Microsoft Security

Microsoft Sentinel Incident experience

Public Preview

Microsoft Corporation

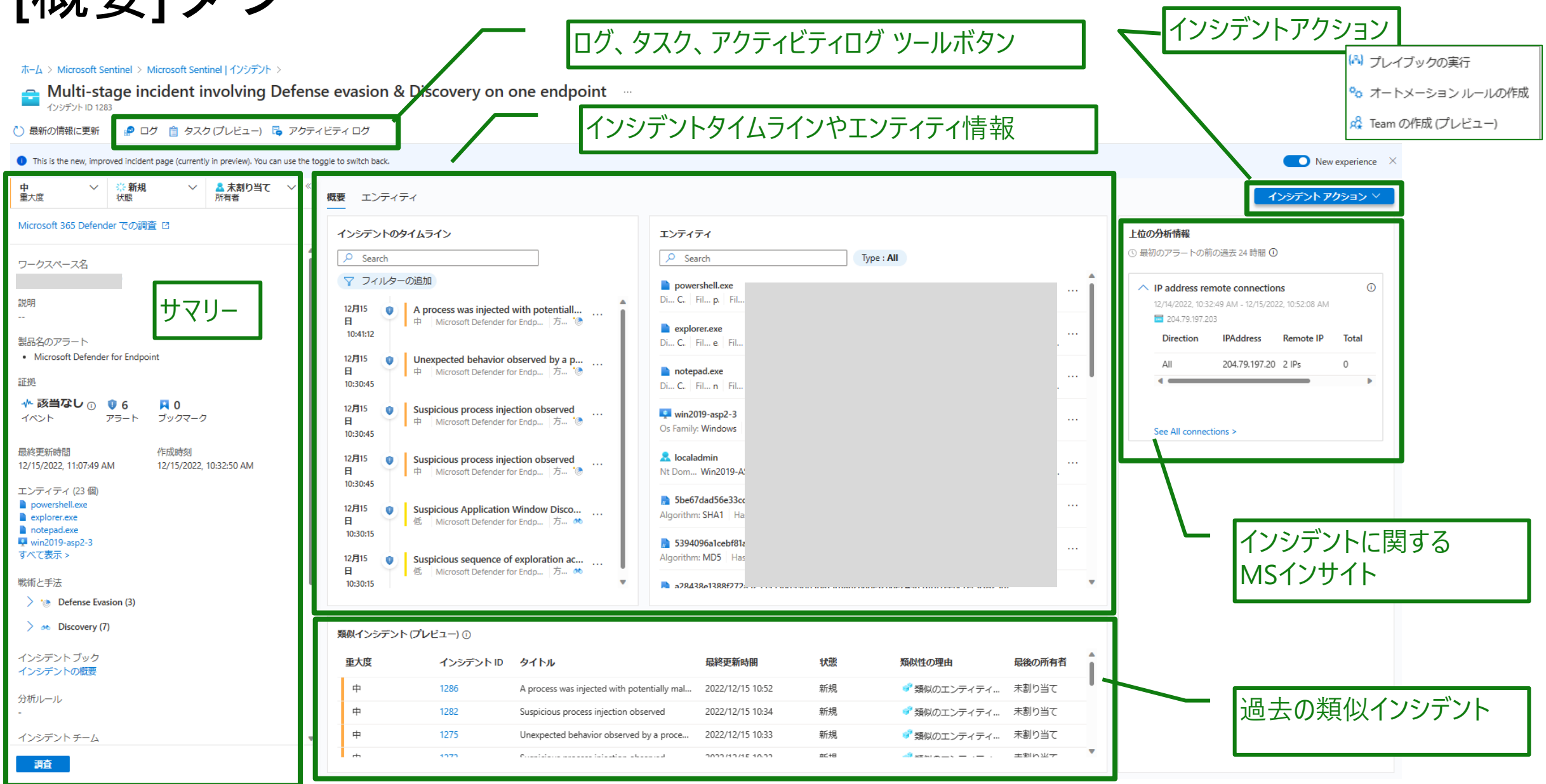
新しい「インシデント調査」ビューについて

- 2023/1/18よりPublic Preview
- SOCアナリストがインシデントに対しより効果的に対処するための新たなインシデント調査ビューを提供
- 新しいデザインを提供することの背景
  - アナリストは、セキュリティ インシデントのトリアージ、調査、対応を行う際に、多くの情報、アクション、ツールに迅速かつシームレスにアクセスする必要がある
  - 新しい調査ページでは、一つのビューでインシデントと侵害の範囲を把握するために必要な情報とツールをアナリストに提供
  - 多くのお客様/パートナー様、およびMS内SOCメンバーからのフィードバックを受けてデザインに反映し、Public Previewとして提供

- リソース

【Microsoft Learn】Navigate and investigate incidents in Microsoft Sentinel | Microsoft Learn
【ブログ】The new incident experience is here! - Microsoft Community Hub
【デモ】Announcing the New Microsoft Sentinel Incident Investigation Experience! - YouTube

