

SC-200

補足資料

Azure Portal

Microsoft Defender for
Cloud

Microsoft Sentinel

Microsoft Defender XDR

Microsoft Defender for
Endpoint

Microsoft Defender for
Office 365

Microsoft Defender for
Cloud Apps

Microsoft Defender for
Identity

Microsoft Purview

コンプライアンス

ガバナンス

Endpoint
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

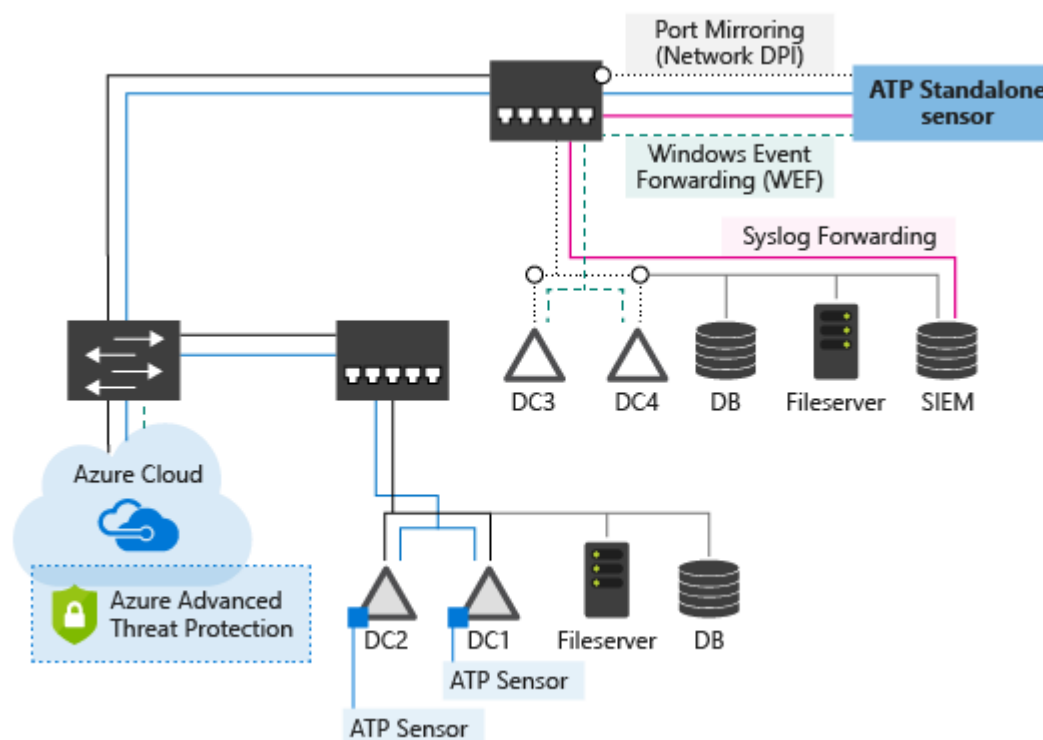
- エンドポイント上の高度な脅威を検出、調査、対応することを可能にするセキュリティ機能
- Windows Defender Advanced Threat Protection (ATP) から名称変更



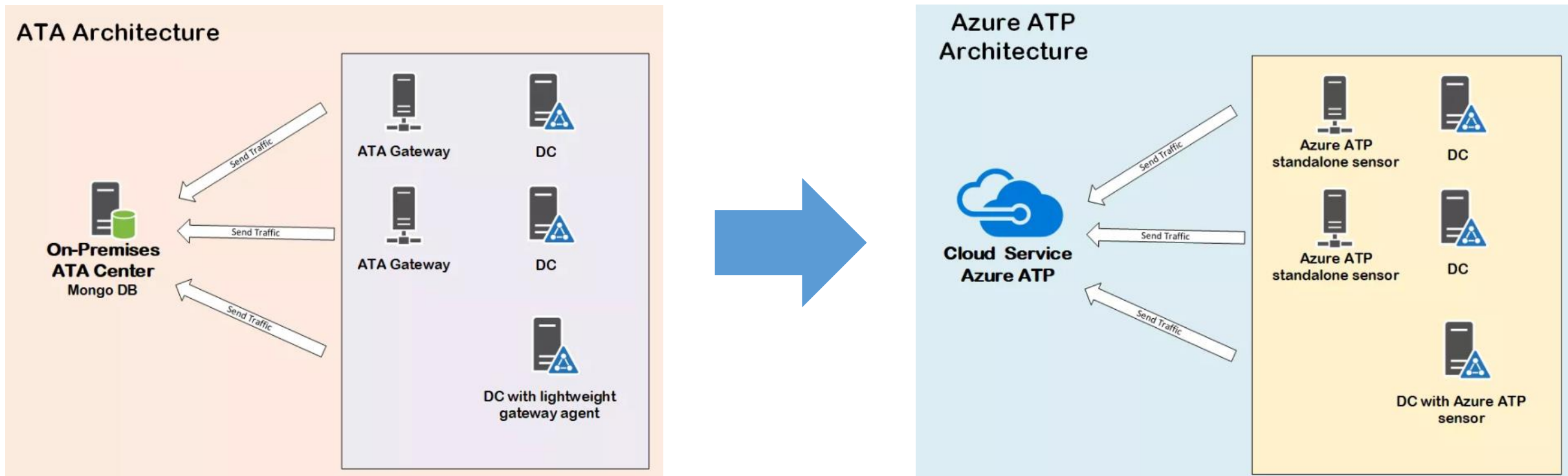
- 複数の種類の高度な対象となるサイバー攻撃や内部の脅威から、エンタープライズのハイブリッド環境を保護するためのクラウド サービス
- サイバーキルチェーンの複数のフェーズ（偵察、感染活動、目的の実行<ドメインの支配>）に重点を置いて、複数の不審なアクティビティを検出

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

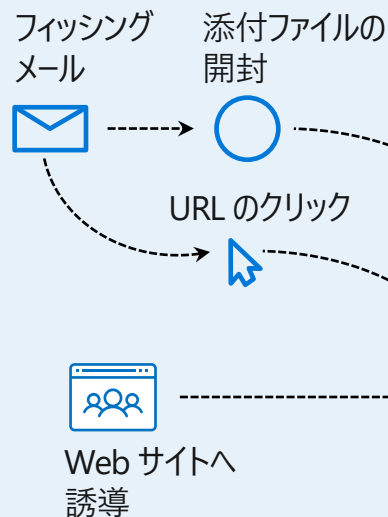
- Protect/Detect（脅威の防止と検出）
- Respond（調査、対応）

に機能を分類できる

| プラン | 防止・検出 | 調査 | 対応 |
|-----|---|--|--|
| EOP | <ul style="list-style-type: none">• スパム• フィッシング• マルウェア• バルク メール• スプーフィング インテリジェンス• 検疫• 管理者とユーザーによる誤検知と検出漏れのレポート• テナントでの許可/禁止<ul style="list-style-type: none">• ドメインとメールアドレス• 偽装• URL• ファイル | <ul style="list-style-type: none">• 監査ログ検索• メッセージ追跡• セキュリティレポートのメール送信 | <ul style="list-style-type: none">• ゼロ時間自動削除 (ZAP)• 許可リストと禁止リストの絞り込みとテスト |
| P1 | <ul style="list-style-type: none">• 安全な添付ファイル（メール、SharePoint、OneDrive、Teams）• 安全なリンク• フィッシング対策ポリシー（しきい値と偽装保護）• アラート用 SIEM 統合 API | <ul style="list-style-type: none">• 検出用 SIEM 統合 API• リアルタイム検出ツール• URL 追跡• Defender for Office 365レポート | |
| P2 | <ul style="list-style-type: none">• 攻撃シミュレーショントレーニング | <ul style="list-style-type: none">• 脅威エクスプローラー• 脅威トラッカー• キャンペーンビュー | <ul style="list-style-type: none">• 自動調査と応答 (AIR)• 脅威エクスプローラーからの AIR• 侵害されたユーザーの AIR• 自動調査用 SIEM 統合 API |

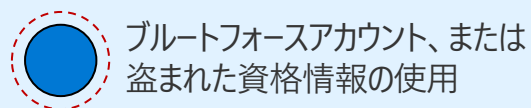
Microsoft Defender for Office 365

マルウェアの検出、安全なリンク、安全な添付ファイル



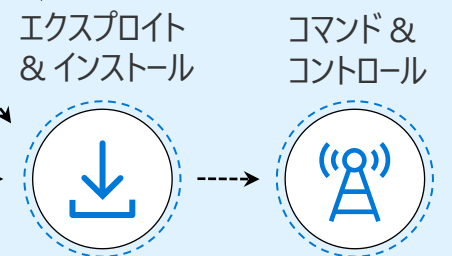
Azure AD Premium P2 Identity Protection

IDの保護、条件付きアクセス



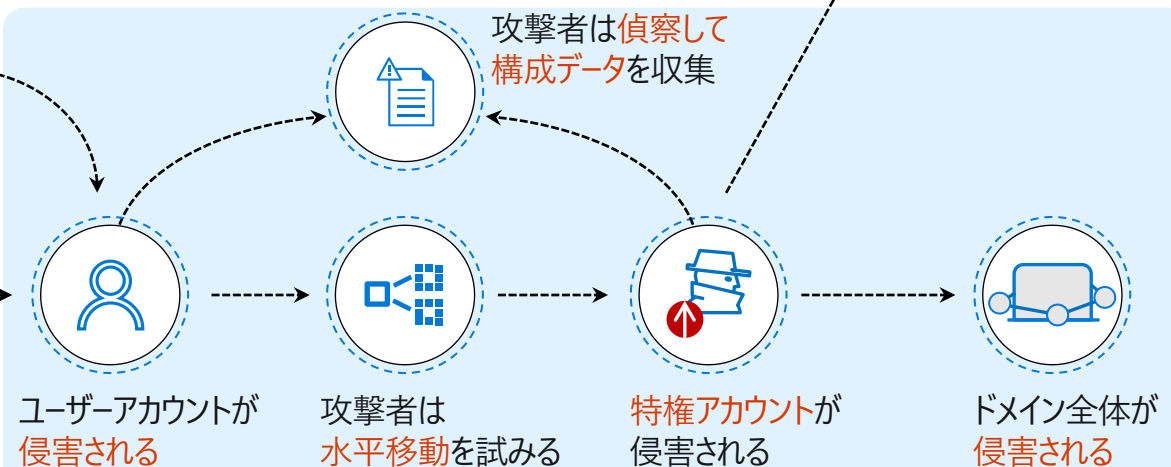
Microsoft Defender for Endpoint

脅威の検出と応答 (EDR)
エンドポイント保護 (EPP)



