BlackBerry UEM

概要とアーキテクチャ

12.20

Contents

BlackBerry UEM とは..... 5
BlackBerry UEM の主な機能.....6
すべてのデバイスタイプに対応する主な機能.....8
各デバイスタイプに対応する主な機能.....11
デバイスタイプ別サポートされている機能.....16

BlackBerry UEM アーキテクチャ..... 22
オンプレミスの BlackBerry UEM のコンポーネント.....27
オンプレミスの BlackBerry UEM の分散インストール.....30

付随する製品およびサービス.....34
エンタープライズアプリおよび BlackBerry Dynamics アプリ.....34
BlackBerry Enterprise Identity の利点.....36
BlackBerry 2FA の利点.....36
BlackBerry Workspaces の利点.....36
BlackBerry UEM Notifications の利点.....37
BlackBerry Enterprise SDK.....37

データフロー：デバイスと BlackBerry Dynamics アプリのアクティブ化.....39
データフロー：管理対象 Google Play アカウントを使用して Android Enterprise 仕事用と個人用 - ユーザーのプライバシー デバイスをアクティブ化する..... 39
データフロー：管理対象 Google Play アカウントを使用して Android Enterprise 仕事用と個人用 - フルコントロール デバイスをアクティブ化する.....41
データフロー：管理対象 Google Play アカウントを使用して Android Enterprise 仕事用領域のみ デバイスをアクティブ化する..... 42
データフロー：Google ドメインで Android Enterprise 仕事用と個人用 - ユーザーのプライバシー デバイスをアクティブ化する..... 44
データフロー：Google ドメインで Android Enterprise 仕事用と個人用 - フルコントロール デバイスをアクティブ化する.....45
データフロー：Google ドメインで Android Enterprise 仕事用領域のみ デバイスをアクティブ化する..... 47
データフロー：デバイスをアクティブ化して Knox Workspace を使用する.....49
データフロー：iOS デバイスのアクティベーション.....51
データフロー：macOS デバイスのアクティベーション..... 53
データフロー：Windows 10 デバイスのアクティベーション.....54
データフロー：デバイスでの最初の BlackBerry Dynamics アプリのアクティベーション.....56
データフロー：すでにデバイスでアクティベートされているアプリがある場合の BlackBerry Dynamics アプリのアクティベーション.....57

データフロー：仕事用データの送受信..... 59

BlackBerry Infrastructure の使用による仕事用データの送受信 60
データフロー：BlackBerry Dynamics NOC を介して BlackBerry Dynamics アプリから仕事用データ送受信する 61
データフロー：BlackBerry Infrastructure を介して BlackBerry Dynamics アプリから仕事用データ送受信する 62
データフロー： BlackBerry Dynamics Direct Connect を使用して BlackBerry Dynamics アプリから仕事用データ送受信する 62
データフロー：BlackBerry Secure Connect Plus を使用する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 63
データフロー：BlackBerry Secure Connect Plus を使用する Android デバイスで BlackBerry Dynamics アプリから仕事用データを送受信する 64
データフロー：BlackBerry Secure Gateway の使用時における iOS デバイスのメールサーバーでの認証 65
データフロー：iOS を使用した BlackBerry Secure Gateway デバイスからのメールの送信 67
データフロー：iOS を使用した BlackBerry Secure Gateway デバイスでのメールの受信 67
VPN または仕事用 Wi-Fi ネットワークの使用による作業データの送受信 68
データフロー：VPN または仕事用 Wi-Fi ネットワークを使用してデバイスからメールを送信する 68
データフロー：VPN または仕事用 Wi-Fi ネットワークを使用してデバイスでメールを受信する 69
データフロー：VPN または仕事用 Wi-Fi ネットワークを使用した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 69

データフロー：デバイス設定の更新の受信 71
データフロー：Android デバイスでの設定更新の受信 72
データフロー：Samsung Knox デバイスのファームウェアを更新する 73
データフロー：iOS デバイスでの設定更新の受信 74
データフロー：macOS デバイスでの設定更新の受信 75
データフロー：Windows 10 デバイスでの設定更新の受信 75

商標などに関する情報 77

BlackBerry UEM とは

BlackBerry UEM はマルチプラットフォーム EMM ソリューションです。統合されたセキュリティおよび接続機能により、デバイス、アプリ、コンテンツを包括的に管理できるため、組織での iOS、macOS、Android、Windows のデバイスの管理に役立ちます。

オンプレミス環境に UEM をインストールすると、サーバー、データ、デバイスを最大限に制御できます。また、UEM Cloud を使用して、使いやすく低コストでセキュリティ保護されたソリューションを利用することもできます。BlackBerry は UEM Cloud をインターネット経由でホストするため、サービスにアクセスするのに必要なのはサポートされている Web ブラウザーのみです。

オンプレミスの UEM および UEM Cloud はともに、信頼性の高いエンドツーエンドのセキュリティを提供し、組織がすべてのエンドポイントと所有モデルを管理するために必要な制御を提供します。

UEM の利点は次のとおりです。

機能	利点
低い総所有コスト	オンプレミスの UEM では、複雑さを軽減し、プールされたリソースを最適化し、アップタイムを最大化することで、オンプレミスソリューションの総所有コストを最小限に抑えることができます。 UEM Cloud では、サービスのインストール、管理、更新の必要性をなくすことで、所有コストを削減します。
単一の Web ベースのインターフェイス	単一の管理コンソールから、iOS、macOS、Android、Windows のデバイス、および追加のサービスを管理できます。
柔軟な所有モデル	カスタマイズ可能なポリシーとプロファイルのセットを使用して、BYOD、COPE、および COBO の各デバイスを管理し、ビジネス情報を保護します。
ユーザーおよびデバイスのレポート	包括的なレポートとダッシュボード、動的なフィルター、および検索機能を使用して、一連のデバイスを管理できます。
簡単なユーザーのセットアップと登録	ユーザーが BlackBerry UEM Self-Service を使用して、UEM 上で自分のデバイスをアクティブ化できるようにします。
業界をリードするモバイルセキュリティ	BlackBerry Infrastructure を活用してすべてのデバイスのデータセキュリティを確保します。
高可用性	オンプレミスで高可用性を構成してデバイスユーザーのサービス中断を最小限に抑えることも、BlackBerry によって UEM Cloud を維持してアップタイムを最大化することもできます。
その他の利用可能なサービス	BlackBerry Workspaces、BlackBerry Enterprise Identity、BlackBerry 2FA、 BBM Enterprise、UEM Notifications などのサービスを有効にして、UEM の展開に付加価値を提供します。

BlackBerry UEM の主な機能

機能	説明
マルチプラットフォームデバイス管理	iOS、macOS、Android、および Windows デバイスを管理できます。
統合された直観的な UI	すべてのデバイスを 1 か所に表示し、単一の Web ベースの UI ですべての管理タスクにアクセスできます。同時に管理コンソールにアクセスできる複数の管理者と責務を共有できます。デフォルトビューと詳細ビューを切り替えて、情報表示のオプションやユーザーリストフィルタリングのオプションを表示できます。
信頼された安全なエクスペリエンス	デバイス制御機能により、デバイスがネットワークに接続する方法、有効にする機能、利用可能にするアプリを詳細に管理できます。デバイスが組織所有かユーザー所有かに関係なく、組織のデータを保護できます。
仕事上のニーズと個人的なニーズの分離	個人および仕事の情報がデバイス上で分離してセキュリティ保護された状態で維持されるように設計された、Android Enterprise、Android Management、および Samsung Knox の技術を使用して、デバイスを管理できます。デバイスの紛失時や侵害時には、デバイスから仕事に関連する情報のみを削除するか、すべての情報を削除するかを選択できます。
セキュリティで保護された IP 接続	BlackBerry Secure Connect Plus を使用して、仕事用プロファイルを持つ iOS および Android デバイスの仕事用領域アプリと組織のネットワークの間に、セキュリティ保護された IP トンネルを提供します。このトンネルによって、ユーザーは、組織のファイアウォール内の仕事用リソースにアクセスするときに、標準の IPv4 プロトコル（TCP および UDP）とエンドツーエンドの暗号化を使用して、データのセキュリティを確保できます。
シンプルなユーザーセルフサービス	BlackBerry UEM Self-Service を使用すると、デバイスを管理するオプションを適時にユーザーに提供するだけでなく、サポートリクエストの数が減り、組織の IT コストを削減することができます。UEM Self-Service を使用して、ユーザーはデバイスのアクティブ化または切り替え、デバイスパスワードのリモート変更、デバイスデータの削除、紛失または盗難デバイスのロックを行うことができます。
他の BlackBerry サービスとの統合	UEM を BlackBerry Workspaces、BlackBerry Enterprise Identity および BlackBerry 2FA と統合して、組織の UEM インスタンスに付加価値を付けることができます。
強力なアプリ管理	UEM は、すべてのデバイスに対応する包括的なアプリ管理プラットフォームです。App Store および Google Play など、すべての主要アプリストアからアプリを導入することができます。

機能	説明
ロールベースの管理	同時に管理コンソールにアクセスできる複数の管理者と責務を共有できます。ロールを使用して、管理者が実行できるアクションを定義し、セキュリティリスクを軽減し、ジョブの責任を分配し、効率を向上させることができます。事前定義されたロールを使用することもできれば、専用のカスタムロールを作成することもできます。
会社のディレクトリ統合	ローカルの組み込みユーザー認証を使用して、管理コンソールとセルフサービスコンソールにアクセスしたり、UEM を組織の環境内で使用されている Microsoft Active Directory、LDAP、または Entra ID ディレクトリと統合したりすることができます。UEM は、複数のディレクトリへの接続をサポートしています。 ディレクトリのユーザーデータを使用して、UEM でユーザーアカウントを作成できます。また、会社のディレクトリグループを UEM にリンクして、会社のディレクトリと同じ方法で UEM でユーザーを整理できます。 また、会社のディレクトリで特定のグループのオンボーディングを有効にし、UEM ユーザーを自動的に作成することもできます。オンボーディングを有効にすると、ユーザーが会社のディレクトリのグループから削除されたときに、デバイスデータまたはユーザーアカウントを削除するようにオフボーディングを設定することもできます。
移行	ユーザー、デバイス、グループ、およびその他のデータを、オンプレミスの UEM のソースデータベースから新しいオンプレミスまたは UEM Cloud インスタンスに移行できます。
Cisco ISE の統合	Cisco Identity Services Engine （ISE）は、デバイスが組織の仕事用ネットワークにアクセスできるかどうかを制御する機能を提供する、ネットワーク管理ソフトウェアです（たとえば、Wi-Fi の許可または拒否、VPN 接続など）。Cisco ISE とオンプレミスの UEM 間の接続を作成できるので、Cisco ISE が UEM 上でアクティブ化されたデバイスに関するデータを取得できるようになります。Cisco ISE はデバイスデータを確認し、デバイスが組織のアクセスポリシーに準拠しているかどうかを判断します。
地域での導入	1 つまたは複数の BlackBerry Connectivity Node インスタンスを専用地域に配置することで、エンタープライズ接続機能の地域接続を設定できます。これはサーバーグループと呼ばれています。各 BlackBerry Connectivity Node には、BlackBerry Secure Connect Plus、BlackBerry Gatekeeping Service、BlackBerry Secure Gateway、BlackBerry Proxy、および BlackBerry Cloud Connector が含まれます。エンタープライズ接続とメールプロファイルをサーバーグループに関連付けることで、これらのプロファイルを割り当てられたユーザーが BlackBerry Connectivity Node コンポーネントを使用するときに、BlackBerry Infrastructure に特定の地域接続を使用できるようになります。サーバーグループに複数の BlackBerry Connectivity Node を導入すると、高可用性とロードバランシングも実現できます。

機能	説明
ウェアラブルデバイス	UEM では、Android ベースの特定のウェアラブルデバイスをアクティブにして管理できます。たとえば Vuzix M300 Smart Glasses を管理できます。スマートグラスでは、通知、ステップバイステップの手順説明、画像、ビデオなど、視覚的な情報にハンズフリーでアクセスできます。また、音声コマンドの発行、バーコードのスキャン、GPS ナビゲーションの利用も可能にします。サポートされる UEM 管理機能の例としては、QR コードや IT ポリシー、Wi-Fi および VPN プロファイルを使用したデバイスのアクティベーション、アプリ管理、位置情報サービスなどがあります。
Microsoft Intune の統合	iOS デバイスおよび Android デバイスで、Microsoft Intune の MAM 機能を使用して Microsoft 365 アプリ内のデータを保護する場合は、UEM によるデバイスの管理を通じて、Intune を使用してアプリデータを保護できます。Intune にはアプリ内のデータを保護するセキュリティ機能が備わっています。例えば、Intune では、アプリ内でのデータ暗号化を要求したり、コピー、貼り付け、印刷、［名前を付けて保存］コマンドの使用を禁止したりできます。UEM を Intune に接続して、UEM 管理コンソール内から Intune アプリ保護ポリシーを管理できます。

すべてのデバイスタイプに対応する主な機能

機能	説明
デバイスのアクティブ化	ユーザーがデバイスをアクティブ化すると、そのデバイスを UEM および組織の環境に関連付け、デバイスの仕事用データにアクセスできるようにします。ユーザーは QR コードまたはメールアドレス、およびアクティベーションパスワードを使用してデバイスをアクティブ化できます。 ユーザー自身がデバイスをアクティブ化できるようにすることも、管理者がユーザーのデバイスをアクティブ化してからデバイスを割り振ることもできます。すべてのデバイスタイプをワイヤレスネットワーク経由でアクティブ化できます。

機能	説明
デバイスの管理	すべてのデバイスを表示し、単一の Web ベースのコンソールですべての管理タスクにアクセスできます。ユーザーアカウントごとに複数のデバイスを管理し、組織のデバイスインベントリを表示できます。デバイスでサポートされている場合は、次の操作を実行できます。 • デバイスのロック、デバイスまたは仕事用領域のパスワードの変更、またはデバイスからの情報の削除を行う • メールおよびカレンダーのサポートに Microsoft Exchange ActiveSync を使用して、デバイスを組織のメール環境に安全に接続する • Wi-Fi および VPN 設定を含め、デバイスを組織のネットワークに接続する方法を制御する • デバイスが組織のネットワークのドメインと Web サービスに自動的に認証されるように、デバイスのシングルサインオンを設定する • パスワード強度のルールの設定、カメラなどの機能の無効化など、デバイスの機能を制御する • アプリのバージョンおよびアプリを必須にするかオプションにするかの指定を含め、デバイス上のアプリの可用性を管理する • アプリストアで直接アプリを検索してデバイスに割り当てる • 証明書をデバイスにインストールし、オプションで自動証明書登録を許可するように SCEP を設定する • S/MIME または PGP を使用してメールセキュリティを強化する
ユーザー、アプリ、およびデバイスのグループの管理	グループは、ユーザー、アプリ、およびデバイスの管理を簡易化します。グループを使用して、類似ユーザーアカウントまたは類似デバイスに同じ設定を適用できます。異なるアプリグループを異なるユーザーグループに割り当てることができ、ユーザーは複数のグループのメンバーになることができます。
Microsoft Exchange ActiveSync にアクセス可能なデバイスの制御	ゲートキーピングを使用すると、UEM によって管理されているデバイスのみが、デバイス上の仕事用メールとその他の情報にアクセスできるように、また組織のセキュリティポリシーを満たすように設定できます。
デバイスを組織のリソースに接続する方法の制御	エンタープライズ接続プロファイルを使用して、デバイスのアプリが組織のリソースに接続する方法を制御できます。エンタープライズ接続が有効な場合は、デバイス管理や、メールサーバー、認証局、その他の Web サーバー、コンテンツサーバーなどのサードパーティアプリケーション用に、組織のファイアウォール内部からインターネットへのポートを複数開くことは避けます。エンタープライズ接続は、すべてのトラフィックを BlackBerry Infrastructure 経由でポート 3101 の UEM へ送信します。
仕事用アプリの管理	すべての管理されているデバイスで、仕事用アプリは、組織がユーザー向けに使用可能にしているアプリです。 アプリストアで直接アプリを検索してデバイスに割り当てることができます。アプリをデバイス上で必須にするかどうかを指定でき、仕事用アプリがデバイスにインストールされているかどうかを表示できます。仕事用アプリは、組織によって開発されたか、サードパーティの開発会社が組織で使用するために開発した独自アプリの場合もあります。

機能	説明
組織のデバイス要件の強制	コンプライアンスプロファイルを使用すると、脱獄やルート化されたデバイス、整合性に関するアラートがあるデバイス、デバイスに特定のアプリをインストールするように要求するデバイスなどに、仕事用データへのアクセスを許可しないといった、組織のセキュリティ要件を強制できます。管理者は、ユーザーに通知を送信して、組織の要件に適合するように指示できます。また、組織のリソースやアプリケーションへのアクセスの制限、仕事用データの削除、またはデバイスからの全データの削除を実行できます。
ユーザーへのメールの送信	管理コンソールから、1 つのメールを複数のユーザーに直接送信することができます。
.csv ファイルを使用した複数のユーザーアカウントの作成またはインポート	複数のユーザーアカウントを 1 つの .csv ファイルで UEM へインポートして、一度に多数のユーザーアカウントを作成またはインポートできます。要件に応じて、.csv ファイル内のユーザーアカウントのグループメンバーシップとアクティベーション設定も指定できます。
ユーザーおよびデバイス情報のレポートの表示	レポートダッシュボードには、UEM 環境の概要が表示されます。たとえば、組織内のデバイス数を通信事業者別に並べ替えて表示できます。ユーザーとデバイスの詳細の表示、情報の .csv ファイルへのエクスポート、およびダッシュボードからのユーザーアカウントへのアクセスを実行できます。
高可用性と障害復旧	BlackBerry データセンターは、世界中に存在し、高可用性と障害復旧を提供するように設計されています。BlackBerry データセンターは、組織のデータを自然災害から守るために役立つ、セキュリティ保護された建物への物理的なアクセス、監視、およびハードウェアの冗長性を提供します。 BlackBerry データセンターには、サービスに関する障害復旧計画があります。計画は、デバイスユーザーへの影響を最小限に抑え、ビジネスの継続性を保証するように設計されています。データおよびアプリは、消失を避けるためにほぼリアルタイムでバックアップされます。
証明書ベースの認証	証明書プロファイルを使用して証明書をデバイスへ送信できます。これらのプロファイルは、Microsoft Exchange ActiveSync、Wi-Fi 接続、または証明書に基づく認証を使用するデバイスへの VPN 接続へのアクセスを制限するために役立ちます
特定の機能とデバイス制御のライセンスの管理	ライセンスを管理し、使用率や有効期限などのライセンスの種類ごとの詳細情報を表示できます。組織が使用しているライセンスの種類によって、管理できるデバイスと機能が決まります。デバイスをアクティブ化するには、事前にライセンスをアクティブ化する必要があります。サービスを試用できるように無料トライアルを使用できます。

各デバイスタイプに対応する主な機能

iOS デバイス

機能	説明
デバイスのアクティベーション	Apple Configurator 2 を使用して、UEM でアクティブ化できるようにデバイスを準備できます。準備のできたデバイスは、BlackBerry UEM Client を使用せずにアクティブ化できます。
Web コンテンツのフィルタリング	Web コンテンツフィルタープロファイルを使用して、ユーザーがデバイスで表示できる Web サイトを制限できます。Web サイトを許可または制限したり、特定の Web サイトのみへのアクセスを許可したりするオプションを使用して、自動フィルタリングを有効にすることができます。
Apple VPP アカウントの UEM ドメインへのリンク	Volume Purchase Program（VPP）を使用すると、iOS アプリを一括で購入して配布できます。VPPアカウントに関連付けられた iOS アプリの購入したライセンスを配布できるように、Apple VPP アカウントを UEM ドメインにリンクできます。
Apple デバイス登録プログラム	UEM を Device Enrollment Program（DEP）と同期するために、UEM を設定して、Apple の DEP を使用できます。UEM を設定すると、管理コンソールを使用して、組織が DEP 用に購入した iOS デバイスのアクティベーションを管理できます。複数の DEP アカウントを使用することができます。複数の Apple DEP アカウントを 1 つの UEM ドメインにリンクできます。
アプリベースの PKI ソリューションのサポート	UEM は、BlackBerry Dynamics アプリの証明書を登録することができる Purebred などのアプリベースの PKI ソリューションをサポートしています。PKI アプリをデバイスにインストールし、BlackBerry Work および BlackBerry Access などの最新バージョンの BlackBerry Dynamics アプリで、PKI アプリを通じて登録された証明書を使用できるようになります。
カスタムペイロードプロファイル	カスタムペイロードプロファイルを使用して、既存の UEM ポリシーまたはプロファイルで制御されていない iOS デバイスの機能を制御できます。Apple を使用して Apple Configurator 設定プロファイルを作成して、UEM カスタムペイロードプロファイルに追加できます。カスタムペイロードプロファイルはユーザー、ユーザーグループ、およびデバイスグループに割り当てることができます。
BlackBerry Secure Gateway	BlackBerry Secure Gateway では、MDM コントロールのアクティベーションタイプで、iOS デバイスを BlackBerry Infrastructure および UEM を介して仕事用メールサーバーに接続することができます。BlackBerry Secure Gateway を使用する場合、これらのデバイスを使用するユーザーが組織の VPN または仕事用 Wi-Fi ネットワークに接続していないときに仕事用メールを受信できるようにするために、メールサーバーをファイアウォールの外側に公開する必要はありません。

機能	説明
BlackBerry Dynamics との統合	BlackBerry Dynamics プロファイルを使用して、iOS デバイスで、BlackBerry Work、BlackBerry Access、および BlackBerry Connect などの BlackBerry Dynamics の生産性向上アプリにアクセスできます。BlackBerry Dynamics プロファイルは、ユーザーアカウント、ユーザーグループ、またはデバイスグループに割り当てることができます。複数のデバイスで同じアプリにアクセスできます。 このプロファイルで、BlackBerry Dynamics がまだ有効になっていないユーザーに BlackBerry Dynamics を有効にできます。
Per-app VPN	iOS デバイスの per-app VPN を設定して、デバイス上でデータ送信に VPN を使用する必要があるアプリを指定できます。per-app VPN は、特定の仕事用トラフィック（たとえば、ファイアウォール内のアプリケーションサーバーまたは Web ページへのアクセス）のみが VPN を使用できるようにすることで、組織の VPN の負荷の軽減を促進します。この機能は、ユーザーのプライバシーもサポートし、VPN 経由で個人用トラフィックを送信しないため、個人用アプリの接続速度も高めます。 iOS デバイスでは、アプリまたはアプリグループをユーザー、ユーザーグループ、またはデバイスグループに割り当てるときに、アプリが VPN プロファイルに関連付けられます。
Apple アクティベーションロック	アクティベーションロック機能では、ユーザーが［iPhone を探す］をオフにしたり、デバイスを消去したり、デバイスを再アクティブ化して使用したりする前に、ユーザーの Apple ID とパスワードを必要とします。アクティベーションロックをバイパスして、COPE または COBO デバイスを別のユーザーに提供できます。
個人用アプリリスト	環境の iOS デバイスにあるユーザーの個人用領域にインストールされているアプリのリストを表示できます。ユーザー詳細ページでは、ユーザーの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確認できます。また、管理コンソールの個人用アプリページでは、ユーザーの個人用領域にインストールされているすべての個人用アプリのリストを確認できます。
アプリロックモードの実行	Apple Configurator 2 を使用して監視される iOS デバイスでは、アプリロックモードプロファイルを使用して、1 つのアプリのみが実行されるようにデバイスを制限できます。たとえば、トレーニング目的や販売時点管理（POS）のデモ用に、アクセスをシングルアプリに制限することができます。
監視対象の iOS デバイスの紛失モード	紛失モードでは、デバイスのロック、表示するメッセージの設定、紛失したデバイスの現在位置の表示ができます。監視対象の iOS デバイスで紛失モードを有効にすることができます。
IBM Notes Traveler サポート	BlackBerry Secure Gateway を介して iOS デバイスを IBM Notes Traveler に接続できます。
Face ID のサポート	UEM は、デバイス認証および BlackBerry Dynamics アプリを開くための Face ID をサポートします。

機能	説明
共有デバイスの管理	iOS デバイスを複数のユーザーで共有できるようにすることができます。ユーザーが共有デバイスをチェックアウトするために受け入れる必要がある使用条件をカスタマイズすることができます。デバイスはローカル認証を使用してチェックアウトできます。完了するとチェックインが可能になり、次のユーザーがデバイスを使用できるようになります。チェックアウトおよびチェックイン中、共有デバイスは UEM に管理されたままです。この機能は、次の設定で、監視対象のデバイス用に設計されています。 • アプリロックモード有効 • VPP アプリ割り当て済み
iPad	iPad デバイスは複数のユーザー間で共有できます。ユーザーが管理対象の Apple ID でサインインすると、そのユーザーのデータがロードされ、ユーザーは自分のメールアカウント、ファイル、iCloud フォトライブラリ、アプリデータなどにアクセスできます。

