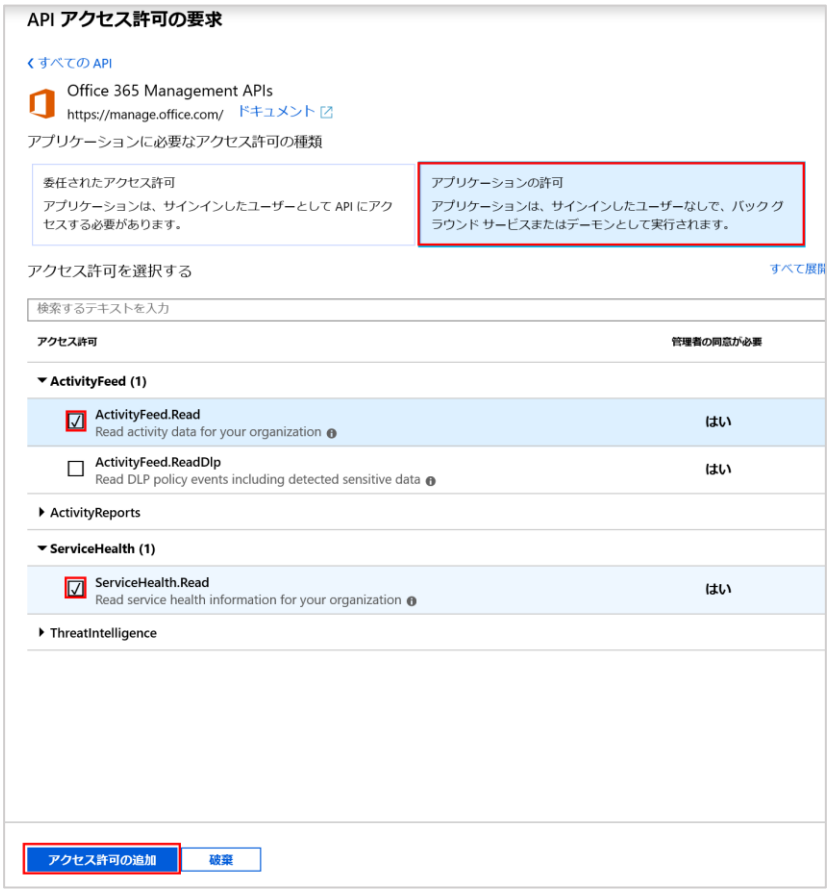
① アプリケーション詳細画面の「API のアクセス許可」を開き、「アクセス許可の追加」をクリックします。

② 「よく利用される Microsoft API」-「Office 365 Management APIs」をクリックします。



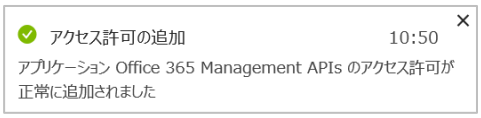
③　右側の「アプリケーションの許可」をクリックすると項目一覧が表示されるので、以下の 2 項目を探し、チェックを入れます。

大項目	項目名	説明
ActivityFeed	ActivityFeed.Read	Read service health information for your organization
ServiceHealth	ServiceHealth.Read	Read activity data for your organization



④　すべてチェックを入れたことを確認し、「アクセス許可の追加」をクリックします。

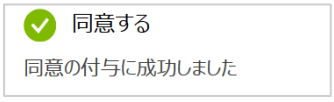
⑤　成功メッセージが表示されることを確認します。



⑥　アクセス許可について「管理者の同意が必要」にメッセージが表示されていますので、
画面下の「○○○(お客様テナント名)に管理者の許可を与えます」をクリックします。

⑦　画面上部に確認メッセージが表示されるので、「はい」をクリックします。

⑧　成功メッセージが表示されることを確認します。



10. シークレットキーの登録

作成したアプリにクライアントシークレットキーを登録します。

ここでは「キーの値」と「有効期限」を取得します。(取得データ③④)

① アプリケーション詳細画面のメニューから「証明書とシークレット」を開き、「+新しいクライアントシークレット」をクリックします。

② 必要な情報を入力し、「追加」をクリックします。

<入力例>

説明：AppKey

有効期限：なし※

※貴社セキュリティルールに沿う場合は、「期限なし」での作成を推奨しております。

※キーの有効期限を過ぎると、監査ログのデータ取得が停止します。

※「1 年」もしくは「2 年」に設定した場合は、期限切れになる前にキーを再作成し、新しいキーの「値」を弊社サポートデスクまでご連絡ください。

③　成功メッセージが表示されることを確認します。

④　作成したクライアントシークレットキーから、値の「クリップボードにコピー」をクリックし、テキストなどに保存します。(取得データ③)

※画面遷移してしまうと、この値は非表示になるため、忘れずにコピーしてください。

※この値は、以降の手順で使用します。

⑤　あわせて、キーの有効期限をテキストなどに保存します。(取得データ④)

11. インテリレポート 管理サイト<https://intelli.report/>にアクセスして、全体管理者アカウントでサインインします。

12. 歯車アイコンの「設定」メニューから、「アクセストークン設定」の「監査ログ」タブを開きます。

13. 「AzureAD を手動で設定する」を選択し、各項目にそれぞれ取得した値を入力して「設定」ボタンをクリックします。

- ディレクトリ(テナント)ID：取得データ①
- アプリケーション(クライアント)ID：取得データ②
- アプリケーション Key；取得データ③
- 有効期限：取得データ④ ※任意

  ※有効期限を登録すると、期限日の 30 日前と 10 日前に全体管理者宛にメール通知が送信されます。
  また期限日 30 日前からダッシュボード上に有効期限が切れる旨のメッセージが表示されるようになります。

14. 「設定が完了しました。」と画面に表示されたら準備は完了です。

補足

本マニュアルは 2022 年 11 月 25 日時点のものとなります。バージョンアップや機能強化などにより、実際にご利用の製品では内容が異なる場合がありますのでご注意ください。

以上