



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
1.1 本書の目的	1
1.2 作業対象者	1
2 作業手順	2
2.1 Office 365 監査機能のアクティブ化	2
2.2 Azure Active Directory アプリ登録	5
2.2.1 自動設定機能でアプリ登録を行う	5
2.2.2 手動でアプリ登録を行う	7
補足	15

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。

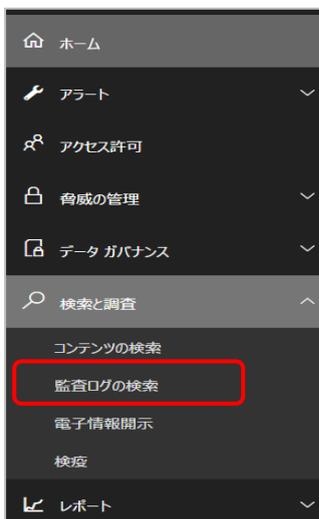
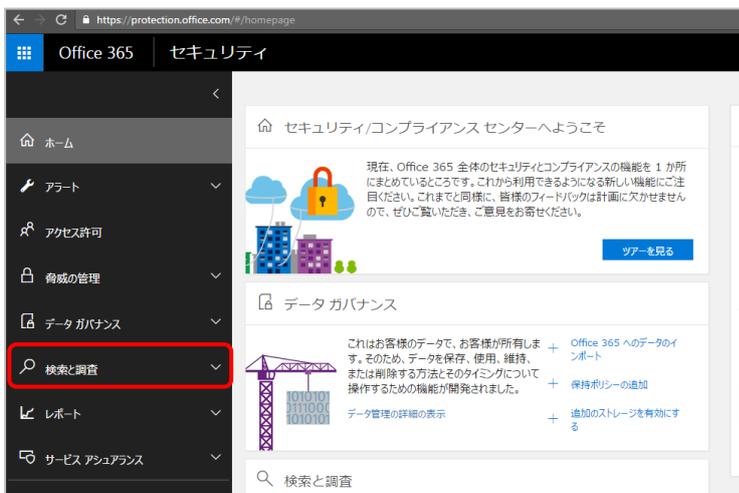
2 作業手順

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。

ホーム > 監査ログの検索

監査ログの検索

ユーザーがドキュメントを削除したかどうかや、管理
たかを確認できます。メール、グループ、ドキュメン

Office 365 監査ログを準備しています。数時間
以内にユーザーと管理者のアクティビティの検索がで
きるようになります。

検索

アクティビティ

すべてのアクティビティの結果を表示 ▾

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。

設定

アクセストークン設定

レポート管理設定

監査ログ対象設定

接続ID管理

アクセストークン設定

アクセスログ 監査ログ

AzureADを自動で設定する AzureADを手動で設定する

サービス管理者サインインアカウント ※ ⓘ ※必須

パスワード ※

設定

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。

アクセスログ 監査ログ

AzureADを自動で設定する AzureADを手動で設定する

サービス管理者サインインアカウント ※ ⓘ ※必須

パスワード ※

設定

※ 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。

Azure Active Directoryにアプリを登録しました。

表示名	Intellireport
アプリケーション ID	[Redacted]
サインオン URL	[Redacted]
応答 URL	[Redacted]
キーの説明	SerectKey
有効期限	2024/09/15 2:40:28
値	[Redacted]

OKを押すとこの画面を再度開く事は出来ません。
必要な情報は保管してください。

OK

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。

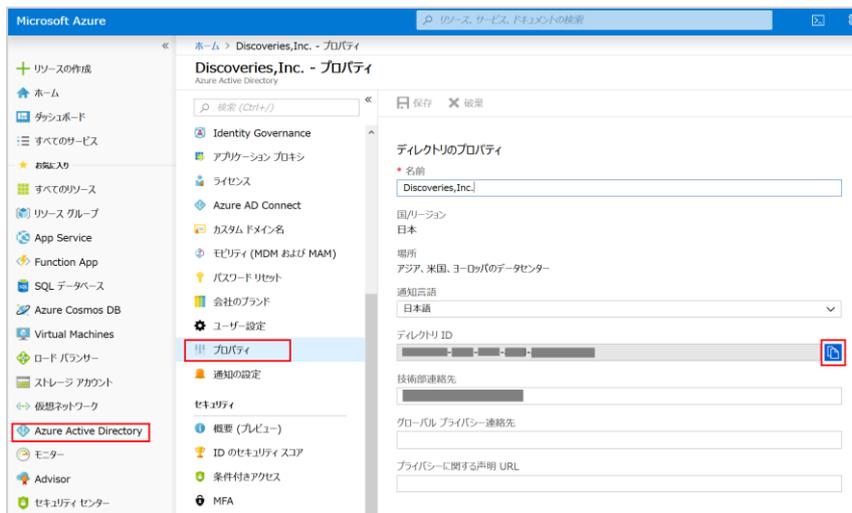
お客様環境の Microsoft Azure において、インテリレポート認証用のアプリケーションを追加します。

