

# 高カスタマイズ性・高信頼性を実現した ジャパンネット認証局運用システムソリューション

## 要 旨

インターネットの普及や電子商取引市場の拡大等により、ネットワーク上での安心・安全な情報交換が求められている。それには通信相手の本人確認や通信内容の真正性確認が必要となるが、その有効な手段として暗号技術を応用した電子認証・電子署名がある。この際に必要となるものの一つに公開鍵基盤(PKI:Public Key Infrastructure)に基づいた電子証明書がある。

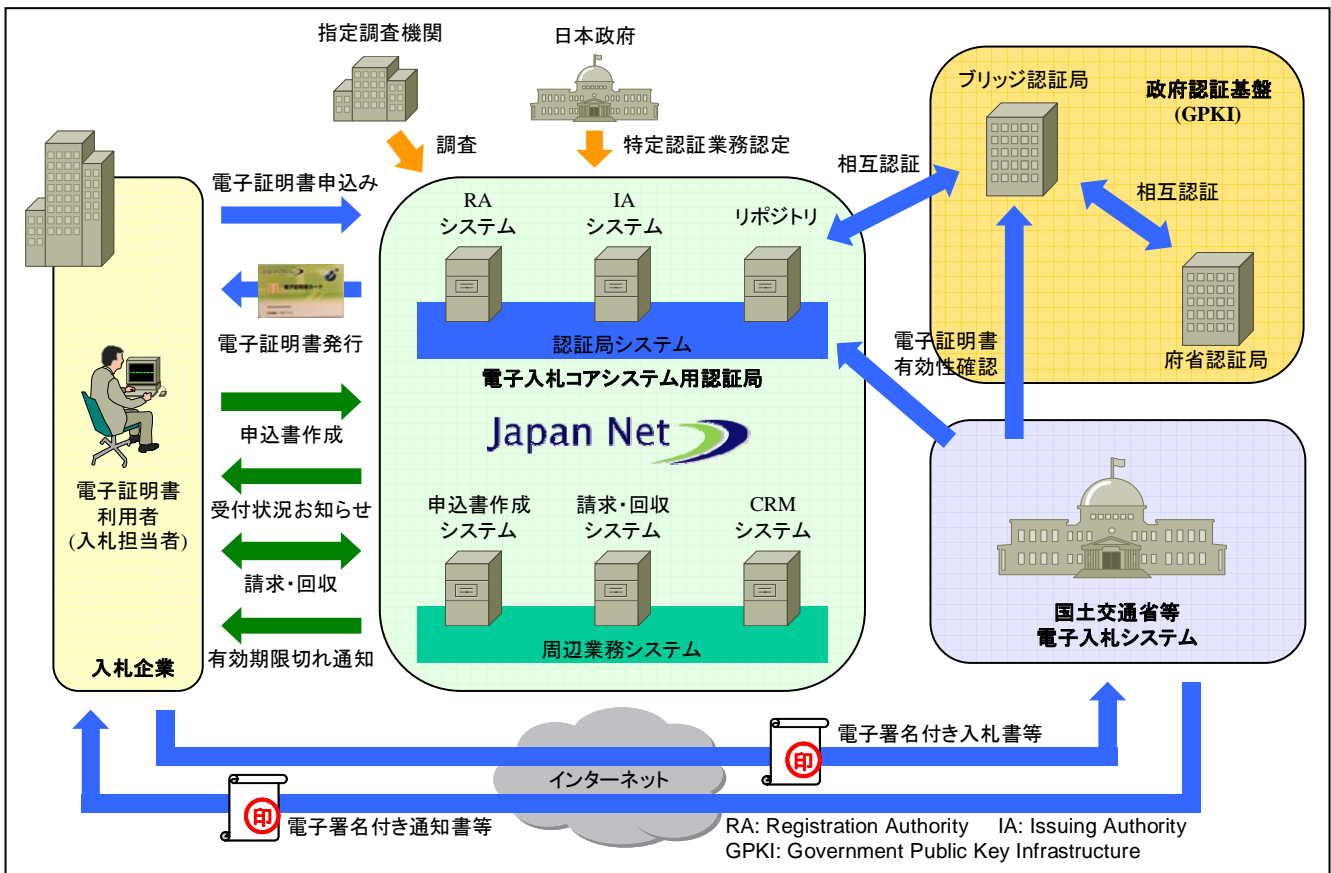
電子証明書の利用には、それを発行するための認証局が必要となるが、電子証明書の信頼性は認証局の信頼性に依存している。そのため、高いセキュリティや厳格な運用による信頼できる認証局が必要とされる。

