情 報 シ ス テ ム 59－1
（1996．5．21）

電子取引におけるセキュリティについての一考察

川越敏司
浦和市下大久保255 埼玉大学経済学部
TEL: 048-858-3289
E-mail: kawagoe@eco.saitama-u.ac.jp

Abstract

本論文では、急速に発展しつつあるInternetを通じた電子取引の時代に向けて、そうした取引の安全性や正当性を保証するための暗号化プロトコルについて、ゲーム理論の立場からその特質と限界を提示し、こうしたプロトコルデザインとゲーム理論との協調作業が重要であることを論じる。

プロトコルデザインにおいては、プロトコルを通じて送られる通信中のメッセージの改ざんを防ぐことで、安全性や正当性を保証するプロトコルを考えることを目標としているが、こうしたプロトコルにおいて送られるメッセージがプロトコルに参加するものの真の情報を含んでいるかについては何の保証も与えられない。

ゲーム理論におけるメカニズムデザインでは、そのメカニズムに参加するプレイヤーの送るメッセージが、真の情報を含むものであることを保証するようなメカニズムを構築することを目標としているが、このメカニズムは参加するプレイヤーがすべて合理的であること、すなわち多項式時間Turing Machine以上の計算能力を持っていることを前提としている。

本論文では、こうした異なる目的を持つプロトコルデザインとメカニズムデザインの成果を互いに補間しあうことにより、よりよい取り引きメカニズムを開発し得るということを主張する。

具体的には、公開鍵交換におけるユーザー認証の問題と、鍵共有プロトコルを用いたマルチパーティプロトコルを取り上げる。

A game theory consideration of cryptgraphic protocol

KAWAGOE, Toshiji
Faculty of Economics, SAITAMA University

Abstract

We insists that there is a complementary relation between designing secure protocols using cryptgraphy and designing incentive compatible mechanism using game theory when we aim to build secure and incentive compatible protocols.

Using the main results of protocol design, we can build secure message transaction protocols in which all players cannot break other person's secret under some computational constraint, but we have no ways of forcing players to reveal their real information by means of these protocols or give players incentive to reveal their real information.

On the other hand, using the main result of game theory we can build incentive compatible mechanism in which all players should reveal their real information, but this machanism require all players to be rational or to have computation power more than Turing Machine has.

We show that collaborations between protocol design and machanism design in game theory is beneficial for both research field and can build more secure and incentive compatible transaction machanism.

In this paper, we consider user authentification problem in exchanging publickey and multiparty protocol using secret sharing to show needs for collaborations between cryptgraphy and game theory.

1 はじめに

Internet の発展とともに、その利用は軍事目的や学術目的から、ビジネスを目的とするものへと変化して来ている。国境を越えたビジネスの可能性が、こうした動きを加速している。

ところで、ネットワークでビジネスを行なう際に、ネットワークを介して契約のやりとりすることを消費者や企業に促すためには、そうしたネットワークを介した取引の全過程で、個人の重要な情報が漏洩しないこと、すなわちプロトコルが安全であることを保証することが重要である。また、そのプロトコルに従うかぎり、取引がまちがいなく行われることを保証することも必要である。こうした暗号化プロトコルの安全性および正当性の要請が満足されないかぎり、消費者や企業がそうしたプロトコルを用いて取引を行うことはできないであろう。

現在用いられている、あるいは用いられようとしている暗号化プロトコルは、こうした要請を満足するために、NP 完全問題に代表される多項式時間計算量の制約のもとでは解くことができない問題を利用しており、数々の優れたプロトコルが開発されてきている。最近話題になってきている電子現金(Chaum [1])などは、その優れた応用であろう。

こうした暗号化プロトコルの応用におけるひとつの重要な問題は、使用される暗号化プロトコルの標準化がなされなければならないことである。暗号化プロトコルが標準化されていないと、異なる相手に異なるプロトコルを使用せざるを得ず、こうした複数のプロトコルを使いわける処理のオーバーヘッドはばかにならないものとなろう。安全性や正当性を満足するように暗号化プロトコルの技術を開発していくことも重要であるが、また同時にそうしたプロトコルを積極的に採用するように、消費者や企業にインセンティブをあたえるためにも、積極的に標準化を進めることも重要な課題であろう。

