２．開発着手から完成までの基本的な方針

２．１　システム構築における基本方針

（１）ベースとする電子入札システムの選定

電子入札システムを取り巻く中央省庁及び新潟県をはじめとする全国の地方自治体の動向を把握し、以下の観点から長岡市がベースとする電子入札システムを選定します。

①システムの導入コストを抑えるため、採用する自治体が最も多いことが予想される電子入札システムをベースに構築することが望ましい。
（一自治体の開発費の大小は、母数となる自治体の数によって決まる）

②受注者の立場からも、入札に参加する自治体毎にシステムが違うと煩雑で混乱のもとになる。また自治体毎にパソコンを用意しなければならないことも考えられる。ゆえに、なるべく統一されたシステムを導入し、どの自治体でも同一の環境、同一の操作で利用できることが望ましい。

以上から、ＪＡＣＩＣ、横須賀市、ＮＴＴデータの各システムを総合的に勘案し、現時点では全国の自治体が多数加入（特別会員）している、ＪＡＣＩＣのコアシステム※1 を採用します。

※1：（財）日本建設情報総合センター（ＪＡＣＩＣ）及び（財）港湾空港建設技術サービスセンター（ＳＣＯＰＥ）により設立された、「電子入札コアシステム開発コンソーシアム」が提供する電子入札のコア部分（コアシステム）をいいます。「電子入札コアシステム開発コンソーシアム」の設立目的、組織等について６４ページ資料１に示します。なお、長岡市は平成１４年２月に特別会員として加入しています。

（２）センター設備の形態

センター設備の形態については、市役所内設置とともに、データセンターの利用についても、市場動向を踏まえ、コスト、セキュリティ、利便性の面で比較検討し、より有利な形態を採用します。

センター設置場所には、現時点では市役所内の電算室等を想定していますが、将来市場動向を踏まえ、データセンターあるいは外部委託を図り、共用センター方式も視野に入れた検討をします。

（３）透明性・公平性の確保

電子入札では発注者と受注者の間をインターネットとコンピューターを介して情報のやりとりが行われるため、その状況が目で確認できません。このため電子入札の透明性・公平性を確保し、盗聴、改竄、なりすまし、事後否認などの不正を排除するため、以下の方法により対応します。

なお、検討にあたっては高い安全性を確保しつつ、簡便な操作で実現できる方式を選定します。

①公平で透明性の高い入札開札手順（電子入札プロトコル）の導入により、受注者、発注者及び第三者による不正を排除する。

②電子署名法に基づく認証方式により、入札書や結果通知書など受注者、発注者から

の文書の正当性を証明する。
さらに、受注者認証は受注者側の負担をなるべく軽減し、より多くの受注者が参加できることとする。
また、市役所側の認証は地方公共団体組織認証基盤（以下「ＬＧＰＫＩ」という）の導入に合わせこれを利用する。

③公証機能により、入札書や結果通知書などの文書の交換、保存に不正が無いことを証明する。

（４）競争性の確保

より多くの入札参加者が電子入札に参加できるようにするため、以下の対応をはかります。

①利用者の操作の負担軽減

受注者側での入札システムの操作は初心者でも、簡単に操作できるよう、画面や入力方法はわかりやすく、間違いを起こしにくいインターフェースにする。

②利用機器、ソフトウェアの負担軽減

受注者側が特別な機器やソフトウェアを用意しなくても、一般に最も多く流通している標準的な機器やソフトウェアで電子入札に参加が可能とする。

③当分の間は、電子入札ができない受注者は紙入札も可能とする。

（５）入札契約事務作業の効率化

制限付き一般競争入札の導入に伴う作業量の増大に対応するため、情報の一元化、集約化（データベースの構築）、即時更新等により事務作業の軽減化および迅速化を図ります。

（６）長岡市電子市役所及び関連システムとの連携

長岡市のポータルサイト（ホームページ）との連携をはかり、さらに財務会計システム、文書管理システム、設計積算システム、地理情報システム、などとも将来の連携を考慮した設計を行います。