ジャパンネット株式会社(Japan Net)では、2003年4月より”電子入札コアシステム用電子認証サービス”を開始し、このための認証局を運用している。これは電子署名及び認

証業務に関する法律(電子署名法)に基づく特定認証業務の認定を受けたサービスであり、その厳格な認定基準を満たす認証局運用規程(CPS:Certification Practice Statement)に従った運用を行っている。

この運用を支える認証局運用システムには2つの特長がある。一つ目は認証局システムだけでなく周辺業務システムも含み、カスタマイズ性が高いこと。二つ目は、信頼できる認証局実現のための運用支援機能が組み込まれていることである。

Japan Netでは、この運用ノウハウ・運用システムを顧客の認証局構築や運用アウトソーシングに生かし、信頼できる電子認証サービスの提供を通じて企業・社会の発展に寄与していく所存である。



## 電子入札コアシステム用電子認証サービス

電子入札コアシステム用電子認証サービスの運用を支えるジャパンネット認証局運用システムソリューションは、信頼できる認証局を実現する認証局システムと、認証局システムに連携する周辺業務システムからなる認証サービスのトータル運用システムソリューションである。

## 1. ま え が き

インターネットの普及や電子商取引市場の拡大等により、ネットワーク上での安心・安全な情報交換が求められている。それには通信相手の本人確認や通信内容の真正性確認が必要となるが、その有効な手段として暗号技術を用いた電子認証・電子署名がある。この際に必要となるものの一つにPKIに基づいた電子証明書がある。電子証明書の利用には認証局が必要であり、電子証明書の信頼性確保のためには信頼できる認証局の構築・運用が必要となる。

## 2. 認証局

認証局は電子証明書の発行・管理・失効を行なうための機関である。また、電子証明書とは公開鍵暗号方式による公開鍵とその利用者情報に対して認証局が電子署名し、ITU-TのX.509規格に従い電子データ化したものである。

電子認証・電子署名は公開鍵暗号方式による鍵ペア(公開鍵・秘密鍵)によって行なう。しかし、この時に入手した公開鍵が本当に情報交換する相手のものであるかの確認が必要となる。電子証明書の発行において認証局は利用者と公開鍵の結びつきを証明する役割を負っている。そのため、電子証明書では電子署名から認証局が発行したことを検証することで、公開鍵が利用者情報に記載された人のものだと信頼できる。(図1)

また、認証局の発行した電子証明書を信頼するためには、認証局自体が信頼できるものである必要がある。このため、認証局はRFC2527またはRFC3647に従った証明書ポリシー(CP:Certificate Policy)と認証局運用規程(CPS)を規定し、これに従った業務を遂行している。CPでは発行する電子証明書の目的や利用用途を規定する。CPSではCPを実現するための認証局運用を規定する。

