

審決

不服 2018-1783

(省略)

請求人 岩村 恵市

(省略)

代理人弁理士 特許業務法人太陽国際特許事務所

特願 2015-509790「処理装置及びプログラム」拒絶査定不服審判事件〔平成 26 年 10 月 9 日国際公開，WO 2014/162539〕について，次のとおり審決する。

結論

本件審判の請求は，成り立たない。

理由

第 1. 手続の経緯

本願は，2013 年 4 月 3 日を国際出願日とする出願であって，

平成 27 年 10 月 2 日付けで国内書面が提出され，平成 27 年 11 月 2 日付けで新規性喪失の例外適用申請書が提出され，平成 27 年 11 月 16 日付けで審査請求がなされると共に手続補正がなされ，平成 28 年 12 月 28 日付けで審査官により拒絶理由が通知され，これに対して平成 29 年 5 月 11 日付けで意見書が提出されると共に手続補正がなされたが，平成 29 年 10 月 30 日付けで審査官により拒絶査定がなされ，これに対して平成 30 年 2 月 7 日付けで審判請求がなされると共に手続補正がなされ，平成 30 年 5 月 18 日付けで審査官により特許法 164 条 3 項の規定に基づく報告がなされ，平成 30 年 6 月 1 日付け，及び，平成 30 年 11 月 14 日付けで上申書の提出がされ，その後，当審において，特許法 150 条 5 項の規定に基づき，請求人に対して，令和元年 8 月 21 日付け証拠調べ通知書によって通知し，令和元年 9 月 12 日付けで，意見書が提出されたものである。

第 2. 原審拒絶査定の拒絶の理由

原審における平成 29 年 10 月 30 日付けの拒絶査定（以下，これを「原審拒絶査定」という）における拒絶の理由は概略以下のとおりである。

1. （新規性）この出願の下記の請求項に係る発明は，その出願前に日本国内又は外国において，頒布された下記の刊行物 1 に記載された発明又は電気通信回線を通じて公衆に利用可能となった発明であるから，特許法 29 条 1 項 3 号に該当し，特許を受けることができない。

2. （進歩性）この出願の下記の請求項に係る発明は，その出願前に日本国内又は外国において，頒布された下記の刊行物 1 に記載された発明又は電気通

信回線を通じて公衆に利用可能となった発明に基づいて、その出願前にその発明の属する技術の分野における通常の知識を有する者が容易に発明をすることができたものであるから、特許法29条2項の規定により特許を受けることができない。

記

・請求項1ないし6

・引用文献等 1, 2

1. 高橋慧, 岩村恵市, クラウドコンピューティングに適した秘密分散法, 電子情報通信学会技術研究報告, 第112巻 第226号, 2012年9月27日, p.11-16

2. 電子情報通信学会, 原稿の提出について, [online], [2016年12月28日閲覧], インターネット

<URL:<https://www.ieice.org/jpn/kenkyuukai/geikou.html>>

・引用文献1は、その発行日である2012年9月27日に頒布され、その引用文献1に記載された発明は、同日に公知となったものと認められ、本願の出願日は、2013年4月3日であるから、本願発明について、引用文献1に記載された発明に対し、特許法第30条第2項の規定を適用することはできない。

第3. 新規性喪失の例外の適否における請求人の主張について

請求人は、平成30年2月7日付け審判請求書等において、引用文献1の発表日は平成24年10月4日であるところ、本願は当該発表日から6月以内に出願されているため、旧特許法30条2項（平成30年法律第33号改正前のもの、以下、これを「旧30条2項」という）の適用がある旨主張しており、その内容は、概略以下のとおりである。

1 平成29年5月11日付け意見書記載の主張

(1) 研究会の資料の信学技報は各研究会開催地に事前に発送する運用になっていたものの、紙媒体の引用文献1は全てガムテープで封印された段ボール箱に入った状態で当該研究会の当日まで保管されていた。したがって、紙媒体の引用文献1は、発行日以降、当該研究会の当日、すなわち、平成24年10月4日まで、「頒布」（特許法29条1項3号）されていない。

