特定認証業務対応 PKI/IC カード発行システムとその利用

Authentication Service Smart Card Issuing System for Public Key Infrastructure and Its Application

鈴　　貴子　　能勢　健一朗　　北井　富士夫

■ SUZU Takako　■ NOSE Ken-ichiro　■ KITAI Fujio

特定認証業務は，電子署名法にのっとり個人を証明する信頼性の高い電子証明書発行を行う業務を指し，政府の電子入札や電子申請，民間の電子契約書などのアプリケーションに使われる。

東芝では，特定認証業務に対応したPKI（Public Key Infrastructure）/IC カード発行システムTARGUSYS$_{TM}$を開発し，高度な信頼性が要求される認証システムの構築サービスを展開した。

An authentication service issues highly reliable digital certificates that serve as a means of personal identification in digital systems. They are used by the Japanese government for electronic bidding and other electronic applications, and by private enterprises for electronic contracts, etc.

Toshiba has developed a smart card issuing system corresponding to the Japanese government's TARGUSYS$_{TM}$ system. This smart card issuing system offers a highly reliable certificate service.

1 まえがき

日本政府は，1999年12月にミレニアムプロジェクトを発表し，2001年1月にスタートしたe-Japan戦略は電子政府，電子自治体に向けて急速に進展してきており，現在様々な中央省庁・地方自治体で行われている電子入札の実験や検証はいよいよ終盤を迎えている。

国土交通省の電子入札もその一つであり，1年の試行期間を終え2003年4月から本格運用に入っている。

電子入札においては，安全な取引きを行うためのセキュリティ確保がなによりも重要であり，入札参加企業を認証するとともに，入札価格を含む申請情報に電子署名を付加し，送信データの秘匿や第三者による改ざん防止及び通信相手の確認を行う必要がある。

このため，民間認証局が入札企業に対し電子証明書を発行するためには，政府が運営する政府認証基盤（GPKI：Government PKI）と相互認証を行う必要があり，入札企業に電子証明書を発行する民間認証局は，社会的にも高度な信頼性が求められ，特定認証業務のみがこれを行うことができる。

当社では特定認証業務対応PKI/ICカード発行システムを開発したので，そのシステムの概要と応用例について述べる。

2 特定認証業務

電子署名法（正式名：電子署名及び認証業務に関する法律施行規則）は2001年4月に施行され，主に以下の二つの意味を持った法律となっている。

⑴　電磁的記録（電子文書など）は，本人による一定の電子署名が行われているときは，真正に成立したものと推定する（手書き署名や押印と同等に通用する法的基盤を整備する）。

⑵　認証業務（電子署名が本人のものであることなどを証明する業務）に関し，一定の基準（本人確認方法など）を満たすものは国の認定を受けることができることとし，認定を受けた業務についてその旨表示することができる。また，認定の要件，認定を受けた者の義務などを定める（認証業務における本人確認などの信頼性を判断する目安を提供する）。

電子署名法における特定認証業務とは，⑵の本人確認方法が一定の基準を満たした認証業務を行う機関として，主務三大臣（総務省，法務省，経済産業省）から認定を受けた認証業務である。

特定認証業務として認定を受けるためには，主に以下の要件を満たす必要がある。

⑴　業務に関する要件

ⓐ　認証局の目的が適正

ⓑ　運営体制の明確化

ⓒ　手続きが明確かつ適正

ⓓ　他の業務から分離

⑵　設備に対する要件

ⓐ　認証業務室の鍵管理

(b) 認証業務室の入退管理設備
(c) 隔離設備の設置
(3) IT(情報技術)システムに関する要件
(a) 秘密情報の消去に対する完全性の保証
(b) 操作者に関する履歴の保存と完全性の保証

これらの要件をすべて満たし，日本品質保証機構(JQA)による書類審査，実地調査にて問題がないと判断されると，主務三大臣から特定認証業務として認定を受けることができる(**図1**)。

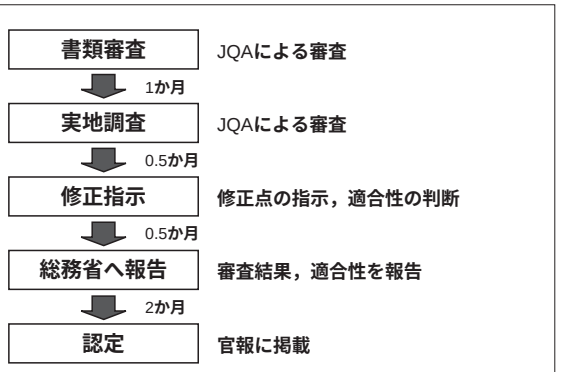


図1．特定認証業務認定の流れ ― 認定に最低でも3か月が必要である。
Authorization flow of authentication service

3 PKI/IC カード発行システム TARGUSYS$_{TM}$

当社のPKI/ICカードシステムTARGUSYS$_{TM}$(ターガシス)は，利用者本人を認証するために電子証明書をPKI/ICカード(TARGUSYS$_{TM}$カード)へ格納する一括発行システムである。

