iOS構成プロファイル リファレンス

Developer

目次

構成プロファイルキーのリファレンス

注意　このドキュメントは、以前は『*iPhone Configuration Profile Reference*』というタイトルでした。

構成プロファイルはXML形式のファイルで、構成情報をiOSベースのデバイスに配布するために使います。多数のデバイスの構成作業を一括して行う、独自の電子メール設定やネットワーク設定をまとめて実施する、多数のデバイスの認証を行う、などの目的に有用です。

iOS構成プロファイルには次のような多数の設定項目があります。

パスコードのポリシー

デバイスの機能制限（カメラを無効にするなど）

Wi-Fiの設定

VPNの設定

電子メールサーバの設定

Exchangeの設定

LDAPディレクトリサービスの設定

CalDAVカレンダーサービスの設定

ウェブクリップ

資格情報とその鍵

携帯電話網に関する高度な設定

構成プロファイルはプロパティリスト形式で、データ値はBase64でエンコードして格納します。`.plist`形式の読み書きはどのようなXMLライブラリでも可能です。

構成プロファイルの配布方法は4通りあります。

- デバイス同士を物理的に接続（『*iPhone Configuration Utility*』を参照）
- 電子メールで配布
- ウェブページ上で配布
- Over-the-Air構成を利用（『*Over-the-Air Profile Delivery and Configuration*』を参照）

iOSには暗号化の機能もあり、プロファイルの内容を保護やデータの整合性保証が可能です。暗号化したプロファイルの配布については、『*iPhoneConfigurationUtility*』または『*Over-the-AirProfileDelivery and Configuration*』を参照してください。

この資料では、iOS構成プロファイルのキーを説明し、実際に作成したXMLペイロードの例を示します。

> **注意** 実際に構成プロファイルを記述する前に、iPhone Configuration Utility（iPCU）を使ってその骨組みを生成しておくとよいでしょう。これをもとに、必要な箇所を修正していくと便利です。

構成プロファイルキー

構成プロファイルはプロパティリスト形式で、その最上位には次のようなキーがあります。

キー	型	内容
`HasRemovalPasscode`	ブール型	必須ではありません。削除パスコードがある場合は`true`。
`IsEncrypted`	ブール型	必須ではありません。プロファイルに暗号化を施している場合は`true`。
`IsManaged`	ブール型	必須ではありません。プロファイルが現行MDMサービスに組み込まれていれば`true`。
`PayloadContent`	配列	必須ではありません。ペイロード辞書の配列。IsEncryptedが`true`の場合は存在しません。
`PayloadDescription`	文字列	必須ではありません。プロファイルの説明。これが「Detail」画面に表示されます。このプロファイルをインストールするべきか、ユーザが判断できるように記述してください。
`PayloadDisplayName`	文字列	必須ではありません。（人が読める形の）プロファイル名。これが「Detail」画面に表示されます。一意的でなくても構いません。
`PayloadIdentifier`	文字列	プロファイルの特定に用いる、逆DNS形式の識別子（たとえば「com.example.myprofile」）。新しいプロファイルが渡されたとき、既存のプロファイルを置き換えるか、新たに追加するかを判断するために使います。

キー	型	内容
PayloadOrganization	文字列	必須ではありません。プロファイルを提供する組織名。人が読める形の文字列で指定します。
PayloadUUID	文字列	プロファイルを特定する汎用一意識別子（UUID、Universally Unique IDentifier）。実際の中身は何でも構いませんが、世界全体で一意な識別子でなければなりません。Mac OS Xでは、uuidgenを使って生成できます。
PayloadRemoval-Disallowed	ブール型	必須ではありません。このキーが存在し値がtrueであれば、ユーザはプロファイルを削除できません（削除パスワードが設定されており、ユーザがそれを知っている場合を除く）。 この方法でロックされている場合、プロファイルを新しいバージョンに置き換えるためには、その識別子が一致し、同じ認証者が署名している必要があります。
PayloadType	文字列	現状では、設定可能な値は「Configuration」に限ります。
PayloadVersion	数値	プロファイル形式のバージョン番号。構成プロファイル全体のバージョンを表します。プロファイルに含まれる個々のペイロードのバージョンではありません。 現状では、常に1を指定してください。
SignerCertificates	配列	必須ではありません。プロファイルの署名に用いた証明書を先頭に置き、その後に中間証明書を列挙した配列。DERエンコードを施したX.509形式で指定します。

ペイロード辞書のキーについては次節で説明します。

どのペイロードにも共通なペイロード辞書のキー

PayloadContent値がペイロードに与えられていれば、配列の各要素は、構成ペイロードを表す辞書になります。以下のキーはどのペイロードにも共通です。

キー	型	内容
PayloadType	文字列	ペイロードの型。詳しくは“ペイロード特有のプロパティキー”（6 ページ）を参照してください。
PayloadVersion	数値	個々のペイロードのバージョン番号。 プロファイルには異なるバージョンのペイロードが混在していても構いません。たとえば、iOSのVPNソフトウェアに新しいバージョンのペイロードを組み込んで新機能に対応する一方、電子メールに関するペイロードは従来のままにしておく、といったことが可能です。
PayloadIdentifier	文字列	当該ペイロードの特定に用いる、逆DNS形式の識別子。通常、ルートレベルのPayloadIdentifier値と同じ識別子に、追加要素を付加して指定します。
PayloadUUID	文字列	ペイロードを特定する汎用一意識別子。実際の中身は何でも構いませんが、世界全体で一意な識別子でなければなりません。Mac OS Xでは、uuidgenを使って生成できます。
PayloadDisplayName	文字列	必須ではありません。（人が読める形の）ペイロード名。これが「Detail」画面に表示されます。一意的でなくても構いません。
PayloadDescription	文字列	必須ではありません。このペイロードの説明。人が読める形の文字列で指定します。これが「Detail」画面に表示されます。
PayloadOrganization	文字列	必須ではありません。このペイロードを提供する組織名。人が読める形の文字列で指定します。 プロファイル全体を提供する組織とは同じでなくても構いません。