(2) 発表者への平成24年10月4日以前の配布はされていない。

(3) 定期購読者に対しても平成24年10月4日以前の配布はされていない。

(4) 他学会で平成24年10月4日以前の配布はされていない。

(5) Web等電子媒体での発行は当時されていない。技報オンラインサービスが開始されたのは、平成25年（2013年）4月からである。

(6) 引用文献2には、研究会資料（技術研究報告書）とその発行日について、発行日が公知日となる旨の記載がある。同様に、電子情報通信学会の特許証明に関する説明にも、「公知日（本会では、発行日※が公知日となります）」、「※発行日：本会論文誌においては、オンライン版が公開された日を公知日としています。」との記載がある。

ここで「オンライン版」とは、技報オンラインサービスであるところ、技報オンラインサービスが開始された平成25年（2013年）4月以降においては、技報の発行日（開催日の1週間前）が常に公知日とされたものである。

したがって、引用文献2等において、発行日が公知日となる旨の記載は、平成25年4月以前、すなわち、平成24年9月27日の時点では当てはまらない。

(7) よって、引用文献1の奥付には、2012年9月27日発行と記載されているものの、当該奥付記載の発行日には頒布されていない。引用文献1が頒布されたのは平成24年10月4日になってからである。

2 平成30年3月26日手続補正書記載の主張

平成27年11月16日付け上申書記載の主張に加えて、引用文献1の配布は、研究会当日の配布、発表者への事前配布、定期購読者への事前配布、他学会での配布、Web等電子媒体での発行以外に、存在していない。

したがって、引用文献1は、研究会当日（平成24年10月4日）まで頒布されていない。

3 平成30年11月14日付け上申書記載の主張

(1) 引用文献1は、以下のとおり取り扱われていたものである。

ア 平成24年10月4日開催の研究会の会場である幕張メッセを届け先とし、宛名を同研究会の世話人である西村明氏として発送

イ 平成24年9月27日電子情報通信学会事務局（機械振興会館）に直接納品

ウ 会場発送日以降(通常研究会開催月の月末)、引用文献1の年間購読者向けの学会発送委託業者である株式会社ASCに直接納品

上記アのルートで発送された引用文献1については、平成24年10月4日に、西村明氏によって研究会会場で配布された。

上記イのルートで納品された引用文献1は4冊で、全て電子情報通信学会事務局内に保管された。内1冊は閲覧用として管理されたが、平成24年9月27日から平成24年10月4日までの間に、引用文献1を閲覧する人物はいなかった。

上記ウのルートで納品された引用文献1については、平成24年11月中旬に、年間購読者宛てに発送された。

また、電子情報通信学会技術研究報告のオンライン公開サービスが開始されたのは、平成25年4月である。

(2) 引用文献1の取り扱いと、特許法29条1項3号の該当性との関係

ア 上記(1)イのルート

証明願中の引用文献1の奥付には、2012年9月27日発行と記載され、上記イのルートで納品された引用文献1の4冊の内、1冊は閲覧用として管理された。

具体的には、引用文献1は、2012年9月27日に、電子情報通信学会

(機械振興会館1階)の閲覧室に配架され、信学技報が閲覧可能な状況になった。電子情報通信学会における閲覧手続については、電子情報通信学芸誌の会告において公開されている。

しかし、電子情報通信学芸誌の購読者は多数ではないため、電子情報通信学会における閲覧手続を知る者は多数ではない。事実、平成24年9月27日から平成24年10月4日までの間に、引用文献1を閲覧する人物はいなかった。

このような状況から引用文献1は、平成24年9月27日から平成24年10月3日までの間、多数の者が閲覧し得る状態ではなかった。

特許法29条1項3号の「頒布された刊行物」に該当するためには、文書が、少なくとも多数の者が見得るような状態におかれなければならないと解すべきところ、上記の具体的事実を鑑みれば、引用文献1は、平成24年9月27日から平成24年10月3日までの間、多数の者が閲覧し得る状態ではなかった。多数の者が見得るような状態におかれていなかった。

よって、引用文献1の奥付に平成24年9月27日発行と記載されているものの平成24年9月27日から平成24年10月3日の間、引用文献1は、特許法29条1項3号の「頒布された刊行物」には該当していなかった。

