入札者情報を秘匿した分散オークションシステムの実装と実証実験

菊池浩明[†] 上杉栄二[††] 川畑博信[††]
宮本昌明[††] 荻野久美子[††]

秘密分散プロトコルと公開鍵暗号を応用することにより，落札者以外の入札者情報が，売り手以外には秘匿されるオークションシステムを Java で実装し，インターネット環境下での運用性および実用性の評価実験を実施した．その結果，実用上十分な動作速度が得られ，良好なユーザインタフェースが実現されていることを確認した．

Implementation and Experimental Run of Distributed Auction System Which Hides Private Information of Bidders

Hiroaki Kikuchi,[†] Eiji Uesugi,[††] Hironobu Kawabata,[††]
Masaaki Miyamoto[††] and Kumiko Ogino[††]

By applying a secure distributed protocol and a public key encryption, we developed an anonymous auction system in Java language. This system has ability to conceal information about bidder except for a successful bidder and a seller. Usability and practicability of the system are evaluated in internet environment. The results of the evaluation confirms that the execution time is good for practical use and the user interface is suitable for beginners.

1. はじめに

電子商取引における大きな課題の 1 つに個人情報の漏洩の問題がある．度重なる購入履歴や信用情報の横流しは内部犯によるものがほとんどで，これが利用者の組織へ対する信頼を低下させ，電子商取引そのものへの否定的な意識を生じさせている．しかし，かといって利用者を不特定にすると，詐欺などの不法行為を増長させることだろう．たとえばオークションにおける入札者情報を考えよう．もしも登録なしの入札が許されているならば，遊び半分に入札する者が出てきて，それらは落札しても無責任にキャンセルするだけなので，結局オークションそのものを無効にしてしまう．あるいは落札値を意図的に制御するために，架空の入札者を利用して高額の入札を行い，他の利用者を敬遠させることも許してしまう．すなわち，入札値の否認不可性を保証するためには，利用者登録は必然的であると考えられる．実際，インターネット上の電子オークションサービスのほとんどは利用者登録を設けて，不正行為に対処している．たとえば，大手商用オークションサービスの「Yahoo!オークション[1)]」では，料金未払などの詐欺行為を抑止するため，2000 年 9 月にエスクローサービス（出品者と落札者との間で代金や品物の受け渡しを仲介するサービス）を開始し，2001 年 5 月にクレジットカードによる本人確認システムと有料制度を導入した．

しかしながら，その一方で，それらのオークション主催者のすべてが信頼できるわけではない．接続業者などからの個人情報漏洩の事件は後を絶たず，これらを取り締まるための個人情報保護の法整備が進められている[2)]．これらの不正行為の背景には，宣伝，勧誘行為，アンケート調査，顧客管理などの商業活動と個人の嗜好に関する情報の大きな市場がある．しかも，オークションの場合には誰がどのような商品にどの程度の価値を見いだしているかが明らかになってしまうので，単なる個人情報の漏洩よりも深刻である．それゆえ，昨今の個人情報の流出が後を絶たないのであって，こんな現状では，たとえ正当なオークションを実

† 東海大学電子情報学部情報メディア学科
Department of Information Media Technology, School of Information Technology and Electronics, Tokai University
†† 株式会社日本総合研究所サイエンス事業本部情報数理技術グループ
Information & Mathematical Science Technology Group, Science Division, The Japan Research Institute, Limited

現するためでも個人情報の登録に抵抗を感じる利用者は多いことだろう．

そこで，主催者への絶対的な信頼を置く代わりに，暗号プロトコルを用いて公平で安全で信用できるオークションを実現する試みが研究されてきている．Franklin らは，1996 年，秘密分散のアイデアを封印オークション（sealed-bid auction）に適用した[3]．彼らのプロトコルでは，オークション主催者は単独ではなく独立したいくつかのサーバから成っており，不正者が多数（1/3）を超えない限り入札値の秘密が守られる．単独のサーバからは，たとえ不正な管理者がいたとしても，入札値などの重要な情報は取り出せない．さらに，入札値の否認不可を実現するために，入札値と等しい額のオフライン電子現金を秘密分散で主催者に分散する．これにより，たとえキャンセルしたくても，主催者たちの合意のもとでは入札額は自動的に回収されてしまう．彼らの研究に触発されて，その後，落札後も入札値を守るプロトコル[4]，第 2 位の価格だけを計算するプロトコル[5]，しきい復号化を用いて落札者以外の値を秘匿するプロトコル[6]，否認不可署名を用いて否認不可を実現したプロトコル[7]，ハッシュチェインを用いて否認不可を実現したプロトコル[8]，時刻情報の保証により公平性を満たしたプロトコル[11),12)]，第三者機関を活用し入札後の処理を効率化したプロトコル[13)]，その他[9),10)]などが次々に提案された．これらの試みの多くは，入札者の振舞いや通信環境などを理想化した仮定の下で，理論的な興味から提案されたものであり，即現実オンラインオークションに置き換えることを意図したものではない．なぜならば，理論的な仮想状態と現実のオークションの間には次にあげる 2 つの相違点があり，これが大きな課題となっていたからである．

