



BlackBerry UEM Client 用 iOS

ユーザーガイド

目次

BlackBerry UEM Client の利用を開始する	5
iOS デバイスのアクティベーション.....	5
仕事用アプリのインストールまたは更新.....	7
仕事用メールの設定.....	7
BlackBerry UEM Self-Service の使用.....	8
BlackBerry 2FA の使用.....	8
直接認証の使用.....	8
ワンタイムパスワードの使用.....	8
デバイスの事前認証.....	9
共有デバイスのチェックアウトとチェックイン.....	10
デバイスのコンプライアンスについて.....	11
IT ポリシーについて.....	12
プロファイルについて.....	13
証明書について.....	14
Entrust 証明書のインポート.....	14
プライバシー情報について.....	15
アプリのレーティングとレビューについて.....	16
BlackBerry Dynamics アプリのパスワードの変更	17
BlackBerry サポートへのログファイルのアップロード	18
デバイスの無効化.....	19
BlackBerry UEM Client の削除.....	19

商標などに関する情報..... 20

BlackBerry UEM Client の利用を開始する

仕事用デバイスをアクティブ化するには、BlackBerry UEM Client を使用します。デバイスをアクティブ化すると、デバイスは BlackBerry UEM と関連付けられ、管理者がデバイスに割り当てた仕事用データと生産性向上アプリへのアクセス権が与えられます。管理者は、自身のロールに基づいてデバイスの保護レベルを決定し、IT ポリシーとプロファイルを割り当てます。この方法により、ユーザーは適切なデバイス機能を利用できるようになり、デバイスでは仕事用データのセキュリティが維持されます。

BlackBerry UEM Client から iOS デバイス用の App Store をダウンロードできます。

iOS デバイスのアクティベーション

管理者からアクティベーションメールを受信したら、デバイスをアクティブ化する準備は完了です。

アクティベーションメールには、デバイスをアクティブ化するのに必要な情報が含まれています。アクティベーションパスワードが期限切れになっている場合は、BlackBerry UEM Self-Service で新しいパスワードを作成するか、管理者に問い合わせてください。

アクティベーションメールでアクティベーション QR Code を受信した場合は、それを使用してデバイスをアクティブ化できます。QR Code を使用してデバイスをアクティブ化する場合、情報を入力する必要はありません。

管理者からエンタープライズ資格情報の使用に関して指示があった場合、デバイスのアクティベーションのために組織のサインインページにリダイレクトされます。

作業を始める前に： デバイス（iOS および iPadOS 16 以降）でロックダウンモードが有効になっている場合、デバイスをアクティブ化するには無効にする必要があります。ロックダウンモードでは、アクティベーションに必要な設定プロファイルのインストールができません。必要に応じて、アクティベーション後にロックダウンモードを有効にすることができます。

1. BlackBerry UEM Client から App Store をインストールします。
2. UEM Client を開きます。
3. 使用許諾契約書を読んで、承諾します。
4. 次の操作のいずれかを実行します。

タスク	手順
QR Code を使用してデバイスをアクティベーションする	<ol style="list-style-type: none">a.  [QR コードをスキャン] をタップします。b. アクティベーションメールの QR Code をスキャンします。
エンタープライズ資格情報を使用してデバイスをアクティベーションする	<ol style="list-style-type: none">a. [管理者から指示された場合は組織のアカウントでサインインする] をタップします。b. 仕事用メールアドレスを入力します。これは、アクティベーションメールを受信したメールアドレスです。[次へ] をタップします。c. ユーザー名を入力し、[次へ] をタップします。組織のサインインページにリダイレクトされます。d. 自分の資格情報を使用してログインします。

タスク	手順
デバイスを手動でアクティベーションする	<ol style="list-style-type: none"> a. 仕事用メールアドレスを入力します。これは、アクティベーションメールを受信したメールアドレスです。[移動] をタップします。 b. 必要に応じて、メールに記載されているサーバーアドレスを入力し、[デバイスをアクティベーション] をタップします。 c. アクティベーションパスワードを入力し、[デバイスをアクティベーション] をタップします。アクティベーションパスワードの有効期限が切れている場合は、BlackBerry UEM Self-Service で新しいパスワードを作成するか、管理者に問い合わせてください。

