NEWS RELEASE

NTT
日本電信電話株式会社

２００１年４月２５日

第三者に取引の正当性が証明できる国内初の電子入札システムを開発

―国内自治体初の電子入札システムとして横須賀市で採用予定―

日本電信電話株式会社（ＮＴＴ）では、日本政府の「電子政府」構想に基づき政府・自治体が導入計画を進めている公共工事入札や調達入札などの電子化に向けて、第三者にも入札取引の正当性を証明できる「電子入札システム」を、国内で初めて開発しました。

この「電子入札システム」は、ＮＴＴサービスインテグレーション基盤研究所（略称：ＮＴＴ－ＳＩ研）が開発を進めてきたもので、ＮＴＴ情報流通プラットフォーム研究所（略称：ＮＴＴ－ＰＦ研）が開発した『電子認証システム（Trust-CANP *1）』と『電子公証システム（Trust-CYNOS *2）』を組み込むことにより、ネットワーク上での安全性と透明性を実現しました。

これまで多大な時間と経費が必要とされた入札業務の電子化については、すでに複数の電子入札システムが発表されています。しかし、いずれもインターネット上での処理として業務の効率化にとどまっており、入札取引の正当性をもシステム自体で検証できるものはありませんでした。

本システムは、発注者と受注者との間に電子公証システム（サーバ）を介在させることにより、両者間でやりとりされる入札情報等の記録を取得・保管する“公証人”としての機能を持たせている点が、他のシステムにはない特徴です。このため、開札後は、必要に応じて電子公証サーバの情報を公開することで、第三者であっても入札が正当に行われたかどうかを確認することもできます。また、入札情報等の機密を開札時まで保持するための電子入札プロトコル（従来の入札方法では「封筒」に相当）に、暗号方式ではなくＮＴＴが考案したハッシュ値公開型電子入札プロトコルを（後述）を用いているため、面倒な暗号鍵の管理が不要な点も、他のシステムには見られない特徴です。

本システムは、本年９月より、国内自治体初の電子入札システムとして、ＮＴＴコミュニケーションズを通じて神奈川県横須賀市に採用される予定です。

また、ＮＴＴの事業会社を通じて全国の地方自治体等への導入を進めてまいります。

＜主な特徴＞　【図1を参照】

1)　電子入札システム一般として

工事発注情報掲示から入札、開札結果の表示にいたる一連の入札業務フローをインターネット上（ブラウザ上）で実現するため、発注者側も入札者側も入札に関して大幅な効率化が可能です。また、インターネットに接続可能な環境であれば容易に応札できるため、入札者側にとっては受注機会の増大にもつながります。また、そのことにより、談合の抑止力としても効果が望めます。

2)　電子公証システムによる公正性の検証

入札過程の全記録（入札参加申請書、入札書等）を、発注者と入札者の間に介在する電子公証システム（公証サーバ）が取得・保管しているため、公証サーバ自体が「信頼できる第三者機関」(TTP:Trusted Third Party)として、内容証明郵便・配達証明郵便相当の証明機能を発揮します。

このため、発注者側の公開情報を信用するほかなかった従来の入札方法、あるいは他の電子入札システムと異なり、入札過程が公正であったかどうかについて、第三者であっても公証サーバの記録をもとに判断することができます。

3)　暗号鍵の管理・運用が不要な電子入札プロトコル

他の電子入札システムにおいては、電子入札プロトコルに共通鍵分散管理方式など暗号処理を用いています。共通鍵分散管理方式を用いた場合、入札者個別に暗号化・復号鍵を生成・管理する必要があり、管理が面倒という難点があります。

