第三者的に事実証明可能な電子入札システムの設計と構築

6R－09

高橋 誠治　浦田 昌和　足立 佳彦
ＮＴＴサービスインテグレーション基盤研究所

1.　はじめに

インターネットを利用した電子入札システムを構築する場合、インターネット上の脅威に対処し、安全に文書を配信すると共に、入札者間で不公平のない入札アルゴリズムを用いる必要がある。

従来の電子入札システムの多くは、入札者と発注者の二者で入札に関する情報をやり取りするモデルであり、SSL や S/MIME などの技術を用いて、盗聴、改竄、なりすましといった脅威に対処している[1]。しかし、二者で情報のやり取りを行う場合、情報の送信時刻や送受信事実等を偽る事実否認という問題が発生する。

事実否認に対する有効な対処手段として考えられるものに、信頼できる第三者機関:TTP（Trusted Third Party）を用いて事実情報の認定、証明を行うという方法がある[2]。

本稿では、TTP として電子公証システムを用いることにより電子データの送受信の事実関係を認定、証明、保管する入札モデル、及び、ハッシュを用いた入札アルゴリズムについて説明し、それらを用いたプロトタイプシステムの構築について述べる。

2.　電子入札モデル

TTP を用いて、入札に関する事実情報の認定、電子データ及び事実情報の保管、配達証明を行う入札モデルを図１に示す。TTP は暗号化、デジタル署名付与された安全な通信路を提供し、認証により入札者、発注者を特定すると共に、送信者が文書を送信した時刻、受信者が文書を受け取った事実を認定し、送信文、受領証を保管する。

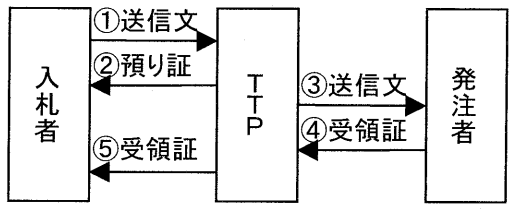

図１：ＴＴＰを用いた電子入札モデル

上記のモデルを電子公証システムを用いて実現するための処理シーケンスを図２に示す。これにより、送信時刻、送受信事実などの事実関係の情報は、第三者である電子公証システムよって認定、保管され、事実否認を防止することが可能となる。

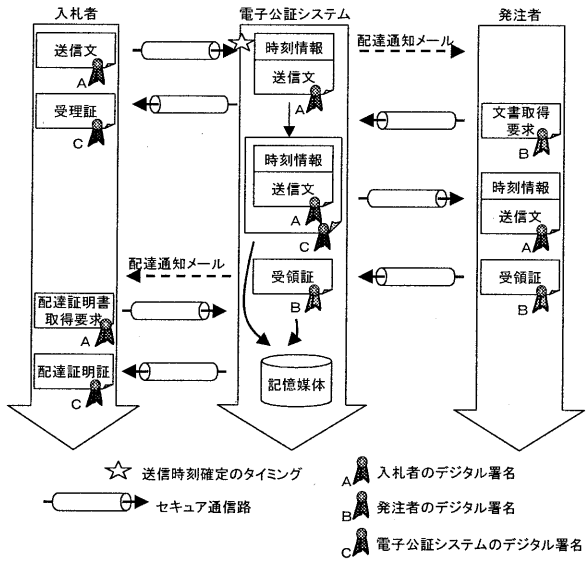

図２：電子公証システムを用いた文書配達のシーケンス

3.　電子入札アルゴリズム

入札では、その公正性を保つために、以下のような条件を満足する必要がある。

入札時：入札金額が記入された入札書の内容を秘匿したまま発注者に提出すること

開札時：秘匿された入札書を開示すると共に、入札書の内容の変更ができないこと

上記の条件を満足するために、図３に示すような

Design and implementation of Electric Sealed-bid Auction System

Seiji Takahashi, Masakazu Urata and Yoshihiko Adachi
NTT Service Integration Laboratories

