神奈川県マンション管理士会 第13回勉強会資料　　2005年1月30日

電磁的方法と電子署名

内 藤 正 裕 ※

1　はじめに

平成 14 年の区分所有法の改正により、管理組合運営で電磁的方法が利用可能になった。法改正により電磁的方法が利用可能になったのは、以下の 3 つである。

(1) 規約・議事録の電磁的方法による作成・保管
　(ただし電子署名が必要)
(2) 電磁的方法による議決権行使
(3) 集会を開かない電磁的方法による決議

これを受けて平成 16 年 1 月に改正されたマンション標準管理規約では電磁的方法が利用可能な場合と、そうでない場合に分けて条文が用意されている。

インターネットの普及により、電子メールを利用した議決権行使書の送付や、ユーザーID とパスワードを使って議決権行使用のホームページにログオンしての電子投票については、誰もが具体的なイメージを抱くことができると思うが、規約・議事録の電子署名については、管理組合が具体的にどのようなことを行えばよいのか、まったく分からないという方も多いと思われる。

ここでは、一般にあまり馴染みのない電子署名について紹介し、実際の管理組合運営の中でどのように対応すればよいかを具体的に示す。

2　電磁的方法が持つリスク

インターネットの急速な普及により、オンラインでの商品購入などが一般の消費者の間でも日常的に行われるようになった。この場合、常に問題になるのが、セキュリティの確保である。電磁的方法には、一般に次の 4 つのリスクが存在する。

(1) 盗聴
(2) 改ざん
(3) なりすまし
(4) 否認

インターネット上では機密情報や個人情報などが第三者によって盗聴されやすく、デジタル情報は改ざんした形跡が残りにくい。また、多くのウィルスメールに見られるように他人の名前を詐称したメールの送信が可能であり、そのために、逆にメールを出した本人が、自分が出したものではないと否認できてしまう。これらのトラブルを防ぐには、暗号化と電子署名を行う必要がある。

3　暗号化とは何か？

電子署名の仕組みを理解するには、まず暗号化について知っておく必要がある。電磁的方法ではすべての情報は数値で表され、暗号化のための「鍵」もその実体は数値である。多くの暗号化方式が存在し、それぞれ特定の計算方法(アルゴリズム)により暗号文が作成される。

(1) 共通鍵暗号方式

暗号化と復号に同じ鍵を用いるものが共通鍵暗号方式(または秘密鍵暗号方式)である。以下、暗号化されていない元の文章を「平文」と言う。

(共通鍵暗号方式の例)

平文に共通鍵を加算(減算)する暗号方式を用い、共通鍵を 13 と定める。

平文 20 に共通鍵 13 を加えて暗号文は 33 となる。復号するときは、暗号文 33 から共通鍵 13 を引けば平文 20 が得られる。

共通鍵暗号方式は高速に処理出来ることがメリットであるが、暗号強度は低い。また、事前に相手に対して秘密裏に鍵を渡しておく必要があるため、自分のパソコンにデータを暗号化して保存したり、限られた特定の相手とのやり取りをしたりする用途に適している。無線 LAN で多く使われている WEP キーによる暗号化はこの方式で、40bit または 104bit の共通鍵が用いられている。

(2) 公開鍵暗号方式

公開鍵と秘密鍵の鍵ペアを用いるものを公開鍵暗号方式(PKI=Public Key Infrastructure)と言う。公開鍵は誰に配布してもよく、公開鍵で暗号化し、秘密鍵で復号するのが基本となる。誰でも公開鍵によって暗号化ができるが、それを復号できるのは秘密鍵を持っている人だけであるため、電子メールやファイルを送る相手の公開鍵で暗号化して送信し、受け取った本人が秘密鍵で復号することで、電子メールの盗聴を防ぐことができる。

最も有名な RSA 暗号方式は、「大きな素数と素数の積を求めるのは容易だが、逆にその積から元の 2 つの素数を求めるのは難しい」という非可逆性を利用したもので、インターネットでのオンライン購入などのセキュリティ確保(SSL=Secure Socket Layer)に用いられるほか、電子署名にも広く使われている。

(公開鍵暗号方式の例)

2 つの素数として 71 と 23 を選び、RSA 方式により公開鍵として 47 と 1633、秘密鍵として 213 と 1633 を定める。

平文 20 を 47 乗した数を 1633 で割った余り 456 が暗号文。この暗号文 456 を 213 乗して 1633 で割った余りを求めると 20 となり、復号ができる。

上の例では秘密鍵 213 が知られない限り、暗号文は安全である。公開鍵 1633 が 2 つの素数 71 と 23 の積であることが分かってしまうと秘密鍵が知られてしまうが、実際には公開鍵には 1024 ビット(16 進法では 256 桁、10 進法では 309 桁という天文学的数字)や 2048 ビットの大きな整数が用いられるため、元の 2 つの素数を知ることは極めて困難である。

実際に筆者がベリサイン社から発行を受けた個人証明書(クラス 1)の公開鍵は図 3-1 のような数値である。この整数の素因数分解に成功すると、暗号が解読されてしまうことになるが、現在最高速のスーパーコンピューターを用いても解読には膨大な時間がかかるので、事実上不可能と考えてよい。

