【Microsoft Sentinel】
サービス概要

2025年4月25日

改訂履歴

版数	発行日	改訂内容
第1版	2025年4月25日	初版発行

本資料の内容は 2025/4/25 時点のものです。製品のアップデートにより変更となる場合がございます旨ご了承ください。

Agenda

1. 前提情報
2. Microsoft Sentinelとは
    1. 企業のセキュリティ課題と解決策
    2. Microsoft Sentinelとは
3. Microsoft Sentinelの基本機能
    1. Microsoft Sentinelの基本機能
    2. 基本機能① データの収集
    3. 基本機能② 脅威の検出
    4. 基本機能③ 調査
    5. 基本機能④ 対応
4. 導入メリットとポイント
    1. 導入メリット
    2. 導入時の注意点とポイント
5. シナリオ別の活用方法
    1. シナリオ別の活用方法
    2. シナリオ① 社内ITインフラの脅威検出と自動対応
    3. シナリオ② 複数クラウド環境の統合監視
    4. シナリオ③ グループ会社を含む分散組織での
       セキュリティ統制
6. データの収集範囲

1. 前提情報

1.1. 用語集

本書で使用する用語及び略称を以下の通り定義します。

No.	用語	説明
1	サイバー攻撃	コンピュータシステムやネットワークに対する不正アクセスや破壊行為。
2	Log Analytics	Azure Monitorの一部で、ログデータを収集、分析、視覚化するためのツール。Kusto Query Language (KQL)を使用して、ログデータに対するクエリを実行し、特定の条件に一致するレコードの取得、傾向の特定、パターンの分析を行う。
3	Syslog	ネットワーク機器やLinuxサーバーなどがログを送信するための標準プロトコル。メッセージは優先度やタイムスタンプなどの構造を持ち、UDP/TCP/TLSで送信可能。
4	CEF	Syslogを拡張した、セキュリティ製品向けの標準ログ形式。ベンダー非依存で、イベントの詳細情報（送信元IP、ユーザー名など）を構造化して出力する。
5	REST-API	ウェブサービスと通信するためのAPI。HTTPプロトコルを使用。
6	Azure Monitor	クラウド環境とオンプレミス環境からの監視データを収集し、分析し、それに対応するための包括的な監視ソリューション。Azure Monitor エージェント (AMA)は、Azure Monitorにデータを送信するための新しいエージェント。
7	Logstash	データ収集、処理、転送を行うオープンソースのデータ処理パイプライン。さまざまな入力ソースからデータを収集し、フィルターを通じてデータを変換し、Elasticsearchなどの出力先に送信する。
8	Kusto クエリ（KQL）	データの探索、パターンの検出、異常や外れ値の特定、統計モデリングなどを行うための強力なツール。

1.1. 用語集

本書で使用する用語及び略称を以下の通り定義します。

No.	用語	説明
9	脅威インテリジェンス	Microsoft Defender 脅威インテリジェンス (Defender TI)は、脅威インフラストラクチャの分析を行い、脅威インテリジェンスを収集するためのプラットフォーム。これにより、トリアージ、インシデント対応、脅威ハンティング、脆弱性管理などのワークフローを合理化する。
10	エンティティ	データベースやデータモデル内で管理・識別される対象（オブジェクト）を指す。具体的には、顧客、商品、注文などの物理的または抽象的な項目を表す。 Sentinelにおけるエンティティは、ユーザー、ホスト、IPアドレス、アプリケーションなどの組織内の重要なオブジェクトを指す。
11	Fusionエンジン	複数のデータソースからの情報を統合し、脅威を検出するエンジン。
12	SSH,RDP	リモートアクセスのためのプロトコル。SSHは主にLinux/Unixシステムで使用され、RDPはWindowsシステムで使用される。
13	MITRE ATT&CK フレームワーク	サイバー攻撃の戦術と技術を体系化した知識ベース。攻撃者の行動を理解し、防御策を強化するために使用される。 ATT&CKは、攻撃のライフサイクルを14のフェーズ（戦術）に分け、それぞれのフェーズで使用される具体的な技術や手法を詳細に説明している。
14	Azure Machine Learning	機械学習モデルの構築、トレーニング、デプロイを支援するクラウドベースのサービス。データサイエンスのワークフローを効率化する。

1.1. 用語集

本書で使用する用語及び略称を以下の通り定義します。

No.	用語	説明
15	HTTP Webhook	イベントが発生した際に指定されたURLにHTTPリクエストを送信する仕組み。リアルタイムでの通知やデータ転送に使用される。
16	VPN,ExpressRoute	セキュアなネットワーク接続を提供する技術。 VPNは、データを暗号化し、仮想的な専用線を作成することで、リモートアクセスや拠点間通信をセキュアに行うことができる。 ExpressRouteは、Microsoft Azureとオンプレミスネットワークをプライベート接続で結ぶサービス。これにより、インターネットを経由せずに高信頼性、低遅延、高セキュリティの接続を実現する。
17	Firewall/UTM	Firewall：ネットワークのトラフィックを監視し、許可された通信のみを通過させることで、外部からの攻撃を防ぐ装置。 UTM（統合脅威管理）：Firewallの機能に加えて、複数のセキュリティ機能（例えば、アンチウイルス、アンチスパム、コンテンツフィルタリング、侵入防止システムなど）を統合した装置。
18	プロキシサーバー	クライアントとサーバーの間に立ち、通信を仲介することで、セキュリティやプライバシーを向上させるサーバー。
19	IDS/IPS	侵入検知システム（IDS）はネットワーク内の不正な活動を検出し、侵入防止システム（IPS）はそれを防止する装置。

2. Microsoft Sentinelとは

2.1. 企業のセキュリティ課題と解決策

近年のデジタル技術の進展と社会への普及に伴い、セキュリティリスクの増加とサイバー攻撃の複雑化・多様化が急速に進んでいます。
ここでは、現在の組織が直面している主なセキュリティ課題とその解決策を説明します。

組織が抱えるセキュリティ課題

サイバー攻撃の複雑化と多様化
ランサムウェア・ゼロデイ攻撃・フィッシングなど、
標的となる対象と攻撃パターンが増加している

多様なセキュリティ製品利用による管理工数の肥大化
各製品が別々にログを管理するため、管理が煩雑になり、
脅威の発見が遅延する

課題解決ソリューション

SIEM（**S**ecurity **I**nformation and **E**vent **M**anagement）

- **複数のサービスや製品のログを統合管理**
- ログの収集、攻撃パターンの検出、リアルタイム分析と通知を行う

SOAR（**S**ecurity **O**rchestration, **A**utomation and **R**esponse）

- SIEM の運用をする上で行う**分析や対処、ワークフローを自動化**
- 運用負荷を軽減し、迅速な対応を実現

Microsoft Sentinel

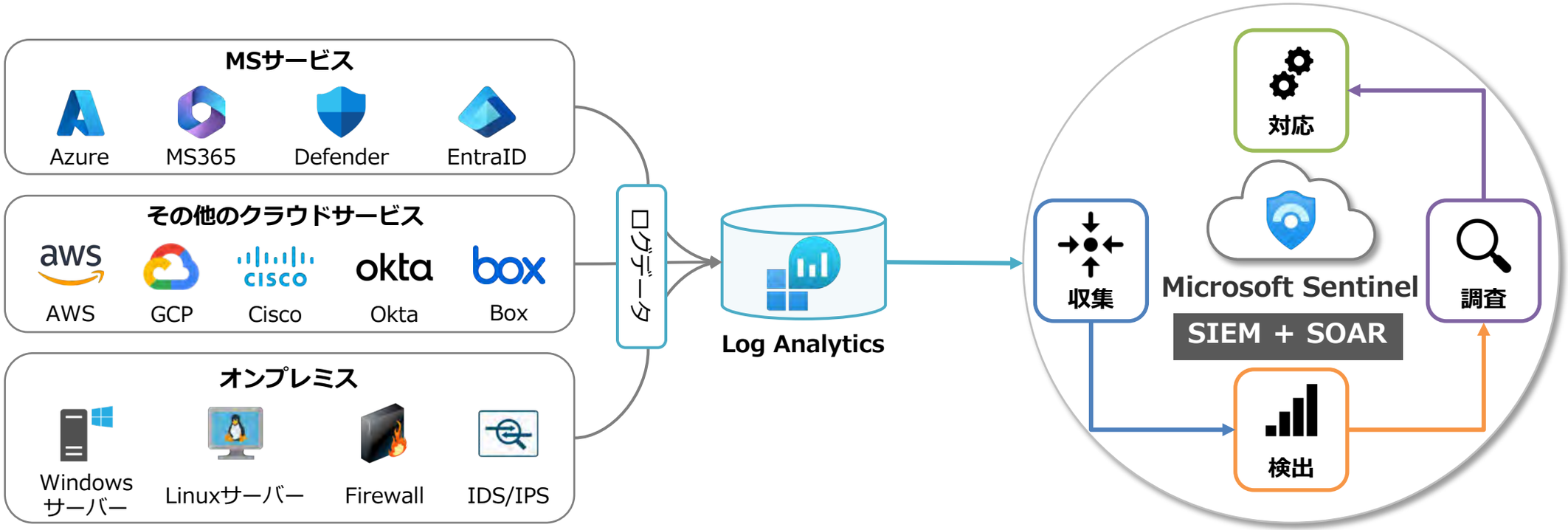
✓ SIEM および SOAR の機能を持つ統合セキュリティ管理
✓ 対象システムのログの収集から検出、調査、脅威への対応までを包括的に対応するサービス

2.2. Microsoft Sentinelとは

Microsoft Sentinelは、Microsoftが提供する統合セキュリティソリューションです。**さまざまなサービスや製品のログを一元管理し、関連性を分析**することで、企業全体のセキュリティを強化します。不審な動きを素早く**検知**し、**対応**できるため、攻撃のリスクを最小限に抑えられます。
簡単に言うと、Microsoft Sentinelはパソコンやネットワークを守る「**見張り役**」であり、**危険をいち早く見つけ、迅速に対応できるツール**です。

