インターネットのあるキャンパス訪問 17

埼玉大学
経済学部
川越研究室

インターネットの研究は、理工学分野からのアプローチだけではなくなってきた。今回訪問した川越研究室では、経済学の分野からインターネットの暗号プロトコルを研究している。経済学の立場から暗号プロトコルにアプローチした研究とは、どのようなものなのだろうか。

URL http://www.saitama-u.ac.jp/

埼玉大学プロフィール

◎所在地

埼玉県浦和市下大久保255

◎沿革

旧制の浦和高等学校、埼玉師範学校などを母体として昭和24年に創設された。5つの学部と5つの大学院研究所を設置しおり、キャンパスの大きさは中規模ながら首都圏の総合大学としての機能を持っている。

◎ネットワーク環境

学内は、埼玉大学全域ネットワーク（SONET）が構築されており、ATMネットワークによって各学部の施設と接続されている。外部のネットワークへは、学術ネットワークであるTRAINと1.5Mbpsで接続しており、そこからインターネットにつながっている。

学生は、申請をすればアカウントが発行され、電子メールなどのインターネットサービスを総合情報処理センターなどで受けることができる。

川越研究室のホームページ
URL http://yaksi.eco.saitama-u.ac.jp/~kawagoe/

経済学が専門ですが、暗号プロトコルの研究を始めたきっかけを教えてください

私が暗号プロトコルに興味を持ち始めたのは去年の冬頃なのですが、埼玉大学のある先生が、デジタルキャッシュに関してレビューした文献を紹介してくれました。これが暗号プロトコルとか電子商取引などの話題を知ったきっかけになったんです。

そこで、その分野を調べているうちに暗号プロトコルに関する基本概念を書いた論文を見つけました。この中で興味深かったのが、暗号プロトコルをゲーム理論と比較するという部分だったのです。私は、経済学の中でもゲーム理論が専門なのですが、この論文で比較対象としてあげられていたゲーム理論は、私からすると時代遅れの理論だったのです。

しかし、さらに考察していってみると、暗号プロトコルの目指すものとゲーム理論が考えていることというのは、近いんだけれどもどこかが違うという印象を持ったのです。

川越敏司先生（中央）と研究室のみなさん

どこが違う点なのでしょうか

暗号理論は、情報の送り手が暗号プロトコルを通じて取り引きを成立させるとき、盗聴とかなりすましとかの妨害をさせない、あるいは妨害があれば妨害されたことが分かるようなプロトコルを作るのが目標です。で、暗号理論というのは、基本的に自分の持っている情報は正直に出すというのが前提条件です。

これに対してゲーム理論は、人は情報を正直に言わないというのが前提になっています。もし、嘘の情報が流されるとすると、情報自体は暗号プロトコルによって妨害なくやり取りできたとしても、取り引きの結果というのは望ましいものにはならない可能性が出てきます。ゲーム理論は、そういった自分の情報を正しく出さない場合を想定し、別の取り引きのメカニズムを考えるのです。その目指すところは、嘘をつきたいんだけれども、一番利益が上がるような嘘のつきかたは、結局正直な情報を出すのがベストであるという結果に導くメカニズムを作るということなのです。それがゲーム理論の発想なのです。

つまり、公正な取り引きの結果を導くという目的の中で、暗号理論というのは情報の通信の妨害をいかに防ぐかということが問題になります。それに対してゲーム理論は、情報そのものをいかに正直に出させるかというのが問題になるのです。

その違いに気が付いたわけですが、暗号理論のほうではゲーム理論のことを知らな

研究室の蔵書は、経済学の分野だけでなく工学や文学など多岐にわたっている。

研究室のひとコマ。厳しい中にも笑いが･･･。

い。ゲーム理論のほうでは、暗号理論のことを知らない。つまりお互いが補完しあう関係にあるのではないかと考えたのです。

研究内容をおおまかに教えていただけますか

暗号理論とゲーム理論の違いを踏まえたうえで、お互いの特徴を活かしたメカニズムを作ろうというのが私の研究です。つまり、盗聴やなりすましなどの妨害行為もできないし、たとえ人が自分のために嘘の情報を流すというような戦略的な行動をとっても、結果的に公正な取り引きが達成できるメカニズムを作ることなのです。それに関して、電子オークションのメカニズム構築を研究しています。

この電子オークションの目標は、あるものを買いたいという人が集まってインターネットでオークションをしながら値段を決めるというとき、その値段が市場で取り引きされたときと同じくらいの妥当な価格になるようなゲーム理論のメカニズムを用います。それと同時に、オークションしている間は、盗聴やなりすましができないようにするということなのです。