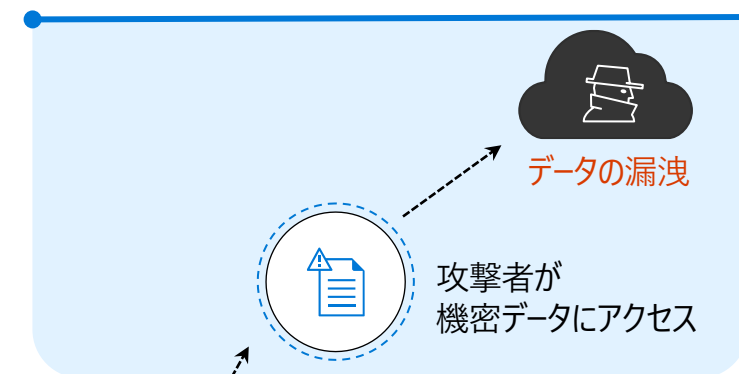
Microsoft Defender for Identity

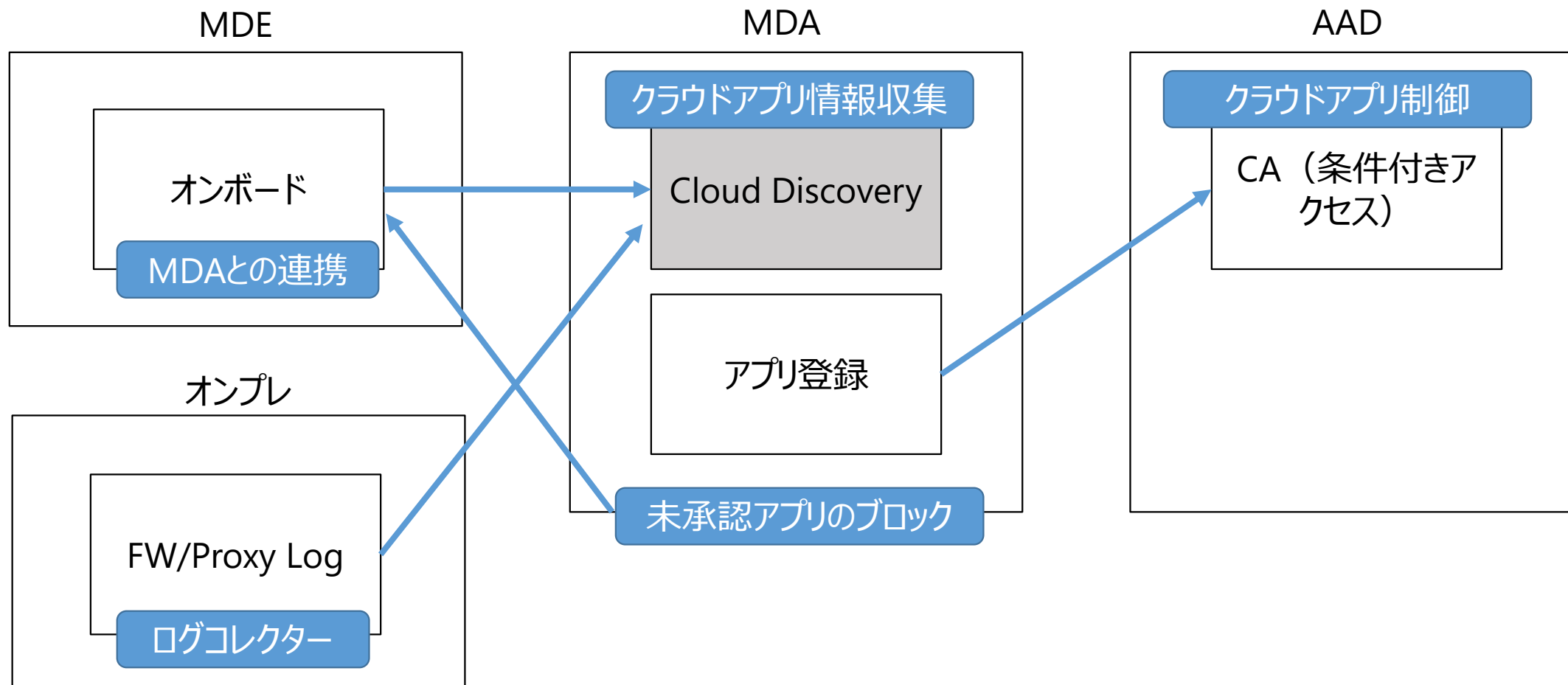
オンプレミス ID の保護



Microsoft Defender for Cloud Apps

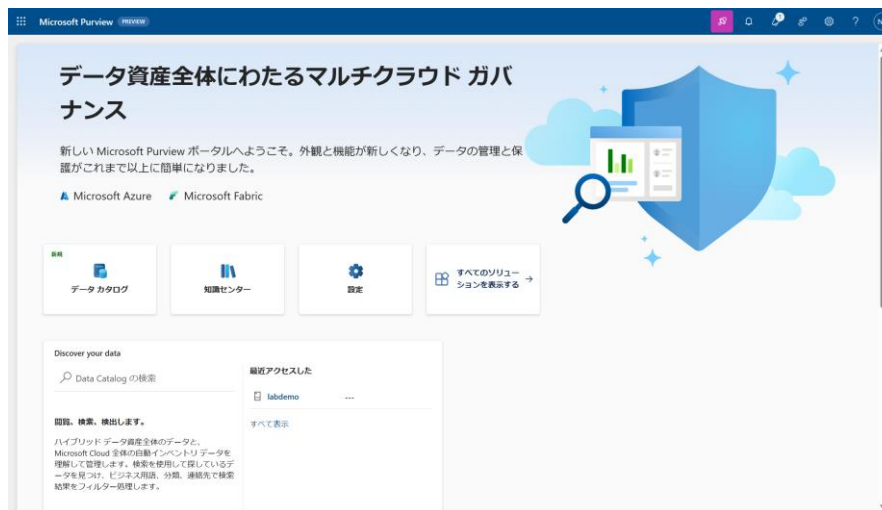
他のクラウドアプリを含めて
クラウド全体の保護と条件付きアクセスを拡張





- データ ガバナンス、情報保護、リスク管理、コンプライアンス ソリューションにまたがるブランドのソリューション
- 2つのポータルによって、それぞれの機能に対応したソリューションを提供

Microsoft Purview ガバナンス



<https://purview.microsoft.com>

Microsoft Purview のリスクおよびコンプライアンス



<https://compliance.microsoft.com/>

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**



Classify(分類)

- ・ **分類とラベル付け**



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



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

分類は、コンテンツを識別してラベル付けして、データ環境を理解するプロセス。

データに対して、「**機密情報の種類**」、「**ラベル**」、「**トレーニング可能な分類子**」、「**ポリシー**」など1つ以上を適用することで実現する。

機密情報の種類

クレジットカードやSSN（ソーシャルセキュリティ番号）など、正規表現や関数で識別できるパターンで定義する

トレーニング可能な分類子

AIとMLを使用して分類する。請求書や契約書などを分類することができる。内容に基づいた項目を識別するようにトレーニングする

ラベル

ドキュメントのスタンプ（社外秘など）のこと
秘密度ラベル・・・保護オプションとしてコンテンツへの透かしや暗号化がある。
保持ラベル・・・ポリシーに基づいたコンテンツの保持期間

ポリシー

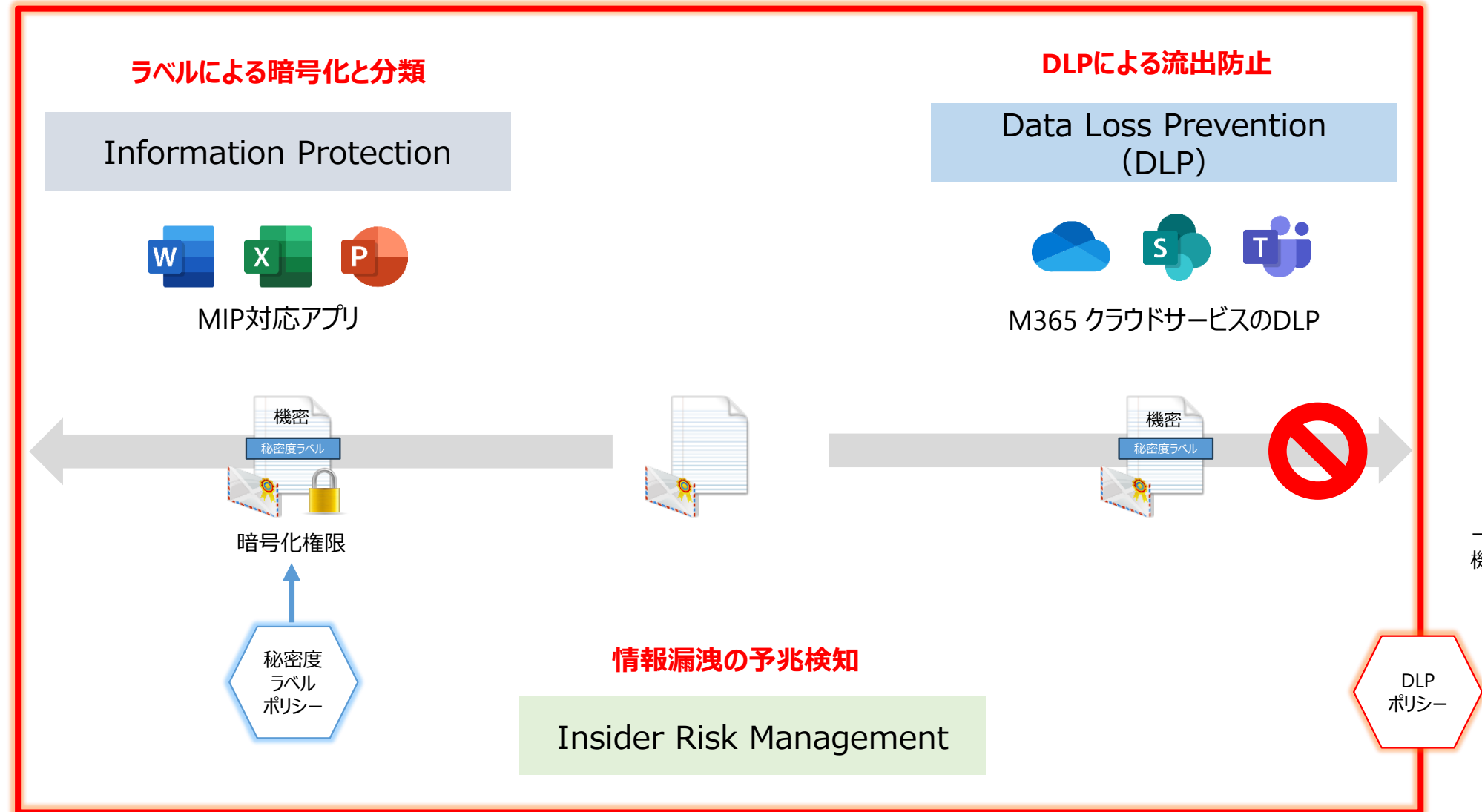
分類したデータをポリシーで管理する。
機密情報の種類、トレーニング可能な分類子、ラベルを使用してポリシーで定義する

