BlackBerry UEM

iOS デバイスの管理

管理

12.12

Contents

iOS デバイスの管理 4
他の Apple デバイスの管理 4

iOS デバイスで制御できるもの 5

iOS デバイスで使用されているライセンス 7

iOS デバイスを管理する手順 8

IT ポリシーによる iOS デバイスの制御 9
iOS のパスワード要件の設定 9

プロファイルによる iOS デバイスの制御 11
プロファイルリファレンス - iOS デバイス 12

iOS デバイスでのアプリの管理 16
MDM 制御 アクティベーションを使用した iOS デバイスでのアプリの動作 16
ユーザーのプライバシー アクティベーションを使用した iOS デバイスでのアプリの動作 20

iOS デバイスのアクティベーション 23
アクティベーションタイプ : iOS デバイス 23
iOS バージョン 12.2 以降のデバイスのアクティベーション（MDM 制御 のアクティベーションタイプ） 25
12.2 よりも前の iOS デバイスのアクティベーション（MDM 制御 のアクティベーションタイプ） 26
Apple ユーザー登録を使用した iOS または iPad OS デバイスのアクティブ化 27

アクティブ化された iOS デバイスの管理と監視 29
iOS デバイスのコマンド 30

商標などに関する情報 34

iOS デバイスの管理

BlackBerry UEM では、iOS デバイスがネットワークに接続する方法、有効にするデバイス機能、利用可能にするアプリを詳細に管理できます。デバイスの所有者が組織かユーザーかにかかわらず、組織の情報にモバイルアクセスを提供しながら、アクセス権を持たないユーザーから保護することができます。

このガイドでは、iOS デバイスの管理オプションについて説明しています。また、利用可能なすべての機能を活用するために必要な詳細情報を確認できます。

他の Apple デバイスの管理

BlackBerry UEM では、macOS および Apple TV デバイスのアクティブ化と管理も可能です。Apple TV は、データを受信して、HDMI ケーブルを介してテレビにデータをストリーミングできるデジタルメディアプレイヤーです。

BlackBerry UEM は、第 2 世代以降の Apple TV バージョンをサポートしています。サポートされている macOS バージョンの詳細については、「互換性一覧表」を参照してください。Apple TV デバイスを管理するには、指示に従って iOS デバイスのプロファイル設定を使用してください。次の BlackBerry UEM 機能が Apple TV でサポートされています。

- BlackBerry UEM Self-Service を使用したデバイスのアクティベーション
- MDM コントロールのアクティベーションタイプ
- Wi-Fi および証明書プロファイル
- アプリロックモードプロファイル
- デバイスのコマンド

ユーザーが Apple TV デバイスをアクティブ化できないようにするには、アクティベーションプロファイル内にデバイスモデルの制限を設定して、Apple TV デバイスが許可されないようにします。macOS および Apple TV デバイスのアクティベーションの詳細については、デバイスアクティベーションの資料を参照してください。

iOS デバイスで制御できるもの

BlackBerry UEM は、iOS デバイスで管理できる機能の制御に必要なツールをすべて備えています。また、デバイスを完全に管理しなくても、デバイスユーザーに作業リソースへの安全なアクセスを提供できる機能も含まれています。

制御レベル	説明
管理されていないデバイスと部分的に管理されているデバイス（BlackBerry UEMでアクティベーションされているが、完全には管理されていないデバイス）	BlackBerry UEM でデバイスをアクティベーションして、デバイスを完全に管理することなく、作業リソースへの安全なアクセスを提供できます。このオプションは、BYOD デバイスによく使用されます。 これらのアクティベーションにより、ユーザーは BlackBerry 2FA を使用して VPN 経由でネットワークにアクセスし、BlackBerry Workspaces を使用してファイルを安全に共有し、BlackBerry Dynamics や BlackBerry Work などの BlackBerry Access アプリをインストールして、仕事用のメールや職場のイントラネットにアクセスできます。
仕事用プロファイルがある部分的管理のデバイス	BlackBerry UEM でデバイスをアクティベーションして、仕事用プロファイル内の作業リソースへの安全なアクセスを提供できます。このオプションは、BYOD デバイスによく使用されます。 このアクティベーションタイプでは、デバイス上に、仕事用アプリとネイティブ Notes、iCloud ドライブ、メール（添付ファイルとメール本文全体）、カレンダー（添付ファイル）、および iCloud Keychain アプリ用の個別の仕事用領域が作成されます。
監視対象デバイス（BlackBerry UEM によって管理されるデバイス）	デバイスをアクティベーションして、BlackBerry UEM で完全に管理できます。このオプションは、企業所有のデバイスによく使用されます。 このオプションでは、コマンドと IT ポリシールールを使用して仕事用のデータを管理できます。BlackBerry Dynamics アプリなどの仕事用アプリをデバイス上で管理できます。 BlackBerry UEM は、監視対象の iOS デバイスの管理をサポートします。IT ポリシールールには、監視対象デバイスでのみサポートされるものがあります。

ユーザーのプライバシー アクティベーションでは、デバイス管理機能を制限できるので、ユーザーは BlackBerry Work や BlackBerry Access などの BlackBerry Dynamics アプリを使用して仕事用データにアクセスできるようになります。次のデバイス管理機能の一部を許可するように選択できます。

- SIM カードとデバイスのハードウェア情報へのアクセス：SIM カードとデバイスのハードウェア情報への BlackBerry UEM アクセスを許可し、SIM ベースのライセンスを有効にします。
- アプリ管理：管理者は仕事用アプリをインストールまたは削除できます。また、インストールされている仕事用アプリのリストを［ユーザーの詳細］画面で表示できます。
- IT ポリシー管理：IT ポリシーの限定されたセットをデバイスに適用するかどうかを指定します（パスワードポリシー、スクリーンショットの許可、管理されている送信元から管理されていない送信先にドキュメントを送信する許可、管理されていない送信元から管理されている送信先にドキュメントを送信する許可）。
- メールプロファイル管理：デバイスにメールプロファイルを適用できるようにします。
- Wi-Fi プロファイル管理：Wi-Fi プロファイルをデバイスに適用できるようにします。

- VPN プロファイル管理：VPN プロファイルをデバイスに適用できるようにします。

iOS および iPad OS デバイスに ユーザーのプライバシー - ユーザー登録 アクティベーションタイプを使用して、ユーザーデータがプライベートに保持され、仕事用データから分離されていることを確認できます。このアクティベーションタイプでは、仕事用アプリと一部のネイティブアプリ用に個別の仕事用領域がデバイスにインストールされます。

このアクティベーションタイプでは、アプリ管理、IT ポリシー管理、メールプロファイル、Wi-Fi プロファイル、per-app VPN が有効になります。管理者は、個人データに影響を与えることなく、作業データを管理（たとえば、作業データの消去）ができます。

