電子入札コアシステム

証明書検証方式説明書

2008 年 1 月

目　　次

1　はじめに

電子入札コアシステム（以下「コア」又は「コアシステム」という。）では、応札者が使用する証明書や発注者が使用する証明書を、サーバ（AP サーバ、鍵管理サーバ）、クライアント（応札者クライアント、発注者クライアント）で検証する処理が存在します。証明書検証は、検証対象、検証する側の立場など、様々な要素によって採用すべき方式が変わります。

この資料は、コアシステムにおける電子署名と認証モデル（2 章）、各検証方式（3 章）、商業登記認証局対応での対処方法（4 章）、コアシステムが推奨する方式（5 章）を解説するものです。5 章では、採用すべき方式がわかるように、発注機関の分類別（中央省庁、地方自治体、その他の発注機関）に、応札者クライアント、発注者クライアント、サーバに対する推奨方式を記述しています。

2　電子署名・認証について

コアシステムは、インターネット上でのやり取りのみで、入札ができるようにしたシステムです。しかし、インターネットは、世界中に公開されたネットワークであり、完全に安全なものではなく、多くの脅威にさらされています。

そこで、コアシステムでは、考え得る危険に対して、様々な対策を講じており、その 1 つとして、PKI（公開鍵基盤：Public Key Infrastructure）を用いた電子署名技術を採用し、なりすましと改ざんを防いでいます。

2-1　PKIを用いた電子署名とは

秘密鍵と証明書（公開鍵証明書）は、公的に認められた民間認証局が発行する、いわば印鑑と印鑑証明書の代わりとなるものです。認証局は、個人を住民票等の公的書類の提出を持ってその個人を特定し、秘密鍵の所有者がその個人であることを証明書で保証します。この秘密鍵と証明書を用いて電子署名を行うことで、実文書に記名・押印したものと同じ効力を発揮するわけです。

発注機関（発注者）側においては、GPKI（政府認証基盤：Government Public Key Infrastructure）が認めた府省認証局の発行する官職証明書、LGPKI（地方公共団体組織認証基盤：Local Government Public Key Infrastructure）が認めた組織認証局が発行する職責証明書が存在します。これらは、個人（職員）を特定するものではなく、官職及び職責（役職）を特定する公印と同じようにして扱われます。

これまで紙の文書に記名・押印してやり取りしていたように、ネットワーク上で電子データをやり取りする際に、この秘密鍵と証明書を用いて電子署名を行います。コアシステムでは、応札者と発注者がやり取りする電子データのすべてに電子署名を行います。

これにより、下記のような、なりすまし、改ざんといった脅威を排除しています。

（1）なりすましを防ぐ（証明書の検証）

電子署名の付いた電子データを受け取った側は、その電子署名と電子署名を付けるために使用した（秘密鍵の対になる公開鍵の）証明書の検証を行います。証明書を検証することにより、その証明書が確かなものであるか、有効なものであるかが確認されます。使用者は、秘密鍵を安全に管理・使用するという義務を負いますが、「証明書が確かなものである」＝「送られてきたデータはその使用者が送ってきたものである」という証明がなされます。

第三者がこの使用者になりすましてデータを送ってきたとしても、同じ秘密鍵を使用しない限り、同じ電子署名を付けることができず、証明書の検証の結果、別人と判断されます。コアシステムの場合、秘密鍵は、証明書（公開鍵）とともに、IC カードに格納して認証局から発行されることを前提としておりますので、複数の同じ秘密鍵は存在せず、安全に IC カードを管理・使用している限り、第三者によるなりすましを防ぐことができます。

万が一、IC カードを盗難、紛失等した場合、早急に発行元の認証局に届け出ることが必要となります。認証局はその届出を受け取ると、証明書の失効処理を行い、その証明書が失効したという情報を公開します。この失効情報は、証明書の検証時に参照され、その IC カードを用いてなりすましを行おうとする第三者がデータを送ってきても、その証明書は無効である、と判断することができます。

