

# SC-200

補足資料

Azure Portal

Microsoft Defender for  
Cloud

Microsoft 365 Defender

Microsoft Defender for  
Endpoint

Microsoft Defender for  
Office 365

Microsoft Defender for  
Cloud Apps

Microsoft Defender for  
Identity

Microsoft Sentinel

Windows  
端末

Microsoft Defender for  
Endpoint

エンドポイントの保護

Microsoft  
ID

Microsoft Defender for  
Identity

IDの保護

Office 365

Microsoft Defender for Office  
365

E-mailの保護

Cloud App

Microsoft Defender for Cloud  
Apps

クラウドアプリの保護

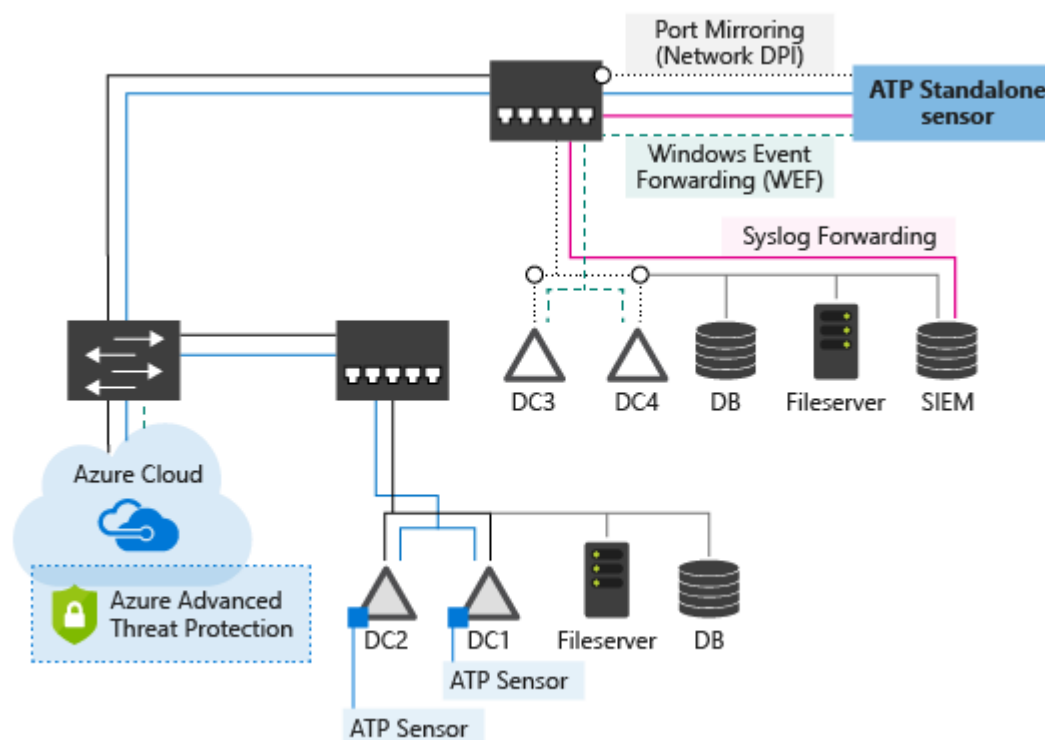
- エンドポイント上の高度な脅威を検出、調査、対応することを可能にするセキュリティ機能
- Windows Defender Advanced Threat Protection (ATP) から名称変更



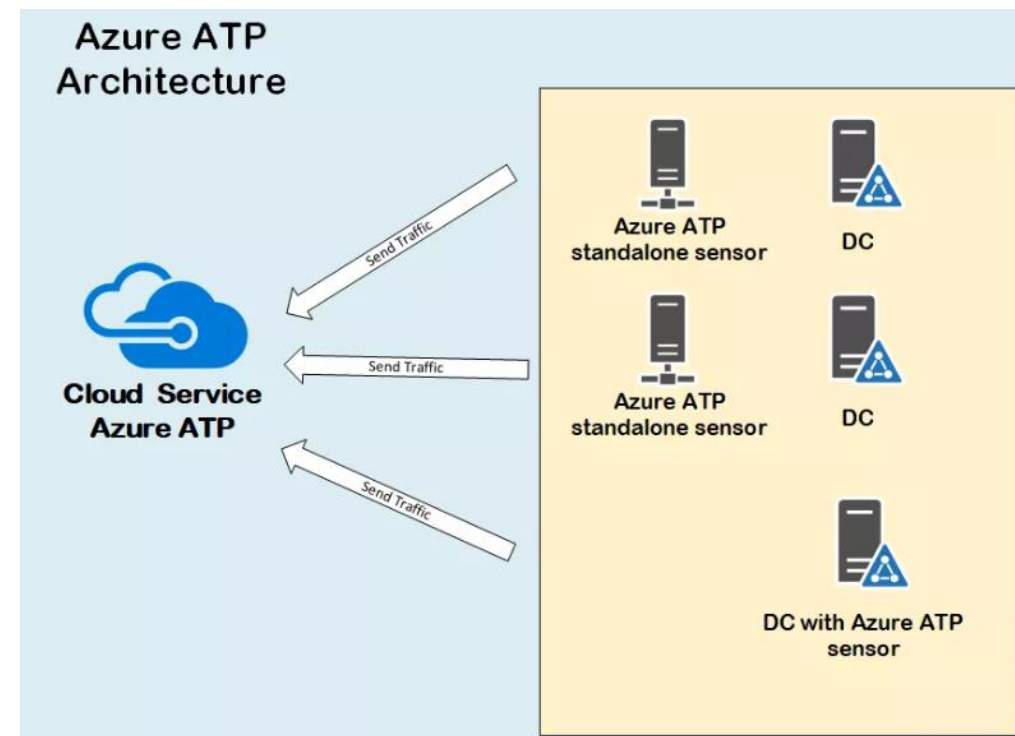
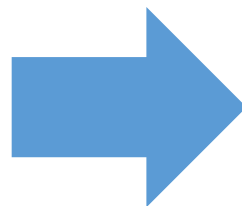
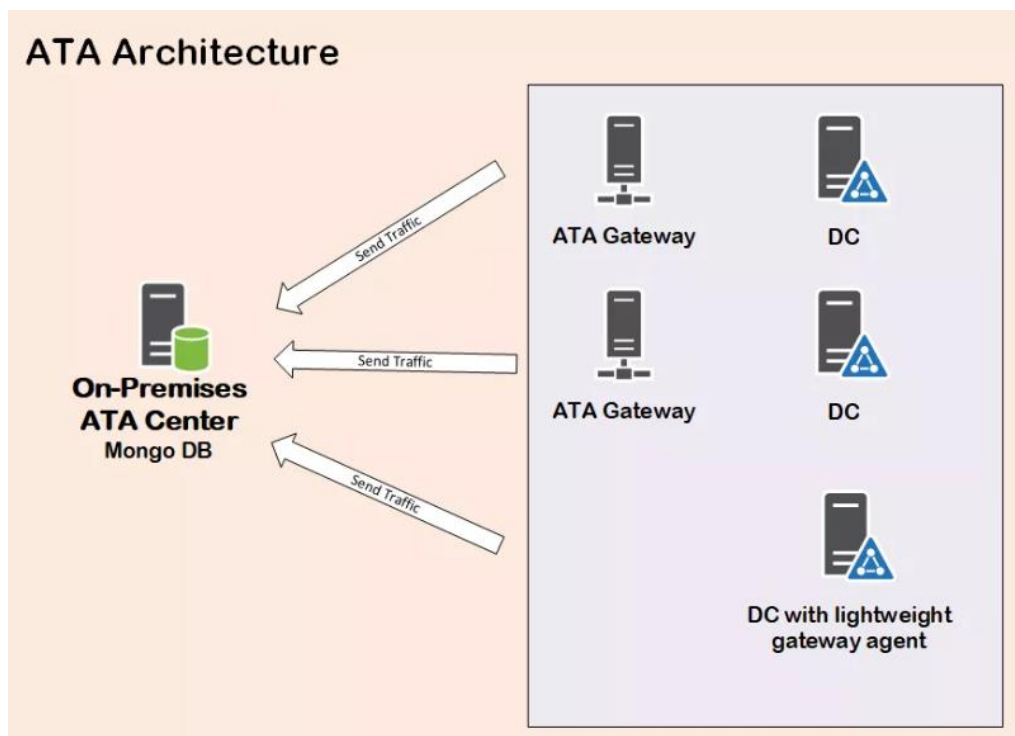
- 複数の種類の高度な対象となるサイバー攻撃や内部の脅威から、エンタープライズのハイブリッド環境を保護するためのクラウド サービス
- サイバーキルチェーンの複数のフェーズ（偵察、感染活動、目的の実行<ドメインの支配>）に重点を置いて、複数の不審なアクティビティを検出

## 悪意のある攻撃、異常な動作、セキュリティの問題とリスクの主な種類の攻撃を検出

- ✓ Pass-the-Ticket (PtT)
- ✓ Pass-the-Hash (PtH)
- ✓ Overpass-the-Hash
- ✓ 偽造 PAC (MS14 068)
- ✓ ゴールデン チケット
- ✓ 悪意のあるレプリケーション
- ✓ ディレクトリ サービス 列挙
- ✓ SMB セッション列挙
- ✓ DNS 偵察
- ✓ 水平ブルートフォース
- ✓ 垂直ブルートフォース
- ✓ スケルトン キー
- ✓ 不自然なプロトコル
- ✓ 暗号化のダウングレード
- ✓ リモート実行
- ✓ 悪意のあるサービスの作成



