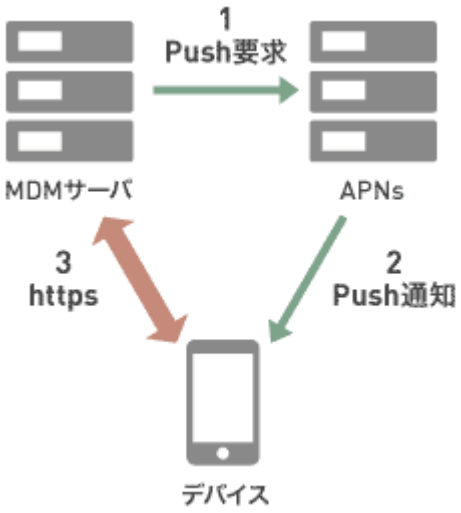
テクニカルセンター（技術情報）

MDM（Mobile Device Management）の仕組み

iOS 対応 MDM の概要

モバイルデバイス管理（MDM)は、iOS 4 以降、Apple が提供した機能で、ネットワーク経由で iOS デバイスを遠隔から管理するものです。iOS に対応する MDM は、大まかに次の流れでデバイスを管理します。



デバイスの管理を行なうサーバを、MDM サーバと呼びます。Apple によって提供される Push サービスは、APNs（Apple Push 通知サービス）と呼ばれ、世界中の iOS デバイスに Push 通知を配信します。APNs は、Apple Push Notification Service の略称です。

デバイスから APNs とのセッションを開く

デバイスが起動し、通信可能になると、APNs 間で TLS セッションを確立します。デバイスは APNs と常時接続され、APNs からの命令を即座に受け取れるようになります。

MDM サーバが Push 要求を送る

MDM サーバは、管理下にあるデバイスとの通信が必要になる度に、APNs に対して、デバイスへの Push 通知を要求します。

APNs からデバイスに Push 通知が届く

APNs に接続しているネットワーク（3G/LTE 回線、もしくは Wi-Fi）を通じて、APNs からデバイスに Push 通知が届けられます。この Push 通知は、iOS 組み込まれているシステムサービス（mdmd）を起動します。iOS の場合、MDM

を利用するためにデバイスにアプリケーションを新たにインストールする必要はありません。

デバイスと MDM サーバが通信する

iOS 組み込まれているシステムサービス（mdmd）は、あらかじめ登録された MDM サーバに対して https リクエストを送ります。MDM サーバはこれを受けて、デバイス上で実行すべき命令を伝えます。

命令の種類

iOS は、デバイス上で実行できる 5 系統の命令があります:

デバイス情報の取得

iOS のバージョンや、インストールされているアプリ一覧など、デバイスの情報を取得します。ただし、デバイスがロックされている時は、セキュリティ情報は取得できません。それ以外の情報は、ロック中でも取得できます。ロック中で情報が取得できなかったという情報は取得できます。

デバイスの設定

デバイスは、Apple Configurator で作成した設定ファイルを受け取ると、設定ファイルの指定通りに、デバイスの設定を変更します。デバイスがロックされている時は、設定ファイルをデバイスは受信できません。ただし、デバイスから設定を削除することは、ロック中でも可能です。

アプリの配布

iOS デバイスは、AppStore アプリや自社開発アプリをデバイスにインストールすることができます。デバイスがロックされている時は、アプリをデバイスにインストール（アップデートも）できません。ただし、デバイスからアプリを削除することは、ロック中でも可能です。

コンテンツの配布

iOS デバイスは、iBook Store のコンテンツや自社コンテンツを iBook にインストールすることができます。デバイスがロックされている時は、コンテンツをデバイスにインストール（アップデートも）できません。ロック中でも、デバイスからコンテンツを削除できます。

特殊命令

- パスコードの消去
- リモートロック
- リモートワイプ

iOS デバイスは、ロック中は暗号化されているため、デバイスがロックされ、スリープしている状態では実行されない命令があります。登録や更新系の命令は、ユーザがパスコードを入力し、デバイスのロックが解除されるまで実行が保留されます。削除系の命令（設定、アプリ、コンテンツ、リモートワイプ）は、ロック中でも即座に実行されます。

