Cylance Endpoint Security

CylancePROTECT Desktop 3.x のアップグレードガイド

Contents

CylancePROTECT Desktop 3.x にアップグレードする利点

CylancePROTECT Desktop バージョン 3.x では、製品の大幅な進歩が図られており、組織のデータとデバイスのセキュリティを維持するために、新機能と使いやすさの強化を実現しています。

CylancePROTECT Desktop 3.x にアップグレードすると、次の機能にアクセスできます。

Windows

機能	説明
OS の互換性	Windows 3.x エージェントは Windows 11 のサポートを追加します。 詳細については、『CylancePROTECT Desktop』の「互換性マトリックス」を参照してください。
エージェントの機能強化	• Windows 3.1 エージェントは、Microsoft の Antimalware Protected Process Light（AM-PPL）テクノロジを使用して信頼できるサービスとして実行され、エージェントのセキュリティプロセスを悪意のあるアクションから保護します。たとえば、エージェントが終了しないように保護することができます。この機能を使用するには、エンドポイントで Windows 10 1709 以降、または Windows Server 2019 以降を実行している必要があります。 • Windows 3.2 エージェントは、エンドポイント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を、管理コンソールにレポートします。この機能を使用すると、管理者は、エンドポイント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、それに応じて対処していくことができます。管理者は、テナントに登録されたエンドポイントを対象として、インストール済みのアプリケーションをすべて表示したり、各エンドポイントのインストール済みアプリケーションのリストを表示したりできます。この機能は、デバイスポリシー（エージェント設定）から有効にできます。

機能	説明
メモリ保護の機能強化	• 違反タイプに新しい機能が追加され、より多くのイベントが生成されるようになりました。 • デバイスポリシーのメモリ保護設定では、「APC 経由のインジェクション」違反タイプが使用可能になっています。このオプションを使用すると、CylancePROTECT Desktop は、非同期プロシージャコール（APC）を使用して、任意のコードをターゲットプロセスに注入するプロセスを検出できます。詳細については、KB 92422 を参照してください。 • デバイスポリシーのメモリ保護設定では、［子プロセスでのメモリアクセス権限の変更］違反タイプが使用可能になっています。このオプションを選択すると、違反しているプロセスが子プロセスを作成し、その子プロセスのメモリアクセス権限を変更したことを、CylancePROTECT Desktop で検出できるようになります。 • メモリ保護制御の使いやすさが改善されました。 • Windows デバイスの LSASS 読み取り違反の検出機能が強化されました。 • メモリ保護の除外のサイズ制限が 64KB から 2MB に増加し、除外対象をさらに追加できるようになりました。 • サードパーティアプリケーション DLL の除外がサポートされて、サードパーティアプリを CylancePROTECT Desktop とともに実行できるようになりました。たとえば、CylancePROTECT に加えてサードパーティのセキュリティ製品を実行している場合は、CylancePROTECT がその製品に関する特定の違反を無視するように、適切な .dll ファイルの除外を追加できます。この機能には、エージェント 3.1.1001 以降が必要です。詳細については、「メモリ保護デバイスポリシーの［DLL 除外として扱う］設定」を参照してください。 • 違反レポートの精度の向上と、不要なアラートの減少に役立つように、［悪意のあるペイロード］違反タイプのメモリ保護センサが改善されました。この機能には、エージェント 3.1.1001 以降が必要です。
保護の機能強化	• 管理者は、Windows 3.1 エージェントで、デバイスポリシー（保護設定）からバックグラウンド脅威検出スキャンを実行するためにカスタムの間隔を設定できます。スキャン間隔は 1〜90 日の範囲で設定できます。デフォルトのスキャン間隔は 10 日です。スキャンの頻度を増やすと、デバイスのパフォーマンスに影響を与える可能性があることに注意してください。 • Windows 3.2 エージェントは、管理者が管理コンソールからオンデマンドでバックグラウンド脅威検出スキャンを開始する機能をサポートしています。このコマンドは、個々のデバイスについて［デバイスの詳細］画面から送信するか、複数のデバイスについて［デバイス］画面から一度に送信することができます。 • 各デバイスの最後のスキャンの日付が、管理コンソールに記録されます。

