



# iPhone と iPad の配備 Exchange ActiveSync



## 対応している Exchange ActiveSync セキュリティポリシー

- ・ リモートワイブ
- ・ デバイスでのパスワード入力を要求
- ・ 最小のパスコード長
- ・ ローカルワイブされるまでのパスワード入力試行の最大数
- ・ 数字とアルファベットの組み合わせが必要
- ・ 分単位の休止時間 (1 ~ 60 分)

## そのほかの Exchange ActiveSync ポリシー (Exchange 2007 および 2010 のみ)

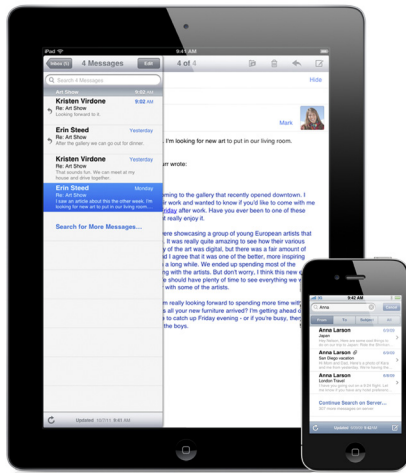
- ・ 単純なパスワードの許可または禁止
- ・ パスワードの有効期限
- ・ パスワードの履歴
- ・ ポリシーの更新間隔
- ・ パスワード内の複合文字の最小数
- ・ ロッキング中に手動のシンクを要求
- ・ カメラの使用を許可
- ・ ウェブブラウジングを許可

iPhone と iPad は、Microsoft Exchange ActiveSync (EAS) を使用して Microsoft Exchange Server と直接通信でき、Eメール、カレンダー、連絡先、タスクを自動的にアップデートします。さらに Exchange ActiveSync によって、ユーザはグローバルアドレス一覧 (GAL) にアクセスできるようになり、管理者はパスコードポリシーを適用したり、リモートワイブ機能を使えるようになります。iOS は、Exchange ActiveSync の Basic 認証と証明書ベースの認証の両方に対応しています。会社で現在 ActiveSync を使用している場合は、iPhone と iPad のサポートに必要なサービスがすでに構成されているため、追加の構成は必要ありません。会社で Exchange Server 2003、2007、2010 を使用しており、Exchange ActiveSync を初めて使用する場合は、次の手順を確認してください。

## Exchange ActiveSync の設定

### ネットワーク構成の概要

- ・ ファイアウォールでポート 443 が開いていることを確認します。会社で Outlook Web Access を使用している場合は、ポート 443 はすでに開かれている可能性があります。
- ・ フロントエンドサーバで、サーバ証明書がインストールされていることを確認し、IIS の Exchange ActiveSync 仮想ディレクトリで SSL を有効にします。
- ・ Microsoft ISA (Internet Security and Acceleration) Server を使用している場合は、サーバ証明書がインストールされていることを確認し、接続を受け入れられるようパブリック DNS をアップデートします。
- ・ ネットワークの DNS から、イントラネットのクライアントとインターネットのクライアントの両方に、Exchange ActiveSync サーバに外部から接続可能なアドレスが一つ返されることを確認します。この確認は、デバイスで双方の接続がアクティブな場合に同じ IP アドレスで接続し、通信できるようにするために必要です。
- ・ Microsoft ISA Server を使用している場合は、Web リスナーと Exchange Web クライアントアクセス公開ルールを作ります。詳しくは、Microsoft の製品ドキュメントを参照してください。
- ・ すべてのファイアウォールとネットワーク機器で、アイドルセッションタイムアウトを 30 分に設定します。ハートビートおよびタイムアウトの間隔については、Microsoft Exchange の製品ドキュメント (<http://technet.microsoft.com/en-us/library/cc182270.aspx>) を参照してください。
- ・ Exchange システムマネージャを使用して、モバイル機能、ポリシー、およびデバイスセキュリティ設定を構成します。Exchange Server 2007 および 2010 の場合は、Exchange 管理コンソールで行います。
- ・ Microsoft Exchange ActiveSync Mobile Administration Web ツールをダウンロードしてインストールします。このツールはリモートワイブを実行するために必要です。Exchange Server 2007 および 2010 の場合は、Outlook Web Access または Exchange 管理コンソールを使用してリモートワイブを実行することもできます。



### その他の Exchange ActiveSync サービス

- グローバルアドレス一覧の検索
- カレンダーでの出席依頼の承諾と作成
- タスクのシンク
- Eメールメッセージのフラグ設定
- Exchange Server 2010 による返信のシンクおよびフラグの転送
- Exchange Server 2007 および 2010 での Eメール検索
- 複数の Exchange ActiveSync アカウントのサポート
- 証明書ベースの認証
- 選択したフォルダへの Eメールのプッシュ
- 自動検出

### Basic 認証 (ユーザ名とパスワード)

- Active Directory サービスを使用して、特定のユーザまたはグループの Exchange ActiveSync を有効にします。Exchange Server 2003、2007、2010 では、これらは組織レベルですべてのモバイルデバイスに対してデフォルトで有効になっています。Exchange Server 2007 および 2010 の場合は、Exchange 管理コンソールの「受信者の構成」を確認してください。
- デフォルトでは、Exchange ActiveSync は Basic 認証を行うように構成されています。Basic 認証を使用する場合は、認証中に資格情報が確実に暗号化されるように、SSL を有効にすることをお勧めします。