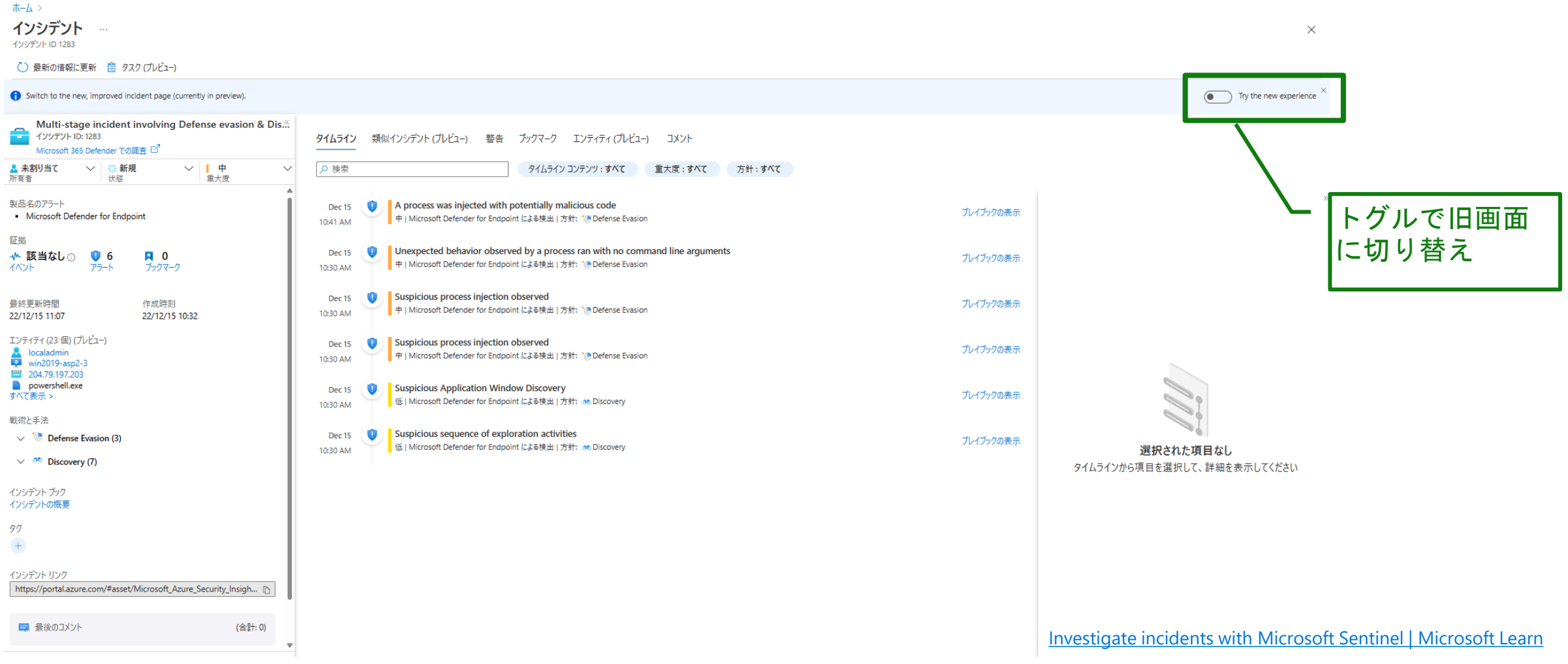
[概要]タブ



Navigate and investigate incidents in Microsoft Sentinel | Microsoft Learn

【ご参考】旧画面

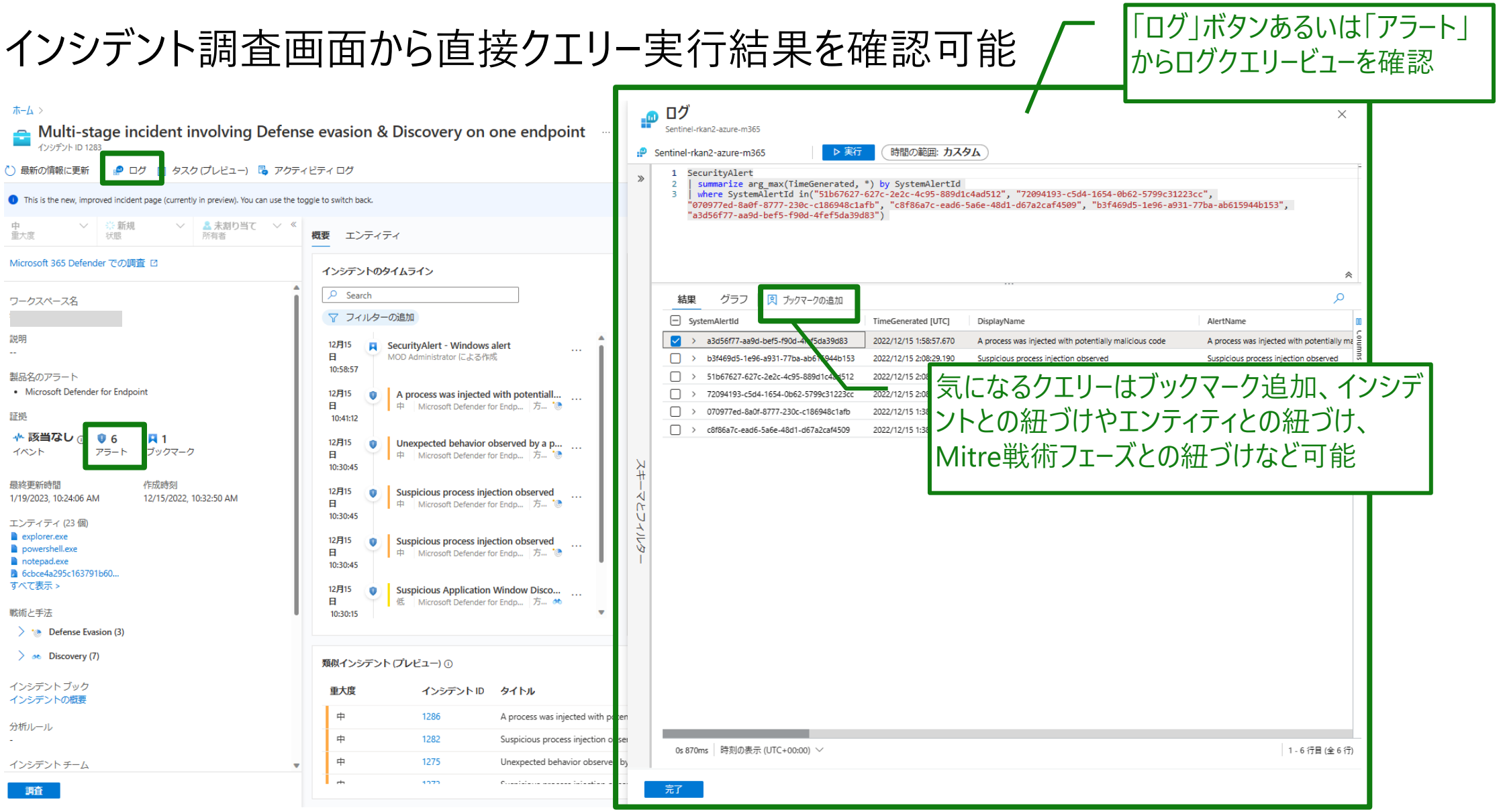