ハッシュを用いた入札アルゴリズムを用いる。以下よりアルゴリズムのフローに沿って説明を行う。

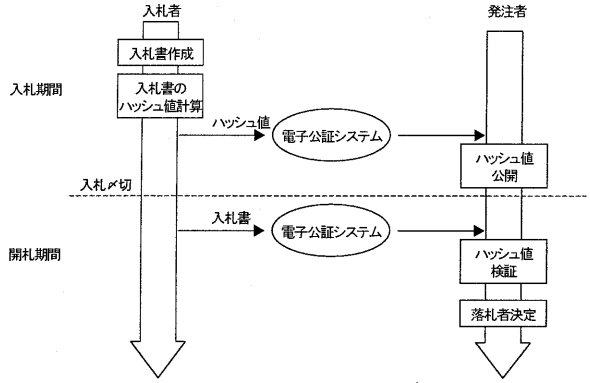

図３：電子入札アルゴリズム

1）入札期間

入札者は、入札金額が記入された入札書を作成する。その後、入札書にハッシュ計算を行い、得られたハッシュ値を電子公証システムを介して発注者へ送信する。発注者は、ハッシュされた入札情報を受信後、そのハッシュ値を公開する。これにより、

① 入札者は、決定した入札金額を秘匿したまま、インターネット経由での入札が可能となる。

② 電子公証システムを介することにより、入札情報、送達事実、送信時刻が証明可能となる。

2）開札期間

入札者は、ハッシュ計算を行う前の入札書を、電子公証システムを介して発注者へ送信する。発注者は、受信した入札書に対するハッシュ値を求め、既に公開されているハッシュ値と比較し検証する。検証後、発注者は落札者を決定し、落札者の入札書を公開する。これにより、

① 入札者が入札後に入札金額を変更していないことを検証することが可能となる。

② 各入札者は落札者の入札書のハッシュ計算を行い、公開されていた落札者のハッシュ値と比較することにより、落札者の正当性を検証することが可能となる。

③ 電子公証システムを介することにより、入札情報、送達事実、送信時刻が証明可能となる。

4. システムプロトタイプの実装

以上のモデル、アルゴリズムを用いた電子入札システムのプロトタイプを構築した。電子公証システムには送受信者特定機能、到達確認機能、盗聴･改竄防止機能、時刻付与機能、原本保管機能を有したシステムを使用し、上記の文書配達シーケンスを実現した。これにより、TTP により事実証明を行う入札モデルが実現可能であることを実証した。図４に入札システム構成図、図５に入札者側の画面イメージを示す。

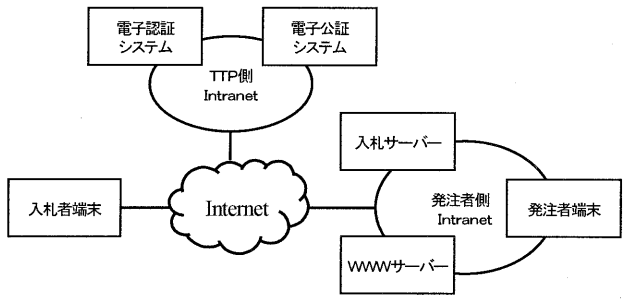

図４：システム構成

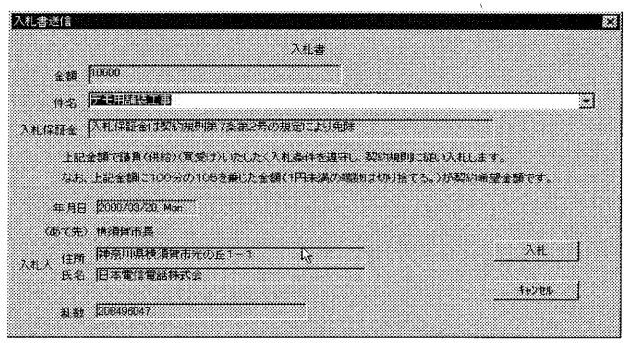

図５：入札者側画面イメージ

5. おわりに

本稿では、電子公証システムを用いて入札における情報のやり取りの事実関係を認定、証明する入札モデル、及び、公正な入札を行うためのハッシュを用いた入札アルゴリズムについて述べ、その実現性を確認した。今後は、本システムの実運用性を評価し、具体化を進めていく方針である。

参考文献

[1] ウォーウィック･フォード　マイケル･バウム：デジタル署名と暗号技術，株式会社プレンティスホール出版（1997）

[2] 岡本龍明：暗号と情報セキュリティ，日経ＢＰ社（1998）