



# Cylance Endpoint Security

ユーザーガイド



# Contents

<b>Cylance Endpoint Security</b> のエンドユーザーとしての使用.....	<b>4</b>
<b>CylancePROTECT Mobile</b> アプリとは.....	<b>5</b>
CylancePROTECT Mobile アプリの主な機能.....	5
<b>CylancePROTECT Mobile</b> アプリを使用する.....	<b>8</b>
CylancePROTECT Mobile アプリのインストールおよびアクティブ化.....	8
CylancePROTECT Mobile アプリでの仕事モードの有効化.....	9
メッセージスキャン機能の有効化.....	10
モバイルの脅威の解決.....	11
CylancePROTECT Mobile アプリで検出されたモバイルの脅威.....	14
BlackBerry への問題の報告.....	15
CylancePROTECT Mobile アプリの非アクティブ化.....	15
<b>Cylance Endpoint Security</b> エージェントの概要.....	<b>17</b>
CylancePROTECT Desktop エージェントのステータスアイコン.....	18
<b>CylanceGATEWAY</b> エージェントの使用.....	<b>20</b>
CylanceGATEWAY エージェントでの仕事モードの有効化.....	20
CylanceGATEWAY エージェントの設定.....	20
CylanceGATEWAY エージェントでのセーフモードのアクティブ化.....	21
商標などに関する情報.....	<b>23</b>

# Cylance Endpoint Security のエンドユーザーとしての使用

このガイドは、CylancePROTECT Mobile アプリおよび Cylance Endpoint Security エージェントが、ネットワークに接続されたデバイスや機密データを、悪意のある脅威やサイバー攻撃からどのように保護するかをエンドユーザーの皆様に理解していただくためのものです。

CylancePROTECT Mobile アプリは、モバイルデバイスの全体的なセキュリティ評価を提供し、セキュリティの脅威について警告し、これらの脅威を解決できるようにします。CylancePROTECT Mobile アプリの詳細については、「[CylancePROTECT Mobile アプリとは](#)」を参照してください。アプリのインストールと使用方法については、「[CylancePROTECT Mobile アプリを使用する](#)」を参照してください。

このガイドでは、Cylance Endpoint Security エージェントがデスクトップデバイスを保護する仕組みについても説明しています。これらのエージェントは、管理者によって設定され、バックグラウンドで実行されます。通常、追加のアクションは必要ありません。デバイスを保護するためのエージェントとその役割の詳細については、次を参照してください：[Cylance Endpoint Security エージェントの概要](#)

CylanceGATEWAY エージェントでは、一部の機能を管理することができます。詳細については、「[CylanceGATEWAY エージェントの使用](#)」を参照してください。

# CylancePROTECT Mobile アプリとは

CylancePROTECT Mobile アプリを使用すると、モバイルデバイスのセキュリティをより認識しやすくなり、管理者の介入なしに脅威を解決するための対策を講じることができます。

CylancePROTECT Mobile アプリには次の機能があります。

- デバイスの全体的なセキュリティ評価
- 検出された悪意のあるアプリまたはサイドロードされたアプリのリスト
- ネットワークの問題や、セキュリティリスクをもたらすデバイス設定に関するアラート
- テキストメッセージ内の悪意のある URL を検出する機能
- 悪意のあるアプリやサイドロードされたアプリのアンインストール、デバイスの設定や条件の修正など、ユーザーにわかりやすい方法で修正措置を講じるように指示することができます

CylancePROTECT Mobile アプリは定期的にデバイスをスキャンして脅威を特定します。アプリが脅威を検出すると、アプリで詳細を表示できます。可能な限り、アプリは脅威を解決するためのガイドを表示し、問題に対処できるデバイス設定を案内します。詳細については、「[CylancePROTECT Mobile アプリの主な機能](#)」を参照してください。

Cylance Endpoint Security 管理者は CylancePROTECT Mobile アプリを設定して、脅威が検出されたときにデバイス通知、メール通知を送信したり、通知を送信しないようにしたりできます。CylancePROTECT Mobile アプリでは常に、アクティブなアラートを表示できます。

Android バージョン 2.3.0.1640 以降の 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、CylancePROTECT Mobile 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。

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。

## CylancePROTECT Mobile アプリの主な機能

CylancePROTECT Mobile アプリは、次の表で説明する警告機能の特徴としています。

アプリのセキュリティ機能	説明
悪意のあるアプリ	アプリを分析して、悪意のある可能性があるかどうかを判断します。悪意があると考えられるアプリをインストールした場合、CylancePROTECT Mobile アプリはデバイス通知を送信します。
サイドロードされたアプリ	サイドロードされたアプリとは、非公式または未知のソースからインストールされたアプリのことです。公式のアプリストアで配布されるアプリと同じ制限や保護に従っていないため、安全ではないと考えられます。サイドロードされたアプリが検出されると、CylancePROTECT Mobile アプリはデバイス通知を送信します。