タイムライン、類似インシデント、アラート内容などタブを切り替える必要あり



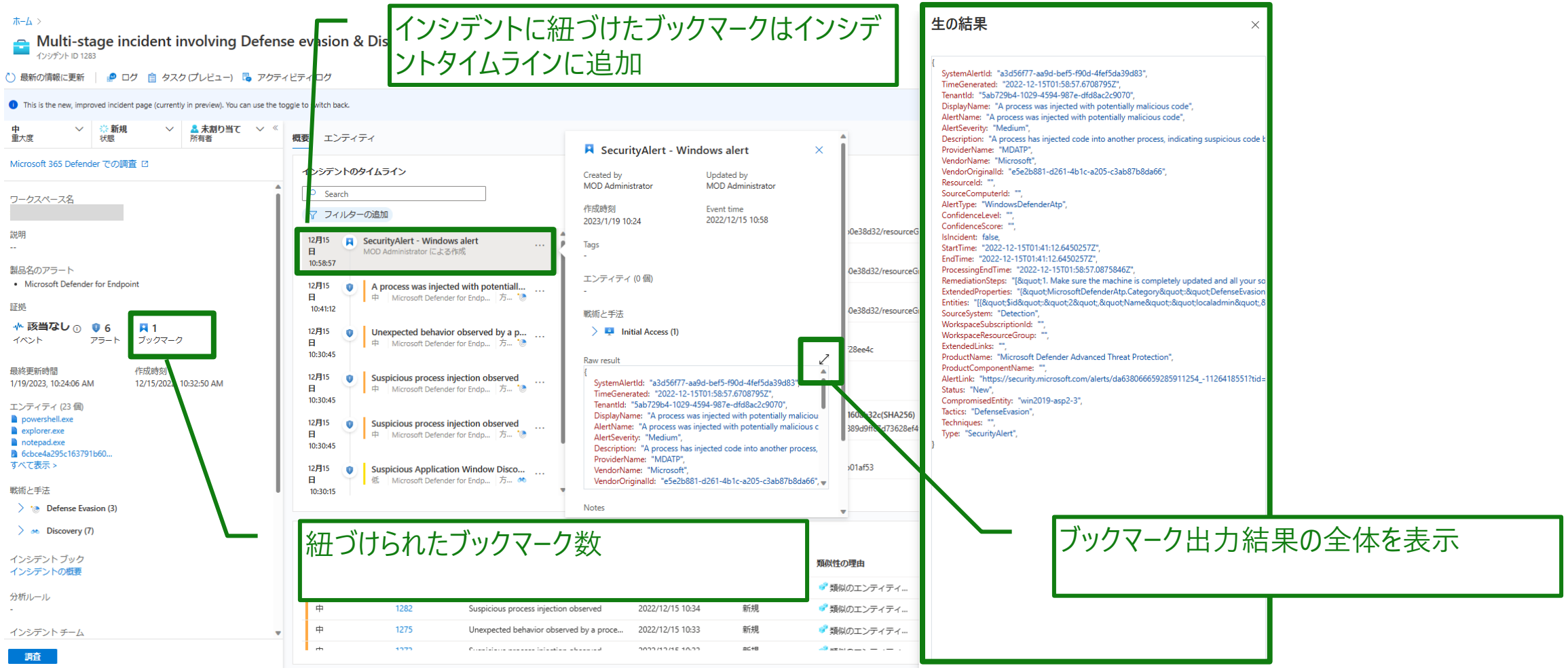
[Investigate incidents with Microsoft Sentinel | Microsoft Learn]

