暗号と知的所有権

辻井　重男

はじめに

1994年8月，村山総理大臣を本部長とする高度情報通信社会推進本部が発足した．情報ネットワーク社会では，これまで，紙ベース，対面ベースで行なわれてきた商取引，証明書発行，医療，教育，勤務等のかなりの部分が，電子媒体—情報ネットワークベースに置き換えられ，これにともなって，法律を広範囲に見直さねばならない．全政府的な推進本部が設置された理由の1つには，このような点にあると思われる．

情報のもつ本質的特性の1つは物理法則からの自由性にある．情報は，エネルギー保存則のような物理的法則に縛られることはなく，コピーしても減るものではないという意味で，物理法則から自由であることにその大きな特徴がある．手書き署名やハンコは，コンピュータに蓄えられ，ネットワークを流れるディジタル信号に姿を変えたとき容易にコピーされてしまい有効性を失う．情報ネットワークを介して諸々の認証行為（署名，相手確認等）を行なえるよう法改正できるための技術的裏付けとなるのが暗号技術である．

暗号と知的所有権というとき，2つの側面が考えられる．1つは，種々の暗号方式を知的財産として認めるという観点からの暗号に関する特許という側面，他の1つは，暗号技術は，ソフトウェアをはじめとする情報財の知的財産権を保護するための強力なツールであるという側面である．後者の方も広く一般的関心を集めると考えられるので，本文では，暗号の特許に関し述べたのち，後者の話題である，いわゆる超流通における暗号の役割について考察することとしたい．

つじい　しげお　中央大学　理工学部
〒112 文京区春日1-13-27

1．現代暗号の特徴

暗号の歴史は古く，東洋でもまた西洋においても，その起源は，2000年前後もさかのぼる．暗号が第二次大戦において演じた重要な役割は種々のエピソードを通して語られているが，その用途は軍事・外交であり，情報の秘匿を主目的とし，暗号アルゴリズムはすべて秘密であった．

これに対し，広く情報ネットワーク社会の基盤技術としての現代暗号は，

（I）公開性
（II）認証・署名
（III）安全性
（IV）数学的手法

等の面で，かつての暗号とは大きく異なる性格をもっている．

（I）公開性

1976年，米国商務省は，アルゴリズム公開型の標準暗号ＤＥＳ（Data Encryption Standard）を制定した．これは，送信者と受信者が，同一の鍵を共有するという意味で，すなわち，暗号システムの基本構成において，ギリシャ・ローマ時代以来の暗号（たとえば，シーザー暗号）方式を踏襲するものであったが，アルゴリズムを公開し，暗号の安全性を鍵にのみ依存させるという点で，暗号の歴史上画期的なものであった．

情報ネットワーク社会では，不特定多数の間で暗号通信が必要となることが多い．また複数のネットワークをさらにネットワーク化することも少なくない．その際，暗号アルゴリズムが標準化されていると好都合である．また，ＬＳＩ化による暗号装置の低価格化の面でも，アルゴリズムの標準化は望ましい．

1986年，ＮＴＴが提案したＦＥＡＬ（Fast data Encipherment ALgorithm）もアルゴリズム公開型で

ある．

ＤＥＳ，およびＦＥＡＬは広く利用されているが，他方，アルゴリズム非公開のものもかなり使われており，アルゴリズム公開型が必ずしも共通鍵暗号方式の主流というわけではない．

しかし，アルゴリズムを非公開としても，管理運用面で秘密が洩れないという保証はない．私見では，オープンに議論ができて，透明感の強い公開型アルゴリズムが主流となることが望ましいと考えているが，この点で，最近の米国のいわゆるクリッパチップの動向は好ましいとは思われない．1993年4月，クリントン政権は，クリッパチップ，あるいはSkipjackと呼ばれる非公開アルゴリズムを用い，裁判所の許可の下で，暗号化された通信内容を解読し得る仕組みを導入する構想を発表した．

