すとなり
2025.01.29

2025 年 2 月 1 日に Azure AD Graph API は廃止されます

2025 年 2 月 1 日以降、既存のアプリケーションが Azure AD Graph API を呼び出すことが段階的に出来なくなります。

【推奨事項】
- Microsoft Entra 推奨事項（ID＞概要＞推奨事項）を参照し、Azure AD Graph API を使用しているアプリケーションを特定し、特定されたアプリケーションを Microsoft Graph API を使用するように移行します
- 上記の対応が難しい場合、アプリケーションの blockAzureAdGraphAccess 属性を false に設定します
  ただし、この対応を行っても 2025/7/1 以降 Azure AD Graph API は完全に使用できなくなります

フェーズ開始日	既存アプリへの影響	新規アプリへの影響
2024/9/1	なし	blockAzureAdGraphAccess を明示的に false に設定しない限り、アプリケーションは Azure AD Graph API にリクエストできません
2025/2/1	blockAzureAdGraphAccess を明示的に false に設定しない限り、アプリケーションは Azure AD Graph API にリクエストできません	
2025/7/1	Azure AD Graph API は完全に削除されます	

https://techcommunity.microsoft.com/blog/identity/take-action-by-february-1-azure-ad-graph-is-retiring/4365743

2025 年 4 月から MSOnline と AzureAD PowerShell は段階的に廃止

MSOnline と Microsoft AzureAD の PowerShell モジュールは 2024 年 3 月 30 日に非推奨になり、段階的に廃止されます。

- MSOnline PowerShell の廃止は 2025 年 4 月上旬に開始され、2025 年 5 月下旬に終了します
- AzureAD PowerShell は 2025 年 3 月 30 日以降はサポートされなくなり、2025 年 7 月 1 日に完全に廃止されます

また、MSOnline PowerShell の移行を確実にするため、下記の一時的なサービス停止が予定されています。
- 2025 年 1 月 20 日から 2025 年 2 月 28 日の間に、少なくとも 2 回数時間（3 時間から 8 時間の間）の停止
- 2025 年 3 月中に、より長い期間の一時的な停止

MSOnline と AzureAD PowerShell からのサインインはいずれも Entra サインイン ログでアプリケーションを「Azure Active Directory PowerShell」にフィルターすることで表示できます。
また、Microsoft Entra 推奨事項（ID＞概要＞推奨事項）を参照することでも特定することができます。

モジュール	サポート終了	一時的な停止	廃止
MSOnline	2025/3/30	2025/1/20-3/30	2024/4 上旬 - 2025/5 下旬
AzureAD		なし	2025/7/1

https://techcommunity.microsoft.com/blog/identity/action-required-msonline-and-azuread-powershell-retirement---2025-info-and-resou/4364991

MDE ですべてのログを取得するオプションがパブリック プレビューしました

Microsoft Defender for Endpoint（MDE）はセキュリティ調査に有効なログをサーバーに送信し、ログは Advanced hunting クエリで調査出来ますが、セキュリティ調査に有効ではないと考えられるログについては収集していませんでした。これは、大量のデータを迅速に調査するためのバランスを考慮した選択でした。

今回、セキュリティ調査に有用かどうかによらず全てのログを収集する「集計レポート」オプションがパブリック プレビューとして提供されました。ただし、下記の注意が必要です。

- 新しいオプションで収集されるデータは 1 時間に 1 回収集されます（通常は 15 分程度）
- Sentinel 等の SIEM や外部ストレージにデータを送信している場合はデータサイズおよび課金額が増加します

https://techcommunity.microsoft.com/blog/microsoftdefenderatpblog/get-greater-visibility-with-aggregated-reporting-of-endpoint-telemetry-signals/4366712

Microsoft Sentinel の STIX オブジェクトのサポートがパブリック プレビュー

Microsoft Sentinel は、脅威インテリジェンスの統合と活用を強化するために、新しい STIX オブジェクトのサポートをパブリック プレビューとして提供開始しました。
これにより、従来の IoC のみを使用したハンティングに加えて、脅威アクター、攻撃パターン、ID、リレーションシップで脅威インテリジェンス データを拡張（オブジェクト化）し、より高度なセキュリティ対応が可能になります。
STIX オブジェクトは STIX TAXII サーバー、API、ファイル、手動入力によって取り込むことができ、オブジェクト間の関係性を定義することでハンティング クエリで使用できるようになります。