ポイント

- ✓ **Azure**のクラウドサービス上で動作
- ✓ 様々なデータソースからセキュリティ関連の**ログを収集し、一元管理**
- ✓ **自動で脅威を検出し、対応**を実施
- ✓ **SIEM + SOARの統合機能**で運用負荷を軽減



3. Microsoft Sentinelの基本機能

3.1. Microsoft Sentinelの基本機能

Microsoft Sentinelは、**収集・検出・調査・対応**の4つの基本機能が連携することで、企業のセキュリティ体制を強化するクラウド型SIEM/SOARソリューションです。これらの機能が一連の流れとして連携し、継続的かつ効率的なセキュリティ運用を実現します。
その結果、脅威の早期検知と迅速な対応が可能となり、組織の安全性を高めることができます。
それぞれの機能について、次のスライドから詳しく説明していきます。

収集

Microsoft製品をはじめとしたクラウドやオンプレミスのさまざまなサービスから
セキュリティ関連データを収集し、一元管理する。

検出

収集したデータをもとに、AIやルールベースの仕組みで不審な動きを自動で検出する。
脅威インテリジェンスやユーザー行動分析を活用し、精度の高い検出が可能。

調査

検出されたアラートをもとに、関連するログや情報を自動で集約し、
インシデントの全体像をわかりやすく表示する。

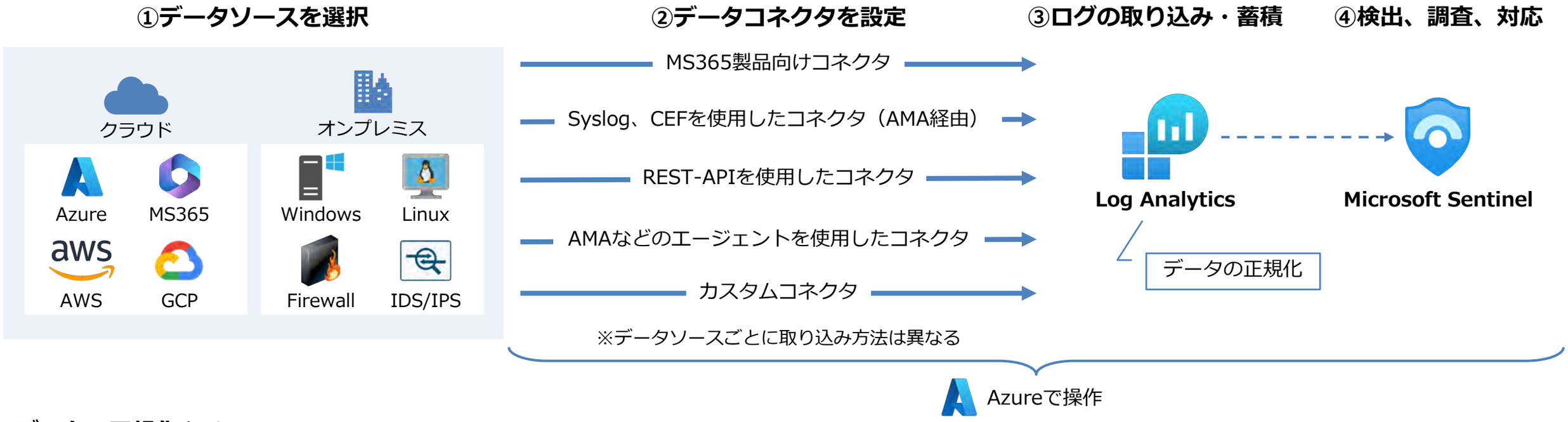
対応

調査結果に基づき、アラートへの対応を自動化する。通知の送信やアカウントの一時停止
などの対応を、あらかじめ定義した手順で自動実行できる。

3.2. 基本機能① データの収集

機能概要

クラウドとオンプレミスの様々なデータソースに対応した豊富な**データコネクタ**を提供し、セキュリティ関連ログを収集できます。
Syslog、CEF、REST-APIなど多様な方法でデータを取り込み、Sentinelと紐づけられた**Log Analyticsワークスペースに一元的に集約**します。
データソースごとに最適な収集方法が用意されており、カスタムコネクタによる拡張も可能です。



データの正規化とは

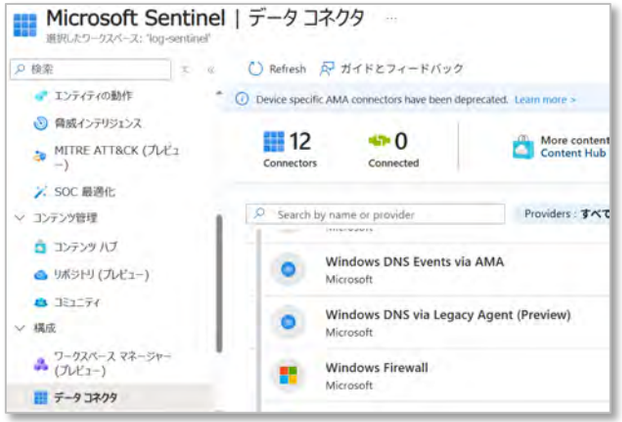
異なる形式のログデータを共通の形式に変換すること。ベンダーやシステムごとに異なるログでも、同じフォーマットで分析・検索が可能になる。
Microsoft Sentinelでは、正規化されたビューを使って統一されたクエリや分析ルールを適用できる。

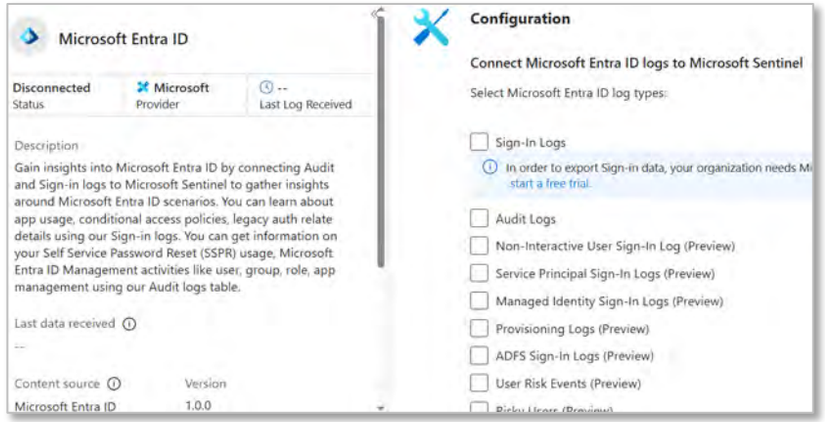
3.2. 基本機能① データの収集

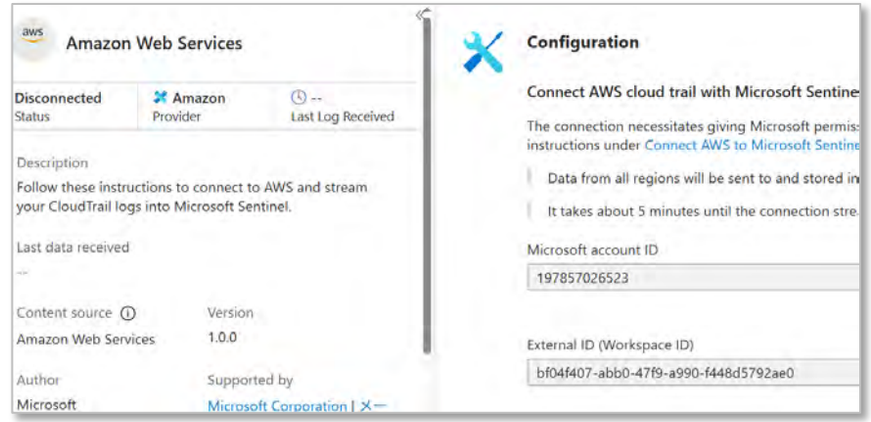
データコネクタ

様々なデータソースからデータを収集する上で重要な役割を果たすのが「**データコネクタ**」です。
Azureポータルからインストールを行い、設定手順に基づいてコネクタの構成を行います。※収集可能なデータ範囲の詳細は第6章に記載
コネクタの構成によっては通信プロトコルの設定が必要です。（例：AMAエージェントベースのデータコネクタには、ポート 443 送信を有効にする）

コネクタのタイプ	説明
Microsoft製品向けコネクタ	Microsoftが提供する標準コネクタ。Microsoft製品（Microsoft Entra ID、Microsoft Defender、Azure Activity、Azure Storage など）のデータ取り込みが簡単に出来る。
サードパーティ向けコネクタ	Microsoft以外のアプリケーション（オンプレミスを含む）（AWS、GCP、Ciscoなど）と連携できるコネクタ。 製品別にデータコネクタが用意されており、データの取り込み方法はそれぞれ異なる。 様々な取り込み方法の中でも、SyslogやCEF、REST-APIによるデータの取り込み、Azure Monitorエージェント（AMA）などを用いたエージェント経由でのデータの取り込みが可能。
カスタムコネクタ	既存の専用コネクタで対応できない場合、Azure MonitorやLogstash、Logic Appsなどを使用して、オリジナルのコネクタを作成可能。これにより、特定の要件に合わせたデータの取り込みや処理が柔軟に行える。







3.2. 基本機能① データの収集

データの保持期間

データは Log Analytics ワークスペースに保存され、保持期間はワークスペース単位、およびワークスペースのテーブル単位で設定できます。
テーブル単位の設定はデータごとに保持期間を分けたい場合に、有効的です。

・ワークスペース全体で、**最初の90日間は無料**で保持される
・ワークスペースおよびテーブル単位で、**最大730日（2年間）**まで延長可能（追加コストが発生）
・それ以上の長期保存が必要な場合は、特定のテーブルに対して**最大12年間**の保存にも対応可能（追加コストが発生）

ユースケース

例①：Microsoft 365 環境のセキュリティ監視
Microsoft 365（Exchange、SharePoint、Teams）や Entra ID から監査ログ・サインインログを収集し、情報漏洩・アカウント乗っ取りの兆候を監視。
活用されるコネクタ例
Microsoft 365 コネクタ、Microsoft Entra IDコネクタ
Microsoft Defender コネクタ