本システムにおいては、ハッシュ値公開型電子入札プロトコル（後述）を用いているため鍵管理の必要がなく、利用者の利便性を高めています。

＜技術のポイント＞　【図2を参照】

本システムに採用されている、ハッシュ値公開型電子入札プロトコルや、認証システム、公証システムは、いずれもＮＴＴ－ＰＦ研が開発した方式・製品です。

とりわけハッシュ値公開型電子入札プロトコルは、ハッシュを巧みに活用した方式であり、入札の正当性の検証においてもキーテクノロジーとなっています。

（ハッシュとは）
　ハッシュとは、電子データを特殊なアルゴリズム（演算）で一定の大きさに圧縮する技術のことです。元の電子データを平文とすれば、ハッシュ計算をおこなって得られる特定長のメッセージダイジェスト（ハッシュ値）は一種の暗号ということができます。
　現代暗号技術に用いられるハッシュでは、ハッシュ値から元の電子データを復元することができない、異なるデータを圧縮したら同一のハッシュ値にはならない（改竄するとハッシュ値が変わる）という条件が実現されています。

（ハッシュ値公開型電子入札プロトコルとは）
　本システムでは電子入札プロトコルにＮＴＴがハッシュ技術を応用して考案した方式を採用しています。
　具体的には、次のような手順で電子入札が行われます。

1)　入札者が応札する際、本システムの電子入札プログラム（ブラウザ）上で入札価格を設定すると、自動的にハッシュ計算が行われ、ハッシュ値が決まります。ただし、入札価格のみではデータとして短すぎるので、実際には、希望する入札価格に特定の乱数を連結して得られるデータにハッシュ計算を行います。乱数も自動的に生成され、電子入札プログラム上に記憶されます。この計算によって得られるハッシュ値からは、元のデータとなる入札価格や乱数を解読することができません。

2)　入札者は、公証サーバを経由してハッシュ値を発注者に送信します。

3)　発注者は、受け取ったハッシュ値を入札情報を公開しているホームページ上に掲載します。この段階では、入札者の会社名等は非公開（受付番号のみの表示）で入札価格は不明です。ホームページの閲覧者には「誰かが入札した」という応札数しかわかりません。

4)　開札時、発注者は封筒を開けたり暗号を復号したりする代わりに、全入札者から、今度はハッシュ計算を行っていない“平文”の入札価格と乱数を送信してもらいます。この“平文”の入札価格を電子的に比較することで落札します。ただし、その金額が入札時と同じものであるかどうかを検証する必要があります。そこで、受注者から送信された入札価格と乱数を電子入札プログラム上でハッシュ計算し、その結果得られるハッシュ値が3)で受け取ったものと同じかどうか確かめます。

5)　落札価格と、その落札者の受付番号、乱数が発注者のホームページに公開されます。第三者は、この情報をもとに、手元の本システム電子入札プログラム上でハッシュ計算を行うことにより、入札が正しかったかどうか確かめることができます。

＜用語解説＞

*1 Trust-CANP
NTT－PF研が開発した電子認証システムです。電子認証システムは、ネットワーク上における本人性の確認などに用いられる公開鍵証明書（実社会の印鑑証明に相当）を発行するシステムです。NTTの電子認証システムは、国産アルゴリズムを含む複数の暗号アルゴリズムをサポートするとともに、リアルタイムな証明書有効性確認ができるなどの特徴があります。

*2 Trust-CYNOS
NTT－PF研が開発した電子公証システムです。電子公証システムとは、電子商取引などにおける、改ざん、なりすまし、事実否認などのトラブルを防ぐため、電子的なやりとりの事実を第三者として証明するもので、実社会の公証役場や内容証明郵便に相当するサービスを提供します。NTTの電子公証システムは、電子認証システムと連携して厳密なユーザ認証や事実証明を行うことを特徴としています。

・（図１）公証を利用した事実証明方式
・（図２）ハッシュを利用した電子入札プロトコル

【本件に関するお問合せ】
ＮＴＴ情報流通基盤総合研究所
企画部 広報担当 倉嶋、佐野、池田
TEL: 0422-59-3663
E-mail: koho@mail.rdc.ntt.co.jp