公的個人認証サービスの技術

PKI相互運用技術 WGリーダ
セコム株式会社 IS研究所
松本　泰

2004年1月29日、地方公共団体が市民に電子証明書を配布する公的個人認証サービスが開始されました。公的個人認証サービスは、いくらか物議をかもしている住民基本台帳ネットワークの情報を元にしていることに対する不安の声や、民業を圧迫する官製認証サービスという批判の声もあるようです。しかし、現状では、公的個人認証サービスに関する技術情報は少なくその技術や背景を的確に理解している人も少ないと思われます。こうした事が、よく知られていない、そして分からないものに対する不安を掻き立てている面も否めないのではないでしょうか。私自身は、公的個人認証サービスの課題は多々あると感じていますが、まずは、多くの人々が、その背景などを正確に把握することが重要だと考えています。

本稿では、現在、公表されている資料や実際の証明書などの情報から、公的個人認証サービスの技術面の説明を行いますが、紙面の都合から信頼モデルを中心について説明するとともに今後の課題について考察します。

1.「公的個人認証サービス」の開始

これまで、中央政府の官職に証明書を発行する政府認証基盤GPKI、地方公共団体の職員に証明書を発行する地方公共団体組織認証基盤LGPKI、そして、民間の認証局が整備されてきました。そして、これらの認証局の証明書ユーザ間で、B2G（民間と政府間）、B2LG（民間と地方公共団体間）における電子申請、電子入札などで利用が始まっています。しかし、こうした認証基盤は業務上必要な人々が利用するだけで一般の市民には無縁な存在でした。公的個人認証サービスの開始で、C2G（市民と政府間）、C2LG（市民と地方自治体間）で認証基盤が利用可能な状況になりつつあります。公的個人認証サービスと、既に運用を開始しているGPKI、LGPKI、そして民間認証局などが揃い、これによってようやく日本の行政系の認証基盤の基本的な整備が出来たことになるかと思います。特に公的個人認証サービスは、広く市民が利用できるということから、これからのIT社会、電子社会への移行において、重要な役割を果たすと考えられます。

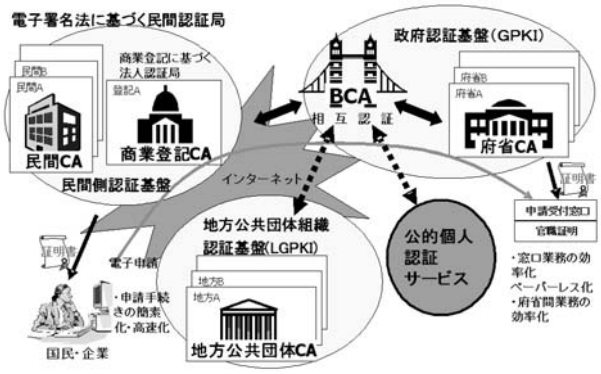

図1

2. 公的個人認証サービスの認証局

公的個人認証サービス（JPKI）の認証局（CA）は、市民に証明書を配布する都道府県CAと、各都道府県CAにCA証明書を発行するJPKIブリッジCAから構成されます。

都道府県CAは、市民に向けて公的個人認証サービスの証明書を発行します。都道府県CAは、各都道府県毎にひとつずつCAが存在します。例えば、三鷹市民であれば、東京都CAが証明書を発行します。この都道府県CAは、自己署名証明書を持った単独で運営が可能な独立したCAとなっています。また、都道府県CAは、JPKIブリッジCAへCA証明書を発行しています。この意味は後で説明します。

次にJPKIのブリッジCAがあります。JPKIのブリッジCAは、各都道府県CAにCA証明書を発行して

いる他、他のドメイン、すなわち、GPKIのブリッジCAへCA証明書（相互認証証明書）を発行しています。この相互認証証明書も後で説明します。通常ブリッジCAは、ユーザの信頼点にはならない、すなわちいわゆるroot CAにはなりません。それに対して、JPKIのブリッジCA はJPKIのWebアプリケーションの信頼点となっているようでありJPKIのWebサーバへSSL証明書を発行しています。