デバイスのセキュリティ機能	説明
開発者オプション	デバイスで開発者オプションを有効にすると、一部の機密設定とオプションが使用可能になります。開発者オプションが有効になっている場合、CylancePROTECT Mobile アプリはデバイス通知を送信します。
ルート検出	デバイスがルート化、またはジェイルブレイク状態になっている場合、この事実は、ユーザー自身または第三者が、デバイスのオペレーティングシステムへのルートアクセスを可能にするソフトウェアまたは操作をデバイスで実行したことを示しています。ユーザー自身または管理者は、デバイスからルート化ソフトウェアを削除するか、デバイスをデフォルトの状態に復元する操作をデバイスで実行する必要があります。デバイスがルート化されているかジェイルブレイク状態であることが検出されると、CylancePROTECT Mobile アプリはデバイス通知を送信します。
フルディスク暗号化	デバイス上の暗号化されていないデータは、許可されていないユーザーが簡単に読み取ることができます。暗号化が有効になっていない場合、CylancePROTECT Mobile アプリはデバイス通知を送信します。
画面ロック	画面ロックを設定すると、デバイスの紛失や盗難などの際も、デバイスへの不正アクセスを防止できます。画面ロックのパスワードまたは指紋が設定されていない場合、CylancePROTECT Mobile アプリはデバイス通知を送信します。
認証	<p>デバイス上の CylancePROTECT Mobile アプリは定期的に整合性と信頼性をチェックします。デバイスがこれらのチェックに合格しない場合、CylancePROTECT Mobile アプリはデバイス通知を送信します。</p> <p>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。</p>
デバイス OS	管理者は、組織のセキュリティ要件を満たしていない一部のデバイス OS バージョンを制限する場合があります。制限対象デバイス OS バージョンがデバイスで実行されていることを検出すると、CylancePROTECT Mobile アプリはデバイス通知を送信します。
デバイスモデル	管理者は、組織のセキュリティ要件を満たしていない一部のデバイスモデルを制限する場合があります。制限対象のデバイス OS モデルがデバイスで実行されていることを検出すると、CylancePROTECT Mobile アプリはデバイス通知を送信します。

ネットワーク保護機能	説明
Wi-Fi セキュリティ	デバイスが、安全でないと考えられるネットワーク暗号化プロトコルを使用している Wi-Fi アクセスポイントに接続している場合、CylancePROTECT Mobile アプリはデバイス通知を送信します。
ネットワーク接続	CylancePROTECT Mobile アプリは、CylancePROTECT Mobile クラウドサービスへのネットワーク接続を評価して、接続が安全かどうかを判断します。接続が安全でないと考えられる場合、CylancePROTECT Mobile アプリはデバイス通知を送信します。
メッセージスキャン機能	説明
SMS メッセージスキャン	URL を含む SMS メッセージを受信すると、URL がスキャンされて、悪意のある可能性があるかどうか判断されます。悪意のある URL が検出されると、CylancePROTECT Mobile アプリはデバイス通知を送信しません。
CylanceGATEWAY の機能	説明
仕事モード	CylancePROTECT Mobile アプリで仕事モードを有効にすると、ネットワークリソースに安全にアクセスできるようにし、不審な、または潜在的に悪意のあるネットワークアクティビティから、デバイスを保護します。

# CylancePROTECT Mobile アプリを使用する

このセクションを使用して CylancePROTECT Mobile アプリをセットアップし、アプリが提供する機能と、モバイルデバイスのアラートを解決するために実行できるアクションを理解します。

## CylancePROTECT Mobile アプリのインストールおよびアクティ ブ化

作業を始める前に：

- 管理者からアプリをアクティブ化するための情報が記載されたアクティベーションメールを受信したら、CylancePROTECT Mobile アプリをアクティブ化することができます。
  - 自分がディレクトリユーザーであるか、BlackBerry Online Account ユーザーであるかについては、管理者から通知される場合があります。自分が BlackBerry Online Account ユーザーで、資格情報を知らない場合は、[BlackBerry Online Account のパスワードリセットページ](#)に移動してメールアドレスを入力し、パスワードリセットメールの指示に従って、CylancePROTECT Mobile アプリをアクティブ化するために使用するパスワードを設定します。
  - JavaScript は、デフォルトのモバイルブラウザで有効にする必要があります。CylancePROTECT Mobile アプリは、Google Chrome、Samsung インターネット、および Safari をサポートしています。
1. CylancePROTECT Mobile アプリは App Store または Google Play からダウンロードしてインストールします。
  2. CylancePROTECT Mobile アプリを開きます。
  3. BlackBerry のプライバシー通知および利用規約を確認し、同意します。
  4. 次の操作のいずれかを実行します。

