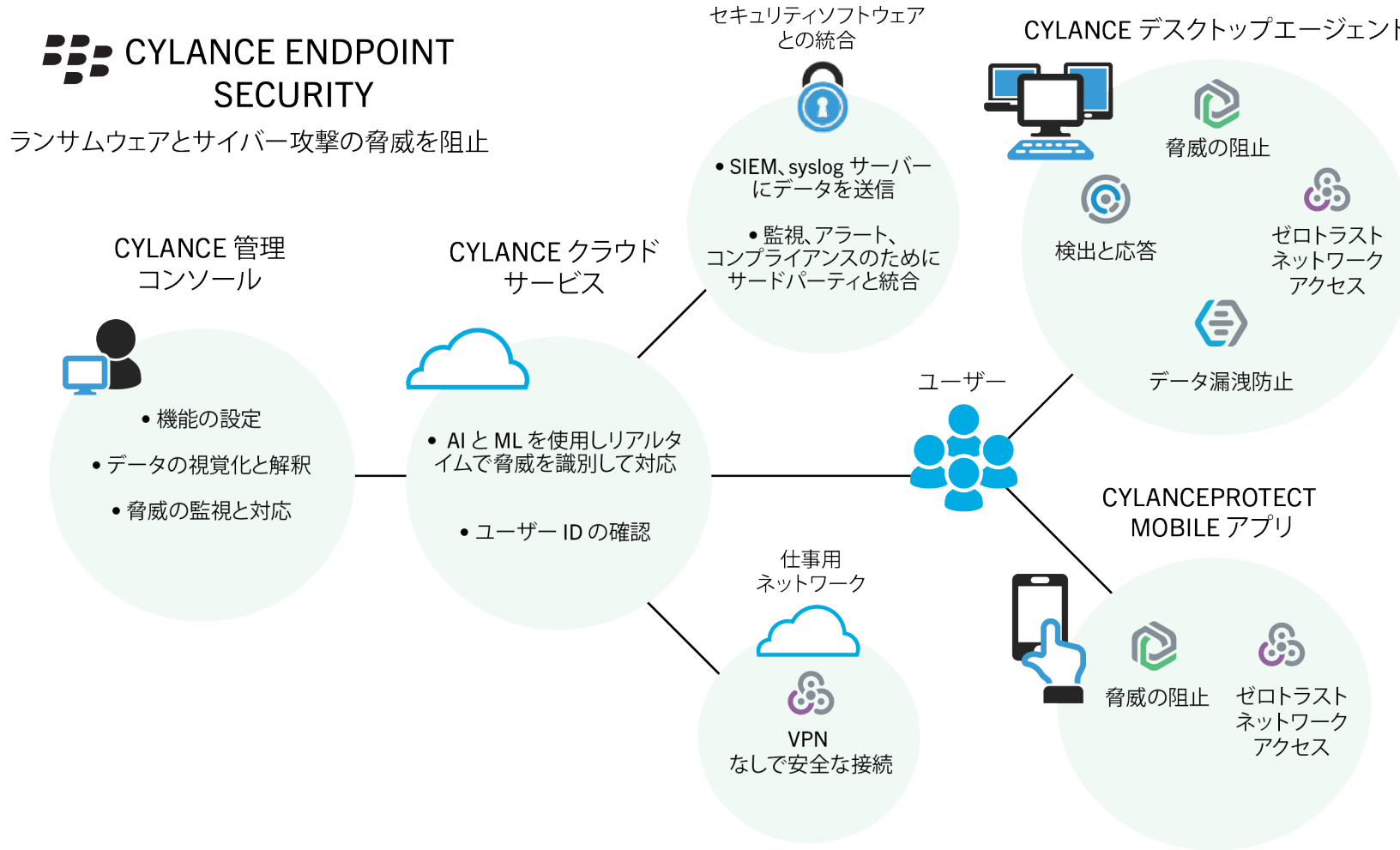
# Cylance Endpoint Security

概要とアーキテクチャ

# Contents

# Cylance Endpoint Security とは




Cylance Endpoint Security は、新たな現実に対応する統合エンドポイントセキュリティソリューションです。すべてのエンドポイントで脅威を検出、保護、修復するための、最適な AI 駆動ツールを統合します。今日のサイバー犯罪者は、人工知能（AI）を使用して攻撃のリーチと影響を最大化する高度な脅威を生み出しています。それに対抗するソリューションも、機械学習と AI の力を活用する必要があります。Cylance Endpoint Security は、デバイス、ネットワーク、アプリ、ユーザーの種類を問わず、ゼロトラストのための AI ベースのソリューションを提供します。

ゼロトラストアプローチは、ネットワークセキュリティを最新化しながら、エンドユーザーのネットワーク体験を強化し、向上させます。ゼロトラストセキュリティモデルは、デフォルトでは仕事用ネットワーク内のユーザーを含め、何も、誰も信頼しません。すべてのユーザー、エンドポイント、およびネットワークは、潜在的に敵対的であると見なされます。ゼロトラストセキュリティでは、ユーザーの身元、アクセスが許可されていること、接続先のネットワークが侵害されていないこと、自身の行動およびデバイスに隠れているマルウェアの動作に悪意がないことを証明するまで、ユーザーは何にもアクセスできません。

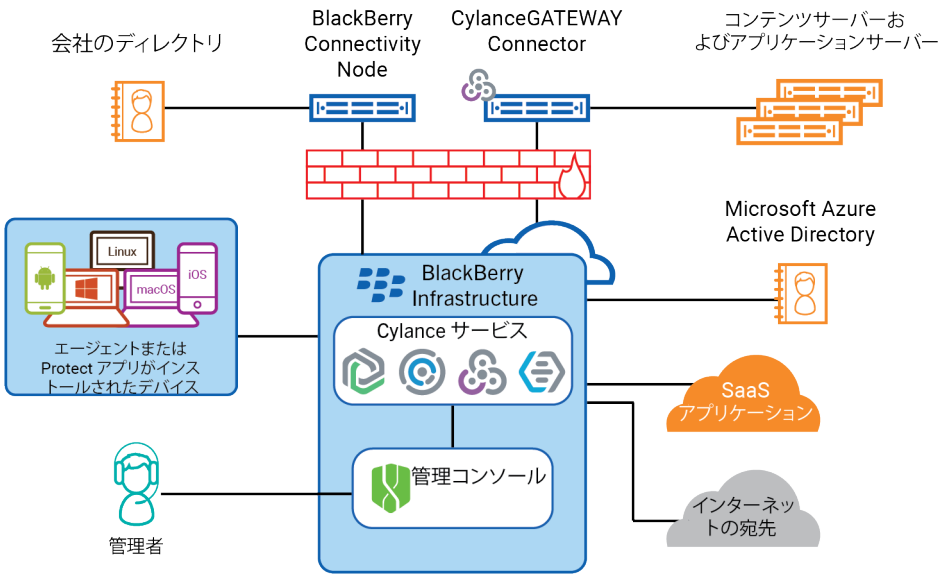
# Cylance Endpoint Security の主な機能

Cylance Endpoint Security は、相互接続されたいくつかの機能を通じて、幅広いセキュリティ機能を提供します。

| 機能 | 説明 |
| --- | --- |
| 脅威（ランサムウェア、マルウェアなど）の検出とブロック | CylancePROTECT Desktop は、マルウェアの識別に数学的手法を使用して、Windows、macOS、Linux デバイス上のランサムウェアおよび他のマルウェアをブロックします。また、事後対応型シグニチャ、信頼ベースシステム、サンドボックスではなく、機械学習技術を使用して、新しいランサムウェア、マルウェア、ウイルス、ボット、将来のバリアントを無効にするエンドポイントの検出と応答を提供します。CylancePROTECT Desktop は、OS レイヤおよびメモリレイヤのランサムウェアや他のマルウェアの潜在的なファイル実行を分析して、悪意のあるペイロードの配信を防止します。 |
| モバイルデバイスの保護 | CylancePROTECT Mobile は、iOS、Android、Chrome OS デバイスに対するモバイル脅威の防御を提供します。マルウェアの識別に加え、CylancePROTECT Mobile では、サイドロードされたアプリ、テキストメッセージ内の悪意のある URL などのセキュリティリスクも検出し、脅威を排除するための具体的なアクションを推奨します。 |
| 攻撃の検出と応答 | CylanceOptics は、Windows、macOS、Linux デバイスを監視し、組織が攻撃を受けている可能性がある場合に通知します。CylanceOPTICS は、デバイスから情報を収集し、クラウドサービスを使用して情報を集約し、悪意のあるイベントが発生するとすぐに追跡、警告、対応を行います。CylanceOPTICS では、攻撃が実行される前にそれを阻止し、攻撃に対する調査と応答を自動化できます。 |
| ネットワークとクラウドベースのサービスへの安全なアクセス | CylanceGATEWAY は、ユーザーの iOS、Android、Windows、 および macOS デバイスにゼロトラストネットワークアクセス（ZTNA）を提供して、拡張ネットワーク境界へのユーザーアクセスの安全を確保し、拡張ネットワークを脅威から守ります。CylanceGATEWAY は、デバイスがネットワークに接続されていない場合でも、デバイスから到達されるのを防ぎたいインターネットの宛先への接続をブロックできるようにすることで、デバイスを保護します。また CylanceGATEWAY は、許可されたユーザーのみにアクセスを許可することで、プライベートネットワークとクラウドベースのサービスを保護します。 |
| 機密データの保護 | CylanceAVERT は、組織の環境内の Windows デバイスにある機密データを特定して分類し、機密ファイルのインベントリを作成しておき、窃盗イベントに機密データが関係していた場合、指定されたユーザーに通知します。CylanceAVERT は、USB デバイスにコピーされたファイル、ブラウザロケーションやネットワークドライブへのアップロード、電子メールメッセージの本文コンテンツや添付ファイルに対するスキャンをして、修復アクションの推奨をすることができます。 |

| 機能 | 説明 |
| --- | --- |
| あらゆる UEM や MDM プラットフォームとの連携 | Cylance Endpoint Security は、BlackBerry UEM と連携させることで最高レベルのエンドポイント管理とセキュリティを提供し、さまざまな脅威から組織を保護できます。<br><br>BlackBerry UEM 以外の統合エンドポイント管理（UEM）やモバイルデバイス管理（MDM）プラットフォームを使用している場合は、Cylance Endpoint Security を使用して、エンドポイントとネットワーク間を移動するデータおよびエンドポイントの保護を強化できます。いずれは、UEM や Microsoft Intune などの MDM ソリューションとの特定の統合が Cylance Endpoint Security に追加され、潜在的な脅威に応じてデバイスを管理する機能が強化される予定です。 |

