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

証明書		?>
全般 詳細 証明のパス		
表示(<u>S</u>): 〈すべて〉	~	
フィールド	値	~
有効期間の開始	2005年1月9日 9:00:00	
□ 有効期間の終了	2005年3月11日 8:59:59	
目サブジェクト	bzb05510@nifty.com, Masahiro	
━公開キー	RSA (2048 Bits)	
	Subject Type=End Entity, Pat	
100月書ポリシー	[1]Certificate Policy:Policy Id	
■ 年−使用法	Digital Signature, Key Enciph	~
$\begin{array}{c} 30 \ 82 \ 01 \ 0.a \ 02 \ 82 \ 01 \ 01 \ 00 \ b6 \ d4 \ 9 \\ 50 \ 16 \ c8 \ 16 \ a3 \ 24 \ 25 \ c5 \ 68 \ 1d \ c1 \ 28 \ c8 \ c2 \\ 50 \ c1 \ 68 \ c1 \ 32 \ 42 \ 55 \ 68 \ 1d \ c1 \ 28 \ c8 \ c2 \\ 50 \ c1 \ 58 \ c2 \ 58 \ c4 \ 30 \ c4 \ 58 \ c4 \ c$	$\begin{array}{c} 5 \ 0 \ 7 \ 0 \ 7 \ 0 \ 7 \ 6 \ 9 \ 5 \ 3 \ 7 \ 9 \ 2 \ 5 \ 1 \ 7 \ 1 \ 7 \ 5 \ 5 \ 5 \ 7 \ 1 \ 7 \ 5 \ 5 \ 1 \ 5 \ 1 \ 7 \ 1 \ 7 \ 5 \ 5 \ 1 \ 1 \ 5 \ 1 \ 7 \ 5 \ 1 \ 5 \ 1 \ 1 \ 5 \ 1 \ 5 \ 1 \ 1$	<
	プロパティの編集(日) ファイルにコピー(ロ)
	0	<

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。

証明書	?
全般詳細証明のパス	
表示(5): 〈すべて〉	~
フィールド	値
臺基本制限	Subject Type=End Entity, Pat
12311日書ポリシー	[1]Certificate Policy:Policy Id
同キー使用法	Digital Signature, Key Enciph
🔂 拡張キー使用法	電子メールの保護 (1.3.6.1.5.5.7
GRL 配布ポイント	[1]CRL Distribution Point: Dis
🚾 拇印アルゴリズム	sha1
式 提印	78 6b 99 3a 49 4e 38 3b 79 b 🗸 🗸 🗸
78 6b 99 3a 49 4e 38 3b 79	ba 19 d6 d6 6d 6d 7d 81 82 04 4e
,	プロパティの編集(2) ファイルにコピー(2)
	ОК

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。

ンターネット オブション	?
全般 セキュリティ プライバシー コンテンツ 接続 プログラム 詳細設定	
コンテンツアドバイザ 規制システムを使用すると、このコンピュータから表示できるインターネット の内容を制御できます。	
「初にするでと…」 「記の書 「記の書 「記の書を使用して個人、証明機関、発行元を確認します。	
	ן
オートコンガートは、以前の設定内容を保存 し、入力する内容に一致するものを提示します。	כ
Microsoft ブロファイル アシスタントは個人情 軸を保存します。	ן
していた。 のK キャンセル 適用(<u>A)</u>
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。

举行先	 举行者	有効期限	フレンドリ名	
Microsoft Boot Cer	Microsoft Boot Certifi	2021/05/	Microsoft Boot	
Class 1 Public Pri	Class 1 Public Primar	2028/08/	VeriSign Class 1	
🔤 Class 2 Public Pri	Class 2 Public Primar	2028/08/	VeriSign Class 2	
🔛 Class 3 Public Pri	Class 3 Public Primar	2028/08/	VeriSign Class 3	
🔛 VeriSign Trust Net	VeriSign Trust Netwo	2028/08/	VeriSign Class 2	
🔛 VeriSign Trust Net	VeriSign Trust Netwo	2028/08/	VeriSign Class 3	
🔛 VeriSign Trust Net	VeriSign Trust Netwo	2028/08/	VeriSign Class 1	
🔛 VeriSign Trust Net	VeriSign Trust Netwo	2028/08/	VeriSign Class 4	
インボートの エクスポ	ート(<u>E)</u>) 削除(<u>R</u>)]		詳細設定(
四日本の日町				

