Cylance Endpoint Security

管理ガイド

Contents

ダッシュボードの使用

ダッシュボードは、さまざまな Cylance Endpoint Security サービスによって収集および分析されたデータを視覚的に把握するのに役立ち、また統計的な要約データを提供します。ダッシュボードを表示するには、メニューバーで［ダッシュボード］をクリックし、表示するダッシュボードを選択します。デフォルトダッシュボードは CylancePROTECT Desktop、CylancePROTECT Mobile、CylanceGATEWAY、のネットワークデータに対して使用できます。

さまざまなサービスで収集されたデータを表示するウィジェットを選択することで、独自のカスタムダッシュボードを作成することもできます。一部のウィジェットにはインタラクティブな要素があり、これらを操作してデータをフィルタリングしたり、詳細情報を表示したりできます。また、管理コンソールの専用画面に詳細情報を表示するためのリンクもあります。

作成または変更したダッシュボードは、他の管理者ユーザーと共有できます。

Cylance Endpoint Security ダッシュボードの主な機能

ダッシュボード	機能
デバイス保護（CylancePROTECT Desktop）	• 実行中の脅威：デバイスで現在実行されている脅威の数を表示します。 • 自動実行の脅威：自動的に実行されるように設定されている脅威の数を表示します。 • 隔離済みの脅威：隔離された脅威の数を表示します。 • Cylance に固有：CylancePROTECT Desktop によって一意に識別された脅威の数を表示します。 • 分析されたファイルの合計数：CylancePROTECT Desktop によって分析されたファイルの合計数を表示します。 • 脅威イベント：直近の 30 日間に検出された脅威を表示し、危険、異常、隔離済み、放棄済み、およびクリア済みとして分類します。 • 脅威からの保護：アクション（隔離、放棄、セーフリストへの追加など）を実行した脅威の割合を表示します。 • デバイス保護：デバイスポリシーで自動隔離が設定されている、危険なファイルと異常なファイルの両方を持つデバイスの割合を表示します。一方または両方のファイルタイプで自動隔離が無効になっている場合、割合を計算するときにデバイスは保護されていないと見なされます。 • 優先度別の脅威：まだ処理されておらず、注意が必要な脅威の総数を優先度別に表示します。 • 脅威の分類：検出された脅威のタイプをヒートマップで表示します。 • 上位 10 リスト：ほとんどのデバイスで検出された上位 10 の脅威、最も脅威の多い上位 10 のデバイス、および最も脅威の多い上位 10 のゾーンを表示します。

ダッシュボード	機能

モバイル保護（CylancePROTECT Mobile）	• 検出されたモバイルアラート：検出されたモバイルアラートの数と未解決のモバイルアラートの数を表示します。
	• アラートがあるモバイルデバイス：CylancePROTECT Mobile アプリでアラートが検出されたモバイルデバイスの数を表示します。
	• アラート検出が有効になったモバイルデバイス：CylancePROTECT Mobile アプリがインストールされ、有効になっているモバイルデバイスの数を表示します。
	• カテゴリ別のモバイルアラート：モバイルアラートのチャートとグラフをカテゴリ別に表示します。
	• 脆弱性があるモバイル OS：National Vulnerability Database によって識別、定義、および追跡されている脆弱性を持つモバイルオペレーティングシステムのグラフを表示します。
	• モバイルアプリアラート：検出された悪意のあるアプリとサイドロードされたアプリの統計情報を表示します。
	• モバイルネットワークアラート：安全ではないネットワークと安全ではない Wi-Fi の検出に関する統計情報を表示します。
	• モバイルデバイスのセキュリティアラート：デバイスのセキュリティ検出の統計情報を表示します（画面ロックが無効になっている、認証に失敗したなど）。
	• 次のカテゴリで上位の脅威のリストと統計情報を表示します。
	  • モバイルアラートがあるデバイスの上位ランク
	  • 安全ではない Wi-Fi ネットワークの上位ランク
	  • 悪意のあるアプリの上位ランク
	  • モバイルアラート検出の上位ランク
	  • サイドロードされたアプリの上位ランク
	  • 安全ではないメッセージURLの上位ランク
	  • 安全ではないネットワークの上位ランク
	  • サポート対象外デバイスモデルの上位ランク
	  • サポート対象外OSの上位ランク
	  • サポート対象外セキュリティパッチの上位ランク

ダッシュボード	機能
ネットワーク（CylanceGATEWAY）	• アクティブな Gateway ユーザーの合計数：アクティブユーザーの数を表示します。 • ネットワーク接続：許可されたネットワーク接続とブロックされたネットワーク接続のチャートを表示します。 • 転送済みバイト数：転送済みバイト数（アップロードおよびダウンロード済み）のチャートを表示します。 • プライベートネットワークアクセス、パブリックネットワークアクセス：プライベートおよびパブリックネットワークアクセスのグラフを表示します。 • プライベート上位ネットワークの宛先、パブリック上位ネットワークの宛先：上位のプライベートおよびパブリックネットワークの宛先と上位のアクションのリストを表示します。 • コネクタ接続履歴：オンラインおよびオフラインの CylanceGATEWAY Connectors のグラフを表示します。 • コネクタのステータス：環境内の CylanceGATEWAY Connectors の接続ステータスを表示します。 • 宛先評価リスク：低、中、高の宛先リスクアラートのリストを表示します。 • セキュリティリスクカテゴリ：指定したカテゴリの許可されたリスクカテゴリ、ブロックされたリスクカテゴリ、およびその組み合わせを表示します。 • TLS バージョン：環境内の TLS バージョンのチャートを表示します。 • ブロックされた上位カテゴリ：指定された宛先リスクレベルの許可された宛先、ブロックされた宛先、および両宛先の組み合わせのグラフを表示します。 • 帯域幅の上位消費者：パブリックパス、プライベートパス、および両パスの組み合わせでの帯域幅の上位消費者のリストを表示します。
情報保護（CylanceAVERT）	• 情報窃盗イベント：CylanceAVERT 窃盗イベントの数を、流出タイプ別にグループ化して表示します。このウィジェットはカスタム時間でフィルタリングできます。 • カテゴリ別の上位 10 窃盗イベント：上位 10 の窃盗イベントの数をカテゴリ別（ポリシー、ユーザー、デバイス、ファイル、およびデータタイプ）に表示します。このウィジェットはカスタム時間でフィルタリングできます。 • カテゴリ別の上位 10 ファイルインベントリアイテム：上位 10 のインベントリアイテムの数をカテゴリ別（ポリシー、ファイル拡張子、情報タイプ、およびデータタイプ）に表示します。 • 場所別の上位 10 窃盗イベント：上位 10 の窃盗イベントの数を場所別（Web ドメイン、メールドメイン、およびリムーバブルメディア）に表示します。このウィジェットはカスタム時間でフィルタリングできます。 • ファイルインベントリ：ファイルインベントリ内の機密ファイルの数を表示します。 • 証拠ロッカー：証拠ロッカー内の機密ファイルの数を表示します。 • アクティブな CylanceAVERT ユーザーの合計数：接続された CylanceAVERT ユーザーの総数を表示します。 • アクティブな CylanceAVERT デバイスの合計数：接続された CylanceAVERT デバイスの総数を表示します。

ダッシュボードの作成

1. 次の操作のいずれかを実行します。

タスク	手順
カスタムダッシュボードの作成	**a.** 管理コンソールのメニューバーで、［ダッシュボード］ > ［モバイル保護］または［ダッシュボード］ > ［ネットワーク］をクリックします。 **b.** ⊕ > ［新しいダッシュボードを追加］をクリックします。 **c.** 空のダッシュボードから始める場合は、ドロップダウンリストで［新しいダッシュボード］をクリックします。ダッシュボードに、CylancePROTECT Mobile、CylanceGATEWAY（ネットワーク）、または CylanceAVERT（情報保護）のデフォルトのウィジェットを含める場合は、ドロップダウンリストでそのオプションをクリックします。 **d.** タイトルを入力します。 **e.** ［追加］をクリックします。
ダッシュボードのコピー	**a.** 管理コンソールのメニューバーで、［ダッシュボード］をクリックし、コピーするダッシュボードをクリックします。 **b.** ⊕ > ［このダッシュボードをコピー］をクリックします。 **c.** タイトルを入力します。 **d.** ［保存］をクリックします。

2. ⊕ > ［ウィジェットを追加］をクリックします。利用可能なウィジェットの詳細については、「Cylance Endpoint Security ダッシュボードの主な機能」を参照してください。
3. ［ウィジェットを追加］パネルから、ダッシュボードに追加するウィジェットをドラッグアンドドロップします。

   ウィジェットは移動してサイズを変更できます。ウィジェットを削除するには、ウィジェットの上にマウスを置いて、⋮ > ［削除］をクリックします。

ダッシュボードの共有

作成または変更したダッシュボードは、他の管理者ユーザーと共有できます。

作業を始める前に：

- ダッシュボードを他の管理者と共有するには、管理者ロールが必要です。
- ダッシュボードの作成。

1. 管理コンソールで、共有するダッシュボードに移動します。
2. ⋯ > ［ダッシュボードを共有］をクリックします。
3. ダッシュボードをすべての管理者と共有するか、管理者を指定するかを選択します。特定の管理者と共有することを選択した場合は、管理者を検索してリストに追加します。
4. ［共有］をクリックします。

ダッシュボードを共有された管理者は、管理コンソールにログインした際に通知を受け取ります。共有ダッシュボードを［ダッシュボード］メニューに追加するには、デフォルトの CylancePROTECT Mobileまたは CylanceGATEWAYダッシュボード、あるいは任意のカスタムダッシュボードに移動し、 **>** ［新しいダッシュボードを追加］をクリックして、新しいダッシュボードのドロップダウンリストで共有ダッシュボードを選択します。ダッシュボードを共有されたユーザーは、共有ダッシュボードを変更することはできませんが、そのダッシュボードをコピーし、変更可能なダッシュボードを新しく作成することはできます。

ダッシュボード名の横にあるアイコンの色は、共有ダッシュボードの所有者である（緑）か、共有ダッシュボードへの読み取り専用アクセス権を持っている（茶）のか、またはそのダッシュボードがすべての管理者と共有されている（橙）のかを示します。

終了したら：

- ダッシュボードを共有するユーザーを変更する場合は、ダッシュボードに移動し、 **> ［共有設定を管理］をクリックします。
- ダッシュボードの共有を停止する場合は、 **> ［このダッシュボードの共有を停止］をクリックします。

Cylance Endpoint Security サービスにわたるアラートの管理

［アラート］表示では、Cylance Endpoint Security サービスにわたって検出および関連付けられたアラートを包括的に確認でき、企業エコシステムで一般的な脅威パターンを識別および追跡し、アラートの収集をより効率的に解決することが、一層簡単になります。［アラート］表示により、それぞれが CylancePROTECT Desktop や CylanceOPTICS など特定のサービス専用になっている、コンソールのさまざまなセクションからのアラートを調査する必要がなくなります。［アラート］表示を使用して、環境でサポートされている Cylance Endpoint Security サービスのいずれのアラートも確認、調査、および管理できます。

サービス	［アラート］表示でサポートされる機能
CylancePROTECT Desktop	デスクトップデバイス上の CylancePROTECT Desktop エージェントからの脅威テレメトリ、メモリ保護アラート、スクリプトコントロールアラート。
CylancePROTECT Mobile	CylancePROTECT Mobile アプリによって検出されたアラート。
CylanceOPTICS	デスクトップデバイス上の CylanceOPTICS エージェントによって検出されたアラート。
CylanceGATEWAY	設定した ネットワーク保護設定、または CylanceGATEWAY によって高リスクと判断された宛先のレピュテーション。
CylanceAVERT	デスクトップデバイス上の CylanceAVERT エージェントからの窃盗イベント。
Okta コネクタ	BlackBerry Okta コネクタを使用した Okta ユーザーイベントテレメトリ。 CylanceENDPOINT Pro ライセンスが必要です。
Mimecast コネクタ	BlackBerry Mimecast コネクタを使用した Mimecast 添付ファイル保護テレメトリ。 CylanceENDPOINT Pro ライセンスが必要です。

最初の［アラート］表示は、優先度、アラート分類、設定された応答、および他の重要なアラート属性などの条件に基づいて類似したアラートをグループ化した概要です。条件の詳細については、「Cylance Endpoint Security がアラートをグループ化する方法」を参照してください。

アラートの自動化されたグループ化では、アラートの頻度と出現率の両方が反映され、アナリストに脅威の発生頻度および発生場所を明確に表示します。デフォルトでは、アラートグループが優先度の降順で並べ替えられて、関連するすべてのセキュリティテレメトリのトップダウン表示が提供されます。各グループには、グループに関連付けられている重要なインジケータアーチファクトのタイプ（ファイル、プロセス、メールなど）のアイコンが表示されます。重要なインジケータアイコンをクリックすると、重要なインジケータの属性を確認できます。必要に応じて、それらの値をコピーまたはフィルタリングできます。新しいアラートは、テレメトリソースから検出および処理されると、既存のグループまたは新しいグループに追加されます。

［アラート］表示では、単一検出アラートと複数検出アラートがサポートされています。アラート検出ルールでは、複数の検出を実行してからアラートを生成して［アラート］表示に表示することがあります。各検出は、イベント（ファイルが開かれた、レジストリキーが追加されたなど）を使用してモデル化されます。

アラートグループをクリックすると、次の情報にアクセスできます。

- そのグループに関連する検出の詳細と重要なインジケータの概要を示す［アラートの概要］タブ。
- ［重要なインジケータ］タブには、グループ内の各アラートで同一の検出属性が表示されます。たとえば、重要なインジケータがファイルハッシュである場合、同じデバイスからものであるか、異なるデバイスからのものであるかに関係なく、各アラートで検出されたハッシュです。重要なインジケータは、親、子、および兄弟オブジェクトの間の関係を示すように視覚的に表示されます。複数検出アラートの場合、重要なインジケータは各イベントに含まれ、実行順に概要が示されます。
- グループ内の個々のアラートのリスト。個々のアラートをクリックすると、詳細情報を開くことができます。また、アラートに関連付けられていて、アイコンとして表示されるすべてのアーチファクトを表示することもできます。アーチファクトには、基礎となる検出エンジンによってキャプチャされたすべてのファセットが含まれています。重要なインジケータと同様に、これらのアーチファクトも、親、子、および兄弟オブジェクトの間の関係を示すように視覚的に表示されます。複数検出アラートの場合、重要なインジケータは各イベントに含まれ、実行順に概要が示されます。
- AI ベースの Cylance Assistant を使用して、アラートグループのサマリー分析、およびアラートグループ内のプロセスアーティファクトの詳細な分析（コマンドラインプロセスなど）を行うことができます。Cylance Assistant では、サイバーセキュリティの豊富な知識ソースを活用して、脅威調査に役立つ貴重な情報が提供されます。詳細については、「AI ベースの Cylance Assistant によるアラートの調査」を参照してください。

グループ内のアラートのタイプによっては、管理アクションを実行することもできます。たとえば、CylancePROTECT Desktop 脅威アラートの場合、グローバルセーフリストまたはグローバル隔離リストにファイルを追加したり、これらのリストからファイルを削除したりできます。

Cylance Endpoint Security がアラートをグループ化する方法

Cylance Endpoint Security は、次の条件を使用して、さまざまなサービスからのアラートをグループ化します。これにより、プロセスが自動化されて、脅威ハンティングおよび解決アクティビティを、関連するアラートの論理的なグループ化にスコープ設定および最適化できます。グループ化ロジックは、BlackBerry によって構築および管理され、さまざまな統合されたサービスからのアラートを処理するように動的に設計されます。その結果が、頻度および出現率分析を自動化するゼロタッチ体験です。これにより、サイバーセキュリティへの取り組みのトリアージおよび優先順位付けが、より簡単になります。

新しいアラートは、次の条件がすべて満たされると、既存のアラートグループに追加されます。

- アラートの優先度、分類、サブ分類、説明、重要なインジケータ、および応答がそのグループと一致する
- アラートがそのグループ内の最古のアラートから 7 日間（168 時間）以内に検出される

これらの条件をすべて満たしてはいないアラートが検出されると、新しいアラートグループが作成されます。

優先度

アラートの優先度は、問題の緊急度と、組織の環境への潜在的な影響に関連付けられ、アラートがグループ化される方法に組み込まれます。［アラート］表示では、テレメトリソースにわたって優先度が最高のアラートがグループ化されるため、最も重要なアラートを最初に表示および解決するのに役立ちます。

アラートの優先度を決定する要因は、サービスによって異なります。

サービス	要因
CylancePROTECT Desktop	• 脅威アラートについては、管理コンソールの［保護］>［脅威］でアラートの優先度が低くても、［アラート］表示では優先度が常に高になります。［アラート］表示でこの昇格した優先度にする目的は、マルウェア検出の緊急性を示すためです。 • メモリ保護およびスクリプト制御のアラートについては、BlackBerry サイバーセキュリティアナリストが設定したイベントの性質によって優先度が決定されます。優先度は、調査の全体的な重大度および関連性に基づいています。
CylancePROTECT Mobile	アラートは、管理コンソールおよび CylancePROTECT Mobile アプリに表示される重大度に対応する優先度値を使用します。
CylanceOPTICS	CylanceOPTICS 検出ルールの設定によって優先度が決定されます。

CylanceGATEWAY	優先度は、設定したネットワーク保護設定、または、CylanceGATEWAY によって高リスクレベルと判断された宛先のレピュテーションに基づいています。たとえば、CylanceGATEWAY は、次のシナリオでアラートを生成して［アラート］表示に表示する場合があります。
	• 宛先のレピュテーションの検出：
	  • 有効にすると、設定したリスクレベルに基づいてアラートが生成されます。たとえば、リスクレベルを［中以上］に設定した場合、アラートは、リスクレベルが中および高のすべての検出について生成されます。
	  • 有効にしないと、デフォルトでは、高リスクレベルであると判断されたアラートが生成されます。
	• 署名検出：
	  • 有効にすると、アラートは、ブロックされた署名検出について生成され、高リスクレベルで表示されます。
	  • 有効にしないと、CylanceGATEWAY はアラートを生成しません。
	• DNS トンネリングおよびゼロデイ検出については、アラートは、高リスクレベルの検出について生成されます。

CylanceAVERT	［アラート］表示では優先度が常に高になります。
Mimecast	優先度は、Mimecast 添付ファイルリスクスコアリングを通じて決定されます。
Okta	優先度は、BlackBerry サイバーセキュリティアナリストが設定します。

分類およびサブ分類

アラート分類およびアラートサブ分類は、基礎になっている検出タイプを識別し、ラベルを付けて、特定のサービスによって検出されたアラートをより適切に説明できる構造化されたアラートコンテンツを提供します。各サービスは、アラートの性質を明確にする分類およびサブ分類の特定のセットを定義します。

分類およびサブ分類データは、類似したアラートを識別およびグループ化するために使用されます。

アラートの分類およびサブ分類を決定する要因は、サービスによって異なります。

サービス	要因
CylancePROTECT Desktop	• 脅威アラートについては、分類およびサブ分類が CylancePROTECT Desktop 脅威アラートのファイル分類に対応します。 • メモリ保護アラートについては、分類およびサブ分類がメモリ保護違反のタイプに対応します。 • スクリプト制御アラートの場合、分類は全体的なアラートタイプ（スクリプト制御、不審なプログラム、マルウェアなど）を示し、サブ分類は詳細（実行されたスクリプト、ブロックされたスクリプトなど）を提供します。
CylancePROTECT Mobile	分類が全体的なアラートカテゴリ（［デバイスセキュリティ］や［ネットワークの脅威］など）に対応し、サブ分類が管理コンソールおよびアプリで表示される特定のアラートタイプ（［悪意のあるアプリ］、［サイドロードされたアプリ］、［安全ではない Wi-Fi］など）に対応します。
CylanceOPTICS	検出ルールには、アラートの分類およびサブ分類を定義する MITRE 戦術、テクニック、サブテクニックが含まれています。
CylanceGATEWAY	分類がアラートの全体的なカテゴリ（［ネットワークアクセス制御］など）に対応し、サブ分類が管理コンソールに表示される特定のアラートタイプ（［レピュテーション］、［DNS トンネリング］、［署名検出］、［ゼロデイ検出］など）に対応します。
CylanceAVERT	窃盗イベントによって分類が決定されます。
Mimecast	アラートの分類は、初期アクセス Mitre 戦術（TA0001）です。同じアラートのサブ分類は、フィッシング Mitre テクニック（T1566）です。
Okta	アラートの分類は、ユーザーアクセス制御（サインイン試行回数の上限を超えたなど）またはネットワークアクセス制御（ブロックリストルールにより IP 要求がブロックされたなど）のいずれかです。アラート分類がユーザーアクセス制御である場合、サブ分類はユーザーロックアウトになります。アラート分類がネットワークアクセス制御である場合、サブ分類は IP アドレスのブロックになります。

説明

アラートの説明は、アラートに関する短いセグメントの情報を提供する特性です。一致する説明を持つアラートは、グループ化される可能性が高くなります。

重要なインジケータ

重要なインジケータは、アラートグループ内の個々のアラートに共通する検出コンテンツです。アグリゲーションプロセスでは、アラートの重要なインジケータを比較して、グループ化するかどうかが決定されます。たとえば、ファイルに重要なインジケータ SHA256 ハッシュが含まれている場合、ハッシュ値はアラートグループ内の各アラート内で同一です。

アラートの重要なインジケータは、サービスによって異なります。

サービス	要因
CylancePROTECT Desktop	• 脅威アラートについては、重要なインジケータは SHA256 ハッシュです。 • メモリ保護アラートについては、重要なインジケータは、イベント固有の特性（SHA256 ハッシュやリスクスコアのようなファイルデータなど）です。 • スクリプト制御アラートの場合、重要なインジケータはイベント固有の特性です（たとえば、ファイルの SHA256 ハッシュ、スクリプトタイプ、スクリプト名）。
CylancePROTECT Mobile	重要なインジケータは、特定のモバイルアラート固有の特性（サイドロードされたアプリのパッケージ名、安全ではない Wi-Fi ネットワークの SSID、サポートされていないデバイスのモデルなど）に対応します。
CylanceOPTICS	重要なインジケータは、アラートに関連付けられている、一意に識別するアーチファクトのファセットです。たとえば、プロセスアーチファクトについては、重要なインジケータは、次のファセットです。SHA256 ハッシュ、ファイルパス、コマンドライン引数。これらのファセットは、他のアラートと比較できるプロセスアーチファクトタイプ固有の署名を確立します。アラートグループの重要なインジケータファセットは、グループ内の個々のアラートにわたって共通です。
CylanceGATEWAY	重要なインジケータは［ネットワーク接続］と［DNS 要求］です。
CylanceAVERT	重要なインジケータは、アーチファクトタイプによって異なります。メールアラートアーチファクトについては、重要なインジケータは conversationID です。ブラウザおよびファイル窃盗アラートアーチファクトについては、重要なインジケータは UserName です。
Mimecast	重要なインジケータは、アラートに関連付けられているアーチファクトのファセットです。たとえば、メール添付ファイルアーチファクトについては、重要なインジケータは、メール添付ファイルの SHA256 ハッシュです。
Okta	重要なインジケータは、ユーザーログイン要求に関連付けられているアカウント、およびブロックされたログイン試行に関連付けられている IP アドレスです。

応答

軽減アクションを実行するサービスについては、これは、検出に応じて実行するようにサービスを設定したアクションです。たとえば、CylancePROTECT Desktop 脅威アラートについては、応答は次のいずれかになる可能性があります。放棄済み、隔離済み、危険、異常。

軽減アクションを実行しないサービスについては、統合されたサービスから、関連する情報を記録します。一致する応答を持つアラートは、グループ化される可能性が高くなります。

時刻

他のアラートに対するアラートの発生時間は、アラートがグループ化される方法に組み込まれます。アラートは、アラートの優先度、分類、サブ分類、説明、重要なインジケータ、および応答がそのグループと一致し、そのグループ内の最古のアラートから 7 日間（168 時間）以内に発生した場合、既存のグループに追加されます。

アラートは、上記の基準に一致しても、グループ内で最古のアラートから 7 日経過後に発生した場合は、新しいグループに追加されます。7 日間の枠により、アラートグループが固定された期間を持ち、無制限に大きくならないことが保証されます。

集約されたアラートの表示と管理

作業を始める前に： 管理者ロールに、［アラート］ビューを使用するために必要な権限があることを確認します。［アラートの表示］権限では、アラートビューへの読み取り専用アクセスが提供されます。このビューでアラートグループや個々のアラートを変更するには、［アラートの編集］および［アラートの削除］権限が必要です。［アラート］ビューを使用して、CylancePROTECT Desktop 脅威アラートからグローバルセーフリストまたはグローバル隔離リストにファイルを追加したり、これらのリストからファイルを削除したりするには、関連するグローバルリスト権限がロールに必要です。詳細については、セットアップガイドで「管理者の設定」を参照してください。

1. 管理コンソールのメニューバーで［アラート］をクリックします。
   表示する列を選択するには、右にスクロールし、|||| をクリックします。
2. 次の操作のいずれかを実行します。

タスク	手順

アラートグループのフィルターとソート	**a.** 列の ▽ をクリックしてフィルター条件を入力または選択します。次のいずれかを行うことができます。
	• 複数のフィルター条件を一度に適用します。フィルターを削除するには、そのフィルターの x をクリックします。
	• 分類、サブ分類、説明、または重要なインジケータでフィルタリングする場合は、次のいずれかを実行します。
	  • 完全に一致するものを検索するには、⚙ > ［次の値に等しい］をクリックします。一致を表示する値を入力します。最大 5 件の一致をクリックしてフィルタリングリストに追加し、［適用］をクリックします。
	  • 指定した値を含む一致を検索するには、⚙、> ［含む］をクリックします。1 つまたは複数の値を入力します（値を追加するには、＋ をクリックします）。［適用］をクリックします。
	  結果を表示するときに、画面上部に表示されているフィルターをクリックして、フィルター条件を追加または削除できます。
	• ［カウント］でフィルタリングする場合は、追加オプションの ⚙ をクリックします（［次の値より大きい］、［次の値より小さい］など）。
	• ［製品］でフィルタリングすると、結果を特定の Cylance Endpoint Security サービスに絞り込むことができます。
	• ［検出時刻］でフィルタリングすると、結果を特定の日時範囲に絞り込むことができます。
	b. アラートグループを列の昇順または降順に並べ替えるには、列の名前をクリックします（該当する場合）。

タスク	手順
アラートグループの重要なインジケータの詳細の表示、および重要なインジケータのタイプまたは値でのアラートグループのフィルタリング	**a.** 重要なインジケータアイコンにマウスポインタを合わせると、オブジェクトまたはイベントのタイプが表示されます。アイコンをクリックすると、詳細が表示されます。 **b.** 必要に応じて、切り捨てられた文字列値のテキスト全体を表示するには、その上にマウスポインタを合わせ、 をクリックします。 **c.** 必要に応じて、値をコピーするには、その上にマウスポインタを合わせ、 をクリックします。 **d.** アラートグループを重要なインジケータでフィルタリングするには、その上にマウスポインタを合わせ、 をクリックします。

タスク	手順
アラートグループおよび個々のアラートの詳細の表示	**a.** アラートグループをクリックします。 **b.** 左ペインで下にスクロールして、インスティゲーティングとターゲットオブジェクト間の関係を表示します。このビューには、個々のイベントに関連する一連の重要なインジケータ（ファイル、ユーザー、実行可能ファイル、プロセスなど）が表示されます。 **c.** 左ペインで下にスクロールして、インスティゲーティングとターゲットオブジェクト間の関係を表示します。このビューには、個々のイベントに関連する一連の重要なインジケータ（ファイル、ユーザー、実行可能ファイル、プロセスなど）が表示されます。 たとえば、子プロセスのインスティゲーティングプロセスである親プロセスオブジェクトまたは実行可能ファイルが表示される場合があります。同じレベルのイベントまたはオブジェクトは、同じ親の下の兄弟と見なされます。 必要に応じて、値の上にマウスポインタを合わせ、 をクリックしてテキスト文字列全体を表示したり、 をクリックして値をコピーしたりできます。プロセスアーチファクトがある場合は、 をクリックして Cylance Assistant によって解析できます。詳細については、「AI ベースの Cylance Assistant によるアラートの調査」を参照してください。 **d.** 個々のデバイスアラートに対して、次のいずれかを行います。 • アラート情報をソートおよびフィルタリングします。 • アラートのステータスを変更します。「アラートのステータス変更」を参照してください。 • アラートをユーザーに割り当てます。 • アラートのラベルを追加または変更します。 **e.** 個々のアラートの詳細パネルを開くには、アラートをクリックします。次の操作のいずれかを実行します。 • 該当する場合は、［検出の詳細］をクリックすると、コンソールの他の領域（CylanceOPTICS の検出ビューなど）の詳細やアクションを表示できます。［検出の詳細］リンクは、CylancePROTECT Desktop 脅威アラートの場合は 60 日間、その他のタイプのアラートの場合は 30 日間有効です。 • アラートに関連するアーチファクトを展開して詳細を確認し、インスティゲーティングとターゲットオブジェクトおよびイベントの関係を表示します。検出ルールに関連するすべてのオブジェクトが、アーチファクトビューに含まれます。 必要に応じて、値の上にマウスポインタを合わせ、 をクリックしてテキスト文字列全体を表示したり、 をクリックして値をコピーしたりできます。プロセスアーチファクトがある場合は、 をクリックして Cylance Assistant によって解析できます。詳細については、「AI ベースの Cylance Assistant によるアラートの調査」を参照してください。

タスク	手順
CylanceMDR サポートの要請	この機能は、CylanceMDR オンデマンドサブスクリプションでのみ使用できます。 疑わしいと思われるアラートを確認し、専門家に脅威を分析してもらいたい場合は、CylanceMDR アナリストにオンデマンドで支援を要請できます。このアラートは、調査のためアナリストにエスカレートされます。CylanceMDR（CylanceGUARD）ポータルを使用して、エスカレートされたアラートについて、エスカレーション画面からアナリストと連絡を取ることができます。たとえば、アラートに関する追加の詳細を求めることができます。 **a.** CylancePROTECT Desktop 脅威アラートを含むアラートグループをクリックします。 **b.** 右ペインで、［**CylanceMDR** サポート］ボタンをクリックします。 **c.** ［サポートを要請］をクリックして、アラートをアナリストにエスカレートすることを確認します。 **d.** 要請については、CylanceMDR （CylanceGUARD）ポータルから追跡します。CylanceMDR 関連の資料を参照してください。 24x7 の脅威監視をご希望の場合は、CylanceMDR Standard サブスクリプションまたは Advanced サブスクリプションをご検討ください。詳細については、CylanceMDR の概要を参照してください。
CylancePROTECT Desktop 脅威アラート：グローバルセーフリストまたはグローバル隔離リストにファイルを追加またはこれらのリストからファイルを削除します。	**a.** CylancePROTECT Desktop 脅威アラートを含むアラートグループをクリックします。 **b.** ［アクション］ **>** ［グローバルリストを管理］をクリックします。 脅威アラートに関連するファイルの SHA256 ハッシュが表示されます。ファイルがグローバルセーフリストまたはグローバル隔離リストにすでに存在する場合は、通知が表示されます。 **c.** グローバルセーフリストまたはグローバル隔離リストにファイルを追加するか、これらのリストからファイルを削除する適切なアクションを選択します。ファイルがすでにグローバルセーフリストまたはグローバル隔離リストに存在する場合は、別のリストに移動できます。 **d.** ファイルをグローバルセーフリストに追加する場合は、［カテゴリ］ドロップダウンリストで該当するカテゴリをクリックします。 **e.** ファイルをリストに追加する場合は、理由を入力します。 **f.** ［保存］をクリックします。 該当するセーフリストまたは隔離リストに変更が適用されます。［アラート］ビューのアラートグループに変更はありません。

タスク	手順
アラートグループのステータス変更	次の操作のいずれかを実行します。 • アラートグループのステータスを変更するには、［ステータス］ドロップダウンリストで適切なステータスをクリックします。 • 複数のアラートグループのステータスを変更するには、アラートグループを選択し、［ステータスを変更］をクリックし、適切なステータスをクリックして、［適用］をクリックします。 「アラートのステータス変更」を参照してください。
ユーザーへのアラートグループの割り当て	次の操作のいずれかを実行します。 • アラートグループをユーザーに割り当てるには、［担当者］列で + をクリックし、ユーザーを検索してクリックし、［割り当て］をクリックします。 • 複数のアラートグループをユーザーに割り当てるには、アラートグループを選択し、［アラートを割り当て］をクリックし、ユーザーを検索して選択し、［割り当て］をクリックします。
アラートグループのラベルの追加または変更	アラートグループにカスタムラベルを追加して、短いメモやリマインダを設定したり、フィルター条件として使用したりすることができます。ラベルを表示するには、［ラベル］列を表示するように設定する必要があります。 **a.** 1 つまたは複数のアラートグループを選択します。 **b.** ［ラベルを変更］をクリックします。 **c.** ラベルを入力して Enter キーを押すか、既存のラベルを検索して選択します。 **d.** ［適用］をクリックします。 ラベルを削除するには、ラベルをクリックし、x アイコンをクリックして、［適用］をクリックします。
アラートデータのエクスポート	次の操作のいずれかを実行します。 • すべてのアラートグループの詳細をエクスポートするには、 をクリックします。ファイル名を指定し、［エクスポート］をクリックします。 • グループ内のすべてのアラートの詳細をエクスポートするには、アラートグループをクリックし、 をクリックします。ファイル名を指定し、［エクスポート］をクリックします。
アラートグループの削除	**a.** 1 つまたは複数のアラートグループを選択します。 **b.** ［削除］をクリックします。 **c.** ［削除］を再度クリックして確定します。

タスク	手順
フィルター結果からのラートグループの削除	**a.** 適切な基準でアラートグループをフィルターします。 **b.** 次の操作のいずれかを実行します。 • フィルター結果からすべてのアラートグループを削除するには、左上のチェックボックスをオンにして［すべて削除］をクリックします。［すべて削除］を再度クリックして確定します。 • フィルター結果から特定のアラートグループを削除するには、アラートグループを選択して［削除］をクリックします。［削除］を再度クリックして確定します。

AI ベースの **Cylance Assistant** によるアラートの調査

AI ベースの Cylance Assistant を使用して、アラートグループのサマリー分析、およびアラートグループ内のプロセスアーティファクトの詳細な分析（コマンドラインプロセスなど）を行うことができます。Cylance Assistant では、サイバーセキュリティの豊富な知識ソースを活用して、脅威調査に役立つ貴重な情報が提供されます。

メモ：

- ［アラート］ビューで Cylance Assistant にアクセスするには、BlackBerry アカウント担当者に連絡して、この機能の有効化をリクエストする必要があります。
- 現在、Cylance Assistant は CylanceOPTICS アラートのみで使用できます。今後の更新では、この機能が他の Cylance 製品やサービスにも拡張される予定です。
- BlackBerry は、Cylance Assistant を強化する AI のトレーニングに顧客データを使用しません。

1. 管理コンソールのメニューバーで［アラート］をクリックします。
2. ［製品］列で をクリックし、［**CylanceOPTICS**］を選択します。
3. アラートグループをクリックします。

タスク	手順
アラートグループのサマリー分析を生成します。	**a.** 左ペインの［概要］セクションで、［アラートの概要］をクリックします。 **b.** をクリックして概要をコピーします。
アラートグループのインスティゲーティングまたはターゲットプロセスの分析を生成します。	**a.** 左ペインで下にスクロールして、インスティゲーティングとターゲットオブジェクト間の関係を表示します。 **b.** インスティゲーティングまたはターゲットプロセスアーチファクトの上にマウスポインタを置き、 をクリックします。 **c.** をクリックして分析をコピーします。

タスク	手順
グループの特定のアラートで、インスティゲーティングまたはターゲットプロセスの分析を生成します。	**a.** アラートグループ内の個々のアラートをクリックします。 **b.** 右ペインで下にスクロールして、インスティゲーティングとターゲットオブジェクト間の関係を表示します。 **c.** インスティゲーティングまたはターゲットプロセスアーチファクトの上にマウスポインタを置き、 をクリックします。 **d.** をクリックして分析をコピーします。

アラートのステータス変更

コンソールの他のセクション（［保護］ > ［脅威］、［CylanceOPTICS］ > ［検出］、および［保護］ > ［Protect Mobile のアラート］など）にある個々のアラートのステータスは、［アラート］表示内の同等のステータスに対応します。別の表示でアラートステータスが変更されると、［アラート］表示でもステータスが更新されます。たとえば、［検出］のアラートのステータスが［偽陽性］に変更された場合、［アラート］表示のステータスが［クローズ済み］に変わります。

［アラート］表示で個々のアラートのステータスを変更すると、［CylanceOPTICS］ > ［検出］表示に、同等のステータス変更が表示されます。現在、［アラート］表示で開始したステータス変更は、［保護］ > ［脅威］表示や［保護］ > ［Protect Mobile のアラート］表示には表示されません。

CylancePROTECT Desktop 脅威アラートについては、次の同等の状態があります。

- ［保護］ > ［脅威］に表示され、［危険］、［異常］、または［隔離済み］ステータスを持つアラートは、［アラート］表示では、［新規］ステータスを持ちます。
- ［保護］ > ［脅威］に表示され、［放棄済み］ステータスを持つアラートは、［アラート］表示では、［クローズ済み］ステータスを持ちます。

アラートグループに対してステータスを設定した場合、そのグループ内の個々のアラートに、選択したステータスが割り当てられます。アラートグループ内の個々のアラートが、手動のステータス変更と異なるステータスを持つか、別の表示（［CylanceOPTICS］ > ［検出］など）からのステータス変更の結果として異なるステータスを持つ場合、アラートグループのステータスが［複数］に変更されます。アラートグループ内の個々のアラートがすべて、同じステータスを持つ場合、アラートグループも同じステータスを持ちます。たとえば、個々のアラートがすべて、ステータス［クローズ済み］を持つ場合、アラートグループのステータスも［クローズ済み］になります。

ユーザー、デバイスおよびグループの管理

このセクションでは、 Cylance Endpoint Security サービスに対して有効になっているユーザーとデバイス、および設定とポリシーを適用するために使用するグループを表示し、管理する方法について説明します。

CylancePROTECT Desktop デバイスおよび CylanceOPTICS デバイスの管理

管理コンソールの［アセット］ > ［デバイス］画面から、CylancePROTECT Desktop エージェントと CylanceOPTICS エージェントを搭載したデバイスを表示および管理できます。エージェントが正常にインストールされ、管理コンソールに登録されているデバイスは、この画面に表示されます。デバイスの検索、デバイスレポートのエクスポート、およびデバイスに対するアクションの実行を行うことができます。たとえば、サポートされていないエージェントを実行しているデバイスのリストをエクスポートしたい場合があります。または、デバイスを別のゾーンにすばやく追加して、ゾーンに応じて適切なデバイスポリシーが割り当てられるようにすることもできます。

次のセクションでは、デバイス画面の新しいデバイスグリッドビューについて説明します。デバイス画面では、クエリベースの検索機能が提供され、必要なデバイスを柔軟に検索したり、クエリを保存したりロードしたりできます。また、情報の密度を調整したり、列をピン留めしたりして、読みやすさを向上させることもできます。

保存済みクエリは、ゾーンルールの作成に使用します。保存済みクエリをロードし、結果内のデバイスのリストを確認してから、それをゾーンルールに使用できます。詳細については、セットアップコンテンツの「CylancePROTECT Desktop と CylanceOPTICS のデバイスを管理するゾーンの設定」を参照してください。

作業を始める前に： レガシービューの場合、画面の右上にある［新しいビューに切り替え］をクリックすると、新しいデバイスグリッドビューに切り替えることができます。

1. 管理コンソールのメニューバーで、［アセット］ > ［デバイス］をクリックします。
   すべてのデバイスのリストが表示されます。
2. オプションで、デバイスグリッドに表示される列をカスタマイズします。
   - 列を追加または削除するには、⚙ をクリックし、表示する列を選択します。スライダを使用して、グリッドに表示される情報の密度を調整したり、📌 をクリックして列をピン留めしたりすることもできます。
   - 列の順序を変更するには、列名を目的の位置にドラッグします。
   - 昇順または降順で並べ替えるには、列の名前をクリックします。
3. デバイスのリストをフィルタリングするには、次のいずれかの操作を行います。

タスク	手順
デバイスの簡易検索	簡易検索を実行するには、空の検索バーに任意のテキストを入力し、列を指定しません。簡易検索方式では、［デバイス名］、［DNS 名］、［IP アドレス］、［MAC アドレス］、および［最後に報告されたユーザー］の列の結果をすばやくフィルタリングできます。 簡易検索は Text フィールドを使用しますが、他のフィールドと組み合わせて結果をフィルタリングするために使用することはできません。他のフィールドに対して検索を実行するには、代わりに詳細検索を実行します。

タスク	手順
デバイスの詳細検索	**a.** 検索バーをクリックします。 フィルタリング可能なフィールドのリストが表示されます。検索を保存するか、最近実行した場合は、保存済みの検索と最近の検索がリストの一番上に表示されます。 **b.** フィルタリングするフィールドを選択します。 **c.** 比較演算子（~ = < など）を選択します。 メモ：現在、IP アドレスフィールドは、［次の値に等しい］（=）および［次の値で始まる］（^=）演算子でのみ機能します。IP アドレスの範囲内のデバイスを検索する場合は、［次の値に等しい］演算子を使用し、カンマを使用してそれらをリストすることができます。または、［次の値で始まる］演算子を使用して、IP アドレスの最初の部分を照合します（たとえば、“IP Address” ^= 192.168 では、アドレス 192.168.x.x のデバイスが検索されます）。今後のリリースでは、IP アドレス範囲によるデバイスリストのフィルタリングがサポートされる予定です。 **d.** フィルタリングするフィールドのパラメーター値を入力します。複数のパラメーターをカンマで区切ることができます（例、Platform ~ macOS, Windowsや"IP Addresses" = 192.168.1.100, 192.168.1.101, 192.168.1.102）。 複数の単語の文字列を含むパラメーター値の場合は、文字列を引用符で囲みます（例、"Windows 11"）。 **e.** 別の式を追加するには、クエリの最後にブール演算子（and or）を追加します。現在、ブール演算子を選択する場合には、クエリ内の後続のブール演算子も同じ演算子にする必要があります。 たとえば、「A=B and C=D and E~F」はサポートされています。 また、「A=B or C=D or E~F」もサポートされています。 一方、「A=B and C=D or E~F」は現在サポートされていません。 **f.** ［検索］をクリックします。
クエリの保存	クエリを保存するには、有効なクエリを検索バーに入力している必要があります。 **a.** 検索を実行し、クエリが有効で期待どおりの結果が生成されることを確認します。 **b.** 検索バーで をクリックします。 **c.** クエリの名前を入力します。 **d.** ［保存］をクリックします。

タスク	手順
保存済みまたは最近のクエリのロード	保存済みまたは最近のクエリをロードできます。保存済みのクエリと最近のクエリは、検索バーが空の場合にのみ表示されます。 **a.** 空の検索バーをクリックします。 をクリックすると、検索バーをクリアできます。 **b.** リストの一番上で、最近のクエリ（）または保存済みのクエリ（）をクリックします。検索バーにクエリがロードされます。 **c.** ［検索］をクリックします。
保存済みのクエリの名前変更	**a.** 空の検索バーをクリックします。 をクリックすると、検索バーをクリアできます。 **b.** リストの一番上の保存済みのクエリの横にある をクリックします。 **c.** クエリの新しい名前を入力します。クエリは変更できません。 **d.** ［保存］をクリックします。
結果の .csv ファイルへのエクスポート	**a.** をクリックします。 **b.** ファイルの名前を入力します。 **c.** ［エクスポート］をクリックします。

4. デバイスに対するアクションを実行するには、次のいずれかの操作を行います。

タスク	手順
デバイスの詳細を表示します。	デバイス名をクリックします。
デバイスポリシーをデバイスに割り当てます。	デバイスは 1 つのデバイスポリシーにのみ関連付けることができます。新しいデバイスポリシーをデバイスに割り当てると、以前のデバイスポリシーが置き換えられます。 **a.** 1 つ以上のデバイスを選択します。 **b.** ［ポリシーを割り当て］をクリックします。 **c.** デバイスポリシーをクリックします。 **d.** ［保存］をクリックします。
デバイスをゾーンに追加します。	ゾーンを使用して、設定の適用および複数のデバイスに対するデバイスポリシーを管理できます。ゾーンの詳細については、Cylance Endpoint Security のセットアップに関するコンテンツを参照してください。 **a.** 1 つ以上のデバイスを選択します。 **b.** ［ゾーンに追加］をクリックします。 **c.** 1 つ以上のゾーンを選択します。 **d.** ［保存］をクリックします。