（７）コストを抑えたシステム開発手法の導入

システムの開発コストを抑えるため、入札業務の開発においては、ＪＡＣＩＣコアシステムの採用や機能コンポーネント化などの手法を用います。

（８）拡張性のあるシステムの構築

将来において、広域市町村圏や市町村合併における、電子入札システムの利用形態を踏まえ拡張性のあるシステムを構築します。

（９）ネットワークセキュリティ対策

①インターネット系ネットワークとの連携を図り、セキュリティ、信頼性、通信速度を考慮したネットワークの設計を行う。

②セキュリティ対策としてはルータ、ファイアウォールの不正アクセス、ウィルス感染、漏洩、改竄等の防止対策を図る。

２．２　システムの実現形態

（１）対象業務

本システムでは以下の業務を対象とします。

ア．入札参加資格者管理業務

インターネットによる入札参加資格審査の申請および更新などの処理を行います。また指名競争入札における業者選定の支援を行います。

イ．入札・見積業務

以下の入札方式を対象に、インターネットにより入札案件の公開、入札・見積、開札・見積合わせ、結果の公表など、一連の入札・見積に関する処理を行います。

（ア）工事
①制限付き一般競争入札
②指名競争入札
③随意契約（見積合わせ、単独随契）
④公募型指名競争入札
⑤簡易プロポーザル方式

（イ）業務委託
①制限付き一般競争入札
②指名競争入札
③随意契約（見積合わせ、単独随契）
⑤公募型指名競争入札
⑥簡易プロポーザル方式

（ウ）物品
①制限付き一般競争入札
②指名競争入札
③随意契約（見積合わせ、単独随契）

ウ．契約事務支援業務

入札・見積結果に基づく契約書作成等の事務作業の支援、およびインターネットによる入札結果の公表などを行います。

エ．施工管理事務支援業務

着工から竣工までの一連の契約検査課における事務作業を支援します。

オ．統計管理資料作成業務

入札契約に関する統計管理資料を作成します。

カ．情報公開業務

インターネットによる工事の発注見通し、建設工事の評定結果、業者名簿などの公開を行います。

キ．データベース管理業務

業者及び入札、契約、工事等に関する情報を蓄積するデータベースのバックアップ等の維持管理作業を行います。

（２）セキュリティ対策

ア．外部からの脅威

（ア）ネットワーク侵入

インターネット（外部）からのネットワークを通じての侵入に対しては、ファイアウォールを設置し、許可したアクセス以外の不正なアクセスを排除します。また、ファイアウォールの外側に設置されたルータへの侵入に対する防御対策を行います。さらに、サーバーは不正アクセスに対する堅牢性を有するオペレーティングシステム（ＯＳ）及び機種を選定します。

ａ．ファイアウォールの導入

ファイアウォールを設けることで、許可したプロトコル以外のアクセスを排除し、不要なプロトコルの侵入を阻止します。

①ファイアウォール１をＷｅｂサーバーやＡＰサーバー、ＤＢサーバーなどに対する、外部からの不正なアクセスによる攻撃を排除するために設置します。

②ファイアウォール２を受注者端末から直接アクセスできる非武装セグメント（DMZ）と直接アクセスできないセキュリティの高いＡＰセグメント、ＤＢセグメントの間に設置します。

受注者端末はＤＭＺセグメントに設置されたＷｅｂサーバーにアクセスし、Ｗｅｂサーバーがファイアウォール２を通過してＡＰサーバーにアクセスします。

具体的な機器構成を、３．２項の図３．２－１「ネットワーク・機器構成概念図」に示します。

ｂ．堅牢なＯＳと機種の選定

ＷｅｂサーバーやＡＰサーバー、DB サーバー等は不正アクセスに堅牢なＯＳと機種を選定し、セキュリティホールを突いた外部からの不正を阻止します。

（イ）盗聴・漏洩

（セキュアな通信方式の採用）

受注者との文書の送受信は文書の暗号化により盗聴や漏洩による被害を防止します。

（ウ）改竄・なりすまし

（公開鍵暗号化方式による署名・証明書の付与）

受注者は公開鍵暗号方式を用い、本人のみが所有している秘密鍵を使って署名および証明書を付与して入札書等を送信します。同様に本システムにおいても受注者に通知する各種通知書等を秘密鍵により電子署名及び証明書を付与して、受注者に送付します。なお、９ページ（３）認証で詳細に示します。

