



Discoveries InSite IntelliReport

Office 365 監査ログ連携機能アクティブ化手順書

第六版 2019年8月29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	アプリケーションの作成	5
2.3	アクセス許可設定	8
2.4	シークレットキーの登録	11
2.5	アプリケーション情報の送付	13
2.6	監査ログ取得開始手順	13
	補足	14

1 はじめに

1.1 本書の目的

本書は、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)へご連絡ください。

1.2 作業対象者

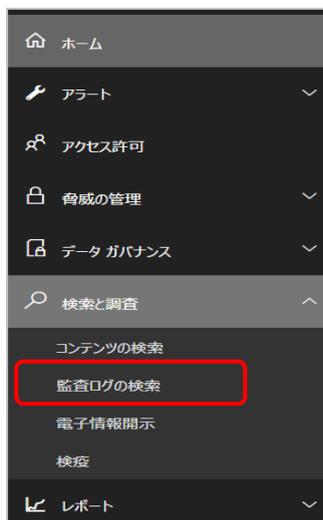
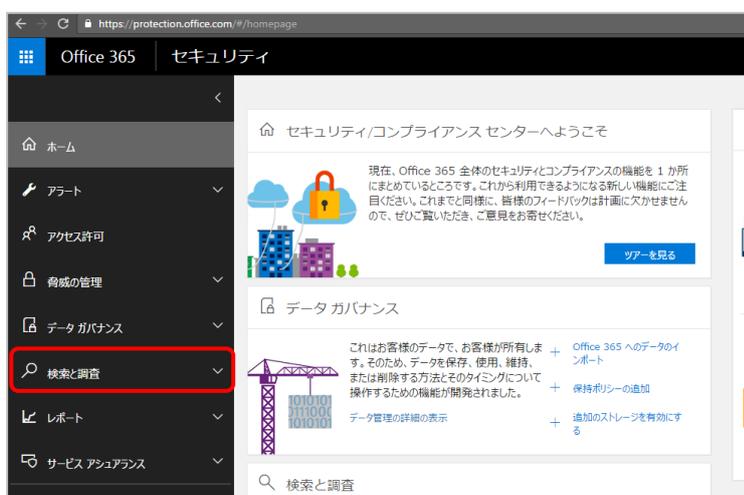
Azure Active directory および、SharePoint Online サイトの管理権限、Office 365 のグローバル管理権限を持っている IT 管理者を対象とします。

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ようお願い申し上げます。

※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 アプリケーションの作成

お客様環境の Microsoft Azure において、インテリ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. 画面右上のメニューから「ディレクトリ+サブスクリプション」をクリックします。
3. 「現在のディレクトリ」欄をコピーし、テキストなどに保存します。