タスク	手順
QR Code を使用してアプリをアクティブ化します。	<ol style="list-style-type: none"><li>a. [QR コードをスキャン] をタップします。</li><li>b. QR Code (受信した CylancePROTECT Mobile アプリのアクティベーションメールからのもの) をスキャンします。</li></ol>
ディレクトリユーザー：仕事用メールアドレスとパスワードを使用してアプリをアクティブ化します	<ol style="list-style-type: none"><li>a. [管理者から指示されたアカウントの資格情報でサインインします] をタップします。</li><li>b. カスタムドメインの入力を求められたら、受信した CylancePROTECT Mobile アプリのアクティベーションメールに記載されているドメインを入力します (オプション C)。[次へ] をタップします。</li><li>c. [ユーザー名] フィールドに、仕事用メールアドレスを入力します。[次へ] をタップします。</li><li>d. [パスワード] フィールドに、仕事用メールのパスワードを入力します。[次へ] をタップします。</li></ol>



タスク	手順
BlackBerry Online Account ユーザー : CylancePROTECT Mobile アプリを BlackBerry Online Account のメールアドレスとパスワードを使用してアクティブ化します	<ol style="list-style-type: none"> <li>[管理者から指示されたアカウントの資格情報でサインインします] をタップします。</li> <li>カスタムドメインの入力を求められたら、受信した CylancePROTECT Mobile アプリのアクティベーションメールに記載されているドメインを入力します (オプション C)。[次へ] をタップします。</li> <li>[ユーザー名] フィールドに、BlackBerry Online Account のメールアドレスを入力します。[次へ] をタップします。</li> <li>[パスワード] フィールドに、BlackBerry Online Account のパスワードを入力します。[次へ] をタップします。</li> </ol>
アクティベーションパスワードを使用して CylancePROTECT Mobile アプリをアクティブ化します	<ol style="list-style-type: none"> <li>[アクティベーションメールに記載されている資格情報を入力します] をタップします。</li> <li>[カスタムドメイン] フィールドに、受信した CylancePROTECT Mobile アプリのアクティベーションメールに記載されているドメインを入力します (オプション B)。</li> <li>[ユーザー名] フィールドにユーザー名を入力します。</li> <li>[アクティベーションパスワード] フィールドにアクティベーションパスワードを入力します。</li> <li>[続行] をタップします。</li> </ol>

5. 管理者による設定によっては、さまざまな機能へのアクセスを有効にして許可するよう求めるプロンプトが複数表示される場合があります。必要に応じてプロンプトに入力して、アクセス権限を許可し、さらに表示される指示を完了します。

Wi-Fi 保護機能のネットワークの変更を検出するには、常にバックグラウンド位置情報権限を許可する必要があります。

終了したら :

- CylancePROTECT Mobile アプリのバックグラウンドアクティビティを許可する必要があります。
- 追加のデバイスに CylancePROTECT Mobile アプリをインストールしてアクティブ化するには、これらの手順を繰り返します。
- Android 用 CylancePROTECT Mobile アプリの新バージョンが Google Play で公開されると、アプリで通知が表示されます。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。
- 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。
- 「[CylancePROTECT Mobile アプリでの仕事モードの有効化](#)」と「[メッセージスキャン機能の有効化](#)」を参照してください。

## CylancePROTECT Mobile アプリでの仕事モードの有効化

管理者がこの CylanceGATEWAY 機能を設定している場合、CylancePROTECT Mobile アプリで仕事モードを有効にして、ネットワークリソースに安全にアクセスし、不審なネットワークアクティビティや潜在的に悪意のあるネットワークアクティビティからデバイスを保護できます。この機能を有効にすると、ネットワークアクティビ



ティを分析するための安全なアクセスが設定され、管理者によって管理されるネットワークアクセスポリシーが適用されます。

作業を始める前に：CylancePROTECT Mobile アプリのバックグラウンド位置情報権限は、常に許可する必要があります。

1. CylancePROTECT Mobile で、次のいずれかを実行します。
  - ・ [仕事モード] 設定を有効にします。
  - ・ [安全に仕事に切り替える] > [仕事モードを有効化] をタップします。
2. [OK] をタップします。
3. [接続要求] ダイアログで、[OK] をタップして確認します。