いずれにしても，アルゴリズムの公開という流れは現代暗号の大きな特徴であり，この公開性という特徴は，公開鍵暗号において決定的となる．

暗号方式は，共通鍵方式と公開鍵方式に大別される．上に述べたように人類が数千年以上にわたって使用してきた方式が共通鍵方式である．公開鍵方式の概念が提案されるまでは，共通鍵方式というような名称は存在しなかった．暗号通信を行なう者同志の約束事として，共通の鍵を持ち合うことは，当然のことであり，暗号と言えば今でいう共通鍵方式に決まっていたから，名称など考えもしなかったわけである．

公開鍵方式が誕生してから，この方式では，暗号化用に公開鍵，復号用に秘密鍵が利用されることに対応して，従来方式を共通鍵方式，対称鍵方式，秘密鍵方式，あるいは慣用鍵方式，等々の名称で呼ぶようになった．

共通鍵方式では，たとえ，アルゴリズムを公開しても，鍵は1種類であるから，当然秘密になるわけである．そこで，秘密鍵方式と呼ばれたりすることになるが，公開鍵方式でも当然ながら秘密鍵はあるわけで，共通鍵方式を秘密鍵方式と呼ぶのは混乱を招きやすい．後で述べるように，公開鍵方式における秘密鍵は，要するにそのユーザの秘密であって，守秘通信（いわゆる暗号通信）では復号用であるが，認証・署名時には，手書き署名やハンコに相当するものである．

公開鍵暗号方式（Public-Key Cryptosystems）はＤＥＳと同時期，1976年に提案されたが，アルゴリズムはもちろん，鍵まで公開するという暗号の歴史2000年の常識を破る画期的な概念であった．鍵を公開してなぜ暗号になるのか．従来からの方式のように，送信者と受信者が同一の鍵を共有するやり方であれば，鍵を見せてはおしまいである．

公開鍵暗号方式では，鍵の構造を2階層とし，各ユーザに固有の秘密鍵をまず作成し，それを内蔵する形で公開鍵を作るのである．ユーザA宛に暗号文を送ろうとするユーザはすべて，Aが公開しているAの公開鍵を用いて暗号化し，受け取ったAは自分だけの秘密鍵を用いて復号する（平文に戻す）．共通鍵方式における鍵の安全な配送という問題は解消されている．（付録A参照）

公開鍵暗号の具体的方式として，ＲＳＡ暗号は，最も著名であり，ＲＳＡ社と呼ばれる企業も設立されて商用化されている．その素因数分解の困難性を利用するアルゴリズムは，素朴な強さをもっており，後述するような証明付安全ではないが（暗号解読と素因数分解との等価性が証明されているわけではないが），安全性については高い信頼感を得ている．

ＲＳＡ暗号以外にも多くの公開鍵方式が提案されているが，ＲＳＡと同じく早い時期に提案された方式にナップザック暗号がある．やさしいナップザック問題を秘密とし，これを難しいナップザック問題に変換して公開鍵とするものである．この方式は，暗号化処理が簡単であるという特徴をもつが，安全性については，暗号の宿命的側面ともいえる「解きつ解かれつ」を通して弁証法的展開をとげている．また，次に述べる認証・署名に適した方式とは考えられていない．

（Ⅱ）認証・署名

手書き署名や実印に要請される機能は，本人しか作成できない（他人が偽造できない）こと，および，他者が容易に本人確認ができることの2点である．情報ネットワークでは，このような物理的手段による本人性の主張は無効となり，これに代わる数値的手段が必要となる．

（Ⅰ）に述べた公開鍵方式は，ユーザ毎に固有の秘密鍵と公開鍵をもたせる方式であった．公開鍵方式は，いわゆる暗号通信，すなわち情報の秘匿に利用するとき，通信に先立つ鍵の配送という面倒な問題を解消するという点で勝れた方式であることはすでに述べたが，実は，それ以上に認証・署名に適した方式なのである．秘密鍵は手書き署名（あるいはハンコ）に，公開鍵は，それを他者が容易に確認するための目（識別能力）に対応すると考えればよい．