機能	説明
スクリプト制御の機能強化	• CylancePROTECT Desktop でアラートを発するか、Python（2.7、3.0〜3.8）スクリプトおよび .NET DLR スクリプト（IronPython など）をブロックするかを選択できます。さらに、これらのスクリプトタイプでは、スクリプト制御をオフにできます。 • スクリプト制御イベントの原因となった埋め込み VB スクリプトは、エージェントバージョン 2.1.1580 でブロックされました。埋め込み VB スクリプト制御違反の検出は、エージェント 3.0.1000 以降で無効になっています。 • Windows 3.1 エージェントは、Microsoft のマルウェア対策スキャンインターフェイス（AMSI）と連携して動作するため、潜在的に危険な XLM マクロが実行されると、脅威情報が管理コンソールに報告され、エージェントはスクリプト制御イベントのデバイスポリシールールに従ってインターフェイスに応答します。たとえば、エージェントは、応答メッセージで、マクロの実行を許可するかブロックするかを質問してきます。この機能を有効にするには、デバイスポリシーの［スクリプト制御］ > ［XLM マクロ］の順にクリックして設定します。デバイスは、Windows 10 を実行している必要があります。Excel ［ファイル］ **>** ［トラストセンター］ **>** ［**Excel** トラストセンター］ **>** ［マクロ設定］の順にクリックして、メニューの VBA マクロを無効にしてください。 • 潜在的に悪意のあるスクリプトが実行されたとき、Windows エージェントが親およびインタープリタープロセスを Cylance に報告します。管理者は、スクリプトの親プロセスまたはインタープリタープロセスの除外を追加して、デバイス上でスクリプトを実行できるようにすることができます。この機能には、エージェントバージョン 3.1.1001 が必要です。 • Windows 3.2 エージェントは、スクリプトスコアリングを使用する、機能強化されたスクリプト制御をサポートしています。危険または異常の脅威スコアが付いたスクリプトの実行をインテリジェントにブロックし、管理コンソールにアラートを通知することができます。管理者は、CylancePROTECT で危険または異常と見なされたスクリプトをブロックするように、デバイスポリシーのスクリプト制御設定を構成できます。 • Windows 3.2 エージェントは PowerShell コンソールスクリプトのアラートモードをサポートしているため、検出されたイベントは管理コンソールにレポートされますが、実行は許可されます。管理者は、PowerShell コンソールのドロップダウンメニューを使用して、デバイスポリシーの［スクリプト制御］タブから設定を制御できます。

機能	説明
マクロ検出の機能強化	• Windows エージェントバージョン 2.1.158x 以降を実行しているデバイスのデバイスポリシーでは、Windows デバイスのマクロ検出機能は、［スクリプト制限］タブから［メモリアクション］タブ（［エクスプロイテーション］ > ［危険な VBA マクロ］）に移動されました。2.1.1578 以前のスクリプト制御オプションでは、アラートおよびブロックアクションがサポートされています。新しいメモリ保護オプションでは、無視、アラート、ブロック、および終了アクションがサポートされています。 • デバイスポリシーのメモリ保護設定で、危険な VBA マクロ違反タイプの除外を追加できるようになりました。 • 危険な VBA マクロ違反の原因となるファイルが管理コンソールに表示されるため、違反しているドキュメントを特定し、除外リストに追加する必要があるかどうかを判断できます。
デバイス制御の機能強化	次の USB デバイスタイプに対して、読み取り専用アクセスを許可できるようになりました。 • 静止画 • USB CD/DVD RW • USB ドライブ • VMware USB パススルー • Windows ポータブルデバイス
グローバルセーフリストの機能強化	SHA256 ハッシュをスクリプトのグローバルセーフリストに追加すると、そのハッシュの関連ブロックイベントは管理コンソールに表示されなくなります。
変更のログ記録	重要なログエントリが、デバッグログレベルから情報ログレベルに移動されました。