（エ）ウィルス感染

（ウィルス感染チェックの実施）

受注者等から受信した入札等のデータに対してウィルス感染してないか確認を行います。もしウィルスに感染していた場合は感染した装置を隔離し、ウィルスの駆除を行い、感染拡大防止に努めます。

イ．内部からの不正利用

（ア）ユーザー認証の実施

本システムでは、システム関係者以外の使用を制限できるセキュリティを確保するため、各操作及び処理の重要性に応じ最適な認証を実施します。

本システムを利用する担当職員はあらかじめシステムにユーザー登録を行い、システムを使用する際にはユーザー認証を行った上で利用権限を与えられた処理に対してのみ操作が可能とします。

（イ）アクセス制御

ファイルなどの資源に対しては、利用者によるアクセス制限を行うことで、権限を持たない利用者からのアクセスを抑制し、データ及びプログラムの破壊や改竄、データの漏洩を防止します。

ウ．物理的な侵入

物理的な侵入を防止するには、設備・運用環境において高い安全性を確保する必要があります。

具体的にはサーバー等の設備を設置する部屋はＩＣカードや暗証番号による施錠設備を有するとともに、入退室ルールを規定して不正侵入の排除をはかります。さらにマニュアルや資料・電子媒体の管理方法も規定します。

（３）認証

電子認証とはインターネット上で、相手（組織）が実在し、その相手が本当に本人（組織）であるか第三者（認証事業者）が証明するものであり、それを実現する仕組みが電子認証システムです。なお、この電子認証システムを利用してインターネット上で交換する文書の作成者を証明することを電子署名による認証といいます。なお、平成１３年４月に電子署名法（電子署名及び認証業務に関する法律）が施行され、電子署名が法的な根拠を持つことになりました。

本システムにおいても受注者と発注者で交換する入札書や通知書等の文書において電子認証システム及び電子署名によりセキュリティの確保を行います。

ア．電子認証と電子署名の仕組みと役割

（ア）電子証明書の発行

電子証明書の発行を依頼する受注者は認証事業者に本人を確認できる書類等を提出し、審査の上本人を確認出来た場合、依頼者の公開鍵を認証局に登録するとともに、電子証明書の発行を受けます。

通常、電子証明書は秘密鍵とともにＩＣカード等で発行されます。（下図①、②）

※電子証明書はよく印鑑の持ち主を証明する印鑑証明にたとえられます。

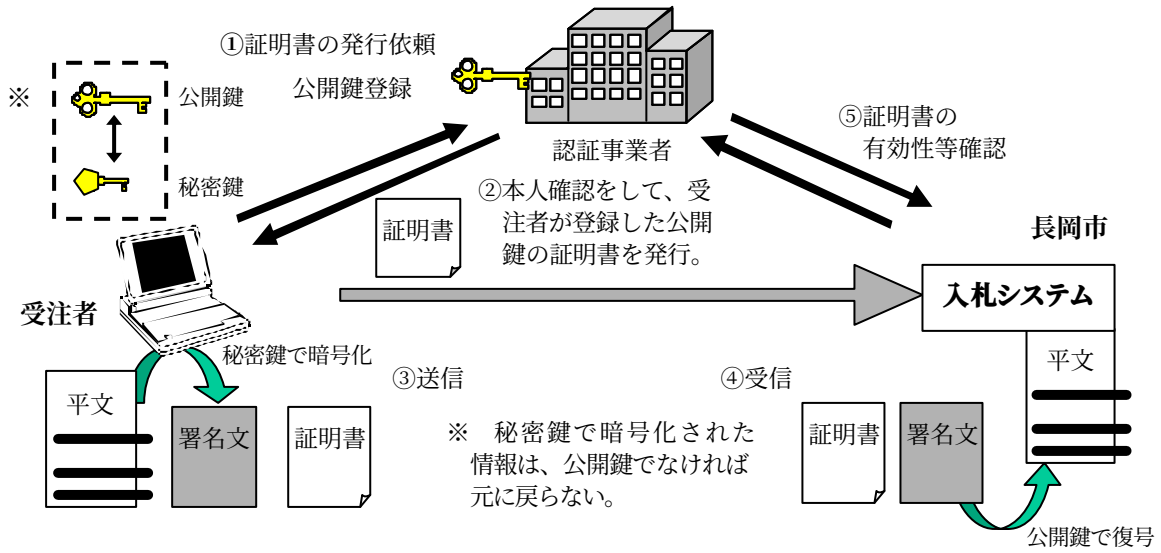
（イ）電子署名による入札書の提出イメージ

①入札書などの文書を送信する場合、ＩＣカードに保存された秘密鍵を利用して送信文書を暗号化し（これを電子署名といいます）、電子証明書を添付して送信します。（下図③）