- Microsoftの高度な脅威分析（ATAとも呼ばれていた）のクラウドベースソリューションが Azure ATP（Microsoft Defender for Identityへ名称変更）
  - オンプレミスドメインコントローラからデータを収集でき、Office 365およびWindowsの他のATP製品と統合されていないオンプレミスソリューション
  - IDの異常と横方向（感染活動）の動きを検出する



## 3 つの主なセキュリティ サービス

- Exchange Online Protection (EOP)
- Microsoft Defender for Office 365 プラン 1 (Defender for Office P1)
- Microsoft Defender for Office 365 プラン 2 (Defender for Office P2)

## Microsoftのセキュリティ体制

- Protect/Detect (脅威の防止と検出)
- Respond (調査、対応)

に機能を分類できる

防止・検出	調査	対応
<p>提供されるテクノロジー:</p> <ul style="list-style-type: none"><li>• スпам</li><li>• フィッシング</li><li>• マルウェア</li><li>• バルク メール</li><li>• スプーフィング インテリジェンス</li><li>• 偽装の検出</li><li>• 管理者検疫</li><li>• 管理者とユーザーによる誤検知と検出漏れの報告</li><li>• URL およびファイルの許可/禁止</li><li>• レポート</li></ul>	<ul style="list-style-type: none"><li>• 監査ログ検索</li><li>• メッセージ追跡</li></ul>	<ul style="list-style-type: none"><li>• ゼロ時間自動削除 (ZAP)</li><li>• 許可リストと禁止リストの絞り込みとテスト</li></ul>

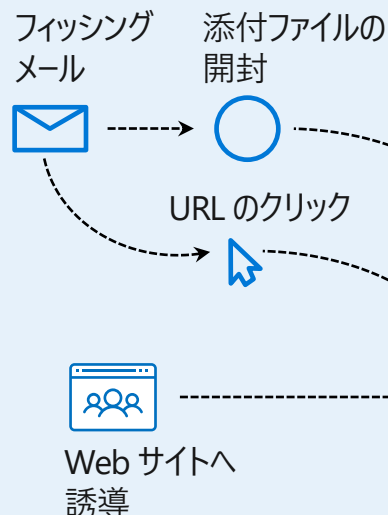


防止・検出	調査	対応
<p>EOP に含まれるすべてのテクノロジーに加えて:</p> <ul style="list-style-type: none"><li>• 安全な添付ファイル</li><li>• 安全なリンク</li><li>• Microsoft Defender for Office 365 によるワークロードの保護 (例: SharePoint Online、Teams、OneDrive for Business)</li><li>• メール、Office クライアント、Teams でのクリック時の保護</li><li>• Microsoft Defender for Office 365 のフィッシング詐欺対策</li><li>• ユーザーの偽装とドメインの偽装の保護</li><li>• アラートおよびアラート用 SIEM 統合 API</li></ul>	<ul style="list-style-type: none"><li>• 検出用 SIEM 統合 API</li><li>• <b>リアルタイム検出ツール</b></li><li>• URL 追跡</li></ul>	<ul style="list-style-type: none"><li>• 同上</li></ul>

防止・検出	調査	対応
EOP および Microsoft Defender for Office 365 P1に含まれるすべてのテクノロジーに加えて: <ul style="list-style-type: none"><li>同上</li></ul>	<ul style="list-style-type: none"><li><b>脅威エクスプローラー</b></li><li>脅威トラッカー</li><li>キャンペーンビュー</li></ul>	<ul style="list-style-type: none"><li>自動調査と応答 (AIR)</li><li>脅威エクスプローラーからの AIR</li><li>侵害されたユーザーの AIR</li><li>自動調査用 SIEM 統合 API</li></ul>

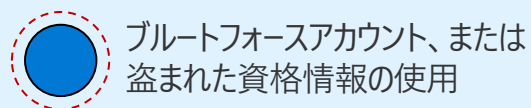
## Microsoft Defender for Office 365

マルウェアの検出、安全なリンク、安全な添付ファイル



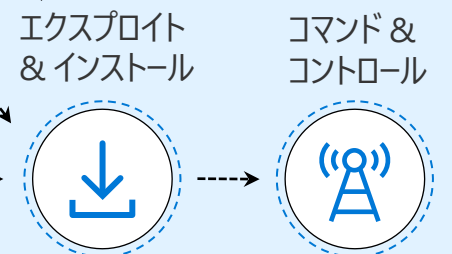
## Azure AD Premium P2 Identity Protection

ID の保護、条件付きアクセス



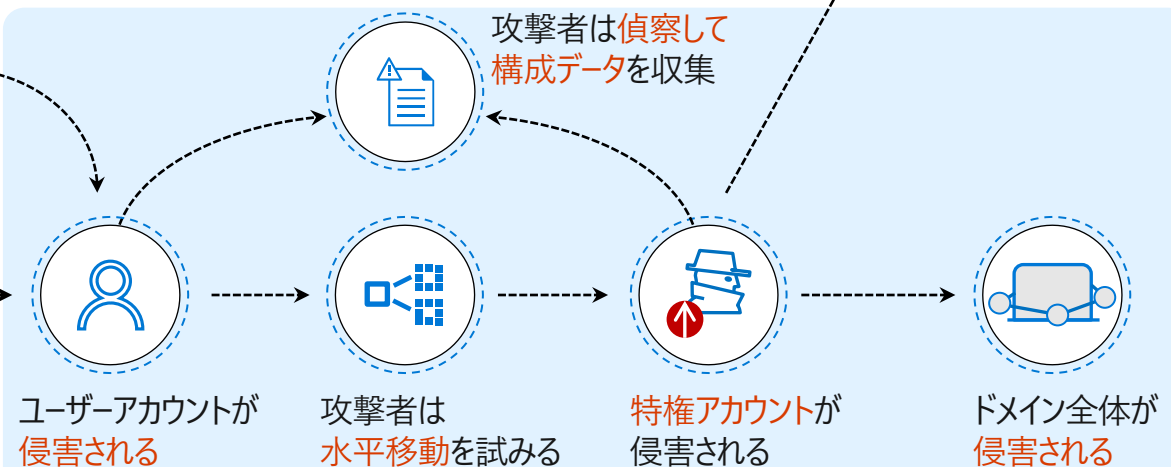
## Microsoft Defender for Endpoint

脅威の検出と応答 (EDR)  
エンドポイント保護 (EPP)