具体的には、どのような手順がとられるのですか

たとえば、美術品などの入札を想定してみましょう。まず、発注者は入札（オークション）の告知を行います。入札者はそれへの参加申し込みをします。それと引き換えに、参加受け付けのIDが発行されます。このIDと入札者が付けたいと思っている値段のセットに対して乱数をかけます。このような形で、値段が封印されたものを発注者のほうに返します。それを発注者が受け取ると、電子署名が自動的に付つけられ、入札者に送り返されます。これで、各入札者の入札は終了です。次に、入札者と落札価格を決める段階に進みます。まず、入札者は値段を送ったときに使った乱数を発注者に送ります。それで、発注者は入札者が送ってきた値段の封印を解きます。そこで初めて、発注者が値段を知ることができます。

そして、一番値段を高く付けた人に落札ということになります。そこで、ゲーム理論によるオークションのメカニズムが登場します。オークションの方式は何十通りも存在しますが、この電子オークションでは、落札者は一番高い値段を付けた人なのですが、実際に支払う値段は2番目に高い値段を付けた人の値段という方式を採用しています。これが、電子オークションの手順です。

この手順を使うと公正な価格を決定できる理由は何なのでしょう

このやり取りの間は暗号がかかっているので、盗聴やなりすましができません。入札者同士はもちろん他の人の値段がわからないので、談合することもできません。また、発注者はどの入札者がどの値段を書いたかわからないので、あらかじめ決めておいた入札者を選ぶというような不正もできません。しかも、発注者が嘘の値段を言って不正に入札者を決めようとしても、入札者の値段の書かれているメッセージには発注者の署名が入っているので、その不正はすぐにばれてしまいます。ここまでは、暗号理論によって公正さを保っているわけです。

そして、落札価格は2番目に高い値段にするというオークションの方式を採用することで、値段は発注者が想定した理想的な値段に落ち着くようになっています。この方式のほかに3つのオークション方式があるのですが、それらは経済学のゲーム理論の分野の中で非常によく研究されていて、どの方法をとっても、落ち着く値段の期待値は同じという結果が知られています。

この電子オークションに、2番目に高い値段をとるオークション方式を採用したのは、オークションの参加者が自分の利益を考えたとき、一番の手は正直に値段を言うことにするためなのです。

このように、暗号理論とゲーム理論におけるオークションのメカニズムデザインの成果を統合することで、理想的な性質をもった電子オークションを実現したわけです。

実際にはどんなことに使われるんでしょうか

オークションというメカニズムは、市場で取り引きされない、または数が少ないので市場取り引きに向かない商品に対して、それが市場で取り引きされた場合を想定した価格決定をさせる機能があるのです。

応用分野として、公共事業の入札などもありますが、身近なところではインターネットのコンテンツやサービスの価格決定に向いていると言えます。これらは、商品としては1つしかないので価格というのが付けにくいものです。しかし、電子オークションを使えば公正に市場で取り引きされた場合と同じ水準になるはずなんです。

ゲーム理論を応用したプロトコルを使って、政策決定を行っている画面。こうして、実証実験を繰り返しながら、取引きのメカニズムが理想的なものかを検証していく。プログラムは、共同研究者である奈良女子大学理学部の曽山典子さんが作成した。

［インターネットマガジン　バックナンバーアーカイブ］ ご利用上の注意

このPDFファイルは、株式会社インプレスR&D（株式会社インプレスから分割）が1994年～2006年まで発行した月刊誌『インターネットマガジン』の誌面をPDF化し、「インターネットマガジン　バックナンバーアーカイブ」として以下のウェブサイト「All-in-One INTERNET magazine 2.0」で公開しているものです。

http://i.impressRD.jp/bn

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容（技術解説、URL、団体・企業名、商品名、価格、プレゼント募集、アンケートなど）は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者（執筆者、写真の撮影者、イラストの作成者、編集部など）が保持しています。
- 著作者から許諾が得られなかった著作物は収録されていない場合があります。
- このファイルやその内容を改変したり、商用を目的として再利用することはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用する際は、出典として媒体名および月号、該当ページ番号、発行元（株式会社インプレスR&D）、コピーライトなどの情報をご明記ください。
- オリジナルの雑誌の発行時点では、株式会社インプレス R&D（当時は株式会社インプレス）と著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

このファイルに関するお問い合わせ先
株式会社インプレスR&D
All-in-One INTERNET magazine 編集部
im-info@impress.co.jp