接続が確立されると、「有効」ステータスが表示されます。

終了したら：

- ・ 管理者からこの CylanceGATEWAY 機能の TCP 接続を有効にするように求められた場合は、CylanceGATEWAY 画面で  または  をタップして、[TCP を使用] オプションを選択します。
- ・ 疑わしいネットワークアクティビティに関する警告を表示するには、[警告を表示] をタップします。[警告] 画面から警告通知をミュートすることもできます。

## メッセージスキャン機能の有効化

CylancePROTECT Mobile アプリのメッセージスキャン機能を有効にして、受信した SMS メッセージをスキャンし、悪意を持っている可能性がある URL を探すことができます。メッセージ内の URL だけが評価対象です。

iOS デバイスの場合、不明な送信者（デバイスの連絡先でない発信元）からのメッセージのみがスキャンされます。悪意を持っている可能性がある URL を含むメッセージは、迷惑メールフォルダにフィルタリングされます。

Android デバイスの場合、既知の連絡先および不明な送信者からのすべてのメッセージがスキャンされます。悪意を持っている可能性がある URL を含むメッセージは CylancePROTECT Mobile アプリに表示されますが、デフォルトのメッセージングアプリで手動で削除する必要があります。

モバイルデバイスで、次のいずれかを実行します。

デバイス	手順
iOS	<ol style="list-style-type: none"><li>a. [設定] アプリを開きます。</li><li>b. [メッセージ] &gt; [メッセージフィルタリング] &gt; [不明な送信者および迷惑メッセージ] の順に選択します。</li><li>c. [メッセージフィルタリング] セクションで、[不明な差出人をフィルタ] 設定を有効にします。</li><li>d. [SMS フィルタリング] セクションで、[Protect] をタップします。</li><li>e. [有効にする] をタップします。</li></ol> <p>これらの手順は CylancePROTECT Mobile アプリの、[デバイスの健全性] &gt; [メッセージのスキャン] から参照できます。</p> <p>iMessage アプリを使用している場合は、アプリで [SMS として送信] オプションを有効にします。</p>

デバイス	手順
Android	<ol style="list-style-type: none"> <li>a. CylancePROTECT Mobile アプリで、[デバイスの健全性] をタップします。</li> <li>b. [メッセージのスキャン] をタップして展開します。</li> <li>c. メッセージスキャン機能を有効にします。</li> <li>d. [メッセージスキャンを許可] 画面で、[許可する] をタップします。</li> <li>e. [OK] をタップします。</li> </ol>

CylancePROTECT Mobile アプリで、「スキャンが有効」のステータスメッセージが表示されます。

## モバイルの脅威の解決

CylancePROTECT Mobile アプリによってモバイルの脅威がデバイスで検出されると、デバイス通知が送られてきます。CylancePROTECT Mobile アプリを開くことで、脅威を速やかに特定して解決できます。

1. CylancePROTECT Mobile アプリを開きます。
2. [デバイスの健全性] をタップします。
3. 次のセクションのいずれかを展開します。
  - ・ アプリのセキュリティ
  - ・ デバイスセキュリティ
  - ・ ネットワーク保護
4. 次の表を使用すると、デバイスで検出された脅威を解決するのに役立ちます。

機能	プラットフォーム	説明	レゾリューション
アプリのセキュリティ			
悪意のあるアプリ	Android	セクションを展開して、アプリによって検出された悪意のあるアプリのリストを表示します。	[修正] をタップして、悪意のあるアプリをデバイス OS からアンインストールします。

機能	プラットフォーム	説明	レゾリューション
サイドロードされたアプリ	Android iOS	<p>サイドロードされたアプリとは、不明または信頼できないソースからインストールされたアプリのことです。</p> <p>Android デバイスでは、セクションを展開すると、アプリが検出したサイドロードされたアプリのリストが表示されます。</p> <p>iOS デバイスでは、セクションを展開すると、信頼され、デバイスにインストールされているサードパーティアプリケーションの開発者プロファイルのリストが表示されます。</p>	<p>[修正] をタップして、サイドロードされたアプリを削除する手順を表示します。</p> <p>Android デバイスでは、デバイス設定でアプリをアンインストールするように指示されます。</p> <p>iOS デバイスでは、[設定] アプリでデバイスから信頼できるアプリプロファイルを削除するように指示されます。</p>
デバイスセキュリティ			
開発者オプション	Android	<p>開発者オプションは、デバイスで開発者モードが有効になっているかどうかを示します。</p>	<p>[修正] をタップして、開発者モードをオフにする手順を表示します。デバイス設定に移動して、開発者モードをオフにするように指示されます。</p>
ルート検出	Android iOS	<p>ルート検出では、デバイスがルート化されているかジェイルブレイク状態であることがアプリによって検出されると、通知が表示されます。</p>	<p>アプリでのアクションはありません。解決策について管理者に問い合わせる必要があります。</p>
フルディスク暗号化	Android	<p>フルディスク暗号化は、デバイスでディスク暗号化が有効になっているかどうかを示します。</p>	<p>[修正] をタップして、ディスク暗号化を有効にする手順を表示します。デバイス設定でディスク暗号化をオンにするように指示されます。</p>