Linux

機能	説明
OS の互換性	Linux 3.2.x エージェントは、次の Linux ディストリビューションのサポートを追加します。 • Amazon Linux 2023 • Amazon Linux 2、カーネル 5.10 Linux 3.1.x エージェントは、次の Linux ディストリビューションのサポートを追加します。 • Red Hat Enterprise Linux 9 および 9.1 • Oracle 9 および 9.1 • Oracle UEK 9 および 9.1 • Oracle 8.7 • Oracle UEK 8.7 • SUSE Linux Enterprise Server（SLES）15 SP4 • Ubuntu 22.04 LTS Linux 3.0.x エージェントは、次の Linux ディストリビューションのサポートを追加します。 • Red Hat Enterprise Linux /CentOS 8.4 • Red Hat Enterprise Linux 8.5 • Oracle 8.4 • SUSE（SLES）12 SP5 • SUSE（SLES）15 SP2 および SP3 詳細については、CylancePROTECT Desktop の互換性マトリックスを参照してください。サポートされている Linux カーネルおよびドライバの全リストを表示するには、サポートされている Linux カーネルスプレッドシートをダウンロードしてください。
バックグラウンド脅威検出オンデマンドスキャン	管理者が管理コンソールからオンデマンドでバックグラウンド脅威検出スキャンを開始できるようになりました。このコマンドは、個々のデバイスについて［デバイスの詳細］画面から送信するか、複数のデバイスについて［デバイス］画面から一度に送信することができます。 この機能には、CylancePROTECT Desktop エージェントバージョン 3.2 が必要です。 各デバイスの最後のスキャンの日付が、管理コンソールに記録されます。
バックグラウンド脅威検出スキャンのカスタムの間隔	• 管理者は、デバイスポリシーからバックグラウンド脅威検出スキャンを実行するためにカスタムの間隔を設定できます。スキャン間隔は 1〜90 日の範囲で設定できます。デフォルトのスキャン間隔は 10 日です。 • この機能には、CylancePROTECT Desktop エージェントバージョン 3.1 が必要です。 • 各デバイスの最後のスキャンの日付が、管理コンソールに記録されます。

機能	説明
Linux ドライバを自動更新	• Linux デバイスの CylancePROTECT Desktop エージェント 3.1.1000 は、更新されたカーネルがシステム上で検出されたときに、サポートされている最新のエージェントドライバへの更新を要求できるようになりました。たとえば、Linux カーネルが更新され、現在インストールされているエージェントドライバがそれをサポートしていない場合、互換性のあるドライバがリリースされたらすぐにエージェントがドライバを自動的に更新できるようになりました。 • この機能には、CylancePROTECT Desktop エージェントバージョン 3.1.1000 およびエージェントドライババージョン 3.1.1000 以降が必要です。 • この機能を有効にするには、管理コンソールの［設定］>［更新］メニューから、ゾーンベースの更新ルールの［Linux ドライバを自動更新］オプションを選択します。
メモリ保護の機能強化	• 違反タイプに新しい機能が追加され、より多くのイベントが生成されるようになりました。 • メモリ保護制御の使いやすさが改善されました。 • メモリ保護の除外のサイズ制限が 64KB から 2MB に増加し、除外対象をさらに追加できるようになりました。

macOS

機能	説明
OS の互換性	• CylancePROTECT Desktop 3.2.x エージェントは macOS 14（Sonoma）のサポートを追加します。 • CylancePROTECT Desktop 3.1.x エージェントは macOS 13（Ventura）のサポートを追加します。 • CylancePROTECT Desktop 3.0.x エージェントは macOS 12（Monterey）のサポートを追加します。
USB デバイス制御	macOS 3.3 の CylancePROTECT Desktop エージェントは USB デバイス制御機能をサポートしており、管理者は USB 大容量ストレージデバイスへのアクセスを許可するかブロックするかを制御できます。管理者は、USB 光学ドライブまたは USB ストレージドライブ（ハードドライブやフラッシュドライブなど）に分類されるストレージデバイスのデバイスポリシーから macOS デバイスのデバイス制御をオンにできます。
バックグラウンド脅威検出オンデマンドスキャン	管理者が管理コンソールからオンデマンドでバックグラウンド脅威検出スキャンを開始できるようになりました。このコマンドは、個々のデバイスについて［デバイスの詳細］画面から送信するか、複数のデバイスについて［デバイス］画面から一度に送信することができます。この機能には、CylancePROTECT Desktop エージェントバージョン 3.2 が必要です。 各デバイスの最後のスキャンの日付が、管理コンソールに記録されます。

