BlackBerry UEM

アーキテクチャとデータフローリファレンスガイド

12.12

目次

BlackBerry UEM アーキテクチャとデータフロー..... 5
アーキテクチャ：BlackBerry UEM ソリューション..... 5

BlackBerry UEM コンポーネント..... 8

BlackBerry UEM の分散インストール..... 11

BlackBerry UEM 地域での導入.....15

デバイスおよび BlackBerry Dynamics アプリのアクティブ化..... 19
データフロー：管理対象 Android Enterprise アカウントを使用して 仕事用と個人用 - ユーザーのプライバシー Google Play デバイスをアクティブ化する.....19
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.....21
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..... 22
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..... 24
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.....26
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..... 28
データフロー：MDM 用 Android デバイスのアクティベーション..... 30
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.....32
データフロー：iOS デバイスのアクティベーション.....33
データフロー：macOS デバイスのアクティベーション..... 36
データフロー：Windows 10 デバイスのアクティベーション.....37
データフロー：BlackBerry 10 デバイスのアクティベーション..... 39
データフロー：BlackBerry Dynamics アプリのアクティベーション.....41
データフロー：BlackBerry Secure Connect Plus が有効になっているときに Samsung Knox Workspace デバイスで BlackBerry Dynamics アプリをアクティブ化する..... 43

仕事用データの送受信 45
BlackBerry Infrastructure の使用による仕事用データの送受信..... 46
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..... 47
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.....48

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 48
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 49
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 50
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 51
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 52
データフロー：BlackBerry 10 デバイスから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 53
データフロー：BlackBerry 10 デバイスからのメールの送信 53
データフロー：BlackBerry 10 デバイスでのメールの受信 53
データフロー：BlackBerry 10 デバイスでのエンタープライズプッシュ更新の受信 54
VPN または仕事用 Wi-Fi ネットワークの使用による仕事用データの送受信 56
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 57
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 57
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 58

デバイス設定の更新の受信 59
データフロー：Android デバイスでの設定更新の受信 60
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 61
データフロー：iOS デバイスでの設定更新の受信 62
データフロー：macOS デバイスでの設定更新の受信 63
データフロー：Windows 10 デバイスでの設定更新の受信 63
データフロー：BlackBerry 10 デバイスでの設定更新の受信 64

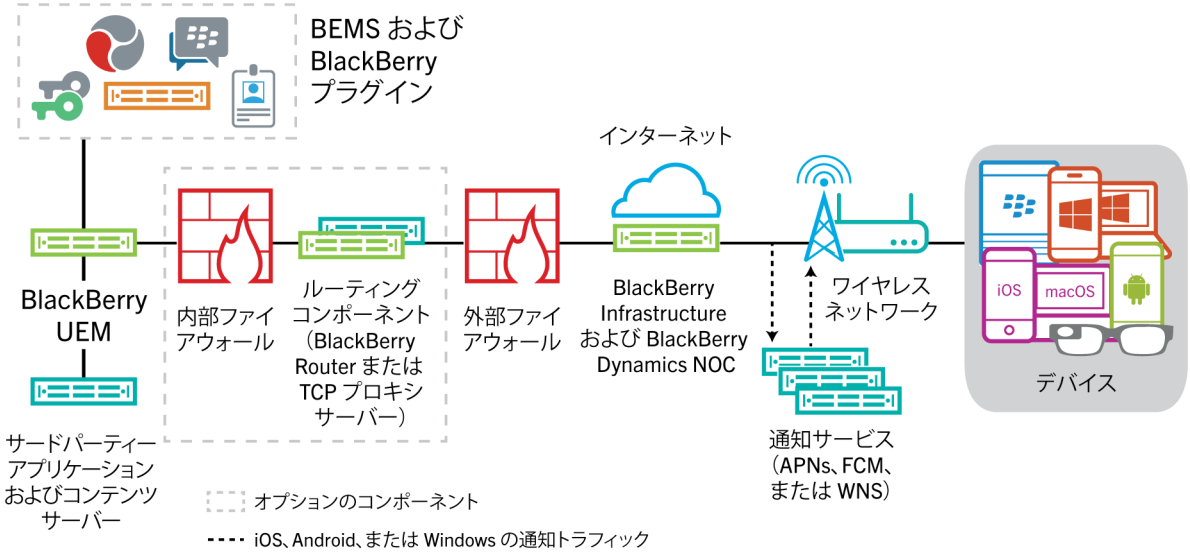
商標などに関する情報 66

BlackBerry UEM アーキテクチャとデータフロー

BlackBerry UEM は、BlackBerry の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、アプリケーション、コンテンツの包括的な管理を提供し、組織での iOS、macOS、Android、Windows 10、および BlackBerry 10 デバイスの管理に役立ちます。

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



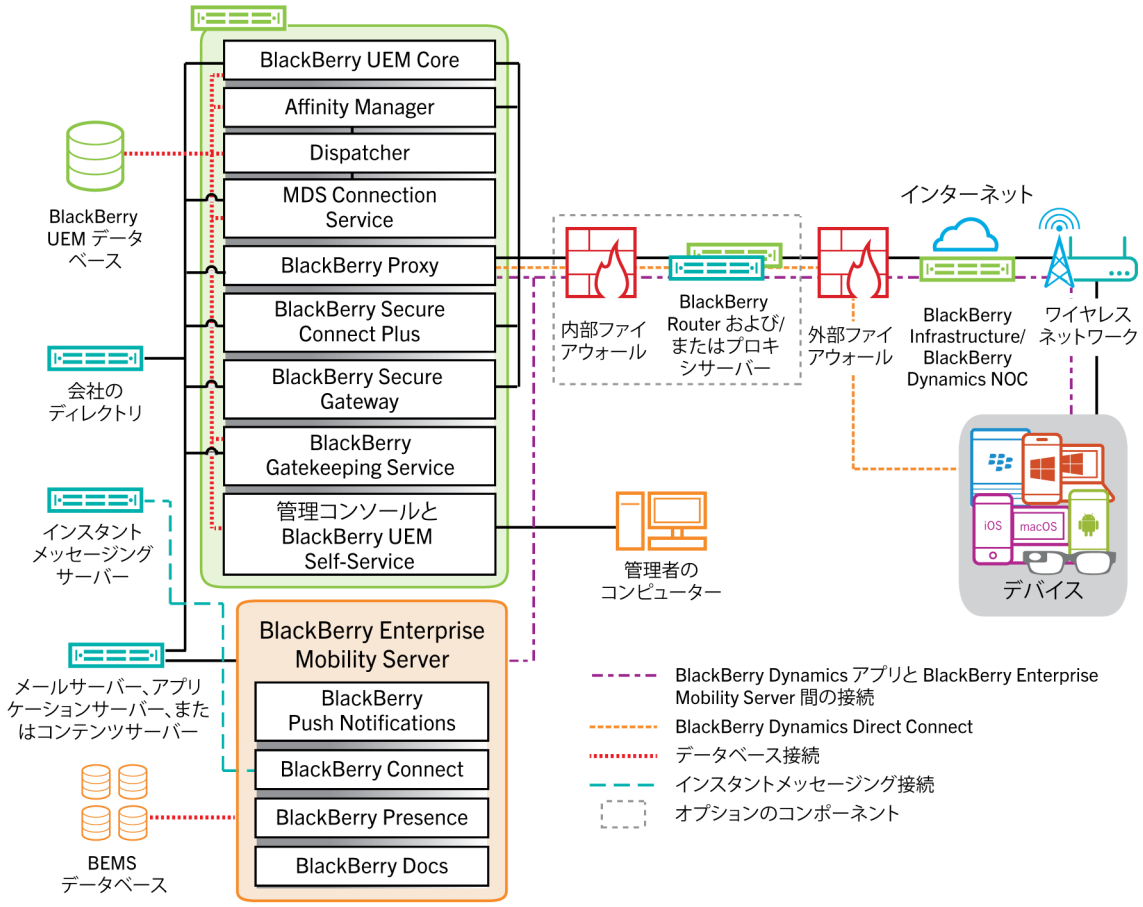
コンポーネント	説明
BlackBerry UEM	BlackBerry UEM は、統合エンドポイント管理ソリューションです。このソリューションでは、セキュリティと接続が統合されており、マルチプラットフォームデバイス、アプリケーション、およびコンテンツを包括的に管理することができます。

コンポーネント	説明
BlackBerry Infrastructure	BlackBerry Infrastructure は、複数の地域に分散されたグローバルなプライベートデータネットワークで、世界中の数千の組織と数百万のユーザー間のデータ転送を可能にし、データをセキュリティ保護します。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。 BlackBerry 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、BlackBerry UEM の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。デバイスと BlackBerry UEM の間で送信されるデータを保護するエンドツーエンド暗号化により、BlackBerry UEM は BlackBerry Infrastructure への一定の接続を維持します。これにより、組織はユーザーにデータを送信するために、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を必要とします。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 BlackBerry UEM の間で移動するすべてのデータが認証され暗号化されます。
BlackBerry Dynamics NOC	BlackBerry Dynamics NOC とは、デバイスおよび BlackBerry UEM と BlackBerry Enterprise Mobility Server で BlackBerry Dynamics アプリ間のセキュリティ保護された通信を提供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、Windows 10、および BlackBerry 10 デバイスをサポートします。
通知サービス	BlackBerry UEM は、通知をデバイスに送信して更新のために BlackBerry 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。

コンポーネント	説明
ルーティングコンポーネント	デフォルトでは、BlackBerry 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。ただし、組織のセキュリティポリシーによって、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、BlackBerry Infrastructure とすべてのデバイスの間の BlackBerry UEM 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。 組織に既に TCP プロキシサーバーがインストールされているか、または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	BlackBerry UEM は、BlackBerry Enterprise Identity、BlackBerry 2FA 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。 BlackBerry Enterprise Mobility Server は、BlackBerry Dynamics アプリとの間で仕事用データを送信するために使用される複数のサービスを提供します。

BlackBerry UEM 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。



コンポーネント間の接続に使用されるポートについては、計画関連の資料の「ポートを設定する」を参照してください。

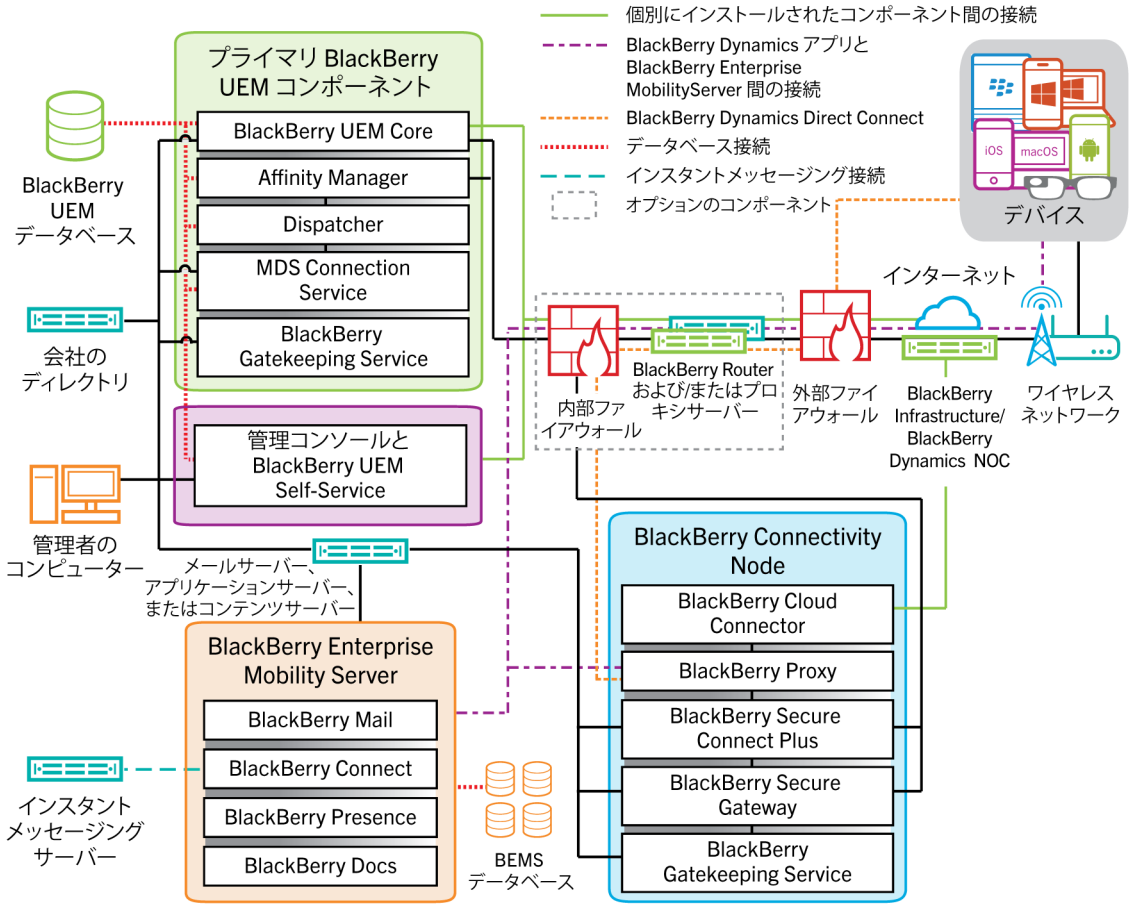
コンポーネント名	説明
BlackBerry UEM Core	BlackBerry UEM Core は BlackBerry UEM アーキテクチャの中心的なコンポーネントです。これは、以下を担当するいくつかのサブコンポーネントで構成されています。 • ログ、監視、レポート、および管理機能 • 認証および認証サービス • コマンド、IT ポリシー、およびプロファイルのスケジュールとデバイスへの送信 • ユーザー、ポリシー、およびその他の設定データをデバイス上の BlackBerry Dynamics アプリに送信