一般に，自分（のカード）であることを相手に納得させるのに，秘密を見せてしまうのは危険である．クレジットカードで国際電話をかけるところを，望遠鏡で覗かれて，番号を盗まれ莫大な被害にあったという話もある．秘密をカードから外に出さないで，カードの真正性，すなわちカードがその秘密を内蔵していることを，相手に納得させることはできないだろうか．こんな発想で1980年代中頃に提案されたのが，零知識相互証明であり，すでに，有料ＴＶ放送等で実用化されている．

（Ⅲ）安全性

“It may well be doubted whether human ingenuity can construct an enigma of the kind which human ingenuity may not,by proper application, resolve.（人間の才能を適当に用いても解けないような謎を人間の才能が果たしてつくり得るものかどうか疑ってみるのも無理はないだろう）”

エドガ・アラン・ポーは，暗号がからんだ名作“Gold bug（黄金虫）”中でこんなセリフを登場人物に言わせている．

第二次大戦中に使用されたドイツのエニグマ暗号，日本の紫暗号もかなり解かれていたようである．現代暗号の研究者たちは，何かと“解きつ解かれつ”の循環を断ち切り，暗号理論をできるだけ強固な数理的基盤の上に構築したいと考えている．その成果の１つが，(II)に述べた零知識証明であり，秘密が洩れないこと，なりすましが不可能なことをチュリングマシンの議論等を用いて証明している．（付録Ｂ参照）

しかし，認証・署名系については証明付安全な方式を構成することも可能であるが，情報秘匿系については，実用的方式を構築することは難しい課題であり，解きつ解かれつを繰り返しつつ安全性を高めていく弁証法的過程も残らざるを得ない．

（Ⅳ）数学的手法

暗号に関する数学的手法としては，数論的・代数的，計算量理論的色彩を濃くしている．証明付安全という場合でも，その根拠が素因数分解，および離散対数問題の困難性に依拠している場合が多い．そうした意味で，暗号理論に利用できる求解の困難な数学的問題を数論的代数幾何学から探究するという興味深い試みもなされている．

2．暗号に関する特許の現状と課題

1．で述べたように，現代暗号は，1976年頃に始まること，そして公開性がその大きな特徴であることを述べた．暗号アルゴリズムが公開である場合，特許としての意義も明確に存在する．

アルゴリズム公開鍵暗号ＤＥＳは，米国商務省標準局（当時）が定めたものであるが，基本的アイディアはＩＢＭ社の特許にさかのぼり，その内容は，1975年から1976年にかけて発行されたU. S. Patents and Trademark OfficeのO. G.（Official Gazette）に記述されている．

次に公開鍵暗号について見てみよう．公開鍵暗号の概念の提唱者Hellman等は，公開鍵暗号方式そのものを特許化し，同時に，具体的方式として，ナップザック方式を特許化している．その経過は下記のとおりである．

1976.11	Diffie & Hellman “New Direction in Cryptography”（論文の発表）
1977.10.6	Hellman & Merkle “Public Key Cryptographic Apparatus and Method”（U. S. A. Patent 出願）
1978.10.6	上記特許の日本出願
1984.12.6	公告（特公昭59：50068）15年有効
1985.6.25	原簿登録（特許発効）

なお，Hellmanらが「公開鍵暗号の一般的方式」を日本に出願しているが，その時，すでに（６ヵ月以前）彼らの論文が発行されていたので，先願主義の日本では特許になるはずはない．しかるに実際には，特許になっているのは，どのような経緯によるものか，筆者

表１　特許出願状況（日本，1986-01～1989-09）

内容／出願	認証	鍵管理	通信システム	コンピュータ電子送金等	音声秘匿	画像秘匿	計
国　内	141	100	224	219	159	63	906
国　外	6	8	32	15	8	4	73

には不明である．

また，ＲＳＡ暗号については下記のとおりである．

1977．4　Rivest, Shamir, Adelman “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems” MIT/LCS/TM 82 に発表