②入札システムは受信した文書を添付された電子証明書に付属の公開鍵で復号化し平文に変換します。（下図④）

③入札システムは受信した電子証明書の有効性等（所有者、有効期限、失効、一時停止等）を認証局に確認します。（下図⑤）

図２．２－１　電子署名・認証の仕組



（ウ）電子署名の役割

上記のとおり電子署名を行うことにより、インターネット上で提出された入札書等の作成者の正当性を確認できるとともに、暗号化により漏洩や改竄などの排除ができます。

イ．本システムにおける電子認証

（ア）受注者側の認証局

受注者における入札書等に対する電子認証はＪＡＣＩＣおよびＳＣＯＰＥが認定する電子入札システム対応認証局を利用します。現在、認定されている認証事業者は帝国データバンクだけですが、今後複数の認証局を認定する予定です。

また、受注者は長岡市の電子入札に参加する際には事前にＪＡＣＩＣが認定する電子入札システム対応認証局のどれかに申請し、ＩＣカード（電子証明書および秘密鍵）を取得します。このＩＣカードで本人認証および電子署名を行います。

（イ）発注者側（長岡市）の認証局

発注者側（長岡市）の認証局はＬＧＰＫＩの導入に合わせ、これを利用します。ただし、現時点ではＬＧＰＫＩの導入時期が未確定のため、利用可能となるまでの期間は電子入札システム対応認証局を利用します。

（４）公証

受注者から提出された入札書は開札までの期間、受注者も発注者も見ることができません。そのため、受注者から入札金額が入札した金額と違うとのクレームをたてられる（事後否認）恐れがあります。また、電子入札システムで実施された電子入札の正当性の証明を求められることも考えられます。このように電子入札の正当性を公に証明することを電子入札の公証といいます。

本システムにおいても公証機能を有し事後否認等のクレームに対し、入札の透明性、公平性を証明する必要があります。

ア．証明の種類

①内容証明

受注者から提出された入札書が改竄されてないことを証明します。

②存在証明

受注者から提出された入札書がある日付・時刻に存在していたことを証明します。

③到達証明

受注者から提出された入札書が確実に入札システムに届いたことを証明します。

イ．本システムにおける公証の実現方式

ＪＡＣＩＣの電子入札コアシステムによる方式を用いて、電子入札契約システムの内部機能として以下の方法により実現します。

①内容証明

入札書の提出時と開札時の入札書のハッシュ値をインターネット上に公開します。２つのハッシュ値を比較し、一致することにより改竄されてないことを証明します。

②存在証明

受注者より入札書が提出された日時を入札システムのログに記録し、その存在の事実を証明します。

③到達証明

受注者が入札書を提出すると、ただちに画面に入札書受領の画面を表示します。また、入札システムから受注者に入札書受付票を電子メールで送付します。これにより受注者側で確実に届いたことを確認します。

※公証の実現方法としては公証サーバーや電子文書証明サービスなどによるものもあります。これらはＴＴＰ（信頼できる第三者）による証明といい一般的に証拠能力が高いとされています。

（５）入札開札手順

受注者のパソコンからインターネットを介して入札書を提出する電子入札システムでは、現行の入札のように発注者が指定した時刻、場所に一斉に会して入札を行うやりかたと違い、その状況が直接目で確認できません。