当然のことですが、デバイスの電源が入っていない場合やネットワークに繋がっていない場合など、Push 通知を受け取れない場合も、命令は実行されません。こうした場合は、電源が入り、ネットワークに接続し、デバイスが Push 通知を受け取れるようになるまで実行が保留されます。

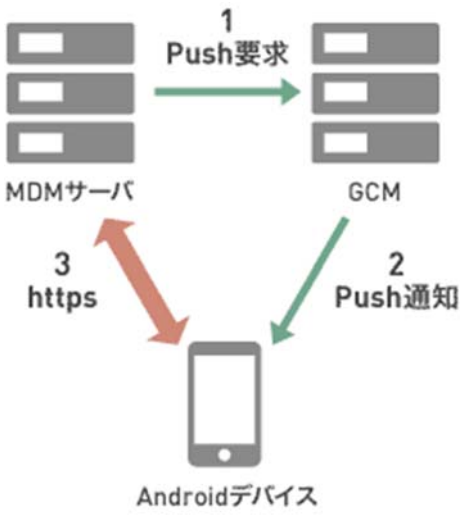
このように、MDM サーバから送った個々の命令がいつ実行されるかは、ネットワークの状態やロック中といった利用状況によって異なります。完了した命令は MDM サーバで確認することができます。ロック時に実行される削除系の命令と、実行されない登録・更新・参照系の命令の併用には注意が必要です。

デバイスの情報取得や設定だけを指して、MDM（Mobile Device Management）と呼ぶ人もいます。アプリ一覧の取得と配布を MAM（Mobile Application Management）と呼ぶ人もいます。さらにコンテンツの配布を MCM（Mobile Contents Management）と呼ぶ人もいます。iOS はサンドボックス構造のため、コンテンツはアプリ内に格納されます。Apple 社は、iOS デバイス上の設定やアプリ、コンテンツなどの資源を一括して扱います。そのため MAM や MCM のように呼ぶことはありません。

Android 対応 MDM の概要

Android デバイスが MDM を利用するには、Android アプリケーションである MDM クライアントをインストールする必要があります。MDM クライアントは、Android マーケット（Google Play）からインストールできます。

Android 対応 MDM は、大まかに次の流れでデバイスを管理します。



デバイスの管理を行なうサーバを MDM サーバと呼びます。GCM (Google プッシュ通知サービス)は、Google 社によって提供される Push サービスで、世界中の Android デバイス上の Android アプリケーション（MDM クライアントを含む）に Push 通知を送信します。GCM は、Google Cloud Messaging の略称です。

デバイス上の MDM クライアントから GCM のセッションを開く

Android デバイスが起動し、通信可能になると、MDM クライアントから **GCM** に接続し、TLS セッションを確立します。これにより、MDM クライアントは GCM と常時接続され、MDM クライアントは、**GCM** からの命令を即座に受け取ることができます。

MDM サーバが Push 要求を送る

MDM サーバは、管理下にある Android デバイス上の MDM クライアントとの通信が必要になると、まず、**GCM** に対し

て Push 通知をリクエストします。

GCM からデバイスに Push 通知が届く

GCM に接続しているネットワーク（3G/LTE 回線、もしくは Wi-Fi）を通じて、**GCM** から MDM クライアントに Push 通知が届けられます。この Push 通知は、MDM クライアントを起動します。

デバイスと MDM サーバが通信する

Push 通知を受けた MDM クライアントは、あらかじめ登録された MDM サーバに対して https リクエストを送ります。MDM サーバはこれを受けて、デバイス上で実行すべき命令を伝えます。