1．複雑な通信や計算処理によるオーバヘッド

主催者の不正を防止するために，単一のサーバを複数のサーバへと分散させて秘密の漏洩を守るアプローチ[3)~6)]では，入札エージェントは多くのサーバと同時に通信する必要がある．通常の Web ブラウザにはこのための機能がなく，専用の入札エージェントを開発するかブラウザに機能拡張する必要が生じる．しかも，複数のサーバへのネットワークのうちどこか一部が故障すると，入札処理そのものを中断させてしまう．また，ダッチオークションのスタイルを利用して敗者の入札値を秘匿するアプローチ[7),8)]では，入札者は落札が終了するまでオンラインで参加し続けていなくてはならず，利用者の利便性を大きく損なう．入札値の種類に対して対数オーダの通信コスト（ラウンド）を実現した[10)]では，単一の処理のために多くの計算コストがかかり，たとえ実現しても落札までに多くの待ち時間が生じて使いものにならないことが予想される．このように，通信環境や利用者の利便性の観点からみると，いくつかのプロトコルは既存のオンラインオークションに遠く及ばない恐れがある．特に，サービス品質に保証がないインターネットにおいては，パケット損失やリンクダウンが日常的で，机上の見積りと大きく食い違う恐れもある．

2．入札者の心理

ゲーム理論などでこれまで考察されていた入札者の振舞いは，一様な規則で理想化されていた．しかしながら，現実の人間の行動には主観に基づく曖昧さがあり，その行動や嗜好は必ずしも単純なモデルでは定式化できない．たとえば，理論的には誘因両立性（入札者の真の評価額を入札することが，最適な戦略となること）を満たすことで知られる Vickrey オークション[17),18)]に対しても，万人がその効果に同意するわけではなく，そのスタイルを採用しているオークションサイトは少ない．Bapna らは，複数アイテムの組合せオークションの普及にともない，入札者の行動が古典的なモデルには従わなくなってきていることを，オークションサイトの実データをもとに指摘し，いくつかの考察を与えている[21)]．このように，より現実的に近づけるためには，理想的なモデルの上だけではなく，実際の入札データや入札者の行動に基づいた検討が必要不可欠となってきている．

そこで，我々は，これらの課題に対して，文献 4), 5) のプロトコルに基づいて，利用者登録のステップを踏まない匿名オークションシステムを実装し，現実のインターネット環境で実際に商品を用意してオークションを開催した．実装システムを用いて通信量や計算時間を測定し，第 1 の課題であったオーバヘッドを同定した．また，参加した入札者にアンケート評価を行い，実装システムの可用性と暗号プロトコルによる信頼性などの効果を検証した．さらに，実験環境で仮想的にオークションを開催し，Vickrey オークションを含むオークションスタイルの違いが落札値にどのように影響するのかを測定した．

本論文では，このオークションシステムの実装方法について述べ，通信コストや利用者の利便性を評価し，プロトコルの設計者が意図したとおりの効果をあげているかを検証する．また，実際に開催したオークショ

ンのログデータや実験結果を示し，入札者の行動を説明するために有益な情報を提供することを目的とする．本論文の構成は次のとおりである．まず，2 章で基本となる匿名オークションプロトコルの概要を述べ，既存のオークション実装技術のいくつかを紹介する．3 章では，システム開発の立場から，実装の問題点を明らかにし，それに対する本実装の設計方針を示す．ならびに，各エンティティの処理フローと管理情報を整理する．4 章では，利用性や入札者心理に関する実験項目，実験環境，および実験結果を示し，それらに基づく考察を与える．最後に，5 章で本報告の結論と今後の課題を述べる．

2. 匿名プロトコル

2.1 概　　要

ここでは，文献 4) をもとにしたオークションプロトコルの概要を述べる．各入札者は，秘密情報として自分の入札者識別子 ID_j を分散されたサーバへ送信していく．識別子には，たとえば，入札者の名前，電子メールアドレス，住所，クレジットカード番号などが用いられる．入札値は，$\omega_1, \ldots, \omega_k$ の k 個の離散値から選ばれる．k 通りの入札値の各々について，その額以上で入札したいときだけ識別子を送るが，そうでない場合は単に 0 を送る．各サーバが秘密を漏らさないまま加算を行うプロトコル（加算のマルチパーティプロトコル）に従って，すべての入札者からの分散された識別子を加算すると，それはその値で入札する意思のある入札者だけの識別子の和になる．ちょうど 1 人だけの入札者がいれば，そのときの和が，落札者の識別子になり，それはすべてのオークション主催者に知られる．

2.2 ファーストプライスオークションプロトコル

Protocol 1

Step 1：公告　オークション主催者は，入札物に関する情報，入札価格幅 $(\omega_1, \ldots, \omega_k)$，全主催者の URL を Web で公開する．また，各主催者に固有の値 $\alpha_1, \ldots, \alpha_m$ も公開する．

Step 2：入札　j 番目の入札者は k 個のランダムな多項式を選ぶ．各多項式は，

$$f_j(x) = s_j + a_1 x + \cdots + a_t x^t \pmod{p}$$

の形式をしており，ここで，t が許容できる不正主催者の最大値である．s_j は，秘密情報であり，入札値 ω と入札者の識別子 ID_j について次式で計算される．

$$s_j = \begin{cases} ID_j & \text{if } \omega \text{ で入札したいなら} \\ 0 & \text{Otherwise} \end{cases}$$

j 番目の入札者は，i 番目 $(i \in \{1, \ldots, m\})$ のオークション主催者に，$f_j(\alpha_i)$ を送信する．

Step 3：開示　決められた開示時間が来たら，i 番目の主催者は，k 個の値の各々について，$F(\alpha_i) = f_1(\alpha_i) + \cdots + f_n(\alpha_i)$ を計算する．すべての主催者が適切な一方向性ハッシュ関数で $F(\alpha_i)$ をコミットした後，各々値を公開する．