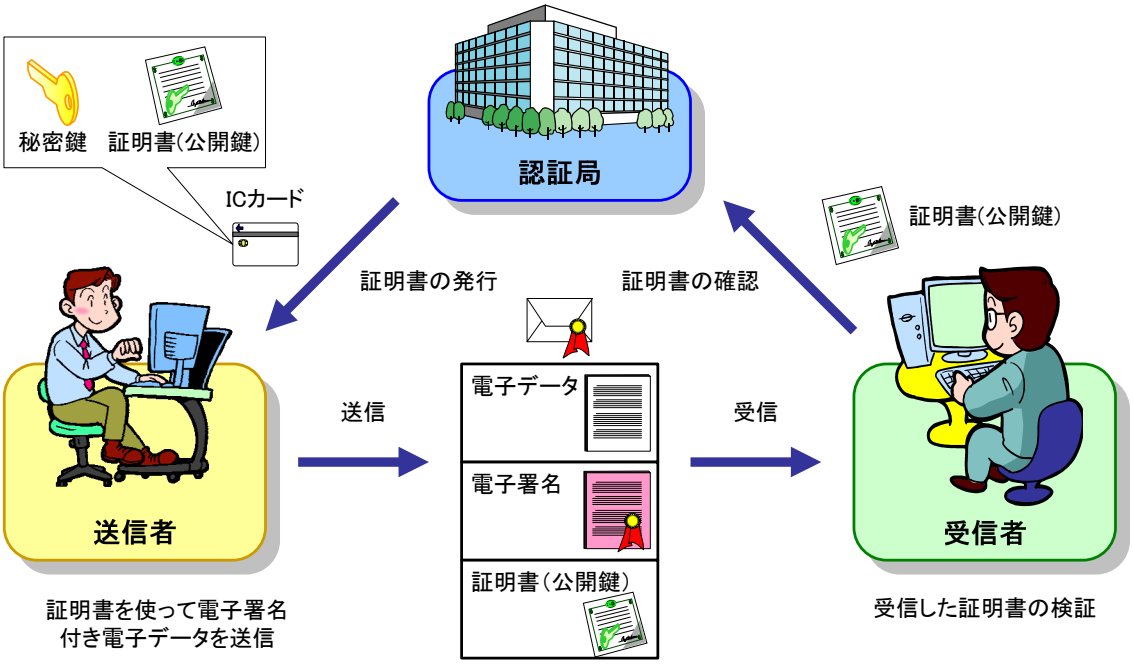

図 2-1　証明書の検証のイメージ

（2）改ざんを防ぐ（電子署名の検証）

電子署名は、電子署名を付けるべき電子データと秘密鍵から生成されます。受け取った側は、電子データ、公開鍵（証明書）、署名値（電子署名）の 3 つをチェックすることにより、このデータが途中で改ざんされていないかを確認することができます。電子データが改ざんされた場合は、改ざんされた電子データと電子署名をチェックすれば、改ざんが検出されます。さらに、改ざんされた電子データを基に新しい電子署名を付加された場合でも、電子署名と公開鍵（証明書）をチェックすれば、電子署名に使用されている秘密鍵が違うことがわかり、改ざんが検出できます。前項で記述したように、秘密鍵は、IC カード内に格納されています。同じ IC カード／秘密鍵は、複数存在しませんので、第三者に同じ電子署名を付けられることはなく、確実に改ざんを検出することができるのです。

コアシステムでは、通信途上の電子データだけではなく、受信した電子データをサーバに格納する時にも、電子署名が付いた状態で保存しています。データベース内に格納された情報は、外部からはアクセスできないようなネットワーク構成及び設定が行われているはずですが、内部では直接データベースにアクセスし、電子データを改ざんすることが可能です。そこで、コアシステムでは、データベースから電子署名付き電子データを取り出した際、再度、電子署名の検証を行い、内部での改ざんが行われていないかを検証しています。

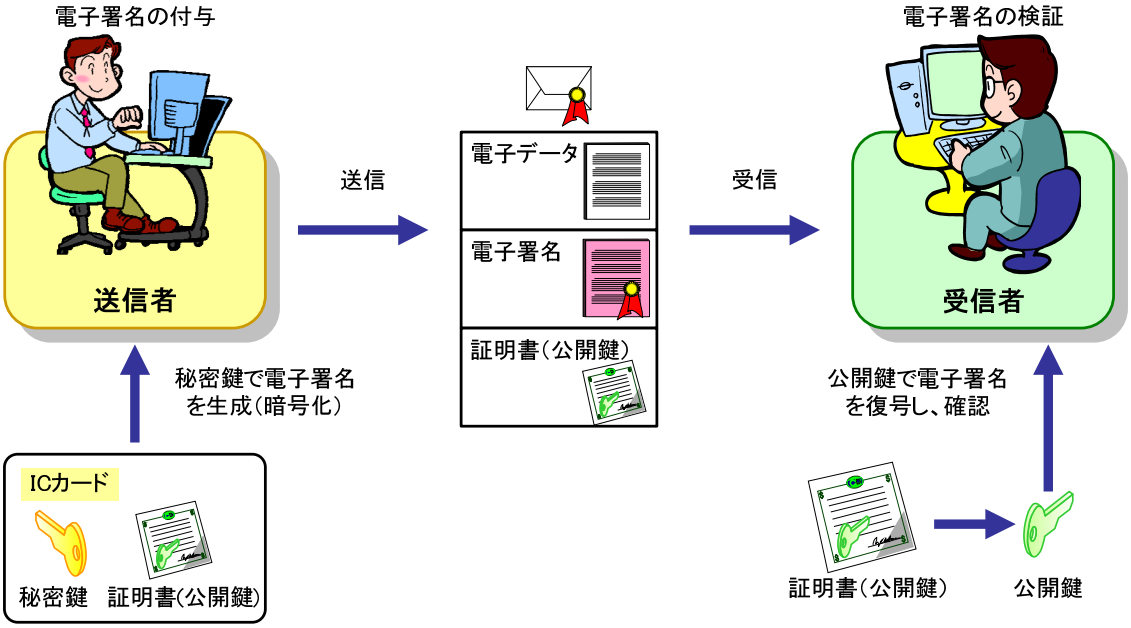

図 2-2　電子署名の検証のイメージ

2-2　コアシステムの認証モデル

コアシステムは、様々な発注機関が利用することから、GPKI や LGPKI を利用できる国の行政機関（中央省庁）や地方自治体等と、その他の発注機関では運用の方法が異なります。そのため、ブリッジモデルとマルチトラストモデルの両方に対応しています。

ブリッジモデルは、ブリッジ認証局（BCA）を介して府省認証局、地域認証局と民間認証局の相互認証を行う方法です。GPKI、LGPKI を利用できる発注機関で運用することが可能な認証モデルとなります。

マルチトラストモデルは、あらかじめ信頼する認証局を複数登録しておく方法で、登録された認証局であれば相互に認証することが可能となります。信頼する認証局を登録するためには、コアシステム利用者のクライアント PC に、あらかじめ信頼する認証局のルート CA 証明書を保存する必要があります。マルチトラストモデルに対応することで、ブリッジ認証局経由で相互認証を行えない、すなわち GPKI、LGPKI を利用できない発注機関においてもコアシステムを運用することが可能となる認証モデルです。