※神奈川県マンション管理士会理事

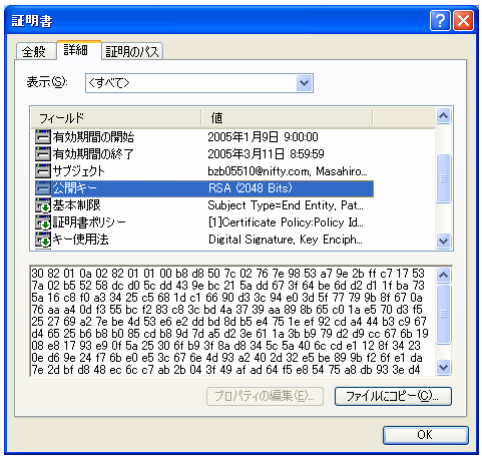

図 3-1　2048 ビットの公開鍵

4　電子署名とは何か？

電子署名には、公開鍵暗号方式の秘密鍵・公開鍵と、認証機関(CA=Certificate Authority)から発行される個人証明書を用いる。平文を秘密鍵で暗号化して、公開鍵と電子証明書を添付したものが電子署名である。公開鍵を用いることにより電子署名された文書を誰でも復号できるが、その暗号文を作成できるのは秘密鍵を持っている本人だけなので、正しく本人が作成した文書であることが証明される。これにより、改ざん、なりすまし、否認を防止できる。

実際には元の文書をそのまま暗号化するのではなく、ハッシュ関数と呼ばれる関数により文書のハッシュ値(またはメッセージダイジェスト)を計算して、それを暗号化する方法が採用されている。ハッシュ関数として最も用いられているのは SHA-1 という関数であり、原文から 160 ビット(16 進数字で 40 桁)のハッシュ値を生成する。その他に 128 ビット(16 進数字で 32 桁)のハッシュ値を生成する MD5 などの関数も使われる。

ハッシュ値は原文を少しでも変更するとまったく違う数値になるという性質を持っており、同じハッシュ値を得る原文を作成することも極めて困難である。このハッシュ値を秘密鍵によって暗号化したものを原文と一緒に送り、公開鍵で復号されたハッシュ値と原文から計算されるハッシュ値が一致することを確認することで、原文が改ざんされていないことが証明される。

ただし、秘密鍵と公開鍵のセットは誰でも簡単に作ることができるので、暗号文に添付された公開鍵が本当に本人のものかどうかを確認する必要がある。公開鍵そのものは数値が大きすぎるので、前述のハッシュ関数を用いて 160 ビットまたは 128 ビットの数値に変換したフィンガープリント(拇印)が用いられる。ホームページなどで公開されたフィンガープリントと照合することにより、その公開鍵は正しく本人のものであることを確認できる。前に紹介した筆者の公開鍵のフィンガープリントは SHA-1 関数により 40 桁の 16 進数字として表示されている(図 4-1)。

しかし、公開鍵のフィンガープリントをその都度自分で確認するのは大変な作業である。その代わりに、鍵ペアを作成した認証局が、その公開鍵に対して電子署名して正しく本人のものであることを証明したものが個人証明書である。その認証局が信頼できれば、その認証局の電子署名がある公開鍵もすべて信頼できることになるので、いちいち自分で公開鍵を確認する必要がなくなる。Microsoft のインターネットエクスプローラには、このような信頼できる認証機関が前もって登録されている。これらの認証局が発行した電子証明書は Windows 上では「問題がありません」と表示される。

ちなみに「電子署名及び認証業務に関する法律」では、この認証業務のうち、本人確認のための一定の基準を満たしたものを「特定認証業務」と定めている。電磁的方法による登記などの場合には、この特定認証業務により発行された個人証明書による電子署名が要求されているが、区分所有法が要求する電子署名はそこまでの本人確認は要求していない。

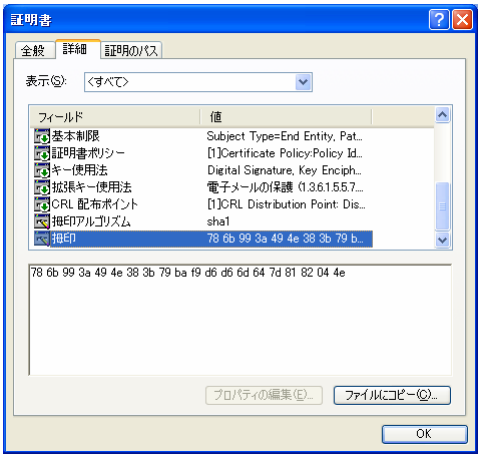

図 4-1　SHA-1 関数によるフィンガープリント(拇印)

さて、確認のため、インターネットのプロパティを開き、「コンテンツ」の中にある「証明書」ボタンを押してみよう。

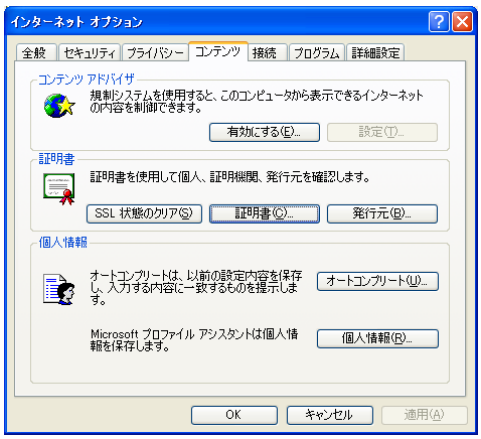

図 4-2　証明書の管理

「信頼されたルート証明機関」の見出しをクリックすると、すでに登録済みの認証局が多数表示される。筆者が個人証明書を取得したベリサイン社の認証局もここに登録されている。

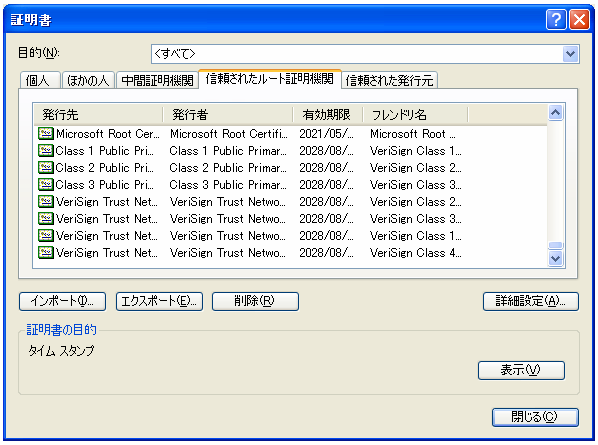

図 4-3　信頼されたルート認証機関(ルートストア)