機能	プラットフォーム	説明	レゾリューション
画面ロック	Android iOS	画面ロックは、画面ロックオプション（パスワードや指紋など）が現在デバイスで有効になっているかどうかを示します。	<p>[修正] をタップして、画面ロックを有効にする手順を表示します。</p> <p>Android デバイスでは、デバイス設定に移動して画面ロックを有効にするように指示されます。</p>
デバイスの認証	Android iOS	<p>Android デバイスでは、CylancePROTECT Mobile アプリで次のいずれかで失敗した場合に通知が表示されます。</p> <ul style="list-style-type: none"> <li>• SafetyNet または Play Integrity 認証</li> <li>• ハードウェア証明書の認証</li> <li>• ハードウェア認証のセキュリティレベルが CylancePROTECT Mobile ポリシーで設定されているセキュリティレベルよりも低い</li> <li>• ハードウェア認証のセキュリティパッチレベルが CylancePROTECT Mobile ポリシーで設定されているものよりも低い</li> <li>• ハードウェア認証のブート状態が未検証</li> </ul> <p>iOS デバイスでは、CylancePROTECT Mobile アプリが Apple DeviceCheck フレームワークを使用した整合性チェックに失敗した場合に通知が表示されます。</p>	<p>Android デバイスの場合、セキュリティパッチレベルが設定されている最小パッチを満たしていない場合は、[修正] をタップしてソフトウェアアップデートを確認します。</p> <p>他の認証アラートと整合性チェックの場合、アプリでのアクションはありません。解決策について管理者に問い合わせる必要があります。</p>
デバイス OS	Android iOS	デバイス OS は、割り当てられた CylancePROTECT ポリシーの要件をデバイス OS が満たしているかどうかを示します。	<p>[修正] をタップして、OS のアップグレード手順を表示します。</p> <p>Android デバイスでは、デバイス設定で OS をアップグレードするように指示されます。</p>

機能	プラットフォーム	説明	レゾリューション
デバイスモデル	Android iOS	デバイスモデルは、割り当てられた CylancePROTECT ポリシーの要件をデバイスモデルが満たしているかどうかを示します。	アプリで実行するアクションはありません。解決策について管理者に問い合わせる必要があります。
ネットワーク保護			
ネットワーク接続	Android iOS	ネットワーク接続は、現在のネットワークが危険かどうかを示します。	<p>[修正] をタップして、安全ではないネットワークから切断する手順を表示します。</p> <p>Android デバイスでは、ネットワークから切断するデバイス設定に移動するオプションがあります。</p>
Wi-Fi のセキュリティ	Android	Wi-Fi セキュリティは、現在の Wi-Fi ネットワークが安全でないかどうかを示します。	<p>[修正] をタップして、Wi-Fi ネットワークから切断する手順を表示します。</p> <p>Android デバイスでは、Wi-Fi ネットワークから切断するデバイス設定に移動するオプションがあります。</p>
メッセージのスキャン機能			
検出されたマルウェアメッセージ	Android iOS	潜在的に悪意のある URL を含む SMS テキストメッセージを識別します。	<p>Android デバイスで、[修正] をタップしてデフォルトのメッセージングアプリに移動し、テキストメッセージを削除します。</p> <p>iOS デバイスでは、テキストメッセージは自動的に迷惑メールフォルダに振り分けられます。</p>


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

CylancePROTECT Mobile アプリには、次の脅威が表示されます。

モバイルセキュリティの脅威	リスクレベル	色
悪意のあるアプリ	高	赤

モバイルセキュリティの脅威	リスクレベル	色
サイドロードされたアプリ	高	赤
デバイスセキュリティ：開発者オプション	中	黄
デバイスセキュリティ：画面ロック	中	黄
デバイスセキュリティ：ルート化されたデバイスまたは侵害されたデバイス	高	赤
デバイスセキュリティ：フルディスク暗号化	中	黄
デバイスセキュリティ：認証	高	赤
デバイスセキュリティ：セキュリティパッチレベル	中	黄
デバイスセキュリティ：デバイス OS	中	黄
デバイスセキュリティ：デバイスモデル	中	黄
ネットワーク保護：ネットワーク接続	高	赤
ネットワーク保護：Wi-Fi セキュリティ	中	黄
SMS メッセージスキャン（Android に対してのみ表示）	中	黄