イ 上記(1)アのルート

上記アのルートで発送された引用文献1は、西村明氏を宛名として発送されたものであって、平成24年10月4日に、西村明氏が研究会会場で受け取るように管理されていたものである。つまり、平成24年10月4日に西村明氏によって配布されるまで、不特定の者に開示されないように管理されていた。

よって、平成24年9月27日から平成24年10月3日の間、引用文献1は、特許法29条1項3号の「頒布された刊行物」には該当していない。

(3)以上より、引用文献1は、平成24年10月4日になって初めて、特許法29条1項3号の「頒布された刊行物」に該当するに至ったものである。

そして、本願は、平成24年10月4日から6月以内に出願されている。

以上より、本願発明について、引用文献1に記載された発明に対し、特許法30条2項の規定を適用することができる。

第4. 当審における証拠調べ通知の要旨

当審において、本願が、旧30条2項に該当するか否かについて、職権に基づく証拠調べをした結果、下記に示すとおり証拠を発見したので特許法150条5項の規定に基づき、請求人に対して、令和元年8月21日付け証拠調べ通知書によってより請求人に通知し、期間を指定してこれに対する意見を求めた。

記

1 一般社団法人電子情報通信学会のウェブサイト

「（省略）」

2 令和元年7月12日付け審判長仲間晃から電子情報通信学会宛のメール文書

「（省略）」

3 令和元年7月12日付け電子情報通信学会から審判長仲間晃宛のメール文書

「（省略）」

第5. 職権証拠調べ通知に対する請求人の意見の要旨

前記第4. の証拠調べ通知に対して、請求人は、令和元年9月12日付け意見書において、引用文献1が「頒布された刊行物」（特許法29条1項3号）に該当するためには、「不特定多数の者が見得るような状態におかれる」ことが必要であると主張したうえで、大要、以下のとおり主張している。

1 引用文献1を閲覧・複写の手続きをできる人は、第1に、電子情報通信学芸誌を購入した会員である「特定の者」である。第2に、非会員であっても引用文献1を閲覧・複写の手続きをできる人は、会員である特定の者から電子情報通信学芸誌を譲り受けた者または閲覧等した者であり、「特定の者」である。

2 引用文献1を閲覧・複写の手続きをできる人は、第1に、電子情報通信学芸誌を購入した会員、第2に、非会員の内、会員である特定の者から電子情報通信学芸誌を譲り受けた者または閲覧等した者であり、多数ではない。実際、平成24年9月27日から同年10月4日までの間に、引用文献1を閲覧した人はいなかったため、「多数の者」が見得るような状態におかれていないから、引用文献1は「頒布された刊行物」には該当しない。

第6. 新規性喪失の例外の適否についての当審の判断

旧30条2項は、特許を受ける権利を有する者の行為に起因して特許法29条1項各号のいずれかに該当するに至った発明について、その該当するに至った日から6月以内にその者が特許出願することを要件としているところ、請求人は以下のとおり、特許法29条1項3号に該当するに至ってから6月以内に本願を出願したと認められない。

1 「頒布された刊行物」の意義

特許法29条1項3号の「頒布された刊行物」とは「公衆に対し、頒布により公開することを目的として複製された文書・図画等の情報伝達媒体であって、頒布されたものを指すところ、ここに公衆に対し頒布により公開することを目的として複製されたものであるということが出来るものは、必ずしも公衆の閲覧を期待してあらかじめ公衆の要求を満たすことができるとみられる相当程度の部数が原本から複製されて広く公衆に提供されているようなものに限られる

としなければならないものではなく、右原本自体が公開されて公衆の自由な閲覧に供され、かつ、その複写物が公衆からの要求に即応して遅滞なく交付される態勢が整っているならば、公衆からの要求をまつてその都度原本から複写して交付されるものであつても差し支えないと解するのが相当である」（最判昭和55年7月4日民集34巻4号570頁）。

2 これを本件についてみると、以下の事実が認められる。

(1) 引用文献1は、「信学技報」と題して定期的に刊行される論文誌であり、定期購読者へ配布するとともに電子情報通信学会の専門委員会の一つであるマルチメディア情報ハイディング・エンリッチメント研究専門委員会が主催した研究会（以下、これを「EMM研究会」という）において配布されている冊子である（西村明の陳述書（請求人意見書添付の証拠1））。