# Cylance Endpoint Security アーキテクチャ




| コンポーネント | 説明 |
| --- | --- |
| BlackBerry Infrastructure | BlackBerry Infrastructure は、複数の地域に分散されたグローバルなプライベートデータネットワークで、世界中の数千の組織と数百万のユーザー間のデータ転送を可能にし、データをセキュリティで保護します。BlackBerry サービスとエンドユーザーデバイス間のデータ転送を効率的に管理できるように設計されています。<br><br>BlackBerry Infrastructure は、エージェントおよび CylancePROTECT Mobile アプリのアクティベーションに関するユーザー情報を登録し、ライセンス情報を検証して、ファイアウォールの内側にインストールされたオンプレミスコンポーネントと、ファイアウォールの内側および外側にあるユーザーのデバイス上のエージェントおよび CylancePROTECT Mobile アプリとの信頼できる接続を維持します。 |

| コンポーネント | 説明 |
| --- | --- |
| CylancePROTECT | CylancePROTECT Desktop は、機械学習技術を使用して Windows、macOS、および Linux デバイス上のマルウェアを検出してブロックし、新しいマルウェア、ウイルス、ボット、将来のバリアントを無用にします。CylancePROTECT Mobile は、iOS、Android、および Chrome OS デバイスでマルウェア、サイドロードされたアプリ、テキストメッセージ内の悪意のある URL、およびその他のセキュリティリスクを検出し、脅威を排除するためのアクションを推奨します。 |
| CylanceOPTICS | CylanceOPTICS は、Windows、macOS、および Linux デバイスを監視するとともに、収集された情報を集約して、悪意のあるイベントが発生したときに、そのイベントを検出、追跡、警告、対応します。CylanceOPTICS 攻撃が開始されたときにそれを検出し、被害が発生する前に調査と対応を自動化して阻止することができます。 |
| CylanceGATEWAY | CylanceGATEWAY は組織のプライベートネットワークおよびクラウドベースのアプリケーションのネットワークアクセスを保護します。これにより Windows、macOS、iOS、および Android のユーザーが拡張ネットワーク境界にアクセスできるようにし、拡張ネットワークを脅威から保護します。 |
| CylanceAVERT | CylanceAVERT は、外部ソースを介して機密性の高い規制情報や組織情報が損失することを検出、防止できます。CylanceAVERT は、会社の機密情報を検出、分類、一覧化し、脅威を検出して不正流出イベントを防止することができます。 |
| Cylance Endpoint Security クラウドサービス | Cylance Endpoint Security クラウドサービスは、それぞれの Cylance Endpoint Security 機能の背後にある脳力です。さまざまな機能に対応するクラウドサービスは、AI、機械学習、またはユーザーモデリングに基づくリスクエンジンを活用して、大量の複雑なデータを処理し、脅威を特定して対応します。詳細については、「Cylance Endpoint Security が高度なテクノロジを使用してユーザーとデバイスを保護する方法」を参照してください。 |
| 管理コンソール | クラウドベースの管理コンソールを使用すると、Cylance Endpoint Security のすべての機能を設定、管理、監視できます。 |
| エージェントまたは CylancePROTECT Mobile アプリを搭載したデバイス | Windows、macOS、および Linux デバイスにインストールされているエージェントと、iOS、Android、および Chrome OS デバイスにインストールされている CylancePROTECT Mobile アプリとは、Cylance Endpoint Security との通信により、潜在的な脅威を検出し、ユーザー、デバイス、およびネットワークを保護するためのアクションを実行します。 |
| BlackBerry Connectivity Node | BlackBerry Connectivity Node は、Cylance Endpoint Security がユーザーとグループをオンプレミス Microsoft Active Directory または LDAP ディレクトリと同期させることができるオプションのコンポーネントです。Cylance Endpoint Security は、BlackBerry Connectivity Node を使用しないでユーザーとグループを Entra Active Directory と同期できます。 |

| コンポーネント | 説明 |
| --- | --- |
| CylanceGATEWAY Connector | CylanceGATEWAY Connector は、BlackBerry Infrastructure とプライベートネットワーク間のセキュリティ保護されたトンネルを確立するために、ファイアウォールの内側とプライベートクラウドネットワークにインストールできるオプションのコンポーネントです。CylanceGATEWAY Connector は、従来の VPN ではなく、CylanceGATEWAY を使用して、ファイアウォールの内側にあるコンテンツサーバーやアプリケーションサーバーと通信できます。 |

# Cylance Endpoint Security が高度なテクノロジを使用してユーザーとデバイスを保護する方法

CylancePROTECT Desktop および CylancePROTECT Mobile は、最先端のクラウドサービスを活用して、ソフトウェア、ファイル、Web サイトが悪意のあるものである可能性があるかどうか、またデバイスのセキュリティに対する脅威であるかどうかを判断します。CylancePROTECT クラウドサービスは、高度な AI、機械学習、効率的な数学モデルを使用して、グローバルソースから得られた大量のデータを処理し、データのパターンや特性を維持して継続的に学習します。また、このデータを使用して、ソフトウェア、ファイル、インターネットの宛先の潜在的なリスクに関するインテリジェントな予測と意思決定を、ほぼリアルタイムで行います。CylancePROTECT サービスは、常に進化して新しいサイバー脅威に対応し、悪意のあるソフトウェアや Web サイトを特定して、組織のインフラストラクチャやデバイスユーザーに影響を与える前に、積極的かつ予防的なセキュリティ戦略を提供します。

CylancePROTECT サービスは、CylancePROTECT Desktop エージェントがスキャンしたファイルの脅威分析を提供します。ファイルが悪意のあるファイルとして識別された場合、CylancePROTECT Desktop エージェントは設定した軽減アクション（警告、隔離など）を実行します。エージェントにはローカル CylancePROTECT サービスモデルが含まれているため、エージェントがクラウドと通信できない場合、エージェントはローカルモデルを使用してファイルをスコアリングします。

CylanceGATEWAY では、マシンラーニングモデル（シグネチャ検出や DNS トンネリング検出など）が提供され、IP レピュテーションデータベースの継続的な監視と動的な適用が行われて、ネットワークトラフィックが監視され、潜在的に悪意のある脅威を含む宛先が特定されます。宛先が潜在的な脅威を含むものとして識別されている場合、CylanceGATEWAY では、設定したアクション（宛先への接続の警告またはブロックなど）が実行されます。CylanceGATEWAY には、ユーザーのデバイスとネットワークを脅威から保護するため、仕事モードとセーフモードの 2 つの動作モードがあります。

CylancePROTECT サービスは、マルウェア検知、SMS メッセージスキャン、セキュアネットワークのチェックなど、いくつかの CylancePROTECT Mobile 機能の中核となるコンポーネントです。CylanceGATEWAY が有効になっている場合、CylancePROTECT Mobile アプリはマシンラーニングを使用してネットワークトラフィックを継続的に監視し、宛先へのユーザーのアクセスをブロックすることもできます。

デスクトップデバイスの CylanceOPTICS エージェントは、収集したデータを CylanceOPTICS クラウドサービスに送信します。データは集約され、安全な CylanceOPTICS クラウドデータベースに保存されます。CylanceOPTICS データ分析サービスは、管理コンソールでアクセスできるデバイスデータを豊富に解釈します。CylanceOPTICS は、コンテキスト分析エンジン（CAE）を使用して、デバイスで発生したイベントを分析し、関連付けます。CAE が特定の関心アーチファクトを特定した場合（通知を表示したり、現在のユーザーをログオフしたりするなど）、CylancePROTECT Desktop の機能を補完するための脅威検出と防止の追加レイヤーを提供する自動応答アクションを実行するように CylanceOPTICS を構成できます。

デスクトップデバイス上の CylanceGATEWAY エージェントは、マシンラーニングと静的レピュテーションデータベースを使用して、潜在的に悪意のある脅威を含む可能性のある宛先を識別します。エージェントでセーフモードも有効にして使用している場合、CylanceGATEWAY は各 DNS クエリをインターセプトして、接続が続行できるか、接続をブロックするかを判断することで、使用ポリシー（UAP）を適用します。

CylanceAVERT エージェントは、エンドポイント上の機密ファイルを識別し、メール、ブラウザのアップロード、ネットワークドライブ、または USB デバイスを介して機密ファイルを流用しようとする試みが行われた場合は管理者に通知します。機密ファイルが窃盗イベントに関与している場合、CylanceAVERT は、管理者が情報保護の設定で指定した軽減アクションを実行します。CylanceAVERT はキーワードとの一致と Regex 検証を使用して、窃盗イベントをトリガーする機密データタイプを識別します。

# CylancePROTECT Desktop とは

CylancePROTECT Desktop は、デバイスに影響を与える前に、マルウェアを検出してブロックします。BlackBerry は、マルウェアの識別に数学的アプローチを使用し、事後署名、信頼ベースのシステム、サンドボックスなどの代わりに機械学習技術を使用します。このアプローチは、新しいマルウェア、ウイルス、ボット、および将来のバリアントを無用にします。CylancePROTECT Desktop は OS 層およびメモリ層におけるマルウェアのファイル実行の可能性を分析して、悪意のあるペイロードの配信を防止します。

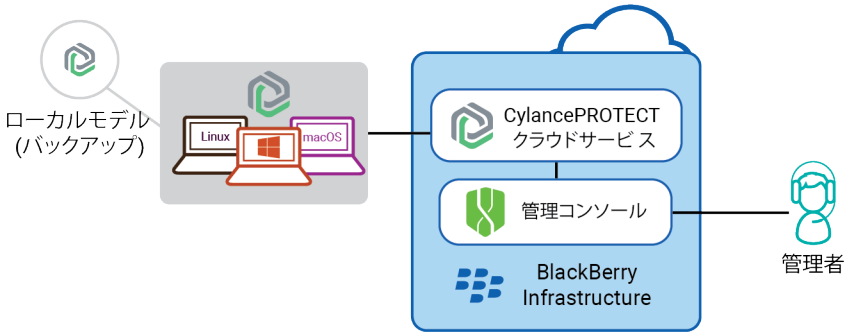
CylancePROTECT Desktop エージェントは、最小限のシステムリソースを使用するように設計されています。エージェントは、実行されるファイルまたはプロセスが悪意のあるイベントである可能性があるため、優先して扱います。ディスク上のファイル（ストレージ内にあるが実行されていないファイル）は、悪意がある可能性があるものの、差し迫った脅威にならないため、優先度が低くなります。

