



iPhone と iPad の配備 デジタル証明書



サポートされている証明書および固有名のフォーマット：

- iOS は RSA キーを使用した X.509 証明書をサポートしています。
- .cer、.crt、.der、.p12、.pfx の拡張子を認識できます。

ルート証明書

iOS には、多数のルート証明書があらかじめインストールされています。プリインストールされているシステムルートの一覧を確認するには、Apple のサポート記事 (http://support.apple.com/kb/HT5012?viewlocale=ja_JP) を参照してください。プリインストールされたルート証明書ではなく、社内で作成した自己署名されたルート証明書などを使用している場合は、本文書の「証明書の配布とインストール」に記載されているいずれかの方法で、証明書を配布することができます。

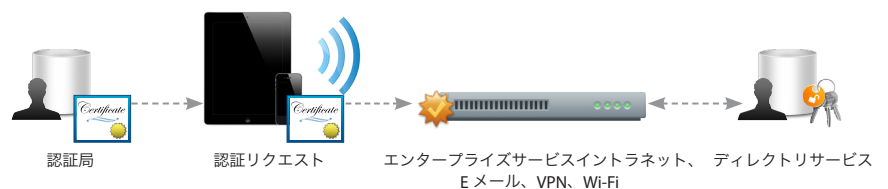
iOS はデジタル証明書をサポートしているので、ビジネスユーザは企業サービスに安全かつ効率的にアクセスできます。デジタル証明書は、公開鍵、ユーザに関する情報、証明書を発行した認証局に関する情報で構成されています。デジタル証明書は効率的な認証、データ整合性、暗号化を可能にする識別方法です。

iPhone と iPad では、証明書は様々な目的で使用されます。デジタル証明書によって署名されたデータは、情報が書き換えられていないことを確認するのに役立ちます。また、証明書は、作成者または署名者の身元を保証するために使用できます。さらに、構成プロファイルやネットワーク通信を暗号化して、機密情報や個人情報をより確実に保護するためにも使用されます。

iOS で証明書を使う

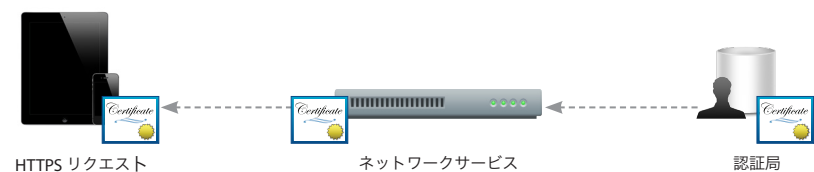
デジタル証明書

デジタル証明書を使って企業サービスに対するユーザ認証を安全に行うことができます。ユーザ名、パスワード、ソフトトークンは必要ありません。iOS では、Microsoft Exchange ActiveSync、VPN、Wi-Fi ネットワークへの接続に対する、証明書ベースの認証をサポートしています。



サーバ証明書

デジタル証明書はネットワーク通信の検証および暗号化に使用することもできます。これにより内部および外部のウェブサイトとの通信を安全に行えるようになります。Safari ブラウザは X.509 デジタル証明書の有効性を確認し、最大 256 ビットの AES 暗号化を使用した安全なセッションを確立します。これにより、そのウェブサイトの身元が正当で、サイトとの通信が安全であることを確認でき、個人情報や機密情報の傍受を防止できます。



証明書の配布とインストール

iPhone と iPad に証明書を配布する方法はシンプルです。証明書を受け取ったら、タップして内容を確認してから、もう一度タップして証明書をデバイスに追加するだけです。固有名証明書をインストールする場合には、この証明書を保護するためのパスフレーズを要求するメッセージが表示されます。証明書の真偽が確認できない場合、デバイスに追加される前に警告が表示されます。

構成プロファイルを使用して証明書をインストールする

Exchange、VPN、Wi-Fi などの企業サービスに関する設定を配布するために構成プロファイルを使用している場合は、証明書をプロファイルに追加することで効率よく配布できます。

メールまたは Safari を使用して証明書をインストールする

証明書が E メールで送信された場合、証明書は添付ファイルとして表示されます。Safari を使用して、証明書をウェブページからダウンロードするという方法もあります。証明書を安全なウェブサイトでホストして、証明書をデバイスにダウンロードするための URL をユーザに知らせることもできます。

SCEP (Simple Certificate Enrollment Protocol) を使って証明書をインストールする

SCEP は、証明書を大規模に配布するための簡単な方法を提供できるように設計されています。この SCEP により、デジタル証明書を無線 (OTA) で iPhone と iPad に登録できます。この証明書は、企業サービスに対する認証と、モバイルデバイス管理 (MDM) サーバへの登録に使用できます。

SCEP および無線 (OTA) 登録について詳しくは、www.apple.com/jp/iphone/business/resources を参照してください。

証明書の削除と無効化

インストールされている証明書を手動で削除するには、「設定」>「一般」>「プロファイル」の順にタップします。アカウントやネットワークへのアクセスに必要な証明書を削除した場合、それらのサービスには接続できなくなります。

証明書をワイヤレスで削除するには、MDM サーバを使用します。このサーバでは、デバイス上のすべての証明書を表示でき、インストールされている証明書を削除できます。

また、証明書のステータスを確認できるように OCSP (Online Certificate Status Protocol) をサポートしています。OCSP に対応した証明書を使用している場合、iOS はリクエストされたタスクを実行する前に、証明書が無効になっていないことを確認します。