総説

情報システム設計のためのセキュリティ要素
— 一方向関数とビット・コミットメント —

森田　光*

Information-Security Elements to Design Information Systems
— One-Way Function and Bit Commitment —

Hikaru MORITA*

1．はじめに

1.1　情報システムとセキュリティの課題

あらゆる組織において、業務効率化のためにＩＴ(Information Technology, 情報技術）を使ったシステム化が大変な勢いで進められている。ＩＴでは、ソフトウェアが計算機の上で動き、計算機は互いにネットワークを経由してデータを授受し、全体として有機的な機能を果たす。これを情報システムと呼ぶ。情報システムは仕事を迅速化し低コスト化する。時には、業務を電子化するばかりでなく、社会的インパクトを与える。後述する横須賀市の電子入札システムが良い例である[1]。

ＩＴの特徴はネットワークにある。同じネットワークでも、現実世界の関係をベースにする電話などを使ったシステムとは異なる。データをやり取りする通信の主体（エンティティと呼ぶ）は必ずしも人間である必要はなく、計算機が人間の相手をすることもあれば、計算機同士が自発的（自動的）にデータのやりとりをすることもある。これでサイバー世界が形成される。

サイバー世界では、空間的に離れている計算機同士が、互いにデータのやりとりだけで何でも実行しようとする。第一の問題は、相手の確認である。例えば、電子オークションでは、取引の約束をサーバー世界でやり、金を振込ませて品物を送らない詐欺事件が頻発している。サイバー世界と現実世界との連動がうまくいってないのである。第２の問題は、データ漏えいの深刻化である。銀行システムでは４桁の暗証番号が昔から問題になっている[2]。それがＩＴの導入で、さらに深刻化する恐れがある。

1.2　情報セキュリティの進展と暗号技術

情報セキュリティは、1980年頃より急速に深さと広がりを増しつつ進展してきた。暗号が、通信相手の確認や書類に付す印鑑の様な認証機能を実現する技術にまで高められたからである。古来より暗号は、盗聴、情報漏えいの切り札とされてきたが、一つ機能が加わったのである。また、一風変わった応用である電子マネーや電子入札では、暗号が技術基盤を与えた。

情報セキュリティの発展の契機は、1976年にディフィーとヘルマンによる公開鍵暗号の概念発明と、IBMによる商用可能なDES暗号の発明であった（経緯は[3]が詳しい。また、技術の概要は[4]参照）。公開鍵暗号は、「秘密とは何であるか」という問いについて強く考えさせ、一方向関数やゼロ知識証明などの学問発展を促した。ユーザが利用している暗号では、携帯電話とインターネットWEBブラウザが代表的である。携帯では、持ち歩く電話機（子機）が本物であることを、暗号を使って確認する。また、インターネットのショッピングでは、クレジット番号を秘密にするために、複数の暗号方式を組合せたSSL（またはTLS）技術を使う。この様に、情報セキュリティは普及例があるものの、その例は多くはない。

1.3　情報システムに対するセキュリティ・デザイン

情報セキュリティも、やっとデザインをする時代になったと思う。従来は、数学を基礎に置き、暗号技術を調べ効率的に作る方法などが検討されてきた。しかし、今は、情報システム設計時に、多者間でどの様に秘密を持ち合い、業務に適用させたらよいかが検討される。

他の工学分野でも、安全、コスト、性能をトレードオフ関係と見て設計している。情報セキュリティでは、暗号の絶対的な安全性を前提に研究されてきた。暗号は有

*教授、経営工学科
Professor, Dept. of Industrial Engineering and Management

限時間で解けるものだが、できるだけ長く守れることを前提に、寿命はあまり考えなかった。しかし、システム化では、信頼できる所（第三者信頼機関、Trusted Third Party, TTP と呼ぶ)、管理する人、守るべきデータ量とその期間を総合的に考え設計する。また、対人間の観点から、利便性、親和性、社会受容性なども考慮する。

1.4 本稿の目的

本稿では、情報セキュリティの一要素（一方向関数）を紹介し、それから数種類の暗号プロトコルのバリエーションが作れることを示す。通信エンティティの数を増やし、それぞれに独自の役割を付加すれば、更に多くのバリエーションが導けるであろう。

ここでは、一方向関数から簡単に導けるビット・コミットメントとそれを繰返すテクニックを示した。実際のシステムでは、エンティティに一定の役割を与え、多くのバリエーションから取捨選択して要求条件にあった物を設計することになる。