以下に認証局（CA）と証明書の関係を示します。

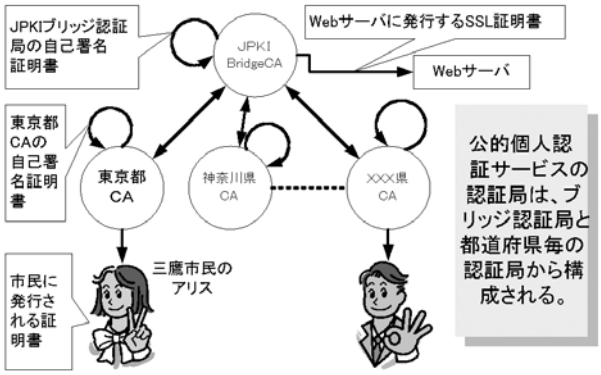

図2

3. 公的個人認証サービスと住基カード

公的個人認証サービス（JPKI）の「証明書と鍵」は、住基カードのJPKI領域に格納されます。JPKIの「証明書と鍵」の格納先は、住基カード以外でもかまわないとされていますが、現時点では、住基カード以外の選択肢はまだないようです。

住基カードのJPKI領域は、住基カード上のひとつのアプリケーションとして領域が確保され、その領域のためのパスワードで保護されます。ちなみに、住基カードを最初に取得した時にもパスワードを設定しますが、これは、住民基本台帳コード（住基コード）を住基カードに格納するためのアプリケーションのパスワードということになります。

住基カードのJPKI領域には、この住基カードホルダーの証明書（公開鍵証明書）とこの証明書に対応した秘密鍵（Private key）が格納される他、この証明書を発行した都道府県CAの自己署名証明書が格納されます。この領域には住基コード自体は格納されませんが、格納されている証明書には、基本4情報と呼ばれる、氏名、生年月日、性別、住所が含まれています。

住基カードのJPKI領域に格納される秘密鍵は、カード保有者の電子署名に使われる非常に重要な鍵です。この秘密鍵は、市町村のJPKIの発行窓口にある鍵ペア生成装置からローディングされます。そして、一旦ローディンされると、この秘密鍵は一生カード外には決して出ない仕組みとなっています。そのため、電子署名は必ずカード上で行われます。

都道府県CAの自己署名証明書も非常に重要な役割を果たします。この証明書の公開鍵は、住基カードホルダーの信頼点となります。市町村のJPKIの発行窓口が、住基カードホルダの信頼点をセキュアに渡し、住基カード上にセキュアに格納そして保護されるということが重要なポイントになります。

4. 公的個人認証サービスの証明書

JPKIは、市民に証明書を発行するのがその役目となります。しかし、JPKIではその他の色々な証明書を発行しています。以下にJPKIで発行される証明書の種類を示します。紙面の関係上個々の証明書については説明できませんが、ここでは、色々な証明書が発行されていることを覚えておいて下さい。

証明書の種類	発行認証局	内　容
BCA自己署名証明書	JPKI BCA	Webサーバなどの信頼点
相互認証証明書	JPKI BCA	都道府県CAへ発行。JPKIリポジトリに公開される。
相互認証証明書（GPKI）	JPKI BCA	GPKIのBCAへ発行
Webサーバ証明書	JPKI BCA	JPKIドメイン内のWebサーバ
コードサイニング証明書	JPKI BCA	アプレットなどへの証明書
都道府県自己署名証明書	都道府県CA	市民の信頼点。JPKIのICカードに格納される。
相互認証証明書	都道府県CA	JPKI BCAへ発行。JPKIリポジトリに公開される。
OCSPサーバ証明書	都道府県CA	JPKI外から証明書の失効を検証
証明書検証サーバ証明書	都道府県CA	市民が官職の証明書を検証
市民向け証明書	都道府県CA	個人の証明書。JPKIのカードに格納される。

