商業登記制度に基づく電子認証

Electronic Authentication Based on Commercial Registration System

黛　博之 MAYUZUMI Hiroyuki
神田　敦 KANDA Atsushi
河本　高文 KOMOTO Takafumi

近年，インターネットを利用した電子商取引（EC：Electronic Commerce）は，急速な勢いで広まってきている。時間や場所の制限を受けないインターネットは，商取引を効率的に行うためのもっとも有効な手段であると言える。一方，従来の商取引は印鑑証明書や対面に立脚した世界を前提としているため，ECにおいてはこれまでの法律や制度だけでは決して十分とは言えず，新たな仕組みが必要となってきている。今般，法務省は，デジタル社会において印鑑証明書と同等の意味を持つ電子証明書を発行する電子認証局を設立し，あわせて法律の整備も実施した。

こうした動向のなかで，当社は，民間企業が法務省の電子証明書を取得するために必要な申請受付端末を開発し，全国の登記所へ納入を開始した。また，電子証明書を扱うために必要な，企業向けの利用者ソフトウェアを開発した。

Electronic commerce has rapidly spread in recent years due to the efficiency and effectiveness of the Internet. In traditional commercial transactions in Japan, a paper-based certificate of a seal issued by a commercial registry office is widely used for authentication of the parties. In electronic commerce, however, a new authentication scheme is required because all transactions should be paperless.

To promote secure electronic commerce, the Ministry of Justice has established a new legal scheme, the Electronic Authentication System based on the Commercial Register, in which an electronic certificate of a digital signature issued by a registry office has equivalent legal validity to the traditional paper-based certificate.

Toshiba has developed a terminal system for the electronic commercial register and delivered it to the Ministry of Justice. Deployment of the system to registry offices throughout Japan has now begun. Toshiba has also developed a software package for corporations that use the certificate for electronic commerce and electronic applications.

1 まえがき

商業登記に基礎を置く電子認証制度の導入などを内容とする「商業登記法等の一部を改正する法律」が，2000年4月に公布された。また同年5月には，電子署名や電子認証を行う業務に一定のルールを課すために，「電子署名及び認証業務に関する法律（以下，電子署名法と略記）」が公布された。

法務省は，これら法的整備を実施したうえで，政府の機関としては初めての電子認証局を設立した。日本国内においては，民間の認証局が既にいくつか存在し，個人や企業の本人性確認の手段として利用されていたが，法的な保証がされていなかったため，日本国内におけるECの普及は決して芳しいものではなかった。しかし，今般の政府機関による電子認証局の設立及び法律の整備により，電子署名や電子証明書の位置づけが明確になったことで，今後，ECは急速な勢いで拡大していくことが予想される。また政府は，“電子政府(注1)”実現のために，各種申請手続きの電子化にも積極的に取り組んでいる。この電子申請の場面においては，情報の作成者を確認して内容の改ざんを防ぐ手段が必要となるが，これらを実現するためには，今般の法務省が発行する電子証明書及び電子署名の仕組みは極めて有効な手段と言える。

当社は，この電子証明書を取得するために必要な申請受付端末と，一般企業が法務省版電子証明書を扱うために必要な利用者ソフトウェアもあわせて開発した。ここでは，これらの商業登記に基づく電子認証を実現するために必要なシステム構築技術について述べる。

2 商業登記制度に基づく電子認証制度

法務省の電子証明書を扱うにあたって，登録申請から電子証明書を取得するまでの手順について述べる（**図1**）。電子証明書を取得しようとする企業は，その法人代表者が専用の利用者ソフトウェアを使って公開鍵（かぎ）と秘密鍵のペアを作成する。この作成した公開鍵と法人の商号，住所，代表者資格，代表者氏名，電子証明書の証明期間などを3.5