命令の種類

Android は、MDM で実行できる４つの系統の命令があります。

デバイス情報の取得

Android OS のバージョンや、インストールされているアプリ一覧など、デバイスの情報を取得します。

デバイスの設定

MDM 管理画面から、各種設定をデバイスに反映させます。

アプリの配布

MDM 管理画面から、Google Play アプリや自社開発アプリを、デバイスに導入します。

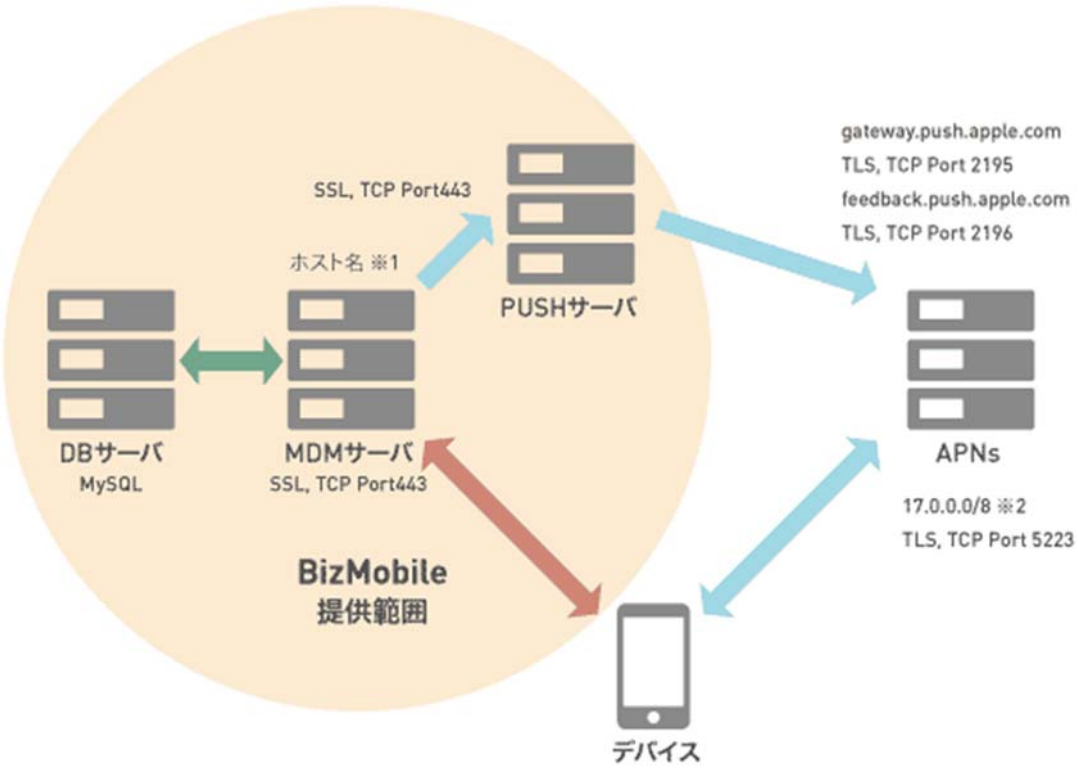
特殊命令

- パスコードの消去
- リモートロック
- リモートワイプ

Android デバイスの場合、命令はデバイスがロックされ、スリープしている状態でも実行されます、ただし、一部の機種ではスリープしている状態では実行されない場合があります。その場合、スリープ解除後に命令が実行されます。デバイスがネットワークに繋がっていないなど、Push 通知を受け取れない状態にあると、命令は実行されません。この場合、デバイスがネットワークに繋がるまで実行が保留されます。実行が完了したかどうかは MDM サーバ上で確認することができます。