5. 公的個人認証サービスの信頼点と証明書パス

ここで三鷹市民のアリスが登場します。アリスがJPKIの証明書発行を受けると、アリスの住基カードのJPKI領域に証明書と秘密鍵が格納されます。秘密鍵がセキュアに格納されることは、非常に重要なことですが、それとともに、アリスの信頼点がセキュアに渡されることも重要なポイントです。住基カードのJPKI領域に、アリスの信頼点である東京都CAの自己署名証明書が格納されますが、アリスはこの信頼点を手がかりに、JPKIに関連した信頼関係を検証することになります。

アリスが電子申請を行なったとします。アリスとA省大臣は、異なった認証主体、すなわち、別の認証ドメイン（別のポリシのドメイン）に所属しています。このような場合、JPKIとGPKIブリッジ認証CAが相互認証することにより、異なるドメインでの検証が可能になります。PKIにおいて相互認証とは、異なるドメインへCA証明書を発行することを意味します。異なるドメインへ発行するCA証明書の意味は後で説明します。

ここでは、アリスがA省大臣の署名を検証する場面を説明します。図3は、アリスの信頼点からA省大臣までの証明書パスなるものを示しています。アリスの信頼点は住基カードにセキュアに保管されています。アリスの信頼点である東京都CAの公開鍵は、アリスに発行された公開鍵証明書や秘密鍵と共に住基カードのJPKI領域に格納されています。アリスは、最初にこの信頼点の公開鍵のみを信頼します。この公開鍵を使って、東京都CAからJPKIブリッジCAへ発行している証明書の検証を行います。この検証が成功するとJPKIブリッジCAの公開鍵を信頼することができます。このJPKIブリッジCAの公開鍵を信頼することができると、JPKIブリッジCAからGPKIブリッジCAへ発行したCA証明書（相互認証証明書）の検証ができます。このようなことを続けていくとA省大臣に発行された証明書の検証ができます。この一連の作業は、証明書パス検証と呼ばれています。証明書パス検証が成功しA省大臣の公開鍵証明書が信頼できるとなると、その証明書に格納された公開鍵からA省大臣の署名文書の検証が可能になります。こうした検証は、アリスの住基カードのJPKI領域にセキュアに保護された公開鍵（東京都CAの自己署名証明書）が起点になっていることが重要なポイントです。

JPKIの場合、（官職）証明書検証サーバなるものが用意されています。実際の証明書検証はこのサーバに依頼して行うことができます。しかしこのサーバの応答の署名の検証は、やはり、アリスの信頼点である東京都CAの公開鍵を使って行われることが重要なポイントです。