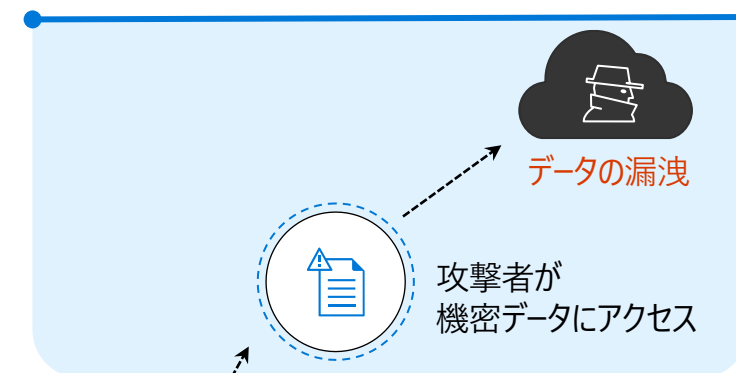
## Microsoft Defender for Identity

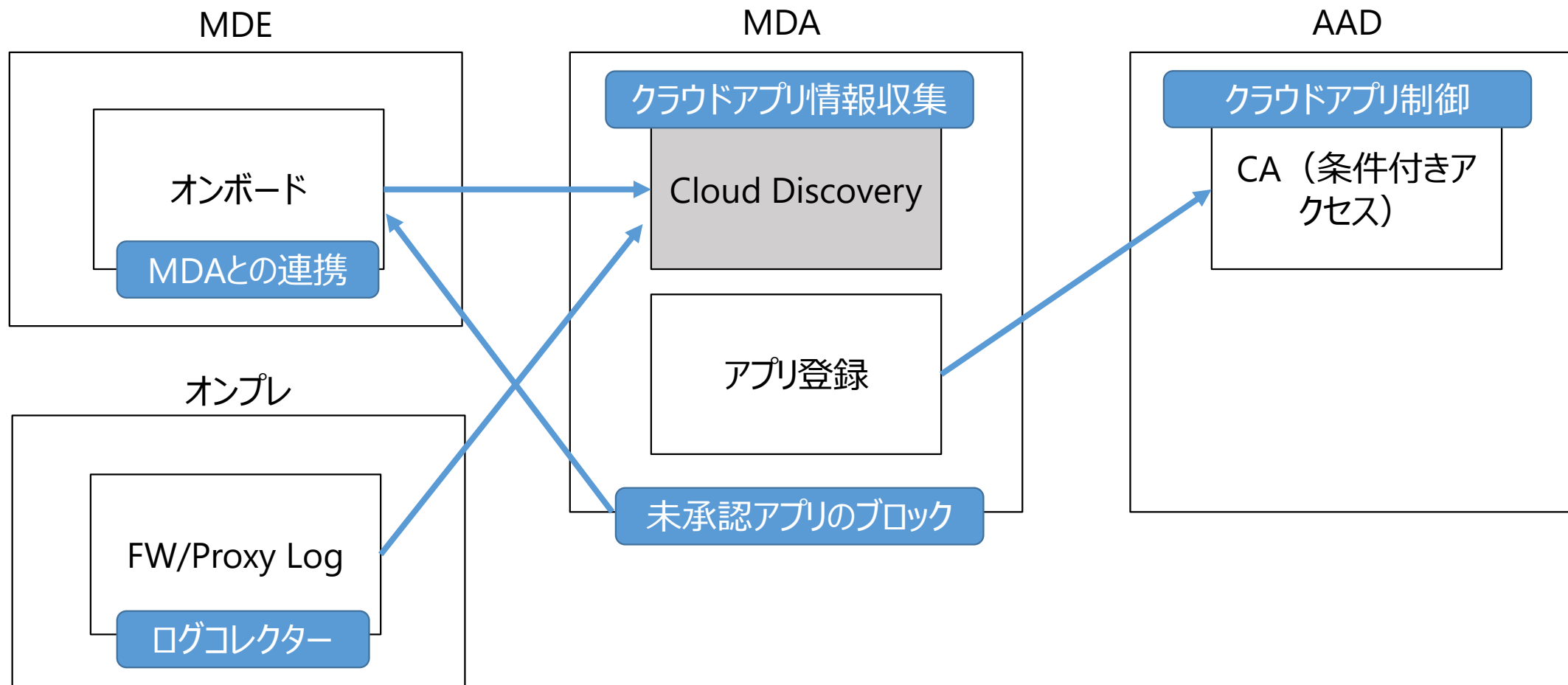
オンプレミス ID の保護



## Microsoft Defender for Cloud Apps

他のクラウドアプリを含めて  
クラウド全体の保護と条件付きアクセスを拡張





## Discover(検出)

機密情報タイプを定義し、機密情報が含まれていないか**自動的に検出**

## Protection (保護)

特定のラベルがついたドキュメントに対して、**任意の保護レベル**(ドキュメントの暗号化やドキュメントへのアクセス権の制限のほか、視覚的なマーキングの適用、ユーザーへのポリシー通知など)を設定

