11

暗号に関する発明の明細書作成のポイント

特許庁特許審査第四部電子商取引
中里 裕正 *nakazato-hiromasa@jpo.go.jp*

学術論文として投稿したものは，査読の結果，受理されたのに，特許として出願したものは，拒絶されてしまった．その理由も「発明ではない」ということだ．学会では高く評価されている技術なのに，これはいったいどうしたことだ．

皆さんのなかには，このような経験をされた方はいらっしゃいませんか．今回は，暗号を題材に，このような事態が生じる理由と，それを防ぐ手だてについて解説したいと思います．暗号はソフトウェアにより実現されることもあり，電子マネーのようなビジネス関連発明にも用いられます．したがって，過去の記事[2), 3)]をご参照いただくと，より理解しやすくなるはずです．

なお，本稿の内容は，個人的な見解を述べたもので，特許庁の公式見解ではないことをご承知おきください．また，本稿の議論がすべてのソフトウェア関連発明やビジネス関連発明に当てはまるとも限らないことにもご留意ください．

■論文と明細書

冒頭で挙げたような不幸な事態は，どうして起こってしまったのでしょうか．それは，「理工系の学術論文と特許出願の明細書は，似て非なるものである」ということが，十分に認識されていない結果であると考えられます．確かに，学術論文も明細書も，科学技術に関する文書であることに変わりはありません．その分野の通常の知識を持つ者が実施可能な程度に，発明を明確かつ十分に記載しなければならない，という実施可能要件の点からみれば，特許出願の明細書は，学術論文程度の記載がなされていれば，必要にして十分といえるかもしれません．

両者の決定的な違いは，特許出願の明細書が法律的効果を生じる文書であるという点です．明細書のうち，特許請求の範囲は，排他独占的な権利の範囲を定めます．発明の詳細な説明は，その範囲に対する具体的な根拠を与えます．そのために，特許出願の明細書には，学術論文とは異なる記載が必要とされるのです．特に，「特許法でいうところの発明」であるか否かという成立性の記載要件が満たされないと，学術的・商業的には価値のあるものであったとしても，特許としては成立しないことになるのです．

それでは，「特許法でいうところの発明」とはどのようなものなのでしょうか．現行の特許法は，発明を次のように定義しています．

特許法第2条第1項

この法律で「発明」とは，自然法則を利用した技術的

思想の創作のうち高度のものをいう.

また，特許を受けることができる発明については，以下の条文にも規定があります.

特許法第 29 条

産業上利用することができる発明をした者は，次に掲げる発明を除き，その発明について特許を受けることができる.（後略）

理工系の学術論文になるような発明の場合，これらの規定のなかで問題となるのは，「自然法則を利用した」というところでしょう．数学的な法則に基づく計算方法などは，それがいかに優れたものであったとしても，「自然法則を利用した」ものとはいえないからです．論文では，計算のアルゴリズムを数式を用いて示すだけで十分でしょうが，特許出願の場合，その程度の記載しかなされていないと，「自然法則を利用していない」として特許にならない可能性が高いといえるでしょう.

ところで，この第 2 条は，昭和 34 年の特許法改正の際に置かれたものです．つまり，それ以前の特許法には明文として存在しなかった規定です．第 29 条の条文も，改正前の対応する条文とは異なっています．「発明」の定義は，なぜこのようになったのでしょうか.

法律の改正には，さまざまな要因が考慮されます．この問いに対する答えも，それだけで 1 つの論文になり得るものです．しかし，これらの規定に影響を与えたと思われる，最高裁判所の判決が 1 つ存在します．それは「暗号作成方法」の発明に対して，特許法上の「発明」であるかどうかの判断を示したものなのです.

■裁判所の判決

昭和 15 年，「欧文字単一電報隠語作成方法」という特許出願（昭和 15 年特許願第 10020 号）がなされましたが，特許庁（当時は特許標準局）は「特許法にいうところの発明」ではないとして特許を認めず，拒絶しました．出願人はこれを不服として，拒絶の取消しを求めて訴えを提起しました．東京高等裁判所は，特許庁の判断を妥当として請求を棄却したため，出願人はさらに最高裁判所に上告しましたが，最高裁判所も東京高裁の判断を認めて上告を棄却しました（昭和 25 年（オ）第 80 号）.

判決[1] によると，この出願の内容は，電報に利用するために，語句を欧文字からなる隠語に置き換えることで暗号化するというものです．この置き換えは，図表を参照して人間の手で行われます．そのため，特許庁は「工業的発明でない」として拒絶したのです．その審決の一部と，根拠となった当時の特許法の条文を挙げておきます.