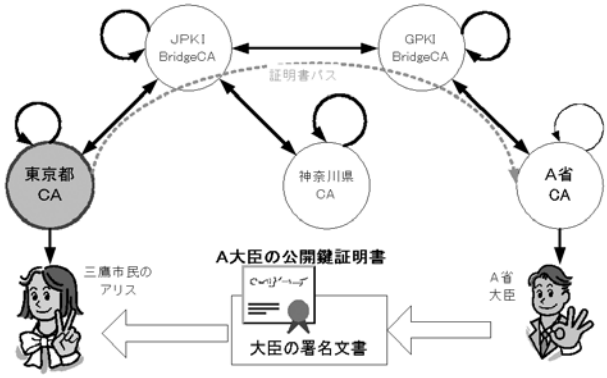

図4

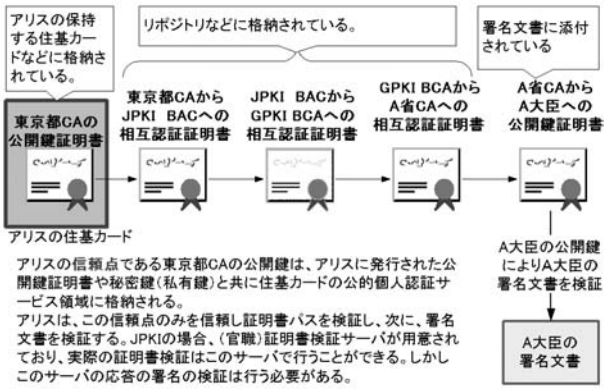

図5

6. 公的個人認証サービスのリポジトリとアプリケーションの構成

PKIではよくリポジトリなるものが出てきます。リポジトリには、一般に証明書ユーザ間で共有される色々な情報が置かれますが、これらの情報は、CAの署名が付与されてリポジトリに置かれます。このリポジトリは、JPKIの場合バックエンドに隠れているとも言えます。しかし、リポジトリ自体は存在し重要な役割を果たしています。JPKIでは、リポジトリにLDAPサーバが使用されており、証明書失効リスト(CRL)や自己署名証明書、相互認証証明書ペアなどが置かれます。これらは、証明書パスの構築や各証明書の失効検証のために利用されます。

署名検証者のアリスは、証明書パス検証のためにリポジトリ(LDAPサーバ)をアクセスしますが、アリスは、リポジトリに格納されたデータの内容を無条件に信頼するわけではありません。アリスの信頼点を元に証明書パス検証を行うことが重要です。

図6は、JPKIのクライアントのJPKIアプリケーション環境を示しています。アリス固有の情報でアリスのみがアクセスする情報である証明書や鍵をクレデンシャルと呼ぶことがあります。このクレデンシャルはアリスが保持する住基カードに格納され、そのクレデンシャルをアクセスするAPIが存在します。JPKIの証明書の取得時に配布されるCD-ROMには、この住基カードの公的個人認証サービスのクレデンシャルをアクセスするためのAPIであるPKCS#11モジュールやMicrosoftのCryptoAPIのためのCSP(Cryptographic Service Provider)といったものが含まれています。

証明書ユーザ間で共有する情報はリポジトリから取得します。これらの情報の多くは、証明書の検証を行なうために存在します。JPKIでは、官職証明書検証サーバが用意されているため、証明書ホルダーが、直接リポジトリにアクセスする必要はありません。しかし、官職証明書検証サーバのメッセージ自体は、やはり、住基カードのJPKI領域に格納されたアリスの信頼点を利用して検証を行います。また、この官職証明書検証サーバにアクセスするためのライブラリもCD-ROMからインストールできるようです。

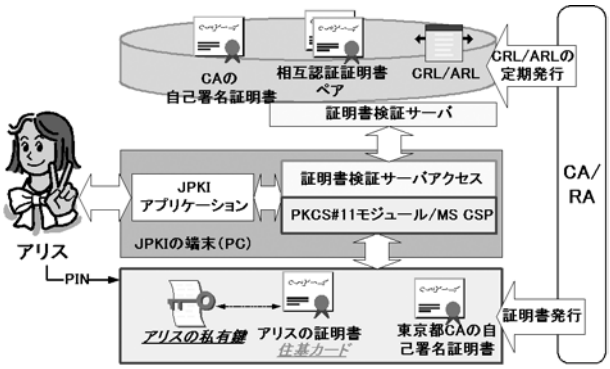

図6

7. 公的個人認証サービスの証明書ポリシーとポリシマッピング

証明書ホルダーの証明書には、証明書ポリシー拡張なるものが含まれています。この証明書ポリシー拡張には、この証明書のポリシーを現すOID(Object Identifiers)が記述されていますが、この証明書ポリシーOIDに対応するポリシーの文書は、東京都認証局運用規程などに記述されています。JPKIの場合、東京都CAに限らず、全都道府県CAで同じOID(1.2.392.200149.8.5.1.1.10)を使用しています。つまり証明書ポリシーを共有しています。例えば東京都CAは、将来東京都民だけのために独自のポリシーを持った証明書を発行することが可能だと考えられます。しかし、現時点では各都道府県CAは同一のポリシーの証明書のみを発行しており、JPKI全体でひとつのドメインを形成していると言えます。

