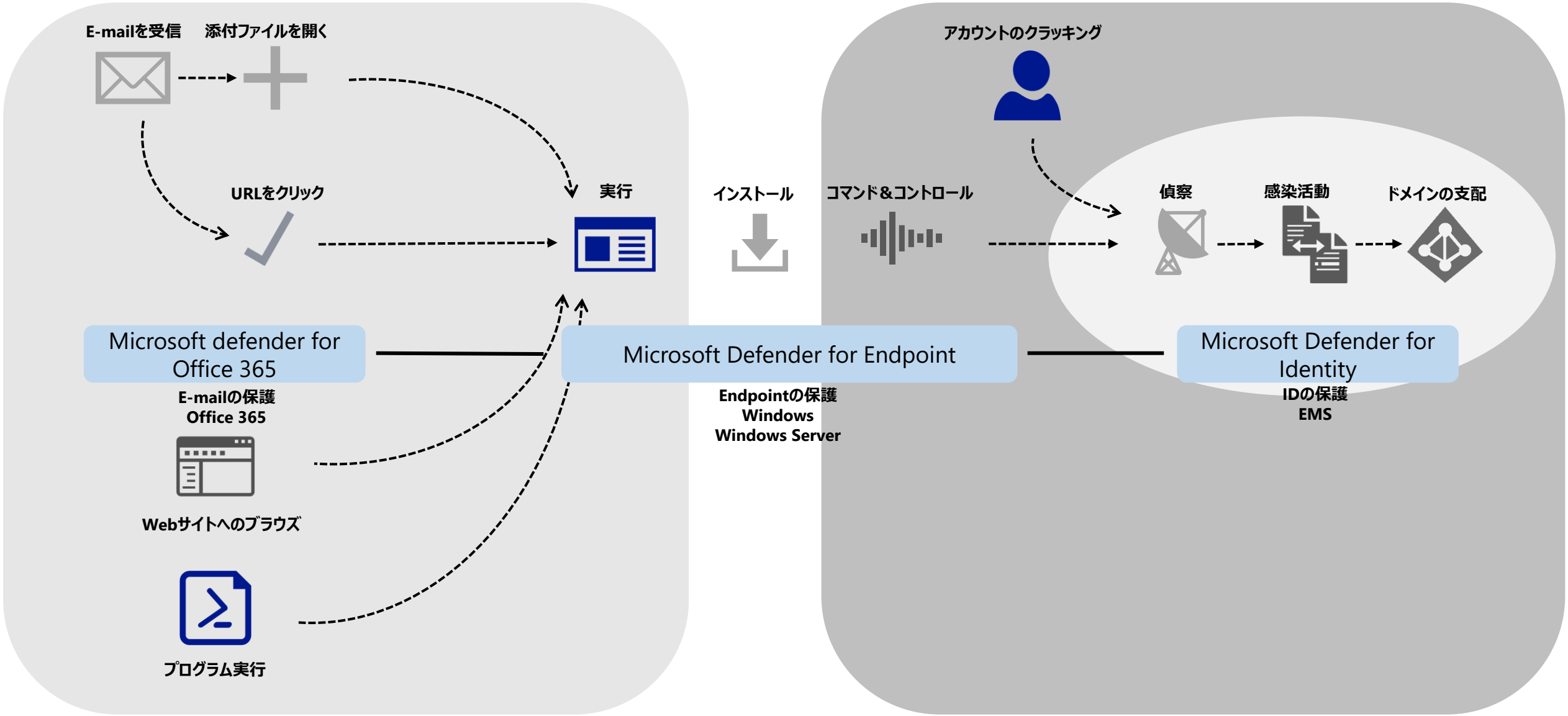
SC-200

補足資料

Microsoft 365 Defender の整理

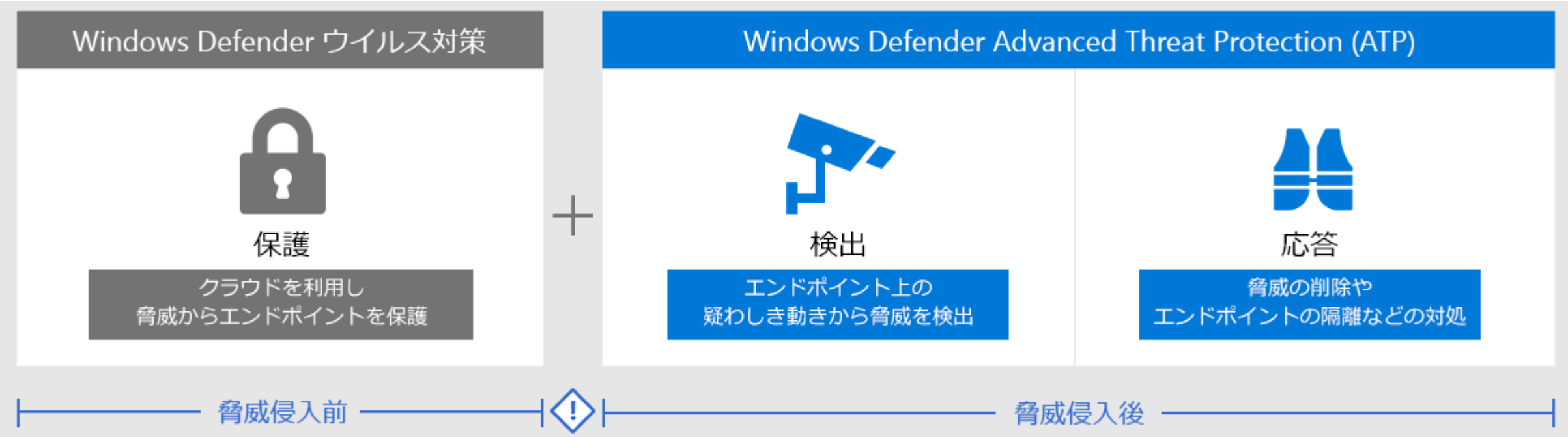
Windows 端末	Microsoft Defender for Endpoint	エンドポイントの保護
Microsoft ID	Microsoft Defender for Identity	IDの保護
Office 365	Microsoft defender for Office 365	E-mailの保護
Cloud App	Microsoft Cloud App セキュリティ	クラウドアプリの保護