機能	説明
バックグラウンド脅威検出スキャンのカスタムの間隔	• 管理者は、デバイスポリシーからバックグラウンド脅威検出スキャンを実行するためにカスタムの間隔を設定できます。スキャン間隔は 1〜90 日の範囲で設定できます。デフォルトのスキャン間隔は 10 日です。 • 各デバイスの最後のスキャンの日付が、管理コンソールに記録されます。
メモリ保護の機能強化	• 違反タイプに新しい機能が追加され、より多くのイベントが生成されるようになりました。 • メモリ保護制御の使いやすさが改善されました。 • メモリ保護の除外のサイズ制限が 64KB から 2MB に増加し、除外対象をさらに追加できるようになりました。

最新の 3.x エージェントの追加機能の詳細、および修正された問題の包括的なリストについては、『Cylance Endpoint Security Release Notes（Cylance Endpoint Security リリースノート）』を参照してください。

CylancePROTECT Desktop の将来バージョンで、これらの拡張機能と改善のメリットを享受できるように、BlackBerry は、2.x.158x 以前のエージェントが搭載されたすべてのデバイスで、最新バージョンのエージェント 3.x にアップグレードすることを強くお勧めします。このガイドは、アップグレードを成功させるための考慮事項と追加の手順について説明します。

CylancePROTECT Desktop 3.x へのアップグレード

このセクションでは、CylancePROTECT Desktop バージョン 3.x へのアップグレードを成功させるための手順とベストプラクティスについて説明します。

手順	アクション
1	テスト環境の準備に関するガイダンスを確認します。
2	エージェントのアップグレードパスを確認して、従うべきパスを判断します。
3	メモリ保護の設定とテスト。
4	マクロ検出の設定とテスト（Windows のみ）。
5	必要に応じて、スクリプト制御マクロの除外を新しいメモリ保護設定に移行します。
6	テスト環境でテストと検証を完了した後で、アップグレードと更新されたデバイスポリシーを実稼働環境に適用します。

テスト環境の準備

- BlackBerry では、アップグレードを実稼働環境に展開する前に、専用のテストゾーンで CylancePROTECT Desktop for Windows 3.x へのアップグレードをテストすることをお勧めします。ゾーンの詳細については、Cylance Endpoint Security セットアップガイドで「ゾーンのセットアップ」に関するコンテンツを参照してください。
- テストデバイスは、実稼働環境を正確に表しているアプリと設定を使用してセットアップします。
- テストゾーンとデバイスで使用する専用のデバイスポリシーを作成します。新しいデバイスポリシーを作成するか、既存のポリシーをコピーして変更できます。
- 管理コンソールでゾーンベースの更新ルールを設定して、3.x アップグレードを、テストに使用する専用ゾーンおよびデバイスに制限します。手順については、Cylance Endpoint Security セットアップガイドで「CylancePROTECT Desktop および CylanceOPTICS エージェントの更新の管理」に関するコンテンツを参照してください。
- BlackBerry では、KB 66596 からサポート収集ツールをダウンロードすることをお勧めします。BlackBerry サポートに問い合わせを行うと、サポートがこのツールを実行して追加データを収集するように求める場合があります。
- エージェントのアップグレードパスを確認して、従うべきパスを判断します。
- このガイドの設定およびテストアクティビティを完了し、テストゾーンでアップグレードを検証した後で、エージェントアップグレードと更新されたデバイスポリシーを実稼働環境に適用できます。

CylancePROTECT Desktop 3.x エージェントのアップグレードパス

次のアップグレードパスがテストされ、正式にサポートされています。

Windows エージェントバージョン **3.x** へのアップグレードパス

現在のエージェントバージョン	アップグレードパス
2.0.154x	→ 2.1.157x → 3.2.1000
2.1.156x	→ 2.1.157x → 3.2.1000
2.1.157x	→ 3.2.1000
2.1.158x	→ 3.2.1000
3.0	→ 3.2.1000
3.1	→ 3.2.1000