## BlackBerry への問題の報告

1. CylancePROTECT Mobile アプリのホーム画面で、 をタップします。
2. [問題を報告] をタップします。
3. 問題についての説明を入力します。
4. [送信] をタップします。

## CylancePROTECT Mobile アプリの非アクティブ化

アプリを非アクティブにすると、デバイスはセキュリティリスクに関する警告通知を受信しなくなります。この CylanceGATEWAY 機能は、作業リソースおよび作業アプリケーションにアクセスすることにも使用できなくなります。

作業を始める前に： デバイスがワイヤレスネットワークに接続されていることを確認します。

CylancePROTECT Mobile アプリのホーム画面で、次のいずれかを実行します。

デバイス	手順
iOS	<ol style="list-style-type: none"><li>🔒 をタップします。</li><li>「非アクティブ化」をタップします。</li><li>再度「非アクティブ化」をタップします。</li></ol>
Android	<ol style="list-style-type: none"><li>🔒 をタップします。</li><li>「非アクティブ化」をタップします。</li><li>再度「非アクティブ化」をタップします。</li><li>「OK」をタップします。</li></ol>

終了したら：デバイスから CylancePROTECT Mobile アプリを削除します。



# Cylance Endpoint Security エージェントの概要



Cylance Endpoint Security エージェントはデスクトップコンピュータ上で実行されます。通常は管理者によって展開され、デバイスに自動的にインストールされます。次の表に、デスクトップエージェントとその使用方法を示します。


エージェント	処理	使用方法
CylancePROTECT Desktop	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。	管理者は、デバイスに展開して自動的にインストールされるようにするか、手動でインストールするための手順を提供します。  CylancePROTECT Desktop は、ユーザーのログイン後、デバイスのバックグラウンドで実行されます。
CylanceOPTICS	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が及ぶ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。	管理者は、デバイスに展開して自動的にインストールされるようにするか、手動でインストールするための手順を提供します。  CylanceOPTICS は、ユーザーのログイン後、デバイスのバックグラウンドで実行されます。
CylanceGATEWAY (デスクトップエージェント)	CylanceGATEWAY は、従来のVPNを必要とせずに、組織のオンプレミスおよびクラウドベースのリソース、サービス、アプリケーションへの安全なアクセスを提供します。また、デバイスを保護するために、組織が危険で悪意のある可能性のある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します。	管理者は、デバイスに展開して自動的にインストールされるようにするか、手動でインストールするための手順を提供します。  ディレクトリ資格情報または CylanceGATEWAY 資格情報を使用して BlackBerry Online Account をアクティブ化する必要があります。CylanceGATEWAY エージェントをアクティブ化すると、次のいずれかが適用されることがあります。 <ul style="list-style-type: none"><li>エージェントから、仕事モードを有効にすることができます。</li><li>管理者がエージェントの起動時に仕事モードを自動的に開始して有効にするようにエージェントを設定している場合、追加のアクションは必要ありません。</li></ul>

エージェント	処理	使用方法
CylanceAVERT	CylanceAVERTでは、組織環境で検出された機密ファイルを識別したり分類したりすることができます。これらの機密ファイルにおいて、さまざまなソース（USB またはネットワークドライブ、メールメッセージ、ブラウザのアップロード）によりデータが流出されそうになると、CylanceAVERTでは、管理者が指定した修正アクションが実行され、データが保護されるようになります。	管理者は、デバイスに展開して自動的にインストールされるようにするか、手動でインストールするための手順を提供します。  CylanceAVERTは、ユーザーのログイン後、デバイスのバックグラウンドで実行されます。

## CylancePROTECT Desktop エージェントのステータスアイコン

CylancePROTECT Desktop がデバイスにインストールされている場合、システムトレイのアイコンがエージェントステータスを示します。

ステータスアイコン	ステータスの説明
	<p>安全：デバイスでは、現在アクティブな脅威は検出されていません。すべての脅威がエージェントによって正常にブロックまたは終了されました。</p> <p>このステータスは、報告されたすべての脅威がブロックされたか、終了されたか、除外リストに追加された場合に表示されます。</p>
	<p>危険：デバイスでは、アクティブな脅威がありますが、実行がブロックされていません。</p> <p>このステータスは、脅威が検出され、Cylance クラウドサービスに報告されたが、デバイスでの実行がブロックされていない場合に表示されます。デバイスポリシーの除外リストにも追加されていません。</p> <p>このステータスを解決するには、次のことを実行します。</p> <ul style="list-style-type: none"> <li>• CylancePROTECT エージェント UI を開いて、脅威のリストを表示します。疑わしいアプリケーションを使用しないようにするか、アプリケーションを終了して脅威を排除します。</li> <li>• 脅威が仕事関連のアプリやスクリプトなど正規のソースからの場合は、管理者に問い合わせてデバイスポリシーで除外を追加します。</li> </ul>