これに対して、GPKIのブリッジCA、各府省CA、各民間CAは、独自の証明書ポリシーを持っています。こうした場合、異なったドメインを乗り越えるためのCA証明書を発行します。JPKIブリッジCAからGPKIブリッジCAへ発行しているCA証明書は、

JPKIの証明書ホルダーの証明書ポリシーと同等のポリシーで検証を行うために、ポリシマッピング拡張なるものが含まれています。このポリシマッピング拡張を含んだ証明書では、証明書発行ドメインのポリシーと、相手のドメインのポリシーが等価であることを宣言することができます。こうした証明書は、相互認証証明書（Cross Certificate）と呼ばれますが、これは、認証ドメインを横断するための証明書ということになります。

JPKIドメイン内では、証明書ホルダーに発行されている証明書以外にも、色々なポリシーの証明書が発行されています。しかし、他のドメインに渡って証明書のパスが検証できる、すなわち、ポリシマッピングが行なわれるものは、証明書ポリシーのOIDの末尾が10のものに限られます。これらの証明書の証明書ポリシー拡張は、クリチカルというフラグが設定されており、処理を必須としています。このように、ドメインを横断するために相互認証証明書が発行されますが、色々なポリシーの証明書が全て他のPKIドメインで有効になるわけではありません。これは、逆に言えば、JPKIドメインでは、自ドメインのユーザの利便性のために、自ドメインにおいてのみ有効な色々な証明書を発行できるということです。

この証明書のポリシーなどにより信頼を制御することをポリシー制御と呼んでいます。ポリシー制御を前提とした場合、証明書には各種の制約拡張なるものが含まれるのが普通です。この制約拡張は、証明書パスの検証を制約する方向に機能します。例えば、アプリケーションの要求により自ドメインのみを信頼するとか、自分の信頼点から遠く離れたCAは信頼したくないといったことが制約にあたります。これは、色々なドメインのPKIを相互認証する場合、特に重要な機能と言えます。ポリシー制御は、小規模なPKIやクローズドなPKIなどにおいては必要のない機能だったため、あまり知られていない面があります。しかし、オープンで広い認証ドメインにおいて、色々なポリシーの証明書が発行される中、自分の要求するポリシーの証明書を受け入れるための重要なメカニズムだと考えられます。

図7に、JPKI、GPKIにおけるポリシマッピングの様子を示します。“CP=J.10”は、JPKIの市民向けの証明書ポリシがOID（1.2.392.200149.8.5.1.1.10）であることを意味します。“PM J.10=X.10）は、JPKIのドメインのJ.10という証明書ポリシーが、GPKIブリッジCAドメインのX.10という証明書ポリシーと等価であるというポリシマッピングを行なっています。

JPKIの署名の検証における証明書パス検証は、ポリシー制御を行なうことを想定され、証明書には各種の制約拡張が含まれます。それに対して、WebサーバのSSL認証では、ブリッジCAから発行される自己書名証明書を信頼点とすることにより、単純な証明書パス検証のメカニズムのみを利用しています。こうすることにより、多くのブラウザ環境において動作させることを可能にしています。ブリッジCAから発行される自己署名証明書は、JPKIの証明書の取得時に配付されるCD-ROMからPCにインストールされます。逆に官職の証明書の検証には、ポリシマッピング拡張や、他の複雑な制約拡張の解釈を含んだ証明書のパス検証が要求されます。JPKIでは、官職証明書検証サーバを利用することにより、クライアントのソフトウェアの負担を減らしています。