## CylancePROTECT Desktop の主な機能

| 機能 | 説明 |
| --- | --- |
| 悪意のあるファイルを検出して隔離する | CylancePROTECT Desktop は、危険または異常であると検出したファイルの処理に関するオプションを提供しています。脅威イベントで識別されたファイルを隔離リストまたはセーフリストに追加して、今後のイベントの処理のために備えることができます。 |
| メモリエクスプロイトからの保護 | CylancePROTECT Desktop は、プロセスの注入やエスカレーションなど、メモリエクスプロイトを処理するオプションを提供します。実行可能ファイルを除外リストに追加して、デバイスポリシーが適用されたときにこれらのファイルを実行できるようにすることもできます。 |
| 悪意のあるスクリプトのブロック | CylancePROTECT Desktop は、悪意のあるスクリプトを監視し、環境内で実行されないように保護します。CylancePROTECT Desktop エージェントは、スクリプトが実行される前にスクリプトとスクリプトのパスを検出してブロックできます。 |
| USB ストレージデバイスからの脅威のブロック | CylancePROTECT Desktop は、USB 大容量ストレージデバイスを組織内のデバイスに接続する際の方式を制御します。USB フラッシュドライブ、外付けハードドライブ、スマートフォンなどの USB 大容量ストレージデバイスを許可またはブロックできます。 |
| 即時アラートの受信 | CylancePROTECT Desktop は、悪意のあるプロセスの実行がないか監視し、危険または異常なものを実行する試みがあったときに警告します。 |
| 非アクティブなデバイスの検出 | 指定された期間、CylancePROTECT Desktop エージェントがコンタクト状態から外れていた場合、デバイスの状態は非アクティブに変わります。非アクティブなデバイスを確認して、管理コンソールから削除する必要があるかどうかを判断できます。 |

| 機能 | 説明 |
| --- | --- |
| 仮想マシンの保護 | このテクノロジは毎日のディスクスキャンを必要としないため、CylancePROTECT Desktop がゲスト単位でリソースを集中的に消費することはありません。CylancePROTECT Desktop がゲスト単位でメモリを集中的に消費することもありません。 |

# アーキテクチャ：CylancePROTECT Desktop




| 項目 | 説明 |
| --- | --- |
| CylancePROTECT クラウドサービス | CylancePROTECT Desktop は、機械学習技術を使用してマルウェアを検出し、ブロックし、新しいマルウェア、ウイルス、ボット、および将来のバリアントを無用にします。<br>CylancePROTECT クラウドサービスは、高度な AI、機械学習、効率的な数学モデルを使用して、グローバルソースから得られた大量のデータを処理し、データのパターンや特性を維持して継続的に学習します。また、このデータを使用して、ソフトウェア、ファイル、インターネットの宛先の潜在的なリスクに関するインテリジェントな予測と意思決定を、ほぼリアルタイムで行います。CylancePROTECT サービスは、CylancePROTECT Desktop エージェントがスキャンしたファイルの脅威スコアリングを提供します。ファイルスコアは、エージェントに割り当てられたデバイスポリシーに基づいて、エージェントがファイルに対して実行するアクションを決定します。 |
| 管理コンソール | クラウドベースの管理コンソールを使用すると、さまざまな脅威関連イベントを表示し、エンドポイントでエージェントを設定するためのデバイスポリシーを管理し、隔離されたファイルと安全なファイルのグローバルリストを管理することができます。 |
| CylancePROTECT Desktop エージェントを搭載するデバイス | デバイスを保護するには、CylancePROTECT Desktop エージェントをデバイス（エンドポイント）にインストールする必要があります。CylancePROTECT Desktop は Windows、macOS、および Linux オペレーティングシステムをサポートしています。 |

| 項目 | 説明 |
| --- | --- |
| ローカルモデル | 各エンドポイントの CylancePROTECT Desktop エージェントは、CylancePROTECT サービスがファイルのスコアリングに使用するモデルの二次的なコピーを保持します。エージェントが CylancePROTECT サービスに接続できない場合には、ローカルモデルによってファイルスコアを計算します。 |

# CylancePROTECT Mobile とは

CylancePROTECT Mobile は、iOS、Android、および Chrome OS デバイス上のサイバー脅威を、従業員の生産性を低下させることなく、リアルタイムでプロアクティブに特定して阻止する、高度なセキュリティソリューションです。

CylancePROTECT Mobile は、次のような最先端テクノロジを組み合わせて使用しています。

- モバイルデバイスの管理、CylancePROTECT Mobile の機能の管理、モバイル脅威に関する詳細の表示に使用できる Web ベースの管理コンソール
- ユーザーのデバイスを定期的にスキャンして脅威を検出し、全体的なセキュリティ評価を行う CylancePROTECT Mobile アプリ。可能な限り、管理者の介入なしで脅威を解決できるよう、アプリはユーザーに明確な指示を与えます。
- 高度な AI と機械学習を使用して、マルウェアやテキストメッセージ内の安全でない URL をリアルタイムで識別するなどの、CylancePROTECT Mobile の重要な機能をサポートする CylancePROTECT クラウドサービス。

これらのテクノロジをシームレスに統合することで、データを保護し、モバイルデバイス上での悪意のあるアクティビティを特定し、プロアクティブに排除する、セキュアなエコシステムを確立します。CylancePROTECT Mobile は、設定が簡単で、エンドユーザーが理解して使用しやすく、常に改善され、ますますスマートになっているクラウドテクノロジを活用しています。

# CylancePROTECT Mobile の主な機能

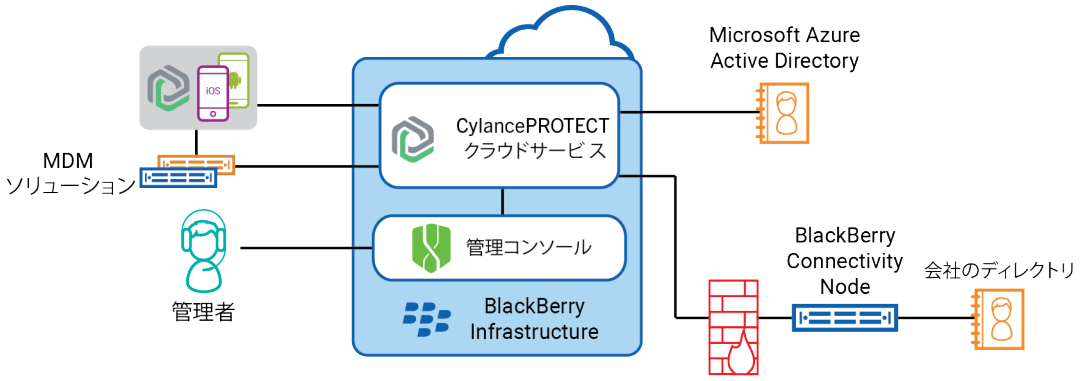
| 機能 | 説明 |
| --- | --- |
| Android デバイスのマルウェア検出 | CylancePROTECT Mobile アプリは Android デバイス上のマルウェアを検知し、ユーザーに悪意のあるアプリをアンインストールするよう指示できます。CylancePROTECT Mobile アプリはユーザーのデバイス上のアプリをスキャンし、アプリファイルを CylancePROTECT クラウドサービスにアップロードします。クラウドサービスでは、AI と機械学習を使用してアプリパッケージを分析し、CylancePROTECT Mobile アプリに戻る信頼度スコアを生成します。信頼度スコアによって、スキャンしたアプリが安全か、悪意のある可能性があるかが決まります。<br><br>アプリが悪意のある可能性があると CylancePROTECT サービスが判断すると、アプリはユーザーに通知し、詳細を提供します。ユーザーはアプリの修正オプションをタップしてデバイス設定に移動し、悪意のあるアプリをアンインストールできます。<br><br>CylancePROTECT サービスが以前に処理していないハッシュがある場合、アプリはサービスにアップロードされます。デバイススキャンで、以前に分析されたことのあるアプリが検出された場合、その一意のアプリハッシュに対して CylancePROTECT サービスが既に生成した信頼スコアが使用されます。アプリに新しいハッシュ（新しいバージョンなど）がある場合、アプリは分析とスコアリングのために CylancePROTECT サービスにアップロードされます（別のデバイスからアップロードされていない場合）。 |

| 機能 | 説明 |
| --- | --- |
| iOS および Android デバイスでのサイドロードの検出 | サイドロードされたアプリは、公式のアプリストアを通じて配布されるアプリと同じ制限や保護を受けていません。CylancePROTECT Mobile アプリは、ユーザーのデバイス上にサイドロードされたアプリが存在するかどうかを検出し、ユーザーに警告して、ユーザーにアンインストールを指示できます。<br><br>iOS の場合、CylancePROTECT Mobile アプリは、ユーザーがデバイス設定で信頼することを選択した、サイドロードされたアプリ開発者証明書のみを検出できます。ユーザーは、アプリ開発者証明書が信頼されていない限り、サイドロードされたアプリを使用できません。<br><br>Android の場合、CylancePROTECT Mobile アプリは、インストールソースに基づいてサイドロードされたアプリを識別します。CylancePROTECT クラウドサービスと CylancePROTECT Mobile アプリは、Google Play、Amazon Appstore、Samsung Galaxy ストアなどの公式アプリソースを信頼できるものと見なします。信頼できないソースからインストールされたアプリは、サイドロードされたものと見なされます。 |
| iOS デバイスで SMS テキストメッセージの URL をスキャンしています | CylancePROTECT Mobile は、SMS テキストメッセージ内の潜在的な悪意のある URL をユーザーに警告できます。<br><br>既知の連絡先からの新しい着信テキストメッセージは自動的に安全と見なされ、不明な送信者からのメッセージのみがスキャンおよび評価されます。ユーザーが URL を含む SMS テキストメッセージを受信すると、CylancePROTECT Mobile アプリはメッセージ全体を CylancePROTECT クラウドサービスにリアルタイムで送信します。CylancePROTECT サービスは、高度な機械学習機能と脅威インテリジェンスフィードから蓄積された知識を使用して、メッセージの安全性を即座に評価します。テキストメッセージから安全ではない URL が検出されると、メッセージは迷惑メールフォルダにフィルタリングされます。<br><br>ユーザーのプライバシーを保護するため、URL を含むメッセージだけが評価されます。追加のメタデータやユーザー識別子が収集または保存されることはありません。 |