特許庁の審決（抜粋）

「本願発明は欧文字数字記号等を適当に組合わせて電報用の暗号を作成する方法であつて何等工業に関係したものではないから特許法第一条にいわゆる工業的と認めることはできない，従つて本願発明は同条に規定されている特許要件を具備しないものと認める.」

旧特許法第一条

新規ナル工業的發明ヲ為シタル者は其ノ發明ニ付特許ヲ受クルコトヲ得

この判断に対して，出願人は以下のように主張しました．特許法にいう「工業的発明」とは狭く工業に関するものに限るのではなく，最も広い意味での「産業」に関するものと捉えるべきである．本願の方法は通信に関するものであって，商取引に利用される．つまり商業の一部であり，商業は産業の一部門をなす．したがって，本願の方法は産業上重要なものであって特許を受けることができるものである.

この主張に対して，高等裁判所の判決では，以下のように述べています.

高等裁判所の判決（抜粋）

「特許に値すべき発明の本体は自然法則の利用によつて一定の文化目的を達する技術的考案ということにある.

従つてそれが寄与し，貢献し，利用せられる産業の種別については格別制限はないが，その利用の態様はあくまで技術産業的であるべきであり，あらゆる産業に寄与しうべき工夫考案のうちこのような性質をおびた発明のみが特許法の保護を受けうるのである．わが特許法は発明のこの特質を表現する語句として工業的という文字を使つたのであつて，その由来するところは，産業部門としての工業は技術産業の中枢をなすからでありこれがため工業的発明を工業に関する発明の意に限定したり，又は広く産業に関する発明の意に解釈する要は少しもないのである.」

「原告の本願発明はその主張の要旨において明なように欧文字，数字，記号，等を適当に組み合せて電報用の暗号を作成する方法であつて，たとえその産業上殊に商

取引において貢献するところが大であり，又，その作成方法が科学的に精緻を極めているとしても，その間何等装置を用いず，又，自然力を利用した手段を施していないのであるから，これを暗号による通信方法であると解しても，暗号による思想表現の方法であるというの外なく，場合により他の権利たとえば著作権により保護されることのあるのは格別，到底特許に値する工業的発明であるということはできないのである.」

判決は，旧特許法の「工業的」という言葉について，狭義の工業に限られるものではないことを認めつつも，それがすべての「産業」に広げられるべきではなく，「技術産業的」なものに限られるという判断を示しています．特許すべき発明は「自然法則の利用」によるものであるという点も，注目すべきでしょう．

最高裁の判決も，この高裁の判決を是認したものとなっています．なお，以下の文で「所論」とは，出願人の主張を指しています．

最高裁判所の判決（抜粋）

「原判決は，あらゆる発明がすべて特許能力を有するものではなく，その発明が工業的であることを要する旨説示したのは正当であるから，本願発明が所論のごとく発明には該当するとしてもそれだけでは特許能力を有するものとはいえない.」

これらの判決によると，暗号を特許にするのはハードルが高そうです．確かに現代の暗号は，コンピュータ上で処理されるものであり，人間が図表を参照しながら手作業で翻訳するようなものではありません．しかし，特に公開鍵暗号を中心とした現代の暗号は，数学的アルゴリズムそのものともいえます．そして，本質が数学的アルゴリズムだからといって，それを明細書にそのまま記載してしまうと，「暗号による思想表現の方法であるというの外なく」ということにより，特許法上の発明ではないということになってしまいます．数学的アルゴリズムとは，数学的な「思想表現の方法」に他ならないからです．

このように暗号を数学的アルゴリズムとして記載してしまうと，そのアルゴリズムが，数学的に高度であるとか，インターネット上の通信に使われるもので電子商取引にかかせないものであるという主張をしても，特許を受けることはできなくなってしまいます．判決は「その作成方法が科学的に精緻を極めているとしても」，「これを暗号による通信方法であると解しても」，「たとえその産業上殊に商取引において貢献するところが大であり」といった条件を挙げたうえで，それでも発明ではないとしているからです．

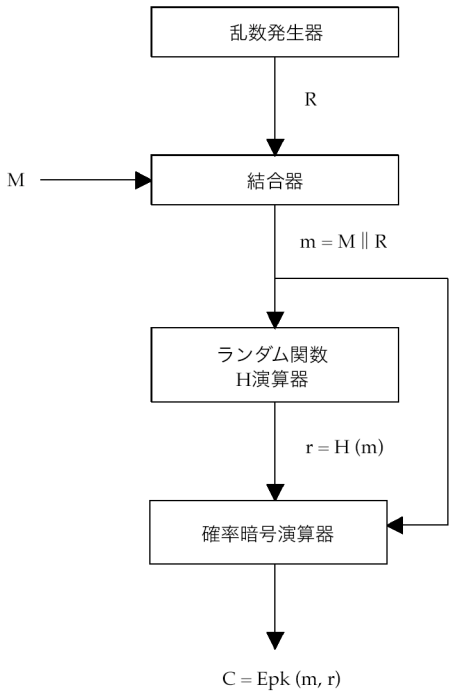

図-1　藤崎－岡本変換を実現する装置

それでは，暗号を特許にする道はないのでしょうか．いえ，道はあるのです．現実に，数学的アルゴリズムに基づいた暗号に関する発明でも，特許になったものは数多く存在します．そのように暗号を特許とすることができる根拠も，先ほどの判決に存在するのです．

