



平成 12 年 9 月 8 日

各 位

株式会社日本総合研究所

匿名オークションシステムを開発

～世界で初めて、個人情報の登録が不要で、

参加者および管理者の不正発生を排除するオークションを実現～

株式会社日本総合研究所（本社：東京都千代田区一番町 1 6 番、社長：小井戸 雅彦）は東海大学（総長・学長 松前 達郎）工学部の菊池浩明助教授と共同で表記の**匿名オークションシステム**を開発しました。このシステムは情報処理振興事業協会（IPA）の平成 11 年度「次世代アプリケーション開発事業」に採択された「匿名プロトコルを用いた公正なオークションシステムの開発と実証」において開発されたもので、現在開発フェーズを終え、実証の最終フェーズに入っています。

【要旨】

1. システム開発の狙い

個人情報の登録が不要で、参加者および管理者による不正発生を排除する仕組みを実装したオークションシステムを実現しました。

2. 本システムの特長

- ①システム管理者を含めた全ての参加者に対し入札者の匿名性が保たれます。
- ②落札者決定時にも匿名性が保たれます。
- ③落札者の個人情報を知りうるのは売り手に限定されます。
- ④売り手と入札者の結託や匿名性を利用した妨害を防ぎ、不正発生を排除できます。
- ⑤複数のオークション方式を実現し、多様なニーズに対応できます。

3. 今後の展開

平成 12 年 12 月を目処に商品化してオークションエンジンとして販売するとともに、カスタマイズや他の EC 機能を含めたシステム構築全般の相談にも応じます。

<照会先>

株式会社日本総合研究所 サイエンス事業本部

(東京) TEL : 03-3288-4761 FAX : 03-3288-4770

担当 安永通晴 yasunaga@osa.sci.jri.co.jp

宮本昌明 miyamoto@ird.jri.co.jp

(大阪) TEL : 06-6536-7621 FAX : 06-6539-0304

担当 川端博信 kawabata@osa.sci.jri.co.jp

岩崎裕 iwasaki@osa.sci.jri.co.jp

1. システム開発の背景と狙い

インターネット上のオークションサイトは現在広く普及し、多種多様なサイトが立ち上がっていますが、セキュリティ上の数々の問題も同時に拡大しています。オークションへ入札する際には、何らかの個人情報を登録する必要があり、システム管理者の秘密厳守が前提となっています。しかし、これまでにインターネット上での個人情報の漏洩が数多く報告されているために、全面的に信頼することが出来ないのが現状です。例えば、今年になってからは、WEB サーバのリプレースの際に作業の不備で一部プロテクションが外れ十数件の顧客情報が漏出した事件、WEB サーバで顧客の氏名、電話番号等を掲載したページが数日間開放された事件などがありました。

また、入札者を単純に匿名にしても、システム管理者は、個人情報・入札額などを知ることができることから、情報漏洩・結託による不正取引などの発生の可能性は必ず残り問題は解決しません。

インターネット上でのオークションシステムの個人情報漏洩に関する問題を解決する手法は広く世界中で研究されており、匿名オークションプロトコルと総称されます。本システムは従来のもものと根本的に異なり、以下の特長により、**個人情報の登録が不要で、参加者および管理者による不正発生を排除する仕組みを実装したオークションシステムを世界で初めて実現しました。**現在ビジネスモデル特許を申請中です。

2. 匿名オークションシステムの特長

(1) 入札者の匿名性

入札者の登録が不要であるので、入札者の入札額及び個人情報が、他の入札者、システム管理者、売り手の全ての参加者に、最初から最後まで分かりません。

(2) 入札値の機密性

集計処理の際にも匿名性を保ったままで落札者と落札額が決定されます。

(3) 落札者の保護

最終的には売り手に、落札者の個人情報と落札額が知らされ、全ての入札者には落札額が公開される為、自分が落札したのではないことが判明し、これによってオークションが成立します。これ以外の一切の情報は入札者や売り手は勿論の事、システム管理者にも知ることが出来ない仕組みになっています。

(4) 不正発生の排除

各入札者・入札額を入札者間はもちろんシステム管理者、売り手にも秘密にするので入札者間、システム管理者と入札者、売り手と入札者などの結託を防ぎ、不正発生を排除した公正で信頼性の高い取引を実現します。

また、匿名性を利用した入札者の悪意による妨害も排除することができます。

(5) 複数のオークション方式に対応

匿名のファーストプライスオークション、セカンドプライスオークション両方のオークション方式を実現し多様なニーズに対応します。本方式は、一般的な公開型の競り上げ方式ではなく、入札は一回のみで、一度入札すると途中でキャンセルや金額変更はできません。

(注意) ・ファーストプライスオークション

入札値の最も高い金額が落札価格になる方式。

- ・セカンドプライスオークション

落札者は最も高い金額を入札した人としませんが、落札価格は 2 番目に高い金額をつけた入札者の入札値とする方式。

3. 今後の展開

平成 12 年 12 月を目処に商品化して、オークションエンジンとして販売するとともに、カスタマイズや他の EC 機能を含めたシステム構築全般の相談にも応じる方針です。