このアクティベーションタイプは、iOS または iPad OS 13.1 以降を実行する非監視対象デバイスでサポートされています。

MDM 制御 アクティベーションは、次の機能を含む iOS デバイス管理を完全にサポートします。

- パスワード要件を強制する
- IT ポリシーを使用してデバイスの機能を制御する（カメラや Bluetooth を無効にするなど）
- コンプライアンスルールを強制する
- Wi-Fi および VPN 接続プロファイル（プロキシを使用）
- メール、連絡先、カレンダーをデバイスと同期する
- 認証と S/MIME のために CA およびクライアント証明書をデバイスに送信する
- 必須アプリ、許可されたパブリックアプリ、内部アプリ（BlackBerry Dynamics アプリを含む）を管理します。
- Apple DEP および VPP の完全なサポート
- 紛失または盗難にあったデバイスの捜索

iOS デバイスで使用されているライセンス

iOS で BlackBerry UEM デバイスをアクティベーションする場合は、管理者がデバイスを管理でき、ユーザーがデバイス上の仕事用データにアクセスできるように、デバイスを BlackBerry UEM に関連付けます。ほとんどの iOS アクティベーションタイプでは、Silver BlackBerry UEMライセンスまたは BlackBerry Secure UEM & Productivity Suites – Choice ライセンスが最低 1 つ必要ですが、ユーザーに対して有効にする機能によっては、他のライセンスが必要になる場合があります。

機能	最低限必要なライセンス
MDM 制御 または ユーザーのプライバシー のアクティベーション	次のいずれか： • Silver • BlackBerry Secure UEM & Productivity Suites – Choice
BlackBerry Secure Gateway	次のいずれか： • Gold • BlackBerry Secure UEM & Productivity Suites – Choice BlackBerry Secure Gateway の詳細については、「BlackBerry UEM 管理関連の資料」を参照してください。
BlackBerry Secure Connect Plus	次のいずれか： • Gold • BlackBerry Secure UEM & Productivity Suites – Freedom BlackBerry Secure Connect Plus の詳細については、「BlackBerry UEM 管理関連の資料」を参照してください。
BlackBerry Access アプリ	BlackBerry Secure UEM & Productivity Suites – Choice
BlackBerry Work および BlackBerry Tasks アプリ	BlackBerry Secure UEM & Productivity Suites – Choice
その他すべての BlackBerry および ISV BlackBerry Dynamics アプリ	BlackBerry Secure UEM & Productivity Suites – Freedom
BlackBerry 2FA 専用のデバイス登録	次のいずれか： • BlackBerry 2FA • BlackBerry Secure UEM & Productivity Suites – Freedom

利用可能なライセンスの詳細については、ライセンス関連の資料を参照してください。

iOS デバイスを管理する手順

手順	アクション
1	インストール手順に従って、BlackBerry UEMをインストールして設定します。iOSデバイスを管理するには、Apple から APN 証明書を取得する必要があります。
2	組織で Apple Device Enrollment Program を使用している場合は、DEP を使用するように BlackBerry UEMを設定します。
3	有効化する機能に関して、iOS デバイスのアクティベーションに必要なライセンスがあることを確認します。
4	デバイスの IT ポリシーを設定します。IT ポリシーをユーザーグループまたは個々のユーザーに割り当てます。
5	デバイス用プロファイルを設定します。プロファイルをユーザーグループまたは個々のユーザーに割り当てます。
6	組織に Apple VPP アカウントがある場合は、それを BlackBerry UEM に追加します。
7	デバイスがインストールできる、またはインストールする必要があるアプリを指定します。
8	デバイスをアクティベーションします。
9	デバイスを管理および監視します。

IT ポリシーによる iOS デバイスの制御

BlackBerry UEM は IT ポリシーを各デバイスに送信します。デフォルトの IT ポリシーを使用することも、独自の IT ポリシーを作成することもできます。さまざまな状況やユーザーに応じて必要な数だけ IT ポリシーを作成できますが、デバイス上でアクティブになる IT ポリシーは 1 つだけです。

iOS の IT ポリシールールは、デバイスの機能と、Apple で提供されるデバイス設定オプションに基づいています。Apple が新しい機能や設定オプションを備えた OS 更新を新規にリリースすると、次の機会に新しい IT ポリシールールが UEM に追加されます。

検索およびソート可能な IT ポリシールールのスプレッドシートをダウンロードできます。このスプレッドシートには、ルールをサポートする最小限のデバイス OS など、UEM で利用可能なルールがすべて記載されています。

IT ポリシーで制御するデバイスの動作には、次のようなオプションがあります。

- デバイスのパスワード要件
- カメラ、Bluetooth、Touch ID などのデバイス機能を許可する
- App Store と iTunes Store の購入、および購入に許容されるコンテンツ評価を許可する
- Safari、Siri、FaceTime などのシステムアプリを許可する
- iCloud の使用を許可する

IT ポリシーのデバイスへの送信の詳細については、管理関連の資料を参照してください。

iOS のパスワード要件の設定

iOS デバイスでパスワードを必須とするかどうかを選択できます。パスワードを必須にする場合、パスワードの要件を設定できます。

メモ：iOS デバイスおよび一部のデバイスのパスワードルールでは、「パスコード」という用語を使用します。「パスワード」と「パスコード」は両方とも同じ意味です。

ルール	説明
デバイスのパスワードを必須にする	デバイスパスワードを設定する必要があるようにするかどうかを指定します。
単純な値を許可する	パスワードに、DEFG や 3333 などの反復または連続する文字を含めることができるようにするかどうかを指定します。
英数字値を要求する	パスワードに文字と数字の両方を含める必要があるかどうかを指定します。
パスコードの最小文字数	パスワードの最小文字数を指定します。iOS デバイスで要求される最小値より小さい値を入力すると、デバイスの最小値が使用されます。
複雑な文字の最小文字数	パスワードに含める必要がある英数字以外の文字の最小数を指定します。
パスコードの最大期限	パスワードを使用できる最大日数を指定します。

ルール	説明
最大自動ロック時間	自動ロック時間に設定できる最大値を指定します。つまり、ユーザーアクティビティのない状態で、ここに指定された分数が経過した後に、デバイスがロックされます。［なし］に設定すると、デバイスでサポートされるすべての値を使用できます。選択値がデバイスのサポート範囲に含まれていない場合、デバイスでサポートされる最も近い値が使用されます。
パスコードの履歴	最近のパスワードの再利用を防ぐため、デバイスがチェックする以前のパスワード数を指定します。
デバイスロックの最大猶予期間	デバイスロックの猶予期間に設定できる最大値を指定します。デバイスのロック後この時間が経過すると、ロック解除のためのパスワードが要求されます。［なし］に設定すると、デバイスですべての値を使用できます。［即座］に設定すると、デバイスのロック後、即座にパスワードが要求されます。
パスワードの最大失敗試行回数	デバイスが消去される前に、間違ったパスワードを入力できる回数を指定します。
パスワードの変更を許可する（監視下のみ）	ユーザーがパスワードを追加、変更、または削除できるかどうかを指定します。