そのため、電子入札システムでは入札書などの文書の漏洩や改竄などの不正が発注者および受注者双方とも絶対にできない入札手順が求められます。

本システムにおいても電子入札の透明性と公平性を確保するため、不正の入る余地のない入札手順のシステムを導入します。

ア．不正を排除するための手順上の要件

①入札書が漏洩しないこと

受注者は提出された入札書が開札までの間、受注者及び発注者の双方から絶対に見ることができないこととします。

②入札参加者名が落札まで公表されないこと（工事指名競争入札は除く）

再入札の可能性があるため、ハッシュ値等の公表や落札決定前の開札処理画面等は受注者名をダミーで表示する等の工夫をします。

③予定価格等が漏洩しないこと

予定価格は開札の直前に封書を開封し、立会人の立ち会いのもとで入力します。

④予定価格の入力に際して、各社の入札額を見ることができないこと

予定額等が入力されないと、入札書の開札ができないようにします。

⑤事前に設定された日時に沿って、確実に入札開札が進められること

入札参加申請開始・終了、入札開始・終了、開札開始等の日時が事前に公表されたとおりに進められることとします。

イ．本システムにおける電子入札手順

ＪＡＣＩＣの電子入札コアシステムによる方式をもとに長岡市の要件を反映した手順で対応します。

①入札受付期間（入札開始～締め切り）

・入札書の暗号化

入札書は暗号化されて提出される。なお、入札書を復号化する鍵は鍵管理サーバーで厳重に保管される。

・入札期間内での入札

入札期間を過ぎた入札書の提出はできない。

②入札締め切り期間（入札締め切り～開札）

・入札書のハッシュ値の公開

入札書の送信後、入札書に改竄がなかったことを証明するため、受注者から提出された入札書のハッシュ値を公開する。

③開札落札処理

（予定価格の入力）

・立会人の前で封書を開封し入力する。

・予定価格を入力しないと改札できない。

（開札処理）
・入札書の復号化による表示
　事前に設定された開札日時になると初めて管理サーバーより鍵を取り出すことができる。これにより受注者から提出された入札書を復号化し開札することができる。
・入札結果が確定するまでは、開札画面の入札者はダミー表示とする。

④結果公開
・入札結果公表等
　落札者が決定後、全ての入札者名（実名）と入札額及び予定価格等を公開する。
・入札書のハッシュ値の公開（改竄の有無を証明）
　開札後の入札書のハッシュ値を計算して②のハッシュ値とともに公表し、入札額の改竄が無いことを証明する。

※１：電子入札の手順はＪＡＣＩＣのコアシステムで採用する方式の他にハッシュ方式や一括署名方式などがあります。いずれの方式も手順や仕組みは異なりますが電子入札における、盗聴や改竄等の不正を排除することを目的に考えられたものです。
なお、ＪＡＣＩＣのコアシステムでは発注者側に鍵管理サーバーを設置するため、その管理は運用及びネットワーク上それぞれ厳重に行う必要があります。

※２：入札手順
　本システムは入札金額の漏洩や改竄、なりすましや事後否認を防ぐために様々な暗号＝鍵、サーバー＝金庫を利用します。本システムで使用する鍵や金庫は以下のとおりですが、実際の操作では鍵や金庫の存在をほとんど意識することなく入札できます。
ここでは現実の行為に例えて分かりやすく入札手順を説明します。

入札用公開鍵……錠前（A）と箱（C）
入札用秘密鍵……鍵（B）
共通鍵……封筒（D）とそれを切るはさみ（E）
受注者秘密鍵……梱包と印鑑を押す行為
受注者公開鍵……梱包を解く行為
鍵管理サーバー……鍵管理用金庫
データベースサーバー…箱管理用金庫

・長岡市は入札案件ごとに錠前（A）とそれを開ける鍵（B）と箱（C）を作成する。
・鍵（B）は鍵管理用金庫で開札時間まで厳重に管理する（開札時間まで時間ロックをかける）。
・受注者側パソコンで入札書を入れる封筒（D）とそれを切るはさみ（E）を自動生成し、封筒（D）に入札額を書いた入札書を入れると同時に入札額をハッシュ値（F）にしておく（この封筒（D）は特別製ではさみ（E）でないと絶対に切ることができない）。

・受注者は長岡市から錠前（A）と箱（C）を取得し、箱（C）の中に入札書を切るはさみ（E）を入れて、錠前（A）で箱（C）に施錠する。
・受注者は箱（C）と封筒（D）とハッシュ値（F）を梱包して、認証局に印影を登録した印鑑を押して長岡市に送付する。
・長岡市は梱包物を受け取り、そこに押してある印鑑が本物かどうか認証局に確認する。
・認証局の確認が取れたら、梱包を解き、ハッシュ値（F）を公開し、箱（C）と封筒（D）を箱管理用金庫に厳重に保管する。
・開札日時になると初めて鍵管理用金庫に保管されていた鍵（B）を取り出せるので箱管理用金庫から箱（C）と封筒（D）を取り出し、鍵管理用金庫から取り出した鍵（B）で箱（C）にかかっている錠前（A）を開ける。
・箱（C）からはさみ（E）を取り出し、封筒（D）を開封し、入札額を確認する。