Step 4：落札　各々の主催者から公開された $F(\alpha_1), \ldots, F(\alpha_m)$ は，定数項に $s_1 + \cdots + s_n$ を持つ t 次の多項式であり，ラグランジェの補完法を適用して解くことができる．こうして計算される k 個の定数項のうち，0 以外の値をとる最も大きな値が落札値であり，その値が落札者の識別子を表している．この計算は，主催者を介する必要はなく，公開された情報を見た利用者ならば誰でも行うことができる．

2.3 既存のオークション実装技術

以下に，代表的なオークションシステムについて述べる．

eBay, Onsale, Yahoo[1]　これらは代表的な商用オークションサイトである．これらは，Web によるユーザインタフェースにより，登録ユーザから成るオークションサービスを提供している．リアルタイムによる競り上げ，競り下げの基本スタイルのほか，代理エージェントによる自動入札などをサポートしている．リアルタイムであるため，入札値に対する秘匿性はなく，入札者の匿名性はサイト管理者への信頼に依存する．

eMediator[23], **MAGENTA**[22]　ワシントン大学の Sandholm は，eMediator と呼ぶ自動入札エージェントを実装している[23]．また，IBM の Tesauro らは，株式市場のダイナミックスを近似予測する MAGENTA という離散時間のシミュレーターを開発している[22]．これらの試みでは，マルチエージェントの視点から，非同期の環境で多くの入札者が参加するオークションでの入札価格の振舞いをいかに予測するかにその興味がある．

AuctionBot[20]　ミシガン大学の Wellman らは，様々なオークションスタイルを実現する汎用オークションシステム AuctionBot を開発した[19),20)]．AuctionBot は Web ベースのユーザインタフェースを備えているが，サーバ側ではいくつかの特種

表 1 AuctionBot と本実装の相違点
Table 1 The comparison between the AuctionBot and the proposed system.

要素	AuctionBot[20]	本実装
入札クライアント	Web ブラウザ	Java Signed Applet
入札者情報格納場所	共通データベース	各入札クライアント
時刻情報管理	（専用）スケジューラー	メタサーバー
落札者の匿名性	N/A	セラー以外に保証

プロトコルを利用している．インターネットでのパケット到達の不公平性を解消するために，時刻の同期をとるスケジューラを導入している点が特徴的である．スケジューラは，集中管理されたデータベースと連携し，全入札者からの意志を確認した後に，意図的に十分な遅延をとってから，落札処理を行う．一時的なネットワーク障害やある限度までのパケット遅延による不公正性は生じない．特種なオークションスタイルとして，Vickrey オークションを一般化した $M+1$ 位オークションにも対応している[19]．

これらに対して，文献 4) のプロトコルでは，封印方式（sealed-bid auction）を採用している．それゆえ，AuctionBot で考慮された時刻の同期の問題は，ここでは生じない．

また，本論文での試みの中心になっているのは，分散サーバによる秘密分散を用いた実装技術であり，これに関しては，電子選挙の試みがこれまでにいくつか行われている．たとえば，藤岡らはブラインド署名を用いた電子投票システムを実装し，インターネット上に分散させたサーバの上で，投票実験を行っている[25),26]．彼らの方式では，匿名性を保証するために MIX-NET と呼ばれるサーバを直列にいくつも接続して用いる必要があるが，ここでのシャッフルには知識の証明などの大きなオーバヘッドが生じる．また，投票クライアントは独自のシステムになっており，一般ユーザが用いるようにするにはまだ課題が残っている．

3. オークションシステムの実装

3.1 概　　要

本実装では，文献 14) のプロトコルに加えて，最高の入札値を秘匿したまま，セカンドプライスオークションの落札値を決定する匿名プロトコルをサポートすることを目的とした．

提案プロトコルを実装するにあたって，最も大きな課題は入札者の個人情報をどこに格納するかであった．AuctionBot などの従来のシステムのように，主催者が信頼できると仮定してしまえばそこが管理すればよい．しかし，本試みでは，主催者が入札者の個人情報を漏洩したり，入札値を横流ししたりする危険性までを考慮している．したがって，危険な主催者サーバのデータベースを利用することはできない．しかも，最終的には落札者の情報だけをセラー（商品出展者）に提供しなくてはならないので，まったく個人情報を無視するわけにはいかない．

そこで，本実装では入札クライアントに個人情報を保存することとした．クライアントの計算機を攻撃されても耐えられるように，個人情報をセラーの公開鍵で暗号化してログファイルに記録する．これにより，入札者は一度だけ登録処理を行えば何度でもオークションに参加することが可能となり，たとえ落札してもその事実は主催者にさえ漏れない．この各入札者が自分の個人情報を自分で管理するという方針が，共通のデータベースに個人情報を集中管理していた AuctionBot との大きな相違点である．この関係を，**表 1** に整理する．このような入札クライアントをインストールの負担なく利用するには，Java Applet が有効である．ただし，通常の Java Applet ではセキュリティ上の考慮からローカルファイルに書き込む権限がないので，商用の認証局から発行された公開鍵証明書を用いて署名した Signed Applet[24] を採用した．

この Java Signed Applet を用いることで，次にあげるような利点も生じた．

- Java Applet として実装することにより，ユーザの設定作業を最小化できる．
- Java による実装では大きな素数を用いて長い個人情報を含む秘密分散計算が実装できるため，ID の事前登録が不要になる．
- 秘密分散計算に用いる個人情報だけでなく，入札の履歴を残すためのログファイルをローカル側に残すことができる．これにより，入札者の入力にかかる手間を省き，自由に過去の入札結果を確認することや，落札結果の問合せなどの処理を自動化できる．
- 暗号プロトコルを実現するうえで必要な，分散された複数のサーバへ対する送信を同時に自動的に処理可能である．

表 2 システム緒元
Table 2 The system specification.