タスク	手順
デバイスを削除します。	デバイスを削除すると、CylancePROTECT Desktop エージェントの登録が解除され、そのデバイスのデータが管理コンソールから削除されます。ユーザーは、エージェントが登録されていないという通知を受け取ります。エージェントを再度登録するには、インストールトークンを提供する必要があります。 **a.** 1 つ以上のデバイスを選択します。 **b.** ［削除］をクリックします。 **c.** ［はい］をクリックして確定します。
ライフサイクル管理からデバイスを除外します。	非アクティブを理由にデバイスをコンソールから自動的に削除しない場合は、デバイスのライフサイクル管理からこれらのデバイスを手動で除外できます。ライフサイクル管理に含まれる非アクティブなデバイスは、自動的に削除される場合があります。 **a.** 1 つ以上のデバイスを選択します。 **b.** ［ライフサイクル管理］をクリックします。 **c.** ［ライフサイクル管理から除外］または［ライフサイクル管理に含める］をクリックします。 **d.** ［はい］をクリックして確定します。 ライフサイクル管理設定を構成して、デバイスの状態がオフラインから非アクティブに変更されるタイミング、および非アクティブデバイスを削除するタイミングを指定できます。詳細については、「デバイスライフサイクル管理の設定」を参照してください。
デバイスの非アクティブ時間をリセットします。	この機能は、デバイスの状態をオフラインに設定し、オフライン日カウンタをリセットし、オフライン日を現在の日付に設定します。これは、オンラインのデバイスには影響しません。 **a.** 1 つ以上のデバイスを選択します。 **b.** ［非アクティブ時間をリセット］をクリックします。 **c.** ［はい］をクリックして確定します。

タスク	手順
デバイスのバックグラウンド脅威検出スキャンを開始します （レガシービューのみ）	デバイスのバックグラウンド脅威検出スキャンをオンデマンドで開始できます。この機能を使用するには、デバイスが CylancePROTECT Desktop エージェントのバージョン 3.2 以降を実行している必要があります。このオプションを使用してバックグラウンドスキャンを開始すると、デバイスで現在進行中のスキャンをすべて終了させてから新しいスキャンが開始されます。 この機能は現在、レガシービューでのみ使用できます。 **a.** 1 つ以上のデバイスを選択します。 **b.** ［バックグラウンドスキャン］をクリックします。 **c.** ［はい］をクリックして確定します。 最新のバックグラウンドスキャンが完了した日時がコンソールに記録されます。割り当てられたデバイスポリシーで定期的なバックグラウンド脅威検出が設定されている場合は、それに応じてスケジュールされた次のスキャン時間が再計算されます。 同じ VM ホストの複数の VM デバイスでバックグラウンド脅威検出スキャンを同時に実行すると、リソースの共有によってデバイスのパフォーマンスが影響を受けるため、注意してください。

ゾーンの管理

ゾーンを使用して、CylancePROTECT Desktop デバイス、および CylanceOPTICS デバイスをグループ化して管理できます。デバイスのグループ化は、地域（アジアやヨーロッパなど）、職務（営業担当者や IT スタッフなど）、または組織で必要な任意の基準に基づいて行うことができます。

デバイスポリシーをゾーンに割り当て、そのデバイスポリシーをゾーンに属する CylancePROTECT Desktop および CylanceOPTICS デバイスに適用できます。ドメイン名、IP アドレス範囲、オペレーティングシステムなど、選択した条件に基づいてデバイスをゾーンに割り当てることができるゾーンルールを追加することもできます。ゾーンルールは、デバイスがルール要件を満たしている場合、ゾーンに新しいデバイスを追加します。

1. 管理コンソールのメニューバーで、［ゾーン］をクリックします。次の操作のいずれかを実行します。
   - ゾーンを列の昇順または降順で並べ替えるには、列の名前をクリックします。
   - ゾーンをフィルターするには、列の をクリックしてフィルター条件を入力または選択します。
2. 次の操作のいずれかを実行します。

タスク	手順
ゾーンの詳細を表示します。	ゾーン名をクリックします。

タスク	手順
新しいゾーンを追加します。	**a.** ［新しいゾーンを追加］をクリックします。 **b.** ［ゾーン名］フィールドに、ゾーンの名前を入力します。 **c.** ［ポリシー］ドロップダウンリストで、ゾーンに関連付けるデバイスポリシーをクリックします。 **d.** ［値］フィールドで、ゾーンの適切な優先度レベルをクリックします。この設定は、ゾーンの管理には影響しません。 **e.** ［保存］をクリックします。
ゾーンを削除します。	**a.** 1 つ以上のゾーンを選択します。 **b.** ［削除］をクリックします。 **c.** ［はい］をクリックします。
ゾーンルールを作成します。	ゾーンルールを作成して、指定した条件を満たすデバイスをゾーンに自動的に追加します。指定したルール条件は、上から下の順に処理されます。 **a.** ゾーン名をクリックします。 **b.** ［ルールを作成］をクリックします。 **c.** ゾーンルールを設定します。 **d.** ［保存］をクリックします。
デバイスをゾーンに追加します。	デバイスが属することができるゾーンの最大数は 75 です。デバイスに 75 個を超えるゾーンがある場合、ポリシーとエージェントの割り当てに予期外の結果が発生するか、「選択したデバイスを選択したゾーンに追加できませんでした」というエラーメッセージが表示されることがあります。 **a.** ゾーン名をクリックします。 **b.** ［デバイス］タブで、［デバイスをゾーンに追加］をクリックします。 **c.** 追加するデバイスを選択します。 **d.** 選択したデバイスにゾーンデバイスポリシーを適用する場合は、［選択したデバイスにゾーンポリシーを適用］チェックボックスをオンにします。 **e.** ［保存］をクリックします。
ゾーン内のすべてのユーザーにゾーンデバイスポリシーを適用します。	このアクションにより、現在デバイスに割り当てられているすべてのデバイスポリシーが、現在ゾーンに割り当てられているデバイスポリシーに置き換えられます。 **a.** ゾーン名をクリックします。 **b.** ［このゾーン内のすべてのデバイスに適用］チェックボックスをオンにします。 **c.** ［保存］をクリックします。

タスク	手順
別のゾーンにデバイスをコピーします。	**a.** ゾーン名をクリックします。 **b.** ［デバイス］タブで、1 つ以上のデバイスを選択します。 **c.** ［デバイスをコピー］をクリックします。 **d.** 1 つ以上のゾーンを選択します。 **e.** ［保存］をクリックします。
ゾーンからデバイスを削除します。	**a.** ゾーン名をクリックします。 **b.** ［デバイス］タブで、1 つ以上のデバイスを選択します。 **c.** ［デバイスをゾーンから削除］をクリックします。 **d.** ［はい］をクリックします。
ゾーンを使用してエージェントの更新を管理します。	ゾーンを作成した後、デバイスで CylancePROTECT Desktop および CylanceOPTICS エージェントを更新するためのゾーンベースの更新ルールを作成できます。詳細については、Cylance Endpoint Security のセットアップに関するコンテンツを参照してください。

CylancePROTECT Mobile アプリを搭載したデバイスの管理

管理コンソールを使用すれば、CylancePROTECT Mobile アプリがインストールされたモバイルデバイスを表示し、管理できます。また、デバイスの現在のリスクレベルを表示することもできます。これは、ユーザーに割り当てられたリスク評価ポリシーでの脅威からリスクレベルへのマッピングを使用して決定されます（デフォルトの評価ポリシーがあります）。リスク評価ポリシーの詳細については、Cylance Endpoint Security のセットアップに関するコンテンツを参照してください。

1. 管理コンソールのメニューバーで、［アセット］ > ［モバイルデバイス］をクリックします。次の操作のいずれかを実行します。
   - デバイスを列の昇順または降順に並べ替えるには、列の名前をクリックします。
   - デバイスをフィルタリングするには、列の ▽ をクリックし、フィルター条件を入力するか、選択します。
2. 次の操作のいずれかを実行します。

タスク	手順
デバイスの CylancePROTECT Mobile アラートを表示します。	**a.** 1 つのデバイスをクリックします。 **b.** ［**Protect Mobile** のアラート］タブを表示します。 デバイスの現在のリスクレベルになったアラートを表示するには、左ペインでリスクレベルをクリックします。
デバイスの CylanceGATEWAY イベントを表示します。	**a.** 1 つのデバイスをクリックします。 **b.** メニューで［イベント］をクリックします。
デバイスのコンプライアンスの詳細を表示します。	**a.** 1 つのデバイスをクリックします。 **b.** メニューで［コンプライアンス］をクリックします。

タスク	手順
デバイスを削除します。	**a.** 1 つ以上のデバイスを選択します。 **b.** ［削除］をクリックします。 **c.** ［削除］を再度クリックして確定します。 デバイスとそれに関連付けられているすべてのアラートとイベントは、Cylance Endpoint Security サービスおよび管理コンソールから削除されます。デバイスを再度追加する場合は、ユーザーは CylancePROTECT Mobile アプリを再度有効にする必要があります。新しいアクティベーションメールを送信する手順については、「CylancePROTECT Mobile アプリと CylanceGATEWAY ユーザーの管理」を参照してください。

CylancePROTECT Mobile アプリと CylanceGATEWAY ユーザーの管理

CylancePROTECT Mobile アプリと CylanceGATEWAY が有効になっているユーザーアカウントは、管理コンソールで表示し、管理できます。

1. 管理コンソールのメニューバーで、［アセット］ > ［ユーザー］をクリックします。次の操作のいずれかを実行します。
   - ユーザーを列で昇順または降順に並べ替えるには、列の名前をクリックします。
   - ユーザーをフィルタリングするには、列の をクリックし、フィルター条件を入力するか、選択します。
2. 次の操作のいずれかを実行します。

タスク	手順
ユーザーのアラートを表示します。	**a.** ユーザーの名前をクリックします。 **b.** メニューで［アラート］をクリックします。 **c.** 適切なタブをクリックします。
ユーザーのイベントを表示します。	**a.** ユーザーの名前をクリックします。 **b.** メニューで［イベント］をクリックします。
ユーザーのデバイス詳細を表示します。	**a.** ユーザーの名前をクリックします。 **b.** メニューで［デバイス］をクリックします。 **c.** デバイスをクリックすると、関連するアラート、イベント、およびコンプライアンス情報が表示されます。

タスク	手順
ユーザーをグループに追加します。	ディレクトリグループは会社のディレクトリで管理されるため、ディレクトリグループにユーザーを追加する際には、次の手順を使用できません。次の手順はローカルグループにのみ適用されます。 **a.** ユーザーの名前をクリックします。 **b.** メニューで［設定］をクリックします。 **c.** ［ユーザーグループを割り当て］をクリックします。 **d.** 1 つ以上のグループを検索して選択します。 **e.** ［割り当て］をクリックします。
グループからユーザーを削除します。	ディレクトリグループは会社のディレクトリで管理されるため、ディレクトリグループからユーザーを削除する際には、次の手順を使用できません。次の手順はローカルグループにのみ適用されます。 **a.** ユーザーの名前をクリックします。 **b.** メニューで［設定］をクリックします。 **c.** グループの横にある をクリックします。 **d.** ［割り当て解除］をクリックします。
ユーザーにポリシーを割り当てます。	**a.** ユーザーの名前をクリックします。 **b.** メニューで［設定］をクリックします。 **c.** ［ユーザーポリシーを割り当て］をクリックします。 **d.** ポリシーのドロップダウンリストで、ポリシーのタイプをクリックします。 **e.** ポリシーを検索して選択します。 **f.** ［割り当て］をクリックします。 ユーザーにそのタイプのポリシーが既に割り当てられている場合は、以前に割り当てられたポリシーが新しく選択したポリシーによって置き換えられます。
ポリシーをゾーンから削除します。	**a.** ユーザーの名前をクリックします。 **b.** メニューで［設定］をクリックします。 **c.** ポリシーの横にある をクリックします。 **d.** ［割り当て解除］をクリックします。
ユーザーからワンタイムパスワード登録を削除します。	ユーザーはワンタイムパスワードに登録する必要があります。 **a.** ユーザーの名前をクリックします。 **b.** ［アクション］ドロップダウンリストで、［**TOTP** 登録を削除］をクリックします。 **c.** ［**TOTP** 登録を削除］ダイアログボックスで、［確認］をクリックします。

タスク	手順
CylancePROTECT Mobile アプリの新しいアクティベーションメールが送信されます。	該当するモバイルプラットフォームを有効にした登録ポリシーがユーザーに割り当てられている必要があります。 **a.** 1 人以上のユーザーを選択します。 **b.** ［招待状を再送信］をクリックします。 **c.** ［招待状を再送信］を再度クリックして確認します。
CylancePROTECT Mobile アプリのユーザーのアクティベーションパスワードを期限切れにします。	**a.** 1 人以上のユーザーを選択します。 **b.** ［パスコードを期限切れにする］をクリックします。 **c.** ［期限切れ］をクリックして確認します。
ユーザーを削除します。	**a.** 1 人以上のユーザーを選択します。 **b.** ［ユーザーを削除］をクリックします。 **c.** ［削除］をクリックして確認します。 ユーザーアカウント、およびそのユーザーに関連付けられているすべての CylancePROTECT Mobile アプリと CylanceGATEWAY イベントおよびアラートは、Cylance Endpoint Security サービスと管理コンソールから削除されます。ディレクトリの同期とオンボーディングを設定していた場合は、同期が行われたときにユーザーが再び Cylance Endpoint Security に追加されないよう、必要に応じてディレクトリグループを変更してください。

CylanceAVERT ユーザーの詳細の表示

管理コンソールの［**CylanceAVERT** ユーザー］ページでは、CylanceAVERT ユーザーおよび関連イベント、デバイス、ポリシーに関する情報を確認できます。CylanceAVERT ユーザーリストからユーザーを選択すると、ユーザーの詳細、そのユーザーに関連付けられたデータ窃盗イベント、ユーザーのデバイスの詳細、ユーザーが割り当てられているユーザーグループとポリシーを表示することができます。

1. 管理コンソールのメニューバーで、［アセット］ **>** ［**Avert** ユーザー］の順にクリックします。
2. 特定のユーザーの詳細を表示するには、Avert ユーザーのリストからユーザー名をクリックします。Avert ユーザーのリストで、ユーザー名、メールアドレス、ユーザーに割り当てられているデバイス数を確認できます。

   メモ：ただし、ユーザーを追加、更新、削除することはできません。ユーザーを管理する場合、［ユーザーの管理］をクリックします。
3. ユーザーの詳細ページでは、次の操作ができます。

   - ユーザーに関連するデータ窃盗イベントの詳細を表示するには、［イベント］タブをクリックします。このタブは、デフォルトで表示されます。
   - デバイス名、OS バージョン、CylanceAVERT エージェントのバージョン、エージェントの登録日、最後にポリシーが割り当てられた時刻など、ユーザーのデバイスに関する詳細を表示するには、［デバイス］タブをクリックします。
   - ユーザーに割り当てられているユーザーグループやユーザーポリシーを表示するには、［設定］タブをクリックします。ユーザーをユーザーグループに割り当てるには、［ユーザーグループの割り当て］をク

リックして、リストからグループを選択します。ユーザーをユーザーポリシーに割り当てるには、［ユーザーポリシーの割り当て］をクリックして、リストからポリシーを選択します。

ユーザーグループの管理

CylancePROTECT Mobile アプリと CylanceGATEWAY ユーザーに対して有効になっているユーザーのユーザーグループを管理できます。ユーザーグループは共通のプロパティを共有する関連するユーザーの集合です。グループとしてユーザーを管理した方が、同時にグループのすべてのメンバーに対してプロパティを追加、変更、または削除できるため、個々のユーザーを管理するより効率的です。ユーザーグループにポリシーを割り当てると、そのグループのすべてのメンバーにポリシーが適用されます。

Cylance Endpoint Security には、次の 2 種類のユーザーグループがあります。

- ディレクトリグループは、会社のディレクトリ内のグループにリンクします。グループのメンバーシップは、ディレクトリ内のメンバーシップリストと同期します。詳細については、「オンボーディングおよびオフボーディングの設定」を参照してください。
- ローカルグループは、管理コンソールで作成および管理されます。任意のローカルユーザーまたはディレクトリユーザーをローカルグループに割り当てることができます。

グループの作成の詳細については、セットアップに関するコンテンツを参照してください。

1. 管理コンソールのメニューバーで、［アセット］ > ［ユーザーグループ］をクリックします。
2. グループにポリシーを割り当てるには、⊕ をクリックし、割り当てるポリシーを選択します。
   ポリシー設定でも、ユーザーおよびグループにポリシーを割り当てることができます。
3. グループ内のユーザーを管理するには、［ユーザー］タブをクリックします。

デバイスライフサイクル管理の設定

CylancePROTECT Desktop エージェントと CylanceOPTICS エージェントは、管理コンソールと通信していない場合（ユーザーがデバイスをオフにした場合など）、オフラインステータスになります。エージェントが長時間オフラインになっている場合は、デバイスが使用されていないことを示している可能性があります。デバイスライフサイクル管理は、モバイルデバイスエージェント（CylancePROTECT Mobile など）や CylanceGATEWAY エージェントには適用されません。

デバイスライフサイクル管理を使用して、管理コンソールでデバイスが非アクティブとしてマークされるまでにオフラインのままでいることができる日数を指定できます。また、指定した日数の経過後、コンソールから非アクティブとしてマークされたデバイスを自動的に削除するように設定することもできます。たとえば、オフラインデバイスが 30 日間オフラインのままになった後、オフラインデバイスを非アクティブとしてマークするように、デバイスライフサイクル管理機能を設定できます。デバイスがさらに 15 日間非アクティブになった後、デバイスをコンソールから削除するように、機能を設定することもできます。

デバイスライフサイクル管理機能が有効にされているか、変更されている場合、システムが各オフラインデバイスのオフライン日をチェックし、24 時間以内にステータスを更新します。たとえば、40 日間オフラインになっているデバイスがあり、デバイスライフサイクル管理機能が有効で、［オフラインになった日数］フィールドが 30 日に設定されると、24 時間以内にデバイスの状態が［非アクティブ］に変わります。別の例を挙げると、25 日間オフラインになっているデバイスがあり、［オフラインになった日数］フィールドが 30 日に設定されている場合、5 日経つと、オフラインのままと仮定してデバイスの状態が「非アクティブ」に設定されます。非アクティブとしてマークされたデバイスは、コンソールと通信していなくても継続的に保護されます。

コンソールは、デバイスがオフラインまたは非アクティブ状態のままになっている日数を追跡します。デバイスがコンソールと再び通信すると、デバイスの状態がオンラインに変わり、タイマーがリセットされます。

1. 管理コンソールで［設定］>［デバイスライフサイクル］をクリックします。
2. ［自動化されたデバイスライフサイクル管理を有効化］設定をオンにします。
   a) ［オフライン日数］フィールドで、デバイスのステータスが非アクティブに変更されるまでにデバイスがオフラインである必要がある日数（7 日から 180 日まで）を指定します。
3. 非アクティブなデバイスを削除するには、［非アクティブなデバイスを削除］設定をオンにします。
   a) ［非アクティブになった日数］フィールドで、デバイスがコンソールから自動的に削除されるまでにデバイスが非アクティブである必要がある日数（7 日から 180 日まで）を指定します。

   デバイスをコンソールから削除すると、デバイスのデータはコンソールから削除されますが、デバイス上でエージェントは削除されません。
4. ［保存］をクリックします。

終了したら：

- デバイスの状態を確認するには、［アセット］>［デバイス］で［状態］列を参照します。
- デバイスがデバイスライフサイクル管理に含まれているかどうかを確認するには、［アセット］>［デバイス］で［ライフサイクル管理］列を参照します。カラムが表示されない場合は、手動でカラムを表示する必要があります。
- オフラインになった後に非アクティブとしてマークされないように、デバイスをデバイスライフサイクル管理から除外するには、「CylancePROTECT Desktop デバイスおよび CylanceOPTICS デバイスの管理」を参照してください。

CylancePROTECT Desktop デバイスにインストールされているアプリケーションのリストの表示

CylancePROTECT Desktop エージェントのバージョン 3.2 は、デバイスにインストールされているソフトウェアアプリケーションのリストをコンソールにレポートします。この機能を使用すると、デバイスにインストールされている脆弱性の原因となりうるアプリケーションを識別し、脆弱性に対するアクションに優先順位を付け、それに応じて管理していくことができます。デバイスにインストールされているすべてのアプリケーションを表示でき、また、個々のデバイスにインストールされているアプリケーションのリストも表示できます。この機能は、デバイスポリシーから有効にできます。

作業を始める前に：

- アプリケーションのリストをコンソールにレポートするには、Windows デバイス上で CylancePROTECT Desktop エージェントのバージョン 3.2 以降を実行している必要があります。
- デバイスには、ソフトウェアインベントリ機能をオンにするデバイスポリシーを割り当てる必要があります。

次の操作のいずれかを実行します。

タスク	手順
テナント内のデバイスにインストールされているすべてのアプリケーションのリストの表示	**a.** コンソールで、［アセット］ **>** ［インストールされているアプリケーション］に移動します。 **b.** アプリケーション名をクリックすると、そのアプリケーションがインストールされているデバイスのリストが表示されます。デバイス名をクリックすると、そのデバイスにインストールされているアプリケーションのリストなど、デバイスの詳細が表示されます。
個々のデバイスにインストールされているアプリケーションのリストの表示	**a.** コンソールで、［アセット］ **>** ［デバイス］に移動します。 **b.** デバイス名をクリックします。 **c.** ［脅威と活動］セクションで、［インストールされているアプリケーション］タブをクリックします。

ユーザーアカウントに登録した FIDO デバイスの削除

ユーザーが登録した FIDO デバイスは削除することができます。たとえば、登録済みデバイスを紛失した場合や、ユーザーが組織を離れた場合に、そのデバイスを削除できます。

1. 管理コンソールのメニューバーで、［アセット］ **>** ［ユーザー］をクリックします。
2. ［アクション］ドロップダウンリストで、［**FIDO** デバイスを管理］をクリックします。
3. ［**FIDO** デバイスを管理］ダイアログでデバイスを選択し、［削除］をクリックします。

保護されていないデバイスの検出

管理コンソールでは、Active Directory から検出され、CylancePROTECT Desktop で保護されていない既知のデバイスをリストで表示できます。表示される既知のデバイスは、CylancePROTECT のインストールをサポートする OS バージョンを実行しているデバイスです。また、デバイスリストをエクスポートし、これらのデバイスに必要なアクション（CylancePROTECT のインストールなど）を実行して、潜在的な脅威からデバイスとネットワークを保護することもできます。

作業を始める前に：［保護されていないデバイスの検出］サービスが有効になっていることを確認します。詳細については、「保護されていないデバイスの検出の有効化」を参照してください。

1. 管理コンソールのメニューバーで、［アセット］ **>** ［保護されていないデバイス］をクリックします。

   デバイスの保護制御ステータスは、次のいずれかになります。

   - サポート対象：検出されたデバイスは、CylancePROTECT Desktop でサポートされている OS バージョンを実行しています。
   - サポート対象外：検出されたデバイスは、CylancePROTECT Desktop でサポートされている OS バージョンを実行していません。
   - 情報不足：十分な情報がないため、デバイスで実行中の OS バージョンが CylancePROTECT Desktop でサポートされているかどうかを判断できません。
2. 次のいずれかの操作を実行します。

   - 列を追加または削除するには、|||| をクリックし、表示する列を選択します。
   - 列をフィルタリングするには、列見出しをクリックします。

- 保護されていないデバイスを .csv ファイルにエクスポートするには、 をクリックします。テーブルの全列をエクスポートすることも、［現在のフィルター］でフィルタリングされた列のみをエクスポートすることも可能です。［エクスポート］をクリックします。

保護されていないデバイスの検出の有効化

新しく追加されたテナントをスキャンし、CylancePROTECT Desktop による保護のされていない既知デバイスを検出して［保護されていないデバイス］画面で一覧表示させるには、［保護されていないデバイスの検出］サービスを有効にする必要があります。このサービスを有効にするオプションが利用可能になるのは、BlackBerry Connectivity Node とのディレクトリ接続のセットアップ後から 24 時間以内です。

このオプションは新しく追加されたテナントに対して最大 24 時間利用できませんが、サービスはスケジューラ上で動作しており、テナントリストおよび他のサービスからのデータを更新しています。この更新は 24 時間ごとに行われます。テナント情報が更新されると、その情報は Unprotected Device Discovery サービスで利用可能になり、これを有効化できるようになります。初めてこのサービスを有効にした場合、保護されていないデバイスが 2 分以内に一覧表示されます。サービスが有効になると、管理コンソールは保護されていないデバイスのリストを 24 時間ごとに更新します。デフォルトでは、各テナントでこの機能は無効になっています。

作業を始める前に：

- ディレクトリ接続の構成で最新バージョンの BlackBerry Connectivity Node が使用されていることを確認します。詳細については、セットアップガイドで「BlackBerry Connectivity Node のインストール」に関するコンテンツを参照してください。
- 保護されていない管理対象デバイスのデバイス OS および OS バージョンを表示するように環境を設定。
- この機能を有効にするための適切な権限をユーザーが持っていることを確認します。権限の詳細については、セットアップコンテンツの「管理者ロールの権限」を参照してください。次の権限が必要です。
  - ディレクトリ接続を表示するユーザーには「ディレクトリ接続を表示」権限が必要です。
  - この機能を有効または無効にするユーザーには「ディレクトリ接続を編集」権限が必要です。

1. 管理コンソールのメニューバーで、［設定］ > ［ディレクトリ接続］をクリックします。
2. ［ディレクトリ接続］リストで、保護されていないデバイスの検出を有効にする接続をクリックします。
3. ［同期設定］タブで、［保護されていないデバイスの検出］を選択します。
4. プロンプトが表示されたら［確認］をクリックして、この設定を環境内のすべてのディレクトリ接続に適用させます。

保護されていない管理対象デバイスのデバイス OS および OS バージョンを表示するように環境を設定

保護されていないデバイスの機能でデバイス OS および OS バージョンを表示するには、必要な属性をドメインコントローラーからグローバルカタログに同期できるようにスキーマを設定する必要があります。

1. Active Directory ドメインコントローラーで、次の手順を実行して Schmmgmt.dll を登録し、スキーマオプションを MMC に追加します。
   a) ドメインコントローラーで、**[スタート] > [ファイル名を指定して実行]** をクリックします。
   b) 検索フィールドに「`regsvr32 schmmgmt.dll`」と入力します。［**OK**］をクリックします。
   c) 操作が完了したら、**[OK]** をクリックします。
2. MMC で、Active Directory スキーマを開き、次の操作を実行します。
   a) **[スタート] > [ファイル名を指定して実行]** をクリックします。
   b) 検索フィールドに「`mmc.exe`」と入力します。［**OK**］をクリックします。

c) **[ファイル]** メニューの **[スナップインの追加と削除]** をクリックします。
d) **[Active Directory** スキーマ**]** をクリックします。
e) ［追加］をクリックします。
f) ［閉じる］をクリックします。［**OK**］をクリックします。

3. グローバルカタログと同期するように属性を更新するには、次の操作を実行します。
   a) Active Directory スキーマビューの左側の列で、**[属性]** をクリックします。
   b) 属性リストで、「**operatingSystem**」を検索し、クリックします。
   c) **[グローバルカタログにこの属性をレプリケートする]** チェックボックスをオンにします。
   d) ［**OK**］をクリックします。
   e) 次下の属性について、手順 a〜d を繰り返します。
      - operatingSystemServicePack
      - operatingSystemVersion

CylancePROTECT Desktop によって検出された脅威の管理

デバイスとは、デスクトップコンピュータやサーバーなど、CylancePROTECT Desktop エージェントがインストールされているエンドポイントです。デバイスは、管理コンソールまたは Cylance ユーザー API を使用して管理できます。管理アクションには、脅威イベントやその他のアラートの確認、正しいデバイスポリシーと設定がデバイスに割り当てられていることの確認、ゾーンを使用したデバイス管理のグループ化と簡素化が含まれます。

CylancePROTECT Desktop 脅威アラートの管理

管理コンソールを使用して、CylancePROTECT Desktop エージェントが検出した脅威アラートを表示および管理できます。安全でないと見なされるファイルまたは異常と見なされるファイルが管理コンソールに表示されます。安全と見なされるファイルは、コンソールに表示されません。

1. 管理コンソールのメニューバーで、［保護］ > ［脅威］をクリックします。次の操作のいずれかを実行します。
   - 列を追加または削除するには、  をクリックし、表示する列を選択します。
   - 脅威アラート情報を 1 つ以上の列でグループ化するには、対象の列を列名の上のスペースにドラッグします。
   - 脅威アラートを列の昇順または降順に並べ替えるには、列をクリックします。
   - 列で脅威アラートをフィルタリングするには、列のフィルターフィールドとアイコンを使用します。脅威アラートをフィルタリングしたら、ページをブックマークしてこれらのフィルターを保存します。フィルターをブックマークとして保存する機能は、脅威アラートにのみ使用できます。
2. 次の操作のいずれかを実行します。

タスク	手順
脅威アラートの詳細を表示します。	脅威アラートの行をクリックします。
脅威の詳細ページを表示します。	ファイル名をクリックします。
脅威フィルターを使用します。	脅威フィルターをクリックします。［閉じる］アイコンをクリックして、脅威フィルターをクリアします。
脅威インジケータを表示します。	［脅威インジケータ］セクションを展開します。脅威インジケータの詳細については、「脅威インジケータ」を参照してください。

タスク	手順
グローバルリストにファイルを追加します。	グローバル隔離リストまたはグローバルセーフリストにファイルを追加します。 **a.** グローバルリストに追加するファイルのチェックボックスをクリックします。 **b.** ［グローバル隔離］をクリックして、グローバル隔離リストにファイルを追加します。［セーフ］をクリックして、グローバルセーフリストにファイルを追加します。
ローカルリストにファイルを追加します。	ローカル隔離リストまたはローカルセーフリストにファイルを追加します。ローカルリストはグローバルリストよりも優先されます。たとえば、組織からのファイルをブロックし、特定のデバイス上のファイルを許可することができます。 **a.** 脅威アラートの行をクリックします。 **b.** ［デバイス］リストの［危険］または［異常］で、該当するデバイスのチェックボックスをオンにします。 **c.** ［隔離］をクリックして、ローカル隔離リストにファイルを追加します。［放棄］をクリックして、ローカルセーフリストにファイルを追加します。
ファイルのローカルリストを変更します。	ファイルは、ローカル隔離リストからローカルセーフリストに、またはローカルセーフリストからローカル隔離リストに変更できます。 **a.** 脅威アラートの行をクリックします。 **b.** ［デバイス］リストの［隔離済み］または［放棄済み］で、該当するデバイスのチェックボックスをオンにします。 **c.** ［放棄済み］リストが表示されている場合は、［隔離］をクリックして、ローカル隔離リストにファイルを追加します。［隔離済み］リストが表示されている場合は、［放棄］をクリックして、ローカルセーフリストにファイルを追加します。

終了したら： 脅威情報を .csv ファイルにエクスポートするには、  をクリックします。エクスポートの範囲を選択し、［エクスポート］をクリックします。

脅威インジケータ

各カテゴリは、悪意のあるソフトウェアで頻繁に検出される領域を表します。

変則

これらのインジケータは、何らかの形で不整合があったり、異常があったりする要素をファイルが持っていることを示します。多くの場合、ファイル内の構造的な要素に不整合があります。

インジケータ	説明
16bitSubsystem	このファイルは、16 ビットサブシステムを使用しています。マルウェアはこれを使用して、オペレーティングシステムの安全性が低く、十分に監視されていない部分に存在し、頻繁に特権昇格攻撃を実行します。
Anachronism	この PE は、記述された時期を偽っているようです。これは、正規のソフトウェアでは異例なことです。
AppendedData	この PE には、ファイルの通常の領域を超えて、追加のコンテンツが付加されています。付加されたデータは悪意のあるコードやデータを埋め込むために頻繁に使用され、保護システムから見落とされることが頻繁にあります。
AutoitDbgPrivilege	AutoIT スクリプトがデバッグアクティビティを実行できます。
AutoitManyDllCalls	AutoIT スクリプトが多くの外部 DLL 呼び出しを使用しています。AutoIT ランタイムには、多数の一般的な機能が既にあるため、外部 DLL から追加の機能を使用することは、悪意があることの兆候である可能性があります。
AutoitMutex	AutoIT スクリプトが同期オブジェクトを作成しています。これは、同じターゲットの複数回の感染を防止するためにマルウェアによって使用されることがよくあります。
AutoitProcessCarving	AutoIT スクリプトが、別のプロセスから来ているようなコードを実行するプロセスカービングを実行している可能性があります。これは、検出を妨害するために行われることがよくあります。
AutoitProcessInjection	AutoIT スクリプトが、おそらく検出されずに留まったりデータを盗んだりするために、他のプロセスのコンテキストでコードを実行するプロセスインジェクションを実行している可能性があります。
AutoitRegWrite	AutoIT スクリプトが Windows レジストリに書き込んでいます。
Base64Alphabet	このファイルは、アルファベットの Base64 エンコーディングを使用している証拠を含んでいます。マルウェアは、一般的な検出を回避することを試みたり、Base64 エンコーディングを使用している他のプログラムを攻撃したりしようとして、これを行います。
CommandlineArgsImport	ファイルは、コマンドラインから引数を読み取るために使用できる関数をインポートします。マルウェアは、これを使用して、以後の実行に関する情報を収集します。
ComplexMultipleFilters	ファイルが、複数のフィルターを持つ複数のストリームを含んでいます。
ComplexObfuscatedEncoding	ファイルが、難読化された名前を異常に多く含んでいます。

インジケータ	説明
ComplexUnsupportedVersion EmbeddedFiles	ファイルが、ファイルで宣言されている PDF 規格より新しいバージョンの EmbeddedFiles 機能を使用しています。
ComplexUnsupportedVersionFlate	ファイルが、ファイルで宣言されている PDF 規格より新しいバージョンの FlateDecode 機能を使用しています。
ComplexUnsupportedVersionJbig2	ファイルが、ファイルで宣言されている PDF 規格より新しいバージョンの JBIG2Decode 機能を使用しています。
ComplexUnsupportedVersionJs	ファイルが、ファイルで宣言されている PDF 規格より新しいバージョンの JavaScript 機能を使用しています。
ComplexUnsupportedVersionXFA	ファイルが、ファイルで宣言されている PDF 規格より新しいバージョンの XFA 機能を使用しています。
ComplexUnsupportedVersionXobject	ファイルが、ファイルで宣言されている PDF 規格より新しいバージョンの XObject 機能を使用しています。
ContainsFlash	ファイルが flash オブジェクトを含んでいます。
ContainsPE	ファイルには埋め込み実行可能ファイルが含まれています。
ContainsU3D	ファイルが U3D オブジェクトを含んでいます。
InvalidCodePageUsed	ファイルが、おそらく検出を回避するために、無効または認識されないロケールを使用しています。
InvalidData	ファイルのメタデータが明らかに偽造であるか、破損しています。
InvalidStructure	ファイル構造が無効です。サイズ、メタデータ、または内部セクター割り当てテーブルが間違っています。これは、エクスプロイトを示している可能性があります。
ManifestMismatch	このファイルは、マニフェスト内の不整合を示しています。マルウェアは、検出を回避するためにこれを行いますが、追跡を深く隠すことはまれです。
NontrivialDLLEP	この PE は、非自明なエントリポイントを持つ DLL です。これは DLL 間では一般的ですが、悪意のある DLL がそのエントリポイントを利用してプロセス内に入り込む可能性があります。
NullValuesInStrings	ファイル内のいくつかの文字列が、途中に null 文字を含んでいます。
PDFParserArraysContainsNullCount	ファイルが、配列内に null 値を異常に多く含んでいます。
PDFParserArraysHeterogeneous Count	ファイルが、異常に多くの異種類の要素を含む配列を含んでいます。

インジケータ	説明
PDFParserMailtoURICount	ファイルが、異常に多くのメールリンク（mailto:）を含んでいます。
PDFParserMinPageCount	ファイルのページオブジェクトの構造が異常です。ノードごとに多数の子ページオブジェクトがあります。
PDFParserNamesPoundName MaxLength	ファイルが、長いエンコード文字列を使用してコンテンツを難読化しようとしている可能性があります。
PDFParserNamesPoundName MinLength	ファイルが、異常に大きな最小長のエスケープされた名前を含んでいます。
PDFParserNamesPoundName TotalLength	ファイルが、コンテンツの多くをエンコード文字列に格納することでコンテンツを難読化しようとしている可能性があります。
PDFParserNamesPoundName UpperCount	ファイルが、大文字の 16 進数値でエスケープされた名前を異常に多く含んでいます。
PDFParserNamesPoundName ValidCount	ファイルが、異常に多くの有効でエスケープされた名前を含んでいます。
PDFParserNamesPoundPerName MaxCount	ファイルが、異常に大きな最大数のエスケープされた文字（1 つの名前あたり）を含んでいます。
PDFParserNamesPound UnnecessaryCount	ファイルが、異常に多くの不必要にエスケープされた名前を含んでいます。
PDFParserNumbersLeading DigitTallies8	ファイルが、10 進数表現の 8 で始まる数値を異常に多く含んでいます。
PDFParserNumbersPlusCount	ファイルが、明示的なプラス記号付きの数値を異常に多く含んでいます。
PDFParserNumbersRealMax RawLength	ファイルが、異常に大きな最大長の実数を含んでいます。
PDFParserPageCounts	ファイルが、異常に多くの子ページオブジェクトを含んでいます。
PDFParserPageObjectCount	ファイルが、異常に多くのページオブジェクトを含んでいます。
PDFParserSizeEOF	ファイルが、異常に長い「ファイルの最後」シーケンスを含んでいます。
PDFParserStringsHexLowerCount	ファイルが、小文字の 16 進数桁でエスケープされた文字列を異常に多く含んでいます。

インジケータ	説明
PDFParserStringsLiteralString MaxLength	ファイルが、異常に大きな最大長のリテラル文字列を含んでいます。
PDFParserStringsOctalZero PaddedCount	ファイルが、文字列内で 8 進数エスケープされた文字を異常に多く含んでおり、文字列が不必要にゼロパディングされています。
PDFParserTrailerSpread	ファイルが、トレーラーオブジェクト間に異常に大きいスプレッドを含んでいます。
PDFParserWhitespaceComment MaxLength	ファイルが、異常に大きな最大長のコメントを含んでいます。
PDFParserWhitespaceComment MinLength	ファイルが、リーダーソフトウェアによって使用されていない、異常に短いコメントを含んでいます。
PDFParserWhitespaceComment TotalLength	ファイルが、異常に大量のコメントアウトされたデータを含んでいます。
PDFParserWhitespaceEOL0ACount	ファイルが、異常に多くの短い行末文字を含んでいます。
PDFParserWhitespaceWhitespace 00Count	ファイルが、空白として使用される 0 バイトを異常に多く含んでいます。
PDFParserWhitespaceWhitespace 09Count	ファイルが、空白として使用される 09 バイトを異常に多く含んでいます。
PDFParserWhitespaceWhitespace LongestRun	ファイルが、異常に長い空白領域を含んでいます。
PDFParserWhitespaceWhitespace TotalLength	ファイルが、異常に大量の空白を含んでいます。
PDFParseru3DObjectsNames AllNames	ファイルが、異常に多くの U3D オブジェクトを含んでいます。
PossibleBAT	このファイルは、標準的な Windows バッチファイルを持っている証拠を含んでいます。マルウェアは、一般的なスキャン技術を回避し、永続性を可能にするためにこれを行います。
PossibleDinkumware	このファイルは、Dinkumware の一部のコンポーネントを含む証拠を示しています。Dinkumware は、さまざまなマルウェアコンポーネントで頻繁に使用されています。
PropertyImpropriety	ファイルが、疑わしい OOXML プロパティを含んでいます。

インジケータ	説明
RaiseExceptionImports	このファイルは、プログラム内で例外を発生させるために使用する関数をインポートします。マルウェアは、標準的な動的コード分析をたどるのを困難にする戦術を実装するために、これを行います。
ReservedFieldsViolation	ファイルが、予約されたフィールドの使用に関する指定に違反しています。
ResourceAnomaly	このファイルは、リソースセクションに異常を含んでいます。マルウェアは、DLL のリソースセクションに不正なビットや他の変則的なビットを含んでいることが頻繁にあります。
RWXSection	この PE は、修正可能なコードを含んでいる可能性があります。これは、最善の場合でも非正統的、最悪の場合にはウイルス感染の症状を示すものです。この特徴は、ファイルが標準以外のコンパイラを使用してビルドされたか、最初にビルドされた後に変更されたことを意味することがあります。
SectorMalfeasance	ファイルが、OLE セクター割り当ての構造的な異常を含んでいます。
StringInvalid	文字列テーブル内の文字列への参照のいずれかが、負のオフセットを指していました。
StringTableNotTerminated	文字列テーブルが null バイトで終了しませんでした。これにより、実行時に、終了しない文字列による障害が発生する可能性があります。
StringTruncated	文字列テーブル内の文字列への参照のいずれかが、ファイルの最後より後の位置を指していました。
SuspiciousPDataSection	この PE は「PDATA」領域に何かを隠していますが、何であるかが不明です。PE ファイルの pdata 領域は一般的に、ランタイム構造の処理に使用されますが、この特定のファイルには他のものが含まれています。
SuspiciousRelocSection	この PE は「relocations」領域に何かを隠していますが、何であるかが不明です。PE ファイルの relocations 領域は一般的に、特定のシンボルの再配置に使用されますが、この特定のファイルには他のものが含まれています。
SuspiciousDirectoryNames	ファイルが、悪に関連付けられている OLE ディレクトリ名です。
SuspiciousDirectoryStructure	ファイルに、OLE ディレクトリ構造の異常があります。
SuspiciousEmbedding	ファイルが、OLE の疑わしい埋め込みを使用しています。
SuspiciousVBA	ファイルが、疑わしい VBA コードを含んでいます。
SuspiciousVBALib	ファイルが、疑わしい VBA ライブラリ使用を示しています。

インジケータ	説明
SuspiciousVBANames	ファイルが、VBA 構造に関連付けられた疑わしい名前を含んでいます。
SuspiciousVBAVersion	ファイルが、疑わしい VBA バージョンを含んでいます。
SWFOddity	ファイルが、埋め込まれた SWF の特定の疑わしい使用状況を含んでいます。
TooMalformedToProcess	ファイルの形式が非常に不正なため、完全には解析できませんでした。
VersionAnomaly	このファイルには、バージョン情報の表示方法に関する問題があります。マルウェアには、検出を回避するためにこれがあります。

コレクション

これらのインジケータは、データ収集の機能や証拠を示す要素をファイルが持っていることを示します。これには、システム構成の列挙や特定の機密情報の収集が含まれる可能性があります。

インジケータ	説明
BrowserInfoTheft	このファイルは、ブラウザーキャッシュに保存されているパスワードを読み取る意図の証拠を含んでいます。マルウェアは、これを使用して窃盗のためにパスワードを収集します。
CredentialProvider	このファイルは、資格情報プロバイダーとのやり取り、または資格情報プロバイダーのように見せようとする証拠を含んでいます。マルウェアがこれを行うのは、資格情報プロバイダーはユーザー名やパスワードといった多種類の機密データにアクセスできるため、資格情報プロバイダーとして機能することで認証の整合性を妨害できる可能性があるからです。
CurrentUserInfoImports	このファイルは、現在ログインしているユーザーに関する情報を収集するために使用される関数をインポートします。マルウェアは、これを使用して特権の昇格経路を特定し、攻撃をより適切に調整します。
DebugStringImports	このファイルは、デバッグ文字列の出力に使用される関数をインポートします。通常、これは、本番ソフトウェアでは無効になっていますが、テスト中のマルウェアではオンのままになっています。
DiskInfoImports	このファイルは、システム上のボリュームの詳細を収集するために使用できる関数をインポートします。マルウェアは、これを一覧表示と組み合わせて使用して、将来の攻撃に備えてボリュームに関する事実を特定します。
EnumerateFileImports	このファイルは、ファイルの一覧表示に使用される関数をインポートします。マルウェアは、これを使用して機密データを探したり、さらなる攻撃ポイントを見つけたりします。