コンポーネント名	説明
BlackBerry UEM データベース	BlackBerry UEM データベースは、BlackBerry 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 MDS Connection Service	BlackBerry MDS Connection Service は、BlackBerry 10 デバイスが仕事用 Wi-Fi ネットワークに接続していないか、VPN 接続を使用していない場合に、そのデバイス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接続を提供します。
BlackBerry Dispatcher	BlackBerry Dispatcher は BlackBerry 10 IPPP を使用してデバイス用のセキュリティ保護された接続を提供します。
BlackBerry Affinity Manager	BlackBerry Affinity Manager は、デバイスが BlackBerry 10 を使用していないときに、BlackBerry Infrastructure デバイスと BlackBerry Secure Connect Plus の間でアクティブな SRP 接続を維持する責任を担います。
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。
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用に確立されます。
BlackBerry Secure Gateway	BlackBerry Secure Gateway は、BlackBerry Infrastructure および BlackBerry UEM を介して、iOS デバイスに対し、組織のメールサーバーへの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 Exchange ActiveSync 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、BlackBerry UEM 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、BlackBerry 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。
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、BlackBerry 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、BlackBerry 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。

コンポーネント名	説明
BlackBerry Enterprise Mobility Server	BEMS は、BlackBerry Dynamics、BlackBerry Push Notifications、BlackBerry Connect、BlackBerry Presence などの BlackBerry Docs アプリとの間で仕事用データを送信するために使用する複数のサービスを統合します。
BlackBerry Enterprise Mobility Server データベース	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。
BlackBerry Push Notifications	BlackBerry Push Notifications は、iOS 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	BlackBerry Connect は、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 および Android デバイスに提供します。
BlackBerry Presence	BlackBerry Presence は、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	BlackBerry Docs では、VPN ソフトウェア、ファイアウォールの再設定、または重複したデータの保存を必要とせずに、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。
BlackBerry Router および/またはプロキシサーバー	デフォルトでは、BlackBerry 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ポリシーで、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。 BlackBerry 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、BlackBerry UEM の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 BlackBerry UEM Core、BlackBerry Proxy および BlackBerry Enterprise Mobility Server 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。

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 BlackBerry 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。



コンポーネント間の接続に使用されるポートについては、計画関連の資料の「ポートを設定する」を参照してください。

コンポーネント名	説明
プライマリ BlackBerry UEM コンポーネント	プライマリ BlackBerry 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。

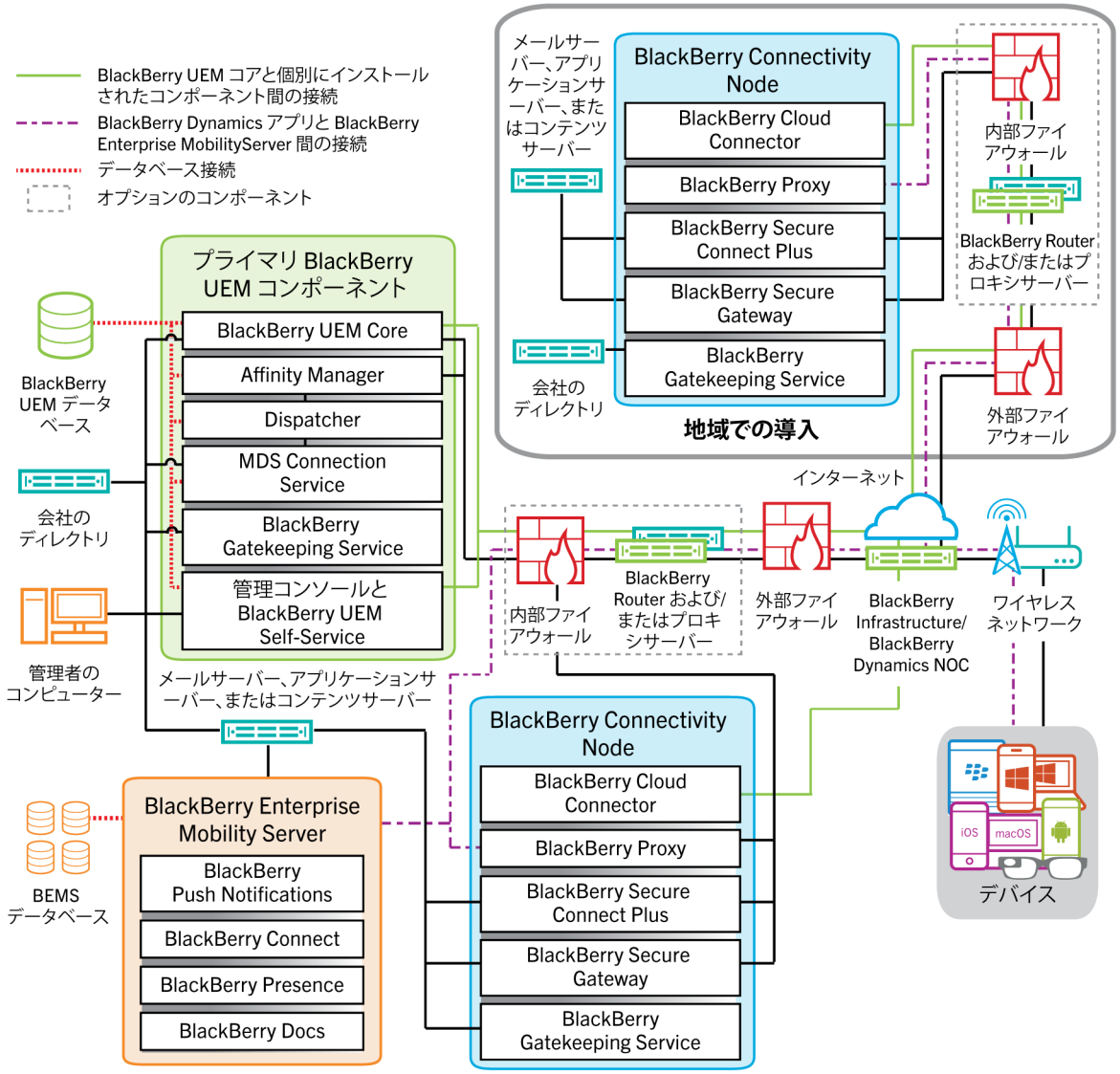
コンポーネント名	説明
BlackBerry UEM Core	BlackBerry UEM Core は BlackBerry UEM アーキテクチャの中心的なコンポーネントです。これは、以下を担当するいくつかのサブコンポーネントで構成されています。 • ログ、監視、レポート、および管理機能 • 認証および認証サービス • コマンド、IT ポリシー、およびプロファイルのスケジュールとデバイスへの送信 • ユーザー、ポリシー、およびその他の設定データをデバイス上の BlackBerry Dynamics アプリに送信
BlackBerry UEM データベース	BlackBerry UEM データベースは、BlackBerry 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 MDS Connection Service	BlackBerry MDS Connection Service は、BlackBerry 10 デバイスが仕事用 Wi-Fi ネットワークに接続していないか、VPN 接続を使用していない場合に、そのデバイス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接続を提供します。
BlackBerry Dispatcher	BlackBerry Dispatcher は BlackBerry 10 IPPP を使用してデバイス用のセキュリティ保護された接続を提供します。
BlackBerry Affinity Manager	BlackBerry Affinity Manager は、デバイスが BlackBerry 10 を使用していないときに、BlackBerry Infrastructure デバイスと BlackBerry Secure Connect Plus の間でアクティブな SRP 接続を維持する責任を担います。
BlackBerry Gatekeeping Service （プライマリ）	BlackBerry Gatekeeping Service は、デバイスが Exchange ActiveSync 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、BlackBerry UEM 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、BlackBerry UEM 管理コンソールを通じて、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。
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 BlackBerry 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	BlackBerry Management Console Core は、管理アクティビティに固有のサブタスクを処理します。

コンポーネント名	説明
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、BlackBerry 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 BlackBerry UEM 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、BlackBerry 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、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 Connectivity Node	BlackBerry Connectivity Node は BlackBerry UEM とは異なるサーバー上の組織のドメインに BlackBerry UEM Core 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 Proxy • BlackBerry Secure Connect Plus • BlackBerry Secure Gateway • BlackBerry Gatekeeping Service
BlackBerry Cloud Connector	BlackBerry Cloud Connector は、BlackBerry Connectivity Node コンポーネントが BlackBerry UEM Core と通信することを許可します。BlackBerry Cloud Connector と BlackBerry UEM Core の間のすべての通信は BlackBerry Infrastructure を通過します。
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。
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用に確立されます。
BlackBerry Secure Gateway	BlackBerry Secure Gateway は、BlackBerry Infrastructure および BlackBerry UEM を介して、iOS デバイスに対し、組織のメールサーバーへのセキュリティ保護された接続を提供します。

コンポーネント名	説明
BlackBerry Gatekeeping Service （BlackBerry Connectivity Node）	BlackBerry UEM は、BlackBerry Connectivity Node とインストールされている BlackBerry Gatekeeping Service のインスタンスを使用して、メールサーバーのゲートキーピングを管理できます。各インスタンスは、組織のゲートキーピングサーバーにアクセスできる必要があります。 プライマリ BlackBerry Gatekeeping Service コンポーネントにインストールされている BlackBerry UEM 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 Gatekeeping Service の BlackBerry Connectivity Node を無効にすることができます。
BlackBerry Enterprise Mobility Server	BEMS は、BlackBerry Dynamics、BlackBerry Push Notifications、BlackBerry Connect、BlackBerry Presence などの BlackBerry Docs アプリとの間で仕事用データを送信するために使用する複数のサービスを統合します。
BlackBerry Enterprise Mobility Server データベース	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。
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、BlackBerry UEM の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 BlackBerry UEM Core、BlackBerry Proxy および BlackBerry Enterprise Mobility Server 間のセキュリティ保護された通信を提供する、別々に配置された NOC です。

BlackBerry UEM 地域での導入

この図は、BlackBerry Connectivity Node の 1 つまたは複数のインスタンスが別の場所にインストールされている場合、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。サーバーグループを使用して、デバイスの接続先の BlackBerry Connectivity Node の地域インスタンスを指定することができます。



コンポーネント間の接続に使用されるポートについては、計画関連の資料の「ポートを設定する」を参照してください。

コンポーネント名	説明
プライマリ BlackBerry UEM コンポーネント	プライマリ BlackBerry 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。

コンポーネント名	説明
BlackBerry UEM Core	BlackBerry UEM Core は BlackBerry 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
BlackBerry UEM データベース	BlackBerry UEM データベースは、BlackBerry 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 MDS Connection Service	BlackBerry MDS Connection Service は、BlackBerry 10 デバイスが仕事用 Wi-Fi ネットワークに接続していないか、VPN 接続を使用していない場合に、そのデバイス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接続を提供します。
BlackBerry Dispatcher	BlackBerry Dispatcher は BlackBerry 10 IPPP を使用してデバイス用のセキュリティ保護された接続を提供します。
BlackBerry Affinity Manager	BlackBerry Affinity Manager は、デバイスが BlackBerry 10 を使用していないときに、BlackBerry Infrastructure デバイスと BlackBerry Secure Connect Plus の間でアクティブな SRP 接続を維持する責任を担います。
BlackBerry Gatekeeping Service （プライマリ）	BlackBerry Gatekeeping Service は、デバイスが Exchange ActiveSync 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、BlackBerry UEM 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、BlackBerry UEM 管理コンソールを通じて、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。
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、BlackBerry 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 BlackBerry UEM 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、BlackBerry 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、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。

コンポーネント名	説明
BlackBerry Connectivity Node	BlackBerry Connectivity Node は BlackBerry UEM とは異なるサーバー上の組織のドメインに BlackBerry UEM Core 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 Proxy • BlackBerry Secure Connect Plus • BlackBerry Secure Gateway • BlackBerry Gatekeeping Service BlackBerry Connectivity Node の地域での導入がある場合、BlackBerry UEM Core とその地域 BlackBerry Connectivity Node を含むサーバーグループとの間の接続を設定する必要があります。
BlackBerry Cloud Connector	BlackBerry Cloud Connector は、BlackBerry Connectivity Node コンポーネントが BlackBerry UEM Core と通信することを許可します。BlackBerry Cloud Connector と BlackBerry UEM Core の間のすべての通信は BlackBerry Infrastructure を通過します。
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。
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用に確立されます。
BlackBerry Secure Gateway	BlackBerry Secure Gateway は、BlackBerry Infrastructure および BlackBerry UEM を介して、iOS デバイスに対し、組織のメールサーバーへのセキュリティ保護された接続を提供します。
BlackBerry Gatekeeping Service （BlackBerry Connectivity Node）	BlackBerry UEM は、BlackBerry Connectivity Node とインストールされている BlackBerry Gatekeeping Service のインスタンスを使用して、メールサーバーのゲートキーピングを管理できます。各インスタンスは、組織のゲートキーピングサーバーにアクセスできる必要があります。 プライマリ BlackBerry Gatekeeping Service コンポーネントにインストールされている BlackBerry UEM 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 Gatekeeping Service の BlackBerry Connectivity Node を無効にすることができます。
BlackBerry Enterprise Mobility Server	BEMS は、BlackBerry Dynamics、BlackBerry Push Notifications、BlackBerry Connect、BlackBerry Presence などの BlackBerry Docs アプリとの間で仕事用データを送信するために使用する複数のサービスを統合します。

コンポーネント名	説明
BlackBerry Enterprise Mobility Server データベース	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。
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、BlackBerry UEM の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 BlackBerry UEM Core、BlackBerry Proxy および BlackBerry Enterprise Mobility Server 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。

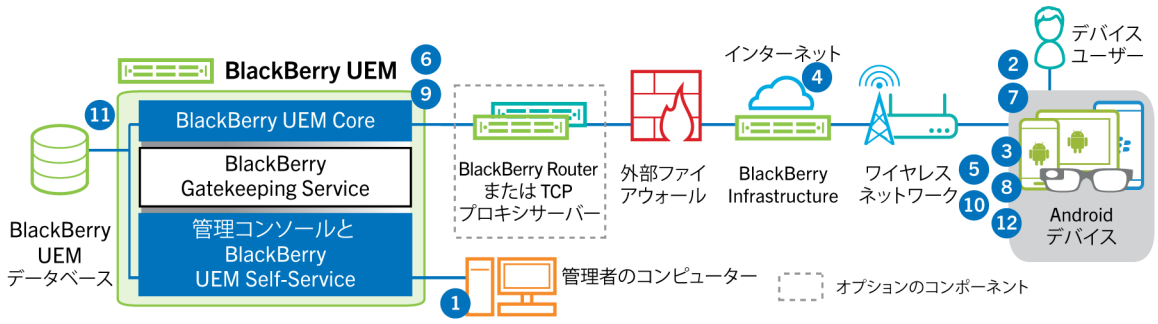
デバイスおよび BlackBerry Dynamics アプリのアクティブ化

ユーザーが BlackBerry UEM でデバイスをアクティブ化すると、管理者がデバイスを管理でき、ユーザーがデバイス上の仕事用データにアクセスできるように、デバイスを BlackBerry UEM に関連付けます。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の詳細については、管理関連の資料の「デバイスアクティベーション」を参照してください。