最大5組の電子証明書と秘密鍵を格納でき，ネットワークへのログオンやWeb認証，暗号メールなど様々な用途に利用可能である。

また，同時にMicrosoft®Windows®(注1)2000スマートカードログオンにも対応しており，確実な本人認証が可能なICカードとして，官公庁の職員証，民間企業の従業員証，又は身分証明書として利用することができる。

TARGUSYS$_{TM}$は，主に統合管理サーバとICカード発行機から構成される。

統合管理サーバは，秘密鍵と公開鍵の生成，認証局システムと連携した電子証明書の一括発行，ICカード発行データの作成を行う。

ICカード発行機では，秘密鍵と公開鍵，及び電子証明書のICカードへの格納のみならず，券面印刷も行うことができ，通常のプリンタで印字するように簡単にICカードを発行することができる。

PKI/ICカードを導入した場合，カードの紛失や電子証明書の失効や更新などに伴う運用業務が予想以上に管理部門の負担となる。

TARGUSYS$_{TM}$は統合管理サーバによるユーザーの情報，秘密鍵，電子証明書などを一元管理しているため，みずからの手で即座にICカードを発行することができ，ICカードの緊急発行や再発行，電子証明書更新も簡単に行うことができる(**図2**)。

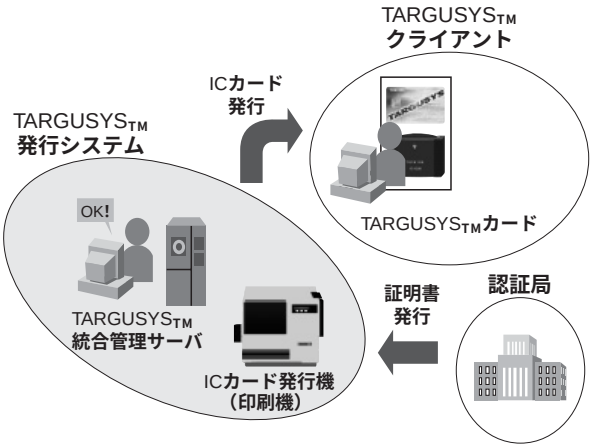


図2．PKI/IC カード発行システム TARGUSYS$_{TM}$ ― 統合管理サーバでユーザー情報が一元管理され，認証局と連携してICカードの一括発行が可能となっている。
TARGUSYS$_{TM}$ smart card issuing system

4 特定認証業務対応 PKI/IC カード発行システムと応用例

TARGUSYS$_{TM}$の機能として，特定認証業務の要件のうちITシステムに関する要件を満たすために，今回，主に以下の機能を実装した特定認証業務対応のPKI/ICカード発行システムTARGUSYS$_{TM}$を開発した。

(1) ユーザー秘密情報(個人情報，秘密鍵情報，ICカードの暗証番号(PIN)の別管理機能
(2) 米国国防総省 DoD5220.22-M準拠方式による，ユーザー秘密情報の完全削除機能(秘密情報の消去に対する完全性の保証)
(3) ICカードのPINを操作者が閲覧できないように自動封入封かんプリンタの導入，及びPIN印刷機能
(4) 操作者用ICカードによるユーザー認証機能(操作者に関する履歴の保存と完全性の保証)
(5) 操作者の操作履歴機能(操作者に関する履歴の保存と完全性の保証)

また，特定認証業務対応PKI/ICカード発行システムだけ

(注1) 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。

でなく，インターネットからの電子証明書申込みがオンラインで可能な申請受付Webサーバ，本人確認のための審査・承認を行う管理Webサーバなどの開発も併せて行い，ASP（Application Service Provider）システムも含んだ特定認証ICカード発行のトータルシステムを実現した。

以下に特定認証業務対応のPKI/ICカード発行システムTARGUSYS™を応用したトータルシステムの例として，申請者が電子証明書の申込みを行い，ICカードを受け取るまでの概略の流れについて述べる（**図3**）。