適用分野としては、入札者の個人情報の漏洩・悪用防止、不正取り引きの防止が強く要求される B2C（企業対個人）C2C（個人間）のオークションや B2B（企業間）の各種取引を考えています。特に、B2B における購買・調達システム、E-マーケットプレイス、各種入札システムなどにおいては、システム管理者および主催者が原理的に不正を出来ない仕組みを構築でき、主催者の公平性・信頼性を大きくアピールできます。

また、B2B 在庫処分オークションや人材派遣のオークションなどでは、入札をしていることを知られたくないという入札企業側の要望にも答えることが出来ます。これら入札者側の要望・売り手側の要望を満たすことにより、インターネットを利用したオークションの新たな市場を開拓していくことができ、本システムに対するニーズは大きいと考えます。

（参考）

1. 論文発表

下記の要領で論文発表します。

- (1) 発表タイトル 「匿名プロトコルを用いたオークションシステムの Java による実装と実証実験」
- (2) 発表学会 コンピュータセキュリティシンポジウム 2000
(<http://www.ee.kagu.sut.ac.jp/css00/>)
- (3) 期間 平成 12 年 10 月 26 日 (木) ～10 月 27 日 (金)
- (4) 会場 学術総合センター(東京)
- (5) 主催 情報処理学会コンピュータセキュリティ研究会
(情報処理学会、電子情報通信学会)

2. 公開実証実験

9 月 12 日～14 日、下記の URL で公開実証実験を行なっています。

<http://210.149.108.158/>

※日本総合研究所のホームページ <http://www.jri.co.jp/pro-eng/anonauc/anonauc.html>
でも紹介しています。

3. 各種オークション方式について

(1) オークションの分類

- ①入札者や現時点の入札価格を公開するか非公開（匿名）にするか。
- ②落札額を最高値（ファーストプライス）とするか 2 番目の価格（セカンドプライス）にするか。
- ③落札値を一回の入札で決定するか、多段階に競り上げ式にするか。

などによって複数の方式があります。

(2) 現在稼働中の代表的オークション

現在インターネット上で開催されているオークションの多くは公開型でファーストプライスの「競り上げ式」といわれる方式で、締切時間内に最も高い値段を入札した人が落札者で、その入札額が落札額となります（イングリッシュオークションとも呼ばれます）。

またその変形としてファーストプライスオークションの競り上げ方式に上限価格設定の自動入札方式のものがああります。入札者があらかじめ自分の予算を指定しておく、システムが現在の最高額よりも少し高い価格を自動入札してくれる仕組みです。これは、入札者の落札額について、セカンドプライスオークションとほぼ同等の効果をもたらします。

いずれも、ニックネームなどを用いたとしても匿名性の保持は十分でなく、個人情報漏洩、不正発生の可能性は残ります。

(3) 今回開発システム

①いずれも非公開型の一回入札方式です。単に非公開ということだけでなく、入札者の情報を秘密にしたまま、実施できるので個人情報漏洩・不正発生などの防止ができます。

②価格決定は、ファーストプライス方式とセカンドプライス方式を用意しています。最高額の決定だけでなく、最低額の決定（官公庁の入札など）にも応用できます。

③セカンドプライスオークションは、締切時間内に最も高い値段を入札した人が落札者で、2 番目に高い値段をつけた入札者の入札額が落札額となるオークション方式です。入札者は自分の出せる限界ま

で入札してもその価格で落札することはないという心理が働き、自分の出せる限界近く入札します。また、有る商品をとにかく手に入れたいというような入札者のニーズにも応える事ができます。

4. 不正発生の排除

当匿名オークションシステムでは、複数のサーバに秘密分散して個人情報・入札額などを送ることから、単独のサーバ管理者が、入札者の個人情報を知ることが出来ない構造になっています。結託したとしても、3人以上のサーバ管理者と売り手が結託しない限り、入札者の個人情報は知ることができません。各サーバは、それぞれ独立した関係にある機関あるいは企業が管理するなどの対策により、複数のサーバ管理者及び売り手が結託する可能性は十分低く出来ます。これによって、入札者の個人情報の漏洩、入札者や管理者の結託による不正などを排除できる仕組みとなっています。

入札者を匿名にすることにより、入札者の安易なキャンセル、入札の妨害などの危険が発生しますが、例えばクレジットカード番号（秘密分散されるため途中の漏洩はありません）を送り決済させることを運営ルール化すれば安易なキャンセルは防止できます。また、その他の妨害については、各管理者の合意のもと再計算すれば妨害者を特定することができます。

5. 匿名プロトコル

ある目標を、匿名性を保ったまま如何にして達成するかのアлゴリズムです。例えば、サーバA,B,Cがそれぞれa,b,cという値を持っていたとします。但し、自分以外のサーバが何の値を持っているかは分からないものとします。このとき、自分の持っている値を秘密にしたまま、全サーバがa,b,cの平均値を知りたいというような目標を実現するものです。匿名オークションプロトコルとは、それぞれのサーバに送られた入札額を秘密にしたまま、落札額がいくらかを計算するアルゴリズムで、匿名プロトコルの一つという位置付けが出来ます。特に、セカンドプライスオークションの場合、最高入札額及び3番目以下の入札額を明らかにしないまま、2番目に高い入札額を計算するところに難しさがあります。