指定するデバイスのタイプとアクティベーションのタイプにより、デバイスと BlackBerry UEM は、設定および仕事用データをデバイスに送信する前に、アクティベーションプロセス中に複数の手順を完了して、相互に認証し、通信チャンネルをセキュリティ保護し、必要な場合には、仕事用領域を作成するか、またはデバイスを暗号化する必要があります。デバイスをアクティブ化する手順については、管理関連の資料の「デバイスをアクティブ化する手順」を参照してください。

BlackBerry Dynamics アプリは、デバイス上の仕事用リソースへのアクセスを提供します。デバイスに BlackBerry Dynamics アプリをインストールした後、仕事用リソースに安全にアクセスできるように、アプリをアクティブ化する必要もあります。BlackBerry Dynamics のアクティブ化の詳細については、管理関連の資料の「BlackBerry Dynamics アプリのアクセスキーの生成」を参照してください。

データフロー：管理対象 Android Enterprise アカウントを使用して 仕事用と個人用 - ユーザーのプライバシー Google Play 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。詳細については、管理関連の資料を参照してください。

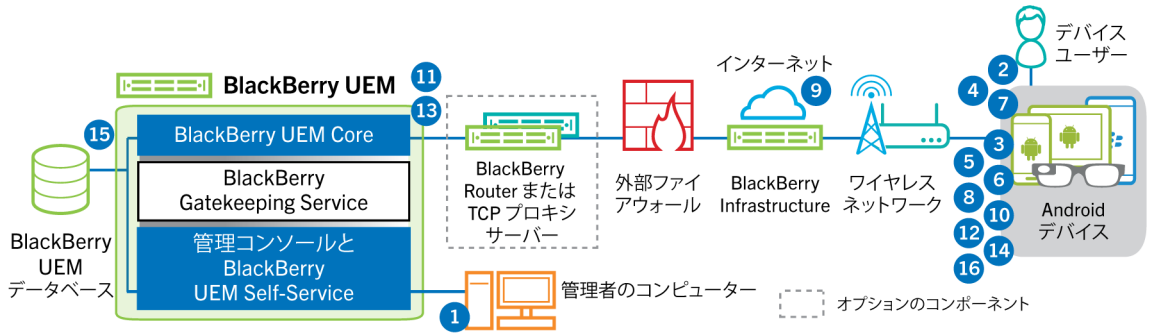
1. 次の操作を実行します。
   a. ユーザーをローカルユーザーアカウントとして、または会社のディレクトリから取得したアカウント情報を使用して、BlackBerry UEM に追加します。
   b. 「仕事用と個人用 - ユーザーのプライバシー 」アクティベーションタイプがユーザーに割り当てられていることを確認します。
   c. 次のいずれかのオプションを使用してユーザーにアクティベーションの詳細情報を提供する
      - デバイスアクティベーションパスワードと、オプションとして、QR Code を自動生成して、アクティベーションの手順を記載したメールを送信する

- 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. 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、監視対象の Google Play ユーザーを作成する
   c. デバイスインスタンスを作成する
   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 セッションに追加する
   f. ユーザーの監視対象 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、次の操作を実行します。
   a. Google に接続してユーザーを確認する
   b. デバイス上に仕事用プロファイルを作成する
   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要求を BlackBerry UEM へ送信する
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。
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



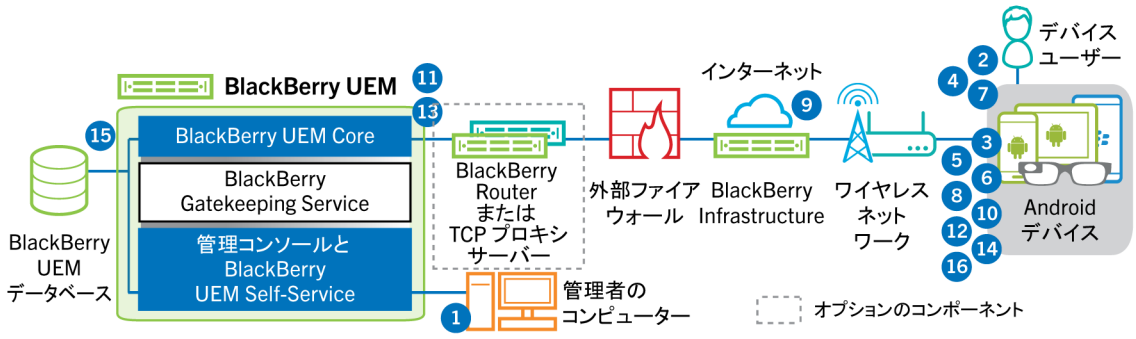
このデータフローは、BlackBerry UEM に Google Play アカウントの管理を許可する場合に適用されます。詳細については、管理関連の資料を参照してください。

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. ユーザーのアクティベーションパスワードを設定
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 ユーザー名の代わりに `afw#blackberry` を入力します。
5. デバイスが次の処理を実行します。
   a. デバイスの暗号化を求めるプロンプトを表示して、再起動する
   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
9. 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 サーバーアドレスを取得する
   c. BlackBerry UEM Client にサーバーアドレスを送信する

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、監視対象の Google Play ユーザーを作成する
    c. デバイスインスタンスを作成する
    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 セッションに追加する
    f. ユーザーの監視対象 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する
12. BlackBerry UEM Client は、次の操作を実行します。
    a. Google に接続してユーザーを確認する
    b. デバイス上に仕事用プロファイルを作成する
    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要求を BlackBerry UEM へ送信する
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。
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：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



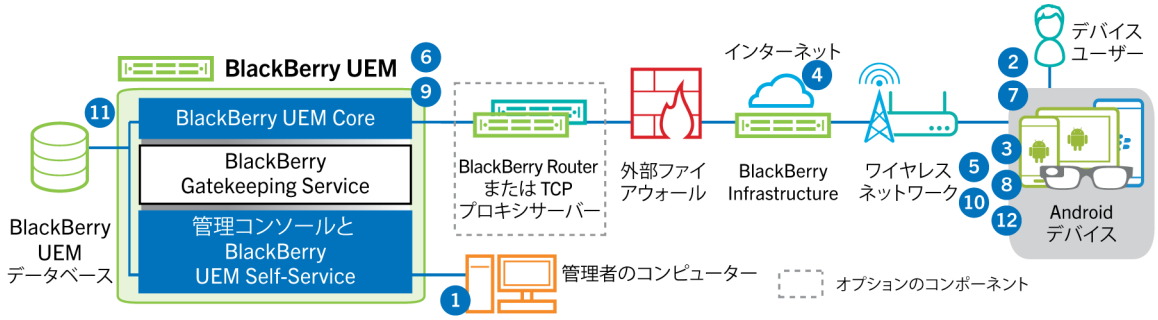
このデータフローは、BlackBerry UEM に Google Play アカウントの管理を許可する場合に適用されます。詳細については、管理関連の資料を参照してください。

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
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 ユーザー名の代わりに `afw#blackberry` 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
9. 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 サーバーアドレスを取得する
   c. BlackBerry UEM Client にサーバーアドレスを送信する
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、監視対象の Google Play ユーザーを作成する
   c. デバイスインスタンスを作成する
   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 セッションに追加する
   f. ユーザーの監視対象 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する
12. BlackBerry UEM Client は、次の操作を実行します。
   a. Google に接続してユーザーを確認する
   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要求を BlackBerry UEM へ送信する
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。

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



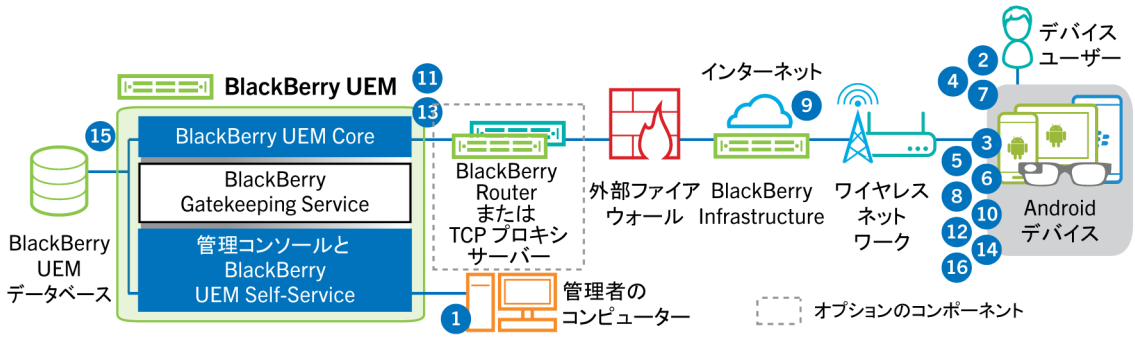
このデータフローは、BlackBerry UEM が Google Cloud または G Suite ドメインに接続されている場合に適用されます。詳細については、管理関連の資料を参照してください。

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. 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する
   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 セッションに追加する
   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、次の操作を実行します。
   a. デバイス上に仕事用プロファイルを作成する
   b. Google アカウント情報の入力を求めるプロンプトを表示する
   c. 監視対象の Google ドメインに接続して、ユーザーを認証する
   d. デバイス上に仕事用プロファイルを作成する
   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要求を BlackBerry UEM へ送信する
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。
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、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：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



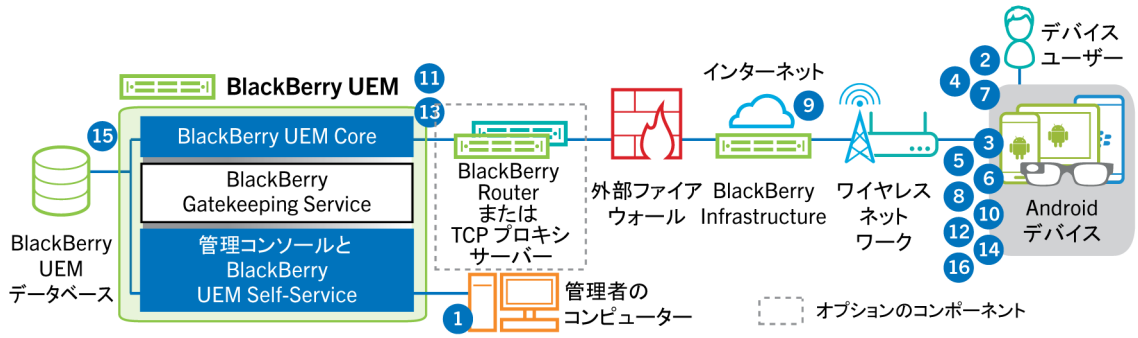
このデータフローは、BlackBerry UEM が Google Cloud または G Suite ドメインに接続されている場合に適用されます。詳細については、管理関連の資料を参照してください。

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
9. 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 サーバーアドレスを取得する
   c. BlackBerry UEM Client にサーバーアドレスを送信する
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する
   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 セッションに追加する
   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、次の操作を実行します。
   a. デバイス上に仕事用プロファイルを作成する
   b. Google アカウント情報の入力を求めるプロンプトを表示する
   c. Google ドメインに接続して、ユーザーを認証する
   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要求を BlackBerry UEM へ送信する
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。
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、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



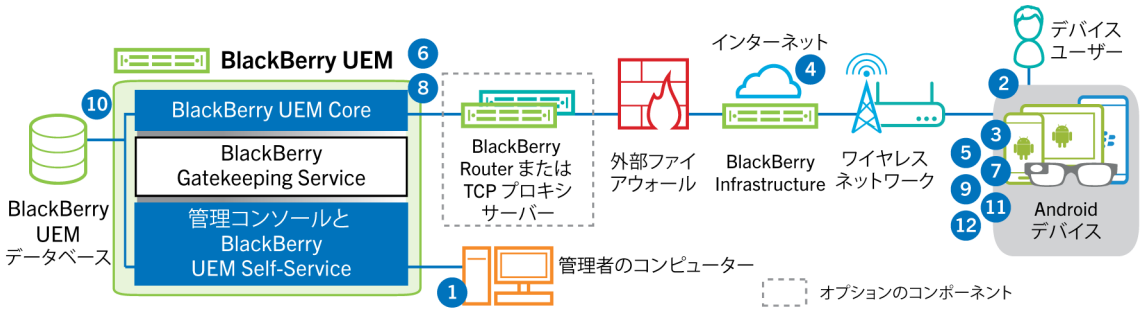
このデータフローは、BlackBerry UEM が Google Cloud または G Suite ドメインに接続されている場合に適用されます。詳細については、管理関連の資料を参照してください。

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
9. 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 サーバーアドレスを取得する
   c. BlackBerry UEM Client にサーバーアドレスを送信する
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する
   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 セッションに追加する
   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、次の操作を実行します。
   a. Google アカウント情報の入力を求めるプロンプトを表示する
   b. Google ドメインに接続して、ユーザーを認証する
   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要求を BlackBerry UEM へ送信する
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。
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、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：MDM 用 Android デバイスのアクティベーション