それは，先ほどの判決のうち「その間何等装置を用いず，又，自然力を利用した手段を施していないのであるから」という記載です．この個所を逆に読めば，何らかの装置を用い，自然力を利用した手段を施したものであれば，数学的アルゴリズムに基づく暗号といえども，特許とすることができる，という考えが導き出せるのです．つまり，**暗号は，数学的アルゴリズムとしては特許にならないが，自然法則を利用した手段を有する暗号装置，あるいは，そのような暗号装置を利用した暗号方法として特許にすることが可能**なのです．

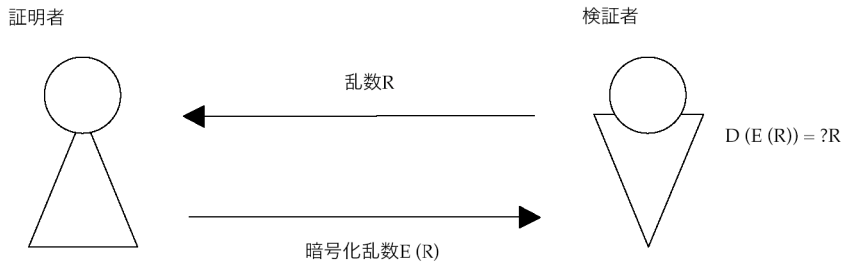

図 -2　人手によるチャレンジ－レスポンス認証

■具体的な事例

それでは，暗号装置として特許になった事例をご紹介しましょう．ここでは，特許請求の範囲の一部のみを挙げます．発明の詳細な説明を参照すれば,「手段」はハードウェアであると解釈できるので，この発明は「自然法則を利用した」技術的思想ということができます．

特許第 3306384 号（請求項 1）

公開鍵暗号 EPOC/PSEC に用いられている，藤崎－岡本変換に関する発明です（**図 -1**）．

「乱数 R を生成する乱数発生手段と，上記乱数 R と平文 M とを結合して値 m を生成する結合手段と，上記値 m を関数 H でランダム化した値 r = H（m）を演算するランダム関数演算手段と，上記値 m と上記値 r と公開鍵 pk を入力して，m を確率的公開鍵暗号により暗号化した暗号文 C = Epk（m, r）を演算する暗号化演算手段と，を具備する暗号装置.」

次に，やや応用的な暗号プロトコルについて，ありがちな例をとりあげて解説します．

「発明」に該当しないと考えられる例

「検証者が証明者を認証するための認証方法であって，検証者が,乱数を生成して証明者に送付するステップと，証明者が，受け取った乱数を暗号化して検証者に送付するステップと，検証者が，受け取った暗号化乱数を復号して生成した乱数と比較し，一致した場合に証明者を正当な者として認証するステップとからなる認証方法」

一般にチャレンジ－レスポンス認証といわれるものです．すでによく知られた手法なので，これで特許を取得することはできないでしょう．しかし，それ以前に問題なのは，この記載では「自然法則を利用した」技術的思想とはいえないことです．

確かに，プロトコルを説明する上では，この記載で十分理解することができます．ですが，何らかの装置や自然法則を利用した手段として解釈できるものが，この記載には何もありません．「証明者」と「検証者」という 2 人の人間が，連絡を取り合いながら，一定の手続きを行っているとしか解釈できないのです（**図 -2**）．

それでは，次のような記載はどうでしょうか．

「コンピュータと通信網を用いて，検証者が証明者を認証するための認証方法であって，検証者が，乱数を生成して証明者に送信するステップと，証明者が，受信した乱数を暗号化して検証者に送信するステップと，検証者が，受信した暗号化乱数を復号して生成した乱数と比較し，一致した場合に証明者を正当な者として認証するステップとをコンピュータにより実行する認証方法」

残念ながら，この記載でも特許を受けることができません．手続きを行う主体は,依然として「証明者」と「検証者」という 2 人の人間です．コンピュータや通信網は,人間が道具として使っているにすぎません（文献 3）の「特許にならない事例」もご参照ください）．「ソフトウェアによる情報処理が，ハードウェア資源を用いて具体的に実現されている」という，ソフトウェア関連発明の審査基準にも適合しないのです．