Android デバイス

機能	説明
Android Enterprise および Android Management デバイスの管理	Android Enterprise または Android Management を使用するように Android デバイスをアクティブ化できます。これらは Google が開発した機能で、Android デバイスのアプリとデータを管理および許可したい組織のセキュリティを強化します。 デバイスは、仕事用プロファイルのみを持つようアクティブ化することも、仕事用と個人用の両方のプロファイルを持つようアクティブ化することもできます。両方のプロファイルを完全に制御してデバイス全体を消去できるようにすることも、個人用プロファイルのプライバシーを許可し、デバイスからの仕事用データの消去のみできるようにすることも可能です。 Samsung デバイスでは、Android Enterprise でアクティブ化された場合、IT ポリシールールの拡張セットを含む追加の管理者オプションを利用できます。
仕事用および個人用 – Android Enterprise デバイスおよび Android Management デバイスのフルコントロールアクティベーション	このアクティベーションタイプでは、デバイス全体を管理できます。デバイス上に仕事用と個人用のデータを分離する仕事用プロファイルを作成しますが、組織はデバイスを完全に管理して、デバイスからすべてのデータを消去することができます。仕事用プロファイルのデータと個人用プロファイルのどちらのデータも暗号化され、パスワードなどの認証方式を使用して保護されます。

機能	説明
Knox MDM および Knox Workspace を使用したデバイスの管理	UEM では、Samsung MDM および Samsung Knox を使用して Samsung Knox Workspace デバイスを管理することもできます。Knox Workspace は、Samsung デバイス上に、暗号化されパスワードで保護されたコンテナを提供します。このコンテナには、仕事用のアプリやデータが含まれます。このコンテナは、ユーザーの個人用のアプリとデータを組織のアプリとデータから切り離し、Samsung が開発した強化されたセキュリティと管理機能を使用して、仕事用のアプリとデータを保護します。 デバイスをアクティベーションすると、デバイスが UEM をサポートするかどうかを Knox が自動的に確認します。UEM には、標準的な Android 管理機能に加えて、Knox をサポートするデバイス向けに次の機能が搭載されています。 • 一連の強化された IT ポリシールール • サイレントインストールおよびアンインストール、制限付きアプリのサイレントインストール、および制限付きアプリのインストールの禁止 • アプリロックモード サポートされているデバイスの詳細については、「互換性一覧表」を参照してください。
BlackBerry Dynamics との統合	BlackBerry Dynamics プロファイルを使用して、Android デバイスで、BlackBerry Dynamics、BlackBerry Work、および BlackBerry Access などの BlackBerry Connect の生産性向上アプリにアクセスできます。BlackBerry Dynamics プロファイルは、ユーザーアカウント、ユーザーグループ、またはデバイスグループに割り当てることができます。複数のデバイスで同じアプリにアクセスできます。 このプロファイルで、BlackBerry Dynamics がまだ有効になっていないユーザーに BlackBerry Dynamics を有効にできます。
Per-app VPN	仕事用プロファイルを持つ Android デバイスの per-app VPN を有効にして、許可リストに追加する特定の仕事用領域アプリに対して BlackBerry Secure Connect Plus の使用を制限することができます。
ゼロタッチ登録	UEM は、ゼロタッチ登録が有効になっているデバイスをサポートします。ゼロタッチ登録により、組織所有の Android デバイスをシームレスに導入することができ、大規模なデバイス導入を迅速、簡単、安全に実現します。ゼロタッチ登録により、IT 管理者はデバイスをオンラインで簡単に設定でき、管理する準備を整えて従業員にデバイスを渡すことができます。Google からの詳細情報については、「ゼロタッチ登録管理」および「ゼロタッチ登録の概要」を参照してください。ゼロタッチ登録では、デバイスの購入、ユーザーへのデバイスの割り当て、組織のポリシーの設定、ユーザーへのデバイスの導入などがわずか数手順で開始できます。販売代理店または通信事業者と協力して、ゼロタッチポータルにアクセスし、ポータルでデバイスを設定する必要があります。

機能	説明
アプリベースの PKI ソリューションのサポート	UEM は、Purebred アプリの証明書を登録することができる BlackBerry Dynamics などのアプリベースの PKI ソリューションをサポートしています。PKI アプリをデバイスにインストールし、BlackBerry Dynamics および BlackBerry Work などの最新バージョンの BlackBerry Access アプリで、PKI アプリを通じて登録された証明書を使用できるようになります。
SafetyNet および Play Integrity	管理者が Android SafetyNet または Google Play Integrity 認証を有効にすると、UEM は Android Enterprise、Samsung Knox、および組織の環境の MDM コントロールのアクティベーションタイプでアクティブ化された Android デバイスの完全性と整合性をテストするチャレンジを送信します。
BlackBerry Dynamics アプリへのセキュリティパッチレベルの強制	セキュリティパッチレベルの強制を BlackBerry Dynamics アプリに適用できます。セキュリティパッチレベルが満たされていない場合には、BlackBerry Dynamics アプリデータを削除するか、デバイスで BlackBerry Dynamics アプリを実行できないようにするか、デバイスで何も実行しないかを選択できます。
派生スマート認証情報	BlackBerry Dynamics アプリ、および Android Enterprise デバイスと Samsung Knox Workspace デバイスの仕事用領域内のアプリの署名、暗号化、認証に、Entrust IdentityGuard の派生スマート認証情報を使用します。
Android Enterprise デバイスの工場出荷時リセット保護	仕事用領域専用のアクティベーションタイプを使用してアクティブ化された、組織の Android Enterprise デバイスに対して、工場出荷時リセット保護プロファイルを設定できます。このプロファイルを使用すると、デバイスを工場出荷時の設定にリセットした後に、デバイスのロックを解除するのに使用されるユーザーアカウントや、サインインする必要がなくなるユーザーアカウントを指定できます。

Windows デバイス

機能	説明
Windows 10 デバイスのサポート	Windows 10 Mobile デバイス、Windows タブレット、コンピューターなどの Windows 10 デバイスを管理することができます。
Windows 10 デバイスのプロキシサポート	Windows 10 デバイス向けに、VPN および仕事用 Wi-Fi 接続を設定することができます。また、Windows 10 Mobile デバイス向けに、プロキシサーバーを Wi-Fi プロファイルの一部としてセットアップすることができます。
Per-app VPN	Windows 10 デバイスの per-app VPN を設定して、デバイス上でデータ送信に VPN を使用する必要があるアプリを指定できます。per-app VPN は、特定の仕事用トラフィック（たとえば、ファイアウォール内のアプリケーションサーバーまたは Web ページへのアクセス）のみが VPN を使用できるようにすることで、組織の VPN の負荷の軽減を促進します。この機能は、ユーザーのプライバシーもサポートし、VPN 経由で個人用トラフィックを送信しないため、個人用アプリの接続速度も高めます。

機能	説明
Windows 10 デバイス向けの Windows 情報保護	Windows 情報保護プロファイルを設定して、デバイス上の個人用データと仕事用データを分離し、保護された仕事用アプリ以外や組織外の人と仕事用データを共有できないようにすることで、不適切なデータ共有の慣行を監査することができます。仕事用ファイルを作成してアクセスするのに、保護された信頼性の高いアプリを指定できます。
ウイルス対策ベンダーの許可	コンプライアンスプロファイルでは、Windows デバイスの「ウイルス対策ステータス」ルールで、あらゆるベンダーのウイルス対策ソフトウェアを許可するか、「許可されたウイルス対策ベンダー」リストに追加したものだけを許可するかを選択できます。許可されていないベンダーからのウイルス対策ソフトウェアがデバイスで有効になっている場合、このルールが適用されます。
Entra ID 参加	UEM は Entra ID 参加をサポートし、Windows 10 デバイスの MDM 登録プロセスを簡素化できます。ユーザーは、Entra ID のユーザー名とパスワードを使用して、デバイスを UEM に登録することができます。Entra ID 参加は、Windows 10 の初期設定中に Windows 10 デバイスを UEM で自動的にアクティブ化できるようにする Windows AutoPilot をサポートするためにも必要です。

macOS デバイス

機能	説明
デバイス制御を使用した基本的なデバイス管理	ユーザーが macOS デバイスをアクティベーションすると、デバイスとユーザーが UEM で別々の存在として設定されます。独立した通信チャネルは、UEM、デバイス、UEM、およびユーザーアカウントの間で確立され、デバイスとユーザーの個別の管理を可能にします。
プロファイルとポリシー	一部のプロファイルは、ユーザーのみに割り当てられています（メールプロファイルなど）。一部のプロファイルは、デバイスのみに割り当てられています（プロキシプロファイルなど）。一部のプロファイルは、デバイスにて起用するかユーザーに適用するかを選択できます（Wi-Fi プロファイルなど）。 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。ユーザーは、BlackBerry UEM Self-Service を使用して macOS デバイスをアクティベーションします。

デバイスタイプ別サポートされている機能

このクイックリファレンスでは、iOS でサポートされる macOS、Android、Windows 10、および BlackBerry UEM デバイスの機能を比較します。

サポートされる OS 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。

デバイス機能

機能	iOS	macOS	Android	Windows 10
ワイヤレスアクティベーション	√	√	√	√
QR コードを使用したワイヤレスアクティベーション	√		√	
アクティベーションに必要なクライアントアプリ	√ [1]		√	
アクティベーションの使用契約書条項のカスタマイズ	√	√	√	√
機種に応じたアクティベーションの制限	√	√	√	
デバイスレポート（ハードウェアの詳細など）の表示とエクスポート	√	√	√	√
非監視対象デバイスの制限	√ [2]	√ [2]		

[1] DEP に登録された iOS デバイスでは、クライアントアプリをユーザーまたはグループに割り当てる必要があります。

[2] MDM コントロールまたは SIM ベースのライセンスを使用した 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のみ。

セキュリティ機能

機能	iOS	macOS	Android	Windows 10
仕事用と個人用のデータを分離する	√ [1]		√ [2]	√
個人用データのユーザープライバシーを保護する	√ [1]		√ [2]	
保存済み仕事用データを暗号化する	√ [1]		√ [2]	√
IT コマンドのデバイスへの送信	√	√	√	√
IT ポリシーを使用したデバイス機能の制御	√	√	√	√

機能	iOS	macOS	Android	Windows 10
アクティビティなしの時間が続いた場合に仕事用データを削除する	√ [1]		√ [1]	
パスワード要件を強制する	√	√	√	√
メディアカードの暗号化を強制する			√ [3]	
内部ストレージの暗号化を強制する			√	√

[1]BlackBerry Dynamics アプリが必要です。

[2] Samsung Knox Workspace、Android Enterprise、Android Management、または BlackBerry Dynamics のアプリが必要です。

[3]Samsung Knox デバイスのみ。

デバイスへの証明書の送信

機能	iOS	macOS	Android	Windows 10
CA 証明書プロファイル	√	√	√	√
SCEP プロファイル	√	√	√	√
共有証明書プロファイル	√	√	√	
ユーザー資格情報プロファイル	√	√	√	

デバイスで仕事用接続を管理する

機能	iOS	macOS	Android	Windows 10
BlackBerry 2FA プロファイル	√		√	
BlackBerry Dynamics 接続プロファイル	√	√	√	√
CalDAV プロファイル	√	√		
CardDAV プロファイル	√	√		
エンタープライズ接続				
BlackBerry Secure Connect Plus	√		√ [1]	

機能	iOS	macOS	Android	Windows 10
Exchange ActiveSync メールプロファイル	√	√	√ [2]	√
BlackBerry Secure Gateway	√			
IMAP/POP3 メールプロファイル	√	√	√	√
プロキシプロファイル	√	√	√	√
シングルサインオンプロファイル	√			
VPN プロファイル	√	√	√ [3]	√
Wi-Fi プロファイル	√	√	√	√

[1]Android Enterpriseデバイスおよび Knox Workspace デバイスのみ。

[2] EDM API をサポートする Motorola デバイス、Android Enterpriseデバイス、および Knox デバイスのみ。

[3]Knox Workspace デバイスのみ。

デバイスの組織の標準の管理

機能	iOS	macOS	Android	Windows 10
アクティベーションプロファイル	√	√	√	√
アプリロックモードプロファイル	√ [1]		√ [1]	√ [1]
BlackBerry Dynamics プロファイル	√	√	√	√
コンプライアンスプロファイル	√		√	
デバイスプロファイル	√		√	
Enterprise Management Agent プロファイル	√		√	√
位置情報サービスプロファイル	√		√	√

[1] 監視対象の iOS デバイス、MDM 制御 でアクティブ化されている Knox デバイス、Windows 10 Education、および Windows 10 Enterprise デバイスのみ。

紛失または盗難にあったデバイスの保護

機能	iOS	macOS	Android	Windows 10
デバイスパスワードを指定する			√	
デバイスのロック	√	√	√	
アクティベーションロック	√			
デバイスパスワードの指定とロック			√	
仕事用領域パスワードの指定とロック			√ [1]	
デバイスをロック解除してパスワードをクリア	√		√	
すべてのデバイスデータを削除	√	√	√ [2]	√
仕事用データのみを削除	√	√	√	√

[1]Android Enterprise デバイスのみ。

[2] EDM API をサポートしている Motorola デバイスでは、メディアカードの情報も削除されます。Knox Workspace デバイスでは、メディアカードにある情報の削除を選択できます。

ローミングの設定

機能	iOS	macOS	Android	Windows 10
ローミング時に自動同期を無効にする	√		√ [1]	
ローミング時にデータを無効にする	√ [2]		√ [3]	√

[1]Knox デバイスのみ。

[2] ネットワーク使用プロファイルでデータローミング設定を指定できます。

[3] Android Enterprise デバイスおよび Knox デバイスのみ。

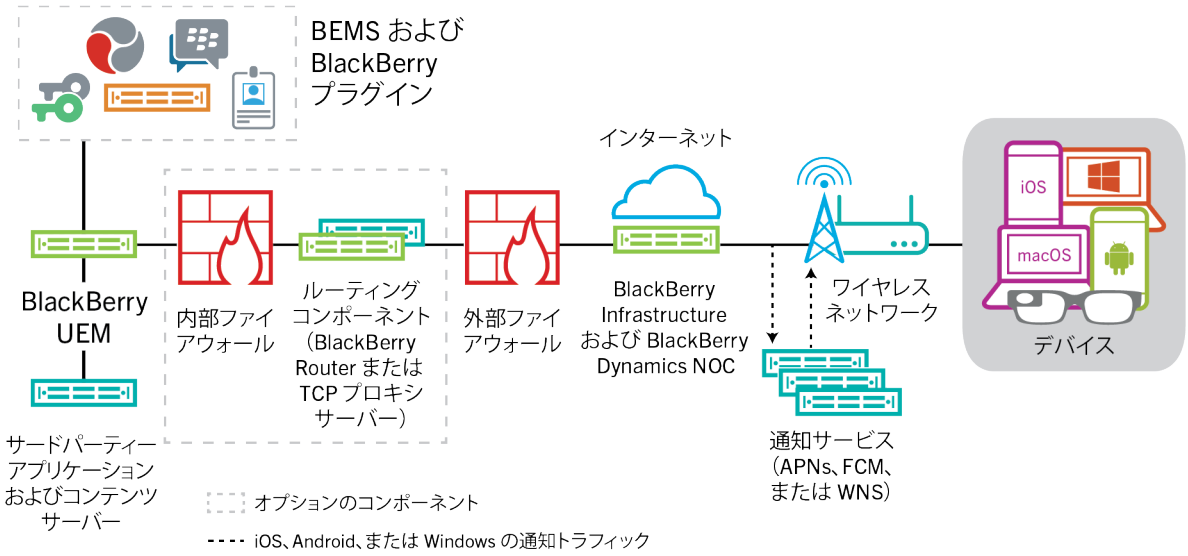
アプリの管理

機能	iOS	macOS	Android	Windows 10
ストアから一般のアプリを配布する（App Store、Google Play、Windows Store、BlackBerry World）	√		√	√
仕事用アプリのカタログを管理する	√		√	√
仕事用アプリのカタログをブランド化する	√			
アプリを制限する	√		√	
内部アプリを配布する	√		√	√
デバイスにアプリのショートカットを追加する	√	√	√	

BlackBerry UEM アーキテクチャ

BlackBerry UEM アーキテクチャは、組織のモバイルデバイスの管理を支援し、組織のメール、コンテンツサーバー、ユーザーデバイス間でデータを転送するための、セキュリティ保護されたリンクを提供します。

アーキテクチャ：**BlackBerry UEM** ソリューション

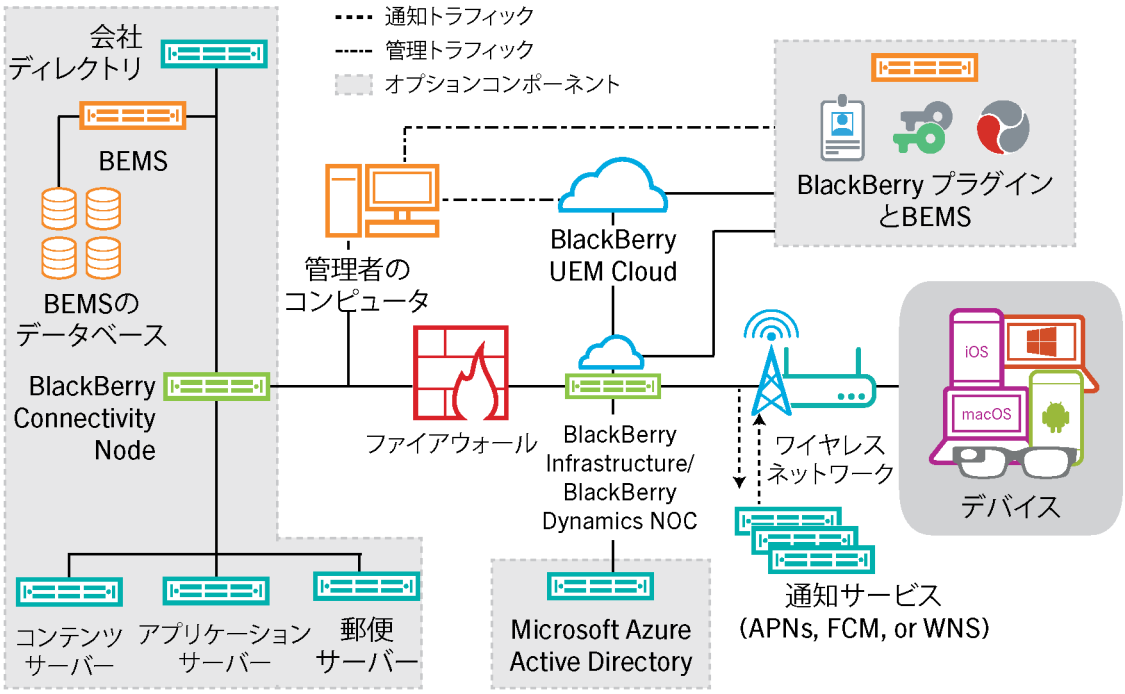


コンポーネント	説明
BlackBerry UEM	BlackBerry UEM は、統合エンドポイント管理ソリューションです。このソリューションでは、セキュリティと接続が統合されており、マルチプラットフォームデバイス、アプリケーション、およびコンテンツを包括的に管理することができます。
BlackBerry Infrastructure	BlackBerry Infrastructure は、複数の地域に分散されたグローバルなプライベートデータネットワークで、世界中の数千の組織と数百万のユーザー間のデータ転送を可能にし、データをセキュリティ保護します。BlackBerry サービスとエンドユ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。 UEM を使用する組織では、BlackBerry Infrastructure は、デバイスのアクティベーションのためにユーザー情報を登録し、ライセンス情報を検証し、強力な暗号化された相互認証に基づいて組織とすべてのユーザーの間に信頼されたパスを提供します。UEM は BlackBerry Infrastructure への常時接続を維持します。そのため、組織がユーザーにデータを送信するのに必要なのは、信頼された IP アドレスへの単一のアウトバウンド接続のみです。ファイアウォール外部のデバイス用に組織へのセキュリティ保護されたチャネルを提供するために、BlackBerry Infrastructure と UEM の間で伝送されるすべてのデータが認証され暗号化されます。

コンポーネント	説明
BlackBerry Dynamics NOC	BlackBerry Dynamics NOC とは、デバイス上の BlackBerry Dynamics アプリ、UEM、および BlackBerry Enterprise Mobility Server の間の通信を保護するネットワークオペレーションセンターです。
デバイス	BlackBerry UEM は、iOS、macOS、Android、および Windows の各デバイスをサポートします。
通知サービス	UEM は、通知をデバイスに送信して更新のために UEM と接続したり、組織のデバイスインベントリ用の情報をレポートしたりできます。これらの通知は BlackBerry Infrastructure に送信され、そこで適切な通知サービスを使用してデバイスへ送信されます。 • APN は、Apple および iOS デバイスに通知を送信するために、macOS が提供するサービスです。 • FCM は、Google が提供する、Android デバイスに通知を送信するためのサービスです。 • Windows プッシュ通知サービス（WNS）は、Microsoft が提供する、Windows デバイスに通知を送信するためのサービスです。
ルーティングコンポーネント	デフォルトでは、UEM はポート 3101 および 443 を介して BlackBerry Infrastructure への直接接続を確立するため、追加のルーティングコンポーネントをインストールする必要はありません。組織のセキュリティ標準によって、内部システムがインターネットへの直接接続を確立できないようにすることが要求される場合は、BlackBerry Router またはプロキシサーバーを使用できます。 BlackBerry Router は、UEM とすべてのデバイスの間の BlackBerry Infrastructure を経由する接続のプロキシサーバーとして機能します。BlackBerry Router は、認証なしの SOCKS v5 をサポートしています。 組織にすでに TCP プロキシサーバーがインストールされているか、ネットワーク要件を満たすために TCP プロキシサーバーが必要な場合は、BlackBerry Router の代わりに TCP プロキシサーバーを使用できます。TCP プロキシサーバー は、認証なしの SOCKS v5 をサポートしています。 BlackBerry UEM Core および BlackBerry Proxy は、HTTP プロキシサーバーを使用して、BlackBerry Dynamics NOC への接続をサポートします。
サードパーティーアプリケーションおよびコンテンツサーバー	会社のディレクトリ、メールサーバー、認証局などを含む、組織の環境内の追加のコンテンツサーバーおよびアプリケーションサーバー。
BlackBerry プラグインと BEMS	UEM は、BlackBerry Enterprise Identity、BlackBerry 2FA、および BlackBerry Workspaces などのその他の BlackBerry エンタープライズ製品と連携して、組織内で UEM 機能を拡張できるようにします。詳細については、「付随する製品およびサービス」を参照してください。 BlackBerry Enterprise Mobility Server では、BlackBerry Dynamics アプリとの間で仕事用データを送受信するサービスが利用できます。詳細については、BlackBerry Enterprise Mobility Server のドキュメントを参照してください。

アーキテクチャ：**BlackBerry UEM Cloud** ソリューション

BlackBerry UEM Cloud アーキテクチャは、クラウド環境における組織のモバイルデバイスの管理を支援し、組織のメール、コンテンツサーバー、ユーザーデバイス間でデータを転送するための、セキュリティ保護されたリンクを提供します。



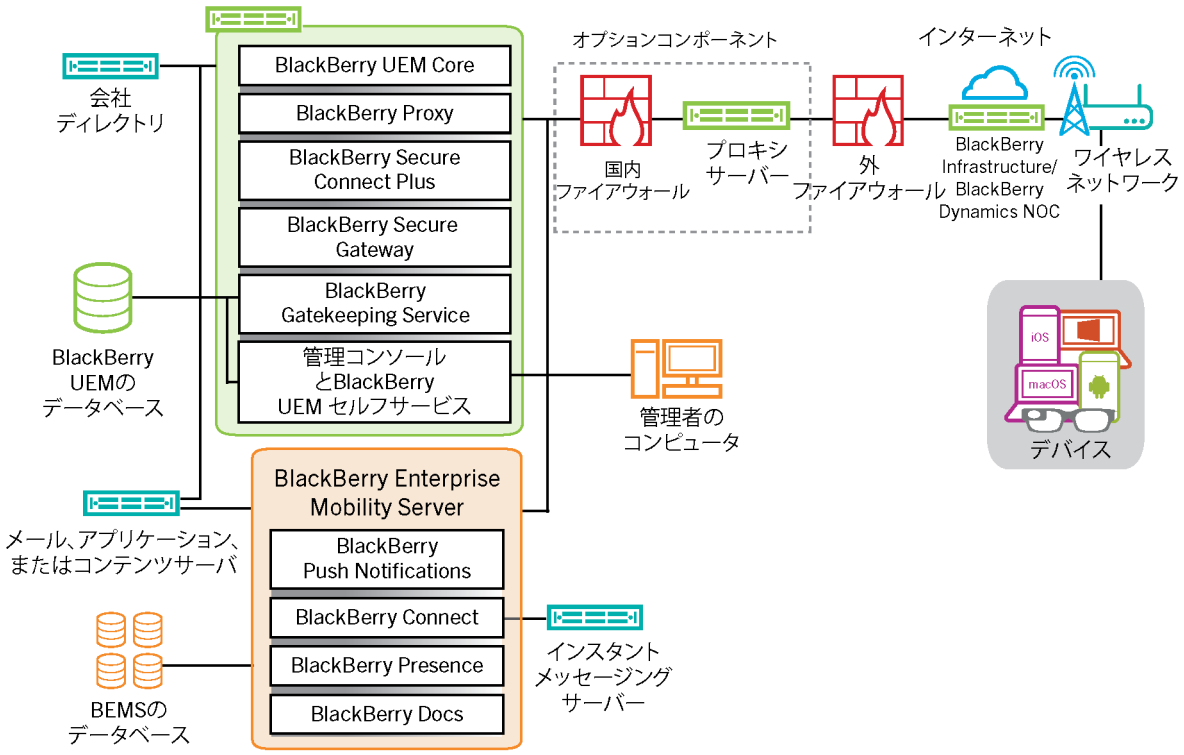
コンポーネント	説明
BlackBerry UEM Cloud	BlackBerry UEM Cloud は、組織の環境内で使用されているデバイスを管理者が管理することができるサービスです。
BlackBerry Infrastructure および BlackBerry Dynamics NOC	BlackBerry Infrastructure は、デバイスアクティベーションのユーザー情報を登録し、ライセンス情報を検証します。BlackBerry Secure Connect Plus または BlackBerry Secure Gateway を有効にすると、これらのサービスを使用する転送データは BlackBerry Infrastructure を経由します。 BlackBerry Dynamics NOC は、デバイス上の BlackBerry Dynamics アプリと BlackBerry Connectivity Node の一部としてファイアウォールの内側にインストールされた BlackBerry Proxy との通信を保護する、別個に配置された NOC です。
デバイス	BlackBerry UEM Cloud は、iOS、macOS、Android、および Windows デバイスをサポートします。