ログ分析クエリウインドウ

インシデント調査画面から直接クエリー実行結果を確認可能



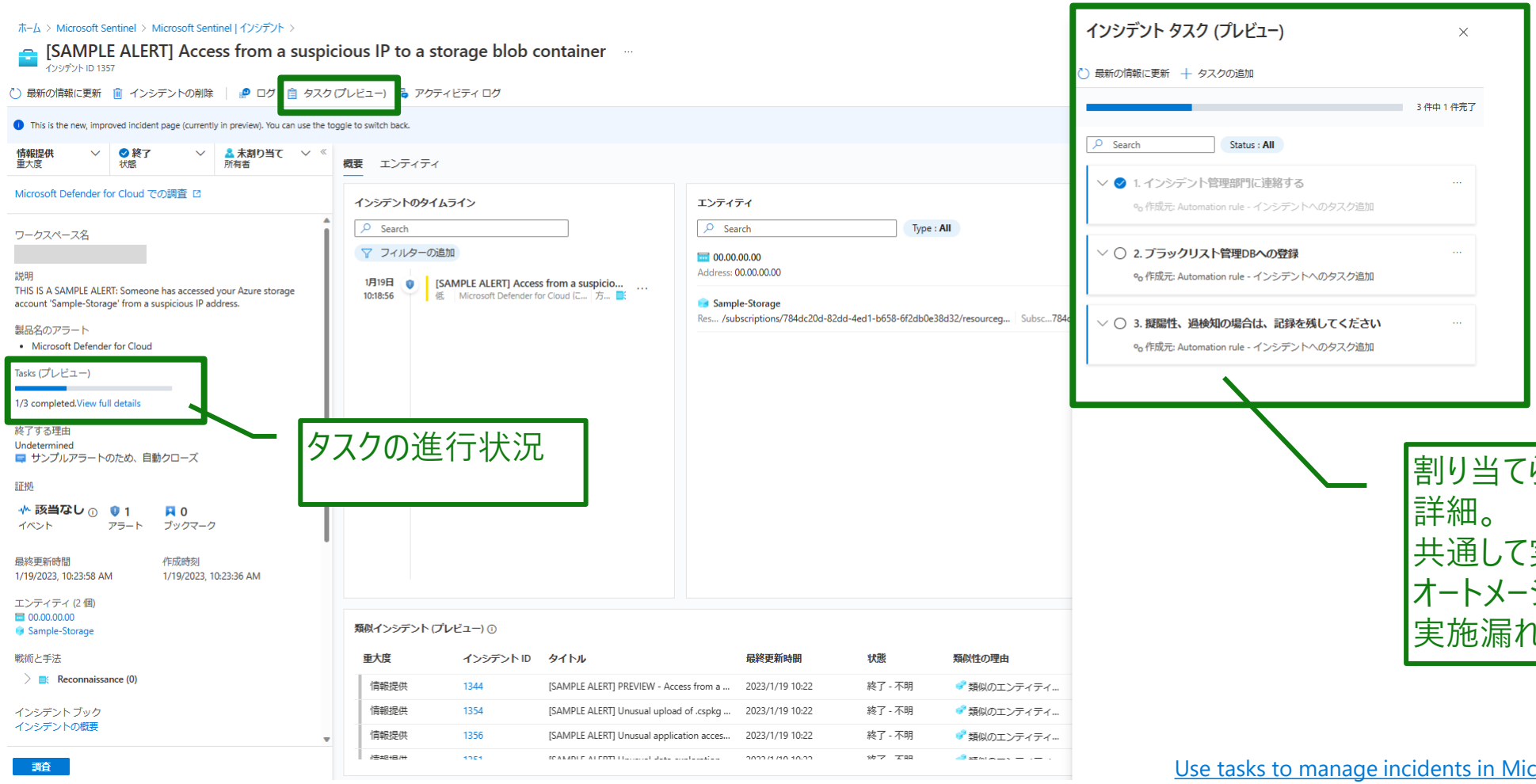
ブックマーク紐づけ



[Use hunting bookmarks for data investigations in Microsoft Sentinel | Microsoft Learn]