認証局は登録局(RA)と発行局(IA)から構成されている。RAは利用者の本人確認や発行に必要なデータ登録を行なう

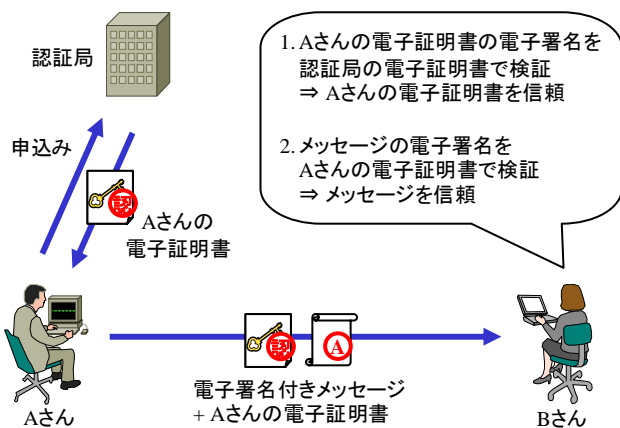


図1. 認証局の役割

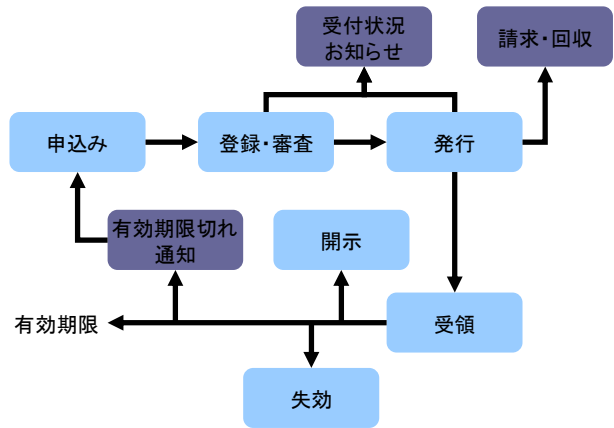


図2. 電子証明書ライフサイクル

機関である。IAはRAにより本人確認・登録が完了したデータをもとに電子証明書の発行を行なう機関である。

## 3. 認証局運用

ジャパンネット株式会社(Japan Net)の”電子入札コアシステム用電子認証サービス”は公共機関の電子入札に参加する際に必要となる電子証明書を発行するサービスである。Japan Netではこのための認証局を運用している。

このサービスは電子署名法の規程に基づき総務大臣・経済産業大臣・法務大臣から認定を受けた特定認証業務である。このため、CP/CPSや認証局運用システムは省令で定められた厳格な認定基準を満たしている。それだけでなく、毎年行われる更新認定の際には、指定調査機関による運用状況の厳格な調査が行われている。また、この認証局は政府認証基盤のブリッジ認証局と相互認証している。

ここでは電子証明書のライフサイクル(図2)に従い、このサービスの運用を紹介する。なお、この運用は単独操作で発生し得る不正行為等を防止するため、表1の体制に要員と役割を分離し、相互牽制により単独操作を防止している。

### 3.1 電子証明書の申込み

申込みには、申込書と印鑑登録証明書や商業登記簿謄本など4~6種類の公的機関が発行した証明書類をRAに郵送する必要がある。

従来、申込書は手書きでの作成が必要であった。しかし、2007年6月より申込書作成システムを導入し、Web画面上で申込情報を入力しての申込書作成が可能となった。

### 3.2 申込みの登録と審査

郵送されてきた申込書に対し、RAで申込書内容の登録と申込みの審査を行なう。審査では複数の受付審査担当者により下記3点を確認し、確認結果をRAシステムに登録する。

(1) 申込書に必要事項が記載されているか

表1. 認証局運用体制

要員区分	主な役割
電子認証局代表者	電子認証局責任者の任命、解任
電子認証局責任者	CPSの策定、開示及び変更管理
審査登録業務責任者	受付審査担当者への作業指示及び結果確認
受付審査担当者	電子証明書申込に係る書類の受付及び審査
RA 操作員	利用者情報の登録
認証業務責任者	電子証明書の発行指示
IA 操作員	電子証明書の発行処理
システム保守員	認証局システムの保守点検

(2) 必要な証明書類が揃っているか

(3) 申込書と証明書類で記載内容や印影が一致しているか  
証明書類を用いた審査により、申込書に記載されている利用者本人からの申込みであることを確認している。これにより、利用者と後に作成する公開鍵との結びつきを認証局が保証できる。なお、審査で申込み不備が見つかった際には、申込者に連絡し訂正・再申込みを依頼する。

RAは専用の施錠管理された区画に設置されている。また、RAシステムはネットワークから切り離されている。

なお、電子証明書の発行記録保存のために、申込書と証明書類は電子証明書の有効期間満了後10年間保存している。審査後などに印刷される作業記録シートやRAシステムに登録された電子的な情報なども同様に保存している。

### 3.3 電子証明書の発行

電子証明書発行では、まずRAシステムで審査完了した申込みの証明書発行要求を生成する。証明書発行要求はIAに持込まれ、これに基づきIAシステムで公開鍵暗号方式の鍵ペアと電子証明書を作成する。作成した鍵ペアの秘密鍵と電子証明書はICカードに格納する。IAでの作業は複数操作員の相互牽制の下で行なわれる。