ペイロード特有のプロパティキー

標準的なペイロードキー（“どのペイロードにも共通なペイロード辞書のキー”（5 ページ）を参照）に加え、個々のペイロード型に特有のキーもあります。以下、ペイロード特有のキーについて説明します。

プロファイルの「Removal Password」ペイロード

「Removal Password」ペイロードは、`PayloadType`の値として`com.apple.profileRemovalPassword`を与えることにより指定します。

ここで指定するパスワードは、ロック済みの構成プロファイルをデバイスから削除する際に使います。このペイロードが存在し、パスワード値が設定されていれば、ユーザがプロファイルの「削除」ボタンをタップしたとき、パスワードを尋ねられるようになります。このペイロードは暗号化してプロファイルに格納するようになっています。

キー	型	値
`RemovalPassword`	文字列	必須ではありません。プロファイルの削除パスワードを指定します。

「Passcode Policy」ペイロード

「Passcode Policy」ペイロードは、`PayloadType`の値として`com.apple.mobiledevice.passwordpolicy`を与えることにより指定します。

このペイロード型が存在すれば、デバイスは英数字から成るパスコードの入力画面を表示するようになります。パスコードに長さや複雑さの制限はありません。

どのペイロードにも共通の設定項目に加え、このペイロードには次のようなキーが定義されています。

キー	型	値
`allowSimple`	ブール型	必須ではありません。デフォルト値は`true`。簡単なパスコードを許可するか否かを指定します。ここで言う簡単なパスコードとは、同じ文字の繰り返し、あるいは単純上昇/下降形（123、CBAなど）の文字列が含まれるもののことです。`false`を設定すれば、minComplexCharsの値として「1」を指定したのと同じ意味になります。
`forcePIN`	ブール型	必須ではありません。デフォルト値はNO。ユーザがPINを設定するよう強制するか否かを表します。この値をYESとするだけで（他の値は指定しなくても）、長さや強度は別として、パスコードの入力を強制することになります。

キー	型	値
maxFailedAttempts	数値	必須ではありません。デフォルト値は11。指定可能な値の範囲は[2...11]。ロック画面で誤ったパスコードを入力しても、この回数までならば再試行が可能です。この回数を超えてしまうとデバイスはロックされ、所定のiTunesに接続しなければ解除できません。
maxInactivity	数値	必須ではありません。デフォルト値は無限大。ここで指定した時間（分単位）デバイスがアイドル状態になると、（ユーザがロック解除しない限り）自動的にロックがかかります。この上限時間に達するとデバイスはロックされ、解除するためにはパスコードが必要になります。
maxPINAgeInDays	数値	必須ではありません。デフォルト値は無限大。パスコードを変更せずに利用できる最大日数を指定します。この日数が経過すると、パスコードを変更しない限りデバイスをロック解除できません。
minComplexChars	数値	必須ではありません。デフォルト値は0。パスコードに含まれるべき「複雑な」文字の最小数を指定します。ここで言う「複雑な」文字とは、「&%$#」のような、英数字以外の文字のことです。
minLength	数値	必須ではありません。デフォルト値は0。パスコードの長さの最小値を表します。やはり必須ではない「minComplexChars」とは独立に指定できます。
requireAlphanumeric	ブール型	必須ではありません。デフォルト値はNO。英字（「abcd」など）を入力しなければならないか、数字だけでよいか、を表します。
pinHistory	数値	必須ではありません。パスコードを変更する際、変更履歴をいくつまでさかのぼって重複を確認するか、を表します。最小値は1、最大値は50です。
manualFetching-WhenRoaming	ブール型	必須ではありません。trueであれば、ローミングの際、プッシュ操作は無効になります。ユーザは手作業で新しいデータをフェッチしなければなりません。
maxGracePeriod	数値	必須ではありません。パスコードを入力せずに電話のロックを解除できる、最大猶予時間（分単位）を表します。デフォルト値は0、すなわち、猶予時間はなく直ちにパスコードを要求されます。