## Classify(分類)

**分類とラベル付け**

## Monitor (監視)

**保護された機密情報を監視**する。機密情報をどのように使用・共有しているかを可視化し、ファイルが不適切に共有されたときはアクセス権を取り消すなど、どんな緊急の問題にも対処して修復できるような機能を提供

Windows  
Information  
Protection



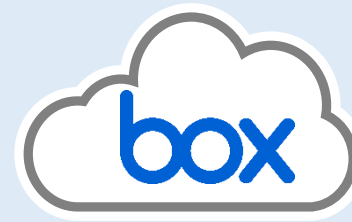
Windows PC

Azure  
Information  
Protection



File 共有

Microsoft  
Defender for  
Cloud Apps

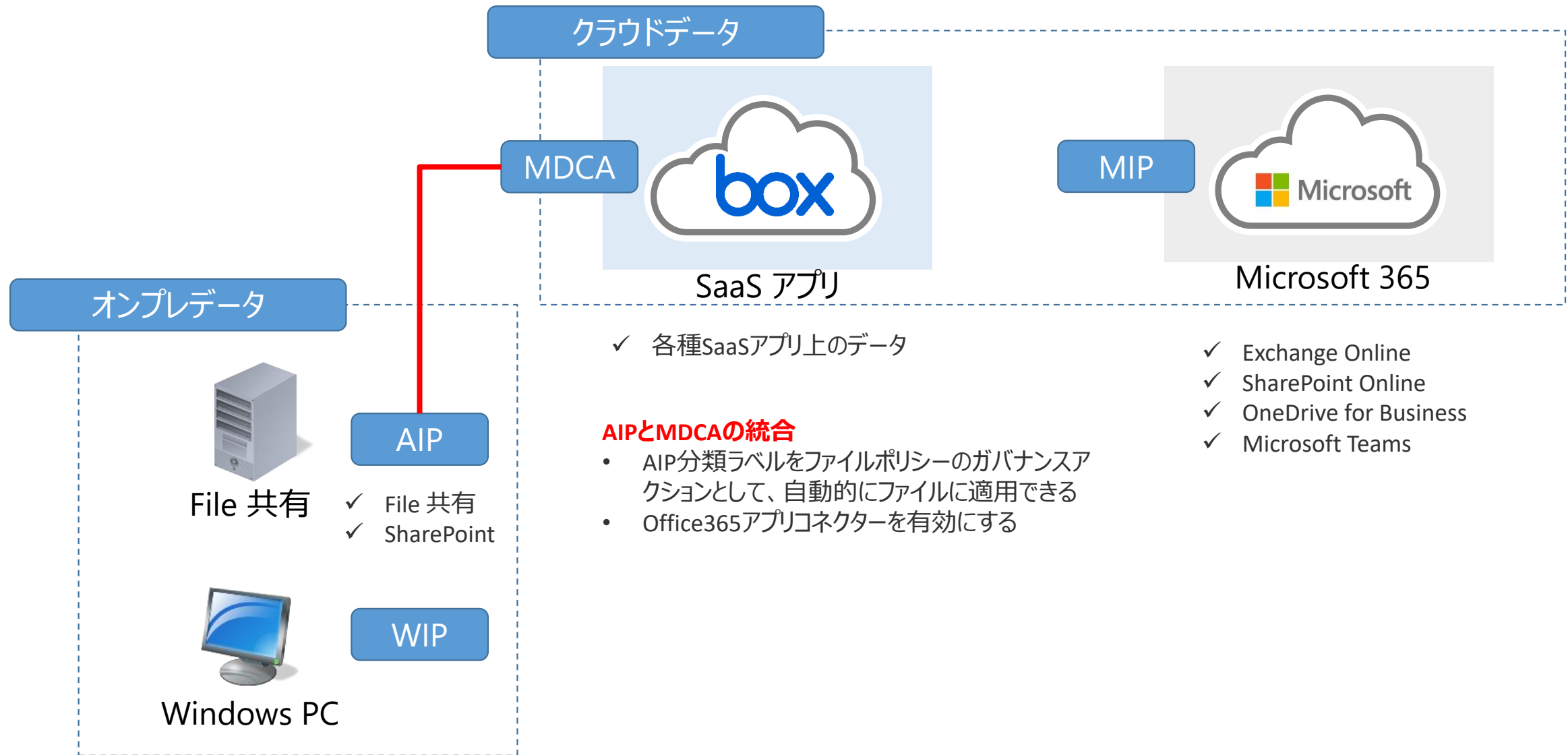


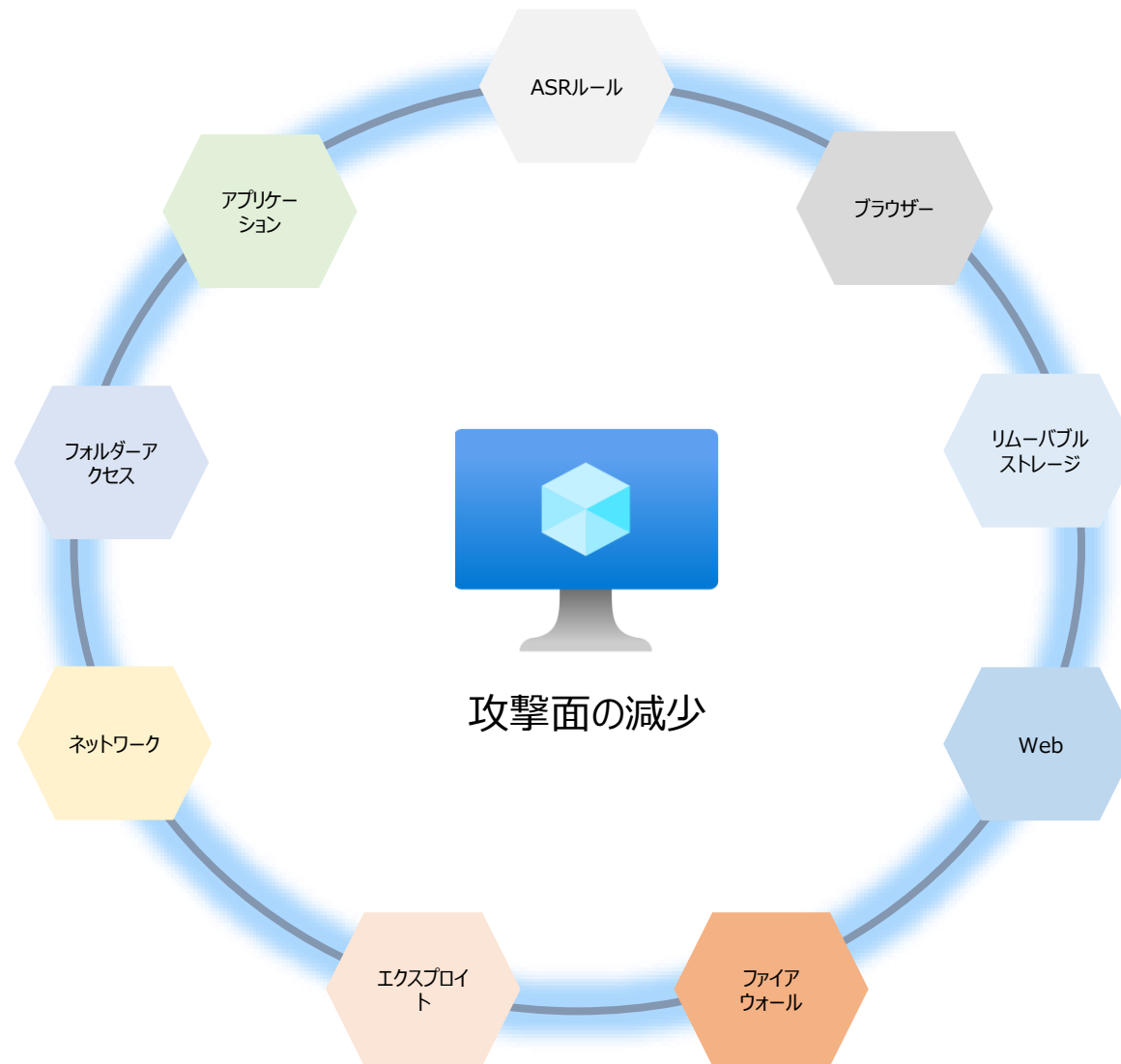
SaaS アプリ

Microsoft 365  
Information  
Protection

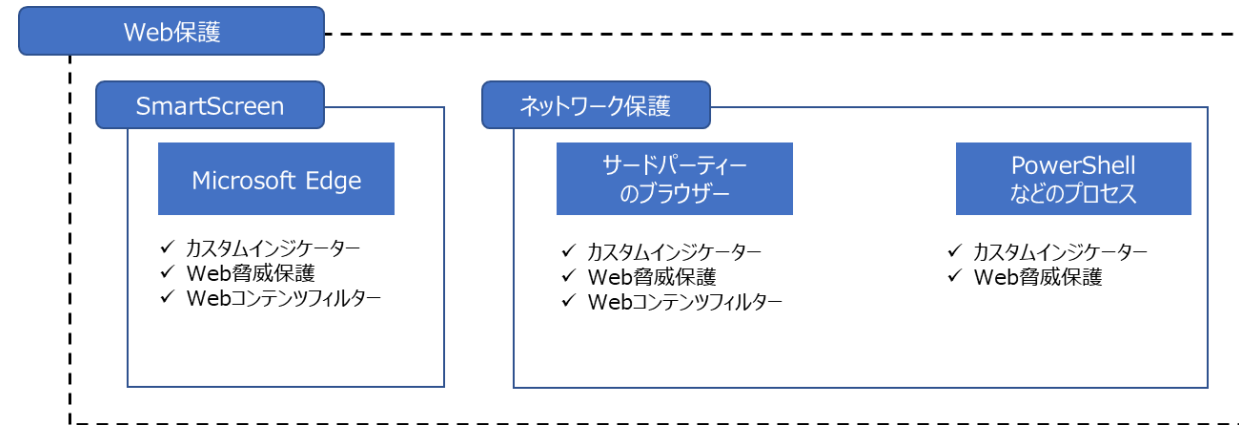
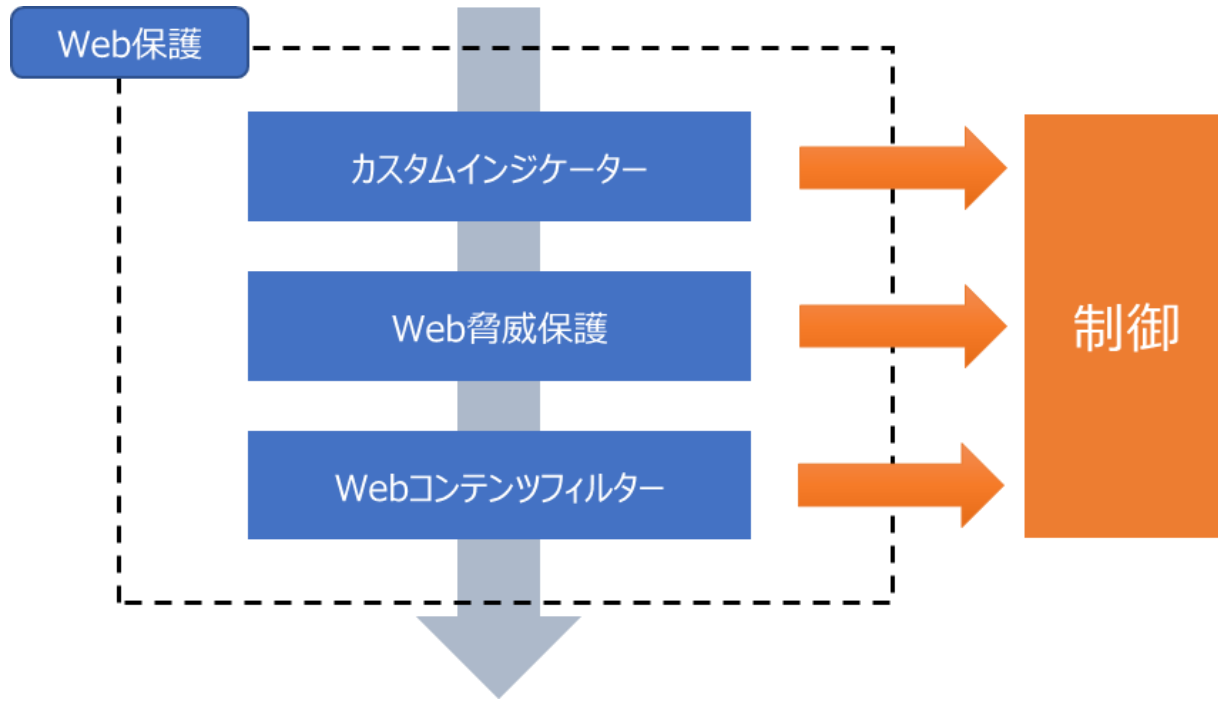