(2) 引用文献1の奥付には、発行日が平成24年9月27日（2012年9月27日）との記載がある。

(3) 平成30年11月15日付け手続補足書添付の平成30年10月30日付け証明願によれば、引用文献1は、印刷所からの発送・納品ルートとして「(2)平成24年(2012年)9月27日電子情報通信学会事務局（機械振興会館）に直接納品」というルートが存在したとともに、上記「(2)・・・納品」のルートで納品された引用文献1は、平成24年9月27日の時点で、4冊全て事務局内に保管され、内1冊は閲覧用として管理されていたことが認められ、この事実は同日付け上申書において請求人自身も自認しているところである。

(4) 上記引用の「一般社団法人電子情報通信学会のウェブサイト」によると、同学会において、「電子情報通信学会技術研究報告」という報告集が発行されているところ、同報告集の冊子は、非会員でも300円で閲覧可能で、さらに1枚10円で複写も可能である。

(5) (4)の事実と同じように、引用文献1は、平成24年9月27日の時点でも、電子情報通信学会の非会員であっても閲覧及び複写が可能であった（令和元年7月12日付審判長仲間晃から電子情報通信学会宛のメール文書及び令和元年7月12日付電子情報通信学会から審判長仲間晃宛のメール文書）。

3 以上2の事実を総合すると、定期的に刊行される論文誌である引用文献1は、発行日である平成24年9月27日の時点で、電子情報通信学会事務局に対して要求があれば、誰でも閲覧及び複写が可能であったと言える。

つまり、引用文献1は、定期的に刊行される論文誌であることから「公衆に対し、頒布により公開することを目的として複製された文書・図画等の情報伝達媒体」であるうえに、平成24年9月27日の時点において誰でも閲覧及び複写が可能であったのであるから「公開されて公衆の自由な閲覧に供され、かつ、その複写物が公衆からの要求に即応して遅滞なく交付される態勢が整つてい」たこと、すなわち「頒布された刊行物」（特許法29条1項3号）に該当するに至っていたと認められる。

よって、引用文献1は、本願の国際出願日（2013年4月3日）の6月より前の平成24年9月27日に、「頒布された刊行物」に該当するに至ったものということができる。

したがって、旧30条2項は、特許を受ける権利を有する者の行為に起因して特許法29条1項各号のいずれかに該当するに至った発明について、その該当するに至った日から6月以内にその者が特許出願することを要件としているところ、本願は特許法29条1項3号に該当するに至ってから6月以内に本願を出願したと認められないため、旧30条2項に規定する新規性喪失の例外適用は認められない。

4 審判請求人の主張について

(1) 請求人は、引用文献1が頒布されるに至った日時は平成24年10月4日である旨を縷々主張しているところ、その主張は概略以下のとおりである。

ア 引用文献1の配布は、研究会当日の配布、発表者への事前配布、定期購読者への事前配布、他学会での配布、Web等電子媒体での発行以外に存在していないところ、引用文献1は平成24年10月4日に至って初めて配布された(平成29年5月11日付け意見書及び平成30年3月26日付け手続補正書)。

イ 特許法29条1項3号の「頒布された刊行物」に該当するためには、文書が、少なくとも多数の者が見得るような状態におかれなければならないと解すべきところ、引用文献1を電子情報通信学会事務局で閲覧・複写の手続きをできた人は特定の者であって、かつ、「多数」ではないから、平成24年9月27日から平成24年10月3日までの間において引用文献1は「頒布された刊行物」に該当していない(平成30年11月14日付け上申書)。

(2) 請求人の主張についての当審の判断

引用文献1が頒布されるに至った日時については、「第6. 新規性喪失の例外の適否について」の1～3において検討したとおりである。

よって、請求人の主張はいずれも採用できない。

5 小括

そうすると、引用文献1は、平成24年9月27日には特許法29条1項3号の『頒布された刊行物』に該当するに至っていたのであるから、その該当する日から6月以内、すなわち、平成25年3月27日が満了するまで(特許法3条1項1号、2号)に本願が出願されなければ旧30条2項が適用されないところ、本願の出願日は、平成25年4月3日であるから、旧30条2項は適用されない。