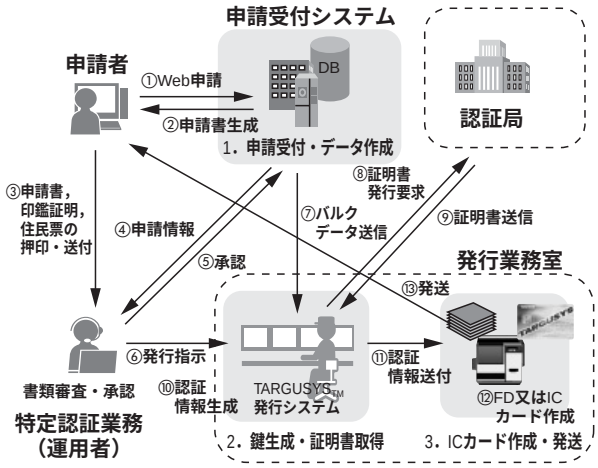


図3．特定認証PKI/ICカード発行システム ― 申請受付システム，認証システム，ICカード発行システムなど，特定認証業務としてのトータルなシステムを提供する。

Authentication service smart card issuing system

⑴　申請者によるオンライン申請　　申請者は，電子証明書の利用申込みを行う場合，電子証明書を発行する認証局のWebページにアクセスし必要事項を入力する（①）。

⑵　申請書の郵送　　入力データを確認後，申請フォームが作成されるので，それを印刷して申請書の原紙とし，本人確認用の書類（住民票，印鑑登録証など）を添付して郵送する（②，③）。これらの作業は，一般のブラウザから利用できるので，操作がとても簡単である。

⑶　特定認証業務による審査・承認　　特定認証業務向けに，申請者が入力した情報をもとに本人確認のための審査・承認を行うことができる。特定認証業務に対応したワークフローを導入することにより，膨大な書類を入力処理する必要もなくなり，処理の軽減を図ることが可能となる（④，⑤）。

⑷　ICカードの発行　　特定認証業務の発行指示のもと，特定認証業務対応のICカード発行システムTARGUSYS™では，統合管理サーバで秘密鍵と公開鍵の生成，認証局からの電子証明書の取得，ICカードPINの印刷を行い，ICカードを発行する（⑥～⑫）。

なお，ICカード発行業務を行う発行業務室においては，生体認証装置（身体的特徴を識別する装置）で認証された作業者のみが入室を許される。

また，発行作業自体も発行業務担当者二人以上による内部牽制（けんせい）を行うなかで実施され，データ改ざんなどの不正アクセス防止の措置を施している。

⑸　ICカードの発送　　発行されたICカードは本人限定郵便にて，ICカードPINは書留郵便にて本人に直接送付される（⑬）。

このような申請受付・承認ASPトータルシステムを実現することにより，従来1か月ほどかかっていた発行サイクルも，約2週間程度に短縮することが可能となった。

5　GPKIと電子入札システム

政府が運営する政府認証基盤GPKIと，2001年4月から施行された電子署名法とは密接に連携しており，99年12月に政府が発表した“ミレニアム・プロジェクト”において，「政府認証基盤（GPKI）の各省庁の認証局を相互に接続するためのブリッジ認証局のシステム構築を行うとともに，各省庁は認証局（CA：Certificate Authority）を構築する」としている。

2003年4月末の時点では，11省，3庁において認証局が構築され，ブリッジ認証局との相互接続が既に完了している。

GPKIとしてのシステムは，ブリッジ認証局と各省庁が運営する府省認証局から構成され，ブリッジ認証局は，府省認証局との相互接続，及び民間認証局などの政府認証基盤外の認証局との相互認証を行い，府省認証局は，行政手続きの処分権者の官職を認証するとともに，ブリッジ認証局との相互認証を行う。

また，電子署名法による特定認証業務の認定を受けた民間認証局については，2003年4月末の時点では5社がブリッジ認証局との相互接続が完了しており，電子政府に対応した電子証明書を発行している。

これにより，各府省に対する申請，手続きを従来の書類によるものではなく，電子申請，電子入札などの電子政府を利用した各種手続きを電子署名で署名した形で行えるようになった。

今後は更に民間認証局の相互接続が予定されており，申請者はそれぞれの認証局から認証されることで，電子政府に対応した電子証明書が発行され，電子政府を利用した各種手続きが加速することが予想される。

これらGPKIによるブリッジ認証局を介した府省認証局と民間認証局の相互接続を利用した電子入札システムの一つに，国土交通省の電子入札システムがある。

国土交通省では，工事及び建設コンサルタント業務などに

おいて，2003年4月から電子入札を全面的に実施した。

2003年度からの電子入札は，複数の認証局から発行されるICカードに対応し，これまでの電子入札システムの機能向上を図るため，新システム（新電子入札コアシステム）を導入している（**図4**）。