Microsoft 365









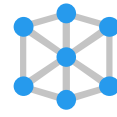
SIEM

## Microsoft Sentinel

企業全体にわたって脅威を可視化

  
Existing security  
portfolio



  
Microsoft  
ecosystem

## Microsoft 365 Defender

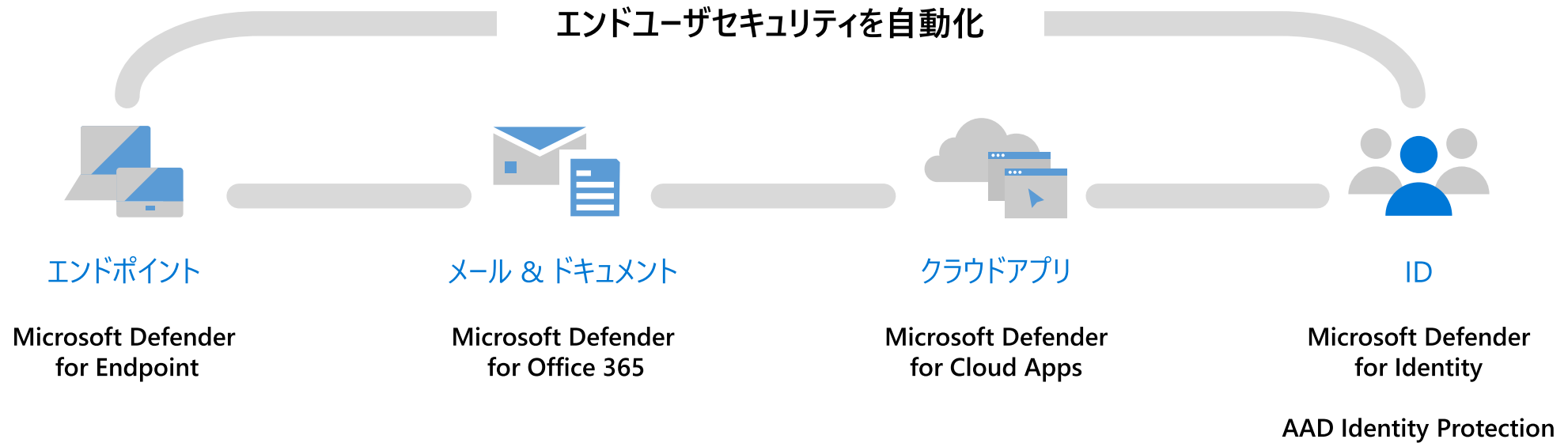
利用者環境の保護・検出

## Microsoft Defender for Cloud

インフラストラクチャの保護・検出

XDR

# Microsoft 365 Defender



## Multi-platform coverage

iOS

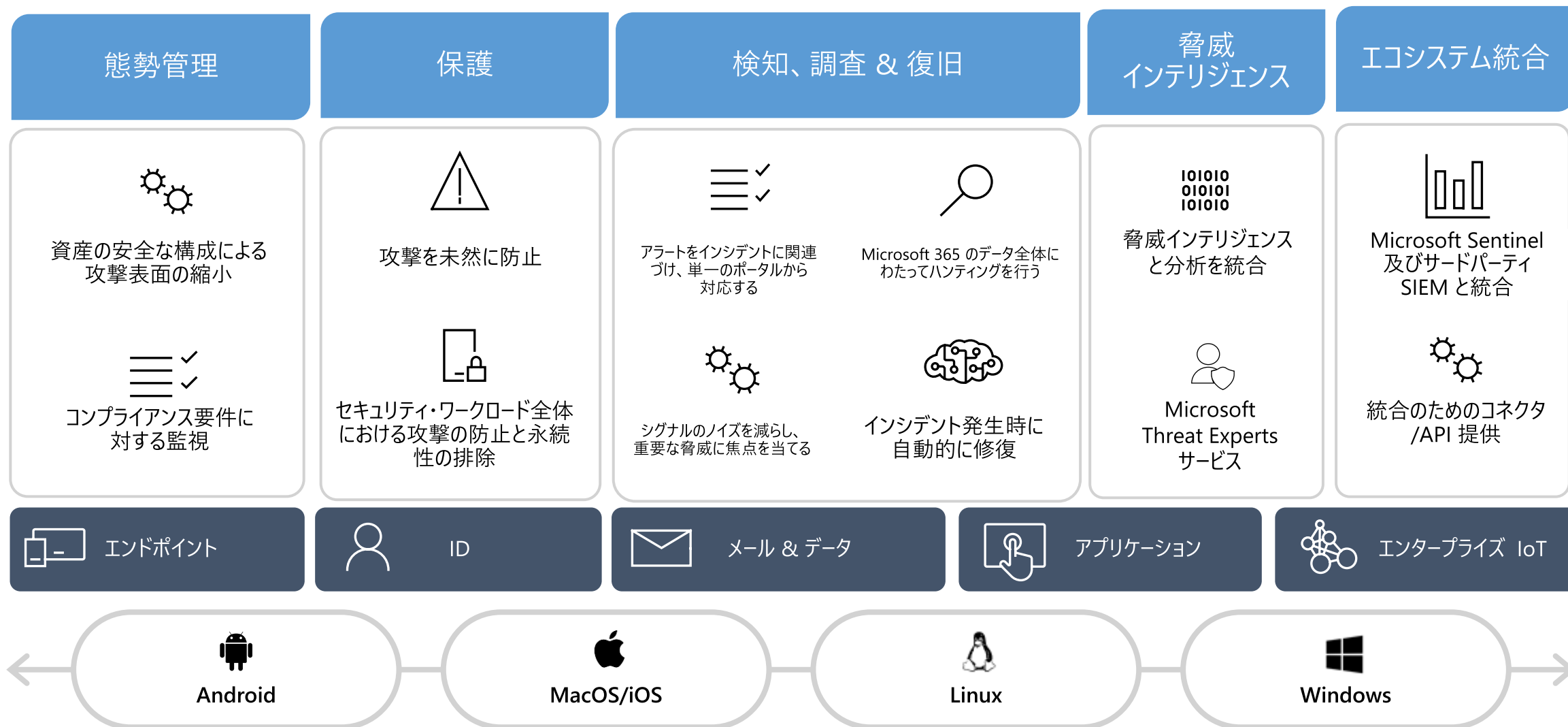


Android



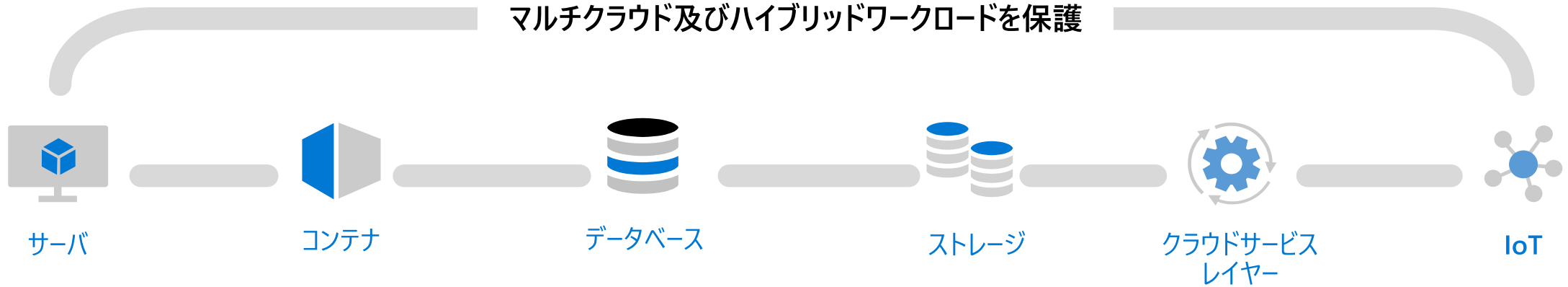
Windows

# Microsoft 365 Defender



# Microsoft Defender for Cloud

マルチクラウド及びハイブリッドワークロードを保護



Multi-cloud coverage



Amazon Web Services

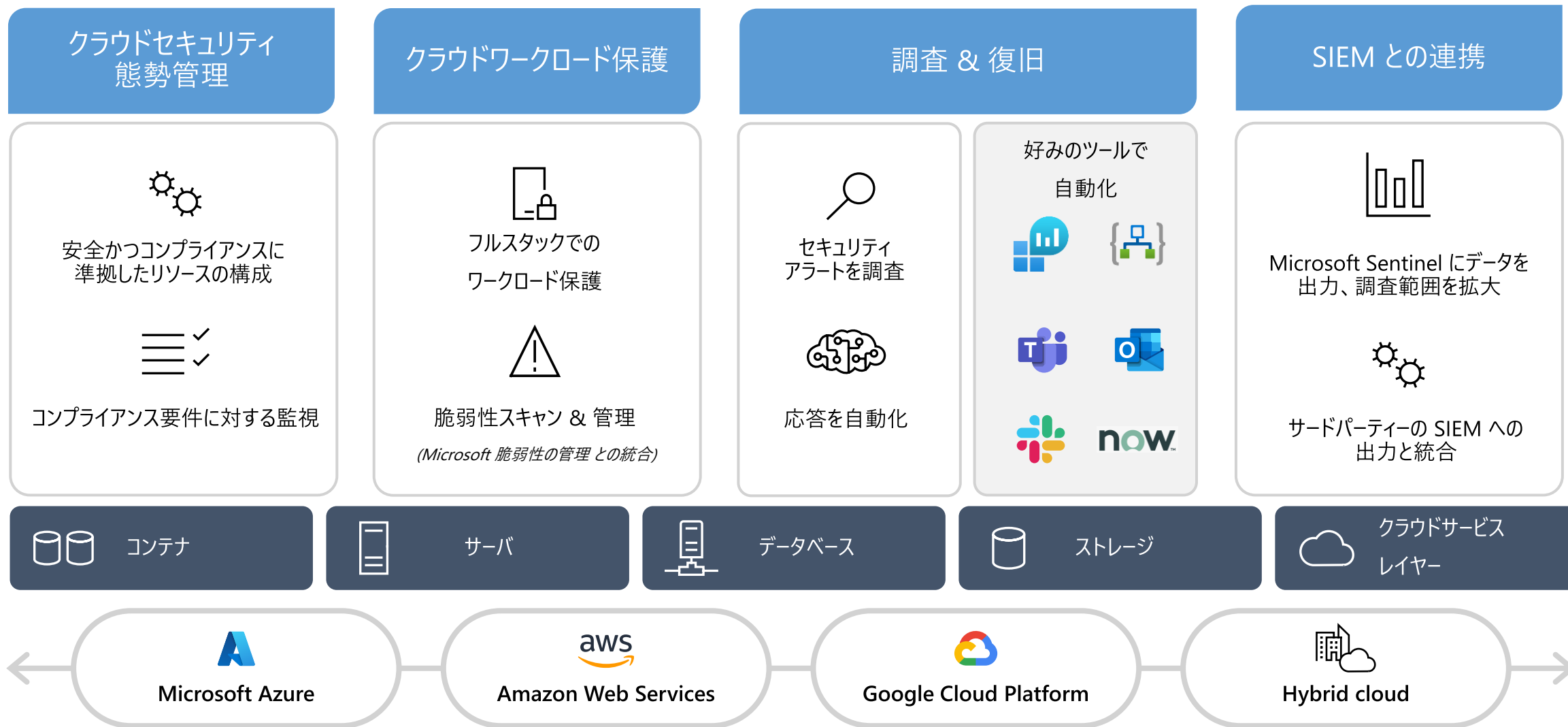


Microsoft Azure

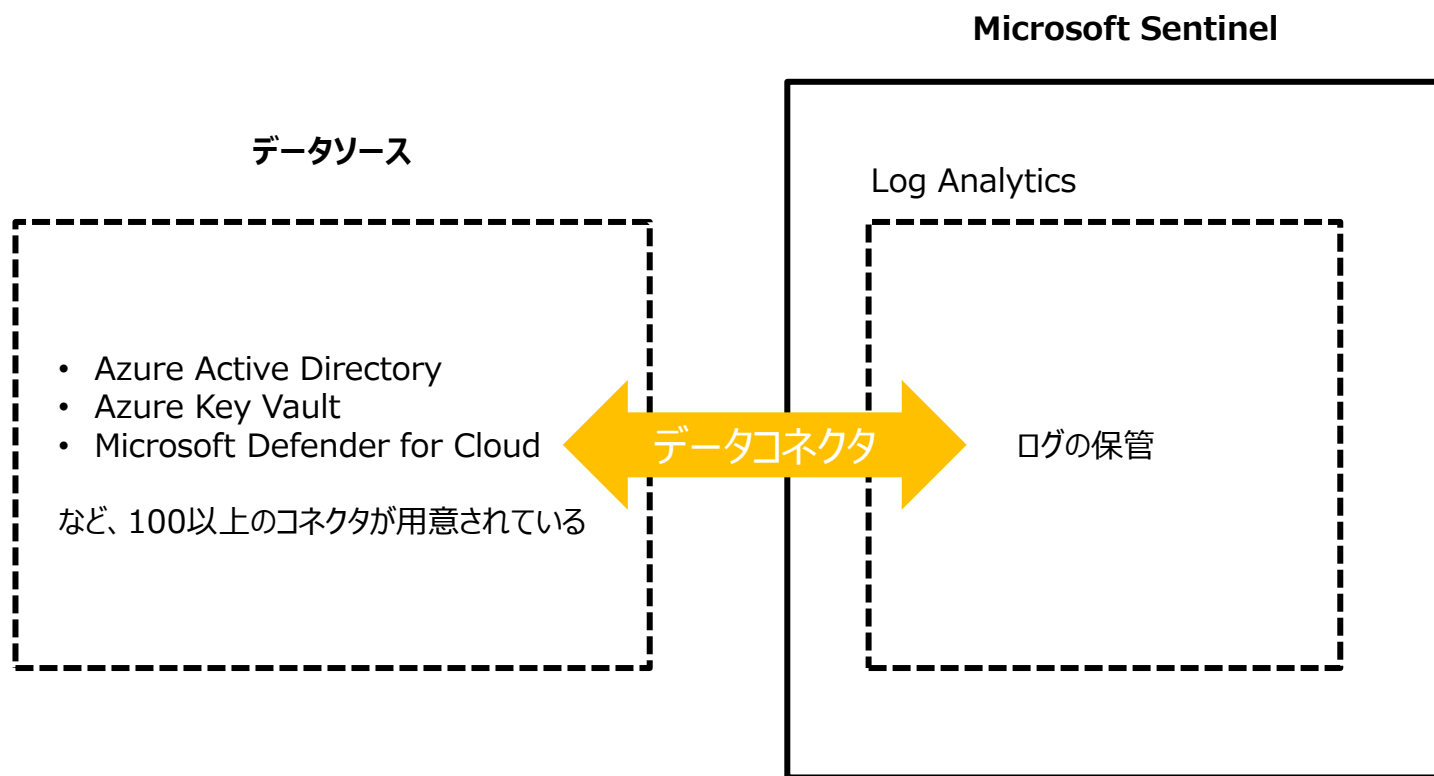


Google Cloud

# Microsoft Defender for Cloud



# Microsoft Sentinel の整理



## • データ収集

- メニューとしては**データコネクタ**
- AADやアクティビティログなどAzureだけではなく、イベントログなどOSのログからPalo等のNW機器など様々なデータソースからLog Analyticsにデータ収集する