秘密度ラベルポリシー・・・Officeアプリ、SharePointサイト、Office365グループに対してコンテンツを保護

DLP（データ損失）ポリシー・・・主に情報漏えい対策として使用。**機密情報の種類**と**保持ラベル**を使用して、保護が必要な情報を含むコンテンツを識別

アイテム保持ポリシー・・・サイト レベルやメールボックス レベルで同一の保持設定を割り当てる

保持ラベルポリシー・・・アイテム レベル (フォルダー、ドキュメント、メール) で保持設定を割り当てる



Windows
Information
Protection



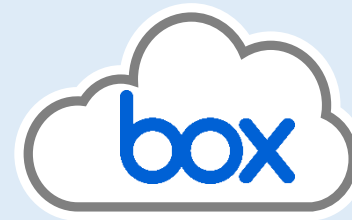
Windows PC

Azure
Information
Protection



File 共有

Microsoft
Defender for
Cloud Apps

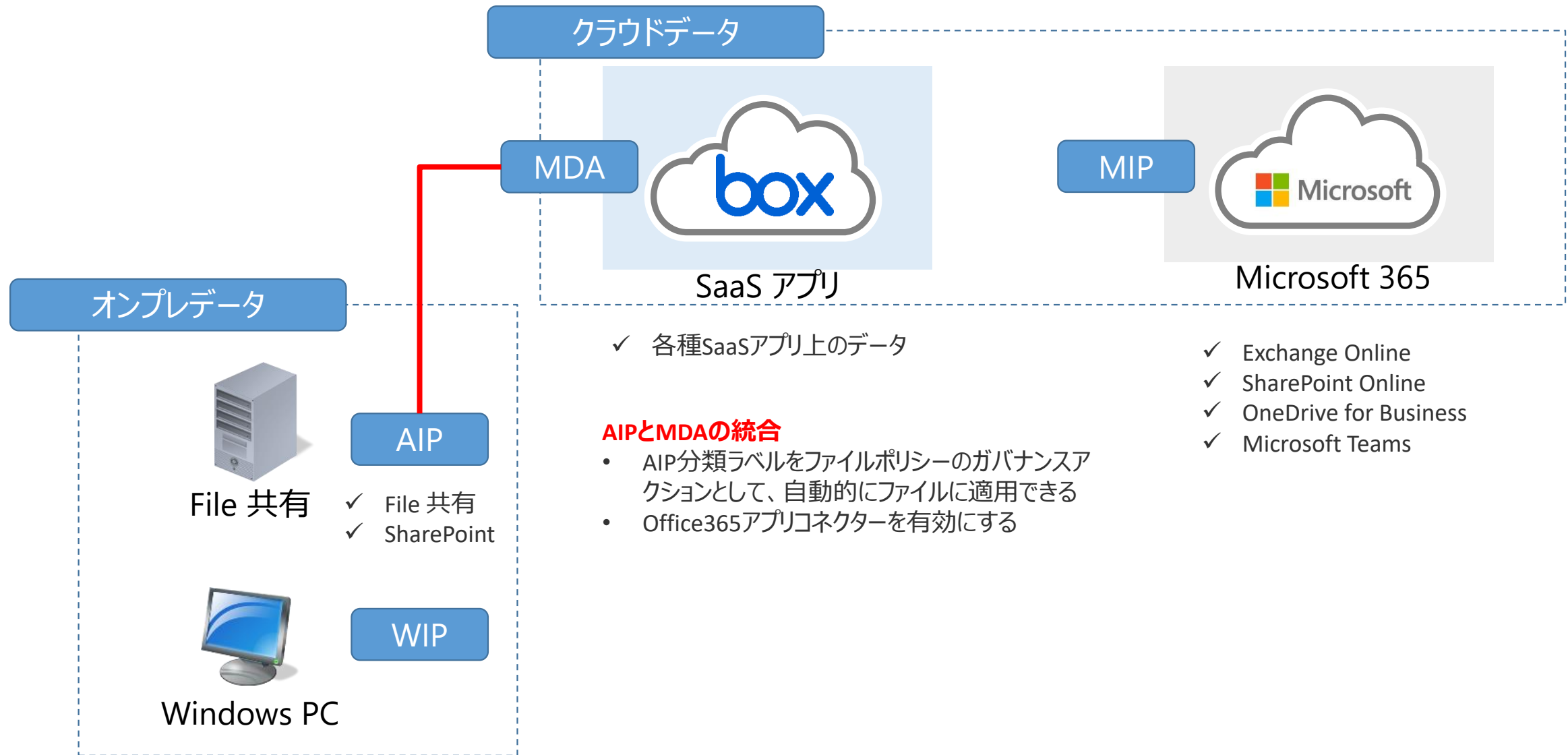


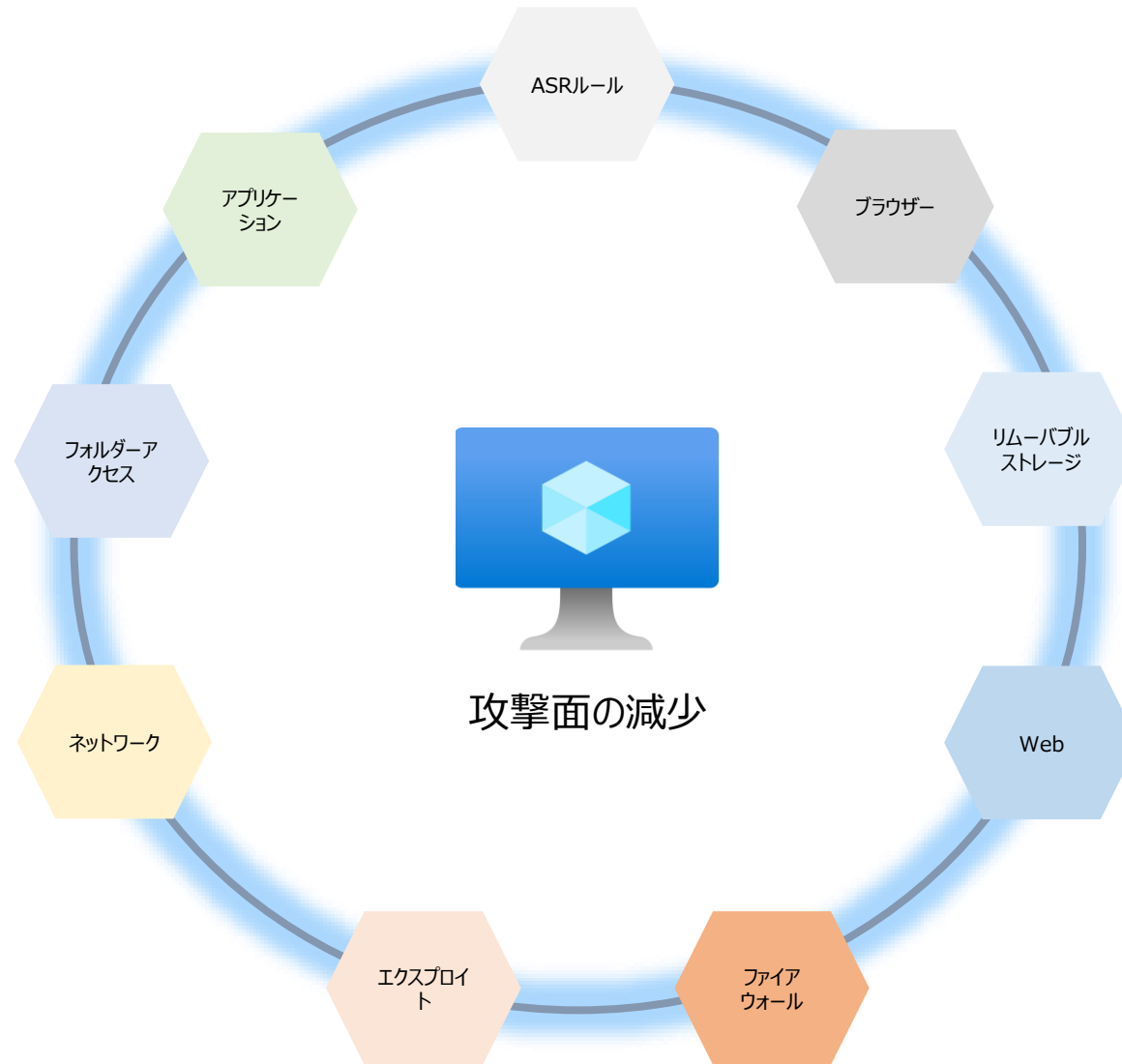
SaaS アプリ

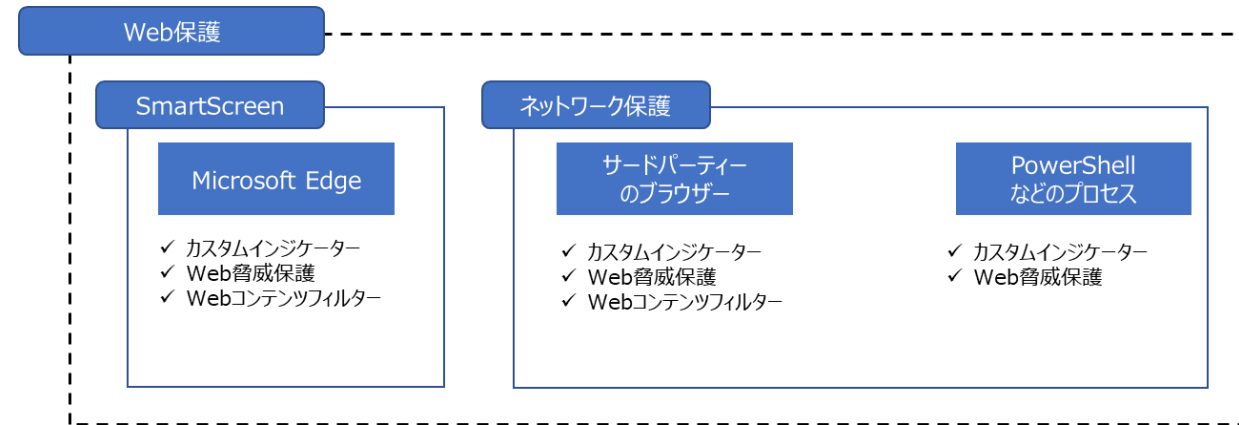
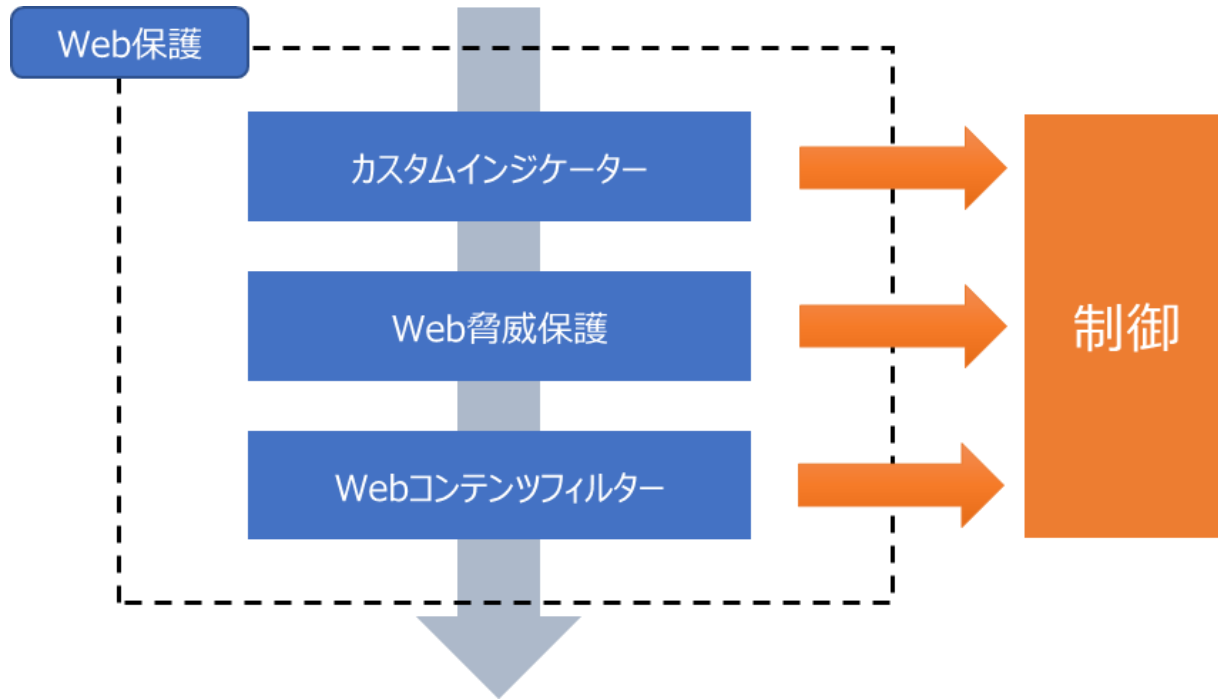
Microsoft 365
Information
Protection