以下、2節で一方向関数について準備する。また、時間の前後関係を証明する手段としてビット・コミットメントを紹介する。3節では、この応用例として、(非対面の）通信によるジャンケン、ワンタイム・パスワード、回数券式の電子マネー、シールド・ビット・オークション（電子入札)、更に敗者のプライバシーを護る電子入札について紹介し、4節でまとめる。

2. 一方向関数とビット・コミットメント

ここでは、数学的厳密さは省くが、一方向関数と、それによって作られる主要な性質であるビット・コミットメントの説明を与える。

定義 x を入力とし、関数 $f(\cdot)$ によって関係付けられた値を $y = f(x)$ とする。ここで、入力 x の定義域は十分大きいとし、出力 y の値域も十分大きいとする。このとき、与えられた入力 x_0 から $y_0 = f(x_0)$ を導出するのは容易であるが、y_0 から $x_0 = f^{-1}(y_0)$ を導出するのが困難なときに、関数 $f(\cdot)$ を一方向関数という。

困難性は、次の様に定義される。

性質1．逆関数が存在しない。

しかし、全ての x_i に対する $y_i = f(x_i)$ を求め記憶すれば、しらみつぶし的（全数探索的）に x_0 を求めることが、原理的に可能であることに注意したい。従って、ここでは、全数探索よりも効率的に実行できる逆関数がないことを言う。

性質2．$x_i \neq x_j$ かつ $f(x_i) = f(x_j)$ なる性質を持つペア (x_i, x_j) を求めることが困難である。

全数探索によって x_0 を探索するよりも、一方向関数の出力が一致する様なペアを探す方が一般に容易である(計算量が少ない)。効率的な探索手法があるからである。例えば、誕生日攻撃法（バースディ・パラドックス法）が知られ、関数 $f(\cdot)$ がランダムな出力をだす場合、探索空間は値域のサイズの平方根程度になることが知られる。

一方向関数として使えそうなものの多くは**性質1**を満たすので、具体的には**性質2**に注意して関数を選択する。特に、定義域および値域のビットサイズが重要である。一方向関数候補の代表例がハッシュ関数である。ハッシュ関数は、米国標準技術局 NIST 発行の FIPS に記載されている SHA（Secure Hash Algorithm）に権威があり、必要とする計算量の大小により、SHA-1, SHA-256, SHA-512の中から選択する。SHA-1, SHA-256, SHA-512はそれぞれ値域のサイズが160, 256, 512ビットであり、定義域のサイズは任意である。SHA-1の場合、攻撃を与える計算機パワーが一方向関数で 2^{80} 回程度の計算量を想定する時に使う。

一方向関数により**ビット・コミットメント**は次の様な手順を持つ：

ステップ1．ある時点で、$y_i = f(x_i)$ を登録する。

ここで、登録とは、信頼できる証人に確認してもらうこと、または広く認めて貰うために公開することなどの意味を含む。後で覆らせないコミットメントにするためである。

ステップ2．x_i を示し、ステップ1の時点でコミットしていた事実を証明する。

ここで、事実とは、x_i を持っている自分が**ステップ1**での登録者であることであり、間接証明を意味する。しかし、x_i が他人の手に渡っても同じ効果が生じる。従って、実際には、複製対策を考慮する。

ビット・コミットメントは次の様に例えることができる。マジシャンが、公開の場で、お客が引き当てるカード番号 x_i を予言する。そのまま見せると、お客に影響を与えるので、封筒にカード番号 x_i を封入し、お客が引いた後、開封する。

この状況を一方向関数に置き換える。マジシャンがカード番号 x_i を予言したら、関数 $f(\cdot)$ により $y_i = f(x_i)$ を生成し、それを公開する。お客が引いた後、カード番

号 x_i を示し、y_i と関連づけられることを示す。

しかし、トランプの様にカードの種類が少ない場合、お客が、全てのカード番号 x_i に対応するハッシュ値 $y_i = f(x_i)$ を事前に表にし、マジシャンが y_i を示した途端に表を見て、カード番号 x_i を知ってしまうかもしれない。そして、お客が意識的にそのカード番号 x_i を避けようとすることが懸念される。この様な不都合を避け、純粋にビット・コミットメントを実現するために、入力にはカード番号 x_i の他に乱数 r も含める。乱数が、バリエーションを大きくするのである。幸いなことに、利用するハッシュ関数の入力長は任意なので、問題ない。ここで、入力は連結（コンカチネート）記号を使って表現する： $x_i \| r$。一方向関数の出力は $f(x_i \| r)$ となり、ステップ2で、マジシャンはカード番号 x_i の他に乱数 r も公開する。