ここでは，「…者」という用語を使った記載についてとりあげましたが，注意すべき用語は他にもあります．センター，エンティティ，認証局，…機関といった用語です．電子マネーのようなものであれば，銀行，店舗と

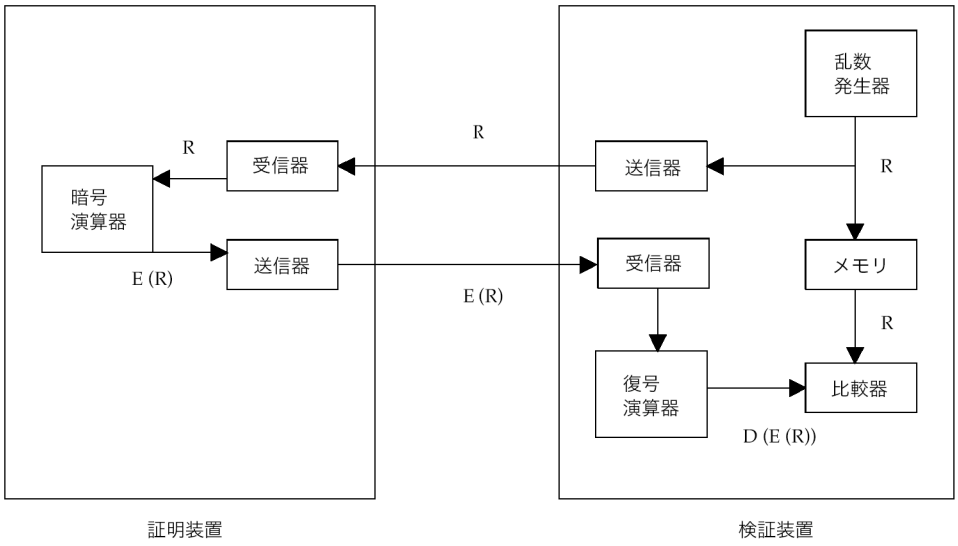

図 -3　チャレンジ－レスポンス認証を実現するシステム

いう用語も含まれるでしょう．これらの用語はみな，第一義的には，ハードウェア資源というより社会的な組織や機構といったものを表すと考えられます．したがって，ソフトウェア関連発明の審査基準に適合しないとみなされるのです．

では，どのような記載であれば，成立性の要件を満たすといえるのでしょうか．先ほどの例に対応するものを，以下に示します．このような記載であれば，ソフトウェアによる情報処理が，ハードウェア資源を用いて具体的に実現されており，自然法則を利用した技術的思想ということができるでしょう．ただし，発明の詳細な説明にも，このような記載に対応するような，ハードウェアとしての記載が存在することが必要です（**図 -3**）．特許第 3035358 号，特許第 2511464 号，特許第 2631776 号の記載なども参考になるでしょう．

「発明」に該当すると考えられる例

「検証装置が証明装置を認証するための認証方法であって，検証装置が，乱数生成手段により乱数を生成して，当該乱数を記憶手段に記憶するとともに送信手段により証明装置に送信するステップと，証明装置が，受信手段により受信した当該乱数を，暗号化手段により暗号化して，送信手段により検証装置に送信するステップと，検証装置が，受信手段により受信した暗号化された乱数を，復号手段により復号し，復号された乱数を前記記憶手段に記憶された乱数と比較手段により比較し，一致した場合に証明装置を正当な装置として認証するステップとを有する認証方法．」

■おわりに

暗号に関する発明については，明細書の「表現」がいかに重要か，ご理解いただけたでしょうか．形式的すぎる，と思われるむきもあるかもしれませんが，一定の形式さえ満たしていればよい，と考えることもできるでしょう．研究開発の段階では数学的アルゴリズムとして記述される暗号も，現実に商取引の対象となる産業製品としては，ハードウェアや，ハードウェア上で実行されることを前提としたソフトウェアといったかたちで提供されます．特許権を行使する対象も，これらハードウェアやソフトウェアのはずです．「権利行使のしやすさ」を考慮すれば，このような，権利の対象をハードウェアやソフトウェアに明確化した記載は，むしろ望ましいといえるのではないでしょうか．

参考文献
1）最高裁判所民事判例集，第 7 巻，第 4 号，pp.461-481．
2）とっきょの話 第 3 回 コンピュータ・ソフトウェア関連発明の審査基準の概要，情報処理，Vol.43, No.6, pp.670-673（June 2002）．
3）とっきょの話 第 5 回 ビジネス関連発明の動向，情報処理，Vol.43, No.8, pp.908-911（Aug. 2002）．

（平成 14 年 12 月 16 日受付）