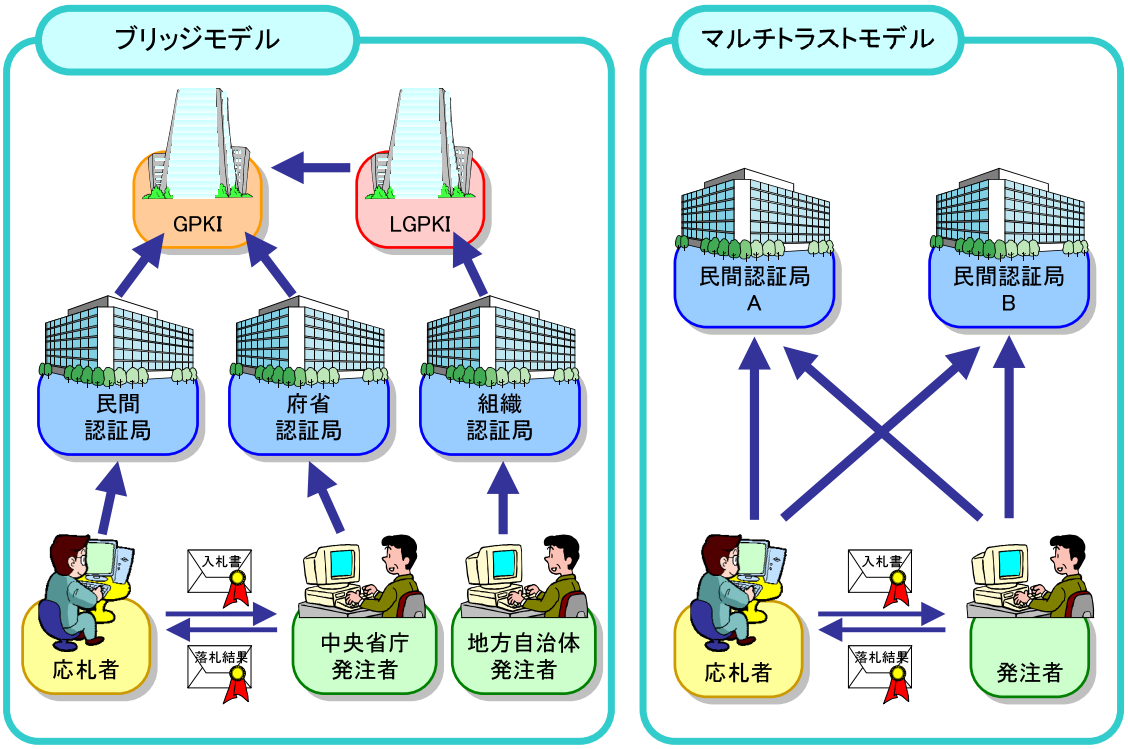

図 2-3　ブリッジモデルとマルチトラストモデルのイメージ

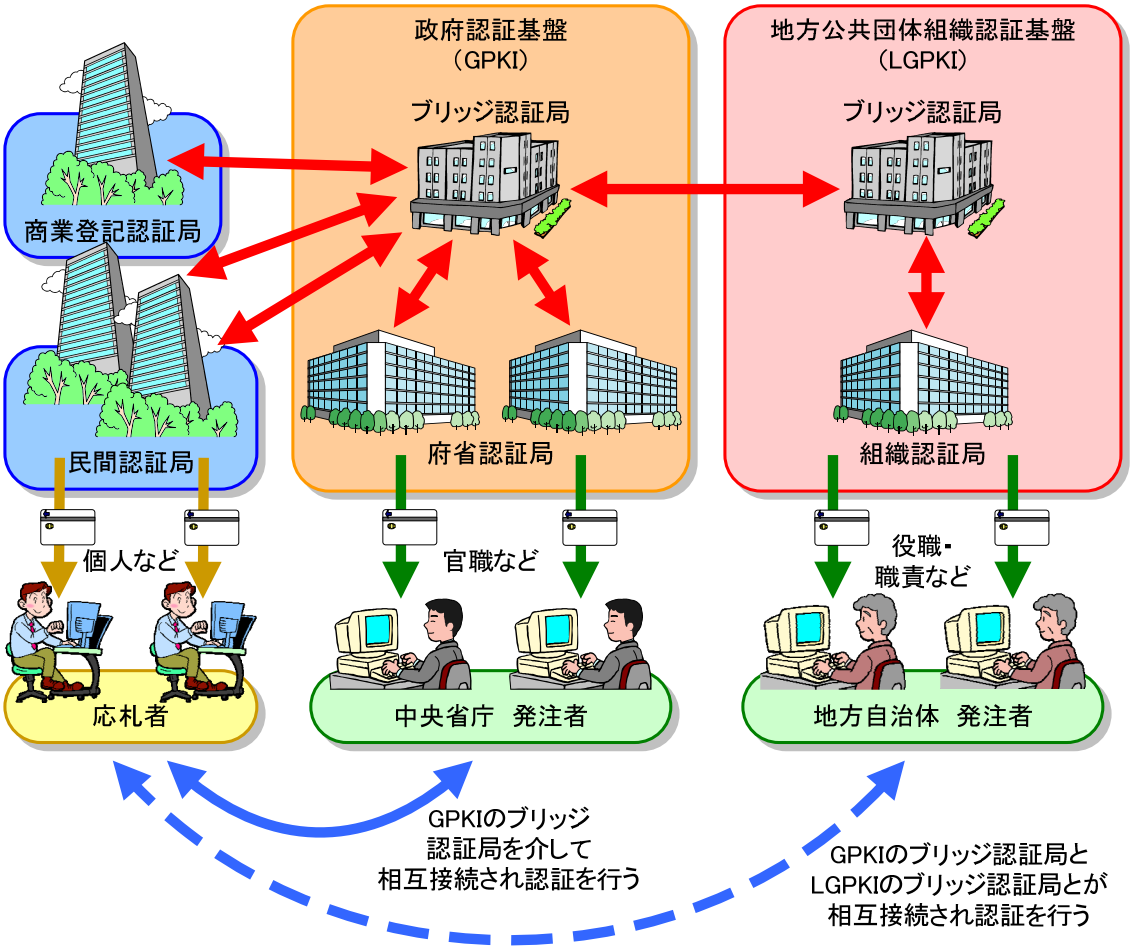

図 2-4　GPKI と LGPKI のイメージ

3　証明書の検証方式

コアシステムは、様々な発注機関が利用することから、GPKI や LGPKI を利用できる発注機関向けのブリッジモデル、それらを利用できない発注機関向けのマルチトラストモデルの 2 つの認証モデルに対応しており、そのモデルによって証明書の検証方式が異なります。また、1 モデル 1 方式とも限りませんし、応札者クライアント、発注者クライアント、サーバでも方式が異なってきます。

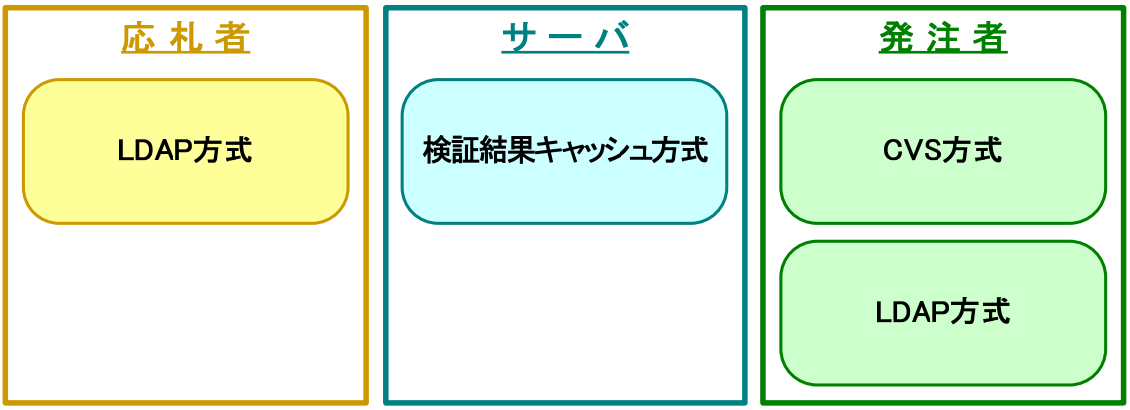

図 3-1　ブリッジモデルにおける検証方式

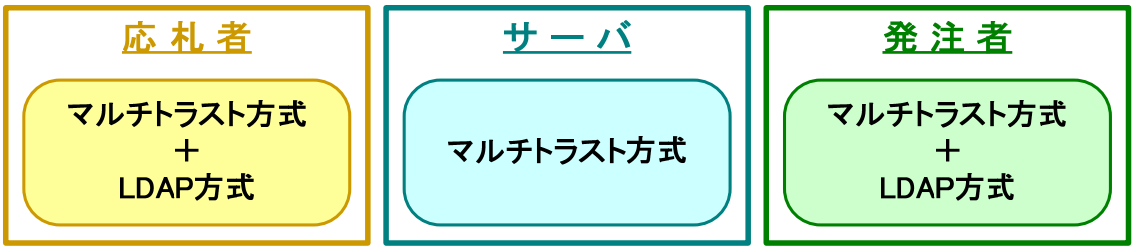

図 3-2　マルチトラストモデルにおける検証方式

以下に、コアシステムが使用する証明書の検証方式を説明します。

3-1 LDAP方式〔応札者クライアント、発注者クライアント〕

発注機関が中央省庁や地方自治体の場合、GPKI、LGPKI のブリッジ認証局を経由して、コア対応民間認証局までパスを構築し、応札者が使用する民間認証局発行の証明書を検証することができます。