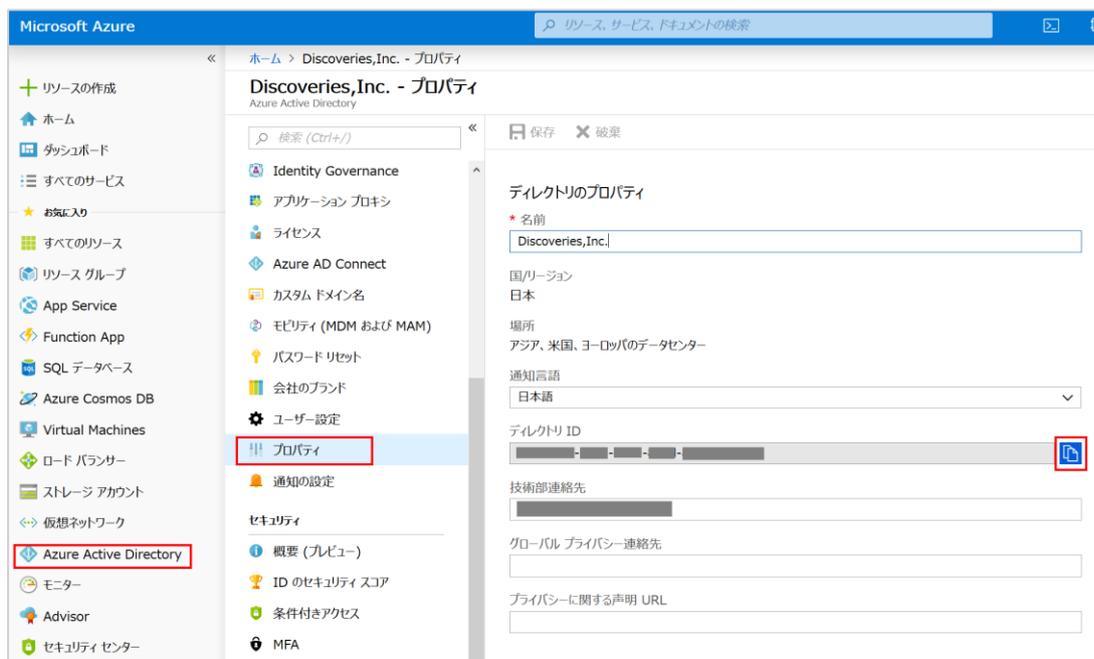
(例)test.onmicrosoft.com

※このディレクトリ名は、以降の手順で使用します。(取得データ①)

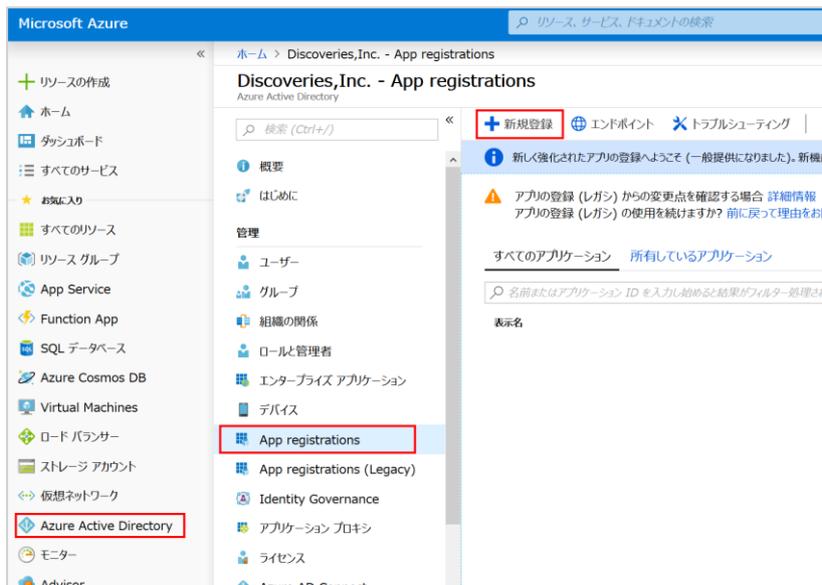


4. 「Azure Active Directory」-「プロパティ」を開きます。
5. 「ディレクトリ ID」欄の「クリップボードにコピー」をクリックし、テキストなどに保存します。

※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②)



6. 「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。



7. 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)。

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だれですか?
 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。

続行す 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 [☑](#)

8. 成功メッセージが表示されることを確認します。



9. 作成したアプリケーションの詳細画面が開きます。

10. 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③)



2.3 アクセス許可設定

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。

ITR_Activity_API - API のアクセス許可

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	-

これは、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](#)

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

API アクセス許可の要求

よく使用される Microsoft API

Microsoft Graph
Office 365、Enterprise Mobility + Security、Windows 10 の大量のデータを活用しましょう。Azure AD、Excel、Intune、Outlook/Exchange、OneDrive、OneNote、SharePoint、Planner などに単一エンドポイント経由でアクセスできます。

Azure Data Lake
ビッグデータ分析シナリオのストレージとコンピューティングへのアクセス

Azure DevOps
Azure DevOps と Azure DevOps Server との統合

Azure Rights Management Services
検証済みのユーザーに、保護されたコンテンツの読み取りと書き込みを許可します

Azure Service Management
Azure portal で利用できる機能の大部分へのプログラムによるアクセス

Data Export Service for Microsoft Dynamics 365
Microsoft Dynamics CRM 組織から外部宛先にデータをエクスポートします