※３：入札書のハッシュ値

入札書を特殊な計算式（ハッシュ関数）により数十文字の長さのアルファベット文字列に変換したものです。ハッシュ値は変換された文字列から元のデータを再現することはできないため、入札書のハッシュ値から入札額を知ることはできません。このことから入札時と開札時のハッシュ値を比較することにより入札書の改竄の有無を確認することができます。

（6）信頼性

ア．信頼性に関わる要件

本システムではインターネットに接続されている情報システムであるという特性と、受注者が入札期間であれば時間にとらわれずいつでも入札できる等の利便性を考慮し、安定した運用が求められます。また、入札の公平性、透明性の確保の観点から、入札開札業務は事前に設定されたスケジュールに従って、確実に行われる必要があります。そのため、システムの開発及び運用において高い信頼性対策が求められます。

イ．信頼性対策

本システムにおける信頼性に対する対策を表２．２－１に示します。

表２．２－１　信頼性対策

フェーズ	区　分		信頼性対策
開発	障害予防	ハードウェア障害予防	ディスクの冗長化など
			機器の設置環境への配慮
			災害対策（地震、水害、火災）
		ソフトウェア障害予防	実績あるオペレーティングシステムの採用
			実績のあるパッケージの導入
運用	運用施策		定期的なバックアップの実施
			ログ及びジャーナルの取得
			運用状況の監視
			障害の自動通知
	復旧対策		運用保守体制の確立
			システム及びデータのリカバリ
			システム動作状況の分析

●ディスクの冗長化

ハードディスク装置を複数のハードディスクユニットで構成し、１台のユニットに障害が発生しても他のユニットによりサーバーを停止せずに処理の継続を可能とします。

●実績のあるオペレーティングシステムおよびパッケージの導入

長時間運転においてもハングアップ等が起こりにくい信頼性の高いソフトウェアを選定します。

●運用状況の監視

サーバー、ネットワーク機器の使用状況を監視します。また、定期的に機器やネットワークの使用率を調査し、現行システムの性能が適正かどうか監査します。

●障害の自動通知

万一システムが故障した場合、自動通知し迅速な対応をはかります。

●保守運用体制の確立

突発的な故障にも迅速に対応できる体制を確立します。

（７）関連システムとの連携

長岡市電子市役所はインターネットをはじめとする様々なＩＴによる共通基盤と文書管理、財務会計等の基幹システムやデータベースなどにより構成されます。電子入札システムにおいても業務の効率化をさらに進め、システムの導入効果を高めるためこれらと連携し、データの二重入力を解消し、多方面での情報の連携・共有化、活用化をはかります。

ただし、今回は電子入札契約システムの導入による業務の改善が主な目的であることから、可能なところから連携を実施していくこととし、現状連携が難しいシステムについては、将来の連携を考慮したシステムの設計を行うこととします。