LDAP（Lightweight Directory Access Protocol）を用いて、検証する側のトラストアンカ（信頼点）から、検証対象の証明書までの認証パスを構築して、リアルタイムで検証を行います。その際、GPKI、LGPKI のブリッジ認証局を経由※しますので、この検証方法を利用できるのは、GPKI の官職証明書を使用する中央省庁等、LGPKI の職責証明書を使用する地方自治体等及び GPKI との相互認証を行っているコア対応民間認証局発行の証明書を使用する応札者となります。

表 3-1　LDAP 方式のメリット、デメリット

メリット	○リアルタイムに検証が行われるので、緊急に失効処理が行われた証明書が存在しても正しく検証できる。
デメリット	●外部インターネットに対し LDAP を通さないネットワーク構成では利用できない。 ●リアルタイムで最大 3 つのリポジトリサーバ（認証情報公開サーバ）から、10 数個のファイル（証明書類と失効リスト類）を取得し、すべての信頼性を確認するため、処理時間がかなり必要となる。

※：LDAP 外部アクセスを制限しているネットワークの時は、経由対象のブリッジ認証局を含めて制限を解除する必要があります。

3-2 CVS方式〔発注者クライアントのみ〕

GPKI、LGPKI が用意する CVS（証明書検証サーバ：Certificate Validation Server）を利用して、証明書の検証を行います。CVS は、証明書の検証依頼を受け、内部でパス構築等の証明書検証処理を行い、その結果を返します。ただし、CVS は、GPKI、LGPKI が、中央省庁、地方自治体向けに行っているサービスであるため、応札側は使用できません。