	メタサーバ	オークションサーバ	セラークライアント	入札クライアント
プラットフォーム	Free BSD 2.2.8	Free BSD 2.2.8	Windows 9x/NT	Windows 9x/NT
ソフトウェア	Apache 1.3.9	Apache 1.3.9	Java VM	MS-IE 5.x
暗号アルゴリズム	N/A	N/A	El Gamal	El Gamal
開発言語	C++ (gcc2.95.1)	C++ (gcc2.95.1)	JDK 1.1.8	JDK 1.1.8
格納情報	オークション開催情報	入札情報，落札結果	セラー，商品，登録情報	入札者個人情報，入札結果

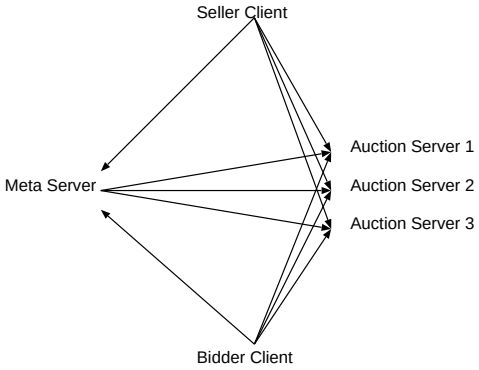

図 1 システム構成図
Fig. 1 The system architecture.

3.2 システム構成

本システムは，以下のサブシステムから構成されている．システムの構成を**図 1** に，その緒元を**表 2** に，および，暗号化と秘密分散に用いたパラメータを**表 3** にそれぞれ示す．

- 入札者が使用する入札クライアント．
- セラーが使用するセラークライアント．
- 入札情報を受信して記録し，集計計算を行うオークションサーバ．
- オークションの進行を制御し，オークションの開催情報を管理するメタサーバ．

3.3 処理の流れ

Step 1：公告 セラーは，オークションにかける商品の情報と，入札価格帯，セラーの公開鍵，締切時刻をメタサーバに登録する．メタサーバはセラーから受け取った上記の情報と，各オークションサーバの URL と秘密分散計算に用いる各オークションサーバに固有の値を，各入札クライアントからの問合せに対して送り返す．

Step 2：入札 各入札者は，匿名オークションプロトコルにしたがって，各価格帯への入札情報を作成し，指定された複数のオークションサーバへ送信する．入札情報を作成する際に用いる入札者の個人情報として，今回は入札者の氏名とメールアドレスを含む文字列をセラーの公開鍵で暗号化したものを用いた．これは，オークション終了後に，セラーが落札者と連絡をとることができるようにするためである．これにより，落札者の確定後に，落札者の個人情報がセラー以外に漏れることを防止できる．

表 3 暗号化および秘密分散アルゴリズム仕様
Table 3 The specifications of encryption and secret sharing algorithms.

個人情報暗号化方式	1,024 bit El Gamal 暗号
秘密分散に用いる素数 p の大きさ	126 byte（1,008 bit）
多項式次数	可変（3 次）
入札者個人情報サイズ	123 byte

Step 3：締切と集計の指示 メタサーバは締切時間が来たら，各オークションサーバに入札受付の締切と集計の指示をする．

Step 4：落札値の決定 オークションサーバは協力して落札値と暗号化された状態の落札者の個人情報を復元する．

Step 5：確認 セラーは落札値と落札者の個人情報をオークションサーバに問い合わせて，自分の秘密鍵で復号化する．正常に復号化できれば，落札者が確定して個人情報が得られたことになる．入札者は，落札値と落札者の個人情報をオークションサーバに問い合わせて，自分が送信した入札値と暗号化された個人情報と比較することで，自分が落札できたかどうかを確認することができる．

3.4 セラークライアント

セラーの公開鍵・秘密鍵の生成機能と，メタサーバに登録するオークションの情報の管理機能を持つ．また，オークション終了後に結果情報を受け取り，落札者の個人情報を秘密鍵で復号化して内容を確認する機能を持つ．

セラークライアントは一般に公開せず，信用のおけるユーザに実験への参加を依頼するため，Java のアプリケーションとして実装して直接配布した．セラークライアントはセラーのローカル側に以下のファイルを残す．

(1) セラー情報ファイル

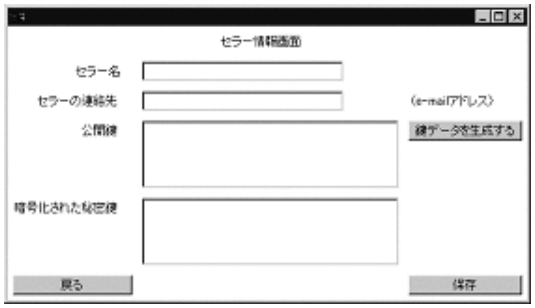

図 2 セラー情報画面
Fig. 2 The snapshot of seller management.

図 3 オークション情報設定画面
Fig. 3 The snapshot of auction management.

図 4 入札画面
Fig. 4 The snapshot of bidding.

図 5 入札結果表示画面
Fig. 5 The snapshot of displayed auction result.