米国証券業協会(SEC) は Edgar プロジェクトとして、主要企業の企業データを SGML 化したうえで、PEM で電子署名を付けて公開している。もちろん、この Edgar のデータを利用するものは、SGML や PEM を導入しなければ、こうしたデータの安全性や正当性を確かめることはできないのであるから、こうしたツールが普及するだけでなく、標準化されていることが必要になろう。

ところで、こうした暗号化プロトコルは、このプロトコルに参加するプレイヤーの提出する情報が真の情報であることを前提として、その情報が通信中に改竄されないようにすることを目的としている。

ところが、これから本格化していくであろう電子取引の世界では、国内・国外を問わず多種多様なユーザーがそれぞれの利益に基づいて取引を行うようになるであろう。この場合、真の情報を偽って取り引きをするものの数が無視できないほどのものになる可能性がある。

たとえば、WWW ホームページなどを通じて電子的に商品カタログを提示したり、また将来的に電子的に証券取引が可能になるとした場合に、投資家を保護するために企業の財務情報などを電子的に公開する際には、そうして公開された情報が改竄されないように電子署名などで保護するとともに、提出されている情報がただしくその企業が提出している真の情報であることを保証する必要があろう。

こうした事態に対しては、もはや技術だけの問題ではなくなり、法的規制や制度設計の問題にまで発展しうるものとなろう。必然的に、こうした課題は暗号やプロトコルデザインといった技術と、社会科学との協同作業により問題に取り組むことが必要になってくるであろう。

ゲーム理論の領域では、あるメカニズムに参加する複数の人間間の情報を集計して一つの社会目標を達成させる際に、参加するプレイヤーが提出する情報が真の情報であること保証するためには、どのようにメカニズムを設計すればよいかを考えるメカニズムデザインという理論領域がある。

この分野ではこのような条件を満たすメカニズムがいくつか提案されているが、そこでは参加するプレイヤーがすべて合理的であること、すなわち多項式時間計算量以上の計算能力をプレイヤーが持っているということが要請される。これは、暗号化プロトコルで想定されているプレイヤーのモデルとは異なった、非現実的なものである。

近年、ゲーム理論においてもこうした前提を取り払い、妥当な計算能力を持ったプレイヤーによって行

なわれるゲームを分析する研究が行なわれて来ている(川越[8])。この意味で、暗号化プロトコルのデザインの分野と、社会科学のゲーム理論の間で相互の研究を補完しあう時期に来ているものと考えている。

本論文では、現行の暗号化プロトコルの基本概念を紹介し、公開鍵交換におけるユーザー認証の問題と、真の情報を提出しないユーザーが存在しうる環境でどのようにして真の情報を提出させるかという問題を、ゲーム理論の立場から解説するものである。

論文の構成は以下の通りである。第2節では公開鍵暗号の基本原理について述べ、続く第3節で公開鍵交換における問題をゲーム理論の立場から考える。第4節では他人数で互いの秘密情報を守りつつ共同である目標を達成するマルチパーティプロトコルの基本原理を、Shamir [7] の鍵共有プロトコルを例にとって解説し、続く第5節でこうしたプロトコルのデザインとゲーム理論におけるメカニズムデザインの基本思想の違いについて考察する。最後に第7節で暗号技術とゲーム理論との共同作業が必要であることを論じる。

2 公開鍵暗号

ネットワークにおいて、重要な文書やクレジットカード番号のような情報を送受信するには、経路の途中でそうした情報を盗み見られたり、改竄されたりする危険があるため、暗号化される必要がある。

暗号をこうした場合に用いるには、送受信者間で暗号化鍵をいかに安全に配布するかという問題が生じる。Diffie & Hellman [2] はこうした問題を効率的に解決する公開鍵暗号を発明した。