表 3-2　CVS 方式のメリット、デメリット

メリット	○通信プロトコルは HTTP（Hypertext Transfer Protocol）（若しくは HTTPS（Hypertext Transfer Protocol Security））であるため、LDAP を使用することによるデメリットが解消される。 ○検証をすべて CVS に依頼し、CVS はリアルタイムに検証するため、緊急に失効処理が行われた場合にも正しく検証が行える。 ○リアルタイムでの検証ではあるが、CVS 内で情報のキャッシュが行われるため、2 回目以降の検証に関しては高速なレスポンスが期待できる。
デメリット	●すべてのクライアントラッパ（電子入札専用ソフト）が対応しているわけではないので、使用する発注者クライアントラッパによっては利用できない（LGPKI 職責証明書用ラッパ※は対応済み）。 ●CVS 自体は外部インターネットに配置されているため、検証自体が高速化しても、ネットワーク負荷等によるレスポンスの悪化の可能性がある。 ●GPKI の CVS は、省庁単位に 1 つ用意されているが、LGPKI の CVS は全国で 1 箇所しかない。そのため各自治体の運用が本格化した際に、処理が集中し、レスポンスの悪化が想定される。 ●LGWAN（総合行政ネットワーク：Local Government Wide Area Network）のように、外部インターネットへの接続が行えない環境下では利用できない。

※：電子入札コアシステム LGPKI 対応電子入札専用クライアントソフトウェア

3-3 マルチトラスト方式〔応札者クライアント、発注者クライアント、サーバ〕

検証対象の証明書を発行する認証局を、あらかじめ信頼してトラストポイントに加えておき、その認証局が発行する証明書は信頼に値すると判断する方式です。

検証対象の証明書を発行した認証局を信頼し、あらかじめその認証局のルート CA 証明書（自己署名証明書）を取得し、検証を行う機器で保持します。CRL（証明書失効リスト：Certificate Revocation List）は、通常 24 時間周期で更新されるので、入札システム側で 1 日 1 回取得し、検証側に公開する必要があります。

CRL を取得するためのツールは、コアシステムから提供されます（検証結果キャッシュツールをパス構築なしのモードで使用）。

表 3-3　マルチトラスト方式のメリット、デメリット

メリット	○パス構築等の処理がないため、レスポンスが良い。 ○検証時に LDAP を使用しない。
デメリット	●CRL の取得間隔内に、緊急な失効等が行われた場合、検証結果に反映されない。 ●対象とする認証局が増えたり、登録済みのルート CA 証明書の有効期限が切れたりした場合、各検証機器に、新しいルート CA 証明書を追加し、CRL 取得処理、公開処理、その設定ファイル等にすべて修正を行う必要がある。 ●何らかの問題が起き、発注側認証局と民間認証局の間の信頼関係が消滅したり、認証局自体の問題でルート CA 証明書を失効させたりしても、検証結果には反映されない。 ●認証局がルート CA 証明書を更新した場合、各検証機器に、新ルート CA 証明書、旧ルート CA 証明書及びこれらのリンク証明書から構成される証明連鎖ファイルを設定し、設定ファイルに修正を行う必要がある。 ●認証局がルート CA 証明書を更新した場合、クライアントでは、検証が行えない。

3-4　検証結果キャッシュ方式〔サーバのみ〕

特にサーバ用途において、検証を LDAP や CVS という外部ネットワークへのアクセスを伴う検証方式を使用することによるレスポンス低下が問題となっていました。この問題を解消するために、LDAP 方式を用いたパス構築を 1 日 1 回実行し、その結果をキャッシュする方式として考案されました。

方法としては、その証明書を発行する認証局（コア対応民間認証局と発注者側証明書発行の認証局）までのパスを構築し、その結果の保持とルート CA 証明書、CRL の保存を行います。この結果から、その認証局に問題はなく、その認証局発行の証明書にも問題はないと判断し、失効状態を CRL から判断します。

コアシステムとしては、保存されたルート CA 証明書、CRL を用い、マルチトラスト方式で動作します。検証を行い、結果を保存するためのツール（検証結果キャッシュツール）は、コアシステムから提供されます。

表 3-4　検証結果キャッシュ方式のメリット、デメリット

メリット	○実行時は、マルチトラスト相当なのでレスポンスが良い。 ○毎回の検証時に LDAP を使用しない。 ○通常のマルチトラストとは異なり、認証局を直接信頼するわけではなく、信頼できる状態にあるかを毎日チェックできる。
デメリット	●検証ツールの実行間隔内に、緊急な失効等が行われた場合、検証結果に反映されない。 ●対象とする認証局が増えた場合、検証結果キャッシュツールの設定を修正する必要がある。 ●登録済みのルート CA 証明書の有効期限が切れた場合、検証結果キャッシュツールが設定に従い、新ルート CA 証明書を取り込むが、取り込んだルート CA 証明書を日々設定しない運用を行っている場合は、その設定を保守する必要がある。

4　商業登記認証局対応について

商業登記認証局対応における検証方式を説明します。

4-1　概要

コアシステムでは、商業登記認証局発行の証明書に対応します。ただし、商業登記認証局発行の証明書は、ファイルベースとなっており、コアシステムが要求する IC カード等の耐タンパ性（不正アクセスに備えるための機能）のある媒体に格納されておりません。証明書を IC カードに格納するサービスを行っている業者がありますので、そこで作成された IC カードを使用する場合のみ、入札に参加できることになります。

商業登記認証局発行の証明書の検証において、他の認証局と大きく異なる点が 2 点あります。1 つは OCSP（Online Certificate Status Protocol）の使用で、もう 1 つは複数のルート CA 証明書の存在です。