例②：クラウドサービスのログ統合（AWS、GCP など）
Azure 以外に利用している AWS や GCP などのクラウドサービスからもログを収集し、Microsoft Sentinel に統合して監視する。
活用されるコネクタ例
Amazon Web Services コネクタ
Google Cloud Platform コネクタ

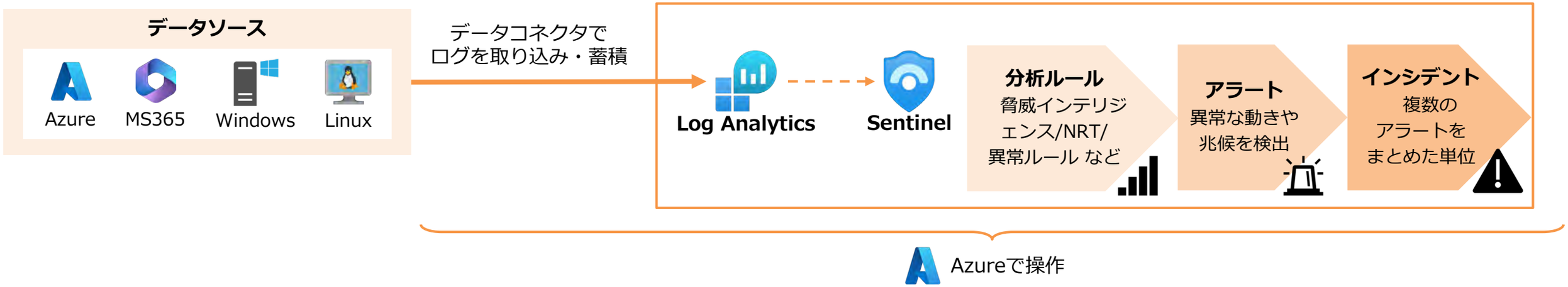
データ収集のポイント

✓ 何のデータを収集できるか？ ▶ クラウドとオンプレミスの両方から、**さまざまなシステムやサービスのログデータを収集**可能
✓ どうやって収集するか？ ▶ **コネクタ**（提供、カスタムコネクタ）を使って自動で収集
✓ どこに保存されるか？ ▶ 収集したデータは **Log Analytics ワークスペース** に保存され、Sentinel で分析・可視化される

3.3. 基本機能② 脅威の検出

機能概要

Log Analyticsへ収集したログをもとに**脅威の兆候を自動で検出**します。たとえば「短時間で多数のログイン失敗」や「国外からの異常なアクセス」など、**分析ルール**に基づいてログを継続的に監視します。検出された異常は「**アラート**」として通知され、必要に応じて複数のアラートが「**インシデント**」として自動的に集約されます。アラートのグループ化（インシデントの作成）は分析ルールの設定時に定義します。



脅威の検出は、Log Analytics に収集されたログをもとに、「**分析ルール**」によって実行されます。
各ソリューションで事前に分析ルールが用意されているため、難しい設定なしでルールをそのまま適用可能です。
分析ルールをテンプレートとして**独自のルールを作成**することもできます。次のスライドでは、分析ルールの主な種類と特徴について説明します。

3.3. 基本機能② 脅威の検出

分析ルールの種類

分析ルールは、収集したログから脅威の兆候を検出するための条件やロジックを定義した仕組みです。
各ソリューションで提供される分析ルールは、7つの種類に分類されます。

種類	説明	ルールの例
スケジュールされたルール	**定期的に実行されるログ分析ルール**で、Kusto クエリ（KQL）に基づいてログデータを評価し、**しきい値を超えた場合にアラートを生成**する。 統計的な処理を通じて異常や外れ値の検出が可能。テンプレートをそのまま使うことも、カスタマイズして新規ルールを作成することもできる。	**Microsoft Entra ID - Authentication Methods Changed for Privileged Account** **概要**： 特権アカウントの認証方法が変更された場合にアラートを出す。攻撃者が認証手段を追加し、持続的なアクセスを確保しようとする動きの検知に有効。 **実行頻度**： 2時間ごとにクエリを実行 **しきい値**： クエリの結果が1件以上ある場合にアラートを発生
準リアルタイム（NRT）ルール	**1分間隔でクエリを実行**する高速な分析ルール。可能な限り**リアルタイムに近い形で脅威を検出**することを目的としており、基本的な仕組みはスケジュールされたルールと同じだが、一部の機能に制限がある。	**Azure Activity -NRT Creation of expensive computes in Azure** **概要**：Azure 上でGPU付きや多数のvCPUを持つ高性能VMの作成を検知。これらは、攻撃者による暗号資産マイニングや防御回避のために利用される可能性がある。 **実行頻度**：1分ごと（NRTルールのため）

3.3. 基本機能② 脅威の検出

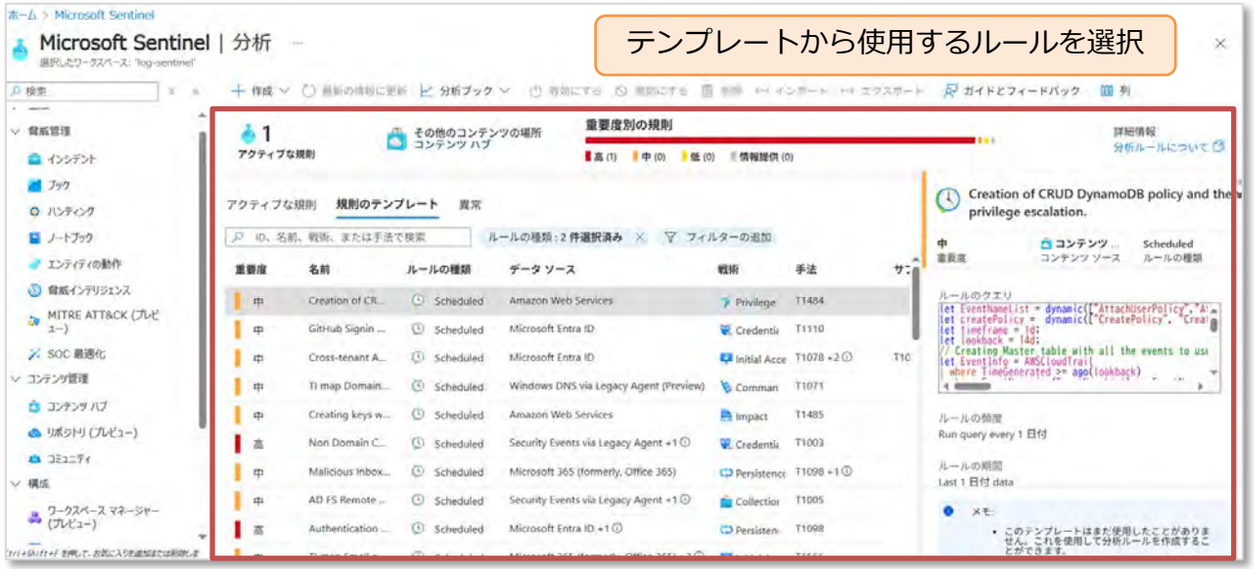
種類	説明	ルールの例
Microsoft セキュリティ規則	Microsoft Defender などの**他の Microsoft セキュリティ製品が生成したアラートを基に、Sentinel 上でリアルタイムにインシデントを自動作成する**ためのルール。 通常のスケジュール型やNRTルールとは異なり、外部ソース由来のアラートに対して**インシデント作成を補完する**役割を持つ。	**Create incidents based on Microsoft Entra ID Protection alerts** **概要：**Microsoft Entra ID Protection で生成されたすべてのアラートに基づいてインシデントを作成する。
脅威インテリジェンス	Microsoft が提供する信頼性の高い**脅威インテリジェンス（IP・ドメイン・URL など）と、組織内のログを自動で照合**して、高精度なアラートやインシデントを生成する仕組み。	**Microsoft Defender Threat Intelligence Analytics** **概要：**データソース（Syslog、Microsoft 365、Azure Activity、Windows DNS、Windows Firewall）から収集した**イベントログを脅威インテリジェンスと照らし合わせ、一致する情報があった場合**にアラートを生成する。 このルールは自動運用され、カスタマイズは不可。
異常ルール	機械学習を活用して、**ユーザーやシステムの通常行動（ベースライン）**を学習し、それから**大きく逸脱する動きを「異常」としてフラグ付け**するルール。 **UEBA**（User and Entity Behavior Analytics）を使用して、接続されたデータソースからログを分析し、ユーザーやエンティティ（ホスト、IP、アプリケーションなど）から**行動パターンのベースライン**を設定。 ベースラインと、**場所・時間・頻度・組織のアクティビティなどを比較して、異常を特定**する。 検出された異常はアラートとしては直接生成されず、「異常テーブル」に記録され、後の調査や脅威分析に活用される。	**Microsoft Entra ID - UEBA Anomalous Failed Sign-in** **概要：**システムや環境内で正当な資格情報を知らない攻撃者が、パスワードを推測してアカウントにアクセスしようとする試みを、UEBAを用いて検出する。 Entra IDのサインイン・監査ログ、Azureサインイン、Windowsセキュリティログなどがデータソースとして使用される。