3．ビット・コミットメント応用例

3.1 2人ジャンケン

Alice と Bob が非対面の時にフェアー（対等）にジャンケンをすることを考える（Fig.1）。まず、Alice はグー・チョキ・パーの何れかを選び、これを変数 x_A で表すとし、乱数 r により秘匿し、公開情報 $f(x_A \| r)$ を Bob に渡す。Bob は自分の決めたグー・チョキ・パーの何れかを表す変数 x_B を Alice に送る。次に Alice は、変数 x_A と乱数 r を Bob に送り、Bob はその真偽を確かめる。なお、Alice と Bob は2つの変数 x_A と x_B さえ知れば、勝敗結果が分かるとする。

このプロトコルは左右対称にできる。その場合、最初の公開情報は Alice と Bob のどちらが先に出しても構わないし、両方がコミットした後ならば、結果が覆らないので、Alice と Bob のどちらが先に情報を公開しても構わない。

Fig.1 で示した例では、片方の秘密が守られれば、もう片方は相手の手の内を知らないまま自分の変数を決定するので、ビット・コミットメントは片方だけにした。但し、同様のプロトコルを n 人のジャンケン（$n \geq 3$）に拡張する場合、$n-1$ 人がビット・コミットメントするので、対称な場合と非対称な場合で効率上の差は僅かになる。

3.2 ワンタイム・パスワード

Server がネットワークを介して User の正当性を確認する場合、最も簡単な方法は、Fig.2 に示すように、予め Server と User が秘密のデータ（認証子）x を共有しておき、User が Server の資源を必要とする時、User が認証子 x を示すことで認証し、User から Server にアクセスすることを許可する。

この原理は、通常の4桁暗証番号からなる銀行システムなどに使われているのと同様であり馴染み深い。正確には、認証子 x の他に、User が Server に自分の ID（銀行の場合、口座番号など）を渡すことが必要になる。

銀行の場合は、User と Server 間の通信が銀行の管理下にあるため、x が同じであっても User にとって通信からの漏えい問題を問題にする必要がなかった（例外的な事例は[2]参照）。むしろ、User の暗証番号の管理や、ATM（自動預金預け払い機）操作中の盗み見を警戒すべきであった。

ところが、携帯電話、インターネットを介した Server-Client のモデルで同じような認証をする場合、無線区間やインターネット区間を情報漏えいしない通信領域と考えることができないため、この認証方式は使えない。そこで、認証子を秘匿化する方法が開発された。ここでは、ビット・コミットメントを使う例を Fig.3 に紹介する。ビット・コミットメント $y = f(x)$ を Server に登録しておき、User はアクセス時に x を提示する。