## • 検知

- メニューとしては**分析**
- 収集データに対してクエリ(デフォルトで準備されているのもあります。)を実行し合致するイベントがあった時に**アラート**を作成する

## • 調査

- メニューとしては**インシデント**
- 影響範囲を特定する

## • 対処

- メニューとしては**オートメーション(プレイブック)**
- Logic Appで構成され検知したアラートに対しての処理を行う

攻撃手法		概要
Initial Access	初期アクセス	攻撃者がネットワークに侵入しようとしている
Execution	実行	攻撃者が悪意のあるコードを実行しようとしている
Persistence	永続化	攻撃者が不正アクセスする環境を確保しようとしている
Privilege escalation	権限昇格	攻撃者がより高いレベルでの権限を取得しようとしている
Defense Evasion	防衛回避	攻撃者が検知されないようにしている
Credential Access	認証情報アクセス	攻撃者がアカウント名とパスワードを盗もうとしている
Discovery	探索	攻撃者がアクセス先の環境を理解しようとしている
Lateral Movement	水平展開	攻撃者がアクセス先の環境を移動しようとしている
Collection	収集	攻撃者が関心のあるデータを収集しようとしている。
Command and control	C&C	攻撃者が侵害されたシステムと通信し制御しようとしている
Exfiltration	持ち出し	攻撃者が情報を持ち出そうとしている
Impact	影響	攻撃者がシステムとデータを操作、中断、破壊しようとしている

攻撃が成功に向かって大きく  
変化するポイント

実害が発生するポイント

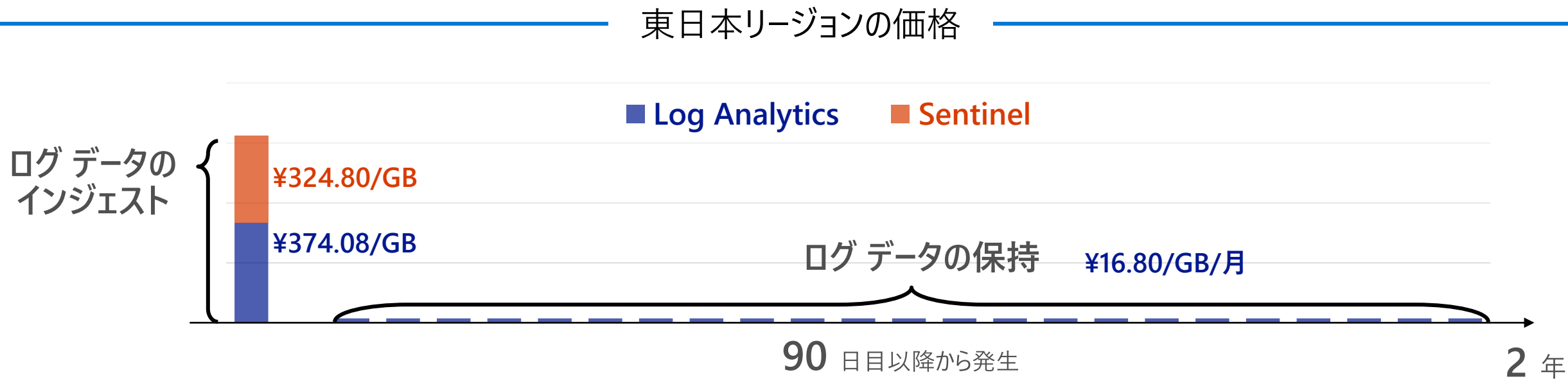


Microsoft Sentinel の課金は、

ログデータのインジェスト (Log Analytics + Sentinel)

ログデータの保持 (90 日目以降から、Log Analytics のみ)

の 2 段階課金



# ログデータのインジェスト費用が無料のデータソース

テーブル名

必要な権限

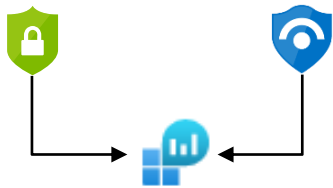
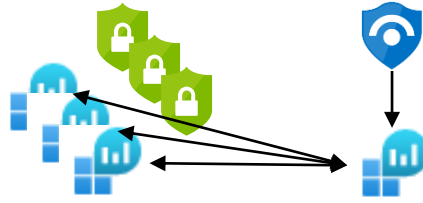
Office 365	OfficeActivity	無償	全体管理者 セキュリティ管理者
Azure AD	SigninLogs		全体管理者 セキュリティ管理者
	AuditLogs		
Microsoft 365 Defender	DeviceInfo		全体管理者 セキュリティ管理者
	DeviceNetworkInfo		
	DeviceProcessEvents		
	DeviceNetworkEvents		
	DeviceFileEvents		
	DeviceRegistryEvents		
	DeviceLogonEvents		
	DeviceImageLoadEvents		
	DeviceEvents		
	DeviceFileCertificateInfo		
Microsoft Defender for Endpoint の生ログ			
Microsoft Defender for Office 365 の生ログ	EmailEvents	Microsoft Defender for Identity の生ログ *DCへのログオンイベント *DNS クエリ等	Coming Soon
	EmailUrlInfo		
	EmailAttachmentInfo	Microsoft Cloud App Security の生ログ *接続アプリのイベント *接続アプリのファイルイベント	Coming Soon
	EmailPostDeliveryEvents		
Microsoft Defender for Office 365	SecurityAlert	無償	全体管理者 セキュリティ管理者
Microsoft Defender for Endpoint	SecurityAlert	無償	全体管理者 セキュリティ管理者
Azure AD Identity Protection	SecurityAlert	無償	全体管理者 セキュリティ管理者
Microsoft Defender for Identity	SecurityAlert	無償	全体管理者 セキュリティ管理者
Microsoft Defender for Cloud App	SecurityAlert	無償	全体管理者 セキュリティ管理者
	McasShadowItReporting		
Azure Information Protection	SecurityAlert	無償	全体管理者 セキュリティ管理者 Azure Information Protection管理者
	InformationProtectionLogs_CL		

無料データソース <https://docs.microsoft.com/ja-jp/azure/sentinel/azure-sentinel-billing#free-data-sources>

# [補足] Log Analytics ワークスペースの設計

Microsoft Defender for Cloud (以下MDfC)、および Microsoft Sentinel とともに Log Analytics ワークスペースを用いるが、同一のワークスペースに保管する方式と個別にワークスペースを分離して接続する方式が選択可能

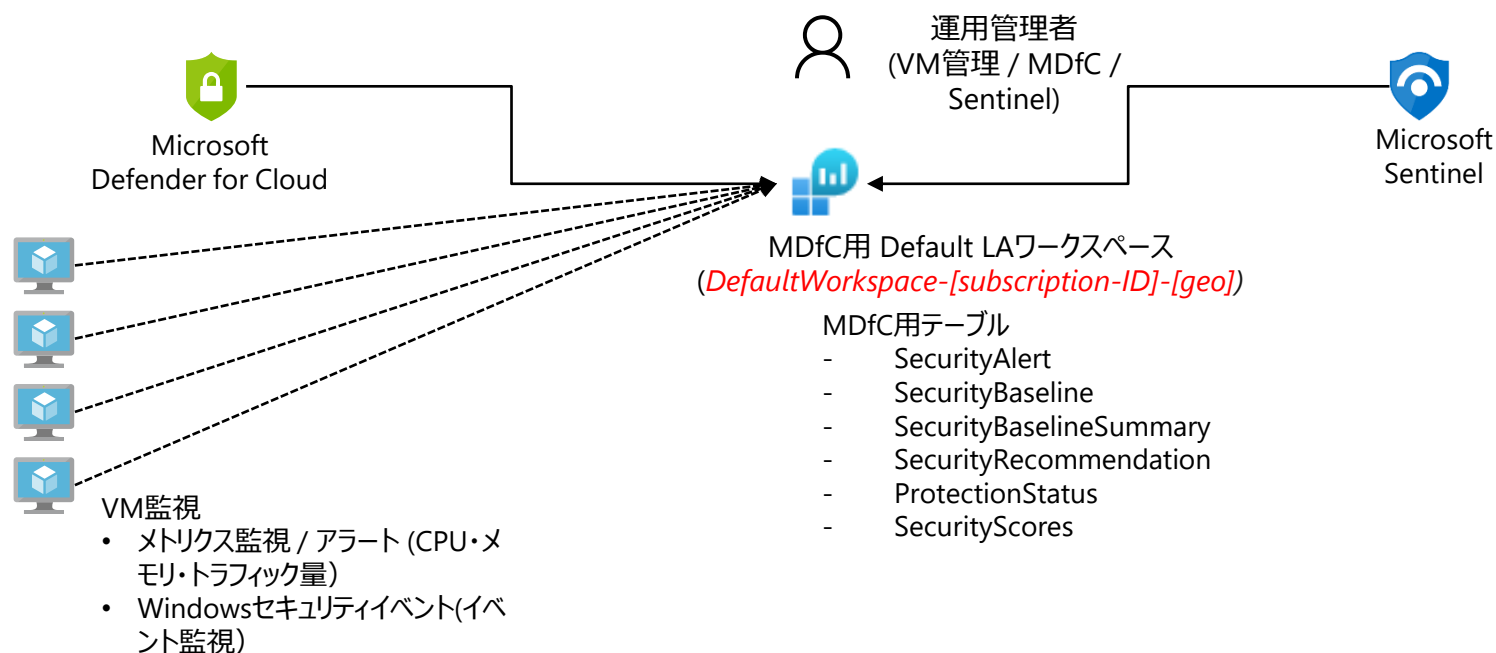
それぞれメリット/デメリットがあるため、お客様の運用要件を検討の上で検討していただきたい