公開鍵暗号の特徴は、平文を暗号化する鍵(暗号鍵)と暗号文を復号化するための復号鍵(秘密鍵)を異なるものとし、暗号鍵を公開することにしている点である。

いま、アキコがイサオに暗号化されたメッセージを送るとしよう。アキコはまず、ネットワークなどからイサオの公開鍵e_iを手に入れ、送りたいメッセージMをイサオの公開鍵e_iと適当な暗号化アルゴリズムfを用いて暗号化する。それから、暗号化された文$f_{e_i}(M)$をイサオに送る。

イサオは受け取ったメッセージを、自分の秘密鍵d_iと適当な復号化アルゴリズムgを用いて復号化する。ここで、$g_{d_i}(f_{e_i}(M)) = M$という関係が成り立つように、暗号化・復号化アルゴリズムが選ばれる。また、e_iからd_iは計算論的に実際的に計算不可能なことが必要とされる。

暗号化・復号化アルゴリズムでこのような条件を満たすものとしては、合成数の素因数分解を求めることの困難さを利用するRSA方式[6]や、離散対数問題を利用するエルガマル暗号方式などがある。

公開鍵を用いる代表的な暗号化ソフトにPhil Zimmermanが作成したPGP(Pretty Good Privacy)やRFC(Request For Commnets)に仕様が規定されているPEM(Privacy Enhanced Mail)がある。

3 信用の輪

前節で公開鍵暗号の基本原理を説明したが、公開鍵暗号系の重要な問題は交換される公開鍵の正当性の問題がある。公開されている公開鍵がたしかにそのIDを持ったユーザのものであることを証明しなければ、その公開鍵を用いて暗号化されたメッセージを送ることはできないであろう。

たとえば、PEMによるユーザーの公開鍵の認証は、何重にも組織的に階層化された認証方法が用いられる。あるユーザーの公開鍵に疑いが生じたならば、その上位機関にその公開鍵の認証を依頼する。さらに、その上位機関の認証に疑いがあるならば、さらにその上位の機関に問い合わせをすることになる。

これに対してPGPでは、各ユーザーが保持する友人の公開鍵のリストによる「信用の輪」によって認証を行なうことになる。

上位機関に認証を依頼するPEMのような方式には次のような問題がある。ひとつは上位機関が安全であること、あるいは不正しないことを保証する必要がある。第二に、上位機関に保持される莫大なデー

タベースがいつも最新のものであることを保証しなければならない。このために必要な費用を誰が分担するか、ということも重要なインセンティブ問題になりうる。信頼できないセンターの存在のもとでいかに個人情報を守りつつ取り引きを行なうか、という問題は第4節で論じる。

一方でPGP方式は、その信頼性をユーザ相互の信頼と自己責任によって保証している面があり、**PEM**より相対的に信頼性が低いという印象を受ける。この**PGP**の認証方式をゲーム理論の立場から見てみよう。

互いに公開鍵を交換し、通信をしようとするプレイヤーが2人いるとし、プレイヤーの戦略としては、入手した相手の公開鍵を信用するか(C)、しないか(D)の2つがあるとしよう。

この場合、互いに相手を信用しなければ通信は行われず、互いの利得は0である。また、互いに信頼して通信が安全に行われれば、相互に利益がもたらされる。もし、片方だけが偽の公開鍵を用いた場合、だまされた方は本来の相手に情報が届かずひどい損失を受ける一方、他方のだました側では秘密のメッセージを受け取ることができて高い利益を得ることになる。この状況はよく知られた囚人のジレンマゲームとして捉えることができる。その利得表は以下の表1のものであるとしよう。

表1: 囚人のジレンマ利得表

		プレイヤー2 C	プレイヤー2 D
プレイヤー1	C	1, 1	-2, 3
	D	3, -2	0, 0

1回限りのゲームにおいては、Nash均衡という解概念のもとで、互いに信頼しあうより望ましい$\{C, C\}$という解があるにも関わらず、互いに信頼しないという$\{D, D\}$がゲームの解となる。