認証局がここに登録されていると、その認証局が発行した個人証明書を表示させた場合、次の図のように「この証明書は問題ありません」という表示になる。

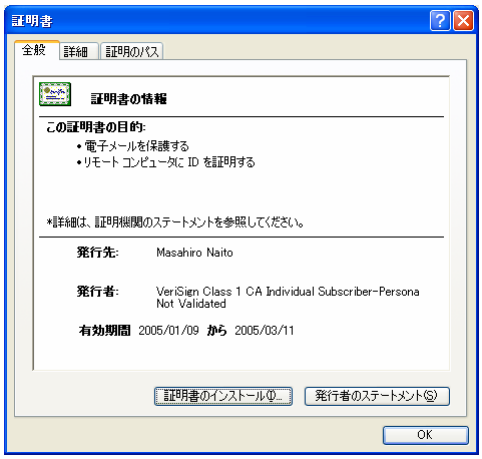

図 4-4　信頼された個人証明書

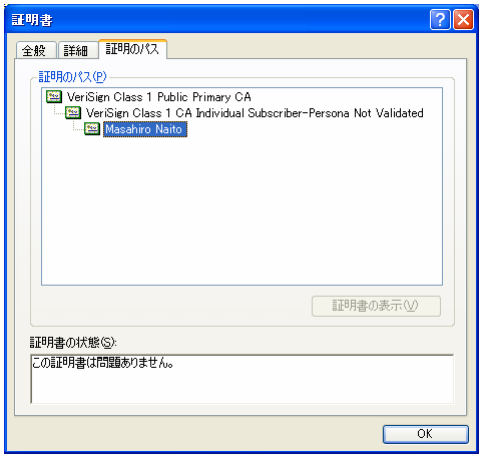

図 4-5　信頼された証明のパス

一方、認証局の登録がない場合は次のような表示になる。

図 4-6　信頼されていない個人証明書

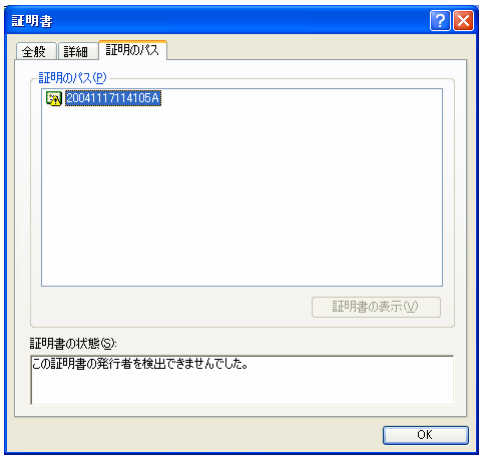

図 4-7　信頼されていない証明のパス

実は上の個人証明書は、公的個人認証サービスにより神奈川県から筆者に発行されたものである。公的個人認証サービスの認証局(筆者の場合、神奈川県)はもともとインターネットエクスプローラに登録されていないので、このような表示になる。

この公的個人認証サービスによる個人証明書は秘密鍵と公開鍵からなる鍵ペアと一緒に住民基本台帳カード(住基カード)の中に書き込まれている。この住基カードは普通の IC カードではなく、暗号化のための CPU を内蔵したもので、「スマートカード」とも呼ばれる。JR の Suica もこのタイプの IC カードである。このカードから暗号鍵を取り出すことは不可能であり、原文を渡すとカードに内蔵された CPU が秘密鍵によって暗号化した結果を返してくる。

この個人証明書が筆者本人のものであることは、神奈川県認証局が電子署名により証明している。そして、この神奈川県認証局の電子署名が本当のものかどうかは、個人証明書の発行を受けたときに市役所の窓口で渡される書類や、「公的個人認証ポータルサイト」(http://www.jpki.go.jp/cps.html)で確認ができる。

この神奈川県認証局の個人証明書名は住基カードから取り出すことが可能で、神奈川県認証局のフィンガープリント

42 48 fe 76 41 bc 24 7d 5d 10 e1 8b f3 eb 00 88 57 b5 e2 8d

と一致することを確認した後に、後述する方法でインターネットエクスプローラに登録すれば、その後の表示は次のようになる。

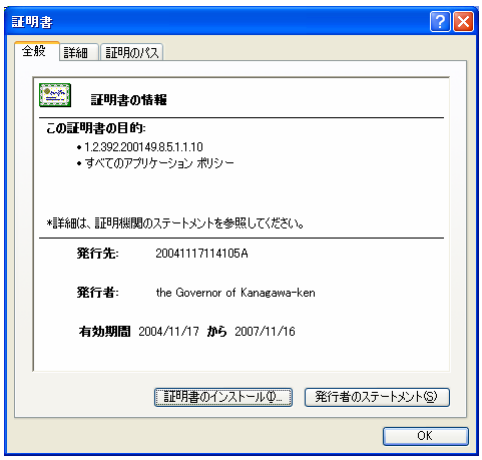

図 4-8　信頼された個人証明書

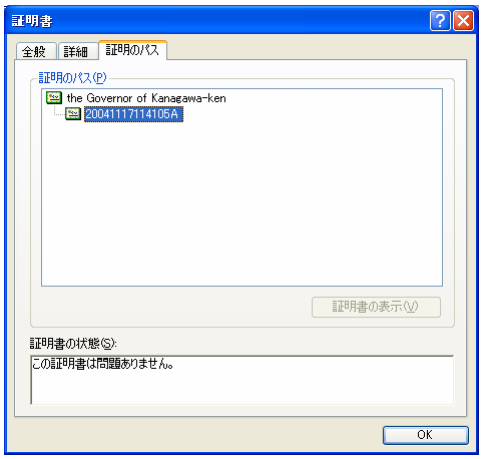

図 4-9　信頼された証明のパス

5　自分で個人証明書を作る方法

電子署名に必要な鍵ペアと個人証明書は、公的個人認証サービスや、民間の認証機関から入手する他に、自分で作成することも可能である。

鍵ペアと個人証明書を自分で作成するためのツールはインターネットを探せば入手できるが、最も簡単なのは Microsoft Office に含まれている Selfcert.exe というプログラムを使う方法である。