ステータスアイコン	ステータスの説明
	<p>オフライン：デバイスが Cylance クラウドサービスに接続できませんでした。</p> <p>このステータスは、次のいずれかの理由で表示される場合があります。</p> <ul style="list-style-type: none"><li>• デバイスがインターネットに接続されていない</li><li>• デバイス接続がファイアウォールまたはポートによってブロックされている</li><li>• デバイスが Cylance クラウドサービスに接続できなくなっている</li></ul> <p>このステータスを解決するには、次のことを実行します。</p> <ul style="list-style-type: none"><li>• 有線またはワイヤレスネットワーク接続を確認します。</li><li>• ネットワーク設定を確認します。たとえば、プロキシまたは VPN 接続を使用している場合は、管理者とともに設定を確認します。</li><li>• 管理者に問い合わせて接続を確認します。</li></ul>

# CylanceGATEWAY エージェントの使用

管理者が CylanceGATEWAY エージェントを設定している場合は、このセクションを使用して、エージェントで管理できる機能を確認します。

## CylanceGATEWAY エージェントでの仕事モードの有効化

管理者が CylanceGATEWAY サービスを設定した場合は、Windows および macOS デバイスの CylanceGATEWAY エージェントで仕事モードを有効にしてネットワークリソースに安全にアクセスし、不審なネットワークアクティビティや潜在的な悪意のあるネットワークアクティビティからデバイスを保護できます。管理者は、エージェントを強制起動し、仕事モードを自動的に有効にすることもできます。

仕事モードを有効にすると、CylanceGATEWAY はデバイスと組織のネットワークおよびパブリックインターネットとの間で安全な接続を確立し、ネットワークアクティビティを分析し、管理者が管理するネットワークアクセスポリシーを適用します。CylanceGATEWAY エージェントをインストールしアクティブ化する方法のチュートリアルについては、「[CylanceGATEWAY エージェントのインストールとアクティブ化の方法](#)」を参照してください。

管理者がセーフモードを有効にするようにエージェントを設定している場合は、[CylanceGATEWAY エージェントでのセーフモードのアクティブ化](#) を参照してください。

作業を始める前に：

- CylanceGATEWAY エージェントをインストールします。エージェントをダウンロードするには、[BlackBerry Web サイト](#)に移動し、[CylanceGATEWAY をダウンロード] セクションまで下にスクロールします。
- ディレクトリまたは BlackBerry Online Account 資格情報を使用してエージェントをアクティブ化します。エージェントのアクティブ化の詳細については、管理者から受信した CylanceGATEWAY アクティベーションメールを参照してください。macOS デバイスでプロンプトが表示された場合は必ず、[Gateway によるネットワークコンテンツのフィルタリングを許可する] を選択するようにしてください。



1. コンピューターで、CylanceGATEWAY エージェントを開きます。

2. 次のタスクのいずれかを実行します。

- 仕事モードを有効化：[仕事モードを有効化] をクリックします。
- 管理者が、ログイン時のエージェント起動と仕事モードの自動有効化の両方を強制している場合、アクションは必要ありません。

接続が確立されると、[仕事モードが有効です] ステータスが表示されます。

終了したら：

- 疑わしいネットワークアクティビティに関する警告を表示するには、 をクリックします。[警告] 画面から警告通知を消去してミュートすることもできます。
- 管理者がエージェントに割り当てたポリシーを表示するには、 をクリックします。
- [CylanceGATEWAY エージェントの設定](#)を行うことができます。