（注1）　行政を効率化し国民負担の軽減を図るため，申請届出手続きや政府調達など，行政手続きの電子化を実現するシステム。

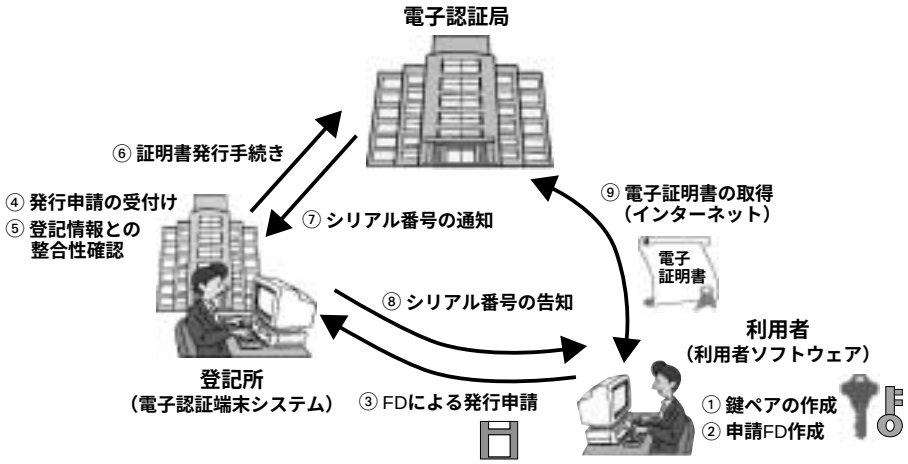

図1．証明書を取得する仕組み　登録申請から電子証明書を取得するまでの仕組みを示す。
Electronic authentication scheme based on commercial register

インチフロッピーディスク（以下，申請FDと略記）に保管し，管轄の登記所へ提出する。

一方，登記所では当社が開発した電子認証端末システムで，各企業からの登録申請を受け付け，あらかじめ登記されている“会社の登記情報”と“申請情報”の整合性を確認し，内容に不備がないことを確認したうえで電子認証局に申請情報を送信する。

電子認証局は，申請情報に基づき，電子証明書及び電子証明書を特定するためのシリアル番号を発行する。申請者は，インターネット環境で，シリアル番号を元に電子証明書を取得することになる。この電子証明書と，署名（秘密鍵による暗号化）した取引文書は，電子認証局に届け出た公開鍵を利用して，セキュアなECに不可欠な身元確認や取引データの改ざん防止が実現できる。

通常，認証局は自身の信頼性を確保するために，その上位に位置する認証局に信頼性を保証してもらうが，今般の法務省が構築する電子認証局は，この最上位に位置するルート認証局となっている。また，公開鍵暗号方式のアルゴリズムには，現在もっとも一般的に用いられているRSA（Rivest−Shamir−Adleman）方式が採用されており，その強度を決定する“鍵のビット長”は，1,024ビットと2,048ビットが採用されている。鍵の安全性と暗号処理の性能はシステムとして重要であり，楕円（だえん）曲線暗号など，他のアルゴリズムの採用が今後予想される。強度においても，ビット数が多ければ多いほど解読困難と一般的に言われており，処理性能を配慮しながら選択する必要がある。公開鍵暗号方式による認証の仕組みは，様々な文献で紹介されているので，ここでは説明を割愛する。

3　電子認証端末システム

法務省が発行する電子証明書を取得するには，申請情報を指定の記録方式でFDに保管し，管轄の登記所へ申請手続きを行う必要がある。ここでは，全国の登記所へ配備される申請受付端末“電子認証端末システム”について述べる。

3.1　申請磁気ディスクの記録方式

電子証明書を取得しようとする企業は，後述の利用者ソフトウエアを用いて申請FDを作成する必要がある。申請FDの仕様については，法務省のホームページに掲載されている。

3.2　署名の検証

まずは，前述した電子証明書の取得手順を思い出していただきたい。法務省へは利用したい側がみずから鍵ペアを作成し，公開鍵だけを証明用に申請することになる。このことは，利用者にとって秘密鍵を認証局にすら公開しないことで秘匿性を高められるとともに，認証局が秘密鍵を知り得ない立場としての中立性を保つという面を持つ。

しかしながら，これでは認証局側で公開鍵データが事実有用であるかを確認する方法がないことも意味する。このため，申請FDには電子署名を付与し，署名検証（届けようとしている公開鍵で復号できることを検証）することで，その公開鍵の有用性を確認している。

3.3　登記情報とのチェック

法務省の電子証明書は，商業登記に基づく電子証明書であり，この電子証明書の記載事項は商業登記簿の記載事項と合致していなければならない。そのために申請受付時には，申請FDに利用者が記載してきた情報と商業登記簿のマッチング検査を行う必要がある。ここで問題となるのが外字の扱いである。

商業登記簿は本店住所，代表者氏名などを扱うために，JIS第1，第2水準では規定されない文字が，Microsoft® Windows®(注2)の外字領域をはるかに超えて登録されており，なおかつ，その領域を有効に活用するために，商業登記独自の方式で外字が格納されている。しかし，汎用的な利用