C:¥Program Files¥Microsoft Office¥Office10
というフォルダの下にある Selfcert.exe を起動すると、次のような画面が現れる。

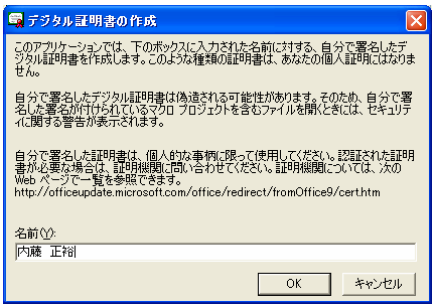

図 5-1　デジタル証明書の作成

ここに名前を入力して OK ボタンを押すと個人証明書が作られて、自動的にインターネットエクスプローラに登録される。この場合、認証局は自分自身である。確認のため、「インターネットオプション」の「コンテンツ」の「証明書」ボタンを押すと、下のように証明書が発行されたことが分かる。

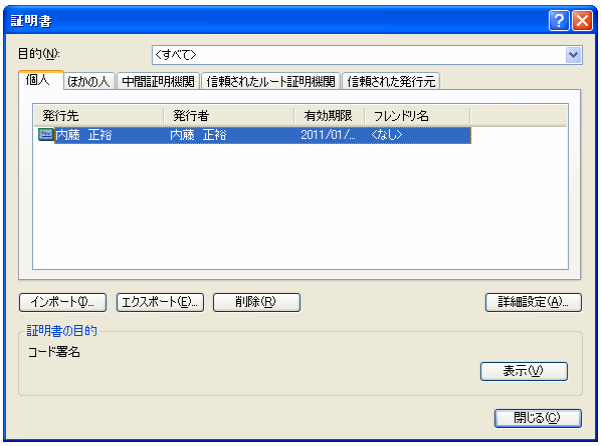

図 5-2 作成された個人証明書

この証明書を開いてみると、まだ信頼されていないので赤い×印がある状態である。

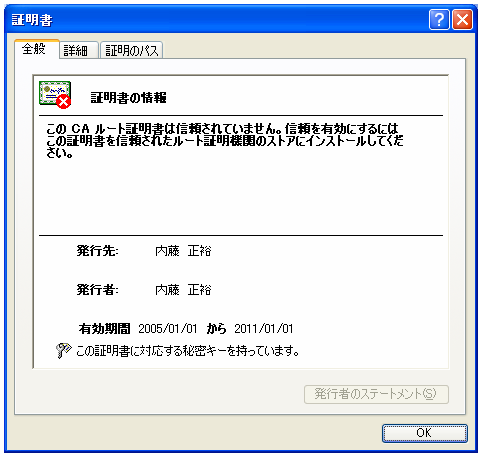

図 5-3 信頼されていないルート証明者

「エクスポート」ボタンを押して、画面の指示に従って個人証明書をファイルに書き出すことができる。ただし Selfcert.exe で作った証明書の場合、秘密鍵を書き出すことはできない。

ここで書き出しされた個人証明書(拡張子は cer)ファイルを今度は「インポート」ボタンを押して「信頼されたルート証明機関」に取り込む。

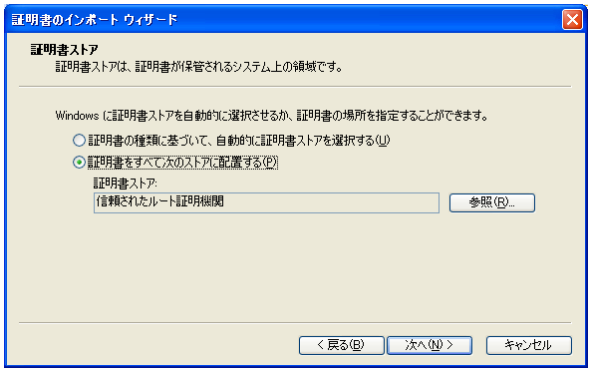

図 5-4 証明書のインポート

すると下のような確認画面が表示されて、「はい」を押すと、信頼されたルート認証機関のストア(ルートストア)に取り込まれる。

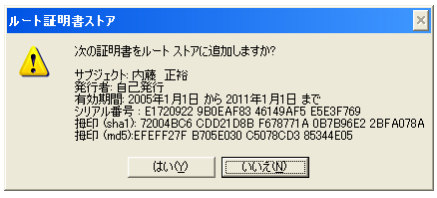

図 5-5 ルートストアへの追加

その後の表示は下のようになる。これは発行者である筆者がルートストアに登録されたからである。

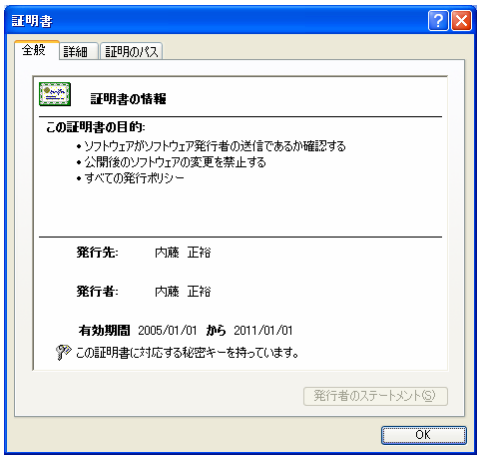

図 5-6 ルートストアに追加後の証明書

6　相手の個人証明書を登録する

あらかじめ署名人の個人証明書(公開鍵)を入手して上のようにルートストアに登録しておくことで、電子署名が本人のものであるかどうかを簡単に検証できるようになる。ただし、相手から送ってもらった証明書をルートストアに追加する場合は、間違いなく当人の証明書であることを確認するために、フィンガープリント(拇印)の照合をすることが肝要である。