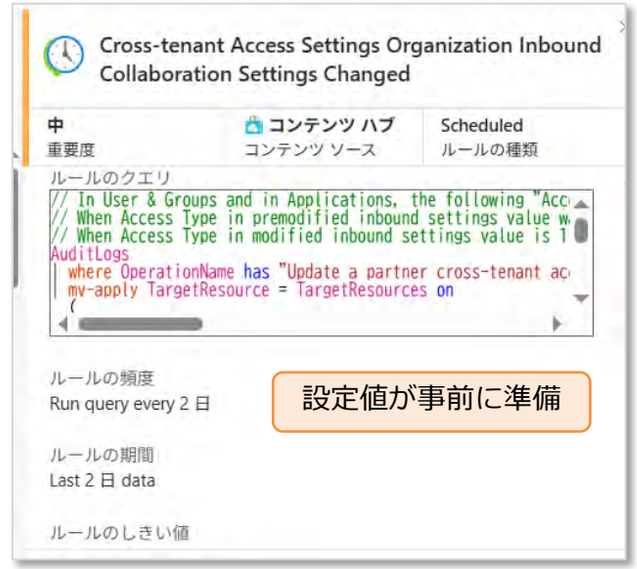
3.3. 基本機能② 脅威の検出

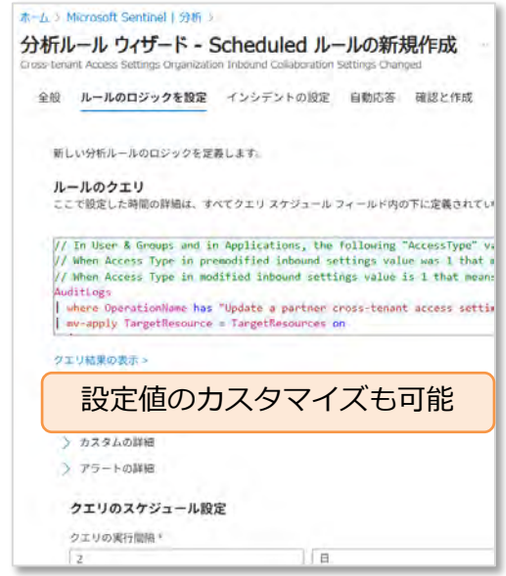
種類	説明	ルールの例
高度なマルチステージ攻撃の検出 (Fusion)	**複数のセキュリティ製品からの低忠実度なアラート**（信頼性が低く、誤検知の可能性が高い）**を機械学習で相関分析し、高忠実度**（信頼性が高く、実際の脅威である可能性が高い）**なインシデントに自動集約**することで、**高度なマルチステージ攻撃を検出**する。 Fusionエンジンによる自動処理で、ロジックは非公開かつカスタマイズ不可。 複数のアラートを相関分析することで、**従来の手法では見逃されがちな複雑な攻撃**を検出し、**少量、高忠実度、高重大度のインシデント**を生成することが可能。	**Advanced Multistage Attack Detection** **概要：**Microsoft Sentinelで既定で有効になる。 例として以下のデータソースからのアラートを分析することが可能。 ・Microsoft Entra ID Protection ・Microsoft Defender for Cloud ・Microsoft Defender for Cloud Apps ・Microsoft Defender for Endpoint ・Microsoft Defender for Identity ・Microsoft Defender for Office 365
機械学習による (ML) 行動分析	Microsoft 独自の機械学習モデルを用いて、**SSH や RDP ログインにおける異常な行動を検出**し、高忠実度なアラートとインシデントを自動生成するルール。 現在はプレビュー段階でカスタマイズ不可。IP アドレス、地理情報、ユーザー履歴などの要素をもとに検知を行う。	**Windows Security Events - (Preview) Anomalous RDP Login Detections** **概要**：異常なRDPログイン活動を検出するルール。 以下のシナリオで異常を識別する。 異常なIP：過去30日間で見かけなかった、または非常に稀に見かけたIPアドレス。 異常な地域：IPアドレス、都市、国などが過去30日間で見かけなかった、または稀に見かけた。 新規ユーザー：新しいユーザーが、過去30日間で見かけなかったIPアドレスや位置情報からログイン。

3.3. 基本機能② 脅威の検出

実際の画面





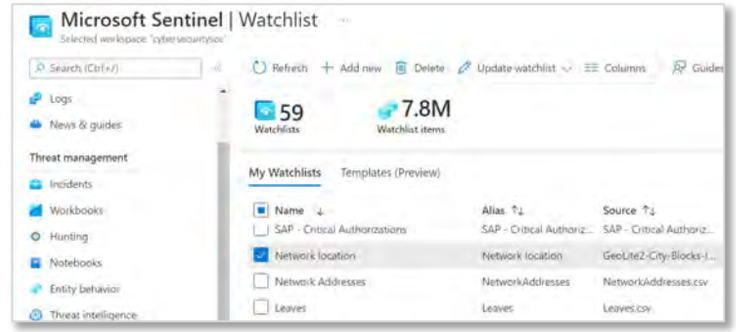


その他の機能

分析ルールに加えて、MITRE ATT&CK による可視化やウォッチリストなど、**検出体制を強化・補完する複数の機能**を利用することが可能です。

①ウォッチリストの活用

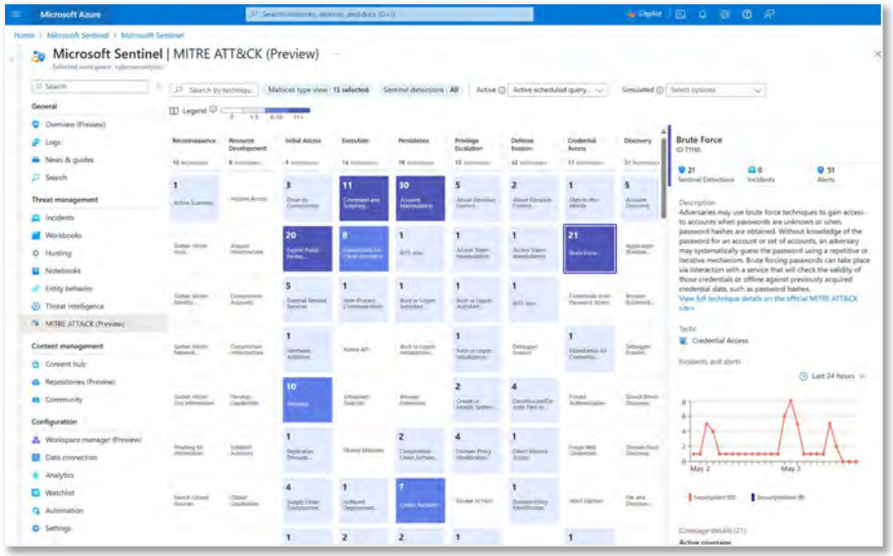
監視対象リスト（重要資産、退職者アカウント、サービスアカウントなど）を作成し、
ログと照合することで**特定対象の行動を重点的に追跡**可能です。
例）退職者アカウントのリストから、許可リストとブロックリストを作成し、
　　特定のユーザーのネットワークログインを検出・防止する
後続の、検索や脅威ハンティング、プレイブックでも使用することが可能です。



3.3. 基本機能② 脅威の検出

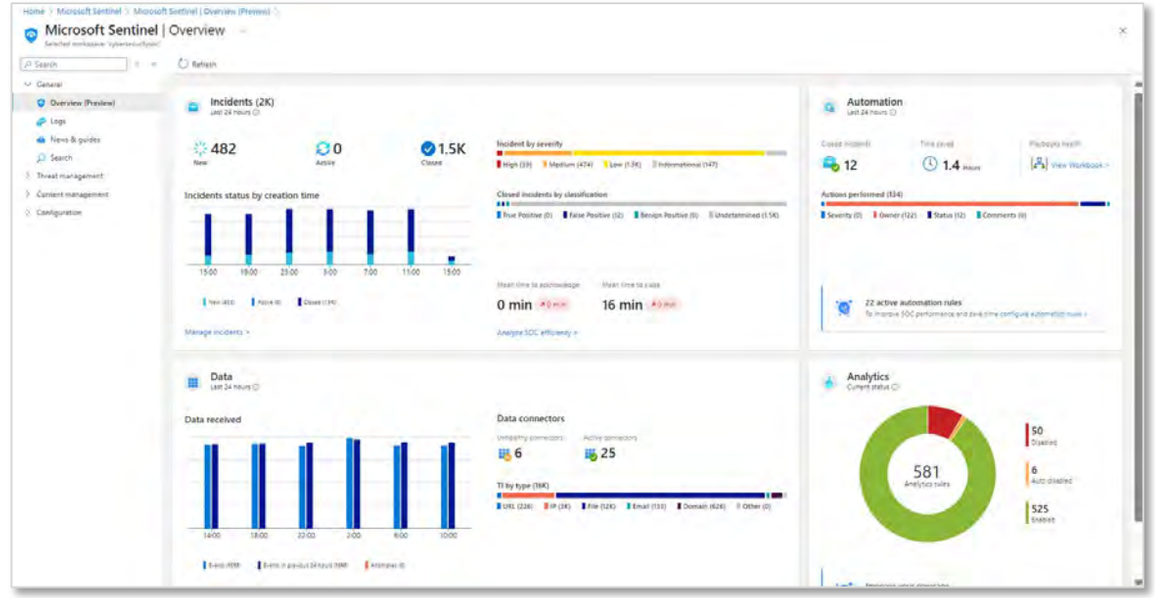
②MITRE ATT&CK カバレッジの視覚化

MITRE ATT&CK フレームワークに基づいて、組織のセキュリティ状態の性質と範囲を視覚化します。現在アクティブな分析ルールと構成可能な検出を確認したり、未構成の検出を含めた場合のセキュリティ状態をシュミレートすることが可能です。



③Workbooks による視覚化

分析ルールの正常性や接続したデータソースの各分析情報を、ダッシュボード形式で視覚化します。組み込みテンプレートの利用、または独自のカスタムブックの作成が可能です。



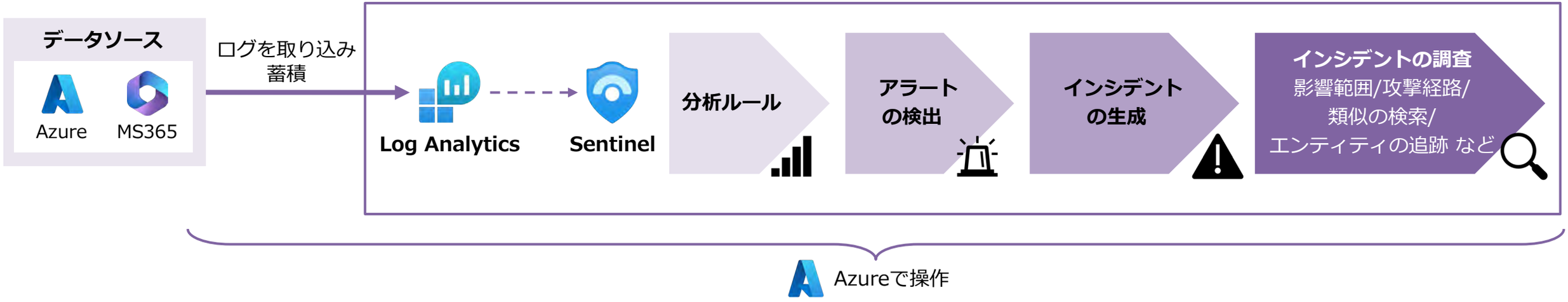
脅威検出のポイント

- ✓ 何を検出できるのか？ ▶ ユーザーやシステムの不審な動き、データ漏洩の兆候など、**セキュリティリスク**となる脅威を検出
- ✓ どうやって検出するのか？ ▶ ソリューション対応の**分析ルール**で、ルールベースや異常検知など複数の手法で脅威を検出
- ✓ 検出後はどうなる？ ▶ 検出された脅威は**アラート**として通知され、重要度に応じて**インシデント化**される