| 機能 | 説明 |
| --- | --- |
| Android デバイスで SMS テキストメッセージの URL をスキャンしています | CylancePROTECT Mobile は、SMS テキストメッセージ内の潜在的な悪意のある URL をユーザーに警告できます。<br>ユーザーが URL を含む SMS テキストメッセージを受信すると、変更されていない URL がリアルタイムで CylancePROTECT クラウドサービスに送信されます。SMS スキャンは、デバイス上のデフォルトの SMS アプリに制限されています。既知の連絡先および不明な送信者からの新しい着信テキストメッセージがスキャンされ、評価されます。<br>CylancePROTECT サービスは、高度な機械学習機能と脅威インテリジェンスフィードから蓄積された知識を使用して、URL の安全性を即座に評価します。URL が危険であると判断された場合、CylancePROTECT Mobile アプリはユーザーに警告し、詳細を提供し、ユーザーにテキストメッセージを削除するように指示します。<br>ユーザーのプライバシーを保護するため、URL を含むメッセージだけが評価されます。追加のメタデータやユーザー識別子が収集または保存されることはありません。 |
| 安全ではないネットワークと安全ではない Wi-Fi チェック | CylancePROTECT Mobile は、次のネットワークの脅威から保護します。<br>• 安全ではないネットワーク接続：iOS と Android デバイスで、CylancePROTECT Mobile アプリは定期的に CylancePROTECT クラウドサービスへの接続を試みます。接続に失敗した場合、CylancePROTECT Mobile はネットワークが安全でないと判断します。<br>• 安全でない Wi-Fi アクセスポイント：Android デバイスでは、CylancePROTECT Mobile アプリが定期的に現在の Wi-Fi アクセスポイントのプロパティをチェックして、セキュリティが確保されているかどうかを判断します。組織が安全および安全でないと考える Wi-Fi アクセスアルゴリズムを構成できます。<br>CylancePROTECT Mobile アプリが安全ではないネットワークや安全ではない Wi-Fi アクセスポイントを検出すると、アプリと管理コンソールに報告されます。 |
| デバイスセキュリティチェック | CylancePROTECT Mobile アプリは特定のデバイス条件とセキュリティ設定をチェックし、サイバー脅威に対する潜在的な脆弱性についてユーザーに通知します。アプリは以下をチェックします。<br>• 開発者モードが有効かどうか（Android のみ）<br>• ディスク暗号化が有効かどうか（Android のみ）<br>• 画面ロックが有効になっているかどうか（パスワードや指紋など）<br>• デバイスがルート化またはジェイルブレイクされているかどうか<br>• サポートしない OS バージョンがデバイスで実行されているかどうか<br>• サポートしないデバイスモデルかどうか<br>アプリが脆弱性を検出すると、潜在的なリスクレベルが示され、ユーザーが問題を解決するためのガイダンスが提供されます。 |

| 機能 | 説明 |
| --- | --- |
| 認証チェック | CylancePROTECT クラウドサービスは定期的に認証チェックを実行し、各ユーザーのデバイス上の CylancePROTECT Mobile アプリの整合性とセキュリティを確認できます。<br><br>Android デバイスでは、CylancePROTECT クラウドサービスは Play Integrity 認証、SafetyNet 認証、およびハードウェア証明書認証を使用して CylancePROTECT Mobile アプリを検証します。SafetyNet 認証は、Play Integrity 認証に置き換えられます。古いバージョンのアプリは、Google がサポートを削除するまで引き続き SafetyNet 認証をサポートする予定です。認証チェックは毎日行われます。また、デバイスに最低限のセキュリティパッチレベルを適用することもできます。アプリは、デバイスが必要なパッチレベルを満たしていないことを検出した場合、更新プログラムを確認するようにユーザーに警告できます。<br><br>iOS デバイスの場合、CylancePROTECT クラウドサービスは、Apple DeviceCheck フレームワークを使用してアプリの整合性をチェックします。整合性チェックは毎日行われます。<br><br>Samsung デバイスでは、CylancePROTECT クラウドサービスで定期的に Samsung Knox Enhanced Attestation を使用して、デバイスの整合性を検証することもできます。Knox Enhanced Attestation はハードウェアベースであり、アプリのヘルスチェックの実行に加えて、デバイスの改ざん、ルート化、OEM のロック解除、IMEI またはシリアル番号の改ざんを検出できます。<br><br>認証の失敗が発生した場合、管理者は管理コンソールに詳細を表示できます。 |
| MDM ソリューションとの統合 | Cylance Endpoint Security を Microsoft Intune に接続して、Cylance Endpoint Security から Intune にデバイスのリスクレベルを報告できるようにすることができます。デバイスのリスクレベルは、Intune 管理対象デバイス上の CylancePROTECT Mobile アプリによるモバイル脅威の検出に基づき、計算されます。Intune は、デバイスのリスクレベルに基づいて軽減アクションを実行できます。 |
| CylancePROTECT Mobile アプリのユーザビリティ機能 | CylancePROTECT Mobile アプリで有効にすることにした機能ごとに、デバイス通知、メールメッセージ、または通知なし（ユーザーは CylancePROTECT Mobile アプリで脅威アラートを表示可能）によってユーザーに脅威を通知できます。<br><br>Android バージョン 2.3.0.1640 以降用の CylancePROTECT Mobile アプリは、Google Play で新しいバージョンのアプリが使用可能になるとユーザーに通知します。30 日経過すると、アプリは自動的に更新をダウンロードし、更新を適用してアプリを再起動するように求めます。60 日後には、アップグレードプロンプトに対応するまでアプリを使用できません。<br><br>iOS 用 CylancePROTECT Mobile アプリは、App Store からの自動更新をサポートしています。 |

# アーキテクチャ：CylancePROTECT Mobile




| 項目 | 説明 |
|---|---|
| CylancePROTECT クラウドサービス | ユーザーのデバイス上の管理コンソールと CylancePROTECT Mobile アプリは、CylancePROTECT クラウドサービスとの通信に安全な接続を使用します。クラウドサービスは、ユーザーアカウントの作成と設定、デバイスへの CylancePROTECT Mobile 機能と設定の適用、イベントとアラートのリアルタイム処理を担当します。<br><br>CylancePROTECT サービスでは、AI と機械学習を使用して、ソフトウェアや Web サイトが悪意のあるものである可能性があるかどうか、またデバイスのセキュリティに対する脅威であるかどうかを判断します。この AI エンジンは、マルウェア検知、SMS メッセージスキャン、ネットワークセキュリティ検証など、いくつかの CylancePROTECT Mobile 機能の中核となるコンポーネントです。そのコア機能により、AI エンジンは、悪意のあるソフトウェアや Web サイトが組織のインフラストラクチャやデバイスユーザーに影響を与える前にそれらを特定する、非常に積極的でプロアクティブなセキュリティ戦略を実現します。 |
| 管理コンソール | クラウドベースの管理コンソールを使用すると、モバイルデバイスの管理、CylancePROTECT Mobile の機能の設定と管理、デバイスステータスと CylancePROTECT Mobile アプリが検出したモバイルアラートの表示を行うことができます。 |
| BlackBerry Connectivity Node | BlackBerry Connectivity Node は、Cylance Endpoint Security が CylancePROTECT Mobile ユーザーとグループをオンプレミス Microsoft Active Directory または LDAP ディレクトリと同期させることができるオプションのコンポーネントです。Cylance Endpoint Security は、BlackBerry Connectivity Node を使用しないでユーザーとグループを Entra Active Directory と同期できます。 |
| CylancePROTECT Mobile アプリを搭載したデバイス | iOS、Android、および Chrome OS デバイスにインストールされた CylancePROTECT Mobile アプリは、デバイスを定期的にスキャンして、デバイスの設定や状況をチェックし、脅威を特定します。脅威が検出されると、ユーザーはアプリで詳細を表示できます。可能であれば、アプリは脅威を解決するためにユーザーに指示を与え、デバイス設定に移動して問題に対応できるようにします。 |

| 項目 | 説明 |
| --- | --- |
| MDM ソリューション | 必要に応じて、Cylance Endpoint Security を Microsoft Intune に接続して、Cylance Endpoint Security から Microsoft Intune にデバイスのリスクレベルを報告できるようにすることができます。デバイスのリスクレベルは、Intune 管理対象デバイス上の CylancePROTECT Mobile アプリによるモバイル脅威の検出に基づき、計算されます。Intune は、デバイスのリスクレベルに基づいてデバイス上で軽減アクションを実行できます。 |

# CylanceOPTICS とは

CylanceOPTICS は、デバイスからフォレンジックデータを収集および分析し、組織のユーザーやデータに影響を与える前に脅威を特定して解決するエンドポイント検出および応答ソリューションです。

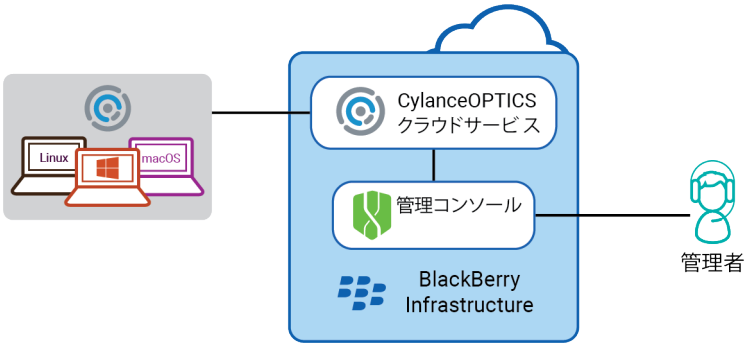
CylancePROTECT Desktop エージェントと一緒に CylanceOPTICS エージェントをインストールして、CylanceOPTICS で Windows、 macOS、または Linux デバイスを有効にします。CylanceOPTICS エージェントは、さまざまなレベルおよびサブシステムでセンサを OS に導入し、 CylanceOPTICS クラウドデータベースに集約および保存される多様なデータセットを監視および収集します。CylanceOPTICS データを使用して、デバイスベースの脅威に対する自動応答を検出、調査、診断、および設定できます。

## CylanceOPTICS の主な機能

| 機能 | 説明 |
| --- | --- |
| CylanceOPTICS データの分析 | 管理コンソールを使用して、 CylanceOPTICS エージェントが収集したデバイスデータを照会し、セキュリティインシデントを調査して侵害の兆候を検出できます。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して、詳細な分析を行うことができます。<br><br>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。拡張クエリは 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 データの視覚化 | 次の視覚化機能を使用して、フォレンジック分析を支援できます。<br><br>• 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に視覚的に表示して、それらのリレーショナルパスを識別して追跡できるようにします。<br>• 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。 |
| イベントの検出および対応 | CylanceOPTICS は、CAE（Context Analysis Engine）を使用して、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および相関付けします。CAE が特定の関心アーチファクトを特定した場合（通知を表示したり、現在のユーザーをログオフしたりするなど）、 CylancePROTECT Desktop の機能を補完するための脅威検出と防止の追加レイヤーを提供する自動応答アクションを実行するように CylanceOPTICS を構成できます。<br><br>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。目的のルールと応答の設定を使用して検出ルールセットを作成したり、既存の検出ルールを複製および変更したり、独自のカスタムルールを作成したりできます。また、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もできます。 |

| 機能 | 説明 |
| --- | --- |
| データを収集するパッケージの展開 | 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）をリモートで安全に実行して、必要なデータを収集し、特定の場所に保存して、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。 |
| デバイスをロックして脅威を隔離 | 感染しているデバイスや感染している可能性のあるデバイスをロックし、LAN 機能と Wi-Fi ネットワーク機能を無効にして、コマンドおよび制御アクティビティ、データの窃盗、マルウェアの横方向の移動を停止できます。組織のニーズに合わせて、さまざまなロックダウンオプションを利用できます。 |
| アクションをデバイスに送信 | リモート応答機能を使用すれば、使い慣れたコマンドラインインターフェイスを使って、管理コンソールから直接、任意の CylanceOPTICS 対応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。 |