セラーの氏名，連絡先とともに，生成した公開鍵・秘密鍵を格納する．その内容の管理は**図 2** のセラー情報画面で行う．

(2) 商品情報ファイル
オークションにかける商品の品名，価格帯，締切時刻などの情報を格納する．価格帯を変更してオークションを再開する場合の手間を軽減するために用いる．**図 3** のオークション情報設定画面で操作する．

(3) セラークライアントログファイル
過去にセラーが登録したオークションの情報を記録する．これを参照することで入札結果を問い合わせるオークションサーバのアドレスを知ることが可能になる．

3.5 入札クライアント

入札者の送信する個人情報をローカルで管理し，オークションの開催情報と，入札者が指定する入札値から秘密分散計算を行って，入札情報をオークションサーバに送信し，オークション締切後に結果情報を受け取り，入札者が落札できたかどうかを確認する機能を有する．**図 4** に入札画面を示す．オークションの条件が表示され，入札値を入力して各オークションサーバへ送信する様子が確認できる．

入札クライアントは，入札者のローカル側に以下のファイルを残す．

(1) 個人情報ファイル
入札者の氏名，メールアドレスなどの情報を格納する．一度登録した情報を繰り返し入力する手間を省くために用いる．

(2) 入札クライアントログファイル
オークションへの参加履歴として，オークションの条件や実際に使用したオークションサーバのアドレス，自分が送信した暗号化された状態の個人情報を含む．
この自分が送信した暗号化された状態の個人情報とオークションサーバからの入札結果情報を比較することで，自分が落札したかどうかを，入札者が判定できる．**図 5** の入札結果表示画面で選択できるオークションサーバのアドレスは，このログファイルから取得する．

3.6 メタサーバ

メタサーバは，セラークライアントからオークションの開催情報受け取り，入札クライアントからの問合せに対して，開催情報を送信する．オークションの締切時刻が来ると，各オークションサーバに対して，入札受付の締切と，集計計算を行う指示を出す．集計計

算のタイミング処理は，メタサーバが指示する．次のファイルを管理する．

- 全サーバリストファイル
  すべてのオークションサーバの情報（URL）．
- アクティブサーバリストファイル
  オークション開催情報を各オークションサーバに送信した際，正常なレスポンスを返してきたオークションサーバ一覧．
- オークション情報ファイル
  セラークライアントから登録されたオークション情報．
- メタサーバログファイル
  メタサーバ管理者の作業内容やオークションサーバのレスポンスの履歴，およびオークション登録情報の受信履歴．

3.7 オークションサーバ

オークションサーバは入札クライアントからの入札値の機密を保持し，集計プロトコルに従った計算結果を集計後に公開する．次のファイルを管理する．

- 開催オークションファイル
  現在開催されているオークションのオークション開催情報．
- 入札情報ファイル
  オークションサーバが入札クライアントから受信した入札情報．
- 入札結果ファイル
  すでに終了したファーストプライスオークションの集計結果．
- 落札者ファイル（Vickrey）
  すでに終了したセカンドプライスオークションの落札者の暗号化された個人情報．
- 落札価格ファイル（Vickrey）
  すでに終了したセカンドプライスオークションの落札価格．
- オークションサーバ活動ログファイル
  オークション処理の開始，入札結果情報，入札結果の問合せ記録．
- 入札ログファイル
  入札クライアントからオークションサーバへの入札情報の受信記録．
- 中間結果ファイル
  集計計算の中間結果．

ここで，（Vickrey）は，第 2 価格入札方式にのみ利用されるファイルを指す．

表 4 サーバの実験環境
Table 4 The experimental environment for servers.

種類	CPU/Memory	帯域 [kbps]
メタサーバ	Pentium III 500 MHz 192 MB	128
サーバ 1	Pentium 166 MHz 96 MB	128
サーバ 2	Pentium III 500 MHz 192 MB	128

4. 実証実験とその評価

4.1 実験項目

(1) インターネット環境でのシステムの通信処理時間測定
LAN やダイヤルアップなどのいくつかの環境において，入札クライアントを利用し遅延時間を測定した．

(2) ユーザインタフェース，レスポンスなどの利用性評価
実際にオークションに参加した利用者に，匿名でアンケート調査を行い，ユーザインタフェースや利用性などを調査した．

(3) 匿名性が入札者に与える心理的効果の評価
匿名性を保証したオークションとそうでないオークションを 2 種類開催し，匿名性がオークションに及ぼす心理的効果をアンケート調査と実際のウェブアクセスパターンから同定した．

(4) オークションスタイルが落札値に及ぼす効果の評価
第 1 価格入札と第 2 価格入札というスタイルの違いが，落札値にどのような影響を及ぼすかを，擬似的なオークションを行って測定した．

4.2 実験環境

実際のインターネット環境でのレスポンスや一般のインターネットユーザの操作性に対する評価を見るため，インターネット上に 3 台のオークションサーバを配置し，うち 1 台がメタサーバを兼ねる構成で実験を行った．**表 4** に使用したサーバのスペックを示す．

本システムの入札クライアントでは，原理的には任意の長さの情報を個人情報として送れるが，本実験では，入札者の氏名とメールアドレスを含む情報（最大 123 バイト）をセラーの公開鍵で暗号化したものを入札情報として用いることとした．この長さは，個人情報の事前登録なしに，落札者が安易にキャンセルすることを防止するのに有効な電子決裁に必要な情報（たとえば，クレジット番号など）を入札情報の中に含むのに，十分な長さといえる．

4.3 インターネット環境でのシステムの通信処理時間

ファーストプライス方式の模擬オークションを，種々の価格帯数 k で実施した．入札クライアントは，現在の平均的なインターネットのユーザを想定して Pentium（133 MHz）から Pentium III（750 MHz）まで合計 27 台を使用した．そして，入札は通常のインターネット接続環境として想定される以下に示す通信環境から行った．

(a) 専用線で接続された社内 LAN からのインターネットへの接続．
(b) ダイヤルアップによるモデムでのインターネットへのアナログ接続．
(c) ダイヤルアップによる ISDN によるインターネットへの接続．
(d) ケーブルテレビからのインターネットへの接続．