5. [許可] をタップして、通知の送信を UEM Client に許可します。[許可しない] を選択すると、デバイスが完全にはアクティベーションされません。
6. 証明書のインストールを求めるプロンプトが表示されたら、[OK] をタップします。
7. 設定プロファイルのダウンロードを求めるプロンプトが表示されたら、[許可] をタップします。
8. ダウンロードが完了したら、[設定] を開きます。
9. [全般] をタップして [プロファイルとデバイス管理] に移動します。
10. プロファイルをインストールするには、[UEM プロファイル] をタップし、画面の指示に従います。
11. インストールが完了したら BlackBerry UEM Client アプリに戻り、アクティベーションを完了します。
12. 必要に応じて、管理者が Microsoft Azure への条件付きアクセスを設定している場合は、次のいずれかを実行します。

タスク	手順
デバイスに Microsoft Authenticator アプリをインストールし、Microsoft Azure にサインインします。	<ol style="list-style-type: none"> a. Microsoft オンラインデバイス登録画面で、[続行] をタップします。 b. Microsoft Azure 資格情報でサインインします。 c. [デバイスの安全を保つためにご協力ください] 画面で、Microsoft Authenticator アプリをダウンロードする必要があります。[アプリを入手] をタップします。 d. アプリメニューで [インストール] をタップします。 e. 診断情報の収集を求めるプロンプトが表示されたら、[OK] をタップします。 f. Microsoft Azure 資格情報でサインインします。 g. [登録] をタップします。

タスク	手順
Microsoft Azure にサインインします。	<ol style="list-style-type: none"> Microsoft オンラインデバイス登録画面で、[続行] をタップします。 アカウントをタップします。 Microsoft Azure 資格情報でサインインします。 [デバイスのセキュリティを維持するためのヘルプ] 画面で、[登録] をタップします。 [開く] をタップして UEM Client 順守画面を表示します。

13. プロンプトが表示されたら、画面の手順に従ってデバイスに仕事用アプリをインストールします。

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

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

仕事用アプリのインストールまたは更新

必須アプリがインストールされていない場合、管理者は仕事用データへのアクセスを制限または削除できます。オプションアプリは管理者が推奨するアプリですが、必ずしもデバイスにインストールする必要はありません。

仕事用の必須アプリまたはオプションアプリをダウンロードするときに、アプリの料金を支払う必要が生じる場合があります。仕事用アプリの料金を支払った場合は、所属組織にその料金を請求してください。

作業を始める前に：[デバイスのアクティベーション](#)

1. BlackBerry UEM Client アプリで、[仕事用アプリ] をタップします。[仕事用アプリ] タブが表示されない場合は、デバイスのホーム画面に移動し、[仕事用アプリ] アプリを開きます。
2. 次の操作のいずれかを実行します。
 - 仕事用アプリをインストールするには、[必須] タブをタップして必要なアプリをすべてインストールしてから、[すべて] タブをタップし、必要なオプションアプリをインストールします。
 - 仕事用アプリを更新するには、[新規] タブをタップし、更新する各アプリの横にある[更新] をタップします。

仕事用メールの設定

デバイスをアクティブ化すると、仕事用メールを設定するための通知が表示されることがあります。画面に表示される手順に従って、セットアップを完了します。仕事用メールが自動的に設定されていない場合は、管理者に詳細を問い合わせてください。

BlackBerry UEM Self-Service の使用

BlackBerry UEM Self-Service コンソールを使用すると、アクティベーションパスワードの設定、BlackBerry Dynamics アプリの管理、デバイスの事前認証に加えて、デバイスのロックやデバイスパスワードの変更など、基本的なコマンドを実行できます。BlackBerry UEM Self-Service の使い方の詳細については、『[BlackBerry UEM Self-Service ユーザーガイド](#)』を参照してください。