IT ポリシーのパスワードルールの詳細については、『ポリシーリファレンススプレッドシート』をダウンロードしてください。

プロファイルによる iOS デバイスの制御

BlackBerry UEM には、デバイス機能のさまざまな側面の制御に使用できるプロファイルがいくつか含まれています。最も一般的に使用されるプロファイルは次のとおりです。

プロファイル名	説明	設定
アクティベーション	アクティベーションタイプ、方法、およびユーザーがアクティブ化できるデバイスの数や種類など、ユーザーのデバイスアクティベーション設定を指定します。	アクティベーションプロファイルの作成
Wi-Fi	仕事用 Wi-Fi ネットワークに接続するデバイスの設定を指定します。	Wi-Fi プロファイルの作成
VPN	仕事用 VPN に接続するデバイスの設定を指定します。	VPN プロファイルの作成
プロキシ	デバイスがインターネットまたは仕事用ネットワークで Web サービスにアクセスする際の、プロキシサーバーの使用方法を指定します。	プロキシプロファイルの作成
メール	デバイスを仕事用メールサーバーに接続し、メールやカレンダーエントリ、オーガナイザーデータを同期する方法を指定します。BlackBerry Work をデバイスにインストールして構成する場合は、メールプロファイルをセットアップする必要はありません。	メールプロファイルの作成
BlackBerry Dynamics	デバイスが BlackBerry Work、BlackBerry Access、BlackBerry Connect などの BlackBerry Dynamics アプリにアクセスできるようにします。	BlackBerry Dynamics プロファイルの作成
BlackBerry Dynamics 接続	BlackBerry Dynamics アプリを使用するときにデバイスが接続できるネットワーク接続方法、インターネットドメイン、IP アドレス範囲、およびアプリサーバーを定義します。	BlackBerry Dynamics 接続プロファイルの作成
コンプライアンス	組織で許容できないデバイスの条件を定義し、強制する操作を設定します。	コンプライアンスプロファイルの作成
エンタープライズ接続	デバイスが BlackBerry Secure Connect Plus を使用できるかどうかを指定します。	BlackBerry Secure Connect Plus を有効化する

プロファイル名	説明	設定
CA 証明書	仕事用ネットワークまたはサーバーとの信頼性を確立するためにデバイスが使用できる CA 証明書を指定します。	CA 証明書プロファイルの作成
ユーザー資格情報	デバイスが仕事用ネットワークまたはサーバーとの認証に使用するクライアント証明書の取得方法を指定します。	ユーザー資格情報プロファイルを作成
SCEP	仕事用ネットワークまたはサーバーとの認証に使用されるクライアント証明書を取得するために使用する SCEP サーバーを指定します。	SCEP プロファイルの作成

デバイスへのプロファイル送信の詳細については、管理関連の資料を参照してください。

プロファイルリファレンス - iOS デバイス

次の表に、BlackBerry UEM デバイスでサポートされる iOS のすべてのプロファイルを示します。

プロファイル名	説明	設定
ポリシー		
アクティベーション	アクティベーションタイプやデバイスの数および種類など、ユーザーのデバイスアクティベーション設定を指定します。	アクティベーションプロファイルの作成
BlackBerry Dynamics	デバイスが BlackBerry Work、BlackBerry Access、BlackBerry Connect などの BlackBerry Dynamics アプリにアクセスできるようにします。	BlackBerry Dynamics プロファイルの作成
アプリロックモード	デバイスで実行する単一のアプリを指定します。 監視対象 iOS デバイスのみ。	アプリロックモードプロファイルを作成
エンタープライズ管理エージェント	プッシュ通知を使用できない場合に、デバイスが BlackBerry UEM に接続してアプリと設定の更新の有無を確認するタイミングを指定します。	エンタープライズ管理エージェントプロファイルの作成
コンプライアンス		
コンプライアンス	組織で許容できないデバイスの条件を定義し、強制する操作を設定します。	コンプライアンスプロファイルの作成

プロファイル名	説明	設定
コンプライアンス（BlackBerry Dynamics）	これは、Good Control からオンプレミス BlackBerry UEM にインポートされたコンプライアンス設定を表示する読み取り専用のプロファイルです。	BlackBerry Dynamics コンプライアンスプロファイルの管理
メール、カレンダー、および連絡先		
メール	デバイスを仕事用メールサーバーに接続し、Exchange ActiveSync や IBM Notes Traveler を使ってメールやカレンダーエントリ、オーガナイザーデータを同期する方法を指定します。	メールプロファイルの作成
IMAP/POP3 メール	デバイスの IMAP や POP3 メールサーバーへの接続方法とメールメッセージの同期方法を指定します。	IMAP/POP3 メールプロファイルを作成
ゲートキーピング	自動ゲートキーピングに使用する Microsoft Exchange サーバーを指定します。	ゲートキーピングプロファイルの作成
CalDAV	デバイスがカレンダー情報の同期に使用するサーバー設定を指定します。	CalDAV プロファイルの作成
CardDAV	デバイスが連絡先情報の同期に使用するサーバー設定を指定します。	CardDAV プロファイルの作成
ネットワークと接続		
Wi-Fi	仕事用 Wi-Fi ネットワークへのデバイス接続方法を指定します。	Wi-Fi プロファイルの作成
VPN	仕事用 VPN へのデバイスの接続方法を指定します。	VPN プロファイルの作成
プロキシ	デバイスがインターネットまたは仕事用ネットワークで Web サービスにアクセスする際のプロキシサーバーの使用方法を指定します。	プロキシプロファイルの作成
エンタープライズ接続	エンタープライズ接続を使用して、デバイスが組織のリソースに接続する方法を指定します。iOS デバイスの場合、エンタープライズ接続プロファイルは、デバイスが BlackBerry Secure Connect Plus を使用できるかどうかを指定します。	BlackBerry Secure Connect Plus を有効にする

プロファイル名	説明	設定
BlackBerry Dynamics 接続	BlackBerry Dynamics アプリを使用するときにデバイスが接続できるネットワーク接続、インターネットドメイン、IP アドレス範囲、およびアプリサーバーを定義します。	BlackBerry Dynamics 接続プロファイルの作成
BlackBerry 2FA	ユーザーのツーファクター認証を有効にし、事前認証および自己回復機能の設定を指定します。	BlackBerry 2FA プロファイルの作成
ネットワーク使用	iOS デバイスの仕事用アプリで、モバイルネットワークやデータローミングを使用できるかどうかを制御できます。	ネットワーク使用プロファイルの作成
Web コンテンツフィルター	ユーザーが監視対象の iOS デバイスで表示できる Web サイトを制限します。 監視対象 iOS デバイスのみ。	Web コンテンツフィルタープロファイルの作成
シングルサインオン	ユーザーがユーザー名とパスワードを初めて入力した後に、デバイスがセキュリティ保護されたドメインでの認証を自動的に実行する方法を指定します。	シングルサインオンプロファイルの作成
管理されているドメイン	信頼済みドメイン外でのメール送信についてユーザーに通知し、内部ドメインからダウンロードしたドキュメントを表示できるアプリを制限するように iOS デバイスを設定します。	管理されているドメインプロファイルの作成
AirPrint	プリンターを AirPrint プリンターリストに追加できます。	AirPrint プロファイルの作成
AirPlay	デバイスをユーザーの AirPlay デバイスリストに追加できます。	AirPlay プロファイルの作成
シングルサインオン拡張	iOS （または iPadOS）13 以降を実行しているデバイスがシングルサインオンを使用して認証できるようにします。	シングルサインオン拡張プロファイルの作成
保護		
Microsoft Intune アプリの保護	Microsoft Intune で保護されているアプリを管理できます。	Microsoft Intune アプリ保護プロファイルの作成
位置情報サービス	デバイスの位置を要求し、地図上のおおよその位置を表示することができます。	位置情報サービスプロファイルの作成
サイレント	定義した日数および時間数の間、BlackBerry Work for iOS の通知をブロックできます。	サイレントプロファイルの作成