攻撃段階全体を通して検出範囲を最大限にする



Microsoft Defender for Endpoint 4

- 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

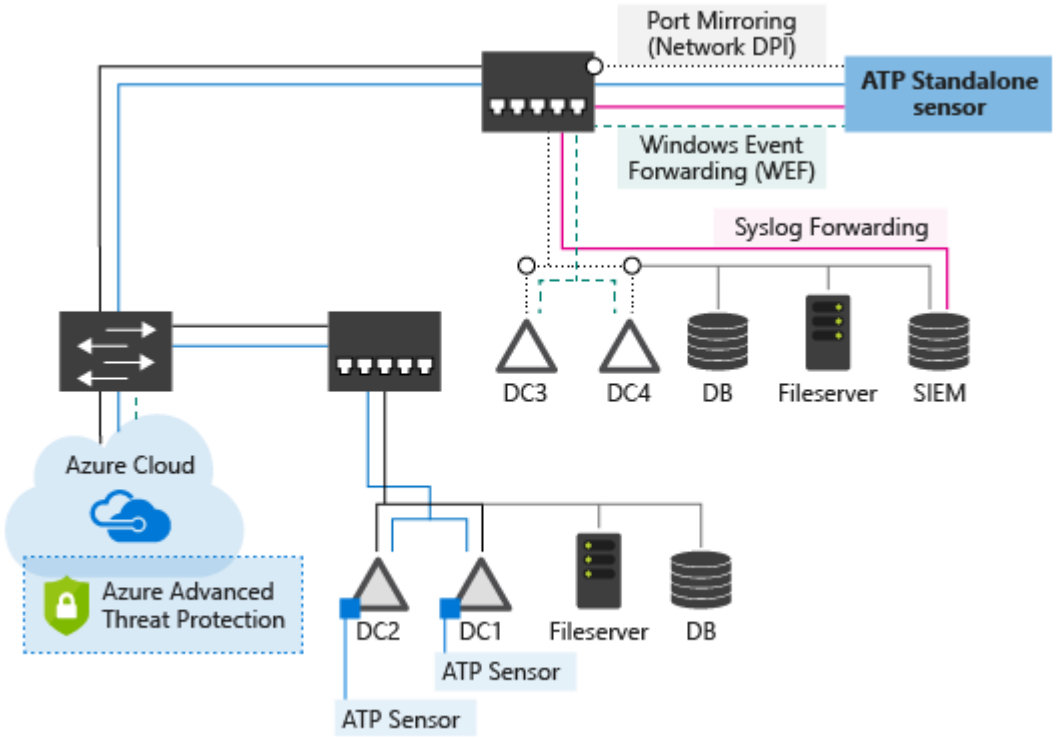


Microsoft Defender for Identity

- 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

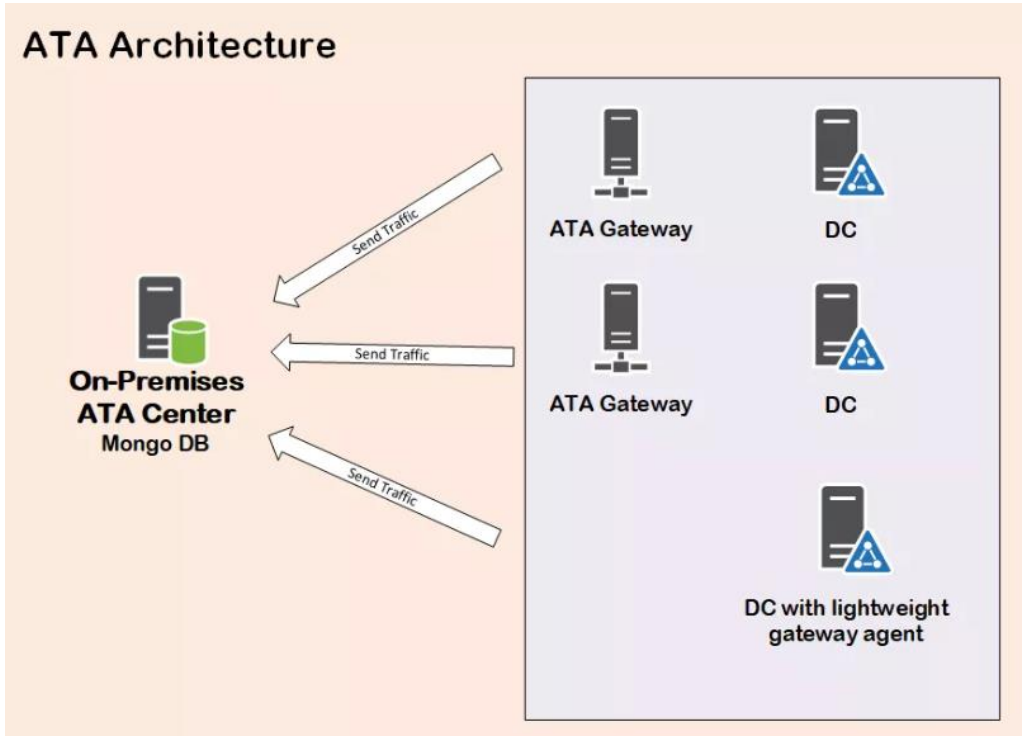
悪意のある攻撃、異常な動作、セキュリティの問題とリスクの主な種類の攻撃を検出

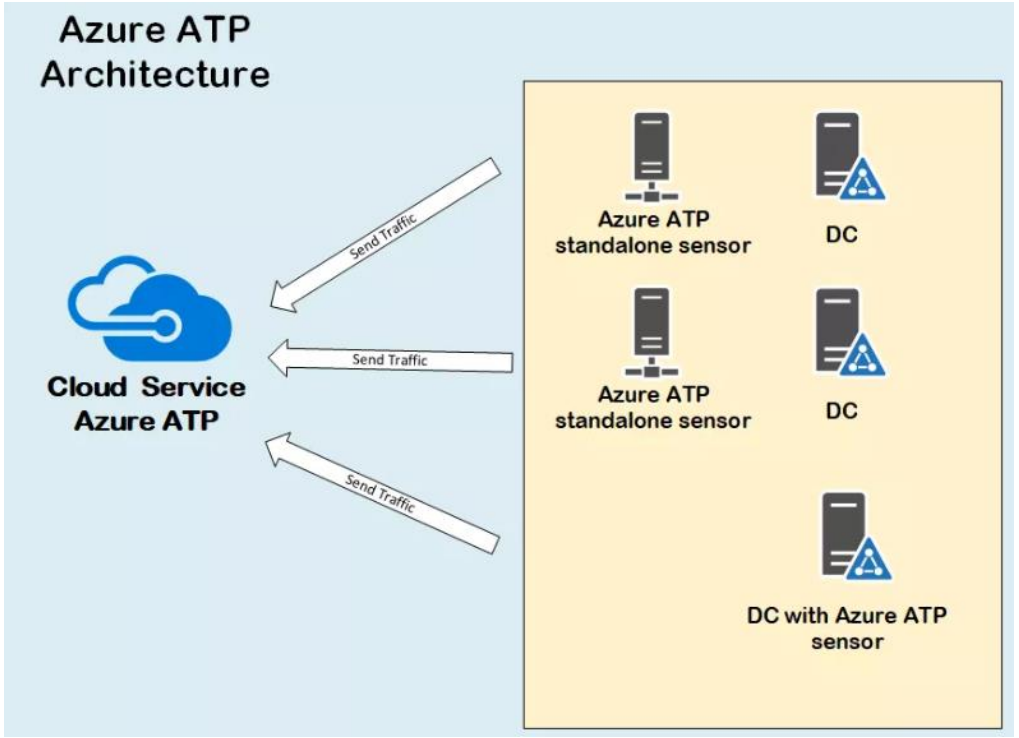
- ✓ Pass-the-Ticket (PtT)
- ✓ Pass-the-Hash (PtH)
- ✓ Overpass-the-Hash
- ✓ 偽造 PAC (MS14 068)
- ✓ ゴールデン チケット
- ✓ 悪意のあるレプリケーション
- ✓ ディレクトリ サービス列挙
- ✓ SMB セッション列挙
- ✓ DNS 偵察
- ✓ 水平ブルート フォース
- ✓ 垂直ブルート フォース
- ✓ スケルトン キー
- ✓ 不自然なプロトコル
- ✓ 暗号化のダウングレード
- ✓ リモート実行
- ✓ 悪意のあるサービスの作成



（参考）Microsoft advanced threat analytics

- 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





Microsoft defender for Office 365（1/2）

- クラウドベースの電子メール フィルタリング サービスであり、堅牢なゼロデイ保護を提供して未知のマルウェアやウイルスから組織を保護するのに役立ち、リアルタイムで有害なリンクから組織を保護する機能が含まれている
- 多機能なレポート機能と URL トレース機能があるので、管理者は組織内で発生する攻撃の種類を見極めることができる
- Office 365 ATA から名称変更

Exchange Online Protection

- EOPはアンチスパム・アンチマルウェア機能を備えたクラウドベースの無害化システム。EOPはForefront Online Protection for Exchange（FOPE）に代わる新しい製品。
- EOPは以下の3つの環境に対応する設定が必要
  - ✓ クラウドのみ
  - ✓ オンプレミスのみ
  - ✓ ハイブリッド
- クラウドのみの場合、EOPはExchnage Online の一部として実装する。