BlackBerry 2FA の使用

管理者がデバイスでツーファクター認証のために BlackBerry 2FA を有効にしている場合、認証の第 2 ファクターとしてデバイスを使用できます。これにより、認証されたユーザーのみが組織のリソースにアクセスできるようになります。例えば、リソースにアクセスするためにディレクトリパスワードを入力した直後に、デバイスで接続を確認するように要求されます。

第 1 ファクターはディレクトリパスワードです。第 2 ファクターは、次のいずれかに指定できます。

- 期限切れになる前に、デバイスで確認する必要があるプロンプト。
- ユーザー名またはディレクトリパスワードと共に入力するワンタイムパスワード。

BlackBerry UEM Client のホーム画面で左または右にスワイプして、管理者が有効にした BlackBerry 2FA 機能にアクセスします。

直接認証の使用

管理者がデバイスに BlackBerry 2FA を設定し、直接認証機能を有効にしている場合、ログインして組織のリソースにアクセスする前に、BlackBerry UEM Client から認証できます。直接認証を使用する場合、管理者が指定した制限時間内に、ディレクトリパスワードを使用して組織のリソースにログインする必要があります。直接認証機能を使用すると、確認プロンプトを受信したり、ワンタイムパスワードを使用したりせずに、組織のリソースへの認証を行うことができます。

1. BlackBerry UEM Client のホーム画面で、[直接認証] 画面にスワイプします。
2. [今すぐ認証] をタップします。
認証が正常に終了すると、成功メッセージが表示されます。

終了したら：[直接認証] 画面で、指定された制限時間内にディレクトリパスワードを使用して組織のリソースにログインします。

ワンタイムパスワードの使用

管理者がデバイスに BlackBerry 2FA を設定し、ワンタイムパスワード機能を有効にしている場合、ログインして組織のリソースにアクセスする際に、BlackBerry UEM Client に表示されるワンタイムパスワードを使用できます。ワンタイムパスワードは、ユーザー名またはディレクトリパスワードと共に入力します。デバイスに十分なネットワーク接続がないために確認プロンプトを受信できない場合に、ワンタイムパスワードを使用できます。

1. BlackBerry UEM Client のホーム画面で、[ワンタイムパスワード] 画面にスワイプします。
2. ワンタイムパスワードを書きとめておきます。ワンタイムパスワードは、30 秒後に期限切れになります。
3. 仕事用リソースにアクセスしようとしているコンピューターまたはデバイスで、次のいずれかを実行します。

- ・ [ユーザー名] フィールドに、ユーザー名、カンマ (,)、ワンタイムパスワードを入力します。ユーザー名とワンタイムパスワードは、カンマ (スペースなし) のみを使用して区切ります。例えば、ユーザー名が「janedoe」で、ワンタイムパスワードが「555123」の場合、「janedoe,555123」と入力します。
- ・ [パスワード] フィールドで、ディレクトリパスワードの前にワンタイムパスワードを入力します (スペースや文字で区切らない)。例えば、ワンタイムパスワードが「123456」で、ディレクトリパスワードが「qweRTY」の場合、「123456qweRTY」と入力します。

デバイスの事前認証

管理者がデバイス用に BlackBerry 2FA を設定した場合、ユーザーは BlackBerry UEM Client から事前認証を要求できます。事前認証では、デバイスでの確認またはパスワード入力を求められることなく、事前に設定された期間、仕事用リソースにアクセスできます。お使いのデバイスへのアクセス権がない場合、携帯電話ネットワークの圏外になっている場合、1 台のデバイスをワイヤレスネットワークまたはホットスポットにのみ接続できる場合などに、事前認証機能を使用できます。例えば、一度に 1 台のデバイスしかネットワークに接続できない場合は、モバイルデバイスで事前認証を行い、他のデバイスから仕事用リソースにログインできます。

BlackBerry UEM Self-Service コンソールから、デバイスを事前認証することもできます。BlackBerry UEM Self-Service の使い方の詳細については、『[BlackBerry UEM Self-Service ユーザーガイド](#)』を参照してください。