コンポーネント	説明
通知サービス	UEM Cloud は、通知をデバイスに送信し、更新のために UEM と接続したり、組織のデバイスインベントリ用の情報をレポートしたりできます。これらの通知は BlackBerry Infrastructure に送信され、適切な通知サービスを使用してデバイスへ送信されます。 • APN は、Apple および iOS デバイスに通知を送信するために、macOS が提供するサービスです。 • FCM は、Google が提供する、Android デバイスに通知を送信するためのサービスです。 • WNS は、Microsoft が提供する、Windows 10 デバイスに通知を送信するサービスです。
BlackBerry Connectivity Node	BlackBerry Connectivity Node は、組織のファイアウォール内にインストールするオプションコンポーネントです。これには UEM Cloud に機能を追加する以下のコンポーネントが含まれています。 • BlackBerry Cloud Connector コンポーネントは、UEM Cloud をファイアウォールの内側にある会社のディレクトリに接続して、基本属性の同期、検索機能、およびユーザー認証サービスを使用できるようにします。BlackBerry Connectivity Node をインストールせず、会社のディレクトリがファイアウォールの内側にある場合は、会社のディレクトリのユーザーアカウントを使用する代わりに、UEM Cloud でローカルユーザーアカウントを作成する必要があります。UEM Cloud を Microsoft Entra ID に接続するのには、BlackBerry Cloud Connector は必要ありません。 • BlackBerry Proxy は組織と BlackBerry Dynamics NOC の間で、セキュリティ保護された接続を維持します。この接続により、BlackBerry Dynamics アプリは、セキュリティで保護された状態でファイアウォール内にある組織のリソースと通信できるようになります。また BlackBerry Dynamics Direct Connect もサポートされているため、アプリデータの転送で BlackBerry Dynamics NOC をバイパスすることができます。 • BlackBerry Gatekeeping Service は、デバイスが UEM Cloud でアクティブになった時点でデバイスを許可リストに追加するように、Exchange ActiveSync にコマンドを送信します。組織のメールサーバーへの接続を試行する管理されていないデバイスは、UEM 管理コンソールを使用して、管理者によって調査、確認され、ブロックまたは許可されます。 • BlackBerry Secure Connect Plus は、デバイス上の仕事用アプリと組織のネットワークとの間にセキュリティ保護された IP トンネルを提供します。標準 IPv4（TCP および UDP）データをサポートする 1 つのトンネルが、BlackBerry Infrastructure を介して各デバイスに確立されます。 • BlackBerry Secure Gateway は、BlackBerry Infrastructure および UEM Cloud を介して、iOS デバイスを組織のメールサーバーに安全に接続します。
会社のディレクトリ	UEM Cloud は、BlackBerry Connectivity Node を使用して、組織の Microsoft Active Directory または ファイアウォールの内側にある会社の LDAP ディレクトリとの接続をサポートします。

コンポーネント	説明
Microsoft Entra ID（旧称 Azure AD）	Microsoft Entra ID はクラウドベースのディレクトリ管理サービスです。組織が Entra ID を使用している場合は、ファイアウォールの内側にある会社のディレクトリの代わりに、またはそれに加えて、Entra ID に接続できます。
コンテンツ、アプリケーション、およびメールサーバー	BlackBerry Secure Connect Plus を有効にしている場合、またはユーザーが BlackBerry Dynamics アプリを使用している場合は、サーバーとインターネット間の直接接続を開くことなく、デバイスを組織のサーバーに接続できます。サーバーとデバイス間で転送される仕事用データは、BlackBerry Secure Connect Plus および BlackBerry Infrastructure を経由して送信されます。BlackBerry Dynamics アプリのデータは、BlackBerry Proxy および BlackBerry Dynamics NOC を介して送信されます。 BlackBerry Secure Gateway は、BlackBerry Infrastructure および BlackBerry Connectivity Node を介して、組織のメールサーバーと iOS デバイス間を安全に接続します。
BlackBerry プラグインと BEMS	UEM は、BlackBerry Enterprise Identity、BlackBerry 2FA、および BlackBerry Workspaces などのその他の BlackBerry エンタープライズ製品と連携して、組織内で UEM 機能を拡張できるようにします。詳細については、「付随する製品およびサービス」を参照してください。 BlackBerry Enterprise Mobility Server では、BlackBerry Dynamics アプリとの間で仕事用データを送受信するサービスが利用できます。詳細については、BlackBerry Enterprise Mobility Server のドキュメントを参照してください。

オンプレミスの BlackBerry UEM のコンポーネント

この図は、すべてのコンポーネントが製品の最もシンプルな設定でいっしょにインストールされているとき、BlackBerry UEM コンポーネントが接続する方法を示しています。



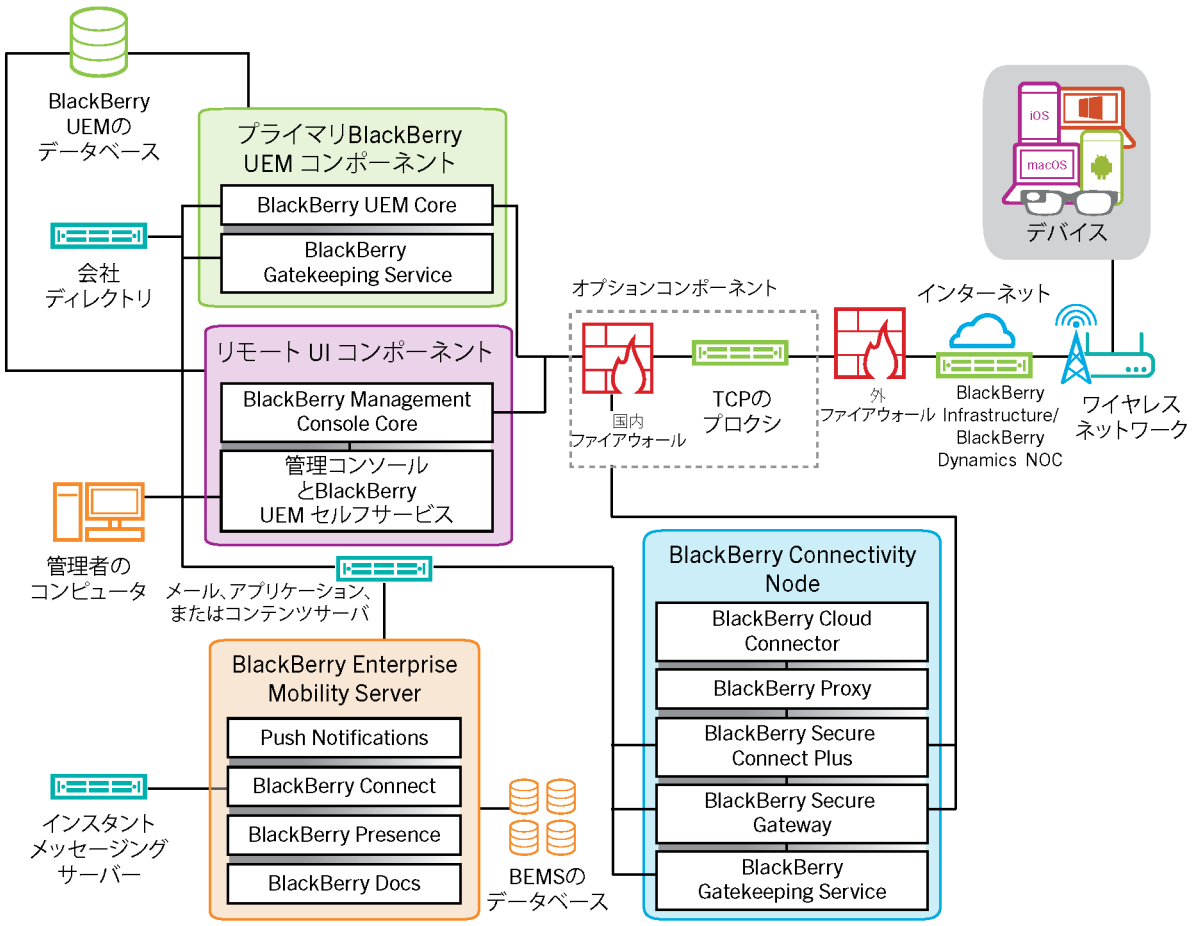
コンポーネント名	説明
BlackBerry UEM Core	BlackBerry UEM Core は UEM アーキテクチャの中心的なコンポーネントです。これは、以下を担当するいくつかのサブコンポーネントで構成されています。 • ログ、監視、レポート、および管理機能 • 認証および認証サービス • コマンド、IT ポリシー、およびプロファイルのスケジュールとデバイスへの送信 • ユーザー、ポリシー、およびその他の設定データの BlackBerry Dynamics アプリへの送信
BlackBerry Proxy	BlackBerry Proxy は、組織と BlackBerry Dynamics NOC との間のセキュリティ保護された接続を維持します。また、アプリデータが BlackBerry Dynamics をバイパスすることを許可する、BlackBerry Dynamics NOC Direct Connect をサポートします。

コンポーネント名	説明
BlackBerry Secure Connect Plus	BlackBerry Secure Connect Plus は、デバイス上の仕事用アプリと組織のネットワークとの間にセキュリティ保護された IP トンネルを提供します。標準 IPv4（TCP および UDP）データをサポートする 1 つのトンネルが、BlackBerry Infrastructure を介して各デバイスに確立されます。
BlackBerry Secure Gateway	BlackBerry Secure Gateway は、BlackBerry Infrastructure および UEM を介して、iOS デバイスと組織のメールサーバーとの間にセキュリティ保護された接続を提供します。
BlackBerry Gatekeeping Service	BlackBerry Gatekeeping Service は、デバイスが UEM でアクティブになった時点でデバイスを許可リストに追加するように、Exchange ActiveSync にコマンドを送信します。管理対象外のデバイスが組織のメールサーバーへの接続を試行すると、管理コンソールを使用して、管理者によって調査、確認され、ブロックされるか許可されます。
管理コンソールと BlackBerry UEM Self-Service	管理コンソールと BlackBerry UEM Self-Service は、UEM への管理者およびユーザーアクセス用の Web ベースのユーザーインターフェイスを提供します。 管理コンソールを使用して、システム設定、ユーザー、デバイス、およびアプリを管理します。 ユーザーは、UEM Self-Service を使用して、アクティベーションパスワードを設定して、パスワードを設定、デバイスをロック、デバイスデータを削除などのコマンドをデバイスに送信できます。
BlackBerry UEM データベース	UEM データベースは、UEM がデバイスと BlackBerry Dynamics アプリを管理するために使用するユーザーアカウント情報と設定情報が格納されたリレーショナルデータベースです。
BlackBerry Enterprise Mobility Server	BEMS は、BlackBerry Dynamics アプリとの間で仕事用データを送受信するために使用する複数のサービスを統合します。これには以下のサービスが含まれます。 • BlackBerry Push Notifications：iOS デバイスと Android デバイスからのプッシュ登録要求を受け入れ、Microsoft Exchange と通信して、ユーザーの仕事用メールアカウントの変更を監視します。 • BlackBerry Connect：安全なインスタントメッセージ、社内ディレクトリ検索、およびユーザープレゼンス情報を iOS デバイスおよび Android デバイスに提供します。 • BlackBerry Presence：リアルタイムプレゼンスステータスを BlackBerry Dynamics アプリに提供します。 • BlackBerry Docs：VPN ソフトウェア、ファイアウォールの再設定、またはデータの重複保存を必要とすることなく、BlackBerry Dynamics アプリユーザーが、仕事用ファイルサーバー、SharePoint、Box、および CMIS をサポートするコンテンツ管理システムを使用して、ドキュメントにアクセス、同期、および共有することができます。 BEMS データベースには、ユーザー、アプリ、ポリシー、および設定情報が保存されます。

コンポーネント名	説明
BlackBerry Router および/またはプロキシサーバー	デフォルトでは、UEM はポート 3101 および 443 を経由する BlackBerry Infrastructure への直接接続を作成します。組織のセキュリティ標準で、内部システムがインターネットに直接接続しないことが要求される場合、BlackBerry Router をインストールするか、認証なしで SOCKs v5 をサポートするサードパーティ製 TCP プロキシサーバーを使用することができます。 UEM Core および BlackBerry Proxy は、BlackBerry Dynamics NOC に接続するためにサードパーティ製 HTTP プロキシサーバーを使用することをサポートします。
BlackBerry Infrastructure および BlackBerry Dynamics NOC	BlackBerry Infrastructure は、デバイスのアクティベーションのためにユーザー情報を登録し、ライセンス情報を検証し、強力な暗号化された相互認証に基づいて、組織とすべてのユーザーの間に信頼されたパスを提供します。 BlackBerry Dynamics NOC は、デバイス上の BlackBerry Dynamics アプリと、UEM Core、BlackBerry Proxy、および BEMS との間のセキュリティ保護された通信を提供する、別個に配置された NOC です。

オンプレミスの BlackBerry UEM の分散インストール

この図は、BlackBerry Connectivity Node とユーザーインターフェイスが両方ともプライマリ UEM コンポーネントと別にインストールされている場合に、BlackBerry UEM コンポーネントがどのように接続されるかを示しています。



コンポーネント名	説明
プライマリ UEM コンポーネント	プライマリ UEM コンポーネントには、BlackBerry UEM Core と同じサーバーにインストールされているすべてのコンポーネントが含まれます。
BlackBerry UEM Core	UEM Core は UEM アーキテクチャの中心的なコンポーネントです。これは、以下を担当するいくつかのサブコンポーネントで構成されています。 • ログ、監視、レポート、および管理機能 • 認証および認証サービス • コマンド、IT ポリシー、およびプロファイルのスケジュールとデバイスへの送信 • ユーザー、ポリシー、およびその他の設定データをデバイス上の BlackBerry Dynamics アプリに送信。

コンポーネント名	説明
BlackBerry UEM データベース	UEM データベースは、UEM がデバイスと BlackBerry Dynamics アプリを管理するために使用するユーザーアカウント情報と設定情報が格納されたリレーショナルデータベースです。
BlackBerry Gatekeeping Service（プライマリ）	BlackBerry Gatekeeping Service は、デバイスが UEM でアクティブになった時点でデバイスを許可リストに追加するように、Exchange ActiveSync にコマンドを送信します。管理対象外のデバイスが組織のメールサーバーへの接続を試行すると、管理コンソールを通じて調査、確認され、ブロックされるか許可されます。
リモート UI コンポーネント	管理コンソールと BlackBerry UEM Self-Service は、他の UEM コンポーネントとは別にインストールできます。それらを別にインストールすると、BlackBerry Management Console Core のインスタンスもインストールされます。
BlackBerry Management Console Core	インストールされている場合、BlackBerry Management Console Core は管理コンソールと UEM Self-Service からの UI 要求のみを処理します。これにより、UEM Core の負荷が高い場合でも、これらのインターフェイスの応答性を確保できます。
管理コンソールと BlackBerry UEM Self-Service	管理コンソールと UEM Self-Service は、UEM への管理者およびユーザーアクセス用の Web ベースのユーザーインターフェイスを提供します。他のコンポーネントとは別にインストールすることができます。 管理コンソールを使用して、システム設定、ユーザー、デバイス、およびアプリを管理します。 ユーザーは、UEM Self-Service にアクセスし、アクティベーションパスワードを設定して、set password、lock device、delete device data などのコマンドをデバイスに送信できます。

コンポーネント名	説明
BlackBerry Connectivity Node	BlackBerry Connectivity Node は UEM Core とは異なるサーバー上の組織のドメインに UEM デバイス接続コンポーネントのインスタンスをインストールします。各 BlackBerry Connectivity Node には、以下のコンポーネントが含まれています。 • BlackBerry Cloud Connector：BlackBerry Connectivity Node コンポーネントが UEM Core と通信できるようにします。BlackBerry Cloud Connector と UEM Core の間の通信はすべて BlackBerry Infrastructure を通過します。 • BlackBerry Proxy：組織と BlackBerry Dynamics NOC との間のセキュリティ保護された接続を維持します。また、アプリデータが BlackBerry Dynamics をバイパスすることを許可する、BlackBerry Dynamics NOC Direct Connect をサポートします。 • BlackBerry Secure Connect Plus：デバイス上の仕事用アプリと組織のネットワークとの間にセキュリティ保護された IP トンネルを提供します。標準 IPv4（TCP および UDP）データをサポートする 1 つのトンネルが、BlackBerry Infrastructure を介して各デバイスに確立されます。 • BlackBerry Secure Gateway：BlackBerry Infrastructure および UEM を介して、iOS デバイスを組織のメールサーバーに安全に接続します。 • BlackBerry Gatekeeping Service：メールサーバーのゲートキーピングを管理します。プライマリ UEM コンポーネントにインストールされている BlackBerry Gatekeeping Service によってのみ、ゲートキーピングデータを管理する場合は、各 BlackBerry Connectivity Node の BlackBerry Gatekeeping Service を無効にすることができます。
BlackBerry Enterprise Mobility Server	BEMS は、BlackBerry Dynamics アプリとの間で仕事用データを送受信するために使用する複数のサービスを統合します。これには以下のサービスが含まれます。 • BlackBerry Push Notifications：iOS デバイスと Android デバイスからのプッシュ登録要求を受け入れ、Microsoft Exchange と通信して、ユーザーの仕事用メールアカウントの変更を監視します。 • BlackBerry Connect：安全なインスタントメッセージ、社内ディレクトリ検索、およびユーザープレゼンス情報を iOS デバイスおよび Android デバイスに提供します。 • BlackBerry Presence：リアルタイムプレゼンスステータスを BlackBerry Dynamics アプリに提供します。 • BlackBerry Docs：VPN ソフトウェア、ファイアウォールの再設定、またはデータの重複保存を必要とすることなく、BlackBerry Dynamics アプリユーザーが、仕事用ファイルサーバー、SharePoint、Box、および CMIS をサポートするコンテンツ管理システムを使用して、ドキュメントにアクセス、同期、および共有することができます。 BEMS データベースには、ユーザー、アプリ、ポリシー、および設定情報が保存されます。

コンポーネント名	説明
BlackBerry Infrastructure および BlackBerry Dynamics NOC	BlackBerry Infrastructure は、デバイスのアクティベーションのためにユーザー情報を登録し、ライセンス情報を検証し、強力な暗号化された相互認証に基づいて、組織とすべてのユーザーの間に信頼されたパスを提供します。 BlackBerry Dynamics NOC は、デバイス上の BlackBerry Dynamics アプリと、UEM Core、BlackBerry Proxy、および BEMS との間で安全に通信できるようにする、別個に配置された NOC です。

付随する製品およびサービス

このセクションでは、BlackBerry UEM で使用できる多くの付随する製品およびサービスについて説明します。

エンタープライズアプリおよび **BlackBerry Dynamics** アプリ

BlackBerry エンタープライズアプリ

BlackBerry では、管理者がデバイスにプッシュしたり、ユーザーがインストールして仕事用データへのアクセスや生産性の向上に役立てたりすることができるさまざまなエンタープライズアプリが利用できます。

コンポーネント	説明
BlackBerry UEM Client	BlackBerry UEM Client を使用すると、UEM で iOS デバイスおよび Android デバイスを管理できます。iOS デバイスまたは Android デバイスをアクティブ化して UEM でモバイルデバイスを管理するには、 UEM Client が必要です。最新のバージョンの UEM Client は、App Store または Google Play からダウンロードできます。それらのデバイスをアクティブ化した後、UEM Client を使用して次のことを実行できます。 • デバイスが組織の標準に準拠しているかどうかを確認する • デバイスに割り当てられているプロファイルを表示する • デバイスに割り当てられている IT ポリシールールを表示する • 仕事用アプリへアクセスする • BlackBerry Dynamics アプリのアクセスキーを作成する • BlackBerry 2FA で事前認証する • ソフトウェアの OTP コードへアクセスする • デバイスログファイルを取得してメールで送信する • デバイスを無効化する 詳細については、UEM Client のドキュメントを参照してください。
BBM Enterprise	BBM Enterprise は、組織内の BBM Enterprise ユーザーと組織内外の他の BBM ユーザーの間で送信される BBM メッセージにエンドツーエンドの暗号化層を追加します。BBM Enterprise は、iOS、Android、Windows、および macOS の各デバイスで使用きます。 BBM Enterprise は FIPS 140-2 検証済み暗号化ライブラリを使用します。暗号化キーを所有しているのは組織であり、他の誰であっても、BlackBerry でさえもアクセスできません。 ほとんどのデバイスで、UEM を使用して BBM Enterprise をユーザーに割り当てることができます。ユーザーが BBM Enterprise を使用できるようにすると、ユーザーは適切なアプリストアからアプリをダウンロードできるようになります。 詳細については、BBM Enterprise のドキュメントを参照してください。

BlackBerry Dynamics アプリ

BlackBerry Dynamics 生産性向上アプリは、仕事用データや生産性向上ツールへのアクセスをユーザーに提供します。

アプリ	説明
BlackBerry Work	BlackBerry Work アプリは仕事用メールへのセキュリティ保護されたアクセスを提供し、ユーザーは添付ファイルの表示および送信、カスタム連絡先通知の作成、メッセージの管理を行うことができます。 詳細については、BlackBerry Work のドキュメントを参照してください。
BlackBerry Access	BlackBerry Access は、ユーザーが仕事用イントラネットや Web アプリケーションにアクセスすることを可能にするセキュリティ保護されたブラウザーです。また、BlackBerry Access は、高レベルでのセキュリティとコンプライアンスを維持しながら、仕事用リソースへのアクセスや、高度な HTML5 アプリの構築および展開を可能にします。 詳細については、BlackBerry Access のドキュメントを参照してください。
BlackBerry Connect	BlackBerry Connect は、ユーザーのデバイス上で使いやすいインターフェイスを提供し、セキュリティ保護されたインスタントメッセージングを使用した通信とコラボレーション、会社のディレクトリの検索、ユーザープレゼンスを可能にします。 詳細については、BlackBery Connect のドキュメントを参照してください。
BlackBerry Tasks	BlackBerry Tasks を使用すると、ユーザーは Microsoft Exchange と同期されるタスクを作成、編集、および管理できます。 詳細については、BlackBerry Tasks のドキュメントを参照してください。
BlackBerry Notes	BlackBerry Notes を使用すると、ユーザーは Microsoft Exchange と同期されるメモを選択したモバイルデバイスで作成、編集、および管理できます。 詳細については、BlackBerry Notes のドキュメントを参照してください。
BlackBerry BRIDGE	BlackBerry BRIDGE は BlackBerry Dynamics で有効になっている Microsoft Intune アプリです。iOS デバイスおよび Android デバイスの BlackBerry Dynamics で、Microsoft Word、Microsoft PowerPoint、および Microsoft Excel などの Intune で管理された Microsoft アプリを使用することで、ドキュメントを安全に表示、編集、保存することができます。 詳細については、BlackBerry Bridge のドキュメントを参照してください。

また、BlackBerry の多くのサードパーティアプリケーションパートナーの 1 社が開発した BlackBerry Dynamics アプリも使用できます。一般的に利用できるアプリの詳細リストについては、BlackBerry Marketplace for Enterprise Software にアクセスしてください。

また、組織は BlackBerry Dynamics SDK を使用してカスタム BlackBerry Dynamics アプリを開発することもできます。詳細については、BlackBerry Dynamics SDK のドキュメントを参照してください。

BlackBerry Enterprise Identity の利点

BlackBerry Enterprise Identity によって、ユーザーは iOS、Android、および従来のコンピューティングプラットフォームなど、あらゆるデバイスからクラウドアプリケーションに簡単にアクセスできます。この機能は BlackBerry UEM と緊密に統合されており、業界をリードする EMM とすべてのクラウドサービスの権限と制御を統合しています。

BlackBerry Enterprise Identity では、Microsoft 365、Google Workspace、BlackBerry Workspaces をはじめ、他にも多数のクラウドサービスでシングルサインオン（SSO）を利用できます。シングルサインオンを使用すると、ユーザーは何回もログインを行ったり、複数のパスワードを記憶したりする必要がありません。管理者は、Enterprise Identity にカスタムサービスを追加して、ユーザーが内部アプリケーションにアクセスできるようにすることもできます。