（注2）　Microsoft，Windowsは，米国Microsoft Corporationの米国及びその他の国における登録商標。

が要件である電子証明書の日本語記述は，JIS第1，第2水準としなければならない必要があった。このため，申請FDには登記簿に記載されている外字を，便宜上，類似の漢字，又はかたかなに置き換えて申請を行うこととされている（例えば，“ 真 ”という外字を“ 真 ”に置き換えて申請すること）。

受け付ける情報は，字形が同じに見えても違う文字である可能性があるため，電子認証端末システムには，商業登記情報とJIS第1，第2水準との文字列のマッチング検査をする機能を付与し，問題点を解消している。

4 利用者ソフトウェア

4.1 電子証明書のフォーマット

認証局が発行する電子証明書を扱うには，電子証明書の方式を理解し取り扱う必要がある。証明書のフォーマットはITU−T（International Telecommunication Union−Telecommunication）のX.509という規格で標準化が成されている。X.509にはバージョン1，2，3があり，バージョン2では認証局及び被認証局の識別子が拡張され，バージョン3ではエクステンションという概念が導入されている。エクステンションは，証明書の使用目的など，アプリケーションソフトウェアが固有に定義できる領域であり，法務省では，登記情報に基づいている部分について，このエクステンションを利用している（**図2**）。

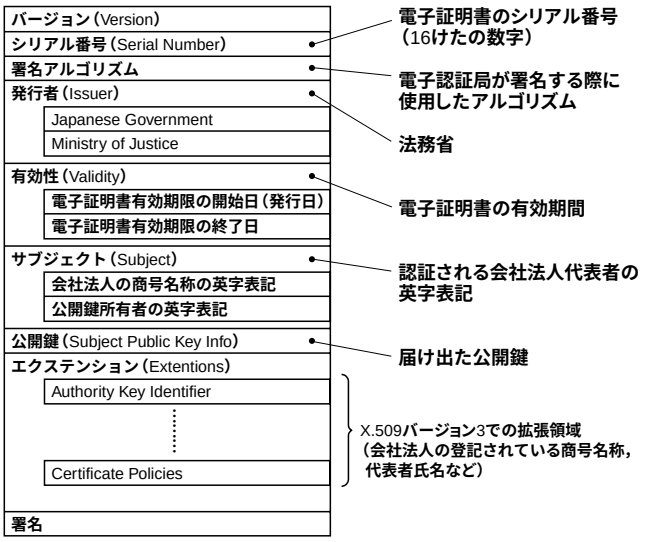

図2．法務省が発行する電子証明書　法務省電子認証局が発行する電子証明書のフォーマットを示す。
Format of electronic register

4.2 利用者ソフトウェアの機能

当社が開発した利用者ソフトウェアは，一般企業が法務省電子認証局の発行する電子証明書を利用して，ECを実現するために必要な一連の機能を提供する。利用者ソフトウェアは，利用者の入力した乱数を基にして，公開鍵と秘密鍵のペアを作成する。乱数を与えることで，より予測の困難な鍵ペアができるよう設計されている。ここで作成した公開鍵を所轄の登記所に提出する。その後の手順は前述のとおりである。

電子認証局にはインターネットで接続し，シリアル番号を指定して電子証明書を取得する。この際，通信プロトコルはHTTP（HyperText Transfer Protocol）で行い，送受信電文はASN.1（Abstract Syntax Notation One）で定義されている。これらの仕様についても，法務省ホームページに掲載されている。

電子認証局から送信される電子証明書は，共通鍵で暗号化されており，更に，この共通鍵は利用者の公開鍵で暗号化されているため，対応する秘密鍵の持ち主（すなわち，利用者本人）にしか復号化できない仕組みになっている。

電子証明書の取得後は，取引きに用いる電子文書へ電子署名を行い取引先へ送信する。取引先は，電子署名を検証し，添付されている電子証明書の有効性で，電子文書の改ざんや，なりすましがないことを確認する。

電子証明書の有効性の確認は，通常，電子認証局で一定期間ごとに更新されるCRL（Certificate Revocation List）と呼ばれる失効リストを検索して行うが，法務省の電子認証局ではOCSP（Online Certificate Status Protocol）と呼ばれる方式で，即時に電子証明書の有効性を確認できるようになっている。市販のメールソフトウェアの中には，電子証明書のフォーマット中に，電子メールアドレスがあることを前提としているものがある。使用するブラウザやメールのソフトウェアによっては，電子署名の機能が実現できないこともあるため，使用にあたっては十分注意が必要である。

