インターネットにおける電子入札システム

2G－5

工藤 道治
日本アイ・ビー・エム(株) 東京基礎研究所

1. はじめに

電子商取引[8]を始めとしてインターネット上のサービスを利用する環境が整ってきた。今後インターネットを利用した様々なサービスが提供されていくが、本稿では入札という業務を取り上げる。インターネット上で実現する際に考慮すべきセキュリティ要件や従来の研究について説明する。

2. 入札とセキュリティ要件

入札には、公開の場で価格を徐々に競り上げていく公開入札(Open-Bid Auction)と、価格を秘密にして入札し最も安い価格/高い価格の者を落札する封印入札(Sealed-Bid Auction)の二つのタイプがある。本稿では、より複雑なセキュリティ要件が求められる封印入札を対象とする。封印入札では、入札の公正性と安全性を満足させることが最も重要な要件となる。公正性とは、

- 特定の入札者が不正な秘密情報を用いて有利な条件で入札できないこと
- 発注者が恣意的に特定の入札者を落札できないこと

である。前者の例としては、他人の入札価格を事前に不正に知りそれより安い価格で入札することや、誰が入札しているかという情報を不正に知り相手により金額を変えて入札することなどが挙げられる。後者の例としては、入札の締め切り後に発注者が特定の入札者の札を後入れしたり、落札規則に従わず恣意的に落札者を決定したりすることが挙げられる。以上の事から、時間前の開封防止、匿名による入札、入札者の確実な身元の判定、札の後入れの防止、恣意的な落札の防止などのセキュリティ要件を満たすことが必要となる。特に、最後の要件については、参加者あるいは一般の検証者が入札の公正性を検証できるように情報公開等を行い、入札の透明性を実現することが望ましい。これらの要件を満足させる解決方法の中で標準化されているものはなく様々な方法が試みられておりそれらを次節で説明する。一方、安全性の面では、

- 秘密情報が盗聴できないこと
- 情報の改ざんができないこと
- 正当な参加者になりすませないこと

などが挙げられるが、これらは通信の暗号化、整合値による検証、相手認証などで解決でき、デジタル署名やSSL等の既存技術で実現可能な要件である。

3. 従来の研究

これまでに行われてきた研究をまとめると、前節のセキュリティ要件を満足させる入札プロセスとなっており、具体的には、入札者は入札期間中にネットワークに金額データを暗号化して送信し、公正な機関がそれらのデータを安全に保管しておき、開札日以後に札を開き落札者を決める、というものである。ここでの落札とは、あくまでもシステム的に落札者を決定できる作業までであり、審査などの人間系のプロセスは含まない。接続形態としては、参加者全員がサーバに同時にオンライン接続して入札を行う同期型ではなく、入札期間中に自由にデータを送り付けるという非同期型である。運営形態としては、公正な機関が入札を管理するものが多い。しかし公正な機関を必要とせず、参加者の間で公正性を検証するモデルの研究もある[2]。研究の中心は、前節の公正性における時間前の開封防止、匿名による入札、の二つの要件の実現方法にある。特に入札時に実名で入札することの危険性については、

- 入札時に入札者を特定できるデータを送信すると、その情報を保持している組織やサーバが買収の対象になり得るので危険である。
- 落札者を決定するとき、金額と落札規則に基づいてのみ行うべきであり実名は必要ない。

が挙げられる。また、入札者の身元を明らかにする必要がある場合、入札者が名乗り出なくても身元を特定できることが要件とされている。

一方、入札者同士の談合を防止することをシステム要件に挙げている研究は少ない。その理由としては、談合に参加しないアウトサイダーを入札に参加さ

Electronic Sealed-Bid Auction System on The Internet, Michiharu KUDO, Tokyo Research Laboratory, IBM Japan, 1623-14 Shimotsuruma, Yamato, Kanagawa 242, Japan

せる以外に談合を防ぐ有効な手だてがないということが挙げられる[3]。従来の入札に関する研究を表1に示す。

表1　入札に関する従来の研究

比較項目＼研究	無記名入札方式 (1991) [1]	Secure auction method(1996) [7]	応札者証明書方式 (1997) [5]	否認不可匿名入札方式(1994) [2]
共通の入札プロセス	・受注者は入札期間中に金額を暗号化し、匿名で応札する ・公正な機関が開札時間後に札を開け、匿名のまま落札者を決める ・落札者の身元を明らかにする ・開札結果は参加者全てで検証する			同左、ただし公正機関がないため、札は発注者が開ける
公正な機関	必要	必要	必要	不要
金額の時間前開封防止	対称鍵を使った入札金額の暗号値の公開	Secret Sharing 技術による入札金額の分散	入札金額のハッシュ値の送付	入札金額のビットコミットメントの公開
匿名性の保持	身元確認センター	Verifiable Signature Sharing 技術	認証局	否認不可署名技術
落札者を決める機関	公正機関 (センター)	公正機関 (サーバ)	公正機関 (入札管理局)	発注者
落札者の特定方法	身元確認センターが身元を明らかにする	受注者が自ら名乗り出る	認証局が身元を明らかにする	否認プロトコルを全登録者と行う

4. 今後の課題

従来の研究では、時間前開封防止の要件を満たすために入札者から金額情報を二回に分けて送信する必要があった(2パスによる送信)。時間管理やデータ管理を二回行うことなく、一度の金額情報の送信(1パス)により時間前開封防止を行う研究も行われており[4][6]、入札者、発注者におけるシステムの運用性を改善することができる。現行の入札方式では金額情報を主として落札者を決定しているが、今後はデザインや美しさなど金額だけでは判断できない要素も取り入れた総合評価方式の適用も考えられ、それを考慮した入札方式の研究も行われている[6]。また実用化時における課題としては、入札トランザクションの増大に対して処理ボトルネックが発生しないようなシステム構成であることが要求される。またシステム資源の拡大に伴ない、セキュリティ管理のコストが増大しないようにセキュリティモデルを考慮する必要がある。

5. おわりに

インターネットにおける電子入札システムに対する要件をまとめ、従来の研究との対応付けを行った。また、今後の課題として時間に依存した暗号の研究、入札方式の多様化に対する研究、システム構成に対する要求などを説明した。

参考文献

[1] 住田他、"暗号を用いた入札プロトコル," 1991年暗号と情報セキュリティシンポジウム、SCIS91-12C, 電子情報通信学会, 1991

[2] 中西他、"否認不可電子匿名入札プロトコル," 信学技報、ISEC 94-3(1994-05), pp. 19-26, 電子通信情報学会, 1994.

[3] 伊藤他、"談合実験、" 日本の企業システム、東京大学出版会、pp. 261-275、 1996

[4] 工藤、"時間暗号プロトコルとその応用、" 電子情報通信学会、1998 年暗号と情報セキュリティシンポジウム、1.3.A、1998

[5] 工藤、"応札者証明書を用いたインターネット入札プロトコル、" 日本ソフトウェア科学会、インターネットコンファレンス'97、1997、

[6] M. Kudo、"Secure Electronic Sealed-Bid auction Protocol with Public Key Cryptography," IEICE Trans. Fundamentals of Electronics, Communications and Computer Sciences, Vol. E81-A, No. 1, 1998

[7] M. K. Franklin, M. K. Reiter, "The design and implementation of a secure auction service," IEEE Trans. Of Software Engineering, Vol. 22, No. 5, pp. 302-312, 1995

[8] 工藤他、"インターネットにおけるクレジット決済システム 2. 仮想商店システム," 情報処理学会第55回全国大会(4)、pp. 451-452、1997