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)

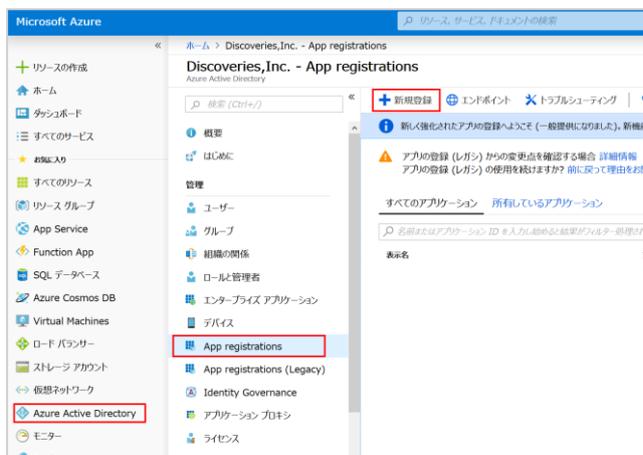
1. Azure ポータルサイトに、Azure 管理者アカウント(Office 365 の管理者アカウント)を使用し、サインインします。
お客様の既存サブスクリプションをご利用ください。

<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

アプリケーションの登録

* 名前
このアプリケーションのユーザー向け表示名 (後ほど変更できます)。
ITR_Activity_API ✓

サポートされているアカウントの種類
このアプリケーションを使用したりこの API にアクセスしたりできるのはどれですか?
 この組織のディレクトリ内のアカウントのみ (DSI)
 任意の組織のディレクトリ内のアカウント
 任意の組織のディレクトリ内のアカウントと、個人用の Microsoft アカウント (Skype、Xbox、Outlook.com など)
[選択に関する詳細...](#)

リダイレクト URI (省略可能)
ユーザー認証が成功すると、この URI に認証応答を返します。この時点での指定は省略可能で、後ほど変更できますが、ほとんどの認証シナリオで値が必要となります。
Web | https://discoveriesintellireport.azurewebsites.net ✓

続行する Microsoft プラットフォーム ポリシーに同意したことになります [?](#)

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

API アクセス許可の要求

<すべての API

Office 365 Management APIs
<https://manage.office.com/> [ドキュメント](#)

アプリケーションに必要なアクセス許可の種類

委任されたアクセス許可 アプリケーションは、サインインしたユーザーとして API にアクセスする必要があります。	アプリケーションの許可 アプリケーションは、サインインしたユーザーなしで、バックグラウンド サービスまたはデーモンとして実行されます。
---	--

アクセス許可を選択する すべて展開

検索するテキストを入力

アクセス許可 管理者の同意が必要

▼ ActivityFeed (1)

<input checked="" type="checkbox"/> ActivityFeed.Read Read activity data for your organization ⓘ	はい
<input type="checkbox"/> ActivityFeed.ReadDlp Read DLP policy events including detected sensitive data ⓘ	はい

▶ ActivityReports

▼ ServiceHealth (1)

<input checked="" type="checkbox"/> ServiceHealth.Read Read service health information for your organization ⓘ	はい
---	----

▶ ThreatIntelligence

アクセス許可の追加 破棄

- 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。

✔ アクセス許可の追加 10:50 ×

アプリケーション Office 365 Management APIs のアクセス許可が正常に追加されました

- 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。

DSI のすべてのアカウントについて、要求されたアクセス許可に対する同意を付与しますか? この操作により、このアプリケーションが既に持っている既存の管理者の同意レコードが、以下の一覧の内容に一致するよう更新されます。

はい いいえ

+ アクセス許可の追加

API / アクセス許可の名前	種類	説明	管理者の同意が必要
▼ Microsoft Graph (1)			
User.Read	委任済み	Sign in and read user profile	-
▼ Office 365 Management APIs (2)			
ActivityFeed.Read	アプリケ...	Read activity data for your organization	はい ⚠ DSI に付与されていません
ServiceHealth.Read	アプリケ...	Read service health information for your organization	はい ⚠ DSI に付与されていません

これらは、このアプリケーションが静的に要求するアクセス許可です。コードを使用して、ユーザーの同意が可能なアクセス許可を動的に要求することもできます。 [アクセス許可を要求するためのベストプラクティスを参照する](#)