3.4. 基本機能③ 調査

機能概要

検出されたアラートは、Microsoft Sentinel によって自動的に「**インシデント**」としてグループ化されます。
アラートのグループ化（インシデントの作成）は分析ルールの設定時に定義します。
インシデントを起点に、関連するログデータを調査し、**ユーザー、IPアドレス、デバイスなどの関係性を時系列で確認しながら、攻撃の流れや原因、影響範囲を特定**します。
生成されたインシデントは、それぞれ影響があるか分析して判断する必要があります。影響が大きい場合、適切な対処を行うことが必要となります。



Microsoft Sentinelでは、セキュリティインシデントの調査に必要な機能がAzure portalに用意されています。
次のスライドから、詳細かつ迅速で効果的な調査を可能にする機能について説明します。

3.4. 基本機能③ 調査

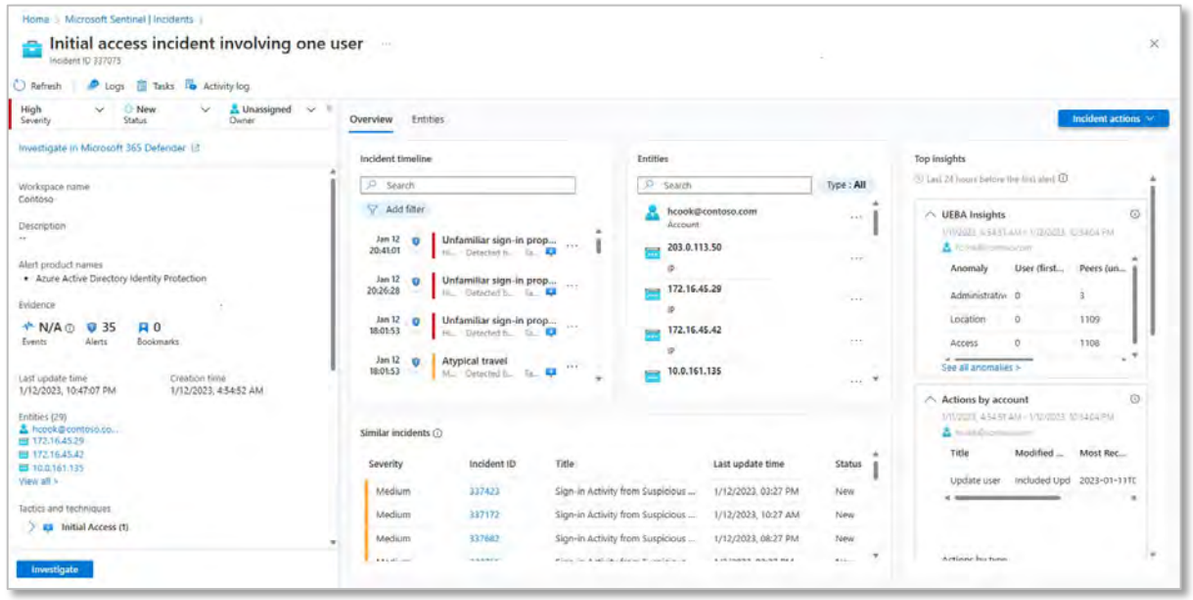
調査方法

Microsoft Sentinel は、発見された脅威をもとに関連情報をまとめて見やすく整理し、調査や対応をスムーズに進めるための仕組みを提供します。

①インシデント詳細ページ

生成された**インシデントの全体像を確認**できます。

・インシデント内のアラートの**タイムライン**が表示。
　発生順序を把握したり、個々のアラートの確認や削除も可能。
・環境内で発生している**類似のインシデント**が表示。
・アラートで特定された**エンティティ（ユーザー、デバイス、アドレス、ファイルなど）**が表示。



②調査グラフ

アラートとエンティティの関係を視覚的に表現することが可能です。
可視化することで、セキュリティ管理者は**脅威の全体像や追加の調査する範囲を判断**することが容易になり、迅速な判断と対処が可能になります。

・インシデントに関連する**エンティティの関係を視覚的**に表示。
・検索クエリを使用して調査範囲を拡大し、**攻撃の全体像や影響範囲を把握**。

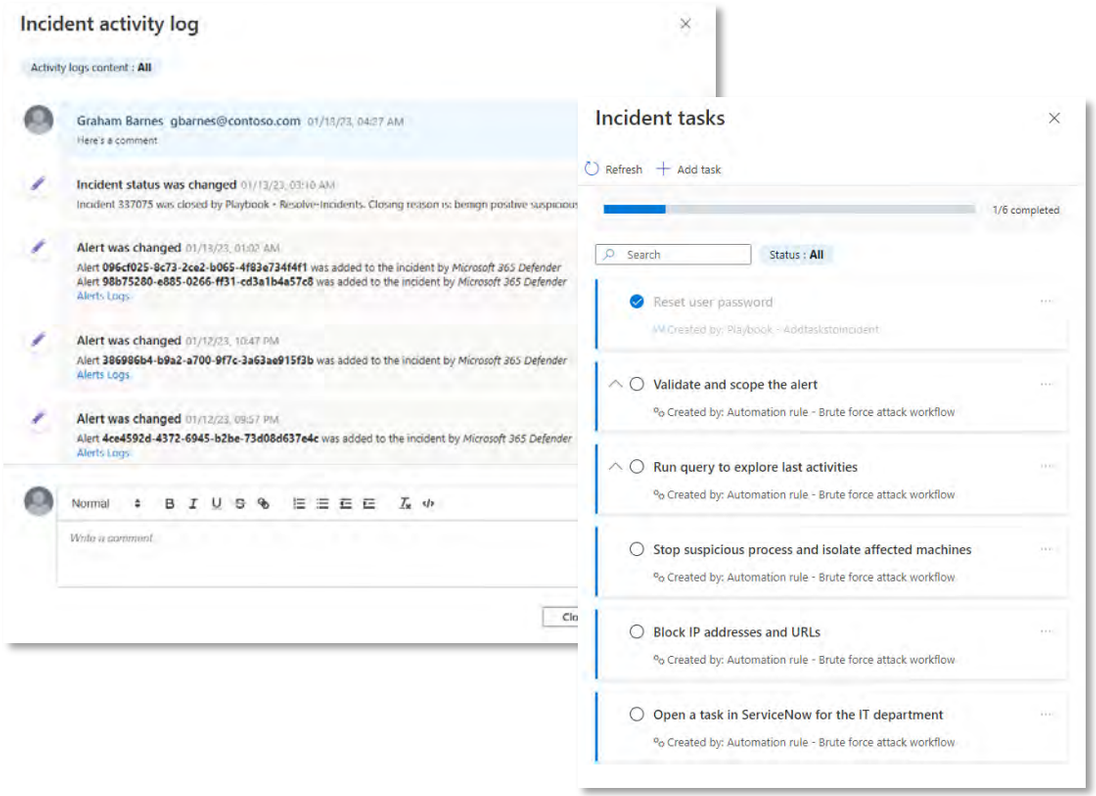
例）ユーザーに関連するアラートやログオンしている端末を検索し、
　　ユーザーが関連する不審な動きやサイバー攻撃の影響範囲を確認する。

3.4. 基本機能③ 調査

③ 調査の効率化

以下の機能を利用することでインシデント対応を効率化し、チーム全体の連携と対応品質を向上させます。

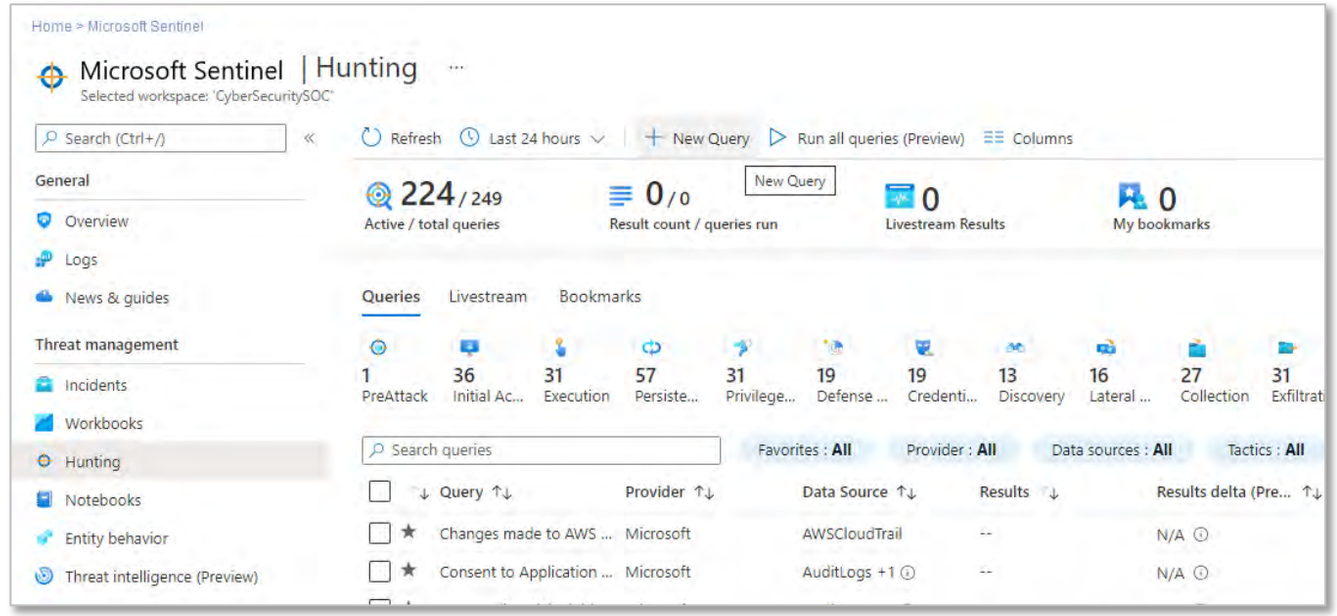
・**タスク管理機能で**対応手順を明確化し、対応の抜け漏れを防止
・**インシデントの操作履歴やコメント**を記録し、チームで共有