Linux エージェントバージョン **3.x** へのアップグレードパス

現在のエージェントバージョン	アップグレードパス
2.1.157x 以前	→ 2.1.158x → 2.1.159x → 3.2.1000
2.1.158x	→ 2.1.159x → 3.2.1000
2.1.159x	→ 3.2.1000
3.0	→ 3.2.1000
3.1	→ 3.2.1000

macOS エージェントバージョン **3.x** へのアップグレードパス

現在のエージェントバージョン	アップグレードパス
2.1.156x	→ 2.1.158x → 3.3.1000
2.1.158x	→ 3.3.1000
2.1.159x	→ 3.3.1000

現在のエージェントバージョン	アップグレードパス
3.0	→ 3.3.1000
3.1	→ 3.3.1000
3.2	→ 3.3.1000

メモリ保護の設定とテスト

CylancePROTECT Desktop 3.x では、さまざまなメモリ保護機能が強化され、デバイス上のアプリケーションとプロセスのアクティビティが可視化されます。アプリケーションは、正当な目的のために処理を実行していても、状況によっては、その実行に悪意があると見なされる場合もあります。BlackBerry は、CylancePROTECT Desktop 3.x エージェントを実稼働環境に導入する前に、次の手順とベストプラクティスに従って適切にチューニングすることをお勧めします。メモリ保護違反タイプの詳細については、Cylance Endpoint Security セットアップガイドで「メモリ保護」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、［ポリシー］ > ［デバイスポリシー］をクリックします。
2. テストデバイスのデバイスポリシーをクリックします。
3. ［メモリアクション］タブで［メモリ保護］チェックボックスをオンにします。
4. ［違反タイプ］テーブルで［エクスプロイテーション］、［プロセスの注入］、および［昇格］の順に展開します。［**Agent** バージョン **2.1.1580** 以降で使用できます］および［**CylancePROTECT 3.0** 以降で使用できます］にリストされているすべての違反タイプについて、［アラート］アクションを選択します。
5. デバイスポリシーを保存します。
6. テストデバイスで CylancePROTECT Desktop 3.x を実行し、アラートを確認して、環境内でこれらの脆弱性が発生するリスクを判断します。これらのアラートのいずれかが低リスクであり、ビジネスに影響を与える場合は、対象となるメモリ保護の除外を追加できます。手順とガイダンスについては、「メモリ保護」を参照してください。

   CylancePROTECT Desktop 3.x をインストールまたはアップグレードした後、各テストデバイスを再起動することをお勧めします。

終了したら： アラートを確認し、必要な除外を追加したら、デバイスポリシーの違反タイプアクションを必要に応じて変更できます（たとえば、ブロックまたは終了）。

マクロ検出の設定とテスト（Windows のみ）

デバイスポリシーには、Windows デバイス上で潜在的に危険なマクロを検出し、応答するためのオプションが 2 つあります。［スクリプト制御］タブの［マクロ］オプションは、Windows エージェント 2.1.1578 以前に適用されます。［メモリアクション］タブの新しい［エクスプロイテーション］ > ［危険な VBA マクロ］オプションは、Windows エージェント 2.1.1580 以降に適用されます。エージェント 3.x へのアップグレードをテストする場合は、マクロの検出と対応方法に関して現在の設定を確認し、新オプションの［危険な VBA マクロ］を適宜設定する必要があります。