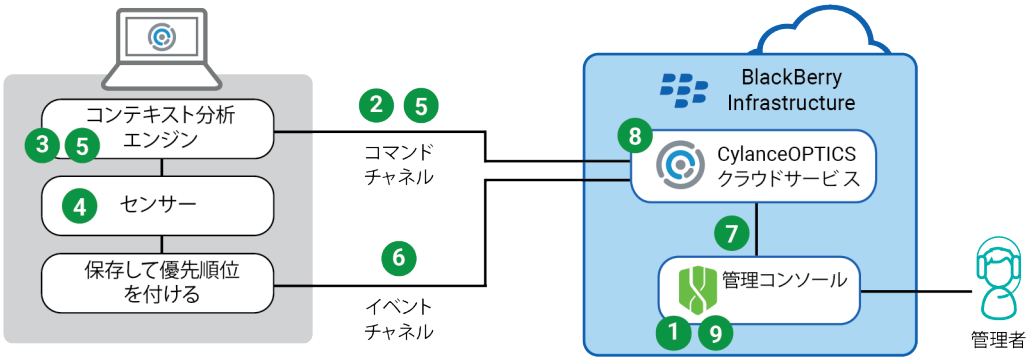
# アーキテクチャ：CylanceOPTICS




| コンポーネント | 説明 |
| --- | --- |
| CylanceOPTICS クラウドサービス | CylanceOPTICS エージェントは、収集したデバイスデータを CylanceOPTICS クラウドサービスに送信します。データは集約され、安全な CylanceOPTICS クラウドデータベースに保存されます。CylanceOPTICS データ分析サービスは、デバイスデータの多彩な解釈を提供し、管理コンソールを使用してアクセスできます。<br><br>CylanceOPTICS エージェントバージョン 2.x 以前のデバイスの場合、CylanceOPTICS データベースはデバイス上にローカルに保存されます。バージョン 3.0 以降では、データが定期的かつ自動的に CylanceOPTICS クラウドデータベースに集約、保存、圧縮、送信されます。 |

| コンポーネント | 説明 |
| --- | --- |
| 管理コンソール | クラウドベースの管理コンソールを使用すると、デバイスにインストールされている CylanceOPTICS エージェントの管理、セキュリティインシデントを調査するための CylanceOPTICS データのクエリ、CylanceOPTICS の監視対象とイベントへの対応方法のカスタマイズ、脅威に応じたアクションの実行が可能になります。 |
| CylanceOPTICS エージェントを搭載するデバイス | CylanceOPTICS エージェントは、Windows、macOS、および Linux デバイスにインストールします。エージェントはデバイス OS にセンサを導入し、脅威を特定して自動応答をトリガーするために使用されるデータを監視および収集します。 |

# データフロー：イベントの検出とイベントへの応答、およびイベントデータの保存（CylanceOPTICS 3.x 以降）




1. 管理者は管理コンソールを使用して検出ルールを設定し、ルールをデバイスポリシーに割り当てます。
2. CylanceOPTICS クラウドサービスは、検出ルールをセキュア Web ソケット接続を介して CylanceOPTICS エージェントを使用するデバイスに送信します。ルールデータには、各イベントに対して設定された応答（すべてのユーザーのログオフ、プロセスの一時停止など）も含まれます。
3. CylanceOPTICS エージェントは、検出ルールを、イベントの分析と関連付けに使用するコンテキスト分析エンジン（CAE）に組み込みます。
4. CylanceOPTICS センサがイベントを検出します。
5. イベントが検出ルールを満たすかどうかは、CAE によって判断されます。判断されると、次のいずれかが行われます。
   - CylanceOPTICS エージェントがイベント応答で既に設定されている場合、エージェントは応答を実行します。
   - エージェントが応答を実行するために追加のデータを必要とする場合（まだデバイスにないプレイブックパッケージが応答に必要な場合など）、エージェントはセキュアな Web ソケット接続を介して検出データを CylanceOPTICS クラウドサービスに送信します。CylanceOPTICS クラウドサービスは検出を処理し、応答を実行するためにエージェントに必要なデータを提供します。
6. エージェントは、イベントデータを優先順位付けし、セキュアな TLS 接続を使用して、専用のイベントチャネル経由で CylanceOPTICS クラウドサービスに送信します。CylanceOPTICS クラウドサービスは、イベントデータを受信して処理し、セキュアな CylanceOPTICS クラウドデータベースに保存します。

7. 管理者は管理コンソールを使用して、検出データを要求するか、InstaQuery、高度なクエリ、またはフォーカスビュー要求を開始します。管理コンソールは、TLS 経由の HTTP を使用して CylanceOPTICS クラウドサービスとやり取りします。
8. CylanceOPTICS クラウドサービスは要求を検証して処理し、CylanceOPTICS クラウドデータベースから要求されたデータを取得して、データを管理コンソールに返します。
9. 検出データ、クエリ結果、またはフォーカスデータが管理コンソールに表示されます。

# CylanceGATEWAY とは

CylanceGATEWAY は、クラウドネイティブな人工知能（AI）支援のゼロトラストネットワークアクセス（ZTNA）ソリューションです。ユーザーが拡張ネットワーク境界にアクセスできるようにするとともに、拡張ネットワークを脅威から保護します。現在、サイバーセキュリティの脅威が巧妙化し蔓延しつつある中で、企業の接続されたエンドポイントの数と、クラウドサービスに送信、保存されるデータの量は急激に増加しており、組織は厳しい環境に直面しています。CylanceGATEWAY は、ネットワークセキュリティを提供すると同時に、エンドユーザーのネットワーク体験を強化し、向上させます。CylanceGATEWAY は、デフォルトでは何も、誰も信頼しません。すべてのユーザー、エンドポイント、ネットワークは潜在的に敵対的であると見なし、ユーザーの身元、アクセスが許可されていること、行動に悪意がないこと、および接続先のローカルネットワークが侵害されていないことを証明するまで、ユーザーは何にもアクセスできません。

CylanceGATEWAY は、デバイスがネットワークに接続されていない場合でも、デバイスから到達されるのを防ぎたいインターネットの宛先への接続をブロックできるようにすることで、ユーザーの iOS、Android、 Windows 10、Windows 11、および macOS デバイスを保護します。BlackBerry は、エンドポイントの接続をブロックできる安全でないインターネットの宛先のリストを継続的に維持します。ユーザーが許容される使用基準を満たしていない特定のサイトへアクセスすることも組織でブロックする場合は、ポリシーを作成して、すべてのユーザーまたは特定のユーザーやグループがアクセスできない別の宛先を指定できます。

## CylanceGATEWAY の主な機能

| 機能 | 説明 |
| --- | --- |
| 仕事モード | ユーザーは、仕事モードを有効または無効にできます。仕事モードでは、ネットワークとデバイスが保護されます。有効にすると、各ネットワークアクセス試行は、各自の環境に設定されているアクセス制御リスト（ACL）のルールおよび指定されたネットワーク保護設定に照らして評価されます。アクセス制御リストは、プライベートネットワークおよびパブリックネットワーク上の許可およびブロックされる対象を定義します。許可されていると、ネットワークトラフィックは安全なトンネル経由で CylanceGATEWAY クラウドサービスに送信されます。 |
| macOS および Windows のセーフモードサポート | ユーザーに対してセーフモードを有効にできます。セーフモードの場合、CylanceGATEWAY は、アプリおよびユーザーが潜在的に悪意のある宛先にアクセスできないようにブロックし、DNS 要求をインターセプトすることで、許容可能な使用ポリシー（AUP）を強制します。CylanceGATEWAY クラウドサービスは、設定されている ACL ルールとネットワーク保護設定（ドメイン生成アルゴリズム（DGA）、フィッシング、マルウェアなどの DNS トンネリングおよびゼロデイ検出など）に照らして各 DNS クエリを評価し、リアルタイムで要求を許可またはブロックするようエージェントに指示します。許可された場合、DNS 要求が、正常にベアラーネットワーク経由で完了します。それ以外の場合、CylanceGATEWAY エージェントが、通常の応答を上書きしてアクセスを防止します。<br><br>メモ：セーフモードを有効にすると、CylanceGATEWAY トンネル（アプリごとのトンネルアクセスや分割トンネルなど）を使用しないすべての DNS トラフィックが保護されます。 |

| 機能 | 説明 |
| --- | --- |
| macOS および Windows で自動的にエージェントを起動、または仕事モードを有効化 | Gateway サービスポリシーでは、macOS または CylanceGATEWAY デバイス上で、ユーザーがログインしたときに Windows エージェントを自動的に実行するようにしたり、エージェントが起動したときに自動的に仕事モードを有効にしたりすることができます。ポリシー設定は、エージェントの［サインインしたら CylanceGATEWAY を起動］および［仕事モードを自動的に有効化］設定より優先されますが、ユーザーはエージェントの起動後または終了後に、手動で仕事モードを有効または無効にすることもできます。 |
| MDM ソリューションとの統合 | Cylance Endpoint Security を BlackBerry UEM または Microsoft Intune に接続すると、Cylance Endpoint Security は、iOS または Android デバイスが UEM または Intune で管理されているかどうかを確認することができます。UEM を使用する前に、デバイスが Intune または CylanceGATEWAY で管理される必要があるかどうかを指定することができます。ネットワークサービスの詳細については、「Cylance Endpoint Security を MDM ソリューションに接続して、デバイスが管理対象であるかどうかを確認」を参照してください。 |
| macOS および iOS でのアプリごとのトンネルアクセス | モバイルデバイス管理（MDM）にある macOS および iOS デバイスでは、CylanceGATEWAY の仕事モードトンネルを使用できるアプリを指定することができます。これを使用すると、仕事モードアクセスをデバイス上のすべてのアプリに拡張しなくても、個人所有デバイスの持ち込みを許可することができます。 |
| Windows および Android でのアプリごとのトンネルサポート | Windows および Android デバイスでは、CylanceGATEWAY トンネルを使用できるアプリを指定または制限することができます。 |
| ネットワークの宛先の継続的評価 | BlackBerry では、機械学習、IP レピュテーション、リスクスコアリングを使用して、進化を続ける悪意あるインターネット宛先リストを維持します。CylanceGATEWAY は、既知および未知のフィッシングドメインや、関連する IP および FQDN の宛先にデバイスが接続されないようブロックし、組織が独自のリストを手動でコンパイルおよび維持する手間を軽減します。 |
| 脅威からの保護 | CylanceGATEWAY が機械学習を使用して、潜在的な脅威がないかネットワーク接続を継続的に監視することで、組織のネットワークを脅威から継続的に保護します。異常が特定されると、ネットワーク保護設定で設定されたリスクレベルに基づいて、その後ブロックまたは警告が行われます。<br>• エンドポイントを、新たに出現するネットワークの脅威や確立された悪意のある宛先、特定された異常（ゼロデイ、フィッシングドメイン、コマンド&コントロール（C2）ビーコンなど）から保護します。<br>• クライアントから攻撃者の DNS サーバーへの DNS トラフィックを CylanceGATEWAY が分析した結果に基づき、DNS トンネリングの異常を検出します。 |
| ネットワークの宛先のリスクレベルの評価 | 管理コンソールを使用して、CylanceGATEWAY クラウドサービスによって分析および判定されたネットワークの宛先のリスクレベルを評価し、それらのカテゴリとサブカテゴリを特定できます。 |