管理者は、UEM 管理コンソールを使用して、サービスの追加、ユーザーの管理、および管理者の追加と管理を行います。UEM との統合により、ユーザーの管理や、デバイスからクラウドアプリケーションやサービスへのアクセス権の付与も容易になります。クラウドサービスおよびモバイルアプリのバイナリをまとめてバンドルし、ユーザーおよびグループに割り当てることもできます。

詳細については、BlackBerry Enterprise Identity のドキュメントを参照してください。

BlackBerry 2FA の利点

BlackBerry 2FA では、2 要素認証を利用して、組織のリソースにアクセスすることができます。iOS デバイスおよび Android デバイスを第 2 の認証要素として使用でき、ユーザーが組織のリソースに接続しようとすると簡単な確認プロンプトが表示されるようになります。

モバイルデバイスを持っていないユーザーや、持っているモバイルデバイスにリアルタイムの BlackBerry 2FA をサポートするのに十分な接続性がないユーザーには、標準に準拠したワンタイムパスワード（OTP）トークンを発行できます。最初の認証要素はユーザーのディレクトリパスワードで、第 2 の認証要素はトークンの画面に表示される動的コードです。

BlackBerry 2FA は UEM 管理コンソールで管理します。BlackBerry 2FA は BlackBerry Enterprise Identity にも統合されています。BlackBerry 2FA を使用して、Enterprise Identity でアクセスを管理するリソースに第 2 の認証要素を提供できます。

詳細については、BlackBerry 2FA のドキュメントを参照してください。

BlackBerry Workspaces の利点

BlackBerry Workspaces は、ユーザーが複数のデバイス間でファイルやフォルダーに安全にアクセス、同期、編集、共有できるようにするエンタープライズファイル管理プラットフォームです。BlackBerry Workspaces は、デジタル著作権管理のセキュリティをすべてのファイルに組み込むことで、データの損失や盗難のリスクを抑えます。これにより、コンテンツがダウンロードされ、他のユーザーと共有された後でも、コンテンツの安全性を確保し、管理の範囲内に収めることができます。ファイルを安全に保管し、管理を維持しながらデータを転送できる機能により、従業員も IT 担当者も安心してデータを共有し、ドキュメントを保護することができます。

ユーザーは、Web ブラウザーから、また、Windows と macOS コンピューターおよび iOS デバイスと Android デバイスのアプリから BlackBerry Workspaces にアクセスできます。コンテンツは、ユーザーがオンラインになっているときはすべてのユーザーのデバイスで同期されるため、ユーザーは任意のデバイスからファイルを管理、

表示、作成、編集、および注釈付けできます。BlackBerry UEM 用の Workspaces のプラグインを使用して、UEM 管理コンソールに Workspaces 管理を統合できます。

組織が BlackBerry Enterprise Identity も実装している場合は、Enterprise Identity を使用して Workspaces へのユーザーの権限を管理できます。

詳細については、BlackBerry Workspaces のドキュメントを参照してください。

BlackBerry UEM Notifications の利点

BlackBerry UEM Notifications により、管理者は BlackBerry AtHoc のネットワーク化された緊急コミュニケーションシステムを活用して、UEM 管理コンソールから重要なメッセージや通知をユーザーやグループに送信できます。

UEM Notifications により、管理者は UEM 管理コンソール内でデバイスと通知を管理できるため、複数のシステム間でユーザーの連絡先情報を管理および調整したり、外部システムのアクセスの問題に対処したりする必要はありません。UEM Notifications では、Microsoft Active Directory の同期を使用して連絡先情報を活用します。また UEM Notifications では、テキスト読み上げ音声通話、SMS、メールなど、柔軟な配信オプションを提供しており、ユーザーが希望する手段でアラートを受信できるため、アクションとコンプライアンスの可能性が高まります。

管理者は、配信方法ごとの詳細なメッセージステータスなど、送信された通知を追跡および管理できます。UEM Notifications では、FedRAMP の承認を受けた配信サービスを使用しており、すべての送信メッセージとそのステータスの包括的なレポートを利用できます。

BlackBerry UEM Notifications は、オンプレミスの BlackBerry UEM の場合のみ使用可能です。

詳細については、UEM Notifications のドキュメントを参照してください。

BlackBerry Enterprise SDK

BlackBerry は、組織が BlackBerry ソリューションをカスタマイズしたり拡張したりするのに役立つ SDK オプションを提供しています。

SDK	説明
BlackBerry Dynamics SDK	BlackBerry Dynamics SDK には、開発者がアプリをセキュリティ保護、展開、および管理する方法を学ぶことなく、有用な生産性アプリの構築に集中できる強力なツールセットが用意されています。開発者は、BlackBerry Dynamics SDK を使用して、セキュリティ保護された通信、アプリ間データ交換、プレゼンス、プッシュ、ディレクトリ検索、シングルサインオン認証、ID およびアクセス管理などの有用なサービスを活用する、すべての主要プラットフォーム向けのアプリを開発できます。 詳細については、BlackBerry Dynamics SDK のドキュメントを参照してください。

SDK	説明
BlackBerry Web Services	BlackBerry Web Services は、SOAP および REST Web サービスの集合で、開発者はこれを使用して、組織の UEM ドメイン、ユーザーアカウント、およびサポートされているすべてのデバイスを管理するアプリケーションを作成できます。BlackBerry Web Services を使用すると、管理者が通常管理コンソールを使用して実行する多くのタスクを自動化できます。たとえば、ユーザーアカウントの作成プロセスを自動化するアプリケーション、ユーザーを複数のグループに追加するアプリケーション、およびユーザーのデバイスを管理するアプリケーションを作成できます。 詳細については、BlackBerry Web Services のドキュメントを参照してください。
BlackBerry Workspaces Android SDK	開発者は BlackBerry Workspaces Android SDK を使用して、ユーザーが BlackBerry Workspaces で保護されたファイルを操作できるアプリケーションを開発できます。 詳細については、BlackBerry Workspaces Android SDK のドキュメントを参照してください。

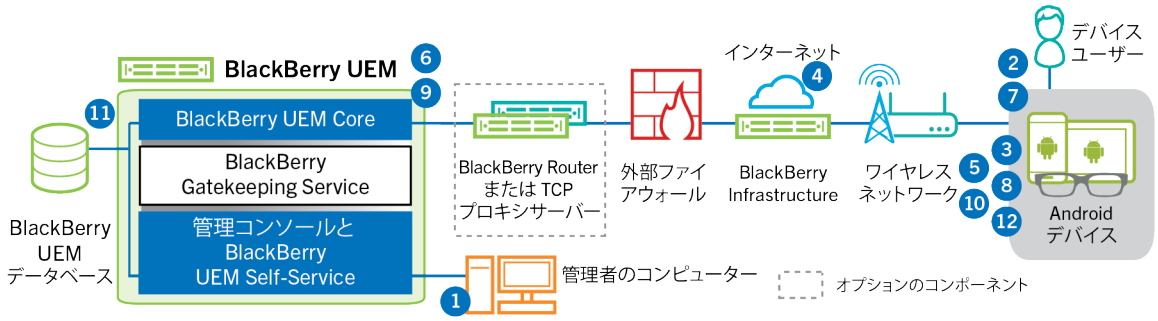
BlackBerry で使用可能なすべての開発者ツールの入手および使用の詳細については、BlackBerry Developers サイトを参照してください。

データフロー：デバイスと BlackBerry Dynamics アプリのアクティブ化

ユーザーが BlackBerry UEM でデバイスをアクティブ化すると、デバイスは UEM に関連付けられます。これにより、管理者がデバイスを管理したり、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なります。デバイスアクティベーションによって、すべてのデータに対するフルコントロール権限から仕事用データのみの特定の制御権限まで、デバイス上の仕事用データと個人用データを制御できる度合いは異なります。アクティベーションタイプおよびデバイスをアクティブ化する方法の詳細については、管理関連の資料の「デバイスのアクティベーション」を参照してください。

このセクションでは、デバイスまたは BlackBerry Dynamics アプリをアクティブ化したときに、データが組織の UEM 環境をどのように移動するかを詳細に示すデータフローを説明します。

データフロー：管理対象 Google Play アカウントを使用して Android Enterprise 仕事用と個人用 - ユーザーのプライバシー デバイスをアクティブ化する



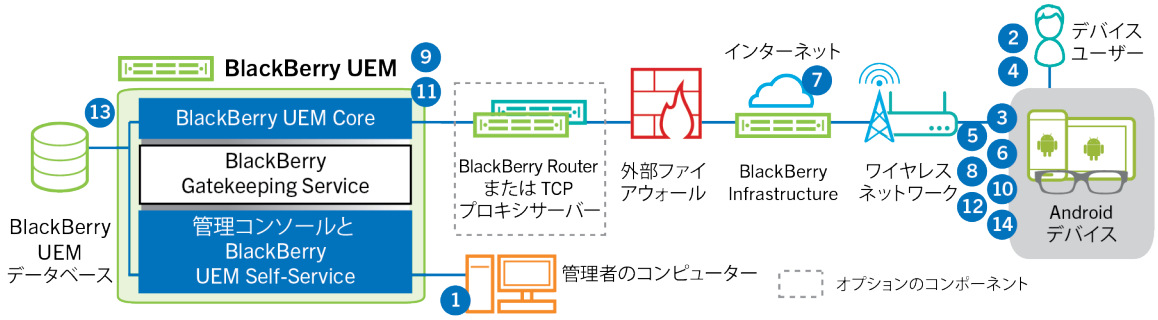
このデータフローは、BlackBerry UEM に Google Play アカウントの管理を許可する場合に適用されます。

1. 次の操作を実行します。
   a. ユーザーをローカルユーザーアカウントとして、または会社のディレクトリから取得したアカウント情報を使用して、BlackBerry UEM に追加します。
   b. 「仕事用と個人用 - ユーザーのプライバシー 」アクティベーションタイプがユーザーに割り当てられていることを確認します。
   c. 次のいずれかのオプションを使用してユーザーにアクティベーションの詳細情報を提供する
      - デバイスアクティベーションパスワードと、オプションとして、QR Code を自動生成して、アクティベーションの手順を記載したメールを送信する
      - デバイスアクティベーションパスワードを設定して、ユーザー名とパスワードをユーザーに直接通知するか、メールで通知する
      - デバイスアクティベーションパスワードを設定せずに、ユーザーが自身でアクティベーションパスワードを設定し BlackBerry UEM Self-Service を表示できるように、QR Code アドレスをユーザーに通知する
2. ユーザーは、BlackBerry UEM Client から Google Play をダウンロードして、デバイスにインストールします。インストール後に、ユーザーは BlackBerry UEM Client を開き、メールアドレスとアクティベーションパスワードを入力するか QR Code をスキャンします。

3. デバイスの BlackBerry UEM Client が次の処理を実行します。
   a. BlackBerry Infrastructure への接続を確立する
   b. BlackBerry Infrastructure にアクティベーション情報を送信する
4. BlackBerry Infrastructure は、次の処理を実行します。
   a. ユーザーが有効な登録済みユーザーであることを確認します
   b. ユーザーの BlackBerry UEM アドレスを取得する
   c. BlackBerry UEM Client にアドレスを送信する
5. BlackBerry UEM Client は、ポート 443 経由で HTTP CONNECT コールを使用して BlackBerry UEM との接続を確立し、BlackBerry UEM にアクティベーション要求を送信します。アクティベーション要求には、ユーザー名、パスワード、デバイスのオペレーティングシステム、および固有のデバイス ID が含まれます。
6. BlackBerry UEM は次の操作を実行します。
   a. ユーザーアカウントに割り当てられたアクティベーションタイプを決定します
   b. Google に接続し、管理対象の Google Play ユーザーを作成します
   c. デバイスインスタンスを作成します
   d. デバイスインスタンスを、指定されたユーザーアカウントに関連付けます
   e. 登録セッション ID を HTTP セッションに追加します
   f. ユーザーの管理対象 Google Play アカウント情報と正常な認証メッセージをデバイスに送信します
7. デバイスが暗号化されていない場合は、デバイスの暗号化を求めるプロンプトが表示されます。
8. BlackBerry UEM Client は、次の処理を実行します。
   a. Google に接続してユーザーを確認します
   b. デバイス上に仕事用プロファイルを作成します
   c. BlackBerry UEM から受信した情報を使用して CSR を作成し、HTTPS を介してクライアント証明書リクエストを BlackBerry UEM へ送信します。
9. BlackBerry UEM は次の操作を実行します。
   a. クライアント証明書要求を HTTP セッションの登録セッション ID と照合して検証します
   b. ルート証明書を使用してクライアント証明書要求に署名します
   c. 署名されたクライアント証明書とルート証明書を BlackBerry UEM Client に返送する

   BlackBerry UEM Client と BlackBerry UEM の間に相互に認証された TLS セッションが確立されます。
10. BlackBerry UEM Client は、すべての設定情報を要求し、デバイスおよびソフトウェア情報を BlackBerry UEM に送信します。
11. BlackBerry UEM は、デバイス情報をデータベースに保存し、要求された設定情報をデバイスに送信します。
12. デバイスは、設定情報を受信し適用したことを示す確認応答を BlackBerry UEM に送信します。アクティベーションプロセスは完了です。

データフロー：管理対象 Google Play アカウントを使用して Android Enterprise 仕事用と個人用 - フルコントロール デバイスをアクティブ化する



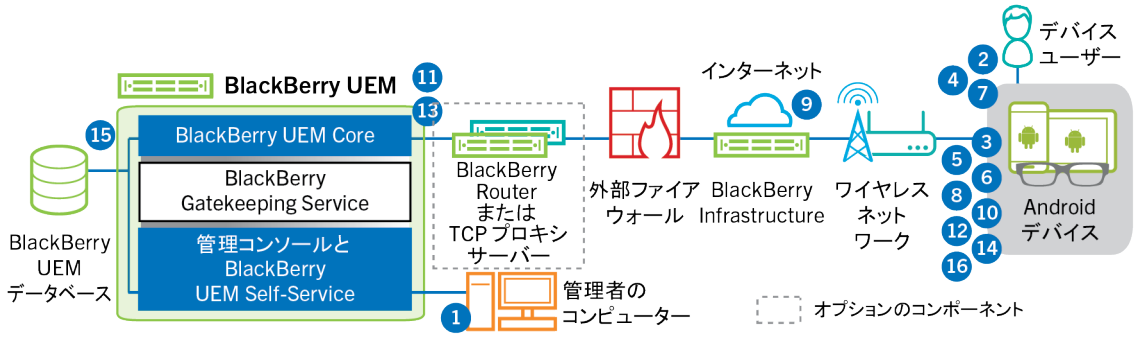
このデータフローは、BlackBerry UEM に Google Play アカウントの管理を許可する場合に適用されます。

1. 次の操作を実行します。
   a. ユーザーをローカルユーザーアカウントとして、または会社のディレクトリから取得したアカウント情報を使用して、BlackBerry UEM に追加します。
   b. 「仕事用と個人用 - フルコントロール 」アクティベーションタイプがユーザーに割り当てられていることを確認します。
   c. アクティベーション QR コードにアクティベーションパスワードと BlackBerry UEM Client をダウンロードする場所を含めることを許可します。
2. ユーザーは、デバイスを工場出荷時のデフォルトの状態にリセットします。
3. デバイスが再起動し、ようこそ画面またはスタート画面が表示されます。
4. ユーザーは次の操作を実行します。
   a. コンピューターまたは別のデバイスで受信したアクティベーションメールを開きます
   b. デバイス画面を 7 回タップして QR コードリーダーを開きます
   c. デバイスを Wi-Fi ネットワークに接続します
   d. 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
5. デバイスが次の処理を実行します。
   a. デバイスの暗号化を求めるプロンプトを表示して、再起動します
   b. QR コードで指定されたダウンロード場所から UEM Client をダウンロードしてインストールします
6. UEM Client は、次の処理を実行します。
   a. BlackBerry Infrastructure への接続を確立する
   b. BlackBerry Infrastructure にアクティベーション情報を送信する
7. BlackBerry Infrastructure は、次の処理を実行します。
   a. ユーザーが有効な登録済みユーザーであることを確認します
   b. ユーザーの BlackBerry UEM サーバーアドレスを取得します。
   c. UEM Client にサーバーアドレスを送信します
8. UEM Client は、ポート 443 経由で HTTP CONNECT コールを使用して BlackBerry UEM との接続を確立し、BlackBerry UEM にアクティベーション要求を送信します。アクティベーション要求には、ユーザー名、パスワード、デバイスのオペレーティングシステム、および固有のデバイス ID が含まれます。

9. BlackBerry UEM は次の操作を実行します。
   a. ユーザーアカウントに割り当てられたアクティベーションタイプを決定します
   b. Google に接続し、管理対象の Google Play ユーザーを作成します
   c. デバイスインスタンスを作成します
   d. デバイスインスタンスを、指定されたユーザーアカウントに関連付けます
   e. 登録セッション ID を HTTP セッションに追加します
   f. ユーザーの管理対象 Google Play アカウント情報と正常な認証メッセージをデバイスに送信します
10. UEM Client は、次の処理を実行します。
   a. Google に接続してユーザーを確認します
   b. デバイス上に仕事用プロファイルを作成します
   c. BlackBerry UEM から受信した情報を使用して CSR を作成し、HTTPS を介してクライアント証明書リクエストを BlackBerry UEM へ送信します。
11. BlackBerry UEM は次の操作を実行します。
   a. クライアント証明書要求を HTTP セッションの登録セッション ID と照合して検証します
   b. ルート証明書を使用してクライアント証明書要求に署名します
   c. 署名されたクライアント証明書とルート証明書を UEM Client に返送する

   UEM Client と BlackBerry UEM の間に相互に認証された TLS セッションが確立されます。
12. UEM Client は、すべての設定情報を要求し、デバイスおよびソフトウェア情報を BlackBerry UEM に送信します。
13. BlackBerry UEM は、デバイス情報をデータベースに保存し、要求された設定情報をデバイスに送信します。
14. デバイスは、設定情報を受信し適用したことを示す確認応答を BlackBerry UEM に送信します。アクティベーションプロセスは完了です。

データフロー：管理対象 Google Play アカウントを使用して Android Enterprise 仕事用領域のみ デバイスをアクティブ化する



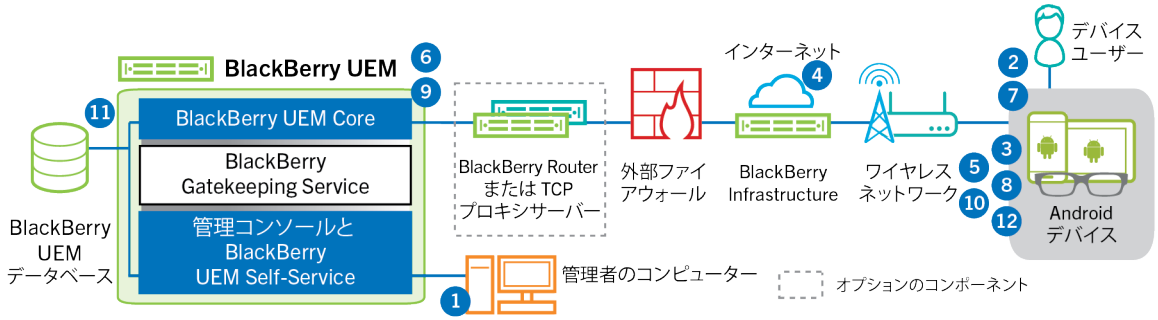
このデータフローは、BlackBerry UEM に Google Play アカウントの管理を許可する場合に適用されます。

1. 次の操作を実行します。
   a. ユーザーをローカルユーザーアカウントとして、または会社のディレクトリから取得したアカウント情報を使用して、BlackBerry UEM に追加します。
   b. 「仕事用領域のみ」アクティベーションタイプがユーザーに割り当てられていることを確認します。
   c. ユーザーのアクティベーションパスワードを設定します。

2. ユーザーは、デバイスを工場出荷時のデフォルトの状態にリセットします。
3. デバイスが再起動し、Wi-Fi ネットワークを選択し、アカウントを追加するように求めるプロンプトが表示されます。
4. ユーザーは、Google 資格情報を入力します。
5. デバイスが次の処理を実行します。
   a. デバイスが暗号化されていない場合は、デバイスを暗号化するように求めるプロンプトを表示して、再起動します。
   b. BlackBerry UEM Client を Google Play からダウンロードして、インストールします。
6. デバイス上の BlackBerry UEM Client により、メールアドレスとアクティベーションパスワードを入力するように求めるプロンプトが表示されます。
7. ユーザーは、メールアドレスとアクティベーションパスワードを入力するか、または QR Code をスキャンします。
8. BlackBerry UEM Client は、次の処理を実行します。
   a. BlackBerry Infrastructure への接続を確立する
   b. BlackBerry Infrastructure にアクティベーション情報を送信する
9. BlackBerry Infrastructure は、次の処理を実行します。
   a. ユーザーが有効な登録済みユーザーであることを確認します
   b. ユーザーの BlackBerry UEM サーバーアドレスを取得します。
   c. BlackBerry UEM Client にサーバーアドレスを送信します
10. BlackBerry UEM Client は、ポート 443 経由で HTTP CONNECT コールを使用して BlackBerry UEM との接続を確立し、BlackBerry UEM にアクティベーション要求を送信します。アクティベーション要求には、ユーザー名、パスワード、デバイスのオペレーティングシステム、および固有のデバイス ID が含まれます。
11. BlackBerry UEM は次の操作を実行します。
   a. ユーザーアカウントに割り当てられたアクティベーションタイプを決定します
   b. Google に接続し、管理対象の Google Play ユーザーを作成します
   c. デバイスインスタンスを作成します
   d. デバイスインスタンスを、指定されたユーザーアカウントに関連付けます
   e. 登録セッション ID を HTTP セッションに追加します
   f. ユーザーの管理対象 Google Play アカウント情報と正常な認証メッセージをデバイスに送信します
12. BlackBerry UEM Client は、次の処理を実行します。
   a. Google に接続してユーザーを確認します
   b. BlackBerry UEM から受信した情報を使用して CSR を作成し、HTTPS を介してクライアント証明書リクエストを BlackBerry UEM へ送信します。
13. BlackBerry UEM は次の操作を実行します。
   a. クライアント証明書要求を HTTP セッションの登録セッション ID と照合して検証します
   b. ルート証明書を使用してクライアント証明書要求に署名します
   c. 署名されたクライアント証明書とルート証明書を BlackBerry UEM Client に返送する

   BlackBerry UEM Client と BlackBerry UEM の間に相互に認証された TLS セッションが確立されます。
14. BlackBerry UEM Client は、すべての設定情報を要求し、デバイスおよびソフトウェア情報を BlackBerry UEM に送信します。
15. BlackBerry UEM は、デバイス情報をデータベースに保存し、要求された設定情報をデバイスに送信します。
16. デバイスは、設定情報を受信し適用したことを示す確認応答を BlackBerry UEM に送信します。アクティベーションプロセスは完了です。

データフロー：Google ドメインで Android Enterprise 仕事用と個人用 - ユーザーのプライバシー デバイスをアクティブ化する



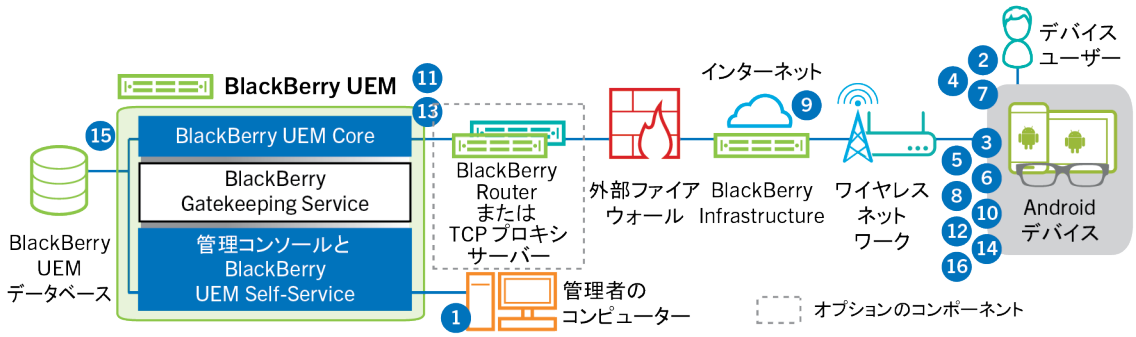
このデータフローは、BlackBerry UEM が Google Cloud または Google Workspace ドメインに接続されている場合に適用されます。