Dynamics 365 Business Central
Dynamics 365 Business Central のデータと機能へのプログラムによるアクセス

Dynamics CRM
CRM ビジネスソフトウェアと ERP システムの機能にアクセスします

Flow Service
フローテンプレートの埋め込みとフローの管理

Intune
Intune データへのプログラムによるアクセス

Office 365 Management APIs
Office 365 と Azure AD のアクティビティログからユーザー、管理者、システム、ポリシーのアクションイベントに

OneNote
OneNote ノートブックでノート、リスト、画像、ファイルなどを作成して管理します

Power BI Service
Power BI のデータセット、テーブル、行などのダッシュボードリソースへのプログラムによるアクセス

PowerApps Runtime Service
強力なデータストレージ、モデリング、セキュリティ、統合の機能

SharePoint
SharePoint データとリモートで対話します

Skype for Business
リアルタイムのプレゼンス、セキュリティで保護されたメッセージング、通話、会議の機能を統合します

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。

[+ 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。

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	- <input checked="" type="checkbox"/> 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 <input checked="" type="checkbox"/> DSI に付与されました
ServiceHealth.Read	アプリケ...	Read service health information for your organization	はい <input checked="" type="checkbox"/> 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。

2.4 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④⑤)

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※

クライアント シークレットの追加

説明
AppKey

有効期限
 1 年
 2 年
 なし

追加 キャンセル

※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。

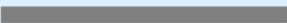


4. 作成したクライアントシークレットキーから、値の「クリップボードにコピー」をクリックし、テキストなどに保存します。(取得データ④)
- ※画面遷移してしまうと、この値は非表示になるため、忘れずにコピーしてください。
- ※この値は、以降の手順で使用します。

クライアント シークレット

トークンの要求時にアプリケーションが自身の ID を証明するために使用する秘密の文字列です。アプリケーション パスワードと呼ばれることもあります。

[+ 新しいクライアントシークレット](#)

説明	有効期限	値	コピー済み
AppKey	2299/12/31		

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⑤)
- 「なし」に設定した場合、「2299/12/31」となります。

2.5 アプリケーション情報の送付

取得したアプリケーションの情報を、弊社までお知らせください。

1. 取得した情報と初期設定を、以下のようにテキストファイルに記載します。

- ConnectionID : お客様のコネクション ID
- TenantName : 現在のディレクトリ名(※取得データ①)
- TenantID : ディレクトリ ID(※取得データ②)
- ClientID : アプリケーション ID(※取得データ③)
- AppKey : キーの値(※取得データ④)
- 有効期限 : キーの有効期限(※取得データ⑤)

```
(例)ディスカバリーズ株式会社_監査ログ連携.txt
ConnectionID : ITR00000000000000000000
TenantName : test.onmicrosoft.com
TenantID : *****_****_****_****_*****
ClientID : *****_****_****_****_*****
AppKey : *****
有効期限 : 2299/12/31
```

2. テキストファイル名を、「お客様会社名_監査ログ連携.txt」として保存します。

(例) ディスカバリーズ株式会社_監査ログ連携.txt

3. 作成したテキストファイルを ZIP ファイル等で**暗号化**していただき、ディスカバリーズ サポートデスクまでご送付ください。

Discoveries Support Desk <support@discoveries.co.jp>

4. 3 営業日以内に、インテリレポート監査ログ連携機能をアクティブ化し、ご案内いたします。

2.6 監査ログ取得開始手順

弊社での連携設定の完了後、まだ監査ログのデータ取得は開始されておりません。

お客様が監査ログの取得対象を有効化する必要がございます。

詳細については、別紙「04_UserManual.pdf(インテリレポート ユーザーマニュアル)」の「5.5 監査ログの取得開始設定」をご参照ください。

※監査ログは、テナント全体のデータが取得されます。

※特定の SharePoint サイトコレクションの監査ログのみをレポートしたい場合は、SharePoint フィルター設定に【サイトコレクション ID】を設定する必要があります。OneDrive 監査ログには、フィルター機能はありません。

補足

本マニュアルは 2019 年 8 月 29 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。

©2019 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