タスク

タスクを使用してインシデントワークフローを表示。
定常的なタスクはオートメーションルールを使って自動的に割り当て可能



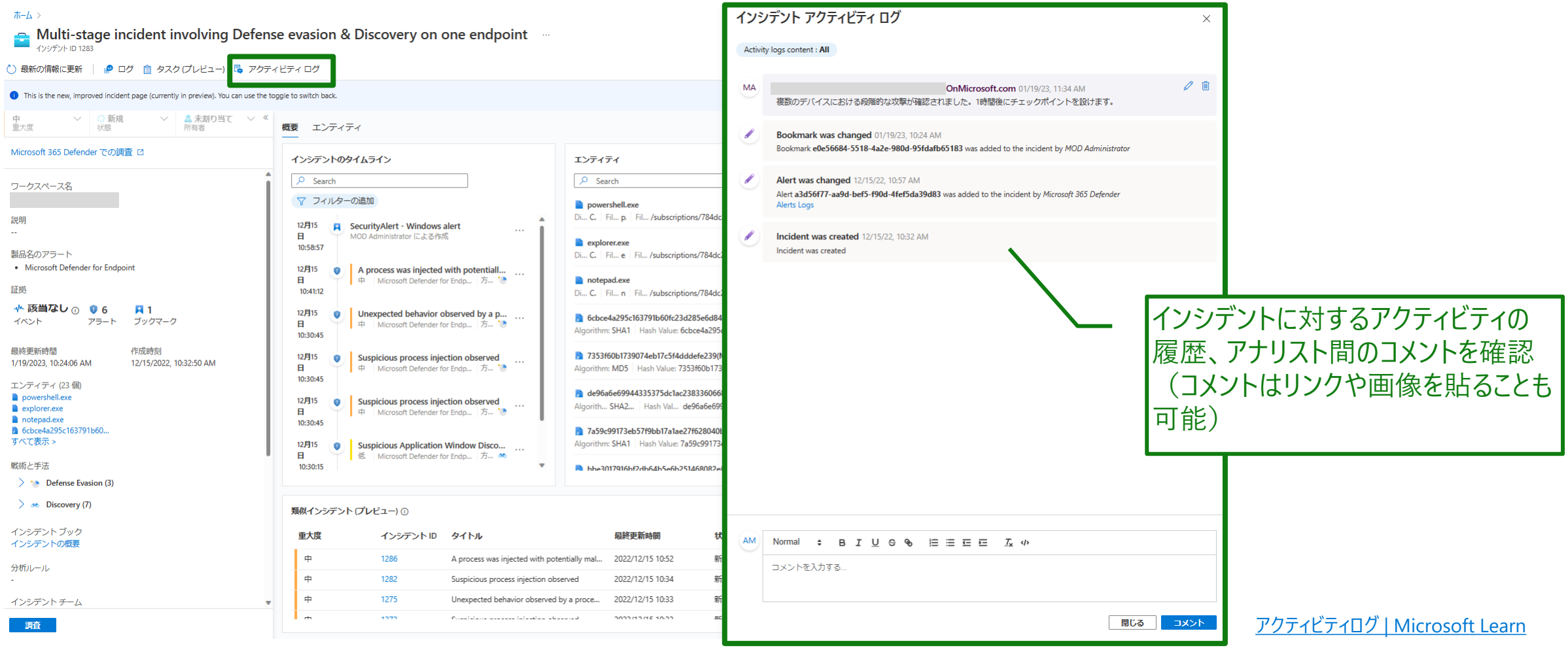
Use tasks to manage incidents in Microsoft Sentinel | Microsoft Learn