プロファイル名	説明	設定
カスタム		
デバイス	デバイスに表示する情報を設定できます。	デバイスプロファイルの作成
カスタムペイロード	デバイスのペイロードコードを使用してカスタム設定情報を指定します。	カスタムペイロードプロファイルの作成
アプリごとの通知	システムアプリと、BlackBerry UEM を使用して管理するアプリの通知設定を指定できます。 監視対象 iOS デバイスのみ。	アプリごとの通知プロファイルの作成
証明書		
CA 証明書	仕事用ネットワークまたはサーバーとの信頼性を確立するためにデバイスが使用できる CA 証明書を指定します。	CA 証明書プロファイルの作成
共有証明書	仕事用ネットワークまたはサーバーでユーザーを認証するためにデバイスが使用できるクライアント証明書を指定します。	共有の証明書プロファイルの作成
ユーザー資格情報	仕事用ネットワークまたはサーバーとの認証に使用されるクライアント証明書を取得するために使用する CA 接続を指定します。	ユーザー資格情報プロファイルを作成
SCEP	仕事用ネットワークまたはサーバーとの認証に使用されるクライアント証明書を取得するために使用する SCEP サーバーを指定します。	SCEP プロファイルの作成

iOS デバイスでのアプリの管理

デバイスで管理および監視するアプリのライブラリを作成できます。BlackBerry UEM は、iOS デバイス上のアプリを管理するために、次のオプションを提供します。

- 一般のアプリを App Store から割り当てます（デバイス上でオプションまたは必須として）。
- UEM にカスタムアプリをアップロードし、オプションまたは必須のアプリとして展開します。
- アプリで許可されている場合、接続設定などのアプリ設定を事前設定します。
- ユーザーが特定のアプリにアクセスできないようにブロックしたり、許可されたアプリをリストアップ（その他のアプリはすべてブロック）したりすることができます。
- Apple VPP アカウントを UEM にリンクして、VPP アカウントに関連付けられたアプリの購入済みライセンスを配布できるようにします。
- 一般、ISV、およびカスタムの BlackBerry Dynamics アプリを設定して、ユーザーが仕事用リソースにアクセスできるようにします。
- UEM を Microsoft Intune に接続することで、Intune アプリの保護ポリシーを UEM 管理コンソールの内部から設定し、Office 365 アプリを導入して管理できます。
- デバイスにインストールされている個人用アプリのリストを表示します。
- 環境内の他のユーザーのために、各ユーザーがアプリを評価およびレビューできるようにします。
- システムアプリと、UEM を使用して管理するアプリの通知設定を指定できます。
- デバイス上の仕事用アプリのアイコンとラベルを指定します。

MDM 制御 アクティベーションを使用した iOS デバイスでのアプリの動作

BlackBerry Dynamics が有効になっているデバイスの場合、「機能 - BlackBerry App Store」資格をユーザーに割り当てている場合は、仕事用アプリのカタログが BlackBerry Dynamics Launcher に表示されます。詳細については、「BlackBerry Dynamics Launcher への仕事用アプリカタログの追加」を参照してください。

MDM 制御 でアクティブ化された iOS デバイスの場合、次の動作が行われます。

アプリタイプ	アプリがユーザーに割り当てられるとき	アプリが更新されるとき	アプリがユーザーから割り当て解除されるとき	デバイスが **BlackBerry UEM** から削除されるとき
種別が必須になっている一般のアプリ	アプリが既にインストールされている場合、UEM によるアプリの管理を許可するように求めるプロンプトがユーザーに表示されます。 監視対象のデバイスで、アプリは自動的にインストールされます。 非監視対象デバイスでは、アプリをインストールするように求めるプロンプトがユーザーに表示されます。 アプリは、ユーザーが詳細を表示したとき（アプリがインストールされていない場合でも）、またはユーザーがアプリをインストールしたときに、「新規/更新」リストから削除されます。 コンプライアンスプロファイルを使用して、必須アプリがインストールされていない場合に実行する操作を定義できます。	iTunes は、利用可能な更新についてユーザーに通知します。 アプリは、ユーザーがアプリを更新したときに、「新規/更新」リストから削除されます。（最大 1 時間かかります） iTunes にアクセスできないデバイスの場合、ユーザーには通知されませんが、デバイスに Apple VPP ライセンスが割り当てられている場合、アプリカタログから更新をダウンロードできます。	アプリは通知なしに自動的に削除されます。 アプリはアプリカタログに表示されなくなります。	アプリは自動的に削除されます。

アプリタイプ	アプリがユーザーに割り当てられるとき	アプリが更新されるとき	アプリがユーザーから割り当て解除されるとき	デバイスが **BlackBerry UEM** から削除されるとき
種別がオプションになっている一般のアプリ	アプリが既にインストールされている場合、UEM によるアプリの管理を許可するように求めるプロンプトがユーザーに表示されます。 ユーザーは、アプリカタログへの変更について通知されます。 アプリは、ユーザーが詳細を表示したときにのみ（アプリがインストールされているかどうかに関わらず）、「新規/更新」リストから削除されます。 ユーザーはアプリをインストールするかどうかを選択できます。	iTunes は、利用可能な更新についてユーザーに通知します。 アプリは、ユーザーが詳細を表示したときに（アプリが更新されているかどうかに関わらず）、「新規/更新」リストから削除されます。	アプリは通知なしに自動的に削除されます。 アプリはアプリカタログに表示されなくなります。	アプリは自動的に削除されます。

アプリタイプ	アプリがユーザーに割り当てられるとき	アプリが更新されるとき	アプリがユーザーから割り当て解除されるとき	デバイスが **BlackBerry UEM** から削除されるとき
種別が必須になっている内部アプリ	アプリが既にインストールされている場合、UEM によるアプリの管理を許可するように求めるプロンプトがユーザーに表示されます。 監視対象のデバイスで、アプリは自動的にインストールされます。 非監視対象デバイスでは、アプリをインストールするように求めるプロンプトがユーザーに表示されます。ユーザーがインストールをキャンセルした場合、アプリカタログからアプリをインストールできます。 アプリは、ユーザーが詳細を表示したとき（アプリがインストールされていない場合でも）、またはユーザーがアプリをインストールしたときに、「新規/更新」リストから削除されます。 コンプライアンスプロファイルを使用して、必須アプリがインストールされていない場合に実行する操作を定義できます。	アプリは、ユーザーがアプリを更新したときに、「新規/更新」リストから削除されます。	アプリは通知なしに自動的に削除されます。 アプリはアプリカタログに表示されなくなります。	アプリは自動的に削除されます。

