



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	こめに	1
	1.1	本書の目的	. 1
	1.2	作業対象者	. 1
2	作業	冬手順	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

☐ データ ガバナンス

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? たかを確認できます。メ-	を削除したかどうかや、 ール、グループ、ドキ:	、管理者がユーザーのパワ ュメント、アクセス許可、	マ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 ィを検索できます。 検索と!	査ログを検索すると、 監査ログに関する詳細で	組織内のコ を表示
ユーザーと管理者のアクラ	ティビティの記録を開始す	る結果					
検索	つ クリア	日付 👻	IP アドレス	ユーザー	アクティビティ	アイテム	a
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	天 示	
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 のすべてまたは一部を	「一名、または URL 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ように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□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 りかア
アクティビティ
9へてのアクティビティの相乗征衣小 ▼

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。

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)

Microsoft Azure		𝒫 リソース、サービス、ドキュメントの検索	Þ.	Ŗ
«	ホーム > Discoveries,Inc プロパティ			
┿ リソースの作成	Discoveries,Inc プロパティ Azure Active Directory			
☆ ホーム □ ダッシュボード		□ 保存 × 破集		
: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		
🗰 すべてのリソース	ライセンス	* 名前 Discoveries,Inc.		
(剤) リソース グループ	 Azure AD Connect カフタルドメイン名 	国/リージョン 日本		
 App Service Function App 	 アメリントレート モビリティ (MDM および MAM) 	ロイ 場所 アジア 米国 ユーロッパのデータセンター		
SQL データベース	 ↑ パスワード リセット ▲ 会社のブランド 	通知言語 日本語 日本語	~	
Virtual Machines	✿ ユーザー設定	デルクトリ ID		-
☆ ロード バランサー 二 ストレージ アカウント	■ 通知の設定	技術部連絡先		1
<⋯> 仮想ネットワーク	セキュリティ			
Azure Active Directory	① 概要 (プレビュー)	クローバルフライバシー連絡先		
 (≥) €=9- Advisor 	 ✓ ID のセキュリティスコア ○ 条件付きアクセス 	プライバシーに関する声明 URL		
セキュリティセンター	O MFA			

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)。
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)
○ 任意の組織のティレクトリ内のアカウント
「社会の相関のティレットの内のパイリットと、Ma人用の Microsoft アルッシト (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 V https://discoveriesintellireport.azurewebsites.net V
続行す 登録 登録

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。
- 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)

ホーム > DSI - アプリの登録 > ITR	Activity_API
ITR_Activity_API	
,p 検索 (Ctrl+/)	≪
- 概要	
📣 クイックスタート	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(レカシ)からの変更点を構
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::
③ 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 ID :
→ APIのアクセス許可	*

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 တို့)アクセス許可				
 ○ 検索 (Ctrl+/) ◎ 検索 (Ctrl+/) ■ 概要 ▲ クイックスタート 	API のアクセス許可 アブリケーションが 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:	求します。これらのアクセス許可は、同意を	を得るプロセスの間に表示され、ユーザーカ	
管理	十 アクセス許可の追加				
🚽 ブランド	API / アクセス許可の名前	種類	說明	管理者の同意が必要	
∋ 認証	 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	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め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				
🛃 所有者	フラフティスを参照する				
🔓 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 老の同意を与えると、エンドコーゼーが対象でプリケーションを使用するときに、同意両面が基本されなくかれま				
🗙 トラブルシューティング	す。	180 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	3CCIC、同意画面の 私外C41/3 くなりま		
🔮 新しいサポート要求	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。

よく使用される Microsoft API		
Microsoft Graph Office 365、Enterprise Mobility + Security、 う。Azure AD、Excel、Intune、Outlook/Exc Planner などに単一エンドポイント経由でア	Windows 10 の大量のデータを活用しましょ change、OneDrive、OneNote、SharePoint、 ′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	Civit 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	。 ゆ 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 ソフトウエアと ERP シス テムの機能にアクセスします	<mark>ノ・ Flow Service フロー テンブレートの埋め込みとフロー の管理</mark>	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	S 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、 今年の時間ですなん」ナス

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
	· · · · · · · · · · · · · · · · · · ·	