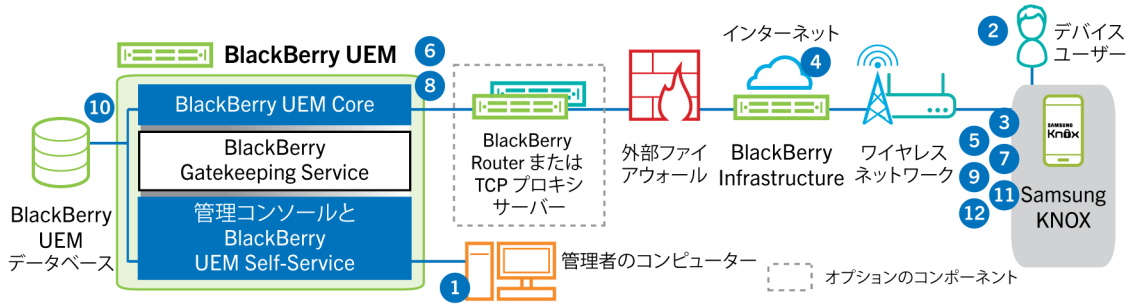
MDM 制御 アクティベーションタイプは、Android 10 を使用するデバイスでは推奨されません。MDM 制御 アクティベーションタイプで Android 10 以降のデバイスをアクティベーションしようとすると失敗します。詳細については、https://support.blackberry.com/community にアクセスし、記事 48386 を参照してください。

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. 「MDM 制御 」のアクティベーションの種類を指定するアクティベーションプロファイル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 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. デバイスの BlackBerry UEM Client が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 MDM を使用して、サポートされる MDM 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 MDM 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され、Knox 管理ライセンスがアクティブ化されます。アクティブ化された後、BlackBerry UEM Client は BlackBerry UEM から Knox MDM 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。

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。

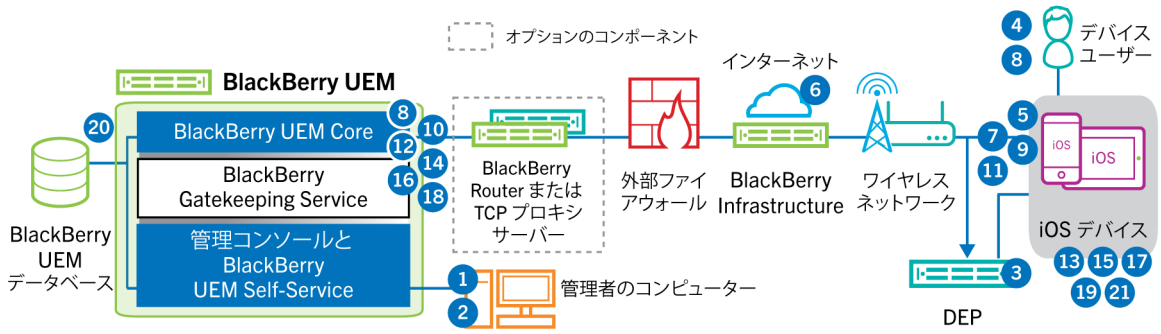
   a. クライアント証明書要求を HTTP セッションの登録セッション ID と照合して検証する
   b. ルート証明書を使用してクライアント証明書要求に署名する
   c. 署名されたクライアント証明書とルート証明書を BlackBerry UEM Client に返送する

   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

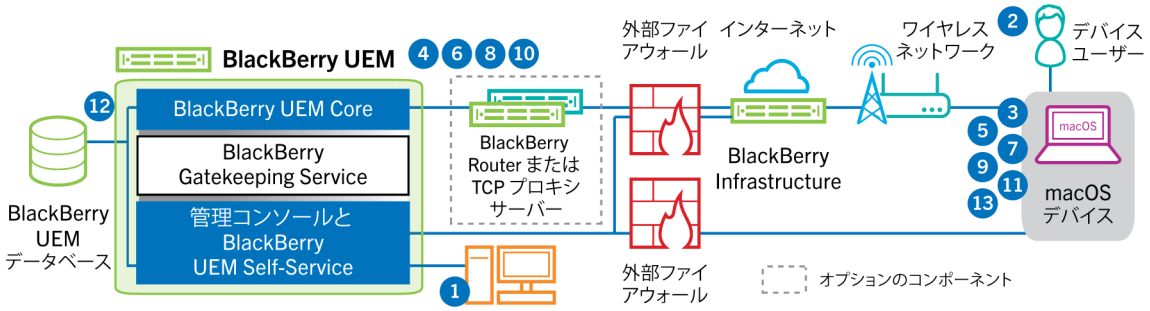
3. デバイスが Apple DEP に登録されている場合には、デバイスは初期セットアップ中に Apple DEP Web サービスと通信します。デバイスが BlackBerry UEM Client アプリをインストールするように設定した場合は、デバイスはダウンロードおよびインストールを自動的に実行します。
4. デバイスが Apple DEP に登録されていない場合、および BlackBerry UEM Client をインストールするようにデバイスを設定していない場合は、ユーザーが手動で BlackBerry UEM Client をデバイスにダウンロードおよびインストールします。インストール後に、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。

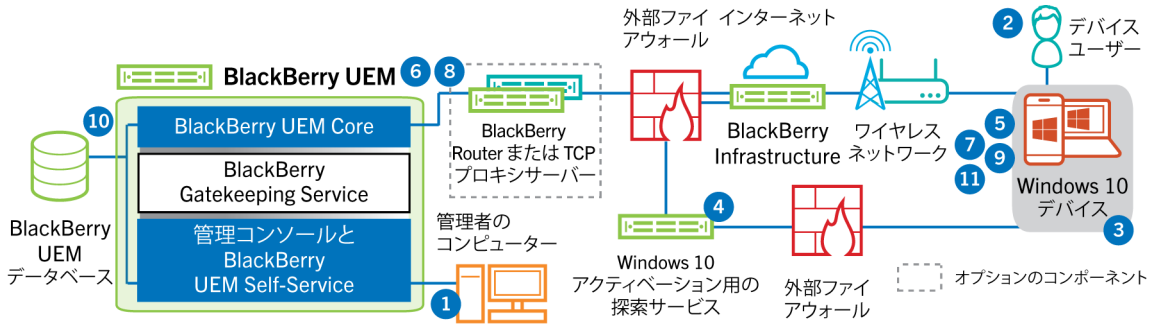
13. デバイス上のネイティブ MDM Daemon は、顧客 ID、言語、および OS バージョンを含むデバイスプロファイルを BlackBerry UEM に送信します。
14. BlackBerry UEM は、要求が CA によって署名されていることを検証し、ネイティブ MDM Daemon に正常に認証されたことを示す通知で応答します。
15. ネイティブ MDM Daemon は、CA 証明書、CA 機能情報、およびデバイスが発行した証明書を求める要求を BlackBerry UEM に送信します。
16. BlackBerry UEM は、CA 証明書、CA 機能情報、およびデバ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



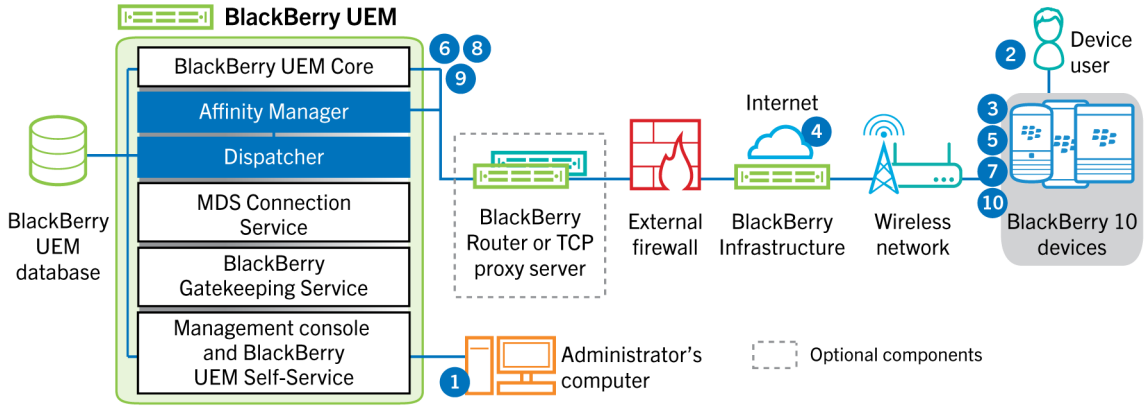
1. 次の操作を実行します。
   a. Windows 10 アクティベーションを簡易化するために検出サービスを設定します。
   b. ユーザーをローカルユーザーアカウントとして、または会社のディレクトリから取得したアカウント情報を使用して、BlackBerry UEM に追加する
   c. 次のいずれかのオプションを使用してユーザーにアクティベーションの詳細情報を提供する
      - デバイスアクティベーションパスワードを自動生成し、アクティベーションの手順を記載したメールを送信する
      - デバイスアクティベーションパスワードを設定し、メールでユーザーにアクティベーション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：BlackBerry 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. 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できるように BlackBerry UEM Self-Service アドレスをユーザーに通知する
2. ユーザーは次の操作を実行します。
   a. ユーザー名とアクティベーションパスワードをデバイスに入力します。
   b. 「仕事用と個人用 - 制限付き 」または「仕事用領域のみ 」アクティベーションの場合は、ユーザーが同意する必要のある使用条件を概略した組織の通知を承認します。
3. アクティベーションが「仕事用領域のみ 」の場合、デバイスはすべての既存のデータを削除し、再起動します。その他のアクティベーションタイプの場合、デバイス上の Enterprise Management Agent 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. Enterprise Management Agent にアドレスを送信する
5. デバイスが次の処理を実行します。
   a. BlackBerry UEM との接続を確立する
   b. アクティベーションパスワードと EC-SPEKE を使って、CSR の保護と BlackBerry UEM への応答に使われる共有対称キーを生成する
   c. 次のように暗号化された CSR と HMAC を作成します。

- 証明書のキーペアを生成します。
- キーペアの公開鍵を含む PKCS#10 CSR を作成します。
- 共有対称キーと、PKCS#5 パディングを含む CBC モードの AES-256 を使用して CSR を暗号化します。
- SHA-256 を使用して暗号化された CSR の HMAC を計算し、それを CSR に付加します。

d. 暗号化された CSR と HMAC を BlackBerry UEM に送信する

6. BlackBerry UEM は次の操作を実行します。

a. 暗号化された CSR の HMAC を検証し、共有対称キーを使用して CSR を復号化します。
b. ユーザー名、仕事用領域 ID、および組織の名前を BlackBerry UEM データベースから取得します。
c. 取得した情報とデバイスが送信した CSR を使用してクライアント証明書をパッケージ化します。
d. エンタープライズ管理ルート証明書を使用してクライアント証明書に署名します。
e. 共有対称キーと、PKCS#5 パディングを含む CBC モードの AES-256 を使用して、クライアント証明書、エンタープライズ管理ルート証明書、および BlackBerry UEM URL を暗号化します。
f. 暗号化されたクライアント証明書、エンタープライズ管理ルート証明書、および BlackBerry UEM URL の HMAC を計算して、それを暗号化されたデータに付加します。
g. 暗号化された データと HMAC をデバイスに送信します。

7. デバイスが次の処理を実行します。

a. HMAC を検証します。
b. BlackBerry UEM から受信したデータを復号化します。
c. クライアント証明書とエンタープライズ管理ルート証明書をキーストアに保存します。

8. BlackBerry UEM は次の操作を実行します。

a. BlackBerry UEM Core は、新しいデバイスをドメイン内の BlackBerry UEM インスタンスに割り当てます。
b. BlackBerry UEM Core は、新しいデバイスが BlackBerry UEM インスタンスに割り当てられたことをアクティブな BlackBerry Affinity Manager に通知します。
c. アクティブな BlackBerry Affinity Manager は、その BlackBerry UEM インスタンス上の BlackBerry Dispatcher に、新しいデバイスがあることを通知します。
d. BlackBerry UEM Core は、エンタープライズ接続設定を含む設定情報をデバイスに送信します。

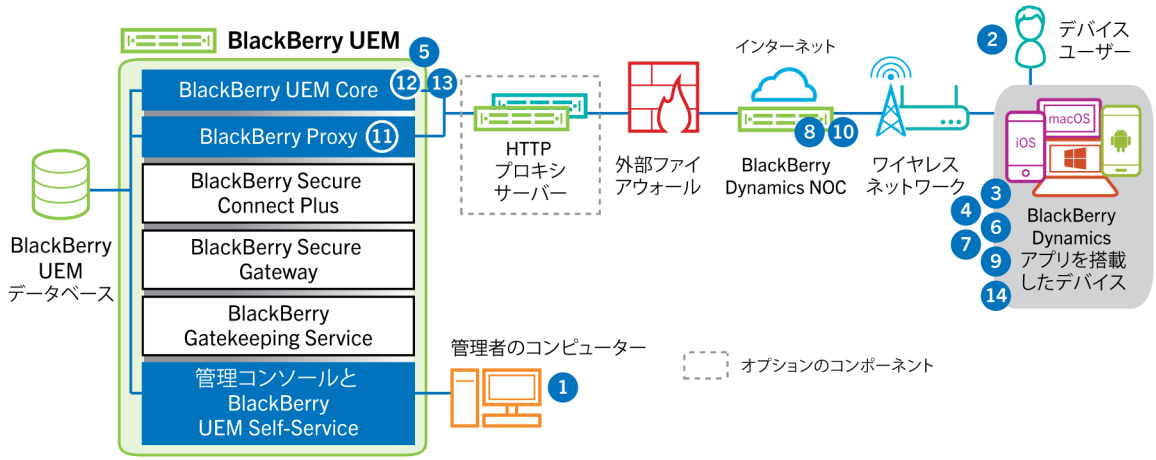
9. BlackBerry UEM Core およびデバイスは、ECMQV、および BlackBerry UEM のクライアント証明書とサーバー証明書から取得した認証済みの長期的な公開鍵を使用して、デバイス転送キーを生成します。このキーは、BlackBerry Secure Connect Plus を使用していないときに仕事用データを暗号化し、IPPP データにプッシュするために使用されます。

10. デバイスは、IT ポリシーとその他の情報を受信して適用し、仕事用領域を作成したことを確認する確認応答を TLS 経由で 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プロセス中に使用される楕円曲線プロトコルは、NIST 推奨の 521 ビット曲線を使用します。

データフロー：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 アプリがアクティブ化され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。