| 機能 | 説明 |
| --- | --- |
| 複数のプライベートネットワークのサポート | 1 つの Cylance Endpoint Security テナントから複数の CylanceGATEWAY Connectors を展開して、オンプレミスとクラウド環境の両方にある複数のプライベートネットワーク（セグメント、データセンター、VPC など）にアクセスを許可できます。指定した各コネクタグループに関連付けられている CylanceGATEWAY Connectors を表示できます。最大 8 個のコネクタグループを作成し、各グループに最大 8 個の CylanceGATEWAY Connector を割り当てることができます。 |
| セグメント化されたプライベートネットワークアクセス | CylanceGATEWAY Connectors をオンプレミスおよびプライベートクラウドネットワークにインストールすると、ネットワークトポロジやルーティングを変更せずに、また着信トラフィックに対してファイアウォールに穴を開けずに、リモートデバイスへのネットワークアクセスを提供できます。CylanceGATEWAY 経由のアクセスでは、選択したネットワークの部分のみがエンドポイントに公開され、エンドポイントはプライベートネットワーク全体に公開されないため、強力に分離されます。CylanceGATEWAY Connector は AWS、vSphere、ESXi、Microsoft Entra ID、または Hyper-V 環境に展開できます。 |
| ネットワークアクセスとトラフィックパターンの監視 | 管理コンソールの CylanceGATEWAY ダッシュボードには、ネットワークトラフィックの監視に役立つ接続、使用パターン、およびアラートを示す複数のウィジェットが表示されます。 |
| ネットワーク保護設定の指定 | ［ネットワーク保護］画面では、設定された最小リスクレベルを下回る、許可されたネットワークイベント（宛先評価や署名検出など）を、［ネットワークイベント］画面で異常として表示するかどうかを指定できます。許可されたイベントは、無効にされると、通常の許可トラフィックとして表示されます。また、ブロックされたイベントのみを送信するように SIEM ソリューションまたは syslog サポートを設定することもできます。これらの機能により、ネットワーク保護と SIEM ソリューションまたは syslog をより詳細に制御でき、アラートによる疲弊を軽減できます。 |
| ［アラート］表示に送信するネットワーク保護設定の指定 | ［ネットワーク保護］画面では、［アラート］表示に送信する検出（宛先評価、署名検出、DNS トンネリング、ゼロデイなど）を指定できます。ブロックされた ACL イベントと許可された ACL イベントは、［アラート］表示に共有されません。この機能により、［アラート］表示に表示されるアラートをより詳細に制御できます。 |
| OS 固有の ACL ルール | ACL ルールを作成し、特定の OS に適用できます。たとえば、一部のリソースへのアクセスをデスクトップデバイス（macOS および Windows）のみに許可することができます。 |
| ワンタッチでの SaaS の設定 | ネットワークサービスを使用することで、SaaS アプリケーションへのアクセスを簡単に設定できます。CylanceGATEWAY が SaaS アプリのサポートを効率化し、環境に設定する ACL ルールで SaaS アプリの接続を有効にするまでに必要な時間を短縮します。ネットワークサービスの詳細については、「ネットワークサービスの定義」を参照してください。 |

| 機能 | 説明 |
| --- | --- |
| コンテンツのフィルタリング | 環境に設定する ACL ルールとネットワーク保護設定によって、ユーザーがアクセスできるコンテンツと宛先がフィルタリングされます。これには機械学習とアクセス制御リストのルールが使用され、ユーザーおよびデバイスが組織の許容される利用要件および規制要件を確実に遵守するようにします。 |
| NAT 詳細レポート | トンネル IP アドレス（BlackBerry ソース IP）に基づいてイベントをフィルタリングし、ユーザーが外部の宛先にアクセスするために使用するトンネル IP アドレスを特定することができます。<br>CylanceGATEWAY Connector は、ネットワークアドレス変換（NAT）が適用された後にトンネルを通過してプライベートネットワークに流れる UDP および TCP フローに関する追加情報を提供します（プライベート NAT ソース IP やプライベートソースポートなど）。これにより、潜在的に悪意のあると特定またはブロックされていて、プライベートネットワークをトラバースするイベントの、ソース IP アドレスやポート番号を特定できます。 |
| Web アクセスファイアウォール | CylanceGATEWAY は、潜在的に疑わしい宛先へのトラフィックをフィルタリング、監視、およびブロックすることにより、デバイスとプライベートネットワークを保護します。CylanceGATEWAY は、環境に設定されている ACL ルールと、指定したネットワーク保護設定を適用することで、この保護を行います。詳細については、以下を参照してください。<br>• 管理コンテンツでのネットワーク接続の監視<br>• セットアップコンテンツでの ACL ルールを使用したネットワークアクセスの制御 |
| IP ピン設定サービスのサポート | ほとんどの SaaS アプリケーションでは、ソース IP ピン設定により、特定範囲の信頼できる IP アドレスからの接続のみにアクセスを制限できます。信頼できるエントリポイントを介した接続のみにユーザーを制限することで、組織はユーザーがサービスを使用する権利があるかどうかの検証レベルを上げることができます。組織では既にこの方法を使用して、SaaS アプリケーションへのアクセスを組織のネットワークに接続されているデバイスが使用する IP アドレスからの接続に制限している可能性があります。CylanceGATEWAY を使用せずにリモートで作業しているユーザーの場合、リモートデバイスと SaaS アプリケーション間のすべてのトラフィックは VPN を経由してネットワークに移動し、その後 SaaS アプリケーションに移動する必要があります。<br>CylanceGATEWAY では、組織専用の CylanceGATEWAY IP アドレスを予約できます。これらの IP アドレスは、組織の IP アドレスに加えてソース IP ピン設定にも使用できます。これにより、リモートユーザーを組織の VPN に接続しなくても、同じレベルのセキュリティを実現できます。 |
| 業界をリードするトンネル技術 | CylanceGATEWAY では、TCP、UDP、ICMP、およびリアルタイムの低遅延トラフィックを伝送する IP トンネルに高度なレイヤ 3 暗号化を提供します。 |

| 機能 | 説明 |
| --- | --- |
| Android および iOS のサポート | CylancePROTECT Mobile アプリはトンネルを経由して CylanceGATEWAY クラウドサービスにトラフィックを送信して、ユーザーに接続統計やステータス情報を提供したり、仕事モードを無効にして接続に CylanceGATEWAY を使用しないようにする機能を提供したりすることができます。 |
| Windows 10、Windows 11、および macOS のサポート | デバイスにインストールした CylanceGATEWAY エージェントはトンネルを経由して CylanceGATEWAY クラウドサービスにトラフィックを送信して、ユーザーに接続統計やステータス情報を提供したり、仕事モードを無効にして接続に CylanceGATEWAY を使用しないようにする機能を提供したりすることができます。 |
| 分割トンネル | リモートユーザーが CylanceGATEWAY をトンネルせずにインターネット上で安全なパブリックインターネットサイトに直接接続できるようにすることができます。<br>有効にすると、分割 DNS クエリにより、［プライベートネットワーク］ > ［DNS］ > ［前方ルックアップゾーン］設定にリストされているドメインの DNS ルックアップを、ネットワークアクセスコントロールが適用されているトンネルを介して実行できます。その他の DNS ルックアップはすべて、ローカル DNS を使用して実行されます。セーフモードを有効にした場合、Gateway トンネルを使用しない DNS トラフィックはセーフモードで保護されます。Android および 64 ビットの Chromebook デバイスは、ネットワークアクセスコントロールが適用されているトンネルを使用します。 |

# アーキテクチャ：CylanceGATEWAY

CylanceGATEWAY アーキテクチャは、ユーザーのデバイスと拡張ネットワークを脅威から保護するように設計されています。次の図は、2 つの動作モードでの CylanceGATEWAY のアーキテクチャを示しています。

- 仕事モード：仕事モードでは、デバイスから CylanceGATEWAY クラウドサービスを通じてネットワークリソースまでセキュリティ保護されたトンネルが作成され、そのパス上のすべてのトラフィックが保護されます。
- セーフモード：セーフモードでは、テナントの ACL ルールと、macOS および Windows デバイスのエンドポイント保護が拡張されます。有効にすると、仕事モードが無効になったときにセーフモードが自動的に有効になり、デバイスが常に保護されます。

**CylanceGATEWAY**：仕事モードが有効です

**CylanceGATEWAY** ：プライベートネットワーク上のユーザー（たとえば、企業ネットワーク上のオフィスのユーザー）用にセーフモードが有効です

**CylanceGATEWAY** ：リモートネットワーク上のユーザー用にセーフモードが有効です（たとえば、ユーザーが出張中）

| コンポーネント | 説明 |
| --- | --- |
| CylanceGATEWAY クラウドサービス | CylanceGATEWAY は、ゼロトラストネットワークアクセスを提供するクラウドベースのサービスで、ユーザーに拡張ネットワーク境界へのアクセスを提供し、デバイスと拡張ネットワークを脅威から保護します。<br>CylanceGATEWAY クラウドサービスは、機械学習を使用して継続的にネットワーク接続を評価します。ネットワーク異常イベントは、CylanceGATEWAY ユーザーが、疑わしい宛先、または悪意のあるコンテンツが含まれている可能性がある宛先に接続しようとした場合に検出されます。検出された異常により、環境に設定されているリスクしきい値に基づいて宛先へのアクセスがブロックされることがあります。 |
| 管理コンソール | クラウドベースの管理コンソールを使用すると、CylanceGATEWAY の設定、管理、監視、および接続を行うことができます。 |
| CylanceGATEWAY Connector | CylanceGATEWAY Connector は、CylanceGATEWAY サービスといずれかのプライベートネットワーク間のセキュリティ保護されたトンネルを確立するために、ファイアウォールの内側とプライベートネットワークにインストールできるオプションのコンポーネントです。CylanceGATEWAY Connector は、従来の VPN ではなく、CylanceGATEWAY を使用して、ファイアウォールの内側にあるコンテンツサーバーやアプリケーションサーバーと通信できます。 |
| BlackBerry Connectivity Node | BlackBerry Connectivity Node は、Cylance Endpoint Security がユーザーとグループをオンプレミス Microsoft Active Directory または LDAP ディレクトリと同期させることができるオプションのコンポーネントです。Cylance Endpoint Security は、BlackBerry Connectivity Node を使用しないでユーザーとグループを Microsoft Entra ID と同期できます。 |
| CylancePROTECT Mobile アプリを搭載したモバイルデバイス | CylanceGATEWAY は iOSおよび Android デバイスをサポートします。モバイルデバイスにインストールされている CylancePROTECT Mobile アプリは、セキュリティ保護されたトンネルを介してインターネットトラフィックを CylanceGATEWAY クラウドサービスに送信します。ユーザーは、仕事モードを有効または無効にして、データトラフィックが CylanceGATEWAY クラウドサービスへのトンネルを使用するかどうかを指定できます。 |