④脅威ハンティング

脅威ハンティングは、標準的なインシデント調査に加えて、**未検出の脅威を積極的に探し出すための機能**です。
MITRE フレームワークに基づく、クエリツールを使用することで、組織のデータソース全体に対して、セキュリティ脅威を**予防的に捜索**できます。

担当者はあらかじめ定義されたハンティングクエリ、または独自のハンティングクエリを実行して、潜在的な脅威を調査します。



3.4. 基本機能③ 調査

⑤Jupyter ノートブック

ノートブックは、標準的なインシデント調査に加えて、**ログデータを柔軟に分析・可視化できるツール**として活用されます。
よく使われるシナリオに対応した**テンプレートも複数用意**されており、複雑なコードをゼロから書かなくても、すぐに高度な分析を始められます。

・Sentinelの通常機能では提供されない、機械学習などの高度な分析をPythonで実行
・Sentinelの通常機能では提供されない、カスタムタイムラインやプロセスツリーによるデータの可視化の作成

※利用にはAzure Machine Learning ワークスペースが必要です。

ユースケース

例①：フィッシング攻撃の影響調査

Sentinelが不審なメール経由でのマルウェア感染を検出。
調査グラフを使い、感染した端末が社内ネットワークにどのような影響を与えたかを分析。
過去のログを検索し、同様の手口での攻撃がなかったかをチェックする。

例②社内ユーザーの不審なログインの調査

海外から短時間に複数の地域でログインがあったユーザーを検知。
関連するIPアドレスや端末情報を調査し、不正アクセスの有無を確認。

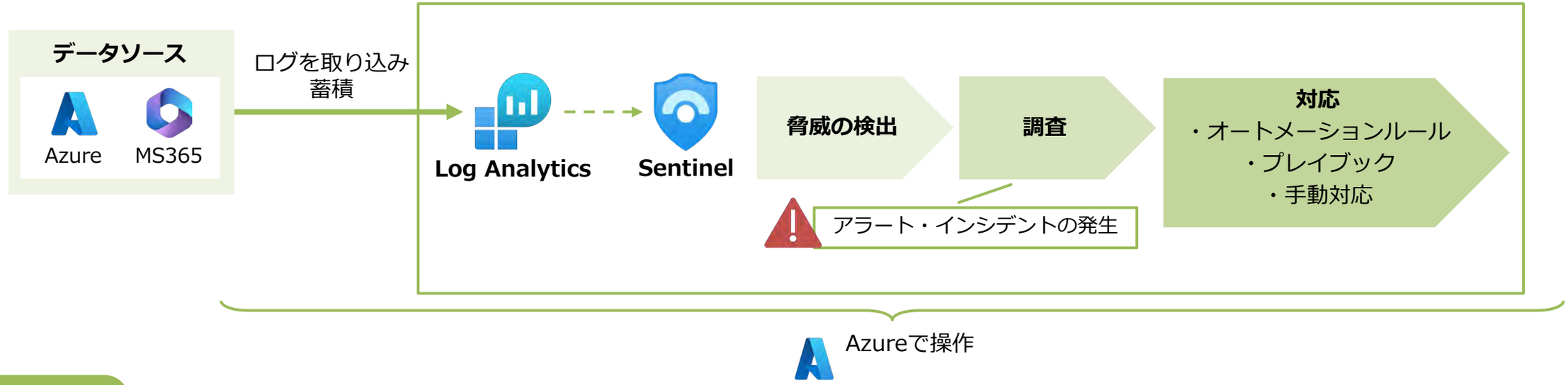
調査のポイント

✓ 何を調査できるのか？	▶ **インシデント**とそれに関連する**アラート**、**エンティティ**（ユーザー、IP など）、影響範囲など
✓ どうやって調査するのか？	▶ インシデント詳細ページ、調査グラフ、脅威ハンティングなどを使用
✓ 調査後はどうする？	▶ インシデント対応、アクションの自動化、再発防止策の実施

3.5. 基本機能④ 対応

機能概要

調査によって脅威の内容や影響範囲が明らかになった後は、速やかに**対応**を行うことが重要です。
Microsoft Sentinel では、**オートメーションルールとプレイブック（自動フロー）を活用**して、ユーザーの隔離や通知、外部ツールとの連携といった対応作業を自動化できます。これにより、対応のスピードと精度が向上し、変化する脅威にも柔軟かつスケーラブルに対処できます。



手動対応

セキュリティ担当者がインシデントを確認し、適切な対策を手動で実施する、手動対応も可能です。
　例：不正アクセスがあったアカウントを即時にロック
手動対応を行った場合、**柔軟性が高く、詳細な調査**を可能にしますが、**時間とコスト**がかかり、**人為的なミスのリスク**があります。
次スライドから、自動対応の仕組みを説明しますが、**状況に応じて手動と自動を使い分ける**ことが重要です。

3.5. 基本機能④ 対応

自動対応（SOAR）

特定のアラートやインシデント発生時に、「**オートメーションルール**」と「**プレイブック**」によって**定義した処理を自動実行**することで、攻撃によって影響を受ける端末の隔離、悪意のあるトラフィックのブロックなどを自動で行うことが可能となり、企業のデータ資産やシステムを脅威から保護します。

機能	概要
オートメーションルール	**インシデントやアラート発生時の対応を自動化する仕組み**で、あらかじめ設定した条件に応じて**プレイブックなどを自動実行**する。 **トリガー・条件・アクション**の流れで「**いつ・どんなときに・何をするか**」を定める、司令塔のような役割を担う。
プレイブック	**インシデントやアラートへの対応アクションを自動で実行する**仕組み。 **Azure Logic Apps** を利用して**ワークフロー**を構築し、メール通知や隔離、外部システム連携などのアクションを、事前に用意されたテンプレートやカスタムフローで自動化できる。 プレイブックは**オートメーションルールによってトリガー**され、実行される。

メリット

- インシデント発生時に**即座に対応**できるため、被害の拡大を防止
- 事前定義されたルールに基づく対応で、**一貫性**のあるセキュリティ対策を実現
- 手動対応に比べて**時間と労力を大幅に削減**し、セキュリティチームの負担を軽減

注意点

- **不必要なアクション**を防ぐため、ルールや条件の精度が重要
- 複雑なインシデントには**手動対応が必要な場合**がある
- 初期導入には**詳細な設定やカスタマイズ**が必要
- **継続的な監視と設定の見直し**が不可欠

3.5. 基本機能④ 対応

Azure Logic Apps とは

Azure Logic Appsは、Microsoft Sentinelのプレイブックを構築するための強力なツールです。

■ワークフローの自動化

インシデントやアラートに対する対応アクションを自動化し、迅速な対応を実現します。

■条件分岐とアクション設定

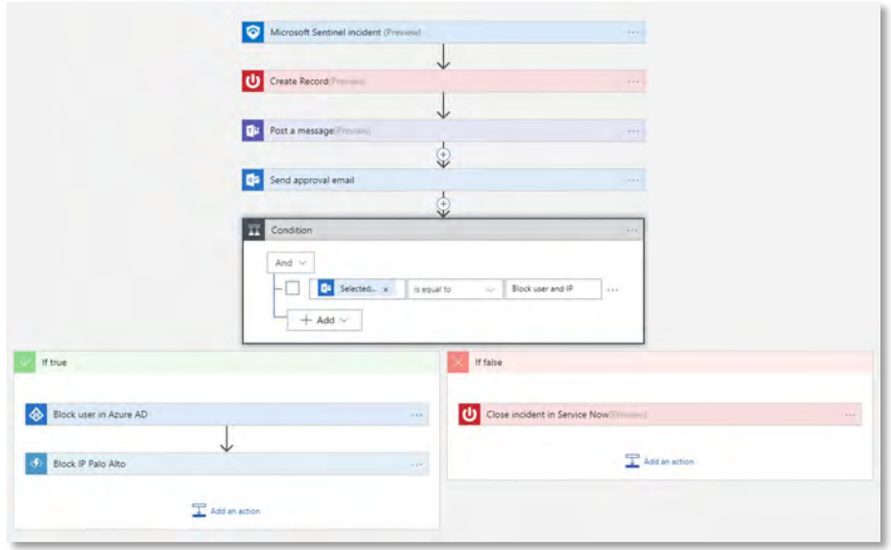
複雑な条件分岐や多様なアクションを設定でき、柔軟な対応が可能です。

■コネクタの利用

様々なシステムやサービスと連携するためのコネクタを使用し、メール通知、
ユーザーの無効化、外部システムとの連携などを実行します。

■テンプレートの活用

事前に用意されたテンプレートを利用して、簡単にプレイブックを作成できます。



自動対応のユースケース

分析ルール（Entra IDにおける、不審なサインインとMFA設定の変更）で高重要度インシデントが発生した際に、Entra IDのユーザーを無効化し、マネージャーに通知するフローを実行します。

※MFA…多要素認証

※プレイブックの実際の設定では詳細なフローが必要です。

オートメーションルール
トリガー：インシデントの作成
条件：
①分析ルール「Suspicious Sign In Followed by MFA Modification」（Entra ID）
②重要度「高」
アクション：プレイブックAを実行

