

平成20年2月29日判決言渡

平成19年(行ケ)第10239号 審決取消請求事件

口頭弁論終結日 平成20年2月27日

判 決

原 告	ルーセント テクノロジーズ インコーポレーテッド
訴訟代理人弁理士	岡 部 正 夫
同	加 藤 伸 晃
同	朝 日 伸 光
同	三 山 勝 巳
被 告	特 許 庁 長 官
	肥 塚 雅 博
指 定 代 理 人	野 仲 松 男
同	橋 本 正 弘
同	吉 岡 浩
同	山 本 章 裕
同	内 山 進

主 文

- 1 原告の請求を棄却する。
- 2 訴訟費用は原告の負担とする。
- 3 この判決に対する上告及び上告受理申立てのための付加期間を30日と定める。

事 実 及 び 理 由

第1 請求

特許庁が不服2004-13406号事件について平成19年2月21日にした審決を取り消す。

第2 事案の概要

本件は、アメリカ国法人である原告が、「ビットの集まりの短縮表現を生成する方法」とする名称の後記発明（本願発明）につき特許出願をしたところ、拒絶査定を受けたので、これを不服として審判請求をしたが、特許庁から請求不成立の審決を受けたことから、その取消しを求めた事案である。

争点は、データ操作に関し長いデータストリングを短いデータストリングに変換する方法であるハッシュ法によりコンピュータ処理を高速に行うための計算手法（アルゴリズム）に関する本願発明が、特許法2条1項ひいては同法29条1項柱書にいう「発明」に該当するか、である。

第3 当事者の主張

1 請求の原因

(1) 特許庁における手続の経緯

原告は、平成11年10月18日、1998年〔平成10年〕10月20日の優先権（米国）を主張して、名称を「ビットの集まりの短縮表現を生成する方法」とする発明について特許出願（特願平11-295775号、請求項の数3、以下「本願」という。甲1）をしたところ、平成15年10月28日付けで拒絶理由通知を受けた。そこで平成16年2月9日付けで特許請求の範囲の記載を変更する補正（請求項の数4、以下「第1次補正」という。甲4）をしたが、平成16年3月29日付けで拒絶査定を受けたので、平成16年6月29日付けで不服の審判請求をした。

特許庁は同請求を不服2004-13406号事件として審理し、その中で原告は平成16年7月29日付けで特許請求の範囲の記載を変更する補正（請求項の数4、以下「第2次補正」という。甲6）をしたが、特許庁は平成19年2月21日、第2次補正を却下した上、「本件審判の請求は、成り立たない」との審決（出訴期間として90日附加）をし、その謄本は平成19年3月5日原告に送達された。

(2) 発明の内容

第1次補正時（平成16年2月9日）の特許請求の範囲は、前記のとおり請求項1～4から成るが、その内容は次のとおりである（以下、そこに記載された発明を順に「本願発明1」～「本願発明4」といい、これらを総称して「本願発明」という）。

「【請求項1】 ビットの集まりの短縮表現を生成する装置において、
少なくとも n ビットを有するキーと、入力された n ビットの集まりとの和をとり、
前記和を2乗して、和の2乗を生成し、
 p を、 2^n より大きい最初の素数以上の素数として、前記和の2乗に対して、法 p 演算を実行して法 p 演算結果を生成し、
 n より小さい n_1 により、前記法 p 演算結果に対して、法 2^{n_1} 演算を実行して法 2^{n_1} 演算結果を生成し、
前記法 2^{n_1} 演算結果を出力している、ビットの集まりの短縮表現を生成する装置。

【請求項2】 ビットの集まりの短縮表現を生成する装置において、
少なくとも n ビットを有する第1のキーと、入力された n ビットの集まりとの和をとって、第1の和を生成し、
前記第1の和を2乗して、第1の和の2乗を生成し、
前記第1の和の2乗と、少なくとも n ビットを有する第2のキーとの和をとって、第2の和を生成し、
 p を、 2^n より大きい最初の素数以上の素数として、前記第2の和に対して、法 p 演算を実行して法 p 演算結果を生成し、
 n より小さい n_1 により、前記法 p 演算結果に対して、法 2^{n_1} 演算を実行して法 2^{n_1} 演算結果を生成し、
前記法 2^{n_1} 演算結果を出力している、ビットの集まりの短縮表現を生成

する装置。

【請求項 3】 ビットの集まりの短縮表現を生成する装置において、
少なくとも n ビットを有するキーと、入力された n ビットの集まりとの和をとり、
前記和を 2 乗して、和の 2 乗を生成し、
前の 3 つのステップを、ステップが繰り返されるごとに相異なるキーを使用して少なくとも 1 回繰り返して、複数の和の 2 乗を生成し、
前記複数の和の 2 乗の和をとって総和を生成し、
 p を、 2^n より大きい最初の素数以上の素数として、前記総和に対して、法 p 演算を実行して法 p 演算結果を生成し、
 n より小さい 1 により、前記法 p 演算結果に対して、法 2 演算を実行して法 2 演算結果を生成し、
前記法 2 演算結果を出力している、ビットの集まりの短縮表現を生成する装置。

【請求項 4】 該生成された短縮表現をメッセージ認証に用いている通信装置である請求項 1、2 又は 3 の装置。」

(3) 審決の内容

審決の詳細は、別添審決写しのとおりである。

その理由の要点は、第 2 次補正は、願書に最初に添付した明細書、特許請求の範囲又は図面に記載されていないだけでなく、自明に導き出せる事項であると認めることもできないから、特許法（以下「法」という）17 条の 2 第 3 項の規定に違反し却下されるべきである、第 1 次補正に係る本願発明 1～4 は、いずれも法 2 条 1 項にいう「発明」に該当しないから法 29 条 1 項柱書の規定により特許を受けることができない、というものである。

(4) 審決の取消事由

しかしながら，本願発明 1 ~ 4 が法 2 条 1 項に規定された「発明」に該当しないとした審決の判断には，以下に述べるとおり誤りがあるから，違法として取り消されるべきである。

ア 審決は，本願発明 1 ~ 4 が法 2 条 1 項の規定する「発明」に該当しないことの理由として，本願発明 1 を引用の上，「...これら各段階は，ビットの集まりに対する数学的計算の段階であって，<1>対象の物理的性質や技術的性質に基づく情報処理を特定したものということとはできず，又，<2>上記数学的計算が機器等に対する制御や制御に伴う処理に関与するものでもない。更に，<3>本願発明 1 は『ビットの集まりの短縮表現を生成する装置』と記載されているのみであって，『ビットの集まりの短縮表現を生成する装置』としての具体的な回路構成や，ソフトウェアとハードウェア資源とが協働した具体的手段が何ら記載されていない。」(9 頁下 7 行 ~ 下 1 行。なお，<1> ~ <3>は原告が挿入) と述べる。

しかし，上記<3>の認定判断については，ソフトウェアとハードウェア資源との協働についての解釈を争い，又は，法 2 条 1 項の「発明」は上記<1> ~ <3>の形態に限られるものではなくそれ以外であっても該当する形態があることの審理に及んでいないから審理不尽であるとして争う。