同意する

管理者は、このディレクトリのすべてのユーザーに代わり同意を与えることができます。すべてのユーザーに管理者の同意を与えると、エンドユーザーが対象アプリケーションを使用するときに、同意画面が表示されなくなります。

DSI に管理者の同意を与えます

- ⑧ 成功メッセージが表示されることを確認します。

✔️ 同意する
同意の付与に成功しました

✔️ 要求されたアクセス許可の管理者の同意が正常に付与されました。

API のアクセス許可

アプリケーションが API を使用する承認を得るには、アクセス許可を要求します。これらのアクセス許可は、同意を得るプロセスの間に表示され、ユーザーがアクセスを許可/拒否する機会が与えられます。

+ アクセス許可の追加

API / アクセス許可の名前	種類	説明	管理者の同意が必要
▼ Microsoft Graph (1)			
User.Read	委任済み	Sign in and read user profile	- ✔️ DSI に付与されました
▼ Office 365 Management APIs (2)			
ActivityFeed.Read	アプリケ...	Read activity data for your organization	はい ✔️ DSI に付与されました
ServiceHealth.Read	アプリケ...	Read service health information for your organization	はい ✔️ DSI に付与されました

これらは、このアプリケーションが静的に要求するアクセス許可です。コードを使用して、ユーザーの同意が可能なアクセス許可を動的に要求することもできます。 [アクセス許可を要求するためのベストプラクティスを参照する](#)

同意する

管理者は、このディレクトリのすべてのユーザーに代わり同意を与えることができます。すべてのユーザーに管理者の同意を与えると、エンドユーザーが対象アプリケーションを使用するときに、同意画面が表示されなくなります。

DSI に管理者の同意を与えます

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※

The screenshot shows the 'クライアント シークレットの追加' (Add Client Secret) form. It has a '説明' (Description) field with the value 'AppKey'. Below it, the '有効期限' (Expiration) section has three radio button options: '1年' (1 year), '2年' (2 years), and 'なし' (None), with 'なし' selected. At the bottom, there are two buttons: '追加' (Add) and 'キャンセル' (Cancel).

※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。

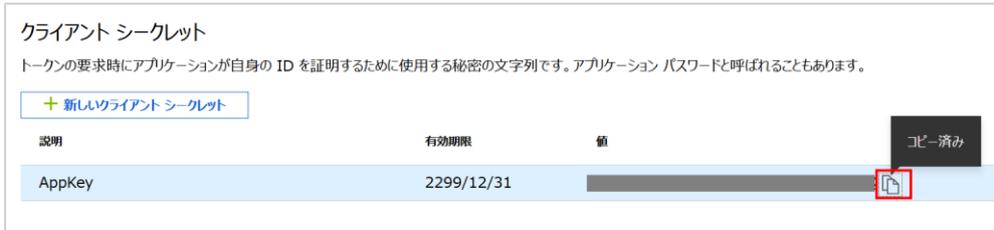
③ 成功メッセージが表示されることを確認します。



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。

アクセストークン設定

アクセスログ **監査ログ**

AzureADを自動で設定する **AzureADを手動で設定する**

ディレクトリ(テナント)ID ※ ※必須

アプリケーション(クライアント)ID ※

アプリケーションKey ※

有効期限 ①

設定

- ・ 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。

アクセストークン設定

アクセスログ **監査ログ**

✓ 設定が完了しました。

ディレクトリ(テナント)ID ※ ※必須

アプリケーション(クライアント)ID ※

アプリケーションKey ※

有効期限 ①

設定

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。

著作権

このドキュメントに記載されている情報（URL 等のインターネット Web サイトに関する情報を含む）は、将来予告なく変更されることがあります。別途記載されていない場合、このソフトウェアおよび関連するドキュメントで使用している会社、組織、製品、ドメイン名、電子メール アドレス、ロゴ、人物、場所、出来事などの名称は架空のものです。実在する名称とは一切関係ありません。お客様ご自身の責任において、適用されるすべての著作権関連法規に従ったご使用を願います。ディスカバリーズは、このドキュメントに記載されている内容に関し、特許、特許申請、商標、著作権、またはその他の無体財産権を有する場合があります。別途ディスカバリーズのライセンス契約上に明示の規定のない限り、このドキュメントはこれらの特許、商標、著作権、またはその他の無体財産権に関する権利をお客様に許諾するものではありません。

© Discoveries Inc. All rights reserved.

Microsoft、Azure、Office 365、SharePoint は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。

以上