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

全般 詳細 証明のパス 証明のパス(P) 型 VeriSign Class 1 Public Prime ビッジ VeriSign Class 1 CA Indik し 図 Masshiro Nato	ary CA idual Subscriber-Persona Not Validated
 正明書の状態(S):	福用書の表示公
この部門月書は問題ありません。	ОК

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。

Eigita ? 🔀
全般 「詳細」 証明のパス
証明書の情報 信報不足のため、この証明書を検証できません。
発行先 : 20041117114105A
発行者: the Governor of Kanagawa-ken
有効期間 2004/11/17 から 2007/11/16
1
ОК

図4-6 信頼されていない個人証明書

■ 正明のパス(P) 20041117114105A	
	証明書の表示(V)
証明書の状態(S):	
この証明書の務行者を検出できませ	んでした。

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 el 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。

全般 詳細 証明のパス
副明書の情報
この証明書の目的:
 1239220014985.11.10 すべてのアプリケーション ポリシー
*順半線は、順理明線開始のステートメントを参照してください。
発行先: 20041117114105A
発行者: the Governor of Kanagawa-ken
有効期間 2004/11/17 から 2007/11/16
[証明書のインストール型_] 発行者のステートメント⑤)
OK

図4-8 信頼された個人証明書

証明書	? 🗙
全般 詳細 証明のパス	
証明のパス(P)	
the Governor of Kanagawa-ken	
	証明書の表示♡
目7月日本 の4半台をたい。	
この証明書は問題ありません。	
	ОК

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。

🛱 デジタル証明書の作成 🛛 🛛 🗙
このアプリケーションでは、下のボックスに入力された名前に対する、自分で署名したデ ジタル証明書を作成します。このような種類の証明書は、あなたの個人証明にはなりま せん。
自分で署名したデジタル証明書は偽造される可能性があります。そのため、自分で署 名した署名が付けられているマクロ プロジェクトを含むファイルを聞くときには、セキュリティに関する警告が表示されます。
自分で署名した証明者は、個人的な事物に限って使用して伏だい。認証された証明 者が必要な場合は、証明規則に聞い合わせて伏だい。証明規則については、次の Web Xージでで見を発明できる。 http://officeupdate.microsoft.com/office/redirect/fromOffice9/cert.htm
名前(1):
内藤 止裕
OK キャンセル

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。

証明書			? 🛛
目的心	<বৃশ(C>		~
個人 ほかの人	中間証明機関(信頼されたル	,ート証明機関 信頼された発行元	
発行先	発行者	有効期限 フレンドリ名	
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□	内藤 止裕	2011/01/ <なし>	
インポートロ	エクスポート(E)) 削除(<u>R</u>	詳細設定(A)
証明書の目的―			
コード署名			
			- source
			<u>閉じる(C)</u>

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。

全	校 詳細 証明のパス
	発行者: 内藤 正裕
	有効期間 2005/01/01 から 2011/01/01 デ この証明書に対応する秘密キーを持っています。
	発行者のステートメント⑤
_	OK

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。

証明書のインポート ウィザード
証明書ストア 証明書ストアは、証明書が保管されるシステム上の領域です。
Windows (ご証明書ストアを自動的に)に違択させるか、証明書の場所を指定することができます。
○ 証明書の種類に基づいて、自動的に証明書ストアを選択する(U)
● 罰証明書をすべて次のストアに配置する(P)
肛明書ストア
信頼されたルート調明機関 参照(R)
< 戻る(B) 次へ(N) > キャンパル