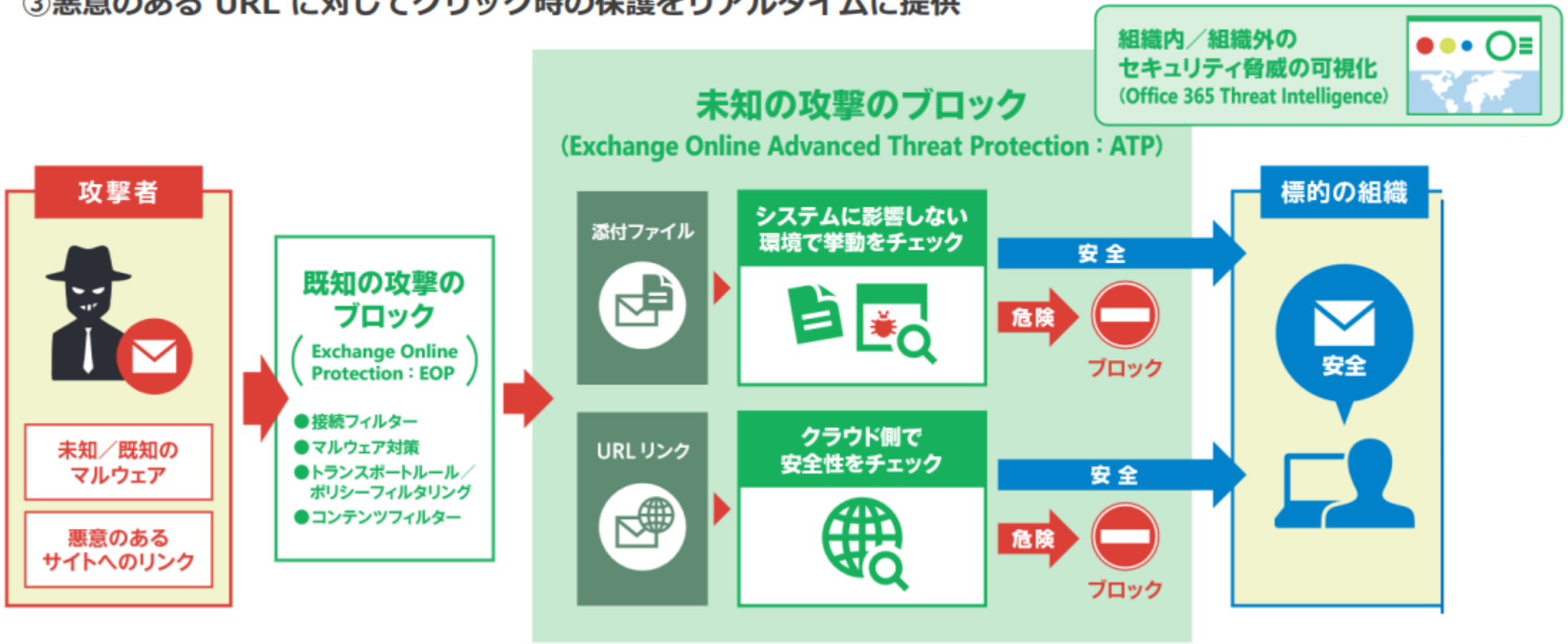
機能	ATP スタンドアロン	Exchange Online Protection
リンク保護	はい	いいえ
添付ファイル保護	はい	いいえ
スプーフィング インテリジェンス	はい	いいえ
検疫	はい	はい
高度なフィッシング詐欺対策機能	はい	いいえ

Microsoft defender for Office 365（2/2）

①既知のマルウエア（ウイルス）に対する保護

②未知のマルウェア（ウイルス）に対する保護

③悪意のある URL に対してクリック時の保護をリアルタイムに提供



サイバーキルチェーンとは

- 米国ロッキードマーチン社が提唱（2009年）
- 標的型攻撃における一連の流れを7つのプロセスに分け、軍事的なシナリオに置き換えたもの

1	偵察(Reconnaissance)
2	武器化(Weponization)
3	デリバリ(Delivery)
4	エクスプロイト(Compromise/Exploit)
5	インストール(Infection/Installation)
6	コマンド＆コントロール（C&C）(Command and Control)
7	目的の実行(Objectives/Exfiltration)

サイバーキルチェーン 3.0 とは

- 米国ウォッチガード・テクノロジー社が提唱
- サイバーキルチェーンをベースに近年の標的型攻撃に即したモデルとして、「武器化」フェーズを削除し、「感染活動」を追加した