1. BlackBerry UEM Client のホーム画面で、[事前認証] 画面にスワイプします。
2. [事前認証を要求] をタップします。
3. 事前認証が適用される時間数を入力します。事前認証を適用できる最大時間数は、管理者が指定します。
4. [要求] をタップします。
事前認証の有効期限を確認する画面が表示されます。
5. [閉じる] をタップします。

共有デバイスのチェックアウトとチェックイン

管理者が、複数のユーザーがデバイスを共有するように割り当てている場合、ユーザーはそのデバイスを使用する際に、デバイスをチェックアウトします。デバイスの使用を完了した場合は、次のユーザーが使用できるように、デバイスをチェックインします。

1. UEM Client を開きます。
2. 必要に応じて、サービス利用規約を読み、同意します。
3. 次のタスクのいずれかを実行します。

タスク	手順
デバイスをチェックアウトする。	<ol style="list-style-type: none">a. 認証オプションを変更するには、ドロップダウンリストをタップし、次の操作を実行します。<ol style="list-style-type: none">1. ドロップダウンリストで、[Microsoft Active Directory] または [ローカル認証] を選択します。2. [完了] をタップします。b. [Microsoft Active Directory] を選択した場合は、組織のドメインを入力します。c. ユーザー名とパスワードを入力します。d. [チェックアウト] をタップします。e. [OK] をタップします。
デバイスをチェックインする。	<ol style="list-style-type: none">a. [チェックイン] をタップします。b. [OK] をタップします。

デバイスのコンプライアンスについて

BlackBerry UEM Client のホーム画面でコンプライアンスステータスをタップすると、コンプライアンスレポートを表示できます。コンプライアンスレポートには、組織がデバイスに適用しているポリシーが一覧表示されます。

デバイスのコンプライアンス違反が発生し、コンプライアンスレポートに表示される日付までにコンプライアンスの問題が解決されない場合、管理者によってデバイスから仕事用リソースまたはネットワークへのアクセスが制限またはブロックされることがあります。問題の解決方法がわからない場合は、管理者に問い合わせてください。

組織が適用できるいくつかのコンプライアンスポリシーを次に示します。

- ルート化または脱獄のステータス：デバイスがルート化されている場合、この事実は、ユーザー自身または第三者が、デバイスのオペレーティングシステムへのルートアクセスを可能にするソフトウェアまたは操作をデバイスで実行したことを示しています。ユーザー自身または管理者は、デバイスからルート化ソフトウェアを削除するか、デバイスをデフォルトの状態に復元する操作をデバイスで実行する必要があります。
- パスワード：組織が指定している複雑さの要件を満たす、デバイスでのパスワード。
- デバイスモデル：組織では、特定のデバイスモデルのみを仕事用にアクティブ化することを許可している場合があります。組織のセキュリティ要件に適合したデバイスを使用する必要があります。
- OS バージョン：組織では、特定のバージョンの Android OS を実行しているデバイスのみを仕事用にアクティブ化することを許可している場合があります。
- セキュリティパッチレベル：セキュリティパッチは、デバイスの製造元によって配布され、デバイスのシステム更新の確認時に検出されることがあります。お使いのデバイスモデルに利用できる最新のセキュリティパッチをインストールしてください。
- デバイスの応答がありません：所定の時間が経過しても BlackBerry UEM が応答不能の場合、デバイスは応答がないこととなります。例えば、デバイスにネットワーク接続がないと、デバイスは応答がないことになる場合があります。
- インストールすべき必須仕事用アプリ：組織がユーザーにデバイスへのインストールを求める必須アプリは、[割り当てられた仕事用アプリ] 画面に表示されます。必須アプリがインストールされていない場合、管理者はその状態を検知することができ、必須アプリがインストールされない限り、仕事用データへのユーザーアクセスを制限できます。仕事用アプリで利用できる更新がある場合は、デバイスにインストールする必要があります。
- インストール済みの割り当て対象外アプリまたは制限対象アプリ：仕事のために割り当てられた必須アプリまたはオプションアプリではなく、関係ないアプリをデバイスにインストールした場合、デバイスからアプリを削除する必要があります。制限対象アプリは、デバイスから削除する必要があります。