まず川原一守氏から送られてきた個人証明書をルートストアに追加してみよう。川原氏当人からは別途フィンガープリントの連絡を受けており、照合済みとする。

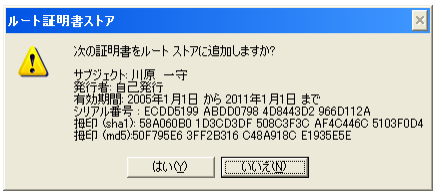

図 6-1 ルートストアへの証明書の追加

同様に日野邦男氏、田中久之氏の個人証明書を追加した状態が次の画面である。

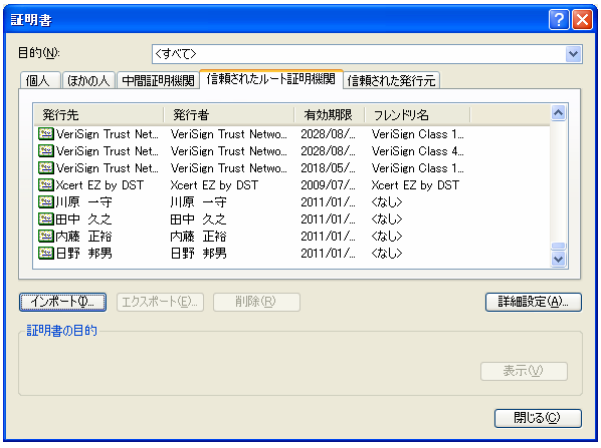

図 6-2 ルートストアの管理

このように Selfcert.exe で各人が作った個人証明書を用いて規約・議事録の電子署名を行うことも理論的には可能である。しかし、この方法で作成した秘密鍵には何のプロテクトもないため、そのパソコンを使う人間なら誰でもこの秘密鍵を使うことができるというセキュリティ上の問題がある。また、区分所有者の各人がそれぞれ証明書を作成し、互いにそれをやり取りするのも現実的なことではない。そこで管理組合がまとめて組合員に個人証明書を発行する方法が考えられる。

7　管理組合が認証機関となって発行する方法

ここでは便宜上、神奈川県マンション管理士会を管理組合とみなして、そこが認証機関となるケースで説明しよう。まず管理士会認証局が署名人全員の個人証明書を発行することから始まるが、そのためのツール(例えば EasyCert 0.89b1 など)はインターネットから入手可能である。ここでは鍵ペアと証明書の作成方法に関する詳しい説明は省略する。

署名人には士会から鍵ペアと電子証明書を含んだファイルが渡される。本人確認のため、「本人限定受取郵便」を利用するか、総会等の場で直接本人に手渡しするのが望ましい。拡張子が「p12」というファイルで、このファイルをダブルクリックするとパスワードの入力を求められる。別途士会から連絡を受けたパスワードを入力し、下の 2 つの四角にチェックを入れて、次へ進む。