プレイブックA

トリガー：インシデント
↓
EntraID：ユーザー情報を取得
↓
EntraID：ユーザー無効化
↓
Outlook：マネージャーに通知

3.5. 基本機能④ 対応

よく利用される自動対応

Azure Logic Appsで用意された様々なコネクタを用いて、様々なシステムやサービスと連携したフローを構築することが可能です。
※利用可能なコネクタは公式ページを参照ください。

カテゴリ	自動対応	内容
通知	Teams通知、メール送信、ServiceNowチケット作成	インシデント発生時に即時アラート通知やチケット登録を行う
ユーザー制御	Entra IDアカウントの無効化／パスワードリセット	不審なユーザー操作が検出された際の迅速なアカウント制御
ネットワーク制御	Firewallルールの変更、IPブロック	攻撃元のIPアドレスを即時遮断して被害拡大を防止
端末操作	Microsoft Defenderで端末の隔離	感染の疑いがある端末をネットワークから隔離する
ログ・分析	特定ユーザーのログを収集、KQL検索の自動実行	調査の一環として自動でログを収集・分析
チケット連携	ServiceNow、Jiraなどの自動チケット登録	インシデント管理システムと連携して記録・通知を自動化
ファイル送信・記録	アラート情報をSharePointやBlobに保存	調査・監査用にアラート情報を自動保存する
外部システム連携	任意のAPI連携（HTTP Webhook）	社内システムやクラウドサービスと柔軟に連携可能

対応のポイント

- ✓ どのように対応するのか？ ▶ **オートメーションルール**で条件を定義し、**プレイブック**を使用して自動フローを実行
- ✓ 何ができるのか？ ▶ 通知、アカウント制御、端末隔離、IPブロック、ログ取得、外部連携など多様な対処が可能
- ✓ 自動化のメリットは？ ▶ 対応の迅速化・標準化・漏れ防止が実現し、セキュリティチームの負担を大幅に軽減

4. 導入メリットとポイント

4.1. 導入メリット

Microsoft Sentinel の導入により、企業が得られるメリットについて説明します。

AI分析と脅威情報を活用し、高精度な脅威検知を実現

従来は担当者の経験に依存しがちだが、Sentinelの場合は**リアルタイムでセキュリティイベントを分析し、即座に対応**することで被害を最小限に抑える。

データの一元管理による業務効率化

複数のクラウドサービスやオンプレミスのデータを統合管理出来るため、各サービスごとの個別対策が不要。**アクセス制御の統一**により、不要なIPアドレスやポートの解放を削減し、セキュリティ強化につながる。

オペレーションミスの削減

インシデント対応の自動化ができるため、セキュリティ担当者のオペレーションミスによる攻撃の被害拡大を防げる。

セキュリティ運用の負担軽減

SOAR機能の活用で、定型業務を自動化し、人的負担を削減。高度な知識を持つ人材が少人数でも、効果的にセキュリティ運用が可能。

4.2. 導入時の注意点とポイント

Microsoft Sentinelを導入する際の注意点やポイントを説明します。

データ収集の考慮

オンプレミスでは**エージェント導入が必要**となり、不要なログ収集は**コスト増や運用負荷**につながる。まず**重要なログから収集を開始し、段階的に範囲を拡大**していく。

コスト管理の工夫

データ量や保持期間に応じて課金されるため、高額請求リスクに注意が必要。**不要なデータの除外や、保持期間の短縮**でコストを抑える。

アラート管理

優先度の低いアラートを除外し、**重要なアラートに集中**する。アラートが多すぎると**対応漏れのリスク**が高まるため、ルールやしきい値を適切に調整し、ノイズや誤検知を防ぐ。

ネットワーク接続の確保

オンプレミス接続時は、VPNやExpressRouteで安全・安定した通信を確保し、**ログ送信によるネットワーク負荷にも注意**する。**送信タイミングや量の調整**で帯域逼迫を防ぐ。

事業継続・災害復旧（BCDR）対策

地域障害に備え、**2つのLog Analyticsワークスペースを適切なリージョンに配置**することが重要。バックアップワークスペースでは、**ビジネス継続に不可欠なデータソースや分析ルールを中心に構成**し、一貫性を保ちながら運用する。
これにより、ダウンタイムやデータ損失が発生することなく、継続的にビジネスを運用できる。

ポイント

Microsoft Sentinelを効果的に活用するためには、**監視対象のログや自動化したいプロセスを事前に明確に定義**し、その後、組織のニーズに合わせて設定を調整していくことが重要です。

5. シナリオ別の活用方法

5.1. シナリオ別の活用方法

本章では、Microsoft Sentinel の活用イメージを持っていただくことを目的に、代表的な3つのシナリオをご紹介します。

No.	シナリオ	重視するポイント
1	社内ITインフラの脅威検出と自動対応	企業内のPC・サーバ・ネットワーク機器など、オンプレミス環境を含む社内ITインフラ全体のセキュリティ監視を行う
2	複数クラウド環境の統合監視	Azure・AWS・Microsoft 365など、複数のクラウドサービスを横断的に監視する
3	分散組織における自立性と統制の両立	グループ会社や子会社など、複数のEntra IDテナント（Azureテナント）にまたがる分散環境でも、本社が一定のセキュリティ統制を維持する

5.2. シナリオ① 社内ITインフラの脅威検出と自動対応

概要

企業内のPC・サーバ・ネットワーク機器など、**オンプレミス環境を含む社内ITインフラ全体のセキュリティ監視**を行う。

要件

・Active Directory（AD）やWindows Serverを中心とした環境
・Defender for Endpoint でエンドポイントのセキュリティ対策を実施
・インシデント対応の自動化（隔離・通知）
・VPN利用者の不審な挙動も検知したい

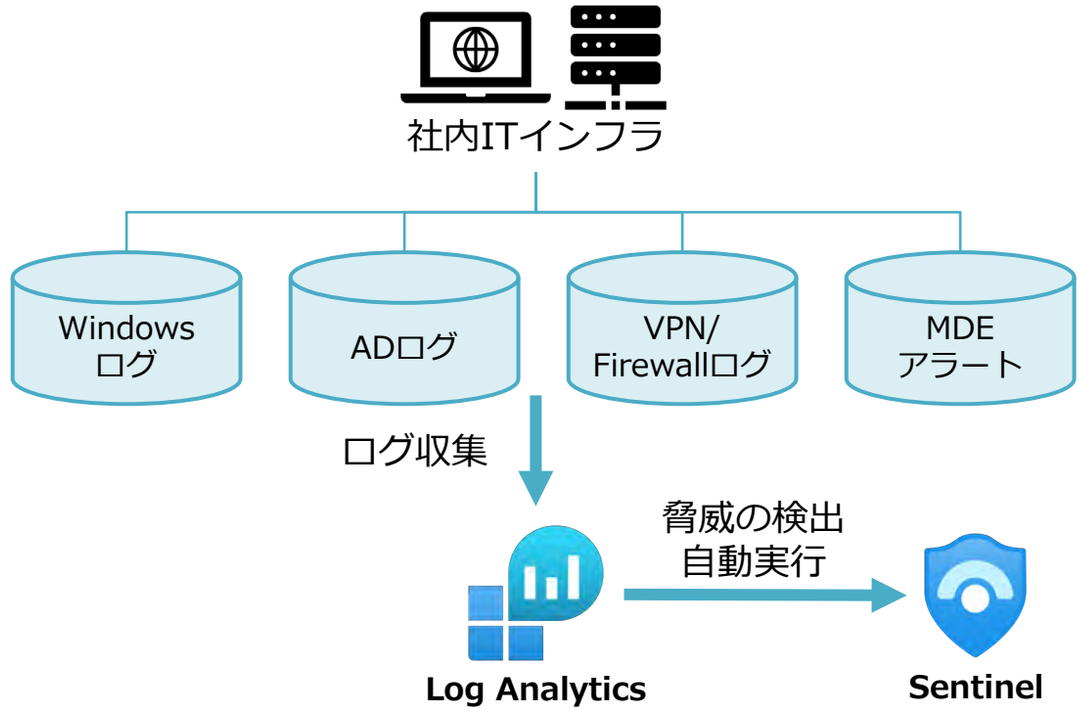
構成

■収集データ

・Windows セキュリティイベントログ
・Active Directory セキュリティイベントログ
・VPNやFirewallのログ
・Defender for Endpoint のアラート

■ワークスペース設計

1つのLog Analytics ワークスペース + Sentinelを使用（集中管理型）



活用方法

・Active Directoryで**ログオン失敗が連続**して発生 ⇒ ブルートフォース攻撃の兆候を検出し、**アラートを発生**
・**VPN経由での異常な通信**を検出 ⇒ アラートを発生させ、感染の可能性がある**エンドポイントを自動的に隔離**
・**MDEで不審なIP通信**を検出し、インシデントとして集約 ⇒ IPがMDEにおいて**ブロック対象として自動登録**される（最大90日）