ア．関連システムと連携対応について

①地方公共団体組織認証基盤（ＬＧＰＫＩ）

長岡市より発する各種通知書などの文書類の認証は共通基盤であるＬＧＰＫＩを使用します。

②長岡市のポータルサイト（ホームページ）

市民への情報公開および入札業務に関わる文書交換は長岡市のポータルサイト（ホームページ）を窓口にします。

③文書管理システム

入札案件に関する伺・契約等の決裁事務との連携が可能です。今後、文書管理システムの導入が可能となった時点で連携を図ります。

④財務会計システム

受注者（債権者）情報や工事代金の支払い（支出命令）等の連携が考えられます。今後、財務会計システム側での対応が可能となった時点で連携を図ります。

⑤積算システム

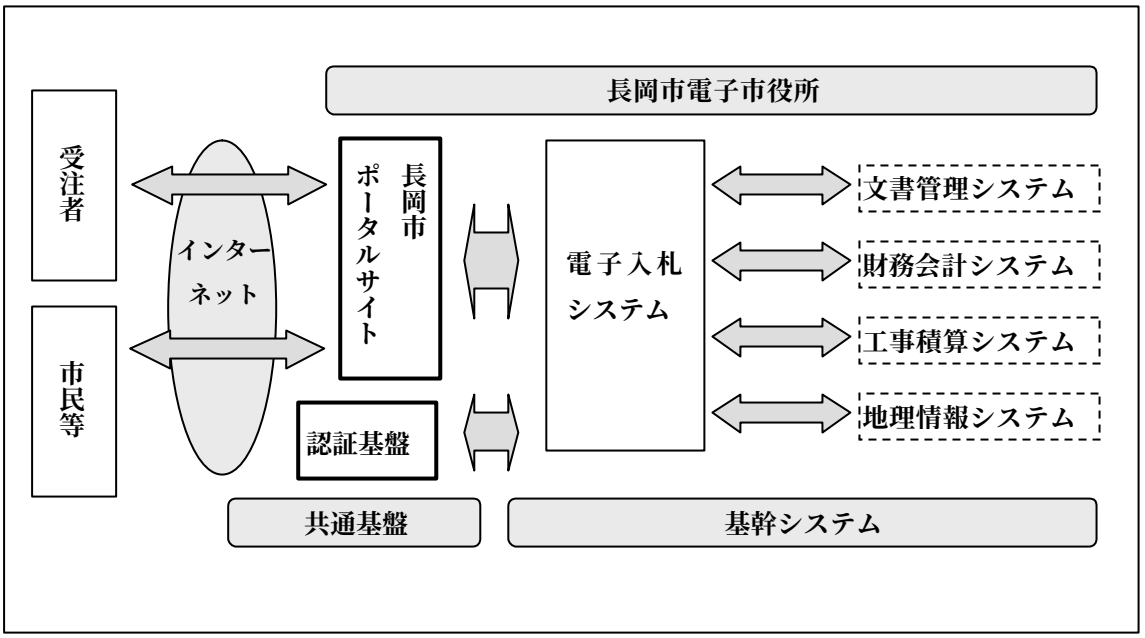
入札案件として工事仕様書、設計価格等の連携が考えられます。今後、積算システム側での対応が可能となった時点で連携を図ります。

⑥地理情報システム（ＧＩＳ）

発注情報における工事場所等の情報を地図によりわかりやすく表示でき、様々な利用が考えられます。今後、電子市役所のシステム基盤となる統合型ＧＩＳの導入が可能となった時点で連携を図ります。

ただし、それまでの間は工事場所を示す紙の図面をスキャナで取り込み、イメージファイルにより表示します。

図２．２－２　関連業務



凡例：　連携対象　　連携対象外、将来の連携を考慮した設計を実施

（8）使用するハードウェア及び基本ソフトウェア等

ア．受注者及び発注者端末

受注者の利便性も考慮し、現在も最も流通している以下の製品を使用します。

（ア）ソフトウェア

ａ．ＯＳ

受注者：マイクロソフト　Windows95 以降

発注者：マイクロソフト　WindowsNT 以降

ｂ．ブラウザ

①マイクロソフト　Internet Explorer5.5 以降

②ネットスケープ　Netscape Comunicator4.6 以降

（イ）ハードウェア

ａ．パソコン本体

上記ソフトウェアが動作する PC/AT 互換機

ｂ．ＩＣカードリードライタ

ＪＡＣＩＣコアシステムで認定する複数認証局のうち、使用する認証局の認める仕様に合致したＩＣカードリードライタ

イ．サーバー機器

ＪＡＣＩＣコアシステムのマルチプラットフォーム対応に伴い、本システムの業務及びセキュリティ、信頼性等の要件を満足する製品を選定し使用します。

（ア）ソフトウェア

ａ．ＯＳ

ＪＡＣＩＣコアシステムで対応予定の下記のＯＳから選定します。

①サンマイクロシステムズ　Solaris8

②マイクロソフト　Windows2000Server

③Linux 系ＯＳ

（イ）ハードウェア

ａ．サーバー本体

上記より、選定したソフトウェアが動作するサーバー用機器

ウ．ネットワーク機器

本システムの業務及びセキュリティ、信頼性等の要件を満足する製品を使用します。