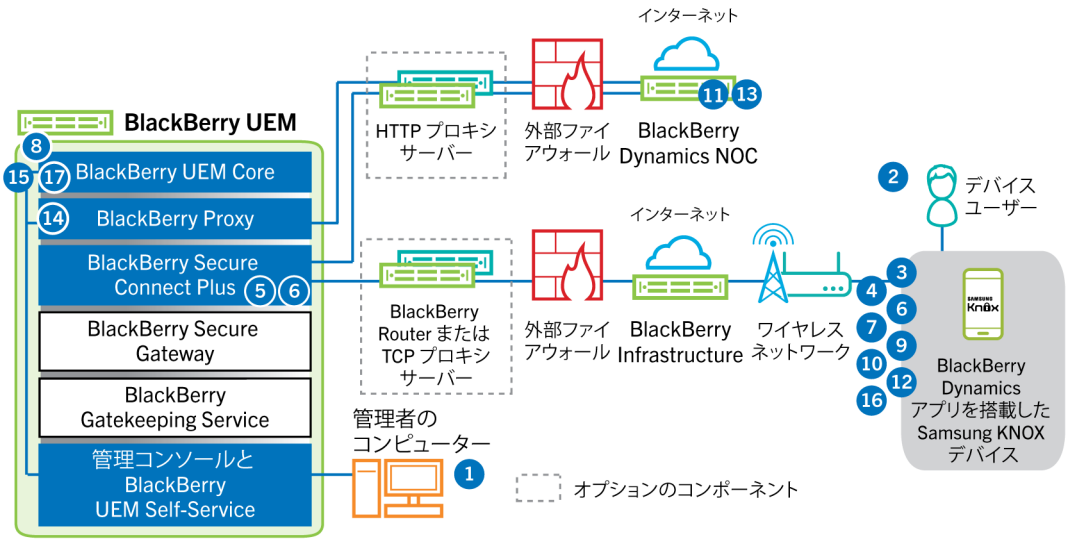
1. 管理者は、1 つまたは複数の BlackBerry Dynamics アプリをユーザーに割り当てます。
2. ユーザーはデバイスにアプリをインストールします。
3. デバイスが Samsung Knox Workspace デバイスではなく、BlackBerry UEM Client がデバイスにインストールされている場合、BlackBerry Dynamics アプリは次の操作を実行します。
   a. デバイス上の BlackBerry UEM Client とセキュアなチャネルを確立します。セキュアチャネルで交換されたデータは、AES-CBC 暗号を使用して暗号化されます。
   b. BlackBerry UEM Client に、新しい BlackBerry Dynamics アプリのアクセスキーを要求するように依頼します。要求にはランダムに生成されたノンスが含まれます。
4. 次のいずれかのイベントが発生します。
   - BlackBerry UEM Client は、アクセスキー要求とランダムに生成されたノンスを BlackBerry UEM Core に送信します。
   - BlackBerry UEM Client がデバイスにインストールされていない場合、またはデバイスが Samsung Knox Workspace を使用していて、これがアクティブ化された最初の BlackBerry Dynamics アプリである場合、管理者はユーザーに送信するアクセスキーを生成するか、または、ユーザーが BlackBerry UEM Self-Service にログインして、アクセスキーを生成します。
   - デバイスまたは Knox Workspace にアクティブ化された BlackBerry Dynamics アプリがすでに含まれている場合、アクティブ化されたアプリはアクセスキー要求とランダムに生成されたノンスを BlackBerry UEM Core に送信します。
5. BlackBerry UEM Core は、要求されたアクセスキーを BlackBerry UEM Client に送信します。
6. BlackBerry UEM Client は、アクセスキーを BlackBerry Dynamics アプリに提供します。
7. BlackBerry Dynamics アプリは BlackBerry Dynamics NOC との SSL 接続を確立し、アクセスキーのハッシュを送信します。
8. BlackBerry Dynamics NOC はアクセスキーを検証し、検証が成功した場合は、マスターリンクキーや接続情報を含むプロビジョニングデータを BlackBerry Dynamics アプリに送信します。

9. BlackBerry Dynamics アプリは、SSL 接続を経由して BlackBerry Dynamics NOC にセキュアチャネルセットアップメッセージを送信することによって、BlackBerry UEM Core との共有の秘密を確立するプロセスを開始します。

   セキュアチャネルセットアップメッセージには、送信者を認証し、メッセージの整合性を保証するために、ユーザー ID（メールアドレス）、短期 ECDH 公開鍵、salt 値、トークン、およびメッセージの MAC が含まれています。
10. BlackBerry Dynamics NOC は、HTTPS 接続を介してセキュアチャネルセットアップメッセージを BlackBerry Proxy に転送します。
11. BlackBerry Proxy は、セキュアチャネルセットアップメッセージを BlackBerry UEM Core に転送します。
12. BlackBerry UEM Core は BlackBerry Dynamics アプリに応答します。応答には、新しい短期 ECDH 公開鍵とメッセージの MAC が含まれています。
13. BlackBerry Dynamics アプリは、BlackBerry UEM Core からプロビジョニングデータを要求します。要求は、BlackBerry Dynamics NOC と BlackBerry Proxy を通過します。
14. BlackBerry UEM Core は、マスターセッションキー、アプリ設定データ、BlackBerry Proxy インスタンスのリストを含む暗号化されたプロビジョニングデータを BlackBerry Dynamics アプリに送信して、アクティベーションを完了します。

データフロー：BlackBerry Secure Connect Plus が有効になっているときに Samsung Knox Workspace デバイスで BlackBerry Dynamics アプリをアクティブ化する

このデータフローは、Samsung Knox Workspace デバイス上の仕事用領域にある BlackBerry Dynamics アプリが BlackBerry Secure Connect Plus 接続を介してアクティブ化されるときに、データが移動する仕組みについて説明しています。



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 Samsung Knox デバイスにアプリをインストールします。
3. デバイスが Samsung Knox Workspace デバイスではなく、BlackBerry UEM Client がデバイスにインストールされている場合、BlackBerry Dynamics アプリは次の操作を実行します。
   a. デバイス上の BlackBerry UEM Client とセキュアなチャネルを確立します。セキュアチャネルで交換されたデータは、AES-CBC 暗号を使用して暗号化されます。
   b. BlackBerry UEM Client に、新しい BlackBerry Dynamics アプリのアクセスキーを要求するように依頼します。要求にはランダムに生成されたノンスが含まれます。
4. 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。
5. 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。
6. 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。
7. BlackBerry UEM Client は、アクセスキー要求とランダムに生成されたノンスを BlackBerry Secure Connect Plus から BlackBerry UEM Core に送信します。
8. BlackBerry UEM Core は、要求されたアクセスキーを BlackBerry Secure Connect Plus から BlackBerry UEM Client に送信します。
9. BlackBerry UEM Client は、アクセスキーを BlackBerry Dynamics アプリに提供します。

10. BlackBerry Dynamics アプリは、BlackBerry Secure Connect Plus を使用して、BlackBerry Dynamics NOC との接続を確立し、アクセスキーのハッシュを送信します。
11. BlackBerry Dynamics NOC はアクセスキーを検証し、検証が成功した場合は、マスターリンクキーや接続情報を含むプロビジョニングデータを BlackBerry Secure Connect Plus を使用して BlackBerry Dynamics アプリに送信します。
12. BlackBerry Dynamics アプリは、BlackBerry Secure Connect Plus を使用して BlackBerry Dynamics NOC にセキュアチャネルセットアップメッセージを送信することによって、BlackBerry UEM Core との共有の秘密を確立するプロセスを開始します。

    セキュアチャネルセットアップメッセージには、送信者を認証し、メッセージの整合性を保証するために、ユーザー ID（メールアドレス）、短期 ECDH 公開鍵、salt 値、トークン、およびメッセージの MAC が含まれています。
13. BlackBerry Dynamics NOC は、HTTPS 接続を介してセキュアチャネルセットアップメッセージを BlackBerry Proxy に転送します。
14. BlackBerry Proxy は、セキュアチャネルセットアップメッセージを BlackBerry UEM Core に転送します。
15. BlackBerry UEM Core は、BlackBerry Secure Connect Plus を使用して、BlackBerry Dynamics アプリに応答します。応答には、新しい短期 ECDH 公開鍵とメッセージの MAC が含まれています。
16. BlackBerry Dynamics アプリは、BlackBerry UEM Core からプロビジョニングデータを要求します。要求は、BlackBerry Secure Connect Plus、BlackBerry Dynamics NOC、および BlackBerry Proxy を通過します。
17. BlackBerry UEM Core は、マスターセッションキー、アプリ設定データ、BlackBerry Proxy インスタンスのリストを含む暗号化されたプロビジョニングデータを BlackBerry Dynamics アプリに送信して、アクティベーションを完了します。

仕事用データの送受信

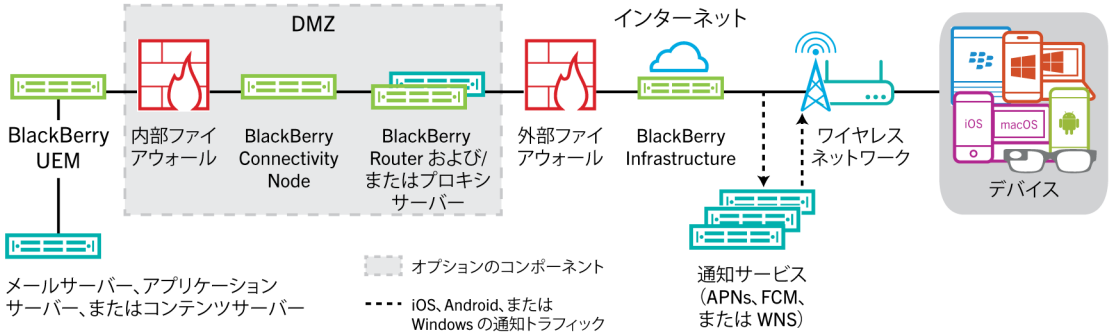
BlackBerry UEM 上でアクティブなデバイスが仕事用データを送受信する場合、これらのデバイスは組織のメール、アプリケーション、またはコンテンツサーバーに接続されます。たとえば、仕事用メールアプリまたはカレンダーアプリを使用している場合、デバイスは組織のメールサーバーへの接続を確立します。仕事用ブラウザーを使用してイントラネット内を移動している場合、デバイスは組織内の Web サーバーとの接続を確立します。

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 Wi-Fi 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 BlackBerry UEM 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 BlackBerry 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。
BlackBerry 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、BlackBerry 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 BlackBerry 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。 • BlackBerry 10、iOS、Android Enterprise、および Samsung Knox Workspace 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。 • BlackBerry 10 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、BlackBerry 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。



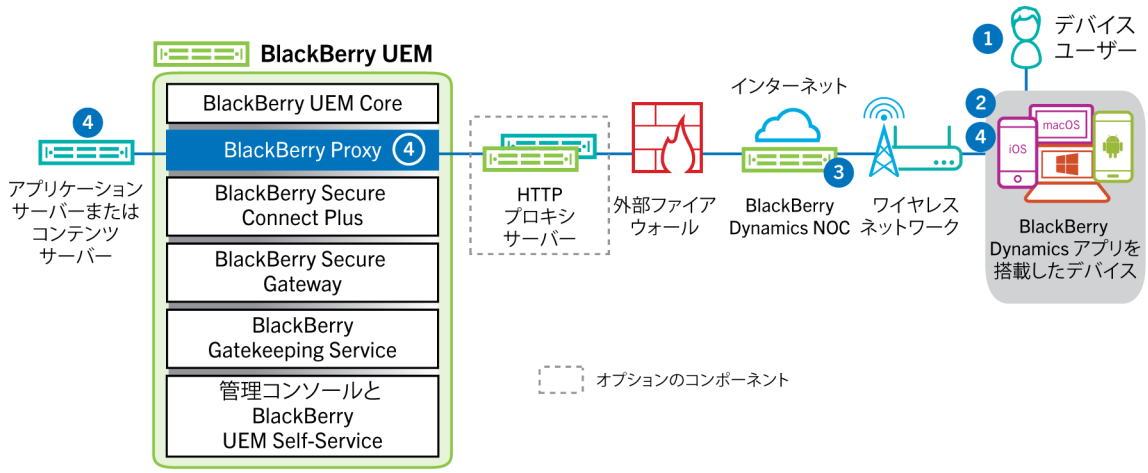
次の表は、デバイスが BlackBerry UEM を経由して BlackBerry Infrastructure および組織のネットワークに接続する場合の状況を示しています。

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	BlackBerry Secure Gateway を有効化すると、iOS デバイスが 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るようになります。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、Samsung Knox Workspace、および BlackBerry 10 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 および BlackBerry 10 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。
BlackBerry 10 デバイス	BlackBerry 10 デバイスは、この通信パスが使用可能な中で最も直接的でコスト効率が高いルートである場合に、このパスを使用して仕事用アプリのデータを送受信します。

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。

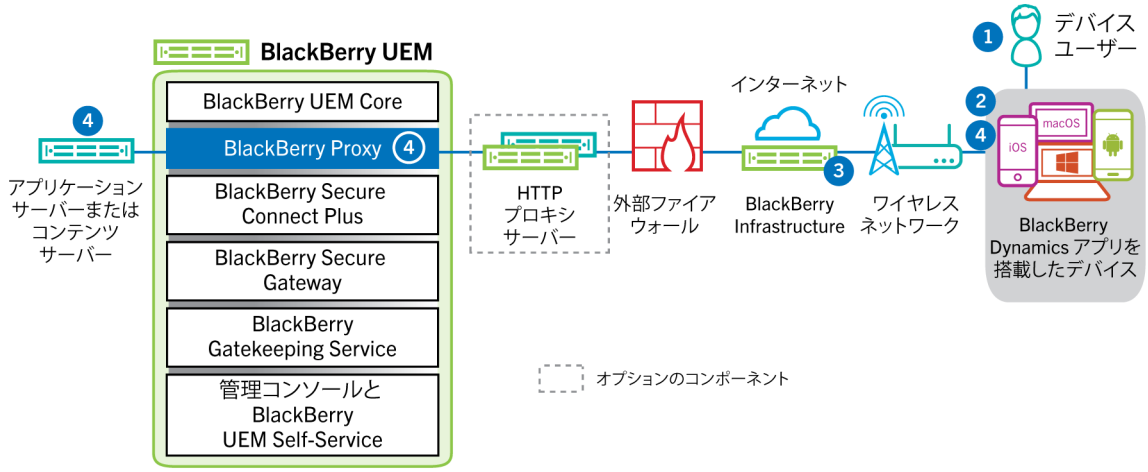


1. ユーザーは、BlackBerry Dynamics アプリを開いて、仕事用データにアクセスします。
2. BlackBerry Dynamics アプリは、BlackBerry Dynamics NOC への接続を確立します。接続は、アプリがアクティブ化されたときに作成されたマスターリンクキーで認証されます。
3. BlackBerry Dynamics NOC は、事前に確立されたセキュリティ保護された接続を介して BlackBerry Proxy と通信し、BlackBerry Dynamics アプリと仕事用データを伝送する BlackBerry Proxy との間でエンドツーエン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。