「Email」ペイロード

「Email」ペイロードは、`PayloadType`の値として`com.apple.email.managed`を与えることにより指定します。

これを指定すると、デバイス上に電子メールアカウントが作成されます。

どのペイロードにも共通の設定項目に加え、このペイロードには次のようなキーが定義されています。

キー	型	値
`EmailAccount-Description`	文字列	必須ではありません。電子メールアカウントの説明を、人が読める形の文字列で指定します。これが「Mail and Settings」アプリケーションに表示されます。
`EmailAccountName`	文字列	必須ではありません。アカウントの完全ユーザ名。送信メッセージなどに埋め込まれます。
`EmailAccountType`	文字列	`EmailTypePOP`、`EmailTypeIMAP`のいずれかを指定します。このアカウントが用いるプロトコルを定義します。
`EmailAddress`	文字列	アカウントの完全電子メールアドレスを指定します。ペイロードに指定がなければ、プロファイルのインストール時に尋ねられます。
`IncomingMailServer-Authentication`	文字列	受信メールの認証スキームを表します。`EmailAuthPassword`、`EmailAuthNone`のいずれかを指定します。
`IncomingMailServer-HostName`	文字列	受信メールサーバのホスト名（またはIPアドレス）を指定します。
`IncomingMailServer-PortNumber`	数値	必須ではありません。受信メールサーバのポート番号を指定します。指定しなければ、プロトコルによって決まっているデフォルトのポート番号になります。
`IncomingMailServer-UseSSL`	ブール型	必須ではありません。デフォルト値は`true`。受信メールサーバが認証用にSSLを利用するか否かを指定します。

キー	型	値
`IncomingMailServer-Username`	文字列	電子メールアカウントのユーザ名を指定します。通常は電子メールアドレスの「@」より前の部分と同じです。ペイロードに指定がなく、当該アカウントが受信メールの認証を要すると設定されていれば、プロファイルのインストール時に尋ねられます。
`IncomingPassword`	文字列	必須ではありません。受信メールサーバのパスワード。これが指定されている場合、プロファイルに暗号化を施す必要があります。
`OutgoingPassword`	文字列	必須ではありません。送信メールサーバのパスワード。これが指定されている場合、プロファイルに暗号化を施す必要があります。
`OutgoingPasswordSame-AsIncomingPassword`	ブール型	必須ではありません。**true**であれば、ユーザがパスワードを尋ねられるのは1度だけで、それ以降は、送信メール、受信メールともにそのパスワードを再利用するようになります。
`OutgoingMailServer-Authentication`	文字列	送信メールの認証スキームを指定します。指定できる値はEmailAuthPassword、EmailAuthNoneのいずれかです。
`OutgoingMailServer-HostName`	文字列	送信メールサーバのホスト名（またはIPアドレス）を指定します。
`OutgoingMailServer-PortNumber`	数値	必須ではありません。送信メールサーバのポート番号を指定します。指定がなければ、ポート25、587、465の順に試みます。
`OutgoingMailServer-UseSSL`	ブール型	必須ではありません。デフォルト値はYes。送信メールサーバが認証用にSSLを利用するか否かを指定します。
`OutgoingMailServer-Username`	文字列	電子メールアカウントのユーザ名を指定します。通常は電子メールアドレスの「@」より前の部分と同じです。ペイロードに指定がなく、当該アカウントが送信メールの認証を要すると設定されていれば、プロファイルのインストール時に尋ねられます。

キー	型	値
PreventMove	ブール型	必須ではありません。デフォルト値はfalse。 trueならば、この電子メールアカウントから別のアカウントにメッセージを移動することはできません。また、メッセージの送信元アカウント以外から、転送や返信をすることも禁じます。 **設定可能なバージョン：**iOS 5.0以降。
PreventAppSheet	ブール型	必須ではありません。デフォルト値はfalse。 trueならば、このアカウントから他社製アプリケーションでメールを送信することはできません。 **設定可能なバージョン：**iOS 5.0以降。
SMIMEEnabled	ブール型	必須ではありません。デフォルト値はfalse。 trueならば、このアカウントはS/MIMEに対応しています。 **設定可能なバージョン：**iOS 5.0以降。
SMIMESigningCertificateUUID	文字列	必須ではありません。このアカウントから送信するメッセージに署名するために用いる、識別証明書のPayloadUUID。 **設定可能なバージョン：**iOS 5.0以降。
SMIMEEncryptionCertificateUUID	文字列	必須ではありません。このアカウントで受信したメッセージの復号に用いる、識別証明書のPayloadUUID。 **設定可能なバージョン：**iOS 5.0以降。

「Web Clip」ペイロード

「Web Clip」ペイロードは、PayloadTypeの値としてcom.apple.webClip.passwordpolicyを与えることにより指定します。

「Web Clip」ペイロードには、ユーザのホーム画面にWeb Clipを表示し、ブックマークとして使えるようにする働きがあります。

どのペイロードにも共通の設定項目に加え、このペイロードには次のようなキーが定義されています。

キー	型	値
URL	文字列	「Web Clip」をクリックしたときに開くURL。URLは「HTTP」または「HTTPS」で始まるものでなければ動作しません。
Label	文字列	ホーム画面に表示される「Web Clip」の名前。
Icon	データ	必須ではありません。ホーム画面に表示されるPNGアイコン。大きさは59×60ピクセルとします。指定がなければ白い矩形の表示になります。
IsRemovable	ブール型	必須ではありません。Noであれば、ユーザは「Web Clip」を削除できませんが、プロファイルを削除すれば同時に削除されます。

「Restrictions」ペイロード

「Restrictions」ペイロードは、PayloadTypeの値としてcom.apple.applicationaccessを与えることにより指定します。

管理者はこのペイロードを用いて、デバイスのある機能（写真を撮るなど）をユーザが使えないよう制限できます。

どのペイロードにも共通の設定項目に加え、このペイロードには次のようなキーが定義されています。

キー	型	値
allowAppInstallation	ブール型	必須ではありません。falseであればApp Storeは使えなくなり、ホーム画面から当該アイコンがなくなります。ユーザはApp Storeのアプリケーションをインストール/更新できません。
AllowAssistant	ブール型	必須ではありません。falseであればSiriが使えなくなります。デフォルト値はtrueです。
allowCamera	ブール型	必須ではありません。falseであればカメラはまったく使えなくなり、ホーム画面から当該アイコンがなくなります。ユーザは写真を撮れません。
allowExplicitContent	ブール型	必須ではありません。falseであれば、iTunes Storeから購入した、未成年者禁止の音楽や動画が見えなくなります。未成年者禁止である旨の設定は、その販売者（レコード会社など）が、iTunes Storeを介して販売する際に行います。