4.3 他のアプリケーションシステムとの互換

利用者ソフトウエアでは，アプリケーションソフトウエア間の相互運用を図るため，作成した鍵や，取得した電子証明書を他のソフトウェアでも利用できるように，PKCS（Public-Key Cryptography Standard）#12フォーマットでのインポート／エクスポートを可能としている（**図3**）。PKCSは，現在PKCS#1から#15までの規約がある。その中でも，PKCS#12は，主にアプリケーションシステム（以下，アプリケーションと略記）間で電子証明書や秘密鍵を受け渡す際に利用されるフォーマットの規定が定められている。鍵や電子証明書がパスワードなどで保護された形式で保管される規定となっているため，アプリケーション間で安全に受け渡すことができる。ただし，このPKCS#12での入出力においても，複数の秘密鍵や複数の証明書を同時に格納することが可能となっているため，アプリケーション間でやり取りするには，どの鍵を扱う仕様としているのかを事前に確認する

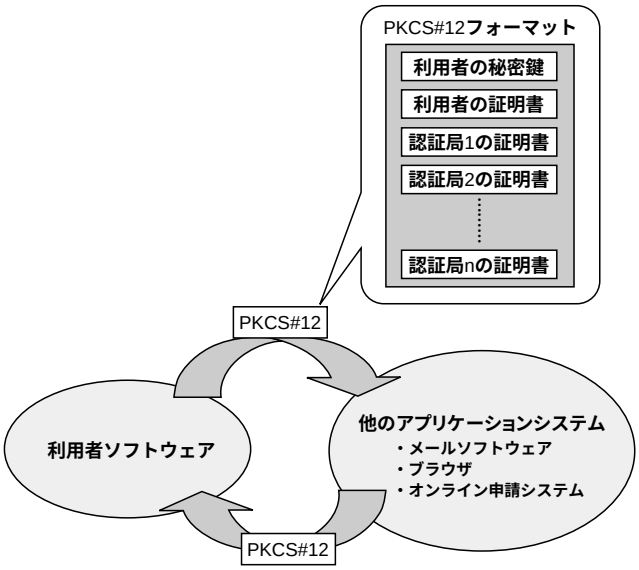

図3．PKCS#12の構造　秘密鍵と証明書をアプリケーションシステム間でやり取りする規定を示す。
Structure of PKCS#12

必要がある。

5 あとがき

商業登記制度に基づく電子認証制度を支援するために，当社が開発したシステムについて述べた。2001年4月から電子署名法が施行され，今後ますます電子認証システムのニーズが高まることが予想される。法務省では，既に，債権譲渡の登記申請をインターネットで受け付けるサービスを開始しており，このオンライン申請には，登記官が発行する電子証明書を添付することとされている。当社としても，暗号技術の高度化，ISO15408などのセキュリティ基準，本人認証技術，耐タンパ技術，暗号技術，認証技術など様々な技術の動向を見据えながら，官公庁業務を支援するシステムの開発を行う所存である。

また，商業登記に基礎を置く電子認証制度の啓蒙（けいもう），普及活動もさることながら，行政手続きの電子申請化，電子政府の実現に向けても努力していきたい。

文　献

⑴　新保　淳，ほか．暗号技術と鍵回復システム．東芝レビュー．**54**，7，1999，p.8－11.

⑵　R.L.Rivest, et al. A method for obtaining digital signatures and public key cryptosystems. Communications of the ACM. **21**, 2, 1978, p.120－126.

黛　　博之　MAYUZUMI Hiroyuki
e-ソリューション社　官公情報システム事業部　官公情報システム技術第一部主務。官公庁向け情報システムの開発に従事。
Government & Public Corporation Information Systems Div.

神田　　敦　KANDA Atsushi
e-ソリューション社　官公情報システム事業部　官公情報システム技術第一部。官公庁向け情報システムの開発に従事。
Government & Public Corporation Information Systems Div.

河本　高文　KOMOTO Takafumi
e-ソリューション社　東京システムセンター　官公システム第一部主務。官公庁向け情報システムの開発に従事。情報処理学会会員。
Tokyo System Center