| コンポーネント | 説明 |
| --- | --- |
| CylanceGATEWAY エージェントを搭載したデスクトップデバイス | CylanceGATEWAY は、macOS および Windows 10 および 11 デバイスをサポートしています。CylanceGATEWAY には、次のような 2 つの動作モードがあります。<br>• 仕事モードの場合、CylanceGATEWAY エージェントは、セキュリティ保護されたトンネルを介してネットワークトラフィックを CylanceGATEWAY クラウドサービスに送信します。ユーザーは、仕事モードを有効または無効にして、データトラフィックがトンネルを使用するかどうかを指定できます。<br>• セーフモードの場合、CylanceGATEWAY は、アプリおよびユーザーが潜在的に悪意のある宛先にアクセスできないようにブロックし、DNS 要求をインターセプトすることで、許容可能な使用ポリシー（AUP）を強制します。CylanceGATEWAY クラウドが、設定されている ACL ルールとネットワーク保護設定に対して各 DNS クエリを評価し、リアルタイムでエージェントに要求を許可またはブロックするように指示します。許可された場合、DNS 要求が、正常にベアラーネットワーク経由で完了します。それ以外の場合、CylanceGATEWAY エージェントが、通常の応答を上書きしてアクセスを防止します。<br>セーフモードが有効になっている場合、プライベートネットワーク上のユーザー（たとえばオフィス内）は、プライベートネットワーク上のリソースにアクセスできます。リモートネットワーク上のユーザーは、プライベートネットワーク上のリソースにアクセスできません。 |
| SaaS アプリケーション | SaaS（Software-as-a-Service）アプリケーションは、クラウドベースのエンタープライズソフトウェアを提供し、複数のデバイス上のユーザーがアプリとデータを利用できるようにします。アプリケーションとデータは、主にベンダーが管理するクラウドベースのサーバー上に存在し、展開を簡素化し、オンプレミスのインフラストラクチャコストを削減しますが、ファイアウォールやその他の境界ベースのセキュリティ方式を超えたセキュリティ対策が必要です。<br>CylanceGATEWAY は、ソース IP のピン設定を有効にすることで、組織のプライベートネットワークを経由するトラフィックを必要とせずに、SaaS アプリケーションへのユーザーアクセスを保護できます。 |
| インターネットの宛先 | パブリックインターネットの宛先には、クライアントアプリがインターネット経由で接続できる IP アドレスを持つ任意の Web サイト、SaaS アプリケーション、またはその他のエンティティが含まれます。BlackBerry は、悪意のあることが知られている宛先のリストを常に増加させています。CylanceGATEWAY は、デバイス上のアプリがリスト上の宛先に接続できないようにすることができます。<br>分割トンネルを有効にすると、指定したデバイスと安全なパブリックサイト間のトラフィックは、CylanceGATEWAY 経由ではなくインターネット経由で直接送信されます。 |

# CylanceGATEWAY が仕事モードを使用してデータを送信する方法

ユーザーがプライベートネットワーク上の宛先または任意のパブリックインターネットの宛先にアクセスしようとした場合、ユーザーはアクセス制御リスト（ACL）ルールによって明示的に許可されている宛先のみにアクセスできます。各ネットワークアクセス試行は、各自の環境に設定されている ACL ルールおよび指定されたネットワーク保護設定に照らして評価されます。ACL ルールで宛先がブロックされている場合、CylanceGATEWAY は接続をブロックし、トラフィックをルーティングしません。ACL ルールがユーザーにプライベートネットワークまたはパブリックインターネットの宛先へのアクセスを許可している場合、接続は 5 分ごとに再評価され、ACL ルールが再適用されます。ユーザーのリスクレベルが変更された場合、またはアクセス試行が確立されてから宛先評価が更新された場合、接続が切断される可能性があります。ACL ルールがユーザーに宛先へのアクセスを許可していても、識別された異常やネットワーク保護設定で設定されているリスクレベルに基づき、接続のブロックまたは警告が行われる場合があります。

- ユーザーのアップロードボリュームまたはダウンロードボリュームが変更された場合、CylanceGATEWAY はトラフィックパターンの異常を警告しますが、ユーザーのトラフィックはブロックしません。
- BlackBerry の安全でないインターネット宛先のリストにある宛先、または悪意があるとして新たに特定された宛先にユーザーがアクセスしようとした場合、ネットワーク保護のリスクしきい値が［高］に設定されていると、ユーザーのアクセスはブロックされます。

CylanceGATEWAY がデバイス上でアクティブな場合、CylanceGATEWAY は次の方法でネットワークトラフィックをルーティングします。

| 移行先 | アクション |
| --- | --- |
| プライベートネットワーク上の許可された宛先 | ユーザーは、アクセス制御リスト（ACL）ルールによって明示的に許可されている場合にのみ、プライベートネットワーク上の宛先にアクセスできます。ACL ルールは各ネットワークアクセス試行を評価し、ルールが一致した場合にプライベートネットワークへのアクセスを許可します。<br><br>デバイスとプライベートネットワークの間のすべてのデータは、業界をリードするトンネルテクノロジを使用して暗号化され、CylancePROTECT Mobile アプリまたは CylanceGATEWAY エージェントから BlackBerry Infrastructure へのセキュリティ保護されたトンネルを経由してルーティングされ、その後、BlackBerry Infrastructure からファイアウォールの内側にインストールされた CylanceGATEWAY Connector へとルーティングされます。 |

| 移行先 | アクション |
| --- | --- |
| 許可されたインターネットの宛先 | ユーザーは、ACL ルールによって明示的に許可されている場合にのみ、パブリックインターネットの宛先に接続できます。ACL ルールは各ネットワークアクセス試行を評価し、ルールが一致した場合に宛先へのアクセスを許可します。<br>パブリックインターネットの宛先への接続は、CylancePROTECT Mobile アプリまたは CylanceGATEWAY エージェントとの間のセキュリティ保護されたトンネルを介して BlackBerry Infrastructure にルーティングされ、CylanceGATEWAY がトラフィックを宛先にルーティングします。<br>分割トンネルを有効にすると、安全なインターネットの宛先へのトラフィックは、CylanceGATEWAY へのトンネルを経由するのではなく、宛先に直接ルーティングされます。たとえば、安全なパブリックサイトへのトラフィックが宛先に直接ルーティングされるようにすることで、CylanceGATEWAY を通過するトラフィックを減らすことを選択できます。 |
| 許可された SaaS アプリ | デフォルトでは、SaaS アプリへの接続は、他のインターネットの宛先への接続と同じ方法でルーティングされます。<br>ソース IP のピン設定を有効にすると、組織所有の IP アドレスと CylanceGATEWAY からの接続のみを受け入れるように SaaS アプリテナントを設定できます。 |
| プライベートネットワーク上のブロックされた宛先 | ユーザーは、ACL ルールによって明示的に許可されている場合にのみ、プライベートネットワーク上の宛先にアクセスできます。宛先が許可されていない場合、CylanceGATEWAY は接続をブロックし、CylanceGATEWAY Connector にトラフィックをルーティングしません。ユーザーが宛先にアクセスしようとした際に ACL ルールによってブロックされると、試行内容とブロックされた理由がユーザーの CylanceGATEWAY エージェントの［警告］画面に表示されます。 |
| ブロックされたインターネットの宛先 | 宛先が ACL ルールによって明示的にブロックされている場合、または BlackBerry によって悪意のある可能性のある宛先であると判断された場合、CylanceGATEWAY は接続をブロックします。ユーザーが宛先にアクセスしようとした際に ACL ルールによってブロックされると、試行内容とブロックされた理由がユーザーの CylanceGATEWAY エージェントの［警告］画面に表示されます。 |

## データフロー：プライベートネットワークのアプリケーションサーバーまたはコンテンツサーバーへのアクセス

このデータフローでは、CylanceGATEWAY を使用するプライベートネットワークのデバイスとサーバー間でデータがどのように転送されるかを説明します。

上の図は、次のシーケンスを示しています。

1. ユーザーが仕事モードを有効にしてアプリを開き、いずれかのプライベートネットワークのリソースにアクセスを試みます。
2. デバイスの CylancePROTECT Mobile アプリや CylanceGATEWAY エージェントは、セキュリティ保護されたトンネル経由で BlackBerry Infrastructure の CylanceGATEWAY に接続を転送します。

3. CylanceGATEWAY は次の操作を実行します。
   a. アクセス制御リスト（ACL）ルールに基づいて、ユーザーがプライベートネットワークのそのロケーションにアクセスできるかどうかを判断します。
   b. ユーザーがアクセス権を持っている場合は、セキュリティ保護されたトンネル経由で接続を CylanceGATEWAY Connector に転送します。
4. CylanceGATEWAY Connector は、接続をプライベートネットワークの宛先に転送します。
5. CylanceGATEWAY Connector は、宛先がプライベートネットワーク上にあるフローにネットワークアドレス変換（NAT）を適用します。コネクタにより、UDP および TCP フローに関する追加情報が提供され、悪意のある可能性があるとしてブロックまたは識別されたイベントの送信元 IP アドレスとポート番号を識別できるようになります。リモート IT ツール（リモートデスクトップ接続など）を使用して、プライベートネットワークから CylanceGATEWAY Connector エンドポイントにアクセスすることはできません。

### データフロー：クラウドベースのアプリケーションまたはインターネット上の宛先へのアクセス

このデータフローは、CylanceGATEWAY を使用してデバイスとクラウドベースの SaaS アプリケーションまたはパブリックインターネットの宛先間でデータがどのように移動するかを示しています。

上の図は、次のシーケンスを示しています。

1. ユーザーが仕事モードを有効にしてアプリを開き、パブリックインターネット経由でクラウドベースのアプリケーションまたは宛先へのアクセスを試みます。
2. デバイス上の CylancePROTECT Mobile アプリまたは CylanceGATEWAY エージェントは、セキュリティ保護されたトンネルを介して暗号化されたデータを BlackBerry Infrastructure の CylanceGATEWAY に送信します。
3. CylanceGATEWAY は次の操作を実行します。
   a. アクセス制御リスト（ACL）ルールに基づいて、ユーザーがそのロケーションにアクセスできるかどうかを判断します。
   b. ユーザーがアクセスできる場合は、データを SaaS アプリケーションに送信するか、インターネットの宛先へのアクセスを許可します。
   c. ソース IP アドレスを置き換えて、SaaS アプリおよびインターネット宛先にアクセスするフローにネットワークアドレス変換（NAT）を適用します。
4. ソース IP ピン設定が有効になっている場合、SaaS アプリケーションは、アクセスを許可する前に、CylanceGATEWAY テナントに関連付けられている IP アドレスから接続が確立されていることを確認します。

