特集論文

スマートデバイス向け証明書発行サービス

小俣三郎*
田口拓也*
向江勇気*

Certificate Issuing Service for Smart Device

Saburo Omata, Takuya Taguchi, Yuki Mukae

要　旨

近年，iPhone／iPad(注1)及びAndroid(注2)を搭載したスマートデバイスが普及してきている。これらは個人ユーザーの一般利用だけではなく，企業においても重要な情報ツールとなりつつある。一方，スマートデバイス携帯時の盗難・紛失等による個人情報漏洩(ろうえい)やなりすましといったセキュリティ上の観点からも，スマートデバイス自体を認証する端末認証のニーズが高まってくる。

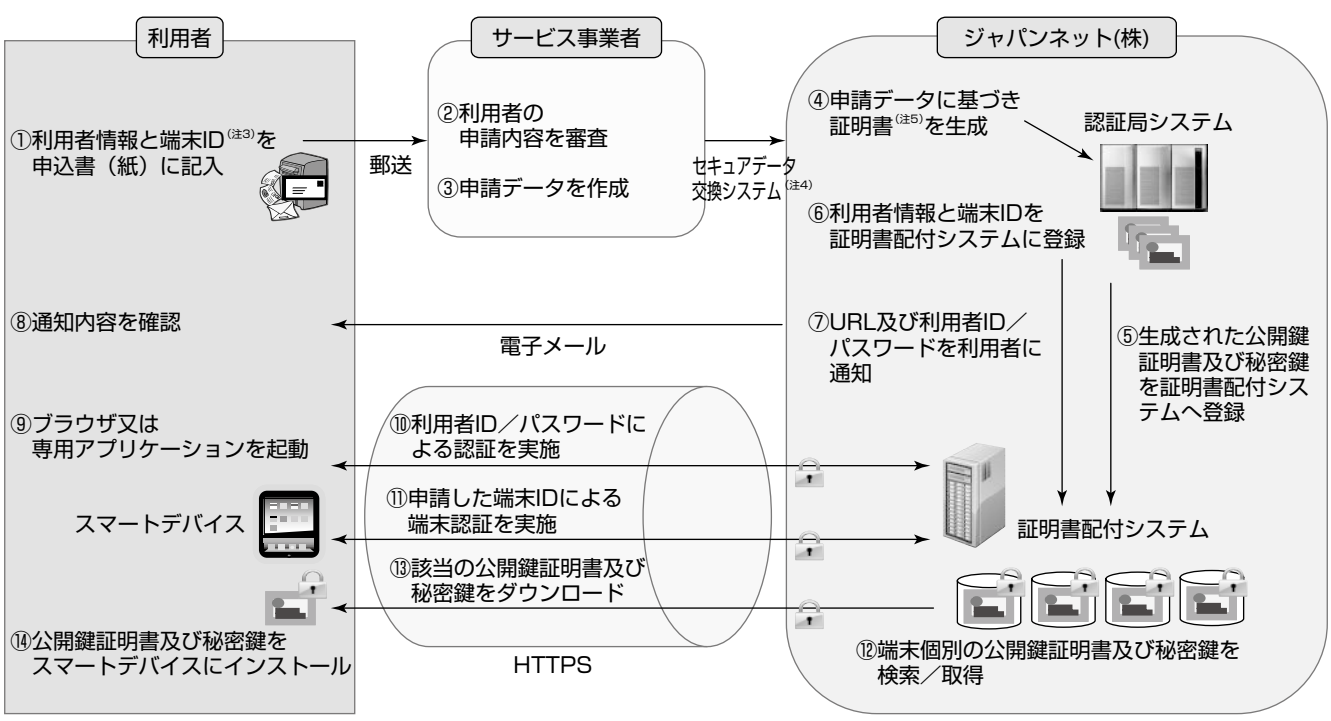
そこで，ジャパンネット㈱では，スマートデバイスに対して安全かつ確実に電子証明書を発行・配付することを目指して，スマートデバイス向け証明書発行サービスの検討を実施した。検討に当たっては，iPhone／iPad及びAndroidの仕様を調査し，方式の統一を図った。

本稿では，スマートデバイス向け証明書発行サービスの実現方法などの技術的特長を述べる。

スマートデバイス向け証明書発行サービスでは，事前にスマートデバイスの端末ID(IDentifier)情報を利用者から申請し，その端末IDに基づいて証明書を発行する。また証明書配付システムでは，なりすまし等を防止するために，①利用者ID／パスワードによる利用者認証，②端末IDによる端末認証という二要素認証を実施するよう，システムを設計した。