方式	メリット	デメリット	推奨する構成
MDfC & Sentinel を一つの Log Analytics ワークスペースでまとめる 	<ul style="list-style-type: none"><li>設計/運用が用意</li><li>RBACやアーカイブ機能、保存期間などの設定が一元管理できる</li><li>LAワークスペースが統合になるため、コスト節約出来る可能性がある</li><li>仮想マシンの Windows Security Event Logs の課金は 500 MB /日 まで無料</li></ul>	<ul style="list-style-type: none"><li>Sentinelを要件・サービス毎に分割するケースには使えない</li><li>MDfCのすべてのログ（推奨事項など）もまとめてSentinelのワークスペースに入ってきてしまう</li><li>メトリクスなどのイベントはSentinel側で見なくても課金対象扱いとなる</li></ul>	小中規模の環境 LAワークスペースを1つにまとめることが出来るユーザーなど  [注意] MDfCでは、初期設定時に Log Analytics ワークスペースを作成するため、Sentinelと統合する場合は作成後に指定ワークスペースへの切替などを設定すること
MDfC / Sentinel 毎に個別の Log Analytics ワークスペースで区分する 	<ul style="list-style-type: none"><li>大規模なお客様ではSentinelの管理が分かれるので、別にする</li><li>個別にワークスペースのアクセス制御が可能（MDfC / Sentinel）</li><li>Sentinelでは、複数のサブスクリプションのMDfCを接続して監視することが可能</li><li>MDfC の Defender アラート / 推奨事項といった個々のテーブルに対して、個別に Sentinel に取り込むかどうか取捨選択が可能</li></ul>	<ul style="list-style-type: none"><li>管理が大変になる（複数のLAワークスペース）</li><li>クロスワークスペースクエリのワークスペース数上限や、パフォーマンス劣化が課題になることがある</li></ul>	大規模なユーザー向け ※Sentinel を複数台建てて、個別運用したいユーザーなど  Sentinel の監視と、MDfCの監視で運用を分けたいユーザー

# [補足] MDfC Log Analytics ワークスペース設計

## MDfC / Sentinel のワークスペースを統合で管理する

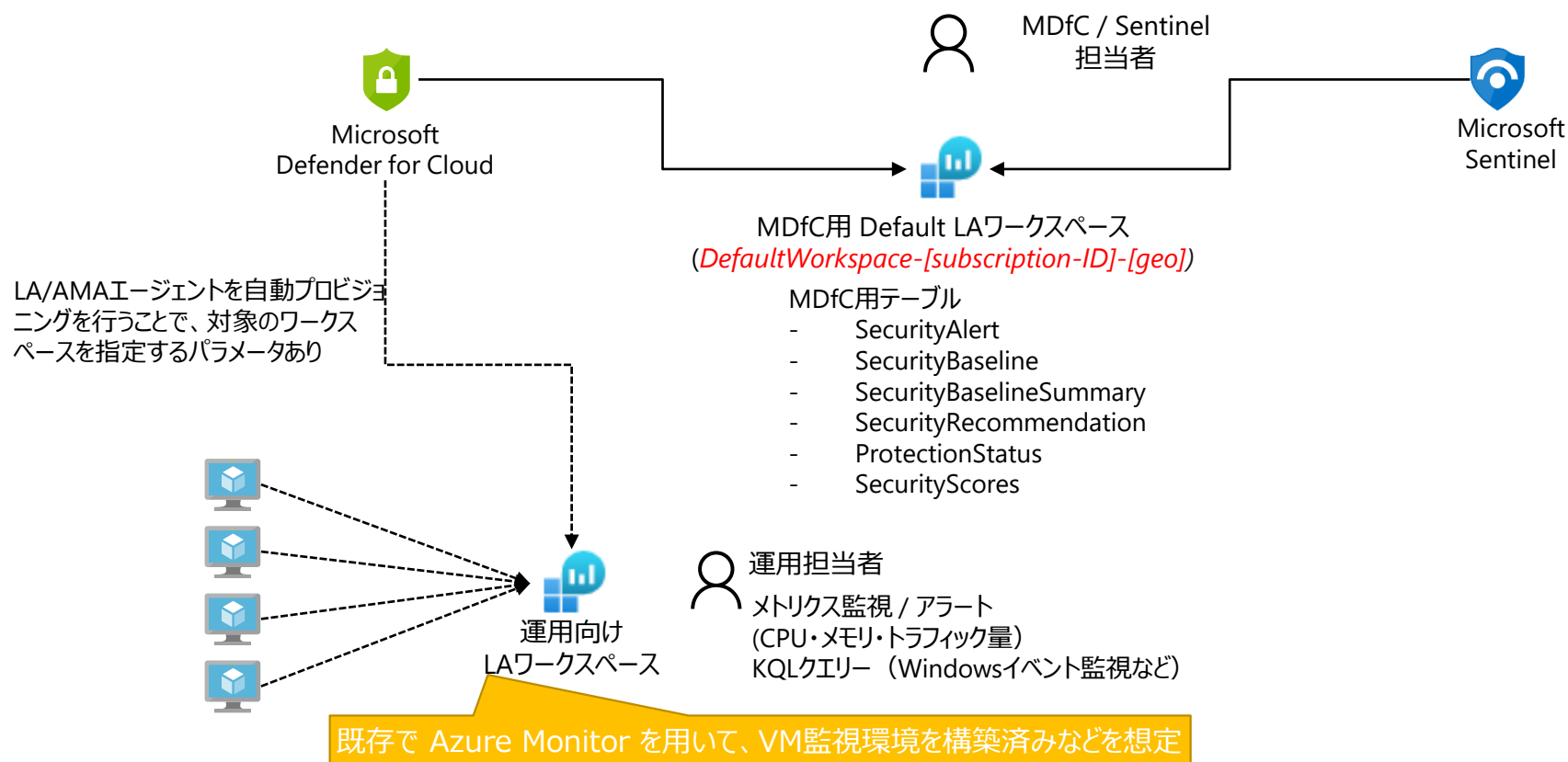
- MDfC / Sentinel のワークスペースを統合して管理する設計は以下の通り
- VM の運用、MDfC、Sentinel を一つの Log Analytics ワークスペースで一元管理する



# [補足] MDfC LogAnalytics ワークスペース設計

## MDfC / Sentinel のワークスペースを統合で管理する

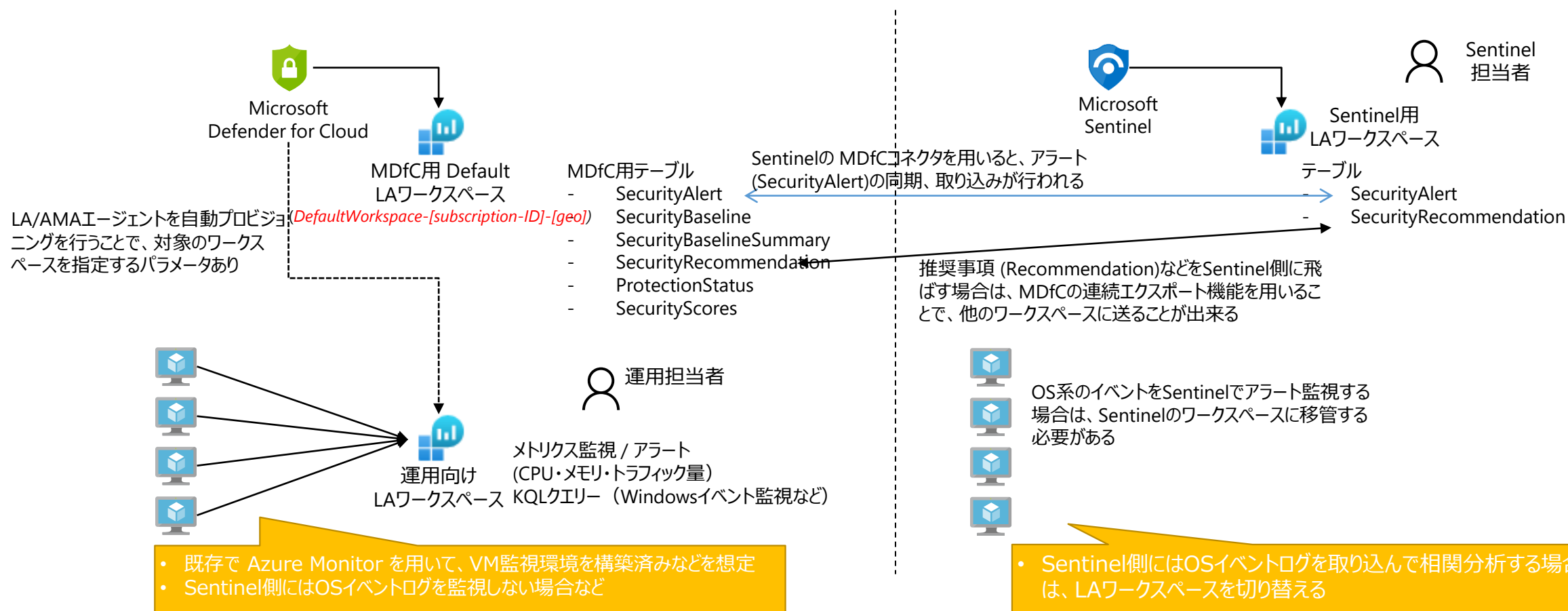
- MDfC / Sentinel のワークスペースを統合して管理する設計は以下の通り。
- VM の運用については、専用のワークスペースで管理する
- MDfC、Sentinel を一つの Log Analytics ワークスペースで一元管理する