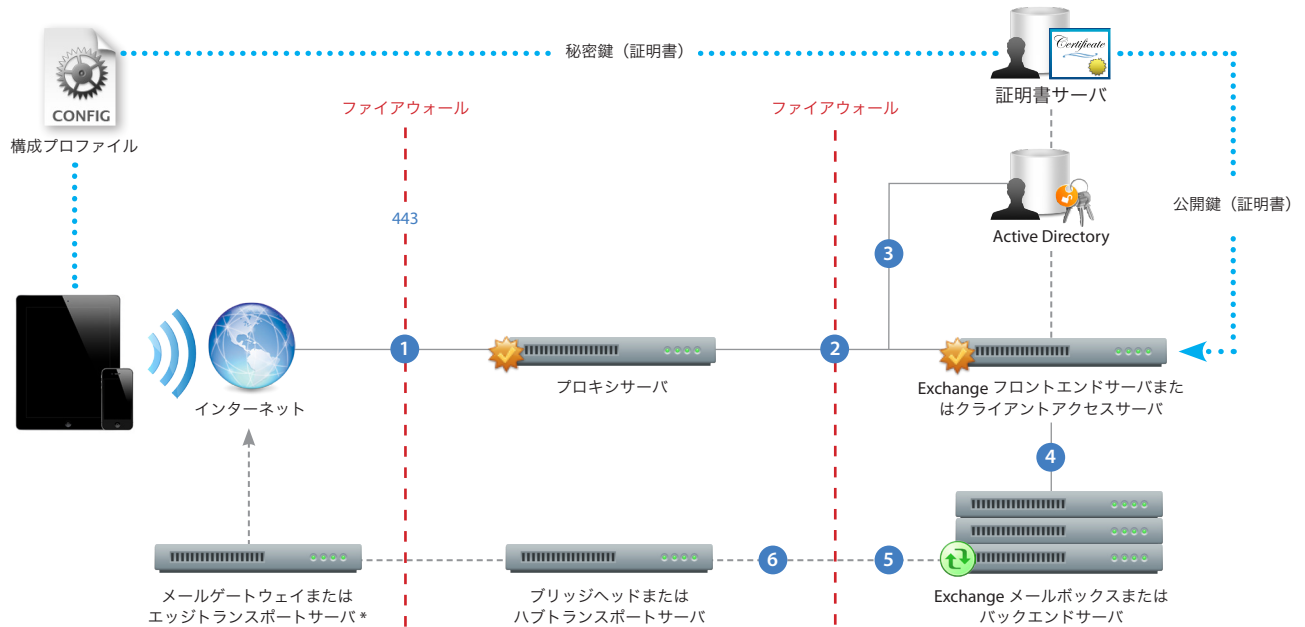
### 証明書ベースの認証

- ドメイン内のメンバーサーバまたはドメインコントローラにエンタープライズ証明書サービスをインストールします (これが認証局サーバとなります)。
- Exchange フロントエンドサーバまたはクライアントアクセスサーバ上の IIS を、Exchange ActiveSync 仮想ディレクトリに対する証明書ベースの認証を受け入れるように構成します。
- すべてのユーザに対して証明書を許可または要求するには、「Basic 認証」をオフにし、「クライアント証明書を受諾する」または「クライアント証明書を要求する」を選択します。
- 認証局サーバを使用してクライアント証明書を生成します。公開鍵を書き出し、この鍵を使用するように IIS を構成します。秘密鍵を書き出し、構成プロファイルを使用してこの鍵を iPhone や iPad に配信します。証明書ベースの認証は、構成プロファイルでのみ構成できます。

証明書サービスについて詳しくは、Microsoft が提供するリソースを参照してください。

## Exchange ActiveSync の配備シナリオ

iPhone や iPad と一般的な Microsoft Exchange Server 2003、2007、2010 との接続例を示します。



\* ネットワーク構成によっては、メールゲートウェイまたはエッジトランスポートサーバが、境界ネットワーク内 (DMZ) にある場合があります。

- 1 iPhone や iPad は、ポート 443 (HTTPS) を使用して Exchange ActiveSync サービスへのアクセスを要求します (このポートは、Outlook Web Access やその他のセキュリティ保護されたウェブサービスで使用されるポートと同じものです。そのため、多くの場合このポートはすでに開かれており、SSL で暗号化された HTTPS トラフィックを受け入れるように構成されています)。
- 2 ISA は Exchange フロントエンドサーバまたはクライアントアクセスサーバへアクセスを提供します。ISA は、プロキシ (多くの場合はリバースプロキシ) として構成され、Exchange Server にトラフィックを通します。
- 3 Exchange Server は、Active Directory サービスおよび認証局サーバを経由して外部からのユーザを認証します (証明書ベースの認証を使用している場合)。
- 4 ユーザが適切な資格情報や証明書を与え、Exchange ActiveSync サービスへのアクセスがある場合、フロントエンドサーバはバックエンドサーバ上の適切なメールボックスへの接続を確立します (Active Directory グローバルカタログ経由)。
- 5 Exchange ActiveSync 接続が確立されます。アップデートや変更はワイヤレスでプッシュされ、iPhone または iPad 上で行われた変更は、Exchange Server に反映されます。
- 6 iPhone または iPad 上の送信済みメールアイテムも、Exchange ActiveSync によって Exchange Server に反映されます (手順 5)。E メールを外部の受信者に送る場合、E メールは SMTP を使って、ブリッジヘッド (またはハブトランスポート) サーバから外部メールゲートウェイ (またはエッジトランスポートサーバ) に送信されます。ネットワーク構成によっては、外部メールゲートウェイまたはエッジトランスポートサーバが、境界ネットワーク内またはファイアウォールの外にある場合があります。