今後は，サービスフローの詳細を確定させ，オンデマンドITサービスとして主に企業向けのスマートデバイスに対する証明書発行サービスを提供していく。

（注１）　iPhone，iPadは，Apple Inc. の登録商標である。
（注２）　Androidは，Google，Inc. の登録商標である。



(注3)　端末ID：MACアドレスなどのスマートデバイス固有の端末識別情報またはそれらの組み合わせ
(注4)　セキュアデータ交換システム：データ送受信のためのWebシステム
(注5)　証明書：PKIにおける公開鍵証明書

HTTPS：Hyper Text Transfer Protocol Security
MAC　：Media Access Control
URL　：Uniform Resource Locator

スマートデバイス向け証明書発行サービスの概念図

企業におけるスマートデバイス利用拡大に伴い，スマートデバイスでのPKI（Public Key Infrastructure）利用のための電子証明書を発行するサービスを提供する。スマートデバイスのポータビリティを考慮し，盗難・紛失等による個人情報漏洩やなりすましのリスクを低減するため，利用者認証及び端末認証による二要素認証を導入した上で電子証明書を配付する。

*三菱電機情報ネットワーク㈱

1. まえがき

ポータビリティ，操作性の高さ，機能の豊富さから，近年多くの企業がiPhone／iPadやAndroid端末といったスマートデバイスに注目している。スマートデバイスを用いることで業務の効率化を期待できる一方で，個人情報漏洩やなりすまし等のセキュリティ上の問題も顕在化するおそれがある。そこで注目されているのが，PKIを利用した端末認証である。

三菱電機グループのジャパンネット㈱は，官公庁・自治体が実施している電子入札や電子申請への参加者（一般企業や団体 等）を電子的に特定するために使用する電子証明書の発行サービス事業を行っている。また，医療や金融，一般ビジネス分野における認証や署名用途で使用する各種の電子証明書の発行サービスを行っている。現在発行している電子証明書は人物を特定するための証明書であるが，最近のスマートデバイスは様々な場面で利用されるケースが増えており，今後は利用する端末を特定するための端末認証用証明書の必要性が高まってくる。

本稿では，スマートデバイス向け証明書発行サービスに関する実現方法などの技術的特長について述べる。

2. 証明書の利用法及び検討方針

2.1 証明書の利用法

端末認証用証明書の利用法として，パソコンでは一般的に広く利用されているHTTPS（SSLクライアント認証），及びVPN（SSL-VPN(注6)及びIPSec(注7)）での利用を想定している。これらの機能はiPhone／iPadでも標準機能として搭載されており，例えばHTTPSによってSSLクライアント認証を必要とするサービスに接続して情報を取得することや，SSL-VPNで外出先から社内ネットワークに接続し，Webメール，グループウェア，スケジュール管理等のWebアプリケーションにアクセスすることで社外から安全に業務を行うことが可能になる。

2.2 実現方法などの検討方針

iPhone／iPadでもAndroid端末でもL2TP(注8)，PPTP(注9)，IPSecをサポートしている。ただしAndroid端末では標準機能でSSLクライアント認証ができないことや，独自の認証局を信頼点として設定するために複雑な操作を必要とするという課題がある。

（注6） Secure Sockets Layer-Virtual Private Networkの略。SSLを利用したVPNの一種。
（注7） Security Architecture for Internet Protocolの略。IPパケット単位で改ざん防止や秘匿機能をもったプロトコル。
（注8） Layer 2 Tunneling Protocolの略。VPNのためのトンネリングプロトコル。
（注9） Point to Point Tunneling Protocolの略。Point to Point Protocolを拡張したトンネリングプロトコル。

このような証明書の利用法及び課題を踏まえながら次の方針で検討する。

①ユーザーの利便性を損なわない
②スマートデバイスの種類に依存しない

3. スマートデバイス向け証明書

3.1 端末IDの確認方法

このサービスの利用者は，証明書の発行申込みを行う際に，まず発行対象となるスマートデバイスが固有に持っている端末IDを確認して申請する必要がある。端末IDを確認する方法に関しては，iPhone／iPadの場合，設定画面またはiTunes(注10)の画面に**表1**に示すような端末IDが表示される。Android端末の場合，設定画面または機種によって表示可否の差はあるが，専用アプリケーションを実行することによって端末IDを表示できる。