以下，本願発明が「発明」に該当することについて，本願発明の技術的課題，特許請求の範囲に記載された具体的構成及び本願発明の技術的作用効果の観点から述べる。

イ 第 1 次補正後の本願明細書(甲 1，4)の段落【0013】~【0014】に記載されているように，本願発明の課題は，長さ w ワードのキーと長さ w ワードのハッシュされるメッセージのハッシュ化において，計算量を従来に比べて減らすことにある。換言すれば，ハッシュ化を実行するデジタル演算装置(プロセッサ又はコンピュータ)において計算時間を減らすことにある。

例えば簡単な具体例で述べると、80ビットのキーと80ビットのメッセージがあるときに、1ワードを8ビットとすると10ワードの長さのキーとメッセージとなるから、従来は w^2 すなわち $10^2 = 100$ 回の乗算計算が行われていた。これに対し本願発明では、 $(w^2 + w) / 2 = 110 / 2 = 55$ 回の乗算計算となる。デジタル演算回路又はプロセッサの本来的ハードウェア上の性質からは、乗算回数が実質的に計算時間を決定する。このような計算時間を減らすことはハッシュ化の実際の応用(装置)にあって要望される技術的課題であることは明らかである。

ウ 原告が本願発明は法2条で規定する「自然法則を利用した技術的思想」であるとする主張の核心は、本願発明の技術的作用効果の性質に基づいたものである。本願発明の技術的作用効果は、上記技術的課題に対応したハッシュ化を実行する装置において計算時間を減少させたことにあり、この作用効果自体は、実際のハードシステムで要望される技術的なものである。

すなわち、デジタル演算装置(コンピュータ)は、 x^n 乗算を n 回のループ(n 回の繰返し演算)により行う。ソフトウェアは論理であるにしても、コンピュータは自然法則に従う物理的装置である以上、1回のループに有限の時間を要し、計算回数は実行時間の長さに対応する。数学的な意味ではアルゴリズムの実行速度に意味はないが、実際にコンピュータがそのアルゴリズムのプログラムを実行するには必ず一定の時間がかかる。この場合、アルゴリズムの性能はコンピュータ上での実行時間又は計算量で評価される。計算機でのアルゴリズムの実際の実行時間は、ハードウェアの性能、コンパイラの性能、プログラミング技術等のファクターに左右されるから、あるアルゴリズムの実行時間の正確な絶対値をこれらファクター抜きで論じることはできないが、そのような個々の事情を除外したアルゴリズムの相対的な評価は、「このアルゴリズムの実行時間は、入力の大きさ n の2乗に比例する」という形で表すことができる($O(n^2)$ のA

ルゴリズム」という。「O」は order (桁) の意味であり、「桁の概念」という粗い評価であるが、特別な利用形態を問わないコンピュータを前提としても、アルゴリズムの計算時間の相対的評価法として用いられているものである。)

本願発明は、ハッシュ法のアルゴリズムを実行する演算装置として定義されているが、アルゴリズムの方に新規な内容があり、コンピュータ内の特別なハードウェア資源の操作形態を前提とするものではない。しかし、本願発明は、人間がペーパーと鉛筆でそのアルゴリズムを計算することを規定するものではない。この場合の計算スピードはその人の有する知識・経験に依存するのだから自然法則によるとはいえず、それでは本願発明の技術的有意義性は生じないからである。本願発明は、明らかに n ビットの集まりを入力し、それを演算処理し、そして演算結果として入力された n ビットの集まりの短縮表現を出力している装置を規定しており、それは物理的な電気回路装置である。そして、当該アルゴリズムは、コンピュータのような有限時間で動作する物理的構造上で実行されるからこそ、計算回数(実行時間)が従来技術に比して約 $1/2$ になるという技術的作用効果を有するのであり、これは、当該アルゴリズムが、コンピュータの特別な利用形態には係っていないが、コンピュータ構造の本来的に有するハードウェア資源の物理的性質そのものに係っているからである。

このように、本願発明のソフトウェアは、自然法則の下に動作するハードウェア資源と組み合わせられることによって初めて技術的作用効果を呈しているのであるから、技術思想上意味のある協働をしていることは明らかであり、また、自然法則を利用した上での技術的作用効果(すなわち、高速処理)を得ているのである。したがって、本願発明は具体的構成の特定されている技術的思想であり、自然法則を利用した技術的思想であるから、法 2 条の規定する「発明」であると認められるべきである。

エ このような「装置」の発明としての本願発明の具体的構成は、示された演算内容に応じて規定される演算回路として明確に記載されている。

すなわち、本願発明は、入力されたnビットの集まりの演算処理ということであるから、それはデジタル論理演算を意味している。デジタル論理演算回路については、布線論理回路 (Wired Logic Circuit) と蓄積プログラム論理回路 (Stored Program Logic Circuit すなわちプロセッサ/コンピュータ) の2つのタイプがある。

このうち布線論理回路は、特定の演算即ち加算、減算、乗算、除算を行う固定的な特殊回路であり、例えば、布線論理回路の2ビットバイナリ加算器、4×4乗算器等は周知であるところ、他の乗算器を含め、本願発明1に記載の演算内容個々にそのまま対応したデジタル論理演算回路の要素は知られた存在であるから、演算内容を記載することは、そのままそれぞれの論理演算回路を直接的に自ら対応的に特定することになり、そのような特定の演算を行うデジタル論理演算回路を組み合わせ配置して布線することで本願発明1の構成に至るのであるから、本願発明1の演算内容の記載は本願発明1の構成を具体的に記載していることになるといえるべきである。

また蓄積プログラム論理回路、すなわちマイクロプロセッサ (CPU) は、メモリに時間的に逐次実行されるべき一連の命令であるプログラムが蓄積されている。クロック各々に応じ命令が逐次読み出されその命令に応じた論理演算が実行される。そして、蓄積プログラム演算論理回路の場合であっても、本願発明1に記載の演算個々とそのまま対応した具体的プログラムの命令内容は知られたものであるから、演算内容を記載することは、それぞれのプログラムを直接的に自ら特定することになり、蓄積プログラム演算論理回路によってプログラムが特定される以上、その論理回路、すなわち装置構成が具体的に記載されているといえるべきである。

なお、装置としての具体的な構成自体が記載されているとする点については、本願発明 2 ~ 4 も同様である。

オ 以上のように、本願発明は装置としての具体的な構成自体は記載されているところ、その上で本願発明の技術的思想性に言及すれば次のとおりである。

本願発明 1 の新規なハッシュ法のアルゴリズムは 普遍、本願発明 2 は 強普遍そして本願発明 3 は 普遍であり、衝突確率の基準を満たし、いずれも実用的なハッシュ手法である(本願明細書の段落【0016】~【0021】及び【0028】~【0032】参照)。つまり、単に発明者が勝手に定めた実用上無意味なアルゴリズムではない(その結果、本願発明 4 も実用的な技術内容である。)