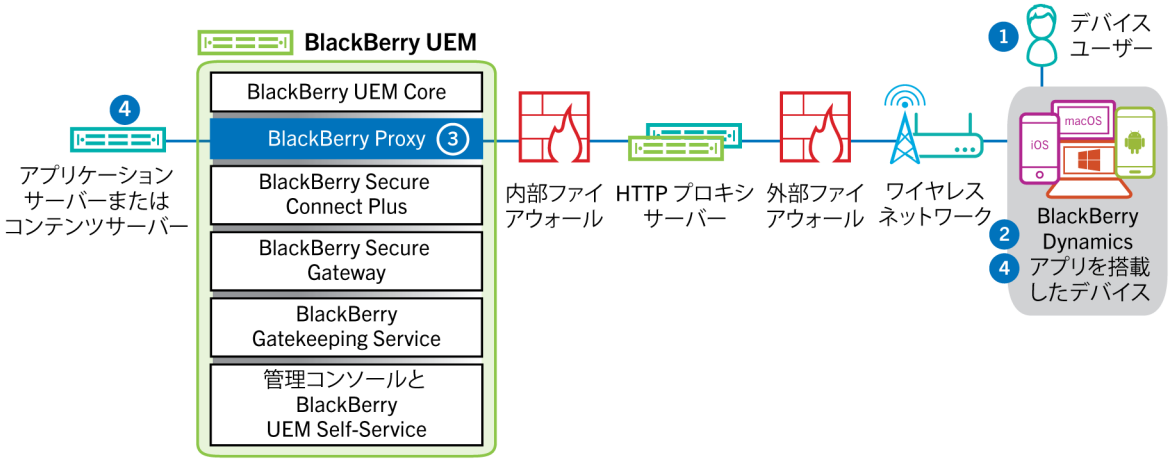


1. ユーザーは、BlackBerry Dynamics アプリを開いて、仕事用データにアクセスします。
2. BlackBerry Dynamics アプリは、BlackBerry Infrastructure への接続を確立します。
3. BlackBerry Infrastructure は、事前に確立された TLS 接続を介して BlackBerry Proxy と通信します。
4. BlackBerry Dynamics アプリは BlackBerry Proxy への TLS 接続を確立し、安全なエンドツーエンド接続を介して仕事用データが交換されます。

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。

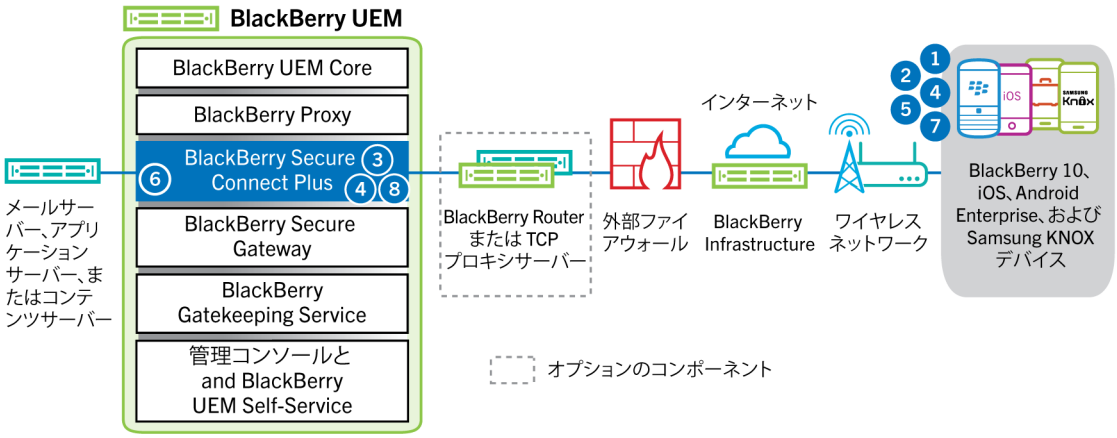


1. ユーザーは、BlackBerry Dynamics アプリを開いて、仕事用データにアクセスします。
2. BlackBerry Dynamics アプリは、BlackBerry Proxy への TLS 接続を確立します。
3. BlackBerry Proxy は BlackBerry Dynamics アプリで認証します。BlackBerry Proxy は、サーバー証明書を使用して、アプリで認証します。BlackBerry Proxy は、BlackBerry Proxy とアプリにのみ知られているセッションキーでキーが付けられた MAC を使用して、アプリを検証します。
4. セ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移動する仕組みを説明しています。

このデータフローは、Android Enterprise 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



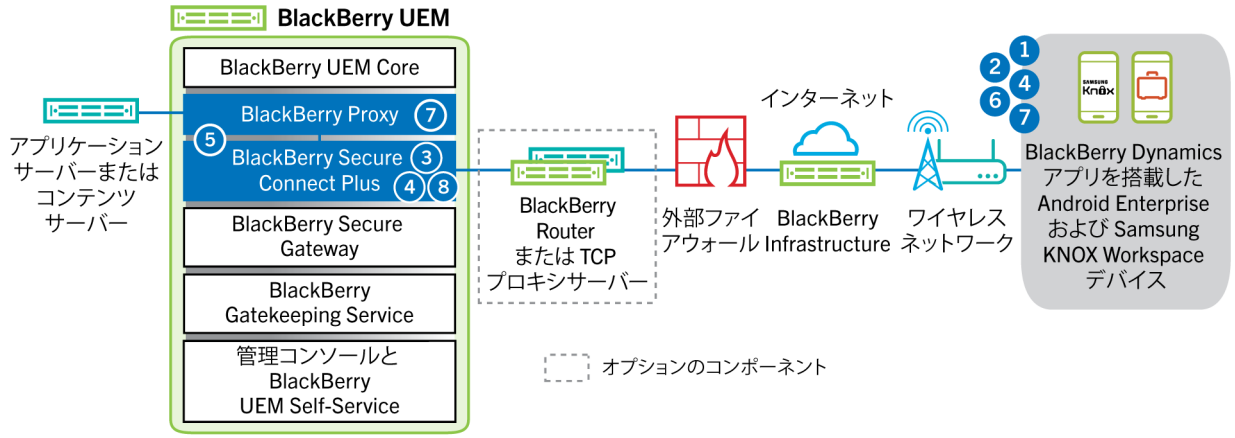
1. ユーザーは、組織のファイアウォール内のコンテンツサーバーまたはアプリケーションサーバーからアプリを開いて、仕事用データにアクセスします。
   - Android Enterprise デバイスの場合、制限するように選択したアプリを除き、すべての仕事用領域アプリが BlackBerry Secure Connect Plus を使用します。
   - Samsung Knox Workspace デバイスの場合、すべての仕事用領域アプリが BlackBerry Secure Connect Plus を使用するか、指定した仕事用アプリのみが使用するかを指定します。
   - iOS デバイスの場合、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。
   - BlackBerry 10 および Android Enterprise デバイスの場合、すべての仕事用領域アプリは BlackBerry Secure Connect Plus を使用します。
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. 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復号化を行います。
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。

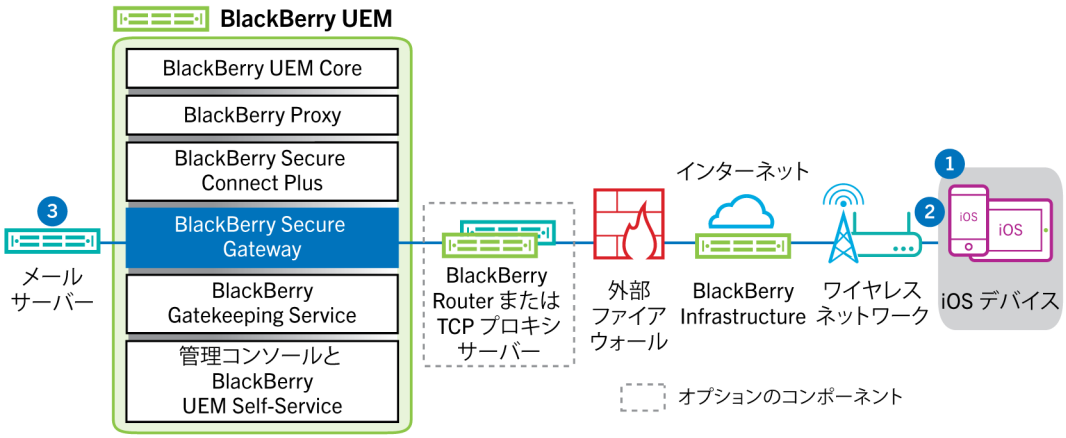
Android Enterprise デバイスまたは Samsung Knox Workspace デバイス上で BlackBerry Secure Connect Plus を BlackBerry Dynamics アプリで使用している場合、ネットワークの遅延を軽減するために、BlackBerry UEM が BlackBerry Dynamics NOC を通して BlackBerry Dynamics アプリデータを送信しないように設定することをお勧めします。



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

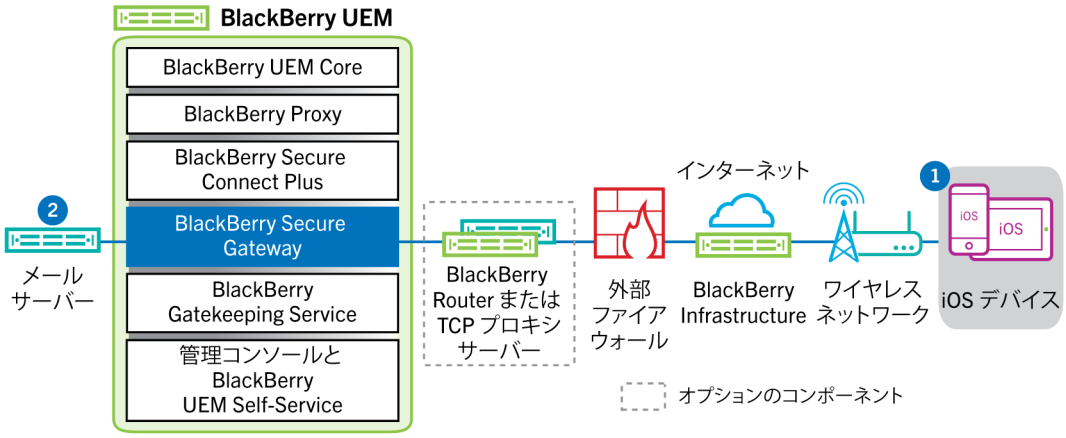
このデータフローは、仕事用メールとカレンダーデータが、BlackBerry Secure Gateway を使用して、iOS デバイスから Exchange ActiveSync サーバーへ移動する仕組みを説明しています。



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

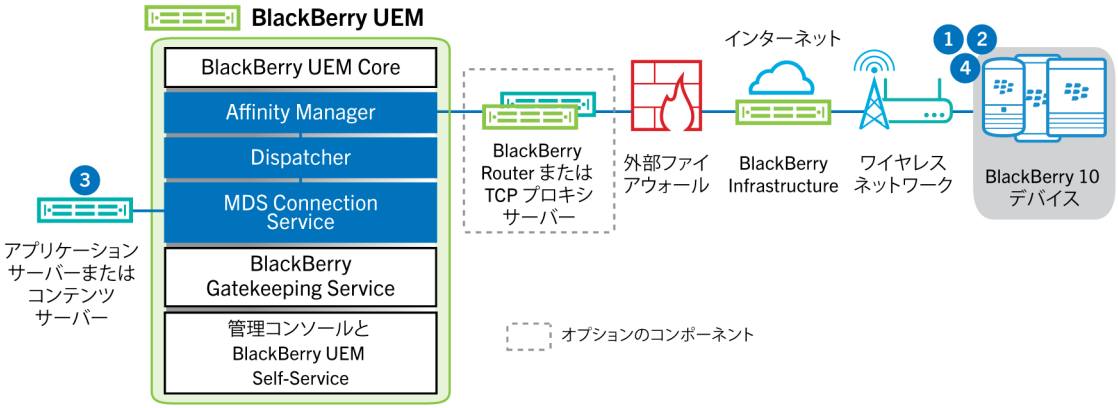
このデータフローは、仕事用メールとカレンダーデータが、BlackBerry Secure Gateway を使用して、iOS デバイスと Exchange ActiveSync サーバー間で移動する仕組みを説明しています。



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。

データフロー：BlackBerry 10 デバイスから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 が有効でない場合、BlackBerry 10 デバイス上の仕事用アプリが、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際に、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、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、仕事用ブラウザーを開いて、イントラネットを使用するか、または BlackBerry Work Drives を使用して、ネットワークドライブ上のファイルにアクセスできます。
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 BlackBerry Infrastructure、BlackBerry Affinity Manager、BlackBerry Dispatcher、および BlackBerry MDS Connection Service を経由して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、BlackBerry MDS Connection Service、BlackBerry Dispatcher、BlackBerry Affinity Manager、および BlackBerry Infrastructure を経由してデバイスに移動します。
4. アプリはデータを受信し、デバイス上に表示します。