1. 次の操作を実行します。
   a. ユーザーの仕事用メールアドレスに関連付けられている Google アカウントを、ユーザーが所有していることを確認します。BlackBerry UEM を設定して、アクティベーションプロセス中にユーザーに Google アカウントを作成することもできます。BlackBerry UEM が Google でユーザー用アカウントを作成する場合に、ユーザーは Google ドメインから Google アカウントパスワードを含むメールを受信します。
   b. ユーザーをローカルユーザーアカウントとして、または会社のディレクトリから取得したアカウント情報を使用して、BlackBerry UEM に追加します。メールアドレスを指定する際には、ユーザーの Google アカウントに関連付けられたメールアドレスを使用します。
   c. 「仕事用と個人用 - ユーザーのプライバシー 」アクティベーションタイプがユーザーに割り当てられていることを確認します。
   d. 次のいずれかのオプションを使用してユーザーにアクティベーションの詳細情報を提供する
      - デバイスアクティベーションパスワードと、オプションとして、QR Code を自動生成して、アクティベーションの手順を記載したメールを送信する
      - デバイスアクティベーションパスワードを設定して、ユーザー名とパスワードをユーザーに直接通知するか、メールで通知する
      - デバイスアクティベーションパスワードを設定せずに、ユーザーが自身でアクティベーションパスワードを設定し BlackBerry UEM Self-Service を表示できるように、QR Code アドレスをユーザーに通知する
2. ユーザーは、BlackBerry UEM Client から Google Play をダウンロードして、デバイスにインストールします。インストール後に、ユーザーは BlackBerry UEM Client を開き、メールアドレスとアクティベーションパスワードを入力するか QR Code をスキャンします。
3. デバイスの BlackBerry UEM Client が次の処理を実行します。
   a. BlackBerry Infrastructure への接続を確立する
   b. BlackBerry Infrastructure にアクティベーション情報を送信する
4. BlackBerry Infrastructure は、次の処理を実行します。
   a. ユーザーが有効な登録済みユーザーであることを確認します
   b. ユーザーの BlackBerry UEM アドレスを取得する
   c. BlackBerry UEM Client にアドレスを送信する

5. BlackBerry UEM Client は、ポート 443 経由で HTTP CONNECT コールを使用して BlackBerry UEM との接続を確立し、BlackBerry UEM にアクティベーション要求を送信します。アクティベーション要求には、ユーザー名、パスワード、デバイスのオペレーティングシステム、および固有のデバイス ID が含まれます。
6. BlackBerry UEM は次の操作を実行します。
   a. ユーザーアカウントに割り当てられたアクティベーションタイプを決定します
   b. 監視対象の Google ドメインに接続して、ユーザー情報を確認します。ユーザーが存在しない場合、BlackBerry UEM は、設定に応じて Google ドメインにユーザーを作成することがあります。
   c. デバイスインスタンスを作成します
   d. デバイスインスタンスを、指定されたユーザーアカウントに関連付けます
   e. 登録セッション ID を HTTP セッションに追加します
   f. 正常に認証されたことを示すメッセージをデバイスに送信する
7. デバイスが暗号化されていない場合は、デバイスの暗号化を求めるプロンプトが表示されます。
8. BlackBerry UEM Client は、次の処理を実行します。
   a. デバイス上に仕事用プロファイルを作成します
   b. Google アカウント情報の入力を求めるプロンプトが表示されます。
   c. 管理対象の Google ドメインに接続して、ユーザーを認証します。
   d. デバイス上に仕事用プロファイルを作成します
   e. BlackBerry UEM から受信した情報を使用して CSR を作成し、HTTPS を介してクライアント証明書リクエストを BlackBerry UEM へ送信します。
9. BlackBerry UEM は次の操作を実行します。
   a. クライアント証明書要求を HTTP セッションの登録セッション ID と照合して検証します
   b. ルート証明書を使用してクライアント証明書要求に署名します
   c. 署名されたクライアント証明書とルート証明書を BlackBerry UEM Client に返送する

   BlackBerry UEM Client と BlackBerry UEM の間に相互に認証された TLS セッションが確立されます。
10. BlackBerry UEM Client は、すべての設定情報を要求し、デバイスおよびソフトウェア情報を BlackBerry UEM に送信します。
11. BlackBerry UEM は、デバイス情報を保存し、リクエストされた設定情報をデバイスに送信します。
12. デバイスは、設定情報を受信し適用したことを示す確認応答を BlackBerry UEM に送信します。アクティベーションプロセスは完了です。

データフロー：Google ドメインで Android Enterprise 仕事用と個人用 - フルコントロール デバイスをアクティブ化する



このデータフローは、BlackBerry UEM が Google Cloud または Google Workspace ドメインに接続されている場合に適用されます。

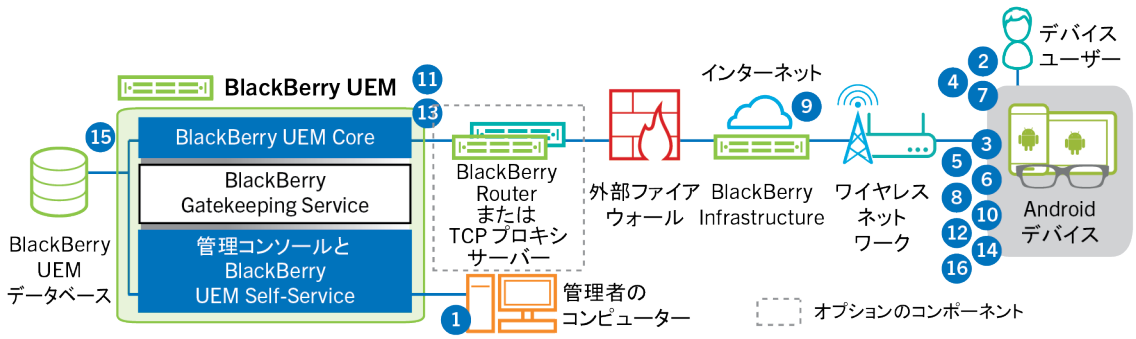
1. 次の操作を実行します。
   a. ユーザーの仕事用メールアドレスに関連付けられている Google アカウントを、ユーザーが所有していることを確認します。BlackBerry UEM を設定して、アクティベーションプロセス中にユーザーに Google アカウントを作成することもできます。BlackBerry UEM が Google でユーザー用アカウントを作成する場合に、ユーザーは Google ドメインから Google アカウントパスワードを含むメールを受信します。
   b. Google ドメインに対して［EMM ポリシーを強制］設定が有効になっていることを確認します。この設定は、アクティブ化されたデバイスを BlackBerry UEM などの EMM 事業者が管理するかを指定します。
   c. ユーザーをローカルユーザーアカウントとして、または会社のディレクトリから取得したアカウント情報を使用して、BlackBerry UEM に追加します。メールアドレスを指定する際には、ユーザーの Google アカウントに関連付けられたメールアドレスを使用します。
   d. 「仕事用と個人用 - フルコントロール 」アクティベーションタイプがユーザーに割り当てられていることを確認します。
   e. ユーザーのアクティベーションパスワードを設定します。
2. ユーザーは、デバイスを工場出荷時のデフォルトの状態にリセットします。
3. デバイスが再起動し、Wi-Fi ネットワークを選択し、アカウントを追加するように求めるプロンプトが表示されます。
4. ユーザーは、仕事用メールアドレスとパスワードを入力します。
5. デバイスは、Google ドメインと通信して、ユーザーが仕事用ユーザーであること、および［EMM ポリシーを強制］設定が有効になっていることを確認します。デバイスが適切な検証を実行した後、デバイスは次の処理を実行します。
   a. デバイスが暗号化されていない場合は、デバイスを暗号化するように求めるプロンプトを表示して、再起動します。
   b. BlackBerry UEM Client を Google Play からダウンロードして、インストールします。
6. デバイス上の BlackBerry UEM Client により、メールアドレスとアクティベーションパスワードを入力するように求めるプロンプトが表示されます。
7. ユーザーは、メールアドレスとアクティベーションパスワードを入力するか、または QR Code をスキャンします。
8. デバイスの BlackBerry UEM Client が次の処理を実行します。
   a. BlackBerry Infrastructure への接続を確立する
   b. BlackBerry Infrastructure にアクティベーション情報を送信する
9. BlackBerry Infrastructure は、次の処理を実行します。
   a. ユーザーが有効な登録済みユーザーであることを確認します
   b. ユーザーの BlackBerry UEM サーバーアドレスを取得します。
   c. BlackBerry UEM Client にサーバーアドレスを送信します
10. BlackBerry UEM Client は、ポート 443 経由で HTTP CONNECT コールを使用して BlackBerry UEM との接続を確立し、BlackBerry UEM にアクティベーション要求を送信します。アクティベーション要求には、ユーザー名、パスワード、デバイスのオペレーティングシステム、および固有のデバイス ID が含まれます。
11. BlackBerry UEM は次の操作を実行します。
   a. ユーザーアカウントに割り当てられたアクティベーションタイプを決定します
   b. Google ドメインに接続して、ユーザー情報を確認します。ユーザーが存在しない場合、BlackBerry UEM は、設定に応じて Google ドメインにユーザーを作成することがあります。
   c. デバイスインスタンスを作成します

d. デバイスインスタンスを、指定されたユーザーアカウントに関連付けます
e. 登録セッション ID を HTTP セッションに追加します
f. 正常に認証されたことを示すメッセージをデバイスに送信する

12. BlackBerry UEM Client は、次の処理を実行します。
    a. デバイス上に仕事用プロファイルを作成します
    b. Google アカウント情報の入力を求めるプロンプトが表示されます。
    c. Google ドメインに接続して、ユーザーを認証します。
    d. BlackBerry UEM から受信した情報を使用して CSR を作成し、HTTPS を介してクライアント証明書リクエストを BlackBerry UEM へ送信します。
13. BlackBerry UEM は次の操作を実行します。
    a. クライアント証明書要求を HTTP セッションの登録セッション ID と照合して検証します
    b. ルート証明書を使用してクライアント証明書要求に署名します
    c. 署名されたクライアント証明書とルート証明書を BlackBerry UEM Client に返送する

    BlackBerry UEM Client と BlackBerry UEM の間に相互に認証された TLS セッションが確立されます。
14. BlackBerry UEM Client は、すべての設定情報を要求し、デバイスおよびソフトウェア情報を BlackBerry UEM に送信します。
15. BlackBerry UEM は、デバイス情報を保存し、リクエストされた設定情報をデバイスに送信します。
16. デバイスは、設定情報を受信し適用したことを示す確認応答を BlackBerry UEM に送信します。アクティベーションプロセスは完了です。

データフロー：Google ドメインで Android Enterprise 仕事用領域のみ デバイスをアクティブ化する



このデータフローは、BlackBerry UEM が Google Cloud または Google Workspace ドメインに接続されている場合に適用されます。

1. 次の操作を実行します。
    a. ユーザーの仕事用メールアドレスに関連付けられている Google アカウントを、ユーザーが所有していることを確認します。BlackBerry UEM を設定して、アクティベーションプロセス中にユーザーに Google アカウントを作成することもできます。BlackBerry UEM が Google でユーザー用アカウントを作成する場合に、ユーザーは Google ドメインから Google アカウントパスワードを含むメールを受信します。
    b. Google ドメインに対して［EMM ポリシーを強制］設定が有効になっていることを確認します。この設定は、アクティブ化されたデバイスを BlackBerry UEM などの EMM 事業者が管理するかを指定します。

c. ユーザーをローカルユーザーアカウントとして、または会社のディレクトリから取得したアカウント情報を使用して、BlackBerry UEM に追加します。メールアドレスを指定する際には、ユーザーの Google アカウントに関連付けられたメールアドレスを使用します。
d. 「仕事用領域のみ 」アクティベーションタイプがユーザーに割り当てられていることを確認します。
e. ユーザーのアクティベーションパスワードを設定します。

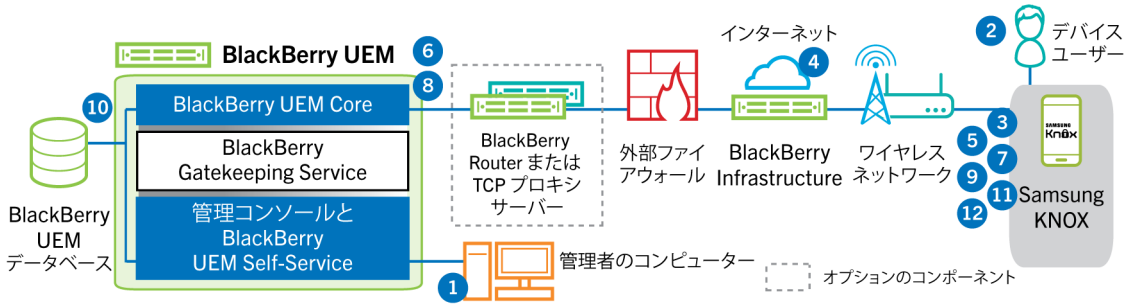
2. ユーザーは、デバイスを工場出荷時のデフォルトの状態にリセットします。
3. デバイスが再起動し、Wi-Fi ネットワークを選択し、アカウントを追加するように求めるプロンプトが表示されます。
4. ユーザーは、仕事用メールアドレスとパスワードを入力します。
5. デバイスは、Google ドメインと通信して、ユーザーが仕事用ユーザーであること、および［EMM ポリシーを強制］設定が有効になっていることを確認します。デバイスが適切な検証を実行した後、デバイスは次の処理を実行します。
   a. デバイスが暗号化されていない場合は、デバイスを暗号化するように求めるプロンプトを表示して、再起動します。
   b. BlackBerry UEM Client を Google Play からダウンロードして、インストールします。
6. デバイス上の BlackBerry UEM Client により、メールアドレスとアクティベーションパスワードを入力するように求めるプロンプトが表示されます。
7. ユーザーは、メールアドレスとアクティベーションパスワードを入力するか、または QR Code をスキャンします。
8. デバイスの BlackBerry UEM Client が次の処理を実行します。
   a. BlackBerry Infrastructure への接続を確立する
   b. BlackBerry Infrastructure にアクティベーション情報を送信する
9. BlackBerry Infrastructure は、次の処理を実行します。
   a. ユーザーが有効な登録済みユーザーであることを確認します
   b. ユーザーの BlackBerry UEM サーバーアドレスを取得します。
   c. BlackBerry UEM Client にサーバーアドレスを送信します
10. BlackBerry UEM Client は、ポート 443 経由で HTTP CONNECT コールを使用して BlackBerry UEM との接続を確立し、BlackBerry UEM にアクティベーション要求を送信します。アクティベーション要求には、ユーザー名、パスワード、デバイスのオペレーティングシステム、および固有のデバイス ID が含まれます。
11. BlackBerry UEM は次の操作を実行します。
   a. ユーザーアカウントに割り当てられたアクティベーションタイプを決定します
   b. Google ドメインに接続して、ユーザー情報を確認します。ユーザーが存在しない場合、BlackBerry UEM は、設定に応じて Google ドメインにユーザーを作成することがあります。
   c. デバイスインスタンスを作成します
   d. デバイスインスタンスを、指定されたユーザーアカウントに関連付けます
   e. 登録セッション ID を HTTP セッションに追加します
   f. 正常に認証されたことを示すメッセージをデバイスに送信する
12. BlackBerry UEM Client は、次の処理を実行します。
   a. Google アカウント情報の入力を求めるプロンプトが表示されます。
   b. Google ドメインに接続して、ユーザーを認証します。
   c. BlackBerry UEM から受信した情報を使用して CSR を作成し、HTTPS を介してクライアント証明書リクエストを BlackBerry UEM へ送信します。
13. BlackBerry UEM は次の操作を実行します。

a. クライアント証明書要求を HTTP セッションの登録セッション ID と照合して検証します
b. ルート証明書を使用してクライアント証明書要求に署名します
c. 署名されたクライアント証明書とルート証明書を BlackBerry UEM Client に返送する

BlackBerry UEM Client と BlackBerry UEM の間に相互に認証された TLS セッションが確立されます。

14. BlackBerry UEM Client は、すべての設定情報を要求し、デバイスおよびソフトウェア情報を BlackBerry UEM に送信します。
15. BlackBerry UEM は、デバイス情報を保存し、リクエストされた設定情報をデバイスに送信します。
16. デバイスは、設定情報を受信し適用したことを示す確認応答を BlackBerry UEM に送信します。アクティベーションプロセスは完了です。

データフロー：デバイスをアクティブ化して Knox Workspace を使用する



1. 次の操作を実行します。
   a. ユーザーをローカルユーザーアカウントとして、または会社のディレクトリから取得したアカウント情報を使用して、BlackBerry UEM に追加する
   b. 「仕事用と個人用 - フルコントロール （Samsung Knox）」、「仕事用と個人用 - ユーザーのプライバシー（Samsung Knox）」、または「仕事用領域のみ - （Samsung Knox）」アクティベーションタイプがユーザーに割り当てられていることを確認する
   c. 次のいずれかのオプションを使用してユーザーにアクティベーションの詳細情報を提供する
      - デバイスアクティベーションパスワードと、オプションとして、QR Code を自動生成して、アクティベーションの手順を記載したメールを送信する
      - デバイスアクティベーションパスワードを設定して、ユーザー名とパスワードをユーザーに直接通知するか、メールで通知する
      - デバイスアクティベーションパスワードを設定せずに、ユーザーが自身でアクティベーションパスワードを設定し BlackBerry UEM Self-Service を表示できるように、QR Code アドレスをユーザーに通知する
2. ユーザーは BlackBerry UEM Client をダウンロードし、デバイスにインストールします。インストール後に、ユーザーは BlackBerry UEM Client を開き、メールアドレスとアクティベーションパスワードを入力するか QR Code をスキャンします。
3. BlackBerry UEM Client は、次の操作を実行します。
   a. BlackBerry Infrastructure への接続を確立する
   b. BlackBerry Infrastructure にアクティベーション情報を送信する
4. BlackBerry Infrastructure は、次の操作を実行します。

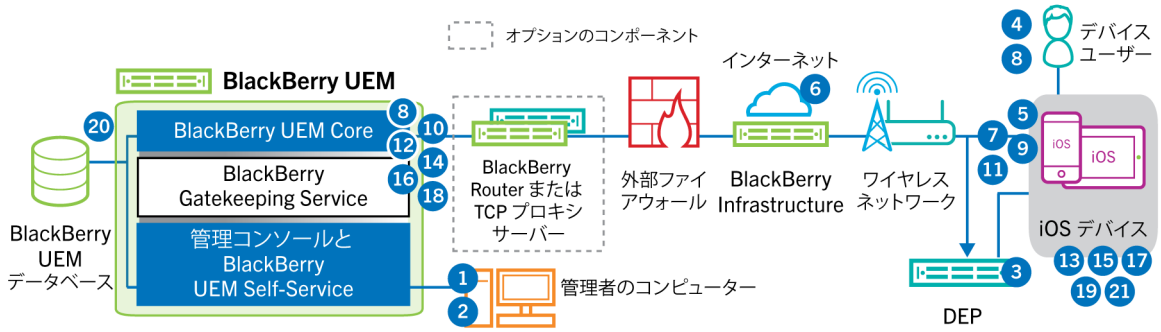
   a. ユーザーが有効な登録済みユーザーであることを確認する
   b. ユーザーの BlackBerry UEM アドレスを取得する
   c. BlackBerry UEM Client にアドレスを送信する
5. BlackBerry UEM Client は、ポート 443 経由で HTTP CONNECT コールを使用して BlackBerry UEM との接続を確立し、BlackBerry UEM にアクティベーション要求を送信します。アクティベーション要求には、ユーザー名、パスワード、デバイスのオペレーティングシステム、および固有のデバイス ID が含まれます。
6. BlackBerry UEM は次の操作を実行します。
   a. 資格情報の有効性を調べる
   b. デバイスインスタンスを作成する
   c. デバイスインスタンスを、BlackBerry UEM データベース内の指定されたユーザーアカウントに関連付ける
   d. 登録セッション ID を HTTP セッションに追加する
   e. 正常に認証されたことを示すメッセージをデバイスに送信する
7. BlackBerry UEM Client は BlackBerry UEM から受信した情報を使用して CSR を作成し、HTTPS を介してクライアント証明書要求を BlackBerry UEM へ送信します。
8. BlackBerry UEM は次の操作を実行します。
   a. クライアント証明書要求を HTTP セッションの登録セッション ID と照合して検証する
   b. ルート証明書を使用してクライアント証明書要求に署名する
   c. 署名されたクライアント証明書とルート証明書を BlackBerry UEM Client に返送する

   BlackBerry UEM Client と BlackBerry UEM の間に相互に認証された TLS セッションが確立されます。
9. BlackBerry UEM Client は、すべての設定情報を要求し、デバイスおよびソフトウェア情報を BlackBerry UEM に送信します。
10. BlackBerry UEM は、デバイス情報をデータベースに保存し、要求された設定情報をデバイスに送信します。
11. BlackBerry UEM Client は、デバイスが Knox Workspace を使用して、サポート対象バージョンを実行しているかどうかを判断します。デバイスが Knox Workspace を使用している場合は、デバイスは Samsung インフラストラクチャに接続し、Knox 管理ライセンスをアクティブ化します。アクティブ化後、BlackBerry UEM Client は、Knox MDM および Knox Workspace IT ポリシールールを適用します。
12. デバイスは、設定情報を受信し適用したことを示す確認応答を BlackBerry UEM に送信します。アクティベーションプロセスは完了です。

アクティベーション完了後、Knox Workspace の仕事用領域のパスワードの作成を求めるプロンプトが表示されます。Knox Workspace 内のデータは、暗号化および、パスワード、PIN、パターン、指紋などの認証方法を使用して保護されます。

メモ： デバイスが 仕事用領域のみ -（Samsung Knox）」アクティベーションタイプを使用してアクティブ化される場合、Knox Workspace のセットアップ時に個人用領域は削除されます。

データフロー：iOS デバイスのアクティベーション

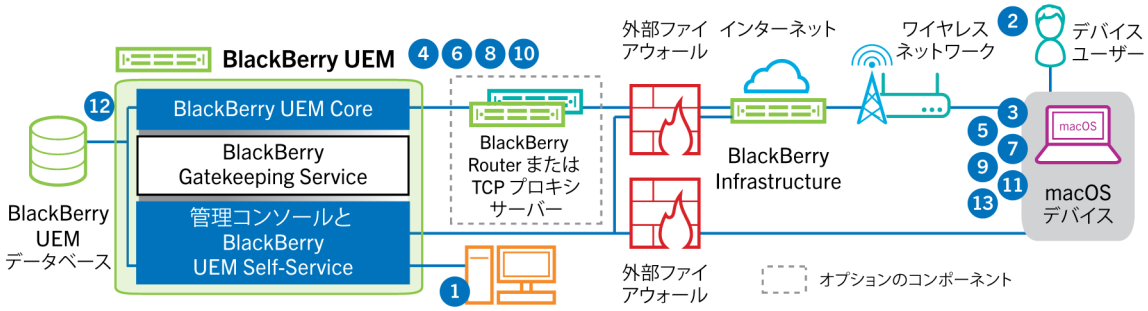


1. Apple の Device Enrollment Program を使用する予定の場合は、次の操作を実行します。
   a. DEP と同期させるため、BlackBerry UEM が設定されていることを確認します。
   b. DEP でデバイスを登録し、MDM サーバーに割り当てます。
   c. 登録設定をデバイスに割り当てます。
2. 次の操作を実行します。
   a. ユーザーをローカルユーザーアカウントとして、または会社のディレクトリから取得したアカウント情報を使用して、BlackBerry UEM に追加する
   b. アクティベーションプロファイルをユーザーに割り当てる
   c. 次のいずれかのオプションを使用してユーザーにアクティベーションの詳細情報を提供する
      - デバイスアクティベーションパスワードと、オプションとして、QR Code を自動生成して、アクティベーションの手順を記載したメールを送信する
      - デバイスアクティベーションパスワードを設定して、ユーザー名とパスワードをユーザーに直接通知するか、メールで通知する
      - デバイスアクティベーションパスワードを設定せずに、ユーザーが自身でアクティベーションパスワードを設定し BlackBerry UEM Self-Service を表示できるように、QR Code アドレスをユーザーに通知する
3. デバイスが Apple DEP に登録されている場合には、デバイスは初期セットアップ中に Apple DEP Web サービスと通信します。デバイスが BlackBerry UEM Client アプリをインストールするように設定した場合は、デバイスはダウンロードおよびインストールを自動的に実行します。
4. デバイスが Apple DEP に登録されていない場合、および BlackBerry UEM Client をインストールするようにデバイスを設定していない場合は、ユーザーが手動で BlackBerry UEM Client をデバイスにダウンロードおよびインストールします。インストール後に、ユーザーは BlackBerry UEM Client を開き、メールアドレスとアクティベーションパスワードを入力するか QR Code をスキャンします。
5. BlackBerry UEM Client は、次の操作を実行します。
   a. BlackBerry Infrastructure への接続を確立する
   b. BlackBerry Infrastructure にアクティベーション情報を送信する
6. BlackBerry Infrastructure は、次の操作を実行します。
   a. ユーザーが有効な登録済みユーザーであることを確認する
   b. ユーザーの BlackBerry UEM アドレスを取得する
   c. BlackBerry UEM Client にアドレスを送信する
7. BlackBerry UEM Client は、ポート 443 経由で HTTP CONNECT コールを使用して BlackBerry UEM との接続を確立し、BlackBerry UEM にアクティベーション要求を送信します。アクティベーション要求には、ユーザー名、パスワード、デバイスのオペレーティングシステム、および固有のデバイス ID が含まれます。

8. BlackBerry UEM は次の操作を実行します。
   a. 資格情報の有効性を調べる
   b. デバイスインスタンスを作成する
   c. デバイスインスタンスを、BlackBerry UEM データベース内の指定されたユーザーアカウントに関連付ける
   d. 登録セッション ID を HTTP セッションに追加する
   e. 正常に認証されたことを示すメッセージをデバイスに送信する
9. BlackBerry UEM Client は BlackBerry UEM から受信した情報を使用して CSR を作成し、HTTPS を介してクライアント証明書要求を送信します。
10. BlackBerry UEM は次の操作を実行します。
    a. クライアント証明書要求を HTTP セッションの登録セッション ID と照合して検証する
    b. ルート証明書を使用してクライアント証明書要求に署名する
    c. 署名されたクライアント証明書とルート証明書を BlackBerry UEM Client に返送する