そして、本願発明は、上述のように実用的なハッシュ手法であると同時に、従来技術のハッシュ手法(本願明細書の段落【0021】の式(4)と(5))に比べ、長さ w ワードのストリングをハッシュするのに w^2 回の演算ではなく $(w^2 + w) / 2$ 回の演算で済む効率的なハッシュ手法が実現されている(段落【0014】参照)。すなわち、本願発明 1 ~ 4 により、実用的で、計算時間の短縮された効率的なハッシュ装置が提供されている。

このような本願発明のハッシュ装置の応用分野の 1 つは、本願明細書の段落【0010】に述べられているテキストストリングの探索である。すなわち、元のテキストの短縮形(ダイジェスト)を記憶し、そのダイジェストを探索し検出されたダイジェストに対応する元のテキストを得る。これは元のテキストの長いビットストリングを探索するよりも効率的な手法である。

他の応用分野として、本願明細書の段落【0011】に述べられているように、通信において通信途中でメッセージが改ざんされていないかを調べるメッセージ認証にも用いられる。送信側でメッセージをハッシュ化し

てダイジェスト(この場合はタグと称する)を生成し、メッセージとタグを送信する。受信側で受信メッセージを自らハッシュ化し受信側のタグを生成すると、この受信側生成タグと送信側から送られてきたタグを比較してその一致性を照合する。もし通信途中で通信メッセージが改ざんされているとタグの照合において不一致が発生する。これらの照合の手法は電子署名に適用されている。

このように、本願発明はその具体的構造が明確であり、かつ、実用的応用分野があり、例えば探索・通信等の技術的分野に適用されるものである。

広辞苑(新村出編、岩波書店発行、1991年〔平成3年〕第3版第9刷、甲8)によれば、「技術」とは 技巧、技芸と、「(technique)科学を実地に応用して自然の事物を改変・加工し、人間生活に利用するわざ」とある。特許法の保護の対象としての技術は、 の技巧・技芸というようなものではなく、後者の の技術の意味であり、したがって、法2条1項の「自然法則を利用した技術的思想」とは、前述の技術の の内容にほかならないとすると、本願発明がハッシュ法のコンピュータ上での高速処理という一定の目的を達成するための具体的手法であって、実際に利用できるものである以上、これが法の保護の対象となり得る資質を有する、科学的で人間生活に利用される技術であることは明らかである。

力 なお、審決は、特許庁の審査基準(甲7)第 部「特定の技術分野の審査基準」、第1章「コンピュータ・ソフトウェア関連発明」の3.2「『発明』に該当するか否かの判断例」(20頁以下)を参照し、本願発明は「ビットの集まりの短縮表現を生成する」装置を実現するためにはどのようなハードウェア資源をどのように利用するかについての具体的な装置構成について何ら記載しておらず、計算処理を実行するソフトウェアとハードウェア資源とが協働していないから、上記判断例の事例2-1で「『発明』に該当しない。」とされた請求項2又は3の類型に本願発明が該当すると

したものと解される。

しかし、本願発明は請求項 2 の事例というより、むしろ内容的に協働関係を有する請求項 4 の事例に該当するとすべきものである。すなわち、事例の請求項 4 の発明では、式 $s = (m + n)^2 - (m - n)^2 / 4$ という演算ソフトウェア自体に技術的意味があるのでなく、2 乗テーブルというハードウェア資源の具体的構成との組合せ、すなわち協働において初めて $m \times n$ の乗算をする上で式 s に技術的作用効果が生じる場合である。一方、前述のとおり、本願発明は、ソフトウェアとハードウェア資源との協働なくしては本願発明でのハッシュ法の計算回数を減少させ結果として演算処理を高速化するという技術的作用効果を生じないのであるから、本願発明は「計算処理を実行するソフトウェアとハードウェア資源とが協働している」と解釈されるべきもので、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場合といえ、むしろ、ハードウェア資源との協働がなされている点では、同事例で「『発明』に該当する。」ものとされた請求項 4 の発明の類型とされるべきものである。

審決は、本願発明のハッシュアルゴリズムは、有限な計算時間を必ず有するという本質的な自然法則上の性質を有する演算装置（計算機）において又はそれと組み合わされたときに初めてその技術的作用効果を呈する点で、上記請求項 2 又は 3 の発明とは異なることを看過したといえる。

あるいは、審決は、上記請求項 4 の類型を狭義に解釈した上で、本願発明はこれに当たらないとしたものとも解されるが、前記のとおり、本願発明の作用効果はハードウェアの本来の性質（本願発明の場合は乗算に時間を要するというデジタル演算回路の性質）に起因し、又はそこから由来していることからすれば、審査基準に従った審査にあつて「ソフトウェアとハードウェア資源の協働」とは上記請求項 4 の場合よりもより広義に解釈すべきで、それを狭義に解釈した審決の判断は誤りであるし、審査基準の

枠外についての審理に及んでいない点は審理不尽である。

2 請求原因に対する認否

請求原因(1)ないし(3)の各事実はいずれも認めるが、同(4)は争う。

3 被告の反論

審決の認定判断は正当であり、原告主張の取消事由はいずれも理由がない。

- (1) 法2条1項は、「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。」と規定しているから、請求項に係る発明が、特許法上の「発明」に該当するか否かは、それが「自然法則を利用した技術的思想の創作」に該当するか否かに従って判断されることになる。

そして、本願発明1は、「ビットの集まりの短縮表現を生成する装置」に係るものであり、本願発明1におけるビットの集まりの短縮表現を生成する処理は、ビットの集まり(数値)に対し、数学的な演算を行って、その短縮表現(別の数値)を求めるもの、すなわち、数学的課題の解決方法又は数学的な計算手順を示したものである。

この点、数学的課題の解決方法自体や数学的な計算手順を示したにすぎないものが、「自然法則を利用した技術的思想の創作」に該当するものでないことは明らかである(東京高裁平成16年(行ケ)第188号・平成16年12月21日判決・判例時報1891号139頁参照)。

その上で、数学的課題の解決方法や数学的な計算手順を含むものが「自然法則を利用した技術的思想の創作」に該当する場合とは、次の3つのケースに整理することができる。

まず、数学的課題の解決方法や数学的な計算手順を含むものであっても、機器等に対する制御又は制御に伴う処理を具体的に行うもの(ケース1)、又は対象の物理的性質や技術的性質に基づく情報処理を具体的に行うもの(ケース2)は、その処理が自然法則を利用したものといえるから、「自然法則を利用した技術的思想の創作」に該当する。そして、これら以外の場合

には、その処理内容自体が自然法則を利用したものとはいえないのであるが、数学的課題の解決方法や数学的な計算手順に関する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場合（ケース3）には、そのことをもって自然法則を利用していると認めることができ、「自然法則を利用した技術的思想の創作」に該当する。