IAは認証局秘密鍵の存在する特にセキュリティが要求される場所である。このため、特別に区画され、生体認証による入退室管理やモーションセンサと監視カメラによる記録がなされる区画に設置されている。

電子証明書は利用者本人に確実に渡すよう日本郵政公社が提供する本人限定受取型郵便で送付する。この郵便物を受取るには、郵便局で運転免許証等の本人確認書類を提示する必要がある。

### 3.4 電子証明書の受領

利用者は電子証明書受取り後に、同封されている受領書に実印で押印し、返送する。受領書の返送をもって、認証局は電子証明者が利用者本人に渡ったことを確認する。認証局ではこのために以下3点を行なっている。

(1) 受領書返送がなされたことをRAシステムへ登録

(2) 電子証明書の発送後20日間受領書の返送がない場合、利用者に受領書の返送を督促

(3) 電子証明書の発送後30日以上受領書の返送がない場合、当該電子証明書の認証局による失効を実施

### 3.5 電子証明書の失効

電子証明書の紛失時等には利用者から失効申請が行なわれる。失効申請も電子証明書申込みと同様にRAで受け付け、審査が行なわれる。

審査を通過すると、RAで証明書失効要求を作成する。IAでは証明書失効要求から該当する電子証明書を証明書失効リスト(CRL:Certificate Revocation List)に追加し、リポジトリ上で公開する。電子入札システムは公開されているCRLを参照し、認証に利用された電子証明書が失効されていないことを確認する。

### 3.6 開示

RAに開示申請書が郵送されてきた場合、利用者本人からの申請であることを審査し、申込書・証明書類の写しと電子証明書記載事項の写しを本人限定受取郵便で送付する。

### 3.7 申込み受付状況のお知らせ

通常、電子証明書の申込みから発送までには1~2週間を要する。そこで、受付・審査・発行それぞれの完了時点で発送予定日を通知するメールを申込者に送信する。

### 3.8 請求・回収

電子証明書発行後にRAシステムから出力される発行情報に基づき、申込者に対して電子証明書料金の請求・回収を行なう。また、販売実績データの出力等も行なっている。

### 3.9 有効期限切れ通知

電子証明書には有効期間があり、その後も引き続き電子入札に参加するためには新規の電子証明書を申込み必要がある。そこで、有効期限切れの2ヶ月前にメールと郵送で通知し、有効期限切れにより利用者の業務に支障をきたさないようにしている。

## 4. 認証局運用システム

電子入札コアシステム用電子認証サービスの認証局運用システムの構成を図3に示す。このシステムは以下に述べる特長を持っている。

### 4.1 周辺業務サポートと高カスタマイズ性

この認証局運用システムには、認証局そのものだけでなく顧客管理や請求・回収などその周辺業務システムも含まれている。認証局そのものを構成するRAシステムやIAシステムに登録されたデータは、信頼できる認証局実現のため極めて厳格に管理される必要がある。このため、RAシステムやIAシステムと周辺業務システムが同じデータベースを利用する構成にはできない。