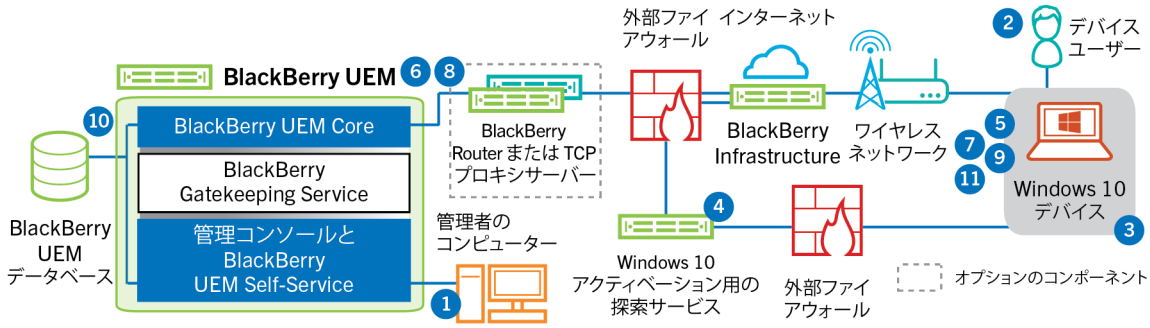
    BlackBerry UEM Client と BlackBerry UEM の間に相互に認証された TLS セッションが確立されます。
11. BlackBerry UEM Client は、アクティベーションを完了するために証明書をインストールする必要があることをユーザーに通知するために、メッセージを表示します。ユーザーは、［OK］をクリックすると、ネイティブ MDM Daemon アクティベーションのリンクへリダイレクトされます。BlackBerry UEM Client は、BlackBerry UEM への接続を確立します。
12. BlackBerry UEM は、MDM プロファイルをデバイスに提供します。このプロファイルには、MDM アクティベーション URL とチャレンジが含まれます。MDM プロファイルは、デバイスがプロファイルを検証できるように、署名者の完全な証明書チェーンを含む PKCS#7 署名付きメッセージとしてラップされます。これによって登録プロセスがトリガーされます。
13. デバイス上のネイティブ MDM Daemon は、顧客 ID、言語、および OS バージョンを含むデバイスプロファイルを BlackBerry UEM に送信します。
14. BlackBerry UEM は、要求が CA によって署名されていることを検証し、ネイティブ MDM Daemon に正常に認証されたことを示す通知で応答します。
15. ネイティブ MDM Daemon は、CA 証明書、CA 機能情報、およびデバイスが発行した証明書を求める要求を BlackBerry UEM に送信します。
16. BlackBerry UEM は、CA 証明書、CA 機能情報、およびデバイスが発行した証明書をネイティブ MDM Daemon に送信します。
17. ネイティブ MDM Daemon は、MDM プロファイルをデバイスにインストールします。BlackBerry UEM Client は、MDM プロファイルと証明書が正常にインストールされたことを BlackBerry UEM に通知し、BlackBerry UEM が MDM アクティベーションの完了を確認するまで、定期的にポーリングします。
18. BlackBerry UEM は、MDM アクティベーションが完了したことを確認します。
19. BlackBerry UEM Client は、すべての設定情報を要求し、デバイスおよびソフトウェア情報を BlackBerry UEM に送信します。
20. BlackBerry UEM は、デバイス情報をデータベースに保存し、設定情報をデバイスに送信します。
21. デバイスは、設定更新を受信し適用したことを示す確認応答を BlackBerry UEM に送信します。アクティベーションプロセスは完了です。

データフロー：macOS デバイスのアクティベーション



1. 管理者は、ユーザーが BlackBerry UEM ユーザーアカウントと、以下を含む BlackBerry UEM Self-Service へのログイン情報を持っていることを確認します。
   - BlackBerry UEM Self-Service の Web アドレス
   - ユーザー名とパスワード
   - ドメイン名
2. ユーザーは自分の BlackBerry UEM Self-Service デバイスで macOS にログインし、デバイスをアクティブ化します。
3. デバイスがポート 443 で BlackBerry UEM アクティベーション要求を送信します。
4. BlackBerry UEM は、MDM プロファイルをデバイスに提供します。このプロファイルには、MDM アクティベーション URL とチャレンジが含まれます。MDM プロファイルは、デバイスがプロファイルを検証できるように、署名者の完全な証明書チェーンを含む PKCS#7 署名付きメッセージとしてラップされます。これによって登録プロセスがトリガーされます。
5. デバイス上のネイティブ MDM Daemon は、顧客 ID、言語、および OS バージョンを含むデバイスプロファイルを BlackBerry UEM に送信します。
6. BlackBerry UEM は、要求が CA によって署名されていることを検証し、ネイティブ MDM Daemon に正常に認証されたことを示す通知で応答します。
7. ネイティブ MDM Daemon は、CA 証明書、CA 機能情報、およびデバイスが発行した証明書を求める要求を BlackBerry UEM に送信します。
8. BlackBerry UEM は、CA 証明書、CA 機能情報、およびデバイスが発行した証明書をネイティブ MDM Daemon に送信します。
9. ネイティブ MDM Daemon は、MDM プロファイルをデバイスにインストールします。
10. BlackBerry UEM は、MDM アクティベーションが完了したことを確認します。
11. デバイスはすべての設定情報を要求します。
12. BlackBerry UEM は、デバイス情報をデータベースに保存し、設定情報をデバイスに送信します。
13. デバイスは、設定情報を受信し適用したことを示す確認応答を BlackBerry UEM に送信します。アクティベーションプロセスは完了です。

データフロー：Windows 10 デバイスのアクティベーション



1. 次の操作を実行します。
   a. Windows 10 アクティベーションを簡易化するために検出サービスを設定します。
   b. ユーザーをローカルユーザーアカウントとして、または会社のディレクトリから取得したアカウント情報を使用して、BlackBerry UEM に追加する
   c. 次のいずれかのオプションを使用してユーザーにアクティベーションの詳細情報を提供する
      - デバイスアクティベーションパスワードを自動生成し、アクティベーションの手順を記載したメールを送信する
      - デバイスアクティベーションパスワードを設定し、メールでユーザーにアクティベーション情報を送信するオプションを選択する
      - デバイスアクティベーションパスワードを設定せずに、ユーザーが自身でアクティベーションパスワードを設定しサーバーアドレスを表示できるように、BlackBerry UEM Self-Service アドレスをユーザーに通知する
   d. デバイスをインストールするために BlackBerry UEM により生成される CA 証明書をユーザーに提供します。
2. ユーザーは、デバイスで以下のアクションを完了します。
   a. デバイスでインターネットがポート 443 で接続していることを確認します。
   b. 証明書を開き、インストールします。
   c. ［設定］>［アカウント］>［職場のアクセス］に移動して、［接続］をタップします。
   d. プロンプトが表示されたら、アクティベーションメールで受信したメールアドレスとアクティベーションパスワードを入力します。
3. デバイスが、組織での Windows 10 アクティベーションを簡易化するために設定した検出サービスとの接続を確立します。
4. 検出サービスが、BlackBerry UEM サーバーの SRP ID が有効であることを確認し、デバイスを BlackBerry UEM にリダイレクトします。
5. デバイスがポート 443 で BlackBerry UEM アクティベーション要求を送信します。アクティベーション要求には、ユーザー名、パスワード、デバイスのオペレーティングシステム、および固有のデバイス ID が含まれます。
6. BlackBerry UEM は次の操作を実行します。
   a. 資格情報の有効性を調べる
   b. デバイスインスタンスを作成する
   c. デバイスインスタンスを、BlackBerry UEM データベース内の指定されたユーザーアカウントに関連付ける
   d. 登録セッション ID を HTTP セッションに追加する

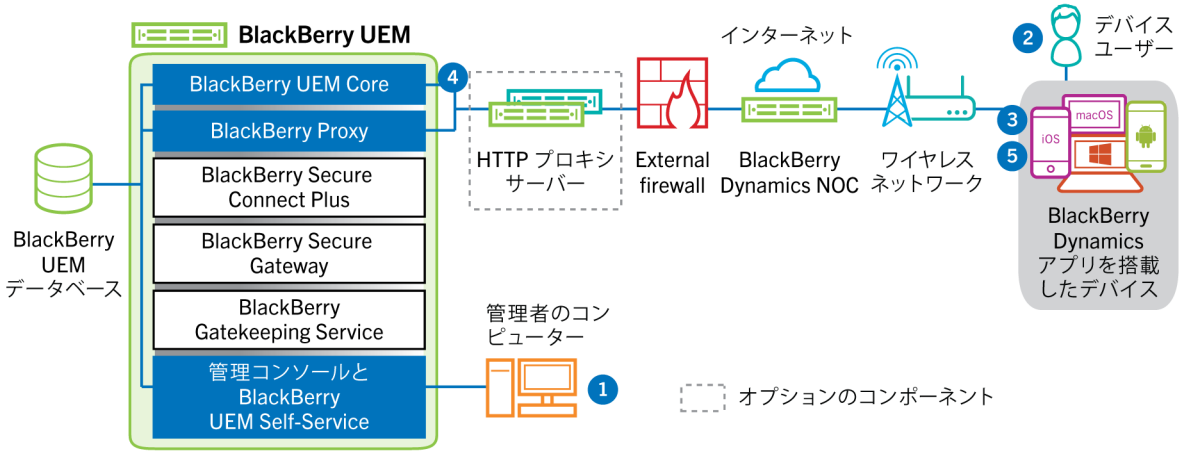
e. 正常に認証されたことを示すメッセージをデバイスに送信する

7. デバイスが CSR を作成し、HTTPS 経由で BlackBerry UEM に送信します。CSR にはユーザー名とアクティベーションパスワードが含まれています。
8. BlackBerry UEM はユーザー名とパスワードを検証し、さらに CSR を検証して、クライアント証明書と CA 証明書をデバイスに返します。

   これで、デバイスと BlackBerry UEM 間のすべての通信が、これらの証明書を使用した、相互認証されたエンドツーエンドの通信となります。
9. デバイスはすべての設定情報を要求します。
10. BlackBerry UEM は、デバイス情報をデータベースに保存し、設定情報をデバイスに送信します。
11. デバイスは、設定情報を受信し適用したことを示す確認応答を BlackBerry UEM に送信します。アクティベーションプロセスは完了です。

データフロー：デバイスでの最初の BlackBerry Dynamics アプリのアクティベーション

このデータフローは、BlackBerry Dynamics アプリがデバイス上でアクティベートされる際に、それ以外にアクティベートされている BlackBerry Dynamics アプリや BlackBerry UEM Client が存在しない場合において、データが移動する仕組みを説明したものです。



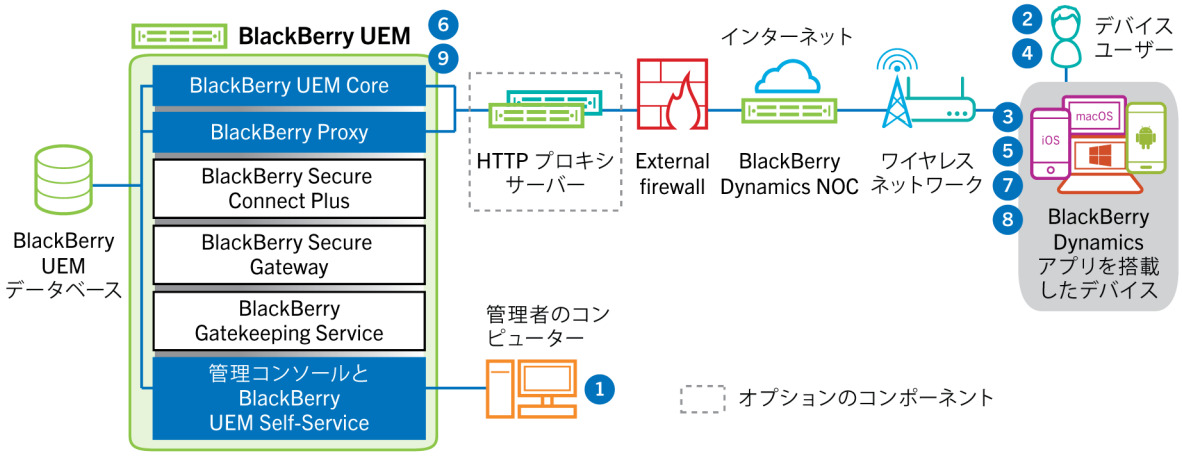
1. 管理者は次の操作を実行します。
   a. 1 つ以上の BlackBerry Dynamics アプリをユーザーに割り当てます。
   b. アクティベーション認証情報（アクセスキー、アクティベーションパスワード、または QR コード）を発行するか、サードパーティ ID プロバイダーを使用してユーザーに送信するか、ユーザーに認証情報を BlackBerry UEM Self-Service から生成するように指示します。
2. ユーザーは次の操作を実行します。
   a. アプリをデバイスにインストールします。
   b. 提供されたアクティベーション認証情報を取得して入力します。
3. BlackBerry Dynamics アプリが次の処理を実行します。
   a. BlackBerry Dynamics NOC に接続して、アクティベーションを完了します。
   b. 次のいずれかの方法を使用して、BlackBerry UEM のアドレスを取得します。
      - ユーザーが認証情報を手動で入力した場合、アプリはアドレスを BlackBerry Infrastructure から取得します。
      - ユーザーが QR コードをスキャンした場合、アプリはアドレスを QR コードから受信します。
   c. BlackBerry UEM に BlackBerry Infrastructure で接続して BlackBerry UEM とのエンドツーエンドの暗号化セッションを EC-SPEKE プロトコルを使用して確立します。

      このセッションは、アクティベーション認証情報を発行した BlackBerry UEM インスタンスによってのみ復号できます。
   d. アクティベーション要求を保護されたセッションを介して送信します。
4. BlackBerry UEM がアクティベーション要求を確認して、暗号化されたアクティベーション応答をアプリに送信します。アクティベーション応答には、クライアント証明書、マスターセッションキー、BlackBerry Proxy インスタンスのリスト、信頼済み認証局を含む、アプリが BlackBerry UEM と通信する際に必要なデータが含まれます。

5. アプリはユーザーにアプリのパスワードを設定して BlackBerry Dynamics NOC を使用する簡単なアクティベーション委任として登録するよう要求し、2 回目以降に BlackBerry Dynamics アプリをデバイスでアクティベートする際にユーザーが新しい認証情報を手動で取得しなくて済むようにします。

データフロー：すでにデバイスでアクティベートされているアプリがある場合の BlackBerry Dynamics アプリのアクティベーション

このデータフローは、BlackBerry Dynamics アプリがデバイス上でアクティベートされる際に、すでにアクティベートされている BlackBerry UEM Client または別の BlackBerry Dynamics アプリが簡単なアクティベーション委任として機能する場合において、データが移動する仕組みを説明したものです。



1. 管理者は、1 つまたは複数の BlackBerry Dynamics アプリをユーザーに割り当てます。
2. ユーザーはデバイスにアプリをインストールします。
3. アプリが次の処理を実行します。
   a. BlackBerry Dynamics NOC をクエリして、デバイス上でアクティベートされている別のアプリを識別する
   b. アクティベーション認証情報を以前にアクティベートされたアプリから要求する
4. ユーザーは、デバイス上で以前にアクティベートされたアプリからのアクティベーション要求を承認します。
5. 以前にアクティベートされたアプリが、認証情報を BlackBerry UEM に送信します。
6. BlackBerry UEM が、認証情報要求と BlackBerry UEM URL を既存のアプリに送信します。
7. 以前にアクティベートされたアプリが、認証情報と URL を新しいアプリに返します。
8. 新しいアプリが次の処理を完了します。
   a. BlackBerry Dynamics NOC でアクティベートする
   b. BlackBerry UEM に BlackBerry Infrastructure で接続して BlackBerry UEM とのエンドツーエンドの暗号化セッションを EC-SPEKE プロトコルを使用して確立します。

      このセッションは、アクティベーション認証情報を発行した BlackBerry UEM インスタンスによってのみ復号できます。
   c. アクティベーション要求を保護されたセッションで送信する

9. BlackBerry UEM がアクティベーション要求を確認して、暗号化されたアクティベーション応答をアプリに送信します。アクティベーション応答には、クライアント証明書、マスターセッションキー、BlackBerry Proxy インスタンスのリスト、信頼済み認証局を含む、アプリが BlackBerry UEM と通信する際に必要なデータが含まれます。

データフロー：仕事用データの送受信

BlackBerry UEM 上でアクティブなデバイスが仕事用データを送受信する場合、これらのデバイスは組織のメール、アプリケーション、またはコンテンツサーバーに接続されます。たとえば、仕事用メールアプリまたはカレンダーアプリを使用している場合、デバイスは組織のメールサーバーへの接続を確立します。仕事用ブラウザーを使用してイントラネット内を移動している場合、デバイスは組織内の Web サーバーとの接続を確立します。

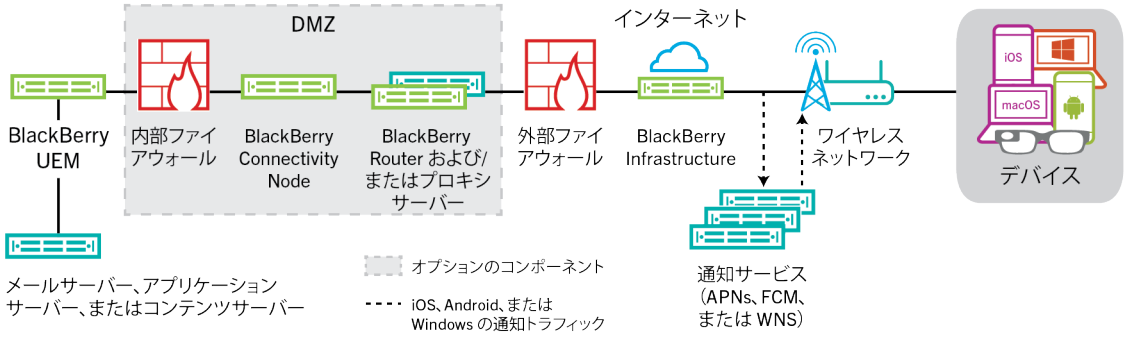
このセクションで は、仕事用データが組織の UEM 環境をどのように移動するかを詳細に示すデータフローを説明します。

デバイスタイプ、アクティベーションタイプ、ライセンスの種類および設定に応じて、デバイスは次のパスを使用して組織のサーバーへの接続を確立することがあります。

データパス	説明
仕事用 Wi-Fi ネットワーク	デバイスが仕事用 UEM ネットワークを使用して組織のリソースに接続できるように、管理者が Wi-Fi を使用してデバイスに Wi-Fi プロファイルを設定することができます。
VPN	デバイスが VPN を使用して組織のリソースに接続できるように、管理者が UEM を使用してデバイスに VPN プロファイルを設定するか、ユーザーが自分のデバイスに VPN プロファイルを設定することができます。
UEM および BlackBerry Infrastructure または BlackBerry Dynamics NOC	デバイス、アクティベーション、ライセンスの種類、および BlackBerry Dynamics アプリの存在に応じて、デバイスが、UEM および BlackBerry Infrastructure を通じて組織のリソースと通信するためにエンタープライズ接続を使用できる可能性があります。 • iOS デバイスの場合、デバイスに適切なライセンスがあれば、BlackBerry Secure Gateway を有効にして、BlackBerry Infrastructure および UEM を介して、デバイスを仕事用メールサーバーに接続できます。BlackBerry Secure Gateway を使用する場合、iOS を使用するユーザーが組織の VPN または仕事用 Wi-Fi ネットワークに接続していないときに Microsoft Exchange に接続できるようにするために、メールサーバーをファイアウォールの外側に公開する必要はありません。 • iOS、Android Enterprise、および Samsung Knox Workspace のデバイスについては、デバイスに適切なライセンスがある場合、BlackBerry Secure Connect Plus を有効にすることでエンタープライズ接続を使用できます。デバイスが BlackBerry Secure Connect Plus を使用する場合、仕事用データは、BlackBerry Infrastructure を介してデバイス上のアプリと組織のネットワーク間で確立された、安全な IP トンネル内で転送されます。 • デバイスにインストールされている BlackBerry Dynamics アプリは BlackBerry Proxy と通信します。設定に応じて、データは BlackBerry Dynamics NOC または BlackBerry Infrastructure を通過して移動することも、BlackBerry Dynamics Direct Connect を使用してそれらをバイパスすることもできます。 • デバイスは、すべての仕事用データにエンタープライズ接続を使用できます。エンタープライズ接続は、すべての仕事用データを暗号化して認証し、UEM および BlackBerry Infrastructure を介して送信します。エンタープライズ接続は、組織の外部ファイアウォールで開き必要のあるポート数を、単一ポートの 3101 に限定します。

BlackBerry Infrastructure の使用による仕事用データの送受信

デバイスは、エンタープライズ接続または BlackBerry UEM を使用して、設定の更新を取得し、仕事用データを送受信するために、BlackBerry Infrastructure 経由で BlackBerry Secure Gateway に接続します。次の図は、デバイスが BlackBerry UEM を経由して BlackBerry Infrastructure および組織のリソースに接続する方法を示しています。



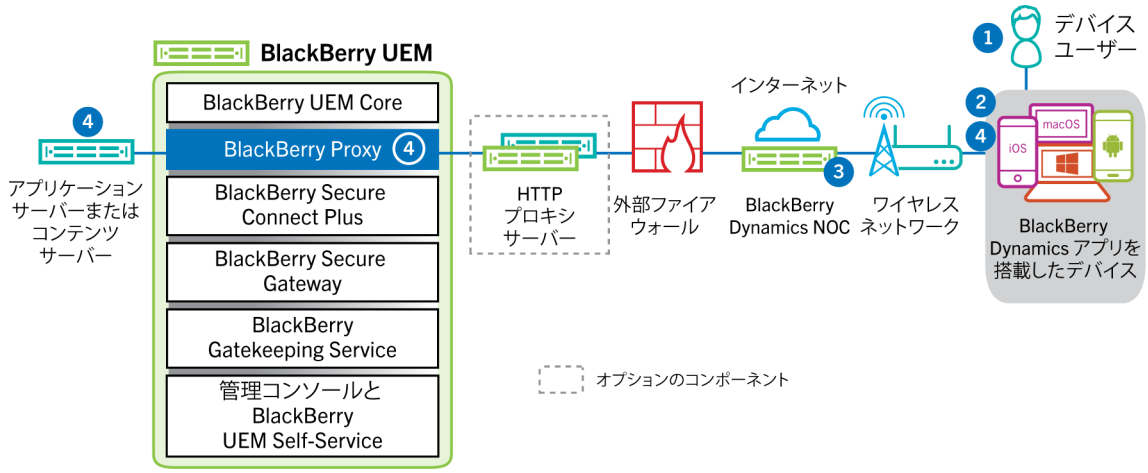
次の表は、デバイスが BlackBerry UEM を経由して BlackBerry Infrastructure および組織のネットワークに接続する場合の状況を示しています。

デバイスタイプ	説明
すべてのデバイス	すべてのデバイスがこの通信パスを使用して、デバイスコマンド、ポリシーとプロファイルの更新、送信デバイス情報、アクティビティレポートなどの設定データを送受信します。詳細については、「データフロー：デバイス設定の更新の受信」を参照してください。
iOS デバイス	iOS デバイスを許可するために BlackBerry Secure Gateway を有効化して、BlackBerry Infrastructure および BlackBerry UEM を介して仕事用メールサーバーに接続できます。BlackBerry Secure Gateway を使用する場合、ユーザーが組織の VPN または仕事用 Wi-Fi ネットワークに接続していないときに仕事用メールを受信できるようにするために、メールサーバーをファイアウォールの外側に公開する必要はありません。

デバイスタイプ	説明
iOS、Android Enterprise、および Samsung Knox Workspace デバイス。	BlackBerry Secure Connect Plus を使用するように設定されているエンタープライズ接続プロファイルが割り当てられたデバイスは、BlackBerry Infrastructure を介してセキュリティ保護された IP トンネルを使用して、アプリと組織のネットワーク間でデータを転送できます。 iOS デバイスの場合、BlackBerry Secure Connect Plus は組織のネットワークとすべてのアプリまたは指定したアプリのみの間に、セキュリティ保護されたトンネルを提供できます。 Android Enterprise デバイスの場合、BlackBerry Secure Connect Plus はすべての仕事用領域アプリと組織のネットワークの間に、セキュリティ保護されたトンネルを提供します。 Samsung Knox Workspace デバイスの場合、BlackBerry Secure Connect Plus は組織のネットワークとすべての仕事用アプリまたは指定した仕事用アプリのみの間に、セキュリティ保護されたトンネルを提供できます。
BlackBerry Dynamics アプリがインストールされている iOS および Android デバイス	BlackBerry Dynamics アプリのエンタープライズ接続では BlackBerry Infrastructure を使用しません。その代わりに、BlackBerry Dynamics アプリと BlackBerry Proxy の間で転送されるデータは BlackBerry Dynamics NOC を通過して移動できるか、または BlackBerry Dynamics Direct Connect を使用して、NOC をバイパスできます。