インジケータ	説明
EnumerateModuleImports	このファイルは、実行中のプロセスが使用するすべての DLL を一覧表示するために使用できる関数をインポートします。マルウェアは、この機能を使用して、プロセス内にロードする特定のライブラリを見つけてターゲットにし、注入しようとするプロセスをマップします。
EnumerateNetwork	このファイルは、接続されたネットワークとネットワークアダプタを数え上げる機能の証拠を示しています。マルウェアは、ターゲットシステムが他のシステムに対してある位置を特定し、考えられる横方向のパスを探すためにこれを行います。
EnumerateProcessImports	このファイルは、システム上で実行中のすべてのプロセスを一覧表示するために使用できる関数をインポートします。マルウェアは、この機能を使用して、注入するプロセスまたは削除しようとするプロセスを特定します。
EnumerateVolumeImports	このファイルは、システム上のボリュームを一覧表示するために使用できる関数をインポートします。マルウェアは、これを使用して、データを検索したり感染を広げたりするのに必要な可能性がある領域をすべて見つけます。
GinaImports	このファイルは、Gina へのアクセスに使用される関数をインポートします。マルウェアは、安全な Ctrl-Alt-Del パスワード入力システムまたはその他のネットワークログイン機能に違反しようとして、これを行います。
HostnameSearchImports	このファイルは、ネットワーク上のホスト名とマシン自体のホスト名に関する情報を収集するために使用できる関数をインポートします。マルウェアは、この機能を使用して、さらなる攻撃の標的の精度を上げたり、スキャンして新しい標的を探したりします。
KeystrokeLogImports	このファイルは、キーボードからキーストロークをキャプチャして記録できる関数をインポートします。マルウェアは、これを使用してキーストロークをキャプチャして保存し、パスワードなどの機密情報を見つけます。
OSInfoImports	このファイルは、現在のオペレーティングシステムに関する情報を収集するために使用される関数をインポートします。マルウェアは、これを使用して、さらなる攻撃をより適切に調整する方法を特定し、情報をコントローラーに報告します。
PossibleKeylogger	ファイルには、キーロガータイプのアクティビティの証拠が含まれています。マルウェアは、キーロガーを使用してキーボードから機密情報を収集します。
PossiblePasswords	このファイルは、一般的なパスワードを含む証拠があるか、一般的なパスワードの総当たり攻撃を有効にする構造を持っています。マルウェアは、これを使用して、パスワードを介して他のリソースにアクセスすることでネットワークへの侵入を試みます。
ProcessorInfoWMI	このファイルは、プロセッサの詳細を特定するために使用できる関数をインポートします。マルウェアは、これを使用して攻撃を調整し、このデータを共通のコマンド&コントロールインフラストラクチャに流出させます。

インジケータ	説明
RDPUsage	このファイルは、リモートデスクトッププロトコル（RDP）とのやり取りの証拠を示します。マルウェアは、これを使用して横展開し、直接的なコマンド&コントロール機能を提供することが頻繁にあります。
SpyString	このファイルは、アクセシビリティ API の使用を介してクリップボードまたはユーザーアクションを監視している可能性があります。
SystemDirImports	このファイルは、システムディレクトリの特定に使用される関数をインポートします。マルウェアは、これを行って、インストールされているシステムバイナリの多くがある場所を見つけます。システムディレクトリは、システムバイナリの中に隠れていることが多いためです。
UserEnvInfoImports	このファイルは、現在ログインしているユーザーの環境に関する情報を収集するために使用される関数をインポートします。マルウェアは、これを使用して、ログインしたユーザーの詳細を特定し、環境変数から収集できる他のインテリジェンスを探します。

データ損失

これらのインジケータは、データの窃盗の機能や証拠を示す要素をファイルが持っていることを示します。これには、送信ネットワーク接続、ブラウザーとして機能している証拠、および他のネットワーク通信が含まれる可能性があります。

インジケータ	説明
AbnormalNetworkActivity	このファイルは、非標準的なネットワークを実装しています。マルウェアはこれを行って、より一般的なネットワークアプローチの検出を回避します。
BrowserPluginString	ブラウザプラグインを列挙またはインストールする機能がファイルにあります。
ContainsBrowserString	このファイルには、カスタムUserAgent文字列を作成しようとしている証拠が含まれています。マルウェアは、一般的な UserAgent 文字列を使用して、送信される要求での検出を回避することが頻繁にあります。
DownloadFileImports	このファイルは、ファイルをシステムにダウンロードするために使用できる関数をインポートします。マルウェアは、これをさらに攻撃を企てる手段としても、送信 URL を介してデータを流出させるための手段としても使用します。
FirewallModifyImports	このファイルは、ローカル Windows ファイアウォールの変更に使用される関数をインポートします。マルウェアは、これを使用して穴を開け、検出を回避します。
HTTPCustomHeaders	このファイルは、他のカスタム HTTP ヘッダーの作成の証拠を含んでいます。マルウェアは、コマンド&コントロールインフラストラクチャとのやり取りを促進し、検出を回避するためにこれを行います。

インジケータ	説明
IRCCommands	このファイルは、IRC サーバーとのやり取りの証拠を含んでいます。マルウェアは一般的に、IRC を使用してコマンド&コントロールインフラストラクチャを促進します。
MemoryExfiltrationImports	このファイルは、実行中のプロセスからメモリを読み取るために使用できる関数をインポートします。マルウェアは、これを使用して、自身を注入する適切な場所を決定したり、実行中のプロセスのメモリからパスワード、クレジットカード、その他の機密情報などの有用な情報を抽出したりします。
NetworkOutboundImports	このファイルは、データをローカルネットワークまたは一般のインターネットに送信するために使用できる機能をインポートします。マルウェアは、データの窃盗またはコマンド&コントロールの手段としてこれを使用します。
PipeUsage	このファイルは、名前付きパイプの操作を可能にする関数をインポートします。マルウェアは、通信およびデータ窃盗の手段としてこれを使用します。
RPCUsage	このファイルは、リモートプロシージャコール（RPC）インフラストラクチャとの通信を可能にする関数をインポートします。マルウェアは、これを使用して広がったり、データをリモートシステムに送信して流出させたりします。

詐欺

これらのインジケータは、ファイルに欺瞞を試みる機能や証拠があることを示す要素をファイルが持っていることを示します。デセプションは、隠されたセクション、検出を回避するためのコード、メタデータやその他のセクションにおける不適切なラベル付けなどの形をとることがあります。

インジケータ	説明
AddedHeader	ファイルが、悪意のある隠れたペイロードの可能性がある、難読化された追加の PE ヘッダーを含んでいます。
AddedKernel32	ファイルが、kernel32.dll（悪意のあるペイロードによって使用される可能性があるライブラリ）への、難読化された追加の参照を含んでいます。
AddedMscoree	ファイルが、mscoree.dll（悪意のあるペイロードによって使用される可能性があるライブラリ）への、難読化された追加の参照を含んでいます。
AddedMsvbvm	ファイルが、msvbvm（Microsoft Visual Basic 6 用にコンパイルされた、悪意のあるペイロードによって使用される可能性があるライブラリ）への、難読化された追加の参照を含んでいます。

インジケータ	説明
AntiVM	このファイルは、プロセスが仮想マシンで実行されているかどうかを特定するために使用できる機能を示しています。マルウェアは、一般的になりつつある仮想化されたサンドボックスでの実行を回避するためにこれを行います。
AutoitDownloadExecute	AutoIT スクリプトがファイルをダウンロードし、実行できます。これは、悪意のある追加ペイロードを配信するために行われることがよくあります。
AutoitObfuscationStringConcat	AutoIT スクリプトが、文字列連結で難読化されている可能性があります。これは、（全体的に）疑わしいコマンドの検出を回避するために行われることがよくあります。
AutoitShellcodeCalling	AutoIT スクリプトが CallWindowProc() Windows API 関数を使用していますが、これはシェルコードの注入を示している可能性があります。
AutoitUseResources	AutoIT スクリプトが、スクリプトとともに保存されているリソースデータを使用しています。マルウェアは多くの場合、重要な部分をリソースデータとして保存し、実行時に展開します。したがって、これは疑わしいように見えます。
CabinentUsage	このファイルは、CAB ファイルを含んでいる証拠を示しています。マルウェアは、多くの検出システムが認識できないような方法で機密性の高いコンポーネントをパッケージ化するためにこれを行います。
ClearKernel32	ファイルが、kernel32.dll（悪意のあるペイロードによって使用される可能性があるライブラリ）への参照を含んでいます。
ClearMscoree	ファイルが、mscoree.dll（悪意のあるペイロードによって使用される可能性があるライブラリ）への参照を含んでいます。
ClearMsvbvm	ファイルが、msvbvm.dll（Microsoft Visual Basic 6 用にコンパイルされた、悪意のあるペイロードによって使用される可能性があるライブラリ）への参照を含んでいます。
ComplexInvalidVersion	ファイルが、誤った PDF バージョンを宣言しています。
ComplexJsStenographySuspected	ファイルが、リテラル文字列に隠された JavaScript コードを含んでいる可能性があります。
ContainsEmbeddedDocument	このファイルには、オブジェクト内に埋め込まれたドキュメントが含まれています。マルウェアはこれを使用して、攻撃を複数のソースに分散したり、実際の形を隠したりできます。
CryptoKeys	このファイルは、埋め込まれた暗号化キーを持っている証拠を含んでいます。マルウェアは、検出を回避するために、そしておそらくはリモートサービス認証としてこれを行います。

インジケータ	説明
DebugCheckImports	このファイルは、デバッガのように動作できるようにする関数をインポートします。マルウェアは、この機能を使用して他のプロセスから読み書きします。
EmbeddedPE	この PE 内には追加の PE があります。これは通常、ソフトウェアインストールプログラムでのみ見られます。マルウェアは、まず PE ファイルを埋め込んでから、ディスクにドロップして PE を実行することが頻繁にあります。この手法は多くの場合、基礎になっているスキャン技術が理解できない形式でバイナリをパッケージ化して保護スキャナを回避するために使用されます。
EncodedDosStub1	PE が、悪意のある隠れたペイロードに属している可能性がある難読化された PE DOS スタブを含んでいます。
EncodedDosStub2	PE が、悪意のある隠れたペイロードに属している可能性がある難読化された PE DOS スタブを含んでいます。
EncodedPE	この PE 内には、追加の PE が隠されています。これは非常に疑わしい行動です。EmbeddedPE インジケータと似ていますが、エンコーディング方式を使用して、オブジェクト内のバイナリをさらに隠そうとしています。
ExecuteDLL	この PE は、一般的なメソッドを使用して DLL を実行する機能の証拠を含んでいます。マルウェアは、一般的な検出方法を回避するための手段としてこれを行います。
FakeMicrosoft	この PE は、Microsoft によって記述されたと主張していますが、Microsoft PE のようには見えません。マルウェアは一般的に、Microsoft PE になりすまそうとします。目立たないように見えるためです。
HiddenMachO	ファイルの内部に別の MachO 実行可能ファイルがあります。これは、適切に宣言されていません。これは、ペイロードが容易に検出されないように隠す試みである可能性があります。
HTTPCustomUserAgent	このファイルは、ブラウザー UserAgent の操作の証拠を含んでいます。マルウェアは、コマンド&コントロールとのやり取りを促進し、検出を回避するためにこれを行います。
InjectProcessImports	PE が、他のプロセスにコードを注入できます。この機能は多くの場合、プロセスが何らかの形で欺瞞を試みているか、敵意を持っていることを意味します。
InvisibleEXE	この PE は、見えない状態で実行されるようですが、バックグラウンドサービスではありません。隠れたままになるように設計されている可能性があります。

インジケータ	説明
JSTokensSuspicious	ドキュメントが、異常に疑わしい JavaScript を含んでいます。
MSCertStore	このファイルは、コア Windows 証明書ストアとのやり取りの証拠を示しています。マルウェアは、資格情報を収集し、不正な鍵をストリームに挿入して、中間者攻撃などのことを促進するためにこれを行います。
MSCryptoImports	ファイルが、コア Windows 暗号化ライブラリを使用する関数をインポートします。マルウェアは、独自の暗号化を持ち歩かずに済むように、これを使用して、ローカルにインストールされた暗号化を活用します。
PDFParserDotDotSlash1URICount	ファイルが、「../」など相対パスを使用してパストラバーサルを試みる可能性があります。
PDFParserJavaScriptMagicseval~28	ファイルが、難読化された JavaScript を含んでいる可能性があるか、eval() で動的にロードされた JavaScript を実行できます。
PDFParserJavaScriptMagic sunescape~28	ファイルが、難読化された JavaScript を含んでいる可能性があります。
PDFParserjsObjectsLength	ファイルが、異常に多くの個別 JavaScript スクリプトを含んでいます。
PDFParserJSStreamCount	ファイルが、異常に多くの JavaScript 関連のストリームを含んでいます。
PDFParserJSTokenCounts0 cumulativesum	ファイルが、異常に多くの JavaScript トークンを含んでいます。
PDFParserJSTokenCounts1 cumulativesum	ファイルが、異常に多くの JavaScript トークンを含んでいます。
PDFParserNamesAllNames Suspicious	ファイルが、異常に多くの疑わしい名前を含んでいます。
PDFParserNamesObfuscatedNames Suspicious	ファイルが、難読化された名前を異常に多く含んでいます。
PDFParserPEDetections	ファイルが埋め込み PE ファイルを含んでいます。
PDFParserSwfObjectsxObservations SWFObjectsversion	ファイルが、異常なバージョン番号を持つ SWF オブジェクトを含んでいます。
PDFParserSwfObjectsxObservation sxSWFObjectsxZLibcmfSWFObjectsx ZLibcmf	ファイルが、異常な圧縮パラメーターを持つ SWF オブジェクトを含んでいます。

インジケータ	説明
PDFParserswfObjectsxObservations xSWFObjectsxZLibflg	ファイルが、異常な圧縮フラグパラメーターを持つ SWF オブジェクトを含んでいます。
PE_ClearDosStub1	ファイルが DOS スタブ（PE ファイルを含むことを示しています）を含んでいます。
PE_ClearDosStub2	ファイルが DOS スタブ（PE ファイルを含むことを示しています）を含んでいます。
PE_ClearHeader	ファイルが、ファイル構造に属していない PE ファイルヘッダーデータを含んでいます。
PEinAppendedSpace	ファイルが、ファイル構造に属していない PE ファイルを含んでいます。
PEinFreeSpace	ファイルが、ファイル構造に属していない PE ファイルを含んでいます。
ProtectionExamination	このファイルは、一般的な保護システムを探しているようです。マルウェアは、システムにインストールされている保護システムに合わせた反保護対策を開始するためにこれを行います。
SegmentSuspiciousName	セグメントに名前として無効な文字列があるか、標準的ではない異常な名前があります。これは、コンパイル後の改ざんか、packer や難読化ツールの使用を示している可能性があります。
SegmentSuspiciousSize	セグメントサイズが、内部のコンテンツ（セクション）の合計サイズと大きく異なります。これは、参照されていない領域の使用、または悪意のあるコードを実行時に展開するための領域の予約を示している可能性があります。
SelfExtraction	このファイルは自己解凍型アーカイブのようです。マルウェアは、この戦術を使用して真の意図を難読化することが頻繁にあります。
ServiceDLL	このファイルはサービス DLL のようです。サービス DLL は svchost.exe プロセスでロードされるため、マルウェアの一般的な永続手法です。
StringJsSplitting	ファイルが、疑わしい JS トークンを含んでいます。
SWFinAppendedSpace	ファイルが、ドキュメント構造に属していない Shockwave flash オブジェクトを含んでいます。
TempFileImports	このファイルは、一時ファイルにアクセスし、一時ファイルを操作するために使用される関数をインポートします。一時ファイルは検出を回避できる傾向があるため、マルウェアはこれを行います。

インジケータ	説明
UsesCompression	このファイルには、圧縮されているように見えるコード部分があります。マルウェアは、この手法を使用して検出を回避します。
VirtualProtectImports	このファイルは、実行中のプロセスからメモリを変更するために使用される関数をインポートします。マルウェアはこれを使用して、実行中のプロセスに自身を注入します。
XoredHeader	ファイルが、悪意のある隠れたペイロードの可能性がある、xor で難読化された PE ヘッダーを含んでいます。
XoredKernel32	ファイルが、kernel32.dll（悪意のあるペイロードによって使用される可能性があるライブラリ）への、xor で難読化された参照を含んでいます。
XoredMscoree	ファイルが、mscoree.dll（悪意のあるペイロードによって使用される可能性があるライブラリ）への、xor で難読化された参照を含んでいます。
XoredMsvbvm	ファイルが、msvbvm.dll（Microsoft Visual Basic 6 用にコンパイルされた、悪意のあるペイロードによって使用される可能性があるライブラリ）への、xor で難読化された参照を含んでいます。

破壊

これらのインジケータは、破壊の機能や証拠を示す要素をファイルが持っていることを示します。破壊的な機能には、ファイルやディレクトリなど、システムリソースを削除する機能が含まれます。

インジケータ	説明
action_writeByte	ドキュメント内の VBA スクリプトが、ファイルにバイトを書き込んでいる可能性があります。これは、正規のドキュメントでは異常な動作です。
action_hexToBin	ファイル内の VBA スクリプトが、16 進数から 2 進数への変換を使用していると思われます。これは、悪意のある隠れたペイロードのデコードを示している可能性があります。
appended_URI	ファイルが、ファイル構造に属していないリンクを含んでいます。
appended_exploit	ファイルが、疑わしいデータをファイル構造外に含んでいます。これは、エクスプロイトを示している可能性があります。
appended_macro	ファイルが、ファイル構造に属していないマクロスクリプトを含んでいます。

インジケータ	説明
appended_90_nopsled	ファイルが、ファイル構造に属していない nop スレッドを含んでいます。これはほぼ確実に、エクスプロイテーションを促進する目的で存在します。
AutorunsPersistence	ファイルが、永続性の一般的な手法（起動スクリプトなど）とのやり取りを試みます。マルウェアは一般的に、永続性を実現するためにこの戦術を使用します。
DestructionString	シェルコマンドを介してプロセスを強制終了したり、マシンをシャットダウンしたりする機能がファイルにあります。
FileDirDeleteImports	この PE は、ファイルまたはディレクトリを削除するために使用できる関数をインポートします。マルウェアは、これを使用してシステムを破壊し、痕跡を隠します。
JsHeapSpray	ファイルが、ヒープスプレーコードを含んでいる可能性があります。
PossibleLocker	このファイルは、一般的なツールをポリシーごとにロックアウトしようとしている証拠を示しています。マルウェアは、永続性を維持し、検出とクリーンアップをより困難にするためにこれを行います。
RegistryManipulation	このファイルは、Windows レジストリを操作するために使用できる関数をインポートします。マルウェアは、永続性を実現し、検出を回避するなど、多くの理由でこれを行います。
SeBackupPrivilege	この PE は、アクセスが許可されていないファイルの読み取りを試みる可能性があります。SeBackup 権限では、アクセス制御に関わりなくファイルにアクセスできます。この権限は、バックアップを処理するプログラムによって頻繁に使用され、多くの場合は管理ユーザーに限定されています。ただし、他の方法では難しい特定の要素へのアクセスを得るために悪意を持って利用される可能性もあります。
SeDebugPrivilege	この PE は、システムプロセスの改ざんを試みる可能性があります。SeDebug 権限は、自分のプロセス以外のプロセスにアクセスするために使用され、多くの場合は管理ユーザーに限定されています。この権限は、他のプロセスへの読み書きと組み合わされることがよくあります。
SeRestorePrivilege	この PE は、アクセスが許可されていないファイルの変更または削除を試みる可能性があります。SeRestore 特権では、アクセス制御を考慮せずに書き込むことができます。
ServiceControlImports	このファイルは、現在のシステムで Windows サービスを制御できる関数をインポートします。マルウェアは、これを使用して、自身をサービスとしてインストールすることによりバックグラウンドで起動したり、保護機能が存在する可能性のある他のサービスを無効にしたりします。

インジケータ	説明
SkylinedHeapSpray	ファイルが、変更されていないバージョンの skylined ヒープスプレーコードを含んでいます。
SpawnProcessImports	この PE は、別のプロセスを生成するために使用できる関数をインポートします。マルウェアはこれを使用して、感染の次の段階(通常はインターネットからダウンロード)を開始します。
StringJsExploit	ファイルが、エクスプロイテーションを行えると思われる JavaScript コードを含んでいます。
StringJsObfuscation	ファイルが JavaScript 難読化トークンを含んでいます。
TerminateProcessImports	このファイルは、実行中のプロセスを停止するために使用できる関数をインポートします。マルウェアはこれを使用して、保護システムを削除したり、実行中のシステムに損害を与えたりします。
trigger_AutoClose	ファイル内の VBA スクリプトが、ファイルを閉じるときに自動的に実行されようとしている可能性があります。
trigger_Auto_Close	ファイル内の VBA スクリプトが、ファイルを閉じるときに自動的に実行されようとしている可能性があります。
trigger_AutoExec	ファイル内の VBA スクリプトが、自動的に実行されようとしている可能性があります。
trigger_AutoExit	ファイル内の VBA スクリプトが、ファイルを閉じるときに自動的に実行されようとしている可能性があります。
trigger_AutoNew	ファイル内の VBA スクリプトが、新しいドキュメントが作成されるときに自動的に実行されようとしている可能性があります。
trigger_AutoOpen	ファイル内の VBA スクリプトが、ファイルが開かれたらすぐに実行されようとしている可能性があります。
trigger_Auto_Open	ファイル内の VBA スクリプトが、ファイルが開かれたらすぐに実行されようとしている可能性があります。
trigger_DocumentBeforeClose	ファイル内の VBA スクリプトが、ファイルが閉じる直前に自動的に実行されようとしている可能性があります。
trigger_DocumentChange	ファイル内の VBA スクリプトが、ファイルが変更されるときに自動的に実行されようとしている可能性があります。
trigger_Document_Close	ファイル内の VBA スクリプトが、ファイルを閉じるときに自動的に実行されようとしている可能性があります。

インジケータ	説明
trigger_Document_New	ファイル内の VBA スクリプトが、新しいファイルが作成されるときに自動的に実行されようとしている可能性があります。
trigger_DocumentOpen	ファイル内の VBA スクリプトが、ファイルが開かれたらすぐに実行されようとしている可能性があります。
trigger_Document_Open	ファイル内の VBA スクリプトが、ファイルが開かれたらすぐに実行されようとしている可能性があります。
trigger_NewDocument	ファイル内の VBA スクリプトが、新しいファイルが作成されるときに自動的に実行されようとしている可能性があります。
trigger_Workbook_Close	ファイル内の VBA スクリプトが、Microsoft Excel ブックを閉じるときに自動的に実行されようとしている可能性があります。
trigger_Workbook_Open	ファイル内の VBA スクリプトが、Microsoft Excel ブックを開くときに自動的に実行されようとしている可能性があります。
UserManagementImports	このファイルは、ローカルシステムのユーザーを変更するために使用できる関数をインポートします。鍵ユーザーの詳細を追加、削除、または変更できます。マルウェアはこの機能を使用して、永続性を実現したり、ローカルシステムに害を与えたりする可能性があります。
VirtualAllocImports	このファイルは、実行中のプロセスでメモリを作成するために使用される関数をインポートします。マルウェアは、実行中のプロセスに自身を注入するためにこれを行います。

シェルコード

これらのインジケータは、ソフトウェア脆弱性のエクスプロイトで小さなコードがペイロードとして使用されていることを示します。通常は、侵害されたマシンを攻撃者が制御する元となる可能性があるコマンドシェルを起動するため、シェルコードと呼ばれていますが、同様のタスクを実行するコードはすべてシェルコードと呼ばれる可能性があります。

インジケータ	説明
ApiHashing	ファイルが、メモリにロードされているライブラリ API を密かに見つけようとするシェルコードのように見えるバイトシーケンスを含んでいます。
BlackholeV2	ファイルが、Blackhole exploit kit からのものであるように見えます。
ComplexGotoEmbed	ファイルが、ブラウザーに特定のアドレスへの移動やアクションの実行を強制できる可能性があります。

インジケータ	説明
ComplexSuspiciousHeader	PDF ヘッダーがゼロ以外のオフセットに配置されています。これは、このファイルが PDF ドキュメントとして認識されないようにしようとする試みを示している可能性があります。
EmbeddedTiff	ファイルが、エクスプロイテーションを促進する nop スレッドを含む、巧みに作成された TIFF 画像を含んでいる可能性があります。
EmbeddedXDP	ファイルが、XML データパッケージ（XDP）として別の PDF を含んでいる可能性があります。
FindKernel32Base1	ファイルが、メモリ内の kernel32.dll を見つけようとするシェルコードのように見えるバイトシーケンスを含んでいます。
FindKernel32Base2	ファイルが、メモリ内の kernel32.dll を見つけようとするシェルコードのように見えるバイトシーケンスを含んでいます。
FindKernel32Base3	ファイルが、メモリ内の kernel32.dll を見つけようとするシェルコードのように見えるバイトシーケンスを含んでいます。
FunctionPrologSig	ファイルが、典型的な関数プロローグ（シェルコードを含んでいる可能性が高い）であるバイトシーケンスを含んでいます。
GetEIP1	ファイルが、メモリ内の他のものを見つけてエクスプロイテーションを促進するために自身のアドレスを解決するシェルコードのように見える、バイトシーケンスを含んでいます。
GetEIP4	ファイルが、メモリ内の他のものを見つけてエクスプロイテーションを促進するために自身のアドレスを解決するシェルコードのように見える、バイトシーケンスを含んでいます。
IndirectFnCall1	ファイルが、間接的な関数呼び出し（シェルコードの可能性が高い）のように見えるバイトシーケンスを含んでいます。
IndirectFnCall2	ファイルが、間接的な関数呼び出し（シェルコードの可能性が高い）のように見えるバイトシーケンスを含んでいます。
IndirectFnCall3	ファイルが、間接的な関数呼び出し（シェルコードの可能性が高い）のように見えるバイトシーケンスを含んでいます。
SehSig	ファイルが、構造化例外処理（SEH）に典型的なバイトシーケンスを含んでおり、シェルコードを含んでいる可能性が高いです。
StringLaunchActionBrowser	ファイルが、ブラウザーに特定のアドレスへの移動やアクションの実行を強制できる可能性があります。
StringLaunchActionShell	ファイルが、シェルアクションを実行できる可能性があります。

インジケータ	説明
StringSingExploit	ファイルが、エクスプロイトを含んでいる可能性があります。

その他のインジケータ

このセクションでは、他のカテゴリに適合しないインジケータについて説明します。

インジケータ	説明
AutoitFileOperations	AutoIT スクリプトが、ファイルに対して複数のアクションを実行できます。これは、情報収集、永続姓、または破壊に使用される場合があります。
AutorunString	自動実行メカニズムを使用して永続性を実現する機能がファイルにあります。
CodepageLookupImports	このファイルは、実行中のシステムのコードページ（場所）を検索するために使用される関数をインポートします。マルウェアはこれを使用して、特定のグループをより適切にターゲット設定するために、システムが実行されている国/地域を識別します。
MutexImports	このファイルは、ミューテックスオブジェクトを作成および操作する関数をインポートします。マルウェアは頻繁にミューテックスを使用して、システムへの複数回の感染を回避します。
OpenSSL 静的	このファイルは、検出されないようにコンパイルされた OpenSSL のバージョンを含んでいます。マルウェアは、強力な証拠を残さずに暗号化保存機能を含めるためにこれを行います。
PListString	オペレーティングシステムによって使用されるプロパティリストとやり取りする機能がファイルにあります。これは、永続性を実現したり、さまざまなプロセスを妨害したりするために使用される場合があります。
PrivEscalationCryptBase	このファイルは、CryptBaseを使用して権限の昇格を使用しようとした証拠を示しています。マルウェアはこれを使用して、影響を受けるシステムでの権限を強くします。
ShellCommandString	偵察、特権の昇格、またはデータ破壊に機密性の高いシェルコマンドを使用する機能がファイルにあります。
SystemCallSuspicious	システムおよび他のプロセスを監視および/または制御し、デバッグのようなアクションを実行する機能がファイルにあります。

CylancePROTECT Desktop スクリプトコントロールアラートの管理

管理コンソールでは、CylancePROTECT Desktop エージェントが検出したスクリプトコントロールアラートを表示して管理できます。安全でないと考えられるスクリプトが、管理コンソールに表示されます。

1. 管理コンソールのメニューバーで、［保護］ > ［スクリプト制御］をクリックします。次の操作のいずれかを実行します。
   - 列を追加または削除するには、  をクリックし、表示する列を選択します。
   - スクリプトコントロールアラートを、ある列で昇順または降順に並べ替えるには、その列をクリックします。
   - スクリプトコントロールアラートを、ある列でフィルタリングするには、フィルターフィールドとアイコンをその列に対して使用します。
2. 次の操作のいずれかを実行します。

タスク	手順
スクリプトコントロールアラートの詳細を表示します。	**a.** スクリプトコントロールアラートの行をクリックします（チェックボックスではありません）。 **b.** スクリプトコントロールアラートによって影響を受けるデバイスを表示します。影響を受けるデバイスのリストが、スクリプトコントロールアラートのリストの下に表示されます。
スクリプトをグローバルセーフリストに追加します。	スクリプトをグローバルセーフリストに追加します。 **a.** グローバルリストに追加するスクリプトのチェックボックスをクリックします。 **b.** ［安全］をクリックします。
［デバイスの詳細］ページを表示します。	**a.** デバイス名をクリックして、［デバイスの詳細］ページを表示します。

終了したら： スクリプト制御情報を .csv ファイルにエクスポートするには、  をクリックします。エクスポートの範囲を選択し、［エクスポート］をクリックします。

CylancePROTECT Desktop 外部デバイスアラートの管理

管理コンソールを使用して、CylancePROTECT Desktop エージェントによって検出された外部デバイスアラートを表示および管理できます。外部デバイスの例としては、スマートフォン、フラッシュドライブ、外付けハードドライブ、デジタルカメラなどがあります。外部デバイス設定は、デバイス制御とも呼ばれます。

作業を始める前に： 外部デバイスを除外する前に、次の点を考慮してください。

- シリアル番号にアンダースコアを含む除外の追加は、外部デバイスアラートページではサポートされていません。デバイスポリシーに除外を追加する必要があります。

- 外部デバイスアラートページから除外を追加すると、デバイスに現在割り当てられているポリシーに影響します。これは、アラートが発生したときに使用されたポリシーではない場合があります。

1. 管理コンソールのメニューバーで、［保護］ > ［外部デバイス］をクリックします。次の操作のいずれかを実行します。
   - 列を追加または削除するには、  をクリックし、表示する列を選択します。
   - 外部デバイスアラート情報を 1 つまたは複数の列でグループ化するには、列名の上のスペースにそれらの列をドラッグします。
   - 列で外部デバイスアラートを昇順または降順に並べ替えるには、列をクリックします。
   - 列で外部デバイスアラートをフィルタリングするには、列のフィルターフィールドとアイコンを使用します。
2. 次の操作のいずれかを実行します。

タスク	手順
外部デバイスをデバイスポリシー除外リストに追加します。	外部デバイス除外は、デバイスポリシーで設定されます。外部デバイスアラートページから除外を追加すると、アラートが検出されたデバイスに割り当てられたデバイスポリシーに除外が追加されます。 **a.** デバイスポリシー除外を追加する外部デバイスアラートの ⊕ をクリックします。 **b.** 必要に応じて、外部デバイスの製品 ID とシリアル番号を変更できます。ベンダー ID は変更できません。 **c.** 必要に応じて、コメントを追加できます。除外またはその他の関連情報の理由を入力できます。 **d.** 次のアクセスタイプのいずれかを選択します。 • フルアクセス：外部デバイスがエンドポイントに接続できるようにし、外部デバイスへのフルアクセス（読み書きアクセス）を提供します。 • 読み取り専用：外部デバイスがエンドポイントに接続できるようにしますが、外部デバイスへの読み取り専用アクセスを提供します。 • ブロック：外部デバイスがエンドポイントに接続できないようにします。 **e.** ［除外を保存］をクリックします。
［デバイスの詳細］ページを表示します。	**a.** デバイス名をクリックして、［デバイスの詳細］ページを表示します。

終了したら： 外部デバイス情報を .csv ファイルにエクスポートするには、  をクリックします。エクスポートの範囲を選択し、［エクスポート］をクリックします。

脅威からの保護

CylancePROTECT Desktop は、ファイルを単に危険または異常として分類するだけでなく、ファイルの静的特性および動的特性の詳細も提供します。これにより、脅威をブロックするだけでなく、脅威となる行動を把握して、さらに脅威を軽減したり対応したりすることができます。

Cylance スコア

Cylance スコアは、このファイルがユーザーの環境に危険をもたらす確実性を表します。スコアが高いほど、このファイルが悪意のある目的に使用される確実性が高くなります。スコアに基づいて、脅威は危険または異常と見なされます。

潜在的な脅威として識別されたファイルのスコアは赤（危険または異常）で表示されます。安全として識別されたファイルのスコアは、緑色で表示されます。通常の状況では、コンソールに安全な（緑色の）ファイルは表示されません。コンソールに安全なファイルが表示されるのは、通常、ファイルがグローバル隔離リストに追加され、デバイス上で隔離されたときです。

危険/異常と見なされたファイル（赤いスコア）は、グローバルセーフリストに追加すると安全と見なされ、コンソールに表示されなくなります。

表示されたスコアがスコアの範囲と一致しない場合でも、ファイルが危険または異常として分類されることがあります。これは、最初の検出後に実行された可能性のある、更新された所見または追加のファイル分析が原因である場合があります。最新の脅威分析を行うには、ポリシーで自動アップロードを有効にします。

Cylance スコアは脅威の分類とは無関係です。ほとんどの脅威分類は、人間の脅威研究者が実施し、ファイルごとに割り当てられる手動プロセスです。ファイルに Cylance スコアを設定することはできますが、しばらく後まで分類を設定することはできません。

危険なファイルと異常なファイル

BlackBerry は、脅威の Cylance スコアを使用して CylancePROTECT Desktop の脅威アラートをグループ化します。これにより、デバイスポリシーを使用して、危険な脅威や異常な脅威をグローバル隔離リストに自動的に追加するなどのアクションを簡素化できます。

- 危険：60～100 の範囲のスコアを持つファイル。危険なファイルとは、マルウェアに非常に類似した属性を持つファイルです。
- 異常：1～59 の範囲のスコアを持つファイル。異常なファイルにはマルウェア属性がいくつかありますが、危険なファイルよりは少ないため、マルウェアである可能性は低くなります。

表示されるスコアが分類の範囲と一致しない場合でも、ファイルが危険または異常と分類されることがあります。最初の検出後に更新された所見や追加のファイル分析が影響してそのようになる場合があります。最新の分析を行うため、デバイスポリシーで自動アップロードを有効にしてください。

ファイルの分類

次の表に、CylancePROTECT Desktop の脅威ごとに表示される可能性があるファイルステータスエントリを示します。

ファイルステータス	説明
使用できないファイル	アップロードの制約（ファイルが大きすぎるなど）により、ファイルを分析できません。ファイルを転送する別の方法について、BlackBerry サポートにお問い合わせください。
空白のエントリ	ファイルがまだ分析されていません。分析が完了すると、新しいステータスが割り当てられます。
信頼済み - ローカル	ファイルは安全と見なされます。ファイルをグローバルセーフリストに追加して、実行を許可し、他のデバイスで識別されたときにアラートが生成されないようにすることができます。
PUP	ファイルは不審なプログラム（PUP）であり、ユーザーがダウンロードに同意した場合でも安全でない可能性があることを示します。一部の PUP は、組織内の限られたシステムセット（たとえば、ドメイン管理者のデバイスで実行できる VNC アプリケーション）上での実行が許可されます。PUP をデバイスごとに放棄またはブロックするか、組織の標準に基づいてグローバル隔離リストまたはセーフリストに追加するかを選択できます。ファイルには、次のサブクラスを指定することができます。 • アドウェア • 破損 • ゲーム • 汎用 • ハッキングツール • ポータブルアプリケーション（インストールは不要） • スクリプトツール • ツールバー
デュアルユース	ファイルが、悪意のある目的でも悪意のない目的でも使用される可能性があります。たとえば、PsExec は別のシステムでプロセスを実行するのに便利なツールですが、その同じ機能を使用して別のシステムで悪意のあるファイルを実行できます。ファイルには、次のサブクラスを指定することができます。 • クラック（ライセンス制限を回避するために別のアプリケーションを変更する） • 汎用 • KeyGen（プロダクトキーの生成、表示、または回復） • 監視ツール • パスクラック • リモートアクセス • ツール（攻撃を促進する管理プログラム）

ファイルステータス	説明
マルウェア	このファイルは、ネットワークへのアクセスを中断または損傷させるか、不正にアクセスするように設計された悪意のあるソフトウェアとして識別されており、できるだけ早く削除する必要があります。ファイルには、次のサブクラスを指定することができます。 • バックドア • ボット • ダウンローダ • ドロッパ • エクスプロイト • 偽のアラート • 汎用 • InfoStealer • 寄生型 • ランサム • レムナント • ルートキット • トロイの木馬 • ウイルス • ワーム
可能性のあるマルウェア	このファイルは疑わしいソフトウェアとして識別されており、異常または危険であるとみなされます。組織の標準に基づいて、グローバル隔離リストまたはセーフリストに追加できます。

ファイルのリスクレベルの評価

管理コンソールを使用して、CylancePROTECT クラウドサービスによって分析および判定されたファイルのリスクレベルを評価できます。この機能を使用すると、CylancePROTECT Desktop エージェントがデバイス上で識別するファイルをどのように分類するかを理解できるようになります。現在、Windows、macOS、および Linux の実行可能ファイルがサポートされています。

作業を始める前に： コンソールでこの機能にアクセスするには、管理者ロールが必要です。

1. 管理コンソールのメニューバーで、［保護］ > ［脅威分析］をクリックします。
2. 次の操作のいずれかを実行します。

アクション	手順
ハッシュでファイルを検索します。	［ハッシュ］フィールドに SHA256 ハッシュを入力するか貼り付けます。ハッシュごとに行を変えて分けてください。最大 32 個のハッシュを追加できます。

アクション	手順
ファイルをアップロードします。	アップロードできるファイルの最大サイズは 10MB です。 **a.** ［ファイルをアップロード］タブで［ファイルを参照］をクリックします。 **b.** 移動して、分析するファイルを選択します。［開く］をクリックします。

3. ［分析］をクリックします。
4. ファイルステータスを確認して、脅威が検出されたかどうか、またはファイルが安全と見なされているかどうかを判断します。

   SHA256 ハッシュでファイルを検索した後に［ファイルが必要］ステータスが表示された場合は、［ファイルをアップロード］タブでファイルをアップロードします。

終了したら： 必要に応じて、グローバル隔離リストまたはグローバルセーフリストにファイルを追加します。手順については、「CylancePROTECT Desktop グローバル隔離リストまたはグローバルセーフリストへのファイルの追加」を参照してください。

CylancePROTECT Desktop レポートの使用

メニューバーで、［レポート］をクリックすることで、次に挙げる CylancePROTECT Desktop レポートを表示できます。レポートは対話形式で、データの一部を選択して詳細を表示できます。

レポート	説明
CylancePROTECT の概要	このレポートには、CylancePROTECT Desktop の使用状況（ゾーンとデバイスの数、自動隔離とメモリ保護の対象となるデバイスの割合、脅威イベントの概要、CylancePROTECT Desktop デバイスのメモリ違反、エージェントバージョン、オフライン数など）のエグゼクティブサマリーが示されます。
脅威イベントの概要	このレポートには、マルウェアや不審なプログラム（PUP）として識別されたファイルの数が示され、具体的なサブカテゴリによる内訳が含まれます。脅威にさらされているファイル所有者とデバイスの上位 10 リストには、マルウェア、PUP、およびデュアルユースの脅威の部類のイベントカウントが示されます。
デバイスの概要	このレポートには、CylancePROTECT Desktop デバイスに関する概要データが表示されます。
脅威イベント	このレポートには、CylancePROTECT Desktop エージェントによって識別された脅威イベントの詳細データが示されます。
デバイス	このレポートには、OS ごとの CylancePROTECT Desktop デバイス数が表示されます。

レポートには、イベントベースの方法で脅威が表示されます。1 つのイベントは、1 つの脅威の単独の事例を表します。たとえば、特定のファイルがデバイス上の 3 つの異なるフォルダにある場合、脅威イベントカウントは 3 になります。レポートデータは、約 3 分ごとに更新されます。CylancePROTECT の概要レポート、脅威イベントの概要レポート、デバイスの概要レポートは .png ファイルとして、脅威イベントとデバイスレポートは .csv ファイルとしてエクスポートできます。

サードパーティ製アプリケーションを使用して脅威データレポートを取得する

詳細な脅威データレポートには、［設定］>［アプリケーション］の［脅威データレポート］セクションにリストされている URL でアクセスできます。またレポートのダウンロードも可能です。URL は、管理コンソールによって生成された一意のトークンを使用しており、［設定］>［アプリケーション］で表示されます。必要に応じて、トークンを削除して再生成できます。トークンを再生成すると、以前のトークンは無効になります。サードパーティ製アプリケーションを使用してこれらの URL からレポートを取得する場合、アプリケーションとホスト OS は、次のものを使用する必要があります。

- TLS 1.2
- TLSv1.2_2021 ポリシーでサポートされている暗号

CylancePROTECT Mobile によって検出された脅威の管理

管理コンソールを使用して、CylancePROTECT Mobile アプリがユーザーのデバイスで検出したモバイル脅威の一覧を表示できます。アラートは最大 120 日間保存されます。ユーザーの CylancePROTECT Mobile サービスを無効にすると、そのユーザーに関連付けられているすべてのアラートが管理コンソールから削除されます。

CylancePROTECT Mobile アラートの表示

1. 管理コンソールのメニューバーで、［保護］ > ［**Protect Mobile** のアラート］をクリックします。
   この画面に表示される CylancePROTECT Mobile アラートの詳細については、「CylancePROTECT Mobile アプリで検出されたモバイルの脅威」を参照してください。
2. オプションで、次のいずれかを実行します。
   - アラートに関して利用可能な詳細（検出時刻や初回インストール時刻など）を表示するには、アラートをクリックします。
   - アラートをグループ化するには、［グループ化］ドロップダウンリストをクリックしてオプションをクリックします。
   - アラートを列の昇順または降順に並べ替えるには、列の名前をクリックします。
   - アラートをフィルタリングするには、列の をクリックして、フィルター基準を入力または選択します。
   - 1 つまたは複数のアラートを無視するには、アラートを選択して［無視］をクリックします。［無視］を再度クリックして確定します。
   - 結果を .csv ファイルにエクスポートするには、 をクリックします。［エクスポート］をクリックします。

次の情報を使用して、アプリまたは証明書を CylancePROTECT Mobile のセーフリストまたは制限対象リストに追加できます。

- iOS のサイドロードアプリの脅威の場合には、［名前］列に開発者証明書の共通名が表示されます。
- Android の悪意のあるアプリやサイドロードされたアプリの脅威については、［説明］列にアプリの SHA256 ハッシュが表示されます。

CylancePROTECT Mobile アプリで検出されたモバイルの脅威

次の表に、［保護］ > ［Protect Mobile のアラート］の管理コンソールで報告できるアラートを示します。

モバイルセキュリティの脅威	UI アラートタイプ	UI アラート名	UI 説明
アプリのセキュリティ：悪意のあるアプリ	悪意のあるアプリ	アプリ名	パッケージ名、パッケージバージョン、SHA256 ハッシュ

モバイルセキュリティの脅威	UI アラートタイプ	UI アラート名	UI 説明
アプリのセキュリティ：サイドロードされたアプリ	サイドロードされたアプリ	Android：アプリ名 iOS：署名 ID	Android：パッケージ名、パッケージバージョン、インストーラソース、SHA256 ハッシュ
アプリのセキュリティ：制限対象アプリ	制限対象アプリ	Android：アプリ名 iOS：署名 ID	Android：パッケージ名、パッケージバージョン、インストーラソース、SHA256 ハッシュ
ネットワーク保護：Wi-Fi セキュリティ	安全でない Wi-Fi	ネットワークSSID ユーザーが無効にした場合：ユーザーが無効にした機能	Wi-Fi アクセスアルゴリズム
ネットワーク保護：ネットワーク接続	侵害されたネットワーク	ネットワークタイプ	ネットワークSSID
デバイスセキュリティ：サポート対象外のデバイスモデル	サポート対象外のデバイスモデル	モデル名	NA
デバイスセキュリティ：サポート対象外の OS	サポート対象外のOS	OS 名、OS バージョン	NA
デバイスセキュリティ：サポート対象外のセキュリティパッチ	サポート対象外のセキュリティパッチ	パッチバージョン： 証明書の検証に失敗した場合：信頼できません	NA
デバイスセキュリティ：ルート/ジェイルブレイクの検出	侵害されたデバイス	Android：ルートされています iOS：ジェイルブレイクされています	OS 名、OS バージョン
デバイスセキュリティ：フルディスク暗号化	暗号化が無効です	暗号化が無効です	OS 名、OS バージョン
デバイスセキュリティ：画面ロック	画面ロックが無効です	画面ロックが無効です	OS 名、OS バージョン
デバイスセキュリティ：開発者オプション	開発者モード	開発者モードが有効になりました	OS 名、OS バージョン

モバイルセキュリティの脅威	UI アラートタイプ	UI アラート名	UI 説明
デバイスセキュリティ：Android SafetyNet または Play Integrity 認証	SafetyNet または Play Integrity 認証失敗	Android SafetyNet Android Play Integrity	認証タイプ、認証の状態
デバイスセキュリティ：Android ハードウェア証明書認証	ハードウェア認証の失敗	Android ハードウェア	ハードウェアキー認証：認証タイプ、認証の状態、ルールの失敗 その他の検出：認証タイプ、認証の状態
デバイスセキュリティ：Samsung Knox Enhanced Attestation	Knox Enhanced Attestation の失敗	Knox Enhanced Attestation	Knox、デバイス障害
デバイスセキュリティ：iOS 整合性チェック	アプリの整合性認証の失敗	iOS アプリの整合性チェック	認証タイプ、認証の状態
メッセージスキャン（Android に対してのみ表示）	安全ではないメッセージ	悪意のある SMS	悪意のある URL のリスト