第7. 本願発明について

本願の請求項1に係る発明(以下、これを「本願発明」という)は、平成29年5月11日付けの手続補正により補正された特許請求の範囲の請求項1に記載された、次のとおりのものである。

「秘密情報をn個に分散し、そのうちk個の分散値を集めれば秘密情報を復元でき、k-1個以下では秘密情報を復元できないシステムにおいて、

秘密情報を特定する情報を記憶する記憶手段と、
分散値を得るために設定手段により設定された鍵情報を用いて、前記記憶手段に記憶された前記秘密情報を特定する情報を暗号化する暗号化手段と、
を備えることを特徴とした処理装置。」

第8. 引用文献に記載の事項

原審における平成28年12月28日付けの拒絶理由（以下、これを「原審拒絶理由」という）において、引用文献1として引用された文献であって、上記「第3. 新規性喪失の例外適用申請の適否について」に検討したとおり、本願の国際出願日前に公知となった文献である、「1. 高橋慧, 岩村恵市, 「クラウドコンピューティングに適した秘密分散法」, 電子情報通信学会技術研究報告, 第112巻 第226号, 2012年9月27日, p.11-16」（以下、これを「引用文献」という）には、関連する図面と共に、次の事項が記載されている。

A. 「秘密分散法とは n 個に分散したデータ内、 k 個 ($k \leq n$) のデータを集めることで元の秘密情報が復元できるという技術であり、 k 個未満のデータから一切秘密情報に関する情報は得られないという技術である。」（11頁左欄13行～17行）

B. 「3. 提案方式

ここではクラウドコンピューティングへの適用に適した秘密分散法である提案方式についての説明を行う。提案方式は図1の様に構成されるクラウドシステムに適した秘密分散法である。

3. 1 提案方式の構成

まず、それぞれの秘密情報 s_i ($i = 1 \dots m$) について以下の分散式を生成する。

$$W_{ij} = s_i + a_{i1} x_j + a_{i2} x_j^2 + \dots + a_{ik-1} x_j^{k-1} \quad (1)$$

ここで、 x_j は各サーバに割り当てられるIDであり、 W_{ji} はサーバID x_j を利用して生成した秘密情報 s_i の分散情報である。また、それぞれの秘密情報に割り振られているデータID $dID[s(i)]$ は秘密情報のデータサイズよりも小さいものとする。

本提案方式はユーザが鍵情報のみを持つ鍵サーバに自身のユーザID $ID[y]$ ($y = 1, \dots, r$) を送信し、それを受け取った鍵サーバが自身の持つ key_j と受け取ったユーザIDを用いて $Eid(y, j) = Enc(ID[y], key_j)$ ($j = 1 \dots l$) を生成してユーザに送信する。ここで $Enc(a, b)$ は a を b という鍵を用いて暗号化する処理を表すとする。ユーザがこれを用いて自身のデータ $dID[s(i)]$ を暗号化し暗号化結果

$q_{ij} = Enc(dID[s(i)], Eid(y, j))$
を m 個の秘密情報全てについて生成したのち、これらが鍵サーバの分散情報に対応するように $W_{1j} = q_{1j}$, $W_{2j} = q_{2j}$, \dots , $W_{mj} = q_{mj}$ と

してそれぞれの秘密情報 s_i ($i = 1 \dots m$) に関する分散係数 $A' = [\alpha_{i1}, \dots, \alpha_{ik-1}]^T$ を求める。」(13頁左欄21行~右欄15行)

C. 「(5) また、ユーザはデータサーバ x_{l+1}, \dots, x_n に関する分散情報 W_{l+1}, \dots, W_n を(4)で生成した係数行列を利用して (k, n) 閾値秘密分散法と同様の手順により算出する。」(13頁右欄下から3行~14頁左欄1行)

第9. 引用文献に記載の発明

1 上記Aの「秘密分散法とは n 個に分散したデータ内、 k 個 ($k \leq n$) のデータを集めることで元の秘密情報が復元できるという技術であり、 k 個未満のデータから一切秘密情報に関する情報は得られないという技術である」という記載、及び、上記Bの「提案方式は図1の様に構成されるクラウドシステムに適した秘密分散法である」という記載から、引用文献には、
“ n 個に分散したデータ内、 k 個 ($k \leq n$) のデータを集めることで元の秘密情報が復元でき、 k 個未満のデータから一切秘密情報に関する情報は得られないクラウドシステム”が記載されていることが読み取れる。