ここでNash均衡とは、すべてのプレイヤーにとって相手の最適反応戦略t^*が与えられたときに、次を満たす戦略の集合の組のことを指す。

$$\forall i, j \in N, \forall s \in A_i, \exists s^* \in A_i, \exists t^* \in A_j, \mu_i(s^*, t^*) \geq \mu_j(s, t^*)$$

ここで、Nはプレイヤーの集合、A_iはプレイヤーiの戦略集合である。

このゲームの場合、ゲームが十分長く繰り返されるならば、以下の戦略を用いることで互いに信頼しあうことができることが知られている(Gibbons [3])。

ユーザは、はじめは入手した公開鍵を信頼する。そして、一度でもその公開鍵の信頼性に疑いが生じるならば、以降その公開鍵を使用しないようにする。これにより、信頼できない公開鍵が排除され、信頼できるもの同士による通信が実現される。こうした「信憑性のある脅し」が効果を持つのは、あくまで十分長い期間ゲームが繰り返される場合であることが重要な注意点である。

このように十分長い期間繰り返しゲームを行うことが条件となるため、実際にこうした戦略を公開鍵の交換・使用に用いるには実用的ではない。

より実用的な方法としては、ある公開鍵に対する信頼性に疑いが生じたときに、この事実を多くの者が観察できる何らかの信頼できるボード上で公開することにより、不正な公開鍵の使用者にレッテルをはり、「村八分」にすることで信頼性のある通信が実現できるであろうと考えられる。実際、プレイヤーがランダムに出会い、囚人のジレンマゲームを行うという設定のもとでこうした「村八分」が信頼の維持に有効であることが知られている(Kandori [5])。

不特定多数のユーザがやり取りをなすInternet上の通信という条件のもとでは、こうした「掲示板」的な公開情報提示の場の普及も、安全な通信の維持に重要なものとなろう。

4 鍵共有プロトコル

公開鍵暗号によって実現される暗号化取引プロトコルにおいては、プロトコルに参加するエージェントが結託をしたり不正をしても、そのプロトコルに参加する他の個人の秘密情報が守られるようなプロトコルを考える必要がある。この目的を達成するために、こうした暗号化プロトコルではゼロ知識証明や一方向関数などが用いられる (Goldreich, at. el [4])。

この分野の重要な結果として、プロトコルに参加するメンバーのうち、どれだけの人間が結託すれば、プロトコルに参加する個人の秘密情報が守られなくなるかについての研究がある。t 人が結託したら個人情報が守られなくなる時、このプロトコルを t-安全プロトコルという。

もっとも典型的な例として、Shamir [7] の (t,k)-しきい値暗号系を考えよう。ある体 F 上の $(t-1)$ 次多項式

$$f(x) = f_0 + f_1 x + \ldots + f_{t-1} x^{t-1}$$

を一つ決める。この多項式の係数は秘密のものとして保管しておく。ここで $f(0) = f_0$ の値を秘密情報としよう。そして、k 個の $x_1, x_2, \ldots, x_k$ に対して $f(x_1), f(x_2), \ldots, f(x_k)$ を計算し、k 人の管理者に $(x_1, f(x_1)), (x_2, f(x_2)), \ldots, (x_k, f(x_k))$ をそれぞれの共有鍵として配布する。

このとき、この鍵をもつものが結託をして、この鍵を破ることで個人の秘密情報を得ようととしてするものがいても、この多項式の係数は少なくとも $t(\leq k)$ 個の対

$$(x_{i1}, f(x_{i1})), (x_{i2}, f(x_{i2})), \ldots, (x_{it}, f(x_{it}))$$

が与えられないと求められないので、t 安全であるといわれる。

そして、t 個の共有鍵が集まれば、次の方程式

$$\begin{pmatrix} 1 & x_{i1} & x_{i1}^2 & \ldots & x_{i1}^{t-1} \\ 1 & x_{i2} & x_{i2}^2 & \ldots & x_{i2}^{t-1} \\ \vdots & \vdots & \ddots & \vdots & \\ 1 & x_{it} & x_{it}^2 & \ldots & x_{it}^{t-1} \end{pmatrix} \begin{pmatrix} f_0 \\ f_1 \\ \vdots \\ f_{t-1} \end{pmatrix} = \begin{pmatrix} f(x_{i1}) \\ f(x_{i2}) \\ \vdots \\ f(x_{it}) \end{pmatrix}$$