くすべての API Office 365 Management APIs https://manage.office.com/ ドキュメント び アプリケーションに必要なアクセス許可の種類 愛転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。 アグセス許可を選択する アクセス許可を選択する 愛々セス許可を選択する 愛々セス許可を選択する 愛々セス許可を選択する アクセス許可を選択する 愛々セス許可を選択する レ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 レービスまたはデーモンとして実行されます。 レ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 レービスまたはデーモンとして実行されます。 レービスまたはデーモンとして実行されます。 レ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 レービス非可を選択する レ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 レービスまたはデーモンとして実行されます。 アクセス許可としてより アクセス許可とした。 アクセストゥーレービスものののでのののでのののでのののでのののでのののでのののでのののでのののでのの	אין איז	APIアクセス許可の要求	
 Office 365 Management APIs https://manage.office.com/ドキュメントビ アプリケーションに必要なアクセス許可の種類 ダ紙されたアクセス許可 アプリケーションに、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。 アクセス許可を選択する 校案するテキストを入力 アクセス許可を選択する をないivityFeed.Read Read activity data for your organization ●	e 365 Management APIs //manage.office.com/ ドキュメントビ ションに必要なアクセス許可の種類 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て、パックク ラウンドサービスまたはデーモンとして実行されます。 デブを選択する マベ キストを入力 Feed (1) ActivityFeed.Read Bead activity data for your organization ① ActivityFeed.ReadDlp Keed DLP policy events including detected sensitive data ② Keed to LP policy events including detected sensitive data ③ Ketwite Health (1) Service Health .Read Read service health information for your organization ④ Keed Service Health .Read	〈 すべての API	
The Application Control In Contrel In Contrel In Contrel In Contrel I	Animageonitection of FFEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEE	Office 365 Management APIs https://manage.office.com/ ドキュメント 区	
	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として API にアク 愛があります。 アブリケーションは、サインインしたユーザーなして、バックク ラウンド サービスまたはデーモンとして実行されます。 マベマ キストを入力 で電音の同意が必要 Feed (1) Activity feed.Read Read activity data for your organization ● はい Activity feed.ReadDlp Read DLP policy events including detected sensitive data ● はい Reports control con	アプリケーションに必要なアクセス許可の種類	
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。 アクセス許可を選択する 検索するテキストを入力 アクセス許可 ActivityFeed Read Read activity data for your organization ● ActivityFeed ReadDlp Read activity Reports ActivityReports	ションは、サインインしたユーザーとして API にアク 愛があります。 アプリケーションは、サインインしたユーザーなして、バックク ラウンド サービスまたはデーモンとして実行されます。 マペイ キストを入力 Feed (1) Read activity deta for your organization ● はい Read activity data for your organization ● はい Read blue policy events including detected sensitive data ● はい Reports Health (1) Service Health.Read Read service health information for your organization ● はい	委任されたアクセス許可	アプリケーションの許可
アクセス許可を選択する 検索するテキストを入力 アクセス許可 管理者の角急が4 マ ActivityFeed (1) ActivityFeed.Read Read activity data for your organization ActivityFeed.ReadDlp Read DLP policy events including detected sensitive data Club ActivityReports マ ServiceHealth (1)	マラを選択する マベス キストを入力 Feed (1) ActivityFeed.Read activity data for your organization ● はい ActivityFeed.ReadDlp Activity Geed.ReadDlp Keed DLP policy events including detected sensitive data ● はい Reports Health (1) Service Health.Read Read service health information for your organization ● はい telligence	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。	アプリケーションは、サインインしたユーザーなしで、バック <i>グ</i> ラウンド サービスまたはデーモンとして実行されます。
検索するテキストを入力 アクセス時可 管理者の向意か マ ActivityFeed (1) C ActivityFeed.Read Civity data for your organization ① はい ActivityFeed.ReadDlp にない Read activity Ged.ReadDlp にない Read DLP policy events including detected sensitive data ② はい ActivityReports ServiceHealth (1)	جکر ۲۰۰۸ التوليق مع مع المحمد الم	アクセス許可を選択する	すべ
アクセス科利 管理者の向応が マ ActivityFeed (1) Image: Comparization の Image: Comparized Read Activity Feed.Read Dip Read activity Feed.Read Dip Policy events including detected sensitive data の Image: Comparized Read Dip Read Policy events including detected sensitive data の Image: ActivityReports Image: Comparized Read Dip Read Policy events including detected sensitive data の Image: Comparized Read Dip Read Policy events including detected sensitive data の Image: ActivityReports Image: Comparized Read Dip Read Policy events including detected sensitive data の Image: Comparized Read Dip Read Policy events including detected sensitive data の	ی بینا بین بین می ب ما بین می بی می بین می بی بین می بی بین می	検索するテキストを入力	
ActivityFeed (1) ActivityFeed Read Read activity data for your organization ActivityFeed ReadDlp Read DLP policy events including detected sensitive data ActivityReports ActivityReports ServiceHealth (1)	Feed (1) ActivityFeed.Read はい ActivityFeed.ReadDlp はい Read activity data for your organization ActivityFeed.ReadDlp Read DLP policy events including detected sensitive data ActivityFeed.ReadDlp Read DLP policy events including detected sensitive data Read DLP policy events including detected sensitive data Read bLP policy events including detected sensitive data Read service health information for your organization Read service health information for your organization Read service health information for your organization 	アクセス許可	管理者の同意が必要
ActivityFeed.Read Read activity data for your organization • ttw ActivityFeed.ReadDlp Read DLP policy events including detected sensitive data • ttw ActivityReports ttw ServiceHealth (1) ttw	ActivityFeed.Read Read Activity data for your organization ActivityFeed.ReadDlp Read DLP policy events including detected sensitive data ActivityFeed.ReadDlp Read DLP policy events including detected sensitive data ActivityFeed.Read DLP policy events including detected sensitive data ActivityFeed.Read DLP policy events including detected sensitive data ActivityFeed.Read Sense Read Read Sense Read Se	▼ ActivityFeed (1)	
ActivityFeed.ReadDlp ttv Read DLP policy events including detected sensitive data • ttv ActivityReports serviceHealth (1)	ActivityFeed.ReadDlp table and the sensitive data ActivityFeed.ReadDlp certain and the sensitive data ActivityFeed.ReadDlp certain and the sensitive data ActivityFeed.ReadDlp certain and the sensitive data ActivityFeed.ReadCertain and the sensitive data Activity Feed.ReadCertain and the sensitive dat	ActivityFeed.Read Read activity data for your organization	はい
► ActivityReports	Reports Health (1) Service Health.Read Read service health information for your organization telligence	ActivityFeed.ReadDlp Read DLP policy events including detected sensitive data	・ ・ の はい
▼ ServiceHealth (1)	Health (1) ServiceHealth.Read Lead service health information for your organization ● LetU telligence	ActivityReports	
	ServiceHealth.Read It information for your organization It is the service health information for your organization It is the service health information for your organization It is the service health information in the service health information is the service health informatio	▼ ServiceHealth (1)	
ServiceHealth.Read two Read service health information for your organization	telligence	ServiceHealth.Read Read service health information for your organization ①	はい
ThreatIntelligence		ThreatIntelligence	
		アクセス許可の追加	