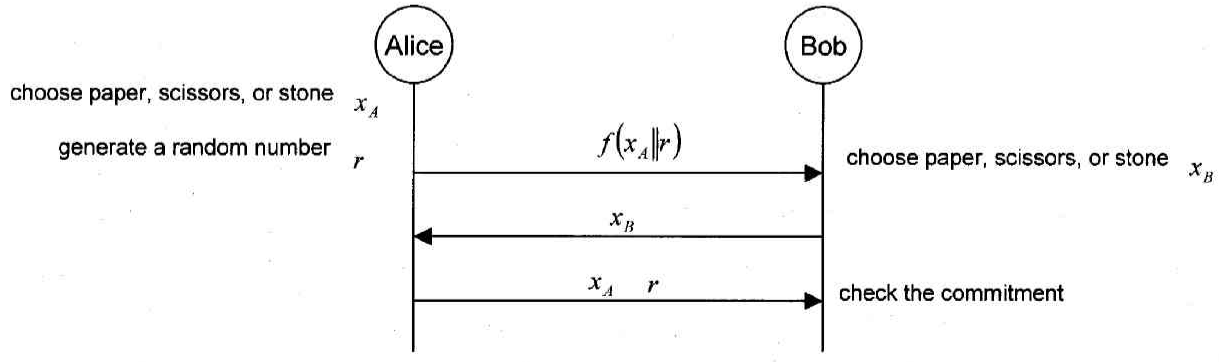

Fig.1 non face-to-face game of paper-scissors-stone between two persons

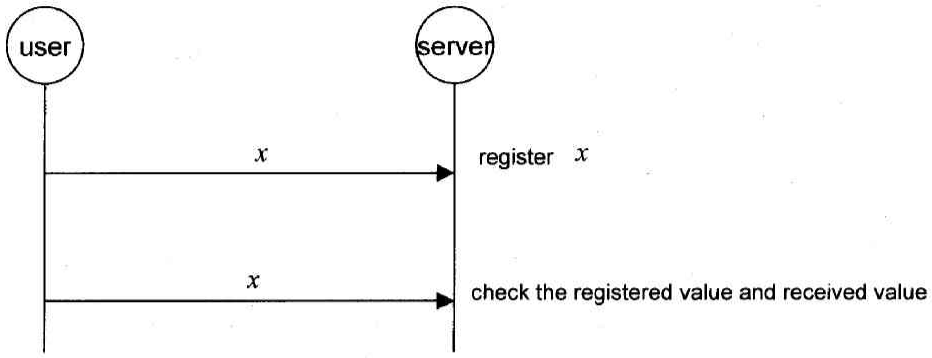

Fig. 2 simple identification

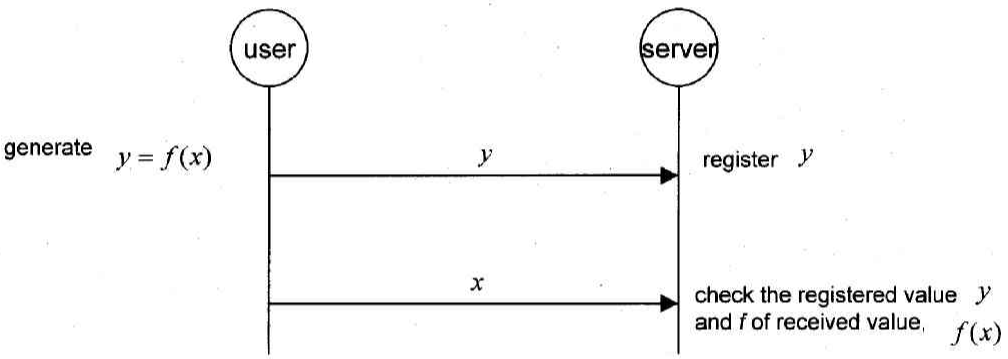

Fig. 3 identification using bit commitment

これを連続的に行いたい場合は、x を提示するとき、次回用の新しいビット・コミットメントの $y' = f(x')$ を一緒に渡せばよい。

一方向関数 $f(\cdot)$ の入力と出力を同じサイズに、つまり定義域と値域のサイズを一致させれば、コミットの開示と次回のビット・コミットメントを同時に 2 つの意味に使える。つまり、x_0 から順番に一方向関数 $f(\cdot)$ に繰り返し代入し、x_i で示す系列を作るとする。ここで、$f(\cdot)$ を施した回数を i 回とするとき $f(\cdot)$ の右肩に i のサフィックスを施し、$x_i = f^{(i)}(x_0)$ の様に表現する。すると、x_i 系列で、サフィックス i をカウントダウンすることで同様の繰返しの認証が実現できる（Fig. 4 参照）。なお、x_i の集合について、サフィックスの連なる集合間は、関数 $f(\cdot)$ により全射の関係をなす。一方向関数が値域でランダムに分布するならば、x_i の定義域ならびに値域のサイズが低減し安全性を損なうことはない。実用上、一方向関数として用いられるハッシュ関数は、ランダムな性質を持つので、この様な用途に適する。