図 6 にファーストプライスオークションにおける，入札者の通信環境別ごとの，入札クライアントとオークションサーバ間の入札情報の送信速度を示す．ファーストプライスオークションでは，計算時間，通信時間が価格帯数 k に依存する．今回の実験環境では，価格の種類 1 つにつき，約 400 byte 通信量が増える．したがって，接続された帯域に応じて，その通信遅延時間も比例する．

この実験で計測した時間は，暗号化・秘密分散計算にかかった時間（「入札」ボタンが押されてから実際に送信が開始されるまでの秒数）と，それぞれのオークションサーバへの送信にかかった時間の平均である．

送信速度は，通信環境により大きく依存すると考えていたが，結果はあまり差がなく，しかも，いずれも回線速度より期待される通信速度が出ていない．入札した時間帯は，深夜（午後 10 時〜午前 8 時）を除く全時間帯に分散していたので，本実験が特殊な環境であったとは考えられないので，本実験の結果が，現実のインターネットでの平均的な通信速度であると考えられる．

実験結果から，ある価格帯 k の秘密分散にかかる時間と 1 台のサーバへの送信にかかる時間を

$$T_1(k) = 0.032k - 0.118$$
$$T_2(k) = 0.0478k - 1.0696$$

で近似する．ここで，k は価格帯数である．入札クライアントで許される遅延の限界を T^* とすると $T^* = T_1(k) + 3T_2(k)$ より，k の上限値を求めることができる．たとえば，$T = 60$ の場合で $k < 433$，$T = 180$ の場合で $k < 1255$ となる．以上の考察により，本システムでは価格帯数約 1,000 までなら，入札に要する時間は 3 分程度となる．より実用的なレスポンスを得るためには，さらに広い帯域か価格帯数をより絞り込んだオークションを開催する必要がある．

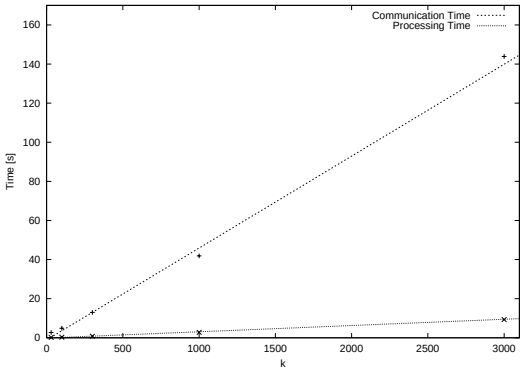

図 6 入札クライアントの計算時間と通信時間
Fig. 6 The execution and communication time for bidding client.

表 5 入札クライアントの操作性
Table 5 The usability of bidding client.

選択項目	割合 [%]
直感的に操作できる	50
マニュアルを見ながら操作できる	33
思うように操作できない	15
無回答	3

表 6 入札クライアントの体感速度
Table 6 The sensible speed at bidding client.

選択項目	割合 [%]
非常に早く感じる	4
早く感じる	25
普通	50
遅く感じる	18
非常に遅く感じる	3

4.4 ユーザインタフェース，レスポンスなどの利用性

上と同じ実験環境で 13 回のオークション実験を行い，入札クライアントアプレットを含むページでアンケートを実施，合計 110 名からアンケートを回収した（実際に入札クライアントを起動したユーザの数で，実際には入札を行っていない者も含む）．

セラーは，株式会社講談社に依頼し，商品として，「サイン色紙付きのキャラクターグッズ」,「著者のサイン入りの書籍」を用いた．入札クライアントの体感速度と入札クライアントの操作性のアンケートの結果を，それぞれ，**表 5** と **表 6** に示す．

体感速度のアンケートでは,「普通」「速く感じる」「非常に速く感じる」の回答者の合計は約 80%であり，

表 7 入札者のアクセスの割合
Table 7 The access patterns of bidders.

入札者の行動	匿名 [%]	非匿名 [%]
エントリ観覧の後入札画面に至った	58	35
入札画面観覧の後入札に至った	55	32

操作性に関するアンケートでも，約半数が直感的に操作できた．よって，良好なユーザインタフェースが実現されていることと結論づける．

4.5 匿名性が入札者に与える心理的効果

匿名性が入札者の行動にどのような影響を与えるかを明らかにするために，次のような非匿名のオークションサイトを用意し，両者に同じ商品を置いて入札者の行動を調べた．

- 入札者の個人情報登録を行う CGI.
- オークション商品を登録する CGI.
- 入札値を送信する CGI.
- オークション商品ごとの入札価格一覧を表示する CGI.

このサイトでは，1) エントリ画面，2) 入札画面，3) 入札の 3 つのステップを踏んで入札値の受付を行う．しかし実際には，種々の理由から 1) や 2) の途中で止めてしまうユーザも多い．すなわち，そのキャンセルする割合が高いほど，ユーザの抵抗が大きいことと解釈できる．このサイトを一定期間運用した後，サーバに残ったアクセスログから集計した入札者のアクセスパターンを**表 7** に表す．匿名オークションと非匿名オークションサイトのそれぞれで集計しているが，匿名オークションの場合だけ Java applet のダウンロードが生じていることに注意が必要である．また，商品による差を最小化するため，キャラクターグッズと書籍の 2 種類の商品についてオークションを行っている．

この結果が示すように，匿名と非匿名とで入札者の行動に変化が観測された．多くの場合は，非匿名サイトで強いられる個人情報の登録が大きな抵抗になっていることが予想される．入札画面を見て入札せずに去っていった人の理由として，本システムでは匿名性が保証されるといっているが，そのこと自体が信じられないと考える人や，入札する意志はないが個人的興味で入札画面を見た人がいたためと考えられる．一方，非匿名オークションの場合には，個人情報の登録に対する抵抗が最も大きな要因であろう．

そこで，実際の入札者に匿名性に対するアンケート調査を行った．匿名性を保証されることが重要であると思うかとのアンケートの結果を**表 8** に示す．これによると,「大変重要」または「重要」と回答した利用者は匿名と非匿名オークションのそれぞれで，72%と 75%であった．

表 8 匿名性の重要度についてのアンケート結果
Table 8 The result of questionnaire on significance of anonymity.