1977.12.14　U. S. A. Patent 出願．（日本には出願されていない．）

1978．2　Communications of the acm に論文発表

1983．9．20　U. S. A. Patent が発効．

ＤＥＳやＲＳＡの発表以来，暗号アルゴリズムとそのシステムへの組み込み法，適用法について多岐にわたる特許が出願されている．たとえば，ある調査レポートによれば，わが国において，1986年1月から1989年9月までの公開特許件数は約1000件に達している．その内訳はおおよそ，表1のとおりである．表1において，国内の出願人としては，電気・情報機器メーカや，ＮＴＴ，ＫＤＤ，ＮＨＫ等の通信・放送業者等，約30を数え，国外からは，フィリップス，ＩＢＭ，ＡＴＴ等が出願している．

ＮＴＴのＦＥＡＬは，1985年～1989年にかけて，日，米，仏，独，英に申請され，U. S. A. Patent は1989年に登録されている．

今後，暗号技術については，情報セキュリティの基幹技術として，暗号アルゴリズム自体の研究開発とともに，管理，運用面まで含めた総合的システムへの利用面について検討が深められ，その過程で，特許出願もますます活発になるものと予想される．

次に，暗号の特許をめぐる課題について考えてみたい．日本と米国における出願方法の相違（先願主義 vs. 先発明主義）は，ボーダレス時代に向けて解決されると思われるが，暗号に固有の課題ではないので，本文では論ずることを差し控える．

（Ⅰ）自然法則の利用という制約について

これも暗号に固有ではないが，“特許は「自然法則を利用した発明」に対して成立する”という制約も困ったものである．筆者らが提案したＩＤにもとづく鍵共有方式に関する出願も，現在，特許庁から，自然法則を利用していないという理由で拒絶されている．一般に，アルゴリズムに発明の中心があるにもかかわらず，あたかも，ハードウェア構成に工夫があるかのように表現しなければ特許にならないというのは，工業時代の発想であり，自然法則に制約されない情報を財とする情報化社会の発想ではない．工学や技術の基礎は自然科学であるという表現も誤解を招きやすい．確かに，工学・技術はその知見の多くを自然科学から得ているが，同時に他の諸科学からも得ており，それらの知見を吸収しつつ，１つの人工科学的体系を成しているのである．

ここで，自然法則と言ったのは，主に物理法則の意味であり，数学法則（数学的真理）はこれに含めていない．数学的法則も自然法則に含めて考えて，数学法則とアルゴリズムの線引きを適正に定めることができればよいのだろうか．

（Ⅱ）標準化との関係

これも必ずしも，暗号のみの問題ではなく，標準化による社会的便宜の大きい通信技術等でよく論じられる課題ではある．しばしば，reasonable な値で特許を利用させるという表現も見受けるが，どの程度が reasonable かが問題となる．

暗号の代表例として，ＤＥＳについて触れておこう．ＤＥＳは FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION 1977 JANUARY 発行の資料番号 FIPS PUB 40 「DATA ENCRYPTION STANDARD」にその全容が記載されており，特許については，

“この標準を実現する暗号装置（Cryptographic devices）は，ＩＢＭに issue された米国および外国特許によってカバーされる．しかしながらＩＢＭは，標準に合致する機器の製造，利用，販売に対し，nonexclusive, royalty-free licenses（非独占的，特許料無料ライセンス）を与えている．”と記されている．

この例のように royalty-free なら問題はないわけである．

（Ⅲ）アルゴリズム非公開型暗号方式と Submarine patents

どのような発明か，その内容を伏せたまま，特許を出願したいという要求は，他の分野でもないわけではないが，暗号分野にとっては，特に関心の高い問題と思われる．暗号アルゴリズムを秘密にしたまま出願し，他者が同様のアルゴリズムを出願したり，あるいは実用化したとき，権利を主張するという手続きである．

わが国では，このようないわゆるSubmarine patentsは考えられなかったが，米国では可能であったようである．しかし1996年より，米国でもSubmarine patentsは不可能になるようである．