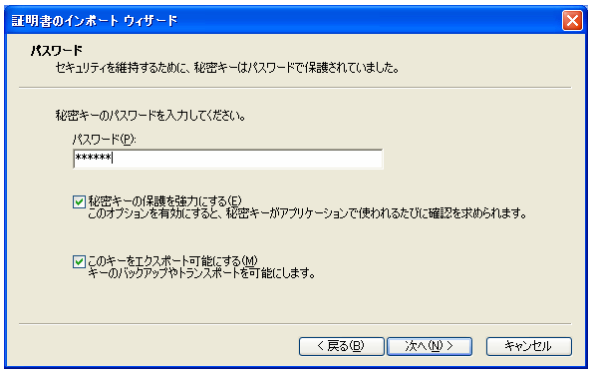

図 7-1 秘密鍵のインポート

次の画面では「自動的に証明書ストアを選択する」を選ぶ。

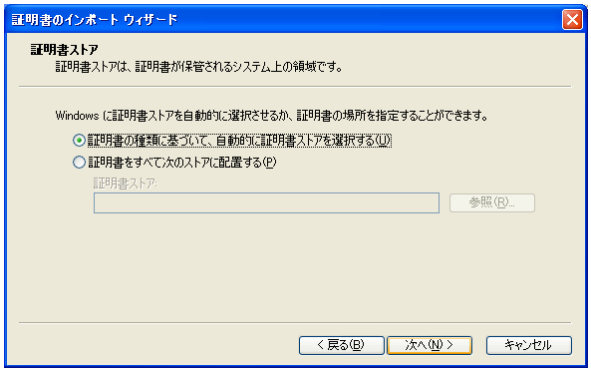

図 7-2 証明書のインポート

下の画面が表示されたら、セキュリティレベルの設定ボタンを押す。

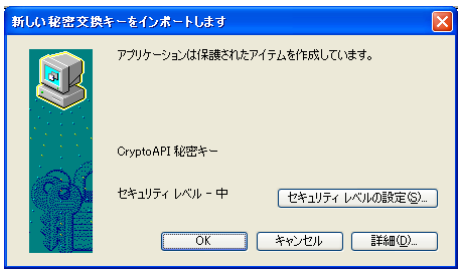

図 7-3 セキュリティレベルの設定

秘密鍵の不正使用を防ぐために「高」を選ぶ。

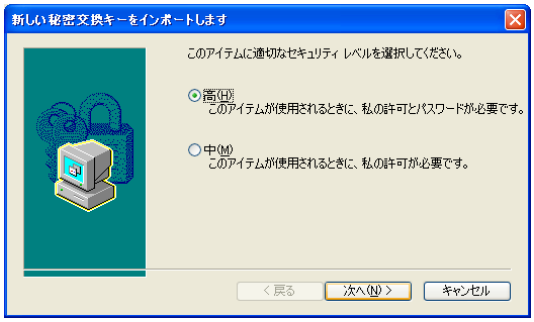

図 7-4 秘密鍵のセキュリティレベル

パスワードの入力を求められるので、任意のパスワードを設定する。このパスワードは電子署名を行う際に毎回必要となるので、忘れないこと。

図 7-5 秘密鍵使用時のパスワード

続いて神奈川県マンション管理士会の証明書をルートストアに追加するかどうか聞かれるので、「はい」を押す。

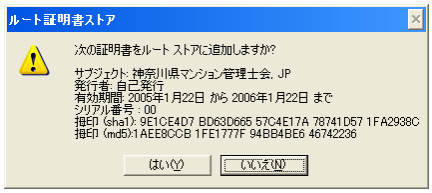

図 7-6 ルートストアへの追加

ただし、別途渡される士会のフィンガープリントと一致していることを確認すること。

個人証明書が正しく取り込まれると次のようになる。

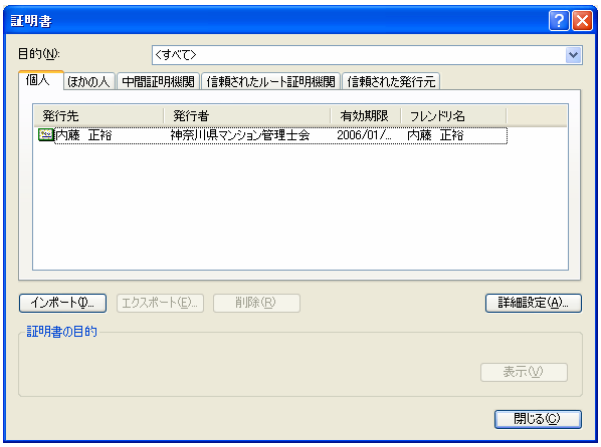

図 7-7 追加された個人証明書

ルートストアには神奈川県マンション管理士会の証明書が追加されている。

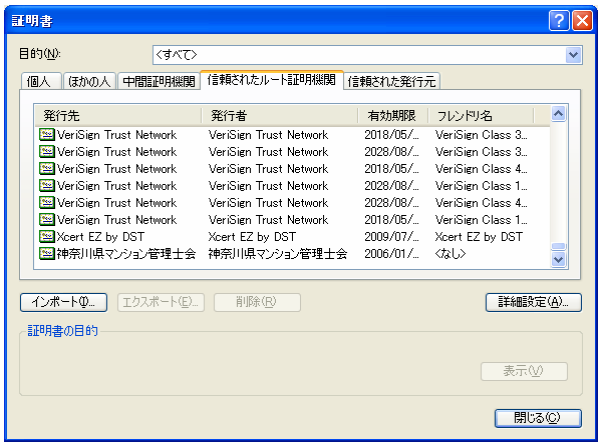

図 7-8 追加された認証局

鍵ペアと個人証明書を取り込んだ後は、元の「p12」ファイルは、安全な場所にバックアップとして保管しておくこと。

8 民間の認証機関のサービスを受ける方法

管理組合が独自に個人証明書を発行し、管理していくのは結構大変なことである。特に問題となるのは、管理組合認証局での秘密鍵の管理だろう。秘密鍵は発行後には確実に消去するのが基本であるが、発行者に悪意があると、他人の秘密鍵を使って規約・議事録の改ざんが出来てしまうからである。

管理組合が認証局となることに不安がある場合、民間のサービスを利用する方法がある。個人で購入できるものとしては、例えば日本認証サービスの AccreditedSign パブリックサービス 1 基本型証明書がある。これは、民間取引用(B to B)の証明書で、価格は有効期間 2 年で 18,000 円、有効期間 3 年だと 24,000 円である。この証明書の発行の際には、「本人限定受取郵便」によって厳密な本人確認を行っており、鍵ペアと個人証明書は暗号化された形でサーバーから本人が直接ダウンロードする。筆者が持つクラス 1 レベルの個人証明書が「認印」レベルだとすると、この個人証明書はベリサイン社のクラス 3 レベルに相当するもので、「実印」レベルのものである。法的にも疑義の生じない電子署名が可能であるが、コスト高であることが難点である。

9 クラス 1 レベルの個人証明書の利用

もう少し安価に実現できる方法としては、例えばベリサイン社のクラス 1 レベルの個人証明書によって電子署名を行うことが考えられる。ただし、ベリサイン社からは直接個人での入手はできないので、提携パートナー等を通して入手となる。確認は取っていないが、有効期限 1 年間の個人証明書が 3,000 円程度で入手可能と思われる。

なお、このクラス 1 レベルの個人証明書は氏名と電子メールの情報のみで発行されるもので、本人確認のレベルは低いが、署名人からメールアドレスや場合によってはフィンガープリントを管理組合に届け出てもらうことにより、その点は補完できる。そもそも規約・議事録の押印には認印で十分であり、電子署名としてもクラス 1 レベルで十分と思われる。具体的な実施方法を次に示す。

ベリサイン社のクラス１個人証明書を用いる方法

(1) まず署名人に対して電子署名や個人証明書に関する教育を行い、個人証明書の不正使用等によるトラブルの防止を図る。

(2) 署名人は電子署名用の電子メールアドレスを管理組合に届け出る。通常個人で使用しているメールアドレスでも良いが、個人のメールアドレスを電子署名として使用したくない場合は、電子署名用に別のメールアドレスを取得していただく。なお、署名人がインターネットにアクセスする環境にない場合は、管理組合からパソコンの貸与やインターネット接続環境の提供を行うことも検討する。