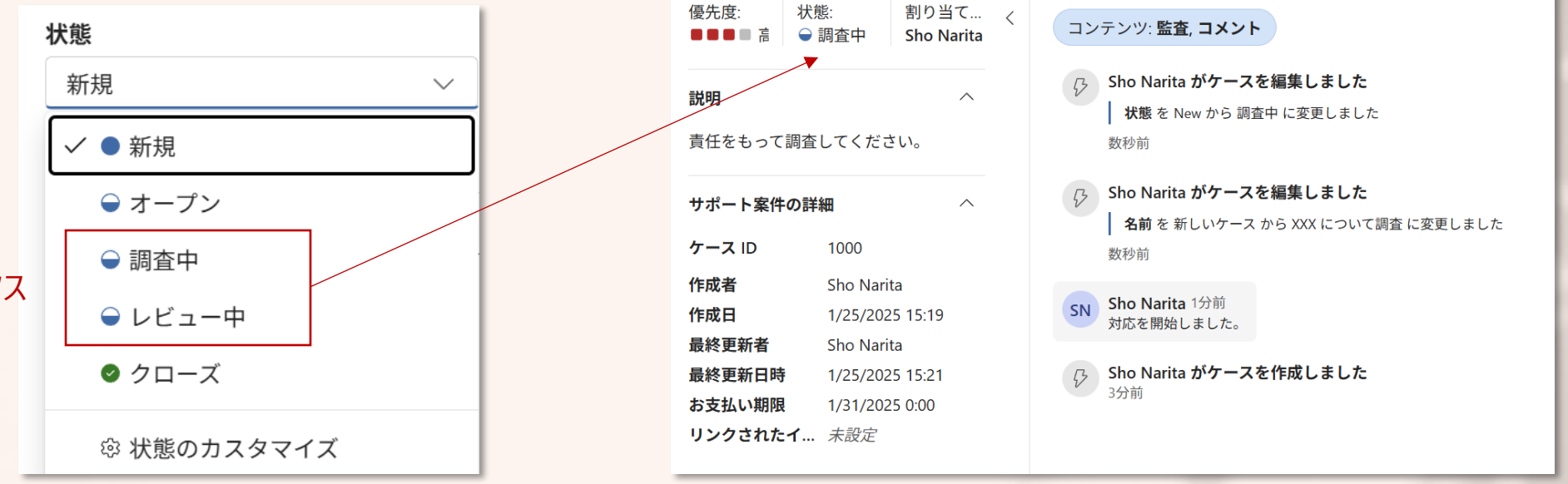
https://techcommunity.microsoft.com/blog/microsoftsentinelblog/announcing-public-preview-new-stix-objects-in-microsoft-sentinel/4369164

統合セキュリティ運用プラットフォームの「ケース」管理による SOC 効率化

統合セキュリティ運用プラットフォーム（Unified Security Operation Platform）を有効にしたテナントにおいて、SOC ワークロードを「ケース」に統合管理できるようにする機能をパブリック プレビューしました。
ケース管理により、専用のチケット管理システムに依存せずに SOC 全体のコラボレーション、カスタマイズ、証拠収集、レポートを実現します。

今回の発表では下記の機能がリリースされました。

- カスタムのステータス値（サブ ステータス）を作成する
- タスクと期日を割り当てることで、説明責任を向上させる
- 複数のインシデントをケースにリンクする



https://techcommunity.microsoft.com/blog/microsoftsentinelblog/improve-secops-collaboration-with-case-management/4369044