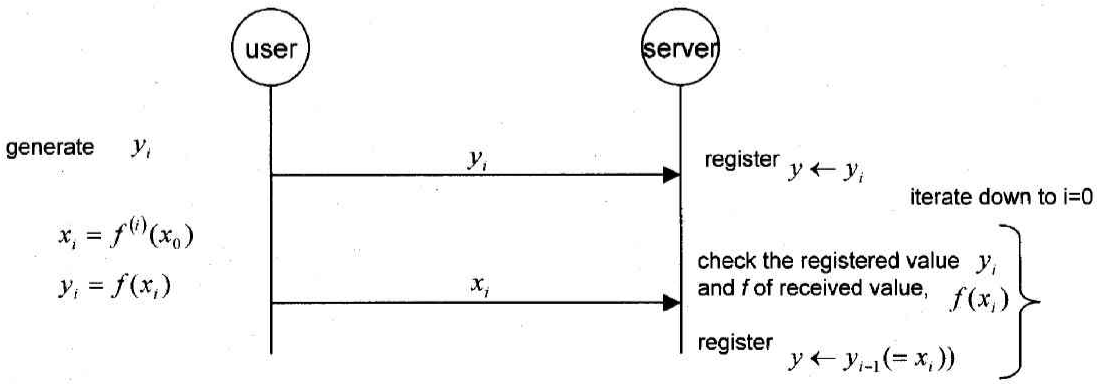

Fig. 4 identification for iterating use

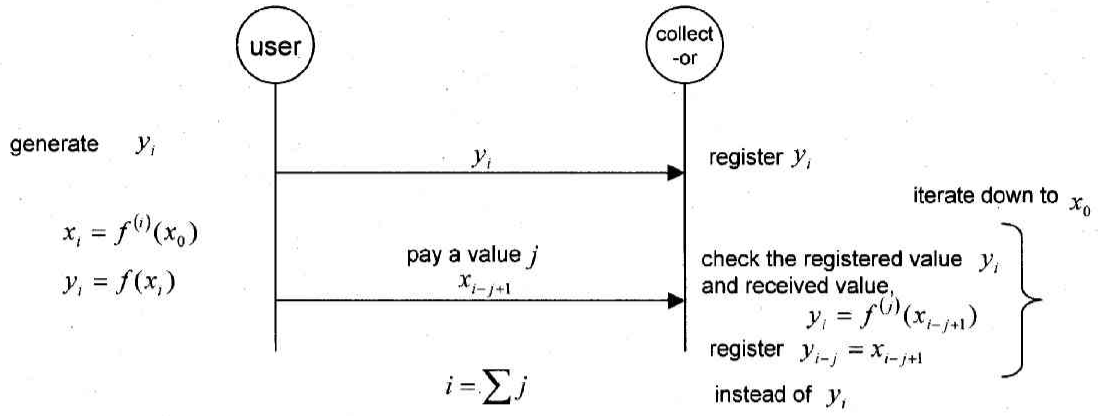

Fig. 5 electronic money like book of tickets

3.3 回数券式の電子マネー

繰返し型の認証方式の応用として、回数券式の電子マネーとすることが可能である。Fig.5 にその例を示す。つまり、あらかじめ y_i が登録され、$x_i = f^{(i)}(x_0)$ および $y_{i-1} = x_i$ なる関係があるならば、x_{i-j+1} を電子マネーとして渡すことで、j だけの価値を通信相手に渡すことができる。ここで、j は $i+1$ までの値をとることができる。

3.4 シールド・ビット・オークション（電子入札）

オークションにはシールド・ビット型とオープン・ビット型がある。市などの公的組織が工事の入札をやる方式はシールド・ビット型に分類され、インターネット上の電子オークションや、市場での競りは一般にオープン・ビット型である。

この他に、価格決定のルールに基づく分類もある。中でも、シールド・ビット型で、参加者が正直に振舞ったときに最良の結果が得られるヴィクリー・オークションが有名であり、経済学に情報の多少を考慮する切掛けを作った[5,6]。

ここでは、電子入札に、ビット・コミットメント技術を導入する方法を紹介する。入札なのでシールド・ビット型である。Fig. 6 に構成を示す。つまり、入札者 bidder が複数いて、それぞれ公的に参照可能な電子掲示板 BBS（Bulletin Board System）に入札データ bid を登録する。シールド・ビット型なので、ここで、BBS には、bid のビット・コミットメントを登録する。登録の証人が要るので、このビット・コミットメントのバリューは即座に公表する。但し、公表範囲は、関係ない第三者まで含めるか、入札参加者に限定するかはシステムのポリシーで決まる。

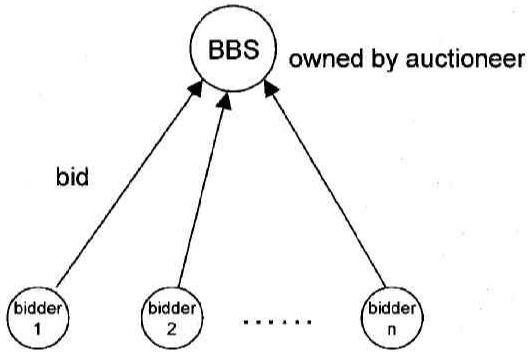

Fig. 6 electronic sealed-bid auction

開札時、入札者はコミットメントした元の入札データ（bid）と一緒に使った乱数 を公表し、前後関係の正当性は一方向関数を使った比較により立証する。ここで、BBS は開札時までは、他のメンバーと同様に秘密の値である bid と r を知りうる立場にないので、BBS の公正性も保たれる。