- 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。						
はいいえ						
+ アクセス許可の追加						
API/アクセス許可の名前 経筑 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						
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 者の同意を与えると、エンド ユーザーが対象アプリケー す。	り同意を与えるこ ・ションを使用する	ことができます。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。				
	2/2427 2511を更す	21.ます マわらのマクセフな可け 同音を得えづつセフの思	ミニ 妻子 さわ ユーザー ポワクセフタ		
許可/拒否する機会が与えられます。	7CA19293				
+ 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。

 観要 クイックスタート 管理 ブランド 	資格情報は、Web アドレスの指定が可 高いレベルで保証するには、資格情報と 証明書 証明書は、トークンの要求時にアプリケー ↑ 証明書のアップロード	能な場所で (HTTPS スキーマを使用して) トークンを5 して (クライアント シークレットではなく) 証明書を使うこ -ションの ID を証明するシークレットとして使用できます。	受信する とをお勧め , 公開キー
	10,60	開始日	
 APIのアクセス許可 APIの公開 所有者 マニフェスト サポート + トラブルシューティング 	このアプリケーションには証明書が追加さ 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!	れていません。 身の ID を証明するために使用する秘密の文字列です。	。 ምታባታ
 ★ トラブルシューティング 新しいサポート要求 		有効明限 ンツトは作成されていません。	60

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			
АррКеу			
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	青報が正常に更
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。					
+ 新しいソライアント シークレット 説明	有効期限	缅	コピー済み		
АррКеу	2299/12/31		N		

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)

- 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
- 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