キー	型	値
`allowScreenShot`	ブール型	必須ではありません。falseならば、画面のスクリーンショットを保存できなくなります。
`allowYouTube`	ブール型	必須ではありません。falseならばYouTubeアプリケーションが使えなくなり、ホーム画面から当該アイコンがなくなります。
`allowiTunes`	ブール型	必須ではありません。falseならばiTunes Music Storeが使えなくなり、ホーム画面から当該アイコンがなくなります。プレビューや購入、ダウンロードはできません。
`forceITunesStore-PasswordEntry`	ブール型	必須ではありません。`true`ならば、購入の際、その都度iTunesパスワードの入力を求められるようになります。 **設定可能なバージョン：**iOS 5.0以降。
`allowSafari`	ブール型	必須ではありません。`false`ならばSafari（ウェブブラウザ）が使えなくなり、ホーム画面から当該アイコンがなくなります。ウェブクリップを開くこともできません。
`allowUntrusted-TLSPrompt`	ブール型	必須ではありません。`false`ならば、信頼できないHTTPS証明書を、ユーザに問い合わせることなく自動的に拒否するようになります。 **設定可能なバージョン：**iOS 5.0以降。
`allowCloudBackup`	ブール型	必須ではありません。`false`ならば、デバイス上のファイルをiCloudにバックアップしないようになります。 **設定可能なバージョン：**iOS 5.0以降。
`allowCloudDocument-Sync`	ブール型	必須ではありません。`false`ならば、ドキュメントやキー値をiCloudに同期する処理が無効になります。 **設定可能なバージョン：**iOS 5.0以降。
`allowPhotoStream`	ブール型	必須ではありません。`false`ならばPhoto Streamが無効になります。 **設定可能なバージョン：**iOS 5.0以降。

「LDAP」ペイロード

「LDAP」ペイロードは、`PayloadType`の値として`com.apple.ldap.account`を与えることにより指定します。

LDAPサーバの使い方を管理するペイロードで、アカウント情報（必要な場合）、問い合わせ時に用いる一連のLDAP検索ポリシーなどを設定します。

どのペイロードにも共通の設定項目に加え、このペイロードには次のようなキーが定義されています。

キー	型	値
`LDAPAccount-Description`	文字列	必須ではありません。アカウントの説明。
`LDAPAccountHostName`	文字列	ホスト。
`LDAPAccountUseSSL`	ブール型	SSLを使うか否か。
`LDAPAccountUserName`	文字列	必須ではありません。ユーザ名。
`LDAPAccountPassword`	文字列	必須ではありません。これが指定されている場合、プロファイルに暗号化を施す必要があります。
`LDAPSearchSettings`	辞書	最上位コンテナオブジェクト。各アカウントに複数持たせても構いません。少なくとも1つあると有用でしょう。 各`LDAPSearchSettings`オブジェクトは、検索の開始点となるLDAP木のノードと、検索範囲（当該ノード、当該ノードおよび直下の子、当該ノードおよびその子孫全体、のいずれか）を表します。
`LDAPSearchSetting-Description`	文字列	必須ではありません。この検索設定の説明。
`LDAPSearchSetting-SearchBase`	文字列	検索の開始点となるノードのパス。たとえば次のように宣言します。 `ou=people,o=example corp`

キー	型	値
LDAPSearchSetting-Scope	文字列	再帰的検索の範囲を表します。 次のいずれかの値を指定します。 LDAPSearchSettingScopeBase：SearchBaseで指定したノードのみ。 LDAPSearchSettingScopeOneLevel：当該ノードおよび直下の子。 LDAPSearchSettingScopeSubtree：当該ノードおよびその子孫全体。

「CalDAV」ペイロード

「CalDAV」ペイロードは、PayloadTypeの値としてcom.apple.caldav.accountを与えることにより指定します。

CalDAVアカウントをユーザのカレンダーリストに追加する働きがあります。

どのペイロードにも共通の設定項目に加え、このペイロードには次のようなキーが定義されています。

キー	型	値
CalDAVAccount-Description	文字列	必須ではありません。アカウントの説明。
CalDAVHostName	文字列	サーバアドレス。
CalDAVUsername	文字列	ユーザのログイン名。
CalDAVPassword	文字列	必須ではありません。ユーザのパスワード。
CalDAVUseSSL	ブール型	SSLを使うか否か。
CalDAVPort	数値	必須ではありません。サーバへの接続に用いるポート番号。
CalDAVPrincipalURL	文字列	必須ではありません。ユーザのカレンダーを指すベースURL。

「Calendar Subscription」ペイロード

「Calendar Subscription」ペイロードは、PayloadTypeの値として
com.apple.subscribedcalendar.accountを与えることにより指定します。