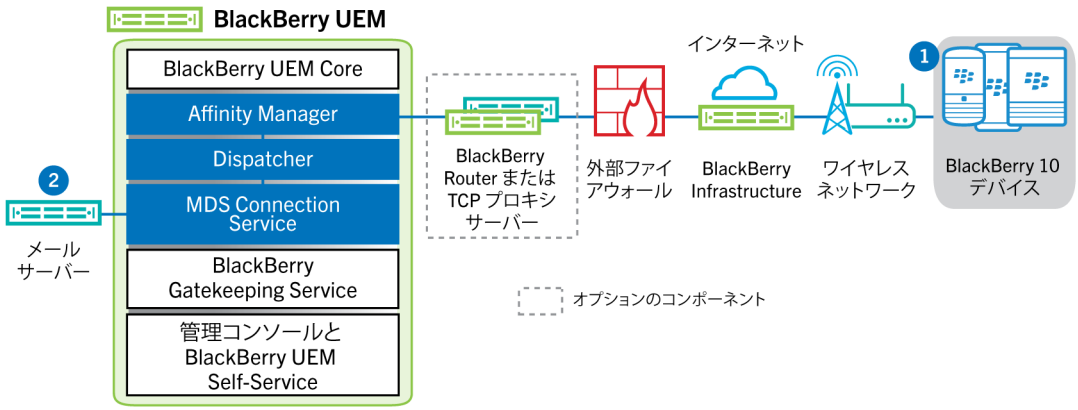
データフロー：BlackBerry 10 デバイスからのメールの送信

このデータフローは、BlackBerry Secure Connect Plus が有効でない場合に、BlackBerry 10 デバイスから Exchange ActiveSync サーバーに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、BlackBerry Infrastructure、BlackBerry Affinity Manager、BlackBerry Dispatcher、および BlackBerry MDS Connection Service 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：BlackBerry 10 デバイスでのメールの受信

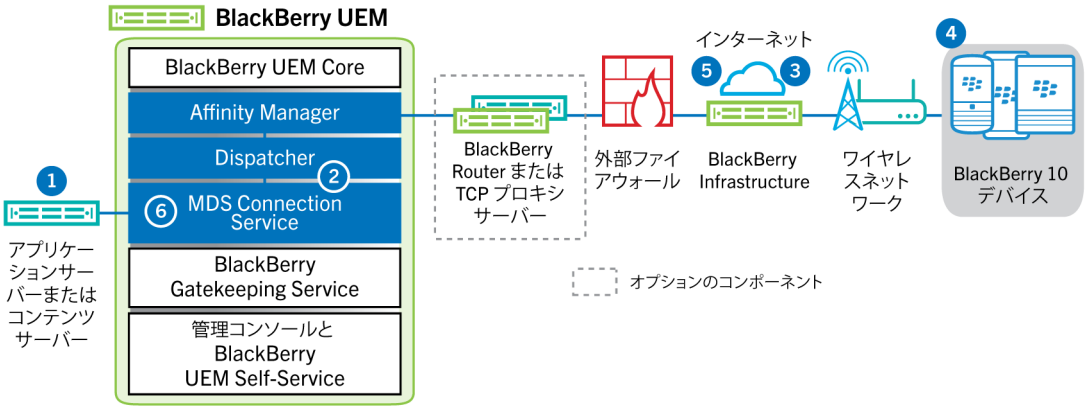
このデータフローは、BlackBerry Secure Connect Plus が有効になっていない場合に、BlackBerry 10 デバイス上の Exchange ActiveSync サーバーから仕事用メールを受信する方法について説明しています。



1. デバイス上のネイティブのメールクライアントは BlackBerry Infrastructure、BlackBerry Affinity Manager、BlackBerry Dispatcher、および BlackBerry MDS Connection Service を通じて、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 MDS Connection Service、BlackBerry Dispatcher、BlackBerry Affinity Manager、および 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。

データフロー：**BlackBerry 10** デバイスでのエンタープライズプッシュ更新の受信

このデータフローは、BlackBerry Secure Connect Plus が有効でない場合に、仕事用データがアプリケーションサーバーから BlackBerry 10 デバイスの仕事用領域にある適切なアプリに移動する仕組みを説明しています。



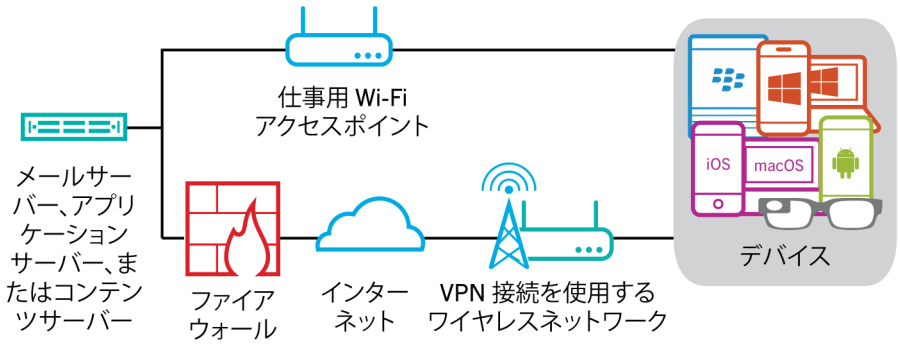
1. BlackBerry 10 デバイスの仕事用アプリに新しいまたは更新されたデータがある場合は、アプリケーションまたはコンテンツサーバーが HTTP または HTTPS 要求を使用して、データを BlackBerry MDS Connection Service にプッシュします。
2. BlackBerry MDS Connection Service は、プッシュされたデータをファイアウォールのポート 3101 経由で BlackBerry Dispatcher、BlackBerry Affinity Manager、および BlackBerry Infrastructure へ送信します。
3. BlackBerry Infrastructure は、データを BlackBerry 10 デバイスへ送信します。
4. BlackBerry 10 デバイスは、配信確認を BlackBerry Infrastructure へ送信します。デバイスのアプリは、受信コンテンツを検出し、ユーザーがアプリを開いたときにコンテンツを表示します。

5. BlackBerry Infrastructure は、BlackBerry Affinity Manager と BlackBerry Dispatcher を介して BlackBerry MDS Connection Service に配信確認を送信します。
6. そうするように設定されている場合は、BlackBerry MDS Connection Service が HTTP 要求を使用して、配信確認をプッシュイニシエーターに送信します。

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

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。組織の VPN を使用するには、MDM 制御 のアクティベーションタイプまたは Samsung Knox Workspace の Android デバイスを持つユーザーは、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。

この図は、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。



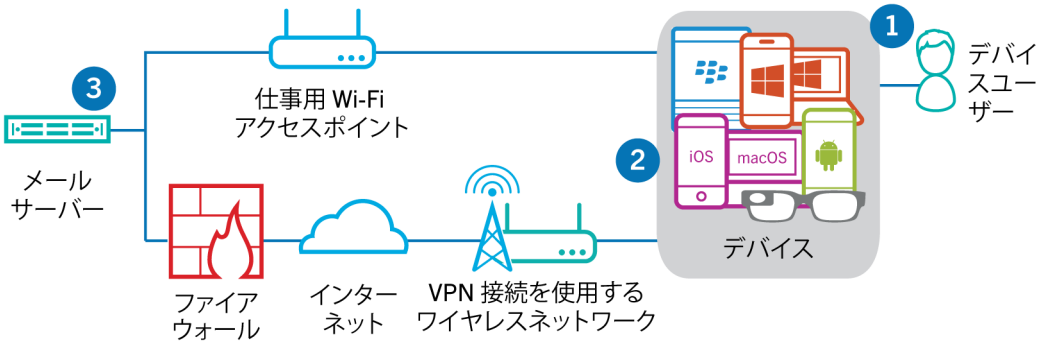
次の表は、デバイスがいつ組織の VPN または仕事用 Wi-Fi ネットワークを使用して、組織のネットワークに接続するのかを示したものです。

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、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、BlackBerry Secure Connect Plus が有効になっていない場合にのみ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の種類の 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の種類の 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。組織の VPN を使用するために、Android デバイスユーザーは、デバイスに 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 が有効でない場合、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。

デバイスタイプ	説明
BlackBerry 10	BlackBerry 10 デバイスは、組織の VPN または仕事用 Wi-Fi ネットワークが使用可能なルートの中で最も直接的でコスト効率が高い場合にこのネットワークを使用して、仕事用データを送受信します。BlackBerry 10 デバイスは、仕事用データにアクセスするときに、ユーザーではなく、管理者によって設定された VPN プロファイルおよび Wi-Fi プロファイルのみを使用します。

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

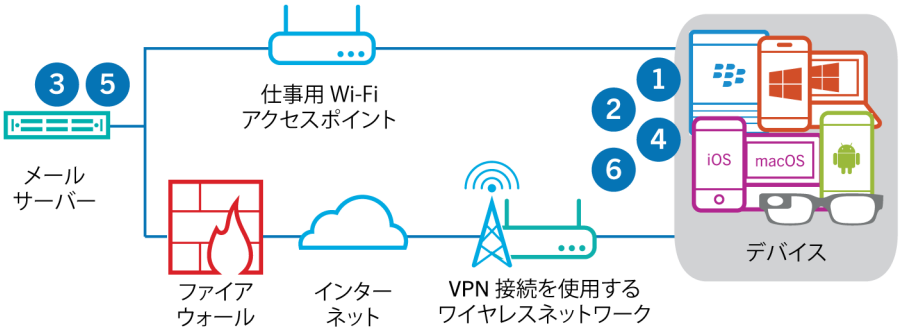
このデータフローは、Exchange ActiveSync を使用して、組織の VPN または仕事用 Wi-Fi ネットワーク経由でデバイスからメールサーバーへ仕事用メールとカレンダーデータが移動する仕組みを説明しています。



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

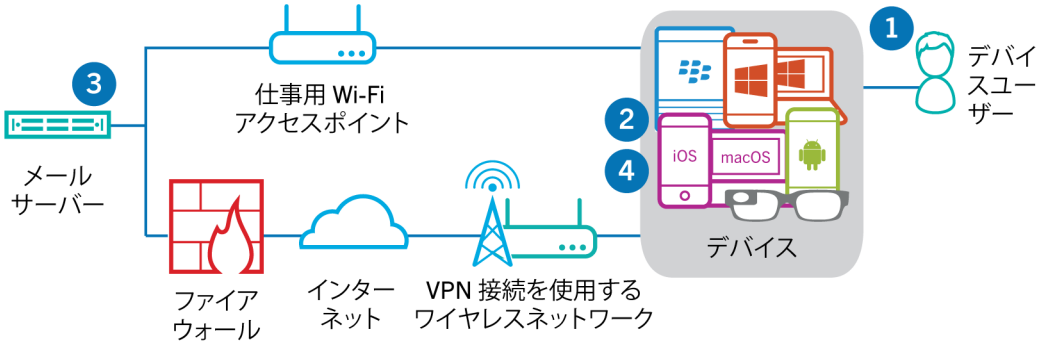
このデータフローは、Exchange ActiveSync を使用して、組織の VPN または仕事用 Wi-Fi ネットワーク経由でデバイスからメールサーバーへ仕事用メールとカレンダーデータが移動する仕組みを説明しています。



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。

設定の更新をデバイスに送信する必要がある場合には、BlackBerry UEM は、設定の更新が保留中であることをデバイスに通知します。デバイスはまた、デバイスで通知が受信されていない場合に、設定の更新を見逃さないように、定期的に BlackBerry UEM をポーリングして、デバイス上で実行する必要のある操作を要求します。

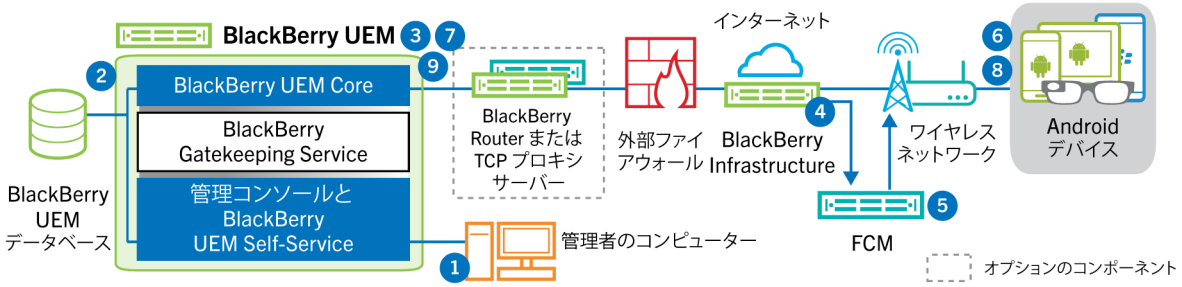
Android デバイスでは、BlackBerry UEM Client がすべての設定更新を受信し完了します。

iOS デバイスでは、BlackBerry UEM Client アプリが、コンプライアンスステータスと、デバイスに割り当てられたアプリやポリシーなどのデバイスに関する設定情報を表示します。ただし、デバイス上のネイティブ MDM Daemon は、デバイスに送信されたすべての設定更新を受信して、処理を終了します。

アクティベーションに BlackBerry UEM Client を要求しない Windows 10 および macOS デバイスでは、ネイティブ MDM Daemon は、デバイスに送信されたすべての設定更新を受信して、処理を終了します。

BlackBerry 10 デバイスでは、Enterprise Management Agent がすべての設定更新を受信し完了します。

データフロー：Android デバイスでの設定更新の受信



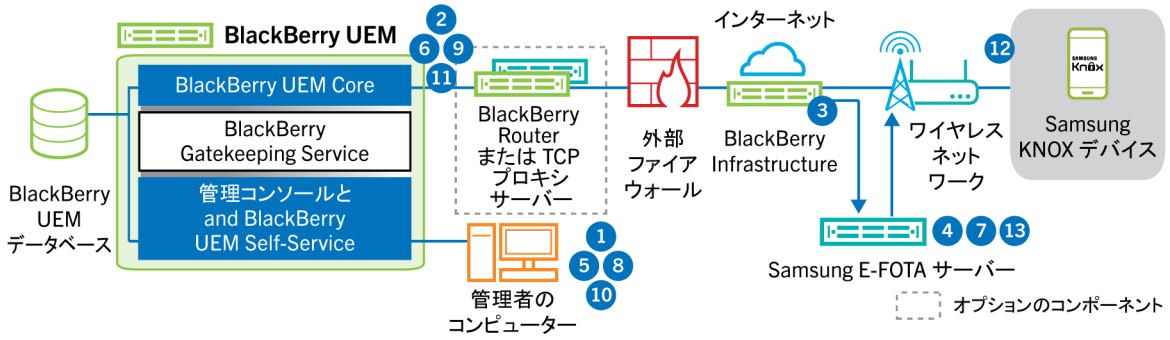
1. Android デバイス用の設定更新をトリガーするアクションは、管理コンソール内で実行されます。
2. 更新が BlackBerry UEM に適用され、デバイスと共有する必要のあるオブジェクトが識別されます。
3. BlackBerry UEM Core は、BlackBerry Router または TCP プロキシサーバー（インストールされている場合）、および外部ファイアウォールのポート 3101 を経由して BlackBerry Infrastructure に接続します。
4. BlackBerry Infrastructure は FCM を使用して、保留中の更新があることを Android デバイスに通知します。
5. GCM は通知を BlackBerry UEM Client デバイス上の Android 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要求します。
7. BlackBerry UEM Core は、BlackBerry Infrastructure および 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、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。