この様な電子入札は、元の物理的な郵送や人前で行われていた入札を電子的に置き換えただけの簡単な機能しかない。しかしながら、これまでの慣習を踏襲できるので、社会的に受け入れられる傾向にあり、実際、横須賀市が導入しているのはこの方式に基づく[1]。

一方、電子入札に参加した入札者の入札値 bid に対する情報保護に重点を置く研究[7]が日本で盛んに行われてきた。その情報保護の問題意識は次の様な場合に例えられる。Fig.7に示すように 4 人が背比べをする。一番背の高い人を勝ちとしたい。その時、勝者である一番背の高い人の身長が公けになることは仕方がない。しかし、従来法では、それを決める過程で、全員の身長を公けにしなくてはならなかった。それに対して、負けた人は、自分の身長を秘密にしたいというのである。

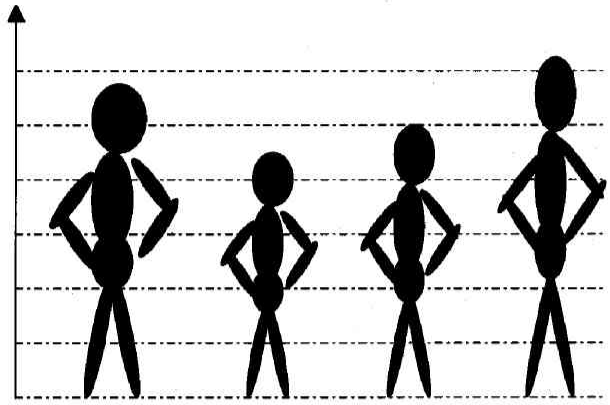

Fig. 7 comparison of height

現実は、工事請負の入札などであるから、落札値に近い値を出せる実力をもっている企業であるかどうかを公けにしたくないとのニーズは確かにあると思われる。逆に、物件購入の入札でも、落札値に近い値を付ける実力を、他に知られたくない場合もあるだろう。

ここでは、従来型の入札を、ビット・コミットメントの技術を使って置き換えたものを「素朴な電子入札」と呼び、敗者の落札値を秘匿にする方式を「敗者のプライバシーを護る電子入札」と呼ぶことにし、以下に説明する。

3.4.1 素朴な電子入札

ジャンケンの変形版として、素朴な電子入札のプロトコルを導く。Fig. 8はその一例である。ここでは、一人の入札者 bidder だけを代表して記している。bidder は入札値 x を決め、乱数 r を生成し、ビット・コミットメントの値 $y = f(x\|r)$ を生成し、BBS へ y を送り、BBS は y を公表する。全 bidder が入札した後、開札のフェーズ（Open Phase）のタイミングを設定し、全 bidder はそれぞれの入札値 x と乱数 r を公表する。入札値から、誰が勝ったかは一目瞭然であるが、通常の入札の様に、発注者側の発注予定の最低価格以下はそのクオリティが無いとして、採用しない様な例外的な場合であれば、それに主催者が説明を加える。但し、その条件も後付は好ましくないので、入札値とは別にビット・コミットメントしておきたい。