2 上記Bの「 x_j は各サーバに割り当てられるIDであり、 W_{ji} はサーバID x_j を利用して生成した秘密情報 s_i の分散情報である」という記載、同じく、上記Bの「それぞれの秘密情報に割り振られているデータID $dID[s(i)]$ 」という記載、同じく、上記Bの「本提案方式はユーザが鍵情報のみを持つ鍵サーバに自身のユーザID $ID[y]$ ($y = 1, \dots, r$) を送信し、それを受け取った鍵サーバが自身の持つ key_j と受け取ったユーザIDを用いて $Eid(y, j) = Enc(ID[y], key_j)$ ($j = 1 \dots l$) を生成してユーザに送信する。ここで $Enc(a, b)$ は a を b という鍵を用いて暗号化する処理を表すとする」という記載、同じく、上記Bの「ユーザがこれを用いて自身のデータID $dID[s(i)]$ を暗号化し暗号化結果 $q_{ij} = Enc(dID[s(i)], Eid(y, j))$ を m 個の秘密情報全てについて生成」という記載、同じく、上記Bの「これらが鍵サーバの分散情報に対応するように $W_{1j} = q_{1j}, W_{2j} = q_{2j}, \dots, W_{mj} = q_{mj}$ としてそれぞれの秘密情報 s_i ($i = 1 \dots m$) に関する分散係数 $A' = [\alpha_{i1}, \dots, \alpha_{ik-1}]^T$ を求める」という記載、及び、上記Cの「ユーザはデータサーバ x_{l+1}, \dots, x_n に関する分散情報 W_{l+1}, \dots, W_n を(4)で生成した係数行列を利用して (k, n) 閾値秘密分散法と同様の手順により算出する」という記載から、引用文献には、
“ユーザが鍵情報のみを持つ鍵サーバに自身のユーザIDを送信し、鍵サーバは、受信したユーザIDを、鍵サーバの有する鍵で暗号化し、得られた値を前記ユーザに送信し、前記ユーザは、鍵サーバから送信された値を用いて、自身の有する m 個の秘密情報それぞれに割り振られているデータIDを暗号化し、得られた値を用いて、分散情報の分散係数を生成し、前記分散係数の係数行列を用いて、分散情報を計算するクラウドシステム”が記載されていることが読

み取れる。

3 以上、上記1及び上記2において検討した事項から、引用文献には、次の発明（以下、これを「引用発明」という）が記載されていることが読み取れる。

“n個に分散したデータ内、k個（ $k \leq n$ ）のデータを集めることで元の秘密情報が復元でき、k個未満のデータから一切秘密情報に関する情報は得られないクラウドシステムであって、

ユーザが鍵情報のみを持つ鍵サーバに自身のユーザIDを送信し、鍵サーバは、受信したユーザIDを、鍵サーバの有する鍵で暗号化し、得られた値を前記ユーザに送信し、前記ユーザは、鍵サーバから送信された値を用いて、自身の有するm個の秘密情報それぞれに割り振られているデータIDを暗号化し、得られた値を用いて、分散情報の分散係数を生成し、前記分散係数の係数行列を用いて、分散情報を計算する、クラウドシステム。”

第10. 本願発明と引用発明との対比及び当審の判断

1 引用発明における「分散情報」、「秘密情報」が、本願発明における「分散値」、「秘密情報」に相当し、

引用発明における「n個に分散したデータ内」から、引用発明においても、「秘密情報」を「n個」に分割していることは明らかであって、

引用発明における「クラウドシステム」が、本願発明における「システム」に相当するので、

引用発明における「n個に分散したデータ内、k個（ $k \leq n$ ）のデータを集めることで元の秘密情報が復元でき、k個未満のデータから一切秘密情報に関する情報は得られないクラウドシステム」が、