Microsoft 365







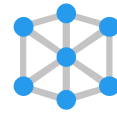
SIEM

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

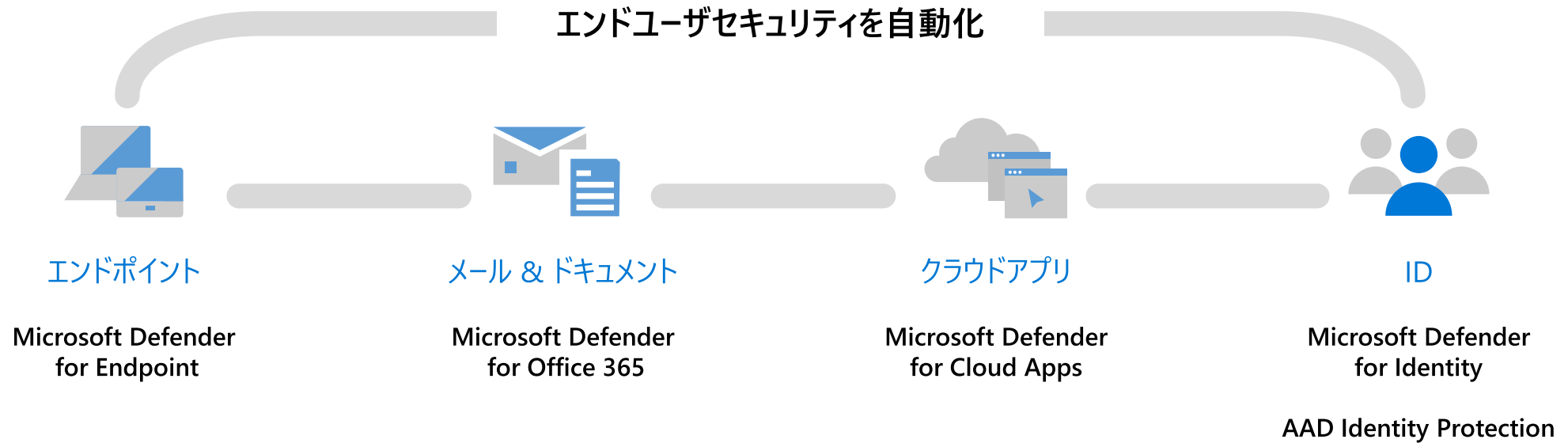
利用者環境の保護・検出

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



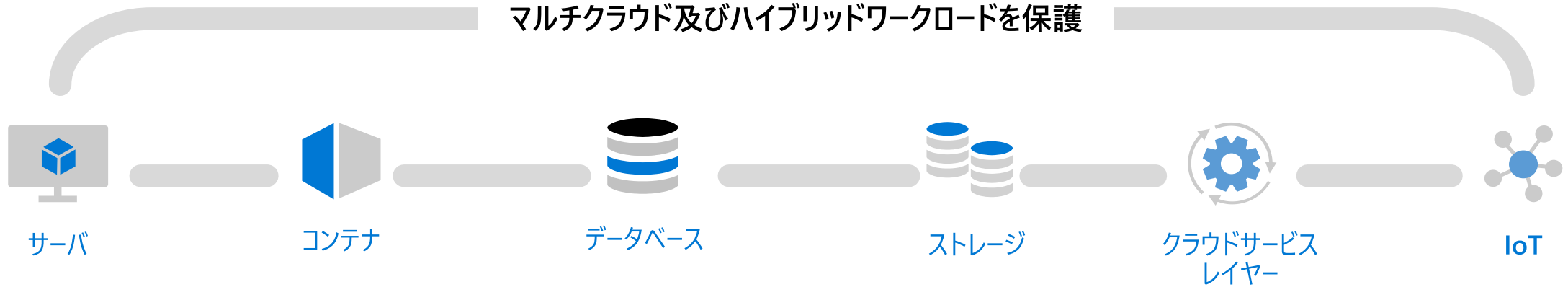
Windows

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

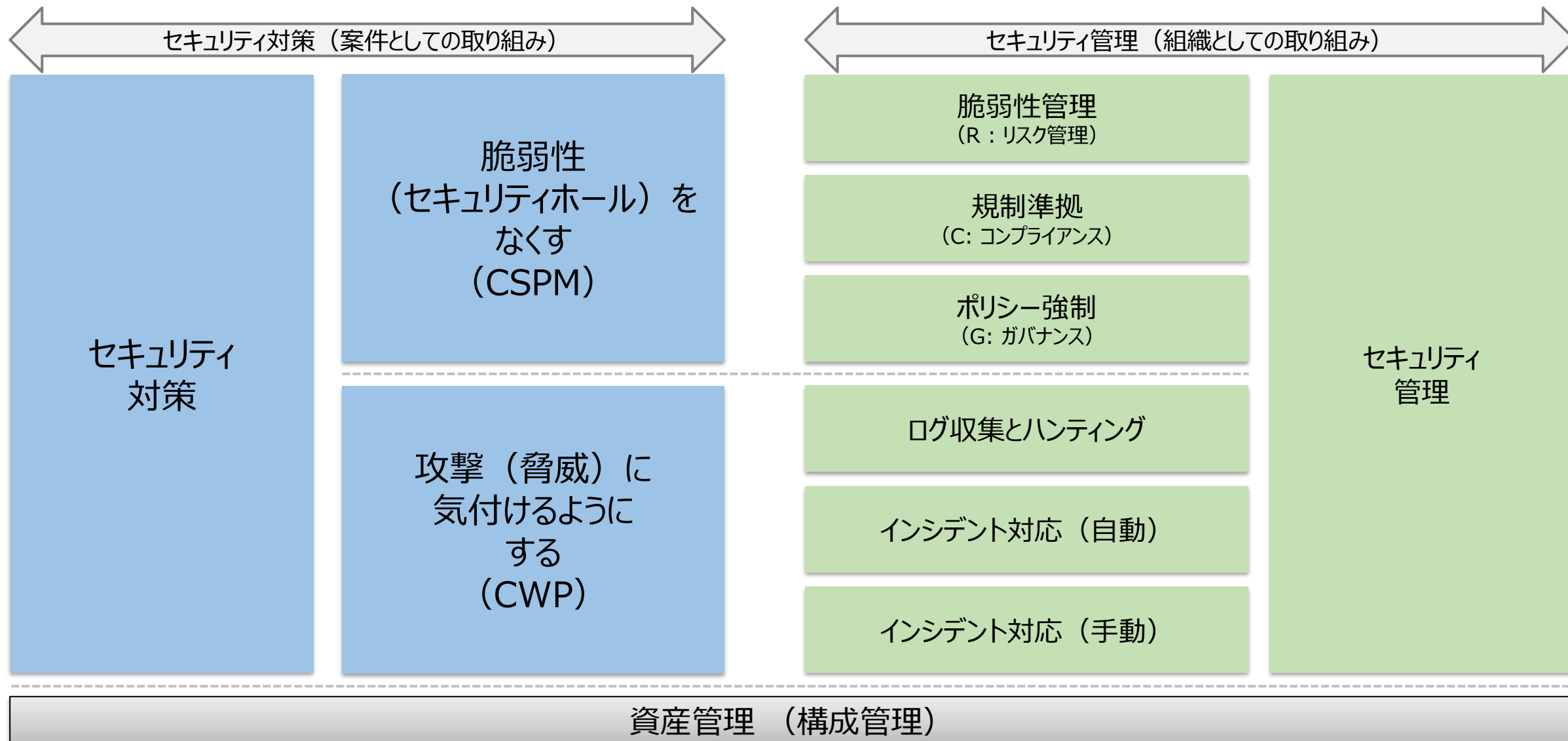


Microsoft Azure



Google Cloud

セキュリティガバナンスの考え方



Microsoft Defender for Cloud

ポリシー強制 (G: ガバナンス)



推奨事項や規制・コンプライアンスに対して、是正機能（Fix, Remediation）を提供

脆弱性（セキュリティホール）をなくす（CSPM）

- ✓ 推奨事項（Recommendations）
- ✓ クラウドサービスや VM 内の設定などに残っている構成設定上の脆弱性を、修正すべき推奨事項として示す

攻撃（脅威）に気付けるようにする（CWP）

- ! セキュリティ警告（Security alerts）
MDE や ASA（Adaptive Security Appliance）などの各種の攻撃検知システム（センサー）から報告された攻撃を通知する

脆弱性管理（R：リスク管理）

- ★ セキュリティ態勢（Security Posture）
各システム（サブスクリプション）でどの程度セキュリティ対策が行われているかを横並び比較する

規制準拠（C: コンプライアンス）

- 🏛️ 規制コンプライアンス（Regulatory Compliance）
業界標準として定義されている最低限行うべきセキュリティ対策をきちんと行っているかを確認・レポートする

Microsoft Defender for Cloud | 概要
サブスクリプション 'ME-MngEnv841187-naokiabe' を表示しています

検索

全般

- 概要
- はじめに
- 推奨事項
- 攻撃パスの分析
- セキュリティ警告
- インベントリ
- セキュリティグラフ
- ブック
- コミュニティ
- 問題の診断と解決

クラウド セキュリティ

- セキュリティ態勢
- 規制コンプライアンス
- ワークロード保護
- Firewall Manager
- DevOps security (preview)

管理

- 環境設定
- セキュリティ ソリューション
- ワークフローの自動化

サブスクリプション 新機能

表示されている情報が限られています

1
Azure サブスクリプション

セキュリティ態勢

11/11
未割り当て

セキュア スコア

56%
セキュア スコア

セキュリティ体制を調べる>

規制コンプライア