BizMobile Go! for iOS の構成

BizMobile Go! for iOS の MDM 構成は次のようになっています。



※1　契約ごとに決定。

※2　Wi-Fi 接続時 17.0.0.0/8 のアドレスのうち、いずれか（開発者プログラム"Technical Note TN2265"より）。

セキュリティ

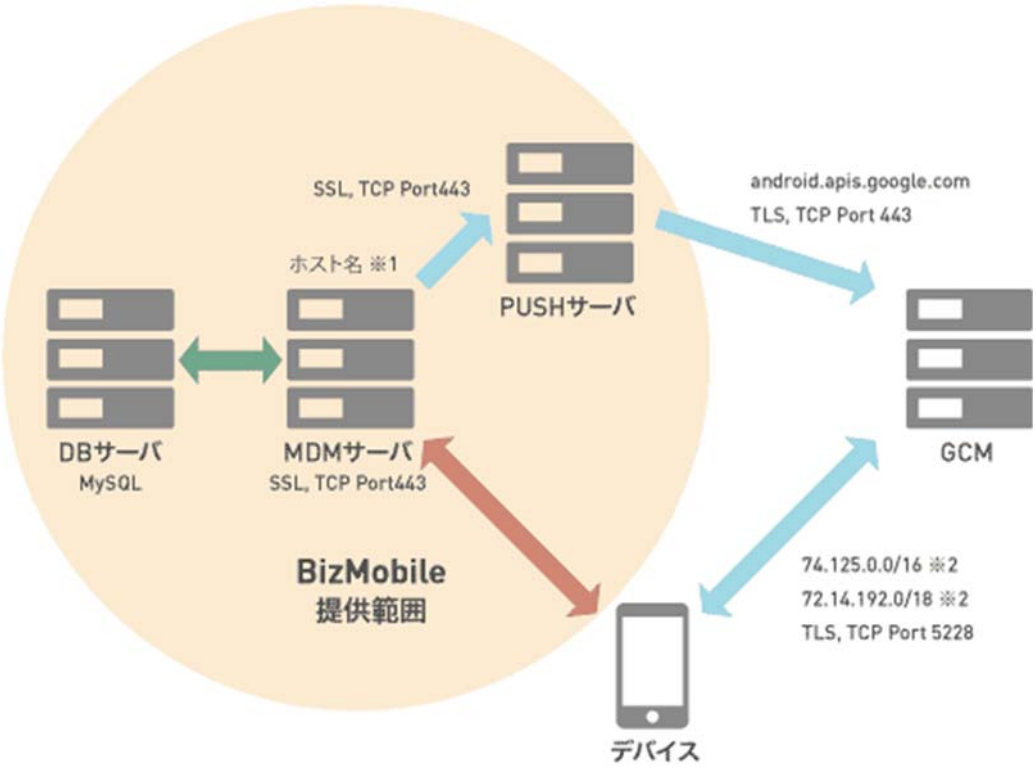
MDM サーバとデバイスとの接続には、SSL サーバ証明書とクライアント証明書を用いた相互認証が行なわれ、セキュリティ的に強固になっています。

クライアント証明書の元となる秘密鍵は、デバイスの内部で生成し、ハードウェアレベルのデバイス保護によって守られます。これにより、第三者がそのデバイスになりすましてサーバに接続することは困難となります。

デバイスは Push 通知に必要となるキーを、信頼するサーバにだけ受け渡します。このキーがなければ Push 通知を送ることは出来ません。更に、デバイスは最初に登録したサーバ以外に接続することはなく、第三者によってデバイスがコントロールされるリスクは小さくなります。

BizMobile Go! for Android の構成

BizMobile Go! for Android の MDM 構成は次のようになっています。



※ 1　契約ごとに決定。

※ 2　現在、Googleの保有するアドレスは 0.0.0.0/0:5228, 0.0.0.0/0:5229, 0.0.0.0/0:5230、TLS,TCP 5228, 5229, 5230です。

セキュリティ

MDM サーバとデバイスとの接続には、独自のトークンを用いて認証が行なわれます。トークンは MDM サーバにより生成されデバイス側に保存されます。（保存先は MDM クライアントアプリのみアクセス可能）第三者がそのデバイスになりすましてサーバに接続することは困難となります。デバイスは Push 通知に必要となるキーを、信頼するサーバにだけ受け渡します。このキーがなければ Push 通知を送ることは出来ません。更にデバイスは最初に登録したサーバ以外に接続することはなく、第三者によってデバイスがコントロールされるリスクは小さくなります。

Push 通知

iOS Push 証明書

Push 通知を送るためには、Apple から組織単位で Push 証明書を取得する必要があります。MDM サーバによって管理される各デバイスは、登録時に組織毎の Push 証明書と関連付けられます。他の組織に向けて発行された Push 証明書を使って通知が送られることはありません。