CylancePROTECT Desktop および CylancePROTECT Mobile のセーフリストと危険リストの管理

このセクションでは、 CylancePROTECT Desktop の隔離リストまたはセーフリストにファイルと証明書を追加する方法、およびアプリ、開発者証明書、IP アドレス、ドメインを CylancePROTECT Mobile のセーフリストまたは制限リストに追加する方法について説明します。

CylancePROTECT Desktop グローバル隔離リストまたはグローバルセーフリストへのファイルの追加

ファイルをグローバル隔離リストに追加して、すべての CylancePROTECT Desktop デバイスからブロックすることができます。グローバルセーフリストにファイルを追加して、すべての CylancePROTECT Desktop デバイスでファイルを許可します。未割り当てのリストは、管理コンソールにリストされているファイルで、グローバル隔離されていない、またはセーフリストに記載されていないファイルです。

デバイスのローカル隔離リストまたはローカルセーフリストにファイルを追加するには、「CylancePROTECT Desktop のローカル隔離リストやローカルセーフリストへのファイルの追加」を参照してください。

次の操作のいずれかを実行します。

タスク	手順
脅威ページからグローバル隔離リストまたはセーフリストにファイルを追加します。	**a.** 管理コンソールのメニューバーで、［保護］ > ［脅威］をクリックします。 **b.** ファイルを選択します。 **c.** 次の操作のいずれかを実行します。 • ファイルをグローバル隔離リストに追加するには、［グローバル隔離］をクリックします。 • ファイルをグローバルセーフリストに追加するには、［セーフ］をクリックします。 **d.** 必要な情報を指定します。 **e.** ［はい］をクリックします。
グローバル隔離またはセーフリストにファイルを手動で追加します。	**a.** 管理コンソールのメニューバーで、［設定］ > ［グローバルリスト］をクリックします。 **b.** ［グローバル隔離］または［セーフ］タブをクリックします。 **c.** ［ファイルを追加］をクリックします。 **d.** ファイル情報を指定します。 **e.** ［送信］をクリックします。

タスク	手順
未割り当てリストから、グローバル隔離リストまたはセーフリストにファイルを追加します。	**a.** 管理コンソールのメニューバーで、［設定］ > ［グローバルリスト］をクリックします。 **b.** ［未割り当て］タブで、ファイルを選択します。 **c.** 次の操作のいずれかを実行します。 • ファイルをグローバル隔離リストに追加するには、［グローバル隔離］をクリックします。 • ファイルをグローバルセーフリストに追加するには、［セーフ］をクリックします。 **d.** ファイルをグローバルリストに追加する理由を指定します。 **e.** ［はい］をクリックします。
ファイルをあるグローバルリストから別のグローバルリストに移動します。	**a.** 管理コンソールのメニューバーで、［設定］ > ［グローバルリスト］をクリックします。 **b.** ［グローバル隔離］または［セーフ］タブをクリックします。 **c.** 移動するファイルを選択します。 **d.** 次の操作のいずれかを実行します。 • ファイルをグローバル隔離リストに移動するには、［グローバル隔離］をクリックします。 • ファイルをグローバルセーフリストに移動するには、［セーフ］をクリックします。 • ファイルを未割り当てリストに移動するには、［リストから削除］をクリックします。 **e.** 必要な情報を指定します。 **f.** ［はい］をクリックします。

CylancePROTECT Desktop のローカル隔離リストやローカルセーフリストへのファイルの追加

ファイルをローカル隔離リストに追加すると、デバイスから特定のファイルをブロックできます。ファイルはデバイス用のローカル放棄リスト（ローカルセーフ）に追加することもできます。これらのアクションはそのデバイスにのみ影響し、組織内の他のデバイスには影響しません。

CylancePROTECT Desktop のグローバル隔離リストやグローバルセーフリストにファイルを追加するには、「CylancePROTECT Desktop グローバル隔離リストまたはグローバルセーフリストへのファイルの追加」を参照してください。

1. 管理コンソールのメニューバーで、［アセット］ > ［デバイス］をクリックします。
2. 1 つのデバイスをクリックします。
3. ［脅威］で、対象のファイルを選択します。
4. ［隔離］をクリックして、ローカル隔離リストにファイルを追加します。［放棄］をクリックして、ファイルをローカル放棄リスト（ローカルセーフ）に追加します。
5. 必要な情報を入力します。

6. ［はい］をクリックします。

証明書の CylancePROTECT Desktop グローバルセーフリストへの追加

適切に署名されたカスタムソフトウェアの場合、証明書は証明書リストに追加して、ソフトウェアを中断せずに実行できるようにします。そうすることで管理者は、証明書の SHA1 サムプリントで表される署名付きの証明書でセーフリストを作成できます。証明書情報を管理コンソールに追加するとき、証明書自体は管理コンソールにアップロードも保存もされません。証明書情報は、抽出されて管理コンソールに保存されます（タイムスタンプ、件名、発行者、サムプリント）。証明書のタイムスタンプは、証明書が作成された日時を表します。管理コンソールでは、証明書が有効期限内か期限切れかはチェックされません。証明書が変更（更新や新規作成など）された場合は、管理コンソールのセーフリストに追加する必要があります。証明書によるセーフリスト機能は、PowerShell、ActiveScript、Office マクロで動作します。

現在この機能は、Windows と macOS でのみ機能します。

作業を始める前に： 署名付きポータブル実行可能ファイル（PE）の証明書サムプリントを確認します。

1. 管理コンソールのメニューバーで、［設定］ > ［証明書］をクリックします。
2. ［証明書を追加］をクリックします。
3. ［追加する証明書を参照］をクリックするか、証明書をメッセージボックスにドラッグアンドドロップします。証明書を参照する場合は、［開く］ウィンドウが表示され、証明書を選択できます。
4. 必要に応じて、証明書の［適用先］ファイルタイプ（［実行可能ファイル］または［スクリプト］）を選択できます。これにより、フォルダの場所ではなく証明書で実行可能ファイルやスクリプトを追加できます。
5. 必要に応じて、証明書についてのメモを追加します。
6. ［送信］をクリックします。発行者、件名、サムプリント、メモ（入力した場合）がリポジトリに追加されます。

終了したら： 証明書の有効期限が切れているか、証明書が失効している場合は、証明書を削除して、新しく発行された証明書を追加する必要があります。証明書を削除するには、証明書を選択して［リストから削除］をクリックしてから、［はい］をクリックして確認します。有効な証明書を再度追加するには、上記の手順を実行してください。

アプリ、証明書、IP アドレス、ドメイン、インストーラソースの CylancePROTECT Mobile セーフリストまたは制限対象リストへの追加

CylancePROTECT Mobile のセーフリストおよび制限対象リストを使用して、次のものを管理できます。

- 特定のアプリまたは開発者署名証明書をマルウェアとサイドロード検出から除外します。
- 特定のアプリまたは開発者署名証明書をマルウェアとサイドロード検出の脅威として分類します。
- IP アドレスまたはドメインをメッセージスキャンから除外します。
- 特定の IP アドレスまたはドメインをメッセージスキャンの脅威として分類します。
- 特定のインストーラソースをサイドロード検出から除外します。
- 特定のインストーラソースをサイドロード検出の脅威として分類します。

作業を始める前に：

- ［保護］ > ［**Protect Mobile** のアラート］でアラートをクリックすると、アプリハッシュ、証明書の詳細、パッケージの詳細などの詳細を表示できます。以下の手順に従って、セーフリストまたは制限対象リストに項目を追加するときに、この情報が必要になる場合があります。
- Android 開発者証明書をセーフリストや制限対象リストに追加する場合は、アプリバイナリから証明書のサムプリントを取得する必要があります。手順については、「KB 70577」を参照してください。

1. 管理コンソールのメニューバーで、［設定］ > ［グローバルリスト（モバイル）］をクリックします。
2. 次の操作のいずれかを実行します。

タスク	手順
開発者証明書をマルウェアおよびサイドロード検出セーフリストに追加します。	**a.** ［セーフ］タブで、［開発者］をクリックします。 **b.** ［証明書を追加］をクリックします。 **c.** 次の操作のいずれかを実行します。 • アプリファイルから署名証明書を追加するには、［アプリを選択して証明書情報を取得する］をクリックします。.apk または .ipa ファイルを参照して選択し、［送信］をクリックします。 • 証明書情報を手動で入力するには、［証明書情報を手動で入力する］をクリックします。証明書の詳細を指定し、［追加］をクリックします。 • .csv ファイルから証明書のリストをインポートするには、［**.csv** ファイルから証明書リストをインポートする］をクリックします。ファイルを参照して選択し、［アップロード］をクリックします。 証明書の有効期限が切れているか、証明書が失効している場合は、証明書を手動で削除して再追加する必要があります。証明書を削除するには、証明書を選択して［削除］をクリックしてから、［はい］をクリックして確認します。有効な証明書を再度追加するには、上記の手順を繰り返してください。

タスク	手順
開発者証明書をマルウェアおよびサイドロード検出制限リストに追加します。 （Android 専用）	**a.** ［制限対象］タブで、［開発者］をクリックします。 **b.** ［証明書を追加］をクリックします。 **c.** 次の操作のいずれかを実行します。 • アプリファイルから署名証明書を追加するには、［アプリを選択して証明書情報を取得する］をクリックします。.apk ファイルを参照して選択し、［送信］をクリックします。 • 証明書情報を手動で入力するには、［証明書情報を手動で入力する］をクリックします。証明書の詳細を指定し、［追加］をクリックします。 • .csv ファイルから証明書のリストをインポートするには、［**.csv** ファイルから証明書リストをインポートする］をクリックします。ファイルを参照して選択し、［アップロード］をクリックします。 証明書の有効期限が切れているか、証明書が失効している場合は、証明書を手動で削除して再追加する必要があります。証明書を削除するには、証明書を選択して［削除］をクリックしてから、［はい］をクリックして確認します。有効な証明書を再度追加するには、上記の手順を繰り返してください。
アプリをマルウェアおよびサイドロード検出セーフリストに追加します。	**a.** ［セーフ］タブで、［アプリ］をクリックします。 **b.** ［アプリを追加］をクリックします。 **c.** 次の操作のいずれかを実行します。 • アプリファイルを追加するには、［アプリファイルを選択］をクリックします。.apk または .ipa ファイルを参照して選択し、［送信］をクリックします。 • アプリのハッシュを手動で入力するには、［アプリのハッシュ情報を手動で入力する］をクリックします。アプリの詳細を指定し、［追加］をクリックします。 • .csv ファイルからアプリのリストをインポートするには、［**.csv** ファイルからアプリリストをインポートする］をクリックします。ファイルを参照して選択し、［アップロード］をクリックします。 メモ：アプリに複数の .apk ファイルが含まれている場合は、各ファイルのハッシュを手動で入力する必要があります。必要に応じて、アプリの署名証明書を代わりに追加できます。

タスク	手順
マルウェア検出制限対象リストにアプリを追加します。 （Android 専用）	**a.** ［制限対象］タブで、［アプリ］をクリックします。 **b.** ［アプリを追加］をクリックします。 **c.** 次の操作のいずれかを実行します。 • アプリファイルを追加するには、［アプリファイルを選択］をクリックします。.apk ファイルを参照して選択し、［送信］をクリックします。 • アプリのハッシュを手動で入力するには、［アプリのハッシュ情報を手動で入力する］をクリックします。アプリの詳細を指定し、［追加］をクリックします。 • .csv ファイルからアプリのリストをインポートするには、［**.csv** ファイルからアプリリストをインポートする］をクリックします。ファイルを参照して選択し、［アップロード］をクリックします。 メモ：アプリに複数の .apk ファイルが含まれている場合は、各ファイルのハッシュを手動で入力する必要があります。必要に応じて、アプリの署名証明書を代わりに追加できます。
IP アドレスをメッセージスキャンセーフリストに追加します。 （Android 専用）	**a.** ［セーフ］タブで、［**IP** アドレス］をクリックします。 **b.** ［**IP** アドレスを追加］をクリックします。 **c.** 次の操作のいずれかを実行します。 • IP アドレスを手動で入力するには、［**IP** アドレス情報を手動で入力する］をクリックします。IP の詳細を指定し、［追加］をクリックします。 • .csv ファイルから IP アドレスのリストをインポートするには、［**.csv** ファイルから **IP** アドレスリストをインポートする］をクリックします。ファイルを参照して選択し、［アップロード］をクリックします。
IP アドレスをメッセージスキャン制限対象リストに追加します。 （Android 専用）	**a.** ［制限対象］タブで、［**IP** アドレス］をクリックします。 **b.** ［**IP** アドレスを追加］をクリックします。 **c.** 次の操作のいずれかを実行します。 • IP アドレスを手動で入力するには、［**IP** アドレス情報を手動で入力する］をクリックします。IP の詳細を指定し、［追加］をクリックします。 • .csv ファイルから IP アドレスのリストをインポートするには、［**.csv** ファイルから **IP** アドレスリストをインポートする］をクリックします。ファイルを参照して選択し、［アップロード］をクリックします。

タスク	手順
ドメインをメッセージスキャンセーフリストに追加します。 （Android 専用）	**a.** ［セーフ］タブで、［ドメイン］をクリックします。 **b.** ［ドメインを追加］をクリックします。 **c.** 次の操作のいずれかを実行します。 • ドメイン情報を手動で入力するには、［ドメイン情報を手動で入力する］をクリックします。ドメインの詳細を指定し、［追加］をクリックします。 • .csv ファイルからドメインのリストをインポートするには、［**.csv** ファイルからドメインリストをインポートする］をクリックします。ファイルを参照して選択し、［アップロード］をクリックします。
メッセージスキャン制限対象リストにドメインを追加します。 （Android 専用）	**a.** ［制限対象］タブで、［ドメイン］をクリックします。 **b.** ［ドメインを追加］をクリックします。 **c.** 次の操作のいずれかを実行します。 • ドメイン情報を手動で入力するには、［ドメイン情報を手動で入力する］をクリックします。ドメインの詳細を指定し、［追加］をクリックします。 • .csv ファイルからドメインのリストをインポートするには、［**.csv** ファイルからドメインリストをインポートする］をクリックします。ファイルを参照して選択し、［アップロード］をクリックします。
サイドロード検出セーフリストにインストーラソースを追加します。	**a.** ［セーフ］タブで［インストーラソース］をクリックします。 **b.** ［インストーラソースを追加］をクリックします。 **c.** 次の操作のいずれかを実行します。 • インストールソース情報を手動で入力するには、［インストールソース情報を手動で入力する］をクリックします。詳細を指定し、［追加］をクリックします。 • .csv ファイルからインストーラソースのリストをインポートするには、［**.csv** ファイルからインストールソースリストをインポートする］をクリックします。ファイルを参照して選択し、［アップロード］をクリックします。
サイドロード検出制限対象リストにインストーラソースを追加します。	**a.** ［制限対象］タブで、［インストーラソース］をクリックします。 **b.** ［インストーラソースを追加］をクリックします。 **c.** 次の操作のいずれかを実行します。 • インストールソース情報を手動で入力するには、［インストールソース情報を手動で入力する］をクリックします。詳細を指定し、［追加］をクリックします。 • .csv ファイルからインストーラソースのリストをインポートするには、［**.csv** ファイルからインストールソースリストをインポートする］をクリックします。ファイルを参照して選択し、［アップロード］をクリックします。

終了したら：

- セーフリストや制限対象リストから項目を削除するには、その項目を選択して［削除］をクリックします。メッセージが表示されたら、再度［削除］をクリックします。
- セーフリストや制限対象リストをエクスポートするには、 をクリックします。［エクスポート］をクリックして確認します。

CylanceOPTICS が収集したデータの分析

このセクションでは、 CylanceOPTICS によって収集されたデータを表示、分析、および使用する方法について説明します。

CylanceOPTICS センサ

デバイスポリシーで CylanceOPTICS をオンにすると、CylanceOPTICS エージェントで次のセンサがデフォルトで有効になります。これらのセンサを無効にすることはできません。有効にできるオプションのセンサの詳細については、「CylanceOPTICS のオプションのセンサ」を参照してください。

デフォルトのセンサとオプションのセンサの両方に関連付けられているイベント、アーチファクト、およびイベントタイプの詳細については、「脅威を識別するために CylanceOPTICS が使用するデータ構造」を参照してください。

センサ	プラットフォーム	説明	イベントタイプ
デバイス	macOS Linux	関連するデバイス情報を収集します	マウント
ファイル	Windows macOS Linux	ファイル操作に関する情報を収集します	• 作成 • 削除 • 上書き • 名前変更 • 書き込み
メモリ	macOS Linux	メモリ操作に関する情報を収集します	• Mmap • MProtect
ネットワーク	Windows macOS Linux	ネットワーク接続に関する情報を収集します	接続

センサ	プラットフォーム	説明	イベントタイプ
プロセス	Windows macOS Linux	プロセス操作に関する情報を収集します	サポートされるイベントタイプは、プラットフォームによって異なります。「脅威を識別するために CylanceOPTICS が使用するデータ構造」の「プロセス」セクションを参照してください。 • 異常終了 • 終了 • 強制終了 • PTrace • 開始 • 一時停止 • 不明なLinuxプロセスイベント
レジストリ	Windows	レジストリ操作に関する情報を収集します	• KeyCreated • KeyDeleting • ValueChanging • ValueDeleting

CylanceOPTICS のオプションのセンサ

次の CylanceOPTICS センサのいずれかを有効にすることにより、標準のプロセス、ファイル、ネットワーク、レジストリの各イベント以外の追加データを収集できます。オプションのセンサを有効にすると、デバイスのパフォーマンスとリソース使用率、および CylanceOPTICS データベースに保存されるデータ量に影響が及ぶ可能性があります。BlackBerry では、最初に少数のデバイスでオプションのセンサを有効にして影響を評価することをお勧めします。

オプションのセンサは、特に記載のない限り、64 ビットオペレーティングシステムでのみサポートされています。

センサ	説明	ベストプラクティス	注
高度なスクリプトの可視性	この CylanceOPTICS エージェントは、JScript、PowerShell（コンソールおよび統合スクリプト環境）、VBScript、および VBA マクロスクリプト実行からのコマンド、引数、スクリプト、およびコンテンツを記録します。 信号対雑音比：高 データの保持とパフォーマンスへの影響の可能性：低から中程度	推奨環境： • デスクトップ • ノートパソコン • サーバー Microsoft Exchange およびメールサーバーには推奨されません。	• Microsoft またはその他のサードパーティ製ソリューションが提供するツールの操作実行は、PowerShell に大きく依存している場合があります。 • データの保持期間を長くするため、BlackBerry では、PowerShell を頻繁に使用する信頼済みツールに対し、検出例外を設定することをお勧めします。
高度な WMI の可視性	この CylanceOPTICS エージェントは、追加の WMI 属性とパラメーターを記録します。 信号対雑音比：高 データの保持とパフォーマンスへの影響の可能性：低	推奨環境： • デスクトップ • ノートパソコン • サーバー	• 一部の Windows のバックグラウンドやメンテナンスのプロセスは、タスクのスケジューリングやコマンドの実行に WMI を使用します。その結果、WMI のアクティビティが短時間急増することがあります。 • BlackBerry は、このセンサを有効にする前に、お使いの環境での WMI 使用状況を分析することをお勧めします。
API センサ	CylanceOPTICS エージェントは、指定された一連の Windows API 呼び出しを監視します。 信号対雑音比：中程度 データ保持とパフォーマンスに影響する可能性：このセンサを有効にすると、デバイスの CPU パフォーマンスに影響を与える可能性があります	推奨環境： • デスクトップ • ノートパソコン • サーバー	• x86 または x64 Windows オペレーティングシステムでサポートされています。 • CylancePROTECT Desktop エージェントのバージョン 3.0.1003 以降が必要です。 • CylanceOPTICS エージェントのバージョン 3.2 以降が必要です。

センサ	説明	ベストプラクティス	注
COM オブジェクトの可視性	CylanceOPTICS エージェントは、COM インターフェイスと API コールを監視して、スケジュールされたタスクの作成などの悪意のある動作を検出します。 信号対雑音比：高 データ保持とパフォーマンスに影響する可能性：このセンサを有効にすると CPU パフォーマンスに影響を与える可能性があります	推奨環境： • デスクトップ • ノートパソコン サーバーには推奨されません。	• Windows のみ。 • CylancePROTECT Desktop エージェントのバージョン 3.2 以降が必要です。 • CylanceOPTICS エージェントのバージョン 3.3 以降が必要です。
クリプトジャッキング検出	この CylanceOPTICS エージェントは、Intel CPU のアクティビティをハードウェアレジスタの使用により処理し、クリプトマイニングやクリプトハッキングのアクティビティの可能性を検出します。 信号対雑音比：中程度 データの保持とパフォーマンスへの影響の可能性：低	サポート対象： • Windows 10 x64 • Intel 第 6 世代から第 10 世代	メモ：BlackBerry では、このセンサの無効化を推奨しています。現在、デバイス OS でこのセンサに起因する安定性の問題を調査しているためです。 • 仮想マシンではサポートされていません。 • Intel 第 11 世代以降のプロセッサではサポートされていません。BlackBerry では、第 11 世代以降でこのセンサを有効にすることをお勧めしません。
DNS の可視性	この CylanceOPTICS エージェントは、DNS 要求と応答、およびドメイン名、解決済みアドレス、レコードタイプなどの関連データフィールドを記録します。 信号対雑音比：中程度 データの保持とパフォーマンスへの影響の可能性：中程度	推奨環境： • デスクトップ • ノートパソコン DNS サーバーには推奨されません。	• このセンサは大量のデータを収集することもありますが、他のツールでは記録が困難なデータを可視化することもできます。 • データの保持期間を長くするため、BlackBerry では、クラウドベースのサービスを大量に利用する信頼済みツールに対し、検出例外を設定することをお勧めします。

センサ	説明	ベストプラクティス	注
強化されたファイル読み取りの可視性	CylanceOPTICS エージェントは、指定されたディレクトリセット内のファイル読み取りを監視します。 信号対雑音比：中程度 データの保持とパフォーマンスへの影響の可能性：低	推奨環境： • デスクトップ • ノートパソコン • サーバー	• サードパーティ製のセキュリティツールの中には、このセンサがデータを収集する Windows API を使用するものがあります。場合によっては、この CylanceOPTICS が、無関係なデータや既に信頼済みのデータを記録することがあります。 • データの保持期間を長くし、信号対雑音比を向上させるため、BlackBerry では、信頼できるセキュリティツールに対し、検出例外を設定することをお勧めします。
ポータブル実行可能ファイル解析強化	この CylanceOPTICS エージェントは、ファイルバージョン、インポート機能、パッカータイプなど、移植可能な実行可能ファイルに関連付けられたデータフィールドを記録します。 信号対雑音比：中程度 データの保持とパフォーマンスへの影響の可能性：低	推奨環境： • デスクトップ • ノートパソコン • サーバー	• このセンサによって収集されたデータは、拡張実行可能ファイル分析を支援するためにコンテキスト分析エンジンに渡され、CylanceOPTICS データベースには保存されません。 • このセンサを有効にしても、CylanceOPTICS のデータ保持にはほとんど影響しません。 • 文字列リソースを分析する検出ルールを追加して有効にすると、CylanceOPTICS エージェントが CPU とメモリのリソースを大量に消費する可能性があります。

センサ	説明	ベストプラクティス	注
強化されたプロセスとフッキングの可視性	この CylanceOPTICS エージェントは、Win32 API およびカーネル監査メッセージからのプロセス情報を記録して、プロセスフックと注入の形式を検出します。 信号対雑音比：中程度 データの保持とパフォーマンスへの影響の可能性：低	推奨環境： • デスクトップ • ノートパソコン • サーバー	• サードパーティ製のセキュリティツールの中には、このセンサがデータを収集する Windows API を使用するものがあります。場合によっては、この CylanceOPTICS が、無関係なデータや既に信頼済みのデータを記録することがあります。 • データの保持期間を長くし、信号対雑音比を向上させるため、BlackBerry では、信頼できるセキュリティツールに対し、検出例外を設定することをお勧めします。
HTTP の可視性	CylanceOPTICS エージェントは、Windows のイベントトレース、WinINet API、WinHTTP API などの Windows HTTP トランザクションを追跡します。 信号対雑音比：高 データ保持とパフォーマンスに影響する可能性：このセンサを有効にすると CPU パフォーマンスに影響を与える可能性があります	推奨環境： • デスクトップ • ノートパソコン サーバーには推奨されません。	• Windows のみ。 • CylancePROTECT Desktop エージェントのバージョン 3.2 以降が必要です。 • CylanceOPTICS エージェントのバージョン 3.3 以降が必要です。
モジュールロードの可視性	CylanceOPTICS エージェントはモジュールのロードを監視します。 信号対雑音比：高 データ保持とパフォーマンスに影響する可能性：このセンサを有効にすると CPU パフォーマンスに影響を与える可能性があります	推奨環境： • デスクトップ • ノートパソコン • サーバー	• Windows のみ。 • CylancePROTECT Desktop エージェントのバージョン 3.2 以降が必要です。 • CylanceOPTICS エージェントのバージョン 3.3 以降が必要です。

センサ	説明	ベストプラクティス	注
プライベートネットワークアドレスの可視性	この CylanceOPTICS エージェントは、RFC 1918 および RFC 4193 アドレス空間内でのネットワーク接続を記録します。 信号対雑音比：低 データの保持とパフォーマンスへの影響の可能性：低	デスクトップに推奨。 非推奨環境： • DNSサーバー • リソースが不足しているシステム • RDP またはその他のリモートアクセスソフトウェアを使用するシステム	• このセンサは大量のデータを収集するため、データが CylanceOPTICS データベースに保存される時間に影響が及ぶ可能性があります。 • BlackBerry では、プライベートネットワークアドレス通信を完全に可視化する必要がある環境でのみ、このセンサを有効にすることをお勧めします。
Windows の高度な監査の可視性	この CylanceOPTICS エージェントは、Windows の追加のイベントタイプとカテゴリを監視します。 信号対雑音比：中程度 データの保持とパフォーマンスへの影響の可能性：低	—	このセンサは、次のイベント ID の監視を有効にします。 • 4769 Kerberos チケットの要求 • 4662 Active Directory オブジェクトの操作 • 4624 ログオンに成功 • 4702 スケジュールされたタスクの作成
Windows イベントログの可視性	この CylanceOPTICS エージェントは、Windows のセキュリティイベントとその関連属性を記録します。 信号対雑音比：中程度 データの保持とパフォーマンスへの影響の可能性：中程度	推奨環境： • デスクトップ • ノートパソコン • サーバー 非推奨環境： • ドメインコントローラ • Microsoft Exchange とメールサーバー	• このセンサが収集したデータ元の Windows イベントログは、通常のシステム使用中に頻繁に生成されます。 • 重複するデータを減らし、データの保持期間を長くするため、Windows イベントログからデータを収集するツールが組織に既に存在しているかどうかを確認してください。

脅威を識別するために **CylanceOPTICS** が使用するデータ構造

イベント、アーチファクト、ファセットは、デバイスで発生するアクティビティを分析、記録、調査するために CylanceOPTICS が使用する 3 つの主要なデータ構造です。InstaQuery、フォーカスデータ、Context Analysis Engine（CAE）などの CylanceOPTICS の機能が、これらのデータ構造を利用します。

このセクションでは、CylanceOPTICS がデバイス上のアクティビティを解釈して関与する仕組みについて詳しく説明します。これにより、検出データ、クエリデータ、フォーカスデータをさらに深く理解して活用できるようになります。

OS 別のデータソース

CylanceOPTICS エージェントは、次のデータソースを使用します。

OS	データソース
Windows	• CyOpticsDrv カーネルドライバ • イベントトラッキング • セキュリティ監査ログ
macOS	CyOpticsDrvOSX カーネルドライバ
Linux	ZeroMQ

CylanceOPTICS によってデフォルトで除外されるネットワークトラフィックのタイプについては、「KB65604」を参照してください。

イベント

イベントとは、デバイスに対して観察可能な変更またはアクションをもたらす構成要素のことです。イベントは、2 つの主要なアーチファクト（アクションを開始するインスティゲーティングアーチファクトと、操作を実行するターゲットアーチファクト）から構成されます。

次の表では、CylanceOPTICS による検出および操作が可能なイベントタイプの詳細を示します。

イベント：任意

- 有効にするデバイスポリシーオプション：CylanceOPTICS チェックボックス
- アーチファクトタイプ：プロセス、ユーザー
- プラットフォーム：Windows、macOS、Linux

イベントタイプ	説明
任意	すべてのイベントは、それらを生成したプロセスと、アクションに関連付けられたユーザーを記録します。

イベント：アプリケーション

- 有効にするデバイスポリシーオプション：高度な WMI の可視性
- アーチファクトタイプ：WMI トレース
- プラットフォーム：Windows

イベントタイプ	説明
フィルターを作成 - コンシューマバインディング	プロセスによって WMI の永続性が使用されました。
一時コンシューマを作成	プロセスによって WMI イベントがサブスクライブされました。
操作を実行	プロセスによって WMI 操作が実行されました。

- 有効にするデバイスポリシーオプション：強化されたプロセスとフッキングの可視性
- アーチファクトタイプ：ファイル
- プラットフォーム：Windows

イベントタイプ	説明
CBT	SetWindowsHookEx API によって、CBT アプリケーションに役立つ通知を受信するためのフックがインストールされました。
DebugProc	SetWindowsHookEx API によって、他のフックプロシージャをデバッグするためのフックがインストールされました。
非同期キー状態を取得	プロセスによって Win32 GetAsyncKeyState API が呼び出されました。
JournalPlayback	SetWindowsHookEx API によって、WH_JOURNALRECORD フックプロシージャが前に記録したメッセージを監視するフックがインストールされました。
JournalRecord	SetWindowsHookEx API によって、システムメッセージキューに入れられた入力メッセージを監視するフックがインストールされました。
キーボード	SetWindowsHookEx API によって、キーストロークメッセージを監視するフックがインストールされました。
低レベルキーボード	SetWindowsHookEx API によって、低レベルのキーボード入力イベントを監視するフックがインストールされました。
低レベルマウス	SetWindowsHookEx API によって、低レベルのマウス入力イベントを監視するフックがインストールされました。
メッセージ	SetWindowsHookEx API によって、メッセージキューに入れられたメッセージを監視するフックがインストールされました。
マウス	SetWindowsHookEx API によって、マウスメッセージを監視するフックがインストールされました。
Raw Inputデバイスを登録	プロセスによって、Win32 RegisterRawInputDevices API が呼び出されました。

イベントタイプ	説明
Windows イベントフックを設定	プロセスによって、Win32 SetWinEventHook API が呼び出されました。
Windows フックを設定	SetWindowsHookEx API によって、リストにないフックタイプ値がインストールされました。
ShellProc	SetWindowsHookEx API によって、シェルアプリケーションに役立つ通知を受信するためのフックがインストールされました。
SysMsg	SetWindowsHookEx API によって、ダイアログボックス、メッセージボックス、またはスクロールバーでの入力イベントの結果として生成されるメッセージを監視するフックがインストールされました。
WindowProc	SetWindowsHookEx API によって、Windows プロシージャメッセージを監視するフックがインストールされました。

- 有効にするデバイスポリシーオプション：API センサ
- アーチファクトタイプ：API 呼び出し
- プラットフォーム：Windows

イベントタイプ	説明
関数	重要な関数呼び出しが実行されました。

- 有効にするデバイスポリシーオプション：モジュールロードの可視性
- アーチファクトタイプ：ファイル
- プラットフォーム：Windows

イベントタイプ	説明
ロード	アプリケーションがモジュールをロードしました。

- 有効にするデバイスポリシーオプション：COM オブジェクトの可視性
- プラットフォーム：Windows

イベントタイプ	説明
作成済み	COM オブジェクトが作成されました。

イベント：デバイス

- 有効にするデバイスポリシーオプション：CylanceOPTICS チェックボックス
- アーチファクトタイプ：ファイル
- プラットフォーム：macOS、Linux

イベントタイプ	説明
マウント	デバイスがマシンに接続されているか、フォルダが特定のネットワークロケーションにマウントされています。

イベント：ファイル

- 有効にするデバイスポリシーオプション：CylanceOPTICS チェックボックス
- アーチファクトタイプ：ファイル
- プラットフォーム：Windows、macOS、Linux

イベントタイプ	説明
作成	ファイルが作成されました。
削除	ファイルが削除されました。
上書き	ファイルが上書きされました。
名前変更	ファイルの名前が変更されました。
書き込み	ファイルが変更されました。

- 有効にするデバイスポリシーオプション：強化されたファイル読み取りの可視性
- アーチファクトタイプ：ファイル
- プラットフォーム：Windows

イベントタイプ	説明
オープン	ファイルが開かれました。

イベント：メモリ

- 有効にするデバイスポリシーオプション：CylanceOPTICS チェックボックス
- アーチファクトタイプ：プロセス
- プラットフォーム：macOS、Linux

イベントタイプ	説明
Mmap	一定のメモリ領域が、特定の目的（通常はプロセスに割り当てられます）に対応付けられました。
MProtect	メモリ領域のメタデータが変更されました。通常はステータスが変更（実行可能になるなど）されます。

イベント：ネットワーク

- 有効にするデバイスポリシーオプション：CylanceOPTICS チェックボックス
- アーチファクトタイプ：ネットワーク

- プラットフォーム：Windows、macOS、Linux

イベントタイプ	説明
接続	ネットワーク接続が確立されました。デフォルトでは、ローカルトラフィックは収集されません。

- 有効にするデバイスポリシーオプション：プライベートネットワークアドレスの可視性
- アーチファクトタイプ：ネットワーク
- プラットフォーム：Windows

イベントタイプ	説明
接続	接続イベントにはローカルトラフィックが含まれます。

- 有効にするデバイスポリシーオプション：DNS の可視性
- アーチファクトタイプ：DNS 要求
- プラットフォーム：Windows、Linux

イベントタイプ	説明
要求	プロセスによって、キャッシュ保存されなかったネットワーク DNS 要求が作成されました。
応答	プロセスによって、DNS 応答が受信されました。

- 有効にするデバイスポリシーオプション：HTTP の可視性
- アーチファクトタイプ：HTTP
- プラットフォーム：Windows

イベントタイプ	説明
ゲット	Windows が WinINet または WinHTTP を使用して HTTP 要求を行いました。
投稿	Windows が WinINet または WinHTTP を使用してデータを送信しました。

イベント：プロセス

- 有効にするデバイスポリシーオプション：CylanceOPTICS チェックボックス
- アーチファクトタイプ：プロセス

イベントタイプ	プラットフォーム	説明
異常終了	macOS Linux	事前選択センサによって、プロセスが完了せずに終了した（例外によるプロセスの終了など）ことが検知されました。

イベントタイプ	プラットフォーム	説明
終了	Windows macOS Linux	プロセスが終了しました。
強制終了	macOS Linux	事前選択センサによって、プロセスが別のプロセスによって強制終了されたことが検知されました。
PTrace	macOS Linux	あるプロセスが別のプロセスを監視および制御できるようにする Unix のシステムツールです。
開始	Windows macOS Linux	プロセスが開始されました。
一時停止	Linux	事前選択センサによって、プロセスが中断されたことが検知されました。
不明な Linux プロセスイベント	macOS Linux	事前選択センサによって、対象としてプロセスで不明なイベントが発生したことが検知されました。これは、悪意のあるソフトウェアがその活動を隠している兆候である可能性があります。

- 有効にするデバイスポリシーオプション：強化されたプロセスとフッキングの可視性
- アーチファクトタイプ：プロセス
- プラットフォーム：Windows

イベントタイプ	説明
SetThreadContext	プロセスによって、SetThreadContext API が呼び出されました。
停止	扇動プロセスによって、別の対象プロセスが終了させられました。

イベント：レジストリ

- 有効にするデバイスポリシーオプション：CylanceOPTICS チェックボックス
- アーチファクトタイプ：レジストリ、ファイル（レジストリキーが特定のファイルを参照している場合）
- プラットフォーム：Windows

イベントタイプ	説明
KeyCreated	レジストリキーが作成されました。
KeyDeleting	レジストリキーが削除されました。
ValueChanging	レジストリキーの値が変更されました。

イベントタイプ	説明
ValueDeleting	レジストリキー値が削除されました。

イベント：スクリプティング

- 有効にするデバイスポリシーオプション：高度なスクリプトの可視性
- アーチファクトタイプ：Powershell トレース
- プラットフォーム：Windows

イベントタイプ	説明
コマンドを実行	Windows PowerShell がコマンドを実行しました。パラメーターは不明です。
スクリプトを実行	Windows PowerShell がスクリプトを実行しました。
ScriptBlock を実行	Windows PowerShell によってスクリプトブロックが実行されました。
コマンドを呼び出す	Windows PowerShell によって、バインドされたパラメーターを持つコマンドが呼び出されました。
スクリプトを禁止	AMSI ScanBuffer の結果は、スクリプトが管理者によって検出またはブロックされたことを示しています。

イベント：ユーザー

- 有効にするデバイスポリシーオプション：高度なスクリプトの可視性
- アーチファクトタイプ：Windows イベント
- プラットフォーム：Windows

イベントタイプ	説明
バッチログオフ	次の Windows イベント ID が発生しました：4634（タイプ 4）
バッチログオン	次の Windows イベント ID が発生しました：4624（タイプ 4）
キャッシュされた対話型ログオフ	次の Windows イベント ID が発生しました：4634（タイプ 11）
キャッシュされた対話型ログオン	次の Windows イベント ID が発生しました：4624（タイプ 11）
対話型ログオフ	次の Windows イベント ID が発生しました：4634（タイプ 2）
対話型ログオン	次の Windows イベント ID が発生しました：4624（タイプ 2）
ネットワークログオフ	次の Windows イベント ID が発生しました：4634（タイプ 3）

イベントタイプ	説明
ネットワークログオン	次の Windows イベント ID が発生しました：4624（タイプ 3）
NetworkClearText ログオフ	次の Windows イベント ID が発生しました：4634（タイプ 8）
NetworkClearText ログオン	次の Windows イベント ID が発生しました：4624（タイプ 8）
NewCredentials ログオフ	次の Windows イベント ID が発生しました：4634（タイプ 9）
NewCredentials ログオン	次の Windows イベント ID が発生しました：4624（タイプ 9）
リモート対話型ログオフ	次の Windows イベント ID が発生しました：4634（タイプ 10）
リモート対話型ログオン	次の Windows イベント ID が発生しました：4624（タイプ 10）
サービスログオフ	次の Windows イベント ID が発生しました：4634（タイプ 5）
サービスログオン	次の Windows イベント ID が発生しました：4624（タイプ 5）
ロック解除ログオフ	次の Windows イベント ID が発生しました：4634（タイプ 7）
ロック解除ログオン	次の Windows イベント ID が発生しました：4624（タイプ 7）
ユーザーログオフ	次の Windows イベント ID が発生しました：4634（リストにないタイプ値）
ユーザーログオン	次の Windows イベント ID が発生しました：4624（リストにないタイプ値）

アーチファクトとファセット

アーチファクトは、CylanceOPTICS が使用できる複合的な情報です。コンテキスト分析エンジン（CAE）は、デバイス上のアーチファクトを識別し、それらを使用してインシデントへの自動応答と修正アクションをトリガーできます。InstaQuery では、クエリの基礎としてアーチファクトが使用されます。

ファセットは、イベントに関連付けられたアーチファクトの特徴を識別するために使用できるアーチファクトの属性です。ファセットは、潜在的に悪意のあるアクティビティを特定するために、分析時に関連付けて組み合わせられます。たとえば、「explorer.exe」という名前のファイルは、本来疑わしいものではないかもしれませんが、ファイルが Microsoft によって署名されておらず、一時ディレクトリにある場合、環境によっては疑わしいものに区別されることがあります。

CylanceOPTICS では、次のアーチファクトとファセットが使用されます。

アーチファクト	ファセット
API呼び出し	• 関数 • DLL • パラメーター
DNS	• 接続 • IsRecursionDesired • IsUnsolicitedResponse • Opcode • RequestId • レゾリューション • ResponseOriginatedFromThisDevice • クエスチョン
イベント	• 発生時間 • 登録時間
ファイル	• 実行可能ファイルレコード（バイナリのみ） • ファイル作成時間（OS による報告） • ファイルパス • ファイルの署名（バイナリのみ） • ファイルサイズ • 最終変更時間（OS による報告） • MD5 ハッシュ（バイナリのみ） • 最近の書き込み位置 • SHA256 ハッシュ（バイナリのみ） • 疑わしいファイルタイプ • ユーザー
ネットワーク	• ローカルアドレス • ローカルポート • プロトコル • リモートアドレス • リモートポート
PowerShell トレース	• EventId • ペイロード • PayloadAnalysis • ScriptBlockText • ScriptBlockTextAnalysis

アーチファクト	ファセット
プロセス	• コマンドライン • 実行可能ファイルの実行元 • 親プロセス • プロセスID • 開始時刻 • ユーザー
レジストリ	• 値がシステム上のファイルを参照しているかどうか • レジストリパス • 値
ユーザー	• ドメイン • OS 固有の ID（SID など） • ユーザー名 ユーザーアーチファクトには、以下のいずれかの値を含めることができますが、ほとんどのデバイスではデータを使用できません。 • AccountType • BadPasswordCount • Comment • CountryCode • FullName • HasPasswordExpired • HomeDirectory • IsAccountDisabled • IsLocalAccount • IsLockedOut • IsPasswordRequired • LanguageCodePage • LogonServer • PasswordAge • PasswordDoesNotExpire • ProfilePath • ScriptPath • UserPrivilege • Workstations

アーチファクト	ファセット
Windows イベント	• クラス • イベントID • ObjectServer • PrivilegeList • プロセスID • プロセス名 • プロバイダ名 • サービス • SubjectDomainName • SubjectLogonId • SubjectUserName • SubjectUserSid
WMI トレース	• ConsumerText • ConsumerTextAnalysis • EventId • Namespace • Operation • OperationAnalysis • OriginatingMachineName

レジストリキーと値

CylanceOPTICS は、一般的な永続性、プロセスの起動、権限の昇格キーと値、および「KB 66266」に示されている値を監視します。

CylanceOPTICS がレジストリ内の永続化ポイントを監視する方法の詳細については、「KB 66357」を参照してください。

CylanceOPTICS で有効になっているデバイスの表示

デバイスにインストールされている CylanceOPTICS エージェントのバージョン、デバイスの IP アドレス、割り当てられたゾーンなど、CylanceOPTICS で有効になっているすべてのデバイスの詳細とステータス情報を表示できます。デバイスビューを使用して、潜在的な脅威を管理するためのアクションを実行できます。

90 日以上オフラインのデバイスはコンソールに表示されません。

1. 管理コンソールのメニューバーで、［**CylanceOPTICS**］ > ［デバイス］をクリックします。
2. をクリックして結果をフィルタリングし、特定のデバイスまたはデバイスのグループを検索します。
3. 次の操作のいずれかを実行します。

タスク	手順
デバイスの概要の詳細を表示します。	デバイス名をクリックします。

タスク	手順
デバイスの詳細を表示し、デバイスのプロパティと割り当てを変更します。	**a.** ［詳細］列で、［表示］をクリックします。 **b.** ［デバイスプロパティを編集］では、デバイス名、割り当てられたデバイスポリシー、割り当てられたゾーン、CylanceOPTICS エージェントログレベル、および保護レベルを変更できます。［保存］をクリックします。 **c.** ［脅威と活動］セクションでは、CylanceOPTICS エージェントが検出した脅威の詳細を表示できます。
デバイスをロックします。	「デバイスのロック」を参照してください。
デバイスからデータを収集するパッケージを展開します。	**a.** デバイス名をクリックします。 **b.** ［アクションを選択］ドロップダウンリストで、［パッケージ展開］をクリックします。 **c.** 「デバイスからデータを収集するパッケージの展開」の手順に従います。
リモート応答セッションを開始して、デバイスにコマンドを送信します。	**a.** デバイス名をクリックします。 **b.** ［アクションを選択］ドロップダウンリストで、［リモート応答］をクリックします。 **c.** リモート応答セッションウィンドウにコマンドを入力します。 詳細については、「デバイスへのアクションの送信」を参照してください。
すべてのデバイスの .csv ファイルをエクスポートします。	をクリックします。

InstaQuery と高度なクエリを使用したアーチファクトデータの分析

InstaQuery と高度なクエリは、アーチファクトデータを分析して侵害の指標を検出し、組織のデバイスでの出現率を判断するための CylanceOPTICS 機能です。クエリの結果は、アーチファクトがいつどのように使用されたかを示すものではありませんが、組織のデバイスやデータに脅威を知らせる、フォレンジック的に重要な方法でアーチファクトが観察されたことがあるかどうかを示します。