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。

ルート証明	明書ストア 🗙
1	次の証明書をルートストアに追加しますが? サブジェクト:内護 正裕 安仁者 日2日 有効期間 2005年1月1日から2011年1月1日まで うジリアル書を1120022 98124F83 461494F5 E5E3F769 14E1 (sha1).72004B06 CD021088 F678771 A 087896E2 28FA078A 指ED (sha1).72004B06 CD021080 F678771 A 087896E2 28FA078A 指ED (sha1).2004B06 CD021080 F678771 A 087896E2 28FA078A 指ED (sha1).2004B06 CD021080 5678020 86344E05
	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5-2 作成された個人証明書



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。

証明書			? 🗙
目的(N): < (個人 ほかの人 中間証明	すべて> 月機関 信頼されたルート語	即機関(信頼された発行元)	•
発行先 E VeriSign Trust Net E VeriSign Trust Net E VeriSign Trust Net E VeriSign Trust Net E VoriSign Tru	発行者 VeriSign Trust Netwo VeriSign Trust Netwo VeriSign Trust Netwo Xcert ZE by DST 川原 一守 田中 久之 内藤 正裕 日野 邦男	有効期限 フレンドリ名 2028/08/-、 VeriSien Class 1 2028/08/-、 VeriSien Class 1 2018/05/-、 VeriSien Class 1 2009/07/-、 VeriSien Class 1 2009/07/-、 Xcert EZ by DST 2011/01/-、 なしン 2011/01/-、 なしン 2011/01/-、 なしン	
「ノンボートの」」 「江川書の目的」	-ト(E)) 前原余(R)		詳細設定(<u>A</u>) 表示(<u>少</u>)
			開じる(<u>C</u>)

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。

証明書のインボート ウィザード	
パスワード セキュリティを維持するために、秘密キーはパスワードで保護されていました。	
秘密キーのパスワードを入力してください。 パスワード(空): *******	
✓ 秘密キーの保護を強力にする(E) このオプションを有数にすると、秘密キーがアプリケーションで使われるたびに確認を求められます。	
ごのキーをエクスポート可能にする(M) キーのパックアップやトランスポートを可能にします。	

次の画面では「自動的に証明書ストアを選択する」を選ぶ。

明書	መኅンポート ዕብቻード
₩.	用書ストア 国証明書ストアは、国証明書が保留されるシステム上の領域です。
	Windows (ご証明書ストアを自動的に)選択させるか、証明書の)場所を指定することができます。
	● 証明書の種類に基づいて、自動的に証明書ストアを選択する(U)
	○ 証明書をすべて次のストアに配置する(P)
	■正明書ストア:
	参照(<u>R</u>)
	< 戻る(B) 次へ(N) > キャンセル

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。

新しい秘密交換	キーをインボートします 🛛 🗙
	アブリケーションは保護されたアイテムを作成しています。
	CryptoAPI 秘密キー
Carl	セキュリティ レベル - 中 セキュリティ レベルの設定(S)
VE	<u>OK</u> キャンセル 詳細(型)

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。

証明書			? 🛛
目的(N):	<すべて>		~
個人 ほかの人 ロ	P間証明機関 信頼されたルート証明	照関 信頼された発行元	
発行先	発行者	有効期限 フレント	7)名
四藤止裕	神奈川県マンション管理士会	2006/01/ 内藤	
インポートΦ_ (1)	ニクスポート(E) 削除(B)		詳細設定(<u>A</u>)
証明書の目的			
			表示♡
			PPIez (c)
			開US (Q)

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。

証明書				?×
目的(N): (すべて)				*
個人 ほかの人 中間証明機関	信頼されたルート証明機関(言頼された発行:	ī t	
発行先	発行者	有効期限	フレン門名	~
🔛 VeriSign Trust Network	VeriSign Trust Network	2018/05/	VeriSign Class 3	
🔛 VeriSign Trust Network	VeriSign Trust Network	2028/08/	VeriSign Class 3	
🔛 VeriSign Trust Network	VeriSign Trust Network	2018/05/	VeriSign Class 4	
🔛 VeriSign Trust Network	VeriSign Trust Network	2028/08/	VeriSign Class 1	
🔛 VeriSign Trust Network	VeriSign Trust Network	2028/08/	VeriSign Class 4	
🔛 VeriSign Trust Network	VeriSign Trust Network	2018/05/	VeriSign Class 1	
Xcert EZ by DST	Xcert EZ by DST	2009/07/	Xcert EZ by DST	
一部では「「「「「「」」」 「「」」 「「」」 「」 「」 「」 「」 「」 「」 「」	神奈川県マンション管理士会	2006/01/	〈なし〉	•
インポートQ (エクスポート(E) (証明書の目的)	削除(<u>R</u>)		【詳細設	定(<u>A</u>)
			表示()	
			開い	3(<u>C</u>)

