



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

Copyright © Discoveries Inc. All Rights Reserved

目次

1 はじ	じめに	. 1
1.1 1.2	本書の目的 作業対象者	. 1 . 1
2 作美	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。
- 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。
- 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。





「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。

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 たかを確認できます。メール、グループ、ドキュメ	理者がユーザーのパン ント、アクセス許可、	スワードをリセットしたかど ディレクトリ サービスなど	うかの確認が必要な場合: 「に開連するアクティビテ	があります。Office 365 の監 イを検索できます。 検索と語	査ログを検索すると、 皆査ログに関する詳細	組織内の: を表示
ユーザーと管理者のアクティビティの記録を開始する	結果					
検索 りかア	日付 🕶	IPアドレス	ユーザー	アクティビティ	アイテム	1
アクティビティ すべてのアクティビティの結果を表示 ・			検索を実	行して結果を表		
開始日						
2017-06-05 🔳 00:00 🖌						
終了日						
2017-06-13 🔳 00:00 🔽						
ユーザー						
すべてのユーザーの結果を表示						
ファイル、フォルダー、またはサイト 🕕						
ファイル名、フォルダー名、または URL のすべてまたは一部を追加してください。						

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。



	セキュリティ
	組織の設定を更新しています。しばらくお待ちください
_	

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				
$\left(\right)$	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 りかア				
	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。

\sim	設定	<	アクセストークン設定
<u>992</u>	アクセストークン設定		アクセスログ 監査ログ
ste	レポーティング管理設定		
×	監査ログ対象設定		
	コネクションID管理		サービス管理者サインインアカウント ※ ① ※必
			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 〇 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 ※ ①	※必須
バスワード ※	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	1
アプリケーション ID	
サインオン URL	
応答 URL	
キーの説明 SerectKey	
有効期限 2024/09/15 2:40:28	
値	
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。	ок

2.2.2 手動でアプリ登録を行う

グロ−バル管理者の管理者ロ−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)

- 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。 <u>https://portal.azure.com/</u>
- 2. 「Azure Active Directory」-「プロパティ」を開きます。
- 「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)

Microsoft Azure				Ð
*	ホーム > Discoveries,Inc プロパティ			
十リソースの作成	Discoveries,Inc プロパティ			
☆ ホーム ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・		日 保存 🗙 破棄		
:Ξ すべてのサービス ★ お気に入り	 Identity Governance ^ アプリケーション プロキシ 	ディレクトリのプロパティ * 名前		
₩ すべてのリソース	ライセンス の Azure AD Connect	Discoveries,Inc.]
(*) リソース グループ	📄 カスタム ドメイン名	国/V-ジョン 日本		
Function App	モビリティ (MDM および MAM) パフロード Utrue	場所 アジア、米国、ヨーロッパのデータセンター		
SQL データベース ≫ Azure Cosmos DB	会社のブランド	通知言語 日本語	~	
Virtual Machines	◆ ユーザー設定	ディレクトリ ID		
ロード バランサー	 ■ 通知の設定 	• • • • • • • • • • • • • • • • • • •	<u> </u>	1
◆→ 仮想ネットワーク	セキュリティ			
Azure Active Directory	 ・ 板要 (プレビュー) ・ ・ ・	クローハル フライハシー連絡先		
Advisor		プライバシーに関する声明 URL		
🟮 セキュリティ センター	Û MFA			_

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

100	
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	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?
	ットットリーンシントのみ (USI)
○ 任意の組織のティし	レクトリ内のアカウント
─任意の組織のディし	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)	
11 (1) (- 00 -1 - 7 (MAR)	
登択に関する詳細	
リダイレクト UF	(1)(1)(1)(1)(1)(1)(1)(1)(1)(1)(1)(1)(1)(
リダイレクト UF ユーザー認証が成功す	KI(自哈中JRE) 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
リダイレクト UF ユーザー認証が成功す すが、ほとんどの認証:	XI (自PG PJ BE) 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 シナリオで値が必要となります。
リダイレクト UF ユーザー認証が成功す すが、ほとんどの認証 Web	(1 (自哈ப) BL) 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 シナリオで値が必要となります。 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。

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)

ホーム > DSI - アプリの登録 > ITR_Activ	vity_API
ITR_Activity_API	
_○ 検索 (Ctrl+/) 《	直 削除 ⊕ エンドポイント
101 005	
114.女	新しく強化されたアプリの登録へようこそ。アプリの登録(レガシ)からの変更点を確
📣 クイックスタート	
管理	表示名 : ITR_Activity_API コピー済み
🧫 ブランド	アプリケーション (クラ):
● 認証	ディレクトリ (テナント…:
📍 証明書とシークレット	オブジェクトロ :
→ APIのアクセス許可	*
 FREE 22 2 40 (12) 	