1. 管理コンソールのメニューバーで、［ポリシー］ > ［デバイスポリシー］をクリックします。
2. 製品デバイスポリシーをクリックします。

3. ［スクリプト制御］タブで、マクロの現在の設定（［アラート］または［ブロック］）を確認し、メモに書き留めます。
4. ［ポリシー］ > ［デバイスポリシー］で、テストデバイスのデバイスポリシーをクリックします。
5. ［メモリアクション］タブで［エクスプロイテーション］を展開します。
6. ［危険な **VBA** マクロ］違反タイプの場合は、適切なアクション（［無視］、［アラート］、［ブロック］、または［停止］）を設定します。
7. デバイスポリシーを保存します。
8. 必要に応じて、スクリプト制御マクロの除外を新しいメモリ保護設定に移行します。
9. 組織でよく使用されるマクロが保存されたファイルを使用して、テストデバイスで CylancePROTECT Desktop 3.x を実行します。安全なマクロに関しては、必要に応じてメモリ保護の除外を追加します。手順とガイダンスについては、Cylance Endpoint Security セットアップガイドで「メモリ保護」に関するコンテンツを参照してください。

スクリプト制御マクロの除外を新しいメモリ保護設定に移行（Windows のみ）

デバイスポリシーの［スクリプト制御］タブでマクロ除外を追加してある場合は、これらの除外を CylancePROTECT Desktop for Windows 3.x の新しいメモリ保護設定に移行する必要があります。スクリプト制御の除外を手動で移行するには、デバイスポリシーの［スクリプト制御］タブで追加した除外を記録し、デバイスポリシーの［メモリアクション］タブで同じ除外を追加するだけです。

BlackBerry が提供する PowerShell スクリプトを使用して既存のスクリプト制御の除外を移行する場合は、次の手順を実行します。

メモ：以下の手順は、Cylance コンソールを使用して管理されるテナントに適用されます。マルチテナントコンソールを使用してテナントを管理している場合は、KB 92149 を参照してください。

作業を始める前に：

- PowerShell がコンピュータにインストールされていること、および PowerShell スクリプトが CylancePROTECT Desktop などのセキュリティソフトウェアによってブロックされていないことを確認します。CylancePROTECT Desktop がコンピュータにインストールされている場合は、デバイスに割り当てられているデバイスポリシーで、［スクリプト制御］ > ［**PowerShell** コンソールの使用をブロック］がオフになっていることを確認します。
- Cylance コンソールで、API 権限を次のように指定して統合を追加し、結果のアプリケーション ID とシークレットを記録します。
  - ポリシー：読み取り、変更
  - ユーザー：読み取り
- ［設定］ > ［統合］で、テナント **ID** を記録します。
- スクリプトを実行するときに、Cylance コンソール管理者アカウントのメールアドレスを指定します。使用するアカウントに、管理者ロールが割り当てられていることを確認します。
- 除外をスクリプト制御からメモリ保護に移行するデバイスポリシーで、スクリプト制御が有効になっており、マクロの除外が存在することを確認します。
  - スクリプトでは、スクリプト制御が無効になっているポリシーや、スクリプト制御の除外がないポリシーは無視されます。
  - スクリプトは、マルチバイト文字を含む除外リストを移行しません。これらの除外は手動で追加する必要があります。
- PowerShell スクリプトをダウンロードします。

1. PowerShell コマンドプロンプトを開き、ディレクトリをスクリプトの場所に変更します。

2. 次の表を参照し、適切なパラメーターを使用してスクリプトを実行します。
   - まずスクリプトを -dryRun モードで実行して、変更を行わずに移行をプレビューします。これにより生成される出力ファイルを使用して、問題があれば特定し、修正することができます。
   - テストに使用する予定のデバイスポリシーのスクリプトを実行します。3.x エージェントのテストと検証が完了した後で、スクリプトを使用して移行を実稼働デバイスポリシーに適用できます。

パラメーター	必須またはオプション	説明
`-copySCExclusions`	必須	このコマンドは、スクリプト制御設定から新しいメモリ保護設定へのマクロの除外の移行を実行します。

`-allPolicies`
または
`-policy '<policy_name>'`
	必須	`-allPolicies` は、テナント内のすべてのデバイスポリシーの移行を実行します。
		`-policy '<policy_name>''` は、指定されたデバイスポリシーの移行を実行します。