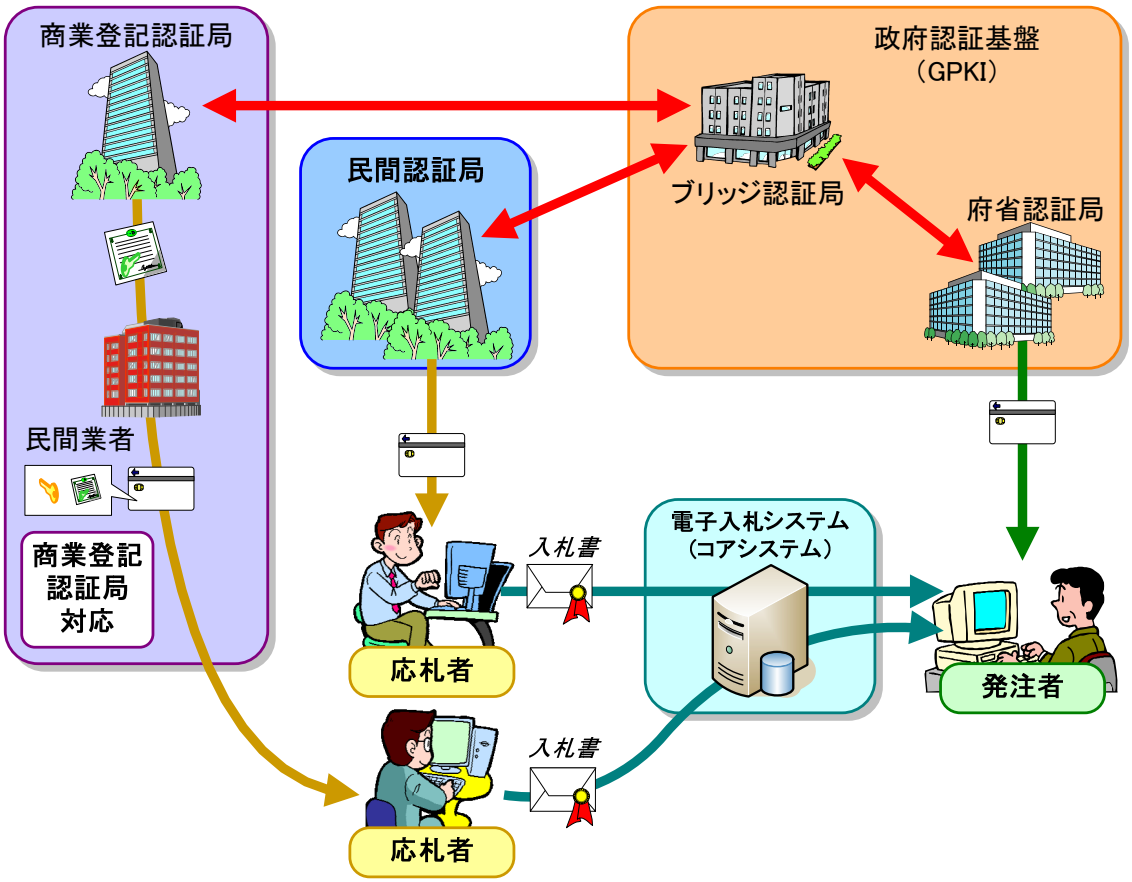

図 4-1　コアシステムの商業登記認証局対応のイメージ

（1）OCSPについて

商業登記認証局は、CRL を公開していません。証明書の失効情報を確認するためには、OCSP サーバに問い合わせを行う必要があります。そのため、マルチトラスト方式、検証結果キャッシュ方式であっても、リアルタイムに外部インターネットへアクセスを行う必要があります。

（2）複数のルートCA証明書について

通常の認証局のルート CA 証明書は、10 年間程度の有効期間を持ち、5 年目に新しいルート CA 証明書を発行して、有効期間の重なりを持った状態で運用が行われます。あわせて、認証局の危殆化対応等の鍵更新の可能性を含めて、ルート CA 証明書が 2 つ以上存在することになります。

これに対し、商業登記認証局のルート CA 証明書は、有効期間とは別に、証明書発行可能な期間が決められています。これが 1 年となっており、毎年新しいルート CA 証明書が作られます。そのため、同時に多くのルート CA 証明書が存在し、有効な状態となっています。

4-2 各方式での対応方法と影響

上記の仕様により、コアシステムの各検証方式に様々な影響があります。方式ごとの対応方法と、そのために必要な対処について、以下に記述します。

(1) LDAP方式〔発注者クライアントのみ〕

LDAP 方式では、リアルタイムで検証対象の証明書までのパスを構築します。この時に、通常であれば検証対象の証明書の失効情報を確認するために CRL を取得しますが、この部分に関しては、OCSP へアクセスを行う必要があります。

(2) CVS方式〔発注者クライアントのみ〕

GPKI、LGPKI が提供する CVS は、商業登記認証局に対応しています。そのため、コアシステム側には影響が及びません。

(3) マルチトラスト方式〔応札者クライアント、発注者クライアント、サーバ〕

マルチトラスト方式は、本来、検証対象の証明書を発行した認証局のルート CA 証明書とその失効情報を格納した CRL をコアシステムのサーバに保持し、ローカルで検証を行う方式ですが、商業登記認証局では CRL が公開されていないため、サーバで保持できません。そのため、商業登記認証局対応のマルチトラスト方式では、ルート CA 証明書のみローカルで確認し、失効状態の確認はリアルタイムで OCSP へアクセスを行う必要があります。

通常のマルチトラスト方式であれば、外部インターネットに接続できない環境であっても、ローカルに保持したルート CA 証明書とコアシステムサーバで公開する CRL を用いて証明書の検証を行うことが可能でしたが、商業登記認証局対応においては外部インターネットへの接続が必須となります。

また、ルート CA 証明書が複数存在するため、マルチトラストの設定ファイルにおいては、それぞれの設定が必要となります。つまり、最低年 1 回は設定を保守する必要があります。