Defender プラン



設定 | Defender プラン ...

ME-MngEnv841187-naokiabe

検索



保存



自動プロビジョニング - 拡張機能

設定



Defender プラン



電子メールの通知



ワークフローの自動化



連続エクスポート

ポリシー設定



セキュリティポリシー



ガパナンス ルール

すべて有効にする

Cloud Security Posture Management (CSPM)

Microsoft Defender CSPM provides advanced security posture capabilities including agentless vulnerability scanning, data-aware security posture, the cloud security graph, and advanced threat hunting. Pricing is based on subscription size, with billing applying only for Servers, Databases, and Storage resources at \$5/Billable resource/month. Foundational CSPM includes asset discovery, continuous assessment and security recommendations for posture hardening and a Secure score which measure the current status of your organization's posture.

| Microsoft Defender for | プラン / 価格 | リソースの数 | 構成 | 状態 |
|------------------------|---|-------------|----------------------------------|--|
| Foundational CSPM | Free 詳細 > | | 完全に構成済み | <input type="radio"/> オン <input type="radio"/> オフ |
| Defender CSPM | \$5/Billable resource/Month, 2023 年 8 月 1 日までは無料 詳細 > | 8 resources | 完全に構成済み 構成の編集 | <input checked="" type="radio"/> オン <input type="radio"/> オフ |

Cloud Workload Protection (CWP)

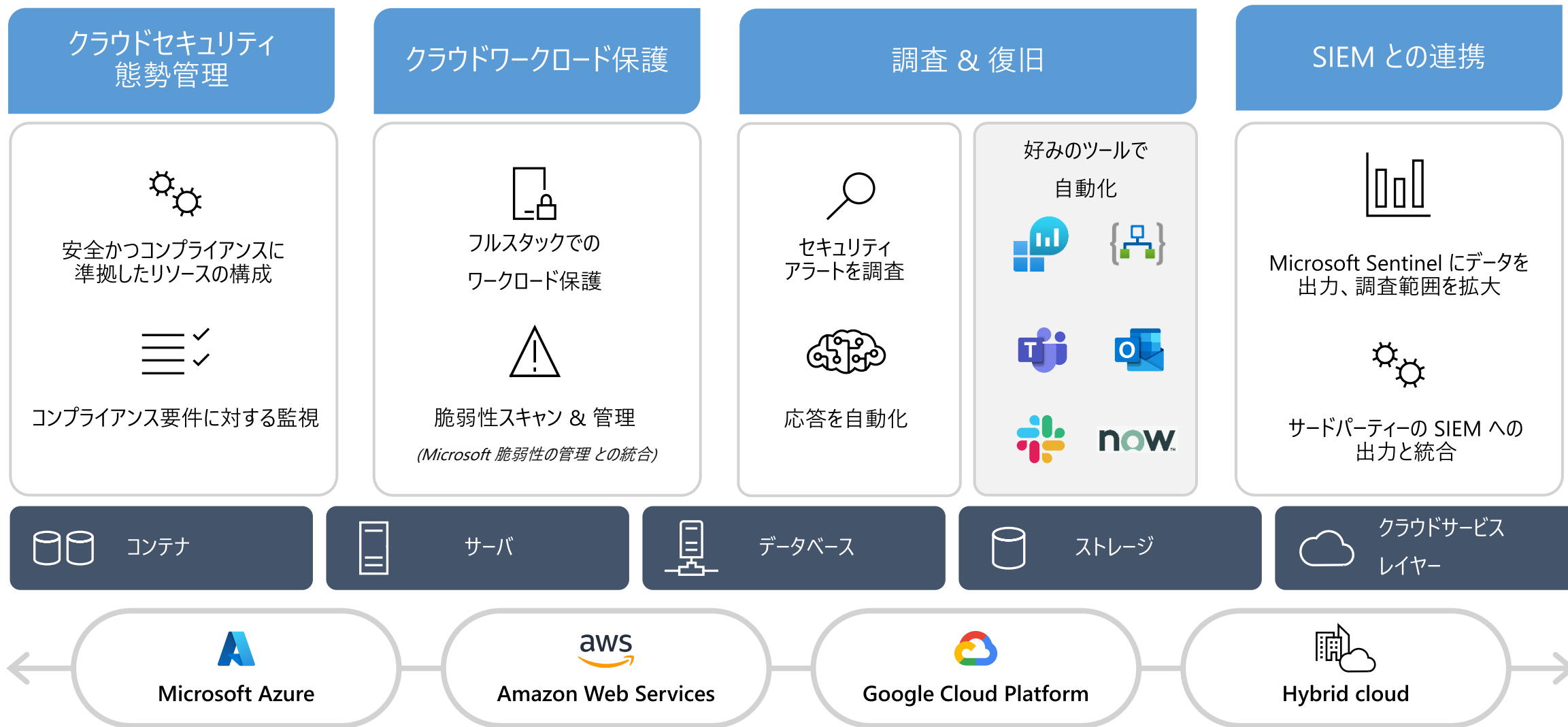
Microsoft Defender for Cloud provides comprehensive, cloud-native protections from development to runtime in multi-cloud environments.