アプリタイプ	アプリがユーザーに割り当てられるとき	アプリが更新されるとき	アプリがユーザーから割り当て解除されるとき	デバイスが **BlackBerry UEM** から削除されるとき
種別がオプションになっている内部アプリ	アプリが既にインストールされている場合、UEM によるアプリの管理を許可するように求めるプロンプトがユーザーに表示されます。 アプリは、ユーザーが詳細を表示したとき（アプリがインストールされていない場合でも）、またはユーザーがアプリをインストールしたときに、「新規/更新」リストから削除されます。	アプリは、ユーザーがアプリを更新したときに、「新規/更新」リストから削除されます。	アプリは通知なしに MDM 制御 でアクティブ化されたデバイスから自動的に削除されます。 アプリは ユーザーのプライバシー でアクティブ化されたデバイスから削除されません。 アプリはアプリカタログに表示されなくなります。	アプリは自動的に削除されます。

ユーザーのプライバシー アクティベーションを使用した iOS デバイスでのアプリの動作

BlackBerry Dynamics が有効になっているデバイスの場合、「機能 - BlackBerry App Store」資格をユーザーに割り当てている場合は、仕事用アプリのカタログが BlackBerry Dynamics Launcher に表示されます。詳細については、「BlackBerry Dynamics Launcher への仕事用アプリカタログの追加」を参照してください。

ユーザーのプライバシー で iOS デバイスをアクティブ化する場合、アプリ管理を許可するかどうかを選択できます。アプリ管理を許可する場合、ユーザーのプライバシー アクティベーションのアプリの動作は MDM コントロールのアクティベーションと同じです。ユーザーのプライバシー でアクティブ化された iOS デバイスのアプリ管理を許可しない場合、次の動作が行われます。

アプリタイプ	アプリがユーザーに割り当てられるとき	アプリが更新されるとき	アプリがユーザーから割り当て解除されるとき	デバイスが **BlackBerry UEM** から削除されるとき
種別が必須になっている一般のアプリ	ユーザーはアプリのインストールを要求されません。ユーザーは、必要なアプリをインストールするためにアプリカタログに移動する必要があります。 アプリは、ユーザーが詳細を表示したとき（アプリがインストールされていない場合でも）、またはユーザーがアプリをインストールしたときに、「新規/更新」リストから削除されます。	iTunes は、利用可能な更新についてユーザーに通知します。 アプリは、ユーザーがアプリを更新したときに、「新規/更新」リストから削除されます。（最大 1 時間かかります） iTunes にアクセスできないデバイスの場合、ユーザーには通知されませんが、アプリカタログから更新をダウンロードすることができます。	アプリはデバイスに残ります。 アプリはアプリカタログに表示されなくなります。	アプリはデバイスに残ります。
種別がオプションになっている一般のアプリ	アプリが既にインストールされている場合は何も起こりません。 ユーザーは、アプリカタログへの変更について通知されます。 アプリは、ユーザーが詳細を表示したときにのみ（アプリがインストールされているかどうかに関わらず）、「新規/更新」リストから削除されます。 ユーザーはアプリをインストールするかどうかを選択できます。	iTunes は、利用可能な更新についてユーザーに通知します。 アプリは、ユーザーが詳細を表示したときに（アプリが更新されているかどうかに関わらず）、「新規/更新」リストから削除されます。	アプリはデバイスに残ります。 アプリはアプリカタログに表示されなくなります。	アプリはデバイスに残ります。

アプリタイプ	アプリがユーザーに割り当てられるとき	アプリが更新されるとき	アプリがユーザーから割り当て解除されるとき	デバイスが **BlackBerry UEM** から削除されるとき
種別が必須になっている内部アプリ	アプリが既にインストールされている場合、UEM によるアプリの管理を許可するように求めるプロンプトがユーザーに表示されます。 アプリは、ユーザーが詳細を表示したとき（アプリがインストールされていない場合でも）、またはユーザーがアプリをインストールしたときに、「新規/更新」リストから削除されます。	アプリは、ユーザーがアプリを更新したときに、「新規/更新」リストから削除されます。	アプリはデバイスに残ります。 アプリはアプリカタログに表示されなくなります。	アプリはデバイスに残ります。
種別がオプションになっている内部アプリ	アプリが既にインストールされている場合は何も起こりません。 アプリは、ユーザーが詳細を表示したとき（アプリがインストールされていない場合でも）、またはユーザーがアプリをインストールしたときに、「新規/更新」リストから削除されます。	アプリは、ユーザーがアプリを更新したときに、「新規/更新」リストから削除されます。	アプリはデバイスに残ります。 アプリはアプリカタログに表示されなくなります。	アプリはデバイスに残ります。

iOS デバイスのアクティベーション

iOS で BlackBerry UEM デバイスをアクティベーションする場合は、管理者がデバイスを管理でき、ユーザーがデバイス上の仕事用データにアクセスできるように、デバイスを BlackBerry UEM に関連付けます。

Apple Configurator 2 を使用するかどうかにかかわらず、BlackBerry UEM でデバイスをアクティベーションして、デバイスのアクティベーションを準備できます。Apple Configurator 2 の使用の詳細については、管理関連の資料の「Apple Configurator 2 を使用した iOS デバイスのアクティベーション」を参照してください。

Apple の Device Enrollment Program に iOS デバイスを登録し、BlackBerry UEM 管理コンソールを使用して、デバイスに登録設定を割り当てることができます。登録設定には、［管理モードを有効にする］など、MDM 登録中にデバイスに割り当てられた追加のルールが含まれています。詳細については、管理関連の資料の「DEP に登録されている iOS デバイスのアクティベーション」を参照してください。

デバイスを DEP に登録していない場合でも、アクティベーションプロファイルの設定を使用して、非監視対象デバイスのアクティベーションを防ぐことができます。

アクティベーションタイプ：iOS デバイス

アクティベーションタイプ	説明
MDM 制御	このアクティベーションタイプは、iOS で利用可能なデバイス制御権限を使用して、基本的なデバイス管理を提供します。個別の仕事用領域はデバイスにインストールされず、仕事用データのセキュリティも追加されません。 コマンドと IT ポリシーを使用してデバイスを制御できます。アクティベーションの実行時に、ユーザーはデバイスにモバイルデバイス管理プロファイルをインストールする必要があります。 BlackBerry UEM がデバイス ID によるアクティベーションを制限できるかどうかを指定するには、［承認されたデバイス **ID** のみを許可する］を選択します。