予約したカレンダーをユーザのカレンダーリストに追加する働きがあります。

どのペイロードにも共通の設定項目に加え、このペイロードには次のようなキーが定義されています。

キー	型	値
SubCalAccountDescription	文字列	必須ではありません。アカウントの説明。
SubCalAccountHostName	文字列	サーバアドレス。
SubCalAccountUsername	文字列	ユーザのログイン名。
SubCalAccountPassword	文字列	ユーザのパスワード。
SubCalAccountUseSSL	ブール型	SSLを使うか否か。

「SCEP」ペイロード

「SCEP（Simple Certificate Enrollment Protocol）」ペイロードは、PayloadTypeの値として com.apple.encrypted-profile-serviceを与えることにより指定します。

電話とSCEPサーバを関連付ける働きがあります（『*Over-the-Air Profile Delivery and Configuration*』を参照）。

どのペイロードにも共通の設定項目に加え、このペイロードには次のようなキーが定義されています。

キー	型	値
URL	文字列	SCEPのURL。SCEPについて詳しくは、『*Over-the-Air Profile Delivery and Configuration*』を参照してください。
Name	文字列	必須ではありません。SCEPサーバが認識可能な任意の文字列。たとえば「example.org」のようなドメイン名を設定します。認証局に複数のCA証明書がある場合、その識別のために利用できます。

キー	型	値
Subject	配列	必須ではありません。X.500名をOIDと値の配列の形で表したもの。たとえば「/C=US/O=Apple Inc./CN=foo/1.2.5.3=bar」という記述は次のように変換されます。 [[["C", "US"]], [["O", "Apple Inc."]], ..., [["1.2.5.3", "bar"]]] OIDはドット区切り番号の形で表すほか、国（C）、市区町村（L）、州（ST）、組織（O）、組織内部門（OU）、共通名（CN）といった省略形が使えます。
Challenge	文字列	必須ではありません。事前に配布した秘密鍵。
Keysize	数値	必須ではありません。ビット単位のキー長（1024または2048）。
Key Type	文字列	必須ではありません。当面は常に「RSA」を指定。
Key Usage	数値	必須ではありません。キーの使い方を表すビットマスク。1は署名、4は暗号化、5は署名と暗号化の両方を施すことを表します。Windows CAなど、暗号化と署名のいずれか一方しか同時には施せないものもあります。

SubjectAltName辞書キー

「SCEP」ペイロードには、必要に応じ、CAが証明書を発行する際に必要な値を格納したSubjectAltName辞書を指定できます。各キーに対して、単一の文字列、または文字列の配列を指定します。

指定する値は実際に用いるCAによって異なりますが、多くの場合、DNS名、URL、電子メールなどを指定することになるでしょう。詳しくは、たとえば"構成プロファイルの例"（26 ページ）や『*Over-the-Air Profile Delivery and Configuration*』を参照してください。

GetCACaps辞書キー

GetCACapsキーの値として辞書を追加すると、デバイスはそこに登録された文字列を、CAの能力に関する権威ある情報源として扱います。辞書がなければ、デバイスはCAにGetCACapsの値を問い合わせ、応答として得られた値を用います。CAが応答を返さなければ、デフォルト値として、GET 3DESおよびSHA-1を採用します。詳細については『*Over-the-Air Profile Delivery and Configuration*』を参照してください。

「APN」ペイロード

「APN（Access Point Name）」ペイロードは、PayloadTypeの値としてcom.apple.apn.managedを与えることにより指定します。どのペイロードにも共通の設定項目に加え、このペイロードには次のようなキーが定義されています。

キー	型	値
DefaultsData	辞書	この辞書にはキーと値の組が2つあります。
DefaultsDomainName	文字列	値は「com.apple.managedCarrier」に固定です。
apns	配列	この配列には辞書をいくつでも指定できます。各辞書には、AP設定と、キー/値の組を記述します。
apn	文字列	APN（アクセスポイント名、Access Point Name）を指定します。
username	文字列	このAPNのユーザ名を指定します。指定がなければ、プロファイルのインストール時に尋ねられます。
password	データ	必須ではありません。このAPNのユーザのパスワードを表します。うっかり他人が見てしまうことを避けるため、エンコードを施してあります。指定がなければ、プロファイルのインストール時に入力を求められます。
proxy	文字列	必須ではありません。APNプロキシのIPアドレスまたはURL。
proxyPort	数値	必須ではありません。APNプロキシのポート番号。

「Exchange」ペイロード

「Exchange」ペイロードは、PayloadTypeの値としてcom.apple.eas.accountを与えることにより指定します。Microsoft Exchangeのアカウントをデバイス上に作成する働きがあります。どのペイロードにも共通の設定項目に加え、このペイロードには次のようなキーが定義されています。

キー	型	値
EmailAddress	文字列	アカウントの完全電子メールアドレスを指定します。ペイロードに指定がなければ、プロファイルのインストール時に尋ねられます。
Host	文字列	Exchangeサーバのホスト名（またはIPアドレス）を指定します。