審決は、このような認識のもとに、本願発明1について、「対象の物理的性質や技術的性質に基づく情報処理を特定したもの」（ケース2）であるか、「機器等に対する制御や制御に伴う処理に関与するもの」（ケース1）であるか、「ハードウェア資源を用いて具体的に実現されているもの」（ケース3）であるかを順次検討して、そのいずれにも該当しないから、「自然法則を利用した技術的思想の創作」ではなく、特許法上の「発明」に該当しないとしたものである。

(2)ア これに対し原告は、本願発明のハッシュアルゴリズムは、有限な計算時間を必ず有するという本質的な自然法則上の性質を有する演算装置（計算機）において又はそれと組み合わされたときに初めて、その技術的作用効果を呈する旨主張する。

イ まず、原告の主張する本願発明のハッシュアルゴリズム（ビットの集まりの短縮表現を生成する手法）の技術的作用効果の内容であるが、これは、従来手法に比べ、長さ w ワードのストリング（ビットの集まり）をハッシュするのに w^2 回の演算でなく $(w^2 + w) / 2$ 回の演算で済み、演算スピードがほぼ倍になるというものである。

そのような演算スピードの高速化は、本願発明のハッシュアルゴリズムが、その計算過程において、ハッシュ対象のビットの集まりとキーの乗算 $(m \times a)$ を用いる代わりに、それらの和の2乗 $(m + a)^2$ を用いるとともに、この2乗の演算を、特定の演算手法（2乗すべき数値をワード単位に分解して、ワード単位の乗算結果の組み合わせとして2乗を計算し、

その際、同じワードの組合せについては、繰り返し乗算を行わずに、加算（ $\times 2$ ）で済ませる）により行うことで、初めて得られるものである。

しかし、本願の特許請求の範囲の各請求項においては、ハッシュ対象のビットの集まりとキーの和の2乗（ $m + a$ ）²を用いることの記載はあるが、この2乗の演算を行うための演算手法については何ら特定されていないから、本願発明により演算スピードがほぼ倍になるという技術的作用効果が得られるとする原告の主張は、本願の特許請求の範囲の記載に基づくものではなく、失当である。

ウ また、一般にアルゴリズムの改善による計算ステップの減少は、改良されたアルゴリズムが特定のハードウェア資源の利用を前提とするのであれば別として、人がペーパーと鉛筆で行う場合であっても、計算機上で実行する場合であっても同様に演算の高速化をもたらす。むしろ、計算量が膨大になった場合に、人手で計算をすることは現実的ではないが、それは実際に計算可能な問題規模の限界の問題でしかない。

この点に関し原告は、人がペーパーと鉛筆で計算を行う場合の計算スピードはその人の有する知識・経験に依存するのだから自然法則によるとはいえず、本願発明による演算スピードの高速化は、有限な計算時間を必ず有するという本質的な自然法則上の性質を有する演算装置（計算機）で実行した場合にのみ生ずると主張するが、原告も自認するように、計算機上による実行の場合でも、その実際の実行時間は、ハードウェアの性能やコンパイラの性能、プログラミング技術等に依存するのであって、アルゴリズムの改良による計算ステップの減少を論ずる場合には、これらの個別的要素を排除して考える必要がある点では、人がペーパーと鉛筆で計算を行う場合と変わるところはない。

(3) また原告は、本願発明は入力された n ビットの集まりの演算処理であるからデジタル論理演算を意味しているところ、デジタル論理演算回路には布線

論理回路と蓄積プログラム論理回路の2つのタイプがあり、いずれの場合であっても、本願発明に記載の演算内容個々にそのまま対応したデジタル論理演算回路の要素又は具体的プログラムの命令内容は知られたものであるから、演算内容を記載することは、そのままそれぞれの論理演算回路又はプログラムを直接的に自ら特定していることになり、装置構成が具体的に記載されている旨主張する。

確かに、本願発明における「ビットの集まりの短縮表現を生成する」処理の各段階の演算内容を実現するようなデジタル論理演算回路の要素やプログラムの命令内容は知られている。しかし、原告も自認するように、布線論理回路として実現するか、蓄積プログラム論理回路として実現するかによっても、すでに2通りの実現方法があり、同じ演算要素を実現するのにも、様々な具体的構成が考えられるのであるから、各段階の演算内容を実現する具体的な回路やプログラムの例が公知であるからといって、演算内容を記載することが、そのまま装置の具体的構成を特定することにはならない。

請求項に係る発明の認定は、あくまで請求項の記載に基づいて行わなければならないのであって、請求項に記載された処理の各段階を実現するための具体的な構成が知られているだけでは、請求項に記載された処理がハードウェア資源を用いて具体的に実現された「自然法則を利用した技術的思想の創作」に当たり特許法上の「発明」に該当する、というには十分でない。

- (4)ア さらに原告は、本願発明のハッシュ手法は、衝突確率の基準を満たす実用的なハッシュ手法であると同時に、計算時間の短縮された効率的なハッシュ手法であって、テキストストリングの探索やメッセージ認証などの実用的応用分野があると主張する。

この点、本願発明のハッシュ手法（ビットの集まりの短縮表現を生成する処理）が、衝突確率を考慮したものであり、テキストストリングの探索やメッセージ認証などの実用的応用分野を有していることに異論はない。

しかし、上記(1)で述べた「ケース1」や「ケース2」のように、数学的課題の解決方法や数学的な計算手順に関する処理が、機器等に対する制御又は制御に伴う処理を具体的に行うもの、又は対象の物理的性質や技術的性質に基づく情報処理を具体的に行うものとして、特許法上の「発明」に該当するものといえるためには、それらの点が特許請求の範囲の記載により特定されている必要があるのであって、単に実用的な応用の可能性があるだけで、特許請求の範囲にはそれらに実際に応用されたものとして記載されていないものは、「自然法則を利用した技術的思想の創作」すなわち特許法上の「発明」に該当するといえないことは当然である。

そして、本願発明におけるビットの集まりの短縮表現を生成する処理は、その特許請求の範囲の記載によれば、ビットの集まり（数値）に対し、数学的な演算を行って、その短縮表現（別の数値）を求めるものであり、何らの応用分野にも限定されていないから、処理対象である「入力されたnビットの集まり」は、何らかの対象の物理的性質や技術的性質を反映したものであるのではなく、演算処理の内容にも、何らかの対象の物理的性質や技術的性質への考察は含まれていない。

したがって、本願発明におけるビットの集まりの短縮表現を生成する処理は数学的な計算手法にすぎないのであって、このことは実用的な応用分野が知られていることにより否定されるものではない。

イ 次に原告は、本願発明は、ハッシュ法のコンピュータ上での高速処理という一定の目的を達成するための具体的手法であって、実際に利用できるものであるから、法の保護の対象となり得る資質を有する科学的で人間生活に利用される技術であると主張するが、法2条の定める自然法則を利用した技術的思想における技術の内容を広辞苑による技術の定義と同一であるとする原告独自の解釈に基づくものであって、失当である。