| Microsoft Defender for | プラン / 価格 | リソースの数 | 構成 | 状態 |
|------------------------|---|------------------------------------|----------------------------------|--|
| サーバー | プラン 2 (\$15/サーバー/月) プランの変更 > | 4 台のサーバー | 一部構成済み 構成の編集 | <input checked="" type="radio"/> オン <input type="radio"/> オフ |
| App Service | \$15/インスタンス/月 詳細 > | 0 個のインスタンス | 完全に構成済み | <input checked="" type="radio"/> オン <input type="radio"/> オフ |
| データベース | 選択済み: 4 個中 4 個 種類の選択 > | 保護済み: 1 個中 1 個のインスタンス | 完全に構成済み 構成の編集 | <input checked="" type="radio"/> オン <input type="radio"/> オフ |
| ストレージ | \$10/Storage account/month On-upload malware scanning (\$0.15/GB) 詳細 > | 5 個のストレージ アカウント | 完全に構成済み 構成の編集 | <input checked="" type="radio"/> オン <input type="radio"/> オフ |
| コンテナ | \$7/月あたりの VM コア 詳細 > | 0 個のコンテナ レジストリ; 0 個の Kubernetes コア | 一部構成済み 構成の編集 | <input checked="" type="radio"/> オン <input type="radio"/> オフ |
| Kubernetes (非推奨) | 2 ドル/月あたりの VM コア | 0 個の Kubernetes コア | 完全に構成済み | <input checked="" type="radio"/> オン <input type="radio"/> オフ |
| コンテナ レジストリ (非推奨) | \$0.29/画像 | 0 個のコンテナ レジストリ | 完全に構成済み | <input checked="" type="radio"/> オン <input type="radio"/> オフ |
| Key Vault | 0.02 ドル/10K トランザクション 新しいプランが利用可能です | 1 個のキー コンテナ | 完全に構成済み | <input checked="" type="radio"/> オン <input type="radio"/> オフ |
| Resource Manager | 4 ドル/1M のリソース管理操作 新しいプランが利用可能です | | 完全に構成済み | <input checked="" type="radio"/> オン <input type="radio"/> オフ |
| APIs | 無料 (プレビュー) 詳細 > | 0 Azure API Management services | Action required | <input checked="" type="radio"/> オン <input type="radio"/> オフ |

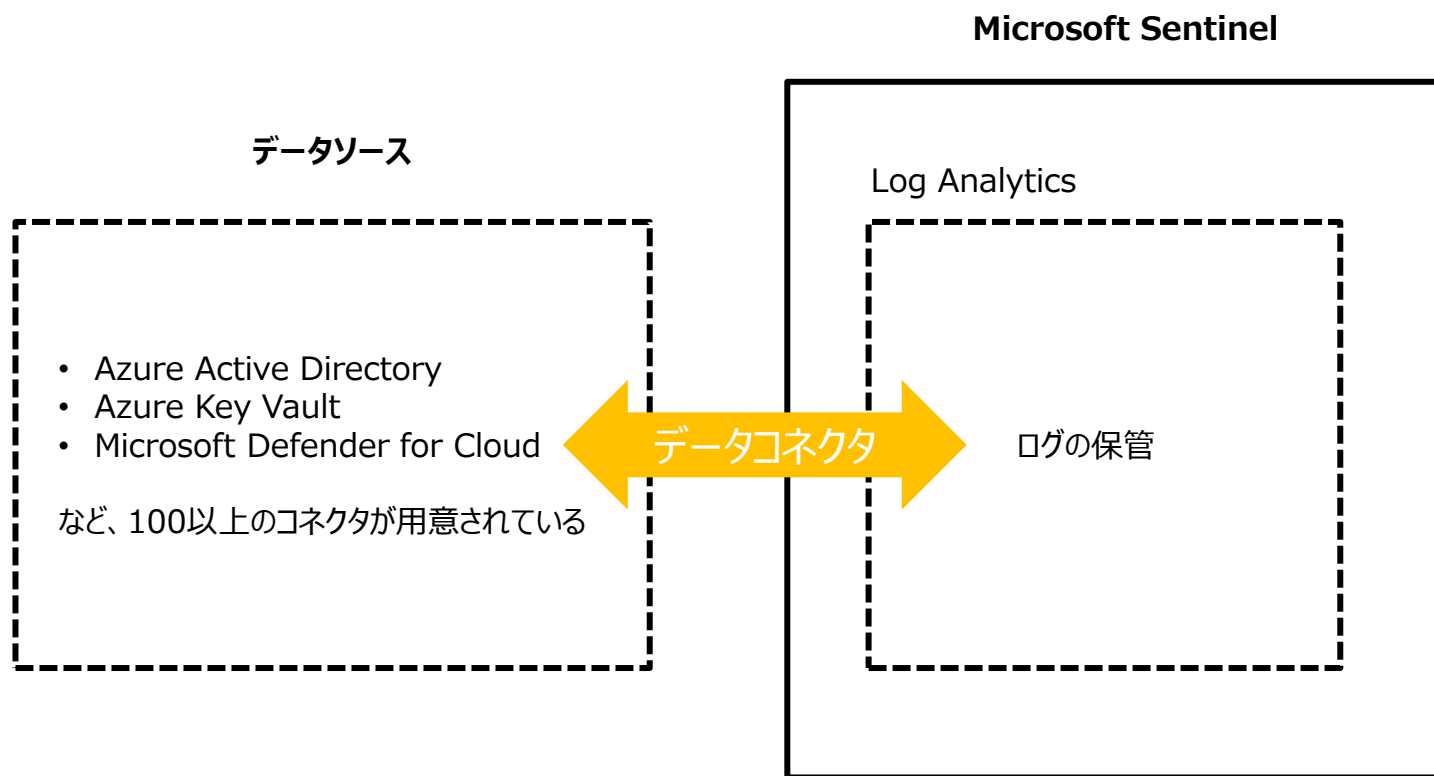
CSPM



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があります。)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

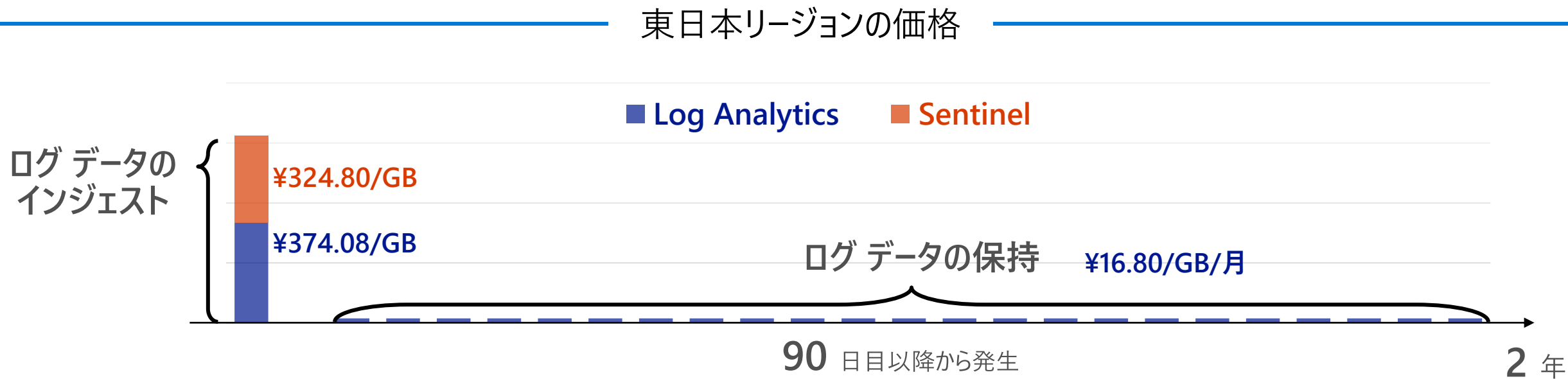
実害が発生するポイント

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

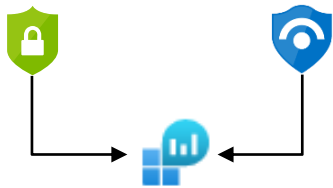
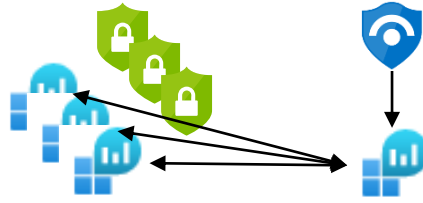
| | | | |
|--|------------------------------|---|---|
| Office 365 | OfficeActivity | 無償 | 全体管理者 セキュリティ管理者 |
| Azure AD | SigninLogs | | 全体管理者 セキュリティ管理者 |
| | AuditLogs | | |
| Microsoft 365 Defender | DeviceInfo | | 全体管理者 セキュリティ管理者 |
| | DeviceNetworkInfo | | |
| | DeviceProcessEvents | | |
| | DeviceNetworkEvents | | |
| | 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