キー	型	値
SSL	ブール型	必須ではありません。デフォルト値はYes。Exchangeサーバが認証用にSSLを利用するか否かを指定します。
UserName	文字列	このExchangeアカウントのユーザ名を指定します。指定がなければ、プロファイルのインストール時に尋ねられます。
Password	文字列	必須ではありません。アカウントのパスワード。これが指定されている場合、プロファイルに暗号化を施す必要があります。
Certificate	NSData blob	必須ではありません。証明書を使って認証するアカウントの場合に、NSData blob形式の.p12識別証明書。
CertificateName	文字列	必須ではありません。証明書の名前または説明。
CertificatePassword	データ	必須ではありません。p12識別証明書に必要なパスワード。これが指定されている場合、プロファイルに暗号化を施す必要があります。
PreventMove	ブール型	必須ではありません。デフォルト値は`false`。 `true`ならば、この電子メールアカウントから別のアカウントにメッセージを移動することはできません。また、メッセージの送信元アカウント以外から、転送や返信をすることも禁じます。 **設定可能なバージョン：**iOS 5.0以降。
PreventAppSheet	ブール型	必須ではありません。デフォルト値は`false`。`true`ならば、このアカウントから他社製アプリケーションでメールを送信することはできません。 **設定可能なバージョン：**iOS 5.0以降。
PayloadCertificate-UUID	文字列	識別資格情報に用いる証明書ペイロードのUUID。このフィールドがあれば、`Certificate`フィールドは使いません。 **設定可能なバージョン：**iOS 5.0以降。
SMIMEEnabled	ブール型	必須ではありません。デフォルト値は`false`。`true`ならば、このアカウントはS/MIMEに対応しています。 **設定可能なバージョン：**iOS 5.0以降。

キー	型	値
SMIMESigning-CertificateUUID	文字列	必須ではありません。このアカウントから送信するメッセージに署名するために用いる、識別証明書のPayloadUUID。 **設定可能なバージョン：**iOS 5.0以降。
SMIMEEncryption-CertificateUUID	文字列	必須ではありません。このアカウントで受信したメッセージの復号に用いる、識別証明書のPayloadUUID。 **設定可能なバージョン：**iOS 5.0以降。

注意 注：VPNやWi-Fiの設定と同様、SCEP資格情報もPayloadCertificateUUIDキーを使ってExchangeの設定と関連付けることができます。

「VPN」ペイロード

「VPN」ペイロードは、PayloadTypeの値としてcom.apple.vpn.managedを与えることにより指定します。どのペイロードにも共通の設定項目に加え、このペイロードには次のようなキーが定義されています。

キー	型	値
UserDefinedName	文字列	VPN接続の説明で、これがデバイスに表示されます。
OverridePrimary	ブール型	トラフィックをすべてVPNインターフェイス経由で伝送するか否かを指定します。trueならば、ネットワークトラフィックはすべてVPN経由で送信されます。
VPNType	文字列	このペイロードの設定を、どの種類のVPN接続に適用するか、を表します。指定できる値は「L2TP」、「PPTP」、「IPSec」のいずれかで、それぞれL2TP、PPTP、Cisco IPSecを表します。

VPN接続の種類が「PPP」または「IPSec」の場合、構成プロファイルの最上位レベルに辞書があります。VPNTypeの値に応じ、それぞれの辞書に設定できるキーを以下に示します。

「PPP」の場合の辞書キー

PPP型のVPNペイロードに設定できる要素を示します。

キー	型	値
AuthName	文字列	VPNアカウントのユーザ名。L2TPまたはPPTPの場合に使用します。
AuthPassword	文字列	必須ではありません。TokenCardがfalseの場合にのみ可視になります。L2TPまたはPPTPの場合に使用します。
TokenCard	ブール型	RSA SecurIDのようなトークンカードを接続に用いるか否かを指定します。L2TPの場合に使用します。
CommRemoteAddress	文字列	VPNサーバのIPアドレスまたはホスト名。L2TPまたはPPTPの場合に使用します。
AuthEAPPlugins	配列	RSA SecurIDを使用する場合にのみ存在するキーで、配列の要素は1つだけであり、その値は「EAP-RSA」でなければなりません。L2TPまたはPPTPの場合に使用します。
AuthProtocol	配列	RSA SecurIDを使用する場合にのみ存在するキーで、配列の要素は1つだけであり、その値は「EAP」でなければなりません。L2TPまたはPPTPの場合に使用します。
CCPMPPE40Enabled	ブール型	CCPEnabledに関する説明を参照してください。PPTPの場合に使用します。
CCPMPPE128Enabled	ブール型	CCPEnabledに関する説明を参照してください。PPTPの場合に使用します。
CCPEnabled	ブール型	接続の暗号化を有効にします。このキーおよびCCPMPPE40Enabledがtrueであれば、暗号化レベルは「自動」になります。このキーおよびCCPMPPE128Enabledがtrueであれば、暗号化レベルが最大であることを表します。暗号化を施さない場合は、CCP関係のキーをいずれもfalseとします。PPTPの場合に使用します。

「IPSec」の場合の辞書キー

IPSec型のVPNペイロードに設定できる要素を示します。

キー	型	値
RemoteAddress	文字列	VPNサーバのIPアドレスまたはホスト名。Cisco IPSecの場合に使用します。
AuthenticationMethod	文字列	「SharedSecret」または「Certificate」。L2TPまたはCisco IPSecの場合に使用します。