本願発明における「秘密情報をn個に分散し、そのうちk個の分散値を集めれば秘密情報を復元でき、k-1個以下では秘密情報を復元できないシステム」に相当する。

2 引用発明において、「自身の有するm個の秘密情報それぞれに割り振られているデータID」は、当該「データID」を記憶するための手段が存在することは明らかである。

そして、引用発明における「自身の有するm個の秘密情報それぞれに割り振られているデータID」が、

本願発明における「秘密情報を特定するための情報」に相当するので、

引用発明における“自身の有するm個の秘密情報それぞれに割り振られているデータIDを記憶する手段”が、

本願発明における「秘密情報を特定する情報を記憶する記憶手段」に相当する。

3 引用発明においては、「鍵サーバは、受信したユーザIDを、鍵サーバの有する鍵で暗号化し」、「得られた値」で、「データIDを暗号化」している

ので、

引用発明における“鍵サーバにおいて得られる値”が、

本願発明における「設定手段により設定された鍵情報」に相当し、

そして、引用発明において、当該「暗号化」をするための「手段」が存在することは明らかであるから、

引用発明において、「鍵サーバから送信された値を用いて、自身の有するm個の秘密情報それぞれに割り振られているデータIDを暗号化」する「手段」が、

本願発明における「設定手段により設定された鍵情報を用いて、前記記憶手段に記憶された前記秘密情報を特定する情報を暗号化する暗号化手段」に相当する。

4 引用発明において、「ユーザ」が、「鍵サーバから送信された値を用いて、自身の有するm個の秘密情報それぞれに割り振られているデータIDを暗号化」することは、「分散情報」を計算するために行っていることであるから、上記3において検討した事項と併せると、

引用発明における「得られた値を前記ユーザに送信し、前記ユーザは、鍵サーバから送信された値を用いて、自身の有するm個の秘密情報それぞれに割り振られているデータIDを暗号化」する「手段」は、

本願発明における「分散値を得るために設定手段により設定された鍵情報を用いて、前記記憶手段に記憶された前記秘密情報を特定する情報を暗号化する暗号化手段」に相当する。

5 引用発明において、「自身の有するm個の秘密情報それぞれに割り振られているデータID」は、「ユーザ」側に保持され、「データIDを暗号化」することは、「ユーザ」側で行われているので、「データID」を“記憶する手段”と、「データIDを暗号化する」手段が、「ユーザ」の装置に存在することは、明らかである。

よって、上記3及び4において検討した事項を踏まえると、

当該5の上記において検討した、引用発明における「ユーザ」の装置が、本願発明における「処理装置」に相当する。

6 以上、上記1～上記5において検討した事項から、本願発明と、引用発明とは、

「秘密情報をn個に分散し、そのうちk個の分散値を集めれば秘密情報を復元でき、k-1個以下では秘密情報を復元できないシステムにおいて、

秘密情報を特定する情報を記憶する記憶手段と、

分散値を得るために設定手段により設定された鍵情報を用いて、前記記憶手段に記憶された前記秘密情報を特定する情報を暗号化する暗号化手段と、

を備えることを特徴とした処理装置。」

である点で一致する。

よって、本願発明は、引用文献に記載された発明である。

そして、本願発明が、引用文献に記載された発明である以上、引用文献に記載の発明から、本願発明を構築することは、当業者であれば容易になし得る事項である。

第11. むすび

したがって、本願発明は、引用文献に記載された発明であるから、特許法29条1項3号の規定により、特許を受けることができない。

加えて、本願発明は、引用文献に記載された発明に基づいて、当業者が容易に発明をすることができたものであるので、特許法第29条第2項の規定により特許を受けることができない。

よって、結論のとおり審決する。

令和1年12月17日

審判長 特許庁審判官 仲間 晃
特許庁審判官 石井 茂和
特許庁審判官 山崎 慎一

(行政事件訴訟法第46条に基づく教示)

この審決に対する訴えは、この審決の謄本の送達があった日から30日（附加期間がある場合は、その日数を附加します。）以内に、特許庁長官を被告として、提起することができます。

〔審決分類〕 P18. 113-Z (G09C)

審判長 特許庁審判官 仲間 晃 8834
特許庁審判官 山崎 慎一 9174
特許庁審判官 石井 茂和 8837