アクティベーションタイプ	説明
ユーザーのプライバシー	ユーザーのプライバシー アクティベーションタイプを使用して、ユーザーの個人データがプライベートの状態であることを確認しながら、デバイスの基本的な制御を提供できます。このアクティベーションタイプでは、別個のコンテナはデバイスにインストールされず、仕事用データの追加セキュリティも提供されません。ユーザーのプライバシー でアクティブ化されたデバイスは、BlackBerry UEM でアクティブ化され、［電話を探す］や［ルートの検出］などのサービスを利用することができます。ただし、管理者はデバイスポリシーを制御できません。 メモ：SIM ベースのライセンスの場合は、アクティベーションプロファイルで［SIM ベースのライセンスを有効にするには、SIM カードとデバイスのハードウェア情報へのアクセスを許可します］を選択する必要があります。ユーザーは、SIM カードとデバイスハードウェアの情報のみにアクセスできる MDM プロファイルをインストールする必要があります。これらの情報は、適切な SIM ライセンス（ICCID、IMEI など）が利用可能であるかどうかを確認するために必要です。 このアクティベーションタイプは Apple TV デバイスではサポートされません。 iOS アクティベーションプロファイルで ユーザーのプライバシー アクティベーションを許可する場合は、組織のニーズに基づいて、デバイスで管理するプロファイルを選択します。次のいずれかを選択できます。 • **SIM** ベースのライセンスを有効にするには、**SIM** カードとデバイスのハードウェア情報へのアクセスを許可します：このオプションは、BlackBerry UEM が SIM カードと ICCID や IMEI などのデバイスハードウェア情報にアクセスして、適切な SIM ライセンスが使用可能なことを確認できるかどうかを指定します。 • アプリの管理を許可する：このオプションでは、デバイスの仕事用アプリをインストールするか削除するかを指定します。ユーザーの詳細画面には、インストール済みの仕事用アプリが一覧で表示されます。アプリのショートカットを許可するかどうかも指定できます。 • **IT** ポリシーの管理を許可する：このオプションでは、IT ポリシールールの限定されたセットをデバイスに適用するかどうかを指定します（パスワードポリシー、スクリーンショットの許可、管理されている送信元から管理されていない送信先にドキュメントを送信する許可、管理されていない送信元から管理されている送信先にドキュメントを送信する許可）。 • メールプロファイル管理を許可する：このオプションでは、ユーザーに割り当てられているメールプロファイル設定をデバイスに適用するかどうかを指定します。 • **Wi-Fi** プロファイル管理を許可する：このオプションでは、ユーザーに割り当てられている Wi-Fi プロファイル設定をデバイスに適用するかどうかを指定します。 • **VPN** プロファイル管理を許可する：このオプションでは、ユーザーに割り当てられている VPN プロファイル設定をデバイスに適用するかどうかを指定します。

アクティベーションタイプ	説明
ユーザーのプライバシー - ユーザー登録	iOS および iPad OS デバイスに ユーザーのプライバシー - ユーザー登録 アクティベーションタイプを使用して、ユーザーデータがプライベートに保持され、仕事用データから分離されていることを確認できます。このアクティベーションタイプでは、デバイスに、仕事用アプリとネイティブ Notes、iCloud ドライブ、メール（添付ファイルとメール本文全体）、カレンダー（添付ファイル）、および iCloud Keychain アプリ用の個別の仕事用領域がインストールされます。 このアクティベーションタイプでは、アプリ管理、IT ポリシー管理、メールプロファイル、Wi-Fi プロファイル、per-app VPN が有効になります。管理者は、個人データに影響を与えることなく、作業データを管理（たとえば、作業データの消去）ができます。 このアクティベーションタイプは、iOS または iPad OS 13.1 以降を実行する非監視対象の iPhone および iPad デバイスでサポートされています。
BlackBerry 2FA 専用のデバイス登録	このアクティベーションタイプは、BlackBerry 2FA によって管理されないデバイス向けの BlackBerry UEM ソリューションをサポートします。このアクティベーションタイプではデバイス管理や制御は提供されませんが、デバイスは BlackBerry 2FA 機能を使用できます。このアクティベーションタイプを使用するには、BlackBerry 2FA プロファイルをユーザーに割り当てる必要もあります。 デバイスがアクティベーションされた場合、管理コンソールで限定されたデバイスの情報を表示したり、コマンドを使用してデバイスを無効にしたりできます。 このアクティベーションタイプは Microsoft Active Directory ユーザーでのみサポートされます。 このアクティベーションタイプは Apple TV デバイスではサポートされません。 詳細については、BlackBerry 2FA 関連の資料を参照してください。

iOS バージョン 12.2 以降のデバイスのアクティベーション（MDM 制御 のアクティベーションタイプ）

これらの手順は、MDM 制御 または MDM オプションを有効にした状態でユーザープライバシーを使用してアクティブ化された iOS バージョン 12.2 以降のデバイスに適用されます。

iOSバージョン 12.2 以降のデバイスで MDM 加入を行う際、ユーザーは BlackBerry UEM Client アプリを終了して MDM プロファイルを手動でインストールする必要があります。これらの手順は、古いバージョンの iOS では必要ありません。

デバイスユーザーに次のアクティベーション手順を送信するか、次のワークフローへのリンクを送信します。iOS デバイスのアクティベーション

1. デバイスに BlackBerry UEM Client をインストールします。App Store から BlackBerry UEM Client をダウンロードできます。
2. デバイスで、［**UEM Client**］をタップし、使用許諾契約に同意します。

3. 次の操作のいずれかを実行します。

タスク	手順
QR Code を使用してデバイスをアクティベーションする	**a.** をタップします。 **b.** BlackBerry UEM Client の写真撮影とビデオ録画を許可するには、［許可］をタップします。 **c.** 受信したアクティベーションメールの QR Code をスキャンします。
デバイスを手動でアクティベーションする	**a.** 仕事用メールアドレスを入力して、アクティベーションパスワードを入力します。 **b.** 必要に応じて、サーバーアドレスを入力します。サーバーアドレスは、受信したアクティベーションメールまたは BlackBerry UEM Self-Service で確認できます。 **c.** ［次へ］をタップします。

4. UEM Client の通知の送信を許可するには、［許可］をタップします。［許可しない］を選択すると、デバイスが完全にアクティブ化されなくなります。
5. 設定プロファイルのインストールを求めるプロンプトが表示されたら、［**OK**］をタップします。
6. 設定プロファイルのダウンロードを求めるプロンプトが表示されたら、［許可］をタップします。
7. ダウンロードが完了したら、［設定］を開きます。
8. ［全般］をタップして［プロファイルとデバイス管理］に移動します。
9. プロファイルをインストールするには、［**BlackBerry UEM** プロファイル］をタップし、画面の指示に従います。
10. インストールが完了したら BlackBerry UEM Client アプリに戻り、アクティベーションを完了します。
11. プロンプトが表示されたら、画面の手順に従ってデバイスに仕事用アプリをインストールします。