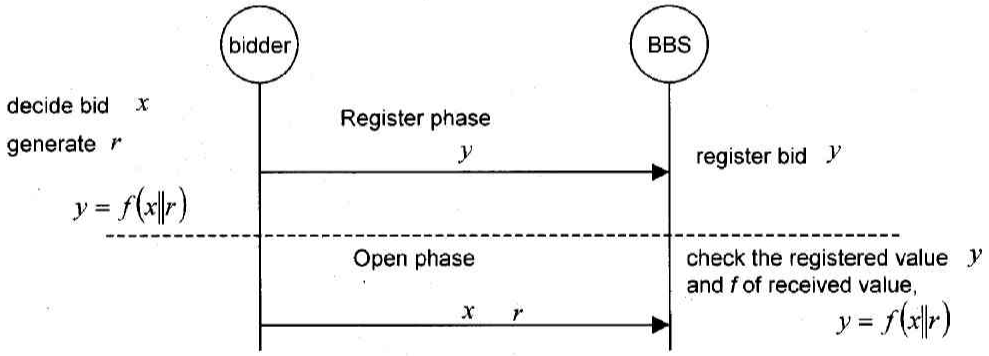

Fig. 8 simple electronic sealed-bid auction using bit commitment

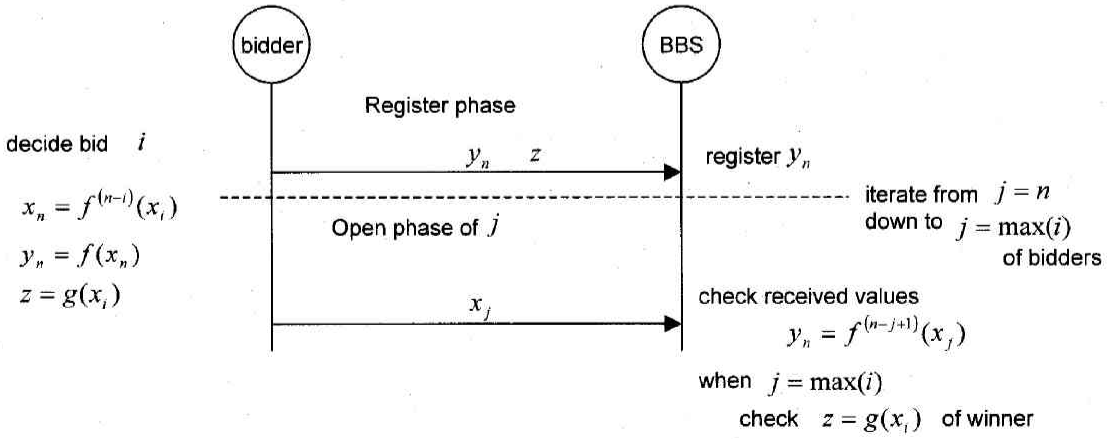

Fig. 9 electronic sealed-bid auction which can compare secret values

素朴な電子入札の最大の特長は、時間的な公正性を保証することであり、入札値 は必ずしも価格などの値だけでは無い。例えば、建築物の図面は数値化できるが、必ずしも図面の数値の大小で優劣は付けられないが、図面の公表を開札時までしないことが、この方式場合、可能である。

しかし、敗者のプライバシーを護ることができない。

3.4.2 敗者のプライバシーを護る電子入札－美人コンテスト

繰返し型のワンタイム・パスワード方式および回数券式の電子マネーの方式を変形して、敗者のプライバシーを護る電子入札方式のプロトコルを構成することが可能である。Fig.9はその一例である[8]。つまり、入札者 bidder は bid の値 i を定め、x_i から繰り返し一方向性関数 $f(\cdot)$ を施し、$x_n = f^{(n-i)}(x_i)$ から $y_n = f(x_n)$ を導出するとともに、$z = g(x_i)$ を導出し、y_n と z を BBS へ送付し、ビット・コミットする。開札フェーズでは、サフィックス j を n からカウントダウンするとし、bidder は、bid の値が異なる時は比較 x_j を示すことで、元のビット・コミットメントが正当であることを証明しつづけ、bid 値であるときは自分がコミットした $z = g(x_i)$ でもあることも証明し、自分の bid 値であることを証明する。敗者になった場合、それ以上カウントダウンの比較に参加することが無いので、勝者の bid と異なる値で入札したものの、自分の bid 値の秘密を維持することができる。

なお、ここで、一方向関数の $f(\cdot)$ と $g(\cdot)$ は、全ユーザで共通である。前述の様に、一方向関数は実用的にはハッシュ関数を用いるが、2種の一方向関数を用いるからといって必ずしも2種類のハッシュ関数が必要になるわけではない。ハッシュ関数を $hash(\cdot)$ とするとき、

$f(x) \equiv hash(0\|x)$ および $g(x) \equiv hash(1\|x)$ と定義して構わないからである。

本比較は、開札時に bidder の協力を仰ぎつつ、逐次カウントダウンの比較が必要なのであまり効率が良くない。しかし、BBS に、ある程度 TTP 機能を付加することで、バイナリー・サーチを可能とする方法もある[9]。

入札の場合、購入であっても販売であっても、比較に用いる bid の座標軸の方向を変えるだけで、価格をあらわすことに変わりはない。美人コンテストなどの様なものでも数値化し、比較する必要が出てくるかもしれない。数値を公けにしても、一番などに選ばれれば問題ないが、そうでなかった場合、不利益を生じてしまう。その様なケースにもこの様な方法を用いることができる。

3.4.3 電子入札の暗号プロトコルと談合

「素朴な電子入札」の暗号プロトコルは、実際に横須賀市に導入されている[1]。当初の狙いは入札業務の合理化とサービス向上にあったと思われる。しかし、ネットワークの持つ広域性により、結果的に落札額を平均約15%カットしたばかりか、入札業者の仕事の進め方を少なからず変えた。さらに、導入したシステムが一種のインフラとなり、他の組織（地方自治体）に使われるまでに至った。