3．知的財産権保護と情報財流通促進のための暗号技術

マルチメディアが高速ネットワークを流れる時代にあって，複雑な権利関係の下で，原作者と改訂者に適切な権利を認めつつ，情報財をスムーズに流通させるため

（I）情報の価値に対する認識と情報通信倫理の高揚

（II）ディジタル情報財に適した法制度の整備

（III）認証・署名，情報秘匿，課金等を適正に行なうための技術的システムの導入

を急がねばならない．(III)の技術的システムの基本技術が暗号である．

さて，ハードウェアの急激な価格低下に対して，潜在的にはより大きな量産効果が期待できるはずのソフトウェアについては生産性が上がっていない．ソースコードレベルで部品化・再利用が行なわれても，組織内に閉じている限りは大きな効果はなく，それらの部品を電子オブジェクトとして市場供給し，対価を得ることができるようなシステムが確立されてはじめて，ソフトウェアの流通と低価格化が実現されよう．

また，近頃騒がしいマルチメディアも，その素材を利用者が自由に処理・加工・編集し，これをネットワークを介して再び流通させ得るようなシステムが必要であろう．

情報自由化時代を迎えて，我々は，情報価値の認識と情報通信倫理感を高めるという精神的構造改革をベースに，上記のようなシステムを，法制面と技術面から確立していくことが急がれている．

ディジタル情報の姿をした知的財産に対しては，複製をもって著作権侵害とするコピーライトの発想，あるいは印刷技術を前提とした法制度は改めるべきときにきており，**利用に対する対価徴収権**を基本とする法制度が適合していると思われる．

このような法制度の下で，情報財の流通を促進し，そのパイを大きくして単価を下げる技術的システムとしていわゆる超流通システム(Super Distribution)が注目されている．超流通システムは，1983年以来，森亮一氏によって提唱されてきた概念であり，大よそ次のような構成となっている．[2]

超流通システムは，情報財（以下，ソフトウェアと呼ぶ）の利用に応じて課金する従量制のソフトウェア流通システムである．料金決済を電子的に行なうために必要な情報が超流通ラベルとして，ソフトウェアに付加される．超流通ラベルとして，次の2項目が含まれる．

（I）ソフトウェアID：個々のソフトウェアを識別し，利用料金の支払先を区別する情報

（II）使用記録：ソフトウェアの利用状況を表わす情報であり，超流通センタに回収され，それにもとづいて料金の決済が行なわれる．

超流通ラベルは料金決済の基礎となるものであり，その改ざんは超流通システムにとって脅威であり，改ざん防止のための暗号が用いられる．また，利用情報の秘匿，認証子生成・確認等のため，暗号技術が駆使され，超流通システムは，暗号と情報セキュリティシステムそのものと言っても過言ではない．

最近，CDROMに暗号化された情報を多数記録し，料金支払いに応じて鍵を配るシステムも商用化されているが，このようなシステムを，いわば，インダストリアルプラットフォームとして，体系化したのが，超流通の概念であると言えよう．

謝辞

本文をまとめるに当たり，ご教示いただいた北陸先端科学技術大学院大学 岡本栄司教授，植松助教授，ならびにNTT森田光博士に感謝する．

文献

[1] 辻井，笠原編著：“暗号と情報セキュリティ”，昭晃堂（1990）

[2] 森他：“電子情報通信学会，情報セキュリティ研究会，超流通および関連する応用分野特集，1994-09 (ISEC 94-13-22)”．特に，大滝：”超流通アーキテクチャにおける開発環境について(ISEC 94-14)”

付録A　公開鍵暗号方式

学生　「暗号というのは，送信者と受信者のペア毎に秘密の鍵を共有するはずですね．それを公開したら暗号にならないと思いますけど？」

先生　「ペア毎に秘密鍵を決めるのではなく，ユーザ毎に固有の秘密鍵とそれに対応する公開鍵と呼ぶ2つの鍵を用意するというように発想の転換をしてみたらどうだろう．暗号通信では，自分（A氏）宛暗号文はどの人にも自分の公開鍵で暗号化して送ってもらい，自分だけが後生大事にしている秘密鍵で復号するので」