`-dryRun`	オプション	このコマンドは、変更を加えずにスクリプトの実行をプレビューします。このモードでスクリプトを実行すると、スクリプトが実行されたディレクトリ内に出力ファイルが作成されます。
`-tenantId '<tenant_ID>'`	必須	このコマンドは、Cylance Endpoint Security テナントの ID を指定します。
`-apiKey '<application_ID>'`	必須	このコマンドは、［設定］>［統合］で追加した統合のアプリケーション ID を指定します。
`-apiSecret '<application_secret>`	必須	このコマンドは、［設定］>［統合］で追加した統合のアプリケーションシークレットを指定します。
`-userEmail '<admin_email>'`	必須	このコマンドは、移行の実行に使用する Cylance コンソール管理者アカウントのメールアドレスを指定します。アカウントには管理者ロールが必要です。

パラメーター	必須またはオプション	説明
`-region '<region_code>'`	必須	このコマンドは、Cylance Endpoint Security テナントの地域を指定します。次のいずれかの値を使用します。 • 北米：na（指定されていない場合のデフォルト値） • 日本： `apne1` • オーストラリア： `au` • ヨーロッパ： `euc1` • 南米： `sae1` • GovCloud： `us`
`-Ignore158xWarning`	オプション	このコマンドは、メモリ保護の除外のサイズ制限に関連するエラーを移行プロセスに無視させます。サイズ制限は、以前のバージョンの CylancePROTECT Desktop では 64KB でしたが、バージョン 3.x では 2MB に引き上げられています。 メモ：このパラメーターは、ターゲットデバイスポリシーに関連付けられているすべてのデバイスがエージェント 3.x 以降を使用している場合にのみ使用してください。
`-ignore158xCompatibility`	オプション	このコマンドは、CylancePROTECT Desktop for Windows 2.1.1580 および 1584 固有の不具合に関連しています（KB 88218 を参照してください）。不具合の修正（除外パスのワイルドカード値にアスタリスク（*）を追加してワイルドカードが**になるようにする）は、デフォルトでスクリプトに組み込まれています。このパラメーターを使用すると、スクリプトに組み込まれている修正が無効になります。 メモ：ターゲットデバイスポリシーがエージェント 1578 以前のデバイスとエージェント 3.x 以降のデバイスに関連付けられている場合は、このパラメーターを使用します。ポリシーがエージェント 158x のデバイスに関連付けられている場合は、このパラメーターを使用しないでください。
`-includeExtensions <extensions>`	オプション	このコマンドは、メモリ保護設定に移行する拡張子を指定します（例：`includeExtensions ps1, ja, xlxs`）。 このパラメーターを使用しない場合、すべての拡張子が移行されます。

メモ：スクリプトを -dryRun モードで実行すると、出力ファイルに「Modify '<*policy_name*>' Policy を開始... ログエラー：要求されたポリシーは MemoryProtection v2 に変換されていません」というエラーが表示されることがあります。これは、デバイスポリシーがしばらく編集されていない場合に発生します。この問題を解決するには、管理コンソールでポリシーを開いて保存します。

移行できなかったスクリプト制御の除外があった場合は、PowerShell の出力に示されます。これらの除外は、メモリ保護設定に手動で追加する必要があります。

例：スクリプトを **-dryRun** モードで実行します

```
.\sc2memdef_copy.ps1 -copySCExclusions -allPolicies -
dryRun -tenantId '00000000-0000-0000-0000-000000000000' -
apiKey '00000000-0000-0000-0000-000000000000' -apiSecret
 '00000000-0000-0000-0000-000000000000' -userEmail 'user@blackberry.com' -region
 'na'
```

例：特定のデバイスポリシーのスクリプトを実行します

```
.\sc2memdef_copy.ps1 -copySCExclusions -policy 'userPolicy'
 -tenantId '00000000-0000-0000-0000-000000000000' -
apiKey '00000000-0000-0000-0000-000000000000' -apiSecret
 '00000000-0000-0000-0000-000000000000' -userEmail 'user@blackberry.com' -region
 'na'
```

例：すべてのデバイスポリシーのスクリプトを実行します

```
.\sc2memdef_copy.ps1 -copySCExclusions -allPolicies -
tenantId '00000000-0000-0000-0000-000000000000' -apiKey
 '00000000-0000-0000-0000-000000000000' -apiSecret
 '00000000-0000-0000-0000-000000000000' -userEmail 'user@blackberry.com' -region
 'na'
```