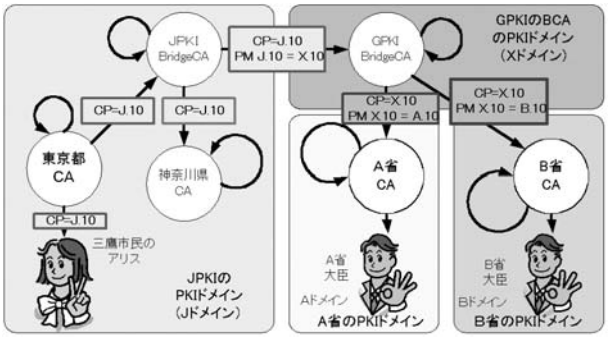

図7

8. 公的個人認証サービスの課題

公的個人認証サービスと似たようなサービスは、世界中で実施、または計画されています。実社会に

おける身分証明書が電子化したものは、よりバーチャルなこれからの情報化社会、ネットワーク社会、そして電子社会においてより重要なものになると考えている地域や国は多いのでしょう。しかし現在まで、こうした電子身分証なるものが成功した事例はまだ少ないようです。これから電子社会には必要になると考えられるが現在のところあまり使い道がないというのが一般的な状況のように見えます。日本の公的個人認証サービスも、現在の延長線上だけでは広く使われるとは考えにくい面があります。しかし、多くの地域や国で検討されているように、公的個人認証サービス、ないし似たようなサービスが来るべき電子社会において必要になると考えている方はやはり多いのではないかと思います。それは、本格化するネットワーク社会を成熟したものにするためには信頼の拠りどころが重要だと考えられているからです。そうした中、このようなサービスが、日本においてどのように計画されているのか、また、どのような技術で実現しようとしているのかといったことは非常に分かり難いものがあります。やはり広く技術情報が公開され多くの人にその内容が理解されることが望まれます。

公的個人認証サービスの普及の鍵のひとつは、セキュアで、かつ、使いやすいアプリケーションが数多く開発されることだと考えられます。しかし現実には、使いやすいアプリケーションを開発しようにも、あまりにも正確な情報が少ないのが現状ではないでしょうか。公的個人認証サービスに限らず、行政に関連したITに関する技術情報は、多くの場合、個々の政府機関や、業界団体などが情報を抱き込んでしまっており、そのため正確な情報が流通していないのが現状に見えます。これは、IT施策に関係している行政関係の方や、ITに関する行政関係の仕事に携われている多くの方にとっても全体像を的確に把握することを非常に困難なものにしています。公的個人認証サービスに関しても、使いやすくセキュアなアプリケーションの開発を促進することを阻害しているように見えます。

以上のようなことも踏まえ、JNSAのチャレンジPKIプロジェクトでは、技術的な観点からオープンで比較的大規模なPKIの相互運用技術の問題点を解決することを目標として活動を行っています。活動のひとつに、政府認証基盤（GPKI）の仕様に基づく相互運用テストフレームワークなどの開発があり、これはGPKIなどのアプリケーションの開発を促進することを目標としています。また、幅広い認証ドメインにおけるPKIのベストカレントプラクティスを示す「マルチドメインPKIの相互運用性に関するメモ」をIETF（Intenet Engineering Task Force）のRFCとして提案するなどの活動も行っています。IETFでの提案は、広く世界に受け入れられる必要があり、そのため、欧米の動向を調査するだけでなく海外とのPKIイニシアチブと連携していくことを検討しています。そして、こうした活動の成果をフィードバックすることにより、現在の技術の状況や、今後の電子署名・認証フレームワークの方向性を多少なりとも示すことができないかと考えています。本稿は、そのほんの一部分ですが、多少なりとも参考になれば幸いです。

参考文献

「公的個人認証サービス」は必要なのか
http://www.rieti.go.jp/it/column/column040210.html
公的個人認証サービスポータルサイト
http://www.jpki.go.jp/
Challenge PKI ホームページ
http://www.jnsa.org/mpki/index_j.html