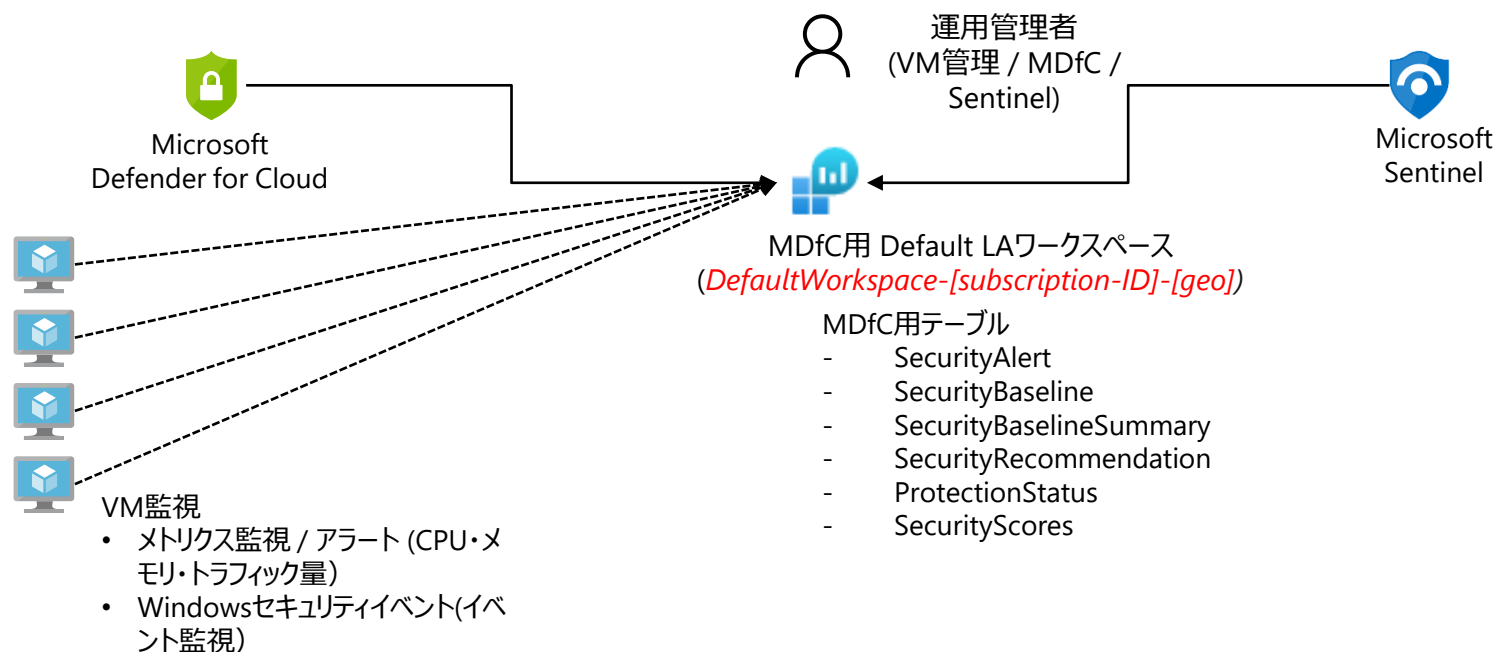
それぞれメリット/デメリットがあるため、お客様の運用要件を検討の上で検討していただきたい

| 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">設計/運用が用意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仮想マシンの Windows Security Event Logs の課金は 500 MB /日 まで無料 | <ul style="list-style-type: none">Sentinelを要件・サービス毎に分割するケースには使えない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 | 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">大規模なお客様ではSentinelの管理が分かれるので、別にする個別にワークスペースのアクセス制御が可能（MDfC / Sentinel）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 | <ul style="list-style-type: none">管理が大変になる（複数のLAワークスペース）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 | 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

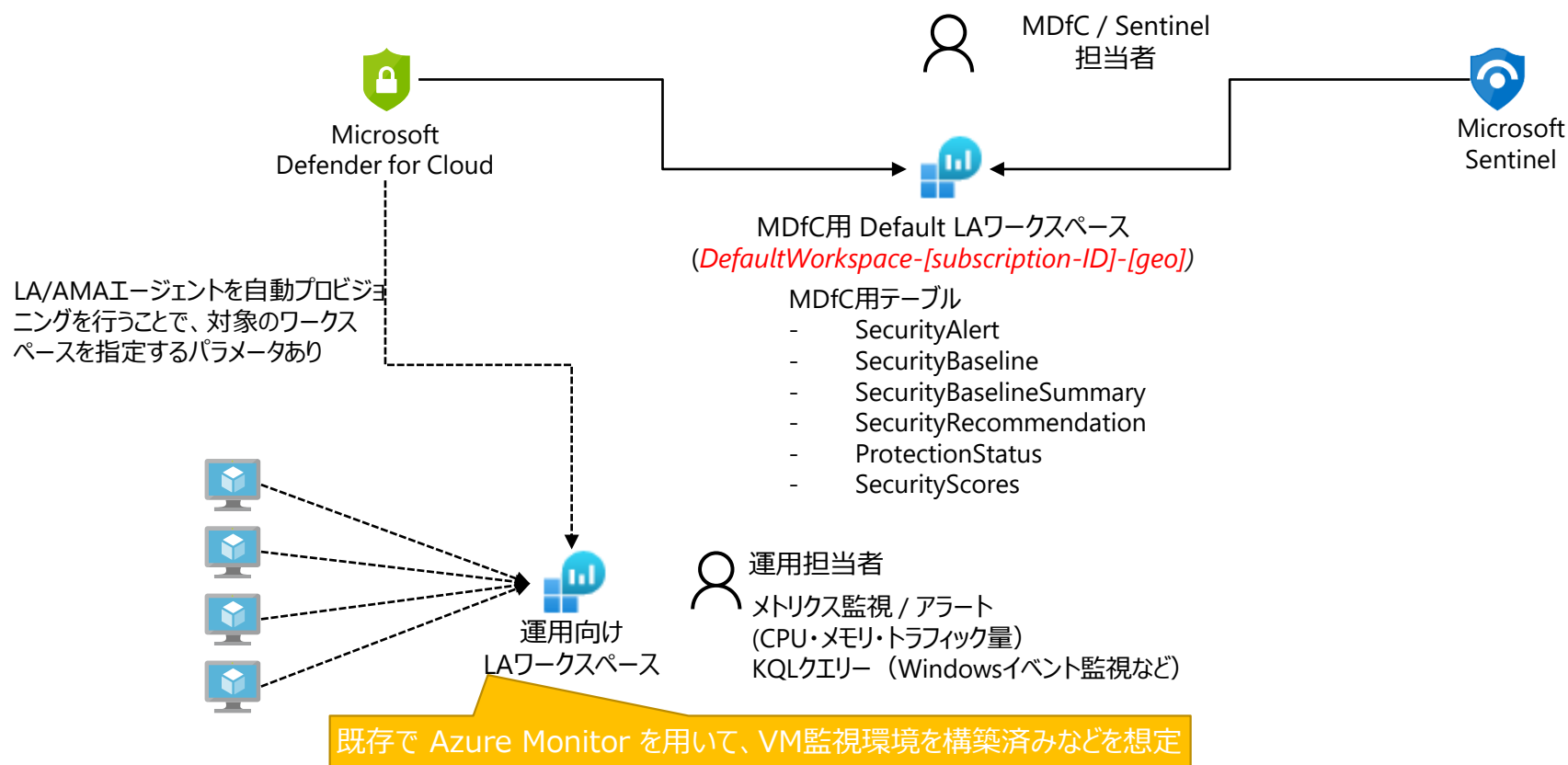
- MDfC / Sentinel のワークスペースを統合して管理する設計は以下の通り
- VM の運用、MDfC、Sentinel を一つの Log Analytics ワークスペースで一元管理する



[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

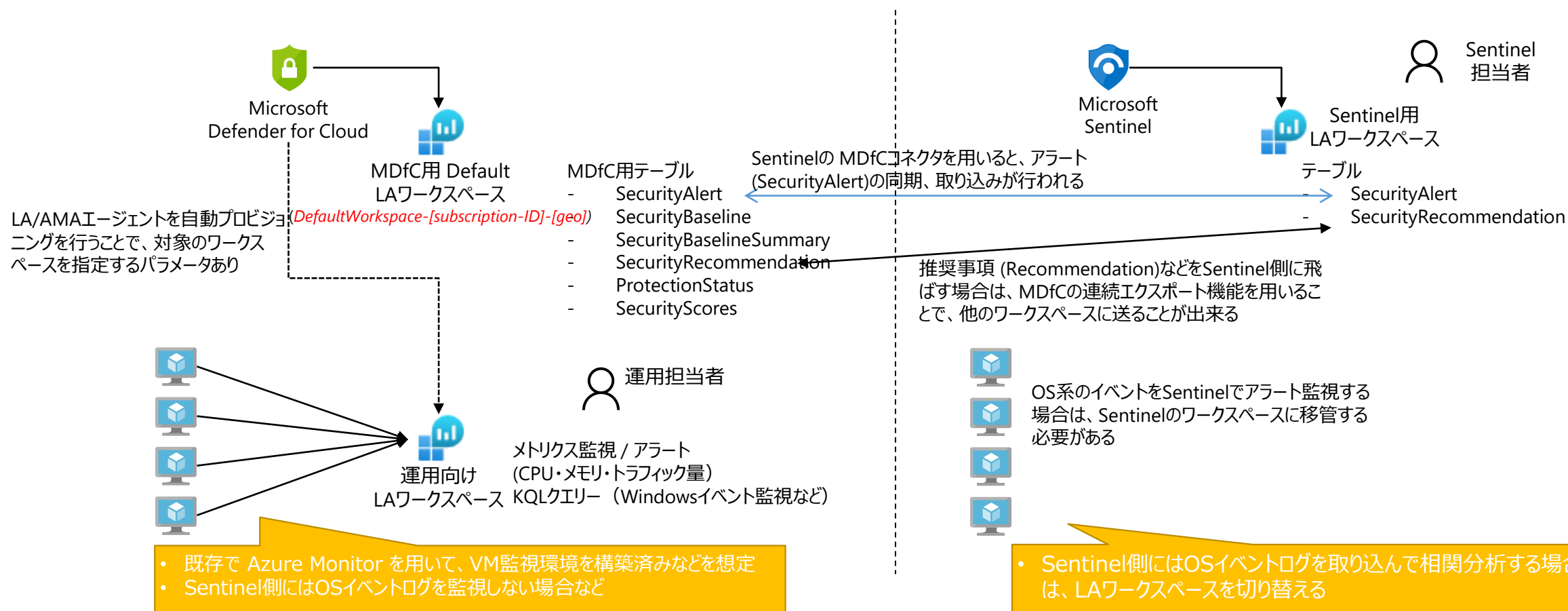
- MDfC / Sentinel のワークスペースを統合して管理する設計は以下の通り。
- VM の運用については、専用のワークスペースで管理する
- MDfC、Sentinel を一つの Log Analytics ワークスペースで一元管理する