アクティビティログ

インシデントにおいてどのようなアクティビティが発生したのか確認可能

（重大度や状態の変更、プレイブックのトリガー、追加されたアラートなど、手動または自動のインシデントのコメント追加など）

他のアナリストの活動状況確認によりコラボレーション、監査の目的で利用可能

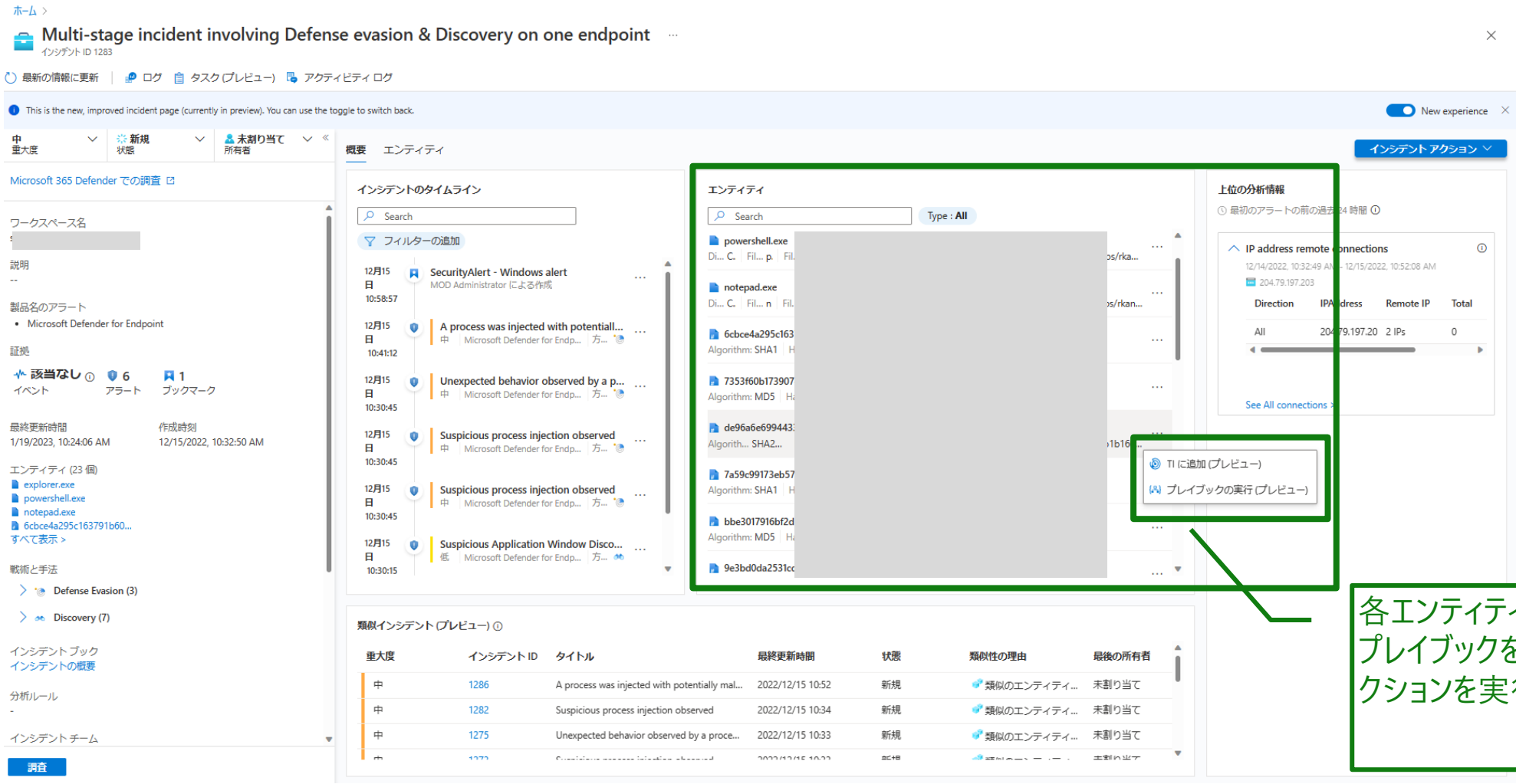


インシデントに対するアクティビティの履歴、アナリスト間のコメントを確認（コメントはリンクや画像を貼ることも可能）

アクティビティログ | Microsoft Learn

エンティティ情報（1/3）

インシデントで識別されたエンティティ情報を表示