は一意に解けて、求められた多項式の係数が保管されている係数と一致すれば正しい鍵と認められて、鍵を開くようにする。一般的な結果として、$t < \frac{k}{3}$ であることが必要である。

この原理を応用すれば、たとえば各投票者の投票内容を他人や選挙の管理者さえにも知られることなく、全体の投票結果を求めることができる。

5 プロトコルデザインとメカニズムデザイン

前節で紹介した Shamir の鍵共有プロトコルでは、不正をするものがプロトコルに参加する人数の三分の一以下であることが、プロトコルが安全に機能するために必要であった。

こうした暗号化プロトコルのデザインの領域では、プロトコルに参加するプレイヤーの結託や不正を暗号化によって防いでいるのであるが、一方でプロトコル参加者が提出する情報は真の情報であることが基本的な前提となっている。

つまり、誰にも改竄されることなく、また情報が洩れることなく各参加者の情報が集まったとしても、その情報に基づいて構成された情報、あるいはその情報に基づいてなされた集団の意志決定が集団全体の情報や意志を反映したものになるかは、また別の問題である。

これに対し、ゲーム理論におけるメカニズムデザインの課題は、真の情報を提出するとは限らないプレイヤーに、自己利益によって真の情報を表明するインセンティブを与えるプロトコルを考えることにある。そこでこの節では、ゲーム理論における重要な結果である顕示原理についてまず述べ、つづいてオークションにおいて、参加者が自分の真の評価額を付け値としてすすんで提出させるメカニズムについて解説することにする。

5.1 顕示原理

ゲーム理論では、選挙やオークションのメカニズムの設計の問題において、なにより重要な問題として考えられたのは、各参加者の表明する選好ないし情報が参加者の真の選好あるいは情報を反映するものであることを保証することであった。なぜなら、真の選好を偽るプレイヤーがいる環境においては、適切な資源の分配が行なわれないために、社会全体の利益が失われるからである。

そこでゲーム理論において、正直に選好を表明することがプレイヤーにとってもっとも利得が高くなるようなメカニズムを設計することができるかということが問題となった。この問題についてのゲーム理論における重要な結果は、顕示原理(revelation principle) であろう (Gibbons [3])。

これは、プレイヤーが真の選好を偽ってうその選好を表明することで個人的に利益を受け得るような戦略的な選択状況において、Social Planner が望ましい社会目標を達成する際に、その目標をプレイヤーの支配戦略を用いて達成することができるとする。このときプレイヤーが自分の真の選好を表明しても支配戦略の場合と同等な利得を得ることができるメカニズムを構成することが可能になり、そのようなメカニズムを用いることで、その社会目標はプレイヤーの真の選好により達成可能になる、というものである。

顕示原理を以下で形式的に記述していこう。

定義 5.1 選択肢の集合 X 上のプレイヤーの選好順序とは、X 上の二項関係 $\mathbf{R}$ で、次の全順序関係を満たすものことである。

$\forall a, b, c \in X$,

1. $a\mathbf{R}a$ （反射律）
2. $a\mathbf{R}b \vee b\mathbf{R}a$ （対称律）
3. $a\mathbf{R}b \wedge b\mathbf{R}c \Rightarrow a\mathbf{R}c$ （推移律）

この条件は、プレイヤーの選択が合理的であるということを要請している。

定義 5.2 N をプレイヤーの集合、A をプレイヤーの選択肢の集合、E_i を $i \in N$ の A 上の選好順序、E_i の直積 $E = \prod_{i=1}^{N} E_i$ を環境と呼び、社会の望ましい状態を記述する社会選択関数を $W : E \to A$ とする。S_i を $i \in N$ の戦略の集合とし、S_i の直積 $S = \prod_{i=1}^{N} S_i$ に対して、関数 $G : S \to A$ をメカニズムという