(4) 検証結果キャッシュ方式〔サーバのみ〕

マルチトラスト方式と同様の影響があります。ただし、ルート CA 証明書の設定に関しては、検証結果キャッシュツールを標準の状態で使用する場合には、日々の運用・保守によってこの設定を取り込みますので、この設定についての特別な保守は必要ありません。

マルチトラストモデルにおける発注者クライアントで、商業登記認証局に対応するために、OCSP へアクセスを行えるようにするには、(3) で示したとおり、すべての発注者クライアントで、毎年、設定を保守する必要があり、実際に運用することはほとんど不可能です。そのため、その対処策として、サーバ検証方式の機能を設けました。

(5) サーバ検証方式〔発注者クライアントのみ〕

マルチトラストモデルにおける発注者クライアントにおいて、商業登記証明書の検証をサーバに委譲し、サーバ側で証明書検証を行う方法です。

4-3　検証方式のまとめ

応札者の商業登記認証局の証明書を、応札者クライアント、発注者クライアント、サーバで検証する際の方式をまとめると以下のようになります。

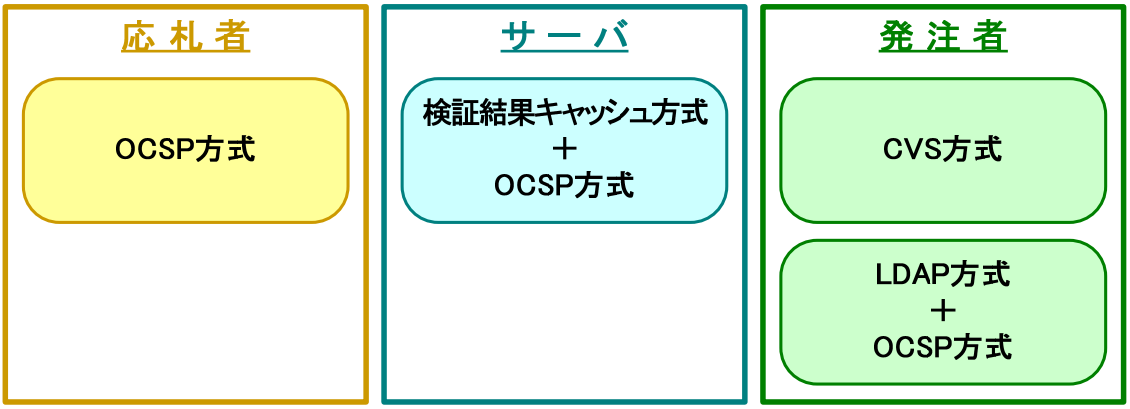

図 4-2　ブリッジモデルにおける検証方式（商業登記認証局対応）

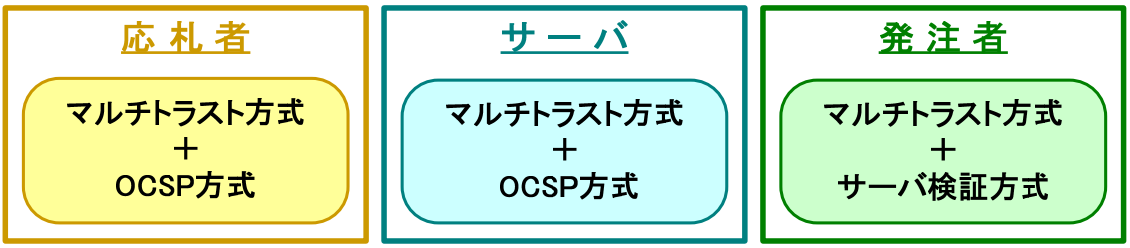

図 4-3　マルチトラストモデルにおける検証方式（商業登記認証局対応）

5　コアシステムが推奨する方式

発注機関の種類により、採用できる検証方式は異なります。しかし、幾つかの方式を組み合わせて使用することにより、コアシステム全体のレスポンス向上を図ることが可能です。