サイバーキルチェーンに基づく多層防御

偵察 Reconnaissance	配送 Delivery	攻撃 Exploitation	インストール Install	遠隔操作 Command & Control	侵入拡大 Lateral Movement	目的達成 Objectives
Protect	**なりすまし メール着弾** 悪意のある添付ファイルや悪意のあるサイトに誘導するための URL が記載されたメールが着弾	**悪意のあるサイトへの誘導** 悪意のあるサイトへ誘導してバックドアを仕込む **悪意のある Office マクロやスクリプトの利用** 攻撃者のサーバーに接続するためのツールとして悪用 **拡張子を偽装した添付ファイルの利用 (RLO 攻撃)** Exe を実行させるために拡張子を右から左に変更し、アイコンを Office や PDFに偽装する	**既知のマルウェア** ウイルス、ワーム、トロイの木馬、スパイウェアなど既知のマルウェア攻撃 **ランサムウェア** データを暗号化し暗号化解除に仮想通貨での支払いを要求する **ファイルレス攻撃** 実行ファイルを利用せず、Power Shell やコマンドなど正規のプログラムを攻撃に活用 **正規のプロセスになりすまして攻撃** プロセスホロウィングなど正規のプロセスに偽装して攻撃を行う	**不審な IP アドレスとの通信** ハッカーのサーバへの通信を確立させ攻撃を継続化させる **攻撃の持続性確保** タスクスケジューラやレジストリの変更により攻撃の持続性を確保	**OS の脆弱性を利用した権限の昇格** MS14-068やMS11-013 の悪用など **他の端末に不正アクセス** Mimikaz や psexec などのツールを使用し、Pass the Hash や Pass the Ticket を利用した不正アクセスを実施 **ドメインを乗っ取るためのネットワークの内部調査** 同じネットワークにいる端末に横展開するための偵察行為	**ドメイン侵害** ドメイン Admin の資格情報を保有する端末に不正アクセスし資格情報を不正に取得
Detect						
Response						

サイバーキルチェーンに基づく多層防御

	偵察 Reconnaissance	配送 Delivery	攻撃 Exploitation	インストール Install	遠隔操作 Command & Control	侵入拡大 Lateral Movement	目的達成 Objectives
Protect		**Office 365 ATP** サンドボックス環境で添付ファイルを実行し不正な動きをするか確認	**Office 365 ATP** 不正なリンクへの誘導を防御 **Windows Defender Application Guard** セキュアブラウザにより不正サイトを介した攻撃を防御 **Windows Defender Exploit Guard** Attack Surface Reduction	**Windows Defender Antivirus** 既知のマルウェア検知、Cloud Protection による未知のマルウェアの検知 **Windows Defender Exploit Guard** Controlled Folder Access **Windows Defender Exploit Guard** Attack Surface Reduction	**Windows Defender Exploit Guard** Network Protection	**Windows Defender Credential Guard** Pass The Hash, Pass the Ticket からの防御 **Azure AD Identity Protection** ID侵害を検知自動ブロック	**Azure Information Protection** 情報の自動暗号化から情報漏洩時のトラッキングを可能 **Microsoft Cloud App Security** クラウドアプリのガバナンス強化、シャドーIT検知
Detect		**Threat Intelligence** Office 365 に届いたメールを削除可能	**Windows Defender ATP** RLO 攻撃を検知	**Windows Defender ATP** プロセスホロウィングなど正規のプロセスからの攻撃を検知	**Windows Defender ATP** バックドアなどの異常行動を検知	**Azure ATP** MS14-068 や MS11-013 のディレクトリサービスへの悪用などの検知 **Azure ATP** 列挙攻撃などの検知 **Azure ATP** Pass the Hash, Pass the Ticket などの検知	**Azure ATP** Golden Ticket や特権アカウントの不正な新規作成などの検知
Respond							

Windows Endpoint Security

Defender for Office 365セキュリティの概要

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

Exchange Online Protection (EOP)

防止・検出	調査	対応
提供されるテクノロジ: • 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 • 偽装の検出 • 管理者検疫 • 管理者とユーザーによる誤検知と検出漏れの報告 • URL およびファイルの許可/禁止 • レポート	• 監査ログ検索 • メッセージ追跡	• 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

Defender for Office 365 プラン 1

防止・検出	調査	対応
EOP に含まれるすべてのテクノロジに加えて: • 安全な添付ファイル • 安全なリンク • Microsoft Defender for Office 365 によるワークロードの保護 (例: SharePoint Online、Teams、OneDrive for Business) • メール、Office クライアント、Teams でのクリック時の保護 • Microsoft Defender for Office 365 のフィッシング詐欺対策 • ユーザーの偽装とドメインの偽装の保護 • アラートおよびアラート用 SIEM 統合 API	• 検出用 SIEM 統合 API • **リアルタイム検出ツール** • URL 追跡	• 同上