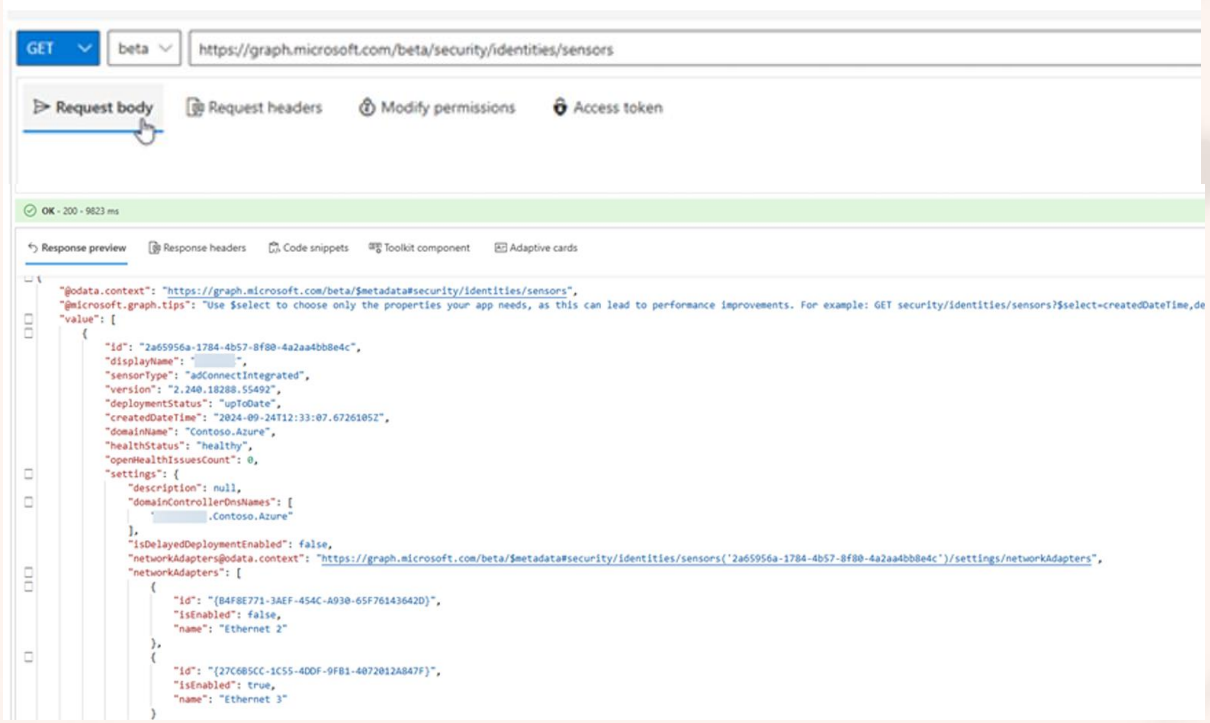
ありがとうございます

narisho

MDI センサーの状態を取得する API がリリースされました

Microsoft Defender for Identity（MDI）はオンプレミス Active Directory の脅威を検出、調査するために使用できます。
MDI は「センサー」と呼ばれるモジュールをドメイン コントローラーなどにインストールしますが、センサーが停止していたり推奨通りに構成されていなかったりした場合には Defender ダッシュボードから確認する必要がありました。
新たに MDI センサー管理 API がリリースされたことで、センサーの状態に問題が発生していないことの確認を自動化できます。

アクセス許可は SecurityIdentitiesSensors.Read.All または SecurityIdentitiesSensors.ReadWriteAll を使用します。



https://techcommunity.microsoft.com/blog/microsoftthreatprotectionblog/introducing-the-new-defender-for-identity-sensor-management-api/4367164

Microsoft Sentinel リポジトリで Bicep をサポート

Bicep は、Azure リソースを宣言的にデプロイするための言語 (DSL) です。JSON ベースの Azure Resource Manager (ARM) テンプレートの進化形として、人が読みやすい簡略化された記述を提供します。

Microsoft Sentinel のリポジトリ機能では、既に GitHub または Azure DevOps と統合して、バージョン管理された状態で Sentinel 構成を管理できます。Bicep サポートの導入により、次のことができるようになりました。

- Sentinel リソースのよりクリーンで保守しやすいテンプレートを作成します
- モジュラー コンポーネントを活用して、カスタム分析ルール、プレイブック、データコネクタを定義します
- Sentinel 構成をデプロイおよび更新する際の反復サイクルを短縮できます

Bicep を使用することで下記の利点を得られます。

- **合理化された構成管理**: 直感的な構文を使用して Sentinel リソースを定義し、従来の ARM テンプレートの複雑さを軽減します
- **コラボレーションの改善**: 好みのリポジトリ内で Bicep テンプレートをバージョン管理できるため、ピア レビュー、自動化された CI/CD パイプライン、追跡可能な変更履歴が可能になります
- **迅速な展開**: 一貫性のある Sentinel 構成を、再利用可能なモジュールとパラメータ化と検証のための組み込みツールでデプロイします

https://techcommunity.microsoft.com/blog/microsoftsentinelblog/whats-new-bicep-support-in-microsoft-sentinel-repositories/4358490

Search-MailboxAuditLog と New-MailboxAuditLogSearch の廃止

2025 年 3 月 1 日以降、メールボックス監査ログへのアクセスで Search-MailboxAuditLog と New-MailboxAuditLogSearch は使用できなくなります。以降は Search-UnifiedAuditLog コマンドレットを使用して Exchange Online 監査ログにアクセスすることができます。

現在 Search-MailboxAuditLog と New-MailboxAuditLogSearch コマンドレットを使用している場合は、下記ステップで移行できます。

【移行ステップ】
1. 対象になるコマンドレットを使用しているスクリプト、ツール、アプリケーションを特定します
2. 法務やコンプライアンス チームと新しいコマンドレットが業務要件を満たしていることを確認します
3. テナントの統合監査ログ（UAL）が有効になっていることを確認します
4. 移行ツール（2025/3 までに提供予定）を使用してコマンドレットを移行します

機能	Search-MailboxAuditLog & New-MailboxAuditLogSearch	Search-UnifiedAuditLog
レコード タイプ	Exchange のみ	M365 全体
フィルタリング	標準	最新
データ保持	設定による	180 日間
コンプライアンス	限定的	完全
UX	断片的	統合

https://techcommunity.microsoft.com/blog/microsoftsecurityandcompliance/microsoft-exchange-online-search-mailboxauditlog-and-new-mailboxauditlogsearch-w/4366310