学生　「奇想天外より来るという感じですね．公開鍵の中に秘密の仕掛けを組み込んでおき，それで開けるわけですね」

先生　「そのとおりです．たとえば，ユーザAは1021と1019という2つの要素を秘密鍵とし，それらの積1040399を公開鍵としてどのユーザにも使わせるという具合です．実際は要素として10進100桁くらいのものを使います」

学生　「認証や署名として公開鍵暗号を使うときは，ユーザAはまず，Aの秘密鍵で，たとえば（氏名＋タイムスタンプ）に署名をつけ，誰でも，Aの公開鍵で開いてみて，Aさんしかできない操作がされていることからAさんの署名であることを確認できるというわけですか」

先生　「そのとおりです．公開鍵方式はむしろ情報ネットワーク時代の署名の必要性からの発想といってもよいでしょう．人類の第1の文明開化期（ヤスパースのいう基軸時代）にギリシャやローマで通常の共通鍵方式のアルゴリズムが芽生え，第2の文明開花期とも言える現代（ヤスパースは第2基軸時代と呼ぶ）の鍵の構造を2階層にした公開鍵方式が生まれたのも情報自由化の必然とも思われます」

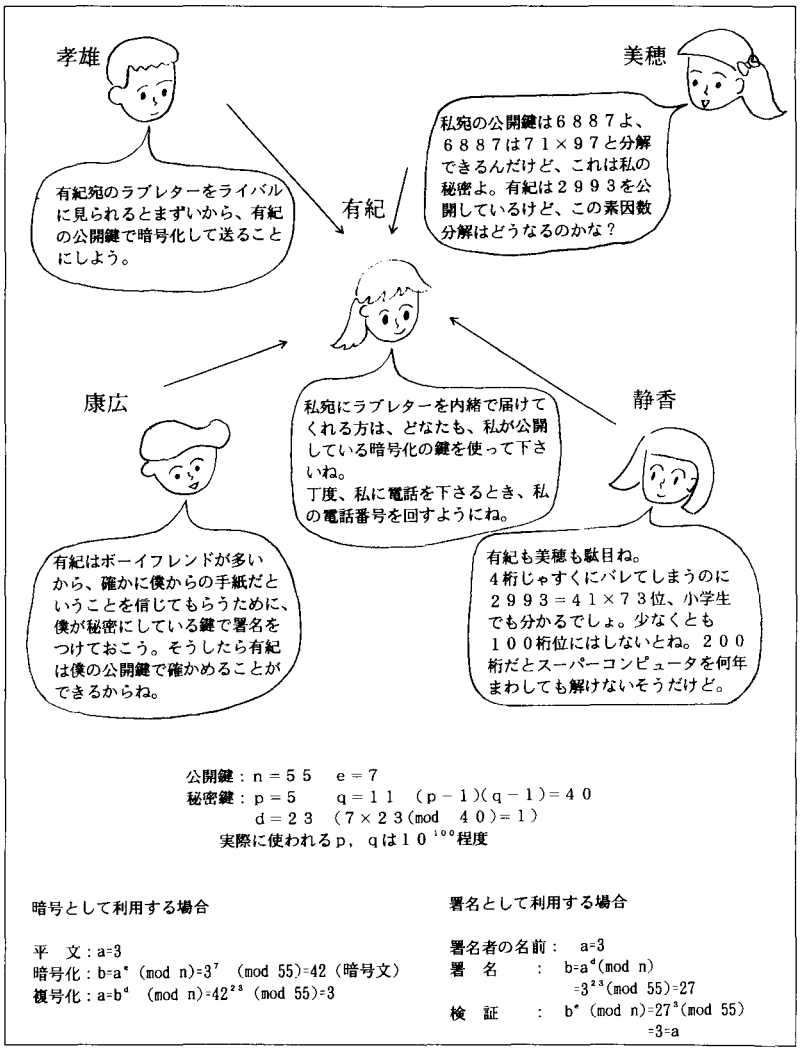

図1　公開鍵番号

付録B　零知識相互証明

学生　「クレジットカード番号で国際電話をかけるところを望遠鏡で覗かれて，莫大な被害を受けたという話を聞きましたが，秘密を見せないで，相手に自分（のカード）に間違いないことを信じてもらえると安全ですね」