終了したら： アクティベーションプロセスの正常な完了を確認するには、次のいずれかの操作を実行します。

- デバイスで BlackBerry UEM Client アプリを開いて、［バージョン情報］をタップします。［アクティブ化されたデバイス］および［コンプライアンスステータス］セクションで、デバイス情報とアクティベーションのタイムスタンプが存在することを確認します。
- BlackBerry UEM Self-Service で、当該デバイスがアクティブ化されたデバイスとして一覧に表示されていることを確認します。ユーザーがデバイスをアクティブ化した後、ステータスの更新に最大で 2 分かかることがあります。

12.2 よりも前の iOS デバイスのアクティベーション（MDM 制御 のアクティベーションタイプ）

MDM 制御 を使用してバージョン 12.2 より前の iOS デバイスをアクティブ化するには、次の手順をデバイスユーザに送信します。

1. デバイスに BlackBerry UEM Client をインストールします。App Store から BlackBerry UEM Client をダウンロードできます。
2. デバイスで、［**UEM Client**］をタップし、使用許諾契約に同意します。
3. 次の操作のいずれかを実行します。

タスク	手順
QR Code を使用してデバイスをアクティベーションする	**a.** をタップします。 **b.** BlackBerry UEM Client の写真撮影とビデオ録画を許可するには、［許可］をタップします。 **c.** 受信したアクティベーションメールの QR Code をスキャンします。
デバイスを手動でアクティベーションする	**a.** 仕事用メールアドレスを入力して、アクティベーションパスワードを入力します。 **b.** 必要に応じて、サーバーアドレスを入力します。サーバーアドレスは、受信したアクティベーションメールまたは BlackBerry UEM Self-Service で確認できます。 **c.** ［次へ］をタップします。

4. ［**OK**］をタップして、設定プロファイルをインストールします。
5. 画面に表示される手順に従って、アクティベーションを完了します。
6. メールアカウントのパスワードまたはデバイスのパスコードの入力が求められたら、画面の指示に従います。

終了したら： アクティベーションプロセスの正常な完了を確認するには、次のいずれかの操作を実行します。

- デバイスで BlackBerry UEM Client アプリを開いて、［バージョン情報］をタップします。［アクティブ化されたデバイス］および［コンプライアンスステータス］セクションで、デバイス情報とアクティベーションのタイムスタンプが存在することを確認します。
- BlackBerry UEM Self-Service で、当該デバイスがアクティブ化されたデバイスとして一覧に表示されていることを確認します。ユーザーがデバイスをアクティブ化した後、ステータスの更新に最大で 2 分かかることがあります。

Apple ユーザー登録を使用した iOS または iPad OS デバイスのアクティブ化

Apple ユーザー登録は、iPad および iPad OS 13.1 以降を実行しているデバイスでのみサポートされています。

登録を開始するには、ユーザーはデバイス上のカメラアプリを使用して、Apple ユーザー登録アクティベーションメールに記載されている QR Code をスキャンし、MDM プロファイルを手動でダウンロードしてデバイスにインストールします。デバイスをアクティブ化するには、ユーザーは、BlackBerry UEM ユーザーアカウントのメールアドレスと一致する管理 Apple ID アカウントにログインします。ユーザーが他の BlackBerry Dynamics アプリのアクティブ化、証明書のインポート、BlackBerry 2FA 機能の使用、CylancePROTECT の使用、およびコンプライアンスステータスの確認を簡単に行えるようにする場合は、VPP ライセンスを使用して UEM Client をユーザーに割り当てる必要があります。ユーザーが使用許諾契約に同意すると、UEM Client のセットアップが開始されます。

次のアクティベーション手順をデバイスユーザーに送信します。

作業を始める前に：

- Apple ユーザー登録用の QR Code が記載されたアクティベーションメールを受信したことを確認します。メールを受信していない場合は、管理者に連絡してください。

- BlackBerry UEM でデバイスがすでにアクティブ化されている場合は、デバイスを無効にする必要があります。
- BlackBerry UEM Client をアンインストールします。
- 組織を通じて管理されている管理 Apple ID アカウントが必要です。
- デバイスは監視対象のデバイスであってはなりません。デバイスが監視対象である場合、Apple ID の近くの設定アプリに表示されます。

1. Apple ユーザー登録用の QR Code が含まれているアクティベーションメールを開きます。QR Code の有効期限がすでに切れている場合は、BlackBerry UEM Self-Service に新しいアクティベーションコードを要求するか、管理者に連絡してください。
2. デバイスでカメラアプリを開き、アクティベーションメールの QR コードをスキャンします。プロンプトが表示されたら、通知をタップして Safari で URL を開きます。
3. UEM 設定プロファイルのダウンロードを求めるプロンプトが表示されたら、［許可］をタップします。
4. ダウンロードが完了したら、［閉じる］をタップします。
5. ［設定］ > **[**一般**]** > **[**プロファイル**]**に移動します。
6. ［**UEM** プロファイル］をタップします。
7. ［ユーザー登録］画面で、［**iPhone** を登録］または［**iPad** を登録］をタップします。
8. パスコードを入力します。
9. 管理 Apple ID 資格情報を使用して Apple ID にログインします。
10. 管理者が BlackBerry UEM Client アプリを割り当てた場合は、プロンプトが表示されたら［インストール］をタップするか、仕事用アプリを開きます。
11. BlackBerry UEM Client アプリを設定するには、アプリを開き、使用許諾契約に同意します。画面に表示される手順に従って、アクティベーションプロセスを完了します。

終了したら： アクティベーションプロセスの正常な完了を確認するには、次のいずれかの操作を実行します。

- デバイスで BlackBerry UEM Client アプリを開いて、［バージョン情報］をタップします。［アクティブ化されたデバイス］および［コンプライアンスステータス］セクションで、デバイス情報とアクティベーションのタイムスタンプが存在することを確認します。
- BlackBerry UEM Self-Service で、当該デバイスがアクティブ化されたデバイスとして一覧に表示されていることを確認します。ユーザーがデバイスをアクティブ化した後、ステータスの更新に最大で 2 分かかることがあります。

アクティブ化された iOS デバイスの管理と監視

デバイスがアクティブ化され、IT ポリシーとプロファイルによって管理されると、ユーザーのデバイスを制御するいくつかの機能を使用できるようになります。

次のオプションがあります。

オプション	説明
利用可能なソフトウェア更新を確認し、デバイスを更新する	すべての監視対象デバイスについて、利用可能な OS 更新を表示できます。次のデバイスに対して、使用可能な更新をインストールするように強制できます。 • iOS 10.3 以降を実行している監視対象デバイス • 監視対象 DEP デバイス 詳細については、管理関連の資料を参照してください。
位置情報設定をオンにして、紛失モードを有効にする	位置情報設定をオンにして、iOS デバイスの位置を追跡できます。紛失したデバイスを見つけるために紛失モードを有効にすることもできます。 詳細については、管理関連の資料を参照してください。
アクティベーションロックを有効にする	iOS デバイスのアクティベーションロック機能では、［マイ iPhone を検索］の無効化やデバイスの消去の際、またはデバイスを再アクティブ化して使用する際に、ユーザーが Apple ID とパスワードを確認する必要があります。 BlackBerry UEM でアクティベーションロック機能を管理するには、次の手順を実行します。 • デバイスは監視対象として設定されている必要があります。 • デバイスに iCloud アカウントが設定されている必要があります。 • デバイスで［マイ iPhone を検索］または［マイ iPad を検索］が有効になっている必要があります。 BlackBerry UEM は、ロックを解除できるバイパスコードを格納するので、ユーザーの Apple ID とパスワードなしでデバイスの消去と再アクティブ化が可能になります。 詳細については、管理関連の資料を参照してください。
デバイスログの取得	デバイスからログを取得して、監視やトラブルシューティングを行うことができます。 詳細については、管理関連の資料を参照してください。