（注10） iTunesは，Apple Inc. の登録商標である。

3.2 端末IDの種類と証明書格納情報

今回検討した証明書発行サービスでは，iPhone／iPadまたはAndroid端末自体に対して電子証明書を発行するが，電子証明書のSubjectというエリアに個々のスマートデバイスの端末ID情報を格納することとしている（**表2**）。ただし，利用者が複数サービスで同じ証明書を利用するケースでは，証明書内に端末IDを格納することで第三者が証明書に格納された端末固有情報を収集，分析することができる場合もあり，結果として端末固有情報を追跡される可能性もある。そのため端末IDを格納するか否か，及び格納する場合でもどの端末IDを格納するか，についてはサービス事業者または利用者によって選択可能としている。また，スマートデバイスの利用年数に応じて，証明書の有効期間も1，2，3，5年から選択可能とし，**表1**に示すIDを証明書のSubjectエリアに格納する。

表1．端末ごとの端末ID及び表示方法／取得方法

端末のOS	取得可能な端末ID	端末での表示方法／取得方法
iOS（iPhone／iPad）	UDID（Unique Device Identifier）	iTunesで表示可能
	IMEI（International Mobile Equipment Identity）	設定画面またはiTunesで表示可能
	ICCID（Integrated Circuit Card ID）	設定画面またはiTunesで表示可能
	MACアドレス	設定画面またはiTunesで表示可能
Android（Galaxy Sの例）	IMEI（or MEID）	OSによって提供される機能で取得可能（android.telephony.TelephonyManagerクラスのgetDeviceId()メソッド）
	MACアドレス	設定画面で表示可能
	IMSI（International Mobile Subscriber Identity）	OSによって提供される機能で取得可能（android.telephony.TelephonyManagerクラスのgetSubscriberId()メソッド）

4. 証明書配付システム

この章では，証明書配付システムの認証方式及び配付方式について述べる。証明書配付システムでは**図1**のように利用者からの申込みに応じて証明書を生成し，配付システムに登録後，利用者認証及び端末認証を経て証明書を配付する。

4.1 利用者及び端末の認証方式

この証明書発行サービスは，次の手順にしたがってスマートデバイス向け証明書を生成する。

⑴ 認証局システムで鍵ペア(秘密鍵と公開鍵)を生成する。

⑵ 生成した公開鍵に対して利用者からの申込み内容に沿って証明書を生成する。

⑶ 証明書と秘密鍵を合わせてPKCS#12(注11)データとしてスマートデバイスに配付する。

手順⑴においては，鍵ペアを認証局が生成する方法と，スマートデバイスが生成する方法が考えられるが，今回は次の理由によって，認証局システムで鍵ペアを生成することにした。①ハードウェア性能などによって，乱数(または乱数の種)として物理乱数など安全性の高い乱数を使用することが可能で，鍵ペアの品質を安定できること，②鍵紛失時に鍵を復元可能とするためのキーアーカイブが可能であること，③スマートデバイス側での利用者によるCSR(Certificate Signing Request)の生成操作が不要。

手順⑶において，PKCS#12データをスマートデバイスへ配付する際は，利用者のなりすまし，及びスマートデバイスのなりすましを防止する必要があるため，利用者ID／パスワードによる利用者の認証，及びスマートデバイスを個別に識別・特定することによる端末認証をともに実施することとしている。

iPhone／iPadのOSであるiOSでは，多数のデバイスの構成情報を一括で設定するために，構成プロファイルと呼ばれるXML(eXtensible Markup Language)(注12)ファイルを使った設定方式[1][2][3]がOSの標準機能として搭載されている。

この機能の一つとして，サーバがスマートデバイスの各種端末ID情報(UDID，IMEI，ICCID，MACアドレス等)を取得する機能がある。この機能によってサーバが認証する必要のある端末IDを細かく指定して要求することができ，またはサービスの種類に応じてサーバが必要とする端末IDのみを認証するといった認証方式が可能である。

一方Androidでは，iOSのようなサーバによる構成プロファイルを利用した端末IDの取得機能はないが，android.telephony.TelephonyManagerクラスから端末IDを取得[4]してサーバに送信するアプリケーションを事前に作成してインストールすることによって，サーバ側ではiPhone／iPadかAndroid端末かを区別する必要なく同じプロトコルで認証及び証明書配付を実施できるようにした。