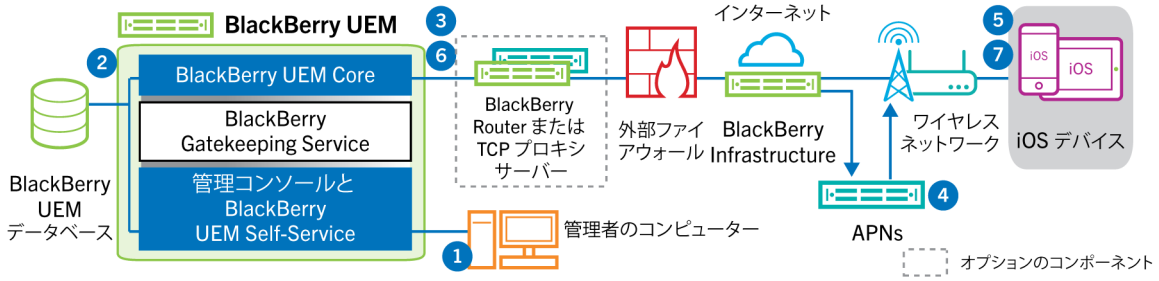
データフロー：Samsung Knox デバイスのファームウェアを更新する

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。詳細については、管理関連の資料の「デバイスにインストールされたソフトウェアリリースの制御」を参照してください。



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。

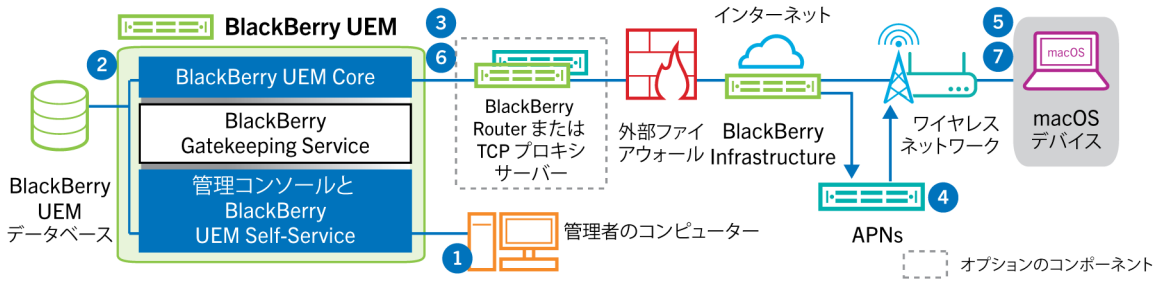
データフロー：iOS デバイスでの設定更新の受信



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。

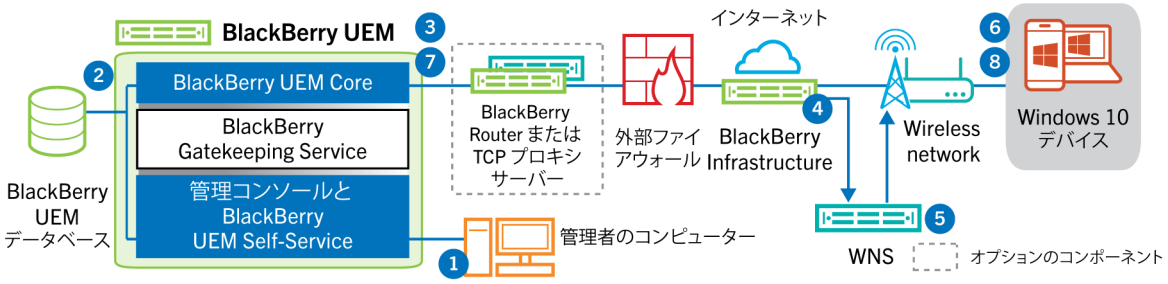
データフロー：macOS デバイスでの設定更新の受信



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。

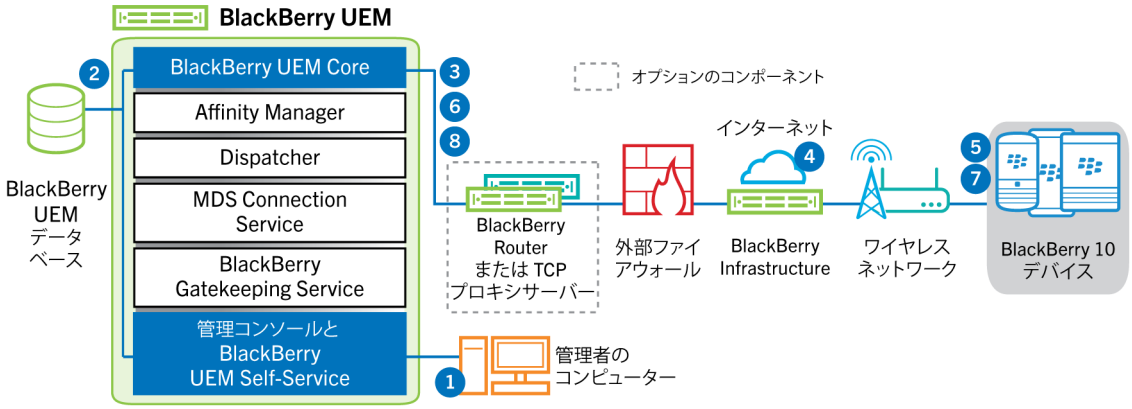
データフロー：Windows 10 デバイスでの設定更新の受信



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。

データフロー：BlackBerry 10 デバイスでの設定更新の受信



1. 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、デバイス用の更新があることを BlackBerry Infrastructure に通知します。通知は、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 を経由します。
4. BlackBerry Infrastructure は、デバイス上の Enterprise Management Agent に更新があることを通知します。
5. デバイス上の Enterprise Management Agent は、BlackBerry UEM Core にポーリングし、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要求します。このポーリング結果は、BlackBerry UEM Core に BlackBerry Infrastructure と BlackBerry Router（インストールされている場合）経由で渡されます。
6. BlackBerry UEM Core は、BlackBerry Infrastructure および 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、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。
7. デバイス上の Enterprise Management Agent が、設定更新を受信し、新しいまたは更新された設定をデバイスに適用します。Enterprise Management Agent 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。
8. 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 6〜8 を繰り返します。

商標などに関する情報

©2020 BlackBerry Limited. BLACKBERRY、BBM、BES、EMBLEM Design、ATHOC、CYLANCE、SECUSMART などの商標（ただし、これらに限定されるとは限らない）は BlackBerry Limited、その子会社および関連会社の商標または登録商標であり、ライセンスに基づいて使用され、当該の商標に対する独占権は明確に留保されています。その他すべての商標は各社の所有物です。

本書は、参照用として本書で取り上げるすべての文書（提供される文書または BlackBerry の Web サイトで参照可能な文書）を含めて「現状のまま」または「参照可能な形で」提供されるか、またはアクセスすることができ、BlackBerry Limited およびその関連会社（「BlackBerry」）はいかなる条件付け、承認、表明、または保証もしないものとし、BlackBerry は本書の誤記、技術的な誤りまたはその他の誤り、エラー、遺漏について何ら責任を負いません。BlackBerry の所有権、機密情報および/または企業秘密を保護するため、本書では一部の BlackBerry テクノロジの側面を一般化された用語で記述している場合があります。BlackBerry は、本書に含まれる情報を定期的に変更する権利を留保します。ただし、BlackBerry には、本書への変更、更新、拡張、または他の追加を適時ユーザーに提供する義務はないものとします。

本書は、第三者をソースとする情報、ハードウェアまたはソフトウェア、製品またはサービス（コンポーネントや、著作権保護されたコンテンツなど）、および/または第三者の Web サイト（これらをまとめて「サードパーティ製品およびサービス」という）への参照を含んでいる可能性があります。BlackBerry は、サードパーティ製品およびサービスの内容、正確性、著作権遵守、互換性、性能、信頼性、適法性、品格、リンク、他の側面などに限定することなく、サードパーティ製品およびサービスを一切管理することはなく、責任も負いません。本書においてサードパーティ製品およびサービスを参照することは、BlackBerry がサードパーティ製品およびサービスまたは第三者を保証することを意味するものではありません。

該当する司法管轄地域の適用法で明確に禁じられている場合を除き、本書で参照されているソフトウェア、ハードウェア、サービス、またはサードパーティ製品およびサービスについて、耐久性、特定の目的または使用に対する適合、商品性、適性品質、権利侵害の不存在、品質満足度、権原、または制定法、慣習法、取引過程、商慣習から生じる、本書またはその使用に関する、または性能または性能の不履行に関する条件付け、承認、表明、保証などに限定することなく、明示的または黙示的に、いかなる条件付け、承認、表明、または保証も除外されます。ユーザーは、国や地域によって異なる他の権利を有する場合もあります。一部の司法管轄地域では、黙示的な保証および条件の除外事項または限定事項は禁止されています。法律で認められている範囲で、本書に関連する黙示的な保証または条件は、上記に定めるように除外できないが限定できる場合、ユーザーが本書または該当する対象物を初めて入手してから 90 日間に限定されます。

該当する司法管轄地域の適用法で認められている最大限の範囲で、本書またはその使用に関連して、または本書で参照されているソフトウェア、ハードウェア、サービス、またはサードパーティ製品およびサービスの性能または性能の不履行に関連して、直接的、必然的、典型的、偶発的、間接的、特殊的、懲罰的、または加重的損害、金銭的損失による損害（利益または収益の損失、予想される貯蓄の未達成、事業の中断、ビジネス情報の消失、ビジネス機会の喪失、データの破損または消失、データの送受信の失敗、BlackBerry 製品またはサービスと併用したアプリケーションに関連する問題、ダウンタイムコスト、BlackBerry 製品またはサービスあるいはその一部の使用機会や通信サービスの使用機会の喪失、代替品コスト、保険料、設備費、保守費、資本コストなど）に限定することなく、損害を予想できたかどうかを問わず、BlackBerry が損害の可能性について勧告を受けていた場合を含め、いかなる場合においても、BlackBerry はいかなる損害の責任も負わないものとします。

該当する司法管轄地域の適用法で認められている最大限の範囲で、契約、不法行為、またはユーザーに対する過失責任または厳格責任について、BlackBerry は他のいかなる義務、責務、または責任も負わないものとします。

本書の限定事項、除外事項、および免責事項は、（A）訴訟原因、請求、またはユーザーによる行為（契約違反、過失、不法行為、厳格責任、その他の法理論など）の性質に関係なく、この契約の基本目的または本書に記載されている救済策の根本的違反または不履行を免れるため、（B）BlackBerry およびその関連会社、その後継

者、譲受人、代理業者、納入業者（通信事業者を含む）、認可された BlackBerry 販売業者（通信事業者を含む）およびその取締役、従業員、および請負業者に適用されます。

上記に定める限定事項および除外事項に加えて、いかなる場合においても、BlackBerry の取締役、従業員、代理業者、販売業者、納入業者、請負業者または BlackBerry の関連会社は、本書に起因または関連する責任を負わないものとします。

ユーザーは、サードパーティ製品およびサービスの加入、インストール、または使用前に、通信事業者がサードパーティ製品およびサービスのすべての機能をサポートすることに同意していることを確認する責任を負います。一部の通信事業者は、BlackBerry® Internet Service への加入によるインターネット閲覧機能を提供しない場合があります。サービスの利用、ローミング、サービスプラン、その他の機能については、通信事業者に問い合わせてください。BlackBerry 製品およびサービスにおけるサードパーティ製品およびサービスのインストールまたは使用には、第三者の権利を侵害または妨害しないように、特許、商標、著作権、または他のライセンスが必要になる場合があります。ユーザーは、サードパーティ製品およびサービスを使用するかどうかを決定し、使用するためにサードパーティライセンスが必要かどうかを確認する責任を負います。必要な場合、ユーザーはライセンスを取得する責任を負います。ユーザーは、必要なライセンスをすべて取得するまで、サードパーティ製品およびサービスをインストールまたは使用してはなりません。BlackBerry 製品およびサービスで提供されるサードパーティ製品およびサービスは、ユーザーの便宜のために「現状のまま」提供され、BlackBerry は明示的にも黙示的にもいかなる条件付け、承認、表明、または保証もしないものとし、BlackBerry はそれに関連するいかなる責任も負わないものとします。ユーザーによるサードパーティ製品およびサービスの使用は、ライセンスまたは BlackBerry との他の契約で明示的に対象になっている場合を除き、個別のライセンスおよび第三者との他の該当契約の条件に従うものとし、その制約を受けるものとします。

BlackBerry 製品またはサービスの使用条件は、個別のライセンスまたは BlackBerry との他の該当契約に定められています。本書の内容は、本書以外に BlackBerry 製品またはサービスの一部に対して BlackBerry が提供した文書による明示的な契約または保証を破棄するものではありません。

BlackBerry Enterprise Software には、特定のサードパーティ製ソフトウェアが組み込まれています。このソフトウェアに関連するライセンスおよび著作権情報は、http://worldwide.blackberry.com/legal/thirdpartysoftware.jsp でご確認いただけます。

BlackBerry Limited
2200 University Avenue East
Waterloo, Ontario
Canada N2K 0A7

BlackBerry UK Limited
Ground Floor, The Pearce Building, West Street,
Maidenhead, Berkshire SL6 1RL
United Kingdom

Published in Canada