ウ また原告は、本願発明の演算手法は、計算速度が自然法則に依存した物

理的回路装置の固有の性質と結びついて初めて所与の作用効果が生じるのであるから，本願発明は，物理的回路装置(ハードウェア)の自然法則上で動作する性質を利用した技術として，すなわち自然法則を利用した技術思想として，法2条の発明の定義に適うものであると主張するが，前記のとおり，本願発明の演算手法は，計算速度が自然法則に依存した物理的回路装置の固有の性質と結びついて初めて所与の作用効果が生じるものとはいえず，そもそも，演算スピードがほぼ倍になるという技術的作用効果も，本願の特許請求の範囲の記載に基づくものではないから，原告の上記主張も失当である。

- (5)ア なお原告は，本願発明のハッシュアルゴリズムは，有限な計算時間を必ず有するという本質的な自然法則上の性質を有する演算装置（計算機）において又はそれと組み合わされたときにその技術的作用効果を初めて呈する点でハードウェア資源との協働がなされているから，審査基準第 部の事例2 - 1の請求項2又は3の発明とは異なり，むしろ請求項4の発明の類型とされるべきであるにもかかわらず，本願発明を事例2 - 1の請求項2又は3の類型に該当するとした審決の判断は誤りである旨主張するところ，このような原告の主張は，審決が，本願発明を審査基準第 部の事例2 - 1の請求項2又は3の類型に該当するとして，特許法上の「発明」ではないと判断したとの理解に基づくもの考えられる。

しかし，審決は審査基準第 部の事例2 - 1について言及していないし，実質的にも，単に，本願発明を審査基準の事例の類型に当てはめることによって特許法上の「発明」に該当するか否か判断したものではない。念のため付言すると，審査基準に記載された種々の事例は，あくまで仮想的な判断事例を参考として示したものであって，網羅的なものではないから，個別の案件を，審査基準の事例のいずれかの類型に当てはめることにより最終的な結論を導くことを想定したものではない。

したがって、原告の上記主張は審決を正解しないものであって、失当である。

イ また原告は、本願発明のハッシュアルゴリズムは、演算装置（計算機）において又はそれと組み合わせられたときに初めてその技術的作用効果を呈する点でハードウェア資源との協働がなされていると主張するところ、同主張は、特許庁の審査基準において「ソフトウェアとハードウェア資源とが協働」しているとは、「所与の技術的作用効果を生じさせる点において論理としてのソフトウェアと物理的装置としてのハードウェア資源とが協働しているという意味」であるとの理解に基づくものと考えられる。

この点、審査基準（甲7）では、コンピュータ・ソフトウェア関連発明について、「『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』場合、当該ソフトウェアは『自然法則を利用した技術的思想の創作』である」とし、「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」場合とは、「ソフトウェアがコンピュータに読み込まれることにより、ソフトウェアとハードウェア資源とが協働した具体的手段によって、使用目的に応じた特有の情報処理装置（機械）又はその動作方法が構築されることをいう。」と説明している（6頁下5行～7頁3行）。これはコンピュータ・ソフトウェア関連発明に関する記載であるが、この考え方は、数学的課題の解決方法や数学的な計算手順に基づく処理がハードウェア資源を用いて実現されている場合に、「自然法則を利用した技術的思想の創作」であるか否か、すなわち特許法上の「発明」に該当するか否かを判断する場合にも適用可能なものであり、前記(1)で述べた「ケース3」に相当する。

審査基準の上記定義は、「ソフトウェアとハードウェア資源とが協働」していることをもって直ちに「自然法則を利用した技術的思想の創作」とするものではないが、「ソフトウェアとハードウェア資源とが協働」して

いることが、重要な判断基準であることは事実であり、原告が指摘するように、審査基準は「ソフトウェアとハードウェア資源とが協働」しているといえる場合についての一般的な定義を与えていない。

しかし、審査基準（甲7）は、第 部の例2（7頁下1行～8頁8行）及び事例2 - 1（20頁以下）において、「『コンピュータ』を用いるということだけでは、数式 $y = F(x)$ の最小値を求める処理とコンピュータとが協働しているとはいえない」（8頁5行～6行）、「計算装置によって計算するというだけでは、計算処理を実行するソフトウェアとハードウェア資源とが協働しているとはいえない」（22頁21行～22行）、「入力手段、演算手段、出力手段が含まれているものの、これらのハードウェア資源は乗算計算を実行するソフトウェアと何ら協働していない」（22頁下7行～下6行）との説明を与えているから、単なる入力、出力といった、通常の情報処理に付随する一般的な処理を除いた、その発明特有の処理がハードウェア資源を用いてどのように実現されているのかが特定されていないものを「ソフトウェアとハードウェア資源とが協働」していないものとしていることは明らかである。

ウ これに対し原告は、事例2 - 1の請求項2及び3に係る発明でも、演算内容に応じた計算装置の構成自体は特定されているが、審査基準がこの場合に協働しているといえないとする理由について必ずしも明らかにしていないとして、「ソフトウェアとハードウェア資源とが協働」しているとは、「所与の技術的作用効果を生じさせる点において論理としてのソフトウェアと物理的装置としてのハードウェア資源とが協働しているという意味」であるとの独自の解釈をする。

しかし、請求項に係る発明の認定は、請求項の記載に基づいて行わなければならないのであり、例えば、上記事例2 - 1の請求項2には、自然数 n と m との乗算 s を、特定の式によって計算する計算装置と記載されてい

のみであるから，上記事例 2 - 1 の請求項 2 及び 3 に係る発明でも，演算内容に応じた計算装置の構成自体は特定されているとする原告の上記主張は失当である。

第 4 当裁判所の判断

- 1 請求原因(1) (特許庁における手続の経緯)，(2) (発明の内容)，(3) (審決の内容) の各事実は，いずれも当事者間に争いが無い。

また甲 7 (審査基準 第 部第 1 章〔1 頁～6 2 頁〕) によれば，コンピュータ・ソフトウェア関連発明に関する特許庁の審査基準として，請求項に係る発明が特許法上の「発明」であるためには，その発明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であることが必要であるが，「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」場合は，当該ソフトウェアは「自然法則を利用した技術的思想の創作」であるとされ，そして，「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」とは，ソフトウェアがコンピュータに読み込まれることにより，ソフトウェアとハードウェア資源とが協働した具体的手段によって，使用目的に応じた情報の演算又は加工を実現することにより，使用目的に応じた特有の情報処理装置（機械）又はその動作方法が構築されることをいう，とされている。

- 2 原告は，本願発明が法 2 条 1 項に規定された「発明」に該当しないとした審決の判断に誤りがあると主張するので，以下この点について検討する。

(1) 法 2 条 1 項は，「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。」と規定し，法 2 9 条 1 項柱書は，「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。」と規定する。すなわち，法により特許として保護の対象とされる発明は，「自然法則を利用した技術的思想の創作」であることを要し，これを欠くときは，その発明は特許を受けることができ