IT ポリシーについて

IT ポリシーは、デバイスのセキュリティ機能と動作を制御するルールの集合体です。例えば、組織内でデバイスのパスワード設定を強制する場合、管理者は、パスワード設定をユーザーに要求するルールを含む IT ポリシーをデバイスに適用します。ホーム画面で、IT ポリシーアイコンをタップすると、デバイスに適用されるルールを表示できます。

IT ポリシールールは変更または無効化できません。デバイスに適用される IT ポリシールールは、組織の総合的なセキュリティポリシーの一部です。詳細については、管理者に問い合わせてください。

プロフィールについて

プロフィールにより、デバイス上の仕事用リソースへのアクセスをユーザーに許可できます。例えば、ユーザーが仕事用メールアカウント、Wi-Fi 接続、VPN 接続、およびセキュリティ証明書にアクセスできるように、管理者はユーザーのアカウントにプロフィールを割り当てます。

ホーム画面で、割り当て済みプロフィールセクションをタップして、デバイスに割り当てられたプロフィールを表示できます。BlackBerry UEM Client に適用可能なプロフィールのみが表示されることに注意してください。

証明書について

証明書は、仕事用リソースとネットワークにアクセスするためにデバイスの認証に使用されます。

管理者がユーザーアカウントに証明書プロファイルを割り当てると、デバイスに証明書をインストールするかどうかを確認するメッセージが表示されます。メッセージに表示された情報を記録して、手順に従って証明書をインストールします。提供されていないパスワードの入力を求められた場合は、管理者に問い合わせてください。

Entrust 証明書のインポート

管理者に Entrust スマート認証情報を割り当てられた場合は、Entrust IdentityGuard セルフサービスポータルからアクティブ化してから証明書を BlackBerry UEM Client の [プロファイル] 画面にインポートする必要があります。

作業を始める前に：

- デバイスを BlackBerry UEM Client でアクティブ化します。
- 1. Entrust IdentityGuard セルフサービスポータルにログインします。
- 2. QR Code とパスワードを Entrust IdentityGuard セルフサービスポータルから取得します。
 - a) [スマート認証情報をアクティブ化するか更新] をクリックします。
 - b) [スマート認証情報をアクティブ化するか更新] オプションを再選択します。 [次へ] をクリックします。
 - c) 使用するスマート認証情報を選択します。 [OK] をクリックします。
 - d) [モバイルデバイスでホストされているモバイルスマート認証情報 ID をアクティブ化中] オプションを選択します。 [次へ] をクリックします。
 - e) [モバイルデバイスに関連付けられたデータネットワークを使用してスマート認証情報をアクティブ化] オプションを選択します。 [次へ] をクリックします。
 - f) [ID 名] フィールドに名前を入力します。 [OK] をクリックします。
QR Code とパスワードが表示されます。
- 3. デバイスで、UEM Client を開きます。
- 4. [プロファイル] > [証明書をインポート] の順にタップします。
- 5. Entrust スマート認証情報の横にある [アクティブ化] をタップします。
- 6. カメラアイコンをタップし、QR Code を Entrust IdentityGuard セルフサービスポータルからスキャンします。
- 7. パスワードを Entrust IdentityGuard セルフサービスポータルから入力します。 [OK] をクリックします。
「アクティブ化しています。お待ちください」というメッセージが表示されます。これには数分間かかります。
- 8. 正常完了の確認メッセージが表示されます。 [OK] をクリックします。

プライバシー情報について

プライバシー情報メニューでは、IT 管理者がデバイスについて表示できる情報と表示できない情報を確認できます。このメニューには、管理者がデバイス上で実行できるアクションと実行できないアクションも一覧表示されます。

メモ：プライバシー情報メニューは、BlackBerry 2FA のアクティベーションを除くすべてのアクティベーションタイプで使用できます。

メモ：プライバシー情報メニューは、お使いのデバイスが BlackBerry UEM バージョン 12.11 に対してアクティビ化されている場合にのみ使用できます。