すなわち、社会選択関数とはある集団における選好を集計したものであり、メカニズムとはプレイヤーの選ぶ戦略を集計した結果であるといえる。ここで、プレイヤーが自発的に選びだす戦略に基づく社会的結果を、プレイヤーの真の選好を集計した社会的結果に一致させることが、Social Planner の課題となる。これが達成されるとき、メカニズムが社会選択関数を implement するという。この implement には、プレイヤーがしたがう解概念によって異なる結果が生じる。ここでは、支配戦略均衡を取り上げる。

定義 5.3 各プレイヤーのとる戦略 S が支配戦略であるときに、メカニズム G によって達成される選択肢の集合 A が、社会選択関数 W が選びだす選択肢の集合 A' と一致するならば、このときメカニズム G が社会選択関数 W を支配戦略で *implement* するという

定義 5.4 メカニズム G が社会選択関数 W を支配戦略で正直に *implement* するとは、S=E であって、プレイヤーの支配戦略がその選好順序と一致するときをいう

以上の準備のもとで、顕示原理を形式に記述することができる。

定理 5.1 (顕示原理 (revelation principle)) 任意のメカニズム G が支配戦略で *Implement* されるなら、それは支配戦略で正直に *implement* される

先に見たように、暗号化プロトコルデザインにおいては、プロトコルを正常に機能させるために暗号を用いて、プロトコルに参加するエージェントの結託や不正を計算論的に防止しようとしていた。しかし、不正を行なおうと結託するものの人数が全プレイヤーの三分の一を越えると、不正を防止することはできない。

一方、メカニズムデザインの立場では、そのメカニズムに参加するプレイヤーのインセンティブを誘導して、それぞれのプレイヤーにとっての最適な戦略が不正を働かないことになるようにメカニズムを設計することによって、プレイヤーを利益誘導するのである。

もちろん、顕示原理の対偶をとればわかるように、あるメカニズムをプレイヤーの正直な選好によって達成することが不可能ならば、どのようなメカニズムでもそのメカニズムを達成することはできない、ということになるので、いつでも理想的なメカニズムをデザインできるわけではないことに注意しよう。

たとえば、メカニズムデザインではもっとも早く知られている結果としては、選挙のメカニズムにおいて、もしそうしたメカニズムが存在するならば、それは独裁的なものであるという Gibbard & Satterthwaite の定理が存在する。

次の節では、メカニズムデザインの成功例としてオークションのメカニズムを紹介する。

5.2 オークション・メカニズム

メカニズムデザインの成功例としては、たとえばオークションのメカニズムがある。通常われわれが考えるオークション方式は、ファースト・プライス・オークション方式、すなわち付け値が封をして提出され、最高値を付けたものが勝つ、というものであろう。しかし、この方式ではオークション参加者の真の評価額を表明させることはできない。

入札者 i は、入札対象の財に対して v_i という真の評価をもっているとし、もし入札者 i が価格 p 競り落とした場合、入札者 i の利得は $v_i - p$ となるものとする。自然が入札者の真の評価を $[0,1]$ 上の一様分布から選んでいるとし、入札者 i の入札額 b_i は非負であるとする。各入札者の評価は $[0,1]$ の一様分布から選ばれるので、任意の 2 人の入札者の評価が一致する確率は 0 であるから、各入札者の利得 u_i は次のようになる。

$$u_i = \begin{cases} v_i - b_i & \text{if } b_i > b_j, for j \neq i \in N \\ 0 & \text{if } b_i < b_j, for i \neq j \in N \end{cases}$$

ここで、このゲームの均衡において入札者 i は次の条件を満たす入札額 b_i をえらぶことになる。

$$\mathbf{max}_{b_i}(v_i - b_i) \cdot \mathbf{Prob}\{b_i > b_j\}$$

結局のところ、この条件を満たす入札額 b_i は $v_i/2$、すなわち各入札者の真の評価額の半分を付け値として提出することになる。これは、付け値が高い程ほどを勝ち取る可能性が高まるが、一方で付け値が安いほど勝ち取った際の利益は大きいという、参加者のトレードオフを反映しているものと解釈できよう。この場合、オークション参加者は自己の真の評価を提出することはない。