キー	型	値
XAuthName	文字列	VPNアカウントのユーザ名。Cisco IPSecの場合に使用します。
XAuthEnabled	整数	XAUTHがONならば1、OFFならば0。Cisco IPSecの場合に使用します。
LocalIdentifier	文字列	AuthenticationMethodがSharedSecretの場合にのみ存在。使用するグループの名前。ハイブリッド認証を用いる場合、この文字列の末尾を「[hybrid]」としなければなりません。Cisco IPSecの場合に使用します。
LocalIdentifierType	文字列	AuthenticationMethodがSharedSecretの場合にのみ存在。値は「KeyID」。L2TPまたはCisco IPSecの場合に使用します。
SharedSecret	データ	このVPNアカウントの共有暗号鍵。AuthenticationMethodがSharedSecretの場合にのみ存在。L2TPまたはCisco IPSecの場合に使用します。
PayloadCertificate-UUID	文字列	アカウント資格情報に用いる証明書のUUID。AuthenticationMethodがCertificateの場合にのみ存在。Cisco IPSecの場合に使用します。
PromptForVPNPIN	ブール型	接続の際にPINを問い合わせるか否か。Cisco IPSecの場合に使用します。

「Wi-Fi」ペイロード

「Wi-Fi」ペイロードは、PayloadTypeの値としてcom.apple.wifi.managedを与えることにより指定します。PayloadVersionの値は0とします。

どのペイロードにも共通の設定項目に加え、このペイロードには次のようなキーが定義されています。

キー	型	値
SSID_STR	文字列	利用するWi-FiネットワークのSSID。
HIDDEN_NETWORK	ブール型	デバイスはSSID以外にも、ブロードキャストの種類、暗号化の種類などの情報を使ってネットワークを識別します。デフォルト値（false）のままであれば、ネットワークはすべてオープンまたはブロードキャストであると仮定します。隠れたネットワークを指定する場合はtrueでなければなりません。

キー	型	値
AutoJoin	ブール型	必須ではありません。デフォルト値はtrue。trueならば、ネットワークには自動的に参加するようになります。falseならば、参加するためにはネットワーク名をタップしなければなりません。 **設定可能なバージョン：**iOS 5.0以降。
EncryptionType	文字列	WEP、WPA、Any、Noneのいずれかを指定します。WPAはWPAとWPA2に対応し、両方の暗号化を施します。 ネットワークアクセスポイントの能力と、この設定が合致していなければなりません。暗号化の種類が不明である、あるいはどの種類の暗号化でも適用したい場合は、Anyを指定してください。 **設定可能なバージョン：**iOS 4.0以降。ただしNoneを指定できるのはiOS 5.0以降です。
Password	文字列	必須ではありません。パスワードがなくても、ネットワークを既知のネットワークリストに追加するだけならば可能です。当該ネットワークに接続する際にパスワード入力を求められます。
ProxyType	文字列	必須ではありません。None、Manual、Autoのいずれかを指定します。 **設定可能なバージョン：**iOS 5.0以降。

ProxyTypeをManualとした場合、次のフィールドも設定する必要があります。

キー	型	値
ProxyServer	文字列	プロキシサーバのネットワークアドレス。
ProxyServerPort	整数	プロキシサーバのポート。
ProxyUsername	文字列	必須ではありません。プロキシサーバの認証に用いるユーザ名。
ProxyPassword	文字列	必須ではありません。プロキシサーバの認証に用いるパスワード。

ProxyTypeをAutoとした場合、次のフィールドも設定する必要があります。

キー	型	値
ProxyPACURL	文字列	プロキシ設定を定義しているPACファイルのURL。

802.1Xエンタープライズネットワークの場合、EAPClientConfiguration辞書が必要です。

EAPClientConfiguration辞書

標準的な暗号化以外にも、エンタープライズネットワーク独自のプロファイルを、「EAPClientConfiguration」キーで指定できます。このキーが存在する場合、その値は辞書であり、次のようなキーの値を設定できます。

キー	型	値
UserName	文字列	必須ではありません。正確なユーザ名を知っている場合を除き、設定をインポートしたとき、このプロパティが現れることはありません。認証の際にこの情報を入力しても構いません。
AcceptEAPTypes	整数の配列	EAP（Extensible Authentication Protocol、拡張認証プロトコル）の型として次のいずれかの値を指定します。 13 = TLS 17 = LEAP 21 = TTLS 25 = PEAP 43 = EAP-FAST
PayloadCertificate-AnchorUUID	文字列の配列	必須ではありません。この認証で用いる、信頼できる証明書を識別する文字列です。各要素には証明書ペイロードのUUIDを設定しなければなりません。このキーを設定しておけば、証明書が信頼できるものかどうか、ユーザに問い合わせることはありません。 このプロパティを指定すれば、動的信頼（証明書ダイアログ）は無効になります。ただしTLSAllowTrustExceptionsの値がtrueである場合を除きます。