# [補足] MDfC LogAnalytics ワークスペース設計

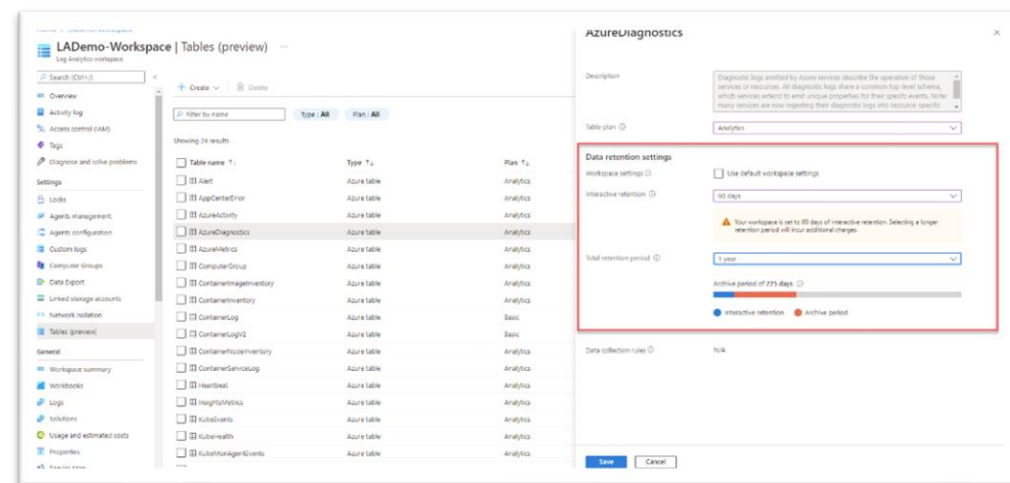
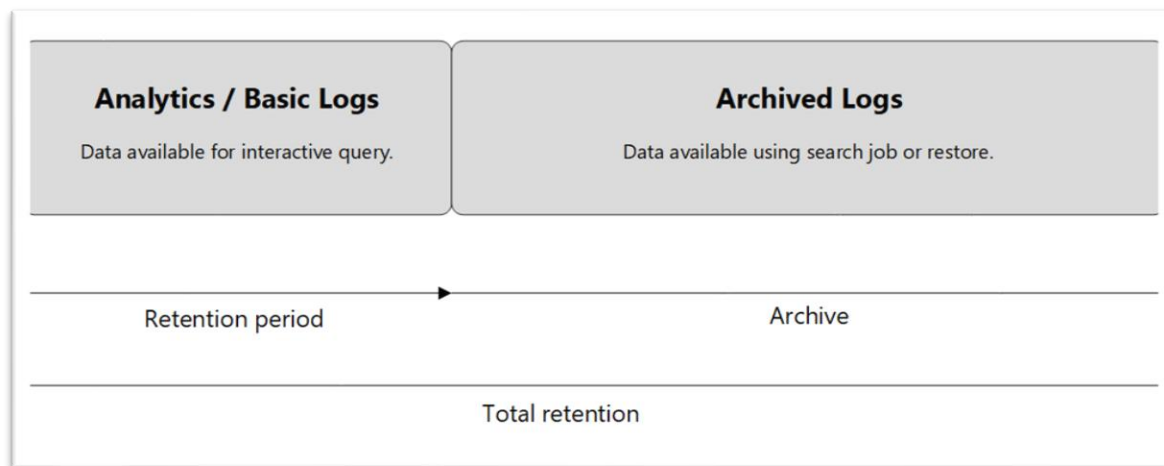
## MDfC / Sentinel のワークスペースを別で管理する

- MDfC / Sentinel のワークスペースを分けて管理する設計は以下の通り。



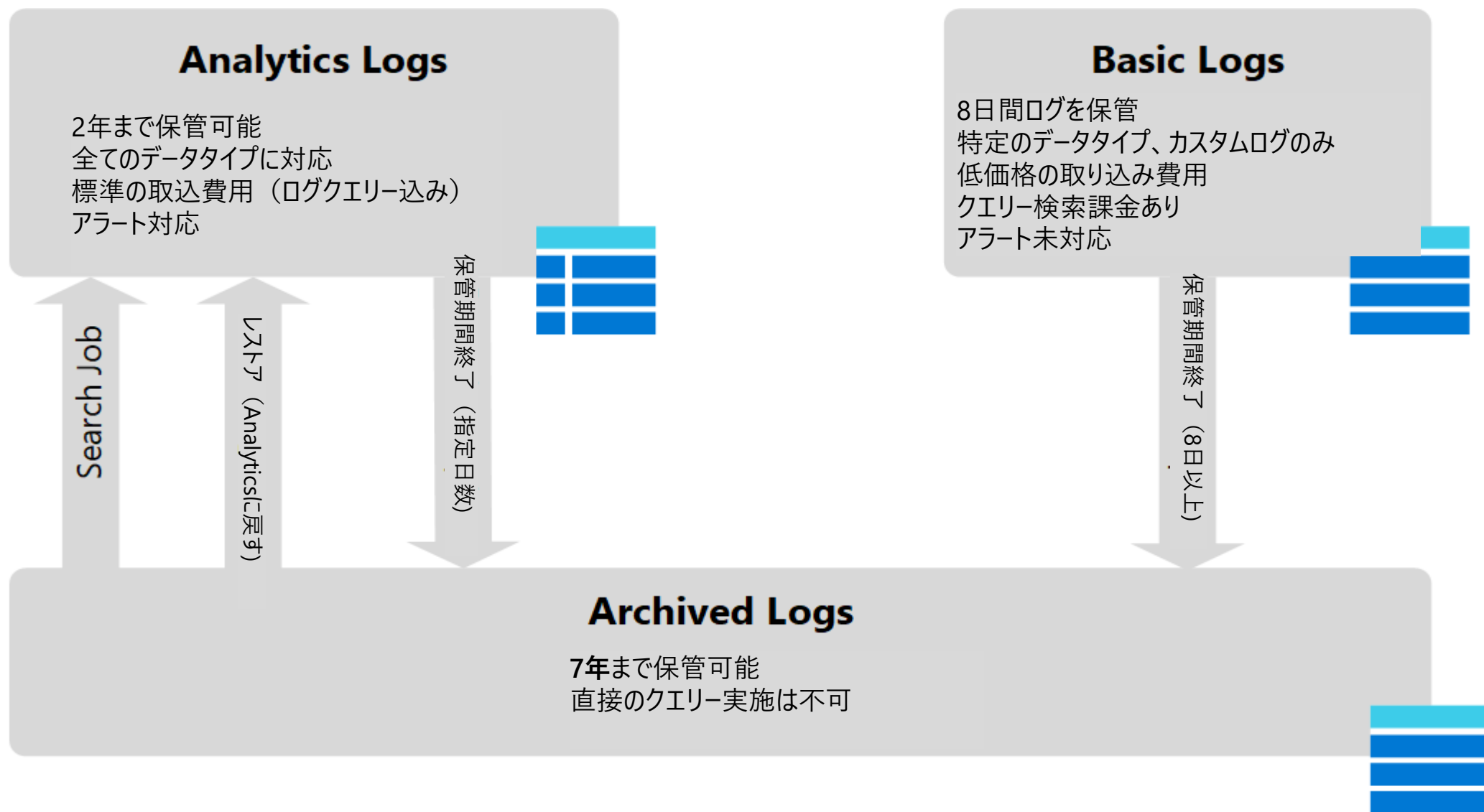
# Log Analytics ネイティブ機能によるログの長期保管

- Log Analytics は Azure リソース、OS イベントログなどを保持するログ管理サービス。
- ワークスペースには複数のテーブルが作成され、それぞれのログデータが保持される。
- 「**Analytics ログ**」 or 「**Basic ログ**」の保持期間 + 「**Archive ログ**」の保持期間」の合計で最大 7年間のログを保持。
- データ保持期間の設定は各テーブルごとに実施する。
  - Analytics ログ：最大2年間保存、すべてのクエリの実行をサポート。
  - [Basic ログ](#)：8日間保存、実行できるクエリに**制限**がある。
  - [Archive ログ](#)：クエリを実行できないログ。保存場所是对話型クエリを使用できるデータと共に同じテーブルに保持される。
- Archive ログは、[検索ジョブ](#)が**復元**することでクエリの実行が可能。



# [参考] Log Analytics ワークスペース Basic / Archived ログの相関関係

Log Analytics ワークスペースの各種ログ機能の比較を以下に示します。





## CEFのAzure VMのアーキテクチャ

次は、Azure の Linux VM の場合のセットアップ図です。