落札額が減ったのは、入札業者が地域に限定されないので、入札にまつわる談合が減った効果と推察される。しかし、これは暗号プロトコルとは関係ない。情報システムの外で人間同士が裏で何を決めているかまで、プロトコルが制御できないからである。入札を、インターネット経由でできるようになった結果、入札者が広域化し、談合グループが少数になったため、談合が減ったと考えられる。

情報システムのデザインという意味では、重要なヒントを与えてくれたと思う。社会や人を含めた総合的な検討を加えれば、良い情報システムを構築できることを示したからである。この様な設計には、暗号プロトコルの構築のみならず総合的な検討が必要になる。経営工学におけるケーススタディ的なアプローチが役立つと思われる。

横須賀市の場合は、電子入札システムだけを単独に作ったのでなく、その基盤となる電子認証システムと電子公証システムという情報セキュリティのインフラを整備した上に、入札システムを構築した。その分、コストがかかったはずである。しかし、横須賀市は、域外の自治体にも同じ電子入札システムを使える様にする、アウトソーシング・ビジネスを始めた。自治体としては初めての試みであるが、長い目で見るとコスト的メリットがあると思われる。インターネットを使ったＩＴ故に可能となったシステムと言えよう。

3.5 その他の暗号プロトコル

ここで使った一方向関数の応用として、他にも電子抽選に使える方法[10]や、競馬・競艇などに使える方法[11]、更には電子証券取引における価格決定[12]などへも拡張することが可能である。電子抽選の方式は、必ずしもビット・コミットメントではないが、同じような考え方が適用できる。また、ジャンケンとともに金持ち比べが文献[13]に紹介されている。

4．まとめ

ここでは、一方向関数を紹介し、ビット・コミットメントの性質を使うだけで、ジャンケン、認証に留まらず、電子入札や電子マネーなどへの応用も可能であることを示した。また、この様な暗号プロトコルは、必ずしも一つで完全という技術ではなく、適用する情報システムや、業務に合わせて変形を考えるべきことについて言及した。これからは、情報セキュリティの技術を、どの様にシステムに利用するかというデザインのセンスが問われる時代になると思う。

参考文献

1)横須賀市、"入札の広場"、WEBページにて参照可能 http://www.city.yokosuka.kanagawa.jp/keiyaku/index.html。
2)森田光、"安全対策を軽視する情報システムと安全を支える情報セキュリティ技術"、経営情報学会誌、14-2（2005-9）pp. 96-101。
3)スティーブン・レビー、"暗号化"、紀伊國屋書店（2002）。
4)太田和夫、國廣昇、"ほんとうに安全？ 現代の暗号"、岩波書店（2005）。
5)太田和夫、今井識、森田光、"電子オークションプロトコルの技術動向－第一価格秘密入札プロトコルについて－"、電気通信大学紀要、16-1（2003-7）pp. 15-21。
6)V. Krishna, "Auction Theory," Academic Press (2002)。
7)H. Kikuchi, M. Karkavy, J.D. Tygar, "Multi-round anonymous auction protocols," Proc. First IEEE Workshop on Dependable and Real-Time E-Commerce Systems (1998) pp. 62-69。
8)K. Kobayashi, H. Morita, K. Suzuki, M. Hakuta, "Efficient Sealed-bid Auction by Using One-way Functions," IEICE Trans. Fundamentals, E 84-A-1 (2001-1) pp. 289-294。
9)K. Chida, K. Kobayashi, H. Morita, "An Auction Protocol Preserving Privacy of Losing Bids with A Secure Value Comparison Scheme," IEICE Trans. Fundamentals, E 87-A-1 (2004-1) pp. 173-181。
10)アグス・ファナル・シュクリ、森田光、太田敏澄、齊藤泰一、"ハッシュ関数を用いた公平な電子抽選方法の提案"、日本社会情報学会論文誌, 16-2 (2004-9) pp.21-29。
11)K. Kobayashi, H. Morita, M. Hakuta, T. Nakanowatari "An Electronic Soccer Lottery System that Uses Bit Commitment," IEICE Trans. Inf. & Syst., E 83-D-5 (2000-5) pp. 980-987。
12)S. Matsuo, H. Morita, "Secure Protocol to Construct Electronic Trading," IEICE Trans. Fundamentals, E 84-A-1 (2001-1) pp. 281-288。
13)太田和夫、渡辺治、黒沢馨、"情報セキュリティの科学－マジック・プロトコルへの招待"、講談社（1995）。