デバイス側の動作

iOS では、3G/LTE 回線、または Wi-Fi 接続を用いて Push 通知が行なわれます。Wi-Fi 接続では、デバイスと APNs との間で切れることのない TLS セッション（TCP ポート 5223）が作られ、APNs 側からデバイスに向けて通知が送られます。デバイスが充電中であるか、バッテリーに余裕のある限りは、15～30 分間隔でキープアライブが交換されます。Push 通知の動作は、デバイスによって若干異なります。

iPhone / iPad 回線モデル（3G/LTE）

デバイスが回線（3G/LTE）により通信できるときには、常に 3G 回線による通知が行なわれます。これらのデバイスでも、回線（3G/LTE）が使えないときには Wi-Fi 接続が利用されます。

iPad Wi-Fi モデル

iPad Wi-Fi モデルでは、Wi-Fi が使える状態にある限りは Push 通知を受け取れます。

デバイスがスリープ状態になっても、TLS セッションは切れることなく維持されます。APNs から通知が送られると、デバイスはスリープ状態から解除され、必要な処理が行なわれます。注意点として、iPad のバッテリーが 20%を切っているとセッションは切断され、Push 通知を受け取れなくなります。この場合、手動でスリープを解除するか、あるいはデバイスの充電を始めると、再びセッションが確立されます。

iPod touch

iPod touch では、デバイスを操作中である(スリープしていない)か、もしくは充電中のときにだけ、Push 通知を受け取れます。

通知の保留

デバイスが Push 通知を受け取れない状態にあるときは、APNs は最後に要求された通知内容をサーバ上に保持します。デバイスが APNs との通信を回復すると、保留されていた Push 通知が送られます。

Android Push 証明書

Push 通知を送るためには、Google アカウントが設定されていて Android Market アプリがインストールされている必要があります。MDM サーバによって管理される各デバイスは、登録時に特定のデバイス上の特定のアプリ（MDM クライアント）に関連付けられます。

デバイス側の動作

Android では、回線（3G/LTE）、または Wi-Fi 接続を用いて Push 通知が行なわれます。Wi-Fi 接続では、デバイスと GCM との間で切れることのない TLS セッション(TCP ポート 5228、5226、5226)が作られ、GCM 側からデバイスに向けて通知が送られます。

3G モデル

3G 回線（Wi-Fi が接続されていない場合）により通信ができるときには、3G/LTE 回線による通知が行なわれます。Wi-Fi が接続されている場合では、Wi-Fi が優先的に利用されます。

Wi-Fi モデル

Wi-Fi が使える状態にある限りは Push 通知を受け取れます。

スリープ状態

デバイスがスリープ状態になっても、TLS セッションは切れることなく維持されます。GCM から通知が送られると、必要な

処理が MDM クライアントで行なわれます。一部の機種ではスリープ状態では MDM クライアントで正しく処理が行われない場合があります。その場合はスリープ復帰後に必要な処理が再度実行されます。

通知の保留

デバイスが Push 通知を受け取れない状態にあるときは、デバイスが GCM との通信を回復すると、保留されていた Push 通知が送られます。一部の Android 端末では Push 通知を受け取れない状態では MDM クライアントで正しく処理が行われない場合があります。その場合は通信回復後に必要な処理が再度実行されます。

サーバ側の動作

一度に送れるデバイス上限（Push）数

一度に送れる Push 数に制限はありません。単位時間（１分間）に送信する Push 数はサーバ側で上限を定めています。

Push 通知の保存期間

MDM サーバにおけるオフライン状態のデバイスに対する要求は、デバイス登録解除されるまで永久に保存されます。APNs における Push 通知の保存期間は、Apple のドキュメントに「一定期間保存後に削除」とあるのみで明確には定義されていません。GCM における Push 通知の保存期間は、特に定義されていません。そのため BizMobile Go! は、１日１回 Push 通知を再送しています。

BizMobile 株式会社　（ビズモバイル株式会社）
〒101-0043　東京都千代田区神田富山町 5-1　神田ビジネスキューブ 3F
http://www.bizmobile.co.jp/