## CylanceGATEWAY エージェントの設定

ユーザーは CylanceGATEWAY エージェントの設定を構成できます。デバイスの OS によっては、設定名が異なる場合があります。

設定	説明
非アクティブ化	CylanceGATEWAY エージェントを非アクティブにするには、このボタンをクリックします。エージェントが非アクティブになると、CylanceGATEWAY からポリシーの更新を受信できなくなります。
問題を報告	このボタンをクリックすると、問題レポートとエージェントログファイルが BlackBerry に送信されます。
TCPを使用	組織のファイアウォールで UDP 接続が許可されていない場合、このオプションを選択して CylanceGATEWAY への接続に TCP を使用します。
サインインしたら CylanceGATEWAY を起動します	CylanceGATEWAY または Windows デバイスにログインするたびに macOS エージェントを起動するには、このオプションを選択します。 管理者が [サインインしたら CylanceGATEWAY を起動] ポリシーを適用している場合は、このポリシーがエージェント設定より優先されますが、手動でエージェントを停止することもできます。
仕事モードを自動的に有効化	CylanceGATEWAY エージェントが起動するたびに仕事モードを有効にするには、このオプションを選択します。 管理者が、エージェントの起動後に [仕事モードを自動的に有効化] するポリシーを適用している場合は、このポリシーがエージェント設定より優先されますが、仕事モードを手動で有効または無効にすることもできます。

重要：CylanceGATEWAY または Windows デバイスにサインインするたびに、macOS エージェントの起動と仕事モードの自動有効化の両方を行うようにする場合は、[サインインしたら **CylanceGATEWAY** を起動] と [仕事モードを自動的に有効化] の両方を選択する必要があります。

管理者が [サインインしたら CylanceGATEWAY を起動] と [仕事モードを自動的に有効化] の両方にポリシーを適用している場合は、このポリシーがエージェント設定よりも優先されますが、エージェントの起動後や停止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。

## CylanceGATEWAY エージェントでのセーフモードのアクティブ化

管理者が CylanceGATEWAY を設定していて、macOS または Windows デバイスでセーフモードを使用するように CylanceGATEWAY エージェントを設定している場合、エージェントは、仕事モードトンネルを使用しないネットワークトラフィックに対してセーフモード保護を自動的に有効にします。管理対象外の macOS デバイスを使用している場合は、セーフモードを使用する前に、CylanceGATEWAY システム拡張機能を許可するように求めるプロンプトが一度表示されます。セーフモードは、設定すると無効にできなくなります。エージェントを手動で停止しようとする、エージェントは自動的にデバイスのバックグラウンドで起動されます。

作業を始める前に：

- CylanceGATEWAY エージェントをインストールします。エージェントをダウンロードするには、[BlackBerry Web サイト](#)に移動し、[CylanceGATEWAY をダウンロード] セクションまで下にスクロールします。

- ディレクトリまたは BlackBerry Online Account 資格情報を使用してエージェントをアクティブ化します。エージェントのアクティブ化の詳細については、管理者から受信した CylanceGATEWAY アクティベーションメールを参照してください。macOS デバイスでプロンプトが表示された場合は必ず、[Gateway によるネットワークコンテンツのフィルタリングを許可する] を選択するようにしてください。




1. macOS または Windows デバイスで、CylanceGATEWAY エージェントを開きます。
2. 管理対象外の macOS デバイスを使用していて、CylanceGATEWAY のシステム拡張機能を許可するように求めるプロンプトが表示された場合。次の操作を実行します。

メモ： macOS デバイスでシステム拡張機能を許可しなかった場合、CylanceGATEWAY エージェントには [仕事モードが無効 - セーフモード非アクティブ] と表示されます。

- a. [セーフモードのアクティブ化] プロンプトで、[セキュリティ環境設定を開く] をクリックします。
- b. [セキュリティとプライバシー] をクリックします。
- c. [ロックをクリックして変更] をクリックします。
- d. [システム環境設定] ダイアログボックスで、デバイスの管理者パスワードを入力します。[ロック解除] をクリックします。

接続が確立されると、[仕事モードが無効 - セーフモードアクティブ] ステータスが表示されます。仕事モードを有効にすると、ステータスに [仕事モードが有効 - セーフモード非アクティブ] と表示されます。

終了したら：

- 接続が確立されない場合は、 をクリックして、エラーに関する詳細情報を表示します。
- 疑わしいネットワークアクティビティに関する警告を表示するには、 をクリックします。[警告] 画面から警告通知を消去してミュートすることもできます。
- 管理者がエージェントに割り当てたポリシーを表示するには、 をクリックします。
- [CylanceGATEWAY エージェントの設定](#)を行うことができます。

# 商標などに関する情報

©2024 BlackBerry Limited. BLACKBERRY、BBM、BES、EMBLEM Design、ATHOC、CYLANCE、SECUSMART などの商標（ただし、これらに限定されるとは限らない）は BlackBerry Limited、その子会社および関連会社の商標または登録商標であり、ライセンスに基づいて使用され、当該の商標に対する独占権は明確に留保されています。その他すべての商標は各社の所有物です。

該当する特許は、次の場所で確認できます：[www.blackberry.com/patents](http://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 テクノロジー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があります。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警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> でご確認ください。

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