この対策として、本認証局運用システムではシステム間連携をCSVファイルにて行い、認証局システムと周辺業務

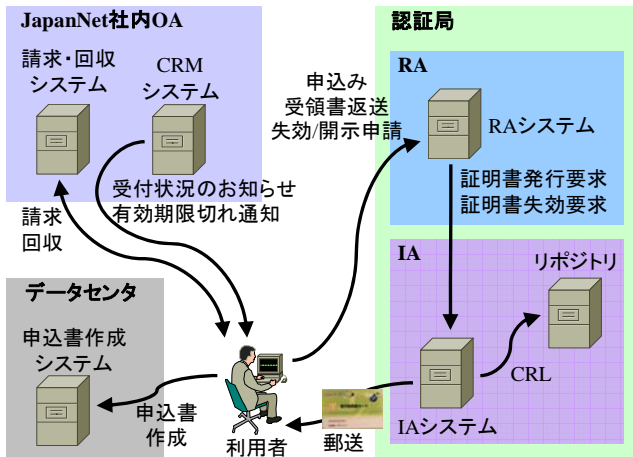


図3. 認証局運用システム

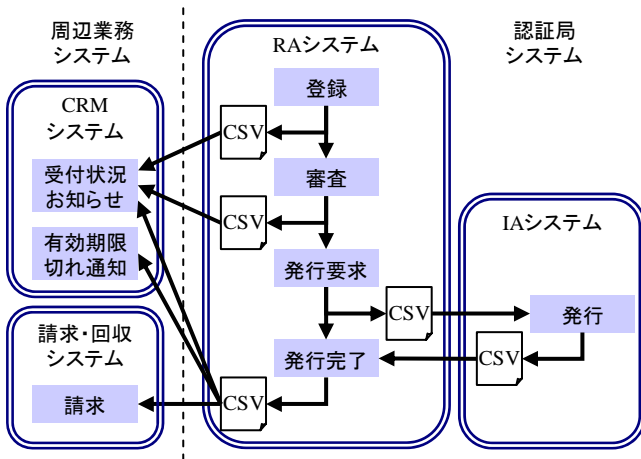


図4. CSVファイルによるシステム間連携

システム間では周辺業務システムによる読み込みのみを行っている(図4)。これにより、認証局システムと周辺業務システムが完全に分離され、認証局システムの登録データが周辺業務システムから保護される。同時に、本サービスのようにセキュリティ上の理由から認証局システムをネットワークから切り離れた運用が可能となる。

また、周辺業務システムと認証局システムの分離により、認証局システムとは独立して周辺業務システムの追加・変更が行なえる。このことにより、本認証局運用システムをベースとして顧客の認証局構築を行う際には、認証局システムの信頼性はそのままに顧客の必要とする周辺業務システムの追加に対応できる。

#### 4.2 信頼できる認証局実現のための運用支援

信頼できる認証局実現のために、CPSにおいては、運用手順だけでなくこれに対する管理・監視・保障のための手順が定められている。このために本認証局運用システムでは以下のことを行なっている。

(1) RAシステムでは作業毎に作業記録シートが印刷され

る。これに作業者のサインと責任者の承認印を残すことにより作業の管理を行なっている。

(2) データベースへの追加・変更やCSVファイル出力の際等に作業者名・作業日時を記録している。また、RAシステムではバックアップを毎日取得し、全世代保存している。これらにより、作業内容をトレース・監視できるようにしている。

(3) RAシステムではCPSに定めた運用手順に個々に対応した画面を用意している。これにより、運用手順外の操作ができなくなり正しく作業が行なわれることを保障している。

CPSの範囲外となる周辺業務システムにおいては、個人情報保護等のためのセキュリティ対策を行っている。請求・回収システムは社内イントラネット上で公開されているWebアプリケーションである。このシステムに対する認証・アクセス制御には、企業内の個人認証・サーバ認証用電子証明書を発行する”ジャパンネットスタンダード電子認証サービス Category2”の電子証明書をUSBトークンに格納して利用している。パスワード認証を採用した際にはパスワード漏洩や脆弱なパスワード使用などの危険性がある。しかし、電子証明書をを用いたSSL(Secure Sockets Layer)クライアント認証を採用することで、これらの危険性がないより強固なセキュリティを実現している。

## 5. むすび

電子証明書を利用しネットワーク上で安心・安全な情報交換を行うためには、信頼できる認証局の構築・運用が必要となる。本稿ではその具体的事例としてJapan Netの電子入札コアシステム用電子認証サービスにおける認証局の運用、及び運用システムについて述べた。

Japan Netでは、電子入札コアシステム用電子認証サービスで培った認証局の運用ノウハウ・運用システムを顧客の認証局構築や運用アウトソーシングに生かし、信頼できる電子認証サービスの提供を通じて企業・社会の発展に寄与していく所存である。

## 参考文献

- (1) 塚田孝則:企業システムのためのPKI - 公開鍵インフラストラクチャの構築・導入・運用, 日経BP社 (2001)
- (2) 村木克己, ほか:ユビキタスセキュアソリューション実現のための認証サービス, 三菱電機技報, 78, No. 4, 255~258 (2004)