ないと解される。

そこで、本願発明が「自然法則を利用した技術的思想の創作」に該当するかについて検討する。

(2) 本願発明の内容は前記第3の1(2)のとおりである。また第1次補正後の本願明細書(甲1, 4)には、次の記載がある。

ア 【発明の属する技術分野】

「本発明は、データ操作に関し、特に、長いデータストリングを短いデータストリングとして表現する効率的な技術に関する。」(段落【0001】)

イ 【従来技術】

(ア) 「ハッシュ法(ハッシング)は、長い長さのデータを短い長さのデータとして表現する技術である。この技術は、2つの相異なる長い長さのデータが同一の短い長さのデータとして表現される確率が比較的小さいようになっている。この特徴は、次の衝突確率で表される。

$$\Pr(h(m_1) = h(m_2)) = 1/2 \quad (1)$$

衝突確率は式(1)によって表される。式(1)は、ハッシュ関数hがストリング m_1 に作用した結果が、ハッシュ関数hがストリング m_2 に作用した結果に等しい確率が1/2すなわち以下であることを示す。

長い未ハッシュストリングに含まれるビット数はnであり、定義域と呼ばれる。短い、すなわち、ハッシュしたストリング内のビット数はmであり、しばしばハッシュ関数の値域という。式(1)を満たすハッシュ関数は、しばしば 普遍(universal)であるという。」(段落【0002】~【0005】)

(イ) 「 $\Pr(h(m_1) - h(m_2) = 0) = 1/2$ 」 (2)

一般にハッシュ関数に関連するもう1つの性質は式(2)によって表

される。式(2)は、ストリング m_1 に対するハッシュ関数 h の出力とストリング m_2 に対するハッシュ関数の出力との差がある所定の数に等しい確率が $1/2$ すなわち以下であることを示す。式(2)を満たすハッシュ関数を一般に 普遍 (universal) ハッシュ関数という。」(段落【0006】～【0007】)

$$(ウ) \quad \Pr(h(m_1) = c_1, h(m_2) = c_2) \leq 1/2 \quad (3)$$

また、あるハッシュ関数は、式(3)で示される第3の性質を有する。式(3)は、入力ストリング m_1 に対するハッシュ関数 h の出力がある所定の数 c_1 に等しく、かつ、入力ストリング m_2 に対するハッシュ関数 h の出力がある所定の数 c_2 に等しい同時確率が $1/2$ すなわち以下であることを示す。式(3)を満たすハッシュ関数を 強普遍 (strongly universal) であるという。式(3)を満たすハッシュ関数は自動的に式(1)および(2)を満たす。」(段落【0008】～【0009】)

(I) 「ハッシュ関数は多くの応用例で用いられる。そのうちの1つは、テキストストリングの探索を単純化することである。テキストストリングの探索に用いる場合、ハッシュ関数は、記憶される情報のサイズを縮小するために用いられ、その場合、同じハッシュ関数は、探索基準のサイズを縮小するために用いられる。そして、所望の情報を効率的に検索するために、縮小した探索基準を用いて、縮小した記憶情報を探索する。所望の情報が検索されると、短縮したテキストに対応する未ハッシュの、すなわち、完全な長さのテキストが与えられる。

また、ハッシュ関数は、ワイヤレス通信においてメッセージ認証のために用いられる。メッセージは、メッセージに対して暗号化関数を作用させることによって計算されるタグとともにメッセージストリングを送

信することによって認証される。メッセージストリングのタグを形成することは計算量が大きい。ハッシュ関数は、実行するのに必要な暗号化処理が少なくなるように、メッセージをタグへと短縮するために使用される。」(段落【0010】～【0011】)

ウ 【発明が解決しようとする課題】

「現在、...線形ハッシュ法や...MMHハッシュ法のような技術は、2つの相異なる長いストリングが同じ短いストリングを生成する確率が比較的小さい場合に、データやテキストの長いストリングを短いストリングとして表現するために使用される。このようなハッシュ関数は、長さwワードのキーと、長さwワードのハッシュされるべきメッセージあるいはテキストとの乗算を必要とする。その結果、1つのデータあるいはテキストのストリングのハッシュを実行するのに w^2 回の演算が必要となる。多くのワードを有する大きいデータあるいはテキストのストリングの場合、これは計算量の大きい演算となる。」(段落【0013】)

エ 【課題を解決するための手段】

(ア) 「本発明は、長さwワードのストリングをハッシュするのに、従来技術の w^2 回の演算ではなく、 $(w^2 + w) / 2$ 回の演算を使用する効率的なハッシュ法を提供する。本発明によれば、キーと、ハッシュされるべきストリングとの積をとるのではなく、キーと、ハッシュされるべきストリングの和を2乗することによって、この効率化を実現する。」(段落【0014】)

(イ) 「 $h(m) = ((m + a)^2 \bmod p) \bmod 2$ (6)

本発明の一実施例では、式(6)に示すように、メッセージmのハッシュは、メッセージストリングとキーストリングaとの和をとった後、その和の2乗をとることによって実行される。2乗演算の結果に対して法p演算(pを法とする剰余を求める演算)を実行し、法p演算の結果

に対して法 2 演算を実行する。この場合， m と a はいずれも同じ長さである。すなわち，長さ n ビットあるいは w ワードである。注意すべき点であるが， a は n ビットより長いことも可能であるが， n ビットであることが好ましい。値 h は，ハッシュの結果として得られる短縮されたストリングの長さのビット数であり，値域という。値 p は， 2^n より大きい最初の素数として選択される。ここで， n は，メッセージストリング m 内のビット数である。注意すべき点であるが，式(6)は，式(1)および(2)を満たすハッシュ法を提供する。すなわち，式(6)のハッシュ法は 普遍である。」(段落【0015】～【0016】)

$$(ウ) \quad h(m) = (((m + a)^2 + b) \bmod p) \bmod 2 \quad (7)$$

本発明の第2実施例では，強普遍ハッシュ法が提供される。この場合，メッセージストリング m とキー a の和をとった後，その結果として得られる和を2乗する。メッセージストリング m とキー a はいずれも，全部で n ビットを含み，長さ w ワードである。注意すべき点であるが，キー a は， n ビットより多くのビット数を含むことも可能であるが， n が好ましい。2乗演算の結果を，少なくとも長さ n ビットの第2のキー b と加算する。2乗項とキー b との和に対して，上記の式(6)の場合のように，法 p 演算を実行する。上記の式(6)の場合のように，法 p 演算の結果に対して法2演算を実行する。このハッシュ法を用いると，式(1)，(2)および(3)を満たす強普遍ハッシュ法が得られる。」(段落【0017】～【0018】)