(注11) Public-Key Cryptography Standard #12の略。RSAセキュリティ社考案の秘密鍵及び証明書を保管するフォーマットの定義。

(注12) 文書やデータの意味や構造を記述するためのマークアップ言語の一つ。

表2．スマートデバイス向け証明書のプロファイル例

領域名		規定内容と設定値
基本部		
version		2(v3)
serialNumber		1001(例)
signature		sha1WithRSAEncryption(ハッシュ，暗号アルゴリズム)
validity		
	notBefore	有効期間(1 or 2 or 3 or 5年)
	notAfter	
issuer		c＝JP（国名）
		o＝Enterprise Premium Service(JNのサービス名称)
		cn＝EnterPrise Premium CA(JNの認証局システム名)
subject		c＝JP
		o＝ABC Corporation(会社名英語(オプション))
		ou＝XYZ Department（部署名英語(オプション))
		ou＝xxxxxxxx(所属又は固有番号等英語(オプション))
		cn＝xxxxxxxx(デバイス識別子英語)
subjectPublicKeyInfo		証明書所有者の公開鍵情報
	algorithm	rsaEncryption(暗号アルゴリズム)
	subjectPublicKey	RSA公開鍵値(1,024bit or 2,048bit)

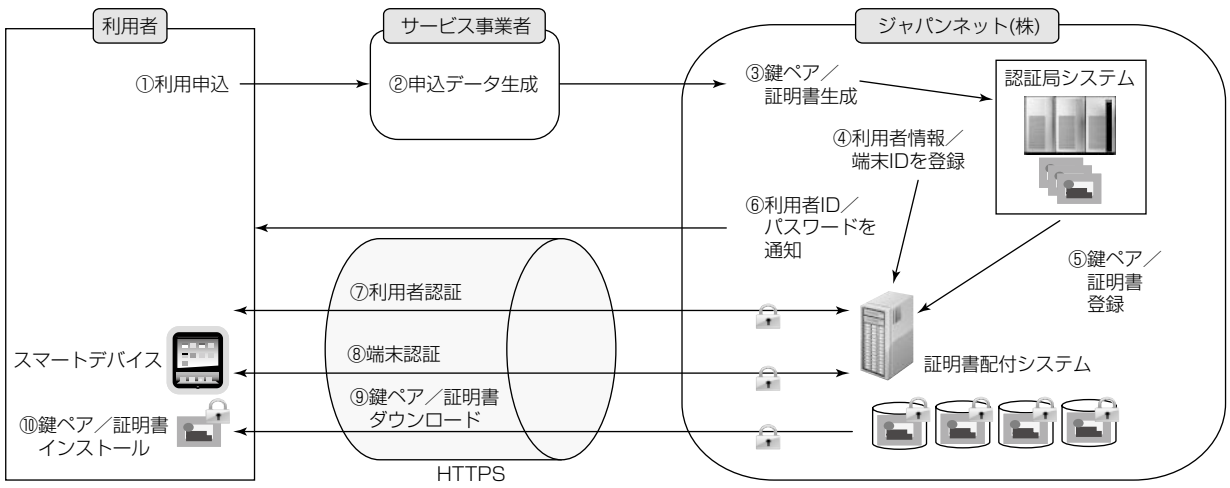


図1．証明書配付システム

4.2 証明書の配付方式

iPhone／iPadでは，無線経由のプロファイル配信とプロファイルによるデバイスの一括設定が可能であり，①認証フェーズ，②証明書の登録フェーズ，③デバイスの構成フェーズという3つのフェーズで構成されるプロトコルを標準でサポートしている。このうち②の証明書の登録フェーズでは，iPhone／iPad側で証明書申請のためのCSRを作成して認証局に送信することで証明書の発行を行うようになっている。

ジャパンネット㈱では，先に述べたとおり認証局で鍵ペアを生成する方式を採用しているため，iPhone／iPadにおける無線経由のプロファイル配信とデバイスの構成のプロトコルをそのまま適用することはせず，①の認証フェーズのうち，サーバがiPhone／iPadの端末IDを取得する機能，及び②の証明書の登録フェーズのスキームを組み合わせることによって，**図2**のような独自の証明書配付方式を採用することにしている。

iPhone／iPadでは，先に述べた構成プロファイルを使って証明書を端末に配付することが可能であるが，Android端末には標準でこのような機能はない。ただし，AndroidはOSとしてPKIの機能自体は持っており[5]，アプリケーションとしては実装可能である。