アプリのレーティングとレビューについて

管理者は、アプリのレーティングとレビューを実行できます。また、他のユーザーのレビューを表示することもできます。レビューしないでアプリのレーティングを指定できますが、アプリをレビューする場合は、レーティングを指定する必要があります。アプリのレーティングとレビューが終了したら、レーティングとレビューの変更、削除が実行できるようになります。

BlackBerry Dynamics アプリのパスワードの変更

管理者が、BlackBerry UEM Client に他の BlackBerry Dynamics アプリを認証する権限を与えた場合、BlackBerry Dynamics アプリのパスワードを BlackBerry UEM Client で変更できます。BlackBerry Dynamics アプリのパスワードを使用して、BlackBerry Dynamics で保護されているアプリをアクティブ化したり、アクセスしたりできます。

1. BlackBerry UEM Client のホーム画面で、 をタップします。
2.  をタップします。
3. [詳細情報] をタップします。
4. [BlackBerry Dynamics アプリのパスワード] をタップします。
5. 現在のパスワードを入力します。
6. 新しいパスワードを入力して確認します。
7. [OK] をタップします。

BlackBerry サポートへのログファイルのアップロード

BlackBerry サポートから求められた場合は、ログファイルをアップロードして、BlackBerry Dynamics アプリに関する問題のトラブルシューティングに役立てることができます。

1.  をタップして BlackBerry Dynamics Launcher を開きます。
2.  をタップします。
3. [サポート] セクションで、[ログのアップロード] をクリックします。[ログのアップロード] ステータスバーにアップロードの進行状況が表示されます。
4. [閉じる] をクリックします。

デバイスの無効化

デバイスの管理を管理者に任せない場合は、お使いのデバイスを無効にできます。デバイスを無効にすると、デバイスと仕事用リソースの間で接続が削除されます。デバイスを無効にした後は、仕事用のメールアドレスまたはカレンダーには接続できなくなります。また、仕事用の Wi-Fi 接続または VPN 接続にもアクセスできなくなります。

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

1. BlackBerry UEM Client のホーム画面で、[バージョン情報] をタップします。
2. [無効化] をタップします。
3. [OK] をタップします。

終了したら： [BlackBerry UEM Client の削除](#)

BlackBerry UEM Client の削除

デバイスから BlackBerry UEM Client を削除すると、デバイスをアクティブ化できなくなります。

作業を始める前に： デバイスを無効にします。

1. **BlackBerry UEM Client** アイコンをタッチし続けます。
2. アイコンの右上にある [x] をタップします。
3. [削除] をタップします。

終了したら： デバイスをアクティブ化する場合は、デバイスに BlackBerry UEM Client を再インストールします。新しいアクティベーションパスワードが必要になる場合があります。BlackBerry UEM Self-Service を使用してアクティベーションパスワードを作成するか、管理者に問い合わせてください。

商標などに関する情報

©2022 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。

App Store は、Apple Inc. の商標です。iOS は、Cisco Systems, Inc. および/または米国およびその他の特定の国における関連会社の商標です。iOS® は、Apple Inc. からライセンスの許諾を受けて使用されます。Wi-Fi は、Wi-Fi Alliance の商標です。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 テクノロジーの側面を一般化された用語で記述している場合があります。BlackBerry は、本書に含まれる情報を定期的に変更する権利を留保します。ただし、BlackBerry には、本書への変更、更新、拡張、または他の追加を適時ユーザーに提供する義務はないものとします。

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

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

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

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

本書の限定事項、除外事項、および免責事項は、(A) 訴訟原因、請求、またはユーザーによる行為（契約違反、過失、不法行為、厳格責任、その他の法理論など）の性質に関係なく、この契約の基本目的または本書に記載されている救済策の根本的違反または不履行を免れるため、(B) BlackBerry およびその関連会社、その後継者、譲受人、代理業者、納入業者（通信事業者を含む）、認可された BlackBerry 販売業者（通信事業者を含む）およびその取締役、従業員、および請負業者に適用されます。

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

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

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

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

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

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

Published in Canada