5.3. シナリオ② 複数クラウド環境の統合監視

概要

Azure・AWS・Microsoft 365など、**複数のクラウドサービスを横断的に監視**し、クラウド特有のリスクを可視化する。

要件

・クラウドごとにバラバラな**セキュリティログを集約**したい
・リソース変更や不審な操作の検知
・コンプライアンス監査のためのログ保持

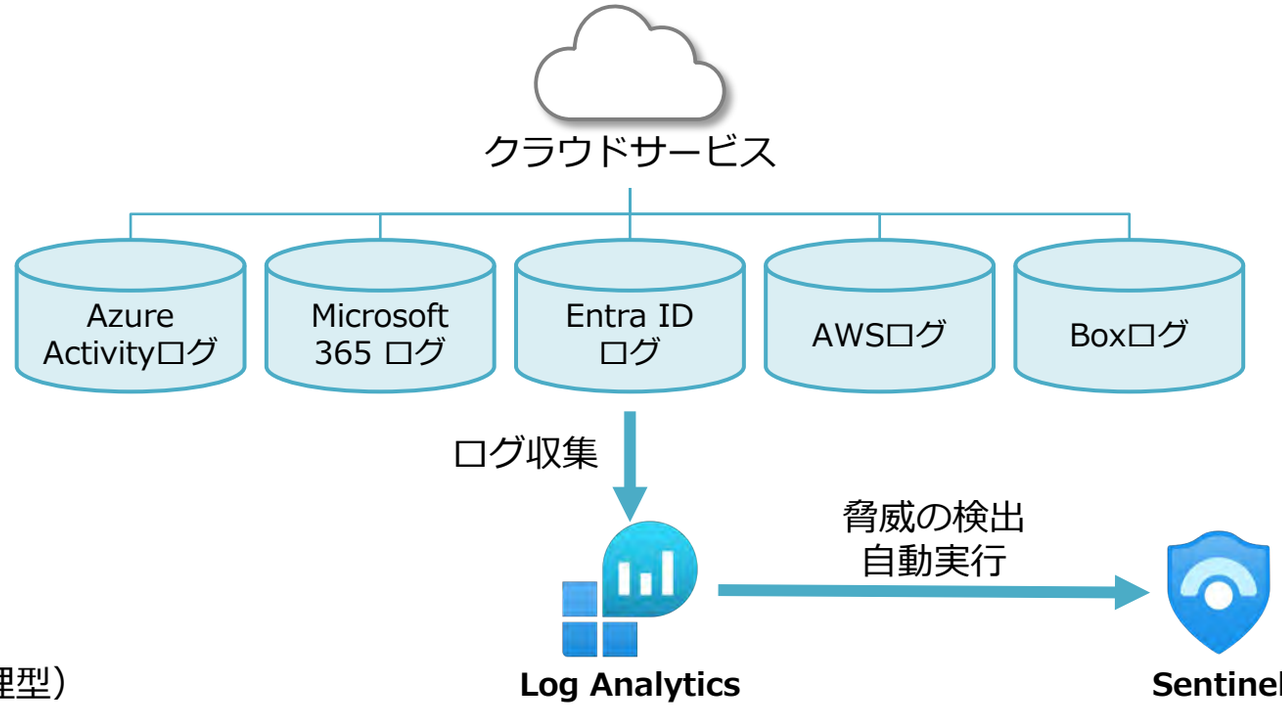
構成

■収集データ

・Azure Activity ログ
・Microsoft 365 アクティビティログ
・Microsoft Entra ID ログ
・AWS CloudTrail、GuardDutyのログ
・Boxログ

■ワークスペース設計

1つのLog Analytics ワークスペース + Sentinelを使用（集中管理型）



活用方法

・Azureで**異常な数のVM作成やデプロイ活動が発生** ⇒ 攻撃者によるクラウドインフラの破壊の兆候を検出し、**アラートを発生**
・Entra IDのサインインログをもとに、**不審な場所からのアクセスを自動でアラート化** ⇒ 該当ユーザーを**自動的に無効化**し、マネージャーに**通知**
・AWSのログデータで**重要度「高」のインシデントが発生** ⇒ インシデント内容が記載された**ServiceNowのチケットを自動作成**して管理

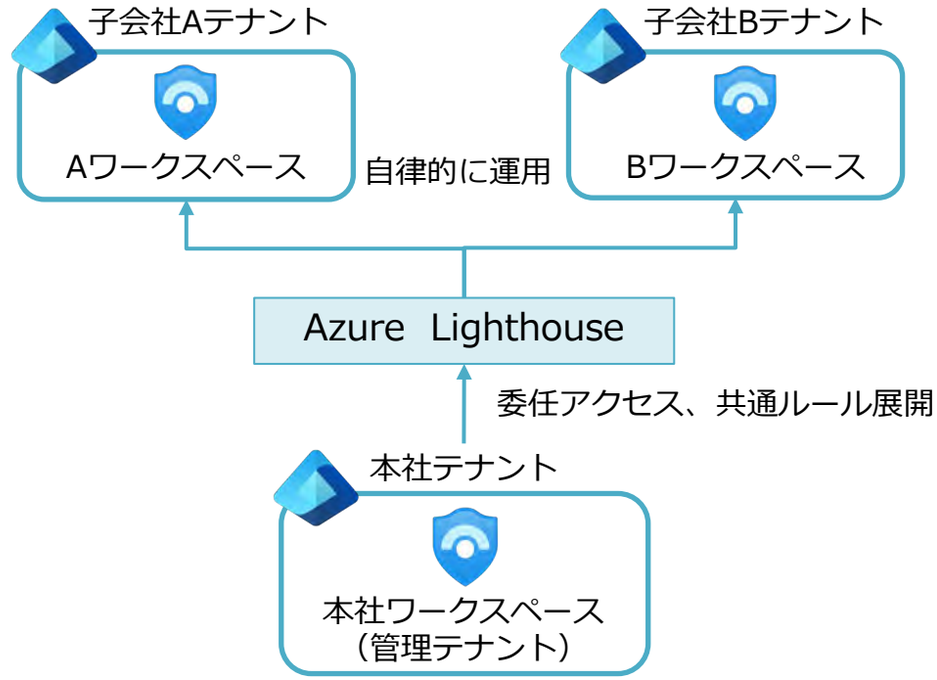
5.4. シナリオ③ グループ会社を含む分散組織でのセキュリティ統制

概要

グループ会社や海外拠点など、**複数のEntra IDテナント（Azureテナント）にまたがる分散環境でも、本社が一定のセキュリティ統制を維持**する。

要件

・本社、子会社が別々の Entra ID テナントを利用
・各テナントにそれぞれ独立した Sentinel ワークスペースを構築
・各テナント、子会社が自律的に運用しつつ、本社が共通ルールを展開したい
・すべてのログは集約せず、必要な情報のみで全体統制を行いたい



構成

■収集するデータ
・各部門が管理するサーバ・クラウド環境のログ
■ワークスペース設計
・子会社ごとに別のAzureテナントでSentinelワークスペースを作成
・本社は統制用のSentinelワークスペースを作成
■補足構成
Azure Lighthouseを用いて、管理テナントに子会社テナントの**リソース管理を委任**し、一元的に監視・管理を実行

活用方法

・子会社側のインシデント検出ルールを**本社から配布・更新**
・本社側ではログ転送なしでも全体状況を俯瞰
・「**ログの共有はしないが、運用ルールは共有する**」という設計が可能

Azure Lighthouseとは

複数のAzureテナントやサブスクリプションを**一元管理**できるサービス。**委任されたアクセス権限**により、他テナントの環境も安全に操作・監視できる。MSPや大企業のIT部門による**多環境の効率的な管理**に最適。

6. データの収集範囲

6. データの収集範囲

Microsoft Sentinelは、クラウド（Microsoft製品やその他のクラウド製品）とオンプレミス（Windows/Linuxサーバー、ネットワーク機器、セキュリティ製品）から広範囲にわたってログを収集できます。
これにより、ハイブリッド環境全体を一元的に監視し、セキュリティインシデントの早期検出や対処が可能です。
※ここで紹介するデータは一部抜粋です。すべての対応ログは公式サイトをご参照ください。

クラウド	ソリューション・コネクタ	収集可能なログ・データ
Microsoft製品	Azure Activity	サブスクリプションレベルのイベントログ（リソース作成・変更など）
	Azure Firewall	DNSプロキシ、アプリケーションルール、ネットワークルールのログ
	Azure Network Security Groups	イベントログ、ルールカウンター（NSGが適用された回数）ログ
	Azure Key Vault	診断ログ
	Azure SQL Database	監査ログ、診断ログ
	Azure Storage	Azure Storage アカウントの診断ログ
	Microsoft Defender for Cloud	Defender for Cloudからセキュリティ アラートを取り込む
	Microsoft Defender for Cloud Apps	Defender for Cloud Appsからセキュリティアラートと検出ログを取り込む
	Microsoft Defender for Endpoint	Defender for Endpointからセキュリティアラートを取り込む
	Microsoft Defender for Identity	Defender for Identityからセキュリティアラートを取り込む
	Microsoft Defender for Office 365	Defender for Office 365からセキュリティアラートを取り込む
	Microsoft 365	Teams、Exchange、SharePointのアクティビティログ
	Microsoft Entra ID	監査、サインイン、プロビジョニング、リスクイベントのログなど
	Microsoft PowerBI	監査ログ

6. データの収集範囲

クラウド	ソリューション・コネクタ	収集可能なログ・データ
その他のクラウド製品	Amazon Web Services (AWS)	AWS CloudTrail、VPCフローログ、AWS GuardDuty、AWS CloudWatchからのログ
	Google Cloud Platform DNS	Cloud DNSクエリログ、Cloud DNS監査ログ
	Google Cloud Platform Load Balancer Logs	GCPロードバランサーのログ
	Google Cloud Platform Audit Logs	GCP監査ログ
	Google Cloud Platform Firewall Logs	ネットワークアクティビティ
	Google Cloud Platform IAM	GCP IAMログ
	Google Workspace Reports	Google Workspaceのアクティビティイベント
	Okta Single Sign-On	監査ログ、イベントログ
	Salesforce Service Cloud	イベントログ
	Cisco Umbrella	イベントログ
	Cisco Secure Endpoint	監査ログ、イベントログ
	Box	イベントログ
	Palo Alto Prisma Cloud CSPM	CSPMアラート、監査ログ

6. データの収集範囲

オンプレミス	ソリューション・コネクタ	収集可能なログ・データ
サーバー関連	Windows Security Events	セキュリティイベント
	Microsoft Active-Directory Domain Controllers Security Event Logs	ドメインコントローラのセキュリティイベントログ
	Windows Forwarded Events	Windows イベント転送(WEF)ログ
	Windows Server DNS	分析ログ、監査ログ
	Windows Firewall	Windows Firewallイベント
	Syslog/CEF	Syslog,CEF形式でログを出力できる、Linuxサーバーやセキュリティデバイス、ネットワーク機器（Firewall、プロキシサーバー、VPN装置、IDS/IPSなど）からのログ ※詳細なコネクタは公式サイト(Syslog)、公式サイト(CEF)を参照
	NXLog LinuxAudit	Linux システムからの監査ログ
	Microsoft Sysmon For Linux	プロセス作成、ネットワーク接続、その他のシステムイベント
データベース	Oracle Database Audit	監査イベント

※Azure VMなどの仮想マシンに設置されたWindowsサーバーやLinuxサーバー、ネットワーク機器からも収集可能です。