(3) 署名人は全員ベリサイン社のクラス１レベルの個人証明書(氏名とメールアドレスの情報をもとに発行されるもの)を入手する。

(4) Microsoft Word のデジタル署名機能を用いて、規約・議事録のファイルに電子署名を行う。

(5) 電子署名された規約・議事録はフロッピーディスク等の電磁的記録媒体に保存し、管理者(管理組合理事長)が保管する。

(6) 署名人の個人証明書は署名を行う時点では有効な電子署名だが、その後は有効期限切れになっても更新は行わない。

１０　公的個人認証サービスの個人証明書の流用

公的個人認証サービスによって発行された個人証明書を流用する手段もある。この場合、有効期限３年間の個人証明書が発行手数料500円で安価に手に入る(別に有効期限10年間の住基カードの発行手数料500円が必要)。

しかし、秘密鍵を住基カードから取り出すことができないため、ICカードリーダーライターをパソコンに接続した状態でしか電子署名ができないなど、使い勝手はあまり良くない。また、この個人証明書はそもそも行政手続の申請目的のものであるため、氏名・住所のほかに、生年月日と性別が、UTF-8という文字コードで記載されている(図 10-1)。これらの情報が規約や議事録の電子署名に記載されることに、抵抗を感じる区分所有者は少なくないと思われる。また、民間での流用が法的に認められるかどうかも別途検証が必要であろう。

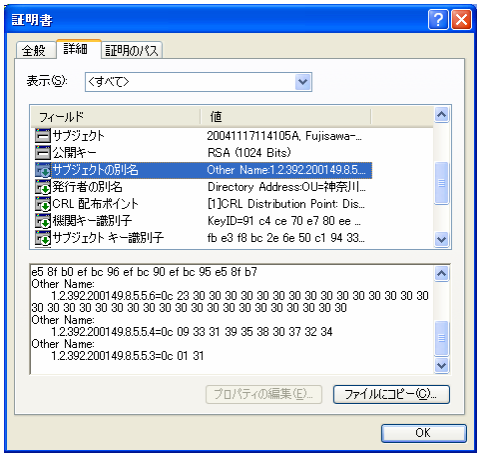

図 10-1 UTF-8 コードで記載された氏名・住所・生年月日・性別

１１　ワード文書に電子署名を行う方法

さて、実際に文書ファイルに電子署名を行う方法を説明しよう。規約や議事録の署名には、複数の署名人が必要になるが、Microsoft Word 2002 では、文書ファイルに複数人の電子署名を行うことが可能になっている。メニューバーの「ツール」の「オプション」を開き、「セキュリティ」の見出しをクリックすると、「デジタル署名」というボタンがある。