そこで，ユーザーインタフェースや認証，証明書配付のプロトコルを統一するため，Android端末用のアプリケーションを開発し，擬似的にiOSと同様にXMLを処理することによって，XMLデータとして送られてきたPKCS#12データを端末にインストールさせることにした。

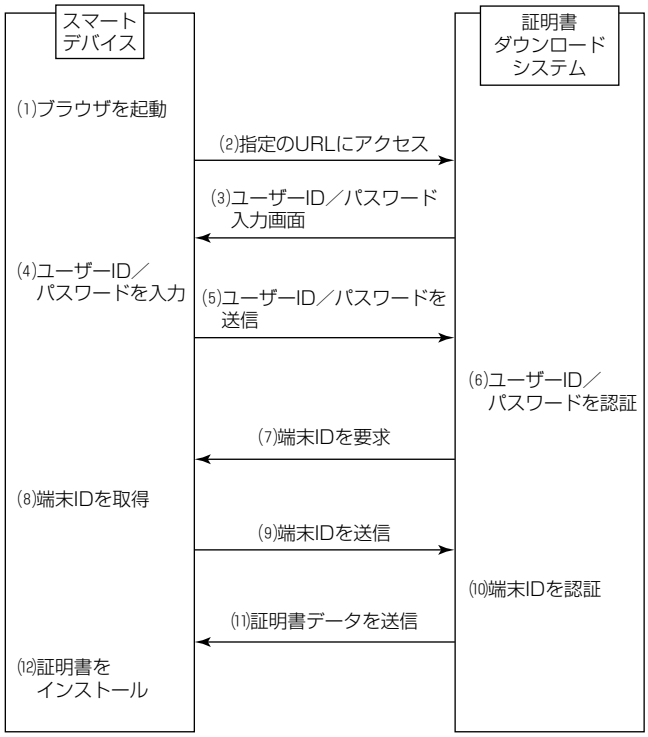


図2．iPhone／iPadの認証方式及び証明書配付方式

5. むすび

iPhone／iPad及びAndroid端末のようなスマートデバイス用OSの機能やユーザーインタフェースなどの特徴を考慮した上で，利用者の利便性を重視した端末認証用証明書の発行サービスの検討内容を述べた。この検討内容は，①証明書配付時に利用者認証及び端末認証の二要素認証を実施し，②iPhone／iPadまたはAndroid端末のOSの種類によらず，同じプロトコル，同じユーザーインタフェースで証明書のインストールが実施できることを特長としており，また，配付可能期間などの運用上必要なパラメータを他社と比較して細かく設定できるようにするなどの工夫をした。今後は，この検討結果を踏まえてシステムの構築及びサービスの提供を行う。

iPhone／iPad及びAndroid端末のようなスマートデバイスが今後，医療，金融，一般ビジネス分野の場において広く普及していくと考えている。また同時に，そのスマートデバイスのポータビリティ性ゆえに，セキュリティがより重要になってくると想定しており，デバイスを認証するための電子証明書のニーズも一層高まってくると考えている。

例えば，医療分野ではスマートデバイスの利用による医療の高機能化が期待されており，在宅医療，在宅介護，訪問薬剤師，電子カルテ，救急病院間の情報共有システムへの適用，又は医師による遠隔診断や治療補助，看護師による急病患者のトリアージ（重症度と緊急性によって傷病者を分別し，治療の優先度を決定すること）等，高い注目を集めている。

今まで人物を認証するための様々な電子証明書を発行してきているが，これまで培ってきた認証局ノウハウを最大限に活（い）かしながら，端末認証用の電子証明書発行に取り組むことによって，電子証明書発行サービス事業の据野を拡大するとともに，安心・安全な社会を下支えすることを目指していきたい。

参考文献

⑴ Apple Inc.，無線経由のプロファイル配信と構成（2010）
⑵ Apple Inc.，iPhone OSテクノロジーの概要（2009）
⑶ Apple Inc.，iPhone OS エンタープライズ配備ガイド，第2版（2010）
⑷ public class Telephony Manager, http://developer.android.com/reference/android/telephony/TelephonyManager.html
⑸ package java. security, http://developer.android.com/reference/java/security/package-summary.html