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。

オプション	? 🛛
スペルチェックと文章校正 変更の履歴 ユーザー情報 文字体裁 既定のフォルダ あい3 ま	互換性 まい検索
 	ビイエリリィ 詳細設定(A)…
この文書のファイル共有オプション 書き込みパスワード(M):	
□ 読み取り専用を推奨(E) □ デジタル署名(D)… 文書の保護(P)…	
プライバシ オプション 「ファイルを保存するとき個人情報を削除する(E) 「変更履歴またはコメントを含むファイルを印刷、保存、送信するときに警告を ▼ 文書の比較と反映の精度を向上するためランダムな番号を保存する(T)	表示する(W)
マクロのセキュリティ マクロ ウィルスが含まれている可能性のあるファイルのセキュリティ レベルを調整し、信頼できるマクロ開発者の名前を特定するように します。	セキュリティ(<u>S</u>)
OK	キャンセル

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。

デジタル署名		? 🗙
署名		
Office が生成したデジタル ありません。詳細については ださい。	署名は、法的に保証されま は、ヘルプのデジタル署名に	と署名を構成するわけでは 関するトピックを参照してく
このドキュメントのデジタル署	四月 :	
署名者	デジタル署名の発行者	日付
四川原 一守	神奈川県マンション管	2005/01/22
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□	神奈川県マンション管…	2005/01/22
◎田中 久之	神奈川県マンション管	2005/01/22
<		>
▶ 新しく追加した署名を付	使用して証明書を添付する	5D
証明書の表示(型)	追加(<u>A</u>)	削除(<u>R</u>)
ヘルプ(H)		
		OK キャンセル

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。

証明書の選択			? 🔀
使用する証明書	を選択してください		
発行先	発行者	有効期限	
220 内藤 正裕	神奈川県マンション	管理… 2006/01/22	
	ОК) キャンセル 証明	書の表示──

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。

デジタル署名		? 🛛
署名		
Office が生成したデジタル署名は、法的に保証された署名を構成するわけでは ありません。詳細については、ヘルプのデジタル署名に関するトピックを参照してく ださい。		
このドキュメントのデジタル	署名:	
署名者	デジタル署名の発行者	日付
▶ 日野 邦男	神奈川県マンション管	2005/01/22
田山 カラ	油奈田県マンバルン燈	2005/01/22
	11/10/178 12/232 6	2000/01/22
		>
 ▲ ▲ ▲ ▲ ▲ ■ ■	「「「「「「「」」」」	
▲ 新しく追加した署名を 証明書の表示(※)	15000000000000000000000000000000000000	2000 01 22 > ①
 ✓ ✓<th>mm mm を使用して都田月書を添付する 【<u>道加(A).</u>】</th><th>(1) (1) (1) (1) (1) (1) (1) (1) (1) (1)</th>	mm mm を使用して都田月書を添付する 【 <u>道加(A).</u> 】	(1) (1) (1) (1) (1) (1) (1) (1) (1) (1)
 ■ 「 ▼ 新しく追加した署名者 ■ 新しく追加した署名者 ■ 野利書の表示 (型 へルブ(出) 	1970日第(フラン 6	● ● ● ●

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。

証明書 ? 🔀
全般 詳細 詳問のパス 詳細のパス(空) 「 詳細(国家)/23) 等理士会 〇 田中 久之
■ 証明書の表示 少 証明書の 状態 (S):
「言頼なれたルート証明規関のストアに存在しないためこの CA ルート証明書は信頼されて いきせん。 OK

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 & (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

 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