オプション	説明
デバイスを無効にする	管理者またはユーザーがデバイスを無効化すると、BlackBerry UEM 内の、デバイスとユーザーアカウント間の接続が削除されます。デバイスは管理できなくなり、管理コンソールに表示されなくなります。ユーザーはデバイス上の仕事用データにアクセスできません。 管理者は、［すべてのデバイスデータを削除］または［仕事用データのみを削除］コマンドを使用してデバイスを無効化できます。 ユーザーは、iOS アプリの［バージョン情報］画面で［デバイスを無効にする］を選択することで、BlackBerry UEM Client デバイスを無効化できます。

iOS デバイスのコマンド

コマンド	説明	アクティベーションタイプ
デバイスレポートを表示	このコマンドを実行すると、デバイスに関する詳細情報が表示されます。デバイスレポートをエクスポートしたりコンピューターに保存したりできます。詳細については、「デバイスレポートの表示と保存」を参照してください。	MDM 制御 ユーザーのプライバシー
デバイスでの操作を表示	このコマンドを実行すると、デバイスで実行中のアクションが表示されます。詳細については、「デバイスアクションの表示」を参照してください。	MDM 制御 ユーザーのプライバシー
すべてのデバイスデータを削除	このコマンドは、デバイスに保存されているユーザー情報とアプリデータをすべて削除して、デバイスを工場出荷時のデフォルト設定に戻します。 このコマンドを送信するときにデバイスが BlackBerry UEM に接続できない場合、このコマンドをキャンセルするか、コンソールからデバイスを削除することができます。削除後にデバイスが BlackBerry UEM に接続すると、仕事用データのみがデバイスから削除されます。 このコマンドを複数のデバイスに送信するには、「一括コマンドの送信」を参照してください。	MDM 制御

コマンド	説明	アクティベーションタイプ
仕事用データのみを削除	このコマンドは、デバイス上の IT ポリシー、プロファイル、アプリ、証明書を含む仕事用データを削除します。 このコマンドを送信するときにデバイスが BlackBerry UEM に接続できない場合、このコマンドをキャンセルするか、コンソールからデバイスを削除することができます。削除後にデバイスが BlackBerry UEM に接続すると、仕事用データがデバイスから削除されます。 このコマンドを複数のデバイスに送信するには、「一括コマンドの送信」を参照してください。	MDM 制御 ユーザーのプライバシー
デバイスのロック	このコマンドは、デバイスをロックします。ユーザーは、デバイスのロックを解除するために、既存のデバイスパスワードを入力する必要があります。一時的にデバイスが見つからない場合、このコマンドを使用することができます。 このコマンドを送信すると、既存のデバイスパスワードが存在する場合に限ってデバイスがロックされます。それ以外の場合、デバイスでは何の操作も実行されません。 Apple TV デバイスでは、このコマンドはサポートされていません。	MDM 制御
ロック解除してパスワードをクリア	このコマンドは、デバイスのロックを解除して、既存のパスワードを削除します。ユーザーは、デバイスパスワードを作成するように要求されます。このコマンドは、ユーザーがデバイスパスワードを忘れた場合に使用できます。 Apple TV デバイスでは、このコマンドはサポートされていません。	MDM 制御
紛失モードをオンにする	このコマンドは、デバイスをロックします。またこのコマンドでは、デバイスに表示する電話番号とメッセージを設定できます。例えば、デバイスが拾われたときに、連絡先情報を表示させることができます。 このコマンドの送信後に、BlackBerry UEM からデバイスの場所を表示できます。 このコマンドは、監視対象 iOS デバイスでのみサポートされます。 Apple TV デバイスでは、このコマンドはサポートされていません。	

コマンド	説明	アクティベーションタイプ
BlackBerry 2FA を無効化	このコマンドは、BlackBerry 2FA アクティベーションタイプでアクティベーションされているデバイスを無効にします。デバイスは BlackBerry UEM から削除され、ユーザーは BlackBerry 2FA 機能を使用できません。 Apple TV デバイスでは、このコマンドはサポートされていません。	MDM 制御
OS の更新	このコマンドは、利用可能な OS の更新をインストールするようにデバイスに強制します。次のデバイスでサポートされています。 • iOS 10.3 以降を実行している監視対象デバイス • 監視対象 DEP デバイス 詳細については、「監視対象の iOS デバイスでの OS の更新」を参照してください。 このコマンドを複数のデバイスに送信するには、「一括コマンドの送信」を参照してください。 Apple TV デバイスでは、このコマンドはサポートされていません。	MDM 制御
デバイスを再起動する	このコマンドは、デバイスを強制的に再起動します。10.3 以降を実行している監視対象 iOS デバイスでサポートされます。 Apple TV デバイスでは、このコマンドはサポートされていません。	MDM 制御
デバイスをオフにする	このコマンドは、デバイスを強制的にオフにします。10.3 以降を実行している監視対象 iOS デバイスでサポートされます。 Apple TV デバイスでは、このコマンドはサポートされていません。	MDM 制御
アプリを消去	このコマンドは、Microsoft Intune で管理している全アプリのデータをデバイスから消去します。アプリはデバイスから削除されません。 詳細については、「Microsoft Intune で管理されているアプリの消去」を参照してください。	MDM 制御

コマンド	説明	アクティベーションタイプ
デバイス情報を更新	このコマンドは更新されたデバイス情報を送受信します。たとえば、新たに更新された IT ポリシールールやプロファイルをデバイスに送信したり、OS バージョンやバッテリ残量などのデバイスに関する最新情報を受信したりすることができます。 このコマンドを複数のデバイスに送信するには、「一括コマンドの送信」を参照してください。	MDM 制御 ユーザーのプライバシー
デバイスを削除	このコマンドは、デバイスを BlackBerry UEM から削除しますが、デバイスからデータを削除しません。デバイスはメールなどの仕事用データをひき続き受信する場合があります。 このコマンドは、回復不能なほど失われたまたは損傷したデバイスを対象としており、サーバーに再度接続することは想定されていません。削除されたデバイスが BlackBerry UEM に接続しようとすると、ユーザーは通知を受信し、再アクティブ化しない限り、デバイスは BlackBerry UEM と通信できなくなります。 このコマンドを複数のデバイスに送信するには、「一括コマンドの送信」を参照してください。	MDM 制御 ユーザーのプライバシー

商標などに関する情報

©2020 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。

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