(I) 「本発明のさらにもう1つの実施例では， k 個のメッセージあるいはストリングは，単一の短いストリングが生成されるようにハッシュされる。

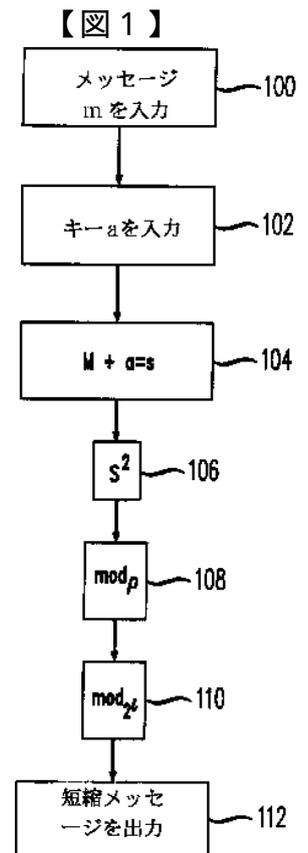
【数2】

$$h(m_1, \dots, m_k) = \left(\left(\sum_{i=1}^k (m_i + a_i)^2 \right) \bmod p \right) \bmod 2 \quad (8)$$

式(8)は、それぞれ長さwワードのk個のメッセージがハッシュされて単一の短いストリングを形成するようなハッシュ関数を例示している。各メッセージ m_i をキー a_i と加算し、その結果として得られる和を2乗する。各メッセージ m_i に対する2乗演算の結果を、k個のメッセージにわたって総和する。その総和に対して法p演算を実行し、法p演算の結果に対して法2演算を実行する。値pおよびは上記と同様に定義される。式(8)に例示したハッシュ法は、式(1)および(2)を満たす 普遍ハッシュ関数を提供する。」(段落【0019】~【0021】)

オ 【発明の実施の形態】

(ア) 「図1に、式(6)の2乗ハッシュ法を実行する方法を示す。ステップ100で、入力ストリングあるいはメッセージmを入力する。ステップ102で、入力キーaを入力する。メッセージあるいはストリングmと、キーaはそれぞれ、wワードからなり、長さnビットである。キーaは、乱数または擬似乱数であり、nビットより長いことも可能であるが、nビットが好ましい。ステップ104で、ストリングmとキーaの和sをとる。ステップ106で、和sを2乗する。ステップ108で、ステップ106の結果に対する法p演算を行う。pは、 2^n より大きい最初の素数である。pは、それより大きい素数とすることも可能であるが、性能が劣化する可能性がある。ステップ110で、ステップ108の結果に対して法2演算を実行する。は、短い出力メッセージあるいはストリング内のピ



ット数である。ステップ112で、法2演算の結果を出力する。図1のプロセスでは、 n ビットのメッセージあるいはストリングをビットのメッセージあるいはストリングに短縮したものが得られる。注意すべき点であるが、図1のプロセスは、式(1)および(2)の性質を満たす
普遍ハッシュ関数を実現する。」(段落【0022】)

(イ) 「図2に、式(7)によって記述される強普遍ハッシュ法を実行する方法を示す。ステップ140で、メッセージあるいはストリング m を入力する。ステップ142で、キー a および b を入力する。メッセージ m 、キー a および b はそれぞれ、 w ワードからなり、長さ n ビットである。ステップ144で、メッセージ m とキー a の和をとり、和 s として記憶する。ステップ146で、和 s の2乗を項 SQ として記憶する。ステップ148で、項 SQ とキー b の和をとる。ステップ150で、ステップ148により得られた結果に対して法 p 演算を実行する。この場合も、 p は、 2^n より大きい最初の素数である。 p は、それより大きい素数とすることも可能であるが、性能が劣化する可能性がある。ステップ152で、ステップ150からの結果に対して法2演算を実行する。 h は、この方法によって出力されるストリングあるいはメッセージ内のビット数に等しい。ステップ154で、長さ h の短いメッセージあるいはストリングを出力する。注意すべき点であるが、図2のプロセスは、式(1)、(2)および(3)の性質を満たす強普遍ハッシュ関数である。」(段落【0023】、なお【図2】は省略)

(ウ) 「図3に、式(8)によって記述される普遍ハッシュ法を実行する方法を示す。ステップ170で、インデックス i を1に等しいとセットし、変数 SUM を0に等しいとセットする。ステップ172で、 k の値を入力する。 k は、単一の短縮されたメッセージを生成するために入力されるストリングあるいはメッセージの数に等しい。ステップ174

で、メッセージあるいはストリング m_i が分離され、ステップ176で、入力キー a_i が入力される。注意すべき点であるが、メッセージあるいはストリング m_i と入力キー a_i の長さは等しく、 w ワードからなり、長さ n ビットである。キー a_i は、乱数または擬似乱数であり、 n ビットより長いことも可能であるが、 n ビットが好ましい。特に、 a_i は乱数であることが好ましい。乱数は、擬似乱数発生器のようなさまざまなソースから生成することが可能である。ステップ178で、メッセージ m_i とキー a_i の和をとることによって和 s_i を形成する。ステップ180で、 s_i の2乗を変数 SQ_i に等しいとセットする。ステップ182で、変数 SUM を、変数 SUM に SQ_i を加えたものに等しいとセットする。ステップ184で、 i の値をチェックし、これが値 k に等しいかどうかを判断する。値 k に等しくない場合、ステップ186で、インデックス i の値を1だけインクリメントした後、ステップ174を実行する。ステップ184で、 i の値が k に等しいと判断された場合、ステップ188で、変数 SUM の現在の値に対して法 p 演算を実行する。前述のように、 p は、 2^n より大きい最初の素数である。 p は、それより大きい素数とすることも可能であるが、性能が劣化する可能性がある。ステップ190で、ステップ188で得られた結果に対して法2演算を実行する。この場合も、 h は、出力ストリングあるいはメッセージを構成するビット数である。ステップ192で、 h ビットの短縮されたメッセージあるいはストリングを出力する。注意すべき点であるが、図3のプロセスは、それぞれ n ビットの k 個のメッセージを1個の h ビットのメッセージに短縮する。また、注意すべき点であるが、図3のハッシュ法は、式(1)および(2)の性質を満たす「普遍ハッシュ法である。」(段落【0024】、なお【図3】は省略)

カ 【発明の効果】

「以上述べたごとく，本発明によれば，長さwワードのストリングをハッシュするのに，従来技術の w^2 回の演算ではなく， $(w^2 + w) / 2$ 回の演算を使用する効率的なハッシュ法が実現される。」(段落【0033】)

(3) 以上によれば，本願発明1～3における「ビットの集まりを生成する装置」とは，nビットの集まりを入力してビットに短縮された演算結果を出力する装置であり，その過程においてハッシュ法，すなわち，「長い長さのデータを短い長さのデータとして表現する技術」(上記3(2)ア)が用いられているものである。