先生　「その理論が1980年代中頃から発達してきました．Zero Knowledge Interactive Proof，略してＺＫＩＰ，日本語で零知識相互証明と呼んでいます．図2はその具体例です．そのシステムでは，公開鍵暗号の例で示したように素因数分解の困難性を利用しています．

（Ｉ）まず，センタは2つの素数を発生し，それをセンタだけの秘密とします．

（II）ユーザAは公開されている自分のＩＤ$_A$（例：電

話番号，社会保険番号）をセンタに登録します．（他のユーザも同様）

(III) センタはID_Aの平方根S_Aを計算し，ユーザAだけの秘密としてこっそり教えます」

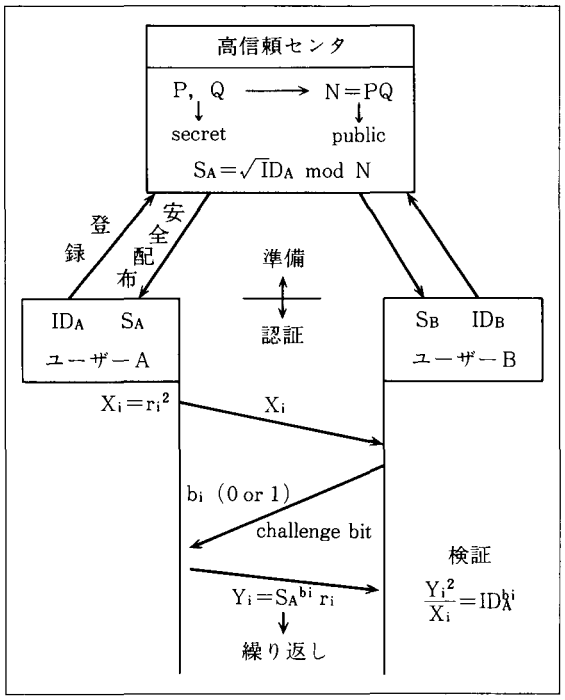

図2　零知識相互証明（ＺＫＩＰ）

学生　「平方根など誰でもとれるではありませんか？」

先生　「ところが合成数を法とする整数の世界では，素因数を知らない人には平方根がとれないんです．もちろん大きな合成数の場合ですが」

学生　「なるほど．それで，図2の零知識相互証明のアルゴリズムで，ユーザAが正しいプロトコルを使う場合だけを想定すれば，1回の通信で済みますが，Aの秘密S_AをもっていないA′がAになりすますのを防ぐために何度かやりとりするわけですね」

先生　「そうです．じっくり眺めてよく理解してください」

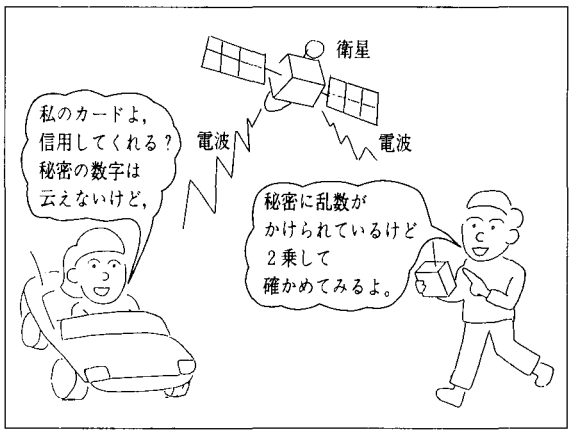

図3　零知識相互証明