キー	型	値
TLSTrustedServer-Names	文字列の配列	必須ではありません。信頼できるものとして受理してよいサーバ証明書の共通名のリスト。「wpa.*.example.com」のようにワイルドカードを使って指定することも可能です。逆に、サーバが提示した証明書がこのリストに載っていない場合、これは信頼できません。 単独で用いるか、またはTLSTrustedCertificatesと組み合わせて使うことにより、ネットワークごとに、信頼できるものと見なす証明書をきめ細かく設定し、動的信頼証明書は使わずに済ますことができます。 このプロパティを指定すれば、動的信頼（証明書ダイアログ）は無効になります。ただしTLSAllowTrustExceptionsの値がtrueである場合を除きます。
TLSAllowTrust-Exceptions	ブール型	必須ではありません。ユーザによる動的な信頼性確認を許可/禁止します。動的な信頼性確認とは、証明書が信頼できない場合に、証明書ダイアログを表示して確認を求めることです。falseであれば、すでに信頼できないと分かっている証明書は、直ちに認証に失敗します。上記のPayloadCertificateAnchorUUIDおよびTLSTrustedNamesを参照してください。 このプロパティのデフォルト値はtrueです。ただし、PayloadCertificateAnchorUUIDまたはTLSTrustedServerNamesが設定されている場合はfalseになります。
TTLSInner-Authentication	文字列	必須ではありません。TTLSモジュールが用いる内部認証です。デフォルト値は「MSCHAPv2」です。 「PAP」、「CHAP」、「MSCHAP」、「MSCHAPv2」のいずれかを指定できます。
OuterIdentity	String	必須ではありません。このキーはTTLS、PEAP、EAP-FASTにのみ関係します。 ユーザの身許を隠すことを許可します。ユーザの実名が現れるのは、暗号化されたトンネル内に限ります。たとえば「anonymous」、「anon」、「anon@mycompany.net」などを設定できます。 攻撃者が認証ユーザ名を容易に知ることができないので、セキュリティ向上に役立ちます。

EAP-Fastの支援機能

EAP-FASTモジュールはEAPClientConfiguration辞書に格納された次のプロパティを参照します。

キー	型	値
EAPFASTUsePAC	ブール型	必須ではありません。
EAPFASTProvisionPAC	ブール型	必須ではありません。
EAPFASTProvisionPACAnonymously	ブール型	必須ではありません。

以上のキーはその性質上、階層構造を成しています。EAPFASTUsePACがfalseであれば、他の2つのプロパティは無視されます。同様に、EAPFASTProvisionPACがfalseであれば、EAPFASTProvisionPACAnonymouslyは無視されます。

EAPFASTUsePACがfalseであれば、認証処理はPEAPやTTLSと同じようになります。すなわち、サーバはその都度、証明書を使って身許を証明します。

EAPFASTUsePACがtrueならば、PACがある場合それを使うようになります。現状では、デバイス上のPACを取得するためには、PACプロビジョニングを許可するしか方法がありません。したがって、EAPFASTProvisionPACを有効にし、さらに必要ならばEAPFASTProvisionPACAnonymouslyも有効にする必要があります。EAPFASTProvisionPACAnonymouslyにはセキュリティ上の弱点があります。サーバを認証できないので、中間者攻撃には脆弱なのです。

証明書

VPNの設定と同様、証明書の識別情報設定を、Wi-Fi設定と関連付けることができます。これはセキュアエンタープライズネットワーク用の資格情報を定義する際に有用です。識別情報を関連付けるためには、PayloadCertificateUUIDキーの値としてペイロードUUIDを指定してください。

キー	型	値
PayloadCertificateUUID	文字列	識別資格情報に用いる証明書ペイロードのUUID。

構成プロファイルの例

「SCEP」ペイロードが含まれる構成プロファイルの例を以下に示します。

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple Inc//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
    <dict>
```

```
        <key>PayloadVersion</key>
        <integer>1</integer>
        <key>PayloadUUID</key>
        <string>Ignored</string>
        <key>PayloadType</key>
        <string>Configuration</string>
        <key>PayloadIdentifier</key>
        <string>Ignored</string>
        <key>PayloadContent</key>
        <array>
            <dict>
                <key>PayloadContent</key>
                <dict>
                    <key>URL</key>
                    <string>https://scep.example.com/scep</string>
                    <key>Name</key>
                    <string>EnrollmentCAInstance</string>
                    <key>Subject</key>
                    <array>
                        <array>
                            <array>
                                <string>O</string>
                                <string>Example, Inc.</string>
                            </array>
                        </array>
                        <array>
                            <array>
                                <string>CN</string>
                                <string>User Device Cert</string>
                            </array>
                        </array>
                    </array>
                    <key>Challenge</key>
                    <string>...</string>
                    <key>Keysize</key>
```

```
                    <integer>1024</integer>
                    <key>Key Type</key>
                    <string>RSA</string>
                    <key>Key Usage</key>
                    <integer>5</integer>
                </dict>
                <key>PayloadDescription</key>
                <string>Provides device encryption identity</string>
                <key>PayloadUUID</key>
                <string>fd8a6b9e-0fed-406f-9571-8ec98722b713</string>
                <key>PayloadType</key>
                <string>com.apple.security.scep</string>
                <key>PayloadDisplayName</key>
                <string>Encryption Identity</string>
                <key>PayloadVersion</key>
                <integer>1</integer>
                <key>PayloadOrganization</key>
                <string>Example, Inc.</string>
                <key>PayloadIdentifier</key>
                <string>com.example.profileservice.scep</string>
            </dict>
        </array>
    </dict>
</plist>
```

書類の改訂履歴

この表は「*iOS構成プロファイルリファレンス*」の改訂履歴です。

日付	メモ
2011-10-17	本題とは無関係のiCloudキーを削除しました。
2011-10-12	iOS 5.0用に更新しました。
2011-03-08	ドキュメント名を変更しました。
2010-09-21	誤字を訂正しました。
2010-08-03	iOS構成プロファイルに用いられるプロパティリストのキーについて説明した新規ドキュメント。

Apple Inc.
1 Infinite Loop
Cupertino, CA 95014
U.S.A.

アップルジャパン株式会社
〒163-1450 東京都新宿区西新宿
3 丁目20 番2 号
東京オペラシティタワー
http://www.apple.com/jp/