[補足] MDfC LogAnalytics ワークスペース設計

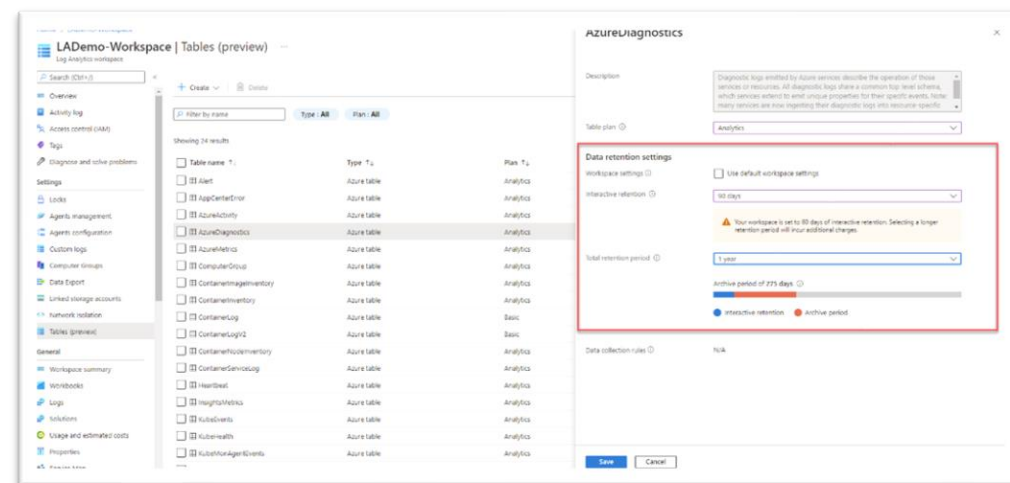
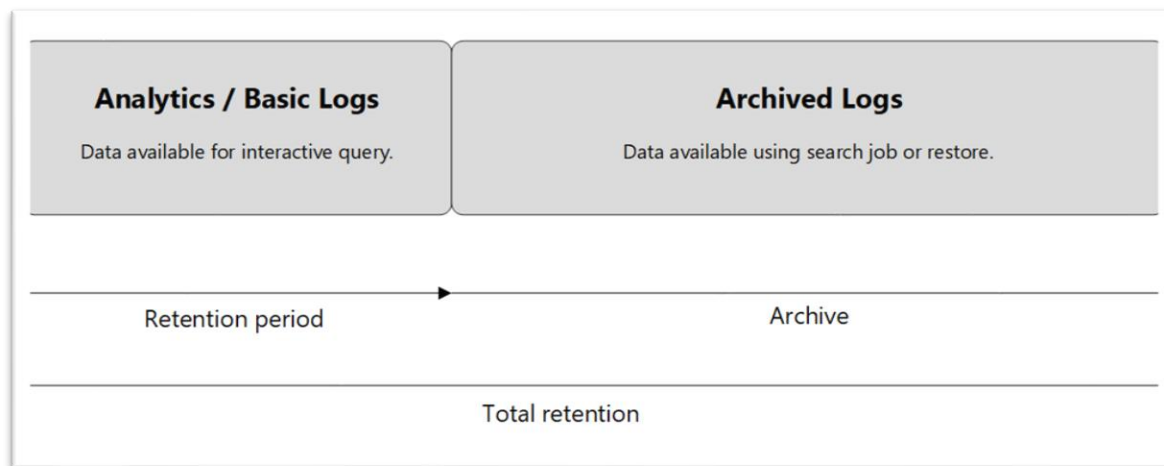
MDfC / Sentinel のワークスペースを別で管理する

- 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。



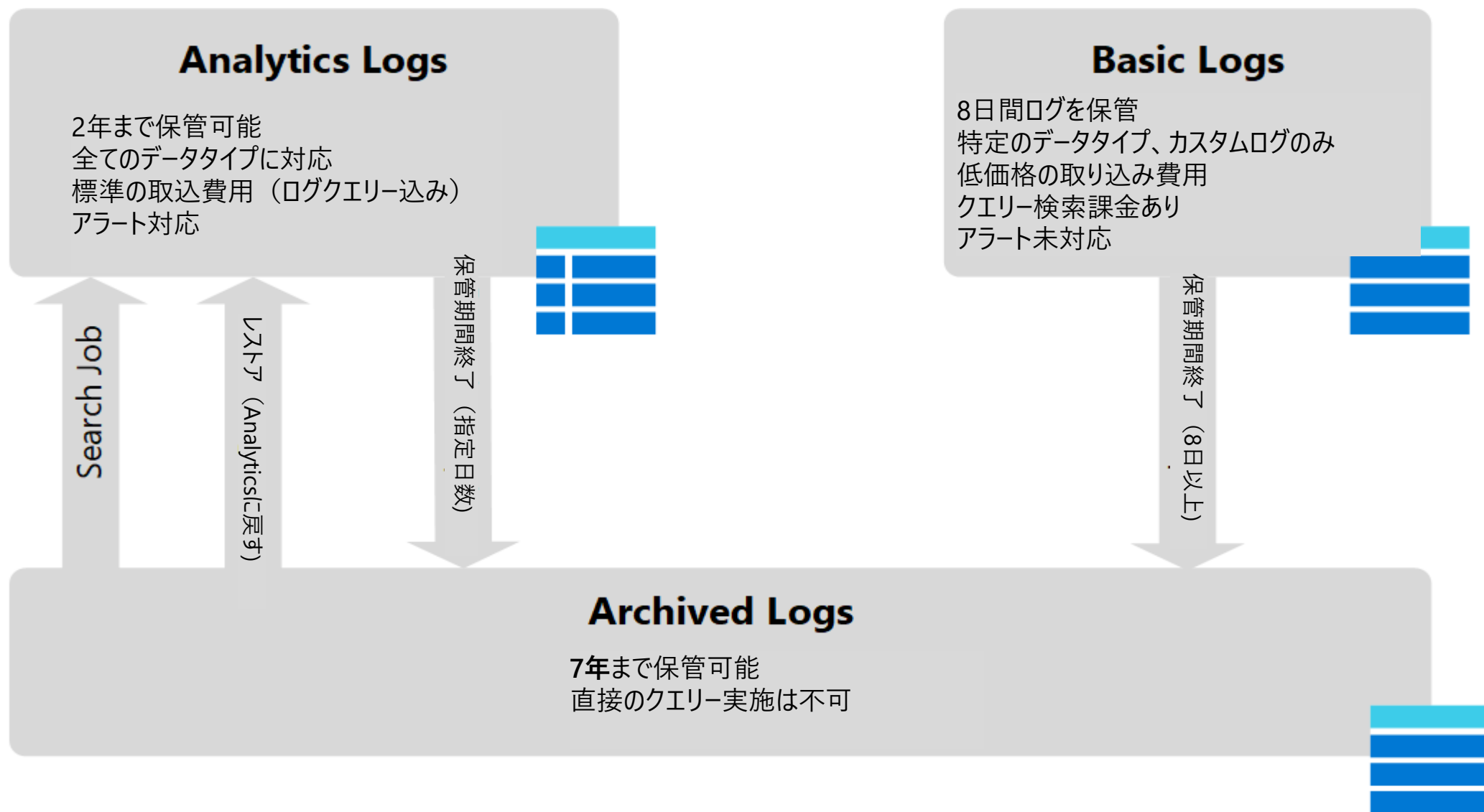
Log Analytics ネイティブ機能によるログの長期保管

- 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。



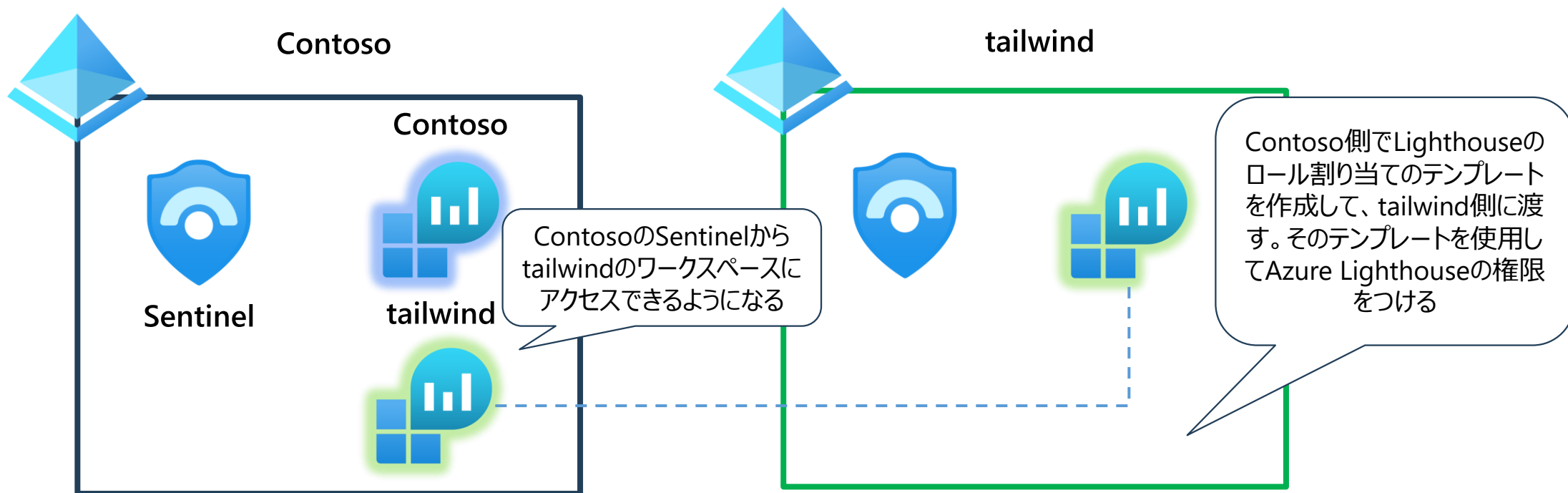
[参考] Log Analytics ワークスペース Basic / Archived ログの相関関係

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。



Azure Lighthouse

- 別テナントのリソースを管理することができる仕組み
 - Microsoft Sentinel ではこの仕組みを使用して、顧客のSentinel ワークスペースを管理することができる。
 - 具体的には、管理側のアカウントを自組織のロールを割り当てる



ワークスペースマネージャー

- 中央ワークスペースの設定を、メンバーワークスペースに反映させることができる
 - 分析ルール
 - アクティブな規則（規則のテンプレートは対象外）
 - 自動化ルール（プレイブックは対象外）
 - パーサー、保存された検索、機能
 - ハンティングクエリとライブストリームクエリ
 - ワークブック