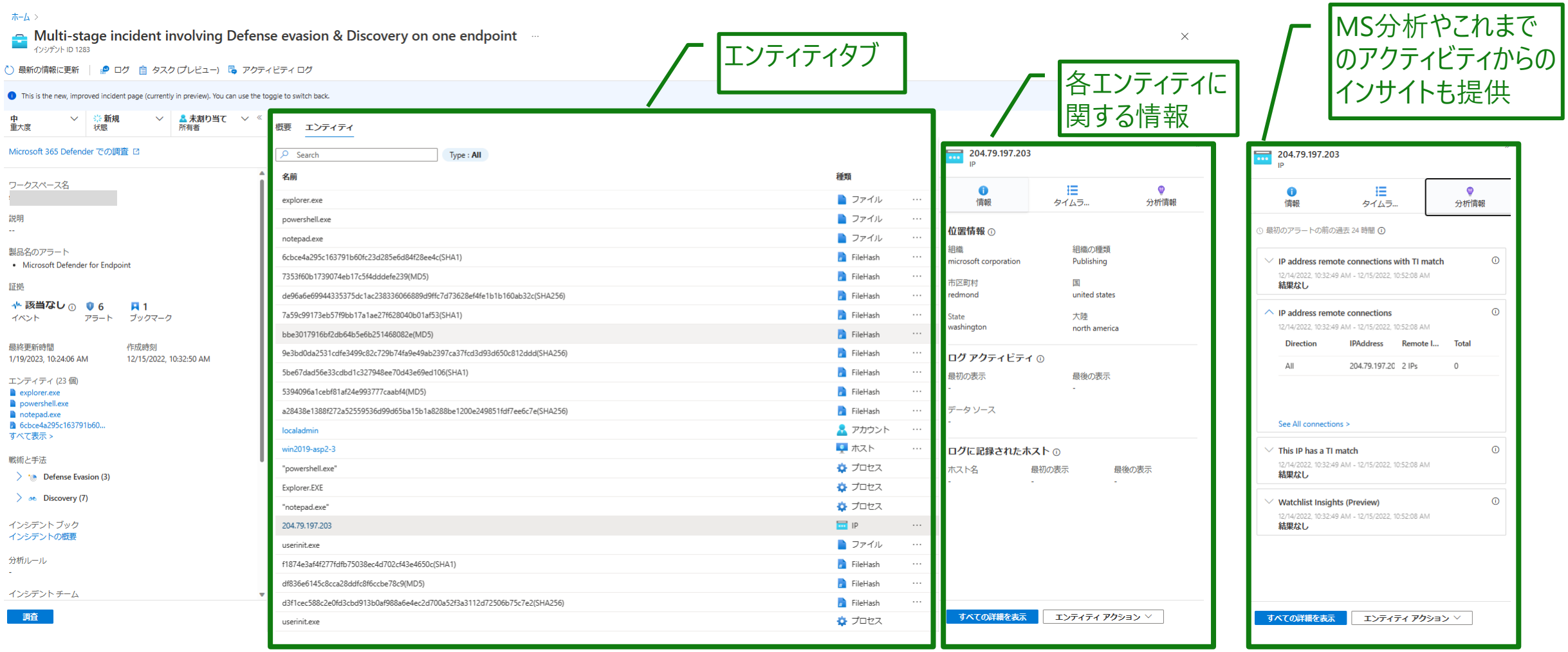


各エンティティについてTIに追加したり、プレイブックを実行することで追加のアクションを実行

エンティティ探索 | Microsoft Learn

エンティティ情報（2/3）

エンティティタブからエンティティの一覧確認、エンティティに関する情報、分析を確認



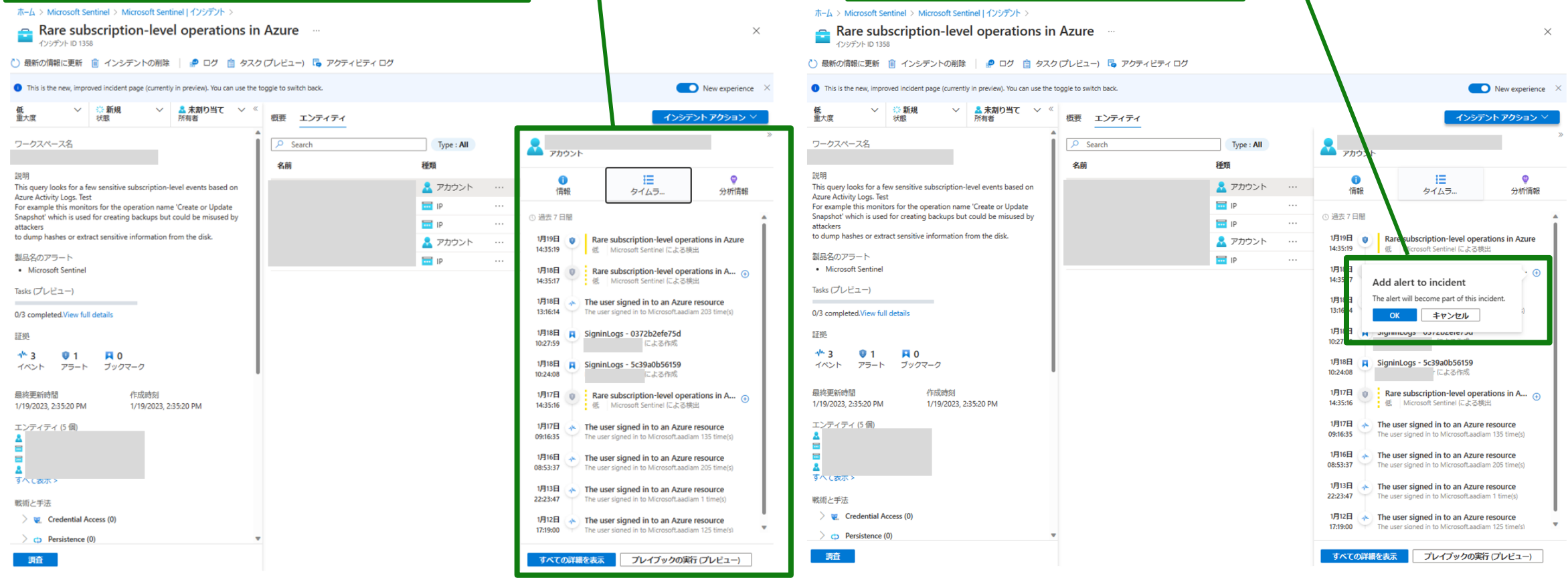
エンティティ探索 | Microsoft Learn

エンティティ情報（3/3）

エンティティの詳細から直近7日間のアクティビティ、関連アラートを確認可能

エンティティタイムライン。