InstaQuery を使用すると、特定のタイプのフォレンジックアーチファクトについてデバイスセットを調査できます。また、デバイスにアーチファクトが存在するかどうか、およびそのアーチファクトがどの程度の頻度で発生するかを判断できます。高度なクエリは InstaQuery を進化させたものであり、EQL 構文を使用する詳細な検索機能で、脅威を特定する機能を強化します。

CylanceOPTICS エージェントをデバイスにインストールして有効にすると、エージェントはアーチファクトを収集し、CylanceOPTICS データベースに保存します。CylanceOPTICS エージェント 2.x 以前のバージョンでは、データベースはデバイス上にローカルに保存されます。CylanceOPTICS エージェント 3.0 以降では、エージェントは自動的にデータを CylanceOPTICS クラウドデータベースにアップロードし、保存します。クエリを作成す

ると、フォレンジック的に重要なデータが CylanceOPTICS データベースから取得されます。管理コンソールで結果を表示し、調査できます。

CylanceOPTICS エージェント 2.x 以前のデバイスでは、デバイスがオンラインの場合にのみクエリを正常に完了できます。エージェント 3.0 以降のデバイスでは、クエリは CylanceOPTICS クラウドデータベースで使用可能な最新データを使用するため、デバイスをオンラインにする必要はありません。

1 つのクエリで、最大 10,000 件の結果を表示し、保持できます。クエリの結果は 60 日間保持されます。

クエリ可能な特定のアーチファクトについて、次の詳細に注意してください。

アーチファクト	詳細
ファイル	CylanceOPTICS エージェントがデバイスにインストールされた後に作成、変更、または削除された特定のファイルをクエリできます。CylanceOPTICS では、コンテンツの実行に使用できるファイル（実行可能ファイル、Microsoft Office ドキュメント、PDF など）に焦点を当てます。
ネットワーク接続	IPv4 と IPv6 の両方の宛先 IP アドレスに対してクエリを実行できます。CylanceOPTICS では、プライベート、ルーティング不能、マルチキャスト、リンクローカル、およびループバックネットワークトラフィックを破棄します。
処理	すべてのプロセスが CylanceOPTICS データベース内でインデックス付けされますが、次の制限があります。 • コマンドラインは 1KiB のデータに制限されています • プロセス名は 256 文字に制限されています • プロセスイメージファイルパスは 512 文字に制限されています • プロセスの開始後に変更されたコマンドラインは監視されません
レジストリキー	CylanceOPTICS は、永続化ポイントとファイル削除ポイントのみを監視します。これらは通常、マルウェアによって悪用される領域です。 CylanceOPTICS によって監視されるレジストリキーと値の詳細なリストについては、「KB66266」を参照してください。 CylanceOPTICS がレジストリ内の永続化ポイントを監視する方法の詳細については、「KB66357」を参照してください。

InstaQuery の作成

1. 管理コンソールのメニューバーで、［**CylanceOPTICS**］ > ［**InstaQuery**］をクリックします。
2. 次の操作のいずれかを実行します。

タスク	手順
新しい InstaQuery を作成します。	以前のクエリを複製する場合には［以前のクエリ］セクションを展開して、クエリを見つけて、［クエリを複製］をクリックします。 **a.** ［検索語句］フィールドに検索する値（ファイル名、ハッシュ、プロセス、レジストリ値など）を入力します。完全一致を検索する場合は、［完全一致］チェックボックスをオンにします。 **b.** ［アーチファクト］ドロップダウンリストで、アーチファクトタイプをクリックします。 **c.** ［ファセット］ドロップダウンリストで、適切なファセットをクリックします。 **d.** ［ゾーン］ドロップダウンリストで、1 つ以上のゾーンを選択します。 **e.** クエリの名前と説明を入力します。 **f.** ［クエリを送信］をクリックします。 **g.** クエリの現在のステータスが［以前のクエリ］セクションに表示されます。クエリが完了したら、［結果を表示］をクリックします。
前の InstaQuery が表示されます。	**a.** ［以前のクエリ］セクションを展開します。 **b.** 表示するクエリについて、［結果を表示］をクリックします。

3. ［**InstaQuery** の結果］セクションでは、［アクション］メニューを展開して、それぞれの結果に対して使用可能なアクションにアクセスできます。結果のタイプに応じて、次のようなアクションがあります。
   - フォーカスデータを要求および表示します。
   - グローバル隔離ファイル。ファイルは、［設定］ > ［グローバルリスト］ > ［グローバル隔離］の、［保護］ > ［脅威］にある、デバイスの詳細の［脅威］セクションに表示されます。
   - ファイルを要求してダウンロードします。他のアーチファクトタイプに関連付けられたファイルについてのパス情報がある場合は、それらのファイルをダウンロードすることもできます。ファイルは、誤って実行されないようにするために、圧縮され、パスワードで保護されています。パスワードは「infected」です。

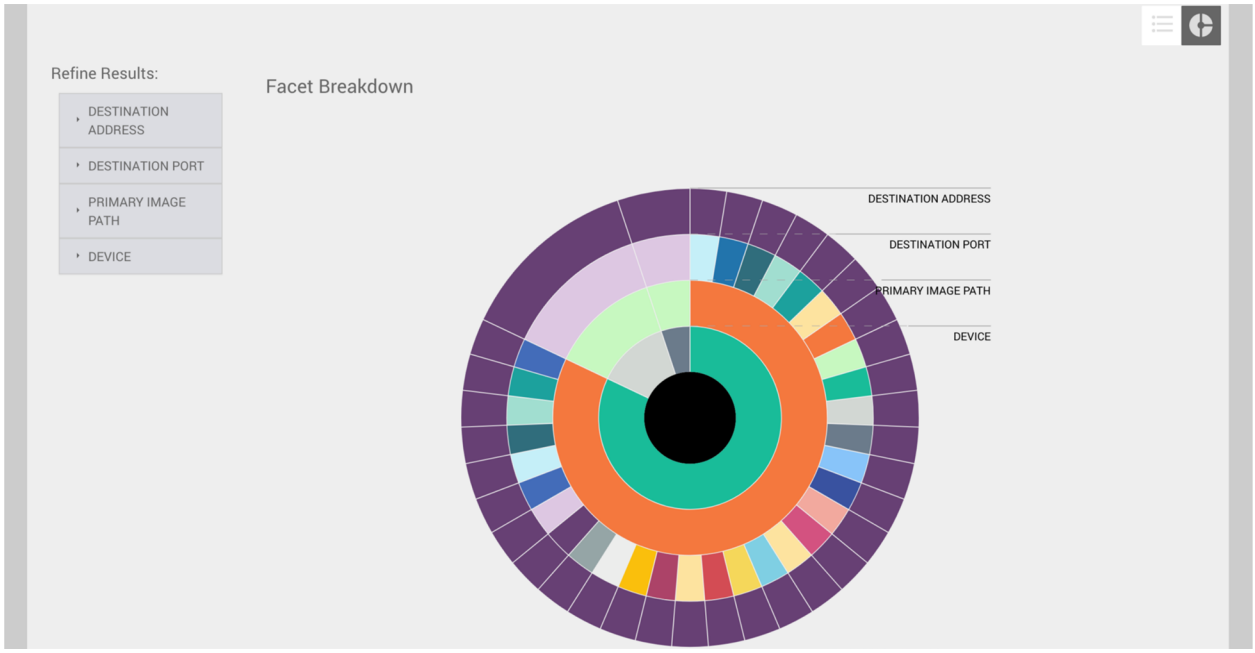
     ファイル取得のサイズ制限は 50MB です。アーチファクトとファイルは、CylanceOPTICS により 30 日間保持されます（この期間は組織のライセンスに基づいて延長できます）。
4. InstaQuery のファセットの詳細を表示するには、［**InstaQuery** の結果］セクションで、ファセットの詳細アイコンをクリックします。

InstaQuery ファセットの詳細の使用

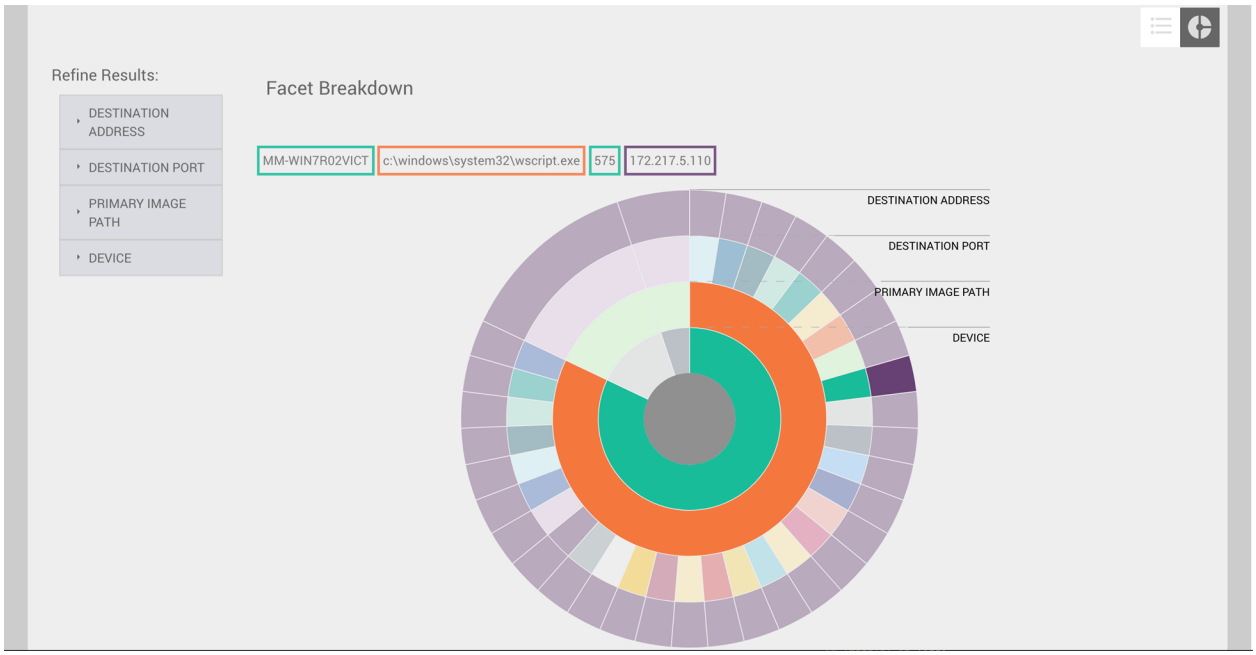
InstaQuery ファセットの詳細は、クエリに関係するさまざまなファセットをインタラクティブかつ視覚的に示すため、そのリレーショナルパスを識別したり辿ったりするために利用できます。

ファセットの詳細のサンバーストモデルは、特定のデータセット内の疑わしいアクティビティを特定するのに役立ちます。たとえば、ある環境または複数のゾーンで疑わしいネットワーク接続を検出しようとすると、データの量と複雑さのために、データパターンと異常を特定するのが困難になることがあります。次の画像は、ファセットの詳細でデータを表示およびフィルタリングして、疑わしいアクティビティをすばやく特定する方法を示しています。

次の画像は、特定の IP アドレスへの接続を検索する InstaQuery を作成することによって生成されました。クエリの結果は、デバイス、プライマリイメージパス、宛先ポート、宛先アドレスというファセットを含むサンバースト図として視覚化されています。

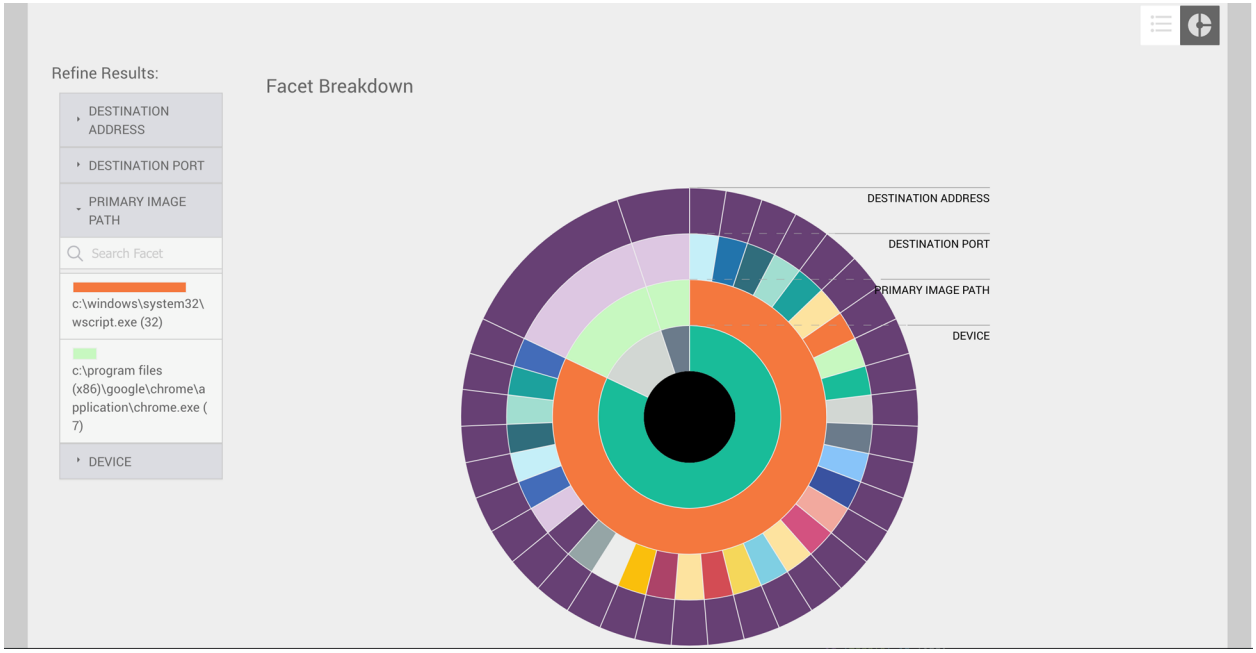


任意のファセットにカーソルを合わせると、関連する値を表示できます。次の画像では、管理者が一番外側のファセットを選択してデバイス名、ネットワーク接続を開始したファイルへのパス、接続に使用されたポート番号、およびリモートシステムの IP アドレスを表示しています。



ファセットにカーソルを合わせると、関連する親ファセットも強調表示され、データポイント間の関係を視覚的に描画するのに役立ちます。上の例では、1 つのデバイスと 1 つの親プロセスが IP アドレスへのほとんどの接続を担当していることがわかります。また、この図は、関連ホストからこの IP アドレスに接続するために多数の異なるネットワークポートが使用されていることを示しています。これは、この図の他の 2 つのホストファセットとは異なります。

また、結果の絞り込みメニューから有用な情報を取得することもできます。各ファセットメニューには、一意の値と各ファセットのオカレンス数が含まれます。次の例では、この IP アドレスへの接続を担当する 2 つのプロセスとして Google Chrome と Wscript があることがわかります。



結果の絞り込みメニューでファセット値をクリックすると、直接関連するファセットが図に表示されます。この機能は、無関係なデータを除外し、より焦点を絞った分析を可能にするのに役立ちます。

高度なクエリの作成

高度なクエリ機能を使用すると、カスタムクエリを作成して脅威探索アクティビティを強化できます。高度なクエリによって、CylanceOPTICS 環境の詳細な可視性、広範なクエリオプション、最適化したワークフローが提供され、関連検索を組み合わせて新しいインサイトを示すことができます。高度なクエリは、CylanceOPTICS エージェントバージョン 3.0 以降を搭載したデバイスでサポートされています。

高度なクエリでは、EQL 構文を使用します。EQL を使用してイベントのクエリを構築すると、その結果では、これらのイベントに関係したアーチファクトについての情報が提供されます。高度なクエリ UI には、EQL クエリの構築に役立つ構文情報が含まれています。

作業を始める前に：「高度なクエリでサポートされる EQL 構文」と「CylanceOPTICS EQL クエリの例」を確認してください。

1. 管理コンソールのメニューバーで、［**CylanceOPTICS**］ > ［高度なクエリ］をクリックします。
2. 次の操作のいずれかを実行します。

タスク	手順
新しい高度なクエリを作成する	既存のクエリテンプレートを使用して新しいクエリを作成する場合は、［テンプレートリストを表示］をクリックしてテンプレートをクリックし、次の最初の手順を省略します。 **a.** クエリフィールドで、クエリの EQL 構文を入力するか貼り付けます。入力を開始すると、構文オプションと検証メッセージが表示され、クエリを作成しやすくなります。 現在のクエリをテンプレートとして保存する場合は、［テンプレートとして保存］をクリックします。名前と説明を入力し、テンプレートをプライベートにするか、全管理者が使用できるようにするかを選択します。［保存］をクリックします。クエリのピン留め、編集、削除は、テンプレートリストから行うことができます。 **b.** クエリの範囲を設定するには、［デバイスを検索］で［ゾーンごと］または［デバイスごと］をクリックします（各デバイスの横にあるアイコンは、デバイスがオンラインであるかどうかを示します）。1 つまたは複数のゾーンまたはデバイスを選択し、［保存］をクリックします。範囲を設定しない場合、クエリはすべてのゾーンとデバイスに適用されます。 **c.** クエリの日付と時刻の範囲を設定するには、をクリックして範囲を設定します。［適用］をクリックします。範囲を設定しない場合、クエリは使用可能なすべてのデータに適用されます。 **d.** 次の操作のいずれかを実行します。 • クエリを実行する場合は、［クエリを実行］をクリックします。 • 特定の日時または定期的な間隔でクエリを実行するようにスケジュールする場合は、［クエリをスケジュール］をクリックします。名前と説明を入力し、クエリをプライベートにするか、すべてのユーザーに表示するかを選択し、日付、時刻、およびオプションの繰り返し設定を指定します。前回の実行以降に収集されたデータにクエリを制限する場合は、［新しいデータのみをクエリする］チェックボックスをオンにします。［クエリをスケジュール］をクリックします。 ［スケジュール済みのクエリ］タブでは、スケジュール済みのクエリを表示および編集でき、その結果を表示およびエクスポートできます。アクティブに実行されているクエリ、または実行するようにスケジュールされているクエリは、最大 25 個まで使用できます。停止したクエリまたは完了済みの単一実行クエリは、この制限にカウントされません。 クエリ結果を保存して後で［クエリのスナップショット］タブから表示する場合は、結果セクションで をクリックします。名前と説明を入力し、結果をプライベートにするか、全ユーザーに表示するかを選択します。
クエリスナップショットを表示する	［クエリのスナップショット］タブで、クエリのスナップショットをクリックします。 なお、これはクエリを保存した時の元の結果を表示します。新しいクエリの結果ではありません。

3. クエリ結果をフィルタリングする場合は、次のいずれかを行います。

- 日付とタイムスタンプでクエリ結果をフィルタリングするには、ヒストグラムの 1 つまたは複数のバーをクリックして、その日付と時間範囲でフィルタリングします。選択した範囲内の任意のバーをクリックすると、その日付と時刻のフィルターが削除されます。
- クエリ結果を列でフィルタリングするには、その列（［デバイス］など）の をクリックして、フィルター条件を選択します。
- 指定した値でクエリ結果をフィルタリングするには、クエリ結果の上にある をクリックし、検索フィールドに値を入力するか貼り付けます（特定のタイムスタンプ、イベント詳細値など）。

4. 結果を展開して詳細を表示します。» をクリックすると、イベントの詳細と関連するアラートに関する情報を含むパネルが開きます（結果ウィンドウを右にスクロールする必要がある場合があります）。1 つまたは複数の特定のファセットの一致を表示するようにクエリ結果をフィルタリングするには、それらのファセットの をクリックします。フィルターを削除するには、アイコンを再度クリックします。
5. クエリ結果で、⋮メニューを展開して、各結果に対して使用可能なアクションを表示します。結果のタイプに応じて、次のようなアクションがあります。
   - フォーカスデータを要求および表示します。
   - グローバル隔離ファイル。このファイルは、デバイス詳細の［設定］>［グローバルリスト］>［グローバル隔離］、［保護］>［脅威］、および［脅威］セクションに表示されます。
   - ファイルを要求してダウンロードします。他のアーチファクトタイプに関連付けられたファイルについてのパス情報がある場合は、それらのファイルをダウンロードすることもできます。ファイルは、誤って実行されないようにするために、圧縮され、パスワードで保護されています。パスワードは「infected」です。ファイル取得のサイズ制限は 50MB です。アーチファクトとファイルは、CylanceOPTICS によって 30 日間保持されます。
6. 結果をピン留めして、その後のクエリで表示された場合に視覚的なマーカーで表示されるようにする場合は、 をクリックします。

終了したら：

- クエリの結果を .csv ファイルにエクスポートする場合は、 をクリックします。名前と説明を入力し、エクスポートした結果をプライベートにするか、すべての管理者に表示するかを指定し、［エクスポート］をクリックします。ファイルの準備ができたら、［エクスポート済みの結果］タブからファイルをダウンロードできます。
- 新しいクエリを追加するには、現在のクエリタブの横にある をクリックします。
- 既存のクエリをコピーするには、そのクエリタブにカーソルを合わせ、 をクリックします。

高度なクエリでサポートされる **EQL** 構文

構文ヘルプ

［CylanceOPTICS］>［高度なクエリ］の構文ヘルプペインには、使用可能な CylanceOPTICS イベントクラスと、それに関連するアーチファクト、タイプ、カテゴリ、およびサブカテゴリが一覧表示されます。入力を開始すると、構文オプションと検証メッセージが表示され、クエリを作成しやすくなります。

EQL クエリ形式

CylanceOPTICS EQL クエリでは、基本クエリに次の形式を使用します。

```
<event class> where <event/artifact>.<facet> == <value>
```

クエリはアーチファクトに関連するイベントを検索するため、クエリで関連するイベントクラスを使用する必要があります。

where 句は、event.type、event.category、event.subcategory、または artifact.facet の値に基づいて結果をフィルタリングできます。

or または and を使用して、複数のフィルター句を組み合わせることができます。

任意のイベントクラスの照合

イベントクラスに any を使用して、すべての利用可能なイベントクラスにマッピングできます。

イベントクラスのエスケープ

特殊文字（ハイフンやピリオドなど）を含むイベントクラスをエスケープするには、スペースを含めるか、数字で始まり、引用符（"）で囲む、または 3 つの引用符（""）で囲みます。

フィールド名のエスケープ

ハイフン、スペース、または数字で始まるフィールド名をエスケープするには、バックティック（`）で囲みます。フィールド名のバックティック（`）をエスケープするには、2 個のバックティック（``）で囲みます。

値のエスケープ

値に引用符やバックスラッシュを含む特殊文字を使用する場合は、前にバックスラッシュを付けてエスケープする必要があります（例：引用符の場合は \"、バックスラッシュの場合は \\）。

条件

条件は、イベントが一致する必要がある 1 つ以上の条件で構成されます。次のセクションで説明する演算子を使用して、条件を指定して組み合わせることができます。

比較演算子

演算子	説明
<	この演算子は、演算子の左側の値が右側の値より小さい場合に TRUE を返します。それ以外の場合は FALSE を返します。
<=	この演算子は、演算子の左側の値が右側の値と等しいか小さい場合に TRUE を返します。それ以外の場合は FALSE を返します。
==	この演算子は、演算子の左側と右側の値が等しい場合に TRUE を返します。それ以外の場合は FALSE を返します。ワイルドカードはサポートされていません。
:	この演算子は、演算子の左右の文字列が等しい場合に TRUE を返します。それ以外の場合は FALSE を返します。文字列の比較にのみ使用できます。

演算子	説明
!=	この演算子は、演算子の左右の値が等しくない場合に TRUE を返します。それ以外の場合は FALSE を返します。ワイルドカードはサポートされていません。NULL 値も結果からフィルタリングされることに注意してください（==NULL を使用して NULL の結果を表示できます）。
>=	この演算子は、演算子の左側の値が右側の値と等しいか大きい場合に TRUE を返します。それ以外の場合は FALSE を返します。文字列を比較する場合、演算子は大文字と小文字を区別した辞書式順序を使用します。
>	この演算子は、演算子の左側の値が右側の値より大きい場合に TRUE を返します。それ以外の場合は FALSE を返します。文字列を比較する場合、演算子は大文字と小文字を区別した辞書式順序を使用します。

= は等しい演算子としてサポートされていません。== または : を使用します。

パターン比較キーワード

演算子	説明
like	この演算子は、キーワードの左側の文字列が右側の文字列と一致する場合に TRUE を返します（大文字と小文字が区別されます）。リスト検索（以下の lookup 演算子を参照）をサポートしており、文字列の比較にのみ使用できます。大文字と小文字を区別しない照合には、like~ を使用します。
regex	この演算子は、キーワードの左側の文字列が右側の正規表現と一致する場合に TRUE を返します（「正規表現の構文」を参照）。list 検索をサポートし、文字列の比較にのみ使用できます。大文字と小文字を区別しない照合には、regex~ を使用します。

```
my_field like  "VALUE*"         // case-sensitive wildcard matching
my_field like~ "value*"         // case-insensitive wildcard matching

my_field regex  "VALUE[^Z].?"   // case-sensitive regex matching
my_field regex~ "value[^z].?"   // case-insensitive regex matching
```

比較の制限

比較を連鎖することはできません。代わりに、比較の間に論理演算子を使用します（以下の論理演算子のセクションを参照）。

たとえば、`foo < bar <= baz` はサポートされていませんが、`foo < bar and bar <= baz` はサポートされています。

関数を使用してフィールドを変更した場合でも、フィールドを別のフィールドと比較することはできません。

次のクエリは、process.parent.name フィールドの値と process.name フィールドを比較するため無効です。

```
process where process.parent.name == "foo" and process.parent.name == process.name
```

次のクエリは、process.parent.name フィールドと process.name フィールドの両方を静的な値と比較するため、有効です。

```
process where process.parent.name == "foo" and process.name == "foo"
```

論理演算子

演算子	説明
and	この演算子は、条件が左右の両方で TRUE を返した場合にのみ TRUE を返します。それ以外の場合は FALSE を返します。
OR	この演算子は、左側または右側のいずれかの条件が TRUE の場合に TRUE を返します。それ以外の場合は FALSE を返します。
not	この演算子は、右側の条件が FALSE の場合に TRUE を返します。

ルックアップ演算子

演算子	説明
in	この演算子は、指定されたリストに値が含まれている場合に TRUE を返します（大文字と小文字が区別されます）。大文字と小文字を区別しない照合の場合は、in~ を使用します。
not in	この演算子は、指定されたリストに値が含まれていない場合に TRUE を返します（大文字と小文字が区別されます）。大文字と小文字を区別しない照合の場合は、not in~ を使用します。
:	この演算子は、指定されたリストに文字列が含まれている場合に TRUE を返します。文字列の比較にのみ使用できます。
like	この演算子は、提供されたリストの文字列と文字列が一致する場合に TRUE を返します（大文字と小文字が区別されます）。文字列の比較にのみ使用できます。大文字と小文字を区別しない照合には、like~ を使用します。
regex	この演算子は、指定されたリスト内の正規表現パターンと文字列が一致する場合に TRUE を返します（正規表現構文を参照）。文字列の比較にのみ使用できます。大文字と小文字を区別しない照合には、regex~ を使用します。

```
my_field in ("Value-1", "VALUE2", "VAL3")                 // case-sensitive
my_field in~ ("value-1", "value2", "val3")                // case-insensitive

my_field not in ("Value-1", "VALUE2", "VAL3")             // case-sensitive
```

```
my_field not in~ ("value-1", "value2", "val3")           // case-insensitive

my_field : ("value-1", "value2", "val3")                 // case-insensitive

my_field like  ("Value-*", "VALUE2", "VAL?")             // case-sensitive
my_field like~ ("value-*", "value2", "val?")             // case-insensitive

my_field regex  ("[vV]alue-[0-9]", "VALUE[^2].?", "VAL3") // case-sensitive
my_field regex~  ("value-[0-9]", "value[^2].?", "val3")   // case-insensitive
```

すべての条件が一致する

イベントカテゴリだけでイベントを照合するには、`where true` 条件を使用します。たとえば、次のクエリはすべてのファイルイベントに一致します。

```
file where true
```

任意のイベントを照合するには、any キーワードを where true 条件と組み合わせます。

```
any where true
```

クエリの例

「CylanceOPTICS EQL クエリの例」を参照してください。

CylanceOPTICS EQL クエリの例

URL を指定して DNS ルックアップをクエリします。

```
network where dns.questions.question_name == "<URL>"
```

WMI の名前空間を指定してクエリします。

```
application where event.subcategory == "wmi" and wmi_trace.namespace ==
 "<namespace>"
```

指定した SHA256 値のいずれかを使用してファイルをクエリします。

```
file where file.sha256 in ("<value>", "<value>", "<value>")
```

プロセス名を指定してプロセスをクエリします。

```
process where process.name == "<name>"
```

コマンドラインに指定した文字列を含むプロセスをクエリします。

```
process where process.command_line like "<string>"
```

IP アドレスとポートを指定して、そこへのネットワーク接続に関する情報をクエリします。

```
network where network.destination.ip_address == "<IP>" and
 network.destination.port == "<port>"
```

フォーカスデータの表示

フォーカスデータを使用すると、一連のイベント、およびそれらのイベントに関連するアーチファクトやファセットを視覚化して分析できます。これにより、マルウェアやその他のセキュリティ脅威がデバイスに発生します。フォーカスデータは 30 日間保持されます。

CylanceOPTICS エージェント 2.x 以前のデバイスの場合、コンソールは、オンラインのデバイスからのみフォーカスデータを取得できます。エージェント 3.0 以降を使用しているデバイスの場合、コンソールは CylanceOPTICS クラウドデータベースから使用可能な最新データを取得できるため、デバイスをオンラインにする必要はありません。

作業を始める前に： デバイスのフォーカスデータの管理コンソールへの自動アップロードを有効にする場合は、デバイスポリシーでこれらのオプションをオンにします。このオプションを選択しない場合は、コンソールを使用してフォーカスデータを手動で要求する必要があります。

次の操作のいずれかを実行します。

タスク	手順
デバイスの詳細からフォーカスデータを表示します。	**a.** 管理コンソールのメニューバーで、［アセット］ **>** ［デバイス］をクリックします。 **b.** デバイスをクリックして、［脅威と活動］セクションを確認します。 **c.** 脅威またはイベントに関し、フォーカスデータの自動アップロードを有効にしていない場合は、［データを要求］をクリックします。 **d.** ［データを表示］をクリックします。
InstaQuery からフォーカスデータを表示します。	新しい InstaQuery を作成するには、「InstaQuery の作成」を参照してください。 **a.** 管理コンソールのメニューバーで、［**CylanceOPTICS**］ **>** ［**InstaQuery**］ **>** ［以前のクエリ］をクリックします。 **b.** InstaQuery については、［結果を表示］をクリックします。 **c.** 結果については、［アクション］ **>** ［フォーカスデータを要求］をクリックします。 **d.** ［フォーカスデータを表示］をクリックします。
マスターリストからフォーカスデータを表示します。	**a.** 管理コンソールのメニューバーで、［**CylanceOPTICS**］ **>** ［フォーカスデータ］をクリックします。 このリストには、管理者によって以前に要求されたフォーカスデータ、またはコンソールに自動的にアップロードされたフォーカスデータが含まれます。 **b.** アーチファクトまたはイベントについては、［フォーカスを表示］をクリックします。

終了したら：

- フォーカスデータ内の一部のアーチファクトまたはファセットには、詳細情報を取得するための［**InstaQuery** を作成］オプションが含まれている場合があります。これはピボットクエリと呼ばれます。アーチファクトまたはファセットのプロパティは事前に設定されているため、適切なゾーンの指定だけが必要です。ピボットクエリの結果は、関連するフォーカスデータとともに使用できます。

- フォーカスデータを .csv ファイルにエクスポートする場合は、 をクリックし、次に をクリックします。

CylanceOPTICS が取得したファイルの表示およびダウンロード

CylanceOPTICS がファイルを潜在的な脅威として識別すると、デバイスからファイルを取得できます（検出の詳細または InstaQuery の結果を確認する場合など）。CylanceOPTICS が取得したすべてのファイルのリストを表示できます。また、このビューからファイルをダウンロードして、さらに分析することもできます。

1. 管理コンソールのメニューバーで、［**CylanceOPTICS**］**>**［アクション履歴］をクリックします。
2. ［ファイルダウンロード履歴］タブをクリックします。
3. 結果をフィルター処理する場合は、 をクリックします。
4. ファイルをダウンロードする場合は、［ファイルをダウンロード］をクリックします。警告を確認し、［ダウンロードを確認］をクリックします。

CylanceOPTICS を使用したイベントの検出と対応

CylanceOPTICS は、コンテキスト分析エンジン（CAE）を使用し、デバイスで発生したイベントをほぼリアルタイムで分析して関連付けます。CAE ロジックはデバイス上にローカルに保存されます。これにより、デバイスが CylanceOPTICS クラウドサービスに接続されていない場合でも、CylanceOPTICS エージェントは悪意のあるアクティビティや疑わしいアクティビティを監視して追跡できます。CylanceOPTICS は、CAE が特定の関心アーチファクトを特定した場合に自動応答アクションを実行するように設定できます。これによって CylancePROTECT Desktop の機能を補完する脅威の検出と防止のレイヤが追加されます。

CylanceOPTICS の検出機能は、組織のニーズに合わせてカスタマイズできます。必要とする検出ルールと応答の設定を含む検出ルールセットを作成すること、既存の検出ルールを複製および変更すること、独自のカスタムルールを作成すること、検出例外を作成して特定のアーチファクトを検出から除外することができます。

検出ルールセットの作成

検出ルールセットを作成して適用し、CylanceOPTICS が検出するイベントのタイプと CylanceOPTICS によるそのイベントへの対応方法を設定します。用意されているデフォルトの検出ルールセットにより、検出ルールの使用方法をテストして評価できます。デフォルトのルールセットでは、検出ルールがすべて有効にされており、自動応答とユーザー通知は無効にされています。

検出ルールセットを作成する場合、初めは、応答アクションとデスクトップ通知を使用せずに目的の検出ルールを有効にすることをお勧めします。検出データを評価した後は、各ルールに対して適切な応答アクションとユーザー通知を設定できます。

作業を始める前に：

- ルールセットを表示するには、［エンドポイント検出応答］セクションの［ルールセットを表示］および［ルールセットを編集］権限を持つ管理者ロールが必要です。
- 組織の環境にインポートできるオプションの CylanceOPTICS ルールの詳細については、「KB76816」を参照してください。

1. 管理コンソールのメニューバーで、［**CylanceOPTICS**］ **>** ［設定］をクリックします。
2. ［ルールセット］タブで、［新規作成］をクリックします。
3. 名前と説明を入力します。
4. デバイスでルールがトリガーされたときに CylanceOPTICS エージェントにメッセージを表示させる場合は、［検出通知メッセージ］フィールドにメッセージを入力します。
5. 使用可能なルールを確認します。各ルールでは、情報アイコンにカーソルを合わせると説明が表示されます。［オン］をクリックして、ルールグループ全体または特定のルールを有効にします。
6. デバイスでルールがトリガーされたときにデスクトップ通知を表示する場合は、ルールの［デバイスに検出通知を表示］チェックボックスをオンにします。
7. デバイスでルールがトリガーされたときに CylanceOPTICS エージェントに応答アクションを実行させるには、ルールの［応答］ドロップダウンリストで、1 つまたは複数のアクションを選択します。各アクションの説明は、情報アイコンにカーソルを合わせることで表示できます。
8. ［デバイスポリシー］ドロップダウンリストで、検出ルールセットを割り当てるデバイスポリシーを 1 つ以上クリックします。

   デバイスポリシーを作成または変更するときに、デバイスポリシーに検出ルールセットを割り当てることもできます。

9. ［確認］をクリックします。要約を確認して、再度［確認］をクリックします。

終了したら： 検出ルールセットをデバイスポリシーに割り当てた後、検出内容を表示および管理できます。次に挙げる任意のタスクを実行することもできます。

- 偽陽性や重複イベントを減らすために、検出例外を作成できます。
- カスタム検出ルールを作成します。
- イベントに対応するパッケージプレイブックの作成。

イベント応答

検出イベントがトリガーされると、CylanceOPTICS エージェントは次の応答アクションを実行できます。

応答	説明
アプリケーションログ	エージェントは検出イベントを Windows アプリケーションログに記録します。
ファイルの削除	エージェントは、関心アーチファクト（AOI）として識別されたファイルアーチファクトを完全に削除します。
レジストリキーの削除	エージェントは、レジストリアーチファクトとして識別されている AOI のレジストリキー全体を完全に削除します。
レジストリ値の削除	エージェントは、レジストリアーチファクトとして識別されている AOI のレジストリ値を完全に削除します。
検出結果のディスクへのダンプ	エージェントは CylanceOPTICS アプリケーションのデータディレクトリに検出データファイルを作成します。
すべてのユーザーをログオフ	エージェントは、すべてのインタラクティブおよびリモートユーザーをログオフにします。
ユーザーをログオフ	エージェントは指定されたユーザーをログオフします。
インタラクティブユーザーをログオフ	エージェントは、現在デバイスを物理的に操作しているすべてのユーザーをログオフします。
リモートユーザーをログオフ	エージェントは、現在システムでリモートセッションが確立されているすべてのユーザーをログオフします。
通知ウィンドウ	エージェントは、CylancePROTECT エージェントの代わりにネイティブな OS の通知ボックスを使用して、指定した検出通知メッセージを含む通知ウィンドウを表示します。
プロセスを一次停止	エージェントは、AOI として識別されたすべてのプロセスアーチファクトを一時停止します。
プロセスツリーを一時停止	エージェントは、AOI として識別されたすべてのプロセスアーチファクトのプロセスツリー全体を一時停止します。AOI がツリーのルートとして扱われます。

応答	説明
プロセスを終了	エージェントは、AOI として識別されたすべてのプロセスアーチファクトを終了します。
プロセスツリーを終了	エージェントは、AOI として識別されたすべてのプロセスアーチファクトのプロセスツリー全体を終了します。AOI がツリーのルートとして扱われます。
ホワイトリストプロセス	このオプションは、指定されたプロセスを CylanceOPTICS による監視から除外します。

検出の表示と管理

管理コンソールを使用して、CAE によって検出されたイベントを表示し分析できます。検出ダッシュボードから、各種時間枠におけるイベントの傾向およびさまざまな検出の重大度を確認でき、各検出の詳細情報にアクセスできます。

作業を始める前に： 検出ルールセットの作成。

1. 管理コンソールのメニューバーで、［**CylanceOPTICS**］ **>** ［検出］をクリックします。
2. 次のいずれかの操作を実行します。

タスク	手順
検出データの範囲を変更します。	［時間経過による検出］ドロップダウンリストで、目的の範囲を選択します。
異なる優先度レベルの検出を含めるか除外します。	グラフには、情報イベント、低優先度イベント、中優先度イベント、高優先度イベントの計数値が表示されます。検出データからイベントを除外するには、該当する計数値をクリックします。同じ項目を再度クリックすると、データに追加されます。
検出の詳細と関心アーチファクトを表示します。	［表示］をクリックします。 検出に関連付けられたアーチファクトに応じて、さまざまなアクションを選択できます（ファイルのダウンロード、ファイルの隔離、フォーカスデータの表示、検出例外の作成などを行えます）。［検出に関する注意］セクションをクリックして、分析に関連するメモを追加できます。
検出に関連付けられたデバイスをロックダウンします。	**a.** ［表示］をクリックします。 **b.** ［アクション］ドロップダウンリストで、［デバイスをロックダウン］をクリックします。 **c.** 「デバイスのロック」を参照してください。
検出の詳細を JSON ファイルにエクスポートします。	**a.** ［表示］をクリックします。 **b.** ［アクション］ドロップダウンリストで、［データをエクスポート］をクリックします。

タスク	手順
検出イベントのステータスを変更します。	次の操作のいずれかを実行します。 • 検出の［ステータス］ドロップダウンリストをクリックし、適切なステータスを選択します。 ［偽陽性］を選択すると、重複した検出の処理方法を確認するプロンプトが表示されます。適切なオプションを選択し、［保存］をクリックします。 • 1 つまたは複数の検出を選択し、［アクションを選択］ > ［ステータスを変更］をクリックします。適切なステータスを選択し、［確認］をクリックします。
1 つ以上の検出を削除します。	検出を選択し、［アクションを選択］ > ［検出を削除］をクリックします。［削除を確認］をクリックします。

カスタム検出ルールの作成

組織のセキュリティニーズと要件を満たすために、 CylanceOPTICS のルールエディターを使用して、管理コンソールで使用可能な検出ルールを複製して変更したり、独自のカスタム検出ルールを作成したりすることができます。コンテキスト分析エンジン（CAE）の柔軟性とロジックを使用して、疑わしい、または悪意のあるアクティビティを検出できます。これには、広範囲の行動特性（特定の命名パターンを使用するファイルなど）や一連のターゲットイベント（たとえば、ファイルを作成し、ネットワーク接続を開始する特定のファイル署名サムプリントを持つプロセス）などが含まれます。カスタム検出ルールは、 BlackBerry が提供する検出ルールと同じワークフローを使用するもので、カスタムルール用に自動応答アクション、ユーザー通知、およびパッケージプレイブックを設定できます。

ルールエディターは JSON を使用しており、組み込みの検証ツールを提供します。ルールを検証する際、エディターは構文をチェックして問題を識別します。ルールが構文チェックに合格すると、 CylanceOPTICS は CAE サービスを使用して、ルールがデバイス上でコンパイルおよび実行されることを確認します。いずれかの検証プロセスで問題が検出されると、修正する必要があるエラーに関する情報が提供されます。ルールが両方の検証チェックを通過すれば、ルールを公開して検出ルールセットに追加できます。

このセクションでは、独自の CAE ルールを作成するためのガイダンスと参照情報を提供します。CAE ルールでは、次のデータとフィルターがサポートされています。

項目	説明
状態	状態は CAE ルールのフローを定義し、 CylanceOPTICS がデバイスで発生する可能性のある一連のイベントをステートフルに監視できるようにします。状態は、「1、次に 2、次に 3」という発生の可能性があるシナリオを表します。
関数	関数は、状態を正常に満たすために必要なロジックを定義します。このロジックは、定義されたフィールド演算子に直接適用され、デバイス上で発生するイベントの属性を表します（たとえば、「A、および B、および C」または「A、および B、しかし C ではない」など）。

項目	説明
フィールド演算子	フィールド演算子は、オペランド（ファセット値エクストラクタ）の評価方法を定義します。フィールド演算子には、equals、contains、および is true のようなアクションが含まれます。
オペランド（ファセット値エクストラクタ）	オペランドは、 CylanceOPTICS が比較する値です。オペランドを使用することにより、イベントに関する特定のデータ（ファイルパス、ファイルハッシュ、プロセス名など）を抽出し、リテラル値（文字列、小数値、ブール値、整数など）と比較できます。
関心アーチファクト	関心アーチファクトは、 CylanceOPTICS が自動応答アクション（プロセスの終了、ユーザーのログオフ、ファイルの削除など）を実行するときにターゲットにできるアーチファクトを定義します。
パス	パスは、ルール内の複数の状態オブジェクトのフローを CAE が解釈する方法を定義します。
フィルター	フィルターは、分析するイベントの数を増減するために、対象とする状態を狭くするか、拡張します。

異常時には多数のイベントを生成する環境で（サーバーシステムやソフトウェアエンジニアリングシステムなど）、パフォーマンスの問題に対処するため、CAE は CylanceOPTICS データパイプラインから特定のイベントを除外するために使用できる除外ルールをサポートしています。CylanceOPTICS は除外されたイベントを分析または記録しません。管理コンソールで使用可能な事前定義済みの除外ルールを使用することも、ルールエディターを使用して、検出ルールと同じ JSON 構造を使用して独自の除外ルールを作成することもできます。除外ルールの目的は、除外するプロセスに基づいて、ルールを満たすことです。

除外ルールを公開すると、検出ルールセットのホワイトリストプロセス応答アクションにそのルールを関連付けることができます。この応答アクションでは、CAE は、関連付けられたルールロジックに一致するイベントとプロセスを自動的に除外します。除外ルールにより、 CylanceOPTICS デバイスの全体的なセキュリティが低下する可能性があるため、注意して使用してください。

サンプル検出ルール

CAE ルールの形式とオプションについては、次のトピックを参照してください。

- States
- 関数
- フィールド演算子
- オペランド（ファセット値エクストラクタ）
- 関心アーチファクト
- パス
- Filters

```
{
    "States": [
    {
        "Name": "TestFile",
        "Scope": "Global",
        "Function": "(a)",
```

```
        "FieldOperators": {
            "a": {
                "Type": "Contains",
                "Operands": [
                    {
                        "Source": "TargetFile",
                        "Data": "Path"
                    },
                    {
                        "Source": "Literal",
                        "Data": "my_test_file"
                    }
                ],
                "OperandType": "String"
                }
            },
            "ActivationTimeLimit": "-0:00:00.001",
            "Actions": [
                {
                    "Type": "AOI",
                    "ItemName": "InstigatingProcess",
                    "Position": "PostActivation"
                },
                {
                    "Type": "AOI",
                    "ItemName": "TargetProcess",
                    "Position": "PostActivation"
                },
                {
                    "Type": "AOI",
                    "ItemName": "TargetFile",
                    "Position": "PostActivation"
                }
            ],
            "HarvestContributingEvent": true,
            "Filters": [
                {
                    "Type": "Event",
                    "Data": {
                        "Category": "File",
                        "SubCategory": "",
                        "Type": "Create"
                    }
                }
            ]
        }
    ],
     "Paths": [
        {
            "StateNames": [
            "NewSuspiciousFile",
            "CertUtilDecode"
            ]
        }
    ],
    "Tags": [
        "CylanceOPTICS"
    ]
}
```