終了したら：

- ターゲットデバイスポリシーの［メモリアクション］タブで、移行された除外を確認し、新しい危険な VBA マクロ違反タイプに適用されないものをすべて削除します。
- 管理コンソールに追加した PowerShell 統合を削除します。

CylancePROTECT Desktop 3.x のトラブルシューティング

Windows

問題	解決策
メモリ保護の除外を追加した後にデバイスポリシーを保存しようとすると、次のエラーが表示される：「ポリシーを保存できませんでした。もう一度お試しください。」	除外パスにワイルドカード値として単一のアスタリスク（*）が含まれている場合は、ワイルドカードにもう 1 つアスタリスクを追加してから（**）、ポリシーを保存し直します。 詳細については、KB 94518 を参照してください。
CylancePROTECT Desktop 3.0.1000 エージェントが、Windows の一時ファイルディレクトリに多数の一時ファイルを作成する。	エージェント 3.0.1005 以降にアップグレードします。 詳細については、KB 94849 を参照してください。
CylancePROTECT Desktop 3.x にアップグレードした後、予期しない数のプロセスがブロックされる。	ガイダンスとベストプラクティスについては、KB 85991 を参照してください。

Linux

問題	解決策

CylancePROTECT ドライバをインストールしようとすると、「許可されていない操作です」というエラーが表示される	CylancePROTECT ドライバをインストールすると、Linux 端末に、次のいずれかのエラー（または同様のエラー）が表示されます。
	`modprobe: ERROR: could not insert 'CyProtectDrvOpen': Operation not permitted`
	`modprobe: ERROR: could not insert 'CyProtectDrv': Operation not permitted`
	`Key was rejected by service`
	このエラーは通常、セキュアブートが有効になっているデバイスに Linux ドライバをインストールしようとしたときに発生します。詳細については、KB 73487 を参照してください。

問題	解決策
仮想化の問題	Linux 向けの CylancePROTECT Desktop エージェントは、BIOS シリアル番号と、dbus によって生成された一意の ID（マシン ID）を使用して、デバイスフィンガープリントを生成します。ゴールドイメージを使用している一部の VM 環境では、問題が発生する場合があります。ゴールドイメージから生成された Linux マシンは、同一の BIOS シリアル番号と、dbus によって生成された ID を保持している場合があります。これにより、VM は、一意のデバイスとして登録されるのではなく、コンソール上の同じデバイスにチェックインされる可能性があります。 この問題が発生した場合は、クローン化されたマシンの BIOS シリアル番号とマシン ID をチェックし、これらの値がマシンごとに一意であることを確認することをお勧めします。詳細については、KB 66123 を参照してください。

macOS

問題	解決策

CylancePROTECT Desktop エージェントの実行時にシステム拡張機能がブロックされる	macOS 11.15.0 の CylancePROTECT Desktop デバイスを最新バージョンの macOS にアップグレードすると、次のエラーが発生します：「システム拡張機能がブロックされました。プログラムで、Cylance, Inc. によって署名された新しいシステムをロードしようとしました。これは、開発者が更新する必要があります。」
	
	この問題は、CylancePROTECT Desktop エージェントのシステム拡張機能を有効にする必要がある場合に発生します。ユーザーは、［システム環境設定］>［セキュリティとプライバシー］に移動し、Cylance 拡張機能に対して［許可］をクリックする必要があります。
	
	JAMF を使用して CylancePROTECT Desktop を展開する組織は、次の設定を使用して、JAMF 設定内からシステム拡張機能を承認できるようにする必要があります。
	
	• ［ユーザーがシステム拡張機能を承認できるようにする］を有効にします。
	• ［許可されたチーム ID とシステム拡張機能］で、以下を指定します。
	  • 表示名：Cylance Protect
	  • システム拡張機能のタイプ：使用可能なシステム拡張機能
	  • チーム識別子：6ENJ69K633
	  • 使用可能なシステム拡張機能：com.cylance.CylanceEndpointSecurity.extension

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。

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