ところが、このオークション方式を、もっとも高い付け値を付けたものが勝利し、代金として2番目に高い付け値を付けたものの価格を支払うというセカンドプライスオークションと呼ばれる方式に変えることで、参加者がすべて自己の評価を付け値として提出し、かつ売り手の利益を最大化することが知られている(Gibbons [3])。

このように、実用的な暗号化取り引きプロトコルでは、暗号を応用して通信される情報の改竄やなりすましを防止しつつ、適切なメカニズムデザインを行なって参加するプレイヤーを利益誘導することによって、各プレイヤーの真の情報を提出させ、プロトコルの安全性、正当性、そしてプロトコルに参加するプレイヤー全体の社会的利益を高めていくことが必要になろう。

6 おわりに

本論文では、急速に発展しつつあるInternetを通じた電子取引の時代に向けて、そうした取引の安全性や正当性を保証するための暗号化プロトコルについて、ゲーム理論の立場からその特質と限界を提示し、こうしたプロトコルデザインとゲーム理論との協調作業が重要であることを論じてきた。

プロトコルデザインが、プロトコルを通じて送られる通信中のメッセージの改ざんやなりすましを防ぐことで、安全性や正当性を保証するプロトコルを考えようとしているのに対し、ゲーム理論におけるメカニズムデザインは、送られるメッセージが真の情報を含んだメッセージであることをインセンティブを働かせて保証しようとしている意味で補完的であることを論じた。

また、公開鍵の認証の問題についても、繰り返しゲームの理論の観点から、何らかの評判を形成するための手段を形成することにより、信用できない公開鍵を淘汰していくことも可能であることも論じた。

もちろん、このように暗号化プロトコルがゲーム理論から学ぶだけではない。ゲーム理論はこれまで合理的なプレイヤーや、無限期間の繰り返しゲームという理想状態を想定した非現実的な設定のもとで主要な結果を導いてきた。これに対し、暗号化プロトコルの研究では、プロトコル参加者を多項式時間計算量のTuring Machineという、計算論的に妥当なモデルをもとに研究を重ねてきた。ゲーム理論の方面でも、近年こうした設定のもとでの研究が進んできているのであるが、まだまだ十分な進展を見せていない。この意味で、ゲーム理論がプロトコルデザインから学ぶところが大いにあるというべきである。

Internetを通じた電子取引という、世界規模の壮大な社会的実験の時代に、暗号化プロトコルの研究という計算機科学と、インセティブを誘導していくメカニズムデザインという社会科学のゲーム理論という領域で、相互協力の研究体制が整うことが望まれるであろう。

参考文献

[1] D.Chaum(1985) "Security without identification: transaction system to make Big Brother obsolete", *Communications of ACM* 28, pp.1030-1044

[2] W.Diffie & M.E.Hellman(1976) "New directions in cryptgraphy", *IEEE Trans. Information Theory* 22, pp.644-654

[3] R.Gibbons(1992) *Game Theory for Applied Economics*, Princeton University Press

[4] O.Goldreich, S.Micali & A.Widgerson(1987) "How to play any mental game", *Proc.ACM annual symposium on Theory of Computing*, pp.218-229

[5] M.Kandori(1992) "Social norms and community enforcement", *Review of Economic Studies* 59, pp.63-80

[6] R.L.Rivest, A.Shamir & L.Adleman(1978) "A method for obtaining digital signatures and publickey cryptsystems", *Communications of the ACM* 21, pp.120-126

[7] A.Shamir(1979) "How to share a secret", *Communications of ACM* 22, pp.612-613

[8] 川越敏司(1995) 「オートマトンゲームにおける計算不可能性」
埼玉大学経済学部社会科学論集 第86号 pp.25-37