カスタム検出ルールの別の例については、「KB66651」を参照してください。

検出ルールおよび除外の作成と管理

作業を始める前に： 既存の検出ルールを複製して変更する場合、または独自のカスタムルールを作成する場合は、次のトピックおよびサンプル検出ルールを確認して、CAE ルールの形式とオプションを理解してください。

- 状態
- 関数
- フィールド演算子
- オペランド（ファセット値エクストラクタ）
- 関心アーチファクト
- パス
- Filters

1. 管理コンソールのメニューで、［**CylanceOPTICS**］ > ［設定］をクリックし、［ルール］タブをクリックします。
   使用可能な検出ルールを並べ替えてフィルタリングし、各ルールの情報を表示できます。
2. 次の操作のいずれかを実行します。

タスク	手順
ルールを .json ファイルにエクスポートします。	検出ルールは、次のいずれかのルールカテゴリからエクスポートできます：カスタム、Cylance 試験的、Cylance 除外、Cylance macOS 公式、Cylance Windows 公式。 ルールに対して をクリックします。
カスタム検出ルールを .json ファイルからインポートします。	**a.** ［ルールをインポート］をクリックします。 **b.** .json ファイルを参照して選択するか、ドラッグアンドドロップします。［インポート］をクリックします。 **c.** 必要に応じて、ルールの設定と構文を変更します。 **d.** ［検証］をクリックします。 **e.** ［公開］をクリックします。 公開後にカスタムルールを編集するには、そのルールの をクリックします。
検出ルールを複製して変更します。	検出ルールは、次のいずれかのルールカテゴリから複製できます：カスタム、Cylance 試験的、Cylance 除外、Cylance macOS 公式、Cylance Windows 公式。 **a.** ルールに対して をクリックします。 **b.** 必要に応じて、ルールの設定と構文を変更します。 **c.** ［検証］をクリックします。 **d.** ［公開］をクリックします。

タスク	手順
カスタムルールを削除します。	ルールはカスタムカテゴリからのみ削除できます。 **a.** ルールに対して をクリックします。 **b.** ［削除を確認］をクリックします。

States

状態は、CAE ルールの最上位の論理レベルであり、多くの必須フィールドがあります。

フィールド名	説明
アクション	このフィールドには、状態内で関心のあるアーチファクトを定義するために使用されるオブジェクトのリストが含まれます。詳細については、「関心アーチファクト」を参照してください。
ActivationTimeLimit	このフィールドでは、イベントをトリガーするイベントを CylanceOPTICS が待つ時間を定義します。推奨されるデフォルト値は -0:00:00:001 です。
FieldOperators	このフィールドには、状態で定義された関数を満たすために検査する必要があるフィールド演算子とオペランドが含まれます。詳細については、「フィールド演算子」を参照してください。
Filters	このフィールドでは、ある状態を満たそうとするときに CylanceOPTICS が検査する必要があるイベントカテゴリ、サブカテゴリ、タイプを定義します。詳細については、「フィルター」を参照してください。
Function	このフィールドには、状態が満たされると見なすために CylanceOPTICS が監視しなければならない論理関数が含まれます。詳細については、「関数」を参照してください。
HarvestContributingEvents	このフィールドは、状態を満たすイベントを CylanceOPTICS が記録するかどうかを定義します。推奨値は、true です。
Name	このフィールドは、ルールが満たされた場合に UI に表示される状態の名前を定義します。
Scope	このフィールドは、関連するイベントを CylanceOPTICS が探す範囲を定義します。ほとんどの場合、推奨値は global です。
States	このフィールドには、1 つまたは複数の状態オブジェクトのリストが含まれます。これらのオブジェクトは、連結することができます。

関数

関数は、CAE ルールの状態を満たすために必要なロジックを定義します。このロジックは、定義したフィールド演算子に直接適用され、デバイスで発生するイベントの「A かつ B かつ C」または「A かつ B だが C ではない」

という属性を表すために使用されます。このロジックは、状態内の定義済みフィールド演算子に直接適用されます。

Function	説明	例
AND - &	状態を満たすには、複数のフィールド演算子と一致する必要があります。	a & b & c
OR - |	状態を満たすには、複数のフィールド演算子の 1 つと一致する必要があります。	a | b | c
NOT - !	状態を満たすには、定義されたフィールド演算子が false であるか、または一致しない必要があります。	a & b & !c
GROUP - ()	フィールド演算子は、より複雑なロジック要件を満たすためにグループ化されます。	(a & b) | (c & !d)

フィールド演算子

フィールド演算子は、CylanceOPTICS が 2 つの値を比較する際のルールの論理的な部分です。オペランドが 2 つ以上のあり、それらが比較条件に一致する場合、CylanceOPTICS は定義された関数のその部分を完全であると見なします。関数のすべての部分が完全になると、状態は満たされます。

フィールド演算子フィールドは、1 つ以上の条件付きオブジェクトで構成されるオブジェクトです。これらの条件付きオブジェクトは任意の値に設定できますが、関数フィールドで参照されている条件付きの値と一致する必要があります。BlackBerry では、これらの名前は、数字や文字など、シンプルで、論理的な値に保つことをお勧めします。

フィールド演算子	説明
Base64Encoding Base64	このフィールド演算子は文字列をトークン化し、いずれかのトークンがオペランドと一致するかどうかを判断します。また、文字列エンコーディングのタイプ（ASCII、UTF-7、UTF-8、UTF-16-LE、UTF-16-BE、UTF-32-LE、UTF-32-BE）も特定しようとします。BOM がない場合は、UTF-8、UTF-16-LE、および UTF-16-BE のみを確実に検出できます。すべての検出に失敗した場合は、デフォルトでシステムのデフォルトのコードページに設定されます。 正：`powershell.exe -ex bypass -e "ZwBlAHQALQBwAHIAbwBjAGUAcwBzAA==" equals ("get-process", )` 負：`powershell.exe -ex bypass "ZwBlAHQALQBhAGwAaQBhAHMA" does not contain ("get-process", )`

フィールド演算子	説明
ContainsAll	このフィールド演算子は、指定したオペランドにセットのすべてのオペランドが含まれているかどうかを判断します。 正："hello, I am a string" には、セット（「ello」、「ng」）のすべての文字列が含まれている 負："hello, I am a string" には、セット（「hi」、「ng」）のすべての文字列は含まれていない
ContainsAllWords	このフィールド演算子は、指定したオペランドにセットのすべてのオペランドが含まれているかどうかを判断します。セットの各オペランドは、空白、句読点、または文字列の終了マーカーあるいは開始マーカーで囲まれた単語として示されている必要があります。 正："hello, I am a string" には、セット（「hello」、「a」、「string」）のすべてが単語として含まれている 負："hello, I am a string" には、セット（「ello」、「ng」）のすべてが単語として含まれていない
ContainsAny 次の値を含む	このフィールド演算子は、指定したオペランドにセットのいずれかのオペランドが含まれているかどうかを判断します。 正："hello, I am a string" には、セット（「ello」、「banana」）のいずれかの文字列が含まれている 負："hello, I am a string" には、セット（「hi」、「banana」）のどの文字列も含まれていない
ContainsAnyWord ContainsWord	このフィールド演算子は、指定されたオペランドにセットのいずれかのオペランドが含まれているかどうかを判断します。この場合、セットの各オペランドは、空白、句読点、または文字列の終了マーカーあるいは開始マーカーで囲まれた単語として示されている必要があります。 正："hello, I am a string" には、セット（「hello」、「banana」）のいずれかの単語が含まれている 負："hello, I am a string" には、セット（「ello」、「ng」）のいずれかが単語として含まれていない
DamerauLevenshteinDistance DLDistance	このフィールド演算子は、距離（あるオペランドを別のオペランドに変換するために必要な変更の数）が許容範囲内かどうかを判断しますが、隣接する記号の転置は許容します。 正：「cat」と「bat」のダメラウレーベンシュタイン距離は 1 以内 正：「hello」と「bell」のダメラウレーベンシュタイン距離は 2 以内 正：「ca」と「abc」のダメラウレーベンシュタイン距離は 3 以内 負：「cart」と「act」のダメラウレーベンシュタイン距離は 1 以内にはない

フィールド演算子	説明
DiceCoefficient Dice	このフィールド演算子は、2 組の文字列の類似性を、共通のバイグラム（文字列内の隣接する文字のペア）の数で判断します。比較の結果が「mincoefficient」と「maxcoefficient」の間にあるかどうかを判断します。 たとえば、プロセス名「Test.exe」と「Tes.exe」を比較すると、0.76923076923076927 が返されます。 「round」を 2 に設定した場合： 正：最小 0.5 < 0.77 < 0.8 最大（含まれない） 正：最小 0.77 <= 0.77 <= 0.77 最大（含まれる） 負：最小 0.8 < 0.77 < 0.85 最大（含まれない） 「round」オプションを指定すると、小数点以下の桁が指定した整数に丸められます。たとえば、「round」が 2 に設定されている場合、.6666666667 は .67 になります。
EndsWithAny EndsWith	このフィールド演算子は、指定した左オペランドが指定した右オペランドで終わっているかどうかを判断します。 正："hello, I am a string" は「ring」で終わっている 負："hello, I am a string" は「bring」で終わっていない
EqualsAny Equals	このフィールド演算子は、指定されたオペランドとセットのオペランドのいずれかが正確に等しいかどうかを判断します。この場合、セットの各オペランドは、数値であるか、空白、句読点、または文字列の終了マーカーあるいは開始マーカーで囲まれた単語として示されている必要があります。 正： 10 はセット（10、20、30）のうちのいずれかの数値と等しい 正："hello" はセット（「hello」、「banana」）のいずれかと等しい 負：100 はセット（10、20、30）のいずれの数値とも等しくない 負："hello" はセット（「ello」、「ng」）のいずれとも等しくない
GreaterThan	このフィールド演算子は、指定した左オペランドが指定した右オペランドより大きいかどうかを判断します。 正： 14.4 は 10.1 より大きい 負： 1 は 1000 より大きくない
GreaterThanOrEquals	このフィールド演算子は、指定した左オペランドが指定した右オペランドと等しいまたは大きい（以上）かどうかを判断します。 正： 14.4 は 10.1 と等しいか大きい 負：1 は 1000 と等しいか大きくない

フィールド演算子	説明
HammingDistance	このフィールド演算子は、等しい長さの 2 つの文字列間の距離を判断します。これは、対応する記号が異なる位置の数です。1 つの文字列をもう 1 つの文字列に変更するために必要な置換の最小数を測定します。 正：「cat」と「bat」のハミング距離は 1 以内 • cat → bat(1) 正：「hello」と「bell」のハミング距離は 2 以内 • hello → bello(1) → bell(2) 正：「ca」と「abc」のハミング距離は 3 以内 • ca → aa(1) → ab(2) → abc(3) 負：「cart」と「act」のハミング距離は 4 以内にはない • cart → aart(1) → acrt(2) → actt(3) → act(4)
HexEncoding	このフィールド演算子は文字列をトークン化し、いずれかのトークンがオペランドと一致するかどうかを判断します。また、文字列エンコーディングのタイプ（ASCII、UTF-7、UTF-8、UTF-16-LE、UTF-16-BE、UTF-32-LE、UTF-32-BE）も特定しようとします。BOM がない場合は、UTF-8、UTF-16-LE、および UTF-16-BE のみを確実に検出できます。すべての検出に失敗した場合は、デフォルトでシステムのデフォルトのコードページに設定されます。 正：「74657374」に「test」が含まれている 負：「696e76616c6964」に「test」が含まれていない
InRange	このフィールド演算子は、指定された中間オペランドが左オペランドと右オペランドの間にあるかどうかを判断します。 正：10 は 1〜20 の範囲に入る 正：5.3 は 5.3〜20.1 の範囲に入る（両端を含む場合） 負：4 は 5〜10 の範囲に入らない 負：20 は 20〜40 の範囲に入らない（両端を含まない場合）

フィールド演算子	説明

IpIsInRange
IpRange
	このフィールド演算子は、TargetNetworkConnection アドレス（Sourceaddress、DestinationAddress）が、指定された「min」（最小値）および「max」（最大値）オプションの範囲内にあるかどうかを判断します。
	許可されるオペランドは次のとおりです。
	`{ "Source": "TargetNetworkConnection", "Data": "SourceAddress" }`
	および
	`{ "Source": "TargetNetworkConnection", "Data": "DestinationAddress" }`
	例:
	`"FieldOperators": { "a": { "Type": "IpIsInRange", "OperandType": "IPAddres", "Options": { "min": "123.45.67.89", "max": "123.45.67.255" }, "Operands": [ { "Source": "TargetNetworkConnection", "Data": "DestAddr" } ] } }`
	ネットワークトラフィックを出力するには、次のフィルターオブジェクトを上記の例に当てはめます。
	`"Filters": [ { "Type": "Event", "Data": { "Category": "Network", "SubCategory": "*", "Type": "Connect" } } ]`

フィールド演算子	説明
IsFlagSet	このフィールド演算子は、ビットマスクの 1 つまたは複数のビットが設定されているかどうかをチェックします。比較値には、base-10 または base-16（「0x」プレフィックスを使用）を使用できます。 正：0x10 は 0x4111 に対して設定されている 正： 3 は 0x7 に対して設定されている 負：0x3 は 0x4 に対して設定されていない 負：2 は 0x5 に対して設定されていない
IsHomoglyph	このフィールド演算子は、左のオペランドが右のオペランドのホモグリフかどうかを判断します。たとえば、US Latin 1 の「e」とフランス語の「e」の文字は同じものに見え、意味も同じですが、値は異なります。 正："3xplor3" は 100% の確度で "explore" のホモグリフである 正："3xplord" は 90% の確度で "explore" のホモグリフである 負："temp" と "temp" は全く同じ文字列であるため、ホモグリフとは見なされない 負："431" と "big" は、両者の間をつなぐ共通の特性がないため、ホモグリフとは見なされない
IsNullOrEmpty	このフィールド演算子は、指定したオペランドが null か空かを判断します。 正：<null> は null または空 正："" は null または空 正：" " は null または空 負："Hello" は null でも空でもない
IsPopulated Exists HasContent	このフィールド演算子は、指定したオペランドが null でも空でもないかを判断します。 正："Hello" は null でも空でもない 負：<null> は null または空 負："" は null または空 負：" " は null または空
IsTrue	このフィールド演算子は、指定された値が真（true）かどうかを判断します。 正：TriState.True 負：TriState.False 負：TriState.Unknown

フィールド演算子	説明
LessThan	このフィールド演算子は、指定した左オペランドが指定した右オペランドより小さいかどうかを判断します。 正： 4.4 は 10.1 より小さい 負： 1000 は 1 より小さくない
LessThanOrEquals	このフィールド演算子は、指定した左オペランドが指定した右オペランドと等しいまたは小さい（以下）かどうかを判断します。 正：4.4 は 10.1 より小さいか等しい 正：14 は 14 より小さいか等しい 負：1000 は 1 より小さくも等しくもない
LevenshteinDistance	このフィールド演算子は、あるオペランドを別のオペランドに変換するために必要な変更の数を距離と見なして、それが許容範囲内かどうかを判断します。 正："cat" と "bat" のレーベンシュタイン距離は 1 以内 正："hello" と "bell" のレーベンシュタイン距離は 3 以内 負："cart" と "act" のレーベンシュタイン距離は 1 以内にはない
LongestCommonSubsequence	このフィールド演算子は、固定の左オペランドと一連の右オペランドを比較し、各比較における最長のサブシーケンスを特定します。結果の数を最小値および最大値と比較して、結果が許容範囲内かどうかを判断します。 「aggtab」と「gxtxayb」の比較： 正：「gtab」は最も長いシーケンス。最小値が 1 で最大値が 10 の場合、これは許容範囲内になります。 負：前の例を使用して、最小値が 5 で最大値が 10 の場合、これは許容範囲内になりません。
LongestCommonSubstring	このフィールド演算子は、左と右のオペランドを比較し、検出された最長のサブ文字列の数を返します。 「ababc」と「abcdaba」の比較： 正：「aba」と「abc」は「abcdaba」の同じサイズの 2 つの結果であり、最長のサブ文字列として 3 を返します。 負：mindistance と maxdistance が 4 に設定されている場合、これは検出された最長のサブ文字列よりも大きくなります。 「ababcd」と「abcdaba」の比較： 正：「abcd」は、検出された最長のサブ文字列。

フィールド演算子	説明
MatchOnFilter NoOp	このフィールド演算子は、操作が実行されていないこと、およびフィルターが対応するイベントを検出した場合に状態が単純に一致することを示します。
RegexMatches	このフィールド演算子は、指定したオペランドが正規表現に一致しているかを判断します。 正："hello, I am a string" は "^hello, [Ii] am [aA] string$" と一致する 負："hello, I am a string" は "^[hi\|hey], I am a string$" と一致していない
ShannonEntropy	このフィールド演算子は、1 つのオペランドを比較するときに状態の予測不可能性の測定値、つまり平均情報量を特定します。 正：「abc」が 1.5849625007211561 と計算され、1.55 と 1.6 の範囲内にある。 負：「Z2V0LXByb2Nlc3M=」が 3.875 と計算され、1.55 と 1.6 の範囲内にない。
StartsWithAny StartsWith	このフィールド演算子は、指定した左オペランドが指定した右オペランドで始まっているかどうかを判断します。 正："hello, I am a string" は "hello, I" で始まっている 負："hello, I am a string" は "help" で始まっていない

オペランド（ファセット値エクストラクタ）

CylanceOPTICS CAE はファセット値エクストラクタを使用して、CylanceOPTICS によって観察されたイベントに関連付けられた単一アーチファクトの個々のプロパティ（ファセット）を識別します。ファセット値エクストラクタの対応範囲は単体では狭いものの、個々のエクストラクタを論理的に連結することで、デバイス上で発生している複雑な行動を分析し、検出イベントをトリガーすることができます。

エクストラクタ名	説明	サポートされるファセット
InstigatingProcess	このエクストラクタは、イベントの扇動プロセスからファセットを抽出します。通常、アクション（別のプロセスの開始、ネットワーク接続の開始、ファイルの書き込みなど）を開始しているプロセスの名前またはコマンドライン引数を検査するために使用されます。	Name（String） CommandLine（String）

エクストラクタ名	説明	サポートされるファセット	
InstigatingProcessImageFile	このエクストラクタは、イベントの扇動プロセスに関連付けられているイメージファイルからファセットを抽出します。通常、イメージファイルのさまざまな属性（名前、パス、ハッシュ、署名ステータスなど）を検査するために使用されます。	Path (String) Size (Integer) Md5Hash (String) Sha256Hash (String) IsHidden (Boolean) IsReadOnly (Boolean) Directory (String) SuspectedFileType (String) SignatureStatus (String) IsSelfSigned (Boolean) LeafDNSString (String) LeafThumbprint (String) LeafSignatureAlgorithm (String) LeafCN (String) LeafDN (String) LeafOU (String) LeafO (String) LeafL (String) LeafC (String)	IssuerDNString (String) IssuerThumbprint (String) IssuerSignatureAlgorithm (String) IssuerCN (String) IssuerDN (String) IssuerOU (String) IssuerO (String) IssuerL (String) IssuerC (String) RootDNString (String) RootThumbprint (String) RootSignatureAlgorithm (String) RootCN (String) RootDN (String) RootOU (String) RootO (String) RootL (String) RootC (String)
InstigatingProcessOwner	このエクストラクタは、イベントの扇動プロセスに関連付けられている所有者からファセットを抽出します。通常、プロセスを所有するユーザーを検査するために使用されます。	Name（String） Domain（String）	

エクストラクタ名	説明	サポートされるファセット
TargetFile	このエクストラクタは、イベントが発生したファイルからファセットを抽出します。通常、ファイルのさまざまな属性（名前、パス、ハッシュ、署名ステータスなど）を検査するために使用されます。	上記の「InstigatingProcessImageFile」を参照してください。
TargetFileOwner	このエクストラクタは、イベントが発生したファイルに関連付けられている所有者からファセットを抽出します。通常、ファイルを所有するユーザーを検査するために使用されます。	上記の「InstigatingProcessOwner」を参照してください。
TargetNetworkConnection	このエクストラクタは、イベントが発生したネットワーク接続からファセットを抽出します。通常、ネットワーク IP アドレスまたは処理対象ポートを検査するために使用されます。	SourceAddress（IPAddress） SourcePort（Integer） DestinationAddress（IPAddress） DestinationPort（Integer）
TargetProcess	このエクストラクタは、イベントが発生したプロセスからファセットを抽出します。通常、処理対象プロセスの名前またはコマンドライン引数を検査するために使用されます。	上記の「InstigatingProcess」を参照してください。

エクストラクタ名	説明	サポートされるファセット
TargetProcessImageFile	このエクストラクタは、イベントが発生したプロセスに関連付けられているイメージファイルからファセットを抽出します。通常、イメージファイルの属性（名前、パス、ハッシュ、署名ステータスなど）を検査するために使用されます。	上記の「InstigatingProcessImageFile」を参照してください。
TargetProcessOwner	このエクストラクタは、イベントが発生したプロセスに関連付けられている所有者からファセットを抽出します。通常、処理対象プロセスを所有するユーザーを検査するために使用されます。	上記の「InstigatingProcessOwner」を参照してください。
TargetRegistryKey	このエクストラクタは、イベントが発生したレジストリキーからファセットを抽出します。通常、処理対象レジストリのキーまたは値を検査するために使用されます。	Path（String） ValueName（String）

パス値エクストラクタ

エクストラクタ名	説明
EnvVar	EnvVar は、OS から環境変数を抽出します。
LiteralWithEnvVar	LiteralWithEnvVar は、環境変数を含むパスを展開します。
Literal	Literal はリテラル値を表し、最も一般的なエクストラクタおよびオペランドです。

関心アーチファクト

アクションフィールドの関心アーチファクト（AOI）を使用して、CylanceOPTICS が自動応答アクションの実行対象にできるアーチファクトのリストを定義できます。AOI はオペランドと同じ構文に従います。状態を満たすイベントまたはイベントセットに関連付けられたアーチファクトはすべて AOI としてマークできます。AOI は、AOI と見なされるためにオペランドとして定義する必要はありません。

フィルターが状態に適用されている場合、一部の AOI は自動応答アクションの対象にできないことに注意してください。たとえば、ファイル作成フィルターが状態に適用されている場合、ファイルやプロセス関連の AOI が使用可能になりますが、レジストリやネットワーク関連の AOI はありません。関係のない AOI が状態で提供された場合、CylanceOPTICS エージェントはその除外を適切に処理します。以下の表に、AOI 関係に適用可能なフィルターの概要を示します。

カテゴリ	サブカテゴリ	種類	適用可能な **AOI**
ファイル	—	Create	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetFile TargetFileOwner
ファイル	—	Delete	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetFile TargetFileOwner
ファイル	—	Rename	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetFile TargetFileOwner
ファイル	—	Write	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetFile TargetFileOwner
ネットワーク	IPv4	Connect	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetNetworkConnection
ネットワーク	IPv6	Connect	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetNetworkConnection

カテゴリ	サブカテゴリ	種類	適用可能な **AOI**
ネットワーク	TCP	Connect	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetNetworkConnection
ネットワーク	UDP	Connect	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetNetworkConnection
プロセス	—	Exit	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetProcess TargetProcessImageFile TargetProcessOwner
プロセス	—	Start	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetProcess TargetProcessImageFile TargetProcessOwner
プロセス	CylancePROTECT Desktop	AbnormalExit	TargetProcess TargetProcessImageFile TargetProcessOwner
レジストリ	—	PersistencePoint: KeyCreating	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetRegistryKey
レジストリ	—	PersistencePoint: KeyCreated	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetRegistryKey

カテゴリ	サブカテゴリ	種類	適用可能な **AOI**
レジストリ	—	PersistencePoint: KeyDeleting	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetRegistryKey
レジストリ	—	PersistencePoint: KeyDeleted	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetRegistryKey
レジストリ	—	PersistencePoint: KeyRenaming	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetRegistryKey
レジストリ	—	PersistencePoint: KeyRenamed	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetRegistryKey
レジストリ	—	PersistencePoint: ValueChanging	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetRegistryKey
レジストリ	—	PersistencePoint: ValueChanged	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetRegistryKey
レジストリ	—	PersistencePoint: ValueDeleting	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetRegistryKey

カテゴリ	サブカテゴリ	種類	適用可能な **AOI**
レジストリ	—	PersistencePoint: ValueDeleted	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetRegistryKey
スレッド	—	Create	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetProcess TargetProcessImageFile TargetProcessOwner
スレッド	—	Inject	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetProcess TargetProcessImageFile TargetProcessOwner

例:

```
"Actions": [
    {
        "Type": "AOI",
        "ItemName": "InstigatingProcess",
        "Position": "PostActivation"
    },
    {
        "Type": "AOI",
        "ItemName": "TargetProcess",
        "Position": "PostActivation"
    },
    {
        "Type": "AOI",
        "ItemName": "InstigatingProcessOwner",
        "Position": "PostActivation"
    }
],
```

パス

パスは、ルール内の複数の状態オブジェクトのフローを CAE が解釈する方法を定義します。パスは、ルールが複数の状態オブジェクトで構成される（複数状態ルールとも呼ばれる）場合に使用します。状態は CAE ルールのフローを定義し、デバイスで発生する一連のイベントを、CylanceOPTICS が状態を追って監視できるようにします。それぞれは、「1、次に2、次に3」という発生の可能性があるシナリオを表します。

ルールに状態オブジェクトが 1 つしかない場合、Paths オブジェクトを使用する必要はありません。ルールは単一の状態オブジェクトで構成され、Paths オブジェクトの使用を明示的には必要としません。Paths オブジェクトを使用するルールは、明示的な定義のためにのみ Paths オブジェクトを必要とします（ルールの機能のためではありません）。

次の例では、2 つの状態オブジェクト（NewSuspiciousFile と CertUtilDecode）が使用されます。各状態には、それ自身のロジックセットがあります。

例 **1**：次の設定では、CAE は NewSuspiciousFile 状態を満たすイベントを探します。この状態が満たされると、CAE は CertUtilDecode 状態を満たすイベントを探します。

```
"Paths": [
    {
        "StateNames": [
            "NewSuspiciousFile",
            "CertUtilDecode"
        ]
    }
],
```

例 **2**：次の設定では、CAE は CertUtilDecode 状態を満たすイベントを探し、続いて NewSuspiciousFile 状態を探します。

```
"Paths": [
    {
        "StateNames": [
            "CertUtilDecode",
            "NewSuspiciousFile"
        ]
    }
],
```

例 **3**：次の設定では、CAE は NewSuspiciousFile 状態か CertUtilDecodee 状態を満たすイベントを探します。これは、状態に異なるフィルターオブジェクトのセットがある場合に役立ちます。この例では、NewSuspiciousFile はファイル書き込みフィルターを使用し、CertUtilDecode はプロセス開始フィルターを使用します。

```
"Paths": [
    {
        "StateNames": [
            "CertUtilDecode"
        ]
    },
    {
        "StateNames": [
            "NewSuspiciousFile"
        ]
    }
],
```

フィルター

フィルターを使用して、分析するイベントの数を増減して、状態の範囲を絞り込む、または広げることができます。イベントフィルターは、「脅威を識別するために CylanceOPTICS が使用するデータ構造」の説明と同じイベントカテゴリ、サブカテゴリ、およびタイプを使用します。

例 **1**： 次の例では、検査するイベントを開始イベントの処理に制限します。

```
"Filters": [
    {
        "Type": "Event",
        "Data": {
            "Category": "Process",
            "SubCategory": "",
            "Type": "Start"
        }
    }
]
```

例 **2** ： 次の例では、すべてのタイプのファイルイベント（作成、書き込み、削除）を検査します。

```
"Filters": [
    {
        "Type": "Event",
        "Data": {
            "Category": "File",
            "SubCategory": "",
            "Type": "*"
        }
    }
]
```

検出例外の作成

検出結果の偽陽性や重複イベントを減らすため、検出ルールの例外を作成できます。検出例外を作成すると、指定されたプロセスは CylanceOPTICS 検出エンジンで評価されません。検出例外を作成する場合は、デバイスの全体的なセキュリティを低下させる可能性があるため、注意してください。

メモ： RegEx 一致のみを条件に使用するルール例外を作成して有効にすると、イベントごとにルール例外が実行されるため、一部のシステムで多数のイベントが発生し、CPU 使用率が通常よりも高くなることがあります。この問題が発生した場合、BlackBerry では、条件に RegEx 一致を使用するルール例外を無効にすることをお勧めします。

1. 管理コンソールのメニューバーで、［**CylanceOPTICS**］ **>** ［設定］をクリックします。
2. ［例外］タブで、［例外を作成］をクリックします。
3. 検出例外の名前を入力します。
4. ［条件］セクションで、例外条件を設定します。［別の条件を追加］をクリックして、追加の例外を設定します。

   検出例外では、AND ステートメントがすべての条件に適用されます。例外が true になるには、すべての条件を満たす必要があります。条件の値を指定すると、その値は ANY ステートメントとして処理されます。2 つ以上の値が追加された場合、いずれかの値が存在すると、条件は true になります。
5. ［保存］をクリックします。

終了したら： メニューバーで、［**CylanceOPTICS**］ **>** ［設定］をクリックし、［ルールセット］タブをクリックします。検出ルールセットを編集し、検出例外を目的のルールに割り当てます。［確認］をクリックします。

デバイスからデータを収集するパッケージの展開

CylanceOPTICS のパッケージ展開機能を使用すると、CylanceOPTICS デバイス上でプロセス（Python スクリプトなど）をリモートかつ安全に実行して必要なデータを収集し、指定された場所に保存して、セキュリティ管理者による詳細な分析を行うことができます。たとえば、ブラウザーデータを収集するプロセスを実行できます。管理コンソールで使用可能な CylanceOPTICS データ収集パッケージを使用することも、独自のデータ収集パッケージを作成することもできます。

オフラインのデバイスにパッケージを展開する場合、それらのデバイスがオンラインになるのを指定された期間だけ待機してから展開します。

作業を始める前に：

- 必要に応じて、デバイス上で実行するパッケージを作成し、特定のデータポイントを収集し、以下の手順で指定するローカルまたはサーバーの場所にデータを出力します。カスタムパッケージの作成の詳細については、support.blackberry.com/community にアクセスして、記事 66563 を参照してください。
- 独自のパッケージを作成する場合は、パッケージを管理コンソールにアップロードする必要があります。コンソールで、［**CylanceOPTICS**］ > ［設定］ > ［パッケージ］を選択し、［ファイルをアップロード］をクリックします。

1. 管理コンソールのメニューバーで［**CylanceOPTICS**］ > ［パッケージ］をクリックします。
2. ［パッケージを展開］をクリックします。
3. ［パッケージ］ドロップダウンリストで、デバイスに送信するパッケージをクリックします。別のパッケージを追加する場合には、［別のパッケージを追加］をクリックします。
4. ［コレクションタイプ］ドロップダウンリストで、パッケージが収集するデータを保存する場所をクリックします。
   - ［ローカル］は、デバイス上の指定されたパスにデータを保存します。
   - ［**SFTP**］、［**SMB**］、または［**S3**］を選択した場合は、必要な情報を指定します。
5. ［次へ］をクリックします。
6. ［デバイス］または［ゾーン］を選択し、パッケージの配信先となるデバイスまたはゾーンを選択します。
7. パッケージ展開のタイムアウト期間と優先度を指定する場合は、［詳細オプションを表示］をクリックして、次のいずれかの操作を行います。
   - ［有効期限］ドロップダウンリストで、目的のタイムアウト期間をクリックします。この期間内にデバイスがオンラインにならない場合、そのデバイスのパッケージ展開はキャンセルされます。
   - ［優先度］スライダを調整して、優先度を高くまたは低く設定します。優先度は、同じデバイスで他の CylanceOPTICS ジョブがキューに入っている場合に考慮されます。
8. パッケージ展開の名前と説明を指定します。
9. ［展開］をクリックします。

終了したら：

- ［**CylanceOPTICS**］ > ［パッケージ］に移動し、パッケージ展開の現在のステータスと進行状況を表示します。
- パッケージ展開ステータスをクリックすると、展開の詳細を表示できます。［ターゲット］セクションを展開すると、各デバイスの個々のステータスを表示できます。進行中のパッケージ展開を停止する場合は、［アクションを選択］ドロップダウンリストで［ジョブを停止］をクリックします。

イベントに対応するパッケージプレイブックの作成

デバイスでセキュリティインシデントが発生した場合、パッケージプレイブックを作成することで、応答時間を最小限に抑えることができます。パッケージプレイブックを使用すると、検出ルールセットで設定した Context Analysis Engine（CAE）ルールがイベントによってトリガーされた場合に、refract パッケージの実行を自動化できます。

パッケージプレイブックは、Python の refract パッケージのみをサポートしています。管理コンソールで使用できる事前定義済みの refract パッケージを使用することも、独自のカスタム refract パッケージを追加することもできます。パッケージプレイブックの内容はデバイスに保存されるため、デバイスがオフラインの場合でも実行できます。パッケージプレイブックは 100 件まで作成できます。

作業を始める前に：

- 検出ルールセットの作成。
- 必要に応じて、検出ルールがトリガーされたときにデバイスで実行できる Python refract パッケージを作成します。カスタムパッケージの作成の詳細については、「KB 66563」を参照してください。
- 独自のパッケージを作成する場合は、パッケージを管理コンソールにアップロードする必要があります。コンソールで、［**CylanceOPTICS**］**>**［設定］**>**［パッケージ］を選択し、［ファイルをアップロード］をクリックします。

1. 管理コンソールのメニューバーで、［**CylanceOPTICS**］**>**［設定］をクリックし、［プレイブック］タブをクリックします。
2. ［プレイブックを作成］をクリックします。

   既存のパッケージプレイブックのクローンを作成する場合、目的のプレイブックのリストに必要なプレイブックを指定し、 をクリックします。
3. 名前と説明を入力します。
4. ［コレクションタイプ］ドロップダウンリストで、パッケージが収集するデータを保存する場所をクリックします。
   - ［ローカル］は、デバイス上の指定されたパスにデータを保存します。
   - ［**SFTP**］、［**SMB**］、または［**S3**］を選択した場合は、必要な情報を指定します。
5. ［次へ］をクリックします。
6. ［パッケージ］ドロップダウンリストで、パッケージプレイブックに含めるパッケージをクリックします。必要に応じて、オプションのコマンドライン引数を指定します。
7. 別のパッケージを追加する場合には、［別のパッケージを追加］をクリックします。1 件のパッケージプレイブックには最大で 20 のパッケージを追加できます。
8. ［保存］をクリックします。

終了したら：メニューバーで、［**CylanceOPTICS**］**>**［設定］**>**［ルールセット］をクリックします。検出ルールセットを編集し、パッケージプレイブックを目的のルールに割り当てます。［確認］をクリックします。それぞれの検出ルールには、最大 10 件のパッケージプレイブックを関連付けることができます。

デバイスのロック

感染しているか、感染している可能性のあるデバイスをロックして、コマンドおよび制御操作、データの窃盗、マルウェアの横移動を停止できます。ロックダウンの選択肢は次のとおりです。

ロックダウンタイプ	説明
完全ロックダウン（全プラットフォーム）	デバイスからのネットワーク通信をすべて禁止します。デバイスは、最大 96 時間ロックできます。ロック解除キーを使用することで、ロックダウン期間が終了する前にデバイスのロックを解除できます。
部分ロックダウン（Windows 用の CylanceOPTICS エージェント 3.1 以降のみ）	デバイスの LAN および Wi-Fi ネットワーク機能を無効にし、CylanceOPTICS クラウドサービスとの通信を維持することで、CylanceOPTICS による検出とセンサデータの受信は継続できるようにします。部分ロックダウンは、無期限に持続されます。ロック解除キーまたはリモートロック解除機能を使用することで、デバイスはいつでもロックを解除できます。
カスタマイズされた部分ロックダウン（Windows 用の CylanceOPTICS エージェント 3.2.1140 以降のみ）	このオプションは部分ロックダウンと同じですが、部分ロックダウン中に許可する追加の通信チャネルを指定することもできます。

作業を始める前に：

- Linux のロックダウン機能をサポートするための要件については、「CylanceOPTICS の要件」を参照してください。
- カスタマイズした部分ロックダウンを使用する場合は、メニューバーで、［設定］ > ［検出と応答］ > ［新しい設定を追加］をクリックします。部分ロックダウン中に許可する通信チャネルの名前、説明や、IP アドレス、ポート、および動作（インバウンド、アウトバウンド、双方向）を指定します。［保存］をクリックします。

1. 管理コンソールのメニューバーで、［**CylanceOPTICS**］ > ［デバイス］をクリックします。
2. デバイス名をクリックします。
3. 次の操作のいずれかを実行します。

タスク	手順
デバイスを完全にロックする（全プラットフォーム）	**a.** ［アクションを選択］ドロップダウンリストで、［ロックダウン］をクリックします。 **b.** Windows デバイスの場合は、ドロップダウンリストで、［完全ロックダウン］をクリックします。 **c.** ロックダウン期間を選択します。 **d.** ［ロックダウンを確認］をクリックします。

タスク	手順
デバイスを部分的にロックする（Windows 用の CylanceOPTICS エージェント 3.1 以降のみ）	**a.** ［アクションを選択］ドロップダウンリストで、［ロックダウン］をクリックします。 **b.** ドロップダウンリストで、次のいずれかを実行します。 • デフォルトの部分ロックダウン設定を使用するには、［部分ロックダウン］をクリックします。 • カスタム部分ロックダウン設定のいずれかを使用するには、設定をクリックします。 **c.** 部分ロックダウン状態にある間にデバイスへのリモート応答セッションを許可する場合は、リモート応答をオンにします。 **d.** ［ロックダウンを確認］をクリックします。 離れたところからデバイスのロックを解除するには、デバイスをクリックし、［アクションを選択］ドロップダウンリストで［デバイスをロック解除］をクリックします。リモートロック解除を確認します。

4. 完全ロックまたは部分ロックされたデバイスを手動でロック解除する場合は、［アクション］ > ［ロック解除キーを表示］をクリックします。一意のロック解除キーをコピーし、デバイスで次のコマンドを実行します。

OS	コマンド
Windows	**a.** CylanceOPTICS の実行可能フォルダに移動します（デフォルトでは「C:\Program Files\Cylance\Optics」）。 **b.** 実行 `CyOptics.exe control --password "<unlock_key>" unlock -a`
macOS	**a.** 実行 `cd /Library/Application\ Support/Cylance/Optics/CyOptics.app/Contents/Resources` **b.** 実行 `sudo ../MacOS/CyOptics control --password <unlock_key> unlock -net`
Linux	実行 `./CyOptics control --password "password" unlock -net`

デバイスへのアクションの送信

リモート応答機能を使用すると、使い慣れたコマンドラインインターフェイスを使用して、管理コンソールから直接、 CylanceOPTICS が有効な任意のデバイスでスクリプトを安全に実行したり、コマンドを実行したりできます。

リモート応答セッションを開始すると、 CylanceOPTICS エージェントはデバイスのネイティブシェルのインスタンス（Windows の場合は cmd、 macOS と Linux の場合は bash）を作成し、シェルとの間でコマンドの転送を処理します。このようにして、ネイティブシェルの機能、およびデバイスで使用可能なアプリとスクリプトにアクセスできます。CylanceOPTICS にはまた、デバイスとの間でファイルを転送するために使用できるいくつかの予約済みコマンドも用意されています。

リモート応答セッションは、オンライン状態のデバイスでのみ開始でき、25 分間操作しないとタイムアウトします。同じデバイスで同時に複数のセッションを開くことができます（最大 50 個）。

リモート応答は、デバイスへの高レベルのアクセスを提供します。そのため、コマンドを発行する際には注意し、組織のセキュリティポリシーに準拠してください。リモート応答を使用すると、送信されるコマンド、ファイル転送に関する情報、および受信した応答などのセッションの詳細が、管理コンソールからアクセスできるデバイスログに記録されます。ログファイルは 30 日間保持されます。

リモート応答セッションの開始

1. 管理コンソールのメニューバーで、［**CylanceOPTICS**］ **>** ［デバイス］をクリックします。
2. デバイスを見つけて、デバイス名をクリックします。
3. ［アクションを選択］ドロップダウンリストで、［リモート応答］をクリックします。
4. リモート応答セッションウィンドウにコマンドを入力します。

   CylanceOPTICS の予約済みコマンドの詳細については、「リモート応答用に予約されたコマンド」を参照してください。

終了したら： リモート応答セッションの記録とともにデバイスログをダウンロードする場合は、メニューバーで［**CylanceOPTICS**］ **>** ［アクション履歴］をクリックします。デバイスを見つけて、［ダウンロードログ］をクリックします。

リモート応答用に予約されたコマンド

次に挙げる予約済みコマンドは、サポートされている OS プラットフォーム全体に共通したもので、デバイスのネイティブのシェルで直接操作することはありません。

項目	説明
`rr-clear`	このコマンドは、リモート応答ターミナルウィンドウをクリアします。
`rr-get <ファイルの絶対パス>`	このコマンドは、指定されたファイル（ファイル名を含む必要があります）をデバイスからコピーして、Web ブラウザーにアップロードし、ローカルシステムに保存できるようにします。ファイルが 70MB より大きい場合、コマンドはエラーで失敗します。 例：`rr-get C:\Program Files\Cylance\Desktop\2021-03-26.log`
`rr-help`	このコマンドは、予約済みコマンドのリストを表示します。
`rr-put <宛先ディレクトリ>`	このコマンドを実行すると、ファイルブラウザーウィンドウが開き、デバイス上の指定したディレクトリ（ユーザーのダウンロードフォルダなど）に送信するファイルをローカルシステムから選択できます。ファイルが 70MB より大きい場合、コマンドはエラーで失敗します。 例：`rr-put C:\Users\username\Downloads`

項目	説明
`rr-quit`	このコマンドは、リモート応答セッションを終了します。ターミナルウィンドウは開いたままとなるため、セッション履歴は確認できますが、コマンドの送受信は行われません。

CylanceGATEWAY によるネットワーク接続の監視

ユーザーのネットワーク接続に関連するアクティビティとイベントを監視できます。CylanceGATEWAY は、デバイスで CylanceGATEWAY の仕事モードが有効になっている全ユーザーのすべてのネットワークアクティビティをログに記録します。デフォルトでは、CylanceGATEWAY ネットワークアクティビティデータは 30 日間保持されます。ログに記録された 30 日間のネットワークイベントを検索できます。

メモ：CylanceGATEWAY がテナントで有効になっていない場合、それを設定するメニューオプションは管理コンソールに表示されません。

ネットワークアクティビティの表示

CylanceGATEWAY は、仕事モードとセーフモードが有効になっているデバイスのすべてのネットワークアクティビティをログに記録します。ネットワークアクティビティログには、試行された各接続イベントに関するユーザー、デバイスモデルと OS、ホスト名、宛先、日時、およびその他の詳細が記録されます。ACL ルールでトラフィックプライバシーが有効になっている場合、ルールが適用されるネットワークアクセス試行は［ネットワークイベント］画面に記録されず、設定されている場合には SIEM ソリューションまたは syslog サーバーに送信されることもありません。

接続が潜在的な脅威として識別された場合、［検出］カラムには検出された脅威のタイプが示されます。

- ［**DNS** トンネリング］の検出とは、クライアントから攻撃者の DNS サーバーへの DNS トラフィックの分析に基づく潜在的な脅威です（たとえば、ホストが感染した場合、マルウェアは作成者とコマンド&コントロール（C2）チャネルを開始して、データ流出を試みる可能性があります）。
- レピュテーションの検出とは、安全でないインターネット宛先の BlackBerry リストにあるアドレスからの潜在的な脅威であり、宛先評価によって検出されます。各宛先にはリスクスコアが割り当てられます。ブロックする宛先評価のリスクレベルを設定できます。
- 署名検出の検出とは、署名検出によって検出された潜在的な脅威を指します。シグネチャベースの検出は、データベースの一部として保存されている既知のマルウェアを検出するために使用される手法です。新しいマルウェアシグネチャが特定されると、サイバーセキュリティのエキスパートがシグネチャをデータベースに追加します。
- ゼロデイ検出の検出とは、以前に特定されていない新たに特定された悪意のある送信先（ドメイン生成アルゴリズム（DGA）やフィッシングなど）を指します。これらの送信先が特定されると、送信先にリスクスコアが割り当てられます。これ以降、ネットワーク保護のために設定したリスクレベルに基づいて、ブロックまたは警告が行われます。詳細については、Cylance Endpoint Security セットアップガイドで「ネットワーク保護設定の構成」に関するコンテンツを参照してください。