ここで用いられるハッシュ法は，「n」というデータを一定の法則に従って短縮化して表現しようとする場合に不可避免的に発生する短縮表現の衝突(n₁というデータを短縮した値m₁と，n₂というデータを短縮したm₂が等しくなってしまうこと)の確率を可能な限り小さくするという数学的な課題を有し，本願発明は，そのための計算手順(アルゴリズム)として，いずれも少なくともnビットを有するキー(a)と，入力されたnビットの集まりとの和をとり，前記和を2乗して，和の2乗を生成し，2ⁿより大きい最初の素数以上の素数pをもって，前記和の2乗に対して，法p演算を実行して法p演算結果を生成し，nより小さいにより，前記法p演算結果に対して，法2演算を実行して法2演算結果を生成し，前記法2演算結果を出力する，という各演算を含むものである。したがって，本願発明1～3はいずれも数学上の計算式，すなわちハッシュ関数として表現可能なものであり，実際にも，発明の詳細な説明においては，本願発明1は「 $h(m) = ((m + a)^2 \bmod p) \bmod 2$ 」(数式(6))，本願発明2は「 $h(m) = (((m + a)^2 + b) \bmod p) \bmod 2$ 」(数式(7))，また本願発明3は，「 $h(m_1, \dots, m_k) = \left(\left[\left(\sum_{i=1}^k (m_i + a_i)^2 \right) \bmod p \right] \bmod 2 \right)$ 」(数式(8))として，いずれも数学的な計算式として表現されているところ

である。

(4) ところで、上記数学的課題の解法ないし数学的な計算手順（アルゴリズム）そのものは、純然たる学問上の法則であって、何ら自然法則を利用するものではないから、これを法2条1項にいう発明ということができないことは明らかである。また、既存の演算装置を用いて数式を演算することは、上記数学的課題の解法ないし数学的な計算手順を実現するものにほかならないから、これにより自然法則を利用した技術的思想が付加されるものではない。したがって、本願発明のような数式を演算する装置は、当該装置自体に何らかの技術的思想に基づく創作が認められない限り、発明となり得るものではない（仮にこれが発明とされるならば、すべての数式が発明となり得べきこととなる。）。

この点、本願発明が演算装置自体に新規な構成を付加するものでないことは、原告が自ら認めるところであるし、特許請求の範囲の記載（前記第3，1(2)）をみても、単に「ビットの集まりの短縮表現を生成する装置」により上記各「演算結果を生成し」これを「出力している」とするのみであって、使用目的に応じた演算装置についての定めはなく、いわば上記数学的なアルゴリズムに従って計算する「装置」という以上に規定するところがない。

そうすると、本願発明は既存の演算装置に新たな創作を付加するものではなく、その実質は数学的なアルゴリズムそのものというほかないから、これをもって、法2条1項の定める「発明」に該当するということとはできない。

3(1) これに対し原告は、デジタル演算回路又はプロセッサの本来的ハードウェアの性質上、乗算回数が実質的に計算時間を決定することから、そのような計算時間を減らすことは、ハッシュ化の実際の応用（装置）にあつて要望される技術的課題であるとし、本願発明の技術的作用効果は、上記課題に対応した装置において計算時間を短縮させたことにあるなどと主張する。

しかし、原告の主張する上記技術的課題は、デジタル演算回路ないしプロ

セッサという装置自体が有する課題であって、演算される数式自体の有する課題ではないところ、計算装置の要する計算時間を短縮するために計算式を変更しても、当該演算装置自体の演算処理能力が改善されるものでないことは明らかである。原告の上記主張は、複雑なアルゴリズムよりも平易なアルゴリズムの方が演算時間が短かくて済むという、いわば数学的な常識を述べたものにすぎず、原告の主張する課題は依然として解決していないのであるから、失当といわなければならない。

なお原告は、本願発明は物理的な電気回路装置であり、かつ、当該アルゴリズムはコンピュータのような有限時間で動作する物理的構造上で実行されるからこそ上記技術的作用効果を有する点で、コンピュータ構造の本来的に有するハードウェア資源の物理的性質そのものに係るとして、本願発明が自然法則を利用した技術的思想に当たることになるとも主張するが、原告の上記主張は、数学的なアルゴリズムであってもコンピュータで演算を実行することで時間が短縮されれば発明になるというに等しく、自然法則を利用しない単なる数式を発明から除外する法2条1項の趣旨を没却するものであって、採用することができない。

(2) また原告は、「装置」の発明としての本願発明の具体的構成は、示された演算内容に応じて規定される演算回路として特許請求の範囲に明確に記載されている旨主張する。

しかし、前記2(3)及び(4)のとおり、特許請求の範囲には数学的なアルゴリズムと、それを実現するものとして単に「装置」と記載されているのみであって、当該数学的アルゴリズムをデジタル演算装置で演算するための具体的な回路構成が記載されているものではない。

また原告の上記主張は、特許請求の範囲にデジタル論理演算を意味する演算内容を記載すれば、これに対応した一般的なデジタル論理演算回路（布線論理回路と蓄積プログラム論理回路）によるプログラムが特定されるという

ものであるが、特許請求の範囲に記載された数学的アルゴリズムがデジタル論理演算回路に置換可能であるとしても、それはプログラム可能な数式一般の持つ特性にすぎず、既存の演算装置に新たな技術的思想に基づく創作が付加されることを直ちに意味するものではない。その意味で、特許請求の範囲に原告主張のデジタル論理演算回路による演算内容が記載されたことは、前記2(4)に述べたところを左右するものではない。

したがって、原告の上記主張は採用することができない。

(3) さらに原告は、本願発明には実用的な応用分野があり、例えば探索や通信等の技術分野に適用される、実用的で効率的なハッシュ装置を提供するものであると主張する。

しかし、本願発明1～3の特許請求の範囲をみても、ハッシュ関数によるアルゴリズムのほかには、単に「ビットの集まりの短縮表現を生成する装置」と記載するのみであって、当該装置がいかなる応用分野に適用されるものであるかを具体的に明らかにするところがない。また本願発明において入力されるものは「ビットの集まり」とされ、「キー」は「少なくとも n ビットを有する」ものとされ、「 p 」は「 $2n$ より大きい最初の素数以上の素数」とされ、「 r 」は「 n より小さい」とされているが、これらは数学的な関係を記述したにとどまり、原告の主張する応用分野におけるいかなる技術的思想に基づいてそのような数値が導き出されるかについて、何ら示唆するところがなく、それらの技術的意義を読み取ることができない。出力される「ビットの集まり」についても、衝突確率が所定以下となるという数学的な説明が与えられているにすぎない。そうすると、本願発明は、抽象的には原告の主張する分野において応用することが可能であるとしても、当該装置自体が直ちに具体的な技術的思想に基づき新たな創作を付加したものと解釈することはできないから、原告の上記主張は採用することができない。

(4) 以上のほか、原告は、審決が審査基準に基づき判断したことは、審査基準

に記載されていない場合の発明該当性の判断を看過するもので、審理不尽の違法があるなどと主張するが、審決は上記2(4)で述べたところと同旨の理由をもって本願発明の「発明」該当性を否定したものと認められるから、そこに審理不尽の違法は認められない。したがって、原告の上記主張も採用することができない。

4 結論

以上によれば、原告主張の取消事由は理由がない。

よって、原告の請求を棄却することとして、主文のとおり判決する。

知的財産高等裁判所 第2部

裁判長裁判官 中 野 哲 弘

裁判官 森 義 之

裁判官 澁 谷 勝 海