## CylanceGATEWAY がセーフモードを使用してデータを送信する仕組み

ユーザーが任意のパブリックインターネットの宛先にアクセスしようとした場合、ユーザーはアクセス制御リスト（ACL）ルールによって明示的に許可されている宛先のみにアクセスできます。セーフモードが有効になっている場合、CylanceGATEWAY は、ユーザーが悪意のある可能性のある宛先にアクセスするのをブロックし、DNS 要求を傍受することで利用規定（AUP）を適用します。CylanceGATEWAY クラウドサービスは、設定された ACL ルールとネットワーク保護設定に基づいて各 DNS クエリを評価し、リアルタイムで要求を許可またはブ

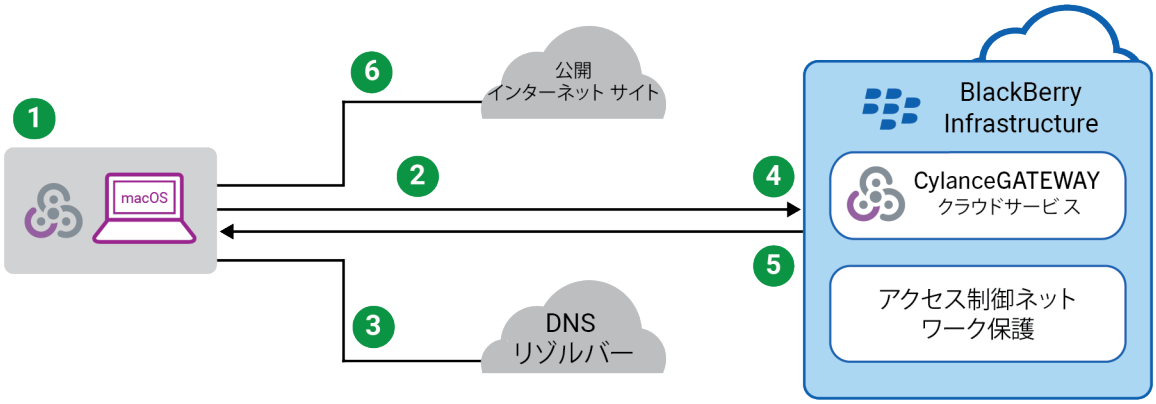
ロックするようエージェントに指示します。ACL ルールで宛先がブロックされると、CylanceGATEWAY はアクセスを禁止します。許可されると、ネットワーク DNS クエリをベアラーネットワーク上で完了できます。

macOS または Windows デバイスでセーフモードが有効になっている場合、CylanceGATEWAY は、次の方法でネットワークトラフィックを送信します。

| 移行先 | アクション |
| --- | --- |
| 許可されたインターネットの宛先 | ユーザーは、ACL ルールによって明示的に許可されている場合にのみ、パブリックインターネットの宛先にアクセスできます。ACL ルールは各ネットワークアクセス試行を評価し、ルールが一致した場合に宛先へのアクセスを許可します。<br>セーフモードを有効にすると、安全なインターネットの宛先へのトラフィックは、CylanceGATEWAY トンネルを経由せずにベアラーネットワーク経由で宛先にルーティングされます。<br>分割トンネルを有効にすると、安全なインターネットの宛先へのトラフィックは、ベアラーネットワーク経由で宛先にルーティングされ、セーフモードで保護されます。これにより、安全なパブリックサイトへのトラフィックが宛先に直接ルーティングされるようにして、CylanceGATEWAY を通過するトラフィックを減らすことができます。 |
| ブロックされたインターネットの宛先 | 宛先が ACL ルールによって明示的にブロックされている場合、または BlackBerry によって悪意のある可能性のある宛先であると判断された場合、CylanceGATEWAY は DNS クエリをブロックします。ユーザーが宛先にアクセスしようとした際に ACL ルールによってブロックされると、試行内容とブロックされた理由がユーザーの CylanceGATEWAY エージェントの［警告］画面に表示されます。 |

## データフロー：コンテンツ、アプリケーション、パブリックインターネットの宛先へのアクセス（セーフモード使用）

このデータフローは、セーフモードを使用して、デバイスとパブリックインターネットの宛先の間でデータがどのように移動するかを示しています。セーフモードの場合、CylanceGATEWAY は、アプリおよびユーザーが潜在的に悪意のある宛先にアクセスできないようにブロックし、DNS 要求をインターセプトすることで、許容可能な使用ポリシー（AUP）を強制します。CylanceGATEWAY クラウドサービスが、設定されている ACL ルールとネットワーク保護設定に対して各 DNS クエリを評価し、リアルタイムでエージェントに要求を許可またはブロックするように指示します。許可された場合、DNS 要求が、正常にベアラーネットワーク経由で完了します。それ以外の場合、CylanceGATEWAY エージェントが、通常の応答を上書きし、アクセスを防止します。




上の図は、次のシーケンスを示しています。

1. CylanceGATEWAY エージェントでセーフモードが有効であり、ユーザーがインターネットの宛先にアクセスを試みます。
2. CylanceGATEWAY エージェントでは、デバイスからの DNS 要求をインターセプトし、その要求からの情報で CylanceGATEWAY クラウドサービスをクエリします。
3. エージェントが、要求を元の DNS サーバーにプロキシします。
4. CylanceGATEWAY クラウドサービスが、設定されている ACL ルールとネットワーク保護設定に対して各クエリを評価し、エージェントに要求を許可またはブロックするように指示します。
5. アクセスが許可された場合、エージェントが、元の DNS 要求への応答として元の DNS サーバーの応答をプロキシします。それ以外の場合、エージェントが、アクセスをブロックする DNS 応答を注入します。
6. エージェントが、許可された DNS 要求の結果を使用してインターネットの宛先にアクセスします。

# CylanceAVERT とは

CylanceAVERT は情報保護ソリューションです。外部ソースを介して機密性の高い規制情報や組織情報が損失することを検出、防止することができます。CylanceAVERT は、会社の機密情報を検出、分類、一覧化し、脅威を検出して不正流出イベントを防止することができます。また、CylanceAVERT は機密性の高いファイルインベントリや脅威管理を提供するだけでなく、メールメッセージの本文ファイルや添付ファイルのスキャン、USB デバイスやネットワークドライブへのコピー、ブラウザエリアへのアップロード、修正アクションの推奨も行います。

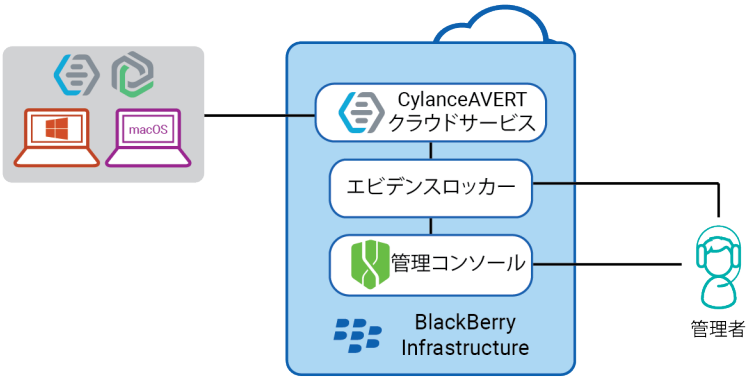
ユーザーが USB、ブラウザのドメイン、メールメッセージを使用して機密データをアップロードしようとすると、CylanceAVERT がコンテンツをスキャンし、情報保護ポリシーに基づいた機密データであるかどうかを判断します。ポリシーに違反している場合、警告がユーザーに送信され、設定されている修正アクションが適用されます。

## CylanceAVERT の主な機能

| 機能 | 説明 |
| --- | --- |
| 機密データのスキャン | CylanceAVERT では、USB ドライブ、インターネットブラウザ、メールの添付ファイルにアップロードされたファイルをスキャンしたり、管理者が情報保護ポリシーで機密として定義した会社データについてメールメッセージの本文コンテンツをスキャンしたりできます。データ窃盗イベントに関するメール通知が送信されます。 |
| 情報保護ポリシー | ポリシー違反をトリガーするために満たす必要がある条件を指定したり、ポリシーで許可するドメイン、およびポリシー違反時に実行するアクションを指定したりできます。詳細については、『Cylance Endpoint Security セットアップガイド』の「情報保護ポリシーの管理」を参照してください。 |
| CylanceAVERT イベント | 情報保護ポリシーを作成して、データや満たす必要がある条件を指定してポリシー違反をトリガーしたり、ポリシーを適用する場所、監視するアクティビティ、およびポリシー違反時に実行する修正アクションを指定したりできます。詳細については、『Cylance Endpoint Security 管理ガイド』の「CylanceAVERT イベント」を参照してください。 |
| 情報保護の設定 | 情報保護設定を使用して、情報保護ポリシーで使用するテンプレートとデータタイプを追加することで、監視対象の機密データを設定できます。また、管理者は、許可され信頼されるブラウザおよびメールドメインを定義し、データ窃盗イベントのために収集する証拠を管理し、その証拠を利用できる期間を指定することもできます。さらに、指定されたメールアドレスにデータ窃盗イベントの通知を送信することもできます。詳細については、『Cylance Endpoint Security セットアップガイド』の「情報保護の設定を使用した機密コンテンツの定義」を参照してください。 |

| 機能 | 説明 |
| --- | --- |
| ファイルインベントリ | CylanceAVERT ファイルインベントリでは、ファイルのトローリングプロセスを通じて、組織内のすべての機密ファイルのレコードが作成されます。詳細については、『Cylance Endpoint Security 管理ガイド』の「ファイルインベントリを使用した機密ファイルの識別」を参照してください。 |
| エビデンスロッカー | 証拠ロッカーを使用して、窃盗イベントに関与したファイルの詳細を表示し、監査目的でファイルをローカルストレージにダウンロードできます。詳細については、『Cylance Endpoint Security 管理ガイド』の「証拠ロッカーを使用した窃盗イベント詳細の表示」を参照してください。 |

# アーキテクチャ：CylanceAVERT




| 項目 | 説明 |
| --- | --- |
| CylanceAVERT | CylanceAVERT は、メールメッセージや添付ファイル、ブラウザのアップロード、USB デバイスを介して機密データが流出するのを防ぎます。 |
| エビデンスロッカー | 証拠ロッカーは、管理者が詳細な検査を行うために、不正流出イベントに関与したファイルを保存するプライベートファイルストレージ領域です。 |
| 管理コンソール | クラウドベースの管理コンソールを使用すると、監視および保護する会社の機密データを定義し、ユーザーポリシーを管理して、窃盗イベントをトリガーするために満たす必要がある条件の指定、組織内の機密ファイルの表示、リスクを評価し修復するためのさまざまな脅威関連イベントの表示を行うことができます。 |
| CylanceAVERT および CylancePROTECT を搭載したデバイス | CylanceAVERT 機能を利用するには、エンドポイントに CylancePROTECT Desktop をインストールする必要があります。CylanceAVERT は Windows 10 および 11 をサポートしています。 |

# 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