選択項目	匿名 [%]	非匿名 [%]
大変重要	29	46
重要	43	29
重要でない	14	25
まったく重要でない	9	0
無回答	5	0

4.6 オークションスタイルが落札値に及ぼす効果

落札価格決定の違いによる入札値の分布を調べるため，非匿名による次のような模擬オークションを実施した．

被験者は，東海大学の学生 71 名（男 54 名，女 17 名）で，商品はインターネット上で実際に広告が見られる商品から，一般の商店で販売されていて容易に手に入り，価格は容易に知ることができる 80 種類を選んだ．商品の一覧画面と入札用画面を用意する．このとき被験者をランダムにグループ 1，グループ 2 の 2 つにに分ける．用意した 80 種類の商品を 40 種類ずつ 2 つに分け，前半 40 種類をグループ 1 はファーストプライス方式で，グループ 2 にはセカンドプライス方式で入札してもらい，残り 40 種類を逆にして落札値を決定する．被験者がより真剣に入札価格を考慮するように，実験参加者間に次の競争のルールを設定する．落札者のみに落札値と商品の実際の市場価格の差がポイントとして与えられる．ただし，ポイントはマイナスもありうるので，むやみに落札しては負けてしまう．落札者以外（オークションの敗者）にポイントはつかない．被験者間で入札値について相談することは禁止する．

実験結果を**表 9** に示す．80 種類の商品には価格の安いものと高いものの差が大きいため，入札値（と落札値）の市場価格に対する比を求めている．この値が大きければ大きいほど，オークションによって値が吊り上がっていることを示している．まず，入札値が両オークションスタイルで変化するかに着目すると，入札値のばらつき程度も平均値もそれほど有意な差は見られなかった．一方，落札値を見ると，ファーストプライス方式がセカンドプライスに対して高い値になっていることが観測できる．理論的には，セカンドプライス方式の方が真の評価額に近づくために，高く落札することが予測されたが，今回の実験結果はそのことを裏付けることには至らなかった．

表 9 オークションスタイルによる入札値と落札値の違い
Table 9 The difference between auction styles in bidding prices and winning bids.

統計情報	ファーストプライス		セカンドプライス	
	入札値/市場価格	落札値/市場価格	入札値/市場価格	落札値/市場価格
平均	1.18	7.08	1.24	3.21
標準偏差	0.83	10.3	0.83	2.58
最小値	0.10	0.34	0.07	0.63
最大値	5.07	70.3	5.07	20.8

5. 結　　論

暗号プロトコルを用いて主催者の不正を不可能にした匿名オークションシステムを開発し，実際にオークションを行った結果を基にその評価を行った．入札クライアントのレスポンス測定，入札者のアンケート調査，および，オークションサーバのログ解析などの評価を行い，本システムが実用的なレベルにあることを明らかにした．

実装にあたって最も大きな課題であった個人情報の登録方法について，本実装では Java Signed Applet を用いて入札クライアント自身に管理させる特徴的な方式を採用した．また，もう 1 つの大きな興味であった，現実の入札者の振舞いに対して，多くの有益な実データが得られた．その中の 1 つは，従来理論的に市場価格を最適化することで知られているセカンドプライスオークション（Vickrey オークション）が必ずしもファーストプライスより高額な落札値を得られなかったことを示した．これらの興味深い入札者の振舞いに対して，十分に説明できる行動モデルを同定することを今後の課題とする．

本論文では十分に述べることができなかったものに，本システムでサポートしていたセカンドプライス方式のプロトコル[5]がある．オークションサーバ間での大きな通信コストがかかり，入札者の通信コストは小さかったが，サーバ数が増えたときには実用的でないことが明らかになった．これらについても，より厳密な評価を今後進めていく．

参 考 文 献

1) Yahoo!オークション．http://auctions.yahoo.co.jp/（2002 年 3 月参照）．
2) 朝日新聞，特集—個人情報保護法案．http://www.asahi.com/national/kjhh/index.html（2002 年 3 月参照）．
3) Franklin, M.K. and Reiter, M.K.: The Design and Implementation of a Secure Auction Service, *IEEE Trans. Softw. Eng.*, Vol.22, No.5, pp.302–312 (1996).
4) Kikuchi, H., Harkavy, M. and Tyger, J.D.: Multi-round Anonymous Auction, *Proc. 1st IEEE Workshop on Dependable and Real-Time E-Commerce Systems*, pp.62–69 (June 1998).
5) Harkavy, M., Tyger, J.D. and Kikuchi, H.: Electronic Auctions with Private Bids, *3rd USENIX Workshop on Electronic Commerce Proceedings*, pp.61–74 (Aug. 1998).
6) Sako, K.: An auction protocol which hides bids of losers, *Proc. PKC'2000*, pp.422–432 (2000).
7) Miyazaki, S. and Sakurai, K.: A bulletin board-based auction system with protecting the bidder's strategy, *Trans.IPSJ*, Vol.40, No.8, pp.3229–3336 (1999).
8) Kobayashi, K. and Morita, H.: Efficient sealed-bid auction with quantitative competition using one-way functions, Technical Report of IEICE, ISEC99-30, pp.31–37 (1999).
9) Naor, M., Pinkas, B. and Sumner, R.: Privacy preserving auctions and mechanism design, *ACM Workshop on E-Commerce*, pp.129–139 (1999).
10) Cachin, C.: Efficient private bidding and auctions with an oblivious third party, *ACM Conference on Computer and Communications Security*, pp.120–127 (1999).
11) Stubblebine, S.G. and Syverson, P.F.: Fair On-Line Auctions without Special Trusted Parties, *Proc. Financial Cryptography 1999*, LNCS 1648, pp.230–240 (1999).
12) Kudo, M.: Secure electronic sealed-bid auction protocol with public key cryptography, *IEICE Trans. Fundamentals*, E81-A(1), pp.20–26 (1998).
13) Watanabe, Y. and Imai, H.: Reducing the Round Complexity of a Sealed-Bid Auction Protocol with an Off-Line TTP, *Proc. 7th ACM Conference on Computer and Communication Security*, pp.80–86 (2000). in *Proc. of SCIS2000*, B09, pp.1–8 (2000).
14) 菊池浩明，中西祥八郎：利用者登録の不要な匿名オークション，*Proc. CSS'98*, pp.243–248 (1998).