以下に、発注機関の種類別にコアシステムが推奨する方式を記述します。

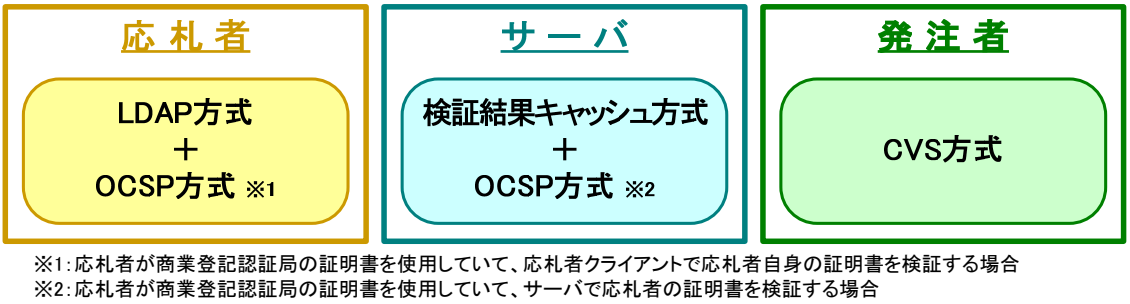

図 5-1　中央省庁、地方自治体（ブリッジモデル）における推奨方式

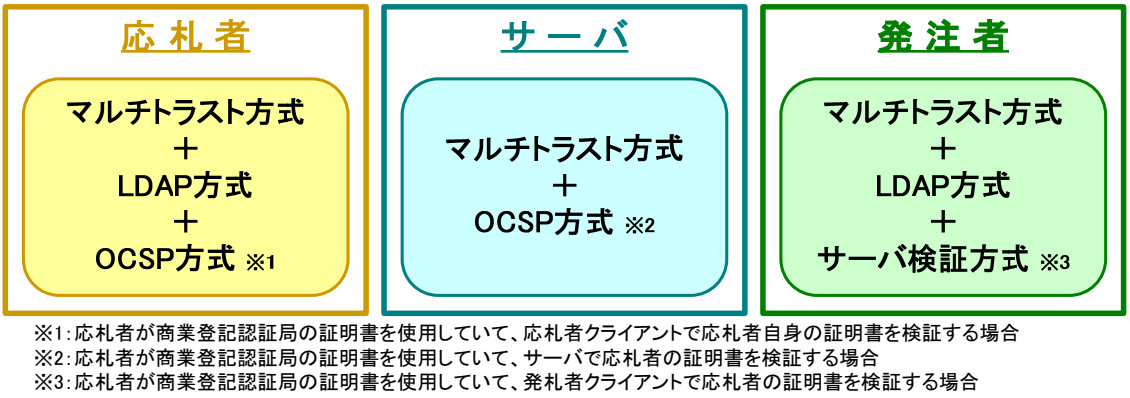

図 5-2　その他の発注機関（マルチトラストモデル）における推奨方式

5-1　中央省庁

中央省庁の場合、証明書検証においては、CVS の利用が推奨されております。しかし、CVS を利用するということは、証明書検証処理の場面すべてで外部インターネットを経由して GPKI が用意する各省庁用の CVS にアクセスすることになります。CVS に対する負荷、ネットワーク負荷等によるレスポンス悪化を考慮し、サーバでは「検証結果キャッシュ方式」、発注者クライアントでは「CVS 方式」を推奨します。応札者クライアントに関しては、CVS が利用できないため、これまでどおり「LDAP 方式」とします。

（1）推奨の理由

GPKI では、CVS の利用が推奨されており、クライアントでは CVS を採用することで、LDAP が不要となります。また、商業登記認証局対応においても、発注者クライアントから追加で OCSP サーバにアクセスする必要がなくなります。

しかし、サーバでは、証明書検証の場面が多く、CVS への負荷が増大します。また、他のネットワーク負荷の影響も受けるため、CVS 方式ではなく、一番レスポンスが良く、かつ GPKI のブリッジを使ったパス構築の結果を使用する検証結果キャッシュ方式の採用を推奨します。

（2）留意点

検証結果キャッシュ方式を採用しても、商業登記認証局の証明書検証を行う際には、OCSP へアクセスを行う必要があります。そのため、外部インターネットに対してアクセスが行えない場所にサーバがある場合、商業登記認証局に対応できません。

発注者クライアントに関しては、府省認証局のクライアントラッパが CVS に対応している必要があります。使用している発注者クライアントラッパの開発元にお問い合わせください。

5-2 地方自治体

地方自治体の場合、証明書検証においては LGPKI が提供する CVS が利用できます。しかし、CVS を利用するということは、証明書検証処理の場面すべてで外部インターネットを経由して LGPKI が用意する 1 つの CVS にアクセスすることになります。CVS に対する負荷、ネットワーク負荷等によるレスポンス悪化を考慮し、サーバでは「検証結果キャッシュ方式」、発注者クライアントでは「CVS 方式」を推奨します。応札者クライアントに関しては、CVS が利用できないため、これまでどおり「LDAP 方式」とします。

（1）推奨の理由

LGPKI では、CVS の利用が可能であり、クライアントでは CVS を採用することで、LDAP が不要となります。また、商業登記認証局対応においても、発注者クライアントから追加で OCSP サーバにアクセスする必要がなくなります。

しかし、サーバでは証明書検証の場面が多く、全国で 1 箇所しかない CVS への負荷が増大します。また、他のネットワーク負荷の影響も受けるため、CVS 方式ではなく、一番レスポンスが良く、かつ LGPKI のブリッジを使ったパス構築の結果を使用する、検証結果キャッシュ方式の採用を推奨します。

（2）留意点

検証結果キャッシュ方式を採用しても、商業登記認証局の証明書検証を行う際には、OCSP へアクセスを行う必要があります。そのため、外部インターネットに対してアクセスが行えない場所にサーバがある場合、商業登記認証局に対応できません。地方自治体の場合、LGWAN 内の ASP サービス等を利用して、外部インターネット環境にアクセスできない場所にサーバが置かれるような運用があり得ますが、この場合、商業登記認証局対応は行えません。

発注者クライアントに関しては、コアから提供している LGPKI 職責証明書用ラッパは CVS に対応しています。しかし、それ以外の証明書、それ以外の発注者クライアントラッパを使用している場合は、そのラッパ開発元にお問い合わせください。

5-3　その他の発注機関

中央省庁や地方自治体以外の GPKI、LGPKI という枠組みの外にある発注機関の場合、ブリッジ経由の LDAP での検証や、CVS を使用することができません。そのため、マルチトラスト方式などの複数の検証方式を組み合わせて対処することになります。

（1）推奨の理由

GPKI、LGPKI の仕組みが使用できませんので、サーバ、クライアントともマルチトラスト方式を中心に、検証の対象となる証明書に合わせ、複数の検証方式を使用することになります。

（2）留意点

マルチトラスト方式を採用しても、商業登記認証局の証明書検証を行う際には、OCSP へアクセスを行う必要があります。そのため、外部インターネットに対してアクセスが行えない場所にサーバがある場合、商業登記認証局に対応できません。

発注者クライアントに関しては、ルート CA 証明書を更新した民間認証局の証明書を検証する場合、直接、民間認証局に LDAP で行いますので、外部インターネットにアクセスできる必要があります。LDAP への対応などについては、使用している発注者クライアントラッパの開発元にお問い合わせください。