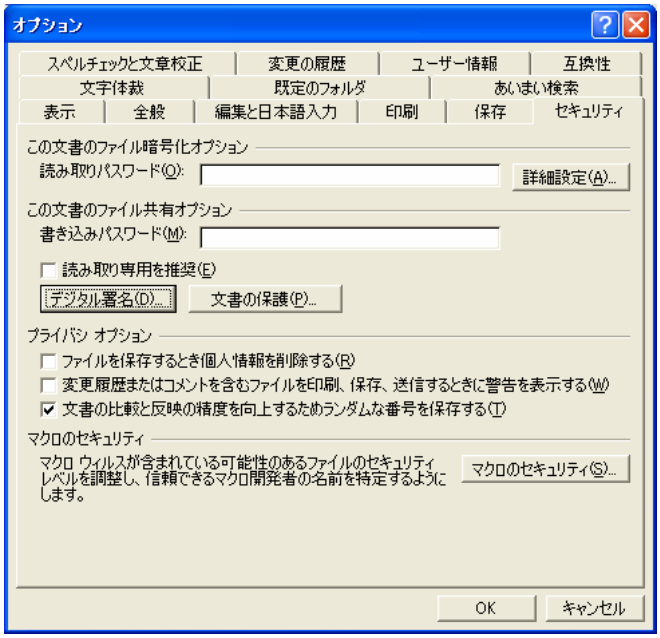

図 11-1 Microsoft Word のデジタル署名

このボタンを押すと、下のような画面が現れて、この文書に誰が署名済みであるかが分かる。正しい署名の例の場合は、下のような画面となる。

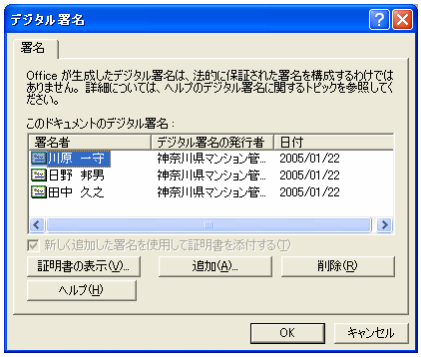

図 11-2 デジタル署名の確認

この画面で「追加」ボタンを押すと、自分が持っている個人証明書で追加の署名ができる。

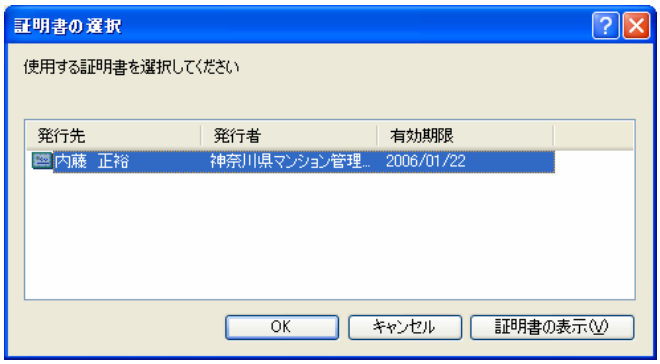

図 11-3 証明書の選択

署名が追加された状態は次の画面となる。

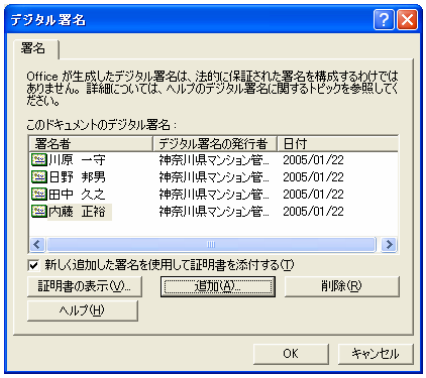

図 11-3 追加された署名

文書に変更(改ざん)が加えられた場合、上のすべての署名が失われる。また、署名が本人のものでないと、この画面で赤い×印が表示されるので分かる。

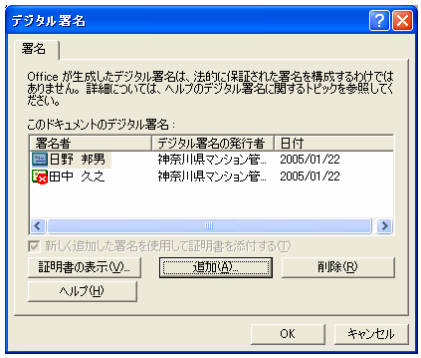

図 11-4 信頼されていない署名

この場合、赤い×印のある田中久之氏の証明書を表示させてみると、「神奈川県マンション管理士会」の名を騙るニセモノの電子証明書であることが分かる。

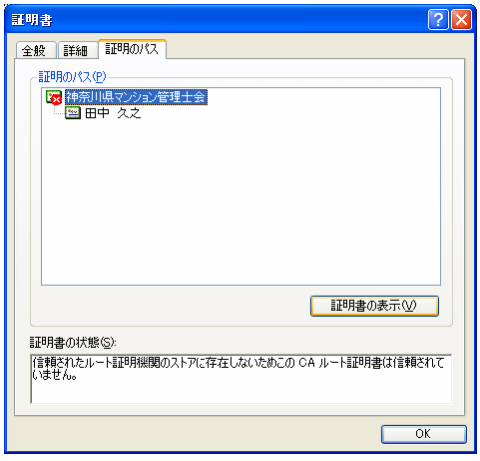

図 11-5 信頼されていない認証局

フィンガープリントを確認すると、まったく異なっていることが分かる(注:これらのフィンガープリントはデモ用に作成したもので、正式なものではありません)。

(正しいフィンガープリント)
9e 1c e4 d7 bd 63 d6 65 57 c4 e1 7a 78 74 1d 57 1f a2 93 8c
(ニセの証明書のフィンガープリント)
d3 f9 ab 10 9b e0 41 fb 1f b6 7b 81 0f 5d 20 e5 e1 5a 97 cc

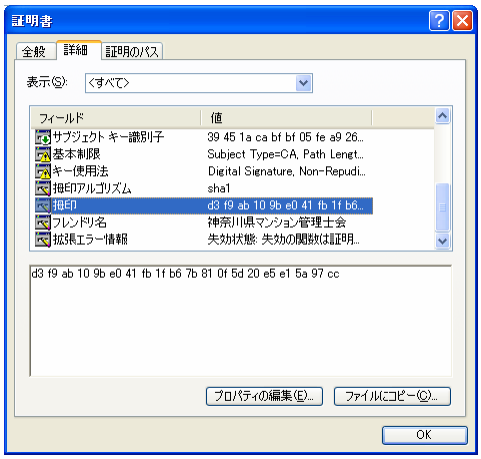

図 11-6 フィンガープリントの不一致

１２　おわりに

区分所有法に規定された規約・議事録の電子署名では、特定認証業務による個人証明書までは要求されていないので、管理組合等が認証機関となって個人証明書を組合員に発行することは法的には問題ない。しかし、規約や議事録の有効性について疑義が生じた際に、電子署名の有効性を主張するには、適正な秘密鍵の管理と、個人証明書の発行の際の本人確認が必要となる。特に秘密鍵の管理については、管理組合が独自に行うことは不可能と思われ、当面はコスト高でも民間の認証機関のサービスを受けるしかない。将来はマンション管理センターや管理業者、管理組合団体等が認証機関となって安価な個人証明書発行サービスを行うことが望まれる。

また、電磁的方法による議決権行使の際にも、その有効性について疑義が生じることのないように、電子署名が行われることが望ましい。あるいは、企業の株主総会での電磁的方法による議決権行使に見られるように、区分所有者にユーザーID とパスワードを付与し、議決権行使用のホームページにログオンして議決権を行使してもらうのも一つの方法である。別途アプリケーション開発が必要となるが、すでに管理組合ホームページを開設しているマンションでは、一考の余地があるかもしれない。その場合の具体的なセキュリティ確保や本人確認の方法については、別の機会に譲りたい。

いずれにしても、管理組合運営に電磁的方法を導入するには、秘密鍵の管理、電子署名の方法、ルートストアの管理など、区分所有者全員が電子署名に対してある程度の知識を持っていることが前提となる。電子署名に対する組合員全員のリテラシーが一定レベルまで向上しない限り、現時点では電子署名の早急な導入は難しいと考える。

将来パスポートのオンライン申請などが可能になり、公的個人認証サービスによる個人証明書の普及が進んだとしても、署名人の生年月日と性別まで電子署名に記載されてしまうため、仮に法的には問題がないとしても、民間での流用はあまり進まないと思われる。むしろ、鍵ペアと個人証明書を IC カードや、携帯電話に保存して、それを電子署名に用いたオンラインでの電子商取引が普及していく可能性のほうが高い。キャッシュカードやクレジットカード、Suica、ETC カード、会員証や社員証に至るまで、すべてのカードが 1 枚の IC カードあるいは携帯電話に統合され、その中に保存された鍵ペアと個人証明書を用いた電子署名が広く一般社会に普及する。区分所有法の電磁的方法に関する条文が活きてくるのは、そうした社会環境が整ったときだろう。そして、それはそう遠くない将来である予感がする。

参考文献

1) 廣田信子「電磁的方法と管理組合運営」マンション管理センター通信、2004 年 11 月