15) 菊池浩明，堀田信司，安部謙介，中西祥八郎：匿名オークションを実現する分散システムの実装と評価，*Proc. CSS'99*, pp.123–128 (1999).
16) 宮本昌明，菊池浩明，荻野久美子：入札値を秘密にしたまま次点の落札値だけを計算する分散オークションサーバ，DICOMO 2000 シンポジウム論文集，pp.547–552 (2000).
17) Sakurai, Y., Yokoo, M. and Matsubara, S.: A limitation of the generalized Vickrey auction in electronic commerce: robustness against false-name bids, *Proc. AAAI annual conference* (1999).
18) Milgrom, P.: Auctions and bidding: a primer, *Journal of Economic Perspectives*, Vol.3, No.3, pp.3–22 (1989).
19) Wurman, P.R., Walsh, W.E. and Wellman, M.P.: Flexible Double Auctions for Electronic Commerce: Theory and Implementation, *Decision Support Systems*, Vol.24, pp.17–27 (1998).
20) Wurman, P.R., Wellman, M.P. and Walsh, W.E.: The Michigan Internet AuctionBot: A configurable auction server for human and software agents, *2nd Int'l Conf. on Autonomous Agents* (May 1998).
21) Bapna, R., Goes, P. and Gupta, A.: Insights and Analyses of Online Auctions, *Comm.ACM*, Vol.44, No.11, pp.42–50 (2001).
22) Tesauro, G. and Das, R.: High-Performance Bidding Agents for the Continuous Double Auction, *ACM Conference on Electronic Commerce* (*EC-01*), pp.206–209 (Oct. 2001).
23) Sandholm, T.: Issues in Automated Negotiation and Electronic Commerce Extending the Contract Net Framework, *Proc. 1st Int'l Conference on Multi-agents Systems*, pp.328–335 (1995).
24) Java Development Kit (JDK) 1.1.x — Signed Applet.
http://java.sun.com/security/signExample
(2002 年 4 月参照).
25) Fujioka, A., Okamoto, T. and Ohta, K.: A Practical Secret Voting Scheme for Large Scale Elections, *AUSCRYPTO '92*, pp.244–251 (1993).
26) 藤岡ほか：実用的な電子投票方式の実装および実験，暗号と情報セキュリティシンポジウム SCIS2000, SCIS2000-48 (2000).

(平成 13 年 12 月 20 日受付)
(平成 14 年 6 月 4 日採録)

菊池　浩明（正会員）

1988 年明治大学工学部電子通信工学科卒業．1990 年同大学院博士前期課程修了．1990 年（株）富士通研究所入社．1994 年東海大学工学部電気工学科助手．1995 年同専任講師．1999 年同助教授，1997 年カーネギーメロン大学計算機科学学部客員研究員．2000 年東海大学電子情報学部情報メディア学科助教授，現在に至る．博士（工学）．ファジィ論理，多値論理，ネットワークセキュリティに興味を持つ．1990 日本ファジィ学会奨励賞，1993 情報処理学会奨励賞，1996SCIS 論文賞．電子情報通信学会，日本ファジィ学会，IEEE，ACM 各会員．

上杉　栄二

1987 年京都大学理学部宇宙物理学科卒業．同年日本情報サービス（株）（現：（株）日本総合研究所）入社．主に原子力分野での人工知能の応用，インターネット関連業務の開発に従事．現在，愛媛県立八幡浜工業高校非常勤講師．

川畑　博信

1979 年 3 月大阪大学大学院工学研究科原子力工学専攻修士課程修了．同年 4 月日本情報サービス（株）（現：（株）日本総合研究所）入社．現在，サイエンス事業本部情報数理技術グループマネジャー．オープンシステム系の情報処理システムの開発に従事．

宮本　昌明

1998 年 3 月北海道大学大学院理学研究科数学専攻修了．同年 4 月（株）日本総合研究所入社．現在，サイエンス事業本部情報数理技術グループ．オークション匿名プロトコルの研究・実装のほか，経営戦略・情報化戦略のコンサルティング業務に従事．

荻野久美子

1999 年 3 月津田塾大学学芸学部数学科卒業．同年 4 月（株）日本総合研究所入社．現在，サイエンス事業本部情報数理技術グループ．オークション匿名プロトコルの研究・実装のほか，主にオープンシステム系の情報処理システムの開発に従事．