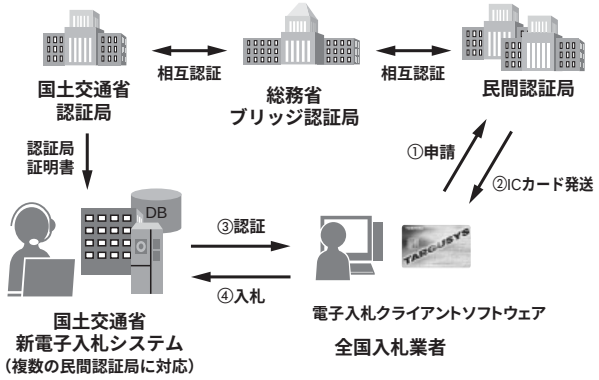


図4．GPKIと電子入札システム— GPKIのブリッジ認証局と民間認証局とが相互接続することにより，民間認証局が発行したICカードで政府が運営する電子入札システムを利用することができる。

Government public key infrastructure (GPKI) and electronic bidding for Japanese government

新電子入札コアシステムは，日本建設情報総合センター（JACIC）がとりまとめている汎用性の高い電子入札システムであり，国土交通省だけでなく，他の府省や地方自治体の一部も導入を検討している。

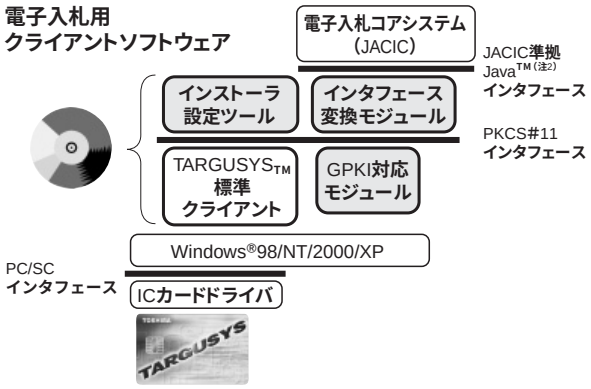
新電子入札コアシステムの特長は，複数認証局に対応していることであり，申請者は新電子入札システムに対応した一か所の認証局から電子証明書を発行してもらうことで，新電子入札コアシステムを導入したシステムであれば，国土交通省だけでなく様々な電子入札システムで利用できる。

なお，今回の特定認証業務対応PKI/ICカード発行システムTARGUSYS$_{TM}$の開発では，新電子入札システムに申請者が利用する，電子入札クライアントソフトウェアも新たに開発した。

これはPKI/ICカード発行システムTARGUSYS$_{TM}$の標準クライアントソフトウェアをベースにし，JACIC準拠のインタフェースを実装することにより，新電子入札コアシステムに対応した電子入札クライアントソフトウェアとなっている（**図5**）。

6 あとがき

今回開発した特定認証業務対応のPKI/ICカード発行システムTARGUSYS$_{TM}$は，e-Japan戦略により急速に進展して



PKCS：Public Key Cryptography Standards
PC：パソコン　SC：Smart Card

図5．電子入札用クライアントソフトウェア— TARGUSYS$_{TM}$標準クライアントを利用し，JACICに準拠したインタフェース機能，GPKIに対応した機能，設定ツールなどを追加することにより，電子入札用クライアントソフトウェアを開発した。

Electronic bidding client software

きた電子政府，電子自治体に向けた電子入札用ICカード発行システムの一つのソリューションであり，その設備のほとんどをデータセンターで運用する業務形態を可能としている。

これにより，TARGUSYS$_{TM}$は単なるICカード発行システムにとどまらず，データセンター向けのセキュリティサービスの一つであると言える。

今後，急速に普及するであろう地方自治体などの電子申請や電子入札，更には民間企業のBtoB（企業間）取引に関連したデータセンター企業などに対し，こうしたシステムとともに特定認証認定のノウハウを提供するサービスを行っていく。

文　献

(1) 能勢健一朗，ほか．PKI構築サービスとPKIカードシステムTARGUSYS$_{TM}$．東芝レビュー，**56**，7，2001，p.34－37.

（注2） Java及びその他のJavaを含む商標は，米国Sun Microsystems社の商標。

鈴　貴子　SUZU Takako

e-ソリューション社 プラットフォームソリューション事業部 プラットフォームソリューション第三担当主務。情報セキュリティ技術の開発に従事。

Platform Solutions Div.

能勢　健一朗　NOSE Ken-ichiro

e-ソリューション社 プラットフォームソリューション事業部 プラットフォームソリューション第三担当主務。情報セキュリティ技術の開発に従事。

Platform Solutions Div.

北井　富士夫　KITAI Fujio

e-ソリューション社 プラットフォームソリューション事業部 ソフトウェア開発担当主務。情報セキュリティ技術のソフトウェア開発に従事。情報処理学会会員。

Platform Solutions Div.