- 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。

 ○ 検索(Ctrl+/) ○ 検索(Ctrl+/) ■ 概要 ▲ クイックスタート 	APIのアクセス許可 アプリケーションボ API を使用する承認を 許可/拒否する機会が与えられます。	得るには、アクセス許可を要求	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、ユーザーカ	
管理 	+ アクセス許可の追加	10.00	HA GIR	原理集の同言が必要	
ブランド		(E)A	8CM3	后进有00H近20-05号	
	Microsoft Graph (1)				
♀ 証明書とシークレット	User.Read	委任済み	Sign in and read user profile	-	
→ APIのアクセス許可	これらは、このアプリケーションが静的に	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			
APIの公開	同意が可能なアクセス許可を動的に要求す	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			
🛃 所有者	ノラウナイスを参照する				
🔮 ロールと管理者					
□ マニフェスト	同意する				
サポート + トラブルシューティング	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				
🗙 トラブルシューティング	白い内蔵をうえると、エント エーワーが対象アンソワーンヨンを使用するとさに、内意画面が表示されなくなります。 す。				
第1しいサポート要要					

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。					
至 Azure Data Lake ビック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	<mark> テータへのプロ</mark> 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 ん、ポリシーのアクションとイベントに	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 グラムによるアクヤス			
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 inf	formation for your organization
ServiceHealth	ServiceHealth.R	lead	Read activity data for	your organization
API アクセス許可の要求 くすべてのAPI Office 365 Management https://manage.office.com, アプリケーションに必要なアク 曼任されたアクセス許可 アプリケーションは、サインイン セスする必要があります。 アクセス許可を選択する	ent APIs / ドキュメント ⑦ /セス許可の種類 として API にアク	アプリケーションの資 アプリケーションの資 アプリケーションは、 ラウンド サービスまれ	河 サインインしたユーザーなしで、バック <i>グ</i> たはデーモンとして実行されます。 すべて <i>限</i> 券	
検索するテキストを人力 アクセス許可			管理者の同意が必要	
▼ ActivityFeed (1)				
ActivityFeed.Read Read activity data for	your organization 🚯		はい	
ActivityFeed.ReadDlp Read DLP policy event	ts including detected sensitive dat	a 🕦	はい	
ActivityReports				
✓ ServiceHealth (1) ✓ ServiceHealth.Read			はい	
ThreatIntelligence	formation for your organization (,		
アクセス許可の送加	2			

- 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「〇〇〇(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 者の同意レコードが、以下の一覧の内容に一	れたアクセス許可に対す 敗するよう更新されます	する同意を付与しますか? この操作により、このアプリク す。	ーションが既に持っている既存の管理
はいいえ			
+ アクセス許可の追加			
API / アクセス許可の名前	種類	設明	管理者の同意か必要
 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め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 者の同意を与えると、エンド ユーザーが対象アン す。	に代わり同意を与えるこ プリケーションを使用する	とができます。すべてのユーザーに管理 5ときに、同意画面が表示されなくなりま	
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。 許可/拒否する機会が与えられます。	こは、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	凱に表示され、ユーザーがアクセスを
+ アクセス許可の追加			
API / アクセス許可の名前	種類	說明	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 同意が可能なアクセス許可を動的に要求すること プラクティスを参照する	するアクセス許可です。コ ともできます。 アクセス語	ードを使用して、ユーザーの 午可を要求するためのベスト	
同意する			
管理者は、このディレクトリのすべてのユーザ- 者の同意を与えると、エンドユーザーが対象ア す。	ーに代わり同意を与えるこ プリケーションを使用する	とができます。すべてのユーザーに管理 5ときに、同意画面が表示されなくなりま	
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)

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。

 - 概要 シイックスタート 管理 ブランド フランド 	 ※ 資格情報は、Web アドレスの指定が可能な 高いレベルで保証するには、資格情報として 証明書 証明書は、トークンの要求時にアプリケーション 証明書のアップロード 	場所で (HTTPS スキーマを使用して) トークンを受信する (クライアント シークレットではなく) 証明書を使うことをお勧 ルの ID を証明するシークレットとして使用できます。 公開キ
ジ 認証	inter	開始日
 API のケクセスます」 API の公開 所有者 マニフェスト 	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 1	LD を証明するために使用する秘密の文字列です。 アプリク
サポート + トラブルシューティング ★ トラブルシューティング ③ 新しいサポート要求	+ 新しいクライアント シークレット 説明	415310000 6 0
■ 新しいサホート要求	このアプリケーションのクライアント シークレット	は作成されていません。

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。

Ø	アプリケーション資格情報の更新	14:25
ア	プリケーション ITR_Activity_API の資格情報	報が正常に更
新る	されました	

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。

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
АррКеу	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。

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 	5
サービス管理者サインインアカウント ※ ①	※必須
パスワード ※	
設	Ē

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Кеу ※		
有効期限()		
例) 2020/01/01		

- 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()	
2024/09/16	
-	

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