管理コンソールでネットワークアクティビティログを表示するには、メニューバーで［**CylanceGATEWAY**］**>**［イベント］をクリックします。

ネットワークイベントの詳細を表示するには、アクティビティログの行をクリックします。イベントの詳細については、「イベント詳細ページの表示」を参照してください。

列をフィルターするには、列の上部にある をクリックします。

自由形式の検索を実行するには、 をクリックして検索クエリを入力します。検索フィールドに文字を入力するにつれて表示されるオプションから一致するものを選択できます。

表示する列を変更するには、列見出しの右側にある をクリックします。

イベント列の順序を変更するには、その列を表示する場所にドラッグします。

ネットワークアクティビティ情報を .csv ファイルにエクスポートするには、 をクリックします。すべてをエクスポートする場合、またはフィルタリングされたネットワークアクティビティのみをエクスポートする場合に選択し、［エクスポート］をクリックします。

ユーザーがアクセスしようとするネットワーク宛先を CylanceGATEWAY が分類する方法については、「ネットワーク宛先のリスクレベルの評価」を参照してください。

イベント詳細ページの表示

イベントページに記録されたネットワークイベントに関する追加のメタデータと詳細を表示することができます。どのようなメタデータが表示されるかは、作成されたネットワーク要求のタイプや ACL ルールの構成など、いくつかの要因によって異なります。たとえば、DNS イベントには DNS 固有の詳細が表示され、TLS イベントには TLS 固有の詳細が表示されます。同じく、ACL ルールによるネットワーク保護が有効になっている場合も、追加のメタデータが表示されます。ネットワークイベントを他のコンソールユーザーと共有して、ユーザーがアクセスしようとした宛先の監査や調査をすることができます。コンソールユーザーが共有イベントを表示するには、適切な権限が必要です。 をクリックすると、イベントへのリンクがコピーされます。

ログに記録されたネットワークイベントは、次のデータフィルターを使用したフィルタリングができます。

フィルター	説明
イベントの概要	
イベントID	これは、テナントのネットワークイベントに対する一意の識別子です。
ソース IP	これは、イベント中にエンドポイントトンネルに割り当てられたプライベートゲートウェイ IP です。
ソースポート	これは宛先のポート番号です。
DNS クエリ名	これは、CylanceGATEWAY エージェントがクエリした DNS サーバーのリソース要求（RR）名です。
DNS クエリタイプ	これは、DNS サーバーに送信された DNS クエリのタイプ（A、AAAA、SRV レコードなど）です。
移行先	これは、イベントの宛先です。宛先 IP アドレスは常に含まれています。また該当する場合は、ネットワークサービス名やホスト名が表示されることもあります。
宛先ポート	これは、アクセスされていた宛先のポートです。

フィルター	説明
プライベート NAT ソース IP	このイベントがいずれかのプライベートネットワークに向かって CylanceGATEWAY Connector から離れたときの、このイベントのソース IP アドレスです。ソース IP が使用できないか、機能が有効になっていない場合、フィルターにより、「不明」と表示されます。 重要：CylanceGATEWAY Connector システム時刻が正確であることを確認する必要があります。CylanceGATEWAY Connector システム時刻が正確なシステム時刻を維持していない場合、コネクタによって報告される NAT 詳細が BlackBerry Infrastructure 内のネットワークイベントと一致しないことがあります。デフォルトでは、CylanceGATEWAY Connector は、Ubuntu のタイムサーバー（ntp.ubuntu.com サーバー）を時刻同期に使用します。または、カスタム NTP サーバーを指定できます。Ubuntu タイムサーバーを使用する場合は、そのタイムサーバーがプライベートネットワークからアクセスできることを確認してください。詳細については、「CylanceGATEWAY Connector の設定」を参照してください。 CylanceGATEWAY Connector は、更新された NAT 詳細を 1 分ごとに［イベント詳細］画面に送信します。 この機能はデフォルトで有効になっています。Cylance コンソールのイベント詳細ページにプライベート NAT ソースの詳細が表示されない場合は、最新の CylanceGATEWAY Connector をインストールしてコネクタを再起動したことを確認します。
プライベート NAT ソースポート	このイベントがいずれかのプライベートネットワークに向かって CylanceGATEWAY Connector から離れたときの、このイベントのソース IP ポートです。ポート番号が使用できないか、機能が有効になっていない場合、フィルターにより、「不明」と表示されます。 この機能はデフォルトで有効になっています。Cylance コンソールのイベント詳細ページにプライベート NAT ソースの詳細が表示されない場合は、最新の CylanceGATEWAY Connector をインストールしてコネクタを再起動したことを確認します。
BlackBerry ソース IP	このイベントが BlackBerry Infrastructure から離れたときの、このイベントの IP アドレスです。この BlackBerry ソース IP は CylanceGATEWAY トンネルを使用しないフロー（セーフモードなど）では使用できません。
トンネル ソース IP	CylanceGATEWAY トンネルに到達したときに BlackBerry Infrastructure に表示されるエンドポイントの IP アドレスです。
プロトコル	これは、ネットワークイベントが宛先へのアクセスに使用したプロトコル（レイヤ 4）です。プロトコルは UDP または TCP です。
アプリプロトコル	これは、通信に使用された TLS、DNS、HTTP などのプロトコル（レイヤ 6 または 7）です。
アクセスタイプ	これは、ネットワークイベントが宛先へのアクセスに使用したアクセスタイプ（セーフモードやゲートウェイトンネルなど）です。

フィルター	説明
ネットワークルート	これによりトラフィックは、トラフィックのルーティングに使用されたパブリックまたはプライベート接続として提供されます。プライベート接続の場合は、コネクタグループ名および各 CylanceGATEWAY Connector でフィルタリングできます。
コネクタ	これは、ネットワークイベントが関連付けられている CylanceGATEWAY Connector です。コネクタに関する詳細を表示するには、コネクタ名をクリックします。
カテゴリ	これは、イベントに適用されるカテゴリです。たとえば、CylanceGATEWAY が宛先を悪意のある脅威を含んでいる可能性があるものとして識別した場合、カテゴリに「動的リスク」が表示されることがあります。動的リスクカテゴリの詳細については、セットアップガイドの「ネットワーク保護の構成」を参照してください。宛先は、それに含まれるコンテンツに基づいて、「コンピュータおよび情報技術」などに分類される場合もあります。宛先コンテンツのカテゴリの詳細については、セットアップガイドの「宛先コンテンツのカテゴリ」を参照してください。
サブカテゴリ	これは、宛先に関連付けられているカテゴリのネットワークトラフィックサブカテゴリの説明です。カテゴリが動的リスクである場合に表示されるサブカテゴリの詳細については、セットアップガイドの「ネットワーク保護の構成」を参照してください。カテゴリが宛先コンテンツのカテゴリの 1 つである場合に表示されるサブカテゴリの詳細については、セットアップガイドの「宛先コンテンツのカテゴリ」を参照してください。
開始時刻（UTC）	これは、ネットワークアクティビティの通信が開始された時刻です。時刻は UTC で表示されます。
終了時刻（UTC）	これは、ネットワークアクティビティの通信が終了した時刻です。時刻は UTC で表示されます。
PID	これは、DNS 要求を開始したプロセスの数値プロセス ID です。PID は、エージェントがセーフモードで有効になっているときに、Windows または macOS デバイスによって報告されます。
パス名	これは、プロセスが実行された実行可能ファイルへのパスです。これは通常、svchost.exe へのパスとして表示されます。このパスは 1024 文字に切り捨てられます。このパスは、セーフモードで有効になっているときに、Windows または macOS デバイスによって報告されます。
転送済み	これは、宛先と CylanceGATEWAY エージェントの間で交換されたバイト数を示します。ここに表示されるのは、サーバーおよび CylanceGATEWAY エージェントにアップロードとダウンロードされた合計バイト数です。
パケットフロー	これは、宛先と CylanceGATEWAY エージェントの間で送信されたパケットの数です。
ユーザー	これは、ネットワークイベントが関連付けられているユーザー名です。ネットワークイベントは、ユーザーの Active Directory ユーザー名と表示名によるフィルタリングができます。イベントページをエクスポートする場合、ユーザー名のみがエクスポートされます。ユーザー名をクリックすると、当該ユーザーに関連付けられているイベントを表示できます。

フィルター	説明
OS	これは、ネットワークアクティビティの開始に使用されたデバイスです（Android、iOS、macOS、Windows など）。
機種	これはデバイスのモデルです（iPhone、Samsung Galaxy、Google Pixel など）。
デバイス	これは、ユーザーの macOS または Windows デバイスのホスト名です（example.com など）。
アクション	これにより、ネットワーク保護設定と環境に指定した ACL ルールに基づいて、ネットワークイベントが許可されるかブロックされるかが判定されます。アクションの追加情報は、アクションのセクションに含まれています。
アクション	
接続フェーズ	これは、アクセス試行プロパティを各 ACL ルールの条件および宛先と比較した際の評価フェーズです。ACL ルールに対して評価されたフェーズ（DNS ルックアップ、接続試行、TLS ハンドシェイク時など）が 1 つまたは複数表示されます。
時刻(UTC)	これは、ACL ルールによってネットワークアクティビティが評価された時刻です。時刻は UTC で表示されます。
適用ルール	これは、ACL ルールの各種フェーズでの評価時に適用された ACL ルールの名前です。
アクション	これは、評価済みフェーズに対してアクションが許可されたかブロックされたかを示します。
アラート	
種類	これは、関連付けられたネットワーク保護レベルの指定を基にしてネットワークアクティビティによってトリガーされた異常を特定しています。サポートされている異常の詳細については、「ネットワークアクティビティの表示」を参照してください。
時刻(UTC)	これは、ネットワークアクティビティがアラートをトリガーした時刻です。時刻は UTC で表示されます。
カテゴリ	これは、アラートをトリガーした異常です。異常の詳細については、「ネットワークアクティビティの表示」を参照してください。
署名	これは、ネットワークイベントによってトリガーされた署名の異常です。
転送済み	
ダウンロード済み	これは、宛先から CylanceGATEWAY エージェントに送信されたデータの合計バイト数です。
アップロード済み	これは、サーバーの宛先から CylanceGATEWAY エージェントに送信されたデータの合計バイト数です。

フィルター	説明
TLS	
TLS バージョン	これは、宛先への接続に使用された TLS プロトコルのバージョンです。
クライアントALPN	これは、宛先から CylanceGATEWAY エージェントに送信された ALPN ヘッダー情報です。
サーバーALPN	これは、宛先から CylanceGATEWAY エージェントに送信されたヘッダー情報です。
SNI	これは、CylanceGATEWAY エージェントが接続を試行した宛先のホスト名です。
発行者	これは、宛先によって提示された証明書です。
サブジェクト	これは、ACL ルールに関連して、さまざまなフェーズ（DNS ルックアップ、接続確立、TLS ハンドシェイクなど）での評価時に適用されたルールの名前です。
発効日	これは、それ以前は証明書が無効な日付です。
失効日	これは、それ以後は証明書が無効な日付です。
HTTP イベント	これにより、分析および脅威ハンティングのための、元のプレーンテキストの暗号化されていない HTTP フローが報告されます。HTTP フローは復号化されないことに注意してください。要求および応答詳細の概要には、次の要求および応答詳細が含まれます。 • HTTP メソッドおよび要求 URL（URI） • ユーザーエージェント • コンテンツタイプヘッダー • HTTP ステータスコード 総数のイベントのうち、最初の 3 つの HTTP イベントが表示されます。バッジには、イベント用に記録されたイベントの総数が表示されます。［すべての **HTTP** イベント］をクリックすると、［イベントの概要］ページにすべてのイベントが表示されます。各イベントをクリックすると、ヘッダー情報など、詳細が表示されます。現時点では、HTTP イベント内で検索およびフィルタリングできません。HTTP の詳細は、次の制限によって切り捨てられます。 • ヘッダー名には、最大 64 バイトを表示 • ヘッダー値には、最大 512 バイトを表示 • 方向ごとの合計ヘッダーサイズ（名前、ボディなど）には、最大 4096 バイトを表示 • 要求および応答ボディには、最大 512 バイトを表示 • 要求および応答は、デフォルトでは Base64 エンコード。ユーザーは、デコードされたボディを表示

フィルター	説明

DNS	これは、DNS クエリと、イベントに関連付けられているすべての応答の詳細を報告します。要求および応答詳細の概要には、次の要求および応答詳細が含まれます。
	• 要求の詳細
	  • クエリ名：CylanceGATEWAY エージェントがクエリした DNS サーバーのリソース要求（RR）名です。
	  • クエリタイプ：DNS サーバーに送信された DNS クエリのタイプ（A、AAAA、SRV レコードなど）です。
	• 応答の詳細
	  • リソースレコード名：CylanceGATEWAY エージェントからのクエリに応答する DNS サーバーの名前です。
	  • リソースレコードタイプ：DNS サーバーに送信された DNS 応答のタイプ（A など）です。
	  • リソースデータ：応答を返す DNS サーバーのアドレスです。
	  • TTL：要求されたリソースデータの有効期間（秒単位）です。
	DNS クエリの応答の総数がバッジに表示されます。

CylanceAVERT での機密ファイルの監視

機密ファイルに関連付けられたアクティビティとイベントを、保存時と転送中の両方で監視できます。組織内の機密ファイルはすべてファイルインベントリに表示されます。窃盗イベントに関与したファイルは CylanceAVERT イベントビューと証拠ロッカーに表示されます。

メモ：CylanceAVERT がテナントで有効になっていない場合、それを設定するメニューオプションは管理コンソールに表示されません。

CylanceAVERT イベント

データ窃盗イベントは、CylanceAVERT イベントのページで保存およびリスト化されます。CylanceAVERT イベントは、イベントリストに 30 日間保存されます。データ窃盗イベントが発生すると、イベントリストに項目が新たに追加され、次の情報が表示されます。

項目	説明
検出時刻	窃盗イベントが発生した日時です。
デバイス	窃盗イベントが検出されたデバイスの名前です。
ユーザー	窃盗イベントを実行したユーザーの氏名、メールアドレス、部署、役職です。リンクをクリックすると、ユーザーの詳細ページを表示できます。
アクティビティ	CylanceAVERT でデータ窃盗イベントとしてタグ付けされたアクティビティのタイプです。Web、メール、USB で表示されます。
場所	機密データがアップロードされた場所です。発生したアップロードのタイプ（Web サイトのルートドメイン、メールドメインおよび受信者、USB ファイルのコピー場所）に従って表示されます。
ファイル	イベントに含まれるファイルの数です。リンクをクリックすると、ファイルの詳細ページが表示されます。複数のファイルが窃盗イベントに関連付けられている場合があります。
ポリシー	違反した CylanceAVERT ユーザーポリシーの数です。複数のポリシーが窃盗イベントに関連付けられている場合があります。
データタイプ	CylanceAVERT イベントをトリガーするのに必要なキーワードや正規表現の数です。

CylanceAVERT イベントの詳細を表示

データ窃盗イベントが発生すると、イベントの詳細が CylanceAVERT のイベントページに表示されます。各イベント行をクリックすると窃盗イベントの詳細が表示され、イベントに含まれる機密データタイプの数、イベントのスニペットの確認、関連ファイルのダウンロードなどができます。次の手順では、イベントページを見つける方法と詳細を表示するための操作について説明しています。暗号化されたファイルまたはパスワードで保護されたファイルの場合、機密データのタイプではなく［暗号化されたファイル］が表示されます。

作業を始める前に：

ファイルスニペットを表示してすべてのファイルをダウンロードするには、次のデータ収集設定を有効にしておく必要があります。詳細については、「データ収集設定の構成」を参照してください。

- ファイルスニペットを生成
- 証拠ファイル収集を有効化

イベント情報を表示するには、次の権限が必要です。

- 一般イベントリストの表示
- デバイス名の表示
- ユーザー名の表示
- ポリシー名の表示
- ポリシーの詳細へのリンク
- データエンティティの表示
- ファイルの詳細の表示
- すべてのファイルのダウンロード

1. 管理コンソールのメニューバーで［**CylanceAVERT**］ > ［イベント］をクリックします。
2. 行をクリックすると、イベントの詳細が表示されます。
3. ［イベントの詳細］ペインで、次のいずれかの操作を行います。
   - ［ユーザーの詳細］でユーザー名をクリックすると、ユーザーの情報ページに遷移します。そのページで、ユーザーに関連付けられたポリシー、イベント、デバイスを確認できます。
   - ［ポリシー違反］でポリシーをクリックすると、違反したポリシーの詳細を確認できます。
   - ［ファイルの詳細］で情報アイコンをクリックするとファイルの詳細（ファイルの種類、スキャンされた機密データのタイプ、そうしたデータタイプの発生回数など）を確認できます。 をクリックすると、窃盗イベントに関するスニペット情報を表示できます。 クリックして、窃盗イベントに関係するファイルをダウンロードすることもできます。証拠ファイルは圧縮された .gz ファイルとしてダウンロードされます。ファイルを解凍して表示するには、7zip などのユーティリティツールが必要です。

ファイルインベントリの表示による機密ファイルの識別

CylanceAVERT がデバイスにインストールされている場合、エンドポイントトローリングプロセスが自動的に開始され、情報保護ポリシーに指定された機密データのタイプを含むすべてのファイルがデバイスで検出されます。機密性の高い組織ドキュメントを含んでいるとのフラグが付けられたファイルは、ファイルインベントリに追加されます。ファイルインベントリを使用すると、環境内にある機密文書の数と種類を確認したり、機密データにアクセス可能なユーザーとデバイスを特定してリスクを評価したりできます。ファイルインベントリリストを、ユーザー、デバイス、データタイプ別にグループ化することもできます。

メモ：CylanceAVERT のインストール後、トローリングプロセスが完全に完了するまでに数時間かかる場合があります。

作業を始める前に：

ファイルインベントリを表示するには、次の権限が必要です。

- ファイル概要の読み取り
- ポリシーのリスト化と読み取り

1. 管理コンソールのメニューバーで、［**CylanceAVERT**］ > ［ファイルインベントリ］の順にクリックします。

CylanceAVERT のファイルインベントリは、機密データタイプを含む全ファイルのリストです。情報保護ポリシーの指定ファイルとして、検索プロセスで検出されたものになります。サポートされるファイルタイプは、.pdf、.ooxml（Microsoft Word、Excel、PowerPoint）、.txt、.rtf、.zip、.csv です。ファイルインベントリリストに表示される情報は、次の表のとおりです。

項目	説明
ファイル名	ファイルの名前です。
ファイルサイズ	ファイルのサイズ（KB）です。
情報タイプ	ファイルが属する情報タイプです。
データタイプ	ファイル内で検出された機密データタイプの数です。
ユーザー	ファイルにアクセスできるユーザーの数です。
デバイス	ファイルにアクセスできるデバイスの数です。
ポリシー	当該のファイルを含むポリシーです（複数の場合あり）。
種類	ファイルタイプです。サポートされるファイルタイプは、.pdf、.ooxml（Microsoft Word、Excel、PowerPoint）、.txt、.rtf、.zip、.csv です。

メモ：このリストにはページ付けがありません。スクロールして他の結果を読み込んだり、フィルタリングのオプションを使用したりすることができます。

最初の検索プロセスが完了すると、CylanceAVERT では、定期的にポーリングを行い、新しい機密データをチェックします。ファイルが部分的にのみスコア付けされ機密情報が検出された場合は、テーブル内のファイルの横にアイコンが表示され、ファイルが部分的にしか分析されていないことを示すアラートが表示されます。

2. 次の操作のいずれかを実行します。
   - ファイル名または情報タイプの列をフィルタリングするには、列見出しの ⏛ をクリックします。
   - 表示する列を変更するには、列見出しの右側にある ||| をクリックします。
   - データをユーザー、デバイス、またはデータタイプ別にグループ化するには、ドロップダウンメニューからグループ化を選択します。グループファイルインベントリビューから、項目をクリックすると、そのグループの詳細情報を表示できます。

   メモ：ファイルインベントリでファイル名や属性を表示することはできますが、ファイルスニペットとフルファイルアクセスはサポートされていません。
3. ファイルインベントリの項目をクリックすると、ファイルの詳細メニューを表示できます。このメニューから、ファイルの詳細、ファイルへのアクセス権を有するユーザーやデバイス、ファイル内で検出されたデータタイプ、ファイルが違反をしているポリシーを表示できます。

部分的に分析されたファイルの表示

CylanceAVERT では、部分的に分析されたファイルのみを表示することができます。CylanceAVERT でファイルの機密性を完全に判定できない場合、そのファイルは［部分的に分析されたファイル］リストに表示されます。ファイルが部分的にのみ分析される場合には、次のような状況が考えられます。

- ファイルが大きいため、スコアリングエンジンが分析を完全に完了できないうちにファイルが流出した場合。
- ファイルが複数レベルの階層を持つ圧縮 zip ファイルであり、最初のレベルのみが分析された場合。

部分的に分析されたファイルは、機密性スコアに基づいて、次の 2 つの結果となることが考えられます。ファイルが部分的にスコア付けされ機密データが検出されるか、ファイルが部分的にスコア付けされ機密データが検出されないかのいずれかです。

ファイルが部分的にスコア付けされ機密情報が検出されない場合、そのファイルは［部分的に分析されたファイル］リストに表示され、部分的にしか分析されていないことを示すアラートが表示されます。

ファイルが部分的にスコア付けされ機密情報が検出された場合、そのファイルは完全にスコア付けされたファイルと同様に扱われ、ファイルインベントリ、イベントビュー、および証拠ロッカーに表示されます。ただし、テーブルおよび詳細ビューのファイルの横にアイコンが表示され、部分的にしか分析されていないことを示すアラートが表示されます。

CylanceAVERT によって完全にスコア付けされなかったファイルのリストを、［部分的に分析されたファイル］ビューで表示することができます。

1. 管理コンソールのメニューバーで、［**CylanceAVERT**］ **>** ［部分的に分析されたファイル］の順にクリックします。

列	説明
ファイル名	部分的に分析されたファイルの名前です。
追加時刻	部分的に分析されたファイルがリストに追加された時刻です。
ファイルサイズ	部分的に分析されたファイルのサイズです。
拡張子	部分的に分析されたファイルの拡張子タイプです。

   メモ：このリストに改ページはありません。スクロールして他の結果を読み込むか、フィルターオプションを使用できます。
2. 次の操作のいずれかを実行します。
   - ファイル名または拡張子の列をフィルタリングするには、列見出しの ⍒ をクリックします。
   - 表示する列を変更するには、列見出しの右側にある ||| をクリックします。
3. 部分的に分析されたファイル一覧の項目をクリックすると、ファイルの詳細メニューを表示できます。このメニューから、ファイルの詳細、ファイルへのアクセス権を有するユーザーやデバイス、ファイル内で検出されたデータタイプを表示できます。

証拠ロッカーを使用した窃盗イベントの詳細の表示

ファイルインベントリ内のファイルがデータ窃盗イベントに関連する場合、そのファイルは BlackBerry が管理する AWS インスタンスに保存され、テナントごとに異なるキーで暗号化され、証拠ロッカーに追加されます。窃盗イベントに関連するファイルは、証拠ロッカーから表示またはダウンロードできます。

作業を始める前に：

証拠ファイルの収集を、情報保護設定で有効にしておく必要があります。詳細については、「データ収集設定の構成」を参照してください。

1. 管理コンソールのメニューバーで、［**Avert**］ > ［証拠ロッカー］をクリックします。

   証拠ロッカーには、データ窃盗イベントに関与した組織内のすべてのファイルのリストが表示されます。次の表では、証拠ロッカーのリストにある情報について説明しています。

項目	説明
追加時刻	これは、ファイルが証拠ロッカーに追加された時刻です。
ファイル名	これは、窃盗イベントに関係したファイルの名前です。
ファイルサイズ	これは、窃盗イベントに関係するファイルのサイズです。
関連イベント	これらは、ファイルが関連付けられている窃盗イベントです。番号をクリックすると、詳細が表示されます。
ダウンロード	これをクリックすると、窃盗イベントに関連するすべてのファイルをダウンロードできます。証拠ファイルは圧縮された .gz ファイルとしてダウンロードされます。ファイルを解凍して表示するには、7zip などのユーティリティツールが必要です。

2. 関連イベント列の番号をクリックすると、CylanceAVERT イベントが表示されます。
3. 追加時刻、ファイル名、またはファイルサイズの列をフィルタリングするには、列見出しの をクリックします。

モバイル OS の脆弱性の表示

管理コンソールを使用して、CylancePROTECT Mobile アプリがインストールされている組織環境におけるあらゆるモバイル OS の共通脆弱性識別子（CVE）の一覧を表示できます。このリストは、『National Vulnerability Database』で識別、定義、追跡されています。各 OS バージョンについて、そのバージョンを使用するデバイスの数、その OS バージョンの合計 CVE 数、各 CVE のリスク分類と簡単な説明、および National Vulnerability Database の全詳細を表示するためのリンクを確認できます。

1. 管理コンソールのメニューバーで、［保護］ > ［脆弱性］をクリックします。
2. ［モバイル **OS**］タブをクリックします。次の操作のいずれかを実行します。
   - 脆弱性を、ある列で昇順または降順に並べ替えるには、列の名前をクリックします。
   - 脆弱性をフィルタリングするには、列の をクリックしてフィルター条件を入力または選択します。
3. ある OS バージョンの脆弱性のリストを表示するには、［合計 **CVE**］列のリンクをクリックします。
   『National Vulnerability Database』の詳細を表示するには、CVE リンクをクリックします。

管理者アクションの監査

監査ログを使用して、組織の管理者が実行したアクションに関する情報を表示およびエクスポートできます。

監査ログの表示

1. 管理コンソールで、 > ［監査ログ］をクリックします。
2. フィルターフィールドで、監査ログ情報のフィルタリングに使用する条件を指定します。
3. 結果を .csv ファイルにエクスポートするには、  をクリックします。エクスポートの範囲を選択し、［エクスポート］をクリックします。

   同時にエクスポートできるレコードは最大 50,000 件です。結果の数は画面下部に表示されます。50,000 件を超えるレコードをエクスポートするには、結果を（日付などで）フィルターしてエクスポートしてから、別のフィルターを適用してエクスポートします。

監査ログ情報：一般管理

次の表に、複数の Cylance Endpoint Security 機能に影響する管理アクションの監査ログに追加される情報を示します。コンソールのフィルタリングオプションを使用して、監査ログの結果をフィルタリングできます。

カテゴリ	アクション	詳細
エージェントの更新	編集	ルール：<ルール名>、ゾーン：<ゾーン>、エージェントバージョン：<バージョン>、Optic バージョン：<バーション>
エージェントの更新	編集	層：<層の名前>、ゾーン：該当なし、エージェントバージョン：<バージョン>、Optic バージョン：<バージョン>
カスタム更新ルール	追加	カスタム更新ルール：<ルール名>、ゾーン：<ゾーン>、エージェントバージョン：<バージョン>、Optic バージョン：<バージョン>
カスタム更新ルール	削除	カスタム更新ルール <ルール *ID*> が削除されました。
デバイス	追加	デバイス：<デバイス名>、ゾーン：<ゾーン名>
デバイス	編集	名前変更：<元の名前> から <新しい名前> に変更、ポリシーの変更：<古いポリシー> から <新しいポリシー> に変更、削除されたゾーン：<ゾーン名>、追加されたゾーン：<ゾーン名>、エージェントロギングレベルの変更：<元の値> から <新しい値> に変更、エージェント自己保護レベルの変更：<元の> から <新しい値> に変更
デバイス	削除	デバイス：<デバイス名>

カテゴリ	アクション	詳細
ログイン	成功	プロバイダー：CylancePROTECT、ソース IP：<*IP* アドレス>
ログイン	失敗	–
ポリシー	追加	ポリシー：<ポリシー名>、検出設定が <変更の詳細> から変更
ポリシー	編集	ポリシー：<ポリシー名>：<変更の詳細>
ポリシー	削除	ポリシー：<ポリシー名>
Syslog	無効化	Syslog が無効になりました。
Syslog	設定の保存	{<構成設定>}
テナント設定	更新	カスタムドメイン名を <名前> に更新しました。
テナントロール	追加	ロール：<カスタムロール名>
テナントロール	編集	ロール：<カスタムロール名>
テナントロール	削除	ロール：<カスタムロール名>
ユーザー	追加	ユーザー：<ユーザー名>、ロール：<ロールタイプ>
ユーザー	編集	ユーザー：<ユーザー名>、メール：<ユーザーのメールアドレス>
ユーザー	削除	ユーザー：<ユーザー名>
ゾーン	追加	ゾーン：<ゾーン名>、ポリシー：<ポリシー名>、値：<"高" / "低" / "正常">
ゾーン	編集	名前変更：<元の名前> から <新しい名前> に変更、現在のポリシー：<ポリシー名>、ゾーン内のすべてのデバイスに適用されるポリシー：<*TRUE / FALSE*>、割り当てられた値：<"高" / "低" / "正常">
ゾーン	削除	ゾーン：<ゾーン名>

監査ログ情報：CylancePROTECT Desktop

次の表に、CylancePROTECT Desktop 管理アクションの監査ログに追加される情報を示します。コンソールのフィルタリングオプションを使用して、監査ログの結果をフィルタリングできます。

カテゴリ	アクション	詳細
アプリケーション設定	カスタム認証の無効化	カスタム認証が無効になりました。
アプリケーション設定	カスタム認証の保存	カスタム認証が保存されました：{*<configuration_settings>*}
アプリケーション設定	エージェントのアンインストール時にパースワードを必要とする設定の保存	エージェントをアンインストールするためにパスワードを必要とする設定が保存されました。
アプリケーション設定	エージェントのアンインストール時にパスワードを必要とする設定の無効化	エージェントをアンインストールするためにパスワードを必要とする設定が無効になりました。
アプリケーション設定	インストールトークンの削除	インストールトークンが削除されました。
アプリケーション設定	インストールトークンの再生成	インストールトークンが生成されました。
グローバルリスト	追加	ソース：CylancePROTECT、SHA256：*<file hash>*、ファイル名：*<name>*、理由：*<value>*、追加先：グローバル隔離またはセーフリスト、カテゴリ： *<value>*
グローバルリスト	削除	SHA256： *<file hash>*
スクリプトグローバルリスト	追加	ソース：CylancePROTECT、SHA256：*<file hash>*、ファイル名：*<name>*、理由：*<value>*、追加先：スクリプト制御除外リスト
スクリプトグローバルリスト	削除	SHA256： *<file hash>*
脅威	セーフリスト	SHA256：*<file hash>*、カテゴリ：*<value>*、理由： *<value>*
脅威	グローバル隔離	ソース：CylancePROTECT、SHA256：*<file hash>*、理由：*<value>*
脅威データレポート	トークンの生成	―
脅威データレポート	トークンの削除	―

監査ログ情報：CylancePROTECT Mobile

次の表に、 CylancePROTECT Mobile 管理アクションの監査ログに追加される情報を示します。コンソールのフィルタリングオプションを使用して、監査ログの結果をフィルタリングできます。

カテゴリ	アクション	詳細
エンドユーザー	追加	ユーザー：<メールアドレス>、タイプ: ローカル
エンドユーザー	インポート	成功数：<回数>、失敗数：<回数>
エンドユーザー	削除	ユーザー：<メールアドレス> 削除された各ユーザーに対してログエントリが生成されます。
エンドユーザー	ポリシーを割り当て	ポリシー：<ポリシー名>、ユーザー：<メールアドレス>
エンドユーザー	招待を送信	ユーザー：<メールアドレス>、成功数：<回数>、失敗数：<回数>
モバイルデバイス	削除	ユーザー：<メールアドレス>、デバイス：<デバイス名>、OS：<*OS* ファミリー>、OS バージョン：<バージョン> 削除された各デバイスに対してログエントリが生成されます。
モバイルデバイス	エクスポート	フィルター：<フィルターフィールドと値> ［すべて］を選択した場合、［フィルター］の値は［なし］になります。［現在のフィルター］を選択した場合は、各フィールドの名前と値が表示されます。
モバイルポリシー	追加	ソース：Protect Mobile、ポリシー：<ポリシー名>、<設定名と値>
モバイルポリシー	編集	ソース：Protect Mobile、ポリシー：<ポリシー名>、<変更後の設定名と値>
モバイルポリシー	削除	ソース：Protect Mobile、ポリシー：<ポリシー名> 削除された各ポリシーに対してログエントリが生成されます。
モバイルの除外	追加	ソース：Protect Mobile、タイプ：<アプリ / 開発者 / ドメイン / *IP*>、カテゴリ：<承認済み / 制限対象>、名前：<名前>、プラットフォーム：<プラットフォーム>、識別子：<識別子>、発行者：<発行者>
モバイルの除外	削除	ソース：Protect Mobile、タイプ：<アプリ / 開発者 / ドメイン / *IP*>、名前：<名前> 削除された各除外に対してログエントリが生成されます。

カテゴリ	アクション	詳細
モバイルアラート	無視	ソース：Protect Mobile、ID：<*ID*>、タイプ：<アラートタイプ>、名前：<アラート名>、説明：<デバイス *OS*> 削除された各アラートに対してログエントリが生成されます。
モバイルアラート	エクスポート	ソース：Protect Mobile、フィルター：<フィルターフィールドと値> ［すべて］を選択した場合、［フィルター］の値は［なし］になります。［現在のフィルター］を選択した場合は、各フィールドの名前と値が表示されます。

監査ログ情報：CylanceOPTICS

次の表に、CylanceOPTICS 管理アクションの監査ログに追加される情報を示します。コンソールで、使用可能なフィルタリングオプションを使用して、監査ログの結果をフィルタリングできます。

カテゴリ	アクション	詳細
高度なクエリ	実行	クエリ： <*EQL_query*>
高度なクエリのエクスポート	追加	名前：<*name*>、説明：<*description*>、共有： <*isShared*>
高度なクエリのエクスポート	ダウンロード	名前：<*name*>、説明： <*description*>
高度なクエリのエクスポート	削除	名前：<*name*>、説明：<*description*>、共有： <*isShared*>
高度なクエリのスナップショット	追加	名前：<*name*>、説明：<*description*>、共有： <*isShared*>
高度なクエリのスナップショット	編集	名前：<*name*>、説明：<*description*>、共有： <*isShared*>
高度なクエリのスナップショット	削除	名前：<*name*>、説明：<*description*>、共有： <*isShared*>
高度なクエリのテンプレート	追加	名前：<*name*>、説明：<*description*>、共有：<*isShared*>、クエリ： <*EQL_query*>
高度なクエリのテンプレート	編集	名前：<*name*>、説明：<*description*>、共有：<*isShared*>、クエリ： <*EQL_query*>

カテゴリ	アクション	詳細
高度なクエリのテンプレート	削除	名前：<*name*>、説明：<*description*>、共有： <*isShared*>
検出	ステータスを変更	検出：<*detection label*>、検出 ID：<*detection id*>、デバイス：<*device name*>、以前のステータス、<*previous detection status*>、新しいステータス： <*new detection status*>
検出	削除	検出：<*detection label*>、検出 ID：<*detection id*>、デバイス：<*device name*>
検出例外	追加	名前： <*name*>
検出例外	編集	名前： <*name*>
検出例外	削除	名前： <*name*>
検出ルール	追加	名前：<*name*>、説明：<*description*>、重大度：<*severity*>、OS： <*OS list*>
検出ルール	編集	名前：<*name*>、説明：<*description*>、重大度：<*severity*>、OS： <*OS list*>
検出ルール	削除	名前：<*name*>、説明：<*description*>、重大度：<*severity*>、OS： <*OS list*>
検出ルールセット	追加	名前：<*name*>、説明：<*description*>、デバイスポリシー：<*device policy name*>
検出ルールセット	編集	名前：<*name*>、説明：<*description*>、デバイスポリシー：<*device policy name*>
検出ルールセット	削除	名前：<*name*>、説明：<*description*>、デバイスポリシー：<*device policy name*>
デバイス	ファイルダウンロード	デバイス：<*device name*>、ファイル： <*file path and name*>
デバイス	ロック	デバイス：<*device name*>、設定プロファイル：<*profile name*>、ロックダウン期間： <*lockdown period*>
デバイス	ロック解除	デバイス： <*device name*>
デバイス	ロックダウンプロファイルを変更	デバイス：<*device name*>、設定プロファイル： <*profile name*>
デバイス	ロック解除キーを表示	デバイス： <*device name*>

カテゴリ	アクション	詳細
フォーカスデータ	追加	デバイス：*<device name>*、タイプ：*<focus view type>*、アーチファクト： *<focus view artifact>*
InstaQuery	追加	名前：*<IQ name>*、アーチファクト：*<IQ artifact>*、ファセット：*<IQ facet>*、語句： *<IQ term>*
InstaQuery	削除	名前：*<IQ name>*、アーチファクト：*<IQ artifact>*、ファセット：*<IQ facet>*、語句： *<IQ term>*
ジョブサービス	停止	名前：*<name>*、サービス： *<parent service type>*
ロックダウン設定	追加	設定プロファイル：*<configuration profile>*、説明：*<description>*、ホワイトリスト定義： *<allowed_connections>*
ロックダウン設定	削除	設定プロファイル： *<configuration profile>*
ロックダウン設定	編集	設定プロファイル：*<configuration profile>*、説明：*<description>*、ホワイトリスト定義： *<allowed_connections>*
パッケージ展開	追加	名前：*<name>*、パッケージ： *<packages>*
パッケージ展開	削除	名前： *<name>*
パッケージプレイブック	追加	名前：*<name>*、パッケージ： *<packages>*
パッケージプレイブック	編集	名前：*<name>*、パッケージ： *<packages>*
パッケージプレイブック	削除	名前：*<name>*、パッケージ： *<packages>*
プレイブックの結果	削除	デバイス：*<device name>*、プレイブック名：*<playbook name>*、検出 ID：*<detection id>*、ステータス： *<status>*
リモート応答	接続	デバイス： *<device name>*
リモート応答	切断	デバイス： *<device name>*
スケジュールされた高度なクエリ	追加	名前：*<name>*、説明：*<description>*、共有：*<isShared>*、スケジュール： *<schedule_details>*
スケジュールされた高度なクエリ	編集	名前：*<name>*、説明：*<description>*、共有：*<isShared>*、スケジュール： *<schedule_details>*
スケジュールされた高度なクエリ	削除	名前：*<name>*、説明：*<description>*、共有： *<isShared>*

カテゴリ	アクション	詳細
スケジュールされた高度なクエリ	結果の削除	名前：<*name*>、説明：<*description*>、結果タイムスタンプ：<*result_timestamp*>、結果： <*result_count*>
スケジュールされた高度なクエリ	開始	名前：<*name*>、説明：<*description*>、共有：<*isShared*>、スケジュール： <*schedule_details*>
スケジュールされた高度なクエリ	停止	名前：<*name*>、説明：<*description*>、共有：<*isShared*>、スケジュール： <*schedule_details*>

監査ログ情報：CylanceAVERT

次の表に、CylanceAVERT 管理アクションの監査ログに追加される情報を示します。コンソールのフィルタリングオプションを使用して、監査ログの結果をフィルタリングできます。

カテゴリ	アクション	詳細

データエンティティ	追加	{
		"id": "<*ID*>",
		"tenantId": "<テナント *ID*>",
		"occurred": "<日付/時刻>",
		"traceId": "<トレース *ID*>",
		"spanId": "<スパン *ID*>",
		"source": "com.blackberry.dlp",
		"type": "AUDIT",
		"category": "Entity",
		"subcategory": "created",
		"message": "admin created DataEntity named <ポリシー名>"
		},
		"admin": {
		"ecoId": "<*Eco ID*>"
		},
		"entity": {
		"id": "<*ID*>",
		"type": "DATAENTITY",
		"displayName": "<エンティティ表示名>"
		},
		"changes": {
		"regions": {
		"new": "<地域>"
		},
		"name":{
		"new": "<データエンティティ名>"
		"description": {
		"new": "<説明>"
		},
		"infoTypes": {
		"new": "<情報タイプ>"
		},
		"Type": {
		"new": "<データタイプ>"
		},
		"Parameters": {
		"new": "<パラメーター>"
		},
		"algorithm":{
		"new":<アルゴリズム>
		}
		}

カテゴリ	アクション	詳細

データエンティティ	編集	{
		"id": "<*ID*>",
		"tenantId": "<テナント *ID*>",
		"occurred": "<日付/時刻>",
		"traceId": "<トレース *ID*>",
		"spanId": "<スパン *ID*>",
		"source": "com.blackberry.dlp",
		"type": "AUDIT",
		"category": "ENTITY",
		"subcategory": "UPDATED",
		"message": "admin updated DataEntity named <データエンティティ名>",
		"crud": {
		"admin": {
		"ecoId": "<*Eco ID*>"
		},
		"entity": {
		"id": "<*ID*>",
		"type": "DATAENTITY",
		"displayName": "<データエンティティ表示名>"
		},
		"changes": {
		"description": {
		"new": "<新しい説明>",
		"old": "<古い説明>"
		}
		}
		}
		}

カテゴリ	アクション	詳細

データエンティティ	削除	{
		"id": "<*ID*>",
		"tenantId": "<テナント *ID*>",
		"occurred": "<日付/時刻>",
		"traceId": "<トレース *ID*>",
		"spanId": "<スパン *ID*>",
		"source": "com.blackberry.dlp",
		"type": "AUDIT",
		"category": "ENTITY",
		"subcategory": "DELETED",
		"message": "admin deleted DataEntity named <データエンティティ名>",
		"crud": {
		"admin": {
		"ecoId": "<*Eco ID*>"
		},
		"entity": {
		"id": "<*ID*>",
		"type": "DATAENTITY",
		"displayName": "<データエンティティ表示名>"
		}
		}
		}

証拠ファイル	ダウンロード	{
		"id": "<*ID*>",
		"tenantId": "<テナント *ID*>",
		"occurred": "<日付/時刻>",
		"traceId": "<トレース *ID*>",
		"spanId": "<スパン *ID*>",
		"source": "com.blackberry.dlp",
		"type": "AUDIT",
		"category": "ENTITY",
		"subcategory": "READ",
		"message": "Evidence File is downloaded",
		"crud": {
		"admin": {
		"ecoId": "<*Eco ID*>"
		},
		"entity": {
		"id": "<*ID*>",
		"type": "<エンティティタイプ>"
		}
		}
		}

カテゴリ	アクション	詳細

証拠ファイル	削除	<pre>{
		    "id": "<*ID*>",
		    "tenantId": "<テナント *ID*>",
		    "occurred": "<日付/時刻>",
		    "traceId": "<トレース *ID*>",
		    "spanId": "<スパン *ID*>",
		    "source": "com.blackberry.dlp",
		    "type": "AUDIT",
		    "category": "ENTITY",
		    "subcategory": "DELETED",
		    "message": "Evidence File is DELETED",
		    "crud": {
		        "admin": {
		            "ecoId": "<*Eco ID*>"
		        },
		        "entity": {
		            "id": "<*ID*>",
		            "type": "<エンティティタイプ>"
		        }
		    }
		}</pre>

カテゴリ	アクション	詳細

ポリシー	追加	{
		"common": {
		"id": "<*ID*>",
		"tenantId": "<テナント *ID*>",
		"occurred": "<日付/時刻>",
		"traceId": "<トレース *ID*>",
		"spanId": "<スパン *ID*>",
		"source": "com.blackberry.dlp",
		"type": "AUDIT",
		"category": "Entity",
		"subcategory": "created",
		"message": "admin created Policy named <ポリシー名>"
		},
		"admin": {
		"ecoId": "<*Eco ID*>"
		},
		"entity": {
		"id": "<*ID*>",
		"type": "PROFILE",
		"displayName": "<エンティティ表示名>"
		},
		"changes": {
		"emailDomainsRule": {
		"new": "<ドメインルール>"
		},
		"condition": {
		"new": "<条件>"
		},
		"policyName": {
		"new": "<ポリシー名>"
		},
		"policyType": {
		"new": "<ポリシータイプ>"
		},
		"description": {
		"new": "<説明>"
		},
		"policyRules": {
		"new": "<ポリシールール>"
		},
		"classification": {
		"new": "<分類>"
		},
		"browserDomains": {
		"new": "<ブラウザドメイン>"
		}
		}
		}