Defender for Office 365 プラン 2

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に加えて: • 同上	• **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	• 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 Information Protection

Windows Information Protection

Windows PC

Azure Information Protection

File 共有

Microsoft Cloud App Security

SaaS アプリ

Microsoft 365 Information Protection

Microsoft 365

MITRE ATT&CKフレームワーク

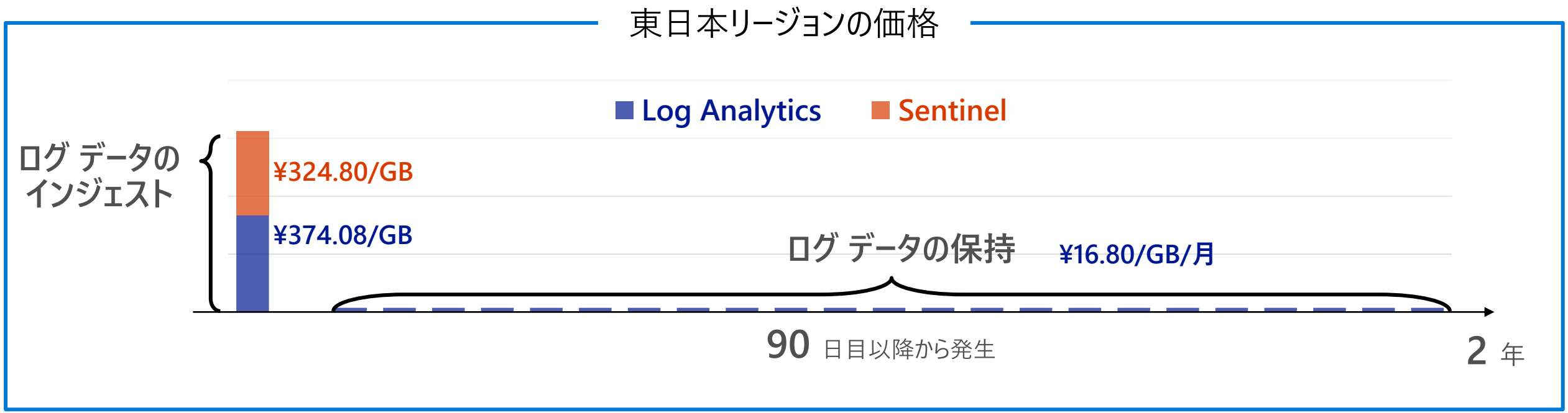
攻撃手法		概要
Initial Access	初期アクセス	攻撃者がネットワークに侵入しようとしている
Execution	実行	攻撃者が悪意のあるコードを実行しようとしている
Persistence	永続化	攻撃者が不正アクセスする環境を確保しようとしている
Privilege escalation	権限昇格	攻撃者がより高いレベルでの権限を取得しようとしている
Defense Evasion	防衛回避	攻撃者が検知されないようにしている
Credential Access	認証情報アクセス	攻撃者がアカウント名とパスワードを盗もうとしている
Discovery	探索	攻撃者がアクセス先の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 価格

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 AuditLogs	全体管理者 セキュリティ管理者
Microsoft 365 Defender		全体管理者 セキュリティ管理者
Microsoft Defender for Endpoint の生ログ	DeviceInfo DeviceNetworkInfo DeviceProcessEvents DeviceNetworkEvents DeviceFileEvents DeviceRegistryEvents DeviceLogonEvents DeviceImageLoadEvents DeviceEvents DeviceFileCertificateInfo	
Microsoft Defender for Office 365 の生ログ	EmailEvents EmailUrlinfo EmailAttachmentInfo EmailPostDeliveryEvents	
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	
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	

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 McasShadowItReporting	全体管理者 セキュリティ管理者
Azure Information Protection	SecurityAlert 無償 InformationProtectionLogs_CL	全体管理者 セキュリティ管理者 Azure Information Protection管理者

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