データフロー：**BlackBerry Dynamics NOC** を介して **BlackBerry Dynamics** アプリから仕事用データ送受信する

このデータフローは、BlackBerry Dynamics アプリが BlackBerry UEM および BlackBerry Dynamics NOC を通じて組織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にアクセスするときにデータが移動する仕組みを説明しています。



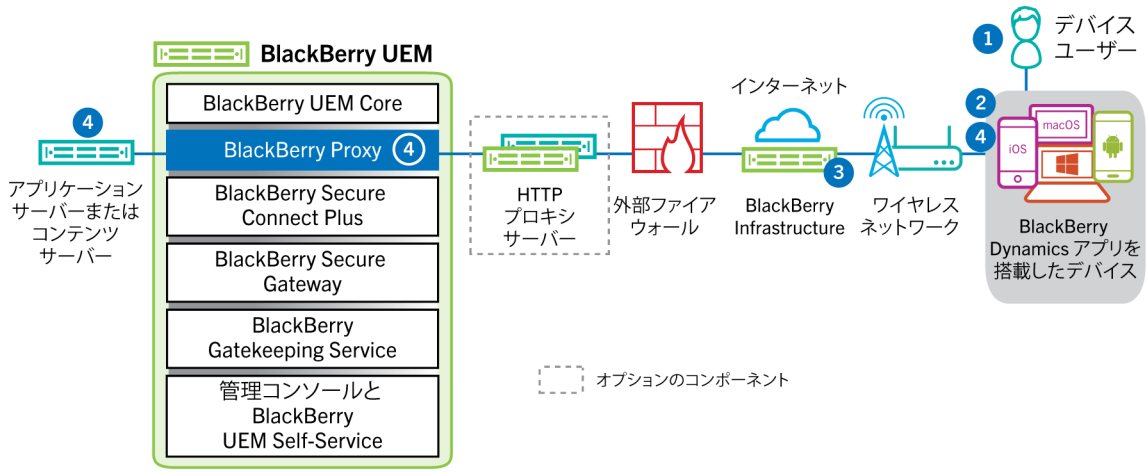
1. ユーザーは、BlackBerry Dynamics アプリを開いて、仕事用データにアクセスします。
2. BlackBerry Dynamics アプリは、BlackBerry Dynamics NOC への接続を確立します。接続は、アプリがアクティブ化されたときに作成されたマスターリンクキーで認証されます。

3. BlackBerry Dynamics NOC は、事前に確立されたセキュリティ保護された接続を介して BlackBerry Proxy と通信し、BlackBerry Dynamics アプリと仕事用データを伝送する BlackBerry Proxy との間でエンドツーエンドの接続を確立します。仕事用データは、BlackBerry Dynamics NOC に知られていないセッションキーで暗号化されます。
4. セキュアなエンドツーエンド接続が確立されると、仕事用データは、BlackBerry Proxy を介してファイアウォールの背後にあるデバイスとアプリケーションサーバーまたはコンテンツサーバーの間を移動することができます。

データフロー：**BlackBerry Infrastructure** を介して **BlackBerry Dynamics** アプリから仕事用データ送受信する

サーバーの設定によっては、BlackBerry Dynamics SDK 7.0 以降で開発されたアプリの仕事用データが BlackBerry Dynamics NOC ではなく BlackBerry Infrastructure を通って移動する場合があります。BlackBerry UEM バージョン 12.12 の新規インストールがある場合、BlackBerry UEM はデフォルトで BlackBerry Infrastructure を使用します。BlackBerry UEM の前のバージョンからアップグレードした場合、この機能を有効にするには、BlackBerry テクニカルサポートに問い合わせる必要があります。

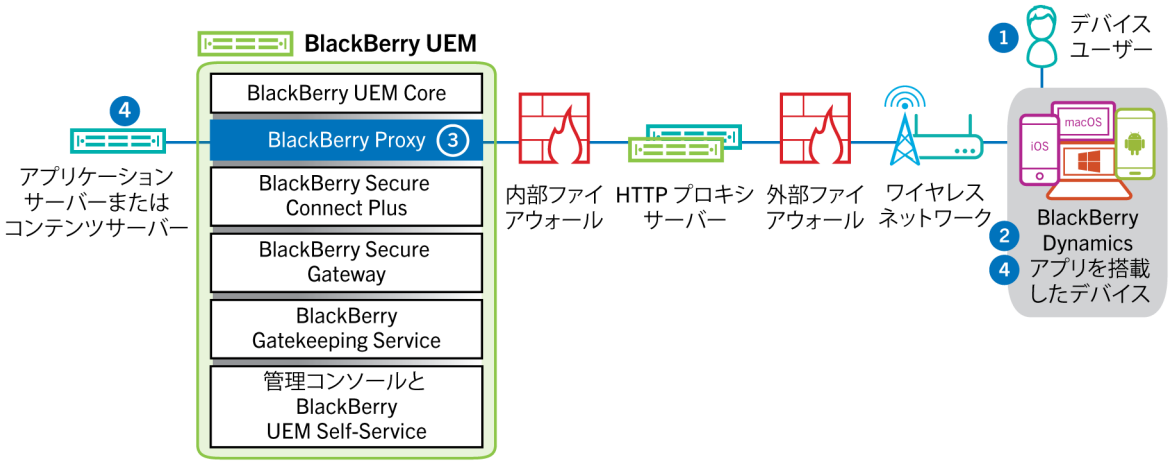
このデータフローは、BlackBerry Dynamics アプリが BlackBerry Infrastructure および BlackBerry UEM を通じて組織のアプリケーションサーバーまたはコンテンツサーバーにアクセスするときにデータが移動する仕組みを説明しています。



1. ユーザーは、BlackBerry Dynamics アプリを開いて、仕事用データにアクセスします。
2. BlackBerry Dynamics アプリは、BlackBerry Infrastructure への接続を確立します。
3. BlackBerry Infrastructure は、事前に確立された TLS 接続を介して BlackBerry Proxy と通信します。
4. BlackBerry Dynamics アプリは BlackBerry Proxy への TLS 接続を確立し、安全なエンドツーエンド接続を介して仕事用データが交換されます。

データフロー：**BlackBerry Dynamics Direct Connect** を使用して **BlackBerry Dynamics** アプリから仕事用データ送受信する

このデータフローは、BlackBerry Dynamics アプリが BlackBerry Dynamics Direct Connect および BlackBerry UEM を通って、組織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にアクセスする際に、データが転送される仕組みを説明しています。Direct Connect の詳細については、「BlackBerry UEM を使用した Direct Connect の設定」を参照してください。

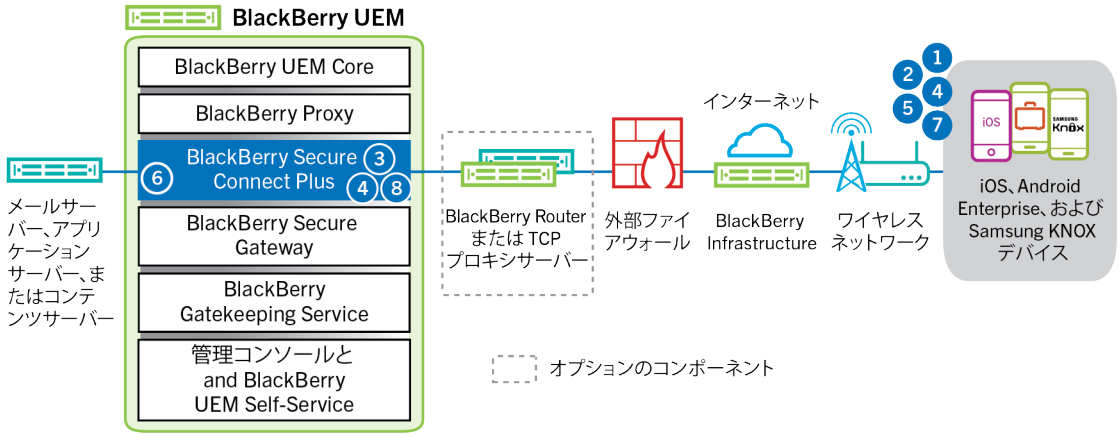


1. ユーザーは、BlackBerry Dynamics アプリを開いて、仕事用データにアクセスします。
2. BlackBerry Dynamics アプリは、BlackBerry Proxy への TLS 接続を確立します。
3. BlackBerry Proxy は BlackBerry Dynamics アプリで認証します。BlackBerry Proxy は、サーバー証明書を使用して、アプリで認証します。BlackBerry Proxy は、BlackBerry Proxy とアプリにのみ知られているセッションキーでキーが付けられた MAC を使用して、アプリを検証します。
4. セキュアなエンドツーエンド接続が確立されると、仕事用データは、BlackBerry Proxy を介してファイアウォールの背後にあるデバイスとアプリケーションサーバーまたはコンテンツサーバーの間を移動することができます。

データフロー：**BlackBerry Secure Connect Plus** を使用する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

このデータフローは、BlackBerry Secure Connect Plus を使用するように設定されているデバイス上のアプリが、組織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にアクセスする場合にデータが転送される仕組みを説明しています。

このデータフローは、Android Enterprise デバイスまたは Samsung Knox Workspace デバイスの仕事用領域にある BlackBerry Dynamics アプリには適用されません。詳細については、次を参照してください データフロー：BlackBerry Secure Connect Plus を使用する Android デバイスで BlackBerry Dynamics アプリから仕事用データを送受信する



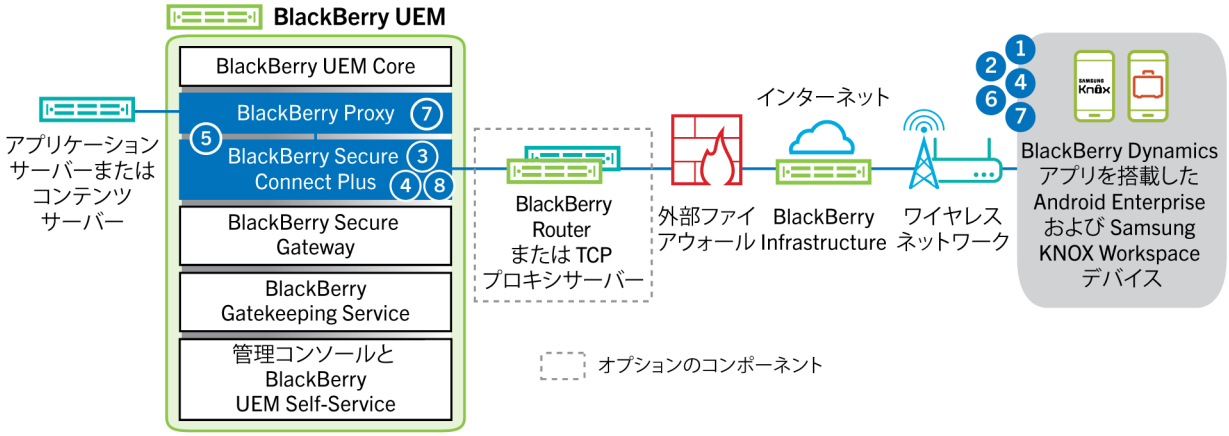
1. ユーザーは、組織のファイアウォール内のコンテンツサーバーまたはアプリケーションサーバーからアプリを開いて、仕事用データにアクセスします。
   - Android Enterprise デバイスの場合、制限するように選択したアプリを除き、すべての仕事用領域アプリが BlackBerry Secure Connect Plus を使用します。
   - Samsung Knox Workspace デバイスの場合、すべての仕事用領域アプリが BlackBerry Secure Connect Plus を使用するか、指定した仕事用アプリのみが使用するかを指定します。
   - iOS デバイスの場合、すべてのアプリが BlackBerry Secure Connect Plus を使用するか、指定したアプリのみが使用するかを指定します。
2. デバイスが、TLS トンネルを介してポート 443 で BlackBerry Infrastructure にリクエストを送信し、仕事用ネットワークに、セキュリティ保護されたトンネルを要求します。信号は、FIPS-140 認定 Certicom ライブラリを使って、デフォルトで暗号化されます。信号トンネルはエンドツーエンドで暗号化されます。
3. BlackBerry Secure Connect Plus は、ポート 3101 を介して BlackBerry Infrastructure からリクエストを受信します。
4. デバイスと BlackBerry Secure Connect Plus は トンネルパラメーターのネゴシエーションを行い、BlackBerry Infrastructure.を介してデバイスのセキュリティ保護されたトンネルを確立します。トンネルは認証され、DTLS を使ってエンドツーエンドで暗号化されます。
5. アプリは、標準 IPv4 プロトコル（TCP および UDP）を使用して、トンネル経由でアプリケーションサーバーまたはコンテンツサーバーに接続します。
6. BlackBerry Secure Connect Plus は、組織のネットワークと IP データ転送のやり取りを行います。BlackBerry Secure Connect Plus は、FIPS-140 認定 Certicom ライブラリを使用して、トラフィックの暗号化および複合化を行います。
7. アプリはデータを受信し、デバイス上に表示します。
8. トンネルが開いている限り、サポートされているアプリはトンネルを使用してネットワークリソースにアクセスできます。組織のネットワークに接続するために使用可能な方法の中で、トンネルが最適な方法ではなくなった場合、BlackBerry Secure Connect Plus は接続を終了します。

データフロー：**BlackBerry Secure Connect Plus** を使用する **Android** デバイスで **BlackBerry Dynamics** アプリから仕事用データを送受信する

このデータフローは、Android Enterprise または Samsung Knox Workspace デバイス上の BlackBerry Dynamics アプリが BlackBerry Secure Connect Plus を使用するときにデータが移動する仕組みについて説明しています。

Android Enterprise デバイス上で BlackBerry Secure Connect Plus を BlackBerry Dynamics アプリで使用している場合、ネットワークの遅延を回避するために、BlackBerry Dynamics アプリが BlackBerry Secure Connect Plus を使用するのを制限することをお勧めします。Samsung Knox Workspace デバイス上で特定のアプリを制限することはできません。

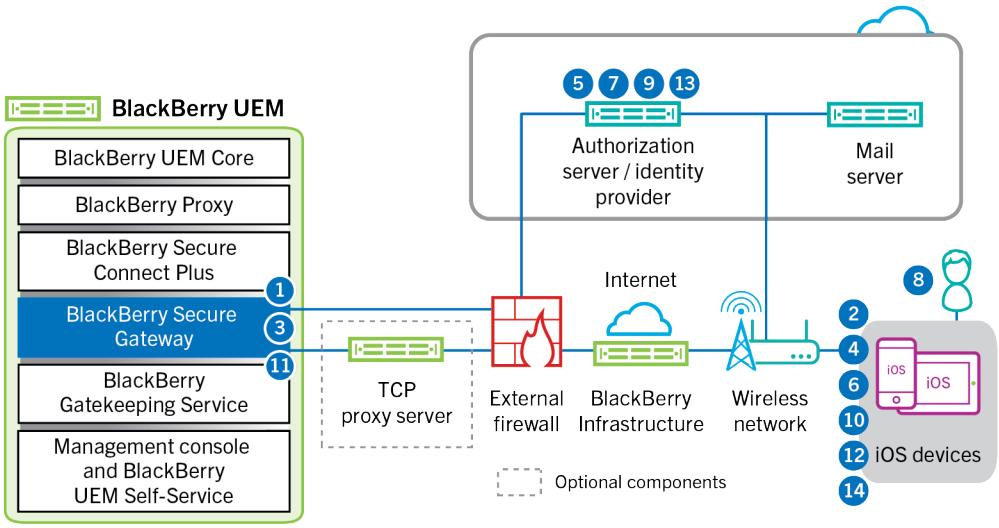
Android Enterprise デバイスまたは Samsung Knox Workspace デバイス上で BlackBerry Secure Connect Plus を BlackBerry Dynamics アプリで使用している場合、ネットワークの遅延を軽減するために、BlackBerry UEM が BlackBerry Dynamics NOC を通して BlackBerry Dynamics アプリデータを送信しないように設定することをお勧めします。



1. ユーザーは、BlackBerry Dynamics アプリを開いて、仕事用データにアクセスします。
2. デバイスが、TLS トンネルを介してポート 443 で BlackBerry Infrastructure に要求を送信し、仕事用ネットワークへのセキュリティ保護されたトンネルを要求します。信号は、FIPS-140 認定 Certicom ライブラリを使って、デフォルトで暗号化されます。信号トンネルはエンドツーエンドで暗号化されます。
3. BlackBerry Secure Connect Plus は、ポート 3101 を介して BlackBerry Infrastructure から要求を受信します。
4. デバイスと BlackBerry Secure Connect Plus は トンネルパラメーターのネゴシエーションを行い、BlackBerry Infrastructure を介してデバイスのセキュリティ保護されたトンネルを確立します。トンネルは認証され、DTLS を使ってエンドツーエンドで暗号化されます。
5. BlackBerry Secure Connect Plus は、BlackBerry Proxy との接続を確立します。
6. BlackBerry Dynamics アプリは、BlackBerry Secure Connect Plus トンネルを使用して BlackBerry Proxy への接続を確立します。
7. BlackBerry Proxy は、サーバー証明書を使用して、BlackBerry Dynamics アプリで認証します。BlackBerry Proxy は、BlackBerry Proxy とアプリにのみ知られているセッションキーでキーが付けられた MAC を使用して、アプリを検証します。
8. BlackBerry Proxy とアプリの間でセキュリティ保護された接続が確立されている場合、仕事用データは、BlackBerry Proxy への BlackBerry Secure Connect Plus トンネルを使用して、ファイアウォールの背後でデバイスとアプリケーションサーバーまたはコンテンツサーバー間で移動できます。BlackBerry Secure Connect Plus は、FIPS-140 認定 Certicom ライブラリを使用して、トラフィックの暗号化および復号化を行います。

データフロー：**BlackBerry Secure Gateway** の使用時における **iOS** デバイスのメールサーバーでの認証

このデータフローでは、iOS デバイスが Microsoft のモダン認証を使用して、BlackBerry Secure Gateway を介してメールサーバーで認証を受ける方法について説明します。



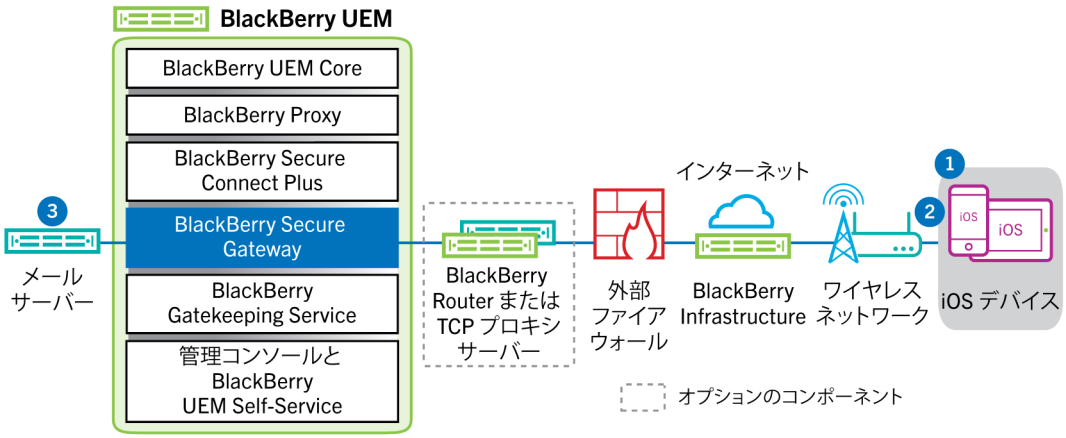
次の手順では、標準データフローについて説明します。Entra テナントの設定によっては、一部の詳細が異なる場合があります。Microsoft ID プロバイダーが認証要求を管理する方法の詳細については、Microsoft のドキュメントを参照してください。

1. BlackBerry Secure Gateway が、BlackBerry Secure Gateway 設定で指定された認証サーバー/ID プロバイダーから検出ドキュメントを取得し、キャッシュします。BlackBerry Secure Gateway は、iOS 13 デバイスのバージョン管理されていない検出ドキュメントに加えて、iOS 14.6 以降のデバイスの v2.0 検出ドキュメントを取得します。
2. デバイスが、BlackBerry Infrastructure 経由で BlackBerry Secure Gateway へのセキュリティ保護された接続を確立します。
3. BlackBerry Secure Gateway が、BlackBerry Secure Gateway 設定で指定された認証サーバー/ID プロバイダーとの間で TLS を確立します。
4. デバイスが、認証コード要求を BlackBerry Secure Gateway 経由で認証サーバー/ID プロバイダーに送信します。
5. 認証サーバー/ID プロバイダーが、302 HTTP リダイレクト応答をデバイスに返します。
6. デバイスが、リダイレクト応答で指定された URL に認証要求を送信します。その要求は、BlackBerry Secure Gateway を経由せずに転送されます。
7. 認証サーバー/ID プロバイダーが、ユーザー認証要求をデバイスに送信します。要求のタイプ（ログインページや Microsoft Authenticator アプリのプロンプトなど）とユーザー認証のメッセージフローは、Entra テナントの設定によって異なります。
8. ユーザーが、要求された資格情報を認証サーバー/ID プロバイダーに提供します。
9. ユーザー認証が完了すると、認証サーバー/ID プロバイダーが認証コードをデバイスに送信します。
10. デバイスが、BlackBerry Secure Gateway に認証サーバー/ID プロバイダーの検出ドキュメントを要求します。
11. BlackBerry Secure Gateway が、検出ドキュメントをデバイスへ送信します。
12. デバイスが、アクセストークン要求を BlackBerry Secure Gateway 経由で認証サーバー/ID プロバイダーに送信します。
13. 認証サーバー/ID プロバイダーが、デバイスにアクセストークンを送信します。
14. デバイスは、メールを送受信する際に、アクセストークンを提示して、メールサーバーへのセキュリティ保護された接続を確立します。

    アクセストークンの有効期限が切れると、デバイスは BlackBerry Secure Gateway 経由で新しいトークン要求を認証サーバー/ID プロバイダーに送信します。

データフロー：iOS を使用した BlackBerry Secure Gateway デバイスからのメールの送信

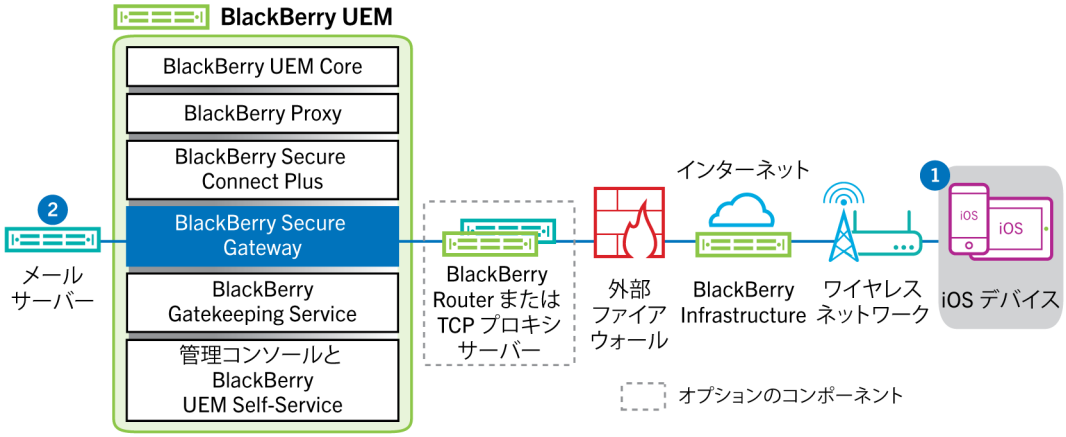
このデータフローは、仕事用メールとカレンダーデータが、BlackBerry Secure Gateway を使用して、iOS デバイスから Exchange ActiveSync サーバーへ移動する仕組みを説明しています。



1. ユーザーは、仕事用領域内でメールを作成するか、オーガナイザーアイテムを更新します。
2. デバイスは、BlackBerry Infrastructure と BlackBerry Secure Gateway を経由して、新規または変更されたアイテムをメールサーバーに送信します。
3. メールサーバーは、ユーザーのメールボックスのオーガナイザーデータを更新するか、メールアイテムを受信者に送信して、デバイスに確認を送信します。

データフロー：iOS を使用した BlackBerry Secure Gateway デバイスでのメールの受信

このデータフローは、仕事用メールとカレンダーデータが、BlackBerry Secure Gateway を使用して、iOS デバイスと Exchange ActiveSync サーバー間で移動する仕組みを説明しています。

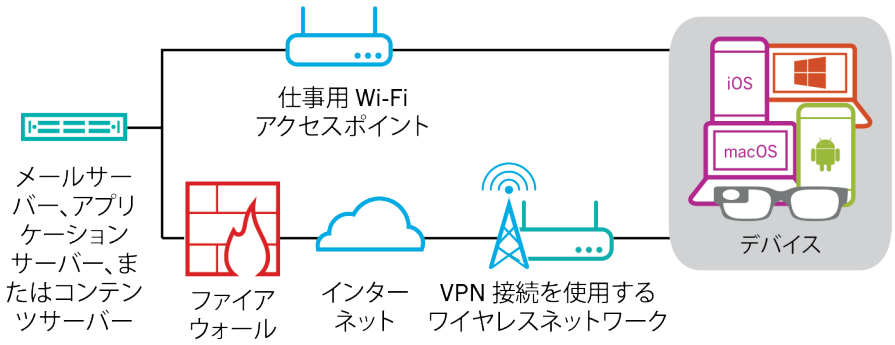


1. iOS 上のネイティブのメールクライアントは、BlackBerry Infrastructure と BlackBerry Secure Gateway の間にある暗号化された認証されたチャネルを介してメールサーバーとの永続的な接続を維持し、メールサーバーで同期用に設定されたフォルダーの変更を検出します。
2. 新規メールや更新されたカレンダーエントリなど、デバイスに新規または変更されたアイテムがある場合、メールサーバーは、Exchange ActiveSync プロトコルを使用し、BlackBerry Secure Gateway と BlackBerry Infrastructure の間のセキュリティ保護されたチャネルを経由して、デバイスのメールアプリやオーガナイザーアプリに更新を送信します。