同一エンティティのアクティビティや類似インシデント内のアラート発生タイミングを確認可能

過去のアラートを当該インシデントに加えることができる

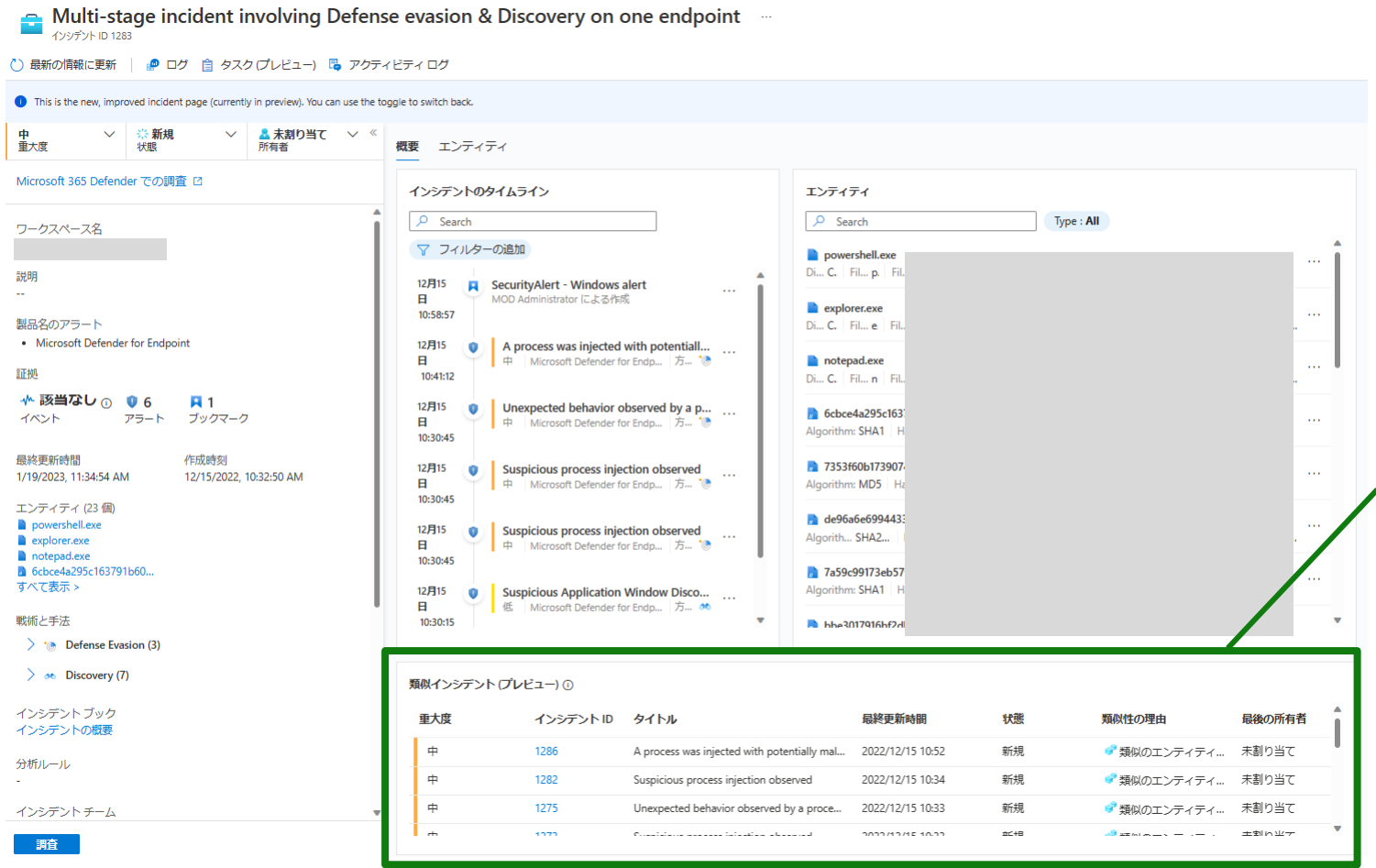


エンティティ探索 | Microsoft Learn

類似インシデント

過去や現在に渡っての類似インシデント発生状況を確認。

大規模攻撃の一部である可能性の確認や類似インシデントでの過去の対応者から知見を得ることに活用。



- 類似インシデント（最大20件表示）
- 類似性の降順で並び替えられる
- 過去14日間のデータに基づいて計算

類似インシデント（Microsoft Learn）