カテゴリ	アクション	詳細

ポリシー	編集	{
		"common": {
		"id": "<*ID*>",
		"tenantId": "<テナント *ID*>",
		"occurred": "<日付/時刻>",
		"traceId": "<トレース *ID*>",
		"spanId": "<スパン *ID*>",
		"source": "com.blackberry.dlp",
		"type": "AUDIT",
		"category": "Entity",
		"subcategory": "Updated",
		"message": "admin created Policy named <ポリシー名>"
		},
		"admin": {
		"ecoId": " "
		},
		"entity": {
		"id": "fbfa8366-e58c-4018-925f-2a536dce4c2d",
		"type": "PROFILE",
		"displayName": "policy-test-name-created-from-auto-test"
		},
		"changes":
		{
		"policyName":{
		"old" : "HIPAA",
		"new" : "HIPAA Compliance"
		},
		"condition": {
		"old": "<古い条件>",
		"new":"<新しい条件>"
		},
		"policyRules": {
		"old":[{<古いポリシールール>}],
		"new":[{<新しいポリシールール>}]
		},
		"policyConfigs": {
		"old":[{<古いポリシールール>}],
		"new":[{<新しいポリシールール>}]
		},
		"browserDomains":{
		"old":<古いブラウザドメイン>,
		"new":<新しいブラウザドメイン>
		},
		"emailDomainsRule": {
		"old":<古いドメインルール>,
		"new":<新しいドメインルール>
		}
		}
		}

カテゴリ	アクション	詳細

ポリシー	削除	<pre>{
		    "id": "<*ID*>",
		    "tenantId": "<テナント *ID*>",
		    "occurred": "<日付/時刻>",
		    "traceId": "<トレース *ID*>",
		    "spanId": "<スパン *ID*>",
		    "source": "com.blackberry.dlp",
		    "type": "AUDIT",
		    "category": "ENTITY",
		    "subcategory": "DELETED",
		    "message": "admin DELETED Policy named <ポリシー名>",
		    "crud": {
		        "admin": {
		            "ecoId": "<*Eco ID*>"
		        },
		        "entity": {
		            "id": "<*ID*>",
		            "type": "PROFILE",
		            "displayName": "<エンティティ表示名>"
		        }
		    }
		}</pre>

設定	更新	<pre>{
		    "id": "<*ID*>",
		    "tenantId": "<テナント *ID*>",
		    "occurred": "<日付/時刻>",
		    "traceId": "<トレース *ID*>",
		    "spanId": "<スパン *ID*>",
		    "source": "com.blackberry.dlp",
		    "type": "AUDIT",
		    "category": "SETTING",
		    "subcategory": "UPDATED",
		    "message": "admin UPDATED DLP settings",
		    "crud": {
		        "admin": {
		            "ecoId": "<*Eco ID*>"
		        },
		        "changes": {
		
		 "ui.tenant.setting.emailRecipients": {
		                "new": "<新しいメール受信者>",
		                "old": "<古いメール受信者>"
		            }
		        }
		    }
		}</pre>

カテゴリ	アクション	詳細

テンプレート	削除	{
		"id": "<*ID*>",
		"tenantId": "<テナント *ID*>",
		"occurred": "<日付/時刻>",
		"traceId": "<トレース *ID*>",
		"spanId": "<スパン *ID*>",
		"source": "com.blackberry.dlp",
		"type": "AUDIT",
		"category": "ENTITY",
		"subcategory": "DELETED",
		"message": "Template <テンプレート名> was deleted",
		"crud": {
		"admin": {
		"ecoId": "<*Eco ID*>"
		},
		"entity": {
		"id": "<*ID*>",
		"type": "TEMPLATE",
		"displayName": "<テンプレート名>"
		}
		}
		}

カテゴリ	アクション	詳細

テンプレート	追加	{
		"id": "<*ID*>",
		"tenantId": "<テナント *ID*>",
		"occurred": "<日付/時刻>",
		"traceId": "<トレース *ID*>",
		"spanId": "<スパン *ID*>",
		"source": "com.blackberry.dlp",
		"type": "AUDIT",
		"category": "ENTITY",
		"subcategory": "CREATED",
		"message": "Template <テンプレート名> was created",
		"crud": {
		"admin": {
		"ecoId": "<*Eco ID*>"
		},
		"entity": {
		"id": "<*ID*>",
		"type": "TEMPLATE",
		"displayName": "<テンプレート名>"
		},
		"changes": {
		"condition": {
		"new": "<条件>"
		},
		"regions": {
		"new": "<地域>"
		},
		"name": {
		"new": "<テンプレート名>"
		},
		"description": {
		"new": <説明>"
		},
		"infoTypes": {
		"new": "<情報タイプ>"
		},
		"type": {
		"new": "<テンプレートタイプ>"
		}
		}
		}
		}

ログの管理

このセクションでは、 Cylance Endpoint Security の各種機能およびサービスのログ設定の変更について説明します。

BlackBerry Connectivity Node ログの設定

BlackBerry Connectivity Node を使用すると、オンプレミスの Microsoft Active Directory、または LDAP ディレクトリと同期して、CylancePROTECT Mobile アプリと CylanceGATEWAY が有効になっているユーザーおよびユーザーグループを追加できます。

BlackBerry Connectivity Node イベントに対するログレベル、syslog 情報、およびローカルファイル情報を設定できます。

1. 管理コンソールのメニューバーで、［設定］ > ［ディレクトリ接続］をクリックします。
2. ［**Connectivity Node**］タブで、［設定］をクリックします。
3. ［サーバーのデバッグレベル］ドロップダウンメニューから、ログに記録するイベントのレベルを選択します。
4. ログを SysLog に送信するには、［**SysLog**］の横にあるボタンをオンにし、［ホスト］フィールドと［ポート］フィールドに値を入力します。
5. BlackBerry Connectivity Node がインストールされているコンピューターにログを送信するには、［ローカルファイルの保存先を有効にする］の横にあるボタンをオンにします。
6. ［ログファイルの最大サイズ］（MB 単位）および［サーバーログファイルの最長保存期間］（日数）フィールドに値を入力します。
7. ログフォルダを圧縮するには、［ログフォルダ圧縮を有効にする］の横にあるボタンをオンにします。
8. ［保存］をクリックします。

CylancePROTECT Desktop エージェントのログの管理

CylancePROTECT Desktop エージェントのログファイルには、トラブルシューティングの問題に役立つ情報が含まれています。トラブルシューティングを行う場合は、詳細ログを有効にして問題を再現し、関連する情報をログファイルに記録します。詳細ログは、より大きなログファイルを作成するので、トラブルシューティングを行う場合にのみ使用してください。エージェントのログファイルは、管理コンソールで 30 日間保持されます。

1. 管理コンソールのメニューバーで、［アセット］ > ［デバイス］をクリックします。
2. 1 つのデバイスをクリックします。
3. 次の操作のいずれかを実行します。
   - ログレベルを変更する場合、［エージェントロギングレベル］ドロップダウンリストで、ログレベルをクリックします。

     ログレベルを詳細（verbose）に変更する場合は、CylancePROTECT Desktop デバイスでの詳細ログの有効化を参照してください。
   - CylancePROTECT Desktopのエージェントログファイルを取得するには、［脅威と活動］（［エージェントログ］タブ）の［現在のログファイルをアップロード］をクリックします。このオプションは、デバイスがオンラインの場合にのみ使用できます。

CylancePROTECT Desktop デバイスでの詳細ログの有効化

作業を始める前に： 管理コンソールで、CylancePROTECT Desktop エージェントのログレベルを「詳細」に設定します。

デバイス OS の手順に従います。

OS	手順

Windows	**a.** システムトレイのエージェントアイコンを右クリックして、［終了］をクリックします。
	b. 管理者としてコマンドラインを開きます。
	c. 次のコマンドを実行します。
	`cd C:\Program Files\Cylance\Desktop`
	d. 次のコマンドを実行します。
	`CylanceUI.exe -a`
	e. システムトレイのエージェントアイコンを右クリックし、［ログ］**>**［すべて］をクリックします。

macOS	**a.** 現在実行中のユーザーインターフェイスを終了します。 **b.** Terminal から次のコマンドを実行します。 `sudo /Applications/Cylance/CylancePROTECTUI.app/Contents/MacOS/CylancePROTECTUI.-a` **c.** システムトレイのエージェントアイコンを右クリックし、［ログ］**>**［すべて］を選択します。

Linux のログ

次のセクションでは、ロギングレベルの設定とエージェントログファイルの収集について説明します。

ロギングレベルの設定

設定されるロギングレベルによって、エージェントログの詳細レベルが決まります。詳細ロギングでは、ログファイルのサイズ増加が非常に速くなります。

作業を始める前に： 次のコマンドを使用して、Linux エージェントの現在のロギングレベルを表示できます。

```
/opt/cylance/desktop/cylance -l
```

ロギングレベルを設定するには、次のコマンドを使用します。

```
/opt/cylance/desktop/cylance -L <level>
```

<level> の値には、次のいずれかを指定できます。

- `0`：エラー
- `1`：警告
- `2`：情報

- 3：詳細

たとえば、次のコマンドは、ロギングレベルを「詳細」に設定します。

```
/opt/cylance/desktop/cylance -L 3
```

Linux デバイスからのエージェントログファイルの収集

Linux デバイスからエージェントログファイルを収集するには、次のコマンドを使用します。ログファイルは 30 日間デバイスに保存されます。ログファイルを収集するには、root 権限が必要です。

Red Hat および **CentOS**：

```
ps aux > ~/ps.txtph product="Cylance">sudo pmap -x $(ps -e | grep cylancesvc | cut
 -d ‘ ‘ -f 1) > ~/maps.txt
cat /proc/cpuinfo > ~/cpu.txt
cat /proc/meminfo > ~/mem.txt
cat /proc/mounts > ~/mounts.txt
cat /proc/modules > ~/modules.txt
cat /proc/slabinfo > ~/slabinfo.txt
tar -cvzf cylancelogs-$(date --rfc-3339=’date’).tgz /var/log/messages* /opt/
cylance/desktop/log ~/maps.txt ~/cpu.txt ~/mounts.txt ~/modules.txt ~/ps.txt ~/
mem.txt ~/slabinfo.txt
```

Ubuntu:

```
ps aux > ~/ps.txt
sudo pmap -x $(ps -e | grep cylancesvc | cut -d ‘ ‘ -f 2) > ~/maps.txt
cat /proc/cpuinfo > ~/cpu.txt
cat /proc/meminfo > ~/mem.txt
cat /proc/mounts > ~/mounts.txt
cat /proc/modules > ~/modules.txt
cat /proc/slabinfo > ~/slabinfo.txt
tar -cvzf cylancelogs-$(date --rfc-3339=’date’).tgz /var/log/syslog* /opt/
cylance/desktop/log ~/ps.txt ~/maps.txt ~/cpu.txt ~/mounts.txt ~/modules.txt   ~/
slabinfo.txt  ~/mem.txt
```

Amazon および **SUSE Linux**：

```
ps aux > ~/ps.txt
sudo pmap -x $(ps -e | grep cylancesvc | cut -d ' ' -f 2) > ~/maps.txt
cat /proc/cpuinfo > ~/cpu.txt
cat /proc/meminfo > ~/mem.txt
cat /proc/mounts > ~/mounts.txt
cat /proc/modules > ~/modules.txt
cat /proc/slabinfo > ~/slabinfo.txt
tar -cvzf cylancelogs-$(date --rfc-3339='date').tgz /var/log/messages* /opt/
cylance/desktop/log ~/ps.txt ~/maps.txt ~/cpu.txt ~/mounts.txt ~/modules.txt ~/
slabinfo.txt
```

SIEM ソリューションまたは syslog サーバーへのイベントの送信

セキュリティ情報イベント管理（SIEM）ソフトウェアは、セキュリティデータを複数のソースから収集、分析、集計して、潜在的なセキュリティの脅威を検出します。Cylance Endpoint Security ソリューションによって検出されたイベントは、組織の SIEM ソフトウェアまたは syslog サーバーに送信するように選択できます。SIEM または syslog サーバーに送信されるアラートデータは、管理コンソールに表示されるアラートデータと同じです。Cylance Endpoint Security ソリューションによって報告された特定のイベントの詳細については、『Syslog ガイド』を参照してください。

1. 管理コンソールのメニューバーで、［設定］ > ［アプリケーション］をクリックします。
2. ［**SysLog/SIEM**］チェックボックスをオンにします。
3. 組織の SIEM または syslog インテグレーションに送信するイベントを選択します。各イベントタイプの詳細については、『Syslog ガイド』を参照してください。
4. SIEM または syslog インテグレーションの情報を指定します。詳細については、『Syslog ガイド』を参照してください。
5. ［接続をテスト］をクリックして設定を確認します。
6. ［保存］をクリックします。

Cylance ユーザー API へのアクセスの有効化

Cylance Endpoint Security は、RESTful API のセットである Cylance ユーザー API を使用して、サードパーティプログラムとの統合をサポートします。これにより、組織は Cylance Endpoint Security 設定および構成をプログラムで管理できます。管理者は、統合設定をカスタマイズして、ユーザーが持つ API 権限を制御できます。セキュリティ上、API ユーザーは、管理者が管理コンソールでカスタムアプリケーションを追加するときに生成するアプリケーション ID とアプリケーションシークレットを必要とします。テナントは、最大 10 個のカスタム統合を持つことができます。

詳細については、『Cylance ユーザー API ガイド』を参照してください。

メモ：2022 年 7 月に、Cylance Endpoint Security の既存のテナントに対してセキュリティ強化が導入されました。管理者ロールを持つユーザーは、アプリケーションシークレットが生成された後、アプリケーションシークレットを管理コンソールから完全に削除する新しい機能を有効にすることができます。これにより、アプリケーションシークレットは、Cylance コンソールにアクセスできるどのユーザーによっても表示できなくなります。[設定] > [統合] でこの機能を有効にした場合、管理者がアプリケーションシークレットを生成または再生成したとき、アプリケーションシークレットは、管理者がダイアログを閉じたり、画面から移動したりするまでに限り表示されます。アプリシークレットは、リストに表示されません。既存のアプリケーションシークレットを削除し、この動作を有効にするには、**[**強化されたセキュリティ機能を利用できます**]** を展開し、**[**シークレットを削除**]** をクリックします。この機能を有効にすると、以前に生成されたアプリケーションシークレットは表示できなくなります。この機能を有効にする前に、既存のアプリケーションシークレットを記録しておいてください。コンソールでアプリケーションシークレットが表示される、以前の動作に戻すことはできません。必要に応じて、新しいアプリケーション ID およびシークレットを生成できます。

2022 年 7 月以降に作成された新しい Cylance Endpoint Security テナントに対しては、この機能はデフォルトで有効になっています。

1. 管理コンソールで、［設定］ **>** ［統合］をクリックします。
2. ［アプリケーションを追加］をクリックします。
3. アプリケーションの名前を入力します。
4. アクセスを許可する API 権限を選択します。
5. ［保存］をクリックします。
   アプリケーション ID とアプリケーションシークレットが表示されます。
6. ［**OK**］をクリックします。

Cylance Endpoint Security のトラブルシューティング

このセクションでは、 Cylance Endpoint Security のサービスと機能のトラブルシューティングに関するガイダンスを提供します。

BlackBerry サポート収集ツールの使用

BlackBerry サポートと一緒に問題解決に取り組む場合は、 BlackBerry サポート収集ツールをダウンロードして、製品データとシステム情報を収集してください。詳細については、support.blackberry.com にアクセスし、記事 66596 を参照してください。

問題の報告機能の使用

CylanceGATEWAY エージェントと CylancePROTECT Mobile アプリには問題の報告オプションが組み込まれており、ユーザーはこれを使用して、IT 管理者に連絡してトラブルシューティングの支援を求めずに、問題レポートとエージェントログファイルを BlackBerry に送信できます。BlackBerry では、トラブルシューティングについて IT 管理者に問い合わせてからレポートおよびエージェントログファイルを BlackBerry に送信するようにユーザーに指示することをお勧めします。詳細については、「CylanceGATEWAY エージェント設定」および「BlackBerry への問題の報告」を参照してください。

BlackBerry Connectivity Node ソフトウェアの Cylance Endpoint Security からの削除

アンインストールアプリケーションを使用すると、インストールされているサーバーから BlackBerry Connectivity Node ソフトウェアを削除できます。BlackBerry Connectivity Node をアンインストールしても、Cylance Endpoint Security 管理コンソールからは削除されません。したがって、後で BlackBerry Connectivity Node ソフトウェアを再インストールする場合は、まず管理コンソールから BlackBerry Connectivity Node インスタンスを削除する必要があります。

BlackBerry Connectivity Node ソフトウェアを削除するには、次の操作を実行します。

手順	アクション
1	ローカルサーバーから BlackBerry Connectivity Node ソフトウェアを削除します。
2	削除するすべてのディレクトリ接続に関連付けられているすべての Active Directory ユーザーを削除します。
3	削除するすべてのディレクトリ接続に関連付けられているユーザーグループを削除します。

手順	アクション
4	Cylance Endpoint Security 管理コンソールから BlackBerry Connectivity Node インスタンスを削除します。

BlackBerry Connectivity Node ソフトウェアのローカルサーバーからの削除

トラブルシューティングを行う場合は、ソフトウェアのアンインストール前に `\Program Files\BlackBerry\BlackBerry Connectivity Node - UES\Logs` をバックアップしておきます。

1. タスクバーで、［スタート］ > ［コントロールパネル］ > ［プログラム］ > ［プログラムと機能］をクリックします。
2. ［**BlackBerry Connectivity Node - UES**］を選択します。
3. ［アンインストール］をクリックします。
4. ［次へ］をクリックします。
5. ［閉じる］をクリックします。
6. コンピュータを再起動すると、BlackBerry Connectivity Node ソフトウェアの削除が完了します。

Cylance Endpoint Security 管理コンソールからの BlackBerry Connectivity Node インスタンスの削除

BlackBerry Connectivity Node のインスタンスをアンインストールした場合、次の手順でインスタンスのデータを Cylance Endpoint Security データベースから削除する必要があります。削除しないと、BlackBerry Connectivity Node のエントリが Cylance Endpoint Security 管理コンソールにそのまま残り、「一時停止」のステータスが表示されます。

作業を始める前に：

- BlackBerry Connectivity Node ソフトウェアはローカルサーバーから削除してください。
- インスタンスを削除する権限を持つユーザーとしてサインインしていることを確認してください。デフォルトは、セキュリティ管理者ロールまたはエンタープライズ管理者ロールです。

1. 管理コンソールのメニューバーで、［設定］ > ［ディレクトリ接続］ > ［**Connectivity Node**］の順にクリックします。
2. ［**Connectivity Node**］タブをクリックします。
3. 削除する BlackBerry Connectivity Node の横にある をクリックします。
4. ［削除］をクリックします。

CylancePROTECT Desktop のトラブルシューティング

このセクションでは、CylancePROTECT Desktop の問題のトラブルシューティングと解決に役立つ情報を提供します。

デバイスからの CylancePROTECT Desktop エージェントの削除

作業を始める前に：

- CylancePROTECT Desktop エージェントを削除するデバイスに、設定が有効になっていないデバイスポリシーを割り当てます。ポリシーで、［保護設定］ > ［デバイスからのサービスシャットダウンを防止］および［アプリケーション制御］がオフになっていることを確認します
- CylancePROTECT Desktop エージェントの削除の際に、パスワードを入力するようにユーザーに要求する場合は、パスワードは、メモに書き留めるようにします。

1. デバイスからエージェントを削除するには、次のいずれかの方法を使用します。

   Windows

   - CylancePROTECT Desktop を手動で削除するには、［プログラムの追加と削除］を使用します。アンインストールパスワードが必要な場合は、パスワード保護コマンドとともに以下のコマンドラインの指定を使用する必要があります。
   - 管理者としてコマンドプロンプトを実行し、次のいずれかのコマンドを使用します。
     - CylancePROTECTSetup.exe:

       ```
       CylancePROTECTSetup.exe /uninstall
       ```

     - CylancePROTECT_x64.msi 標準：

       ```
       msiexec /uninstall CylancePROTECT_x64.msi
       ```

     - CylancePROTECT_x64.msi Windows インストーラ：

       ```
       msiexec /x CylancePROTECT_x64.msi
       ```

     - CylancePROTECT_x86.msi 標準：

       ```
       msiexec /uninstall CylancePROTECT_x86.msi
       ```

     - CylancePROTECT_x86.msi Windows インストーラ：

       ```
       msiexec /x CylancePROTECT_x86.msi
       ```

     - 製品 ID GUID 標準：

       ```
       msiexec /uninstall {2E64FC5C-9286-4A31-916B-0D8AE4B22954}
       ```

     - 製品 ID GUID Windows インストーラ：

       ```
       msiexec /x {2E64FC5C-9286-4A31-916B-0D8AE4B22954}
       ```

   オプションのコマンド：

   - 簡易アンインストール：

     ```
     /quiet
     ```

   - 簡易および非表示：

     ```
     /qn
     ```

   - パスワード保護：

     ```
     UNINSTALLKEY="<パスワード>"
     ```

- 自動隔離済みファイル：

  ```
  QUARANTINEDISPOSETYPE=<0 または 1>
  ```

  - 0 はすべてのファイルを削除
  - 1 はすべてのファイルを復元
- アンインストールログファイルの生成：

  ```
  /Lxv* <ファイル名を含めたパス>
  ```

macOS

次のコマンドを実行します。

```
sudo /Applications/Cylance/Uninstall\ CylancePROTECT.app/Contents/MacOS/
Uninstall\ CylancePROTECT
```

アンインストールパスワードが必要な場合は、次のパラメーターを追加します。

```
--password=<パスワード>
```

Linux

a. エージェントをアンインストールするには、次のいずれかのコマンドを使用します。

- RHEL/CentOS:

  ```
  rpm -e $(rpm -qa | grep -i cylance)
  ```
- Ubuntu/Debian:

  ```
  dpkg -P cylance-protect cylance-protect-ui cylance-protect-driver cylance-
  protect-open-driver
  ```
- Amazon Linux 2/SUSE:

  ```
  rpm -e $(rpm -qa | grep -i cylance)
  ```

b. Linux エージェントドライバをアンインストールするには、次のいずれかのコマンドを使用します。

- RHEL/CentOS:

  ```
  rpm -e CylancePROTECTDriver CylancePROTECTOpenDriver
  ```
- Ubuntu/Debian:

  ```
  dpkg -P cylance-protect-driver cylance-protect-open-driver
  ```
- Amazon Linux 2:

  ```
  rpm -e CylancePROTECTDriver-<パッケージバージョン>.amzn2.x86_64
  rpm -e CylancePROTECTOpenDriver-<パッケージバージョン>.amzn2.86_64
  ```

2. 管理コンソールの［アセット］**>**［デバイス］でデバイスを選択し、［削除］をクリックします。［はい］をクリックして確定します。

Linux エージェントの再登録

何らかの理由でエージェントがコンソールから登録解除された場合、ユーザーがトークンを使用してデバイスを再登録する必要があります。次のいずれかのコマンドを使用して、デバイスを再度登録します。token は、テナントからのインストールトークンに置き換えます。

Red Hat、**CentOS**、および **Ubuntu**：

```
/opt/cylance/desktop/cylance --register=token
```

CentOS の場合は、次のコマンドを使用することもできます。

```
/opt/cylance/desktop/cylance --r=token
```

Amazon および **SUSE Linux**：

```
/opt/cylance/desktop/cylance -r token
```

CylancePROTECT Desktop の更新、ステータス、および接続の問題のトラブルシューティング

CylancePROTECT Desktop の更新、ステータス、および接続の問題をトラブルシューティングするときは、次の点を考慮してください。

- 「CylancePROTECT Desktop エージェントのステータスアイコン」を確認します。
- ファイアウォールポート 443 が開いており、デバイスが BlackBerry サイトを解決して接続できることを確認します。
- 管理コンソールでデバイス情報を確認します。デバイスがオンラインかオフラインか、および最後に接続された時刻を確認します。
- インターネットに接続するためにデバイスでプロキシが使用されているかどうか、および資格情報がプロキシで正しく設定されているかどうかを確認します。
- Cylance サービスを再起動して、コンソールへの接続を試みます。
- デバッグログを収集します。「CylancePROTECT Desktop エージェントのログの管理」を参照してください。
- 問題が発生したときのシステム情報の出力を収集します。
  - Windows：msinfo32 または winmsd
  - macOS：システム情報

Linux デバイスで多数の DYLD インジェクション違反が報告されている

考えられる原因

Splunk、Dynatrace、AppDynamics、DataDog など一部のサードパーティアプリケーションはモジュール（プロセスの LD_PRELOAD 環境変数）をプリロードしようとするため、アプリケーションが監視しているプロセスについて DYLD インジェクション違反イベントが発生します。

解決策

次の手順に従います。

1. 2.1.1574 より前のバージョンの CylancePROTECT Desktop エージェントを使用している場合は、2.1.1574 以降にアップグレードします。BlackBerry では、最新の拡張機能を利用できるようにエージェントを最新バージョンにアップグレードすることを強くお勧めします。
2. サードパーティアプリケーションが注入を試みる .so コンポーネントについてメモリ保護の除外を追加します。LD_PRELOAD 変数を調べて、除外を追加する必要がある .so コンポーネントを特定します（「man ld.so」で簡単なガイダンスを取得できます）。ベストプラクティスは、サードパーティアプリケーションのサポートリソースに該当する .so ファイルを問い合わせることです。

CylancePROTECT Desktop のタイムゾーンの差異

CylancePROTECT Desktop の日付と時刻の情報を表示する場所によっては、使用するタイムゾーンが異なる場合があります。

この UI に表示される日時	使用されるタイムゾーン
CylancePROTECT Desktop エージェント（イベント通知とエージェントログを含む）	ローカルマシンのタイムゾーン。
管理コンソール（［レポート］タブとエクスポートされたデータを除く）	コンソールを使用している管理者のタイムゾーン。
管理コンソールの［レポート］タブ	コンソールを使用している管理者のタイムゾーン。 レポートをエクスポートすると、エクスポートで UTC タイムゾーンが使用されます。
Syslog イベント	UTC タイムゾーン。
脅威データレポート、および管理コンソールからエクスポートされたデータ	UTC タイムゾーン。

サードパーティのセキュリティ製品で CylancePROTECT Desktop を使用する場合のフォルダの除外

サードパーティのセキュリティ製品と CylancePROTECT Desktop を併用する場合は、Cylance ディレクトリを除外するように構成して CylancePROTECT Desktop との同時実行が問題なく行えるようにしておく必要があります。

Windows で除外する **CylancePROTECT** のディレクトリ、ファイル、プロセス

Windows のバージョン	パス
Windows（すべてのバージョン）	C:\Program Files\Cylance C:\ProgramData\Cylance C:\Documents and Settings\All Users\Application Data\Cylance\Desktop\q C:\Windows\System32\Drivers\CyProtectDrv*.sys C:\Windows\System32\Drivers\CyDevFlt*.sys C:\Windows\System32\Drivers\CylanceDrv*.sys C:\Windows\CyProtect.cache C:\Windows\CylanceUD.cache C:\Windows\Temp\CylanceDesktopArchive C:\Windows\Temp\CylanceDesktopRemoteFile C:\Program Files\Cylance\Desktop\CylanceSvc.exe C:\Program Files\Cylance\Desktop\CylanceUI.exe C:\Program Files\Cylance\Desktop\CyUpdate.exe C:\Program Files\Cylance\Desktop\LocalePkg.exe

macOS で除外する **CylancePROTECT** ディレクトリ

macOS バージョン	パス
macOS X（10.9〜10.11）、macOS 10.12 以降	/Library/Application Support/Cylance/Desktop/q /Library/Application Support/Cylance/ /System/Library/Extensions/CyProtectDrvOSX.kext/ /private/tmp/CylanceDesktopArchive /private/tmp/CylanceDesktopRemoteFile

Linux で除外する **CylancePROTECT** ディレクトリ

プロキシ設定に関連するパスはオプションで除外できます。これらは、CylancePROTECT 用にプロキシの上書きが設定されている場合にのみ必要です。

Linux のバージョン	パス
Amazon Linux	CylancePROTECT ： /opt/cylance /usr/src/CyProtectDrv-1.2 /tmp/CylanceDesktopArchive /tmp/CylanceDesktopRemoteFile /lib/modules/*/extra/CyProtectDrv.ko /etc/sysconfig/modules/cylance.modules /etc/modprobe.d/cylance.conf /etc/init/cylancesvc.conf /etc/dbus-1/system.d/com.cylance.agent_server.conf /var/run/cylancesvc.pid プロキシ設定（必要な場合のみ）： /etc/init/cylancesvc.override CylanceUI: Amazon Linux では使用できません。
Amazon Linux 2 Amazon Linux 2023	CylancePROTECT ： /opt/cylance /usr/src/CyProtectDrv-1.2 /tmp/CylanceDesktopArchive /tmp/CylanceDesktopRemoteFile /lib/modules/*/extra/CyProtectDrv.ko /etc/sysconfig/modules/cylance.modules /etc/modprobe.d/cylance.conf /usr/lib/systemd/system/cylancesvc.service /etc/dbus-1/system.d/com.cylance.agent_server.conf /var/run/cylancesvc.pid プロキシ設定（必要な場合のみ）： /etc/systemd/system/cylancesvc.service.d/proxy.conf CylanceUI: Amazon Linux 2 または Amazon 2023 では使用できません。

Linux のバージョン	パス

RHEL/CentOS 6.x	CylancePROTECT：
	`/opt/cylance`
	`/usr/src/CyProtectDrv-1.2`
	`/tmp/CylanceDesktopArchive`
	`/tmp/CylanceDesktopRemoteFile`
	`/lib/modules/*/extra/CyProtectDrv.ko`
	`/etc/sysconfig/modules/cylance.modules`
	`/etc/modprobe.d/cylance.conf`
	`/etc/init/cylancesvc.conf`
	`/etc/dbus-1/system.d/com.cylance.agent_server.conf`
	`/var/run/cylancesvc.pid`
	プロキシ設定（必要な場合のみ）：
	`/etc/init/cylancesvc.override`
	CylanceUI:
	`/etc/xdg/autostart/cylance-protect.desktop`
	`/usr/share/applications/cylance-protect.desktop`

Linux のバージョン	パス
RHEL/CentOS 7.x、8.x Oracle Linux7、8、9	CylancePROTECT ： /opt/cylance /usr/src/CyProtectDrv-1.2 /tmp/CylanceDesktopArchive /tmp/CylanceDesktopRemoteFile /lib/modules/*/extra/CyProtectDrv.ko /etc/sysconfig/modules/cylance.modules /etc/modprobe.d/cylance.conf /usr/lib/systemd/system/cylancesvc.service /etc/dbus-1/system.d/com.cylance.agent_server.conf /var/run/cylancesvc.pid プロキシ設定（必要な場合のみ）： /etc/systemd/system/cylancesvc.service.d/proxy.conf CylanceUI: /etc/xdg/autostart/cylance-protect.desktop /usr/share/applications/cylance-protect.desktop /usr/share/gnome-shell/extensions/cylance-protect@cylance.com
SUSE（SLES）11.x	CylancePROTECT： /opt/cylance /usr/src/CyProtectDrv-1.2 /tmp/CylanceDesktopArchive /tmp/CylanceDesktopRemoteFile /lib/modules/*/extra/CyProtectDrv.ko /etc/modprobe.d/cylance.conf /etc/init.d/cylancesvc /etc/dbus-1/system.d/com.cylance.agent_server.conf /var/run/cylancesvc.pid CylanceUI: /etc/xdg/autostart/cylance-protect.desktop /usr/share/applications/cylance-protect.desktop

Linux のバージョン	パス
SUSE（SLES）12 SP1、SP2、SP3、SP4 SUSE（SLES）15	CylancePROTECT： /opt/cylance /usr/src/CyProtectDrv-1.2 /tmp/CylanceDesktopArchive /tmp/CylanceDesktopRemoteFile /lib/modules/*/extra/CyProtectDrv.ko /etc/sysconfig/modules/cylance.modules /etc/modprobe.d/cylance.conf /usr/lib/systemd/system/cylancesvc.service /etc/dbus-1/system.d/com.cylance.agent_server.conf /var/run/cylancesvc.pid プロキシ設定（必要な場合のみ）： /etc/systemd/system/cylancesvc.service.d/proxy.conf CylanceUI: /etc/xdg/autostart/cylance-protect.desktop /usr/share/applications/cylance-protect.desktop /usr/share/gnome-shell/extensions/cylance-protect@cylance.com
Ubuntu LTS/Xubuntu 14.04	CylancePROTECT： /opt/cylance /usr/src/CyProtectDrv-1.2 /tmp/CylanceDesktopArchive /tmp/CylanceDesktopRemoteFile /lib/modules/*/extra/CyProtectDrv.ko /etc/modprobe.d/cylance.conf /etc/init/cylancesvc.conf /etc/dbus-1/system.d/com.cylance.agent_server.conf /var/run/cylancesvc.pid プロキシ設定（必要な場合のみ）： /etc/init/cylancesvc.override CylanceUI： /usr/share/applications/cylance-protect.desktop /etc/xdg/autostart/cylance-protect.desktop

Linux のバージョン	パス

Ubuntu LTS/Xubuntu 16.04、18.04、20.04
Debian 10、11
	CylancePROTECT：
	`/opt/cylance`
	`/usr/src/CyProtectDrv-1.2`
	`/tmp/CylanceDesktopArchive`
	`/tmp/CylanceDesktopRemoteFile`
	`/lib/modules/*/extra/CyProtectDrv.ko`
	`/etc/modprobe.d/cylance.conf`
	`/lib/systemd/system/cylancesvc.service`
	`/etc/dbus-1/system.d/com.cylance.agent_server.conf`
	`/var/run/cylancesvc.pid`
	プロキシ設定（必要な場合のみ）：
	`/etc/systemd/system/cylancesvc.service.d/proxy.conf`
	CylanceUI:
	`/usr/share/applications/cylance-protect.desktop`
	`/etc/xdg/autostart/cylance-protect.desktop`

Linux ドライバがロードされていません。ドライバパッケージをアップグレードします。

原因

デバイス上の CylancePROTECT Desktop ドライバに Linux カーネルとの互換性がありません。

解決策

次のいずれかのシナリオに基づいて Linux ドライバを更新してください。

項目	説明
デバイスがバージョン 3.1 以降のエージェントを実行している場合	次の操作のいずれかを実行します。 • Linux ドライバを自動的に更新するようにゾーン更新ルールを設定します。 • Linux ドライバを手動で更新します。
デバイスがエージェント 2.1.1590 以降（3.0 以前）を実行している場合	• Linux ドライバを手動で更新します。

CylanceOPTICS のトラブルシューティング

このセクションでは、CylanceOPTICS の問題のトラブルシューティングと解決に役立つ情報を提供します。

Linux 上の CylanceOPTICS エージェントの問題のトラブルシューティング

問題	解決策
kernel-header と kernel-devel パッケージがカーネルと一致しない。	yum update kernel を使用して、デバイスを再起動します。 再起動できない場合は、次のいずれかのコマンドを使用します。 • RHEL/CentOS または Amazon Linux 2 : `yum install kernel-headers-`uname -r` kernel-devel-`uname -r`` • Ubuntu : `sudo apt-get install linux-headers -$(uname -r)`
デバッグロギングを有効にすると、「Corroborator found a match for PID...」メッセージがログに記録される。	このメッセージは想定されたもので、バグや他の問題を示すものではありません。

デバイスからの CylanceOPTICS エージェントの削除

デバイスから CylanceOPTICS エージェントをアンインストールすると、CylanceOPTICS によって保存されたローカルデータおよびログファイルも削除されます。CylancePROTECT エージェントをアンインストールする場合には、その前に CylanceOPTICS エージェントをアンインストールする必要があります。

エージェントをアンインストールするには、OS で使用可能な標準のアンインストールオプションを使用します（たとえば、Windows の場合には［プログラムの追加と削除］、macOS の場合には Finder > ［アプリケーション］によるアンインストールなど）。または、Cylance Endpoint Security の設定に関するコンテンツに記載されている OS コマンドを使用して CylanceOPTICS エージェントをアンインストールします。

Windows で、OS コマンドを使用してエージェントをアンインストールする場合、ユーザーはローカルシステムが所有するファイルとディレクトリの所有権を取得する必要があります。Windows 用の CylanceOPTICS エージェントのサービスシャットダウン防止機能を（デバイスポリシーの保護設定で）有効にしていた場合、CylanceOPTICS エージェントの削除を試行する前にこの機能をオフにするか、この機能が有効になっていない別のデバイスポリシーを割り当てる必要があります。

エージェントをアンインストールした後で、デバイスを再起動することをお勧めします。

CylanceOPTICS エージェントの macOS デバイスからの削除

CylanceOPTICS エージェントが削除されたことの確認

次のコマンドを実行します。

```
kextstat | grep -i cyoptic
```

macOS Big Sur（11.x）の場合は、次のコマンドも実行します。

```
systemextensionsctl list | grep -i cyoptics
```

コマンドは何も出力しないはずです。

次のパスとファイルがシステムに存在しないことを確認します。

- /Library/Application Support/Cylance/Optics
- /Library/Application Support/OpticsUninstall
- /Applications/Cylance/Optics
- /Library/LaunchDaemons/com.cylance.cyoptics_service.plist
- /Library/LaunchDaemons/com.cylance.optics.postuninstall.plist
- /Library/LaunchDaemons/com.cylance.cyopticsesfservice.plist

macOS Big Sur（11.x）デバイスでは、**ssh** セッションを使用して **CylanceOPTICS** エージェントをサイレントアンインストールした後も、「**/Applications/Cylance/Optics/CyOpticsESFLoader.app**」はそのまま残り、システム拡張機能がアクティブのままです

この問題は、 Apple に、エンドユーザーによる明示的な確認なしにシステム拡張機能をサイレントアンインストールする仕組みがないために発生します。

この問題を解決するには、ファインダーを使用して CyOpticsESFLoader.app を見つけ、ゴミ箱にドラッグしてから、システム拡張機能を無効化して削除する UI プロンプトを確認します。

ファイルをゴミ箱にドラッグしたときに権限エラーが発生した場合は、次のコマンドを実行して CylancePROTECT Desktop を一時的に無効にします。

```
sudo launchctl unload /Library/LaunchDaemons/com.cylance.agent_service.plist
```

コマンドを実行した後、ファイルをゴミ箱にドラッグして UI プロンプトを確認してください。CylancePROTECT Desktop をアクティブなままにする場合は、デバイスを再起動します。

メモ： CyOpticsESFLoader.app は、デバイスから CylancePROTECT Desktop エージェントを削除する前に、この方法で削除する必要があります。このタスクを完了する前に CylancePROTECT Desktop エージェントを削除すると、そのデバイスから CyOpticsESFLoader.app も含めて /Applications/Cylance が削除されるため、それを手動で削除してシステム拡張機能を無効にすることができません。

商標などに関する情報

該当する特許は、次の場所で確認できます：www.blackberry.com/patents。

本書は、参照用として本書で取り上げるすべての文書（提供される文書または BlackBerry の Web サイトで参照可能な文書）を含めて「現状のまま」または「参照可能な形で」提供されるか、またはアクセスすることができ、BlackBerry Limited およびその関連会社（「BlackBerry」）はいかなる条件付け、承認、表明、または保証もしないものとし、BlackBerry は本書の誤記、技術的な誤りまたはその他の誤り、エラー、遺漏について何ら責任を負いません。BlackBerry の所有権、機密情報および/または企業秘密を保護するため、本書では一部の BlackBerry テクノロジの側面を一般化された用語で記述している場合があります。BlackBerry は、本書に含まれる情報を定期的に変更する権利を留保します。ただし、BlackBerry には、本書への変更、更新、拡張、または他の追加を適時ユーザーに提供する義務はないものとします。

本書は、第三者をソースとする情報、ハードウェアまたはソフトウェア、製品またはサービス（コンポーネントや、著作権保護されたコンテンツなど）、および/または第三者の Web サイト（これらをまとめて「サードパーティ製品およびサービス」という）への参照を含んでいる可能性があります。BlackBerry は、サードパーティ製品およびサービスの内容、正確性、著作権遵守、互換性、性能、信頼性、適法性、品格、リンク、他の側面などに限定することなく、サードパーティ製品およびサービスを一切管理することはなく、責任も負いません。本書においてサードパーティ製品およびサービスを参照することは、BlackBerry がサードパーティ製品およびサービスまたは第三者を保証することを意味するものではありません。

該当する司法管轄地域の適用法で明確に禁じられている場合を除き、本書で参照されているソフトウェア、ハードウェア、サービス、またはサードパーティ製品およびサービスについて、耐久性、特定の目的または使用に対する適合、商品性、適性品質、権利侵害の不存在、品質満足度、権原、または制定法、慣習法、取引過程、商慣習から生じる、本書またはその使用に関する、または性能または性能の不履行に関する条件付け、承認、表明、保証などに限定することなく、明示的または黙示的に、いかなる条件付け、承認、表明、または保証も除外されます。ユーザーは、国や地域によって異なる他の権利を有する場合もあります。一部の司法管轄地域では、黙示的な保証および条件の除外事項または限定事項は禁止されています。法律で認められている範囲で、本書に関連する黙示的な保証または条件は、上記に定めるように除外できないが限定できる場合、ユーザーが本書または該当する対象物を初めて入手してから 90 日間に限定されます。

該当する司法管轄地域の適用法で認められている最大限の範囲で、本書またはその使用に関連して、または本書で参照されているソフトウェア、ハードウェア、サービス、またはサードパーティ製品およびサービスの性能または性能の不履行に関連して、直接的、必然的、典型的、偶発的、間接的、特殊的、懲罰的、または加重的損害、金銭的損失による損害（利益または収益の損失、予想される貯蓄の未達成、事業の中断、ビジネス情報の消失、ビジネス機会の喪失、データの破損または消失、データの送受信の失敗、BlackBerry 製品またはサービスと併用したアプリケーションに関連する問題、ダウンタイムコスト、BlackBerry 製品またはサービスあるいはその一部の使用機会や通信サービスの使用機会の喪失、代替品コスト、保険料、設備費、保守費、資本コストなど）に限定することなく、損害を予想できたかどうかを問わず、BlackBerry が損害の可能性について勧告を受けていた場合を含め、いかなる場合においても、BlackBerry はいかなる損害の責任も負わないものとします。

該当する司法管轄地域の適用法で認められている最大限の範囲で、契約、不法行為、またはユーザーに対する過失責任または厳格責任について、BlackBerry は他のいかなる義務、責務、または責任も負わないものとします。

本書の限定事項、除外事項、および免責事項は、（A）訴訟原因、請求、またはユーザーによる行為（契約違反、過失、不法行為、厳格責任、その他の法理論など）の性質に関係なく、この契約の基本目的または本書に記載されている救済策の根本的違反または不履行を免れるため、（B）BlackBerry およびその関連会社、その後継

者、譲受人、代理業者、納入業者（通信事業者を含む）、認可された BlackBerry 販売業者（通信事業者を含む）およびその取締役、従業員、および請負業者に適用されます。

上記に定める限定事項および除外事項に加えて、いかなる場合においても、BlackBerry の取締役、従業員、代理業者、販売業者、納入業者、請負業者または BlackBerry の関連会社は、本書に起因または関連する責任を負わないものとします。

ユーザーは、サードパーティ製品およびサービスの加入、インストール、または使用前に、通信事業者がサードパーティ製品およびサービスのすべての機能をサポートすることに同意していることを確認する責任を負います。一部の通信事業者は、BlackBerry® Internet Service への加入によるインターネット閲覧機能を提供しない場合があります。サービスの利用、ローミング、サービスプラン、その他の機能については、通信事業者に問い合わせてください。BlackBerry 製品およびサービスにおけるサードパーティ製品およびサービスのインストールまたは使用には、第三者の権利を侵害または妨害しないように、特許、商標、著作権、または他のライセンスが必要になる場合があります。ユーザーは、サードパーティ製品およびサービスを使用するかどうかを決定し、使用するためにサードパーティライセンスが必要かどうかを確認する責任を負います。必要な場合、ユーザーはライセンスを取得する責任を負います。ユーザーは、必要なライセンスをすべて取得するまで、サードパーティ製品およびサービスをインストールまたは使用してはなりません。BlackBerry 製品およびサービスで提供されるサードパーティ製品およびサービスは、ユーザーの便宜のために「現状のまま」提供され、BlackBerry は明示的にも黙示的にもいかなる条件付け、承認、表明、または保証もしないものとし、BlackBerry はそれに関連するいかなる責任も負わないものとします。ユーザーによるサードパーティ製品およびサービスの使用は、ライセンスまたは BlackBerry との他の契約で明示的に対象になっている場合を除き、個別のライセンスおよび第三者との他の該当契約の条件に従うものとし、その制約を受けるものとします。

BlackBerry 製品またはサービスの使用条件は、個別のライセンスまたは BlackBerry との他の該当契約に定められています。本書の内容は、本書以外に BlackBerry 製品またはサービスの一部に対して BlackBerry が提供した文書による明示的な契約または保証を破棄するものではありません。

BlackBerry Enterprise Software には、特定のサードパーティ製ソフトウェアが組み込まれています。このソフトウェアに関連するライセンスおよび著作権情報は、http://worldwide.blackberry.com/legal/thirdpartysoftware.jsp でご確認いただけます。

BlackBerry Limited
2200 University Avenue East
Waterloo, Ontario
Canada N2K 0A7

BlackBerry UK Limited
Ground Floor, The Pearce Building, West Street,
Maidenhead, Berkshire SL6 1RL
United Kingdom

Published in Canada