VPN または仕事用 Wi-Fi ネットワークの使用による作業データの送受信

管理者またはユーザーによって VPN プロファイルまたは Wi-Fi プロファイルが設定されているデバイスは、組織の VPN または仕事用 Wi-Fi ネットワークを使用して組織のリソースにアクセスできる場合があります。MDM 制御 のアクティベーションタイプが設定された Android デバイスや、Samsung Knox Workspace デバイスのユーザーが組織の VPN を使用するには、各自のデバイスで VPN プロファイルを手動で設定する必要があります。

以下の図は、デバイスが組織の VPN または仕事用 Wi-Fi ネットワークを使用して組織のリソースに接続している場合に、データがどのように転送されるかを示しています。

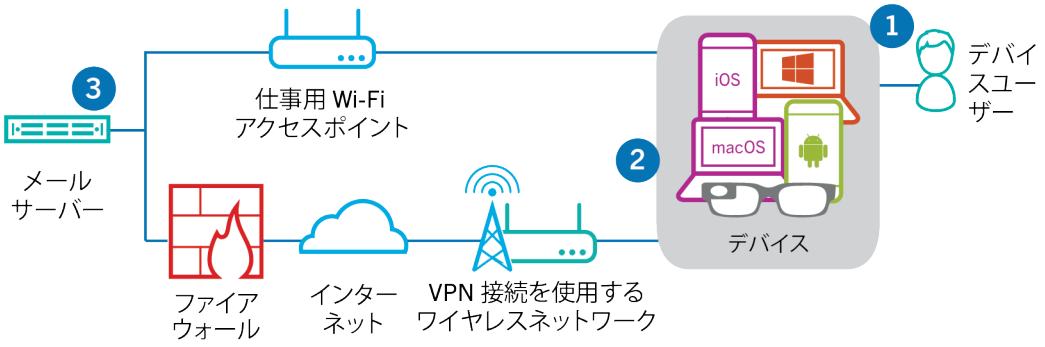


次の表は、デバイスがいつ組織の VPN または仕事用 Wi-Fi ネットワークを使用して、組織のネットワークに接続するのかを示したものです。

デバイスタイプ	説明
Android Enterprise デバイスと Knox Workspace デバイス	デフォルトでは、BlackBerry Secure Connect Plus が有効になっていない場合にのみ、Android Enterprise および Knox Workspace デバイスは組織の VPN または仕事用 Wi-Fi ネットワークを使用して仕事用データを送受信します。
Windows および macOS デバイス、および MDM 制御 のアクティベーションタイプが設定された Android デバイス	Windows および macOS デバイス、および MDM 制御 のアクティベーションタイプが設定された Android デバイスは、組織の VPN または仕事用 Wi-Fi ネットワークを使用して仕事用データを送受信します。Android デバイスのユーザーが組織の VPN を使用するには、各自のデバイスで VPN プロファイルを手動で設定する必要があります。
iOS	iOS デバイスは、BlackBerry Secure Gateway が有効になっていない場合に、組織の VPN または仕事用 Wi-Fi ネットワークを使用して Exchange ActiveSync データを送受信します。他のすべての仕事用データは、組織の VPN または仕事用の Wi-Fi ネットワークを使用します。

データフロー：VPN または仕事用 Wi-Fi ネットワークを使用してデバイスからメールを送信する

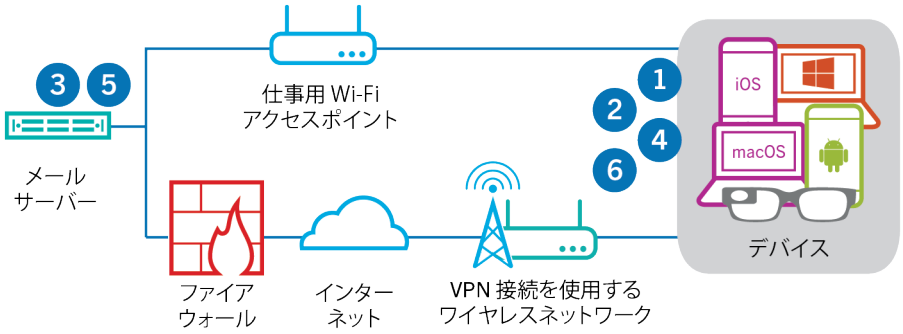
このデータフローは、Exchange ActiveSync を使用して、組織の VPN または仕事用 Wi-Fi ネットワーク経由でデバイスからメールサーバーへ仕事用メールとカレンダーデータが移動する仕組みを説明しています。



1. ユーザーは、仕事用領域内でメールを作成するか、オーガナイザーアイテムを更新します。
2. デバイスは、組織の VPN または仕事用 Wi-Fi ネットワーク経由で、新規または変更されたアイテムをメールサーバーへ送信します。
3. メールサーバーは、ユーザーのメールボックスのオーガナイザーデータを更新するか、メールアイテムを受信者に送信して、デバイスに確認を送信します。

データフロー：VPN または仕事用 Wi-Fi ネットワークを使用してデバイスでメールを受信する

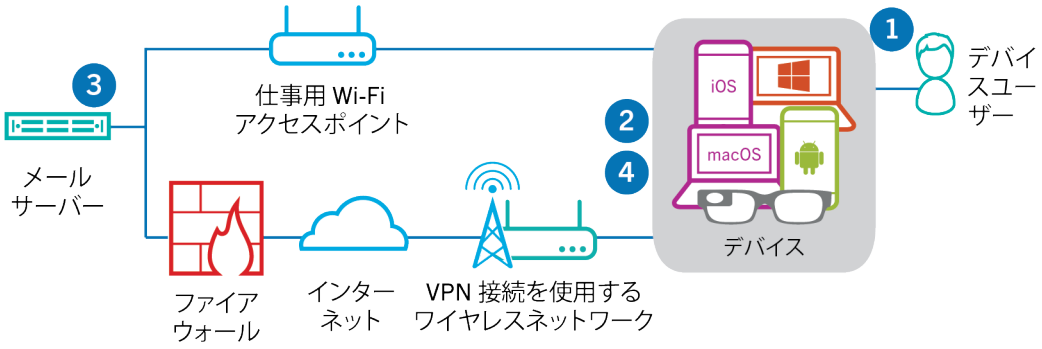
このデータフローは、Exchange ActiveSync を使用して、組織の VPN または仕事用 Wi-Fi ネットワーク経由でデバイスからメールサーバーへ仕事用メールとカレンダーデータが移動する仕組みを説明しています。



1. デバイスはメールサーバーに HTTPS 要求を発行し、同期設定されているフォルダー内のアイテムが変更された場合にメールサーバーがデバイスに通知するよう要求します。要求は、組織の VPN または仕事用 Wi-Fi ネットワーク経由でメールサーバーへ移動します。
2. デバイスは待機します。
3. 新規メールや更新されたカレンダーエントリなど、デバイスに新規または変更されたアイテムがある場合、メールサーバーは更新をデバイスに送信します。新規または変更されたアイテムは、組織の VPN または仕事用 Wi-Fi ネットワークを経由して、デバイスのメールまたはオーガナイザーデータアプリに移動します。
4. 同期が完了すると、デバイスは別の要求を発行して、プロセスを再度開始します。
5. この期間に新規または変更されたアイテムがない場合、メールサーバーまたはアプリケーションサーバーは Exchange ActiveSync プロトコルを使用してメッセージをデバイスに送信します。
6. デバイスは、新しい要求を発行して、プロセスを再度開始します。

データフロー：VPN または仕事用 Wi-Fi ネットワークを使用した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

このデータフローは、組織のアプリケーションまたはコンテンツサーバーとデバイス上のアプリとの間で、VPN 接続または仕事用 Wi-Fi ネットワークを使用してデータが移動する仕組みを説明しています。



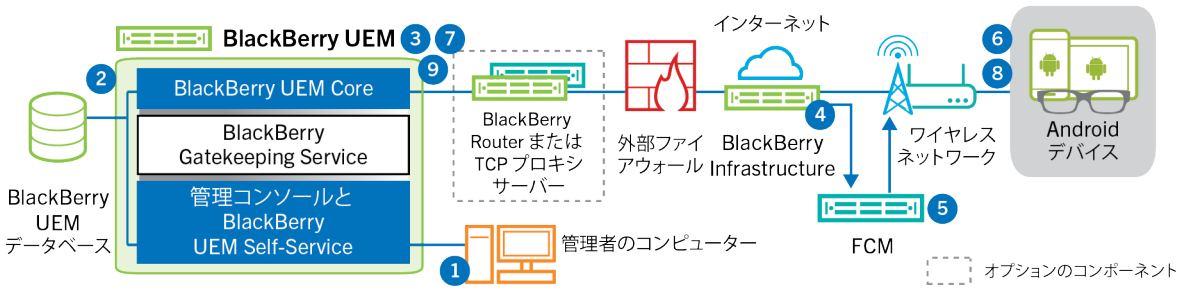
1. ユーザーは、仕事用アプリを開いて、仕事用データを表示します。たとえば、ユーザーは、仕事用ブラウザーを開き、イントラネット内を移動するか、社内で開発されたアプリを使用して組織の顧客データにアクセスします。
2. アプリは、アプリケーションまたはコンテンツサーバーとの接続を確立して、データを取得します。要求は、VPN または仕事用 Wi-Fi ネットワーク経由でアプリケーションまたはコンテンツサーバーへ移動します。
3. アプリケーションまたはコンテンツサーバーは、仕事用データで応答します。仕事用データは、VPN または仕事用 Wi-Fi ネットワークを通じて、デバイスの仕事用領域のアプリへ移動します。
4. アプリはデータを受信し、デバイス上に表示します。

データフロー：デバイス設定の更新の受信

管理コンソールを使用して、デバイスをロック、仕事用データを削除などのデバイスコマンドを送信する場合、または、ポリシー、プロファイル、アプリ設定または割り当てなどの他のデバイス管理タスクを実行する場合には、デバイスの設定の更新がトリガーされます。

このセクションでは、デバイスが設定の更新を受信したときに、データが組織の UEM 環境をどのように移動するかを詳細に示すデータフローを説明します。

データフロー：Android デバイスでの設定更新の受信



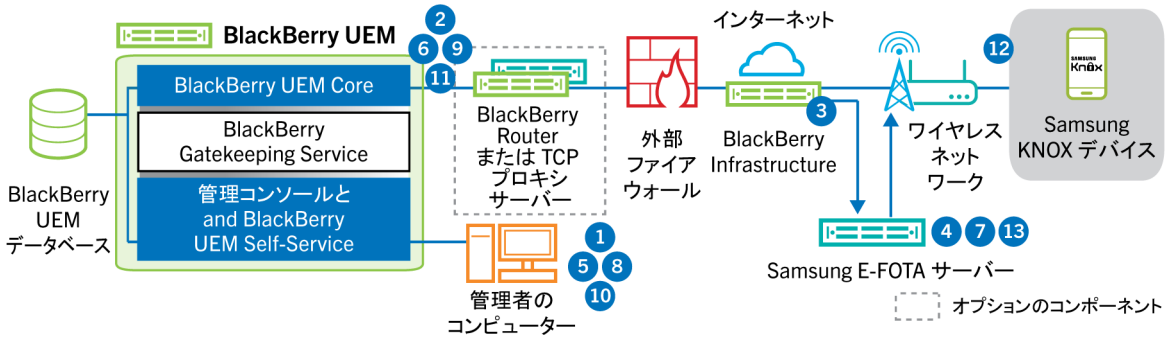
1. Android デバイス用の設定更新をトリガーするアクションは、管理コンソール内で実行されます。
2. 更新は、BlackBerry UEM と、識別されたデバイスと共有する必要のあるオブジェクトに適用されます。
3. BlackBerry UEM Core は、インストールされている場合は BlackBerry Router または TCP プロキシサーバー、およびポート 3101 を介した外部ファイアウォールを経由して BlackBerry Infrastructure に接続します。
4. BlackBerry Infrastructure は FCM を使用して、保留中の更新があることを Android デバイスに通知します。
5. FCM は通知を Android デバイス上の BlackBerry UEM Client に送信し、BlackBerry UEM Core に接続します。
6. BlackBerry UEM Client は、外部ファイアウォールのポート 3101 で BlackBerry UEM Core に接続し、デバイス上で実行する必要のある保留中のアクションとコマンドをリクエストします。
7. BlackBerry UEM Core は、BlackBerry Infrastructure および、インストールされている場合は BlackBerry Router または TCP プロキシサーバー経由で、優先度が最高のアクションで応答します。

   優先度は、デバイスデータを削除、デバイスをロックなどの IT 管理コマンドに付与され、次にデバイス情報のリクエスト、インストール済みアプリなどに付与されます。BlackBerry UEM Core は、一度に 1 つだけコマンドを送信します。必要に応じて、追加情報が応答に含まれます。
8. BlackBerry UEM Client は、応答を調べ、処理するコマンドをスケジュールして、コマンドの実行を待機します。BlackBerry UEM Client は、BlackBerry UEM Core 経由で BlackBerry Infrastructure へ応答を送信し、コマンドステータスを更新します。ステータスは、コマンドが正常に実行されたかどうかを示し、失敗した場合はエラーメッセージを提供します。
9. デバイスに対して保留中のアクションまたはコマンドがまだ残っている場合、BlackBerry UEM Core は BlackBerry Infrastructure 経由で、優先度が一番高いアクションを実行して応答します。デバイスに対して保留中のアクションまたはコマンドがない場合、BlackBerry UEM Core はアイドルコマンドで応答します。

   デバイスで実行する必要のある保留中のアクションまたはコマンドがなくなるまで、手順 7～9 を繰り返します。

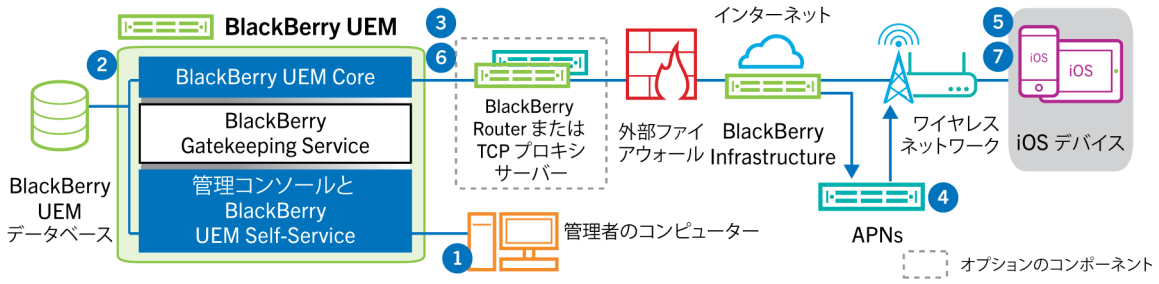
データフロー：Samsung Knox デバイスのファームウェアを更新する

このデータフローでは、Samsung Enterprise Firmware Over the Air を使用して Samsung からのファームウェア更新がデバイスにインストールされるタイミングを制御するときにどのようにデータが移動するかについて説明します。



1. 管理者が、Samsung E-FOTA 顧客 ID とライセンスキーを BlackBerry UEM に追加します。
2. BlackBerry UEM Core が、TLS 接続経由で BlackBerry Infrastructure にライセンス情報を送信します。
3. BlackBerry Infrastructure が Samsung E-FOTA サーバーと TLS 接続を確立し、顧客 ID とライセンスキーを提供します。
4. E-FOTA サーバーが、情報を検証し、BlackBerry Infrastructure 経由で BlackBerry UEM Core にライセンス情報を返します。
5. 管理者が、デバイス SR 要件プロファイルを作成し、新しい Samsung デバイスファームウェアルールの Samsung デバイスモデル、言語、および通信事業者を指定します。
6. BlackBerry UEM Core が、TLS 接続の BlackBerry Infrastructure を介して E-FOTA サーバーに接続し、指定された条件を E-FOTA サーバーに送信します。
7. E-FOTA サーバーが、条件を検証し、BlackBerry Infrastructure 経由で BlackBerry UEM Core にライセンス情報を返します。
8. 管理者が、新しいデバイス SR 要件プロファイルを保存します。
9. BlackBerry UEM Core が、TLS 接続の BlackBerry Infrastructure を介して E-FOTA サーバーに接続し、プロファイルを Samsung クラウドに送信します。
10. 管理者が、デバイス SR 要件プロファイルを 1 人または複数のユーザーに割り当てます。
11. BlackBerry UEM が、ユーザーの Samsung デバイス上の BlackBerry UEM Client にプロファイルを送信します。
12. Samsung デバイスが E-FOTA サーバーに登録されます。
13. デバイス SR 要件プロファイルで指定されたパラメーターを満たすファームウェア更新が利用可能な場合、E-FOTA サーバーはその更新をデバイスに送信します。

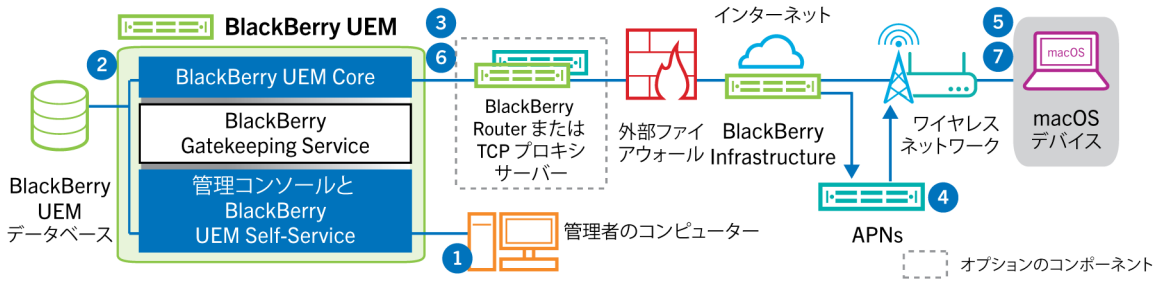
データフロー：iOS デバイスでの設定更新の受信



1. iOS デバイス用の設定更新をトリガーするアクションは、管理コンソール内で実行されます。たとえば、IT ポリシーを更新したり、新しいプロファイルまたはアプリをユーザーアカウントへ割り当てたりします。
2. 更新が BlackBerry UEM に適用され、デバイスと共有する必要のあるオブジェクトが識別されます。
3. BlackBerry UEM Core は、次の操作を実行します。
   a. BlackBerry Router または TCP プロキシサーバー（インストールされている場合）、および外部ファイアウォールのポート 3101 を経由して BlackBerry Infrastructure に接続します。
   b. BlackBerry Infrastructure を介して APN に要求を送信し、保留中の更新があることをデバイスに通知します。
4. APN は通知を iOS 上のネイティブ MDM Daemon に送信し、BlackBerry UEM Core に接続します。
5. iOS デバイス上のネイティブ MDM Daemon は、通知を受信すると、BlackBerry Router または TCP プロキシサーバー（インストールされている場合）を経由して、外部ファイアウォールのポート 3101 で BlackBerry UEM Core に接続し、保留中のアクションを取得します。
6. BlackBerry UEM Core は、優先度が最高のアクションで応答します。優先度は、デバイスデータを削除、デバイスをロックなどのデバイスのアクションに付与されます。BlackBerry UEM Core は、一度に 1 つだけコマンドを送信します。必要に応じて、追加情報が応答に含まれます。デバイスに対して保留中のアクションまたはコマンドがない場合、BlackBerry UEM Core はアイドルコマンドでデバイスに応答します。
7. iOS デバイスのネイティブ MDM Daemon が次の操作を実行します。
   a. BlackBerry UEM Core からの応答を調べ、処理するコマンドをスケジュールして、コマンドの実行を待機します。
   b. BlackBerry UEM Core へ応答を送信し、コマンドステータスを更新します。ステータスは、コマンドが正常に実行されたかどうかを示し、失敗した場合はエラーメッセージを提供します。

   デバイスで実行する必要のある保留中のアクションまたはコマンドがなくなるまで、手順 6 と 7 を繰り返します。

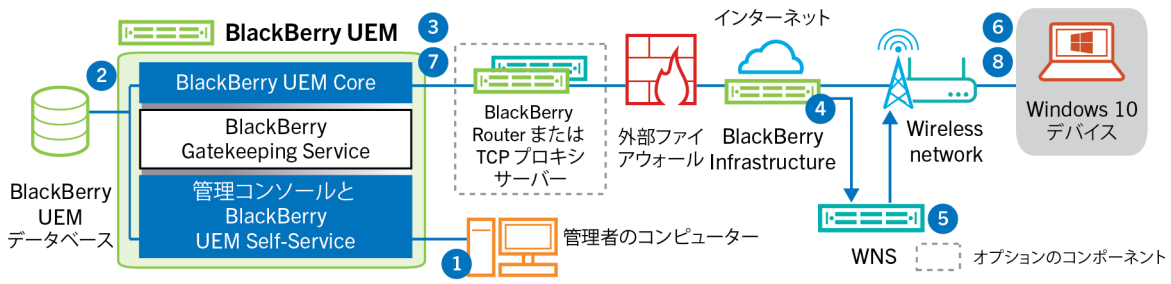
データフロー：macOS デバイスでの設定更新の受信



1. macOS デバイス用の設定更新をトリガーするアクションは、管理コンソール内で実行されます。たとえば、IT ポリシーを更新したり、新しいプロファイルまたはアプリをユーザーアカウントへ割り当てたりします。
2. 更新が BlackBerry UEM に適用され、デバイスと共有する必要のあるオブジェクトが識別されます。
3. BlackBerry UEM Core は、次の操作を実行します。
   a. BlackBerry Router または TCP プロキシサーバー（インストールされている場合）、および外部ファイアウォールのポート 3101 を経由して BlackBerry Infrastructure に接続します。
   b. BlackBerry Infrastructure を介して APN に要求を送信し、保留中の更新があることをデバイスに通知します。
4. APN は、BlackBerry UEM Core に接続するための通知をデバイスに送信します。
5. デバイスが通知を受信すると、BlackBerry UEM Core に接続し、外部ファイアウォールのポート 3101、BlackBerry Router または TCP プロキシサーバー（インストールされている場合）経由で、保留中のアクションを取得します。
6. デバイス用の保留中の更新がある場合、BlackBerry UEM Core は優先度が最高のアクションで応答します。優先度は、デバイスデータを削除、デバイスをロックなどのデバイスのアクションに付与されます。必要に応じて、追加情報が応答に含まれます。デバイスに対して保留中のアクションまたはコマンドがない場合、BlackBerry UEM Core は空のメッセージでデバイスに応答します。
7. デバイスが次の処理を実行します。
   a. BlackBerry UEM Core からの応答を調べ、処理するコマンドをスケジュールして、コマンドの実行を待機します。
   b. BlackBerry UEM Core へ応答を送信し、コマンドステータスを更新します。ステータスは、コマンドが正常に実行されたかどうかを示し、失敗した場合はエラーメッセージを提供します。

   デバイスで実行する必要のある保留中のアクションまたはコマンドがなくなるまで、手順 6 と 7 を繰り返します。

データフロー：Windows 10 デバイスでの設定更新の受信



1. Windows 10 デバイス用の設定更新をトリガーするアクションは、管理コンソール内で実行されます。たとえば、IT ポリシーを更新したり、新しいプロファイルまたはアプリをユーザーアカウントへ割り当てたりします。
2. 更新が BlackBerry UEM に適用され、デバイスと共有する必要のあるオブジェクトが識別されます。
3. BlackBerry UEM Core は、BlackBerry Router または TCP プロキシサーバー（インストールされている場合）、および外部ファイアウォールのポート 3101 を経由して BlackBerry Infrastructure に接続します。
4. BlackBerry Infrastructure は WNS を使用して、保留中の更新があることをデバイスに通知します。
5. WNS は、BlackBerry UEM Core に接続するための通知をデバイスに送信します。
6. デバイスが通知を受信すると、BlackBerry UEM Core に接続し、外部ファイアウォールのポート 3101、BlackBerry Router または TCP プロキシサーバー（インストールされている場合）経由で、保留中のアクションを取得します。
7. デバイス用の保留中の更新がある場合、BlackBerry UEM Core は優先度が最高のアクションで応答します。優先度は、デバイスデータを削除、デバイスをロックなどのデバイスのアクションに付与されます。必要に応じて、追加情報が応答に含まれます。デバイスに対して保留中のアクションまたはコマンドがない場合、BlackBerry UEM Core は空のメッセージでデバイスに応答します。
8. デバイスは、応答を調べ、処理するコマンドをスケジュールして、コマンドの実行を待機します。デバイスは、BlackBerry UEM Core へ応答を送信し、コマンドステータスを更新します。ステータスは、コマンドが正常に実行されたかどうかを示し、失敗した場合はエラーメッセージを提供します。

   デバイスで保留中のアクションまたはコマンドがなくなるまで、手順 7～8 を繰り返します。

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